Vol.2012-EIP-55 No.6
2012/2/10

# 「情報処理の高度化等に対処するための刑法等の一部改正」に関する一考察

須川賢洋†

2011(平成 23)年の刑法改正により、ようやく我が国でもいわゆるウィルス作成罪などが制定された。しかしながら、そこに至るには多くの紆余曲折があり、特に技術者サイドからの危惧の念が大きかった。本論文ではこの制定の経緯や条文からなぜそのような声があったのか検証する。

# A study for “Revision of criminal law about cyber crime”

Masahiro SUGAWA†

Crime of “creating computer virus” was added in Japanese criminal law finally by revision of 2011. However, it has lead to many twists and turns, the greater sense of concern, especially from the technical side. In this paper, to verify whether and why there was a voice from the background and provisions of this enactment.

## 1. はじめに

2011(平成 23)年 6 月 24 日、「情報処理の高度化等に対処するための刑法等の一部を改正する法律」案が国会を通過し公布された。これにより長年の課題であった、いわゆる「ウィルス作成罪」等がようやく刑法に規定された。そして同罪に関する罰則は基本的には翌月の 7 月 14 日から施行されている。その他にも電子的証拠1の保全、差押え等に関して刑事訴訟法の一部が改正されている。しかしながらこれらの法改正は、サイバー法関連の他の法規と同様に、技術と法律の狭間でその解釈や運用を巡って様々な議論がある。さらにひどい場合には風評に近い誤解までがネット上や一部技術者の間で広まってしまっている2。

一方で、Stuxnet (スタクスネット)のような新世代のコンピュータ・ウィルスの登場は、現在のコンピュータ・ネットワークがインフラの為の基盤インフラとなっている社会そのものへ多大な危険を及ぼすものである。

そこで、本稿ではサイバー法の視点から、今回の法改正を改めて検討してみることとする。

## 2. 歴史的経緯

### 2.1 それ以前のコンピュータ関連犯罪における刑事法と問題点

1987(昭和 62)年の改正で刑法に、「電磁的記録不正作出及び供用罪」（第 161 条の２）、「電子計算機損壊等業務妨害罪」（第 234 条の 2)、「電子計算機使用詐欺罪」（第 246 条の 2）などが追加された。そして、2001(平成 13)年には多発するテレフォンカード偽造等に対処するため「支払用カード電磁的記録に関する罪」として「支払用カード電磁的記録不正作出罪」（第 163 条の 2)、「不正電磁的記録カード所持罪」（第 163 条の 3)、「支払用カード電磁的記録不正作出準備罪」（第 163 条の 4）が新設された。

さらに上記の刑法改正の際には時期尚早として見送られた、いわゆる「コンピュータに対する無権限アクセス」がインターネットの民間普及と共に非常に深刻な問題となり、1997 年のデンバー・サミットでの合意を受け、「不正アクセス禁止法」が 1999(平成 11)年 8 月に公布、翌年施行されている。不正アクセスに関しては、刑法本体を改

† 新潟大学
Niigata University

1) 「電子的証拠」というのは筆者の造語である。「電磁的記録（刑法 7 条の 2 で定義）」を含む一連のコンピュータ関連情報の証拠を「デジタル・フォレンジック用語」として総じて何と呼ぶかに関しては、原稿執筆時点では、まだはっきりとした合意がない。よって本稿では「電子的証拠」と称することとする。
2) 本法案が閣議了承されたのは、東日本大震災の当日、平成 23 年 3 月 11 日である。それ故一部のネットの無規制を主張する人々の間で「震災のどさくさに紛れて通過させたネット管理の強化法案」などと揶揄されている表現を良く目にするが、官邸発表等の時間を追えば地震発生前の午前中のうちに閣議決定されたことが分かり、このようなことは当てはまらないことが明確である。

正して罪を追加するのではなく、刑事罰付きの個別立法となっているところが、他のコンピュータ犯罪とは異なる点である。また、制定当時、郵政省・通産省・警察庁の共管として制定された。

不正アクセス禁止法では、刑法の「電子計算機損壊等業務妨害罪」のように電磁的記録の改変・消去などは、犯罪の成立要件として必要なく、ただ他人管理のネットワークシステムに侵入したか否かのみをもって、犯罪の成否を問うている。言ってみれば「住居侵入罪」(刑法 第 130 条) のサイバー空間版のような格付けで作られている。

それ故、電子計算機損壊等業務妨害罪等に比べて、刑罰も「一年以下の懲役又は五十万円以下の罰金」と低くなっており、また犯罪の準備行為は原則取り締まることはできないという基本理念から、もし自身が所有するサーバがポートスキャン3)を受けたとしても、その相手に対して不正アクセス禁止法を適用することができない。また、近年被害が深刻化しているフィッシングに対しても対応できない4)。

上述のことは、法理論からしてみれば比較的抵抗なく受け入れることのできるものであるが、(以下は筆者の個人的な見解であるが、) 技術者側からしてみれば、「その後に深刻な犯罪を行うことが分かりきっている最初の行為を取り締まる法律がこの程度の軽微な罰則で抑止できるわけがない」という感覚が非常に強いようである。事実、ネットワーク管理者の業務は、不正侵入を許さないことこそ、まさにその責任業務のすべてでありその成否のみをもって評価されるといっても過言ではない。筆者も同法成立時に、多くの技術者から「ずいぶんと罪が軽いのですね」という声を聞いたものである。

思うに、この「できあがった不正アクセス禁止法の刑罰を見てみたら、技術者が予想するものよりずいぶんと軽かった」ということから技術者のサイバー犯罪法政への不信が始まったのではないかと、筆者は見る。今回の刑法改正にあたっても技術者側から多くの疑問や注文がなされ、未だに反論や誤解があるのも、成立に 10 年近くを要してしまったことや、このようなことが合い絡まったことが起因するのではないかと思われる。

### 2.2 ウィルス作成罪等成立までの経緯

「コンピュータ・ウィルス作成に関する罪」を導入するための刑法改正法案が最初に国会に提出され際には5、いわゆる「共謀罪」の設置を含むものであったが為、度重なる政権交代による国会の不安定も手伝って、何度も廃案になったことは非常に著名な事実であり、共謀罪に関する議論も本稿とは直接関係ないため、ここでは省略する6。

コンピュータ・ウィルスの作成自体を取り締まるための法規の制定は、いわゆるネットの普及によって必然的に要求されるものであったことはもちろんであるが、国の政策としてそれを整備する直接の強制力となったものは、「サイバー犯罪条約」7)である。この条約は欧州評議会 (Council of Europe) が主体となり制定された条約で、日本もオブザーバ国として参加していた。2001(平成 13)年 11 月署名、2004(平成 16)年 4 月国会承認　同年 7 月発効のものである。この条約を批准するためには、コンピュータ・ウィルスの作成等を取り締まれるようにしたり、条約締結国からのコンピュータ犯罪捜査にスムースに協力できるような体制をつくる必要があり、それ故、その為の国内法整備が必要となったのである。

しかしながら、その成立までに非常に長時間を要したことは前述の通りである。今回の平成 23 年の国会への提出法案によってようやく共謀罪の部分を切り離し、法案名の通り「情報処理の高度化等に対処するための刑法等の一部を改正する法律」として可決・制定された。

サイバー犯罪条約の署名から足かけ十年近い歳月をようしているため、いささか遅すぎるとされても致し方がないと言えよう。以下も個人的見解であるが、「共謀罪の部分を切り離し、コンピュータ・ウィルス作成罪のみを先に制定すべし」という意見は何年も前からほとんどの情報法系の研究者が主張していたはずであるが、これがなかなか受け入れられなかったのは、やはり顕著なサイバー犯罪がさほど多くなかった故に、このような罪状の重要性が官僚や議員達の間で認識されていなかったからであると言えよう。しかしながら、ここ数年は、ネットワークの普及と共にその安全性を脅かす事件が多発し、ここにきてようやくことの重大に気付いたと考えることは想像に難くない。

#### 2.1.1 原田ウィルス事件

コンピュータ・ウィルス作成に関する直接の懲罰規定がないことで、非常に複雑な罪状構成をして逮捕・起訴せざるをえなかった事件に、当時、関西の大学の大学院生が起こした、Winny などの P2P ネットワークを利用した二つのコンピュータ・ウィルス製作／配付事件がある。いわゆる「原田ウィルス事件」8)と「イカ・タコウィルス事

3) ポートスキャン行為はリアル空間においては、さしずめ各家の門や窓に鍵がかかっているかを片っ端から確かめていく行為と言えよう。
4) フィッシングに関しては、不正アクセス禁止法が適用できるよう改正法案が 2012 (平成 24) 年国会に提出される予定。
5) 2004(平成 16)年 2 月 20 日「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」
6) 法案の成立までの経緯は吉田雅之『法改正の経緯及び概要』ジュリ No.1431, pp.58- や、同 吉田『情報処理の高度化等に対処するための刑法等の一部を改正する法律について』ひろば 2011 年 10 月号, pp51- に詳しい。
7) 外務省の Web ページに条約文の和文あり
http://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html
8) 京都地判 平 20.5.16

件」9である。

これらはまさにコンピュータ・ウィルスを作成した本人に直接にたどり着くことができた事件であったが、手頃な直接の罪状がないため、原田ウィルス事件の際は「著作権侵害」での逮捕を行っている。これは、同ウィルスに感染した際にたまたまコンピュータのディスプレイ上に、アニメのキャラクターが表示されるため、そのことをもって著作権の複製権等を侵害したとしたものである。本事件における京都地裁の判決は、執行猶予付きの懲役刑であったところ、この同一人物が、執行猶予期間中に今度は感染するとファイルアイコンがイカやタコの絵のものに代わり、コンピュータ内のファイルを次々に書き換え破潰してしまうというコンピュータ・ウィルス事件を作成した。この事件に対しては、刑法 261 条の器物損壊罪を持って逮捕・起訴している（注：。234 条の 2 電子計算機損壊等業務妨害罪ではない）。もちろん裁判では、このような場合に器物損壊にあたるかどうかも争われたが、裁判所は罪状の成立を認め、実刑判決を言い渡した。

#### 2.1.2 Stuxnet の発見

2010(平成 22)年中頃に発見された「Stuxnet (スタクスネット)」の登場は、一般のパソコンユーザには未だその存在すら知らないものが多いが、少なくとも社会インフラに係わるセキュリティ関係者には大変な衝撃をあたえた。折しも情報セキュリティ政策会議をはじめとする政府や行政機関では「重要インフラ」の安全を高めるための様々な政策を講じている最中であり、そのような状況の中で特定のインフラや制御ソフトだけを狙い撃ちにするウィルスが現れたことによってコンピュータ・ウィルス対策が急務になったと言える。

#### 2.1.3 ウィルス・アーカイブサイトの存在

これに関しては、事件となっていないため判例等は存在しないが、自身の Web ページやダウンロードサイトなどに多数のコンピュータ・ウィルスや悪意あるプログラムなどを保管しそれを配付しているアーカイブサイトが存在することが問題となっていた。IPA（情報処理推進機構）や警察の関連部署などに苦情や相談の連絡が国内外からあっても、適用可能な法律がないため、静観するしかない状況であった10。

今回の法改正までには以上のような経緯があった。

9) 東京地裁 平 23.7.20
10) 実際、筆者もこれらの機関の関係者から相談を受けたことがあるが、「直接可罰法規はなし」としか回答できなかった

## 3. 条文の検討

今回の法改正では、情報システムの開発・管理にあたる現場の技術者の不安や萎縮を軽減しようとした努力の痕跡が多く見られる。例えば、参議院では法務委員会における附帯決議が付されており、法律の施行において特段に配慮すべき項目を五項目挙げている11。その中には、「不正指令電磁的記録に関する罪における……同罪の構成要件の意義を周知徹底することに努めること。……ソフトウェアの開発や流通等に対して影響が生じることのないよう、適切な運用に努めること。」、「通信記録の保全要請に関しては……通信事業者の負担を考慮した適切な運用に努めること。」といった文言が見て取れる。

以下に主な条文を個別に検討してみたい。

### 3.1 不正電磁的記録に関する罪

**刑法** 第十九章の二 不正指令電磁的記録に関する罪

（不正指令電磁的記録作成等）
第 168 条の 2 正当な理由がないのに、人の電子計算機における実行の用に供する目的で、次に掲げる電磁的記録その他の記録を作成し、又は提供した者は、三年以下の懲役又は五十万円以下の罰金に処する。
一 人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録
二 前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録
2 正当な理由がないのに、前項第一号に掲げる電磁的記録を人の電子計算機における実行の用に供した者も、同項と同様とする。
3 前項の罪の未遂は、罰する。

（不正指令電磁的記録取得等）
第 168 条の 3 正当な理由がないのに、前条第一項の目的で、同項各号に掲げる電磁的記録その他の記録を取得し、又は保管した者は、二年以下の懲役又は三十万円以下の罰金に処する。

11) 参議院 Web ページなどで閲覧可
http://www.sangiin.go.jp/japanese/gianjoho/ketsugi/177/f065_061601.pdf

本条文の保護法益は「電子計算機のプログラムに対する社会一般の者の信頼を保護法益とする罪であり，文書偽造の罪（刑法第 17 章）などと同様，社会的法益に対する罪である」となっている12。ここに来て、ようやく情報セキュリティの三要素 CIA（機密性：**C**onfidentiality、完全性：**I**ntegrity、可用性：**A**vailability）の確保を念頭に置き、情報システム自体を重要な社会インフラとの認識が法律の制定趣旨にも表れてきたと言えるのではなかろうか。

### 3.2 168 条の 2 が意味するところ

第 1 項がいわゆる「ウィルス作成罪・提供罪」になり、第２項が「供用罪」になる。

作成・提供・供用とはそれぞれ『「作成」とは、当該電磁的記録等を新たに記録媒体上に存在するに至らしめること、「提供」とは、当該電磁的記録等を取得しようとする者が事実上これを使用できる状態に置くこと、「供用」とは、当該電磁的記録等を、電子計算機を使用している者が実行しようとする意思がないのに実行される状態におくことを、それぞれ意味する』13とされている。（定義が多少曖昧にはなるが、）平易な言葉で表せば、「提供」はコンピュータ・ウィルスを欲している者にそれを渡るようにすることであり、「供用」は他人のコンピュータに勝手にコンピュータ・ウィルスを仕込むことになる。

１ 項１号は「そのままの状態で電子計算機において動作させることができるもの」ということであり、つまりは、即時実行できるバイナリデータであるウィルスそのもので、２号はソースコードの状態のものも含むということになる。

１号は電磁的記録に限定しているが、２号ではその他の記録も含まれるため、必ずしも電子媒体である必要はなく、紙媒体でも良いことになる。極端な話として、T シャツにデザインとして印刷した場合が考えられるが、「人の電子計算機における実行の用に供する目的」が必要になるので、ソースコードを「意味は分からなかったがデザイン的に綺麗な文字列だったので採用した…」とデザイナーが言い張れば　適用されないことになる。PGP の暗号規制の際に同様のことが行われていることを考えると、このようなことは、可能性としては考慮すべきではなかろうか。また今であれば、QR コードなどで　そこにアクセスすれば感染というものを作ることも可能であるので、そのような場合にどうなるのかは、一考の余地がある。

なお、技術者の間で、完成度の低い OS や、深刻なバグを含むプログラム自体がこの「不正指令電磁的記録」にあたるのではないかという危惧があるようであるが、本罪が成立しうるのは、それが不正指令電磁的記録と認識された時点以降の行為であり、仮にそのようなものを開発してしまったからといって、本罪が適用されるわけではない。また仮にそのような深刻なバグを含むプログラム自体が不正指令電磁的記録とされるには、当然に一般社会通念上の合意が必要となるはずであり、バグが不可避と考えられている現状においてはそのようなことは起こらないと言えよう。つまりは、一部のコンピュータの専門家だけが、「このような不完全なプログラムは、けしからん」などと言っていても到底まかり通るものではなく、一般のすべてのコンピュータ・ユーザが「このプログラムはウィルスだ」という認識を持つことが必要なわけである。供用罪についても同様で、そのプログラムを第三者が実行できる状態においた時点で不正指令電磁的記録を認識していなければ成立しない14。

また、条文の読み方から、供用罪には２号事例（つまり、ソースコード状のもの）は含まれない。また、未遂罪が可罰なのも２号の供用罪のみとなる。

さらに、コンピュータ・ウィルスによる攻撃によって、相手のサーバのデータを破壊するような悪質ウィルスを実行させるような場合には、不正指令電磁的記録供用罪だけでなく電子計算機損壊等業務妨害罪も適用することを妨げるものではないであろう。この場合は、五年以下の懲役又は百万円以下の罰金に処するとなる可能性もある。

### 3.2 168 条の 3 が意味するところ

同条はコンピュータ・ウィルスの「取得」「保管」について前条よりも多少軽微な罪を定めたものであるが、ここでいう『「取得」とは、不正指令電磁的記録等を自己の支配下に移すことを、「保管」とは、当該電磁的記録等を自己の支配領域内において置くことをそれぞれ意味する』15ものである。

### 3.3 当初法案からの修正点

法務省の公開している条文の修正点を見ると16、当初は「正当な理由がないのに」という文言は存在しなかったものを、今期提出の法案に際して付記したことが分かる。これは、まさに対ウィルスソフトの開発や研究、またバグ等を内包したプログラムを開発してしまった技術者への杞憂を低減することを目的に追加したことになる。しかしながらこの点に関しては、『正当な事件等は、システム管理者等の同意を得てなされている以上、1 項の「人」の要件が欠けるし、「電子計算機における実行の用に供する目的」も欠けている。そこで従前の犯罪化案の下でも適切な対応は可能であった。』17との見解があり、筆者もこれに同意見である。しかしながら、今井も述べているとおり、これは技術者の萎縮の低減、つまりプログラム開発者の不安

12) 法務省公開資料「いわゆるコンピュータ・ウイルスに関する罪について」
http://www.moj.go.jp/content/000076666.pdf
13) 今井猛嘉「実定法の視点から」ジュリ No.1431 p.67 左段
14）吉田　前掲　による見解も同様である。ジュリ No.1431 pp.61-61 脚注部
15) 今井　前掲　ジュリ No.1431 p.68 左段
16 同法案に関して掲載している Web ページ内にある修正点一覧表
http://www.moj.go.jp/keiji1/keiji12_00025.html
17) 今井　前掲　ジュリ No.1431 p.68 右段

をより明確に取り除くために挿入されたと言え，これがなければ、実験・研究でのウィルスの作成や些細なバグ付きソフトの配付などが違法などだという考え方は早計である。

## 4. その他の刑法の修正

その他にも、今回のサイバー犯罪対応の修正として、第 175 条（わいせつ物頒布罪等）に、「電磁的記録に係る記録媒体その他の物」を含むとし、「電気通信の送信によりわいせつな電磁的記録その他の記録を頒布」も頒布の範疇に含めるとした。これは従前の判例や現在の捜査・検挙事例を明文化したものと言えよう[18]。
した者も、同様とする。

また、あわせて第 234 条の２（電子計算機損壊等業務妨害罪）に第 2 項として未遂罪が追加された。不正指令電磁的記録作成罪等ばかりが大きく取り上げられ、この件に関して関心が低いようであるが、筆者は、本罪に未遂罪が適用可能になったことは非常に大きな意味を持つ、すなわち高い実用性・即効性が期待できるものと思われる。

なお、今回の改正本法案のタイトルは「情報処理の高度化等に対処するための刑法等の一部を改正する法律」であるが、実は、強制執行妨害関係の罰則追加も合わせて行われている。なぜそれが情報処理の高度化と関係があるのかに関して疑問の余地があるが、この点に関しては本稿では検討の対象外とする。

## 5. 考察

本論冒頭にも述べたとおり、2010 年 7 月に Stuxnet が発見されてから、コンピュータ・ウィルスは新たな次元に入ったと言えよう。コンピュータ・ウィルスの作成目的も、初期の愉快犯から、金銭目的へのものへと代わり、最近では標的型攻撃による特定の情報収集を目的にしたものや、特定の企業・組織を対象とした攻撃まで現れ始めている。

このような状況の中で、コンピュータ・ネットワーク自体を社会的保護法益とした本改正は評価できるものである。

一方で、2009(平成 21)年の不正競争防止法への図利加害行為追加に関する改正の時もそうであったが、果たして国家転覆を謀るようなサイバーテロが行われた際に関してまで、通常のコンピュータ犯罪と同じ条文を適用することが良いのかどうかは疑問が残る。

また、今回の改正に際しては、プログラムにおけるバグが必然的なもの、不可避なものと決めつけられて議論されているような感がある。筆者もバグが回避可能であるものとは思ってはいないが、少なくとも法律としてバグの性質が定義できていない以上、バグに関してはもう少し慎重な議論をしても良かったのではないかと思われる。例えば、民事上の責任や製造物責任（ハードと一体化したプログラム）における「欠陥」や「瑕疵」といった概念とバグが一致するかは PL 法制定時より議論されているが結論がない。刑事法制の上ではより慎重な議論が求められるのではなかろうか。

また、わいせつ物頒布罪等に電磁的記録に関する規定が追記されたことに関しては、諸外国への心情を高めるという点が評価したい。海外からの日本に対する批判で多いのは、むしろポルノ問題（この場合、児童ポルノではなく、児童ポルノに勘違いされる若い日本女性の裸体写真など）であり、サイバー犯罪条約に対する PR 効果からもこの条文を追加することに意味があったと思われる。

### 5.1 今後の課題…刑事訴訟法改正部分の検討の必要性

本稿では、同時に改正された刑事訴訟法の電子的証拠の確保の部分についての考察を行っていないため、今後、サイバー犯罪条約との関連も含めて、こちらの考察も必要である。例えば、通信履歴（いわゆる、ログ）の保全機関の要請については、当初は保全期間が 90 日だったものの、ISP 等の負担を考慮して 30 日に下げられた経緯がある。しかしながら国際的には 90 日が標準となっている現状において、日本だけが 30 日（最長で 60 日）でとしたことが果たした良いことなのかどうかなどである。大容量のストレージの記憶装置が矢継ぎ早に開発されている現在においては、ISP の負担とはすなわち、その分の調達コストであり、高度に技術的な負担を強いるというわけでない。つまりは各々のユーザにストレージ代を課せば可能にはなるという意味であって、ネットワーク社会の安全の為の国民のコンセンサスが得られるかどうかという問題になるわけである。

また、この刑事訴訟法の改正が、証拠保全を行う民間企業などの個々の技術者にどのように影響してくるかについてもまだ未検討である。刑事訴訟法の改正部分に関しては電子証拠を扱うべき対象が主に捜査官であるため、直接的には現場技術者にはさほど影響があるとは思われない。しかしながら、自身の管理するネットワークシステムがコンピュータ犯罪に巻き込まれた場合、証拠の保全要請がある日突然に捜査機関から依頼される可能性や、「(クラウド）ネットワーク上のこの ID に関する通信記録を（令状によって）保全したい」という要求を受ける可能性はあるため、それに応対

18 たとえば、猥褻図画のデータを含有するハードディスクそのものが「猥褻物」であるとした「アルファネット事件」最高裁決定がある。裁決 平 13.7.16

できるような心構えは必要となるであろう。
　これらについては、今後の検討課題としたい。

### 5.2　おわりに

　サイバー犯罪条約署名当時、我が国の条約への対応は不正アクセス禁止法や著作権法におけるデータベースの定義、公衆送信権など、比較的進んでいるほうであった。しかしながら、最大の課題として残っていた部分が今回の改正部分この部分であり、これを今日まで引っ張ったが為に、逆にどちらかといえば対応が遅い国のほうになってしまった。
　また、サイバー犯罪はもともと犯人が見えにくい上に、手口がいっそう組織的かつ巧妙になった今日において、サイバー犯罪条約に添ったからといって情報化社会の安全性がただちに守られるわけではなく、国家安全保障も含めた非常に広い視野でのサイバーワールドの安全確保の為の法制が必要であると言える。　（以上）