



HOKKAIDO UNIVERSITY

Title	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
Author(s)	岡部，天俊
Citation	北大法学論集，70(6)，155-173
Issue Date	2020-03-31
Doc URL	https://hdl.handle.net/2115/77199
Type	departmental bulletin paper
File Information	lawreview_70_6_05_Okabe.pdf



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 ——

岡 部 天 俊

(1) 問題の所在

2018年6月、ウェブサイト に一定のプログラムを埋め込むことにより、ウェブサイトの閲覧者に無断でそのコンピュータに仮想通貨マイニング（以下、マイニングという）を実行させ収益を得ていた16名が、不正指令電磁的記録保管などの疑いで全国各地で摘発を受けたとの報道¹がなされ、これにより、コンピュータ利用者に無断でマイニングを実行させるプログラムにつき不正指令電磁的記録に関する罪²（以下、不正指令電磁的記録関連罪という）の成否が問題となり得るということが本格的に認知されはじめたといえよう³。さらに、事案はかなり異なる（詳細は後述）ものの、同年7月には、他人に無断でそのコン

¹ 日本経済新聞2018年6月15日朝刊39頁。国家公安委員会2018年6月14日定例委員会説明資料（<https://www.npsc.go.jp/report30/06-14.pdf>）も参照。なお、引用ウェブサイトの最終閲覧は2019年11月7日であり、以下の引用ウェブサイトについても同様である。

² 「情報処理の高度化等に対処するための刑法の一部を改正する法律」（平成23年法律第74号）により導入され、平成23年7月14日に施行されたものである。

³ 同様の事件は、近時ドイツにおいても生じているようである（vgl. *Olivia von Westernhagen*, Malvertising-Kampagne setzt auf Krypto-Mining in fremden Browsern, heise online 15.9.2017; *Achim Barczok*, Pirate Bay lässt heimlich Krypto-Miner auf Nutzer-PCs laufen, heise online 16.9.2017）。

コンピュータにマイニングを実行させるプログラムをインストールさせる行為につき、不正指令電磁的記録供用罪の成立を認める裁判例⁴が登場しており、今後、ユーザーに無断でマイニングを実行させるプログラム全般が不正指令電磁的記録関連罪の対象となるという観測が不可能ではない状況となっていた。

こうした状況において、2019年3月27日、横浜地裁第1刑事部は、ウェブサイト閲覧者に無断でそのコンピュータにマイニングを実行させるという内容のプログラムをウェブサイトに埋め込んでいたという事案（いわゆるコインハイブ事件）において、当該プログラムの不正指令電磁的記録該当性を否定することにより、不正指令電磁的記録保管罪の成立を否定し無罪とする判断を示し（以下、本判決という）、大きな注目を集めた⁵。本判決は、問題となったプログラムにつき、「社会的に許容し得るかどうか」が問題とされる不正性の要件を満たさないことを理由として、不正指令電磁的記録該当性を否定したのである。しかし、後述のように極めて多数のプログラムが反意図的動作の要件を満たし得るという今日の状況においては、前述のように理解されたかたちでの不正性の要件のみによって構成要件該当行為の範囲を限定するというアプローチは、大きな問題を抱えているといわざるを得ない。「社会的に許容し得るかどうか」という高度に開かれた基準でもって多数のプログラムの客体性の有無を判断するというのでは、客体性の有無をめぐる判断が非常に不明確となり、不正指令電磁的記録関連罪の新設に際して懸念されていた、プログラムの開発者や利用者への萎縮的効果が発生しかねないように思われる⁶。

以上のような問題意識から、本稿は、不正指令電磁的記録概念に再検討を加え、同概念の明確化を試みるものである。

（２）従来の一般的理解とその問題点

⁴ 仙台地判平成30・7・2LEX/DB25560905。

⁵ LEX/DB25570338。本判決の評釈・解説として、板倉陽一郎「解題 コインハイブ事件」Law & Technology No. 85（2019年）15頁以下、高木浩光「判批」Law & Technology No. 85（2019年）20頁以下、永井善之「判批」新・判例解説 Watch 刑法 No. 145（https://www.lawlibrary.jp/pdf/z18817009-00-071451837_tkc.pdf）がある。

⁶ 第177回国会参議院法務委員会「情報処理の高度化等に対応するための刑法等の一部を改正する法律案に対する附帯決議」（平成23年6月16日）参照。

不正指令電磁的記録関連罪における保護法益は、電子計算機のプログラムに対する社会一般の信頼という社会的法益であるとされ⁷、具体的には、電子計算機のプログラムが反意図的な動作ないし不動作を惹起する不正な指令を与えるものではないということについての社会一般の者の信頼であるとされる。

こうした保護法益理解をもとに、「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」とは、当該プログラム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、その機能につき一般に認識すべきとされるところの使用者の意図に反する動作ないし不動作を惹起するものであることをいうとされる⁸（以下、この要件を反意図的動作の要件という）。したがって、当該プログラムが実行される局面において、一般的な使用者が当該プログラムの惹起する動作ないし不動作について認識していると認められる場合には、反意図的動作の要件を満たさないということになる。

次に、「不正な」とは、社会的に許容し得ないものであることをいうとされ⁹、反意図的動作の要件を満たすプログラムの中で例外的に保護法益を侵害しないと解されるものを除外するための要件として付加されている。たとえば、ソフトウェア開発会社が自社の提供するソフトウェアの不具合修正プログラム（パッチ・プログラム）を、ソフトウェアのユーザーに無断でそのコンピュータにインストールさせたという場合には、当該プログラムは反意図的動作の要件を満たすものの、「不正な」ものではないとされる。

後述のように、本判決も、基本的には、以上のような一般的な理解を踏襲したものと解される。

しかしながら、以上のような立案担当者の解説を基礎とする一般的な理解は、少なくとも現在においては大きな問題を含んでいるといわざるを得ない。その

⁷ 大塚仁ほか（編）『大コンメンタール刑法 第8巻』（青林書院、第3版、2014年）341頁〔吉田雅之〕、杉山徳明＝吉田雅之「『情報処理の高度化等に対応するための刑法等の一部を改正する法律』について（上）」曹時64巻4号（2012年）66頁、西田典之（橋爪隆補訂）『刑法各論』（弘文堂、第7版、2019年）412-413頁。

⁸ 大塚ほか（編）・前掲注（7）344-345頁〔吉田〕。

⁹ 今井猛嘉「実体法の観点から（特集・情報処理の高度化等に対処するための刑法等の改正）」ジュリ1431号（2011年）67頁、大塚ほか（編）・前掲注（7）346頁〔吉田〕、杉山＝吉田・前掲注（7）72頁、西田・前掲注（7）413頁。

第一の理由は、現在では反意図的動作の要件を満たし得るプログラムは無数に存在しており、一般のユーザーもごく日常的にそうしたプログラムに接しているということである。特に、トラッキングを目的としたプログラムや広告プログラムは非常に多様化しており、一般のユーザーがその動作をおよそ認識し得ないようなものも存在している。立案担当者はおそらく、「通常、インターネットの利用に随伴するものであることに鑑みると、そのようなものとして一般に認識すべきと考えられる」として反意図的動作の要件を満たさないと考えていたものと思われる^{9a}が、上述のようなプログラムのすべてについてそのような説明するのは無理がある。そこで、一般に不正指令電磁的記録には該当しないと考えられている無数のプログラムが不正指令電磁的記録の概念に含まれないような解釈として、反意図的動作の要件における一般的な使用者のリテラシーを非常に高く想定するという方向性があり得るが、それではもはや社会一般の者の信頼を保護法益とする不正指令電磁的記録関連罪の前提と乖離すると思われる。第二の理由は、現在の一般的な理解によれば、革新的なプログラムが悉く反意図的動作の要件を満たすことになりかねないということである。革新的なプログラムは、当然のことながら従来の常識からしてその動作内容が不明であり、反意図的動作の要件が充足され得ることから、そうしたプログラムを客体から除外するためには、不正性を否定するしかないことになるのである。

そうであるとすれば、非常に多くのプログラムの客体性が「社会的に許容され得るかどうか」という高度に開かれた基準によって判断される不正性の要件によって決定的に左右されることになってしまい、結果として、反意図的動作と不正性といういずれも処罰範囲を限定する機能の乏しい要件によって不正指令電磁的記録概念が形成されることになる。これにより、不正指令電磁的記録関連罪の運用が恣意的なものとなり、ひいてはプログラムの開発者や利用者にとって萎縮的な作用を及ぼすことにもなりかねない。したがって、不正指令電磁的記録概念をめぐる妥当かつ明確な基準の再構成が喫緊の課題であるように思われる。

(3) 立法経緯とそれに基づく制限的解釈

^{9a} 杉山＝吉田・前掲注（7）71頁参照。

不正指令電磁的記録をめぐる解釈を再考するにあたって大きな示唆を与えるのは、不正指令電磁的記録関連罪の立法経緯である。そもそも、不正指令電磁的記録関連罪は、サイバー犯罪条約（以下、条約という）の国内担保法としての役割を担っている¹⁰ものであり、具体的には、条約6条1項（a）（i）を担保するものである^{11・12}。したがって、不正指令電磁的記録関連罪が条約6条1項（a）（i）を念頭に置いて作成されたということは明らかである。そこで、条約6条1項（a）（i）に目を転じてみると、そこでは予備罪的な構成が採用さ

¹⁰ 今井・前掲注（9）66頁、鎮目征樹「ソフトウェアの無断インストールと不正指令電磁的記録に関する罪」研修792号（2014年）3頁、杉山＝吉田・前掲注（7）67頁注3。

¹¹ 条約6条1項（a）（i）による加盟国の犯罪化義務をめぐるのは、vgl. *Kai Cornelius*, Zur Strafbarkeit des Anbietens von Hackertools, CR 2007, S. 683 f.; *Martin Daxecker*, in: Otto Triffterer et al. (Hrsg.), Salzburger Kommentar zum Strafgesetzbuch, 26. Lfg., 2012, § 126c Rn. 1 ff.; *Marco Gercke*, Analyse des Umsetzungsbedarfs der Cybercrime Konvention – Teil 1: Umsetzung im Bereich des materiellen Strafrechts, MMR 2004, S. 731; *Dieter Kugelman*, Die „Cyber-Crime“ Konvention des Europarates, DuD 2001, S. 217; *Andreas Popp*, § 202c StGB und der neue Typus des europäischen »Software-Delikts«, GA 2008, S. 376 f.; *Fernando Sanchez-Hermosilla*, Neues Strafrecht für den Kampf gegen Computerkriminalität – Konvention des Europarates und neuer Rahmenbeschluss des Europäischen Union im Vergleich mit dem deutschen Strafrecht, CR 2003, S. 775 f.; *Irini E. Vassilaki*, Das 41. StrÄndG – Die neuen strafrechtlichen Regelungen und ihre Wirkung auf die Praxis, CR 2008, S. 135; Bundestag Drucksache 16/3656 (zit.: BT-Drs. 16/3656), S. 8; Erläuternde Bemerkung zur Strafrechtsänderungsgesetz 2002, 1166 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXI. GP (zit.: EBRV 2002), S. 29; Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010 (zit.: Botschaft 2010), S. 4707 ff.

¹² もっとも、条約6条1項（a）（i）は、「第2条から前条までの規定に従って定められる犯罪を主として行うために設計され又は改造された装置（コンピュータ・プログラムを含む。）」と規定しており、わが国の不正指令電磁的記録関連罪は、このうちプログラムに関する行為のみを対象としている。プログラムを除く「装置（device）」については、わが国は留保している状況である。

れ、それにより規制対象となるプログラムの動作内容が明確に限定されていることがわかる¹³。しかしながら、これに対してわが国における不正指令電磁的記録関連罪では予備罪的な構成が採用されていない¹⁴。この点を形式的に理解する限り、わが国の不正指令電磁的記録関連罪は、ある特定の犯罪類型の予備罪として構成されていないのであるから、不正指令電磁的記録概念は条約6条1項(a)(i)が予定しているプログラムの概念よりも大幅に拡張されているという理解も不可能ではないということになる。そこで、わが国の不正指令電磁的記録関連罪がなぜ予備罪的な構成を採用しなかったのかが重要な点である。

条約6条1項(a)(i)では、条約2条乃至5条の犯罪を(主として)行うために設計または改造されたプログラム等が客体として規定されている。条約2条の犯罪は違法アクセス(illegal access)、条約3条の犯罪は違法傍受(illegal interception)、条約4条の犯罪はデータ妨害(data interference)、条約5条の犯罪はシステム妨害(system interference)である。わが国における条約2条乃至5条の担保状況(マルウェア関係)であるが、条約2条に関しては、不正

¹³ 条約6条1項(a)(i)を担保する諸外国の規定もそのようなかたちとなっている。たとえば、ドイツ刑法202c条1項2号(„Computerprogramme, deren Zweck die Begehung einer solchen Tat [= Straftat nach § 202a oder § 202b] ist“)・303a条3項・303b条5項、オーストリア刑法126c条1項1号(„ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a), einer Verletzung des Telekommunikationsgeheimnisses (§ 119), eines missbräuchlichen Abfangens von Daten (§ 119a), einer Datenbeschädigung (§ 126a), einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) geschaffen oder adaptiert worden ist“)、スイス刑法143条の2第2項(«Passwörter, Programme oder andere Daten, von denen er weiss oder annehmen muss, dass sie zur Begehung einer strafbaren Handlung gemäss Absatz 1 verwendet werden sollen»)・144条の2第2項、フランス刑法323-1条(«un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3»)参照。

¹⁴ この点についての批判的検討として、渡邊卓也『ネットワーク犯罪と刑法理論』(2018年)263-268頁。

アクセス禁止法によって¹⁵、条約3条に関しては、電気通信事業法、有線電気通信法および電波法によって¹⁶、条約4条に関しては、公用電磁的記録毀棄罪（刑法258条）、私用电磁的記録毀棄罪（同259条）および電磁的記録不正作出罪（同161条の2）によって、条約5条に関しては、電子計算機損壊等業務妨害罪（同234条の2）によって担保されているとされる。しかしながら、わが国の国内法規定によって捕捉される行為の領域は、条約2条乃至5条が予定している行為の領域よりも大幅に矮小化されているという点に留意する必要がある。まず、不正アクセス禁止法における不正アクセスの概念は、行為者自身が制限されている特定利用をし得る状態にさせる行為を前提としている¹⁷のに対して、条約2条は必ずしもそうした行為に限定する趣旨ではない。現に、条約2条を担保するドイツ刑法202a条（„sich Zugang verschaffen“）およびオーストリア刑法118a条（„sich Zugang verschaffen“）においては、他人のコンピュータ上のデータをコピーして送信させるプログラムをインストールさせる行為などが対象となると解されている¹⁸⁻¹⁹。また、条約4条は、あらゆるデータの消去や改竄等を捕捉するものであるのに対して、わが国においてこれを担保する国内法規定においては、公用電磁的記録および私用电磁的記録のいずれにも該当しない電磁

¹⁵ ただし、付加的要件の宣言（declaration）により、いわゆるスタンドアローン・コンピュータに対する不正アクセスは不可罰とされている（https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations?p_auth=usVUF9Yi（Declaration contained in a letter from the Consul General of Japan deposited with the instrument of acceptance on 3 July 2012）参照）。

¹⁶ 電気通信事業法179条、有線電気通信法14条、電波法109条以下参照。

¹⁷ 不正アクセス対策法制研究会（編著）『不正アクセス行為の禁止等に関する法律』（立花書房、第2版、2012年）64頁以下参照。

¹⁸ Siehe [Deutschland] *Jörg Eisele*, Computer- und Medienstrafrecht, 2013, 4. Kapitel Rn. 19; *Klaus Malek/Andreas Popp*, Strafsachen im Internet, 2. Aufl., 2015, Rn. 162; BT-Drs. 16/3656, S. 9; [Österreich] *Susanne Reindl-Krauskopf/Farsam Salimi/Martin Stricker*, IT-Strafrecht – Cyberdelikte und Ermittlungsbefugnisse, 2018, Rn. 2.18; *Clemens Thiele*, in: Otto Triffterer/Christian Rosbaud/Hubert Hinterhofer, Salzburger Kommentar zum Strafgesetzbuch, 15. Lfg., 2007, § 118a Rn. 35.

¹⁹ さらに、アメリカの諸州法においても“access”は非常に広く定義されている（カリフォルニア州刑法502条（b）（1）など参照）。

的記録の消去や改竄等は捕捉されていない²⁰。当局は、そうした行為については犯罪化義務がないとされる「軽微又は重要でない不正行為 (petty or insignificant misconduct)」²¹とみなしたようである²²。さらに、条約5条は、システムに対する重大な妨害を捕捉するものであるのに対して、わが国においてこれを担保する電子計算機損壊等業務妨害罪 (刑法234条の2) は、人の業務に使用されていない電子計算機が問題となる場合は捕捉し得ず、当局は、そうした場合には「重大な (serious)」妨害がないと解したようである²³。以上のように、条約2条乃至5条に関しては、それらに完全に対応し得るだけの処罰範囲を確保できないという事態があったとしても、あくまでも既存の規定によって担保するというのが、当局の徹底した方針であったといえよう。後述のように、この点が不正指令電磁的記録概念の特殊性に関係しているように思われる。

以上の点を踏まえ、条約6条1項(a)(i)を担保するために新設された不正指令電磁的記録関連罪における不正指令電磁的記録概念についての再検討を試みる。わが国の不正指令電磁的記録関連罪においては、条約6条1項(a)(i)のような予備罪的な構成が採用されておらず、それに伴い、特定の犯罪類型との関連性が規定されていない。立案担当者は、わが国における不正指令電磁的記録関連罪が条約6条1項(a)(i)と大幅に異なるかたちで規定された根拠として、予備罪的構成の場合には当罰性のあるプログラムが客体から外れてしまうことを挙げている²⁴。先述のように、わが国において条約2条乃至5条を

²⁰ 条約4条を担保するオーストリア刑法126a条においては、損害の結果が必要とされるものの、行為者が利用権限を有しないあらゆるデータの消去・改竄等が処罰対象とされている。

²¹ Siehe *Council of Europe*, Explanatory Report to the Convention on Cybercrime, ETS No. 185, Nr. 37: “The drafters of the Convention understood that Parties may exclude *petty or insignificant misconduct* from implementation of the offences defined in Articles 2-10.”

²² 佐伯仁志「サイバー犯罪条約への実体法上の対応」ダニエル・フット＝長谷部恭男 (編)『メディアと制度』(東京大学出版会、2005年) 93頁、山田利行「欧州評議会サイバー犯罪に関する条約 (仮称) の概要等」ジュリ1257号 (2003年) 30頁参照。

²³ 佐伯・前掲注 (22) 93頁、山田・前掲注 (22) 30頁。

²⁴ 杉山＝吉田・前掲注 (7) 66頁。

担保する既存の国内法規定による処罰範囲が、条約2条乃至5条の予定する処罰範囲よりも大幅に狭くなってしまったため、条約2条乃至5条を担保する既存の国内法規定の予備罪を創設するというかたちであれば、当罰性のあるプログラムが処罰対象から除外されてしまうという懸念があったのであり、このことこそが予備罪的構成が回避されたことの決定的な理由であるように思われる。具体的には、立案担当者は、個人情報流出させるプログラムやメールを勝手に送信するプログラム、権利・義務に関するものでない私電磁的記録を勝手に消去・改変するプログラムなどが不正指令電磁的記録の概念に含まれなくなってしまうという点を懸念していたようである²⁵が、まさに、条約2条乃至5条を担保する国内法規定の予備罪というかたちである限り、これらのプログラムは規制の対象外に置かれることとなってしまうのである。したがって、わが国の不正指令電磁的記録関連罪が予備罪的構成を採用しなかったのは、決して条約6条1項(a)(i)が予定するプログラムよりも広い範囲のプログラムを捕捉するためではないのである。むしろ、立法者は、(その当否はともかく)条約2条乃至5条の担保を既存の国内法規定によって達成するという方針を貫きつつも、少なくともプログラムに関しては、条約6条1項(a)(i)に匹敵する処罰範囲を備える犯罪類型群として不正指令電磁的記録関連罪を創設したものと考えられる。

以上のように考えれば、条文上明らかではないものの、わが国における不正指令電磁的記録概念においても、条約2条乃至5条において予定されている実害との結びつきが要求されると解するのが適切であろう。すなわち、わが国における不正指令電磁的記録関連罪は、実行しようとするプログラムが、使用者の意図に反して、条約2条乃至5条に相当する実害を惹起するような動作(不動作)に至らしめるべきものではないということについての社会一般の者の信頼を保護しているものと解される。したがって、原則的な客体性を基礎づけることとなる反意図的動作の要件が満たされるためには、一般的な使用者の意図に反して、条約2条乃至5条に相当する実害を惹起するような動作(不動作)に至らしめるものである必要があるということになろう^{26・27}。こうして再構成

²⁵ 杉山＝吉田・前掲注(7)66頁参照。

²⁶ 高木・前掲注(5)28頁は、「筆者の見解としては、『意図に反する動作』か否かの区別は、プログラムの使用目的によって判断されるものではなく、指令

された不正指令電磁的記録概念によれば、従来不正指令電磁的記録該当性が争いなく認められてきたプログラムについて不正指令電磁的記録該当性が難なく認められるとともに、不正指令電磁的記録該当性の判断基準が大幅に明確となるように思われる。

(4) 具体的帰結

以上のような理解に基づけば、具体的にどのような帰結が導かれることになるであろうか。以下では、コインハイブ事件において問題となったプログラムを中心に検討を加える。

(a) コインハイブ事件

コインハイブ事件において問題となったプログラムは、条約2条乃至5条に相当する事態を惹起するものとはいえないがゆえに、明らかに反意図的動作の要件を満たさないことになる^{28,29}。すなわち、当該プログラムに関しては、条約

の挙動のみによって判断されるべきものとする。ワームや自己増殖型の典型的なウイルスだけでなく、情報を盗むものや、悪質な書込みを自動的に行うといったものも、指令の挙動のみに基づいて『意図に反する動作』をさせるものということができる」として、指令の挙動自体が一般的な使用者の意図に反するか否かを判断すべきとの見解を示している。反意図的動作の要件によって客体の範囲を制限しようとする点は本稿の立場と軌を一にするが、本稿は、指令の挙動自体が一般的な使用者の意図に反するとしても、条約2条乃至5条に相当する実害を惹起するような動作（不動作）に至らしめるものでないのであれば、なおも反意図的動作の要件の充足は否定され则认为。

²⁷ これに対して、石井徹哉「サイバー犯罪と刑法上の課題」犯非168号（2011年）67頁は、「不正か否かの判断にあたっては、動作内容の実質的な考察が必要となる。この実質的考慮を担うのが、情報セキュリティの侵害の有無である」とし、不正性の要件によって客体の範囲の制限を試みる。

²⁸ 高木・前掲注（5）28頁も、コインハイブ事件において問題となったプログラムは反意図的動作の要件を満たさないとする。

²⁹ なお、ドイツにおいては既に、ウェブサイト閲覧者に無断でそのコンピュータにマイニングを実行させるプログラムをめぐる行為の可罰性について論じられており、そうしたプログラムの利用は不可罰と解されていることが注目され

4条1項および条約5条に相当する実害を惹起するような動作に至らしめるべきものといえるかが問題となり得るが、まず、当該プログラムは、ウェブサイト閲覧中にブラウザを通じてマイニングの指令を与えるものにすぎず、決して閲覧者のコンピュータ上のデータを変更するなどの指令を与えるものではないことから、条約4条1項に相当する実害を惹起するものとはいえない。このことは、本判決における、「その影響はa閲覧中に限定され、aの閲覧を終了すれば、本件マイニングも（裏で持続することなく）終了する」という点によって基礎づけられることになる。また、当該プログラムは、閲覧者のコンピュータにある程度の影響を及ぼすものの、本判決も指摘しているように、その影響の程度は通常の使用に支障を来たすようなものであるとは到底いえないことから、条約5条に相当する実害を惹起するものともいえない³⁰。このことは、本判決における、「本件プログラムコードにより本件マイニングが実行されると、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プ

る（vgl. *Dieter Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl., 2018, Rn. 884: „Nicht mehr eindeutig greifbar sind die Fälle, wo beim Surfen oder Streaming quasi beiläufig Rechenleistung von Server gegen den Client abgegriffen wird, um nebenbei das Mining zu betreiben.“）。

³⁰ なお、条約5条は、システムの機能に対する妨害が重大（serious）であることを要求しており、この基準の決定は締約国に委ねられている（*Council of Europe*, a. a. O. (Fn. 21), Nr. 67）。この重大性につき、ドイツ刑法303b条やオーストリア刑法126b条のような規定をもたないわが国においては、さしあたり Explanatory Report の方針に依拠して考えるべきであろう。この点、Explanatory Report は、システムの所有者等におけるシステムの利用可能性または他のシステムとの通信可能性に対し著しい有害な影響を与えるような形式、サイズまたは頻度でのデータ送信が「重大」であるとして、DoS 攻撃を指令するプログラムやシステム操作を不可能にしましたは著しく遅延させるプログラム、メールボムを指令するプログラムを例示している（*Council of Europe*, a. a. O. (Fn. 21), Nr. 67）。したがって、現状としては、あるプログラムが条約5条に相当する実害を惹起するものであるかの判断は、Explanatory Report における基準に照らして行うべきであろう。もっとも、不正指令電磁的記録該当性が問題となる多くのプログラムは、条約2条または条約4条1項に相当する実害を惹起するものと認められるように思われる（vgl. EBRV 2002, S. 28; Botschaft 2010, S. 4707）。

ログラム等の場合と大きく変わることがないものとうかがわれる」という点によって基礎づけられることになる。

これに対して、本判決は、反意図的動作の要件に関しては立案担当者の解説を基礎とする一般的な理解を忠実に踏襲しつつ、不正性の要件の判断の中で様々な事情を考慮要素とするというアプローチを採用している。当該プログラムにつき不正指令電磁的記録該当性を肯定することに対して非常に慎重な姿勢を見せたという意味においては、評価に値しよう。しかしながら、繰り返し述べているように、反意図的動作の要件は、それが満たされれば客体性を原則的に基礎づけるという性格のものであり、ここで何らかの制御弁を設けない限り、極めて多数のプログラムの客体性の有無が不正性の判断に委ねられることとなる。そして、当然のことながら、本判決のように不正性の判断にあたって様々なファクターを考慮することは、不正性が否定される方向のみならず、不正性が肯定される方向にも傾き得る。したがって、本判決のようなかたちで不正性を重視するアプローチは、あまりにも判断の安定性を欠くこととなり、妥当とはいえないように思われる。

(b) その他のプログラムの不正指令電磁的記録該当性について

なお、本稿の立場からは、立案過程において予備罪の構成を採用した場合に不正指令電磁的記録に該当しないことになってしまうとの懸念がなされていたプログラムについても、不正指令電磁的記録該当性は基本的に肯定されることになる。たとえば、個人情報情報を漏洩させるプログラムは、少なくとも条約2条に相当する実害を惹起し得るものであることから反意図的動作の要件の充足が肯定されることになる。また、電子メールを勝手に送信するプログラムは、悪意のないソフトウェアであるかのように装ってインストールさせるようなものであれば条約4条1項に相当する実害を惹起し得るものであるし、勝手に送信する電子メールにコンピュータ内のデータを添付させるなどのようなものであれば条約2条に相当する実害を惹起し得るものであることから、基本的に反意図的動作の要件の充足が肯定されることになる。さらに、権利・義務に関するものでない私電磁的記録を勝手に消去・改変するウイルスは、明らかに条約4条1項に相当する実害を惹起し得るものであることから、反意図的動作の要件の充足が肯定されることになる。

近時注目を集めた無限アラート³¹については、報道の通り、ブラウザを閉じることによりその動作が終了するものであれば、反意図的動作の要件を満たさないということになろう。すなわち、コインハイブ事件において問題となったプログラムと同様に、ブラウザを通じた指令にすぎないことから、コンピュータ上のプログラムに変更を加えていない上に、ブラウザを終了させるのみでその動作が終了するものである以上、システムに対する重大な妨害を惹起し得るとまではいえない³²ため、反意図的動作の要件が満たされるとは考えにくいからである。

さらに、本稿の立場からすれば、不正指令電磁的記録該当性を肯定した従来の各種裁判例の結論は、妥当なものと解される³³（仙台地判平成30・7・2LEX/DB25560905については次項において言及する）。

①京都地判平成24・7・3LEX/DB25482154は、アダルト動画サイトにおいて「動画再生」と表示されたボタン画像をクリックした者のコンピュータの画面上に、マウス操作による移動や最小化ができず、閉鎖しようとしても数秒後に再表示され、かつコンピュータを再起動しても再表示される機能を有した、同サイトの有料会員登録が完了した旨および同サイトの閲覧料金を支払うまでそのウィンドウが消えない旨などを半裸の女性像や卑わいな文言と共に表示するウィンドウを常時表示させるプログラムにつき不正指令電磁的記録該当性が肯定された事例である（供用罪成立）。当該プログラムは、コンピュータを再起動しても機能し続けるものであり、一般的なユーザーの意図に反して、コンピュータ上のデータの変更（alteration; Veränderung）という実害に至らしめるものといえることから、反意図的動作の要件を充足することになる³⁴。

②千葉地判平成25・11・8裁判所ウェブサイトは、Android OSが稼働する

³¹ https://www.bengo4.com/c_23/n_9333/（弁護士ドットコム『『無限アラート』で女子中学生を補導、『リンク貼り付け』で摘発をどう考えるか』（2019年3月7日））、https://www.bengo4.com/c_23/n_9697/（弁護士ドットコム『『アラートループ』で書類送検の男性2人、不起訴処分 弁護士『検察はお茶を濁した』』（2019年5月29日））など参照。

³² システム妨害の重大性をめぐっては、前掲注（30）参照。

³³ いずれについても、不正性が否定されることはないということを前提とする。

³⁴ 名古屋地岡崎支判平成29・9・22Westlaw/DB2017WLJPCA09226001も同様である。

電子計算機に記録された電話帳データをユーザーの意図に基づかずに所定のサーバコンピュータに送信させるプログラムにつき不正指令電磁的記録該性が肯定された事例である（保管・供用罪成立）³⁵。当該プログラムは、ユーザーの意図に基づかずに携帯電話上のデータを行為者が支配するサーバコンピュータに送信させるものであり、少なくとも、一般的なユーザーの意図に反して、条約2条に相当する実害に至らしめるものであるから、反意図的動作の要件を充足することになる。

③東京地判平成27・2・4LEX/DB25505940は、コンピュータ使用者が認識できない状態で自動的にインターネット掲示板に接続し同掲示板に書き込まれた指令を参照・実行する機能等を有し、時間計測ほか4種類のソフトウェアに偽装した不正プログラム等を生成する機能を有するプログラムにつき不正指令電磁的記録該性が肯定された事例である（供用罪成立）。当該プログラムは、一般のソフトウェアに偽装し、真実はいわゆる代理投稿をさせるものであるから、一般的なユーザーの意図に反して、コンピュータ上のデータに変更を加えるものである。したがって、当該プログラムも反意図的動作の要件をも充足することになる。

④広島地判平成27・12・7LEX/DB25542007は、インターネット回線を通じて携帯電話機の通話履歴およびSMS履歴の取得等の指令を与えるプログラムにつき不正指令電磁的記録該性が肯定された事例である。当該プログラムは、被告人の手によってその機能を秘して他人の携帯電話機にインストールされたものであり、ユーザーの意図しないかたちで通話履歴やSMS履歴の取得を行うものであるから、一般的なユーザーの意図に反して、条約2条に相当する実害を惹起するものであり、反意図的動作の要件が充足されることになる。

⑤東京地判平成29・4・27裁判所ウェブサイト³⁶は、インターネット接続されたコンピュータ内で起動すると自動的にインターネットを介して行為者が使用するコンピュータとの通信を開始させるとともにIPアドレス情報等を同コンピュータに通知する機能および同コンピュータでの操作によって起動場所であるコンピュータ内の電磁的情報を検索して行為者が使用するコンピュータに

³⁵ こうしたスパイウェアをめぐることは、vgl. *Kochheim*, a. a. O. (Fn. 29), Rn. 865 ff., 886; *Annette Marberth-Kubicki*, Internet und Strafrecht, DRiZ 2007, S. 214.

³⁶ 本件の控訴審判決として、東京高判平成31・3・28LEX/DB25563539がある。

送信させる機能等を有するプログラムにつき不正指令電磁的記録該当性が肯定された事例である（供用罪成立）。まず、当該プログラムは、「ご注文決済のお知らせ」と題する電子メールに添付されたものであり、特に問題のないメールであると誤信してメールを開封した者のコンピュータ上のデータに変更を加えるものであるから、一般的なユーザーの意図に反して、条約4条1項に相当する実害を惹起するものであるという意味において反意図的動作の要件が充足されることになる。さらに、当該プログラムは、起動場所であるコンピュータ内の電磁的情報を検索することを可能にするものであり、一般的なユーザーの意図に反して、条約2条に相当する実害を惹起するものでもあるから、この意味においても反意図的動作の要件が充足されることになる。

⑥徳島地判平成30・12・21LLI/DBL07351231は、インターネット回線を通じて携帯電話機の位置情報を取得させ、携帯電話機の位置情報等をインターネット回線を通じて特定のサーバコンピュータに送信させるプログラムにつき不正指令電磁的記録該当性が肯定された事例である（作成・供用罪成立）。当該プログラムは、被告人の手によって同意なく他人の携帯電話機にインストールされたわけであるが、その内容が、携帯電話機の位置情報等を取得させて特定のサーバコンピュータに送信させるものであることから、一般的なユーザーの意図に反して、条約2条に相当する実害を惹起するものであり、反意図的動作の要件が充足されることになる³⁷。

⑦大阪地判平成31・1・17裁判所ウェブサイトは、あるウェブサイトに接続すると、接続者の意思に反して、指定された攻撃対象のウェブサイト指定の間隔で連続して多数回アクセスさせて、当該サイトのサーバに負荷をかけるプログラムが問題となった事例である（作成罪成立）。当該プログラムは、所定のウェブページに接続した者の電子計算機に、攻撃対象のウェブサイト多数回接続する指令を与える攻撃用スクリプトである。こうした指令は、攻撃対象サイトのサーバ上のデータへのアクセスを不可能にし得るものであるから、一般的なユーザーの意図に反して、DoS (Denial of System) 攻撃などが含まれ得

³⁷ ただし、位置情報等取得させるプログラムの供用と位置情報等送信させるプログラムの作成・供用を区別して処罰の対象としている点については、なお検討の余地がある。

る条約4条1項におけるデータの隠蔽 (suppression; Unterdrücken)³⁸という実害に至らしめるものであり、反意図的動作の要件が満たされることになる。

⑧横浜地判平成31・4・16LLI/DBL07450551は、あるOSが稼働する電子計算機である携帯電話機を用いて実行した際に、実行者の意図に基づかず同携帯電話機に記録されたLINEメッセージ、通話履歴、SMSメッセージ、電話帳データ、端末位置情報、動画・静止画等をインターネット回線を通じて特定のサーバコンピュータに送信させるプログラムにつき不正指令電磁的記録該当性が肯定された事例である(作成罪成立)。当該プログラムは、判例②と同様に、ユーザーの意図に基づかずに携帯電話上のデータを行為者が支配するサーバコンピュータに送信させるものであり、一般的なユーザーに反して、条約2条にあるところの違法アクセスに相当する実害に至らしめるものであるから、反意図的動作の要件をも充足することになる。

(5) 「指令を与える電磁的記録」の捉え方について

コインハイブ事件において問題となったプログラムについて不正性が否定されるということは、他人に無断でそのコンピュータにマイニングを実行させるプログラム全般について反意図的動作の要件が充足されないということを意味するわけではない。現に、そうしたプログラムにつき不正指令電磁的記録供用罪の成立が認められた裁判例として、仙台地判平成30・7・2LEX/DB25560905(以下、仙台地裁判決という)が登場しているが、この事案は、実際にはコンピュータ使用者の意図に反してそのコンピュータにマイニングを実行させるプログラムであるにもかかわらず、他用途のプログラムを装って他人のコン

³⁸ Vgl. *Council of Europe*, a. a. O. (Fn. 21), Nr. 61: “Suppressing of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored.”; auch *Eisele*, a. a. O. (Fn. 18), 4. Kapitel Rn. 73 f.; *Reindl-Krauskopf/Salimi/Stricker*, a. a. O. (Fn. 18), Rn. 2.148 f. なお、こうした場合、スイスにおいては刑法144条の2第1項における利用を不可能にする行為(Unbrauchbarmachen)として捕捉されることになる(vgl. *Philippe Weissenberger*, in: Marcel Alexander Niggli/Hans Wiprächtiger (Hrsg.), *Basler Kommentar, Strafrecht II*, 4. Aufl., 2019, Art. 144^{bis} Rn. 33 ff.)。

コンピュータに当該プログラムをインストールさせたというものであった³⁹。先述の通り、無断マイニングを内容とするプログラム自体は、必ずしも反意図的動作の要件を満たさない。したがって、むしろこの事案において重要なのは、無断マイニングを実行するプログラムであるにもかかわらずそうでないプログラムに仮託してそれをインストールさせる機構全体としてのプログラムである。つまり、使用者の操作（クリック操作やタップ操作等）により、使用者において無断マイニングを実行するプログラムがインストールされることが認識できないようなかたちでそのインストールがなされるという機構を形成する全体としてのプログラムこそが、不正指令電磁的記録に該当することになる。よって、仙台地裁判決の事案においては、「他のプログラムに仮託して無断マイニングを実行するプログラムをインストールさせる」という内容のプログラムの作成・供用が問題となったのであり、まさにこうしたプログラムは、一般的な使用者の意図に反して条約4条1項に相当する実害を惹起し得るものといえることから、不正指令電磁的記録該当性が肯定されるのである^{40・41}。

以上のように、コンピュータ使用者に無断でマイニングを実行するという点

³⁹ 具体的には、マイニングを実行するプログラム「cpuminer-sse2.exe」を実行するプログラム「MapleTools.exe」を含む圧縮ファイルである「MapleTools.zip」をダウンロードさせ実行の用に供したようである（D1-Law/DB28263173参照）。高木・前掲注（5）20頁注8も参照。

⁴⁰ 「マルウェアを用いてビットコインをマイニングさせる行為は、不正指令電磁的記録供用罪（一六八条の二第二項）に該当する」とするものとして、仲道祐樹「他人のコンピューターを利用したビットコインのマイニング——可罰性と収奪の可否」判時2379号（2018年）127頁。

⁴¹ これに対して、本稿の立場からは、使用者が通常認識できないかたちでマイニングを実行するプログラムを、他人の電子計算機に密かに手でインストールする行為は、不正指令電磁的記録供用罪に該当しないことになる。なぜなら、マイニングを実行するプログラムは、それ自体としては反意図的動作の要件を満たさない上、それを意図しないかたちでインストールさせるというプログラムを伴っていないからである。こうした帰結は、条約4条1項の担保を限定的なものとしつつ、条約6条1項（a）（i）に匹敵する処罰範囲を確保した不正指令電磁的記録関連罪を創設したことに伴う、必然的なものである。上記の行為は、わが国において広くデータの変更・改竄等を処罰対象とした場合にはじめて可罰的となる。

にのみ着目したかたちで理解されるプログラムは、必ずしも反意図的動作の要件を満たさないと考えられるものの、そのようなプログラムを実行の用に供するための機構を形成するプログラムを含めて理解される全体としてのプログラムが不正指令電磁的記録に該当する場合はあり得る。このことは、通常であれば不正指令電磁的記録に該当しないソフトウェアを他人に無断でそのコンピュータにインストールさせた場合に不正指令電磁的記録供用罪が成立し得るのと同様である⁴²。不正指令電磁的記録該当性を判断する場合には、核となるプログラム自体に着目するのではなく、それを実行の用に供するための機構を形成するプログラムを含めた上で、反意図的動作および不正性を満たすような「指令を与える電磁的記録」に該当するかを見極める必要があろう。

(6) おわりに

不正指令電磁的記録関連罪に対しては、制定前より、プログラムの開発や利用を委縮させるのではないかと懸念が向けられていたが、コインハイブ事件は、まさにそうした懸念が現実化した事例であったといえよう。わが国の不正指令電磁的記録関連罪は、(その当否はともかく)わが国における立法政策として、サイバー犯罪条約のような予備罪な構成を採用することはできないとの判断に基づいて、サイバー犯罪条約とは大幅に異なる独自の規定として構成されたのであるが、この規定の相違は、予備罪な構成を採用しないかたちでありながらも(マルウェアに関しては)サイバー犯罪条約に匹敵する処罰範囲を確保するためのものであるということが明らかとなった。そうであるとすれば、不正指令電磁的記録の解釈においては、本稿が示したように、サイバー犯罪条約の趣旨をも考慮したかたちでの解釈が要請される⁴³のであり、そうすることによって、どのようなプログラムが不正指令電磁的記録に該当するかが明確となり、かつ、妥当な結論が担保されることになろう。

⁴² この問題についての詳細な検討として、鎮目・前掲注(10) 3頁以下がある。

⁴³ Vgl. *Eisele*, a. a. O. (Fn. 18), 4. Kapitel Rn. 1: „konventionskonform“ (zu § 202a dStGB); *Daniel Schuh*, Computerstrafrecht im Rechtsvergleich – Deutschland, Österreich, Schweiz, 2012, S. 38: „völkerrechtskonform“.

【補遺】

脱稿後の2020年2月7日、コインハイブ事件につき控訴審・東京高裁は、原判決を破棄し有罪とする判断を示した（日本経済新聞2020年2月8日朝刊37頁）。控訴審判決の検討は他日を期するほかないが、少なくとも同判決においては、不正指令電磁的記録関連罪の趣旨や、当該プログラムを不正指令電磁的記録とすることによりプログラムの開発者や利用者に対し過度に委縮効果を与えかねないということが十分に踏まえられていないように思われる。最高裁においてはこれらを十分に踏まえた検討がなされることに期待したい。