

IT革命とコンピュータ関連犯罪

石 堂 功 卓

1 はじめに

- ① ハイテク犯罪の現状
 - ② 匿名性と刑罰抑止力の低下
 - ③ 被害の即時性と甚大性
 - ④ 犯罪の曖昧性と刑法理論
- ## 2 名誉毀損罪との関連
- ① 名誉毀損罪とインターネット

3 わいせつ犯罪との関連

- ② 法益概念の相対性
 - ③ 公然性―伝播可能性
 - ④ 被害者の特定とハンドル名
 - ⑤ リンクの態様
- ① ネットワーク利用のわいせつ犯罪の性質
 - ② 規制の必要性

- ③ わいせつ物の特定
 - ④ マスクの問題
 - ⑤ 公然陳列の意義
- 4 電子商取引との関連
- ① インターネット詐欺
 - ② 「なりすまし」の問題
 - ③ 不正アクセス行為の禁止等に関する法律
- 5 プロバイダーの刑事責任
- ① 自ら提供する違法コンテンツ
 - ② ユーザーの違法コンテンツ
 - ③ 不作為の共犯
 - ④ 風俗営業等の規則及び業務の適正化等に関する法律
- 6 まとめ

1 はじめに

いわゆるIT革命は、コンピュータ関連犯罪に様々な影響を及ぼすものと考えられている。コンピュータおよび情報技術を利用したいわゆる「ハイテク犯罪」の検挙件数だけを見ても、平成五年に三二件であったものが、平成一〇年には四一五件となり、爆発的な増加をみせている(警察白書平成一一年版)¹⁾。このようにいわゆるハイテク犯罪の増加の要因としては、パ

ソコン一台があれば、容易にインターネットに接続でき、しかも違法行為者の識別がIDとパスワードだけで行われるため、それを盗用すれば他人になりすますことが極めて簡単にできることになることが指摘されている。すなわち、犯罪を行う者の特定が困難である点が、逆に犯罪を行いやすくしているという皮肉な状況がある。ここでは、刑罰による抑止力は、通常の犯罪と比較して、当然低下することが予想されるのである。

さらに、ハイテク犯罪では、たとえば、プロバイダーのシステムの一瞬の破壊あるいは、銀行のシステムに不正に侵入して、金銭を自分の口座に一瞬にして振り込んでしまうなど、その被害の甚大性と即時性が指摘されている。最近においても、中央官庁のホームページが改ざんされたり、いわゆる「I LOVE YOU ウイルス」が世界的な被害をもたらしたり、ハイテク犯罪はサイバー・テロともいえる性格を有し、極めて深刻な問題を提起している²⁾。

このような状況において、刑事法としてどのような対応をとるべきかについては、現在まで十分な分析・検討が行われていない。しかしながら、従来の伝統的な犯罪に比較すると、ハイテク犯罪においては、犯罪の輪郭が曖昧であるし(特に法益が何かについては深刻な問題がある)、インターネットを介した犯罪のグローバル化や、いわゆる電子商取引の急激な拡大を考慮すると、はたしてこれまでの刑法理論がそれに対応できるのかが憂慮されるのである。

こうして、コンピュータを利用したハイテク犯罪は、現在、刑事法上重大な問題提起をしているのであり、特にネットワーク利用犯罪については、その犯罪内容の急激な変質が予想されるのである。したがって、本稿では、現在ハイテク犯罪として認知されている犯罪の解釈論的な問題点を指摘するとともに、今後の研究の一里塚としたい。

2 名誉毀損罪との関連

「公然と事実を摘示し」て、人の名誉を毀損することが、名誉毀損罪の構成要件であるが、インターネット上の名誉毀損罪の成否についてもその成立要件が修正を余儀なくされるようなことはないと思われる。しかしながら、なお、若干の問題点が指摘される。つまり、通常の名誉毀損行為においては、その伝達手段の制約から、法益侵害がそれほど大きくないものでも、ネットを利用した同種行為が、思いの外甚大な被害を惹起するケースが少なくないということがある。したがって、伝統的な名誉毀損罪の解釈では、法益侵害性のないものが、ネットを介した名誉毀損においては、可罰性が肯定される可能性が出てくるのである。これには法益概念の相対性を認める必要があるが、名誉毀損の他の成立要件との関係上、一概に否定はできないであろう。

ネット上の名誉毀損について、「公然性」の要件は緩和される可能性が大いにありうることである。判例によれば、公然性

は「伝播可能性」を基礎にして判断されるものと思われるが、インターネットにおける「伝播可能性」は極めて大きく、ホームページや掲示板への掲載ばかりでなく、メールリングリスト利用の場合にも当然「公然性」は肯定されることになるであろう。このような要件の緩和は、ネット上の名誉毀損行為の法益侵害性の大きさと密接な関係にあるが、処罰範囲を無限定にしないためには、「伝播可能性」概念の見直しが必要になるものと思われる。

また、ネット上においては、被害者がハンドル名で登場し、実名の不明であるケースがよくある。名誉毀損罪においては、被害者の特定されることが要件としてあげられるが、ハンドル名による名誉毀損がこの要件を満たしているかどうかはかなり難しい。しかし、およそ誰の名誉を毀損しているかわからないという意味での「匿名性」を問題とするなら、つまり、ネット上のハンドル名をもつ「その人」の名誉を毀損していると判断されるなら、被害者の特定の要件はクリアされているといえるであろう。

名誉毀損罪との関係では、この他、リンクを張る行為がどのように評価されるかが問題となる。たとえば、名誉毀損と評価されるホームページへのリンクを張ったとしても、そこに名誉毀損となる記述が直接書かれているわけではないという点を重視すれば無罪説もありうるのである。しかし、ホームページの構造自体が階層を成していることからすれば、リンクを張るこ

とは、名誉毀損行為の故意があるならば、自分のホームページにその情報を掲載するのとそれほど異なるものとはいえないのである。リンクを張る行為が名誉毀損情報の閲覧のみを目的とするなら、名誉毀損罪の成立を妨げる事情はないといえよう。もっとも、それが正犯か従犯かという問題はなお残されているといわなければならない。ケース・バイ・ケースで判断しなければならぬ問題である。

3 わいせつ犯罪との関連

平成十一年において、ハイテク犯罪の中で最も検挙件数の多い犯罪がわいせつ物頒布等の犯罪で、ネットワークを利用した犯罪の中でも群を抜いて多く、二四七件中一四七件にも上っている(警察白書一一年版)³⁾。そして、このような犯罪については刑法一七五条のわいせつ物公然陳列罪の適用を認めるのが判例・通説の立場であると理解されているわけである。もっとも、インターネットの特質から、わいせつ物の規制の緩やかな外国からのわいせつ画像の流入を阻止できない以上、国内の規制を強化しても意味がないとの議論も少なくない。しかしながら、これは犯罪の多発は規制を不要にするという不合理な主張につながりかねないので、採用するわけにはいかない。わいせつ罪の規制自体を我々が放棄すべきであるとの主張をするならばともかく、現行法解釈において、サイバー・ポルノを従来のわいせつ犯罪の枠組みから外すことはできないと考えるのである。イ

ンターネットが大衆化した現在、通信の秘密からの規制緩和論ももはや説得力を欠くといえるであろう。

ところで、解釈論として問題となるのは、まず、デジタル画像が保存されたサーバー・コンピュータ全体を「わいせつ物」とすることの正当性であろう。すでに判例は、映画フィルムや録音テープ自体がわいせつ物であることを認めているので、たとえば、写真や絵のような可視性を要求することは現実的ではないと考えるのである。したがって、サーバー・コンピュータに蓄積されたわいせつ画像といえども、それを各人が自分のコンピュータにダウンロードしてディスプレイに再生することが簡単にできるようになった現在、わいせつ物の特定は十分可能であるといえよう。しかしながら、画像情報自体をわいせつ物と認めることはできないのであって、「物」概念をサイバー・ポルノに限って無限定にする根拠はみあたらない。その意味で、罪刑法定主義の要請は、IT革命の超えることができない壁であるということもできるであろう。

なお、わいせつ画像をマスク処理した上で、インターネットに流したとしても、マスクはずしが容易に行われるならば、わいせつ物としての特性が失われるわけではなく、わいせつ物罪の成立に何ら妨げとなるものではない。ところで、刑法一七五条の解釈論として、さらに「公然陳列」が問題となるといわなければならない。公然陳列とは、「不特定多数の者がその画像内容を見ることができるようになること」を意味し、かつそれ

で足りると解すべきである。⁽⁴⁾したがって、現実に見ることまでは必要としない。閲覧までを要件とすると、法が陳列を犯罪としたことの意味がなくなるし、抽象的危険犯としての本罪の性格を考慮すれば、サーバー・コンピュータにわけせつ画像をアップロードした段階で、既遂となると考えられる。また、これは、たとえば、海外のサーバーに画像をアップロードした場合でも、不特定多数の者が閲覧・認識できるように状態にしたことが実行行為であるとすると、それは国内で行われた犯罪であり、国外犯の問題は生じないということになるのである。

4 電子商取引との関連

周知のごとく、世界的な視野で注目されているのは、インターネットを介した電子商取引の問題である。この問題は、経済構造を変えかねない電子商取引といえるのであって、今後、爆発的な発展をするものと思われるが、それと同時にそれに対応した法的整備の必要性も叫ばれているところである。ここでは、犯罪として規制すべきものを、断片的にはあるが、とりあげることとする。

まず、インターネットを利用した詐欺についてである。これが手段としてインターネットを利用しただけの、本質において人を欺罔するという伝統的な形態の詐欺であるならば、刑法二四六条の詐欺罪が成立することに問題はないといえる。しかし、たとえば、電話回線を利用して、銀行のシステムに不法に侵入

し、虚偽の情報を与え、振込送金させるような場合には、人の欺罔がない以上、刑法二四六条の二の電子計算機使用詐欺罪が適用されることとなる。このような場合には、実質的に財産移転があるわけで、電子計算機使用詐欺罪の成立にそれほど大きな問題は生じないが、たとえば、同様の方法で、有償の情報等を不正に得たというような場合には、問題が生じることとなる。電子計算機使用詐欺罪においても、情報そのものが保護の対象となるものではないからである。したがって、学説においては、正当な契約者のIDやパスワードを不正使用する不正アクセスによって情報等を得ることにより、正当な契約者の課金ファイルの結果として改ざんする点を基礎にして、電子計算機使用詐欺罪の成立を認めようとするのである。つまり、自己の課金ファイルが本来作成されなければならないところ、それを不正に作成しなかったことにより、支払いを免れたと評価されることになるからである。

上述のようなネットワーク利用詐欺は、多くの場合、インターネットの匿名性という特質を利用して、いわゆる「なりすまし」を行うものである。このような「なりすまし」は、架空名義の作成であろうと、他人名義の冒用であろうと、一定の情報をそれによって送信する場合には、刑法一六一条の二の電磁的記録不正作出・同供用罪が問題となる。たとえば、架空あるいは他人名義のメールアドレスを不正に獲得し、それを利用して電子メールで契約の申し込みをする場合や、電子商取引の決済にお

いて、それを他人のクレジットカード番号の送信によって行う場合などが考えられる。学説には、インターネットにおいては、正しいコンピュータ操作をしない限り、常に誤ったログ記録の作成が行われる以上、かなり広い範囲で電磁的記録不正作犯罪が成立する可能性を認める者もいるけれども、本罪は「人の事務処理を誤らせる目的」を要する目的犯であるばかりか、単なる形式犯ではないことを認めることによって、合理的な処罰は可能となるであろう。

なお、このような「なりすまし」は、電子取引のみならず、他の様々なインターネット上の犯罪を助長するおそれがある。そこで、平成一二(二〇〇〇)年二月に施行された「不正アクセス行為の禁止等に関する法律」により、「なりすまし」自体が処罰されることになったのである。すなわち、他人のIDおよびパスワードを不正使用してアクセスした場合を、独立して処罰するのである。この処罰自体は、国民の納得を得られるし、犯罪を促進する環境をできるだけ排除するための有効な方策ともいえよう。しかしながら、その保護対象が何であるのかについてはなお若干の問題が残るところである。つまり、不法侵入と同様の個人法益的な性格ととらえるのか、それとも、健全なネットワークを保護する公共危険的な性格のものと考えるのが明確とは言えないのである。処罰範囲を曖昧にしないためには個人法益関係的に構成する他ないと思われるのであるが、ネットワークという輪郭の曖昧なものが客体である以上、ある

程度の抽象化はやむを得ないという外ないであろう。今後の検討課題となるところである。

5 プロバイダーの刑事責任

インターネット利用には、プロバイダーが介入することは周知の事実である。したがって、ユーザーが様々な不正行為を行う際には、プロバイダー等の責任が問題となるのはむしろ当然である。特に、プロバイダーが単なる仲介者以上の役割を当該犯罪において果たしていない場合が問題となると考えるのである。プロバイダーが自ら違法なコンテンツを情報提供しているような場合には、当然に刑事責任を問われるのであるが、ユーザーがそのプロバイダーにアップロードしたホームページにおいて、違法行為を行う場合、なおプロバイダーに刑事責任が認められるのかは、かなり問題となるところがある。たとえば、電話によって脅迫行為を行う場合、NTTにその共犯行為があったとはいえないのと同様に、プロバイダーの責任をストレートに認めることはできない。もっとも、プロバイダーがその違法コンテンツの内容を認識しており、あえて削除などの措置を講じていない場合に、不作為による共犯の成立を完全に否定できるかという点、これにも若干の疑問が残るといわざるをえない。プロバイダーの犯罪関与の程度問題と不作為犯における保障人的地位の問題とが複雑に絡み合う問題がそこに介入するように思えてならない。ただし、わいせつ画像については、一九九八

年に改正された「風俗営業等の規則及び業務の適正化等に関する法律」により、「映像送信型性風俗特殊営業」に関して、わいせつ画像のアップロードについて、その送信防止のための措置を講ずることになっているため、これを根拠にして保障人的地位を肯定しやすくなったとはいえるであろう。むしろ、新聞倫理綱領などにならって、「プロバイダー倫理綱領」を新しく策定する方がベターであると提言したいのである。

6 まとめ(今後の課題)

本稿では、極めて限定的な範囲ながら、IT革命によってもたらされる刑事法的な問題を、コンピュータ関連犯罪を中心に、その解釈論的視点より若干考察・検討を加えてみた。この種の問題については、むしろ立法論的アプローチが必要であることも多いかと思われる。しかし、現在もネットワークはどんどん発展しつつあり、非常に流動的な状況が存在する。そのような状況の中では、ひとまず犯罪となるものとならないものの限界を慎重に見極めることがより重要であるとの指摘をして、本稿の結びとした⁵⁾。

なお、ここで取り上げた問題以外に「電子計算機損壊等業務妨害罪、電子計算機使用詐欺罪、電磁的記録毀棄罪」などの関連問題があるけれども、これらの検討については他日を期したいと考えている。

注

(1) 犯罪白書平成一二年版二四六頁は、コンピュータ関連犯罪の検察庁新規受理人員が、平成一一年末で総計四六一名にも、のぼっていることを報じている。なお、関聡司「ハイテク犯罪の現状と対策」(法律のひろば二〇〇〇年六月号)参照。

(2) 犯罪白書平成一二年版二四九頁によれば、こうしたハイテク犯罪への対応策として、二〇〇〇年五月主要国政府・産業界関係者によるハイテク犯罪対策合同会議が開催されたことも明らかにしている。

(3) こうした動きに対応して、平成一一年五月には、「児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律(平成一一年法律第五二号)」が制定され、インターネットを利用して不特定又は多数の者に対し児童ポルノを閲覧させる行為を含む児童ポルノの公然陳列に関する処罰規定が設けられたことは、周知の事実である。

(4) 拙著、現代刑事判例研究第一巻(成文堂)一七六頁以下の説明に詳しい。

(5) O・E・C・D・レポートでは、国際間にまたがるコンピュータ関連犯罪が多発することを予想し、それらの犯罪に対応するためには、国際的な協調体制の確立の必要性をいち早く打ち出しており、今やその具体的な方策がツメの段階を迎えている。わが国で開催された二〇〇〇年七月の九州・沖縄サミットにおいて、犯罪のない安全なサイバー空間を強化するため、関係国が協調することと、二〇〇一年第二回政府・産業界合同会議の開催が決定され、さらに、「グローバルな情報社会に関する沖縄憲章」(IT憲章)が

採択されたことは、この間の事情を物語る動きとして、特
記されてよいであろう。