

情報セキュリティに関連する  
ソフトウェアの取扱いに係る  
法律上の位置付けに関する調査

- 報告書 -

2008年5月

**IPA**<sup>®</sup> 独立行政法人 情報処理推進機構  
セキュリティセンター

# はじめに

## 序

本報告書は、法律の定めや解釈が、情報セキュリティ活動の遂行に障害になっていないかどうかという観点から、近時の情報セキュリティと社会とのかかわりで問題になった事項について、総合的に考察するものである。

情報ネットワークの普及および広帯域化、ネットワーク参加者数の爆発的増大、攻撃者側の主体の組織的・営利的傾向の顕著化などの影響により、情報セキュリティに対する危険は、日増しに増大しているといえることができる。そして、それに対抗すべくセキュリティ向上のための行為（情報セキュリティ活動）の重要性は、極めて増しているといえることができる。

しかしながら、種々の法律の定めは、今日のようなネットワークの発展のもと、情報セキュリティの確保を果たす上記各行為が、社会的に極めて重要な役割を担っているということ認識して整備されているものではない。それゆえ、本来その性質上、適法と解されるべき情報セキュリティ活動の適法性につき、ある種の「曖昧さ」が生じており、それがもたらす萎縮効果が現実として大きな問題となっている。

本報告書は、このような認識のもと、独立行政法人 情報処理推進機構（IPA）より委託を受けて、情報セキュリティ活動と法律の関係について、比較法的な視点を念頭に起きつつ、世界における現状を俯瞰し、我が国における法律のあり方について、情報セキュリティ活動に関する産業推進という観点から、一定の方向性を提案するものである。

## セキュリティ活動と法調査委員会

委員長 高橋郁夫  
委員 町村泰貴  
委員 石井徹哉  
委員 吉田一雄  
委員 土井悦生  
委員 池村 聡

## 1 本調査の手法

後述の情報セキュリティ活動と法的な論点について、調査項目の詳細と背景を記載した質問事項書を作成し、アメリカ合衆国、連合王国（英国）、フランス、ドイツ、オーストラリアの各国の制定法、判例法、各種解釈論などについて現地の法律専門家の回答をえた上で、それを分析することで総合的に検討するものとした。これは、上記のような先進的な問題については、文献調査のみによって調査しうる事項に一定の限界が存在するためである。本研究は、これらの調査と我が国における解釈論についての文献調査によって、上記各論点についての法的な問題点と今後の方向性が示唆しようとするものである。

## 2 調査委員会における検討

調査対象国である米国・英国・フランス・ドイツ・オーストラリアの各国ネットワーク法の専門家をメンバー（調査委員）とする調査委員会を構成した。当該調査委員会において、現地法律専門家に対して質問書の送付により回答を求める方法などにより回答を求めた回答書をもとに、各国の法律状況を分析した。

（アメリカ合衆国）

土井悦生（ポールヘイスティングス法律事務所・外国法共同事業 弁護士）

**Richard Field** （米国 弁護士）

（英国）

高橋郁夫（弁護士／㈱ITリサーチ・アート代表取締役）

**Graham J.H.Smith**（英国 弁護士 **Bird & Bird** 法律事務所）

（フランス）

町村泰貴（北海道大学法学研究科教授）

**Frédéric Sardain**（フランス **Avocat a la Cour de Paris** パリ控訴院付き弁護士）

（ドイツ）

石井徹哉（千葉大学法経学部教授）

**Thomas Hoeren** 博士・教授（ドイツ/ミュンスター大学およびデュッセルドルフ控訴裁判所判事）

（オーストラリア）

吉田一雄（清和大学 法学部 法律学科 教授）

**Brendan Scott**（**Opensourcelaw.biz**）

（日本法）

高橋郁夫

池村聡（森・濱田松本法律事務所 弁護士）

### 3 調査協力者

なお、本調査にあたっては、論点の抽出、翻訳、検討にあたって、早稲田大学 **Pauline Reich** 教授、セキュリティコンサルタント **Gohsuke Takama** 氏、**Cambridge** 大学 **Richard Clayton** 教授から協力をえた。ここに感謝の意を表する。

また、IPA より、セキュリティセンター長 山田 安秀氏、同情報セキュリティ技術ラボラトリー長 小林 偉昭氏、前田 祐子氏、中野 学氏が、オブザーバーとして本調査委員会に参加した。ここに感謝の意を表する。

はじめに .....	2
1 本調査の手法.....	3
2 調査委員会における検討.....	3
3 調査協力者 .....	4
第1 概念 .....	8
1 情報セキュリティ活動の概念 .....	8
2 本調査の対象.....	9
2.1. 検討の対象となる情報セキュリティ活動.....	9
2.2. 背景事情.....	9
2.3 法的論点の抽出.....	9
第2 リバースエンジニアリングに関する法的問題.....	11
1 リバースエンジニアリングの手法と情報セキュリティ活動.....	11
1.1. リバースエンジニアリングの概念.....	11
1.2. 情報セキュリティ調査のためのリバースエンジニアリング.....	11
1.3. リバースエンジニアリングの具体的な手法（音楽 CD に関する Rootkit 事件を一例に） .....	12
2 日本におけるリバースエンジニアリングを用いたセキュリティ活動と著作権の問題について .....	13
2.1. リバースエンジニアリングの著作権侵害性 .....	13
2.2. 調査研究協力者会議報告書およびそれ以前の論文等 .....	13
(1) 調査研究協力者会議報告書.....	14
(2) 調査研究協力者会議報告書公表以前の論文、公表直後の論文等 .....	17
2.3. 調査研究協力者会議報告書公表後の政府機関による見解、裁判例議論の進展.....	18
(1)公正取引委員会「ソフトウェアライセンス契約等に関する独占禁止法上の考え方ーソフトウェア独占禁止法に関する研究会中間報告書ー」（平成14年3月20日公表） .....	18
(2) 文化審議会著作権分科会法制問題小委員会 契約・利用ワーキングチーム検討結果報告（平成18年7月） .....	18
(3)東京地裁平成18年2月10日判決.....	19
2.4. 現在の議論状況とまとめ .....	20
(1) 現在の議論状況.....	20
(2)今後の方向性 .....	21
3 諸外国における脆弱性調査のためのリバースエンジニアリングの適法性をめぐる議論 .....	23
3.1. 概観 .....	23

3.2.	米国における公正使用の法理とリバースエンジニアリング	23
3.3.	リバースエンジニアリングをめぐるEU諸国における制定法	24
	(1) ソフトウェア指令	24
	(2) コピーライト指令	25
	(3) 英国	26
	(4) フランス	27
	(5) ドイツ	28
3.4.	オーストラリア	29
4	検討	30
	4.1.比較法的な調査結果	30
	4.2.脆弱性調査のためのリバースエンジニアリングの適法性について	30
第3	セキュリティ修正ソフトウェアと法律	33
1	セキュリティ修正ソフトウェア	33
2	第三者におけるセキュリティ修正ソフトウェアの提供	33
	2.1. 近時の動向	33
	2.2. 第三者の提供するセキュリティ修正ソフトウェアの必要性と問題点	34
	2.3 第三者がセキュリティ情報ソフトウェアを開発・提供する行為に対する法的な問題の可能性	35
3	我が国における第三者によるセキュリティ修正ソフトウェアの開発・提供に関する法的問題	35
	3.1.著作権法	35
	3.2. ライセンス契約上の問題	36
4	諸外国における議論の状況	37
	4.1. 米国における議論状況	37
	4.2. EU 諸国における議論状況	37
	(1)英国	37
	(2)フランス	37
	(3)ドイツ	37
	4.3. オーストラリアにおける議論	38
5	検討	38
	5.1.第三者の修正ソフトウェアの必要性	38
	5.2.我が国における許容性について	38
第4	著作権技術的保護手段等の脆弱性調査について	40
1	技術的保護手段等とは	40
	1.1.概念	40
	1.2.技術的保護手段等と暗号技術	40

2	諸外国における技術的保護手段と法律の解釈の交錯.....	41
2.1.	米国デジタルミレニアム著作権法と技術的保護手段の回避.....	41
	(1)米国における技術的保護手段の定め.....	41
	(2) デジタルミレニアム法と暗号研究との交錯.....	41
	(3)その余の問題.....	42
2.2.	その余の法域における具体的な暗号研究と著作権の交錯.....	42
	(1)EU 指令.....	42
	(2)構成国における国内法化.....	43
	(3)オーストラリアにおける制定法.....	43
3	技術的保護手段、権利管理情報に関する法律上の規定と検討.....	44
3.1.	日本における技術的保護手段、権利管理情報についての規定.....	44
3.2.	暗号研究との交錯についての検討.....	45
	提言.....	47
1	提言の趣旨.....	48
	(1) 「情報セキュリティ活動の促進をはかり」.....	48
	(2) 「安全で信頼性の高い IT を利用できる環境を整える」.....	48
	(3) 「産業の基盤を支える創造性を促進することになり」.....	48
	(4) 「以下の対応をとることが望ましい。」.....	48
2	脆弱性調査目的のデコンパイルの適法性の確認.....	49
	(1) 「コンピュータプログラムの脆弱性調査のため」.....	49
	(2) 「デコンパイル行為およびそれに当然付随する複製等の行為」.....	49
	(3) 「著作権法上、適法であること」.....	49
	(4) 「著作権法改正等の手段」.....	50
3	第三者による脆弱性修正プログラム作成の適法性の確認.....	50
	(1) 「セキュリティ修正プログラム」.....	50
	(2) 「利用者の利用に必要なかぎりでなされる場合」.....	50
	(3) 「適法になしうること」.....	50
4	ソフトウェア利用契約における禁止条項の効力.....	51
	(1) 効力を有しないこと.....	51
	(2) 明らかにされるべき.....	51
5	技術的保護手段等と暗号研究.....	51
	(1) 情報セキュリティとしてなされる暗号研究.....	51
	(2) 明らかにされるべき.....	52

# 第 1 概念

## 1 情報セキュリティ活動の概念

情報セキュリティ産業において行われている情報セキュリティ活動には、種々の行為が含まれる。本書において「情報セキュリティ活動」とは、情報セキュリティに関連して行われるセキュリティ向上のための行為一切をいう。その中の代表的行為としてソフトウェア等の脆弱性<sup>1</sup>を分析・発見・修正・公表する一連の行為をあげることができよう。したがって、コンピュータのアクセス制御機構についての研究・プログラムの脆弱性の分析をはじめとするコンピュータセキュリティについての活動であると、ネットワークにおける脆弱性の調査・ネットワーク活動についての分析行為・情報共有などのネットワークセキュリティ活動についての活動であるとを問わない。セキュリティ向上のための一切の活動をいうことから、脆弱性に対する修補行為のみならず脆弱性の分析行為をも含み、また、それらの研究成果の発表やこれに対する批判などをも含む概念である。

本研究は、特にソフトウェアとの関係で、情報セキュリティ活動の活性化、かかる活動による成果の円滑な流通という観点から、現状問題となりうる関係法規の解釈論等を分析するとともに、立法論等を含め、そのあり方につき、一定の提案を行うことを目的とするものである。

情報セキュリティ活動と法規制の問題という観点から考察すれば、この他例えばネットワーク管理活動や違法有害情報対応の局面においては、「通信の秘密」などの問題等も、極めて重要な検討課題として位置付けられよう。しかしながら、本研究においては、専らソフトウェアの脆弱性を分析する等の行為に対する法規制の関係について限定して考察することとしたい。

---

<sup>1</sup> 本書では、「脆弱性」という用語を、「ソフトウェア等脆弱性関連情報取扱基準」（平成 16 年 7 月 7 日経済産業省告示第 235 号。 <http://www.ipa.go.jp/security/vuln/index.html>）にならって、「ソフトウェア等において、コンピュータウイルス、コンピュータ不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所。ウェブアプリケーションにあっては、ウェブサイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような、安全性が欠如している状態を含む。」という意味で使用する。

## 2 本調査の対象

### 2.1. 検討の対象となる情報セキュリティ活動

情報セキュリティ活動に関連するソフトウェアの取扱いに関する法律問題について検討することが求められる活動としては、具体的に、

- (1) ソフトウェアの解析およびそれに基づく脆弱性の調査
- (2) 脆弱性を有すると認められるソフトウェアに対する、脆弱性対策方法の実行（具体的には、脆弱性を修正するソフトウェアの開発、実行等）
- (3) (1)において、当該ソフトウェアにいわゆる技術的保護手段等が施されている場合、それを回避等して行う脆弱性の調査などを、差し当たり挙げることができる。

### 2.2. 背景事情

上記各活動について、検討すべき法律上の問題としては、以下のものが考えられる。

- (1) ソフトウェアの解析およびそれに基づく脆弱性の調査  
ソフトウェアの解析およびそれに基づく脆弱性の調査に関しては、リバースエンジニアリングがその手法として最も有効である。しかしながら、我が国において、リバースエンジニアリングの適法性に関しては、（具体的には著作権侵害に該当するか否かという点において）古くから議論がなされているところであり、未だ不明確なところがある。かかる状況のもと、実際の脆弱性調査におけるリバースエンジニアリングに対し、その違法性を恐れるがゆえのいわゆる萎縮効果が分析者に対して働く可能性が存在する。

- (2) 脆弱性を有すると認められるソフトウェアに対する、脆弱性対策方法の実行（具体的には、脆弱性を修正するソフトウェアの制作、実行等）

あるソフトウェアにつき脆弱性が認められる場合、その製品開発者は、脆弱性を修正するソフトウェアの開発等、これを回避するための対応策を公表することが求められる。しかしながら、情報セキュリティ産業においては、種々の理由から、開発者以外のものが、修正ソフトウェアの開発等を行うことがある。開発者以外の第三者によるこのような行為に対する法的評価如何によっては、情報セキュリティ活動に対し萎縮効果が働く可能性がある。

- (3) (1)において、当該ソフトウェアにいわゆる技術的保護手段等が施されている場合、それを回避等して行う脆弱性調査

調査対象たるソフトウェアにつき技術的保護手段等が施されている場合、その脆弱性調査のために、当該技術的保護手段等を回避する必要がある場合が存する。当該回避行為が、技術的保護手段等の保護を目的とした不正競争防止法、著作権法の各規定に抵触するか否かにつき、脆弱性調査に対する萎縮的効果の有無という観点から諸外国の例をも参考に検討することは有意義であろう。

### 2.3 法的論点の抽出

上記の手法に存在する法的論点として、以下の論点を抽出した。

①脆弱性調査のためのリバースエンジニアリングの法的位置づけ

②リバースエンジニアリングを一定の要件のもと許容したECの1991年5月14日付け「コンピュータ・プログラムの法的保護に関するEC閣僚理事会指令」（以下、「ソフトウェア指令」という。）の各国制定法における実装状況および、脆弱性調査に対する適用の可能性をめぐる議論の調査・検証

脆弱性を有するソフトウェアに対する修正行為の法的位置づけ（具体的には著作権法第47条の2、同20条2項3号の解釈等）および調査対象各国における、右条項の有無、解釈

技術的保護手段等についての法的保護およびこれについての米国デジタルミレニアム著作権法における例外（リバースエンジニアリング、暗号調査、セキュリティテスト）に相当する法律の解釈の状況

これらの論点について各国の現状を分析して、それらをもとに我が国に対して提言をなすのが、調査委員会の目的となる。

## 第2 リバースエンジニアリングに関する法的問題

### 1 リバースエンジニアリングの手法と情報セキュリティ活動

#### 1.1. リバースエンジニアリングの概念

「リバースエンジニアリング」は、非常に多義的な概念である。最広義においては、ソフトウェアやハードウェアなどを分解、あるいは解析し、その仕組みや仕様、目的、構成部品、要素技術などを明らかにすることをいう。プログラムの分野では、モジュール間の関係の解明やシステムの基本仕様の分析といった行為を含む概念である。

具体的には、

- (a) マニュアルの調査
- (b) テストラン
- (c) 接続テスト
- (d) 回線トレース
- (e) 記憶媒体のダンプ
- (f) メモリダンプ
- (g) ディスアセンブル・デコンパイル
- (h) ソースプログラムの調査

などの段階に分けて、それぞれ行われる。これら各段階で実施される行為の具体的内容については、本書の性質上省略するが、上記のうち、(g) ディスアセンブル・デコンパイルの際には、当該対象ソフトウェアのオブジェクトコードの複製物（又は翻案物）が作成されることが多い。また、そもそもの分析作業の際に、オブジェクトコードの複製を行うことが一般的ともいえる。

リバースエンジニアリングは、情報セキュリティ活動においては、「悪意あるコードの発見」、「予測していない欠陥の発見」、「他人のコードの利用の発見」、「利用されることが意図されていないにもかかわらずシェアウェアやオープンソースコードが利用されている事実の発見」、「異なった領域・目的の製品からの学習」等の領域において、有効な手法であるとされており、特に悪意あるソフトウェアの実際の動作分析をはじめとするソフトウェアの脆弱性分析のためには、必要不可欠な技術とあってよい。

#### 1.2. 情報セキュリティ調査のためのリバースエンジニアリング

情報セキュリティの調査のためのリバースエンジニアリングは、様々な分野で用いられている。プログラムの具体的なコードを調べ、そのプログラムに脆弱性が存在していないかを分析することにも使われている他、悪意あるソフトウェア（いわゆるマルウェア）を解析して、その脅威を分析し、対策を講じることにも使われている。

そして、具体的な手法としては、以下のものが挙げられる。

(a) システムレベル分析

「システムレベル分析」は、情報取得、プログラムの実行機能の検査、あるいはプログラムのインプット・アウトプット等の追跡をするために、ツールとなるプログラムを実行させ、基本ソフトの種々のソフトのサービスを利用するものである。これらの情報は、基本的に、基本ソフトから得られることになる。

この種のシステムレベル分析を行うモニタリングツールとしては、FileMon、TCPView、TDIMon、RegMon、PortMon等が存在する。

(b) コードレベル分析

「コードレベル分析」は、プログラムのバイナリーから、デザインのコンセプトとアルゴリズムを引き出す手法等により、ソフトウェアの脆弱性を分析していく手法であり、どのような環境で分析を行うかにより、オフラインコード分析とライブコード分析に分けることができる。

例えば、オフラインコード分析に用いられる逆アセンブラーとしては、IDA Pro、ILDasmといったツールが有名であり、情報セキュリティ調査を行う者は、これらのツールを用いて、具体的なコードで、種々の脆弱性を招きやすい部分などを調査していくことになる。

### 1.3. リバースエンジニアリングの具体的な手法（音楽 CD に関する Rootkit 事件を一例に）

2005年11月、Sony BMG Music Entertainment社は、コピーコントロール技術「XCP」を施した音楽CDを交換・回収することを発表した<sup>2</sup>。この事件は、コピーコントロール技術「XCP」が、ファイル、レジストリ・キーその他のシステム・オブジェクトをセキュリティソフトから隠蔽する「Rootkit」と呼ばれる技術を採用していたことに端を発しており、XCPを搭載する音楽CDをパソコンで再生すると当該パソコンにセキュリティホールが作られてしまうという深刻な問題が生じ、事実、当該機能を悪用し、ウイルス対策ソフトからの検出を逃れるウイルスも出現するに至った。

当該事件に関連し、以下の手法により、上記音楽CDから RootKit の存在を確認したことが、インターネット上でレポートされている<sup>3</sup>。

- ア RootkitRevealer (RKR) の最新版をテストしたことにより、自身のパソコンに RootKit が入り込んでいる形跡が判明する。
- イ カーネル・デバッガを使用し、稼働中のシステムの内部を調査。テーブルをダンプ出力したところ、いくつかの横取りされたファンクションが発見される。
- ウ 横取りされているファンクションを表示させてみたところ、デバイス・ドライバ Aries.sys 内のものが、カーネルモード API を横取りしていることが判明する。

<sup>2</sup> <http://www.sonymusic.co.jp/xcp/uninstall.html>

<sup>3</sup> 「ソニーが音楽 CD に組み込んだ “Rootkit” とは何者か？」 Mark Russinovich 著／畑中 哲 訳

([http://www.atmarkit.co.jp/fwin2k/insiderseye/20051109rootkit/rootkit\\_01.html](http://www.atmarkit.co.jp/fwin2k/insiderseye/20051109rootkit/rootkit_01.html))

- エ **Aries.sys** ファイルを隠蔽されていないディレクトリにコピーし、これを逆アセンブラソフト **IDA Pro** に読み込ませる。
- オ **Aries.sys** ファイルが、名前が“**\$sys\$**”で始まるファイルやディレクトリ、レジストリ・キー、プロセスをすべて隠す機能があることが判明する。
- カ 隠されていたファイルの多くには、製品名やファイル名、会社名の情報が含まれており、その会社が、音楽CD用の **DRM** 技術を販売している事実が判明し、自身が最近購入した音楽CDが原因であることを突き止めた。

この記事は、リバースエンジニアリング（特にツールを利用したディスアセンブルの手法）が実際のソフトウェアの動作、脆弱性の検証、調査に有効な手法であることを如実に物語っている。

## 2 日本におけるリバースエンジニアリングを用いたセキュリティ活動と著作権の問題について

### 2.1. リバースエンジニアリングの著作権侵害性

我が国において、ソフトウェアのリバースエンジニアリングは、著作権侵害（具体的には複製権侵害又は翻案権侵害）に該当するか否かという形で、古くから議論が行われていることは周知の事実である。

具体的には、リバースエンジニアリングにおけるディスアセンブル・デコンパイルの段階で、オブジェクトコードからソースコードを抽出し、それを記録媒体に保存したり、プリンターで印字したりする場合に、「複製」（ないし翻案）が行われることから、これを著作権法上どのように評価すべきかが問題となる（なお、その抽出行為が、コンピュータのディスプレイ自体で行われている限りにおいては、いわゆるRAMへの一次的複製に過ぎないことから、著作権侵害の問題は生じないと考えられる<sup>4</sup>。したがって、本書においてもかかる行為については特段検討の対象としない。）。

この点、特許法は、第69条第1項において、試験又は研究のための実施は特許権侵害とならない旨規定していることから、同法の下ではリバースエンジニアリングは原則として許容される。しかしながら、著作権法においては、このような趣旨の規定はなく、さらには、第30条以下の権利制限規定中も正面からリバースエンジニアリングを許容する規定は存しないことから、その法的評価が問題となるのである。

### 2.2. 調査研究協力者会議報告書およびそれ以前の論文等

リバースエンジニアリングの著作権法上の問題点を検討したもののうち、国際的動向への言及という意味も含め最も詳細なものは、文化庁が平成5年に設置した「コンピュータ・プログラムに係る著作権問題に関する調査研究協力者会議」における報告書「コンピュータ・プログラムに係る著作権問題に関する調査研究協力者会議報告書—既存プログラムの調査・解析等について—」（平成6年5月公表。以下、「調査研究協力者会議報告書」という。）であり、同報告書は、当時のこの問題に対する、いわば集大成として捉えることが可

---

<sup>4</sup> 例えば田村善之「著作権法概説（第2版）」（有斐閣、2006）228頁等。

能である<sup>5</sup>。

そこで、本書では、まず調査研究協力者会議報告書およびそれ以前の論文等につき検討を行う。

### (1) 調査研究協力者会議報告書

#### ア 報告書における検討対象

調査研究協力者会議報告書は、①既存プログラムの調査・解析について、②プログラムに係る著作権の権利制限規定について、③コピープロテクション解除装置の規則、の3つの問題につき検討するものであり、このうち①において、リバースエンジニアリングに関する検討が行われている。

なお、同報告書においては、「リバースエンジニアリング」という用語は用いず、「調査・解析」という用語を用いることにより、調査解析の結果を利用した新たなプログラムの開発については検討の対象としていない<sup>6</sup>。

そして、調査・解析の主な目的として、①著作権侵害の調査、発見、②プログラムの保守（バグの発見、修正）、③プログラムの改良、移植、④プログラムの性能、機能の調査、⑤互換プログラムの開発、⑥接続プログラムの開発、⑦記憶媒体による情報交換、⑧コンバータの開発、を挙げるとともに、その手法として、上記1. 1で述べた8手法、すなわち①マニュアルの調査、②テストラン、③接続テスト、④回線トレース、⑤記憶媒体のダンプ、⑥メモリダンプ、⑦逆アセンブル、逆コンパイル、⑧ソース・プログラムの調査、を挙げ、当該手法のうち、①～⑤については、著作権法上問題となるような複製又は翻案行為は存在しないものの、⑥～⑧については、「既存プログラムの磁気ディスク等への固定又はプリントアウトなどの著作権法上問題となり得る複製又は翻案行為が存在する場合があります」と考えられる。」とする。

#### イ 国際的動向の紹介

次いで、国際的動向として、①ECソフトウェア指令（特に第5条第3項と第6条）、アメリカ合衆国におけるフェアユース法理（アメリカ合衆国著作権法第107条）およびプログラムの解析・調査がフェアユースに該当するという趣旨の判決例、③スイス、オーストラリアの現状をそれぞれ紹介し、さらには、国際的な場における検討として、ガット・ウルグアイ・ラウンド、WIPOでの議論等の有無、議論の内容につき紹介している。

---

<sup>5</sup> 同報告書は、文化庁監修「著作権法百年史 資料編」（著作権情報センター、2000）415頁に掲載されている他、著作権情報センターのサイトにも掲載されている

（[http://www.cric.or.jp/houkoku/h6\\_5/h6\\_5\\_main.html](http://www.cric.or.jp/houkoku/h6_5/h6_5_main.html)）。その他、文化庁文化庁著作権課による報告書概要の紹介として、「コンピュータ・プログラムの調査・解析等に関する検討」（NBL547号8頁、1994）、当該会議の調査研究者による見解として、松田政行「コンピュータ・プログラムの逆コンパイルに関する著作権問題」（NBL547号14頁、1994）等がある。

<sup>6</sup> この点について同報告書は、「新たなプログラムの表現が既存プログラムの表現の複製又は翻案に当たるときは、権利者の許諾がない限り、著作権侵害となることは当然であり、この点については改めて検討するまでもないと考えられる。」とする。

ウ 既存プログラムの調査・解析に伴う複製又は翻案に関する権利制限規定についての意見紹介

次に、既存プログラムの調査・解析に伴う複製又は翻案に関する権利制限規定についての意見の紹介に移り、我が国においては、当時、以下のような四つの意見が存することが報告されている。

①調査・解析一般について、それに伴う複製又は翻案に関する権利制限規定を設けるべきであり、調査・解析の目的は特定すべきではないとする見解

(主な理由)

- ・ 著作権法は表現を保護するが、その背後にあるアイデアを保護するものではなく、調査・解析を禁ずることは、アイデアへのアクセスを禁ずることになる。
- ・ 調査・解析は社会全体の技術発展に不可欠であり、特許法第69条第1項・半導体集積回路の回路配置に関する法律第12条第2項においては許容されている。

調査・解析に伴う複製又は翻案に関する権利制限規定を設けるべきであるが、特定の目的（競合プログラムの開発、海賊版プログラムの開発等）の場合には許されないとすべきとする見解

(主な理由)

- ・ プログラム中の技術思想の解読を可能とし産業・文化の発展を促すという要請と先行的な技術開発のインセンティブを守るという要請との調整を図るべきである。
- ・ バグの修正、接続プログラムの開発、純粋な学問的研究等を目的とする場合には、調査・解析対象プログラムに対し市場における不利な影響を与えるものではなく、商品開発のインセンティブを減退させる結果にはならないから、これらの場合には権利は制限されるべきである。

調査・解析に伴う複製又は翻案に関する権利制限規定を設けるべきであるが、許容される調査・解析は特定の目的（相互運用性の確保、エラー修正等）のためのものに限定すべきであるとの意見

(主な理由)

- ・ 相互運用性確保、エラー修正、著作権侵害の発見などは正当な目的として許容されるべきである
- ・ 新たな創作活動へのインセンティブを与えるという著作権法の基本的な目的に照らし、権利の制限は社会要請により合理性があると認められる必要最小限の範囲にとどめるべきである。

調査・解析に伴う複製又は翻案を認める必要はなく、権利制限規定は設けるべきではないとの意見

(主な理由)

- ・ 著作権法上著作権者は著作物のいかなる複製又は翻案についても排他的権利を専有するのが原則であり、プログラムの調査・解析に伴う複製又は翻案につき特別扱い

する必要はない。

- ・ 既存プログラムの連続的な変更による海賊行為に利用されることになる。
- ・ 調査・解析は、プログラムの創作に必要な費用及び時間を回避し対象プログラムの著作権者に対する商業的優位を得るために用いられるものであるから、それに伴う複製又は翻案を許容すると、著作物の通常の利用を妨げ、著作者の正当な利益を不当に害することになる。

#### エ 結論

そして、同報告書は、これら各見解を踏まえ、「…確定的な判断を下すためには、プログラムの研究・開発に係る技術の状況、産業の実態等を見極めつつ、著作権法上それらをどのように評価するかについての詳細な検討がなお必要であることが明らかになった。」と述べるとともに、国際的動向に関しては、「…立法による対応の一つの先例と考えられる EC ディレクティブについても、許容される範囲が必ずしも具体的に明確になっておらず、今後の実際の運用状況を注視する必要があるほか、米国をはじめ諸外国の法解釈、判例の動向についても見極める必要があり、いまだ国際的な動向も定着しているとは言い難いことが指摘された。」とされ、これらを踏まえた最終的な結論としては「現時点では本協力者会議として具体的な法改正の内容を提言するとの結論を得るには至らず、当面は現行法の解釈に関する判例、学説等の発展を待つとともに、今後の国内外の状況の進展に応じ改めて検討を行うことが適当と考える。」という判断がなされるに至っており、いわば結論先延ばしの形で終了している。

このように結論先延ばしとされた背景には、当時、米国のソフトウェア産業から、リバースエンジニアリングを適法とする立法化に対して強硬な反対意見が出されたことが影響しているとされる<sup>7</sup>。

なお、同報告書は、参考として、仮に権利制限規定を設けることとした場合に、どのような考え方があるかについても、(1) 許容される目的（無限定とする見解、競合プログラムの開発等の特定目的の場合は許容されないとする見解、エラー修正等特定の目的の場合のみ許容すべきとする見解）、(2) 許容される行為（調査・解析の過程における必要な限度の複製又は翻案とする見解、許容される目的を達成するための調査・解析の過程における必要不可欠な限度の複製又は翻案とする見解）、(3) 付加的条件の必要性（付加的条件は不要とする見解、必要な情報が予め利用可能でないこと、代替手段がないこと等を条件とすべきとする見解）、(4) 許容される行為の主体（主体を限定しないとする見解、プログラムの複製物を使用する正当な権原を有する者に限定すべきとする見解）、(5) 調査・解析の過程で作成された複製物又は翻案物の廃棄（廃棄義務は不要とする見解、調査・解析の目的達成後は廃棄しなければならないとすべきとする見解、プログラムの複製物を使用する権原を失った後は廃棄しなければならないとすべきとする見解）、(6) 調査・解析

---

<sup>7</sup> 「リバースエンジニアリング、文化庁、法制化見送り」（日本経済新聞平成6年5月31日朝刊）等。

の過程で作成された複製物又は翻案物の公表、頒布等の禁止（公表、頒布等の禁止については異論がないとされている。）、（7）入手した情報の扱い（調査・解析の結果入手した情報については、許容される目的以外のために利用することは禁止されるべきであるとする見解、利用は制限されるべきでないとする見解）、（8）セーフガード規定（著作権者の利益を不当に害する場合はこの限りでないとするセーフガード規定を設けるべきとする見解、セーフガード規定は不要であるとする見解）、（9）契約との関係（権利制限規定で許容される行為を禁止する契約も有効であるとする見解、そのような契約は無効であるとする見解、プログラムの種類、性格等を踏まえて効力は決せられるとする見解）、（10）通知義務（調査・解析を行った者に著作権者に対する通知義務を課す規定を設けることを検討すべきとする見解）、の各点から検討を加えている。

#### オ 現行法の解釈

同報告書は、上記結論を述べた後、「参考」として、現行法の解釈により調査・解析に伴う複製又は改変を一定の範囲で許容することの可能性についても報告を行っており、ここでは、①著作権法第30条以下の権利制限規定は限定列举であり、プログラムの調査・解析に関する規定がない以上、現行法上認められないとする見解、②接続の確保、エラーの除去等のプログラムの保守、改良及び移植を行う前提として複製又は翻案を伴う解析を行うことは、著作権法第47条の2第1項により、プログラムの複製物の所有者が自らのコンピュータにおいて利用するために行う場合は許容されているとする見解、③著作権法第1条の「文化的所産の公正な利用」という目的に鑑みれば、公正な目的のためのプログラムの調査・解析に伴う複製又は解析を著作権侵害として主張することは民法第1条の権利濫用に該当し、信義誠実の原則に反するとする見解、④調査・解析の過程において中間的に複製物又は翻案物が生じてもそれは複製物又は翻案物の固有の目的による利用に供されるものではないので、法的な意味での複製又は翻案とは評価されないとする見解、がそれぞれ指摘され、それぞれが持つ問題点（批判）と共に紹介されている

#### (2) 調査研究協力者会議報告書公表以前の論文、公表直後の論文等

リバースエンジニアリングの著作権法上の問題については、調査研究協力者会議報告書の公表以前より、様々な研究結果が発表されており、また、同報告書公表に前後し、同報告書の内容に言及する優れた論文も多い<sup>8</sup>。しかしながら、これらについては、本稿におい

---

<sup>8</sup>主なものとして、三木茂「リバースエンジニアリング」（ジュリスト928号78頁、同929号60頁、1989）、山地克郎「リバース・エンジニアリングに関する技術面からの考察（概要）」（AIPPI Vol. 34 No. 11、638頁、1989）、渡辺左千夫・寺本振透「リバース・エンジニアリングと著作権法（上）（中）（下）」（NBL424号17頁、同426号22頁、429号11頁、1989）、阿部浩二・北川善太郎・斎藤博「リバース・エンジニアリングの法的枠組み法モデルの提唱」（AIPPI Vol. 35 No. 3、136頁、1990）、高石義一「コンピュータ・プログラムの所謂『リバース・エンジニアリング』（逆コンパイル・逆アセンブル）についての一考察（「法とコンピュータ」8号84頁、1990）、藤木久「リバースエンジニアリングに関する覚え書き」（「民事特別法の諸問題 第3巻」、第一法規、1990）、（財）ソフトウェア情報センター編「コン

ては、紙幅の都合上、その内容については触れないものとする。

### 2.3. 調査研究協力者会議報告書公表後の政府機関による見解、裁判例議論の進展

調査研究協力者会議報告書公表後における公的機関による主な見解や裁判例として、以下のものがあげられる。

#### (1)公正取引委員会「ソフトウェアライセンス契約等に関する独占禁止法上の考え方—ソフトウェア独占禁止法に関する研究会中間報告書—」（平成14年3月20日公表）

公正取引委員会が平成14年3月20日に公表した「ソフトウェアライセンス契約等に関する独占禁止法上の考え方—ソフトウェア独占禁止法に関する研究会中間報告書—」<sup>9</sup>（以下、「中間報告書」という。）において、リバースエンジニアリングの法的問題につき論じられており、ディスアセンブル・デコンパイルについては、侵害に当たるという立場がある一方で、著作権法上も許容されるとされる見解もあるということが紹介されている（同報告書27頁）。その上で、独占禁止法上の解釈としては、ソフトウェアの製品市場、技術市場におけるライセンシーの研究開発活動が阻害され、ハードウェアの製品市場等における公正な競争が阻害される場合（具体的には、当該ソフトウェアのインターフェース情報が必要であり、ライセンサーが当該インターフェース情報を提供しておらず、ライセンシーにとって、リバースエンジニアリングを行うことが、当該ソフトウェア向けにソフトウェアやハードウェアを開発するために必要不可欠な手段となっているような場合）には、不公正な取引方法（具体的には一般指定13項拘束条件付取引）に該当し、そのようなリバースエンジニアリング行為を禁止するライセンス契約の条項は、著作権法上の権利の行使と認められる行為とは評価されないとして違法になるとの見解が示されている。

#### (2) 文化審議会著作権分科会法制問題小委員会 契約・利用ワーキングチーム検討結果報告（平成18年7月）

同報告は、契約によるオーバーライドの問題（「著作権法第30条以下の権利制限規定が定めている自由利用の態様や範囲を契約により『ひっくり返す（オーバーライドする）』ことが可能かどうか」という問題）につき論じたものであるが、「リバースエンジニアリング

---

ピュータ・プログラムのリバースエンジニアリング—実態と法的評価—」（1990）、泉克幸「著作権法と著作物創作の中間段階における複製」（工業所有権法研究1990-12-No. 106、12頁、1990）、大橋正春「リバースエンジニアリング」（「コンピュータと法律」64頁、共立出版、1992）、北川善太郎「技術革新と知的財産法制」174頁（有斐閣、1992）、山中伸一「コンピュータ・プログラムのリバース・エンジニアリングについて（上）（下）」（ジュリスト1019号102頁、1020号137頁、1993）、根岸哲編著「コンピュータと知的財産権」121頁、中山信弘「ソフトウェアの法的保護（新版）」127頁（有斐閣、1993）、内田晴康「コンピュータ・プログラムのリバース・エンジニアリングについての考え方」（特許管理Vol. 44 No. 12、1671頁、1994）、詹智玲「プログラムのリバース・エンジニアリングの著作権保護」（本郷法政紀要4号290頁、1995）等。

<sup>9</sup> <http://www.jftc.go.jp/pressrelease/02.march/020320.pdf>

等の制限について」と題し、

リバースエンジニアリング、逆コンパイル、逆アセンブル等を行うこと自体は著作権が働く利用行為ではないものの、これを制限することについて、当事者間では合意をしたのであれば、契約自由の原則に基づき、基本的にはこれを無効とする理由はない。

ただし、特許法では、試験又は研究のためにする特許発明の実施については特許権が及ばないものとされており（特許法第69条）、リバースエンジニアリング等により試験又は研究を行うことが認められている。これは、特許権の効力を試験又は研究にまで及ぼすことは、かえって技術の進歩を阻害するという趣旨によるものである。同様の発想に基づけば、技術的性格の強いプログラムの著作物についても、リバースエンジニアリング等を認めることで技術進歩が促進されるとの観点も考えられることから、場合によっては無効とすべきであるとの考えもありうる。

また、競争法の観点からも、とりわけ相互接続性の確保を目的として行うものについては、リバースエンジニアリング等の制限を無前提に認めるのは問題があると考えられる。

なお、仮に、契約によるリバースエンジニアリング等の制限が不当であり、契約が無効と判断されるべき場合があったとしても、一般に、リバースエンジニアリング等を行う過程には複製及び翻案を伴う。このような複製及び翻案行為については、現行著作権法の解釈で一定の範囲で許容されると考えられる一方で、著作権法上の複製権及び翻案権の侵害の責任を問われる可能性もあることから、これに対応するため、必要な範囲で権利制限規定を設けることも考えうるのではないかとの指摘があった。

と報告されている。

### (3)東京地裁平成18年2月10日判決

本書で検討しているような、デイスアセンブリ・デコンパイルの違法性につき、正面から争われ、裁判所による判断がなされた事件は、存在しないが、若干参考になると思われる裁判例として、東京地裁平成18年2月10日判決がある。当該事件は、原告（ネットプレーン株式会社）は、ライブラリを被告（松下電器産業株式会社）にライセンスしており、当該ライセンスにおいては、リバースエンジニアリング禁止規定が存するという事実関係において、原告と被告の開発等がうまくいかなかったことから、最終的に被告が、別個に、「関数名、引数、戻り値の特定」「特定された関数の処理内容の推測及び実装」という二段階の開発手法により、被告ライブラリを開発し、これを使用した被告行為の著作権侵害が一つの争点となったものであったところ、裁判所は、かかる争点に関し、「被告ライブラリが原著作物である原告ライブラリの創作的な表現を再生していると認めることはできないし、また、被告ライブラリが開発行為が原告ライブラリに依拠して行われたものと

認めることもできない。これに対し、原告は、原告ライブラリによる処理結果としての出力情報を調査解析して被告ライブラリが作成されたことをもって、違法なリバースエンジニアリングである旨主張する。しかしながら、原告ライブラリへの入力と出力との関係を調査解析して得られるものは、当該関数の実現している機能であり、それは、飽くまでアイデアにすぎないものとして著作権法上保護されないものといわざるを得ない。よって、この点に関する原告の主張は採用することができない。」という判示している。

## 2.4. 現在の議論状況とまとめ

### (1) 現在の議論状況

上記のとおり、平成6年5月に公表された調査研究協力者会議報告書においては、「…確定的な判断を下すためには、プログラムの研究・開発に係る技術の状況、産業の実態等を見極めつつ、著作権法上それらをどのように評価するかについての詳細な検討がなお必要であることが明らかになった。」「…立法による対応の一つの先例と考えられる EC ディレクティブについても、許容される範囲が必ずしも具体的に明確になっておらず、今後の実際の運用状況を注視する必要があるほか、米国をはじめ諸外国の法解釈、判例の動向についても見極める必要があ(る)」と述べ、「現時点では本協力者会議として具体的な法改正の内容を提言するとの結論を得るには至らず、当面は現行法の解釈に関する判例、学説等の発展を待つとともに、今後の国内外の状況の進展に応じ改めて検討を行うことが適当と考える。」といわば結論が先送りにされ、更なる議論の必要性が強調されていた。にもかかわらず、調査研究協力者会議報告書以降、判例、学説等の積み重ねは、ほぼ皆無に等しいといってよい状況にあり<sup>10</sup>、文化庁分科審議会著作権分科会において立法化の動きが表面化したという事実も全く認められない。

調査研究協力者会議報告書公表時においても、そして現在においても、我が国著作権法の解釈上、リバースエンジニアリングの過程におけるプログラムの複製又は翻案が著作権侵害には該当しない(あるいは該当すると解すべきではない)とするのが、変わらぬ通説的理解であるといつてよい。代表的な概説書、例えば中山信弘「著作権法」(有斐閣、2007年)においては、リバースエンジニアリングに関し、「技術は積上げの性質を有しているため、リバースエンジニアリングは技術発展にとって必要であり、産業財産権の分野では一般的に認められている(特69条1項、新案26条、半導体12条2項)。それに対して著作権法は表現保護法であるため、作品を見たり聞いたりするだけで表現を感得できるはずであり、リバースエンジニアリングの必要性は少なく、それを認める規定は存在しない。しかし絵画や小説とは異なり、プログラム、特にオブジェクト・プログラムの本質は技術であり、それを眺めただけでは内容を知ることができず、何らかの解析をして始めて

---

<sup>10</sup>調査研究協力者会議報告書以降の主要なリバースエンジニアリングの法的問題に関する論文としては、椛山敬士「ソフトウェアの著作権・特許権」29頁(日本評論社、1999)、高橋明弘「知的財産の研究開発過程における競争法理の意義」165頁(国際書院、2003)等が存する。

中身であるアイデアを知ることができる。著作権法における複製概念は単に物理的な複製の有無によってのみ決定されるべきではなく、規範的に捉えるべきであり、プログラムの中身を知るための解析過程に複製・翻案行為が介在しても、必要な限度で、原則として著作権法上の複製・翻案ではないと解すべきであろう。このリバースエンジニアリング問題は、特にプログラムの互換性確保にとって重大な意味を有しており、少なくとも互換性確保目的のための複製・翻案は違法とすべきではないし、この点に関しては国際的なコンセンサスができあがりつつあるように見える。」と述べている（104頁、105頁）。また、田村善之「著作権法概説（第2版）」（有斐閣、2001年）は、「プログラムは、人間にとって理解可能なソース・コードの形にしない限り、その思想を読み取ることができない。表現のみを保護し、思想の自由利用を認めようとする著作権法の建前から考えると（10条3項3号も参照）、オブジェクト・プログラムを著作物として保護することにより、その思想を読み取る行為までも禁止するとすれば、著作権法の自殺行為に近い」と述べた上で、「…狭義のリヴァース・エンジニアリングに随伴する必要限度の複製、翻案は著作権侵害にならないと考えるべきであろう。そして、リヴァース・エンジニアリングの結果、開発した新たなプログラムが元のプログラムの類似性の範囲内にある場合にも、それにより遡って一連のリヴァース・エンジニアリングに関連する行為が違法となるわけではなく、その新たなプログラムがリヴァース・エンジニアリングに必要な限度を超えて複製された場合に…（中略）…、その行為を捉えて著作権侵害を問うることにすれば足りるといえよう」としている。さらには、作花文雄「詳解著作権法（第3版）」（ぎょうせい、2004）においても、「著作権法により、複製権が付与されているとしても、制限規定で明示的に除外されていない以上、文字通りいかなる『複製』にも権利が及ぶものと解すべきではない。先人の文化的所産を踏まえて新たな創作活動を促進することは、法制度の趣旨にも適うものであり、プログラムに限らず、言語の著作物や美術の著作物であっても、新たな創作活動の作業過程における複製は許容されるものと解すべきである。米国法におけるフェア・ユースの法理は存在しないものの、権利の濫用の法理や権利の本来的な内在的制約などの考え方により妥当な結論を導き出すべきものとする。」と述べられているところである（691頁）。

これらはいずれも、調査研究協力者会議報告書において「参考」として紹介されている現行法の解釈可能性に他ならず、同報告書以降、議論の状況に変化がないことを物語っているものといえよう。

## (2)今後の方向性

以上のように、わが国においては、リバースエンジニアリングは著作権侵害に該当しない適法行為であるとする見解が、（その理由付けに違いは認められるものの）通説的なものであるといつてよい。

しかしながら、我が国著作権法は、「複製」の定義につき、「印刷、写真、複写、録音、録画その他の方法により有形的に再製すること」と定めている以上（第2条1項15号）、

文言上はリバースエンジニアリングの過程における複製がこれに該当しうるとは否定しがたく、また、権利制限規定については、これを限定列挙であると解するのが通説的理解であり<sup>11</sup>、裁判例上も、米国におけるフェアユースの法理は明確に否定されている以上<sup>12</sup>、現行法の下で、リバースエンジニアリングの過程における複製・翻案が著作権侵害に該当しないという解釈に一抹の不安が残るのもまた事実であるといわねばならず<sup>13</sup>、さらには、これを著作権侵害であると解く根強い見解が一部に存することも事実である<sup>14</sup>。

このように、法解釈が一種曖昧なものであるという状況が、ディスアSEMBル・デコンパイルを必要不可欠とするソフトウェアの脆弱性を調査する立場に対して萎縮効果を与えていることは想像に難くなく、情報セキュリティ産業の発展、ひいてはセキュリティリスクの防止という観点からすれば、現在の状況は決して望ましいものとはいえない。

その一方で、いうまでもなく、今日のネットワーク社会において、ソフトウェアの脆弱性調査の必要性は極めて高く、かつ、社会的な関心は高いものといえることができる（社会的な関心を指し示すものとして、リバースエンジニアリングを中心的に取扱う書籍の公刊が相次いでいることや、リバースエンジニアリングをテーマにしたシンポジウムが開催されるようになってきていることなどがあげられる。）。

以上に照らせば、我が国において、脆弱性調査目的のためのリバースエンジニアリングについて、これが著作権侵害に該当しない合法的なものであることを確認することは極めて大きな意義が存するものといえるが、それに留まらず、調査研究協力者会議報告書から14年を経た今、リバースエンジニアリングが適法であることを著作権法上明確に規定すべく、具体的な立法作業に着手すべき時期に來たといわねばならない。そして、調査委員会は、以下において、そのような立法作業の一助とすべく比較法的な見地から、脆弱性の調査のためのリバースエンジニアリングの許容性についての調査を行ったのである。

---

<sup>11</sup> 権利制限規定につき詳細に論じた近時のものとして、上野達弘「著作権法における権利制限規定の再検討ー日本版フェア・ユースの可能性ー」（コピーライト2007年12月号2頁）があり、同講演録では、現行著作権法上、権利制限規定が存せず、その法的評価に問題が生じる種々の行為を紹介した上で、かかる不都合を解決する手法として、権利制限規定に（「受け皿規定」としての）一般条項を設けることを立法論として検討すべきと提言している。

<sup>12</sup> 例えば、東京地判平成7年12月18日判時1567号126頁（ラストメッセージ in 最終号事件）、東京高判平成6年10月27日知的裁集26巻3号1151頁（ウォールストリートジャーナル事件）等。なお、東京高判昭和51年5月19日無体裁集8巻1号200頁（パロディモンタージュ事件）は、「本件モンタージュ写真の作成は、他人の著作物のいわゆる『自由利用』（フェア・ユース）として、許諾さるべきものと考えられる」とし、フェアユースの抗弁を肯定したが、最高裁はこれを否定している（最判昭和55年3月28日民集34巻3号244頁）。

<sup>13</sup> これらに加え、権利濫用や信義則違反といった一般条項が頼みの綱、という解釈も望ましいものとはいえないだろう。

<sup>14</sup> 例えば、（財）ソフトウェア情報センター編「ソフトウェアと独占禁止法に関する調査研究報告書」（1997年）23頁以下においては、日本アイ・ビー・エム(株)の担当者が、リバースエンジニアリングは著作権法上明らかに違法であるとの見解を記している。

### 3 諸外国における脆弱性調査のためのリバースエンジニアリングの適法性をめぐる議論

#### 3.1. 概観

我が国における脆弱性調査のためのリバースエンジニアリングの適法性について検討するために、諸外国の国内法の状況を以下において、概観することにする。もっとも、各国において、かかる論点についての議論をみる前に、米国における公正利用の法理とリバースエンジニアリングとのかかわり、およびEUにおける著作権に関する指令を紹介しておくことは有意義であろう。

#### 3.2. 米国における公正使用の法理とリバースエンジニアリング

米国においては、リバースエンジニアリングは、適法な調査の手段であるとしてフェアユースの一つとして認められている。これは、従来からの判例法においてもそうであるし、制定法にもその根拠がある。そして、フェアユース例外は、著作権法第107条によって定められており、コンピュータプログラムについても適用される。したがって、EU諸国において、ソフトウェア指令によって許容される相互運用性のためのリバースエンジニアリング、エラー修正のための複製、動作の観察の行為については、米国においては制定法の具体的な定めを議論する必要もないほどである。

ソフトウェアについて、より一般的にリバースエンジニアリングを認める判決例としては、**Atari Games Corp. v. Nintendo of America, Inc., 975 F.2d 832 (Fed. Cir. 1992)**、**Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir.1993)**、**Sony Computer Entertainment, Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000)**がある。

そして、連邦著作権法においては、独自に創作したコンピュータプログラムとその他のプログラムとの互換性を達成するためにリバースエンジニアリングを行うことは、フェアユースとされている。**Bowers v. Baystate Technologies, Inc., 320 F.3d 1317 (Fed. Cir. 2003)**参照。脆弱性調査のためにデコンパイル技術を利用する場合の合法性についての具体的な判決例は、存在しないが、上記の法理からして、調査のための手法として趣旨で認められるものと思われる。なお、エラー修正のための類似の規定は、著作権法117条にある。

著作権保護システムとの関係で定められているデジタルミレニアム著作権法においては、そのような相互運用性確保のためのリバースエンジニアリングを許容する規定がある(デジタルミレニアム著作権法第1201条(f)(1))。

もっとも、契約書の条項におけるリバースエンジニアリングの禁止の条項の効力については、議論がある。この問題は、一般にはフェアユース例外について、契約が消費者契約であるときに、これを規制する条項は有効かという形で議論がなされている。リバースエンジニアリングは、公共政策の見地から、高いものとして位置づけられている。しかしながら、多くの裁判所は、ライセンス契約における規制条項の有効性を認めている。

### 3.3. リバースエンジニアリングをめぐるEU諸国における制定法

#### (1) ソフトウェア指令

EU諸国が、その域内の法律を調和させようとするときに、最初にその調和が必要となったものの一つは、コンピュータプログラムについての法的な規制である。このための規制についての定めは、「コンピュータ・プログラムの法的保護に関する1991年5月14日の理事会指令」であり、「ソフトウェア指令」もしくは「プログラム指令」といわれる。この「ソフトウェア指令」は、コンピュータプログラムを著作権によって保護するようにするものである。そして、そのうち、ソフトウェアのリバースエンジニアリングに関係する指令の条項を抜き出すと以下のようなになる<sup>15</sup>。

#### 第5条（制限される行為の例外）

- 1 契約に特段の定めがないときは、エラー修正を含め、適法な所有者がその所定の目的に沿って、コンピュータ・プログラムを使用するために必要な場合には、前条（a）及び（b）に掲げる行為（注：プログラムの複製及び翻案、改変等）は権利者による許諾を必要としない。
- 2 コンピュータ・プログラムを使用する権利を有している者によるバックアップ・コピーの作成は、その使用に必要な限り、契約によって妨げられない。
- 3 コンピュータ・プログラムの複製物を使用する権利を有している者は、権利者の許諾を得ることなく、プログラムの要素の基礎になるアイデア及び原理を確認するため、プログラムの機能を観察、研究又は検査する権限が与えられる。ただし、当該プログラムのロード、ディスプレイ、ラン、トランスミット、ストアのいずれかを実行中に当該行為を行う場合に限る。

#### 第6条（デコンパイルーション）

次の条件が満たされる場合で、第4条（a）及び（b）にいうコードの複製及びその形式の翻訳が、独立して創作されるコンピュータ・プログラムと他のプログラムとの相互運用性（interoperability）を達成するために必要な情報を得るために必要不可欠なときは、権利者の許諾は必要とされない。

- (a) これらの行為が、利用許諾を得た者（licensee）、プログラムの複製物を使用する権利を有する者又はそれらの者に代わって権限を与えられた者によって行使されること；
- (b) 相互運用性を達成するのに必要な情報が（a）に掲げる者にあらかじめ利用可能でないこと；及び
- (c) これらの行為が、相互運用性を達成するのに必要なオリジナル・プログラムの一部の範囲に限られること。

---

<sup>15</sup> ソフトウェア指令の翻訳は、前出協力者会議の報告書(注5参照)による。

2 前項の規定は、その適用によって得られる情報を次のように利用することを許容するものではない。

- (a) 独立して創作されるコンピュータ・プログラムの相互運用性を達成するため以外の目的のために使用すること；
- (b) 独立して創作されるプログラムの相互運用性に必要なときを除き、他の者に提供すること；
- (c) 実質的に表現が類似しているコンピュータ・プログラムの開発製作及び販売又は著作権を侵害するその他の行為のために使用すること。

3 「文学的及び美術的著作物の保護に関するベルヌ条約」の規定に沿い、本条の規定は、権利者の正当な利益を不当に害し、又はコンピュータ・プログラムの通常の利用を妨げるような方法の適用を許すものと解釈してはならない。

#### (2) コピーライト指令<sup>16</sup>

理事会は、ソフトウェア指令に引き続いて、データベース指令、貸与権および貸出権指令、放送およびケーブル再送信指令などを発表した。しかしながら、これらの一連の指令は、1988年のグリーンペーパーに依拠していた。グリーンペーパーにおいては、1対1の複製、自宅での複製が、技術の進化によって劣化なしにおこなわれることにより配布や貸与の問題がおきることについて議論がなされていたが、その状況は、インターネットによって変化してしまった。海賊複製行為についての主な関心は、インターネットに向けられるようになったのである。デジタル化によって、著作物や著作隣接権によって保護された作品の複製、改変、配布がなされ、それについて、追跡がなしえないという新たなリスクが出現したのである。

このような状況のもと、理事会は、指令をインターネット時代に合わせる必要があった。理事会は、「情報社会における著作権および関連権のハーモナイゼーション指令」(Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society)を公表し、情報社会に関して、著作権や隣接権についての種々の局面についての調和を計ろうとした。この指令は、一般に、EU著作権指令(EUCD)もしくは、情報社会指令(Infosoc)といわれている(なお、本報告書については、以下、コピーライト指令という)。

この指令のポイントは、

- ・ 著作者、実演者、制作者および放送組織は、いかなる手段の複製、公衆への送信および配布について排他的権利を有する
- ・ 技術的プロセスを構成する一時的な複製行為に対して排他的な権利に対する狭義な「強行法規として (mandatory)」の例外を設定する

---

<sup>16</sup> 日本語の翻訳として原田文夫訳「情報社会における著作権および関連権の一定の側面のハーモナイゼーションに関する欧州議会およびEU理事会のディレクティブ」(社団法人著作権情報センター、2001)

・ 「技術的保護手段」に対して、みずからもしくは、第三者が回避する行為を規制する手段を設ける

・ 構成国家が、国内法化を望む際に選択をなしうる、著作権保有者の排他的権利の「任意的 (optional)」例外のリストを作成した

・ 特定の例外行為の実行に対して、著作権保有者が、「適切な補償」を受領しうることである。

このコピーライト指令は、コンピュータプログラムに関連するものではないが、技術的保護手段等についての記述を含んでいたり、また、この指令への対応を機に各国国内法においてコンピュータプログラムに対する例外規定の適用関係について整理されたりして興味深いものがあるといえよう。

### (3) その余のEUにおける著作権に関する指令

EUにおいては、その後も知的財産権に関連する指令を明らかにしているが、そのなかで、興味深いものは、知的財産権行使指令 (**Directive 2004/48/EC on the enforcement of intellectual property rights**) である<sup>17</sup>。この指令においては、証拠保全手続、侵害配布ネットワークや侵害品の出所に関する情報開示の定め、そのための中間的差止命令の定め、審理後の救済手段などが論じられている。この指令については、特に中間的差止命令に関して、ISP に対する命令も可能とされているために、ISP の負担を増加させるのではないかと議論されたところでもある。

### (3) 英国

1988年英国著作権、デザイン、パテント法 (以下、CDPA1988という) は、著作権侵害行為に関連して、第29条および第30条において「公正使用抗弁(フェア・ディーリング)」<sup>18</sup>を提供している。すなわち、

(1) 研究・個人的学習のための公正使用について、第29条(1)および(1C)

(2) 批判または評論のための公正使用について、第30条(1)

(3) 時事についての報告の目的のための公正使用について、第30条(2)

を明らかにしたさいに、責任を負わないとしている。しかしながら、ソフトウエア指令においては、上記のような公正使用抗弁の適用は、一般に制限されており、英国でも、ソフ

<sup>17</sup> 指令本文については、

[http://eur-lex.europa.eu/pri/en/oj/dat/2004/l\\_195/l\\_19520040602en00160025.pdf](http://eur-lex.europa.eu/pri/en/oj/dat/2004/l_195/l_19520040602en00160025.pdf)

なお、要領よく説明するものとして Will James<sup>1</sup>, Joel Smith, and Herbert “The IP enforcement directive Is further legislation really necessary to level the playing field? A UK perspective” Computer Law & Security Report vol.20 no.5 2004 がある。

<sup>18</sup> CDPA は、公正使用抗弁以外に、以下の抗弁を定める

(1)付随的使用 31条(1)

(2)公共の利益のための公開 (制定法の定めはない)

(3)図書館利用 37乃至44条

(4)教育利用

など

トウェア指令の国内法化によってもたらされた変更によって、結果として、研究、個人的学習の抗弁は、コンピュータプログラムについては、排除されている(同法第29条(4))。

その一方で、ソフトウェア指令第6条のデコンパイル例外は、CDPA1988の第50条Bにおいて定められている。もっとも、第50条(B)は、目的が、相互運用性のためであることを必要としており、脆弱性調査目的のためにリバースエンジニアリングをすることは、相互運用性のためであるとは考えられないので、かかる条文をもとに脆弱性調査目的のためのリバースエンジニアリングを合法であるということはできないものと考えられている。

一方、ソフトウェア指令第5条(1)における適法な使用者の抗弁は、CDPA1988第50条Cにおいて定められている。セキュリティの脆弱性が、第50条Cの「エラー」となるかどうかという点についての論考を指摘することはできず、第50条Cの文言およびその根底をなすソフトウェア指令からは、そのような広い解釈が目されていたかどうかは、疑問である。

また、ソフトウェア指令5条(3)の行為について、CDPA1988は、第50条BAによって「コンピュータプログラムの観察、学習、テスト」を例外として認めている。もっとも、この例外といえども、コンピュータプログラムのデコンパイルを例外として認めることにはならないと解されている。

また、これらの例外行為を契約上の規定によって排除しうるかどうかという点については、第50条C(1)によれば、適法な使用者の抗弁については、契約上の規定による排除が認められている。それに対して、「コンピュータプログラムの観察、学習、テスト」例外や相互運用性確保のためのリバースエンジニアリング例外については、これを排除する規定は、無効なものとしてされている。

もっとも、このエラー修正例外について契約によって排除しうるという立場については、反論もあり、そのような契約条項についても、著作権者みずから修正をしないことが明らかかな場合、修正することができない場合については、かかるリバースエンジニアリング禁止条項の効力を否定すべきではないかということが議論されている。

なお、CDPA1988は、従来の公正使用の抗弁が、プログラムにおいては、排除されることを明らかにしているが、公益による排除の抗弁まで排除するものではない。

#### (4) フランス

フランスにおいては、1991年5月14日指令(以下「指令」という)は、1994年5月10日法律361号により、知財法典の中にL.122-6-1条IVおよびVの規定が設けられ国内法化された。この規定は、デコンパイルを相互運用性の目的での場合にのみ許し、その他のすべての場合に禁止して、ソフトウェアのデコンパイル禁止の原則を設定した。しかしながら、この条文との関係では、コンピュータセキュリティの脆弱性を明らかにする目的のためのデコンパイル操作は、独立して作成されたソフトウェアを相互運用できるようにするためのものではないと考えられている。従って、そのような脆弱性調査のためのデコンパ

イル行為は、フランスでは、デコンパイルについての例外の適用をうけないことになる。この理を明言する判決例が存在する（**Cour d'Appel de Paris, 13e chambre, 21 fév. 2006 : RLDI juill.-août 2006, p. 24, n° 528**）。

また、エラー修正に関する規定は、知財法典 **L.122-6-1** 条 I に国内法化されている。これが、脆弱性調査の目的でのリバースエンジニアリングに適用されるかどうかという点については、具体的な判決例は、存在しない。また、指令 5 条（3）における趣旨は、知財法典 **L.122-6-1** 条 III において、表現されている。

脆弱性調査のためのリバースエンジニアリングがフランス著作権法上許容されるかどうかという問題は、フランスでは、きわめて新しい問題であると認識されている。

なお、リバースエンジニアリングを契約上、禁止することができるのかという問題については、知財法典 **L.122-6-1** 条 I は、あらゆる調整行為（「バグ」や「セキュリティの脆弱性」を修復することを目的とする）について、ソフトウェアの著作者が契約によってそれらの行為を許諾することができることを意味している。したがって、契約によって、リバースエンジニアリングを禁止しているのであれば、その定めは有効であるということになる。

#### （5）ドイツ

ドイツにおけるリバースエンジニアリングの合法性は、1965年著作権法のいくつかの制定法の規定に関連している。ドイツ著作権法は、ソフトウェア指令第6条に対応して、第69条eにおいて、相互運用性（**interoperability**）を実現するために限定して、リバースエンジニアリングを用いることを許容している。この例外は、裁判所によって広く認められている。たとえば、デュッセルドルフ控訴裁判所は、相手方当事者が、リバースエンジニアリング例外を誤解したということを証明しなければならないと解釈している。

また、同法第69条d(1)は、ソフトウェアの複製（**reproduction**）と改変（**alteration**）は、適法な取得者によってその目的に適合する使用（エラー修正を含む）に必要なかぎりではなされる場合には、権利保有者の許諾を必要としないとしている。これは、同指令第5条（1）に対応している。そして、多くの論者は、ソフトウェア指令第5条1項すなわち、第69条d(1)は、リバースエンジニアリングにも適用しうると解釈されている。それゆえに、ソフトウェアが、重大なバグを有しており、リバースエンジニアリングによってのみ調査し、そして、修正しうるときに、合法であると解釈しうるものとされている。また、本条に定めるエラーは、広義に解されている。エラーは、（開発）後に明らかになったものも許容されるのでありアンチウイルスモジュールの実装は、この例外によって保護される。連邦最高裁判所が、先導的事案である“**Programmfehlerbeseitigung**”において論じているが、第69条d(1)は、第三者によってなされたテストさえも相互運用性目的であるとして正当化されると解している。その上、オーストリアにおいては、著作権法第40条d(2)で、ソフトウェアの改変を「利用者の必要に応じる」ための改変を許容する文言で定めており、そこでは、脆弱性調査の目的のためのリバースエンジニアリングが許容

されることになる」とされている。

さらに、第69条d(3)は、権限にもとづいてなすプログラミングのロード (loading)、ディスプレイ (displaying)、実行 (running)、送信 (transmitting) または、保存 (storing) におけるプログラム動作時に、プログラムの要素の根底にあるアイデアと原則をみきわめる、プログラムの機能を観察、研究、テストすることを許容している。それゆえに、脆弱性の問題調査のためのデコンパイルがここで保護されるかは、議論があるものの、この条項のもとで、広義にリバースエンジニアリング技術として論じられる行為のうち、多数<sup>19</sup>が、合法であると考えられる。

また、リバースエンジニアリング禁止条項の効力については、EUソフトウェア保護指令の曖昧さを根拠に、意見が分かれたが、連邦最高裁判所の先導的な事案である“**Programmfehlerbeseitigung**”においては、裁判所は、ソフトウェア指令第5条(1)は、強行法規的性質を有すると認識し、ソフトウェア制作者が、エラーを修正することができない、もしくは、修正しようとしめない場合でなければ、ソフトウェア制作者が、エラー修正のチャンスを自己のもとにとどめておくという契約を認めるにいたったのである。

### 3.4. オーストラリア

オーストラリアにおいては、著作権法第47D条が、ソフトウェア指令第6条に規定されたと同様の概念を含む条項を与えている。しかしながら、著作権法第47D条は、脆弱性評価のためのリバース・エンジニアリングを許可していない。

また、ソフトウェア指令第5条第1項に規定されたと同様の概念は、オーストラリアにおいては、第47B条(コンピュータ・プログラムの通常使用及び研究を理由とする侵害には適用除外を創設)および第47E条(エラー修正のための侵害には適用除外の創設)によって定められている。しかしながら、エラーという文言は、オリジナル・コピーに供与された仕様書またはその他の文書に従って、機能することを妨げるものでなくてはならないと条文上、定められているので、脆弱性は、一般に、機能を実際に「妨げる」ことはなさそうなので、(なおも可能性はあるとしても)、ネットワークその他の脆弱性がこの基準を充足することはなさそうとされ、かかる条文が脆弱性調査のためのリバースエンジニアリングの許容の根拠とはならないと考えられる。

しかしながら、オーストラリアにおいては、著作権法第47F条において、セキュリティテストを理由とする侵害に対する特定の例外を創設している。同条は、著作物のオリジナル・コピー、または、オリジナル・コピーがその一部をなすコンピュータ・システム、また

---

<sup>19</sup> ブラックボックス・テクニク、テスト・アプリケーション、ヘックス・ダンプ・コントロール、通信信号の記録、デバッガやライントレーサーの利用などを指す。また、フランクフルト地方裁判所は、69条eの意味における(正当化されず、禁止される)デコンパイルではなく、著作権法69条d(3)における自由なテストであるとして、近時、メモリーのブートセクターを複製し、ソフトウェアに関する記録をチェックするテストを許容した。

はネットワークの「セキュリティのテストをすること」または、「セキュリティの欠陥、または無権限アクセスへの脆弱性を、調査または修正する」過程における複製を許容する。この規定の適用によって、脆弱性調査のためのデコンパイル自体も許容されることになる。

## 4 検討

### 4.1.比較法的な調査結果

各国比較法的な結果を見ると、前出した調査研究協力者会議報告書の公表のあとに世界各国において、相互運用性目的のためのリバースエンジニアリングの許容性、適法な使用者の一定の複製を認める規定のなかにエラー修正を認める規定、実行中の観察の許容性を認める規定が制定された事実が明らかになった。具体的には、その間に、EU各国において、ソフトウェア指令に基づき法律が制定され、また、理事会は、各国の国内法化の状況についての評価を行っている状況にある。米国においては、デジタルミレニアム著作権法が定められ、特定の場合におけるリバースエンジニアリングの例外条項が制定法をもって明らかにされているのである。

そして、世界的には、この間における情報ネットワークの発展には著しいものがあり、それに対応して、情報セキュリティ活動の重要性、特に脆弱性調査のためのリバースエンジニアリングは、極めて重要なものとなってきているのも事実である。

しかし、具体的に脆弱性調査のためのリバースエンジニアリングが、複製権または翻案権の侵害ではないかという問題について考えると、各国の調査結果は、EU 諸国については、明確に肯定的な結果が報告された国は、存在しないということがいえる。その意味で、EU 諸国においては、そのようなリバースエンジニアリングの適法性の問題は、微妙であるといえるように思える。その一方で、米国においては、従来のフェアユースの概念で、そのようなリバースエンジニアリングの合法性をとらえることができるだろうとされること、また、オーストラリアについては、独自にセキュリティテストのための例外条項が導入されており、かかる条項の適用によって、脆弱性調査のためのリバースエンジニアリングの合法性が裏付けられるという報告も得ている。また、オーストラリアにおいては、「利用者の必要に応じる」ための改変を許容するという報告もされている。

もともと、EU 諸国において、脆弱性調査目的のためのデコンパイルの適法性が微妙であるといっても、具体的に活発に議論されている問題ではないようである。また各国の有力な論者は、その結果から生じる不合理さを認識しているところでもある。

### 4.2.脆弱性調査のためのリバースエンジニアリングの適法性について

まず、この問題については、わが国の法律上、システムレベル分析で使用される手法は、著作権法上、問題が生じるものではないということが明らかにされなくてはならないことになる。リバースエンジニアリングの適法性という議論で、このような手法まで、法的問題についての議論があると捉えることは誤解になる。

議論の中心は、脆弱性調査目的のためのディスアセンブル・デコンパイル作業による分析

ということになる。この段階で、複製権または翻案権の侵害ではないかという問題については、このデコンパイルされたコードが、一時的なメモリーへの展開を越えて、複製された場合に初めて法的な問題になる。本報告書においては、以下は、趣旨を明らかにするために、このデコンパイルの法的位置づけについて特定して論じることとする。その際には、具体的なコードの方法に随伴する脆弱性が分析されるのである。

そして、上述の検討の結果からいって、わが国において、このような目的のもとでのデコンパイル作業(とそれに伴う複製)は、著作権法上、複製権または翻案権の侵害ではないと明らかにされるべき時がきているものと考えられる。

まず、比較法的に一般的に許容されており、わが国でも、公正取引委員会の報告書が許容すべきとしている相互運用性確保目的のリバースエンジニアリングに比較するとき、あらたなプログラムの作成ということはあるので、著作権者の利益を侵害する程度は格段に低いものということができる。

また、現段階においては、コンピュータプログラムをネットワークに接続されたコンピュータによって使用することが当然の環境となっており、現代社会においては、脆弱性対応のためにも適法な使用者がみずからの判断でエラー修正のためにデコンパイルの手段を用いて、分析すること(そしてそのために複製すること)は当然に認められてしかるべきである。

ソフトウェア指令において、エラーを修正することが認められているものの、各国においては、いまだ、脆弱性修正にまで、その解釈が広められていないが、現代社会におけるネットワークコンピューティングの現実を前提とするときには、エラー修正に脆弱性修正を含むという広い解釈になるべきであろうと思われる。

ソフトウェア開発者といえども、その開発したソフトウェアに脆弱性がないようにと務めるのは、善良な開発者の義務ともいえるのであり、そのために、デコンパイルを認めないということができる正当な利益があるものとも思えない。ソフトウェアの脆弱性をできる限り減少させるというネットワークの安全性という利益を犠牲にしてまで、開発者の利益を守るべきものとは思えないのである。

現実に、ソフトウェアの脆弱性について、これを分析するのは、専門的な手法のもとになされるのであり、かかる分析が、そのような分析を業とする情報セキュリティ産業によって担われるのは当然と考えられるし、また、そのような産業の育成を推進するように社会的な環境を整えるべきであると考えられる。

また、上述のような方策をどのような手法で実現すべきかということになるが、法律の解釈の明確化という手法によることも可能であろうが、限界の明確化という観点からも、脆弱性調査をはじめとした情報セキュリティ対策のためのデコンパイルが法的に許容されることを明確にする立法的措置によってなされるべきである。

具体的な立法措置としては、比較法的な見地からして、以下のような手法が考えられる。(ア)著作権法 47 条の 2 を改正して、(他人のためにもする)脆弱性修正のための複製を認めるものとする(ドイツ報告書参照)。

(イ)公共目的のためのデコンパイルを許容する条項を設ける（アメリカ報告書参照）。

(ウ)コンピュータプログラムのセキュリティテストのためのデコンパイルを許容する条項を設ける（オーストラリア報告書参照）。

具体的には、本報告書を契機として、それぞれの方策について議論がなされることが望ましいものといえよう。

### (3) デコンパイル禁止の条項の法的効力について

また、脆弱性調査目的のためのデコンパイルが法的に許容されることを明確にする立法措置と同時に、契約書上のデコンパイル禁止条項の法的効力についても議論が深められるべきである。この点についての比較法的な検討もすでになされているように、ソフトウェア指令においては、エラー修正については契約書での制限が有効であるが、それ以外の相互運用性目的のため、プログラム動作中の観察・検査のための例外についてはこれらを制限する契約書上の規定は無効とされている。また、米国においては、原則としてかかる制限は、許容されているが、いろいろと議論はある。

ソフトウェア指令との関係で考えてみると、エラー修正についてのデコンパイル禁止の条項が、法的に正当なものとして許容されるのは、メンテナンスなどの契約がなされる場合に、そのソフトウェア提供者の法的な利益は、保護に値するので、その利益とも関連して、デコンパイルの禁止も許容すべきだという判断に基づくものである。そうだとすると、そのような利益をほとんど考慮するようなことがない場合、すなわち、一般消費者宛に販売がなされているソフトウェア、サポートポリシーによるサポートのみで、特別のサポートが契約によって定められているわけではない場合などについては、このようなソフトウェア提供者の利益を保護する必要はないものといわなければならない。また、ソフトウェア提供者は、自ら脆弱性を発見し、脆弱性をできる限りなくすべき立場にあるのは間違いないので、第三者のそのような発見行為を禁止するという正当な利益があるものもいえないだろう。

このような見地からすると、ソフトウェア提供者に正当な利益のないような場合のデコンパイル禁止条項については、これを法的に無効にすべきものと思われる。その場合、消費者契約法や民法の解釈によって無効となるべきものと思われるが、具体的な基準・場合などについては、いまだ明らかではない。この観点から、かかる条項の有効性についても議論が尽くされるべきと思われる。

## 第3 セキュリティ修正ソフトウェアと法律

### 1 セキュリティ修正ソフトウェア

本書において「セキュリティ修正ソフトウェア」とは、脆弱性に対して、これを排除、回避することを目的とするソフトウェアをいう。セキュリティパッチ・修正パッチということもできよう。

なお、セキュリティ修正ソフトウェアが、もともとのソフトウェアの動作に対して、どのような作用を具体的に追加するかという点については、本書においては、検討の対象とはしない。

### 2 第三者におけるセキュリティ修正ソフトウェアの提供

#### 2.1. 近時の動向

近時、情報セキュリティに関して、脆弱性情報が公開される前に、その脆弱性を悪用した攻撃が行われることがある。いわゆる、レス・ザン・ゼロデイ攻撃<sup>20</sup>である。そして、このような攻撃に対抗するため、情報セキュリティ産業、特に米国の情報セキュリティ産業の実態としては、ソフトウェア開発者以外の者（情報セキュリティ企業の場合もあれば個人の場合もある）が、開発者からの許諾を受けずに、当該ソフトウェアの脆弱性に関し対策を施すべく、セキュリティ修正ソフトウェア（いわゆる「第三者パッチ」）を提供することが実際に行われている。

このような第三者パッチの具体例としては

- ・ Windows Meta File (WMF) の脆弱性に対する修正ソフトウェア（2006年1月）<sup>21</sup>
- ・ Internet Explorer における「createTextRange()」メソッドの処理方法に関するもの（2006年3月）<sup>22</sup>

---

<sup>20</sup> むしろ、正当な定義によれば、このような攻撃も「ゼロデイ攻撃」とされる。

『レス・ザン・ゼロデイ』の脅威に注意を——専門家が警告

(<http://www.computerworld.jp/topics/apple/51709.html>)

<sup>21</sup> Tom Espiner 訳・河部恭紀 (ZDNet UK) 「WMF 問題の非公式パッチサイト、Windows ユーザーが殺到--アクセスが一時不能に」

(<http://japan.cnet.com/news/sec/story/0,2000056024,20093899,00.htm>)

<sup>22</sup> Joris Evers 訳・尾本香里 (CNET News.com) 「IE 修正用の暫定セキュリティパッチ、サードパーティが先に公開」

(<http://japan.cnet.com/news/sec/story/0,2000056024,20099485,00.htm>)

・ **Month of Apple Bugs** で公開された脆弱性に対する修正ソフトウェア（2007年1月）<sup>23</sup>等が挙げられる。

また、**Windows** において **Microsoft** 社のサポート対象外になったバージョンに対して、第三者がパッチを提供するという事案も報道<sup>24</sup>されている。

## 2.2. 第三者の提供するセキュリティ修正ソフトウェアの必要性と問題点

あるソフトウェアに関して脆弱性が発見された場合、情報セキュリティ業界の一般慣行によれば、まず脆弱性の発見者が、当該ソフトウェアの開発者に対して、その脆弱性に関する情報を提供し、これに基づき、開発者自身の手によって、セキュリティ修正ソフトウェアが開発されることになる<sup>25</sup>。

しかしながら、仮にセキュリティ修正ソフトウェアの開発がなされても、開発者は、種々の環境における動作のテストを実施し、副作用等がないことを確認しなくてはならず、また、その指摘された脆弱性についての分析にも時間と労力をかける必要がある。このような場合に、脆弱性の発見者が、その脆弱性の危険度が極めて高いものであることを理由として、発見者自らにおいてセキュリティ修正ソフトウェアを開発・提供するということがしばしば行われる。

特に脆弱性の危険度が極めて高く、一分一秒も早いセキュリティ修正ソフトウェアの開発・提供が強く望まれるような場合においては、セキュリティ確保の観点からこのような第三者提供にかかるセキュリティ修正ソフトウェアの必要性は高いといえる。しかしながら、その一方で、開発者が上記の如く慎重に開発し、公表するセキュリティ修正ソフトウェアに比したとき、動作の保証はなされないし、また、種々の環境において適用されるだけの動作テストが実施されているわけではないという問題がある。そして、このような問題を避けるために、開発者としては、第三者によるセキュリティ修正ソフトウェアの開発を契約によって禁止し、あるいは、第三者によるセキュリティ修正ソフトウェアが公表された場合において、その適用を薦めないという態度に出ることになるのである。

上記のようなケース、すなわち開発者によるセキュリティ修正ソフトウェアの開発・提供

---

<sup>23</sup> 「「Mac は安全」神話崩壊? - Month of Apple Bugs プロジェクト 1 月より」

(<http://journal.mycom.co.jp/articles/2006/12/22/apple/>)

「Mac に深刻なバグが続々と -"Month of Apple Bugs"プロジェクトがスタート」

(<http://journal.mycom.co.jp/news/2007/01/05/360.html>)

<sup>24</sup> **Joris Evers** 「セキュリティ専門家グループ、サポート対象外の **Windows** パッチを発表」  
([CNET News.com](http://cnet.com))

(<http://japan.cnet.com/news/sec/story/0,2000056024,20256447,00.htm>)

<sup>25</sup> 我が国においては、ソフトウェア製品の脆弱性等について、「脆弱性関連情報の流通制御」と「対策方法の適用の迅速化」を両立させるために、脆弱性関連情報の公表に係るルールが策定されている。「ソフトウェア等脆弱性関連情報取扱基準」（平成 16 年経済産業省告示第 235 号）参照のこと。なお、本報告書 第 5 2. 2. 参照。

に時間を要するケース以外にも、脆弱性の発見者において開発者と連絡を取ることができないケースや、開発者が脆弱性が存する事実を認めないケース、あるいは、開発者において当該脆弱性を修正する意向がないといったケースにおいては、第三者がセキュリティ修正ソフトウェアを開発・提供する必要性、そして開発者がこれを許容すべき必要性が認められるといえる。そもそも、個々の各ユーザーが自らにおいてセキュリティ修正ソフトウェアを開発するなどということは、およそ困難なことであって、かかる観点からも、第三者によるセキュリティ修正ソフトウェアの開発・提供行為については、一定の必要性が認められよう。

### 2.3 第三者がセキュリティ情報ソフトウェアを開発・提供する行為に対する法的な問題の可能性

ソフトウェアの適法な使用者が、自己の使用するコンピュータで実行するソフトウェアにつき、それが有する脆弱性のゆえに、適切な機能を果たさない場合において、ソフトウェアの著作者又は著作権者以外の第三者が、そのソフトウェアの脆弱性を修正するためのセキュリティ修正ソフトウェアを開発して、当該適法な使用者に提供することができるか、という事例を考えた場合、法的にクリアすべき問題が発生する。

例えば、“**The rise of zero-day patches**”という記事<sup>26</sup>の中で、**MacOS X**の脆弱性に対して、セキュリティ修正ソフトウェアを開発・提供している **Landon Fuller** 氏に対して「**MacOS X**のライセンスは、フィックスの開発／配布の妨げにならなかったか」とか「パッチを充てようとするファイルを含んでいたのか、法的な問題をもたらすとは思わなかったのか」といった質問がなされており、第三者によるセキュリティ修正ソフトウェアの開発・提供行為それ自体が、もとのソフトウェアの著作者、著作権保有者との関係といった問題や、ライセンス契約への抵触性といった問題を孕んでいることを示しているといえることができるであろう。

## 3 我が国における第三者によるセキュリティ修正ソフトウェアの開発・提供に関する法的問題

### 3.1. 著作権法

セキュリティ修正ソフトウェアの開発において複製翻案を伴わないのであれば、そもそも同条の適用を受けるまでもなく、著作権侵害の問題は生じない（著作者人格権の問題については後述する。）。

しかしながら、その修正ソフトウェアの開発において、複製翻案をとまなう場合について法的な問題はないのかという点が問題になる。我が国著作権法は、第47条の2第1項において「プログラムの著作物の複製物の所有者は、自ら当該著作物を電子計算機において利用するために必要と認められる限度において、当該著作物の複製又は翻案（これにより創作した二次的著作物の複製を含む。）をすることができる。」と定めている。これは、

---

<sup>26</sup> **Federico Biancuzzi** “**The rise of zero-day patches – The experts speak**”  
([http://www.theregister.co.uk/2007/03/02/zero-day\\_patches\\_interviews/](http://www.theregister.co.uk/2007/03/02/zero-day_patches_interviews/))

プログラムをコンピュータで利用するには、プログラムをインストールし（複製）、バックアップを取り（複製）、異機種に移植するために変更し（翻案）、バグを取り除く（翻案）等の作業が必然的に伴うことになる<sup>27</sup>ことから、これらの行為については権利者の許諾は不要としたものであり、このように定めたとしても著作権者の不利益にもならないことが根拠とされている。当該規定によれば、少なくともソフトウェアの使用者自らが、セキュリティ修正ソフトウェアを開発し、これを実行する過程において、もとのソフトウェアの複製又は翻案を伴ったとしても、著作権侵害の問題は生じないことになる。

これに対して同条は、あくまで「自ら当該著作物を電子計算機において利用するために必要と認められる限度において」と明確に規定している以上、第三者がこれを行う場合には当該条項の適用は受けられないと解されかねない（前掲田村概説228頁）。

なお、本条について「電子計算機において利用するために必要と認められる限度」がいかなる意義を有するかにつき、加戸守行『著作権法逐条講義（五訂新版）』（著作権情報センター、2006年）は、「プログラムの種類等により、この必要と認められる限度は違ってまいりましょう」とする（313頁）。この点については、例えば、開発者によるサポートが既に満了しており、後継商品が存在する商品に対して、セキュリティ修正ソフトウェアを開発して、脆弱性を防ぐという行為が、「利用するのに必要と認められる限度」に該当するの点については、なおも曖昧さが残るといわざるを得ず、（仮に上記第三者による複製・翻案につき立法化による解決がなされる場合において）当該課題についても検討すべきと思われる。

次に、セキュリティ修正ソフトウェアは、結果的にもとのソフトウェアの表現を改変することになるため、著作者人格権、具体的には同一性保持権への抵触性という問題が生ずることになる（著作権法50条により、上記47条の2第1項の規定は、著作者人格権に影響を与えないことになる。）。しかしながら、著作権法第20条第2項第3号の、「特定の電子計算機においては利用し得ないプログラムの著作物を当該電子計算機において利用し得るようにするため、又はプログラムの著作物を電子計算機においてより効果的に利用し得るようにするために必要な改変」については、同一性保持権が及ばないことを規定しており、本件で検討するようなセキュリティ修正ソフトウェアによる改変がこれに該当することは論を待たないだろう。従って、セキュリティ修正ソフトウェアによるもとのソフトウェアの改変は、もとのソフトウェアの著作者との関係で同一性保持権侵害には該当しないと考えるのを相当とする<sup>28</sup>。

### 3.2. ライセンス契約上の問題

我が国においても、ソフトウェアのライセンス契約中に、セキュリティ修正ソフトウェアの開発・提供を禁止する規定が存する場合、その有効性が問題となる。当該問題について

---

<sup>27</sup> 中山、前出 298 頁

<sup>28</sup> 中山・前掲 401 頁は、著作権法20条2項3号をもって、「事実上プログラムには同一性保持権がなきに等しいことになった」と評する。

は、リバースエンジニアリングを禁止する条項と同様にその有効性を解すべきではなからうかと思われる。

## 4 諸外国における議論の状況

### 4.1. 米国における議論状況

第三者のセキュリティ修正ソフトウェアの作成を禁止するライセンス契約の条項が法的な効力を有するかどうかという点については、具体的な議論がなされてはいない模様である。

### 4.2. EU 諸国における議論状況

#### (1)英国

修正ソフトウェア(「パッチ」)(プログラムの複製もしくは改変の結果として作成されたもの)自体が、プログラム(もしくは、その実質の一部)を構成するものを含む場合には、修正ソフトウェアの公開は、CDPA 1988第50条Cによって、保護されないことになる。パッチは、侵害行為となるだろうというのである。しかしながら、解釈論としては、請負人の作業と考えることによって許容されるという立場が示唆されている。一方で、仮に、修正ソフトウェアが、プログラムの複製もしくは実質的な一部を含んでいないとすれば、修正者は、その修正ソフトウェアを公開することができ、適法に取得したプログラムの「エラー」を訂正するため、他の適法な使用者によって使用することができる。

これとも関連して、第三者の修正ソフトウェア公開が、ライセンス契約に反するのではないか、もしくは、修理の法理の適用のもと許容されるのではないかという議論もある。もっとも、これらの問題は、詳細には議論されていない問題である。

#### (2)フランス

修正ソフトウェアに関しては、修正対象となるプログラムの複製、翻案のいずれももたらさないときに限って、修正しようとするプログラムの権利者の事前の同意を得ることなくコンピュータセキュリティの脆弱性を修正するソフトウェアを作成することができる。逆に、修正ソフトウェアが、対象となるプログラムの複製または翻案をもたらす場合には、権利者の許可が必要となる。

また、プログラムの修正について著作権者の同意が必要であるとする契約の条項の有効性についての規定は、制定法には存在しないが、その契約の条項は効力を有するものと考えられる。

#### (3)ドイツ

修正ソフトウェアが、オリジナルからデコンパイルされたものをもとに作成されたのであれば、著作権法のもとで許容されないと考えられる(著作権法第69条 e)。その過程が、デコンパイルなしでなされたのであれば、著作権法第69条 d (3) –そして、特別の状況のもと–第69条 d (1)のもと、許容されると考えられる。ソフトウェアのバグの修正が、ソースコードへのアクセスなしになされたのであれば、第69条 d (1)すなわち、

ソフトウェア指令第5条（1）の例外に該当すると認識されるとされる。また、新しい問題として、著作者としての氏名を表示するかという問題があると指摘されている。

#### 4.3. オーストラリアにおける議論

ソフトウェアに翻案を生じないソフトウェアの小さな変更を含む修正ソフトウェアは、ソフトウェアの権利保有者の同意を必要としない。修正ソフトウェアを適用することが、技術的保護方法の回避をする場合には、そのソフトウェアを配布することは、法における技術的保護方法の回避の適用除外に含まれる必要がある。また、例えば、作品の著者が、修正ソフトウェアの適用は作品の価値を損なう取扱いにあると主張する場合には、著作権保有者が著作者人格権を侵害したとすることができる。もっとも、関係する著者が修正ソフトウェアの適用に同意していたか否か、および修正ソフトウェアに関する実務が関連する業界でどのようなものであるかを含む、事件の特定の事実により、それが著作者人格権を侵害しているのかが決定される。

## 5 検討

### 5.1. 第三者の修正ソフトウェアの必要性

日本の著作権法第47条の2の「プログラムの著作物の複製物の所有者は、自ら当該著作物を電子計算機において利用するために必要と認められる限度において、当該著作物の複製又は翻案（これにより創作した二次的著作物の複製を含む。）をすることができる。」の規定や諸外国の実際の議論を見ていく際に、実際のセキュリティ活動に対して、法律の定めが追いついていないのではないかという疑念を抱くところである。

現実においては、脆弱性公表以前に、その脆弱性の脅威分析がなされ、それに対する対応が議論され、開発者でも修正ソフトウェアを開発するとともに、第三者からの修正ソフトウェアが公表・配布される。いわば、緊急避難的な側面もあるのである。その一方で、ライセンス契約においては、このような行為を禁止する条項が存在していることが多いが、そのような条項に従い、それらの活動をすべてプログラムの著作権を侵害する行為であるとか、ライセンス契約違反ということは、以下の考察のようにできないものと考えられる。

### 5.2. 我が国における許容性について

もっとも、法的な正確な位置づけとしては、修正ソフトウェアの作成にあたり、どのような手法が用いられたのか、また、その修正ソフトウェア自体が、もとのプログラムとの関係で、翻案にあたるのかという点を確定しないと判断がなしえないところである。

また、この修正ソフトウェアが、もとのプログラムとの関係で、複製もしくは翻案にあたるとしても、もともとのプログラムの脆弱性を修補するのみで、性能の向上や、結果の変更等を意図するものではないということを当然の前提にしていることに留意しなければならない。（解釈論としては、前述のような「必要な限り」という文言の解釈論として現れよう）

本報告書においては、種々の制約により、かかる修正ソフトウェアにまつわる事実関係を

分析する余裕がなかった。修正ソフトウェアとされるもののなかには、もともとのプログラムとの関係で検討した場合に、翻案にも該当しないものも多いものと思われる。

仮に翻案に該当するものとしても、電子計算機の利用者が、かかる修正ソフトウェアを利用する行為は、電子計算機において利用するために必要と認められる行為であり、その修正ソフトウェアの適用によって、もともとのプログラムが翻案されたとしても、**47 条の 2**において許容されると考えられるであろう。そして、その利用者の行為について、かかる修正ソフトウェアの提供行為者は、その行為者の補助者として、分析し、修正ソフトウェアを開発すると考えられる。したがって、その修正ソフトウェアが、客観的に、もともとのプログラムに対して翻案をなすプログラムであったとしても、**47 条の 2**の行為として許容される行為の幫助ということなので、(その違法性は、利用者の行為に従属するので) それ自体、違法性はないことになるものと思慮される。

このような検討をした際に我が国における**第 47 条の 2**の「自ら当該著作物を電子計算機において利用するために必要と認められる限度」という規定が、セキュリティ修正を行う公的な機関や情報セキュリティ産業等が、第三者としてセキュリティ修正ソフトウェアを開発し、配布することができるかという問題について「自ら」という文言に意味をもたせて解釈した場合に、そのような行為が独立して違法であると解される可能性があるので、この点について許容されることを明確にするために立法的対応をするということもひとつの方向ということになるものと思われる。

また、セキュリティ修正ソフトウェアの提供行為者は、仮に、ライセンス契約によって、そのような分析行為や修正プログラム作成行為が禁止されていたとしても、上記のような各利用行為者の電子計算機利用行為に必要な行為のためのツールを作成するために行為をなすことができ、そのような行為に適用されると解される限りにおいて、分析行為・修正ソフトウェア作成禁止条項は、効力を有しないと解されるべきであると思われる。

もっとも、上記著作権法**47 条の 2**との関係で、「必要と認められる」限りというのは、どのような場合をいうのかという問題がある。前述のようにセキュリティ修正対応のソフトウェアを後継製品で発表している場合に、第三者が、セキュリティ修正ソフトウェアを提供しうるとすべきかは問題があるようにも思える。この限界点については、一定の議論が必要であるように思われる。

## 第4 著作権技術的保護手段等の脆弱性調査について

### 1 技術的保護手段等とは

#### 1.1.概念<sup>29</sup>

我が国においては、平成11年の著作権法改正により、デジタル化・ネットワーク化の進展に対応した著作権保護の新たな国際的枠組みであるWIPO新条約に盛り込まれている事項に関して著作権制度の整備がなされるに至った。具体的には、譲渡権の創設、上映権の拡大等と共に、映画ソフト等に用いられているコピープロテクション等技術的保護手段の回避専用装置等の公衆への譲渡等の規制、著作権等に付され著作権等の管理に用いられる権利管理情報の改変等の規制などが改正事項とされた。

技術的保護手段及び権利管理情報に関する改正の趣旨は、デジタル化の進展、ネットワーク化の進展により、高品質の複製物を公衆に向けて発信することが可能となり、著作物等の取引・流通経路が拡大され、その結果、無許諾のままの複製等が増大し、特にネットワークを通じた無許諾送信のように、侵害者の発見が困難な権利侵害行為が急増したことを背景に、かかる状況に対応するために用いられる技術的保護手段・権利管理情報につき、技術的保護手段の回避に係る行為と、権利管理情報の改変等の行為を規制することをその内容としている。

なお、同時期に不正競争防止法も改正され、「営業上用いられている技術的保護手段等」の効果を妨げる機能を有する専用装置・プログラムの譲渡等が「不正競争」に追加されている（詳細は、後述する）。

上記同趣旨の規定は、世界各国で広く導入されている。しかしながら、これら同趣旨の規定は、世界的にみると暗号研究に対して法的な緊張感をもたらしているといつてよい（後述する）。

#### 1.2.技術的保護手段等と暗号技術<sup>30</sup>

上記のような技術的保護手段として現在利用されているものには、以下のように暗号技術が利用されているものがある。

・CPM (Content Protection for Pre-recorded Media) : コンテンツは、記録時に全て暗号化され、再生時に、メディア鍵などの情報が適正であるかどうかによって再生の可能性

<sup>29</sup> 改正にいたる経緯等については、越田崇夫『著作権法の一部を改正する法律』について（前編）「コピーライト1999年7号、24頁等を参照されたい。

<sup>30</sup> 文化審議会著作権分科会法制問題小委員会 デジタル対応ワーキングチーム「文化審議会著作権分科会法制問題小委員会 デジタル対応ワーキングチーム検討結果報告」平成17年7月 ([http://www.mext.go.jp/b\\_menu/shingi/bunka/gijiroku/013/05072901/002.htm](http://www.mext.go.jp/b_menu/shingi/bunka/gijiroku/013/05072901/002.htm))

を制御する

・ C P R M (Content Protection for Recordable Media) : C P P M と基本的に同一の技術を用いた記録可能メディア用規格

・ D T C P (Digital Transmission Content Protection) : IEEE-1394 等を使って接続した機器間で認証とデータの暗号化を行い、コンテンツの伝送を保護し、不正コピーを防止する技術

暗号研究は、暗号や暗号解読についての理論的研究から成り立っている。そして、暗号を著作権等の技術的保護手段として応用している「技術的保護手段」についても、その理論的研究は、情報セキュリティ活動としての重要な地位を占めているといえることができる。しかしながら、このような暗号研究が、技術的保護手段の脆弱性に関する調査・学問的研究においてなされたとき、以下のとおり、米国においては、具体的な問題が起きているのである。

## 2 諸外国における技術的保護手段と法律の解釈の交錯

### 2.1. 米国デジタルミレニアム著作権法と技術的保護手段の回避

#### (1) 米国における技術的保護手段の定め

上記技術的保護手段が米国において実装されたのは、デジタルミレニアム著作権法による。同法は、著作権保護システムの回避についての規定を包含している (合衆国法典 17 編 1201 条) ものであり、1998 年 10 月に成立し 2000 年 10 月に施行された。

条文としては、

第 1201 条 著作権保護システムの回避

(a) 技術的手段の回避にかかる違反

(1) (A) 何人も、本編に基づき保護される著作物へのアクセスを効果的にコントロールする技術的手段を回避してはならない[...]

となっている。

この規定との関係で、許容される例外が制定法において定められており、具体的には、(相互流用性目的のための) リバースエンジニアリング (第 1201 条 (f))、暗号技術のための脆弱性調査 (第 1201 条 (g))、セキュリティテスト (第 1201 条 (j)) が、例外として含まれている。これらの例外規定の条文については、社団法人著作権情報センターが翻訳を準備している (インターネット上からも <http://www.cric.or.jp/gaikoku/america/america.html>) でアクセスが可能)。

米国においては、この技術的手段を回避してはならないという規定と暗号研究との関係で、いろいろな問題が起きている。

#### (2) デジタルミレニアム法と暗号研究との交錯

(ア) Felton v. RIAA 事件

2000 年 9 月、SDMI (Secure Digital Music Initiative) は、Hack SDMI Challenge

という企画を発表し、自らが提供するデジタル透かしを利用した DRM の脆弱性の有無についてテストをさせ、脆弱性を発見したものに1万ドルを提供しようとした。これに対し、プリンストン大学の Edward Felton 教授は、研究チームとともにその DRM の脆弱性を発見し、論文にまとめた。Hack SDMI Challenge は、同チームに1万ドルを提供したものの、Felton 教授はこれを辞退し、この発見した脆弱性情報を保持するとともに、これを公表することを選択した。

同教授のかかる行為に対して、SDMI と RIAA (全米レコード協会) からデジタルミレニアム著作権法に抵触するため、思い留まるよう申し入れたところ、同教授が DMCA により研究を制限されたと主張し、デジタルミレニアム著作権法は憲法修正第1条を侵害し、ソフトウェアの発展及び科学的研究を妨げているとして SDMI と RIAA を相手取り訴訟を提起するという事態に発展している (なお、2001 年 11 月、ニューヨーク地区連邦控訴裁判所は、原告主張を退ける判決を下している。)

#### (イ) US v. Sklyarov 事件

ロシア人プログラマーである Dmitry Sklyarov 氏は 2001 年 7 月 16 日、ラスベガスで開かれた Def Con というセキュリティに関する会議で講演した後、デジタルミレニアム著作権法違反の容疑で逮捕された。Sklyarov 氏は、ロシアの Elcom Soft 社の従業員であったが、米 Adobe Systems 社が著作権保護目的で『Adobe Acrobat eBook Reader』に施していたセキュリティー暗号を解除するソフトウェア『Adobe eBook Processor』の試用版を配布したとして逮捕されたものであり、具体的には、本のような著作権保護された著作物を配信するための eBook ファイルの暗号を解読し、どのような PDF リーダーでも読めるようにするソフトウェアを販売したものであった。その後、プログラマー達による抗議活動、不買運動等もあり、Adobe 社が Sklyarov 氏を釈放するよう当局に要請し、最終的に同氏は違法性の意識を欠くことを理由に釈放されている。なお、当該事件に関しては、Elcom Soft 社を被告人とする刑事訴訟となったが、最終的に陪審員が無罪という判断を下している。

#### (3)その余の問題

米国においては、上記以外にも、暗号研究に関して、輸出管理法と大学における教育活動との抵触の問題が議論されている。詳細は、別途公開される米国の報告書参照のこと。

## 2.2. その余の法域における具体的な暗号研究と著作権の交錯

### (1)EU 指令

ソフトウェア指令は、その第7条で、ソフトウェアに対する保護手段についての法的保護を定めている。具体的には、「コンピュータ・プログラムの保護のために適用されている技術的装置の無許諾での除去又は回避を促進することのみを目的としている手段を流通させ又は商業用目的で所持する行為」に対しての権利者の救済措置を定めるものとするとしているのである (同指令第7条)

また、コピーライト指令は、著作物 (プログラム以外) についての技術的保護手段に対する回避を禁止する。その第3章は、「技術的手段および管理情報の保護」と題し、第6条

においては、技術的手段に関する義務を定め、第 7 条においては、権利管理情報の保護を与えるものである。

## (2)構成国における国内法化

### (ア)英国

英国においては、コンピュータプログラム以外に対する技術的保護手段についての規定は、CDPA の 296ZA 技術的手段の回避の条項において保護が定められている。もっとも、同条(2)において、暗号研究の目的のためになされる行為に対しては、適用されないことが明らかになっている。

なお、コンピュータプログラムに対しては、296 条が適用されることになる。この条文はコンピュータプログラムの著作権保護のために技術的手段が付されている場合に、その回避製品の販売、輸入、配布等(同(1)(b)( ))や除去もしくは回避の情報を公表もしくは他人のかかる行為を幫助することについて(同( ))著作権侵害とするものである。したがって、コンピュータプログラムについては、許容されるリバースエンジニアリングに対する対抗措置として、技術的手段が採用されている場合であっても、技術的手段の回避をして、リバースエンジニアリングをした場合、その回避をしたという手法自体については、法的には、著作権の侵害とされることはないことになる。

### (イ)フランス

フランスにおける技術的保護手段についての規定については、L 331-5 to 331-10 の規定によって規制されている。もっとも、これらの規定は、コンピュータプログラムには、適用されていない。

また、技術的保護手段は、相互流用性を防止する効果を有してはならず、技術的保護手段の提供者が必要情報を拒絶する場合には、ソフトウェア発行者等が、当局 (**Authority of Regulation of Technological measures**) に対して、相互流用性を確保するように要請できるとか、技術的保護手段の提供者が、技術的保護手段と両立しうるソフトウェアの公開や技術的文書の公表を差し止めうるのは、技術的保護手段の安全性に深刻な影響を及ぼすときのみであるとかの規定がある。

### (ウ)ドイツ

ドイツにおいて技術的保護手段についての規定については、著作権法 95 条 a 及び同条 b によって、技術的保護手段の回避に対する規制がなされている。もっともかかる規定は、コンピュータプログラムについて適用されるものではない (同法 69 条 a)。

また、技術的保護手段とその回避について具体的な問題になった具体例は存在しない。

## (3)オーストラリアにおける制定法

2007 年 1 月 1 日から効力を有している改正著作権法は、アクセス・コントロールの技術的保護方法回避の禁止を含んでいる。具体的には、第 116AN 条は、民事責任を創設しており、第 132APC 条は、「その者が当該行為 (すなわち、民事責任を生ずる行為) に商業的な優位または利益を得る意図で関わる」場合には) 刑事責任を創設している。

また、この116AN条は、(a) 相互運用性—第116AN条第3項(b) 暗号研究—第116AN条第4項、および(c) コンピュータ・セキュリティ・テスト—第116AN条第5項についての例外を含むものである。したがって、このような許容される例外に該当する場合においては、技術的保護方法の回避がなされたとしても責任を問われることはないことになる。

### 3 技術的保護手段、権利管理情報に関する法律上の規定と検討

#### 3.1. 日本における技術的保護手段、権利管理情報についての規定

上記のとおり、我が国著作権法においては、平成11年改正により、技術的保護手段及び権利管理情報に関する諸規定が整備された。

このうち、「技術的保護手段」については、

『電子的方法、磁気的方法その他の人の知覚によつて認識することができない方法（次号において「電磁的方法」という。）により、第十七条第一項に規定する著作者人格権若しくは著作権又は第八十九条第一項に規定する実演家人格権若しくは同条第六項に規定する著作隣接権（以下この号において「著作権等」という。）を侵害する行為の防止又は抑止（著作権等を侵害する行為の結果に著しい障害を生じさせることによる当該行為の抑止をいう。第三十条第一項第二号において同じ。）をする手段（著作権等を有する者の意思に基づくことなく用いられているものを除く。）であつて、著作物、実演、レコード、放送又は有線放送（次号において「著作物等」という。）の利用（著作者又は実演家の同意を得ないで行つたとしたならば著作者人格権又は実演家人格権の侵害となるべき行為を含む。）に際しこれに用いられる機器が特定の反応をする信号を著作物、実演、レコード又は放送若しくは有線放送に係る音若しくは影像とともに記録媒体に記録し、又は送信する方式によるものをいう。』

と定義され（2条1項20号）、①電磁的方法により、著作権等を侵害する行為の防止又は抑止をする手段であること、②著作権等を有する者の意思に基づくことなく用いられているものでないこと、③機器が特定の反応をする信号を著作物等とともに記録し、又は送信する方式によるものであること、という3要件を充たすものをもって、「技術的保護手段」としている。

そして、かかる技術的保護手段について、技術的保護手段の回避専用装置又は、回避専用プログラムの複製物を、①公衆に譲渡又は貸与した者、②公衆に譲渡又は貸与する目的で製造し、輸入し、又は若しくは所持した者、③公衆の使用に供した者、④技術的保護手段の回避専用プログラムを公衆送信し、又は送信可能化した者、⑤業として公衆からの求めに応じて技術的保護手段の回避を行つた者、について非親告罪の刑事罰が科されている（120条の2）。また、私的使用目的の複製であっても、技術的保護手段の回避により可能となった複製を行うことは権利制限から除外とされ、著作権侵害の対象とされている（30条1項2号）。

次に、「権利管理情報」については、

『第十七条第一項に規定する著作者人格権若しくは著作権又は第八十九条第一項から第四項までの権利（以下この号において「著作権等」という。）に関する情報であつて、イからハまでのいずれかに該当するもののうち、電磁的方法により著作物、実演、レコード又は放送若しくは有線放送に係る音若しくは影像とともに記録媒体に記録され、又は送信されるもの（著作物等の利用状況の把握、著作物等の利用の許諾に係る事務処理その他の著作物等の管理（電子計算機によるものに限る。）に用いられていないものを除く。）をいう。

- イ 著作物等、著作権等を有する者その他政令で定める事項を特定する情報
- ロ 著作物等の利用を許諾する場合の利用方法及び条件に関する情報
- ハ 他の情報と照合することによりイ又はロに掲げる事項を特定することができることとなる情報』

と定義され（2条1項21号）、かかる権利管理情報につき、①権利管理情報として虚偽の情報を故意に付加する行為、②権利管理情報を故意に除去し、又は改変する行為、③②が行われた著作物等につき、情を知って行う（a）複製物を頒布する行為（b）複製物を頒布の目的をもって輸入し、又は所持する行為（c）公衆送信し、又は送信可能化する行為、をみなし侵害行為とすると共に（113条3項、4項）、営利目的で権利管理情報の改変等を行った者には、親告罪の刑事罰を科すこととされた（119条1項、120条の2）。

さらには、不正競争防止法は、「技術的制限手段」という概念を設け、同用語につき、

『電磁的方法（電子的方法、磁気的方法その他の人の知覚によって認識することができない方法をいう。）により影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録を制限する手段であつて、視聴等機器（影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録のために用いられる機器をいう。以下同じ。）が特定の反応をする信号を影像、音若しくはプログラムとともに記録媒体に記録し、若しくは送信する方式又は視聴等機器が特定の変換を必要とするよう影像、音若しくはプログラムを変換して記録媒体に記録し、若しくは送信する方式によるもの』

と定義すると共に（2条7号）、技術的制限手段により視聴や記録、複製が制限されているコンテンツの視聴や記録、複製を可能にする機器又はプログラムを譲渡等する行為を不正競争として規制対象としている（2条1項10号、11号）。なお、技術的制限手段の試験又は研究のために用いられる装置等の譲渡等については、適用除外とされている（19条1項7号）。

### 3.2. 暗号研究との交錯についての検討

我が国においては、上記各規定につき、特に情報セキュリティ活動との関連での議論は殆どなされていないと思われる。この点、（回避装置等の譲渡等を伴わない）「暗号研究」

それ自体が上記各規定に抵触することは想定し難いものの、脆弱性調査に際し、暗号を外した上でリバースエンジニアリングを実施し、プログラムの複製が生じたケースや、権利管理情報を著作物等から除去したうえで、当該管理情報を分析するケースにおいては、前者にあつては、複製権侵害の有無が問題となり得るし、後者にあつては、みなし侵害（113条3項）への該当性が問題となり得る。

このうち前者については、リバースエンジニアリングに関し明文をもって適法と謳う際、併せて技術的保護手段等の回避を伴う複製についても権利制限等の対象とすることを視野に検討すべきであると思われる。

また、後者については、かかる行為が文言上「除去」に該当することは否定しえず、また、暗号研究は、著作物ではなく、それに付された暗号の分析を目的とする以上、「著作物又は実演等の利用の目的及び態様に照らしやむを得ないものと認められる場合」（著作権法113条3項2号カッコ書き）が想定している態様ともいえず、適法性を担保するに十分な状況とは言い難い。このような場合、権利者側が著作権侵害を主張する可能性それ自体は高くないものと思われるが、脆弱性を分析されることを良しとしない権利者から著作権侵害を主張されるリスクは依然としてゼロとはいえない。

リバースエンジニアリングにおける議論と同様に、このような場合の権利行使は権利濫用に該当する等の構成や、正当行為による違法性阻却等の構成により、適法であるとの結論に導くことが可能であろう。もっとも、立法によりかかる研究に対する不当な制限がかされないような手当が望まれるように思われる。

## 提言

既述のとおり検討のもと、当調査委員会は、以下を提言する。

情報セキュリティ活動の促進をはかり、安全で信頼性の高い IT を利用できる環境を整えることは、産業の基盤を支える創造性を促進することになり、産業及び政府部門の「競争力」を向上させ、ひいては、国民生活に資するものとなるとの認識のもと、以下の対応をとることが望ましい。

(A) コンピュータプログラムの脆弱性調査のためのデコンパイル行為およびそれに当然付随する複製行為について、著作権法上、適法であることを、著作権法改正等の手段によって、明確にされるべきである。

(B) コンピュータプログラムの脆弱性を修正するセキュリティ修正プログラムについて、利用者の利用に必要なかぎりで行なわれる場合については、修正プログラムの作成が、適法になしうることが著作権法改正等の手段によって明確にされるとともに、許容される具体的な場合について、明確な判断基準が提供されるべきである。

(C) ソフトウェア利用契約においてなされるデコンパイル禁止条項・修正プログラム開発禁止条項については、脆弱性調査目的のための活動に対しては、効力を有しないことが明らかにされるべきである。

(D) 技術的保護手段が、暗号技術を用いて提供されている場合について、情報セキュリティ活動としてなされる暗号研究については、その技術的保護手段の回避として認識されてはならないことが明らかにされるべきである。

かかる提言の意味は、以下のとおりである。

## 1 提言の趣旨

情報セキュリティ活動の促進をはかり、安全で信頼性の高い IT を利用できる環境を整えることは、産業の基盤を支える創造性を促進することになり、産業及び政府部門の「競争力」を向上させ、ひいては、国民生活に資するものとなるとの認識のもと、以下の対応をとることが望ましい。

### (1) 「情報セキュリティ活動の促進をはかり」

情報セキュリティ活動とは、情報セキュリティに関連して行われるセキュリティ向上のための行為一切（ソフトウェア等の脆弱性を分析・発見・修正・公表する一連の行為）をいう。

これらの行為について、できる限り自由な活動が保障され、その活動のもと、情報セキュリティの向上がはかれるのが、かかる活動の促進をはかるために必要なことである。いうまでもなく、情報セキュリティ活動は、その性質上、責任をもってなされる必要があり、そのために必要最小限の法的規制は必要になるし、また、他の法益との調整も必要になるが、それらの法的な規制は、その外延ができる限り明確になされなくてはならないことになる。

### (2) 「安全で信頼性の高い IT を利用できる環境を整える」

情報セキュリティ活動は、安全で信頼性の高い IT を利用できる環境を整えるものである。脆弱性の分析・発見・修正・公表の過程によって、IT の利用環境は、より安全で信頼性の高いものになっていくのである。

### (3) 「産業の基盤を支える創造性を促進することになり」

現代社会のように産業活動がきわめて IT 技術に依存してなされるようになっている現状において、安全で信頼性の高い IT 環境は、その産業活動自体の創造性に関係してくる。

IT を安全に信頼をもって利用できない環境においては、情報の自由かつ迅速な交換が妨げられ、それらによって触発される個人の創造性がその基盤を失ってしまいかねないのである。

### (4) 「以下の対応をとることが望ましい。」

調査委員会としては、立法・司法・行政当局にたいして、上記認識をもとに法の改正、法の解釈、指針等の作成等をなすのが望ましいと認識している。

## 2 脆弱性調査目的のデコンパイルの適法性の確認

(A) コンピュータプログラムの脆弱性調査のためのデコンパイル行為およびそれに当然付随する複製等の行為について、著作権法上、適法であることが、著作権法改正等の手段によって、明確にされるべきである。

### (1) 「コンピュータプログラムの脆弱性調査のため」

調査委員会は、コンピュータプログラムの脆弱性調査のための行為についての適法性を検討した。これは、そのプログラムを利用者が安全に信頼しうるように利用できるようにするための調査という点について限定して論じたものである。もともとのプログラム著作権者のアイデアを調査し、そのアイデアを利用して、何らかの独立したプログラムを開発するという行為がある場合については、開発者の利益との衝突ということを考えることができるとしても、上述の脆弱性調査という点については、もともと、プログラムの著作権者が、そのプログラムの脆弱性については、誠意をもって対応すべき地位にあることから、著作権者の利益が不当に損なわれることがないといえ、著作権法との関係で、適法行為であると認識されるべき必要性が極めて高いものといえることができる。

### (2) 「デコンパイル行為およびそれに当然付随する複製等の行為」

一般にリバースエンジニアリング行為といわれるもののうち、我が国の著作権法上で、複製・翻案権との関係で問題となるのは、デコンパイル行為が中心的なものであるといえる。それ以外の行為については、そもそも、複製権・翻案権との関係で、法的に問題が生じないものが一般である。そこで、提言としてデコンパイル行為についての適法性を明確にすべきものとしている。

もっとも、そのデコンパイル行為自体のみの適法性を考えたとしても、十分ではない。そのデコンパイルも(1)記載の目的のためになされるのであり、その目的遂行に必要な調査の準備行為、調査行為自体、その調査結果の報告行為などにおいても、当然、複製等の行為がなされることになる。そのような当然付随する行為についても適法性が明らかにされるべきであるといえる。

### (3) 「著作権法上、適法であること」

かかる調査の過程において、デコンパイルがなされ、また、もとのプログラムについての複製もしくは翻案がなされたとしても、その複製・翻案は、著作権法上、例外として許容されるものと認識される。これは、そもそも、コンピュータプログラムの脆弱性が、プログラム開発者によって、業界の善良な慣行に従い、調査・分析・修正されるべきであるという立場から、第三者の善意の調査・分析行為については、プログラム開発者は、これについて著作権者としての、排他的権利を主張しうるべき合理的な利益を有さないと考えられる。

かかる利益状況をもとに、解釈論としては、現行法のもとでも、かかる目的のための(2)の行為が、適法であると解すべきであること当然である。

#### (4)「著作権法改正等の手段」

情報セキュリティ活動の促進という観点からは、かかる情報セキュリティに対して制約となりうる法的規制については、必要最小限で、かつ、明確であることが必要とされることはいままでもないことである。このような観点からは、上記(3)の事項について、明確な手段によって、確認されることが必要である。そのためにもっとも有効な手段としては、著作権法の改正が考えられる(具体的には、権利制限規定の追加等)。

### 3 第三者による脆弱性修正プログラム作成の適法性の確認

(B) コンピュータプログラムの脆弱性を修正するセキュリティ修正プログラムについて、利用者の利用に必要なかぎりでなされる場合については、修正プログラムの作成が、適法になしうることを著作権法改正等の手段によって明確にされるとともに、許容される具体的な場合について、明確な判断基準が提供されるべきである。

#### (1) 「セキュリティ修正プログラム」

セキュリティ修正プログラムについては、まず、もともとのプログラムとの関係で、複製、翻案になるものであるかどうかによって、法的な問題が生じうるかどうかという点に留意が必要である。

本提言においては、もともとのプログラムとの関係で、複製、翻案になる場合を念頭において、提言をなしている。複製、翻案にならない場合まで法的な問題があるかのように誤解してはならない。

#### (2) 「利用者の利用に必要なかぎりで行なわれる場合」

第三者によるセキュリティ修正プログラムは、複製・翻案になる場合であったとしても著作権法第47条の2第1項の規定により許容されることになると解する立場から、そのセキュリティ修正プログラムの限界を画する要件として必要となるものである。

#### (3) 「適法になしうること」

著作権法47条の2、同20条第2項第3号の規定の趣旨からすれば、コンピュータの利用者が、みずからその利用に必要なかぎりにおいてなされる複製、翻案は、法的に許容されることになる。たしかに法文において、「自ら」という文言があり、かかる文言が、他人のコンピュータにおいて実行されるべき場合における複製については、これを許容していないと解する余地がある。しかしながら、その修正プログラムの作成者も、自己のコンピュータにまず適用し、その修正プログラムの状況を分析するのであり、みずから利用しているのに必要なものとして開発しているともいえる。また、配布については、他人に利用させるものとして、かかる文言との関係が問題になりうる。

#### 4 ソフトウェア利用契約における禁止条項の効力

(C) ソフトウェア利用契約においてなされるデコンパイル禁止条項・修正プログラム開発禁止条項については、脆弱性調査目的のための活動に対しては、効力を有しないことが明らかにされるべきである。

##### (1) 効力を有しないこと

一般消費者あてのソフトウェアに関して、情報セキュリティ活動を制限するソフトウェア利用契約については、かかる情報セキュリティ活動を防止する開発者の利益は、保護に値するものが存在しないのではないかというのは、本報告書で検討した通りである。デコンパイル禁止条項については、調査目的であるかぎり合理的な理由がないし、また、修正プログラム開発禁止条項についても、その保護されるべき開発者の利益というのは、保護に値するか疑問である。もっとも、開発終了後、後継商品を市場に提供しているような場合においてまで、修正プログラム開発禁止条項の効力を無効と解して、第三者による修正を認めるべきかという点については、もはや必要とされる範囲を超えたものと考えられよう。

##### (2) 明らかにされるべき

この論点については、明確な解釈論や確定した判決例などが存在していないものといえる。また、世界的にも、通常的一般消費者向けに売買されるパッケージソフトウェアの場合には、本件契約条項は、無効とされやすいという一定の傾向は、看守しうるものの、断定しうるものともいえないであろう。このような認識のもと、調査委員会としては、情報セキュリティ活動の促進という見地から、脆弱性調査目的のための活動に適用されるかぎりにおいて、当該条項は無効であるという解釈が望ましいものとする。そして、そのような解釈については、立法的手法（例えば、著作権法改正、著作権法改正に伴う立法趣旨の明確化が考えられる。）もしくは準則等による解釈提案という形で、社会的に明確になることを望むものである。

#### 5 技術的保護手段等と暗号研究

(D) 技術的保護手段等が、暗号技術を用いて提供されている場合について、情報セキュリティ活動としてなされる暗号研究については、その技術的保護手段等の回避として認識されてはならないことが明らかにされるべきである。

##### (1) 情報セキュリティとしてなされる暗号研究

技術的保護手段等の脆弱性などについて、もっぱら情報セキュリティ活動からしてなされる場合については、そのセキュリティ研究としてのもつ意義に鑑み、その活動が保障されなくてはならず、著作権法の適用においてもかかる利益は、十分に保護されなくてはな

らないということになる。

## (2) 明らかにされるべき

技術的保護手段等の暗号研究の見地からなされる脆弱性調査が、著作権法上、著作権侵害行為とみなされる（第113条3項、4項）場合があることは、本報告書 第4・3.2. で述べたとおりである。

このような場合が、著作権侵害行為とみなされる可能性があることは、きわめて問題である。立法により、かかる研究に対する不当な制限が課されないような手当てが望まれる。