参考資料２

2016 年 2 月 19 日

文化庁長官官房著作権課 御中

一般社団法人インターネットユーザー協会

TPP 批准にかかる著作権法改正についての要望

文化庁によってまとめられた『環太平洋パートナーシップ（TPP）協定に伴う制度整備の在り方等について（案）』（以下報告書案）に対して、以下の通り意見を述べます。

著作権侵害の非親告罪化について

著作権侵害の非親告罪化については、二次創作活動を中心に、その範囲の策定の議論が進んでいます。しかし非親告罪化される範囲は、報告書案の検討結果が二次創作活動以外においてもそのまま適用されることを明確にする必要があります。これは社会貢献活動や企業内利用における軽微な複製が、別件逮捕の便利な事由として使われることを防ぐためです。

アクセスコントロール回避規制について

報告書案によれば「今回の制度整備においては、著作権者等の利益の保護及び国民の情報アクセスの自由との均衡を図る必要があることに鑑み、権利者に不当な不利益を及ぼさない形で行われる回避行為が広く例外規定の対象となり得るような制度設計とすることが適当である」とあり、この点が盛り込まれたことは大変評価できます。

アクセスコントロール回避規制は、国民の情報へのアクセスや表現の自由の毀損につながるおそれがあります。またアクセスコントロールを回避することは支分権侵害の該当行為ではなく、また表現の自由は経済的な自由に優越します。加えて経済的自由という観点からも、近年ではいわゆる「いじる自由」（Freedom To Tinker）がイノベーションの源泉であることが様々な研究から指摘されています。アクセスコントロールはいじる自由を阻害します。またアクセスコントロール回避規制は、新しい技術を制限するようなものであってはなりません。

ゆえに例外規定の策定にあたっては、権利者に不当な不利益を及ぼさない回避行為、特に下記に列挙する回避行為については、それが当然に可能となるような例外規定を広く設けることが必要です。

- オープンソースソフトウェアなどを用いた情報アクセスのための回避行為
  - ○ Linux や VLC Player での DVD/Blu-ray 視聴
- 視聴を目的とした複製のための回避行為
  - ○ DLNA などのネットワーク経由での視聴
  - ○ スマートフォンやタブレットでの視聴
- 引用や批評、二次創作を目的とした回避行為
  - ○ テレビ放送、DVD や Blu-ray のキャプチャ
- 機器やソフトウェアの安全性チェックを目的とした回避行為

- ユーザーが自分の機器で自由なソフトウェアを動作させるための回避行為
  - ○ jailbreaking や rooting のような管理者権限取得行為
- 技術の互換性や相互運用性を保つための回避行為
- 解除技術が提供されなくなったコンテンツやソフトウェアを利用するための回避行為
- 不正告発のための回避行為

※各項目の詳細は別紙の通り

正当な著作物の利用をする消費者の利便性の向上は、ひいてはコンテンツ産業の成長に資することは間違いありません。インターネットにおける違法な著作物流通については、すでに違法アップロード行為と違法ダウンロード行為は刑事罰の対象となっており、海賊版流通対策としては、著作権侵害の非親告罪化が導入されることになっています。違法な著作物流通についてのエンフォースメントはこの数年で十分に強化されています。

コンテンツの批評や引用など、著作権法で認められた用途においても、アクセスコントロールによって著作物を利用することができない状況を解決する必要があります。また、技術進歩は急速であり、自動車や家電など、従来はそう見なされていなかった機器でもコンピュータ化、ネットワーク化、ブラックボックス化が進んでいます。また技術革新に伴って、コンテンツの新たな用途や利用形態が開拓されることも想像に難くありません。これらに伴い、アクセスコントロール回避の新たな形態が求められるようになる可能性は非常に高いと考えられます。その上では例外規定を制定する上では、個別規定ではなく、包括的な一般規定を定めることが適当です。

米国では 2015 年 10 月 27 日に著作権法が改正され、前項で述べた正当なアクセスコントロール回避行為について、権利制限が制定されました[1]。TPP 批准のための著作権法改正においては、加盟国の法改正にも注視することが重要です。

権利制限の一般規定（フェアユース）の導入について

TPP 批准にかかる著作権法改正で導入が議論されている項目は、すべて著作権の保護強化に繋がるものであり、著作物の利用とのバランスに関する議論がされていません。ついては保護と利用のバランスを取るうえでは、著作物の利用促進にかかる条項の導入が必要です。

その上では公正で市場で原著作物に与える影響の少ない利用に関する権利制限の一般規定（フェアユース）を TPP 著作権条項の国内立法までに導入すべきです。またフェアユース規定の導入にあたっては、単なる産業振興策ではなく、言論の自由を担保し、教育やエンタテインメント、ユーザーによる技術検証・改善に資するものを目指すべきです。

以上

[1] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (米国 連邦官報) https://www.federalregister.gov/articles/2015/10/28/2015-27212/exemption-to-prohibition-on-circumvention-of-copyright-protection-systems-for-access-control

【別紙】

アクセスコントロール回避規制の例外とすべき行為について

1. オープンソースソフトウェアなどを用いた情報アクセスのための回避行為

現状ではオープンソースソフトウェアを用いて、合法的に DVD/Blu-ray を視聴する環境は実質的に存在しない。これはアクセスコントロールが理由でフリーなソフトウェアの開発が不可能なこと、さらに利用者が少ないために、有償のソフトウェアであっても開発コストが回収できる見込みが少ないためである。しかしながら、オープンソースソフトウェアの利用を制限する現状の制度は、コンテンツ利用促進の観点からも負の影響が大きい。例えば Linux のような自由かつ無償の OS の上で DVD の視聴を可能とすることは、情報デバイドを解消する上で非常に重要な施策だ。また ChromeOS のような教育現場で使われるシステムへの対応も考慮する必要がある。

2. 視聴目的の複製のための回避行為

DVD や Blu-ray の専用プレーヤーが家庭内において必須ではなくなった現状では、DVD/Blu-ray に収録されているコンテンツをディスクのまま視聴する環境は限られている。特にスマートフォンやタブレット端末については、その機器の特性上、視聴のための機器の他にディスクドライブを用意して視聴することは、その利便性を大きく害する。仮に DLNA などを用いてコンテンツをネットワーク経由で視聴するには、そのコンテンツが汎用データとしてネットワーク上に存在することが必要だ。

正当に入手したコンテンツを視聴することは、その手段を問わず、権利者の権利を害するものではない。また技術的に可能な視聴を著作権を理由に縛ることは、消費者の権利を不当に制限している。合法に入手したコンテンツをその視聴のために複製することは、フォーマット変換を含めて権利制限とすべきである。

3. 引用や批評、二次創作を可能とするための回避行為

引用や批評を正しく行える環境は、言論の自由を担保する上で非常に重要だ。またリミックスやパロディについても同様で、各国の著作権法制ではそのような利用を可能とする権利制限規定が導入されている。しかし現状では、アクセスコントロールがかかったテレビ番組や DVD/Blu-ray などを使い、そのような行為を行うことができない。テレビで放送された内容を引用し、評論する行為がおこなわれなければ、放送内容の正当性などについて、広い知見で検証することは不可能だ。

書籍や新聞、論文といった文字情報については、引用の有用性は広く理解され、これによる論考の深まりは、国民の重要な利益となる。現在インターネット上に流通する多くの情報が、文字から映像へとシフトしつつある現状を踏まえると、映像情報についても、引用の有用性を拡張すべき時期に来たと考える。

また技術はエンジニアだけのものではなく、それをユーザーに使ってもらうことに意味がある。そのためには、技術的動作を記録し、公表できることが重要だ。またその動作をコンピュータ上で拡大してみたり、止めてみたりして検証する必要がある。

しかし現状、特に映像機器において、映像コンテンツに課せられたアクセスコントロールが理由で、動作画面をコンピュータ上に記録することができない。これによって映像機器や映像作品の画質の比較や、ユーザーへの取り扱い情報の提供、ユーザーインターフェースの批評活動が実質不可能になっている現状がある。技術の進歩には、正しい技術批評や教育が必要だ。そのような行為を目的として行われるアクセスコントロール回避は、規制に当たらないような権利制限が必要である。

4. 機器やソフトウェアの安全性のチェックのための回避行為

DRM やセキュリティの確保を理由に、利用者にとって不利益となる悪質なソフトウェアが事業者より提供されるケースが散見される。

DRM についてはソニーBMG 製の CD に rootkit と呼ばれる、ユーザーに知られることなくコンピュータに侵入できるマルウェアが意図的に組み込まれたことがある。

例）ソニーが音楽 CD に組み込んだ"Rootkit"とは何者か？ （@IT）
http://www.atmarkit.co.jp/fwin2k/insiderseye/20051109rootkit/rootkit_01.html

またスマートフォンのファームウェアやプレインストールアプリケーションにバックドアやスパイウェアが仕込まれている事件も近年繰り返し話題になっている。

例) 人気の Samsung デバイスにバックドアが？（Kaspersky Lab Daily）
https://blog.kaspersky.co.jp/popular-samsung-devices-allegedly-contain-backdoor/2989/

例) 中国製スマホにスパイウェアがプリインストールされていることが発見される - Gigazine
http://gigazine.net/news/20140618-star-n9500-peinstall-spyware/

例) 公式 Android ファームウェアに潜む危険なトロイの木馬（株式会社 Doctor Web Pacific）
http://news.drweb.co.jp/show/?i=921&lng=ja&c=2

また、広く用いられているアプリケーション開発キット（SDK）を通じて多数の複数の開発元のアプリケーションにバックドアが仕込まれた事件も最近大きく話題となっている。

例）トレンドマイクロ、Baidu の SDK「Moplus」の脆弱性について注意喚起 （MdN Design Interactive）
http://www.mdn.co.jp/di/newstopics/43061/

また機械の動作を偽って、性能以上のものに見せかける企業の実態も明らかとなった。

例）フォルクスワーゲンのエンジニア、二酸化炭素排出量に関する不正行為を認める（Autoblog 日本版）
http://www.huffingtonpost.jp/autoblog-japan/vw-scandal_b_8548986.html

例）サムスン Galaxy S4、特定ベンチマークだけ最高性能を出す「最適化」が発覚（Engadget Japanese）
http://japanese.engadget.com/2013/07/30/galaxy-s4/

このような事例の多くは、情報セキュリティ企業だけでなく、市井のエンジニアたちが検証し、インターネット上でその事実を報告したことで明るみに出るケースがほとんどである。このような検証には、ソフトウェアにかけられた暗号や難読化を解析して、実際にどのような動作が行われているかを細かくチェックすることが必要となる。

ユーザーが正当に手に入れた機器で、どのようなプログラムがどのように動いているかを把握することは、ユーザーの権利である。

コピーコントロールやアクセスコントロールを解くこと自体が違法となった場合、このような検証を行うことができなくなり、ユーザーが自身で安全を保つことができない。米国諜報機関による大規模な通信傍受が明るみに出た今、このような回避行為は公正であり、法的にも十分認められるべきものである。

5. ユーザーが自分の機器で自由なソフトウェアを動作させるための回避行為

スマートフォンを例として考えると、現在市販されているスマートフォンのほとんどは、Apple の iOS か Google の Android がインストール済の状態で販売されている。ただしこのような OS は幾つかの理由から、一部のソフトウェアを動作させないように管理者権限（root）をユーザーに開放していない。そこで世界中のエンジニアたちがそのような制限を外すためにソフトウェアを分析し、Jailbreak（脱獄）など、管理者権限を取得するソフトウェアを開発し、配布している。また iOS や Android 以外の Firefox OS や Ubuntu touch などの OS を機器にインストールするためにも、そのような管理者権限の取得が必要となる。

ユーザーが正当な手段で手に入れた機器で、自身の動かしたいソフトウェアを動かすことはユーザーの権利だ。またスマート OS を開発する技術を学ぶうえでも、実機で動作チェックをすることは重要である。

現状ではこのような管理者権限の取得行為は違法ではないが、今後このような技術にアクセスコントロールがかかった場合、それが違法行為となる。スマートフォンに限らず、あらゆる電子機器（自動車なども含む）の上で、知識のあるユーザーが自己の責任において自由にソフトウェアを動かすことを妨げないように、アクセスコントロール回避行為は認められるべきだ。またソフトウェア開発を萎縮させないように、法改正にあたっては管理者権限の入手行為（Jailbreak や root 化）が違法ではないことを確認し、発表すべきである。

6. 技術の互換性や相互運用性を保つための回避行為

米国において、プリンタの互換インク等に関し、著作権法のアクセスコントロール回避規制に基づく訴訟が提起された事例がある（Lexmark International, Inc. v. Static Control Components, Inc., 387 F. 3d 522 (2004)）。アクセスコントロール回避規制は、このように技術の互換性や相互運用性を損なうかたちで利用される可能性が否めず、たとえば、今後 3D プリンタのフィードストック（樹脂インク）でも同様の問題が発生する可能性が考えられる。よって、技術の互換性や相互運用性が確保されることを何らかの形で明確にする必要がある。

7. すでに解除技術が提供されなくなったコンテンツやソフトウェアを利用するための回避行為

コピーコントロール CD（CCCD）を例に考えると、現在はその技術を用いた新たなコンテンツの配信は実施されておらず、またその解除を可能とするソフトウェアが公式に提供されているわけではない。つまり正当に手に入れたコンテンツを、合法に利用する手段がないことになる。またハードウェアドングルを必要とするソフトウェアで、そのドングルが最新の環境に対応していない場合、正当に入手したソフトウェアであっても実行が不可能である。

このような事情にもかかわらず、アクセスコントロールを回避することが違法とされることは、正規にコンテンツを入手した消費者の正当な権利を害している。すでにサポートが終了したアクセスコントロールについては、その解除もしくは除去が正当なものであると認めるべきだ。

8. 不正告発を可能とする回避行為

TPP は加盟国に TRIPS 協定および知的財産権に関する新たな規制を求め、企業の貿易秘密の漏洩阻止を図っている。今回加えられた条項 （TPP 協定 暫定仮訳 知的財産章 第 18・78 条 2-(a)および(c))は、コンピュータシステムにおける権限の与えられていない、かつ意図的な貿易秘密へのアクセスおよび開示に対する懲罰を可能にしており、しかもこれら情報へのアクセスや開示を保護する条文は存在しない。この条文は貿易秘密保護という目的を濫用する可能性があり、公的な利益のために働く不正告発者やジャーナリストを萎縮させてしまう。

健全な民主政治の運営には不正告発を可能にするエコシステムが必要不可欠であり、必要以上の制限は政治腐敗を引き起こす。アクセスコントロールを回避する目的のひとつには政治の不正告発や情報開示といったものがある。そのうえで、TPP には「知財保護」を銘打ちながら、こうした不正告発に懲罰を与えることが可能な条文があることに留意し、不正告発者やジャーナリストが萎縮しないような仕組みづくりをする必要がある。

以上