IIR

Internet
Infrastructure
Review

Sep.2019
Vol.44

定期観測レポート

ブロードバンドトラフィックレポート
–トラフィック量は緩やかな伸びが継続–

フォーカス・リサーチ

IIJ Public DNSサービスについて

IIJ
Internet Initiative Japan

Internet Infrastructure Review

September 2019 Vol.44

エグゼクティブサマリ

8月23日の午後、Amazon Web Services（AWS）の東京リージョンにおいて、6時間ほどサービスが停止するという事故がありました。世界有数のクラウド事業者のサービスが停止したことで、非常に多くの企業のシステムやサービスが影響を受け、一般の利用者がそれらの企業のサービスを受けられない状態になりました。インターネットは究極の分散ネットワークである一方、クラウドの普及によってデータ処理の集中が加速しています。AWSという単一企業の事故により、あれだけ広範な影響が出たことで、インターネットにおける集中をあらためて認識させられた次第です。また、29日にはいくつかのISPにおいて、MicrosoftのWindows Updateによる急激なトラフィックの増加が原因と見られるインターネットの通信障害が報告されました。本件も単一企業に関する活動が、インターネットというインフラに大きな影響を与えたことにおいて、印象的な事件でした。

「IIR」は、IIJで研究・開発している幅広い技術の紹介を目指しており、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、特定のテーマを掘り下げた「フォーカス・リサーチ」から構成されています。

1章の「定期観測レポート」は、恒例のブロードバンドトラフィックレポートです。本レポートは2009年の「IIR」第4号から毎年掲載しているもので、インターネットのトラフィック動向を10年以上遡って見ることができる貴重なデータであると自負しています。本年も固定ブロードバンドサービス、モバイルサービス共に昨年と同等の増加が観測されたものの、ここ数年、利用者ごとの利用量は大きく変化していないという結果になっています。

2章の「フォーカス・リサーチ」では、インターネットを支える重要な基盤の1つであるDNSを取り上げました。IIJは今年5月からDNS over TLS（DoT）、DNS over HTTPS（DoH）による名前解決を行う「IIJ Public DNSサービス」を、IIJユーザだけでなく、どなたにでも使っていただけるサービスとして提供しています。本稿では、DoT/DoHの技術的内容やDNSSECとの違いを説明したうえで、「IIJ Public DNSサービス」の実装や実装上の工夫について解説しています。

IIJはこのような活動を通じて、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続けています。今後も企業活動のインフラとして最大限に活用していただけるよう、様々なサービス、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 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。

ブロードバンドトラフィックレポート –トラフィック量は緩やかな伸びが継続–

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][*6][*7][*8][*9][*10]。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。

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、それぞれのOUTの最新値を1として正規化しています。

ブロードバンドに関しては、前回からIPv6 IPoEのトラフィック量も含めて示しています。IPv6 IPoEを含まない分は、"broadband-IPoE"として細線で示します。IIJのブロードバンドにおけるIPv6は、IPoE方式とPPPoE方式がありますが[*11]、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直接IIJの網を通らないため、以降の解析の対象にはなっていません。2019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19%、OUTで14%と、昨年同月よりそれぞれ7ポイントと6ポイント増えていて、IPoE利用が拡大しています。

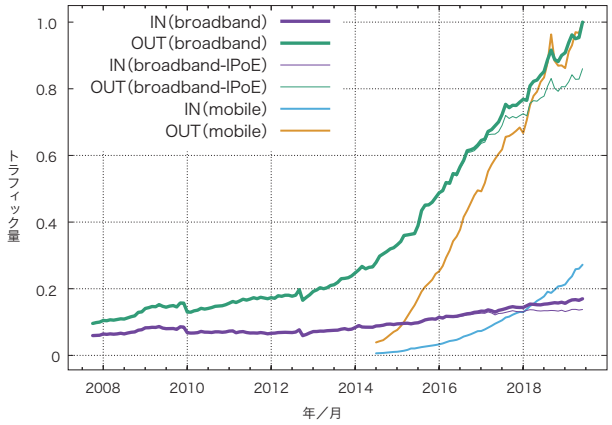

図-1 ブロードバンド及びモバイルの月間トラフィック量の推移

ブロードバンドトラフィック量は、INは12%の増加、OUTは19%の増加となっています。1年前はそれぞれ12%と20%の増加でしたので、増加率はほぼ同じです。モバイルは、この1年で、INは60%、OUTは22%の増加と、1年前の69%と36%に比べると伸びが鈍化しています。また、総量ではまだブロードバンドより1桁少ない状況です。

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、SampledNetFlow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、使用量についてはアクセスゲートウェイの課

*1 長健二朗. ブロードバンドトラフィックレポート: ダウンロードの増加率は2年連続で減少. Internet Infrastructure Review. Vol.40. pp4-9. August 2018.
*2 長健二朗. ブロードバンドトラフィックレポート: トラフィック増加はややペースダウン. Internet Infrastructure Review. Vol.36. pp4-9. August 2017.
*3 長健二朗. ブロードバンドトラフィックレポート: 加速するトラフィック増加. Internet Infrastructure Review. Vol.32. pp28-33. August 2016.
*4 長健二朗. ブロードバンドトラフィックレポート: ブロードバンドとモバイルのトラフィックを比較. Internet Infrastructure Review. Vol.28. pp28-33. August 2015.
*5 長健二朗. ブロードバンドトラフィックレポート: この1年でトラフィック量は着実に増加、HTTPSの利用が拡大. Internet Infrastructure Review. Vol.24. pp28-33. August 2014.
*6 長健二朗. ブロードバンドトラフィックレポート: 違法ダウンロード刑事罰化の影響は限定的. Internet Infrastructure Review. Vol.20. pp32-37. August 2013.
*7 長健二朗. ブロードバンドトラフィックレポート: この1年間のトラフィック傾向について. Internet Infrastructure Review. Vol.16. pp33-37. August 2012.
*8 長健二朗. ブロードバンドトラフィックレポート: マクロレベルな視点で見た、震災によるトラフィックへの影響. Internet Infrastructure Review. Vol.12. pp25-30. August 2011.
*9 長健二朗. ブロードバンドトラフィックレポート: P2Pファイル共有からWebサービスへシフト傾向にあるトラフィック. Internet Infrastructure Review. Vol.8. pp25-30. August 2010.
*10 長健二朗. ブロードバンドトラフィック: 増大する一般ユーザのトラフィック. Internet Infrastructure Review. Vol.4. pp18-23. August 2009.
*11 小川晃通. プロフェッショナルIPv6. 付録A.3. IPv6 PPPoEとIPv6 IPoE. ラムダノート. July 2018.

金用情報を、使用ポートについてはサービス収容ルータでのSampledNetFlow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ています。今回は、2019年５月27日から6月2日の1週間分のデータを使っていて、前回解析した2018年5月28日から6月3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。また、NetFlowではパケットをサンプリングして統計情報を取得しています。サンプリングレートは、ルータの性能や負荷を考慮して、1/8192 ～1/16382に設定されています。観測された使用量に、サンプリングレートの逆数を掛けることで全体の使用量を推定しています。

IIJの提供するブロードバンドサービスにはファイバー接続とDSL接続がありますが、今ではファイバー接続の利用がほとんどとなっています。2019年には観測されたユーザ数の98%はファイバー利用者で、ブロードバンドトラフィック量全体の99%以上を占めています。

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日の利用量とは各利用者の1週間分のデータの1日平均です。

今回から、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。法人利用者は利用形態が様々で、かつ、一部の法人の利用傾向に影響を受けやすく、そのため全体の分布に歪みが目立つようになってきました。それに対して、個人利用者のみの分布は滑らかな形状で安定しています。そのため、利用傾向を掴むには個人利用分だけを対象にした方が、より一般性がありかつ分かりやすいと判断しました。また、過去の数字も個人利用者だけを対象にしたものに置き換えています。なお、次章のポート別使用量の解析は区別が難しいため法人も含めたデータを使っています。

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軸に示しており、2018年と2019年を比較しています。X軸はログスケールで、10KB（10^4）から100GB（10^{11}）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、概ね100GB（10^{11}）までの範囲に分布しています。

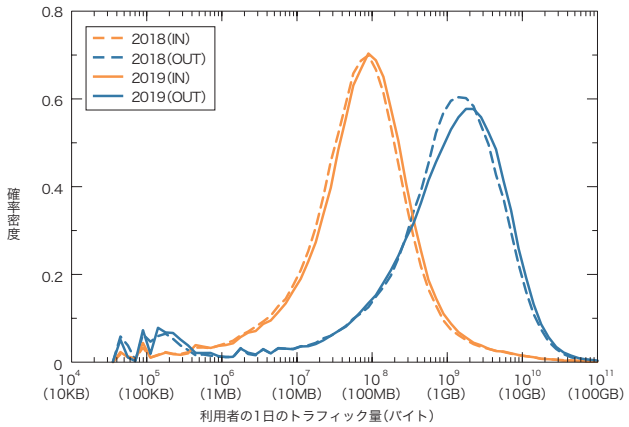

図-2 ブロードバンド利用者の1日のトラフィック量分布
2018年と2019年の比較

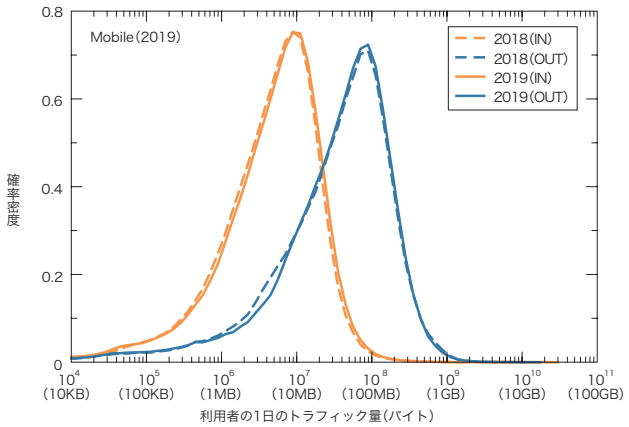

図-3 モバイル利用者の1日のトラフィック量分布
2018年と2019年の比較

ブロードバンドの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り右へなだらかに減少する、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。2018年と2019年で比較すると、INとOUT共に分布の山がわずかながら右に少し移動しており、利用者全体のトラフィック量が増えていることが分かります。しかし、数年前に比べると分布の移動量は小さくなってきています。

右側のOUTの分布を見ると、分布のピークはここ数年間で着実に右に移動していますが、右端のヘビーユーザの使用量はあまり増えておらず、分布の対称性が崩れてきています。一方で、左側のINの分布は左右対称で、より対数正規分布に近い形です。

図-3のモバイルの場合、ブロードバンドに比べて利用量は大幅に少ないことが分かります。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、左右非対称な形になります。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。そのため、1週間分のデータから1日平均を求めると、1日単位で見た場合より利用者間のばらつきは小さくなります。1日単位で同様の分布を描くと、分布の山が少し低くなり、その分両側の裾が持ち上がりますが、基本的な分布の形や最頻出値はほとんど変わりません。モバイルの分布も昨年からの違いはわずかです。

	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
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

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

	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

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

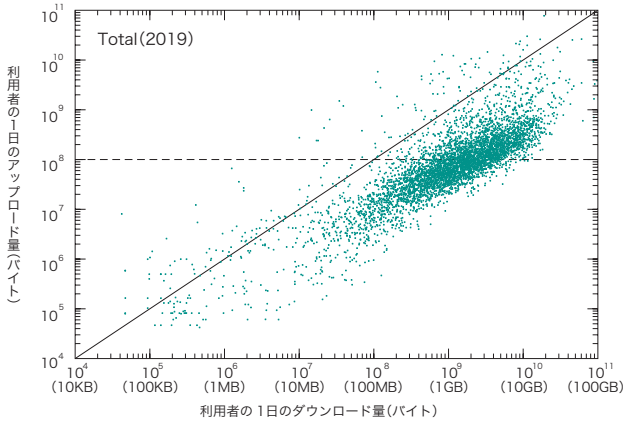

図-4 ブロードバンド利用者ごとのIN/OUT使用量

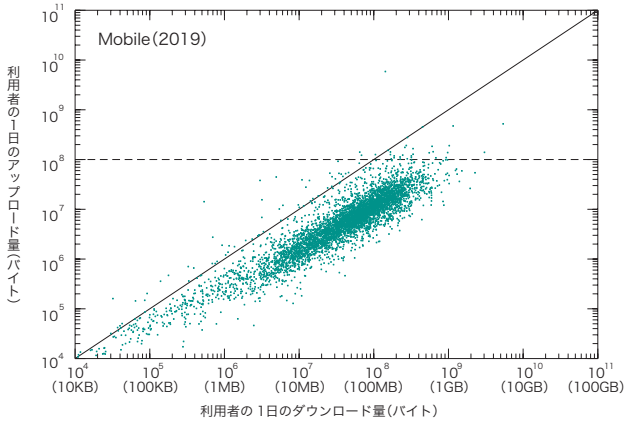

図-5 モバイル利用者ごとのIN/OUT使用量

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2018年と2019年で比較すると、INでは79MBから89MBに、OUTでは1585MBから1995MBに増えており、伸び率で見ると、INとOUT共に1.3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、2019年には、INの平均は479MB、OUTの平均は2986MBと、最頻出値よりかなり大きな値になります。2018年には、それぞれ428MBと2664MBでした。

モバイルでは、表-2に示すように、ヘビーユーザが少ないため、平均と最頻出値が近い値になります。2019年の最頻出値は、INで9MB、OUTで79MBで、平均値は、INで11MB、OUTで85MBです。最頻出値は、INもOUTも昨年と同じ値となっています。最頻出値は変わっていませんが、平均値と中間値は増加しており、図-2の分布の山の左側が示すライトユーザの割合が少し減った影響だと考えられます。

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。

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。ブロードバンドでは、以前は右上の対角線上あたりを中心に薄く広がるヘビーユーザのクラスタがはっきり分かりましたが、今では識別ができなくなっています。また、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。これらについても、2018年との違いはほとんど分かりません。

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少なく、IN/OUTのばらつきも小さくなっています。

図-6及び図-7は、利用者の1日のトラフィック量を相補累積度分布にしたものです。これは、使用量がX軸の値より多い利用者の、全体に対する割合をY軸に、ログ・ログスケールで示したもので、ヘビーユーザの分布を見るのに有効です。グラフの右側が直線的に下がっていて、ベキ分布に近いロングテールな分布であることが分かります。ヘビーユーザは統計的に分布しており、決して一部の特殊な利用者ではないといえます。

モバイルでも、OUT側ではヘビーユーザはベキ分布していますが、IN側では直線的な傾きが崩れていて、大量にアップロードするユーザの割合が大きくなっています。

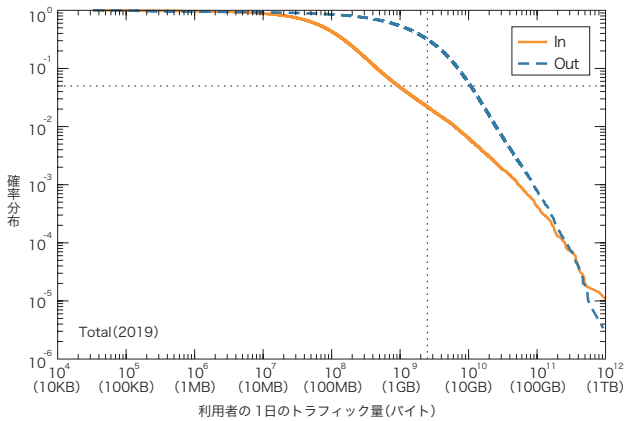

図-6 ブロードバンド利用者の1日のトラフィック量の相補累積度分布

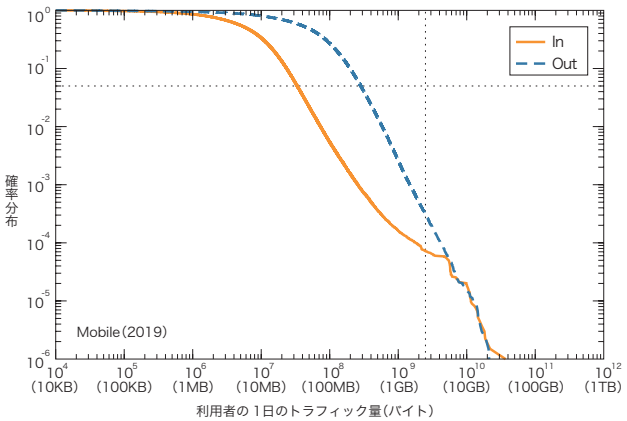

図-7 モバイル利用者の1日のトラフィック量の相補累積度分布

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52%、INの82%を占めています。更に、上位1%の利用者がOUTの17%、INの58%を占めています。ここ数年のヘビーユーザ割合の減少に伴い、わずかながら偏りは減ってきています。モバイルでは、上位10%の利用者がOUTの43%、INの47%を、上位1%の利用者がOUTの12%、INの18%を占めています。対象を個人利用者のみにしたことで、昨年までのレポートより偏りが少なくなっています。

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いえます。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の過去5年間の推移を示します。2019年の全体トラフィックの81%はTCPです。前回少し減少したHTTPSのTCP443番ポートの割合は、41%から52%に大きく増えています。HTTPのTCP80番ポートの割合は27%から20%に減っており、前回まで増えていたGoogleのQUICプロトコルで使われるUDP443番ポートも、10%から8%に減っています。このことから、HTTPからHTTPSへの移行が継続している一方で、QUICの拡大傾向には少しブレーキが掛かったと言えます。

減少傾向のTCPの動的ポートは、2019年には8%にまで減りました。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8080番でも0.5%となっています。また、Flash Playerが利用する1935番は減少傾向で、約0.3%に減りました。これら以外のトラフィックは、ほとんどがVPN関連です。

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おり、モバイル利用者もブロードバンドと同様のアプリケーションの使い方をしていることがうかがえます。

year	2015	2016	2017	2018	2019
protocol port	(%)	(%)	(%)	(%)	(%)
TCP	**80.8**	**82.8**	**83.9**	**78.5**	**81.2**
(< 1024)	63.3	69.1	72.9	68.5	73.3
443(https)	23.3	30.5	43.3	40.7	51.9
80(http)	37.9	37.1	28.4	26.5	20.4
993(imaps)	0.1	0.1	0.2	0.2	0.3
22(ssh)	0.2	0.2	0.1	0.1	0.2
182	0.4	0.3	0.3	0.3	0.2
(>= 1024)	17.5	13.7	11.0	10.0	7.89
8080	0.3	0.2	0.3	0.3	0.5
1935(rtmp)	1.8	1.5	1.1	0.7	0.3
UDP	**11.4**	**11.1**	**10.5**	**16.4**	**14.1**
443(https)	0.9	2.4	3.8	10.0	7.8
4500(nat-t)	0.2	0.2	0.2	0.2	0.3
ESP	**7.4**	**5.8**	**5.1**	**4.8**	**4.4**
IP-ENCAP	**0.2**	**0.2**	**0.3**	**0.2**	**0.2**
GRE	**0.2**	**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	2015	2016	2017	2018	2019
protocol port	(%)	(%)	(%)	(%)	(%)
TCP	**93.8**	**94.4**	**84.4**	**76.6**	**76.9**
443(https)	37.4	43.7	53.0	52.8	55.6
80(http)	52.5	46.8	27.0	16.7	10.3
31000	0.0	0.2	1.8	2.9	6.4
993(imaps)	0.5	0.5	0.4	0.3	0.3
1935(rtmp)	0.5	0.3	0.2	0.1	0.1
UDP	**5.2**	**5.0**	**11.4**	**19.4**	**17.3**
443(https)	1.0	1.5	7.5	10.6	8.3
12222	0.0	0.1	0.1	2.3	3.4
4500(nat-t)	0.3	0.2	0.2	4.5	3.0
53(dns)	0.1	0.2	0.1	0.1	0.1
ESP	**0.7**	**0.4**	**0.4**	**3.9**	**5.8**
GRE	**0.3**	**0.1**	**0.1**	**0.1**	**0.0**
ICMP	**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量

図-8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、2018年と2019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。2018年と比較すると、TCP443番ポートの割合が更に増えて、TCP80番ポートが減っているのが分かります。全体のピークは19:00から23:00頃です。土日には昼間のトラフィックが増加しており、家庭での利用時間を反映しています。

図-9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。モバイルでも、TCP443番ポートの割合が増えた分、TCP80番ポートが減っています。ブロードバンドに比べると、朝から夜中までトラフィックの高い状態が続きます。平日には、朝の通勤時間、昼休み、夕方17:00頃から22:00頃にかけての3つのピークがあり、ブロードバンドとは利用時間の違いがあることが分かります。

1.5 まとめ

ここ数年のトラフィック量は緩やかな伸びが続いています。緩やかといっても、それ以前に比べて緩やかなだけで、年率で20%なので4年で2倍以上になるペースで増えています。トラフィック量は、ブロードバンドもモバイルも増減を繰り返しながら増えてきています。両方同じ時期にトラフィックが増えたり減ったりしているので、共通の要因があると推測できますが、具体的な要因までは特定できていません。

利用者ごとの利用量を見ると、ブロードバンド、モバイル共に、ここ数年あまり変化がないことが分かります。この間、トラフィックを押し上げるような新しいサービスが出てきていないこと、その結果、利用者のネット利用状況があまり変わっていないことがうかがえます。動画については、解像度は確実に上がってきていますが、コーディックの圧縮率も向上してきているため、トータルでトラフィックの伸びが抑えられているのだと思われます。

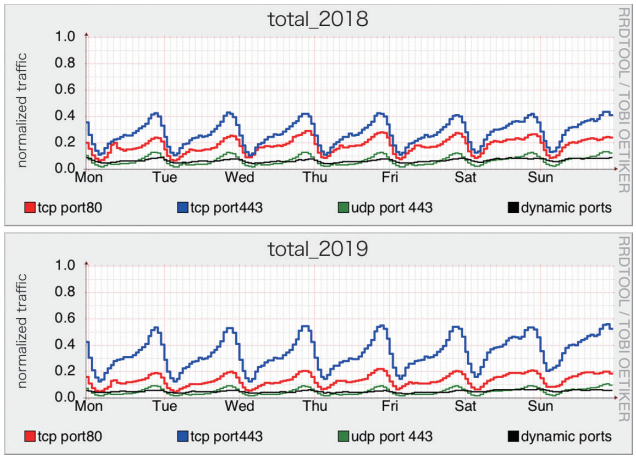

図-8 ブロードバンド利用者のポート利用の週間推移
2018年(上)と2019年(下)

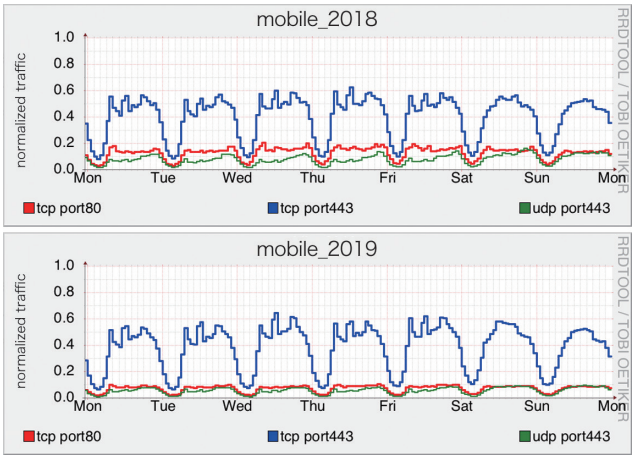

図-9 モバイル利用者のポート利用の週間推移
2018年(上)と2019年(下)

執筆者:
長 健二朗（ちょう けんじろう）
株式会社IIJ イノベーションインスティテュート 技術研究所所長。

IIJ Public DNSサービスについて

2.1 はじめに

IIJ Public DNSがベータ版サービスとして5月にリリースされました。DNS over TLS（以下 DoT）、DNS over HTTPS（DoH）「だけ」、すなわち通常のUDP/TCPによる名前解決をサポートせず、そしてIIJのユーザだけでなく誰でも使っていただけるキャッシュDNSサービスです。

本稿では、DoT/DoHが通常のDNSとどのように異なるか紹介すると共に、サービスを提供するに当たって検討したポイントと今後の課題について解説します。

2.2 DoT/DoH とは

2.2.1 DNSとプライバシー

DNSに登録される情報は広く公開されるのが前提です。そのため、DNSのセキュリティといえば、長い間「改ざんされないこと」すなわち完全性の確保が主眼であり、「盗聴されないこと」すなわち機密性の確保に重きが置かれることはありませんでした。

しかし、2013年のいわゆるスノーデン事件で、アメリカ国家安全保障局（NSA）による大規模な通信監視・情報収集活動PRISMの存在が告発されました。IETFはこれを受けて、"Pervasive Monitoring Is an Attack"（広範な監視は攻撃である）と宣言し（RFC7258）、今後策定されるプロトコルは広域監視に耐え得る設計であることが求められるようになりました。

PRISMの監視対象にDNSが含まれていたことも明らかになり、IETFでは新設のDPRIVE（DNS PRIVate Exchange）ワーキンググループにより、これまでおざなりにされてきたDNSのプライバシー確保の仕組みが検討されることになりました。DPRIVE WGではQname Minimisation（RFC7816）、EDNS（0）padding option（RFC7830、RFC8467）などDNSに対する様々なプロトコル拡張・修正を行いましたが、中でも比重の大きかったのがトランスポート暗号化です。

2.2.2 DNSトランスポート暗号化

従来のDNSは下位プロトコル（トランスポート）として主にUDPを、補助的にTCPを使います。しかし、素のUDP/TCPやその上に乗るDNSに機密性確保の機能はなく、通信が平文のまま行われるため盗聴も容易です。そこで、DNSと下位層の間に暗号化の層を置いて保護することにしたのです。

暗号化の層として様々なものが提案され、現在までにTLSを利用するDNS over TLS（RFC7858）、DTLSを利用するDNS over DTLS（RFC8094）、HTTPSを利用するDNS over HTTPS（RFC8484）が標準化されています。他にQUICを利用するDNS over QUICのドラフトがIETFに提出され議論が始まっています。また、同じく議論中のHTTP/3が標準化されると、DoHも自動的にHTTP/3に対応することになります（図-1）。

これら様々な暗号化層はどれかに一本化されるのではなく、現状ではユーザの都合に合わせて好きなものを選んで使えば良いことになっていますが、乱立してしまうとそれはそれで不便なので、将来的にはいくつかを残して残りは非推奨になることも十分考えられます（現状でもDNS over DTLSは仕様だけがあって実装は存在しておらず、今後使えるようになる可能性は小さいでしょう）。

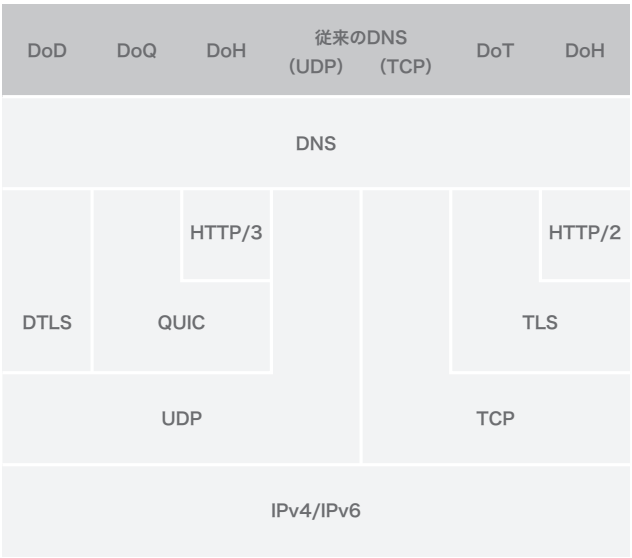

図-1 DNSのトランスポートプロトコル

2.2.3 トランスポート暗号化とDNSSEC

ところで、DNSには電子署名でDNS情報の真正性を検証するDNSSECという仕組みが既にあります。なぜDNSSECがあるのに新たにトランスポート暗号化が必要になるのでしょうか。また、トランスポート暗号化により、今後DNSSECは不要になるのでしょうか。

この問いに答える前に、まずトランスポート暗号化の使われる範囲について解説します。DNSは、ユーザがDNSの大本の情報を登録したサーバ(権威サーバ)に直接問い合わせるのではなく、ISPなどが提供するキャッシュサーバに情報を問い合わせ、キャッシュサーバが権威サーバへの問い合わせを行う構成が一般的です。

トランスポート暗号化が行われるのは、現状ではユーザとキャッシュサーバの間だけです。キャッシュサーバと権威サーバの間は暗号化されず、従来のDNSがそのまま使われます。

一般に暗号化は完全性と機密性のどちらも保証しますが、DNSのトランスポート暗号化についていえば、その範囲はユーザとキャッシュサーバの間に限られます。キャッシュサーバと権威サーバの間は暗号化されない従来のDNSが使われるため、キャッシュサーバが入手した情報の完全性の保証はなく、それを暗号で保護しても完全性は得られません。つまり、一般的な暗号化とは異なり、DNSトランスポートの暗号化はユーザとキャッシュサーバの間の機密性だけが保証されるプロトコルということになります(図-2)。

一方、DNSSECは「改ざんされないこと」を目的に導入されたものです。電子署名を使うことで完全性を保証しますが、通信自体は平文で、機密性はありません。

つまりトランスポート暗号化とDNSSECはどちらもDNSのセキュリティ向上のための仕組みですが、一方は機密性の保証に特化して完全性がなく、もう一方は完全性の保証に特化して機密性がないという相補的な関係になっていて、一方でもう一方を置き換えることはできません。それぞれが守るものが異なるので、トランスポート暗号化があるからDNSSECは要らないということにはならず、その逆もありません。

2.3 IIJ Public DNSサービスとDoT/DoH

DoT/DoHは下位層のトランスポートプロトコルが異なるだけで、DNSのプロトコル自体は従来のものと変わりません。しかし、サービスとして提供するに当たっては乗り越えなければならない壁がいくつかありました。ひとつひとつ見ていきましょう。

2.3.1 TCPの壁

DoT/DoHが従来のDNSと大きく異なるのは、TLSで暗号化されるということ以前に、すべてのやりとりがTCPになることです。従来のDNSはトランスポートとしてTCPとUDPのどちらも使えますが、主に使われるのはUDPで、TCPが使われるケースは限定的です。

TCPは上位層のプロトコルのやりとりが始まる前にセッション確立のための処理を行い、確立後も送信されたパケットが受信

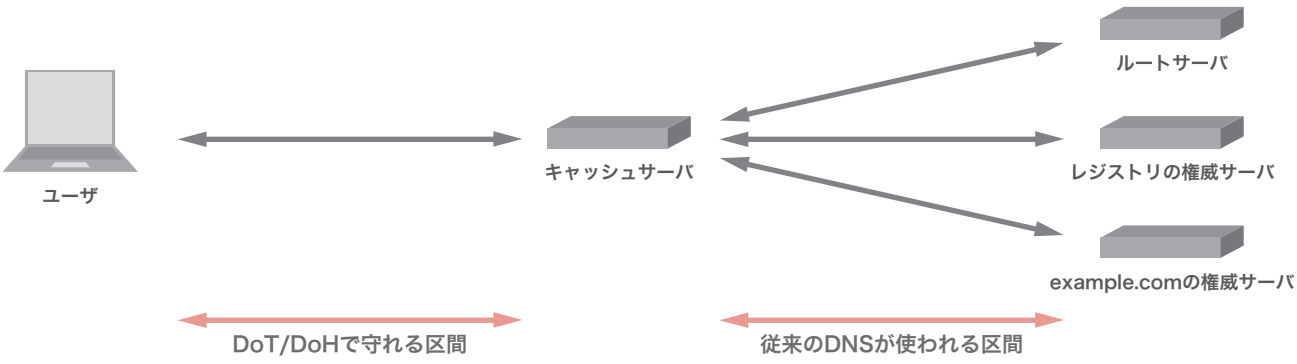

図-2 トランスポート暗号化のスコープ

されたかどうかチェックして必要に応じて再送するなど、通信の信頼性を確保するために様々な処理を行っています。

DNSはやりとりされるデータが非常に小さく、問い合わせ、応答ともにほとんどの場合で数百バイト以上になることはありません。このような用途でTCPを使うと、実際のDNSメッセージのやりとりよりも、セッションの確立・終了処理にかかるやりとりが大半を占めることになり、非常に効率が悪くなってしまいます。負荷の問題ならばサーバの数を増やすという富豪的なアプローチでも解決できますが、パケットの往復回数が増えることによるレイテンシ(遅延)の増大はどうしようもありません。

UDPはそのような仕組みを持たない分、単純・高速で、DNSやNTPなど小さなパケットのやりとりで完結するプロトコルで多く使われてきました。その一方で信頼性は低く、キャッシュポイズニングやDNS amp攻撃など、これまでに見つかったDNSに対する攻撃手法の多くは、DNSというプロトコル自体の問題というよりは、下位層にUDPを利用していることに起因しています。

TCPを使うことでこういった攻撃手法は成立しなくなる、ないしは大幅に脅威が減じられることは分かっているのですが、小さなパケットを大量にやりとりするというDNSの性質上、オーバーヘッドの非常に大きなTCPを主に利用する方向に転換することはこれまでできずにいました。2008年、これまで知られていた手法に比べてはるかに効率よくキャッシュポイズニングが可能なKaminsky Attack[*1]が公表された時でさえ、TCPに乗り換えることなく、ソースポートランダマイゼーション[*2]という対症療法でUDPのままなんとか乗り切ったぐらいです。

それほどTCPのオーバーヘッドを嫌っていたDNSですが、TLSが要求されることになると、必然的にTCPも必要になります。UDPを利用するDNS over DTLSもありますが、オーバーヘッドが大きいという点ではTCPとさほど変わらず、そもそも仕様だけの存在で実装が存在しないので誰も使えません。

とはいえ、安全なキャッシュDNSサービスを提供するための基盤とするなら、これまでの常識を捨てて考えなければなりません。IIJ Public DNSサービスがアクセス制限せず世界中の誰にも使っていただける"public"なDNSサービスとして提供できるのも、信頼性の低いUDP上のDNSを使わないことにして、DNS ampなどの攻撃の踏み台にされる懸念を払拭できたことが大きな要因となっており、TCPであることの利点にも積極的に目を向けなければなりません。

2.3.2 TLSの壁

DoT/DoHでは、UDPが一切使われずTCPになってオーバーヘッドが大きくなった上、更に暗号化のTLSのレイヤーがその上に載ります。TLSはHTTPSなど広く使われている技術ではありますが、決して処理が軽いわけではなく、DNSのように小さなデータを高速でやりとりする必要のあるプロトコルでは大幅な性能劣化をもたらします。

UDPによる従来のDNSと比べて大幅にパフォーマンスが劣化するということは理屈では分かるものの、実際どの程度劣化するのか調べるには測定のための道具が必要です。TCPによるDNSは、使われる場面が限定的だっただけで以前から存在していたので道具もあります。しかしDNS over TLSはまったく新しいものです。パフォーマンスを測定するための道具も満足なものがないのです。どれだけの劣化があるのか、どれだけの負荷があるのかを計測し、サービスとして提供するに当たりどれだけの設備を用意する必要があるのか見積もるために、我々はパフォーマンス測定ツールから開発する必要がありました。

TLSは非常に重い処理であるが故に、以前接続した際の情報を再利用してセッションを再開したり(TLS session resumption)、最新のTLS 1.3ではハンドシェイク手順の最初にやりとりされるClientHello/ServerHelloの中にアプリケーションのデータを入れる(0-RTT)などの方法でオーバーヘッドを小さくしたりといったオプションが利用できるようになっています。

---

*1 例えば、JPRS トピックス＆コラム、「新たなＤＮＳキャッシュポイズニングの脅威～カミンスキー・アタックの出現～」(https://jprs.jp/related-info/guide/009.pdf)など。

*2 クライアントが問い合わせの際に用いるソースポートをランダムにすることで、攻撃者がパケットを偽造するに当たって推測を的中させなければならない要素を増やし、攻撃の成功確率を下げる手法。

ただ、TLSのプロトコルで利用できる機能であっても、アプリケーションがそれを活用しなければ意味がありません。これらのオプションをフルに使いこなさないと大規模環境で実用的に動かすのは困難です。

IIJ Public DNSで利用しているのはオランダのNLnet Labsが開発しているUnboundというDNS実装で、これはかなり古く、DoTがIETF draftになる以前からTLSに対応していました。しかし、UnboundのTLS対応を調査した結果、こういったTLSのオーバーヘッドを減らすための仕組み、具体的にはTLSセッション再開機能が欠けていることが分かりました。パフォーマンス測定の結果でも十分な性能を出せていません。また、利用する暗号アルゴリズムによってもパフォーマンスが大きく変化しますが、これはソースコードに埋め込まれていて設定では変えられません。そのため、IIJではこれらに対応する機能を実装しています。成果はNLnet Labsにフィードバックされ、既に最新版では我々のコードが取り込まれた状態で配布されています。

TLSの壁はパフォーマンスの問題以外にもう1つあります。暗号化されていることそれ自体です。

DNSの安定運用のためには、異常な問い合わせが多数来ていないか、問い合わせは異常でないのに応答で異常なものが増えていないかなどの統計情報を取得し、もし異常があればそれを調査・対応できる仕組みが欠かせません。従来のDNSでは、こういった統計情報取得やトラブルシューティングはDNSサーバ自身で行うのではなく、DNSパケットをキャプチャすることにより実施するケースがほとんどでした。DNSサーバとは独立に処理を行えるため、利用するDNSサーバの実装によらず同じ手法を使えます。

しかし、TLSではキャプチャしたパケットは暗号化されています。いまはPerfect Forward Secrecy(PFS)が当たり前になっていて、サーバの秘密鍵があっても復号できません。これまで情報取得に使っていたツールがまったく使えなくなるということです。内々の実験ならともかく、サービスとして広く使っていただくためにはこれができなければ提供を断念せざるを得ないぐらい必須の機能です。そのためパケットキャプチャに頼らずDNSサーバ自体から得られる情報を用いてこれまで同様の統計情報を取得する基盤を作り直すことになり、ようやくサービス開始できるところにこぎ着けました。

2.3.3 HTTPの壁

実はHTTPの壁はそんなに高くありません。

DoHでは、TLSの後で更にDNSメッセージをHTTPメッセージにカプセル化する必要があります。DNSサーバ自身にHTTPを喋らせようとするのならばかなり苦労するでしょうが、一般的なHTTPサーバで問い合わせを受け、メッセージ形式を変換して背後のDNSサーバと通信するような2段構成であれば、バックエンドがDNSサーバであること以外はどこにでもある当たり前のWebアプリケーションでしかありません。

従来のUDPではなくTCPでありTLSである以上、レイテンシその他のパフォーマンスの問題から逃れられないのは明らかです。しかし、これまでの蓄積がなく手探りで行わなければならないDNSのレイヤーではなく、これまでに十分な実績のあるHTTPのレイヤーで面倒な部分の大半を解決できるため、それほど大きくつまずくことはありません。

2.3.4 壁は乗り越えられたのか

サービスを開始してから本稿執筆時点で約4ヵ月が経っています。

プレスリリース時には国内初のDoT/DoHサービスとしてそこそこ話題になり、Android用DoHクライアントであるIntra[*3]の設定UIでは、選択肢からIIJ Public DNSサービスを選ぶだけで使えるようにもなりました(選択肢に入れてくれとこちらからお願いしたわけではないのですが)。

*3 Intra(https://play.google.com/store/apps/details?id=app.intra&hl=ja)。

順調にスタートを切ってまったく問題なし、と胸を張りたいところですが、残念ながらそうなってはいません。

前述のとおり、UnboundにはもともとTLSセッション再開機能がなく、それを我々の手で実装したのですが、Android9のDoTはTLSセッションの有効期間が非常に短いようで、せっかく実装したセッション再開が有効に機能しないケースが多いことが分かっています。AndroidスマートフォンでWebページを読み込み、その後別のページを見に行こうとリンクを辿ると、そのときには前回の名前解決の際に確立されたTLSセッションが既にタイムアウトしており、ハンドシェイクを初めからやり直さなければならない、という事象が頻発するのです。ネットワークが混雑しているようなケースではこのハンドシェイクに失敗することも多々あり、結果として名前解決ができない、ネットが使えない、という現象がたびたび起きてしまうのです。

しかも、現在（執筆時点で）開発中ベータのAndroid10では、現行のAndroid9よりも更にパフォーマンスが悪化してしまうようです。

これ以外については特に大きな問題は起きていません。従来のDNSに比べてレイテンシが悪化するはずですが、体感的には問題ないようでお叱りを受けることもありません。

DoT/DoHはまだ新しい技術であり、根幹の仕様がやっと固まったばかりで、周辺仕様はこれから決める、という部分が多く残っています（例えば、現時点ではDoT/DoHサーバは手作業で設定するしかなく、ネットワーク管理者が設定を配布して自動で適用させる、ということができません）。

今後は問題点の改善に向けて引き続き調査・検討を進めると共に、将来標準化される新しい仕様を実装して最新の技術を安心して使っていただけるよう努め、また、サービスの運用で得られた知見をコミュニティに広く還元していく予定です。

2.4 パブリックDNSとDoT/DoH

最後に、IIJ Public DNSサービス以外の動きについて概観します。

本来キャッシュDNSサーバは組織内部のユーザに提供するもので、外部に公開する性質のものではありませんが、公開してもそれほど害はないという認識だったため、アクセス制限されていないもの（オープンリゾルバ）が大半でした。しかし、DNS ampという攻撃手法が発見され、DDoS攻撃の踏み台として広く利用されるようになったため、2010年頃からは必要な範囲からのアクセスだけに制限するのが常識になっています。

その一方で、接続元アドレスによる制限ではなくレート制限などの方法で攻撃の対策をした上で、幅広いユーザに使ってもらおうというサービスが出てきました。その先駆者となったのはOpenDNS[*4]ですが、その後に登場したGoogle Public DNS[*5]が定着して以降は、このような意図してオープンリゾルバにしているサービスを「パブリックDNS」と呼ぶのが通例になっています。

DoTのRFCが標準化されたのは2016年です。翌2017年11月にサービス開始したパブリックDNSであるQuad9[*6]、2018年4月開始のCloudflare[*7]は当初から、Googleも2019年1月からDoTに対応しています。

DoHが正式にRFCになったのは2018年10月ですが、ドラフトをベースにした実装が先行し、Cloudflareでは2018年4月の開始当初から、Quad9もRFC8484が出る2週間前にDoHに対応し、遅れてGoogleも2019年6月に対応しました。

クライアント側でもAndroidがOSとして2018年8月からDoTに、10月にアプリとしてDoHクライアントIntraがリリースされています。WebブラウザではFirefoxが2018年8月にDoHに対応、Chromeは執筆時点では開発版でのみの対応ですが、本稿が世に出る頃には正式版でも利用できるようになっているかもしれません。

＊4　OpenDNS（https://www.opendns.com/）。
＊5　Google Public DNS（https://developers.google.com/speed/public-dns/）。
＊6　Quad9（https://www.quad9.net/）。
＊7　Cloudflare（https://developers.cloudflare.com/1.1.1.1/）。

このように、DoT/DoHへの対応は急速に進んでいますが、その一方で懸念もないわけではありません。

Firefoxではゆくゆくは名前解決をデフォルトでDoHにしたい、すなわちユーザが特に設定しなければFirefoxが選定したパブリックDNSサービスを自動で使わせる意向であると伝えられています[*8]。しかし、パブリックDNSはパブリックであるが故に、イントラネットなどプライベートな名前空間の解決ができません。また、DNSを利用したペアレンタルコントロールサービスなどを利用している場合、OSの設定とは異なるDNSサーバをブラウザに勝手に使われてしまうと制御できなくなってしまいます。こういった点から、デフォルトでDoHの設定を「押しつける」ことの是非については議論があります。

Google Public DNSはDoT/DoHに対応しており、これを使うことでユーザとGoogleの間の機密性が保証されることになります。その一方で、GoogleはEDNS0 Client Subnet (ECS; RFC7871) にも対応しています。ECSはキャッシュサーバに問い合わせてきたクライアントの属するネットワークの情報をキャッシュサーバから権威サーバに伝えることで、コンテンツ配信のトラフィックマネジメントに役立てようというものですが、ECSが使われるキャッシュサーバと権威サーバの間は常に従来のDNSが使われるということに注意しなければなりません。ユーザがDoT/DoHを使っていればGoogleまでの間の経路上では盗聴されませんが、Googleと権威サーバの間の経路上は機密性のない従来のDNSが使われるため盗聴が可能で、ここに含まれるECSの情報からユーザのプライバシーが漏れかねないのです。

DNSトランスポートが暗号化されていくという流れ自体はもはや確定的であり、これを押しとどめることは到底できそうもありません。しかし、すべてを是とするのではなく、ほんとうにそれは正しいのかひとつひとつ検証していくこともまた、新たにパブリックDNSサービスを始めた我々の重要な責務といえるでしょう。

執筆者:
山口 崇徳（やまぐち たかのり）
IIJ アプリケーションサポート部アプリケーションサポート課。DNSサービスのサポート等に従事。

*8 Firefox Nightly News、"What's next in making Encrypted DNS-over-HTTPS the Default" (https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default)。

September 2019 Vol.44

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2019年9月時点のものです。

IIJ-MKTG019-0044

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