IIR

Internet
Infrastructure
Review

Dec.2018
Vol.41

定期観測レポート

IIJインフラから見るインターネットの傾向

フォーカス・リサーチ(1)

URL文字列の深層学習による詐称サイト識別

フォーカス・リサーチ(2)

海底ケーブルとインターネットの信頼性

IIJ
Internet Initiative Japan

Internet Infrastructure Review

December 2018 Vol.41

エグゼクティブサマリ

第5世代移動通信システム（以下、5G）に関するニュースが増えてきました。アメリカではVerizonが2018年10月より一部都市で5Gのサービスを開始しています。サービス名は「Verizon 5G Home」といい、移動通信ではなく、家庭向けのブロードバンドサービスで、FWA (Fixed Wireless Access）と呼ばれる利用方法です。一方、韓国でも移動通信3社が2018年12月にサービスを開始するとのニュースがありました。こちらは、まず産業向けのソリューション提供を目指しているようです。

日本においては、2020年に本格的な5Gのサービスの開始が予定されていますが、移動通信3社は、2019年中に5Gのプレサービスを開始するとしています。2018年10月に開催された総務省の会合で各社が明らかにしたプレサービスの内容は、地方創生に関わるものや、競技場のVRなど多様でした。

プレサービスに先立って、2019年3月末までに5Gのための周波数が割り当てられる予定で、その指針が去る11月に総務省から公開されました。全国で使われる周波数として、3.7GHz帯、4.5GHz帯、28GHz帯から計10枠・1,800MHz幅が提示されたほか、自営用などで利用できる割当枠について検討するとのことで、4.5GHz帯に200MHz幅、28GHz帯に900MHz幅の周波数が残されました。この周波数がどのように割り当てられるかは、これからの議論次第となりますが、従来の全国系移動通信事業者以外からも特徴のあるサービスが提供されることが期待されます。

「IIR」はIIJで研究・開発している幅広い技術のご紹介を目指しています。私たちが日々のサービスの運用から得られる各種データをまとめた「定期観測レポート」と、特定テーマを掘り下げる「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、IIJインフラから見るインターネットの傾向と題して、IIJのネットワークインフラで観測している各種データのなかから、BGPの経路数、DNSの問い合わせ数、IPv6トラフィック、モバイル・トラフィック、バックボーン・トラフィックに関する分析を紹介しています。BGPの経路数は、IPv4アドレス在庫の枯渇にともない、移転を目的としたアドレスブロックの分割が進んでいるためか、/22、/23、/24の経路が増加していることや、増加を続けている32-bit only ASがIPv4のみで運用されていることなど、興味深い分析結果が出ています。また、BGP経路数、DNS問い合わせ、各種トラフィックのいずれからも、IPv6の利用が進んでいることが読み取れました。

2章では、フォーカス・リサーチ（1）として、詐称URLの判断に深層学習を応用する試みを紹介しています。インターネットを爆発的に普及させ、私たちの社会活動に大きな影響を与えたのはWWWであることに間違いはありません。そのように社会に深く浸透したWWWの悪用例として、オンラインサービスや銀行のサイトの詐称行為が挙げられます。このような詐称サイトへのアクセスから利用者を守ることは、ネットワークサービスの提供に携わる者にとって重要な課題の1つです。詐称サイトの判定には多くの手法が提案されています。今回、ご紹介するのは、簡単なニューラルネットワークモデルによる検証ではありますが、高い精度でURLの分類が行えました。

3章のフォーカス・リサーチ（2）では、海底ケーブルを取り上げています。インターネットにおける国際データ通信の99%は、海底ケーブルによって運ばれており、海底ケーブルは、グローバルなインターネットにおいて非常に重要な存在です。本稿では、海底ケーブルに関する公開情報から、海底ケーブルの成長と現状を明らかにし、海底ケーブルの障害によるインターネットへの影響について、実際の障害における各種の観測データをもとに考察する手法を提案しています。

IIJでは、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、お客様の企業活動のインフラとして最大限にご活用いただけるよう、様々なサービス及びソリューションを提供してまいります。

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。

IIJインフラから見るインターネットの傾向

IIJではインターネットサービスを提供するために、国内でも有数規模のネットワーク・サーバインフラを運用しています。ここでは、IIJのインフラ運用を通じて得られた情報を元に、現在のインターネットがどのような傾向を持っているのかを検討し、紹介します。

取り上げるテーマは、ネットワークの経路情報、DNS問い合わせ情報、IPv6利用状況、モバイル接続サービス利用状況です。また、IIJのトラフィックの大部分を支えるバックボーンネットワークの現状についてもあわせて報告します。

Theme 01

BGP・経路数

昨年のIIR Vol.37（https://www.iij.ad.jp/dev/report/iir/037.html）に続いて、まずは弊社網から他組織に広報している「IPv4フルルート」の情報を確認していきます（図-1、表-1）。なおこの1年の間にRIPE NCCでは最後の/8ブロックからの割り振り/割り当てが終了しており（ARINに続いて2つ目）、またIANA "Recovered IPv4 Pool"から各RIRへの割り振りサイズは/22（1024アドレス）にまで減少しました。IPv4アドレスの取得はアドレス移転に頼らざるを得ない傾向が進んでいると言えます。

経路総数は過去8年間で最大の増加となり70万経路を超えました。またプレフィクス長ごとで見ると/22及び/23経路の増加率が10%を超えており、これらに/24経路を足した計3プレ

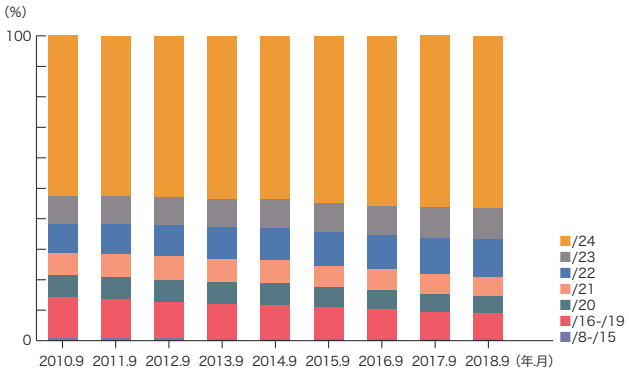


図-1「IPv4 フルルート」に占める各プレフィクス長経路数の比率の推移

表-1「IPv4 フルルート」に含まれるプレフィクス長ごとの経路数の推移

年月	/8	/9	/10	/11	/12	/13	/14	/15	/16	/17	/18	/19	/20	/21	/22	/23	/24	total
2010年9月	20	10	25	67	198	409	718	1308	11225	5389	9225	18532	23267	23380	30451	29811	170701	324736
2011年9月	19	12	27	81	233	457	794	1407	11909	5907	9885	19515	26476	26588	35515	34061	190276	363162
2012年9月	19	14	29	84	236	471	838	1526	12334	6349	10710	20927	30049	31793	42007	39517	219343	416246
2013年9月	16	11	30	93	250	480	903	1613	12748	6652	10971	22588	32202	34900	48915	42440	244822	459634
2014年9月	16	12	30	90	261	500	983	1702	13009	7013	11659	24527	35175	37560	54065	47372	268660	502634
2015年9月	18	13	36	96	261	500	999	1731	12863	7190	12317	25485	35904	38572	60900	52904	301381	551170
2016年9月	16	13	36	101	267	515	1050	1767	13106	7782	12917	25229	38459	40066	67270	58965	335884	603443
2017年9月	15	13	36	104	284	552	1047	1861	13391	7619	13385	24672	38704	41630	78779	64549	367474	654115
2018年9月	14	11	36	99	292	567	1094	1891	13325	7906	13771	25307	39408	45578	88476	72030	400488	710293
増減数(※)	-1	-2	0	-5	8	15	47	30	-66	287	386	635	704	3948	9697	7481	33014	56178

※2017年9月からの値

フィクスで経路増加数の89%、経路総数の79%を占めるまでになりました。移転を目的としたアドレスブロックの分割が更に進むに従ってこれらのプレフィクスの占める割合がどこまで伸びるのか、今後も注視したいと思います。

次に「IPv6フルルート」の情報を確認します(表-2)。こちらも経路総数は過去8年間で最大の増加となりました。但し総数の74%はプレフィクス長が/33 ～/48の経路で占められ、更にその76%以上は割り振り(/割り当て)ブロックを分割しての経路広報によるものと計算されます。経路数はIPv6普及の目安の1つになりますのでその増加は望ましいことですが、分割広報が全体の半数を超える現状は「経路広報を集約することで経路表の増大を抑制する」という初期にあったIPv6の理想(?)から程遠く、少々残念でもあります。

最後に追加で「IPv4/IPv6フルルート」広報元AS(Origin AS)の数も見ておきましょう(表-3)。IANAの16-bit AS番号poolが2016年7月に枯渇していることもあり、16-bit AS番号のOrigin AS数は同年から減少に転じています。一方の32-bit only AS番号(2007年1月割り当て開始)のOrigin AS数は順調に増加を続けていますがその大多数はIPv4のみで運用されているようです。これは、IPv4アドレス在庫が既に枯渇した状況下でAS番号を取得しBGP運用を開始したであろう新規組織であっても多くはIPv6の利用を考慮しない、という問題を示していると考えられ、IPv6の普及はまだまだ先が長いという現状が見て取れます。とはいえIPv4アドレスの取得がこの先より難しくなっていくであろうことは間違いありませんのでこの状況が今後も継続するのか否か、こちらも注視していきたいと思います。

表-2「IPv6 フルルート」に含まれるプレフィクス長ごとの経路数の推移

年月	/16-/28	/29	/30-/31	/32	/33-/39	/40	/41-/43	/44	/45-/47	/48	total
2010年9月	38	3	10	2023	33	2	9	4	17	436	2575
2011年9月	68	13	22	3530	406	248	45	87	95	2356	6870
2012年9月	102	45	34	4448	757	445	103	246	168	3706	10054
2013年9月	117	256	92	5249	1067	660	119	474	266	5442	13742
2014年9月	134	481	133	6025	1447	825	248	709	592	7949	18543
2015年9月	142	771	168	6846	1808	1150	386	990	648	10570	23479
2016年9月	153	1294	216	8110	3092	1445	371	1492	1006	14291	31470
2017年9月	158	1757	256	9089	3588	2117	580	1999	1983	18347	39874
2018年9月	168	2279	328	10897	4828	2940	906	4015	2270	24616	53247
増減数(※)	10	522	72	1808	1240	823	326	2016	287	6269	13373

※2017年9月からの値

表-3「IPv4/IPv6 フルルート」の広報元AS数の推移

AS番号	16-bit(1～64495)					32-bit only(131072～4199999999)				
広報経路	IPv4+IPv6	IPv4のみ	IPv6のみ	total	(IPv6 -enabled)	IPv4+IPv6	IPv4のみ	IPv6のみ	total	(IPv6 -enabled)
2010年9月	2083	32399	67	34549	(6.2%)	17	478	3	498	(4.0%)
2011年9月	4258	32756	115	37129	(11.8%)	90	1278	13	1381	(7.5%)
2012年9月	5467	33434	125	39026	(14.3%)	264	2565	17	2846	(9.9%)
2013年9月	6579	34108	131	40818	(16.4%)	496	3390	28	3914	(13.4%)
2014年9月	7405	34555	128	42088	(17.9%)	868	4749	55	5672	(16.3%)
2015年9月	8228	34544	137	42909	(19.5%)	1424	6801	78	8303	(18.1%)
2016年9月	9116	33555	158	42829	(21.7%)	2406	9391	146	11943	(21.4%)
2017年9月	9603	32731	181	42515	(23.0%)	3214	12379	207	15800	(21.7%)
2018年9月	10199	31960	176	42335	(24.5%)	4379	14874	308	19561	(24.0%)

Theme 02

DNS

IIJでは利用者がDNSの名前解決を利用できるようフルリゾルバを提供しています。この項では名前解決の情況を解説し、IIJで2018年5月17日に行ったフルリゾルバの1日分の観測データから、主にコンシューマサービス向けに提供しているサーバのデータに基づいて分析と考察を行います。

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

IIJが提供するフルリゾルバの観測データを見てみると、利用者の利用傾向を示すように時間帯によって問い合わせ量が変動し、朝4時頃に問い合わせ元のIPアドレス当たり最小の0.05query/sec、昼13時頃にピークを迎えて0.22query/sec程度になっています。問い合わせ傾向を通信に使われたIPv4とIPv6のIPプロトコル別に見てみると日中は大きな違いはなくほぼ同じ傾向を示している一方、夜20時以降はIPv6でIPアドレス当たりの問い合わせが増える傾向が見えています。家庭でIPv6が利用できる環境が整備されてきていることを示唆していると考えています。

近年の特徴的な傾向として、毎正時などキリの良い時刻に一時的に問い合わせが増加しています。問い合わせ元数も同時に増えているため、利用者の端末でタスクをスケジュールしたり、目覚まし機能などで端末が起動することに伴う機械的なアクセスが原因ではないかと推測しています。これをもう少し細かく分析すると、毎正時の14秒前にも問い合わせが増加しています。毎正時後は増加後、緩やかに問い合わせ量が減っていくのに比べて、毎正時の14秒前の増加では直ぐにそれまでの問い合わせ量程度に戻っています。つまり多くの端末が綺麗に同期して問い合わせを行っていることから、何かすぐに完了する軽量なタスクが実行されているのではないかと推測しています。例えば何らかの実装で接続確認や時刻同期など基本的なタスクを本格的なスリープ解除前に終わらせる機構があり、これに利用している問い合わせなどが影響していると考えています。

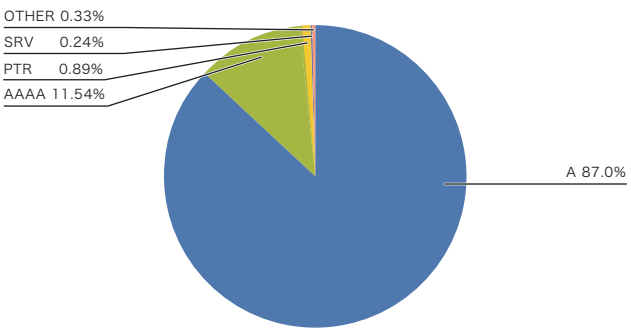


図-2 クライアントからのIPv4による問い合わせ

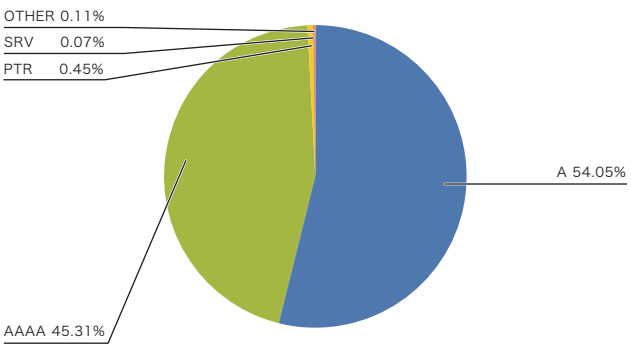


図-3 クライアントからのIPv6による問い合わせ

問い合わせレコードタイプに注目すると、ホスト名に対応するIPv4アドレスを問い合わせるAレコードとIPv6アドレスを問い合わせるAAAAレコードがほとんどを占めています。昨年と比べるとANYタイプの問い合わせが減少しています。

これはANYタイプの問い合わせが反射攻撃などに悪用され、IETFで対策の議論も続いているなどの現状があり、段々と利用されなくなってきているためだと考えています。問い合わせのIPプロトコルごとに傾向を見ると、IPv6による問い合わせが問い合わせ元IP数、実際の問い合わせ数共にIPv4よりも多くなっています。AとAAAAの問い合わせ傾向は通信に利用されるIPプロトコルで違いが見られ、IPv6での問い合わせではより多くのAAAAレコード問い合わせが見られます。IPv4での問い合わせでは、全体の87%程度がAレコード問い合わせ、11%程度がAAAAレコード問い合わせです(図-2)。一方IPv6での問い合わせでは、全体の54%程度がAレコード問い合わせ、45%程度がAAAAレコード問い合わせとAAAAレコード問い合わせの比率が高まっています(図-3)。

Theme 03

IPv6

前回IPv6の状況についてお伝えした「Internet Infrastructure Review Vol.37」からおよそ1年が経過しました。今回も、IPv6のトラフィックがIIJバックボーン全体でどれくらいの流量なのか、及び主に利用されているプロトコルは何か、解説します。また、今回は特にIPv6トラフィックが増加しているモバイルサービスのトラフィックについて、現状と要因を考察します。

■ トラフィック

前回同様、IIJのコアPOP(東京・大阪・名古屋)のバックボーンルータで計測した、IPv4トラフィックとIPv6トラフィックを図-4に示します。期間は2017年10月1日から2018年9月30日までの1年間です。IPv4のトラフィックはこの1年で約20%増加、IPv6のトラフィックは1年で約80%増加しました。全トラフィックに占めるIPv6の割合は、約6%となり、

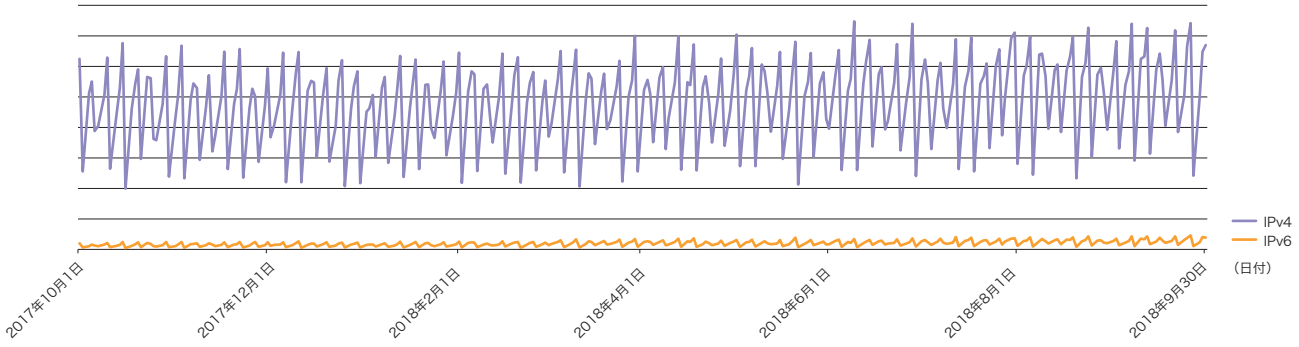


図-4 IIJのコアPOP(東京・大阪・名古屋)のバックボーンルータで計測した、IPv4トラフィックとIPv6トラフィック

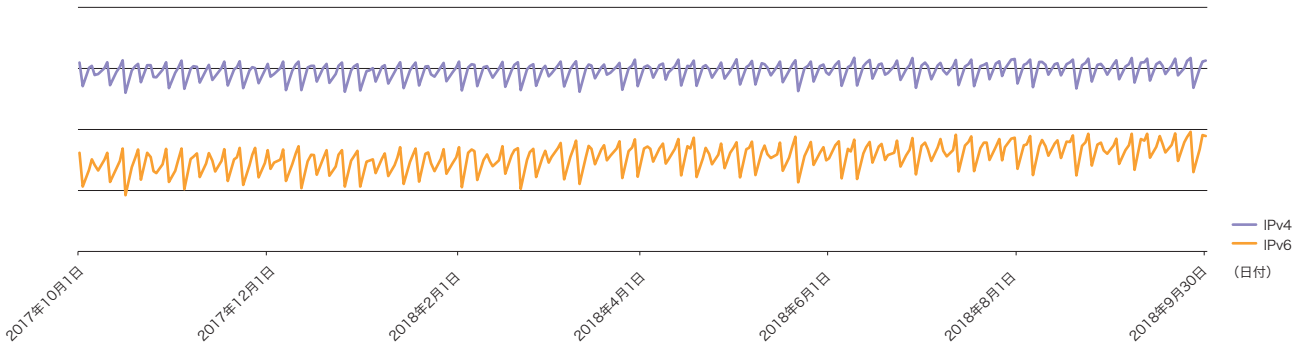


図-5 IIJのコアPOP(東京・大阪・名古屋)のバックボーンルータで計測した、IPv4トラフィックとIPv6トラフィック(ログスケール)

昨年の約4%から増加しています。図-5は同じ期間をログスケールで描画したものです。トラフィックの絶対量としては、IPv6はIPv4の1/10以下ですが、伸び率ではIPv4より大きいことが分かります。

次に、2017年10月から2018年9月までの1年間の、IPv6とIPv4の平均トラフィック送信元組織(BGP AS番号)の上位を図-6と図-7に示します。

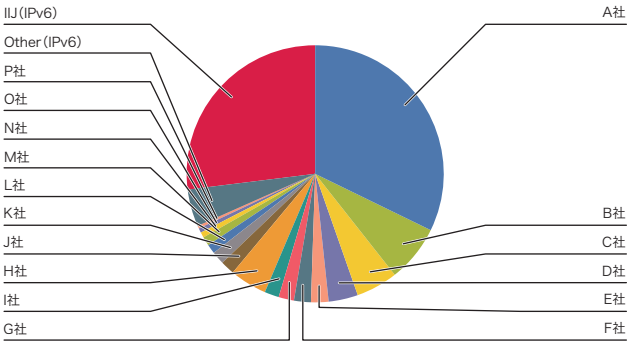


図-6 2017年10月から2018年9月までの
1年間の平均IPv6トラフィック送信元組織(BGPのAS番号)の上位

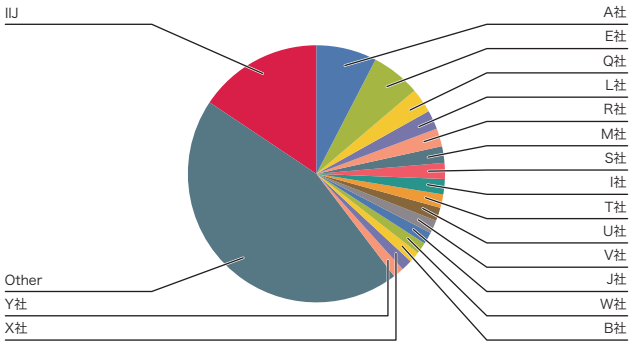


図-7 2017年10月から2018年9月までの
1年間の平均IPv4トラフィック送信元組織(BGPのAS番号)の上位

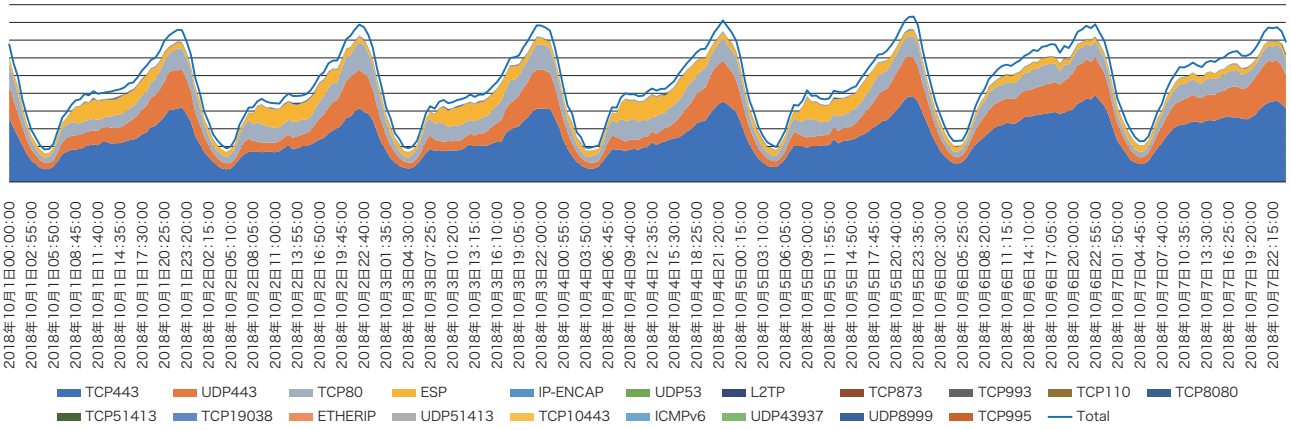


図-8 IPv6トラフィックのProtocol番号(Next-Header)と送信元ポート番号で解析したグラフ

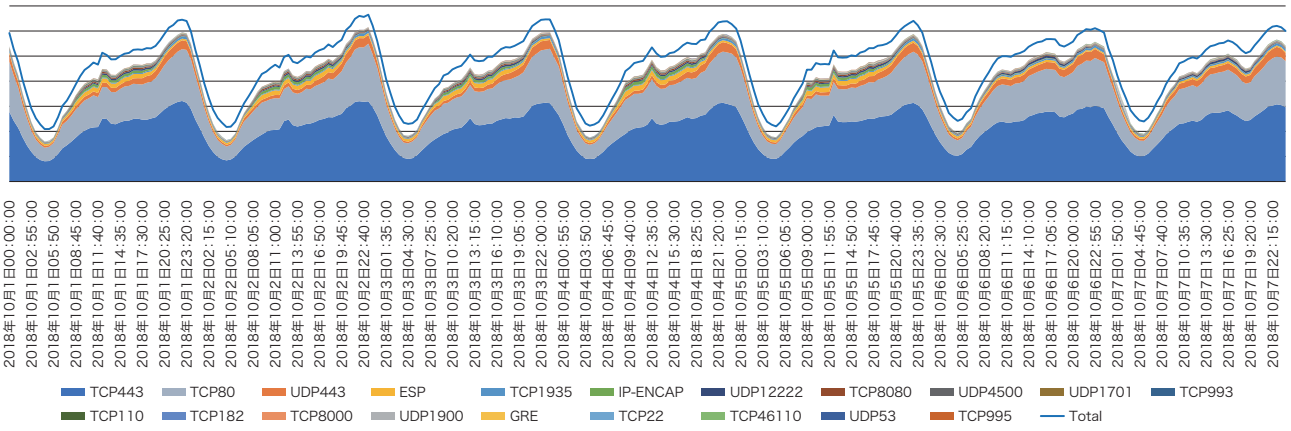


図-9 IPv4トラフィックのProtocol番号と送信元ポート番号で解析したグラフ

1位は昨年同様の事業者ですが、2位以降とのトラフィック量の差が縮小し、占有率は前回と比べ半分程度まで下がっています。2位以降の事業者においてもIPv6の活用が進んでいることがうかがえます。また、フレッツ光ネクストでIPv6 IPoE接続サービスを提供している事業者のトラフィックも4位と6位に入ってきており、IPv6 IPoEの普及がIPv6の利用増につながっているものと考えられます。

■ 利用プロトコル

IPv6トラフィックのプロトコル番号(Next-Header)と送信元ポート番号で解析したグラフを図-8に、IPv4トラフィックのプロトコル番号と送信元ポート番号のグラフを図-9に示します(2018年10月1日からの1週間)。

昨年と同様の傾向ですが、TCP/UDP443、TCP80が全体に占める割合が更に増加し、トラフィックのほとんどがWeb系のアプリケーションで占められています。これはIPv6に限らず、IPv4も同様の傾向です。

また、昨年6位だったIP-ENCAP (プロトコル番号4)の順位が5位に上がっています。グラフ上は潰れて見えませんが、数値的には昨年から倍以上の伸びとなっており、DS-Lite(RFC6333)などIPv4 over IPv6系技術を用いたトラフィックが増加しているものと推察しています。

■ モバイルサービスのIPv6トラフィック

今回は新たにモバイルサービスのIPv6トラフィックについて紹介します。

図-10のグラフは、IIJのモバイル系サービスにおける2016年10月1日から2年間のトラフィックグラフです。ちょうど真ん中あたりが2017年9月下旬になりますが、その近辺からIPv6トラフィックが急に増加しています。

これは、米Apple社のiPhoneやiPadのOSであるiOSバージョン11のリリースと重なります。iOSバージョン11では、MVNOのAPNプロファイル(モバイル網に接続するための情報ファイル)

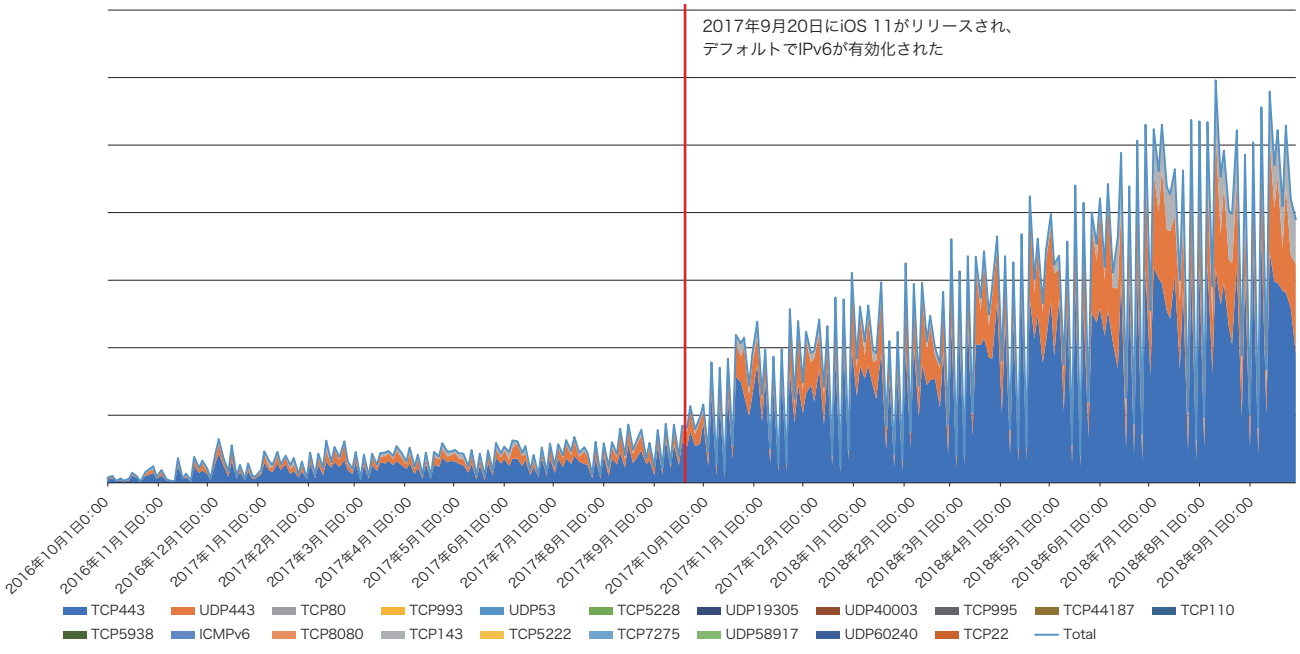


図-10 IIJのモバイル系サービスにおける2016年10月1日から2年間のトラフィック

でも、デフォルトでIPv6接続が有効化されたことから、多くのユーザの端末でIPv6が利用され始めたためと考えられます。

また、モバイルのIPv6トラフィックのほとんど（98%以上）がWeb系アプリケーションのトラフィックです。

■ まとめ

今回はIPv6のトラフィック量、利用プロトコル、そしてモバイルサービス個別のIPv6トラフィックについて見てきました。全体としてIPv6トラフィックは増加しており、IPv4の増加率よりも高くなっていました。これは、「フレッツ光ネクストにおけるIPv6 IPoEサービスの普及」「Apple iOS11のリリース」などにより、一般ユーザが利用する端末においてもIPv6の利用が進んだこと、及び、IPv6でサービスを提供する事業者の多様化が進んだことが一因と考えられます。2019年中頃には、IPv4アドレス在庫が残っている最後の地域レジストリであるAFRINIC（アフリカ地域）のIPv4枯渇が予想されているため、今後はますますIPv6の活用が進んでいくものと思われます。

Theme 04

モバイル・ブロードバンド

ここではモバイルとブロードバンドのトラフィックを分析してみます。なお、本項のブロードバンドにFLETSのIPoEは含まれません。

図-11はモバイルとブロードバンドそれぞれについて、利用者から見たダウンロード方向、アップロード方向のトラフィック量（bps）をそれぞれのピーク値で正規化したグラフです。このグラフを見ると、モバイルは昼の12時前後に、ブロードバンドは夜の22時前後にトラフィックのピークがあることが分かります。モバイルは外出先で利用されるケースが多いため日中のトラフィックが多くなっています。また、通勤通学、帰宅時間帯にも増加が見られ、人の活動と相関が強いことが分かります。一方のブロードバンドは、帰宅後に自宅で利用されるため夜間のトラフィックが多くなっています。

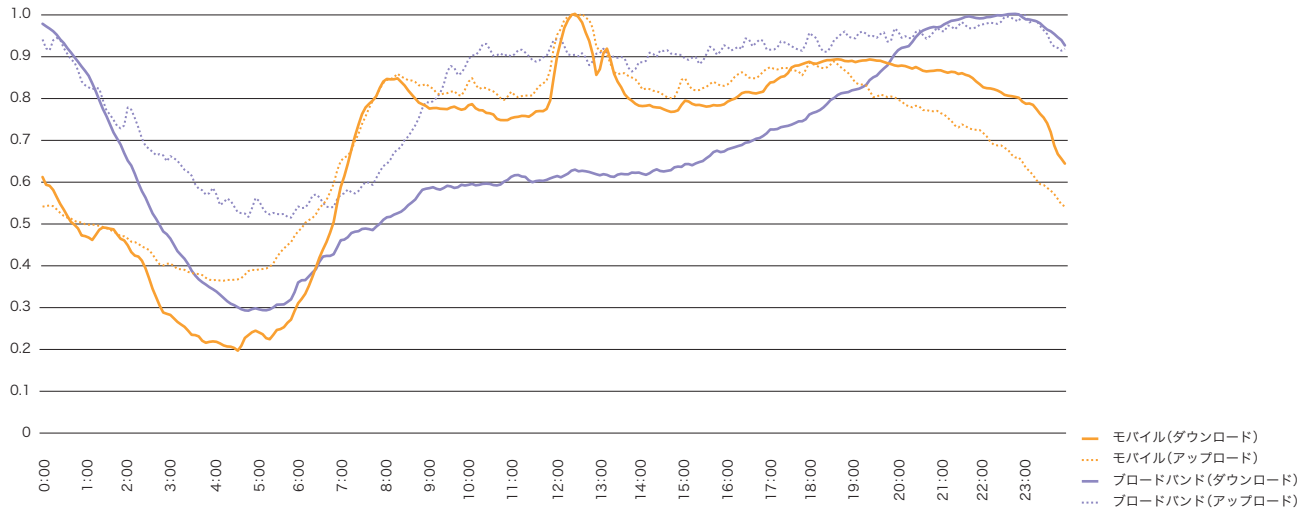


図-11 ピークに対するトラフィック比

また、モバイル、ブロードバンド共にダウンロードの方が1日を通じた変動が大きくなっています。ブロードバンドは朝方から夜のピークにかけて徐々にトラフィックが増え続ける傾向にあり、一方のモバイルはブロードバンドと比べ、朝になると急激に増え、その後も日が変わる直前まで利用が多いことが分かります。

参考までに、総務省が公開している「我が国の移動通信トラヒックの現状（平成30年6月分）」に記載された移動通信事業者5者のトラフィック状況を見ると、トラフィックのピークはIIJのブロードバンドと同じく夜にあるようです。現状、IIJのモバイル（MVNO）はMNOと比較し、新しいものに敏感なアーリーアダプタと呼ばれる顧客層が多いと考えられ、これらの顧客層は自宅にブロードバンド回線を保有していて、夜間はそちらにトラフィックがオフロードされる割合が高いと推測されます。MVNOが更に普及しマジョリティ層が増えるに従い、トラフィックのピークもMNOと同じく夜にシフトしていくものと思われます。

次に、ダウンロードとアップロードの比率を比較します。図-12はモバイルとブロードバンドそれぞれについて、ダウンロードのトラフィック量（bps）をアップロードで割った比率を表しています。

このグラフを見ると、モバイルよりブロードバンドの方がダウンロードの比率が高いことが分かります。技術の進歩によりモバイルの通信速度は日々向上していますが、一般にはまだブロードバンドの方が安定して高速な通信が可能です。また、基本的に使い放題なブロードバンドに比べ、モバイルは様々な形で転送量に上限を設けている場合が多くあります。そのため、ブロードバンドの方がより大容量のダウンロード通信が発生しているものと思われます。

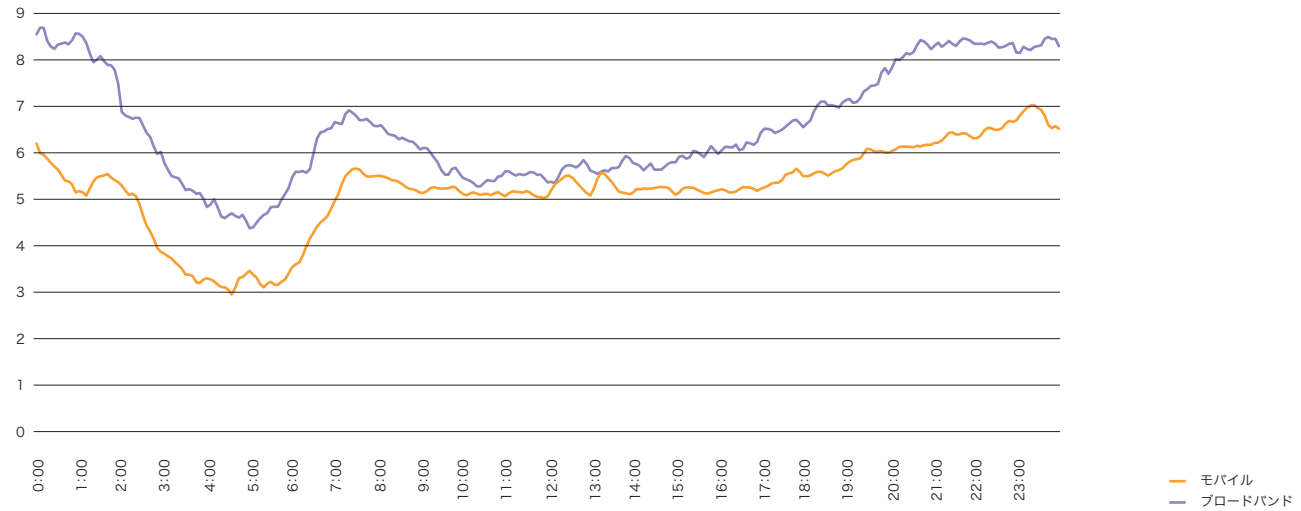


図-12 ダウンロードに対するアップロードのトラフィック比

次はプロトコルを比較します。図-13と図-14はモバイルとブロードバンドそれぞれについて、ダウンロード方向のトラフィック量(bps)に関するプロトコルの割合(プロトコル、ソースポート)を示したものです。

モバイルとブロードバンド、いずれもHTTP関連プロトコル(443/tcp及び80/tcp)が全体の約3/4を占めています。また、443/udpを使うQUICという比較的新しいプロトコルも上位に入っています。なお、QUICの通信先は特定のインターネットサービス事業者に著しく偏りが見られます。興味深いのは、ブロードバンドよりもモバイルの方が443/tcp、つまりはHTTPSの割合が高い点です。モバイル利用者の多くはスマートフォンを使用していると推測されますが、単純にWebページを汎用的なブラウザから閲覧するよりも、ある用途に特化した様々な専用アプリケーションを使う機会が多く、そこで利用されるプロトコルは多くがHTTPSであるのかもしれません。

次はIPv6の利用率を見てみます。表-4はモバイルとブロードバンドの接続種別の割合を示しています。この表が示すとおり、若干ながらモバイルの方がIPv6利用率が高くなっています。現在新規に販売されるスマートフォンの多くはIPv6に対応しており、ユーザが意識しなくてもIPv6が自然と利用できる環境が整っています。NTTのFLETSにおいても、対応したホームゲートウェイを利用していればユーザは特に意識することなくIPv6が利用できますが、自身でブロードバンドルータを用意する場合には個別に設定をする必要があります。なお、FLETSにはPPPoE接続とIPoE接続という２つの接続方法があり、昨今は通信速度上のボトルネックが少ないIPoE接続を利用するユーザが増えています。IPoE接続の場合は標準がIPv6接続であり、IPv4通信を行うためにはDS-Liteなど IPv6の上でIPv4通信を行うプロトコルに対応した環境が必要になります。

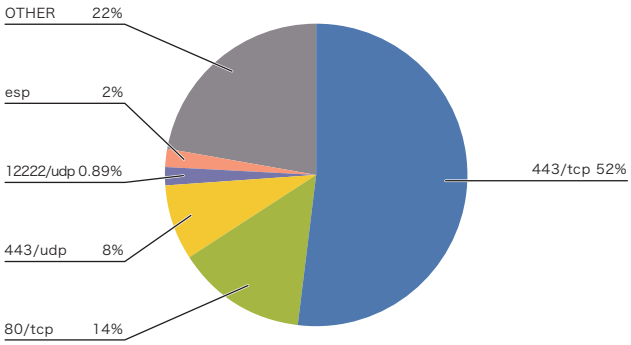


図-13 ダウンロード方向のトラフィック量(bps)に関するプロトコルの割合(モバイル)

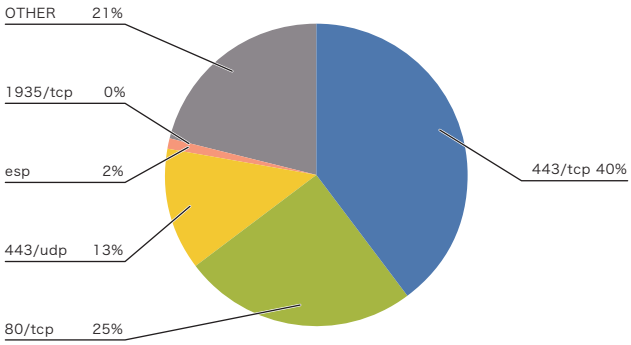


図-14 ダウンロード方向のトラフィック量(bps)に関するプロトコルの割合(ブロードバンド)

モバイルには一定数、IPv6のみを利用しているユーザがいます。IPv6でもIPv4と同等にコンテンツを提供するサービスも増えていますので場合によってはIPv6のみで需要を満たせるケースがあるかもしれませんが、これだけのユーザがいるのには驚かされます（端末によってはIPv4/IPv6同時利用の設定を行うと何故かIPv4、IPv6を別々に接続することがあり、この影響も考えられます）。

最後に、モバイルで利用されている端末種別を見てみます。モバイルのユーザ通信はGTPというプロトコルを利用していますが、接続時に行う一連の処理の中で移動機は自身の端末種別（IMEI：International Mobile Equipment Identity）をネットワークに対して申告します。IMEIはメーカ、製品名などの情報から成り立っていて、これらを解析することでユーザが使っている端末をおおよそ把握することができます。

図-15は、メーカ別の割合を示したものです。世界の中でも日本は特にApple社の比率が高いと言われていますが、IIJの個人系モバイルサービスでも4割近くを占めています。IIJではスマートフォンの販売を行っていますが、Apple社の製品は扱っていないにもかかわらずこれだけの割合を占めることは驚異的であり、ユーザにとっていかに魅力的な端末であるかが分かります。

モバイルにおいて移動機、つまりスマートフォンはユーザ体験に非常に大きな影響があり、それ故に各モバイル事業者はスマートフォンの販売に非常に力を入れています。特にIIJなどのMVNOは、MNO契約時に使っていたスマートフォンをそのままMVNOでも利用するケースがあり、これらを含めてどのようなスマートフォンが利用されているかを把握することはサービス戦略上重要になってきます。

表-4 モバイルとブロードバンドの接続種別の割合

	IPv4	IPv6	IPv4v6
モバイル	70.43%	0.02%	29.55%
ブロードバンド	75.48%	24.52%	NA

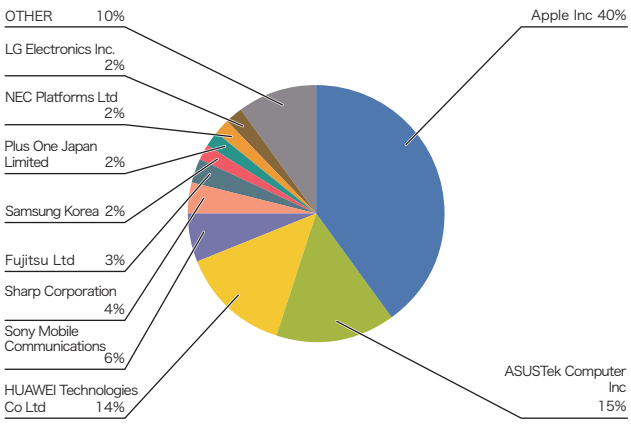


図-15 端末種別

Theme 05

IIJインフラ(バックボーン)

IIJではIIJのネットワークを適切に運用するために、ネットワークの状態を様々な視点から観察しています。今回は、その中でも主要な指標である総トラフィックについて紹介します。

IIJはISPですが、ISPの規模を表す数値として、総トラフィックという指標が用いられることがあります。しかし、この総トラフィックが何を表しているのか明確に説明されている例をあまり見ません。ここでは総トラフィックを「IIJのバックボーンに出入りする通信の帯域の合計」と定義します。ここで言うバックボーンは、ルータの集合です。通信元/通信先となるホストは含みません。一部ルータ宛の通信がないわけではありませんが、無視しても良いような量でしょう。

こう定義した上で、IIJのバックボーンの出口/入口を考えてみます。主に次の3種類に分類できます。

1. IIJの接続サービスのお客様
   - インターネット接続サービス、データセンター接続サービスなどの接続サービス
   - IIJ GIO(クラウドサービス)のインターネット接続サービス
   - ブロードバンド(NTT東西のフレッツなど)接続サービス
   - モバイル接続サービス
2. IIJのサービスホスト
   - メールやWeb関係のサービス
   - 配信サービス
3. 相互接続事業
   - 他のISPとの相互接続(ピア)
   - クラウド事業者/コンテンツ事業者との相互接続

これに基づいて、この10年の総トラフィックをグラフ化すると図-16のようになります。グラフは積み重ねになっています。外向きというのが出口を観測したもの、内向きというのが入口を観測したものです。一部の攻撃トラフィックなどは

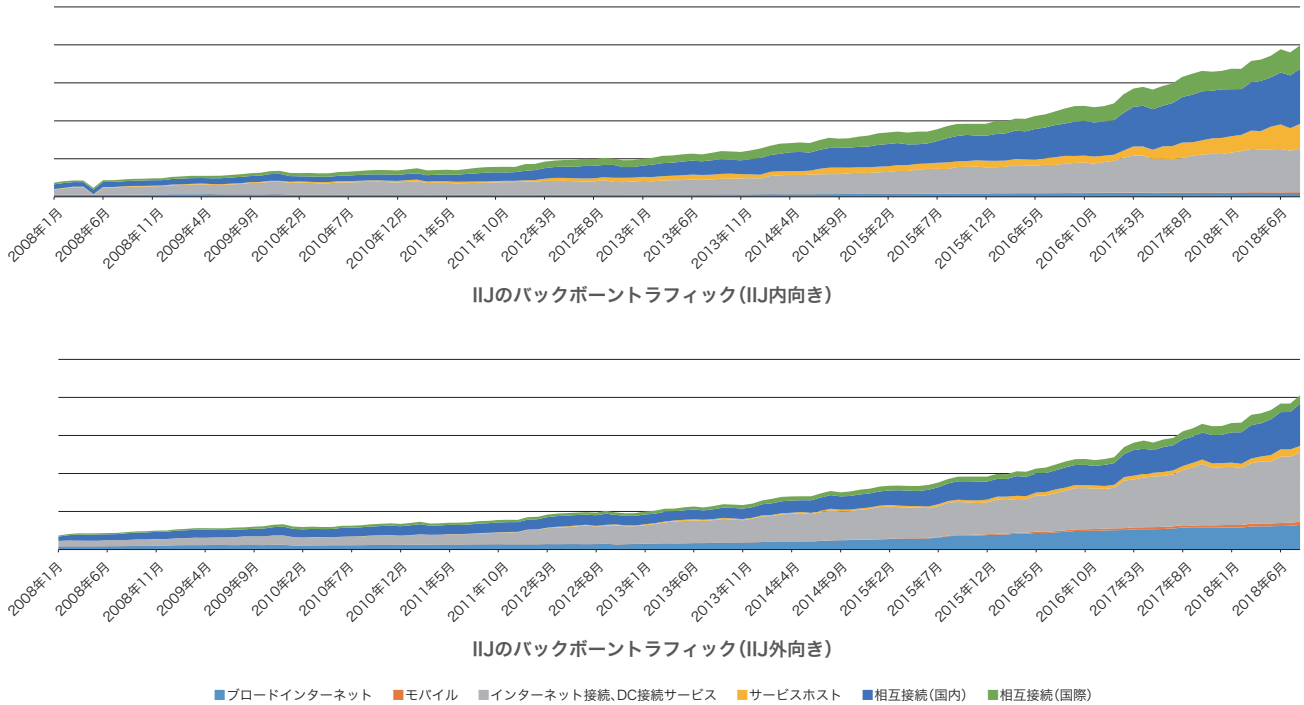


図-16 2008年～2018年の総トラフィック

バックボーンの中で破棄されることもありますが、基本的には入ってきたトラフィックはすべてどこかに出て行くので、合計はほぼ同じになります。

まず、一見して分かるのはトラフィックがこの10年で10倍以上になっていて、伸びが加速していることです。留まる気配はなさそうです。外向きのトラフィックに関しては、下の3つがお客様に向かうトラフィックです。モバイルのトラフィックが3年程前から徐々に増えてきていますが、割合的にはまだまだ少ない状況です。かなり大雑把ですが、ブロードバンドとモバイルのトラフィックは大部分が個人のお客様です。着実に増えていますが、灰色の主に法人のお客様(個人向けにサービスを行っている法人のお客様も含まれます)のトラフィックの方がこの10年の伸び率は高いです。IIJのお客様のトラフィックに関しては、個人よりも法人の方が伸びているのです。

内向きのトラフィックを見てみます。ブロードバンド、モバイルのトラフィックが少ない傾向です。情報を殆ど発信していないと言うことです。特にブロードバンドはトラフィックは伸びているものの、その率が小さく、全体に占める割合はどんどん低下していっています。また、サービスホストの割合が増えてきています。配信やWeb系のサービスが伸びているからでしょう。

外向きと内向きの対比に注目すると、ブロードバンドの場合は内向きが2倍程度にしかなっていないのに対して、外向きは9倍近くに達しています。1つ1つのコンテンツが巨大化していることがここからも分かります。また、対外接続に注目した場合、国内は内向きと外向きが拮抗していますが、国際は内向きの方が明らかに多くなっています。国際の相互接続に関しては、まだIIJのコンテンツの力は弱いということでしょう。

今回は、IIJの総トラフィックのグラフを紹介しました。トラフィック1つを取っても、視点や注目するポイントを変えると別の側面が見えてきます。また、トラフィック以外にもバックボーン内の遅延やエラーなど、全く別の指標も記録を取っています。これからも、IIJのネットワークの観察を続け、その変化を定期的にレポートして行ければと考えています。

執筆者:

1.BGP・経路数
倉橋 智彦(くらはし ともひこ)
IIJ サービス基盤本部 インフラ企画部

2.DNS
松崎 吉伸(まつざき よしのぶ)
IIJ サービス基盤本部 インフラ企画部

3.IPv6
佐々木 泰介(ささき たいすけ)
IIJ サービス基盤本部 ネットワーク技術部 副部長

4.モバイル
堀 高房(ほり たかふさ)
IIJ サービス基盤本部 ネットワーク技術部 ネットワーク技術課長

5.IIJインフラ(バックボーン)
篠井 隆典(ささい たかのり)
IIJ サービス基盤本部 ネットワーク技術部 バックボーン技術課長

URL文字列の深層学習による詐称サイト識別

便利なサービスがインターネットで提供されるようになった一方で、悪用される事例も増えています。複雑化、巨大化したシステムをすべて人手で見守ることは困難になっており、すでに様々な自動化の仕組みが運用されています。ここ数年、セキュリティ分野では深層学習の活用に注目が集まっています。経験と知識が重要となる分野において、深層学習による補助が実現できれば、より多くの人材が高度な運用に関わることが可能となり、結果的に安全なサービスが実現できるでしょう。本稿では、深層学習をサイバー攻撃の防御に活用する試みを紹介します。

2.1 Webの登場と詐称サイトの戦い

欧州原子核研究機構(CERN)のフェローとして活動していたTim Bernars-Leeが最初のワールドワイドウェブ(WWW)サーバ、CERN HTTPdを公開してからおよそ30年が経ちます。ハイパーテキストをインターネットで実現したこの仕組みは、同氏らによって同時期に提案されたHTTP (Hypertext Transfer Protocol)とURL (Uniform Resource Locator)との抜群の組み合わせにより、瞬く間に世界の情報を繋ぐ技術になりました。1980年代から90年代は、TCP/IPを実装したBSD UNIXが学術機関を中心に爆発的に普及した時期でもあり、世界中のコンピュータが相互に接続される土壌が育ちつつあったことも無関係ではないでしょう。更に、米国立スーパーコンピュータ応用研究所(NCSA)がGUIを備えたWebブラウザMosaicを公開したことにより、コンピュータ技術者でなくても簡単に世界の情報にアクセスできるようになります。Web技術の進化は今なお続いており、毎日どこかで新しいサービスが立ち上がっています。

あらゆる技術に共通して当てはまることですが、世界を良くすることができる技術は同時に世界を悪くすることもできます。様々なサービスがWebで提供されるようになるにつれ、それを利用した詐称行為が登場します。よく見られるのは、有名なオンラインサービスサイトや銀行サイトに似せたWebページを準備し、偽メールなどを通じて利用者を誘導、個人情報やパスワードなどを盗み取るというものです。もちろん、詐称行為自体はWeb以前から存在するものですが、迷惑メールと同様、電子化によって低コストでより多くの人を狙うことができるようになりました。情報化は、表の世界と裏の世界、分け隔てなく恩恵を与えてくれたということです。

詐称サイトへのアクセスから利用者を守ることは、近年のネットワークサービス運用者にとって重要な課題の1つです。ISPであれば、接続を提供している顧客に詐称サイトブロックなどのサービスを提供している場合も多いでしょう。もしあなたが組織の情報システム担当者なら、自組織内の利用者に対して何らかのセキュリティ対策ソフトウェアの導入を推進したりしているかもしれません。現在広く利用されている詐称サイト防御技術は、基本的にはブラックリストを用いた手法です。ただし、容易に想像できるように、単なるブラックリストでは広大なWeb空間を網羅することは困難です。研究者たちは、より効率的に悪性サイトを判別する方法を模索してきました。例えば、既存の詐称サイトのドメイン名に類似した文字列を機械的に推測して、少ないブラックリストからより多くの悪性ドメイン名の候補を作り出す試みがありました[*1]。また、単なるリストの範疇を超え、ドメイン名が登録された時期、Googleでの検索順位などを参考にし、登録されて間もないドメイン名や、順位の低いドメイン名の信頼度を低く見積もる手法などもありました[*2]。実際にアクセスされたページの内容を透過プロキシなどで解析し、サイトが悪性かどうかを判断する技術なども提案されています[*3]。更に、近年の深層学習の発展に伴い、セキュリティ分野への深層学習応用も進んできています。

*1 P. Prakash, M. Kumar, R. R. Kompella, and M. Gupta, "PhishNet: Predictive blacklisting to detect phishing attacks," in 2010 Proceedings IEEE INFOCOM, ser. INFOCOM, 2010, pp. 1–5.
*2 S. Garera, N. Provos, M. Chew, and A. D. Rubin, "A framework for detection and measurement of phishing attacks," in Proceedings of the 2007 ACM Workshop on Recurring Malcode, ser. WORM '07. New York, NY, USA: ACM, November 2007, pp. 1–8.
*3 Y. Zhang, J. I. Hong, and L. F. Cranor, "CANTINA: A content-based approach to detecting phishing web sites," in Proceedings of the 16th international conference on World Wide Web, ser. WWW '07. ACM, May 2007, pp. 639–648.

2.2 URL文字列に隠された意味

詐称サイトとの戦いに終わりはありません。何らかの防御技術が考え出されれば、それを回避する仕組みが生み出されていきます。それでも、より安全なインターネットの利用のため、新しい防御技術を検討していくことが重要です。

詐称サイトの判定率でいえば、実際にアクセス先のコンテンツを確認して判断するプロキシ型のものが有利です。ただし、実サイトへアクセスするという行為は危険な場合もあります。処理負荷やプライバシーなどの課題もあり、実際のコンテンツへアクセスしない手法も多く提案されています。最も単純な手法が、URLそのものだけを見て判断する方法です。この場合、URLを構成する文字列に詐称サイトか否かを判断するための何らかの意味が含まれているのかどうかが問題となります。

この疑問に対する正確な答えを持っている人はいません。ただ、過去の研究を調べてみると、意味があると考えた人もいたことが分かります。例えば、よく知られた考え方の1つとして、ドメイン名は発音可能な文字列である、というものがあります。ドメイン名は何か現実の物やサービスに関連したものであることが多いため、自然言語や名称を元にした文字列が多く、必然的に人間が発音できるものになりやすいというものです。マルウェアの中には、機械的に生成されたドメイン名(Domain Generation Algorithm、DGA)を利用しているものもあり、多くの場合これらの名前は発音不可能な文字列で構成されることになります。この区別ができれば、通常のアクセスと疑わしいアクセスを区別できるのではないかという考え方です。

また、異常に多いサブドメイン(たくさんのドットが含まれているホスト名)や、異常に深いパス(たくさんのスラッシュが含まれるURL)が使われる場合は悪性の場合が多いという考え方もあります。経験則に基づいた様々な条件を検討し、それらの組み合わせを用いて悪性かどうかを判断するのが、この分野では一般的な手法です。

そしてその最前線に位置する技術として、深層学習を活用したURL判定技術が検討されています。

2.3 深層学習の復活

深層学習が一般にも注目されるようになったのは5〜6年程前でしょうか。深層学習で使われるニューラルネットワーク自体は古典的といっても良いくらい昔からある考え方です。ただ、多層のニューラルネットワークを用いる深層学習の仕組みは、その計算量の多さや、適切に学習させることの技術的困難さから、長らく実用化が困難であると考えられてきました。ところが、2010年代に入ると画像認識の分野で目覚ましい成果を挙げる手法が考案され、一躍注目を浴びるようになります。諸説あると思いますが、2012年に開催された大規模画像認識競技会(ILSVRC、ImageNet Large Scale Visual Recognition Challenge)でAlex Krizhevskyらによって実証された深層学習を用いた画像認識システム[*4]が、今に通じる深層学習の流れの始まりとみなされることが多いようです。それまで25%程度だった誤り率を一気に10%も向上させ、深層学習が現実的な場面に応用できる可能性を示したのです。以降、主に画像や音声認識の分野で広く深層学習が使われるようになり、言語の翻訳、文書の分類、果ては囲碁に至るまで様々な分野に応用されていきました。

ネットワークについても、主にセキュリティ分野で深層学習を用いた技術が次々と提案されている状態です。この記事では、私たちが提案するURL文字列から詐称サイトを判定する手法[*5]を紹介しますが、当然この提案が世界初の試みというわけではあ

*4 A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," Advances in neural information processing systems, 2012.
*5 K. Shima, D. Miyamoto, H. Abe, T. Ishihara, K. Okada, and Y. Sekiya, "Classification of URL bitstreams using Bag of Bytes," in Proceedings of First International Workshop on Network Intelligence(NI2018), 2018.

りませんし、またこれからもたくさんの研究者・技術者がより良い方法を提案していくことになると思います。ネットワーク、特にインターネットのような自律分散環境では、永久に動作する何かを作り出すことは困難です。時代と共にシステムもデータも変遷していき、そのすべての情報を把握することは不可能です。私たちは常に世界の一部しか見えておらず、見えている情報ですら瞬く間に古くなっていくからです。

深層学習は万能の仕組みというわけではありません。巷でいわれているような人間を超える知能がそこから生まれるのかどうか、まだ私たちには分かりませんが、今できることは分かっています。

深層学習は機械学習の一手法であり、ある入力ベクトルに対して、一定の演算を行い、別のベクトルを出力します。これが分類問題や識別問題に使われることになります。画像認識の例でいえば、猫の画像（をベクトルの形に変換したもの）を入力して、それが猫かどうかを0/1で出力するなどです。「一定の演算」の内容を決めるため、深層学習では大量のデータを必要とします。猫の例でいえば、大量の猫の画像と、猫以外の画像などです。これらは学習データと呼ばれ、あらかじめ答えが分かっているものを使う場合を教師あり学習、そうでない場合を教師なし学習と呼びます（その中間もあります）。深層学習は、こういった分類問題で大きな成果を収めています。

2.4 URLのベクトル化

さて、いよいよURLの分類の話に進んでいきたいと思います。目的は、与えられたURLが問題のない通常のサイトなのか、詐称サイトなのかを判定することです。深層学習の手法を利用するため、まずはURLを深層学習の入力に利用できるベクトルの形に変換しなければなりません。

深層学習以前の機械学習では、このベクトル定義（特徴量の定義）が重要な工程でした。対象データを区別するために必要十分な情報を如何に事前に定義できるかが性能に大きく影響するためです。先にも述べたとおり、URL分類では、発音可能かどうか、ドットやスラッシュの数、アルファベット、記号、数字の比率、文字の出現場所、n-gram文字列の出現頻度など、様々な要素がURLを区別する特徴として検討され、検証されてきました。やみくもに特徴量を増やしてしまうと計算時間に影響してくるため、従来の機械学習の手法では対象データの深い知識を持った専門家が、既存のデータをあの手この手で解析しながら役に立ちそうな特徴を厳選していました。

これに対し、深層学習では、大量のデータを用いて学習させることによって、自分で特徴量を見つけてくれるといわれています。実際にはそう単純ではなく、注意深いデータの前処理が最終的な結果に影響してくることも多いと思いますが、特徴量定義の負担をある程度物量でカバーしてくれることも事実でしょう。

今回、URLを分類するにあたり、既存の特徴量は使わないこととします。その代わり、単純な変換処理を定義してURL文字列を固定長のベクトルに変換します。確かに、URLの分類に関しては先人の知恵を活用することもできたと思いますが、今後他のデータセットを対象としていく場合、常に有用な特徴量が定義できるとは限りません。もし、単純な前処理と大量の学習データでURLの識別が可能であると分かれば、他のデータセットでも同様の戦略を取ることができるかもしれないという淡い目論見もあります。

今回私たちが用いたベクトル化の手順は次のようになります。

1. URLを文字単位に分割する
2. 各文字をASCIIコードの16進表記に変換する
3. ホスト部、パス部それぞれの先頭から1バイトずつ、4ビットずつシフトしながら、出現する値を列挙する
4. ホスト部、パス部それぞれに出現した値（0x00から0xFF）の個数を数え、256次元のベクトルにする
5. ホスト部、パス部から計算された256次元のベクトルを連結し、512次元のベクトルにする
6. ベクトルを正規化する

手順1から3を図-1に示します。続く手順4で値の個数を数えます。図-1に示した例では、ホスト部の値は次の通りです。

0x16(1個)、0x2E(3個)、0x42(1個)、0x61(1個)、0x64(1個)、0x69(2個)、0x6A(2個)、0x70(1個)、0x72(1個)、0x77(5個)、0x96(2個)、0xA2(1個)、0xA7(1個)、0xE6(3個)

ホスト部のベクトルをVとし、次元iの値をv_i(i:出現した値)とすると、$v_{0x16} = 1$、$v_{0x2E} = 3$、$v_{0x42} = 1$、...、$v_{0xE6} = 3$となります。出現しなかった次元の値は0です。元のURLが何であれ、URLの長さがいくつであれ、必ず512次元のベクトルに変換することができます。ただし、このままではURL文字列が長くなるとベクトルのサイズが増大してしまうため、手順6で正規化しておきます。こうして変換した512次元のベクトルを、「URL特徴ベクトル」と定義します。

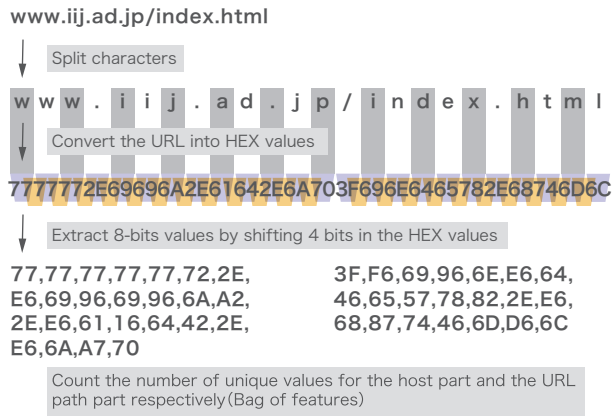


図-1 URLのベクトル化

2.5 ニューラルネットワーク設計

URLを固定長のベクトルに変換する準備は整いました。次は、そのURL特徴ベクトルをどう学習させるのかを決めなければなりません。今回の試みでは、シンプルな3層のニューラルネットワークを用いました。深層学習というにはいささか浅いネットワークですが、この種の手法に効果があるのかどうかを確認するためには十分だと考えます。

図-2に今回利用したニューラルネットワークのトポロジを示します。このトポロジをどこかで見たことがある方もいるかもしれません。この3層全結合トポロジは、株式会社Preferred Networksが開発しているオープンソース深層学習ライブラリChainer(https://chainer.org/)のサンプルとして登場し、MNISTデータセット(http://yann.lecun.com/exdb/mnist/)

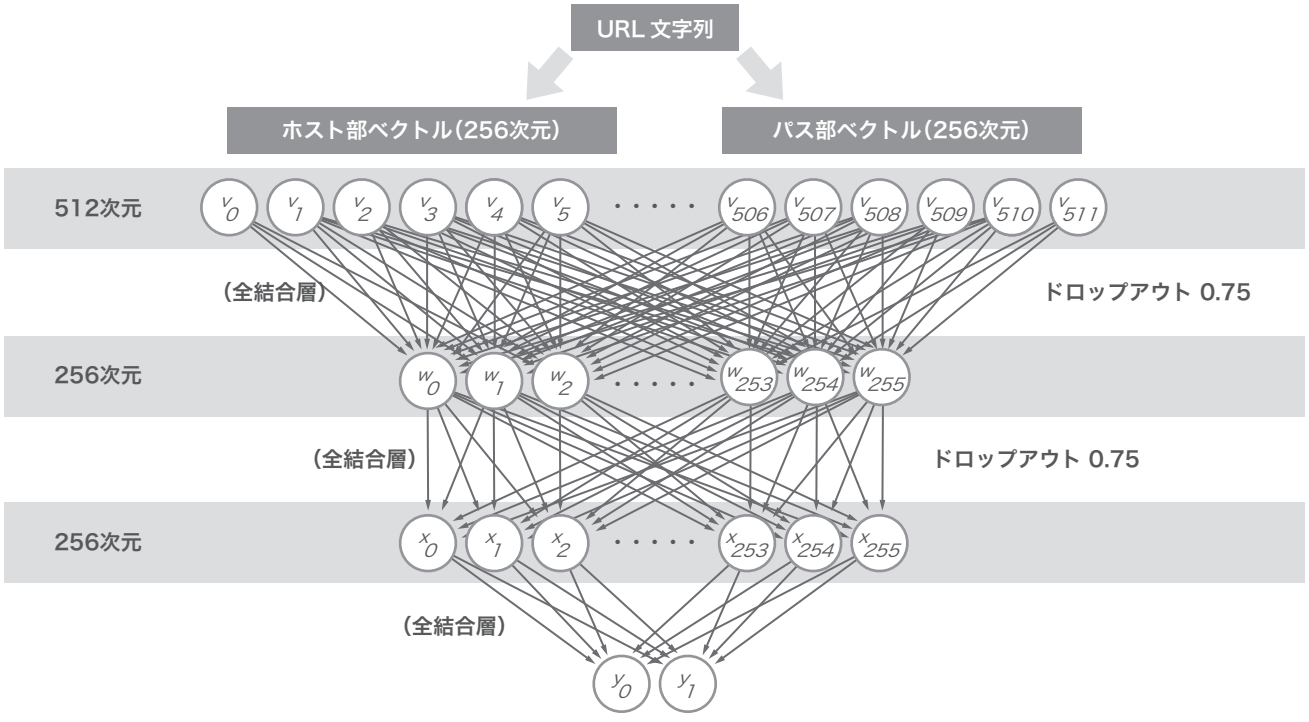


図-2 ニューラルネットワークトポロジ

を利用した手書き数字の認識モデルとして使われています。これを元に、次の2つの変更を加えました。

1. 入出力次元数：MNISTサンプルの場合、入力画像の縦横サイズが28x28なので、784次元の入力、出力が0から9までの数字なので10次元の出力となっていました。今回は、入力が512次元のURL特徴ベクトル、出力はURLが詐称サイトかどうかを示す0か1の2次元に設定しています。
2. ドロップアウト率：MNISTサンプルでは過学習を抑えるための仕組みであるドロップアウトを利用していませんが、今回のデータに関しては激しい過学習が観測されたため、高めのドロップアウトを設定しています。

今回は、提案手法の検証にもChainerを用いています。Chainerで定義したニューラルネットワークモデルを表-1に示します。

2.6 データソースの選定

データ構造とニューラルネットワークモデルが揃ったので、実際のデータを使って検証してみます。インターネットのようなダイナミックな環境では次の2つが大きな課題になります。

1. データの正確性：MNISTのようなデータは、すべてのデータが事前に検証され、あらかじめ正しいラベル（MNISTの場合だと、手書きの数字画像と、その画像が表す数字の値）が準備されています。ところが、インターネット上で観測・収集されるデータに正確にラベルを付けることは困難です。もし、間違った情報で学習を進めてしまえば、当然間違った答えを推測するモデルが育ってしまいます。
2. 網羅性：学習に使うデータが真に一般的なデータなのかどうかを示すことはできません。偏ったデータで学習してしまうと、それ以外のパターンが出現したときに対応できなくなります。これは手書き数字認識などでも同じことがいえるのですが、0から9までの数字という、ある程度問題が限定された場合と、インターネット上のURL文字列のような無限に広がる空間では、自ずと対応できる範囲に差が出てしまいます。

こういった問題があることを前提としつつ、なるべく正確な、網羅性の高いデータを準備することが大切です。今回、詐称サイトのデータとしてPhishTank.com（https://www.phishtank.com/）に登録されているアクティブな詐称サイトのデータを利用します。全世界すべての詐称サイトが登録されているわけ

```
from chainer import Chain
import chainer.functions as F
import chainer.links as L
class Model(Chain):
    def __init__(self):
        super(Model, self).__init__()
        with self.init_scope():
            self.l1 = L.Linear(None, 256)
            self.l2 = L.Linear(None, 256)
            self.l3 = L.Linear(None, 2)
    def __call__(self, x):
        h1 = F.dropout(F.relu(self.l1(x)),
                       ratio=0.75)
        h2 = F.dropout(F.relu(self.l2(h1)),
                       ratio=0.75)
        y = self.l3(h2)
        return y
```

表-1 Chainerによるニューラルネットワークモデル

ではないため、網羅性は保証できませんが、詐称サイトかどうかの判断は人の目による投票ベースの処理が入るためある程度信頼できます。より難しいのは「詐称サイトではない」通常のサイトのデータです。検証では、ある研究組織のアクセスログから、前述のPhishTankに登録されたものを取り除いたものを詐称サイトではないURLと定義して利用していますが、より網羅性を高めるためには異なる種類のアクセスログでの追試が必要になるでしょう。

2.7 深層学習の適用可能性

前節で準備した2種類のデータソースから、それぞれおよそ26,000個ずつ、ランダムにURLを抜き出します。このうち80%を学習に使いました。残った20%で分類精度(Accuracy)を確かめたところ、94%のデータに対して正しく詐称URLとそうでない通常のURLを区別することができました。この結果が良いのか悪いのか、意見の分かれるところだと思います。過去に提案されている分類手法では、この値よりも良い値を実現するものもあります。それらの手法は、単なる文字列だけではなく、他の情報(例えばWhoisの情報やGoogleの検索順位の情報など)を用いている場合もあるので単純な比較はできません。また、URL文字列のみを用い、私たちと同様に深層学習を活用した試みもあり[*6]、こちらも、今回の私たちの結果よりも高い分類精度を実現しています。ただ、彼らの提案したニューラルネットワークモデルを独自に実装し、私たちのデータセットを用いて追試してみたところ、論文で示されているような高い値を出すことはできませんでした。学習に用いたデータセットによって、同じニューラルネットワークモデルでも精度に大きく差が出るということです。

全世界すべてのデータを入手できない以上、ある程度の偏りのある学習になってしまうことは避けられません。最近ではビッグデータという言葉を聞かなくなりましたが、広範囲のデータを大量に持っている組織が有利になる状況は深層学習の世界でも継続、むしろ以前よりもその差が拡大するのではないかと思います。

2.8 まとめ

本稿では、詐称URLの判断に深層学習を応用する試みを紹介しました。簡単なニューラルネットワークを用いた検証だったにもかかわらず、94%の精度でURLの分類が可能となりました。同時に、データ収集の困難さ、データを持つことの強みについても再確認できました。

ネットワークデータへの深層学習応用はこれからどんどん進歩していくと思います。コンピュータの能力も向上し、比較的簡単に深層学習を利用することもできるようになりました。今後も新しい技術を取り込みつつ、より安全なインターネットの実現を目指していきたいと思います。

《 謝辞 》
本研究は、JST、CREST、JPMJCR1783の支援を受けたものです。

執筆者:
島 慶一(しま けいいち)
IIJ 技術研究所 主幹研究員。

*6 J. Saxe and K. Berlin, "eXpose: A character-level convolutional neural network with embeddings for detecting malicious URLs, file paths and registry keys," CoRR, vol. abs/1702.08568, February 2017.

海底ケーブルとインターネットの信頼性

IIJ技術研究所では計測や解析を通じてグローバルなインターネットの信頼性向上に貢献する研究を行っています。本稿では、インターネットを支える海底ケーブルを理解することで、信頼性の向上を目指す研究について報告します。なお本稿は、ACM HotNet2018で発表した論文の要約です[*1]。

3.1 はじめに

インターネットにおける国際データ通信の99%は海底ケーブルによって運ばれています[*2]。19世紀半ばから敷設が始まった海底ケーブルは指数関数的な勢いで総容量が増えており、今日では総長100万キロメートル[*3]を超え、数百本のケーブルからなる複雑な網目構造が、世界のほぼすべての地域を結んでいます(図-1)。この中には、大手事業者のグローバルサービスの大容量運用バックボーンに加え、陸上接続の乏しい地域への接続を確保するためのケーブルがあります[*4][*5]。

海底ケーブルは、これだけ大規模かつ重要であるにもかかわらず、既存研究では特定の回線障害に着目されたりブラックボックス扱いされたりしており、グローバル・インターネットにおける役割があまり理解されていません。

本稿では、海底ケーブルに関する公開情報から海底ネットワークの成長と現状を明らかにし、海底ケーブルの障害によるネットワークへの影響について、各種の観測データをもとに考察する手法を提案します。

3.2 海底ケーブルをとりまく状況

最初の商用の海底ケーブルは1850年に英国海峡に敷設されました。初期のケーブルは、電話用の撚り銅線でした。光ファイバーケーブルは1980年代に開発され、1888年に大西洋横断ケーブル(TAT-8)で初めて稼動しました。今日ではほぼすべてのケーブルが光ファイバーとなっています。現在の光ファイバーは、水深に応じて、銅チューブ、アルミ防水材、撚り線シールド、ポリエチレンシールドなどを多層に巻いて保護されています(図-2)。ケーブルの種類は、直径約10cm、重さ約40t/kmの浅海ケーブルから、直径約2cm、重さは約1.5t/kmの深海ケーブルまで様々なものがあります。

ほとんどの海底ケーブルは、共同事業として構築、管理され、複数の通信会社によって共有されています。例えば、先述のTAT-8には、AT & T、ブリティッシュ・テレコム、フランス・テレ

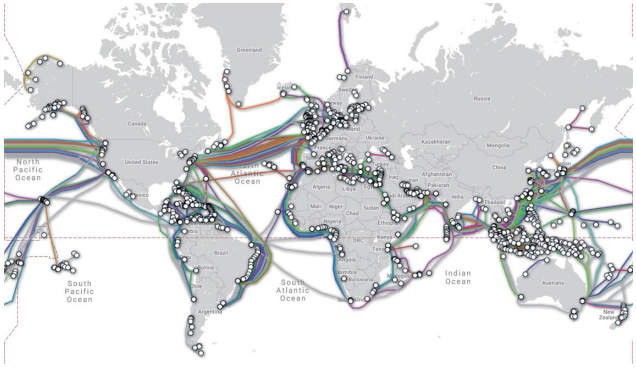


図-1 TeleGeograpyによる海底ケーブル図(2018年6月)[*6]

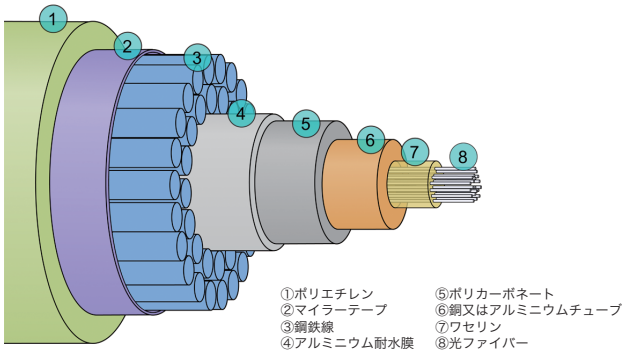


図-2 多層に保護された海底ケーブルの断面

*1 Zachary S. Bischof and Romain Fontugne, Fabian E. Bustamante. Untangling the world-wide mesh of undersea cables. In Proc of HotNet, November 2018.
*2 P. Edwards. A map of all the underwater cables that connect the Internet, 2015(https://bit.ly/2Ep19i4)。
*3 The various threats to subsea cables.Ultramap(https://bit.ly/2Ld9LKW)。
*4 NEC begins construction of submarine cable links to the islands of Palau, Yap and Chuuk. NEC, May 2017(https://bit.ly/2JqQQaE)。
*5 Z. S. Bischof, J. P. Rula, and F. E. Bustamante. In and out of Cuba: Characterizing Cuba's connectivity. In Proc. of IMC, October 2015.
*6 TeleGeography.Submarine cable map(https://www. submarinecablemap.com/)。

コムなど当時の大手国際通信事業者をはじめとする35社が関わっていました[*7]。最近の敷設ブームは、GoogleやFacebook、Microsoft、Amazonなどのコンテンツ事業者が牽引しているようです。Telegeographyによれば、コンテンツ事業者が配備した容量は、2013年から2017年で10倍に増加し、他のすべての顧客の増加率を上回っています[*8]。

3.2.1 海底ケーブルに関わる問題

海底ケーブルの全長が急速に拡大し続けるにつれて、ケーブル問題に起因するネットワークトラブルの可能性も増えています。地震や津波などの大規模災害をはじめ、海底の地滑りや海流による岩盤擦れ、サメによる被害など、自然環境に起因する潜在的なリスクが数多くあります。

また自然の力以上に、意図的であるか否かを問わず、人間の行動はケーブルに対する最大の脅威です。ケーブル破壊の約70%は漁業用トロール網や船舶の錨によって引き起こされている[*3]ほか、脆弱なケーブルに対する意図的な攻撃に対する懸念も高まっています。例えば、米海軍関係者は、重要な海底ケーブル付近でロシアの潜水艦やスパイ船を観測することに懸念を表明しています[*9][*10]。

海底ケーブルの障害の影響は、接続冗長性の高い地域では限定的だと思われますが、特に脆弱と思われる地域もあります[*11][*12][*13]。例えばアジア・アメリカ・ゲートウェイ・ケーブル(AAG)は、東南アジアと米国を結び、ベトナムの国際インターネットトラフィックの60%以上を扱っていますが、頻繁に故障することで有名です。2017年だけでも、AAGは少なくとも5回の障害を起こしています[*14]。

また、2013年にエジプト沖でSE-WE-ME-4海底ケーブルを切断したダイバーが逮捕された事件では、インターネットの速度が60%低下しました[*11][*15]。更に、2018年4月には1本の海底ケーブルが切断されたことにより、モーリタニアなどの国全体がオフラインとなりました[*12]。

このようなリスクを把握するには、グローバルネットワークの構成要素としての海底ネットワークの役割を明らかにする必要があります。ネットワーク層で異なるパスであるように見えるルートが、物理層では同じケーブルに依存していることもあります。

大規模通信事業者は、太平洋横断や大西洋横断などの特に重要なルートでは複数のケーブルを利用しています。しかし、レイヤー3のトポロジーの詳細を開示していても、ネットワークが物理的にどの管路や海底ケーブルで接続されているかが分からないため、第三者が特定の海底ケーブルへの依存度を知ることは困難です。

3.2.2 世界の海底ケーブル

海底ケーブルの情報は、いくつかのWebサイトで公開されています。本稿では、TeleGeograpyの海底ケーブルマップ[*6]とGreg(Mahlknecth)のケーブルマップ[*16]の2つのサイトから収集したデータを用いて、ケーブルの数や容量の観点から海底ネットワークインフラの成長と現状を見ていきます。どちらのサイトも、数百本の海底ケーブルのグローバルマップを各ケーブルの詳細と共に公開しています。重なりも多くありますが、片方にしかない情報もあり、TeleGeogaphyのマップにはGregのマップよりもかなり多くのケーブル情報が含まれています。

*7 N. Starosielski. The Undersea Network. Duke University Press.
*8 A. Mauldin. A complete list of content providers' submarine cable holdings.
*9 M. Birnbaum. Russian submarines are prowling around vital undersea cables. it's making NATO nervous. The Washington Post, December 2017(https://wapo.st/2NW71QP)。
*10 D. E. Sanger and E. Schmitt. Russian ships near data cables are too close for US comfort. The New York Times, October 2015(https://nyti.ms/2uqCnXh)。
*11 C. Arthur. Undersea internet cables off Egypt disrupted as navy arrests three. The Guardian, March 2013(https://bit.ly/2mlluZK)。
*12 C. Baynes. Entire country taken offline for two days after undersea Internet cable cut. Independent, April 2018(https://ind.pn/2L0zlOn)。
*13 R. Noordally, X. Nicolay, P. Anelli, R. Lorion, and P. U. Tournoux. Analysis of Internet latency: The Reunion Islan case. In Proc. of AINTEC, 2016.
*14 B. Anh. Vietnam Internet returns to normal after AAG repairs. Submarine Telecom Forum, June 2018.
*15 A. Chang. Why undersea Internet cables are more vulnerable than you think. Wired, April 2013(https://bit.ly/2KYFP5Y)。
*16 G. Mahlknecht. Greg's cable map(https://www.cablemap.info/)。

注意すべき点は、どちらのマップも公表されたケーブルに関する詳細のみを掲載していることです[*17]。TeleGeographyによると、2018年初めまでに世界で約448本の海底ケーブルがサービスを提供しており[*18]、その90%が公表されているということです。残りの民間所有の非公開のケーブルの大部分は、データセンター間ネットワークの一部として海底ケーブルに多大な投資を行った、FacebookやGoogleなどのコンテンツ事業者ネットワークです[*17]。本稿では、パブリックなインターネットを支えている海底ケーブルを取り上げていますが、パブリックとプライベートの関係については今後の研究課題です。

各サイトは、ケーブルの名前、所有者、陸揚げ地点、ケーブル長、開通日などを公開しています。いくつかのケーブルについては、外部Webサイトへのリンクを提供しています。図-3は、Telegeographyで公開されている情報の一例で、ケーブル長、所有者、陸揚げ地点などが示されています。

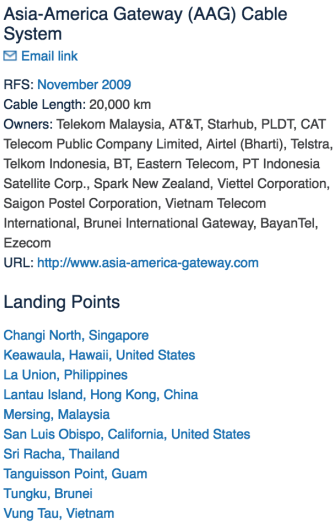
3.2.3 ネットワークの成長と現状

海底ケーブルネットワークの数は、1980年代後半以降、一定して増加しています。図-4は、TeleGeographyサイトから収集したデータを用いて、開通日をもとに現在利用されているケーブル数をグラフにしたものです（2020年までに運用開始を計画中のケーブルを含みます）。図-4（左軸）が示すように、過去30年間にわたって平均すると毎月1本新しいケーブルがサービスを開始しています。このデータには廃止されたケーブルは含まれません。例えば、TAT-8（1988年に敷設された）は、TATシリーズの最初の海底ケーブルですが、2002年に廃止され、現在のTeleGeographyのデータには含まれていません。後続のTAT-14は2001年に運用を開始しました。従って、図-4のグラフは、少なくともこれ以上のケーブルが運用されているという数を示しています。

海底ネットワークは、ケーブルの数だけでなく、これらの総ケーブル長においても増加しています。図-4（右軸）は、各年において運用中のケーブルの総延長（右軸）を示しています。2018年に運用中の総ケーブル長は、120万kmを超えています。

グラフからは、総ケーブル長は2015年頃から急に増えていることが読み取れます。それより伸びが速い1997〜2001年は、ドットコム・ブームの時期に当たります。

今日、グローバルな海底ネットワークには、1Pbpsを超える帯域があり、この数十年間で総容量が数桁増加しています。Gregのケーブルマップで公開されている帯域の情報から、海底ケーブルの全帯域幅の増加を示したものが図-5です。図-4のグラフと比較してみると、最近敷設されたケーブルがイン


Asia-America Gateway (AAG) Cable System

Email link

RFS: November 2009
Cable Length: 20,000 km
Owners: Telekom Malaysia, AT&T, Starhub, PLDT, CAT Telecom Public Company Limited, Airtel (Bharti), Telstra, Telkom Indonesia, BT, Eastern Telecom, PT Indonesia Satellite Corp., Spark New Zealand, Viettel Corporation, Saigon Postel Corporation, Vietnam Telecom International, Brunei International Gateway, BayanTel, Ezecom
URL: http://www.asia-america-gateway.com

Landing Points

Changi North, Singapore
Keawaula, Hawaii, United States
La Union, Philippines
Lantau Island, Hong Kong, China
Mersing, Malaysia
San Luis Obispo, California, United States
Sri Racha, Thailand
Tanguisson Point, Guam
Tungku, Brunei
Vung Tau, Vietnam

図-3 TeleGeographyのデータ例

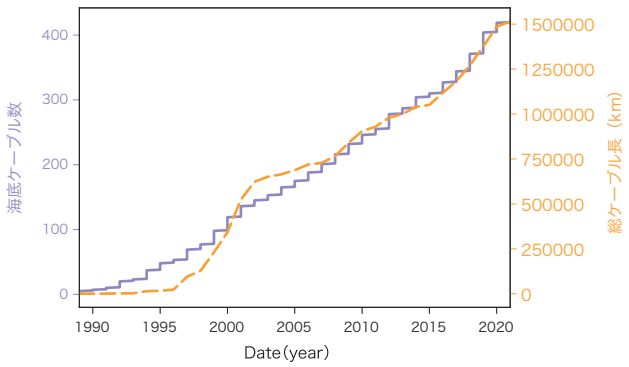


図-4 ケーブル数と総ケーブル長の変化

*17 A.Mauldin. A complete list of content providers' submarine cable holdings. Telegeography blog, November 2017（https://bit.ly/2Lw7DLm）。
*18 Telegeography. Submarine cable 101（https://bit.ly/2qcGSTc）。

ターネットトラフィックの大部分を運んでいることが分かります。図-5と図-4から新設ケーブルの平均容量の変化を示したものが図-6です。1990年代の値にはノイズがありますが、おおよそ2015年までにケーブルの平均容量は2～3桁増加していることが分かります。1995年から2010年にかけてはあまり増えていませんが、近年になって急増しています。

これらのデータは、廃止されたケーブルを含んでおらず、またデータは公表されているものに限るため、あくまで推定下限値です。

3.3 海底ケーブルとインターネット

ここからは、これらの海底ケーブルとインターネットとの関係について考察していきます。ここでの課題を、(1)海底ケーブルネットワークの接続グラフを作成し、ケーブルの切断などによって影響を受けやすい地域を特定する、(2)物理レイヤーとネットワークレイヤーを関連づけるために、通信がどの海底ケーブルを通って行われているかを推測する、(3)海底ケーブル障害がインターネットユーザに及ぼす影響を調査する、の3つに設定します。

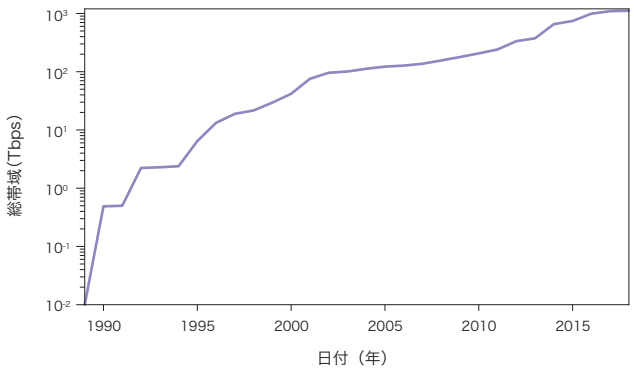


図-5 運用中のケーブルの総帯域の変化(Gregケーブルマップより)

図-6 新設ケーブルの平均容量の変化(Gregケーブルマップより)

3.3.1 海底ケーブル接続グラフの作成

第1の研究課題である海底ケーブルネットワークの接続グラフ作成は、一見簡単そうですが、異なる国や地域の陸揚げ地点を結ぶ多様なケーブルを1つのグラフに表すのは容易な作業ではありません。

簡素化のため、陸上ネットワークで繋がっている近接地区はグループ化して1つのノードとして扱い、海底ケーブルをノード間のエッジにマップします。たとえば図-7に示すGreenland connectと呼ばれるケーブルは、カナダからグリーンランドの2ヵ所、アイスランドの1ヵ所に接続されています。この場合、グリーンランドの2か所は地上ケーブルによって接続されていると考えてグループ化し、海底ケーブルはカナダとグリーンランド、グリーンランドとアイスランドを結びます[*19]。しかし、陸続きだからと言って陸上ネットワークが存在するとは限りません。例えば、パナマとコロンビアは隣国ですが、ダリエン地峡をまたぐ交通手段はなく、よってケーブルの管路もないため、接続性の点からみるとこれらは別の地域となります。そこで我々は現在、Google MapsとOpen Street Mapの地図データを用いて、このような陸上接続性のない地域を特定しようとしています。

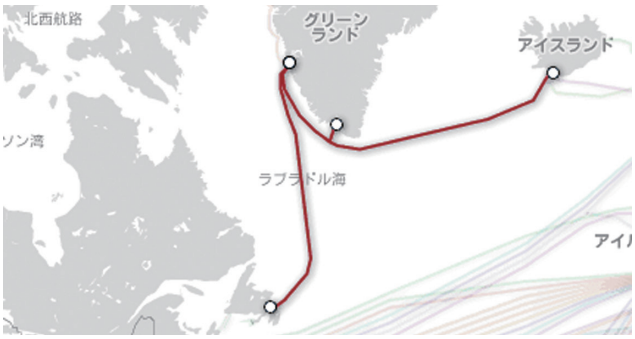


図-7 Greenland connect(Telegeograpyケーブルマップより)

*19 実際には、この「単純な」例でさえ、それほど簡単なものではありません。同じ陸上にあるにもかかわらず、グリーンランドの2つの地点をつなぐネットワークはないので、別地域であると扱う必要があります。

多数の陸揚げ地点が近接している場合は、更に難しくなります。例えば、図-8に示すACE（Africa Coast to Europe）や図-9に示すTelkom IndonesiaのJasukaを見てみましょう。グリーンランドの例とは異なり、アフリカの数十カ国とヨーロッパ大陸の2ヵ所（ポルトガルとフランス）の計22ヵ所に接続しているとあります。この場合、ヨーロッパの2点はまとめることができたとしても、西アフリカの接続点をどうまとめてよいのかは分かりません。Jasukaは更に複雑で、スマトラ島の周りの11ヵ所を接続しており、もはや陸揚げ地点の定義も明確ではありません。

我々は今後、上記のような基本的な方法を応用し、公開されている様々な情報を用いて推定した接続図の共有リポジトリを構築する計画です。このような海底ケーブルのグラフ情報は、地理的な場所と物理ケーブルとの依存関係を調査し、接続性の観点からリスクの高いリンクを特定するのに役立ちます。

3.3.2 インターネットへのマッピング

インターネットトポロジに関するほとんどの研究は、ネットワーク層での測定で行われています。ところが、ネットワーク層では別々のネットワーク経路を通っているように見えるトラフィックは、実は同じ物理リソースに依存している可能性があるので、ネットワーク層での分析から信頼性を推測することには限界があります。データセンターなどの共有設備を使っていることもありますし、海底ケーブルは複数のネットワークオペレータによって共有またはリースされています（例えばTAT-14は、30を超えるネットワークオペレータによって共有されています）。

ネットワーク層での測定とネットワークをつないでいるケーブルとの関係を理解することは、インターネットの頑健性を正確に評価する上で重要です[*20]。将来的には、通過した海底ケーブルの情報を表示する経路探索コマンドサービス（traceroute）があれば便利になるでしょう。

その実現に向けて我々は、RIPE Atlas[*21]のトポロジデータから海底ケーブル区間を特定する研究を行っています。RIPE Atlasは、RIPE NCCによるインターネット計測プロジェクトで、世界中のユーザからtracerouteなどの情報を収集しています。我々は、2018年1月から4月の間にRIPE Atlasプロジェクトによって収集された5億を超えるtracerouteデータを使

図-8 ACE（Africa Coast to Europe）（Telegeographyケーブルマップより）

図-9 Telkom Indonesia のJasuka（Telegeographyケーブルマップより）

*20 R. Durairajan, P. Barford, J. Sommers, and W. Willinger. Intertubes: A study of the US long-haul fiber-optic infrastructure. In Proc. of ACM SIGCOMM, August 2015.
*21 RIPE NCC. RIPE atlas（http://atlas.ripe.net）。

用し、我々が開発した区間RTT推計手法を用いて各経路でのルータ間の遅延を推定しました[*22]。ここでは、traceroute内の隣接ルータのIPアドレスの組の区間RTTを統計的な手法を用いて推定します。個別のRTTデータには大きなバラつきがありますが、大量のデータを統計処理することで精度を上げることが可能です。

次に、RIPEの地理位置情報サービス[*23]を使用して、各ルータのIPアドレスのおおよその位置を取得します。位置が特定できたIPアドレスの組に対し、地理的距離と区間RTTを比較することで、海底ケーブルを利用している可能性を調べます。具体的には、IPアドレスの組が特定の海底ケーブルを通過すると仮定して、陸揚げ地点を経由した距離を計算します。この値を区間RTTと光の伝搬速度から求めた距離と比較することで、その海底ケーブルを通過している可能性を判断することができます。

取得したRIPE AtlasのデータにおいてIPの各組についてこの解析を実行した結果、海底ケーブルを通過した可能性がある3,429個のIPアドレスの組を抽出することができました。

現在のところ良好な結果を得ていますが、この方法には課題もあります。まず、一部のルータについては位置を得ることができません(例えば、正確な位置推定値を得るために必要なデータがないなど)。また、90%を超えるIPアドレスの組が、2つ以上の海底ケーブルに対応してしまいます。これは、複数の海底ケーブルが同じような地点で上陸し、設備を共有しているため、また、RTTベースの分析の精度の限界によるもので、充分に起こり得ることです。

我々は、精度向上のため、他の方法の追加に取り組んでいます。例えば、各ケーブルの利用事業者の情報を使うと、IPアドレスが属する組織(AS)が利用する可能性のあるケーブルを減らすことができるはずです。

ケーブルの識別のために我々が調査している別の方法は、サービス停止情報の利用です。海底ケーブルは、しばしば保守や故障のため、サービス停止することがあります。ケーブルのサービス停止は、多くの場合、ニュースまたは個人や研究グループのTwitterなどで報告されています。サービス停止と区間RTTの相関から関連性を特定できます。

Palmer-Felgateらは[*24]、2008年から2014年の間に1,000を超える海底ケーブルのサービス停止と復旧の情報を解析しました。解析したケーブルの可用性は最大でも99%に留まり、大多数は年間に9日以上停止していました。過去のtracerouteのデータとケーブルの停止情報を比較することによって、ケーブルの停止と同期して観測されなくなるIPアドレスの組を特定することができます。

3.3.3 ケーブル故障の影響解析

ルータのIPアドレスを特定の物理ケーブルに紐づけることで、海底ケーブルの停止がインターネットユーザに与える影響を調べることができます。

我々は、RIPE Atlasのtraceroute情報を用いて、ここ数カ月のケーブル停止の影響を調べました。その中には、東南アジアにおける最近の障害と復旧の情報があり、大きなネットワーク障害には至らなかったものの、遅延に大きな影響があったことが分かりました。

2018年5月10日のSEA-ME-WE-3ケーブルの破損について見てみます。SEA-ME-WE-3は、西オーストラリアから中東

*22 R. Fontugne, C. Pelsser, E. Aben, and R. Bush. Pinpointing delay and forwarding anomalies using large-scale traceroute measurements. In Proc. of IMC, November 2017.
*23 M. Candela. Multi-approach infrastructure geolocation. Presentation at RIPE 75, October 2017.
*24 A. Palmer-Felgate and P. Booi. How resilent is the global submarine cable network. SubOptic, 2016(https://bit.ly/2L5JHST)。

を経由して西ヨーロッパに至る世界最長のケーブルです。このケーブルが損傷すると、特定のトラフィックがより長い代替経路を通らなければならず、結果として遅延が増えます。図-10は、障害前後のオーストラリアとシンガポールの間の遅延の変化を示しています。RTTが97msから、320ms以上と3倍以上になったことが分かります。海底ケーブルの修理が完了するには数週間かかる可能性があり、この遅延の上昇は数日間続きました。

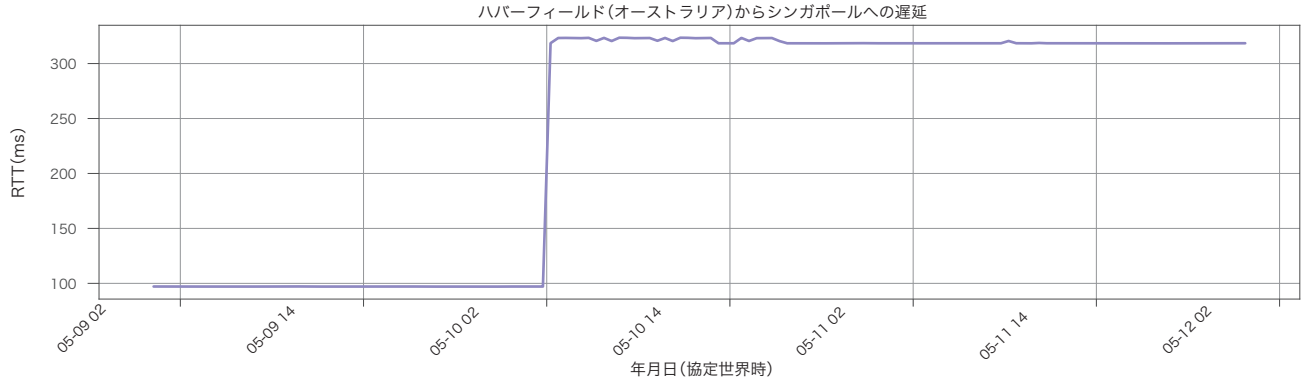


図-10 South-East Asia - Middle East - Western Europe 3(SEA-ME-WE-3)の海底ケーブル故障時のオーストラリアとシンガポールの遅延の変化(2018年5月10日)

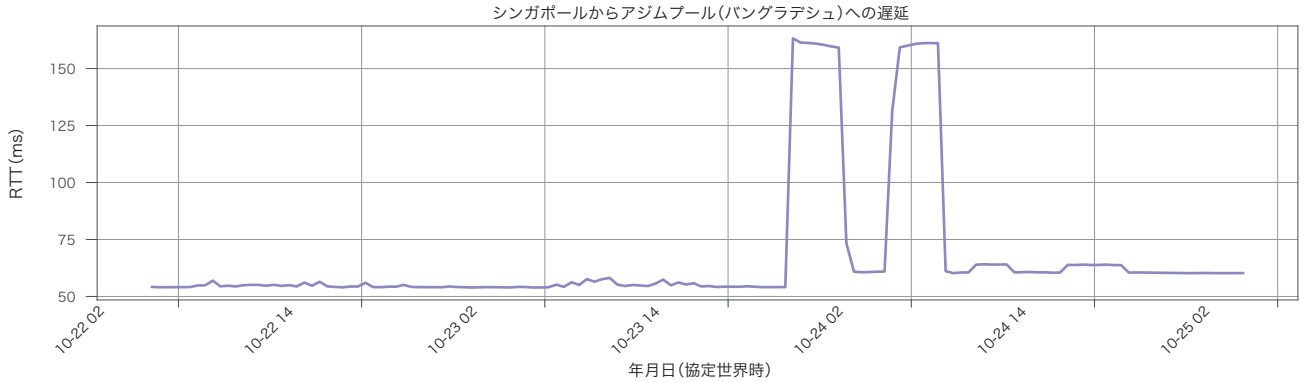


図-11 South East Asia - Middle East - Western Europe 4(SEA-ME-WE 4)のケーブル構成変更(2017年10月)

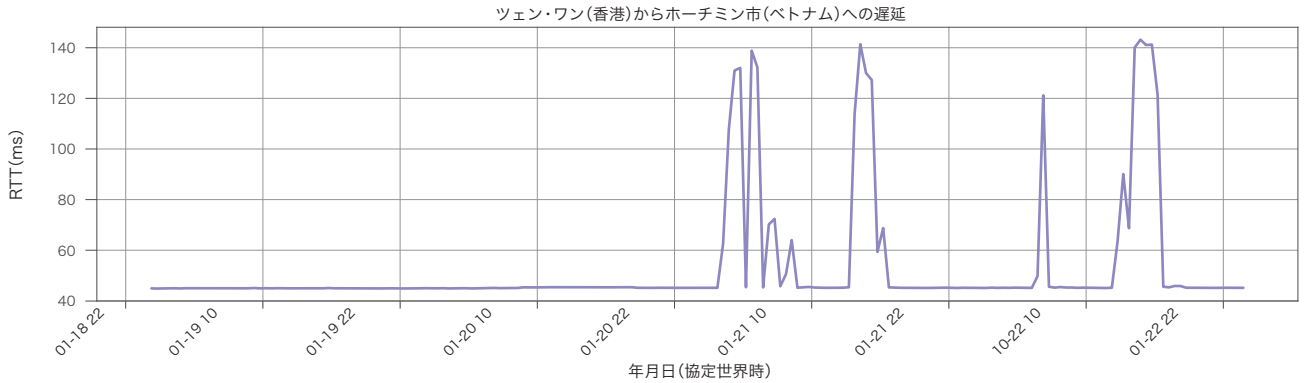


図-12 Asia-America Gateway(AAG)ケーブルの構成変更時の香港とベトナムの遅延の変化(2018年1月)

他に遅延の変化を引き起こす可能性がある原因として、海底ネットワークの設定ミスや保守があります。図-11は、SEA-ME-WE4海底ケーブルの構成変更時の遅延の増加を示しています[*25]。約12時間にわたり、シンガポールからバングラデシュへの経路で遅延がほぼ3倍になっていたことが観測されています。

同様に、2018年1月21日から始まったアジア・アメリカ・ゲートウェイ(AAG)ケーブルの構成変更では、図-12に示すように、香港とベトナムとの間の遅延への影響が観測されています。

このように、大陸をまたぐ通信のtracerouteデータを、海底ケーブルと対応づけて解析すると、遅延の急な変化の原因を探ることができます。更に、tracerouteデータからケーブルに対応する区間が消えれば、ケーブル切断またはルーティングの変化を意味します。これらの情報の相関を見ることで、性能異常の根本原因の究明につながることを期待しています。

ネットワーク運用者にとっても、海底ケーブルとIPの経路とのマッピング情報があると、ネットワークと海底ケーブルの依存関係を理解しやすくなります。この情報は、将来のネットワークインフラの拡張を計画するために重要です。例えば、信頼性を向上させるために追加する上流ISPを決める場合、異なる海底ケーブルを利用するISPを選ぶことができるようになります。

更に、tracerouteに現れるケーブルを追跡することは、特定の地域で過度に依存度の高いケーブルの発見につながります。そのようなケーブルが損傷を受けた場合、性能及びルーティングに重大な影響を及ぼすことは必至です。Durairajanらは、米国における陸上の長距離光ファイバーに対しての同様の研究を行い[*20]、高リスクのリンクを特定し、リスクと遅延の両方を低減するために特定の地域に新しいリンクを増設する提案を行っています。我々も海底ネットワークで同様の解析を行う予定です。

3.4 まとめ

仮想ネットワークの信頼性向上への取り組みは高い関心を持たれていますが、それを可能にする物理的ネットワークに対する理解はあまり進んでおらず、今後深刻な脆弱性になる可能性があります。本稿では、公開されているデータを利用して海底ネットワークの状況を調査するために、ケーブル情報とネットワーク層での測定値を組み合わせて解析する手法を提案してきました。これにより、物理的経路による接続リスクを考慮した上で、インターネットの冗長性や信頼性を推測できると考えています。

《 謝辞 》
本研究は、JSPS外国人特別研究員プログラムとNSF CNS 1619317の助成を受けています。

執筆者:
Zachary BISCHOF(ビショフ ザカリー)
IIJ イノベーションインスティテュート技術研究所 訪問研究員。
ネットワーク上の大規模な分散システムの計測に関する研究開発に従事。
DNSやトラフィックの解析を通じて、ブロードバンドネットワークの特徴を明らかにすることを目指している。

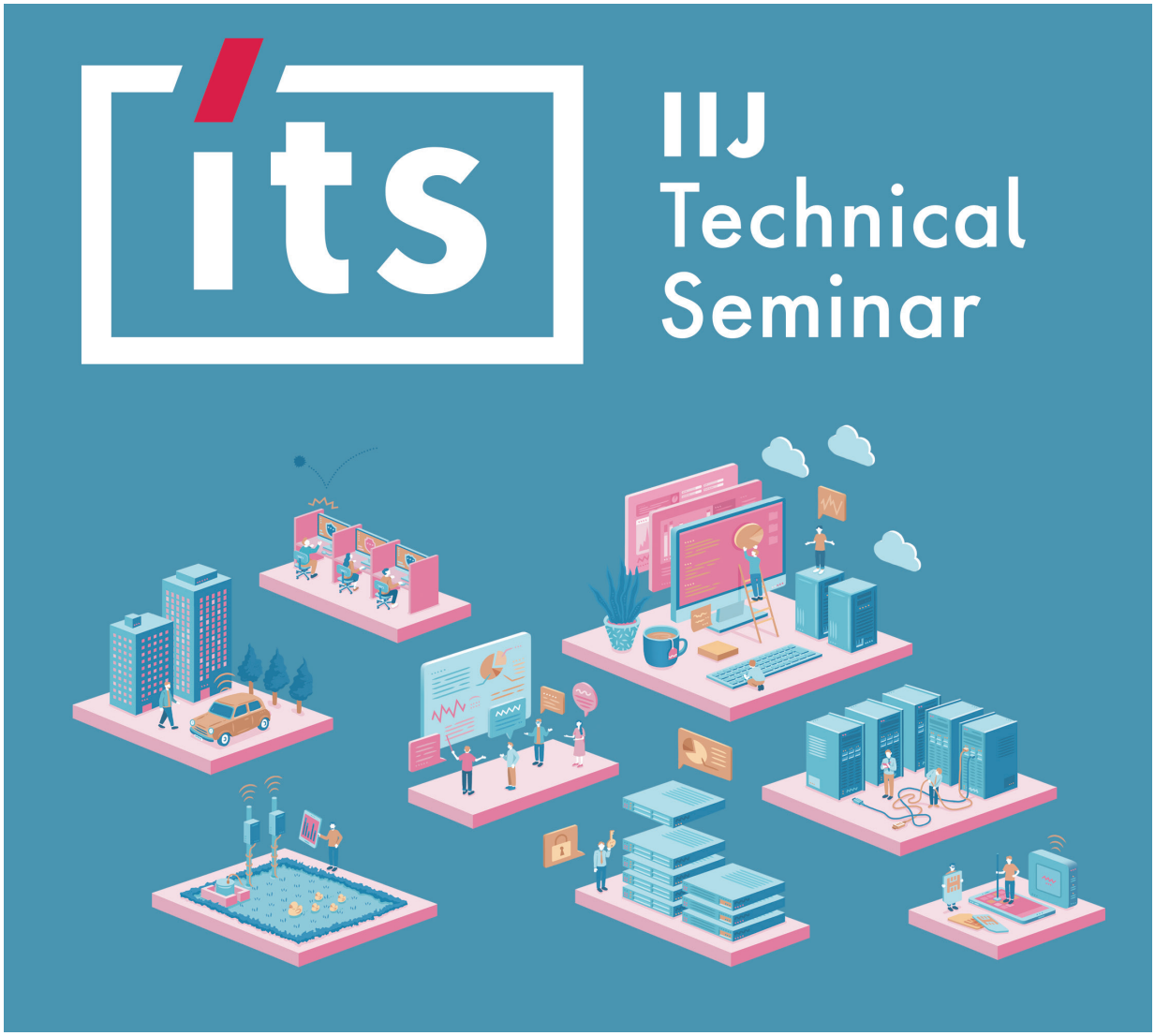
共著者:
Romain FONTUGNE(フォンテュニュ ロマン)
IIJ イノベーションインスティテュート技術研究所 主幹研究員。

Fabián E. Bustamante(バスタマンテ ファビアン)
米国ノースウェスタン大学 教授。

*25 T. D. Star. Internet to be slow for next 4 days(https://bit.ly/2LmlNSn)。

Information

IIJ Technical Seminar「its」のご案内



IIJでは、年間を通してエンジニアを対象にしたイベントを開催しています。

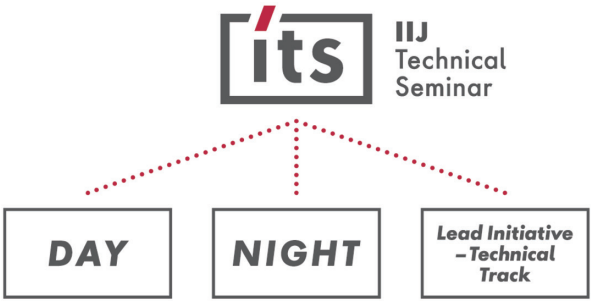
今年に入り、イベントの総称をIIJ Technical Seminar「its」と改め、去る11月22日には「IIJ Technical Seminar DAY2018」を開催しました。DAY2018は、2003年から2017年まで15年間続く老舗イベント「IIJ Technical WEEK」の後継として、昼から夜までIIJのエンジニアによる技術セッションを一日かけてお届けしました。当日は、多くのお客様に足を運んでいただき、また会場に来られないお客様にはインターネット中継にて視聴いただきました。

プログラムの内容や講演資料をはじめ、今年度実施した「its」の関連情報はIIJ Webにて紹介しています。ご興味のある方はぜひご覧ください。

■ IIJ Technical Seminar（https://www.iij.ad.jp/dev/tech/）
最新のイベントや、イベント当日のライブ配信、過去の開催一覧をご覧いただけます。

■ イベント案内を受け取る（https://iij.connpass.com/）
connpass内にありますIIJグループにメンバー登録いただきますと、イベント開催時にメールにてご案内いたします。今後、イベントへの参加をご検討の方は、ご登録をお願いいたします。

イベント紹介



■ IIJ Technical DAY：年1回、11月開催
平日の午後～夜までインターネットの技術に触れるIIJの文化祭。

さまざまなジャンルの最新動向に触れて新たな発見を持ち帰ってもらえれば幸いです。

■ IIJ Technical NIGHT：年3回程度、平日19：00開始
平日の夜、1時間1テーマでおおくりする勉強会。

勉強会の後にはビールとピザをつまみながらの交流会も。インターネット中継している回もありますので、遠方の人も。

■ Lead Initiative Technical Track：年1回、10月開催
IIJ最大級のイベント「Lead Initiative」に2018年から新設されたTechnical Track。

企業のシステム部門の方をメインに、組織におけるインターネットのお役立ち情報をお届けします。

[お問い合わせ先]　IIJ Technical Seminar 事務局：its@iij.ad.jp

December 2018 Vol.41

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。

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