●論文●

最近のサイバー犯罪

園田　寿
（甲南大学法科大学院教授）

一　はじめに

コンピュータを悪用した違法行為はますます増加傾向にあるが、犯罪の道具としてのコンピュータは、すでに一九六〇年代頃から問題となっている。しかし、キャッシュカードと情報処理システムをターゲットとして、とくに銀行の金融システムが狙われた七〇年代から八〇年代までは、コンピュータ犯罪といえばかなり高度な知識と技術を要する、いわばプロによる特殊な犯罪の部類に属した。ところが、九〇年代の終わりにインターネットが大ブレイクし、コンピュータの操作もますます簡単になり、インターネットの接続環境がダイアルアップから常時接続に移行するに伴い、ネット空間で生じるサイバー犯罪についても質的な変化が見られるようになった。かつてのように特殊な専門的技術を必要としないふつうの詐欺や名誉毀損、個人情報の漏えい、わいせつ情報など、むしろ古典的な犯罪が多くなっている。インターネットがもはや現代の生活にとってなくてはならない必需のメディアになった証拠だと思う。

平成一六年度におけるサイバー犯罪の検挙件数は二、〇八一件で、前年と比べ約一三％の増加であり、平成一二年と比べて二倍以上となっている（**表1**）。中でも犯罪の遂行にあたりネットワークを不可欠な手段として利用した「ネットワーク利用犯罪」は一、八八四件で検挙件数の約九一％を占めている。また、都道府県警察のサイバー犯罪相談窓口等が平成一六年度に受理した相談受理件数（**表2**）

表1　サイバー犯罪の検挙状況

罪名＼年	H12	H13	H14	H15	H16	増減
不正アクセス禁止法違反	67	67	105	145	142	−3（−2.0%）
コンピュータ・電磁的記録対象犯罪	44	63	30	55	55	±0（±0.0%）
電子計算機使用詐欺	33	48	18	34	42	+8（+23.5%）
電磁的記録不正作出・毀棄	9	11	8	12	8	−4（−33.0%）
電子計算機損壊等業務妨害	2	4	4	9	5	−4（−44.4%）
ネットワーク利用犯罪	802	1,209	1,471	1,649	1,884	+235（+14.3%）
詐欺	306	485	514	521	542	+21（4.0%）
児童買春・児童ポルノ法違反 児童買春	8	117	268	269	370	+101（+37.5%）
児童買春・児童ポルノ法違反 児童ポルノ	113	128	140	102	85	−17（−16.7%）
著作権法違反	80	86	66	87	174	+87（+100.0%）
青少年保護育成条例違反	2	10	70	120	136	+16（+13.3%）
わいせつ物頒布等	154	103	109	113	121	+8（+7.1%）
脅迫	17	40	33	38	58	+20（+52.6%）
名誉毀損	30	42	27	46	26	−20（−43.5%）
その他	92	198	244	353	372	+19（+5.4%）
合計	913	1,339	1,606	1,849	2,081	+232（+12.5%）

表2　サイバー犯罪等に関する相談状況

区分＼年	H12	H13	H14	H15	H16	増減
詐欺・悪質商法に関する相談（インターネット・オークション関係を除く）	1,396	1,963	3,193	20,738	35,329	+14,591（+70.4%）
インターネット・オークションに関する相談	1,301	2,099	3,978	5,999	13,535	+7,536（+125.6%）
違法・有害情報に関する相談	2,896	3,282	2,261	4,225	4,157	68（−1.6%）
迷惑メールに関する相談	1,352	2,647	2,130	2,329	3,946	+1,617（+69.4%）
名誉毀損、誹謗中傷等に関する相談	1,884	2,267	2,566	2,619	3,685	+1,066（+40.7%）
不正アクセス・コンピュータウイルスに関する相談	505	1,335	1,246	1,147	2,160	+1,013（+88.3%）
その他	1,801	3,684	3,955	4,697	7,802	+3,105（+66.1%）
合計	11,135	17,277	19,329	41,754	70,614	+28,860（+69.1%）

出典：http://www.npa.go.jp/cyber/statics/h16/h16_22.html

（平成17年２月24日付け、警察庁広報資料による）

は、七〇、六一四件で、前年に比べ約一・七倍の増加であり、平成一二年と比べると六倍以上に急増している。内訳としては、詐欺や悪徳商法、インターネット・オークションに関する相談が全体の約七割を占めている。

以下では、ネットワーク利用犯罪の中でも、とくに学生が被害にあいやすい犯罪行為について、その問題と対策について述べたいと思う。なお、ネット空間では、法的な整備が必ずしも十分とはいえない部分があり、適法行為と違法行為の境界があいまいなものも多い。そのような場面では、犯罪の被害者だけではなく、法違反の明確な意識なしに違法な領域に踏み込んでしまい、犯罪の加害者になっている場合もあることに注意しなければならない。意図せずに加害者となり、結果的に被害者から損害賠償責任を追及されたり、最悪の場合には刑罰に処せられたりすることも、ネットワークの落とし穴に落ちてしまった結果といえるだろう。

二　ネット利用詐欺にあわないために

（一）オークション詐欺

インターネット上で販売者と購買者の取引を仲介し、電子商取引を促進させるネットオークションが急成長している。出品者は、オークションサイトに商品情報・最低落札価格・発送方法などを提示して商品をセリに出し、それにもっとも高い値段をつけた者が落札する。誰でも簡単に参加できる手軽さと、希少価値のある品物が見つかることもあり大人気となったが、ネット取引では相手の顔が見えないというネットの匿名性と参加者に対する個人認証の甘さを突かれた詐欺事犯が続出している。

商品を落札すれば、出品者と落札者との間でメールなどで具体的な交渉が開始される。企業対個人の場合は、代引きや後払いといった安全な決済方法があるが、個人対個人の場合は、まず代金を指定された口座に振り込むのが通常である。その場合、相手のメールアドレスが無料アドレス、携帯電話番号も契約者不在の番号（しかもその振込先が架空名義の口座）であれば、詐欺の被害にあう可能性が高い。

一個の商品を複数の者に売ったり、存在しない商品をセリにかけたり、偽ブランド品を本物と偽って代金を振り込ませるといった手口が多数報告されている。また、掲載された商品の写真が実物と異なっていたために後日トラブルになったり、出品者自らが別のＩＤで入札者に成りすまし、金額をみずから吊り上げるといったケースもある。

このようなネット詐欺師のカモにならないためにはどうすればよいか。現実社会と同様、詐欺師の甘い言葉に乗らない姿勢が基本だ。代金振込みの前に、相手の住所・自宅の電話番号・メールアドレスを確認し、商品について詳しく確認する。応対に不審を感じれば乗らないこと。何よりも個人認証が強化されているオークションサイトなら一応信頼はできる。さらに最近では、出品者と落札者を仲介し、代金の振込み・支払い・商品の発送などを代行するエスクローサービス業者と提携するオークションサイトもある。もちろん、その場合には手数料が必要となるが、詐欺の被害にあわないためには高くはない保険料といえるだろう。

（二）架空請求詐欺

最近増えているのが「架空請求」や「不当請求」事案である。

実際に利用した事実がないにもかかわらず、何らかの有料サービスを利用したか、あるいは有料サイトの会員登録を行ったといったような内容のメールを送り付け、料金を振り込ませようとする手口である。金額も面倒なトラブルの処理を考えればそれほど高い金額ではなく、またあやしげな「債権回収業者」に料金の請求を委ねたといったように、メールを受け取った者の恐怖心を煽ったりする悪質なケースも多い。

実際に当該ホームページを訪れ、事実上何らかのサービスを受けたような場合には、法的には契約が成立するようなケースがないわけではない（ボタンをクリックすると国際電話に架電すると小さく書かれてあり、そのボタンを不用意にクリックしたために、後日国際電話料金の請求が来たというケースもある）。しかし、ほとんどの場合は、契約じたいが成立しておらず、請求じたいが不当となるので、あくまでも冷静に対処することが必要となる。

絶対にしてはならないことは、慌てて請求先にこちらから問い合わせることである。問い合わせることで、逆に不当請求者にこちらの電話番号、メールアドレス、住所、氏名等の個人情報を開示することになり、その結果、今度はそれが悪用されて恐喝の被害に発展することがある。また、まれに裁判所から本物の書類が郵送されてくるケースもある。このような場合、その書類を無視すると民事裁判で不利になる可能性があるので、弁護士や消費者生活センター、警察などに相談すべきである。とくに契約が有効か否かについては、素人で判断せずに専門家に相談すべきである。

三「掲示板」での誹謗中傷にあわないために

ネット空間での発言は基本的に匿名であり、それは情報発信を容易とする反面、発信段階で他者による内容のチェ

ックがかからないという危険性をはらんでいる。しかも、そこでのコミュニケーションが、基本的に文字だけのコミュニケーションであることから、稚拙な表現に起因した誤解も生じやすい。発言は瞬時にきわめて広範囲の者に認識される可能性があるなど、現実社会における通常のコミュニケーションとはかなり異なった性質をもっている。

とくに電子掲示板などでの議論では、双方が冷静さを失い、勢いにまかせて発言し、応酬が感情的にエスカレートすることがある。これは、「フレーミング」（炎上）と呼ばれている現象であるが、フレーミングの過程では、結果的に下品な人格攻撃などにまで発展しやすい。このようなケースの場合、いわば「喧嘩両成敗」的な解決がとられることがある。たとえば、東京地裁平成一三年八月二七日判決では、問題の書き込みが被害者の挑発的な発現がきっかけになっていたと認定し、被害者の反論が容易な媒体で、反論が十分な効果をあげている場合には名誉毀損は成立しないとして、原告の損害賠償請求を棄却した。このような考えの背景には、言論による名誉侵害は言論で回復可能な場合があり、両者が対等なメディアを利用できるならば、法的制裁を科す前に、反論、すなわち「対抗言論」での名誉回復を図るべきだという発想があり、学説でも支持する見解も多い。

このようなフレーミングの果てに生じた誹謗中傷とは異なり、掲示板やホームページなどで一方的に誹謗中傷されるケースは、現実社会と変わらぬ名誉侵害であり、最終的には、民法や刑法による救済が可能である。また、いわゆるプロバイダ責任法によって、一方的に書き込まれた発言の削除をプロバイダに要請することも可能である。しかし、法的な可能性と現実の実効性とは別の問題であり、完全に身元を隠して書き込まれた発言者に対しては、損害賠償などの法的手段を取ることは不可能に近く、またいわゆるファイル交換ソフトのネットワークに残された情報などについては、それをネットワーク上から完全に消去することは不可能である。日頃から自宅の電話番号や携帯電話の番号、メールアドレスなどの個人情報を、他者に不必要に開示しないように心がけたほうがよい。

四　「成りすまし」の被害にあわないために

銀行や企業からのメールを装い、受信者を偽のホームページにアクセスするように誘導し、会員番号やパスワードの更新などと偽って、クレジットカード番号、ＩＤ、パスワード等を入力させて、個人情報を不正に入手する「フィッシング（Phishing）」という手口が流行っている。現実空

間では、印鑑や筆跡など、物理的な痕跡で個人を確認することができるが、ネット空間ではそのような方法は不可能であり、現在一般的な個人認証の手段は、ＩＤとパスワードという任意の文字列による認証である。したがって、他人のＩＤとパスワードを入力すれば、ネットワークは当該個人を本人と認め完全にその他人に成りすますことができる。逆にいえば、被害者は、それは自分ではないと否認することが非常に難しくなる。

通常、銀行や企業などは、メールなどで個人の金融情報（クレジットカード番号、ＩＤ、パスワード等）を聞き出すことは絶対にないし、そのような内容の書類が送付されてきても、当該銀行や企業に問い合わせることが必要である。また、個人情報などを入力する際は、ブラウザの下部にＳＳＬ通信（インターネット上で重要な情報を暗号化して送受信する通信方法）であることを示す「鍵のマーク」がロックされた状態で表示されているか確認することも大切である。

五　ウイルスの感染被害にあわないために

二〇〇〇年五月、コンピュータ・ウイルスを含んだ「I LOVE YOU」というタイトルのメールが、受信者のメールソフトのアドレス帳に登録されているアドレスのすべてに同じウイルスを送りつけ、わずか数十時間でウイルスを世界中にばら撒き、多大の被害をもたらした。現実社会では、病院や研究所から細菌・ウイルスなどの微生物が外部へ漏出してひき起こされる災害や障害（バイオハザード）が問題となっているが、サイバースペースでも、悪意に満ちたプログラムの伝播・感染が現実の問題となっている（デジタルハザード）。インターネットの拡大に伴い、「I LOVE YOU」ウイルスのように、メールの機能を悪用したウイルスが瞬時に世界中に広がる環境が形成されており、今後はＯＳ（基本ソフト）の違いを超えて動作し、感染の事実すら気づかれない間にファイルやディスクを破壊し、自らは消滅してしまう高度なウイルスが登場する可能性も懸念されている。

多くのコンピュータ・ウイルスは、ブラウザやメールソフトなどのソフトウェアの既知のセキュリティ・ホールを悪用しているので、利用しているブラウザやメールソフトなどのソフトウェアに対する修正プログラムを適用するか、最新のバージョンに更新することが大切である。

また、コンピュータ・ウイルスをパソコンから駆除するために、ワクチンソフトをインストールし、ウイルス定義ファイル（パターンファイル）を最新のものに更新してい

くことも有効である。プロバイダによっては、メールに対するウイルスチェックを行っている場合もあるので、そのサービスを利用することもウイルス対策としては効果的である。

六　犯罪者にならないために

(一) 違法コピー

有料無料にかかわらず、原則としてすべての著作物には著作権がある。しかし、情報のデジタル化によって、オリジナルとコピーが判別不能となり、しかもコピーコストがゼロに等しく、コピーが容易でもあることから、著作物の違法コピーがネット空間に蔓延している。もちろん違法複製は著作権法で処罰される犯罪行為だが、著作権法には、著作権者は自己の著作物を公衆へ伝達する権利やネットワークへのアップロードの権利を専有していることも明記されているので、著作権者の許諾をえずに著作物をサーバーなどにアップロードし、不特定多数のユーザーがダウンロードできる状態にする行為も処罰の対象となっている。したがって、ネットサーフィンをして、気に入った画像や映像などを見つけ、それをダウンロードし、個人的に楽しむ限りは問題はないが、それらを勝手にホームページや掲示板に掲載するといった行為は、例外的に許される場合もあるが、まず犯罪行為となると考えて間違いない。

最近は、PtoPソフトと呼ばれるファイル交換ソフトを使うことが流行っているが、他人の著作物をダウンロードすることじたいは法に触れなくとも、ファイル交換ソフトの中には、ダウンロードと同時にそれをファイル交換ソフトのネットワークに自動的にアップロードするような機能をもったものもある。そのようなソフトの場合には、他人の著作物を無断でアップロードすることは著作権法に違反する違法行為であるから、そのファイル交換ソフトの使用じたいが違法行為となることに注意しなければならない。

一定のルールと手続きを踏めば他人の著作物を掲載・引用することができるので、事前に著作権者の許諾を得るなど、他人の著作物の利用については細心の注意を払わなければならない。

(二) 不正アクセス

不正アクセス禁止法では、ネットワークに接続されたコンピュータ利用についてIDとパスワードによるアクセス制御機能が設けられている場合、そのアクセス制御機能を保護することがネットワーク全体に対する信頼性を高めることにつながると考えられている。したがって、不正アク

セスという犯罪行為は、ネットワークの管理者が特定の個人に対してのみアクセスを許可したという、アクセス制御機能に対する社会一般の信頼を保護するという意味で、文書偽造罪などと同じように、いわゆる社会的法益を保護する犯罪に分類されている。個人の所有物である物について所有者がその処分に同意すれば犯罪ではなくなるが、社会的な利益の処分については、個人が処分権限をもたないので、犯罪の成立を阻却することはない。不正アクセス禁止法においても、プロバイダが設定したアクセス制御機能は個人的な利益の問題ではないので、個人間でのIDとパスワードの貸し借りも犯罪行為として処罰の対象となっている。現に、会員制のネットワークゲームにおいて、友人の同意を得て、その友人のIDでネットワークゲームを行った者が検挙されたケースがある。IDとパスワードを個人で厳重に管理するということは、ネットワーク社会の基本的なマナーであり、その点についての個人の成熟度を測るもっとも基本的な事項なのである。

七　おわりに

家に鍵をかけるのを忘れて、泥棒に入られたとしても、もちろん入った者が犯罪者として非難の対象となる。ところが、ネットワークでも同じ考えが妥当するかと言えば、必ずしもそうではない。違法な情報を規制する場合、その発信を規制する発信規制と受信側でそれをコントロールする受信規制とがあるが、グローバルなネットワークでは、情報の規制基準が各国で異なるために、発信規制を貫くことが難しく、受信規制を中心に置かざるをえない。また、局地的な物理的破壊があっても、システム全体が機能し続けることを目的としてインターネットが開発されてきたわけであるから、インターネットにとっては物理的破壊も規範的な情報規制も等価となり、情報を規制しても、インターネットはその規制を迂回して情報を流し続ける性質をもっている。

このような点から、インターネットでは自己防衛が非常に重要な考え方となる。中央集権的にネットワーク全体の安全性を高め、ユーザーにとって他律的にネットワークの安全性を維持していくことは大変難しいことである。しかし、ネットワークに参加している個々人がみずから情報の有用性について判断する能力を高め、各人がIDやパスワード、金融情報などの個人情報の管理を確かなものとしていくことによって、全体としてのネットワークの安全性もまた確実に高まることは否定できない事実なのである。