紹　介

河崎貴一『インターネット犯罪』

澤　喜司郎

(I)

著者は「犯罪者や悪意のある人物ほど，新しい技術にさといものだ。インターネットは，通信手段の中でも，もっとも便利で，自由で，匿名性が高い。世界中を股にかけて犯罪を行うテロリスト集団やスパイが，通信手段として選んだのが，インターネットなのだ」とし，「インターネットは，TCP/IPという方式の共通のプロトコルを利用する。しかも，インターネットの通信回線は，世界中に網の目のように張りめぐらされているので，犯罪が，伝染するのも，パソコン通信の比ではない。とくに，コンピュータ・ウィルスは，数日で世界中のコンピュータが感染するほどである」という。

そして「インターネットの技術が進んで，犯罪の手口もハイテク化し，レベルアップしている。デジタル技術は難解であるが，利用することは子供でもできる。したがって，誰でも犯罪を実行することが可能なのである。実際に，未成年者のインターネット犯罪も多く，年々，増加し続けている。逆に言えば，それだけ被害者も増加している。もし，インターネット犯罪手口がわかっていれば，被害にあっても適切な対応が取れるし，それ以前に，被害者にもなりにくい」とし，そのため著者は本書を「犯罪防止マニュアルのつもり」で著したとし，「インターネットやパソコンは，人間の道具であって，決して目的ではない。あまり過信しすぎると，思わぬ被害にあいかねない。パスワードやプライバシーなどの取り扱いには，くれぐれもご用心を」と記している。

なお，本書の構成は

第5章　アダルト・サイトとわいせつ事件
第6章　ウィルス同時感染の恐怖
第7章　ハッカーは透明人間のごとく
第8章　どうやって防ぐか—法とセキュリティ
おわりに

であり，以下，本稿では各章の内容を要約的に紹介したい。

(Ⅱ)

日本のインターネット人口は1999年末で2,706万人に達し，前年比59.7%という驚異的な増加率を示し，そのインターネット人口の増加に比例するようにインターネットを利用した犯罪がインターネットが普及し始めた1995年以降には加速度的に増加して社会問題になっているという。警察庁の統計ではハイテク犯罪は「コンピュータ，電磁的記録対象犯罪」と「ネットワーク利用犯罪」に分類され，前者は電子計算機損壊等業務妨害，電磁的記録不正作出罪，電子計算機使用詐欺罪等の罪名にあたる犯罪で，それはコンピュータの持ち主や管理者でない第三者が不正にコンピュータに記録されているデータの書き換えや消去をしたり，データを持ち出したり，詐欺を行う犯罪である。後者は，コンピュータネットワークを悪用する詐欺罪やわいせつ物頒布罪等の違法行為で，それは金銭や物品を騙し取る，わいせつな画像や動画をネットワークに掲載する，他人のIDやパスワードを使用してアクセスを許可された第三者に成りすましてネットワークに接続するなどの行為である。しかし，前者の「コンピュータ，電磁的記録対象犯罪」のほとんどが最近はネットワークに不正アクセスしてから行われることが多く，今ではネットワークの犯罪そのものが問題となり，広義のネットワーク犯罪とは実際にはインターネット犯罪に他ならないとしている。

警察庁によれば，平成12年上半期のハイテク犯罪の特徴には①ネットワーク利用犯罪の大幅な増加，②インターネット・オークションを利用した事件の多発，③児童買春・児童ポルノ禁止法違反事件検挙者数の大幅増，④名誉毀損，商標法違反等の発生があり，なかでもネットワーク利用の詐欺事件は全詐欺事件の約半数を占めているという。そして「オークションは，1台の商品をせりにかけるのが一般的だが，文面をよく読むと，商品を特定多数の相手に売り込もうとする怪しい下心がミエミエ。それなのに，コンピュータ・ショップでは現品を前にしても石橋を叩いても渡らない用心深い買い物客でさえ，インターネットに商品の写真と文面を掲載し

ただけの匿名の相手を，いともカンタンに信じてしまう」から不思議で，このようなインターネット犯罪には未成年者，それも中高生による犯罪が多いという。

著者によれば，彼らは最初は両親が支払っているIDを使ってインターネットに接続し，それから次第に他のサーバーに侵入してそのIPアドレスを変更したり，プロクシーという特殊なサーバーを経由してインターネット内を辿った足跡を消したり，架空のIDを購入して透明人間に成りすましたりして悪事を働くようになる。彼らが「対面しているのは，コンピュータに接続されたディスプレイだけ。インターネットで接続された相手はバーチャルの世界で，そこで犯罪を行うのはゲーム感覚だ。銀行口座に入金があるという実益がある割には，被害者の苦しみを見ないですむ。これほど，楽しいコンピュータ・ゲームはない。一度やったら，やめられなくなる。実際，ネットワーク犯罪で逮捕された容疑者の多くが常習者だった」としている。「彼らの親たちは，子供部屋にコンピュータを置き，電話回線まで引いていることが，結果的に犯罪のお膳立てをしていることに気づいていない」し，「中高生が，個人の勉強にコンピュータを使うことは，ほとんどないと言ってもいい。が，親たちは，子供がコンピュータに向かっているだけで，勉強していると勘違いしてしまっているのだ」と指摘している。

また「インターネットの参加者には，大人と子供の区別はないし，区別することは不可能だ。しかし，未成年者が大人顔負けの犯罪を起こしても，検挙されれば，少年法で温かく守られる。少年だから，名前や顔写真が報道されることもなく，大人の犯罪者に比べ罰則もけた違いに軽い」。著者は「今やインターネットはあらゆる犯罪の温床になっている」ため，「子供たちが，インターネットによってどんどん壊されていくような気がしてならない」と危惧している。

さらに，1998年には大学生2名と会社員1名がわいせつ図画販売の疑いで逮捕され，大学生2名はアメリカのトライポッドというレンタル・サーバーにホームページを開設し，受注のために契約した日本のプロバイダーには大学内のサーバーから接続していたことから，「昨今の学生は，学内のメール・アドレスを割り当てられて，大学からの連絡やレポートの提出にも，インターネットを使っている。その裏で，大学はこのようなアルバイトやハッキングなどの犯罪行為の温床にもなっている」と指摘する。

(Ⅲ)

世界的にインターネットの利用者が爆発的に増えたきっかけは，1995年にマイク

ロソフトの「ウィンドウズ95」というOSが発売されて個人レベルでホームページや電子メールが比較的簡単に利用できるようになったからで，これほど利用者が増えたのはインターネットが便利な情報通信手段だからであるという。そこで利用されている機能は電子メールで，「電話回線や携帯電話があれば，いつでもどこでも郵便以上の情報を送受信することができて，画像や音声も添付が可能だ。同時に多数の相手にメールを送信することもできて，郵便料金よりコストは安い」し，さらに「ファイルを転送するためのFTP機能はブラウザから起動して無意識に使っている」が，「実は，FTPは他のサーバーに不正侵入するために使われている…ことは，あまり知られていない」という。

そして「犯罪者ほど新しい技術に目ざといのは，古今東西の習いで」，「日本警察がコンピュータやネットワーク犯罪に本格的に取り組むようになったのは，オウム真理教がきっかけだったと言っても過言ではない」としている。

また「ネットワーク上の危ない出会いの場は，パソコン通信時代や電話の伝言ダイヤルなどにもあったが，インターネットが普及してからは，ホームページの掲示板が使われるようになった。パソコン通信では，管理者が内容をチェックして削除することもできたが，インターネットには，たとえ危険な内容でもチェックなしに，無料で掲載させてくれるサーバーがある。とくに，外国のサーバーは，日本語のチェックに甘く，犯罪の巣になりがち」と指摘し，自殺を請け負う「ドクター・キリコの診察室」もアメリカのgeocitiesという無料サーバーにあったという。インターネット自殺事件に象徴されるように，日本でも自殺者が年々増える傾向にあり，「自殺の善悪判断や周囲に与える影響は別として，自殺はやろうと思えば誰にでもできる。だが，自殺志願者に毒物を与えて自殺を勧めることは，自殺ほう助という犯罪にあたることを，知っておく必要がある」。

さらに「ドクター・キリコの診察室」のように，「自殺系のホームページで売買された自殺薬は，ほとんど購入した人物が使ったり，自殺する人に転売する。ところが，同じ違法の危険薬物でも，薬物系といわれるホームページは，購入した人物がそうしたこととはまったく無関係の相手に犯罪目的で使用するので，もっとやっかいなことになる」とし，「青酸カリ，筋弛緩薬，クロロホルム…などの違法な薬物を，たとえインターネットで買ったとしても，確実に届けられるという保証はない。代金を振り込んだ後で品物を送って来なくても，実名で警察に訴え出る人は，まずいないだろう。そんな犯罪者の心理を逆手に取った詐欺が多いのも，インターネットの特徴である」という。

ただし「インターネットで仮名のアクセス権利を使い，仮名の銀行口座を使っている透明人間でも，現金を引き出すのは，生身の人間なのである。ここが，インターネット犯罪者の最大の弱点だ」が，「逮捕うんぬんする以前に架空口座を持つこと自体が違法なのだから，カードや通帳での自動支払機の利用ができないように，法改正ができないものだろうか。意義があれば，銀行のカウンターで，身元確認の上で利用できるようにすればいい」し，「インターネット犯罪が急増しつつある今だからこそ，インターネット犯罪が割に合わないことを，知らしめる必要がある」と問題提起をしている。

（Ⅳ）

ネットワーク上に危ない出会いの場があるように，「インターネットには，悪の心をそそのかす魔力が潜んでいるのかもしれない。見ず知らずの人間から，面と向かって犯罪に誘われても，そうカンタンに応じられるものではない。ところが，インターネットの向こうから，正体不明の悪魔がささやくと，時たま応じる人間が現れるのだ。その悪魔とは，インターネットの匿名性だ…。匿名が許されていると，悪の心が頭をもたげてくる。わざと発信者の情報を隠してアクセスして，犯罪的な内容を掲示しようとするやからもいる」ため，「犯罪的な書き込みには，書き込みを削除するなり，事情を確認するなりして，必要があれば，厳正な処置をすべきだ」が，現実はそうではなく，ネットワーカーどうしが結託して悲劇も起こっている。それは「インターネットで感染する悪魔の心は自己中心的になって，まわりを見えなくするから始末が悪い」ばかりか，「インターネットは，自分の素性をさらす必要がないので，ふだんは口にさえできない本性を書き込むことができる。同好者が見つかると，もう１人の自分に会えたような，特異な連帯感ができるらしい。そして，インターネット・ゲームの主人公になっているような錯覚で，犯行に及んでしまったのだろう」という。

そして「日本では，家に鍵をかけなくても泥棒が入らないことが，安全な社会の象徴とされている。ところが，西欧では，自らの安全に加えて，相手に犯罪の心を起こさせないためにも，鍵をかけるという。インターネットでの犯罪を防止するためにはどちらが有効か。それは，言うまでもない。危険な内容の掲載には，透明人間の素性を明らかにして，必要なら責任を追及するようなルールやシステムを作ることが必要ではないか。インターネットに関する規制には，自由な発言を阻害すると，反対論もある。が，自由には義務も伴わなければ意味がない」と主張している。

また，1999年には告発ホームページが相次いで開設されて社会問題にもなったが，「告発ホームページの内容が間違っていたとしても，それは言論の自由で，刑法の名誉毀損に抵触する以外は，犯罪にならない。しかし，インターネットがメディアであるにもかかわらず，報道機関のように，報道する前に，内容が正しいかどうかを，審査するチェック機関がなく公開されてしまうことが問題」で，「今後，このような告発ホームページは，ますます増えると思われる。一般人や企業，団体などが，インターネットに実名やプライバシーを公開されて，告発されることも起きるだろう」としている。「誹謗中傷や名誉毀損に相当する内容については，警察に親告し，裁判所にホームページの削除や損害賠償請求の訴訟を起こすことも可能である」が，「写真やプライベートなデータは，インターネットに一度掲載されると，掲載者もどうにもならないほど一人歩きしてしまう」し，「ネットワーカーは，記録を取っておくものなので…ホームページをまるごと記録するソフトも市販されている」のである。

他方，あるサイトに接続して指示に従って操作していると，突然，ソフトのダウンロード画面に切り替わることがある。「実は，このソフトはダイヤラーという電話をかけるソフトで…あらかじめ設定されている電話番号に，パソコン使用者が知らないうちに，自動的にかけてしまうのだ。その接続先はダイヤルQ^2の有料サイトだったり，国際電話だったりする。いずれにしても，後で驚くほど高額の請求書が送られてくるハメになる。ダイヤルQ^2の場合は，料金の徴収代行するNTTの規制があって，有料の注意書きを表示することになっているが，中には，その表示が小さくわかりにくいものもある。もっと高額の請求書が送られてくるのは，国際電話接続ソフトだ。国際電話をかけるなどという注意書きは一切ないのに，自動的に接続してしまう。そのソフトを一度使用すると，以後，インターネットに接続する際には，すべて国際電話をかけるように接続の設定を書き替えてしまうものまであった。…明細書の対話地名には，旧ソ連やオセアニア地域の小国が記され」，自動ダイヤル・ソフトを配布したサイトの開設者は「相手国の電話会社や組織から，なんらかの方法で，国際電話(料金)の一部がバックマージンされるらしく，そのため，この商売が始まった」という。

(V)

コンピュータ・ネットワークが進化すると，ウィルスという名称の人為的なコンピュータ病が急増し，しかもインターネットに接続されている全世界の何十億台と

いうコンピュータが瞬時に感染して世界中のインフラが同時に麻痺する危険性をはらんでいる。コンピュータ・ウィルスそのものはOSやアプリケーション・ソフトと同じように「0」と「1」の信号で書かれたプログラムで，フロッピーディスクなどの外部記録媒体に記録されているだけでは害を及ぼすことはない。

しかし，いったんコンピュータ内のメモリやハードディスクに侵入すると，プログラミングされた潜伏期間を経たり，日付や時間など一定の状態になるのを待って突然発症する。コンピュータ・ウィルスの症状はさまざまで，メッセージや画像を表示するイタズラ程度からハードディスクに記録されている内容を消去したり，記録されているIDとパスワードを盗んで特定のメール・アドレスに送るものや，ハードディスクのデータをすべて消去した上で記録されているメール・アドレス全員にウィルスを配布するものなど悪質なものもあり，「高速通信で世界中のコンピュータが結ばれているインターネットにとっては，最大の脅威」といえる。

ウィルスは8,000種類以上存在するといわれ，そのうち約半数がマクロウィルスというワープロソフト「ワード」や表計算ソフト「エクセル」のファイルを媒介するウィルスで，メールに添付されて広がり，アプリケーション・ソフトを起動すると感染する。そのマクロウィルスはプログラムを部分的に書き替えることが可能なので，ウィスルの種類は無制限といえ，新種のウィルスも毎月のように発見されている。このようなコンピュータ・ウィルスはワクチン・プログラムを使ってシステムやデータを補修し，ウィルスを削除する必要があるが，「ウィルス対策用ワクチンです」と偽装工作したウィルスもあり，被害を拡大しているケースもあると指摘している。そして，「I」というイニシャルのホームページには約90種類のウィルスそのものが登録してあり，いつでも誰でもダウンロードでき，このホームページのアドレスからイギリスのサーバーであることがわかるが，日本語表記されていることから日本人が日本から発信していると思われる。

アメリカはインターネット先進国だけにウィルスをバラまいた罪は想像以上に重く，刑事責任だけではなく，ウィルス被害を受けた企業が容疑者に損害賠償請求訴訟を起こしたなら一生かかっても償いきれないほどの賠償金が科せられるが，日本では同様の犯罪で裁かれると，「業務妨害罪(3年以下の懲役もしくは50万円以下の罰金)，電磁的記録不正作出罪(5年以下の懲役もしくは50万円以下の罰金)，不正アクセス禁止法(1年以下の懲役もしくは50万円以下の罰金)に抵触する可能性があるが，いずれも米国より軽い。まして，少年犯罪の場合は，罰はないに等しい」のが現状である。

なお,「コンピュータやネットワークが進化するにつれて，予想をはるかに上回る速度であらゆるウィルスが出現し…新種のウィルスが，続々と現れては被害を与え続けている。それまでのウィルスはプログラムまたはメールに添付されたファイルの形を取ることがほとんどだったので，それらのプログラムやファイルを，起動したり，開かなければウィルスに感染することはなかった。ところが，最近のウィルスは，本人が気づかずに感染するものが多い。たとえば，ホームページ用のHTML言語で書かれているHTMLウィルスと，Javaというプログラム言語のJavaウィルスは，ホームページを閲覧するだけで，感染してしまう」。

(Ⅵ)

インターネットにつながっているコンピュータ，とくにウィンドウズ・マシンのほとんどはネットワークを通して内部が覗け，外部のコンピュータから遠隔操作をしてファイルのコピーや削除，書き込みも簡単にでき，またネットワークを管理しているサーバーのrootやsuのパスワードを盗めばメンバー全員のメールを見たり，ホームページを書き換えることも可能だという。さらに，ホームページを見ただけでもクッキーという機能でアクセスした閲覧者のIPアドレスが先方に知られてしまうケースもあり，データ漏洩の危険性が指摘されている。

また，特定のサーバーや個人ユーザーのIPアドレスを知るにはいろいろな方法があり，例えば前述した「I」というイニシャルの日本語のホームページにはハッキングというコーナーがあり，そこでは最新のハッキング・ツールやマニュアルまでが掲載され，そのハッキング・ツールをダウンロードすることもできるばかりか，同じコーナーには個人が電話回線を利用してインターネット接続する時のユーザーIDやパスワードを表示させるソフトまで登録されており，そのため「コンピュータ・ネットワークの知識に詳しくなくても，これらのツールを使えば，ハッカーになることができる」という。

さらに，ネットワークのホール(セキュリティの穴)を探すために市販されているハッキング防止ツール(約60万円)を組み込んだコンピュータをLANに接続すると，ネットワークに接続されているすべてのコンピュータのユーザーIDやパスワードや電子メールなど，あらゆる情報を見ようと思えば見ることができ，ログ(通信記録)を消せば侵入した形跡も残らず,「高度なハッキング防止ツールは，ハッキング・ツールでもある」としている。そして「企業や団体の場合は，ネットワーク内にファイアーウォールを設置して，外部からの不正侵入を防いでいる。しかし，侵入者の

ユーザーIDやパスワードが正しかったり，セキュリティ・ホールから侵入されると，ハッキングされる可能性が高くなる。個人が常時接続して固定アドレスを使用するようになると，このハッキングの可能性は高くなる。家庭内LANを組んで，〈ファイルを供用できるようにする〉に設定しておくと，外部から，データを盗み見られるだけでなく，コンピュータの内部を消去される恐れもある。それ以上に，個人のIPアドレスを踏み台にしてハッキング行為が行われる可能性も高い。個人用のファイアーウォール機能を備えたルーター(交換器)も…完璧ではない。結局，ユーザーIDとパスワードを複雑にして，こまめに変更するしか自衛手段はない。どうしても，ハッキングされたくなかったら，インターネットに接続しないことだ。究極のセキュリティは，オフライン(非接続)しかない」と指摘している。

他方，2000年1月に日本の中央省庁や公的機関など16カ所のホームページが次々にハッキングされたが，ハッキングのために踏み台にされたサーバーの一つが東大など国内の大学であり，これらのハッキングには「バッファ・オーバー・フロー攻撃」が行われた。その方法は，サーバーに1秒間に数百回から数千回もデータを送りつけるとサーバーの処理能力の限界を越えて誤作動するようになるものがあり，その時の誤作動によって生じたセキュリティホールを通って外部から侵入するというものである。この事件でもハッカーは自分の足跡を消しており，足跡を消すにはプロクシーという代理サーバーを使う方法がある。プロクシーを経由してインターネットに接続すると前回接続した時の設定が残らず，IPアドレスで接続しているパソコンが特定されなくて，クッキーが機能しなくなる。プロクシーは本来，ホームページを閲覧する時などに代理サーバーとしてデータを蓄積できるので，速く表示できるメリットがあるが，ネットワーク上の透明人間になるために悪用されることもあるという。同様に，マイクロソフトの「ホットメール」という無料の電子メールサービスを利用するにあたっては，必ずしも個人情報を正確に申告する必要はなく，そのためインターネットで悪用されることもあると指摘している。

(Ⅶ)

インターネット関連の犯罪を摘発するために制定された「犯罪捜査のための通信傍受に関する法律」(2000年8月施行)によって電子メールの盗聴が可能になり，捜査対象者が送受信する電子メールは捜査当局に転送されるという。インターネット犯罪を防止するために多くの法律の成立をみているが，インターネット犯罪は増加の一途をたどり，それは「現状ではあまりにも容易に犯罪に手を染めることができ

る環境がネット上に整いすぎている」からだという。

インターネットは国境のない自由な通信ツールで，それが便利な反面，インターネット犯罪が急増して自由な通信の弊害にもなり，将来的にはもっと悲惨な犯罪が起こる可能性も指摘されているため，「その犯罪を防ごうとすれば，インターネットの自由を考え直すべきではないだろうか。自由と民主主義を守るためには，国民の一定のルールが必要なように，インターネットもルールを設ける時期にきている」といい，インターネット免許制を提案するとともに，インターネット犯罪が若年化する中で子供たちに対するインターネット教育が急務であると指摘している。

著者は，上述のように「昨今の学生は，学内のメール・アドレスを割り当てられて，大学からの連絡やレポートの提出にも，インターネットを使っている。その裏で，大学はこのようなアルバイトやハッキングなどの犯罪行為の温床にもなっている」と指摘していることからも，大学におけるインターネット教育を早急に実施する必要があろう。

以上，やや詳細に本書の内容を紹介したが，それは多くのインターネットユーザーとりわけ学生諸君に本書をぜひとも読んでいただきたいからである。最後に，筆者が浅学非才なために本稿において本書の的確な紹介ができず，また筆者の不勉強による誤読の可能性もあり，この点については著者のご海容をお願いする次第である。

（文春新書，2000年，225頁，690円＋税）