資料１０

サイトブロッキングの有効性に関する議論について

株式会社ドワンゴ
取締役 CTO 川上量生

問題提起したいポイントについて

これまで海賊版対策タスクフォースは、6 月 22 日開催の第 1 回から 7 月 25 開催の第 4 回までと、8 月 10 日の勉強会を合わせて、5 回にわたって議論を行ってきた。
その中でサイトブロッキングの有効性について疑問であるという内容を含む資料が、JPNIC の前村氏と JAIPA の立石氏の両委員より、前村氏については第 1 回、第 3 回および勉強会において合計 3 点、立石氏については、第 4 回の合計 1 点が提出されている。
しかしながら、特に前村氏提出の資料において、「サイトブロッキングは効果がない」という一般的な結論と、その技術的な根拠が、個別の各論として示されているが、なぜ、個別の各論が、総体としてブロッキングが効果がないという結論になるのかについては、論理的な説明はされていない。例を挙げると、前村氏提出の資料において、費用がかかったり、オーバーブロッキングなどの副作用についての記述のほとんどは、今回、主に検討されていると考えられる海賊版サイトに対する DNS ブロッキングには当てはまらないものばかりであり、回避策についても限定的なものである。また、その他、副次的効果や弊害について記載されているものはいくつかあるが、弊害があるということは事実であったとしても、「効果がない」という根拠にはなりえない。
実際には前村氏、立石氏の両委員も指摘されているように、サイトブロッキングには、さまざまな種類があり、それぞれ問題点と回避策が存在している。
サイトブロッキングの実施にあたっては、効果的であり、一般ユーザーの多くは選択しないであろう回避策しかないようなものであることを大前提として、費用や副作用なども考慮して、実施にかかるプロバイダの負担が、長期的に維持可能かなどの観点から現実的な手法を選択すべきである。
ブロッキングはアクセス自体を制限する手法であるから、一義的には海賊版サイト対策として効果があるのは自明である。ただし、インターネットにおいては、ほぼ、すべてのブロッキングの手法に対して、回避手段が存在するというのも、また、事実だろう。従って、効果があるかないかを議論するのであれば、回避手段があるかどうかではなく、その回避手段をとれるユーザー、もしくは取る決断をするだろうユーザーの割合がどれくらいかを見積もることが本筋であると考える。

具体的に議論すべきと思われるテーマ

（１）OP53B の採用について

採用されるサイトブロッキングの手法については児童ポルノ同様に DNS ブロッキングであるということを前提とする。
その場合、前村委員、立石委員の資料でも指摘されているように、一般ユーザーが DNS サーバーを変更する、という技術的には一般ユーザーでも簡単にとれる回避手段が存在する。
これを防ぐ手段として、プロバイダ以外の DNS サーバーを設定することをできなくする OP53B という手法が存在する。これは迷惑メール対策として導入されている OP25B の設定をポート番号を変更するだけであり、プロバイダにとって実現は容易である。

DNS ブロッキングに OP53B を組み合わせた場合には、立石委員提出の資料でも指摘されているように考えられる回避策は次の 4 点ぐらいであり、一般のユーザーの多くがとるとは思えないものしか存在しない。

① ユーザー自身が DNS サーバーを設置する。
② VPN あるいは DoH でブロッキングを行っていない Public DNS サーバーに接続する。
③ ブロッキングを行っていない Public DNS サーバーが設定されている無線 WiFi ルーターなどを利用する。（市販品が存在する）
④ ブロッキングを回避するツールまたはアプリを利用する。（これも上記同様に Public DNS サーバーを利用する）

DNS ブロッキングと同時に実施を検討すべきである。

（２）Public DNS サーバーについて

DNS ブロッキングにおいて、現在はユーザーが接続しているプロバイダの DNS サーバーを対象としているが、DNS サーバーはプロバイダ以外にも設置している場合がある。
企業または個人が自己の使用の目的のために設置している DNS サーバはやむを得ないとしても、一般の利用者の多い Public DNS サーバに対しては、ブロッキングの対象とすべきである。
これをおこなえば上記の立石氏の資料でも指摘されている②③④の 3 点の回避策についても、ほぼ、防ぐことが可能になる。
もちろん、すべての Public DNS サーバーに対してブロッキングを実施してもらうことは不可能である。ただし、現実的には主に利用されている Public DNS サーバーの数は限られている。
具体的にはクラウドフレアの 1.1.1.1 とグーグルの 8.8.8.8 を対象とすべきである。上記、②③④の回避策においても、ほぼ、どちらかが設定されている。
これらは海外の DNS サーバであり、日本の行政、または司法による命令に従わない可能性がある。だとしても、彼らが、日本ユーザーからのアクセスに対して日本の法制度に従うか、そうでないかの立場をはっきりとさせる踏み絵としても、国内の DNS サーバー同様にブロッキングをおこなうことを要請すべきであると考える。

（３）リーチサイトの定義について

現在、リーチサイト違法化のための議論が進んでいると認識しているが、上記の③④の回避策を自覚的に提供する業者は、海賊版コンテンツへのアクセスを容易にする手段により人気を集めようとしている点では、リーチサイトの仕組みと構造的には変わらない。
リーチサイトの違法化とは、著作権侵害の幇助をおこなうことを違法化することであると解釈しているが、であるならば、③④についても対象となってしかるべきであると考える。
リーチサイト違法化にあたっては、リーチサイトというウェブサイトだけではなく、著作権侵害コンテンツへのアクセスを容易にするツールやアプリについても、対象となるように留意していただきたい。

以上