サイバーローに関する若干の試論

原　禎嗣

一　はしがき

一九九五年一一月、マイクロソフトウィンドウズ95日本語版が発売された。この基本ソフト(Operating System：OS)を活用するためには、それまで使われていたOSの場合よりも遙かに高性能なコンピュータ本体が必要となるにもかかわらず、大きな人気を集めた。これと並行するように、国内向けパーソナルコンピュータの出荷台数も飛躍的に向上したことは記憶に新しい。昨今、こうしたコンピュータの出荷台数にも陰りが見えるとのことであるが、普及そのものを妨げるものでないことは無論である。

もう一つ、我が国一般家庭へのコンピュータ普及の要因として、「インターネット」(Internet)ブームが上げられよう。一九六〇年代、米国の軍事研究機関が、核攻撃の際にも破壊されない情報伝達方法確立を目指して開始したARPA

PANET[1]は、瞬く間に政府機関、大学等のコンピュータシステムを結合させ、やがて、プロバイダと呼ばれる民間向け接続会社の誕生を促した。

我が国においても、一九八四年、東京大学、慶応義塾大学、東京工業大学が実験的ネットワーク作りを開始した[2]。この動きは、やはり民生用に拡大し、一九九四年にはわずか数社しか存在しなかった国内プロバイダも、一九九七年には一七〇〇社を越えたのである[3]。

そして今日、世界中で、一体どれほどのコンピュータが、こうしたネットワークに接続されているのか、正確に計ることは不可能である。

こうしたコンピュータネットワークの普及は、その利便と同時に、既存の法体系では対処の困難な多くの問題をもたらした。今日、「サイバーロー(Cyber Law)」定立の必要性が指摘されつつある所以である。筆者は、基礎法学系を専攻するものとして、また、インターネットやパソコン通信のユーザーとして、このサイバーローという新しい法分野に関し、卑見を述べることを試みる。

(1) ARPANETは、Advanced Research Projects Agency Network の略。既存の「集中型」情報伝達方式では、拠点に障害が発生すると全ての通信が不可能になるため、情報伝達経路を固定しない「分散型」通信方法の研究が行われた。この方式では、特定の二地点間に複数の経路を設け、その時々に利用可能な経路を自動的に選ぶことにより、万一の障害の際にも、別経路に迂回することで通信は保たれる。ARPANETに言及する文献は数多いが、ここでは、古瀬幸広・廣瀬克哉「インターネットが変える世界」岩波新書・一四頁以下・一九九六年一月、村井純「インターネット」岩波新書・四六頁以下・一九九五年一一月、岡村久道・近藤剛史「インターネットの法律実務」新日本法規・四~五頁・一九九六年五月を参照した。

(2) 前掲村井「インターネット」一三八頁以下。

(3) http://www.mpt.go.jp/policyreports/japanese/group/internet/net-1.html に掲載された資料による、九七年三月時点の数

字。以後も漸増を続けているものと考えられる。

二　所謂「コンピュータネットワーク」の現状　―技術的なアプローチ―

（1）　BBS

はじめに若干述べたように、あるコンピュータを他の機器と接続するという試みは、決して目新しいものではない。我が国においても、一九七〇年代、パーソナルコンピュータが市場に登場すると、電話回線を通じてこれらを接続し、各種サービスを提供する、BBS（Bulletin Board System）が出現した。いわゆるパソコン通信である。商用BBSでは、ユーザーがBBSの本体ともいうべき大型コンピュータにアクセスし、そこに集中的に蓄積されたデータを取り出し、あるいは、データを書き込むという形式で利用する。そこでは、データベース検索、プログラム提供、電子会議、電子メールといったサービスが用意されていたが、当然、そのBBSの会員のみが利用資格を有する、「クローズドネットワーク」であった。

やがて、「電子メール」サービスに関しては、BBS間で相互乗り入れが可能となり、他のBBSの会員との間で、「メールコミュニケーション」が実現した。

現在、BBSは、全国にアクセスポイントを持ち、一〇〇万人単位の会員を有する大手数社と、特定地域でのみ活動する中小、個人で運営するものなど、数百が稼動している。このBBSは、コンピュータ普及の当初から活動しているため、その接続に要する機器の性能も必ずしも最高水準である必要はなく、安価な機器で利用できる。また、独自のソフトウェアを開発し、利用者の便を計るところも多く、操作が簡易であるという利点を持つものが多い。しか

し逆に、会員のみを対象とし、独自のソフトウェア仕様を持つＢＢＳは、本質的に他のＢＢＳやネットワークとの接続を前提としておらず、後述するインターネットに対しては、長らく電子メールの窓口という役割を演ずるに止まっていた。なお、大手ＢＢＳでは、既存のサービスとは別にプロバイダ事業に進出する例も増えている。

(2) インターネット

先に述べたごとく、今日、インターネットの一般家庭への普及は著しい。

ところで、インターネットとは、一体いかなるものなのであろうか。ごく大雑把にいえば、世界中に散在する大小さまざまなネットワークを結び付けた、「ネットワークのネットワーク」ということになろう。上述のＢＢＳも、インターネットの一部として機能する例が少なくない。

筆者は文科系研究者、かつインターネットを始めとするコンピュータネットワークの利用者であるから、大規模な世界的ネットワークの構造をここに描出し得ないことは勿論であるが、筆者なりの立場から、知るところを整理し、以下の論述の便に供することにしたい。

① しくみ・構造・ＢＢＳとの違い

現在、我々利用者に供される「インターネット」には、大別三種類の情報、乃至伝達方法がある。まず第一は、ＷＷＷ（World Wide Web）と呼ばれる、文字や画像、音声などを組み合わせて表示されるデータ形式で、「ホームページ」という言葉で知られている。このホームページは、ＨＴＭＬ（Hyper Text Markup Language）と呼ばれる「コンピュータ言語」で記述されたテキストファイルの形でそれぞれのサーバーに蓄積される。ユーザーは、データの場所を示す記述をＵＲＬ（Uniform Resource Locator）を使ってサーバーにアクセスし、ＨＴＴＰ（Hyper Text Transfer

Protocol)という方式でＨＴＭＬデータを自分のコンピュータに転送し、専用のブラウザと呼ばれるアプリケーションを用いて閲覧する。およそインターネットと称する時、例外なくイメージされるのは、このＷＷＷである。ＨＴＭＬで記述されたデータは、読む、あるいは見ることのできるデータの外に、他のデータの場所を埋め込むことができ、利用者は、この記述を手がかりに、様々なデータ、あるいはホームページを瞬時に移動し、目的のデータを捜すことができる。このしくみをリンクという。(1)

ＨＴＭＬが普及する以前は、ユーザーはＧｏｐｈｅｒ、あるいはＡｒｃｈｉｅと呼ばれるアプリケーションを利用して求めるデータを検索し、見つかるとＦＴＰ (File Transfer Protocol) という方式で、データを自分のコンピュータまで転送した。だが、ＨＴＭＬと専用ブラウザの発達により、これらの手間は格段に軽減され、インターネットの普及に貢献している。

第二に、ＵＳＥＮＥＴと呼ばれる「ネットニュース（電子掲示板）」が上げられる。これは、もっとも早い段階で発達したインターネットの利用法であり、現在、世界中で三万以上もの、さまざまな話題に特化したニューズグループが存在している。ユーザーは、自分の接続先（大学や企業、個人の場合はプロバイダ）が設置したニュースサーバーにアクセスし、そこで希望するニュースグループを開き、記事を受信したり、メッセージを発信したりすることができる。(2)

第三が、Ｅ－ｍａｉｌである。従来から存在するＢＢＳの電子メールと同様、ユーザー間、あるいはコンピュータ間で一対一のコミュニケーションを実現する。ネットワークのユーザー、厳密にはネットワークに接続された各コンピュータにはＩＤが与えられており、これを住所氏名の代りに、電子的に手紙のやり取りを行うのである。

このような「サービス」から構成されるインターネットは、「放送」的な性格を持つＷＷＷ、通信としてのＥ－ｍａｉｌ、新聞のような文字メディアであるＵＳＥＮＥＴの三者からなる全く新しいメディアである。ＷＷＷは、情報の作成者と受信者から成る点では放送に近いが、アクセスによりいつでも閲覧が開始できる完全なＯｎ　Ｄｅｍａｎｄ

状態は、現在のテレビ、ラジオでは実現されていない。USENETは、基本的に文字が伝達手段である点で活字メディアに近いが、発信、受信に時間的、空間的制約がないことが特徴である。またE-mailは、瞬時に届くという点で郵便とは異なり、相手が機器の前にいなくても送信可能な点で電話と異なるのである。

このような「インターネット」におけるサービスのうち、ネットニュースおよびE-Mailは、既存のBBSにおいても同様な機能を利用することができる。WWWはインターネットの特徴の一つであるが、個人の持つ情報を提示するのみならば、ネットニュースやBBSの掲示板サービスを用いることも可能である。ではあるが、インターネットとBBSとは、決定的な相違点がある。それは、インターネットには管理者が存在しない、ということである。インターネットにおけるWWW、USENET、E-Mailなどの「サービス」は、特定の機関が管理、提供するものではなく、インターネットという、ある意味できわめて「漠」とした、しかし巨大なネットワーク上で標準化された使用法を意味する。

BBSは、言うまでもなく、それを運営する企業、団体あるいは個人が管理者となり、管理上必要なルールを定め、会員に対して遵守を要求する。違反するものに対しては、資格剥奪といった強制的措置も用意されている例が殆どである。BBSは、会員が利用するサービスがすべて、BBSの運用するホストコンピュータに蓄積されているため、これへのアクセスを停止することにより、特定会員の排除は容易である。

ところが、インターネットは、特定のコンピュータにデータがすべて入っている、という形式ではない。極論すれば、接続されたコンピュータすべてがデータの蓄積と収集を行う端末として機能するのであるから、総体としてのインターネットを管理することは不可能なのである。

したがって、世界中に張り巡らされている高速通信回線に、自らのコンピュータを接続するしくみを利用できるものはすべて、自己責任においてインターネットを利用することになる。もし仮に、何らかの不都合が発生したとして

も、特定の機関や団体が責めを負うといったシステムは存在していないのである。[3] つまり、インターネットとは、優れて無政府的状態で増殖し続けている最新のメディアであるということができよう。

② 接続方法

次に、個々のコンピュータとインターネットへの接続方法についても触れておこう。

一般に、研究機関や政府機関、大手企業では、組織内に独自のコンピュータネットワークを持っている。これをLAN（Local Area Network）という。ユーザーは、LANに接続されたコンピュータから、LAN内部に蓄積された、あるいはそのLANに接続された他のコンピュータが持つデータを検索、閲覧したり、相互にE－Mailの送受信を行うことができる。さらに、LAN全体をインターネットに接続することで、LAN経由で世界と情報のやり取りをすることが可能となる。

この場合、それぞれの組織にIPアドレス（Internet Protocol Address）が与えられる。IPアドレスは、三二bit（bitは電子的データの大きさの単位）の数値で、電話番号のイメージに近いが、例えば電話番号のような、市外局番―市内局番―個別番号といった統一された形式にはなっていない。

そこで、IPアドレスよりも覚えやすい略号を使って、それぞれの組織を表示することが一般的となっており、これをドメインネーム（Domain Name）と呼ぶ。ドメインネームには幾つかの階層があり、最高位をトップドメイン、以下の階層をサブドメインという。インターネット発祥地であるアメリカを除き、通常トップドメインは国名、次に組織の種類、組織の名称というように、サブドメインが付けられる。

インターネットに接続されたLANは、二四時間稼動し続けることが通例であり、個々のユーザーは、自分のコンピュータを使用している時間中、常に、インターネットに接続し続けることが可能である。

こうしたLANを有する組織に所属していない場合、すなわち、一般家庭からインターネットを利用しようとする場合などは、民間の接続会社であるプロバイダと契約し、公衆電話回線を利用してコンピュータをプロバイダと接続する方式が普及している。この場合は、コンピュータにMODEM（Modulator Demodulator）という機械を繋ぎ、コンピュータの発するデジタル信号を電話線で送受信できるアナログ信号に変換する。そして、TCP／IP（Transmission Control Protocol/Internet Protocol）と呼ばれる方式に則った電話線利用接続専用アプリケーションを利用し、プロバイダと接続した後、WWWブラウザやニュースリーダー、メーラーといった、既述三種類の情報形式に応じたアプリケーションを起動することになる。この接続方式をダイヤルアップ接続と呼ぶ。ユーザーのコンピュータは、プロバイダと接続されている間のみ、一時的にインターネットの一部となり、情報の送受信を行うことができる。(4)

MODEMを使った通信速度は、五六〇〇〇bps（Bit per Second）がおおむね実用可能な最高速となる。この速度では、理論上一秒間に、漢字三五〇〇文字を転送できることになるが、LAN接続と比較すると、数百分の一程度にしかならない。そこで、電話回線そのものを高速化に対応させたISDN（Integrated Services Digital Network）という規格が普及し始めており、これを利用すると通常六四〇〇乃至一二八〇〇bpsまで速度を上げることができる。

さて、このようなソフト、ハード面での技術革新の結果、我が国においてもインターネット利用者は飛躍的に増加している。そして今日、インターネットといえばWWWを指すものといっても差し支えない。既述のとおり、WWWのデータには、文字や画像データと同時に、他のデータの場所を埋め込むこと（リンク）が可能で、ユーザーは、このリンクを頼りに、自分の求めるデータにアクセスする。つまり、ユーザーは随時、自分の希望する内容のみを求めることが可能となっている。一方、従来からあるBBSでは、固定されたメニューに従い、定型化されたデータを入手するが、臨機に他のデータにアクセスするといった使い方はできない。勿論、他の機関が持つデータにリンクさせる

といったことは行われていない。ここにおいて、完全とはいえないまでも、ユーザーと情報提供者との間に「双方向」的な関係が発生することが、WWWを普及せしめた第一の要因であると考える。

（1）データの場所を示すURLは例えば、http：//www. aaa. ac. jp/data/index. htm といった形式で記述する。この場合、「aaa という日本の研究機関のサーバーの data という領域にある index.htm というファイルを、http 方式で転送せよ」というコマンドになる。リンクは、ファイルの中に書き込まれるもので、例えば、〈A HERF = http：//www. bbb. or. jp/b. htm〉画像〈/A〉といった形式となる。ユーザーのブラウザには、「画像」という文字が表示され、これをマウスでクリックすると、bbb という機関にある b.htm というファイルが表示されるのである（上記URLは共に架空）。

（2）WWWの場合は、ユーザーは、データのある場所をブラウザに入力するか、リンクをクリックするかして、データのオリジナルの「置き場」から直接転送することになるが、USENETは、自らの所属するLANまたは契約するプロバイダのニュースサーバーにアクセスして情報の送受信を行う。あるニュースハーバーのニュースグループに投稿されたデータは、「バケツリレー」のように隣接するサーバーのニュースグループに送られ、やがて当該グループを受信する設定になっている世界中の全てのニュースサーバーに到達する。

（3）ユーザーが表示するデータに関するプロバイダの責任については、小向太郎「インターネット・プロバイダーの責任―会員の情報発信をめぐって」（「ジュリスト」一一一七号・一九九七年八月）一九頁以下に詳しい。なお後掲三本文及び註（19）参照。

（4）ダイヤルアップ接続の場合、IPアドレスは、電話線を経由した接続が確立した時点で、プロバイダ側から一時的に割り振られる。従って、固定した番号ではなくなるため、このアドレスから、アクセスしている個人を特定することが難しくなる。なお、後掲三註（8）参照。

三　ネットワークをめぐる諸問題

上述のごとき「ネットワーク」は、今日の日本社会に爆発的に普及し、多くの利点と、同時に多くの問題を投げか

けている。様々な不正、違法な行為の出現である。コンピュータネットワークを道具として利用した違法行為、例えば詐欺といった事例や、コンピュータネットワークの性質抜きには考えられない不正侵入、データ盗用、猥褻図画陳列、著作権侵害など、まさに枚挙に遑ない状況といえよう。

こうした問題について、既に刑事処分がなされる例も見られるようになったが、既存の法体系でこれらに対応することの困難さも、はっきりと認識されつつある。

かかる不正行為が頻発していることは事実であるが、反面、それはネットワーク利用者という人々の間でのみ認知されることとなり、幸いなことに、社会全般に悪影響を与えるといった段階にまで達しているとはいえない。だからこそ、ネットワークの有用性を十分に生かしつつ、不正を排除し、新しいメディアの健全な発展を期するために、サイバーローの定立を目指すことが求められると考えるものである。

インターネットは、WWWの普及により、旧来のBBSと比較して視覚的効果が高めることが容易である。既存のマスメディアとは異なり、現時点ではそれを見ることのできる人が数的に限られるにしても、ユーザーに与える影響は大であり、一旦違法な状態が出現した場合、その波及的効果も少なくないと考えざるをえない。しかし、これが、まだ新しいメディアであることを併せ考える時、単純に規制を強化するのみでは、メディアとしての健全な発達を促すことはできないであろう。

もちろん、広範な規制のみを先行させるがごとき方法は、ネットワークの発展を阻害するのみであるし、憲法上の表現の自由を犯すといった事態も予想される。筆者が理想と考えるのは、最小限の法的規制と、それを有功ならしめるユーザー側の自主規制があいまって進展することである。

以下本章では、昨今のネットワークをめぐる諸問題のうち、刑法に触れるかまたはその可能性がある事例、あるいは現行法では対応不能であるが違反者に対して罰則を規定することが妥当と考えられる事例をいくつか紹介し、簡単

な分析を試みる。[1]

ところで、インターネットの出現によりネットワークは国境を越えるメディアとなり、いながらにして世界各国の情報を、ほとんど瞬時に入手できるようになった。反面、それが同時に、国境のない違法行為を発生せしめていることも理の当然である。従って、ネット上の不正行為を考える場合、まず第一に法管轄の決定が重要である。しかしながら、ネットワークという、国境のないメディアの出現に対処しうる法制度を持った国家はなく、[2]仮にそのような国家が存在したとしても、国境を越えて発生した被害にまで対処できるものではなく、国際的ルール策定までは、まだ長い時間を要するであろうことは論を俟たない。以下では、行為の態様をいくつかに分類し、基本的に行為地が日本国内の場合に限定した上で、現行法の適用を前提として考察を進めることとする。

（1）正常なトラフィックへの侵害行為

①　ウィルス等

まず、トラフィックに物理的な障害を発生させ、正常に運用されているネットワークの機能を低下、ないしは停止させるがごとき行為について考える。ネットワークの末端には、多くの場合、パーソナルコンピュータが接続されている現状においては、これらに対する侵害行為も、ネットワークを介して行いうる状態となった。即ち、コンピュータウィルスの問題である。[3]

コンピュータウィルスは、実行型ファイルの形式で配布され、それを起動すると、最悪の場合、ハードディスクが使用不能になるといった被害が発生する。従来、文書ファイルであれば、ウィルス的機能を付加することができなかったが、近年では、ワードプロセッサや表計算ソフトに装備された自動実行機能を悪用した「マクロウィルス」も出

現している。

ネットワークの普及以前においては、コンピュータウィルスの感染は、専らフロッピーディスク等の外部記録媒体を経由し、その移転には距離に比例した時間を要した。ところが、ネットワークを経由すると、瞬時に新種のウィルスが世界中に広まることもあり得る状態になったのである。

従来のウィルスへの対抗策は、検査、除去ソフトの利用、出所不明なプログラムを利用しない、といった個人レベルのもののみであったが、実際、この程度の注意で、ウィルスの被害を防ぐことができた。ネットワークを利用する場合でも、ネットを通じて配布されるプログラム使用の際に、同様の注意を払うことで対応が可能であったが、マクロウィルスの出現は、更に慎重な対応を、末端のユーザーに求める契機となるものである。

そして、今日では、インターネットでホームページを閲覧するにも、相当の注意を要することとなった。ホームページ記述言語であるHTMLの機能を拡張するための最新の技術を応用すると、あるページにアクセスしたコンピュータをリセットさせ、あるいはハードディスクをフォーマットさせるといったトラップも可能である。これによって生ずる被害は、停電でコンピュータが停止することと大差がないかもしれないが、たまたまアクセスした、行為者とは無関係のユーザーに被害を与える点から見れば、ウィルスと同等とも言える。

ウィルスの場合、それを作成、配布した者を特定することはきわめて困難であるが(4)、あえて、法規制の重用性を強調しておきたい。ウィルスには、画面に特定の文字を表示したり、あるいは音楽を演奏したりするだけで、コンピュータの機能に何ら影響を与えない「ジョークソフト」に類するものも存在するが、ユーザーが意図せずに起動し、あるいは意図するものとは異なる詐害的機能を実現するプログラムはみな、ウィルスと定義するべきで、ウィルスの配布行為そのものに対する処罰が必要であろう。その上で、発生した結果に対する加重処罰が可能であると考えられる。

ホームページ上にトラップを仕掛ける場合は、処罰の対象とするか否か、意見の分かれるところであろう。筆者は、

現状の技術水準から考え、ページ作成者がデータを置くサーバーの管理者との関係、プロバイダとの契約関係で対処しうると考えるが、技術が進み、更に高度な機能をホームページ上に装備できるようになれば、当然、処罰を含めた規制の範疇に盛り込まれるものと考える。

これらは、不特定のコンピュータ、あるいはネットワークユーザーを対象とする違法行為であるが、近時、「メール爆弾」と称するプログラムが、ネットワーク上で配布されている。これは、特定のメールアドレスに対して、連続して数千通のメールを発信するというもので、そのアドレスは、メールがあふれかえり、事実上使用不能な状態に陥る。それどころか、そのアドレスが存在するメールサーバーの処理能力を超えるメールが送り込まれれば、サーバーそのものが停止してしまい、結果、同じサーバー上にアドレスを有する全てのユーザーに、メール送受信不能という事態を引き起こすのである。この種のプログラムの配布行為は、ウィルスプログラムの配布と同様、処罰の対象となすことが必要であろう(5)。

上述の各種「仕掛け」に対する現行法の適用可能性を考えると、何らかの被害が発生した場合、電子計算機損壊等業務妨害罪の成立が考えられるが、それのみで十分とはいえないことは論を俟たないのである。

②　不正侵入

ネットワークへの不正侵入事例も大変に多い。他人が設置するサーバーに侵入し、データを閲覧、あるいは書き換えるという行為が頻繁に発生するという、極めて深刻な状態である(6)。

不正侵入の手口として最も一般的なものは、「他人への成りすまし」である。他人のネットワークＩＤとパスワードを何等かの方法で入手し、これを用いることで、自らはアクセス権のないネットワークに容易に侵入することができる。そして、「他人」としてあるネットワークに入り込み、そこから更に別のネットワークに不正侵入を働くという事

例も知られている。

既に諸方面で指摘されていることであるが、ネットワークＩＤとパスワードという、ネットワーク活用に不可欠な個人データの管理が杜撰であることが、大きな原因の一つといえる。また、無関係の第三者が容易にアクセスできるような「しくみ」を採用しているネットワークも存在してる。こうした不正侵入に対処するためには、まず、ネットワーク設置者、同管理者に、徹底した安全管理のための方策を採ることを求めなければならないだろう。と同時に、個々のユーザーにも、自らのＩＤとパスワードの管理を厳重にし、パスワードは定期的に変更するといった個別の安全策を採ることが求められるのである。

一方、法制面の整備も疎かにはできない。ネットワークに不正に侵入した何者かが、破壊的な行為を行ったのなら、電子計算機損壊等業務妨害罪をもって対応可能であるが、単に侵入しただけで、なにも壊さなかった場合、「覗き見」に等しい行動を取った場合は、対応は困難である。しかし、ネットワークへの不正侵入自体が、ネットワークというインフラへの信頼性を揺るがす重大な事象であること、つまり不正侵入は、多くの場合、③以下に述べる行為類型の発生基点となるに鑑み、何らかの法規正が必要であると考える。(7)

③　データ改竄

不正侵入を試みる者の対象は、高度な専門的情報を保有している研究機関や企業のサーバーだけとは限らない。一般のインターネットユーザーが通常目にするＷＷＷデータを保存するサーバーが対象となり、そこに置かれていたデータが改竄されるという事例も発生している。記憶に新しいところでは、所謂「朝日放送」事件があげられよう。(8)事件は、何者かによって朝日放送のホームページ上の天気図データが猥褻画像と置き換えられた、というものであるが、この事件は、当該ＷＷＷサーバーのセキュリティ対策が全くなされていなかったことを示した。通常、ＷＷＷサーバ

ーへのアクセスは、誰にでも許可される、というよりむしろ、誰にでも公開されているものであるが、許可されるのは置かれている「データの読み出し」のみであり、書込みができるとは考えない。書込みを行うためには、そのためのアクセス権を証明するＩＤとパスワードが求められることが一般的である。ところが朝日放送のサーバーには、書き込みに関する規正がなされていなかったものと思われる。

この問題は、不正侵入の発展形として位置付けることが可能であり、ネットワーク管理者によるセキュリティーの徹底が求められる。

ところで、一見して「偽物」であることが明白なデータが置かれたことで、この事件は直ちに発覚し、被疑者が逮捕されたが、もし真贋の判別が困難なデータが置かれたとしたら、事態は更に複雑となる。

現代社会において、「文書の真実性」が問題となる場合、第一に考えるべきことは、その文書が複写されたものであるかどうか、ということであろう。文書の発行権者が正規に作成した複写ではなく、第三者が複製を作成すると、文書そのものの有効性が失われることがある。その理由としては、真実性の証明として用いられる署名、印判を真正と確認することができなくなることが挙げられる。

肉筆の文書は、署名、印判以外にも、筆跡、筆圧等で真贋を判定することが可能である。しかし、電子化された文書では、これらの方法は一切使用できない。それどころか、紙をコピーする場合と異なり、何度複製してもデータが劣化することはない。そして、誰かが内容を改竄したとしても、真正なデータと比較検討しない限り、それと気がつくことはないのである。

こうした問題を回避することは、極めて困難であるといわざるをえない。しかし、可能な限り、このような被害を防ぐための努力を続けない限り、ネットワークは、真に成熟した新たなメディアとはなりえない。

④ データ盗用

ＢＢＳやプロバイダにアクセスする場合、一般に、ユーザーを識別し、かつアクセス権を認証するＩＤとパスワード（Password）が要求される。もっとも単純な個人情報の漏出形態としては、このＩＤとパスワードを他人に知られるという事態を挙げることができる。これは、必ずしも電気的な手段による必要はなく、ユーザーの手元を盗み見るといった、いたって原始的な手法でも実現する。ＩＤとパスワードを入手すれば、誰でも他人になりすましてネットに入ることができ、もし、そのネットワークが有料の場合、ＩＤとパスワードを不正に入手したものの使用料も、すべて本人に請求されることになるのである。(9)

ＢＢＳ、またプロバイダは、この不正利用を防ぐため、ユーザーにパスワードの変更を呼び掛けることが多い。ＩＤはＥ－Ｍａｉｌのアドレスとなることがあるため、完全に非公開とすることはできないが、パスワードは該当するユーザーのみが知りうる情報であり、任意の変更を許すことで、不正利用の危険を回避しようとする。と、同時に、パスワード管理の責任はユーザーにあることを明確にする意味を持つ。

ところが、ネットワークに不正に侵入した何者かが、そのネットワーク利用者のＩＤとパスワードを記録したデータを「盗み出し」不正に使用したり、公表したりするといった事例も発生している。(10)

また、ネットワークユーザーにとって潜在的危険性の高い問題は、ネット上に流れる信号を「盗み見」られることであろう。

インターネットは、既存のネットワークを高速通信線で結び付けて成立しているものであり、ネットワーク間の接続は、各ネットの「善意」に拠っている。そして、Ｗｅｂという言葉からも判るように、接続は一対一で確立しているのではなく、例えば、日本国内のある家庭から、合衆国のある大学に接続を試みた場合、信号の経路は無数に存在

するのである。つまり、日本の家庭から発せられた接続を求める信号は、途中、いくつものネットワークを経由し、目的のコンピュータに届く。そして、この経路は、その時々の回線使用状況によっても変わるものであり、ユーザーが指定することはできないのである。更に、送信されたデータが、複雑な経路の途中で行方不明になることもある。その場合、予期せぬ第三者がそのデータを見ないとは、決して断言できない。[11]

電話の盗聴と同じように、インターネットを流れる情報を盗み取ることは可能である。極言すれば、盗み見ができないような対策を施さずに流されたデータは、誰でも見ることが可能なのである。

たが、インターネットを始めとするネットワークを流れるデータすべてに、厳重な「盗聴」防止策が必要かというと、必ずしもそうとは言い切れない。E－Mailにしても、日常会話程度の内容しか持たないものも多いし、盗み見をした第三者に理解できる「会話」とも限らない。膨大なトラフィックを発生させるWWWデータにしても、不特定への公開を前提としているものが大半であることを考えると、データに対するセキュリティは、専ら送り手の認識に応じて考慮されるべきものとも言えよう。

（2）不正常なデータの送信

次に、ネットワーク、または端末コンピュータの機能に影響を与えることはないが、ネット上に流されるデータ自体に問題があるケースについて考える。

①猥褻図画の掲出

国内におけるインターネット上の猥褻図画に関する事例[12]として、嚆矢ともいえるのが「ベッコアメ事件」である。この事件では、外国のホームページから入手した猥褻画像を、ホームページから参照可能な状態にした被疑者二名が

逮捕、補導された。[13][14]

この後も、猥褻図画の頒布行為を行うものは跡を絶たず、規制の必要性が叫ばれている。判例は、押し並べて現行刑法の猥褻図画陳列の成立を認めるが、最近では、ネットワークの特質から発する「リンク」の性格が争われる事態が生じている。現在係争中の「大阪FLマスク事件」は、インターネット猥褻事犯に関する画期となる可能性を持つものと考える。被告人は、専ら猥褻画像に可逆的修正を加える目的のみで使用される「FLマスク」と称するプログラムを、シェアウェアとして[15]頒布し、多数の利用者から二千万円に及ぶ利益を得た。そして、FLマスクを置いた自己のホームページから、猥褻画像を掲示したホームページへのリンクを設置したことが、猥褻図画陳列幇助に問われている。[16]

このようなホームページを利用した猥褻図画の掲出事例は跡を絶たない。しかし、より重大な違法性を持つ可能性のあるメディアは、「ネットニュース」である。

既述のとおり、ネットニュースは、インターネットの実験開始時点から広く利用されているサービスであり、WWWの大流行の影に隠れて注目されることは少ないようであるが、今日世界中で三万以上のグループが稼動している。ネットニュースは初期に発達したサービスであるため、送受信されるのは「文字データ」である。従って、我が国では、簡単な操作で画像や音声までも受信できるWWWがユーザーの嗜好と一致したようであるが、一方、ネットニュースには様々なテーマが設けられており、我が国の刑法では猥褻と定義される可能性の高い画像を専門にやり取りするグループも多数存在する。データのやり取りは、画像やその他の文字以外のデータを一定の方式で「文字化」し、特定グループに「投稿」する。投稿されたデータは、そのグループを受信するプロバイダ、あるいはLANのニュースサーバーに転送され、それぞれのプロバイダに契約するユーザー、LANの利用権を持つユーザーは、自らのニュースサーバーにアクセスしてデータを取り出し、必要に応じて画像等の形式に復元することができるのである。「文字

化」、「復元」をそれぞれ、ＥＮＣＯＤＥ、ＤＥＣＯＤＥといい、専用のプログラムを必要とした。また「文字化」の方式にもは様々な種類があり、「復元」するためにはどの方式で文字化されたものか、判別する必要があった。

しかし、インターネット関連ソフトウェアの急激な進化により、今やユーザーは、文字化されていることすら意識することなく、データを受信し、また送信することが出来るようになっている。ＷＷＷと全く同様に、画像やプログラム、音声など、文字以外のデータを入手できるのである。

ホームページを利用した猥褻図画掲出の場合、画像データは、行為者が利用するＷＷＷサーバーの上のみに置かれている。しかしネットニュースに猥褻画像を投稿した場合、データは世界中のニュースサーバーに「配信」され、まさに無数に存在することになるのである。[17]

猥褻図画を野放しにすることは、到底許されないであろう。しかし、現行刑法の規定にのみ依存して、現今の多様なネットワーク社会を律することは困難である。[18]ネットを経由して頒布される猥褻画像等の増加に対応し、プロバイダに監視、削除などの義務を負わせるべきか、との議論がなされているが、プロバイダに「検閲」を許すような方向に進むことは避けなければならない。蓋し、インターネットは優れて「無政府的」に発達したボランタリーなネットワークだからである。アクセスするものの年齢によるフィルタリングなど、早急に着手が可能な方策を進めるとともに、[19]刑法の猥褻規定についても、再考を要する時期に来ていると考えるものである。

②　名誉毀損

ネットワークの匿名性を悪用した名誉毀損事例も、近時増加しつつあるように感じられる。

ネットワーク上で一般社会における「氏名」に相当するものは、「メールアドレス」や「ＩＰアドレス」と呼ばれる一種の符号である。これらは、ネットワークの通信機の鵜を実現するために企画化された様式に則って付されるもの

で、符号から直ちに利用者本人を特定することは難しい。このほか、従来のBBSのユーザーの間で「ハンドルネーム」という通称を利用することが習慣化しており、これがインターネットにもそのまま用いられている。これも、本人特定に結び付くものではない。

BBSにおいて広く利用されていたサービスに、電子掲示板がある。これはBBS管理者が用意する掲示板であり、ユーザーは、ハンドルネームを表示してここに意見を書込む。掲示板上での意見交換は、相手の顔が見えないという事情が災いして、とかく過激になりやすいことが指摘されているが、BBS管理者が一定の基準を設け、発言の交通整理を行ったり、不穏当な発言を削除することで、秩序を維持していた。

インターネットでは、同様のサービスとして「ネットニュース」があるが、近時のユーザーが最も利用していると思われるWWWとは別の形態で提供されるサービスであるため、日本ではこれまであまり注目されることはなかった。ところが、WWWの上に、特定のプログラムを機能させて電子掲示板を実現することができるようになり、事情は一変する。

再三述べているように、インターネットは優れて無政府的なメディアであり、そこで誰でも簡単にアクセスできる掲示板が出現すると、匿名性[20]を背景とする違法行為を招くことになりかねないのである。筆者が偶目した範囲に限定しても、発信者のアドレスを何等かの方法で秘匿した上で、当該掲示板の主催者や参加者を誹謗中傷する発言を掲載したり、あるいは無意味なデータを大量に掲示して掲示板の機能そのものを停止させてしまうといった例もみられる。更には、自らの発言の中に、外国のサーバーに存在する猥褻画像のURLをリンクさせたり、画像自体を表示させるといった、悪質な嫌がらせも行われることがある。こうした「掲示板荒らし」と呼ばれる行為に現行法で対処することは困難であると言わざるをえない。

そして、このWWW上の掲示板において他者の名誉を毀損したり、あるいは侮辱するという事例が発生し、有罪判

決が下ったことは記憶に新しい。[21]

一旦、ネットワークに流された情報は、これを完全に消去することはもちろん、伝達経路を追尾することすら事実上不可能であり、[22]ネットワーク上に、特定の害意をもって何らかの不正な情報を掲出すること自体について、何らかの規制が考えられるべきであろう。こうした場合、情報掲示を可能ならしめたプロバイダ、あるいは掲示板設置者に、管理義務を負わせることも考えられよう。[23]

このように、ネット上で、他人の名誉を毀損する発言がなされた場合、行為者の国籍を問わず日本国内からなされた発言、あるいは日本人が行った発言が、日本人の名誉を毀損したのであれば、名誉毀損罪等の成立の余地があろう。では、国外から、日本人以外のものが行った発言が、日本人の名誉を毀損した場合、どのように考えられるであろうか。[24]発言者は、日本法の管轄下にはない。しかし、行為の結果は日本で発生するようなケースを、明治四一年に施行された現行刑法は、全く想定していない。

また、一旦ネットに流された発言等は、以後、どこに転送され、第三者の目に触れるか、発信人すら想像できない。ネットを経由した発言は、容易に世界中に広がる可能性を持っており、何人かの名誉を毀損する恐れのある、あるいは何人かの利益に反する発言が、一旦ネットに公表されると、それがどの程度流布するか、ということを予測することはできないのが現状といえる。

（3）その他の問題

以上言及した問題点は、何れも既発の事例を簡単に取り上げたものであるが、ネットワーク技術の著しい進歩は、今後、全く未知の違法行為をももたらす可能性を十分に持っている。筆者が現在注目している問題として、「プロクシーサーバーの悪用」がある。

プロクシーサーバーは、ネットワークと外部との接点に設けられるもので、内部から外部へ、必要以上のトラフィックを発生させないために活用される重要なサーバーである。通常、インターネットに接続されたLANはもとより、民生用プロバイダーも大半がこれを設置する。

一般のユーザーから見ると、このプロクシーは、「代理サーバー」として機能する。これは、プロクシーを経由してWWW等にアクセスした場合、ユーザーのコンピュータに表示されるデータは同時に、プロクシーにも貯えられるのである。次に他のユーザーから同じWWWデータへのアクセスがあったとき、プロクシーは、自分が貯えているデータをユーザーに送る。こうすることにより、ユーザーにはより高速にデータが転送され、外部に対しては同じデータの転送によるトラフィックの発生を止めるという二重の効果が期待されるのである。

ということは、多くの会員を要する大規模なプロバイダのプロクシーには、「人気」のあるWWWデータは常に貯えられるであろうし、小規模プロバイダのプロクシーを経由しても、経路が長くなるだけでユーザーの利点は少ない。そのため、「公開プロクシー」という実験が行われつつあるやに仄聞している。これは、ある機関が自らのプロクシーサーバーを、その機関とは直接関係のない一般ユーザーに開放し、ネットワークの「渋滞」対策の一助としようというものである。ところがこうした例を除けば、プロクシーは、個々のプロバイダやLANのために設置される機構であり、当然、当該プロバイダあるいはLANのメンバー以外が利用することを前提としていない。

ではあるが、近時、ネットワーク上で、プロバイダや研究機関のプロクシー情報が流されている。このデータを入手したものは、自らが当然利用できるプロクシーに代えて、大手や、より高速と考えられるプロクシーにただ乗りすることができるのである。

プロクシーに貯えられたデータに財物性を認めることができない以上、この行為自体を直ちに違法と考えることはできない。[25] しかし、特定のプロバイダのプロクシーに、外部から処理能力を超えるアクセスが殺到した場合、最悪、

そのプロクシー周辺のトラフィックが停止することも考えなければならない。とすると、当該プロバイダの正規の利用者の権利を侵害し、プロバイダの業務を妨害することとなるのではないか。プロクシー設置者には、外部からのアクセスを許すか否か、明確に決定する必要があるものと考える。

もう一つ、プロクシーには、特殊な機能がある。そこを経由してアクセスするものの「アドレス」を隠すことができるのである。プロクシーから先のサーバーには、プロクシーのアドレスのみが伝えられることになり、ネットワークの匿名性を一層強化することにもなるのである。「匿名性」そのものについては、決してこれを否定するものではないが、害意を持ったネットワークユーザー、あえて言うならばクラッカーが、自らの痕跡を消すために、不正にアクセス権のないプロクシーを利用することまで許容する必要はない。プロバイダは、トラフィック軽減のためにプロクシーの利用を推奨する傾向にあるが、上述のごとき現状も範疇に入れ、今後の技術の進展と、ネットワーク社会の自発的秩序形成の過程で、検討を要する課題であろう。

（1）ネットワーク上の犯罪行為に関しては、近年優れた研究が多く発表されているが、ここでは特に、稲垣隆一「インターネット犯罪をどう防ぐか」（藤原宏高編「サイバースペースと法規制」日本経済新聞社・一九九七年一〇月所収）二八五頁以下を参照した。

（2）例えば、A国のホームページから入手したデータを、B国のホームページで公開した場合、B国法で処罰の対象となる可能性がある。近時、カナダのプロバイダにあるホームページに「ナチズム」を肯定する発言が掲載されたことがあったが、これは、ネオナチ活動家がドイツ国内での規制を逃れるため、海外のサーバーにホームページを開いたものであった。ドイツ政府には、カナダのプロバイダの活動を制限する権限はなく、各国政府に対して「規制」を求めた（「毎日新聞」一九九六年一二月二一日朝刊）。

同様に、日本国内のプロバイダではなく、海外のプロバイダにホームページを開設し、猥褻図画を掲出している事例も散見せられる。この点に関しては後継本文及び註（14）参照。

（3）我が国におけるコンピュータウィルスの被害も、近年激増している。通産相の外郭団体である情報処理振興事業協会（ＩＰＡ）に

よると、一九九七年一月から九月までの届け出件数は一七八〇件余を数え、過去最高だった一九九四年を越えたという(「朝日新聞」一九九七年一〇月三〇日朝刊)。

(4) ウィルス作成者から直接感染するケースは希で、多くの場合、ウィルスに感染した他の実行型ファイルを起動することで被害が発生する。「潜伏期間」をおいてから発症するウィルスの場合には、ユーザー、あるいは善意のプログラム作成者、提供者の知らぬ間にウィルスに感染することもあり、経路の特定、第一の加害者の特定は困難である。

(5) メール爆弾を入手、使用できる程度のネットワークに関する知識を有するユーザーは、匿名化ホームページ(後掲註(22)参照)を経由する、等の方法で、発信元を秘匿するものと考えられ、発信者を確認することは困難であろうと思われる。結果、一旦被害が発生すると、受け手のサーバーが機能を停止するまで、または、爆弾プログラムの設定送信数が完了するまで、被害は継続することとなり、影響は甚大となる。

(6) 新聞報道によると、我が国の通信技術研究の最先端にあるNTT情報通信研究所のコンピュータが何者かによって不正な侵入を受けたという。行為者は、インターネットで入手したり自作したりした通称ハッキングツールというプログラムを使って、ネットワークの管理者になりすまし、該コンピュータに侵入したという。また、東京大学大型計算機センターが不正侵入の被害を受けたことが明らかとなっている(「毎日新聞」一九九七年一〇月六日朝刊、同日夕刊、同一〇月一六日朝刊)。この他にも、著名な大学や研究機関のコンピュータが多数「被害」を受けているといわれるが、実態は公表されにくい傾向にある。蓋し、高度な情報を集積した研究機関等の、外部からの侵入に対するセキュリティが不十分であることを示す結果になるからである。

なお、日本では、不正侵入者をハッカー(Hacker)と呼称する例が多く見られるが、この表現は正しくない。このためハッカーには、ネットワークの破壊を行うもの、といったネガティブなイメージが定着しているが、本来は、コンピュータハードウェア、ネットワーク技術に通暁したユーザー、という意味の隠語で、MITが発祥であるという。それが、破壊者として定着してしまっているわけだが、筆者は、マイナスの意味でのハッカーという語は使用せず、不正侵入者と標記し、データの破壊等が加わった場合にはクラッカー(Cracker)との表記も用いることとする。

(7) この問題に関しては、社会安全研究財団情報セキュリティ調査研究会が、九七年四月に法的規制の必要性を主張する報告を行っている(「毎日新聞」一九九七年一〇月八日夕刊)。

(8) 九七年五月、大阪市の朝日放送が開設するホームページの天気予報画面が、女性の裸体写真と置き換えられるという事件が発生し

た。数日後、容疑者が逮捕されたが、容疑者は、偽名と偽クレジットカードとを使ってプロバイダと契約し、ダイヤルアップ接続でインターネットに入り、該ホームページにいかがわしい写真を転送した。捜査当局は、朝日放送のホームページに残された「アクセスログ」という記録からプロバイダを特定し、プロバイダ側の接続記録から容疑者を割り出した（以上「読売新聞」一九九七年五月一九日朝刊、二三日夕刊）。セキュリティ対策が不十分なホームページでは、データの書換えがいかに容易かを示す例となった。

この事例は、猥褻な画像の掲出という、一種の典型的ネットワーク犯罪であったため、猥褻図画公然陳列と偽計業務妨害の刑責が問われたが、では、不正侵入者が、置き換えではなくネット上のデータを破壊した場合はどうだろうか。ネット上のデータは、電磁的記録であるが、これが財物であるかどうかは意見が分かれるであろう。財物であるとすることができないなら、器物損壊の罪に問うことはできない。データの破壊によって被害者の業務を妨害した場合のみ、刑責を問いうると考えられるが、これに当たらない場合、例えば、個人が趣味で開設しているホームページのデータを破壊したような場合には、刑責の追求は困難である。そしてこれらの場合、被害者は、不法行為による損害賠償請求を行いうるが、加害者の特定が第一の難関となることは疑いない。不正侵入者にとっては、自分自身を含め、全てのアクセス記録を消し去ることもありうるのである。そうしないまでも、世界中に無数にあるコンピュータのなかの一台を操る不正侵入者を特定することは、決して容易ではない。

(9) 前掲註(6)に掲げた東京大学大型計算機センターの事例は、ＩＤ、パスワードの盗用の典型である。他人のパスワードを利用し、有料ネットワークにアクセスした場合、この行為は、「電算機利用詐欺罪」を構成すると考えられが、しかし、実際に生じた被害を確定することは困難である。ネットワークは、パスワードが正しければ、全て、真正なアクセスとして接続を行うのであり、その中に含まれる「不正なアクセス」を峻別する技術が存在しないのである。勿論、真のユーザーによるアクセスが、全く不可能である期間中に、同人のパスワードを使用するものがあれば、不正を確定することができるが、それ以外は、事実上、野放しにせざるをえない状態なのである。

(10) 最近の報道に見られるだけでも、複数の大手プロバイダが不正侵入の被害を受け、個人データが流出したことが明らかとなっている。（「毎日新聞」一九九七年一二月二九日朝刊）。しかし、こうした事例において、行為者が特定のファイルを「見た」としても、当該ファイルの占有は移転しておらず、盗犯として処罰することができない。

(11) 「オンラインショッピング」等の決済方法として、ネット上でクレジットカードの番号を入力させる方式が行われているが、この

番号が盗用される危険があることは早くから指摘されている。特にインターネットを利用したカード決済は、暗号化等の手段を講じない限り、危険であるといわざるをえない。なお、暗号化に関し、現在注目されている方式の一つに、PGP（Pretty Good Privacy）と呼ばれる「公開鍵」暗号がある。「公開鍵」とは、まず、データの受信者が「錠前」と「鍵」に相当する暗号コードを作成し、「錠前」だけを公開する。公開の方式は、E－Mail、WWWへの搭載などどのような方法でも良い。データを送ろうとするものは、この「錠前」を入手し、送信すべきデータに「錠前」で鍵を掛ける、即ち、暗号化を行い、しかる後、これをネットを通じて受信者に送る。受信者は、あらかじめ作成しておいた「鍵」を使い、暗号化されて送られたデータを復元するのである。「錠前」は、いくら公開しておいても、それだけでは暗号化にしか用いることができず、復号して内容を取り出すことは、「鍵」の作成者にしかできない、という要領なのである。「錠前」にあたるのは、一見すると無意味な文字の羅列で、通常一KB（一〇二四byte）という大きさである。これを元に、「鍵」を用いずに暗号を解読しようとすることは、極めて困難であると考えられている。なおPGPに関してはhttp：//ac3. aimcom. co. jp/~macpgp/に詳しい。

(12) ネットワーク上の猥褻データに関しては、園田寿「サイバーポルノと刑法」（「法学セミナー」五〇一号・一九九六年九月）四頁以下、前田雅英「インターネットとわいせつ犯罪」（「ジュリスト」一一二号・一九九七年六月）七七頁以下、前傾稲垣「インターネット犯罪をどう防ぐか」二九五頁以下、山口厚「コンピュータ・ネットワークと法」（「ジュリスト」一一七号・一九九七年八月）七三頁以下を参照した。また園田教授のホームページ（http：//w3. scan. or. jp/sonoda/）では、極めて貴重な情報の閲覧が可能である。

(13) 容疑者のうち、青年者に対しては、一九九六年四月二二日、東京地裁において懲役一年六月執行猶予三年の有罪判決が言い渡され、確定した（「判例タイムズ」九二九号・二六六頁）。

(14) ベッコアメ事件の容疑者の一人は、自らのホームページを示すリンクを、海外のサーバーに置き、一旦海外のサーバーのデータを閲覧しなければリンクを辿れない構造を作っていた。この後、猥褻画像データの置かれたホームページが海外にある場合は摘発されないという状況が見られたが、国内に居住するものが国内からデータを発信し、且つ、閲覧希望者から振り込まれる代金の受け取り口座を国内に開設していた事例で摘発が行われた。データが海外に置かれているという事情を除けば、行為の一切が国内で行われていると認定されたものである（「朝日新聞」一九九七年二月一一日朝刊）。

(15) シェアウェアは、一定期間試験的に使用した後、継続を希望するユーザーは代金を支払う形式のソフトウェア。

（16）この事件に関しては、牧野二郎弁護士のホームページ（http：//www. asahi-net. or. jp/~VR5J-MKN/）に詳しい。

（17）前掲二本文及び註（2）参照。

（18）インターネット上の猥褻図画陳列に関する判例は既に数件を数えるが、直近の平成九年一二月岡山地裁判決（http：//www. asahi-net. or. jp/~VR5J-MKN/okayama. htm）は、該事例の困難さを露呈したものと考えられよう。従来の判例では、陳列された猥褻物を有体物に限定して解釈するために、コンピュータに接続され、猥褻な画像データを蔵置しているハードディスクを「猥褻物」と判示してきた。しかしながら、この解釈には疑問を禁じえない。蓋し、これまでの猥褻事犯の「猥褻物」は、可視的な状態にあるものとしては写真、図書等の印刷物、不可視な状態にあるものとしてはビデオテープ、フロッピーディスク、CD－ROMなどがあるが、これらに共通するのは、その可搬性である。翻って言うならば、可搬性即ち客体の占有の移転がなされるという意味である。この点で、一般的にコンピュータ内部に固定されるハードディスクを猥褻物と考えることには抵抗を感じる。

ところが岡山地裁は、上述の判決において、ハードディスクではなく、ハードディスクに記録された「画像データ」を猥褻物と認定した。ハードディスクよりもデータのほうがより実態に近いと考えらるが、法の改正を待たずにこれまで固守してきた有体物概念を否定することは、処罰対象範囲を拡大しすぎる恐れが強い。しかも該判決では、FLマスク等によって可逆的な修正を加えた画像を、「復元が容易である」との理由で猥褻と認定している。この点に関しても、解釈の範囲を広げすぎるとの批判があてはまるものと考える。なお、この判決以前に、「電磁化され」た画像データも一七五条の図画にあたるとの指摘は、堀内捷三「インターネットとポルノグラフィー」（「研修」五五八号・一九九七年六月）三頁以下に見られる。

（19）郵政省は、九七年一一月、インターネットを利用して、猥褻図画等を含む有害情報規制に関するアンケートを実施した（このアンケートに関しては郵政省ホームページ（http：//www. mpt. go. jp/pressrelease/japanese/new/980105j601. html）参照）。そこでは、有害情報が置かれた場合にプロバイダに削除の責任を負わせるべきか、といった選択肢が存在していたが、筆者はこれには基本的に反対である。なるほど、ホームページに限って考えるならば、それは不特定に対する「公開」を前提としているもので、むしろ「放送」に近いメディアと位置付けることが可能であり、現行の通信事業者に対する「通信の秘密」保持という義務は生じないかもしれない（プロバイダは通信事業者である）。ではあるが、仮に、猥褻図画に限定したとしても、猥褻の定義自体が確定的でない現在の日本の状況下で、プロバイダがデータ削除を強行することは、表現の自由への直接の侵害にあたる可能性が大きいものと危惧する。削除という強制的行為を正当化するためには、少なくとも内容を評価する第三者機関のような組織が必要となるだ

ろうし、その経費までユーザーに負担させることとなれば、インターネット先進国であるアメリカ合衆国と比して極めて割高な日本のインターネットコストを一層引き上げる結果となり、このメディアの発展を著しく阻害する。プロバイダにかかる義務を負わせるとすれば、ブラウザソフトと、青少年保護のために「有害情報」へのアクセスを不可能にするフィルタソフトの併用を義務づけ、データを公開する者にフィルタで識別できるコードのような符号を付けることを求めることから始めるべきではないだろうか。フィルタコードを付さずに「有害」データを公開する者があった場合、始めてプロバイダの強制的削除を認めても遅くはないのである。

なお、風俗営業法の改正案で、ネットワーク上の猥褻情報に関しても規制を行う方針が示された(「読売新聞」一九九八年二月一三日朝刊)。同法改正案では、プロバイダに「努力義務」を課しているが、実効性は疑わしい。

(20) 既に述べたようにインターネット上では、接続されたコンピュータにIPアドレスという符号が付されるが、それを操作する個人を特定する何物も存在しないのが実情である。掲示板サービスでは、書込みを行う者に実名を要求することは不可能であり、多くの場合、便宜的な「通称」を求めるに過ぎない。

(21) インターネットの掲示板を使った名誉毀損、侮辱事例としては、九七年一一月、続けて二件が報道された。一件は秋田、他の一件は東京で起ったものであるが、いずれも、実在の女性の氏名や電話番号と、当該女性を侮辱しあるいは中傷する内容の文章を掲出したものである(「読売新聞」一九九七年一一月二〇日夕刊、二七日夕刊)

(22) メールやニュースグループへの投稿記事は、ある程度まで経路をたどることができる。しかしながら、我が国のインターネットユーザーの大半が、「ダイヤルアップ」式接続を用いていることから、完全な経路追尾を困難にしている。ダイヤルアップ式の場合、ネットワーク上の「番地」に相当するIPアドレスは固有のものではなく、接続のたびにプロバイダによって割り振られるため、直ちに行為者を特定することができないのである。匿名化ホームページを経由した場合などは更に事情は悪化する。アクセスを受けた側に残るアクセスログには、匿名化ホームページ以前の経路情報は一切失われ、アクセスをした者を特定することは不可能となる。

(23) 掲示板管理者が、自らの掲示板に、書き込み禁止となる情報の種類を明示したり、書込みがなされた場合に削除する旨を宣言するといった場合も見られる。第一義的には設置者が、二義的にプロバイダが責任を負うという体系を確立することは、困難ではないであろう。

ＢＢＳにおいては、掲示板に投稿された記事を設置者が削除するという例が見られる。例えば、ＢＢＳの大手ニフティサーブは、神戸で発生した連続児童殺傷事件に際し、同社設置の掲示板に投稿された、容疑者の顔写真を販売するという趣旨の発言を、「公序良俗に反する発言は削除する」との会員規約に触れるとの理由で削除した（「毎日新聞」一九九七年七月三日朝刊）。同じ児童殺傷事件に際し、筆者は、インターネット上で、個人の開設する複数の掲示板に、被疑者である少年の氏名と思しき記載が多数書き込まれたことを確認している。また、個人の開設するホームページには、雑誌に掲載された少年の顔写真が掲載された。これらの行為は、少年法の趣旨に反する重大な問題であるが、その後、具体的な対応がなされたか否かは判然としない。クローズドネットワークであるＢＢＳでは、設置者の強制力である程度の秩序維持が可能となるが、全体としての管理者は存在しないインターネットの場合は、現実にデータを管理する者（例えば掲示板設置者）に管理責任を問うこととなろう。

(24) インターネット上で、橋本竜太郎総理の名をかたり、尖閣列島の帰属をめぐって反日運動が広がっている台湾、香港に、活動家を刺激するような内容の投書を行った者があった。海外に現れた「偽発言」に対し日本国内法での対応は不可能であり、官邸のホームページに、こうした投書がにせものであることを訴える、次のような文書が掲載された。

インターネット上で、ネットニュースや特定のホームページ上に、橋本総理や首相官邸の名をつかって、ニセのメッセージを発信しているものが出現していますが、これらは当首相官邸とは一切関わりがないことを、念のため、お断りいたします。
(http：//www. kantei. go. jp：80/index. html)

しかし、この掲示を見るためには、官邸のホームページにアクセスしなければならない。日本の首相官邸のホームページにアクセスしようとしないまま、橋本総理名で出された過激な文章を、真実だと考える者がいたとしても不思議はないのである。

(25) インターネットにおいては、データの流れる経路をユーザーが指定することはできない。特定のプロクシーを指定してデータ受信を試みた場合でも、中継点の一つを指定するに過ぎず、当該プロクシーを設置するサーバーに若干の負荷をかける程度となる。

四　対応策私案　むすびにかえて

これまで述べたことは、ネットワークをめぐって発生した、あるいは今後発生が予想される問題の、ほんの一部である。そして、繰り返しになるが、ネットワークという概念すら存在しない時期に整備された我国の現行法体制では、これらの問題に十分に対処することはできないのである。

しかし、急激に増殖を続けるネットワークに対し、法的に無策であったり、あるいは旧来の法規の解釈を拡張して対応することは、決して望ましいとは考えられない。

もちろん、まず考えるべきことは、ネットワーク、特にインターネットの発達により、今、目の前にあるコンピュータは、国内に止まらず、世界中のいたるところから有用無用な情報を表示する機能を持った、ということである。つまり、一国の法律をもって律しきれない世界が、容易に出現するのである。

ただ、一国で対処できる、あるいはすべきである問題には、早急に着手する必要があろう。例えば、「ネットワークへの不正侵入」に対して、刑事罰をもって臨むことも、検討すべきである。既述のとおり、現在、クラッカーによる被害が発生したとしても、データが破壊されない限り、法的に対処することは困難である。技術的な問題は一応おくとして、資格のない者がネットワークに不正に侵入する行為自体を処罰する規定がなければ、クラッカーに対する根本的対策を講じることは不可能である。

同様に、不正に入手した情報の利用に付いても、処罰を検討すべきであると考える。出所の不明確な情報の利用を法的に規正し、情報を盗み見、それを第三者に提供して利益を得、また第三者に利益を得せしめる行為を併せて処罰対象とし、情報盗用に対する強力な対抗策とすることを提言したい。

ネット上を流れる個人情報は、誰がどのようなネットワークに入っているか、何時、どのようなデータを入手した

かなど、さまざまなものが考えられるが、これらはすべてプライバシーの範疇に属し、厳格に保護される必要がある。これを不正に入手し、あるいはこれをもとに利益を得るものがあれば、それはネットワークに対するユーザー全体、ひいては全世界のネットワーク利用者にとって、計り知れない不利益をもたらすのである。

不正な侵入を監視する技術は、必ずしも、実用の域に達しているとは言いがたい。この点については、今後の技術革新に期待せざるをえないが、末端で、不正に入手された、言い換えれば出所を明確にできない情報を利用するものを把握することは、さほど困難ではなかろう。近時、組織犯罪に対処するため、不正な利益の没収などを含む法律の制定が検討されているが、ネットワーク上の犯罪についても、早急に対策を講ずる必要があろう。

ここでは、刑法分野に限定して卑見を述べた。しかし、ネットワークをめぐる法律問題が、ひとり刑法に限定して発生するという意味ではない。そこでは、ネットに掲載された文書、図画、音楽、コンピュータプログラム等、あらゆるデータに関する著作権を始めとする知的所有権の問題、マスコミにおいて、ポルノグラフィーなどを通じて表面化する表現の自由に関する憲法問題、不法行為など民事上の問題、さらには、国境のないネットワークに宿命的に存在する管轄権の問題など、枚挙に遑ない。これら、現在認識可能な問題に加え、ネットの普及と技術革新を引き金として、様々な問題が新たに発生してくることは必定といえよう。そのため我々は、ネットワークという仮想現実空間と現実の世界とを架橋し、交通整理をするための新たな法分野、サイバーローに取り組む必要があるのである。

ただ、サイバーローを確立するためであっても、国家レベルの性急な規制には反対することを重ねて強調しておきたい。なぜならば、現在、世界中の立法、司法機関で、ネットワーク社会が十分に認識されているとは言い難いからである。仮に、ポルノや犯罪に結び付く情報が流れる可能性があるからといって、ネットワークを利用すること全体に直結しかねない規制を先行させたならば、ネットワークの健全な発達すら期待できなくなるからである。

ここで述べた立法への期待は、サイバーローの中でももっとも現実の空間に近く、かつ、現実に発生しつつある危

機に対処するための最低限の規制であり、ネットワーク自身の自己防衛のために必要なものなのである。

補註　本稿脱稿後、警察庁がネットワーク犯罪対策のために法的整備に乗り出す旨が報道された。内容については詳らかでないが、今後とも注目していきたいと考える。

本稿執筆にあたり、平成九年度北陸大学特別研究助成金の交付を受けた。規程によりここに記す。