

「インターネット上の海賊版対策に関する検討会議」 中間まとめ（案）（2018年10月15日）への意見書

2018年10月15日
カドカワ株式会社
代表取締役社長 川上 量生

中間まとめに現時点からの変更を求めるものではないが、ブロッキングの技術的な問題点の記述について、実際以上に困難であると誤解を与える表現がみられるため、以下にまとめる。

■ 1. DNS ブロッキングにおけるオーバーブロッキングの可能性について

・該当箇所：P89

（6）ブロッキングの要件等について（「イ アクセス制限（ブロッキング）の方法」）

また、アクセス制限（ブロッキング）の方法（上記④について）には「DNS ブロッキング」「URL ブロッキング」「IP ブロッキング」「DNS と URL のハイブリッドブロッキング」があるところ、各方法の特徴は下記のとおりである。

○DNS ブロッキングは、ユーザーがリクエストした URL に対して、偽の IP アドレスを返すことで該当サイトへの接続を遮断する方式であり、比較的低いコストで実施できるが、オーバーブロッキングが発生する可能性が高く、簡易な回避策もあるというデメリットがある。

・当社からの意見

DNS ブロッキングは、他のブロッキングに比べて、オーバーブロッキングは発生しないのではないか。

この表現は JPNIC 前村委員提出の資料から抜粋された文言だと思われるが、原典と思われる 8 月 10 日の勉強会において配布された Internet Society が作成した英文資料によると DNS ブロッキングでオーバーブロッキングが発生する理由として、facebook.com を例示して、侵害コンテンツと同じアドレスに侵害していないコンテンツが存在した場合を挙げている。これは漫画村などのようにサイト全体がほぼ海賊版で占められていると考えられるサイトが、今回の議論の対象になっていることを考慮すると、当てはまらない記述である。

■ 2. IP ブロッキングにおけるオーバーブロッキングと割り当てについて

・該当箇所：P89

（6）ブロッキングの要件等について（イ アクセス制限（ブロッキング）の方法）

IP ブロッキングは、該当するサーバーの IP アドレスをルータや専用装置で遮断する方式で、回避策がないとされている。だが、一般的に複数のサイトが同じ IP アドレスを使用しているため、オーバーブロッキングが発生する可能性が高い。また、IP アドレスの割り当ては頻繁に発生するため、通信障害を引き起こす可能性が高く、実際に導入することは難しいとされている。

・当社からの意見その 1

「オーバーブロッキングが発生する可能性が高い」との指摘があるが、これは CDN やレンタルサーバ（バーチャルドメイン）等を利用している場合に限ると考えられる。このため、「オーバーブロッキングが発生する場合がある」等の表現のほうに誤解を招かない。

また、漫画村レベルの大型海賊版サイトが DHCP による IP アドレス付与をされるようなインターネット接続を行うことは非現実的であるため、そもそも「オーバーブロッキングが発生する」という指摘には疑義がある。

・当社からの意見その2

「通信障害を引き起こす可能性が高く」との指摘があるが、迷惑メール送信サーバ対策においてはIPアドレスブロッキングが有効な手段の一つとして実施される場合がある。

迷惑メール送信サーバの送信元として用いられたIPアドレスは、「悪質行為がなされているIPアドレス」としてIPアドレス評価事業者により分類され、ブラックリスト入りする。このブラックリストを元に通信事業者は迷惑メール送信サーバ対策としてIPアドレスブロッキングを含めたアクセス制限を行うことがある。

前記のとおり「IPアドレスブロッキング」はすでに世界中で発生しており、本論点において特有の事象ではない。そのため、本論点特有の問題ではない以上、問題提起としては不相当だと考える。

以上