

IIJR

Internet
Infrastructure
Review

Sep.2026

Vol. 71

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
～安定成長が続くトラフィックと
水面下の変化～

定期観測レポート(2)

証明書“47日”時代に備える
「止めないメール基盤」
～自動化×ディフェンス対応で実現する
お客様保護～

フォーカス・リサーチ

国内プロバイダ初、Webメールの
BIMI表示対応
～IIJmioセーフティメールの安全対策～

IIJ

Internet Initiative Japan

Internet Infrastructure Review

September 2026 Vol.71

エグゼクティブサマリ	3
1. 定期観測レポート(1)	4
1.1 概要	4
1.2 データについて	5
1.3 利用者の1日の使用量	5
1.4 ポート別使用量	7
1.5 Cloudflare Radarとの比較	9
1.6 まとめ	11
2. 定期観測レポート(2)	12
2.1 インターネットの安全性を高める暗号化通信技術	12
2.1.1 通信経路暗号化に不可欠なPKI	12
2.1.2 暗号化通信とCA/Bフォーラムの動向	12
2.1.3 サーバ証明書の自動化プロトコル「ACME」	14
2.1.4 IJセキュアMXサービスの事例	15
2.1.5 今後の課題と展望	16
2.2 割合で見るディフェンス対応の効果	17
2.3 送信ドメイン認証とメールの経路暗号化統計	18
3. フォーカス・リサーチ	20
3.1 IJmioセーフティメールにおけるBIMIアイコン表示対応	20
3.2 IJmioセーフティメールについて	20
3.3 BIMIについて	20
3.3.1 BIMIの送信者対応について	22
3.3.2 BIMIの受信者対応について	24
3.4 IJmioセーフティメールでのブランドアイコン表示について	26

エグゼクティブサマリ

当社では2026年5月のAIに関する事業戦略の発表以降、社内業務プロセスへのAI活用の検討が本格化しています。特にソフトウェア開発においては、AIによる効率化や属人化の排除について一定の効果が見込まれることが明らかになっており、複数のプロジェクトで実際に成果が現れるなど、急速に活用が拡大しています。

一方、一部の米国企業で顕在化していたAI利用コストの問題が、当社でも現実味を帯びてきました。大規模モデルの高性能化やAIエージェントの普及により、トークン消費量は急増しており、単純な利用規模の拡大がそのままコスト増加につながるケースも少なくありません。

また、当社のような通信事業者においては、保護すべき「通信の秘密」に関わるデータや顧客情報などの機密情報をAIで扱ううえでの課題もあります。単に「ソブリンAI」や「ソブリンクラウド」を導入するという話ではなく、自社の重要なデータや知的資産をどのようなルールのもとで活用するのかという本質的な課題に直面しているのです。AI活用が競争力そのものになりつつある今、データ主権を維持しながら安全に活用できる基盤技術の重要性はますます高まっています。

こうしたAIを取り巻く環境変化や課題を踏まえ、当社では顧客課題を解決するサービス開発と新たな価値提供の準備を今まさに進めています。

さて、今号の紹介に移ります。

第1章では、恒例のブロードバンド・トラフィックレポートをお届けします。全体としてトラフィックは引き続き安定した成長を続けていますが、水面下では新たな変化の兆候も見え始めています。特に注目したのは、AIエージェントの普及に伴うポットトラフィックの増加と、レジデンシャルプロキシによるトラフィック構造の変化です。不正利用を可能にするレジデンシャルプロキシについては、まだ明らかになっていない部分も多く、現時点で日本への影響は限定的ですが、今後、日本のブロードバンドサービスも攻撃対象となる可能性が示唆されています。

第2章では、サーバ証明書の有効期限短縮という業界全体の大きな変化を背景とした、「IJセキュアMXサービス」における自動化への取り組みを紹介します。2029年にはサーバ証明書の有効期限が47日まで短縮される予定であり、従来の運用手法では対応が困難になります。本章では、ACMEやLet's Encryptを活用した自動更新の仕組み、DANE対応による不正利用抑制の効果、そして送信ドメイン認証やメール経路暗号化の最新動向について解説します。

第3章では、国内プロバイダとして初めて実現した「IJmioセーフティメールサービス」で提供している、Webメール「Mailviewer」におけるBIMI (Brand Indicators for Message Identification) 表示対応について解説します。フィッシングメールやなりすましメールへの対策が重要性を増すなか、利用者が直感的に送信者の正当性を判断するための仕組みとして、BIMIへの注目が高まっています。本章では、BIMIの仕組みや、ブランドアイコン表示に利用される二種類の電子証明書であるVMC (Verified Mark Certificate) 及びCMC (Common Mark Certificate) の活用方法について、IJmioセーフティメールサービスへの実装事例を通じて紹介します。

当社は「技術で社会を支える」という使命のもと、ネットワーク、セキュリティ、データ利活用といった基盤技術の高度化に取り組んできました。今後もこうした基盤技術とAIを適切に融合しながら、持続的なサービス進化と新たな価値創出に取り組んでまいります。



染谷 直 (そめや なおし)

IJ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、IJ入社。直後にIJテクノロジー(2010年にIJに吸収合併)へ出向。IJ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IJ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。昨年度より「IIR」編集長に就き、IJ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 ～安定成長が続くトラフィックと水面下の変化～

1.1 概要

このレポートでは、毎年IJ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、IJ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、新型コロナウイルス感染拡大前の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。

図-1から分かるように、ブロードバンドトラフィック総量は減少しました。これは、IJがIPv6サービスを提供していた某

ISPとの契約が終了した結果、利用者数が減ったことによる影響です。個別事情による減少なので、一般にブロードバンドやIPv6のトラフィックが減っている訳ではありません。ブロードバンドトラフィック量は、INは0.9%の減少、OUTは9.6%の減少となっています。1年前はそれぞれ9%と4%の増加でした。

ブロードバンドに関しては、IPv6・IPv4のトラフィック量も含めて示しています。IJのブロードバンドにおけるIPv6は、IPv4方式とPPPoE方式があります。先述のIPv4利用者数減少の結果、2026年6月時点で、IPv4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44%と、昨年同月よりINは変わらず、OUTで5ポイント減少しました。

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30%、OUTは19%の増加となっています。1年前はそれぞれ29%と9%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。

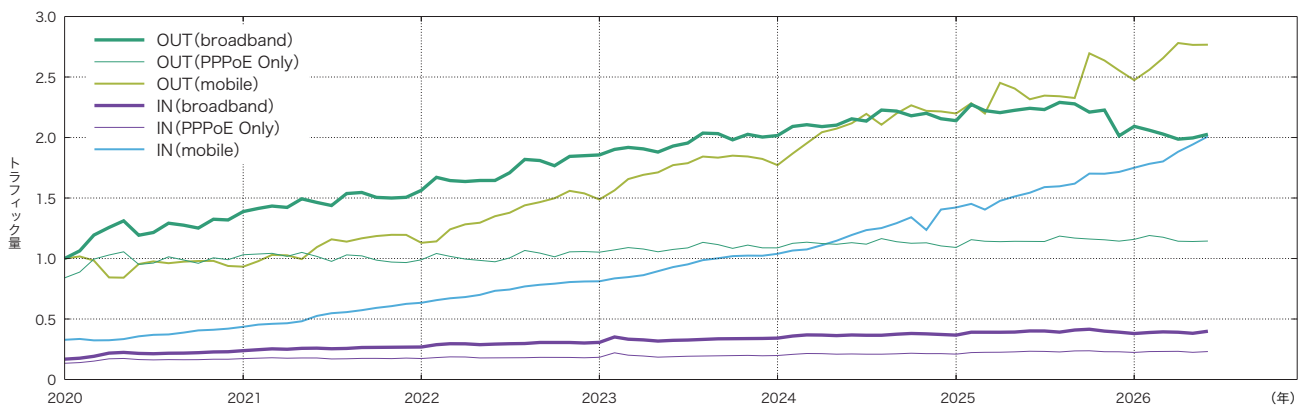


図-1 ブロードバンド及びモバイルの月間トラフィック量の推移

*1 長健二郎. 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. Internet Infrastructure Review. Vol.67. pp4-11. September 2025.

*2 長健二郎. ブロードバンドトラフィックレポート: この5年を振り返って. Internet Infrastructure Review. Vol.64. pp4-11. September 2024.

*3 長健二郎. 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.

*4 長健二郎. 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.

*5 長健二郎. 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.

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、2026年6月1日～6月7日の1週間分のデータを解析して、前回解析した2025年6月2日～6月8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ルド社のtransixサービスを利用し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。

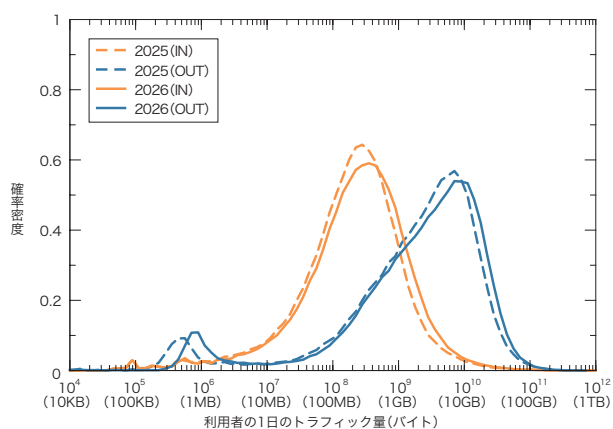


図-2 ブロードバンド利用者の1日のトラフィック量分布
2025年と2026年の比較

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及び図-3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、2025年と2026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。

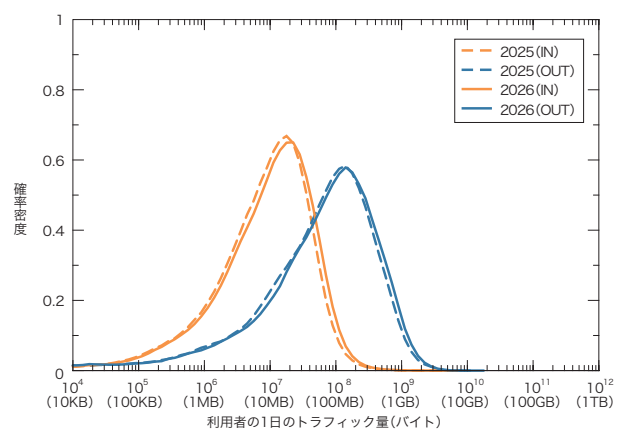


図-3 モバイル利用者の1日のトラフィック量分布
2025年と2026年の比較

*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。

まず、図-2のブロードバンドの分布を見ます。2025年と2026年と比較すると、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-3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。

年	IN (MB/day)			OUT (MB/day)		
	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
2026	1067	241	355	7746	3059	7943

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

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。分布の最頻出値を2025年と2026年で比較すると、INでは282MBから355MBに、OUTでは6310MBから7943MBに増えています。伸び率で見ると、INで1.26倍、OUTも1.26倍となっています。一方、2026年の平均値は、INで1067MB、OUTで7746MBでした。2025年には、それぞれ886MBと6538MB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IPv6利用者を統合した数字になっています。

表-2はモバイルの値の推移で、2026年の最頻出値はINで18MB、OUTで141MB、平均値はINで23MB、OUTで194MBです。2025年の最頻出値はINで16MB、OUTで126MB、平均値はINで19MB、OUTで172MBでした。

図-4及び図-5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。

年	IN (MB/day)			OUT (MB/day)		
	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
2026	22.5	11.1	17.8	194.4	82.5	141.3

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

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、2025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49%、INの71%を占めています。更に、上位1%の利用者がOUTの13%、INの41%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11%、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。

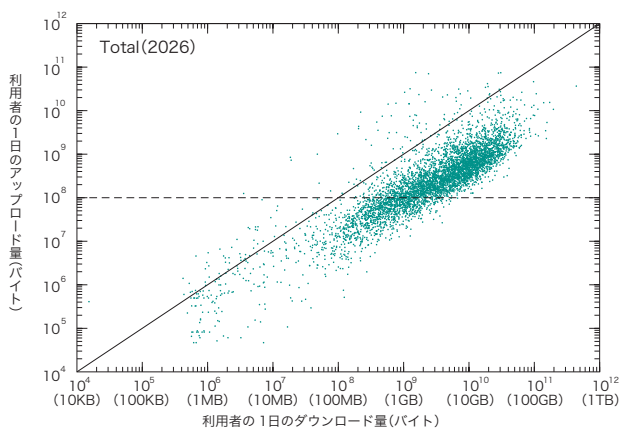


図-4 ブロードバンド利用者ごとのIN/OUT使用量

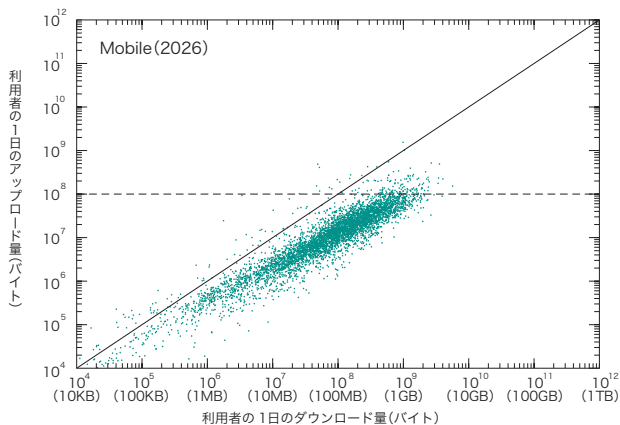


図-5 モバイル利用者ごとのIN/OUT使用量

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known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えます。

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。2026年の全体トラフィックの64%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5%で1ポイント減っています。QUIC

year	2022	2023	2024	2025	2026
protocol port	(%)	(%)	(%)	(%)	(%)
TCP	71.6	70.5	67.5	65.5	64.1
< 1024	65.4	64.8	61.1	59.8	58.5
443(https)	55.7	56.9	53.8	53.2	52.5
80(http)	8.9	7.2	6.5	5.9	5.2
993(imaps)	0.1	0.1	0.1	0.2	0.2
22(ssh)	0.1	0.1	0.1	0.1	0.1
183	0.2	0.2	0.2	0.1	0.1
>= 1024	6.2	5.7	6.4	5.7	5.6
31000	0.9	1.1	1.2	1.6	1.7
8080	0.3	0.4	0.3	0.3	0.3
7664	0.0	0.0	0.7	0.3	0.3
1935(rtmp)	0.2	0.2	0.3	0.2	0.1
UDP	24.3	25.4	28.2	30.6	31.8
443(https)	16.3	18.2	21.0	23.1	24.6
4500(nat-t)	0.8	1.0	0.9	0.7	1.1
3478(stun)	0.0	0.2	0.2	0.3	0.5
ESP	3.8	3.8	4.0	3.6	3.8
GRE	0.2	0.1	0.2	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

プロトコルで使われるUDP443番ポートは、25%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1.7%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

year	2022	2023	2024	2025	2026
protocol port	(%)	(%)	(%)	(%)	(%)
TCP	71.6	71.0	71.0	69.8	69.0
443(https)	42.3	42.1	42.2	37.8	35.0
80(http)	4.1	3.5	1.8	1.5	0.8
993(imaps)	0.1	0.1	0.1	0.1	0.1
1935(rtmp)	0.1	0.2	0.1	0.1	0.1
UDP	24.4	26.5	27.5	29.3	30.4
443(https)	17.9	20.9	22.5	24.8	26.5
4500(nat-t)	2.7	2.5	1.8	1.5	1.1
51820	0.1	0.2	0.3	0.3	0.3
53(dns)	0.2	0.2	0.2	0.2	0.2
8801	0.3	0.2	0.1	0.1	0.1
ESP	3.9	2.4	1.4	0.8	0.5
ICMP	0.0	0.1	0.0	0.1	0.1
GRE	0.0	0.0	0.0	0.0	0.0

表-4 モバイル利用者のポート別使用

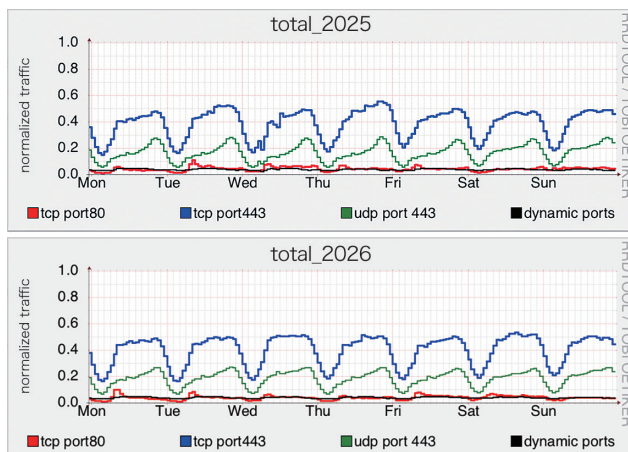


図-6 ブロードバンド利用者のポート利用の週間推移
2025年(上)と2026年(下)

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IPv6を含まないで、固定ブロードバンド全体の傾向を表しているとは限りません。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、IPv6でも同様の傾向があると考えられます。

図-6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、2025年と2026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。2025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-7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。2025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、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。

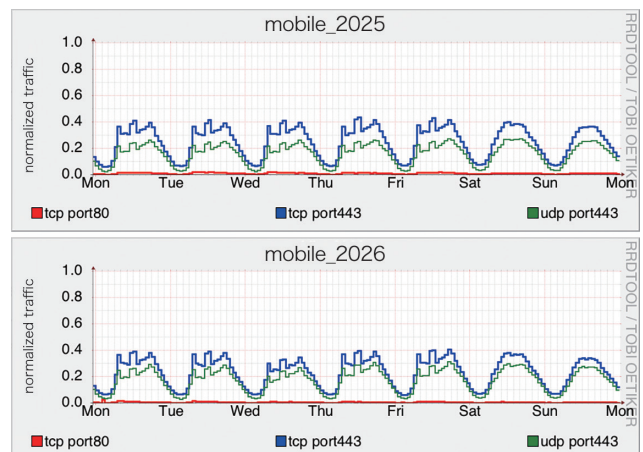


図-7 モバイル利用者のポート利用の週間推移
2025年(上)と2026年(下)

1.5 Cloudflare Radarとの比較

今回は、本稿の報告内容を米国のクラウドフレア社が公開している情報と比較してみます。クラウドフレア社は、コンテンツ配信、セキュリティサービス、サイバー攻撃対策、DNSサービスなどのネットワーク基盤サービスをグローバルに提供する大手ネットワークサービス企業です。

クラウドフレア社のCloudflare Radar (<https://radar.cloudflare.com/>) は、彼らのグローバルネットワークとそのサービスで観測されたトラフィックやプロトコル情報を解析して無償提供している、2020年に始まった公開サービスです。最近では、筆者がトラフィックのトレンド情報を得るために、最も利用している公開サービスでもあります。

Cloudflare Radarでは、Web上で可視化された情報をグローバル、地域別、国別、あるいはAS番号別にブラウズ可能な他、APIを使ってデータを取得することもできます。

図-8に示したのは、日本の情報を今回のレポートと同じ6月1日から1週間分表示したものです(Cloudflare Radarの時刻はUTCなので、正確には本稿とは9時間ずれています)。上部のトラフィックグラフを見ると、日本時間で夜の11時ごろにピークがあり、また、土日には平日より昼間のトラフィックが多いなど、本稿で報告しているブロードバンドトラフィックのパターンとおおむね一致しています。

元になっているデータは、あくまでクラウドフレア社のサービスネットワークで観測したもので、また、各情報に具体的にどの

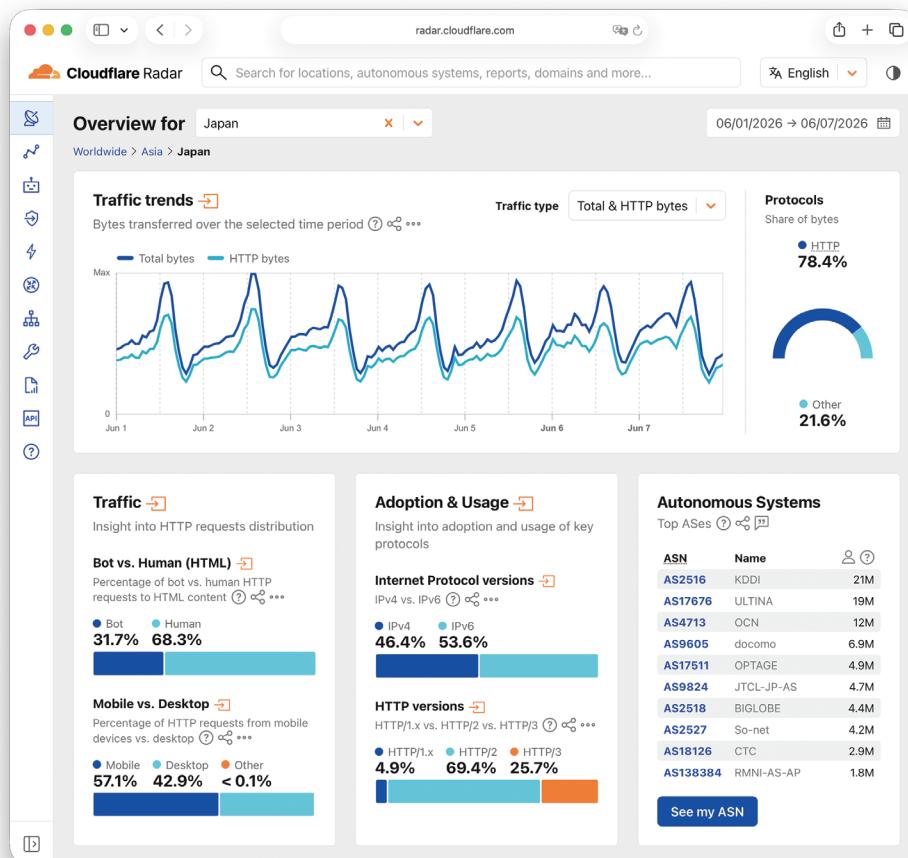


図-8 Cloudflare Radar: Webインタフェース

サービスのデータを使っているかも開示されていません。今回取り上げるトラフィックやプロトコルの情報は、主にコンテンツ配信のHTTPアクセスログデータを使っていると推測できます。Webサーバがユーザからのリクエストを記録するHTTPアクセスログには、日時、クライアントIPアドレス、リクエストしたコンテンツのURL、コンテンツサイズ、ステータスコード、ブラウザ情報などが記録されます。

このように、観測対象も観測方法も本稿とはまったく違うので、必ずしも直接比較はできないのですが、取り扱っている項目に共通点も多く、いろいろ参考になります。また、同じ期間のグローバル及び国別の情報と比較することができるため、日本のトラフィックの特徴を把握することもできます。

表-5に、Cloudflare Radarから得られたグローバル、米国、イギリス、フランス、韓国、日本、そして、AS2497（IIJのAS番号）の6月1日からの1週間の情報と、本稿のブロードバンドとモバイルの情報を比較します。Cloudflare Radarでは、国別などの地理情報の特定には、外部のIPジオロケーションデータベースを利用しているとのこと。

なお、AS2497の情報はあくまでクラウドフレア社が外部から観測したIIJのトラフィックであり、ここでは本稿で報告しているブロードバンドとモバイル以外のビジネストラフィックが多くを占めています。したがって、比較の対象としては適切ではありませんが、AS番号別の表示例として挙げています。

以下に、表の行の項目について見ていきます。最初のHTTPの割合は、トラフィック量に占めるHTTPの割合で、その下のHTTP/1.x、HTTP/2、HTTP/3を合算したものだと考えられます。HTTPのバージョンはアクセスログの情報からだと推測できます。IIJデータでは、HTTPプロトコルのバージョンは分からないので、TCP80番ポート、TCP443番ポート、UDP443番ポートの割合を記入しています。

HTTPの割合は大体70%程度ですが、韓国が94%と突出して高くなっています。IIJデータのモバイルでHTTP割合が低いのは、一部の企業向けサービスの影響です。

IPv4とIPv6の割合についても、アクセスログの情報からだと推測します。IIJデータのブロードバンドでは正確な割合は分からないため、PPPoEとIPoEの割合を記入しています。IPv6割合は、フランスが68%と高く、韓国が17%と低いのが目立ちます。

モバイルとデスクトップの区別は、やはりアクセスログのUser-Agent（ブラウザ情報）を元にして推測できます。日本はモバイルが57%と高くなっています。

ボットと人間の区別についても、アクセスログのUser-AgentやRefererなどを元に、機械学習なども使って推測しているようです。世界的には、ボットのトラフィック増加が目立っているようですが、日本と韓国はボット割合が低くなっています。

	Cloudflare Radar							IIJ	
	Global	US	UK	France	Korea	Japan	AS2497	broadband	mobile
HTTP(%)	76.2	74.7	77.8	71.2	94.1	78.4	84.5	82.3	62.3
HTTP/1.x(%)	9.0	7.9	7.7	6.3	8.0	4.9	9.1	6.3	1.3
HTTP/2(%)	58.6	62.6	64.2	59.0	54.6	69.4	71.5	63.8	56.2
HTTP/3(%)	32.4	29.6	28.1	34.8	37.4	25.7	19.3	29.9	42.5
IPv4(%)	58.6	47.1	60.9	32.5	83.3	46.4	79.5	56.7	68.3
IPv6(%)	41.4	52.9	39.1	67.5	16.7	53.6	20.5	43.3	31.7
Mobile(%)	39.9	28.8	42.9	38.9	42.3	57.1	51.0	-	-
Desktop(%)	60.0	71.1	56.9	59.7	57.7	42.9	49.0	-	-
Bot(%)	57.1	69.7	47.2	65.7	35.1	31.7	12.8	-	-
Human(%)	42.9	30.3	52.8	34.3	64.9	68.3	87.2	-	-

表-5 Cloudflare Radar国別トラフィックとIIJデータの比較

1.6 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。前回のレポートでは、そろそろ次の変化の波が来る可能性について述べましたが、今のところまだその兆候はうかがえません。

とは言うものの、世界的に見るとボットのトラフィックが増えています。日本のボット割合はまだ低いのですが、水面下で変化が起きている、やがて日本にも波及してくる可能性は十分にあります。

前回のレポートでは、次の変化の考察の中で、AIチャットボット利用が増えてもブロードバンドトラフィック量への影響は少ないと予想しましたが、今回はもう少し深掘りしてみます。

従来型のボットは、検索エンジン用途などの目的で、特定の組織から来るものが多く、直接ブロードバンドには関係ありませんでした。AI学習用のコンテンツを幅広く収集するスクレイピングボットも、これまではこのタイプが主流で、Cloudflare Radarが報告しているボットもこのタイプが主流ではないかと思われます。

しかしながら、AI利用拡大に伴い、ボットの影響がブロードバンドにも現れる2種類のシナリオが想定できます。1つめのシナリオは、AIエージェントの一般利用の拡大に伴って、ユーザのデバイス上で動くAIエージェントが自身で検索したり、コンテンツにアクセスすることによる影響です。AIエージェントの利用が拡大すると、ブロードバンドにおけるボット割合も上がります。

これだけだと人間の代わりにAIボットがWebアクセスするだけとも考えられますが、更に長期的な影響も考えられます。現

状の検索エンジンは人間が検索することを想定していて、人間が使いやすいように最適化されています。更に、広告によって収益を上げる構造になっています。ところが、AIエージェントにとっては、このような最適化や広告は無用なだけでなく、出力品質低下要因でもあります。そこで、AIエージェント用にコンテンツを加工する、もとい、加工を取り除くサービスも台頭してきています。つまり、AIエージェントの利用拡大で、これまでのWebの世界を牽引してきた検索と広告という構造そのものが変化を強いられる可能性が考えられるのです。

2つめのシナリオは、レジデンシャルプロキシと呼ばれる一般ユーザのデバイスを踏み台にしてアクセスを行うサービスの影響です。レジデンシャルプロキシを使うと、指定した国や都市の一般ユーザからのアクセスを装うことができるので、これをブロック回避手段として悪用する攻撃や、一般ユーザになりすましてAI学習用のデータ取得をする利用が増えているとの報告があります^{*7}。そして、ニーズがあるので、不正な手段やグレーな手法によって、一般ユーザのデバイスを所有者が気づかないうちにレジデンシャルプロキシ化して第三者に転売する不正なビジネスが横行しているようです。レジデンシャルプロキシに関してはまだ分からないことも多く、有効な検出方法もブロック方法も確立されていません。日本では、まだレジデンシャルプロキシの影響は限定的だとされていますが、高帯域かつ高品質の日本のブロードバンドサービスが狙われることを想定しておく必要があります。

日本においても、ボットトラフィックの拡大がそう遠くない将来に起こると想定できますが、その拡大ペースによって具体的にどのような影響をもたらすかはまだよく分かりません。今後とも、このような変化の兆候に注意を払い、適切な対応が取れるように準備をしていきたいと考えています。



執筆者：
長 健二郎（ちょう けんじろう）
IJJ 技術研究所 所長。

*7 Craig Labovitz. One year later: the residential proxy botnet problem got bigger, not smaller. 23 Jun 2026. (<https://www.nokia.com/blog/one-year-later-the-residential-proxy-botnet-problem-got-bigger-not-smaller/>)。

証明書“47日”時代に備える「止めないメール基盤」 ～自動化×ディフェンス対応で実現するお客様保護～

2.1 インターネットの安全性を高める暗号化通信技術

2.1.1 通信経路暗号化に不可欠なPKI

現代社会においてインターネットは必要不可欠な存在となっており、その通信の安全性を確保することが極めて重要です。インターネットの初期には、通信内容が暗号化されずに伝送されることが一般的でしたが、2013年、元米国CIA職員だったエドワード・スノーデン氏による米国NSAの世界規模の個人情報収集・監視活動の告発が明るみに出たことで、通信の安全性とプライバシーへの関心が高まりました。

以来、インターネットにおける通信の経路暗号化(以降、「暗号化」)が急速に進み、現代のインターネットはおおむね常時TLSで暗号化されるようになりました^{*1}。この暗号化には、PKI(Public Key Infrastructure)と呼ばれる公開鍵基盤が重要な役割を果たしています。PKIでは認証局(Certificate Authority)^{*2}が、通信相手の認証や暗号化に必要なサーバ証明書の発行をしていますので、認証局とそのサーバ証明書は、現代の暗号化通信においてとても重要な役割を担っていることが分かります。

2.1.2 暗号化通信とCA/Bフォーラムの動向

皆さんが日々利用しているWebブラウザはインターネットへの入り口です。暗号化通信を開始する際、利用者は意識せずともブラウザは通信相手を信じるかを最終的に判断しています。そこで2005年、認証局(CA)とブラウザ(Browser)ベンダーが同じテーブルについてインターネットの安全性を議論・規律する「CA/Bフォーラム^{*3}」という業界団体が設立されました。

CA/Bフォーラムでは、認証局がどのように振る舞うべきかのルールを策定し、認証局が遵守すべき最低限の要件をBR(Baseline Requirements)^{*4}として定めて公開しています。現代では認証局がCA/Bフォーラムのメンバーであるかどうかに関わらず、CA/Bフォーラムでの決定は事実上、強制力を持つものとして扱われています。

そして2024年10月、CA/Bフォーラムにおいて、公開認証局が発行可能なサーバ証明書の有効期限を段階的に47日まで短縮する提案(SC-081)^{*5}がApple社のメンバーにより提出されました。当時、発行可能なサーバ証明書の最大有効期限は398日の約1年間であり、年1回程度のサーバ証明書の更新で運用が可能でしたが、この提案が可決されると、証明書の更新頻度は約1ヵ月に1回となるため、運用体制や業務フロー・仕組みの見直しが求められることになります。

社内外のサーバ運用者視点では、サーバ証明書の更新作業にかかる工数やオペレーションリスクの増大は、事業継続性や運用上のリスクを高める要因となり得ます。特に、サーバ証明書の更新に関連する作業は、事業活動に直接的な利益を生み出さず、サービス利用者にとっても付加価値がありません。こうした作業負担が増加すると、場合によっては事業運営の根幹を揺るがす可能性も否定できない状況です。

この少々過激とも思える提案は様々な賛否と議論が交わされましたが、2025年4月、最終的にはフォーラムメンバーの投票により賛成多数で可決されました^{*6}。表-1は、有効期限短縮のスケジュールを整理したものです。

*1 ウェブ上でのHTTPS暗号化 - Google透明性レポート(<https://transparencyreport.google.com/archive/https/overview>)。

*2 インターネットの通信は1対多になるため、事前にすべての通信相手と信頼関係を作るのは現実的ではありません。そこで認証局という第三者を介在し、あらかじめ信頼している認証局が発行した証明書を相手から提示されたら、その通信相手は信頼できるという方法をとることで担保しています。なお、あらかじめ信頼している認証局は利用者のOSやブラウザに組み込まれており自動的に更新もされるため、通常利用者が意識することはありません。こうした手続きは、現実世界における役所が発行する営業許可証の仕組みに似ています。

*3 CA/Browser Forum(<https://cabforum.org/>)。

*4 Baseline Requirements(<https://cabforum.org/working-groups/server/baseline-requirements/>)。

*5 SC-081: Introduce Schedule of Reducing Validity and Data Reuse Periods(<https://github.com/cabforum/servercert/pull/553>)。

*6 Initial Vote Results on Ballot SC-081v3: Introduce Schedule of Reducing Validity and Data Reuse Periods(<https://groups.google.com/a/groups.cabforum.org/g/servercert-wg/c/9768xgUUfhQ>)。

本稿発行時点で1回目の短縮は既に終わっており、2026年9月時点で発行できるサーバ証明書の最大有効期限は200日間です。認証局による発行の事務手続きや、更新時に設ける安全マージンを考慮すると、実際に利用できる期間はこれよりも短くなることがあります。

なぜCA/Bフォーラムでは、このような決定をしたのでしょうか？こうした背景と目的は次のとおりです。

1. サーバ証明書の信頼性向上

- 認証局からサーバ証明書を発行する際には発行審査の手続きがあります。しかし、一度発行されたサーバ証明書が、有効期間中に再検証されるわけではありません^{*7}。従って、発行したサーバ証明書は時間の経過と共に信頼性が低下していくと考えることができますので、そのような証明書を時間の経過で排除することができます。
- コンピュータの計算速度は日進月歩で進化しており、また研究によって暗号の解読手法が明らかになることがあります。これを暗号アルゴリズムの危殆化(きたいか)と呼びます。危殆化によって従来の暗号に対する信頼性が低下した際に必要となる証明書の再発行・再設定を早めることができます^{*8}。

2. セキュリティリスクの低減

- 認証局が発行するサーバ証明書は、ペアとなる秘密鍵を厳重に管理しなければなりません。万が一、秘密鍵が漏えいした場合、攻撃者によるサーバのな

りすまじや、中間者攻撃などに悪用されるリスクがあります。

- 過去には、認証局によるサーバ証明書の誤発行が発生した事例が確認されています。有効期限を短縮することで、誤発行された証明書が悪用されるリスク期間を限定できるため、セキュリティ上の対策として有効です。

3. ライフサイクル管理と品質の向上

- 有効期限が短くなると、短いサイクルで反復的な作業を強いられるようになるため、運用現場ではオペレーションを自動化するモチベーションにつながります。
- サーバ証明書の更新を自動化すれば、更新作業を失念してサーバ証明書の有効期限が切れてしまうといった事故を防ぐことができます。また更新作業に伴う人為的なオペレーションミスが発生するリスクも低減することができ、サービスの安定性を向上させることができます。

特に3番目は、サーバ証明書の有効期限に関わらず、運用現場では工数省力化の観点で大きなメリットがあります。

	発行可能な証明書の期限
2026/03/14より前	最大398日間
2026/03/15以降	最大200日間
2027/03/15以降	最大100日間
2029/03/15以降	最大47日間

表-1 有効期限短縮のスケジュール

*7 発行済サーバ証明書を再認証するのではなく失効させ、それを確認できる方法として、RFC 5280(<https://datatracker.ietf.org/doc/html/rfc5280>)のCRL(Certificate Revocation List)、RFC 6960(<https://datatracker.ietf.org/doc/html/rfc6960>)のOCSP(Online Certificate Status Protocol)という仕組みがあります。ただし、失効情報の配布や確認方法は実装によって異なり、いずれのRFCでも実装はOPTIONAL(任意)とされています。

*8 2015年ごろにサーバ証明書で利用されているSHA-1アルゴリズムの危殆化(きたいか)が発表された事例があります(<https://www.cryptrec.go.jp/topics/cryptrec-er-0003-2015.html>)。当時のサーバ証明書の有効期限は最大5年間でしたが、危殆化が発表されても、なかなか証明書の入れ替えが進まなかったことも、今回の決定を後押しする要因として挙げられています。

2.1.3 サーバ証明書の自動化プロトコル「ACME」

このような状況を踏まえ、証明書更新作業の自動化が求められています。では、どのようにこのプロセスを自動化すれば良いのでしょうか。サーバ証明書の更新を自動化するプロトコルとして、RFC8555で標準化されたACME(Automatic Certificate Management Environment)^{*9}がよく知られています。英語圏では「アクミー」と発音されます。

ACMEに対応した認証局の中でも、Let's Encryptは特に広く認知されています。同認証局は非営利団体ISRG(Internet Security Research Group)によって運営されており、サーバ証明書の発行から利用まですべてのサービスを無償で提供しています。現在、世界中で7億以上のWebサイトがLet's Encryptのサービスを利用しており、その普及率は非常に高いと言えます。

また、Let's Encryptに対応したACMEクライアントは複数の実装がインターネット上で公開されており、次のようなクライアントが有名です。仕組みがシンプルなので、動きを確認する目的で手作業でも証明書を取得することができます。

- ・ Certbot(広く利用されておりプラグインが豊富)
- ・ acme.sh(シェルスクリプトのため依存が少ない)
- ・ lego(Go製で高速・シンプル)

サーバ証明書を発行するためには、認証局が発行審査を行う必要がありますが、このプロセスも当然自動化されています。なお、サーバ証明書には発行審査の違いとして、表-2の3種類がありますが、どの証明書を利用しても暗号化やTLSの機能面に差はありません。本稿ではDVについて記載します。

サーバ証明書を発行する方法として、主に「HTTP-01 Challenge」と「DNS-01 Challenge」の2つが標準的に利用されています。表-3は、それぞれ特徴や手順をまとめたものです。

証明書の種類	発行審査の違い
DV(Domain Validation)	ドメイン名の管理権限を確認する
OV(Organization Validation)	DVに加え、組織の実在・申請権限確認をする
EV(Extended Validation)	OVに加え、追加・拡張された審査を実施する

表-2 サーバ証明書の種類

	HTTP-01 Challenge	DNS-01 Challenge
発行審査の方法	サーバ証明書を発行しようとするWebサーバの管理権限を検証する。認証局が指定したファイルをWebサーバ上に設置し、そのファイルをHTTP経由で正しく返すことができるかを認証局が確認する。	サーバ証明書を発行しようとするドメイン名の管理権限を検証する。認証局が指定したトークンを元に生成した値をDNSのTXTレコードに記載できるかを認証局が確認する。
メリット	・サーバ証明書の発行に伴う手続きがWeb単体で完結する。 ・DNSサーバの変更が不要なため手軽。	・Webサーバが外部公開されていない環境でも取得が可能。 ・ロードバランサーなどで複数のサーバを管理・冗長化している環境に向いている。 ・ワイルドカード証明書の発行ができる。
デメリット	・HTTP(80)ポートが外部からアクセスできる必要があり、Webサーバを持たない環境では利用できない。 ・ロードバランサー配下では、検証の要求(以下、手続き4.)を適切に応答できる仕組みが必要。	・DNSのTXTレコードを操作できる権限が必要。 ・ACMEクライアントと同期的にDNSを操作する必要があるため、自動化するためにはDNSのAPIなどが必須。
手続き	1.ACMEクライアント→CA サーバ証明書を要求 2.CA→ACMEクライアント HTTP-01 Challengeとなるトークンを提示 3.ACMEクライアント Webサーバの/.well-known/acme-challenge/<token>ファイルを作成 4.CA→Webサーバ HTTP GETでアクセスしファイルの存在・内容を検証 5.CA 内容が一致すれば検証成功とし証明書を発行する 6.ACMEクライアント 3.で作成したファイルを削除	1.ACMEクライアント→CA サーバ証明書を要求 2.CA→ACMEクライアント DNS-01 Challengeとなるトークンを提示 3.ACMEクライアント DNSに_acme-challenge.<domain>のTXT レコードを追加 4.CA→DNS _acme-challenge.<domain>を問い合わせ・内容を検証 5.CA TXTレコードの値が一致すれば検証成功とし証明書を発行する 6.ACMEクライアント 3.で追加したDNSレコードを削除

表-3 サーバ証明書の発行方法の特徴や手順、メリット・デメリットの比較

*9 RFC8555 Automatic Certificate Management Environment(ACME) (<https://datatracker.ietf.org/doc/html/rfc8555/>)。

2.1.4 IIJセキュアMXサービス^{*10}の事例

ここまで、Webブラウザで暗号化通信を行う際にはサーバ証明書が必要であることを説明しましたが、メールの暗号化通信においても、SMTPの拡張機能であるSTARTTLSを利用する際、メールサーバ側でサーバ証明書が必要です。従って、CA/Bフォーラムでの決定はメールサーバの運用もその例外ではなく、同じ影響を受けることになります。

IIJセキュアMXサービスでは、インターネット経由でメールを受信するサーバだけでなく、お客様のメールクライアントやメールサーバから送信されるメールをリレーする送信サーバ、更にWebメールやAPIのエンドポイントなど、多岐にわたる機能を提供しています。同サービスにおいて、サーバ証明書の更

新が必要となる対象を調査したところ合計で13カ所あることが分かりました。また、機能ごとに可用性と性能向上のために冗長化・スケールアウトしており、すべてのサーバの証明書が更新対象です。

なお、CA/BフォーラムがSC-081の提案を行う前の2023年3月、Google社がサーバ証明書の有効期限を最大90日に短縮する方針を発表していました^{*11}。その後、CA/Bフォーラムでサーバ証明書の有効期限短縮に関する議論が活発になっていることに着目し、IIJセキュアMXチームでは、先んじた対策が必要と判断、社内で検討を開始していました。

図-1は、構成の概略図です。

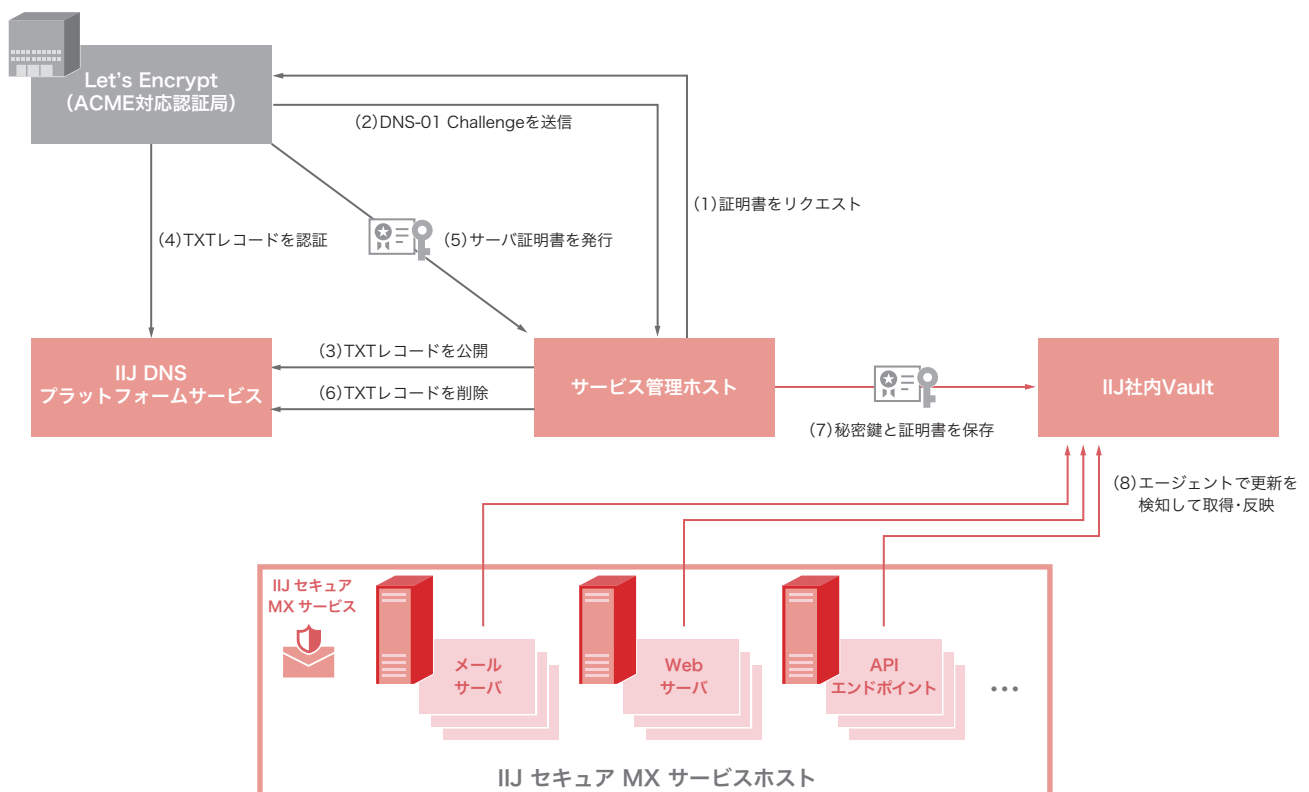


図-1 IIJセキュアMXサービスにおけるサーバ証明書の自動更新概略図

*10 企業向けクラウド型メールセキュリティサービス (<https://www.ij.ad.jp/biz/smx/>)。

*11 "Moving Forward, Together"- Chrome Root Program Policy (<https://chromium.googlesource.com/website/+5943ad5e004c1cde2f869f1d67008a729e9ec12e/site/Home/chromium-security/root-ca-policy/moving-forward-together/index.md>)。

IJセキュアMXサービスはメールサーバのようにWebインタフェースを持たないサービスがあること、ワイルドカードの証明書が利用できること、複数のサーバに証明書を配布する必要があることから、DNS-01 Challengeを利用しています。

幸いにもIJにはIJ DNSプラットフォームサービス^{*12}という、API経由でDNSレコードを編集できるサービスがあり、Let's Encrypt対応のACMEクライアント「lego」が、同サービスに標準対応しています^{*13}。従って個別に実装する必要があるのは、取得した証明書を各サーバに配布する部分(8)のみです。また、秘密鍵と証明書は社内のシークレット情報を保管するVault^{*14}に格納し(7)、各サービスホストのエージェントが更新を検知して取得・反映する仕組みとしました。legoは後処理のプロセスも追加可能なので、この拡張も容易です。

チームメンバーによるPoC (概念実証)を経て社内稟議が承認され、2024年9月よりサーバ証明書更新の自動化を開始しました。当初の想定どおり、運用チーム内でサーバ証明書の更新作業をすることが不要となり、作業工数の大幅な削減と人為的ミスなどのリスク低減を同時に実現することができました。図-2は社内の経緯とサーバ証明書の有効期限のタイムラインを示したものです。

なお、社内稟議及び作業前のリスクアセスメントにおいて、認証局の変更によるリスクが重要な検討項目として挙げられま

した。特に、当時はメールサーバにLet's Encryptを導入している他社事例が存在しない状況だったため、未知の運用リスクやサービス安定性への影響が懸念されました。これらのリスクについては、事前にお客様への十分なお案内を行った上で、サービスとしてリスクを受容する方針を取りました。その結果、運用開始後に大きな問題や反響は発生せず、スムーズな移行が実現しました。新たな技術導入に積極的に取り組み、サービス進化を推進できたことは、現場にとっても大きな成果となったのです。

2.1.5 今後の課題と展望

今回、Let's Encrypt及びACMEの仕組みを活用することでサーバ証明書の更新自動化を実現しました。しかしながら、万が一Let's Encryptのサービスが停止すると、そこがサービス全体の単一障害点となるリスクが残る点は、IJセキュアMXサービスに限らず、グローバルに共通する課題として認識されています。このリスクは有効期限が短くなればなるほど大きくなります。

このような背景を踏まえ、IJでは単一障害点のリスクを軽減し、サーバ証明書の発行・更新を自動化する新たなサービスの開発に取り組んでいます。IJサービスのみならず、サーバ証明書の管理で課題をお持ちのお客様にも、まもなく本ソリューションをご提案できる予定ですので、続報をお待ちください。

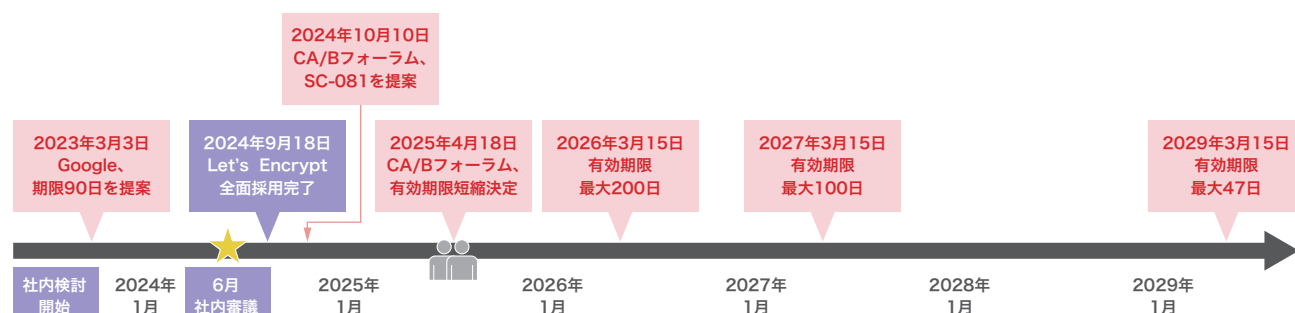


図-2 IJセキュアMXサービスの経緯とCA/Bフォーラムの動き

*12 IJ DNSプラットフォームサービス(<https://www.ij.ad.jp/biz/dns-pfm/>)。

*13 legoのIJ DNSプラットフォームサービスへの対応について(<https://eng-blog.ij.ad.jp/archives/13861>)。

*14 Vaultを使うる基盤として整備し、みんなに使ってもらえるようになるまで(<https://speakerdeck.com/takahiko/building-vault-as-a-core-platform-and-driving-broad-adoption>)。

2.2 割合で見るディフェンス対応の効果

メールサービスが悪用されてフィッシングメールなどの送信に利用されてしまうケースが後を絶ちません。このような不正利用はIJに限らず、他ISPや他社サービスでも日常的に発生しています。

そこでIJセキュアMXサービスでは、2024年5月1日より、お客様を保護しサービスの品質を守るための新しい取り組みを開始しています。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段階で必要な範囲で通信を制限するもので、「ディフェンス対応」と名付けました^{*15}。

図-3はabuse対応とディフェンス対応の件数を集計し、積み上げたグラフの最新版です。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ています。

グラフから読み取れるのは、次の3点です。

- ・ ディフェンス対応により、不正利用によるメール送信の過半数(黄色)を事前に抑制することに成功しています。
- ・ 実際に悪用が確認されてから通信を制限するabuse対応の件数(青色)に着目すると、それまでの水準より約5分の1までに減少しています。
- ・ 従来は横ばいで推移していた通信制限の総件数が、2025年度以降は減少傾向へと転じています。

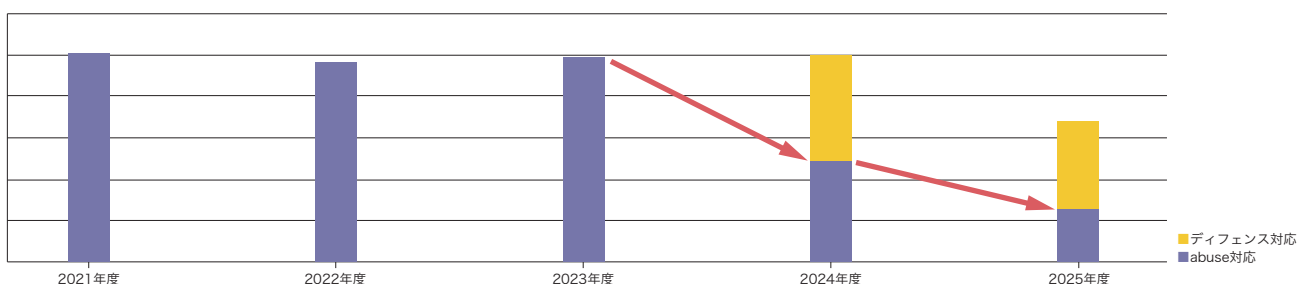


図-3 abuse対応とディフェンス対応件数比較

*15 取り組みの詳細は、IIR Vol.63「日々高度化するサイバー攻撃からお客様を保護するための取り組み」をご参照ください(<https://www.ij.ad.jp/dev/report/iir/063/01.html>)。

IIJでは不正利用を防ぐためのモニタリングを24時間体制で実施しており、通信制限を行った際には、お客様へのご連絡を行うため、サポート部門とも連携しなければなりません。本業務は営業時間外や休日、深夜帯も含めて対応しています。

ディフェンス対応の取り組みにより、こうした不定期で突発的なabuse対応件数が約80%削減されていることは、対応エンジニアの業務負担の軽減だけでなく、インターネットインフラの安定運用に大きく寄与していることが実際のデータからも明らかになりました。また、メールサービスの不正利用件数が減少していることも、実際の統計から裏付けられており、「ディフェンス対応」の有効性が実証されています。

サイバー攻撃は日々進化しています。お客様が安心してサービスをご利用いただけるよう、IIJでは、今後もお客様を保護するための研究・取り組みを続けてまいります。

2.3 送信ドメイン認証とメールの経路暗号化統計

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-4～図-7に示します。期間は2026年3月の1ヵ月です。

前回の報告^{*16}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上昇していますが、いくつか注意すべき点

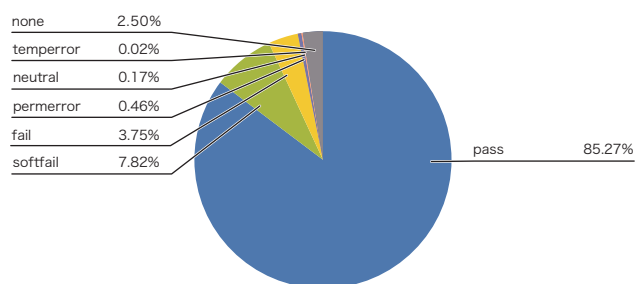


図-4 SPFによる認証結果割合

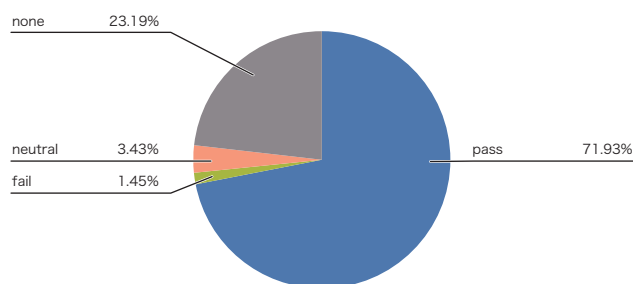


図-5 DKIMによる認証結果割合

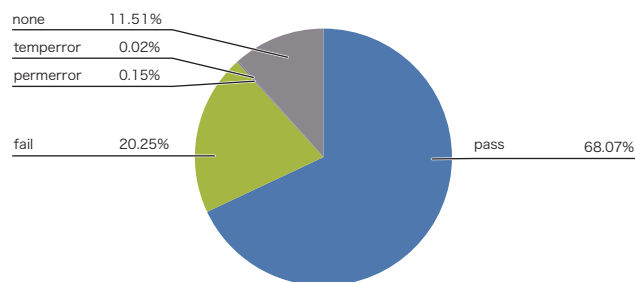


図-6 DMARCによる認証結果割合

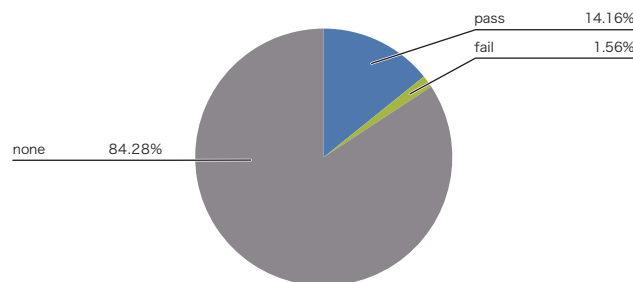


図-7 ARCによる認証結果割合

*16 Internet Infrastructure Review (IIR) Vol.67 (<https://www.iiij.ad.jp/dev/report/iir/067/02.html>)。

があります。昨年度の特徴は、日本を標的にしたフィッシングメールが急増しており、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多数を占めていたことでした。

従って、これまでの報告を踏まえて考察すると、送信ドメイン認証の検証に失敗したメールの割合が戻った、または攻撃者も送信ドメイン認証に対応したフィッシングメールを送信していると考えられます。実際にIJで運用しているハニーポットに着信したメールで、送信ドメイン認証に対応したフィッシングメールを観測しています。どのセキュリティ対策にも言えることですが、複数の対策を効果的に組み合わせることが肝要です。

次にIJ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-8は受信メールに対する経路暗号化の種類と割合です。2025年10月ごろからTLSv1.3で接続される割合が増加していることが読み取れ、TLSv1.0/1.1での接続はほぼ見られなくなりました。

図-9はIJ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集計ですが、前回の報告と同様、おおむね100%に近い推移で経路暗号化が行われています。時折、100%から落ち込んでいるときが見受けられますが、暗号化非対応のメールサーバに大量のメールが配信されたときのデータが影響を及ぼしているようです。

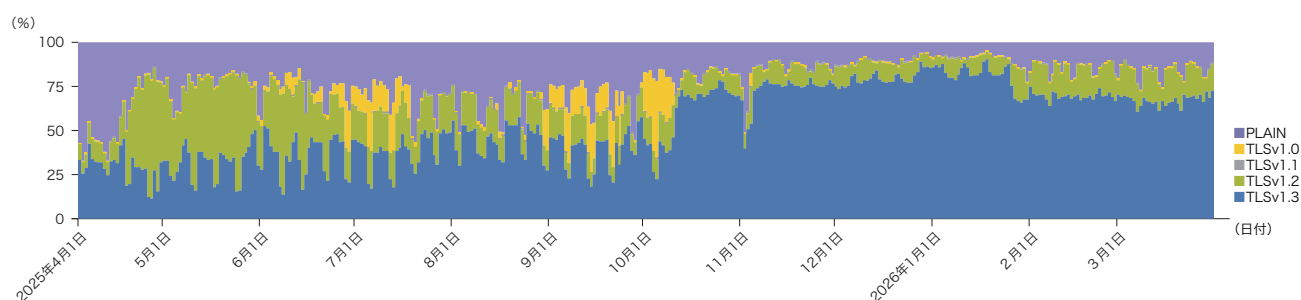


図-8 受信メールにおける経路暗号化の割合

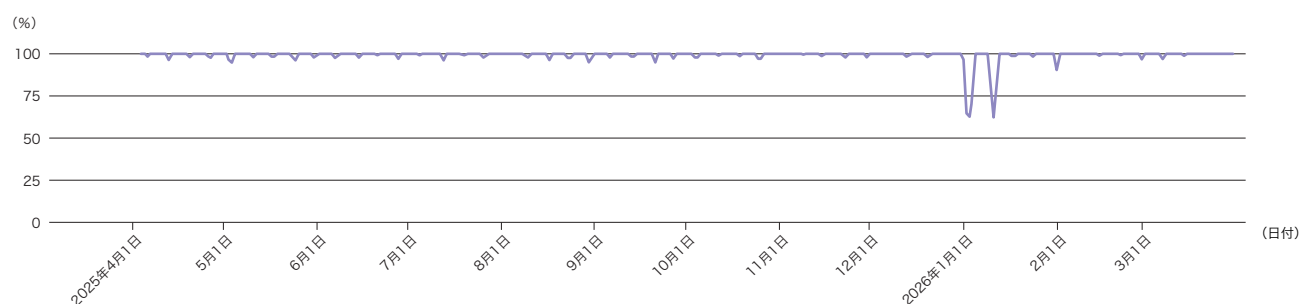


図-9 送信メールにおける経路暗号化の割合



執筆者：
古賀 勇 (こが いさむ)

IJ ネットワーク本部 アプリケーションサービス2部 運用技術課 課長、(兼)証明書技術課 課長
2007年IJ入社。メールサービス、PKI関連サービスの業務に従事。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・講演。M3AAWG、WIDE Project、openSUSEなどで幅広く活動中。

国内プロバイダ初、WebメールのBIMI表示対応 ～IIJmioセーフティメールの安全対策～

3.1 IIJmioセーフティメールにおける BIMIアイコン表示対応

2025年12月、IIJmioセーフティメールで提供中であるWebメール、「Mailviewer」において、BIMIを用いたブランドアイコンの表示機能が追加されました。

BIMIを利用したアイコンの表示機能に対応しているWebメールは、Google社のGmailが世間によく知られています。IIJで観測した限り、日本国内の各インターネットサービスプロバイダが提供するWebメールが後述するVMC及びCMCを区別してBIMI表示に対応したのはMailviewerが日本国内初です。

本稿では、BIMIの現在の仕様についての解説と、MailviewerでのBIMI表示について紹介をします。

3.2 IIJmioセーフティメールについて

IIJmioセーフティメールは、IIJが個人のお客様に提供しているメールサービスです。IIJでは、IIJmioブランドの前身である、IIJ4Uブランドを提供していた頃より個人のお客様向けにもメールサービスを提供しています。

サービス名が示すとおり、安全性を重視した設計になっており、ウイルススキャンやスパム検知機能、SPF・DKIM・DMARCといった送信ドメイン認証を利用したなりすましメール対策フィルタを、従来から提供しています。そんなIIJmioセーフティメールで提供しているWebメール「Mailviewer」は2000年代に提供を開始した、IIJ謹製のWebメールシステムです。当

時はメールを読む、書くという最低限の機能しか備えておらず、名前の由来もそのあたりから来ています。2021年12月にリニューアルをして、現在多くの機能を備えたWebメールとしてMailviewerの名をそのまま受け継ぎ、サービス提供を続けています。

今回のブランドアイコン表示機能は、そんなMailviewerに新たに加わったBIMIという仕組みを使った機能です。

3.3 BIMIについて

BIMIとは、Brand Indicators for Message Identificationの略です。WebメールやMUA (Mail User Agent) でブランドアイコンを表示するための規格であり、IETFでInternet Draftとして2019年2月から公開されています。

BIMIはBIMI groupにて様々な議論がされていますが、RFCとして採番をされているわけではありません。SPF、DKIM、DMARCからなる送信ドメイン認証技術を応用して、ブランドアイコンの表示／非表示をするための仕組みですが、一般のメールユーザがメールを実際に参照するアプリケーションは様々であり、提供している企業によって実装が多様であるため、明確に規格があるわけではなく、あくまでもロゴマーク表示のための指針として議論がされているようです。

BIMIには、表示するブランドアイコンファイル用の電子証明書が存在し、VMC (Verified Mark Certificate) とCMC (Common Mark Certificate) の2種類があります。



図-1 IIJmioセーフティメール概要ページ

- ・ VMC(Verified Mark Certificate) : 商標登録されたアイコン用の証明書
- ・ CMC(Common Mark Certificate) : 組織による利用実績が認められたアイコン用の証明書

それぞれの違いは表-1のとおりです。

CMCについては、シーズンごとにアイコンの一部を装飾したり、VMCを取得するまでの間利用する、といった用途での利用が想定されているようです。VMCは商標登録したアイコンにしか使えないため、企業が提供するサービスによってはCMCを用いてシーズンごとに切り替えたりすることができれば、ユーザ目線でも分かりやすいかもしれません。

図-2 IIJmio Mailviewerログイン画面

正式名称	Verified Mark Certificate	Common Mark Certificate
商標登録	必須	不要
ロゴ所有確認	商標で確認	組織による利用実績 (12か月継続利用)などで確認
取得難易度	高い	低い
コスト	高め	安め
発行期間	長め	短め

表-1 ブランドアイコンファイル用の電子証明書

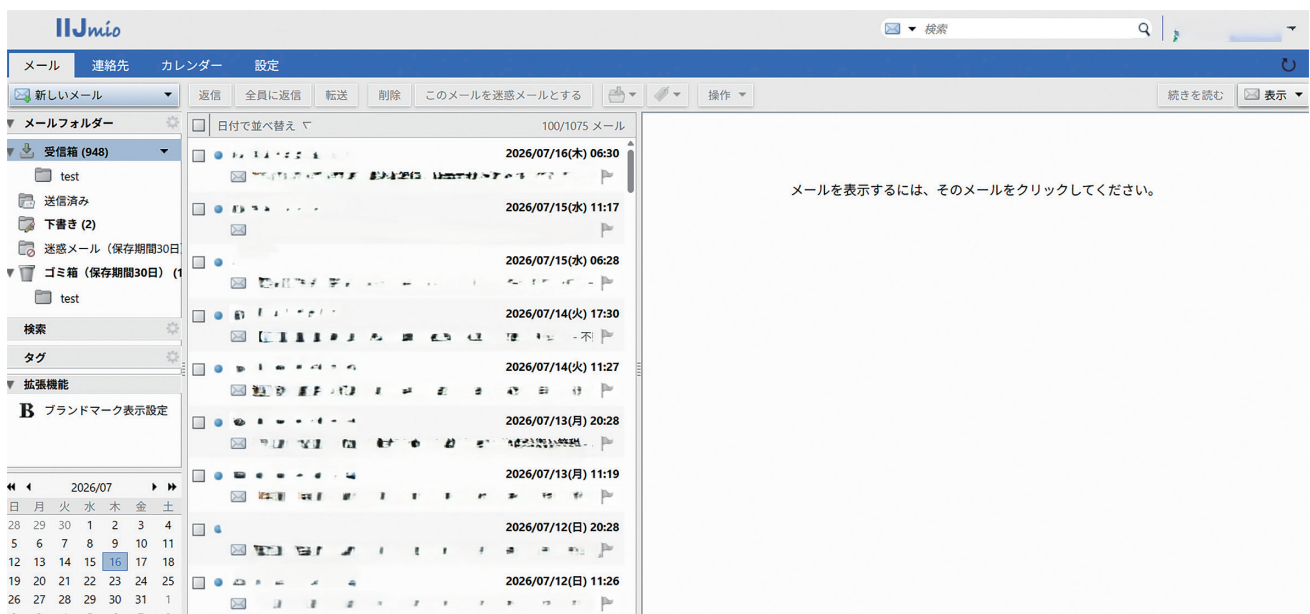


図-3 Mailviewer Webメール画面(メール一覧加工処理済み)

例えばIJmioの場合、青を基調としたデザインとピンクを基調にしたデザインがあるため、CMCを利用することでユーザの皆様へ送るメールの種類によってアイコン画面の出し分けが可能です。

VMCを用いた場合は、すべてのアイコンについてそれぞれ個別に商標登録をしなければならないため、アイコンの種類が膨大にあるブランドであったりすると、CMCの方が使い勝手は良いかもしれません。

また、時期によってアイコンを少し変えたい、というようなメール送信側の需要に応える側面もあるため、ブランド広告メールへのシーズンアイコンなどに利用することもCMCを利用することで実現できます。

これらの証明書は、BIMI GroupによるとDigiCert、GlobalSign、SSL.comが対応した証明書を発行しているとのこと^{*1}。VMC、CMCは表示するアイコン画像ファイルに対する電子署名であり、受信システムの評価の方法に依存しますが、MVA (Mark Verifying Authority) として広く知られている認証局から発行されたものでないと効果を発揮しない場合が多いです。また、これらの証明書は必須ではありません。証明書を検証するかどうかは、受信したメールを表示する各WebメールやMUAの実装に委ねられています。

前述したように、BIMIは送信ドメイン認証技術の元に成り立っており、ブランドアイコンを表示するための前提として、そのメールの送信元ドメイン(RFC5322.From)と、その親ドメインのDMARCポリシーがquarantineまたはrejectでないと表示ができません。

DMARCポリシーについては以前、IIR Vol.55でIJで利用しているij.ad.jpのポリシーをp=rejectにしたことをIIRに書いていますので、参考にしてください^{*2}。

3.3.1 BIMIの送信者対応について

まずはBIMIの仕組みについて送信側の視点と、受信側の視点で解説をしていきたいと思います。

まず、メールの送信者はRFC5322.Fromに対して下記の対応をします。

- (1) FromドメインのDMARCポリシーの宣言(p=quarantineまたはp=reject)とDMARC検証をpassさせるための各種ITリソースの整理
- (2) Fromドメインに対するロゴファイル(svgファイル)の準備
- (3) ロゴファイル公開に対応した証明書の準備
- (4) ロゴファイルと証明書のWebサーバでの公開
- (5) BIMIレコードの公開



図-4 IJmioアイコン

*1 BIMI, 「Mark Certificate Issuer Information」(<https://bimigroup.org/vmc-issuers/>)。

*2 Internet Infrastructure Review (IIR) Vol.55 (<https://www.ij.ad.jp/dev/report/iir/055/01.html>)。

■ (1) FromドメインのDMARCポリシーの宣言(p=quarantineまたはp=reject)とDMARC検証をpassさせるための各種ITリソースの整理

DMARCを導入する際に多くの方が検討することだと思いますので、ここでの説明は省きます。が、DMARCは導入して終わり、ではなく継続的な観測と確認、是正が必要です。

BIMIを用いたアイコンの表示をするためにはそのドメインのサブドメインのポリシー(spタグ)もsp=noneを宣言してはいけません。

■ (2) Fromドメインに対するロゴファイル(svgファイル)の準備

2つ目は、実際にメールを受信したシステムで表示するロゴファイルの用意についてです。

実際に表示するロゴについては、決められた規定を満たしたものでないといけません。BIMIのインターネットドラフトが公開された当初から言われているのが、"商標登録されているロゴマーク"です。また、2024年後半頃から、少し緩和がされていて、"12ヵ月間継続的な利用が第三者機関で認められたロゴマーク"についても使用できるロゴマークとして認められるようになりました。

これらの画像ファイルは、svgというファイル形式かつ、SVG Tiny 1.2をベースとしたSVG P/S (Portable/Secure)という形式のファイルであることが決められています。筆者も画像ファイルの形式についてはあまり明るくはありませんが、いくつか調べたところ下記のような経緯があるとのことでした。

- ・ SVG Tiny 1.2はモバイル端末や組み込み機器などの、大きなファイルのやり取りが難しい端末向けの軽量版SVGファイル規格であり、一部アニメーションやJavaScriptの埋め込み、外部参照が可能

- ・ SVG P/Sはより機能を制限したプロファイルであり、Tiny 1.2でも可能であったアニメーションやJavaScript、外部参照などの機能も制限されている

BIMIにおいては、公開されたSVGファイルを様々な端末のMUAで表示することを目的としているため、不必要な要素をそぎ落としてファイルサイズも小さくすることができるSVG P/Sが採用されているようです。

■ (3) ログファイル公開に対応した証明書の準備

前述したとおり、ロゴの種類により取得する証明書の種類が異なります。用意したロゴファイルの種類によって、VMCもしくはCMCどちらかを取得します。また、前述したとおりこの証明書はBIMIにおいて必須のものではありません。しかし、証明書の検証をするかしないかは受信システムの実装に依存しており、現状BIMI表示に対応しているいくつかのWebメールやMUAはこの証明書の検証を必須としているものもあるため、準備するに越したことはなさそうです。

■ (4) ログファイルと証明書のWebサーバでの公開

4つ目については、これらのSVGファイルならびに証明書をWebサーバで公開するのみで、特に制約などはありません。

■ (5) BIMIレコードの公開

5つ目については、下記のフォーマットでBIMIレコードを公開します。

```
default._bimi.example.jp 3600 IN TXT "v=BIMI1; l=https://example.jp/bimi/logo.svg; a=https://example.jp/bimi/certificate.pem; lps=noreply, support"
```

それぞれのタグについては表-2のとおりです。

タグ	例	備考
v	BIMI1	BIMIバージョンの指定、現在は BIMI1 のみ
l	https://example.jp/bimi/logo.svg	SVG Tiny P/Sロゴの公開URL (HTTPS指定)
a	https://example.jp/bimi/certificate.pem	VMC/CMC 証明書 (PEM形式) の公開URL (HTTPS指定)
lps	noreply, support	Local Part Selector RFC5322.Fromのローカルパートに記載の文字列を指定することで受信側システムで参照するローカルパートとセレクトタの宣言が可能

表-2 タグ

左辺の"default"の部分はDKIMと同様のセレクトアとなっており、セレクトアとIpsタグを組み合わせて利用することで表示アイコンの出し分けが可能です。

3.3.2 BIMIの受信者対応について

では、次に受信側がどのような対応をするのかを見ていきます。

受信システムでは、受信したメールについて下記の対応が必要です。

- (1) 各種送信ドメイン認証 (SPF、DKIM、DMARC) の検証
- (2) BIMIの評価
- (3) BIMI評価結果をヘッダに付与
- (4) BIMI評価結果に応じてSVGファイルを取得してMUAで表示できるようにする

■ (1)各種送信ドメイン認証 (SPF、DKIM、DMARC) の検証

送信ドメイン認証の検証は、既に多くのメールシステムが対応をしているかと思いますが今回は説明は省略します。

■ (2)BIMIの評価

続いて、BIMIの評価を実施します。前述した検証のうち、DMARCの検証結果がpassしたメールについて、RFC5322.FromドメインのDMARCポリシーを確認して、p=quarantineもしくはp=rejectが宣言されているメールがBIMI評価の対象となります。DMARCがpassしていなかった場合、転送などを考慮してARCの検証結果を元にBIMIを利用するか否かを選択が可能です。

どのメールをBIMI評価の対象とするかはそのシステムの設計によると思いますが、アイコンを表示できるメールはDMARCがpassしたメールに限られますので、すべてのメールについて検証する必要はないかもしれません。

実際のBIMI評価の際には、前述したBIMIレコードの探索から始めます。もし評価対象のメールのヘッダにBIMI-Selectorヘッダがあれば、そのセレクトアを利用して宣言されたBIMIレコードの評価を実施します。また、BIMIレコードを参照した際のIpsタグにRFC5322.Fromのローカルパートが存在すれば、その文字列をセレクトアとして利用します。もしそのどちらでもなければ、defaultをセレクトアとして評価をします。

BIMIレコードに記載のあるSVGファイルならびにVMC/CMC証明書の確認をして、それらのファイルの検証をします。検証の結果、BIMIがpassするについにMUAやWebメールでのロゴ表示が可能なメールと判断されます。また、BIMIの評価結果によってどのようなメールに対してブランドロゴを表示するか、については明確な決まりはなく、メールを受信したシステムの実装によります。

■ (3)BIMI評価結果をヘッダに付与

BIMIの評価結果は下記のようなヘッダを用いることが一般的です。

■ Authentication-Resultsヘッダ

Authentication-ResultsヘッダにBIMIの評価結果を付与します。受信システムによっては、bimi.selectorにBIMIセレクトア、bimi.authorityにvmc/cmcを付与することもあるようです。

```
Authentication-Results: mx.example.com spf=pass smtp.mailfrom=example.com dkim=pass
header.i@example.com dmarc=pass header.from=example.com header.d=example.com
header.selector=default bimi=pass
```

■ BIMI-Locationヘッダ

BIMIの評価がpassになった際、受信サーバがメーラ (MUA) に対して、具体的にどのロゴアイコン (SVG) と証明書 (PEM) を表示に使うべきかを指定するためのヘッダです。

```
BIMI-Location: v=BIMI1; l=https://example.com; a=https://example.com;
```

各タグの値には表-3の要素が挿入されます。

■ BIMI-Indicatorヘッダ

BIMI-Indicator: PD94bWgdmVyc2lvdj0iMS4wIiB1bmNvZG... (以下、Base64 文字列が続く)

受信サーバはBIMI検証が成功すると、BIMIレコードに記載のあるIタグに記載のURLから取得したブランドロゴのSVGファイルをBase64エンコードした値をBIMI-Indicatorヘッダに挿入します。これは、メールをMUAで表示する際の通信によるプライバシーへの懸念や、表示の遅延などに考慮し、サーバ側で事前に取得したデータをヘッダに挿入すること

でメーラはメール表示時に外部と通信することなく、安全に高速にロゴ描写をすることができます。

■ (4)BIMI評価結果に応じてSVGファイルを取得してMUAで表示できるようにする

こちらについては、MUAでは3にて紹介したBIMI-Indicatorのヘッダの値を参照することで、実際に表示するアイコンを取得します(図-5)。

また、2026年7月現在DKIM2^{*3}などメールにおける送信ドメイン認証技術に関する新しい規格についての議論もあり、BIMIについても現在の仕組みから大きな変更がある可能性があります。

タグ	概要
v (Version)	BIMIバージョン、現在はBIMI1のみを指定
l (Location)	検証済みのブランドロゴ (SVG) のURL
a (Authority)	検証済みの証明書 (VMCやCMC) のURL

表-3 タグ

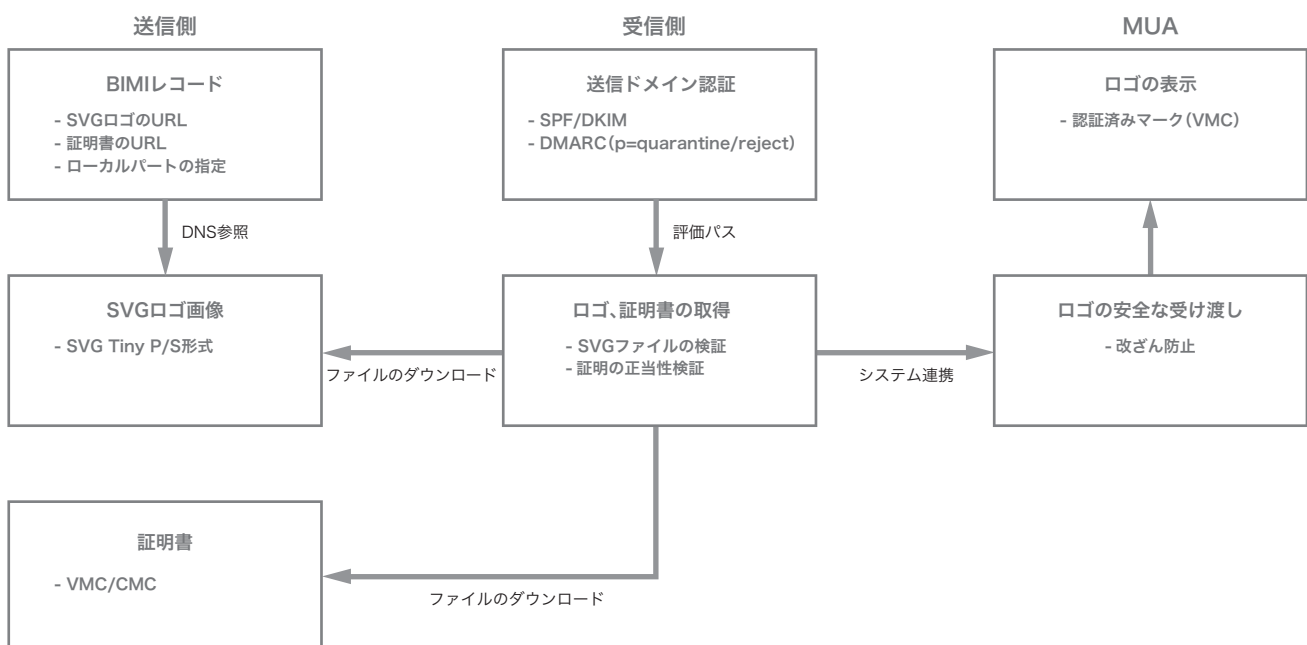


図-5 アイコン取得のフロー

*3 IETF, "DomainKeys Identified Mail Signatures v2 (DKIM2)draft-ietf-dkim-dkim2-spec-04" (<https://datatracker.ietf.org/doc/draft-ietf-dkim-dkim2-spec/>)。

3.4 IJmioセーフティメールでのブランドアイコン表示について

さて、BIMIについて話してきましたが、IJmioセーフティメールでは2025年12月にMailviewerにてブランドアイコン表示機能を実装しました^{*4}。

IJmioではお客様に提供する各メールサービスにて、SPF、DKIM、DMARCといった送信ドメイン認証技術にいち早く対応してきました。今回のブランドアイコン表示機能についても、IJmioセーフティメールの利用者向けになりすましメール被害を少しでも防ぐための機能として実装をしています。

図-6はCMCを用いた際の表示例です。MailviewerではVMCに対応したブランドロゴの場合、差出人の右に緑のチェックマークが表示されます。

ブランドアイコン表示はいわば、自宅の表札を出すようなものです。表札(ロゴファイル)と、その表札が本物であることを証明する身分証明書(VMC/CMC)を、誰でも確認できる場所に

掲げておく。メールを受け取った側のシステムは、メールが届くたびにこの「表札」を確認しに行き、本物であることが確認できれば、初めてロゴを表示する、という流れになっています。この確認作業はすべて自動で行われるため、利用者が意識することはありません。

これまでMailviewerでは、送信者の情報はメールアドレスや表示名でしか判断できませんでした。本機能により、DMARCを厳格に運用しBIMIレコードと証明書を正しく公開している送信元からのメールであれば、企業のロゴが一覧画面に表示されるようになります。

利用者にとっては、見慣れたロゴが表示されているかどうか、「本当にその企業から届いたメールか」を直感的に見分ける手がかりの1つになります。もちろんBIMI表示だけで100%の安全を保証するものではありませんが、なりすましメールとの違いに気づくきっかけを増やすという点で、実用的な効果が期待できます。

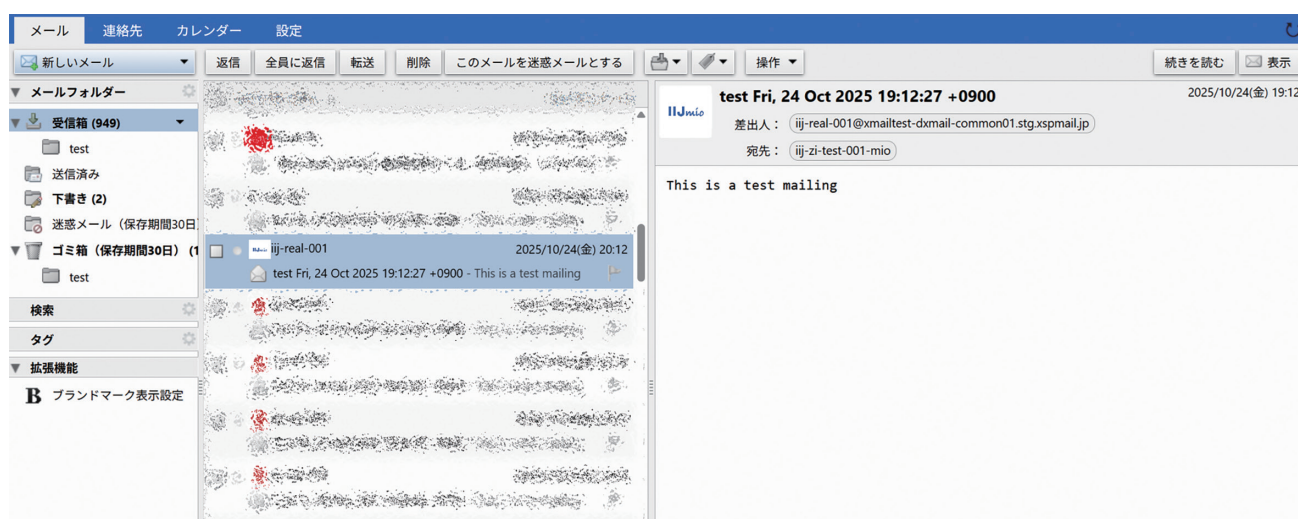


図-6 ブランドロゴ表示の様子(一部画像加工済み)

*4 IJmio、「なりすまし対策強化のためのブランドロゴ表示機能(BIMI)導入について」(<https://www.ijmio.jp/info/ijj/1765171401.html>)。

BIMIという仕組み自体には、迷惑メールやフィッシングメールを防ぐ根本的な効果はありません。あくまでブランドアイコンを表示することでメールを参照するユーザに対してそのメールが正規の送信元から送信されているメールかどうかの判断を補助する役割を果たします。ただ、ブランドアイコンを表示するためにはDMARC認証をパスする必要があるため結果的に一定のセキュリティが担保されているような形になります。

BIMIは長年、internet draftという形でIETFで各文書が公開されています。メールに限らず、これらは時間を経てRFCに採番されることが多いですが、BIMIについてはメールを表示するアプリケーションの数も多く実装も様々であるため現在はずぐに明確な国際規格として制定せずに、メール関連技術における1つの指針として多くの関係者の間でinternet draftとして継続的に議論がされています。

昨今、迷惑メールやフィッシングメールの被害が急増していることもあり、多くの企業が送信ドメイン認証やBIMIへの対応を進めています。送信ドメイン認証技術を土台としたこの仕組みは、フィッシング対策とブランド保護の両面から、今後更に多くのメールサービスへ広がっていくことが見込まれます。特に、商標登録を必要としないCMCの普及が進めば、これまでコストの面でBIMI導入をためらっていた企業にとっても対応への敷居が下がり、結果として「ロゴが表示されていないメールの方が珍しい」という世の中になっていく可能性もあります。

IJは今回、国内のプロバイダに先駆けてMailviewerへのBIMI表示機能を実装しました。今後もお客様がより安心してメールをご利用いただけるよう、なりすましメール対策フィルタやウイルスプロテクションといった既存のメールフィルタリング機能と併せて、セキュリティ関連機能の充実に取り組んでまいります。



執筆者：
今村 侑輔（いまむら ゆうすけ）

IJ ネットワークサービス事業本部 ネットワーク本部 アプリケーションサービス1部 xSPサービス課 課長代行。
2015年IJ入社。メールサービスの運用業務に従事。IJ Europeでの就業経験を活かし、日々グローバルに活躍中。



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2026年9月時点のものです。

©Internet Initiative Japan Inc. All rights reserved.
IIJ-MKTG019-0071

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>