

ブロッキングによるインターネットへの影響

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)

◆JPNIC の提言(要旨)

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)における主な論点・スケジュール(案)資料によると、タスクフォースでは、法制度整備に関わる論点として、“ブロッキングに関わる制度整備を行う場合の論点”とある。この論点について、知的財産に関する権利は適切に保護されなければならないことについては明らかではあるものの、保護するための手法としてブロッキングを前提とした検討を行うことは、ブロッキング以外にも様々な手法が存在する点を考慮すると、検討範囲の設定が不十分である。

また、仮にブロッキングに関する検討が主要検討事項であったとしても、ブロッキングによる効果とインターネットへ与える副作用を論点としていないことは、必要かつ十分な検討を行っているものではない。

JPNIC は、インターネットの安定運営に資することを理念に掲げ、1991年から25年以上に渡り事業を行ってきた。そのような観点から、本稿では、ブロッキングとその連鎖によるインターネットへの影響について情報共有する。

初めに、1.ブロッキングがもたらすインターネットへの影響の分析、としてブロッキング実施後のインターネットの状況を段階的に説明し影響を指摘する。

- (1) 今回政府から要請のDNSによるブロッキングとその効果が限定的であること
- (2) ブロッキングの効果を維持するための想定される追加のブロッキングについて
- (3) 追加のブロッキングにとどまらない更なるブロッキングの連鎖とその影響について

次に、2.当センターの見解、として、

- (1) 一般ユーザの積極的な意思を持ってアクセスすることが想定される海賊版サイトに対してのブロッキングは効果的だとは言えないこと
- (2) 不法コピーを送信可能化し、それによって利益を得ることが本件の本質であるので、その本質にメスを入れる手段が最大限検討される必要があること、
- (3) ブロッキング法制化ばかりをこのタスクフォースの論点とするべきでない、

以上を当センターの見解として、提言する。

◆JPNIC の提言(詳細版)

1. ブロッキングがもたらすインターネットへの影響

(1) DNS ブロッキングとその効果の限定について

今回、政府によって要請されたブロッキングは、通信事業者がエンドユーザへ提供する DNS キャッシュサーバ¹にて行われる。そのため、ユーザが通信事業者の DNS キャッシュサーバを名前解決に利用しない場合、効果はない。2018 年現在、DNS キャッシュサーバは、基本的にインターネットへ接続するユーザ、企業は誰でも構築でき、ユーザは、利用する DNS キャッシュサーバを任意に選択できる。

通信事業者の DNS キャッシュサーバにてブロッキングを行っても、ユーザは自ら DNS キャッシュサーバを運用すること、または、ユーザは第三者が提供する DNS キャッシュサーバの利用を選択すること、によりブロッキングは無効化される。

(2) 想定される追加のブロッキングについて

DNS ブロッキングの効果を維持するためには、ユーザに対し通信事業者が提供する DNS キャッシュサーバのみを使うように強制する必要があるが、そのような制限には数多くの回避策があるため追加のブロッキング施策の実施が懸念される。

その代表的な施策が、Outbound Port 53 Blocking² (OP53B) である。DNS の通信では、TCP/UDP Port 53 を使用する。OP53B では、一般ユーザからの TCP/UDP Port 53 を宛先とする通信を、通信事業者の DNS キャッシュサーバのみに制限し、それ以外を遮断することにより、ユーザによるキャッシュサーバの構築もしくは第 3 者により提供されている任意の DNS キャッシュサーバの選択を不可能とするものである。

先行事例として、迷惑メール対策としての Outbound Port 25 Blocking³ (OP25B) が知られている。OP25B では、理由を問わず OP25B を望まないユーザに対し適用を除外する仕組み (Opt-out) などが整備、提供されている。

OP53B にも Opt-out が提供される場合、ユーザ自ら DNS キャッシュサーバを運用すること、ユーザは第三者が提供する DNS キャッシュサーバの利用を選択することは維持され、プロ

¹ JPNIC, DNS キャッシュ, JPNIC ニュースレター, No.51, <https://www.nic.ad.jp/ja/newsletter/No51/0800.html>

² 山口崇徳, IP53 の概要, Internet Week 2014, D1 DNSDAY, P6, <https://www.nic.ad.jp/ja/materials/iw/2014/proceedings/d1/d1-yamaguchi.pdf>

³ JPNIC, OP25B(Outbound Port 25 Blocking)とは, インターネット用語一分解説, <https://www.nic.ad.jp/ja/basics/terms/OP25B.html>

ッキングの無効化は継続される。OP53B に Opt-out が導入されない場合においても DNS over TLS/DTLS、DNS over HTTPS (DoH)⁴の標準化、実装および第3者による試験的提供が行われており、Port 53 を閉じるだけではブロッキングが成立しない未来を想定することはブロッキングの効果を検証する上では重要である。

ここまで、予測可能な将来像として DoH のブロッキングまでを論じた。これ以上の予想については現実味の薄れる議論であることは承知の上で申し上げますと、DoH の追加ブロッキング以後も続くブロッキングの連鎖により、新たな名前解決手法の創出の結果、表からは見えづらい名前解決の地下化、潜伏化など、有害サイトへの本質的な対策がさらに困難になってしまうことを懸念する。

加えて、残念ではあるが、ブロッキング開始後においてもブロックされたサイトの閲覧を欲するユーザは、回避策の適切性や自らへの影響を理解せず、安直に、いわゆる"ブロッキング回避のためのアプリ"等をインストールする行動を促すことに繋がる。そのようなアプリでは、ブロッキングを回避するだけでなく、期待される機能に加えて、アプリに悪意が混入されていることも想定され、ユーザ保護の観点からも慎重な対応、注意喚起が必要であることを申し添える。

(3) 追加のブロッキング後に想定されるブロッキングの連鎖について

DNS over TLS/DTLS では Port 853 を使用するため、Outbound Port 853 Blocking (OP853B) による追加のブロッキングが想定される。一方、DoH では、DNS の通信に HTTPS を利用して行うため、DoH では通常の Web 閲覧データを運ぶ HTTPS と DNS over HTTPS の判別を行うことが暗号化により困難となる。結果、DoH 環境下でのブロッキングは、特定の IP アドレス宛通信を DoH と乱暴に想定し、IP を基にした追加ブロッキングに繋がりオーバーブロッキングが多く発生することが懸念される。最終的には、DoH を制御するため、Outbound Port 443/80 Blocking (OP443/80B) による追加のブロッキングが実行される。エンドユーザの通信は、通信事業者の中継システムの経路が強制され、インターネットの利便の著しい低下を招く。

このように、Web 上のインターネットサービスが必要とする自由な通信が損なわれることは、結果としてインターネットを活用した新たなサービスやイノベーションの誕生の機会を

⁴ JPNIC, DNS over HTTPS とは、インターネット用語一分解説, <https://www.nic.ad.jp/ja/basics/terms/dns-over-https.html>

妨げられることにつながり、インターネットの安定した運営、持続的な発展が阻害⁵されると予測する。

2. 当センターの見解

(1) ブロッキングについて効果は少ないことの総括

本稿において当センターは、意思を持ってアクセスするユーザに対してブロッキングを実施した場合にそのようなユーザが簡単に利用可能な回避策が存在し、実施した瞬間から効果が大きく薄れ始め、さらにはこれまで慎重に行われてきたブロッキングをも無効化してしまう懸念を主張する。あわせて、ブロッキングの効果を維持するためのブロッキングの連鎖、濫用はインターネットの存在自体を揺るがしかねないことにも懸念を表明する。

(2) 対策の本質

当センターは検討すべき事項として、不法コピーを送信可能化し、それによって利益を得ることが本件の本質であると認識している。このような不法なマネタイズを可能としているエコシステムの各部分をつまびらかにしてその対策をとる手段を検討すべきである。

(3) 本 TF での論点についての提言

結論として、インターネットを破壊しうるブロッキングは、可能な限り回避すべきと考えており、本タスクフォースにおいても、ブロッキング法制化のみを論点とするべきではない。

以上

⁵ Internet Society, Internet Society Perspectives on Internet Content Blocking, <https://www.internetsociety.org/doc/internet-content-blocking>