Vol.2020-CSEC-91 No.13
Vol.2020-SPT-40 No.13
Vol.2020-EIP-90 No.13
2020/11/25

セキュリティ面から見た近年の著作権への一考察

須川 賢洋 [1]

概要：著作権法を始めとする知的財産権関連法は情報セキュリティ確保のための主たる法律ではないが、セキュリティの為の外周を固めるための法律としては欠かせないものである。
しかしながら、依然として旧体質に縛られており、最新のデジタル技術やネットワーク技術との不整合な箇所が多い。最新の情報セキュリティのニーズに応えるためには知的財産関連の法も最新技術に対応したものにしなければならない。その為にはまず知的財産権法とセキュリティの関係性について一度整理しておくことが必要である。本稿では、その予行として、主に著作権法に主眼をおき情報セキュリティ面での論点のピックアップを試みる。

キーワード：情報セキュリティ，著作権，著作権法，リバースエンジニアリング，デジタル・フォレンジック

A consideration of recent copyrights from a security perspective.

Masahiro SUGAWA[†1]

Abstract: the main laws for ensuring information security. But they are indispensable as laws for solidifying the outer circumference for security.
However, it is still tied to the old constitution, and there are many inconsistencies with the latest digital technology and network technology. In order to meet the latest information security needs, intellectual property-related laws must also be compatible with the latest technology. For that purpose, it is first necessary to sort out the relationship between the Intellectual Property Law and security. In this paper, as a rehearsal, we will mainly focus on copyright law and try to pick up issues related to information security.

Keywords: Information Security, Copyrights, Copyright act, Reverse engineering, Digital forensics

1. はじめに

情報セキュリティの為の法律と言った場合には、通常は刑法の電磁的記録に関する犯罪や不正アクセス禁止法、あるいは電気通信事業法などがまずその中心に据えられると言ってよいであろう。しかしながら知的財産の保護もまた広義の意味での情報セキュリティであり、されば著作権法も広義に捉えれば情報セキュリティを確保するための一連の法律の内にあると言える。また、知的財産とセキュリティの関係においては、その視点を攻撃側に置くか、あるいは防御側に置くかによって二つの観点に分けられる。すなわち、自らの持つ知的財産権をいかにして守るのかということに関しては、これは通常の情報保護やシステム防御の話と同一になる。すなわちその知的財産に対して情報セキュリティ確保の為の CIA（Confidentiality：機密性，Integrity：完全性，Availability：可用性」）が適用できると言えば良いであろう。その一方で例えば、もし自組織の中の人間が他人の著作権を侵害してしまった場合、その会社等はコンプライアンスをきちんと確保していなかったということになり、損害賠償への訴訟リスクや風評被害を受けることとなり、経営面からのセキュリティ対策が必要な話となる。

しかしながら、実際にはこのような単なる二分化だけで済まされる話ではなく、パッチワークのように次々と継ぎはぎしてきた法制度であるが故に、また日本の独自な行政システムに影響されるが故に、多くの細かな問題点や論点を含んでいる。デジタル庁の設置検討やビジネスの DX(デジタルトランスフォーメーション）などと新しいデジタル時代が叫ばれる今、知的財産法制とセキュリティの関係性について一度整理しておくことが必要である。本稿では、その準備段階として今後検討しなければならない問題を探し出すため、まずは著作権法を中心に情報セキュリティ面での論点うちのいくつかを拾い出しどのような問題や事態が想定されるのかを考察することとする。

2. 知的財産、著作権とセキュリティの関係

情報保護という観点では、組織の持つ情報の多くはなんらかの知的財産権に含まれるものであり、その範囲は、個人情報や情報システムそのもののアーキテクト情報などと言ったその他の"守られるべき情報"よりも広いと言えよう。（図１）
また、著作権侵害は刑事罰を伴うものであり、その適用範囲は狭いが最大量刑は不正アクセス禁止法などよりははる

1 新潟大学法学部
Faculty of Law, Niigata University

Vol.2020-CSEC-91 No.13
Vol.2020-SPT-40 No.13
Vol.2020-EIP-90 No.13
2020/11/25

かに重いことも特徴である。情報セキュリティに関する法の組み合わせを概念図にすると（図２）のようになる。

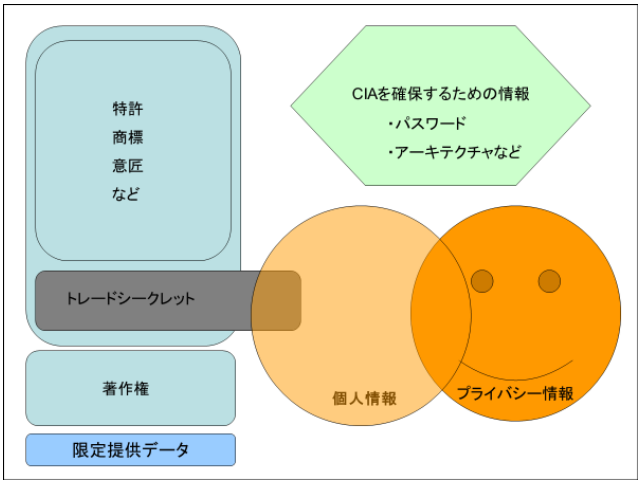

図１　守られるべき情報の種類　（筆者作図）

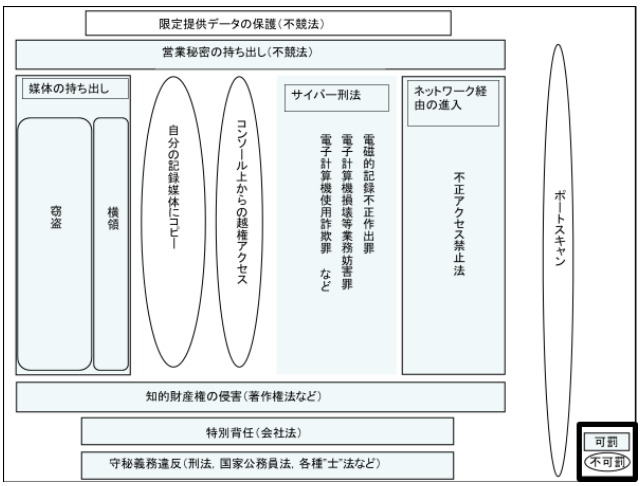

図 2　情報セキュ里程に関する法律（筆者作図）

著作権の保護は、自身（あるいは自社）の持つ知的財産を守るという意味で広義のセキュリティの為の法律とも言える。さらには、例えば産業スパイ、政治的なスパイを問わず、スパイ行為などがあった場合に、持ち出された情報がもし著作物であれば、著作権侵害をもって犯罪として立件することが可能であり、からめ手の情報保護のための法としても使える。もちろん、不正競争防止法の営業秘密漏洩罪を使う方が速い場合もあるだろうが、不競法を使うためには持ち出された情報が「営業秘密」である必要があり、必ずしもそうとは限らない場合も多い。また、内部の人間によるコンピュータ・プログラムの持ち出しなどということも多分に考えられ、このような場合は著作権侵害を問うことのほうが迅速な対処が可能である。この点においては、新潟鉄工事件1の時の議論などが参考になるであろう。

(1)　簡易な分類の試み

著作権に限らず知的財産権分野の法律とセキュリティとの関係はいくつかの段階に分類することができると言える。以下に示すと

- (a)外部からの知的財産侵害から守るという最も広義なセキュリティ
- (b)自身の側が他人の知的財産を侵害しないようにすること（コンプライアンスの確保）
- (c)犯罪組織や反社会組織への金銭供給のカット
- (d)プログラムそのものが情報セキュリティ上の問題を含む場合

などである。

(c)は、海賊版やコピー商品を購入することが、知的財産侵害を助長させ強いては社会情勢を不安定にさせることを意味する。令和２年の著作権法改正での「リーチサイト」規制、つまりリーチサイトの運営行為／リーチアプリの提供行為やリンク提供行為を規制したこともここにグルーピングすることができる。

なお、この令和２年法改正は、著作権法 113 条の「侵害とみなす行為」を大幅に追記し、ここにリーチサイトやリーチプログラム（アプリ）に関する詳細な定義や規定を記載することにより実施しているものである。法改正の結果、これらの行為には親告罪にて刑事罰が科されることになり、リンク提供者には最大で 3 年以下の懲役もしくは 300 万円以下の罰金又はこれの併科、サイト運営者2には最大 5 年以下の懲役もしくは 500 万円以下の罰金又はこれの併科となる。

(d)は更に

d-1 : 海賊版の OS やソフトウェアを導入した場合に、セキュリティパッチを充たらない問題

d-2 : 海賊版ソフトや非公式マーケットからダウンロードしたアプリや動画にウィルスやマルウェア等が内合されている場合

d-3 : 正規版ソフトウェアであっても、セキュリティ上非常に深刻な欠陥やバグ（いわゆるセキュリティホール）が存在する場合

などに分類される。特に(d-3)は、ソフトウェアのリバースエンジニアリングが必要な話であり平成 30 年改正との関係で重要である。これに関しては３．にて検討する。

この(d)の場合には、システムやパソコンのサポート室だけではなく、ネットワークのエンジニアや管理者が対処しなければならないレベルの話になることも十分にあり得る。

また、ソフトウェア自体に重大なバグや欠陥があった場合の問題としては、著作権法だけではなく、ソフトウェアへの製造物責任（無過失責任）法理の適用など、別な次元での議論が必要も必要になるが、本稿では省略する3。

Vol.2020-CSEC-91 No.13
Vol.2020-SPT-40 No.13
Vol.2020-EIP-90 No.13
2020/11/25

(2) その他、最新技術との乖離箇所

著作権法を細かく見ていくと、他にも情報セキュリティの観点からは不整合のあるところが多々見出せる。Twitter での写真のリツイートの際に撮影者の名前が自動的にトリミングされてカットされることが著作権法 19 条（氏名表示権）の侵害だとした最高裁の判断4も、その典型例であろう。しかし、これは法が技術に追いついていないのではなく、逆に技術が法に合っていない事例だと言える。ただし Twitter 社の存在する米国の著作権の考え方は、我が国の著作権法の著作者人格権の考え方とは異なるところもあり、これをただちにコンプライアンス意識の欠如と決めつけることは早計だと言える。氏名表示権に限らず著作者人格権規定は、流通や改変が容易なデジタル技術とはもっとも相性の悪いところだということもでき、我が国の人格権規定が果たしてこのままで良いのかについても再考の余地があると言える。

また、著作権法の規定するネットワークや LAN の考え方も、現在の暗号化通信や VPN などを想定しておらず、現行法は同一構内であるかどうかをもって LAN である、つまり公衆送信ではないとする考え方をしていると取れ、この事もいずれ問題が生じる可能性がある5。

3. 平成 30 年改正とソフトウェアのリバースエンジニアリング，デジタル・フォレンジック

3.1 リバースエンジニアリング

著作権法は他の法律に比べ非常に改定頻度の高い法律で、2.3 年に一度は改正されている。しかしながら、この法律はそもそもの目的（第 1 条）が「著作物並びに実演、レコード、放送及び有線放送に関し著作者の権利及びこれに隣接する権利を定め、これらの文化的所産の公正な利用に留意しつつ、著作者等の権利の保護を図り、もつて文化の発展に寄与すること」であり、そもそもセキュリティ概念とは程遠いものである。よって度重なる改正においても、俗に言うアーチストやコンテンツディストリビューターの保護強化が絶えず優先されてきた。そんな中で、例えば昭和 60 年(1985 年)にコンピュータプログラムの保護を内包し、翌年にはデーターベースの保護規定を取り込んだことは、ある意味非常に革新的なことであり、かつ例外的なことであったと言える。次のこのような大変遷は平成 9 年（1997 年）の「公衆送信権」の導入までない。これは、著作権法の管轄官庁はあくまで文化庁であって、IT や ICT を司る管轄官庁である経済産業省や総務省とむしろ利害が対立しやすい省庁であるがためと言えよう。

そのような、いわば保守的体質の著作権法において平成 30 年（2018 年）の改正時になって、ようやく改正の際の目的の内の一つに「サイバーセキュリティ」という言葉が使われるようになった。

とは言っても、平成 30 年の著作権法改正の主目的は「柔軟な権利制限規定」の制定であり、これはいわば、平成 24 年改正で導入した日本版フェアユース規定を再度整理することにあった。そのような中ではあるが、『サイバーセキュリティ確保等のためのソフトウェアの調査解析（リバース・エンジニアリング）』という項目が挿入されたことは、筆者の見解からすればまさに画期的なものであると言える（図２参）。

しかしながら、この改定規定は今に至るまでそれほど注目されていない。これは、もう一方の法改正理由である官民挙げての AI やディープラーニングの国力向上のための支援のほうに重点が置かれてしまったことが最大の理由であると思われる。もっとも、この結果、事が起こった後の証拠保全には有利になったと思われるが、この点は次節にて述べる。

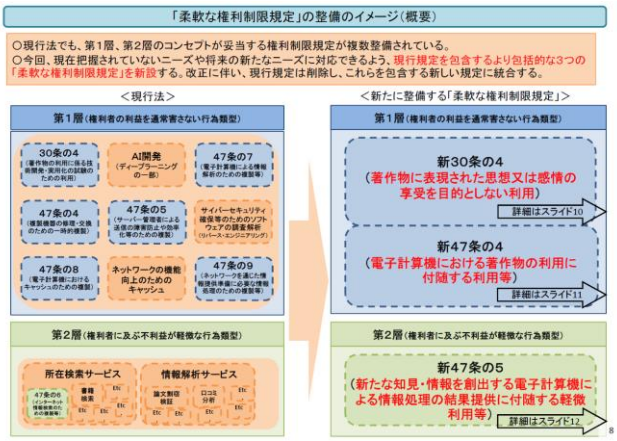

図 3　平成 30 年度著作権法改正時の文化庁概要説明資料6より

さて、このサイバーセキュリティ確保等のためのソフトウェアの調査解析であるが、むろん前述 1.(1)の(d)として挙げた場合への対処要求が時代として高まったからであることは間違いないが、それ以外にも同改正により「キャッシュ」の著作権法上の取り扱い、つまり権利制限に該当するということを明確化した結果、こちらにも対応せざるをえなかったとも言えよう。なぜならば、そもそも著作権法として取り扱ってきたのは、ネットワークセキュリティ技術というよりは、『「キャッシュ」＝「複製』という呪縛だったからである。そもそも、ソフトウェア技術の先進国かつ独占国であった米国はその地位を維持するためにソフトウェアのリバースエンジニアリングを禁じたいという思惑があった。その為の手段として著作権法を用いたのが事の始まりであるからである。ソフトウェアをリバースエンジニ

Vol.2020-CSEC-91 No.13
Vol.2020-SPT-40 No.13
Vol.2020-EIP-90 No.13
2020/11/25

アリングする為には逆コンパイルする過程があり、その段階で「複製」が生まれる→結果として著作権を侵害することになるという論法が長く用いられてきた。しかしながら、ソフトウェア技術で追いつきたい日本では、電源を切れば消える揮発性メモリ上への展開は複製に当たらないという解釈でなんとかリバースエンジニアリングを行いたい思惑があった。この結果、リバースエンジニアリング自体の扱いが宙に浮いた状態になっていたといえる。ところが技術の進歩が揮発性メモリと不揮発性メモリ、そしてストレージの境界を曖昧にし、またネットワークという導管の上でのキャッシュ蓄積が不可欠になってしまったいま、この理屈でキャッシュを扱うことができなくなったとも言える。

いずれにせよ、脆弱性調査のためのリバースエンジニアリングが認められたことは、セキュリティの確保の為には非常に喜ばしいことであるが、この運用詳細がはっきりせず、ビジネスの現場においては NDA 等との絡みで実効性の面で疑問が残る。このあたりの問題は一層の研究が必要となろう。

3.2 デジタル・フォレンジック

平成 30 年改正によって、「著作物に表現された思想又は感情の享受を目的としない利用」がはっきりと権利制限として扱われるようになったことは、AI やビッグデータに限らずデジタル技術に関する研究において非常にメリットが大きい。しかし同時に、本条によってデジタル・フォレンジックにその調査対象に著作物が含まれていることが予想できる場合にでも適用できると考えられる。あいにくと文化庁の改定資料の中にはデジタル・フォレンジックの文言を見出すことができないが、デジタル・フォレンジック技術はもはや犯罪捜査の場合だけに留まらず、企業内における不正調査や知的財産の流出事故に対しても頻繁に使われるため、デジタル・フォレンジックと著作権の関係の明確化は必要であると言える。

4. おわりに

本稿は冒頭にも述べたように、情報セキュリティと著作権の関係を再整理するために、さしあたって目につく問題点を列挙したものである。ここの問題点について今後検討していくつもりであり、また抽出できていない問題点そのものもまだ多く存在すると思われる。

セキュリティ確保のためのリバースエンジニアリングの問題一つ取ってみても、その実効性やソフトウェア使用契約との関係でどのようなバッティングがあるのかなどについては詳細に検討する必要があると思われる。また、デジタル・フォレンジック技術は、証跡調査だけでなく本来はデジタルコンテンツのネットワーク上でのトレーサビリティを確保するには好都合な手段のはずであるのだが、このことに関しても研究が進んでいない。これらを今後さらに調査・研究していきたい。

脚注

1 東京高裁 昭和 60 年 2 月 4 日判決，判時 1190 号 143 頁
2 なお、補足であるが本条に関しては、現在問題になっておるプラットフォーム・サービス提供者（プラットフォーマー）は規制対象外であることが法案の改正過程で明文化されている。
文化庁：著作権法及びプログラムの著作物に係る登録の特例に関する法律の一部を改正する法律(説明資料) 5 枚目
https://www.bunka.go.jp/seisaku/chosakuken/hokaisei/r02_hokaisei/pdf/92359601_02.pdf
3 著作権は、その著作物が有害なものであっても成立の可否には関係ないため。
4 最高裁第三小法廷　令和 2 年 7 月 21 日判決
5 「IoT 時代の産業への最新情報処理技術導入時に起きる現行法とのミスマッチと，解消の糸ー知的財産や製造物責任を中心にー」電気学会論文誌C5（電子・情報・システム部門誌）2018 年 138 巻 3 号 p. 249-253 参
6 文化庁 : 著作権法の一部を改正する法律（平成 30 年法律第 30 号）について--著作権法の一部を改正する法律　概要説明資料-- 9 枚目
https://www.bunka.go.jp/seisaku/chosakuken/hokaisei/h30_hokaisei/pdf/r1406693_02.pdf