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.）

【大阪弁護士会電子商取引問題研究会】
弁護士　森　拓也　弁護士法人きっかわ総合法律事務所　mori@kikkawalaw.com
立命館大学法科大学院非常勤講師（情報法）
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

はじめに

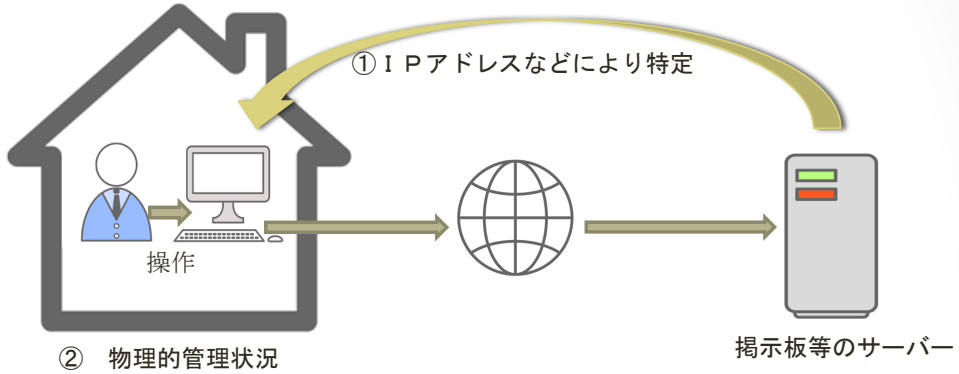
- 近時、コンピュータウイルス等を使って、他人のパソコンを遠隔操作するなどの方法により犯罪予告の書き込みをさせたことから、遠隔操作されたパソコンの管理者が誤認逮捕されるといった事件の発生。

- 刑事事件における犯人性及び管理者としての幇助犯の成立
- 民事の損害賠償請求事件などにおける本人性及び管理者責任
- 発信者情報開示請求

のそれぞれについて検討。

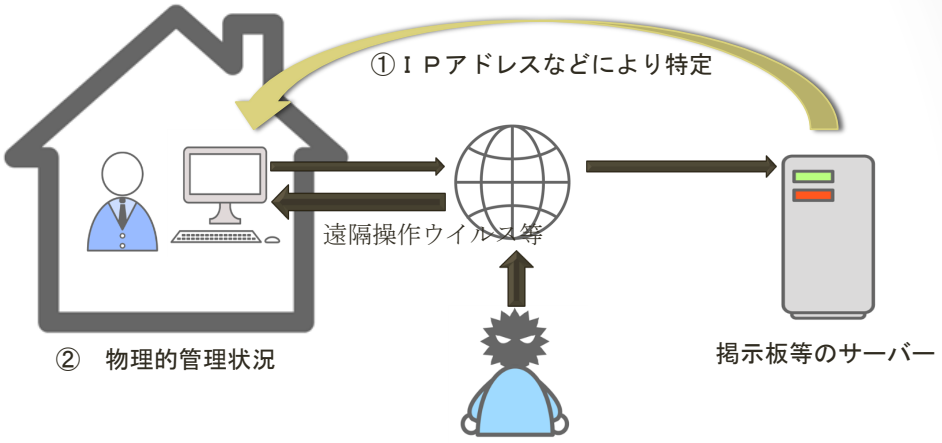
刑事事件における犯人性の立証

(1)　犯人性についての従来の事実認定の概略



従前は、「ＩＰアドレス等による機器の特定」　に加えて
① 当該通信機器の設置場所や設置状況（自宅、持ち運び等）
② 物理的な犯行の可能性（アリバイ等）
などの他の間接事実で補完し、
「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」こと
の証明により、ほぼ合理的な疑いを排除できるだけの立証あり。

(2)　遠隔操作ウイルス等の登場による影響



「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、犯人性の立証としては十分ではなくなった。

⇩　追加立証が必要

(2)　遠隔操作ウイルス等の登場による影響

⇩　具体的には

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（単にウイルスがなかっただけでは足りない）。
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、被害者との人的関係性、動機
④ 書き込みの内容それ自体。
⑤ ウイルス等の侵入経路に関する被告人の供述内容。
⑥ 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。

(3)　強制捜査に与える影響

【誤認逮捕・起訴事案の問題点】

- ＝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評価。

【逮捕や捜索の要件論への影響】

- ＝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、とするか？
- →　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

＊実際に事件を担当した弁護人の問題意識

1　捜査機関が、第三者の犯行を考慮していなかったこと

2　捜査機関が、十分なＩＴ知識を持ち合わせていない点

(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

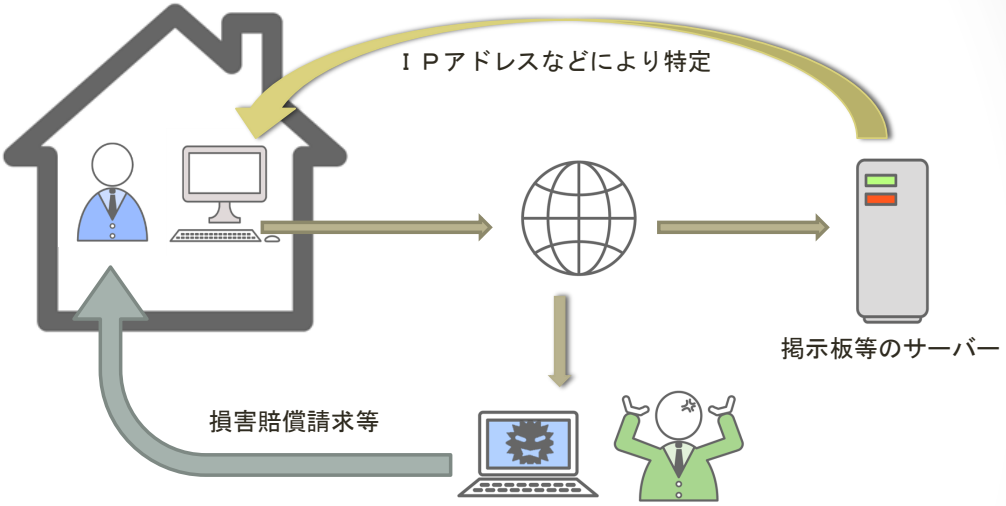
① これを認めるとあまりにも幇助犯の範囲が広がりすぎること等から、不作為の幇助犯の成立自体に疑問がある。

② 幇助犯における故意の範囲についてのいわゆる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。

- 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。

民事事件における本人性の立証

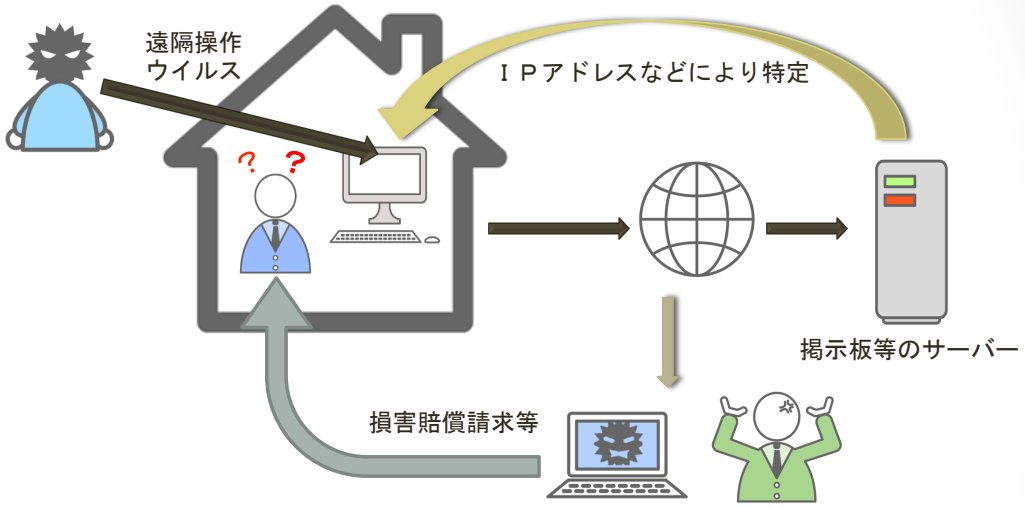
(1)　民事事件における立証責任一般



【証明責任に関する一般原則】

- 一定の法律効果を主張する者は、その効果の発生を基礎づける適用法条の要件事実につき証明責任を負う（法律要件分類説）。
- したがって、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。

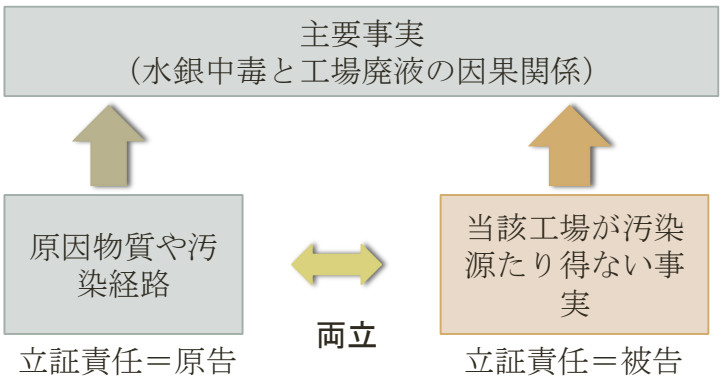
(2)　遠隔操作ウイルス等に関する主張の特殊性



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ため、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あり。

(3)　立証責任の分配によって解決することの可否

【間接反証理論】
ある主要事実につき証明責任を負う当事者が、その主要事実を推認させるに足る間接事実の存在を証明した場合に、相手方が、右間接事実と両立しうる別の事実の存在を立証することによって、右間接事実による主要事実の推認が疑わしいことを明らかにし、主要事実につき裁判官が心証を形成するのを妨げるための証拠ないし証明活動。
→　証拠が偏在する公害訴訟の因果関係の認定などで採用



(3)　立証責任の分配によって解決することの可否（私見）

- 公害事件においては、因果関係を時系列を逆になぞって、①原因物質の特定、②摂取経路、③排出の3段階に分け、①と②を原告が立証し、被告の門前まできた場合に③について強い蓋然性を持つものとして事実上の推定を行っていると解される。
- 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が低下。
- 反証の対象が被告のパソコン等の内部だけの問題ではなくなり、そこまでの推定力を認めるのは、被告に酷。
- 従前の裁判例においても、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いる。

間接反証の前提となる一応の推定力をＩＰアドレスの特定という事実は持ち得ない。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。

(4)　機器の管理者としての責任（私見）

- 自動車の運行供用者責任に近い責任を立法の手当なく通信機器の管理者に負わせることになる。
- 条理に基づく管理責任の強調は、国民のインターネット利用を阻害する。
- ひいては全ての通信機器の登録制度を導入など、通信機器に対する国家の管理強化が行われ、不当な表現の自由や通信の秘密の侵害が行われる虞れ。

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。

発信者情報開示請求事件への影響

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、機器管理者＝発信者という推定力は下がった。この結果、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。】

【定義】

- 「発信者」
  ＝特定電気通信役務提供者の用いる特定電気通信設備の記録媒体に情報を記録し、又は当該特定電気通信設備の送信装置に情報を入力した者（2条4号）

- 「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（4条1項）

総務省令で定めるもの

① 発信者その他侵害情報の送信に係る者の氏名又は名称
② 発信者その他侵害情報の送信に係る者の住所
③ 発信者の電子メールアドレス
④ 侵害情報に係るIPアドレス
⑤ 侵害情報に係る携帯電話端末又はPHS端末からのインターネット接続サービス利用者識別符号
⑥ 侵害情報に係るSIMカード識別番号のうち、当該サービスより送信されたもの
⑦ 上記④のIPアドレスを割り当てられた電気通信設備、⑤の携帯電話端末等からのインターネット接続サービス利用者識別符号に係る携帯電話端末、⑥のSIMカード識別番号に係る携帯電話端末から、開示関係役務提供者の用いる特定電気通信設備に侵害情報が送信された年月日及び時刻

私見

① 条文上、開示の対象は、「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おり、これらが開示対象となることは文言上、当然。
② 遠隔操作ウイルスの感染等により、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。
③ 4条1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以上、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しない。
④ 遠隔操作ウイルス等の存在は、当該機器の管理者と発信者の同一性の証明力に影響を与えるものに過ぎず、従前からこの同一性は証明の対象とされてこなかった。

メールアドレス以外は影響なし。
メールアドレスに関しては文言解釈上は、困難か？

メールアドレスの開示が認められる余地はないか

- 侵害情報が、電子メールにより送信された場合（ブログ、掲示板への電子メールを利用した投稿も含む）については、仮に第三者による遠隔操作の可能性があるとしても、同第三者が利用したメールアドレスは「発信者」が利用したメールアドレスに当たらないか。
- SNS（Facebook、Twitter等）のログインIDとしてメールアドレスが利用されている場合、当該IDで侵害情報が投稿された場合も、仮に第三者による遠隔操作の可能性があるとしても、当該投稿を行った時点で「発信者」が利用していたIDのメールアドレスは「発信者」のメールアドレスと解すことはできないか。
- プライバシー権等に考慮しつつ、情報の流通による被害の救済を図る発信者情報開示制度の趣旨に照らすと、権利侵害に当該メールアドレスが利用されている場合は、開示の対象となってしかるべきではないか。

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。