応
般

不正プログラム判断の混沌
―無限アラート事件と Coinhive 無罪判決から考える―

楠　正憲 | 国際大学 Glocom

警察庁は 2019 年 3 月 7 日，2018 年におけるサイバー空間の脅威について情勢を発表し，サイバー犯罪の検挙件数が過去最多の 9,040 件に達したことを発表した．来年に迫った 2020 年東京オリンピック・パラリンピック競技大会へ向けて，さまざまなサイバーセキュリティ対策を推進する計画だという．一方で最近のサイバー捜査について，エンジニアの間では不安の声も広がっている．

2019 年 3 月，兵庫県警は電子掲示板に不正プログラムへのリンクを書き込んだ不正指令電磁的記録供用未遂の疑いで女子中学生を家宅捜索のち補導，男性 2 人を家宅捜索し書類送検した．報道で 2018 年にも男子中学生と男子大学生が同様の罪状で摘発されていたことが明らかとなった．

いわゆる補導というと，深夜の街を徘徊して補導され，親に引き渡されるといったものを想像しがちだが，今回は家宅捜索が行われているなど，もっと深刻な事態といえる．書類送検された男性は前科がつき ESTA（電子渡航認証システムによるビザ免除プログラム）で米国に入国できずビザが必要となるなど，重いペナルティを負う．

今回問題となった不正プログラムは「何回閉じても無駄ですよ～」とメッセージを表示し，OK ボタンを押してダイアログを消しても何度もダイアログが表示され続けるという稚拙なものだ（図 -1）．

このプログラムが表示するダイアログは最新のブラウザであれば，ブラウザのウィンドウやタブを閉じることで，簡単に消すことができる．

当該サイトは 2014 年ごろから米国ネバダ州に登記され大阪市の企業が運営している FC2 にホスティングされ，2 ちゃんねるなどの巨大掲示板からしばしばリンクされていた．データを破壊する，他に感染するといった有害な機能はなく，ちょっとしたジョークプログラムで，必ずしも悪質とは言いがたく，世の中でいうところのコンピュータウィルスやマルウェアとは言いがたい．もっと範囲の広い PUPs（Potentially Unwanted Programs）の定義にさえあてはまらないのではないか．

ここで改めて刑法の「不正指令電磁的記録供用」について，その定義を確認すると**「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず，又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録」**とある．

確かにダイアログを消したい利用者に対して，

```
for（；；）{
window. alert("　∧_∧　ババババ¥n（・ω・)=つ≡つ¥n（っ ≡つ ＝つ¥n`/　　)¥n( ノ∏U ¥n何回閉じても無駄ですよ～ ww¥nm9（＾Д＾）プギャー！！")
}
```

図 -1　問題となった JavaScript プログラム

OK ボタンを押し続けても幾度となくダイアログを表示することは「その意図に沿うべき動作」とはいえず，「その意図に反する動作」といえないこともない．報道によると補導された女子生徒は「自分が困ったのでほかの人が同じ被害に遭えば面白いと思った」と話したということで，当該 URL に利用者を誘導することで，困らせようという犯意があったとされる．専門家にとっては他愛のない無害ないたずらであっても，古いブラウザを利用していたり，平均的 IT リテラシーであれば忙しいタイミングで本当に迷惑となる可能性もある．意図して他人を困らせた場合は，罪に問われるべきだという考え方もできよう．

しかしながら UI プログラミングでループを使うことはごく一般的で，OK を押してもダイアログが表示され続けるといった状態も，時にはバグで起こってしまうことも少なくない．

単なるループを書くだけで逮捕されたのではかなわないということで，データサイエンティストの加藤公一氏は「みんなで逮捕されようプロジェクト」を立ち上げ，Github 上で補導の原因になったものと同様のプログラムを公開した．セキュリティエンジニアの ozuma 氏は，逮捕を避けるためにセキュリティ勉強会の開催を保留するなど「既に萎縮している」といい，兵庫県警に対して何を根拠に犯罪と見なすのかの情報公開を請求した．日本ハッカー協会の実施した裁判支援のための募金活動には，612 名から計 7,074,553 円もの寄付が寄せられたという．

何がサイバー犯罪にあたって，何があたらないか，その定義は揺れているのが実情だ．2018 年 6 月に閲覧者のブラウザで同意を得ずに暗号資産 Monero を採掘していた Web デザイナが神奈川県警に逮捕された事件では 2019 年 3 月 27 日に無罪判決が出た．判決では Coinhive について，閲覧者の同意を得る仕組みがなかったため「人の意図に反する動作をさせるべきプログラム」にあたるとしつつも，消費電力の増加や処理速度の低下といった影響は「大きく変わらない」と判断．「不正な指令を与えるプログラムと判断するには，合理的な疑いが残る」としている．

Coinhive を巡っては，全国 10 の県警が合計 16 人を検挙し，多くは略式起訴で罰金刑を科され，その刑は確定している．今回の裁判で Coinhive が不正指令電磁的記録ではないという判決が出ても，その前科が消えるわけではない．

Coinhive の場合，その社会的評価が定まる前であったことも無罪判決の理由となった．利用者はコンピュータの中で何がどう動いているか，必ずしも詳しいわけではなく，Web サイトのソースコードを解析するわけでもなく，個々のコードの挙動について想像が働くとも限らない中で，データ同期やアクセス解析など，目に見えないさまざまなプログラムがブラウザで動いている．さまざまな新技術に対して，その社会的評価が定まる前に「利用者の意図に沿うべき動作」かどうかだけで断罪されかねないことに対して技術者が漠とした不安を感じるのは無理からぬことだ．

刑法での「不正指令電磁的記録供用」の定義において，反意図性の輪郭が非常に広い上，不正性について輪郭が不明確で，社会での合意形成が追い付かず，警察と利用者，専門家の間で認識に齟齬を生じやすいことが，こうした問題が起こる原因ではなかろうか．

米英仏独をはじめとして多くの国々がマルウェアの作成や配布は規制しているが，データの破壊や改竄，不正取得といった具体的な悪意ある挙動に対して規制しており，日本の刑法と比べて処罰の対象となる行為が明確となっている．

現状の定義のままでも，早期に被害を抑制する観点からいえば，いきなり逮捕のための証拠固めから入るよりは，サイトが法に触れる可能性について事前に警告を行ったり，ホスティング事業者を通じてサイト自体を停止させる方法が有効だ．

たとえば前述の無限アラート事件の場合，2014

年頃から存在した当該サイトを止めるのではなくて，リンクを張った中学生をいきなり補導する，という選択は妥当だったのだろうか．本当に無限アラートのサイトが悪質で，被害者がいるのであれば，リンクを張った者を補導なり逮捕するよりも前に，2014年の段階でサイト自体を止めるべきだった．

サイバー犯罪の検挙が増えている一方で，2018年に起こったコインチェック事件やZaif事件，横行するICO（Initial Coin Offering：新規に暗号資産を発行して資金調達すること）詐欺といった大規模な被害のあった事案では犯人が逮捕されていない．外野から見ると，巨悪を放置したまま，簡単に捕まえられる微罪ばかり挙げているようにも見える．

県境どころか国境さえないサイバー犯罪に対して，捜査体制は今も県警単位の縦割りとなっているため，本来は優先度が高い大規模事案に捜査能力を集中できていないのではないか．また，特に国境を越えた事案に対して国際捜査協力を行うにも限界があり，高度な技術で足跡を消そうとする悪質犯罪を追跡しようにも技術的に限界があることは確かだ．米欧での摘発事例を見ると，おとり捜査が有効であることが分かっているが，日本の法令では厳しく制限されている．

増大するサイバー犯罪に対して，警察は被害の大きな事案で成果を挙げられない状況にある．無限アラート事件やCoinhive事件といった悪質性に対する評価が分かれる事例に拙速に取り組むことは，被害の抑止よりも立場の弱い容疑者に飛びついて検挙件数の積み上げを優先しているように見られる．そんなふうに見られることは警察としても決して本意ではないだろう．

歴史をたどれば，無実の思想犯を弾圧した戦前の反省を踏まえて，戦後日本は国家警察を廃止して都道府県単位の警察を整備した．戦前の反省から生まれた制度が，サイバー犯罪の時代においてはかえって県単位の縦割りによる人材不足や不十分な捜査体制と，微罪逮捕に結びついているとしたら，とても皮肉な話だ．

サイバー犯罪の増加に直面しているいま，国境を越えた悪質なサイバー犯罪に対して毅然とした措置を講じつつ，社会的評価の定まっていない新技術に対しては実態の把握と被害の抑止を迅速に行えるよう体制を整備することが大事である．うわべの検挙件数を追うよりも，まずは被害の抑制を図るべく，取り組むべきことがほかにもあるのではないだろうか．

(2019年4月3日受付)

楠　正憲（正会員）　masanork@gmail.com
マイクロソフト，ヤフーなどを経て2017年からJapan Digital Design CTO．内閣官房 政府CIO補佐官としてマイナンバー制度を支える情報システム等の構築に従事．