

技術的手段の回避行為に係る例外規定について

提案団体名、ご担当者	日本知的財産協会 著作権委員会 藤野 忠 著作権政策研究会 今子さゆり
連絡先（メール）	略 略
連絡先（電話番号）	略

- ① 技術開発のために、どのような形でアクセスコントロールの回避行為を行うことになるのか（現状どのように回避行為を行っているのかという実態など）、具体的にご記載ください。

当協会は、そもそも論として、TPPの義務を履行するために必要であるならその限りでの法改正はやむを得ないものの、改正に際しては、現行法で維持されてきた研究開発（回避されるアクセス・コントロールを改良するためになされる研究開発も含むがそれに限られない）の自由が、そのまま維持されるようにすべきであると考えている。

アクセス・コントロールの回避行為は、現状は著作権法（30条1項2号に規定される一定の例外を除く）でも不正競争防止法でも規制されていない行為であり、現行法の下では、あらゆるアクセス・コントロールについて、技術の研究開発目的を含むあらゆる態様での回避行為をすることができるのが原則である。

現在行われている個別の回避行為の態様を集めて、その限りで例外とするアプローチを目指すのであれば、それは原則と例外の逆転に他ならず、わが国産業の今後の研究開発活動への弊害を生じるものであって、適切とは思われない。

以下では、照会の趣旨に添い、典型的なアクセス・コントロール技術である暗号を一例として、研究開発における暗号回避がどのような理由で必要となっているのか等を説明するが、冒頭で申し上げた内容の趣旨についても、合わせて十分斟酌していただくようお願いしたい。

なお、回避行為の対象となる暗号化された情報が、著作物等であるのか否かは、復号してみなければ分からない場合もあるため、規制対象を著作物等の利用に関連したものに限定しようとしても、現実の影響範囲は広がりをもっており、暗号に関する研究開発全体への委縮効果を有していることにご留意いただきたい。

また、今回の照会は「回避行為」のみを対象としているが、回避行為そのものだけでなく、現行法では公衆譲渡・貸与目的での製造に対象が限定されている「回避行為に必要とされる装置やプログラム等の製造行為」の規制について法改正を行う場合にも、既に述べたのと同様の懸念があることを付言する。

<技術開発における暗号回避行為について>

- ① 日本では、暗号等の情報セキュリティ技術の研究にかかわる人材層が薄く、その育成が急務であるとされているが、規制によって研究開発に支障が出ると、研究者が国外に流出する等、さらに技術力の低下を招く結果となる。その結果、日本として暗号技術を自前で持てないこととなり、安全保障上の問題にもなりうる。

一方、米国の著作権法や米国通信法では包括的な例外が規定されており(*)、またこれら以外

にナショナルセキュリティの名の下で、規制に優越して認められる（現実に行われている）行為があるものと想像されるところ、米国以外の国において例外規定が限定的となることで、気づいたときには暗号関係の技術や装置は全てが米国発となってしまう、という懸念も杞憂ではない。

（*）通信法 605 条(e)(4)では、衛星放送の不正受信、並びに不正受信に用いるデコーダーの規制が置かれているが、同条(f)に以下が規定されている。

(f) Rights, obligations, and liabilities under other laws unaffected Nothing in this section shall affect any right, obligation, or liability under title 17, any rule, regulation, or order thereunder, or any other applicable Federal, State, or local law.

この規定によれば、著作権に関して一般則的な DMCA の例外によって、暗号研究目的での無断デコードに関しても抗弁できるように解される。

- ② ICT 産業界を中心に、これまで公益法人等から、暗号の脆弱性確認のための「攻撃プログラム」の作成委託を受けている。そうしたツールを使った脆弱性確認・強度評価は社会的に要請されていることである。
- ③ 現行の放送で使われている暗号は古いもので既にその「穴」もよく判っているため、それ自体を研究対象とすることはないが、今後の放送においてどのような暗号が使われるのかは未確定、不分明であり、将来にわたってその脆弱性を研究することは重要である。
- ④ リバース・エンジニアリング（プログラムの機能、インターフェースの調査解析）の前提としての暗号の回避が考えられる。暗号を解除し復号しなければその後に機能等の解析もできないのであり、さらにその後になされる正当なプログラムの開発行為や、マルウェアや不正コンテンツに対応するための対策ソフトの開発ができない。
- ⑤ この他、衆知を集めてセキュリティの脆弱性を評価する SECCON (<http://www.jnsa.org/seccon>) や、JP CERT (<https://www.jpCERT.or.jp>) の取組みも行われている。

法改正による影響で、上記のような取り組みができなくなることが懸念される。

② 技術開発目的以外で例外と位置付けるべき事例はあるか、ある場合はその具体的な内容（例外を認めるべき必要性、権利者の利益を不当に害しない理由など）をご記載ください。

(1) 対象となる「アクセス・コントロール」の限定

著作権侵害とは無関係のアクセス・コントロール回避行為を規制することは、TPPにおける義務とはなっていないのであるから、現行法と同様に、「著作権の支分権に関わるコピー・コントロールの効果を直接担保し、アクセス・コントロールの回避を規制しなければコピー・コントロールの効用が担保できず、著作権侵害を生ずる蓋然性が極めて高いもの」に対象を限定し、それ以外のアクセス・コントロールを規制対象としないようにすることが必要である。

また、ここで検討されるべき「例外」は、権利者の排他的権利を制限するものではないため、「権利者の利益を不当に害しない」という点を、今般の検討において直接的に配慮すべきかどうかについては疑問もあるが、現行法が規定している範囲を踏襲し、著作権侵害の蓋然性が極めて高いものに対象を限定する、ということであれば、権利者の利益を不当に害することなく、利用者との利益バランスを適切に担保できるものと評価されるのではないかと考えている。

(2) 権利制限規定で許容された行為の前提として必要となる回避行為

現行法では、30条にかかる行為において技術的保護手段を回避することが禁止される一方で、そのほかの権利制限規定にかかる行為については、回避行為が禁止されていない。

TPPにおいても、「著作権侵害とならない利用行為を可能とすること」は例外とすることが認められていることを考えると、上記のような回避行為を許容する現行法の規律は、維持されるべきである。

また、「権利者の利益を不当に害しない」点については、(1)と同様、現行法の規定を踏襲するものに過ぎない以上、権利者の利益を不当に害することとはならないと理解される。

(3) 米著作権法で配慮された利益バランスのための措置

上記(1)(2)に関わらず、TPPの義務を履行するために、アクセス・コントロール回避行為並びに回避に用いる装置等の規制を実質的に拡大するのであれば、著作権者と利用者・研究開発者等との利益バランスを失わないように、米国著作権法において配慮されている例外行為並びに例外を認めるための手続きと同様の手続きを、合わせて立法することが最低限必要である。

米国法をそのまま継受するような立法をすることについては忸怩たるものがあるかもしれないが、アクセス・コントロール回避規制そのものが米国著作権法の考え方を移入するものである以上、例外も同様に移入しなければ、米国における社会生活や企業活動等に比較して、わが国におけるそれが不当に制約されることにならざるを得ない。

(参考・米国著作権法における例外行為及び例外の検討手続)

(i) 規制によって生ずる弊害を除去するための、一定期間で繰り返される例外の検討（米国著作権法 1201 条(a) (1) (B)～(D)）

最近行われた例外見直しによって認定された対象（行為）は、日本の立法においても参考となる。

<https://www.federalregister.gov/articles/2015/10/28/2015-27212/exemption-to-prohibit-ion-on-circumvention-of-copyright-protection-systems-for-access-control>

(ii) 回避規制の例外として定められた行為（米著作権法 1201 条(d)～(j)）

なお (i) (ii) ともに、現行では利益バランスを確保するための措置として不十分ではないかとの問題意識から、見直しが検討されている状況にある。

<http://copyright.gov/1201/2015/introduction-analysis.pdf>

アクセス・コントロールの回避規制については、規制範囲について慎重な検討が必要であり、不測のマイナス効果が生ずる場合に対処するために、法施行後に常に適切な見直しがなされていく仕組みの導入が必要である。