論　説

コインハイブ事件と不正指令電磁的記録に関する罪

上　野　幸　彦

Ⅰ　序　論

最高裁判所は、2022年１月20日、いわゆるコインハイブ事件において不正指令電磁的記録保管罪（刑法第168条の３）で起訴された被告人に対し、無罪を言い渡した(1)。この事件は、事実関係について争いはなく、争点はもっぱら被告人が保管していたとされるプログラムが「不正指令電磁的記録」（同第168条の２第１項第１号参照）に該当するか否かという解釈上の判断についてである。既に同種の事案で略式命令請求により罰金刑が確定している例も見られた(2)ようであり、最高裁が無罪とする解釈判断を示したことは、極めて注目に値する。本稿では、裁判の経過をやや詳しく辿りながら、最高裁の判断について分析を行い（Ⅱ）、この事件が示唆している不正指令電磁的記録の罪の規定の在り方に関する問題について、立法の経緯を振り返りながら明らかにするとともに（Ⅲ）、あらためて本罪の解釈適用について若干の考察を試みることにしたい（Ⅳ）。

日本法学　第八十八巻第三号（二〇二三年一月）

Ⅱ　コインハイブ事件の概要と裁判の経過

1．コインハイブ事件とは

ビットコインに代表される暗号資産(3)は、一般にブロックチェーンと呼ばれる仕組みを利用して取引が記録される。この記録の改竄を防ぐために、マイニングという作業が行われる。そして、マイニングと引き換えに暗号資産を与えることにより、取引データの完全性を維持しているのである。ビットコインの場合には、マイニングにおけるハッシュ計算量が膨大で、個人のパソコンでは到底及ばない。しかし、Coinhive Team は、暗号資産の一種である Monero に関して、個人のパソコンでも十分にマイニングできる専用スクリプトを開発し、これによりウェブサイトにアクセスする利用者のコンピュータで計算を行い、コインハイブに登録したウェブサイト運営者が収入を得られるコインハイブ（Coinhive）(4)というウェブサービスを提供した。このコインハイブのプログラムは、JavaScript を利用しており、ソースコードも公開されている。ウェブサイトに設置して用い、同サイトを閲覧する利用者のブラウザー上で動作する。その動作内容は、Monero を獲得できるための演算、すなわちマイニングを行うものである(5)。

今回の事件は、サイト運営者が、コインハイブに登録し、登録キーを利用して自己のサイトにアクセスした利用者をこのコインハイブのマイニングスクリプトをライブラリとして呼び出すプログラムコードを作成し、自己のウェブサイトの HTML に記載しそのサイト上に設置し、コインハイブ社から収入を得ようと企図したものである。この事件のサイト運営者は、ウェブデザイナーであり、楽曲に関するウェブサイトを運営していた。サイトの維持管理費用は広告収入に拠っていたが、コインハイブに関する記事を読み、収入源として試験的に利用することとし、登録者に発行されるサイトキーを取得して、これを記述したコードを2017年 9 月21日に自己の運営するサイトに設置した。これによって、サイトを閲覧した利用者のコンピュータで自動的にマ

イニングが実行され、総採掘量の7割が登録者であるサイト運営者の報酬として分配された。この事件では、同年11月9日にプログラムコードが削除されたが、この間800円程度の総収益を得たとされている。

コインハイブは、登録したサイト運営者のサイトにアクセスした利用者のパソコンでマイニングの演算処理が行われる仕組みとなっており、サイトを閲覧している利用者が知らない間に、勝手にそのパソコン内のCPUが利用されているという状態となる。サイト閲覧者のパソコンのいわば無断利用を伴う事態を問題視した警察当局は、サイト閲覧者に無断でコインハイブのマイニングスクリプトに誘導し、閲覧者のパソコン上でマイニング作業を行わせるサイト運営者を対象に、複数の都道府県警連携の下で摘発を行った。2018年6月には、警察庁がHP上で注意喚起を呼びかけている(6)。

摘発された本件被告人は、不正指令電磁的記録取得罪および同保管罪として、横浜簡易裁判所で罰金10万円の略式命令を受けたが、これを不服として正式裁判を申し立てた(7)。

2．刑事裁判の経過

(1) 第1審（横浜地裁平成31年3月27日）(8)

検察官の公訴事実は、次の通りである。「被告人は，インターネット上のウェブサイト『a』を運営する者であるが，a閲覧者が使用する電子計算機の中央処理装置にその同意を得ることなく仮想通貨甲の取引履歴の承認作業等の演算を行わせてその演算機能を提供したことによる報酬を取得しようと考え，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，平成29年10月30日から同年11月8日までの間，a閲覧者が使用する電子計算機の中央処理装置に前記演算を行わせるプログラムコードが蔵置されたサーバーコンピューターに同閲覧者の同意を得ることなく同電子計算機をアクセスさせ同プログラムコードを取得させて同電子計算機に前記演算を行わせる不正指令電磁的記録であるプログラムコードをA株式会社が運営管理する日本国内に所在するサーバーコンピューター上のaを構成するファイル内

に蔵置して保管し，もって人が電子計算機を使用するに際して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を保管したものである」。

本件の事実関係自体についてはとくに争いはなく、不正指令電磁的記録保管罪の成否を巡って、本件プロムラムコードにおける不正指令電磁的記録該当性の有無を焦点に、もっぱらその解釈判断が争われた。不正指令電磁的記録とは、「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」である。客体の要件は、第1に「意図に沿うべき動作をさせず」又は「意図に反する動作をさせるべき」指令を内容とし、かつ第2に「不正な」指令であることである（以下、前者を「反意図性」、後者を「不正性」と呼ぶ）。

検察官は、暗号資産のマイニングが一般に周知されていない演算であり、閲覧者においてその実行に気づくこともできないのであり、意図に反する動作に当たると主張した。これに対して、弁護人は、Web閲覧者はJavaScriptの実行について、それが危険や有害なものでない限り、黙示の承諾をしているのであり、本件プログラムは広告用のスクリプトと何ら変わるものではなく、反意図性の要件を備えるものではないと反論した。また、不正性の要件に関して、検察官は、反意図性が存在すれば、原則として不正であり、例外的に許容される場合が認められるけれども、本件でとくに正当性が認められる根拠はないと主張したのに対し、弁護人は、コインハイブには閲覧者のパソコンを破壊したり情報漏洩を起こすような危険な作用はなく、不正なプログラムには当たらない等と主張した。

横浜地裁は、まず反意図性の判断基準について、「個々のプログラムが使用者の意図に反するものといえるかどうかは，個別具体的な使用者の実際の認識を基準とするのではなく，当該プログラムの機能の内容や機能に関する説明内容，想定される利用方法等を総合的に考慮して，当該プログラムの機能につき一般的に認識すべきと考えられると

ころを基準として判断するのが相当である」と判示している。そのうえで、本件プログラムコードについて、a. 機能の内容であるマイニングの実施につき、説明もなく、その実行について閲覧者の同意を得る仕組みも設けられていない、b. コインハイブをめぐって、賛否両論がある中で、ユーザーの計算リソースを勝手に利用する点で批判も出る等、一般的なユーザー（閲覧者）の間で広告表示等に代わる新たな収益化の方法として認知されていたとみとめることはできない、c. 閲覧者において本件マイニングに気づくことはなく、容認したとみることはできない点を指摘して、本件マイニングの実行の点について、「閲覧者等の一般的なユーザーが認識すべきと考えられるものということはでき」ず、反意図性要件の該当性が認められるとの判断を行っている。しかし、同地裁は、不正性の要件に関しては、なお合理的な疑いが残るとして、結論として客体該当性を否定し、無罪を言い渡した。この点について、同地裁は、不正な指令に限定された趣旨を、反意図性のあるプログラムの中に、「社会的に許容し得るものが例外的に含まれることから，このようなプログラムを処罰対象から除外する」点にあるとし、その判断基準について、「ウェブサイトを運営するような特定のユーザー及びウェブサイト閲覧者等の一般的なユーザーにとっての有益性や必要性の程度，当該プログラムのユーザーへの影響や弊害の度合い，事件当時における当該プログラムに対するユーザー等関係者の評価や動向等の事情を総合的に考慮し，当該プログラムの機能の内容が社会的に許容し得るものであるか否かという観点から判断するのが相当である」との一般的な基準を示している。そのうえで、a. 本件プログラムの実行により、消費電力の増加、処理速度の低下等の影響が生じるが、その程度は広告表示等のプログラムの場合と大きく変わらない、b. コインハイブをめぐっては、賛否両論があり、ウェブサイト閲覧者の同意を得ないでマイニングを行うことににつき、当時、公的機関による注意喚起や警告等もない中、「いきなり刑事罰に値するとみてその責任を問うのは行き過ぎの感を免れない」と指摘して、「本件プ

ログラムコードが社会的に許容されていなかったと断定することはできない」と結論づけ、不正性を否定したのである(9)。

(2) 控訴審（東京高裁令和2年2月7日判決）(10)

第1審の無罪判決に対し、検察官が控訴し、東京高裁に係属することになった。検察官は、原判決には法令の解釈適用の誤りや事実誤認があるとして争った。主要な内容を整理すると、反意図性が肯定される場合には、例外的に不正性が否定されるべきところ、①原判決は、サイト運営者のような特定のユーザーにとっての有益性・必要性等を不当に重視する一方、無断かつ無償でマイニングをさせられた閲覧者の利害を不当に軽視している、②ウェブサービスの質の維持向上のためにサイト運営者において報酬を受け得ることで、閲覧者に不利益を与えるとすることは許容できない、③賛否が分かれていることは、社会的許容性を肯定する事情とはいえない、④公的機関による注意喚起の有無等は、社会的許容性判断に影響するものではない等と主張した。

東京高裁は、検察官の論旨には理由があると認め、不正指令電磁的記録該当性を否定した原判決には第168条の2第1項の解釈の誤りがあるとして、これを破棄し、一転して被告人に有罪を言い渡した。

東京高裁は、不正指令電磁的記録該当性について、反意図性および不正性それぞれについて検討を加えている。まず、反意図性については、原判決がその判断に当たって、もっぱらプログラムの機能の認識可能性を基準にするもので、プログラムの機能の内容そのものを踏まえた規範的な検討をしていないと批判し、判断手法が正当ではないと説いている。同高裁によれば、不正指令電磁的記録に関する罪は、「電子計算機において，使用者の意図に反して実行されるコンピュータ・ウイルスなどの不正なプログラムが社会に被害を与え深刻な問題となっていることを受け，電子計算機による情報処理のためのプログラムが，『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』を与えるものではないという社会一般の者の信頼を保護し，電子計算機の社会的機能を保護するために，意図に沿う

べき動作をさせない，又はその意図に反する動作をさせるという反意図性があり，社会的に許容されない不正性のある指令を与えるプログラムの作成，提供，保管等を，一定の要件の下に処罰対象とするものである」とし、この趣旨を踏まえ、プログラムの反意図性につき、「当該プログラムの機能について一般的に認識すべきと考えられるところを基準とし上で，一般的なプログラムの使用者の意思に反しないものと評価できるかという観点から規範的に判断されるべきである」という。そのうえで、①本件プログラムコードは、閲覧者にその電子計算機の機能を提供させてマイニングを行わせるものであり、その実行について表示は予定されておらず、報酬についても閲覧が得ることは予定されていない。②ウェブサイト閲覧者は、閲覧のために必要なプログラムの実行については承認していると考えられるものの、本件におけるマイニングは閲覧のために必要なものではない、③閲覧者の電子計算機に一定の負荷を与えるものであるのに、報酬が発生した場合にも閲覧者には利益がもたらされない、④閲覧者に、マイニングの実行により電子計算機の機能が提供されていることを知る機会、これを拒絶する機会の保障もない点を指摘し、本件プログラムコードについて、「このようなプログラムの使用を一般的なプログラム使用者として想定される者が許容しないことは明らか」として、反意図性を肯定することができるのであり、この点に関する結論には原判決に誤りはないと判断している。

その一方で、東京高裁は、原判決が不正性を否定した判断に対して、解釈を誤った不合理な判断であると結論づけている。不正性の要件について、同高裁は「一般的なプログラム使用者の意に反するプログラムであっても，使用者として想定される者における当該プログラムを使用すること自体に関する利害得失や，プログラム使用者に生じ得る不利益に対する注意喚起の有無などを考慮した場合，プログラムに対する信頼保護という観点や，電子計算機による適正な情報処理という観点から見て，当該プログラムが社会的に許容されることがあるので，

そのような場合を規制の対象から除外する趣旨である」と述べる。そこで、本件プログラムにつき、「その使用によって，プログラム使用者（閲覧者）に利益を生じさせない一方で，知らないうちに電子計算機の機能を提供させるものであって，一定の不利益を与える類型のプログラムといえる上，その生じる不利益に関する表示等もされていないのであるから，このようなプログラムについて，プログラムの信頼保護という観点から社会的に許容すべき点は見当たらない」と判示して、不正性を肯定している。そして、原判決において不正性を否定する論拠として指摘された諸点について、逐一論難を加え、その不当性を摘示している。まず、ウェブサービスの質の維持向上に関し、この種の利益につき使用者が気づかない方法で受忍させて実現されるべきものでないと批判する。プログラムに対して賛否両論ある点については、そのこと自体で社会的許容性を基礎づけることはできないのであり、本件のように反意図性が肯定できる場合には、賛否が分かれていることは、むしろ否定する方向に働く事情であると説いている。さらに、注意喚起の有無といった事情、消費電力や処理速度の低下等が使用者の気づかない程度のものであったという事情は、反意図性・不正性を左右するものではないと指摘する。

以上により、控訴審では、第１審の無罪判決を不合理な判断であるとして退け、被告人に不正指令電磁的記録保管罪の成立が認められたのである(11)。

(3) 上告審の判断（最高裁第１小法廷令和４年１月20日判決）(12)

控訴審の有罪判決に対し、弁護人は、第168条の２第１項に規定する「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」の文言が、漠然不明確であるとして、憲法第21条第１項、同第31条に違反する等として、最高裁に上告を行った。最高裁は、弁護人による憲法違反の主張についてはいずれも排斥したが、不正指令電磁的記録の解釈を誤っているとして控訴審の判決を破棄し、被告人に無罪を言い渡した。

最高裁は、不正指令電磁的記録に関する罪の趣旨および保護法益について、「不正指令電磁的記録に関する罪は，電子計算機において使用者の意図に反して実行される不正プログラムが社会に被害を与え深刻な問題となっていることを受け，電子計算機による情報処理のためのプログラムが，『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』を与えるものではないという社会一般の信頼を保護し，ひいては電子計算機の社会的機能を保護するために，反意図性があり，社会的に許容し得ない不正性のある指令を与えるプログラムの作成，提供，保管等を，一定の要件の下に処罰するものである」と説く。これに基づいて、反意図性の解釈として、「当該プログラムについて一般の使用者が認識すべき動作と実際の動作が異なる場合に肯定されるものと解するのが相当」とし、一般の使用者が認識すべき動作の認定に当たり、「当該プログラムの動作の内容に加え，プログラムに付された名称，動作に関する説明の内容，想定される当該プログラムの利用方法等を考慮する必要がある」と指摘する。

また、不正性の解釈として、「電子計算機による情報処理に対する社会一般の信頼を保護し，電子計算機の社会的機能を保護するという観点から，社会的に許容し得ないプログラムについて肯定されるものと解するのが相当」であると判示し、「その判断に当たっては，当該プログラムの動作の内容に加え，その動作が電子計算機の機能や電子計算機による情報処理に与える影響の有無・程度，当該プログラムの利用方法等を考慮する必要がある」と指摘している。

上記の一般的な解釈判断に基づいて、本件への具体的な適用を図っている。まず反意図性の点に関して、一般的なウェブサイトにおいて、運営者が閲覧を通じて利益を得る仕組みとして広告表示プログラムが広く実行されている実情に照らし、一般の使用者がサイト閲覧中に閲覧者の電子計算機を一定程度使用して運営者が利益を得るプログラムが実行され得ることは、「想定の範囲」でもあるといえるものの、こうしたプログラムとして、本件プログラムコードの動作を一般の使用者

が認識すべきといえるかについて、①マイニングの実行について同意を得る仕組みになっていないこと、②マイニングに関する説明、その表示もなかったこと、③閲覧者の電子計算機にマイニングを行わせるという仕組みは一般の使用者に認知されていなかったという事情を摘示して、反意図性は肯定された。

一方、不正性に関して、①電子計算機の機能やその情報処理に与える影響は、閲覧者がその変化に気づかない程度のものであったこと、②ウェブサイトの運営者が閲覧を通じて利益を得る仕組みは、情報の流通にとって重要であり、社会的に受容されている広告表示プログラムと比較して、閲覧者の電子計算機の機能やその情報処理に与える影響に有意な差異はないこと、③マイニング自体、仮想通貨の信頼性を確保するための仕組みであり、社会的に許容し得ないものではないことを挙げて、「本件プログラムコードの動作の内容，その動作が電子計算機の機能や電子計算機による情報処理に与える影響，その利用方法等を考慮すると，本件プログラムコードは，社会的に許容し得ないものとはいえず，不正性は認められない」と結論づけられた(13)。

下級審で無罪と有罪とに判断が分かれ、最高裁に持ち込まれたケースであるが、争点は、もっぱら本件プログラムコードが不正指令電磁的記録に当たるか否かという解釈判断に係るものであり、構成要件上の客体に関する要件解釈の仕方が犯罪の成否を左右することになった。

不正指令電磁的記録の罪を構成する客体について判断を行う場合に、本罪の保護法益・罪質についての理解が影響を及ぼし得る。この点について、控訴審および最高裁は、いずれも、プログラムに対する社会一般（あるいは社会一般の者）の信頼の保護と電子計算機の社会的機能の保護を挙げている。もっとも、控訴審では、社会一般の者の信頼の保護が重視されているように思われる。これに対して、最高裁は、不正性の判断基準を示す際に、社会一般の信頼の保護と並べて、あらためて電子計算機の社会的機能の保護を掲げ、不正性と関連させつつ社会的に許容できないプログラムに限定される旨を説示している。そして、

不正性を判断するに当たって考慮すべき事情として、電子計算機の機能やその情報処理に与える影響の有無・程度、利用方法が例示されており、むしろ電子計算機の社会的機能の側面を重視する内容になっている。

Ⅲ　不正指令電磁的記録に関する罪の制定経緯と立法上の問題

1．制定の経緯

(1)　サイバー犯罪条約の採択と国内での検討

不正指令電磁的記録に関する罪（第19章の2）の罪は、2011年、「情報処理の高度化に対処するための刑法等の一部を改正する法律」（平成23年法律第74号）により、刑法典中に新たに追加新設された。本章の追加は、2001年、欧州評議会により、サイバー犯罪に関する世界で初めての国際条約である「サイバー犯罪条約」が採択[14]されたことを契機としている。本条約の成立にあたり、日本もオブザーバーとして参加し、条約に準拠しつつ国内法の整備が進められた。条約の批准・承認のための国内刑法の整備の一環として、本章が新設されたのである[15]。

サイバー犯罪条約では、第6条で「装置の濫用」（Misuse of devices）が規定され、その中で、不正アクセス（同条約第2条）、不正な傍受（同第3条）、データの妨害（同第4条）、システムの妨害（同第5条）に規定する犯罪を実行する意図で、特定の装置（ソフトウェアを含む）あるいはデータの製造・販売等の行為についての犯罪化が盛り込まれている（同第6条（a）（ⅰ））[16]。

条約批准に向けた国内法における対応を検討するため、経済産業省では、サイバー刑事法研究会（座長・山口厚）[17]を設置し、2002年にその報告書が提出された[18]。この報告書では、研究会の意見として次のように取りまとめられた。「第6条（a）（ⅰ）に規定する犯罪使用目的による不正プログラムの製造・頒布等の処罰化については、留保が可能であるため、新たな立法化をせずとも条約への加盟は可能であるが、

仮に当該行為を処罰するとすれば、産業界、とりわけ情報セキュリティ関係企業、研究機関等への影響も大きいと考えられる。『不正』な結果を発生させ得るプログラムであっても、正当な業務目的でも利用される場面が考えられるため、プログラムの客観的な性質だけで『不正』か否かを決することは難しく、理論的には、プログラムの客観的な性質に加えて、犯罪を行うために使用する意図の有無により処罰の対象となるか否かを判断するという判断枠組みが必要となると考えられる。もっとも実際上は、結果が発生して初めて目的の存在が確認される場合が多くなると思われる。正当な業務目的、研究目的で用いられ得るセキュリティ監査ツールなども、犯罪目的がある場合にはその所持について処罰の対象となる可能性が生じるため、仮に、以上のような処罰規定を新たに設ける場合であっても、自由なプログラム開発やビジネスに抑制効果が生じないよう、構成要件の明確性については十分な検討が必要である」[19]と。

その後、2003年3月に法務大臣が法制審議会に対し、ハイテク犯罪に対処するための刑事法の整備に関する諮問を行い、法制審議会では同年9月に「ハイテク犯罪に対処するための刑事法の整備に要綱（骨子）」[20]を採択し、これを法務大臣に答申した。これを受けて、法務省において、関係省庁とも協議を行い、具体的な法案の準備が進められたのである。

⑵　ドイツ刑法の対応

サイバー犯罪条約は、前述したように、同条約第2条ないし第5条が規定する犯罪についてそれらの予備的行為の処罰化を要求するものであった。ドイツでは、2007年の刑法改正の法律により、条約第6条第1項に対応するため、刑法第202条c（データの探知及び傍受の予備）が規定されることとなった[21]。同規定の条文は次の通りである[22]。

① 1．データ（第202条a第2項）へのアクセスを可能とするパスワード若しくはその他の保護コード，又は，

2．このような行為の遂行を目的とするコンピュータ・プログラ

ムを製造し，自ら取得し，若しくは他の者に取得させ，販売し，他の者に引き渡し，頒布し，又はその他利用可能にすることにより，第202条 a 又は第202条 b に定める犯罪行為の予備をした者は，2 年以下の自由刑又は罰金刑に処する。

② 第149条第 2 項及び第 3 項を準用する。

ドイツ刑法第202条 c は、同第202条 a、第202条 b、第303条 a、第303条 b に対する危険な予備的行為を独立して処罰するものである(23)。犯行の客体は、第一にデータへのアクセスを可能にするパスワードその他の保護コード（第 1 項第 1 号）であり、第二に第202条 a、第202条 b、第303条 a、第303条 b の犯行を目的とするコンピュータ・プログラムである(24)。これらの客体の製造、取得、販売等により上記規定が定める犯罪の予備を、第202条 c が処罰対象として定めている。このようにドイツ刑法は、サイバー犯罪条約の要請に沿って、不正アクセス、不正な傍受等に係る予備罪として、第202条 c を規定している。

それまでは、ハッキング・ツールの製造や販売について処罰対象とはされていなかった(25)。せいぜい第202条 a の幇助が問題となるに過ぎず、共犯として可罰的となるためには第202条 a の正犯の実行が必要であり、実行が欠ける場合には可罰的ではない未遂の幇助に止まらざるを得ない(26)。202条 c の立法理由について、提案者によれば、そのような行為の高い危険性は処罰の必要性を擁護し、とくに違法な目的で作られたいわゆるハッキング・ツールについてはそうであり、インターネットを通じて広く流布し得、入手も容易であるため、その単純な利用は直ちに相当な危険を生じるので、そのような危険な手段の流布を処罰の対象とすることにより、効果的に抑止することができると説明されている(27)。そこで、第202条 c 第 1 項第 2 号は、第202条 a や第202条 b 等の犯罪の遂行を目的とするコンピュータ・プログラムの製造、販売等を通じた犯罪の予備を処罰するものとして規定された(28)。本規定は、過剰な処罰化を回避するために、犯罪の遂行を目的とすることを要件として規定し、コンピュータ・プログラムに客観的な制限

を設けているのである[29]。

(3) 日本での立法化について

予備罪として規定されたドイツ刑法に対し、日本ではこれと異なる立法形式が採用された。日本における立法化を検討する議論の過程で、予備罪的構成によった場合、①個人情報を流出させたり、勝手に電子メールを送信するウイルス等が含まれなくなる、②業務妨害の予備罪として構成する場合には、個人の場合を捕捉できなくなる、③現行法上、予備罪は極めて重い犯罪に関してのみ処罰対象としているところ、早期規制の必要性、害悪蔓延の危険性を根拠に処罰するとした場合に、法定刑はかなり軽くならざるを得ないといった意見が出され[30]、適切な方法ではないとして排除されたのである[31]。

不正指令電磁的記録に関する罪（第19章の２）の新設に際し、罰則の必要性について、立案当局者は、「近時，いわゆるコンピュータ・ウイルスが，広範囲の電子計算機で使用者の意図に反して実行され，広く社会に被害を与え，深刻な問題になっており，これを放置すれば，人は，電子計算機による情報処理のプログラムを実行するに際して，そのプログラムを信頼することができないこととなり，ひいては，社会的基盤となっている電子計算機による情報処理が円滑に機能しないこととなる」[32]と指摘し、そのうえで、「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ものではないという社会一般の者の信頼」を保護するために、こうした不正プログラムについて、その作成・提供・供用・取得・保管の各段階の行為を処罰するものであると説明している。この説明に示されているように、保護法益は、プログラムに対する「社会一般の者の信頼」に求められた。こうした理解を前提として、文書の真正さに対する信頼を保護する文書偽造罪との類似性が見出されて、社会的法益として位置づけられるとともに、「偽造のアナロジー」[33]に基づいて条文化され、偽造罪に続いて規定が配置されることになったのである。

2．立法上の問題

(1) 文書偽造のアナロジー？

確かに、不正プログラムの作成という行為態様が偽造と類似している側面は認められるものの、不真正な（物理的な）文書の創出と不正プログラムの作出とでは、それぞれが有する社会的なリスクの内容やその性質に違いがある。つまり、不真正な文書の流通による社会的な害悪ないし弊害は不正プログラムの流布の場合と同一視できないということである。文書偽造罪では、文書が社会的に一定の証明作用を果たし、経済取引活動においても重要な機能を担うものであるために、文書に対する信頼、信用は必要不可欠であり、文書自体の真正性の確保が要求された。これは、文書自体を社会関係の中で他人が見る（読む）ということを前提にしている。一方、不正プログラムの場合には、それ自体が物理的な意味で存在し、そのようなものとして流通するわけではない。問題なのは、そのプログラムによる作用である。立案当局者自身も「社会的基盤となっている電子計算機による情報処理が円滑に機能し」なくなる弊害について指摘していた。そして、このような事態が生じたときは、大きな社会的な混乱を招くことが予想されるのである。文書偽造罪の場合には、立法目的の観点から、その手段として偽造それ自体を処罰する意味あるいは必要性が認められる。これに対し、仮に立法の目的として、コンピュータによる情報処理の円滑な機能を含むものとすれば、その手段として刑事規制の対象とすべきなのは、そのような機能に何らかの影響を及ぼす可能性のあるプログラムに限定するのが合理的であると考えられる。にもかかわらず、偽造罪とのアナロジーを根拠に、法所定の電磁的記録一般を対象にその作成等を独立して処罰するという立法は、目的に照らして規制の対象が広汎に過ぎる虞を生じ、憲法上の問題を招きかねない(34)。まさに、コインハイブ事件は、このような立法上の問題を露呈するものといえよう。

⑵ 最高裁における処理の特徴

最高裁は、この問題について、不正性の要件を用いて解決を図っている。本罪の法益について、最高裁は、―立法当局者の説明と同様に―「情報処理に対する社会一般の信頼」および「電子計算機の社会的機能」を指摘する。本罪の法益を前者とした場合、社会的に許容されているか否かという判断基準を導出することは難しいように思われる。最高裁の判示で注目すべきなのは、不正性要件の解釈を展開するに当たって、あらためて上記二つの法益を指摘しつつ、社会的許容性に言及している点であろう(35)。読み方によっては前者の法益を主として反意図性の要件に、後者を主として不正性の要件に関連づけて把握し、反意図性を備える電磁的記録であったとしても、後者の法益保護（目的）との関連で「社会的に許容し得ないプログラム」に限定され、社会的に許容される範囲では不正性が欠如し、客体から除外されると判断したものと解することができる。控訴審でも、同様の法益理解が示されていたが、反意図性が存在すれば原則的に不正性も認められるという見方が強調されていた。これに対して、最高裁は、不正性の要件に反意図性とは異なる独立した意義を認め、具体的妥当性が得られる柔軟な判断を可能とする解釈上の余地を残し、この要件に積極的な役割を与えていると見ることができる。

コインハイブ事件における裁判での表面的な争点は不正指令電磁的記録該当性に係る解釈についてであるが、この法律解釈の問題は、不正指令電磁的記録の罪による刑事規制の介入とサイバー空間における自由で創造的な発展可能性の確保という要求との緊張関係を背景としている。このような場面で過剰な刑事規制が強行されることになれば、萎縮効果をもたらし、自由な発展可能性を阻害する虞が生じる(36)。コインハイブ事件は、まさにこの点に関する価値判断が法律の解釈問題として表面化した事件であったと言っても過言ではない。そして、最高裁は、不正性という要件の法律解釈を通じて、実質的にサイバー空間における自由で創造的な発展に一定の配慮を示す価値判断を行った

ものとする評価も可能である[37]。

Ⅳ　不正指令電磁的記録に関する罪の法益とその解釈

１．法益（罪質）の理解について

一般に刑罰法規を解釈するに当たって、その目的やこれと関連して法益が一つの指針を提供することについては広く承認されている[38]。コインハイブ事件における最高裁の判断においても、法益が一定の解釈を導くうえで重要な機能を果たしているのである。そこで、あらためて不正指令電磁的記録の罪の法益について確認しておこう。

日本では、不正指令電磁的記録の罪の規定を設ける際に、予備罪をモデルとする規定方法を放棄し、偽造罪類似モデルによる方法を採用した結果として、―文書偽造罪の体裁と揃えるために―「プログラムに寄せられる社会一般の信頼」が保護法益として持ち出されたものと推察される。通説も、立法当時における立案当局者の意図に沿って、本罪の法益をそのように理解している[39]。しかし、この選択には問題があったように思われる。予備罪として構成する場合には、時系列として予備行為の後に想定される可罰的な犯行の遂行との関連で、予備行為自体に内在する（抽象的な）危険性を処罰根拠とし、当該犯行の遂行目的の存在を要件とすることにより処罰範囲の限定を図ることが可能であった。これに対して、偽造類似モデルに拠ったために、法益が「信頼」に変換され、このことによって実害と関連する何らかの危険性から切り離されてしまったのである。保護法益に社会一般の信頼を持ち込んだことが、本罪の罪質理解を曖昧にし、処罰範囲の広汎化を招く要因になっているのではないだろうか[40]。そもそも、プログラムに対する「信頼」は、プログラムによる社会における害悪・弊害の発生を防止してこそ、醸成されるものである。文書偽造罪における文書の真正性に対する信頼に擬して、不正指令電磁的記録の罪の場合にも同様と理解する信頼保護構成は、文書それ自体の流通を前提とする文書

偽造罪とそれを予定することのないプログラムとを同列に取り扱っているのであり、適切とは思われない。

立法過程の議論の中で指摘された予備罪構成とする場合の問題点（前記（2）〔iii〕参照）について、果たして的確な指摘であったか疑いがある(41)とともに、偽造罪のアナロジーとして理解することの妥当性について検討が十分であったのか、検証を要する問題である。立法自体に内在する問題については、コインハイブ事件を通じて広く認識されるようになってきており、不正指令電磁的記録の罪が成立する範囲を合理的に限界づけるため、電磁的記録概念の実質化を試みる見解(42)も見られる。その意図は適切であると考えられるものの、保護法益を社会的信頼とする前提はそのまま維持されている点で、なお疑問が残る。というのも信頼という法益には多様な内容を盛り込み得るからである。論者は、一定の実害惹起の可能性が認められる場合やサイバー犯罪条約が予定する場合に可罰性を限定しようとしているのであって、この視点は現実的な法益侵害ないし危険性に犯罪性を求めるものである。この考えを徹底するのであれば、むしろ社会的信頼という法益自体を問い直す必要が生じるのではないだろうか。この意味で、もはや信頼保護という前提的な法益理解を無批判に維持することは妥当ではない(43)。

いまや、社会はコンピュータ・ネットワークに依存して成立していると言っても過言ではない。デジタル化されたネットワークシステムは、社会の重要なインフラとなっているのである。このため、ウイルス等のプログラムによって、システムが正常に機能せず、大きな被害を惹起するリスクにさらされている。このようなサイバーセキュリティに対するリスクをコントロールするために、刑事規制の介入は必要不可欠であると考えられる。そして、デジタル化されているプログラムである限り、サイバー空間では広範に流通し得ることを考慮すれば、悪意のあるコンピュータ・ウイルスの作成自体を可罰的とする必要性も十分に根拠づけられる。仮に、不正指令電磁的記録に関する罪

を、このような観点から理解するのであれば、理論的には、不特定または多数の人の生命、財産等の法益を包括的に保護するという意味で、一種の公共危険犯[44]として位置づけることも可能なのではないだろうか。立法目的が、コンピュータ・ウイルスによって「広範囲の電子計算機で使用者の意図に反して実行され，広く社会に被害を与え」ることを抑止する点にあるとすれば、偽造類似型の信頼保護ではなく、社会における不特定または多数の人の法益保護を目的とし、それに対する抽象的危険[45][46]を処罰の根拠として規制を図るものとして、第168条の2の規定を理解することも決して不合理ではない。この意味で、従来の社会一般の信頼という法益を排除し、本罪を公共危険犯と位置づけ、コンピュータ・システムおよびコンピュータ・ネットワークの正常な機能確保を目的とするこれらの公共的な利用の安全を保護法益として理解する方が適当であろう[47]。

2．客体の意義に関する解釈

上記の法益理解によるのであれば、第168条の2第1項が規定する「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」とは、悪意（害意）性のあるウイルスを指す表現と解するのが相当である。コインハイブ事件において、いずれの裁判所も共通に反意図性を認めた最大の理由は、サイトを閲覧した利用者の同意を得ずに、その資源を無断で利用した点であろう。裏を返すと、利用者の同意を得ていたならば、特段の問題はなかったことになる。そうだとすると、プログラム自体の問題とは関連しないと考えることも可能である。本件プログラムコード自体は、コンピュータの正常な機能に影響を与えるようなものではない[48]とすれば、コンピュータ・ネットワークに対しておよそ抽象的な危険を伴うプログラムとはいえず、もはや不正指令電磁的記録には該当しないと判断すべきである。

Ⅴ　結　語

コインハイブ事件を素材にして、刑事裁判の経過を辿りながら、最高裁の判断の特徴を明らかにするとともに、この事件によって顕在化した第126条の２の解釈適用上の問題が、不正指令電磁的記録の罪を偽造罪類似として立法化した点に起因していると分析したうえで、従来の信頼保護という法益理解を批判し、本罪を（抽象的）公共危険犯として把握すべきことを主張し、これに基づく解釈を試みた。もとより、思い付きの域を出ない論証にとどまっており、試論に過ぎない。法益に関してより精確な考察の必要性を痛感しているし、可罰範囲についての詳細な検討も要する。差し当たって、解釈上の一つの可能な選択肢として試みに提示することで、大方の批判を仰ぎたい。

（１）　最高裁判所第一小法廷令和４年１月20日判決（令和２（あ）457号 不正指令電磁的記録保管被告事件：裁判所ウェブサイト https://www.courts.go.jp/app/files/hanrei_jp/869/090869_hanrei.pdf　閲覧日2022年８月20日。以下、本稿でのウェブサイトの最終閲覧日はすべてこの日付による。）

（２）　高木浩光「コインハイブ事件で否定された不正指令電磁的該当性とその論点」Law and Technology No.85（2019年）21頁。

（３）　事件当時は「仮想通貨」と呼ばれていたが、その後「情報通信技術の進展に伴う金融取引の多様化に対応するための資金決済に関する法律等の一部を改正する法律」（令和元年法律第28号）により、「暗号資産」に変更されたため（「資金決済に関する法律」第２条第５号参照）、この呼称を使用する。

（４）　ドイツの Badges 2 Go 社が2017年９月から提供するサービスであったが、2019年３月に打ち切られている（高木・前掲注（２）20頁注２）。

（５）　齊藤貴義・IPUSIRON『Wizard Bible 事件から考えるサイバーセキュリティ』（2021年）78頁〔平野敬〕参照。

（６）　高木・前掲注（２）20頁のほか、大橋充直「サイバー（ハイテク）犯罪の捜査　第108回」捜査研究 No.859（2022年）86-87頁参照。

（７）　本件の弁護活動については、受任した平野敬弁護士による詳しい説明がある（前掲注（５）74頁以下）。

（８）　横浜地裁平成31年３月27日判決（平成30年（わ）第509号）LLI/DB 判例秘書 L07450537。

(9)　本判決の論点とその検討につき、高木・前掲(2)25頁以下。

(10)　東京高裁令和2年2月7日判決（令和元年（う）第883号）LLI/DB判例秘書L07520082。

(11)　控訴審の判断については、批判的な見解が少なくない。たとえば、永井善之「判批」新・判例解説Watch刑法No.147、品田智史「判批」法学セミナー787号（2020年）134頁、西貝吉晃「技術と法の共進化を企図した法解釈の実践―コインハイブ高裁判決を素材に」法学セミナー792号（2021年）43頁以下、岡田好史「判批」刑事法ジャーナル68号（2021年）163頁など。肯定的なものとしては、白鳥智彦「判批」警察学論集73巻9号（2020年）217-218頁。これらのほか、本判決の検討として、高木浩光「コインハイブ不正指令事件の控訴審逆転判決で残された論点」Law and Technology No.91（2021年）49頁以下。

(12)　前掲注(1)。

(13)　最高裁判決の検討として、永井善之「判批」新・判例解説Watch刑法No.176（2022年）、品田智史「判批」法学セミナー809号（2022年）130-131頁、西貝吉晃「サイバーセキュリティの保護とイノベーションの促進の両立―コインハイブ事件最高裁判決を素材に」法学セミナー808号（2022年）40頁以下、高木浩光「判批」Law and Technology No.96（2022年）51頁以下、神渡史仁「判批」法律のひろば75巻7号（2022年）56頁以下、池田知史「最高裁時の判例」ジュリスト1574号（2022年）107頁以下など。

(14)　この条約（通称、ブタペスト条約）は、2001年11月の欧州評議会閣僚委員会会合で正式に採択され、2004年に発効した。2022年2月現在、締約国数は、G7諸国を含む66か国に達している（外務省「国際組織犯罪に対する国際社会と日本の取組」https://www.mofa.go.jp/mofaj/gaiko/soshiki/cyber/index.html　参照）。

(15)　サイバー犯罪条約に関し、日本では2004年に締結についての国会承認手続を済ませ、「不正指令電磁的記録に関する罪」の新設により、サイバー犯罪条約上の犯罪化に対応する国内刑法の整備が完了したことを受けて、2012年に受諾書の寄託を行い、同年11月に日本において法的効力が発生した（外務省「サイバー犯罪に関する条約」mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html　参照）。

(16)　ただし、第6条については、締約国における留保を可能としている。

(17)　西田典之ほか編『注釈刑法　第2巻　各論（1）』(2016年) 543頁〔嶋矢貴之〕。

(18)　サイバー刑事法研究会「欧州評議会サイバー犯罪条約と我が国の対応について」(https://dl.ndl.go.jp/view/download/digidepo_1285853_po_Cybercriminallawreport.pdf?contentNo=1&alternativeNo=)。

(19)　前掲注(18)21頁。

(20) 答申された要綱（骨子）の内容は、ジュリスト1257号（2003年）34-35頁に資料として掲載されている。諮問から法制審議会における審議の経過については、北村篤「ハイテク犯罪に対処するための刑事法の整備に要綱（骨子）」ジュリスト同号6-7頁参照。

(21) BT-Drucks. 16/3656.S.8（https://dserver.bundestag.de/btd/16/036/1603656.pdf）;*Kinhäser/Neumann/Paeffgen* [Hrsg.],StGB Band 2,5.Aufl.,2017, S.1600〔*Kargel*〕.

(22) § 202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder

2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

本条項新設当時、1項の法定刑は1年以下と定められていたが、2015年の改正により、上記のように法定刑の上限が2年に引き上げられた。本文の邦訳は、法務省刑事局『刑事法制資料　ドイツ刑法典』(2021年) 189頁によるものである。

(23) BT-Drucks.16/3656,S.19（https://dserver.bundestag.de/btd/16/036/1603656.pdf）; *Kinhäser/Neumann/Paeffgen* [Hrsg.],StGB, Bd.2, S.1600f.〔*Kragel*〕. ドイツ刑法第202条aは、データの探知につき、第1項で「自己のために予定されておらず，かつ無権限のアクセスから特に保護されているデータへのアクセスを，権限なく，アクセス保護措置を突破して，自ら取得し，又は他の者に取得させた者は，3年以下の自由刑又は罰金刑に処する」と規定し、データへの無権限アクセスを処罰する規定である。これは、サイバー犯罪条約第2条に対応するものである。第2項は、ここにいうデータの意味に関する規定であり、「電気的，磁気的又はその他直接には知覚できない形で保存され，又は伝達されるものに限る」と定めている。第202条bは、データの傍受につき、「技術的手段を用いて，自己のために予定されていないデータ（第202条a第2項）を，非公然に伝達されるデータから，又はデータ処理装置が発する電磁波から自ら取得し，又は他の者に取得させた者」を処罰の対象とする規定であり、サイバー犯罪条約第3条に対応している。第303条aはデータの改変、第303条bはコンピュータの破壊に関する規定であり、サイバー犯罪条約第4条、第5条に対応するものである（引用したドイツ刑法の邦訳は、前掲注(22)188-189頁による。）。

(24) *Kinhäser/Neumann/Paeffgen* [Hrsg.],StGB, Bd.2, S.1602〔*Kragel*〕.
(25) *Kinhäser/Neumann/Paeffgen* [Hrsg.],StGB, Bd.2, S.1600〔*Kragel*〕.
(26) *Kinhäser/Neumann/Paeffgen* [Hrsg.],StGB, Bd.2, S.1600〔*Kragel*〕.
(27) BT-Drucks.16/3565,S.12（https://dserver.bundestag.de/btd/16/036/1603656.pdf）.
(28) BT-Drucks.16/3565,S.12（https://dserver.bundestag.de/btd/16/036/1603656.pdf）.
(29) BT-Drucks.16/3565,S.19（https://dserver.bundestag.de/btd/16/036/1603656.pdf）.
(30) 山口厚「コンピュータ・ウイルス罪の論点」法とコンピュータ30号（2012年）60頁、同「サイバー犯罪に対する実体法的対応」ジュリスト1257号（2003年）17-18頁。さらに、杉山徳明＝吉田雅之「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」について（上)」法曹時報64巻４号（2012年）66頁、鎮目征樹「不正指令電磁的記録作成等」（168条の２・168条の３）法学教室407号（2014年）30頁参照。
(31) これに対し、予備罪構成を支持する見解も存在する（渡邊卓也『ネットワーク犯罪と刑法理論』（2018年）267頁以下)。
(32) 杉山＝吉田・前掲注(30)65頁。
(33) 山口・前掲注(30)60頁。
(34) 憲法上の問題、とくに明確性の観点から違憲性を論じるものとして、木下昌彦「コンピュータ・プログラム規制と漠然性故に無効の法理（上)」NBL1181号（2020年）７-８頁、同「コンピュータ・プログラム規制と漠然性故に無効の法理（下)」NBL1182号（2020年）42頁以下、大石和彦「『コインハイブ事件』に含まれる憲法上の争点」筑波ロー・ジャーナル29号（2020年）９頁以下。
(35) 永井・前掲注(13)３頁。さらに、西貝・前掲注(13)48-50頁参照。
(36) 稲谷龍彦「道徳的問題への刑事法的介入」法学セミナー785号（2020年）107頁。学説上も、結論として無罪とする結論を支持する見解が多いと思われるが、この点を考慮するものも少なくない（たとえば、渡邊卓也「不正指令電磁的記録に関する罪における反『意図』性の判断について」Information Network Law Review,Vol.19（2020年）29頁、大石・前掲注(34)18頁、西貝・前掲注(11)55頁、・前掲注(35)46頁など)。
(37) もっとも、最高裁はあくまでも本件における具体的態様の下での判断を行ったに過ぎず、マイニング一般について正当化する趣旨ではないという指摘（神渡・前掲注(13)65頁）にも留意する必要がある。
(38) たとえば、井田良『講義刑法学・総論［第２版]』（2018年）20-21頁参照。
(39) 大塚仁ほか編『大コンメンタール刑法（第３版） 第８巻』（2014年）341頁〔吉田雅之〕、井田良『講義刑法学・各論』（2016年）483頁、西田典

之ほか編・前掲注(17)545頁〔嶋矢〕、西田典之〔橋爪隆補訂〕『刑法各論第７版』（2018年）412頁など。

(40)　このような問題意識については、ある程度共有されているように思われる（たとえば、鎮目征樹ほか編『情報刑法Ⅰ　サイバーセキュリティ関連犯罪』（2022年）157頁〔鎮目征樹〕参照）。

(41)　木下・前掲注(34)「コンピュータ・プログラム規制と漠然性故に無効の法理（上）」７-８頁。

(42)　たとえば、永井善之「不正指令電磁的記録概念について」金沢法学63巻１号（2020年）84-85頁、105頁、岡部天俊「不正指令電磁的記録概念と条約適合的解釈―いわゆるコインハイブ事件を契機として―」北大法学論集70巻６号（2020年）163頁。

(43)　最近では、不正指令電磁的記録の罪につき、サイバーセキュリティの観点から、情報セキュリティの分野で情報の要素とされる、機密性（confidentiality）、完全性（integrity）、可用性（availability）の侵害可能性を問題とすべきであり、こうしたCIAを法益として位置づけるべきであるとする主張（西貝吉晃「不正指令電磁的記録に関する罪の解釈論」罪と罰58巻３号（2021年）24頁）も展開されている。この見解につき、鎮目ほか編・前掲注(38)158頁〔鎮目〕。

(44)　公共危険犯の一般的な意義については、さしあたり上野幸彦＝太田茂『刑事法入門』（2018年）82頁〔上野幸彦〕。公共危険犯の法益は公共の安全であるが、それは個人の生命、自由、財産等を内含する包括的かつ集合的な利益として理解することができる。したがって、不正指令電磁的記録の罪は、こうした法益に対する抽象的危険の発生を処罰根拠とするものと解される（抽象的危険犯と法益との関係については、金尚均『危険社会と刑法』（2001年）124-134頁参照）。

(45)　予備罪として規定したドイツにおいては、第204条ｃにつき抽象的危険犯であると解されている（Z.B., *Kinhäser/Neumann/Paeffgen* [Hrsg.],StGB, Bd.2, S.1601〔*Kragel*〕）。

(46)　抽象的危険犯に関する精緻な分析として、嘉門優『法益論―刑法における意義と役割―』（2019年）132-161頁。

(47)　公共危険犯とする法益理解はかなり飛躍的な考え方であるかもしれないが、たとえば、佐久間教授は、不正アクセス禁止法を一種の公共危険罪と把握する見解（佐久間修『最先端法領域の刑事規制』（2003年）353頁）を示されており、中核刑法における法益分類としても十分に可能であると考えられる。

(48)　岡田好史「不正指令電磁的記録に関する罪をめぐる現状と課題」専修大学法学研究所所報No.60（2020年）109頁、同・前掲注(11)163頁。なお、コインハイブ事件で被告人が利用するJavaScriptの技術的な安全性に関して、小田啓太＝西貝吉晃「アプリ開発の実務を踏まえた不正指令電磁的

記録に関する罪の一考察」千葉大学法学論集36巻１号（2021年）32-31頁参照。

＊本稿は、2022年５月28日に、日本政治法律学会春季大会における報告に基づき、これに加筆、補正して作成したものである。