IIR

Internet
Infrastructure
Review

Sep.2025
Vol. 67

定期観測レポート(1)

ブロードバンドトラフィックレポート ～トラフィックは安定成長が継続～

定期観測レポート(2)

「ディフェンス対応」の効果と 送信ドメイン認証(ARC)に対するIIJの対応

フォーカス・リサーチ(1)

脱VMwareへの回答 ～ Kubernetesと仮想環境の親密な関係～

フォーカス・リサーチ(2)

3G停波とMVNO

IIJ
Internet Initiative Japan

Internet Infrastructure Review

September 2025 Vol.67

エグゼクティブサマリ

「IIR (Internet Infrastructure Review)」は、IIJが2008年から四半期ごとに発行している技術情報誌です。本号(Vol.67)より「エグゼクティブサマリ」の執筆を前任の島上に替わり、染谷が担当します。以下、本号の内容について紹介します。

第1章「定期観測レポート(1)」では、IIJが運用するブロードバンド・モバイルサービスのトラフィック動向を詳細に分析しています。2024年から25年にかけても、トラフィックは全体として安定的な成長を続けており、利用傾向に大きな変化は見られませんでした。ただし、近年利用が拡大しているAIの普及がもたらすトラフィックへの影響は今のところ限定的ですが、今後も引き続き注視が必要です。

第2章「定期観測レポート(2)」では、IIJが2024年から本格導入した「ディフェンス対応」について報告しています。これは、従来のabuse(迷惑行為)対策を進化させ、悪意ある通信を事前に検知・遮断することで、利用者や社会全体の安全性を高めるものです。実際にディフェンス対応を導入したことで、迷惑メールやフィッシング攻撃の被害件数が大幅に減少し、IIJのメールサービスの信頼性も大きく向上しています。また、送信ドメイン認証(SPF、DKIM、DMARC、ARC)や経路暗号化(STARTTLS)の普及状況も分析し、国内外の最新動向を紹介しています。

第3章「フォーカス・リサーチ(1)」では、VMware問題を契機とした仮想化基盤の見直しや、Kubernetesを活用した次世代プラットフォームへの移行について、IIJの現場における実践と課題を解説しています。VMwareのライセンス価格高騰を受け、IIJでは自社開発のKubernetesディストリビューション「IKE(IIJ Kubernetes Engine)」をVMwareの代替として本格導入し、コスト削減、運用効率化、品質向上を図っています。本来Kubernetesはコンテナのオーケストレータでしたが、コンテナとVMを用途に応じて使い分ける混在環境での活用により、将来性を有した選択肢としてサービス価値の源泉になると考えられます。

第4章「フォーカス・リサーチ(2)」では、2026年3月末に予定されているNTTドコモの3Gサービス終了に向けたIIJの取り組みを解説しています。3G停波は、MVNO事業者や利用者にとって、音声通話、SMS、データ通信などに影響が出る可能性があります。IIJでは早期から技術的・運用的な課題を洗い出し、4G/5Gへ円滑に移行できるよう支援・準備を進めています。今回は特に、端末の実装内容に応じた動作の違いを解説し、具体的な対応方法も示しています。

「IIR」では、IIJのエンジニアが日々直面する課題や社会インフラを支える現場のリアルな声を通して、読者の皆様に新たな気づきや示唆を提供することを目指しています。変化の激しい時代において、IIJは「技術で社会を支える」という使命を胸に挑戦と進化を続けてまいります。

染谷 直(そめや なおし)

IIJ常務執行役員 ネットワークサービス事業本部 クラウド本部長。1998年、IIJ入社。直後にIIJテクノロジー(2010年にIIJに吸収合併)へ出向。IIJテクノロジーではSI事業の立ち上げに携わり、多くのインターネットシステムの構築やコンサルティングに従事。その後、16年よりIIJのサービス事業部門に異動し、クラウド事業の中期事業戦略を担当。19年、クラウド事業責任者に就任。今年度より「IIR」編集長に就き、IIJにおけるリアルな技術情報を横断的かつ積極的に読者の皆様へお届けしたいと考えている。

ブロードバンドトラフィックレポート ～トラフィックは安定成長が継続～

1.1 概要

このレポートでは、毎年IIJが運用しているブロードバンド接続サービスのトラフィックを分析して、その結果を報告しています[*1*2*3*4*5]。今回も、利用者の1日のトラフィック量やポート別使用量などを基に、この1年間のトラフィック傾向の変化を報告します。

全体として、過去数年と同様に、今年もトラフィックは安定した成長が続いています。今のところその傾向に目立った変化は見られません。

図-1は、IIJの固定ブロードバンドサービス及びモバイルサービス全体について、月ごとの平均トラフィック量の推移を示したグラフです。トラフィックのIN/OUTはISPから見た方向を表し、INは利用者からのアップロード、OUTは利用者へのダウンロードとなります。トラフィック量の数値は開示できないため、新型コロナ感染拡大前の2020年1月の両サービスのOUTの値を1として正規化しています。

この1年のブロードバンドトラフィック量は、INは9%の増加、OUTは4%の増加となっています。1年前はそれぞれ14%と12%でしたので、増加率は少し下がりました。ブロードバンドに関しては、IPv6・IPoEのトラフィック量も含めて示しています。IIJのブロードバンドにおけるIPv6は、IPoE方式とPPPoE方式があります。2025年6月時点で、IPoEのブロードバンドトラフィック量の全体に占める割合は、INで42%、OUTで49%と、全体の5割弱がIPoEとなっています。増加率は、昨年同月よりINで1ポイント減少、OUTで1ポイント増加とほとんど変化なく、IPoEへの移行が一巡したようです。

モバイルサービスは、コロナ禍の最初1年ほどは外出が減ったことで、トラフィックは横ばいでしたが、その後は増加傾向が続いています。モバイルはこの1年でINは29%、OUTは9%の増加となっています。1年前はそれぞれ29%と20%でした。モバイルサービスのINの比率が高いのは、アップロードが多い法人向けサービスの影響で、個人向けサービスに限ればIN比率はブロードバンド同様1/10程度です。

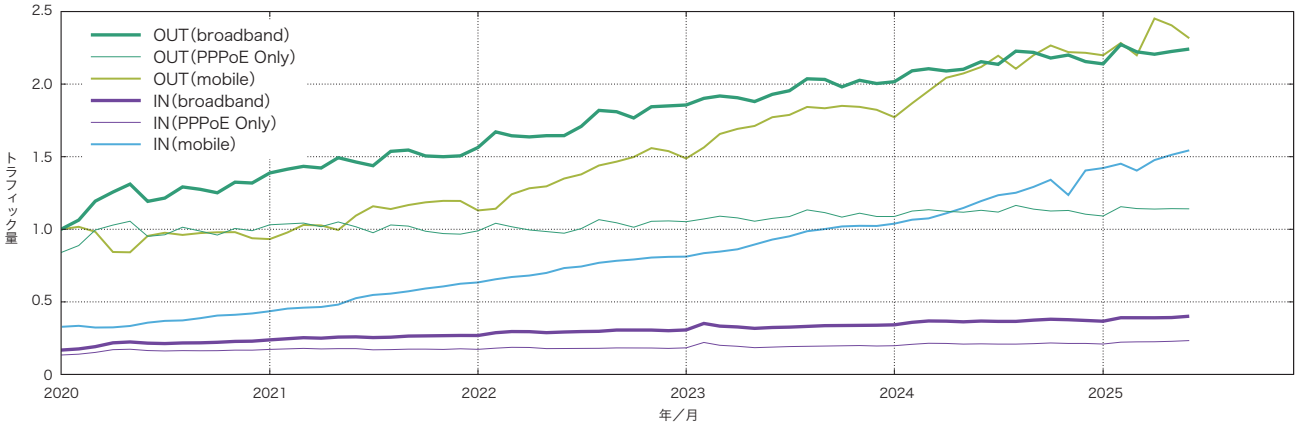


図-1 ブロードバンド及びモバイルの月間トラフィック量の推移

＊1　長健二朗. ブロードバンドトラフィックレポート: この5年間を振り返って. Internet Infrastructure Review. vol.64. pp4-11. September 2024.
＊2　長健二朗. ブロードバンドトラフィックレポート: コロナ禍を経てトラフィックは安定増加傾向. Internet Infrastructure Review. vol.60. pp4-11. September 2023.
＊3　長健二朗. ブロードバンドトラフィックレポート: コロナ禍3年目のトラフィックは小康状態. Internet Infrastructure Review. vol.56. pp4-11. September 2022.
＊4　長健二朗. ブロードバンドトラフィックレポート: 2年目に入ったコロナ禍の影響. Internet Infrastructure Review. vol.52. pp4-11. September 2021.
＊5　長健二朗. ブロードバンドトラフィックレポート: 新型コロナウイルス感染拡大の影響. Internet Infrastructure Review. vol.48. pp4-9. September 2020.

次に、この1年の平日の時間別ブロードバンドトラフィック量の推移を見ていきます。図-2に、昨年6月初旬の週から約4ヵ月おきに4つの週を選んで、各週の月曜から金曜の各時間の平均トラフィック量を示します。ここ数年学校が休みの時期は平日昼間のトラフィック量が増えるようになったので、学期途中の週を選んでいます。ここでのトラフィック量はPPPoEとIPoEの合計値です。下側の破線はそれぞれの週のアップロード量ですが、今回もダウンロード量に注目すると、夜中から早朝にかけてはトラフィック量はあまり増えていないものの、午前から夜にかけた時間帯においては着実に増えてきています。

1.2 データについて

今回も前回までと同様に、ブロードバンドに関しては、個人及び法人向けのブロードバンド接続サービスについて、ファイバーとDSLによるブロードバンド顧客を収容するルータで、Sampled NetFlowにより収集した調査データを利用しています。モバイルに関しては、個人及び法人向けのモバイルサービスについて、使用量にはアクセスゲートウェイの課金用情報を、使用ポートにはサービス収容ルータでのSampled NetFlowデータを利用しています。

トラフィックは平日と休日で傾向が異なるため、1週間分のトラフィックを解析します。今回は、2025年6月2日～6月8日の1週間分のデータを解析して、前回解析した2024年6月3日～6月9日の1週間分と比較します。

ブロードバンドの集計は契約ごとに行い、一方モバイルでは複数電話番号の契約があるので電話番号ごとの集計となっています。ブロードバンド各利用者の使用量は、利用者に割り当てられたIPアドレスと、観測されたIPアドレスを照合して求めています。なお、IPoEトラフィックはインターネットマルチフィード社のtransixサービスを利用していて詳細なデータが取得できていないため、ポート別解析の対象にはなっていません。

1.3 利用者の1日の使用量

まずは、ブロードバンド及びモバイル利用者の1日の利用量をいくつかの切り口から見ていきます。ここでの1日の利用量は各利用者の1週間分のデータの1日平均です。

2019年のレポートから、利用者の1日の使用量は個人向けサービス利用者のデータのみを使っています。これは、利用形態が多様な法人向けサービスを含めると分布の歪みが大きくなってしまうため、全体の利用傾向を掴むには個人向けサービス分だけを対象にした方が、より一般性があり分かりやすいと判断したからです。なお、次節のポート別使用量の解析では区別が難しいため法人向けも含めたデータを使っています。また、2021年からブロードバンドにはIPoEの利用者のデータも加えて、PPPoEとIPoEを統合してブロードバンドとして示しています[*6]。

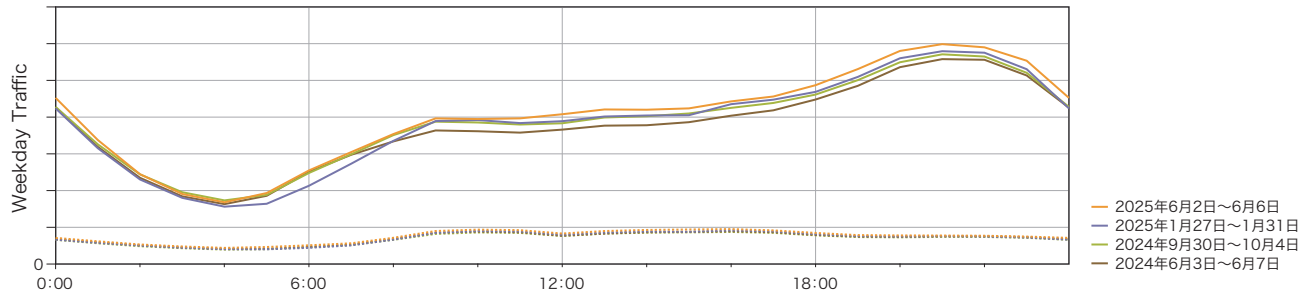


図-2 この1年の平日時間別ブロードバンドトラフィック量の推移

＊6　利用者がPPPoEとIPoEの両方を使っている場合はそれぞれ別の利用者として扱われています。

図-3及び図-4は、ブロードバンドとモバイル利用者の1日の平均利用量の分布（確率密度関数）を示します。アップロード（IN）とダウンロード（OUT）に分け、利用者のトラフィック量をX軸に、その出現確率をY軸に示していて、2024年と2025年を比較しています。X軸はログスケールで、10KB（10^4）から1TB（10^{12}）の範囲を示しています。一部の利用者はグラフの範囲外にありますが、おおむね1TB（10^{12}）までの範囲に分布しています。

図中のINとOUTの各分布は、片対数グラフ上で正規分布となる対数正規分布に近い形をしています。これはリニアなグラフで見ると、左端近くにピークがある、いわゆるロングテールな分布です。OUTの分布はINの分布より右にずれていて、ダウンロード量がアップロード量より1桁以上大きくなっています。

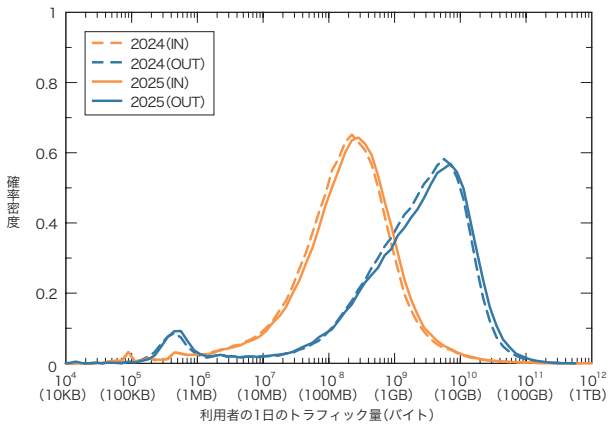


図-3 ブロードバンド利用者の1日のトラフィック量分布 2024年と2025年の比較

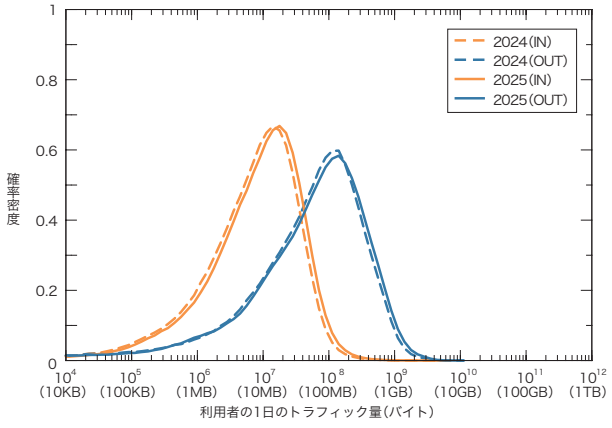


図-4 モバイル利用者の1日のトラフィック量分布 2024年と2025年の比較

まず、図-3のブロードバンドの分布を見ます。2024年と2025年を比較すると、INとOUT共に分布全体がわずかながらも右側に移動していて、全体的に利用量が増えていることが分かります。

図-4のモバイルの場合も、分布の山が昨年に比べ少し右に移動していて、全体の利用量が増えていることが分かります。モバイルの利用量は、ブロードバンドに比べて大幅に少なく、また、使用量に制限があるため、分布右側のヘビーユーザの割合が少なくなっています。極端なヘビーユーザも存在しません。外出時のみの利用や、使用量の制限のため、各利用者の日ごとの利用量のばらつきはブロードバンドより大きくなります。

表-1は、ブロードバンド利用者の1日のトラフィック量の平均値と中間値、分布の山の頂点にある最頻出値の推移を示します。分布の山に対して頂点が少しずれている場合は、最頻出値は分布の山の中央に来るように補正しています。分布の

	IN（MB/day）			OUT（MB/day）		
年	平均値	中間値	最頻出値	平均値	中間値	最頻出値
2007	436	5	5	718	59	56
2008	490	6	6	807	75	79
2009	561	6	6	973	91	100
2010	442	7	7	878	111	126
2011	398	9	9	931	144	200
2012	364	11	13	945	176	251
2013	320	13	16	928	208	355
2014	348	21	28	1124	311	501
2015	351	32	45	1399	443	708
2016	361	48	63	1808	726	1000
2017	391	63	79	2285	900	1259
2018	428	66	79	2664	1083	1585
2019	479	75	89	2986	1187	1995
2020	609	122	158	3810	1638	3162
2021	714	143	200	4432	2004	3981
2022	727	142	178	4610	2010	3981
2023	804	166	224	5456	2369	5012
2024	834	178	224	5743	2372	5620
2025	886	202	282	6538	2615	6310

表-1 ブロードバンド個人利用者の1日のトラフィック量の平均値と最頻出値の推移

最頻出値を2024年と2025年で比較すると、INでは224MBから282MBに、OUTでは5620MBから6310MBに増えています。伸び率で見ると、INで1.26倍、OUTは1.12倍となっています。一方、平均値はグラフ右側のヘビーユーザの使用量に左右されるため、2025年には、INの平均は886MB、OUTの平均は6538MBと、最頻出値より大きな値になります。2024年には、それぞれ834MBと5743MBでした。なお、前述のように2020年分まではPPPoE利用者のみの数字で、2021年以降はPPPoE利用者とIPoE利用者を統合した数字になっています。

	IN (MB/day)			OUT (MB/day)		
年	平均値	中間値	最頻出値	平均値	中間値	最頻出値
2015	6.2	3.2	4.5	49.2	23.5	44.7
2016	7.6	4.1	7.1	66.5	32.7	63.1
2017	9.3	4.9	7.9	79.9	41.2	79.4
2018	10.5	5.4	8.9	83.8	44.3	79.4
2019	11.2	5.9	8.9	84.9	46.4	79.4
2020	10.4	4.5	7.1	79.4	35.1	63.1
2021	9.9	4.7	7.9	85.9	37.9	70.8
2022	12.8	6.0	10.0	113.7	49.2	89.1
2023	14.1	6.8	11.2	129.2	56.0	100.0
2024	16.3	8.2	14.1	150.4	66.7	112.2
2025	19.3	9.7	15.8	172.2	73.5	125.9

表-2 モバイル個人利用者の1日のトラフィック量の平均値と最頻出値

表-2はモバイルの値の推移で、2025年の最頻出値はINで16MB、OUTで126MB、平均値はINで19MB、OUTで172MBです。2024年の最頻出値はINで14MB、OUTで112MB、平均値はINで16MB、OUTで150MBでした。

図-5及び図-6では、利用者5,000人をランダムに抽出し、利用者ごとのIN/OUT使用量をプロットしています。X軸はOUT(ダウンロード量)、Y軸はIN(アップロード量)で、共にログスケールです。利用者のIN/OUTが同量であれば対角線上にプロットされます。

対角線の下側に対角線に沿って広がるクラスタは、ダウンロード量が1桁多い一般的なユーザです。各利用者の使用量やIN/OUT比率にも大きなばらつきがあり、多様な利用形態が存在することがうかがえます。モバイルでも、OUTが1桁多い傾向は同じですが、ブロードバンドに比べて利用量は大幅に少なくなっています。ブロードバンド、モバイル共に、2024年との違いはほとんど分かりません。

利用者間のトラフィック使用量の偏りを見ると、使用量には大きな偏りがあり、結果として全体は一部利用者のトラフィックで占められています。例えば、ブロードバンド上位10%の利用者がOUTの50%、INの73%を占めています。更に、上位1%の利用者がOUTの15%、INの44%を占めています。モバイルでは上位10%の利用者がOUTの48%、INの46%を占めていて、上位1%の利用者がOUTの12%、INの13%を占めています。これらの割合は昨年からほとんど変わっていません。

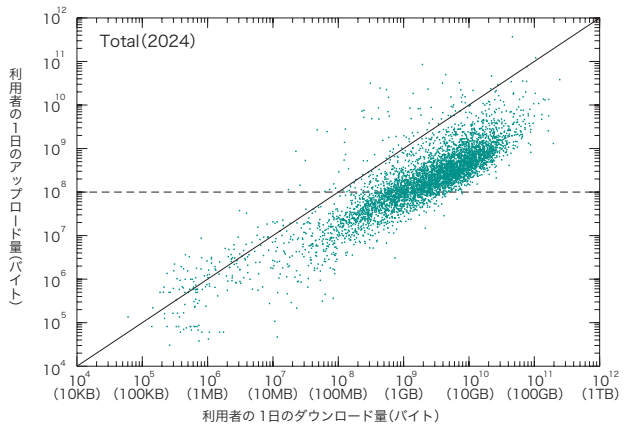


図-5 ブロードバンド利用者ごとのIN/OUT使用量

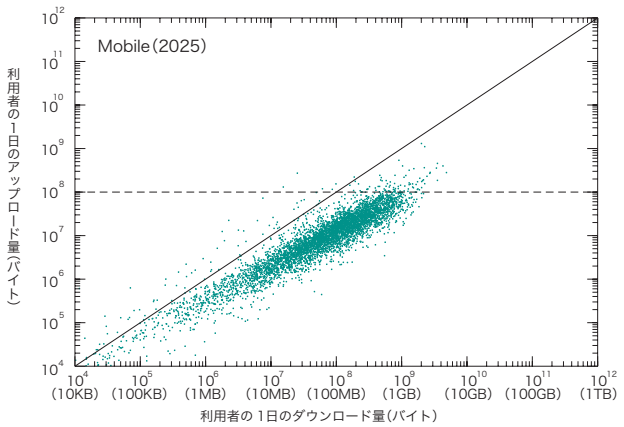


図-6 モバイル利用者ごとのIN/OUT使用量

1.4 ポート別使用量

次に、トラフィックの内訳をポート別の使用量から見ていきます。最近では、ポート番号からアプリケーションを特定することは困難です。P2P系アプリケーションには、双方が動的ポートを使うものが多く、また、多くのクライアント・サーバ型アプリケーションがファイアウォールを回避するため、HTTPが使う80番ポートなどを利用します。大まかに分けると、双方が1024番以上の動的ポートを使っていればP2P系のアプリケーションの可能性が高く、片方が1024番未満のいわゆるウェルノウンポートを使っていれば、クライアント・サーバ型のアプリケーションの可能性が高いと言えます。そこで、TCPとUDPで、ソースとデスティネーションのポート番号の小さい方を取り、ポート番号別の使用量を見てみます。

表-3 はブロードバンド利用者のポート使用割合について過去5年間の推移を示します。2025年の全体トラフィックの66%はTCPで、昨年から2ポイント減りました。HTTPSのTCP443番ポートの割合は、53%で前回からわずかに減りました。HTTPのTCP80番ポートの割合は6%で1ポイント減っています。QUICプロトコルで使われるUDP443番ポートは、23%で2ポイント増えました。

TCPの動的ポートは、わずかに減って6%でした。動的ポートでの個別のポート番号の割合はわずかで、最大の31000番でも1.6%となっています。

表-4はモバイル利用者のポート使用割合です。全体的にはブロードバンドの数字に近い値となっています。これは、スマートフォンでもPCと同様のアプリケーションを使うようになってきたことに加え、ブロードバンドにおけるスマートフォンの利用割合が増えているからだと考えられます。

ブロードバンドのポート別データは、PPPoEだけでIPoEを含まないので、固定ブロードバンド全体の傾向を表していると

year	2021	2022	2023	2024	2025
protocol port	(%)	(%)	(%)	(%)	(%)
TCP	**71.9**	**71.6**	**70.5**	**67.5**	**65.5**
(< 1024)	65.8	65.4	64.8	61.1	59.8
443(https)	53.5	55.7	56.9	53.8	53.2
80(http)	11.6	8.9	7.2	6.5	5.9
993(imaps)	0.1	0.1	0.1	0.1	0.2
183	0.1	0.2	0.2	0.2	0.1
22(ssh)	0.2	0.1	0.1	0.1	0.1
(>= 1024)	6.1	6.2	5.7	6.4	5.7
31000	0.6	0.9	1.1	1.2	1.6
8080	0.4	0.3	0.4	0.3	0.3
1935(rtmp)	0.2	0.2	0.2	0.3	0.2
UDP	**24.5**	**24.3**	**25.4**	**28.2**	**30.6**
443(https)	15.9	16.3	18.2	21.0	23.1
4500(nat-t)	0.8	0.8	1.0	0.9	0.7
8801	0.9	0.6	0.4	0.4	0.3
ESP	**3.3**	**3.8**	**3.8**	**4.0**	**3.6**
GRE	**0.2**	**0.2**	**0.1**	**0.2**	**0.2**
IP-ENCAP	**0.1**	**0.1**	**0.1**	**0.1**	**0.1**
ICMP	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

表-3 ブロードバンド利用者のポート別使用量

year	2021	2022	2023	2024	2025
protocol port	(%)	(%)	(%)	(%)	(%)
TCP	**70.3**	**71.6**	**71.0**	**71.0**	**69.8**
443(https)	44.4	42.3	42.1	42.2	37.8
80(http)	5.0	4.1	3.5	1.8	1.5
993(imaps)	0.2	0.1	0.1	0.1	0.1
1935(rtmp)	0.1	0.1	0.2	0.1	0.1
UDP	**23.8**	**24.4**	**26.5**	**27.5**	**29.3**
443(https)	16.3	17.9	20.9	22.5	24.8
4500(nat-t)	3.7	2.7	2.5	1.8	1.5
51820	0.0	0.1	0.2	0.3	0.3
53(dns)	0.2	0.2	0.2	0.2	0.2
8801	0.7	0.3	0.2	0.1	0.1
ESP	**5.8**	**3.9**	**2.4**	**1.4**	**0.8**
ICMP	**0.0**	**0.0**	**0.1**	**0.0**	**0.1**
GRE	**0.1**	**0.0**	**0.0**	**0.0**	**0.0**

表-4 モバイル利用者のポート別使用量

は限りません。モバイルでのIPv4とIPv6の違いを見ると、IPv6ではTCPもUDPも443番ポートの割合がより大きくなっていて、IPoEでも同様の傾向があると考えられます。

図-7は、ブロードバンド全体トラフィックにおける主要ポート利用の週間推移を、2024年と2025年で比較したものです。TCPポートの80番・443番・1024番以上の動的ポート、UDPポート443番の4つに分けてそれぞれの推移を示しています。グラフでは、ピーク時の総トラフィック量を1として正規化して表しています。全体のピークは19時～23時頃です。2024年と比較して、全体では大きな変化はありませんが、UDPポート443番が少し増えています。

図-8のモバイルでは、トラフィックの大半を占めるTCP80番ポートと443番ポート、UDP443番ポートについて推移を示します。2024年と比べると、ブロードバンドと同様にUDPポート443番が少し増えています。ブロードバンドに比べると、平日には、朝の通勤時間、昼休み、夕方と3つのピークがあるなど利用時間の違いがあります。

今回は主要コンテンツ事業者の平日の時間別トラフィックを見ていきます。図-9は、ブロードバンドのTCP及びUDPの送信元443番ポートのトラフィックについて、送信元IPアドレスから登録組織IDに当たるAS番号を取得し、主要コンテンツ事業者のAS番号について、平日の時間別のトラフィック量

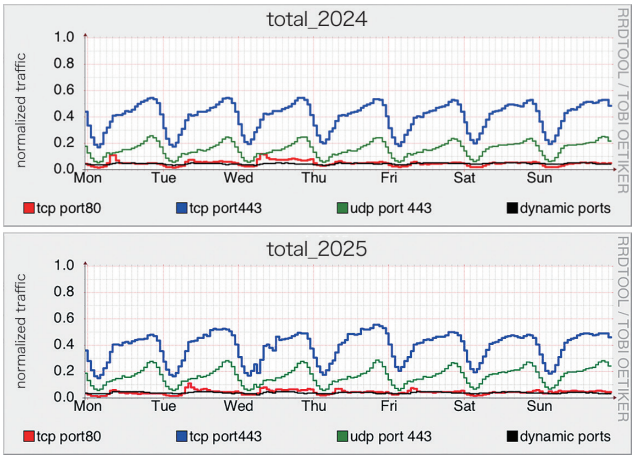


図-7 ブロードバンド利用者のポート利用の週間推移
2024年(上)と2025年(下)

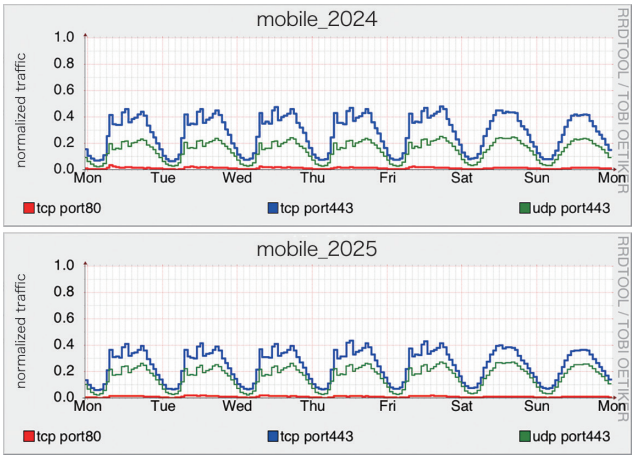


図-8 モバイル利用者のポート利用の週間推移
2024年(上)と2025年(下)

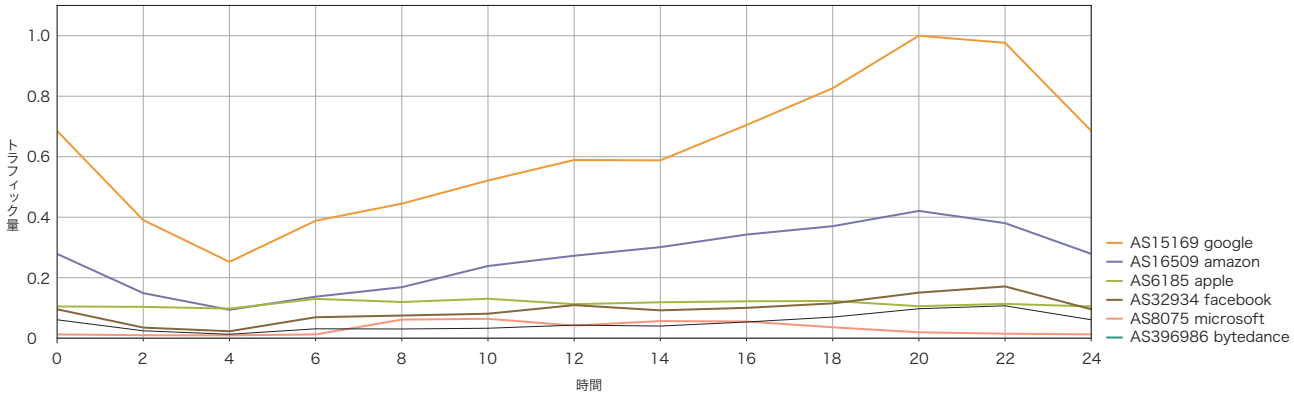


図-9 大手コンテンツ事業者の平日時間別ブロードバンドトラフィック量

を2時間おきにプロットしたものです。主要コンテンツ事業者の多くは複数のAS番号を使っていますが、ここではトラフィック量が最も多いAS番号のみを取り上げます。また、これらの事業者は外部のコンテンツ配信ネットワーク（CDN）も使っていますが、外部CDN経由で配信されたコンテンツ分はカウントできません。従って、各事業者のトラフィック量はその事業者の総量を示す訳ではなく、あくまでAS単位のトラフィック量です。

トラフィックが最も多いのはGoogleで、ここにはYouTubeが含まれます。次はAmazonで、ここにはAmazon Prime Videoも、Amazon Web Serviceを利用する他社のトラフィックも含まれます。Google、Amazon、Facebook、そしてTikTokを運営するBytedanceは、いずれも動画コンテンツの多い事業者で、夕方から夜にかけてピークがあり、一般家庭での動画視聴傾向を反映しています。これに対して、Appleは時間に関わらず一定したトラフィックがあり、自動的にアプリ更新などが行われている影響だと思われます。Microsoftは昼間の時間のトラフィックが多く、リモートワークなどの仕事関係の利用が窺えます。また、UDPの443番ポートだけを見ると、67%がGoogle、13%がFacebook、6%がBytedanceとなっています。

1.5 まとめ

ここ数年ブロードバンドトラフィックは比較的安定した成長を続けていて、その傾向にもあまり変化はみられません。とはいえ、過去を振り返ると、トラフィック的にあまり変化のない時期が数年続くと、また次の変化がやってくるということを繰り返してきているので、近いうちに次の波がやってくるのかも知れません。

次の波の候補として、いま話題のAIの影響も挙げられますが、一般ユーザのAI利用が増えても、ブロードバンドトラフィックへの影響は限定的だと思います。例えば、検索がこれまでのキーワード検索からAIチャットボットに替わることは予想で

きますが、データサイズに大きな変化はないので、トラフィック量にはあまり影響はないでしょう。

他の可能性として、クラウドAIで監視カメラの映像を解析するサービスが、もしかすると大きなテロなどを契機に、急速に普及してアップロードが急増するシナリオが考えられます。このようなサービスは、今後拡大はするでしょうが、第三者に監視カメラ映像を提供することにはプライバシー侵害の懸念もあるので、急成長は難しいのではないかと思います。

一般ユーザから見えないところでは、大規模なAIモデル開発をする一部の組織が、AI学習用のデータとするため大量のコンテンツ取得をしていて、コンテンツ事業者側には負荷増大などの影響が出ているようです。

現状、ブロードバンドのトラフィック増加は、データの大きい動画コンテンツの増加に牽引されています。最近では、インターネット動画視聴は、家庭でもモバイルでもストレスなくできるようになってきました。電車の中でもスマートフォンで動画を観ている人がたくさんいます。今後もトラフィックの増加のペースに大きな変化はないとしても、動画コンテンツの利用者数、1人当たりの視聴時間、画質向上に伴うデータサイズは、いずれも当面は増え続けると考えられます。

これらはあくまで量的な変化ですが、誰もがスマートフォンでビデオを撮影し、簡単に加工や共有ができるようになったことは質的な変化で、更にAIで動画活用が簡単になり飛躍的に発展すると予想できます。このことは、単にインターネット上の動画視聴が増えている現象にとどまらず、これまでの文字中心の文化から、SNSでの写真と短い文章による発信、更に動画やアニメーションへと、テクノロジーによって我々のコミュニケーション、ひいては文化そのものが本質的に変化してきている社会現象だと捉えています。

執筆者:
長 健二朗(ちょう けんじろう)
IIJ 技術研究所 所長。

「ディフェンス対応」の効果と送信ドメイン認証(ARC)に対するIIJの対応

2.1 お客様を保護するための新たな取り組み「ディフェンス対応」の効果

2.1.1 前号レポートを踏まえて

前回の報告で、悪意のある者がメールアカウントを乗っ取り、メールサービスを用いてフィッシングメールなどの送信に利用されてしまう問題についてレポートしました。

悪意のある者によってメールサービスが不正利用されると、フィッシングメールなどの宛先ユーザが攻撃対象となってしまうだけでなく、サービス設備の可用性の低下や、宛先のメールサービスへの到達性低下など、メールサービスを利用している他のお客様にも影響が波及してしまいます。このようなインターネット上での迷惑行為や不正行為はIIJに限らず、他ISPや他社サービスでも日常的に発生しており、一般的にabuse(アビューズ)と呼ばれますが、事後対処しかできない点が課題でした。

そこで、メールサービスの品質を維持し、お客様を保護するための取り組みとして、不正利用の準備行為を察知した場合、実際にフィッシングメールなどが送信される前に必要な範囲で通信を制限し、abuseに至らないようにする新しい取り組みを、2024年5月1日より、IIJセキュアMXサービスの契約行為として開始しました[*1]。

2.1.2 ディフェンス対応の効果

abuse対応は実際に行われた迷惑行為の事後対処であるのに対し、不正利用の準備行為を事前に察知してお客様を保護することから、この新しい取り組みを「ディフェンス対応」と名付けました。

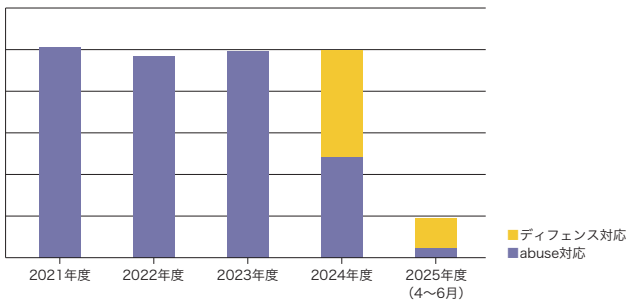


図-1 abuse対応とディフェンス対応件数比較

さて、「ディフェンス対応」を開始してから約1年が経過しました。本稿では、この取り組みによって、どのような効果があったのかを報告します。

図-1は、abuse対応とディフェンス対応の件数を集計し、積み上げたグラフです。縦軸がabuseまたはディフェンス対応が発生した件数で、横軸は年度ごとの合計件数(4月〜翌年3月)です。参考までにディフェンス対応を開始する3年前(2021年度)からの集計も付け加えました。

グラフからも読み取れるように、直近3年間のabuse対応発生件数はほぼ変わっていないのに対し、2024年度からのディフェンス対応の取り組みによって、abuse対応の件数は約半分まで削減されています。

冒頭で説明したように、abuse対応が発生すると、メールサービスの品質が損なわれたり、この対応のためにエンジニアの突発的な稼働が発生したりします。ディフェンス対応によって、こうした要因を約50%排除できたことが分かります。

また、ディフェンス対応によって事前にメールの送信を制限し、悪用を防げているということは、IIJのネットワークから送信されるフィッシングメールなどの送信が抑制できていることを意味します。電子メールは送信者と受信者の立場が表裏一体ですから、これはインターネットインフラの安定運用を支え、信頼性向上に資する技術的取り組みであり、大きな効果を上げていると捉えることができるでしょう。

なお、本稿発行の都合上、2025年度は6月までの集計となっていますが、更に興味深い結果が浮かび上がってきました。2024年度はabuse対応とディフェンス対応がおおむね半々の割合だったのに対し、2025年度の3ヵ月はディフェンス対応の件数の割合が、abuse対応の件数より増加している点です。

*1 この詳しい背景や取り組みの内容はIIR Vol.63でご覧いただけます(https://www.iij.ad.jp/dev/report/iir/063/01.html)。

IIJのメールサービスが悪意のある者にとって使いづらいインフラとなれば、次第に悪用されなくなっていくことが推測されます。そしてサービスのプロダクトオーナーの視点から言えば、abuseの対応件数が減少していけば、その分、エンジニアの稼働を運用改善や品質向上、そしてお客様サポートといった別の取り組みに回すことができます。

IIJでは、今後ともお客様を保護するための取り組みを続けてまいります。

2.2 送信ドメイン認証(ARC)に対するIIJの対応

2.2.1 背景と対応の概要

2023年にGoogle、Yahooが送信ドメイン認証(SPF、DKIM、DMARC)必須化を発表したことを受け、IIJでも社内システムの対応作業を行いました。

対応作業の過程で、Microsoft 365(以下、M365)宛に転送を行う場合、ARC(Authenticated Received Chain)認証が失敗する事象を確認しました。ARCは、メール転送時にSPFやDKIMの認証結果を再評価し、それらの結果と署名情報をヘッダーに追加することで、DMARCポリシーによる誤判定を防ぐ役割を果たします。検証時のメールヘッダーには、以下のようにarc=fail(47)の記述があり、認証が失敗していることが示されています。

```
ARC-Authentication-Results: i=2; mx.microsoft.com 1; spf=fail (sender ip is
...) smtp.rcpttodomain=iijsmxstg.onmicrosoft.com
smtp.mailfrom=iij.ad.jp; dmarc=pass (p=reject sp=reject pct=100) action=none
header.from=iij.ad.jp; dkim=pass (signature was verified) header.d=iij.ad.jp;
arc=fail (47)
```

この問題がIIJ側のシステムに起因するものか、他メールシステム側の処理に起因するものかを切り分けるため、複数プロバイダに対してARC検証を実施しました。

表-1は、各プロバイダへの転送結果をまとめたものです。各プロバイダへの転送結果をまとめた表です。IIJ-officeはIIJ社内で業務利用 しているメールシステム、SMXはIIJセキュアMXサービスで異なるメールシステムです。

2.2.2 問い合わせ

ARC認証失敗の原因を特定するため、RFC 6376およびRFC 8617準拠のPythonライブラリ「dkimpy」を用いて署名検証を行ったところ、IIJからM365宛のメールにおいてARC-Message-Signature(AMS)のverifyに成功することが確認されました。

```
>>> import dkim
>>> dkim.ARC(open("iijsmx-forward-365-arc-fail-20231127.eml","br").read()).verify()
```

```
(b'fail', [{'instance': ..., ...; spf=... smtp.rcpttodomain=... smtp.mailfrom=...;
dmarc=... action=... header.from=...; dkim=... header.d=...; arc=fail (47)\r\n',
'ams-domain': ..., 'ams-selector': ..., 'ams-valid': True, 'as-domain': ...,
'as-selector': ..., 'cv': ..., 'as-valid': ...}], "x= ...")
```

この結果を基に被疑を深めMicrosoft社へ問い合わせを行ったところ、Microsoft社からの回答として、ARC署名の検証を行った際のハッシュ値が一致しないためarc = failとなっており、署名を行った時点から改変された可能性があるとの見解が示されました。

ハッシュ値の計算前には正規化が行われますが、確認したところ、IIJではsimpleアルゴリズムを使用していたのに対し、M365ではrelaxedアルゴリズムを使用していることが判明しました。

正規化とは、メールの内容を一定の形式に変換する処理であり、DKIMの標準であるRFC 6376に準拠しています。RFC 6376では、ヘッダーと本文の正規化アルゴリズムとして「simple」と「relaxed」の2種類が定義されています。「simple」は改行や空白をそのまま使用する方式で、送信時の内容を忠実に保持します。一方「relaxed」は空白や改行を無視し、連続する空白を1つにまとめるなどの処理を行います。

ARCの標準であるRFC 8617では、ARCがDKIMの構文と処理を踏襲することが明記されており、特にbh(body hash)タ

転送経路	i=1	i=2	i=3	ARC結果
IIJ-office → SMX → Google → FastMail	IIJ-office	SMX	Google	fail
IIJ-office → SMX → Google → Microsoft	IIJ-office	SMX	Google	fail
IIJ-office → SMX → FastMail	IIJ-office	SMX	-	pass
IIJ-office → SMX → Microsoft	IIJ-office	SMX	-	fail

表-1 各プロバイダへの転送結果

グの扱いについては、DKIMと同様に正規化後の本文に対してハッシュ値を計算することが求められています。

また、他のGmailやOSSを用いてIIJサービスが生成するハッシュ値と一致すること、M365側の正規化アルゴリズムが他サービスやOSSと異なっている可能性がある旨も併せて伝えましたが、IIJ側のメールシステムがarc=failの原因である可能性を完全に否定できないことから調査が難しいとのことだったため、問い合わせはクローズとなりました。

2.2.3 再検証と不具合の特定

その後、別件で確認されたarc = failの事象に対して、IIJ側の不具合を修正し、本文の正規化アルゴリズムをsimpleからrelaxedに変更する暫定対応を行いました。この変更により、ARC認証失敗の問題は解消されると想定されましたが、引き続きarc=failとなる事例が確認されたため、再度詳細な調査を行いました。

1度目の問い合わせの内容と同じく他プロバイダへの転送と並行して、メールヘッダーの中の値をより詳細に確認するようにしました。本文が空であるメールとテキストがあるメールを検体として検証を行ったところ、本文が空の場合bhタグのハッシュ値がIIJ側とM365側で異なっていました。IIJ からは、Microsoft社に本不具合を修正するよう要請しました。

```
ARC-Message-Signature: i=3; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com;
 s=arcselector9901;
 h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-
AntiSpam-MessageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-
Exchange-AntiSpam-MessageData-1;
 bh=47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU=;

b=P0BjQ+kWDc+ghsJ3atV7ElnsRM8v6qSXVbWk+sT59USGlCYId0vvOL5H0s5sfLj58Ow4HnWmYG9RN8As9
rDEBb3IlWihg13+kPDEM8/S3HydFI58bT3KjHuWzM5UGH3MBv+lriGKciDpbDRhnlaz2mvZNnBMuBqCD0eD
8NAa3soY6oP8/jh6t692dWiDRD9pI+D8ho9VhpRZw1SFQ7UIJAtWMLNuY6YG9WlGXmdSi9nCALdhBzwGjod
1Xx0/+RnxLZQAg56eSYYAqCTC5At/YbCjK8b6Yk7+MLcuJBAL/JYAy69uJiBcNo3sroAbnjp7zhgi4FvILn
oM3pMvzFidnA==

ARC-Message-Signature: i=2;a=rsa-sha256;c=relaxed/relaxed;d=securemx.jp;h=
      Content-Type:MIME-Version:Subject:Message-Id:To:From:Date:DKIM-Signature;s=
      arc20190303;t=1713939099;x=1713937899;bh=frcCV1k9oG9oKj3dpUqdJg1PxRT2RSN/XK
      dLCPjaYaY=;b=XT741y7ourI4cRnEqfSt2iNOXIsKAbHFNGzRrMz0R/Rfnm/UuewENteicKQbQZ
      A5E6dfKj1osLQvWGSIwUDQjb405Y0yt3PS/rrV4Eb+LmfvXLGdbVCUT7Q8HPchkyIXgy6D2LEB3
      eF69Br0MF97GW2jz5YF9Dj51I6VuytabrDa31B1w62ENmz7N/gTT62aAPYLUBuHL9DhuJi1d9lm
      +uZLh3ia8iswz8FxZDkuRbrBwQu8eyzinlPyqAfUdPcTbERf+GuGDOfkFyL2NHUg4HUHGaaoqQI
      yt3Vuqt31eM/Uz75LGcPITpRWPGUxZviMLTMiV/Jeoxd4CA2+wbEcOg==

ARC-Message-Signature: i=1;a=rsa-sha256;c=relaxed/relaxed;d=securemx.jp;h=
      Content-Type:MIME-Version:Subject:Message-Id:To:From:Date:DKIM-Signature;s=
      arc20190303;t=1713933098;x=1713937898;bh=frcCV1k9oG9oKj3dpUqdJg1PxRT2RSN/XK
      dLCPjaYaY=;b=T0diE3VZQzYgPwNPb3mPL/hc9Bsw/xc2LOvdgzq5D/P19MlMswEm7oO7a1pKgr
      EvtHRelRPQFCPFP4p5Fc6/CFITiMjRBBDLaqBguN3VsbjwyRbp1BSTzFzEm8+/2hI6hFri6XwfY
      TmfiE799hedDK5XoFCjURuT/gv4MSFjdTzLkdZY2M4CY00fHPiM9g7av9aJU3OYfku8DUrFev4t
      dIWI/7jT6tRpsN/roh3WEb1j3ll9YUqTMMOhN4fzO2Teo+4BCLxjGVZLL60iglOA8tkO899QtCo
      aDJqM8BeSWFc0m8WO1CYTg92HukBJQphxb3g8XMayEB0n6B3sQ20E0A==
```

テキストがある場合はbhタグのハッシュ値が同じようでした。

```
ARC-Message-Signature: i=3; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com;
 s=arcselector9901;
 h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-
AntiSpam-MessageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-
Exchange-AntiSpam-MessageData-1;
 bh=KXMY6AzIdALlOzgkBat5CPcMk0Vqq3IozVvMgC0v4D0=;

b=hoDE5ZJ2ZnJuUTrPAsRdaZjjfsIHGRAH16O7Syq0uNPc7MPkKWyCUaRhU5JR14hg+TIClmfdauNL9nLN6
MDPrdAWBGwQr00h8fQrcy4AHrK206Cex9YV07/AjBu7eO09ld7wTWr3IwJc8wzQ83CYXQ4AIoXqK+mzsXo8
rQDOaPOxgTmNwvfGm+Q0Q5AdNzoesniZdAfmC1ZjKw774bezqKlTEY9P9ylwQPyQ830nHpbToug4PlQN5la
QReb2wxFVQUzfY8Wser0l/31hzuM1kB1Regz9o9+gRBJiMs3YBP4ENLUOqp0Oq7dUhIDhZ9T++hGHvNZtZN
Ckheo4HIClOw==

ARC-Message-Signature: i=2;a=rsa-sha256;c=relaxed/relaxed;d=securemx.jp;h=
      Content-Type:MIME-Version:Subject:Message-Id:To:From:Date:DKIM-Signature;s=
      arc20190303;t=1713933207;x=1713938007;bh=KXMY6AzIdALlOzgkBat5CPcMk0Vqq3IozV
      vMgC0v4D0=;b=zLi0vrLrkhYhpkGqnKJ2IyYywsXPSc3vGsVUjV5UOzuX+Pg3VdgwdXgXDbANw9
      PdpDJ/uBklbyU0v52Vw7Sa8RPiB3QdaZOfLoIyEa3uDAGqy7cKd+yAXfnkBGQoZhP8ddkT8yQZz
      uK9/Vz0F5tQb+RTzkjjugHuavng6OKA1YTCIYPB654uqicxyx+L6TwLzajKv20TKZIDYq6fpQFO
      4vW0bclHa4hKk91lkI7yAPZ6WpuhZv6S9ySnIs6PujDSXYV2GEMcu8aTa4VHAXNGLu3zqtS2Btx
      cW6EGC3/xGDxI0BaU9Itr/73vwH3ZNilw2uE0xbhxkehShmL1hZns2A==

ARC-Message-Signature: i=1;a=rsa-sha256;c=relaxed/relaxed;d=securemx.jp;h=
      Content-Type:MIME-Version:Subject:Message-Id:To:From:Date:DKIM-Signature;s=
      arc20190303;t=1713933205;x=1713938005;bh=KXMY6AzIdALlOzgkBat5CPcMk0Vqq3IozV
      vMgC0v4D0=;b=heR13lSXC71wKTNdzf9UmnChz5/bqf5L2qZ5X7i8xTsk2x2o42rqKN9Fzpweeb
      Lplf9Msm09ki7XWRJMQci3oi+Ut5Z7Hmjo3UdTrbMjaT621GPKID+gVbDpKxCDlWiCzc5ox3wrw
      MYDoM6A/2rQwjXsgTMoWovEmxyB795Db1y+J5dyCzkpWcJ/2JEXBU0PbQ4Qr1Ofkzq7Rsum5Cyi
      lHeXJw64GDbbh6uY5j1HM92CtGo9Ejw+r6c63snjJRvfrjCcB11hgrx84CclJw9klt9PtUct7P
      +l90RENzLmpelNYa0w9Y2LAGjRztzayIunJnvw0WJ1uniz6iuufwJkA==
```

ARCが準拠しているRFC 6376のセクション3.4.4では、relaxedモードにおいても末尾の改行は除去してはならないと記述されています。

一方、M365では末尾改行を除いた状態でハッシュ値を計算していたため、bhタグの値が一致しませんでした。

このRFCの記述を根拠としてMicrosoft社に問い合わせた結果、M365側の不具合であることが認められました。

2.2.4 おわりに

ARCの普及率はSPF、DKIM、DMARCなど他の送信ドメイン認証と比較して依然として低く、多くのメールシステムではARC認証が実装されていないのが現状です。これはARC認証を設定しなくても現時点では大きな問題が発生しないこと、またARCのRFCであるRFC8617がまだExperimental（実験的）であることが一因と考えられます。

Googleの送信者ガイドラインでもメールを定期的に転送する場合、ARC認証を使用することが推奨されています。また、ARCが適切に実装されていないと転送の過程で元のSPF、DKIMの検証が正しく行えなくなる可能性があり、DMARCポ

リシーによっては受信拒否され、メールの到達性に影響を及ぼす可能性があります。

ARCにはメール転送を行う中間システムの協力が不可欠です。IIJでは今後もARCを含む送信ドメイン認証技術への対応を継続し、メールの信頼性と到達性の向上に努めてまいります。

2.3 日本を標的にしたフィッシングメールの急増

2024年の年末、IIJのメールサービスで過去最大級のフィッシングメールの量を観測しました。図-2はIIJが運用しているハニーポットに着信し、迷惑メール判定された数を集計したグラフです。

11月末頃からフィッシングメールの総量が急激に増加しており、年末頃にピークを迎えています。このときのフィッシングメールは、「Amazon」、「佐川急便」、「税務署(e-Tax)」、「ETC利用照会サービス」などで、本文はすべて本物のメールを模した偽物でした。特に税務署を騙ったフィッシングメールは確定申告の時期と重なっており、攻撃の成功率を上げることを狙ったものと考えられます。

なお、フィッシング対策協議会の月次報告書「フィッシング報告状況」[*2]によると、2024年12月はフィッシング報告数が過去最高値であったとレポートされており、IIJで観測した状況と同様の傾向が読み取れます。この結果から、IIJのみならず他ISPでも同様に観測しており、日本国内を標的としたフィッシングメールが数多く送られていたことが分かります。同レポートの総評として、日本国内の組織では、送信ドメイン認証を代表とするセキュリティ対策が遅れており、海外と比較してフィッシングメールが利用者に届きやすい状況になっていることを挙げています。

2025年以降も高い水準でフィッシングメールを観測しており、引き続き警戒が必要です。

ところで、2021年6月に発行した以前のIIR Vol.51[*3]でもこのようなフィッシングメールの急増についてレポートしました。当時は新型コロナウイルス感染症を発端に、テレワークが急速に広まった時期です。これに便乗したフィッシングメールも観測しました。また、2019年にはメールに添付されたパスワード付きZIPファイルで感染を広げるEmotetが日本国内で猛威をふるい、広範囲での影響が確認されました。

このように、フィッシングメールやウイルスは活動の休止と再開を繰り返し、手を替え品を替え、時代の変化にも合わせてきています。

従って、セキュリティ対策は一度実施すれば終わるものではなく、脅威の進化に応じて継続的に見直し、強化していく必要があります。そしてそれは、終わりのない戦いであり、持続的な投資であり、組織全体で取り組むべき活動です。今後もIIJは、安心・安全な環境の維持に向けて、不断の努力を重ねてまいります。

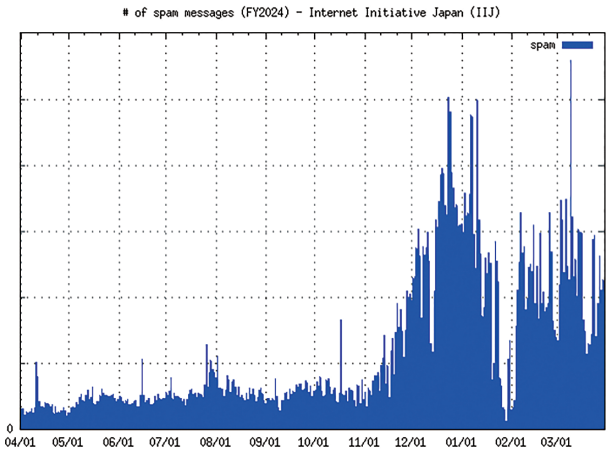


図-2 IIJハニーポットに着信した迷惑メール

＊2　フィッシング対策協議会、月次報告書 2024/12 フィッシング報告状況(https://www.antiphishing.jp/report/monthly/202412.html)。
＊3　Internet Infrastructure Review(IIR)Vol.51(https://www.iij.ad.jp/dev/report/iir/051.html)。

2.4 送信ドメイン認証と経路暗号化統計

定点観測として、IIJが提供するメールサービスで集計した、送信ドメイン認証の結果の割合を図-3～図-6に示します。期間は2025年3月の1ヵ月間です。

前回の報告から送信ドメイン認証の検証に成功(pass)した割合がいずれも低下しています。日本国内の送信ドメイン認証、特にDMARCの対応は、Google Sender Guidelines[*4]の発表で大きく普及していることが分かっています[*5]。

従って、図-2のデータと合わせると、これは通常メールに対して、送信ドメイン認証に対応していない、または送信ドメイン認証の検証に失敗(fail)したフィッシングメールの量がデータに対して支配的になり、割合が低下したと考えるのが自然です。

なお、今回からARCの集計結果を追加しました。ARCは必ずしもすべての組織に対応が求められるものではありませんが、法人向けメールセキュリティのIIJセキュアMXサービスでは受信メールに対するARC署名に2019年から対応済みです。

次にIIJセキュアMXサービスで集計した経路暗号化(STARTTLS)について見ていきます。図-7は受信メールに対する経路暗号化の種類と割合です。PLAINは経路暗号化されていないことを示しています。

受信メールでは7割近くの通信で経路暗号化が行われていました。TLSv1.3による通信も半数近くで行われています。なお、12月にフィッシングメールが急増したことを2.3章で報告しましたが、このグラフでは12月頃にTLSv1.2の割合が増加していることが読み取れます。この結果から、当時フィッシングメールの送信にもTLSによる暗号化通信が行われていたことが分かります。

図-8はIIJセキュアMXサービスから送信されるメールに対しての経路暗号化の割合です。こちらは設備の都合で割合のみの

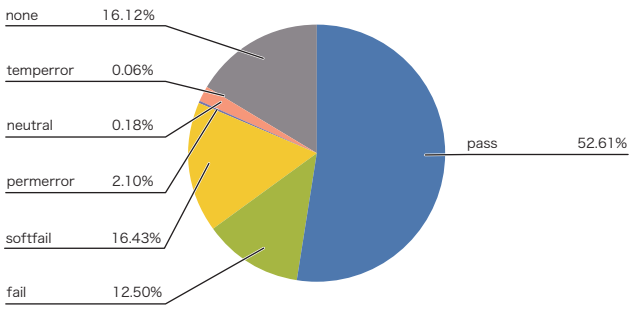


図-3 SPFによる認証結果割合

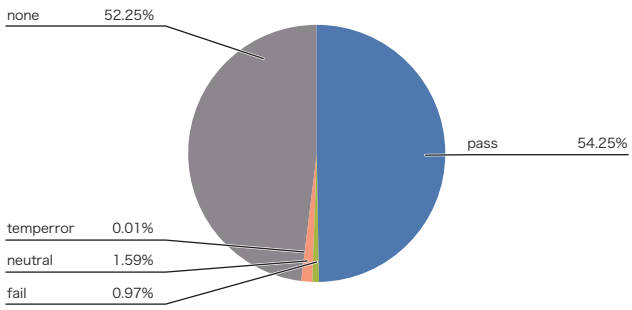


図-4 DKIMによる認証結果割合

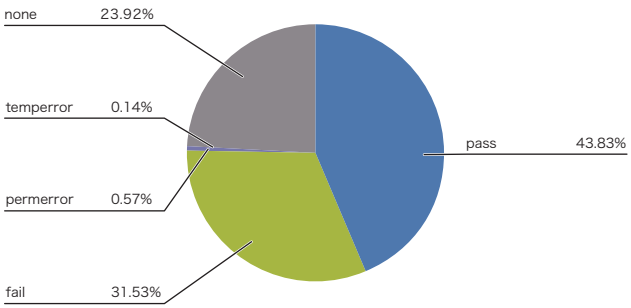


図-5 DMARCによる認証結果割合

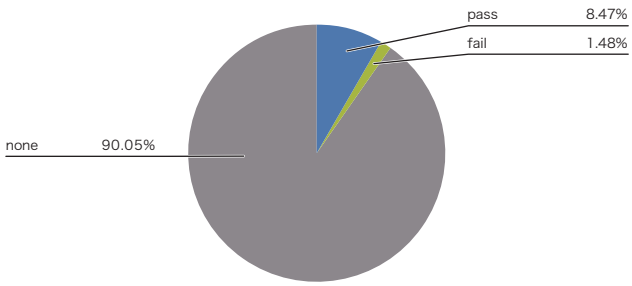


図-6 ARCによる認証結果割合

*4 Email sender guidelines、Google(https://support.google.com/a/answer/81126)。
*5 DNSOPS.JP 統計情報、日本のDNSSEC/SPF/DMARC 対応状況(https://stats.dnsops.jp/chart/all/dmarc)。

集計ですが、概ね100%に近い推移で暗号化通信が行われていることが分かります。

前回、IIR Vol.59[*6]で報告したときには80〜90%の間で推移していましたので、約2年経過してWebと同様、メールの世界も常時TLSの時代に突入したと考えて良さそうです。

なお、Google透明性レポート[*7]でもメールの経路暗号化割合が公開されていますが、ほぼ同様の傾向が読み取れます。2023年に発表されたGoogle Sender Guidelinesで、STARTTLSを要件に盛り込んだことが大きな影響を与えたと考えられます。

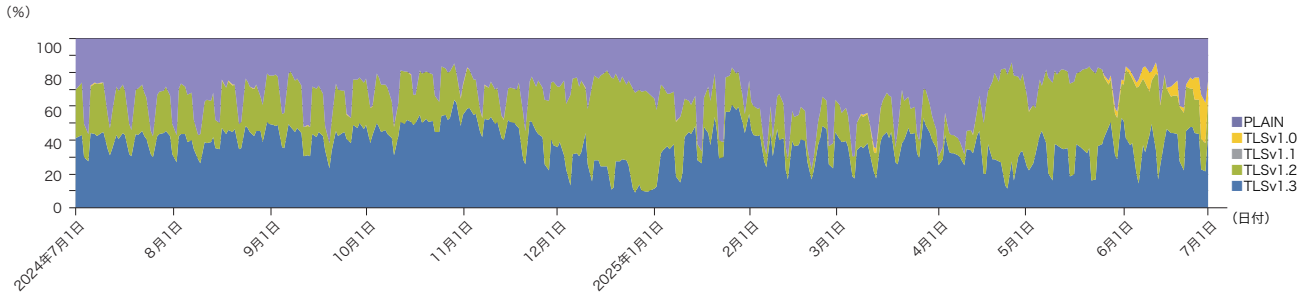


図-7 受信メールにおける経路暗号化の割合

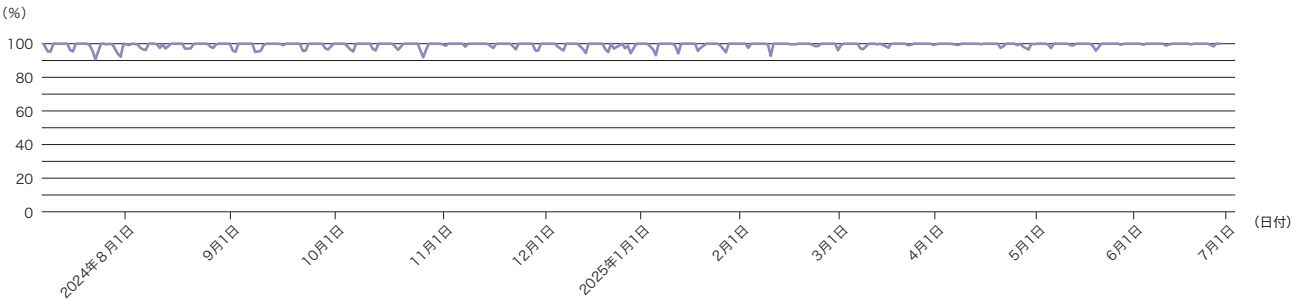


図-8 送信メールにおける経路暗号化の割合

執筆者:

2.1 お客様を保護するための新たな取り組み「ディフェンス対応」の効果、2.3 日本を標的にしたフィッシングメールの急増、
2.4 送信ドメイン認証と経路暗号化統計
古賀 勇(こが いさむ)

IIJ ネットワーク本部 アプリケーションサービス2部 アプリケーションサービス運営課 課長。2007年IIJ入社。メールサービス、IDガバナンス管理サービスの運用業務に従事。お客様のメールボックスを守るため、最新の攻撃手法や、迷惑メールのトレンド、対策情報などを発信・公演。M^{3}AAWG、WIDE Project、openSUSEなどで幅広く活動中。

2.2 送信ドメイン認証(ARC)に対するIIJの対応
山下 隼平(やました しゅんぺい)

IIJ ネットワーク本部 アプリケーションサービス2部 メールサービス開発課。2021年IIJ入社。メールサービス開発業務に従事。

＊6　Internet Infrastructure Review(IIR)Vol.59(https://www.iij.ad.jp/dev/report/iir/059/01.html)。
＊7　透明性レポート、Google(https://transparencyreport.google.com/safer-email/overview)。

脱VMwareへの回答 ～Kubernetesと仮想環境の親密な関係～

3.1 業界を揺るがすVMware問題

昨年から「脱VMware」を巡る議論が絶えません。曰く、VMwareのライセンス価格が高騰しており他仮想化基盤への見直しを検討すべきだ。曰く、ベンダーの論理が優先され既存顧客がないがしろにされているのではないか。本当でしょうか？

様々な条件が影響するため一概には言えませんが、仮想化市場全体を見渡してニュートラルに評価すれば、同社の行動は主戦場となるスイートパッケージをVMwareにおいても主力に位置付け、顧客をより高付加価値で競争力のあるパッケージへ誘導しようとしている、と見ることができます。見方によっては、競合他社と戦略的な差異が少なくなったと言えるでしょう。特定の他社製品に肩入れするわけではありませんが、ラインナップにしろ、価格にしろ、適正化を図ったと表現しても違和感はないように感じます。もっとも、それに伴っておそらくボリュームゾーンであろうシンプルなパッケージのユーザを中心に大きく割を食うことになり、コスト上昇の影響を被ることになったのは変わらぬ事実です。

そこで対策案を検討するわけですが、安直にライセンス費用だけにフォーカスして代替製品への見直しを検討すれば、期待した結果が得られるかは甚だ疑問です。何しろ、VMwareの製品としての魅力が損なわれたわけではないのですから。バージョンアップによって望まない機能変更が行われたり、信頼が失われるような問題を起こしたのであればともかく、これは純粋にコストの問題です。仮にライセンス費用の面で有利な選択肢を見いだせたとしても、いまだ仮想化市場の第一人者であるVMwareと比較して機能、安定性、将来性、その他多くの要素について遜色のない条件を満たさなければなりません。更に、脱VMwareを実行するには大規模なマイグレーションコストが発生します。ともすれば、そのコストは期待していたコストダウン効果を相殺してしまうかもしれません。

つまり、脱VMwareを成功させるには、コストメリットだけに着目するのではなく、VMware以上に優れたプラットフォームとは何か？を考える必要があるのです。もしそれらを両立させることができれば、ライセンス問題への回答となるだけでなく、プラットフォームの世代交代が自社ビジネスに競争力をもたらすことでしょう。

この非常に困難なチャレンジに対する1つの回答としてIIJが取り組んでいるのが、VMwareからKubernetesへのマイグレーションです。オープンソースを最大限に活用し、自社開発のKubernetesディストリビューションIKE(IIJ Kubernetes Engine)をVMwareの代替に位置付け、大きくライセンスコストを削減すると共に、IaaS層では実現し得ない運用の効率化、品質の向上などを実現するというものです。

3.2 あらゆるワークロードを飲み込むKubernetes

ある程度クラウドネイティブ技術に通じているエンジニアであっても、その多くはKubernetesを「コンテナオーケストレータ」と捉えていると思います。実際、大半のKubernetesはコンテナのオーケストレーションに利用されているはず

です。しかし、近年はコンテナに限らずVMのオーケストレータとしても徐々に採用が進んでいることをご存じでしょうか。既に良く知っているという方は相当な通と言えるでしょう。クラウドネイティブの推進者を自認する筆者ですら、技術的には成熟しつつあるものの、実環境での採用まではまだ時間がかかるだろうと感じていたぐらいです。

ところが、VMwareを震源とするプラットフォーム見直し議論の中でKubernetesが最有力後継者へと躍り出ることになり、大きく潮目が変わったように思えます。これはIIJに限った話ではなく、IT業界全体の潮流であるとも感じています。

KubernetesがVMwareの代替プロダクトとして注目を集めるに至った理由は枚挙にいとまがありません。技術的な理由があることはもちろんですが、それ以上に信頼性によるところが大きいように感じます。例えば、Linux Foundationによってベンダーニュートラルに運営され、ベンダーロックインの不安が少ないオープンソースプロジェクトであること。ハードウェアベンダー、ソフトウェアベンダーにかかわらず、広くIT業界全体から支持されエコスシステムが急速に成長していること。その結果、サーバOSにおけるLinuxと同様に、Kubernetesがオーケストレータのデファクトスタンダードと見なされるようになり、長期的な投資を決断できる存在となったこと。そうした積み重ねが信頼を獲得してきたのです。

もっとも、Kubernetesの役割がコンテナのオーケストレータにとどまるのであれば、主流と見なされることはなかったかもしれません。サーバサイドシステムでコンテナの採用が急増しているとはいえ、VMとコンテナのどちらがプライマリであるかと問われれば、現時点では明らかにVMだからです。ただ逆に、将来を考えるとVMしか管理できないプラットフォームがいつまでも主流であり続ける可能性は高くはないでしょう。VMとコンテナを同等のワークロードとして扱うことができるKubernetesに注目が集まるのは必然と言えます。

3.3 IIJにおけるKubernetesプラットフォームIKE

段階的にVMwareからKubernetesへのマイグレーションを進めているIIJですが、早い段階で脱VMwareの手段としてKubernetesを選択できたのは、既にコンテナプラットフォームとしてKubernetesの運用経験を十分に積んでいるからです。もし、脱VMwareを契機に初めてKubernetesの運用に取り組んだのだとしたら、少なからず躊躇したことでしょう。

というのも、Kubernetesの運用ノウハウは一朝一夕に身に付けられるものではないからです。Kubernetesはクラウド時代のOSに例えられるように、サーバ、ネットワーク、ストレージといったシステムリソースに対する調停者です。しかも、OSのように1台のサーバに閉じた制御ではなく、データセンターに収められた大規模なあらゆるシステムが連携して協調するように1つのKubernetesによって管理されます。そのために、Kubernetesは物理的なシステムを隠蔽し、あたかもデータセンターを1つの巨大なリソースプールであるかのように抽象化します。そして、利用者はパブリッククラウドを利用する場

合と同じように、あらゆる操作でKubernetesを通じて指示を出すことになります。これこそがKubernetesを活用するモチベーションの1つなのですが、こうして抽象化されたシステムの設計と運用を行うには、熟練のエンジニアであっても既存の知識が十分に生かせるとは限りません。一方、Kubernetesだけに詳しくなったところで、それはオペレーションの能力が身に付くだけで、システムを運用する能力が身に付くわけではありません。Kubernetesを利用しても結局のところ最終的にはハードウェアの制御に行き着くため、Kubernetesへの操作が実システムに対してどのように反映されるのかを理解できなければ、やはり十分な品質での運用は困難だからです。このような話はVMwareのような仮想化基盤を利用しても同様に存在するのですが、Kubernetesはより抽象化のレベルが高い分だけ更に複雑と言えます。

一方、IIJがサービス基盤としてKubernetesを導入したのは2018年のことです。当時はKubernetes v1.9を利用しており、今よりもはるかにシンプルなシステムにすぎませんでした。それが今では23回のアップグレードを施されてv1.32にまで至りました。その間にKubernetesそのものだけでなく、当初から稼働していた多くのプラグインやコントローラ類はアップグレードされたり、差し替えられたりして、初期に存在していたKubernetesクラスタの構成要素のほとんどは跡形もありません。にもかかわらず、古くからこのKubernetesクラスタ上で稼働していた数々のワークロードは、いまだに安定して運用が続けられているのです。

これは非常に重要なポイントです。Kubernetesにはマイナーバージョンアップのたびに数多くの機能が追加されていますが、それでも致命的に互換性が失われるようなことは7年間1度も起きていないことを意味するからです。更に、低レイヤーで見ればハードウェアもソフトウェアも実装は大きく変化しているにもかかわらず、Kubernetes上のシステムへの影響は非常に軽微であったということは、Kubernetesによる抽象化が効果的に機能していることの証明でもあります。これはKubernetesの継続性、安定性、拡張性、将来性が高いレベルで実現されており、今後についても期待ができるということです。

もっとも、それは自然に実現したわけではなく、アップグレードのたびにその内容と影響範囲を詳細に把握し、適切なアップグレードを行ってきた結果です。その過程で蓄積された経験が脱VMwareにおいても大いに役立っています。もちろん、もっと短時間でKubernetesの運用スキルを身に付ける方法はいくらでもあると思いますが、自信が付くにはある程度の時間を要するものです。

3.4 KubernetesでVMを扱う際の課題はネットワークにあり

十分に知見が蓄積されているとはいえ、実のところIIJにとってもKubernetesにVMをデプロイし始めたのはまだ1年前のことです。評価を始めた際にはコンテナ用KubernetesとVM用Kubernetesを設備から分けることも視野に入れてい

ましたが、そのような考慮はまったく不要であることがすぐに分かりました。それどころか、コンテナとVMを用途に応じて使い分け、混在してシステムを構成できることこそがKubernetesのメリットであるとすら言えます。それほどまでにKubevirtによって実現される環境は素晴らしく、誤解を恐れず言えば、Pod(コンテナを起動する際に利用するリソース)をVirtualMachine(VMを起動する際に利用するリソース)に読み替えるだけで、ほとんどのKubernetesの機能をVMに対しても活用可能です。

PodとVirtualMachineを同等のワークロードとして扱えることのメリットは計り知れません。

- Kubernetesが発展していくと、2倍の手間をかけることなく、その恩恵をコンテナでもVMでも享受できる
- オンプレミスでKubernetesを扱う場合、コンテナ用とVM用で設備を分けずに済むため稼働率を高く維持できる
- PodとVirtualMachineは同じネットワーク(pod network)に接続されるため、相互運用が容易
- VMとして構築されていたシステムをコンテナでリプレースすることが容易。VMからコンテナへのマイグレーションパスとしても有用

ただし、脱VMwareの手段としてKubernetesを選択したとき、課題がないわけではありません。既存の多くのKubernetes環境では、Kubernetesクラスタごとに1つだけ用意されたネットワーク(pod network)にすべてのコンテナとVMを接続する構成が一般的です。一方、VMを中心に運用されている環境ではL2ネットワークが複数用意され、アプリケーションごとに独立したネットワークを利用する構成が珍しくありません。Kubernetes上でも同等のネットワークを用意することは可能ですが、今のところ一般的ではありませんし、L2ネットワークの実現手段がインフラに依存したりプロプライエタリなネットワーク製品に依存することも多く、慎重な検討が求められます。複雑なネットワーク構成が求められる場合、既存のKubernetesクラスタの拡張だけでは対応できず、脱VMware専用Kubernetesクラスタを必要とするかもしれません。

ただ、課題らしい課題がネットワークに集中していることは朗報と言えるでしょう。Kubernetesユーザにとっても VMを利用するために身に付けるべきスキルは本当に少なく、ごくわずかなトレーニングだけで利用可能です。運用する立場としてはそうもいきませんが、プラットフォームエンジニアだけが苦労すれば済むのであればむしろ冥利に尽きるというものです。

脱VMwareはまだ道半ばではありますが、Kubernetesが1つの回答になり得るのは間違いありません。ただし、要件がワークロードごとに千差万別であることは言うまでもなく、正しい選択が複数存在することもまた間違いありません。お客様へ価値あるサービスをご提供するに当たり、固定観念にとらわれず、最適な選択をしていきたいものです。

執筆者:
田口 景介(たぐち けいすけ)
IIJ ネットワークサービス事業本部 ネットワーク本部 SRE推進部長。
メール、DNS、サーバホスティング、クラウドIaaSサービスと数々のサービス立ち上げに参画。近年は過去の経験を活かしてプラットフォームエンジニアリング部門を発足。100を超えるサービス/プロジェクトをホストするプラットフォームに育て上げる。市場や技術の変化を捉え、自らをアップデートし続けることがビジネスを成功に導く秘訣と考えるストラテジスト。

3G停波とMVNO

4.1 はじめに

2026年3月31日をもってNTTドコモが提供する3Gサービス提供が終了します。詳細は下記のリンクから参照可能です。

● NTT ドコモ公式情報
「FOMA」及び「i モード」サービス終了のご案内
https://www.docomo.ne.jp/info/3g_closed/index.html

● IIJ 公式情報
NTT ドコモ FOMA（3G）停波に伴う IIJ モバイルの継続利用につきまして
https://www.iij.ad.jp/svcsol/mobile-support/news/3g_closed.html

NTT ドコモ FOMA（3G）停波につきまして（IIJmio モバイル タイプ D）
https://www.iijmio.jp/info/iij/1712655772.html

NTT ドコモ 3G サービス終了に関するモバイルデータ通信機能の対応
https://support.seil.jp/
→サポート情報→技術情報→NTT ドコモ 3G サービス終了に関するモバイルデータ通信機能の対応

NTTドコモは2019年にサービス提供終了に関する情報を発表しており、遂に来年3月に迫りました。これにより、IIJを含むMVNO事業者の3G回線も利用不可となり、音声通話・SMS・データ通信に影響が及びます。

当然ながら、3Gにのみ対応する端末は利用できなくなりますが、4G(LTE)対応端末であってもこの影響で利用できなくなる可能性があることについて、あまり知られていません。

本稿では、なぜこのようなことが起こるのか技術的な解説をします。あまり期間的な猶予はありませんが、多くの方に3G停波により突然通信サービスが利用できなくなる問題を回避するための準備をしていただき、2026年3月末を乗り切る一助になれば幸いです。

4.2 なぜ3G停波が必要なのか？

3G停波で発生する問題の解説に入る前に、セルラー方式のモバイル無線技術の進化について説明します。2Gから続く、現在のモバイルの無線技術は1991年の2G導入から約10年おきに新しい無線規格が商用サービスに導入され、進化してきました(図-1)。

一方で、新しい無線規格が導入されると

- 前世代の無線規格の機器への投資が大きく減り、既存設備の維持や保守のみになる
- 結果、機器ベンダーが製品の製造を停止し、サポートも徐々に停止する
- そのため、古い設備の維持や保守が年々難しくなる

という流れになるため、新しい無線設備への置き換えが必要となります。また、古い無線規格に比べると、新しい無線規格は限られた周波数資源をより効率的に使える技術が規定されているため、新しい規格に移行するのは自然な流れとなります。

そのため、どこかのタイミングで古い無線規格の利用を止めて、新しい無線規格に移る必要があります。3G停波がまさにこの状況となり、自然な流れとなります。図-1を補足する資料として、世界の端末ベンダーの業界団体GSAが公開している世界のキャリアの2G/3Gの停波状況の推移を示します(図-2)。2025年をピークとして2G/3Gの停止が相次ぎ、4G以降の無線世代に一気に移行します(図-2)。

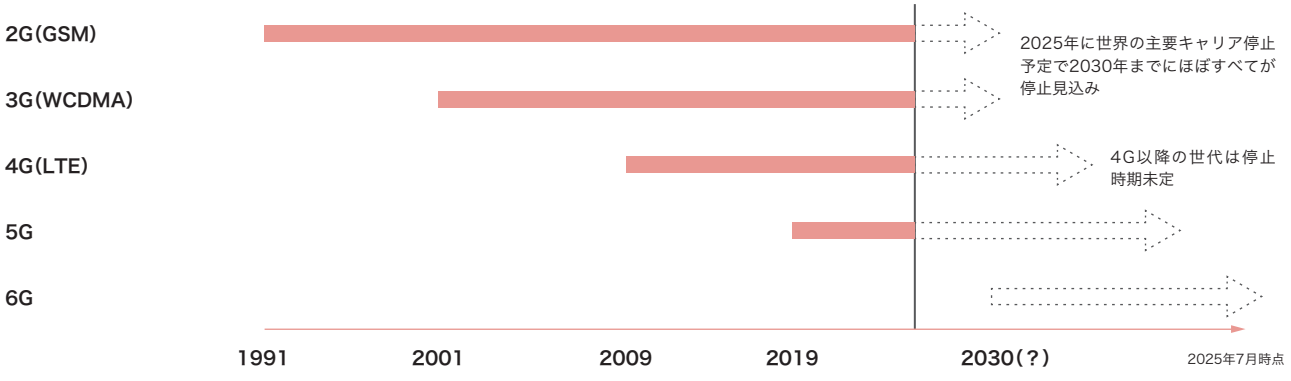


図-1 セルラー方式モバイル無線技術の世界でのサービス開始時期と利用期間

一方で、新しい無線規格の導入初期では新しい無線網を使えるエリアが広くないため、過去の無線規格を利用してエリアを補完するように無線網が構築されるのが一般的です。この際、無線網間の連続性を保つため、コアネットワーク同士を連携させることで接続が切れずに、新旧の無線網をシームレスに移動が可能となります。

このような状況を想定して、端末は新旧の無線規格に対応するように作り込まれており、新旧の無線網が存在している状態では問題になりません。しかし、今回の3G停波のように古い無線網が廃止される場合に、この連携ができる前提で作られた端末では問題となります。以下の解説でこの問題の詳細について説明します。

4.3 3G停波による影響

前節でも述べましたが、端末実装の問題により3G停波で下記のような影響を受けます。

(1) 3Gにのみ対応の端末(4G非対応)の場合 -> 3G電波がなくなるので利用不可
(2) 3G/4G両対応の端末の場合 -> 4G電波があっても3G電波がないため利用できなくなる場合がある

上記の(2)の3G/4G両対応の端末の問題を更に分類すると、大きく分けて下記のようになります。

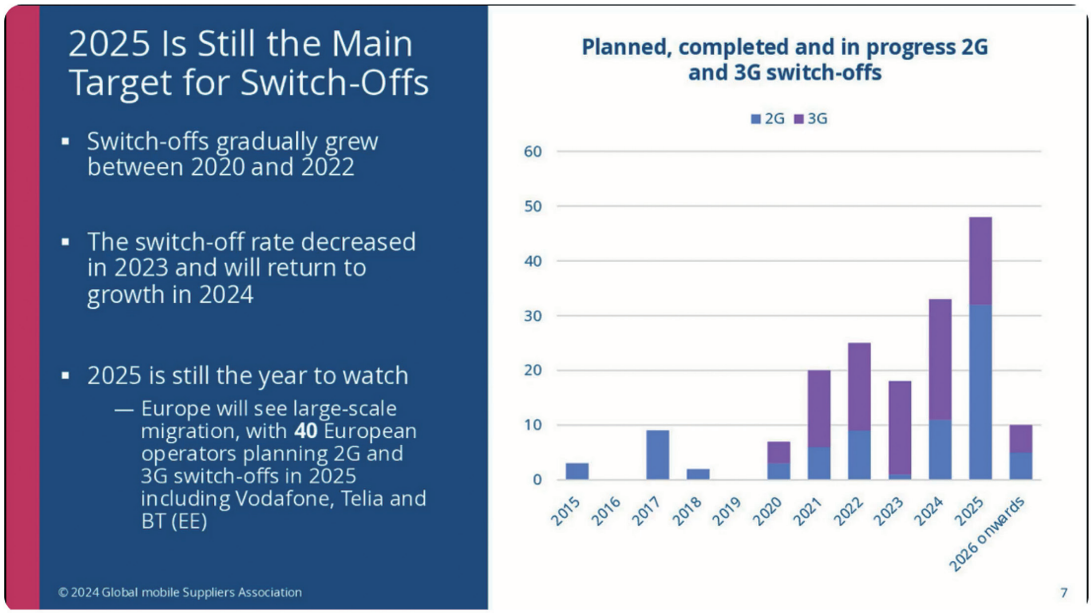
(2-1) 音声対応端末(スマートフォンなど)に起因する問題
(2-1) 端末が必ず最初に3G網に接続してしまう問題

以下の節ではそれぞれの問題について解説します。

4.4 音声対応端末(スマートフォンなど)に起因する問題

モバイルの無線規格を規定する3GPPの仕様では4G端末は大きく分けて2つのモード(UE usage setting)に分類できますので、それぞれについて解説します。

(1) 音声通信優先モード(規格上はVoice centric)
- "絶対に"音声機能を利用できる網に接続するモード
  - スマートフォンの大半はこの実装になっています
  - VoLTE(4G無線を利用した音声通信)またはCSFB(CS Fall Back)と呼ばれる3G網に切り替えての音声通信のどちらかが利用できれば正常に動作
- 一方で、このモードは4G網接続時にVoLTEとCSFBのどちらも利用できない場合に下記のような問題が発生します



出典: https://gsacom.com/webinar/2g-3g-sunset-and-implications-for-5g-broadcast/

図-2 引用元GSA、2G/3G sunset and implications for 5G Broadcast

- この場合は、3GPP規格上の挙動として、4G網との接続を切り、音声が利用可能な別の網（3Gなど）を探しに行くモードに移行します
- 接続可能な3G網の電波が見つからない場合は圏外が継続して、データ通信が利用できなくなります
- 3G停波後に端末実装や通信サービスの制約の組み合わせで、この問題に陥る可能性があります

・ 3G停波後に問題になるケースは下記のものがあります
- VoLTE非対応の4G（LTE）端末を利用の場合
- VoLTE対応4G（LTE）端末を利用しているが、サービスがVoLTEに対応してない場合

（2）データ通信優先モード（規格上はData centric）
・ データ通信端末（ルータ、USBモデム、通信モジュール）は大半がこちらの実装
・ 音声機能が利用できなくても（1）のように圏外にならない
・ 3G停波後に圏外になるような問題は発生しない

IIJでは3G停波後に、（1）の音声通信優先モードの端末で問題が発生する可能性があることを把握しているため、フルMVNOを利用して提供しているIIJモバイルサービス/タイプIでは、ネットワーク側でこの問題が発生しないような対処をすることを予定しています。

4.5 端末が必ず最初に3G網に接続してしまう問題

こちらの問題は音声通信優先モード以外の多くの4G（LTE）端末でも発生している可能性がある問題です。実装や接続設定の問題で、接続時に4G網でなく、3G網に最初に接続してしまう場合があります。このとき、一定時間経過後に4G網に接続が切り替わる挙動の場合が多く、この問題に気づけていない場合があります。

3G網と4G網の両方が使えている状態であれば、最初に3G網に接続し、しばらくすると4G網に切り替わる程度の問題で済んでいましたが、3G停波後は3G網がないため、4G網に接続できない原因となります（図-3）。

この問題は端末側に起因するものであるため、ネットワーク側では対応できず、端末を利用するユーザ側での対応が必須となり、このような事象に遭遇していた場合は早急に対応する必要があります。IIJが把握している範囲で、この問題がどのような原因で発生するかを分類すると下記のように分けることができます。

（a）最初に必ず3G網に接続するように実装されている端末で、修正対応や設定変更が不可能な端末
- 3G停波後にこの端末は利用できなくなるため、端末交換が必要となります

（端末例）

法人向けのIIJモバイルサービスで過去に販売していた510FU、520BU（USBモデム）がこれに当てはまります

（b）最初に必ず3G網に接続するように実装されている端末だが、端末ファームウェアの更新で改善可能な端末
- 古いファームウェアのままだと3G停波後に利用できませんが、端末メーカから最新ファームウェア入手して更新することで設定が変更され、4G網への接続が最初に行われるようになります。このような端末は3G停波後も利用することが可能です
- このような対応で3G停波後に利用可能かは、端末メーカに確認の必要があります

（端末例）

1.富士ソフトFS040U（セキュア接続モード）
2.ネクスUX302NC、UX302NC-R
3.アットマークテクノArmadillo-IoT G4/G3M1

（c）デフォルト設定では最初に3G網に接続するが、4G網への接続が最初になる設定変更が可能な端末
- 何もしないと3G停波後に利用できなくなりますが、端末で設定変更を行うことで、3G停波後でも利用することが可能です
- このような機能を持っているか、また、設定方法はどうすればいいのかについては、端末メーカへの確認が必要です
- 以下はこの事象に当てはまる代表的な端末で、4G網への接続を最初にする方法となります

（端末例）

Google Pixelシリーズ（APN設定のAPNタイプで“ia”設定の追加が必要）
Microsoft Surfaceシリーズ（APNの種類：イン

ターネットおよびアタッチ設定が必要)

(d) スマートフォンや通信モジュールのAPN設定の問題で3G網に最初に接続してしまう事象

- 法人向けIIJモバイルサービスを利用するお客様から頻繁に申告がある問題です
- IIJモバイルサービスの仕様としてAPN設定で、ユーザ名/パスワード/認証方式の入力が必須であり、設定されていないと接続できない仕様となっています
- 一方で、様々な理由で端末が4G接続時にユーザ名/パスワード/認証方式の値を設定しない場合があり、この場合IIJ設備で接続が拒否されて、4G網への接続ができなくなります
- 上記の理由で4G網への接続が拒否された後に、端末が3G網にフォールバックし、3G網への接続時にはユーザ名/パスワード/認証方式が正しく設定されるため、正常に接続が可能となります
- 事象の詳細は紙面の都合で省きますが、4G網と3G網で初期接続時の方法が異なるために発生する事象となります
- 以下は代表的な端末での対応方法となります

(端末例)

スマートフォン(Apple端末全般)

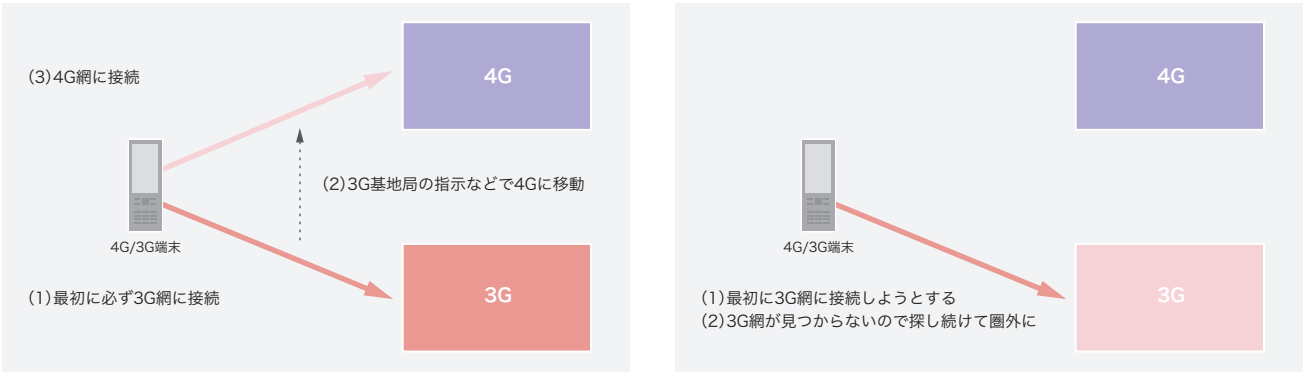
iOS APN構成プロファイルを利用することでこの問題の回避は可能です

通信モジュール全般(Quectel EC25-Jなど)

実装に依存するATコマンド(QuectelではAT+QICSGP)で、事前に通信モジュールに、ユーザ名/パスワード/認証方式を設定することで回避可能です

4.6 むすび

2026年3月31日にNTTドコモの3Gサービス提供が終了した際に、4G(LTE)対応端末でも、4G無線網に接続できなくなる問題があることを本稿では解説しました。3G停波まで1年を切っており、時間的猶予がありませんが、本稿の後半で解説した事象は、気付いていないが発生している場合が多いため、本稿をきっかけとして改めて3G停波対応が大丈夫かを確認していただき、問題なく乗り切れることを切に願います。



3G停波前　　3G停波後

図-3 3G網に最初に接続してしまう問題

執筆者:
大内 宗徳(おおうち むねのり)
IIJモバイルサービス事業本部 MVNO事業部 基盤開発部 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。

Information（1）

IIJアカデミー 第6期の受講生を募集

IIJアカデミーはネットワーク社会の根幹を支える高度な技術をもつIT人材を増やすことを目的に、ネットワーク技術とソフトウェア開発技術に精通したエンジニアを育成するプログラムです。

IIJ アカデミーでは第6期受講生を現在募集しています。

【募集期間】 2025年8月18日(月)～2025年10月6日(月)12:00
【 開 講 日 】 2025年11月4日(火)

第7期受講生は2026年3月頃募集を開始する予定です。
詳細は、IIJアカデミーWEBサイトをご覧ください。

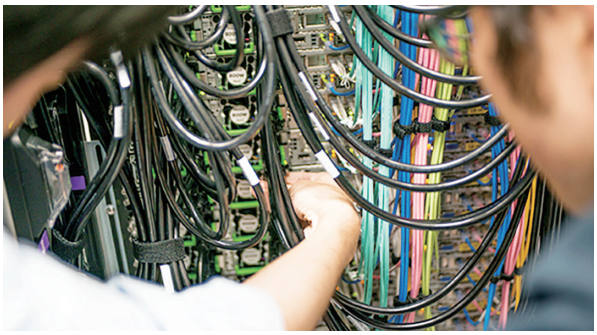
IIJアカデミー
公式サイト

■IIJアカデミーとは

「IIJアカデミー」は未来のネットワーク社会を担うトップエンジニア育成のため、IIJ創業30周年を記念して立ち上げられました。IIJが創業以来培ってきたインターネットサービス開発・運用の知見をベースに、実践的な知識・スキルを習得できる学びの場を提供し、未来のネットワーク社会とIT産業の根幹を支える高度な技術を持つIT人材を育成することを目指しています。

■これからのエンジニアに求められる実践的な学びの場

- 実践的な実習中心の教育プログラム
- マンツーマン方式で個々人の課題や目標に応じた指導
- インターネット事業者ならではの設備を利用した実習環境
- 経験豊富なIIJ現役社員による指導



Information (2)

IIJ Techチャンネル

IIJのエンジニアが技術的な情報や取り組みを動画で紹介します。
最近の技術動向や普段携わっている業務での気づき、インターネットにまつわる小難しい事柄を分かりやすく紹介するミニ解説など、出演者独自の視点でお送りします。

IIJTechチャンネル

各種ブログを更新した際には、以下のX/Facebookアカウントにてお知らせを投稿しています。気になる情報がありましたら、ぜひこちらもフォローしてみてください。

【X】

■ @IIJ_ITS
IIJが行うセミナーのお知らせや各種技術ブログの更新など、様々な技術情報をお届けします。

■ @IIJ_doumae
IIJエンジニアの堂前が興味のある技術ネタについてつぶやきます

■ @SEIL_SMF
IIJが開発するルータ「SEIL（ザイル）」の情報やファームウェアの更新のお知らせなど

■ @IIJ_PR
プレスリリース、イベント情報

【Facebook】

■ IIJ公式ファンページ（https://www.facebook.com/IIJPR）
IIJの公式ファンページです。プレスリリースやお知らせ、技術・開発情報、イベント・セミナー情報など、IIJに関する様々な情報をお届けします。

■ SEIL公式ファンページ（http://www.facebook.com/SEIL.jp）
IIJ独自開発ルータ「SEIL（ザイル）」の公式ファンページです。SEILに関連する最新情報や活用方法、便利な設定方法、開発秘話、などをお届けします。

September 2025 Vol.67

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。

本冊子の情報は2025年9月時点のものです。

IIJ-MKTG019-0067

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