コンピュータウイルス等有害プログラムの法的規制に関する国際動向調査

高橋郁夫法律事務所

第1章 調査の契機および報告概略

第1節 背景についての事実認識

第1項　メリッサ・ウイルス出現

1999 年 3 月 26 日 午後 7 時(GMT)に、コンピューター緊急対策レスポンスチームは、マイクロソフトのワード 97 とワード 2000 に関するマクロウイルスの報告を受けた。このマクロウイルスは、　MSword 及びマイクロソフト社の Outlook がインストールされている環境で、ウイルスに感染した文書を開くと、ウイルスが動作し、Outlook のアドレス帳に登録されているメールアドレス５０カ所に対して、ウイルスに感染した文書を添付したメールを送信するというもので、このウイルスは、そのコードに使われていた名前などから「メリッサ(Melisa)」となづけられた。このメリッサの被害は、かなりのものがあり、マイクロソフトでも、メールによる外部に対する被害拡大の防止のために社内のメールシステムをとめたほどである[1]。

第2項 メリッサ・ウイルス事件の法的帰趨

この事件の容疑者(David L. Smith)は、AOL からの情報提供などをもとに、公共通信妨害、違法共謀、違法共謀未遂の容疑で、4 月 1 日に逮捕された。さらに、コンピュータ・サービス窃盗罪、コンピュータ・システムへの違法なアクセスという 2 つの微罪の容疑もかけられていたとのことである。そして、連邦法の関係では、セクション 1030(a)(5)(A)の「故意にプログラム，情報，コード（code）もしくはコマンドを送信（transmission）させ，その行為の結果として，故意に，無権限に、保護されるコンピュータ（protected computer）に損害を発生させる」 の容疑で捜査された。
スミス容疑者は、容疑を否認するであろうとの報道もなされていたが、結局、1999 年 8 月には、メリッサウイルスを作成したことを認め、12 月 8 日には、州および連邦の容疑を認める司法取引をなした。翌日には、司法省から、この司法取引に関するリリースも発表されている[2]。

---

[1] なお、このメリッサのインパクトなどについては、http://cnet.sphere.ne.jp/News/1999/Item/990424-4.html の関連記事からのリンクを参照のこと、また、要領のよいまとめとして議会の公聴会における発言 http://www.fbi.gov/pressrm/congress/congress99/vatis1.htm がある

[2] http://www.usdoj.gov/criminal/cybercrime/compcrime.html

第3項　コンピューター・ウイルスの頻繁な流布

1999年には、上述のメリッサ・ウイルス以外にも、種々のコンピューター・ウイルスが発見され、しかも、より、強力に、改変されている点が注目されている状況にいたっている。
具体的な例としては、バブル・ボーイウイルス、バビロニア・ウイルスなどがある。バブルボーイは、1999 年 11 月 8 日に発見された、ユーザーがメールや添付ファイルを開かなくても感染する初のコンピ ューター・ウイルスであるとされる。これは、 テレビのコメディー番組『サインフェルド』(Seinfeld)にちなんで『バブルボーイ』と名づけられた[3]。また、バビロニア・ウイルス(『W95.バビロニア』-(W95.Babylonia)は、同 12 月 7 日(米国時間)頃に、オンラインのチャットルーム で広がりつつあったもので 2000 年問題バグの修正プログラムを装ったウイルスである。このウイルスは、 初めての「拡張性のあるワーム」で、インターネット・リレー・チャット(IRC)のユーザーを攻撃することができ、ウイルスの作者が、攻撃の仕方やデータの盗み方を日替わりで変えられると いう危険性をもつものである。
また、これらのコンピューター・ウイルスが、ウエブページ上に公開され、一般に広まり、また、より攻撃力をましたような形で改変されるという危険性も指摘されるにいたったのである。

第2節　有害プログラム

第1項　概念

Charles P.Pfleeger”Security in Computing” Prentice Hall PTRによると、「有害プログラム(害意あるコードおよび悪劣プログラム Malicious code or rogue program)とは、ダメージを及ぼすエージェントの意図による、予期しない、ないしは望まない影響を及ぼすプログラムやそのプログラムの一部分の一般的な名称である。」(Malicious code or rogue programis the general name for unanticipated or undesired effects in programs or program parts, caused by an agent intent on damage.)と定義されている。この定義は、基本的に二つの要素を含むことになる。その一つは、そのプログラムなどがコンピューターのユーザーの「予期しない、ないしは望まない影響を及ぼす」ことであり、今ひとつは、そのプログラム等の作者が、「ダメージを及ぼすエージェントの意図」を有していることである。したがって、このような定義からすれば、「害意あるプログラム」には、意図的ではない誤り(たとえばバグ)も含まれることはないし、良いプログラムがたまたま悪い影響を及ぼすのも含まれないことになる。しかしながら、この定義についても、境界線上にはいろいろな問題がある。

第2項　ウイルス

まず、従来からも議論されているものについては、コンピューターウイルスがある。 Pfleeger の本では、ウイルスは、「ウイルスは、悪意あるコードを他の悪意が存在しないプログラムに、

[3] http://www.hotwired.co.jp/news/news/Technology/story/3354.html

改変によって伝えるもの」(A virus is a program that can pass on malicious code to other nonmalicious programs by modifying them)と定義しており、「感染」をメルクマールにしている。このウイルスには、移転性(transient)のものと滞在性(resident)のものがあるとされる。このウイルスも、現在におけるネットワークの発展に伴う問題も発生しているところである。従来は、ユーザーに「予期しない、ないしは望まない影響を及ぼす」ことによって直接的に業務阻害をきたす(ただし、その阻害性についてはきわめて強弱がある)ものが一般的であったといってよい。
このような直接的な業務阻害性を有するウイルスについては、従来その寄生する場所をメルクマールにして、「ブートセクター感染型」「ファイル感染型」「マクロウイルス」などに分類されていた。
しかしながら、1999 年の 3 月 26 日に急速に被害が拡大したメリッサウイルスのように、それ自体では、直接的な業務阻害性を有しないにも関わらず、ネットワークの発展、一般化によって、業務阻害を引き起こしてしまうという形態が、注目を浴びるようになってきている。

第3項　その他の害意あるコード

そのほかに、害意あるコードとして従来議論されているものについては、「トロイの木馬」「悪意あるスクリプト」などがある。これらは、「ユーザーの予期しない動作」「制作者の害意」という二つの要件を満たすものである。また、例えば、わいせつサイトによく見られるもので、このソフトをダウンロードしてくださいとなった場合に、そのソフトが自動的に海外へのダイヤル Q2 の番号へのネットワークを作成して、本人の知らない間に、極めて多額の電話料を請求されるという事案も有る。

第4項　限界事例

さらに視点を広げると、ユーザーに「予期しない、ないしは望まない影響を及ぼす」ものではなるが、そのプログラムの作者としては、「害意」は有していないとしている場合が有る。この代表例としては、Back Orifice が挙げられる。このソフト自体は、公式には、リモートコントロールソフトということになる。作者からいわせるととくに害意が有るわけではないことになる。しかしながら、その実際は、いわゆるハッカーツールである。また、知らない間に、個人情報ないしはコンピューターの構成を読み取られ、送信されることがある。これらは、作者に害意はなく、単にお節介だけなものであろうが、しかしながら、ユーザーのコンピューターに関する自己決定権を保護するという傾向からすれば、議論を呼ぶところである。

第5項　ユーザーの「望まない影響」による分類

上記でも見てきたが、有害プログラムの法的分析については、その及ぼす影響ごとに分類することが有効なものと考えられる。
それらは、(以下、後の議論の便宜上、便宜的に名称をつけた)

1)業務阻害型

業務自体を阻害してしまうもの(ブートセクター破壊型が代表)

2)処理能力低下型

業務を直接に阻害するわけではないが、その処理を低下させてしまうもの(ファイル寄生型の一つ)

3)過負荷能力低下型

実行されたコンピューター自体の業務阻害ないしは処理能力を低下させるものではないが、ユーザーの予期しない動作をさせることにより、多数に移転する性質から特にネットワークに必要以上に負荷をかけて、ネットワーク・コンピューター自体の性能等を低下させてしまうもの(メリッサウイルスなど)

4)詐欺的実行型

ユーザーの予期しない動作により、コンピューターに別個の動作をさせ、それがネットワークの課金のシステムなどを介することによってユーザーに予期しない損害を与える場合(アダルトサイトのダイアラー自動実行プログラム)

5)詐欺的情報提供型

ユーザーに金銭的損害、業務阻害等を与えるものではないが、ユーザーの個人的な情報を外部に送信するものであって、金銭的な損害を与える危険性のあるもの(「トロイの木馬」)、ないしは、システムの弱点を伝えるもの(Back Orificeのようなもの)

6) 嫌悪感惹起型

ユーザーの予期しない動作により嫌悪感を引き起こす特定の動作をするもの(スクリーンセーバーの起動・特定の音をだすもの)

7)単純情報提供型

ユーザーの個人的な情報を外部に送信するものであって、ユーザーに金銭的損害、業務阻害等を与えるものではないもの(cookie、Java scriptなど)
などに分けられるものと思われる。

第3節　調査の必要性

1 わが国における刑事法的対応

わが国での有害プログラムに対する刑事法的対応としては、まず、昭和 62 年の刑法改正の段階においては、時期尚早であるとして、コンピューターウイルスに対する直接的な対応は、見送られている。では、現行法によって全く対応できないかといえば、そのようなことはない。
一般的には、このような行為については、データ自体の改変、システムに対する脅威、業務自体に対する妨害の観点などから捉えることができるであろう。しかしながら、やはり以下のような限界に直面しているということはできそうである。
データ自体の改変という観点からすると、電磁的記録の改変、消去については、その電磁的記録が人の権利義務に関するものであることなどが要求されており、メリッサ型のコンピューターウイルスに対して直接に対応しきれるということはいえない。
業務阻害に関して、上述の業務阻害型および処理能力低下型については、「電子計算機損壊等業務妨害罪(刑法 234 条の 2)」および「業務妨害罪(刑法 233 条)」の各規定の適用が問題になる。しかしながら、処理能力低下型については、この要件をみたすものといいきれるかどうかが問題になるものと思われる。また、単純な嫌悪感を惹起するものについては、一般の業務妨害ともいえないとも考えられる。
また、詐欺的実行型については、詐欺罪での適用を考えることはできるが、その準備段階にあるもの((5)の詐欺的情報提供型)については、具体的な犯罪類型としてとらえることは、困難なように思われる(ただし、ID およびパスワードの収集については、不正アクセス対策法の点で対応が可能とも思われる)
また、(3)過負荷能力低下型については、直接に業務阻害を目的にしていないこともあって、その構成要件適合性については、議論の余地があるように思われる。
その上、コンピューターウイルスにおいては、作成した者のみが問題になるわけではない。それをウエブ・ページなどで、ウイルスであると承知のうえで、拡散するものもいる。そのような者にたいし、どのような法的対応をすべきかという問題もある。
これらの観点からいって、コンピューター・ウイルスに対するわが国の刑事法的対応については、現時点においては、対応として不明確なところが存在するということもいえよう。

2 調査の必要性

わが国における刑事法的対応において、なおも、曖昧な点も存在し、また、業務阻害性自体が犯罪成立のメルクマールになることもあり、実際の事件が起きた際に、法の適用に困難をきたすことも予想できる。
その際に、実際に諸外国において、どのような対応がなされているかを検討することは極めて重要である。

第4節　調査課題および調査方法

第1項　調査対象事項

私たちは、上記のような「有害プログラム」のもたらす害について、それらを法的に看過することはできないという認識にたっている。民事的な対応についてもそうであろうし、また、特に刑事的な対応がさらに必要であるか詳細に検討すべき時期にきているというのが、現状認識である。
基本は、従来型のコンピューターウイルスに対する世界各国における法的対応(制定法および判例)の具体的な調査を基礎とする。そして、メリッサのような新たなウイルスに対して各国がどのような法的対応をなすことができるか、また、対応をしようとしているのかについて情報を集めることがさらなる目標となる。とくに上述のように境界線とでもいうべきメリッサ型のウイルスについて、諸外国の法律はどのような対応をしているのかを調査することが最大の目標になる。

第2項　調査手段

その手段については、事前の文献調査および聞き取り調査、質問書による調査および聞き取り調査、事後の補充調査による。

1 事前調査

対象国の関連法規を入手するとともに、その時点における調査者の手元における資料により、対象国の「有害プログラム」に対する刑事的規制について調査する。とくに具体的な事例があれば、刑事的事例およびその争点、また、民事的事例についても参考になるかぎりでちょうさをすることが望ましい。

2 現地調査

対象国の現地語による質問書を作成し、現地に出向き、コンピューターセキュリティの法律問題について専門的な知識を有する専門家との面談によって、現地での問題状況を把握する。この場合、一定の費用を前提に現地法律事務所に対する法的意見書等の作成も可能である。
また、現地において最新の情報を収集する必要がある。

3 補充調査

調査報告書を作成するとともに、各国における問題点をメーリングリストで意見交換するとともに、その過程で発見した問題点についてさらに調査をする。

4 調査体制

調査の受託の主体としては、高橋郁夫法律事務所が主体となるが、実際の調査においては、調査対象国ごとに担当の大学の刑事法・ネットワーク法専攻の研究者ないしは弁護士に報告のとりまとめを依頼する。その上で、議論の上、各国報告のとりまとめおよびわが国における問題提起を行う。

上記調査体制につき、以下の陣容で調査を行う。

アメリカ合衆国

連邦法および州法	明治大学教授・弁護士	夏井 高人
判例調査	弁護士	土井 悦生
メリッサ事件調査	新潟大学助手	須川 賢洋

カナダ

弁護士 岡村 久道

フランス

亜細亜大学講師　島岡まな

イギリス

弁護士 高橋郁夫

ドイツ

神奈川大学講師　石井徹哉

第5節 各国調査内容の概略

第1項 アメリカ合衆国

アメリカ合衆国は、連邦法および州の制定法により、害意あるコードに対する対応が図られている。連邦法においては、第 1030 条が対応しており、また、州においては、コンピューターウイルスに対する特別の規定でを有する州もあり注目される。かかる制定法の適用が問題になった事件はきわめて少ないが、1999 年 3 月に起きたメリッサ事件は、州および連邦法の適用を前提に司法取引がなされた。

第2項 カナダ

カナダ法には、特に悪意あるプログラムの配布等に対応することを目的とした規定は存在しない。しかし、刑事法及び民事法の法原理は、こうした配布等の行為に適用しうる可能性を有している。すなわち、刑事法においては、1987 年の「データに関する損壊の罪」および「無権限使用の罪」によりそうした「悪意あるプログラム」の作成・投与・配布等に対応することが可能であると思料される。

第3項 フランス

フランスにおいて、コンピュータ・ウィルス等の有害プログラムに関する特別法は存在しないため、新刑法典のコンピュータ犯罪規定の一部によって、この問題に対処しようと考えられている。現時点では、有害プログラムに対する具体的な適用判例もなく議論もありうるが不正アクセス罪（フランス刑法典第 323-1 条）、コンピュータ業務妨害罪(同第 323-2 条、データ不正操作罪(第 323‐3 条)により刑事的規制がなされるものと考えられる。

第4項 イギリス

メリッサ型のいわゆる電子メール・ウイルスについては、争いがありうるものの、それが実際のファイルの消失をきたすということがなくても、コンピューター不正利用法第 1 条(無権限アクセスの禁止)、第 3 条(無権限改変の禁止)に違反するものとして処罰されるものと考えられる。また、電気通信法 1984 第 43 条の規定により、そのようなウイルスの送付・拡散が規制される点に特長が有る。

第5項 ドイツ

コンピュータ・ウィルスによる侵襲という視点からみた場合、問題となる条文は、刑法典上の情報へのアクセスに対するインテグリティを問題にとする 202 条 a (データの探知)、303 条 a(データ変更) 、303 条 b (コンピュータ妨害)が問題の中心となる。メリッサ型のウイルスについては、故意の点に問題がなければ、コンピュータ妨害となるものと認識されている。1987 年の第二次経済犯罪対策法の導入に関しての議論がなされたこともあって、ドイツにおいては現在、この 3 つの条項で基本的には有害プログラムに対する対応は十分であると認識されている。

第6節 我が国に対する示唆概要

わが国では、データの探知やデータの損壊というアプローチは実効的ではないが、偽計ないしは威力業務妨害罪によって、コンピューターウイルスの投与について問題となるケースのかなりの部分は、カバーできるものと考えられる。しかしながら、この場合でも、実際の適用上の問題と、本質的な限界の 2 つの問題点があることについては留意しておく必要がある。

実際の適用上の問題点というのは、その「業務妨害」の文言の解釈で見た問題点である。前述したように判例の立場を前提とする限り、業務妨害罪は、実質的に抽象的危険犯として解されている(それゆえにコンピューターウイルスによる不都合が、かなりの程度、構成要件該当性を、満たすものと解されているのである)。もっとも、マジックホン事件を前提とする時、わずかな作用阻害の虞でも、業務妨害が成立するという立場も可能であろう。また、業務妨害の結果についても、故意の対象となるので、投与ないしは拡散行為について認識していないと有罪とはならない。実験でウイルスを作っていたのが、うかつにも流失してしまったという場合には、刑事的な処罰の対象とはならないものと考えられる。そのため、モーリス事件のような場合は、業務妨害の成立が否定される可能性が高いことになる。

本質的な限界というのは、業務「妨害」という性質をメルクマールにするので、むしろ、悪意あるプログラム自体の情報の取得、流出という行為に対する対応迄は対応しきれないと考えられることである。トロイの木馬やバックオリフィスなどは、その性質上、情報の取得、流出という問題点に対して正面から対応しきれない。なんら悪さをしなくても情報が流出する自体で業務が妨害されるということもできなくはないであろうが、妨害概念が拡散し過ぎるという批判がなされるであろう。まず、現在の判例の立場を前提として、実際の業務の妨害を許容される限りで、コンピューターウイルスや悪意あるプログラム一般に対する対応を考えるというアプローチがなされうるであろう。現在の判例が、業務妨害の結果および手段に対して広範な解釈を取っていることから、実際上の問題点というのはあまり現実にはおこりえないという考え方もありうるであろう。

それに対して、業務の妨害やその手段についての解釈をそれ自体の文言の意味を維持して厳格にしようというアプローチからは、現実の適用に対して、問題がおこりうる可能性がある。バックオリフィスやトロイの木馬については、何らかの規制を考えるという点については、異論がないとしても、ある種のスクリプトやクッキーなどは、利用者にことわりなく利用者の個人情報を流出してしまうのである。

(第一章担当 弁護士 高橋郁夫)

各国別調査報告

第2章　アメリカ合衆国

第1節　総　説

アメリカ合衆国においては，周知のとおり，コンピュータ犯罪を含む刑事法的対処のための法制は，連邦と州とで事物管轄を異にしており，それぞれ別の法制によって規律されている。ウイルス犯罪に対処するための法制でも同様であり，連邦の事物管轄に属する犯罪類型については連邦法により，州の事物管轄に属する犯罪類型については州法により，それぞれ規律されている。以下，特に指示しない限り「コンピュータ犯罪」の中に「ウイルス犯罪」を含めて論述する。

まず，アメリカ合衆国の各州内で発生するコンピュータ犯罪であって，連邦によって保護されるコンピュータ以外のコンピュータに関連するコンピュータ犯罪等以外のコンピュータ犯罪に関しては，各州の制定法（statutes）によりそれが処罰対象となるかどうかが定められている。すなわち，各州内のコンピュータ犯罪の事物管轄権は，第一次的には州の法執行機関及び州裁判所に属し，また，適用法も各州の定める制定法である。州法の立法例中では，各州の刑法典（Penal Code / Criminal Code）中でコンピュータ犯罪に関連する規定をまとめ独立の章として規律する立法例が多い。

これに対し，州際取引（interstates trade）及び国際取引（international trade）に関連するコンピュータ犯罪並びに連邦のコンピュータその他連邦法で指定されたコンピュータ（連邦によって保護されるコンピュータ）に関連するコンピュータ犯罪の事物管轄権は，連邦の法執行機関及び連邦裁判所に属し，適用法も連邦の制定法である。連邦法による法的対処は，大きく分けて２つの制定法によってなされている。一方は，連邦の刑法典である合衆国連邦法律集第18編の第47章（U.S.C. title 18 chapter 47）の中にある第1030条（sec.1030）であり，他方は，同編の第121章（chapter 121）中にある第2701条ないし第2711条（sec.2701-2711）である。前者は，コンピュータ犯罪の中でも「無権限アクセス（unauthorized access to computer）」に対する処罰法規を中心とする刑罰法令であり，後者は，電子通信中のプライバシー侵害に対する処罰法規を含む法令である[4]

この２つの連邦制定法における条文の文言のみに基づいて解釈論を検討する限り，この２つの制定法のいずれかによって，ほぼすべてのタイプのウイルス犯罪に対する対処が可能である

[4] 普通の「詐欺」の手段としてコンピュータ・ウイルスを用いる犯罪があり得ることがアメリカ合衆国においても既に指摘されている。このことは，日本の刑法においても同様であり，詐欺だけではなく，器物損壊罪，業務妨害罪，文書毀損罪など様々な犯罪類型について，コンピュータ・ウイルスの応用を考えることができる。これらの行為については，当然のことながら，詐欺罪その他の刑法上の一般的な犯罪が成立することになる。本報告では，報告の性質上，こうした一般犯罪については，触れないこととする。

と思われ，そのいずれの法令によって処罰されることになるのかが必ずしも明確であるとはいえない。しかし，後に述べるように，Morris 事件についての連邦控訴裁判所の理解を前提にすると，たとえばマイクロソフト社のアウトルック用のアドレス・ブックを無権限で参照し，自動複製されたメールを自動転送するようなタイプのウイルスやワームを含め，連邦法によって保護されるコンピュータに感染するものである限り，ほとんどすべてのタイプのウイルスが第 1030 条（特に 1030 条(a)(5)）によって処罰可能である。また，1996 年改正法についての合衆国司法省の解説（資料編参照）においても，第 1030 条によってウイルス犯罪又はワーム犯罪がカバーされていることを当然の前提とする論述がなされている。したがって，アメリカ合衆国における法執行実務及び判例法を前提にすると，アメリカ合衆国連邦におけるウイルス犯罪は，そのほとんどすべてが「無権限アクセス」として第 1030 条によって対処可能だと理解することができる。

本報告書においては，まず連邦法に関して第 1030 条についての検討結果を報告し，次に各州のコンピュータ犯罪法中でウイルス犯罪に対処するための何らかの条項を有するものを中心に，その検討結果を報告する。その上で、具体的な判例について概観し、メリッサ事件についての処理を時系列的に追うことにする。

第2節　連邦制定法の検討

第1項　合衆国連邦法律集第 18 編第 47 章第 1030 条

第 1030 条が最初に制定されたのは 1984 年である。当時既に数多くなされつつあった州のコンピュータ犯罪法立法には遅れるものであったが，この法律によって，連邦の管轄・管理するコンピュータに対する無権限アクセスが処罰可能となった。

その後，同条は，1986 年及び 1994 年にそれぞれ一部改正がなされている。現行法として有効な法律は，「1996 年国家情報基盤保護法」（後掲資料参照）により更に一部改正がなされた後の法律である。

現行第 1030 条の条文は，後掲資料のとおりであるが，一読して非常に理解しにくいと言わざるを得ない。とりわけ，コンピュータ犯罪の成立要件を定める同条第(a)項内にある各規定，就中，同条同項第(1)号の規定は，長文であることもあって，非常に難解である。このことは，合衆国の法律家にとっても同様であったようである。合衆国対 Morris 事件は，インターネット・ワームによる加害事案につき同条(a)項(5)号(A)を根拠法規として起訴された。この事件の控訴審判決（1991 年 3 月 7 日連邦控訴裁判所第二巡回区裁判所）の中でも第 1030 条（1986 年改正法）に定める犯罪成立要件（犯意要件及び無権限アクセス要件）について詳細な検討がなされている（後掲資料参照）。この判決によって明らかにされたことは 2 点である。

第 1 点：

1030 条(a)項(5)号(A)の犯意の要件である「意図して（1984 年法では「故意に」）」は，「アクセスする」にのみかかものであって，無権限アクセスの結果としての損害発生等については犯意要件がかからない。日本法に則して言うと，損害の発生は，結果的加重犯における加重的結果に相当することになる。従って，損害の発生を意図してい

なくても，無権限アクセスになることを意図していれば，そこから発生する重大な結果に対しても刑事責任を負うことになる[5]。

第２点：

直接にアクセスするコンピュータについてはアクセス権限を有している場合であっても，それとネットワークを介して接続されている他のコンピュータについてはアクセス権限がなく，かつ，そのアクセス権限のないコンピュータにネットワークをアクセスする行為を（意図して）実行すれば，無権限アクセスである[6]。

Morris 事件判決において，連邦第２巡回区控訴裁判所は，このような理論的理解を前提にした上で，Morris が作成したワーム・プログラムはセキュリティ上の欠陥をついて他のコンピュータに自動的にアクセスするものであり，そして，その他のコンピュータの中には政府機関のコンピュータも含まれており，それらのコンピュータが機能障害を起こして損失を発生させたのだから，Morris が最初にワームを流し込んだコンピュータがアクセス権限のあるコンピュータであったとしても，第 1030 条(a)項(5)号(A)に定める無権限アクセスに該当し有罪であると判断した。

この判断に従うと，合衆国連邦によって保護されるコンピュータのみを避けて通るように特別に設計されたウイルス又はワームでない限り，どこの国の誰によってどのコンピュータからウイルス等が導入されたものであったとしても，そのウイルス等を導入したコンピュータが合衆国連邦によって保護されるコンピュータにネットワークを介して接続（通信）可能なものである限り，第 1030 条(a)項(5)号(A)に定める無権限アクセス罪が成立し得ることになる。

そして，このような無権限アクセス罪によって処罰されるのは，最初にウイルス等を作成してネットワーク上に流し込む者だけではなく，他の者が作成してウイルスを導入する者やそれを意図的に転送・配付する者も当然に含まれる。

かくして，合衆国連邦によって保護されるコンピュータに関する限り，意図的になされるほぼ全ての種類のウイルス導入行為，配付行為，転送行為は，第 1030 条の当初の(a)項(5)号(A)によって処罰可能であると解釈すべきことになった。なお，現行法（1996 年改正後の条文）上では，意図的に損害を発生させた場合には(a)項(5)号(A)により，過失によって損害を発生させた場合には(a)項(5)号(B)により，無過失で損害を発生させた場合には(a)項(5)号(C)によりそれぞれ処罰されることになる。これら各類型に対応して，同条(c)項において処罰規定が定められている。

ただ，単にパスワード等の盗取のみを目的とし，損害の発生を目的としないトロイの木馬型ウイルスについては，第 1030 条(a)項(6)号に定める「州際取引若しくは国際取引に悪影響を及ぼす場合」又は「合衆国政府により若しくはそのために利用される場合」という結果を発生させる場合には「詐欺的なトラフィック」という概念に含まれるものとして対処がなされているが，それ以外の場合には 1030 条はカバーしているとは言えない（これ以外の場合として想定さ

---

[5] 日本国刑法の解釈では，結果発生について予見可能性及び過失を要するという見解もある。しかし，刑事裁判実務においては，一般に，故意による行為と重い結果発生との間に因果関係が存在するのみで有罪とする例が多い。連邦法第 1030 条の解釈論としては，この点は不明であるが，調査した範囲内では，日本の裁判所の態度と同様に，意図に基づく行為とその結果との間に因果関係の存在が認められさえすれば，重い結果発生についての過失や予見可能性を問題にすることなく，その重い結果発生に対する刑事責任を問うことができると解されているようである。

[6] この判例理論によれば，インターネットは，（研究・実験等の目的で適法に）ウイルスを導入する権限を有しないコンピュータ・システムが無数に接続されていることは当然であり，そのことを認識することも可能であるから，インターネットに接続されたコンピュータ装置に対してウイルス・プログラムを導入することは，それだけで常に無権限アクセス行為になり，その無権限アクセス行為についての処罰要件の充足性だけが問題になると理解すべきことになる。この点，日本の不正アクセス禁止法では，非常に限定された行為のみを不正アクセスとしていることと大きく相違するので，注意を要する。

れるのは，連邦の制定法の事物管轄ではなく，各州の制定法の事物管轄に含まれるものがほとんどであろうと思われる。その意味では，連邦法はすべての場合をカバーしているということもできる。)。

なお，印刷された論文（law School の Review を含む。）及びインターネット上のドキュメントを含め，この報告書における結論と反対の見解を見いだすことは，できなかった。

第2項　合衆国連邦法律集第 18 編第 47 章第 1030 条各条項の解釈

1030 条の規定は，非常に分かりにくい構造をしているが，その犯罪成立要件及び犯罪毎に対応する処罰規定を表形式にまとめると，後掲資料（Excel 形式の表）のようになっており，まず，犯罪類型が定められ，犯罪類型毎に，被害額の大小等に応じて，軽罪又は重罪として処罰されることとされている。すなわち，1030 条は，複数の犯罪構成要件を準備すると同時に，犯罪被害の大きさに応じた刑罰を細かく区別して規定するものということができる。

条項毎に構成要件を説明する。

(1)　sec.1030 (a)(1)

a)無権限で又は授与されたアクセス権限を超過して，コンピュータにアクセスしたとの認識を持つこと

b)下記のいずれかについて入手したデータの保持の目的を有すること

i) 執行命令若しくは制定法の規定に従い合衆国政府によって国防若しくは外交関係上の理由で無権限の情報開示に対する保護すべきであると決定された情報

ii)1954 年原子力法 11 条 y 項に定義する禁止データ

c) 当該情報が合衆国の利益を侵害する目的で利用され又は外国に有利となるように意欲して通信する目的で利用され得るものであると信ずべき根拠を有すること

d)　意欲して，次のいずれかの行為をすること

i) 通信し，配付し，伝送すること

ii)通信され，配付され，伝送されるようにすること

iii)通信，配付，伝送を試みること

iv)それを受信する権限のない者に対して，配付され，伝送されるようにすること

v)受信権限を有する合衆国の吏員若しくは労働者に対して配達されるべきものを保留し，それが配達されないようにすること

(2) sec.1030 (a)(2)

a)意図して，無権限で又は授与されたアクセス権限を超過して，コンピュータにアクセスすること

b) それによって，以下のものを入手すること

i) 第 15 編第 1602 条第(n)項に定義する金融機関若しくはカード発行者の融資記録に含まれる情報，または，公正信用報告法(15 U.S.C. 1681 et seq.)で定義する用語の意味における消費者信用調査機関のファイルの中に含まれる情報

ii)合衆国の省庁若しくは政府機関からの情報

iii)行為の中に州際取引若しくは国際取引を含む場合には，保護されるコンピュータからの情報

(3)sec.1030 (a)(3)

a)意図して，合衆国の省庁若しくは政府機関の非公開コンピュータにアクセスする権限なしに，次のいずれかの行為をすること

i) 合衆国政府の利用のため省庁若しくは政府機関が排他的に利用するコンピュータにアクセスすること

ii)排他的な利用にかかるコンピュータでない場合には，合衆国政府により若しくは合衆国のために利用されるコンピュータにアクセスすること

b)その行為によって合衆国政府による利用もしくは合衆国政府のための利用に障害を発生させること

(4)sec.1030 (a)(4)

a)詐欺の対象及び入手するものがコンピュータ利用のみによって構成され，かつ，その１年間内の利用額が 5,000 ドルを超えない場合であること

b)無権限で又は授与されたアクセス権限を超過してなされること

c)故意に，詐欺の意図で，保護されるコンピュータにアクセスすること

d)そのような行為を手段として，意図した詐欺を実行し，何らかの有価物を入手すること[7]

(5)sec.1030 (a)(5)

a)次のいずれかの行為をすること

i) 故意に，プログラム，情報，コード若しくは命令の伝送を惹起させ，その行為の結果として，意図的に，無権限で，保護されるコンピュータに対し損害を発生させること

ii)意図的に，無権限で，保護されるコンピュータにアクセスし，その行為の結果として，不注意に損害を発生させること

iii)意図的に，無権限で，保護されるコンピュータにアクセスし，その行為の結果として，損害を発生させること

(6)sec.1030 (a)(6)

a)故意かつ意図的に，無権限でコンピュータにアクセスできるようにする目的を有すること

b)パスワードその他これに類する情報の（第 1029 条で定義する）詐欺的なトラフィックをすること[8]

c)次のいずれかであること

i) 当該トラフィックが州際取引若しくは国際取引に悪影響を及ぼす場合であること

ii)当該コンピュータが合衆国政府により若しくはそのために利用される場合であること

(7)sec.1030 (a)(7)

a)人，会社，組合，教育機関，金融機関，政府の組織その他の法人から金銭その他の有価物を不正取得する意図を有すること

b)州際取引若しくは国際取引において，保護されるコンピュータに損害を発生させる危険を含む通信を伝送すること

---

[7] 保護されるコンピュータに対する無権限アクセスを手段とする詐欺については，この条項により，別に一般の詐欺罪が成立する余地がなくなったことになると解される。

[8] 日本の不正アクセス禁止法における助長行為の禁止と類似する規定である。

第3項　メリッサ型ウイルスに対する対処等について

上記のとおり，1030 条は，一般に，すべてのタイプのウイルス犯罪について「無権限アクセス罪」の成立を成立可能とするものである。その中には，メリッサ型ウイルスも含まれると解されており，メリッサ型ウイルスの作者に対する訴追も同条によってなされ，有罪の答弁も同条違反の罪についてなされた。調査した範囲内では，この点について，特に異論はないようである。

なお，適用条文としては，実際に発生した結果及び損害の別に応じて，sec.1030 (a)(3), (5)ないし(7)のいずれかが適用可能と思われる。

今後，電子メールを利用したウイルス犯罪が増加するものと見込まれるが，この点は十分に留意すべきである。

第3節　アメリカ合衆国各州のウイルス犯罪対策立法

例えば、アメリカ合衆国各州のウイルス対策立法を比較検討した結果は次のとおりである。

第1項　犯罪成立要件のとらえ方

コンピュータ・ウイルスが機能・作用する場所の相違（BIOS レベルか，OS レベルか，アプリケーション・レベルか）を意識して犯罪類型の分別をする州制定法とそうでない州制定法とが存在する。

当然のことながら，コンピュータ・ウイルスが機能・作用する場所の相違を意識した立法例は，コンピュータ・ウイルスの定義規定を有する州制定法のみである。現在存在する州制定法のうち，何らかの形式によるコンピュータ・ウイルスの定義規定を持つかどうかで分類してみると，３つの立法スタイルに分類できる。

Ａ：独立犯罪タイプⅠ（定義規定あり）

コンピュータ・ウイルス（ワームを含む。）の定義規定を有し，これらの導入等の行為を処罰対象とするタイプの立法例である。

Ｂ：独立犯罪タイプⅡ（定義規定なし）

コンピュータ・ウイルス（ワームを含む。）の定義規定を有しないが，これらの存在を所与の前提として，又は，コンピュータ・ウイルスと同視可能な破壊的プログラム

の定義規定を設けることによって，その導入等の行為を処罰対象とするタイプの立法例である。

Ｃ：一般犯罪タイプ

不正アクセス行為の中の一類型としてコンピュータ・ウイルス等によるシステム破壊行為等を処罰対象とするタイプの立法例である。
このタイプの立法例では，「コンピュータ・ウイルス」による犯罪であることが重要なのではなく，コンピュータ・システムの破壊等の結果の発生又は結果発生の危険性を重視している。

第2項　コンピュータ・ウイルスが機能・作用する場所を意識した立法例

BIOS，OS 及びアプリケーションのいずれかを明示するか否かで分類し，表形式で示すと，次のとおりとなる。

	BIOS	OS	application	data	other resource
カリフォルニア州	△	○	○	○	○
メーン州[*1]	△	○	○	○	○
テキサス州[*2]	？	○	○	×	○[*3]

[凡例]

×：除外されている。

？：明確でない。

△：文言はないが，文脈から明示されていると読み取りできる。

○：明示されている。

[注記]

*1：コンピュータ・ウイルスの感染場所に限定

*2：コンピュータ・ウイルスの感染対象に限定

*3：メモリに限定

第3項　立法スタイルの相違に着目した個別的検討

独立犯罪タイプⅠの立法例の検討

A　カリフォルニア州刑法

カリフォルニア州刑法は，「コンピュータ汚染物質（*Computer contaminant*）」の定義の中で，コンピュータ・ウイルス及びワームがこれに含まれると規定している。

コンピュータ・ウイルス及びワームの要件は，次のとおりである。

a)自己増殖能力又は自己複製能力を有すること

b)コンピュータ命令であること

c)次のいずれかの結果を発生させ得るものであること

i) コンピュータ・プログラム又はデータ[9]の汚染

ii) コンピュータ・リソースの消費

iii)記録の改変又は破壊

iv)データ送信

v) コンピュータ・システム等の制御の奪取

d)一般にコンピュータ・ウイルス又はワームと呼ばれるものであること

同法でいうコンピュータ汚染物質とは，コンピュータ・システム等の中にある記録や送信情報を破壊するプログラムを指す。ただし，コンピュータ・ウイルス及びワームがこれに含まれるとはいえ，コンピュータ汚染物質それ自体については自己増殖能力を要件とするような限定がなく，通常のコンピュータ・ウイルスのような自己増殖機能や寄生機能を有しないコンピュータ・プログラムも含まれることになる。このことから，破壊機能を有するプログラムであれば，従来の分類によるコンピュータ・ウイルス又はワームに含まれない不正プログラムであっても同法によって対処することが可能である。

なお，コンピュータ・ウイルス及びワームの定義中には，コンピュータ・ウイルス又はワームによってもたらされる結果の一つとして「制御の奪取」が含まれているが，これは，トロージャン型のプログラムを含む趣旨と思われる。

この立法例は，コンピュータ・ウイルス及びワームの実質内容を定義規定の中に持ち込んだ上で，それよりも広い周辺的な不正プログラムをも処罰対象に取り込むために包括的な定義規定を構成した立法例であるということができる。アメリカ合衆国各種のウイルス対策立法の中では，最も包括的であり，かつ，適用範囲の広いものであると評価することができる。

同州の刑法では，権限なしになされるコンピュータ汚染物質の導入行為を処罰対象としている。したがって，結果の発生は犯罪の成立要件ではないが，結果を発生させた場合には刑の加重がなされる。

---

[9] 同州刑法においては，「データ」とは，情報，知識，事実，概念，コンピュータ・ソフトウェア，コンピュータ・プログラム又は命令の表現を意味する。

B　メーン州刑法

メーン州刑法は,「コンピュータ・ウイルス」の定義規定を有している。コンピュータ・ウイルスの要件は，次のとおりである。

a)命令，情報，データ又はプログラムであること

b)次のいずれかの結果をもたらし得るものであること

i) コンピュータ・システム等の能力の低下

ii) コンピュータ・システム等の使用不能

iii)コンピュータ・システムの損壊又は破壊

c)自らを他のコンピュータ資源[10]に感染させる能力を有すること

d)感染が次のいずれかの場合に発生すること

i) プログラム，データ又は命令が実行される場合

ii) リソース，データ又は命令の実行される中で他のイベントが実行される場合

この定義規定によると，感染能力を有しないプログラムは，コンピュータ・ウイルスとして扱われないことになる。

同州の刑法では，権限なしになされるコンピュータ・ウイルスの導入行為又はその導入を許容する行為を，コンピュータ・プライバシーの加重侵害罪として処罰対象としている。したがって，結果の発生は犯罪成立要件ではない。

C　テキサス州

テキサス州刑法は,「有害行為」の定義規定の中で「コンピュータ・ウイルスの導入」を例示し，さらに「コンピュータ・ウイルス」の定義規定を有している。コンピュータ・ウイルスの要件は，次のとおりである。

a)コンピュータ・プログラムその他の命令セットであること

b)メモリ，オペレーティング・システム又はプログラムの中に挿入されるものであること

c)自己複製能力を有するものであること

d)他のプログラム又はファイル内にその複製を感染させる能力を有するものであること

e)他のプログラム又はファイルに悪影響を及ぼすものであること

この定義規定によると，自己複製能力及び感染能力を有しないプログラムは, コンピュータ・ウイルスとして扱われないことになる。また，実害を発生させる可能性のないプログラムもコンピュータ・ウイルスとして扱われないことになる。

同州の刑法では，有害行為（コンピュータ・ウイルスの導入を含む。）の目的でなされる無権限アクセス行為を処罰対象としている。なお，実損害が発生した場合には，その損害額の総額の大きさに応じて刑が加重される。[11]

---

[10] メーン州の刑法においては，「コンピュータ資源（Computer resource）」とは，コンピュータ・プログラム，コンピュータ・ソフトウェア，コンピュータ・システム，コンピュータ・ネットワーク，コンピュータ情報，または，これらの組み合わせを意味する。

独立犯罪タイプⅡの立法例の検討

A　ノースカロライナ州

ノースカロライナ州の刑法には，無権限アクセス行為の中には「自己複製型プログラム」又は「自己増殖型プログラム」の導入行為が含まれるとの定義規定がある。

そして，これらのプログラムの導入することによってコンピュータ・システムが改変，毀損又は破壊する行為及び詐欺の目的でこれらのプログラムをコンピュータ・システムに導入する行為を処罰対象としている。

この定義規定によれば，自己増殖能力又は自己複製能力を有しないプログラムは，処罰に値する違法なコンピュータ・プログラムとしては扱われないことになり，かつ，コンピュータ・システム等の改変，毀損又は破壊の結果が生じない場合には犯罪が成立しない。

B　ネブラスカ州

ネブラスカ州の刑法には，自己複製型プログラムを「破壊的なコンピュータ・プログラム」の一例として例示する定義規定がある。

そして，無権限アクセスをした者が，コンピュータ・システム等を毀損又は破壊する目的で破壊的なコンピュータ・プログラムを配布する行為を処罰対象としている。

この定義規定によれば，この定義規定によれば，自己複製能力を有しないプログラムは，処罰に値する違法なコンピュータ・プログラムとしては扱われないことになる。

C　ミネソタ州

ネブラスカ州と同様である。

D　イリノイ州

次の要件を満たすプログラムを他のコンピュータ又はコンピュータ・プログラムに挿入する行為並びにその未遂行為をコンピュータ不正使用罪として処罰対象としている。

a) プログラムであること

b) 次のいずれかの結果をもたらすものであること

i) アクセスするコンピュータ又は他のコンピュータの毀損又は破

ii) アクセスの結果としての他のコンピュータのプログラム又はデータの削除，改変，移動（またはその可能性）

iii) アクセスするコンピュータのユーザ又はそのコンピュータにアクセスするためのコンピュータユーザにおける損害発生

c) b)の結果発生を認識しているか，又は，合理的に認識可能であったこと

---

[11] コンピュータ・ウイルスの事案ではないが，コンピュータ・システム内のコンピュータ。データの無権限削除について，Burlesson v. State, 802 S.W.2d 429(Tex. Ct. App. 1991)は，加重有害行為に該当するとしている。

一般犯罪タイプの立法例の検討

A　ペンシルバニア州

ペンシルバニア州の刑法は，コンピュータの違法使用行為を処罰対象としている。この違法使用行為の一種である無権限損壊行為の中には，コンピュータ・ウイルスによる損壊行為も含まれると解釈可能である。

B　フロリダ州

アメリカ合衆国内で最初にコンピュータ犯罪対策のための特別立法（1978 年）をしたことで有名な州である。

フロリダ州の刑法は，コンピュータ・システムへの正規ユーザのアクセスを妨害する行為を処罰対象としている。このアクセス妨害行為の中には，コンピュータ・ウイルスによるアクセス妨害行為も含まれると解釈可能である。

C　その他の州

コンピュータ無権限使用罪を持つ州では，一般に，コンピュータ無権限使用行為の中にコンピュータ・ウイルスの導入が含まれると解釈可能である。また，コンピュータ損壊罪を持つ州では，一般に，コンピュータ損壊行為の中にコンピュータ・ウイルスによる破壊行為等が含まれると解釈可能である。

但し，コンピュータ犯罪に関する書籍や論文等の中で，コンピュータ・ウイルスについての適用可能性の問題に触れているものは極めて少なく，判例も乏しい[12]。

(以上 第 2 章・第 1 節から第 3 節まで担当 明治大学・弁護士 夏井高人)

[12] コンピュータ・ウイルスの事案ではないが，ニューヨーク州の裁判所は，シャットダウン・コマンドの自動実行行為を違法行為であると判断している（people v. Versaggi, 83 N.Y.2d 123, 629 N.E.2d 1034(N.Y.1994)）。この判決を前提にすると，コンピュータ・システムに不正な命令を自動実行させるタイプのウイルスの導入も違法行為として処罰されるであろうと推測される。

第4節 アメリカ合衆国判例法にみるコンピューターウイルスへの対応

第1項 総説

訴訟の件数が我が国とは比べものにならないくらい多いアメリカ合衆国においても、悪意あるプログラムに関する判例は、刑事、民事ともに少ないということが特徴としてあげられるであろう。
刑事判例では、コンピュータ詐欺及び不正使用防止法が連邦規制の中心的規定となり、判例もかかる規制法の適否に関するものが多い。判例上争点となったのは、主に故意の対象がアクセスに限られるのか、その他の構成要件にも及ぶのかということである。この点、連邦裁判所は故意の対象がアクセスに限られることを明記している点が注目に値する。
なお、本報告の直接の対象ではないが、民事判例に関しては、不法行為法の適用の可否が判例上中心的争点として若干の判例があり資料において言及してある。不法行為法（州単位に制定されるものではあるが）は、悪意あるプログラムを様々な既存の請求原因に当てはめることで悪意あるプログラムによる損害に対する賠償請求を認めることに、消極的であるというわけではない。これらの請求原因の中には、過失（negligence)、ビジネス関係に対する故意の妨害行為（intentional interference with business relations）や conversion が含まれる。
連邦検察及び州検察もまた、害意あるコンピュータプログラムによって損害を生ぜしめた者に対して、今では珍しくなくなったコンピュータ犯罪規制を目的とする法律を使って、積極的に規制していこうという姿勢を示している。

第2項 刑事判例の検討

連邦政府も殆どの州政府も、害意あるコンピュータプログラムによる侵害行為を刑事犯罪としているが[13]、刑事判決の数は以下のように限られている。

[13] ダニエル・クルース著「コンピュータウイルスの脅威・近時刑事法典の調査」（ハムリン・ロー・レビュー13巻297号(Daniel J. Kluth, THE COMPUTER VIRUS THREAT: A SURVEY OF CURRENT CRIMINAL STATUTES, 13 Hamline L. Rev. 297）（１９９０年春刊）は、４９州の各コンピューター犯罪規制法を紹介している。

アメリカ合衆国対モリス（アメリカ合衆国連邦控訴審裁判所第二巡回区裁判所 1991 年）[14]

被告ロバート・タッパン・モリスは、コーネル大学のコンピュータサイエンスの博士過程の学生であった。1988 年 11 月、モリスは後に「インターネットワーム」として知られるようになるコンピュータプログラムの作成にとりかかり始めた。モリスはこのプログラムは相対的にはそれほど悪質なものではなく、単に自己増幅しインターネット（当時は殆どが大学、政府または軍のネットワークであった）に広がるだけと考えていた。モリスの主張によれば、プログラム作成の目的は、単に当時のコンピュータネットワークのセキュリティの問題性を示すだけであった。同年 11 月 2 日、モリスはそのプログラム（「ワーム」）を一台のコンピュータに送り込んだ。しかしながら、モリスはまもなくそのワームが国中のコンピュータに損害を与え、数多くの大学、軍や医療調査機関等のコンピュータをクラッシュさせていることに気が付いた。各損害は、２００ドルから５３、０００ドルの範囲であった。モリスは、18 U.S.C.1030(5)(A)条（コンピュータ詐欺及び不正使用防止法 1986 年）に基づき、起訴された。
同法は、以下の行為をした者は、いかなる者でも、犯罪を構成すると規定している。すなわち、

> 正当な権限なく、故意に、連邦政府と利害関係にあるコンピュータ(Federal interest computor)にアクセスし、かかる行為の一つ以上により、かかる連邦政府と利害関係にあるコンピュータの情報を改変し、損害を及ぼし、または破壊した者、もしくは、正当な権限をもってかかるコンピュータまたは情報へアクセスすることを妨害し、それによって一年以内に一人または複数の者に合計１０００ドル以上の損害を被らせる行為をした者[15]

訴訟においてモリスは、ワームの作成目的が単に当時のコンピュータネットワークのセキュリティの問題性を示すだけであって、損害等を生ぜしめる目的はなかったと主張し、検察側も争わなかった。そしてモリスは、上記「故意」は、上記規定の全ての構成要件につき存在しなければならないと主張した。連邦控訴審裁判所は、「故意に」という副詞は、「アクセスする」という言葉のみにかかるもので、同条項の他の構成要件にかかるものではない、と判示した。従って、アクセスすることの故意さえあれば、たとえ改変、破壊または損害を生ぜしめることにつき故意がなくても、同条の犯罪を構成する。
モリスには、３年間の保護観察処分（probation）、４００時間の地域奉仕活動（community service)、及び 10,500 ドルの罰金が科せられた。

なお、この判決については、資料編を参照のこと

---

[14] アメリカ合衆国対モリス（合衆国控訴審裁判所判例集第２編第９２８巻 504 ページ（控訴審第 2 巡回区裁判所１９９１年）（*United States v. Morris*, 928 F.2d 504 (2d Cir. 1991)）。

[15] 同条の英語原文は下記のとおりである。

> intentionally access a Federal interest computer without authorization, and by means of one or more instances of such conduct, alter, damage, or destroy information in any such Federal interest computer, or prevents authorized use of any such computer or information and thereby cause loss to one or more others of a value aggregating $1,000 or more in any one year period

アメリカ合衆国対サブラン （アメリカ合衆国連邦控訴審裁判所第九巡回区裁判所 1996 年）[16]

現状に不満を抱いていた銀行の元従業員であったサブランは、銀行のコンピュータシステムの数個の重要なファイルを削除し損壊したことを理由に、改訂前の当時の 18 U.S.C.1030(3)条に基づいて起訴された。サブランは銀行のコンピュータシステムにアクセスしたことは認めたが、ファイルを削除したのは故意ではないと主張した。モリス同様、サブランも、故意でファイルを削除し、ファイルに損害を生ぜしめ、またはファイルを改変したわけではないから、同犯罪の構成要件を満たさないと主張した。モリスにおけると同様、裁判所は、「故意に」は、コンピュータにアクセスするという構成要件にのみ適用される副詞であり、第二の構成要件である「コンピュータの改変、損壊、または損害を生じさせること」には適用されない、と判示した。
これに対し、サブランは、選択的主張として、18 U.S.C.1030(3)条は故意（scienter）の要件を欠き、mens rea を要件を欠くから憲法違反である旨主張した[17]。裁判所はかかる主張を斥け、最高裁判所の幾つかの判決で必要であるかのように示唆されているけれども[18]、故意（scienter）の要件は刑法規定に憲法上要求されている要件ではない、と判示した。合衆国連邦控訴審裁判所第九巡回区裁判所は、コンピュータにアクセスすることに対する悪意（wrongful intent）があれば、故意（scienter）の要件に関する合憲性をクリアするのに十分である旨判示した。

更にサブランは刑罰の不当性を争った。サブランの刑は、彼女が生ぜしめた損害額ゆえに引き上げられた。また、サブランは貧困であることを理由に不当利得(restitution)返還命令を受けることに異議を申し立てた。サブランの刑は維持され、控訴審裁判所はその時点での市場価値に基づき損害額の全額は科刑上考慮されなければならない旨判示した。サブランの科刑の詳細については明らかではないが、現在の連邦刑罰宣告ガイドライン(Federal Sentencing Guidelines)によれば、その刑は最低でも６ヶ月の収監と考えられる。

アメリカ合衆国対ツビンスキ （アメリカ合衆国連邦控訴審裁判所第一巡回区裁判所 1997 年）

ツビンスキは、ＩＲＳ（Internal Revenue Service）の職員として、無権限で知人のＩＲＳに関する秘密記録をブラウズしたことを理由に、改訂前の当時の 18 U.S.C.1030(3)条に基づき起訴され有罪判決を受けた。控訴審裁判所は、単なるデータのブラウジングでは同条で有罪にするには不十分であるとして、有罪判決を破棄した。すなわち、同条は、データを改変、損壊または破壊するか、あるいは何らかの価値のあるものを取得しない限り、同条を構成せず、単に

---

[16] アメリカ合衆国対サブラン（合衆国法律集第 3 編第９２巻 865 頁（合衆国控訴審第九巡回区裁判所 1996 年））（United States v. Sablan, 92 F.3d 865 (9th Cir. 1996)）

[17] アメリカ法上、犯罪が成立するためには、原則として客観的な actus reus (悪しき行為)と主観的な mens rea が存在していなければならない。何人もべつだんの定めがない限り、purpose(目的的故意)、knowledge(認識的故意)、recklessness（未必の故意ないし認識ある過失）または negligence(過失)により行為したのでなければ、罪を犯したものとされない（英米法辞典第 552 頁、編集代表田中英夫、東京大学出版会）。

[18] アメリカ合衆国対エクサイトメント・ビデオ（最高裁判例集第 115 巻４６４頁、１９９４年）（United States v. X-Citement Video, 115 S.Ct at 464 (1994) ）において、最高裁判所は、故意（scienter）の要件を規定していない制定法は、その合憲性につき憲法上重要な疑問がある（ “would raise serious constitutional doubts”）と判示した。

データを見るだけでは不十分と判示した。その後、同条は改訂され、ツビンスキの行為も刑法上犯罪とできるようになった[19]。

バウチャー対グリーンフィールド教育委員会　（アメリカ合衆国連邦控訴審裁判所第七巡回区裁判所 1998 年）

被告バウチャーは、当時高校生であったが、匿名で非公式な学校新聞に学校のコンピュータシステムにハックインするにはどうしたらいいかについて教える記事を書いた。事件が発覚した後、バウチャーは退学になった。バウチャーは、退学処分がアメリカ合衆国憲法及びウィスコンシン州憲法の規定する言論の自由を侵害するとして、退学処分の差止請求を申し立てた。地方裁判所はかかる請求を認めたが、控訴審裁判所はかかる原審判決を破棄した。
控訴審裁判所は、コンピュータシステムにハックインするにはどうしたらいいかについて教え、ハックインすることを奨励する記事が憲法上の言論の自由により保障されることにつき疑問を表明した。更に、控訴審裁判所は、バウチャーの記事がウィスコンシン州コンピュータ犯罪法上違法であると十分主張できると付言した。すなわち、同法は「権限なき者に、制限されているアクセスコードその他の制限されている情報を開示すること」が犯罪を構成する旨規定している[20]が、バウチャーの行為はこれに該当すると十分主張できると付言したのである。問題となっている記事のかかる違法の可能性に鑑み、控訴審裁判所は、差し止めを認めた原審判決が誤っている旨結論づけた。

人民対ロートン（カリフォルニア州控訴審裁判所　　）

被告ロートンは、コンピュータシステムに無権限でアクセスすることを禁止する州法に違反したとして有罪判決を受けた。ロートンは、公立図書館のデータベースをいじろうとして、公立図書館の一般利用者向けのコンピュータターミナルを利用した。ロートンは、カリフォルニア刑法５０２条（ｃ）（７）に基づき、起訴され有罪とされた。同条は、「故意に、そして許諾なく、あらゆるコンピュータ、コンピュータシステムまたはコンピュータネットワークにアクセスすること、またはアクセスする状況を作出すること」[21]が犯罪を構成すると規定する。同条の構成要件は、（１）許諾なく故意にアクセスすること、及びその対象が（２）コンピュータ、コンピュータシステム、またはコンピュータネットワーク、であること、といえる。
控訴審において、ロートンは、当該コンピュータが公立図書館で公衆に開放されていたものであることから、原審裁判所が許諾なくアクセスしたとして有罪にしたことは誤りである旨主張した。すなわちロートンは、当該コンピュータが公衆に開放されていたことから、彼にはアク

[19] 合衆国法律集第 18 巻 1030(a)(2)(B) 条（18 U.S.C. §1030(a)(2)(B)）は、アメリカ合衆国の行政部署や代理人からの許可なく、故意にコンピュータにアクセスして情報を入手する行為をすることを禁止している。
[20] ウィスコンシン州制定法第 943.70(2)条（Wis. Stat. §943.70(2)）。
[21] 人民対ロートン、カリフォルニア州判例集第 2 編第５６巻５２１頁(People v. Lawton, 56 Cal. Rptr.2d 521)。また、アメリカの判例を紹介する場合、通常は当事者名により、自然人の場合には姓のみを記載する。合衆国や州が当事者であるときは、United States というように記載する。州が当事者の場合には、州名のみを揚げるが、当事者である州と同じ州の裁判所に係属した事件の場合には、州名を掲げず、単位 ” State,” ”Commonwealth,” ”People”などとする。従ってここでも人民（People）とあるのは州が当事者であることを示す

セスに対する許諾があった、と主張したのである。控訴審裁判所は、同条を慎重に検討した結果、当該コンピュータがパブリックターミナルであったことから、かかる「コンピュータ」に許諾なくアクセスしたとはいえないが、当該コンピュータを利用して図書館のデータベースにアクセスすることには許諾がなかったとして、許諾なく「コンピュータネットワーク」にアクセスしたことを理由に有罪であると判示した。控訴審裁判所は、同犯罪の構成要件には、ハードウェアへのアクセスが許諾されている場合でもソフトウェアへのアクセスが許諾されていない場合には、これに該当すると判示した。ロートンの有罪判決は確定し、保護観察(probation)に処せられた。

バールソン対テキサス（テキサス州控訴審裁判所 1991 年）[22]

原告バールソンは、その雇用者であるテキサス州のブローカレッジハウス及び保険会社から１９８５年９月に解雇された。その後まもなく、元バールソンと一緒に働いていた従業員が、１６８０００件の会社のセールスコミッション記録がなくなっていることに気が付いた。その後、システム全体がクラッシュし、作動不能に陥った。バールソンの元の雇用者は、バールソンがコンピュータシステムに、無作為にメモリーを破壊し、新たな名前で自己増殖し、一ヶ月後に自動的に実行するプログラムをインストールしていたことを突き止めた。バールソンは、テキサス州刑法のコンピュータ不正使用防止法の①コンピュータまたはそのオペレーションに２５００ドル以上の損害を与えると重罪(felony)になる、②コンピュータを所有者の許諾なく無断使用すると軽罪(misdemeanor)になる、という規定に基づき、有罪とされた。裁判所はバールトンに１１８００ドルの罰金を科し、７年間の保護観察処分に付した。

(第 2 章　第 4 節　担当　弁護士　土井悦生)

第5節　メリッサ事件に対する刑事的対応

第1項　概説

メリッサ事件の概要は、本報告書の序でふれた通りであり、容疑者は、逮捕の上、司法取引によって有罪となった。その事件の経緯および司法取引における法律の適用は、アメリカ合衆国におけるがいいあるプログラムに対する刑事法的対応についてきわめて参考になるといえる。

[22] バールソン対テキサス、サウス･ウエスト判例集第 2 編第８２巻 429 頁(Burleson v. Texas, 082 S.W.2d 429 (Tex. App. 1991)

第2項 メリッサ事件についての事件の経過

ウィルスの発見から犯人逮捕までの流れ[23]

メリッサは電子メールを介してコンピュータのシステム内に侵入する。そのメールは、「Important Message From ***(***からの重要なメッセージ) 」というタイトルであり、”list.doc” という名の MS-Word のファイルが添附されている。本文には「Here is that document you asked for ... don't showanyone else, (頼まれていた資料です。他の人には見せないで下さい。) 」と記載されており，添附ファイル（要するにマクロウィルス）のダミー可視部分には 80 のポルノサイトのリストが添付されている。
それまでも MS-Word や Excel のマクロ機能を利用して感染するウィルスやワームは多く存在したが、Melissa は感染後、Outlook のアドレス帳に登録されている上位 50 人に対して、同じ感染メールを再配布するため、ねずみ算的に感染コンピュータが増えていく。その経緯は、以下のとおりである。

1999 年 3 月 26 日　最初の痕跡

ニュースグループ alt.sex.に最初にメリッサウィルス付きの記事が投稿される。

3 月 27 日　CERT[24]が警告を発する。

またさらに、FBI や NIPC(National Infrastructure Protection Center[25])といった公的な法執行機関がこの種の事態に対して警告を出したことも前例がないことである。

3 月 29 日　ワクチンソフトの提供

この日までには、ネットワークアソシエイツなどのアンチウィルスソフトベンダーがワクチンソフトを提供している。

4 月 1 日　容疑者逮捕

Davit L.Smith（ニュージャージ州アバディーン在住 当時 30 才）がこの件の容疑者として、兄弟宅にて FBI に逮捕された。

4 月 2 日　Smith 保釈

彼は、逮捕時及び逮捕後はわりと協力的だったようで、2 日朝には保釈されている。保釈金は 100,000 ドルであった。

4 月 8 日　ニュージャージー州モンマウス郡上級裁判所で初審判

---

[23] http://news.cnet.com/news/0-1005-200-340474.html?feed.cnetbriefs(米)
http://cnet.sphere.ne.jp/News/1999/Item/990330-3.html (日)
http://www.zdnet.com/news/products/9903/29nai.html などを参照のこと

[24] カーネギー・メロン　コンピュータ緊急対策チーム

[25] NIPC:全米インフラストラクチャー保護センターは 1998 年の米国政府サイトへの侵入（クラッキング）事件を機に FBI と司法省の合同で設置されたもので、ネットワークの中で広がっているウイルスへの「警告」と「調査」の二つの目的を持つ。

逮捕までの捜査の経緯と逮捕時点での法的論点

逮捕までの捜査の経緯

メリッサが最初に広まったのは、usenet 上のニュースグループ alt.sexで、米国時間 3 月 26 日の朝のことだとされる。当初、このウィルスは西ヨーロッパから発信されたと思われていたようである。alt.sex はこの種の情報を広めるにはまさに最適な場所と言える。このウィルスを広めようと思った者が、意図的にこの場所を選択した蓋然性はかなり高いであろう[26]。

alt.sex上には、まず AOL 経由で SkyRoket という ID を使って投稿されたとされる[27]。それ故、今後の捜査においても AOL の協力が重要な位置を示す。当初は捜査官も、その投稿した者がウィルスを作り出した犯人であろうと思った[28]。後に、その際に利用された ID は盗まれたものであることが後に判明する。web サイト上には、その際に使われた AOL のアカウントを持つ Steinmetz 氏なる人物の困惑のコメントも掲載されている[29]。そしてその後、捜査当局は VicodinES というハンドルネームを持つ、ウィルスライターに目をつけ、その行方の追跡を始めている[30]。Web 上のウィルス登録サイトにある、Shiver と Groovie2 というウィルスが Melissa と酷似しており、共通の GUID[31]を持つという理由である[32]。ただし今回の調査では、この VicodinES と、後に逮捕される容疑者が、果たして同一人物だったのかをはっきりと示した資料は見つけられなかった。いずれにせよ FBI はこの VicodinES がしばしば登場した Web サイトを捜査し、サーバを差し押さえ、サイトの閉鎖を命じている[33]。

Smith の逮捕が様々な機関の連携により成功したことがあらゆるところで大きく取り上げられている。捜査は、そのすべての過程においれ AOL の全面的な協力の下にすすめられた[34]。当初は FBI と NIPC によって始められ、やがて FBI ニューアーク地区支局のバックアップのもとニュージャージ州警察に受け継がれた。おそらくは、AOL の通信記録（アクセスログ）より容疑者の電話番号の割り出しに成功し、それが同州内からのものだと判明した時点で実質的な捜査が州警察に引き継がれたものと思われる。

逮捕時点での法的議論

アメリカの法律系の新聞（リーガルニューズペーパー）に最初にメリッサに関する記事が見受けられるのは、4 月 5 日の「New Jersey Law Journal」である。そこに”a federal-state task

---

[26] 後に逮捕される容疑者 Smith は拡散の意図を否定している。

[27] Chicago Daily Law Bulletin June 9, 1999, Wednesday

[28] Federal Human Resources Week May 31, 1999

[29] http://news.cnet.com/news/0-1005-200-340553.html?feed.cnetbriefs（米）
http://cnet.sphere.ne.jp/News/1999/Item/990331-2.html（日）

[30] LRP Publications Federal Human Resources Week May 31, 1999

[31] この事件の非常にスピーディーな犯人逮捕に、様々な機関の協力があったことは先に述べたが、その一方で、プライバシーへの懸念もささやかれている。今回、容疑者 Smith を特定できた陰には、Microsoft の Word によって文書生成時にバイナリデータとして埋め込まれた、GUID:Global Unique Identifier が利用された言われている。この GUID は MS-Word 一本一本事にことなり製品番号と一対一でリンクしている。そのためその文書を作成した MS-Word の所有者を特定することが可能だというのである。

[32] http://www.zdnet.co.jp/news/9904/01/louderback.html

[33] http://www.zdnet.co.jp/news/9904/01/melissa1.html

[34] Federal Human Resources Week (May 31, 1999)に「この協力なしに容疑者逮捕はありえなかったと、Rhodes(General Accounting Office's technical director for computers and telecommunications)が下院科学技術委員会で証言している。

force snares David Smith, an Aberdeen man suspected of originating the Melissa e-mail virus. “との記述がある。

最初の専門的な解説の記事は同じく 12 日の「New Jersey Law Journal」に見られる。
この記事では”Now, what do cyberlaw enforcers do with him?” （サイバー法施行者は、彼をどう処遇するか？）という書き出しで、Smith に対してどうのような犯罪を当てはめられるかについて論説している。本紙によれば、Smith の弁護士 Edward Borden Jr は”The virus does not delete any files, it doesn’t corrupt any files, it doesn’t format a hard drive, it doesn’t, on its own, do anything to harm a computer.”すなわち、「そのウイルスは、どのファイルも削除しない、どのファイルも破壊しない、ハードドライブをフォーマットしない、それ自身では、コンピュータを害する何もしない。」との弁護の発言をしている。

法廷は木曜日（記事の日付からするに 5 月 8 日のことか？）に、Smith に対して公共通信の中断（N.J.S.A.2C:17-3）と、コンピュータサービスへの窃盗・損壊、及び不法アクセス（N.J.S.A.2C：20-25 et seq.）の罪で召還手続きを行った。同時にその共謀罪についても責任を問うている。このことから、捜査当局も当初は、彼の単独犯なのかどうかを計りかねていたことが想像つく。

しかしながらこの件の適用はあまり先例がなく、同紙においても「コンピューター法弁護士とサイバー犯罪研究者は、そのケースがアメリカ合衆国の先例の薄い不足のため、遂行するのが難しいと言う。」との論説を乗せている。
そもそもニュージャージ州のこの法律は、コンピュータへの不法アクセスによって、物理的に作られた損害を懲らしめるために立法されたものだともされている。

モーリス事件以来、合衆国の連邦法及び州法は、外部から進入してデータを改竄することにも対応するように改められている。しかしながらその趣旨はあくまでデータの破壊とプライバシーの侵害に対する備えである。

本誌上のコメントとして、William Boni は、いくつかの興味深いコメントを載せている。すなわち、ニュージャージ州法もまた破壊とアクセスに焦点を当てたものであって、連邦法が 1988 年にモリスを起訴することができた悪意があるコードの規定を含まない、そしスミスがコンピュータ・システムを破壊したという証拠がなく、そして彼はパーツを破壊しなかったと。オーバーロードによるダウンに関しても、ニュージャージ法が物理的な破壊を念頭に置いているので適応が難しいとも言っている。

しかし、Michael Prigoff は、企業が応対しにくい金曜に配布に着手したことは、意図的なものだとしている。Boni 氏も意志があったであろうとしており、彼も、刑罰はそのために投資された才能や時間を考慮する必要があるとしている。

第3項 被害の実態

実際にどのよう機関で被害があったかの一例を抜検討すると、CERT によれば、3 月 29 日までには、Melissa ウィルスは 300 以上の組織の最低 100,000 台以上のコンピュータに届いたとある。45 分間で 32,000 部の Melissa を受けたサイトもあるという[35]。そして、多くの会社はそのウイルスを含むために彼らの電子メール・サービスをシャットダウンした。マイクロソフト社でさえ、一次的に社内メールのシステムを停止せざるをえなかったという報告もある[36]。また同様にメールシステムを停止したり、一部のサブシステムに Melissa が侵入した所として

インテル

[35] New York Law Journal July 13, 1999, Tuesday
[36] http://www.zdnet.co.jp/news/9903/27/melissa.html

ルーセント・テクノロジー
ロッキード・マーティン
デュポン
ハネウェル
ノースダコタ州政府
ＡＰ通信
コンパック

といった米国の大きな会社や公的機関の名前があげられる。

被害額算定及び請求の困難

まず実際の損害額を算出すること自体がかなり難しい。とくにメリッサの場合のはデータの破壊を行わないため、機械的な破損による算出ではなく、システムがダウンしたことによる影響額を算出せざるを得ない。また仮にそれが算出できたとしても、それが膨大が金額になることは用意に予想がつき、一介のコンピュータ少年（青年）に払える額ではとうていないからである。現実的には民事的な損害賠償は不可能であろう。

第4項 逮捕後の経緯－司法取引へ

Smith はまず、8 月の時点で自らが Melissa ウィルスを作り出したことを認めた。そして 12 月 8 日には 100 万のコンピュータ・システムに影響を及ぼして、8000 万ドルの損害を引き起こしたことを認め、司法取引に応じた。この司法取引のリリースを分析することによって、メリッサ事件に対するアメリカにおける刑罰法規の適用状況が明らかになる。

この司法取引の書類について、一般情報、司法取引の申し入れの書類、当時のプレスリリースを見つけることができる[37]。
司法取引の内容はおよそ次の二点である。
一つには、ニュージャージー地区連邦検察官による、Smith が自らメリッサを作り出し意図的にこれを配布したことを認める見返りとして、その他の訴因についてはこれを維持しないという申し入れであり、もう一点には、ニュージャージ州検察当局による、連邦と州の収監の刑期を並行して行うというものである。州法による刑期の方が連邦法より長いため（後述）、これによって Smith は州法による服役だけで済むことになると思われる。

[37] 司法省からのリリースとしては、
http://www.usdoj.gov/usao/nj/me1209_r.htm
http://www.usdoj.gov/criminal/cybercrime/meliinfo.htm
“Plea Agreement with David Smith” (http://www.usdoj.gov/criminal/cybercrime/meliplea.htm)があり、

また web 上のニュースサイトとしては
http://www.hotwired.co.jp/news/news/culture/story/3466.html などがある。

連邦からの被告人に対する司法取引の申し入れの書類によれば、被告 David Smith は、故意に、意図的に "Melissa virus"を送信し、その結果として、保護されたコンピューターに対し権限なしに損害を惹起したのであって、これは、連邦刑法の Title 18、Sections 1030(a)(5)(A) and 2. 違反である。 この連邦法違反により、Smith は最大で 5 年の服役と 25 万ドルの罰金が課せられる。

また同リリースによれば Smith は、ニュージャージ州法刑法典違反としては、N.J.S.A. 2C:20-25(a)及び 2C:20-26(a)に基づく、第 2 級コンピューター関連窃盗の訴因をも認めている。同州裁判所は、被告に対して同法違反に基づく最も長期の 10 年の服役を要求している。
前述のように.1030 条 (a)(5)(A)は、故意に，「 プログラム，情報，コード若しくは命令の伝送を惹起させ，その行為の結果として，意図的に，無権限で，保護されるコンピュータに対し損害を発生させること」を処罰しており、連邦法としてはかかる条文が、適用されたものと考えられる。

また、ニュージャージーの刑事法典 TITLE 2C の 2C:20-25 は、 Theft of Computer-related theft (コンピューター関連窃盗)を規定しており、かかる規定が適用されたものと考えられる。この条文は、

「 意図的に、もしくは故意に、権限なく以下の行為をする者は有罪である。

a. コンピューター、コンピューターシステムないしはコンピューターネットワークの内部ないしは外部に存在するデータ、データベース、コンピュータープログラム、コンピューターソフトウエアないしはコンピューター機器の変更、損壊、取得ないしは破壊をなす;

b. コンピューター、コンピューターシステムないしはコンピューターネットワークの変更、損壊、取得ないしは破壊をなす;

c. 詐欺のスキームを実行する、または、コンピューターの所有者からサービス、財産、または金銭を取得する目的で、コンピューター、コンピューターシステムないしはコンピューターネットワークにアクセスするまたはアクセスを試みる

d. 金融設備を変更、改竄、取得、傍受または破壊をなす」

2C:20-26
「75,000 ドル以上の財産またはサービス；犯罪の程度」

a. もし行為の結果、75,000 ドルかそれ以上の財産やサービスに対する改竄、損壊、破壊または搾取をともなうならば、セクション４以下の行為に基づく窃盗は第２級の犯罪を構成する。またもし行為の結果、公共の通信や、輸送や、水や、ガスやエネルギーの供給、その他の公益事業に実質的な中断や損傷を伴ったならば、それもまた第２級の犯罪である。

b. もし意図的にまたは故意に、75000 ドル以上の価値を持ついかなるデータ、データベース、コンピュータ、コンピュータ・プログラム、コンピュータ・ソフトウェア、コンピュータ・装

置、コンピュータ・システムそしてコンピュータ・ネットワークにアクセスし、意に介さない改竄、損壊、破壊を行い、あるいは搾取したならば、その人間は第３級の犯罪で有罪である

と定めており[38]、コンピュータ単体やデータ、ネットワークシステムの如何をとわず、いかなる電算機器に対しても直接的な損壊の観点から刑事的処罰を定めており、さらにはその行為の結果生じるライフラインへの影響にまで言及しており、かかる条文が適用された点は注目に値する。

(第 5 節担当 新潟大学 須川賢洋)

米国報告における参考資料・参考サイト

The National Information Infrastructure Protection Act of 1996 : Legislative Analysis by The Computer Crime and Intellectual Property Section; by United States Department of Justice

---

[38] 原文は以下のとおりである

N.J. Stat. @ 2C:20-25 (2000)

@ 2C:20-25. Computer-related theft

A person is guilty of theft if he purposely or knowingly and without authorization:

a. Alters, damages, takes or destroys any data, data base, computer program, computer software or computer equipment existing internally or externally to a computer, computer system or computer network;

b. Alters, damages, takes or destroys a computer, computer system or computer network;

c. Accesses or attempts to access any computer, computer system or computer network for the purpose of executing a scheme to defraud, or to obtain services, property, or money, from the owner of a computer or any third party; or

d. Alters, tampers with, obtains, intercepts, damages or destroys a financial instrument.

N.J. Stat. @ 2C:20-26 (2000)

@ 2C:20-26. Property or services of $75,000 or more; degree of crime

a. Theft under section 4 of this act constitutes a crime of the second degree if the offense results in the altering, damaging, destruction or obtaining of property or services with a value of $75,000.00 or more. It shall also be a crime of the second degree if the offense results in a substantial interruption or impairment of public communication, transportation, supply of water, gas or power, or other public service.

b. A person is guilty of a crime of the third degree if he purposely or knowingly accesses and recklessly alters, damages, destroys or obtains any data, data base, computer, computer program, computer software, computer equipment, computer system or computer network with a value of $75,000.00 or more.

<http://www.usdoj.gov/criminal/cybercrime/1030_anal.html>
The Electronic Frontier: The challenge of unlawful conduct involving the use of the Internet - A Report of the President's Working Group on Unlawful Conduct on the Internet; by United States Department of Justice
<http://www.usdoj.gov/criminal/cybercrime/unlawful.htm>
Common Fraud Crimes and Tips for Reducing Revictimization; by Kathryn M. Turman(Acting Director Office for Victims of Crime) & Chuck Wexler(Executive Director Police Executive Research Forum)
<http://www.ojp.usdoj.gov/ovc/infores/fraud/psvf/appendd.htm>
E-LAW 4: Computer Information Systems Law and System Operator Liability; by David J. Loundy
< http://www.Loundy.com/E-LAW/E-Law4-full.html#VII>
Computer Viruses: Making The Time Fit The Crime; by Joseph N. Froehlich, Edward M. Pinter and John J. Witmeyer III (Ford Marrin Esposito Witmeyer & Gleser, L.L.P.)
<http://www.fmew.com/archive/virus/>
Safety Issues at Cyberspace Law Bibliography of UCLA
<http://www.gseis.ucla.edu/iclp/bib5.html#Safety>

第3章　カナダ

-「カナダにおける『悪意あるプログラム』の法的規制に関する動向」-

第1節　　序　論

以下に述べるとおり、カナダではコンピュータに関連する不正行為への法的対応は刑法において一定限度は行われているものの、民事法・刑事法ともに、コンピュータ・ウィルスをはじめとした、悪意あるプログラムの配布等を正面から対象とした規定は存在しない。
したがって、こうした問題に対しては、既存の法律を適用することによって対応する他ない状態である。
また、現時点においては、悪意あるプログラムに関連する判例は公表されていない。
しかし、既存の立法を柔軟に解釈することにより、こうした悪意あるプログラムへの対応を裁判所が図る余地は十分にあるものと考えられている。
本報告は、オタワの GOWLING, STRATHY & HENDERSON 法律事務所にカナダ法に関する助言を求め、作成したものである。

第2節　　カナダ刑法典と悪意あるプログラム

カナダにおいて、日本の刑法典に相当するものは、カナダ刑法典（The Criminal Code of Canada）である。
カナダ刑法典は、カナダ司法省（The Department of Justice Canada）の Web サイト（http://www.leg.wa.gov/）において、その全文を閲覧することができる（http://canada.justice.gc.ca/FTP/EN/Laws/Chap/C/C-46.txt）。
カナダ刑法典には、「コンピュータ犯罪（Computer Crime）」に類する一般的な犯罪類型は規定されていない。まして、コンピュータ・ウィルスのような、悪意あるプログラムの配布等を正面から対象とした刑罰規定はなんら存在しない。
しかし、コンピュータ及びデータに関連したさまざまな不正行為は、刑法典に規定された各種の犯罪類型に該当した犯罪行為になり得るものと考えられている。
その中で、悪意あるプログラムの配布等に対応しうる可能性のある規定は、次の３つの規定である。

(1)　セクション 430(1)「損壊」（Mischief）

(2)　セクション 430(1.1)「データに関する損壊」（Mischief in relation to data）

(3)　　セクション 342.1(1)「コンピュータの無権限使用」（Unauthorized use of computer）

以下、これらの規定の内容について、項を改めて説明を加える。

第3節　「損壊」（Mischief）の罪について

第1項　従来の「損壊」（Mischief）の罪

(1)　　刑法典セクション 430(1)「損壊」（Mischief）

損壊の罪に関する定義は次のとおりである。
Section 430(1)
故意に次の損壊を犯した者（Every one commits mischief who wilfully）

(a)　　財産を破壊、又は損傷を与えること（destroys or damages property;）

(b)　　財産を、危険な状態にし、使い物にならなくし、不稼働にし、又は効果を失わせること（renders property dangerous, useless, inoperative or ineffective;）

(c)　　財産の権限ある使用、活用又は使用を、妨害、中断、あるいは干渉すること、もしくは（obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property; or）

(d)　　財産の権限ある使用、活用あるいは使用を行う者を妨害、中断、干渉すること（obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.）

(2)　　「損壊」（Mischief）に対する刑罰

「損壊」（Mischief）に対する刑罰は、刑法典セクション 430(2)以下で規定されている。
(i)刑法典セクション 430(2)により、損壊が生命に対する現実の危険性を惹き起こした場合には、終身刑を最高刑とする刑罰が科せられる。
（法　文）
Section 430(2) Every one who commits mischief that causes actual danger to life is guilty of an indictable offence and liable to imprisonment for life.
(ii)　　刑法典セクション 430(3)により、損壊が遺言に関する書類あるいは 5000 ドル以上の価値を有する財産に関する場合には、10 年以下の自由刑に処せられ又は、略式判決に処することができる。

（法　文）
Section 430(3) Every one who commits mischief in relation to property that is a testamentary instrument or the value of which exceeds five thousand dollars

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or

(b) is guilty of an offence punishable on summary conviction.

(iii) 刑法典セクション 430(4)では、その他の財産に関する損壊に対し、2 年以下の自由刑が科せられる。

（法　文）
Section 430(4) Every one who commits mischief in relation to property, other than property described in subsection (3),

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or

(b) is guilty of an offence punishable on summary conviction.

第2項　「データに関する損壊」（Mischief in relation to data）の罪について

本規定は、1985 年にカナダ議会が、コンピュータに関連した不正行為に対する刑法的対応を図るために新設した２つの規定のうちのひとつである。
日本でいえば、コンピュータ犯罪への対応を目的とした 1987 年の刑法一部改正に対応するものである。

(1) 刑法典セクション 430(1.1)「データに関する損壊」(Mischief in relation to data)

Section 430(1.1)
故意に次の損壊を犯した者（Every one commits mischief who wilfully）

(a) データの破壊又は改ざん（destroys or alters data;）

(b) データを無意味にし、使い物にならなくし、あるいは効用を失わせること（renders data meaningless, useless or ineffective;）

(c) データの権限ある使用を妨害、中断、又は干渉すること、もしくは（obstructs, interrupts or interferes with the lawful use of data; or）

(d) データを権限をもって使用する者を、妨害、中断、干渉し、又はアクセス権限ある者によるデータへのアクセスを拒否すること（obstructs,

interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.）

(2)　「データに関する損壊」（Mischief in relation to data）に対する刑罰

「データに関する損壊」（Mischief in relation to data）に対する刑罰として、刑法典セクション 430(5)において、10 年以下の自由刑が定められている。

（法　文）

Section 430(5) Every one who commits mischief in relation to data

(a)　is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or

(b)　is guilty of an offence punishable on summary conviction.

(3)　「データ」（data）の定義

本セクションにおける「データ」（data）の意味については、セクション 430(8)において、セクション 342.1.と同様の意味を有する（In this section, “data” has the same meaning as in section 342.1.）とされている。
セクション 342.1.の(2)(b)(ii)において、「データ」とは、「コンピュータシステムの使用に適した形式で用意される、又は用意された情報又はコンセプトを表現したもの」を意味するものとされている（”data” means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;）。
こうした「データ」には、コンピュータ・プログラムも含まれる。
すなわち、セクション 342.1.の(2)において、「『コンピュータ・プログラム』とは、コンピュータシステムを実行した時に、コンピュータシステムが機能を果たすようする指令あるいはステートメントを表現したデータを意味する。」（”computer program” means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;）と規定されている。
本規定は、「データ」に「コンピュータ・プログラム」が含まれることを逆説的に表している。
わが国では 1987 年の刑法一部改正によりコンピュータ犯罪への対処が図られた際、刑法 7 条の 2 において「電磁的記録」の定義規定が設けられた。すなわち、「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。」と定義されている。
これをカナダ刑法典セクション 342.1.の「データ」の定義と対比すると、「コンピュータ・プログラム」が含まれていないという点では日本法の方が狭い。
また、日本の刑法にいう「電磁的記録」とは、「一定の記録媒体の上に情報あるいはデータが記録、保存されている状態を表す概念」を指すと解されている（米澤慶治編『刑法等一部改正法の解説』（1988）91 頁）。したがって、送信中のものは含まれな

いと考えられている。この点、カナダ刑法典にいう「データ」に、送信中のものが含まれるか否か不明である。

(4) 日本法との対比

わが国で 1987 年に刑法が一部改正されたことは前述したがによりコンピュータ犯罪への対処が図られた。その際、電磁的記録不正作出及び供用罪（161 条の 2）、公正証書原本等不正作出罪（157 条）、電子計算機損壊等業務妨害罪（234 条の 2）、電子計算機使用詐欺罪（246 条の 2）、公用文書等毀棄罪（258 条）、私用文書等毀棄罪（259 条）といった一連の処罰規定が新設された。

このうち、電磁的記録不正作出罪というのは、「人の事務処理を誤らせる目的で、その事務処理の用に供する権利、義務又は事実証明に関する電磁的記録を不正に作った者は、五年以下の懲役又は五〇万円以下の罰金に処する。」（1 項）というものであり、「公務所又は公務員により作られるべき電磁的記録に係るときは、一〇年以下の懲役又は一〇〇万円以下の罰金に処する。」として、刑罰が加重されている（2 項）。

供用罪については、こうして作られた権利、義務又は事実証明に関する電磁的記録を、このような目的で、人の事務処理の用に供した者は、その電磁的記録を不正に作った者と同一の刑に処するとされている（3 項）。未遂も処罰される（4 項）。

こうしてみると、日本の電磁的記録不正作出罪に最も類似した犯罪類型としては、カナダ刑法典 Section 430(1.1)のうち、(a)「データの・・・改ざん」であると考えることができよう。

次に、日本の公用文書等毀棄罪は、「公務所の用に供する文書又は電磁的記録を毀棄」する罪であり、私用文書等毀棄罪は「権利又は義務に関する他人の・・・電磁的記録を毀棄」する罪である。

これらの罪に最も類似した犯罪類型を、カナダ刑法典 Section 430(1.1)から探すと、(a)「データの破壊・・・」、(b)「データを無意味にし、使い物にならなくし、あるいは効用を失わせること」ということになろう。

電子計算機損壊等業務妨害罪とは、「人の業務に使用する電子計算機・・・の用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害」する罪である。

これらの罪に最も類似した犯罪類型を、カナダ刑法典 Section 430(1.1)から探すと、(c)「データの権限ある使用を妨害、中断、又は干渉すること、」もしくは、(d)「データを権限をもって使用する者を、妨害、中断、干渉し、又はアクセス権限ある者によるデータへのアクセスを拒否すること」ということになろう。

第3項　国 対 Turner 事件

カナダにおいて、コンピュータにおけるデータに関する損壊に関し、公表されている唯一の判例は、国 対 Turner 事件（*R. v. Turner* (1984), 13 C.C.C. (3d) 430 (Ont. H.C.)）である。

しかし、本件は、刑法典セクション 430(1.1)「データに関する損壊」の罪が新設される前のケースであったので、セクション 430 が規定する一般的な「損壊」の罪が適用されている。

事案は、被告人が無権限で、米国に置かれていた磁気テープ上のデータを、電話回線を経由してアクセスして、データ所有者が適切に見ることができないような形に暗号化したというものである。
本判決によれば、本件における暗号化プロセスは次のとおりである（判決第４パラグラフ）。
すなわち、前記アクセスによって、テープ上に初めに記録されているものを読みとり、そしてその記録上の情報を取り出して、それを暗号化するという方法によるものであった。
暗号化プロセスは、テープ上に電磁的に保存されているデータを電子的に変更するものであり、テープそのものを物理的に変更するようなものではなかった。証言によれば、データそのものは破壊されなかったが、ダイアル・データ社によって使われていたプログラムがアクセスできないように、テープ上に保管されていた各々の記録中の電子的なキャラクター（コード）をずらすことによって暗号化されていた。
データは暗号化されたアルファベットを知っている者にはアクセス可能な状態で残るものの、米国の会社が使っていた元のプログラムを通じてアクセスしうるものではなくなっていた。
そうした暗号化の影響は、適当なカギ(key)があれば、データがアクセス可能な状態になるような効果をもったロック機能をもたらした。
証言によれば、ダイアル・データ社のソフトウエアも部分的に暗号化され、プログラムが適切なデータの上で動かなくなるようになっていたということである。
前述のとおり、本件は、セクション 430(1.1)ではなくセクション 430 の一般的な損壊条項について判決がなされたものである。
そこで本件では弁護人は、テープは何ら影響を受けていないから、刑法典に定義されているような不法な侵害をなされた（interfered）財産は何も無いと主張していた。
しかし、Gray 判事は、オンタリオ州上訴裁判所の国対 Stewart 判決に従い、データは秘密の情報であるから「財産（property）」みなすことができるとして、次のとおり判示した。
問題となっているのは、財産の活用への妨害であり、財産の物理的な変更ではない。
私は、博学の州法廷判事が正しく、損壊の論点についての拘留命令を破棄する用意はないとの結論に達した。
私は、サブセクション 385 及び 387(1)[現在のサブセクション 428 及び 430(1)]の文言に通常の普通の意味を与えるつもりである。
米国の会社が彼らの仕事を処理し、あるいは彼らのテープを使うことができないことは証拠上明らかである。
セクション 387(1)(d)[現在のセクション 430(1)(d)]によって、財産の物理的変更は犯罪行為の要素ではなくなった。
財産の活用を妨害することが犯罪行為の要件である。私は、セクション 387(1)[現在のセクション 430(1)]の文言に明確で曖昧さのない意味を与える。

第4項　「データに関する損壊」の罪に関する判例

カナダにおいて、コンピュータ・ウィルスをはじめとして、コンピュータ犯罪に関連した起訴が増加しつつあることは明らかである。
ところが、刑法典セクション 430(1.1)「データに関する損壊」の罪に関する判例につき、現在では公表されたものはない。したがって、この 430(1.1)に関し、裁判所がど

のような解釈を加えることになるのかについては、現時点では必ずしも明らかとはいえない。
しかしながら、前記 GOWLING, STRATHY & HENDERSON 法律事務所によれば、次のとおり、本テーマと関連した未公表の有益な判例が存在している。

(1) 国 対 Donald Lewis Orr 事件

本件は、会社に不満を持った従業員が、日附検索プログラム（date searching program）が、毎年 4 月 1 日と同じ、あるいはそれより大きな日附を検索したときに、コンピュータが、システムの使用を妨げるような別のプログラムを実行するようなプログラムを、会社のコンピュータシステムに入れたという事案である。
オンタリオの地方裁判所は、被告人を無罪とした（判決年月日未詳）。
その理由であるが、刑事法院（the Crown）が、被告人がコンピュータシステムにウィルスを植え付けた本人であると、合理的疑いを越えるまで証明することができなかったからであった。システムにアクセスしたことがある人が数多く存在しており、ウィルスを植え付けることが可能だったという事実は、この証明責任を著しく難しくしたのである。

(2) 国対 Dessureault 事件（1990 年 2 月 16 日）

やはり未公表のケースであるが、被告人 2 名が 22,000 ドルの公的資金を、家庭のホームコンピュータを使って、個人的な銀行口座に奪って入れたとして告発されたという事件である。
被告人のうち 1 名は、盗んだ金のうち 14,000 ドルを返還して、自分はもう一人の被告人である自分の男友達にそそのかされたのだと主張した。
ケベックの裁判所は、両名に 1 年に 1 日足りない自由刑を言い渡した。

第4節 コンピュータの無権限使用（Unauthorized Use of Computer）

前述した 1985 年の刑法典改正により新設された第 2 の刑罰規定は、コンピュータの無権限使用への対応を図ったセクション 342 である。
以下では、その主要部分を解説する。

第1項 セクション 342.1

セクション 342.1 においては、コンピュータの無権限使用に対する刑罰が規定されている。
Section 342.1 (1)
何びとも不正かつ権限なくして（Every one who, fraudulently and without colour of right,）

(a) いかなるコンピュータサービスを、直接的あるいは非直接的に、取得すること（obtains, directly or indirectly, any computer service, ）

(b) 電磁的、音響的、機械的又はその他の装置によって、コンピュータシステムの機能を、直接的あるいは非直接的に、傍受したり又は傍受されるようにすること（by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,）

(c) 第(a)項又は第(b)項又はデータあるいはコンピュータシステムに関連するセクション 430 に該る犯罪行為を犯す意図で、直接的あるいは非直接的に、コンピュータシステムを使用したり又は使用されるようにすること、もしくは（uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or）

(d) 他人が第(a)項、第(b)項又は第(c)項に規定される犯罪行為を犯すことができるようにコンピュータパスワードを使用したり、保有したり、取り引きしたり、あるいは他人がアクセスできるように許諾したりすること（uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)）

を行った場合には、起訴され、10 年以下の自由刑に処せられ、又は略式判決に処することができる（is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.）。

第2項　セクション 342.2

セクション 342.2 は、正当な免責事由なしに、セクション 342.1 の下での犯罪遂行に役立つような機器又は装置の作成、所有、販売又は供給を犯罪行為と規定している。

Section 342.2 (1)

主としてセクション 342.1 の犯罪行為の遂行に役立つよう設計された機器又は装置あるいはそれらの構成部分を、当該機器、装置又はそれらの構成部分が、上記セクションに背いて犯罪行為の遂行に使われるよう意図されていた、あるいは意図されている、又は意図されたと合理的な推論を招くような状況の下で、法的な正当事由又は免責事由なくして、作成、所有、販売、販売の申し出、もしくは供給をした者（Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section,）

(a) は２年以下の自由刑に処し、もしくは（is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or）

(b) 略式判決に処することができる（is guilty of an offence punishable on summary conviction.）。

第3項　悪意あるプログラムの配布等との関係

前記 GOWLING, STRATHY & HENDERSON 法律事務所によれば、こうした規定の下で、コンピュータ・ウィルスが問題となったケースは公表されていないが、ウィルス配布が、セクション 342.1(b)に沿って、「コンピュータシステムの機能を、直接的あるいは非直接的、傍受すること」と考えられ得ることは可能であるとしたうえ、近時の未公表判決であるが、ケベック州の法廷が、22 歳のセキュリティコンサルタントが複数の企業体のシステムに侵入しようとした行為とともに、いくつかのカナダ及び米国連邦政府のコンピュータに侵入(ハッキング) するために不正にコンピュータパスワードを使用した行為に、刑法典のこれらの規定を適用した。本法廷は、12 ヶ月のコミュニティサービスとあわせて 12 ヶ月の執行猶予の判決を言い渡したとしている。
上記事案は「不正アクセス」行為であり、悪意あるプログラムの配布等とは直接関係するものではない。したがって本稿の目的との関係では、適切なケースと言い難い。
しかし、「不正アクセス」のために「トロイの木馬」を侵入先コンピュータに埋め込むような行為は、この 342.1(b)によって対処することができる可能性があることは否定できないであろう。
むしろ©の類型には、「セクション 430 に該る犯罪行為（たとえば 430(1.1)の 「データに関する損壊」）を犯す意図で、直接的あるいは非直接的に、コンピュータシステムを使用したり又は使用されるようにすること」が含まれている。
これは、主として「不正アクセス」により他人の Web サイトのデータを改ざん・抹消するような行為への適用が想定されるる類型である。
しかし、これを字義どおりに解釈すれば、たとえば 430(1.1)の「データに関する損壊」の罪を犯す意図で、そうしたデータ損壊の機能を有するウイルスを、コンピュータを使用して配布する行為について、処罰の対象としうる可能性を有しているものと思われる。

第5節 民事責任

悪意あるプログラムの配布等によって発生した損害等について正面から定めた実定法は存在しない。
しかし、不法行為法をはじめとするコモンローが、民事的救済に役立ちうる可能性があるものと考えられている。
カナダ史を簡単に説明すると、1535 年５月、フランス人探検家ジャック・カルテイエが、西洋人で初めてカナダを訪れ、フランス統治時代を経て、英仏間における戦争の末、1759 年９月からイギリス統治時代が開始された。その後、1841 年、イギリスにおいて連合法が可決され「連合カナダ」が誕生し、1867 年７月１日、カナダ連邦が結成されている。ケベック州をはじめ、なおフランス文化圏を重視する州が存在している状況ではあるが、たとえば民事法をみるとコモンロー原理が適用されている。
もっとも、公表されたケースとしては、民事法分野においてコンピュータ・ウィルスが問題となった判例等は存在しない。

第6節　まとめ

カナダ法には、特に悪意あるプログラムの配布等に対応することを目的とした規定は存在しない。しかし、刑事法及び民事法の法原理は、こうした配布等の行為に適用しうる可能性を有している。
すなわち、刑事法においては、損壊の犯罪行為及び無権限使用はそうした配布等に対応することが可能である。
民事法においては、一般的なコモンローの法原理は、コンピュータウィルスの配布や他の発生してくるコンピュータの不正使用をカバーできるように拡張され、発展されていく必要があるものと考えられている。
(担当 弁護士 岡村久道)

第4章 フランス

-フランスにおける有害プログラムに対する刑事法的対応-

第1節 フランスにおけるネットワーク刑法

フランスでは、「不正情報処理に関する１９８８年１月５日の法律」により、いわゆるコンピュータ犯罪に対処するための規定が当時の旧ナポレオン刑法典中に挿入され、１９９２年７月に全面改正された新刑法典（１９９４年３月１日施行）の規定に受け継がれた。

フランスにおいて、コンピュータ・ウィルス等の有害プログラムに関する特別法は存在しないため、新刑法典のコンピュータ犯罪規定の一部によって、この問題に対処しようと考えられている。

第1項 不正情報処理に関する１９８８年１月５日の法律の制定

「不正情報処理に関する１９８８年１月５日の法律第１９号」は、フランスにおける最初のコンピュータ犯罪処罰立法であり、この法律によって当時の旧ナポレオン刑法典（１８１０年制定）第３部「重罪、軽罪及びその処罰」第２編「個人に対する重罪及び軽罪」中の第１章「人身に対する重罪及び軽罪」、第２章「財産に対する重罪及び軽罪」の次に第３章「情報に関する罪」として、コンピュータへの不正アクセス罪（第４６２条の２）、コンピュータ業務妨害罪（第４６２条の３）、データ不正操作罪（第４６２条の４）、コンピュータ・データ偽造罪（第４６２条の５）等が挿入された。

その後、ほとんどの規定が１９９２年７月に全面改正された新刑法典（１９９４年３月１日施行）の諸規定に受け継がれたが、コンピュータ・データ偽造罪のみは、文書偽造罪（フランス新刑法典第４４１－１条）の客体が「文書又はその他すべての思想表現手段」へと拡張されたことに伴い、削除された。

第2項　3つのハイテク基本犯罪類型

フランス新刑法典は、第３部「財産に対する重罪及び軽罪」（第１部「総則」、第２部「人に対する重罪及び軽罪」）第２編「財産に対するその他の侵害」（第１編「不法領得」）第３章「データの自動処理システムに対する侵害」（第１章「贓物隠匿及びその周辺の犯罪」、第２章「破壊、毀損及び毀棄」）の中に、以下の３つのハイテク犯罪基本類型を定めている。以下に、条文及び解説を掲げる。

第３２３‐１条〔不法アクセス等〕

第３２３‐１条〔不法アクセス等〕？不法に、コンピュータ（直訳はデータの自動処理システム、以下同様）の全体又は１部にアクセスし又は滞留する行為は、１年以下の拘禁刑又は１０万フラン以下の罰金で罰する。

？前項の行為により、システム中のデータの消去若しくは改変、又はシステムの動作の悪化が生じた場合、刑は２年以下の拘禁刑又は２０万フラン以下の罰金とする。

〔解説〕第 323-1 条１項にいう不法アクセスとは、故意に、権限なく、コンピュータの一部又は全部にアクセスする行為である。不正に入手したパスワードを使用してアクセスする場合が典型的な例である。

また、故意ではなく、偶然に、又は過失によって他人のコンピュータにアクセスしてしまった者が、ただちに接続を切断する代わりにそのアクセス状態を維持した場合は、不法滞留となる（一種の不作為犯と考えられている）。同様に、アクセスする権限のある者が権限の範囲を超えて不正にコンピュータを使用した場合も、不法滞留となる。

第 323-1 条２項は、不正アクセス又は滞留によって、データの消去若しくは改変、又はシステムの動作の悪化が生じた場合、すなわち、第 323-3 条データの不正操作罪及び第 323-2 条コンピュータ業務妨害罪と同じ結果が、故意ではなく、結果的に生じた場合を処罰する。

「権限なく」とは、管理者の意思に反するすべての行為を含む。

第３２３‐２条[コンピュータ業務妨害]

第３２３‐２条〔コンピュータ業務妨害〕コンピュータの動作を妨害し、又は不調にする行為は、３年以下の拘禁刑又は３０万フラン以下の罰金で罰する。

〔解説〕コンピュータの動作を妨害する（entraver）行為とは、コンピュータを麻痺させるなど、動作そのものを妨げる場合であり、不調にする(fausser)行為とは、動作を妨げるまでは行かないが、予定された動作をさせず、又は予定されていない動作をさせることによって、コンピュータを無益なものにさせることをいう。

第３２３‐３条〔データの不正操作〕

第３２３‐３条〔データの不正操作〕不法にコンピュータへデータを入力し、又は、そのシステムが収納するデータを不法に消去若しくは改変する
行為は、３年以下の拘禁刑又は３０万フラン以下の罰金で罰する。

〔解説〕データとは、事実、情報、概念を情報処理のための形態（電磁的記録）で表示するものや、コンピュータを作動させるプログラムを含む。

また、第３２３‐４条は、第３２３‐１条ないし第３２３‐３条に定める犯罪の１又は数個を準備することを目的として結成された団体又は成立した共謀に参加した者も、犯罪が実現された場合は各罪について定める刑又は最も重く罰せられる犯罪について定める刑で罰するとし、いわゆる共謀共同正犯のような概念を規定している。

第３２３‐５条は、５年以下の期間の公民権、私法上及び家族法上の権利の禁止、犯罪の遂行中又は遂行の機会になされていた公務執行又は職業活動若しくは社会活動の禁止、犯罪の実行に用いられた事業所の１若しくは数個又は全部の閉鎖、公契約からの排除、小切手振出しの禁止と、犯罪の実行に用いられ若しくは用いられようとした物又は犯罪から生じた物の没収、判決の掲示又は公告等の自然人に対する補充刑を定める。

第３２３‐６条第１項は法人の刑事責任を、同第２項は法人に対する刑、同第３項は法人に対する補充刑を定める。

第３２３‐７条は、第３２３‐１条ないし第３２３‐３条の未遂を既遂と同１の刑で罰することを規定する。これにより、例えばコンピュータ・ウィルスを作成したり、配布するような行為もコンピュータ業務妨害罪ないしデータの不正操作罪の未遂で処罰することが可能であると思われる。

第2節　その他の法律

.ハイテク犯罪は、政治的なサイバー・テロのような形態をとるとき、国家の存立に もかかわる深刻な被害をもたらし得る点が懸念されているが、フランス新刑法典では第４部「国民、国家及び公共の平和に対する重罪及び軽罪」の中に、ハイテク犯罪をも捕捉しうる特別規定を置いている。

すなわち、第１編「国民の基本的利益に対する侵害」第１章「大逆及び諜報」第３節「外国への情報の引渡し」（第１節「外国への領土の全部又は１部の引渡し、軍事力又は物資の引渡し」、第２節「外国との通謀」）の中に、第４１１‐６条情報の引渡し罪、第４１１‐７条情報の不正入手罪、第４１１‐８条情報の不正収集罪を設け、それぞれ「外国政府、外国に属し若しくは外国の支配下にある企業若しくは組織又はその要員に対して、情報、技法、物品、文書、情報処理データ又はファイルを引き渡し又はこれらを入手させる行為」、「外国政府、外国に属し若しくは外国の支配下にある企業若しくは組織又はその要員に引き渡す目的をもって、情報、技法、物品、文書、情報処理データ又はファイルを入手し又は収集する行為」、「外国政府、外国に属し若しくは外国の支配下にある企業若しくは組織又はその要員のために、装置、情報、技法、物品、文書、情報処理データ又はファイルを取得し又は引き渡す目的をもって活動する行為」が「それらの利用、漏洩又は収集が国民の基本的利益を害する性質を帯びる場合」に、前者を１５年以下の禁固又は１５０万フラン以下の罰金で、後２者を１０年以下の禁固又は１００万フラン以下の罰金で罰している。

さらに、第４節「サボタージュ」の中に、第４１１‐９条サボタージュ罪を規定し、「? すべての文書、物資、建築物、装備、設備、器具、技術的装置又はデータ自動処理システム若しくはファイルを破壊し若しくはその効用を害する行為、又はこれらに誤った情報をもたらす行為は、その行為が国民の基本的利益を害する性質を帯びる場合」、１５年以下の禁固又は１５０万フラン以下の罰金で罰し、「? 前項に掲げる行為が、外国政府、外国に属し若しくは外国の支配下にある企業若しくは組織の利益を図る目的で行われた場合」は、２０年以下の禁固又は２００万フラン以下の罰金で罰する。

また、第３章「国防に対するその他の侵害」（第２章「共和国の制度又は領土の完全性に対するその他の侵害」）第２節「国防の秘密に対する侵害」（第１節「軍隊の安全及び国防上の保護地帯に対する侵害」）中の第４１３‐９条国防の秘密罪の客体にも国防に関係する情報、技法、物品、文書のほかに、情報処理データ又はファイルを含めている。

第3節 有害プログラムによる攻撃と犯罪の成否

第1項　ハイテク犯罪の現状

有害プログラムによる攻撃の事例は、統計に現れるほど多くないため、参考までに、一般的なハイテク犯罪の現状を挙げれば、以下の通りである。

（１）フランスにおけるハイテク犯罪は、日本と同様、毎年増加の１途を辿っている。国家警察（Police Nationale）を統括する内務省と憲兵隊（Gendarmerie Nationale）を統括する防衛省が毎年発行している「フランスで認知された犯罪と非行」によれば、ハイテク犯罪を扱った刑事手続き数は、１９９３年に５８件、１９９４年に７２件、１９９５年に１４９件、１９９６年に１６１件、１９９７年には４２４件と急増している。

同書１９９５年版では、ハイテク犯罪を？コンピュータ・情報通信ネットワークを手段とする犯罪と、？コンピュータ・情報通信ネットワークが攻撃対象となる犯罪とに分類し、前者？に伝統的な経済犯罪（詐欺、背任、会社犯罪等）と不正な個人情報ファイルの作成による個人の自由に対する侵害罪（情報処理と自由に関する１９７８年１月６日の法律に規定）を含め、後者？にはソフトウェアの著作権侵害罪（Contrefaçon de logiciel＝１９９２年７月１日の法律に規定）やデータの信用や完全性に対する侵害罪（１９８８年１月５日の法律に規定）を含めている。また、行政機関や銀行、民間企業、大学や研究機関等、官民のすべての分野のコンピュータが狙われていると指摘し、ハイテク犯罪についてよく言われることであるが、被害者が信用を失うのを恐れ、また損害保険の請求にも被害届は必要でないため、被害を受けても警察に届け出ず、暗数はかなりの数に上るであろうと推測している。さらに、コンピュータや情報通信を利用した詐欺罪など伝統的な財産犯は、一般的に実務家により馴染みが深く刑罰も重い当該財産犯として分類されることが多いため、ハイテク犯罪処理件数が実際のハイテク犯罪数を正確に反映するものではないとしている。

１９９５年版ではハイテク犯罪として分類された犯罪のうち、１９％が著作権侵害罪、データの不正操作が１７％、個人の自由に対する侵害罪（１９７８年１月６日法違反）が３％、プログラムに関係する犯罪が２％でその他の５９％がいわゆるコンピュータ・スパイ（Piraterie informatique）と呼ばれるコンピュータへの不正アクセス罪等としている。さらに、その中でデータの改変を伴わない不正アクセスのみが６％、データの改変又は消去を伴ったものが５３％あったとしている。また、ハイテク犯罪全体の７７％は不正に利益を得ることを目的とし、１３％は単なるサボタージュを目的としていたという。被害額は、１９％が１００万フラン（２０００年２月現在で約１７００万円）以上であり、社会保障を扱う機関の手当て受領者のコンピュータ・データが改変され、１７００万フラン（同約２億９０００万円）が横領された事件などが紹介されている。

１９９７年版の統計では、４２４件のハイテク犯罪のうち、不正アクセス関係が８４％に上り、１２％の著作権侵害罪、２％の個人の自由に対する侵害罪、１％の電気通信法違反を大き

く引き離している。８４％の不正アクセスのうち、６８％はフランス・テレコムのテレホンカードの不正使用を含む電気通信をめぐる犯罪であるという。また、インターネットを使用した新たな犯罪も増加しているとし、児童買春に関する６事件や、殺人の脅迫を伴う２事件、違法な薬物の使用を呼びかけた１事件があったと紹介している。

１９９８年版では、全体数はわからず、不正アクセス関係が６４％、著作権侵害罪が１４％、個人の自由に対する侵害罪が２％、詐欺が１１％、その他が６％という割合のみが紹介されている。不正アクセスに関係する犯罪のうち、８１％が情報通信を不正に利用したものであり、１０％が単なる不正アクセスのみ、９％がデータの消去や改変、すなわちデータの自走処理システムの動作を妨害する行為であったとしている。またクレジットカードの不正使用と組み合わされたハイテク犯罪（サイバー・ポルノへの無権限アクセスやインターネット売買による商品の詐取等）や、インターネットを利用した児童売春や売春斡旋等の摘発事例が紹介されている。

（２）このようなハイテク犯罪への対応として、フランスでは「不正情報処理に関する１９８８年1月5日の法律第１９号」を中心として、「ソフトウェアの保護に関する１９８５年法(１９９２年7月１日法により改正された＝筆者注)」、「情報処理と自由に関する１９７８年法」を加え、包括的な立法を用意しており、１９９１年のヨーロッパ綱領の勧告にも先んじていると自負している。また、ハイテク犯罪捜査のための警察官の技術教育にも力を入れ、１９９４年には既に、中央司法警察局（Direction Centrale de la Police Judiciaire）の中に中央ハイテク犯罪処罰班（Brigade Centrale de Répression de la Criminalité Informatique）を設置している。

第2項　有害プログラムに関する判例

フランスにおける有害プログラムに関する判例で入手できたものは、以下の３件のみである。

パリ控訴院１９９４年3月１５日判決（論理爆弾によるコンピュータ業務妨害＝積極）

【事実の概要】　情報処理会社の幹部職員と会社員は、顧客の１人に請求書代金を支払わせるため、コンピュータ・システムに、システムの動作を麻痺させる論理爆弾（une bombe logique）を挿入した。
【判旨】　パリ控訴院は、幹部職員を旧刑法第４６２‐３条（新刑法第３２３‐２条）のコンピュータ業務妨害罪で、会社員を同罪の共犯として有罪とし、幹部職員に執行猶予付６月の拘禁刑、罰金５万フランを、会社員に罰金４０００フランを言渡したパリ大審裁判所の判決を支持し、控訴を棄却した。

パリ控訴院１９９５年3月１５日判決（フロド事件）

（コンピュータ・ウィルスによるコンピュータ業務妨害＝消極）

【事実の概要】　１９９１年4月１０日に発売されたコンピュータ関連雑誌「ソフト・ミクロ」の無料付録で、ヴェガというソフトウェアの試供版が記録されたフロッピーディスクが「フロド（Frodo)」と呼ばれるウィルス（利用者のファイルを次第に破壊してゆくもの）に感染しており、多数の被害者が出た（以来、「ソフト・ミクロ」誌は廃刊となってしまった)。ヴェガを製造したアルゴシエル社は、フロッピー複製会社に6万５千の複製を作るよう依頼し、その費用を下げるためにフロッピー複製会社の子会社ミルデータ社製ソフトウェアのカタログをフロッピーに挿入することを了承していた。

フロッピー複製会社及びミルデータ社の社長とフロッピーディスクの製造者が、それぞれ旧刑法第４６２-３条（新刑法第３２３‐２条）のコンピュータ業務妨害罪、第４６２‐４条（同第３２３‐３条）のデータ不正操作罪で起訴された。パリ軽罪裁判所１９９４年2月１０日判決は、２人の被告人にそれぞれデータの不正操作罪を適用し、共に執行猶予付２年の拘禁刑及び１０万フランの罰金刑を言渡した。被告人が控訴し、パリ控訴院は、次のように判示して２人の被告人に無罪を言渡した。

【判旨】　1)フロッピーディスクの製造者に対する旧刑法第４６２‐４条（同第３２３‐３条）のデータ不正操作罪について、被告人は証拠不充分で無罪とされるべきである。フロッピーの製造過程でウィルス感染が起こったという客観的証拠は全くない。ウィルス感染は、完成したフロッピーの試験段階やその後の他社での複製過程で起こった可能性もあり、正常なフロッピーをウィルスに感染したコンピュータに挿入したために感染が起こった可能性もある。

２）同様に、フロッピー複製会社及びミルデータ社の社長に対する旧刑法第４６２-３条（新刑法第３２３‐２条）のコンピュータ業務妨害罪についても、被告人は証拠不充分で無罪とされるべきである。被告人がフロッピー複製の過程で当該フロッピーがウィルス「フロド」に感染していることを知っており、多くの読者に配布されることを知りつつ雑誌に添付されるがままにしたという証拠はどこにもない。

破棄院刑事部１９９６年１２月１２日判決

（フロド事件の上告審、破棄差し戻し）

【事実の概要】フロド事件の上告審のため、同事件参照。パリ控訴院１９９５年3月１５日判決が２人の被告人に無罪を言渡したため、検察官が上告した。

【判旨】破棄院刑事部は、証拠調べが十分に尽くされていないとして原審を破棄し、パリ控訴院に審理を差し戻した。

第3項 ハイテク犯罪に関するその他の判例

（1）コンピュータ（ネットワーク）利用型犯罪

1.破棄院１９９０年１２月１２日判決（コンピュータの無権限使用（窃盗罪）＝消極）

【事実の概要】　被告人 F.T.は、ミニテル（１９８０年代末から１０年程フランス全土で普及していたコンピュータ網の端末＝筆者注）を権限なく使用し、電話料金を不正に利得して地域美容師協会に損失を与えた事実につき、窃盗罪で起訴された。原審であるレンヌ控訴院は、電話料金の不法利得は領得（appropriation）という概念になじまず、刑法第３７９条の物（chose）の範疇にも入らないとして、被告人を無罪としたため、検察官が上告した。

【判旨】　破棄院は、「電話料金の不法利得は領得という概念になじまず、刑法第３７９条の物の範疇にも入らない」としたレンヌ控訴院の判断は正しいとして、上告を棄却した。

2.パリ控訴院１９９２年１１月２５日判決（ソフトウェアの不正コピー＝窃盗については消極、著作権侵害罪については積極）

【事実の概要】　被告人 M.P.は、１９８９年5月３０日に、コンピュータ・ネットワークのサイト・リラ（Lilas）に侵入し、ボーラン社製ソフトウェア「ターボ C」の第２バージョンのデータを窃取した。被告人 M.L.は、M.P.によってなされた窃盗の共犯であり、さらに同年パリでボーラン社製の「スプリント１.５」というソフトウェアのデータを窃取した。被告人 M.A.は、M.L.によってなされた窃盗の共犯であった。被害者からの告訴　　により、３人は窃盗罪で起訴されたが、ボビニー大審裁判所は、３人に無罪を言渡したため、検察官が控訴した。パリ控訴院は、以下のように判示して、共に２千フランの罰金刑を言渡した。

【判旨】１）無形的データの移転は、そのデータにいかなる知的価値があろうとも、有体物の不法領得を要求する刑法第３７９条窃盗罪の客体とはならない。

２）ソフトウエアの媒体であるフロッピーの窃取を伴わないコンピュータ・データの移転は窃盗罪を構成しないが、刑法第４２５条の著作権侵害罪を構成する。

3.エクサン・プロヴァンス控訴院１９９６年１０月２３日判決（コンピュータ・システムへの不法アクセス＝積極）

【事実の概要】　被告人 J.-C.H.は、１９８２年以来、ニースの中央雇用センター電話部門の技術管理・監視を共同被告人 P.M.と担当していた。１９８９年初頭、当部門にミニテルが設置され、J.-C.H.は、プレイテルというサーバー・コンピュータ会社が接続時間に応じたポイントを集めて商品券を当てるキャンペーンを展開していることを知り、P.M.と共謀の上、１日中試用電話回線を通じてミニテルをプレイテルに接続し、その形跡を隠蔽する作業を行った。

以上の事実につき、J.-C.H.と P.M.は、１９８９年から１９９１年にかけてフランス・テレコムの電話回線を不法に使用した事実につき、旧刑法第３７９条、第３８１条、新刑法第３１１‐１条、３１１‐３条の窃盗罪で起訴された。ニース軽罪裁判所１９９６年1月３１日判決は、罪名を窃盗罪から旧刑法第４６２‐２条のコンピュータ・システムへの不法アクセス罪に変更し、被告人 J.-C.H.に執行猶予付６月の拘禁刑、P.M.に執行　　猶予付２月の拘禁刑を宣告し、被告人が控訴した。

【判旨】　エクサン・プロヴァンス控訴院は控訴を棄却すると共に、J.-C.H.に執行猶予付１０月の拘禁刑、P.M.に執行猶予付５月の拘禁刑を宣告した。

4.パリ軽罪裁判所１９９６年１１月５日判決（コンピュータ・システムへの不法滞留＝積極）

【事実の概要】　パリ裁判所、元老院、その他の各省庁のの電話回線設置及び管理を担当していたフランス・テレコムの社員は、某社のホームページへの接続時間に応じたポイント数（３５秒ごとに１ポイント）によって商品を獲得するキャンペーンに参加した。その際、フランス・テレコムが５分間コンピュータのディスプレイに変化がない場合は自動的に接続を遮断する事実に着目し、ハッカーの間で「ディスプレイの冷却（ rafraîchissement d'ecran）」と呼ばれる技術を使って、フランス・テレコムの課金装置を作動させずに接続を維持することにより、電話料金を不法に利得した。
【判旨】　パリ軽罪裁判所は、キャンペーンの３加者に刑法第３２３‐１条のコンピュータ・システムへの不法滞留罪を、ディスプレイの冷却を行うソフトウェアを企画した某プロバイダーの管理者に同第３２３‐２条のコンピュータ業務妨害罪を適用し、共に有罪を言渡した。

5.チオンヴィル軽罪裁判所１９９７年6月３日判決（コンピュータを利用した詐欺＝積極）

【事実の概要】 フランス領モーリシャス島の健康保険信用金庫の職員は､職場のコンピュータ・システム内に、金庫の資金を共犯者が管理する２つの会社に振り込ませるプログラムを開発して挿入し、１７００万フランを詐取した。正犯者、教唆者、不正なプログラムの開発者が組織的な詐欺罪（escroqurie en bande organisée）で起訴された。
【判旨】裁判所は、３人の被告人を組織的な詐欺罪で有罪とし、正犯者に５年、教唆者に４年、不正なプログラムの開発者に３年の拘禁刑を言渡した。

（２）コンピュータ（ネットワーク）関連型犯罪

1.破棄院刑事部１９９４年１月５日判決（データの不正操作＝積極）

【事実の概要】　情報処理サービス会社社員 A は、退職する直前、コンピュータに入力するためのデータを収集した手書きファイルの中にその会社の製品に対する消費税率に関する不正確な情報を追加し、その情報の一部を自分自身で会社のコンピュータの製品管理システム中に挿入したために、作成中であった当該システムの実施を遅らせた。
【判旨】　不正確なデータを故意にコンピュータ・システムの中に挿入する行為は、それが第３者に助けられた場合でも、データの不正操作罪(刑法第３２３‐３条)を構成する。上告棄却。

2.パリ控訴院１９９４年4月5日判決（コンピュータ・システムへの不法滞留＝積極）

【事実の概要】　情報通信会社社長、そのサーバー・コンピュータ・センターの管理者及び情報処理技術者は、多数のメールを多数人に集中的に送信することにより、競争会社のサーバー・コンピュータへ多くの接続を瞬時に殺到させて普通の人の接続を不可能にし、顧客が自社のサーバ ―・コンピュータへ接続するよう誘導した。被告人らは刑法第３２３‐１条のコンピュータ・システムへの不法滞留罪及びコンピュータ業務妨害　　罪で起訴された。パリ大審裁判所１９９３年1月２８日の有罪判決に対し被告人が控訴していたが、パリ控訴院は、次のように判示して控訴を棄却した。
【判旨】１）刑法第３２３‐１条にいう不法アクセスとは、コンピュータ・システムへのあらゆる不法な侵入をいい、同じコンピュータの別のシステムをすでに使用していたか、遠隔地から行ったか、電話回線へ接続したかなどの態様を問わない。
２）同様に、不注意からシステムに侵入してしまった者や当初は合法的にアクセスした者も、不法にシステム内に留まる場合は、不法滞留罪を構成する。
３）システムへの不法滞留罪が成立するためには、システムに何らかのセキュリティ装置が施されていることは必ずしも必要ではなく、当該システムの管理者が権利者のみにアクセスを制限する意思を表明していれば足りる。
４）アクセスが合法的な場合でも、行為者が１種の資格転位（interversion de titres）により当初の資格を奪われたときは、その後の滞留は不法なものとなる。

3.ポワティエ軽罪裁判所１９９７年6月２６日判決（コンピュータ業務妨害＝消極）

【事実の概要】　被告人 A は、P.L.F.社のコンピュータに PICK 言語の生産管理システムを導入するため、１９９３年8月１７日に雇用された。１９９５年１２月１１日、P.L.F.社は A が A のアシスタント G に研修をさせていないことを非難する手紙を送り、１９９６年1月１９日に急に出社を拒否された。
1月２９日、A は「情報へのアクセスを不能にするロックシステムや情報処理手続きの消去」を理由として解雇され、その後刑法第３２３‐２条のコンピュータ業務妨害罪で起訴された。ポワティエ軽罪裁判所は、以下のように判示して、被告人に無罪を言渡した。
【判旨】１）被告人 A が会社の要求に応じて設置したシステムの動作方法を他の社員に説明しなかったことは非難されるべきものではない。なぜなら、同社には当システムを使いこなす能力のある社員は A 以外におらず、その研修には１定の時間を要したにもかかわらず、彼は急に解雇されたからである。

２）A は、P.L.F.社のコンピュータ・システムにパスワードを施してロックすることにより故意にシステムを妨害したとは見られず、彼が開発したシステムを彼の後任社員が使いこなせるとも思われない。
３）たとえ、社員が作成した情報処理システムが彼の退職後も会社の財産として残るとしても、それは使いこなされる必要がある。
４）それゆえ、本質的に知的レヴェルに属し、その保存については極端に不安定なこの知的財産の移転のために時間と有能な話し相手を見つけられないまま突然解雇された会社員に罪を負わすことはできない。

第4節　検討

以上、適用可能な条文と少数の判例を概観していえることは、フランスにおける有害プログラムに対処するための中心規定は、コンピュータ業務妨害罪（フランス刑法典第 323-2 条）及びデータ不正操作罪（同第 323-3 条）であるということである。
しかし、実際には、判例に見られるように、立証の困難性からフランスで有罪とされた例はまだない。
コンピュータ業務妨害罪に関しては、旧刑法第４６２条の３が「故意に、かつ第３者の権利を害して、記録の自動処理システムの運行機能を阻害し、または破壊した者」を処罰していたのに対し、新刑法第３２３‐２条は「コンピュータの動作を妨害し、又は不調にする行為」とのみ規定し、日本の電子計算機損壊等業務妨害罪（刑法第２３４条の）のように行為態様の限定もないため、実質的に処罰範囲を拡張している。また、故意犯のみならず、それが不法アクセスの結果である場合は、過失犯も処罰される（第３２３‐１条第２項）。
ただし、上記解説でも述べたように、コンピュータの動作妨害とは、コンピュータを麻痺させるなど、動作そのものを妨げる場合であり、不調とは、動作を妨げるまでは行かないが、予定された動作をさせず、又は予定されていない動作をさせることによって、コンピュータを無益なものにさせることをいうとされているので、規定の解釈に当たっては、かなり重大な結果が考えられているようであり、単なる愉快犯的なコンピュータ・ウイルスの配布行為のみでは、当該条文での処罰は不可能であるように思われる。
これに対し、データ不正操作罪におけるデータにはプログラムを含むとされているので、コンピュータ・ウイルスの配布もデータの不正操作に当たる可能性があるが、法定刑が３年以下の拘禁刑又は３０万フラン以下の罰金でコンピュータ業務妨害罪より重いので、前者に当たらない行為をより重いデータ不正操作罪で処罰できるのかという疑問も出てくる。
さらに、単なるメールの複製は、コンピュータ業務妨害罪にもデータ不正操作罪にも当たらないが、不正アクセス罪（フランス刑法典第 323-1 条）は、管理者の意思に反したすべての行為を含むため、同罪に当たる可能性が出てくる。
日本でも、放送会社がインターネット利用者に提供するために開設した天気予報画像を消去しわいせつな画像に置き換えた行為につき、電子計算機損壊等業務妨害罪（およびわいせつ図画公然陳列罪）に当たるとした判例があるが、大量のコンピュータ・ウィルスを会社のコンピュータに送りつけた男が威力業務妨害罪の容疑で逮捕されたという。今後、日仏両国の判例の動向が注目されよう。
ただし、日本の電子計算機損壊等業務妨害罪には未遂規定が無いため、コンピュータ・ウィルスの作成者と配布者が異なる場合の作成者は処罰できないが、フランスのコンピュータ業務

妨害罪には、他のすべてのハイテク犯罪と同様、未遂も共謀共同正犯も処罰されるため、かなり広範囲の処罰が可能となっている。
　結局、フランスでは、日本に比べてかなり規定も包括的で、運用によって非常に広範囲の処罰が可能となる点が特徴的であるといえよう。
(担当　亜細亜大学講師　　島岡まな)

第5章　英国

-コンピューター不正利用法 1990 とコンピューターウイルス-

第1節　序

コンピューターウイルス等の有害プログラムによるネットワーク社会の混乱については、この報告書の序章でふれたとおりである。そして、本稿では、その調査の一環として、英国における有害プログラムをめぐる問題点について、検討する。後述するように、英国ではコンピューターウイルスをめぐる事件が何件か報告されており、それらの事案を検討することは重要である。本稿では、コンピューター不正利用法 1990 の制定について簡単に紹介するとともに、セクション 1 および第 3 条の解釈について触れることにする。そして、バード&バード事務所のレポートを参考にしながら、個別のケースについて紹介していくことにする。

第2節　英国のコンピューター・不正利用法 1990 の制定

第1項　不正利用法の導入-Dr Popp 事件

コンピューター不正利用法が導入される前に、いわゆる「トロイの木馬」に関する事件として Dr.Popp 事件を紹介しておくことは有意義である。これは、1989 年に、39 才の Dr Popp という男が、「トロイの木馬」をしかけて、世界中で、パーソナルコンピューターのユーザーを脅迫した事件である。ロンドンの 2 万人にニセのフロッピーを送り、彼は、エイズ・ウイルスにかかるリスクを評価するプログラムを含んでいたとするが、そのフロッピーは、実際には、ユーザーのコンピューターに「トロイの木馬」を導入する手段にすぎなかったのである。このプログラムは、ユーザーが 100 回コンピューターを利用すると、発病するようになっており、パナマの銀行口座に 225 ポントを送金しないと、コンピューターは機能を停止すると警告されたのである。Dr Popp は、英国に引き渡しがなされたが、彼の精神状態が原因で、公判までにはいたらなかった。

この事件は、現在、起きたとすれば、第 3 条の犯罪と考えられている[39]。

第2項 コンピューターの不正利用の考察

コンピューターの不正利用 (不当利用)による被害についての議論がおこなわれるようになり、スコットランド法律委員会が 1987 年にレポート[40]をだし、また、英国の法律委員会は、ワーキングペーパー[41]において不正利用を

A コンピューター詐欺

B コンピューターに対する無権限アクセスの確保

C データないしはソフトウエアの無権限による変更ないしは消去

D データないしはソフトウエアの無権限のコピー

E データ保護法 1984 により保護される情報の利用

とにわけて論じたこと、およびその内容については、別稿[42]を参照されたい。このワーキングペーパーなどを前提に、コンピューターの不正利用に対する立法を進めるべきとするレポート(以下、法律委員会報告書という)が議会に提出された[43]。このレポートにおいては、コンピューター・ウイルスなどについてさらに詳細な検討がなされることとなった。その報告書は、

パート 1 導入

パート 2 新たな犯罪の必要性

パート 3 新たな犯罪の要件

パート 4 管轄、証拠、手続き

パート 5 要約

という構成からなっている。

その報告書における有害プログラムに関する部分の論述を取り上げると以下のようになる。

そのパート 1 の C 事実的背景によれば、指令の変更ないしは、プログラム変更による不当使用のみでなく「基本システム(ないしは実際の情報システム)は、また、ウィルスやワームなどの導入による攻撃に対してきわめて脆弱である。私たちは、これらの用語を技術的に用いるわけではないが、自分自身を複製する無権限プログラムを述べるのに一般的で便利な表現である。そのようなプログラムは、コンピューターシステムの能力を使い切ってしまい、また、適切なプログラムまたはファイル(もしくはその双方)を変更ないし削除してしまう。」と表現されている(同 1・17)。そして、「直接的な消去にせよ、ウイルスの接種にせよ、コンピューター内の情報の破壊は、深刻な結果を伴ってしまう。」としているのである。

このような事実認識をもとに、パート 2 では、新たな犯罪の導入の必要性が論じられている。その必要性についての部分は以下の通りである。

---

[39] Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses! (http://webjcli.ncl.ac.uk/1996/issue3/akdeniz3.html)

[40] Scottish Law Commission,"Report on Computer Crime"SLC No.106(1987)(Cm 174,1987)

[41] Law Commission "Computer Misuse" Working Paper No.110 (1988)

[42] 拙稿 「コンピューターの無権限アクセスの法的覚書-英国・コンピューター不正利用法 1990 の示唆」判例タイムズ 1006 号(95 頁)

[43] The Law Commision (LAW COM. NO.186) "Criminal Law Computer Misuse" Cm 819 HMSO 1989

コンピューター内部のデータ・プログラムの消去や改変などに対応する従来の制定法は、刑事的タメージ法 1971 であり、その第 1 条は、

「適法な理由もなく他人に属する「財産(property)」を、破壊、損害を与える意図をもって、もしくは、破壊されるないしは損害を加えられることを省みないで、破壊もしくは損害を加えた者は犯罪である」

と定めている。

この「損害を加える(damage)」という用語は、広く解されていた。財産の価値ないし利便性を害う障害すべてを含むものと解されており、データやプログラムの保存されているデバイスに対する損害を与える行為をカバーするものと考えられていた。しかしながら、このような解釈自体は当然であるとしても、英国においては、コンピューター不正利用法 1990 制定過程の議論において、制定法による「明確化」が、必要とされると考えられた。報告書の 2・28 によると「データの無権限改変および動作コンピューターの再プログラミングが、刑事罰化されるべきであるのは、当然のものとして真剣に疑問にされなかった。それは、私たちの顧問たちの見解であり、私達それは正しいとかんがえている。データの無権限での変更ないしは消去は、法律による正当化事由のない場合、なにも社会的に価値のないものである。他人の財産に対する故意の妨害であるし、単に財産に対する侵入だけではなく、情報をみつめるだけでもない。それは、(略)実際の損失をもたらし、基本システムの場合には、物理的な危険をもつのである。」と述べている。

そして、 従来の解釈との関係については、

1)刑事的タメージ法 1971 における「財産」とは、有体物をいうとしている。Cox v Riley 事件(1986)83 Cr App Rep54 は、プラスティックの回路カードに保存されていたコンピュータープログラムを消去した事件である。しかしながら、プログラム自体は、有体物ではない。それゆえに犯罪は成立しないということになりそうであったが、それが回路カードに保存されていたために、そのカードがダメージを受けたとして法律の適用が可能であり、現に被告人は、そのような観点から有罪とされた。しかしながら、電気的パルスの手段によって保存されている場合、どの有体物であるかを特定しなければならず、法律の適用において、不確実性を増やすことになる。

2)Cox v Riley 事件においては、Fisher 事件の分析と類似しており、この事件は、以前の悪意ダメージ法 1861 の「破壊もしくは効用を無にするダメージ」という用語の解釈に関して「効用を無にする」という要件を「ダメージ」とは別の要件として認めたものと解される余地があったものである。有体物になんらの物理的損傷を与えないときにもダメージは起きるという見解は、1971 年法による法の廃止の後も生き延びているかどうか完全には明確ではないことになる。 Cox v Riley 事件(そして、未報告の Henderson and Battley 事件も)は、正面から、辞書の「ダメージを与える」という定義が、物に対して損傷を与えるということを指摘していないのであり、これが問題である。その結果、これらの判例は、現在の法の「ダメージ」の意味についての十分な判例とはしがたい。

3)また、このような理論的な困難さと同様に、裁判官、マジストレート、陪審員に事実が、現在の刑事的ダメージの現行法に適合することを説明するのに、たびたび困難を感じるということがある。

4)また、刑事法 1977 は、刑事審理の様式を刑事的タメージの損害が 2000 ポンド以下の場合には、簡易審理により治安判事が進めることになることを定めている。実際には、データおよびプログラムのダメージは、その評価が困難である。そして、このことは、刑事的タメージ法の改正では、十分に対応しきれないのである。

という点があると考察している。

これらの考察の結果、報告書は
「いずれの見解によっても、不法にデータを改変し、消去したものに対する処罰が、現在では、不明確であり、その程度は、容認しがたいものである。しかしながら、データのそのような改変ないし消去を刑罰化することを明らかにすることは、そのような行動が、刑事的ではないということを前提としてしまう。そのような結論が許容し得ないのは明らかである。それゆえに、データおよびプログラムの改変および消去が、コンピューターの動作ないしは、データの信頼性を損なう意図によりなされるときには、刑事的犯罪とされるべきである」として、5 年以下の懲役を課す犯罪として、正式および簡略の両方の審理ができるように推奨しているのである。この明確化の方法としては、刑事的ダメージ法の改正により「財産」について「データ」と「プログラム」を含むとする方法も考えられることになる。しかしながら、このアプローチは、

1)刑事的ダメージ法が有体物についての定しかおいていないこと

2)上述の簡易審理しかない刑事法 1987 の規定との関係

3)刑事的ダメージ法が、故意のある場合と無謀な場合とに対して、意図的な場合のみをカバーするものでなければならないこと。

などの観点から、新しい刑罰を定めることとなったのである。

第3節　不正利用法の構成

第1項　不正利用法の制定

これらの考察をもとに英国は、1990 年 6 月 29 日、コンピューター・不正利用法 1990 を制定する。
その条項の構成は、

コンピューター・不正利用犯罪（Computer misuse offences）

1. コンピューターに対する無権限アクセス（Unauthorised access to computer material.）
2. さらなる犯罪の意図を有するコンピューターに対する無権限アクセス（ Unauthorised access with intent to commit or facilitate commission of further offences.）
3. コンピューターに対する無権限改変（ Unauthorised modification of computer material. ）

管轄（Jurisdiction）

4. この法律における地域的観点（Territorial scope of offences under this Act.）
5. 国内管轄との重要な関連性（Significant links with domestic jurisdiction.）
6. 本法律における 未遂行為の地域的関連（Territorial scope of inchoate offences related to offences under this Act.）
7. 本法律に関連する外国法律の 未遂行為の地域的関連（ Territorial scope of inchoate offences related to offences under external law corresponding to offences under this Act.）
8. 外国法律の関連性（Relevance of external law.）
9. 英国国籍の無関係（British citizenship immaterial.）

諸規定および一般(Miscellaneous and general)

10. 法執行機関の留保(Saving for certain law enforcement powers)
11. セクション 1 の犯罪に対する手続き(Proceedings for offences under section 1)
12. セクション 2 ないし 3 の手続きにおけるセクション 1 の犯罪の宣告(Conviction of an offence under section 1 in proceedings for an offence under section 2 or 3.)
13. スッコトランドの手続き(Proceedings in Scotland.)
14. セクション 1 犯罪の捜査令状(Search warrants for offences under section 1.)
15. 犯罪人引き渡し法 1989 スケジュール 1 の適用される引き渡し(Extradition where Schedule 1 to the Extradition Act 1989 applies.)
16. 北アイルランドへの適用(Application to Northern Ireland)
17. 解釈(Interpretation.)
18. 引用、施行その他(Citation, commencement etc.)

となっている[44]。

第2項　不正利用のタイプ

一般に上記の法律は、コンピューターの不正利用についての新しい処罰規定をさだめるものとされており、そこで導入された不正利用には、3 つのタイプがあると
いう。具体的には、

[44] http://www.hmso.gov.uk/acts/summary/01990018.htm

1 「ハッキング」すなわち、無権限アクセス(第 1 条犯罪)

これは、物理的ないしは電気的に権限のない人間(a person without authority physically or electronically) が、コンピューターシステムに「侵入(penetrates)-(広義)」することである。
ここでは、鍵を壊して、侵入することに比較され、さらなる犯罪は意図されていないのである。

2「深刻な無権限アクセス」(more serious form of unauthorised access)(第 2 条犯罪)

これは、権限を有しない人が、窃盗などのさらなる目的をもってコンピューターにアクセスすることである。なお、このさらなる目的は、コンピューターを利用するもので
あるとないとを問わない。

3 デジタル犯罪(第 3 条 犯罪)

これは、デジタル情報を破壊する、ないしは、デジタル情報へのアクセスを損なう行為である。
ありふれた例としては、コンピューター・ウイルスがある。
とされている。
有害プログラムに対する検討に際しては、第 1 条の適用も問題となるので、その要件についても検討することにする。

第3項　第 1 条の構成要件

構成要件

不正利用法 1990 の第 1 条は、以下のように定めている。
1 （1）A person is guilty of an offence if -(次の行為を行った者は、有責である。)
（a）he access a computer to perform any function with intentto secure access to any program or data held in any computer;(コンピュータに蓄積されたプログラム又はデータにアクセスする意図をもってコンピュータを作動させること)
（b）the access he intends to secure is unauthorised ;and (そのアクセスが無権限であること)
（c）he knows at the time when he causes the computer to perform the function that that is the case(コンピュータを作動させる時点において、アクセスが無権限であることを知っていること)
(なお、訳は警察白書 98 37 ページの訳による)
となっている。

客観的要件

ここでは、「何がコンピューターの作動させるのに必要となるか」と「プログラム又はデータにアクセスする」とはなにかが問題になるのである。詳細については、別稿(前出の脚注 41)を参照されたい。

主観的要件-意図(mens rea)

検察側は、2 つの点を証明しなければならない。1 つは、「コンピューター」の「プログラムないしはデータ」にアクセスしようとしたことである(「アクセスの意図」)。いま 1 つは、コンピューターを作動させたときに、被告人のなそうとしたアクセスが無権限であることである。ここで問題となるのが、無権限の解釈である。

a)「無権限」について

セクション 1 の問題として、重大な問題を提起しているのが、この「無権限」の解釈である。セクション 17(5)によれば、

「(5)Access of any kind by any person to any program or data held in the computer is unauthorised if(いかなる人の、いかなるプログラムないしはデータののいかなる種類のアクセスも、以下の場合に、無権限である)

(a)he is not himself entitled to control access of the kind in question to the program or data;and (その者が、問題のプログラムないしはデータに対してアクセス・コントロールを与えられていない場合)

(b)he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.(問題のプログラムないしはデータに対しアクセス・コントロールを与えられている者の同意を有しない場合)」

に「無権限」であるとされる。

そこで、「外部者」「内部者」の区別をここに導入するかという問題がある。詳細については、別稿に譲るが、英国においては、「外部者」「内部者」の区別をすることもないし、また、2 台のコンピューターが必要であるという解釈もとられることはないのである。

b)「認可」

内部者が、有罪であるとされるためには、二つの意図の証明というハードルがあるとされている。その二つとは、

1)プログラムないしはデータに対するアクセスの意図

2)コンピューターを作動させた時点においてアクセスする権限を有しないことを知っていた

ということである。

第4項　第 3 条の構成要件について

第 3 条の条文

コンピューター・不正利用法 1990 の第 3 条(1)は、以下のようになっている。
「3(1)以下の行為をなしたものは犯罪である
(a)無権限で、コンピューターのコンテンツに改変を加えるいかなる行為をした場合かつ
(b)その行為の時点で、必要な意図と必要な認識を有している場合
(2)サブセクション(1)(b)の目的のために、必要な意図とはいかなるコンピューターのコンテンツを改変し、かつ、そうすることによって
(a)コンピューターの作動を損ない
(b)コンピューター内のデータないしはプログラムへのアクセスを妨害し、または、遅延させる
(c)プログラムの動作を損ない、またはデータの信頼性を損なうことをいう」
そして、この条文は、シンプルな無権限改変を対象とするものであり、かつ、電磁的な方法によるものを問題としている。そして、物理的なものは、刑事的ダメージの一般法による。そして、この対象として、ウイルス、ワーム、トロイの木馬、ロジック・ボムなどが考察の対象となる。

行為-actus reus

無権限

この点については、いわゆる「不正アクセス法案」で検討した通りであり、また、報告書においても、とくにこの無権限改変等の解釈については、触れられてはいないところである。
しかしながら、この無権限改変については、セクション 1 の場合に比較して、内部における改変の権限の問題があるとされている点については留意を要する。

改変

「改変をおこすこと」については、「コンピューターのメモリーないしストレージ・メディアのコンテンツに対するいかなる変更・消去ないしは追加をカバーすることになる」と解されている。「コンテンツ」とは、技術的な意味ではなく、例えば、データおよびプログラムを含むものであって、情報や指示というものをなにがなすかという説明を避けるものじであるとされている。それによって、ワームなどのプログラムが、どのように働いたかという点について説明する必要がなくなるとされている。

証明

もっとも、この無権限改変については、その証明の問題がある。いうまでもなくウイルスのコードを保有することは違法ではなく、悪意のあるコードを書くことは禁じられているものではない。そうだとすると、その悪意のあるコードを配布するか、そのリリースに貢献したことを証明することが重要になる。逆にいえば、ウイルスは、それを書いた人間ではなく、第三者によって、広がることがよくあり、被告の行為によって被害が発生したというのを立証するのは大変な負担となる。また、コードが誰の作成によるものかがはっきりしないのがいま一つの問題となる。

意図-mens rea

この犯罪の主観的な要素としては、「必要な認識」と「必要な意図」が必要になる。この点については、第 3 条(2)が定めているとおりである。

「必要な認識」

この「必要な認識」としては、「目指された改変が、無権限であること」を認識することである。この認識としては、セクション 1 と同様である。

「必要な意図」

委員会としては、「無権限改変でも、コンピューターの動作に関して改良する、ないしは、影響を与えない場合、罰しないというのは、重要である」と考えている。
この意図としては、次の 4 つの結果を引き起こす意図が必要となる。その 4 つの結果を検討すると以下のようになる。

a)コンピューターの動作を損なうこと(impair the operation of any computer)

特定のプログラムを損なうことなくこの結果が導かれるものとしてワームの例がある。ワームのコード自体は、プログラムやデータに寄宿することは必要としない。コンピューター内で、増殖されて、コンピューターの処理速度を遅くしてしまう。
ワームは、技術的には、コンピューター内のデータ・プログラムを変更したり、追加したりする必要はない。しかしながら、感染コンピューターは、プログラムとデータが、改変されるのである。とくにコンピューターが、インターネットで接続されている場合はそうで、その場合に対処するのが、まさにこの法律の目的ということになる。

b) プログラムないしデータへのアクセスを妨害し、ないしは、遅延すること (Prevent or hinder access to any program or data)

ワームは、プログラムないしデータのアクセスを遅延させる。他のウイルスも、同様である。例えば、一定の時間に一定のメッセージをながしたりするウイルスの場合には、その時点で、他のプログラムの作動を妨げていることになる。また、論理爆弾も同様である。例えば、自分が会社をやめて、自分の名前が、消えたときに会社の重要なデータに暗号がかけられるということはもちろんのこと、データを暗号化し、消去するときに暗号をとくシステムをつくった IT マネージャーが有罪になった事案が紹介されている(報告書)。

c)プログラムの作動を損なうこと(Impair the operation of any such program)

これば悪意あるコードのために、プログラムの動作に障害が生じる場合をいうことになる。

d)データの信頼性を損なうこと(Impair the reliability of any such data)

この点については、感染したコンピューターのオーナーが、主観的にデータを信頼できなくなったということだけではなく、客観的な根拠をもって、データの質が低下し
たことを明らかにしなければならないとされている。

意図の対象-一般意図

この上記の意図については、一般意図とでも言うべきもので足りると説明されている(レポート 3.73)。すなわち、何らかのコンピューターの機能を損なう、ないしは何らかのデータを破壊することを意図すれば足りるのであって、特定のコンピューター・データに対する意図は必要としないのである。この趣旨は、条文にも明らかにされており、第 3 条(3)は、
「意図は、

(a)特定のコンピューター

(b)特定のプログラムもしくはデータもしくはいかなる種類のプログラム ないしはデータ

または

(c)特定の改変ないしはいかなる種類の改変に向けられたものであることを要しない」

とされている。

第4節 刑事的ダメージ法 1971 との関係

報告書においては、無権限改変などが、物理的なダメージになった場合には、なおも刑事的ダメージ法の適用も可能であるという点が指摘されており、この趣旨は、法律の条文上も明らかにされている。
第 3 条(6)は
「刑事的ダメージ法の目的のため、コンピューターの内容の改変は、それが、コンピューターないしはコンピューターストレージ手段を物理的に損壊しないかぎりはコンピューターないしは、そのストレージを損壊するものと考えない。」
としているのである。

第5節　コンピューター不正利用法をめぐる具体的判例

では、このコンピューター・不正利用法が、コンピューターウイルスに対して、どのように適用されるか、具体的な例で検討していくことにする。なお、コンピューターに対する無権限ア

クセスについての判例は、種々のものを挙げることができ、その事案と判決の分析は、資料編のバード・アンド・バード事務所のレポートの翻訳から参照できるが、害意あるプログラムについては、若干の判例を報告できるにすぎない。

第1項　Goulden 事件

被告人は、印刷会社にあるワークステーションにサキュリティパッケージをインストールしたが、そこにパスワードなしでのアクセスを拒絶する仕様を含ませておいた。 .これは、£2,275 におよぶ報酬の助けにと、この仕様を用いたのである。 この印刷会社は、£36,000 の損失を被ったとして、 裁判所は、1993 年 5 月 31 日に 2 年間条件付き免責と£1,650 の罰金を言い渡した事件である。

第2項　Bedworth 事件

当時 18 才の Paul Bedworth は、 the Financial Times のデータベースに侵入し、変更をなし、また、 The European Organisation for the Research and Treatment of Cancer に対して£10,000 の電話の請求書を残した。彼は、不正利用法のもと共謀で起訴されたのである。この事件においては、被告は、「コンピューター傾向シンドローム」'computer tendency syndrome'であると抗弁をなし、陪審員は、裁判官の説示があるにもかかわらず、無罪であるとしたのであった。この決定を「ハッカー憲章」とか「ハックのライセンス」という人もいるくらいである。

第3項　Whitaker 事件

Whitaker は、ソフトウエアの支払について紛争のある場合に、働かなくする論理爆弾を仕掛けておいたのである。 Whitaker は、報酬についての支払について問題のある場合に、そうする権利があるとしたが、裁判所はそのような主張は認めなかった。

第4項　The Pile Case

これは、アンダーグランド界では、'Black Baron'として知られていたChristopher Pile,が、Pathogen' と'Queeg'という二つのウイルスを作成したことなどを理由に、セクション 1 および 5 つの無権限改変(第 3 条)および他人のウイルス作成の教唆の訴えで、 訴えられた事件である。被告人“Black Baron”は、“Pathogen”と “Queeg”というウイルスを作成した。彼は、第 2 条と第 3 条、そして、第 3 条違反を教唆したとして起訴さた。彼は、罪を認め、18 ケ月の懲役を宣告された。彼が、どのコンピューターが、彼の放ったウイルスによって影響されたかというのを知らなかったという事実は、犯罪を犯すさいの意図についての上述の要件についての特定の規定にてらして有罪を妨げるものではないとされている。

第6節　まとめ

第1項　　英国における害意あるプログラムについての法適用の概観

「メリッサ」などのような電子メールウイルスは、特定のデータやプログラムの実行を妨害するものではなく、単純に、電子メールシステムについて、それ自体を電子メールのディレクトリーを用いて、増殖させるものであるが、コンピュータ不正利用法第 1 条および第 3 条を犯し、有罪であるものと考えられる。
電子メールシステムは、電子メールシステムを受信するように意図されているものである。第 1 条の適用の可能性については、そのウイルスが、まさにウイルスとして電子メールのサーバーにアクセスしていく、ないしは、アドレス帳のファイルにアクセスしていくこのである。この点を考え、そのようなアクセスについて、アクセスの管理側としておよそ許容していないものと考える時には、第 1 条のもとでは、受信者の電子メールプログラムを用いて、電子メールウイルスを受信し、電子メールシステムにより電子メールウイルスを増殖させることは、議論の余地はある[45]が、無権限の性質を有し、それゆえに、第 1 条のもとで、起訴されるであろうということになる。
第 3 条に関して、最初にコンピューターの無権限改変が存在するかが問題になる。最初に、受信システムが、電子メールの受信にオープンで、それゆえに内容の改変がさけられないとしても、意図された電子メールシステムの利用を越えて、実際になされた改変が、無権限であるとされるのではないかが議論としてが可能になる。第 1 条と同様の議論があるが無権限であると解されている。コンピューターの操作を損なったり、 ないしは、コンピューターのプログラムないしはデータへのアクセスを妨害、遅延させたり、そのようなデータの動作を損なったり、信頼性を損なったりなどの意図が必要になるが、そのような意図を伴う場合には、第 3 条にも

[45] この点についてはバードアンド・バード法律事務所のレポートの本分の最後の部分を参照のこと

違反することになる。「損なう」のは、広い概念であり、私たちは、種々の事案において、ウイルスの効果を、この概念の中に取り込むことが可能であろうとされているのである。
また、悪意あるプログラムの拡散については、電気通信法 1984 第 43 条の規定に注意すべきである。第 43 条(1)は、以下の行為をしたものを有罪とする。

> “(a) 公衆の電気通信システムを用いて、ぞっとするほど腹立たしい(grossly offensive)ないしは、下品な(indecent)、わいせつな(obscene)、脅迫的な(menacing)メッセージないしはものを送信する
> (b)そのような手段によって、困惑、不便、ないしは不必要な他人に対する不安感を惹起する目的で、虚偽であることを知っているメッセージを送信すること、もしくは、その目的で公衆電気通信システムを継続的に使用すること

この犯罪に対する刑罰は、1990 年法第 1 条と同様である。いくつかの事件(起訴された事件の一覧表参照) において 1990 年法および電気通信法に基づいて起訴がなされている。害意あるプログラムを拡散したものについては、この条文の適用の可能性があることは指摘されるべきである。

第2項　英国の法規制の特徴

英国の法規制の特徴としては、無権限アクセスからのアプローチとデータの改変からのアプローチで悪意あるプログラムを捉える点にある。また、主観面として実際に結果の発生についての意図が必要とされるが、その意図については、かなり抽象的なものでも結果として捉えているように思える。そのためにアドレス帳の記載されているアドレスにメールを送信するという行為のみをとらえたとしても(解釈上の争の余地はあるものの)犯罪として捉えることができるものといえよう。(担当 弁護士高橋郁夫)

第6章 ドイツにおける有害プログラムの刑事的規制

第1節　ドイツにおけるネットワーク刑法

コンピュータ・ウィルスとの関係において?

1　ドイツのネットワーク刑法をコンピュータ・ウィルスによる侵襲という視点からみた場合、問題となる条文は、刑法典上の 202 条 a、303 条 a、303 条 b が問題の中心となるが、さらに不正競争防止法(UWG)17 条ならびに連邦情報保護法(BDSG)43 条、48 条もその射程にはいってくることとなる。まず、これをネットワーク刑法の保護法益である情報のインテグリティという観点から整理してみる。

情報のインテグリティ(Integrty of data)を情報の正確性という点でみるなら、情報それ自体の正確性の確保すなわち情報の損壊ないし変更に対するインテグリティと情報へのアクセスに対するインテグリティという二つの側面でみることができる。前者の情報の損壊に対するインテグリティを問題にするのが、ドイツ刑法 303 条 a および 303 条 b である。これに対して、情報へのアクセスに対するインテグリティを問題にとするのが、刑法 202 条 a であり、さらに情報内容に応じて、不正競争防止法 17 条が営業上の秘密について、連邦情報保護法 43 条が個人情報についてその保護を図っている[46]。

2　ドイツ刑法 202 条 a[47]は、データの探知、すなわち媒体に記録された情報および伝送中の情報への無権限のアクセスを処罰するものであり、いわゆる「ハッキング」行為[48]を捕捉す

[46] もちろんこれらの法律はネットワーク上の侵害行為にのみ限定して適用されるものではなく、当該構成要件に該当する以上、ネットワークを用いない場合であっても処罰されうる。さらに、刑法 202 条 a、303 条 a および 303 条 b は、1987 年の第二次経済犯罪対策法によって導入されたものであり、そのときにコンピュータ詐欺罪などの規定も立法されたが、ここでは問題領域外にあるため、言及しない

[47] 202 条 a　データの探知(Aussphaen)

(1)　権限がないのに(unbefugt)、自己のために予定されておらずかつ無権限(unberechtigt)のアクセスに対して特別に保護されているデータを、取得しまたは他人に得させた者(sich oder einem anderen verschaffen)は、３年以下の自由刑または罰金に処する。

(2)　１項の意味におけるデータは、電子的、磁気的またはその他直接認知しえない形態で貯蔵されまたは伝送されるものに限られる。

る。その意味では、情報セキュリティの重要な部分を保護するものといえる[49]。ただし、刑法上の保護法益という点では、形式的秘密を保護するものであり、このかぎりでは、わが国の信書開披罪に類比するものとして位置づけることができる。基本的な構成要件は、データの無権限のアクセスであり、データの管理者が保護しようとしているデータに対して権限なくアクセスした場合、データ探知罪が成立する。

これに対して、情報の実質的秘密の保護はその情報の内容、すなわち何に関する情報であるかによってさらに別の構成要件に該当することとなる。不正競争防止法 17 条は企業秘密についてその保護を図るものであり、連邦情報保護法 43 条[50]は個人情報を保護するものである。いずれも、ネットワーク上のデータに限定されず、権限なく企業秘密あるいは個人情報を入手する行為を処罰するものである。もっとも、これらの犯罪はネットワーク上の行為あるいは電磁的記録に関するかぎりいずれも 202 条 a を前提とし、各々観念的競合の関係にたつ。また、202 条 a はデータの内容如何をとわず保護するものである。したがって、以下の考察ではもっぱら刑法 202 条 a を取り扱うものとする。

３　データの損壊、すなわちデータの正確性それ自体を問題とするのが刑法 303 条 a[51]ある。すなわち、データの無権限の変更・毀損をその構成要件とする。さらに、刑法 303 条 b は、たんなるデータの損壊だけでなく、情報処理過程に対する利益をも保護する。その意味では、コンピュータによる情報処理の一般的な安全性を保護するものといえる。この点で、303 条 b[52]

---

[48] ただし、サーバへのたんなる侵入行為、無権限のコンピュータの使用は処罰の対象とはならない。この点においてわが国の不正アクセス防止法よりは処罰の限定がなされている上、その規制目的も明確である。

[49] 情報セキュリティをどのようなものとするかについては、異論もあろうが、(1)デバイスに記録されたデータの正確性、(2)伝送中のデータの正確性、(3)伝送されたデータの受領の正確性が最低限保証される必要があろう。202 条 a はこのうち(1)(2)の両方を保護するものとして重要である。

[50] 連邦情報保護法 43 条は次のとおりである。
(1)　権限なく、この法律で保護されている公開されていない個人に関係するデータを
1. 貯蔵、変更もしくは伝送し、
2. 自動化された方式によって呼び出せるように準備をし、または
3. データ補完装置（補完場所）から呼び出しもしくは自己または第三者のために入手した者は、１年以下の自由刑または罰金刑に処する。
(2)　この法律で保護されている公開されていない個人に関係するデータの伝送を不正な指示によって領得し、
1. 16 条４項１文、28 条４項１文に反して、また 29 条３項、39 条１項１文または 40 条１項との関連において伝送されているデータを第３者に譲渡することによって他の目的のために利用し、または
2. 30 条１項２文に反して 30 条１項１文において特徴づけられているメルクマールまたは 40 条３項３文に反して 40 条３項２文おいて特徴づけられているメルクマールを集めた者も同様に処罰する。
(3)　行為者が有償または自己もしくは第三者の利益をはかりあるいは第三者に損害を与える目的で行為した場合は、２年以下の自由刑または罰金刑に処する。
(4)　略（親告罪の規定）
連邦情報保護法の 16 条の規定は、非公的な立場の者へのデータの伝送が許容される場合を列挙しているもの、28 条以下は具体的な目的に応じてデータの蓄積に関してガイドラインをしめすもの。

[51]
303 条 a　データ変更
(1)　データ（第 202 条 a 第 2）違法に消去し、隠蔽し、使用不能にし、または変更した者は、２年以下の自由刑または罰金に処する。
(2)　本条の未遂は罰する。

[52] 303 条 b　コンピュータサボタージュ（コンピュータ妨害）
(1)　他人の経営体、他人の企業または官庁にとって本質的に重要であるデータ処理を次に掲げる行為によって妨害した者は、５年以下の自由刑または罰金に処する。
１　第 303 条 a 第１項の行為をおこなうこと
２　データ処理施設またはデータ貯蔵媒体を破壊し、毀損し、使用不能にし、除去しまたは変更すること
(2)　本罪の未遂は罰する。

は個人的法益をこえた利益を保護するものといえる。ただし、303 条 b は、データの変更・毀損による行われる情報処理の阻害のみならず、コンピュータ等情報処理のためのハードウェアの毀損によるものも処罰をしているが、ウィルスとの関連においては、1 号による 303 条 a の行為によるものにその考察を限定してよいであろう。わが国との比較において重要なことは、ドイツでは、わが国における業務妨害罪と同様の処罰規定を有していないてため、情報処理を阻害する業務妨害のみが処罰されることになる点である。

さらに、これらの罪はいずれも未遂を処罰する点がウィルスの投与の可罰性を考える上で重要となる。すなわち、ドイツ刑法 22 条は「その行為についての表象にしたがって、構成要件の実現を直接に開始した」場合を未遂と定義している。それゆえ、以下の論述に見られるような有害なプログラムを被害者のシステムに送付ないし投与した場合、303 条 a ないし b の罪の未遂犯の成立を認めることができるであろう。

加害行為の態様	問題となる有害なコード	罰条	侵害されるセキュリティの内容
データの毀損	ウィルス ワーム	303条a 303条b (303条) (317条)	データの正確性の侵害 データの改変・破壊に対するインテグリティ
システムの毀損			
システムへの侵入	Back 0rifice	202条a	データ・アクセスに対するインテグリティ
無権限アクセス	トロイの木馬	UWG17条 BDSG43条	

第2節　有害プラグラムによる攻撃と犯罪の成否

第1項 有害プログラムによる情報のインテグリティの侵害

1　ネットワークに関わる有害なプログラムによる利益侵害も情報のインテグリティの侵害である。したがって、ウィルスによる攻撃対象も前節において述べたインテグリティの点による二つの類型に対応する。無権限のデータアクセスとしてのコンピュータ・スパイとデータ破壊としてのコンピュータ・サボタージュがそれである。

２　コンピュータ・スパイに利用されるプログラムとして考えられるものは、いわゆる「トロイの木馬」タイプ[53]のプログラムや Back Oriffice に代表されるようなリモート・アクセスのプログラムである。典型的なウィルスでこのような機能をするものもあるが、ドイツではまだ問題になっていないようである[54]

コンピュータ・サボタージュとして問題となる有害プログラムによる攻撃において、その行為の客体となりうるのは、コンピュータのハードウェアとソフトウェアの両方である。すなわち、あるプログラムがシステムの基本的なソフトをはじめとするプログラムファイルを破壊ないし削除することによって、303 条 a ないし b の成立が問題なるだけでなく、通常の器物損壊罪の成否すらも問題とされる。このようなプログラムの典型的なものは、ハードディスクを初期化したり、特定のファイルを削除する機能を有するウィルスであろう。さらには http によるアクセスに際して、ActiveX などを組み込むことで同様の機能を果たさせることも可能であり、その場合にも問題となる。また、アメリカにおけるインターネットワーム事件[55]にみられるように、ワームもデータないし情報処理の適正性を侵害することがありうる。

３　以下では、上述のふたつの視点をもとに、有害プログラムの機能に着目し、刑法上の問題点を検討することとする。

第3節　コンピュータ・スパイ

第1項　トロイの木馬の事例

コンピュータ・スパイに利用される典型的なコードは「トロイの木馬」と呼ばれるものである。これは、プログラムのなかに、データの消去、変更または送出をおこなう下位のコードが組み込まれているものである。ドイツにおいて問題となったのは T-online Power Tools 事件[56]

---

[53] トロイの木馬をプログラムの保持者が予期しえない動作を示すタイプのものを指称する定義もあるが、ネットワークで問題とされる場合には、個人のパソコン等から ID やパスワードを盗み取るタイプのものさすのが通例である上、ドイツにおける議論ではトロイの木馬は後者のタイプのものであること前提に議論されている。

[54] U. Sieber, Teil 19 Strafrecht und Strafprozeｱrecht, in:T. Hoeren/ U. Sieber (Hrsg.), Handbuch Multimedia-Recht, 1999, Rdn. 44 は日本におけるニフティ・サーブ（当時）で広まったパスワード探知のウィルスを例にあげている。

[55] このワームプログラムは、ネットを通じて他人のコンピュータに侵入するために、標準化されたハッキングツールを使用する。それによって、数日で約 6000 のコンピュータを麻痺させたものである。この事件の行為者は、ワームプログラムがどのくらい早くインターネットに広まっていくのかテストしようとしただけなのに、少数の位を書き間違ったためにプログラムがコントロールできずに広まることになったと、反論した。この主張にみられるように、ウィルスの拡散に対する処罰に関しては、故意の証明の問題が生じる。

[56] この事件の内容は、以下のとおりである。

「少年ハッカー、T-online をクラック

二人の 16 歳の少年が、あきれるほど簡単な方法で、数百人の T-online の顧客のアクセスデータを入手した。 このいたずらは、ホームバンキング、E-コマースおよびいわゆる「使用料」に関して争いのある事例における判例に関する帰結をもたらしたといえるであろう。

と呼ばれるものである。1997 年の末に起きたこの事件では、二人の少年が、表向きはネットへのアクセスを最適化する T-online Power Tools をインターネットにアップロードし、一般にダウンロードできるようにしたのであるが、このソフトは、インストールによって、T-online へのアクセスに関するデータをユーザの知らないうちにこの二人の少年たちに伝送するというものであった。もちろん T-online へのアクセスするためのユーザ ID とパスが伝送されるのは、利用者のハードディスクにそれらが記録されているばあいだけであったが、それでも、この事件は当時まで世間では完全であると考えられていたドイツのオンラインサービスへのアクセスに脆弱性があること示すものとして注目された。

第2項　トロイの木馬に関わる刑法的問題

1　では、一般的にトロイの木馬を配布することはどのような刑法的問題が生じるであろうか。この点については、次のような例をもとに考察してみることとする。

AはBにメールをつかって「トロイの木馬」を送った。これは（Bに気づかれずに）そのパスワードをAに伝送するものである。このパスワードをつかって、Aは、のちにBのコンピュータに侵入し、関心のあるデータをコピーした。

2　まず問題となるのは、コンピュータへの侵入の点である。すなわち、トロイの木馬をBのコンピュータへ組み込むことはどのように解すべきかが問題とされる。もっとも、Bのコンピュータへたんに侵入しただけでは不可罰のままである。それでも、保護されたデータのコピーをおこなった時点でそれは可罰的なものとなりうる。

Aはデータをコピーすることによって自己の支配に移し、202 条 a 1 項の意味でデータを「入手した」ものである。しかも、それらのデータは権限者の意思によるとAのために予定されているとはいえないものである。202 条 a の適用の可否の点でもっとも問題となるのは、それらのデータについて特別のアクセスの保護が存在していたかどうかということである。Bはたしかにそのデータをパスワードによって保護していたが、それでも、その障害はAにとってたいした困難もなく克服できたのである。202 条 a にいう「保護」が客観的に一定程度のセキュリティ措置を施すことを要求するのであれば、この場合、202 条 a は成立しえない。しかしながら、202 条 a は個人の形式的秘密を保護するものであるから、その成立にとっては、権限者の保護意思を明確に示すいかなるアクセス保護も十分であるとの前提に立つと解するのが妥当であるとされる。したがって、このような事例についても、202 条 a の可罰性を肯定できることになるとされる。

クラックした ID とパスワードをつかって、二人のハッカーは、これらの顧客に費用を負担させることで、ドイツ最大のオンラインサービスににについて課金され、電話料金で差し引かれるすべての機能を利用できるようになった。同様の方法で、彼らは、ホームバンキングの口座へのアクセスも手に入れることができた。

T-Online の業務執行役員である Eric Danke は、「きわめて真剣に受け止めるべき事件」であり、これはすべてのセキュリティ構想を熟慮し、発展させることになるだろう。短期的には、T-Online はこの具体的な攻撃に抵抗できるデコーダ・アップデイトを提供するであろう、と語った。

ふたりの少年は、その行為によって、何らかの損害を惹き起こそうとしたのではなく、T-Online の基本的なセキュリティの欠如とデコーダ・プログラムのセキュリティの不十分さをおおやけにしようというものであった。ふたりは、"T-Online Power Tools"という有名なサポートプログラムの著者であり、このソフトを「トロイの木馬」としてアクセスデータを極秘に伝送するために利用した。彼らは、優れたプログラミング知識を利用していないにもかかわらず、アクセスデータの単純な暗号化を短期間にハックすることができたのである。ハック後３ヶ月して、彼らはその行為を中止し、その大胆な行為をわれわれに対して打ち明けた。」

３　つぎに、パスワードの入手について、パスワードを転送したことそれ自体が 202 条 a１項に該当するかが問題となる。第一に、システムに貯蔵されたパスワードは 202 条 a２項の意味での「データ」とみることができる。また、パスワードの性質上、それが第三者のために予定されたものとは当然いえない。問題となるのは、パスワードがそれ自体権限のないアクセスに対してとくに保護されていたのかということである。この場合、パスワードそれ自体による保護は問題にならない。というのは、その種のアクセス制限は他のデータを権限のないアクセスから保護するものだからである。そこで、パスワードが通常基礎としている秘密保持は、202 条 a１項の意味での保護と考えることができる。というのは、パスワードの秘密保持は客観的な作用を有しているからである。アクセスの可能性は、パスワードによって、ソフトウエア技術上の保護によるのと同様に、信頼できる形で阻止されている。したがって、202 条 a の成立を肯定することができよう。

４　最後に、「トロイの木馬」を送付・機能させたことについて、トロイの木馬をうまく隠して配置したことが 303 条 a の構成要件に該当しないかが問題となる。まず、データの抑圧・使用不可能にするとのメルクマールについてみてみる。Aはたしかにトロイの木馬を転送することによってBのハードディスクの一部を占拠した。それでも、その点について、データを「抑圧する」ということも「使用できなくする」ということも認めることはできないとされる。つぎに、データの変更というメルクマールについてであるが、Bの固有のデータの存在する領域を別のデータを挿入することによってデータを変更したと認めることが可能であるとされる。なぜなら、303 条 a は権限者のそのデータの完全な使用可能性という利益を利益を保護するものだからである。しかしながら、トロイの木馬の配置によってBの固有のデータの使用可能性が制限されたかというと、トロイの木馬の無権限の転送はそのような使用可能性の制限はともなわず、したがって、トロイの木馬の無権限の転送は 303 条 a の構成要件に該当せず、303 条の可罰性も排除される。なお、202 条 a は未遂を処罰しないため、データの無権限のアクセスの意図をもってトロイの木馬の送付しても、それだけでは不可罰の未遂である[57]。

第3項　Back Oriffice の投入とその使用

Back Orifficeによる他人のコンピュータのリモート操作は、まず、データのアクセスの点について、原則としてトロイの木馬の場合と同様に解することができ、無権限に保護されたデータにアクセスした場合にかぎり、202 条 a が成立しうる。したがって、無権限にリモートコントロールするにとどまるかぎりは不可罰である。このことは、その他のリモートコントロールプログラムについても同様に解することができる。しかしながら、たんなる無権限のリモートコントロールをこえて、他人のコンピュータにあるデータを変更ないし消去した場合には、303 条 a が成立することになり、さらに、そのことが情報処理を阻害したときは 303 条 b に該当することとなる。

[57] 以上の点については Hilgendorf, Grundfälle zum Computerstrafrecht, JuS 1997, 130ff.

第4節 コンピュータ・サボタージュ

第1項 コンピュータ・ウィルス、ワーム

1　コンピュータ・ウィルスは特定の宿主に寄生することで、増殖する点に特徴があるが、そのコードの機能形態は多様である。ドイツのネットワーク刑法においてウィルスを投入したことが処罰されるためには、ウィルスの機能が刑法 303 条以下に規定される構成要件的結果を惹起する必要がある。そのかぎりで、ウィルスのタイプがいわゆるブートセクタ・ウィルスであるか、マク・ロウィルスであるかあるいはコンパニオン・ウィルスであるかといった宿主の種類と犯罪の成否は無関係である。これに対して、ワームは独立のプログラムがコンピュータシステムに侵入することで攻撃をおこなうものであるが、ウィルスと同様、その効果としてどのような結果を惹起したのかが問われる。

2　刑法 303 条は、他人の「物」を損壊しなければならない。有体物に対する物理的損壊が問題となる。しかし、この場合、有体物それ自体の物的な破壊だけをとらえるのではなく、その正規の使用を不可能にする場合をも含めるならば、ウィルスなどがコンピュータのハードディスクを初期化した点について、客観的に刑法 303 条の通常の器物損壊罪の構成要件に該当することとなる。したがって、このことによって業務、企業ないし官庁にとって本質的に重要な情報処理を阻害すれば、303 条 b１項２号により、コンピュータサボタージュの構成要件に該当することになる。このような機能を果たさなくとも、有害なコードによって、データの消去、変更がおこなわれ、あるいは使用できない状態にされた場合には、303 条 a のデータ変更の構成要件に該当し、このことによって業務、企業ないし官庁にとって本質的に重要な情報処理を阻害したときは、303 条 b１項２号によるコンピュータサボタージュの罪が成立することになる。それゆえ、ウィルスの拡散について処罰を考慮するばあいには、ハードディスクの初期化のように明確なデータの損壊の場合は別として、ウィルスの機能が 303 条 a の構成要件的結果を惹起するのものかが重要である。

3　ドイツにおいて、ウィルスによるコンピュータサボタージュが問題となった事件は、クリスマスツリー事件といわれるものである。これは、クリスマスグリーティングのメールにクリスマスツリーをディスプレイに表示させるプログラムを添付したものであるが、このプログラムに組み込まれたコードが、ディスプレイへのデータの表示と同時に、自己のプログラムを複製して同一のクリスマスグリーティングのメールをメールクライアントプログラムのアドレスデータにアクセスし、アドレスに記載されている全員に送付するというものであった。そのため、感染したデータを受け取った者がプログラムを起動するたびに雪だるま式に感染データの配布メールを送出する結果となり、そのことがネットワークへの過大な負荷をかけたことによってシステムダウンへといたったのである。このプログラムの作者は告訴されたものの、「『クリスマスツリーワーム』では、きわめて限定的な範囲でのみ実験しようとしただけであり、ワームを解き放って損害が発生することなど考えていなかった」と主張した。そのために、器物損壊、データの改変およびコンピュータサボタージュを理由とする有罪判決は、ネットワークの損害に関して故意が証明されないとして、不可能であるとされた。 故意の点については問題がないとの意見も存する（後述第 2 項参照）。

この事例は、メリッサ型のマクロウィルスと同様のものである点は重要である。すなわち、メリッサ型ウィルスの投与・配布は、その故意の点に問題がなければ、同様にドイツ刑法 303 条 b による可罰的となるということである。

４　このような故意の点に問題ない場合、303 条以下の規定は未遂を処罰するため、刑法 22 条の未遂の一般原則にしたがい「直接的な開始」が認められるときは、未遂犯の成立を考えることができる。たとえば、コンピュータウィルスをあるコンピュータに投入したが、しかしまだその攻撃客体となるデータへの作用がない場合には 303 条 a の未遂犯が成立する[58]。

第2項　ウィルスの拡散における故意の問題

ウィルスなどデータの改変をもたらすコードを投入する行為を処罰するためには、故意が必要である。しかしなが、ドイツ刑法 15 条にいう故意は、いわゆる未必の故意で十分である。したがって、303 条以下の犯罪の成立にとっても未必の故意で足りることとなる。この点、ドイツの判例および通説は、未必の故意について、結果を是認しつつ甘受したということが客観的指標にしたがって認められれば故意を肯定することができるとしている。すなわち、その判断にとって、結果の明白性、危険性だけでなく、危険回避のための予防措置への関与という点が重要な基準となる。そこで、可罰的な結果の発生を相当程度の蓋然性をもって予見したが、それにも関らず、それを回避することをおこなわなかった者は、たとえその結果を実際には「望んでいなくとも」、故意を以って行為している。これに対して、一定の予防措置を講じて、「すべてうまくいくにちがいない」と考えたことから、結果をほんのわずかの蓋然性しかないと考えた者は、通常、認識ある過失により行為しているのである。そのため、これをクリスマスツリーワーム事件にあてはめた場合、行為者は、そのような損害のそれほど遠くない可能性を認識しているが、しかし、結局どうでもよいと考え、そのため自分の実験の現実化を受け入れていた場合には、その種の未必の故意を肯定することは可能であったとする意見もある[59]。

第3項　メール攻撃によるコンピュータサボタージュ

１　昨年問題となったメリッサ、さらにはドイツにおけるクリスマスツリー事件が示すように、ネットワークにおけるメール機能を利用した攻撃が生じている。多量のメールの送付行為も、情報処理を阻害することがある場合には 303 条 b の成否を検討する必要がある。

ＡはＥメールをつかってＢに無限メールを送付し、重要な報告（いくつかの匿名の通信を含め複数の取引のもう込み）がＢに届くことを妨げた。そのことによって、Ａが予見したように、Ｂは著しい財産的損失を被った。

２　この事例をもとに、スパムなどのメール送付に関わる解釈論的問題を明らかにしてみる。この事例で二つの客体を考えることが可能である。第一はＢのメールボックスにあるデータである。このデータについては 303 条 a１項のデータの変更といえるかが問題となる。Ｂのメールボックスへ無限メールを転送する行為は、受取り手のデータを無限メールによって変更しておらず、そのメールボックスのデータの記憶スペースを満杯にしただけしかない。したがって、データの改変それ自体は問題とすることができない。そのため、303 条 b１項２号の成否を考慮するにあたっては、Ｂのメールボックスを使用できなくしたといえるかが重要となる。この点、303 条 b１項２号にいう「使用できなくする」とは、当該ハードウエアが正規の方法で使用できないほど重大な程度の使用可能性の侵害をいい、その使用可能性の侵害が相当程度

[58] Vgl. auch Schönke/Schröder/Stree, 303a Rdn. 7.
[59] U. Sieber. a.a.O., Rn. 47ff.

継続的なものであり、それゆえただちに除去できないものでなければならない。それゆえ、Aの無限メールをBは容易にハードディスクから削除することができ、それによってメールボックスの機能を回復することが可能であるため、メールボックスおよびメールボックスの内容についてAは不可罰であるとせざるをえない。この結論については法政策的には問題のある帰結であると評価する者もいるが、妥当であるとの見方が強い。

3　第二に、Bに第三者によって送付されたデータについて 303 条 a の成否が問題となる。すなわち、Aの無限メールがそのデータのBへの到達を妨げていることが「隠匿した」といえないかということである。この場合、データの隠匿とは継続的あるいは一時的なものであっても、権限ある者のアクセスからデータを奪うことをいう。そこで、Aは到着した電子メールをBのアクセスから奪ったのではなく、たんにBのアクセス可能性をそもそも生じることを妨げているすぎず、直接的にはこの定義に該当しないといえる。しかしながら、274 条1項1号に関する RG の判例によると、郵便配達人が誤って間違った住所へ配達した手紙へのアクセスを妨げた場合にも、「隠匿した」といえ、行為者が抑制した手紙について自己の処分権限を保持していたことも決定的な相違を基礎づけるものではないとする。この判例を本事例にあてはめるならば、データを権限者のアクセスから奪った場合だけでなく、権限者に存すべきデータがそのアクセス領域に到達することを妨げた場合にも、データを隠匿したといえると解することができよう。

4　では、当該電子メールが権限者のアクセスから奪われていたといえるであろうか。前提として、問題のデータについて誰が権限者であるといえるかを明らかにする必要がある。303 条 a の客体となるデータの権限者は、Skripturakt[60]によってデータを生み出した者であるとするのが通説である。この理解からすれば、電子メールの送信者が権限者であると解されることになる。これに対して、名宛人への送信によってデータの権限を委譲したとの考え方もありうるが、データの権限がデータの責任をも包含するということを考えると、データの権限の委譲は、原則として、名宛人による事実上の支配可能性の引受けがあってはじめて認められるべきである。

こうして、電子メールの送信者がアクセスを奪われていたといえるであろうか。通常、電子メールのコピーが送信者の手元に残っているのであり、送達不可能な電子メールは送信者の元に戻ってくる。とすれば、電子メールの送信者は、そのデータのアクセスの可能性をBのメールボックスに無限メールが占拠したことによって失われてはいないものといえる。この点で、権限者のアクセスは制限されていないし、それどころか.保護されているといえ、したがって、303 条 a 1項の成立は排除される。

5　なお、この事例では、274 条1項2号による証拠上重要なデータの隠匿も問題となる。274 条1項2号の保護法益はデータの証拠権限、証拠上の重要性である。すなわち、法取引における証拠を一定のデータによって提出権利がその中心的位置を占める。問題となるデータの範囲は、274 条1項2号の文言によると、202 条 a 2項の意味におけるデータすべてであるが、本条項の位置づけおよび保護法益に鑑みると、法取引において証拠としての適性があり、特定されていて、かつ名義人を認識させるものであり、そのためそれが視覚的に認知可能であるならば文書が存在するであろうような思想の表明が問題となる。そこで、匿名の送信の場合は名義人の認識可能性を欠くのでこれに該当しないが、取引に関するメールはこれに該当するといえる。そのほかに、主観的構成要件要素として他人に損失を加える目的が必要とされるが、これが肯定されれば、未必の故意の問題はあるものの、本罪の成立を肯定することができる[61]。

---

[60] Welb, IuR 1988, 443ff.

[61] ドイツ刑法 26 条ないし 27 条における共犯の従属性の規定は共犯行為独自の可罰性を限定する。

6　以上はいわゆるスパムあるいはメールボムによる攻撃についての検討であるが、ウィルス等によって同様の効果が生じる場合についても、同一の法解釈がなされるものといえる。

第4項 コンピュータ・ウィルスのネットワークへの配布行為の可罰性

1　以上の検討は、行為者自身がウィルスを投与する場合だけを問題としてきた。しかしながら、ウィルスの作者またはウィルスを保有している者がネットワーク上のウエッブページあるいはニュースグループなどを通じて配布した場合についてはどのようになるであろうか。

2　有害プログラムを保有している者が 202 条 a または 303 条 a ないし 303 条 b を実現する意図を有する者にその手段として利用するためのウィルス等の有害プログラムを配布した場合に、それらの罪の幇助犯が成立することに争いはない。ウィルスを配布してそれらの罪の実行を教唆した場合についても、教唆犯が成立することになる。

3　問題は、たんに一般的にネットワーク上のサーバにウィルス等の有害プログラムをアップロードした場合である[62]。単純のアップロードにとどまっているかぎりは何らの罪責も生じないであろう。しかしながら、第三者が有害プログラムのアップロードをどこかで知り、アップロードされたウィルス等を取得し、これを 202 条 a または 303 条 a ないし 303 条 b を実現すべく被害者のコンピュータに投与し、これらの罪が実現された場合にはどのようになるであろうか。

たとえば、アップロードした者がたんにデータをアップしただけでなく、html ファイルにウィルスであることを明記し、ウィルスの投与・他人のシステムの破壊を煽動した文言を付している場合、当該データを取得した者が実行にでたときに、概括的な故意による教唆犯の成立を認めることは可能である。しかしながら、有害プログラムのデータだけをアップロードしている場合、または、ウィルス等であること示しただけである場合については、かならずしも教唆犯の成立を認めることは困難である。この場合、教唆の成立に必要な故意の実行行為の特定が欠如しているからである。同様の理由により幇助犯の成立を認めることも困難であろう。誰かがダウンロードして配布するであろうという意図であったとしても、それだけを根拠に処罰するのは妥当ではない。 さらに、たとえ共犯としての行為形態を認めえたとしても、共犯の従属性があるため、配布行為を単独で処罰することはできない。ドイツにおいては、上述のコンピュータ刑法の構成要件に該当しないウィルス等有害なプログラムの配布行為を処罰するという刑法的保護の前提領域への可罰性の拡大については、否定的である[63]。

第5節 有害なコードに対する将来的な展望

現在のところ、ドイツにおいては、コンピュータウィルスをはじめとする有害なコードに対する新たな特別のストラテジーは存在しないとされる。現行の 303 条 a および 303 条 b で完全

[62] もちろん、TLG５条によりサーバを管理する企業がこれを排除する義務が生じうる可能性はある。
[63] この点はジーバー教授に対する口頭ならびに私信による質問によるものである。

に十分である考えられており、この点で争いは存在しない。そのかぎりで、抽象的危険犯の形態での「前提領域」の保護が必要であるとの議論すら存在しない。これは、刑法を法治国原理への適合させることためには、具体的な法益侵害性が必要であるとの認識が一般化していることが基本的な理由であろう。わが国に比べてより未遂犯の成立時期を早い段階で認め、かつ不能犯を可罰的とする法制にあり、そのような状況で未遂以前の段階である「前提領域」へその保護を拡大することは、刑法の謙抑性を害するものと考えられるからである。さらに、1987 年の第二次経済犯罪対策法の導入に際しては、この「前提領域」の保護についての一般的な議論がすでに十分検討され、現行の刑法の形態で十分であるとの認識が一般的に形成されているといえる。 もっともこのような考えの背景には、303 条 a ないし b が未遂犯を処罰しているため、たんにウィルスを配布・投与しただけでも処罰可能となるからである。この点、器物損壊罪および業務妨害罪について未遂処罰規程を持たないわが国の法制と比較する際に注意することが必要である。

さらに、わが国は、一般的な業務妨害罪の処罰に加え、電子計算機業務妨害罪が存在している。通常の業務妨害罪の構成要件については、争いがあるものの、判例にしたがい、その罪質を危険犯と理解するならば、ドイツにおいて未遂として処罰されているもの、あるいはウィルス等の有害なコードの配布行為それ自体も、わが国の現行法において捕捉することは可能となろう。このように、考えるならば、ドイツとの比較において、その処罰に相違があるのは、データ探知がわが国では不可罰であるという点である。不正アクセス禁止法は、認証の回避による無権限のサーバーへのアクセスを処罰するものであり、データ一般に対する無権限のアクセスからの法的保護は存在していない。情報処理の中核がデータにあると考えられる以上、その法的な保護を規定することがわが国の今後の課題となろう。

(担当 神奈川大学講師 石井徹哉)

第7章　イタリア報告訳

イタリア・Studio Pellegrino & Dragotti
Gualtiero Dragotti
(訳・弁護士 高橋郁夫)

第1節 序

このレポートは、イタリアの刑事法に基づいてコンピューター・ウイルスのプログラミング、拡散、および使用についての存在する犯罪を概略するものである。

第2節 関連する法律

コンピューター犯罪は、イタリアに法律 547/93 によって導入された。その法律は、刑法典を改正し、新しい犯罪を追加し、存在する犯罪をコンピューター分野に広げるものであった。
上記の法 547/93 は、「コンピューターウイルス」に言及するものではないが、刑法典において、第 615 条 5 項は、コンピューターシステムやネットワークに損害を与えるコンピュータープログラムの拡散を処罰している(以下、参照)。
また、コンピューターウイルスに関連する他の犯罪も存在する。刑法典に対応する条文は、以下に述べられる。

第1項 第 392 条 –コンピュータープログラムの不当な変更ないしは消去; コンピューターネットワークの棄損または不全.

この犯罪は、もともは、人が、問題の権利の行使するために有体物を棄損するのを防ぐことを狙ったものである。「物」が、コンピュータープログラム、電子的データ、コンピューターネットワークの適切な機能であったとしても同様の行為は違法とされる。問題の権利の行使のために誰かのコンピューターにウイルスを導入する行為は、第 392 条に違反すると考えられる。

第2項 第 615 条 3 項 – コンピューターシステムないしはネットワークへの無権限アクセス

コンピューターシステムまたはコンピューターネットワークが、セキュリティ手段によって保護さている時に、コンピューターシステムまたはコンピューターネットワークに不当に(abusively)にアクセスし、または、システムまたはネットワークに権限を有するユーザーまたは所有者の意思に反して滞在することは犯罪である。
この条文に反する犯罪は、3 年までの懲役である。
最低 1 年以上 5 年以下の懲役は、犯罪が、(–inter alia–)システム管理者によっておかれた場合、ないしは、犯罪が、システムに保存されたデータ、情報、プログラムを破壊、損壊するだけではなくて、システムの動作を破壊、損壊、妨害したときに、適用される。
「アクセスする」は、直接的なアクセスおよびリモートアクセスの両者を包含する。
アクセスが、「不当(abusive)」であるとは、かれ自身がシステムにアクセスする権限を有していない、または、限定された目的のみで権限を有しており、彼の認可が、アクセスがなされた目的を含まない場合である。
上述の条文は、いくつかの判例によれば、最低限のセキュリティ手段(例、システムパスワード、施錠してあるドア)であれば十分であるとされているが、基本的な手段では十分ではなく高度な保護のレベルが必要とされ、コンピューターシステムないしネットワークが、セキュリティ手段によって保護されていることを必要とする。
「標的」のシステムをコンピューターウイルスで感染させることがシステム自体に対するアクセスを要するのであれば、第 615 条 3 項は、適用される。

第3項 第 615 条 4 項- アクセスコードの不当な残留ないしは拡散

利益を得る又は損害を惹起するためにシステムないしはネットワークにアクセスするためのアクセスコード、キーワードないしは、他の手段を不当に取得し、複写紙、拡散し、通信し、または、配布することは犯罪である。
この条文のもとの犯罪は、1 から 2 年の懲役および 1 万リラ(およひ 5000 アメリカドル)の罰金により処罰される。

第4項 第 615 条 5 項 – コンピューターシステムの損壊ないしは妨害するコンピュータープログラムの拡散

たとえ第三者により作成さていたとしても、以下の目的ないし効果を有するコンピュータープログラムを拡散、通信、配布るすことは犯罪である:
? コンピューターシステムないしはコンピューターネットワークに損害を与える;

? コンピューターシステムないしはネットワークに存在するデータないしはプログラムに損害をあたえる(その上に関連するデータないしはプログラムを含む);

? コンピューターシステムまたはネットワークの機能を妨害し、または、損なうこと

この条文のもとで 2 年までの懲役および 20.000.000 イタリアリラ(1 万アメリカドル)までの罰金である。
この条文のある解釈によれば、標的システムに「損害(ダメージ)」を与えないコンピューターウイルスの政策、拡散、ないし配布は、可罰的でないという。「ウイルス」プログラムの存在のみが、システムを害うことを意図しているのでなければ、この解釈は、法律の文言に対応するものである(少なくてもそれはシステムメモリーを減少させ、記録メディアのスペースを占有するのであるから) 。
標的システムに存在するデータないしはプログラムに影響するすべてのコンピューターウイルスは、プログラムないしはデータの軽微な変更さえも「損害(ダメージ)」と解釈されるので、上記の解釈の利益を受けることができない。

第5項 第 617 条 6 項 –コンピューターメッセージないしは通信の 偽造、変造、または禁止

コンピューターメッセージの内容ないしはコンピューターシステムないしネットワークにおいて交換される情報の内容を、利益を得る、または、ダメージを与える目的で偽造、変造または禁止することは、部分的であっても、犯罪である。
添附書類の形にせよコンピューターメッセージを変更するコンピューターウイルスは、この条文に該当する。

第6項 第 635 条 2 項 –コンピューターシステムないしネットワークへの損害(ダメージ)

他人に、所有されていたとしても、コンピュータープログラム、情報ないしデータのみではなくコンピューターシステムないしネットワークを破壊、損害、深刻に影響を与えることは、犯罪である。
本条文のもとでの犯罪は、6 ケ月から 3 年までの懲役である。
最低 1 年から 4 年までの懲役は、犯罪が、とりわけシステム管理者によっておかれた場合に、適用される
この条文は、犯罪が他の条文に該当しない場合のみに適用される。

第7項 第 640 条 3 項 – コンピューター詐欺

コンピューターシステムの変更またはコンピューターシステムないしネットワークに記録されているデータ、情報またはプログラムにいかなる程度にせよ権限なしにアクセスすることにより、不当なダメージを与え、不法な利益を得ることは犯罪である。

判例法によれば、作者の利益および被害者の損害が、犯罪に必要である。
この条文のもとでの犯罪は、6 ケ月から 3 年までの懲役および 200 万リラ(1000 米ドル)の罰金である。
犯罪が、とりわけシステム管理者によっておかれた場合に、最低 1 年から 5 年までの懲役が適用される

第8項 第 648 条 – 禁制物の受領

利益を得るために、犯罪の実行に供されたものないしは犯罪により生じたものを購入し、受領し、隠匿することは犯罪である。
本条違反の犯罪は、2 年ないし 8 年の懲役および 20.000.000 リラ(約 1 万米ドル)までの罰金である。
この条文は、種々の事件において補助的な犯罪として適用され、ほとんどの事件において、刑罰のレベルを著しく増加させる。
コンピューターウイルスが、他の犯罪として実行された事案においては、ウイルスを発進したり、保持したりする者は、この犯罪によって訴追される。

第3節 コンピューターウイルスに関連する刑事問題

上記の犯罪のうち大部分(第 615 条 5 項をのぞく)は、直ちにコンピューターウイルスに関連するものではない。
それにも関わらず、大多数の事件においてこれらの犯罪において、コンピューターウイルスが犯罪実行の手段となるかもしれない。
例えば、トロイの木馬ウイルスは、コンピューターネットワークの乱用アクセスを得るために一般に用いられる(第 615 条 3 項)。論理爆弾ウイルスは、コンピューターシステムやネットワーク(第 635 条 2 項また第 392 条参照)の損壊に用いられる。ウイルスの手段によって、無権限の者が、コンピューターシステムないしネットワークに存在するアクセスコードを取得するかもしれないし、それらを拡散するかもしれない(第 615 条 4 項)。ウイルスは、コンピューター詐欺を犯す(第 640 条 3 項)ためにコンピューターシステムないしはネットワークの動作を改変するために用いられるかもしれない。
第 615 条 5 項にもどれは、この犯罪に関して公になった事件はない。
たくさんのコンピュータープログラムは、いままでにコンピューターのシステムにダメージを与えてきたし、そうしたかもしれない(例えば、MS DOS および WINDOWS 基本ソフトの FDISK.EXE プログラム)ので、違法な動作は、広く定義されると指摘するものもいる。
条文の用語は、コンピューターのプログラムが「拡散、通信、配布される」こととなっており損害を与える明確な意図を要するわけではない。これは、犯罪者がプログラムが損害を与えかねないことを知っているのであれば、コンピューターシステムにダメージを与える効果を有するかもしれないプログラムを単に移転しただけでもこの犯罪の定義に該当することう意味する。
上記の故意の必要性は、コンピューターウイルスの無意識の拡散、通信、配布を違法とするのに妨げになる。 コンピューターウイルスに汚染されたシステムを使用したとき、そうして、さ

らにウイルスを拡散し、ほかのシステムを感染させたとき、彼の行為は、彼がそのシステムが感染していることを知らない限り、犯罪の定義には該当しない。
犯罪の定義は、「コンピューターなどにダメージを与える目的ないし効果をもつコンピュータープログラム」を保持すること(detention)を違法としているわけではない。それゆえに、例えば、文書化や解毒剤研究目的のために、コンピューターウイルスのデータベースやライブラリーを維持することは違法ではない。

第4節 電子メールウイルスおよびマクロウイルス(メリッサ、パーク、その他)

メリッサのような電子メールウイルスおよびマクロウイルスは、自己複製を繰り返し、その能力を拡散し続ける。
それにもかかわらず第 615 条 5 項によれば、この特徴は、犯罪の定義に含まれていない。
電子メールウイルスの拡散、通信、配布は、それゆえに、以下の目的ないしは効果がある限りにおいて犯罪である。:

(a) コンピューターシステムないしはコンピューターネットワークに損害を与える;

(b) コンピューターシステムないしはネットワークに存在するデータないしはプログラムに損害をあたえる (その上に関連するデータないしはプログラムを含む)

(c) コンピューターシステムまたはネットワークの機能を妨害し、または、損なうこと

もし、ウイルスが、その行動を自己複製に限定していれば、それが、(a)ないし (b)においてコンピューターシステムに「損害を与え」たといえるかは、議論がある。もし、自己複製が、重要なマシーンないしはネットワークの動作を含んでいれば、ウイルスが、(c)のもとでシステムないしはネットワークのを「損なう」とすることも可能である。
要するに第 615 条 5 項は、実際にターゲットのシステムに損害を与えるウイルスを拡散、通信、配布することを処罰することをもっとも狙ったものであるが、同様に電子メールおよびマクロウイルスを拡散、通信、配布することを防止すると解することができる。
刑事的規定は、広範囲に解されてはならないことは正当に考慮されるべきであり、電子メールウイルスの拡散に対する第 615 条 5 項の起訴は、どのような結果になるか不確かである。547/93 法が施行される前のコンピューター犯罪に関する判決例は、しかしながら、イタリアの法廷は、この分野の犯罪の定義は、ハードウエアおよびソフトウエアの急速な進歩を考慮に入れて解釈される必要があるということを意識している。それゆえに、より広いアプローチおよび犯罪定義のより広い定義が許容されるべきである。
電子メールウイルスの拡散は、ウイルスが、コンピューターシステムを経由しないしはそれらの間でのメッセージを改変し、犯罪者が利益を得たり、損害を与える限り、第 617 条 6 項(コンピューターメッセージないしは通信の 偽造、変造、または禁止)の違反になりうる。
電子メールウイルスを受信コンピューターシステムに対して電子メールないしはマクロウイルスを感染させる目的で、電子メールを送付することが、第 615 条 3 項(コンピューターシステムないしはネットワークへの無権限アクセスに)該当すると考えられるかは疑問である。「アク

セス」の概念は、犯罪者に対して、ターゲットのコンピューターシステムをコントロールする権限を与えるものではない行為を含むようには思えない。それにもかかわらず「コントロール」の概念は、「ターゲット」コンピューターシステムがシステムの保有者の意思にコントロールされずに、そしてその意思に反して動作する(例えば、ウイルスの複製およびさらなる配布)可能性を含むのを除外していない。
電子メールウイルスの配布は、ウイルスの配布者が利益をえない限り(一般にはありえないことである)は第 640 条 3 項(コンピューター詐欺)の犯罪にはならない。
電子メールウイルスの配布は、ウイルスが、ターゲットシステムを破壊、損害を与え、または、(システムの部分が利用できなくなるような意味で)深刻な影響を与える場合に限って第 635 条 2 項(コンピューターシステムまたはネットワークの損壊)の犯罪と考えられる。ダメージの限定的な概念(深刻な損害のみを含む)が適用されるように思え、それゆえ、電子メールおよびマクロウイルス(メリッサ)は、この条文の定義に該当しない。

関連する判決例.

- *第 652 条 2 項(以前の 635 条) によれば、コンピューターを操作するために新しいデータを挿入しなければならないようにコンピューターメモリーからデータを消去することは犯罪である。*(**最高裁判所, 1996 年 12 月 13 日**, in Giur. It. 1997, II, 647.)

  裁判所は、「無体物」(データまたはプログラム)に影響する損害が、無体物が回復しうるときも第 635 条 2 項の意味で損害であることを明らかにした。
  この判決例は、コンピュータープログラムに損害を与えることは第 635 条違反の犯罪にはならないとしたトリノ裁判所の 1983 年(法が施行される以前)の判決と反対である。

- *第 615 条 3 項によれば、他の目的のために犯罪者がシステムへアクセスを認可された場合や、アクセスが、拒否ないしは制限される以前に、複写の動作をおこす場合でも、複写したデータをデータの保有者の意思に反して後に用いようと決意し、システムにアクセスすることは犯罪である*

  「セキュリティ手段」は、コンピューターシステムの保有者が、システムないしはデータへのアクセスう制限する意思を明らかにする含むいかなる手段(鍵のかかったドア、パスワード) をも意味する。

  いう。

  会社の電子的データをコピーすることは、コピーそれ自体が会社に損害を与えることを意図していないのでコンピューター詐欺(第 640 条 3 項) ではない。 (トリノ裁判所 1997 年 12 月 4 日, in Giur. It. 1998, 1923)

  二つ目の傍論は、ほとんどの論者から、初歩的なパスワードシステムは、すべてのコンピューターに一般的になっているので、それらは、システム保有者の意思を明らかにしているのに十分であると考えられるべきではないと批判されている。
  第三傍論は、コンピューター詐欺の限定された解釈を示唆するものであり、同様の行為(その事案では、会計データの無権限複写)が、犯罪者の不当な利益であり、かつ被害者に現実の損害を発生させることを必要とする。

- *第 615 条 4 項によれば、カードの保有者にテレビ信号を不当に解読できるようにする登録コードのあるカードを保持し、または配布することは犯罪である。* (最高裁判所 1998 年 7 月 2 日, in Ced Cass. 211519).

- *第 392 条によれば、「タイムプロック」をコンピュータープログラムのなかに犯罪者のアフターサービスを得るようにあらかじめ決められた時間にプログラムの機能を停止するために埋め込むのは犯罪である。* (トリノ治安裁判所, 1996 年 5 月 15 日, in Dir. Pen e Proc. 1997, 614).

  「タイムプロック」機能は、コンピューターウイルスではない(それは、自己増幅しない)けれども、それは、あらかじめ決められた時間にコンピューターシステムを損ない、または妨害しうるプログラムであり、なぞらえうるものである。

- *第 635 条によれば、磁気的メディアに保存されたコンピュータープログラムを消去し、または変更することは犯罪である* (トリノ控訴裁判所 1990 年 11 月 29 日, in Foro It. 1991, II, 228).

この裁判所は、損害を受けたものが、バードウエア、ソフトウエアそして、データの記録されている記録メディアを含む「コンピューターシステム」の場合の 1989 年の治安裁判所の決定を確認した。

参考書類

CASO Roberto
Criminalità Informatica: bombe logiche e danneggiamento di software
Foro It. 1991, II, 228

CASO Roberto
Sabotaggio del software e reato di danneggiamento
Foro It. 1990, II, 462.

CORRERA Michele M., MARTUCCI Pierpaolo e CERESI Alessandro
La fenomenologia dei «virus» nei computer crimes - Aspetti criminologici e giuridici.
Riv. polizia, 1996, 545

DI MARTINO Roberto
Tutela del software - Il virus informatico più diffuso al mondo.
Dir. ind., 1995, 1155

FROSINI Vittorio
La criminalità informatica.
Dir. informazione e informatica, 1997, 487

LUSITANO Domenico
In tema di accesso abusivo a sistemi informatici o telematici
Giur. it., 1998, 1923

NUNZIATA Massimo
Il delitto di «accesso abusivo ad un sistema informatico o telematico»
Bologna, 1996

NUNZIATA Massimo
La prima applicazione giurisprudenziale del delitto di «accesso abusivo ad un sistema informatico» ex art. 615 ter c.p.
Giur. merito, 1998, 711

TOSI Emilio
I problemi giuridici di Internet
Milano 1999

第8章 ロシア報告訳

ベーカー &マッケンジー事務所(モスクワ事務所)による情報処理振興事業協会に対するコンピュータ不正使用にかかるウイルスおよび制定法に関するレポート
(訳・弁護士高橋郁夫)

コンピュータウイルスの作成および拡散に対する刑事制定法による制裁

第1節 導入

現在のロシア刑事法典(「法典」)は、1996年に連邦法1996年6月13日No 64-FZとして採択されたものであり、RSFSR(ロシア・ソビエト社会主義連邦共和国-ソビエト社会主義連邦共和国の構成共和国)の1960年刑事法典にとってかわるものである。
法典は、12の編から成り立っており、それぞれが特定の犯罪を取り扱っている。第9編は、「公共の安全および秩序に対する犯罪」には、コンピューター情報の局面に関する犯罪として個別に28章がある (法典の第272-274条).

第2節 一般原則.

ロシアの刑事法典は、会社(法人)に対する起訴を予定していない点および自然人のみが刑事的に処罰されるものであることについて留意されたい。それゆえに、それゆえに、ロシア法人であれ、外国法人であれ、刑事罰を課することはできない。しかしながら、法典は、他人の権利(例えば知的財産権)を侵害する法人の役員の刑事的責任を認めている。
28章が、法典に設けられたのは、コンピューター関連犯罪に関連して刑罰を設けようとしたものである。章は、以下の3つの犯罪を設けている。:

第1項 損害(ハーム)を与えるプログラムの作成、使用、拡散

第 273 条は、ソフトウエアプログラムの作成ないしは存在するプログラムの改変が、*故意に(意図的に)*情報の 刑罰のない(unsanctioned)破壊、妨害、改変、複写を導く、ないしは、コンピューター、コンピューターシステムないしはネットワークの働きを破壊する場合に刑事罰を定めている。同様の刑罰が、そのようなプログラムないしはその可読メディアの使用および拡散に対して適用される。
これらの行為は、同じ条項によって 3 年以下の懲役および 200 以上 500 以下の最低制定法月給-“MSMS”(現在では、だいたい 580 から 1450 アメリカドルの範囲)か有罪の人間の 2 乃至 5 ケ月の収入の罰金を課される。実際の損害を与えた場合には、懲役は、7 年までに増える。

第2項 コンピューター情報に対する違法なアクセス

*法律によって保護されている*コンピューター情報に対する違法なアクセスは、法のく第 272 条によって刑事訴追を課される。
同条のもとで、(i)コンピューター情報を破壊、妨害、変更、複写すること (ii)コンピューター、コンピューターシステムないしはネットワークの働きを妨害することは有罪である。
法典によって「違法なアクセス」として理解されるものについての明確な定義は存在しないけれども、問題の人が情報を検索、精通し、そのような情報を処分する権限を有しない場合、アクセスは、違法と考えられるのが一般である。情報を取得する手段については、定義がなされていないが、実際のパスワードを違法に用いたり、防護システムを突破するように設けられた特別なデバイスを用いたり、機械-可読メディアを 盗んだりすることなどを多分、含んでいる。
違法なアクセスの一つの特定の形は、コンピューターネットワークないしはその他の情報データベースに対する故意の虚偽ないしは、ミスリーディングな情報の無権限の導入である。
上述の条項のもとでの犯罪は、2 年以下の懲役ないし 6 ケ月から 1 年までの強制労働(forced corrected labor)ないし 200 から 500 までの“MSMS”(現在では、だいたい 580 から 1450 アメリカドルの範囲)か、または、有罪の人間の 2 乃至 5 ケ月の収入の罰金を課される複数の人間によってなされる、ないしは、自分の職務上の地位を用いた場合、または、コンピューター、コンピューターシステム、ネットワークにアクセスしていた人の場合には、懲役は、5 年まで、罰金は、500 から 800 MSMS、2 年までの強制労働に過重される。

第3項 コンピューター、コンピューターシステム、ネットワークの操作方法についての利用規則の違反

コンピューター、コンピューターシステム、ネットワークに適法にアクセスした人間のコンピューター、コンピューターシステム、ネットワークの操作方法についての利用規則の違反は、法の第 274 条によって、そのような違反が、法によって保護されているコンピューター情報を破壊、妨害、変更、複写することを引き起こす場合に刑事訴追を受ける。上述の犯罪的所為が、実際の損害を引き起こした場合、同条のもとで有罪である。
その犯罪は、2 年迄の自由の制限ないしは 180 ないしは 240 時間の強制労働、5 年までの仕事、職業の制限の刑罰が課される。
その犯罪的所為が、実際の損害を引き起こしたさいには、その責任は、4 年までの懲役に加重される。
個々の事件において第 273 条および 274 条に関して実際の損害の評価をするときは、裁判所は、関連する一切の事情を考慮に入れ、評価を数量的なベースのみではなく損害の質的な評価をも適用して、評価する。

第3節 ソフトウエア・データベースの複製・悪用防止のための利用可能な保護

ソフトウエアとデータベースは、特に、著作権の保護の対象とし特に論じられており、制定法においても、1992 年 9 月 23 日のソフトウエアとデータベースの法的保護についてのロシア連邦法 3523-1(「ソフトウエア法」)および著作者の権利および隣接権についての 1993 年 7 月 9 日のロシア連邦法 No5531-1(「著作権法」)によって保護が与えられている。
ソフトウエア法は、特に著作権の保護が、ソフトウエアに対して「文芸作品」として拡張されると述べている。ソフトウエアは、ソフトウエア法のもとで、「データおよび指令のセットで、電子計算機(コンピュータ)および他の計算デバイスにおいて結果を受け取るための機能を果たためのオブジェクトフォーム」と定義されている。ソフトウエアは、また、プログラムをプロセッシングする過程得られる 準備的素材およびそれによって生み出される音楽・映像的対象物(スクリーン)も含む。ソフトウエア法によって認められる法的保護は、ソースコードおよびオブジェクトコードを含むいかなる言語およびいかなる形態のすべてのタイプのソフトウエア(基本ソフトおよび複雑なプログラム)に拡張される。
著作権法およびソフトウエア法のもとでは著作者(乃至は相続人)は、作品に関して作品を*いかなる形態*、*手段*により利用することについての排他的権利を有する。作品の排他的利用権は、とりわけ、作品(の一部であれ)の複製(複製権)、翻案、アレンジないしは改作権(modify, arrange or otherwise adopt a work) を含む。著作権法第 16 条に述べられている権利は、著作権法 18 ないし 21 条において述べられている例外(ないしは自由利用)の場合以外は著作権者の契約を通じてのみ移転される。

第4節 ソフトウエア法および著作権法の実際の適用

ソフトウエアないしはデータベースの保有者の認可なしで(いかなる形態ないし手段で) ソフトウエアないしはデータベースを利用することは、その侵害になる。
民事制裁が課せられるのに加えてロシアの法律は、ソフトウエアの無権限利用は**刑事的犯罪**であるとしている。
ロシア刑事法典の第 146 条は、著作権および隣接権の対象の実際的損害を発生させる違法利用の場合の刑事的制裁を定めている。それゆえに争いがあコンピューターウイルスの作成は、第三者のオリジナルソフトウエアを改変するのであり、著作権侵害になると考えられる。
これらの行為は、同一の条文によって、2 年までの懲役ないしは 180 時間から 240 時間までの強制労働または 200 ないしは 400“MSMS”(現在では、だいたい 580 から 1160 アメリカドルの範囲)、または有罪の者の 2 ないし 4 ケ月の収入分の罰金が課せられる。
ロシア刑事法典のこれらの規定は、(近頃起草されたので)比較的新しく、それゆえに与えられている保護について信頼できる実務的経験はほとんどない。 しかしながら、ロシアの内務省(経済犯罪対策部)といくつかの外国のプロデューサーと著作権の執行について協力した例があり、著作権侵害者は、刑事手続で審理されて判決がくだされた。しかしながら、コンピューターウイルスに関連して著作権侵害がなされた事案は知らない。

第5節 ロシアにおけるコンピューター犯罪の刑事訴追の実務

コンピューター犯罪についてのロシア刑法典の上記の条文は、新しいものである。それゆえに、いまだ適用されたのを聞いたことがない。
新法典が、施行される前に、犯された犯罪があり、法典の第 272 条によって訴追される可能性があった。
例えば、ロシア市民の ウラジミール・レビン と同胞は、ニューヨークの“シティバンク・アメリカ”から大金を盗むことを共謀した。1994 年の 6 月から 9 月にかけて、犯罪者集団を結成し、ロシアのサンクト・ペテルブルグ市所在のパーソナルコンピューターを用いて銀行の対無権限(セキュリティ)アクセスシステムをハックした。合計して彼らは、シティバンクの銀行口座から約 1000 万アメリカドルを違法に移転した。レビン氏は、英国に旅行した時に逮捕され、英国で裁かれた。
損害を与えるコンピュータープログラムの作成の具体例は、ロシアの法廷の実務において 1983 年に見受けられるのみであるかもしれない。自動車工場のプログラマーが、工場のコンベアーに供給する部品をコントロールするために提供されるソフトウエアに意図的に変更をなした。その行為により、100 台の車の製造に欠陥を引き起こした。その当時存在した古いロシア連邦

共和国の刑事法典には、コンピューター犯罪が存在しなかったので、プログラマーは、公共の財産を毀棄したとして、発生した損害の賠償と 3 年間の懲役(執行猶予付)となった。現在では、刑事法典の第 273 条が、その事件に適用される。
コンピューターに関連する刑事法典の条文を利用するにあたっての主要な問題点は、ロシアの判事および捜査スタッフにおける経験の欠如である。コンピューター犯罪と戦っている部門は、取り扱いを始めたばかりである。さらに犯罪者のコンピューターのレベルは、捜査官のレベルより平均的にに高い。それゆえに、無権限アクセスないしは、損害を与えるプログラムなどの製造・拡散について参加しているという証拠がないために起訴が不可能になることもしばしばである。

第9章 各国のコンピューターウイルスに対する対応の比較考察

第1節 コンピューターウイルスの投与に対する分析の視点

すでに各国におけるコンピューターウイルスの対応については、検討した通りである。そこでコンピューターウイルスの作成・投与に対する刑事法的対応の方向性としてどのようなアプローチで検討していくことができるかである。
この点については、

(1)コンピューターウイルスをデータ・プログラムの改変といった方向からとらえるもの

(2)無権限アクセスの方向から考えるもの

(3)コンピューターに与える損害(ないしはそのコンピューター処理による業務に与える損害)という視点から考えるもの

という視点から分析できるものと思われる。
これらの考察の視点から、それぞれの各国の報告をまとめていくことにする。

第1項 データないしはプログラムの無権限改変というアプローチ

これは、アクセス制御のなされているデータを権限を有しないで、改変・消去を含む変更をするという観点から、刑事罰を課する場合をいう。データ自体のインテグリティの確保という観点から、その破壊、改竄、信頼性の喪失、使用の干渉などを図る行為をそれ自体に着目して、刑事罰を課することになる。

このアプローチを代表する規定としてカナダの刑法典の規定を例にあげることができる。カナダ刑法典においては、１９８５年の「データに関する損壊」の罪が、かかるアプローチから、いわゆる無権限改変行為を処罰するものであり、条文においては、データの重要性について（例えば、権利義務に関するか否かなど）の限定はなく、また、その損壊の定義自体が、改変、または、動作の干渉を含んでいる点で、(判例として問題になった事案はいまだないとしても)こ

の規定の射程距離は広いものといえる。したがって、電子メールウイルスおよびマクロウイルスへの可罰性を示唆するものであるということができる。

また、、一定の認識と意図とが必要とされているが、英国のコンピューター不正使用法の第 3 条も同様のアプローチを採用しているということができよう。同条は、「(a) 無権限で、コンピューターのコンテンツに改変を加えるいかなる行為をした場合」に適用されることとされている。そして、メリッサを代表とするいわゆる電子メールウイルスに対しても争いのある余地はあるが、刑事罰として可罰可能であると報告がなされている。

フランスにおいては、新刑法典第 323-3 条において、データの不正操作罪として、不法にデータを入力したり、不法に消去もしくは改変する行為についての処罰がなされている。電子メールウイルスおよびマクロウイルスにこの条文が適用されるかどうかは、適用が可能と報告されているが、なお不明なところも多い。

また、ドイツにおいても、刑法 303 条 a が、データの無権限改変を規定している(データを違法に消去し、隠蔽し、使用不能にし、または変更したものを処罰する)。その点で、データの無権限改変に対するアプローチをも含むといえる。しかしながら、これが電子メールおよびマクロウイルスに適用される場合には、ハードウエアが正規の方法で使用できないほど、使用可能性が、継続的に侵害される必要があることが報告されている。

ロシアについては、破壊をもたらすような破壊、妨害、改変、複写を導く場合に、刑事罰の成立を認めている(第 273 条)。実際の適用事例がなきいので不明であるが、この条文の限りでは、電子メールウイルスは、その動きのみで複写をもたらすプログラムとして同条の規定が適用されるものと思われる。

イタリアにおいては、第 392 条によって、「コンピュータープログラムの不当な変更ないしは消去」が処罰されているが、これは不当な目的のためのものであり、単なる嫌がらせなどの場合では、成立しないものとされており、電子メールおよびマクロウイルスへの適用は否定さている。むしろ、この改変については、（３）とも関連するが、損害を与える改変であることが必要とされている。

米国における各州の定めについては、いろいろな方向性が見て取れる。データ・プログラムの改変というよりも、むしろ、コンピューターウイルスについての独自の規定としてさだめていく方向性が見受けられる州も多い。その際には、プログラム・データの汚染、リソースの消費、データ送信などがいわば、ウイルスの結果として必要になることが注目される。

全般的に見て、データを改変したこと自体で犯罪の成立を認める方向性をとる国（カナダ、イギリス、フランス、ロシア？）となんらかの実害を伴う改変であることを必要とする国（ドイツ、イタリア）があるといえよう。

また、データを改変しただけで、犯罪の成立を認めるアプローチを採用する国においても、主観面との関係で細かく見ていくと、それぞれ特徴がある。

アメリカのモーリス事件が、ウイルスの投与について故意があれば、犯罪が成立するものとしており、また、フランスの第 323-1 条 2 項が、不正アクセスまたは滞留によってデータの消去もしくは改変、またはシステムの動作の悪化が生じた場合、すなわち結果に対して故意がない場合にも、かかる犯罪が成立するとしているのに対して、英国は、そのような一定の意図を要件として、そのような結果に対して過失しか有しない場合の処罰を除外している点が特徴である。ドイツは、故意犯としていながらも、危険回避のための措置を講じないような向こう見ずな行為者に対しては、故意犯が認められるのであり、これは、英国の否定する立法例と正反対であるといえる。

第2項　無権限アクセスからのアプローチ

米国においては、この点が、モリス事件の際に争点になっている。結局、無権限アクセスを意図したことが必要で、損害をその結果として惹起すれば、連邦法１０３０条第(a)項第(5)号(A)が適用されるとしたのである。逆にいうと、損害についての認識さえも必要とされないのである。これは、ウイルスについての刑法の適用について、無権限アクセスからのアプローチとして位置づけることもできるであろう。
カナダにおいては、いわゆる電子メールウイルスの場合についての適用の可否は不明であるが、無権限アクセスの規定が、データ損壊を犯す意図で、コンピューターを使用する場合として、適用される可能性のあることが報告されている。
英国においては、アクセス権限を限定的にとらえること(具体的にいえば、メールサーバーに対して、不正な動きをするプログラムについては、アクセスを許可しないという限定的な考え方)が前提となっているということができる。この解釈については､異論もあり得るところであり(現に、下級審と貴族院での判断が分かれているところである。)、なお明確であるとはいえないが、無権限アクセスに関するミスユース法第１条の適用の可能性が指摘されている。
ドイツにおいては、202 条 a のデータの権限者は、データを生み出した者と解されており、その関係では、そのような電子メールウイルスは、なんら権限者のアクセスを制限しているものとはいえないとされている。
ロシアにおいては、第 272 条の規定が電子メールウイルスに対して適用されるかについては、その具体例からして否定されるように思われる。むしろ、アクセス権限の具体的な違反から犯罪の成立を認めるものとしては、第 274 条によって操作方法についての利用規則違反についての犯罪成立を認めており、かかる方向からの刑事罰が他の国の無権限アクセスからのアプローチに匹敵するように思われる。ただし、そのような操作方法についての利用規則違反がこのような場合に適用されるかについては明らかではない。
イタリアにおいては、コントロールを行為者が得るものではないため、電子メールおよびマクロウイルスは、無権限アクセスを定める第 615 条 3 項の該当する行為ではないと報告されている。
フランスにおいては、不明である。
概して、無権限アクセスのアプローチについては、電子メールのサーバーが、基本的に、どのような電子メールでもデータとして受領するという性格にも関連して、否定される場合も多いということができよう。

第3項　損害等の観点から

コンピューターに対して、損害を与えるという観点から評価する場合、具体的には、損害を与えるものが、コンピューターという有体物であるかいなか、また、ネットワークでの動作速度の遅延について、損害をあたえたと評価するかという点で問題がある。

米国においては、損害の額によって適用の条文がことなっていることもある。しかしながら、損害の認定がきわめてゆるやかなように思われ、その限りで、むしろ、実害の発生というアプローチであると位置づけるのは、妥当ではないように思われる。

カナダにおいては、むしろ、1985 年に「データに関する損壊」の罪が制定される以前においては、、データも「財産」として、その財産の活用が妨害されたとして犯罪を認めていた(国対 Turner 事件 1984 年)。ただし、現在では、データ自体の損壊が適用されるものと思われる。

英国においては、この点について、損害を与える対象物が、かならずしも有体物である必要はないことは、認められていたが、その解釈上の問題点を整理するために、コンピューターミスユース法が制定された経緯がある。実際の問題としては、刑事的損害法は、一般のコンピューターウイルスには適用される可能性は乏しいであろう。

イタリアにおいては、一般論としては、メリッサ型のウイルスが、損害をあたえうるものであることが一般論としては肯定されているが、ウイルスの行動が自己複製であれば、重大な結果を惹起しない限り、損害をあたえたものと評価されないであろうとされている。

一般的にいえば、カナダおよびイギリスなどで、データの損壊自体を損害として特別に規定が済んだこともあり、この点について、あまり意識されなくなってきていると評することができるかもしれない。

第2節 コンピューターウイルスの拡散についての各国の対応

ウイルスの拡散については、

(1)刑罰法規の適用において、各共犯などからとらえる立場

(2)それぞれ、有害なプログラム等の通信装置を用いての拡散について特別の規制を有している立場

から検討される。

第1項 コンピューター犯罪規定の適用

コンピューターウイルスの拡散行為に対してコンピューター犯罪規定の適用ないしはその共犯規定の適用があるかどうかついては、各報告書において、あまり明らかではないところである。アメリカにおいては、例えば、連邦法の構成要件からしても、通信、配布、伝送がメルクマールになっており、それ自体において、無権限アクセスの規定が直接的に適用されるものと考えられる。

イギリスにおいては、レポートについての質疑応答において、報告担当者である Graham Smith 弁護士より、無権限アクセスないしは改変を起こそうとウイルスを投与することが、1990 年法の犯罪の基礎であり、それゆえに、第三者の作成したウイルスを公表したとしても 1990 年法においては、犯罪にならないという報告がなされている。

ドイツにおいては、単なるデータのアップロードのみでは、犯罪の成立は困難であるが、ウイルスの明示、破壊の煽動などの場合に、ウイルスの取得者による投与があった場合については、教唆犯の成立の可能性があるが、そのような場合でなければ、逆に配布行為単独での処罰は困難であるということになる。

その余の国については、不明である。

第2項 特別規定の適用のアプローチ

ウイルスに関する行為については、作成・投与・拡散があることはすでに見たが、拡散については、特別法によって、規制するトイウアプローチも存在する。

そのようなアプローチとしてはイギリスにおける電気通信法 1984 第 43 条の規定に注意すべきである。この第 43 条(1)は、「(a) 公衆の電気通信システムを用いて、ぞっとするほど腹立たしい(grossly offensive)ないしは、下品な indecent、わいせつな obscene、脅迫的な menacing メッセージないしはものを送信する」としており、従前のウイルスの犯罪においても、コンピューター不正使用法とともに、この条文の適用がなされていた。拡散行為が、かかる送信行為として、同条が適用されることはありうるものと思われる。

第10章 わが国における刑事的対応についての示唆

第1節　わが国のアプローチについて

各国の刑事的規制についての報告で検討したように、コンピューターウイルスに対する刑事的対応の手段としては、

(1) コンピューターウイルスを無権限改変といった方向からとらえるもの
(2)無権限アクセスの方向から考えるもの
(3)コンピューターに対して与えた損害という視点から考える考え方

の三つの観点から考察を加えうるものとなる。

また、実際に国際的な観点からの検討が必要になっていることが示唆されているということができよう。

(1)については、わが国において、これに対応する法律を有しない。電磁的記録不正作出および供用罪(刑法 161 条の 2)および電磁的記録の毀棄罪(刑法 258 条・259 条)が、類似するアプローチともいえそうである。その要件についての比較検討が必要となるであろう。
(2)については、不正アクセス禁止法との関係が問題となる。
(3)これについては、「電子計算機損壊等業務妨害罪」「偽計業務妨害罪」「文書毀棄」「器物損壊等」のそれぞれの適用範囲について検討することが必要となる。

第2節　刑法の適用が問題となる具体的な行為

具体的に悪意あるプログラムを考えた時に、刑法の適用が問題になる行為としては、かかるプログラムの製造、投与、拡散があげられる。 そもそも、なにをもって投与といい、なにをもって拡散というかであるが、被害コンピューターを想定して、そのコンピューターに直接働きかけるものを投与といい、被害コンピューターを考慮せずに、有害なファイルを例えば、ホームページ上にダウンロードできるような形で置いていくのが拡散ということがいえるであろう。

一般的には、加害の意図がある場合には、製造、投与が同一人によってなされることが多いであろう。その場合には、製造が、投与という実行行為の準備的な行為であるということになりそうである。そうすると、まず、投与行為がどのような刑法の規定によってカバーされるのか、ということになる。そして、その規定の適用が検討されたあとで、拡散、製造がどのようにとらえることができるかということになる。さらに悪意あるプログラムの性質によって、わが国の刑法の規定が左右されることがあるのかという問題があり、もし、規定の適用でいわば、「漏れ」があるとしたら、それはそのまま放置しておくことが許されるのかということである。

第3節　具体的なわが国のアプローチの検討と限界

第1項　データの無権限改変からのアプローチ

データの無権限改変というアプローチから考えると、日本刑法においては、昭和 62 年改正による電磁的記録の不正作出・同供用の規定および毀棄の規定が対応するものといえよう。

まず、昭和 62 年の改正における「電磁的記録」の定義であるが、これは、「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるもの」をいうとされている。これは、一定の記録媒体上に情報またはデータが記録、保存されている状態であり、その内容から、データや情報ともに含むのであり、諸外国の保護の対象とされているデータと比較して、ほとんど同義である(この点について直接比較するものとしてカナダ報告書 参照)。

しかしながら、その一方で、その電磁的記録については、電磁的記録の不正作出・同供用の規定においては、その記録が「事務処理の用に供する権利、義務又は事実証明に関する」ものであることが必要とされており、また、毀棄の規定においては、「公務所の用に供する」もの、もしくは「権利義務に関する」ものであることが必要とされる。

私たちの考察する「悪意あるプログラム」の動作結果について考えると、むしろ、上記のような電磁的記録に影響を与えない場合の問題のほうがはるかに多いものといえよう。その意味で、わが国で、悪意あるプログラムに対してデータの無権限改変のアプローチが採用されているとはいいがたいのである。この点で、英国において「コンテンツに対する無権限改変」がそれ自体で処罰されているのと比較する必要が有る。英国においては、データに関するアクセス・コントロールが基準に権限が考えられていてそれが改変のメルクマールにされていることは特長がある。立法過程からもわかるように、行為の実際の結果を考えないで、刑事的に取り扱えるようにする意図があったのである。

第2項 不正アクセス禁止法とコンピュータウイルス

また、諸外国において、コンピューターウイルスのかなりの動作については、無権限アクセスで処理することが可能であるという議論を紹介してきた。

しかしながらわが国において、無権限アクセスに対する対応規定であるいわゆる不正アクセス禁止法においては、かかる悪意あるプログラムに対する対応ができないことに注意すべきである。特定電子計算機に対するアクセス制御機能の回避もしくは他人の識別情報によるアクセスという観点から規制さており、個別のメールサーバーについてのアクセス権を前提として概念が構築さているわけではない。コンピューターウイルスが、メールウイルスの形でやってきたとしても、不正アクセスになるわけでばないし、また、フロッピーの頒布という形で投与されたとてしも、不正アクセスになるわげではないのである。

第3項 「業務妨害」からのアプローチ

偽計業務妨害または威力業務妨害罪(刑法第 233 条・第 234 条)の検討

偽計業務妨害罪・威力業務妨害罪の構成要件と解釈の一般論

また、コンピューターウイルスの作成・投与が問題となりそうな条文としては、刑法２３３条のいわゆる偽計業務妨害罪または刑法 234 条の威力業務妨害罪がある。偽計業務妨害罪・威力業務妨害罪の構成要件は、

（1）偽計を用いて (または威力を用いて)
（2）「業務」を
（3）妨害した
ことである。

1 偽計を用いて (または威力を用いて)

ここで、「偽計を用いて」という要件の解釈が問題となる。まず、「偽計を用いて」については、欺罔に限定する説、欺罔に限らず誘惑をも含むとする説、欺罔・誘惑に限らず人を陥れる一切の方法をいうとする説がある。また、この要件の解釈は、人に対するものであることを要するか、それともおよそ不正な手段一切ということになるか、という観点からの対立とも考えられそうである。電子計算機に当てはめると、「人に対する偽計」と「電子計算機に対する加害行為」というのが峻別されるという立場もなりたちうるであろう。しかし、判例においては、このような峻別するような態度は採用されていない。この点については、いわゆるマジックホン事件[64]は、「マジックホンと称する電気機器を加入電話回線に取り付け使用して、応当信号の

[64] 最決昭和 59 年 4 月 27 日刑集 38 巻 6 号 2584 頁

送出を妨害するとともに発進側電話機に対する課金装置の作動を不能にした行為が(略)偽計業務妨害罪にあたるとした原判断は正当である」としている。判例の立場としては、偽計とは、およそ不正な手段一切を用いることをいい、電子計算機損壊等業務妨害罪は、電子計算機に対する直接の加害行為で「動作阻害」という中間結果を発生させた過重類型ということになる。

また、「威力を用いて」とは、「人の意思を制圧するような勢力」をいうとされており、その内容は、犯人の威勢・人数、および四囲の状況よりみて被害者の自由意思を制圧するにたるものとされている。また、「威力を用いて」となっている関係で、直接業務に従事している人になされることを要しないと解されているところである。怒号をあげたりというのは「威力を用いて」という概念に当てはまるであろうが、詳細に見ていくと、限界的な事例がある。判決例によると、工場の配電用スイッチを切断する行為、弁護士の重要書類在中の鞄を奪取する行為、猫の死骸を事務机の引き出し内にいれて被害者に発見させる行為などが、限界事例ではあるが、威力業務妨害罪とされている。ウイルスについていえば、そのウイルスの動作が被害者の畏怖するような性格のものであるか否かで、威力とされるか、偽計とさるかということになるのであろう。

現実に、コンピューターウイルスに関連する行為が、偽計ないしは威力業務妨害罪として捉えられる事案が増加している。その具体的な例を挙げると、コンピューターウイルスを添付した電子メールを送り付けた事件で、少年が、威力業務妨害の疑いで逮捕されたという事件が報道されている[65]。

2 業務性

業務性については問題がなかろう。

3 妨害の結果

また、ここで、(3)妨害したという「妨害の結果」についての解釈も問題となる。

条文上は、「その業務を妨害したる者」と明示しており、業務妨害罪は(形式的には)侵害犯であるということになる。しかし、問題は、その「結果」とはなにかということであろう。判例からすれば、刑法 233 条の規定する業務妨害罪は、虚偽の風説を流布しまたは偽計を用い人の業務の執行またはその経営に対して妨害の結果を発生しむべき虞ある行為をなすにより成立し現実に妨害の結果を生ぜしめたることを必要としないということになる。

この場合に侵害犯が具体的危険犯の形態を利用して表現されているということになるのであろう。その結果、被害が軽微でも結果が発生させる虞があったとされているのである。

ただし、この結果が、具体的にどのような「妨害の結果」を発生しむべき虞ある行為である必要があるかというとはっきりしないところである。電子計算機の動作との関係で論じる場合に、妨害が、「個々の判断作用を害するにすぎない」ものである場合に、結果発生の危険があったといえるかという点が問題となる。この点については、電子計算機損壊等業務妨害罪についての記述であるが、「何らかの加害行為によって電子計算機の働きが害されたとしても、その結果が業務遂行上の個々の判断を誤らせるにとどまる場合はいまだ業務を妨害したものとはいえない」とする立場がある。この立場をとるとなると、データに対するアクセスを遅延させる行為については、本罪で対処しきれない可能性があろう。もっとも、この立場であっても、意図しない指令を発する場合(具体的には、電子メールのアドレス帳を除き、そのアドレス帳の対

[65] 2000/02/23 日本経済新聞 夕刊

象にメールを送付する)には、そのメールが、ほんの少しの数であれば別であろうが、一般的に、業務妨害の結果が生じたといえるように思われる。わが国においては、一般論としては、実害を伴うウイルス(ファイルを消去してしまうという性質を持ったものはもちろん、メールを多数の者に送信するというものであっても)についてはかなりの部分が、業務妨害罪でカバーされるものといってかまわないであろう。

電子計算機損壊等業務妨害罪の検討

1 構成要件と解釈の一般論

電子計算機損壊等業務妨害罪(以下、本罪という)の構成要件は、
1)電子計算機に向けられた加害行為
2)電子計算機の動作阻害
3)業務妨害
の 3 つであり、そして、それらが故意で貫かれていることが犯罪の成立に必要である。

個別に検討すると
1)電子計算機に向けられた加害行為
これは、
「電子計算機もしくはその用に供する電磁的記録の損壊」
「電子計算機に虚偽の情報もしくは不正の指令を与え」
「またはその他の方法」
などが方法として上げられている。

一般的な悪意あるコードの動作について考えたときに、ウイルス、ワームなどは、上の三つのどれかに当たることは十分に考えられる。もっとも、上記の条文からすると感染コンピューターに対する直接な動作であることが要件であるように思われる。電子計算機に「向けられた」加害行為とされているのである。また、現に、的場・河村著「コンピュータ犯罪 Q&A」109 頁は、「コンピューターに直接に向けられた加害行為」としている。しかしながら、一般には、積極的に悪意有るプログラムを作動させることもあれば、プログラムに忍び込ませておくこともあり、しらずにダウンロードした人間が知らないうちに拡散させてしまうというものであろう。この「向けられた」という要件がどの程度、要件として必要なものであるか、逆にいえば、プログラムの拡散を予知して公開していれば、コンピューターにむけられた加害行為であると解することができるものと考えられるが、立法の際の意図とは異なっている可能性があり、議論を呼ぼう。 的場・河村著「コンピュータ犯罪 Q&A」123 頁は、悪意あるプログラムの作成が、加害手段となることを認めているが、感染コンピューターに直接与えることを前提としており、どの程度、ネットワーク感染を意識しているものか疑問である。

2)電子計算機の動作阻害

この動作阻害は、「使用目的に沿うべき動作をさせず」もしくは「使用目的に反する動作をさせる」こというものである。問題は、この「使用目的に」沿う、とか、反するという場合の「使用目的」として、どのような具体的なレベルが念頭におかれているかであろう。 この点

について、使用者の目的を前提に考える使用者説と、設置者の目的をいうという設置者説とがあるとされている。例えば、5 時にメールを書こうとしたところ、アルプス一万尺のメロディーが流れてきて、入力ができなくなる場合には、この条文にもあたるかどうかについての問題が生じるであろう。また、誰の目的かという論点とは別に「動作」とは、「電子計算機の機械としての働き、すなわち、情報処理のためにおこなう入出力、演算等の機械としての働きのこと」であると説明する立場もある（河村・注解刑法　頁)。具体的な解釈としては、設置者説と同様の傾向になろう。具体的な業務遂行を保護の対象とするのであるから、具体的な使用者の目的を前提として考えるという立場を採用したとしても、アルプス一万尺の例のようなきわめて具体的な指令の実行ができない場合は含まないように思える。 立法過程における米沢説明員の説明でも「構成要件の明確性を重要視して、いわゆる中間結果の発生を構成要件に取り組んだ」と説明してシステムダウンや三角形を作ろうとして四角形になった場合をいうと説明されていることでもある[66]。

また、「他人のパスワードを用いて、データベースの情報を不正に入手すること、あるいは他人の電子計算機を無断で使用することなどは、電子計算機による情報の提供ということ自体は行われており、業務遂行の外形的妨害は生じていない」として「使用目的に反する動作をさせて業務を妨害したことにはならない」と記述されており、動作の効率の低下・若干の混乱を「動作阻害」とは、いえないものと考えられる。

3)業務妨害

この業務妨害については、偽計業務妨害罪での検討と同様である。業務遂行上の個々の判断を誤らせるだけでは妨害とはいえないであろうという点については、具体的な適用において、問題が生ずるおそれは払拭しきれないといえよう。

4)主観的要件

これらの行為のすべてが故意によって貫かれなくてはならないのであり、とくに業務妨害の故意については、問題が生じよう。また、数値を読み違えた RT モーリスの事件などの場合にどのような対処をするかという問題もあろう。

2 電子計算機損壊等業務妨害罪の判例

もっとも、具体的な判例を見ていくときに、上記の説明がそのまま通用するかどうかは問題である。

この条文が適用された事案としては、コンピュータ制御式旋盤機の肯定プログラムを消去・改竄し、会社の製造業務を妨害した事案（京都地峰支部平成２年３月２６日判例集未登載)、雇用保険失業給付受給者がゴルフパターなどを用いて公共職業安定所内で暴れ、労働省総合的雇用情報システム受理端末送致のキーボード、プリンターなどを損壊して同安定所職員らの職務を妨害した事案（山口地徳山支部判決平成８年８月１０日）などが紹介されている。

[66] 的場・河村著「コンピュータ犯罪 Q&A」126 頁

近頃の判例で注目すべきものとして、朝日放送ホームページ不正書換事件判決（大阪地裁平成 9 年(わ)第 2305 号電子計算機損壊等業務妨害，わいせつ図画公然陳列被告事件)がある。 被告人は，朝日放送株式会社（大阪市）のホームページ内の天気予報画像をわいせつな画像に置き換えたという事案である。この被告人の行為に対して、「ハードディスク内に記憶・蔵置されていた天気予報画像のデータファイル 9 個を消去して損壊する」とともに，(省略)「右利用者らが右わいせつな画像のデータファイル 5 個分のデータを受信してこれを再生閲覧することが可能な状況を設定し、右ホームページにアクセスしてきたＢら不特定多数の者にこれを再生閲覧させ、もって，人の業務に使用する電子計算機の用に供する電磁的記録を損壊し、かつ、同電子計算機に虚偽の情報を与え，電子計算機に使用目的に反する動作をさせて人の業務を妨害する」とした。

この朝日放送の事件においては、朝日放送のホームページにおいては、その天気予報の情報を伝えることがその業務の本来の目的であり、それが損なわれると「使用目的に反する動作をさせる」と解したことになる。使用目的を、どのような情報をつたえるかという点までに具体化して論じている点は注意しておく必要があるであろう。

第4項　コンピューターウイルスの拡散について

コンピューターウイルスについては、それの作成以外に、むしろ、それをどのようにして拡散させるかという点が実際の被害のあり方に影響していく。メリッサウイルスが、それがアダルトサイトのパスワードファイルであると称して、ニューズグループに投稿されたというのが、きわめてその被害が拡散した理由であるといえるであろう。では、ウイルスの拡散行為は、刑法的にどのように把握されるかということである。

前項において、ウイルスの投与行為が、そのウイルスの効果にもよるが、威力(または偽計)業務妨害として把握できる場合が多いものと考えられることを見てきた。拡散行為は、その共犯として捉えることができるものと考えられる。また、その拡散が被害を惹起することが確実とでも言うべき方法ないしは態様であった場合には、それ自体、投与行為と同視し、実行行為そのものということがいえるであろう。

第4節　コンピューターウイルスの刑事法的対応に対する示唆

第1項　わが国の刑事法的対応の限界

すでに検討したようにわが国では、一般の業務妨害罪によって、コンピューターウイルスの投与および拡散についてカバーできるものと考えられる。しかしながら、この場合でも、実際の適用上の問題と、本質的な限界の 2 つの問題点があることについては留意しておく必要がある。

実際の適用上の問題点というのは、その「業務妨害」の文言の解釈で見た問題点である。前述したように判例の立場を前提とする限り、業務妨害罪は、実質的に抽象的危険犯として解されている(それゆえにコンピューターウイルスによる不都合が、かなりの程度構成要件該当性を、満たすものと解されているのである)。しかしながら、それでも、妨害が、「個々の判断作用を害するにすぎない」場合には、抽象的危険さえも存在しないものと解する立場が存在する。このような立場を前提とすると、作用が微妙なウイルスについては、業務妨害さえもないと解される虞がある。もっとも、マジックホン事件を前提とする時、わずかな作用阻害の虞でも、業務妨害が成立するという立場も可能であろう。どちらにしても、解釈の余地が存在していることは否定しえないと思われ、それ自体が望ましいのかいう問題もある。また、業務妨害の結果についても、故意の対象となるので、投与ないしは拡散行為について認識していないと有罪とはならない。実験でウイルスを作っていたのが、うかつにも流失してしまったという場合には、刑事的な処罰の対象とはならないものと考えられる。そのため、モーリス事件のような場合は、業務妨害の成立が否定される可能性が高いことになる。その結論が妥当か、という問題もある。

本質的な限界というのは、業務「妨害」という性質をメルクマールにするので、むしろ、悪意あるプログラム自体の情報の取得、流出という行為に対する対応迄は対応しきれないと考えられることである。トロイの木馬やバックオリフィスなどは、その性質上、情報の取得、流出という問題点に対して正面から対応しきれない。(なんら悪さをしなくても情報が流出する自体で業務が妨害されるということもできなくはないであろうが、妨害概念が拡散し過ぎるという批判がなされるであろう。)

第2項　限界の克服を目指して

上述のような問題点をどのように位置づけてておくかという問題がある。まず、現在の判例の立場を前提として、実際の業務の妨害を許容される限りで、コンピューターウイルスや悪意あるプログラム一般に対する対応を考えるというアプローチがなされうるであろう。現在の判例が、業務妨害の結果および手段に対して広範な解釈を取っていることから、実際上の問題点というのはあまり現実にはおこりえないという考え方もありうるであろう。

それに対して、業務の妨害やその手段についての解釈をそれ自体の文言の意味を維持して厳格にしようというアプローチからは、現実の適用に対して、問題がおこりうる可能性がある。また、故意との関係で結果発生の認識がない場合についてもどのように対応するかという問題もある。

このような観点から、コンピューターにおいて保存されている情報について、個々の情報データのアクセス権を考えて、これがないのに、改変消去することを一つの犯罪とするというアプローチも可能であろう。電磁的記録については、アクセス権の設定を要件に、その改変・消去自体を犯罪とするのであり、英国、アメリカのいくつかの州のアプローチが参考になる。

もっとも、そのようなアプローチをとったとしても、コンピューターの利用者の意思に反したデータの活動という問題は残る。バックオリフィスやトロイの木馬については、何らかの規制を考えるという点については、異論がないとしても、ある種のスクリプトやクッキーなどは、利用者にことわりなく利用者の個人情報を流出してしまうのである。これらに対してどのような対応がのぞましいか、それとウイルスとの関係についてどのように認識すべきかなどという問題について議論すべき時期にきているような気がするのである。

(第 10 章　担当　弁護士高橋郁夫)