論　説

いわゆる「デュアル・ユース・ツール」の刑事的規制について(中)

石　井　徹　哉

第２節　ドイツにおけるツール開発行為の刑事規制(承前)

第３款　202条ｃ１項２号とデュアル・ユース・ツール(承前)

第２項　学説の対応

１　以上のように、連邦憲法裁判所の202条ｃに関する解釈は、立法者の趣旨に依拠しつつ、202条ｃの目的を客観化して理解するアプローチをとる。立法者は、「(202条ａまたは202条ｂの)行為の遂行がその目的

であるプログラム」という文言によって過度の犯罪化を防げるものとする[49]。この場合、プログラムの犯罪遂行の目的を客観化すべきであるとするが、コンピュータ犯罪の遂行に排他的に特化されている必要はなく、202条aまたは202条bの犯罪行為の予備の目的にも役立つ場合であっても十分とされている。しかし、他方で、一般的にインストールされうるプログラミングツールおよびアプリケーションプログラムは、202条cに該当しないものとされる[50]。

しかしながら、このような立法者の説明については、明確な法律上の根拠があるとはいえないと批判される[51]。実際問題として、情報システムの管理者または情報セキュリティに携わる者が通常使用するツール、ソフトウエアは、デュアルユースの性格を有することが多い。それだけでなく、憲法裁判所への申立人にみられるように、一般的に有害なツール(ハッカーツール)としてしか位置づけられないプログラムですら、セキュリティ検査を実施する場合には、使用されるのであり、不正行為者ないし犯罪者が使用することが想定されるツールによる検査こそが必須ともいえるとされる[52]。したがって、202条cの解釈、とりわけ「目的」の特定を客観化[53]することによって、これらの場合をどのように除外可

---

49 この限定は、ドイツ刑法263条a 3項と同様のものであるが、この条項についても、犯罪の限定として有効だとはいえないとの批判がある。Duttge Vorbereitung eines Computerbetruges: Auf dem Weg zu einem „grenzenlosen" Strafrecht, Festschrift für Ulrich Weber, 2004, S. 285ff., 301.; vgl. Fischer, a.a.O.(Anm. 15), §263a Rnd. 32. さらに、ドイツの道路交通法22条b 1項3号(vgl. BverG NJW 2006, 2318.)、著作権法95条a、108条bの文言についても同様の問題があるとされる(Hilgendorf, a.a.O.(Anm. 9), §202c Rdn. 13.)。

50 BT-Drucks 16/3656, S. 12, ferner S. 20, 33f.; vgl. Fischer, a.a.O.(Anm. 15), §202c Rnd. 5.

51 Vassilaki, a.a.O.(Anm. 29), S. 135.

52 Hilgendorf, a.a.O.(Anm. 9), §202c Rdn. 14.

53 目的は、人間によって設定されるものであり、そのかぎりでつねに主観的なものであるから、目的を客観化することはあり得ないとの批判もある。Bosch, a.a.O.(Anm. 36), §202c Rdn. 3, 6.

能化ということが問題となる(54)。

2　連邦憲法裁判所は、この点について、客観化された目的を追求しようとする。このような考え方は、すでにコーネリウスの見解(55)にみられる。コーネリウスは、立法者の説明を根拠として、目的の要件を客観化すべきであるとする。そこで、まず、ソフトウエアが違法な目的に適しているかどうかを確定し、次に、客観化しうる基準によりソフトウエアが違法な目的に使用されるものといえるかどうかを検討するということで、目的の要件を判断すべきものとする。この際、判断の基準としては、作成者の頒布の構想および製品の普及のための努力(製品の告知、販売促進の宣伝、使用説明)が決定的な手がかりであるが、収益獲得の意図は重要でないとする。また、実際にどの使用の可能性に重点が置かれているのかということは、法的には基準とすべきでないとする。それは、新しい技術が発展する場合、実際の使用がどのように展開するのかは、かならずしも最初から明らかとはいないということを理由にしている(56)。これは、連邦憲法裁判所が、プログラム開発者の意図から出発しつつも、しかし、付随的に外部で確定可能なその意図の発現を要求するという解釈によって、考慮することができるとして、そのような外部への発現は、プログラムそれ自体の形態に存在していることもあるが、作成者の一義的に違法な使用を目標としている販売方針および宣伝にも存在しうるものとしているのと軌を一にしているといえる。

このような見解は、目的を客観化するとしつつも、その特定に際しては、必然的にプログラムの作成ないし著作者の意思へと遡ることになる(57)。202条ｃ１項２号の所為客体は、そこで指示されている「犯罪行

---

(54) Hilgendorf, a.a.O.（Anm. 9）, §202c Rdn. 15は、目的は、プログラムと継続的に結びついている特性ではないし、目的を設定する人間の主観と関連づけることなしに確定し得ないものであるのに、立法者がこのことを十分に考慮していないため、数多くの解釈が生じる契機を与えてしまったとする。

(55) Cornelius, Zur Strafbarkeit des Anbietens von Hackertools, CR 2007, S. 682ff, 685ff.

(56) Cornelius, a.a.O.（Anm. 55）, S. 687.

為を遂行するために投入するという意図をもって開発または修正した」[58]プログラムに限定されることとなる。この点において、連邦憲法裁判所の解釈は、客観的基準に主観的基準を結合し[59]、これにより可罰性の認められる範囲を限定しようとするものといえる[60]。このような客観的基準と主観的基準を結合することは、刑法上の違法を主観と客観の結合によって形成されるとする理解を前提するものであり、そうでない立場からは、体系的に一貫しない[61]ものとなる。

このように202条ｃを解釈すると、犯罪の意図をもって、客観的には犯罪遂行に適しているが、しかし、作成者によってはその目的に特定されていないプログラムを入手した場合、この立場からは、202条ｃ１項２号を適用できないことになってしまう。しかしながら、この場合に、202条ｃの処罰目的からみて、当罰性が欠如しているとはいえないであろう。また、作成者の意思へと遡及することは、いかにして作成目的を正確に確定するのかという問題が生じることになる[62]。

---

57 Hilgendorf, a.a.O.（Anm. 9），§202c Rdn. 19.

58 BVerfG CR2009, S. 675f.

59 そのほか、客観的な観点と主観的な観点を結びつけて目的要件を解釈しようとするものとして、Schultz, a.a.O.（Anm. 29）, S. 782. がある。シュルツは、当該プログラムにおいて、どのような使用の可能性が優勢であるかを決定的なものとすべきであるとしつつ、それが疑わしい場合には、著作者の心情によって判断しなければならないとする。しかし、適法にも違法にも同等に使用可能である場合、明確に決することはできず、結局、行為者ないしユーザの主観に依拠せざるを得なくなり、処罰範囲が著しく縮小する可能性が生じる。Vgl. Hilgendorf, a.a.O.（Anm. 9），§202c Rdn. 18.

60 Kudlich, VerfassungsmäBigkeit des Verbots von „Hacker-Tools", JA 2009, S. 739ff., 742. 見解が分かれている解釈について、はじめて「杭を打った」ものだとして、連邦憲法裁判所の見解を肯定的に評価する。

61 Bosch, a.a.O.（Anm. 36），§202c Rdn. 6. ボッシュは、客観的に不明確なメルクマールを主観的な目的設定によって憲法に適合するように限定するアプローチは、立法者が構成要件において社会的に相当な行動態様を限界づけるための十分に明確な基準を意識的に基礎づけていない場合には、否定されるべきであるとする。

62 Vgl. Hilgendorf, a.a.O.（Anm. 9），§202c Rdn. 19.

3　これに対して、202条cにいう「目的」をあくまで客観的に判断すべきであるとする見解がいくつか有力に主張されている。例えば、202条c 1項2号にいうプログラムと認めることができるのは、その本質的、第一次的目的が当該犯罪に使用する場合であるとする見解[63]がある。しかしながら、本質的目的、第一次的目的といっても、適法な目的にも違法な目的にも利用可能なプログラムについては、なんらの判断基準を示したものとはいえない。どのようにして本質的目的を見極めるのかを判断する基準をさらに示すべきであって、この見解は、問題の所在を言い換えたにすぎないものといえよう[64]。また、「本質的」などといった限定を附さず、問題となるプログラムに202条cで問題とされている予備行為をする客観的な可能性が存在するかどうかによって判断すべきとの見解もある。この見解によれば、同条1項2号にいう「目的」が、202条aまたは202条bの犯罪行為への客観的な適性と解釈するのと同じことになる。しかし、「目的」を149条1項1号における「適している(geeignet)」と規定されていることと同じことを解釈論によってとることになってしまい、解釈による立法ともいいうることになる[65]。また、犯罪行為への適性だけでは、同条により捕捉されるプログラムは、広範囲なものとなってしまう[66]。

202条1項2号の客体の特定については、あくまで客観的に判断しつつ、処罰範囲の限定を行為者の主観面に求める見解もある。まず、2号の客体は、その客観的な目的が202条aまたは202条bの所為の遂行であるプログラムであるとする。この場合、典型的な「ハッカーツール」が含まれるものであって、その客観的な機能によれば、原則として、他の目的に利用されるものであって、犯罪遂行のために投入することが濫用を意味することになるプログラムは、除外されるとする[67]。しかしなが

63　Schumann, Das 41. StrÄndG zur Bekämpfung der Computerkriminalität, NStZ 2007, S. 675ff., 678; ferner, Schönke/Schröder/Eisele, Strafgesetzbuch, 28. Aufl., 2010, §202c Rdn. 4

64　Vgl. Hilgendorf, a.a.O.（Anm. 9）, §202c Rnd. 16.

65　Hilgendorf, a.a.O.（Anm. 9）, §202c Rdn. 16.

66　Vgl. BVerfG CR2009, S. 675.

ら、他の目的にも利用できるが、濫用の可能性が高いプログラムならびにセキュリティ企業のテストプログラム、システム管理者のプログラム作成およびインターネットにおいて自由に入手できたり、コンピュータ雑誌の付録メディアに収録されている検査ツールについて、適用の余地があることとなる。そのため、よいソフトから有害なソフトを区別することができるように目的の特定を客観化することは、まったく可能ではなく、上述の場合について、処罰の限界づけは、もっぱら主観的要素ないしは故意によってのみ可能になるとする[68]。

問題を主観的要素の領域へ移すとしても、同条の故意を未必の故意で足りる[69]ものとし、超過的内心傾向を、将来の202条 a または202条 b の所為の遂行へと向けられていなければならないという限度でしか要求せず、この将来の所為の具体化は、抽象的危険犯であることを理由として、教唆犯および従犯の意味では、要求されないとする[70]ならば、ほとんど処罰範囲を限定することはできないであろう。202条 c が予備行為を犯罪化していることから、202条 a 等の同条で規定される犯罪の予備行為をする意思があったかどうかによって、処罰の限定をしようとする見解[71]もある。

しかしながら、自ら当該犯罪行為を遂行する場合はともかく、頒布目的等をもってプログラムを開発する場合には、そのプログラムを利用して犯罪を遂行するかどうかは、実際の行為者の意思に依拠するのであって、通常、故意を肯定することが困難であろう。結局、あるプログラム

---

(67) Fischer, a.al.O.（Anm. 15），§ 202c Rdn. 5. Ernst, Das neues Computerstrafrecht, NJW 2007, S. 2661ff., 2663. は、すでにその構造上の性質および態様からして違法な行為を遂行することに向けられていて、インターネットから広範囲に匿名でダウンロード可能なプログラムを特に対象としているとする。

(68) Fischer, a.al.O.（Anm. 15），§ 202c Rdn. 6.

(69) Schönke/Schröder/Eisele, a.a.O.（Anm. 63），§ 202c Rdn. 6 は、未必の故意で足りるとしつつも、これは、サイバー犯罪条約より過度に犯罪化することになるとする。

(70) Fischer, a.al.O.（Anm. 15），§ 202c Rdn. 8.

(71) Ernst, a.a.O.（Anm. 67），S. 2663f.

が所定の所為を遂行する目的を実際に有しているかどうかは、デュアル・ユース・ツールの場合、現にそれを使用する者の意思に依拠せざるをえないが、それを、202条ｃの主体の主観的要件としてプログラムの開発時に要求することは、現実的ではない。また、たしかに職業上セキュリティサービスを提供する者については、当該プログラムの違法な使用の可能性を有しておらず、その範囲にのみ提供する場合には、未必の故意は、否定される。しかし、より広範囲にプログラムを提供する場合には、故意を否定することは困難である[72]。

4　202条ｃ１項２号の客体と故意の要件をより抜本的に改めるべきことを主張する見解もある。ホルツナー[73]は、児童ポルノ(Kinderporngraphische Scriften)[74]の作成および所持の予備について、184条ｂ５項において「もっぱら適法な、職務上のまたは職業上の義務」を履行する場合に、構成要件に該当しない旨を定めていることを参照し、これを類推して、202条ｃ１項２号の適用範囲を制限すべきであるとする。そして、児童ポルノにおいては、法執行機関、鑑定人、弁護士および医師だけでなく、学問上の研究の委嘱および計画の充足も含まれることから、202条ｃにおいても同様に限定されることになる。しかしながら、このような限定をする根拠がまったく存在しないため、立法的な解決の提案でしかないともいえる。それでも、情報通信技術に係るプログラムについては、いわゆる職業的な専門家だけが適法に使用できるわけではないことを考慮するならば、このような限定によって、デュアル・ユース・ツールの開発に対する適切な解決をなし得るかははなはだ疑問である。

⑺② Hornung, CR 2009 677ff., 678.

⑺③ Holzner, Klarstellung strafrechtlicher Tatbestände durch den Gesetzgeber erforglich, ZRP 2009, S. 177f., 178.

⑺④ ドイツ刑法は、児童ポルノ(Kinderporngraphische Scriften)を14歳未満の者の性行為またはこれらのものに対する性行為を対象とするものと規定し(184条ｂ１項、176条)、14歳から18歳までの者に関する少年ポルノ(Jugendporngraphische Scriften)と区別して犯罪化している(184条ｃ)。後者は、2003年の児童の性的搾取および児童ポルノ撲滅のための欧州連合理事会の枠組決定に基づき立法されたものである(BGBl Ⅰ 2149)。

ヒルゲンドルフ(75)は、条文の文言を基礎とし、サイバー犯罪条約の趣旨に適合するようにとの立法者の意思にできるだけ近づけるためには、202条ｃ１条２号の客体としてのプログラムを認めることができるのは、①202条ａ、202条ｂ、303条ａまたは303条ｂの犯罪行為を遂行することに適しており、②行為者(すなわち、当該プログラムを作成しあるいは自己または第三者のために入手した人物)が、所為行為を実行するにあたって、上記の所為の予備をする目的を設定して行為し、③この目的設定が客観的に現出し、したがって客観的な基準にしたがって証明されうる場合であるとする。さらに、②の点については、未必の故意では足りず、直接的故意を要求する。この見解は、202条ｃ所定の犯罪の予備行為の目的を客観化して特定し、かつ、この客観化された目的について未必の故意では不十分であって、直接的故意が必要であるとすることにより、デュアル・ユース・ツールについて合理的な処罰範囲を画するものといえる。しかし、この見解も、やはり直接的故意を要求する根拠は、合理的な処罰範囲を画するという点にのみあり、条文上の根拠または理論的な根拠に乏しい。やはり、直接的故意に限定するためには、立法的解決が必要ではないかと解される。

第４款　小括

ドイツにおけるデュアル・ユース・ツールないしは有害なソフトウエアに関する議論は、次のような特徴がある。

まず、なんらかのソフトウエアを使用して202条ａ、303条ａまたは303条ｂなどの犯罪を実現した場合、その犯罪に使用されたツールを提供した者は、通常の共犯論の枠組みにしたがって処罰の可否を判断するということにある。この際、当該ツールの本来的な機能はどれかということに関する評価は重要ではなく、当該ツールの使用により犯罪が実現したことおよびそれに対する故意があることが決定的なものとされている。ここでは、デュアル・ユース・ツールかどうかということは、共犯の成否にとっては考慮されていない。

---

(75) Hilgendorf, a.a.O.（Anm. 9）, § 202c Rdn. 21.

次に、デュアル・ユース・ツールに関する議論は、もっぱら202条ｃの適用の可否をめぐってなされている。202条ｃが立法される前は、有害なプログラムの作成、保管または提供について、予備行為にすぎず、現に犯罪が遂行されない限り、処罰し得ないとされてきた。しかし、202条ｃによって、今度は、処罰範囲が過度に広がりすぎるとして問題となり、その議論の中心にデュアル・ユース・ツールが取り上げられている。もっとも、デュアルユースの概念は、それほど明確でなく、情報セキュリティを侵害する違法な使用にしか想定し得ないツールであっても、それがセキュリティテストに使用されることから、場合によって202条ｃの成立を否定すべきとの考え(76)もみられる。この点を鑑みると、202条ｃ１項２号の客体について、目的要件を客観化したとしても、それだけでは、相当広い範囲で処罰に値しない場合を含むことになってしまう可能性が高くなる。これを回避するには、ヒルゲンドルフが提案するように、主観面で限定せざるを得ず、直接的故意の場合にのみ犯罪の成立を認めるべきことになろう。

ドイツにおいて、デュアル・ユース・ツールの規制の問題を中心として202条ｃが解決困難な問題に直面したのは、結局、202条ａ、202条ｂ、303条ａおよび303条ｂの予備行為を、しかも他人予備をも含めて独立処罰しようとし、かつ、これを抽象的危険犯として位置づけたところにある。しかし、202条ａおよび202条ｂについては、未遂処罰規定がなく、正面から予備行為を構成するように202条ｃを起草できなかったところに解釈論的な問題を生じさせる根本的な原因があるものと考えられる。通常の予備罪の規定形式をもって条文を起草できたのであれば、問題は生じなかったか、より緩和された形になったであろうことが推測され

(76)　Höffinger, ZUM 2009, S. 751ff., 752. は、proof of concept（脆弱性をつくコードを実証するためのもの）やMetasploit Framework（ペネトレーションテストによるセキュリティ検証ツールの一つ）については、連邦憲法裁判所の枠組みにおいてもなお規制される可能性があるとする。さらに、未必の故意でたりるとすることで、セキュリティの専門家がエクスプロイットの公表を差し控え、いわゆるハッカーツールを封印して保管することになるとする。

る。すなわち、予備罪では、具体的な犯罪を遂行する目的が要件とされるのが通例であり、この目的要件によって、202条cにおける確定的故意と同様のものを犯罪の成立に要求することができるからである。抽象的危険犯として犯罪化する際に、予備罪としての特性を否定するために、203条a等の犯罪との関連づけを客観的に規定しようとしたところに、解釈論上の問題を生じさせている要因があるといえよう。いずれにしても、ドイツにおける202条cをめぐる議論は、予備罪的な構成をとるアプローチでは、適切な処罰範囲を条文上明確化することが困難であり、精緻な立法技術が必要とされることが示されている。

なお、202条cは、1項1号によって、いわゆるフィッシング行為を処罰することを可能にしている。不正アクセスをデータへの無権限のアクセスとし、これに対する予備的行為を規制するなかで、フィッシング行為の規制を可能にしている点については、参考に値すべきものである。

第3節　わが国におけるツール開発行為の刑事規制

第1款　不正指令電磁的記録に関する罪とデュアル・ユース・ツール

サイバー犯罪条約6条の規定の国内法における対応について、わが国は、不正指令電磁的記録に関する罪を新たに創設することでおこなった。この立法にあたって特徴的なことは、サイバー犯罪条約の文言に即した形ではなく、独自の規制形式を採用した。すなわち、「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」(平成24年法74号)において、不正指令電磁的記録に関する罪(刑法第2編第19章の2)が新設されたが、本罪は、偽造の罪の各章に続いて規定され、その保護法益が社会的信頼に関係づけられる社会的法益に対する罪としての位置づけられている。そのため、規制対象となる客体も、電子計算機の動作や不正アクセス行為と結びつけることなく規定されている。以下では、解釈論的な問題に若干言及しつつ、わが国おけるデュアル・ユース・ツールの刑事的規制との関連を検討する(77)。

第1項　不正指令電磁的記録に関する罪の保護法益・罪質

1　上述のように、不正指令電磁的記録に関する罪は、サイバー犯罪

条約６条に対応することを目的として起草された(78)。その内容は、以下の通りである。

（不正指令電磁的記録作成等）
第168条の２　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、３年以下の懲役又は50万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１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。
（不正指令電磁的記録取得等）
第168条の３　正当な理由がないのに、前条第１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、２年以下の懲役又は30万円以下の罰金に処する。

しかし、同条約６条において規定される形式（同助役における違法なアクセス（２条）、違法な傍受（３条）、データの妨害（４条）およびシステムの妨害（５条）に対応する罪の予備罪）をとらなかった。わが国の刑法でいえば、電子計算機損壊等業務妨害罪（刑法第234条の２第１項）や公電磁的記録ないし私電磁的記録毀棄罪（同法第258条、259条）等の予備罪として位置づけられていないし、またこれらに関連する処罰の早期化の形式をもとっ

(77)　以下、所管する法務省による本罪の位置づけや考え方等については、http://www.moj.go.jp/keiji1/keiji12_00025.html所掲の資料に依拠している。
(78)　サイバー犯罪条約との関係については、山口厚「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）15頁以下参照。

ていない。このことから、以下で検討するように、前節で概観したようなドイツにおける相応の処罰規定における解釈論的な問題ないし困難は、回避されることになる(79)。この点においては、法制度的に優れた面をもつものといえる(80)。

もっとも、わが国において予備罪的な構成ないし処罰の早期化としての構成が採用されなかったのは、サイバー犯罪条約に規定される不正アクセス、不正傍受、データ妨害、システム妨害に関する犯罪が、刑法典のみにおいて規定されているわけではなく、不正アクセス禁止法、電気通信事業法、電波法等の特別刑法に分散していることも影響しているように解される。さらに、不正アクセス禁止法は、電子計算機に対する不正アクセス行為のみを処罰の対象とし、毀棄罪や電子計算機損壊等業務妨害罪の対象となる行為も限定的なものといえ、これらの予備罪や処罰の早期化といった構成をとることが困難であったという事情もある(81)。もっともこれらの事情は、わが国においては、情報セキュリティの刑事的保護を十分におこなっていないことの裏返しであって、立法的課題がなお残るものといえよう(82)。

2　不正指令電磁的記録に関する罪は、犯罪化に際して、とりわけ起草当時社会的に問題とされるようになった立法事実に即して起草されたところに特徴がある。インターネットが社会的に普及することによって、専門的な知識を有する者だけでなく、ごく普通の一般の人たちの多くがネットを利用するようになり、インターネットを介して情報通信、

---

(79)　本罪の法案は、もともと2003年に提出されたものであり、ドイツ等諸外国の問題状況を反映したわけではないと思われるが、十分に熟慮されて準備されたものであるといえる。山口・前掲注(78)・16頁は、「条約上の義務を履行しつつも、条約が採用する形式・構成にしばられることなく、わが国に妥当する国内用として、可能な限り優れた法制を考案することが望まれる」とする。

(80)　予備行為を処罰する罪として構成し、処罰範囲の限定を図るほうが望ましいとするものとして、渡邊卓也「サイバー関係をめぐる刑法の一部改正」刑事法ジャーナル30号(2011年)27頁以下、29頁。

(81)　山口・前掲注(78)・16頁以下。さらに、処罰の早期化というアプローチ自体にも問題があることを指摘する(山口・前掲注(78)・17頁)。

情報処理が一定の社会的基盤となったが、これに比して、有害なプログラムにより、コンピュータを利用した情報処理、情報通信が阻害されることが顕著になってきたことである。これに加え、有害なプログラムの動作内容が、コンピュータのデータの破壊や動作の阻害にとどまらず、個人の私的情報や秘匿したい情報を知らないうちに第三者に送信するものも出現し、一般の人たちが安心してコンピュータを使用できない状況が出現しているというものである。

こうした事実に着眼し、コンピュータによる情報処理の正常性に対する信頼が確保されることが必要であるとして、プログラムの動作が意図せざるものではないとの信頼を害する行為を処罰の対象とする必要があるとして、不正指令電磁的記録の罪が立法されたものである(83)。コンピュータによる情報処理の正常性は、公電磁的ないし私電磁的記録損壊罪や電子計算機損壊等業務妨害罪等においても阻害される。しかし、不正指令電磁的記録の罪において問題とされるのは、個人が情報ないしデータを管理・支配しつつ処理をする前提として、コンピュータが意図通りに動作することで情報ないしデータの管理・支配を確保できることを保護すべきであるということである。コンピュータの動作に対する信頼が重要なのは、この信頼が害されることによって、情報処理における情報の管理・支配が危うくされるからである。この意味において、自己の保有する情報ないしデータの管理・支配という観点での情報セキュリティの前提条件としてのコンピュータにおけるプログラムの動作の信頼を保護法益とするものと理解できる。

立法担当者(84)は、不正指令電磁的記録に関する罪を、電子計算機のプ

---

(82)　佐久間修「情報犯罪・サイバー犯罪」ジュリスト1348号(2008年)109頁以下、112頁は、不正指令電磁的記録に関する罪をネットワークを直接に保護する犯罪であるとして評価するが、情報セキュリティの保護が十全ではない現状において、情報セキュリティの保護の前段階的なところを処罰するにすぎないものであって、少々過大評価ともいえる。また、本罪で問題となる行為は、かならずしもネットワークの存在を前提としないことにも注意を要する。

(83)　山口・前掲注(78)・18頁。

ログラムが、「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」を与えるものではないという、電子計算機のプログラムに対する社会一般の者の信頼を保護法益とする罪として理解する。その社会的信頼の具体的な内容は、明らかでないが、上記の意味において理解すべきである[85]。

このような社会的信頼の保護という点について、電子計算機損壊等業務妨害罪等の他の犯罪と処罰の重複があるのと同時に法益の抽象化によって事実上処罰の早期化を図るものであるとの批判[86]がある。しかしながら、偽造の罪も、もともとは詐欺罪と一体化されて犯罪とされてきたが、社会ないし経済状況の進展に応じて分化し、取引の安全を直接担保する詐欺罪とその前段階の行為を処罰する偽造罪とに独立している。この場合、偽造罪における通貨の社会的信頼という法益が抽象化されて処罰が早期化されているとか、詐欺罪の処罰と重複する[87]から、不当であると主張することはないであろう。現実の社会状況に基づく適切な立法事実が存在し、これにより基礎づけられる[88]のであれば、立法上の問題はない。重要なことは、解釈にあたって、社会的信頼の保護といった

---

(84) 特に断りのない限り、以下、立法担当者の見解は、前掲注(77)の法務省のウェブページにリンクが張られている「いわゆるコンピュータ・ウイルスに関する罪について」というPDFファイルに依拠している。

(85) 同様に社会的な信用を保護法益とする偽造罪でも、第一次的には社会的信用を保護するものとであるとしても、間接的ないし最終的には、取引・契約等の安全を保護されるものと理解される(例えば、松宮孝明『刑法各論講義』(第2版・2008年)356頁)のと同様である。

(86) 渡邊・前掲注(80)・29頁。

(87) 偽造通貨行使罪は、詐欺罪を吸収するものとして、処罰の重複を回避する結果となっているが、これは収得後知情行使罪が詐欺に比して軽く処罰されていることによるものである。偽造私文書行使罪と詐欺罪は、実体法上別罪として成立するものとされている。

(88) 社会の発展により、法益が抽象化することは、複雑な社会的実態を捕捉する上で、ある意味不可避ともいえる。重要なことは、法益の抽象化に甘んずるのではなく、立法論および解釈論において実質的なはどめを設定するアプローチを探ることである。

抽象的な法益のみに依拠するのではなく、副次的ないし最終的に保護されている取引きの安全といった利益を十分に反映させていくことである[89]。

3　いずれにしても、不正指令電磁的記録の罪をプログラムの動作に対する社会的信頼を保護するものとして理解することは、同罪を社会的法益に対する罪として理解すると同時に、その条文の刑法上の位置も示すように、偽造の罪と類比して犯罪が構成されることを意味することになる。例えば、通貨偽造の罪では、偽造通貨行使罪が通貨に対する社会的信用を直接害するものであり、偽造行為それ自体は、この点において当罰性を充足するものではない。しかし、行使の目的をもって偽造行為をおこなうことによって、処罰に値する違法性が具備されるものとされる[90]。同様に、不正指令電磁的記録の罪においても、不正指令電磁的記録供用罪(168条の2第2項)がいわばプログラムの動作に対する社会的信頼を直接危うくするものであり、不正指令電磁的記録作成罪(同条1項)、不正指令電磁的記録取得罪・同保管罪(168条の3)は、「人の電子計算機における実行の用に供する目的」(以下、「供用目的」)をもっておこなってはじめて、プログラムの動作に対する社会的信頼を危うくし、違法性を具備することによって、当罰性をみたす[91]ものとなる(この意味で、二つの行為が一つの行為に短縮された犯罪(verkümmert zweiaktige De-

---

89　例えば、不正指令電磁気記録の罪の客体を「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」と規定するが、プログラムの動作に対する信頼を第一次的な保護法益としつつも、その背後に情報セキュリティの保護が存在することを考慮するのであれば、「不正の」の解釈にあたっては、たんに意図に反する動作をするだけでは足りず、情報セキュリティ上の脅威となる実体が必要と解すべきことになる。園田寿『情報社会と刑法』(2011年)73頁は、日本語入力ソフトの変換プログラムにおける誤変換をもって、当該プログラムを不正指令電磁的記録にあたるとするが、これは「不正の」の文言解釈をいたずらに無視するものであって、不当である。

90　例えば、平野龍一『刑法総論I』(1972年)124頁以下。

91　山口・前掲注78・19頁は、作成罪をプログラムの信頼性に対する危険犯、供用罪をプログラムの信頼を害する侵害犯として理解する。

likte)である[92])。

なお、不正指令電磁的記録の罪は、いずれも、抽象的危険犯であり、プログラムの動作に対する社会的信頼を害しうるかという観点から個々の構成要件の解釈をおこなうべきではあるが、具体的な事案において現にそのような社会的信頼の侵害ないし危険が存したことまでは、犯罪の成立要件とはならない。不正指令電磁的記録供用罪は、未遂処罰規定(168条の2第3項)をもつが、「実行の用に供した」という文言が不正指令電磁的記録が実行可能な状態にあるという結果とそのような結果をもたらすための行為を併せて規定しているにすぎないためであり、この文言から侵害犯として構成されるわけではない[93]。

第2項　不正指令電磁的記録に関する罪の客体

1　以上から、不正指令電磁的記録の罪の中核的な要素は、客体である不正指令電磁的記録にあることが明らかとなる。168条の2第1項1号は、「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[94]を与える電磁的記録」として客体を規定する[95]。このような不正指令に該当する

---

[92] 園田・前掲注[89]・67頁以下における作成罪の当罰性に関する批判は、このような目的犯の犯罪構造を無視するか理解していないものであり、妥当ではない。その批判が妥当するならば、通貨偽造罪も独自の違法性を具備する(69頁において、通貨偽造罪は独自の違法性をもつとしている)ことはあり得ず、その論理に矛盾をきたしている。

[93] これは、現住建造物放火罪(108条)が、現住建造物の焼損という結果を構成要件要素としつつもなお公共の安全に対する抽象的危険犯として理解されていることと同様である。

[94] 以下では、「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「不正指令」と呼ぶ。

[95] 不正指令電磁的記録作成罪・同提供罪では、1号の客体のほか、2号において、1号の不正な指令を記述した電磁的記録も客体となる。本稿の目的であるデュアル・ユース・ツールの規制という観点では、2号のような実行可能状態になっていないものについては、ほとんど対象とならないため、その詳細は、割愛する。

かどうかは、本罪がプログラムの動作に対する社会的信頼を保護するものであるという点から検討されなければならない。したがって、「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」か否かは、現に具体的な個人の意図に反したか否かではなく、当該電磁的記録の諸機能、これらについての説明、具体的に想定されうる利用者および利用方法等を基礎として判断されることになる。これは、偽造通貨行使罪において、現に偽造通貨を受領した人が偽造通貨と見破ったとしても、一般的に真正な通貨と見誤る外観を備えている限り、偽造通貨とされることと同様である。

2　不正指令電磁的記録の罪は、コンピュータによる情報処理過程を前提とし、情報処理過程には多様な態様があることを考慮するならば、不正指令か否かの判断において、具体的な利用状況等を加味することは必要であり、プログラム等単体でのみ判断すべきではない(96)。もっとも、プログラムの機能ないし構造上、「不正指令」を与えるものとして設計されているものもあり、このようなプログラムは、それ自体で不正指令電磁的記録に該当するといえる(これを「真正な不正指令電磁的記録」と呼ぶ)。例えば、ウエブページに無限に大量の画像情報が掲載されているページをポップアップして開いていくスクリプトを記述している場合、当該スクリプトが実行されれば、ブラウザがつねにポップアップウインドウを開き続けるためブラウザを使用しているコンピュータの正常

---

(96)　この点は、すでに文書偽造罪における偽造についても認められているといえよう。一般に、偽造といえるためには、一般人から見て真正に作成されたものであるとの外観が必要であるとされている(大判明治44年9月14日刑録17輯1531頁)が、無人型ローンカード契約機におけるイメージスキャナでの読み込みとそのディスプレイでの表示を前提にした場合には、免許証にコピーした紙片を切り貼りし、メンディングテープを貼付した(実物を直接見ればただちに偽造とわかる外観を有している)事案においても、なお偽造にあたるとされている。さらに、偽造か否かは行為態様をも考慮すべきとするものとして、札幌高判平成17年5月17日高検速報平成17年343頁。ただし、このような考え方に否定的とみられるもののある(保険証のコピーを切り貼りして改ざんしたものをファックスで送信した事案で、東京高判平成20年7月18日判タ1306号311頁)。

な使用が困難になり得る。このような場合、当該スクリプトを記載したウエブページのファイルは、それだけで[97]不正指令電磁的記録に該当することになる[98]。

これに対して、立法担当者の説明あるように、例えば、ハードディスク内のファイルをすべて消去するプログラムが、その機能を適切に説明した上で公開されるなどしており、ハードディスク内のファイルを全て消去するという動作が使用者の「意図に反する」ものでない場合、処罰の対象とすることはできない。この場合、ハードディスク内のファイルをすべて消去するプログラムは、具体的な機能説明[99]や利用状況等との関係において不正指令電磁的記録として処罰可能かどうかが決まることになる(これを「不真正な不正指令電磁的記録」と呼ぶ)。

したがって、おそらく、ほとんどのデュアル・ユース・ツールと呼ばれるものは、不真正な不正指令電磁的記録にあたり、具体的な利用状

97　実質的にはブラウザで開かせるという使用状況が想定はされているが、その使用状況もプログラムの機能との関係で一義的に確定されているともいえる。

98　168条の2第1項2号の客体は、この真正な不正指令電磁的記録についてのみ該当しうると解すべきことになる。

99　機能の説明といっても、利用許諾や詳細な使用説明書の一部に記載されていれば足りるわけではない。コンピュータにおいて現に当該プログラムを利用するに際して、その動作の信頼を保護しようというものであるから、具体的な利用段階においてその意図に反しうる動作がされないような状況が必要となる。例えば、ハードディスクの内容をすべて消去するプログラムをサーバにアップロードし、一切の説明をすることなく、たんにウエブページにリンクを張っているだけでは、不正指令電磁的記録の罪には該当しないとものと解すべきである。また、利用許諾書の一文に、リンクをクリックすると、利用料支払請求画面が利用者の画面に表示され、利用料の支払いによってはじめて消去可能になる旨の記載があったとしても、それが現に当該リンクをクリックする際に、一般的に認知可能な形態で明示されていない限り、不正指令電磁的記録の罪にあたることとなる。ただし、そのような画面表示がブラウザをはじめ利用者のコンピュータの使用を阻害するような態様である場合には、当該プログラムは、利用状況を考慮せずとも、それ自体不正指令電磁的記録に該当することになるであろう。

況、提供状況等を考慮した上で、はじめて不正指令電磁的記録に該当しうることになる。デュアルユースとされる以上、プログラムの機能を適切に理解しうるからこそ多様な使用方法が想定されうるのであって、プログラム等の開発段階においては、そ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と齟齬を生じさせるようになっていないものといえるからである。

第3項　供用行為・供用目的

1　不正指令電磁的記録作成、提供、取得および保管罪は、いずれも目的犯であり、「人の電子計算機における実行の用に供する目的」(以下、「供用目的」)が必要である。これは、すでに述べたように、不正指令電磁的記録を実行の用に供する不正指令電磁的記録供用罪のもつ処罰の実質を目的要件にいれることで、作成行為等に処罰根拠を具備させる機能を持つものである。不正指令電磁的記録の罪がプログラムの動作に対する社会的信頼を保護するものであることから、供用罪および供用目的における「人の電子計算機における実行の用に供する」とは、不正指令電磁的記録を、コンピュータ等の電子計算機[100]を使用する者がこれを実行しようとする意思がないのに実行されうる状態に置くことを意味することになる。

2　以上のような供用ないし供用目的の理解に対しては、供用行為それ自体価値中立的[101]概念であってそのように解釈する必然性がないとの批判[102]がある。しかし、不正指令電磁的記録供用罪において、供用(行為)は、構成要件要素であって、その充足によって原則として犯罪が成立するものであるから、このような違法の実質を担う要素を価値中立

---

(100)　本罪が情報処理過程におけるプログラムの動作の信頼を保護するものである以上、コンピュータ、携帯電話等に限らず、電子的な情報処理機能を有する装置であれば足り、いわゆる情報家電も含まれると解される。もっとも現実に起こりうるとはいえないものもあろう。

(101)　近時、とりわけネット関係の犯罪の成否が問題とされる場面で、「価値中立的」との言葉が多々使用される傾向にあるが、ほとんどがその内実を精査することなく、濫用されているように感じられる。

(102)　渡邊・前掲注(80)・30頁。

的なものとする前提自体に誤りがある。このような批判によれば、「正当な理由がないのに」の要件に違法の実質的判断を移行することになるが、結局、これは正当化事由が存在しないことを意味するという程度しか解釈することができず、他方で正当化事由の不存在を積極的に認定することが要求されることになるであろう。このような実質的違法性判断を構成要件該当性判断に持ち込むことは、不正指令電磁的記録の罪の構成要件をいわば「開かれた構成要件」[103]とするだけでなく、「正当な理由がないのに」以外の構成要件要素から違法の基礎づけ機能を奪うことになり、解釈論上、明確な限定をすることを妨げることになる[104]。

3　立法担当者は、供用行為ないし供用目的における「人の」という文言の解釈として、自己以外の第三者を意味するだけでなく、情を知る者もこの「人の」から除外されるとしている。これに対して、同意殺人罪や同意傷害の例を持ち出し、そのような解釈に合理性がないとする批判がある。しかし、同意殺人罪や傷害罪における「人」が同意ある者を含むとするのも、これらの犯罪の保護法益や罪質から導かれる解釈にすぎない。例えば、同意傷害について同意を構成要件段階で検討する立場からすれば、傷害罪における「人」は、同意のある者を除外することになるであろう。

むしろ、不正指令電磁的記録の罪における解釈において参照されるべきは、社会的信頼の保護という共通性を有する偽造罪における解釈である。偽造通貨行使罪においては、偽造通貨が流通に置かれることによって通貨の真正性に対する社会的信用が害されうるということから、「行使」を偽貨を真正な通貨として流通に置くことと解し、偽造通貨をその情を知っている者に渡す場合は、交付罪の成立を認めると解釈され

---

[103] 松宮孝明『刑事立法と犯罪論体系』(2003年)114頁以下参照。このような「開かれた構成要件」としての構成は、もっぱら錯誤論の妥当な解決に向けられていたことに注意すべきである。

[104] このような論者の立場からは、住居侵入罪における「侵入」もたんに住居棟への立ち入り行為のみを意味することになり、管理権者ないし住居権者の立入への許諾がないことは、実質的な違法性判断として「正当な理由がない」の解釈としてなされることになるであろう。

る(105)。偽造文書行使罪における行使も、偽造文書・虚偽文書であることを知らない者を相手方とする場合に限定されている(106)のも、同様である。さらに、私文書偽造における偽造の意義について、文書の名義人の承諾がある場合について、一般に文書の真正性を偽るものでないとして偽造罪の成立を否定するが、例外的に文書の性質上名義人以外の者が作成することを法律上許されない文書については偽造罪が肯定されると解されている(107)。これも、文書偽造罪の保護法益ないし罪質から帰結される解釈である。

以上のような点をふまえると、不正指令電磁的記録の罪がプログラムの動作に対する社会的信用を保護するものであること、そのような社会的信用を保護することによって最終的には個人の保有する情報・データの管理・支配の意味での情報セキュリティの確保が図られうることなどに鑑みると、不正指令電磁的記録との情を知る者は、「人の電子計算機」の「人」から除外されると解釈するのが妥当である。また、不正指令電磁的記録の定義において「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」とあり、この文言における「その」が冒頭の「人」を指すことは明らかであり、このことは、不正指令の実行に際してコンピュータ等の電子計算機を使用する者が不正指令の存在を知らないことを示しているといえる。また、犯罪行為として、供用目的作成罪と供用罪のみならず、供用目的提供罪および保管罪が規定されていることから、相手方の知情のある提供罪とそれがない供用罪という区分を前提にしているものといえる。

4　デュアル・ユース・ツールが不真正な不正指令電磁的記録として位置づけられる限り、当該ツールのもつ機能を的確に説明し、その機能を正面から使用させるものとして開発されている場合、不正指令電磁的記録作成罪に該当することはないといえる。他方で、このようなデュア

---

(105)　例えば、西田典之『刑法各論』(第5版・2010年)322頁。

(106)　偽造有価証券行使罪について、情を知る相手方に対する行使を行使罪の未遂とした東京高判昭和53年2月8日高刑集31巻1号1頁参照。

(107)　最決昭和56年4月8日刑集35巻3号57頁。なお、このような解釈の当否は、ここでは論じない。

ル・ユース・ツールをその本来の機能を覆い隠し、一般的に利用者に意図しない動作をさせるべく外観をつくりかえ、不正指令電磁的記録とした場合には、不正指令電磁的記録作成罪[108]、同供用罪が成立することになる。この場合、元々のツールの開発者は、その本来の機能をその機能通りに提供すべく開発していることから、不正指令電磁的記録を作成したとはいえない(したがって、開発行為は適法である)が、ツールの外観を改変する行為(誤解を招くファイル名への変更、説明書き等の附加)によって不正指令電磁的記録が作成されたことになる。

もっとも、デュアル・ユース・ツールであっても、そのすべてが不真正な不正指令電磁的記録であるわけではなく、真正な不正指令電磁的記録にあたる場合もありうる。その場合は、構成要件に該当することを否定できないことになるであろう。

(未完)

---

[108] この場合、もとのツールの外観の改変行為が作成行為に該当するととなる。したがって、改変行為が同時に供用行為となる場合には、作成罪と供用罪は、一個の行為によるものとして観念的競合となる(通例は、偽造罪と同様、牽連犯となる)。