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.172)

海賊版サイト対策の動向 ④

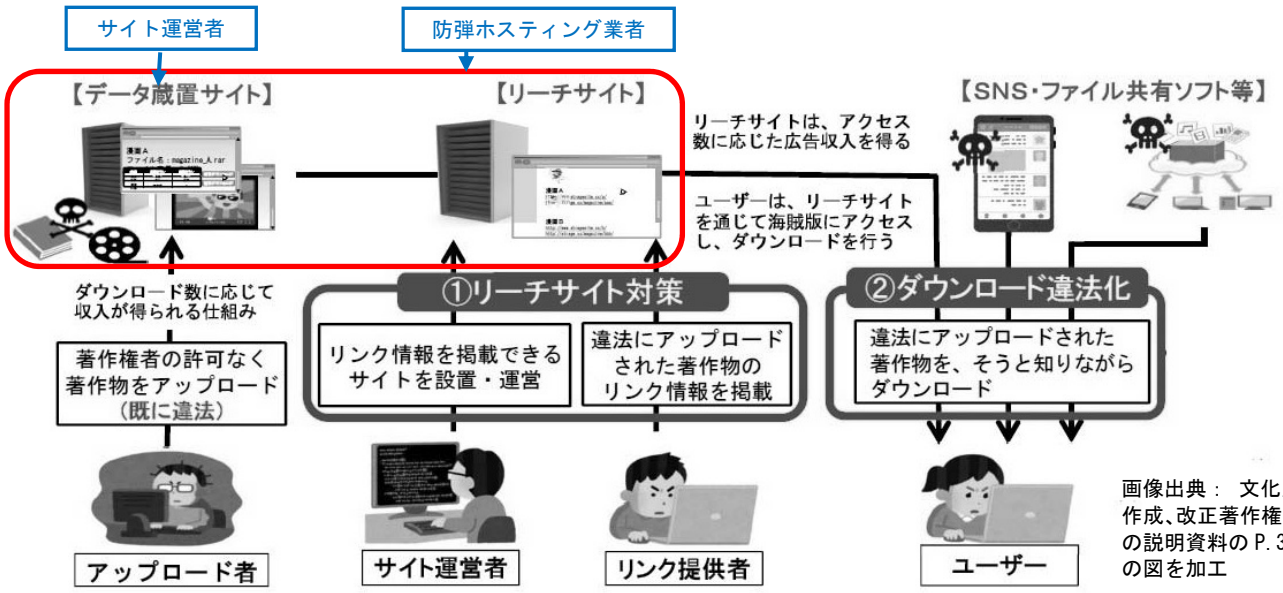
防弾ホスティング

海賊版サイトのサーバの多くは海外にあり、個人情報保護の名目でユーザー情報を開示しない防弾ホスティングで守られているため、サイト運営者を特定するのは容易ではありません。

1. 海賊版対策のイメージ図に防弾ホスティングを追記

先の通常国会で成立した改正著作権法により、データ蔵置サイトだけでなくリーチサイトも10月1日以降は明確に違法となります。今まで「合法だ」と言い張っていたリーチサイトの運営者達を、彼らがサイトを続けるならば捕まえて刑事罰を科すこともできるようになるのですから、海賊版対策にとって大きな前進です。

とは言え、この手のサイトの多くは後述の防弾ホスティングで守られているため、運営者の特定は簡単ではありません。下図は、前回掲載した改正著作権法の海賊版対策のイメージ図(出典は文化庁作成の法案説明資料の p.3)を白黒化して、防弾ホスティングの守備範囲を赤枠で囲んだものです。また、元の図には記載がなかった「(データ蔵置サイトの)サイト運営者」と「防弾ホスティング業者」を青字で書き加えました。



画像出典： 文化庁作成、改正著作権法の説明資料の P. 3の図を加工

データ蔵置サイトは著作権を直接侵害しているサイトであり、防弾ホスティングは海賊版のみならず様々なサイバー犯罪の温床となっている悪の巣窟です。

こうして図示してみますと、海賊版との戦いを城攻めに例えるならば、「敵城の本丸を防弾ホスティングという内堀(赤枠)が守っている。今回の法改正(上図の①②)は外堀を埋める有効な一手と思われるが、本丸への直接の攻撃ではない」といった感じに見えます。

しかし国際的な犯罪に対して国内法だけでできることには限りがありますので、これは仕方ないのかもしれません。今後は、国内法整備だけでなく、サイト運営者を取り逃がさないための国際連携、国際捜査共助などの海外への働きかけの強化も望まれます。

2. なぜ防弾ホスティングがまかり通っているのか

通常のホスティングサービス会社は、警察からユーザー情報開示等の捜査協力依頼があれば、友好的に応じるものです。貸しているサーバが悪事に使われないためです。ところが、防弾ホスティングサービス（bulletproof hosting service、BPHS と略）は、個人情報保護／匿名性維持を口実に、こうした開示要求に応じず、外部から通報があってもサーバを停止しません。このような特徴を売りにして、海賊版サイトだけでなく、フィッシングサイト等の様々なサイバー犯罪サイトの運営者達を集めているのです。なぜこのような悪事のためとしか言いようのないサービスが、取り潰されもせずにまかり通っているのでしょうか？　ネット上で散見された理由をいくつか挙げてみます。

①BPHS は、以下のような**善意のユーザーにも必要なサービスである**と主張。

例1：　人権保護団体の秘密保持。例えば、虐待されていた人を保護する団体は、住所等の情報を秘匿する必要がある。

例2：　政府機関が機密保持用に利用している。

【補足】 大半が犯罪用途なのに「善意のユーザーもいるから全部を見逃せ」というのはおかしな話ですが、BPHS 会社はよくこれを言います。

②BPHS は例えるなら郵便屋であり、**「我々は手紙の中身（が犯罪かどうか）までは見ずに配達するだけだ」**と主張。

【補足】 これも BPHS の定番の主張です。ご参考までに、「Most Dangerous Town on the Internet」で検索してみることをお奨めいたします。セキュリティソフトでおなじみのノートンが制作した、ジャーナリストが BPHS 数社を突撃取材した 24 分弱の動画が検索結果に出てきます。動画の中盤で、スウェーデンの BPHS であるバーンホフ社がこの郵便屋の例えを口にしています。

③BPHS は、ウクライナなど**データ開示の法律が緩い国にあるため、捜査の手が及ばない。**

【補足】 旧ソ連のウクライナやロシアはサイバー犯罪が盛んな所なので、BPHS の所在地として「さもありなん」と思えます。ところが意外にも西欧先進国であるオランダやスウェーデンも BPHS 所在国として有名です。「なぜ西欧なのに？」との疑問に一言で答えるなら、これは個人情報保護の行き過ぎでしょう。EU は個人情報保護を基本的人権の一つと位置付けており、略称 GDPR で知られる世界一厳しい個人情報保護規則を施行しています。こうした背景から、BPHS に対する取り締まりも、①②の主張を前にして、及び腰になってしまっているのではないかと感じられます。

④ビットコイン等の仮想通貨での支払が可能。他の電子的支払い手段よりも匿名性が高い。

⑤核シェルター内などの特殊な場所にサーバが置かれていることもあり、警察でも差し押さえが困難。

⑥CDN によって、所在が分かりにくくなっている。

【補足】 CDN（Content Delivery Network）は、元のコンテンツを持つオリジンサーバの他に、コピーを持つ複数のキャッシュサーバを使って負荷を分散させる仕組みですが、サイトが CDN 上に構築されるとサーバの所在特定が難しくなります。CDN については、（BPHS に手出しできない場合でも） CDN 会社を突くことでサイト運営者特定の道が開ける可能性があるので、次回取り上げるつもりです。

（第 172 回：2020 年 9 月 7 日）