# 第５部

# 特集5 海賊版サイトに関するブロッキングの法制化に関する活動

江崎 浩

## 第１章　はじめに

「エンド・ツー・エンド」とは、インターネットにとって、そして、インターネットの遺伝子にとって、非常に重要な特性の一つです。ネットワークの端（エンド）にあるユーザの機器が知性を必要とする高度な処理を行い、ネットワークのなかにある機器が単純な処理のみ（stupid）を行うような構造にすることです。ユーザの機器がその機能と性能を向上させることで、イノベーションを持続させるとともに、それによってユーザたちがグループやコミュニティを自由に形成することを目指しています。エンド・ツー・エンドに基づいたシステムの設計は、以下のように整理することができます。

## 第２章　ユーザ間での機能はユーザの責任

インターネットのインフラは、多様なコンテンツを共通のデジタル小包であるIPパケットを用いて目的地まで届ける機能を提供します。インターネットが大規模化しても、IPパケットの転送を担当するルータの負荷が急増しないように、できる限りシンプルに全体のシステムが設計されています。ルータは、IPパケットを受け取ったら、次の中継地のルータ（あるいは目的地のコンピュータ）に転送する機能だけと実行します。基本的には、これ以外の仕事はしません。IPパケットを転送する際には、ルータは送信元のコンピュータがどれなのかをまったく気にせず、IPパケットに格納されている宛先の情報（Destination IP Address）だけを頼りにして、最も適切と考えられる隣接のルータに転送します。

このように、ルータは「送信元のコンピュータ」と「受信先のコンピュータ」の間でのIPパケットの転送がしっかり行われたかどうかには、いっさい責任を負う必要がありません。ルータはユーザ間での通信を管理することなく、隣のルータから受け取ったIPパケットを、また隣のルータに中継するだけでよいのです。このような単純なサービスが、最大限の努力、すなわち、ベストエフォートで実行しているのです。したがって、ユーザ間で正確なあるいは良好なデータ通信は、始点のコンピュータと終点のコンピュータ、つまり端（エンド）のコンピュータが持つという考え方となっています。つまり、インターネットのインフラがから提供するサービスは、IPパケットをたんに宛先のコンピュータに送信するだけということになります。

ユーザのなかには非常に高度な通信機能を要求する・提供する者もいれば、そうでない人もいるので、どのような機能をエンドのコンピュータ間に提供するかはユーザ（＝エンド）のコンピュータに完全に任せるということになります。そのために、インターネットのインフラは、エンドのコンピュータ間に「透明性」を持ったIPパケットの転送サービスの提供が求められます。透明性とは、受け取ったIPパケットに修正や変換などをまったく加えないという意味になります。

## 第３章　透明性が持続的進化を可能にした

インターネットでは、ルータが透明性を持ったIPパケットの転送を行うことで、各ユーザ（＝エンド）による多様なサービスが自律的かつ分散的に実現されることになりました。ここでいう「エンドのコンピュータ」とは、各種プロバイダからサービスを提供されるユーザのコンピュータだけではなく、そうしたサービスをユーザに提

供するためにサーバのコンピュータも指します。つまり、ウェブサーバや電子メールサーバのように、プロバイダのなかで稼働しているサーバのコンピュータもエンドのコンピュータなのです。

さて、ファイアウォール・ルータは、ユーザにとって危険と判断されたIPパケットを選択的に廃棄して、エンドのコンピュータには意図的に転送しない機能を持っています。いわば透明性を持たないルータと言えるでしょう。とはいえ、どのようなポリシーで、またどのようなアルゴリズムで転送しないIPパケットが決められるのか、それを利用するユーザは知っておくべきでしょう。インターネットのユーザが情報の送受信を自由に行うためには、「通信の秘匿性」が保証されることが重要であり、ファイアウォール・ルータの適用にあたっては、それをどこまで守る必要があるのかということを考慮しなければなりません（つまり、ファイアウォール・ルータによるサービスを提供する事業者は、通信の中身を知ることになっても、その内容を秘匿しなければならない）。

## 第４章　ブロッキングとフィルタリング

2018年4月に、日本政府の知的財産戦略本部・犯罪対策閣僚会議で国内のインターネット接続事業者（以下、接続事業者）に対し、海賊版サイトへのサイトブロッキングの実施を促す緊急対策が表明され、その後、これに呼応する形で一部の接続事業者から、DNSを用いたサイトブロッキングの実施の方針が表明されました。

DNSブロッキングそのものが、通信の秘匿性に反する可能性が非常に大きいことに加えて、主要ISP・キャリアによるDNSブロッキングによるアクセス遮断は、インターネットの重要な遺伝子の機能である「エンド・ツー・エンド」と「通信の透明性」を棄損してしまうことになります。どのエンドノードからのどのIPパケットの受信を拒否するのか、どのIPパケットをどの宛先のエンドノードには送信しないのかの意思決定を行うのは、基本的には、エンドノードのユーザでなければなりません。エンドノードのユーザは、その責任とその権利を持っているのです。もちろん、この作業を誰か（他のコンピュータ）に、お願いしてその実行を移譲することは可能です。重要なことは、この作業実行の移譲先の選択肢が複数存在するようにすることと、移譲の意思決定がエンドノードのユーザによって行われることです。これが、「フィルタリング」になります。

一方、「ブロッキング」は、エンドノードのユーザには、上述の意思決定の権利を剥奪し、インターネットのインフラ（具体的にはISPやキャリア）が勝手に、エンドノードのユーザの意思を確認することなく、一律的に、指定された条件に合致するIPパケットを廃棄する運用になります。すなわち、「ブロッキング」は、IPパケットの送受信の制御はエンドノードが実施し、インターネットのインフラは単純な透明なIPパケットの転送のみを行うというインターネットのエンド・ツー・エンドの原則と通信の透明性の両方が棄損することになってしまうのです。

つまり、DNSによりサイトアクセスのブロッキングの実施は、インターネットの重要な遺伝子の機能を無効化してしまうことになると考えられるのです。

3つのサイトを総理と総理官邸が名指しで、緊急対策として対応すべきとの意見に対応して、DNSブロッキングを用いた該当サイトへのアクセス遮断を行うことをNTTグループが表明しました。その後、DNSブロッキングを行うことを前提とした議論が行われているように思え、大変な違和感を感じてしまいます。DNSブロッキングそのものが、通信の秘匿性に反する可能性が非常に大きいことに加えて、主要ISP・キャリアによるDNSブロッキングによるアクセス遮断は、日本国内のユーザに対して小さくない程度の効果はあるとしても、DNSブロッキングの回避方法が多数存在すること、さらに、DNSブロッキングの実施により、インターネットシステム、DNS運用者コミュニテイー、さらに、エンドユーザへの悪影響の議論が十分には行われていません。筆者は、理事を務めるISOC（Internet Society）が出したアクセス遮断に関するレポートをもとに、意見書の提出を行いました。

（1）違法コンテンツ提供者、ユーザともに、アクセス遮断を回避する方法を容易に取れる
（2）オーバーブロッキングの可能性がある

(3) ISP、DNS運用者への人的・財務的経費が発生する

さらに、

ア. オーバーブロッキングに対して、国、ISP、ブロッキングの要請者に対する損害賠償訴訟の可能性

イ. エンドユーザ(特に遮断回避策を行った自覚のある青少年)が、有罪意識から脅迫を受ける可能性の増大

ウ. DNS運用者の減少

エ. 有効な対策は、エンド(提供サイトとユーザ)での対策

特に、インターネットは、関係者間でのコンセンサスの形成に基づいた「自律分散協調」がその重要な遺伝子であり、その持続的発展を支えてきた。DNSコミュニテイーでのコンセンサス形成が行われず、政府による議論に基づいた運用者への一方的な指示・命令は、DNS運用者のサービス継続を阻害する結果を産む可能性を持ちます。多様で多数のDNS運用者の減少は、DNSサービス提供者の寡占化を進め、特に、通信の秘匿性の制約を持たないコンテンツプロバイダによる情報収集(特にこれまで彼らが取得することが難しかった下位のIPレイヤでのアクセス履歴情報)の寡占化が進む危険性を持っているのではないでしょうか。つまり、winner takes allの加速です。また、多様な運用者による分散環境と協調環境が縮退してしまうことが危惧されます。多様性と多様な関係者間での協調が、インターネットの環境変化に対する堅牢性と持続性の大きな特性であり遺伝子なのです。今回のDNSブロッキングの実施を前提にした議論は、インターネットの重要な一つの遺伝子を削除しようという方向性に思えます。

(注)「ブロッキング」と「フィルタリング」の区別を正確に行う必要がある。「フィルタリング」は、エンドユーザの「許諾・承認」の手続きを持っており、エンドユーザに「選択権」という意味での「自由」を提供している。一方、「ブロッキング」は、エンドユーザによる選択権も、ブロッキングを拒否する自由もないものである。

## 第5章　検閲社会への懸念

小説「1984」で提示された世界は、市民のすべての活動が情報ネットワークとIoTによって政府に検閲・把握され、市民の自由とプライバシーが奪われ、恐怖政治の社会です。すべてのデジタル機器がオンライン化・ネットワーク化され、これを用いて、政府がすべての国民の行動・言動を検閲し、政府の意向に沿わない市民は強制的に拘束・逮捕され、措置が行われるというものです。多くの人が、このような社会が、インターネットとIoTさらにビッグデータ、人工知能によって実現されそうだという危惧を持ち始められたような気がします。実際、その可能性は、否定することはできないでしょう。しかし、すべての技術には、良い面と悪い面があります。諸刃の剣(Double Edges)です。

最近は、逆に、インターネットが、この「1984」の世界の実現を阻止するものではなか、との意見が出てきています。そのためにも、「エンド・ツー・エンド」と「通信の秘匿性(透明性)」を維持して、政府による検閲が行われないようにしなければなりません。エンド・ツー・エンドによる通信の暗号化・認証は、そのために必須のものとなりますし、特に政府による「ブロッキング」は、回避されなければなりません。

一方、通信の内容をチェックすることができないのは、テロリストのような社会悪の人達の通信を把握・阻止することを困難にしてしまいます。我々は、ネットワークの利用者が、自律分散協調して、このような、活動を検出するような仕組みを作る必要があります。一番危険なのは、このような仕組みが構築・確立されていないので、「政府による検閲機能が正当化される」ことであると認識すべきなのです。「通信の秘匿性」は、日本国憲法にも、米国憲法にも明記されている、基本原理なのですから。

2018.09.12

**著作権法違反を理由とする接続遮断措置(サイトブロッキング)についての意見表明**

WIDEプロジェクトは著作権法違反を理由とする接続遮断措置(サイトブロッキング)について、以下を表明します。

・海賊版サイト対策としてのサイトブロッキングは、グローバルなインターネット、及び、すべての社会産業活動に影響を及ぼすものであり、その導入・実施に反対します。
・海賊版サイトに対する総合的な対策を進めるため、本件に関するすべての利害関係者とインターネット業界が産業の発展を目的とした、民間での議論を進める体制を整えるべきであり、その場の形成と参加に協力します。
・正規版の流通促進に寄与する技術の検討・開発・検証活動の推進に協力します。

政府は、2018年4月13日の知的財産戦略本部・犯罪対策閣僚会議で国内のインターネット接続事業者(以下、接続事業者)に対し、海賊版サイトへのサイトブロッキングの実施を促す緊急対策を表明しました。その後、これに呼応する形で一部の接続事業者が、サイトブロッキングの実施の方針を表明しています。

インターネットは、各国の経済、行政・司法など、すべての社会産業活動を共通インフラとして支援している、グローバルな基盤です。サイトブロッキングの導入・実施はインターネットの破壊への第一歩であり、インターネットの破壊は、日本はもちろん、周辺の国々のすべての産業活動に影響を及ぼすことになります。

インターネットでは通信の制御は通信当事者が行い、ネットワーク上のシステムは単純な中継・転送を行うという、エンドツーエンド原理が基本です。また、接続事業者におけるサイトブロッキングの実施は通信当事者の意思に反して通信の構成要素を知得・窃用するものであり、通信の秘密を侵害するおそれがあります。

海賊版サイトの問題は、速やかに解決されるべき喫緊の問題です。しかし、今回の政府の緊急対策の表明と、それに伴うインターネット上の海賊版対策に関する検討会議(タスクフォース)における検討の進行により、「ブロッキングを前提にしている」とみられてしまい、本来、連携・協力して解決策を見出すべき関係者間に、非建設的な対立関係を生み出してしまいました。

インターネットではこれまで、マルチステークホルダーによるオープンな議論[*1]と合意により、全体方針が決定されてきました。WIDEプロジェクトは、グローバルな関係者間でのオープンな議論と合意による今後の持続的発展を実現するための有効な解決策がもたらされるよう希望し、かつ、最大限の努力を進めてまいります。

以上

---

＊1　ISOC (Internet Society)
Internet Society Perspectives on Internet Content Blocking: An Overview:
https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/
IETF (Internet Engineering Task Force)
RFC 7754 - Technical Considerations for Internet Service Blocking and Filtering
https://tools.ietf.org/html/rfc7754