Wizard Bible事件から考えるサイバーセキュリティ

著者　齊藤貴義　IPUSIRON

PEAKS

Wizard Bible事件から考えるサイバーセキュリティ

著者　齊藤貴義　IPUSIRON

PEAKS

はじめに

本書はサイバー犯罪関連法の問題点について警鐘を鳴らすことを目的としています。

国民をサイバー犯罪から守るための法律が、近年になってサイバー犯罪とは必ずしも言い難い事例に適用されて大きな問題となりました。これにより、日本のセキュリティ研究が萎縮する事態に陥っています。本書では、その代表的な事件として「Wizard Bible 事件」「Coinhive 事件」「アラートループ事件」を採り上げて詳細を解明していきます。

Wizard Bible 事件　2017 年に読者投稿型の Web マガジン「Wizard Bible」を運営していた IPUSIRON さんが、読者投稿でコンピュータウイルスのプログラムが公開されているとして家宅捜索と略式起訴されました。しかし、問題とされた読者投稿は単純なネットワークプログラムだったのではないかと指摘する専門家も多数います。

Coinhive 事件　2018 年から 2019 年にかけて、Web サイトに仮想通貨のマイニングツール Coinhive を無断で設置していたとして警察から 21 人が家宅捜索を受けました。Coinhive はコンピュータウイルスのような不正利用には該当しないとする見解が多数出ています。

アラートループ事件　2019 年にブラウザを不正操作するリンクを掲示板に投稿したとして、警察から 3 人が家宅捜索を受けました。しかし、貼られたリンク先に設置されたプログラムは JavaScript のアラート機能を利用したジョークプログラムであり、セキュリティ関係者や IT エンジニアを中心に警察の捜査に大きな疑問の声が湧き起こりました。

これらの事件では、一般人がサイバー犯罪とは思われない容疑で家宅捜索を受けました。次はこの本を読んでいるあなた自身やあなたの身近な人にも同じような事件が起きるかもしれません。

一連の事件を通じて、日本のサイバーセキュリティ研究を立て直すために何が必要なのかを究明していきます。また本書では、事件を追うだけではなく、現行法上でどのように自衛すべきかというサバイバル術も考えていきます。

無実の罪でサイバー犯罪の摘発に巻き込まれないために本書は役に立ちます。また、もし自分が身に憶えのないサイバー犯罪の摘発に遭ってしまったら、まず本書を読んでください。そしてご家族に本書を渡してください。

本書ではサイバー犯罪関連法の改正についても検討していきます。本書を通じてサイバー犯罪関連法についての議論が活発となり、日本のセキュリティ研究が進歩することを願っています。

本書は、第 6 回技術書典で頒布した同人誌『Web セキュリティのミライ』が元になっています。『Web セキュリティのミライ』は「第 1 回 刺され！技術書アワード」において大賞を受賞し、PEAKS でクラウドファンディングを開催することになりました。クラウドファンディングは開始 2 日目で目標金額を達成し、その後も多数の支援がありました。この支援を元に本書は執筆されました。

目次

第 1 章

不正指令電磁的記録に関する罪とは何か

本章では、Wizard Bible 事件・Coinhive 事件・アラートループ事件を検証していくために、まずこれらの事件が捜査される原因となった「不正指令電磁的記録の罪」を解説していきます。法律を知ることで何が争点となったのかが明確になります。また法律自体にどのような問題があるのかも理解できるようになるでしょう。

1.1 不正指令電磁的記録の罪の条文

コンピュータウイルスを作ることは犯罪であると多くの人が認識しています。しかし、それを処罰する法律がどのような内容になっているのかを正確に把握している人は少ないでしょう。その法律は、刑法の「不正指令電磁的記録に関する罪」（以降、不正指令電磁的記録の罪）と言います。

コンピュータウイルスを取り締まる法律ですから、何がコンピュータウイルスに該当するのかやどんな行為が処罰されるのかは条文で明確に規定されていると思っている方もいるかもしれません。しかし、もし明確な定義が無かったとしたらどうでしょうか。

刑法第 19 章「印章偽造の罪」の第 168 条の 2 項および 3 項に、不正指令電磁的記録の罪が書かれています。この不正指令電磁的記録の罪は、一般的には「ウイルス作成罪」として知られており、コンピュータ使用者の意図に反して（不正指令）動作するプログラム（電磁的記録）の作成を罰するための条文です。

第 168 条の 2
（不正指令電磁的記録作成等）
正当な理由がないのに、人の電子計算機における実行の用に供する目的で、次に掲げる電磁的記録その他の記録を作成し、又は提供した者は、三年以下の懲役又は五十万円以下の罰金に処する。
一. 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
二. 前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録
2. 正当な理由がないのに、前項第一号に掲げる電磁的記録を人の電子計算機における実行の用に供した者も、同項と同様とする。
3. 前項の罪の未遂は、罰する。

第 168 条の 3
（不正指令電磁的記録取得等）

正当な理由がないのに、前条第一項の目的で、同項各号に掲げる電磁的記録その他の記録を取得し、又は保管した者は、二年以下の懲役又は三十万円以下の罰金に処する。

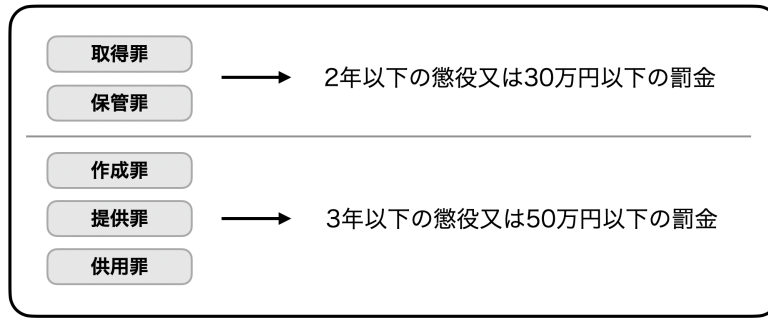
条文は難解ですが、幾つかのキーワードを抽出してみていくと基本構造がわかります。そのキーワードとは「正当な理由がないのに」「実行の用に供する」「意図に反する動作をさせるべき不正な指令」です。

つまりこの不正指令電磁的記録の罪は、とても簡単に表現すると、正当な目的がないのにコンピュータ利用者の意図に反する不正な指令を実行させるプログラムを実用目的で作成したり所持したりする人を処罰する条文となっています。つまり何をもってコンピュータウイルスとするかは人間の意思に依存します。

不正指令電磁的記録の罪には大きく 5 つの種類の罪があります。「取得罪」「保管罪」「作成罪」「提供罪」「供用罪」です。

不正なプログラムをネットなどから新規に入手する「取得罪」、不正なプログラムを手元に置いておく「保管罪」は比較的罪が軽く、2 年以下の懲役または 30 万円以下の罰金となっています。

不正なプログラムを作成した場合の「作成罪」やサイトなどで提供した場合の「提供罪」、リンクに誘導させるなど他人に意図的に実行させた場合の「供用罪」は比較的罪が重く、3 年以下の懲役または 50 万円以下の罰金となっています（図 1.1）。



●図 1.1　不正指令電磁的記録の罪の種類

なぜ、このような人間の意図でもってコンピュータウイルスを処罰する法律が制定されたのでしょうか。

1.2　不正指令電磁的記録の罪が制定された経緯

不正指令電磁的記録の罪が制定された経緯について解説します。インターネット利用者が拡大するにつれて、インターネットを利用した犯罪については国内でも海外でもその対策が求められていました。

日本政府はインターネット犯罪の増加に対処するため、2000 年に不正アクセス禁止法を国会で成立させました[注1)]。その後、世界各国が協調してサイバー犯罪対策に取り組んでいくために、2001 年に欧州評議会が中心となってサイバー犯罪条約が起草されました。

日本政府もこのサイバー犯罪条約に批准[注2)]するため国会の承認を取り付けたのですが、国内法が未整備のため長らく批准できませんでした。日本政府は、不正指令電磁的記録の罪を制定するため刑法改正案を 3 回も国会に提出しましたが、共謀罪[注3)]を制定する条文改正とセットであったため廃案となっていました。

しかし、2011 年 3 月 11 日、東日本大震災が起きた日に、刑法改正案から共謀罪を除いた「情報処理の高度化等に対処するための刑法等の一部を改正する法律」が閣議決定されました。その直後に起きた東日本大震災と原発事故による社会の混乱がまだ収まらない中、国会で審議が行われました。審議中の 2011 年 5 月に、江田五月法務大臣が「コンピュータのバグを放置した場合も不正指令電磁的記録に当たる」と答弁して大きな問題になりました。後にこの見解は撤回されていますが、何をもって不正指令電磁的記録を指すのかが曖昧であることを示す一例と言えるでしょう。

情報処理学会、インターネットユーザー協会などが反対声明を出す中、2011 年 6 月に国会で改正案が承認されました。参議院で審議された際、以下の附帯決議[注4)]も合わせて採択されました。憲法の保障する表現の自由や、ソフトウェア開発・流通に影響を生じることがないように努めるよう指摘した決議です。

■ 附帯決議

政府は，本法の施行に当たり、次の事項について特段の配慮をすべきである。
不正指令電磁的記録に関する罪（刑法第 19 章の 2）における「人の電子計算機における実効の用に供する目的」とは，単に他人の電子計算機において電磁的記録を実行する目的ではなく，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ない電磁的記録であるなど当該電磁的記録が不正指令電磁的記録であることを認識認容しつつ実行する目的であることなど同罪の構成要件の意義を周知徹底することに努めること。また、その捜査等に当たっては，憲法の保障する表現の自由を踏まえ、ソフトウェアの開発や流通等に対して影響が生じることのないよう、適切な運用に努めること。

そしてこの法律は 2011 年 7 月に施行されました。これにより、日本はサイバー犯罪条約に加盟する準備が整い、国内でも条約が効力を発生することになりました。

注1） この不正アクセス禁止法によって Librahack 事件が発生した。2010 年 3 月に愛知県岡崎市の岡崎市立図書館で蔵書検索システムに障害が発生。岡崎市立図書館の蔵書検索システムにクローラーで自動的に情報を収集していた男性が、愛知県警によって偽計業務妨害容疑で逮捕された。専門家や IT エンジニアからクローラーを設置しただけでは罪には問えないとして疑問の声が多数あがった。この事件は「岡崎市立中央図書館事件」または男性が Librahack というサイト http://librahack.jp/ を開設したことから「Librahack 事件」と呼ばれている。

注2） 条約を取り結ぶための最終的な同意手続き。

注3） 組織犯罪処罰法の改正法案。テロ対策としてテロを計画したり準備したりするだけで処罰される。法案を巡って日本国内で賛否が分かれた。

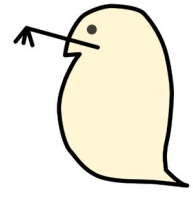
注4） 議決された法案に対して付けられる意見書。法的拘束力はない。

第 2 章

Wizard Bible 事件ロングインタビュー

2017 年にアンダーグラウンド[注1)]系 Web マガジン『Wizard Bible』を主宰していた IPUSIRON さん[注2)]は不正指令電磁的記録提供の容疑で宮城県警から家宅捜索を受け、検察から略式起訴されて Wizard Bible を閉鎖しました。この一連の騒動は「Wizard Bible 事件」と呼ばれています。

2019 年 3 月 15 日に IPUSIRON さんにロングインタビューを行い、前作の同人誌『Web セキュリティのミライ』に掲載しました。『Web セキュリティのミライ』は、技術書典「刺され！技術書アワード」第 1 回の大賞を受賞して、より内容を充実させた本書『Wizard Bible 事件から考えるサイバーセキュリティ』のクラウドファンディングが成立しました。本書を執筆するにあたり、再度インタビューを行いました。Wizard Bible 事件がどのようにして起きて、なぜ Web サイト閉鎖に至ったのか明らかにしていきます。



●図 2.1　IPUSIRON さんの SNS アイコン

■ IPUSIRON

1979 年、福島県相馬市生まれ。1999 年 5 月頃にアンダーグラウンドサイトを公開。2003 年頃に Wizard Bible を発行開始。2017 年に Wizard Bible の記事の件で警察から家宅捜索を受け、2018 年に検察から Wizard Bible を閉鎖するよう迫られ Wizard Bible を閉鎖。その後、略式起訴されて罰金刑が確定。2018 年に相馬でサークル「ミライ・ハッキング・ラボ」を設立。

業務アプリなどの設計・開発、スマホアプリや Web アプリの検査・デバッグ、機械警備・防災設備の設置に従事。情報セキュリティと物理的セキュリティを総合的な観点から研究しつつ、執筆を中心に活動中。

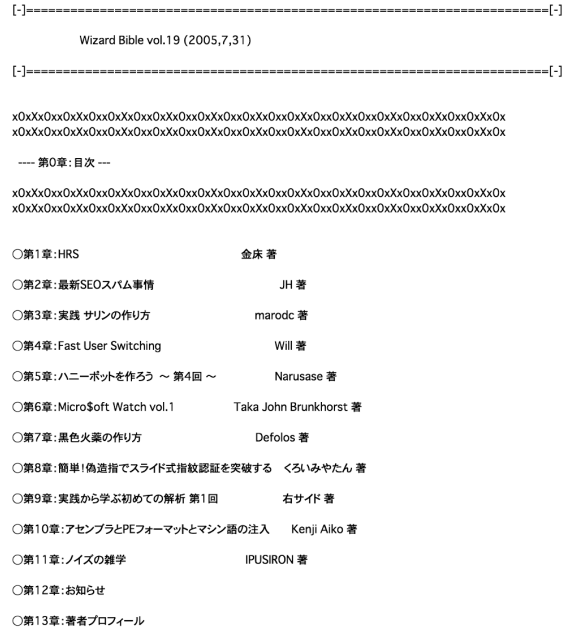
『ハッキング・ラボのつくりかた』『暗号技術のすべて』『ハッカーの学校』『ハッカーの学校 個人情報調査の教科書』『ハッカーの学校 鍵開けの教科書』『パスワード解析 完全版』など多数の著書を刊行。

注1）「地下」「地面の下」から転じて、裏の世界のことを指す。「アングラ」「UG」と略されることもある。コンピュータ系のアンダーグラウンドでは、ハッキング、クラッキング、ソフトウェア解析、電話のタダ掛け、ウイルス作成、匿名化、コピー技術などが扱われていた。

注2）https://twitter.com/ipusiron

■ **Wizard Bible**

セキュリティ・アカデメイアというサイトで発行されていたアンダーグラウンド系 Web マガジン（E-magazine）。プレーンテキスト形式。
コンピュータ関連のセキュリティやハッキングの話題が多かったが、広義のアンダーグラウンドの情報を扱っており、武器の作り方・ピッキング・詐欺・宗教問題など投稿者が自分の好きな話題を自由に投稿できた。2003 年に創刊号が出て、2017 年に vol.64 が発行されていた。検察からの圧力により 2018 年に閉鎖。


[-]==========[-]

Wizard Bible vol.19 (2005,7,31)

[-]==========[-]

x0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0x
x0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0x

---- 第0章：目次 ---

x0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0x
x0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0xx0xXx0x

○第1章：HRS　金床 著
○第2章：最新SEOスパム事情　JH 著
○第3章：実践 サリンの作り方　marodc 著
○第4章：Fast User Switching　Will 著
○第5章：ハニーポットを作ろう ～ 第4回 ～　Narusase 著
○第6章：Micro$oft Watch vol.1　Taka John Brunkhorst 著
○第7章：黒色火薬の作り方　Defolos 著
○第8章：簡単！偽造指でスライド式指紋認証を突破する　くろいみやたん 著
○第9章：実践から学ぶ初めての解析 第1回　右サイド 著
○第10章：アセンブラとPEフォーマットとマシン語の注入　Kenji Aiko 著
○第11章：ノイズの雑学　IPUSIRON 著
○第12章：お知らせ
○第13章：著者プロフィール

●図 2.2　Wizard Bible vol.19

2.1 IPUSIRON さんへのインタビュー

今回のインタビューのきっかけ

齊藤　2019 年 3 月、兵庫県警は中学生と 2 人の成人を JavaScript のブラクラ[注3)]を共有したとして不正指令電磁的記録供用の疑いで家宅捜索しました。ネットではこの JavaScript は単にループ処理を実装したものであり、これだけでは罪に問えないのではないかと指摘されています。また、

注3)　ブラウザクラッシャーの略。ブラウザに深刻な悪影響を与える Web ページやプログラムを指す。

ループ処理を書いたり共有したりするだけで罪となってしまうようではコードを書く人が萎縮してしまうのではないかという議論が出ています。

この兵庫県警のアラートループ事件や Coinhive 事件をきっかけとして、インターネット上では、不正指令電磁的記録の罪に関する法律が現場の警察によって恣意的に運用されているのではないかという問題意識が広がっています。その原点に位置する事件として、Wizard Bible 事件について本書では取り上げていきたいと思います。そもそも何が問題であったのか、警察がどのように取り調べを行ったのか、その中から得られる教訓についてお話を伺おうと思います。まず Wizard Bible を始められたきっかけについて教えて頂けますか？

アンダーグラウンドへの目覚め

IPUSIRON　大学受験の自宅浪人時代の 1999 年頃に、受験勉強の反動からパソコンが欲しくなりました。それまでは Windows パソコンを持っておらず、パソコン雑誌だけを軽く読んでいました。受験勉強の真っ最中ともいえる自宅浪人の 11 月頃に、仙台の Laox で人生初の Windows マシンを貯金で購入しました。メビウスノートで当時は 30 万円くらいしたかと思います。

ノートパソコンを購入した帰りに、Laox の同ビル内のパソコン書籍専門の本屋に寄りました。目に入った本がデータハウスの『コンピュータ悪のマニュアル 2』でした。それを購入しました。初めて Windows マシンを入手した当日に、アンダーグラウンドに出会ったといえます。

仙台から相馬へ電車で帰る中、その本を読み、掲示板荒らしやメールボム[注4)]という用語に触れました。これが私の心に強烈なインパクトを与え、今でもその電車の様子が思い出となって脳裏に刻まれています。当時はインターネットの知識もなかったので、読んでいて想像の域を超えなかったのですが、大学に入学したらインターネットをやってみたいと決意しました。

大学に入学し、東京で一人暮らしを始めました。インターネットに接続するために、プロバイダと契約しました。ダイヤルアップでしたので、テレホーダイ[注5)]にも加入しました。その頃は第 2 次アンダーグラウンドブームであり、アンダーグラウンド系の本・雑誌が氾濫している時代でした。ネット上ではアンダーグラウンドサイトが毎日のように作られていました。当時は全くパソコンやアンダーグラウンドの知識がなかったので、毎日わくわくしながらアンダーグラウンドリンク集を起点にしてサイトを巡回していました。

その当時のインターネットはブログや Twitter などもまだなく、個人が情報を発信する時にはサイトを制作するしかありませんでした。かなりの手間と HTML などの知識が必要です。当時アンダーグラウンドサイトを制作するというブームがありました。私は普通のサイトさえ作ったことがなかったのですが、日本のジオシティーズ[注6)]にサイトを構築しました。これがセキュリティ・アカデメイアの前々サイトに相当します。アンダーグラウンドのスキルを学びながら、その技術を公開しつつ、アンダーグラウンドサイトを巡回することが日常となりました。

テレホーダイは深夜早朝の時間帯は 23 時から翌日 8 時までです。インターネットにはまり 8 時以降もつい継続してしまうことがありました。もちろん電話代がかさみ、1 ヶ月の電話代が 3 万円を超えかけたときは焦りました。

注4）　相手のメールアドレスに大量のメールを送りつけること。あるいはそのプログラム。

注5）　NTT が提供していた電話料金定額サービス。23 時から翌日 8 時まで指定した電話番号への電話料金が定額となった。

注6）　無料の Web サイト作成サービス。90 年代〜00 年代初頭に掛けて多数のサイトが開設された。2000 年に Yahoo! Japan がジオシティーズを買収。2019 年 3 月末にサービス終了。

第3章

Coinhive事件

Coinhiveは、ドイツのBadges2Goという会社が2017年9月から提供していたコンピュータプログラムです。JavaScriptで開発されており、Webサイトに貼り付けて、閲覧者のCPUを用いて仮想通貨Moneroのマイニング（採掘作業）をするものでした。総採掘量の3割を団体の収益とし、7割を登録者の報酬として分配するサービスです。

神奈川県警などの警察は、CoinhiveをWebサイトに設置することが不正指令電磁的記録の取得罪や保管罪にあたるとして、2018年～2019年の間に21人を検挙しました。この事件はCoinhive事件と呼ばれています。

3.1 仮想通貨のマイニングとは

ビットコインなどの仮想通貨では、ブロックチェーンと呼ばれる仮想の取引台帳システムを採用しています。ブロックチェーンは、P2P型ネットワークに参加したノードと呼ばれる分散コンピュータ群において共有・保管されており、取引が行われると伝言ゲームのように記録されていきます。

ブロックチェーンの改ざんを防ぐために存在するのがマイニングという手法です。取引を確認してブロックに記録するためには、ハッシュ計算をする必要があります。ブロックは「取引データ」や「ナンス値」[注1)]が保存されています。これをハッシュ関数でハッシュ値にしたものが利用されます。

ブロックの作成は複数ノードで同時に行われますが、最も長いチェーンのみが正しいと見なされます。悪意のある攻撃者がブロックチェーンを改ざんするためには、他のブロックチェーン参加者のハッシュ計算を上回り、かつ後続のハッシュ値も計算しなければなりません。これは事実上不可能であり、ブロックチェーンの信頼性が保たれることになります。そして、この計算を完了して適切なナンス値を見つけた者には仮想通貨が報酬として与えられます。

ビットコインなど大手の仮想通貨のマイニングで利益を上げるためには、高性能のCPUやGPUを搭載したマシンが幾台も必要になりますが、Moneroの場合はCoinhiveのようなWebサイト訪問者の僅かなCPUを使っても利益を稼げるという特徴があります。

注1）　一度だけ使われる、32ビットで形成された使い捨ての値。

3.2 元 Coinhive ユーザーさんインタビュー

Coinhive 事件で家宅捜索された人のうち、元 Coinhive ユーザーさん[注2)]から取材許可の返答がありました。元 Coinhive ユーザーさんは Coinhive 事件当時、未成年で受験勉強中でした。趣味で立ち上げたサイトに Coinhive を設置したところ、家宅捜索を受けることになりました。以下、元 Coinhive ユーザーさんのインタビューです。

色々な技術を試している中で Coinhive を導入した

齊藤 どのような事件で家宅捜索されたのでしょうか？

元 Coinhive ユーザー 私がサーバーを借りホスティングしていたサイト上で、不正指令電磁的記録である Coinhive を保管したという容疑です。正確に言うと、保管されていたのは Coinhive を呼び出すスクリプトで、Coinhive 本体のプログラムについては Coinhive 側のサーバに保管されています。

齊藤 Coinhive はどこで知ったのでしょうか？

元 Coinhive ユーザー GIGAZINE の「人気サイトがアクセス数の多さを利用し閲覧者の CPU パワーで仮想通貨マイニング、広告に代わる収入源になるか？[注3)]」という記事を読んで知りました。

齊藤 Coinhive はどのように動作するプログラムと思っていましたか？

元 Coinhive ユーザー 元々 CPU や GPU でのマイニングを試したりもしていましたので、人よりは細かい点まで認識していたかと思いますが、結局は JavaScript でハッシュ値の計算を行わせているという、一般的な認識であったと思います。

齊藤 Coinhive をどのようなサイトに貼り付けたのでしょうか？

元 Coinhive ユーザー 私が管理するゲーム関連のサイトです。私が作成・ホスティングする代わりに、仲間内から自由に色々試しても良いとなっていたため、そのドメインと VPS を使用して色々な試行錯誤をしていました。

齊藤 Coinhive を貼り付けた目的を教えて頂けますか？

元 Coinhive ユーザー 当時のそのサイトには、一応広告は置かれていましたが、PV 数は少なく、収益になるものではありませんでした。Monero は、CPU マイニングの効率が良い通貨ですから、数円・数十円程度になることは期待していましたが、最低出金額には満たないだろうと思っていました。先に書いたとおり、自分がホスティングしていたサイトが当時そのサイトのみで、色々な技術を試せる所でしたので、そのサイトを使用するのは自然なことでした。

齊藤 サイトのアクセスはどれくらいありましたか？

元 Coinhive ユーザー 元々ほとんどありませんでした。1 年で 5000PV といった程度であったかと思います。

注2） https://twitter.com/coinhiveuser
注3） https://gigazine.net/news/20170920-pirate-bay-mining/

齊藤 サイトには Coinhive を使っていることは記載していたでしょうか？

元 Coinhive ユーザー サイトで常用していた Google Analytics については、About ページに使用している旨の記述をしていましたので記載しても良かったのですが、試用であったので、記載しなくてもいいと放置していました。ブラウザ上の JavaScript の利用について記載しなかったからといって、犯罪にあたるとされ、半年後に警察がやって来るとは思ってもいませんでした。

齊藤 Coinhive でどれくらいの収入がありましたでしょうか？

元 Coinhive ユーザー ブラウザでどれくらい掘れるのだろうと、私のいくつかの端末で数日開きっぱなしにしてみたりもしていましたが、最終的な収益は 80 円相当で、最低出金額を満たしていなかったため実質的に収入はありません。

齊藤 サイト訪問者から Coinhive について何か連絡が来たことはありましたか？

元 Coinhive ユーザー 何もありませんでした。

警察による家宅捜索

齊藤 警察から家宅捜索を受けた時はどのような状況だったのでしょうか？

元 Coinhive ユーザー 2018 年 5 月の早朝、部屋で寝ていると両親が私を呼ぶ声がしたので起き上がって部屋の外へ出ました。私の部屋の前まで捜査員が数人入ってきました。突然のことで驚きましたが、令状を見せてほしいと話すと、「不正指令電磁的記録供用」と書かれた令状を見せられました。コンピュータ・ウイルス関連の話だとはすぐわかったものの、何の出来事で捜査を受けたのか、最初は全くわかりませんでした。

捜査員に「(Coinhive を設置したドメイン）○○の話ですか？」と聞くと、「そうだ。何か使わなかったか？」と聞かれました。以前読んだ日経オンラインの記事[注4)]を思い出し、まさかと思いながら「Coinhive？」と答えると「そうだ」と言っていました。それで Coinhive のことだとわかったのです。

齊藤 家宅捜索で警察からどのようなものを押収されたのでしょうか？

元 Coinhive ユーザー 家族共有のパソコンとスマートフォンが押収されました（図 3.1)。家族共有のパソコンについては、偶然にも、家宅捜索を受ける前の週に、故障品から新しいものへと組み直したばかりで、何もログが残っていないとわかったため、家宅捜索の終了時点でそのまま返却されました。これは本当に運が良かっただけで、もし前の PC のままであったら、データのコピーのため持ち帰られていたかと思います。スマートフォンについては、データをコピーした後返却すると説明され、その日の午後に返却されました。返却時にはいくつかのアプリが開かれたままであり、自分で使用した覚えのない、ドコモのバックアップアプリのログを確認したところ、バックアップしようとしたが失敗したというログが残っていました。

注4） https://www.nikkei.com/article/DGXMZO24462980Z01C17A2SHA000/
Coinhive が不正指令電磁的記録にあたるのではないかという弁護士のコメント付きの記事。この記事が出た時点で Coinhive は削除済みだった。

3.9 最高裁判所へ

東京高裁の有罪判決を受けて、モロさんは最高裁判所（以降、最高裁）へ上告しました。執筆時点では、最高裁は上告審の弁論を 2021 年 12 月に開くことを決定しました。最高裁は二審の判断を変更する場合に弁論を開くことが多いため、東京高裁の判決が見直される可能性があります[注13)]。

3.10 モロさんへのインタビュー

Coinhive 事件がどのようなものであったのか、当事者のモロさんにインタビューを行いました[注14)]。

Coinhive 設置の目的

齊藤 当時、どのようなネット活動をされていたのでしょうか？

モロ デザインやフロントエンド周りを業務でやらせてもらったり、趣味の Web サイトをいくつか運営したりしていました。

齊藤 ご自身が家宅捜索された事件について、どのような事件で家宅捜索されたのでしょうか？

モロ 「Coinhive」というマイニングツールを自サイトに設置したことで家宅捜索を受けました。

齊藤 Coinhive はどのような動作をするプログラムと思っていましたか？

モロ ブラウザを介して閲覧者の CPU リソースを使い、仮想通貨 Monero をマイニングする JavaScript 製のスクリプトと理解しています。

齊藤 Coinhive をどのようなサイトに貼り付けたのでしょうか？

モロ 当時、趣味で運営していた音楽情報系の Web サイトに設置していました。

齊藤 Coinhive を貼り付けた目的を教えて頂けますか？

モロ 運営費用が広告頼りだったため、Coinhive を利用することで広告をなくし、より見やすく使いやすいサイトにしたいと考えていました。

Coinhive からの収入は 0 円だった

齊藤 サイトには Coinhive を使っていることは記載していたでしょうか？

モロ していませんでした。

齊藤 Coinhive でどれくらいの収入がありましたでしょうか？

注13） コインハイブ事件、最高裁で 12 月弁論　逆転有罪の二審判断見直しか https://www.bengo4.com/c_1009/n_13674/
注14） このインタビューは、本書の解説とは無関係です。

モロ 当時の円のレートで 800 円程度の Monero を得ましたが、Coinhive の仕様で 5,000 円程度から出金可能となるため実質的な収入は 0 円でした。

齊藤 サイト訪問者から Coinhive について何か連絡が来たことはありましたか？

モロ 一度だけ同業者と思しき方から「改ざんされて Coinhive を埋め込まれていないか？」と Twitter で連絡をいただいたことがありました。

家宅捜索を受けた時の状況

齊藤 家宅捜索されたときの状況を詳しく教えて頂けますか？

モロ 仕事で出社しているときに警察から「とある事件の捜査に協力してほしい」と電話があり、自宅にいないことを伝えると職場まで迎えに来て、自宅前で令状を見せられ家宅捜索を受けました。

自宅にあった PC やスマートフォンを操作されながら淡々と聞かれたことに応えていたのですが、内容がやや抽象的だったため、運営しているサイトや使用しているツールについて話す中で、ようやく Coinhive についての捜査だと気付きました。

齊藤 ご家族や友人から心配されたり誤解されたりはしませんでしたか？

モロ 当時入籍したばかりで、妻や両親には大いに心配をかけてしまったと思います。内容が専門的なためわからないことも多い中、それでも私を信じて支えてくれました。実名報道等はなかったため、限られた親しい人にだけ伝えられたのは幸いでした。

警察や検察の取り調べ

齊藤 警察や検察の捜査や対応についてどのような印象を抱きましたか？

モロ 警察には技術的な部分に明るくない方も多かったようで、何度も同じ説明をさせられたり、的はずれな回答が多かったり、一体何の関係があるのだろうと思うような幼少期の話をさせられたり、そんな話をするために仕事をすっぽかしている事実が頭をよぎったりして、精神的に大いに参りました。検察での取り調べについては、本当に二、三言しかやりとりしていないため、ほとんど印象にありません。

齊藤 家宅捜索では警察にどのようなものを押収されましたか？

モロ デスクトップ PC、ノート PC、スマートフォン各 1 台とプロバイダとの契約書類が押収されました。

齊藤 押収されたことによって困ったことはありませんでしたか？

モロ 基本的にすべて業務でもプライベートでも使用していたものなのですべての仕事は一時的に滞り、謝罪の連絡手段にも苦労しました。

齊藤 家宅捜索の捜査官、取り調べの捜査官、取り調べの見張り役の印象・態度はどうでしたか？

モロ 全体的な印象として、技術的な話に極めて疎い以外は特に高圧的ということもなく、淡々とした印象でした。

ただ、調書に私の「反省しています」という言質を取りたかったようなのですが、一方で私は「技術的な話に疎いだけで説明したらわかってもらえる」と的はずれな楽観を持っていたためいつまでも話が噛み合いませんでした。最終的にはガタイのいい高圧的な捜査官の方が出てきて、強引

第 4 章

Coinhive 事件における弁護活動（平野敬弁護士）

Coinhive 事件の裁判とはどのようなものであったのか、平野敬弁護士[注1)]に寄稿してもらいました。ここでの「筆者」とは平野敬弁護士自身をさすものです。[注2)]。

●図 4.1　平野敬弁護士の SNS アイコン

4.1 はじめに

本稿の位置づけ

本稿は Coinhive 事件において筆者が行った刑事弁護活動につき、その体験をまとめたものである。想定読者として 2 つの方向を意識している。

法律実務家に向けて

第 1 に、筆者同様に IT 関係の複雑な事件について刑事弁護を受任することとなった弁護人[注3)]に対し、指針と手がかり、あるいは批判的教訓を提供することにある。

刑事弁護と IT は食い合わせが悪い。今日、得意分野として IT 関係を掲げる弁護士はありふれているし、司法試験を受ける前には IT 関係の会社に勤めていたという人も少なくない。他方、刑事弁護の世界で研鑽と名声を積み上げている弁護士も数多い。しかし、この積集合、すなわち IT と刑事の両方について実績のある弁護士となると極端に数が少なくなる。大多数の IT 系弁護士は企業法務を中心とする民事事件を志向しており、刑事については経験が乏しい。研修で義務付けら

注1）　https://twitter.com/stdaux
注2）　この寄稿は本書の解説とは無関係です。
注3）　「弁護士」は資格の名称。「弁護人」は刑事事件において弁護活動を行う役割の呼称。弁護人を務めることができるのは、原則として弁護士のみである（刑訴法 31 条 1 項）。

れた最低限の国選を受けた経験があるだけという人も含まれる。

さらに、そもそも IT 絡みの刑事事件という存在自体がマイナーである。筆者の知る限り、司法試験で不正指令電磁的記録供用罪や電磁的記録不正作出罪が出題されたことはないし、刑法各論の教科書を紐解いても記載は数行程度しかない。ごく普通に司法試験を受けて、ごく普通に弁護士になった場合、これらの罪名を意識する機会すら乏しいと思われる。

かくいう筆者も、弁護士として一応 IT を主軸業務としてはいたものの、Coinhive 事件以前の実績としては、もっぱら企業法務を含む民事事件に集中していた。刑事については経験が薄く、IT 絡みの刑事弁護というのは初めてであった。

Coinhive 事件の受任当時は独立間もない時期であった。経験も資源も乏しい中ではあったが、試行錯誤を繰り返して弁護活動を行い、周囲の支援や幸運にも恵まれ一定の成果を出すことができた。その思考や行動の軌跡を記し、後世の一助としたい。

IT エンジニアに向けて

第 2 に、IT 関係の刑事事件について被疑者・被告人となった者、あるいは将来的にその可能性がある者に対し、未知の世界であろう刑事手続の知識を提供することにある。すべての IT エンジニアは潜在的に被疑者・被告人となり得るのであるから、IT エンジニア一般が想定読者ということになる。

刑事弁護の観点からすると、IT 関係の事件における被疑者・被告人というのはかなり特殊な類型である。大学卒や大学院卒といった高学歴者が多く、記憶力や抽象的思考力が高い。有名企業に勤務して相当の収入を得ている者も少なくない。前科前歴がなく、少年時代も含めて警察のご厄介になったことがない。つまり、いわゆる「いい子」であって、秩序を重んじ、穏和で従順である。

こうした特性は一般に美徳とされるものであるが、反面、被疑者・被告人としては弱点ともなり得る。大声で威圧されること、狭い留置場や取調室に長時間閉じ込められること、敵対的な尋問を受けること。彼ら彼女らには、こうした局面への耐性がほとんどない。

エンジニアとしての良心が枷になることもある。たとえば、「ブラジルの蝶の羽ばたきがテキサスで竜巻を起こす可能性が絶対にないと言えるか」と質問された場合、エンジニアとして誠実な応答は「絶対にないとは言えない」だろう。理論的にはそれで良い。しかし取り調べでそう答えた場合、あなたの調書にはこう書かれることになる。「私は、この羽ばたきが竜巻を引き起こす危険なものかもしれないとあらかじめ認識していました」。誠実な議論に慣れているがゆえの陥穽である。また、自己の無知を率直に認め、他人の専門性を重んじるエートス[注4)]を叩き込まれているために、捜査官[注5)]が説明した法的手続やその根拠を特に疑うこともない。

後述するように、刑事事件においては後から劣勢を覆すというのが非常に難しい。あなたが被疑者として取り調べを受けることになった場合、むろん遅からず弁護人を選任して身を守ろうとするだろう。しかし弁護人が動き出すまでに、すでに取られてしまった調書により、すべての選択肢が失われていたということもあり得る。本稿の記載が、IT エンジニア各位において「もし自分が罪に問われたらどうするか」という将来の備えになれば幸いである。

注4)　人間の行為の持続的な反復によって得られる習性。
注5)　取り調べにあたる警察官や検察官の総称。

記載に関するスタンス

事実記載と匿名性

筆者は Coinhive 事件に関し 6 人の依頼者から弁護人として選任された。うち 1 人が「モロ」さんであり、最初の依頼者である。モロさんについてはマスメディア等で大きく報道され、本人も積極的な発言を行っていることから、本稿では特にフェイク表記などは行わない。

他方、他の 5 人については不起訴に終わっている。個々人の特定を防ぐため、あえて各自の事件を分けて書かず、一体として記載することとする。

法律上の概念や用語について

正規の教科書ではないので、個々の法的概念について都度詳細に定義を詳説することはしない。もっとも、IT エンジニアを想定読者とする以上、初学者への配慮も必要である。最低限、誤解や混同を招きかねない点については本文または脚注で補うこととする。

4.2 Coinhive との邂逅（相談〜弁護方針決定）

モロさんからの連絡

2018 年 3 月 29 日、筆者はモロさんから「ウイルス罪について相談したい」という趣旨の電子メールを受信した。メール内には、友人から Web に詳しい弁護士として筆者の紹介を受けたこと、同年 2 月からモロさんが警察の取り調べを受けたこと、被疑事実[注6)]は Web サイトに仮想通貨のマイニングを行う JavaScript を設置したというものであること、罪名は不正指令電磁的記録保管罪[注7)]であること、3 月に略式手続で罰金 10 万円の刑を言い渡されたこと、略式命令[注8)]に対する異議申し立ての期間は 4 月 12 日までであることが記載されていた。

公判弁護の難しさ

この時点での筆者の内心としては、弁護人を引き受けることについてかなり消極的であった。事件の見立てをさておくとしても、この相談の時点で弁護人としてできることがあまりにも限られていた。

刑事弁護人の仕事は 3 段階に分けて考えられる。

注6） 犯罪にあたるとされ捜査対象となっている事実。

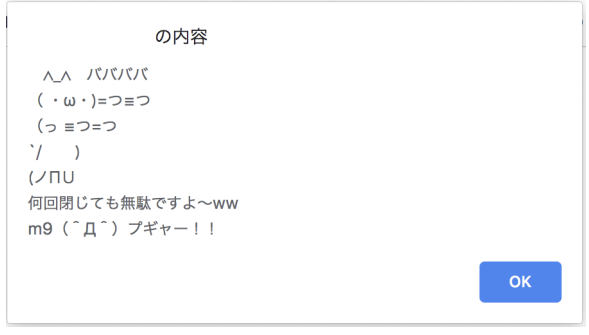
注7） 刑法 168 条の 3。不正指令電磁的記録に関する罪は大きく分けて、作成・提供罪（168 条の 2 第 1 項）、供用罪（同第 2 項）、取得・保管罪（168 条の 3）となっている。実務上、ウイルスの被害者がいる場合には供用罪、いない場合には保管罪として検挙されることが多いようである。

注8） 刑事裁判は公開の法廷で行わなければならない（憲法 32 条、82 条 1 項）。この原則に対する例外として刑事訴訟法に設けられているのが略式手続である（刑訴法 461 条）。被疑者が同意している場合に、正式な手続を踏まずに書面審理だけで罰金刑を科す（略式命令）。被疑者は略式命令を受けてから 14 日以内に正式裁判を請求することができ、請求がない場合には確定判決と同じ扱いになる（470 条）。裁判所や検察官にとっては事務工数の削減になり、罪を全面的に自白している被疑者にとっては長期間の裁判に拘束されないという利益がある。しかし、取り調べに納得はしていないが一刻も早く刑事手続から逃れたいという一心で、よくわからないまま略式手続に同意してしまう被疑者もおり、問題の多い制度である。

第5章

アラートループ事件

2019年3月、女子中学生と成人男性2人（あひるさん[注1)]、啓発者さん[注2)]）がネット掲示板に不正なプログラムを書き込んだとして、兵庫県警は3人に対して家宅捜索を行いました。しかし、不正なプログラムと見なされたのはJavaScriptのfor文によるループ処理と、ポップアップ処理であるalert()を使ったジョークプログラムの一種であり、この処理はブラウザのタブを閉じれば簡単に終了できるものでした。この事件は「アラートループ事件」と呼ばれています。



●リスト 5.1　不正プログラムとして摘発されたコード

```
for ( ; ; ) {
window.alert("　ﾍ_ﾍ　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！！")
}
```

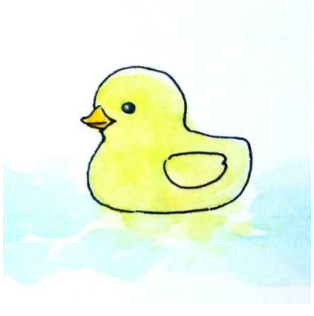
アラートループ事件が起きると、このようなスクリプトで家宅捜索を受けたという事実に、インターネット上でITエンジニアを中心に多くの人が問題視しました[注3)]。日本ハッカー協会[注4)]が成人男性2人の裁判費用の寄付を呼びかけたところ約700万円もの寄付金が集まりました[注5)]。海外でも日本の警察がJavaScriptのポップアップで13歳の少女を家宅捜索したニュースは衝撃を持って伝えられました[注6)]。JavaScriptの生みの親であるブレンダン・アイク氏は「日本に行って無罪だと証言できる」と苦言を呈していました（図5.1）。

注1）　https://twitter.com/pYDPLjyqv2j1r3T
注2）　https://twitter.com/keihatusyaA
注3）　その一方で、ヤフーニュースのコメント欄では一般の人々が警察の対応を支持するコメントで溢れていました。
注4）　一般社団法人日本ハッカー協会。ハッカーの地位向上を目指して活動している団体。
注5）　https://www.hacker.or.jp/alertloop/
注6）　https://www.zdnet.com/article/japanese-police-charge-13-year-old-for-sharing-unclosable-popup-prank-online/

●図 5.1　ブレンダン・アイク氏のツイート

アラートループ事件がどのようなものであったのか、当事者のあひるさんと啓発者さんにインタビューしました。これからアラートループ事件の真相を明らかにしていきます。

5.1 あひるさんへのインタビュー



●図 5.2　あひるさんの Twitter アイコン

警察による家宅捜索

齊藤　ご自身がどのような事件で逮捕されたかお話いただけますか？

あひる 朝 6 時半、鹿児島県の自宅に兵庫県警の私服の人達が 4〜5 人来て、家の前で私の名前を呼んでいました。早朝でしたので、自分の名前を呼ぶ来訪者が来るとは想定しておらず、最初は何が起きているのかわからず呆然としていました。玄関を開けたところで私服警察だと分かり、警察から不正指令電磁的記録供用罪に関する家宅捜索の令状と車両差し押さえ令状を見せられ、「なぜ来たかわかるか？」と言われました。

私は最初「あれ、何か悪いことをしたかな？」と思いながらも、やはり何が起きたのかわかりませんでした。警察は兵庫県警と名乗っていました。もし何か事件を起こしたならば、私が住んでいる場所ですと鹿児島県警が管轄だと思っていたので、最初は全然意味がわかりませんでした。そして家の中に警察が入ってきて、「携帯電話を出しなさい」と言われました。その時、司法巡査に私

の調書を取られました。

その場で司法巡査・刑事たちと 1 時間半〜2 時間くらい話をしました。私の調書を取っている人とはある程度しっかり対話できましたが、他の知らない人が私の家の中で秘かに話をしていたり、家の中を物色したり、「パソコンなどを持っていたら押収するから出しなさい」と言ってきたりして戸惑いました。

ちょうど仕事に行く時間になったため、「会社に今日は休むという連絡をさせてください」と警察に伝えたところ、「それはダメだ」と却下され、もう完全に犯罪者扱いでした。そこで、せめてスマホだけでも返してもらうようにお願いをして、何とか会社に電話できました。

会社に「今日はちょっと休ませてください」と話したら、会社から「なぜ休むの？」と返されたので、「今、兵庫県警の刑事さんが来ていて家宅捜索を受けてます」と素直に言いました。会社は自宅から 10 分もかからない場所にあり、社長が家までやってきました。心配の延長だったと思います。そして私と刑事たちで色々話をした後、私は調書を取られるために地元の鹿児島県警の警察署に出頭することになりました。手錠はされませんでしたが、やはり人の目も気になります。そんな思いから、「自分の車で出頭したいです」と話したら何とか許可が出ました。警察車両はパトカーではなく普通車 2 台だったと思います。1 台は私の車の前を走り、もう 1 台は私の車の後ろを走っていました。警察車両に挟まれるような感じです。

警察による取り調べで短縮 URL が問題視された

齊藤　警察による取り調べはどのようなものでしたか？

あひる　警察署に着いてから取調室に入りました。最初の 1 時間くらいは私が遊んでいた掲示板の話はされず、「あなたのやった行為は犯罪だ」と決めつけるように言われ続けました。話をしていくうちに、私が掲示板に張ったリンクを警察が問題視していることがわかりました。しかし、それはジョークスクリプトを呼び出す URL に過ぎません。

私の中ではジョークスクリプトへのリンクが犯罪になる理由がわからず、「ジョークスクリプトのリンクのどこが犯罪行為で、なぜ私はこういう状況に置かれているのでしょうか？」と警察官に質問しました。ジョークスクリプトに対する私の認識と、警察が主張するジョークスクリプトの犯罪性がどうしてもかみ合っていないのです。

私がよく遊びに行く掲示板があります。ある日、そこで頻繁に悪ふざけの投稿をしている方が、地震に関するジョークスレッドを立ち上げました。それに気付いた私は、そのスレッド内で「大変だ、甚大な被害だ」という文章と一緒に URL を書き込みました。その URL をクリックするとジョークスクリプトが置かれたサイトに移動します。URL は他人の書き込みからコピーしたものですが、スマホあるいは掲示板によって自動的に短縮 URL に変換されて書き込まれました。長い URL をコピーしたはずなのに、掲示板に貼り付けた時点で意図しない短縮 URL になっていたのです。警察によると、URL を短縮して隠蔽する行為や、ジョークスクリプトに誘導する行為が犯罪であると言っていました。「載せた URL も悪質なプログラミングだ」「現行法でいうところのフィッシング詐欺などと同じレベルの悪質なものだ」といった主張もしていました。

警察からそのように迫られた私は、「現行法でジョーク関係のプログラムは犯罪になる」という誤った知識を植え付けられてしまいました。その間違った解釈のまま、調書も書かれてしまいました。犯罪者という扱いで顔の三面写真を撮られ、手の指紋をすべて取られました。会社の社長には保護者という形で警察署に来てもらい、その日の取り調べは終わりました。

第 6 章

事件の考察と今後の展望

ここまで Wizard Bible 事件・Coinhive 事件・アラートループ事件の各事件について、当事者の証言を中心に振り返ってきました。

3 つの事件は、いずれも第 1 章の法務省のガイドラインの説明からは大きく乖離した事件です。なぜこのような事件が立て続けに起きたのでしょうか。また、このような事件を引き起こさないようにする解決策はないのでしょうか。本章では、一連の事件への考察と解決策を考えていきます。

6.1 一連の事件の問題点

今回の一連の事件における問題点を確認してみます。

警察の技術や法律への理解不足

一連の事件を通じて明らかになったのは、警察の技術や法律への理解不足です。3 つの事件において当事者たちは、警察は技術的な説明を理解していなかったと証言しています。

そして法務省のガイドラインにあるように、不正指令電磁的記録に関する罪は、国民の表現の自由を侵害するものではなく、コンピュータ・ウイルスの自由な研究を阻害するものでもないと説明されています。それが警察や検察によって拡大解釈され、本来は表現の自由やコンピュータ・ウイルスの研究に該当する分野にまで捜査が行われたのが実情です。

さらに警察や検察は決めつけにより、自分達に都合のよい調書を作ろうとしていました。Coinhive 事件やアラートループ事件では自白の強要も行われました。自白に頼る日本の捜査の問題点が如実に出ていたと言えるでしょう。

見せしめと検挙数という指標

アラートループ摘発事件において、兵庫県警のサイバー対策課は Net IB News の取材に対して「安易に行っている者への警鐘とインターネットモラルの向上を意図していた」と見せしめの摘発であったことを認めています[注1)]（図 6.1）。

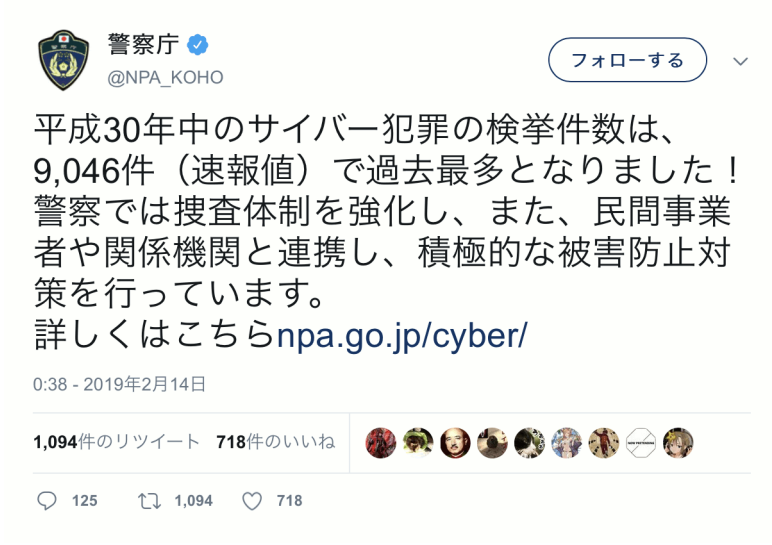
注1）　https://www.data-max.co.jp/article/28329

兵庫県警サイバー犯罪対策課は取材に対し、不正指令電磁的記録供用事件に対して集中取り締まりを行い、3件を家宅捜索。そのなかの1件で実際にアドレスを貼ったのが若年者だと発覚したものと回答。

「いたずらだったことは重々承知しているが、現行法では懲役、もしくは罰金刑になる犯罪」と指摘。個人を攻撃する意図があったものではないとして、今回の取り締まりについて、「安易に行っている者への警鐘とインターネットモラルの向上を意図していた」と述べた。
同課は「みんなで〜プロジェクト」について、「自分の子どもにもそんなことが言えるのか」と述べ、否定的な考えを示した。

●図 6.1 「みんなで逮捕されようプロジェクト」がネット上で拡散中〜サイバー犯罪対策課は「自分の子どもにもそんなことが言えるのか」と反発（Net IB News）

そして警察においては検挙数が指標として使われています。第 1 章でも確認したように警察白書などでも検挙数が重要な指標として登場します。また、警察関連の Twitter アカウントでも検挙数を誇るように宣伝しています[注2)]（図 6.2）。



●図 6.2 警察庁の公式 Twitter アカウントのツイート

また、警察庁が全国の県警へ宛てた「不正指令電磁的記録に関する罪の取締りの推進及び取締りに当たっての留意事項について」[注3)]という行政文書では、「被害が拡散しやすい不正指令電磁的記録」「挙動があまり認知されていない不正指令電磁的記録等」を「重点的に検挙するなど、犯罪抑止効果も企図した積極的な取締りを推進すること」として、積極的な検挙を推進している箇所があります。

注2） https://twitter.com/NPA_KOHO/status/1095965518870134784
注3） https://it-giron.com/401

■ 不正指令電磁的記録に関する罪の取締りの推進及び取締りに当たっての留意事項について

サイバー犯罪捜査担当課においては、サイバーパトロールや警察安全相談の精査を徹底するなど、本罪に係る積極的な端緒情報の収集に努めること。また、事件化に当たっては、捜査員が有する経験、特別捜査官や情報技術解析部門の職員が有する高度な情報技術に係る知識·技能を活かし、被害が拡散しやすい不正指令電磁的記録、挙動があまり認知されていない不正指令電磁的記録等を重点的に検挙するなど、犯罪抑止効果も企図した積極的な取締りを推進すること。

この文書が出されたのは 2019 年 2 月 15 日であり、アラートループ事件が起きる前月になります。直接的な原因となったかは不明ですが、このような積極的な検挙を呼びかける文書が警察内部で交わされている中で一連の事件が起きたと考えられます。

警察が検挙数を指標にしているのだとしたら、最も簡単に検挙数を上げる方法は、捜査が難しい高度な犯罪の摘発に取り組むのではなく、単純で軽度な行為を取り締まることです。交通違反でも、警察は敢えて運転者が間違いをおかしやすい交差点などに張り込んで点数を稼いでいます。それと同じことがサイバーセキュリティの世界でも起きていると推察できます。

組織対個人の非対称性

一連の事件でもう一つ明らかになったのは、警察という組織と個人との非対称性です。家宅捜索や起訴された時に正式裁判で受けて立てる人達は決して多くはありません。IPUSIRON さんは母親の葬儀や地縁などの事情により、正式裁判を断念せざるを得ませんでした。

Coinhive 事件でもモロさんは正式裁判の手続きをしましたが、略式起訴を受け容れた人達もいます。アラートループ摘発事件で家宅捜索されたあひるさんと啓発者さんは、正式裁判で受けて立つ弁護士費用を日本ハッカー協会の寄付の呼びかけでようやく調達できました。

このように、警察や検察といった組織に対して生身の個人は脆弱です。正式裁判は時間が掛かります。家族や職場での理解が必要ですし、弁護士費用など金銭的な支出も大きいです。この脆弱さや非対称性を利用して、軽微な犯罪や素人を狙って検挙数を上げようとしているのだとしたら大問題だと言えるでしょう。

前科や前歴となる

不正指令電磁的記録問題で起訴もしくは略式起訴されたりした人達は、刑が確定した場合に前科として記録が残ります。また、刑が確定しなくても警察から捜査を受けて被疑者として扱われた場合は前歴が残ります。前歴は消せません。今後の人生に半永久的に影響を及ぼすことが、警察や検察の恣意的な見せしめや啓蒙活動で左右されてはならないのです。

IPUSIRON さんの母親は家宅捜索後、決着を知らないまま亡くなりました。また、Coinhive 事件のモロさんは、結婚直前に家宅捜索されました。あひるさんはストレスで体を壊しました。人生への影響は甚大だったと言えます。

高木さんの記事で明らかになった事

今回のインタビュー前後に起きた出来事として、高木浩光さんが「しそうけいさつ化する田舎サ

第 7 章

セキュリティの未来のために

前章までは、Wizard Bible 事件、Coinhive 事件、アラートループ事件の概要とその関連性について解説しました。事件の当事者たちのインタビューによると、誰もが事件に巻き込まれることを全く想定していかったことがわかります。つまり、自分は絶対に大丈夫だと思ってはいけないのです。セキュリティエンジニアやセキュリティ初学者はもちろんのこと、一般の IT エンジニアやインターネットユーザーでさえ、事件に巻き込まれる可能性を否定できないからです。

本章ではこれまでの集大成として、自衛するための具体的かつ技術的な方法について解説します。本章の特筆すべき点は「事件に巻き込まれないための自衛策」に終始せず、「万が一巻き込まれてしまった場合の対応策」まで解説していることです。Wizard Bible 事件の当事者が、事件を通して得られた教訓、および事件後に考察した内容についてまとめました。

7.1 本章の読み方

読者の状況や立場によって、本章を読む観点が異なります。最初に読む際には、ここで示す分類を参考にしてください。再読する際には分類にこだわらず、必要な箇所を熟読してください。

1. インターネットユーザー…本章をざっくりと読む。取り調べ・留置場・拘置所・刑務所についての概要を把握する。自身が事件に巻き込まれたり、裁判で証言を求められたりした際に役立つ。
2. IT エンジニア…過去の事例から考えると、セキュリティ関係者以外もサイバー事件に巻き込まれる可能性がある。自分では「不正指令電磁的記録の罪」に該当しないと思っていても、突然に家宅捜索されることが起こりえる。それらを踏まえ、本章において家宅捜索や取り調べの解説を読み、知識武装しておくことが望ましい。
3. 身近（家族・友人・同僚）に IT エンジニアがいる…身近な IT エンジニアが将来、サイバー事件に巻き込まれる可能性がゼロとは言えない。本書を紹介したり貸してあげたりしてほしい。
4. セキュリティ初学者…本章ではセキュリティ書籍が推奨する環境、および専門家が実際に活用している環境を紹介している。セキュリティに関して実験する際には、それらを参考にすることを心掛ける。前章までを熟読して、Wizard Bible 事件、Coinhive 事件、アラートループ事件の 3 つの事件の顛末を念頭に入れておく。そして、自分がサイバー事件の当事者になった場合を想像して、これらの事件の顛末を参考にして、どういった行動をとるべきかをシミュレーションしておくことが望ましい。知識を得るだけでなく、実際に行動することが

重要である。結果として家宅捜索や逮捕されないように予防できる。

5. セキュリティ専門家…日頃から同業のセキュリティ専門家たちと情報交換しておく。もし事件に巻き込まれたら、周囲に情報を展開して協力を仰ぐ。会社がどういった対応をしてくれるのかも事前に確認しておく。
6. 家宅捜索されてしまった人…Wizard Bible 事件は一人で抱え込むという大失敗を犯した。それでも運よくいくつかの問題を乗り越えられたが、他の人が同じようにうまくいくとは限らない。家宅捜索後は次の 2 ケースに分けられる。
   a) 在宅事件のため拘束されていない…自分で相談相手や弁護士を探せる状況にある。Coinhive 事件やアラートループ事件の顛末を参考にして、専門家や弁護士に相談する。
   b) 身体拘束された…すぐ弁護士に連絡を取ること。取り調べに対してどう臨むのかについては弁護士と相談する。
7. 身近にサイバー事件に巻き込まれた方がいる人…今すぐ本書を読み、その人に協力してあげる。巻き込まれてしまった当事者にとって、協力者が 1 人でもいることはとても心強いことである。状況の把握、ならびに困ったことがないかを確認するために、面会もする。冤罪で逮捕されたのかどうかを専門家に確認する。そして、差し入れや手紙も積極的に行ってほしい。
8. ペットがいる人…身柄を拘束されてしまうと自宅に帰れない。協力者が同居していれば、事前にペットの世話の仕方（餌や薬など）についての情報を共有しておく。逆に協力者が同居していなければ、ペットの生死にかかわる問題となる。それを避けるためにも、事前に協力者の候補を選んでおこう。協力者は自分やセキュリティに対して理解のある人物を選ばなければならない。ペットや身の回りの世話（差し入れや連絡）をお願いする時に必ず事件の詳細を話すことになるからである。

7.2 事件に巻き込まれないための自衛策

「メールでウイルスが届いた」「ダウンロードしたファイルにウイルスが付いていた」などの場合は、故意にウイルスを得たわけではありません。よって、PC から削除してしまえば不正指令電磁的記録の罪の観点からは問題ありません。注意すべき状況は、次に示すようなセキュリティの研究・調査の過程で危険なプログラムを扱うという場面です[注1)]。

- マルウェアの解析
- ハニーポットの運用
- ペネトレーションテスト
- 脆弱性診断
- 攻撃手法の学習

マルウェアの解析では「備えている機能を明らかにする」「対策技術を検討する」「作成者やその

注1) セキュリティの技術を進歩させるには最先端の攻撃技術を学ぶことが必要不可欠である。攻撃の高度化に伴い、マルウェア解析の必要性は増している。

目的を明らかにする」「攻撃対象を明らかにする」「セキュリティソフトを強化するための情報を得る」などを目的としてマルウェアを調査します。解析手法は表層解析、動的解析、静的解析に大別されます。表層解析はマルウェアのメタデータを分析することです。動的解析はマルウェアを実際に動作させて挙動を調べることです。実行端末の動作、ネットワークへの通信などを明らかにできます。静的解析は逆アセンブラ[注2)]やデバッガー[注3)]を用いてコードレベルで調査することです。動的解析では再現しない潜在的な機能を見つけたり、特徴的なバイト列を収集したりできます。

ハニーポットとは、脆弱に見せかけたシステムに攻撃者を誘い込んで、攻撃手法を解析する技術とシステムの総称です。ハニーポットを用いて攻撃を収集する行為は直接的に違法ではありませんが、攻撃者の行動次第では危険なプログラム[注4)]を配置される危険性があります。また、マルウェアを収集するためにハニーポットを用いることもあります。

ペネトレーションテストとは、攻撃者の観点で攻撃を行い、侵入などの目的を達成できるかを調べる手法のことです。侵入実験または侵入テストとも呼ばれます。ペネトレーションテストの過程で危険なプログラムを扱うこともありますし、ペネトレーションテスト用の OS に危険なプログラムが含まれていることもあります（使用の有無にかかわらない）。

脆弱性診断とは、システムの脆弱性やセキュリティの不備を検査することです。検査は定型的な手法で網羅的に行われ、ペネトレーションテストよりも広範囲をカバーしますが、ペネトレーションテストのような侵入を目的とした攻撃までは行いません。

攻撃手法を研究したり学習したりする状況を考えてみます。すべてのセキュリティ専門家は、最初から会社や学校といった後ろ盾があったわけではありません。セキュリティ専門家は、業務以外でも調査・実験を行います。公私、いずれの状況であっても実際に手を動かして独学することは重要であり、その過程で危険なプログラムを扱わざるを得ません。

セキュリティ書籍を参考にした自衛策

セキュリティ関連の書籍は和書・洋書を問わずたくさん存在しており、実際に手を動かして学ぶタイプの本も多々あります。不正指令電磁的記録の罪は 2011 年に施行されたため、これ以降に発行された日本の書籍であれば、著者や出版社が何らかの配慮をしていることが期待できます。手元にセキュリティ本が数十冊あるので、そこからマルウェアの解析やサーバーの侵入に特化した本を選び出して、どのような扱いになっているのかを調べました。その結果は次の通りです。なお、調査対象の出版社は本書の出版社と異なるため、具体的な書名を伏せておきます。

- ハッキング関係の洋書は一般的に過激な内容のものが多い。しかし、日本語に翻訳される過程で不正アクセス禁止法や不正指令電磁的記録の罪についての配慮が見て取れる。
- 「本書の内容を不正に利用しないこと」「許可を得ずに自分以外の個人や組織、インフラ等に対して攻撃実験しないこと」「他者や所属組織が所有する機器を利用しないこと」「攻撃の実践は仮想環境か閉域環境で実施すること」「高い倫理観を持つこと」といった免責が記載されて

注2）　0 と 1 で表現される機械語で書かれたプログラム記述（オブジェクトコード）を、より人間が理解しやすいアセンブリ言語による表記（ソースコード）に変換するソフトウェアのこと。

注3）　プログラムの不具合やバグの発見を支援するソフトウェアのこと。プログラムの実行を任意の位置で中断したり再開したりできる。また、中断した状態におけるメモリーや変数の状態を調べられる。

注4）　バックドア（不正に侵入するための裏口）、Exploit（脆弱性を突いて有害な動作を行うプログラム）、マルウェア、C&C サーバー（マルウェアに感染した端末を制御するサーバー）など。