

# コンピュータ・ネットワークに関連する犯罪と刑事立法（二・完）

南 部 篤

- I はじめに
- II コンピュータに関連する犯罪の概念
  - 1 検討対象とコンピュータ「犯罪」
  - 2 コンピュータ犯罪の登場
  - 3 コンピュータ犯罪の広がり
  - 4 コンピュータ犯罪からネットワーク犯罪へ
- III 法解釈による対応の限界
  - 1 データの侵害と文書犯罪
  - 2 コンピュータを用いた不正な財産的事務処理と財産犯罪
  - 3 コンピュータを利用する業務への加害行為など（以上前号、以下本号）

IV ネットワーク犯罪をめぐる刑事立法の動向

1 コンピュータ犯罪刑事立法

2 不正アクセス刑事規制立法

3 ネットワーク犯罪刑事立法

V ネットワーク犯罪刑事規制の課題

1 ネットワーク犯罪刑事立法の検討

2 刑事立法のあり方——フランス刑法との比較から——

VI むすび

IV ネットワーク犯罪をめぐる刑事立法の動向

1 コンピュータ犯罪刑事立法

(1) 一九八七年(昭和六二年) 刑法一部改正

一九八〇年代ころのコンピュータ関連犯罪をめぐる法状況は、すでにみたように、①データの改ざん行為と偽造罪、②コンピュータへの加害行為と業務妨害罪、③コンピュータ・システムを用いた財産的利得行為と財産犯罪、④データの消去行為と毀棄罪などの点で、法解釈上の困難性から刑事規制が大きな課題に直面し、拡張的解釈による対応が限界点に達した感があった。さらに、⑤データの不正入手、⑥コンピュータの無権限使用・無権限アクセス等、新たな犯罪化の要否が検討を迫られる状況にあった。<sup>62)</sup>

そのような背景の下で、一九八六年から刑事立法に向けた具体的な動きがはじまり、翌一九八七年五月二七日、コンピュータ犯罪関係の処罰規定の新設を重要部分とする「刑法等の一部を改正する法律」（以下「一九八七年改正」という。）が成立し、同年六月二日に公布された。

この改正は、「もともと現行刑法による的確な処罰が可能であった行為と同様の行為であるにもかかわらず、コンピュータの出現に伴い事務処理形態が変化したため、的確な処罰が困難となった類型の行為について、処罰規定を整備しようとする」趣旨の下に、上の①から④の点に関する処罰規定の新設を行うことを中心とするものであった。<sup>64</sup> ①ないし④の点が、従来の文書偽造罪・業務妨害罪・財産犯罪・毀棄罪に対応する行為であり、それらの罪の分類とも合致するのに対して、⑤と⑥の点については、新しい問題であり保護の範囲・程度などさらに種々の観点から検討すべき点が多いことから、法制審議会での審議の段階で立法化は見送られた。<sup>65</sup>

改正の主な内容は、①データの改ざん行為を捕捉するための「電磁的公正証書原本不実記録・供用罪（一五七条・一五八条）」、「電磁的記録不正作出罪（二六一条の二）」、「不正作出電磁的記録供用罪（二六一条の二第三項・第四項）」、②コンピュータへの加害行為を捕捉するための「電子計算機損壊等業務妨害罪（二三四条の二）」、③コンピュータ・システムを用いた不正な財産的利得行為を捕捉するための「電子計算機使用詐欺罪（二四六条の二）」、④データの消去行為を捕捉するための「電磁的記録毀棄罪（二五八条・二五九条）」、の処罰規定を新設し、また、「電磁的記録の定義（七条の二）」を設けるものであった。<sup>66</sup>

この改正の特徴は、まず、コンピュータ犯罪処罰規定を盛り込んだ特別法を制定するという方式に依らず刑法典中に規定を新設する方式がとられたこと、また、法典中に「電子情報処理組織に関連する罪」のような独立の章を設け

るのではなく、上にみたように、文書偽造罪、業務妨害罪、詐欺罪、文書毀棄罪といった既存の犯罪類型を修正・拡張した類型を創設し、それらを従来の条文の前後に配置し、あるいは従来の条文中に組み入れるという方法をとった点にある。

内容的には、「不正作出」の概念の導入により、記録の有形偽造的行為、無形偽造的行為を区別せずに不正なデータを作り出す行為を捕捉することとした点が重要である。これにより処罰範囲は実質的に拡張されたともいえる。文書偽造と電磁的記録不正作出とをパラレルに考えると、「文書の信用性（証明機能）の保護」のために作成名義の偽りの有無が問題になるのだから、「データの信用性（証明機能）の保護」のためには、そのデータの作成名義を問題にせざるをえないのではないかと思われる。そうすると、この電磁的記録不正作出罪は、従来の文書偽造罪の保護法益とパラレルにとらえられるもの（データの信用性・証明機能）とは大きく異なる、「情報処理の正しさ」とでもいべきものを保護法益とする、情報処理阻害を処罰する規定になってしまっており疑問があるという見方もできることとなる。<sup>67</sup>

電子計算機損壊等業務妨害罪については、従来の業務妨害罪に比して重い法定刑が設定された点など、特に厚くコンピュータの保護を計ろうとした側面もないわけではない。<sup>68</sup>

しかし、諸外国の立法例と比べれば、概して慎重な態度をとった比較的制限的な立法といえるものであるとの評価が一般的であった。そして、従来の犯罪の周辺にある当罰性が明白な行為に絞って犯罪化が行なわれたため、不正アクセスなどシステムへの侵害行為や、コンピュータの無権限使用、システム中のデータの不正取得（入手）などが欠落した立法となったこと、すなわち、それらの最も大きな問題を孕んだテーマを、いわば「積み残された課題」とした点が、このわが国初のコンピュータ犯罪刑事立法の最大の特徴といえるであろう。

(2) 二〇〇一年(平成十三年) 刑法一部改正

今日、クレジットカードやキャッシュカード、プリペイドカードなど多種多様なカードが普及し、その利便性と安  
全性等から代金・料金の支払い、預貯金の引き出しなどに広く用いられている。このような各種カードの著しい発展  
が、自動化された電子的決済によって瞬時に確実に事務処理が行われることに支えられていることはいうまでもない。  
そして、そのような処理は、消費者の所持する各種カードに組み込まれた電磁的記録を専用の機器が読み取るなど、  
自動化された所定の処理が行われることにより実現されている。すなわち、ここでも、社会生活がこのような電子的  
処理・決済手段の働きに大きく依存するようになってきていることが背景となっているのである。

すでに見たように、キャッシュカードの偽造事案などを契機として、電磁的記録の不正作出行為を犯罪化するよう  
立法的手当てが行われていたが、その後、「スキミング」とよばれる手口でクレジットカードの電磁的記録中の情報  
のみを不正に入手して、偽のカードを作り出して使用するという犯行が組織的に行われる等被害が急増した。ところ  
が、偽造されたクレジットカードの所持や偽造の準備行為を処罰する規定がなかったため、大量の偽造カードを所持  
する者が発見されても、スキミング行為が確認されても、検挙できなかったのである。また、支払い決済手段という  
社会的機能の共通性にもかかわらず、クレジットカード、キャッシュカードの改ざん等は文書偽造・電磁的記録不正  
作出で処罰され、他方、プリペイドカードは有価証券偽変造と扱われることで、処罰される行為の態様や法定刑に不  
均衡を生じていたのである。<sup>69)</sup>

このような事情を背景に、二〇〇一年六月二六日、各種支払用カードを構成する電磁的記録の不正作出、所持、そ  
の情報の不正取得などの処罰規定を整備する「刑法の一部を改正する法律」(以下「二〇〇一年改正」という。)が成立し、

同年七月四日に公布された。

改正の内容は、刑法典の「第十八章 有価証券偽造の罪」の次に、新たな章である「第十八章の二 支払用カード電磁的記録に関する罪」を追加し、①支払用カード電磁的記録不正作出（一六三条の二第一項）、②不正作出支払用カード等供用（一六三条の二第二項）、③不正作出支払用カード等譲渡・貸与・輸入（一六三条の二第三項）、④不正作出支払用カード等所持（一六三条の三）、⑤支払用カード電磁的記録不正作出準備（一六三条の四）の各規定を新設するものである。⑤の電磁的記録不正作出の準備行為に関する規定は、<sup>(70)</sup>①カードの不正作出のための情報を取得する行為と情報を提供する行為を（同条一項）、<sup>(71)</sup>②その情報を保管する行為を（同条二項）、<sup>(72)</sup>③不正作出のための器械、原料の準備行為を（同条三項）を処罰対象として規定している。

立案当局の見解では、本罪は、支払用カードを構成する電磁的記録の真正、ひいてはこれら支払用カードを用いた支払いシステムに対する社会的信頼を保護法益とするものであり、通貨偽造の罪、有価証券偽造の罪と並ぶ偽造罪と位置づけられている。<sup>(71)</sup>しかし、電磁的記録部分を有する各種の支払用カードの多くが、自動化された機械に用いることを予定しており、中にはプリペイドカードのように対人的な使用を想定していないものも多いことから、人の判断作用を前提とする従来の各種偽造罪とは異なる性質の法益を保護する犯罪類型となっているのではないか、という疑問が生じる。<sup>(72)</sup>この点は、後に検討を加える。

なお、支払用カード電磁的記録不正作出準備罪（一六三条の四）は、電磁的記録の情報の取得、提供、保管の処罰を規定した。この、情報自体を、初めて構成要件の中に侵害行為の向けられる客体として取り込む規定が設けられた点は重要であろう。これは、偽の支払用カードを不正に作る目的で行われるカード情報の「スキミング」という、ま

さに物の占有を害することなく、情報だけをすくい取る手口を直接捕捉しようとする規定であることから分かるように、刑法が、容易に物から分離して取得・複製・保存・利用される情報を、正面から捉える必要に応えたものであるとみることができると思われる。<sup>(73)</sup>

## 2 不正アクセス刑事規制立法

### (1) 不正アクセス禁止法制定の背景

すでに見たように、一九八七年改正の際、コンピュータ・システムへの不法侵入（不正アクセス）行為については、今後の検討課題として犯罪化が見送られた経緯がある。そこでは、不正アクセスは、結局のところ、データの不正操作・不正入手、コンピュータの無権限使用・破壊といった諸類型の予備的手段であり、コンピュータの情報処理機能に対する実質的加害とは必ずしも言えないということが理由とされた。<sup>(74)</sup> 外部からのコンピュータへのアクセス行為が管理されている状態は、未だ刑罰的保護が必要なものとは評価されなかったのである。

しかし、一九九〇年代半ば以降のインターネットの急激な普及により状況は一変する。ハードウェア・プログラム・データなど個々の部分の保護から、それらの機器、通信環境、技術の結合により実現される「コンピュータ・ネットワーク・システム」の機能が、社会の最も重要なインフラとして働くようになると、その保護の必要性が自覚されるようになる。たとえば、従来、閉じた内部ネットワークを介してコンピュータを利用していた研究機関や行政機関、金融機関等のコンピュータも、今日では一般に開放されたインターネット接続環境の中で利用されているのである。<sup>(75)</sup>

このような事情を背景に、一九九九年八月一三日、不正アクセスを禁止し、罰則その他の規定を定め、ネットワー

クを介して行われる犯罪の防止とネットワークに関する秩序の維持を図ることを目的とする「不正アクセス行為の禁止等に関する法律」が成立し、同年二月に公布された。<sup>(76)</sup>

(2) 不正アクセス罪の保護法益と問題点

本法が処罰対象とする行為の中心、不正アクセスとは、アクセス制御機能のあるコンピュータに、電気通信回線を通じて、権限なく接続を確立する行為をいう(同法二条四項)。これは、「アクセス制御機能の存在」と「無権限のアクセス」との組み合わせによつて、アクセスコントロールの侵害を捉え処罰しようとするものである。すなわち、このような不正アクセス行為を処罰する理由は、「アクセス制御機能による利用権者等の識別に対する社会的信頼を害することにより、コンピュータ・ネットワークにおけるハイテク犯罪の抑止力を失わせてこれを助長するおそれを生じさせるとともに、ネットワークを無秩序な状態にし、安心してネットワークを利用できない事態を招いてネットワーク相互の接続を抑制し、ひいては高度情報通信社会の健全な発展を阻害する危険性を有する」<sup>(77)</sup>からにほかならない。したがつて、本罪は、コンピュータ・ネットワークの秩序に対する社会的信頼を保護法益とするものと考えられる。

一九八七年改正以来の状況の変化が、ネットワーク外部からのコンピュータへのアクセスが管理されている状態自体を刑罰で保護すべき、との認識を導いたといつてもよい。無権限のアクセスを財産犯罪等の予備的な行為とする認識<sup>(78)</sup>は、ネットワーク社会の発展段階が、適正なアクセスコントロールが及んでいる状態自体に刑罰による保護の必要性を認めるほどに達していなかったからにほかならない。

なお、本罪が財産犯罪等の予備的性格のものではないとしても、本罪Ⅱ不正アクセス行為を手段に、(それ自体は直接の罰則を欠く)コンピュータの無権限使用やデータの不正入手が行われる場合は、不正アクセス罪で捕捉可能と

なった段階で処罰が可能となるのは当然である。すなわち、情報の不正取得等の手段として行われた無権限のアクセスを処罰することにより、結果的に、ネットワーク上の情報に対する刑罰的保護として働くものとなっているともいえる。<sup>(79)</sup>

さらに、二〇〇三年の改正によって「不正競争防止法」に導入された、営業秘密の不正取得、使用および開示を処罰する規定<sup>(80)</sup>は、「管理侵害行為」によつて取得された営業秘密を不正に使用する行為、開示する行為等を処罰しているが、ここにいう管理侵害行為の一つとして「不正アクセス行為」が規定されており、不正アクセス行為によつて得られた一定の情報の不正使用等が可罰的なものとされている。<sup>(81)</sup>

### 3 ネットワーク犯罪刑事立法

コンピュータ・ネットワークの発展・普及が一層進むなかで、ネットワークを利用する犯罪や、ネットワークを侵害対象とする犯罪は猛威をふるい続けた。<sup>(82)</sup> 前者のネットワーク利用犯罪には、詐欺をはじめとして多様なものが含まれるが、①電子メディアを用いたわいせつ物頒布等の罪の適用に関し解釈上の問題を生じていた。後者のシステムを侵害する不正行為には、不正アクセスなどが含まれるが、②コンピュータ・ウイルスの問題に関し、立法による対処が待たれていた。また、「ヨーロッパ評議会サイバー犯罪に関する条約 (Council of Europe Convention on Cybercrime) (二〇〇一年一月八日、ヨーロッパ評議会閣僚委員会採択、同月二三日、わが国も署名) の批准に向け、国内法整備の一環として法改正を要する事態が続いていた。

このような背景の下で、当初の法案提出から七年あまりを経て、二〇一一年六月一七日、サイバー犯罪関係の罰則等の整備を中心とする「情報処理の高度化等に対処するための刑法等の一部を改正する法律」が成立し、同月二四日

に公布された。<sup>(83)</sup> 以下に、上の①、②の点に関する改正内容について検討を加える。

(1) わいせつ物頒布等の罪関係

改正前のわいせつ物頒布等の罪(刑法一七五条)は、「わいせつな文書、図画その他の物」の陳列行為等を処罰の対象としていたため、有体物以外は客体とすることが困難であった。典型的なものとしては、写真や絵画のようにわいせつな映像がそこに表示された可視的対象物が想定されていたが、映画フィルムやビデオテープ、録音テープなど再生用機器を用いてわいせつ情報を発現させることのできる形態の物も含めて客体とされてきた。<sup>(84)</sup>

陳列行為の客体は、フィルム、ビデオテープ、録音テープというわいせつ情報が固定された有体物と考えられており、このような解釈手法は、やがて登場したパソコン通信、さらにインターネットを用いたわいせつ画像提供行為をわいせつ物陳列罪に問う多くの裁判例——そこではわいせつ画像データを保存したコンピュータのハードディスクが客体と捉えられた——に引き継がれていき、やがて最高裁により承認されることとなる。<sup>(85)</sup>

この決定については、「わいせつ性の顕在化の容易性を条件として、その物自体から直接的なわいせつ性の認識可能性までは要求せず、他方でその物についての有体物性は堅持するという、一七五条の罪の客体性についての従来からの判例解釈上の展開を踏襲するもの」<sup>(86)</sup>とか、「従来、すでに実務上固まっていたと見ることができ」<sup>(87)</sup>このような法的処理が、「最高裁によつて是認された」<sup>(88)</sup>との評価が示されたが、画像データ自体を陳列の客体とする構成を採る裁判例や、画像データ自体を客体と解する学説<sup>(89)</sup>もあり、学説上の争いは収束したとはいえない状況にあった。

また、最高裁により承認されたハードディスク客体説は、その説明が不自然で技巧的な印象を与える点を除けば、妥当な結論を導く無難な解釈といえるかもしれないが、電子メールを用いたわいせつ画像送信事案の発生が、そのよ

うな法解釈の限界をあきらかにした。すなわち、ネット上の広告に応じて代金を支払った客宛に画像データを電子メール添付で送信したケースである。このような事案に、わいせつ物販売罪の成立を肯定するためには、画像データ自体を同罪の客体と認めるほかなかったのである。実際にこれを認めて有罪を言い渡した二件の判決が現れたが、いずれも、客体の有体物性の要求を説得力の不十分な説明で乗り越えようとしたことから強い批判にさらされたのである。<sup>91</sup>

こうして、電子データを用いた事案のような、当罰性において従来のわいせつ物販売とまったく変わらないもの——法益侵害性の点ではより悪質ともいえる事案——の処罰が不可能になり、立法的解決が必要とされるにいたったのである。

そこで、この改正により、①一七五条の客体に、「電磁的記録に係る記録媒体」がつけ加えられ、②同条後段に、「電気通信の送信によりわいせつな電磁的記録その他の記録を頒布した者」を、同様に罰する規定が設けられたのである。この①頒布と公然陳列の客体の例示に、「電磁的記録に係る記録媒体」を付け加えた部分は、前述の最高裁の判例を追認したものであり、処罰範囲を明確にするという意義を認めうる。これに対して、②の電気通信の送信によるわいせつな電磁的記録の頒布を処罰する規定を設けた点は、処罰範囲を拡張し、電子メール送信のようなケースを捕捉可能にするという意義を有するものである。

しかし、陳列による場合は、客体が有体物に限定されるが、頒布による場合は有体物であると、無形の電磁的記録自体であることを問わないことになるが、ネットワーク経由で送信する頒布の場合は客体足りうるのに、ネットワーク経由の陳列の場合は客体足りえないこととなるのはなぜかという疑問が生じる。また、「電気通信の送信によりわい

せつな電磁的記録その他の記録を頒布した」とは、電子メールへのファイル添付による場合を想定したものとと思われるが、前段にいう、記録媒体の公然陳列が想定する、ウェブページによるわいせつ画像の提供も、「電気通信の送信」による電磁的記録送付行為とみる余地があるのではないか。<sup>(92)</sup> これらの点からは、この改正が、一方で有体物性の要求に拘りながら、同時に処罰の間隙を埋めるために電磁的記録等の送信行為を捕捉しようとし、そのため、電子データ等と物との関係の整合的な把握を欠いたままに規定の新設が行われたのではないか、という疑問を払拭できないのである。<sup>(93)</sup>

## (2) 不正指令電磁的記録作成関係

「コンピュータ・ウイルス」は、コンピュータに侵入してユーザーの意図とは異なる動作をさせるよう作られた不正なプログラムを、生物に感染する病原体になぞらえて用いられるようになった表現であるが、一九八四年にアメリカの研究者によって使われたのが最初の用例とされる。<sup>(94)</sup> わが国においては、一九八八年にアメリカ製輸入ソフトのウイルス感染が初めて発覚し、また同年に、日本電気社が主催する国内最大級パソコン通信のPC-VAN上でウイルスが発見され、その後次々とウイルスの被害が明らかになり、情報化社会を脅かす大きな脅威として注目を集めた。「コンピュータウイルス元年」などと呼ばれたが、いずれもインターネット普及以前の事案であり、一般のユーザーのなかにネット経由でウイルスが感染力・破壊力を発揮する時期の到来以前のことである。<sup>(95)</sup>

コンピュータ・ウイルスは、経済産業省の「コンピュータウイルス対策基準」(通商産業省告示・第一三九号)によれば、「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、①自己伝染機能(自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコ

ピーすることにより、他のシステムに伝染する機能)、②潜伏機能(発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能)、③発病機能(プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能)のうち、いずれか一つ以上の機能を有するものをいう。」と定義される。<sup>(96)</sup> また、警察庁は、「コンピュータウイルスとは、不正プログラム(不正命令)であつて、増殖機能を有するもののうち、正常なプログラムに組み込まれた状態で存在するものをいう。」と定義づけている。<sup>(97)</sup> なお、コンピュータ・ウイルスは、コンピュータ・システムの正常な動作に害をもたらす多種多様な不正プログラムの「家族の一員」である——刑事規制の対象とすべきは、ウイルスを含むそれら不正プログラムの総体ということになる——といわれている。<sup>(98)</sup>

前出の「コンピュータウイルス対策基準(経済産業省(制定時、通商産業省)告示)」に基づいて、感染被害を発見した場合、「被害の拡大および再発を防止するために必要な情報を経済産業大臣が別に指定する公的機関に届け出ること」とされているが、その指定公的機関である情報処理推進機構(IPA)によれば、ウイルス届出件数は、制度が開始した一九九〇年の一四件から、二〇〇〇年に一〇、〇〇〇件代に急増し、二〇〇五年のピーク時には五四、一七四件となり、二〇一〇年には一三、〇〇〇件あまりと、現在はやや減少傾向をみせているもの<sup>(99)</sup>、ウイルスがコンピュータによる円滑な情報処理を阻害する要因となつており、刑事立法による対応が必要な事態が続いていたことはいうまでもない。なお、このような状況にもかかわらず、平成一六年第一五九回国会に最初の法案が提出されて以来、本刑事立法が実現するまでに七年を要した理由は、法案中に「組織的な犯罪の共謀罪の新設を含む：罰則規定が含まれており、特に同罪の新設について様々な意見があつたこと」にあるとされる。<sup>(100)</sup>

この間には、たとえば人気アニメ画像の入ったウイルスを不特定多数に配布・感染させ、コンピュータの動作阻害

等を惹起したケースに、器物損壊罪適用を断念し、著作権法違反で立件した事案<sup>101</sup>や、本改正法施行の約一年前の「タコイカウイルス」と呼ばれる不正プログラムを他人のパソコンに感染させてデータを使用不能にしたケースに、ウイルス作成を直接罰する規定がなかったことから、ハードディスクの物理的破壊をとみなわれないにもかかわらず器物損壊罪を適用して有罪判決を言い渡した判決が出されるなど、刑法解釈の限界線上で処罰の要求に応えようとする実務の対応がみられたのである。

この改正により、刑法典の「第一九章 印章偽造の罪」の次に、新たに「第一九章の二 不正指令電磁的記録に関する罪」の章が挿入され、一六八条の二（不正指令電磁的記録作成等）と一六八条の三（不正指令電磁的記録取得等）の二つの条文が新設された。また、一九八七年改正により設けられた二三四条二（電子計算機損壊等業務妨害）の罪の未遂処罰規定が新設された。

中心となる不正指令電磁的記録（以下「ウイルス」という）作成罪は、「正当な理由なく、他人のコンピュータで実行させる目的で、ユーザーの意図に沿う動作をさせず、またはその意図に反する動作をさせるような不正な指令を与える電磁的記録等を作成し、提供する行為」を処罰する犯罪類型（一六八条の二第二項）である。加えて、ウイルス供用・取得・保管の各罪（一六八条の二第二項・同三項・一六八条の三）<sup>103</sup>が設けられた。

本罪は、人がコンピュータを使用するとき、「コンピュータのプログラムが、その意図に沿った動作をさせず、またはその意図に反する動作をさせるような不正な指令を与えるものではない」との信頼、すなわち、そのような「コンピュータのプログラムに対する社会一般の信頼」を保護法益とするものであつて、文書偽造の罪等と同様に社会的法益に対する罪であるとされる。<sup>104</sup>

ウイルスによる実害発生に着目し、電磁的記録毀棄罪や電子計算機損壊等業務妨害罪の予備罪的構成とすることも可能であったところ、立法者は、コンピュータ・プログラムに対する社会的信頼を保護法益とし、ウイルスのもたらす各種実害とは無関係の独自の犯罪類型としたわけである。すでに法案段階において、ウイルス作成行為は、「社会に害悪をもたらす根源を生み出す行為として、重い犯罪性を備えたものと評価されることになり、それは単なる加害行為の予備との評価にとどまるものではないことになる。これは、通貨偽造罪が：単なる詐欺罪の予備にとどまるものではないことと同様である。」<sup>(105)</sup>と述べ、このような罪質・構造の類型として構想することを肯定的にとらえる見解が示されていた。これに対して、本罪が実害と切り離された独自の類型とされた点について、このような構成は、法益の抽象化によって事実上の処罰の早期化を図るものであり、また、適用範囲の重複など未解決の問題もある等から、ウイルス罪を予備罪的行為を処罰する罪と構成した上で処罰範囲の限定を図るといふ選択肢もあつたのではないかとする批判も加えられている。<sup>(106)</sup>この点については、後に検討を加える。

(62) また、コンピュータ犯罪は一定のレベルに情報化が達成された社会に必然的に生じる問題現象であり、この時期の先進諸国に共通の重要課題の一つでもあつた。一九七〇年代から州法、連邦法の立法の動きが始まつたアメリカ合衆国では、一九八四年に連邦法が成立し、一九八五年にカナダ、一九八六年に西ドイツ、一九八七年に日本（本法）、一九八八年にフランス、とコンピュータ犯罪処罰のための刑事立法が相次いだことがそれを物語っている（廣畑史朗「コンピュータ犯罪と諸外国の立法（上）・（下）」警察學論集三六卷四号八八頁・三六卷五号一二三頁（一九八三）、山口厚「アメリカにおけるコンピュータ犯罪処罰法」ジュリスト八四六号（一九八五）三五頁、井田良「西ドイツにおけるコンピュータ犯罪への対応」同誌同号四二頁、河村博「イギリスにおけるコンピュータ関連刑事立法」同誌同号四七頁、林幹人「アメリカにおけるコンピュータ犯罪規制立

- 法(上)(下)判例時報二二〇二号六頁・二二〇四号二二頁(一九八六)、クラウス・ティーディマン(神山敏雄訳)「コンピュータ犯罪と一九八六年の西ドイツ刑法改正(二)・(三完)」警察研究五九卷二頁・三頁一六頁(一九八七)、神山敏雄「西独における第二次経済犯罪対策法の制定」法律時報五八卷一頁(一九八七)五三頁、山口厚「アメリカにおけるコンピュータデータの刑罰による保護」刑法雑誌二八卷四号(一九八八)五四九頁、瀬川晃「イギリスにおけるコンピュータ犯罪とデータの保護」刑法雑誌二八卷四号(一九八八)五九二頁、拙稿「フランスのコンピュータ犯罪と刑法」法学紀要二九卷一六九頁(一九八八)、拙稿「情報処理関連不正行為に関する一九八八年一月五日の法律第八八一号」国学院法学二六卷一七二頁(一九八八)、恒光徹「フランスの一九八八年コンピュータ犯罪立法について」岡山大学法学会雑誌三八卷四号(一九八九)九三頁、など参照。
- (63) 法制審議会に対する、「電子計算機による情報処理組織の普及にかんがみ、緊急に刑法その他の罰則整備する必要があるか。あるとすればその骨子を示されたい。」との諮問が行われ、審議が開始され、翌年、所定の改正を行うべきことを内容とする「刑法一部改正の骨子」が採択される(米澤慶治編『刑法等一部改正法の解説』立花書房(一九八八)一三頁以下)。
- (64) 米澤慶治「刑法等一部改正法の概要」ジュリスト八八号(一九八七)六五頁。学説の側からも、「今回の改正は、いわゆるコンピュータ犯罪について整備された処罰規定を設けるというのではなく、現行法上の犯罪類型を基礎にして、コンピュータの普及によって生じた可罰性の間隙を埋め…あるいは、コンピュータ利用に関わる不正行為の重大性に見合った処罰を規定する…というものである」って、「今回の改正提案は当面の必要に即した抑制的なものだといえる」という評価が加えられていた(中森喜彦「コンピュータ犯罪と刑法の一部改正」法学教室八一号(一九八七)九三頁)。
- (65) 米澤慶治編『刑法等一部改正法の解説』前掲(註(63))一四一―一五頁。
- (66) この改正を扱った論稿はかなりの数にのぼるが、主なものとして、〈特集コンピュータ犯罪と刑法改正〉山口厚「電磁的記録と文書犯罪規定の改正」、芝原邦爾「コンピュータ犯罪による情報処理と業務妨害罪」、西田典之「コンピュータの不正操作と財産犯」ジュリスト八八号四頁(一九八七)、古田佑紀・多谷千香子「刑法等一部改正法概説(二)」警察学論集四〇

卷八号三一頁（一九八七）、的場純男・川村博「同（二）」同四〇卷九号一二九頁（一九八七）、鶴田六郎Ⅱ横島裕介「同（三）」同四〇卷一〇号一九一頁（一九八七）、横島裕介「同（四）」同四〇卷一一号一〇七頁（一九八七）、横島裕介「コンピュータ関連犯罪に対処するための刑法一部改正の概要（一）」（三完）NBL三八〇号一三頁、三八一号三六頁、三八二号三〇頁（一九八七）、川村博「刑法等一部改正法の概要について」警察研究五八卷一〇号三三頁（一九八七）、的場純男・河村博「コンピュータ犯罪Q&A」三協法規（一九八八）、日弁連編『コンピュータ犯罪と現代刑法』三省堂（一九九〇）などがあり、また、この改正法施行直後の適用事例について検討を加えたものとして、渡辺恵一Ⅱ角田正紀「刑法一部改正（昭和六二年）以後のコンピュータ犯罪（一）・（二）・（三）・（四）」警察公論四四卷一一号二八頁・同誌同卷一二号二八頁、同誌四五卷一七七八頁、同三号七〇頁（一九八九、一九九〇）がある。

(67) 山口厚「電磁的記録と文書犯罪規定の改正」前掲（註(66)）五頁以下。

(68) 神山教授は、わが国の立法は三つの類型に限定するなどアメリカ、ドイツに比してその規模においてやや控えめであるとしながらも、それぞれの中身はかなり包括的で随所に「コンピュータの特権化」が見られると批判した（中山研一Ⅱ神山敏雄編『コンピュータ犯罪等に関する刑法一部改正（改訂増補版）』成文堂（一九八九）四五頁以下「神山敏雄」）。

(69) 長瀬敬昭「刑法の一部を改正する法律について」警察學論集五四卷九号（二〇〇一）一〇二頁。

(70) この改正の経緯および内容については、長瀬敬昭「支払用カードの偽造等の犯罪に対処するための刑法改正に関する要綱案（骨子）の概要」金融法務事情一六〇二号（二〇〇一）六頁、長瀬敬昭「支払用カードの偽造等の犯罪に対処するための刑法改正の概要」金融法務事情一六一九号（二〇〇一）一〇頁、今井猛嘉「支払用カードの保護に関する刑法の一部改正」法律時報七五卷二号（二〇〇一）四五頁、川端博Ⅱ西田典之Ⅱ河村博Ⅱ笠井治「〈座談会〉支払用カードの偽造等に対処するための刑法の一部改正をめぐる」現代刑事法三〇号（二〇〇一）五二頁、井上宏「刑法の一部を改正する法律」同誌同号六四頁、夏井高人「支払用カード罪新設のための刑法一部改正とその問題点」判例タイムズ一〇六一号（二〇〇一）六四頁、を参照。

(71) 井上宏「刑法の一部を改正する法律」ジュリスト一二〇九号（二〇〇一）一〇頁、同「支払用カードの偽造等の犯罪に対処するための刑法改正に関する法制審議会の答申について」ジュリスト一一九五号（二〇〇一）一〇四頁、長瀬敬昭「刑法の

一部を改正する法律について」前掲(註(8))一〇七頁。

(72) 西田典之「カード犯罪と刑法改正」ジュリスト二二〇九号(二〇〇一)一六頁、同『刑法各論(第四版補正版)』弘文堂(二〇〇九)三二八頁。

(73) 拙稿「情報、電子データと物概念の変容」日本法学七六卷四号(二〇一三)五四九頁。この点について、情報窃盗の処罰に一步を踏み出すことになるのではないかという危惧を示す指摘がある(川端博ほか「座談会」支払用カードの偽造等に対処するための刑法の一部改正をめぐって」前掲(註(70))六二頁「笠井治発言」)。

(74) 米澤慶治編『刑法等一部改正法の解説』前掲(註(63))一二頁。

(75) この間の変化については、本稿「II 4 「コンピュータ犯罪からネットワーク犯罪へ」」を参照。

(76) 不正アクセスの規制問題については、研究者、実務家等が参加し、多くの研究機関や官庁により詳細な検討が行われた。たとえば、情報セキュリティ調査研究委員会『情報セキュリティ調査報告書』日本実業出版(一九九七)、情報セキュリティビジョン策定委員会『情報セキュリティビジョン策定委員会報告書』東京法令出版(一九九八)、警察庁・情報システム安全対策研究会・不正アクセス対策法制分科会『不正アクセス対策法制に関する調査研究報告書』(一九九八)警察庁ウェブサイト<<http://www.npa.go.jp/cyber/research/h10/housei/nsreport.html>>visited on Dec. 25, 2011. なす。

(77) 不正アクセス対策法制研究会編著『不正アクセス行為の禁止等に関する法律(補訂第二版)』立花書房(二〇〇八)六六頁。

(78) 米澤慶治編『刑法等一部改正法の解説』前掲(註(63))一二頁。

(79) もとより、ネットワークを介することが「不正アクセス」の前提であるため、他人のパソコンのマウス、キーボード等を直接操作してパソコン内部のデータを無断で自分の持ち込んだメディアに複製し取得しても、同罪に問うことはできない。

(80) この改正は、従来、「営業秘密が有体物(財物)に化体していない場合」にあつては、直接的には刑事的保護が図られていなかった。しかしながら、経済社会の情報化等の進展に伴い、有体物(財物)に化体していない営業秘密が害されるリスクが増大し、このような『処罰の間隙』について罰則を設ける必要性が高まっていた」こと等をその理由とするものであった(経

済産業省知的財産政策室編著『逐条解説・不正競争防止法(平成一八年改正版)』有斐閣(二〇〇七)二二頁。

(81) もとより、アクセス制御に対する社会的信頼が不正アクセス罪の保護法益と解するべきである以上、この不正アクセスの概念に、「情報の不正入手」などの意味を混入させる理解は正しくないであろう(園田寿「ネットワーク犯罪の現状と法的対応」刑事法ジャーナル一五号(二〇〇九)五頁)。

(82) 近時の情勢について、警察白書は、サイバー犯罪の検挙件数が増加の一途をたどっており、二〇一〇年には過去最多となり、なかでもネットワーク利用犯罪は前年の三一・三%増加し過去最高となったことをつたえている(警察庁編『平成二三年度警察白書』(二〇一三)二〇頁)。

(83) 杉山徳明・吉田雅之「『情報処理の高度化等に対処するための刑法等の一部を改正する法律』について(上)、(下)」法曹時報六四卷四号(二〇一三)一頁以下、五号(二〇一三)五五頁以下。法案段階で検討を加えた論稿として、北村篤「ハイテク犯罪に対処するための刑事法の整備に関する要綱(骨子)」ジュリスト一二五七号(二〇一三)六頁、山口厚「サイバー犯罪に対する実体的対応」ジュリスト一二五七号(二〇一三)一五頁、山口厚「サイバー犯罪の現状と課題」現代刑事法六巻一号(二〇一四)四頁、今井猛嘉「ネットワーク犯罪」法学教室三〇三号(二〇一五)五六頁など。

(84) わいせつ情報の多様な発現形態に関する判例については、塩見淳「猥褻物と猥褻情報」判例タイムズ八七四号五八頁以下(二九九五)、佐久間修『最先端法領域の刑事規制』現代法律出版(二〇一三)二九七頁以下、拙稿「わいせつ情報とわいせつ物頒布等の罪の客体」『現代社会型犯罪の諸問題』勁草書房(二〇一四)所収を参照。

(85) 最決平成一三年七月一六日刑集五五卷五号三一七頁。

(86) 永井善之『サイバー・ポルノの刑事規制』信山社(二〇一三)一六四頁。

(87) 山口厚「サイバーポルノとわいせつ物公然陳列罪(最高裁平成一三年七月一六日第三小法廷決定)」平成一三年度重要判例解説一六六頁以下(二〇一三)。

(88) 岡山地判平成九年一二月一五日判時一六四一号一五八頁以下。

(89) 堀内捷三「インターネットとポルノグラフィ」研修五八八号三頁以下(一九九七)、拙稿「わいせつ情報とわいせつ物

頒布等の罪の客体」前掲(註(22))。なお、データ説を明言するものではないが、画像データは、電子的方式により組み立てられた一まとまりの電子データ化された情報であつて、「保存性・可搬性」を備えたものといえらるゝと見解が示峻的である(林陽一「わいせつ情報と刑法一七五條」現代刑事法六卷一號(二〇〇四)一〇頁)。

(90) 横浜地裁川崎支判平一二・七・六、横浜地裁川崎支判平一二年一月二四日(いずれも公刊物未登載。事案の内容等については、拙稿「わいせつ情報とわいせつ物頒布等の罪の客体」前掲(註(84))を参照。ほかには、二〇〇一年に東京都知事と長野県知事宛に電子メールに添付してわいせつ画像を送信した疑いで三人の中学生が自宅の搜索を受け、わいせつ凶画公然陳列の事実で書類送検されたケースがある(二〇〇一年三月二七日付け毎日新聞、同年四月四日付け同紙)。

(91) 園田寿「わいせつ画像データを有料で送信した行為にわいせつ凶画販売罪が認められた事例」判例セレクト二〇〇一(二〇〇一)三七頁、永井・前掲書(註(86))二四八―二四九頁。

(92) インターネットを用いた多くのわいせつ物陳列罪に関する裁判例の判決文中に、「画像を送信し」、「わいせつ画像データを送信し」、「データを送信し」といった表現がみられる。

(93) こういった点に関しては、法案段階で、「このことは、従来の有体物を客体とする規制構造との連続性を重視しすぎた立法態度に原因があるように思われる。有体物を客体とする場合と無体物を客体とする場合とは、異なつた文言による規制を模索すべきであろう。客体の特性に応じた的確な行為態様を含む立法が為されることが望まれる。」との批判が示されていた(渡邊卓也『電腦空間における刑事的規制』成文堂(二〇〇六)三〇九頁)。

(94) 細貝康夫『コンピュータウィルスの安全対策』につかん書房(一九九二)六〇頁、岡田好史『サイバー犯罪とその刑事法的規制』専修大学出版局(二〇〇四)七四頁以下。

(95) 一九八八年から一九九〇年までの主な感染事例二二件を挙げる資料をみると、感染したコンピュータの利用状況は、①大学・研究所等が三件、②コンピュータ・ショップ三件、③コンピュータ・メーカー三件、④パソコン通信会員が二件、⑤ゲームソフト・メーカー一件、となつており、この時期のコンピュータ・ネットワークがまだ発展途上であつたことが反映していることがわかる(細貝康夫『コンピュータウィルスの安全対策』前掲(註(94))三三―三四頁)。

- (96) このウィルスの定義を示した「コンピュータウイルス対策基準」については、経済産業省ウェブページ（<http://www.meti.go.jp/policy/netsecurity/cvirusCMG.htm>） visited on Jan. 9, 2011.）。
- (97) 警察庁コンピュータ・システム安全対策研究会「コンピュータ・ウィルス等不正プログラム対策指針」（一九八九）（同指針については、細貝康夫『コンピュータウイルスの安全対策』前掲（註(94)）八頁以下を参照）。
- (98) それらウィルスの登場以前から知られているものも含めて、不正プログラムには、「トロイの木馬（Trojan Horse）」「論理爆弾（Logic Bomb）」「時限爆弾（Time Bomb）」「ワーム（Worm）」「トラップドアまたはバックドア（Trap Door or Back Door）」「サラミ攻撃（The Salami Attack）」「ボギーバック（Bogyback）」「コバート・チャンネル（Covert Channel）」「ガーベージ・コレクション（Garbage Collection）」「スーパージッピング（Superspapping）」など多様なものがあるが、「コンピュータ・ウィルス（Computer Virus）」の特徴は、ワームなど他の不正プログラムがOSのもつ自動実行機能を利用するのと異なり、被害者による実行を利用する点にあるとされる（細貝康夫・前掲書（註(94)）八一―一六頁）。
- (99) コンピュータ・ウィルス届出件数の動向等については、情報処理推進機構（IPA）ウェブページ<http://www.ipa.go.jp/security/outline/todokede-j.html> visited on Jan. 9, 2011. による。
- (100) 榊清隆『情報処理の高度化等に対処するための刑法等の一部を改正する法律』の概要「刑事法ジャーナル三〇号（二〇一一）四頁。
- (101) 二〇〇八年一月二四日付毎日新聞夕刊。
- (102) 二〇一一年七月二〇日付毎日新聞夕刊。
- (103) すでに本改正法の施行（二〇一一年七月一四日）後、最初の適用事案として、①インターネットのファイル交換ソフトの利用者に感染させる目的でウィルスをパソコンに保管していたとして警視庁が被疑者を不正指令電磁的記録保管罪（一六八条の三）で逮捕したケース（二〇一一年七月二二日付毎日新聞夕刊）、②他人のウェブサイトにウィルスを送信したとして栃木県警が被疑者を不正指令電磁的記録供用罪（二六八条の二第二項）で逮捕したケース（二〇一一年一月二日付毎日新聞朝刊）がみられる。

(104) 榑清隆・前掲(註(39))「『情報処理の高度化等に対処するための刑法等の一部を改正する法律』の概要」四頁。

(105) 山口厚「サイバー犯罪に対する実体的対応」前掲(註(83))一九頁。なお、山口「コンピュータ・ウイルス罪の論点」法とコンピュータ三〇号(二〇一二年)五九頁以下参照。

(106) 渡邊卓也「サイバー関係をめぐる刑法の一部改正」刑事法ジャーナル三〇号(二〇一二年)二八―二九頁。

## V ネットワーク犯罪刑事規制の課題

### 1 ネットワーク犯罪刑事立法の検討——ネットワークの刑法的保護の視点から

(1) 一九八七年(昭和六二年)刑法一部改正の意義

一九八七年の刑法一部改正は、わが国初のコンピュータ関連犯罪に対する刑事立法であるが、すでにみたように、その性質上現行刑法による的確な処罰が可能であった行為と同様の行為であるにもかかわらず、コンピュータの利用に伴い事務処理形態が変化したため、処罰が困難となった類型の行為を的確に捕捉・処罰できるよう処罰規定を整備しようとする趣旨で行われたものであつて、各種のコンピュータ関連犯罪に一体的に対応する特別法ではなく、文書偽造罪、業務妨害罪、詐欺罪、文書毀棄罪といった刑法典中の既存の犯罪類型を修正・拡張した類型を創設し、それらを従来の条文中に組み入れたり、その前後に配置するという方法に依つたものであつた。<sup>(107)</sup> 新たな犯罪化を、従来の犯罪と実質的に同質性を備えた当罰性の明らかな行為に絞つた、必要最小限の立法的手当ての枠を踏み外さない、控えめな立法例との評価が一般であつた。また、これら刑法典の規定に加えられた改正(後の二〇〇一年刑法一部改正も

含めて)は、「いずれも、旧来の偽造罪や財産罪の処罰範囲を拡張したにすぎ」ず、「実質的にも、刑法典の枠組みを何ら変えるものではない」との評価もみられる<sup>108</sup>。要するに、この一九八七年改正は、コンピュータの無権限使用や不正アクセスを将来の課題として切り捨てた点に象徴されるように、新たに社会のインフラを形成しつつあるコンピュータ・システム固有の機能の保護を考慮の外にいたものである、との見方が一般的である。

しかし、そう言い切れるかには疑問がある。わたくしは、情報処理システム——ひいてはコンピュータ・ネットワーク——の機能阻害自体を保護しようとする指向は、すでにこの一九八七年改正のなかに現れているのではないかと考えている。

すなわち、電磁的記録不正作出罪(二六一条の二)は、その客体を権利、義務または事実証明に関する記録に限定している点から、従来の文書偽造罪文書の証明機能を保護するのとパラレルに、電磁的記録の証明機能に着目した規定であつて、その限りでは偽造罪の保護法益を変容させるようなものではない。しかし、電磁的記録の性格上、その作成名義人を認識することが困難であることから、立法者は、作成名義の偽りの有無によって有形偽造と無形偽造を区別し、私文書については有形偽造のみの処罰を原則とする——私文書の無形偽造行為に対しては作成名義人への追及可能性により、作成名義人への信用を介して文書の信用性確保をはかる——という文書偽造に関する従来の規定方法を放棄したのである。その結果、電磁的記録不正作出罪は、文書偽造とは正反対に、作成名義の真偽ではなく、内容の真偽こそが処罰の可否を決する要素となる犯罪類型となつている。本罪は、電磁的記録(コンピュータ・データ)の証明作用ではなく、情報処理が正常に行われることに重点をおいたものと考えらるべきであろう。そうだとすると、一九八七年改正による本罪の新設は、コンピュータ・データの信用性保護を超えて情報処理阻害的不正行為の捕捉に

向けられたものとの評価できるのではないだろうか。<sup>109</sup>

また、電子計算機損壊等業務妨害罪(二三四条の二)についても、従来人により行われていた作業がコンピュータにより行われるようになりつつある現状をふまえ、コンピュータに向けられた加害を手段とする業務妨害行為をとらえて処罰しようとするもの、との従来の業務妨害罪の加重処罰類型にすぎないという立案当局の説明<sup>110</sup>にもかかわらず、特にその「又は使用目的に反する動作をさせて」という部分について、コンピュータが機械自体としては正常に機能している場合を想定しているので、「使用目的に反する」か否かが決定的な判断要素となり、「使用目的」の解釈ひとつで、犯罪化を見送ったはずのコンピュータの無権限使用やデータの不正入手を処罰範囲にとりこんでしまうことにもなりかねないものとなっている。このような点で、本罪も、電磁的記録不正作出罪とらんで、情報処理阻害的行為の捕捉への指向——コンピュータ・ネットワーク・システムへの加害行為の捕捉への指向——を含んだものとなっているように思われる。<sup>111</sup>

(2) 二〇〇一年(平成一三年) 刑法一部改正の意義

二〇〇一年改正により新設された支払い用カード電磁的記録に関する罪については、前述したように、支払用カードを構成する電磁的記録の真正、ひいてはこれら支払用カードを用いた支払いシステムに対する社会的信頼を保護法益とするもの、というのが立案当局の見解であった。通貨偽造罪や有価証券偽造罪と並ぶ偽造罪と位置づけられたわけである。しかしここでも、伝統的なそれら偽造罪の保護しようとする価値・利益をはみ出す新しい犯罪類型への指向性を読み取ることができるよう思われる。<sup>112</sup>

すなわち、電磁的記録部分を有する各種の支払用カードが普及発展したこと理由は、それが自動化された機械に

用いることを予定したものであって、従来の人間の手作業による財産的事務処理・決済とは比較にならない効率化が図られた点にある。プリペイドカードのように対人的な使用をほとんど想定していないものも多いことを考えると、そもそも人の判断作用を前提とする従来の各種偽造罪とは異なる性質の法益を保護する犯罪類型となっていることを率直に認めるべきではないだろうか。この点、西田教授は、本罪の客体にプリペイドカードやデビットカードのような機械に対してのみの使用が予定されているものも含まれており、ホワイトカードに磁気テープ等を貼り付けただけのカードの作製にも本罪の成立が肯定されるので、保護法益は、「電磁的記録を構成部分とする支払用カードによる支払決済システムの安全かつ円滑な運用であると解すべき」と指摘している<sup>113</sup>。また、今井教授は、「支払用カード電磁的記録に関する罪の重点は、直接的には人の信用を向け得ない（直接的な可読性を欠く）電磁的記録にあり、その保護法益は、電磁的記録を構成部分とする支払用カードによる支払い決済システムの安全性にある」とされる<sup>114</sup>。このような観点からは、本罪は、コンピュータ・ネットワークシステムによって実現される取引決済システムの機能保護を指向する点で、ネットワーク犯罪規制の役割を果たすべき規定と位置づけることができるものと考えられる。

なお、支払用カード電磁的記録不正取得の罪（二六三条の四）は、いわゆるスキミング行為によって電磁的記録にかかるカード情報を不正に取得する行為を処罰するものであるが、これは、一九八七年改正の際見送られた「データの不正入手」の一部——ごく一部の限定されたデータ入手行為ではあるが——を犯罪化したものともみることができるとように思われる。

### （3）一九九九年（平成十一年）不正アクセス禁止法制定の意義

不正アクセス禁止法は、わが国初のネットワーク犯罪を正面に見据えた刑事立法というべきものであるが、そのよ

うな立法が行われた背景には、コンピュータに関連する各種の不正行為・犯罪現象の動向における重点の変遷があったと考えられる。従来から論じられてきた「コンピュータ犯罪」は、「現在においては、情報通信ネットワークの大規模な展開により、『ネットワーク犯罪』へと変貌を遂げ、それに伴いその問題性は変容を見せ、かつ大きな広がりを示すに至っている<sup>16)</sup>」のである。

すでに検討したところから、上の一九八七年改正および二〇〇一年改正が、コンピュータ・システムによる情報処理の機能保護を指向し、さらには、コンピュータ・システムにより実現される自動化された取引決済システムの機能保護をはかるものであることを確認したが、この一九九九年の不正アクセス行為の禁止等に関する法律による不正アクセス行為の犯罪化（不正アクセス罪、同法三条・八条）は、さらにすすんで、具体的な財産等各種利益の侵害を念頭においた各種犯罪の予備罪的性質の行為の犯罪化をはかったものではなく、正面からコンピュータ・ネットワークの機能自体を保護しようとするものであることも疑いない。同法が定める不正アクセス罪が、コンピュータ・ネットワークに対する信頼をその保護法益とするものと考えられることはすでに述べたとおりである<sup>17)</sup>。

この点について、不正アクセス罪のこうした保護法益の理解に疑問を投げかける見解は、不正なアクセスという行為態様（ネットワーク経由でアクセス・コントロールを破ってコンピュータに侵入すること）ではなく、不正アクセスしたネットワーク内部で行われるデータ処理の観点から同罪の罪質を理解すべきであるという視点から、「電子計算機の利用とはその本質的な部分はデータの処理にあるといえることからするならば、アクセス制御機能を付加する対象は（電子計算機そのものではなく（註：筆者）電子計算機において処理されるデータであると解すべき）であって、同罪の保護法益としてとらえるべき処罰の実質は、「ネットワークにおける情報処理に関するセキュリティにあるとみるの

が適切である。」より具体的には、「データに対するアクセス制御という意味での情報の保持の側面における情報のインテグリティがここではもつとも重要なものとして理解されるべきである。」と述べる。<sup>118</sup> このような見解は、不正アクセスの罪質をネットワーク内部の情報処理との関係で把握する点で基本的に正しい方向性をもつものといえるが、立法者は——論者自身が指摘するように<sup>119</sup>——情報へのアクセスを捕捉・処罰することが情報窃盗を処罰することにながるとの懸念もあつて、こうした規定方法を採用しなかつたものと思われる。

不正アクセスの刑事規制は、わが国では刑法典中に規定を設ける方法——たとえば次項で検討するフランスのやり方——に依らず、特別法の制定により行われた。このような立法形式のあり方については、不正アクセスに代表される情報犯罪・サイバー犯罪の名称にふさわしい刑事立法が、その都度個別的な特別刑法によって行われてきたことに関し、「こうした犯罪類型を刑法典中に取り込むのを放棄して、もっぱら特別立法にゆだねるならば、情報犯罪やサイバー犯罪に対する刑法典の役割は、ますます低下してゆくであろう。」との指摘が行われている。<sup>120</sup>

その後、警察庁が、企業を装ったサイトに電子メールの受信者を誘導してID・パスワードをだまし取る「フィッシング」に関するアンケートをおこなったところ、九五%がフィッシングの犯罪化を支持し、不正アクセス罪の法定刑の引き上げについても八八%が支持する回答があつたということが報じられたが、警察庁、総務省、経済産業省およびインターネット関連の民間事業者で不正アクセス対策を検討する「官民意見集約委員会」は、不正アクセス禁止法改正に向けた検討作業を進め、二〇一二年三月には、右のような新たな犯罪化、処罰範囲の拡張、処罰の強化等を含む内容とする「不正アクセス行為の禁止等に関する法律の一部を改正する法律」が成立、同年五月一日に施行されている。<sup>122</sup> 不正アクセス罪は、「既に、ネットワークにおけるデータ通信並びに利害関係人の信用を保護する上で、不可欠

の存在になったと言えるであろう。」との評価がなされていたが、ネットワーク犯罪規制の中心を担う法制としてさらなる整備がはかられたのである。<sup>123)</sup>

(4) 二〇一一年(平成二十三年) 刑法一部改正の意義

この改正によつて、「不正指令電磁的記録に関する罪」が刑法典中に新設され、すでにみたように、「正当な理由なく、他人のコンピュータで実行させる目的で、ユーザーの意図に沿う動作をさせず、またはその意図に反する動作をさせるような不正な指令を与える電磁的記録等を作成し、提供する行為」を罰するウイルス作成罪などの犯罪類型が設けられ、それまで処罰規定を欠いていたコンピュータ・ウイルス関係の不正行為の犯罪化が行われた。この改正については、実害と切り離された、コンピュータ・プログラムに対する社会的信頼が保護法益とする独自の類型との理解が(法益の抽象化により処罰の早期化を図る点など問題があるとする批判もあるが)<sup>124)</sup> 大方の承認をえるところとなっている。

コンピュータによる正常な情報処理に向けた社会一般の信頼が保護法益とされる点に関しては、この改正が、従来 of コンピュータ犯罪立法と異なり、ネットワーク侵害に伴う現実社会の損害や不利益を捉えるのではなく、「仮想社会のインフラであるネットワークそれ自体を直接に保護しようとする」意味において、「初めて、サイバー犯罪を正面から捉えた」ものとする評価が示されている。<sup>125)</sup> こうした見方は、コンピュータ犯罪が登場した当初の、ハードウェアやデータ、プログラムなど部分的な刑事的保護の対応にとどまった「コンピュータ犯罪」の時期、さらにはその犯行手段の巧妙化・大規模化・国際化の脅威を印象づけた「ハイテク犯罪」といった過渡期を経て、今日、サイバースペースに形成された仮想社会の基盤を担うコンピュータ・ネットワークが刑法による保護の対象となりつつある「ネットワーク犯罪」が問題となる現実を示唆している点で、正当なものと考えられる。

本罪については、すでにみたように、法益の抽象化により処罰が早期化すること、また、電子計算機損壊等業務妨害罪とその未遂罪との関係で適用範囲の重複など未解決の問題が残ることなどの批判があり、また、不正指令電磁的記録作成等の罪の客体に、「その他の記録」として、ウイルスをアナログデータとして記録してある紙媒体等も含まれるので、実行可能な状態にないウイルス・コードの記述も客体となる点で、「法益に対するものではなく、電子計算機の作動障害及びそれに起因する損害に対するもの」という意味でも、極めて抽象度の高い危険を処罰するもの」との指摘<sup>126</sup>も行われているが、反対に、この改正は、本罪を刑法典の偽造罪と偽証罪の中間に位置づけるといって、未だ情報伝達・事実証明の手段という側面に囚われており、刑事規制の対象とされるのは不正な指令を含むプログラムに限定され、「ネットワーク設置者自身による不正操作も含め、およそ虚偽の情報流通を阻止して、サイバー社会の安全性を確保しようとする趣旨ではない」として、さらなるネットワークの保護の徹底の必要性を主張する見解<sup>127</sup>も示されている。このような主張は、「コンピュータは、個人人が使用するものであるが、コンピュータの利用が社会全般に普及した現在においては、コンピュータの作動を基礎付けるプログラムの正常性は、不特定多数人の利害に直結しており、この意味で社会的に重要な利益になっている。」という現状認識に支えられたものであるということが<sup>128</sup>きよう。

なお、ウイルス作成罪と同供用罪とが同等に位置づけられている点について、供用罪が想定するのはウイルスが実行可能な状態にされていて被害惹起の危険が具体的になっているのに対して、作成罪は未だその危険が抽象的な段階にとどまっているのに、その法定刑が同一とされるのはなぜか——ウイルス作成と供用とが同等に評価されるのはなぜか——という疑問が提起されている<sup>129</sup>。たしかに、各種偽造罪においても、通貨・文書の偽造、支払用カード電磁的

記録不正作出行為が行使・供用行為と同じ刑罰評価が行われている。「使う行為」に至らないその前段階にあたる「作る行為」が、使う行為と同等に扱われているのである。しかし、同じ社会的法益に対する罪であっても、わいせつ物頒布等では、実際に頒布・陳列などによりわいせつ情報を社会に拡散するという法益侵害惹起に直結する行為以前の「わいせつ表現物の製造」自体は処罰すらされないのである。そうすると、問題は、作成されるものの自体の危険性——コンピュータ・ウイルスの危険性——をどのように考えるか、に帰着することになる。すなわち、立法者が、ウイルス作成行為を、コンピュータ・ネットワーク社会に害悪をもたらす根源を生み出す、重い犯罪性を備えたものと評価されるべきものであつて、単なる各種の加害行為の予備にとどまるものではないと<sup>130</sup>考えたことが読み取れるのである。

コンピュータウイルスの犯罪化に踏み切ったこの立法は、立法者が好むと好まざるとにかかわらず、コンピュータ・システムの利用によって実現される個々の業務の保護や、システムによる処理に置き換えられた決済手段の運用の保護の前提となる、具体的な個々の権利・利益・価値の保護とは次元を異にする、コンピュータ・ネットワーク・システムの正常な機能（サイバースペース独自の働きと秩序）それ自体の保護を指向するものとなりえているのではないかと考えられるのである。

## 2 刑事立法のあり方——フランス刑法との比較から——

以上に、わが国のコンピュータ・ネットワークに関連する犯罪にかかわる刑事立法の検討を試みたが、わが国とほぼ同時期に情報処理技術の利用・普及がすすみ、同程度の社会の情報化が達成されたフランスでも、やはりほぼ同じころにコンピュータ犯罪関連の刑事立法が行われている。そこで、最後に、大陸法の枠組みの刑法システムをもつ点

でも共通するフランスが、コンピュータ犯罪ないしネットワーク犯罪にどのような刑事立法で対応したかを見ておくこととする。

(1) コンピュータ犯罪刑事立法前の状況と「バダンテール法案」

フランスにおいて、コンピュータ犯罪に関する最初の刑事立法の動きといえるのは、一九八六年に上院に提出された刑法典改正法案（当時の司法大臣の名をとり「バダンテール法案」とよばれる<sup>131</sup>）の中に「情報処理に関連する犯罪」の章をおいていたことである。後に廃案となったこの法案の関係部分は以下のとおりである。<sup>132</sup>

第七章 情報処理に関連する犯罪 (Les infractions en matière informatique)

第三〇七―一条 自動情報処理システムのプログラム、データ、またはその他すべての構成要素を不法に取得する行為は、拘禁刑三年および罰金一〇〇万フランで罰する。

第三〇七―二条 他人の権利を無視して、自動情報処理システムのプログラム、データ、またはその他すべての構成要素を使用し、伝送し、または複製する行為は、拘禁刑三年および罰金一〇〇万フランで罰する。

第三〇七―三条 故意に、かつ他人の権利を無視して、自動情報処理システムの全部または一部を破壊もしくは改変し、またはその機能を阻害し、もしくは誤らせる行為は、拘禁刑五年および罰金二五〇万フランで罰する。

第三〇七―四条 自動情報処理システムを不法に使用することによって、違法な利益を得、または他人をしてこれを得させる行為は、拘禁刑五年および罰金二五〇万フランで罰する。

ところで、フランス刑法は、財産犯の体系を含めてわが国の刑法とかなりの程度基本的共通点を持つものであるが、当時の法状況を比較すると、わが国の「司法機関は、実際にコンピュータ濫用の事件が発生すると、伝統的犯罪規定の下で巧みな解釈技術を駆使し、その殆どのものを処罰してきた。」<sup>133</sup>と評されるものであったところ、フランスにおいても、一般に先端技術を用いて行なわれる新しい手口の不正行為への伝統的条文の適用には、刑法学者は慎重であるが、「裁判官たちがこういった新たな状況に対して伝統的条項を適用することに躊躇することはほとんどない」という傾向にあったようである。<sup>134</sup>

ただし、詐欺罪に関する部分では、①パリのデパートの情報処理技術者が、偽造クレジット・カードを使用して購入した商品の価格金額が計上されないようにコンピュータの操作を行ない、総額約一千万フランの不法な利得を得ていたというケースや、<sup>135</sup>②銀行から銀行への口座の振り替え指示を傍受し、金額があたかも正当な口座へ振り込まれるかのようにメッセージを偽造したというケース、<sup>136</sup>③銀行預金の利息の端数を、一定の端数以下は切り捨てるようにプログラムを行ない、これを行為者があらかじめ用意していた別の口座に振り込まれるようにプログラムを操作したという「鬻（perruque）」と呼ばれる手口を用いたケース<sup>137</sup>などの虚偽のデータの入力やプログラムの不正操作による財産上の不法な利益の取得行為に対しては、詐欺罪の適用が可能とされている点が注目される。ここでは、そのような手段が「コンピュータを欺いた」といい得るかが問題となりそうである（この点が、わが国の刑法上詐欺罪成立の最大のネックとなり、電子計算機使用詐欺罪（日本刑法二四六条の二）を生んだ）<sup>138</sup>が、フランスにはパーキング・メータの不正使用について詐欺罪の成立を認めた一九七〇年の破棄院の判例があり、<sup>138</sup>「機械の背後に人間が、コンピュータの背後に銀行・企業の責任者がいることは全く明白」だから、コンピュータが常に人間に使用されている以上、「この障害は

容易に克服され得る」こととなるのである。<sup>139)</sup>

なお、盗罪——わが国の窃盗罪に相当——の適用に関しては、他人のカードでCD機から不正に現金を引き出すような行為について、「交付の任意性」を理由に盗罪の成立を否定する学説もある<sup>140)</sup>。しかし、自動支払機からの取得という人間が介在しない状況にもかかわらず、前述のパーキングメータのケースに関する破棄院の判例の論理に加え、フランス刑法が欺罔行為による場合のほかに、「偽名または虚偽の資格の使用」があつたときにも詐欺罪の成立を認める規定となつていることから、この学説は、詐欺罪での処罰を肯定している<sup>141)</sup>。このように、詐欺罪の射程範囲の点を除けば、おおむね当時のフランスの財産犯罪等の適用関係はわが国とほぼ類似の状況にあつたといつてよいと思われる。

これに対して、直接情報それ自体に向けられた「盗み見」「傍受」等のコンピュータ・スパイのようなケースは、わが国同様、いかなる伝統的犯罪規定もこれを捕捉しえない状況にあつた。情報が「物」の観念と相容れない性質のものであることはいうまでもないが、それは単に「無形のものである」という理由だけで排除されているわけではない。フランスの判例は盗電行為に盗罪を認めている<sup>142)</sup>が、情報の性質を電気との対比において考えると、「電気はそれを作り出した者によつてそれを使用するために受け取る消費者へと引き渡され、物質的に確認され得る伝送の効果によつて、最初の者の所有から次の者の所有へと移動するものである以上、刑法（筆者註…フランス旧刑法）三七九条の意味における『物』とみなされるべきものである。この比較は、情報の領得行為が同様の方法——電話回線上で通信の方向を変更するように接続を行なうこと等——で行なわれれば、ますます類似してくる。しかしながら、この情報の領得行為は、知られているように、やはり単なる電磁波のキャッチにより行なわれ得るのであり、このことは『家

庭用の『電気とコンピュータの記憶装置に蓄えられた情報との間の還元不能の性質上の差異をはつきりと示しているように思われる。情報は、量的に把握することは出来ないし、測定することも出来ない。つまり、水道盗または電気盗に関するすべての判例が、まさに、『不正に変更された』メーターはその変更された部分の測定が可能であるという事実<sup>143</sup>に根拠を置いているのに対して、情報は測定できないからである。』ということになる。データはその性質上盗罪の客体たりえず、またそれは複製という形で取得されるので、元のデータがなくなるわけではなく元のままにある(情報の非移転性)からである。さらに、詐欺罪の適用も困難である。欺罔的手段が認められても、可動の有体物が対象でなければならず、データはもちろんそのようなものにはあたらないからである<sup>144</sup>。

コンピュータの無権限使用についてはどうか。フランスでは、「時間盗(vol de temps)」、「マシン・タイムの盗用(vol de temps-machine)」などと呼ばれるが、やはりハードウェアそのものの奪取がない以上、考えられるのは可罰的な「使用盗罪(vol d'usage)」の適用のみであるが、この自動車の不正使用処罰を念頭に判例が認めた可罰的な使用盗罪は、「所有者としてふるまう意思」を要件としているため、複数の者が一台のコンピュータを「同時に」使用するような形態(タイムシェアリング)を前提とすると、通常想定される無権限使用は、そのシステムの「所有者としてふるまった」とは到底いえず、不可罰とせざるをえない<sup>145</sup>。もとより単純な無権限アクセス、「面白半分の不法侵入(viol Judique)」については、当時のわが国と同様に、これを捕捉できるいかなる罰条もないという状況にあった<sup>146</sup>。このような法状況の下、コンピュータ犯罪への対策の必要性が自覚され、上にみたように刑法改正法案の中に「コンピュータ関連犯罪」として盛り込まれていったのである。このいわゆる「バダンテール法案」は廃案となるが、そのコンピュータ犯罪に関する部分は、その後の立法作業に強い影響をもたらした、とされる<sup>147</sup>。

## (2) 一九八八年刑法一部改正

フランスの最初のコンピュータ犯罪刑事立法となったのは、従来、刑罰法令による捕捉が不可能なし困難なままにおかれていた情報処理領域の不正行為を、刑法上の犯罪として処罰しようという構想の下に、一九八六年、ゴドフラン議員により下院にその法案（ゴドフラン法案とよばれる）が提出され<sup>148</sup>、その後上下両院による一年あまりをかけた審議を経て、翌一九八七年に可決成立し「情報処理関連不正行為に関する一九八八年一月五日の法律第八八一一九号」となったものである。立法の背景には、伝統的犯罪類型による処罰の体系に、コンピュータ犯罪の入り込みうる種々の空隙が生じており、立法による介入が不可欠という状況にあったことが指摘しうる<sup>150</sup>。

この立法が、刑法領域に新しい「コンピュータ犯罪」のカテゴリーを導入し、刑法典に新しい独立の章を創設するという本格的な刑事立法でありながら、速やかな立法作業となったのは、「この種の立法の必要性につき議会において合意があったから」であるが、同時に、審議を通じて幾度も両院を往復し、大幅な修正が加えられた結果、可決された時点では「形式的にも内容的にも当初の姿を全くとどめなくなっていた」という点については、情報処理領域に固有の犯罪の処罰体系を構築することの技術的困難さを示しているというべきであろう<sup>151</sup>。本法の主要関係部分（犯罪類型の規定部分）は以下のとおりである。

唯一条 刑法典第三部第二編中第二章の後に、次の第三章を挿入する。

### 第三章 情報処理関連犯罪 (De certaines infractions en matière informatique)

第四六二条の二 不正に、データの自動処理システムの全体もしくは一部にアクセスし、または滞留した者は、二

月以上一年以下の拘禁および二、〇〇〇フラン以上五〇、〇〇〇フラン以下の罰金で罰し、またはこれらいずれかの刑で罰する。

② 前項の行為に因り、同システム中に収納されたデータの消去もしくは改変、または同システムの動作の悪化を生じさせたときは、本条の拘禁は二月以上二年以下とし、罰金は一〇、〇〇〇フラン以上二〇〇、〇〇〇フラン以下とする。

第四六二条の三 故意に、他人の権利を無視して、データの自動処理システムの動作を妨害しまたは狂わせた者は、三月以上三年以下の拘禁および一〇、〇〇〇フラン以上一〇〇、〇〇〇フラン以下の罰金で罰し、またはこれらいずれかの刑で罰する。

第四六二条の四 故意に、かつ他人の権利を無視して、直接または間接に、データの自動処理システムにデータを入力し、または同システムに収納されたデータもしくはは処理・伝送に関する方法 (modes) を消去もしくは改変した者は、三月以上三年以下の拘禁および二、〇〇〇フラン以上五〇〇、〇〇〇フラン以下の罰金で罰し、またはこれらいずれかの刑で罰する。

第四六二条の五 他人に損害を与えるような性質の、情報処理記録の偽造を行なった者は、その記録の形式の如何を問わず、一年以上五年以下の拘禁および二〇、〇〇〇フラン以上二二、〇〇〇、〇〇〇フラン以下の罰金で罰する。

第四六二条の六 事情を知りながら、前条の客体である情報処理記録を使用した者は、一年以上五年以下の拘禁および二〇、〇〇〇フラン以上二二、〇〇〇、〇〇〇フラン以下の罰金で罰し、またはこれらいずれかの刑で罰する。

この改正によって、①システムへの不正アクセス・滞留の罪、②システムの動作妨害の罪、③データの無権限入力およびデータ、プログラムの消去・改変の罪、④情報処理記録偽造および同記録使用の罪の各犯罪類型に関する規定が（ほかに全ての罪の未遂処罰、共謀の処罰および没収に関する規定が）設けられた。

この立法の特徴は、まず、処罰規定を特別法によらず刑法典中に設けたことである。この点はわが国と同じであるが、異なるのは、情報処理犯罪に関する規定を一つにまとめて規定し法典中の独立の章とした点である。すなわち、新たな章「第三章 情報処理犯罪」は、刑法典第三部第二編「個人に対する重罪および軽罪」中の第一章「人身に対する重罪および軽罪」、第二章「財産に対する重罪および軽罪」に続く第三章として法典のなかに位置づけられた。コンピュータ犯罪に関する規定が、財産犯の章に含められることなく、独立の章として配置されることとなったのは、コンピュータ犯罪の類型を財産犯体系へ導入することが、ファイルやソフトウェアなど無形のもの所有権を事実上是認してしまうことに通じるのではないかという立法者の懸念に由来するもの<sup>152</sup>のようである。このような法典中の位置づけは、実際の規定の解釈・適用上さほど重要な意味を持つわけではない<sup>153</sup>としても、新たに犯罪化された類型を、財産犯とは別の「情報処理に関連する (en matière informatique)」(ある種の (de certaines)) 犯罪 (infractions)」と位置づけた点は重要であろう。すなわち、ゴドフラン議員により提出されたときの最初の法案は、「一方において当該領域のすべての不正行為を網羅すること、他方において盗罪や詐欺などの従来の犯罪類型の適用における判例の躊躇と学説の反対を一扫することを目的とし」<sup>154</sup>、各種の犯罪の客体に情報処理記録を加え、盗罪の節中にデータ、プログラムの不法入手罪を新設するなど、コンピュータ犯罪処罰に関わる全ての問題を立法により解消することを目指した包括的な刑事立法を目指すものであった。このような意図をもった法案は、後の大幅な修正により情報盗などの規定を

廃し、コンピュータ犯罪に限定するいくつかの条文を独立の章にまとめたかたちの本法となったのである。

コンピュータ(情報処理)関連犯罪に関する刑事立法に際して、伝統的な財産犯罪の原則への考慮が強く働き、最終的には技術革新が生んだ新しい脅威に対する刑事規制にあたっては、控えめな立法態度に収束して行った点は、やはりわが国と共通の指向がみられる。伝統的な法原則を尊重するところに安定感を見出す点では共通のものがあると思われる。しかし、フランスのこの一九八八年改正法の特徴は、上にみたように、情報処理に関連する不正行為を、他の既存の類型と切り離した情報処理領域特有の犯罪類型として構想し、最初のコンピュータ犯罪刑事立法である本法において、典型的なネットワーク侵害行為である不正アクセスの処罰に焦点を当てた点にある。わが国も、ほぼ同時期(一九八七年)に刑法一部改正によるコンピュータ犯罪対策立法を行っているが、すでにみたように不正アクセスの犯罪化は見送られ、文書偽造罪、業務妨害罪、詐欺罪、文書毀棄罪といった既存の犯罪類型を修正・拡張した類型を創設し、それらを従来の条文の前後に配置し、あるいは従来の条文中に組み入れるという方法をとったのである。こうした方法は、新設された犯罪類型を既存の類型の延長線上に位置づけ、既存の類型と共通性を有する行為に処罰範囲をとどめようとする力が働く(たとえば電磁的記録不正作出罪を文書偽造罪とパラレルに理解しようとする保護法益論などにそれがみられた)ため、新しい価値の保護を指向する刑事立法の発展にとってはブレーキとなってしまうのではないだろうか。

わが国では、不正アクセスの刑事規制は特別法の制定によって実現したが、刑法典中におかれたフランスの不正アクセス罪(四六二条之二)は、その成立に何らの侵害結果の発生も要求しない点で共通する。また、コンピュータへのアクセスが可罰的であるためには、「不正に」それが行なわれることを要する点でも共通するように見える。しか

し、わが国の不正アクセス禁止法上の不正アクセスは、すでに見たように、ネットワーク経由で、セキュリティ措置の施されたコンピュータ・システムに侵入する行為を指し、その「不正アクセス」は「無権限アクセス」を意味するものである。これに対して、フランス刑法における不正アクセス罪の「不正に (Frauduleusement)」とは、その意味を異にしている。すなわち、その立法過程では、不正アクセス罪の客体を無権限アクセスからの保護措置 (セキュリティ手段) を備えたシステムに限定することが主張されたが、このセキュリティ手段の要求は、「不正に」という文言からその条件が当然に導かれるとされ、結局明文化されなかつた経緯がある<sup>155</sup>。すなわち、本罪の客体は一定の保護措置 (ID・パスワードによるアクセスコントロールのような) が施されたシステムに限定されるものではないということになる。このように保護装置についての明文を欠いたことについては、システムの管理者 (maître du système) の意思に反するシステムへの侵入一般を不正と解し得るようになった結果、「ある一人の人物が情報の全体を『私物化』し、情報の検索についての絶対的な独占権を確保することが承認される」ことにもなりかねない、との批判が加えられた<sup>156</sup>。「立法者はその本来の意図以上に処罰領域をかなり拡大したように思われる。」<sup>157</sup>との指摘のように、本罪は、運用如何によつては、立法者の意図を離れて過度に広範な処罰を招く可能性が無いとはいえないであろう<sup>158</sup>。

フランスの一九八八年一月五日法は、以上のとおり、データの自動処理システム——電子計算機ではない——の概念を中核に、それへの不正アクセスをはじめとする、コンピュータの登場に伴つて初めて現われた情報処理領域固有の不正行為を捉えようとするものであつた。そしてとくに、本法は、通信回線を経由して容易に行なわれる不正アクセスの規制や、データ伝送のモード (通信に関するソフトウェア) の保護などの点で、コンピュータと電気通信の結合を念頭に、ネットワーク犯罪規制への指向性を明確にした立法例といえる。

本法は、各種の定義規定を置かず、客体の限定の明文化を避け、不正アクセス罪をはじめ相当広い処罰範囲もつ類型をおき、更にすべての罪の未遂、共謀の処罰の規定を置いたことなどから、全体としてかなり広範囲な処罰領域を有する立法の外観を呈している。その点では、わが国と対照的な立法例のようであるが、しかし、他方で、最初に議会に提出された法案は、データ・プログラムの不正取得などに関する類型を持つていた<sup>159</sup>ところ、そういった角度からの犯罪化は注意深く避けられ、不正アクセスに関する罪の規定に取って代わられた。つまり、不正アクセス罪の射程を広くとつたことにより、直接の処罰を避けた情報の不正入手を、間接的に刑事規制の枠内におさめようとしたとも考えられる。

フランスのコンピュータ犯罪立法は、わが国で規制が見送られた部分をむしろ中心的にとり込んだ、立法形式、内容ともに対照的なものであるが、同時期のコンピュータ犯罪立法例としてこれほど差異がみられる理由には、フランス刑法の体系と関わる観点からの考慮を除けば、情報通信の発展という点で当時のフランスがわが国より一歩先を歩んでいたという事情があつたかもしれない。当時のフランスは、世界に先駆けて家庭や職場に置かれた端末をセンタールのコンピュータと結び、情報の利用、やり取りをするヴィデオテキストの普及に国をあげて取り組んでおり、「ミニテル (minitel)」と呼ばれる専用端末が無料配布され、人々の生活の中に入り込んでいた。はじめ電子電話帳サービスとして一九八三年にスタートしたが、一九八九年当時で四七〇万台が設置済といわれていた<sup>160</sup>。このような事情とコンピュータ犯罪との関係について実証的な考察は行なわれていないようであるが、「フランスにおいては、ミニテルの急激な普及以来コンピュータ犯罪は急速に増加しており」、「三〇〇万台のミニテルが、コンピュータに慣らされた一〇〇〇万人近くの人々を作り出したという状況にあつては、今後もコンピュータ犯罪が増加しないというこ

とはありえない」との指摘がなされていた。<sup>161</sup> さらに、「ミニテルの使用の増加は、情報や金銭の横領を助長する傾向を導く」として、料金を支払わずに不正にデータ・ベースを使用する手口を紹介する意見も散見された。<sup>162</sup> フランスが情報通信の保護をも念頭においた情報犯罪型のコンピュータ犯罪立法を行なった背景として、その影響は間接的であるかもしれないが、<sup>163</sup> 以上のような事情の存在も考慮されよう。同じく急速な情報化がすすんでいる時期であっても、わが国のように、研究機関や一部の企業、金融機関などにユーザが限定されていたコンピュータの利用形態の社会と、それがネットワーク化により一般に広く用いられていた社会とでは、不正行為の発現形態や性質に違いが生じるともいえるのではないだろうか。

### (3) 一九九二年刑法全面改正

フランスは、一九九二年七月に、それまでの刑法典（二八一〇年制定のナポレオン刑法典）を全面改正した（施行は一九九四年三月一日）<sup>164</sup> が、上にみた、情報処理関連不正行為に関する一九八八年一月五日法により設けられた規定は、ほぼそのまま新刑法典に継承された。本法成立時の情報処理犯罪主要関係部分（犯罪類型の規定部分）は以下のとおりである。

### 第三章 データの自動処理システムに対する侵害

第三三三―一条 【不法アクセス等】 ① 不法に、データの自動処理システムの全体または一部にアクセスし、ま

たは滞留する行為は、一年の拘禁および一〇万フランの罰金で罰する。

② 前項の行為により、システム中の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ときは、

その刑を二年の拘禁および二〇万フランの罰金とする。

第三三三―二条【コンピュータ業務妨害】 データの自動処理システムの動作を妨害し、または不調にする行為は、三年の拘禁および三〇万フランの罰金で罰する。

第三三三―三条【データの不正操作】 不法に自動処理システムにデータを入力し、または、そのシステムが収納するデータを不法に消去もしくは改変する行為は、三年の拘禁および三〇万フランの罰金で罰する。

一九九二年刑法改正に伴い、情報処理記録（コンピュータデータ）の偽造罪のみが削除されているが、これは、文書偽造罪の客体が「文書その他すべての思想表現手段」へと拡張されたことによるものであるが、<sup>165</sup>他はほとんど同様の形式・内容を維持して新法典に移植されている。

#### (4) 二〇〇四年刑法一部改正

その後、フランスは、「ヨーロッパ評議会サイバー犯罪に関する条約（Council of Europe Convention on Cybercrime）」（二〇〇一年一月八日、ヨーロッパ評議会閣僚委員会採択）の批准に向けた国内法整備の一環として、二〇〇四年に法改正<sup>166</sup>を行い、上の「データの自動処理システムに対する侵害」の章にウィルス作成罪など新たな規定を付加する等、刑法典に修正を加えている。その主な内容は、<sup>167</sup>①第三三三―三条の後に、次の新たな規定を設けるもの、である。

第三三三―三―一条 正当な理由なく、第三三三―一条ないし第三三三―三条に定める一つまたは複数の罪を犯す目的で考案され、または特別に調製された設備、機器、コンピュータ・プログラム、またはすべてのデータを、

輸入し、所持し、提供し、譲渡し、またはその用に供する行為は、各罪について定めた刑、または最も重く罰せられる罪について定めた刑で罰する。

また、②三三三―一条の一項（不法アクセス罪）の法定刑を「一年の拘禁および一〇万フランの罰金」から、「二年の拘禁および三万ユーロの罰金」に引き上げ、二項（加重処罰）の法定刑を「二年の拘禁および二〇万フランの罰金」から、「三年の拘禁および四万五〇〇〇ユーロの罰金」に、<sup>168</sup>同様に、③三三三―二条（コンピュータ業務妨害罪）の法定刑を「三年の拘禁および三〇万フランの罰金」から、「五年の拘禁および七万五〇〇〇ユーロの罰金」に、<sup>169</sup>④三三三―三条（データの不正操作罪）の法定刑を「三年の拘禁および三〇万フランの罰金」から「五年の拘禁および七万五〇〇〇ユーロの罰金」に、<sup>170</sup>それぞれ引き上げる内容のものである。

新たに付加された三三三―一条の罪は、サイバー犯罪条約批准に向けた国内法整備の一環として、コンピュータ・ウイルス処罰を定めたものである。<sup>171</sup>サイバー犯罪条約は、コンピュータ・システムの「装置の濫用（六条）」として、「（違法なアクセス・傍受・システム妨害等の）犯罪を主として行うために設計され又は改造された装置（コンピュータ・プログラムを含む。）を、これら「犯罪を行うために使用されることを意図して」、「製造し、販売し、使用のために取得し、輸入し、頒布し又はその他の方法によって利用可能とすること」の犯罪化を要請しているが、<sup>172</sup>本罪の規定はほぼ忠実にその要請にこたえようとする内容となっている。<sup>173</sup>

この改正は、他の情報処理犯罪の法定刑を大きく引き上げたことも含めて、フランスのネットワーク関連犯罪の状況に対応すべく、情報処理領域固有の刑事法制の整備を積極的に図ったものにほかならない。そして、もつとも重要

な点は、それが、広範なコンピュータ・ネットワークの形成により実現されたサイバースペースを基盤にした経済活動等の発展を見据えた法改正であることである。この二〇〇四年の刑法一部改正は、「デジタル経済における信頼(の確保)のための二〇〇四年六月二日・法律第二〇〇四一五七五号」<sup>174</sup>の制定によつて行われたが、同法は、インターネット等コンピュータと通信テクノロジーの活用により行われる経済活動のインフラとなるサイバースペースの維持発展を図るというデジタル経済 (economie numérique) に関するフランスの政策の一環として、多数の法令に修正を加える総合的・包括的な立法措置の一部として行われたものなのである。わが国でも「サイバーエコノミー」や「サイバーモール」という表現がポピュラーになりつつあるが、<sup>175</sup>広範で高度なネットワーク化の進展により出現したサイバースペースで行われる経済活動がますます活発化して行くことが予想されるとすると、このような政策の推進が強く求められることになる。<sup>176</sup>

以上に見てきた、フランスのコンピュータ・ネットワーク関連犯罪に関する立法態度については、他国と比べ特に犯罪現象自体多いとはいえないのに、そのような犯罪に対処可能な立法上の武器を、「世界に先駆けて用意している点特徴的」であり、「早くからハイテク犯罪立法を行い、議論を積み重ねてよりよい規定に整理・統合していったフランスの姿勢には、日本も見習うべき点が少ない<sup>177</sup>」との評価が行われている。日本とフランスの立法方式のどちらが優れているかは一概に断じられないが、少なくとも、一貫して強くネットワーク犯罪の刑事規制を行うことにより、新しい価値の保護を指向し続けてきたフランスの態度は、今日、刑法典がサイバー犯罪の規制に取り組む選択肢を積極的に模索すべきである<sup>178</sup>とすれば、参考にする意義は大きいと思われる。

(107) コンピュータ犯罪に対する刑事立法の方法には、「(一) コンピュータに関連した反社会的行為を広くコンピュータ犯罪として捕捉し、総合的なコンピュータ犯罪処罰法を指向する考え方と、(二) コンピュータの適正な機能を害する行為に限定して刑事立法を行う考え方とがあるが、今回の改正は(二)の方向に沿ったものである。」との評価が示されている(曾根威彦「コンピュータとデータの保護」刑法雑誌二八巻四号(一九八八)四六八頁)。

(108) 佐久間修「情報犯罪・サイバー犯罪」ジュリスト一三四八号(二〇〇八)一〇九頁。

(109) これに關し、批判的な立場から、山口教授は、電磁的記録の作成名義の真偽を問題としない規定のあり方について、そのような方法には、「データの証明機能ではなく、情報処理の正しさを保護法益とすることにならざるをえないのではないかという、基本的な問題があるように思われる」としたうえで、「コンピュータについてだけ、情報処理阻害を処罰する実質的理由があるか、疑問がある」と指摘している(山口厚「電磁的記録と文書犯罪規定の改正」前掲(註(66)八一―九頁)。また、「電磁的記録不正作出罪における『不正』は、『権限なく』よりもはるかに抽象的であり、立法趣旨も有形偽造に限定することを意識的に避け、無形偽造をも処罰する意図で右のような表現をしたということであれば、文書に比較して電磁的記録の特権化するもの」との批判も加えられている(中山研一ほか「コンピュータ犯罪等に関する刑法一部改正」前掲(註(68)四六頁「神山敏雄」)。

(110) 米澤慶治編『刑法等一部改正法の解説』前掲(註(63)九六頁以下)。

(111) この点について、芝原教授は、こうした困難な問題を生じるのは、「この部分の実体がコンピュータに関する情報処理阻害行為の処罰を意図しているところにある。本罪の背景には、器物毀棄による業務妨害と、情報処理阻害による業務妨害の二つの『原型』が存在するとみることができる。」とし、立案作業の過程で情報処理阻害を正面から処罰する方針が捨て去られた後も、「この情報処理阻害罪の実質は、試案の『不正動作』や骨子の『使用目的に反する動作』(改正案では『使用目的二違フ動作』)というかたちで取り込まれているとみることができる。」と指摘している(芝原邦爾「コンピュータ犯罪による情報処理と業務妨害罪」前掲(註(66)一五頁)。

(112) 本稿「IV 1 (2)」参照。

- (113) 西田典之「カード犯罪と刑法改正」前掲（註(72)）一七頁、同『刑法各論』前掲（註(72)）三一八頁。
- (114) 今井猛嘉「支払用カードの保護に関する刑法の一部改正」前掲（註(70)）四六一―四七頁。なお、渡邊卓也「電子マネーの不正取得と電磁的記録不正作出罪」姫路ロー・ジャーナル五号（二〇一一）二五頁以下は、「カード」以外の形状の記録媒体（たとえば「おサイフケータイ」機能を有する携帯電話機中のチップ）に保存された電磁的記録についても、支払用カード中のそれと同等に保護を図る必要があることを主張している。
- (115) 佐伯教授は、本法成立の前に、無権限アクセス規制に関して、ネットワーク経由での外部からの侵入に対するセキュリティ措置が施されたコンピュータ・システムに無権限で侵入する行為に限って処罰する方向が考えられる、としたうえで、「このような方向は、無権限アクセスをコンピュータ犯罪よりもネットワーク犯罪として位置づけるものである。」としていた（佐伯仁志「無権限アクセス規制に関する覚書」研修六〇二号（一九九八）一一頁）。
- (116) 山口厚「情報通信ネットワークと法」岩村正彦ほか編『現代の法六 現代社会と刑事法』岩波書店（一九九八）一〇五頁。
- (117) 本稿「IV 2 (2)」参照。
- (118) 石井徹哉「不正アクセス禁止法の意義と限界」千葉大学法学論集一九卷三号（二〇〇四）二五頁、三五頁。
- (119) 石井徹哉「不正アクセス禁止法の意義と限界」前掲（註(118)）一七頁。
- (120) 佐久間修「情報犯罪・サイバー犯罪」前掲（註(108)）一一五頁。
- (121) 二〇一一年二月八日付け毎日新聞夕刊。
- (122) 二〇一一年二月二三日付け毎日新聞朝刊。成立した「不正アクセス行為の禁止等に関する法律の一部を改正する法律（平成二四年法律第二二号）」については、四方光「不正アクセス禁止法改正の背景・経緯及び不正アクセス対策の今後の課題」警察学論集六五巻六号（二〇一一）一三頁以下、蔵原智行「不正アクセス行為の禁止等に関する法律の一部を改正する法律」について」同誌同号二二頁以下、蔵原「フィッシング行為、ID・パスワードの不正取得等の禁止・処罰等」時の法令一九〇九号（二〇一一）四頁以下を参照。
- (123) 今井猛嘉「ネットワーク犯罪」前掲（註(83)）五五頁。

- (124) 本稿「IV 3 (2)」参照。
- (125) 佐久間修「情報犯罪・サイバー犯罪」前掲(註(108))一三三頁。
- (126) 伊東研祐『刑法講義各論』日本評論社(二〇一一)四二八頁。
- (127) 佐久間修「情報犯罪・サイバー犯罪」前掲(註(108))一一三頁。
- (128) 今井猛嘉「ネットワーク犯罪」前掲(註(83))五七頁。
- (129) 園田寿『情報社会と刑法』成文堂(二〇一一)六八頁以下。
- (130) 山口厚「サイバー犯罪に対する実体法的対応」前掲(註(83))一九頁。
- (131) PROJET DE LOI portant réforme du code pénal, Journal officiel No 300/SÉNAT, Annexe procès-verbal de la séance du 20 février 1986, Imprimerie du Sénat.
- (132) 詳細はこの改正法案を検討する、拙稿「フランスのコンピュータ犯罪と刑法」前掲(註(62))一六九頁以下、恒光徹「フランス一九八六年刑法典改正法案(四)・完」岡山大学法学会雑誌二八卷二号(一九八八)一三五頁以下、参照。
- (133) 中山研一・神山敏雄編『コンピュータ犯罪等に関する刑法一部改正』前掲(註(68))三九頁。
- (134) Jean Pradel et Christian Feuillard, Les infractions commises au moyen de l'ordinateur, Revue de droit pénal et de criminologie, 1985, p.307.
- (135) Pierre Sargos et Michel Massé, Le droit pénal spécial né de l'informatique, Informatique et droit pénal, Cujas, 1983, p.26.
- (136) Pradel et Feuillard, op. cit., p. 309.
- (137) Ibid., p. 310.
- (138) Crim. 10 décembre 1970, D.S. 1972, J. 155.
- (139) Pradel et Feuillard, op. cit., p.311.
- (140) Pradel et Feuillard, op. cit., p.314.
- (141) Ibid., p. 315.

- (142) Crim. 3 août 1912, S. 1913, I, 337.
- (143) Sargos et Massé, op. cit., p.28.
- (144) Pradel et Feuillard, op.cit., pp.317 et 318.
- (145) Ibid., p.320.
- (146) Ibid.
- (147) Françoise Chamoux, La loi sur la fraude informatique: de nouvelles incriminations, J.C.P. 1988, I, 3321, n° 2.
- (148) Proposition Assemblée Nationale, n° 352, 5 août 1986.
- (149) Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, J.O. 6 janv. 1988; J.C.P.1988, III, 61042. 本法を解説する拙稿「情報処理関連不正行為に関する一九八八年一月五日の法律第八八一―一九号」國學院法學二六卷一号二七九頁以下(一九八八)、拙稿「コンピュータ犯罪と一九八八年のフランス刑法一部改正」前掲(註(62))、を参照。なお、情報処理犯罪全般について Raymond GASSIN, Informatique (Fraude informatique), Repertoire de droit pénal et de procédure pénal, 1995, p.2 et seq. 参照。
- (150) Hervé Croze, L'apport du droit pénal à la théorie générale du droit de l'informatique, J.C.P., 1988, I, 3333, n° 1.
- (151) 恒光徹「フランスの一九八八年コンピュータ犯罪立法について」前掲(註(62)) 九八頁。
- (152) Chamoux, op. cit., n° 3.
- (153) Croze, op. cit., n° 2.
- (154) 恒光徹「フランスの一九八八年コンピュータ犯罪立法について」前掲(註(62)) 九九頁。
- (155) 恒光徹「フランスの一九八八年コンピュータ犯罪立法について」前掲(註(62)) 一〇九頁。
- (156) Croze, op. cit., n° 10.
- (157) Ibid.
- (158) この点については、不正の概念による限定は裁判官により最大限尊重されることとならうとする立法者の認識 (Rapport

René André, *Assemblée Nationale*, n° 744 (1986-1987), p.13.) や、「不正行為の概念は判例によってよく限定されている」ので「この表現はフランス法に適合した申し分のないもの」とする評価 (Chamoux, *op. cit.*, n° 5.)<sup>159)</sup> が示されている。

(159) この法案は、その第四条で、「故意に、権限無く、記録されたデータまたはプログラムを取得した者」を罰すべきものとしていた (*Proposition Assemblée Nationale*, n° 352, 5 août 1986.)。

(160) 一九八九年一月二〇日付け毎日新聞夕刊。設置台数を比べると、一九八八年の資料では三〇〇万台と、同時期のわが国の「キャプテン・システム」の四万五〇〇〇台、イギリスの「プレステル」の七万六〇〇〇台と驚異的な開きがある (一九八八年一月三日付け以降連載の読売新聞「生活情報新世紀——ミニテルの冒険——(一)——」)。

(161) Chamoux, *loc. cit.*

(162) Philippe Rosé, *La criminalité informatique*, Presses Universitaires de France, 1988, p.65.

(163) このような見方に否定的な見解として、恒光徹「フランスの一九八八年コンピュータ犯罪立法について」前掲(註(62))九五頁。

(164) このフランスの新しい刑法典については、法務大臣官房司法法制調査部編『フランス新刑法典』法曹会(一九九五)を参照。なお、同書の情報処理犯罪に関する部分は筆者が翻訳を担当しているので、以下の条文の訳文は同書からそのまま引用する。

(165) 島岡まな「フランスにおけるハイテク犯罪の最近の動向」『宮澤浩一先生古稀祝賀論文集(第三卷) 現代社会と刑事法』成文堂(二〇〇〇)二一九頁。

(166) Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, <<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT00000801164&dateTexte=>> visited on Dec. 26, 2011. 本法の解説として Emmanuel DERIEUX, *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et le droit de la communication*, JCP n° 29, 14 juillet 2004, 1305.

(167) Loi n° 2004-575 du 21 juin 2004, art. 46-1.

- (168) Loi n° 2004-575 du 21 juin 2004, art. 45- I.
- (169) Loi n° 2004-575 du 21 juin 2004, art. 45- II.
- (170) Loi n° 2004-575 du 21 juin 2004, art. 45- III.
- (171) Frédérique CHOPIN, Cybercriminalité, Répertoire de droit pénal et de procédure pénal, 2009, p.3 et seq.
- (172) 渡邊卓也「サイバー関係をめぐる刑法の一部改正」前掲(註(106))二七―二八頁。
- (173) 法案段階で、フランスがこのような改正を選択すれば、サイバー犯罪条約の求める最小限の要求に応えるのにいかなる不都合もなくなるであろう」との指摘もなされていた (Jean-François FORGERON et Virginie PRAT, Le projet de la loi portant approbation de la Convention sur la cybercriminalité, Gaz. Pal., 2004, 1, Doctr. 80.)。
- (174) Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. 前掲(註(166)) 参照。
- (175) 本稿「II 4 (3)」参照。
- (176) 平成二二年版の情報通信白書は、その後のフランスが、デジタル経済を将来の成長のエンジンと位置づけ、包括的な国家戦略「デジタルフランス二〇一二」を発表し、大規模な投資を行おうとしていることを紹介している (総務省編『平成二二年版情報通信白書』(二〇〇九) 八頁以下)
- (177) 島岡まな「フランスにおけるハイテク犯罪の最近の動向」前掲(註(165))一三五頁。
- (178) 佐久間修「情報犯罪・サイバー犯罪」前掲(註(108))一一六頁。

## VI むすび

コンピュータ犯罪研究の創始者として知られるパーカーは、一九八〇年代前半の著書の中で、コンピュータ犯罪は一つの犯罪類型ではなくあらゆる犯罪の変異型であって、やがてはこの変異型の方が優勢になり、将来は非コン

コンピュータ犯罪とコンピュータ関連犯罪を区別する意味がなくなるであろう、と述べている。<sup>179</sup> その専門性と結びついた特殊な例外的な犯罪として登場したコンピュータ関連犯罪が、やがてコンピュータ・テクノロジー利用の普及・普遍化・インフラ化にともない増殖し、旧来の犯罪を念頭においた犯罪統制手段を凌駕するにいたることを予言したものと受けとれる。事態は、情報処理と進化する通信テクノロジーとの融合という要因によって、パーカーの予測が前提としていた状況とはその方向性をやや変えたが、コンピュータ・ネットワークに関連する犯罪が、今や不断にそれへの対策を講じなければならぬ普遍的な重要課題となっていることは疑いない。<sup>180</sup>

本論文は、このような刑法学の直面する今日の課題を意識しながら、コンピュータ・ネットワーク犯罪対策刑事法制の発展の経緯を跡づけ、今後の方向性を探る作業を試みた。

そこで、まず確認しなければならないのは、わが国最初のコンピュータ犯罪関連立法以降の部分的・断片的といわれる立法的対応が、すでにその中に伝統的な法益保護をはみ出した部分、すなわち情報処理の機能、ひいてはコンピュータ・ネットワークの機能の保護への指向を胚胎していた点である。さらにいえば、一九八七年の最初のコンピュータ犯罪対策立法前夜に、ネットワーク犯罪の捕捉を指向する刑事立法発展を示唆する見方は現れていた。たとえば、「コンピュータ・システムの性能の向上と普及の進展は、通信システムの分野にも波及し、電子交換機等の機器の導入により通信ネットワーク自体がコンピュータ・システムとみなし得るものとなり、あるいはそのようなネットワークを介して複数のコンピュータ・システムの間で情報の通信や処理が行われるようになるなど、コンピュータ・システムと通信ネットワークが融合化し、一体となって情報処理と情報通信を行う『情報システム』を形成するようになりつつある。<sup>181</sup> (傍点筆者)」との警察当局の認識などがそれである。

次に、コンピュータの利用に関連して生じた不正行為に直面し、刑事司法と刑法学説が、伝統的な刑法の保障原則をふまえた解釈と、合理的・効率的な犯罪統制を目指す解釈との間で揺れ動きつつ、立法の方向が模索され、わが国独自の情報処理領域の刑事立法が発展してきた経緯を跡づけた。ここでは、フランスのような情報処理犯罪固有の規制に焦点を合わせた総合的立法方式を採らず、既存の処罰の体系を尊重する控えめで現実的な対応を選択したともいえる方法が選択されたことが確認された。それは、刑法システムの枠組みへの大きな変革を避けようとする慎重な姿勢のあらわれかもしれない。大胆な変革を迫る主張に応えるよう、今後の立法が方向を転換すべきなのかはひとまず措くとして、最初の刑事立法以来、特別法を含めたコンピュータ・ネットワーク犯罪関連の刑事規制法制の体系が、情報処理とネットワークの保護の方向性をもつて、徐々に形成されつつある現状を注意深くみまもる必要がある。

(179) パーカー『コンピュータ犯罪研究総論』前掲(註(8))「序Ⅺ―Ⅻ」。

(180) 佐久間教授は、刑法典誕生百年に際して、「近年の立法論および解釈論において、刑法典に最も多くの課題を突きつけたテーマが、情報犯罪・サイバー犯罪の領域であり、とくにその背景には、「コンピュータ・ネットワークの構築を契機とした仮想(バーチャル)社会の出現がある」ことを指摘している(佐久間修「情報犯罪・サイバー犯罪」前掲(註(108))一〇八頁)。

(181) 警察庁長官官房編『情報化とセキュリティネットワーク社会への対応』ほうしゅう出版(一九八六)「はしがき」。