

スプリンターネットを巡る 議論

中央大学

実積 寿也

日本ネットワークインフォメーションセンター
(JPNIC)

前村 昌紀

BBIX Singapore Pte Ltd

白畑 真

日経 BP

堀越 功

慶應義塾大学 SFC 研究所

小宮山 功一朗

東日本電信電話株式会社

水越 一郎

筆者らは、2022年10月に研究合宿を実施し、スプリンターネットという事象に関する議論の機会をもった。わずか一泊二日、計9時間超の議論では、明確な結論や解決策に到達することは叶わなかったものの、相互の情報交換を通じて、問題への理解を深めることができた。本稿は、合宿の成果を踏まえ、各自がそれぞれの分析・見解を個人の立場でまとめたものである。なお、論考を本稿に収録することは叶わなかったが、匿名を条件に検討に参加し、貢献した者がいたことを付言しておく。

全体の構成と概要を以下に示す。

第1節 スプリンターネットの動機と その変質についての仮説（実積 寿也）

グローバルな接続性確保を目的とするインターネットを断片化・分割しようというスプリンターネットには20年近い歴史があり、それを推進する側にも阻止する側にも一定の合理的理由が存在し得る。スプリンターネット推進側の動機は、防衛的なものから攻撃的なものへ進化しつつある。有事におけるインターネットガバナンスの在り方について早急に議論を進める必要がある。

第2節 インターネット技術コミュニティから 見たスプリンターネット（前村 昌紀）

国や企業が競合してもグローバルに単一のインターネットを保全するのがコンセンサスとインターネット技術調整団体は指摘する。インターネットは強大なネットワーク効果を生み出し企業や個人に便益を提供してきたが、一方で深刻なセキュリティ脅威やグローバル規模の寡占も引き起こした。グローバルな単一のインターネットの上で、適切な区分けを行うことが、これからのインターネット前提社会では必要だろう。

第3節 インターネットのカタチ：2022 （白畑 真）

スプリンターネットの議論の前提は「インターネット」の断片化にある。しかし、インターネットそのものの形態については必ずしも最新の認識が共有されているとはいえない。本稿では、近年のインターネットトラフィックにおけるビッグテックと呼ばれる大手OTT事業者による寡占化の実情、またインターネットを構成する主要な要素であるデータセンタ、CDN、海底ケーブルなどの面における大手OTT事業者の大

きな役割を示す。

第4節 標準化団体を舞台にした スプリンターネットの兆候（堀越 功）

国家によるインターネット統制を進めている中国やロシアなど権威主義国家は、インターネットガバナンスを、現在のマルチステークホルダー体制から国家主導のマルチラテラル体制へ移行しようと行動を続けている。中国やロシアの行動は、インターネットの分断である「スプリンターネット」を加速させる可能性がある。標準化団体を舞台にした権威主義国家と民主主義国家の対立も目立っている。これまでの経緯と今後を展望する。

第5節 インターネットは分断するか （小宮山 功一郎）

スプリンターネットの検討という本稿の課題に対して、本節は以下の2つのアプローチを試みるものである。まず、スプリンターネットが意味するところ、つまりインターネットが分断されるとはいかなる状態であるかを先行研究を手がかりに再確認する。既にサイバー空間について、デジタル冷戦（Mueller, 2013）、インターネットのヤルタ体制（Klimburg, 2013）、サイバー空間のバルカン化（Henriksen, 2019）、データローカライゼーション（須田, 2021）などと大国間のパワーゲームを連想させるキーワードを使った議論がされている。スプリンターネットはそれらと共通の問題認識に根ざしていることを明らかにする。

次に、2010年代に国家のサイバースペース観の改革、とりわけサイバー空間における国家の主権の見直しが起こっていたことを解説し、それが分断の直接的な要因であることを主張する。最後に、今後私達が実現すべきは「オープンで、グローバルなインターネット」ではなく「信頼できる、保護された、国際的な通信インフラ」ではないかという問題提起を行う。

第6節 スプリンターネットへの企業の対応 （水越 一郎）

企業によるスプリンターネットは既に日本企業でも発生している。しかし、スプリンターネットに対する企業の動きには推進だけでなく抑止も存在する。企業が政府規制の影響下にあるのは当然だが、民主主義国家において規制は所与のものではなく、自身

の考えに基づいてそこに影響力を行使すべきである。スプリンターネットについて単なるインターネットの変容と捉えず、それがもたらす結果についてより議論する必要がある。

第1節 スプリンターネットの動機と その変質についての仮説

中央大学 実積寿也

1. スプリンターネットとは

ネットワークのネットワークとして構築・運用されているインターネットは、「開かれた、自由で、グローバルで、相互運用可能で、信頼性のある、安全な」¹⁾ 通信インフラであり、すべての端末や関連機器を繋ぐことで大きな価値を実現することが期待されている。一方、そうしたグローバルな接続を損なう行為は、「インターネットの断片化（internet fragmentation）」、あるいは、インターネットの分割（splitもしくはsplinter）という意味で「スプリンターネット（splinternet）」²⁾ と呼ばれる。近年、ロシアのウクライナ侵攻を契機に、国家間の対立がインターネットに亀裂をもたらす動きが顕在化し、インターネット技術コミュニティがそうした行為に対し一定の対応を迫られる事態が発生している。

スプリンターネットという行為自体はウクライナ侵攻後に初めて登場した現象ではない。治安維持などの目的を掲げた政府により、当該国のネットワークが海外から切断される事態は、中国のグレートファイアウォール（金盾）やアラブの春などの先例がある。2004年以來のGoogleサーチにおけるキーワード検索回数の推移を示すGoogleトレンドによると、splinternetという単語の検索のピークは2004年6月であり、ウクライナ侵攻後のピーク検索回数（2022年4月）はその17%の水準に過ぎない。

また、スプリンターネットを起こすのは政府だけではない。例えば、Malcomson（2006）は、より効果的な広告配信を実現するための利用者のセグメント化が、民間プレイヤーによるwalled garden化を招き、スプリンターネットを実現すると述べる。途上国貧困層に対する無料のネット接続提供を目指したFacebook Zeroの試みが、無料コンテンツの恣意

1) 「未来のインターネットに関する宣言」（2022年4月28日発表）（https://www.soumu.go.jp/main_content/000812030.pdf）より

2) splinternetという言葉は分割するという意味をもつsplitと、インターネット（internet）を組み合わせた新語である。その他にも、splinterとinternetを組み合わせた新語であるという記述もネット上には存在する。英語版Wikipediaは後者に依拠している。ただし、google検索のヒット数を比較すると、「split + splinternet」は「splinter + splinternet」の8倍超存在している（2022年10月25日現在）。そのため、本稿では前者の説を採用する。なお、Merriam-Websterではsplinterの意味として「1: to split or rend into long thin pieces」と「2: to split into fragments, parts, or factions」の2つをあげている。splinterの定義中にsplitの単語が入っていることから、どちらの説をとってもsplinternetの意味するものに差はないと想定される。

的選択によるwalled garden構築を通じ、かえって貧困層のインターネット経験を阻害するという批判（Wallace [2020] など）を受けたことも記憶に新しい。

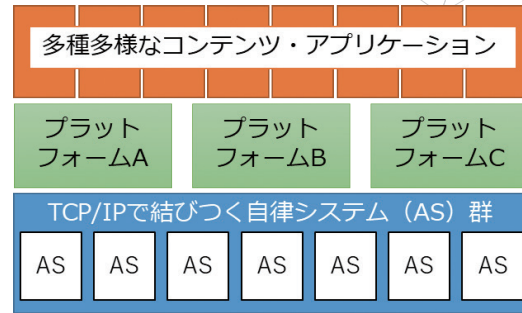
こうした背景の下、スプリンターネットの動きに対抗する主要勢力のひとつであるインターネットソサエティは、スプリンターネットに対して以下の定義を与えている（York, 2022）。

The “Splinternet” is the idea that the open, globally connected Internet we all use splinters into a collection of fragmented networks controlled by governments or corporations.

（「スプリンターネット」とは、私たちが使っているオープンでグローバルに接続されたインターネットが、政府や企業によってコントロールされた断片的なネットワークの集合体に分割されてしまうという考え方である。【筆者翻訳】）

この定義の抱える最大の問題は「分割」がどういう状況を指すのかが不明な点である。そもそも、目の前の状況を描写するために与えられている選択肢は「統合」と「分割」の2つだけなのか、あるいは、その間に「部分的分割」といった中間的な選択肢があり得るのか。回線設備を物理的に切断するような行為が「分割」に値することは論を俟たないであろうが、切断行為がソフトウェア的に実行され、容易に原状復帰が可能な場合はどうか。政府にとって都合の悪い情報を取り扱っているトラヒックだけを阻害することは「分割」に値するのか、ペアレンタルコントロールの場合はどうか。

現状のインターネットは、下位レイヤにおいては技術的なサービス品質（quality of service, QoS）の意味で統合されていると言えるが、プラットフォームや巨大テック企業による寡占化の結果、walled garden化が進行している上位レイヤについては、QoSの点からは「統合寄りの不完全分割状態」とであると評価できるというのが筆者の見立てである（図表1）。この場合、現状が「何らかの対策を講じるべきスプリンターネット」の名に値するか否かを判断するにあたってはエンドユーザーのquality of experience（QoE）の視点が必要となる。スプリンターネットがもたらすさまざまな経済損失³⁾や、さらには民主主義への脅威として捉えられているエコーチェンバーやフィルターバブルは、QoEの観点から初めて問題となるためである。留意すべきは、QoSとQoEの関係



図表1 インターネット断片化の現状

は直線的ではないという事実である。また、あらゆるQoS低下がQoE毀損をもたらすわけではないし、あらゆるQoE毀損がQoS低下に起因するわけでもない。さらに、QoEの判断基準が極めて属人的であるため、現状をスプリンターネットと称すべきか否かという問いかけに対しては利用者一人ひとりが異なる解を持つという可能性さえ存在する。

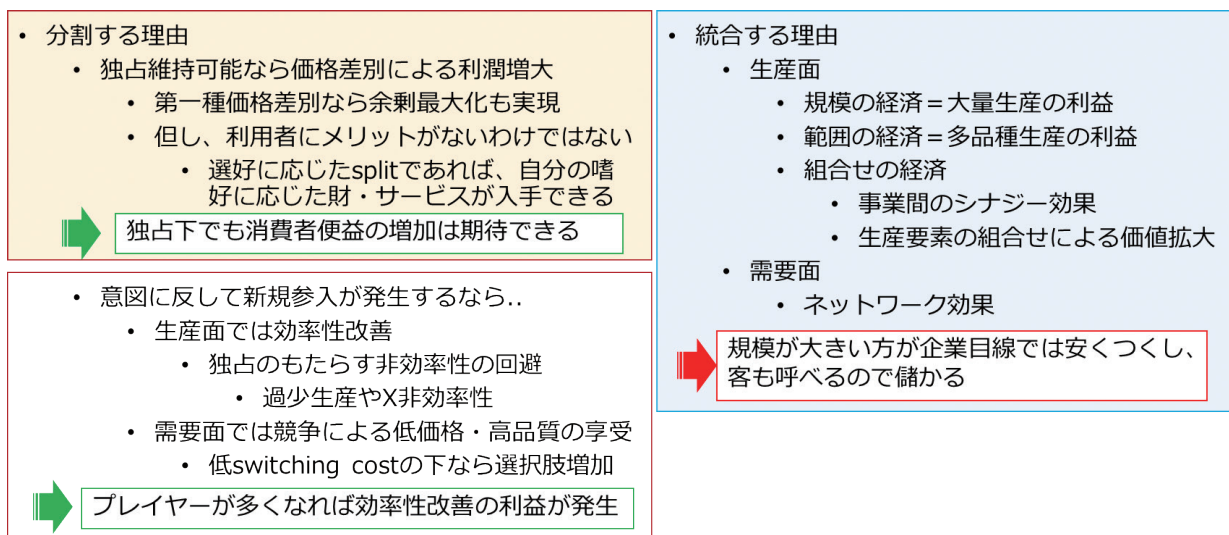
こうした課題を考慮すると、スプリンターネットという事象について現時点で一度冷静に検討し、詳細な政策検討の基礎を構築しておくことは有益であろう。これが本研究の動機である。

2. 分割する理由、統合する理由

ある事業、活動、市場を、分割する理由と統合する理由について検討しよう（図表2）。結論を先取りすると、インターネットをセグメントに分けようという分割戦略にも、反対に現状のまま維持するという統合（非分割）戦略にも、それぞれ合理的な理由がある。そのため、最適戦略の決定は個別事情を勘案した上でケースバイケースに行わざるを得ず、一般解というものは存在しない。

まず、サービス提供者にとっての経済的理由に焦点を当てる。日本を含む多くの先進国において、インターネットの維持・管理・拡張は民間プレイヤーが主体となって実施しているため、経済的に正当化されない戦略は長期的には維持可能ではない。なお、議論の大前提として、分割戦略を企画・実行できるプレイヤーは、あらたに設定したセグメント境界を取引相手に強制できるだけの影響力を持っている必要がある。地理的に市場を分割しようとしても、境界をまたぐ移動が容易であれば、その分割は機能しない。利用者属性による分割の場合は、偽装を防止するために、個々人の属性を検知・認証する強固なメカニズムが必要である。本稿の主要対象であるスプリンターネットの場合、国境コントロールや公的

3) “The Cost of Internet Shutdowns” (Statista, May 22, 2022) (<https://www.statista.com/chart/23864/estimated-cost-of-internet-shutdowns-by-country/>)



図表2 統合戦略と分割戦略それぞれの経済的理由

ID登録というシステムが、利用者の国境を超えた自由な移動を制約する具体的なメカニズムとして機能する。

分割戦略がサービス提供者に与えるのは、価格差別の可能性である。利用者の嗜好や、価格弾力性、所得水準に応じた分割を実施し、かつ分割後も各市場セグメントへの支配力を維持できるなら、セグメント毎に独占価格の水準に等しい最適価格を設定し、利潤を拡大することができる。この利潤拡大は消費者余剰の負担を伴うが、このことがすべての消費者に不利益をもたらすわけではなく、消費者全体にとってマイナスであるとは限らない。価格差別により平均費用を下回る価格付けが特定セグメントで可能となる結果、一律価格の下では購入できなかった消費者への市場拡大を伴うため、一定の消費者メリットが発生する。分割戦略の結果、各セグメントの消費者の嗜好をより反映するような財・サービスの投入がなされれば、消費者効用へのプラス効果も期待できる。なお、所得分配の問題を捨象できるのであれば(もしくは事後的に対処可能であるならば)、市場細分化が進み、第一種価格差別が可能になれば、死荷重損失の発生は回避され、経済全体としては最適な結果が実現する。一方、企業の意図に反し、分割の結果、一部セグメントへの市場支配力を喪失し、新規参入に余地が生まれる可能性もある。この場合、価格競争により独占レントは失われ、生産面での各種非効率性は解消され、さらに、利用者にとっては提供価格の低下、製品バリエーションの増大が期待できる。結果として、生産者余剰の減少を上回る規模で消費者余剰は増大する。

それに対し、統合戦略がサービス提供者に与える最大の経済的インセンティブは、生産効率性の改善

である。大量生産による平均費用低廉化(規模の経済性)や、多品種生産による共通設備の有効活用の利益(範囲の経済性)を得ることで、事業収益率の改善、あるいは平均費用の低下を価格競争力の源泉として活用することで、市場支配を強固にすることが期待できる。新たに統合されたセグメント間のシナジーが新しい価値をもたらす可能性もある。加えて、需要面におけるネットワーク効果の活用による消費者誘因も経済的インセンティブとして期待される。事業領域拡大による利用者数増が、提供している財・サービスをさらに魅力的にすれば、品質競争を通じて市場シェアが拡大し、さらなる収益性増大がもたらされる。

経済的理由に加えて、非経済的な理由も重要である。分割戦略の背後には、安全保障や国家アイデンティティ確保、文化的価値の保存といった動機がある。アラブの春におけるインターネット遮断や、中国の金盾は非経済的理由に起因するインターネット分割の典型である。国境外からの不適切な情報流入により国内の治安やネットワークセキュリティが脅かされていると判断される場合、緊急避難の措置としてネットワークを遮断することには一定の合理性があり、その趣旨は国際電気通信連合憲章第34条(電気通信の停止)、同第35条(業務の停止)にも反映されている。また、国外企業により市場が席卷されている場合、産業政策的見地から、外国企業の活動に一定の制約を加えることが正当化され得るが、国外への情報持ち出しに一定の制約をかけるデータローカライゼーションなどの規律は、その手段のひとつとなる。一方、統合戦略は、自国文化や価値観を域外に提供し、グローバルスタンダード化するための合理的な選択となる。

3. スプリンターネットの三局面と攻撃型への進化

インターネットについて統合と分割が議論される局面は複数存在する。Drake et al. (2016) の指摘によれば、オープンなインターネットは、技術、制度、ビジネスという3つの局面の協調によって実現されており、そのうち1つでも機能不全が発生すれば、インターネットの断片化が発生する虞がある。各局面における機能不全をもたらす要因については計28個が列挙され、分析・評価されている。その中には、ルーティング機能の毀損、DNSの障害のように、インターネットの完全な分割 (complete split) をもたらす要因から、データローカライゼーションの要求や、特定コンテンツの geo-blocking (地理的制限) のように、インターネットそのものの分割ではなく、その上で実現する自由なデータ流通に一定の制約を加える、つまりインターネットという機能の一部分だけに分割 (partial split) をもたらす要因までが含まれている。

リスト化されたこれらの要因は、そのままスプリンターネットの手段としても活用できる。分割を追求する側はいずれか1つの局面を選択し、目的に最適な水準の手段を費用対効果等の観点から選択すれば良い。それに対し、統合を志向する側はこれらすべての要因に配慮する必要がある。インターネットの現状が「統合寄りの不完全分割状態」であり、統合を目指す側が現状維持を目的とするのであれば、分割を志向する側に対して一つひとつの試みに直接対応することは、利用可能な資源の量から見て明らかに手に余る。分割するという試みにペナルティを課すよりも、統合を維持することで大きな便益が得られるというシナリオを説得力のある形で提示することが正しい統合戦略であろう。

国が主体となっていく分割戦略については、ウクライナ侵攻を契機に態様が変化しているように見受けられる。アラブの春や中国の金盾で観察されるスプリンターネット戦略は、国内の治安維持を目的に、

国外との情報流通を制限することに主眼があり、その意味で、「防御的な性格」を持つものであった (スプリンターネット1.0)。それに対し、2022年2月28日付けのウクライナの第一副首相兼デジタルトランスフォーメーション大臣ミハイロ・フェドロフが求めた以下の3項目は、敵対国をグローバルなインターネットから締め出すための分割戦略という「攻撃的な性格」を持つ (スプリンターネット2.0)。

- ①ロシアの ccTLD (.ru, .su, .P Φ) の無効化
- ②これらの ccTLD に対する SSL 証明書の無効化推進
- ③ロシア連邦に設置された2つのルート DNS サーバの無効化

本要請については、ICANN側の拒否により実行には移されず、その結果、技術という局面ではロシアに対するインターネット分割は実施されていない⁴⁾。ICANNのこの判断は米国やEU、G7諸国の対ロシア制裁とも軌を一にしている。2022年4月6日に米国ホワイトハウスが公開したファクトシート⁵⁾によれば、人道的活動に不可欠なセクターへの支援を継続するという視点から、情報の流れを支える電気通信サービスやロシア国民に外部の視点を提供するインターネットへのアクセスについては対ロシア経済制裁の対象外とされている。

ただし、本節冒頭に示した通り、スプリンターネットは技術の局面だけで発生するわけではない。2022年3月4日、米通信大手Cogent Communicationsはロシアの顧客に対してインターネットサービスの提供を停止した⁶⁾。さらに、MastercardとVisa、PayPalはロシア向けの決済サービスを停止し⁷⁾、Microsoft⁸⁾やApple⁹⁾、Meta¹⁰⁾、YouTube¹¹⁾はロシアでのサービスに一定の制限を加えている。民間企業によるこうした一連の対応により、ロシアからインターネットへのアクセスが不可能になるわけではもちろんないが、ロシア国内からの利用に際しQoSやQoEが低下し、インターネット上の経済活動に支障が生じている可能

4) ウクライナからの要請に対するICANNの対応については、2022年3月11日付けJPNICブログ (「ウクライナ侵攻とインターネット」、<https://blog.nic.ad.jp/2022/7359/>) に簡潔にまとめられている。

5) “FACT SHEET: United States, G7 and EU Impose Severe and Immediate Costs on Russia” (White House, Apr. 6, 2022) (<https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/06/fact-sheet-united-states-g7-and-eu-impose-severe-and-immediate-costs-on-russia/>)

6) 「米通信大手Cogent、ロシアでインターネットサービスを停止」(ZDNet Japan, 2022年3月8日) (<https://japan.zdnet.com/article/35184553/>)

7) 「PayPal、Mastercard、Visaがロシアでサービス停止 - 制裁の動き広がる」(CNET Japan, 2022年3月7日) (<https://japan.cnet.com/article/35184509/>)

8) “Microsoft to remove RT apps, ban Russian state-owned media ads” (REUTERS, Feb. 28, 2022) (<https://www.reuters.com/business/media-telecom/microsoft-remove-rt-apps-ban-russian-state-owned-media-ads-2022-02-28/>)

9) “Apple Stops Sales in Russia—and Takes a Rare Stand” (WIRED, Mar. 1, 2022) (<https://www.wired.com/story/apple-russia-iphone-ukraine-traffic-maps-rt-sputnik-app-store/>)

10) <https://twitter.com/nickclegg/status/1498395147536527360?s=20&t=vJJA5m70VXm2R31T2Qaew>

11) “YouTube bans Russian media outlets across Europe” (POLITICO, Mar. 1, 2022) (<https://www.politico.eu/article/youtube-bans-russian-media-outlets-across-europe/>)

性がある¹²⁾。つまり、ビジネスという局面でのスプリンターネットは実現している可能性がある。

特筆すべきは、こうした民間企業の行為が各社の自主的判断、おそらくは「正義」に加担することは各社の長期的な収益性にプラスであろうという判断に基づき、政府の不介入方針にもかかわらずスプリンターネット2.0を実現していることである。スプリンターネット1.0が安全保障や治安維持の観点から政府主導によって実施されたのとは対照的に、ロシアを対象とするスプリンターネット2.0は現状では西側諸国の民間企業主導で実現されていることになる。

4. 継続検討の必要性

インターネットが社会経済生活に不可欠なインフラとして組み込まれたことにより、その提供に携わるプレイヤーが負う社会的責任は増すばかりである。インフラである以上、平時のみを想定して運営することは許されず、有事や戦争下においての役割も日頃から考慮しておくことが求められる。ロシアによるウクライナ侵攻を機に再び組上にあがったスプリンターネットというテーマは、インターネットに携わる多彩なステークホルダーに、そうした社会からの期待にどのように応えていくのかを改めて考えさせる良い機会であろう。

民間プレイヤーがインターネットに関与するルールを定めるのがインターネットガバナンスの主要テーマだとすれば、スプリンターネット1.0や2.0をどう取り扱うのか、より一般的には有事の（あるいは、有事に転化する可能性が高い平時の）インターネットはいかに運営すべきか、について我々は議論を開始すべき時期に来ているのかもしれない。その際、スプリンターネットに対処してインターネットの統合を維持しようという方針が、サイバー攻撃の場を用意することと同義である点にも考慮する必要がある。ただし、サイバー攻撃に関する国際法のルールを包括的に記述した『タリン・マニュアル2.0』（Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations）の規則92によれば「A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.（サイバー攻撃とは、攻撃としてであるか防御としてであるかを問わず、人に対する傷害若しくは死、又は物に対する損害若しくは破壊を引き起こすことが合

理的に予期されるサイバー行動である〔翻訳は中谷他（2018, p.104）より引用〕』とされているため、スプリンターネット単独では国際法上のサイバー攻撃には該当しない。しかしながら、スプリンターネットに関わる行為が、戦時国際法上どのように位置づけられ、それに関わる政府や民間主体がどのような義務を負うのかについては、『タリン・マニュアル2.0』¹³⁾をベースとした詳細な検討が必要であると思われるが、この点については本稿の範囲を大きく超えるため、今後の課題としたい。

参考文献

- Drake, W.J., Cerf, V.G., and Kleinwächter, W. (2016) “Internet Fragmentation: An Overview,” Future of the Internet Initiative White Paper, World Economic Forum, available at <https://www.weforum.org/reports/internet-fragmentation-an-overview/>
- Malcomson, S. (2016) *Splinternet: How Geopolitics and Commerce Are Fragmenting the World Wide Web*, OR Books.
- Wallace, S. (2020) “In the Developing World, Facebook Is the Internet,” The Startup, Sep 7, available at <https://medium.com/swlh/in-the-developing-world-facebook-is-the-internet-14075bfd8c5e>
- York, D. (2022) “What Is the Splinternet? And Why You Should Be Paying Attention,” Internet Society, March 23, available at <https://www.internetsociety.org/blog/2022/03/what-is-the-splinternet-and-why-you-should-be-paying-attention/?fbclid=IwAR1xMQ6bALe8Wysmg61Mu2KVnldGyYgCYjLnled-gqqpN6587XlzipMttqg>
- 中谷和弘・河野桂子・黒崎将広（2018）『サイバー攻撃の国際法—タリン・マニュアル2.0の解説』信山社。
- 中谷和弘（2020）「④タリン・マニュアルについて—サイバー攻撃に関する国際法—」『情報処理』61(7), 687-692.

12) なお、ウクライナ侵攻後にロシア政府の側からもスプリンターネット1.0的な利用制限が実施されている。Statistaの推計によれば、侵攻後543時間分の利用制限でロシアが被った経済コストは12.1億ドルに達する (<https://www.statista.com/chart/23864/estimated-cost-of-internet-shutdowns-by-country/>)。

13) 『タリン・マニュアル2.0』の簡単な解説は中谷（2020）を参照されたい。

第2節 インターネット技術 コミュニティから見た スプリンターネット

日本ネットワークインフォメーションセンター (JPNIC)
前村昌紀

1. ウクライナ政府からの依頼と その顛末

ロシアのウクライナ侵攻が始まった後、ウクライナ政府は2022年2月28日に、ウクライナの第一副首相兼デジタルトランスフォーメーション大臣である Mykhailo Fedorov 氏の名前で、ICANN¹⁴⁾ の CEO、Göran Marby 氏に書簡¹⁵⁾ を送り、ロシアの ccTLD (.ru, .su, .PΦ) の無効化などを要請した。これに対してマービー氏は同3月2日に返信¹⁶⁾ においてこの要請を拒否した。同様に RIPE NCC¹⁷⁾ に対しては IP アドレスの利用権取消の要請が送られ¹⁸⁾、RIPE NCC でも要請の拒否を旨とする返信を行った¹⁹⁾。その理由はいずれも、端的に言えば、そもそも取消や切り離しを行う権能を持たないということである。

2. 民間主導によるグローバルな インターネット

インターネットはその黎明期から、開発や運用を行う当事者の直接関与によって運営方針が検討、制定されてきた。インターネットは民間主導で発達したため国境を意識せずグローバルな広がりを持っている。ICANN は米国カリフォルニア州、RIPE NCC はオランダで設立された非営利法人だが、ドメイン名や IP アドレスの管理に関して政府の関与はない²⁰⁾。それぞれ定款など²¹⁾ によって、コミュニティメンバーや会員による方針策定と運営を規定している。国によっては、国内の電気通信基盤の保全管理の意味合いから IP アドレスやドメイン名の管理を法制化する例²²⁾

もあるが、グローバルなインターネットの運営に対して国内法が影響を及ぼすことは極めて稀である。

ICANN のキャッチフレーズに One World, One Internet という言葉がある。この言葉が示すように、インターネットを作り運営してきた技術コミュニティはグローバルに単一のインターネットを志向しており、先述した通り、IP アドレスやドメイン名において特定の国を切り離す権能がそもそもないということも、この単一インターネット志向の表れとも取れる。RIPE NCC の Managing Director である Hans-Petter Holen 氏は、国々や民間企業は常に他と競合状態にあるにも関わらず、単一のグローバルインターネットを共有しており、それがインターネットに関するコンセンサスである、と指摘している (Holen, 2022)。Internet Society の CEO、Andrew Sullivan 氏は、インターネットの分断という問題に関して、インターネットにおける各種サービスは、グローバルに分散したさまざまな機能を組み合わせて構成され提供されるので、切り離した「ローカルインターネット」はもはやインターネットではなくその否定に過ぎない、インターネットはさまざまな形で冗長化されており、悪条件の中でも復元性が高く、簡単に遮断できない、分断することで偽情報の流入は避けることができるが、真実も届かなくなる、などと主張している (Sullivan, 2022)。アジア太平洋地域の IP アドレス管理組織 APNIC (Asia Pacific Network Information Centre) の Director General である Paul Wilson 氏は、インターネット発展の歴史を振り返ると、いくつかの別々の用途や方針を持つネットワークが、自発的な選択によって相互接続されていき、違いのあった仕様が統一され、最終的に単一のインターネットを構成したと指摘する²³⁾。グローバルに単一のインターネットは、世界中全ての企業や個人が共有し、協働するプラットフォームとなる。

14) Internet Corporation for Assigned Names and Numbers。米国カリフォルニア州の非営利法人で、インターネットの IP アドレス、ドメイン名、プロトコルパラメータの管理台帳機能である IANA (Internet Assigned Numbers Authority) を運営している (<https://www.icann.org/>)。

15) <https://www.icann.org/en/system/files/correspondence/fedorov-to-marby-28feb22-en.pdf>

16) <https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf>

17) Réseaux IP Européens Network Coordination Centre。世界に5つある IP アドレス管理団体、Regional Internet Registries (RIRs) の1つで、欧州、中央アジア、中東を管轄している。オランダの非営利法人 (<https://www.ripe.net/>)。

18) <https://www.ripe.net/publications/news/announcements/request-from-ukrainian-government.pdf>

19) <https://www.ripe.net/publications/news/announcements/ripe-ncc-response-to-request-from-ukrainian-government>

20) ICANN は IANA 機能の運営を米国商務省からの受託という形で行っていたが、この契約関係は2016年10月に解消している。

21) ICANN の定款 ("Bylaws for Internet Corporation for Assigned Names and Numbers") (<https://www.icann.org/resources/pages/governance/bylaws-en>)、RIPE NCC の定款 ("RIPE NCC Articles of Association (2021)") (<https://www.ripe.net/publications/docs/ripe-752>)

22) 一例として韓国のインターネット資源法 (https://elaw.klri.re.kr/eng_service/lawView.do?hseq=48158&lang=KOR)

23) "Taiwan Internet Governance Forum 2022 The Challenge of Internet - and How the Future Internet will be" (Taiwan IGF, Sep. 28, 2022) (<https://youtu.be/RuNPNMkiAfA>)

3. ステークホルダーとそれぞれの権能

スプリンターネットをインターネットガバナンスの問題として論じるうえでは、インターネットがさまざまなステークホルダーの協力によって運営されており、ステークホルダーごとの権能が尊重されることを踏まえて論を進めたい。

政府は国内の公共政策、他国との関係においては外交政策を制定し実施する。現在ロシアに対しては、ウクライナへの軍事行動を受けて経済制裁を課す国が多く、日本やEUも例外ではない。経済制裁では、民間企業に対して条件に合致する輸出を禁止することを求めるが、これによって、ロシアに対する役務提供が禁じられ、通信事業者がロシア企業へのネットワーク接続を切断することは起こり得る。

通信事業者の多くは民間企業であり、事業を通じて利益を得ることが目的である。電気通信が公共的な事業であるとして、差別的提供を禁じるなどの規制を敷かれていることは多いが、IPアドレスやドメイン名、プロトコルを用いて利用者のデータを送り、通信を繋げているのは事業者である。政府の外交政策によって切断を強いられることもあり得るが、利用者をつなぐこと、切断することを決めているのは事業者なのだ。IPアドレスやドメイン名を管理運営する技術コミュニティは、通信が実現できるように識別子を管理して、条件を整えているに過ぎない。グローバルに単一なインターネットは、インターネットの設計思想としてあるべき姿であるが、それを事業者に強いることはできない。ここは公共政策を担う政府と異なる点である。

2. で、グローバルなインターネットの運営に対して国内法が影響を及ぼすことは極めて稀である、と述べたが、この極めて稀なことが、ロシアのウクライナ侵攻によって起こっていることを紹介したい。これはEUの対露制裁の影響である。EUの対露制裁の中で、特定の個人や法人に向けた経済資源や資金の提供が禁止されたが、IPアドレスがこの経済資源と認定されたため、制裁対象となっているごく限られた個人や法人に対して、新規のIPアドレスの登録ができなくなった。EUの経済制裁方針の実施は、各国政府に委ねられているため、RIPE NCCはオランダ政府当局との間で方針の解釈や実施容態に関して調整と確認を行い、IPアドレスの提供という事業目的が最大限維持できるように努めている（Fragkouli, 2021）。

4. One Internetなのか

パンデミックで外出自粛となり、2020年以降在宅勤務が本格化した。業務プロセスのペーパーレス化デジタル化が一気に進み、本格的に、インターネット上であらゆる経済活動や市民生活が行えるようになった感がある。もはや、インターネットを前提とした社会、と言って過言ではない。One World, One Internetというキャッチフレーズを紹介したが、Internetがほぼほぼ社会だと言えるのであれば、One World, One Societyと言ってしまえるだろうか、と考えた。しかし現実には、世界は200程度の国に分けられ、さまざまな文化があり、さまざまな言語がある。我々の世界は、実に多様だとも言え、そのようにソフトに分断されている。実積氏の論考にあるように、One Internetと称されるインターネット基盤の上で、プラットフォームやアプリケーションがしのぎを削って競合しており、別々の世界を作っている。国によっては閲覧できる情報を制限するためにフィルターを実装している。通信回線を繋ぐ、切るという物理的な接続・切断以外に、あらゆるレベルのソフトな手段で、インターネット空間が分けられている。世界中の利用者に便益をもたらすインターネットは、不正を働こうとする者にも大きな便益を与え、セキュリティ対策は日に日に難しくなっている。また、グローバルに単一なインターネットによって得られた強大なネットワーク効果は、GAFAなどと称される強大なプラットフォーム事業者によるかつてない規模の寡占に結び付いた。インターネットは確実に利用者の便益をもたらしているが、今のインターネットは黎明期に目指したものになっているのだろうか。グローバルに単一なインターネットに、適切な分けを始めとして、どういう取り扱いをすれば、より安全で便利なインターネットになるのか、インターネット前提の社会で、すべての関係者が真剣に考える必要がある。

参考文献

Fragkouli, A. (2021) "How Sanctions Affect the RIPE NCC," RIPE Labs, Nov. 18, available at <https://labs.ripe.net/author/athina/how-sanctions-affect-the-ripe-ncc/>

Holen, H.P. (2022) "An Open Internet Remains the Goal," RIPE lab, Apr. 6, available at https://labs.ripe.net/author/hans_petter_holen/an-open-internet-remains-the-goal/

Sullivan, A. (2022) "Why the World must Resist

Calls to Undermine the Internet,” Internet Society, Mar. 2, available at <https://www.internetsociety.org/blog/2022/03/why-the-world-must-resist-calls-to-undermine-the-internet/>

第3節 インターネットのカタチ：2022

BBIX Singapore Pte Ltd 白畑 真

1. はじめに

インターネットは、1990年中盤までの黎明期にはアカデミアや研究所などのコミュニティが、1990年代中盤以降のインターネット商用化やブロードバンド化の時期においては通信会社がその主役を担ってきた。しかし、2010年代において大手のコンテンツ事業者（ないしはOTT: Over The Top事業者）とクラウド事業者が通信事業者をしのぐ規模で、インターネットインフラを担う役割を増していることは必ずしも広く知られていない。

本稿では大手コンテンツ事業者・クラウド事業者のインフラの現状を明らかにすることで、スプリンターネットの議論の前提となっている「インターネット」そのものの姿に対する理解の一助となれば幸いである。なお、本稿は個人の意見であり、筆者の所属先の意見ないしは見解を表明するものではない。

2. トラフィック寡占化が進むインターネット

インターネットはネットワークのネットワークとして、多数のネットワークが相互接続する形で成長してきたが、少数のコンテンツ事業者のネットワークにインターネット全体の大部分のトラフィックが集中している。

Labovitz et al. (2010) では、インターネットの通信全体の傾向を継続的に分析しており、2007年にはトラフィック全体の約50%の通信先は約2,000のAS²⁴⁾に分散していたが、2009年には150ASにまで減少しており、特定の通信先ネットワークへのトラフィックの集中化の傾向が見られた。その後、大手コンテンツ事業者とのトラフィックの増加が進み、2019年にお

いては、トラフィック全体の約50%の通信先がわずか5サイトによって占められていたという (Labovitz, 2019)²⁵⁾。

日本においても、2020年6月に開催されたネットワークエンジニアが集うカンファレンスであるJANOG46の発表において、地域系通信事業者が通信トラフィックの概況を明らかにしており、通信先1位の事業者だけで全通信量の約4割、上位15ASで全体の約83%を占めるという (吉浜, 2020)。

仮にスプリンターネットを推進する立場にあれば、中小規模の多数の事業者が存在する市場環境よりも、特定少数の事業者が寡占的立場にある市場の方が、より容易かつ効率的に規制を実装できると考えられる。このため、スプリンターネットの現状把握においてはトラフィックの寡占的立場にある大手のコンテンツ事業者・クラウド事業者に対する各国政府の規制や事業者自身の動向が重要となる。

3. コンテンツ事業者規模の巨大化・寡占化

インターネット全体においては少数のコンテンツ事業者・クラウド事業者によるトラフィックの寡占化が進んでいる。これらの事業者は莫大なトラフィックを処理・配信するための大規模かつ高品質なインフラを全世界的に展開しており、本稿ではこれらのインフラの例として、CDN、データセンタ、海底ケーブルについて触れる。

① CDN

CDNとは、コンテンツ配信に特化したDNSやサーバ群からなるシステムである。一般的には、世界中のさまざまな地域にサーバを配置することで、利用者との良好な通信が期待できるサーバからコンテンツを配信できるようにしている。

従来、これらのCDNのサーバは、通信事業者の集まるキャリアホテルと呼ばれるデータセンタに設置されることが多かったが、ここ10数年ほどは通信事業者のネットワーク内部にCDN用のサーバを設置（コンテンツ事業者から見た立場でOff-netキャッシュサーバ、ないしは通信事業者から見た立場でOn-netキャッシュサーバとも呼ばれる）し、当該通信事業者を利用しているユーザーにはそのサーバからコン

24) AS: Autonomous System (自律システム) はインターネットにおいて自律的な経路制御を行う単位で、各システムは固有の番号であるAS番号ないしはASNを有する。通信事業者やコンテンツ事業者単位で自律システムを運用することが多いが、大規模な事業者では複数の自律システムを有し、地域単位やサービス単位で運用することもある。

25) 2019年の調査においては、AS単位の分類ではなく、サイト単位での分類としている。これは複数のASや他社CDNのASも含めた実質的な集計を行うためと見られる。

テンツが優先的に配信される。

ユーザーに最も近い場所からコンテンツが配信されることにより、通信の遅延などの品質やコストの面で有利な立場にあると言える。また、通信事業者にとっては、キャッシュサーバの設置により外部との通信トラフィックを減らすことによるコスト削減効果が期待できる（Akamai, 2011）。この形態でCDNサーバの分散展開で先行していたのはAkamai社のAkamai Accelerated Networks Programであった。

しかし、GoogleやFacebook、Netflixなどの大手コンテンツ事業者はここ10年ほどでCDNを内製化、全世界的に規模を拡大している。Gigis et al. (2021) によれば、2021年4月時点で、Googleは3810AS、Facebookは2214AS、Netflixは2115AS、Akamaiは1463ASにキャッシュサーバを設置しており、大手コンテンツ事業者の自営CDNは、大部分のCDN専業事業者をしのぐ規模となっていると考えられる。

通信事業者のネットワーク内部に設置されるCDN用のサーバは、サーバ1台から数台程度と小規模な構成であることが多く、データを保存できる容量などに制約がある。このため、一部の非常に人気のあるコンテンツのみをキャッシュし、それ以外のコンテンツについては従来通りインターネット経由での配信を行うなど、CDN基盤の階層化と大規模化の重要な一部を担っている。

② データセンター

インターネットのコンテンツを保存・提供するため、サーバを設置する施設がデータセンターである。データセンターにおいてはサーバが安定的に稼働できるようにするため、電力会社から受電系統の冗長化、商用電源が停電した場合に備えたUPSや非常用発電機などを備えていることが一般的である。

データセンターの中でも、特定の顧客がデータセンターをビル一棟単位、フロア単位、ないしは部屋単位で利用することを前提とした大型データセンターのことをハイパースケールデータセンターと呼ぶ。大手コンテンツ事業者・クラウド事業者においては、ハイパースケール事業者からの賃借、ないしは自前でのデータセンター建設・運用を行うことが多い。

データセンターやクラウドの市場調査を行うSynergy Research Group (2022) は、全世界でハイパースケールDCの総数は2021年2Q時点において全世界で659カ所、2016年半と比較して倍に増加したとの調査結果を明らかにしている。Amazon, Microsoft,

Googleの3社だけでハイパースケールDCの面積の過半数超を賃借しているという。また、2021年9月時点では直近の1年は、ByteDance、Tencent、Alibabaの中国企業3社のDCの成長率が際立つとしている（Synergy Research Group, 2021）。

日本においても、ハイパースケールDCの台頭は著しい。インプレス総合研究所（2022）によれば、従来型のリテール型DCのラック数は横ばいとなっている一方、ハイパースケールDCは外資系事業者による新規参入と既存事業者による規模の拡大により急速に成長を遂げており、2023年にはハイパースケール型DCがリテール型DCを累積ラック数で逆転すると予測している。このことは、日本においても特定の少数の事業者による大規模なDCインフラの集中化を示唆している。

③ 海底ケーブル

海底通信ケーブルは世界中の大陸間の電気通信トラフィックの99%以上を伝送する役割を担っており（Rauscher, 2010）、今日のインターネットを中心とする社会インフラとして極めて重要な役割を果たしている。

Telegeographyの調査（Mauldin, 2017）によれば、2010年代前半までは、海底通信ケーブルは主に通信事業者によって敷設、利用されていたが、近年、Google、Meta、Microsoft、Amazonなどの大手コンテンツ事業者が海底ケーブルの敷設、利用を拡大している。2011年以前は国際伝送容量のうちコンテンツ事業者が占める割合は10%未満であったものが、2020年においては全体の66%を占めるまでに拡大している。これらの海底ケーブルは主に米国や欧州、アジアの主要データセンター間を相互接続するのに利用されるほか、これらのコンテンツを各国のユーザーに配信するためにも利用されている。

④ 大手コンテンツ事業者のインフラの実例

大手コンテンツ・クラウド事業者においては、各社間で情報開示の度合いに差があるが、中でもGoogleは自社のインフラについてわかりやすく開示を行っている。

Googleによれば、同社のインフラは「データセンター」「エッジPOP」「エッジノード」の三層構造で構成されている^{26), 27)}。

Googleは、大規模なDC群を自営している。これらのDCは大容量の通信回線で相互接続され、コンテンツは複数のDCに複製、分散保管することで耐障害性

26) “Google Edge Network” (Google, <https://peering.google.com/#/infrastructure>)

27) 拠点数の数はいずれも2022年11月現在

を有している。また、ユーザーに近いDCからのコンテンツを配信することで低遅延、高品質なデータ配信を可能にしている。なお、これらのDCはパブリッククラウドサービスであるGoogle CloudのDCとは必ずしも同一ではない。全世界23カ所に建設されており、その内訳は大陸別に北米14カ所、南米1カ所、欧州6カ所 アジア2カ所となっている。アジアでは台湾の彰化県、シンガポールの他、2023年には日本でも千葉県印西市にDCを開設するとしている（Google, 2022）。

「エッジPOP」は、いわゆるキャリアホテルと呼ばれる種類の通信事業者が集積するDC内に設置された拠点である。PeeringDBへの登録データ²⁸⁾によれば、これらの拠点は全世界134カ所、日本国内では東京6カ所（AT TOKYO（CC1/2）、ComSpace I、Equinix TY2、Equinix TY4、KDDI Otemachi、NTT Com（NW1））、大阪3カ所（Equinix OS1、NTT Com OS2（Dojima 2）、NTT Com OS7）の合計9カ所と開示されている。これらの拠点は、GoogleはIXや専用回線を通じて他の通信事業者、自社DC拠点と相互接続する役割を果たしている。

エッジノードはGoogle Global Cache（GGC）とも呼ばれ、通信事業者などのネットワーク内部にGoogleのCDN基盤となるキャッシュサーバを設置するもので、全世界で約4,000ASに展開している。GGCにはYouTubeの人気動画やGoogle Playのデータなど人気のある静的コンテンツが一時的にキャッシュされる。また、一部の拠点においては性能向上のためにGoogle Searchなどの検索サービスを中継することもあるとしている。

4. 寡占化と分断の兆候

インターネットにおいて寡占化が進むのは全体的なトラフィック面だけではない。2000年代後半に広がったソーシャルネットワークングサービス（SNS）においてもグローバルな寡占化が進んでいる。

Vincenzo Cosenzaの調査（2022）によれば、2009年6月時点では東アジア・東南アジア各国での最大のSNSは、日本ではmixi、韓国ではCyworld、中国ではQQ空間、フィリピンではFriendster、ベトナムではZingであり、各国ごとで異なるSNSが利用されていた。

一方、2022年現在では中国を除くすべての国でFacebookないしはInstagramというMeta傘下のSNS、中国ではWechat(微信)が最大のSNSとなっている。もはや、全世界のSNSは西側諸国を中心

とした全世界で展開するMetaと、中国で展開するWeChat、ロシアと旧ソ連諸国の一部で利用されるVK（旧VKontakte）の3社の寡占状況が生じていると言えるのではないかな。

5. まとめ

本稿ではスプリンターネットが脚光を浴びる昨今、インターネットインフラにおける、大手コンテンツ・クラウド事業者によるインターネットの姿を明らかにした。また、国や地域によって人気のあるコンテンツ・クラウド事業者が異なり、結果としてインターネットのインフラの所有者・運用者が分断されつつある姿を示した。

インターネットが商用化されてから四半世紀が経過した。インターネットとその基盤は社会に欠かせない存在となり、いわば社会がインターネット上に成り立っている状況が広がりつつある。今後、スプリンターネットが拡大した場合、1930年代のブロック経済体制が21世紀にデジタルブロック経済体制として再演される可能性もあるのではないだろうか。

参考文献

Akamai (2011)「アカマイサーバ設置の効果について」、available at <https://enog.jp/wordpress/wp-content/uploads/2011/06/20110624-ENOG.pdf>

Cosenza, V. (2022) “World Map of Social Networks,” VONCOS Blog, available at <https://vincos.it/world-map-of-social-networks/>

Gigis, P., Calder, M., Manassakis, L., Nomikos, G., Kotronis, V., Dimitropoulos, X., Katz-Bassett, E., and Smaragdakis, G. (2021) “Seven Years in the Life of Hypergiants' Off-Nets,” ACM SIGCOMM (21, August 23–27, 2021, Virtual Event, USA), available at <https://conferences.sigcomm.org/sigcomm/2021/files/papers/3452296.3472928.pdf>

Google (2022)「日本社会の更なるデジタル化に貢献するために～インフラとデジタル人材の育成に投資するデジタル未来構想」Google Japan Blog, Oct. 7, available at <https://japan.googleblog.com/2022/10/jdi.html>

Labovitz, C., Iekel-Johnson, S., McPherson, D., Oberheide, J., Jahanian F., and Karir, M. (2010) “ATLAS Internet Observatory 2009 Annual Report,” available at <https://archive.nanog.org/meetings/nanog47/>

28) <https://www.peeringdb.com/net/433>

[presentations/Monday/Labovitz_ObserveReport_N47_Mon.pdf](#)

Labovitz, C. (2019) “Internet Traffic 2009-2019,” available at <https://www.lacnic.net/innovaportal/file/4016/1/lacnog-internet-traffic-2009-2019.pdf>

Mauldin, A. (2017) “A Complete List of Content Providers' Submarine Cable Holdings,” TeleGeography BLOG, Nov. 9, available at <https://blog.telegeography.com/telegeographys-content-providers-submarine-cable-holdings-list>

Rauscher, K. (2010) “The Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) Report v201,” available at <https://www.ieee-rogucci.org/report/HTML/files/assets/seo/page85.html>

Synergy Research Group (2021) “Hyperscale Data Center Count Grows to 659—ByteDance Joins the Leading Group,” Synergy Research Group, Sep. 13, available at <https://www.srgresearch.com/articles/hyperscale-data-center-count-grows-to-659-bytedance-joins-the-leading-group>

Synergy Research Group (2022) “Pipeline of Over 300 New Hyperscale Data Centers Drives Healthy Growth Forecasts,” Synergy Research Group, Mar. 23, available at <https://www.srgresearch.com/articles/pipeline-of-over-300-new-hyperscale-data-centers-drives-healthy-growth-forecasts>

インプレス総合研究所（編）（2022）『データセンター調査報告書 2022』インプレス

吉浜賢（2020）「沖縄のインターネット事情2020」JANOG46 Meeting in Okinawa（2020年8月26日）（<https://www.janog.gr.jp/meeting/janog46/wp-content/uploads/2020/06/%E6%B2%96%E7%B8%84%E3%81%AE%E3%82%A4%E3%83%B3%E3%82%BF%E3%83%BC%E3%83%8D%E3%83%83%E3%83%88%E4%BA%8B%E6%83%852020v4.pdf>）

第4節 標準化団体を舞台にした スプリンターネットの兆候²⁹⁾

日経 BP 堀越功

1. 民主主義国と権威主義国の対立

インターネットガバナンスの在り方を巡って現在、世界で2つの陣営の対立が目立っている。第1の陣

営は、米国や欧州など民主主義（Democracy）国家だ。これらの国々は、現在の「自由で開かれたインターネット」を標榜し、インターネットはエンジニアや企業、学者、市民、そして政府という多様な人々の意見を民主的に反映したマルチステークホルダー（Multi-stakeholder）体制によって管理されるべきだという立場を取る。

第2の陣営は、中国やロシアなどの権威主義（Authoritarianism）といわれる国家である。これらの国々は、国家によるインターネットの統制を強め、自国内のインターネットに支配力を及ぼすべきだという「サイバー主権（Cyber Sovereignty）」を標榜している。その考えに基づき、インターネットガバナンスは、マルチラテラル（Multilateral）と呼ばれる国家間の交渉をベースにした体制によって運営されるべきだという立場を示す。

近年、中国やロシアは国家によるインターネットの統制を強めている。中国は国内からの欧米諸国の情報やサービスへのアクセスを遮断する「グレート・ファイアウォール（金盾）」を長く運営している。中国は、東南アジアの国などに対し同様の技術を支援しているとされる。

ロシアは政府によるネットワークの集中管理強化を目的とした法案を可決。「RuNet」と呼ばれるロシア国内のインターネットについて、国家による監視を高め、グローバルなインターネットと切り離れた「ロシア化したインターネット」を目指しているとされる（Sherman, 2021）。これら権威主義国家によるインターネットの統制は、断片化されたインターネットである「スプリンターネット（Splinternet）」を加速させる動きにつながる。

インターネットの基盤となる技術は、1960年代末に米国の研究開発プロジェクトから生まれた。現在のインターネットガバナンスは、「自由で開かれた」という米国の価値観を色濃く反映している。例えば、インターネットのドメイン名やIPアドレスなどを民間主導でグローバルに調整する非営利団体「ICANN（The Internet Corporation for Assigned Names and Numbers）」は、マルチステークホルダー体制で運営されている。インターネット関連技術の標準化を推進する任意団体「IETF（Internet Engineering Task Force）」も、誰もが個人で自由に参加でき技術仕様を提案できるマルチステークホルダー体制で進められている。

中国やロシアは、現在のインターネットガバナンスの体制は、米国の影響力が強い点を批判する。さら

29) 本節は、筆者が日経BPの技術メディア「日経クロステック」に公開した記事（堀越, 2022a, 2022b）をベースに改稿した。

にこうしたインターネットガバナンス体制は先進国中心であり、新興国の意見を十分に反映できていないとも指摘する。

2. ITUに接近する中国

国家によるインターネットガバナンスを目指す中国は、国連の専門機関であるITU（International Telecommunication Union、国際電気通信連合）において影響力を高める行動に出ている（Sherman, 2022）。

ITUは1865年に設立された電気通信の国際標準化や周波数の国際的な分配などを担う組織だ。現在193の国・地域と約700の民間団体が加盟している。投票権は1国1票が原則であり、国家間の交渉であるマルチラテラルな体制で運営されている。

中国は、インターネットの管理体制を、現在のICANNやIETFからITUへと移管するべきだという意見を表明している。ITUへの影響力を高める中国の狙いは、1国1票という運営の仕組み上、インターネットの管理体制をマルチラテラルな体制へ転換しやすいと考えているからだろう。

さらにITUで策定された勧告（Recommendation）は「デジュール標準（de jure standard）」と呼ばれ、国や政府間で取り決められる国際標準となる。デジュール標準になれば、新興国にも広まりやすい。中国が掲げるインフラ開発プロジェクト「一带一路構想」と親和性が高い点も背景にあると見られる。

中国は20年近くにわたり、インターネットの管理体制をICANNやIETFからITUへと移管するべく行動を続けている。例えば中国は2005年の国連インターネットガバナンス作業部会（WGIG）において、ICANNによるインターネットの管理体制を批判し、「（インターネットの管理体制は）国連の枠組みの下で、主権者である政府が主導的な役割を果たすべきだ」と主張した。中国はさらに2012年のITU世界国際電気通信会議（WCIT）において、ロシアやサウジアラビアと共同でITUが他のインターネット組織の権限と機能を引き継ぐべきだという提案した（Welch, 2012）。しかし米国や英国などその他多くの国が署名を拒否したことから、ITUはこの提案を取り下げた³⁰⁾。

2014年にはITUのトップである事務総局長に中国の趙厚麟氏が就き、ITUにおける中国の影響力をさらに高めている。趙氏は2018年に事務総局長に再選し、2022年まで任期を務める。

3. 物議を醸す「New IP」

中国は2019年、ITUにて、インターネットの根幹をなすプロトコルであるIP（Internet Protocol）に代わる新たなプロトコルも提案している。それが「New IP」である。

IPは1970年代に基本的な仕組みが開発された。データの送信元と送信先のIPアドレスをHeader部分に記載し、Payloadにデータを格納する仕組みである。機器が壊れても自動的に経路を迂回することで、粘り強く通信を確立できる。どんな環境でも受け入れられるIPの仕組みが、インターネットを世界に広げる大きな原動力になったと言える。

ただIPの登場から半世紀近くが過ぎ、限界も指摘されている。2030年代に向けてロボットの協調制御や自動運転のアシストといった新たなアプリケーションが想定される中、速度保証できずベストエフォートの通信となるIPがボトルネックになるという指摘がある。セキュリティについてもIPは十分に考慮されていない。

New IPは、中国の通信機器大手、華為技術（Huawei Technologies）とHuaweiの関連会社で米国の研究部門であるFuturewei Technologiesが中心となって提案した。

現時点でNew IPの完全な仕様は公表されていない。しかしHuaweiがITUに提出した資料（Jian, 2019）や、米国の学会・標準化団体である「IEEE」に提出した招待論文（Li et al., 2020）などから、New IPの基本的なコンセプトや、技術的なポイントを把握できる。

New IPの狙いは、工場内の通信やスマート農業、クラウドによる自動運転のアシスト、ホログラフィック通信など2030年をめどに登場するような多様なアプリケーションの要件に向けて、現在のIPを進化させることである。

例えば複数のロボットを協調制御するような通信を考えてみよう。このようなユースケースでは、それぞれのロボットに対してパケットの到着時間を保証するような機能が求められる。現在のベストエフォート型のインターネットでは実現が難しい。

そこでNew IPでは、既存のIPのHeaderとPayloadの間に、「Contract specification」という新たなフィールドを設ける。例えばこのフィールドには、以下のようなパケット配送についての指示を指定できる。

- BoundedLatency(t): 指定した時間(t)までにパケットを配送

30) ITUが2012年12月10日にTwitterに投稿した内容を参照 (<https://twitter.com/ITU/status/278079049983721472>)

- OnTimeDelivery(t, t'): 決められた時間内 (t から t' の時間内) にパケットを配送
- Coordinate: 複数ユーザーのアプリケーションでパケット配送タイミングを調整
- NoPacketLoss: パケットをロスしないようにあらゆる手段で配送

New IPは、パケットの配送について、よりTime Sensitiveな通信を可能にするというコンセプトだ。これまでのIPが、いつ届くかわからない普通郵便だとすれば、New IPは速達や追跡機能付きの郵便サービスと理解すればよいだろう。

New IPは、IPアドレスも拡張する。現在のIPv4やIPv6のような決められた固定長ではなく、可変長にして変えられるようにする。IoT向けに使う低消費電力、小メモリーのデバイスにおいては、より短いIPアドレスを利用したほうが、効率が良い。

2030年に向けては、衛星通信などのNTN (Non-Terrestrial Network) と、地上系ネットワークの統合が進むだろう。こうした状況においてIPアドレスは、経度や緯度とも関連付けたほうが、効率的に送受信できるという指摘がある。New IPでは、多様なユースケースをターゲットに、フレキシブルなアドレス体系を選べるようにする。

Huaweiは、将来のインターネットは、異種ネットワークがシームレスに共存する「ManyNets」になるとしている。このようなManyNetsの時代には、可変長のIPアドレスのほうが、多様なユースケースを収容しやすいというのが、New IPの考え方である。

New IPは、IPパケットにおけるPayload部分にも拡張を加える。例えばネットワークが混雑した場合、Payloadに格納したデータから、優先度が高い部分だけをまずはタイムリーに通信できるようにする。これによってネットワーク全体のスループットの改善や遅延解消につながるとする。

New IPは、既存のIPに、(1) Contract specificationを追加、(2) IPアドレスを可変長に拡張、(3) Payloadを拡張、の3点を追加したと整理できる。

ただし既存のIPと互換性はない。可変長のIPアドレスを採用するNew IPは、既存のルーターでは対応できず、New IP対応のルーターが必要になる。このようなNew IPのコンセプトが明らかになるにつれて、インターネット業界からは次々と懸念の声が挙がっている。

IETFは2020年3月、New IPに対し、「既存のIPを

全面的に置き換えるトップダウンのアプローチは有害である」と考える。相互接続性を損ない、ネットワークの離れ小島を作り出すことは間違いない。トップダウンのアプローチでは、継続的に進化するアプリケーションの多様なニーズには対応できない」と批判した³¹⁾。

欧州の通信関連団体である欧州電気通信事業者協会(ETNO)も2020年12月、「インターネットのプロトコルとアーキテクチャーは、ITUのようなトップダウンなプロセスではなく、IETFやIEEEのようなオープンでマルチステークホルダー、ボトムアップの方法で開発され続けるべきだ」と意見表明した(ETNO, 2020)。

ICANNも2020年10月、「New IPはIPアドレスと利用者との間に強い結び付きをもたらし、広範囲な監視を容易にする。公開されたコンテンツへの監視が強化される可能性がある」と指摘。プロバイダーや国家による監視能力が高まる点についての懸念を示した(Durand, 2020)。

各方面からの批判を受けてITU-TのSG11とSG13は2020年12月、New IPの提案について議論したものの、欧州各国や米国、日本など多くの国はNew IPの提案に反対に回り、結局ITU-Tは少なくとも2022年3月に開催の世界電気通信標準化総会(WTSA)まで議論しないことを決めた³²⁾。

4. 今後の展望

批判が相次ぎ、ITUでは棚上げになった「New IP」だが、中国とHuaweiは諦めた様子はない。Huaweiは批判を受けたNew IPという名称を、「Future Vertical Communication Networks (FVCN)」に変更して説明しているという。だが提案の基本的な内容は変わっていないようだ。

中国国内では「deterministic IP (決定論的IP)」という名称で、New IPに関連した9つの国内標準が策定されているという。Huaweiは2021年5月、中国国内のテストベッドで試験したdeterministic IPの実証実験の結果も発表した。2021年6月には、中国政府が支援する紫金山研究所などと共同で、deterministic IPに関するホワイトペーパーも公表している(第五届未来网络发展大会组委会, 2021)。

Huaweiは2022年に入り、New IPやdeterministic IPと同じような内容を「IPv6+」と称して、新興国を中心していると報じられている(Bertuzzi, 2022))。これらの動きからHuaweiと中国政府が、New IPのような新たな仕様を広げたいという継続的な意志が

31) "Liaison statement, Response to LS on New IP, Shaping Future Network" (IETF, March 2020) (<https://datatracker.ietf.org/liaison/1677/>)

32) "Huawei's 'New IP' Proposal - Frequently Asked Questions" (InternetSociety.org, Feb. 22, 2022) (<https://www.internetsociety.org/resources/doc/2022/huaweis-new-ip-proposal-faq/>)

浮かび上がってくる。

中国とHuaweiが継続的にNew IPに注力する理由は、特定のユースケースを対象にIPを拡張したいという考えからなのか。それとも中国が標榜するサイバー主権の土台としてNew IPを広げたいからなのか。もし後者だとすれば、New IPはスプリンターネットを世界に加速させる可能性がある。今後も継続的に中国やHuaweiの動きを注視していく必要がある。

なお2022年9月にルーマニアのブカレストにおいて、次期ITU事務総局長選挙が行われた。ここでも中国など権威主義国家と米国などの民主主義国家が真っ向から対立した。中国などが支持するロシアのRashid Ismailov候補と、民主主義国家が支持する米国のDoreen Bogdan-Martin候補が一騎打ちとなったからである。

投票結果は、米国のDoreen Bogdan-Martin氏が172票中139票を獲得し、圧勝した³³⁾。中国などが支持するロシアのRashid Ismailov候補が当選した場合、ITUにインターネットガバナンスを移管する動きがさらに加速するのではという見方が出ている。そのシナリオは一步後退した。

ただ長年にわたる中国の行動を見る限り、インターネットガバナンスをITUに移管させようという取り組みは今後も続いていく可能性が高い。中国が標榜する「サイバー主権」が世界各国に広がると、インターネットは必然的に断片化した「スプリンターネット」へと変貌していくだろう。

参考文献

Bertuzzi, L. (2022) “China Rebrands Proposal on Internet Governance, Targeting Developing Countries,” Euractiv, Jun. 6, available at <https://www.euractiv.com/section/digital/news/china-rebrands-proposal-on-internet-governance-targeting-developing-countries/>

Durand, A. (2020) “New IP,” ICANN, OCTO-017, Oct. 27, available at <https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf>

ETNO (2020) “ETNO position paper on the New IP proposal,” ETNO, Nov. 5, available at <https://www.etno.eu/library/positionpapers/417-new-ip.html>

Jiang, S. (2019) “New IP Networking for Network 2030,” Huawei Technologies, available at [https://www.itu.int/en/ITU-T/Workshops-and-](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019101416/Documents/Sheng_Jiang_Presentation.pdf)

[Seminars/2019101416/Documents/Sheng_Jiang_Presentation.pdf](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019101416/Documents/Sheng_Jiang_Presentation.pdf)

Li, R., Makhijani, K., and Dong, L. (2020), “New IP: A Data Packet Framework to Evolve the Internet: Invited Paper,” 2020 IEEE 21st International Conference on High Performance Switching and Routing (HPSR), available at <https://ieeexplore.ieee.org/document/9098996>

Sherman, J. (2021) “Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior,” Atlantic Council, July 12, available at <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/>

Sherman, J. (2022) “China’s War for Control of Global Internet Governance,” SSRN, July 2022, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4174453

Welch, C. (2012) “Russia, China, and Other Nations Draft Proposal to Give ITU Greater Influence over the Internet,” The Verge, Dec. 9, available at <https://www.theverge.com/2012/12/9/3747402/countries-propose-greater-itu-influence>

第五届未来网络发展大会组委会 (2021) 「未来网络白皮书——确定性网络技术体系白皮书 (2021版)」, available at <https://www-file.huawei.com/-/media/%20corporate/pdf/news/future-network-whitepaper.pdf>

堀越功 (2022a) 「ネットの管理巡り米欧と中露が対立、中国がITUに接近する理由」『日経クロステック』、11月7日、available at <https://xtech.nikkei.com/atcl/nxt/column/18/02225/110200002/>

堀越功 (2022b) 「『IPはもはや限界』、『ファウエイの新提案が世界で物議』『日経クロステック』、11月8日、available at <https://xtech.nikkei.com/atcl/nxt/column/18/02225/110200003/>

第5節 インターネットは断断するか

慶應義塾大学 SFC 研究所 小宮山功一朗

1. インターネットが断断されたとは一体どのような様を表すのか

スプリンターネットやインターネットの断断という言葉の定義はまだ発展途上にある。ここでは、長年

33) “Member States elect Doreen Bogdan-Martin as ITU Secretary-General” (ITU, Sep. 29, 2022) (<https://www.itu.int/en/mediacentre/Pages/PR-2022-09-29-ITU-SG-elected-Doreen-Bogdan-Martin.aspx>)

にわたり、インターネットガバナンス研究をリードしている米国の研究者ミルトン・ミュラーが、2017年に上梓した『Will the Internet Fragment?』（インターネットは分断するか?）という本を道標として用いる。

ミュラーは多くのワシントンD.C.を拠点とするシンクタンカーと違い、米国の国益とグローバルに機能するネットワークのバランスを模索しているように見える。ゆえに、彼の言説は中国やロシア、途上国の専門家からも一目置かれ、たびたび引用されている。スプリンターネットの議論にあたっては、幅広い価値観との妥協点を見付けることが必要になることを踏まえると、議論の出発点として適していると考えた。ただ第4節の最後でも述べられている通り、長年にわたる中国の行動を見る限り、インターネットガバナンスをITUに移管させようという取り組みは今後も続いていく可能性が高い。中国が標榜する「サイバー主権」が世界各国に広がると、インターネットは必然的に断片化した「スプリンターネット」へと変貌していきだろう。

同書の中で、ミュラーはインターネットの分断を2つに分けて捉えることを主張した。意図的でない分断と意図的な分断である。意図的でない分断は、さらにインフラの障害と構造的な互換性欠如の2つに分けることができる。前者は、例えば、ある国や地域が、自然災害等でケーブルが切断され、数千人が数時間にわたってインターネットを使えない状況を指す。後者はいわゆるデジタル・デバイドと呼ばれていた現象で、一部の途上国や離島のように、未だにその場所の住人の多くがグローバルなインターネットへの接続ができない状態を指す。

対して意図的な分断とは、何者かがグローバルなインターネットに繋がることを制限し、管理するという決定を下した結果である。意図的な分断の意味は広い。例えば、スパムメールのフィルターや、不正な通信をブロックするファイアーウォールというセキュリティ製品の使用も意図的な分断に含まれる。そのような製品の使用は、誰かがグローバルなインターネットに繋がることを管理するからである。

意図的な分断の決定者が民間企業であることもある。例えば、動画共有サイトやオンラインゲームのコンテンツに、地域によって視聴不可能なものがある。これは民間企業が特定の地域において視聴可能なコンテンツを自主規制している場合が多い。あるいは、ニュースサイトに掲載される記事の全文を読むためには、有料会員になるしかないことがある。これらはメディアやプラットフォームが決定した制限であり、意図的な分断に含まれる。意図的な分断の決定者は政府であることもある。政府がインターネットサービ

スプロバイダーに命じ、有害あるいは違法なコンテンツを含む、特定のURLやドメインへのアクセスを禁じるというのは、多くの国で行われてきた。

本稿の執筆者グループはこの問題について長時間の議論を行った。その際にもスプリンターネットという言葉が指すところは、意図的な分断であり、かつ決定者が政府の場合を指すという捉え方が主流であった。つまり本稿においてのスプリンターネットとは、「国家がグローバルなインターネットにつながることを制限し、管理するという行動。それによって引き起こされる情報の断絶」という定義ができそうである。ミュラーが捉えるインターネットの分断の範囲に比べて、ここでのスプリンターネットはより限定的な問題の捉え方をしている。そしてスプリンターネットの理解においては、意図的な分断の決定者たる国家または政府の意図の重要性が増している。

2. 国家によるインターネットの管理・統制のニーズが高まる

わずかに十数年前まで、多くの専門家はインターネットやサイバー空間は、国家の直接的な統制が及ばない世界だと考えていた。それゆえに、中国政府が行うさまざまなコンテンツ規制に対しては、自由でオープンなインターネットの理想に反すると、あからさまに批判してきた。

多くの民主主義国家も、サイバー空間のグローバル性を追認した。それは国家戦略文書や国際会議の発言記録にも残されている。カナダのサイバー戦略は「サイバー空間は相互接続された情報技術ネットワークであり、17億人が相互に繋がり、アイデアやサービスや友情を生むグローバル・コモンズ」とし、それがグローバル・コモンズであると断言している（Government of Canada, 2010）。日本も「国境を意識することなく自由にアイディアを議論でき、そこで生まれた知的創造物やイノベーションにより、無限の価値を生むフロンティア」と、そのグローバルな性質、言い換えれば一国の意思だけでは好きにコントロールできない側面に言及している（内閣サイバーセキュリティセンター, 2015）。しかし近年、さまざまな事情から、民主主義国家もまたサイバー空間における自国の主権確保に乗り出している。

風向きが変わったのは2010年から2013年の間である。直接的にはスノーデン事件などが契機と考えられるが、ブラジルやロシアだけでなく民主主義国家のドイツでさえも、自国内にデータを囲い込むことを検討するようになる。ドイツのアンゲラ・メルケル首相は「ヨーロッパのインターネット」の創設を呼びか

け、その問題意識は、ヨーロッパのプライバシー重視の伝統と合流し、2016年に制定されたEU一般データ保護規則へと繋がっていく。

国連などでの政府間協議では、サイバー空間における国家の役割が議論された。2013年と2015年の国連政府専門家会合では、国連憲章に規定される国家の「固有の権利」を含む国際法が、サイバー空間に適用されることで合意している。そして2015年のレポートでは、「国家は自国領土内にあるICT機器の管轄権を有する」と明示的に国家の管轄権が認められた (United Nations, 2015)。政府専門家会合は20数カ国の専門家によるクローズな会合であるが、サイバー空間の管轄権をまとめたレポートは、国連総会において全会一致で採択された。あまり知られていないが、比較的重要な決定が2015年になされていたのである。

実のところ、これを持ってサイバー空間に国家主権が認められるかについては現在も意見が分かれる。紙幅の都合から、細かい検討はできないが、前提となる国家主権自体が解釈の幅を持つ概念であり (クラズナー, 2001)、さらにサイバー空間における国家主権については、問題の新しさゆえのさまざまな論点 (河野, 2015; 八塚, 2017) が残っているからである。

3. 信頼できる、保護された、国際的な通信インフラへの展望。まとめて代えて。

以上の議論をまとめると、スプリンターネットの問題の核心はサイバー空間の管理に国家がどれだけ関与するのかという点にある。そして、国家がサイバー空間に関与する必要性が生まれるのはつまり、これまで目指してきた「自由で、オープンで、グローバルなインターネット」という目標の魅力が色褪せてきたからである。本当に必要なのは、「信頼できる、保護された、国際的な通信インフラ」なのではないか³⁴⁾。

自由は大切だが、信頼性も同様に大切なのではない。インターネットの運営者は身体の安全、家族の安全、民族の安全、宗教の安全は言論の自由と同等に重要であることに正面から向き合っていないのではないだろうか。サイバー空間上で、何かトラブルが起きれば、その影響で多くの人々の生命や安全が損なわれる。ここで我々は、人間が自由や開放性だけを希求するわけではないことを自覚しなければならない。

オープンネスは重要だが、弱者が保護される環境

はより重要なのではない。開放性を重視するあまり、弱者を保護する仕組みが、言い換えればインターネット上での福祉が真剣に検討されてこなかったのではない。

グローバル性は大切だが、これを突き詰めると一部のテック企業の力がさらに高まる。テック企業の技術的な優位性に疑問の余地はないが、それらの企業のガバナンスは多くの権威主義国家と同じくらい不透明である。そのような企業に対抗する手段として、実は国という行動単位は今でも強力である。

誕生から50年を経て、インターネットは世界中の人々にとって欠かすことのできない、インフラとなった。スプリンターネットという論題は、「自由で、オープンで、グローバルなインターネット」という当初の目標を見直す機会を我々に与えてくれているのかもしれない。

参考文献

Fick, N., Miscik, J., Segal, A., and Goldstein, G.M. (2022) "Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet," available at <https://www.cfr.org/report/confronting-reality-in-cyberspace>

Government of Canada (2010) "Canada's Cyber Security Strategy for a Stronger and More Prosperous Canada," available at https://publications.gc.ca/collections/collection_2010/sp-ps/PS4-102-2010-eng.pdf

Henriksen, A. (2019) "The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace," *Journal of Cybersecurity*, 5(1), 1-9.

Klimburg, A. (2013) "The Internet Yalta," Center for a New American Security (CNAS), August 5, available at <https://www.cnas.org/publications/commentary/the-internet-ylta>

Mueller, M. (2013) "Are We in a Digital Cold War?" Internet Governance Project, July 19, available at <https://www.internetgovernance.org/2013/07/19/are-we-in-a-digital-cold-war/>

United Nations (2015) "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / by the Secretary-General," A/70/174, available at <https://digitallibrary.un.org/record/799853?ln=en>

34) 「信頼できる、保護された、国際的な通信インフラ」というコンセプトは米国の外交評議会のレポート (Fick et al., 2022) に拠る。

クラズナー, スティーブン・D. (2001)「第2章 グローバリゼーション論批判 主権概念の再検討」『グローバル・ガヴァナンス』(渡辺昭夫, 土山實男編集)、東京大学出版会、45-68.

河野桂子 (2015)「サイバー・セキュリティに関する国際法の考察—タリン・マニュアルを中心に—」『戦略研究』、15、25-46.

須田祐子 (2021)『データプライバシーの国際政治: 越境データをめぐる対立と協調』、勁草書房. 内閣サイバーセキュリティセンター (2015)「サイバーセキュリティ戦略」available at <https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku.pdf>

八塚正晃 (2017)「サイバー安全保障に対する中国の基本的認識」『NIDS コメンタリー』、60号.

第6節 スプリンターネットへの企業の対応

東日本電信電話株式会社 水越一郎

1. 日本企業のスプリンターネット

スプリンターネットは政府だけではなく企業も引き起こしている。日本国内でも新聞社・雑誌社サイトでのpaywall³⁵⁾は一般的である。コンテンツの興味深く、重要な部分をpaywallの先に置くことで収益増を図ることは通常の企業活動であるが、コンテンツが分割されるという点でpaywallもスプリンターネットの一形態である。また、Yahoo! Japanは2022年4月6日から欧州経済領域 (EEA) およびイギリスで利用できなくなっている³⁶⁾。ヤフー広報は「今後の法令遵守対応コストなどの観点から、継続的にサービス利用環境を提供していくことが難しいと判断した」とその理由を説明しており、GDPR (EU一般データ保護規則) との関連が指摘されている³⁷⁾。サービス提供対象国の制限は企業の経営判断であるが、制限された側がスプリンターネットと捉えることもまた自然である。

以上のように企業によるスプリンターネットは日本国内でも発生している。

2. スプリンターネットの推進と抑止

先の日本の事例はPaywall、法令遵守コストといったわかりやすい経済的合理性に基づくものであった。また本稿1.3で実績はウクライナ侵攻に対する米国企業のロシアからのサービス撤退・制限の理由を長期的な収益性に対するプラスに求めている。いずれの例もスプリンターネットを推進するものであり、合理的判断に基づく企業行動にはそれ以外の選択肢はないのであろうか？

これについては検閲・監視を逃れるためにTorネットワークに対応するサービスを企業として提供している例が挙げられる。違法情報がやり取りされるダークWebとTorネットワークは同一視されることも多い³⁸⁾。しかしTorの本来の目的は追跡、監視、および検閲を回避するための通信経路の匿名化であり³⁹⁾、その主旨に沿う使い方を企業が提供していると言える。具体的にはTwitterは2022/3/1にロシアのニュースメディア (RT, Splunk) に対するアクセス制限を実施⁴⁰⁾する一方で、2022/3/8にはTor経由での閲覧をできるようにしている⁴¹⁾。またBBC⁴²⁾、Facebook⁴³⁾はウクライナ侵攻以前からTor経由でのアクセスを可能にしている。

このようにスプリンターネットに対する企業行動は多面的である。

3. 企業行動の合理性

政府規制を遵守することは企業判断として当然であり、政府がスプリンターネットを推進している場合、企業が迎合的な態度を取ることは致し方ない面がある。これに対しTor経由でのアクセスのように追跡、監視、および検閲を回避するための手段を明示的に提供することは、規制を行っている政府からは脱法・違法行為と捉えられる蓋然性が高い。このようなリスクを含む判断にはシンプルな経済合理性だけでなく各社のミッションあるいはパーパスの存在が考えられる。前節で例示したBBC、Meta、Twitter

35) Webサイトでコンテンツの一部が有料化され、対価を支払ったユーザーのみアクセスできる状態

36) <https://privacy.yahoo.co.jp/notice/globalaccess.html>

37) <https://news.yahoo.co.jp/byline/yamaguchikenta/20220201-00280146>

38) <https://jp.norton.com/blog/general-security/dark-web-darksociety>

39) <https://www.torproject.org/>

40) <https://twitter.com/nickclegg/status/1498395147536527360?s=20&t=vJIAf5m70VXm2R31T2Qaew>

41) 「Twitter、Tor経由Webサイトを開設 ロシアからも閲覧しやすく」(IT media、2022年3月9日) (<https://www.itmedia.co.jp/news/articles/2203/09/news103.html>)

42) “BBC News launches ‘dark web’ Tor mirror” (BBC News, Oct. 23, 2019) (<https://www.bbc.com/news/technology-50150981>)

43) “Facebook over Tor” (Facebook, May 24, 2021) (<https://www.facebook.com/facebookcorewwi/posts/pfbid02iXMKbNSDBJVhUkhh9JRtQt2u8W8A2kwb8AgowGUChXaTyMvex2RZW5jUmg8t8WSUj>)

各社のミッション（Twitterはパーパス）は以下の通りであり（太文字部筆者）、各社とも自社のサービスを世界中の人々に提供することを掲げている。（正確には、BBCはpurposeの具体的な記述⁴⁴⁾の中で世界への積極的関与を宣言している。）

① BBC⁴⁵⁾

Our mission is “to act in the public interest, serving all audiences through the provision of impartial, high-quality and distinctive output and services which inform, educate and entertain.”

② Meta (Facebook)⁴⁶⁾

Originally founded in 2004 as Facebook, Meta’s mission is to give people the power to build community and bring the **world** closer together. Our products empower more than 3 billion people around the **world** to share ideas, offer support and make a difference.

③ Twitter⁴⁷⁾

Twitter’s purpose is to serve the public conversation. Violence, harassment and other similar types of behavior discourage people from expressing themselves, and ultimately diminish the value of **global** public conversation. Our rules are to ensure all people can participate in the public conversation freely and safely.

4. 企業の姿勢

米国政府はイラン政府のスプリンターネットを阻害するために、監視・検閲を逃れるためのVPNツールなどを制裁リストから除外⁴⁸⁾することでイラン政府のスプリンターネットを阻害しようとしており⁴⁹⁾、前節のTorの事例も米国企業であるTwitter、Facebookにとって政府と対立するものではない。しかし、仮に自国政府がスプリンターネットを推進する規制を行っている場合、企業が明示的にこれに抗うことは難しい。

本稿1.2節で実績が述べたように分割する理由、統合する理由にそれぞれ合理的理由があり優劣を決めることはできない。しかし、民主主義国家の方向性は自らが定めるものであり、所与のものとして与えられるものではない。スプリンターネットについても、各企業自身の考えを持ち、政府方針に対して積極的に関与すべきであろう。

5. 私見：スプリンターネット

Vint CerfはInternet Access Is Not a Human RightでInternetの可能性“the ability that the Internet offers to communicate, organize and publicize everywhere, instantaneously”を称賛しつつも、あくまでもInternetは“critical freedoms like **freedom of speech** and **freedom of access to information**”を実現する手段としてのひとつに過ぎないことを強調している（Cerf [2012]、太文字部筆者）。そして、終段で“Improving the Internet is just one means, albeit an important one, by which to improve the human condition.（インターネットの改善は、人間の状態を改善するための重要な手段だがそのうちのひとつに過ぎない。【筆者翻訳】）”と述べている。

スプリンターネットの推進に筆者が覚える忌避感も、freedom of speech、freedom of access to informationに対する抑圧的スタンスにあり、この問題を単なるインターネットの変容ではなく、それがもたらす結果についてより深く議論すべきものと考ええる。

参考文献

Cerf, V.G. (2012) “Internet access is not a human right,” New York Times 4, 25-26, available at <https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html>

44) The BBC should provide duly accurate and impartial news, current affairs and factual programming to build people’s understanding of all parts of the United Kingdom and of the **wider world**.

45) “Mission, values and public purposes” (BBC) (<https://www.bbc.com/aboutthebbc/governance/mission>)

46) DAQs (Meta) (<https://investor.fb.com/resources/default.aspx#:~:text=Originally%20founded%20in%202004%20as,bring%20the%20world%20closer%20together>)

47) The Twitter Rules (<https://help.twitter.com/en/rules-and-policies/twitter-rules#:~:text=Twitter%27s%20purpose%20is%20to%20serve,public%20conversation%20freely%20and%20safely>)

48) “U.S. Treasury Issues Iran General License D-2 to Increase Support for Internet Freedom” (U.S. Department of the Treasury, Sep. 23, 2022) (<https://home.treasury.gov/news/press-releases/jv0974>)

49) 「イランでインターネットやSNS遮断、女性死亡への抗議激化受け 米政府が対抗策で抗議を支援」(BBC News Japan, 2022年9月24日) (<https://www.bbc.com/japanese/63018261?fbclid=IwAR0N-kLiHD0-iqDbLiKLdgxkDDqIdQIPvFTXL5vEWp1sk65rK4vKXysi3H0>)

情報法制研究所 理事

中央大学総合政策学部 教授

情報通信学会 常務理事

博士（国際情報通信学）

実積 寿也（じつづみ・としや）

2017 年より現職。情報通信エコシステムの事象について主として経済学の観点からアプローチ。現在の研究テーマは、ネット中立性、AI、プラットフォーム規制。著書に、『通信産業の経済学 R1』（九州大学出版会、2019 年）、『図解即戦力 通信業界のしくみとビジネスがこれ1冊でしっかりわかる教科書』（共著、技術評論社、2022 年）などがある。

一般社団法人日本ネットワークインフォメーションセンター（JPNIC）政策主幹

国際大学グローバルコミュニケーションセンター（GLOCOM）客員研究員

前村 昌紀（まえむら・あきのり）

1994 年国内大手 ISP のサービス立ち上げにネットワーク技術者として参画。ネットワーク設計運用、技術渉外を担当。以来自網に留まらない商用インターネットの運営への関与を深め、2000 年から 2016 年まで、アジア太平洋地域の IP アドレスを管理する APNIC (Asia Pacific Network Information Centre) 理事（うち、2003 年から理事会議長）、2016 年から 2022 年まで、全世界のドメイン名と IP アドレス管理を統括する ICANN (Internet Corporation for Assigned Names and Numbers) 理事を歴任。

BBIX Singapore Pte. Ltd. Growth Manager

白畑 真（しらはた・しん）

1997 年より Web ホスティング事業者にてネットワーク構築、運用、サービス企画、システム構築、運用などを担当。その後、シンガポールの Web ホスティング事業者、IX 事業者、通信事業者を経て、2018 年よりさくらインターネット入社。2022 年 4 月より BBSakura Networks、同年 10 月より BBIX Singapore に出向し、シンガポールを中心とする IX 事業の成長施策を担当。

日経 BP 日経クロステック先端技術副編集長

堀越 功（ほりこし・いさお）

2004 年から通信専門誌「日経コミュニケーション」記者として通信業界を取材。通信専門ニューズレター編集長を経て、2017 年から 2020 年にかけて日本経済新聞社企業報道部（現ビジネス報道ユニット）で通信分野を担当。2020 年から現職。近著に『通信地政学 2030』（日経 BP、2022 年）、『官邸 VS 携帯大手』（日経 BP、2020 年）。大学講師や政府委員も務める。

一般社団法人 JPCERT コーディネーションセンター 国際部部长

慶應義塾大学 SFC 研究所 上席所員

博士（政策・メディア）

小宮山 功一朗（こみやま・こういちろう）

専門分野はサイバーセキュリティと安全保障、サイバー空間の規範、インシデント対応組織 CSIRT など。JPCERT コーディネーションセンターの国際部部长として、セキュリティインシデント対応に従事する。著書に、『偽情報戦争 あなたの頭の中で起こる戦い』（共著、ウェッジ、2023 年）などがある。

東日本電信電話株式会社 ビジネス開発本部 担当部長

一般社団法人 JPCERT コーディネーションセンター 理事

情報セキュリティ大学院大学 客員研究員

水越 一郎（みずこし・いちろう）

パソコン通信黎明期の商用サービス（ASCIINET）でシステム運用・開発を担当。

その後、ISP 数社（ネットワーク情報サービス、東京インターネット）を経て 1997 年 NTT に入社、OCN の運用に携わる。2006 年 10 月から東日本電信電話株式会社、主に FLET'S 関連サービスの運用・開発に従事。2005 年 4 月から JPCERT 理事に就任。