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[1]

[1] 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。

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[2]。

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[3]。

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

---

[2] 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。

[3] 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。

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[4]

(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[5]

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

---

[4] 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。

[5] 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。

(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

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[6]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

---

[6] 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。

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。

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[7]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

---

[7] 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。

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。[8]

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）

---

[8] 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。

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

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[9]。

(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)

---

[9] 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[10]、刑事判決の数は以下のように限られている。

[10] 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）[11]

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**[12]

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。

---

[11] 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)）。

[12] 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

なお、この判決については、資料編を参照のこと

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）[13]

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[14]。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[15]、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。

---

[13] 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)）

[14] 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）。

[15] 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。

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[16]。

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[17]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。

---

[16] 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。

[17] ウィスコンシン州制定法第 943.70(2)条（Wis. Stat. §943.70(2)）。

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」[18]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）[19]

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

---

[18]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

[19] 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)

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。

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[20]

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[21]が警告を発する。

---

[20] 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

またさらに、FBI や NIPC(National Infrastructure Protection Center[22])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

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[23]。

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[24]。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[25]。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[26]。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[27]。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[28]を持つという理由である[29]。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

---

[21] カーネギー・メロン　コンピュータ緊急対策チーム

[22] 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。

[23] 後に逮捕される容疑者 Smith は拡散の意図を否定している。

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

[25] Federal Human Resources Week May 31, 1999

[26] 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）

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

[28] 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。

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

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[30]。

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[31]。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 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。

---

[30] http://www.zdnet.co.jp/news/9904/01/melissa1.html
[31] 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。

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[32]。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[33]。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
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

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

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[34]。
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。

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;

---

[34] 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。

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、破壊または窃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、あるいは窃取したならば、その人間は第３級の犯罪で有罪である

と定めており[35]、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

---

[35] 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

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
<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>

---

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.