HOKKAIDO UNIVERSITY

Title	個人情報の刑法的保護の可能性と限界について(1)
Author(s)	佐藤, 結美
Citation	北大法学論集, 65(3), 300 [1]-259 [42]
Issue Date	2014-09-30
Doc URL	https://hdl.handle.net/2115/57030
Type	departmental bulletin paper
File Information	lawreview_vol65no3_Part5.pdf

Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP

論　　説

個人情報の刑法的保護の可能性と限界について（1）

佐　藤　結　美

目　　次

第１章　はじめに
　第１節　問題の所在
　第２節　研究方法

第２章　日本法における個人情報保護の現状
　第１節　秘密漏示罪
　第２節　信書開封罪
　第３節　支払用カード電磁的記録不正作出準備罪
　第４節　不正指令電磁的記録に関する罪
　第５節　不正アクセス禁止法
　第６節　個人情報保護法
　　第１項　成立過程と概要
　　第２項　刑罰に関する議論
　　第１款　個人情報保護検討部会の議論
　　第２款　個人情報保護法制化専門委員会の議論
　　第３款　「個人信用情報保護・利用の在り方に関する懇談会」報告書
　第７節　小括　　（以上、本号）

第３章　イギリス法における個人情報保護
　第１節　1998年データ保護法の概要
　第２節　個人データの不法な取得等に対する直接罰規定について
　第３節　情報コミッショナーによる個人情報保護の現状について

第４節　センシティブな個人データ（sensitive personal data）に関する法的規制
第５節　小括

第４章　フランス法における個人情報保護
第１節　1978年情報処理・情報ファイル及び諸自由に関する法律の概要
第２節　刑事罰について
第３節　CNIL による制裁について
第４節　小括

第５章　ドイツ法における個人情報保護
第１節　連邦データ保護法の概要について
第２節　データ保護法における過料と刑事罰について
第３節　監督官庁による規制の実態
第４節　小括

第６章　保護法益としての個人情報と規制方法
第１節　個人情報の法益性
第２節　個人情報の侵害に対する妥当な規制のあり方
第３節　小括

第７章　おわりに

第１章　はじめに

第１節　問題の所在

本研究は、個人情報それ自体を刑法における保護法益として捉えることが可能であるか、そして、個人情報が保護法益たり得るとすれば、どのような保護が妥当であるかということについて検討するものである[1]。

[1] 従来の先行研究では、財産的な性質を有する情報の保護について議論が行われてきた。そのような情報の一例として、営業秘密の刑法的保護という問題も

「個人情報保護」の重要性は誰もが賛同するものであるが、個人情報保護の妥当な在り方については明確な方針が定まっていない。企業や学校から氏名や住所などの個人情報が漏洩する事件が繰り返し発生している一方で、そのような事件の多発を受けて「個人情報保護」を理由とした過度の情報の秘匿などといった「過剰反応」も見られる。このように、個人情報を取り巻く状況は二極化している。日本の個人情報保護法制において、どのような情報がどのように保護されるべきなのか、情報の取り扱いがどのように規制されるべきなのかということについての議論が曖昧で不十分だからではないだろうか。

では、日本の現行法において個人情報はどの範囲で保護されているのか。例えば、刑法134条の秘密漏示罪は、「医師、薬剤師、医薬品販売業者、助産師、弁護士、弁護人、公証人又はこれらの職にあった者」と「宗教、祈祷若しくは祭祀の職にある者又はこれらの職にあった者」が「正当な理由」なく「その業務上取り扱ったことについて知り得た人の秘密を漏らした」場合に処罰するという方法により、限定された状況下で個人情報の保護を行っている。第２章第１節で後述するように、刑法134条以外にも、特別法によって様々な職業の者について刑罰を伴う守秘義務が規定されており、個人の秘密は広く保護されているように見える。しかし、これらはいずれも身分犯であり、何らかの方法によって守秘義

興味深いテーマではあるが、本論文で扱う対象は個人情報に限定する。

営業秘密の刑法的保護についての代表的な研究としては、加藤佐千夫「刑事罰による営業秘密の保護と不正競争防止法の変遷」中京法学44巻３・４号（2010年）263 ～ 289頁、「企業秘密の刑法的保護（１）（２）」名古屋大学法政論集116号（1987年）207 ～ 242頁、117号（1987年）283 ～ 316頁、「企業秘密の刑法的保護・再論―財産犯的構成の批判的検討を通して」名古屋大学法政論集127号（1989年）107 ～ 131頁、山口厚「営業秘密の侵害と刑事罰」ジュリスト962号（1990年）45 ～ 51頁、「営業秘密の刑事罰による保護」NBL820号（2005年）12 ～ 18頁、佐久間修『刑法における無形的財産の保護―企業秘密、コンピュータ・データを中心として―』（成文堂・1991年）、一原亜貴子「不正競争防止法による営業秘密の刑事法的保護」商学討究56巻２＝３号（2005年）279 ～ 301頁、「営業秘密侵害罪の保護法益」商学討究59巻４号（2009年）165 ～ 197頁、「営業秘密侵害罪に係る不正競争防止法の平成二一年改正について」岡山大学法学会雑誌60巻３号（2011年）477 ～ 494頁などがある。

務者から秘密を知った第三者がそれを他人に漏らし、その結果として個人に不利益がもたらされたとしても、刑法134条等に規定されている主体ではない以上、共犯でない限り処罰することはできない。

続いて、2003（平成15）年に制定された個人情報保護法では、民間部門の個人情報取扱事業者に対して、個人情報に関する義務違反行為を直接的に処罰するという直罰方式ではなく、主務大臣の命令に違反して初めて処罰されるという間接罰方式を採っている。

個人情報保護法における「個人情報」の定義は幅広く、様々な情報を含んでいることから、個人情報に関する義務違反行為を一律に直接処罰する方式を採らなかったことは、その限りでは了解可能な帰結であると思われる。しかし、「個人情報」と一口に言っても、氏名・住所・電話番号・生年月日といった基本的な情報から、職業・年収・信用情報・学歴・趣味嗜好といった、特に他人に知られることを欲しないような情報まで多岐にわたっているので、本来であれば、そのような情報の性質によって保護の在り方が異なるべきものである。また、個人情報保護法における個人情報取扱事業者の義務も多岐にわたっており、情報の利用目的の明確化や情報の不正取得の禁止、情報管理や従業員の監督といった様々なものがある。このように、個人情報保護法が間接罰の対象とする「個人情報保護における義務違反についての主務大臣の命令に対する違反」という行為の範囲も幅広いものになっていることから、重要性の低い情報に対する比較的軽微な侵害も、重要性の高い情報に対する重大な侵害も一律に、主務大臣の命令とその違反に対する罰則という扱いを受け得ることになり、均衡を失するのではないかと考えられる。

以上のように、日本の現行法は個人情報を重要なものとして保護する姿勢を採りつつも、保護の仕方が断片的であり、個人情報それ自体を保護法益とするという考え方には至っていないと思われる。一般法であるはずの個人情報保護法も、情報の性質や重要性、情報侵害の行為態様に着目することなく、「個人情報保護における義務違反」「主務大臣の命令に対する違反」という抽象的な概念によって情報侵害を規制しようとしているので、個人情報の漏洩や売買といった問題に対して効果的に対処することが困難になっている。

昨今では、企業による個人情報の大規模な流出事件が多発しており、

個人情報の流出・漏洩自体による直接的な被害の他、漏洩した情報が他の犯罪に利用されるといった二次被害の発生も否定できない。情報漏洩について、企業が損害賠償責任を負うケースも見られるが、損害賠償責任を課され得るという可能性が、どの程度の抑止力になっているのかという疑問がある[2]。

このように、日本の現行個人情報保護法には情報の漏洩や窃盗などを直接的に処罰する規定は存在しないが、情報の売買や窃盗といった不正な取り扱いを処罰するための試みとして、情報の不正収集を財産犯によってカヴァーするという考え方が判例によって示されている。

まず、大日本印刷事件[3]は、被告人が稟議決裁一覧表の原本を社内で借りて、これを会社のコピー用紙に複写して、そのコピー用紙を持ち出した行為が、窃盗罪に問われた事案である。東京地裁は、「当初からの意図のとおり大日本印刷内で、ほしいままに、同社の機密書類を同社所有のコピー用紙に同社の複写機を使って複写し、これを社外に持ち出したものであるから、全体的にみて、単なるコピー用紙の窃取ではなく、同社所有の複写した右稟議決裁一覧表を窃取したものと認めるのが相当である」としている。コピー用紙それ自体の財物としての価値は低いので、単なるコピー用紙の窃盗であれば可罰的違法性が否定され得るが、情報を入手するという被告人の意図が重視されている。

続いて、新薬産業スパイ事件[4]は、製薬会社の代表取締役社長と顧問が、

---

[2] 今井猛嘉「刑法における情報の保護」『刑法の争点（新・法律学の争点シリーズ２）』（2007年）163頁も、個人情報が刑法典における保護の対象となっていないという立法の在り方は、①個人情報やプライヴァシーの価値が十分に議論されていなかったこと、②個人情報に対する重大な侵害が想定できなかったことに由来しているものの、現在ではインターネット等を通して、民事的制裁では対応しきれない重大な侵害が容易になされ得るので、新たな検討が必要であると述べている。

[3] 東京地判昭和40年６月26日判時419号14頁。

[4] 東京地判昭和59年６月28日判時1126号６頁。他にも、会社の機密資料である調査資料購読会員名簿をコピーするため、名簿を一時的に社外に持ち出した行為が窃盗罪に当たるとされた東京地判昭和55年２月14日判時957号118頁（建設調査会事件）と、区役所内での閲覧が許されている住民基本台帳閲覧用マイク

他の会社の新薬開発研究の成果を不正に入手するために、国立予防衛生所の厚生技官に、秘密資料を持ち出させてコピーを採らせ、もとの場所に戻させたというものである。東京地裁は、「情報の化体された媒体の財物性は、情報の切り離された媒体の素材だけについてではなく、情報と媒体が合体したものの全体について判断すべきであり、ただその財物としての価値が、主として媒体に化体された情報の価値に負うもの」であるとして、コピー用紙に財物性を認めている。

このように、判例は「情報窃盗」といえる行為を処罰するために、情報の化体された媒体に財物性を認めて、これに対する窃盗を認めているが、学説はこのような判断に対して、可罰的違法性の理論でいえば単なる紙の窃盗は不可罰となることと矛盾すると批判している[5]。情報は他の財物や財産上の利益と異なり、移転しないということと、他人に情報を入手されたとしても、情報の持ち主がその情報を失うわけではないという特殊性があることから、情報を財産犯の枠組みで保護することの困難性が指摘されている[6]。

判例は窃盗罪以外にも、横領罪・背任罪の枠組みで情報の不正取得を

ロフィルムを、正規の手続きで借り出した上、区役所外に無断で短時間持ち出した行為につき窃盗罪の成立が肯定された札幌地判平成５年６月28日判タ838号268頁がある。

[5] 藤木英雄「産業スパイと刑事責任」ジュリスト428号（1969年）34 ～ 35頁。

[6] 西田典之「財産的情報の刑法的保護―共同研究の基本的視点とまとめ―」刑法雑誌30巻１号（1989年）６頁、松原芳博「情報の保護」法学教室298号（2005年）54頁。また、キャッシュカードの暗証番号を脅迫により聞き出す行為につき２項強盗罪の成否が争われた事件の原審さいたま地川越支判平成20年６月１日（公刊物未搭載）においても、刑法236条２項の「財産上不法の利益」は移転性のある利益に限られるが、被告人がキャッシュカードの暗証番号を聞き出したとしても、暗証番号に関する情報が被告人と被害者との間で共有されるだけで、被害者から失われるわけではないと判断され、このような情報の非移転性と非喪失性を根拠に、236条２項における利益性が否定される結果となった（なお、２審の東京高判平成21年11月16日判タ1337号280頁では、情報の非移転性と非喪失性という性質そのものについては特段の言及をせず、被告人はキャッシュカードと暗証番号を併せ持つことによって預貯金を引き出し得る地位を得たとして、２項強盗罪の成立が肯定された）。

カヴァーすることを試みている。まず、横領罪の成否が問題となった事件に、新潟鉄工事件がある[7]。本件は、新潟鉄工の社員が、会社内において自分で保管していた秘密資料を、退職後に新しい会社で利用するためにコピーを作成しようと考え、社外に持ち出してコピーをした後、元に戻しておいたというものである。この事案につき東京地裁は、「内容自体に経済的価値があり、所有者以外の者が許可なくコピーすることの許されない機密資料をコピー目的で許可なく持ち出す行為には、その間の所有者を排除して資料を自己の所有物と同様にその経済的用法に従って利用する意思が認められ、使用後返還する意思があったとしても、不法領得の意思が認められる」として横領罪の成立を肯定した。

このように、財物を一時的に持ち出す「使用窃盗」の事例において不法領得の意思が認められるか否かについては、不法領得の意思がないとして窃盗罪の成立を否定した下級審裁判例[8]が存在するものの、最決昭和55年10月30日刑集34巻５号357頁は、財物の返還意思があったとしても不法領得の意思が存在するとして、窃盗罪の成立を肯定した。新潟鉄工事件判決は、返還意思を考慮しないという点で前述昭和55年決定と共通しており、その後の判例[9]により「経済的用法に従って利用する意思」という要件が緩和され、「何らかの効用を享受する意思」があれば足りると解された。しかし、「単に『資料をコピーする意思』だけでは、『資料を読んで記憶する意思』『資料の写真を撮る意思』と異ならず、『資料

[7] 東京地判昭和60年２月13日刑事裁判月報17巻１＝２号22頁。他の事例として、勤務会社からの退社時に、自己の業務において保管していた機密の薬品と、秘密書類としていた「各種文献ファイル」１冊を持ち出す行為につき、業務上横領罪の成立が肯定された大阪地判昭和42年５月31日判タ209号260頁（鐘淵化学事件）がある。また、神戸地判昭和56年３月27日判時1012号35頁（東洋レーヨン事件）では、会社の製造部工務技術課員である被告人が、職務上の参考資料として利用するため上司から預かって保管していた秘密資料１冊を100万円で他社に売却した行為について、背任罪ではなく業務上横領罪の成立が肯定されている。

[8] 京都地判昭和51年12月17日判時847号112頁。

[9] 東京地判昭和62年10月６日判時1259号137頁。

の効用を享受する意思』にまでは至っていない」[10]。このことから、新潟鉄工事件判決においても、事案に即して、「資料をコピーし、それによって得られた内容を当面の販売業務に利用する意思」をもって利用・処分意思を認定すべきであったと指摘[11]されている。このように、「不法領得の意思」の解釈如何によっては、窃盗罪・横領罪の成立が否定され得る。

そして、背任罪の成否が問題となったものとして綜合コンピュータ事件[12]がある。この事案は、コンピュータ・ソフトウェアの開発販売等の会社に勤務する被告人が、会社が新聞販売店用に開発した購読者管理システムのプログラムを同社の顧客である新聞販売店に設置されるコンピュータに入力して、その使用方法について技術指導するなどの業務を行っていたところ、会社に無断で、ある新聞販売店と契約し、そのコンピュータにプログラムを入力して、プログラム代金を受け取ったというものである。この事案は資料の持ち出しの場合とは異なり、会社のプログラムを入力しただけであるので、窃盗罪も横領罪も成立し得ない。そこで、東京地裁は被告人の行為につき、「プログラムの入力使用等に当たっては、同社が業務として同社の顧客方に設置するオフィスコンピューターに対してのみ、右フロッピーシートを使用するなど、同社のために忠実にその業務を遂行すべき任務があった」として、任務違背行為により背任罪が成立すると判断した。

綜合コンピュータ事件のように、窃盗罪や横領罪が成立しない場合でも、背任罪の成立を認められる場合があるものの、当該情報の管理を業務としていない一般従業員は背任罪の主体にはなり得ず、まして外部者は対象とならないという点で、背任罪の成立を認めることができるのは例外的な場合に限られる[13]。そして、背任罪が成立するには、財産上の損害の発生が必要であるので、財産的価値に換算することのできない情

[10] 城下裕二「判批」別冊ジュリスト『刑法判例百選Ⅱ各論（第６版）』（2008年）133頁。松原・前掲注（６）58頁、内田文昭「秘密資料の無断持ち出しと窃盗罪」判タ538号（1984年）47頁も同趣旨。

[11] 城下・前掲注（10）133頁。

[12] 東京地判昭和60年３月６日判時1147号162頁。

[13] 佐伯仁志「刑法による情報の保護」宇賀克也・長谷部恭男（編）『情報法』（有斐閣・2012年）241頁。

報の場合には、財産上の損害を認めることができない[14]。したがって、企業秘密等に該当しない単なる個人情報の場合には、財産上の損害を肯定することは容易ではないだろう。

これらの財産犯の判例は、事案によって限界はあるものの、情報が紙やフロッピーといった有体物に化体されているケースの解決としては、一定程度の意義を有している。しかし、有体物に化体されていない情報を不正に収集等する行為自体を窃盗罪・横領罪によってカヴァーすることはできず、背任罪によって捕捉可能な範囲も限られている。さらに、情報そのものには「非移転性」と「非喪失性」という特殊な性質があることから、従来の刑法の解釈によって個人情報それ自体の窃盗や漏洩などを処罰可能なものとするのは困難である。そして、当該個人情報の重要性と侵害態様の強度によっては、主務大臣の命令に反して初めて刑罰を科されるという間接罰方式ではなく、直罰方式による処罰の必要性があると思われる。したがって、本研究では、個人情報を保護する刑事罰の可能性と限界について議論を進めることによって、個人情報の侵害に対する妥当な規制方法について検討する。

第２節　研究方法

本研究では、刑事罰を視野に入れつつ、個人情報の侵害に対する妥当な規制方法について検討するために、個人情報（データ）の不正な取り扱いを直接的に処罰する規定と、その他の規制方法（第三者機関による規制）を有する外国法の議論を参照する。まず第２章では、日本の現行法における個人情報保護の現状について概観することによって、現行法において個人情報の保護が不十分な領域を整理する。

続いて第３章では、イギリスの1998年データ保護法について検討する。イギリスのデータ保護法には、個人データの漏洩・窃盗などを直接処罰する規定が存在する。第４章では、フランス刑法における個人情報保護の規定と、情報処理・情報ファイルおよび諸自由に関する1978年の法律について扱う。フランス刑法には個人情報に対する様々な侵害行為が設

[14] 佐伯・前掲注（13）241頁。

けられており、1978年法において、第三者機関が個人情報の不正な取り扱いを規制することが定められている。

第５章では、ドイツ連邦データ保護法について検討する。ドイツ連邦データ保護法は、個人データを扱う機関が、違法または不当なデータの収集・処理・利用によって本人に損害を与えた時に、損害賠償の責任を負うことを規定している。この他に、故意または過失による個人データの様々な侵害行為は過料の対象になり、対価を得て、又は図利他害目的で個人データの侵害行為をした場合には、刑事罰の対象になることが規定されている。

第３章から第５章までは、比較対象としてイギリス・フランス・ドイツの法律を扱うが、この三国は個人情報（データ）の保護のために、直接の刑事罰以外にも第三者機関による監視といった刑罰以外の規制手段が講じられている点で共通している。そして、個人情報（データ）の中でも特に重要性の高い「センシティブ情報」という概念を別個に設けて、「センシティブ情報」の取り扱いを他の一般的な情報と区別している点も共通している。日本の個人情報保護法が「個人情報」の重要性によって情報の取り扱いを区別せず、個人情報の侵害行為につき直接罰ではなく間接罰で臨んでいることに比して、この三国では個人情報の多様な保護の方法が採られているが、これらの外国法の規定をそのまま日本法に導入することが妥当ではないことは論を俟たない。そこで、第３章から第５章において、英仏独の個人情報保護法制における処罰規定についての判例・学説・第三者機関による報告について触れ、各国において刑罰や第三者機関による規制がどの程度功を奏しているのかを検討する。

そして第６章では英仏独の議論を参照しつつ、（１）保護法益としての「個人情報」の定義と範囲、（２）英仏独における「センシティブ情報」のような法概念を取り入れるべきか否か、取り入れるとすればどのように定義するかということ、（３）個人情報の侵害の行為態様はどのようなものかということ、（４）個人情報の不正収集・利用等を直接処罰する必要性と、その条件という観点から、個人情報の侵害に対する妥当な規制方法を検討する。

第２章　日本法における個人情報保護の現状

本章では、日本の現行法の枠組みにおいて、個人情報や秘密がどの程度保護されているかということについて整理する。

第１節　秘密漏示罪

まず本節では、刑法134条の秘密漏示罪について扱う。

第１章第１節で述べた通り、医師や弁護士など、限定された職業の者が業務上知り得た人の秘密を正当な理由なく漏らす行為は秘密漏示罪として処罰される。その事実の内容を広く知られていないことと、本人が当該事実を秘匿する意思を有していること、それを秘匿する利益[15]が本人にある場合に、当該事実が秘密であると判断される。秘密の内容がどれほど重要なものであるとしても、134条所定の身分の者が漏示した場合でなければ処罰の対象とはならない。また、刑法134条に規定されていなくとも、国家公務員や看護師などの特定の職業の者が有する守秘義務についても、各々の職業に関する法律において規定されている[16]。

このように、個人の秘密や情報を取り扱う機会のある職業の多くは、刑法や他の関連法規によって刑罰を伴う守秘義務を課されているので、日常生活の様々な局面において、個人の秘密や情報は幅広く保護されているように見える。その一方で、秘密漏示罪に関連して、守秘義務の身分を持たない者による個人情報・秘密の公表が問題になり得るケースとして、最決平成24年２月13日刑集66巻４号405頁がある。

この事案は、精神科医である被告人が、現住建造物等放火・殺人等の少年Ａの保護事件につき、家庭裁判所から少年の精神鑑定を命じられて

[15] 山口厚『刑法各論（第２版）』（有斐閣・2010年）132頁など。

[16] 国家公務員法100条１項には、「職員は、職務上知ることのできた秘密を漏らしてはならない。その職を退いた後といえども同様とする」と規定されており、保健師助産師看護師法42条の２、地方公務員法34条１項、裁判員の参加する刑事裁判に関する法律108条１項から７項、司法書士法24条、柔道整復師法17条の２、自衛隊法59条１項、国立大学法人法18条、地方独立行政法人法50条１項等にも同様の規定がある。

その作業を進める中、ジャーナリストＣから取材を受け、その要求に応じて少年事件記録の写しや鑑定書等を閲覧させるなどしたことについて、刑法134条の秘密漏示罪が成立すると判断されたものである。本件においては、Ｃが被告人から入手した情報を基にして書籍を出版したことから、少年の事件に関する事実と、Ａと実父Ｂの関係等の家庭環境がさらに広く知られるところとなった。

まず、被告人の行為についての争点と裁判所の判示について見て行くこととする。本件において被告人は、被告人がＣに情報を提供したという外形的事実を認めたものの、①少年の鑑定人であった被告人は本罪にいう「医師」にあたらず、医師である鑑定人が行う場合でも、鑑定は本罪にいう「業務」に当たらない、②被告人は少年の利益を図るため、Ｃの行う取材に対する協力としてＣに供述調書等を閲覧させたのであるから、その目的は正当であり、手段も相当であるから、被告人の行為には「正当な理由」があり、違法性が阻却される等と主張した。

第１審（奈良地判平成21年４月15日刑集66巻４号440頁参照）は以下のように判示して、被告人につき懲役４月執行猶予３年の有罪判決を下した。

①まず、奈良地裁は「刑法134条１項が秘密漏示の主体として掲げる『医師』とは、医師国家試験に合格し、厚生労働大臣の免許を受けた者（医師法２条）をいうものと解されるところ、被告人がこの『医師』に当たることは……明らかである。……本罪の主体として掲げられている者は、弁護人が指摘するように、秘密の主体である相手方との信頼関係に基づき、相手方が自ら打ち明けたことによってその秘密を知るのが通常だといえるが、業務上取り扱ったことについて人の秘密を知り得たのであれば、相手方に意思能力がない場合や業務上必要な調査を行う過程で取得した内容がその相手方の秘密に当たる場合等、相手方の意思、相手方との信頼関係の有無や程度等にかかわらず、正当な理由がない限りその秘密を漏らすことは違法である」として、被告人が刑法134条１項にいう「医師」であることを肯定した。

続いて、被告人が行った精神鑑定の業務性については、「その免許を前提に、専門的知見及び経験に基づき継続的に行う事務に関して人の秘密を取り扱えば、『その業務上取り扱った』ものと解することができる

……そうすると、被告人がＡについて行った精神鑑定は、本罪における医師の『業務』に当たる」と判断した。

さらに、被告人が閲覧させた供述調書等の秘密性については、以下のように判断した。

②奈良地裁は、「本罪が個人の私生活上の秘密を保護法益とするものであることからすれば、本罪における『秘密』とは、一般に知られていない非公知の事実であって、これを他人に知られないことが本人の利益と認められるものをいう」と一般論を提示した上で、本件について、「本件保護事件は、少年事件として審判手続が進められているさなかにあり、Ａに対する審判結果も出されていなかったこと……からすれば……本件……各書面……については、その存在及び内容が一般には知られていなかったものと認められる」として、事実の非公知性を肯定する。その上で、「各書面は、Ａ、Ｂの家庭内に関する諸事情、Ａの生育歴や学校の成績、Ａの精神状態を判断するために行われた各種心理検査の結果やその所見、精神鑑定の内容となるＡの家族歴、本人歴や症状、診断等いずれもＡやＢのプライバシーに極めて深くかかわる個人的な事項を内容とするものであるから、これらは、一般的にみて何人も他人に知られることを欲しない事項といえ、他人に知られないことがＡ及びＢにとって利益である」として、供述書類等が本罪にいう「秘密」にあたることを認めた。

そして、被告人がＣに書類を閲覧させたことに「正当な理由」があったか否かについては以下のように判示している。

「被告人は、ＡやＢに関する報道内容に疑問を持っており、Ａに殺意がないことを対外的に明らかにしたいとの思いを抱いていたことは認められる。しかし、被告人は……自らが抱く問題意識や考え方を明確に示した上で、Ｃにその報道を求めたり、記事に関する提案を行ったりすることはなく、Ｃが自分の意図を理解し、誤った報道を正してくれると思っていたにすぎないのであり……被告人が抱く前記のような思いは、主観的なものにとどまっていた」と述べている。また、「被告人は、Ａの鑑定人としての立場にありながら……本件事件記録を、自ら立ち会わず、対象も何ら限定なしにＣらに自由に閲覧させ、さらには、解説書面や心理検査の結果等の書面を閲覧謄写させたり、鑑定書と同等の写しを交付したりしたのであって、被告人が抱いていた……思いは、その立場と相

いれず……Ａの利益にかなうものとはいえないばかりか……Ａ及びＢのプライヴァシー等の秘密に対する配慮を欠いた、非常に軽率な行為」であるとして、手段の相当性も否定した。

本判決は、被告人に係る「正当な理由」の有無について、「取材に応じ、あるいはこれに協力する者の行為が秘密漏示罪に該当するか否かの判断に当たっては、取材協力であることから直ちにその違法性が阻却されると考えるべきではなく、取材行為の目的、手段及び方法に係る正当性、取材協力行為を行った者の立場、目的、同行為の態様等と、漏示対象となる秘密の内容や秘密の主体が受ける不利益を具体的に考慮」すべきであると判示した上で、前述のように、Ａの利益を図りたいという被告人の思いが主観的なものにとどまっていることと、Ｃに書類を閲覧させる手段の相当性を欠いていることから、被告人の行為には「正当な理由」がないと判断した。

第１審の有罪判決に対して、被告人は控訴したが、第２審（大阪高判平成21年12月17日刑集66巻４号471頁参照）も被告人の控訴を棄却したので、最高裁に上告した。

最高裁は、被告人がＡ及びＢから鑑定を委託されていないことから、被告人の精神鑑定はあくまでも「鑑定人の業務」であって、本罪において規定される「医師の業務」にあたらないとする被告人側の主張に対して、「医師が、医師としての知識、経験に基づく、診断を含む医学的判断を内容とする鑑定を命じられた場合には、その鑑定の実施は、医師がその業務として行うものといえるから、医師が当該鑑定を行う過程で知り得た人の秘密を正当な理由なく漏らす行為は、医師がその業務上取り扱ったことについて知り得た人の秘密を漏示するものとして、刑法134条１項の秘密漏示罪に該当する」と判示し、被告人の上告を棄却した。

本件では、刑法134条１項の主体のひとつである「医師」に、精神鑑定人としての医師が含まれるか、秘密の主体から委託を受けていない精神鑑定は本罪にいう「業務」といえるか、被告人の行為には「正当な理由」があったか否かが争われた。本罪の保護法益を（団体、法人等も含む）個人の秘密とする観点から、法益侵害が認められるためには個人の秘密が134条所定の主体によって漏示されれば足り、秘密の主体と漏示の主体との間に特別の依頼関係や信頼関係は不要であるとして、第１審につ

き、被告人は134条所定の「医師」であり、精神鑑定が本罪の「業務」にあたると判断した点を肯定する見解がある[17]。改正刑法草案317条は、秘密漏示罪の主体を「依頼者との信頼関係に基づいて人の秘密を知ることとなる業務に従事する者」と規定していたが、信頼関係の有無について明言せず、医師や弁護士といった特定の職業の者を主体として限定列挙する134条の条文に照らすと、特段の信頼関係や委託関係がないからといって、本件被告人を134条の主体にあたらず、精神鑑定は本罪の「業務」にあたらないと判断する理由はないであろう。

次に、本判決は被告人の手段の相当性が欠如しており、それによってＡやＢの利益が侵害されたことを根拠に「正当な理由」を否定している。この点については、少年審判の制度趣旨という観点から、違法性阻却は困難であるとする見解が多い[18]。

医師などの守秘義務を有する者による秘密漏示行為については、判例では「正当な理由」の有無について目的・手段の相当性や利益衡量の観点から検討がなされ、妥当な解決が図られているように思われる。

しかし、その一方で本件事案では、守秘義務の身分を持たないジャーナリストであるＣによる個人情報・秘密の公開という問題が残されている。秘密漏示罪は、秘密を漏示される相手方の存在を必要とする必要的共犯（片面的対向犯）である。この点につき、本罪は人の秘密を扱う職業の者に漏示禁止義務を課すことで秘密を保護するものであるという理由から、たとえ相手方が積極的に漏示をそそのかしたとしても相手方は

[17] 松宮孝明「判批」立命館法学337号（2011年）1694頁。豊田兼彦「判批」新・判例解説 Watch 刑法 No.71も同旨。柑本美和「精神医療の実行における守秘義務と情報共有―『僕はパパを殺すことに決めた』事件を題材に―」町野朔・岩瀬徹・日髙義博・安部哲夫・山本輝之・渡邊一弘（編）『刑法・刑事政策と福祉　岩井宜子先生古稀祝賀記念論文集』（尚学社・2011年）174 ～ 175頁も、秘密提供者と医師との信頼関係に基づいてやり取りされた秘密のみを本罪の保護の対象とすることは、診察以外にも医師の業務の範囲が拡張されている現状に鑑みると、人の秘密の保護としては不十分であると述べている。

[18] 澁谷洋平「判批」年報医事法学25号（2009年）158頁、松宮・前掲注（17）1699頁、田坂晶「判批」刑事法ジャーナル33号（2012年）134 ～ 135頁、澁谷洋平「判批」判例セレクト2012［Ⅰ］（法学教室389号別冊）37頁。

処罰されないとする見解がある[19]。他方、相手方が犯罪の成立に欠くことのできない関与行為をした場合は処罰されないということから、秘密を知っただけでは秘密漏示罪の成立に欠くことのできない関与行為に留まるので処罰されないが、自己に漏示するように教唆した場合には、秘密漏示罪の教唆または幇助として処罰されるという見解も主張されている[20]。

本件のCも「身分なき共犯」として告訴されたが、嫌疑不十分で不起訴処分となっていることから、Cのように守秘義務者に積極的に漏示を働きかけたり要求したりする者は共犯として処罰される可能性もあると思われる。ところが、Cは被告人に対し秘密漏示を要求するのみならず、被告人から得た供述調書等をもとに書籍を出版することによって、AやBの秘密や個人情報を広く公表していることから、書籍出版行為は新たな法益侵害といってもよい。書籍出版によって秘密を漏らす行為は名誉毀損罪でカヴァーすることも可能であろう。しかし、広く秘密を公表するという行為にまで至らなくとも、秘密漏示罪が相手方の不特定多数であることを要求していないことに鑑みれば、守秘義務者から秘密を得たCのような立場の者が、例え少数の相手方であっても他の者に秘密を漏示すれば、そのような行為によって新たな法益侵害が発生するといえないだろうか。現行の秘密漏示罪では、法定された守秘義務者ではない者が守秘義務者に対して秘密漏示を要求したにとどまる場合は共犯として処罰される可能性があるものの、秘密を知った非守秘義務者がさらなる漏示行為を行った場合は処罰の対象外となっている。

第２節　信書開封罪

刑法133条は、封をしてある信書を正当な理由なく開ける行為を処罰している。信書を「開ける」というのは、封を破棄して信書の内容を知り得る状態を作り出すことであり、信書を実際に読んだり、信書の内容

[19] 松宮・前掲注（17）1703頁。
[20] 平野龍一『刑法総論Ⅱ』（有斐閣・1975年）379頁。

を探知したりすることまでは要しないと解されている[21]。本罪の法的性質については、①個人の秘密に対する抽象的危険犯であるとする見解[22]に対して、②「封をしてある信書」という秘密の形式、または「信書が勝手に開かれない利益」に対する侵害犯であるとする見解[23]も主張されている。後者の立場を採れば、信書の内容が秘密である必要はなく、信書の内容が単なる事務的な連絡事項であったとしても、信書の封を開けた時点で既遂に達することになる。

続いて、信書開封罪における「信書」は個人のものに限るか否かが争われている。本罪が個人的法益犯罪であるという見地から、国・地方公共団体相互間の信書を除外すべきとする見解[24]がある一方で、信書の内容を秘匿する利益は個人のみならず、法人や国・地方公共団体も享受し得るとする見解[25]もある。いずれの見解を採ったとしても、国・地方公共団体と個人との間でやり取りされた信書であれば、その内容は個人情報を含むものといえると考えられるので、本罪は信書であるという条件のもとで個人情報を保護する犯罪類型であるといえる[26]。本罪では信書という範囲内において、個人の秘密や情報が幅広く保護され得るが、本罪がカヴァーするのは信書の秘密を探知する行為までであり、その内容

---

[21] 西田典之『刑法各論（第６版）』（弘文堂・2012年）106頁。

[22] 大塚仁『刑法概説（各論）（第３版増補）』（有斐閣･2005年）127頁、大谷實『刑法講義各論（新版第４版）』（成文堂･2009年）157頁、曽根威彦『刑法各論（第５版）』（弘文堂・2012年）83頁など。

[23] 松宮孝明『刑法各論（第３版）』（成文堂・2012年）139頁、山口・前掲注（15）137頁。

[24] 大谷・前掲注（22）156頁、西田・前掲注（21）105頁。

[25] 山口・前掲注（15）130頁。

[26] 時武英男「刑法におけるプライバシーの保護」中山研一・西原春夫（編）『現代刑法講座　第４巻　刑法各論の諸問題』（成文堂・1982年）138 ～ 139頁も、本罪をプライヴァシー保護の規定であることを前提として、「信書の内容がたとえ国・地方公共団体の秘密であろうと、また発信人・受信人のいずれかが国などであろうとそれは必ずしも問うところではない……なぜなら、本罪が保護しようとするのは私人のプライバシーであるからその可罰性の根拠は、信書の内容もしくは開披行為にではなく、信書の開披によって他人に知られたくない内容・事柄つまりプライバシーが侵害されたという点にある」と述べている。

を他者に公表する行為等については本罪によって評価されるものではない。

第３節　支払用カード電磁的記録不正作出準備罪

刑法163条の４第１項は、人の財産上の事務処理を誤らせる目的で、その事務処理の用に供する電磁的記録であってクレジットカードその他の代金又は料金の支払い用カードを構成するものを不正に作出する行為（163条の２第１項前段）や、預貯金の引出用のカードを構成する電磁的記録を不正に作出する行為（163条の２第１項後段）の用に供する目的で、①電磁的記録の情報を取得する行為と、②情を知ってその情報を提供する行為を処罰対象とする。不正に取得された電磁的記録の情報を同様の目的で保管する行為（163条の４第２項）や、器械又は原料を準備する行為（163条の４第３項）も処罰される。

163条の４は情報窃盗的な性質を有する犯罪類型であると同時に、163条の２の予備罪となっている。これらの罪は、電子機器を用いてカードの電磁的記録をひそかに取得して（スキミングにより）カードを偽造し、偽造カードを利用して商品の購入等が行われるようになったので、このような事態への対処方法として新設されたものである[27]。対象となる電磁的記録の情報は、支払用カードによって支払いを行うためのシステムにおいて、情報処理の対象となるひとまとまりの情報であるとされており、情報の「取得」は、スキミングによって不正に取得する行為や、記録媒体に記録されたカード情報を記録媒体ごと取得する行為など、自己の支配下に情報を移転させる行為をいう[28]。このように、個人のカード情報を不正取得する行為が処罰対象となっているものの、支払用カード電磁的記録に関する一連の犯罪は、社会的法益としての「支払用カードを構成する電磁的記録の真正さ、ひいては支払用カードを用いた支払決済システムに対する社会的信頼」を保護法益としている[29]ので、個人の

[27] 山口・前掲注（15）486頁。
[28] 山口･前掲注（15）494頁、高橋則夫『刑法各論』（成文堂･2011年）537頁など。
[29] 山口・前掲注（15）487頁、高橋・前掲注（28）532頁。

カード情報は反射的に保護されるにすぎない。

第４節　不正指令電磁的記録に関する罪

近年増加しているコンピュータ・ウイルスによるコンピュータへの攻撃や、コンピュータ・ウイルスを悪用した犯罪を防止するために、「犯罪の国際化および組織化並びに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案」が第159回通常国会（平成16年）に提出され、2011（平成23）年の刑法改正で「不正指令電磁的記録に関する罪」が設けられた。これによって、刑法168条の２の「不正指令電磁的記録作成等罪」では、正当な理由なくコンピュータ・ウイルス等を作成、提供する行為が処罰され、168条の３の「不正指令電磁的記録取得等罪」では正当な理由なくコンピュータ・ウイルスを取得、保管する行為が処罰される。これらの犯罪類型は、コンピュータ・ウイルスによる情報流出を防ぐために創設されたといわれているが、情報という個人的法益を保護するというよりも、コンピュータ・プログラムの安全性・健全性に対する公共の信用という社会的法益に対する抽象的危険犯として規定されている[30]。したがって、本罪においては、コンピュータ・ウイルスによって個人情報が漏洩されない利益が反射的に保護されているといい得るが、コンピュータ・ウイルスの作成・提供等の行為によって実際に個人情報の漏洩が発生したか否かということは本罪における法的評価の対象外である。

第５節　不正アクセス禁止法

不正アクセス禁止法は1999（平成11）年に成立し、2012（平成24）年に改正された。
法３条では「何人も、不正アクセス行為をしてはならない」と規定されており、２条４項は不正アクセスの定義について以下のように規定して

[30] 山中敬一『刑法各論（第２版）』（成文堂・2009年）627頁、曽根・前掲注（22）268頁、伊東研祐『刑法講義各論』（日本評論社・2011年）427頁、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）18頁。

いる。

①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（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）

②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よる特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）

③電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為

これらの行為のいずれかに該当するものが「不正アクセス行為」である。

続いて、2012（平成24）年の改正により、「何人も、不正アクセス行為（第２条第４項第１号に該当するものに限る。第６条及び第12条第２号において同じ。）の用に供する目的で、アクセス制御機能に係る他人の識別符号を取得してはならない」とする４条と、「何人も、不正アクセス行為の用に供する目的で、不正に取得されたアクセス制御機能に係る他人の識別符号を保管してはならない」とする６条が新設され、処罰の対象となることが12条で定められた。

４条と６条の新設により、他人の識別符号（ID とパスワード）を不正取得する行為と不正保管する行為が犯罪化された趣旨は、従来から禁止・処罰の対象となっていた「不正アクセス行為の禁止の実効性を確保するためであるが、不正アクセス行為につながる危険性が大きいのは、不正アクセス行為の用に供する目的で他人の識別符号を取得したり保管したりする場合であり、不正アクセス行為の用に供する目的がない取得行為

や保管行為は、仮にそれが不正なものであっても不正アクセス行為につながる危険性は小さく、そのような行為まで禁止・処罰の対象とすることは適当ではないことから、目的要件により禁止・処罰の対象範囲が限定されたものである」[31]とされている。４条と６条により、ID とパスワードという個人情報が保護法益として位置付けられているように見えるものの、条文が目的犯構成を採っていることから、識別符号の不正取得罪と不正保管罪は、その先にある不正アクセスを未然に防ぐための手段として位置付けられていることがわかる[32]。

次に、５条は「何人も、業務その他正当な理由による場合を除いては、アクセス制御機能に係る他人の識別符号を、当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る利用権者以外の者に提供してはならない」と規定することにより、不正アクセス行為を助長する行為が禁止され、処罰の対象となっている（12条・13条）。

続いて、実在するアクセス管理者になりすましてフィッシングサイトを公開したり、フィッシングメールを送信したりすることにより、利用権者に ID・パスワードを入力させてだまし取るといったフィッシング行為も７条により禁止され、12条４号により処罰されることとなった。条文は次の通りである。

７条（識別符号の入力を不正に要求する行為の禁止）

「何人も、アクセス制御機能を特定電子計算機に付加した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、次

---

[31] 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（2012年）25頁。

[32] 渡邊卓也「不正アクセス罪の罪質とその立法動向」Law & Practice No.07（2013年）134頁によると、「不正アクセスの用に供する目的」が「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」も含むと解されることから、不正アクセス行為を助長する罪（５条）であり、不正アクセスの予備罪である識別符号提供を行う目的で識別符号を取得及び保管する行為を４・６条において犯罪化することは、「予備の幇助の予備を処罰する規定となり得る」ので、「過度の処罰の拡張との批判が向けられる余地」があるとされている。

に掲げる行為をしてはならない。ただし、当該アクセス管理者の承諾を得てする場合は、この限りでない。

1　当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該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（公衆によって直接受信されることを目的として公衆からの求めに応じ自動的に送信を行うことをいい、放送又は有線放送に該当するものを除く。）を利用して公衆が閲覧することができる状態に置く行為

2　当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該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、電子メール（特定電子メールの送信の適正化等に関する法律（平成14年法律第26号）第２条第１号に規定する電子メールをいう。）により当該利用権者に送信する行為」

フィッシング行為は、不正アクセス禁止法が制定された1999年当時には想定されていなかったので、旧法では禁止・処罰の対象とされていなかったが、他人の識別符号の不正取得手段としてフィッシングが多用されるようになり、不正アクセス行為やこれを手段とする詐欺等につながる危険性が高い[33]ことから、新たに処罰の対象とされることとなった。７条１号で禁止されるのは、フィッシングサイトを公開して識別符号を入力させるフィッシング行為であり、７条２号ではフィッシングサイトを用いるのではなく、電子メールを利用者に送信することによって識別符号を詐取するフィッシング行為が禁止される。

このように、不正アクセス禁止法では、①不正アクセス行為、②不正アクセス行為を助長する行為、③他人の識別符号を不正取得・不正保管する行為、④識別符号の入力の不正要求行為（フィッシング行為）が禁止・処罰の対象とされている。

③④の犯罪により、識別符号という個人情報そのものが保護法益として位置付けられているようにも見えるが、本法において、識別符号は個人的法益として保護されているのだろうか。まず、この法律の目的は「不

[33] 蔵原・前掲注（31）30頁。

正アクセス行為を禁止するとともに、これについての罰則及びその再発防止のための都道府県公安委員会による援助措置等を定めることにより、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及び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を図り、もって高度情報通信社会の健全な発展に寄与すること」（１条）とされている。そして、法改正前は不正アクセス行為とそれを助長する行為のみが処罰対象とされており、不正アクセス行為を処罰することは結果的には情報の不正入手を処罰することと同じであるが、情報の取得が不正アクセス罪の成立要件とされていなかった[34]ことから、不正アクセス禁止法の保護法益は、「ID およびパスワードなどによる認証システムによって担保されているアクセス制御に対する社会的な信頼、すなわち正当な利用者がアクセス制御機能によって正しく識別されていることに対する信頼」[35]であり、不正アクセス罪は社会的法益に対する犯罪である[36]と解されていた。法改正により識別符号の不正取得等が禁止・処罰の対象となったものの、その目的は不正アクセスの予防と、不正アクセスを手段とする他の犯罪の予防であることに鑑みれば、不正取得等の罪も不正アクセス罪等と同様に社会的法益に対する罪としての性格を有していると考えられる[37]。

---

[34] 不正アクセス対策法制研究会『逐条　不正アクセス行為の禁止等に関する法律［補訂］』（立花書房・2001年）24頁以下。

[35] 前掲注（34）21頁以下。

[36] 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』（第一法規株式会社・2004年）365 ～ 368頁では、「アクセス制御機能に対する社会的な信頼」の実質的な意義について議論が展開されている。論者によると、コンピュータの利用につきアクセス制限を付加するいくつかの目的には社会的な意義・性格が付与されていることから、その目的の達成手段であるアクセス制御機能も原則的に社会的信頼の対象となる。社会的な意義を有するアクセス制限の目的として、①情報またはシステムの「不正操作の防止」、②情報の「機密性の保持」、③情報等の「真正性の保証」が挙げられている。

[37] 不正アクセス禁止法制研究会『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）によると、不正アクセス行為は処罰することが適当な行為であると認められるにしても、前法律的に反規範性を有する行為であるとまではいえないということから、不正アクセス罪は行政犯である（77

以上のように、個人情報保護の側面のある規定には様々なものがあり、情報を個人との関係において保護する規定・法律は、秘密漏示罪と信書開封罪、後述する個人情報保護法であるといえる。支払用カード電磁的記録不正作出準備罪や、不正アクセス禁止法所定の不正アクセス罪・不正アクセス助長罪は社会的法益に対する罪であり、これらの犯罪の下では個人情報は反射的・結果的に保護されるにすぎない。そして、不正アクセス禁止法の改正によって新設された識別符号の不正取得罪・不正保管罪と、識別符号の入力の不正要求（フィッシング）の罪も、IDとパスワードという個人情報が不正に扱われるのを禁止するという側面はあるものの、その目的は不正アクセスの防止であり、個人情報そのものが保護法益として位置付けられているとはいえないだろう。

第６節　個人情報保護法

第１項　成立過程と概要

個人情報の漏洩や悪用を防ぎ、個人情報の取り扱いを規制する一般法として、2003（平成15）年に「個人情報の保護に関する法律」（個人情報保護法）が成立した。ここでは、個人情報保護法の成立過程[38]と、法律の概要について説明する。

日本の行政機関においては、1959（昭和34）年３月から電子計算機が使用されるようになり、行政効率の向上という利益が重視されると共に、

～78頁）。そして、他人の識別符号の不正取得や不正保管等の罪を不正アクセスの「準備段階の罪」であると位置づけ、「行政犯については命令、禁止により達成しようとしている行政上の目的が保護法益である」ことから、不正アクセス関係の犯罪は「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及び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を図り、もって高度情報通信社会の健全な発展に寄与する（第１条）ことが法益となる」と解する。より具体的には、「このような犯罪の抑止力としての、また、ネットワークの利用、接続の基礎としてのアクセス制御機能に対する社会的信頼に法益がある」とされている（139～140頁）。

[38] 宇賀克也『個人情報保護法の逐条解説（第４版）』（有斐閣・2013年）１頁以下、宇賀克也『個人情報保護の理論と実務』（有斐閣・2009年）３頁以下、51頁以下参照。

コンピュータによる個人のプライヴァシー侵害が懸念され始めた。そのような背景を受けて、1975（昭和50）年に行政監理委員会は「行政機関等における電子計算機利用に伴うプライバシー保護に関する制度の在り方についての中間報告」を提出した。その後、1980（昭和55）年には「プライバシー保護と個人データの国際処理についてのガイドラインに関するOECD理事会勧告」が出され、その勧告付属文書にOECD８原則[39]という個人情報保護の基本原則が示されている。これは、個人情報保護の法制化を行っていた米仏独等の法律を参照して、個人情報の自由な流通の必要性に配慮しつつ個人情報保護を図るためのもので、個人情報保護の国際的な基本原則となっている。このOECD理事会勧告が、加盟国に対して各々の国内法の中でOECD８原則に配慮することを要求したことにより、日本も個人情報保護法制についてさらなる検討を迫られた。

OECD８原則後の日本は、行政部門における個人情報保護法制の整備を優先させるようになった。その契機となったのは、1983（昭和58）年の第２次臨時行政調査会答申であり、この答申において「法的措置も含め個人データに係る制度的方策について積極的に対応する」と提言されたことである。このような動きを受けて、1988（昭和63）年に「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」が制定された。このように、行政部門における個人情報保護法制については早くから議論がなされていた一方で、民間部門における個人情報保護の一般法制定に関する議論は後退していた。

しかし、1995（平成７）年にEUが「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令（EU個人情報保護指令）」を出し、その25条において、個人データの第三国への移転は、当該第三国が十分なレベルの情報保護措置を確保している場合に限って行うことができると規定されている。これに加えて日本の民間部門における個人情報漏洩事件が相次いだことから、1998（平成10）年の高度情報通信社会推進本部の「高度情報通信社会推進に向けた

[39] OECD８原則は以下の通りである。①収集制限の原則、②データ内容の原則、③目的明確化の原則、④利用制限の原則、⑤安全保護の原則、⑥公開の原則、⑦個人参加の原則、⑧責任の原則の８つから成る。

基本方針」において、「民間による自主的取り組みを推進するとともに、法律による規制も視野に入れた検討を行っていく必要がある」と規定されるに至った。

このような背景を受けて、1999（平成11）年６月の参議院本会議において当時の内閣総理大臣の小渕恵三が、個人情報保護のために必要な措置について、「民間部門をも対象とした個人情報保護に関する法整備を含めたシステムを速やかに整えることなどを示すものと認識しております」と答弁し、行政部門のみならず民間部門も含めた個人情報保護法制が政府において行われることになった。1999（平成11）年11月19日には、政府機関である高度情報通信社会推進本部の下に置かれていた個人情報保護検討部会によって「我が国における個人情報保護システムの在り方について（中間報告）」が出され、2000（平成12）年10月には高度情報通信社会推進本部の個人情報保護法制化専門委員会による「個人情報保護基本法制に関する大綱」が、「中間報告」を踏まえた上で出されている。

そして、前述の「大綱」を基にして、第156回通常国会（平成15年）に「行政機関の保有する個人情報の保護に関する法律案」、「独立行政法人等の保有する個人情報の保護に関する法律案」、「情報公開・個人情報保護審査会設置法案」、「行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律案」「個人情報の保護に関する法律案」の個人情報保護関係５法案が提出され、可決成立した。

以上のように、日本の個人情報保護のための一般法は、まず行政部門において整備され、その後の国際情勢や日本国内における世論の要求によって、民間部門における個人情報保護法制が整備されるに至った。個人情報保護関係５法の制定により、日本の個人情報保護法制の体系は次の通りになる。

個人情報保護法は、１章から３章までの基本法にあたる部分と、４章から６章までの、民間部門の個人情報保護の一般法にあたる部分から成る。そこで、民間部門には個人情報保護法の１章から６章までが適用され、国および実質的に政府の一部をなす法人には、個人情報保護法の１章から３章までに加え、行政機関個人情報保護法と独立行政法人等個人情報保護法が適用される。そして地方公共団体には、個人情報保護法の１章から３章までと、各地域の個人情報保護条例が適用される。つまり、

個人情報保護法の１章から３章までは、様々な機関が保有する個人情報を包括的に保護する基本法として位置づけられている。

ここからは、個人情報保護法の規定内容について述べる。

個人情報保護法では、個人情報は次のように定義される。まず、生存する個人に関する情報であり、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるものである。他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものも個人情報に含まれる（２条１項）。加えて、「個人データ」とは、個人情報のうち「個人情報データベース等を構成する個人情報」であるとされている（２条４項）。この法律において個人情報と個人データを区別した理由は、開示請求等の対象となるのは、体系的に整理され、容易に検索できる個人情報に限定するとしたことにある[40]。また、死者の個人情報が対象外となっているのは、情報の開示請求等の自己情報コントロール権を有するのは生存者であり、死者に関する個人情報が同時に遺族の個人情報ともいえる場合には、それを生存者である遺族等の個人情報として保護すれば足りるからであると理解されている[41]。

個人情報保護についての義務規定である本法４章が適用されるのは、「個人情報取扱事業者」である。個人情報取扱事業者とは、「個人情報データベース等を事業の用に供している者」のことであるが、国の機関、地方公共団体、独立行政法人、地方独立行政法人、その取り扱う個人情報の量および利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定める者を除くとされている（２条３項）。「政令で定める者」については、個人情報保護法施行令２条によって、「その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去６か月以内のいずれの日においても5000を超えない者」とされている。つまり、「個人情報取扱事業者」は5000件以上の個人情報を扱う民間事業者であり、日本国内の多くの企業等がこれに該当する。

---

[40] 平松毅『個人情報保護―理論と運用』（有信堂・2009年）73頁。

[41] 宇賀・前掲注（38）『理論と実務』57 ～ 58頁。

このように主体を限定した上で、個人情報保護法４章は個人情報取扱事業者が遵守すべき義務について規定している。本法では個人情報の利用目的の特定（15条）、利用目的による制限（16条）、個人情報の適正な取得（17条）、取得に際しての利用目的の通知等（18条）のほか、個人データの内容の正確性の確保（19条）、安全管理措置（20条）、従業員の監督（21条）、データの委託先の監督（22条）、第三者提供の制限（23条）、個人情報の取り扱いに関する苦情の適切かつ迅速な処理（31条）などが義務として定められている。これらの義務は、前述のOECD８原則の考え方を具体化したものであると考えられている[42]。

本法の特色には、個人情報取扱事業者による個人情報の不当な取り扱いにつき、多様な救済システムを採用していることが挙げられる。個人情報取扱事業者自身（31条）、認定個人情報保護団体（42条）、地方公共団体（13条）、そして国（９条）などが苦情処理にあたることが定められている。しかし、このような苦情処理システムによって解決を図ることができない場合につき、個人情報取扱事業者の事業を所管する主務大臣は報告徴収（32条）、助言（33条）、勧告（34条１項）、違反行為の中止その他違反を是正するために必要な措置をとるべきとする命令（34条２・３項）をすることができる。そして、実効性担保の手段として、違反行為につき直接刑罰を科すという方式ではなく、個人情報取扱事業者が命令に従わない場合に初めて刑罰（６か月以下の懲役または30万円以下の罰金）を科すという間接罰方式を採っている（56条）。

第２項　刑罰に関する議論

第１項で見てきたように、個人情報保護法では間接罰方式が採られている。個人情報には様々な内容のものが含まれており、個人情報取扱事業者の義務内容も多岐にわたっていることから、違反行為に対して一律に直接刑罰を科すという方法を採らなかったことは、その限りでは了解可能である。しかし、主務大臣の命令に違反して初めて刑罰を科すという方法は、企業等による個人情報の大量漏洩のような重大な情報侵害に対応できるのだろうか。この点を検討するため、第２項では個人情報保

[42] 園田寿「個人情報保護法の成立」現代刑事法55号（2003年）81頁。

護法における罰則として、直罰方式ではなく間接罰方式が採用されるに至った経緯について、（１）個人情報保護検討部会[43]と（２）個人情報保護法制化専門委員会[44]の議論を通して概観する。そして、通産省（現・経済産業省）および大蔵省（現・財務省）によって設置された「個人信用情報保護・利用の在り方に関する懇談会」が1998（平成10）年６月12日に公表した報告書を併せて参照する。

第１款　個人情報保護検討部会の議論

まず、1999（平成11）年７月23日の第１回個人情報保護検討部会において、「罰則の在り方とその適用範囲」について、安冨潔委員は「刑事罰の関係で最も考えなければいけないのは、保護すべき個人情報の範囲」であり、「法規制によって自由な情報の流通というものが阻害されてはならない。他方で、情報保護のために刑事罰が必要になってくることもある」が、情報保護のために刑罰を用いる根拠は何かということが問題となると述べている。そこで、安冨委員は従来の刑法の財産犯の枠組みで情報を捕捉することができるのかということも含め、保護すべき個人情報の範囲について議論が必要であると述べている。

保護法益としての個人情報という問題は、第２回以降の検討部会でも議論されている。1999（平成11）年８月６日の第２回の部会において、安冨委員は「刑事罰ということになりますと、伝統的な刑法の枠組みの中で考えることになりますから、どういう保護法益ととらえるかという非常に難しい議論になってまいりますし、少なくとも今の日本の刑法では、現実の空間といいますか、そういう場で物理的に存在する物の保護という発想から保護法益を理解していく考え方から抜け切っておりませんから、バーチャルというか、電子空間のようなものとそうでない現実の空間との境がなくなってきたという発想は、なかなか刑事法の中ではとりにくいということがあります」と述べている。第１回検討部会にお

[43] 個人情報保護検討部会の議事録は、http://www.kantei.go.jp/jp/it/privacy/index.html を参照した。

[44] 個人情報保護法制化専門委員会の議事録は http://www.kantei.go.jp/jp/it/privacy/houseika/index.html を参照した。

ける前述の発言と同様に、情報という異質なものを、存在が明確な財物と同様に扱うことの困難性に言及している。

続いて、1999（平成11）年９月21日の第５回検討部会では、日弁連が1998（平成10）年に発表した「個人情報大綱」を題材に議論が展開された。日弁連の大綱は、プライヴァシーを始めとする個人情報の保護を主目的とする法律を制定し、個人情報の妥当な保護のために必要最小限度の罰則を設けるべきであるとの立場によるものである。

これに対して安冨委員は、「財産権的な考え方でこの個人情報というのをとらえての罰則規定の御趣旨なのでしょうか。あるいは……もし民間部門の方で刑罰規定を設けるとするならば、いかなる保護法益に対する侵害行為に対して処罰を設けるという構想なのか」と質問したところ、大綱について報告した弁護士は、プライヴァシーを保護法益としつつ、様々なルール違反行為の中でも「罰則によって規制しようというのはもうちょっと実質的な侵害につながるようなものに限定」して、情報を不正入手する行為と、情報を渡す行為を中心に構成すると述べている。質問者の安冨委員が要約するところによると、「個人情報というもの、それに一定の価値があるとして、それを侵害するから罰するということではなくて、行為態様について、不正な活動というか、それに実質的な違法があると見るという理解」であり、「情報そのものの種類だとか、価値とか、そういうところに着目をするとなかなか罰則を設けることはできない」ので、行為態様から捕捉するのがこの大綱の手法となっている。大綱には、「保護法益としての個人情報」の範囲よりも処罰に値する行為態様を検討する方が、刑罰の明確性に資するという問題意識があったように思われる。

これまでの検討部会における議論や各種専門機関からのヒアリングを踏まえて、堀部政男座長は「座長私案」を作成し、1999（平成11）年10月20日の第７回検討部会において報告した。座長私案では、「そもそも罰則の創設には謙抑的であるべきであり、他の手段によって実効性担保が全く期待できない場合に限り、その創設を検討することが適切と考えられる」という一般論が提示され、「分野を問わず一律に罰則等の規制措置を設けることについては、構成要件の明確化の観点から、前提として全分野を通じた登録制度や届出制度の創設が必要となる可能性が高い」

ことが指摘されている。

このように、座長私案は罰則を設けることに対して慎重な姿勢を採っているが、鈴木文雄委員は「不当な収集」、換言すれば「情報窃盗」についての刑法の手当というものを考える必要があるのではないかと問題提起している。これに対して、安冨委員は「情報というのは財産だけに純化できるものではありません。そういう意味で言いますと、情報窃盗というものを果たして現行の刑法の枠組みの中で、果たして処罰できるようにつくり上げられるかというと、恐らくこれは非常に難しいだろうと思います」と述べている。

また、安冨委員は保護法益よりも行為態様に着目して、これに何らかの規制をかけて罰則を作ることが可能かどうかという問題提起も行っている。ここでは、個人情報の収集権限のあるところに何らかの形で登録されている情報を不正な行為によって盗む、漏洩するという行為態様なら罰則を設けることが可能だと思われるが、およそ広く一般的に不正な入手ということを処罰するのは、現行刑法の枠組みからいって困難であることが指摘されている。これに対しては、情報の侵害について苦情処理や相談窓口はあるものの、社会的な抑止力になっているとはいえないという意見が原早苗委員から出された。また、情報には財物とは異なる性質があるものの、売買の対象となっており、悪意による情報の詐取等に刑事罰を与えることができるような法的整備が必要であるという西垣良三委員の意見もあった。このように、個人情報の漏洩などに有効に対処すべきであるという社会的な問題意識と、「個人情報窃盗」を犯罪構成要件化することの困難性との矛盾が顕在化している。

1999（平成11）年11月９日の第８回検討部会では、悪意による情報の詐取については刑罰で臨むべきなのか、それとも情報窃盗罪の創設には慎重になるべきかという議論がなされ、1999（平成11）年11月19日の第９回検討部会では「我が国における個人情報保護システムの在り方について（中間報告）」が出された。この中間報告では、罰則について「刑事法の一般理論として、罰則の創設には謙抑的であるべきであり、他の手段によっては実効性担保が期待できない場合に限り、その創設を検討することが適切である」「分野を問わず一律に罰則等を設けることについては、各分野における個人情報の利用の形態等が様々であるので、構成

要件の明確化の観点から問題が多い」「広く薄い罰則であっても、あらゆる分野の一般多数の事業者にとっては、自由な事業活動の阻害要因となるなど、他の保護されるべき権利、利益が損なわれるおそれがある」といった理由から、「あらゆる分野を通じた一般多数の事業者を対象とする基本法において、罰則等を創設することについては、慎重に考えるべきである」という結論に至った。

第２款　個人情報保護法制化専門委員会の議論

個人情報保護検討部会では、一定以上の個人情報侵害行為につき罰則を設けることが議論されたが、個人情報を従来の刑法の保護法益においてどのように位置づけるのかということと、犯罪としての構成要件化につき困難があったことから、中間報告において罰則の制定を提示するには至らなかった。続いて、検討部会の中間報告を受けて法制的な観点から専門的な検討を行うために設置された個人情報保護法制化専門委員会の議論について概観する。

個人情報保護法制化専門委員会においても、個人情報保護検討部会と同様に、外国法の参照、日本の現行法の分析、関係省庁のヒアリング等を通して、保護されるべき「個人情報」とは何かということが議論されている。その中で、2000（平成12）年４月28日の第13回委員会において、高橋和之委員から「苦情処理などを行政機関が勧告し、勧告を聞かなかった場合にはサンクションを与えるというようなこともあり得るのではないか」との問題提起がなされた。これは、個人情報保護検討部会の中間報告が直接的に刑罰を用いることに対して消極的な姿勢を採っていることと、民事責任は必ずしも制裁として有効な方法とはいえないのではないかという疑問による。そこで、行政に勧告権限を与え、勧告を無視するような場合には罰則の対象とすることを視野に入れてもよいというのである。このような考え方は、現行個人情報保護法における間接罰方式の原型となっている。

2000（平成12）年９月８日の第24回委員会において、上谷清委員から「非常に悪質な個人情報の処理をする者については何らかの罰則は是非設けてほしい。当面、私が考えていますのは、第三者提供にまつわるような不正な情報の処理です」という提案があった。上谷委員は、処罰範囲は

①情報の内容面と②手段の悪質性の観点から限定することができるとした上で、個人情報取扱事業者に限らず一般の個人であっても、個人の秘密に関わるようなものを第三者に提供したり、何らかの形で個人情報を盗み出して第三者に提供したりする場合が罰則の対象となり得ると述べる。

ここで小早川光郎委員長代理は、情報の内容と手段の悪質性からの二重の絞りによる処罰範囲の検討方法につき、産業界は従業員が職務上の横領背任のような形で、必ずしも秘密ではなくとも集積すれば経済的価値があるものを、自己の利益のために使うような行為に対し処罰を要求していると述べた。これに対して上谷委員は、そのように幅の広い保護法益で重い罰則を科すことは困難であり、個人情報が集積して経済的価値を帯びるということを構成要件化することも困難であると述べている。

続いて2000（平成12）年９月14日の第25回委員会では、第24回委員会で罰則につき意見を述べた上谷委員が出したＡ案と、委員会事務局が作成したＢ案が議論の題材となった。

まず、Ａ案では（ア）「正当な理由なく、人の秘密に属する個人情報を第三者に提供した者及びその提供を受けた者について罰則を設ける」、（イ）「情報を管理する者の同意を得ないで、人の秘密に属する個人情報を取得した者について罰則を設ける」とされている。いずれも主体を限定していないが、名誉毀損罪や侮辱罪等の個々の既存の刑事罰の対象にならないような個人の秘密についてうわさ話をするだけで罰則の対象になることにつながるのではないか、情報を受動的に得た受領者も罰則の対象になるのかという疑問が司会者から出されている。

一方、Ｂ案では（ア）「法令で定められた守秘義務規定に違反して提供される個人情報であることを知りながら、それを取得した者について罰則を設ける」、（イ）「（ア）に違反して取得された個人情報であることを知りながら、それを第三者に提供した者について罰則を設ける」とされている。そしてＢ案は、この委員会で一貫して問題となっている「悪質な第三者提供」について、主務大臣は個人情報取扱事業者に対して単なる改善指示を行うよりも、行政処分としての改善または中止命令をできることとして、その違反について罰則を設けるという考え方が提示されている。

このように、A案では「人の秘密に属する個人情報」の範囲が広くなっているが、現代社会では大量に集積・蓄積された情報が本人に知らされずに流通することが問題となっているという観点から、保護客体を集積された個人情報や、個人情報データベースに限定する必要があるという意見が藤原靜雄委員から出された。

そして、2000（平成12）年9月29日の第27回委員会では、「大綱」の完成に向けて、間接罰についての議論が展開されている。高橋和之委員は第13回委員会において、「苦情処理などを行政機関が勧告し、勧告を聞かなかった場合にはサンクションを与えるというようなこともあり得るのではないか」と提案したが、第27回では「行政官庁から命令を出しておいてそれに違反の場合というワンクッションを入れる罰則のつくり方というのは……罰則の規定の仕方というのは基本は法律で定めることであるわけで、法律で罰すべきことを定めないで抽象的に定めて行政機関が具体化するというようなやり方」に対しては、行政機関の裁量の拡大という観点からの批判もあることを述べている。

間接罰方式について、個人情報保護検討部会座長の堀部政男は、従業員が個人情報を漏らしたり悪用したりしているケースには対応できないのではないかと主張しているが、藤井昭夫内閣審議官は、事業者の監督責任が問われる可能性があり、情報を漏らす等の行為をした従業員には解雇の可能性があることを指摘する。

このような議論を受けて、個人情報保護法制化専門委員会は、2000年10月11日に大綱[45]を出している。罰則についての大綱は以下のとおりである。

「『個人情報』、『個人情報の取扱い』には様々なものがあるが、本基本法制においては、これらを広く捉えるとともに、個人の権利利益の侵害を事前に防止する仕組みとしていることとの関係で、これと並べて個人情報の『質』と『侵害の態様』を重視する刑事罰の規定を設けることになじまない面がある……また、本基本法制において、個人情報の第三者提供等を行政上の観点から規律するということになれば、その行政上の規

[45] 個人情報保護法制化委員会による大綱は http://www.kantei.go.jp/jp/it/privacy/houseika/taikouan/1011taikou.html を参照した。

律を確実に守らせるための仕組みが必要との考え方もあるところである。

そこで、本基本法制においては、個人情報の第三者提供等について、一定の要件の下に主務大臣が改善・中止命令を発し、それが守られない場合に罰則が適用される仕組みを設けることが適当である。

一方、政府は……個人情報の取扱いに関連する既存の各法律の守秘義務規定を中心に、個人情報の『質』と『侵害の態様』に応じた個人情報保護の観点から、早期に見直して罰則規定の整備を図るとともに、今後、本基本法制の趣旨に沿って各関係の法律を整備するに当たっても、同様の観点から罰則規定の整備を検討することが求められる」。

このように、大綱では間接罰方式を採ることを明言しており、それが法律に受け継がれている。個人の権利侵害を事前に防止する法的性格との関係で、個人情報の「質」と「侵害の態様」に基づく刑事罰とはなじまないとされているが、刑事罰には事後的な解決の他に予防という側面もあることから疑問が残る。検討部会の中間報告とは異なり、専門委員会では早い段階から、罰則の導入を視野に入れた議論が行われていたが、処罰範囲が不当に拡大されないよう慎重な検討が行われていたことは両者に共通する点である。間接罰方式について、「個人情報にはさまざまな種類の情報が含まれており、個人情報取扱事業者にもさまざまな種類の事業者が含まれているから、一律に違反行為に対する直罰方式を採用しなかった法律の態度は妥当である。個人情報の中でも特に保護の必要性が高いいわゆるセンシティブ情報、たとえば個人の医療情報や信用情報などに関しては、直罰方式を含めたより厚い刑法的保護を特別法で導入することを検討すべきであろう」とする学説[46]の他、「主務大臣の命令を必要以上に強力なものとし、政府が個人事業者の日常的な業務にまで広範に介入する可能性を開くものである」「情報の『質』を度外視して主務大臣の命令違反といういわば行為無価値的側面からの一般的な処罰規定を置くことについては原則的な問題がある」という批判[47]もある。

個人情報を内容と侵害の行為態様によって区別すべきとする考え方は委員会でも挙げられていたが、大綱および法律には反映されていない。

---

[46] 佐伯・前掲注（13）205頁。

[47] 園田・前掲注（42）82頁。

検討部会も専門委員会も、刑罰の謙抑性の原則が重視されていたという点では共通するが、第13回専門委員会の議論に見られるように民事責任のサンクションとしての有効性が疑問視されていたことから、検討部会の議論に比して罰則を設けることに抵抗感は少なかったようである。だが、その後の専門委員会の議論を見ると、個人情報の「質」と「侵害の態様」に着目した規定を設けるには、その構成要件化が困難であるという論調であったことも併せると、間接罰方式を提示する「大綱」は、刑罰の行き過ぎた回避と濫用のいずれにも偏ることがないようにという問題意識による暫定的な結論であったと思われる。しかし、実際には様々な程度・内容のものを含む「主務大臣の命令違反」につき一律に罰則を科すことによって、広く薄い罰則を設けることとなってしまった。このような方法のもとでは、企業による個人情報の大量漏洩という重大な違反も、個人情報の取得後にその利用目的を本人に通知するのが多少遅延したという比較的軽微な違反も、すべて同様に扱われ得ることになり、罪刑の均衡を欠く。したがって、構成要件化が困難であるという指摘はあるものの、比較法的考察などを通して、個人情報をその重要性と侵害の行為態様という観点から分類した上で、妥当な保護のあり方を検討することが求められる。

第３款「個人信用情報保護・利用の在り方に関する懇談会」報告書

個人情報保護法制化のための議論と同時期に、個人信用情報の保護のあり方についても議論がなされていた。「個人信用情報・利用の在り方に関する懇談会」の報告書では、「個人信用情報保護のための措置」として「民事訴訟手続きによる救済」「行政機関による監督」「自主規制による対応」等の様々な手段が提案されており、刑罰についても次に引用する７つの詳細な提言[48]がなされている。

（１）個人信用情報の漏洩事件が数多く発生していることや、情報保有者が情報管理を適切に行っていたとしても、外部のものの侵害行為を完全には防止することができないことから、刑罰の適用により個人信用情

[48] 報告書「Ⅲ　個人信用情報保護のための措置」の「10. 刑罰の適用等」を参照。http://www.fsa.go.jp/p_mof/singikai/kojin/tosin/1a029e1.htm.

報の漏洩、不正取得等の抑止を図ることが必要であると考えられる。情報主体と契約関係にある場合には、契約に基づくコントロールが可能であるが、契約関係にない第三者の侵害行為については、刑罰による抑止以外には特段有効な手段がない。

（2）刑罰の適用を考える場合、現状では個人情報一般について、その侵害行為が刑罰の対象とされているわけではないこととのバランスや、また、補充性の原則（他の手段で抑止が可能であれば、まず、それを用い、刑罰は補充的に用いるとの考え方）を考慮する必要がある。したがって、刑罰適用による保護の対象としては、個人信用情報の全てとするのは適当ではなく、ハイリーセンシティブ情報や信用判断に直結する情報等重要な情報に限定すべきであるとも考えられる。実際に情報漏洩、不正取得等が生じる場合には、通常これら重要な情報も含まれていることから、処罰の適用対象を限ったとしても問題解決に不都合は生じないものと考えられる。他方、情報の内容・種類による区別は困難であり、与信業者等が収集・保有する個人信用情報を全て対象とすべきという意見もあった。なお、刑罰の対象とならないものについても、行政罰等により担保措置を講じることは必要である。

（3）情報保有者による不正行為としては、情報の漏洩、不正提供、不正利用があるが、これらに対し刑罰を科す必要がある。場合によっては、いわゆる両罰規定によって法人に対しても刑罰（罰金）、業務停止等の行政処分を課すことも考えられよう。なお、最近の事件の実態を見ると、内部の従業員や元従業員が無断で不正提供、不正利用を行うケースが一般的である。このようなケースについても、同様に処罰の対象とする必要がある。また、従業員による不正に対しては刑罰の適用だけではなく、業者自体が服務規定により処分を行うことも必要である。

（4）例えば、信用情報機関の内部の者、あるいはネットワークに侵入した外部の者が登録データを改ざんする等情報の偽造を行った場合、電磁的記録不正作出罪等刑法による一定の措置はあるが、個人信用情報の内容の正確性が担保されることは、信用情報システムの維持に不可欠であること、また、情報主体にとっても情報の内容は個人の信用を左右するものであることから、同法が適用できない範囲に対する措置も必要である。

（5）業務受託者による不正行為として、情報を不正に蓄積し、それを利用・提供することもあり、こういった行為に対する措置も必要である。（6）外部のものによる不正行為として、窃取、詐欺、強迫その他不正の手段により情報を取得することがある。従来、情報が記録されたフロッピーディスク等の「物」を窃取した場合には窃盗罪の適用が可能であったものの、情報自体の窃取は処罰できなかったが、個人信用情報の不正な取得を刑罰の対象とする必要がある。

（7）近年の情報漏洩事件の多発は個人信用情報が名簿業者等で売買され、流通されるようになったことが一つの要因として考えられる。情報の不正な流通を防止することは、これらの事件の再発の防止にも役立つものと考えられる。この観点から、不正取得又は不正提供された情報であると知りつつ情報を入手し、その利用・提供を行うことに対する措置も必要である。

第1款・第2款で扱った個人情報保護検討部会と個人情報保護法制化専門委員会による議論では、構成要件化が困難であること、刑罰の謙抑性を担保しなければならないことを理由として、刑罰の適用について慎重な姿勢が採られていた。個人情報保護法制化専門委員会の議論では、個人情報の「質」と「侵害態様」に応じて、個人情報の侵害に対する処罰の範囲を限定すべきとする見解が主張されていたものの、結果的に、専門委員会の「大綱」にも個人情報保護法にも反映されていない。一般法としての個人情報保護法制定のための議論に比して、「個人信用情報・利用の在り方に関する懇談会」による報告書は、情報の侵害行為に対する刑罰の適用に積極的な姿勢を採っており、間接罰ではなく直接的な刑罰の適用が示唆されている。報告書によると、個人信用情報保護の必要性の根拠は次の通りである。

まず、①個人信用情報の漏洩が相次いで社会問題となっており、この保護のための法整備が緊急の課題となっていることである。次に、②個人信用情報は、与信時に半ば強制的に提供を求められること、③その内容も個人の信用力を判断するため、個人生活に係わる詳細な、かつセンシティブな情報が中心であり、いわゆる与信業者のみが信用情報機関を通じて登録された情報を利用することができ、与信業者間で共有されることが多いこと、そして、④情報の持つ経済的な価値が大きいため、実

際に情報の不正入手・目的外利用の事件が発生していること[49]が根拠とされている。このように、報告書において個人信用情報の刑法的保護が積極的に提言されていることの背景には、個人信用情報の重要性がある。そして、個人信用情報は「与信業者に対して開示しなければ与信を受けられないという事情のもとで半ば強制的に提供させられるものであるから、医者に対して自己の病歴等のプライヴァシーを開示しなければ適切な医療が受けられない場合と同様の関係」にあるので、「秘密漏示罪で保護されるのと同等の刑法的保護の適格性を有するものといいうる」[50]。「報告書」においても刑罰の謙抑性・補充性には言及されていたが、個人信用情報のこれらの特徴から、刑罰適用の必要性が重視されたものと思われる。

信用情報については、2006（平成18）年に貸金業法が改正され、41条の16により「指定信用情報機関の役員若しくは職員又はこれらの職にあった者は、信用情報提供等業務に関して知り得た秘密を漏らし、又は盗用してはならない」との守秘義務が規定され、47条の３第１項５号により、守秘義務の違反が処罰されることが規定されている。

そして、41条の38第１項は次のように定める。

「加入貸金業者又はその役員若しくは職員は、次に掲げる調査以外の目的のために加入指定信用情報機関に信用情報の提供の依頼（第１号の資金需要者等及び第２号の主たる債務者に係る他の指定信用情報機関が保有する個人信用情報の提供の依頼を含む。）をし、又は加入指定信用情報機関から提供を受けた信用情報を返済能力等調査以外の目的に使用し、若しくは第三者に提供してはならない。

１．当該加入貸金業者の顧客である資金需要者等の借入金の返済能力その他の金銭債務の弁済能力の調査

２．前号に掲げるもののほか、当該加入貸金業者が締結する保証契約に係る主たる債務者の借入金の返済能力その他の金銭債務の弁済能力の

---

[49] 報告書「Ⅱ基本的考え方　１．個人信用情報保護の必要性（５）」を参照。http://www.fsa.go.jp/p_mof/singikai/kojin/tosin/1a029d1.htm.

[50] 西田典之「個人信用情報と刑事罰」『刑法解釈論集』（成文堂・2013年）303頁（初出ジュリスト1144号（1998年））。

調査」

41条の38第２項は「加入貸金業者又はその役員若しくは職員は、加入指定信用情報機関から提供を受けた信用情報について、これらの者に該当しなくなった後において、当該信用情報を使用し、又は第三者に提供してはならない」と規定することにより、個人信用情報の目的外使用を禁止し、47条の３第１項６・７号により、目的外使用が犯罪となることが定められている。

指定信用情報機関制度は、信用情報の適切な管理や全件登録などの一定の要件を満たす信用情報機関を内閣総理大臣が指定し、貸金業者が借り手の総借入残高を把握できる仕組として新設された。刑法134条の秘密漏示罪と各種職業の者による秘密漏洩の罪と同様、秘密や情報の漏洩を処罰されるのは（共犯でない限り）あくまでも守秘義務者に限られ、守秘義務者から何らかの方法で当該秘密や情報を知った非守秘義務者が第三者にそれを漏らす行為は処罰対象ではないので、信用情報の保護が十分であるとは必ずしもいえない。しかし、一般的な個人情報の漏洩等を直接的に処罰する法規定が存在しない中、改正貸金業法の枠組みにおいて信用情報が刑法的保護の対象とされているのは、個人情報の重要性に基づく保護が行われているという点で妥当である。

第７節　小括

本章では、日本の現行法において個人情報や個人の秘密がどの程度保護されているのかということについて検討してきた。

まず、刑法134条の秘密漏示罪をはじめとする様々な職業についての秘密漏洩の罪によって、個人の秘密は様々な局面で厚く保護されているように見える。たしかに、個人情報の漏洩などの不正な取り扱いは、個人情報や秘密を知る機会のある職業の者によることが多い。しかし、法律で定められた守秘義務者以外の者による個人情報・秘密の漏洩が行われる危険性もある。刑事事件を起こした少年の精神鑑定を行った医師の秘密漏示罪が問題となった前掲最決平成24年２月13日では、ジャーナリストＣが被告人の精神科医に対して情報提供を積極的に要求して、被告人から得た情報をもとに少年についての書籍を出版したが、秘密漏示罪

の教唆や幇助等で処罰されることはなかった。秘密漏示罪は特定の職業の者が個人の秘密を漏らすことを処罰する規定であるがゆえに、何らかの方法で個人の秘密を知った非守秘義務者が秘密を漏らし、それによって秘密主体の利益が侵害されたとしても、処罰することはできない。秘密漏示罪、そして各種の秘密漏洩の罪にはこのような処罰の間隙がある。

続いて、信書開封罪は、個人の秘密に対する抽象的危険犯なのか、信書の秘密の形式や信書を勝手に開かれない利益に対する侵害犯なのかという点で争われている。そして、信書が個人のものに限定されるか否かという点でも争われているが、信書の内容が個人に関するものであれば、それを開封されたことによって個人情報や秘密を探知され得る。したがって、本罪は信書という範囲内で個人情報や秘密を保護しているといえる。

秘密漏示罪と信書開封罪は個人的法益に対する罪であり、個人との関係で情報や秘密を保護している。その一方で、不正アクセス禁止法や不正指令電磁的記録に関する罪は、それぞれコンピュータ・プログラムの安全性・健全性に対する社会の信頼、アクセス制御に対する社会的な信頼が保護法益であるとされており、個人情報そのものは保護法益として位置付けられていない。また、支払用カード電磁的記録に関する罪では、電磁的記録の情報を窃取する行為が処罰の対象となるが、本罪の保護法益は電磁的記録の真正性と支払決済システムへの社会的信頼であって、個人のカード情報そのものではない。このように、現行刑法典では、個人情報は断片的に保護されているにすぎない。

個人情報保護の一般法としての法的性質を有するのが、個人情報保護法である。本法では、個人を識別する情報が幅広く保護されており、個人情報取扱事業者は個人情報保護のために様々な義務を有する。義務違反に対して直ちに刑罰が発動されるのではなく、主務大臣の命令に違反した場合に初めて罰則の対象となる。

個人情報保護法の法制化につき、個人情報保護検討部会と個人情報保護法制化専門委員会で議論が行われ、それぞれ「中間報告」及び「大綱」が提示されている。個人情報の侵害に対する刑罰を設けることにつき、両者ともに刑罰の謙抑性という観点を重視していたが、専門委員会は民事責任の有効性に懐疑的であり、刑罰に対する抵抗感が少なかったよう

に見受けられる。検討部会の中間報告には罰則について具体的な提案がなかったが、専門委員会の大綱には主務大臣の命令違反に対して罰則を設ける旨が記載されている。専門委員会の議論の段階においては、個人情報の「質」と「行為態様」に応じた罰則の在り方が提案されていたにもかかわらず、実際の大綱には間接罰という広く薄い刑罰方式が提示され、それが現行法のもととなった。個人情報の「質」と「行為態様」に応じた構成要件化が困難であることも議論の中で指摘されていたが、このような罰則方式では重要な個人情報に対する重大な侵害も、軽微な個人情報の侵害も同様に扱われることとなり、罪刑の均衡を欠く。情報の重要性に応じた保護という点で、改正貸金業法が指定信用情報機関による信用情報の漏洩等を処罰しているのは妥当である。現行の個人情報保護法のように広く薄い刑罰を一律に科すのではなく、個別具体的な状況に応じた構成要件化のための議論が必要である。

そこで、個人情報の侵害に対する妥当な規制方法について検討するために、第３章、第４章、第５章では、イギリス・フランス・ドイツの個人情報保護法制における処罰規定についての判例・学説・第三者機関による報告について触れ、刑罰や第三者機関による規制がどの程度功を奏しているのかを検討する。

［付記］　本稿は、北海道大学審査博士（法学）学位論文（2014年３月25日授与）「個人情報の刑法的保護の可能性と限界について」に加筆・修正したものである。