社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2006－DPS－128 (21)
2006－GN－ 61 (21)
2006－EIP－ 33 (21)
2006／9／15

サイバーストーカー（ネットストーカー）の現状と対応

井出 明
近畿大学

近年、高度情報化社会の進展に伴って、ネットワーク上のストーキング行為が多数報告されつつある。リアルスペースでのストーキング行為に関する規制法は、既に立法化され、不十分ではあるものの一定の効果を上げつつある。本稿では、リアルスペースとサイバースペースにおけるストーキング行為を比較しながら、サイバーストーカー（=ネットストーカー）の特性について検討し、行為主体と行為客体に基づいて類型化を図る。その上で、可能な対策についても類型別に提示した後、将来的な展望にも言及する。

The Present Situation of Cyberstalkers and Our Measures

Akira Ide
Kinki University

These days, with the progress of information society, many cases of cyberstalking have been reported. The laws for real stalkers were already legislated and it is effective in some situations though the effects are not yet perfect. In this paper, I will compare the behaviors of real stalkers with those of cyberstalkers. Then, analyze the characteristics of cyberstalkers to classify them in terms of the subjects and objects of their behaviors. Finally, possible measures will be presented in accordance with the classes of the characteristics, and future views would be also referred.

1． サイバーストーカーとは何か

サイバーストーカーとは、ネットワーク上でストーキング行為を行うものの総称であり、ネットストーカーとも呼ばれる。日本では、ネットストーカーという用語を用いる傾向があるが、ストーカー対策の先進地であるアメリカでは、サイバーストーカーという用語を使うことが多い。本稿では、アメリカでの慣用に従い、サイバーストーカーという用語を用いることにする。

サイバーストーカーという言葉は、一般的な概念であろうか。検索エンジンを廻すと、かなりの数のサイトがヒットし、すでに多くの人々に認知された用語であることは分かるが、しかしながら、その用語の意味するものは一義ではない。サイバーストーカーという用語に対して、各人が各様に独自の定義を作り、それぞれが無秩序に用語を好き勝手に用いていると言っても過言ではない。また、国立国会図書館の NDL-OPAC を引く限り、サイバーストーカーを分析的に取り扱った邦書は無く、小説の素材として取り上げられているにすぎないことが分かる。そこで本章では、ストーカー概念そのものの再検証を行う。

1．1．日本におけるリアルストーカー

日本では、桶川ストーカー事件を契機として、ストーカー規制法（正式名称は「ストーカー行為等の規制等に関する法律」）が制定された[1]。本法では、ストーカーの定義として、２条２項で“「ストーカー行為」とは、同一の者に対し、つきまとい等（略）を反復してすることをいう。”と定義している。つまり、つきまとい等を繰り返して行っている者をストーカーと定義しているわけであるが、このつきまとい等とは具体的に何を指すのであろうか。

同法２条１項では、「特定の者に対する恋愛感情その他の好意の感情又はそれが満たされなかったことに対する怨恨の感情を充足する目的で、当該特定の者（略）に対し、次の各号のいずれかに掲げる行為をすることをいう。」とされている。この各号に掲げる行為として、同条同項は、以下の限定列挙を行っている。

一　つきまとい、待ち伏せし、進路に立ちふさがり、住居、勤務先、学校その他その通常所在する場所（以下「住居等」という。）の付近において見張りをし、又は住居等に押し掛けること。
二　その行動を監視していると思わせるような事項を告げ、又はその知り得る状態に置くこと。
三　面会、交際その他の義務のないことを行うこ

とを要求すること。
四　著しく粗野又は乱暴な言動をすること。
五　電話をかけて何も告げず、又は拒まれたにもかかわらず、連続して、電話をかけ若しくはファクシミリ装置を用いて送信すること。
六　汚物、動物の死体その他の著しく不快又は嫌悪の情を催させるような物を送付し、又はその知り得る状態に置くこと。
七　その名誉を害する事項を告げ、又はその知り得る状態に置くこと。
八　その性的羞恥心を害する事項を告げ若しくはその知り得る状態に置き、又はその性的羞恥心を害する文書、図画その他の物を送付し若しくはその知り得る状態に置くこと。

翻って、一般にサイバーストーカーと呼ばれている類型が、本法が想定するストーカーに該当するかを検討する。まず、ストーカー規制法におけるストーカーとして定義されるためには、「特定の者に対する恋愛感情その他の好意の感情又はそれが満たされなかったことに対する怨恨の感情を充足する目的」が前提となるが、サイバーストーキング行為は、後述するように好悪感情に基づくものが極端に少ない。好悪感情に基づいていない以上、現行のストーカー規制法で対応することが出来ない。これは、立法の経緯を鑑みれば当然のことで、立法直前の警察庁の調査によれば、もともと悪質な「つきまとい」の 88%が恋愛感情のもつれによるものであり、そのつきまといを防止することが本法の立法趣旨であったからである [2]。つまり、リアルでのつきまとい以外は、あくまでも副次的な規制の対象なのである。

仮に、好悪感情に基づいて、サイバースペース上で何らかの行為を行った場合、上述の２条１項一号から八号に該当するかを次に検討しなければならない。このうち、サイバースペースにおいて可能となりうる行為は、二、三、七、八の各号程度である［注１］。しかし、いずれもサイバースペースに固有の行為というわけではなく、インターネットもその手段の一つとなり得るという程度にすぎない。コミュニケーション手段が何であるかは問題にしておらず、内容面が規制の対象となっている。

この文脈において、サイバースペースで一般に“ストーキング行為”といわれる活動を、従来型のストーカー概念で捉えることは無理がある。換言すれば、サイバーストーカーという概念は、日本法におけるストーカーとは似て非なる異質の概念であって、現実社会のストーカーとは分けて考える必要がある。

１．２．　海外におけるストーカー規制

ここで、日本のストーカー規制法に大きな影響を与えたアメリカの事例を検証し、サイバーストーカーの考察についても役立ててみたい。

アメリカでは、1989 年の女優殺害事件に端を発し、カリフォルニア州を皮切りにストーカー規制法が整備されていった。その後、多くの州のストーカー規制法は、全米刑事司法協会（NCJA）が定めた“ストーキング防止のための模範法典(Anti-Stalking Code)”を元に策定された [3]。アメリカ法の場合、３つの要件（①ある特定の人物やその家族が生命、身体の安全について恐怖心を抱くと思われるような行為を意図的に継続②ある特定の人物が恐怖心を感じる状況に陥るであろうことを知っていたこと③実施にその特定の人物に恐怖心を抱かせたこと）を満たした場合、ストーキング罪として処罰されることとなっている。　なお、同様の法律は“嫌がらせ威行為保護法”としてイギリスにもあり、明確に差別主義者や迷惑な隣人を取り締まることを明言している。米英ともに、日本法よりも処罰の客体も行為も広い点が特徴となっていると言えよう。

１．３．日本法の特徴

前節までの考察を踏まえて日本法のストーカー規制法の特殊性を考える。アメリカの場合、偏執狂による殺人事件を機に立法が行われたため、処罰範囲や処罰対象が広くなっているのに対し、日本の場合は桶川ストーカー事件を端緒として法整備がなされたため、本法の射程が狭く且つ短いという特徴を持つ。英米の概念では、ストーカーに“困った人々”を概念上含んでいるが、日本法では対象から外れている。したがって、日本でサイバーストーカーと呼ばれる一般的迷惑行為を処罰するためには、ストーカー規制法以外の別の法律に頼らざるを得ない。どのような場合に、どのように対応するかという論点を考察するために、次章ではサイバーストーカーの類型化を試みる。

２．サイバーストーカーの類型化

ここでは現実に起きているサーバーストーキングについて、ある分析の視点を提供する。前章で見たとおり、好悪感情に基づくストーキング行為は、現行法で対応可能なので、ここでは深く立ち入らない。また、行為の違法性が甚だしい場合は、脅迫（刑法２２２条）なり、名誉毀損（同２３０条）なりで対応できるため、本稿では、現行法では対応が難しい領域について、考察の対象とする。

警察庁が運営するセキュリティ情報サイト“@ポリス”では、サイバーストーカーに関する記述も見られる [4]。警察庁は、サイトの中の定義集でネットストーカーを「何度もメールを送りつけるなど、ネットワークを利用してしつこくつきまとう者をいう。掲示板を使って誹謗中傷をしたり、なんらかの手段で住所などを割り出して物理的なストーカー行為に発展することもある。」と述べている。海外のサイバーストーキングの事例集においては、チャットへの個人情報の掲示などもストーキング行為の例としてあげられ、主体も複数になりうることが説明されている [5]。また、日本ではネットストーキングとしてはあまり認識されていないが、１．２．で言及したとおり、イギリ

スでは特定個人ではなく、人種などの集団的な“属性”に対する攻撃もストーキング行為となる。このような文脈からストーカー行為の類型化を試みると、ストーキング行為の主体が個人であるか複数であるか、またストーキング行為を受ける被害の客体が個人であるか複数であるかという観点から社会現象としてのストーキング行為を分類することが出来る。表１は、この考察を模式化したものである。

表１

被害者＼加害者	主体が個人	主体が集団
客体が個人	①	③
客体が集団	②	④

３．各類型への対応

２．で試みた分類に基づき、類型ごとの対応を考える。

３．１．個人が個人に攻撃を仕掛ける類型

①の類型は、個人が個人を中傷するという典型的なサイバーストーキングの事案である。刑事罰に問える場合は、弁護士と協議の上、被疑者不詳であっても被害届を出すなどの対応をとることが望ましい。刑事罰に相当するレベルの電子メールの送付や掲示板への書き込みは、警察による素早い対応が被害の拡散を防止する。

問題なのは、刑事罰に問えないレベルの権利侵害である。発信者が分からない場合は、プロバイダ責任法を用いて、とりあえず発信者情報の開示を図るべきである。本法の制定当時は、“海外発信に対応できない”“プロキシーから書き込まれると発信者情報の開示手続きが煩雑になる”“ネットカフェから書き込まれた場合、発信者を特定できない”などの多くの問題点が指摘されたが、これらの指摘は実はあまり大きな問題ではない[6]。なぜなら、誹謗中傷を多くの目に触れさせるためには、何らかのポータルにリンクを張ることが必要となるが、かつてこの種の迷惑行為の温床となっていた“２ちゃんねる”でも、海外の IP や逆引きの出来ない IP からの書き込みは多くの板で規制がかかっている。ネットカフェも、今や多くの店で ID の提示を義務づけており、ネットの匿名性は現在縮小されつつある。プロバイダ責任法が抱える問題点は、手続きがあまりに煩雑である点にあり、総務省も改善を模索している[7]。

発信者が特定できている場合でも、被害が押さえられるかという点については難しい問題がある。嫌がらせの当事者に社会常識がある場合は、弁護士からの警告等によって事態が沈静化する可能性もある。しかし、加害者がいわゆる“困った隣人（＝違法とまでは言い切れない嫌がらせを繰り返すような人々）”に当たるような場合は、効果的な法的対応をとりにくい。リアルの嫌がらせであれば、引っ越しをするという対応をとることもあり得るが、サイバースペースの場合逃げる場所も無いため、事態はより深刻化する。

プロバイダ責任法の制定当時、プロバイダ事業者達は、「トラブルは当事者間で解決する方向へ」という主張を行っていた[8]。しかし、当事者間での解決を図る為には、両当事者が解決を望んでいる必要があるが、実際には“困った隣人”はもともと解決を望むという意識はなく、嫌がらせそのものが自己目的化している場合がある。

日本の裁判制度においては、行為や行動を制限する判決を得ることは極めて困難であり、発信者情報が開示されたとしても、実効性のある対策をとりにくい。そこでネット上での嫌がらせ行為を抑止する為の立法が別途必要となるが、この点については後の５．で述べる。

３．２．個人が集団を攻撃する類型

この類型は、個人が企業に対する嫌がらせを行ったり、人種や出自などの面で社会的マイノリティに属する集団に攻撃する等のパターンが考えられる。

前者は、いわゆるクレーマーであり、個人が攻撃している限りはあまり大きな問題とはならない。但し、クレームが集団化してくる場合は、後述するように企業にとって脅威となりうるので、心して取り組む必要がある。

後者の社会的マイノリティに対する攻撃は、日本ではストーキング行為と捉えられていないが、先述の通り諸外国ではストーキングの行為類型に当てはまる。特にアメリカの場合は、人種的マイノリティや障害者への差別的発言は連邦の公民権法の規制対象となる場合があり、ネット上での発言においても注意が必要となる。この社会的マイノリティを攻撃するというパターンは、プロバイダ責任法も適用しにくい。プロバイダ責任法は、“自己の権利を侵害された者”を対象としており、総務省はこの“自己”を自然人のみならず、法人及び権利能力無き社団にまで含むことを明言しているが、社団要件を満たさない抽象的なマイノリティについては、開示請求の主体となり得ないという問題点がある[9]。

３．３．集団が個人に攻撃を仕掛ける類型

現在、もっとも問題が顕在化している類型がこの③のタイプである。ネット上での何らかの発言が多数派からの非難を浴び、ブログが“炎上”するなどの事例が多く報告されている。攻撃を行う加害側は多人数であり、互いに意思の連句はない。

この類型の場合、書き手の人数が多すぎて発信者情報を開示したとしても具体的な対応が出来ないという現実がある。また、著名人だけが狙われるというわけではなく、反感を持たれた一般市民や個人情報が流出した一般市民を標的に、ネットにおける“大衆”が嫌がらせ行為を繰り返すという事例も多く見られる［注２］。話せば分かるという類のものではないので、ネットでの情報発信を一時中断し、騒ぎが収まることを待つしかないのが現状である。

３．４．集団が集団に攻撃を仕掛ける類型

④で示されるこのタイプは、３．３．と同様、攻撃する側に意思の連絡はないという特徴を持つが、攻撃対象が企業なり社会的マイノリティなりに向けられている類型である。企業が対象となる場合は、企業に何らかの帰責性がある場合が多く、単なるうわさや憶測が大きな騒動となる場面は少ない。それでも虚偽の風説がはびこりそうな場合は、早い段階で公式情報を打ち出すことが、デマの防止に有効である[10]。また、被害側が法人もしくは法人と同視できる体裁を整えている場合は、プロバイダ責任法３条により削除要請が可能である。なお、掲示板等での企業への悪意の書き込みを発見したのち、様々な対応をとるサービスを提供している会社もあるが、攻撃対象となる企業がこの種のサービスを利用していると噂される場合、さらに大きな非難を浴びる事例もあるため、導入には慎重な検討が必要である。

法人と同視できないマイノリティの社会集団が攻撃の対象となっている場合、現行法ではいかんともしがたい。日本法の法体系は、具体的な権利の侵害がない場合の救済を念頭に置いていないからである。このタイプの被害集団を救うためには、立法その他、新たな社会的対応が必要となるが、５．で扱うこととする。

４．事前対策

前章では、問題が起こってしまった場合の事後対応について検討したが、本章では被害に遭わないための事前対応について考察する。

集団が被害を受ける場合は、弱者差別等何らかの社会上の構造的要因に基づいている場合が多く、個人で対応しきれるものでもない。これは事前対策の枠組みからは外れる。

個人が被害者とならないためには、月並みながらサイバースペースにおいて対人関係や発言に気を配るべきであるということになる。特に、３．３．で述べたように、一対多の対立構造となる場合、“多”の相乗効果や群集心理が働くため、あらかじめブログのトラックバックやコメント機能に制限をかけておくことも重要となる。また、情報発信のプロでない個人は、発信する必然性のない情報については、謙抑的であるべきであろう。ホームページの制作をはじめとして、電子ネットワークによる情報の発信は、新たな交流をもたらすとともに、同時に潜在的に危険性を持つ。自分の発する情報が社会的文脈の中でどのように位置づけられるかという点について想像力を働かせることが出来ない場合は、ネット上での情報発信をやはり控えなくてはならない。換言すれば、情報発信に関係するリスクの引き受けを自己責任で行えない場合は、発信すべきではないのである。現在までのメディアリテラシー教育は、受信の能力についてはかなり向上しているものの、発信のリテラシーについては未だ体系的教育が行われていない。誰もが気軽に情報発信が出来る現状に適したリテラシー教育に変えていくべきである[11]。

５．立法論と社会的対応

３．では、主体と客体という視点からサーバーストーキングを分類し、可能な対応を検討した。本章では、将来を踏まえて、これからどのように社会的な対応を採用していくべきかという点について考察する。なお、加害者側が個人で、被害者側が集団という類型は、３．２．でも検討したとおり、加害者が単数にとどまる限り被害者側にとって大きな脅威にならないため、ここでは検討の対象から外す。

５．１．個人間でのストーキング行為について

好悪感情に基づかない個人間のストーキング行為については、実は各地の“迷惑防止条例”が規制の対象としており、実際に発動された例もある。この種の条例の多くは、ネットワークに関係する行為類型を直接の規制の対象としておらず、あくまでもリアルでの行為を処罰の対象としている。現在まで、各地の迷惑防止条例はストーカー規制法や刑法が対象に出来なかったストーキング行為や痴漢行為を規制対象に取り込み、今も進化を続けている。そして、条例のこのような進化は、地域住民から一定の評価を受けている。

このように有効に機能している迷惑防止条例であるが、各自治体で運用に差があるとともに、電子ネットワークを用いた事案については管轄の観点から適用しにくい為、国で統一的な立法を行うことが期待される。

５．２．加害者が集団の場合の将来的対応

５．２．１．法の限界

表１の③④に区分される類型を、規制するためにはどうすれば良いであろうか。実は、諸外国には、社会的マイノリティへの差別表現を規制する法律は、前述の公民権法をはじめとして例が多い。日本でも 2002 年に人権擁護法案の導入が検討され、国会に上程されたが廃案となってしまった。人権擁護法案の精神自体は、なるほどすばらしく、国際的な流れにも合致していた。

しかし、表現の自由への強力な抑止装置となりかねないとともに、恣意的な運用への懸念が払拭できなかったため、可決の運びとはならなかったのである。

法律によって表現の自由に基づいた表現行為を萎縮させることは、民主主義国家にとっての自己矛盾となりかねない。国家による介入を防ぎつつ、人権の擁護を行うためにはどうすればよいのであろうか。

５．２．２．自主規制

表現行為全般を規制しかねない法律に対する懸念がある以上、法的対応に全てを期待することは得策ではない。そこで、別の策として、職業的メディアがこれまで行ってきた自主規制や事後救済の仕組みをインターネットに応用するという道が考えられる。出版界はこれまで、差別語や差別表

現に関し、出版前に十分な検討を行ってきた。放送の場合、事後になる場合もあるが、訂正放送などで不適切な表現に対応してきている。

インターネットプロバイダの場合、これら既存のメディアとどのような差異があるのであろうか。インターネットによる情報発信については、発信前にプロバイダが関与することは難しく、プロバイダが③④のストーキング行為に関して関与できるのは、情報の発信後に限られる。プロバイダ責任法でもこの実態が尊重され、プロバイダに何らかの責任が発生してくるのは、プロバイダが違法な書き込みの存在に気づいたあとに限られている。

このプロバイダ責任法の精神を一歩前進させ、悪意のある表現を規制するためのガイドライン作りを行うべきではないだろうか。日本プロバイダ協会では、行政法律部会を設立し、必要な法制度の策定などを行政に働きかけている[12]。しかし、逆の発想も必要であり、行政や法律事項で対応できない分野については、自主規制による対応を積極的に考えていく時期に来ている。これまで、知的財産権侵害やプライバシー侵害についてはある程度の研究成果が蓄積されてきている。今後はこれらに加え、公共空間で使うべきではない用語の選定や発信規制などについても研究を深めていかなければならない。そして、新たに策定されるガイドラインに抵触する利用については、顧客に対する勧告や指導なども検討されて良いだろう。プロバイダー社だけがこのようなことを行っても効果は薄いため、協会がエンジンになるべきであると考える。

禁止用語を選び出し、掲示板等へのアップロード先への規制とセットで、いわば発信のフィルタリングを行うことは技術的には難しくない。このような仕組みを作るならば、その際大切なのは、情報公開と適正手続きの保障である。廃案になった人権擁護法案においても、人権擁護委員の選出過程などがあまりにも不透明であったために、国民は理念よりもシステムに不安を感じ、同法案に対する反対運動がわき起こった。インターネットプロバイダが、どのような基準とどのような手続きによって悪意のある言葉を選び出し、発信規制をかけているのかを透明にする必要がある。さらに、発信が規制された表現の当事者が、十分に反論できる機会が保障されてこそこのような制度は初めて機能する。制度に対する信頼は、公正と公平によって担保されうるのである。

なお、プロバイダとの契約は一般的な双務契約であるから、多くのプロバイダは問題のある顧客との間で契約を解除できる旨を約款で定めている。従って、問題の多い顧客とは契約を解除するとともに、プロバイダ協会を通じたブラックリストの管理を行い、プロバイダ協会加盟他社での再入会の制限を行うのであれば、自主規制は十分な実効性を確保できる。

終わりに

ネットワーク上でのストーカー概念は、ストーカー規制法よりも広い。このような認識を踏まえた上で、安全なネットワークの利用と発信者と受信者の相互の人権保障を実質化することはかなり難しい問題である。本稿における分類や考察および提言は、この問題を体系的に扱った論考が少ないために、問題提起の意味も含めて行った。今後、より議論が深まることを期待している。

［注１］本法２条２項５号は、そもそも電子メールについて、完全に規制の枠外においている。これは、法の制定当時にまだ電子メールが普及していなかったことも理由の一つであるが、電子メールの場合は、受信拒否の設定やメールアドレスの変更などの自衛策をとりやすいからであると考えられる。

［注２］代表的事案としては、２０００年６月に著作権法違反のコンテンツをオークションで売り渡そうとした少年が、支払いを受けられなかったことに腹を立て、先方を２ちゃんねるで告発しようとした事案がある。この事件は、少年が著作権法違反のコンテンツを売ろうとしたことが逆に読者から問題視され、少年の自宅にまで張り込みがつき、少年のプライバシーが侵されるという事件に発展した。詳細は、以下のURLを参照のこと。
http://piza.2ch.net/net/kako/966/966754926.html

参考文献

1　小島妙子『ジェンダーと法 I』信山社 pp153-pp155（2004年11月）

2.　ストーカー規制法研究会・園田寿著『わかりやすいストーカー規制法』大谷實監修、有斐閣 pp14（2002年3月）

3.　岩下久美子　『人はなぜストーカーになるのか』文藝春秋　pp182-pp189（2001年1月）

4.　警察庁　『@police－用語集』
http://www.cyberpolice.go.jp/words/index.html#na　（2006年8月15日確認）

5.　Douglas Schweitzer “How to combat cyberstalking” Computerworld （2003.July16）
http://www.computerworld.com/securitytopics/security/story/0,10801,83106,00.html（2006年8月15日確認）

6.　井出明　「プロバイダ責任法の実務的問題点」『FIT2002 講演論文集４分冊』情報処理学会 pp273-pp274（2002年9月）

7.　共同通信　「ネットでのひぼう・中傷、発信者突き止めろ」佐賀新聞　2006年07月11日掲載

8.　国分明男　「プロバイダ責任制限法とプロバイダの責任」『情報ネットワーク法学会設立総会および第１回研究大会予稿・資料集』ネットワーク法学会 pp30（2002年7月）

9.　総務省編　『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―逐条解説―』 pp22-pp36 (2002 年 5 月) オンライン入手先
http://www.soumu.go.jp/s-news/2002/pdf/020524_1_a.pdf
10. 井出明他 「正確な防災情報流通のための制度的および技術的担保」『DICOMO2003 シンポジウム』情報処理学会 pp749-pp752 (2003 年 6 月)
11. 井出明 「情報化社会の法と倫理」GW vol32、情報処理学会 pp23-pp28 (1999 年 5 月)
12. 社団法人日本インターネットプロバイダー協会・行政法律部会
http://www.jaipa.or.jp/active/admin_index.html (2006 年 8 月 15 日確認)