コンピュータ・ネットワークに関連する犯罪と刑事立法（一）

南部篤

Ⅰ　はじめに

情報・通信テクノロジーのめざましい発展は、わたくしたちの社会に、はかりしれないほど大きな恩恵をもたらした。しかし同時に、コンピュータ・ネットワークに関連する不正行為という、この社会にとっての深刻な脅威も生み出した。

コンピュータによる情報処理技術がさまざまな分野に応用されるようになり、やがて電気通信技術と結びついてネットワーク化が進行し始めると、その利用度・利用分野は加速度的に大きくなる。それとともに、社会のコンピュータ・ネットワークへの依存度は、それなしには社会が立ち行かなくなるほど高まって行く。コンピュータなしには身動きがとれない社会、コンピュータに支えられた社会は、いいかえれば情報テクノロジーをその成立の基盤と

する社会にほかならない。したがって、その依存度が高まれば高まるほど、それが宿命的に持つ性質であるヴァルネラビリティ（vulnerability、脆弱性）も、必然的に背負いこむこととなる。[1] ひとたびシステムの障害が生じると、小さなほころびが想像もできない大きなものに拡大し、社会生活が麻痺したり大規模な災害に発展することもありうる。[2] その原因が、事故による場合であろうと、ここに論じようとする犯罪・不正行為による場合とでかわりはない。むしろ、ネットワーク化の進展[3]が、空間的な制約から人間の能力を解放し、拡大したことにより、故意の行為――システムへの不正侵入・加害など――の機会も大きく広がった点では、事故よりも故意の犯罪・不正行為の脅威こそがより深刻といってよいかもしれない。こうした観点からは、今日注目されているクラウドコンピューティングの発展を背景に、この問題が今後さらに重要性を増していくように思われる。

このクラウドコンピューティングとは、ネットワーク上に点在するＩＴリソース（コンピュータ資源）を活用するための利用技術の発展形態であり、ネットワークという情報通信テクノロジーを活用することによって、ユーザが必要とするＩＴリソースを必要に応じて必要な分だけ利用できるよう提供する画期的なサービスである。クラウドコンピューティングの登場・発展により、情報通信分野にパラダイムシフトが起きつつあるともいわれる。[4] 今日のクラウドコンピューティングの普及発展は、ＩＴ利用コスト縮減による効率化、高機能化、地理的に離れた場所に情報資源を置くことによる自然災害への有効な備え等の点でも意義を有するが、同時に、今後はネットワーク上からの不正な干渉・侵入への対処という課題もさらに重要性を増すこととなると思われる。[5]

情報セキュリティと法とのかかわりを考える場合、情報処理の過程に人間の目が届きにくく、一般のユーザにとってブラックボックスの領域が大きいこと、また不正な操作により記録の改ざんなどが行われても痕跡が残り難く発見

が困難であるといった特徴などから、犯罪・不正行為への対処がつねに中心的な課題とならざるをえない。社会環境や人々の生活様式、価値観に大きな影響を与えつつある新しいテクノロジーの発展という変化の中で、それまでなかった新しい手口の不正行為や、新たに生まれた価値を侵害する不正行為などが次々と現れ、刑事法の領域において多くの問題を提起し続けている。

刑事規制の分野では、はじめに合目的的・拡張的な法解釈による対応が試みられるが[6]、やがて柔軟な法解釈による対応の困難さが臨界点を超えた部分から順次刑事立法による対処が行われていく[7]。

本論文は、このようなコンピュータ・ネットワークにかかわる不正行為・犯罪現象に対する刑事規制立法の展開過程を眺め、その課題を明らかにし、あるべき刑事規制の方向性を探ろうとするものである。いいかえれば、刑事立法の指針を見出すための基礎的考察を行おうとするものである。

本論文においては、まず、コンピュータの利用に関連して生じた不正行為――刑罰法令で捕捉できる範囲外のものも含める趣旨で「不正行為」というべきであるが、便宜上、以下では端的に「コンピュータ犯罪」という――に直面した時期の刑事司法・刑法学がどのように対応したかを、コンピュータ犯罪概念の把握の点から概観する。次に、コンピュータ・ネットワーク社会（高度情報化社会）の段階に達した今日において、「コンピュータ犯罪」がどのように変容したかを、ネットワークの悪用とネットワークの侵害とを対比しつつ検討する。次いで、刑事立法による対応の軌跡を跡づけ、その問題点を探り、コンピュータ・ネットワーク犯罪に対する刑事規制の考察を試みる。止まることのないテクノロジーの進歩がさらなる課題を生み続けることが避けられない以上、今後のあるべき刑事立法の方向性を探りつづけることが重要な作業と考えられるからである。

(1) コンピュータ・テクノロジーへの依存の問題性は、その技術が、不可避的な属性として脆弱性・脆さをともなうことから生じる。たとえば、情報処理技術に依存する社会が事故や犯罪の脅威に対していかに抵抗力が弱いものであるかを描いた、August Bequai, How to Prevent Computer Crime, 1983. の日本語訳書である、堀部政男＝堀田牧太郎訳編『情報犯罪』（啓学出版、一九八六）は、そのサブタイトルに「コンピュータ社会のバルネラビリティ」を掲げていた。

(2) これを強く印象付けたのが、一九八四年（昭和五九年）に発生した世田谷電話ケーブル火災事故である。一般電話八九〇〇〇回線に加えて、データ通信用の三〇〇〇回線が不通となったため、多くの銀行のオンライン・システムが不通となり、警察・消防への緊急通報も途絶し、周辺道路では、信号機が車両通行量を検知して点滅間隔を調整する信号制御ができなくなるなどの事態が生じ、完全復旧までに九日間を要した。

情報化社会のインフラを直撃した初の都市型災害として知られるこの事故は、情報化社会のヴァルネラビリティを端的に示したものといえる（野村好弘＝小賀野晶一「電気通信事業者の損害賠償責任――世田谷通信ケーブル火災事故を素材にして――」時の法令一二五八号二六頁（一九八五）、松本恒雄「電気通信事故と損害賠償論の課題（上）」法律時報五八巻六号八七頁（一九八六）、落合誠一「電気通信事業者の損害賠償責任」ジュリスト増刊・ネットワーク社会と法二八頁（一九八八）。）。

(3) わが国で一九九三年に商用サービスが開始されたインターネットは、利用者数が、一九九七年の一一五五万人から二〇一〇年の九四六二万人と、一三年間で八・二倍に拡大した（総務省編『平成二三年版情報通信白書』三三頁（二〇一一））。

(4) クラウドコンピューティングのわが国の利用実績はアメリカに比べ著しく立ち遅れており、日米間の利用実績格差は二〇一〇年度で二・五倍といわれている。しかし、二〇〇九年度は三・八倍の差であったから、格差は急速に縮小しつつあるともいえる（総務省編『平成二三年版情報通信白書』二七一頁）。

(5) クラウド・コンピューティングという「次世代コンピューティング・パラダイム」の進展については、二〇一〇年度から二〇一一年度、国産クラウド元年、大企業はプライベート・クラウドの検討を優先、二〇一二年度から二〇一三年度、海外クラウドの日本進出が本格化、二〇一四年度以降、さまざまなＩＴリソースが利用可能となり大企業はハイブリッド・クラウド環境へ移行、という細かな予測（ロードマップ）を示したうえで、そこでの課題がセキュリティに対する懸念の払拭等にある

ことが指摘されている（野村総合研究所『ＩＴロードマップ二〇一一年版』東洋経済新報社（二〇一一）六五頁）。

（6）後述する自動車登録ファイル事件、オンラインシステム不正操作事件、キャッシュカード偽造事件、テレフォンカード偽造事件などがそれである。

（7）後述するように、電磁的記録の改ざん行為・消去行為等の明確な犯罪化、コンピュータを用いた財産的事務処理における不正行為の処罰、不正アクセス行為の犯罪化、スキミング等によるカード偽造準備行為等の犯罪化、電子メディアによるわいせつ表現の規制の明確化、ウィルス作成行為等の犯罪化などがその例である。

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」

本稿においては、いわゆる「コンピュータ犯罪」が注目を浴び検討の俎上に載せられ、やがて急速なテクノロジーの発展とコンピュータシステムの普及にともない、「情報犯罪」、「ネット犯罪」、「サイバー犯罪」等さまざまな呼称が現れる過程を考察の対象とするが、そこでの「コンピュータ犯罪」という用語については、法律上の犯罪の定義からある程度自由な用法によることを確認しておかなければならない。

いうまでもなく、厳密には、刑罰法令に規定された犯罪構成要件に該当する違法な行為であって、それについて行為者を非難しうる場合（犯罪成立が肯定しうる場合）に、はじめて犯罪と呼ぶべきである。しかし、コンピュータ犯罪として検討対象とされるべきさまざまな行為の重要部分は、処罰規定を適用することが困難であること自体が検討を要することの理由となっているのである。したがって、不正な行為であることが明らかで、放置しておくことが耐え

難い行為でありながら、既存の処罰規定による捕捉が困難な逸脱行為こそが、解釈論において、立法論において、検討すべき対象ということになる。処罰可能な不正行為と法の不備により処罰から抜け落ちる不正行為との限界はどこか、また、後者のどの部分までを立法により犯罪化すべき範囲かを検討することが重要である以上、ここではひとまず、ひろくコンピュータに関連する不正行為を指してコンピュータ「犯罪」と呼ぶことから検討をはじめることとする。[8]

2　コンピュータ犯罪の登場

(1)　新たな犯罪現象としてのコンピュータ犯罪

一九七一年（昭和四六年）の石田晴久氏の「コンピュータを悪用する犯罪の手口」[9]が、わが国で最初にコンピュータ犯罪を紹介したとされる論稿であるが[10]、それは、一九七〇年に開催されたアメリカの学会で、「コンピュータ犯罪」という「あまり学会らしからぬテーマの研究発表」が行われたことを紹介するものであった。そこでは、コンピュータ犯罪を、A．プログラムの改変により横領を行う、B．計算機時間を売る、C．自社のソフトウェアを競争相手に売る、D．自社の保持するデータを売る、E．ハードウェアを盗み出して売る、という五つの手口に分類し、その特徴として、発覚しにくいことと、発覚しても法律上処罰が困難なことをあげ、また、磁気記録の消去やプログラムのパンチカードの引き抜きなど容易にできる不正操作が大混乱、大損害を生むという「コンピュータがきわめてもろい面をもっている」ことを指摘し、「どうもアメリカのみならず日本でもコンピュータ犯罪などというものに対しては、法律はまったく無防備なようである。もうそろそろ将来に備えて、電子計算機法律学とでもいった新分野を、開拓する人が出てもいいような気がする。」というきわめて先見性に富む指摘が行われている点が印象的である。[11]

刑法学者も、このころから、コンピュータに関連する犯罪に目を向けるようになる。そこでは、「何が刑法の適用対象となるか」と、「どこが刑法解釈の限界点か」を意識したアプローチがとられている点が特徴的である。一九七一年に発表された西原春夫博士の論稿は、現行法の解釈範囲内でどのような犯罪が成立しうるかという観点から、コンピュータに関連する不正行為を、①コンピュータに向けられた犯罪と、②コンピュータを悪用する犯罪とに分けて論じられている。(12)

（2）コンピュータ関連事犯の増加とコンピュータ犯罪

一九八〇年台に入ると、後述するように、キャッシュカードや、銀行オンラインシステム悪用事案が注目をあびるようになる。このころ多くの論稿を発表された板倉宏博士は、コンピュータに関連する犯罪を広くコンピュータ犯罪として取り上げ、それを、①コンピュータを悪用する行為、②コンピュータに害を加える行為、③コンピュータによって得られた情報を悪用する行為、に分類し論じられている。(13) また、①コンピュータを悪用する行為、②コンピュータに加害する行為、③コンピュータの情報を盗み取る行為、④キャッシュカード犯罪、の四つに分類して論じる論稿(14)や、CD犯罪を除くコンピュータ犯罪として、①不正なデータの入力、②データやプログラムなどの不正の入手、③コンピュータの破壊、④コンピュータの不正使用、⑤プログラムの改ざん、⑥磁気テープなどの電磁的記録物の損壊、に分類して論じるもの(15)などがこのころ発表されている。(16)

一方、この時期の警察の対応を見ると、一九八二年にコンピュータ犯罪を特集した「警察學論集」誌上の論稿では、「警察庁では、コンピュータ犯罪を『コンピュータ（プログラム及びデータを含む。）に向けられた犯罪又はこれを悪用した犯罪』と定義し、犯罪捜査及び防犯対策上参考となる事例は広くこれを含める」とする見解が示されていた。(17) ま

た、一九八二年版警察白書には、前年の金融機関の現金自動支払システムを利用した犯罪や、不正データの入力、無権限使用等各種事犯が多発したことなど、初めて「コンピュータ犯罪」の記述が現れたが、翌一九八三年版（昭和五八年版）警察白書は、「科学技術の進歩と犯罪」との節を設けてコンピュータ犯罪を正面から取り上げている。それによれば、「警察では、コンピュータ犯罪を『コンピュータ・システムに向けられた犯罪又はこれを悪用した犯罪』と定義して、その発生実態の分析と、捜査及び防犯上の対策を進めているところであ」り、「コンピュータ犯罪は、犯行の態様から、ＣＤ犯罪…とそれ以外のコンピュータ犯罪の二つに分けることができる。」とした上で、ＣＤ犯罪を除外したコンピュータ犯罪には、「『不正データの入力』、『データ、プログラム等の不正入手』、『コンピュータの破壊』、『コンピュータの不正使用』、『プログラムの改ざん』、『磁気テープ等の電磁的記録物の損壊』の六つの類型がある。」としていた（なお、これらの類型にあたる事案の一九八一年から八二年までの認知状況が各年二、三件程度だったものが、ここ数年で増加に転じつつあることが示されている[18]。）。

（3）　初期の不正行為の特徴とコンピュータ犯罪

以上のコンピュータに関連する犯罪をめぐる議論をながめると、まず、一九七〇年代に、文字どおりのコンピュータ先進国アメリカの状況が伝えられた時期においては、コンピュータは、研究機関やごく一部の企業などにしか利用されておらず、専門的知識・技能を有するオペレータなどが扱うもので、身近なものとはいえなかった。そこで、「コンピュータに向けられた犯罪」としては、磁気テープなどに保存された電磁的記録の改ざんや消去の問題が取り上げられ、「コンピュータを悪用する犯罪」としては、たとえば、銀行員が顧客の預金の利子計算に関し虚偽データを入れて差額を自分の口座に組み入れてしまうとか、在庫管理のデータを不正操作して製品を横領する、といった

ケースが想定されるに過ぎなかった。そのため、コンピュータ犯罪の多くは、「プログラマーやパンチャー、現場のオペレーターなど、専門的な知識と技術を持つ者のみが犯すことができ、第三者は一般にそれらの者と共謀することが必要となる」ものと考えられていた[19]のである。

3　コンピュータ犯罪の広がり

(1)　コンピュータ犯罪の急増

しかし、一九八〇年代に入り、さまざまな分野へのコンピュータの利用が大きな広がりをみせるようになると、コンピュータに関連する各種の不正行為も急速に増え、注目を集めるようになる。

一九八一年には、銀行職員のオペレータがオンライン端末を不正操作して架空口座から一億三〇〇〇万円を引き出した三和銀行事件や、機械のテストと偽り端末操作をさせて架空口座から三〇〇〇万円を引き出した平和相互銀行事件、社員ぐるみで長期間にわたりオンライン端末を不正操作し架空貸付口座から一億二〇〇〇万円を引き出した北浜クレジット事件、銀行職員のオペレータがCDカードにデータを書き込むなどして不正に作り二〇〇〇万円を引き出した近畿相互銀行事件、他人のID、パスワードを無断使用し電話回線経由で大学のコンピュータを不正に使用した岡山大学事件など[20]、次々にコンピュータに関連する犯罪が起こり、「コンピュータ犯罪元年」などと呼ばれた[21]。

この時期は、多くのコンピュータに関連する事案が発生し、また被害も小さくないものの、依然としてコンピュータの利用が金融機関を中心とする企業と研究機関などに限られていたため、コンピュータ犯罪の概念にそれほど変化は見られない。なお、金融機関のオンラインシステムなどのコンピュータシステムによるサービスの提供が一般に開かれていく分野では、それにともないCD犯罪などが増加して行くが、窃盗等の伝統的な財産犯罪の延長線上の新た

な手口に過ぎないため、前述のように、CD犯罪を除いてコンピュータ犯罪が把握されることとなる。

(2) システムの機能に対する加害の視点

また、はじめはコンピュータ犯罪を、「コンピュータ（プログラム及びデータを含む。）に向けられた犯罪又はこれを悪用した犯罪」としていた[22]警察庁は、後に、「コンピュータシステムの機能を阻害し、又はこれを不正に使用する犯罪」と定義を変更しているが[23]、コンピュータのハードウェアやプログラム、データというような、いわば部分的な侵害対象のとらえかたから、「システムの機能」に着目した把握へと発展的に定義を変更している点が、この間のコンピュータ犯罪の急速な増加を反映した変化といえるかもしれない。

しかし、この時期、基本的には従来とほぼ同様の意味で「コンピュータ犯罪」という言葉が用いられ続け、コンピュータに関連する刑事法学の議論の状況にも、立法その他の法状況にも大きな質的変化はみられない。

(3) ネットワーク化の緩やかな進行

インターネットの利用は、一九九〇年代に入り徐々にひろがりを見せ始めるが、依然として大学や研究機関の学術ネットワークという段階にとどまっており、コンピュータを用いた情報のやり取りは、金融機関の業務用システムなどの閉ざされたネットワークが中心であった。一般の個人ユーザーが参加するのは会員同士のパソコン通信があるのみで、これも開かれたものではなく、一九九〇年代前半ころまではコンピュータ・ネットワークの利用は発展途上ともいえる過渡的段階にあった。金融機関のオンライン悪用型の財産侵害行為（内部者による不正送金、CD犯罪）や、データの不正入手、ハードウェアやプログラムに向けられた侵害などは増加し続け、刑事立法による対応が行われる（後述する一九八七年の刑法一部改正）ものの、そこではネットワークの保護を正面に見据えた対応は見送られたのであ

る。

4　コンピュータ犯罪からネットワーク犯罪へ

（1）インターネットの急速な普及

状況が大きく変わるのは、一九九〇年代の半ば以降である。ハードウェアやソフトウェア、通信機器等の進歩と通信環境の整備が進み、一般の個人や企業がパーソナルコンピュータをインターネットに接続して利用する形態が急速に普及し、ウェブページの閲覧や電子メールによるコミュニケーションが容易になり開かれたネットワークが実現すると、金融機関の内部者などによる事案にとどまっていたコンピュータ犯罪は大きく変容をみせる。すなわち、ネットワークを利用した詐欺や名誉毀損、ポルノグラフィの事案などが急増し、またネットワークへの不正侵入事案（いわゆるハッキング等）が増加したのである。インターネットの普及が便利で強力な犯行手段を提供するようになったためといいうるであろう[24]。

この時期以降には、「コンピュータ犯罪」に代わって、「ハイテク犯罪」が用いられることが多くなり、やがて、「サイバー犯罪」との呼称が現れる。こういった、コンピュータ＝情報処理技術に関連する不正行為の呼称の変化は何を意味するのか。

（2）コンピュータ犯罪からハイテク犯罪へ

まず、「コンピュータ犯罪」は、コンピュータがスタンドアローンないしは専用回線で結ばれた閉じたネットワークにとどまっていた時期の、その悪用を意味する名称として出発した。しかし、コンピュータが犯行手段として「本格的に」その威力を発揮するようになるのは、それが電気通信技術と結びつき、通信テクノロジーの発展により大

量・迅速な情報のやり取りの能力を獲得するようになってからである。二〇〇〇年前後に動き出したe-Japan構想という政府の政策も、インターネット常時接続の一般化、ブロードバンド化を推進し、そのような流れを加速した。そしてその段階、すなわち、社会経済構造全体が情報処理・情報通信技術（Information-Comunication Technology）に依存したものとなって以降、コンピュータ・システムへの加害行為は、きわめて深刻な脅威として自覚されるようになって行く。

「ハイテク犯罪」はそのようなタイミングで注目をあびたのである。一九九八年、英国バーミンガムで開催された第二四回主要国首脳会議（バーミンガム・サミット）において、国際犯罪のテーマの中でハイテク犯罪（high-tech crime）が取り上げられ、高い関心を集めた。首脳会議の討議の結果は、共同コミュニケの中に、ハイテク犯罪と闘うための証拠としての電子データの取得・保存等に関する手続法的枠組み整備と、国際協力、産業界に対する協力の呼びかけなどが盛り込まれたが、「こうしたことが、われわれの、インターネットおよびその他の新たなテクノロジーの悪用を含む広い範囲の犯罪との闘いに寄与することになる」[25]ことが確認されている。[26]以後、これをきっかけに、「ハイテク犯罪」という呼称がひろく用いられることとなる。しかしこれも、先端的技術革新がもたらした新たな事態――ネットワーク化というキーワードで了解しうる変化の途上にある事態――であって、やはり過渡的な状況を背景とする表現であった。

（3）ネットワークの発展とサイバー犯罪

ネットワーク化の進展にともない、インターネットにより実現される新たな情報空間を意味するサイバースペース（cyberspace）という言葉がポピュラーになり、サイバー・エコノミー（cyber economy）、サイバー・モール（cyber mall）、

サイバー法（cyber law）などが新しい仕組み・枠組みとして注目されるようになるにつれ[27]、次には、「サイバー犯罪」[28]という言葉が用いられるようになって行く。

サイバー犯罪は、第一に、コンピュータ・ネットワークを犯行手段に用いたさまざまな犯罪、または、コンピュータ・ネットワークを加害対象とする犯罪を中心とする不正行為の範疇という特徴を有するものである。第二に、より重要な点は、サイバースペース自体の機能・秩序・価値を侵害する不正行為を含むという性質を持つことである。そこでたとえば、後述するように、コンピュータ・ウィルスを作成・使用する行為は、伝統的な「業務妨害罪」の延長線上に捉えられる犯罪――業務妨害の予備段階を犯罪化する「処罰の前倒し」――にとどまらず、サイバースペースの正常な機能・秩序を害し、サイバースペースという電子情報空間への信頼を害する性質を持つものと考えられることになる。こうして、「コンピュータ犯罪（コンピュータ関連犯罪）」は、テクノロジーの発展段階にそって、「ハイテク犯罪」、「サイバー犯罪」へと姿を変えてきたのであるが、そのような変化をもたらした中心的要素に、ネットワーク化の進展があったことが重要であると考えられる。そこで、本論文は、この問題領域の中心的本質的要素を考慮しつつ、かつ、検討対象をもらさず広くとらえる趣旨で、「コンピュータ・ネットワークに関連する犯罪」との呼称を用いることとした。こうした視点をふまえながら、以下に、法解釈上の限界の問題、刑事立法の対応の問題を検討して行く。

（8）　たとえば、この分野の研究の草分け的存在として知られるドン・パーカーは、研究対象を設定するにあたり、ひろく、「何らかの形でコンピュータに関連しており、それにより被害者は損失をこうむるかその可能性があり、加害者は利益を得る

かその可能性があるような意図的な行為」を「コンピュータ悪用」と定義するところから出発している（ドン・B・パーカー著・鵜澤昌和監訳『コンピュータ犯罪研究総論』秀潤社（一九八四）二〇頁以下）。研究対象の設定にあたり、意識的に、「コンピュータ犯罪（computer crime）」ではなく、「コンピュータ悪用（computer abuse）」という表現が用いられていた（Parker, Fighting Computer Crime, 1983,pp.16-17.）点が示唆的である。

(9) 石田晴久「コンピュータを悪用する犯罪の手口」蟻塔一八五号昭和四六年三月号一頁（一九七一）。なお、その後の、石田「コンピュータ犯罪について」法律のひろば二四巻六号二九頁（一九七一）も参照。

(10) 西原春夫「コンピュータの導入と刑事法上の諸問題」ジュリスト四八四号三五頁（一九七一）。

(11) 石田「コンピュータを悪用する犯罪の手口」前掲（註(9)）論文一頁以下。

(12) 西原「コンピュータの導入と刑事法上の諸問題」前掲（註(10)）論文三六頁。

(13) 板倉宏「コンピュータ犯罪」判例タイムズ四二九号（一九八一）二一頁。なお、同「コンピュータ犯罪と法律」ビジネスコミュニケーション一九巻七号五一頁以下（一九八二）、同「コンピュータ犯罪と刑法」法学セミナー一九八二年七月号一〇〇頁以下（一九八二）、同「コンピュータ犯罪と刑法上の問題点」研修四〇九号三頁以下（一九八三）、同「新しい犯罪への対応」法学セミナー三七〇号六七頁以下（一九八五）、同「情報犯罪と刑事立法」法学セミナー三八五号九八頁以下（一九八七）、同「情報犯罪と刑事法」警察学論集四〇巻四号一〇九頁以下（一九八七）、同「コンピュータ犯罪と刑事法」ジュリスト七〇七号参照。

(14) 大谷實「コンピュータ犯罪（上）――刑法の改正問題および罪刑法定主義と関連づけて――」法学セミナー三六三号二〇頁（一九八五）、同「コンピュータ関連犯罪と刑法の改正」判例タイムズ六〇二号二頁（一九八六）。

(15) 宮野彬「情報犯罪」ジュリスト増刊『高度情報化社会の展開と課題』二六四頁。

(16) この他にも、コンピュータ犯罪の多種多様性・広範性、現行法規に触れないものも含める必要がある等の理由をあげ、「コンピュータ犯罪とは、コンピュータが直接的あるいは間接的に何らかの形で介在した社会悪行為」と定義する見解（鳥居壮行「コンピュータ犯罪研究」警察学論集三二巻六号（一九七九））や、定義にとらわれて視点をゆがめたり形式論に陥るこ

とを避ける等の考慮から、「コンピュータを利用した反社会的行為、ならびにコンピュータの存在によって現われた反社会的行為」と捉える見解（金井浄「コンピュータ犯罪の特質」警察学論集三五巻六号（一九八二））がみられる。

(17) 人見信男（警察庁捜査第一課課長補佐）「コンピュータ犯罪の発生状況」警察学論集三五巻一一号一〇頁（一九八二）。また、廣畑史朗（警察庁調査統計官付警視）「コンピュータ犯罪と刑法の適用」同誌同号四五頁（一九八二）は、コンピュータ犯罪の態様分類については、CD犯罪を除くコンピュータ犯罪を、「①コンピュータに不正のデータを入力することにより不法に財物を得たもの、②コンピュータに入力されているデータを不正な方法で入手したもの、③コンピュータを破壊したもの、④権限なくコンピュータを使用したもの」に分類し論じている。

(18) 警察庁編『昭和五八年版警察白書』（一九八三）五頁以下。

(19) 西原「コンピュータの導入と刑事法上の諸問題」前掲（註(10)）論文三七―三八頁。なお、同時期に発表されたコンピュータ犯罪に関する著作には、プライバシー侵害を中心に論じるものなど（たとえば、堀内恭一『コンピュータ犯罪――情報とプライバシー――』日本工業新聞社（一九七四））が多かったといえる。

(20) これらの事件については、小林道男「コンピュータ犯罪防止対策」警察学論集三五巻一一号六四頁以下（一九八二）、人見「コンピュータ犯罪の発生状況」前掲（註(17)）、安井正男『コンピュータ・システムとコンピュータ犯罪』財経詳報社（一九八四）一六九頁以下、菅野文友『コンピュータ犯罪のメカニズム――コンピュータ・セキュリティへの対応――』日科技連出版社（一九八九）五五頁以下、菅野文友『コンピュータ犯罪のからくり』コロナ社（一九九〇）二八頁以下、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（注釈）改定増補版』成文堂二九頁以下（一九八九）参照。

(21) トマスホワイトサイド・湯沢章伍訳『コンピュータ犯罪 恐るべきアメリカ』（一九八二）は、「訳者あとがき」の中で、これらのケースについて、「いずれの事件も、本書に引用されたアメリカのコンピュータ犯罪に源流を見る、〝本格的〟な犯罪」とし、「昭和五六年（一九八一年）はコンピュータ犯罪元年といえるのでは」ないかと述べている（同書一九〇頁）。なお、この時期には、「法とコンピュータ学会」が機関誌「法とコンピュータ」創刊号を刊行しているが、同誌は、コンピュータ犯罪を中心に編まれたものであった（《特集 コンピュータと犯罪：三浦賢一「コンピュータ犯罪概観」、金井浄「コンピュータ

犯罪の特質について」、加藤直「コンピュータ犯罪の予防――コンピュータ室管理者としての対応――」、白石高義「データ保護の技術的対策」、中山隆夫「コンピュータ犯罪とセキュリティ対策」、辛島睦「アメリカにおけるコンピュータ犯罪立法」、宮澤浩一「日本の刑法から見たコンピュータ犯罪」》法とコンピュータ一号（一九八三）五頁以下）。

(22) 人見「コンピュータ犯罪の発生状況」前掲（註(17)）一〇頁。

(23) 警察庁編『一九九〇年版警察白書』九二頁。

(24) ネットワーク侵入事案の増加等のこのような変化の予測は、一九八〇年代にはすでに行われていた。「わが国のコンピュータ犯罪の今後について、楽観を許さないその他の要因としては、パーソナル・コンピュータの普及による、いわゆる『ハッカー予備軍』の青少年の急増や、通信回線の自由化に伴う、個人レベルでのデータ通信利用の機会の増加などもしばしば指摘されてい」たのである（原田豊「コンピュータ犯罪に関する研究動向」科学警察研究所報告二五巻二号九一頁（一九八四））。

(25) 共同コミュニケの全文は、外務省のウェブ・ページを参照した（The Birmingham Summit: Final Communique, Sunday 17 May 1998, Ministry of Foreign Affairs of Japan Website〈http://www.mofa.go.jp/policy/economy/summit/1998/fin_commiq.html〉visited on Dec. 21, 2011.）。なお、バーミンガム・サミットにおける「コミュニケ」と、その別添、「ハイテク犯罪と闘うための原則と行動計画」については、「ハイテク犯罪の現状と警察の取組み」を特集する一九九八年版の警察白書が詳しい。

(26) 警察白書は、初めてコンピュータ犯罪に言及した一九八二年以来、一九九七年まで「コンピュータ犯罪」の呼称を用いてきたが、一九九八年から「ハイテク犯罪」との表記に改め、さらに二〇〇四年からは「サイバー犯罪」の項目でこの問題を扱うようになり現在にいたっている（警察庁編『昭和五七年～平成二三年版警察白書』）。サイバー犯罪とは、インターネット等の高度情報通信ネットワークを利用した犯罪やコンピュータ、電磁的記録を対象とした犯罪等、情報技術を利用する犯罪を指すものとされる。警察庁は、従来、ハイテク犯罪と呼称していたところを、「国際的動向を踏まえて」、サイバー犯罪と称するよう変更することとしたとされる（同『平成一六年警察白書』一二八頁）。これに対して、コンピュータ技術以外の他の先端技術も含む「ハイテク」という用語を避け、意識的に「ネットワーク犯罪」の名称を用いる論稿として、佐久間修「ネットワーク侵害と財産犯」産大法学三二巻二・三号（一九九八）一五〇頁以下を参照。

(27)「サイバースペース」、「サイバー・エコノミー」、「サイバー・モール」、「サイバー法」等の意義については、北川高嗣＝須藤修＝西垣通＝浜田純一＝吉見俊哉＝米本昌平『情報学辞典』弘文堂（二〇〇二）を参照。

(28) サイバー犯罪とは、不正アクセスや、コンピュータ・電磁的記録対象犯罪、ネットワーク悪用犯罪など「コンピュータ技術及び電気通信技術を悪用した犯罪」を意味するものとされる（本田尚志「サイバー犯罪の現状と対策について」警察時報六〇巻一二号（二〇〇五）一五頁）。

Ⅲ　法解釈による対応の限界

コンピュータ・システム関連の事故や不正行為は、情報化社会のネガティブな側面にほかならないが、それが登場した際には、そのときの法制度と法律学が全く予想していなかったタイプの問題現象であった。そのような急激な技術革新から生じた新しい課題に、既存の伝統的な法体系・法制度が十分対応できないのは、もとより当然なことであったともいえる。犯罪と刑罰に関する基本法である刑法もその例外ではない[29]。

すべての法は、それが制定された時代の社会状況を反映したものであることはいうまでもないが、一九〇七年（明治四〇年）制定の現行刑法も、その時代の社会の生産・流通・消費のあり方、技術革新の程度など、その当時の社会構造や人々の生活様式のありようを前提に作られたものである以上、時代が下ると、個々の犯罪類型の内容において――さらには基本的枠組みの一部においてさえ――、今日の社会に適合しない部分を生じるのである。

文書概念を例にとれば、従来の紙に記載されて利用・保存に供されてきた文書は、あらゆる分野の事務処理で急速にデジタルデータ（磁気記録）化されていった。今日では、行政が扱う各種の記録をはじめとしてほとんどの情報が

電磁的記録の形態で記録・保存され利用に供されている。これは、伝統的な文書概念が予想していなかったことである。文書偽造罪や文書毀棄罪は、紙などの物体に書かれた可視性・可読性ある文書を念頭に、それぞれ文書の公共信用性、文書の効用を保護しようとしていたが、デジタルデータに置き換えられたところから、保護が及び難い部分を生じて行ったのである。

そこで、以下に、最初のわが国のコンピュータ犯罪対策刑事立法となった一九八七年（昭和六二年）刑法一部改正以前の状況を中心に、法解釈による対応の限界線上に現れた問題状況を概観することとする。

1　データの侵害と文書犯罪

（1）データの信用性の侵害

文書は、取引や各種の証明事務など社会生活上種々の場面で重要な証明手段として機能しているものであるところ、その偽造・変造などの公共信用性を害する行為を文書偽造の罪として処罰することにより、刑罰を担保に文書の公共信用性が保護されている。

文書を保護する理由がそのようなものである（人がその文書を見て一定の事実を読み取りその文書の存在を拠り所として各種の取引・事務処理等を行うという重要な機能を営むものであるということ）から、刑法上保護される文書とは、「文字またはこれに代わるべき符号を用い、一定程度の永続性をもって、物体上に記載された意思や観念の表示をいう」と解されてきた(30)。

ここでは、紙などに記載され、可視性・可読性を有するものであることが当然の前提とされているのである。ところが、すでに述べたように、情報処理技術がさまざまな分野で利用されるようになったことから、従来の紙上に固

定・表示された文書は次々にコンピュータによる処理に適したデジタルデータに置き換えられて行き、その結果、多くの重要な記録が、伝統的な刑法上の文書が要求する「可視性・可読性」を持たないものに移し替えられて行ったのである。ここでの問題は、以下の事案にみられるように、そのようなコンピュータ記録を刑法上の保護の対象となしうるのかという文書概念をめぐる解釈上の課題として現れた。

①キャッシュカードのデータ改ざんの事案

今日では、銀行など金融機関の預金の払い戻し等の処理は、ＡＴＭ（Automated Teller Machine＝現金自動預払機）を用いて行われるのが通例であり、そこで用いられるキャッシュカードも、ＩＣチップへのデータ記録や生体認証方式の採用など不正行為への効果的な対処に意を尽くした方法が採られている。しかし、オンラインシステムが稼働を始めてしばらくのあいだ――ＣＤ（Cash Dispenser＝現金自動支払機）の利用が主流であった――、そこで用いられていた初期のキャッシュカードは、暗証番号などのデータをカード自体の磁気記録部分に保存したものであったため、比較的容易に他人のキャッシュカードの預金をＣＤ機から引き出すことのできる偽のカードを作り出すことができた。たとえば、一九八一年に発生した近畿相互銀行事件は、銀行のオペレータの職にあった被告人が、職務上知った他人のキャッシュカードの暗証番号情報を利用し、窃取したカードの磁気ストライプ部分にデータを印磁するなどして不正にキャッシュカードを作りだし、これを用いてＣＤ機から約二〇〇〇万円を引き出したというものである。この事案では、不正に作られた電磁的記録部分を含むカードが文書に当たるといえるかが争われたが、裁判所は文書性を肯定し、有印私文書偽造罪、窃盗罪等で有罪を言い渡した[31]。

②自動車登録ファイルへの虚偽記録の事案

自動車登録制度は最も早い時期にコンピュータ・システムによる処理が導入されたものである。従前の紙の登録簿に調製されていたものに代わって、コンピュータのハードディスク等の記録媒体が、従来の自動車登録簿と同様に自動車登録ファイルとして用いられるようになったのである。

そのような中で、この電磁的記録にかかるファイルの性格が文書性との関係で問題となった事例、すなわち、自動車登録をしようとした者が、その際に虚偽の申告をして磁気ディスクに収納された自動車登録ファイルに不実の記載をさせたところ、このような登録ファイルに不実の記録をさせる行為が、（当時の刑法一五七条所定の）公正証書原本不実記載罪にあたるかが争われた事案が生じたのである。最高裁は、電磁的記録物である自動車登録ファイルは「公正証書の原本にあたる」との判断を示した[32]。

まず、①のキャッシュカードの事案では、被告人が、「㋑発行銀行名が記名印字されたプラスチック製のキャッシュカード原版に、他人の氏名を凸字で刻字し、㋺磁気ストライプ（磁性体の塗布された樹脂製磁気テープを帯状に埋め込んだ形態）部分に、エンコーダ（磁気印字機）を用いて暗証番号を印磁した（磁気的に書き込んだ）行為が有印私文書偽造罪にあたるかが争われた。そこでは、㋑の部分は可視性・可読性を備えており文書性に問題ないが、㋺の部分はカードリーダー等専用の機器によらなければ人が読み取ることができず、文書性を肯定することが困難であった。しかし、キャッシュカードの用途・性質上は、ＣＤ機に用いて現金の引き出しを行うことにあり、その本来的機能からみると最も重要なのは㋺の部分なのである。そこで、検察官は、(a)カードの暗証番号等の電磁的記録は、ＣＤ機に内蔵されたカードリーダーによって視覚可能であり、(b)電磁的記録のうち口座番号等の内容は、ＣＤ機から打ち出されるプリント上に文字・数字として読み取れる、と主張したが、裁判所もこれを認めた。キャッシュカードの磁気スト

ライプ中の暗証番号等の内容は、マイクロフィルムなどと同様に直接肉眼で視覚できないが、ＣＤ機に用いれば読み取りが可能となり、また取引店番号、口座番号などが打ち出されるレシートも、カードの磁気記録とは形式的には別の文書ではあるが、内容的に一体不可分の関係にある、ということを理由とする。

しかし、文書偽造の概念の中核部分は、作成名義の偽りにあるが、電磁的記録は性質上作成名義人が誰かを観念することが難しいのである。そこで、右のような文書偽造の成立を認める見解も、カードの券面上に表示された銀行名や預金者の氏名部分と、電磁的記録部分とを一体的に捉える見方に支えられたものであったということができよう。(33)

したがって、可視的表示部分を全く欠いた場合は、もはや文書偽造に問うことはできないことになる。実際、もっぱらＣＤ機に挿入使用する目的で、銀行名も預金者名の表示もまったくない白地のプラスティック版に磁気テープを貼り付け、そこに銀行の通信回線から取得したデータを解読して得た暗証番号等を印磁したカード（「キャッシュカード」の外観をまったくもたないもの）を作り出してＣＤ機から現金を引き出し窃取した事案（いわゆる札幌電電公社事件）では、私文書偽造罪での訴追は見送られている。(34)

このように、キャッシュカードの電磁的記録部分を不正に作り出す行為を文書偽造罪に問うことには、可視性・可読性のない記録を不正に作り出す行為に「文書の公共信用性」の侵害を認めうるか、作成名義の偽りが公共信用性侵害を惹起するところ、それ自体に作成名義を観念しにくい電磁的記録を文書と同列に論じることができるのか、という本質的に困難な点があったのである。つまり、データの信用性の保護を、文書の信用性の保護の枠組みに期待することには無理があったと考えられる。

次に、②の自動車登録ファイルに関する事案であるが、自動車登録ファイルに、不実の記録をさせる行為に関して

は、公正証書原本不実記載罪の成立を認めた高裁判例の集積があった[35]が、前述のキャッシュカードの事案と異なる点は、自動車登録ファイルの内容が公開されている点である。この点、キャッシュカードの「磁気ストライプの電磁的記録は、CD機を作動させる、いわば合鍵のような機能を果たすものであり、視覚可能な状態に再生されたものが公共の目にさらされることはあまりない」こととの対比で、自動車登録ファイルの文書性は認めやすいとすることには理由があるとする指摘もあった[36]。

しかし、②の最高裁決定については、これを、電磁的記録として保存されたファイル一般の文書性をひろく認めたものとは言い難い、と解する見方も有力であった。また、同決定には、本件の自動車登録ファイルは「文書」ではないが、「公正証書の原本」にはあたるとする谷口裁判官の補足意見が付されていた。「公正証書の原本」は必ずしも「文書」でなくてもよいというのである。しかし、このような考え方は、法解釈の一貫性からも疑問のあるところであって、いずれにせよ電磁的記録一般を「文書」とするには刑法の解釈上、かなりの困難があったことは否定できないのである[37]。

なお、一九八七年刑法一部改正後の事案であるが、プリペイドカードの通話可能度数データ改ざんのケースも、法解釈の限界を示したものといえる。

今日、一般に普及しているプリペイドカードのさきがけとなったテレホンカードは、偽変造行為の被害にさらされた点でも最初のものである。すなわち、テレホンカードの通話可能度数データも、一九八七年改正後の刑法一六一条の二にいう電磁的記録にほかならないので、これを不正に改変する行為は、「人の事務処理を誤らせる目的で、その事務処理の用に供する権利・義務に関する電磁的記録を不正に作ったもの」として、私電磁的記録不正作出罪に該当

することになる。しかし、一定の通話サービスに関する権利が化体された電磁的記録部分とあわせて、そのような権利を表示した外観をもち、譲渡性をそなえた有価証券として流通している実態があったのである。そこで、可視性を欠く電磁的記録部分と、可視的なカード面全体とを一体的にとらえると、電磁的記録部分のみの改ざん行為も、有価証券の変造罪にあたるとみることが可能になる。私電磁的記録不正作出罪は五年の懲役を上限とするのに対し、有価証券変造罪は一〇年の懲役を上限としている。そして特に、一六一条の二は、行使の目的で人に交付する行為を処罰する規定を欠くため、テレホンカードの変造が有価証券変造にあたらないとの解釈をとると、多くの不正に作られたテレホンカードの密売行為が放置されてしまうことになることから、この点が激しく争われた。

裁判所は、ほぼ積極の見解をとったが[38]、なかには消極の判断を示したものもあった。その代表的なものとして、千葉地裁の無罪判決は、有価証券は文書であることが前提とされているところ、「昭和六二年の刑法一部改正によって電磁的記録の定義規定が新設されたことに関して、文書の多くが電磁的記録に置き換えられつつある現状に鑑み、これ等の記録の改竄、毀棄等の不正行為を的確に処罰することが困難なため、従前の文書の偽変造罪、毀棄罪等と同様の処罰規定を設ける必要が生じたが、従来の文書概念では可視性可読性がその要件とされていたり、作成名義が観念されていたのに対し、電磁的記録については人の五感の作用では記録の存在及び状態を認識することができないものであり、またその作成過程についても入力したデータがプログラムによってほかのデータなどとともに処理、加工されて作り出されるなど複数の者の意思や行為がかかわることが多く、作成名義も観念することが困難な状態にあるので、新たに電磁的記録についての定義規定を置いたものである。こうして、従来の文書概念と電磁的記録とを截然と区別することとなり、従来の文書偽造・同行使に見合う電磁的記録の不正作出・同供用という構成要件を新設した。

そうだとすれば、テレホンカードの電磁的記録部分は文書ではなく、有価証券にもあたらないことになる。」とした[39]。

従来、有価証券も文書の一種であり、当然に文書性が要求されると解されてきたが、電磁的記録不正作出罪を新設した一九八七年改正後も、プリペイドカードを有価証券として扱うためには、すでにみた自動車登録ファイルの最高裁決定のケースのように、「有価証券」にあたるか否かを端的に検討し、その際「文書」にあたるかどうかは問題ではない、とする立論によることが考えられる。しかし、それは、すでに述べたように法解釈の一貫性・体系的整合性の点から疑問があり、妥当とはいえない。この領域でも、立法的対応が必要とされていたのである[40]。

(2) データの効用の侵害——電磁的記録の消去と毀棄罪——

文書は、すでに述べたように、社会生活上さまざまな場面で重要な機能を営んでいる。そこで、文書の「信用性の保護」とは別に、その「効用の保護」という角度から、刑法は公用文書、私用文書の毀棄罪を規定している。しかし、ここでも、伝統的な文書概念とコンピュータ記録とのギャップが、法解釈上の困難な問題として現れたのである。

前述のデータの改ざん等とは異なり、磁気テープやディスク等の記録媒体に収納されたデータを消去する行為が実際に問題とされた事案はほとんど現れてこなかった[41]が、この問題については、可視性・可読性を欠くため刑法上の文書とはいえないとすると、コンピュータ記録に置き換えられた多くのデータが刑法による保護の埒外に置かれることになるのではないか、との観点から、議論の俎上に乗せられることが多かった[42]。伝統的な文書毀棄行為の態様が、書類を引き裂く、焼き捨てるなどを典型的な行為として想定しているため、物理的破壊を伴わない場合には適用の可否が判然としなかったためである。

厳格に解すると、ディスク等のデータを保存した媒体ごと一つの「電磁的記録物」と考え、その内容の消去を器物

損壊罪に問うことには無理がある。ディスク等記録メディアの「データを記録する」という効用自体は害されていないからである。このように毀棄罪を「物の効用」を保護するものと考えると、他人のビデオテープの録画内容を無断で消去しても、器物損壊罪などにあたらないことになる。(43)

これに対して、価値のある内容、重要なデータが収納されている媒体（たとえばビデオテープ、ディスクなど）の「効用」は、「記録を行える」という働きだけでなく、そこに記録されている「内容を再生・利用できる」という働きも含まれると考えると、内容の消去自体が毀棄罪を構成すると解する余地も出てくることになる。(44)

こうして、コンピュータ・データ自体の効用は、毀棄罪による保護の範囲ないし保護が及ぶか否かが明確でなく、不安定なままにおかれていたのである。

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

情報処理技術の応用分野の中でも比較的初期の段階で実用化され普及が始まったのが金融機関などの業務である。そこでは、従来、手作業で行われていた金銭の決済処理などの財産的事務処理の大部分が、コンピュータ・システム（機械）を用いて人の判断作用を全く介さずに行われる方式に置き換えられていった。詐欺罪などの財産犯罪は、人の判断作用に働きかけて行われる不正行為を念頭においているが、自動化された電子データの処理に適用するのは難しい。また、現金や証券など物体の移動をともなわない、いわゆる電子マネーの移転によって取引の決済が行われるのが常態になると、窃盗、横領などの伝統的な犯罪類型の適用に困難を来す部分も生じたのである。

（1）　CD犯罪

わが国で、コンピュータ・システムを悪用する犯罪として最初に注目されたのが、金融機関のオンラインシステム

を利用した財産犯罪であったことはすでに述べたとおりである。なかでも、他人のキャッシュカードを用いてCD機（Cash Dispencer）、ATM機（Automated Teller Machine）から不正に現金を引き出す犯罪が最もポピュラーであるが、その理由は、誰にでも容易に犯行の機会があるということに由来する。他人のキャッシュカードを拾得、窃取、詐取、横領などにより取得した者が、何らかの方法で暗証番号を知り現金を引き出すという形態が一般的である。(45)

これらの多くは、銀行など金融機関の設置するCD機から不正に現金を引き出す手口がほとんどであって、伝統的な財産犯罪と実質が異なるものではない。CD機からの不正な現金の引出し行為に窃盗罪の成立を認めるのが確立した判例である。CD機は、銀行など金融機関が設置・管理し稼働しているものであり、機器の中に収納されている現金の占有は金融機関にあるので、権限なくカードを用いて口座名義人の預金を引き出す行為は、他人（＝金融機関）の占有を侵害して財物を窃取したと評価される。(46)

なお、自己名義のカード悪用につき、「返済の意思がないのに、当初から不正に使用する目的でキャッシングサービスを受けられるクレジットカードの交付を受けて、これを使用し自動支払機から現金を引き出す行為は窃盗罪を構成する」としたものがある。(47)

以上のように、いわゆるCD犯罪については、窃盗罪の適用による処理に格別問題はなく、安定した法状況にあったといいうる。

（2）オンライン・システムの悪用と財産犯罪

これに対して、銀行など金融機関の内部の者によるオンライン・システム悪用の事案は、これも本質的には伝統的な財産犯罪の新しい手口といってよいものであるが、CD犯罪とは異なる性格を有するものとして現れた。金融機関

の職員など内部者が、オンライン・システムの端末から不正な操作を行い現金や財産上の利益を取得するこの形態の犯罪は、たとえば、銀行の行員が、あらかじめ用意した口座に宛てて架空の入金操作を行ない、後にそこから現金を引き出したり、振替を行ったりする態様で行われた。本稿Ⅱ―３―(1)でふれたように、三和銀行事件をはじめ、平和相互銀行事件、北浜クレジット事件、大阪サラ金事件など多数の事例がある[48]。

これ等の事例は、内部関係者――あるいは元内部者――によるものが多く、大きな被害にもかかわらず発覚しにくい密室犯罪であるという性格を持ち、中にはコンピュータに関する専門知識を駆使した巧妙な犯行という特徴を持つものもある。いずれも現金等を取得した時点では、窃盗・詐欺・横領等の財産犯罪に問うことのできるものではあるが、しかし、現金の引出し前の段階では、次のような問題点があった。

① 不正に端末を操作してデータを入力し、あらかじめ準備した口座（当時は架空名義の口座が比較的容易に開設できた）に架空の入金操作を行い、その口座残額を増加させたとしても、それだけでは窃盗にも詐欺にも問えなかった。現金（＝財物）が取り出されていない段階では窃盗罪にあたらず、また、一連の財産的事務処理が人の判断作用を介することなく機械によって行われている以上――機械は錯誤に陥ることはない――、詐欺罪の余地はなく、したがって二項詐欺でも捕捉できないからである[49]。

② 架空の入金が行われた口座から自動的に引落しが行われても（債務の弁済がなされ行為者が具体的に財産上の利益を得ていても）同様に依然として罪責を問うことが困難であった。

③ 引出された段階で窃盗罪に問う場合にも問題があった。たとえば、元々行為者の預金が一〇〇万円あった口座に、架空入金により一〇〇万円が増加し預金残高が二〇〇万円の状態となった後に一〇〇万円が引出された場合、

元々あった一〇〇万円と架空入金された一〇〇万円とは論理的に判別不可能であり、一〇〇万円の引き出しを「他人の物」を窃取したと評価するのは困難である。

このように、あきらかにその実質が窃盗、詐欺などの財産犯罪に等しい内実の不正行為であるにもかかわらず、現金の引き出しや財物の取得を待たなければ罪責を追及できない事態――処罰の間隙――が生じ、それが、後述する刑事立法を促す最も大きな動因となっていくのである。

3　コンピュータを利用する業務への加害行為など

(1)　コンピュータへの加害と業務妨害罪

コンピュータ・システムの普及がすすむにつれ、それが、さまざまな場面で人の業務に用いられることも増えて行った。コンピュータは、すでに見たように、家庭で、趣味やプライベートな用途等に幅広く利用されるようになる今日の状況に先だって、まずは研究所など専門家による利用や、一部の企業活動における利用が行われたことから、むしろ業務に用いられる場面が先行したともいえる。そして、種々の業務におけるコンピュータの重要度がますます高まっていくにともない、業務に用いられているコンピュータへの加害行為をどのように捉えるべきかということが重要な課題として意識されるようになった。

すなわち、人の業務用のコンピュータへの加害行為により業務が妨害された場合、業務妨害罪（刑法二三三条・同二三四条）の適用が検討されることとなる。ここにいう「業務」とは、精神的であると経済的であるとを問わず、広く職業その他、社会生活上の地位に基づき継続的に行われる事務または事業を意味するものとされる[50]ところから、そのような業務に使用中のコンピュータに向けられた加害行為は、同罪を構成する可能性があることになる。

しかし、業務妨害罪は、「虚偽の風説の流布」、「偽計」、「威力」を実行行為として規定しているが、そのいずれもが、人の意思・判断作用に働きかけて妨害を行うことを念頭においており――判例実務上相当程度拡張的に把握されているとはいえ[51]――、コンピュータ・システムに直接加えられる物理的破壊や動作阻害を捉えることは難しかったのである。「威力」業務妨害にも、「偽計」業務妨害にも問えない場合が生じるからである。社会生活のコンピュータ・システムへの依存度の高まりや、加害行為が重要な社会のインフラを直撃しかねない事態も想定される以上、コンピュータを用いた業務のより適切な保護が大きな課題となっていったのである[52]。

（2）コンピュータの無権限使用・不正アクセス

研究機関や企業の所有する運転コストの高額なコンピュータ・システムを、無断で不正に使用する行為は、比較的はやい時期に現れている。次のようなものがある。

①一九八〇年五月、マイコン・ショップの従業員が、岡山大学の助教授の同大学計算センター登録番号（ＩＤ）とパスワードを入手し、これを用いて数カ月の間、のべ四五時間にわたり電話回線経由で同センターのコンピュータにアクセスし無断で使用していた（使用料約一六万円）ことが発覚した。②一九八一年八月、某公団職員らが、全国高等学校野球選手権大会の試合に関して、現金合計一六万円余りを賭けて、いわゆる「野球トトカルチョ」と称する賭博を行い、その際、賭け金の計算処理を行う特別のプログラムを作成した上、同公団のコンピュータを不正に使用していたことが発覚した。いずれも、コンピュータの不正使用については適用条文を欠くため立件されなかった[53]。

このような利用権限のない者によるコンピュータの不正使用――マシン・タイムの盗用とも呼ばれる――は、一台のコンピュータを並行して同時に複数のユーザが利用できるタイム・シェアリング処理を用いて、本来の業務で稼働

中の運転コストの高額なシステムを、不正に対価を支払わずに使用することとなる点で、ある種の「利益窃盗」とみることができる。そのため、発覚した事案のような大型のコンピュータでなくとも、勤務先のコンピュータを私的な目的で使用したり、外部から電話回線等を介して接続して使用したりする行為も含めて、処罰するためのいかなる刑罰法令も存在しなかったのである。しかし、この「無権限使用」の問題性は、他人の所有するコンピュータという重要な「資源」を無断で利用することに重点があるのではなく、利用するために無断でシステムに侵入するという側面にあったというべきであろう(54)。

すなわち、上のコンピュータの無権限使用や、データの不正入手、データ・プログラムの消去や改ざんなど多くの不正行為は、コンピュータ・システムへの不正な侵入（無権限のアクセス）を手段に行われるのであるから、犯罪化の要否が検討されなければならないのは、ハッキングなどの不正なアクセス行為ということになる。一九八五年、わが国では電気通信事業の自由化が行なわれたが、この通信の自由化がハッカーを生む土壌となるということが早くから指摘されていた(55)。公衆通信回線を経由するなどして不正に他人のシステムに侵入し、データやプログラムを盗み見たり、破壊・消去・改変などを行ない個人情報や企業秘密、行政機関の情報、さらに国家の防衛に関する秘密情報を侵害したり、あるいは、システムに致命的なダメージを与えるなどの事態もありうるのである。

この時期のわが国の実例としては、①ＫＤＤ（当時の国際電信電話公社）の国際公衆データ伝送サービスの契約利用者（企業や公立の研究機関）のシステムが、海外から不正侵入され、ファイルに落書きされる等の被害を受けた事例(56)、②筑波学園研究都市の文部省高エネルギー物理学研究所のコンピュータ・システムが、ＫＤＤの国際通信回線を介して西ドイツから不正侵入された事例(57)、また、実害が生じたものとして、③大阪工業大学のコンピュータ・システムの

磁気ディスク中に収納された研究用数値プログラム、学生の成績・入試処理プログラム等二五〇〇件の最重要データが、何者かが何らかの方法で入手したパスワードを用いて学内の端末からシステムに侵入し消去プログラムを打込むという手口で消去したという事例がある[58]。[59]

これらの不正侵入事案は、いずれも刑事責任の追及は行われていない。重要データの消去という実害を生じた③の事案も、毀棄罪適用による訴追は全く不可能ではなかったと思われるが、法的責任を含め追及は断念されている[60]。

その後、わが国においては、多くの有力な刑法学者をメンバーとする「情報セキュリティと法制度調査研究委員会」によって、コンピュータ・システム侵害行為に関する検討が行われ、積極的な立法提言を含む検討結果「コンピュータによる情報処理システムへの加害行為に関する刑事法的対応」が明らかにされる[61]など、不正アクセス等の刑事規制に向けた動きがみられるようになって行くのである。

(29)　たとえば、旧刑法下に、電気の利用普及という技術革新にともなって、従来想定されていなかった電気盗用の事案が現れたが、最初は「管理可能性」を用いた拡張的法解釈による解決が図られ（大判明三六・五・二一刑録九輯八七四頁）、後に立法的解決が行われた――現行刑法制定時に電気を「財物とみなす」二四五条が設けられた――経緯がある。

(30)　大判明四三・九・三〇刑録一六輯一五七二頁。学説も、「文字その他の符号によって意思または観念を表示した物」（団藤重光『刑法綱要第三版』創文社（一九九〇）二七一頁）とするのが通説である。なお、「①媒体の上に可視的・可読的な状態で固定された、人の意思・観念の表示であって、②意思・観念の表示の主体である作成名義人が認識可能なものをいう」とする山口教授は、「作成名義人の認識可能性の要件が付加されるのは…文書が証拠として保護されることに由来する」とされる（山口厚『刑法各論（第二版）』有斐閣（二〇一〇）四三〇頁）。

(31)　大阪地判昭五七・九・九判例時報一〇六七号一五九頁。

(32)　最決昭五八・一一・二四刑集三九巻九号一五三八頁。

(33)　積極の見解を支持する学説も、カード券面上の可視的表示部分と一体的に観察すれば作成名義は明らかであることをあげて、このような行為に私文書偽造罪を肯定することにはそれほど問題はない、としている（板倉宏「キャッシュカードと私文書偽造罪――大阪地裁九月九日判決をめぐって――」法律のひろば三五巻一二号二五頁（一九八二））。ほぼ同様にこの判決を支持する見解として、戸田信久「キャッシュカードの改ざんに対し有印私文書偽造罪の成立が肯定された事例」研修四一三号（一九八二）四七頁以下。

(34)　但木敬一「キャッシュカードと文書偽造罪の成否」研修四〇八号五五頁。

(35)　名古屋高裁金沢支判昭五二・一・二七判例時報八五二号一二六頁（その評釈として、宮澤浩一「自動車登録ファイル（電磁的記録物）は刑法一五七条一項の『公正証書の原本』か」判例評論二三二号（一九七八）一五六頁以下。）、広島高判昭五三・九・二九判例時報九一三号一一九頁。なお、自動車登録ファイルが公正証書の原本にあたるとした最初の判決（そしてまた、電磁的記録の文書性を肯定した最初の判決）は、福岡地裁久留米支判昭四九・一二・四（判例集未登載）とされる（原田國男「コンピュータ磁気テープの文書性」研修三三二号六七頁）。

(36)　板倉「キャッシュカードと私文書偽造罪」前掲（註(33)）二七頁。なお、吉田淳一「自動車登録ファイルは公正証書原本か」警察學論集三〇巻一二号（一九七七）一七四頁は、消極的見解に立ち、「やはり本来立法的解決を要すべき事柄であるように思われるといわざるを得ない」とする。

(37)　積極の結論を支持する学説も、谷口補足意見が、自動車登録に関する法令の改正（従来の自動車登録原簿から自動車登録ファイルへと変更したもの）により刑法の構成要件が補足修正されたとの理論構成を、「窮余とはいえ巧妙な説明」とし、多数意見が公正証書の原本にあたることは認めながら、その文書性について格別の判断を示していないことも「意味深長というべき」と評している（団藤『刑法綱要第三版』前掲（註(30)）二九八―二九九頁）。

(38)　東京地判平一・八・八判時一三一九号一五八頁など。

(39) 千葉地判平一・一一・二判例時報一三三二号一五〇頁。この点につき、後に最高裁は、テレホンカードを刑法上の有価証券と認める積極判断を示し、争いに終止符を打っている（最決平成三・四・五判例時報一三八三号一一八頁）。

(40) 改ざんテレホンカードの問題について、詳しくは、拙稿「いわゆる改ざんテレホンカードと変造有価証券交付罪の成否」法学紀要三二巻三九七頁以下（一九九〇）参照。

(41) コンピュータ犯罪の事案を詳細に紹介した当時の論稿によれば、アメリカなど海外の事例として、保険会社のコンピュータ担当職員が会社の重要な磁気テープの中身を消すなどして二三億円余りの損害を生じさせた例や、会社の従業員が磁石を使って磁気テープのエラーチェック・コードを消去した事例、磁気テープを先のとがった道具で突いて使用不能にした、などの実例が紹介されているが、わが国の実例はあげられていない（人見「コンピュータ犯罪の発生状況」前掲（註(17)）一〇頁以下）。

(42) コンピュータ犯罪を早い時期に扱った論稿のなかにも、磁気記録の消去行為を文書毀棄や器物損壊に問うことができるかを詳細に論じたものがみられる（西原「コンピュータの導入と刑事法上の諸問題」前掲（註(10)）三六頁）。

(43) 板倉「コンピュータ犯罪と刑法」前掲（註(13)）一〇二頁。

(44) 廣畑史朗「コンピュータ犯罪と刑法の適用」警察學論集三五巻一一号五四頁（一九八二）。

(45) 今日でも、このような単純な手口のCD犯罪は、クレジットカード不正使用と並び、カード犯罪の大半を占めているとされる（警察庁編『平成二三年版警察白書』七五頁）。

(46) 窃取した他人名義のキャッシュカードを用いて銀行のCD機から現金を引き出した事案につき、「カードを利用した現金の窃盗罪が成立し、銀行がカードの名義人に対して免責を受けることがあるとしても同罪の成立を妨げるものではない」とした裁判例がある（東京高判昭五五・三・三刑裁月報一二巻三号六七頁）。

(47) 高松高判昭六〇・五・三〇高検速報四二六号。

(48) 人見「コンピュータ犯罪の発生状況」前掲（註(17)）九頁、小林道男「コンピュータ犯罪防止対策」警察学論集三五巻一一号六四頁以下（一九八二）、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（注釈）改定増補版』成

文堂二九頁以下（一九八九）参照。

(49) 実際に、前述の三和銀行事件では、犯人は数回にわたり計一億八〇〇〇万円の架空振替入金操作を行って架空口座にその金額を記帳させたが、罪責を問われたのは、最終的に手にした現金、保証小切手計一億三〇〇〇万円分にとどまっている（人見「コンピュータ犯罪の発生状況」前掲（註(17)）三一頁）。

(50) 大判大一〇・一〇・二四刑録二七輯六四三頁。学説上もこれを承認する見解が通説といってよい（団藤『刑法綱要第三版』前掲（註(2)）五三五頁、前田雅英『刑法各論講義（第四版）』東京大学出版会（二〇〇七）一六五頁、山口『刑法各論（第二版）』前掲（註(30)）一五五―一五六頁など）。

(51) 山口『刑法各論（第二版）』前掲（註(30)）は、虚偽の風説の流布・偽計・威力は、「本来、人の意思を介した妨害手段を意味すると解されるが、…判例により拡張され、端的な業務妨害までが捕捉されるに至って」おり、「妨害の態様として、犯罪成立を限定する意義は極めて薄れているのが実情である。」とされる（同書一六二頁以下）。

(52) なお、この業務妨害に関連して、コンピュータ・ウィルスの問題が後に重要なテーマとなるが、昭和六二年改正前のこの時期には問題とされておらず、立法課題とはされていない。

(53) 人見「コンピュータ犯罪の発生状況」前掲（註(17)）三五頁。なお、同論文に、海外のさまざまな不正使用事案の紹介がある（同二三頁以下）。

(54) 対価を払わずに他人の物を権限なく使用する行為一般を犯罪化する必要がないことはいうまでもない。たとえば、勤務先会社の機器を用いた仕事中の私用電話やファクシミリなどは、内部的ルール等に委ねられることで十分規律しうるのである。

(55) この時期、コンピュータ犯罪の将来について、原田「コンピュータ犯罪に関する研究動向」前掲（註(24)）九一頁は、通信回線自由化にともないデータ通信利用機会が増加することに加え、憂慮すべき点として、パーソナル・コンピュータ普及による「ハッカー予備軍」急増の点をあげていた。

(56) 一九八六年二月二四日付毎日新聞。

(57) 一九八六年二月三日付毎日新聞。

(58)　一九八四年七月二七日付毎日新聞。

(59)　以上のコンピュータへの不正侵入等の実例については、それらを詳細に紹介する、室伏哲郎『コンピュータ犯罪戦争――日本のネットワーク犯罪・攻防最前線――』サンマーク出版（一九八七）を参照。

(60)　室伏『コンピュータ犯罪戦争』前掲（註(59)）一〇二頁以下。

(61)　日本情報処理開発協会『コンピュータによる情報処理システムへの加害行為に関する刑事法的対応』（一九九〇）。なお、これを紹介する記事として、「システム侵害罪立法化の動き」経営法務一七九号二二頁以下（一九九一）。