インターネット上の不法行為などにおける本人性について

（The degree of proof of who has carried out illegal acts on the Internet.）

森　　拓　也／今　村　昭　悟／　岡　田　健　一[1]

1　本人性の問題についての現状

インターネット上の犯罪や不法行為が行われた場合、その行為を行った者の特定の問題（本人性）が生じる。従前は、ＩＰアドレスなどから特定された機器を物理的に管理している者が行為者である蓋然性が高いと認められてきたが、近時、コンピュータウイルス等を使って、他人のパソコンを遠隔操作するなどの方法により犯罪予告の書き込みをさせたことから、遠隔操作されたパソコンの管理者が誤認逮捕されるといった事件が発生した。この事件に代表される遠隔操作ウイルス等の登場により、今後の刑事事件、民事事件における本人性の立証、さらには発信者情報開示請求は、どのような影響を受けるのか。

2　刑事事件における犯人性の立証

(1)　犯人性についての従来の事実認定の概略

インターネットにおいて広く採用されている通信規格の仕様上、ＩＰアドレス等は、特定時点においては、特定の通信機器に割り当てられるから、発信の時間および発信元のＩＰアドレス等が判明すれば、当該通信機器から、情報が発信されたことが、一義的に確定できる。かかるＩＰアドレス等の特性は、科学的証拠として、一般に高い証明力が認められる。

したがって、遠隔操作ウイルス等の存在を考えなければ、インターネット上の犯罪においては、「犯行の際に記録されたＩＰアドレスが割り当てられた通信機器を所持していた」事実は、強い推定力を持つから、せいぜい、当該通信機器の設置場所や設置状況、物理的な犯行の可能性などで補完し、「当該通信機器を手に取って使用できたのは、被告人だけである」ということが認定できれば、ほぼ合理的な疑いを排除できるだけの立証があったと言えたであろう。

(2)　遠隔操作ウイルス等の登場による影響

しかし、ごく当り前のことながら、ＩＰアドレスによって証明される間接事実は、「当該情報を発信したのは、当該通信機器である」ということであって、被告人の犯人性を直接、証明するものではない。

とすると、パソコン等の通信機器がウイルス等によって遠隔操作される可能性がある、という現状では、もはやＩＰアドレスが当該通信機器に割り当てられたというだけでは、その管理者の犯人性について強い推定力を及ぼすとは認められない。つまり、「当該通信機器を現に手に取って使用できたのがＡである」という事実に加えて「当該通信機器が遠隔操作ウイルス等によって外部から操作されたのではないか」という合理的な疑いを払しょくできなければ、犯人性の立証と

[1] 弁護士森拓也　弁護士法人きっかわ総合法律事務所・立命館大学法科大学院非常勤講師（情報法）mori@kikkawalaw.com
弁護士今村昭悟　北尻総合法律事務所　imamura@kitajiri-law.jp
弁護士岡田健一　石井義人法律事務所　okada@ishii-law.com

しては十分ではなくなったのである。

具体的には、検察官は、これまで行ってきた犯人性の立証内容に加え、①当該通信機器を精査した結果、ウイルス等の痕跡を認められなかったこと、②ウェブサイトへのアクセスの頻度や書き込みの態様等、ウイルス等のプログラムに特徴的な事実、通常人の書き込みとしては不自然な事実の有無、③先行的な書き込みの存否や、被害者との人的関係性、④ウイルス等の侵入経路に関する被告人の供述内容や、⑤実際に同様の遠隔操作ウイルスがインターネット上にどのような態様で仕掛けられているか、といった事実を犯人性に関する重要な間接事実として立証していくことになると考える。

(3)　強制捜査に与える影響

近時報道された誤認逮捕の事案において、最も問題が大きい点は、捜査機関が、ＩＰアドレスが割り当てられた通信機器を保有していた、という事実が持つ犯人性の推定の程度を過大に評価し、被疑者の取り調べに臨んだ点にあると指摘されることがある。

かかる観点を重視すれば、逮捕や捜索の要件論として、ＩＰアドレスによる機器の特定だけではこれを行うことができない、とする考え方もあり得ようが、条文の文理や捜査の段階的、発展的性格、現実の身柄の確保や立証の必要性からすれば現実的ではない。

見直されるべきは、むしろ、捜査機関の意識であり、今後、捜査機関はインターネット犯罪の捜査のあらゆる過程において、第三者の犯行可能性の吟味を十分に行わなければならない。

(4)　踏み台にされた通信機器の管理者の幇助犯の成立について

遠隔ウイルス等によってインターネット上の犯罪に利用された通信機器の管理者が、そのことをもって、刑事上の責任を追及されることはあり得るか。

このような場合、管理者には、不作為による幇助犯が成立するかということが問題となるが、これを認めるとあまりにも幇助犯の範囲が広がりすぎること等から、その成立自体に疑問がある。また、幇助犯における故意の範囲については、いわゆる Winny 事件最高裁判決に照らせば、同機器が、具体的な犯罪に使われることを認識認容してインターネットに接続した場合や、その客観的情況等に照らし、例外的ではない範囲で、第三者から犯罪の踏み台に使われる、という認識および認容がある場合に初めて幇助犯の故意が認められると解される。

したがって、少なくともこのような故意が認められる特殊な例外を除き、管理者に幇助犯の成立は認められないと考える。

３　民事事件における本人性の立証

(1)　民事事件における立証責任一般

不法行為に基づく損害賠償等を求める民事事件における立証責任の分配によれば、原告が「被告本人が書き込み等を行った者である」ことに対する立証責任を負うことになる。

かかる一般原則によれば、被告が遠隔操作ウイルスによる書き込み等の主張を行ったときには、当該機器を被告以外の第三者が使用して送信していないことや

被告の知らないところで遠隔操作されて送信していないことを原告が立証しなければならないことになる。

(2)　遠隔操作ウイルス等に関する主張の特殊性

遠隔操作ウイルス等を用いる者は、自らが行為者であると分からないようにするために行うのであり、通常は、第三者はもちろん、機器を管理している被告自身にも遠隔操作ウイルス等の仕業であると分からないような工夫が施されている。そのため、このような立証責任の分配を貫くと、機器を管理すらしていない原告側に事実上、不可能を強いることになり、インターネット上で権利侵害された原告の民事的救済を全く図れない結果となる危険性がある。

(3)　立証責任の分配によって解決することの可否

上記のような危険性と立証責任の公平な分配という観点から、問題となる書き込みなどが遠隔操作ウイルスに感染したこと等により行われたことについての立証責任を被告側に負わせるべきとして、ＩＰアドレス等による機器の特定がなされた場合には、本人性に関する推定を働かせるべきであるとの考え方もあり得る。

しかし、遠隔操作ウイルス等の登場によって、ＩＰアドレスの本人性に関する証明力は下がっているにも関わらず、そのような本人性の推定を認める考え方は採り得ない。

そして、本人性の事実認定は、遠隔操作ウイルス等の問題に限らず多種多様であることも考えると、これを安易に立証責任の問題として解決することはできない。

ＩＰアドレスによる機器の特定は、あくまで本人性に係る重要な間接事実の一つに過ぎず、主要事実である本人性との関係では、遠隔操作ウイルス等により第三者によって当該行為が行われたという事実と同じ位置づけである。

したがって、これらの本人性に関する間接事実の優劣を両当事者の主張・立証を通じて丁寧に検討した上で、事実認定していくべき問題と考える。この点、従前、本人性が争われた事例においても、背景事情やアリバイといった間接事実を踏まえて事実認定が行われており、今後もこのような実務運用によって、公平な裁判の実現を図るしかないと思われる。[23]

(4)　機器の管理者としての責任

遠隔操作されるような通信機器を放置していたことに基づく、いわば管理責任については、多くの人が利用するインターネットに接続する機器を利用する以上、それに伴う責任が全く存在しないと考えることはできない。

しかし、この責任を強調しすぎることは、自動車の運行供用者責任[4]に近い責任を機器の管理者に負わせる考え方になりかねない。自動車における運行供用者の責任は、自動車の身体・生命に対する危険性に鑑みて、特に立法的な手当をし

---

[2] 東京地判平成 19 年 4 月 11 日（平成 18 年（ワ）第 16523 号）。

[3] 東京地判平成 24 年 1 月 31 日（判時 2154 号 80 頁）。控訴審（東京高判平成 24 年 6 月 28 日）。

[4]自動車損害賠償保障法 3 条参照

て認めた責任であるが、現状、インターネットに接続できる通信機器がこのような直接的な危険性を持つものとまでは認められない。

逆にこのような法的責任を管理者に認めることは、国民のインターネット利用を阻害するだけでなく、場合によっては、全ての通信機器について、自動車と同様に登録制度を導入する引き金になりかねない。これでは、通信機器が国家の監視下におかれ、不当な表現の自由や通信の秘密の侵害が行われる虞が生じる。

したがって、条理上、第三者の権利を不当に侵害しないように配慮する注意義務についても、一定程度、認められるべきではあるが、インターネットが誰でも自由に利用できる環境であるという点が重視されている我が国の現状においては、その注意義務の程度を高く設定することは妥当ではない。

４　発信者情報開示請求事件への影響

遠隔操作ウイルス等による第三者による侵害情報の送信等の可能性を受け、発信者情報開示請求において、開示請求者は、遠隔操作ウイルスに感染した上での送信ではないことの主張・立証責任まで負担するか。

開示請求を認める同法４条１項は開示対象について、「発信者」とは別に「発信者情報」を定義し、これを「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」と定めている。そしてこれを受けた政令においては、「発信者」そのものの情報のみならず周辺情報である「侵害情報の送信に係る者」の住所や、「侵害情報」に係るＩＰアドレス、タイムスタンプ情報、インターネット接続サービス利用者識別符号、ＳＩＭカード識別番号等を開示の対象として指定している。また、同項１号は、開示請求の要件として「権利が侵害されたことが明らかである」ことを規定しているが、これが「発信者」によってなされたことを要件としていない。

このような条文の規定を前提にすると、侵害情報に係るＩＰアドレスやタイムスタンプ情報等の開示が認められることは当然である。また、遠隔操作ウイルスの感染により、意思に基づかずに侵害情報の送信が行われていたとしても、その管理の下にある機器によって侵害情報が送信されている以上、端末管理者は「侵害情報の送信に係る者」に該当し、電子メールアドレス以外の情報の開示は認められると解される。

そのため、遠隔操作ウイルス等への感染可能性は、発信者情報開示請求において具体的な攻撃防御方法には該当せず、与える影響はそれほど大きくないといえる。

５　まとめ

以上見てきたとおり、遠隔操作ウイルス等の登場によって、ＩＰアドレスと本人性をつなぐ推定力は低下したが、刑事事件、民事事件ともにこれを実際の運用で対応せざるを得ないと思われる。今般、ＩＰアドレスを偽装するサービスの提供もなされ始めていることを鑑みると、今後、この傾向はさらに加速すると思われる。このためインターネット上での犯罪対応や不法行為に対する法的救済が困難となる虞があることから、ＩＰアドレスを偽装するような行為に対する直接的な法規制といった対応について検討する必要があると思われる。

以上