オープンプロキシの利用について

原　禎嗣

はしがき

インターネットの急速な普及に伴い、その多彩な利便性が喧伝されると同時に、従来の法体系が予想しなかった不正、違法行為の発生を見ることとなった。サイバーポルノ、ウィルス送信、ＩＤの不正使用、名誉毀損、著作権侵害など、遺憾ながら枚挙に遑ないという現状である。

平成一二年二月、「不正アクセス行為の禁止等に関する法律」[1]（以下、不正アクセス禁止法と略す）が施行され、これまでは処罰できなかったネットワークへの不正な侵入行為が処罰対象となり、平成一三年には「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」[2]（以下、プロバイダ法と略す）が成立し、ネット上の権利侵害における責任の範囲に道筋がつけられた。これら両法は、ハイテク犯罪など、インターネットにまつわるマイナスな部分への法的対処として画期となるものであるが、その実効性に関し、危惧を抱かざるをえない点も存する。

何故に危惧を抱くか。それは、インターネットの持つ「匿名性」ゆえである。インターネット上では、接続されたコンピュータ一つ一つにＩＰアドレスが割り振られて識別がなされるが、そのコンピューターを実際に操作する

人格を識別することは、現時点では一般的ではない。インターネットカフェで、一台の端末を複数人が連続して使用したとしても、ＩＰは変わらない。この匿名性が、極めて重要なインターネットの特徴であり普及の一因でもあるが、同時に、匿名性を悪用し、反社会的用法を試みる者も跡を絶たないのである。

匿名といっても、ＩＰアドレスという識別符号は存在する。その識別符号から、コンピュータの使用者を割り出すことは不可能ではない[3]。ところが、インターネットにある程度習熟した利用者は、自分のコンピュータに割り振られたＩＰアドレスを秘匿、改変することができる。本稿で取り上げるオープンプロキシは、世界中に無数に存在するプロキシサーバーの「ある状態」[4]をさすが、これをＩＰアドレス秘匿のために用いることが可能なのである。筆者の所属大学においても、短期間だがプロキシがオープン状態にあり、その際のログの一部を閲覧する機会に恵まれた[5]。

筆者は、コンピュータとインターネットを常用する法律研究者の一人として、かつて、サイバーローに関する小考を発表した[6]。以下本稿においては、右のログに関する分析を踏まえ、前稿で十分に掘り下げることができなかった、インターネットの匿名性という特質と、二つの新法に関わる問題とについていささかの愚見を呈し、大方のご批判を待ちたいと思う。

(1) 同法については、園田寿「不正アクセス」(http://w3.scan.or.jp/sonoda/text/access/access.html)、黒澤正和「不正アクセス行為の禁止等に関する法律の制定について」、北村博文「不正アクセス行為の禁止等に関する法律の制定の経緯」、露木康浩、砂田務、檜垣重臣「不正アクセス行為の禁止等に関する法律の解説」(以上「特集・ハイテク犯罪対策法制の整備―不正アクセス禁止法を中心として―」(『警察学論集』第五二巻第一一号・一頁以下・平成一一年一一月)所載)、露木康浩「不正アクセス禁止法の意義と今後の課題」(『警察政策』第二巻第一号・一五九頁以下・平成一二年二月)、園田寿、野村隆昌、山川健『ハッカーＶＳ．不正アクセス禁止法』平成一二年六月に、詳細な検討が見られる。

(2) 同法については、総務省ホームページの同法に関する項目（http://www.soumu.go.jp/joho_tsusin/top/denki_h.html）以下に掲載された各資料を参照した。

(3) たとえば「朝日放送ホームページ書換事件」（「読売新聞」一九九七年五月一九日朝刊、二三日夕刊）は、このＩＰアドレスが容疑者特定の重要な手がかりとなった事件である。

(4) ローカルエリアネットワーク（ＬＡＮ）では通常、不正な侵入を防止するため、直接インターネットに接続することができないようになっていることが多い。このためＬＡＮ内部からインターネットへ接続する場合には、ＬＡＮへの侵入を防止するファイヤーウォールの外側（インターネットとの接点）にプロキシ（代理）サーバーを設置し、これがＬＡＮ内部の個々のコンピュータに代ってインターネットと交信する。そのため本来は、ＬＡＮ内部からのみのアクセスのみを許すサーバーが、外部からの接続を受け付ける場合がある。これをオープンプロキシという。なお民間プロバイダもプロキシサーバーを設置しているが、多くのＬＡＮの場合とは異なり、該プロバイダ利用者が必要的にこれを経由するとは限らない。

(5) ログの閲覧に際し、北陸大学情報システム検討委員会委員長（現、北陸大学情報センター長）亀田幸彦教授に格別の御高配を賜った。特記して深甚の感謝の意を表す。

(6) 拙稿「サイバーローに関する若干の試論」（「北陸法学」第五巻第四号・五一頁以下・平成一〇年三月）、拙稿「インターネットにおける猥褻物陳列行為処罰の可能性と限界」（「北陸法学」第七巻第一号・五五頁以下・平成一一年六月）。

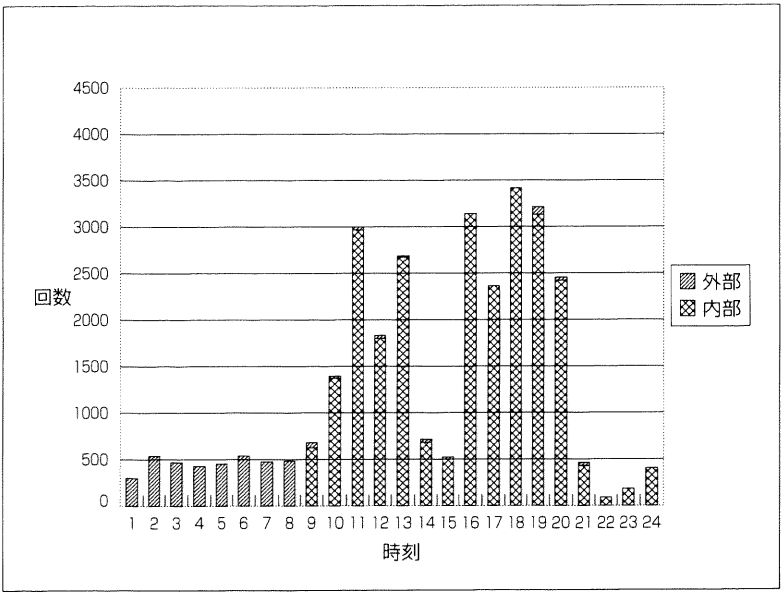
ログの分析

事実の概要

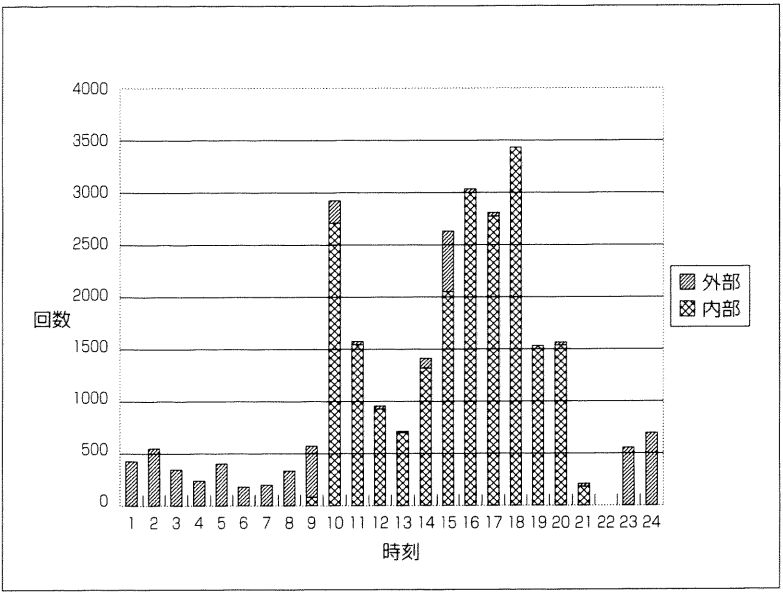
一九九八年当時、筆者の所属大学は学内ＬＡＮ構築準備中であった。二ヶ所のキャンパスのうち一ヶ所に試験的にＬＡＮを設置し、そこからインターネットへの接続を可能にしていた[1]。この時、同時に設置されたプロキシサーバーに対し、外部からのアクセスが記録された[2]。

今回、分析対象とした同年八月六日から九日までのプロキシログ[3]では、計七二、二八九件の通信データ[4]が記録されている。これを日別時間ごとに整理したグラフを示す。

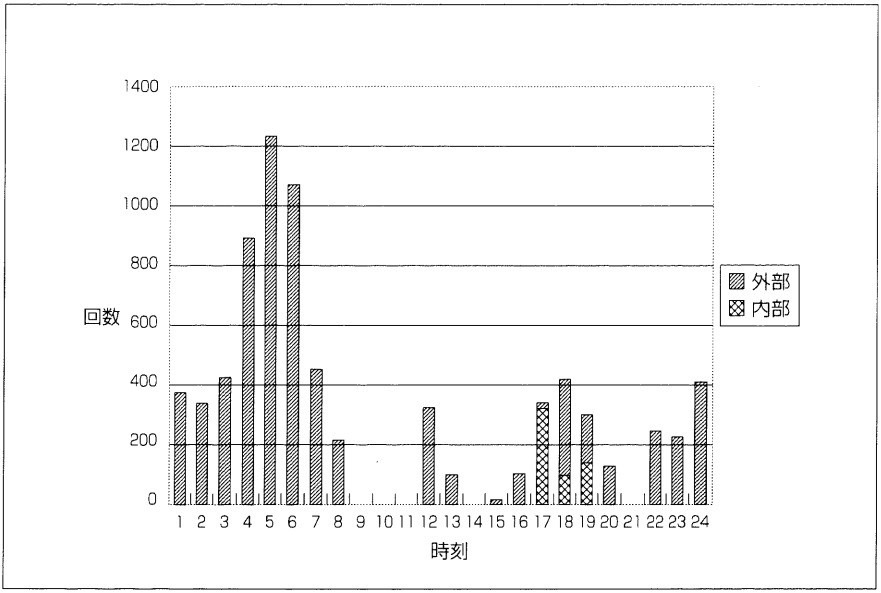
8月6日（木）　総計　30652回



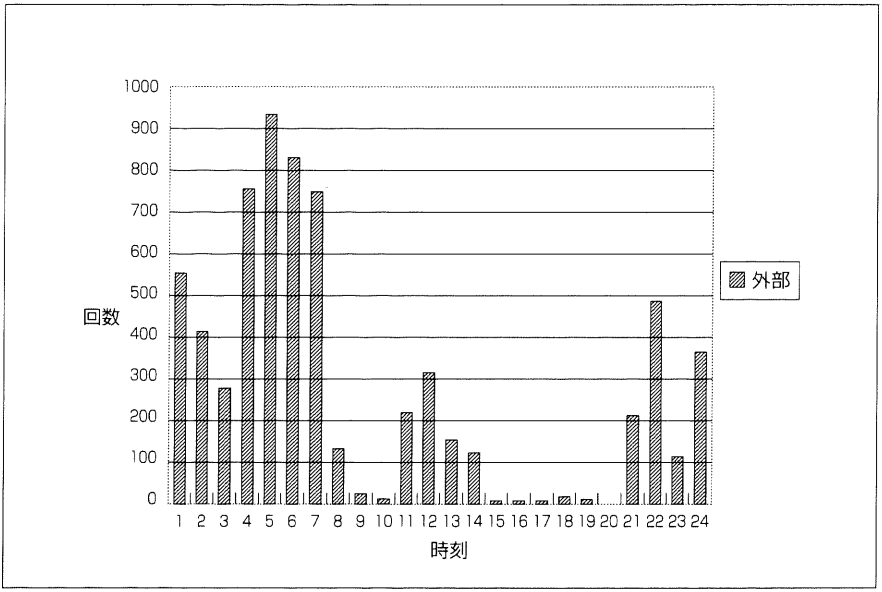
8月7日（金）　総計　27415回



8月8日（土）　総計　7548回



8月9日（日）　総計　6674回



グラフから、極めて顕著な傾向として、個人のインターネット利用者が増加する夜間ないし深夜に外部からのアクセスが増加し、日中は、正規の利用資格者である内部ユーザーが専らとなっている。そして週末になると午前五時、六時といった時間帯に、外部から大量の通信が行われていることがわかる。

また、外部からのアクセスについて、記録されているＩＰアドレスまたはドメイン名の個数は八月六日が六五、七日が五七、八日が四六、九日が五八であった。

外部からの接続元の多くは、民間プロバイダのダイヤルアップサーバーであるが、日本の自治体や大学、また海外のネットワークからのアクセスも小数ながら見られた。異なる日に同一のドメインからのアクセスが見えるため、同一のユーザーがプロキシの設定を変更せず、何度もアクセスしている可能性もあるが、少なくとも不特定多数のインターネット利用者が、当該プロキシのＩＰアドレスを知り得る状態にあったことは確実といえよう。

プロキシ利用の理由

自らの所属するネットワーク以外のプロキシを利用するケースは、決して少なくないと思われる。その理由は、大きく二つに分けられよう。一つは、通信速度の向上である。

インターネット利用者は、通常、どのようなサイトにアクセスしようとも、自分のコンピュータから相手先までの到達経路を指定することはできない。ところが外部のプロキシサーバーを経由すると、直接にアクセスした場合とは異なる経路を辿ってデータが往復する可能性が生じる。これはあくまで可能性であり、仮に経路が変わったとしても、速度が向上する保障はない。しかし、ネットワーク上の情報伝達遅延は、どこに原因があるか判然としないことが多いため、「迂回」は、希望的にではあるが速度向上に資するものがあるともいえる。

今回分析したデータに見えるアクセスに関しては、接続先が一般のホームページであることが大半であること、インターネットのアクセス速度が低下する夜間に利用が集中していることなどから、速度目的のために該プロキシサーバーを経由したものと考えてよい。

プロキシ利用のもう一つの理由は、アクセス者本来のＩＰアドレスを秘匿する、言い換えれば、「匿名化」することである。アクセス先のログには、接続者本来のＩＰアドレスまたはドメイン名は記録されず、中継したプロキシサーバーのＩＰアドレスが記録されるのである。

通常、インターネットのホームページを閲覧するブラウザソフトは、相手先に対し、接続者に関する様々な情報を送信する。次に、民間プロバイダに接続されたコンピュータから、筆者のホームページに設置したプログラムに対して送られる情報の一部分を、直接接続の場合とプロキシ経由の場合とに分けて示す。[5]

表の中で、「REMOTE_ADDR:」という項目がアクセス元のコンピュータを示すが、プロキシを経由することで、これが全く異なる数字に変わっている。[6] アクセス先のコンピュータからは、変更後のデータしか見ることができないのである。[7]

今回の分析対象であるログには、外部からのアク

直接接続

HTTP_USER_AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Windows 98; Win 9x 4.90)
GATEWAY_INTERFACE: CGI/1.1
HTTP_HOST: www.hokuriku-u.ac.jp
SERVER_SOFTWARE: Apache/1.3.22 (Unix)
SERVER_ADMIN: ********@hokuriku-u.ac.jp
REMOTE_ADDR: **.198.82.***
SCRIPT_NAME: /y-hara/****/env1.cgi
SERVER_NAME: www.hokuriku-u.ac.jp

プロキシ経由

HTTP_USER_AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Windows 98; Win 9x 4.90)
GATEWAY_INTERFACE: CGI/1.1
HTTP_HOST: www.hokuriku-u.ac.jp
SERVER_SOFTWARE: Apache/1.3.22 (Unix)
SERVER_ADMIN: ********@hokuriku-u.ac.jp
REMOTE_ADDR: ***.35.243.*
SCRIPT_NAME: /y-hara/****/env1.cgi
SERVER_NAME: www.hokuriku-u.ac.jp

（表注）各サーバーのセキュリティのため、項目の一部を伏せる。

セスの中に、僅かではあるがデータの送信が記録されていた。そしてその接続先がＣＧＩプログラムであることから、このアクセス者には、掲示板等への書込みに際し、自らのＩＰを秘匿する目的があったと考えられる。また、同じく数件ではあるが、海外の匿名化サイトを経由しての接続も見られた[8]。明らかに、自らのＩＰアドレスを秘匿する意図をもっての接続である。

プロキシサーバー情報の取得

民間プロバイダ、ＬＡＮ管理者は、それぞれの正規の利用者に対しプロキシサーバーのアドレスを開示するが[9]、それは、仮に外部からのアクセスを禁止するよう設定されていないにしても、不特定多数に提供、開示される性質のものではない。しかし現実に、インターネット上には、殆ど無数のプロキシサーバーのアドレスとポート番号を記したホームページや掲示板が存在する[10]。更に、外部から接続可能なプロキシサーバーを検索する方法やプログラムを紹介するホームページも存在する。そして、これら「情報」を掲出するホームページ等は、著名な検索サイトから容易にたどり着くことができるというのが現状である。

(1) この時点でインターネットへの接続は、ＮＴＴの一般向けデジタル通信サービスＩＳＤＮ一回線を利用していた。研究教育機関のインターネット回線としては極端に遅い部類に属するが、試験運用中であったため、高速な専用回線はまだ敷設されていなかった。なお、当時は、このＩＳＤＮ回線よりも低速の接続方式も広く用いられていたため、本節本文で後述する速度向上目的でも効果は期待できたと考えられる。

(2) 筆者が閲覧したログには、接続元（ＩＰアドレスまたはドメイン名）、日時、接続先ＵＲＬ、データ受信、送信の別などが記録されている。

なお、この時のプロキシサーバーは、既に外部からのアクセスができないよう設定を変更してある。

(3) 閲覧したプロキシログファイルは、ひとつで数十メガバイトを越える極めて大きなもので、当然ながら、通常使用が予定されているＬＡＮ内部からのアクセスと外部からのアクセスとが混在しており、判読が困難な状態であった。そこで、大学が夏季休業に入り、学内からのアクセスが極端に減少する八月五日から数日間のデータを分析対象とした。

(4) プロキシログの記録は、例えば一つのホームページに対する接続であっても、当該ページの文書部分であるＨＴＭＬファイルへのアクセスだけでなく、そのＨＴＭＬに記述された画像、音声などのファイル個々へのアクセスも記録される。従って、本文中の通信記録数は、所謂「アクセスの回数」を示すものではない。

(5) ここでは、アメリカ企業が開設する匿名化サイトを経由してアクセスすることにより、同社のプロキシサーバーを利用した。

(6) プロキシサーバーは、設定や機能により、情報秘匿の度合が異なる。大別すると、①本来のＩＰアドレスが完全に隠蔽され、更にプロキシ経由であることもわからなくなるもの、②元のＩＰアドレスは隠されるがプロキシ経由であることがわかるもの、③元のＩＰアドレスが、別の項目として残るもの、となる。

(7) このため、プロキシサーバーを経由することは、不正アクセスの手口の一つしてあげられる「踏み台」行為に類似するともいえる。しかし、プロキシサーバーには接続者本来の情報を記録するログが残ること、プロキシへのアクセス自体が不正とはいえないことなどから、いわゆる「踏み台」行為に比して、きわめて初歩的な証跡隠蔽行為に止まる。なお、「踏み台」と呼ばれる行為の場合は、本来外部からのアクセスを受け付けないサーバーをスキャンして接続口を探し、そこから侵入してサーバーを機能させ、再侵入用の入口を確保し、さらにそのサーバーに残るアクセスログを消去するなどした上で、他のサーバーに侵入を試みる。こうした行為では、「踏み台」にされたサーバーのログが消されるため、行為者の特定が不可能となる可能性が高い。

(8) この場合、ログには接続先として、「匿名化サイトのアドレス」／「接続先のアドレス」という書式で記録が残る。閲覧ソフトにプロキシを設定した上で匿名化サイトにアクセスし、所定のフォームに接続先を入力するという方式を取れば、このような接続形態が可能となる。

(9) 本稿はしがき註(4)に述べたように、特にＬＡＮ内部の端末からインターネットに接続する場合には、プロキシを必要とすることが多い。また、プロキシサーバーは、それを経由して転送されたデータを一時的に保存する機能を持つので、複数のユーザーが同一のデータにアクセスする場合、二度目以降のアクセス時には、一時保存したデータをユーザーに送ることによって、内部（Ｌ

ＡＮ）に向かっては反応速度を上げ、外部（インターネット）にはトラフィックを軽減するという「有益」な機能を果たす。

(10) これらのホームページ、掲示板には、筆者の所属大学のプロキシのＩＰ等を「公開」するものも存在した（当該ページは既に閉鎖されている）。該プロキシのアドレスは非公開であり、何人かがスキャン等の手法でこれを発見、掲示板サイトに掲出したものであろう。本体ログに記録された外部からの利用者が、かかるサイトから情報を入手、利用した可能性は非常に高いと思われる。

法的評価

不正アクセス禁止法との関係

不正アクセス禁止法は、

第三条　何人も不正アクセス行為をしてはならない。

２　前項に規程する不正アクセス行為とは次の各号の一に該当する行為をいう。

一　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）

二　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）

三　電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為[1]

として、禁止すべき「不正アクセス行為」の範囲を限定する。禁止されるのは、他人のＩＤ、パスワードなどの「識別符号」を用いるいわゆる「なりすまし」行為（二項一号）、正規のアクセス方式とは異なる手法でコンピュータに侵入、利用する「ハッキング」[2]行為（同二号）、そして、アクセス制限機能を有するコンピュータ（認証サーバーなど）をハッキングし、利用可能となった他のコンピュータにアクセスする行為（同三号）である。

同条からは、オープンプロキシへのアクセスは、本来想定された利用資格者以外による無権限利用であっても処罰の対象とはならない[3]。前節で分析対象としたログが蓄積された一九九八年当時は勿論、不正アクセス禁止法施行後であっても、外部からの接続を遮蔽しないプロキシサーバーは、同法にいう特定電子計算機には相当せず、これに接続を行うことは、該プロキシサーバーが過剰な負荷により機能低下するといった事態が起らない限り[4]、違法ではない[5]。また、プロキシサーバー検索プログラム類を利用する行為も、その機能紹介を見るかぎり、インターネットに接続されたサーバーコンピュータに信号を送り、対する応答からサーバーの性質や、通信可能なポート番号を判断するものであり、不正アクセス禁止法第三条第二項各号に定める特定利用制限がなされたコンピュータに対してその制限を免れる情報等を送信する行為には当たらず、同法による規制、処罰はできない。また、当該プログラムの利用から得られた情報をホームページ等で公開しても同様である[6]。

このように見ると、オープンプロキシの利用と不正アクセス禁止法には直接の関連性は存在しないかに思えるが、プロキシの持つ匿名性は無視しえない。同法違反行為の捜査においては、行為者の特定等に要する重要な情報を、

アクセスログ[7]から得る必要がある。しかし、アクセス者の本来のＩＰアドレスを隠蔽する機能を持ったプロキシを経由した場合、不正アクセスの被害を受けたコンピュータのログからは、プロキシのＩＰアドレスしか得ることはできないのである。前節で述べたように、プロキシサーバーには、アクセス者のＩＰアドレスと接続先のＵＲＬ等を記録したログが残るが、行為者特定を困難ならしめることは疑いない。複数のプロキシサーバーを経由した場合は更に捜査は困難になろうし、海外のプロキシが利用された場合には、行為者特定が不可能となる可能性すらある。

プロバイダ法との関係

プロバイダ法においては、ネットワーク上の掲示板等に何人かの権利を侵害する情報が公開された場合に、被害者が、プロバイダやサーバー管理者、運営者に対し、情報流通の防止や発信情報開示を求めうることを明示した。[8]

例えば同法成立以前、ネットワーク上の掲示板サービスにおいて争われた名誉毀損事件として、「ニフティ事件」[9]があるが、該事件は、インターネットが普及する直前の時期に、クローズドネットワークであるパソコン通信のフォーラム内で発生した名誉毀損事件であり、インターネットによるコンピュータネットワークの爆発的拡大が進行した今日においては、いささか様相が異なる。最近では、インターネット上の掲示板サービスに、個人または法人の私的情報とともに虚偽の情報を掲出し、もって対象となった個人または法人を侮辱し、あるいは名誉を毀損するといった事例が散見される。[10]プロバイダ法施行以後、同様の事例が発生すれば、被害を受けたとする者は、掲示板管理者等に対し、当該情報の削除、また当該情報発信者の情報開示を要求することになろう。発信者の情報とは、管理者等において知り得るのならば氏名等、あるいは当該情報を掲出した者のＩＰアドレスなど、接続元に関する情報で、大半がログに記録されたものとなろう。

このとき、情報を掲出した者がプロキシサーバーを経由し、本来のＩＰアドレスを隠蔽していた場合は、プロキシのアドレス以外の情報はログに記録されない可能性がある。プロバイダ法は次のように定める。

第四条　特定電気通信による情報の流通によって自己の権利を侵害されたとする者は、次の各号のいずれにも該当するときに限り、当該特定電気通信の用に供される特定電気通信設備を用いる特定電気通信役務提供者（以下「開示関係役務提供者」という。）に対し、当該開示関係役務提供者が保有する当該権利の侵害に係る発信者情報（氏名、住所その他の侵害情報の発信者の特定に資する情報であって総務省令で定めるものをいう。以下同じ。）の開示を請求することができる。

一　侵害情報の流通によって当該開示の請求をする者の権利が侵害されたことが明らかであるとき。

二　当該発信者情報が当該開示の請求をする者の損害賠償請求権の行使のために必要である場合その他発信者情報の開示を受けるべき正当な理由があるとき。

２　開示関係役務提供者は、前項の規定による開示の請求を受けたときは、当該開示の請求に係る侵害情報の発信者と連絡することができない場合その他特別の事情がある場合を除き、開示するかどうかについて当該発信者の意見を聴かなければならない。（第三項以降略）[11]

同条にいう「開示関係役務提供者」は、この場合、掲示板サービス等を設置しているサーバーの管理者、掲示板サービス開設者、同運営者等を指す。それとは無関係に存在し、かつ無権限で利用されたプロキシサーバーの管理者が含まれるとは考えられない。つまり、「開示関係役務提供者」のもつ発信者情報からは、個人の特定ができない可能性が生じると思われるのである。[12]

（1）　http://www.ipa.go.jp/security/ciadr/law199908.html。

(2) 本稿において「ハッキング」は、制限つきネットワークへの侵入という意味に限定して用いる。侵入先のコンピュータ上で、情報の窃取、改竄、破壊等を行う場合は、「クラッキング」と表現すべきである。

(3) IPA（情報処理振興事業協会）の統計によると、平成一二年に二件、オープンプロキシへのアクセスが届け出されているが(http://www.ipa.go.jp/security/crack_report/20010222/00all.html)、本来、届け出の対象となる不正アクセスに分類される行為ではない。

(4) 例えば、DOS攻撃のごとく、当該プロキシサーバーを経由して大量のデータ送受信をなし、もって当該プロキシサーバーの正常な動作を妨げるにいたった場合には、当該プロキシサーバーを客体とする電算機損壊等業務妨害罪が成立すると考えられる。

(5) 不正アクセス禁止法にいうアクセス制限機能は、ID、パスワード等による利用資格認証のみを想定する。特定のIPアドレスをもつコンピュータからのアクセスを拒絶するためのパケットフィルタリングは、実質的なアクセス制限機能ではあるが、明示的にID、パスワード等の発行、認証を行わないために、同法のアクセス制限には該当しない。仮に、パケットフィルタリング式ファイヤーウォール等のアクセス制限を破る行為が禁止類型に追加されれば、オープンプロキシの利用によって自らの制限されたIPアドレスを偽装する行為も当然に処罰対象となる。

(6) 不正アクセス助長行為を禁止する同法第四条は、あくまで他人のIDやパスワードを利用権者以外に提供する、いわゆる「ID屋」的行為を禁止するに止まる。

(7) 不正アクセス禁止法立案段階では、プロバイダに対し一定期間のログ保存を義務づけることも検討されが、個々の事業者の業務上の必要性や負担、あるいは国際的動向などの観点から法制化が見送られた（前掲「不正アクセス行為の禁止等に関する法律の制定の経緯」・二一頁）。警察庁は、記録されるログの内容を、日付、入力されたIDと入力したコンピュータのIPに限定し、三ヶ月の保存を義務づける案を有していた（同書二二頁註(17)）。ログは、不正アクセス事件捜査に不可欠の資料であるが、同時に、犯罪とは無関係な無数の通信情報を含むものであり、通信の秘密やプライバシー保護の観点から、最高度の配慮が要求されることはいうまでもない。

(8) 同法は、掲示板サービスへの書込みによる名誉毀損や侮辱、ホームページへの記述、また他者の著作物掲載等を想定していると考えられる。同法では、ネットワーク上で権利侵害が発生した場合に、直接に侵害行為をなしたもの以外の関係者、すなわちサーバー設置者、掲示板等設置者、同運営者に生じる可能性のある賠償責任の範囲を限定し、被害者には発信者情報開示請求権を確認

する（第一条）（http://www.soumu.go.jp/joho_tsusin/top/pdf/jyoubun.pdf）。これは、情報発信者、それにより被害を受けたと主張する者、そして情報が公開されたサーバーの管理者等、三者間の権衡に配慮しつつ、当事者間の、または民事訴訟による紛争解決に一定の道筋をつける効果を有するが、開示された情報から行為者が特定できなかった場合は想定していない。

(9) 本件については、山下幸夫「サイバースペースにおける名誉毀損とプロバイダーの責任」（「ＮＢＬ」第七二三号・平成一三年一〇月・三四～九頁）に詳細な解説がある。

(10) 最近の事例として、日本生命が、著名な掲示板サイト「2ちゃんねる」に同社を誹謗中傷する書込みがなされたとして、記事の削除を求める仮処分を申し立て、平成一三年八月、申し立てを認める決定が下された（http://www.mainichi.co.jp/digital/netfile/archive/200108/31-1.html）。

(11) 前掲http://www.soumu.go.jp/joho_tsusin/top/pdf/jyoubun.pdf。

(12) こうした実態を反映し、掲示板プログラムには、書込みを行ったもののＩＰアドレスを表示させたり、プロキシ経由のアクセスを禁止したりする設定を備えたものが見られる。プロキシ経由を禁止した場合、必要的にプロキシを用いるＬＡＮからのアクセスができなくなるが、掲示板開設者の自衛的手段として用いられることがある。

結び

インターネット上でオープンプロキシを利用することは、接続元のＩＰアドレスを隠蔽する初歩的で簡便な手段である。昨今、「ハッカー」という言葉を冠した多くの書籍が、ＩＰ技術解説書と並んで販売されているが、それらは、およそ例外なくＩＰアドレス隠蔽を目的としてプロキシの使用法に言及する。

だが、現在のネット環境からは、ＩＰアドレスの隠蔽行為に積極的効能を認めることもできる。かつて、研究機関のような団体以外では不可能だった高速回線を使った常時接続が、民間プロバイダ経由でも容易に実現した結果、ＩＰアドレスの不用意な漏示により、個人のコンピュータが「踏み台」目的等の不正アクセスの対象とされる危険が生じている。インターネット上にある無数のホームページのどこででも、接続元のＩＰアドレスを取得すること

は容易である。リンクを辿ってネットサーフィンする過程で、悪意の開設者が設置したページにアクセスしても、アクセス者はそれと気づくことなく、ＩＰアドレスを知られてしまう可能性がある。こうした危険を回避するために、匿名化機能を持ったオープンプロキシを経由する者も、少なからず存在するのではなかろうか。

マイナスの側面が明らかに認識できる以上、筆者は、オープンプロキシ利用を推奨することはしない。しかし、その禁止を主張するものでもない。そもそも、世界各地に無数に存在するプロキシサーバーを全て、外部からのアクセスを遮蔽するよう設定することは不可能である。インターネットという新しいインフラにおけるコミュニケーションが、パケットという微細な電気信号のやりとりだけで成立し、国境すら意味をなさないことを考えれば、ひとり日本のみでより強力な法的対応を考えることは無意味である。

不正アクセスを禁止し、ネット上の権利侵害に対し法的措置をもって回復を図ることは、ハイテク問題に関する国際的取組み[1]という意味からも望ましい。だが、日々進歩する技術社会を遺漏なく規律しうる全備な法は、存在しないのである。不正アクセス禁止法、プロバイダ法には、高度な技術を有しない至極一般的なインターネット利用者の違法行為を摘発し、権利侵害時の接続情報を開示して賠償請求を容易ならしめ、それによって、同程度の知識を有する他のユーザーの、興味本位の違法行為を抑止することが期待される。しかし、オープンプロキシ利用のような初歩的な手法でも、ある程度の証跡隠蔽が可能であることから考えれば、より高度な技術を有する行為者が故意に何らかの違法行為をなした場合には、その行為者を特定することすら困難であるといわざるをえない[2]。

向後、国際的な協力体制の強化、ＩＰｖ６に代表される技術革新、セキュリティー対策の徹底など、全方位的な対策がさらに進み、安全で秩序あるネット環境が構築されることを切に希望する。オープンプロキシというインターネット上の存在のみによっても、現実社会においてならば期待し得る法の効果が発揮されない可能性がある以上、それを利用し、あるいはさらに巧妙な手口でなされるより悪質な違法行為を抑止するためには、法だけではなく、

まさに全方位的取り組みが必要なのである。そして、将来なされるであろう関係法規の制定改廃にあたっては、法をもってネットワークを変えるのではなく、ネットワークの発達によって法が変わっていくのだということを、常に意識する必要があると考える。

（1）平成九年のデンバー、一〇年のバーミンガムサミットで、ハイテク犯罪への対応が議論されたのは記憶に新しい。

（2）園田教授は、前掲「不正アクセス」において、「ネットワークの中には非常に高度な技術をもった者も暗躍している。彼らにとっては不正アクセスの痕跡すら消し去ることが可能である。現実にそのような事件も発生している。刑罰の抑止効果も、彼らには期待できないおそれがある。」（http://w3.scan.or.jp/sonoda/ text/access/access.html）と指摘されている。