〔論　説〕

不正アクセス罪の罪質とその立法動向

渡　邊　卓　也

Ⅰ　問題の所在

本稿では，近時改正法が成立し施行された，不正アクセス行為の禁止等に関する法律（以下，「本法」という）について検討する。本法は，制定当初から，「不正アクセス行為」及び当該行為を「助長する行為」を禁止し（本法3条，5条），その違反に対して刑罰をもって臨んできた（11条，12条2号。以下，「不正アクセス罪」及び「助長罪」という）[1]。今回の改正は[2]，これらの罪の法定刑を引き上げるとともに，新たな罪を創設して処罰範囲の拡張を行うものである。

---

[1] 本法の解説として，不正アクセス対策法制研究会編著『逐条不正アクセス行為の禁止等に関する法律［第2版］』（立花書房，2012年）の他（以下，『逐条』という），露木康浩ほか「不正アクセス行為の禁止等に関する法律の解説」警察学論集52巻11号28頁（1999年），露木康浩「不正アクセス行為の禁止等に関する法律について」ジュリ1165号51頁（1999年），檜垣重臣「ハイテク犯罪の現状と対策について」自正51巻10号30頁（2000年）等がある。

[2] 改正案は，第180回国会に「不正アクセス行為の禁止等に関する法律の一部を改正する法律案」（閣法37号）として提出された（2012年2月21日）。その後，約1カ月強で成立・公布され（同年3月30日，31日），さらに，その約1カ月後には施行された（同年5月1日）。

確かに，いわゆるフィッシング（phishing）や[3]，連続自動入力プログラムによる不正ログイン攻撃は[4]，本法制定当初には想定されていなかった新しい現象であり，不正アクセス行為禁止の「実効性」を確保するためには，これらの行為を規制する必要があるのかも知れない[5]。また，不正アクセス行為禁止の必要性自体が高まり[6]，それが法定刑引上げに現れているのだとすれば，これに伴い，その準備段階の行為をも処罰の対象とし，処罰の拡張を図ることも，立法政策として必ずしも不当とはいえないであろう。しかし，これらの立法事実を承認する前提として，そもそも，不正アクセス行為を禁止し，これを犯罪として規制することに充分な理由があるかを明らかにしなければならない。その上で，今回の改正の具体的内容が立法事実に合致しているかについて，検討する必要があろう。

そこで以下では，まず，本法の目的規定を手掛かりに不正アクセス罪の罪質を分析し，不正アクセス行為犯罪化の意義を論ずる。次に，今回の改正における具体的な改正点を確認し，新設された規定を含めて各罪の位置付けを明らかにした上で，立法事実との整合性を検証する。以上を通じて，改正の妥当性について検討を加えることとする[7]。

改正の経緯については，『逐条』18 頁以下，岡田好史「不正アクセス行為の発生状況の現状と課題（3）」専修法学論集 116 号（2012 年）1 頁以下，四方光「不正アクセス禁止法改正の背景・経緯及び不正アクセス対策の今後の課題」警察学論集 65 巻 6 号（2012 年）13 頁以下等参照。この他，改正法の解説として，川原匡平「不正アクセス行為の禁止等に関する法律の一部を改正する法律」警察公論 67 巻 7 号 20 頁（2012 年），同「不正アクセス行為の禁止等に関する法律の一部を改正する法律について」捜査研究 733 号 13 頁（2012 年），蔵原智行「『不正アクセス行為の禁止等に関する法律の一部を改正する法律』について」警察学論集 65 巻 6 号 21 頁（2012 年），同「フィッシング行為，ID・パスワードの不正取得等の禁止・処罰等」時の法令 1909 号 4 頁（2012 年）等がある。

[3] アクセス管理者が公開したウェブサイト又は送信した電子メールであると利用権者に誤認させて，識別符号の入力を求める旨の情報を閲覧させ，当該符号をだまし取ることをいう。具体的な仕組みと，従来の規定による刑事規制の可能性については，岡田好史「フィッシングに対する刑事規制について」専修大学法学研究所紀要 32 号（2007 年）22 頁以下参照。

[4] 識別符号のリストを多数のウェブサイトに次々と試行入力して，不正アクセス行為を敢行しようとすることをいう。このような攻撃が増加した背景には，1 人の人間が利用するウェブサイトの増加により，同一の識別符号を複数のサイトで使い回す例が一般化したことがある。

[5] 『逐条』18 頁以下。

[6] 近時の発生状況については，岡田好史「不正アクセス行為の発生状況の現状と課題（1）」専修法学論集 114 号（2012 年）143 頁以下，同「不正アクセス行為の発生状況の現状と課題（2）」専修法学論集 115 号（2012 年）43 頁以下等参照。

[7] 本法制定後，2001 年に採択された欧州評議会（Council of Europe）の「サイバー犯罪に関す

Ⅱ　不正アクセス罪の罪質

１　犯罪の防止

立案担当者によれば，本法制定の趣旨は，以下のようなものである。すなわち，今日，インターネットを中心としたコンピュータ・ネットワークの著しい発展の中で，これを利用した「ハイテク犯罪」が増加している[8)]。その中には，広範な被害や影響を及ぼすものが多く見られるところ，「その助長要因を除去し，未然防止を図る必要性」がある。ハイテク犯罪の最大の問題は，「犯行の抑止力が働きにくい」点であり，その手段としての不正アクセス行為を放置したままでは，ますます「抑止力が低下してそれが助長される」と同時に，「ネットワークの秩序が乱され，その相互接続が阻害される」こととなる。そこで，「不正アクセスを禁圧することが喫緊の課題」である[9)]。

ここでは，不正アクセス行為そのものというよりも，むしろ，その後に行われる犯罪による実害が問題とされているともいえる。この実害に対しては，既に電磁的記録不正作出罪（刑法 161 条の 2），電子計算機損壊等業務妨害罪（234 条の 2），電子計算機使用詐欺罪（246 条の 2）及び文書等毀棄罪（258 条，259 条）等

る条約（Convention on Cybercrime）」において，「違法なアクセス」として，「コンピュータ・システムの全部又は一部に対するアクセスが，権限なしに故意に行われること」の犯罪化が要請され（同条約 2 条），また，当該「犯罪を行うために使用されることを意図して」，「コンピュータ・システムの全部又は一部にアクセス可能となるようなコンピュータ・パスワード，アクセス・コード又はこれらに類するデータ」を「製造し，販売し，使用のために取得し，輸入し，頒布し又はその他の方法によって利用可能とすること」及びその「保有」の犯罪化も要請された。もっとも，「販売，頒布又はその他の方法によって利用可能とする行為に関するもの」以外は，留保可能である（6 条）。今回の改正は，同条により我が国が留保した行為の一部の犯罪化と位置付けられる。

8) ハイテク犯罪とは，1997 年に開催されたデンヴァー・サミットにおいて用いられた呼称であり，「コンピュータ及び電気通信技術を悪用した犯罪」のことをいう。その対策に取り組むことを各国が合意する中で，我が国においても，国際協調の観点から不正アクセス行為の犯罪化が必要とされた。なお，現在では，ハイテク犯罪に代えて，「サイバー犯罪」という呼称を用いるのが一般である。例えば，サイバー犯罪に関する条約前文において，その内容は，「コンピュータ・システム，コンピュータ・ネットワーク及びコンピュータ・データの秘密性，完全性及び利用可能性に対して向けられた行為並びにコンピュータ・システム，コンピュータ・ネットワーク及びコンピュータ・データの濫用」とされている。

9) 『逐条』1 頁以下。

が存在しているが[10]，不正アクセス罪を，この実害との関係で，不正アクセス行為の段階まで処罰が早期化された，いわば予備的行為を処罰する罪と構成することも可能である（以下，「予備罪的構成」という）。本法の目的規定において，まずもって「電気通信回線を通じて行われる電子計算機に係る犯罪の防止」が掲げられていることを，このような文脈で理解することも可能であろう[11]。

しかし，このように「社会的な有害性とはほど遠い事態」を根拠とすることは，「将来の犯罪予防のための保安処分と同種のものになりうる」との批判もある[12]。他方で，例えば，データの不正入手（いわゆる「情報窃盗」）や，コンピュータの無権限利用といった実害については，それを捕捉する罪が存在していない。これは，上述の電磁的記録不正作出罪等に係る 1987 年の刑法一部改正の際に，処罰すべき範囲や処罰の程度等についてのさらなる検討が必要とされ，これらの行為の犯罪化が見送られた経緯があるからである[13]。それにもかかわらず，その予備的行為を処罰することの当否が問題となる。

この点，不正アクセス罪の成否が問題となった下級審判例の中には，その趣旨を，予備罪的構成から理解し得る判示をしたものもある。事案は，プログラマーである被告人が，勤務先会社の前任者が利用権者となっているサーバに対して，同社のコンピュータのアクセス履歴から読み取った ID 及びそこから推測したパスワードを使用してアクセスし，前任者の開発に係るプログラムのソースコードを含む全てのファイルをダウンロードしたというものである。

以上のような事実関係の下で，東京地裁は，同罪の成立を認めた[14]。弁護人は，当該行為による「具体的・実質的な被害」は生じていないなどと主張して控訴した[15]。これに対して東京高裁は，「ネットワーク社会において，ネットワーク

---

[10] その他，「電気通信事業者の取扱中に係る通信の秘密」に係る，通信の秘密侵害罪（電気通信事業法 179 条，4 条）等が考えられる。

[11] サイバー犯罪に関する条約においても，違法なアクセスが「コンピュータ・データを取得する意図その他不正な意図をもって行われること」を要件とし得るとされており，予備罪的構成が想定されているといえる。

[12] 立法過程における警察庁案について，石井徹哉「不正アクセス禁止法の意義と限界」千葉大学法学論集 19 巻 3 号（2004 年）11 頁以下。むしろ，「犯罪の誘発要因をいかに効果的に除去するかが必要」とする。

[13] 『逐条』27 頁。当時の議論については，米澤慶治編『刑法等一部改正法の解説』〔古田佑紀=多谷千香子〕（立花書房，1988 年）14 頁以下等参照。

[14] 東京地判平成 14 年 12 月 25 日判時 1846 号 159 頁。

[15] この他，当該サーバは勤務先が管理するものであり，被告人にもアクセスが許されていたと認識していたから故意がない，当該ソースコードの著作権は勤務先会社の関連会社に帰属して

を通じてコンピュータを利用する者を正しく識別できなければ，侵害行為に対する抑止力が失われ，アクセス制御機能により保護を図ることとしている業務の円滑な遂行や関係者の権利・利益に対し具体的な侵害の危険が生じるからこそ，法により不正アクセスに対する罰則が定められているのであって，具体的，現実的に権利・利益が侵害される前の段階において処罰しようとするのが法の趣旨である」とした上で，「ファイルを閲覧されたことによるノウハウや著作権の侵害や，プライベートな情報を見られた可能性があることによる精神的な損害がなかったとも断じ難い」などとして控訴を棄却した[16]。

ここでは，「業務の円滑な遂行や関係者の権利・利益」に対する実害の「危険」が同罪を基礎付けていることが認められている[17]。もっとも，その危険の発生は，あくまでも，アクセス制御機能が回避されたことで「侵害行為に対する抑止力が失われ」た結果とされている。そこで，このように「抑止力」に言及することが，同罪の罪質との関係で如何なる意義を持つのかが問題となる。

この点，立案担当者は，同罪の法益を，利用権者等の識別が正しく行われているという「アクセス制御機能に対する社会的信頼」としており[18]，このような解釈は一般に受け入れられている[19]。そして，犯罪の防止は，この信頼を保護することにより犯行の「抑止力」を維持することを通じて実現されるところ，信頼が失われた場合に「犯罪が行われやすい環境が生ずる」ことが問題であって[20]，

おり，被告人は業務遂行という正当な目的のために行為に及んだのだから正当業務行為であるなどと主張したが，いずれも排斥されている。

16) 東京高判平成 15 年 6 月 25 日判時 1846 号 155 頁。評釈として，岡田好史「判批」専修法学論集 93 号 211 頁（2005 年），佐久間修「判批」判例評論 563 号 36 頁（2006 年）。もっとも，量刑不当の主張に関して，被告人の行為が「いわば鍵の掛かった他人の家を勝手に開けて入り込む行為であり，ネットワークの秩序を乱し，ひいては高度情報通信社会の健全な発展を阻害しかねない」とも述べている。

17) これに対して，岡田・前掲注 16）215 頁は，「明らかに法の趣旨を誤って解している」とする。

18) 『逐条』140 頁。

19) さらに，園田寿ほか「ハイテク犯罪と刑事法」現代刑事法 1 巻 8 号〔前田雅英発言〕（1999 年）16 頁以下は，「ネットワーク社会に対しての国民の信頼」を，佐久間・前掲注 16）38 頁は，「電子ネットワーク全体に対する社会的信頼」ないし「国民一般の利用と結び付いた情報通信システムに対する社会全体の信頼」を法益とする。同旨，同『実践講座・刑法各論』（立花書房，2007 年）221 頁。既に，本法制定前に，佐伯仁志「無権限アクセス規制に関する覚書」研修 602 号（1988 年）8 頁も，「コンピュータ・ネットワークシステムの安全性に対する信頼」を挙げていた。

20) 園田ほか・前掲注 19）〔露木康浩発言〕16 頁も，「インターネットが犯罪の巣窟になったりしないようにしようという環境設定という観点から規定した」とする。

「個々の不正アクセス行為が特定の犯罪に結び付くおそれ」は問題ではないとされる。すなわち，不正アクセス罪は，「社会的信頼の侵害というその行為自体の危険性を処罰の根拠としている」のであり，「予備的行為を処罰しようとする趣旨にでたものではない」とされるのである[21)]。

確かに，このような観点からすれば，不正アクセス罪の存在意義を，アクセス後の実害とは区別して理解することが可能となろう。また，これと同様のことを，ハイテク犯罪禁止規範の実効性確保という観点から説明することも可能である。すなわち，例えば，盗品等関与罪（刑法 256 条）を，盗品等の市場形成を防止することを目的とした規定と把握するのと同様に，不正アクセス罪を，ハイテク犯罪が行われやすい環境形成を防止することを目的とし，それを助長する行為について処罰の拡張を認めた規定として理解するのである[22)]。

しかし，ある犯罪が増加し，それを抑止する必要性が高まった場合には，当該犯罪自体を重罰化するとか，その未遂や予備を犯罪化することによって処罰を早期化すべきとの政策判断が行われるのが通常であろう。そのような措置を講じないままで，当該犯罪の抑止力自体を問題とし，しかも，当該犯罪の予備的行為が行われないとの信頼を保護することによってその抑止力の維持を図るなどという政策判断は，余りにも迂遠であって，犯罪の防止との関係で実効性があるとは思われない。

したがって，このような構成は，少なくとも，ハイテク犯罪の増加という立法事実との関係では，論理の飛躍があるといわざるを得ない。犯罪の防止は，まずは当該犯罪の禁止規範自体の再検討を通じて，直接的に実現されるべきである。なお，その際には，捕捉する罪が存在しない実害についても，犯罪化の是非を検討する必要があろう[23)]。

２　秩序の維持

本法の目的規定においては，犯罪の防止と並んで，「アクセス制御機能により実現される電気通信に関する秩序の維持」も掲げられている。ここでの「秩序」

---

21) 『逐条』28 頁以下，140 頁。同旨，岡田・前掲注 16）214 頁以下。なお，立崎正夫「判批」別冊 NBL79 号サイバー法判例解説（商事法務，2003 年）84 頁以下。

22) もっとも，禁止規範の実効性確保という観点からの処罰の拡張は，必ずしも一般的とはいえない。渡邊卓也「判批」刑事法ジャーナル 34 号（2012 年）128 頁以下参照。

23) 今井猛嘉「ネットワーク犯罪」法教 303 号（2005 年）52 頁参照。

の意義は必ずしも明らかではないが，例えば，これを電気通信が円滑に行われている状態と捉えることも可能であろう。本法について，「コンピュータによる業務処理，情報処理の安全性・確実性を保護することを目的とするもの」とする見解も[24]，これと同旨といえよう。しかし，不正アクセス行為は，それだけでは対象サーバに対する危険をもたらすに過ぎず，「不特定・多数の者に対する脅威たりえない」との指摘もある[25]。また，そのような秩序の維持を問題とするならば，それは，犯罪の防止をも包摂する概念ともなりかねない[26]。

この点，立案担当者は，ここでの秩序とは，「ネットワークが発展する前提としての電気通信の利用上のルールを指すもの」であって，犯罪の防止を包摂する概念ではないとしている[27]。すなわち，ルールの遵守こそが秩序であって，その違反は，実害との関係を問わず，およそ抑止すべきということである。しかし，実害と切り離されたルールの遵守自体を，刑罰をもって維持しようとすることには疑問がある[28]。それゆえ，ここでのルール違反も，あくまでも，犯罪を含めた実害との関係で捉えるべきであろう。

なお，目的規定においては，さらに，上記 2 つの目的の達成を「もって高度情報通信社会の健全な発展に寄与すること」が掲げられている。立案担当者によれば，これは本法の「究極の目的」とされる。すなわち，犯罪の防止と秩序の維持という「直接の目的」は「相互に観点を異にするものであって，論理必然的に結びつくものではない」ところ，「アクセス制御機能による社会的信頼を確保するという事柄に関しては，高度情報通信社会の健全な発展に寄与することを究極の目的とする点において一致し，その限りで 1 個の法目的といい得る」

---

[24] 西田典之『刑法各論［第 6 版］』（弘文堂，2012 年）134 頁。

[25] 石井・前掲注 12）13 頁以下。「電気通信の安全とは，物理的レイヤーなどきわめてローレベルのレイヤーにのみかかわるものであり，不正アクセスはむしろこのレベルにおいてはそのレイヤーを利用するものであり，危殆化することは不正アクセスすら困難にする」として，「いたずらに不要な局面を犯罪化において考慮するものとなり，不当である」と批判する。反対，今井・前掲注 23）54 頁。

[26] なお，成瀬幸典「不正アクセス罪についての一考察」阿部純二先生古稀祝賀論文集『刑事法学の現代的課題』（第一法規，2004 年）362 頁は，「一般的な『犯罪の防止』を法の目的とし，不正アクセス罪の保護法益とすることは問題」であるから，犯罪の防止は，秩序の維持の「手段として位置付ければ足りる」とする。

[27] 『逐条』32 頁以下。

[28] 今井・前掲注 23）52 頁，同「『不正アクセス』の意義をめぐって」研修 719 号（2008 年）7 頁。

とされるのである[29]。しかし，「社会の健全な発展」などという，およそ無内容な概念を設定すれば，如何なる目的との関係でも，それが究極の目的となり得るのは当然である。それゆえ，このことによって「本法が統一された体系の下に構成された」と考えるのは[30]，単なる自己満足に過ぎないといえよう。

いずれにしても，立案担当者は，この秩序についても，犯罪の防止と同様に社会的信頼との関係で位置付けている。すなわち，ここでの秩序とは，「アクセス制御機能による利用権者の識別が正しく行われているとの信頼感によって実現される電気通信に関する秩序である」というのである[31]。しかし，秩序の維持が問題であれば，当該秩序を乱したこと自体を犯罪化するとか，その未遂や予備を犯罪化することによって処罰を早期化すべきとの政策判断が行われるのが通常であろう。そのような措置を講じないままで，秩序を乱す行為の予備的行為が行われないとの信頼を保護することによってその維持を図るなどという政策判断は，余りにも迂遠である。

この点，学説の中には，「情報通信の安全性」を確保するためには，「情報セキュリティ」，とりわけ「情報のインテグリティ」を法益と捉え，「情報へのアクセスコントロール」の侵害を問題とすべきとした上で，当該法益の主体を「情報の外形の保持者すなわちコンピュータシステムの管理者」とし，不正アクセス罪を，「アクセス制御機能の侵害を実質的な違法とする個人的法益に対する罪」と把握すべきとの見解もある[32]。このように考えた場合，一般に不可罰とされる情報窃盗との異同が問題となり得るが[33]，この点については，アクセスコントロールは，「外形に対する管理」を問題にする点で，「内容に対する所有・支配」を問題にする情報窃盗とは異なると説明されている[34]。

---

29) 『逐条』33 頁。

30) 『逐条』33 頁。警察庁と旧郵政省とが，ハイテク犯罪対策と電気通信の安全性という異なる観点から検討を進めたという立法経緯からすれば，「統一された体系」の構築は最初から不可能である。

31) 『逐条』32 頁。

32) 石井・前掲注 12）16 頁，25 頁以下，35 頁以下。いわば「個人のデータの外形に対する形式的な自己決定権」が問題となるとされる。なお，同「企業をめぐる情報通信技術と犯罪」甲斐克則編『企業活動と刑事規制』（日本評論社，2008 年）137 頁以下参照。

33) 園田寿『情報社会と刑法』（成文堂，2011 年）38 頁。

34) 石井・前掲注 12）25 頁以下，35 頁以下。今井・前掲注 23）52 頁も，「秘密の侵害」に止まり，「情報の不正入手」とは区別し得るとする。同旨，佐伯・前掲注 19）8 頁。なお，石井・前掲注 32）136 頁以下参照。

この見解は，社会的信頼という法益理解を見直す契機となり得る点で興味深い。これに対しては，データ処理に着目することは「基本的に正しい方向性を示している」としながらも，アクセス制御機能を回避することで危殆化される「ネットワーク内部でのデータ処理の確実性とそれへの信頼」ないし「コンピュータ・データの処理に利害関係を有する不特定多数の者の，データ処理の確実性に対する信頼」を法益とすべきとの指摘もある[35)]。しかし，これでは，再び信頼の保護を問題にすることで，情報セキュリティを直接に問題にしようとするこの見解の価値を減じかねないといえよう。

情報へのアクセスコントロールの侵害を問題とすべきとする見解は，少なくとも立法論として検討の余地があるが[36)]，アクセスコントロールに，情報自体の価値とは異なる実体があるかについては議論の余地があろう。それゆえ，むしろ，情報自体の実体的価値を論じ，情報窃盗の処罰化ないしその処罰の早期化として，アクセスコントロールの侵害を位置付けるという選択肢もあるように思われる。

ところで，立案担当者は，「不正アクセス行為が横行すれば，アクセス制御機能により実現される電気通信に関する秩序が乱され，利用者の中に安心してネットワークが利用できないとの不信感を生み，ネットワーク相互の接続が抑制されるおそれが生じる」とも述べている[37)]。ここでは，信頼によって秩序が実現されるというよりも，秩序によって信頼が醸成されると述べられているようでもある。すなわち，不正アクセス行為によるアクセス制御機能の回避は，「電気通信の利用上のルール」に違反し，それ自体，秩序を乱す行為であるところ，当該行為の横行によって，ネットワークに対する信頼が失われることとなる。そして，そのことは，秩序を乱すことではなく，「ネットワーク相互の接続が抑制される」ことに繋がるからこそ問題とされているのである。

---

35) 今井・前掲注 23）53 頁以下，同・前掲注 28）9 頁。当該法益は，「最終的には個人的法益に還元されるべきである」が，「個人の集合体が有する」社会的法益であるとする。なお，佐伯・前掲注 19）8 頁参照。

36) 石井・前掲注 12）36 頁。園田・前掲注 33）39 頁も，「新たな立法を講じて，『不正アクセス』の概念そのものを再構成すべき」とする。なお，岡田好史『サイバー犯罪とその刑事法的規制』（専修大学出版局，2004 年）119 頁以下。さらに，今井・前掲注 23）55 頁，同・前掲注 28）9 頁以下参照。

37) 『逐条』32 頁。園田ほか・前掲注 19）〔露木康浩発言〕16 頁は，「ネットワークにつなげたくなくなる行為が行われないような秩序を維持する」という趣旨とする。

そこで次に，社会的信頼の保護とネットワーク相互の接続の維持との関係について，偽造の罪（刑法 148 条以下）の保護法益論を参照しつつ検討することとする。

３　信頼の保護

不正アクセス罪を社会的信頼の観点から把握するならば，同罪は，一般に「公共の信用」を法益とするとされる偽造の罪に類似する，社会的法益に対する危険犯と構成されることとなる（以下，「信頼保護構成」という）。また，利用権者のみがアクセス制御機能を通過して特定利用ができるというシステムに対する関係者の信用を利用して，目的を実現するという点においても，不正アクセス罪は，偽造の罪との罪質の共通性を指摘し得る[38]。後述のように，助長罪が識別符号の「提供」を問題としており，また，不正アクセス罪が，いわば，その供用によって実現されると解し得る点で，偽造の罪に類似した行為態様を予定していることも，このような文脈で理解可能である。

すなわち，偽造の罪が，「文書」等により実現される取引システムの維持を目的とした規定と把握され得るのと同様に，不正アクセス罪も，アクセス制御機能により実現されるネットワークで相互に接続されたコンピュータ・システムの維持を目的とした規定と把握し得るのである。上述の，信頼が失われることでネットワーク相互の接続が抑制されるとの説明も，これと同旨と解し得る。

確かに，偽造の罪が，偽造文書を用いた詐欺罪（刑法 246 条）等の実害を捕捉する罪から分化して成立したという歴史的経緯に鑑みれば，偽造の罪における法益理解が一般に受け入れられている以上，信頼保護構成も，必ずしも不当とはいえない[39]。しかし，偽造の罪における法益理解は，そのような構成の正当性を推認させるとはいえても，それを確証するとまではいえないように思われる。近時は，財産犯における「利益」概念の抽象化ないし処罰の早期化が認められ

---

[38] もっとも，このことは，例えば，罪数判断において援用され得るとしても，法益理解とは直接の関係はない。渡邊卓也「判批」姫路法学 50 号（2009 年）257 頁以下参照。

[39] 不正指令電磁的記録に関する罪（刑法 19 章の 2）について，石井徹哉「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）」千葉大学法学論集 26 巻 4 号（2012 年）79 頁以下。「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」とする。

る[40]。ここから，偽造の罪と財産犯との間で，事実上の違法評価の重複を問題とし得るところ，財産犯体系の再構築と併せて，偽造の罪についても再構築が迫られているといえる[41]。このことからも，偽造の罪における法益理解を当然視すべきではない。また，上述のように，実害を捕捉する罪が充分に整備されていないことからも，本法と偽造の罪とでは状況を異にするといえよう。

そもそも，信頼保護構成は，システムの維持という，およそ全体像を把握し難い抽象的な目的を設定することで処罰の正当化を図る点に，問題があるように思われる。この点，「『信頼』という概念自体が一人歩きすることで，構成要件の解釈において個々の構成要件メルクマールを拡張してしまい，その処罰範囲を不明確にする危険がともなう」と同時に，刑罰が「保護法益との関連性」を喪失し「国民の法意識の教育」の手段とされてしまうばかりか，そのような立法は，「政治問題の解決を任務とした象徴的立法」であって，「刑罰を正当化しうるだけの実体を備えていない」との批判もある[42]。

学説の中には，「アクセス制限を付加することによって達成しようとする目的が社会的な意義・性格（公共性）を有する場合には，当該目的の達成手段であるアクセス制御機能も社会的意義を有し，社会的信頼の対象であるといえる」として，信頼が向けられる対象を類型化しようと試みる見解もある[43]。しかし，信頼を問題とする以上，その判断は明確とはなり得ないように思われる[44]。

また，上述のように，不正アクセス行為によるアクセス制御機能の回避が，それ自体，秩序を乱す行為であるとすれば，アクセス制御機能に対する信頼とは，秩序を乱す行為が行われないことに対する信頼を意味することとなる。しかし，それは，秩序の維持と区別された独自の法益ではあり得ない。そのよう

---

40) このことは，例えば，電子マネーの取得自体を電子計算機使用詐欺罪の客体とした事例にみられる。渡邊卓也「電子マネーの不正取得と電磁的記録不正作出罪」姫路ロー・ジャーナル 5 号（2011 年）31 頁以下参照。

41) 渡邊・前掲注 40）40 頁。

42) 石井・前掲注 12）17 頁以下。同・前掲注 32）140 頁も，「刑法の謙抑性からみて問題」とする。なお，岡田・前掲注 36）142 頁以下参照。

43) 成瀬・前掲注 26）364 頁以下。例えば，「コンテンツの法的価値が乏しく，入会料も無料で，会員資格に特に制限もなく，個々の会員に付加されている識別符号も極めて単純なものである場合」は，これにあたらないとされる。

44) 今井・前掲注 23）53 頁は，上述の事例でも「当該ネットワーク内部でのデータ処理には多数の者の利害が関係しており，不正アクセスにより，この利益が侵害される危険が生じる点で差はない以上，基本的には，他の事例との間で保護の態様を区別すべきではない」とする。

な信頼は，あらゆる法益に含まれているもので，それと別物ではないといえよう[45]。

いずれにしても，信頼保護構成によって立法の正当性に関する検証を曖昧にすることは，厳に慎むべきである。目的規定において，犯罪の防止（とそれを含み得る秩序の維持）が直接の目的として掲げられていることに鑑みれば，信頼保護構成は，法益の抽象化によって事実上の処罰の早期化を図るものであって，法益論において体裁を整えることで，予備罪的構成の実質を隠蔽したに過ぎないといえる。この点，「サイバー犯罪の形態が多様化したこと」を理由に「その入り口となる不正アクセス行為それ自体の規制が必要」とする見解は，予備罪的構成を，「もはや社会の実態に即していない」と批判する[46]。しかし，この見解も，「多様化した」犯罪への対処の必要性を論ずることで，実質的には処罰の早期化を主張しているように思われる。むしろ，それによって実害の危険の有無の検証が度外視されかねない点にこそ[47]，問題があるといえる。

したがって，本法の立法にあたっては，むしろ，不正アクセス罪の罪質を予備罪的構成から理解した上で，処罰範囲の限定を図るという選択肢もあったように思われる。

Ⅲ　改正とその評価

１　不正アクセス罪

本法は，不正アクセス罪における不正アクセス行為を，「アクセス制御機能」を有する「特定電子計算機」に電気通信回線を通じて当該アクセス制御機能に係る他人の「識別符号」を入力して当該特定電子計算機を作動させ，当該アクセス制御機能により制限されている「特定利用」をし得る状態にさせる行為（本

---

[45] 賄賂の罪（刑法 197 条以下）の法益論において，職務の公正に対する「信頼」の保護を問題とする見解について，山口厚『刑法各論［第 2 版］』（有斐閣，2010 年）611 頁。「たとえば，殺人罪の保護法益を問題とする場合，『人の生命』と『人の生命が侵害されないことに対する社会一般の信頼』との間に何の差異もない」とする。今井・前掲注 23）53 頁参照。

[46] 佐久間・前掲注 16）38 頁以下。

[47] 園田ほか・前掲注 19）〔前田雅英発言〕16 頁以下は，「行政刑法」として，「具体的にまったく危険性がない」場合も，「システムとして刑事的に処理」すべき場合があるとする。

法2条4項1号）及び特定利用の制限を免れることができる「情報」又は「指令」の入力による同様の行為（同条同項2号，3号）と定義している（以下，前者を「識別符号盗用型」，後者を「セキュリティ・ホール攻撃型」という）[48]。

特定電子計算機とは，「電気通信回線に接続している」電子計算機をいい，特定利用とは，「当該電気通信回線を通じて行う」当該特定電子計算機の利用をいう（同条1項）[49]。識別符号とは，「アクセス管理者」において「利用権者等」を「区別して識別することができるように付される符号」をいい（同条2項），例えば，ID及びパスワードを「組み合わせたもの」がこれにあたる。アクセス管理者とは，特定電子計算機の「動作を管理する者」（同条1項），すなわち，それを「誰に利用させるか」を決定する者をいい[50]，利用権者とは，特定利用につきアクセス管理者の「許諾を得た者」をいう（同条2項）。そして，アクセス制御機能とは，「特定電子計算機の特定利用を自動的に制御するために当該特定利用に係るアクセス管理者によって当該特定電子計算機又は当該特定電子計算機に電気通信回線を介して接続された他の特定電子計算機に付加されている機能」であって[51]，識別符号の入力を確認して「当該特定利用の制限の全部又は一部を解除するもの」をいう（同条3項）[52]。

なお，「アクセス管理者がするもの」及び「アクセス管理者又は利用権者の承諾を得てするもの」については，不正アクセス行為から除外されている。立案担当者によれば，これらの場合には，利用権者の「識別が困難になることも

---

48) 『逐条』62頁以下及びそこに掲載された図参照。

49) 『逐条』65頁以下によれば，本法の対象が特定電子計算機の特定利用に限定されているのは，いわゆるスタンド・アローンのコンピュータ等の場合には，当該コンピュータのある部屋や建物への入退出管理の徹底等の手段による利用制限が可能であることが理由とされる。なお，上述の情報へのアクセスコントロールの侵害を問題とすべきとする見解からは，当該コンピュータ内の情報も保護されるべきこととなる。

50) 『逐条』37頁。

51) 「他の特定電子計算機」にアクセス制御機能がある場合とは，いわゆる認証サーバやゲートウェイ・サーバを用いた方式を指す。『逐条』51頁の図参照。

52) 『逐条』48頁によれば，アクセス制御機能が識別符号による形態に限定されているのは，そのような形態が「一般的に広く採用され」，それ以外の形態の内容・意義が必ずしも明確でないことが理由とされている。なお，佐伯・前掲注19）10頁以下参照。この点について，石井・前掲注12）28頁以下は，「個々具体的なものを遺漏なく法律で取り上げることは法技術的に困難」としつつ，例えば，「特定IPアドレスによる利用制限の方法」が対象とならない点で，「アクセス制御の意味を十分にとらえているものとはいえない」と批判する。今井・前掲注23）56頁も，立法的な対応の必要性を示唆する。

なく，犯罪の防止及び電気通信に関する秩序の維持の観点からの問題も生じない」ことが，その理由とされる[53]。その趣旨は必ずしも明らかではないが，例えば，偽造の罪については，虚偽であるとの情を知る者に文書等を提示しても，法益侵害の結果を生ぜず「行使」の未遂にとどまるとされるところ[54]，これと同様に，これらの場合には，不正アクセス罪の法益とされる社会的信頼は害されないとの解釈もあり得よう[55]。それゆえ，被害者の承諾の観点からする信頼保護構成との整合性についての批判は[56]，必ずしも適切ではないといえる。

いずれにしても，識別符号盗用型であれセキュリティ・ホール攻撃型であれ，不正アクセス行為の方法は，あくまでも，ネットワークに接続されている特定電子計算機に設定されたアクセス制御機能の回避でなければならず，それ以外の方法による無権限のアクセスは，たとえそれが当罰的であるとしても，本法の対象とはならない[57]。そこで，不正アクセス行為により回避されることとなる，アクセス制御機能の意義が問題となる。すなわち，まず，当該機能の有無について，如何なる基準によって判断すべきか，さらに，当該機能が設定されていることを前提として，当該機能による「特定利用の制限」の有無について，如何なる基準によって判断すべきかが議論されている[58]。このうち，前者については，例えば，上述の情報へのアクセスコントロールの侵害を問題とすべきとする見解から，「立法的解決」が提案されていた[59]。また，後者についても，現行

---

53) 『逐条』72 頁以下。なお，セキュリティ・ホール攻撃型において利用権者の承諾がある場合は考えられないから，そのような場合は除外範囲に含まれない。

54) 偽造有価証券行使等罪（刑法 163 条）について，東京高判昭和 53 年 2 月 8 日高刑集 31 巻 1 号 1 頁。不正指令電磁的記録に関する罪について，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）30 頁参照。

55) なお，園田寿「定められた『罪』と『罰』」園田寿ほか『ハッカーvs.不正アクセス禁止法』（日本評論社，2000 年）205 頁。これに対して，今井・前掲注 23）54 頁は，「利用権者の利益も独立した保護法益であることを前提とするもの」とする。

56) 石井・前掲注 12）12 頁。承諾がない場合との差が「行為者の主観的な犯罪の危険性でしかない」から，「現代の刑法理論から許容されない」との指摘も，適切ではない。

57) サイバー犯罪に関する条約においても，「違法なアクセス」が「防護措置を侵害することによって行われること」や「他のコンピュータ・システムに接続されているコンピュータ・システムに関連して行われること」を要件とし得るとされている。

58) この点が争われた下級審判例として，東京地判平成 17 年 3 月 25 日判時 1899 号 155 頁判タ 1213 号 314 頁がある。大橋充直「情報漏えい犯罪の新判例（ACCS 事件）」捜査研究 647 号（2005 年）66 頁以下，同「続・情報漏えい犯罪の新判例（ACCS 事件）」捜査研究 648 号（2005 年）66 頁以下，園田・前掲注 33）27 頁以下等参照。

59) 石井・前掲注 12）36 頁。

法上，明確な客観的基準を見出す契機は無いといわざるを得ない[60]。それにもかかわらず，今回の改正においては，これらの問題についての立法的解決は為されなかった。

他方で，法定刑については，旧規定よりも引き上げられた（1年以下の懲役又は50万円以下の罰金から3年以下の懲役又は100万円以下の罰金）。立案担当者によれば，これは，「インターネットが社会・経済活動にとって極めて重要なインフラとして国民生活を支える状況となり，アクセス制御機能に対する社会的信頼の確保の重要性が増大していたこと」の他，不正指令電磁的記録作出等罪（刑法168条の2）の法定刑（3年以下の懲役又は50万円以下の罰金）や，電子計算損壊等業務妨害罪（5年以下の懲役又は100万円以下の罰金）及び電子計算機使用詐欺罪（10年以下の懲役又は100万円以下の罰金）の法定刑等との均衡が理由とされる[61]。しかし，信頼保護構成からすれば，少なくとも，実害を捕捉する罪である後二者との比較は適切ではない。むしろ，予備罪的構成から，このような法定刑の設定を基礎付けることが可能であろう。

２　不正アクセス助長罪

上述のように，本法は，制定当初から，不正アクセス罪に加え，助長罪を規定してきた。立案担当者によれば，同罪制定の趣旨は，以下のようなものである。すなわち，不正アクセス行為を行うためには，識別符号を調べる等の様々な準備作業や専門的知識ないし技術が必要となるところ，識別符号を入手することができれば，誰もが簡単に当該行為を行うことが可能となる。そこで，不正アクセス行為禁止の「実効性」を担保するため，他人の識別符号の利用権者以外の者への「提供」を，当該行為を「助長する行為」として禁止することとした[62]。

ここでは，不正アクセス行為禁止の実効性の担保が，その準備段階の行為をも処罰の対象とした根拠とされている。そして，助長罪は，想定し得る様々な準備行為のうち，いわば不正アクセス行為の道具ともいえる識別符号の提供に

60) なお，これらの問題については，別稿における検討を予定している。
61) 『逐条』141頁以下。
62) 『逐条』84頁以下。

着目した規定である[63]。すなわち，同罪は，不正アクセス罪の幇助的な行為の一部を，独立に犯罪化した規定と位置付け得る（独立共犯）。ただし，実行従属性が不要となる点で，不正アクセス罪の従犯よりも処罰が拡張されている点に，独立共犯としての特徴がある。また，立案担当者によれば，助長罪には，不正アクセス行為を「容易にすること」の認識を不要とする点にも，他の独立共犯とは異なる特徴があるとされる[64]。しかし，同罪が，当該行為の助長を処罰根拠とすることからすれば，このような解釈が必然とはいえないであろう。

いずれにしても，不正アクセス罪との関係で，処罰の拡張を図る規定と位置付け得る以上，同罪の立法は，立法政策として必ずしも不当とはいえないであろう。それゆえ，「個人情報の保護の問題と情報処理上の阻害行為の問題とを混同する」との批判は[65]，適切ではない。もっとも，予備罪的構成によれば，同罪は，いわば犯罪の予備の幇助を処罰する規定となる。その意味では，過度の処罰の拡張との批判が向けられる余地もあろう。

ところで，上述のように，不正アクセス罪は，偽造の罪との罪質の共通性を指摘し得るところ，本法における提供は，偽造の罪でいえば，支払用カード電磁的記録不正作出準備罪における電磁的記録の「情報」の「提供」（刑法 163 条の 4 第 1 項）に類似する行為である。しかし，同罪における「提供」が，不正作出の「用に供する目的」での「取得」に向けられた行為として規定されていることからすれば，それは，供用（163 条の 2 第 2 項）の前段階に位置付けられる不正作出（同条 1 項）の，さらに前段階に位置付けられることとなる。それゆえ，上述のように，不正アクセス行為が供用に対応する行為と解し得ることからすれば，同罪における「提供」と本法における提供とは，異なる段階に位置付けられることとなろう。

---

63) 『逐条』84 頁以下。セキュリティ・ホールに関する情報の提供やクラッキング・ツールの頒布等の他の助長行為については，「不正アクセス行為からの防御措置を施すことに資するという正当な目的で行われている場合も少なくない」ことを理由に，禁止の対象とされなかった。同旨，園田ほか・前掲注 19）〔露木康浩発言〕20 頁。なお，園田・前掲注 55）210 頁は，前者は不正アクセス罪の教唆犯となり得るとする。

64) 『逐条』86 頁以下。

65) 石井・前掲注 12）12 頁。

むしろ，本法における提供は，偽造された通貨や有価証券の「交付」（刑法 148 条 2 項，149 条 2 項，152 条，163 条）及び不正作出された電磁的記録をその構成部分とする支払用カードの「譲り渡し」ないし「貸し渡し」（163 条の 2 第 3 項）に対応する行為といえる[66]。もっとも，客体が無体物である点で共通していることもあり，本法における提供について，偽造の罪における「提供」に係る解釈が援用されることが多い[67]。これらは，本法と偽造の罪との罪質並びに行為態様及び客体の類似性に由来するから，本法の法益理解とは直接の関係はない。それゆえ，予備罪的構成によっても，偽造の罪の解釈を援用することが可能である。

なお，本法制定当初は，提供には，「その識別符号がどの特定電子計算機の特定利用に係るものであるかを明らかにして，又はこれを知っている者の求めに応じて」為されたという要件が付されていた（本法旧 4 条）。すなわち，受領者において当該符号を利用すべき対象となる電子計算機が明らかである場合でなければ，容易に不正アクセス行為を実行することができないから，助長にあたらないというのである[68]。しかし，上述の連続自動入力プログラムによる不正ログイン攻撃の登場等により，その容易性に変化が生じたとの認識から，今回の改正で当該要件が削除され，提供一般が禁止の対象となった[69]。同罪が不正アクセス行為の助長を処罰根拠としており，その評価が当該行為の容易性に由来する以上，この改正については，必ずしも理由がないとはいえないであろう。

また，制定当初は，「当該アクセス管理者がする場合又は当該アクセス管理者若しくは当該利用権者の承諾を得てする場合」が除外されていた（本法旧 4 条ただし書）。すなわち，これらの場合，提供に「通常，何らかの正当な理由がある」ことに加え，「通常，これを特定電子計算機に入力して当該識別符号に係る特定利用を行うことも承諾したものと考えられ」ることから，不正アクセス

---

66) さらに，同じく偽造の罪との類似性が指摘されている不正指令電磁的記録に関する罪における，コンピュータに不正な指令を与える「電磁的記録」等の「提供」（168 条の 2 第 1 項）にも対応する。

67) 『逐条』90 頁。大塚仁ほか編『大コンメンタール刑法 第 8 巻［第 2 版］』〔井上宏〕（青林書院，2001 年）382 頁参照。

68) 不正アクセス対策法制研究会編著『逐条不正アクセス行為の禁止等に関する法律［補訂第 2 版］』（立花書房，2010 年）93 頁以下。

69) 『逐条』87 頁。

行為にも，その助長にもあたらないというのである[70]。今回の改正では，これに代えて，「業務その他正当な理由による場合」の除外が規定されることで，より一般的な正当化規定が創設されたといえる。

しかし，改正前の除外範囲は，必ずしも，行為の正当性のみに由来するとはいえない。例えば，上述のように，不正アクセス行為における同様の除外規定については，法益侵害性ないし被害者の承諾論との関係で，これを基礎付ける解釈もあり得る。その趣旨が「助長する行為」における除外規定にも及ぶとすれば，改正後の規定においても，これを含み得る除外範囲が設定されるべきであったといえよう[71]。他方で，確かに，「社会通念上，正当と認められるような場合」は改正前の除外範囲以外にも想定され得るところ[72]，正当化すべき行為を過不足なく類型化することは困難であるから，立法技術的には，規範的判断に期待し，「正当」といった文言に頼らざるを得ないことも理解できる。しかし，既に「正当な業務による行為」の不処罰を定めた総則規定（刑法 35 条）がある以上，同様の文言を重ねて規定することに意味はない。処罰範囲の明確性の観点からは，あくまでも各論的に，正当化すべき行為を可能な限り類型化する努力をすべきといえよう[73]。

同罪の法定刑については，提供の際に「相手方に不正アクセス行為の用に供する目的があることの情を知って」いたとの要件（以下，「知情要件」という）が充足された場合（本法 12 条 2 号）と，充足されなかった場合（13 条）とで差が設けられた（前者が 1 年以下の懲役又は 50 万円以下の罰金，後者が 30 万円以下の罰金）。立案担当者によれば，これは，提供が「その外形的行為自体に不正アクセス行為を助長する高度の危険性が認められる」にもかかわらず，両者の間に「加えるべき法的非難の程度」に差があることを理由とした改正とされる[74]。その趣旨は

---

70) 不正アクセス対策法制研究会編著・前掲注 68）96 頁以下。『逐条』92 頁参照。

71) なお，その趣旨は，提供の相手方からアクセス管理者及び利用権者が除外されていることにも現れている。『逐条』89 頁以下参照。

72) 『逐条』91 頁以下。例えば，「情報セキュリティ業者がインターネット上に流出している識別符号のリストを契約している企業に提供する行為」や「よく用いられがちな単純な ID・パスワードを設定すべきでないものとして示す行為」等が挙げられている。

73) なお，不正指令電磁的記録に関する罪における「正当な理由がないのに，」という文言についても同様のことを指摘し得る。渡邊・前掲注 54）30 頁参照。

74) 『逐条』91 頁，151 頁。

必ずしも明らかではないが，旧規定の法定刑が後者と同一であったことに鑑みれば，知情要件には，法定刑の差を基礎付けるに足りるだけの理由が必要であろう。

この点，例えば，偽造の罪においても，上述の「交付」等について，「行使の目的」ないし「財産上の事務処理を誤らせる目的」が要求されている[75]。しかし，知情要件は，他人の供用目的を認識していたことを示すに過ぎないから，偽造の罪における，自ら供用目的がある場合の加重根拠を援用することは困難である。他方で，その認識内容は，いわゆる幇助の故意に類似するから[76]，知情要件が充足された場合の法定刑を設定するにあたっては，不正アクセス罪の従犯の刑を基準とし得る。その上で，上述のように，助長罪は，独立共犯である点で従犯よりも当罰性が低いといえるから，それよりも軽い法定刑を設定すべきこととなろう。これに対して，知情要件が充足されなかった場合については，その程度の認識内容では充分な「法的非難」が基礎付けられないから，さらに軽い法定刑を設定すべきこととなろう。それゆえ，その意味では，妥当な法定刑が設定されたといえよう。

もっとも，提供が不特定又は多数の者に対して行われる場合を含むとされていることに鑑みれば[77]，個別の「不正アクセスと同等か，あるいはそれ以上に」法益侵害性が強い場合もあり得る[78]。このような観点からすれば，そのような形態の提供が類型的に多数と認められる限度で，法定刑の設定を再考する余地もあろう。

---

75) 不正指令電磁的記録に関する罪においても，「実行の用に供する目的」が要件とされている。
76) 『逐条』149 頁参照。
77) 『逐条』90 頁。もっとも，例えば，児童買春，児童ポルノに係る行為等の処罰及び児童の保護等に関する法律においては，児童ポルノの「不特定若しくは多数の者」に対する提供（同法 7 条 4 項）が別に規定されていることから，その単なる「提供」（同法 7 条 1 項）とは，特定かつ少数の者に対する行為を意味すると解されている。
78) 改正前の規定について，岡田・前掲注 36）120 頁，同・前掲注 3）35 頁。同旨，園田ほか・前掲注 19）〔園田寿発言〕20 頁。園田・前掲注 55）219 頁も，「セキュリティの高さで対抗できるものではな」いから，「当罰性の評価については今後に問題を残すもの」としていた。同旨，岡田・前掲注 2）20 頁。

３　識別符号取得罪及び保管罪

今回の改正により，不正アクセス行為の「用に供する目的」での識別符号の「取得」や「保管」についても，新たに禁止された上で（本法 4 条，6 条），処罰の対象とされた（12 条 1 号，3 号。以下，「識別符号取得罪」及び「識別符号保管罪」という）。立案担当者によれば，その趣旨は，助長罪と同様である。すなわち，不正アクセス行為禁止の実効性を確保するためには，識別符号の不正流出，不正流通を防止する必要がある。そこで，従来から規制されていた識別符号の提供に加え，その取得及び保管を含めた「不正アクセスに至る一連の行為」を禁止することとした[79)]。

このように，取得及び保管は，不正アクセス行為の準備行為の一部といえる[80)]。すなわち，不正アクセス罪との関係で，処罰の早期化を図る規定と位置付け得る以上，これらの罪の立法は，立法政策として必ずしも不当とはいえないであろう。これらの罪において，供用目的が要件とされている点も，これを補強するといえる。もっとも，ここでの供用目的は，「識別符号の転得者が不正アクセス行為に及ぶ可能性があることを認識しつつ，当該識別符号を第三者に提供する目的」も含むと解されている[81)]。すなわち，取得及び保管は提供の前段階の行為ともいえるから，これらの罪は，助長罪との関係でも処罰の早期化を図る規定といえる。それゆえ，予備罪的構成によれば，これらの罪は，いわば犯罪の予備の幇助の予備を処罰する規定となり得る。したがって，過度の処罰の拡張との批判が向けられる余地もあろう。

ところで，取得及び保管は，偽造の罪でいえば，支払用カード電磁的記録不正作出準備罪における電磁的記録の「情報」の「取得」（刑法 163 条の 4 第 1 項）及び「保管」（同条 2 項）に類似する行為である。しかし，同罪における「取得」

---

79) 『逐条』79 頁以下，93 頁。なお，フィッシングについては，後述の識別符号入力要求罪による規制が，コンピュータ・ウィルスを添付したメールを送付し，これを感染させることにより機密情報を外部に送信させる等の被害を与える，いわゆる「標的型メール攻撃」については，不正指令電磁的記録に関する罪による規制が予定されている。

80) また，後述の識別符号入力要求罪との関係では，同罪の実行後に不正アクセス行為に至る過程において想定される行為が犯罪化されたともいえる。なお，岡田・前掲注 36）134 頁，同・前掲注 3）33 頁は，識別符号の「探知行為」との関連で，「不正入手」の犯罪化を提案していた。

81) 『逐条』81 頁，93 頁。

が，不正作出の「用に供する目的」を要件としていることからすれば，それは，供用の前段階に位置付けられる不正作出の，さらに前段階に位置付けられることとなる。それゆえ，不正アクセス行為が供用に対応する行為と解し得ることからすれば，偽造の罪における「取得」と本法における取得とは，異なる段階に位置付けられることとなろう。この点は，「保管」についても同様である。

むしろ，本法における取得及び保管は，偽造された通貨の「収得」（刑法 150 条）及び不正電磁的記録カードの「所持」（163 条の 3）に対応する行為といえる[82)]。もっとも，客体が無体物である点で共通していることもあり，本法における取得及び保管について，偽造の罪における「取得」及び「保管」に係る解釈が援用されることが多い[83)]。これらは，本法の法益理解との直接の関係はないから，予備罪的構成によっても，偽造の罪の解釈を援用することが可能である。

これらの罪の法定刑については，知情要件を充足した場合の助長罪と同一とされた（1 年以下の懲役又は 50 万円以下の罰金）。立案担当者によれば，これは，不正アクセス行為の準備行為として，不正アクセス罪の法定刑を参酌したものとされる[84)]。上述のように，これらの罪と助長罪とでは，後者が不正アクセス行為の幇助的な行為と解される点で，準備行為としての位置付けが異なるから，このような法定刑の設定は必然ではない。また，これらの罪は，助長罪との関係でも処罰の早期化を図る規定といえるから，この点も考慮する必要があろう。もっとも，不正アクセス罪の予備罪的行為を含み得る以上，その法定刑を参酌して上限を定めたこと自体は妥当といえよう。

---

82) さらに，同じく偽造の罪との類似性が指摘されている不正指令電磁的記録に関する罪における，電磁的記録等の「取得」及び「保管」（168 条の 3）にも対応する。なお，偽造の罪における「収得」及び「所持」については「行使の目的」ないし「財産上の事務処理を誤らせる目的」が，不正指令電磁的記録に関する罪における「取得」及び「保管」については「実行の用に供する目的」が要件とされている。

83) 『逐条』83 頁，96 頁。大塚ほか・前掲注 67）〔井上宏〕382 頁参照。ただし，本法における取得については，媒体に記録された状態での情報の取得のみならず，「識別符号を知得する行為（再現可能な状態で記憶する行為）」も含むとされている。

84) 『逐条』148 頁。

４　識別符号入力要求罪

また，今回の改正により，アクセス管理者に「なりすまし」，その他当該アクセス管理者であると「誤認させて」，利用権者に対して「識別符号を特定電子計算機に入力することを求める旨の情報」を，「電気通信回線に接続して行う自動公衆送信」を利用して「公衆が閲覧することができる状態に置く」こと（サイト構築型）及び「電子メール」により当該利用権者に「送信する」ことも（メール送信型），新たに禁止された上で（本法 7 条。以下，「入力要求」という），処罰の対象とされた（12 条 4 号。以下，「識別符号入力要求罪」という）。立案担当者によれば，同罪制定の趣旨は，以下のようなものである。すなわち，近年，フィッシングが識別符号の取得手段として多用されているところ[85]，犯罪の防止及び秩序の維持という本法の目的を達成するために，これを禁止することとした[86]。

このように，入力要求は，フィッシングを類型化したものであり，それは，識別符号の取得のため，これを利用権者から提供させることを誘引する行為といえる。すなわち，識別符号取得罪との関係で，処罰の早期化を図る規定と位置付け得る以上，識別符号入力要求罪の立法は，立法政策として必ずしも不当とはいえないであろう。もっとも，予備罪的構成によれば，同罪は，いわば犯罪の予備の予備の予備を処罰する規定となる。また，上述のように，識別符号取得罪は，助長罪との関係でも処罰の早期化を図る規定といえるから，識別符号入力要求罪は，いわば犯罪の予備の幇助の予備の予備を処罰する規定となり得る。それゆえ，例えば，偽造の罪における「行使の目的」ないし供用目的に対応する要件がないことに鑑みれば，過度の処罰の拡張との批判が向けられる余地もあろう[87]。

---

85) 例えば，他人の開設したサイトへのログイン画面を無断で複製し，それによって得た他人の識別符号を用いて不正アクセス行為を行った上で，他人のメールをのぞき見るなどしたという事案について，東京地判平成 17 年 9 月 12 日<LEX/DB 28135296>は，不正アクセス罪の他，ログイン画面が複製されたことを捉えて，著作権侵害罪（著作権法 119 条 1 項）の成立を認めた。しかし，同罪は，本法とは目的が異なり，入力要求自体を処罰するものではない。『逐条』100 頁，岡田・前掲注 3）29 頁以下参照。

86) 『逐条』97 頁以下。これに対して，岡田・前掲注 2）21 頁以下は，現行規定では処罰の間隙が生じ得るとして，さらなる改正が必要とする。

87) ただし，行為者には，「利用権者を誤認させようとする意図」は必要とされる。『逐条』101 頁参照。なお，偽造の罪においては，入力要求に対応する行為は規制されていない。

この点，立案担当者によれば，「フィッシング行為自体が有する危険性と悪質性」が，目的要件がない理由とされる[88]。その趣旨は必ずしも明らかではないが，例えば，サイト構築型のように，「公衆」に向けられた入力要求の場面では，相手方が不特定又は多数に及ぶことから影響範囲が広範となり得る。メール送信型であっても，不特定又は多数の者が相手方となることもあり得る。これらが他の準備行為と異なる特徴であって，そのことが，処罰範囲の限定を必要としない理由ということも可能かも知れない。

なお，入力要求についても，「アクセス管理者の承諾を得てする場合」が除外されている（本法7条ただし書）。立案担当者によれば，これは，フィッシング行為に対処するための「訓練」や「注意喚起」のための行為を除外する趣旨とされる[89]。すなわち，行為の正当性が除外の根拠とされているといえる。これに対しては，「助長する行為」における除外規定の場合と同様の批判が可能である。

同罪の法定刑については，識別符号取得罪との関係で処罰の早期化を図る規定と位置付け得るにもかかわらず，その「危険性と悪質性」を理由として，同罪よりも軽く設定する必要はないとされ[90]，同一の法定刑が規定された（1年以下の懲役又は50万円以下の罰金）。しかし，上述のように，そのような理由は，既に目的要件がない理由として挙げられているから，それを再び法定刑の高さを説明する場面で主張し得るかについては，疑問の余地があろう。

Ⅳ　結　語

以上のように，今回の改正は，不正アクセス行為自体についてはその内容を維持した上で，これを助長する行為における限定を解除し，また，これらの行為についての処罰を早期化する規定を新設することによって，処罰の大幅な拡

88) 『逐条』99頁。
89) 『逐条』105頁。なお，同・98頁では，このような場合を除いて「何らの社会的有用性が認められない」ことも，犯罪化の理由とされている。これに対して，岡田・前掲注2）32頁は，「行為反価値性」を理由とすべきではないと批判する。
90) 『逐条』99頁，150頁。

張を行うものである。法定刑が全体的に引き上げられたことも考え合わせると，今回の改正からは，不正アクセス行為を是が非でも抑止したい，という意識が見てとれる。

しかし，その前提となる，不正アクセス罪の罪質の理解については疑問がある。上述のように，それは予備罪的構成と信頼保護構成とに整理し得るが，後者の構成は，情報窃盗等の実害を捕捉する罪が存在しない現状において，法益論において体裁を整えることで，予備罪的構成の実質を隠蔽したに過ぎないといえる。また，不正アクセス行為ないしこれを助長する行為の処罰を早期化する規定についても，過度の処罰の拡張との批判が向けられる余地があることに加えて，それらの規定における具体的要件の位置付けや法定刑の設定の趣旨について，必ずしも明確ではない点が見受けられる。

したがって，不正アクセス罪の罪質に関する議論を踏まえた上で，本法における妥当な処罰範囲ないし適切な刑罰とは如何なるものであるのかを，改めて検討すべきである。そして，その際には，捕捉する罪が存在しない実害についても，犯罪化の是非を検討する必要があろう。

※ 本稿は，科学研究費補助金（基盤研究(C)）「サイバー犯罪に関する国際的対応と情報刑法の体系化」（研究課題番号 24530067）における，研究成果の一部である。