印刷業界の新技術情報を三美印刷がお届けするメールニュース
sanbi-i-com (No.170)

海賊版サイト対策の動向 ②

ブロッキング法制化は棚上げ

前回ご紹介した 2018 年 4 月の漫画村の閉鎖をきっかけに海賊版対策の手段として大いに注目されたサイトブロッキング(接続遮断)ですが、法制化は棚上げとなっています。

1. 棚上げに至った経緯

今国会(第 201 回通常国会)で審議中の著作権法の改正案には「リーチサイト規制」と「ダウンロード違法化の対象拡大」という二つの海賊版対策が盛り込まれています(これらの内容については、次回以降の sanbi-i-com で取り上げるつもりですが、今回は割愛させていただきます)。このように海賊版対策のための法整備が進められている一方で、サイトブロッキング(接続遮断)の法制化は頓挫して棚上げとなっており、当面、実現の見込みはありません。こうなった経緯は以下の通りです。

●法制化への機運が高まる

漫画村が猛威を振るっていた 2018 年 4 月、政府は「法整備が行われるまでの臨時/緊急の措置として、ISP(プロバイダ)の自主的取組としてブロッキングを行ってほしい」という要請を出し、一部の ISP が応じる姿勢を示しましたが、ブロッキングは実際には行われませんでした。しかし、これにより「事実上ブロッキングが功を奏した(閉鎖をもたらした)」という評価と「きちんと法制化しよう」という機運が高まりました。

●検討会議で意見取りまとめできず

2018 年 6 月～10 月に、政府・知的財産戦略本部主催の有識者による検討会議(正式名は「インターネット上の海賊版対策に関する検討会議」)が計 9 回開かれ、ブロッキングの法制化も主要議題の一つとして議論がなされましたが、賛否両論が対立し、委員 18 名中の 9 名から反対の意見書が提出されるなどもあって、意見の取りまとめができませんでした。この結果を受け、政府はブロッキングの法制化を当面断念することとなりました。

●主な反対理由

反対派が挙げた主な反対理由は、大まかに言って以下の三点です。1)と2)の内容は、次項以降でご説明いたします。

1) 違憲(憲法 21 条違反)の疑いがある
2) 抜け道があり、海賊版にアクセスできてしまうため、効果は限定的
3) 他にもできる対策があるのに実施していない

2. 違憲の疑いとは

憲法第 21 条の②の通信の秘密の侵害に当たる疑いです。条文は以下の通りです。

> **第 21 条 ①集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。**
> **②検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。**

ブロッキングは、ユーザがどこにアクセスしようとしているのかを ISP がチェックして、該当サイトであればアクセスを遮断します。これは通信の秘密侵害の三類型とされる「知得」「窃用」「漏洩」の「知得」と「窃用」に当たるので違憲だとする見解です。

異論もあります。通信の秘密侵害の一般的な定義といえば、「第三者が」知得、窃用すること、または「第

三者に」漏洩することですが、ブロッキングは ISP とユーザの間だけで完結するので、第三者は情報を知得しません。この見方に立てば、ブロッキングは通信の秘密侵害には当たりません。

ブロッキングで警戒すべきは、21 条-②の通信の秘密よりもむしろ、同じ 21 条の①の「表現の自由」の方でしょう。違法でも何でもないサイト、例えば政府批判の意見を載せているサイトを、政府が恣意的にブロッキング対象にするといった乱用、悪用がなされれば、それこそ表現の自由の侵害であり、重大な憲法違反になるからです。従って、ブロッキングを法制化するならば、対象を明確に限定し、間違っても恣意的な拡大ができないようにしておくことが求められます。

3. ブロッキングの仕組みと限界

反対理由2)の「抜け道があるので、効果は限定的」に対して、賛成派は「抜け道があっても、カジュアルなユーザには効果がある」「海外の実施例では効果が出ている」などと反論していますが、効果の大小はさておき、現状ではどのようなブロッキング手法を使おうと抜け道があるのは事実です。

ブロッキングに関する Internet Society 日本支部による解説記事「海賊版サイトをブロッキングするための 5 つの手法(その仕組みと限界および問題点)」(URL は下記)では、タイトルにある通り、以下の5つの手法が紹介されています。

https://internet.watch.impress.co.jp/docs/special/1128898.html

1) 検索エンジンからの除外
2) **DNS ブロッキング**
3) IP ブロッキング
4) URL ブロッキング
5) DPI によるブロッキング

このうち、先述の検討会議が主に想定していた手法は、児童ポルノ対策で既に実施されている 2)の DNS ブロッキングです。海賊版サイトのドメイン名を xxx.com とし、その IP アドレスを 255.255.255.255 とすると、DNS ブロッキングなしとありの場合の違いは以下の通りとなります。**赤文字ゴシック体**の所がポイントです。

＜ブロッキングなしの時の流れ＞

①ユーザがブラウザで xxx.com を入力
②ISP の DNS(Domain Name System)サーバは
xxx.com を 255.255.255.255 に変換し、ユーザに回答
③ユーザ(ブラウザ)は 255.255.255.255 を要求
④ISP のルータは 255.255.255.255 に接続し、ブラウザに海賊版サイトが表示される

＜DNS ブロッキングありの時の流れ＞

①ユーザがブラウザで xxx.com を入力
②ISP の DNS サーバは;
・xxx.com の **IP アドレスを返さない、もしくは**
・xxx.com を**ダミーの IP アドレス** 255.255.255.000 **に変換しユーザに回答**
(以下、ダミーの IP アドレスの場合)
③ユーザ(ブラウザ)は 255.255.255.000 を要求
④ISP のルータは 255.255.255.000(警告画面用サーバ)に接続し、ブラウザに警告画面が表示される

DNS ブロッキングの抜け道としては、簡単な方法だけを挙げますと、以下があります。

●ユーザが対象サイトの IP アドレスを知っていれば、DNS を使わずにサイトに直接アクセスできてしまう
●サイト側は、ドメイン名変更で回避できる

DNS ブロッキング以外の手法の仕組みと限界(抜け道)についても知りたい方は、上記の解説記事のサイトをご覧ください。

(第 170 回: 2020 年 5 月 13 日)