

コンピュータウイルスを中心とする情報セキュリティ  
に関する米国各州の法制度調査

1999年12月

情報処理振興事業協会  
セキュリティセンター

## 目次

<b>第一章</b>	<b>総論</b> .....	<b>4</b>
1.	連邦法及び州法でのウイルスの作成、公開、配布に関する規約.....	4
2.	米国におけるコンピュータ犯罪の実態.....	5
3.	コンピュータ・ウイルスの実態.....	7
	コンピュータ・ウイルスの種類.....	7
	ウイルスによる被害.....	8
	各コンピュータ・ウイルスの特徴.....	8
	ウイルス作成者.....	9
4.	代表的なウイルスによる大型事件.....	10
	メリッサ.....	10
	チェルノブイリまたは CIH.....	12
	WormExplore.Zip.....	12
	バブル・ボーイ.....	12
5.	ウイルス対策ソフト産業.....	12
<b>第二章</b>	<b>連邦レベルにおける法規制及び執行</b> .....	<b>14</b>
1.	背景.....	14
2.	連邦関連法の成立、修正.....	15
	中核法の確立.....	15
	86年の改正で CFAA へ.....	16
	1994年改正とガイドライン設定.....	16
	1996年、NIIPA 制定.....	17
	連邦政府によるコンピュータ犯罪対策法令.....	18
	その他関連法.....	19
3.	連邦コンピュータ犯罪対策プログラム.....	19
	NIPC.....	20
	CERT.....	21
	スパイ行為対策センター.....	21
	その他.....	22
4.	問題点.....	22
	財政・人材不足.....	22
	管轄区域.....	22

被害者の消極的・懐疑的な態度 .....	23
未成年による犯罪 .....	23
犯罪の簡易化、深刻化 .....	23
<b>第三章 州レベルにおける規制 .....</b>	<b>25</b>
1. 州法の整備状況 .....	25
2. 州の条例 .....	26
カリフォルニア州 .....	27
イリノイ州 .....	28
フロリダ州 .....	29
ジョージア州 .....	29
ニューヨーク州 .....	30
3. 問題点と解決策 .....	31
管轄区域間の調整 .....	31
法執行体制 .....	31
資金不足 .....	32
民事訴訟の奨励 .....	32

## 第一章 総論

### 1. 連邦法及び州法でのウイルスの作成、公開、配布に関する規約

米国にはウイルス配布と教育に関する連邦法及び州法が存在し、ウイルス作成、配布、教育を安易に実施させないような効果を持っている。連邦及び州法において、ウイルスの作成、配布、教育そのものを違法とは定めていない。しかし、その結果として第三者が意図的に損害を起こした場合は、ウイルスを配布したものの、教育を行ったものの、作成した者が罰せられる場合がある。従って、ウイルスの作成、または、不特定多数の者に対してウイルスの配布及び教育を行うことには多大なリスクを伴うことになる。そのため、何らかの損害が与えられた場合の罰則を定める法律が牽制力として働き、ISP（インターネット・サービス・プロバイダー）や個人によって自主規制が行われている。

連邦法は、最初 1984 年に制定されて以来、何度か修正が加えられ、今日に至っている。その経緯に関しては第二章 2.において詳しく述べる。現在、コンピュータ・ウイルス犯罪に適用されている連邦法は、タイトル 18、チャプター 47、セクション 1030 の(a)の(5)となっており、以下に原文とその訳を示す。ここでも明らかのように、「コンピュータ・ウイルス」という定義は用いられておらず、その他の犯罪法と同様、「どのような被害がもたらされたか」という点に焦点が当てられ、コンピュータ・ウイルスは、意図的に損害を与えるような行為の“一手段”として位置づけられている。

United States Code TITLE 18, PART 1, CHAPTER 47,

米国規約 タイトル 18, パート 1, チャプター 47,

SECTION 1030: Fraud and related activity in connection with computers

セクション 1030: コンピュータにおける不正及び関連した行為

(a)

(5)

(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(意図的に、プログラム、情報、コード、またはコマンドの転送を行い、または、そのような指導の結果として、認可なく意図的に「保護されたコンピュータ」に対して損害を起こした場合)

- (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or  
(意図的に「保護されたコンピュータ」に認可なくアクセスし、または、そのような指導の結果として、無闇に損害を起こした場合)
- (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;  
(意図的に「保護されたコンピュータ」に認可なくアクセスし、または、そのような指導の結果として、損害を起こした場合)

州法においては、コンピュータ・ウイルスによる犯罪の定義は、各州において異なっている。例えば、カリフォルニア州法では、「通常ウイルスと呼ばれるコンピュータ汚染物 (“computer contaminant” means any set of computer instructions....commonly called viruses....)」とウイルスを明確に定義している。一方、フロリダ州法は、その他多くの州と同様、ウイルスの定義はなされず、「意図的に損害を起こす行為」の1つとして適応されるようになっている。カリフォルニア州、フロリダ州、ジョージア州、ニューヨーク州の州法の詳しい分析は、第三章 2.において行う。

## 2. 米国におけるコンピュータ犯罪の実態

ハッカーやクラッカー、海賊版作成者など、ありとあらゆる形のコンピュータ犯罪に関わる者が後を絶たない現在、サイバースペースにおける秩序を守ることは至難の業となっている。国際経済の起爆剤となっているコンピュータの新技术も、法律立案者や警察当局にとっては、次から次へと出現するコンピュータ犯罪の元凶であり、捜査上の頭痛の種となっている。1980年代の中頃までは、コンピュータ犯罪と言えば、電算センターに接続されているネットワークに限られた攻撃のことを意味していた。しかし、インターネット革命の到来により、人々の生活様式からビジネスのやり方までが一変し、1980年代の終わりには、「カッコウの卵 (Cuckoo's Egg)<sup>1</sup>」<sup>1</sup>、「モリス虫 (Morris Worm)<sup>2</sup>」<sup>2</sup>と呼ばれる代表的なコンピュータ・ウイルス犯罪が発生した。その後、コンピュータ犯罪は拡大の一途をたどり、91年には司法省によって、サイバー・クライムを調査するための特別部隊がFBI内に設定された。

1999年にコンピュータ・セキュリティー研究所 (CSI: Computer Security Institute) が行った調査結果によると、民間企業や金融機関、大学、政府機関を含めた521の機関のうち、外部者によ

---

<sup>1</sup> 1989年、ドイツのハッカーが米国コンピュータに侵入し、そこから得た情報を当時のソビエト連邦に売却した。

<sup>2</sup> 1989年、コーネル大学生のロバート・モリスが作成したウイルスがインターネットに接続された数

ってシステムの侵入を受けた機関は3年連続で増加し、全体の30%に上っている。そのうち163の機関が被害額を提示しており、被害額の合計は1億2,400万ドルに上っている。現在、「機密情報の盗難 (theft of proprietary information)」が最も深刻な脅威と見なされており、現在までに23件で総額4,250万ドルの被害が報告されている。損害額の多さで2番目にランクされているものが「金融詐欺 (financial fraud)」で、報告件数は27件と「機密情報の盗難」よりも多いものの、損害額は3,970万ドルとなっている。

1999年には、米国上院、国防総省、FBI、陸軍、大統領府、議会といった政府機関のウェブサイトが、次々とハッカーによって侵入された。しかし、政府機関によって管理されているサイトに外部者が侵入するのは初めてのことでなく、昨年には、システムの脆弱性を見極めるために、陸軍のウェブサイトシャットダウンし、軍の全施設がインターネットによるコンピュータ操作を一時的に停止した。現在のところ、米国の安全保障を脅かすような大事には至っておらず、ハッカーたちの目的は、機密情報を盗み出すというよりは、政府重要機関ウェブサイトへに侵入することで軍や警察当局に恥をかかせるのが目的であることみられている。

犯罪の攻撃性は年々増している一方、日々凶悪化するコンピュータ犯罪に立ち向かうために必要な予算、人材などが不足している。現在、マクロ機能<sup>3</sup>を搭載したソフトウェアが普及しており、高度なコンピュータ知識を持たない者でもマクロ・ウイルスを作成してウェブサイトへの攻撃を容易に行うことができる。また、多くのコンピュータがネットワークで接続されているため、ハッカーはネットワーク上を自由自在に移動できる。政府にとってこれら無数とも言えるハッカーに対応することはますます困難なものとなっている。

市民の不安を煽るという理由で、政府または民間セクターにおけるコンピュータ犯罪件数の公式統計は発表されていない。ペンシルバニア州ピッツバーグにあるコンピュータ緊急対応チーム (CERT: Computer Emergency Response Team) のコーディネーション・センターが行った調査によると、1998年に約4,000件あったシステム侵入の件数は、今年に入って倍増しているという。政府コンピュータの不正を監視する「連邦コンピュータ犯罪対応センター (Federal Computer Incident Response Capability Center)」によると、99年6月に、68件のコンピュータ犯罪があり、これによって14万5,737台の政府コンピュータに影響があった。この数は半年前のものと比較すると約3倍になっているという。さらに、ある政府機関が、自らの3万8,000台のコンピュータを使って試験攻撃を行ったところ、65%のコンピュータに対する攻撃が成功し、わずか4%が攻撃を感知した。また、攻撃を感知したコンピュータのうち、わずか27%が攻撃の報告を行ったという結果

---

千のコンピュータを停止させた。

<sup>3</sup> ソフト内で使用される複数のコマンドをまとめて実行する機能。

も出ており、早急な対策が求められている。

### 3. コンピュータ・ウイルスの実態

#### コンピュータ・ウイルスの種類

FBIによると、現在問題となっているコンピュータ犯罪の主なものとして、(1)コンピュータ・ウイルス、(2)企業の給与情報などの重要データの盗難、(3)データの不法閲覧、が挙げられるという。第一の問題として挙げられているコンピュータ・ウイルスとは、ウイルスのコピーをコンピュータのファイルに注入することによりファイルを感染させることのできる寄生的なプログラムのことをいう。ウイルスはハード・ドライブの中に一定期間、住むことができ、ウイルスが一旦ハード・ドライブの中に注入されると、次々と自らのコピーを作成してウイルスを拡散する。ウイルスは、ディスクもしくはインターネット上で電子メールを通して伝達され、ネットワーク間を移動しながら広がっていく。

ウイルスは 1980 年代の半ばより出現し、最近になるまで一般のコンピュータ・ユーザーの注意を引くことはなかった。しかし、1992 年に「ミケランジェロ<sup>4</sup>」というデータ破壊ウイルスによる大規模な被害が発生し、一般ユーザーの意識を上げるきっかけとなった。

コンピュータ・ウイルス事件が日常茶飯事になっている現在、一体いくつのコンピュータ・ウイルスが存在するのかという問いに正確な答えを出すのは非常に困難である。しかし、その数が急激に増加しているということは明らかである。1989 年に公式確認されたウイルスの数は 50 種類以下であった。ウイルス対策ソフトウェアの大手ベンダーであるシマンテックおよびネットワーク・アソシエーツ (Symantec、Network Associates) は、現在、約 4 万種類のウイルスが存在すると推定している。しかし、その中の約 150 種が「イン・ザ・ワイルド (in-the-wild)」、つまりラボ施設の研究用ではなく、実際に一般使用の場で発見されたものとなっている。この約 150 種のうちわずかな数だけが、データ破壊や消去を行うような有害なものであるとみなされている。しかし、毎週、約 300 もの新しいウイルスがハッカーによって書かれていると言われており、ウイルス対策の困難さを物語っている。しかも、一度、新しいウイルスが普及すると、他のウイルス・ライターがその改良版を次々と作成し、鼠講式にウイルスが増えて行くという状況が存在する。

---

<sup>4</sup> 1992 年、台湾製のソフトウェアを使って、世界中の数十万代のハードディスクからデータが抹消された。

### **ウイルスによる被害**

ペンシルベニア州カーリスルにあるアイ・シー・エス・エー( ISCA: International Computer Security Association )が行った調査によると、コンピュータのウイルス感染率は急上昇しており、ウイルス対策ソフトのベンダーはそのスピードに追いつかない状態であるという。ウイルスによる直接的被害はデータの破壊であるが、間接的被害として「コンピュータのアクセスを妨害される」、「コンピュータを使うことができない( denial-of-service )」などの影響がある。例えば、最近の大型ウイルス事件として注目を集めた「メリッサ」は、データを破壊するわけではないが、ネットワークを遮断して「サービス拒絶( denial-of-service )」を起こす。これは明らかに犯罪と見なされており、例えば緊急病院のシステムがこのウイルスに感染すれば、バックアップも停止されることから被害は拡大することが予想される。

1999年に同じく ISCA が行ったコンピュータ・ウイルス拡散調査( Computer Virus Prevalence Survey )によると、ウイルス対策ソフトウェアの開発が進んでいるにもかかわらず、コンピュータ・ウイルス感染状況は過去4年の間に悪化しているという。99年に発生したウイルスの半数以上が電子メールによって広がっており、感染の主な源がフロッピーディスクから電子メールに移行していることも明らかになっている。この調査の中で、1997年1月から1999年2月までの間に300の機関が、26万3,784件のウイルス被害( 80万6,614台のコンピュータが対象 )に遭ったことが報告されている。これは「1ヶ月間に1,000台のコンピュータにつき13件のウイルス感染が起こった」という計算になる。調査の対象となった機関のうち約43%が「25台以上のコンピュータ及びサーバーが同時に感染するなどの被害を被った」と答えている。同調査では、被害に遭った91%が「サーバーが最高1時間の停止」を報告し、80%が「復旧のために最高50時間( 中央値は24時間 )を要した」と答えている。( 3人の回答者は「復旧のため最高1,000時間サーバーを停止した」と答えている。)また、復旧のためのサーバー停止によるコストを5,000ドルから100,000ドルと見積もった回答者が26%となっている。

### **各コンピュータ・ウイルスの特徴**

1995年に入るまで、ほとんどのウイルスは「ファイル感染・ウイルス」と「ブート・セクター・ウイルス」の2種類に分けられていた。「ファイル感染・ウイルス」は、実行可能なプログラムファイルを汚染する。現在では、プログラムの規模が大きくなり、値段もより安価になったことから、アプリケーションを交換するユーザーが減り、「ファイル感染・ウイルス」は全体の約5%に留まっている。「ブート・セクター・ウイルス」は、ディスクドライブの一部に潜入し、フロッピーディスクを通して感染する。ディスクドライブの一部には、起動プログラム・情報が保存されており、作動指示を得るためにコンピュータが起動後、最初に行われる場所である。しかしこれも、電子メールとネットワークの台頭により、発生数が急激に減少しつつある。

今日、独占的な位置を占めるのが「マクロ・ウイルス」と呼ばれるものである。マクロとは、ソフトウェアの機能を自動化し、アプリケーションをユーザー・フレンドリーにするものであり、マイクロソフトの Excel や Word などはこのマクロ機能が使用されている。このマクロ機能を悪用したのが「マクロ・ウイルス」である。「マクロ・ウイルス」は、添付ファイルに乗って、添付ファイルがついた状態で開かれた文書から感染する。これが、マイクロソフトの文書・表計算ファイルがウイルス感染し易いと言われる所以である。「マクロ・ウイルス」は Visual Basic などのプログラミング言語で書かれているため比較的簡単に作成できるという点でも脅威とみなされている。

ウイルスによって引き起こされる影響・活動は「ペイロード (payload)」と呼ばれる。あるウイルスは、コンピュータが一定の日時に一定回数で再起動された後、感染されたファイルを起動すると、「ペイロード」を誘発するようにプログラムされている。「ペイロード」は、コンピュータにある操作を行うよう指示する実行可能コードであり、被害はなくても迷惑なスクリーン・ディスプレイを見せたり、有害なものではファイルを破壊 / 消去したり、コンピュータの起動セクターを破壊したりする。しかし、「ペイロード」を含んでいないウイルスも存在し、探知されないうまま何年間もコンピュータの内部に潜伏していた、というような例も報告されている。ファイルやハード・ドライブを永久に消去してしまうようなウイルスはむしろ少数派ということがいえる。

「寄生虫 (Worms)」や「トロイの木馬 (Trojan horses)」と呼ばれるものは、感染機能を持たない。トロイの木馬は、偽のファイル名とアイコンがつけられており一見無害に見えるため、ユーザーが誤って開いてしまうことから偽装プログラムと呼ばれる。寄生虫は、通信ネットワークで接続されたコンピュータ間を自己複製しながら移動し、コンピュータやネットワーク内で、コンピュータがクラッシュするまで増殖し続ける。新しい型のウイルスには、寄生虫とトロイの木馬の両方の機能を持っているものもある。

### **ウイルス作成者**

米国において、ウイルスを故意に広げようとする行為は犯罪と見なされ起訴の対象となるが、コンピュータ・ウイルスのプログラムを書くこと自体は合法の扱いとなっている。ウイルス・プログラムのライターが一体何人くらい存在するのか見極めることはほとんど不可能であるが、あるウイルス対策リサーチャーによると、現在、「コード・ブレイカーズ (CodeBreakers)」や「最終カオス (Ultimate Chaos)」など約 15 のウイルス・コード作成グループがあり、約数百人のウイルス・プログラム・ライターが属しているという。これらのグループは、インターネット・ウイ

ルス交換グループ (Internet Virus eXchange group) を略して VX (ヴィーエックス) や Vxers (ヴェクサーズ) と呼ばれることもある。このようなグループのメンバーは、ティーンから中年の会社幹部まで様々なプロファイルを持つ者で構成されている。また、ライター予備軍として、ウェブサイトで提供されるハッカー・キットを使用して、高度なプログラミング知識を持たないまま、比較的簡単にウイルスを作成してしまう者も増加してきている。

ウイルスを含んだファイルは、インターネット上で簡単に交換することができるため、ウイルス・ライターや Vxers、コーダーズ (coders) は、既存のウイルスを使って独自のウイルスを作成する。このような VX サークルでは、ノートン・アンチ・ウイルス (Norton Anti Virus) やマカフィー・ウイルス・スキャン (McAfee VirusScan) など、大手ベンダーによるウイルス対策ソフトウェアに、自分達のウイルスがシグニチャー・ファイル (signature file)<sup>5</sup>として掲載されることを至上の喜びとしている。

ウイルス交換者 (VXers) 達は、自分の書いたウイルスがあまり大きな被害をもたらさないと分かった時点であきらめる傾向にあるという。以上のような傾向からみても分かるように、ほとんどのウイルス・プログラマーは、犯罪を犯すことを目的というよりは、自分のプログラミング・レベルを試すためにゲーム感覚でウイルスを書いている。しかし、「メリッサ」のケースでも証明されたように、作成されたウイルスが爆発的な破壊力をもつようになる可能性もあるため、軽率なハッカーを軽視することはできない。

#### 4. 代表的なウイルスによる大型事件

ソフトウェア開発業者によってマクロ機能を使用した簡単なソフトウェア・パッケージの導入が進んでおり、マクロ機能を悪用したウイルスによる被害は年々増加していると関係者はみている。また、新たな 32 ビットプログラムに感染するウイルスや、ネットワークを悪用して感染が広がるウイルスが増加している。その証拠に 1999 年だけでも、3 月には「メリッサ」が、続いて 4 月に「チェルノブイリ」もしくは「CIH」が、そして 6 月には「WormExplore.Zip」(12 月に改訂版が流行) が全米を襲っている。

##### メリッサ

メリッサは、他の多くのウイルスと同様、マイクロソフト・ワードで作成された文書を汚染し、

---

<sup>5</sup> シグニチャー・ファイルとは、脅威と見なされるウイルスを定義するデータ・ファイルであり、ウイルス対策ソフトのベンダーは、対策ソフトのアップデート・バージョンを作成する度に新しいウイルスを追加していく。

史上最高の感染範囲の広がりを見せた。メリッサが他のウイルスと違っていたのは、そのペイロードであった。一度ウイルスがシステムを汚染すると、ウイルスは電子メールのアプリケーションであるマイクロソフト・アウトルックのアドレス帳に掲載されている最初の 50 人に、汚染された電子メールを自動的に発送する。従ってウイルスのコピーがそれぞれ次の 50 人に送信されれば、機械的にはそれが 2,500 人に広がる計算となる。メールの中身は「この前から頼まれていたものです。他の人には見せないでくださいね。」Here is that document you asked for...don't show anyone else ;-)」（最後のマークはウィンクした顔）」というもので、多くの被害者がこのような一見、無害な添付ファイルを開いたことにより被害が瞬く間に広がって行った。メリッサの危険性がそれほどまでに高まった他の要因として、メールのメッセージが実際の友人や同僚などから送信されてくるため、それまで常識となっていた「良く知っている人から来たメールの添付だけを開くようにする」という警戒心を持つことが無意味となってしまったことが挙げられる。このウイルスは、メッセージに自動的に独自の言葉を加えたりするため、本当に知っている人から来たメールのように見えるところが特徴となっている。CERT によると、メリッサは 1999 年 3 月 26 日のデビュー後、世界で 233 の機関を攻撃し、述べ 8 万 1,285 台のコンピュータを汚染した。しかもこの数字は報告されたものだけであり、実際の被害はさらに大きなものであったと考えられている。

メリッサの出現後、FBI は VicodinES (略して Vic) として知られていた「コード・ブレイカーズ」のある引退メンバーに最初、的を絞って捜査を行った。FBI は、この Vic と呼ばれる人物によって以前作成された PSD2000 というウイルス(彼のウェブサイトのコピーが出来るようになっていた)がメリッサと似通っていたため、Vic とメリッサ・ウイルスを結びつけた。しかし、インターネット・サービス・プロバイダーであるアメリカ・オンラインより提供されたネットワーク・オーディット・ログが調査され、これにより、メリッサを最初に発信したユーズネット・ポストとして、ニュージャージー州アバーディーン在住のデイビッド L.スミスというプログラマーを付きとめることに成功した。

デイビッド・スミスは、ニュージャージー州による「公共の通信の妨害、コンピュータ・サービスの窃盗、コンピュータ・システムの不正なアクセス ( interruption of public communication, theft of computer service, and wrongful access to computer systems )」を行ったという刑事起訴に対し、有罪の申し立てを行った。これにより、5 年から 10 年の禁固刑と最高 15 万ドルの罰金が課せられることになる。スミスは、「保護されたコンピュータへ損害を与えるようなコードを送信すること ( to send code that causes damage to a “protected” computer )」を違反行為と定めた連邦法である「コンピュータ詐欺と濫用に関する法律 ( Computer Fraud and Abuse Act )」下においても裁かれることとなっている。

### **チェルノブイリまたはCIH**

チェルノブイリ、もしくはCIHと呼ばれるウイルスは、1998年6月にその存在が報告された。しかし、今年の初めになるまで、wild、つまり実際に使用されているコンピュータには影響が見られなかった。メリッサと違い、このウイルスは破壊的なペイロードを持っている。CIHおよびその変体(variants)は、4月26日、6月26日もしくは毎月26日に誘発されるようになっており、ウイルスは、コンピュータが立ち上げられた時に起動するチップであるフラッシュBIOSを上書きする。これによりパソコンが立ち上がらなくなる場合がある。また、ハードドライブが上書きされる。

### **WormExplore.Zip**

WormExplore.Zipは、最初、イスラエルで発見された寄生虫型のウイルスで、メリッサに比べると少数のコンピュータを汚染したものの、破壊力のレベルと感染の広がる速度から、より危険度の高いウイルスであると位置付けられている。このウイルスは、ユーザーが感染以降受信したメールの送信元に、ウイルスが自ら作成した電子メールを送信する。メールには添付文書がついており、この添付文書がユーザーによって開かれるとコンピュータに潜入する。添付文書はジップ(圧縮)されたファイルに見えるものの実際はそうではない。ウイルスのプログラムは偽のエラー・メッセージを出してユーザーを欺き、その間に、ファイルをゼロ・バイトに変更しながら破壊して行く。

### **バブル・ボーイ**

通常、ウイルスは電子メールに添付文書として送信され、拡散する。もっと危険なのは、そのウイルス・プログラム自体がメール本文内に組み込まれてしまうことである。今年11月に報告された「バブル・ボーイ」は、HTML形式の電子メール本文によって運ばれるウイルスの一例である。バブル・ボーイの初版はペイロードを持っていなかったため被害はなかったものの、言うまでもなく、バリエーションを作成して破壊的な修正版を作成することは特に難しいことではない。

## **5. ウイルス対策ソフト産業**

ウイルスの被害が高まるのと同時に、ウイルス対策ソフトウェア産業が活発になっており、対策ソフトウェア市場は、1997年の7億ドルから、2001年には26億ドルにまで成長するとみられている。新しいウイルスが発見される度に、対策ソフトの売上が伸びると言われており、バージニア州レストンにあるコンピュータ市場調査会社であるPC Dataによると、メリッサが猛威を振るった1999年の3月28日から4月3日の間に、ウイルス対策ソフトウェアの売上が約67%もの

伸びを見せたという。ウイルス対策ソフトウェア・ベンダー大手には、ネットワーク・アソシエーツ (Network Associates)、シマンテック (Symantec) などがあり、今後も産業界でのシェアを伸ばしていくものとみられている。

ますます深刻化するウイルスに対抗するため、ウイルス対策ソフトの技術も高度化の一途をたどっている。コンピュータ・ウイルスは、日々その機能を拡大しながら変化するため、ウイルス対策ソフトの更新と管理が簡単に行えることが、ウイルス対策ソフトを導入する際の鍵となる。「メリッサ」「バブルボーイ」など、99年に次々と出現した強力ウイルスの影響で、多くの企業が毎週のようにウイルス対策ソフトの更新をするようになったという。最新のウイルス脅威に通じ、そして対応していることが、ウイルス対策戦略の最も重要な点となる。通常のプログラムは、継続した管理と更新は必要ではないが、ウイルス対策ソフトは定期的なアップデートが必要になるため、その管理には特別のアプローチが取られる必要がある。

コンピュータ・セキュリティー研究所 (CSI: Computer Security Institute) が 1998 年に行った調査によると、前年に比べて増加したとはいえ、民間企業におけるインフォメーション・セキュリティー担当員の割合は社内におけるわずか 1% となっている (割合は産業別、企業の規模別などによって違ってくる)。ウイルス対策ソフトの技術がより高度化、複雑化している現在、セキュリティー管理を確実に行うためには、単に技術面だけではなく、ネットワーク・アーキテクチャから電子商取引、セキュリティー長期計画、対策立案にいたる全てに関する知識を持った専門家が必要とされていることが原因の 1 つとも考えられている。このような状況を受け、インフォメーション・セキュリティー業務をアウトソーシングする傾向が様々な組織、企業間において強まっており、インフォメーション・セキュリティー管理を専門としたコンサルティング企業による事業の伸びが見こまれる。

## 第二章 連邦レベルにおける法規制及び執行

### 1. 背景

コンピュータを使用する国々は、コンピュータ犯罪をどのように定義するのかという初歩的な問題から、犯罪に対処するための法律の整備まで様々な問題を抱えている。米国もその例にもれず、連邦政府レベルでの法制度の立案・立法件数は、過去10年から15年の間に、コンピュータ犯罪の急増に伴い増加している。十分な統計が出されていないため、現在、施行されている法律が効果的であるか否か、という問に答えるのは簡単ではない。一方、ますます多くの日常生活における活動・行為がオンラインで処理されるようになり、コンピュータ犯罪が人々の一般生活にまで浸透している。最近のコンピュータ犯罪の例としては、ハッカーがDVDプレーヤーのコードを解読し、映画の海賊版をコンピュータのデスクトップにコピーできるようにしていた、などの事件が起きている。このように、より複雑化、日常化するコンピュータ犯罪にどのようにして連邦政府が対策を講じていくべきなのかをめぐり、米国において活発な議論が展開されている。

金融サービスなど、主要産業による電子商取引への拡張が進み、ネットワーク・インフラの普及が日常化した現在、米国を始めとする世界各国において、コンピュータ犯罪が年々、より深刻になっている。1998年、カリフォルニア州サンフランシスコに本部を置くコンピュータ・セキュリティ研究所(CSI: Computer Security Institute)が、FBIの国際コンピュータ犯罪班(International Computer Crime Squad)と合同で調査を行った。その結果、企業や政府機関、金融機関、大学など520の組織でコンピュータ・セキュリティ担当者の64%が「過去24ヶ月の間にコンピュータ・セキュリティの被害を受けたことがある」と答えており、この数字は、1997年に行われた同類の調査の回答より16%も増加している。241の機関が被ったコンピュータ犯罪による被害のうちドルに換算することのできる額の合計は、1億3,700万ドルに上っており、97年より36%の増加となっている。被害額が最も大きかった例では、組織内部からの違法アクセスによるもので、被害額は5,100万ドルであった。その他、被害額が大きい順から犯罪の種類を述べると、資産情報の窃盗(3,350万ドル)、電気通信詐欺(1,720万ドル)、金融詐欺(1,120万ドル)となっている。

最近、犯罪検挙数が頭打ちになっており、現時点では、犯罪者の方が連邦政府の対策の上手を行っているという見方がされている。コンピュータ犯罪を検挙する妨げとなっている1つの理由として、コンピュータ犯罪をどのように定義するかという点で未だ合意が行われていないことが挙げられる。現在の時点では、一般的にコンピュータ犯罪は以下のように分類されている。

1. 違法なインターネット・アクセスなどの、コンピュータによるサービスの窃盗。ここではコン

ピュータは犯罪の対象となる。

2. ウイルスの使用や論理爆弾 (logic bomb)、スニファーズ (sniffers) (ユーザー名やパスワードを盗む) など、コンピュータが、犯罪の物理的な現場もしくは源、または知的所有権を含めた資産の紛失の理由となる場合。ここではコンピュータは犯罪の主体となる。
3. 他人のクレジットカード情報を収集して違法な使用を行うなど、コンピュータが道具として使われる場合。

## 2. 連邦関連法の成立、修正

現在、コンピュータ犯罪取締法として、96年に制定された「全米情報とインフラ保護法 (National Information and Infrastructure Protection Act of 1996)」が適用されている。この法律は、1984年に最初のコンピュータ対策連邦法令である「偽造アクセス機器とコンピュータ詐欺・濫用に関する法律 (Counterfeit Access Device and Computer Fraud and Abuse Act)」が制定された後、数年間に渡って修正、改正が加えられた結果、現在のような形をとっている。主な改正としては、84年法が、1986年に「コンピュータ詐欺と濫用に関する法律 (Computer Fraud and Abuse Act)」として修正され、94年、さらに修正が加えられる。同法は、96年にその一部が「全米情報とインフラ保護法」となったが、この法律も、現在、見直しが進められている。このように、84年の法律が制定されて以来、「犯罪を抑制するためには有効に働いていない」という批判に対応する形でその都度、法律改正が行われている。このように米国の連邦法は、ハッカーの後ろを追うような形で、法整備がされ、常に犯罪者が法律の先を行っているとする見方もある。また、法整備そのものよりも犯罪者を実際に取り締まるエンフォースメント体制に問題があると指摘する声も聞かれる。

### 中核法の確立

コンピュータ犯罪は、1960年代から70年代にかけて、タイムシェアリング・システムの到来と共に出現した。警察当局は、当初、現行法をコンピュータ犯罪に適用しようとしたが、1980年の初め、軍や企業の機密データが、コンピュータ・ウイルスやハッカーによって攻撃され、現行法ではコンピュータ犯罪の対策が効果的に行われていないことが明らかになった。その後、連邦及び州レベルにおける新しい法律の制定が提案され、警察当局のコンピュータ犯罪に対する意識が高まった。このような社会的意識の高まりを受けて、1984年、「偽造アクセス機器とコンピュータ詐欺・濫用に関する法律 (Counterfeit Access Device and Computer Fraud and Abuse Act)」が制定され、議会はコンピュータ犯罪を新しい連邦犯罪として確立した。この法律は当初、防衛及び外交情報、金融機関、消費者窓口データ、政府のコンピュータへのアクセス情報などに的を絞っていた。また、この法律は、WWW (ワールド・ワイド・ウェブ) が普及する前に採択されたため、一般ユーザーではなく、政府関連機関や企業の大規模コンピュータ・システムに対する不正

行為を対象としていた。この法律は定義があいまいであったため結果として、あまり大きなインパクトはなかった。特に、同法成立後の逮捕件数が1件だけという、取締に関しては骨抜きの状態であった。

### **86年の改正でCFAAへ**

84年の法律がコンピュータ犯罪に対応するどころか、「コンピュータ犯罪者を起訴することがかえって難しくした」との批判を受け、その2年後、同法に手が加えられた。その結果、「コンピュータ詐欺と濫用に関する法律(Computer Fraud and Abuse Act)」の成立となった。この改正法により、議会は法律が適用される範囲を拡大し、各用語の定義を明確にしようと試みた。この法律により「所有権の明らかになっているコンピュータのプログラム、情報、コード、コマンドを意図的に移動し、不正にそれらに損害を与える行為(knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer)」が重罪(felony)と定義された。また、承認なし(unauthorized use)に連邦政府のコンピュータにアクセスしようとする行為自体が犯罪とみなされることとなった。しかし、承認を得ている(authorized user)内部犯罪者による被害を抑えるための手段として同法が役に立っていないという問題点が指摘された。

### **1994年改正とガイドライン設定**

「1989年1月から1993年の4月までにわずか76件のコンピュータ犯罪人の逮捕しか行われていない」という報告があった。1994年、CAFAAはさらに改正されることになった。その背景には、94年の改正法は、コンピュータ犯罪の取り締まり強化と共に、ユーザー人権擁護にも焦点が当てられた。これは、FBIのコンピュータ犯罪に関する一連の捜査において、容疑者の人権が犯されてしまうような事件が相次いで起きたため、捜査手順を確立する必要があったからだ。そのようなFBIによる捜査手順の不備を現す事例が数例、存在する。例えば、警察当局は、コンピュータ犯罪を取り締まる手段として、ハッカーの集合場所として当時、活発な活動を行っていたBBS(bulletin board system)と呼ばれる掲示板に的を絞って捜査を行った。しかし、1990年3月にテキサス州オースティンにてFBIが差し押さえた掲示板は全くの合法会社であり、このステイブ・ジャクソン・ゲームという会社は後に政府を相手取って訴訟を起こし、5万1,000ドルの損害賠償を受け取った。また、1990年の「サンデビル作戦(Operation Sundevil)」でFBIは、42台のコンピュータ、25のBBS、2万3,000枚のフロッピーディスクを差し押さえたものの、その結果、実際に逮捕されたのはわずか4件という結果に終わった。その際、多くの誤った容疑者からコンピュータなどの個人財産が没収された。このようなFBIによる捜査のやり方に対し、一般ユーザーの基本人権の侵害として人権擁護団体から糾弾を受ける結果となった。

これらの事件をきっかけとして「電子フロンティア財団 (Electronic Frontier Foundation)」が設立された。同団体は現在、コンピュータによる市民人権擁護団体として政府に対して積極的なロビー活動を展開している。また、捜査過程における人権侵害をなくすため、司法省は、1994年に非公式のガイドラインを出版し、捜査状や証拠の提示義務など、基本的人権問題に関わる理解を深めるため連邦政府機関と裁判官に対し一定の基準を示している。この「コンピュータの捜査と没収に関するガイドライン (Federal Guidelines for Searching and Seizing Computers)」は、ハードウェア、ソフトウェア、印刷物など、証拠として捜査及び没収の対象となるものをカテゴリー別に分け、無差別没収が2度と起こらないようにした。

しかしながら、94年の改正法では、「故意に」損害を与えるハッカーに焦点が当てられ、「悪意のない」行為は軽犯罪として軽く見られる定義が定着してしまった。従って「悪意」を証明できないハッカーの攻撃が見過ごされる結果となった。また、法律をより広範囲なものにしようとしたのが、その逆の結果を招き、政府及び金融機関のコンピュータから連邦保護が誤って取り除かれてしまった。それにより、内部による合法処理が違法意行為として検挙される結果となってしまった。また、米国判決委員会 (U.S. Sentencing Commission)<sup>6</sup>が議会に提出した96年の報告書によると、1996年の6月時点で依然としてわずか174人のコンピュータ犯罪者しか起訴されていなかった。このような状況を受け、同法は96年に再度、改正されることになる。

### 1996年、NIIPA 制定

96年、CFAAの一部は「全米情報とインフラ保護法 (National Information and Infrastructure Protection Act of 1996)」と改正された。この改正法より議会は、「被害者は一定額の金銭的被害を被っている必要がある」とした条件を、ある程度軽減、場合によっては削除した。さらに、承認なしの不正アクセスは即時に犯罪とみなされることとなった。この法律以前では、被害を成立させるためには、承認を受けていないユーザーが情報をダウンロードしたという証拠を、被害者が提出する必要があった。同時に、個人用のネットワーク上のウェブサーバーからネットワークの他の部分を検索できるわけではないため、個人使用と公のコンピュータとの違いが明らかにされた。また、コンピュータ、ネットワーク、プログラム、データに対する攻撃の脅威を区別して「被害」を再定義した。また、「常習的犯行」の部分が取り除かれ、ハッカーは、法律の全く同じ項目を破らなくても、同種の犯罪を犯せば、常習犯としてより厳しい判決を受けることになった。

96年法においては、対象となるコンピュータが「連邦法に関わるコンピュータ (federal interest

---

<sup>6</sup> 米国判決委員会とは、Sentencing Reform Act of 1984を受けて設立された司法独立連邦機関である。委員会は連邦裁判における判決ガイドラインの設定、犯罪や判決に関するデータの収集、議会・大統領府・最高裁判所へのリソース提供などを行う。

computers)」から「保護されているコンピュータ (protected computers)」と定義された。以前は、連邦管轄として多数の州に設置されているコンピュータが同時に使用される犯罪だけが対象となっていた。しかし、改正法では、「保護されているコンピュータ」はインターネットで接続された全てのコンピュータが対象となる。また、電子メールによって送られてくるウイルスや、コンピュータ・システムへの不正アクセスによる各種犯罪にも言及されており、ウイルスとハッカー対策条項が以前より明確なものとなっている。

1996年の改正法では、アクセスの権限を持たない者が「保護されたコンピュータ (protected computers)」に不正アクセスを行うとその行為自体が重罪となる、とされた。同時に、アクセス権限を持った内部者による不正行為も、「損害を与えようとする悪意」が証明された場合にのみ有罪となる、とされた。しかし、「悪意」を証明するのがほとんど不可能であるため、違反者を起訴するのが困難であるという点が、同改正法の弱点とされ、この問題はまだ未解決のままになっている。また、改正法ではハッカーについての条項がほとんどで、ウイルス問題にはあまり言及されておらず、拡大するウイルス犯罪に対応しきれていないという批判も聞かれた。別の問題としては、「侵入によって何らかの被害を与えられた」場合を、起訴の条件とすることが定義されたが、「被害」の定義が明らかになっていないという点も挙げられる。

96年の「全米情報とインフラ保護法 (National Information and Infrastructure Protection Act of 1996)」は、新しいコンピュータ技術の開発状況に対応するため、近いうちにもまた改正が行われるものと見られている。司法省は、「コードを破壊するような行為を犯罪と見なす」、「繰り返し罪を起こす者に対する懲罰を重くする」、「不正アクセスを企てるのに使用されたコンピュータ機器没収を合法化する」というような新条項を改正案に加えるよう提言を行っている。

### **連邦政府によるコンピュータ犯罪対策法令**

米政府は、1980年代半ばから、不正対策、プライバシー、知的所有権保護、セキュリティに至るまで、一連のコンピュータ関連法を成立させている。以下に主要な法律を示す。米国では、広範囲におけるコンピュータ犯罪法の中でウイルスの位置づけがなされており、ウイルス関連犯罪も位置付けられており、ウイルスだけに特化した形での特別な連邦法は存在していない。また、ウイルスはコンピュータ犯罪のツール(手段)の1つであり、ウイルスそのものよりも、それによって生じた被害やインパクトに応じて該当する法律が適応される。

1984年

「偽造アクセス機器とコンピュータ詐欺・濫用に関する法律 (Counterfeit Access Device and

Computer Fraud and Abuse Act )」

1986 年

「コンピュータ詐欺と濫用に関する法律 ( Computer Fraud and Abuse Act )」

1986 年

「電子通信プライバシー法 ( Electronic Communications Privacy Act )」

1987 年

「コンピュータ安全法 ( Computer Security Act )」

1988 年

「コンピュータ詐欺と濫用に関する法律 ( Computer Fraud and Abuse Act )」

1989 年

「コンピュータ保護法 ( Computer Protection Act )」

1996 年

「経済スパイ法 ( Economic Espionage Act )」

1996 年

「全米情報とインフラ保護法 ( National Information and Infrastructure Protection Act )」

1996 年

「電気通信法 ( Telecommunications Act )」

1997 年

「コンピュータ・セキュリティ促進法 ( Computer Security Enhancement Act )」

1998 年

「児童保護と性犯罪者懲罰法 ( Child Protection and Sexual Predator Punishment Act )」

1999 年

「コンピュータ・セキュリティ促進法 ( Computer Security Enhancement Act )」

#### **その他関連法**

過去数年に渡り、連邦政府法令やその他関連法を強化するという目的で、コンピュータ犯罪項目を設けた多くの法律が施行された。1996 年の電気通信作法法 ( Communications Decency Act ) ( 憲法違反であるとして最高裁判所で却下された ) や、郵便物と電話回線による詐欺に関する法令と旧来の浸入に関する法律である「全米窃盗財産法 ( National Stolen Property Act )」がその一例である。

### **3. 連邦コンピュータ犯罪対策プログラム**

## NIPC

1997 年の「重要インフラ保護に関する大統領委員会 (President's Commission of Critical Infrastructure Protection)」(委員長の名前を取って「マーシュ・レポート」と呼ばれる)による報告書の中で「コンピュータ犯罪が国家に対する脅威となり得る」との分析が行われ、国家重要インフラをコンピュータ犯罪から保護するために、政府と産業界との新しいパートナーシップを確立することが提唱された。このマーシュ・レポートがきっかけとなり、1998 年 2 月に、全米インフラ保護センター (NIPC: National Infrastructure Protection Center) が 2,950 万ドルの費用を投じて FBI に設立された。

同センターは、首都ワシントン DC にある FBI に本部を置き、映画スターウォーズさながらの機密ハイテク司令部と化しているという。NIPC は、FBI、CIA、国家安全保障機関(National Security Agency)、国防総省、エネルギー省、運輸省、その他の省庁横断組織となっている。しかし、NIPC が最もユニークな機関とされているのは、政府機関による公的プロジェクトにも関わらず、民間セクターとの緊密な協力体制を敷いており、その活動内容、スピーディーな対応、非官僚的な組織構成から、民間企業の特徴を持っている点である。

FBI、連邦機関、州政府機関、地方警察、そして民間企業から 100 人以上の代表者がこのセンターに結集し、複数の州によって異なったシステムで管理されている電気通信、金融、緊急対策、政府、電力、交通などのインフラを統合し、一局集中監視体制を構築する。主な使命として、コンピュータ・ウイルスなどのサイバー・アタックを探知し、地域社会へ警告を発し、そして犯人を割り出す。

NIPC は以下のような 4 段階を経てコンピュータ・ウイルスを阻止する。

1. ウイルスを識別する。
2. ウイルスに関する警告や、「どのようにしてウイルスに対抗するか」というような防御情報をユーザーに向かって発信することにより啓蒙活動を行う。
3. ウイルスのリバース・エンジニアリングを行うことによりウイルス対策ソフトを開発し、ウイルス撲滅に努める。(この任務は、NIPC よりウイルス対策ソフト会社によって主に実行されている。)
4. 犯人を見つけだし、刑事法に則って裁く。

今日、以上の 4 段階の過程は、連邦、州、民間機関のそれぞれによって別々に行われている。NIPC は、「ウイルスの識別」「警告の発信」「犯人の居場所突き止め」に焦点を絞って活動を行っている。

1999年5月に、ハッカーが上院とFBIのウェブサイトを破壊し、FBIを侮辱する言葉を残していくという事件が発覚するなど、FBIの課題は山積みしている。しかし、NIPCは、FBIとニュージャージー州を支援し、今年の春に流行した「メリッサ」の犯人を付きとめるのに成功している。

### **CERT**

「コンピュータ緊急対応チーム (CERT: Computer Emergency Response Team)」コーディネーション・センターは、コンピュータの不正アクセス対応・新種ウイルスの警報、関連情報の配布を専門に行うために設立された。CERTは、カーネギー・メロン大学内に設置された官民支援の研究開発センターである「ソフトウェア・エンジニアリング・インスティテュート (SEI: Software Engineering Institute)」の一部である。CERTは、インターネットの先駆けであるアーパネット (Arpanet) (当時わずか1万8,000人のユーザーを持っていた) を「モリス虫 (Morris Worm)」によって破壊されるという事件が発覚した後、1988年にその対策機関として設立された。センターは、現在では、ウイルス発覚後の対応専門家へのトレーニング、セキュリティー脆弱性の原因の追求、システム・セキュリティーの強化、大規模ネットワーク管理などを提供している。CERTによると、同機関によって取り扱われたウイルス事件数は、1995年の2,412件から98年の3,734件、99年の6,844件と増加しているという。「メリッサ」と「ExploreZip」が発見された数時間内に、CERTは、200万人以上のインターネット・ユーザーに警告と指示を発信し、「メリッサ」のリバース・エンジニアリングに成功した。

現在、CERTは、カーネギーメロン大学ピッツバーグ・キャンパスにおいて50人のスタッフと共に活動を行っており、NIPCに技術的な情報を提供しながらNIPCと協力体制をとっている。

### **スパイ行為対策センター**

連邦政府レベルにおけるコンピュータ犯罪に対する最近の対策として、連邦政府がオンライン・スパイ行為に対抗するための新しいセンターを、コロラド州コロラド・スプリングに設立することが1999年10月に発表された。このセンターは、空軍の管轄となり、国防総省の管轄下にある米国航空司令部 (U.S. Space Command) (コロラド州コロラド・スプリングス) の領域内に設置される。昨年、国防総省やその他政府機関や民間コンピュータ・システムから、入札や契約文書など「機密レベルではないものの重要な」データが大量に盗難にあった。FBIによってこの事件が上院へ報告されるや否や、緊急対策としてこのセンターが設立された。その後、国防総省は、2億ドル相当の新しい暗号化技術を発注している。

## その他

FBI の国際コンピュータ犯罪班、経済情報活動プログラム（Economic Counterintelligence Program）、コンピュータ調査とインフラに対する脅威分析センター（Computer Investigations and Infrastructure Threat Assessment Center）、司法省（DOJ）のコンピュータ犯罪と知的財産部（Computer Crime and Intellectual Property Section）も連邦政府法令を支援する機関として含まれる。しかしこれらプログラムの有効性については賛否両論がある。

## 4. 問題点

### 財政・人材不足

警察当局にとって、コンピュータ犯罪対策のための財源不足が捜査を進める上で足かせとなっている。FBI や司法省など、コンピュータ犯罪対策の主要機関でさえも、専門スタッフの人員不足など、深刻な問題を抱えている。連邦裁起訴を手掛ける各州の検事総長の各事務局には、ハイテク専門員が1人づつしか配置されていないというような事態も指摘されている。コンピュータ犯罪対策を強化するためには、専門家のスタッフを配置することが要となってくる。新しい専門家を育てると同時に、既存の専門家のノウハウをサイバー犯罪分野に適用していく過程も必要である。連邦政府機関の担当官に対し、旧来の調査技術をサイバーワールドに適用できるよう訓練するためには、様々なリソース（ヒト、カネ、モノ）が必要とされる。今までに、多くのオンライン児童ポルノ犯罪に関わる犯人を起訴してきた業績の裏には、コンピュータ外でのこの分野における知識が既に警察当局内で確立されていたという背景がある。このように、既存の捜査知識と技術がそのままサイバー犯罪に適応される場合もあれば、コンピュータ犯罪捜査には既存の警察官の交替（職務ローテーション）制度は通用しないなど、何らかの新しいシステムを導入する必要もある。また、政府法令が有効に稼働しないもう1つの理由として、コンピュータの高度知識を持つ専門家は、より良い待遇を求めて民間企業に流れる傾向にあり、警察当局におけるポジションに魅力を感じる者が少ないため、有能なスタッフが欠如していることが挙げられる。

### 管轄区域

コンピュータ犯罪捜査はその性質上、州をまたがって行われることが多く、警察当局は、州際のコーディネートに必要な資金を必要としている。サイバースペースには地理的な境界線がないため、コンピュータ犯罪者は各警察管轄区域を自由自在に移動する。そのため、FBI 当局は、犯人が何か行動を起こす前に、サイバースペースの全地域を自由自在に移動できるシステムを保持しておくことが、犯人逮捕に必要不可欠となる。

### **被害者の消極的・懐疑的な態度**

コンピュータ犯罪の犠牲者は、株主の信頼を傷つけたり、競合会社から否定的な広告として使用されたり、または弱点を曝してさらなるハッカーからの攻撃を招いたりすることを恐れるあまり、被害の届出を控える傾向にある。そのため、多くの企業が、ネットワーク攻撃の被害届を出さずに内密に処理してきた。また、裁判所における訴訟にかかる費用と手間を避けるために被害届を控えるケースも数多く存在すると考えられている。警察当局はそのような懐疑派に対し、「現在では、捜査のために被害届のあった会社の全てのネットワークをシャットダウンさせるようなことはなくなり、また、裁判で業務上の機密書類を提示する必要もなくなった」として、被害届の実施を呼びかけている。多くの被害者が、コンピュータ犯罪は警察当局から真面目に取り合ってもらえない、と感じていることも、被害届率が低い原因となっている。

「ウイルス対策ソフトのベンダーや警察当局が意図的に宣伝をしているだけで、コンピュータ犯罪は実際には深刻な問題ではない」とする声が多く聞かれるのも確かであり、一般市民の非協力が犯罪対策の促進を妨げている側面もある。また、産業界では、ウイルス対策ソフトのベンダーが、何か新しいウイルスが発見される度に新製品の販売を大々的に行うものの、実際には、ウイルスの大半が「スマイリー・フェース」のような無害なものである場合が多々あり、ウイルス対策ソフトのユーザーに対する実益に関して懐疑的になる者も増えている。

### **未成年による犯罪**

犯人逮捕後の問題として、多くの犯人が未成年犯罪者であり、起訴にまで持ちこむことが困難となっていることが挙げられる。コンピュータ犯罪で逮捕されたほとんど全ての犯人が、罪状を認めることによって有罪答弁に持ちこんで、陪審員に裁かれるのを回避する傾向にある。そうすることにより、多くの犯人がコンピュータ犯罪法ではなく、その他の法規の下で軽犯罪として有罪判決を受けることになる。これは、社会に影響を与えるような主要な裁判がいつまでたっても現れないということの意味し、「コンピュータ犯罪で禁固刑にまで課せられることはない」というような、違法行為自体を軽く見る風潮を作り出すことにつながっている。同時に、どれだけ「悪意」を持った行為であったのかを証明することが非常に難しいと考えられている。システム監査や電子メール及び電話のログなど、裁判所で証拠として提示するための証拠をネットワーク管理者が収集できないことが、有罪判決の件数が非常に低い原因となっている。

### **犯罪の簡易化、深刻化**

操作の自動化が進んだことや、多くのプログラムがユーザー・フレンドリーになったことにより、ネットワーク攻撃も容易になったと考えられている。起訴された多くの犯人が、初歩的なコンピュータ専門知識しか持ち合わせていないことから、このことを裏付けている。かつてコン

ピュータ・ハッカーが、のぞきを趣味とした単なる異常者ぐらいに扱われていた時代があった。しかし、最近では「バブル・ボーイ」や「ExploreZip.worm」などのような、電子メールを介したコンピュータ・ウイルス被害がより深刻化、広範囲化してきており、ハッカーに対する認識は確実に変化してきている。

### 第三章 州レベルにおける規制

#### 1. 州法の整備状況

議会在コンピュータ詐欺と乱用に関する条例 (Computer Fraud and Abuse Act of 1986) を制定する前から、早くも 1970 年代にコンピュータ犯罪法案を通過させる州がいくつか存在した。そのうち約半数の州が 1977 年もしくは 79 年の「連邦コンピュータ・システム保護条例 (Federal Computer Systems Protection Act)」を参考にし州法の草案を作成している。その他の州は、連邦法を参考とせず独自の法規を作成している。現在のところ、33 の州がコンピュータ犯罪関連の法規を設定しており、州法はコンピュータ技術が更新されるたびに大幅に変更されている。その他 11 州が、州法設定をめぐる審議中となっており、残る州が何らの対策も取っていない。

カリフォルニア、フロリダ、ジョージア、イリノイ、ニューヨークの州が最も進んだ対策を取っているとみなされており、バージニア州も、ネットワーク・インフラが集中していることから、最近になって積極的な対策が行われている。その他にも、オハイオとマサチューセッツの 2 州は、犯罪規定の再定義を行っており、新しい法規が特殊性の高いコンピュータ犯罪にも適用されるように体制を整えている。コンピュータ犯罪を明確に定義することが、コンピュータ・セキュリティを促進する上で必須の条件となっており、この過程を踏まないことには犯罪抑制や起訴の増加を実現することはできない。

各州法規には、様々な機構と専門用語が存在するが、そのほとんどが以下のような大きく分けて 3 つの目標を掲げている。

- (1) コンピュータ及びデータベースの不正アクセスもしくは使用を防ぐ
- (2) 詐欺を目的としたコンピュータ使用を防ぐ
- (3) オンライン破壊行為を目的としたコンピュータ使用を防ぐ

以上 3 つの法規目標は、以下のようにさらに 10 のカテゴリー<sup>7</sup>に分けることができる。

1. 既存の「財産」定義の拡張。既存の「財産」定義を電子またはコンピュータ技術を含むよう拡張することでコンピュータ犯罪を取り締まる。
2. 破壊。多くの州が、「コンピュータ・プログラム及びファイルを改ざん、破損、消去、破壊する行為」を犯罪行為と見なしている。

---

<sup>7</sup> Jay Michael Hatcher and Stacy McDannell, "Computer Crimes," *The American Law Review* Vol. 36, No.3 (Summer 1999), pp. 397-444.

3. 教唆・幫助。コンピュータを使つての着服や詐欺などの犯罪。
4. 知的所有権に関わる犯罪。不法侵入（不正のコンピュータ・アクセス）、破壊・蛮行（コンピュータ・データを悪意を持って改ざん、消去する）、盗難（プログラムおよびデータを不法にコピーする）など、既存の犯罪用語をそのまま新しいコンピュータ犯罪に適用したもの。この法規下では、損害が報告されなくても以上の行為を行っただけで起訴の対象となる。
5. 故意の不正使用。持主の承認を受けずにコンピュータを使用、もしくはアクセスすることを禁じる。
6. 不正の複製。連邦著作権侵害法に似ている。しかし、著作権に関する法規を設定する独占権利を議会が有しているため、ほとんどの州がコンピュータ・プログラムおよびデータの複製行為を、州に対する重要犯罪と定義していない。
7. 認証使用の妨害。この法規は約 4 分の 1 の州によって採択されており、承認を受けたユーザーによるコンピュータ・システムの完全使用を妨げるような行為を禁止するものである。例えば、不正のプログラム使用が、情報処理の機能のスピードを遅らせ、「サービス停止（denial of service）」を引き起こしたような場合は、この法規下で犯罪行為と見なされる。
8. 不法な注入及び汚染。ウイルス、寄生虫（worms）、論理爆弾（logic bombs）などを、電話線もしくはフロッピーディスクを通してコンピュータ内に移植もしくは伝送する行為を犯罪行為とみなす。犯罪に使用されるプログラムは、ネットワークもしくはフロッピーディスクを通して間接的に伝達される可能性が高いため、違法者が実際にコンピュータを使用、もしくはアクセスしなくても、「不法な注入行為に至るまでの行為」とみなされ、起訴の対象となる。
9. 不法閲覧。コンピュータには広範囲における機密個人情報保存してある場合が多い。一般市民のプライバシーの権利を保護するため、コンピュータ・システムへの不正アクセスを、データの変更および抽出を行わなかった場合でも、その行為を犯罪とみなす。
10. 所有権の略奪。コンピュータ・システムもしくはシステム内の内容を不正でコントロールする行為。

1998 年、99 年と続々と報告された「チェルノブイリ」、「メリッサ」、「Worm.ExploreZip」などの洗練されたウイルスが大流行したことを受け、コンピュータ・ウイルス違反者を取り締まるために多くの州政府が新しい法規の制定、もしくは既存の法規の改正を行っている。

## 2. 州の条例

第一章でも述べたように、コンピュータ犯罪対策法は各州によって異なる。ここでは、カリフォルニア州、イリノイ州、フロリダ州、ジョージア州、ニューヨーク州の条例を例に挙げて紹介する。

## カリフォルニア州

カリフォルニア州は、他州と異なり、コンピュータ・ウイルスの定義を一步踏み込んだ形で明確に行っている。「所有権に対する犯罪」という規約内に「コンピュータ犯罪」を設け、用語定義の項目(b)において、「computer contaminant (コンピュータ汚染物)」を「computer instructions commonly called viruses (通常ウイルスと呼ばれるコンピュータによる指示)」と定義している。そして、項目(c)で、「意図的にコンピュータ汚染物を導入する行為」を犯罪と見なす、と明記している。

CALIFORNIA PENAL CODE, TITLE 13. Crimes Against Property, CHAPTER 5. Larceny

カリフォルニア州刑事規約、タイトル 13、所有権に対する犯罪、チャプター5、窃盗罪

502. Computer crimes

502.コンピュータ犯罪

(b)

(10) "Computer contaminant" means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, which are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

(“コンピュータ汚染物”とは、情報の持ち主による許可なしに、コンピュータおよびコンピュータ・システム、コンピュータ・ネットワーク内の情報を、変更または損害を与えたり、破壊、記録、もしくは送信するようデザインされた一連のコンピュータによる指示を指す。コンピュータ汚染物には、通常ウイルスもしくは寄生虫と呼ばれ、自己再生または自己繁殖を行い、他のコンピュータ・プログラムやデータを汚染し、コンピュータの資源を消費し、データを変更、破壊、記録、送信し、ある場合には、コンピュータおよびコンピュータ・システム、コンピュータ・ネットワークの通常行われるべき操作を奪取するようデザインされた一連のコンピュータによる指示を含み、これのみに留まらない。)

(c)

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

( コンピュータおよびコンピュータ・システム、コンピュータ・ネットワークに、意図的に、コンピュータ汚染物を導入する行為 )

### イリノイ州

イリノイ州は、「コンピュータ犯罪」という規約内に「コンピュータ不正操作 ( Computer Tampering )」を設けている。他の多くの州と同様、「ウイルス」による犯罪という明言は避け、「コンピュータに損害を与える、もしくは破壊するような情報もしくはコマンドを含むプログラム」という表現が使用されている。そうすることにより、できるだけ広範囲における被害が対象となるよう意図されている。

#### ARTICLE 16D COMPUTER CRIME

##### 条項 16D コンピュータ犯罪

Short Title: Computer Crime Prevention Law

##### コンピュータ犯罪防御法

Sec. 16D-3 Computer Tampering

##### 16D3 節 コンピュータ不正操作

(a)

(4) Inserts or attempts to insert a “program” into a computer or computer program knowing that such “program” contains information or commands that will or may damage or destroy that compute, or any other computer subsequently accessing or being accessed by that computer, or that will or may alter, delete or remove a computer program or data from that computer, or any other computer program or data in a computer subsequently accessing or being accessed by that computer, or that will or may cause loss to the users of that computer or the users of a computer which accesses or which is accessed by such “program”.

コンピュータに損害を与える、もしくは破壊するような情報もしくはコマンドを含む『プログラム』を、意図的にコンピュータ内に注入する行為、またはそのコンピュータによって他のコンピュータが続いてアクセスしたり、またはアクセスされたり、または、そのコンピュータからコンピュータ・プログラムもしくはデータが変更、消去、撤去されたり、または、そのコンピュータのユーザーもしくはそのような『プログラム』にアクセスした、またはアクセスされたコンピュータのユーザーに何らかの損失を与えたり、将来与える可能性がある場合。

## フロリダ州

フロリダ州は、「コンピュータ関連犯罪」に「コンピュータ・ユーザーに対する犯罪」を設けている。ここでも、イリノイ州、その他と同様、いわば典型的な条例を設けており、カリフォルニア州法にあるようなウイルスに的を絞った明確な定義は行っていない。その代わりに、ウイルスは、「意図的に承認なしでコンピュータにアクセス」することにより損害を引き起こす 1 つの方法として位置付けられている。

TITLE XLVI CRIMES, CHAPTER 815, COMPUTER-RELATED CRIMES

タイトル XLVI 犯罪、チャプター815、コンピュータ関連犯罪

815.06 Offenses against computer users.

815.06 コンピュータ・ユーザーに対する犯罪

(1) Whoever willfully, knowingly, and without authorization accesses or causes to be accessed any computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another commits an offense against computer users.

意図的に承認なしでコンピュータおよびコンピュータ・システム、コンピュータ・ネットワークにアクセス、またはアクセスされるよう図った者、または、意図的に承認なしで承認ユーザーによるそのようなコンピュータ・システムの使用拒否を引き起こし、そのコンピュータが他の者によって全部及び部分的に所有、または他の者のために機能している場合、その者はコンピュータ・ユーザーに対して犯罪を犯すことになる。

## ジョージア州

ジョージア州は、「偽造および詐欺」に「コンピュータ・システム保護」を設けている。ここでも「ウイルス」の明言は避け、「コンピュータ停止などを引き起こす行為」として、広義における定義がなされている。

TITLE 16. CRIMES AND OFFENSES, CHAPTER 9. FORGERY AND FRAUDULENT PRACTICES

タイトル 16 犯罪、チャプター9、偽造および詐欺

ARTICLE 6. COMPUTER SYSTEMS PROTECTION

条項 6 コンピュータ・システム保護

16-9-92.

(9) “use” includes causing or attempting to cause:

「使用」とは以下のような結果を引き起こす、または引き起こそうとする行為を含む。

(A) A computer or computer network to perform or to stop performing computer operations;

コンピュータおよびコンピュータ・ネットワークを使用する、またはコンピュータ操作を停止させる。

(B) The obstruction, interruption, malfunction, or denial of the use of a computer, computer network, computer program, or data; or

コンピュータおよびコンピュータ・ネットワーク、コンピュータ・プログラム、データなどの妨害、中断、故障、使用拒否を起こす。

(C) A person to put false information into a computer.

コンピュータに不正な情報を注入する人物。

### ニューヨーク州

ニューヨーク州も、「ウイルス」という言葉は使わず、「窃盗に関連する犯罪」に「コンピュータの不正使用」を設け、「コンピュータを承認なしで意図的に使用」することを「不正使用 (Unauthorized use of a computer)」として広義における定義を行っている。

PENAL LAW PART THREE Specific Offenses TITLE J Offenses Involving Theft

刑法パート 3、特定犯罪、タイトル J、窃盗に関連する犯罪

ARTICLE 156 Offenses Involving Computers; Definition of Terms

条項 156、コンピュータに関する犯罪、用語定義

156.05. Unauthorized use of a computer

156.05 コンピュータの不正使用

A person is guilty of unauthorized use of a computer when he knowingly uses or causes to be used a computer or computer service without authorization and the computer utilized is equipped or programmed with any device or coding system, a function of which is to prevent the unauthorized use of said computer or computer system.

コンピュータおよびコンピュータ・サービスを承認なしで、意図的に使用、もしくは使用されるよう図り、使用されたコンピュータが、前記のコンピュータおよびコンピュータ・システムの不正使用を防止するための機器またはコーディング・システムが装備およびプログラムされている場合、その者は、コンピュータの不正使用によって有罪となる。

Unauthorized use of a computer is a class A misdemeanor.

コンピュータの不正使用は A 級の軽犯罪である。

### 3. 問題点と解決策

#### 管轄区域間の調整

コンピュータ犯罪のほとんどが複数の州をまたがって行われるため、コンピュータ犯罪者を起訴するためには、連邦と州政府による合同作業が必要となる。連邦政府と州政府との間における協力体制は徐々に確立されつつあるものの、依然として、連邦と州政府との間でその管轄権をめぐる意見の食い違いがみられる。さらに、州の警察は、他州において、捜査令状の使用、目撃者の召喚、関連文書の没収、容疑者の逮捕を行うことができないため、州間、または地方自治体間の調整も必要となる。

スパイ行為や連邦政府財産に対する犯罪、誘拐や麻薬取引などの複数の州をまたがって行われる従来の犯罪は、連邦法の管轄分野としてみなされ、コンピュータ犯罪も一般的には連邦レベルで取り締まりが行われるとみなされていた。しかし、最近、州レベルにおいてもウイルス氾濫を含めたコンピュータ犯罪を積極的に取り締まる動きが見られる。司法管轄権を確立するために、裁判管轄区条項 (venue provisions) を設定して、州の権限を拡大しようとする州も存在する。「コンピュータ犯罪発生場所」を明確に定義した条項を既存の州法に追加することで、州が司法管轄権を確立することができる。「コンピュータ犯罪発生場所」の定義として、犯罪が行われるまでに何らかの行動が取られた場所、被害者の居住区または主要事業場所、または不法アクセスがなされたコンピュータ・システムが位置していた場所、および犯罪者が違法に入手したものをコントロールまたは保持していた場所、とされている。モデムを使用すればどこからでもコンピュータにアクセスできることから、コンピュータ犯罪者は、1 つの犯罪で多数の管轄地域において起訴される可能性がでてくる。

#### 法執行体制

州レベルでは法整備に加えて、犯罪者の摘発、逮捕などのエンフォースメントの体制を整えることが課題となる。いくつかの州・地方自治体ではコンピュータ犯罪を取り締まるための特別チームを編成している。例えば、ニューヨーク州においては、1990 年代の初期から半ばにかけて、ニューヨーク州警察、ニューヨーク市、いくつかの周辺地方自治体が、特殊コンピュータ犯罪対策ユニットを設立している。これによりニューヨーク州警察は 90% の逮捕率を報告している。西海岸では、カリフォルニア州のサクラメントにある 4 つの郡部が合同で対策委員会を設置し、コンピュータ犯罪の抑止を行っている。この対策委員会では 1997 年から数千人もの担当官に対して特別トレーニングを行っており、全米モデルケースとして注目を浴びている。

しかし、コンピュータ犯罪の対策として特別な対応もしくはトレーニングを施していない州も存在している。このような州においては、警察官の数を増やしたり、コンピュータ技術を持つ担当員をもっと雇い入れることにより現状を改善することが望まれている。

### **資金不足**

多くの州や地方自治体が財政難のため、コンピュータ犯罪取締のための人材確保やトレーニングなどを行えない状態となっている。その解決策として、犯罪に使用されたコンピュータ機器を没収する権限を拡大するためにコンピュータ犯罪に関わる州法を改正する州も存在する。例えばイリノイ州は、没収したコンピュータ機器から得られた資金を、コンピュータ犯罪捜査を担当する地方自治体と、起訴を行う郡とに与え、担当官のコンピュータ・トレーニングに使用する、とした条項を規定している。また基金の一部は州検事裁判所への特別基金としても使用され、このような取り組みは、州の資金不足が解決されるとして注目を浴びている。

### **民事訴訟の奨励**

連邦政府と同じように、州政府や地方自治体の警察当局は、コンピュータ違反者を起訴にまで持ち込むことは困難であるとの見方をしている。特に、刑事訴訟にかかる時間と費用を敬遠して被害者が捜査に協力的でない場合が多い。このような問題を解決するために、アーカンソー、ジョージア、オクラホマ、ロードアイランドなどの州では、損害賠償を要求できるという側面を強調し、被害者が民事訴訟に出ることを奨励し、それによってコンピュータ犯罪の報告数を増やすことを試みている。