論　　説

個人情報の刑法的保護の可能性と限界について（2）

佐　藤　結　美

目　　次

第３章　イギリス法における個人情報保護

第１章・第２章では、日本の現行法の枠組みにおいて、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を検討した。用紙等の有体物に化体されている個人情報については、窃盗罪や横領罪等の財産犯の枠組みで保護する試みが従来の判例によってなされており、第１章で述べた通り、事案による限界があるものの、一定の意義がある。

一方、本研究で検討するのは、有体物に化体されていない個人情報そのものが窃取されたり、無断で第三者に提供されたりした場合の扱いである。現行法上、個人情報や個人の秘密を、個人との関係において刑罰によって保護するのは、刑法133条の信書開封罪と、134条の秘密漏示罪（これに加えて、特別刑法における特定の職業の者についての秘密漏洩の罪）、そして（間接罰方式ではあるが）個人情報保護法である。信書開封罪と秘密漏示罪が、限定された条件下で個人情報や秘密を保護しているのに対して、個人情報保護法は一般法として位置付けられているものの、主務大臣の命令に違反して初めて刑罰を科されるという間接罰方式が採られている。このように、日本の現行法には個人情報の窃盗や第三者提供といった侵害行為を直接的に処罰する規定が存在せず、近年問題となっている個人情報の漏洩や売買等に対して効果的に対処するのが困難である。したがって、本稿ではイギリス・フランス・ドイツの個人情報保護法を参照することにより、直接的な刑罰も視野に入れた個人情報保護の在り方について検討する。

そこで本章では、イギリスの1998年データ保護法（Data Protection Act 1998）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。後述するように、1998年データ保護法は、不正に個人データを取得等した者を直接的に処罰する規定を設けており、データ保護についての第三者機関である情報コミッショナーが情報保護のための厳罰化に積極的な姿勢を示している。個人情報の侵害を処罰する規定を日本法に設けることを検討するにあたり、イギリス法における直接罰規定の意義と、情報コミッショナーの役割と実務について分析する。

まず、1998年データ保護法が成立するまでの過程について述べる。

コンピュータの普及に伴うデータ保護立法の必要性と、データの取り扱いによる個人のプライヴァシーへの脅威に関する議論が起こり、1998年データ保護法の前身である1984年データ保護法（Data Protection Act 1984）が制定された。1984年データ保護法制定前の法律は、各種機関によって保有される多くの個人情報の取り扱いに対する規制としては不十分であったことから、国際法律家委員会イギリス支部（Justice）は1970年に「プライヴァシーと法（Privacy and Law）」という報告書を発表した。この報告書では、権利を侵害された者が不法行為を主張することを可能にするような、プライヴァシーの法的な権利を確立すべきであることが提案された。報告書には、プライヴァシー権法の草案も含まれていたが、これらの提案は「表現の自由」が制限されることを懸念した報道機関からの批判の対象となった。そこで政府はプライヴァシーの法的保護を検討する委員会の設置を決定した。

続いて1972年に、Kenneth Younger を委員長とするプライヴァシー委員会（Committee on Privacy）は、個人データを処理するコンピュータの使用にあたって次のような10の指針を発表した[1]。

（a）　情報は､特定の目的のために保有するとみなされるべきであり、適切な許可なく他の目的のために使用されてはならない。

（b）　情報へのアクセスは、情報を提供した目的のために許可された者に限定するべきである。

（c）　収集または保有される情報の量は、特定の目的を達成するために必要最小限にすべきである。

（d）　統計目的のために情報を処理するコンピュータシステムでは、識別データと残りのデータを分離するための設計及びプログラムにおいて、適切な対策をすべきである。

（e）　主体が自らについて保有される情報について知らされる手段を準備すべきである。

（f）　システムによって達成されるべき安全のレベルは、事前に利用者が決定すべきであり、情報の意図的な濫用や誤用に対する予防策も含

[1] Report of the Committee on Privacy (Cmnd.5012,1972), 183-184. 委員長の Younger の名前から、Younger Report と称されることがある。

むべきである。

（g）　監視システムは、セキュリティーシステムの違反の探知を容易にするために提供されるべきである。

（h）　情報システムの設計において、情報保有期間の限界を定めるべきである。

（i）　保有されるデータは正確でなければならない。不正確な情報を是正し、最新化するための機構が必要である。

（j）　価値判断の規約化に注意を払うべきである。

Younger 委員会は、個人や各種機関によるプライヴァシーの侵害に対して更なる保護を与えるための立法が必要か否かを検討していたので、委員会はデータの保護よりもプライヴァシーの保護の方により関心を持っていた。Younger 委員会の提案は立法には至らなかったが、委員会の報告を受けたイギリス政府は、将来的に設置するデータ保護委員会の委員長に Younger を指名していた。しかし、Younger が死亡したことにより Norman Lindop が委員長に就任することとなった。

Lindop 委員会は報告書において、以下のように述べている。

「Younger 委員会はプライヴァシーについて扱っているが、我々はデータ保護について扱う。実際、この２つの領域は一部重なっており、重なる部分は『情報プライヴァシー』または『データプライヴァシー』と呼ばれる。これは重要な領域であり…（中略）…データプライヴァシーの概念と意義、その結果を検討することは有意義なことである。この目的のために、データプライヴァシーという用語を、自分に関するデータの伝達に対するコントロールを個人が要求することという意味で用いる」[2]。

Lindop 報告書は、データ保護のための機関を設立し、ビジネス界によるデータの取り扱いに対する特別な法典を制定するべきであると提言する。Lindop 報告書はデータ保護を検討対象とした上で、プライヴァシー権を「ひとりで放っておいてもらう権利」ではなく「自己情報コントロール権」として解すべきことを明らかにした。当時の政権交代によ

[2] Report of the Committee on Data Protection (Cmnd.7341,1978), 9-10. 委員長の名前から、Lindop Report と称されることがある。

り、結果的にLindop報告書も立法には至らなかったが、その内容は1984年データ保護法に受け継がれることになった。

このように、1984年データ保護法は、個人データの濫用や誤用によるプライヴァシー侵害に対する保護の必要性という観点から制定されたが、1995年10月14日のEUデータ保護指令（EU Directive on Data Protection）に基づく法改正が行われた。EU指令が出された場合、加盟国は指令の内容に沿った国内法を制定することを義務付けられるので、多くの加盟国が法律の制定や改正を行った。データ保護指令は、加盟国間の情報流通を容易にするために、加盟国間における個人データ保護のレベルの格差を撤廃することを目的としている。データ保護指令７条は、個人データが取り扱われる前に満たさなければならない多くの条件を定めており、データの取り扱いが法的義務の履行に必要な場合や、データ主体の生命にかかわる場合などの例外的な場合を除いて、データの取り扱いにはデータ主体の同意が必要であるとされている。そして、指令８条では、個人の人種・民族的出自、政治的意見、宗教的・哲学的信条、労働組合の一員であること、健康または性生活に関する情報といった特別なカテゴリーの情報[3]の取り扱いに際し、一定の厳格な条件を満たすことが必要であり、その中の１つがデータ主体の明確な同意であることが規定されている。続いて、データ保護指令12条・14条・15条はデータ主体の権

[3] 2012年１月25日に欧州委員会は「個人データの取扱い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規則提案」を公表し、2014年３月12日に欧州議会がその修正案を第１読会で可決した。1995年のEUデータ指令を改正するものであり、加盟国の立法措置を必要とする「指令」から、加盟国に直接適用される「規則」への変更がなされるものである。

規則提案９条では、これまでEUデータ指令８条で「特別なカテゴリーの個人データ」として規定されていたものの他に、遺伝データと刑事上の有罪と、それに関連する保安処分に関するデータが追加されている。そして、議会修正案では性的指向（sexual orientation）、性同一性（gender identity）、労働組合活動、バイオメトリックデータ、行政的制裁、判決、犯罪の容疑が追加された。

一般データ保護規則提案についての解説として、石井夏生利・牧山嘉道「海外の個人情報・プライバシー保護に関する法制度（２）－最新の国際的動向－」国際商事法務42巻６号（2014年）901～912頁がある。

利について規定している。

このようなデータ保護指令に従って1998年データ保護法が制定され、2000年３月１日に施行された。1984年法との主な相違点は以下の通りである。まず、1998年法では、自動処理されたデータのみならずマニュアルデータにまで保護の対象が拡大されている。続いて、指令の内容を受けて、一般的な個人データとは別に、より厳格な保護を要する「センシティブな個人データ」という概念が設けられた[4]。そして、EU 加盟国間の適切な情報流通という趣旨を有するデータ保護指令を受けて、情報の取り扱いについて一定の条件を満たさない限り、欧州経済領域（European Economic Area）に加盟していない国にデータを流通させることが禁止されるようになった。データ主体の権利も強化され、データの不正な取り扱いによって被った損害や苦痛に対する損害賠償が認められるようになった。このように、1998年法は個人データの保護と監督をさらに強化するものとして成立した[5]。

第１節　1998年データ保護法の概要

本節では、1998年データ保護法の概要について述べる。

---

[4] 1984年データ保護法にも類似の規定は存在したが、「センシティブな個人データ」という文言は用いられていない。1984年法２条３項は、「国務大臣は、次に掲げる事項に関する情報からなる個人データに関し、追加的保護措置を講ずるため、命令により、データ保護原則を修正し、または補足することができる。(a) データ主体の人種、(b) データ主体の政治的意見もしくは宗教的信条またはその他の信条、(c) データ主体の肉体的もしくは精神的健康状態またはその性生活、(d) データ主体の犯罪歴」と定めている。他の一般的な個人データよりも厳重な保護をし得ることが定められつつも、実際にどれほど保護を厚くするかということは国務大臣の裁量に委ねられていたという点で、1998年法と異なっている。

[5] 1998年データ保護法成立までの過程については、Peter Carey, Data Protection: a practical guide to UK and EU law, 1-10 (3d ed 2009), Gerald Dworkin, Report of Committees The Younger Committee Report on Privacy, Vol.36 Issue4,The Modern Law Review, 399-400 (1973) を参照した。

第１項　基本事項について

この法律では、「個人データ（personal data）」が保護の対象になる。個人データとは、「(a) データによって特定される生存中の個人に関する当該データ、または (b) データ管理者が保有するか保有する可能性があり、かつ個人に関する意見（opinion）の表明及び個人に関するデータ管理者若しくは他の者の意向（intention）の表示を含む、データ及び他の情報によって特定できる生存中の個人に関するデータ」[6]と定義されている（１条（１）項）。たとえば、特定の者が「怠け者である」というのは「当該個人に関する意見の表明」であり、「怠け者であるから、解雇する」というのは「意図の表示」とされている[7]。したがって、日本の個人情報保護法における「個人情報」より範囲が広いと言えるので、本章では保護の対象を「個人データ」「センシティブデータ」と表記する。また、この法律では一般的な個人データよりも厳格な取り扱いを要する「センシティブな個人データ（sensitive personal data）」という概念がある。

この法律では、データ主体（data subject）である生存する個人には、次の権利が認められている。それは、①個人データへのアクセス権（７条）、②個人に損害や不利益をもたらし得る取り扱いを止めさせる権利（10条）、③ダイレクトマーケティング（11条（３）項において、特定の個人に向けられた広告または宣伝資料のあらゆる手段による伝達を意味すると規定されている）を目的としたデータの取り扱いを止めさせる権利（11条）、④個人に関する評価などを行う目的で、自動的手段による取扱いのみに基づいて個人に重大な影響を及ぼす決定を下すというオンライン決定（automated decision-taking）を行わないよう求める権利（12条）、⑤損害賠償を請求する権利（13条）、⑥不正確な個人データを修正（rectification）、封鎖（blocking）、抹消（erasure）、破棄（destruction）する権利（14条）である。

---

[6] イギリスのデータ保護法の邦訳は、木村光江・星周一郎「海外の個人情報保護法における刑事規制（１）イギリスのデータ保護法の概要とその運用状況―刑事規制を中心に」クレジット研究27号（2002年）258 ～ 268頁と、石井夏生利『個人情報保護法の理念と現代的課題』（勁草書房・2008年）を参照した。

[7] 堀部政男「個人情報の法的保護」法とコンピュータ20号（2002年）70頁。

この法律において、データの処理に関わるのは「データ管理者（data controller）」である。データ管理者は、「（４）項の規定に従い、（単独または共同で、または他の者と協力して）個人データが処理され、または処理されるべき目的および方法を決定する者」（１条（１項））と定義されていて、個人・法人・社団の如何を問わないとされている。この法律ではデータの取り扱い（processing）が規制されているが、「取り扱い」とは「情報やデータの取得、記録または保有、何らかの操作や一連の操作をすること」であり、「(a) 情報やデータの編成、修正、変更、(b) 情報やデータの検索、参照、利用、(c) 伝送、頒布その他の方法によって情報やデータを提供すること、(d) 情報やデータの配列、結合、封鎖、抹消、破棄」を含む（１条（１）項）。

データ管理者には、①情報コミッショナー（Information Comissioner）に通知する義務（通知について、16条から26条まで）と、②データ保護８原則（後述）を遵守する義務がある（４条（４）項）。情報コミッショナーは、単独法人（corporation sole）であり、女王・政府から独立してデータの取り扱いを監督する機関である。データ保護法違反のおそれのある事業所等を調査したり、参考人に対する事情聴取といった行政的な措置を採ったりしている。そして、データ管理者は情報コミッショナーへの通知義務に基づいて、個人データを取り扱うにあたって、データに関する項目と、第７データ保護原則（情報の安全性の確保）を遵守するための措置を通知しなければならない（18条（２）項）。

第２項　データ保護原則（Data Protection Principles）について

ここでは、データ保護法４条（４）項により、データ管理者が遵守すべきとされるデータ保護原則について述べる。1998年データ保護法の附則（schedule）１には、８項目のデータ保護原則が規定されており、データの取り扱いにおける重要な指針となっている。

まず、第１原則は、「個人データは公正に、合法的に処理されなければならない（Personal data shall be processed fairly and lawfully）」と規定した上で、「センシティブな個人データ（sensitive personal data）」と言われる重要な情報（後述）については、後述する附則３の条件のうち少なくとも１つを遵守する必要があり、その他の個人データ一般につ

いては後述する附則２の条件のうち、少なくとも１つの遵守が必要であるとされている。附則２の規定する条件には、①データ主体がデータ処理に同意していること、②データ主体が当事者となる契約を実行するためにデータ処理が必要であること、③データ主体の重要な利益をはかるためにデータ処理が必要であることといったものがある。

第２原則は、「個人データは１つまたは２つ以上の特定の適法な目的のためにのみ取得されなければならない。そして、その目的またはそれらの目的と適合しない方法でさらに処理されてはならない」として、限定された目的のためのデータ処理を指示している。

第３原則は、「個人データは処理される目的に応じて適切で、関連するものでなければならず、取り扱われる目的あるいは諸目的に照らして過度であってはならない」として、データ処理の目的適合性を規定する。

第４原則は、個人データは正確（accurate）で、必要に応じて最新のものでなければならない（where necessary, kept up to date）と規定する。

第５原則は、個人データは取り扱われる目的のために必要な期間よりも長く保管されてはならないと規定する。

第６原則は、個人データはこの法律におけるデータ主体の権利に基づいて取り扱われなければならないと規定する。

第７原則は、無許可による、あるいは不法な個人データの取り扱い、または個人データの偶発的な損失・破壊・個人データに対する損害が発生しないように、適切な技術的・組織的措置が採られるべきであると規定する。

第８原則は、欧州経済領域（EEA）以外の国または地域に個人データが移転されてはならないと規定する。ただし、当該国または地域が個人データの処理に関して、データ主体の権利または自由に対して十分なレベルの保護を保障している場合を除く。

第３項　罰則について

続いて、データ保護法における罰則について概要を述べる。

第１款　データ保護原則の違反

データ管理者がデータ保護８原則に違反した場合には、まず、情報コ

ミッショナーから執行通知（enforcement notices）が出される。執行通知について、1998年データ保護法40条（１）は以下のように定める。「データ管理者がデータ保護原則に違反したか、もしくは違反していることをコミッショナーが確信した場合には、コミッショナーはデータ管理者に対して通知（本法では「執行通知」という）を出すことができる。その通知は、データ管理者に対して、当該原則または諸原則の遵守のために、以下のいずれか一方または両方を行うように要求することができる。

（a）通知に明記されるであろう期間内に、明記された措置を行うこと、または、通知に明記されるであろう期間の後は、明記された措置を行わないこと

（b）明記されるであろう期間の後は、いかなる個人データ、もしくは通知に明記されたいかなる個人データの取り扱いも行わないこと、または、明記された目的で、もしくは明記された方法で個人データを取り扱わないようにすること」

データ管理者は違反があった、または違反が行われていると判断された当該データ保護原則につき、上記の執行通知を受けることになっており、通知の内容に基づいて是正措置を採ったり、データの取り扱いを中止したりすることを要求される。

また、執行通知とは別に、情報通知（information notices）（43条）、特別情報通知（special information notices）（44条）がある。前者は、個人データの取り扱いに利害のある者から、データ保護法が遵守されているか否かについての評価（assessment）の請求があった場合に、またはデータ保護原則に違反しているか否かを判断するという目的による情報請求があった場合に、情報コミッショナーがデータ管理者に対して、請求に関する指定された情報（specified information）を提出すること、またはデータ保護原則の遵守を要求する通知を出すことができる、という制度である。後者は、データの取り扱いが特別目的（special purpose）[8]のためだけに行われていないことをコミッショナーが疑う合理的な根拠がある場合には、コミッショナーはデータ管理者に対して、指定された

[8] データ保護法３条によると、(a) ジャーナリズムの目的 (b) 芸術目的 (c) 文学的目的の中の１つ以上に該当するものをいう。

情報を提出するように要求する通知を出すことができるという制度である。

そして、データ管理者が執行通知・情報通知・特別情報通知を無視した場合に、刑事罰が科される（47条１項）。このように、データ管理者はデータ保護原則に違反しても直ちには処罰されず、違反に対する是正通知を無視した場合に初めて刑罰の対象となるという点で、日本の個人情報保護法における主務大臣の命令に対する違反のように、間接罰方式が採られている。

第２款　個人データの不法取得等の罪

データ管理者に対する処罰規定の他に、データ保護法には、「個人データの不法な取得等（unlawful obtaining etc. of personal data）」を行った個人に対する処罰規定がある。データ保護法55条（１）項では、「何人も、データ管理者の同意がなければ、故意または無謀に（knowingly or recklessly）（a）個人データもしくは個人データに含まれる情報を取得し若しくは開示し（obtain or disclose）、または（b）個人データに含まれる情報について他の者に開示を周旋（procure）してはならない」とされており、55条（３）項において、これらの行為が犯罪を構成するものであることが規定されている。一方で、55条（１）項の行為は、55条（２）項に該当する場合には許容される。55条（２）項は、「（a）個人データの取得、開示、または他の者に開示の周旋をする行為が、（i）犯罪を予防するため、または犯罪捜査のために必要である場合、（ii）制定法、法の規則、または裁判所の命令（order of a court）によって要求され、または正当化される場合、（b）データや情報を取得したり開示したり、事情によっては情報の開示を他の者に周旋したりする法律上の権利があるとの合理的な信念（reasonable belief）を持って行為した場合、（c）データ管理者が取得、開示または周旋が行われたこととその状況を知っていれば、データ管理者の同意を得たであろうとの合理的な信念を持って行為した場合、（d）特別の状況において、取得・開示・周旋行為が公共の利害（public interest）に資するものとして正当化される場合」には55条（１）項の対象にはならないと規定している。

55条（１）項所定の行為の他に、55条（４）項では（１）項に違反して

個人データを売却する行為が処罰され、55条（５）項（a）号では（１）項に違反してデータを取得した上で個人データの売却を申し出る行為が、(b) 号では売却を申し出た後に（１）項に違反してデータを取得する行為が処罰の対象となる。データの取得や開示・周旋に対しては正当化事由が存在するのに対して、売買やその申し出については正当化事由が規定されておらず、後者の行為態様は侵害性が高いものと解されているのではないだろうか。

55条違反の罪の法定刑は、①略式起訴による有罪判決の場合は「法定最高額（the statutory maximum）」を超えない罰金であり、②正式起訴による有罪判決の場合は罰金額の上限がない（60条（２）項）。1991年刑事司法法（Criminal Justice Act 1991）[9]17条によると、略式起訴による有罪判決の場合の「法定最高額」は5000ポンドである。そして、55条違反の罪を犯した者に対して拘禁刑を科す旨の命令を主務大臣が発布することが可能になった[10]。

以上、イギリスの1998年データ保護法の概要について整理した。1998年データ保護法については、以下のことが問題となる。第１に、データ管理者の同意なく情報を不正に取り扱った個人が55条による直接罰の対象となっているが、55条の射程範囲と意義は何かということである（第２節）。続いて、女王・政府から独立した第三者機関である情報コミッショナーが、個人情報の保護のためにどのような活動を行っているのかということである（第３節）。そして、センシティブな個人データの詳細と、その合法的な取り扱いの条件と、一般的な個人データの取り扱い条件との違いについて検討する（第４節）。

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

本節では、1998年データ保護法における個人データ不法取得等の犯罪の意義と射程範囲について検討する。

---

[9] 1991年刑事司法法の解説について、瀬川晃『イギリス刑事法の現代的展開』（成文堂・1995年）77 ～ 81頁などがある。

[10] 詳細は第２節第２項で後述する。

前述の通り、1998年法55条では、データ管理者の同意なく個人データを取得・開示したり、個人データの開示を周旋したり売却したりするといった幅広い行為が、個人データの不法な取り扱いとして処罰の対象となっている。これは「情報窃盗」等の行為を処罰する規定の一例であり、日本の実定法には存在しないものである。個人情報の侵害に対する妥当な処罰のあり方を検討するにあたって、1998年データ保護法55条の罪の成立条件について検討する。

第１項　1998年データ保護法55条の制定過程と行為態様

1998年データ保護法55条では、データ管理者の同意なく個人データを取得、開示、他人に対し開示の周旋をした者を直接処罰する規定であるが、この法律の前身である1984年法（Data Protection Act 1984）にはこのような規定は存在せず、これらはEUデータ保護指令に由来するものでもない。1984年法５条（１）項では、データ利用者（data user）、または他の者にデータに関するサービスを提供するコンピュータ・ビューロー（computer bureau）をも営むデータ利用者として登録簿に登録されていない限り、個人データを保有（hold）することが禁止されていた。５条（５）項では、（１）項に違反した者、または故意や無謀によって５条の他の規定に違反した者は有罪となることが規定されている。このように1984年法では、個人データの取り扱いについては登録が義務付けられていたので、５条（２）項以降では、登録されている個人データの種類や目的を超えて個人データを保有または使用（use）したり、登録外の者に個人データを開示（disclose）したりする等の行為が禁止されていた。登録をした者のみが個人データを取り扱うという前提に立っていたことから、無権限者が個人データを保有することを超えて、個人データを開示したり売却したりする行為を処罰の対象とするという発想がなかったものと思われる。しかし、データ管理者以外の個人がデータを不正に取り扱う行為を広く処罰する現行法55条が設けられるに至った背景には、後述するように、不正な行為によって、第三者が情報を入手するケースが増えて社会問題となっており、これを予防するために刑罰への期待が寄せられたことがある。

情報コミッショナー事務局（Information Commissioner's Office）が

2006年５月10日に提出した報告書「プライヴァシーの価値とは何か？（What price privacy?）」[11]において、55条成立の間接的な原因となった具体的事件が紹介されている。それは、1992年11月に、当時の大蔵大臣であったNorman Lamont氏のクレジットカードの購入記録に関する情報を銀行員が洩らしたというものである。その後、彼がロンドンの酒類小売店で購入したものについての報道が過熱し、「大蔵大臣がJulian Barnesで赤ワインを購入した」という雑誌記事も発表された。この事件において、個人の銀行や税金記録に関する情報と他の個人情報が開示されたという問題は、当時のデータ保護登録官（現在の情報コミッショナー）であったEric Howeによる1993年の年次報告で取り上げられた。Eric Howeは、個人情報への不正アクセスを試みたり実際に行ったりする者に対する処罰という考え方について論じた。第３節で詳述するが、情報コミッショナーは個人データの保護のための厳罰化に積極的である。

続いて、1994年にはイギリス情報局長のStella Rimingtonの私生活についてマスコミが報道するという事件[12]が発生した。報道によって、彼女が火曜日の午後にいつも買い物をする場所についての情報が開示されたが、この情報は彼女が利用する金融機関に偽の電話を掛けることで入手されたものであることが判明した。この件についての苦情がデータ保護登録官事務局（the Office of the Data Protection Registrar. 現在の情報コミッショナー事務局）に寄せられたが、偽の電話によって情報を入手した者が「データ使用者」としての登録をしていなかったことにつき、故意も無謀もなかったということにより、事務局は訴追しないことを決定した。このような事件は、ジャーナリストや私立探偵等によって不正に個人情報が入手され得ることを明らかにした。

1994年３月の貴族院の議論で、政府は不正によって個人情報へのアクセスを得る行為について特別の犯罪規定を設けるつもりであることを発表した。これを受けて、1994年刑事司法及び公共秩序法（Criminal Justice and Public Order Act 1994）161条により、1984年データ保護法５条の罰則が拡大された。この法改正により、コンピュータに入力され

[11] 詳細は第３節で後述する。

[12] Rosemary Jay, Data Protection Law and Practice,717 (4th ed 2012).

た個人情報の開示、開示の周旋、売却等の行為を処罰する条項が設けられ、1998年データ保護法では対象が個人データ一般に拡大された。

以上の法改正により、55条において処罰の対象となる行為の範囲が問題となる。1998年データ保護法55条は、データや情報を開示する者と、それらを直接入手したり開示を周旋したりする者を対象にしているが、間接的に情報やデータを入手する者や、情報やデータの入手によって最終的に利益を得る者は含まれていないように思われる。そして、55条（４）項と（５）項では、データや情報を売却する者と、売却を申し出る者が処罰されるが、データの購入者と購入を申し出た者については明記されていない。条文を文字通りに解釈すれば、私立探偵等から情報やデータを間接的に得る者は55条（１）項に抵触しないことになるだろう。

しかし、55条は犯罪となる範囲を1984年法より拡大しており、このことから、55条（１）項は、個人データや情報を直接入手した者に限定していないと考えられる[13]。更に、1998年法は個人データの「取り扱い（proceeding）」の定義を、データについて行われ得ることのすべてに拡大していることから、55条（１）項における「取得（obtaining）」という単語は、単なる情報の呼び出し行為や、コンピュータ・スクリーン上の情報を読むこと等も含んでおり、同様に、私立探偵から情報やデータを入手した弁護士の活動等にも適用され得る[14]。

1998年データ保護法制定以前の事例として、R. v Brown [1996] 2WLR203がある。債権回収会社を経営する友人を助けるために、警察官 Brown が、警察のコンピュータデータベースに貯蔵されている情報をコンピュータ・スクリーンに呼び出すよう同僚に依頼したところ、警察官は1984年法所定の、登録簿に記載された目的を超える個人データの使用の罪で告発されたというものである。この警察官の行為は、単にコンピュータ・スクリーン上に表示されている情報を読んだだけにとどまっていたので、1984年法における「使用する（use）」に該当するか否かが問題となった。この争点につき、貴族院は、「使用する」の概念は、

[13] Catrin Evans, The Offence in Section55 DPA-Unlawful Obtaining of Personal Data, Vol.3 Issue6, Privacy and Data Protection,3 (2003).

[14] Evans, supra note13,at 3.

データベースから情報を検索（retrieval）しただけの行為にまで拡大されないと判断した。一方、1998年データ保護法55条は、個人データに含まれる情報を「取得する」行為を犯罪としているので、現行法の下ではBrownのようにコンピュータ・スクリーン上にある情報を読み取る行為も55条の罪で処罰される可能性がある[15]。このように、個人データや情報を何らかの方法で知る行為は広く55条でカヴァーされている。

また、情報の「開示」行為に関する重要な判例として、R. v Rooney [2006] EWCA Crim1841がある。被告人Jacqueline Mary Rooneyは警察職員であり、他の職員の個人データにアクセスして情報を第三者に開示したとして有罪となった。被告人の姉（もしくは妹）は警察職員Aと2003年に別居した。その後Aは別の警察職員Tとイギリスの Tunstallという地域で同居を開始し、二人の詳しい住所が警察の職員データベースに掲載されていた。被告人はAとTの住所に関する情報に何度もアクセスし、被告人の姉（もしくは妹）に、AとTが現在 Tunstallに住んでいることを伝えたが、正確な住所については言わなかった。被告人は、個人データを取得して第三者にそれを開示したとして訴追されて有罪となったが、被告人は正確な住所を言っていないことを理由に、自己の行為が「開示」に該当しないとして控訴した。これに対して控訴院刑事部は、データ保護法55条（1）項は個人データのみならず、個人データに含まれる情報を開示する行為を処罰対象としていることから、AとTがTunstallに住んでいるという情報から正確な住所を特定することができないとしても、犯罪の成立を妨げないとして被告人の控訴を棄却した。「個人データに含まれる情報」の範囲の解釈如何によって、処罰範囲の無限定な拡大が可能になるので、検討の余地があるだろう。

第２項　55条違反の犯罪の主観的要素

前項では、1998年データ保護法55条の制定までの流れと、55条の処罰対象となり得る行為について扱った。55条（1）項は、データ管理者の

[15] Peter Carey, Data Protection: a practical guide to UK and EU law, 189 (2d ed 2004). 第３版である Carey, supra note 5は、Brown事件について言及していない。

同意なく、(a) 個人データもしくは個人データに含まれる情報の取得または開示する行為、(b) 開示の周旋を「故意または無謀」によって行った場合に処罰の対象となることを規定している。そして、データや情報の売却等の行為もまた、「故意または無謀」によって（１）項に違反することを前提とする。刑罰法規においては、故意犯のみを処罰するのが原則であるので、「無謀」の意義と範囲は重要な問題である。そこで本項では、主に「無謀」の有無が問題となった判例の検討を行う。

（１）Data Protection Registrar v Amnesty International [1995] Crim. L.R.633. (unreported)

この事件が発生した当時は、1984年データ保護法が適用されていた。アムネスティ・インターナショナルのイギリス支部（以下、「アムネスティ」とする）は、他の慈善団体と各々のメーリングリストを交換する協定を結んだ。交換の方法は、他の慈善団体のために運営され、ダイレクトメール発送業務を行っていたメーリングハウスに対して、アムネスティのメーリングリストを開示する（disclosure）というものであり、両者のやり取りは金銭の授受なしに行われた。データ登録官は、アムネスティが個人データを登録外の目的で使用（use）し、個人データを登録されていない者（メーリングハウス）に開示したことから、1984年法の５条（２）(b) 項と (d) 項の罪を犯したとして訴追した。アムネスティがデータを開示したことによって、アムネスティの支持者に対して、協定の相手方となった慈善団体への寄付を求めるメールが送られたので、メールの受取人の一人が登録官に苦情を申し立てたことが端緒である。登録官は、アムネスティがデータの使用と開示が登録内容に沿うものか否かを確認しなかったことにつき、無謀が肯定されると主張した。

有給治安判事（stipendiary magistrate）は裁判の結論において、以下の理由により登録官の訴えを退けた。まず、過去の判例であるＲｖ Lawrence [1982] A.C.510と MPC v Caldwell [1982] A.C.341では、「深刻で有害な結果（serious harmful consequences）」が発生するという予見がなければ無謀の存在は認められないとされている。本件アムネスティの行為の結果は、寄付を要求する望まないメールが届いたことであり、これは「深刻で有害な結果」というよりも苛立たしい（irritating）と表現

される感情的なものにすぎないと判断され、アムネスティに対して無罪が言い渡された。

これに対して、登録官は合議法廷（Divisional Court）に控訴した。控訴審は、訴追者が1984年法５条における主観的条件である「無謀」の存在を証明するには、以下のことを示さなければならないと判示した。

①データ保護法５条が回避しようとしている損害（mischiefs）を発生させ得る可能性に対して、通常の分別ある個人としての注意（attention of the ordinary prudent individual）がなされていたことを示す状況、および、そのような損害の発生する危険（the risk of those mischiefs occurring）が少なくないことから、通常の分別ある個人であればその危険を取るに足らないものとして扱うことはできないということ。

②行為に出る前に、被告人（アムネスティ）がそのような危険の発生する可能性について何らの配慮もしなかったか、可能性については認識していたものの行動に移してしまったこと。

無謀の有無の判断の際には、データ保護法５条（２）項において予定されている損害結果の予見（foresight of the consequences）の有無が問題となったが、本件の評釈では、結果の予見という判断基準をこの文脈で用いるのは不適切であると批判されている[16]。評釈によると、データ使用者として登録している者が、登録されている個人データ以外のデータを保有（hold）した場合に５条（２）(a) 項の犯罪が成立するので、データの保有による結果や損害の予測があったか否かを判断する必要性がないのは明確である。同項で予定されている損害は、保有されるべきではないデータが保有されることであり、それ以上の現在する、予想される、あるいは予想され得る結果について考慮する必要はない。５条（２）(a) 項の意義は明確であり、登録されたデータ使用者が、自己の保有するデータの性質について気づいていないということに注意を払わないことである。この犯罪は無謀によって損害を発生させるという点で軽い性質のものであり、同じ損害を故意によって発生させる犯罪よりも、常に軽く罰せられるべきである。したがって、無謀の有無を判断する際に深刻な結果の予見可能性を求めることは、軽い犯罪をより重い性質の犯罪へと転

[16] [1995] Crim L R 633,634.

化することにつながるという点で疑問であると解されている。

評釈では、データ使用者による５条違反の犯罪の中で最も単純な類型である（２）(a) 項を挙げて論じられているが、当該犯罪による損害の程度がさほど深刻ではない上、故意犯よりも軽い犯罪の構成要素である無謀の有無を判断する際に「深刻な損害の予見可能性」を要求することは妥当ではないという趣旨であると思われる。

（２）Information Commissioner v Islington London Borough Council [2002] EWHC Admin 1036; [2002] All E.R. (D) 381.

この事件も、1984年データ保護法が施行されていた時期に発生したものである。

あるソリシタから、自分の顧客に対して税金の支払いを求める文書を送付するために、自治体がソリシタの事務所の住所情報を用いたという旨の苦情が情報コミッショナー事務局に持ち込まれた。情報コミッショナー事務局の調査の結果、データを使用するにあたって義務付けられている登録の期間が終了していたことが判明し、自治体は催促状が来ていたにもかかわらず、多忙と事務的なミス（pressure of work and clerical error）によって登録更新をしていなかったことを認めた。登録が無効になっている間も、自治体による個人データの取り扱いは続いていたので、情報コミッショナー事務局は、自治体を無謀による1984年データ保護法５条違反で起訴した。

この事例において問題になったのは、データ使用のために登録を義務付けられているのは自治体であったが、個人データを使用したのは従業員であったということである。治安判事裁判所において公訴が棄却され、法律問題記載書（case stated）の方法で上訴された。文書では、無謀の有無を判断する際に、自治体の行為と責任はどのように考慮されるべきであるかということと、確実な登録を怠ったことは無謀を構成するのに十分な要素であるか否かということが問われていた。高等法院女王座部は、「この事件で問題となった自治体のような地域の団体が登録更新をしなかった場合、その不作為の認識があったことが合理的に推測され、このケースでは、自治体が関連する公務員の行為を通して、更新の必要性と、更新をしていなかったことに気づいていたのであれば、その推測

が強化される。その後に、正当な範囲で業務を行う他の公務員の行為の結果として、自治体が登録なしに個人データを用いる場合は、自治体には禁止に対する違反につき、故意または無謀があったと考えるべきである」と判示した。

この事例は、登録更新を怠った主体と実際にデータの使用をした者が異なることから、自治体の無謀の有無を検討する際には、データ使用における従業員の行動を合わせて考慮するという判断枠組みを提示するものである。本件はデータ使用にあたる職員を管理する立場にあった自治体自らの無登録に関する無謀が問題となった事例であるが、従業員が55条に違反して情報を取得等した場合に、使用者の立場にある者は刑事責任を負うのかということも問題となっている。例えば、ソリシタに命じられて情報収集等を行っていた私立探偵が55条に違反し、ソリシタがその情報を私立探偵経由で得た場合、ソリシタが私立探偵に対して55条に違反しないようにとの適切な助言をする等の予防措置を事前に採っていた場合は、当該ソリシタは情報やデータを「故意または無謀により」入手したとはいえないと解されている[17]。

これらは55条違反の犯罪において無謀の有無が問題となったものとして代表的な判例であるが、無謀の意義が直接言及されているのは（1）のアムネスティ事件である。アムネスティ事件では、深刻で有害な結果が発生するという予見があったか否かという観点から無謀の有無が争われたが、前述の通り、このような理解は MPC v Caldwell [1982] AC341 にも見られる。Caldwell 事件では、「財産が破壊または侵害されるか否かについて、行為者の無謀が肯定されるのは以下の場合である。（1）財産が破壊または侵害される明白な危険を創出する行為に出て、そして（2）そのような危険の可能性について何らの考慮をせずに行為に出た場合、またはそのような危険を認識しながらも行為に出た場合である」と判示された。ここでいう「危険」というのは正当化されない危険のことであり、自動車の通常の運転や、医師による手術等はそれに含まれない。正当化される危険か否かは、行為者の主観によって決まるのではな

[17] Evans, supra note13,at 4.

く、裁判所が当該行為の社会的有用性と、深刻な侵害結果の発生する可能性を比較衡量して判断するのである[18]。

Caldwell 事件判決における無謀概念は、危険のあることを認識せず行為に出た場合と、認識した上で行為に出た場合の両方をカヴァーしていたが、Caldwell 事件以降に出された R v G [2003] UKHL50によって、無謀の有無の基準が変更された。G 事件では、「行為者が、1971年刑事毀棄法（Criminal Damage Act 1971）１条所定の無謀によって行為に出たか否かは、以下の観点から判断される。（ｉ）存在し、または存在するであろう危険を行為者が認識しているという状況、（ii）発生するであろう結果の認識を行為者がしている場合の結果と、行為者が認識しているという状況下では、そのような危険を冒すのは不合理であるということ」と判示された。

この判断は、1971年刑事毀棄法の犯罪における無謀が問題となった事例に対するものであるが、行為者が危険を認識していたことと、危険を冒すことの不合理性によって無謀の有無を判断する手法は一般的に定着しているようである[19]。Caldwell 事件判決の基準では、危険に対する認識があった場合もなかった場合も両方含んでいたので、無謀と不注意（negligence）の区別が曖昧になるという問題があったが、G 事件判決により、両者の区別を危険性に対する認識の有無で明確に区別することが可能になったと解されている[20]。したがって、今後はデータ保護法55条違反の犯罪における「無謀」も、正当化されない危険性を認識した上で行為に出ることとして解釈されることになると思われる。

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

前節までは、1998年データ保護法55条の規定の意義について検討してきた。続いて、本節では55条の運用の在り方を含んだ情報コミッショナーの実務について扱うこととする。

---

[18] Russell Heaton and Claire de Than, Criminal Law, 66 (3d ed 2011).

[19] Heaton et al, supra note 18, at 73.

[20] Heaton et al, supra note 18, at 73.

1998年データ保護法は、女王から独立した第三者機関として情報コミッショナー（Information Commissioner）と審判所（The tribunal）を置いている。情報コミッショナーは個人情報保護に関して直接的な監督を行っており、51条（１）項では「データ管理者が善良な実務を守ることを促進し、特に、データ管理者が本法に基づく要件を遵守することを促進することに関し、本法に基づき自らの権能を行使する」ことが情報コミッショナーの義務であると規定されている。具体的な業務には、データ管理者からの通知事項を登録簿に記録する（18条・19条）、データ保護原則に違反したデータ管理者に対して執行通知を送る（40条）、違反者を訴追する（60条（１）項）といったものがある。そして、52条（１）項には「コミッショナーは、両議院に対して、本法における自らの権能の行使に関する年次報告書を提出しなければならない」と規定され、52条（２）項には「コミッショナーは両議院に対して、自らが適切であると判断した権能について、他の報告書を適宜提出することができる」と規定されている。このように、情報コミッショナーは個人情報保護の推進のための活動を行っており、議会に対して責任を負っている。情報コミッショナーは1998年データ保護法52条（２）項に基づいて、「プライヴァシーの価値とは何か？（What price privacy?）」という報告書を2006年５月10日に、そして「続・プライヴァシーの価値とは何か？（What price privacy now?）」という第２報告書を2006年12月13日に提出している。これら２つの報告書では、個人情報の適切な保護のために罰則を強化すべきであるという提言がなされており、この報告書を受けて法改正も行われている点で興味深い。そこで、本節第１・２項ではこの２つの報告書から、刑罰に対する情報コミッショナーの考え方と実務について詳述する。

続いて、2010年４月から、情報コミッショナーにはデータ保護原則の重大な違反に対し金銭的制裁を科す権限が与えられた。そこで、本節第３項では、情報コミッショナーによる金銭的制裁の実務について検討する。

第１項　報告書「プライヴァシーの価値とは何か？（What price privacy?）」

まず、この報告書では情報コミッショナーの Richard Thomas 氏によ

る序文があり、刑罰に関する問題意識が表れているので、少々長くなるが以下引用する。

「個人のプライヴァシーを保護することは、データ保護の法律における私の責任の中心的なものである。1998年データ保護法55条は、故意または無謀により、データを保有する機関（organization holding the data）の同意なく、秘密の個人データ（confidential personal data）を入手、開示、または開示を周旋することについて刑罰を設けている。今、わが職員（筆者注：情報コミッショナー事務局の職員であると思われる）と警察による調査の結果、そのような情報の不法な売買に向けられた産業が拡大していることが明らかになった。

個人情報は、それが有名人、政治家、その他の公的な人物に関する恥ずかしい秘密であろうと、またはいくらかの借金をしていると思われる私人の所在であろうと、価値のあるものである。これらの不正取引における全てのケースは、個人の私的な情報が含まれており、情報を保有する機関はその開示を認めていないという点で共通している。コンピュータに貯蔵されていることが多く、特定の個人として一人の人間を浮かび上がらせ得るジグソーパズルのピースのような情報がある。このような情報における取引は、個人のプライヴァシーに対する深刻な脅威となるので、これを本法の特別な権限に従って、議会に対して提出する最初のレポートとする。

現在、55条違反の犯罪には拘禁刑が設けられていない。秘密の個人情報の不正な周旋や売却に関するケースが裁判所に持ち込まれた場合、少額の罰金（derisory fine）か条件付き刑の免除（conditional discharge）にすぎない有罪判決が下されることが多い。軽い刑罰は世論におけるデータ保護に関する犯罪の重さを低く評価し、裁判のシステムにおいてさえ、犯罪の本当の重大性を隠蔽してしまう。同様に、刑罰が軽ければ、本来は私的なものにとどまっているべき秘密の情報を購入したり提供したりする行為を予防することは困難である。私が提案する解決策は、正式起訴による有罪判決を受けた者（persons convicted on indictment）に対して最大２年間の拘禁刑を、略式起訴による有罪判決（summary conviction）の場合は最大６か月の拘禁刑を導入することである。より多くの人々を刑務所に送ることが目的なのではなく、情報を購入する者

であろうと提供する者であろうと、このような不正な取引に関わろうとする全ての人々を思いとどまらせることが目的である。

個人は、第三者が個人の情報に対する不正アクセスに成功した時に被害を受ける唯一の存在ではない。企業にも、顧客の信用と公共部門における信頼を失うリスクがある。情報社会の基盤とシステムが安全でない限り、情報社会を適切に構築することはできない。改革型政府（Transformational Government）のスローガンの下、政府は公共サービスと連携したコンピュータ・システムのプログラムを作り出しているので、ギャップを埋めることはより切迫性を帯びる。しかし、政府の保有する情報へのアクセスが増加していることは、本来であれば法によってその入手を否定されている情報への手段を購入・詐取・交換することを欲する者に対して道を開くものではないことを確認する必要がある。

これらの問題と重罰化の必要性は、憲法事項省（Department for Constitutional Affairs）に挙げられた。私が今のところ受け取った前向きな回答は励みとなるものである」[21]。このように、深刻化する個人情報への侵害行為に対する抑止力として、刑罰が期待されている。そして、情報の売却や無断提供などの行為の重大性に比して、法定刑が軽すぎると解されており、拘禁刑を設けることによって罪刑の均衡を図ることが主張されている。

続いて、この報告書では、情報コミッショナー事務局への苦情受付の実態と罰金刑の実態調査の結果が「本法における苦情と訴追（Complaints and prosecutions under the Act）」において記されている[22]。これによると、1998年データ保護法が施行された2000年３月１日からの６年間で、情報コミッショナーに寄せられた苦情で55条に関するものは約1000件であり、自らのプライヴァシーが侵害されたと考える個人からの苦情が多

[21] What price privacy? http://www.ico.org.uk/for_the_public/topic_specific_guides/~/media/documents/library/Corporate/Research_and_reports/WHAT_PRICE_PRIVACY.pdf, 3.（2014年９月30日最終閲覧。本章で引用するイギリス1998年データ保護法に関する Web 上の他の資料についても同様）。

[22] What price privacy? supra note21, at 12-13.

い。情報コミッショナーは自らの訴追権限に基づいて、2002年11月中旬から2006年１月までの間、イングランドとウェールズの刑事裁判所と治安判事裁判所に対し、25件の訴追を行った。そのうち、22件が有罪、２件が訴えの取り下げ（withdrawal）、１件が裁判官の命令による中止（discontinuance on the orders of the judge）である。本報告書の別表A[23]に詳細が記載されており、22件の有罪のうち、１件は刑の絶対的免除（absolute discharge）、５件が条件付き刑の免除である。22件の有罪のうち９件は、１犯罪あたりの罰金額が50ポンドから150ポンドで、複数の犯罪が行われた事案（multiple-offence cases）において、2000ポンドから3000ポンドの罰金が科されたのは３件である。罰金の合計額が5000ポンドを超える事案は１件のみであった。別表Aに記載されている訴追事例には、データ保護法55条に違反して個人データを取得または開示するものが多い。

情報コミッショナーは苦情の受付と訴追のみならず、犯罪の実態調査[24]も行っている。例えば、情報コミッショナーは、秘密の個人情報が組織的に取引されていることを疑っていたので、デーヴォン＆コーンウォール警察管区（Devon & Cormwall Constabulaty）の召喚状（warrant）に基づき、組織的な法律違反・闇市場の証拠収集のため、サリー州（Surrey）の建物等の捜査を行い各種の証拠を確保した。その結果、違法な情報取引の実態が明らかとなった。報告書によると、情報を購入するのはメディア（特に新聞）、保険会社、債権者、夫婦・家族関係の紛争の関係者、詐欺の意図を有する者や、証人や陪審員の脅迫を目的とする者等である。秘密の個人情報を得る方法は２つに大別され、一つは職務を通して情報にアクセスできる者を買収することである。もう一つは、データ主体や公務員に成りすまして情報を得る「ブラッギング（blagging）」という方法である。私立探偵がブラッギングに関わっており、得られた情報は仲介者を経て最終購入者に渡される。このような個人情報の違法な売買における料金の一覧も報告書に掲載されている。この中で最も低額なのは選挙人名簿の住所情報で、１件につき17.5ポンド

[23] What price privacy? supra note 21,at 38-39.

[24] What price privacy? supra note 21,at 15-16,22,24.

である。最も高額なのは携帯電話の登録内容の750ポンドで、次に高額なのは犯罪情報の500ポンドである[25]。「センシティブ情報」に該当するか否かにかかわらず、機密性の高い情報の方がより高額で取引されていることがわかる。

このように、情報コミッショナーは個人情報の違法な取引による個人のプライヴァシーの侵害が発生しているという調査結果に基づいて、現行の55条には罰金刑しか設けられていないことを批判する[26]。報告書は、個人情報の不法取得等に対する刑罰が軽いことは犯罪の重大性を矮小化することにつながり、判決も低額の罰金刑に留まっていることを指摘し、犯罪の予防にためには拘禁刑を設けるべきであると主張する。報告書は、データ保護法60条（２）項を改正し、55条違反の罪の法定刑を引き上げ、最大２年間の拘禁刑もしくは罰金またはそれらの併科、略式起訴による有罪判決の場合は最大６か月の拘禁刑もしくは罰金、またはそれらの併科が違反者に対してなされるべきであると提案する。「最大２年」という法定刑は、秘密の情報を不法に開示する行為につき「本条の罪を犯した者には、正式起訴の有罪宣告により、２年を超えない拘禁刑または罰金、またはそれらの併科がなされる」と規定する ID カード法（ID Cards Act 2006）27条を参照したものである。

そして本報告書は、重罰化と共に、情報提供の流れに関わる全ての者が55条で有罪となり得ることも強調されるべきであると主張する[27]。それまで、私立探偵（private investigators）は、情報取得のために他人を使ったり、仕事を他の私立探偵に下請けさせたりすることによって、刑罰から距離を取ろうとしていたが、このようなアウトソーシングを行ったとしても正犯（principal）は処罰を免れないことが指摘されている。私立探偵が単独で情報収集を行うケースばかりではなく、私立探偵と何名かの仲介者が協力して情報取得が行われている実態に即した指摘である。

---

[25] What price privacy? supra note 21,at 24.

[26] What price privacy? supra note 21,at 27.

[27] What price privacy? supra note 21 ,at 29.

第２項　第２報告書「続・プライヴァシーの価値とは何か？（What prices privacy now?）」

情報コミッショナーは、前項で扱った報告書の半年後に第２報告書を提出した。第１報告書では個人情報の不正取引の実態が詳述されていたが、第２報告書でも、不正取引に対して、強力な抑止とより深い認識、そして組織によるコントロールが必要であると解されている。このような問題意識に基づくものとして、第２報告書では、2006年５月以降も個人情報の不正取引の事件が発生しており、情報コミッショナー事務所は２件の55条違反事件について訴追を行い、１件については警告（caution）を受け入れさせたことが述べられている[28]。

まず、第１のケースとして、1998年データ保護法55条に違反して金融機関から入手した情報につき、私立探偵業者に関わっていない個人が情報コミッショナー事務所の警告を受け入れたことが挙げられている。続いて、訴追が行われたケースのうちの１つは、私立探偵会社を経営するAnthony Gerald Clifford が、55条違反の罪について2006年11月３日に罪状を認めたというものである。Clifford は多くの個人情報を取得した上で、それを売却したり、情報開示を周旋したりしており、情報を取得するためにブラッギングの手法を用いていた。

もう１つのケースは、2006年11月14日、私立探偵であったAnderson夫妻が、不法に情報を取得・売却した罪について認めたというものである。妻は14個の罪について、夫は11個の罪について罪状を認めたところ、妻には合計で4200ポンドの罰金、夫には合計で3300ポンドの罰金が科された。Anderson夫妻はイギリス歳入税関庁（Her Majesty's Revenue and Customs）、イギリスの大手電気通信事業者であるブリティッシュ・テレコミュニケーションズ（British Telecommunications plc）の他、様々な銀行を含む多くの機関から、ブラッギングによって、電話番号や所得税の情報などの個人情報を取得した。個人情報が不正に取得される多く

---

[28] What price privacy now?
http://www.ico.org.uk/for_the_public/topic_specific_guides/~/media/documents/library/Corporate/Research_and_reports/what_price_privacy_now_report.ashx,6-8.

の事例において、「ブラッガー（blagger）」が金融機関等に潜り込み、当該機関等の職員を欺いて情報を開示させるということが行われている。

このように、情報コミッショナーは第１報告書の提出以降も、個人情報の不正取引の取締のために活動を続けており、第１報告書の刑罰に関する提案は行政府にも影響を及ぼした。2006年７月24日、憲法事項省（the Department fot Constitutional Affairs）は、熟慮に基づき、かつ故意による個人データの悪用（deliberate and wilful misuse of personal data）に対して刑罰を強化する政府協議（government's consultation）を開始した。この協議文書（consultation document）は、現行法の刑罰は個人データの不正取引を防止するために有効ではないという第１報告書の考え方に明確に言及しつつ、政府は1998年法60条を改正して、略式起訴による有罪判決では６月の拘禁刑を、正式起訴による有罪判決では２年の拘禁刑を導入することを提案した。個人情報の不正取引の防止のためには、55条に拘禁刑を導入する切迫した必要性があるという、第１報告書から一貫した情報コミッショナーの考え方が政府にも受け入れられているが、第２報告書の結論部分において、最も深刻なケース（the most serious cases）にのみ拘禁刑が用いられるべきであるとする情報コミッショナーの意見が記載されている[29]。

情報コミッショナーによる報告書によって法案提出がなされ、2008年刑事司法及び入国管理法（Criminal Justice and Immigration Act 2008）が2008年５月８日に成立した。この法律の77条は個人データの不法取得等に対する処罰を変更する権限（Power to alter penalty for unlawfully obtaining etc.personal data）について以下のように定めている。

77条（１）項　主務大臣（The Secretary of State）は、命令により、1998年データ保護法55条違反で有罪となる者に対し、次のような責任を負わせることができる。

（a）略式起訴による有罪判決の場合、所定期間（specified period）内の拘禁刑、もしくは法定上限額を超えない金額の罰金（a fine not exceeding the statutory maximum）、あるいはそれらを併科すること

（b）正式起訴による有罪の場合、所定期間内の拘禁刑、もしくは罰金、

[29] What price privacy now ? supra note 28 ,at 27.

あるいはそれらを併科すること

77条（２）項　第（１）項 (a)(b) が定める「所定期間」は命令によって定められるが、以下の期間を超えてはならない。

(a) 略式起訴による有罪判決の場合は、12か月（北アイルランドでは６か月）

(b) 正式起訴による有罪の場合は、２年

77条（４）項　本条に基づいて命令を発する前に、主務大臣は次の者に意見を求めなければならない。

(a) 情報コミッショナー

(b) 主務大臣が適切であると判断する報道機関、及び

(c) 主務大臣が適切であると判断するその他の者

このように、77条（２）項の法定刑の上限は情報コミッショナーによる提案に従ったものになっている。情報コミッショナーは刑罰の発動に対して積極的な姿勢を有しているが、最も深刻なケースにのみ拘禁刑が用いられるべきであると述べていることから、主務大臣の裁量を認めているのは刑罰の濫用を防ぐ趣旨によるものであると考えられる。

刑事司法及び入国管理法77条により、主務大臣にはデータ保護法違反の罪を犯した者に拘禁刑を科す命令を下す権限が付与されたものの、現在のところ命令は下されていない。政府は、個人データの悪用は既存の法律でカヴァーされており、特に調査権限規制法（Regulation of Investigatory Powers Act 2000）におけるコミュニケーションの不法な妨害（unlawful interception of communications）と、コンピュータ不正使用法（Computer Misuse Act 1990）におけるコンピュータへの無権限のアクセスの罪では最大２年間の拘禁刑が科され得ることを指摘[30]しつつ、データ保護法55条違反の罪に対して拘禁刑を導入することについて

[30] The Government Response to Shakespeare Review of Public Sector Information, June 2013.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/252172/Government_Response_to_Shakespeare_Review_of_Public_Sector_Information.pdf,25.

消極的な態度を採っている。

第３項　金銭的制裁について

前述の通り、2010年４月から、情報コミッショナーには、データ保護原則の重大な違反に対して金銭的制裁を科す権限が与えられた。その根拠条文は、データ保護法55A 条であり、主要な条文を列挙する。

55A 条（１）項　以下の条件を満たす場合、コミッショナーはデータ管理者に対し、金銭的制裁通知（monetary penalty notice）を行うことができる。

(a) データ管理者による、４条（４）項の重大な違反（serious contravention）があった場合

(b) 当該違反が、現実的な損害または危険を生じさせる可能性があり、そして

(c)（２）項または（３）項が適用される場合

（２）項　本条は、違反が熟慮に基づく（deliberate）場合に適用される。

（３）項　本条は、データ管理者が

(a) 以下のことを知っていた、または知るべきであった場合に適用される。

（ｉ）違反が発生する危険性があり、かつ

（ii）そのような違反が、現実的な損害または危険を生じさせる可能性があるが、

(b) 違反を予防するための合理的な手段（reasonable steps）が採られていない場合

（４）項　金銭的制裁通知は、データ管理者に対して、コミッショナーによって決定され、通知に明記された金額の制裁金をコミッショナーに支払うことを要求する通知である。

（５）項　コミッショナーによって決定される金額は、規定の金額（prescribed amount）を超えてはならない。

（６）項　制裁金は、通知で明記された期間内に、コミッショナーに支払われなければならない。

このように、金銭的制裁の対象となるのは、データ保護原則の違反が深刻なケースに限定されている。55A 条（５）項では金銭的制裁が「規

定の金額」を超えないことが定められているが、金銭的制裁と制裁の上限と通知に関する2010年データ保護規則（The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010）２条により、50万ポンドが制裁金の上限とされる。

「金銭的制裁」という用語は、データ保護法55A 条と2010年規則では単に“monetary penalty”と表記されているが、情報コミッショナーの2009年・2010年報告書には“civil monetary penalty”と表記されている[31]。そして、情報コミッショナーは司法手続を経ずに金銭的制裁を科し得る[32]ことから、金銭的制裁は刑罰としての罰金とは区別される民事的制裁である。

情報コミッショナーは金銭的制裁制度について解釈の指針（guidance）を発表する義務があり（55C 条（１）項）、2012年に指針が出されている（Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998）。指針において、金銭的制裁の対象となるデータ保護原則の「重大な違反」の例として、（１）適切な安全措置（暗号化されたファイルやデバイスの使用、作業手順（operational procedures）、指針など）の欠如により、個人データが入力されているディスクが失われた場合、（２）データ管理者が安全措置に違反したことにより、センシティブデータを含む医療の記録が失われた場合が挙げられている[33]。

続いて、データ保護原則の「熟慮に基づく違反」の例として、会社が個人データを本人の同意なく競争目的で収集し、そして商業目的でデー

---

[31] Information Commissioner's Office Annual Report 2009/10 http://www.ico.org.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2010.pdf,36.

[32] 消費者庁「諸外国等における個人情報保護制度の監督機関に関する検討委員会・報告書」におけるイギリスの章（加藤隆之）の説明による。http://www.caa.go.jp/planning/kojin/h22report1.pdf.28.

[33] Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998 http://ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ico_guidance_on_monetary_penalties.pdf,13.

タベースを作成するために、利害のある個人に通知することなく、それを知りながらデータを開示する行為が挙げられている[34]。

違反に対して初めて金銭的制裁が科された2010年11月22日から2014年４月１日まで、金銭的制裁が科された事例は56件であり、2010年は２件、2011年は７件、2012年は25件、2013年は18件、2014年は４件である[35]。情報コミッショナーの2012年・2013年の報告書では、金銭的制裁の対象となるのはセンシティブデータを扱う健康関係の部門と地方行政団体が多いことが指摘されている[36]。

金銭的制裁の上限は50万ポンドとされているが、実際には５万ポンドから15万ポンド前後のケースが多い。しかし、特に重大なケースでは25万ポンド以上の金銭的制裁を科される場合もある。以下では高額な金銭的制裁を科されたケースについて概観する。

2014年４月１日までの段階で、最も高額な制裁金を科されたのは、2012年５月28日の Brighton and Sussex University Hospitals NHS (National Health Service) Foundation Trust（国立健康サービストラスト）におけるセンシティブ情報漏洩の事例[37]である。

事案の概要は次の通りである。トラストの IT サービスプロバイダーである Sussex Health Informatics Service (HIS) は、業務を会社 A に下請けさせていた。2010年４月、トラストが管理する病院のひとつである Brighton General Hospital に約1000のハードディスクが保管されるが、会社 A ではなく別の会社 B の個人 C が破棄業務を担当することとなった。C は本来であれば業務終了時に、ディスクの「破棄証明書」を提出

---

[34] http://ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ico_guidance_on_monetary_penalties.pdf,16.

[35] ICO のホームページ内に “Monetary penalty notices” というページがあり、金銭的制裁が科されたケースの一覧である “Civil monetary penalties issued” が閲覧可能である。http://ico.org.uk/enforcement/fines.

[36] http://ico.org.uk/about_us/performance/~/media/documents/library/Corporate/Research_and_reports/ico-annual-report-201213.ashx,32.

[37] http://ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Notices/bsuh_monetary_penalty_notice.ashx.

すべきであったところ、これが提出されていなかった。

2010年12月、データ復元会社（data recovery company）は４つのハードディスクをインターネットオークションにおいて、Cから当該ディスクを購入した売人から購入した。データ復元会社は、ディスクに入力されているデータがトラストに所属するデータであることに気づき、それらのディスクを直ちに解析に回した。当該ディスクには患者の健康状態や治療に関する情報、身体障害に関する情報が含まれており、その中にはHIVや泌尿生殖器疾患の患者の情報もあった。そして、患者のみならずスタッフの国民保険番号、自宅住所、病院のID、刑事事件の有罪判決、疑いをかけられた犯罪についての情報等の、高度にセンシティブな情報も含まれていた。そして、警察の捜査の結果、Cが少なくとも232のハードディスクをネットオークションで売却したことが判明した。

データ保護法１条（１）項所定のデータ管理者であるトラストは、破棄されるはずであったディスクをCがどのように持ち出したのかということを認識していなかった。しかし、Cが休憩のために病院を離れたことと、病院は外部からアクセス可能であったことを認識していたのみならず、ハードディスクの移動と破棄に関する記録が存在しなかったにもかかわらず、Cがディスクの大多数を破棄したと信じていた。

情報コミッショナーは、データ管理者につき「個人データの無権限または不法による取り扱いと、個人データの偶発的な損失、破壊、個人データに対する損害が発生しないように、適切な技術的・組織的措置が採られるべきである」とするデータ保護第７原則の重大な違反があるとして、トラストに対して32万5000ポンドの金銭的制裁を科した。

この事例は、HISが下請けのCにデータの取り扱いをさせた結果、Cがデータの入力されたディスクを適切に破棄せず、ディスクを売却したことにより被害が拡大したというものである。情報コミッショナーは、データ管理者であるトラストの責任について次のように判断している。まず、データ管理者はHISが下請け業者にデータの取り扱いをさせる可能性を考慮すべきであり、その可能性に基づき、個人データを取り扱うCが信頼に足りる人物であるか否かを確認することが可能であったにもかかわらず、確認をしなかった。次に、ハードディスクの破棄について、Cが安全措置の観点から十分な保証をしているか否かを確認する

ことが可能であったにもかかわらず、確認しなかった。結果的に、データ管理者はHISがCにハードディスクの破棄を下請けさせていたことを認識していなかったことから、ハードディスクの偶発的な喪失とデータの性質に由来する損害が発生し得ることに対する適切な安全措置を確実なものにすることができなかったと指摘されている。データ管理者のHISに対する監督が不十分であったことと、Cがディスクを適切に破棄したと軽信したことが、金銭的制裁を科される根拠となったものと考えられる。

また、より新しい事例としては、ソニーのゲーム部門（Sony Computer Entertainment Europe (SCEE)）がデータ保護法の重大な違反を犯したとして、情報コミッショナーがSCEEに25万ポンドの金銭的制裁を科した、2013年１月14日のケースが挙げられる[38]。事案の概要は次の通りである。2011年４月にソニーのPlay Station Networkがハッキングされたことにより、数百万人の顧客の氏名、住所、メールアドレス、生年月日、パスワードを含む情報が漏洩した。

情報コミッショナー事務局の調査によれば、ソフトウェアが最新の状態に保たれていればハッキングを防ぐことが可能であり、パスワードの保護も不十分であった。このことから、「個人データの無権限または不法な取り扱いと、個人データの偶発的な損失、破壊、個人データに対する損害が発生しないように、適切な技術的・組織的措置が採られるべきである」とするデータ保護第７原則の重大な違反があると判断され、金銭的制裁の対象となった。

制裁金制度が導入されてから日が浅いものの、重大な違反に対してのみ制裁金を科すという55A条の規定に従いつつ、特に悪質なものについては高額な金銭的制裁を科すという方針は一貫しているようである。イギリスのデータ保護法には、センシティブデータの不法取得等を一般的な個人データと区別して処罰する特段の規定は設けられていないが、前述の通り、金銭的制裁を科される事例の多くはセンシティブデータの不法な取り扱いが問題となったケースであることが、結果的に、センシ

[38] http://ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Notices/sony_monetary_penalty_notice.ashx.

ティブデータ独自の刑罰規定の代替措置となっている側面もあるだろう。

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１項　センシティブな個人データに含まれるデータについて

1998年データ保護法には、センシティブな個人データという、日本の法律には規定されていない概念がある。日本では「センシティブ情報」と呼ばれることも多い。データ保護法２条によると、次のデータが「センシティブな個人データ」となる。

(a) データ主体の人種的または民族的出自（the racial or ethnic origin）
(b) データ主体の政治的思想（political opinions）
(c) 宗教的信条または類似の性質を持つ他の信条（religious beliefs or other beliefs of a similar nature）
(d) 労働組合のメンバーであるか否か（1992年労働組合及び労働関係法における意味の範囲内で）
(e) 身体的または精神的な健康もしくは状態（physical or mental health or condition）
(f) 性生活
(g) 犯罪をしたこと、または犯罪をしたと申し立てられていること、または
(h) データ主体が犯した犯罪、もしくは犯したと申し立てられている犯罪に対する訴訟手続、そのような訴訟手続による処分、もしくはそのような訴訟手続において裁判所が下した刑の宣告

データ保護法２条は、上記のデータのみをセンシティブな個人データとして規定している。したがって、金融情報や年齢に関する情報はセンシティブな個人データには該当しない[39]。センシティブ情報に該当するか否かは、データ主体がそれを他者の知るところとなるのを望まないと

[39] Richard Morgan and Ruth Boardman, Data Protection Strategy : implementing data protection compliance,9 (2d ed 2012).

いう主観によってではなく、当該データが上記に該当するか否かという客観的な観点から判断される。

２条 (a) の「人種的または民族的出自」について、国籍に関する情報はセンシティブな個人データに該当するか否かということが問題となる。ある個人がアメリカ国籍を有している場合には、外国からの移民である可能性もあるので当該個人の民族的な背景が特定される可能性は高くないが、ニジェール（ナイジェリア）国籍の場合には当該個人の人種的または民族的出自が特定されやすいことから、国籍がセンシティブな個人データに該当するか否かを明確に判断するのは困難であるとする指摘[40]がある。また、名前がそれ自体でセンシティブな個人データに該当するか否か、苗字のデータを取り扱うことによって、データ主体の人種的または民族的な出自に関するデータを集めることになるか否かということも問題となっている。苗字のデータの取り扱いが、単に顧客の一般的なデータベースなどの氏名リストを作成するようなものだったのか、それとも苗字から判明し得る人種や民族的出自の内容と関係のあるものだったのかによって異なるとされている[41]。

２条 (b) 所定の「政治的思想」について、National Anti-Vivisection Society v Ingland Revenue Commissioners [1974] UKHL4では、団体の主たる目的が、法律改正によって動物実験を全面的に禁止することである場合、その団体は政治的なものであり、慈善事業にとどまるものではないとされた。

２条 (c) の「宗教的信条または類似の性質を持つ他の信条」について、「類似の性質を持つ他の信条」には、ヒューマニズム (humanism)、または個人のあらゆる人生観 (any system of belief by which an individual orders his or her life) を包含し得る[42]。2010年平等法 (The Equality Act 2010) 10条２項によると、「信条」はあらゆる宗教的または哲学的信条を意味しており、信条への言及は、何も信条を持っていないことに言及することも含む (Belief means any religious or philosophical belief and a

[40] Morgan et al, supra note 39, at 130.

[41] Carey, supra note 5, at 83.

[42] Jay, supra note 12, at 209.

reference to belief includes a reference to a lack of belief）ことから、当該個人が無宗教であることも２条（c）所定の情報であると解される。

前述の通り、金融情報や年齢といった、本人が他人に知られるのを好ましくないと考えるような性質のデータであっても、データ保護法２条で列挙されているデータに客観的に合致するものでなければセンシティブデータには該当しない。センシティブな個人データが一般的な個人データよりも厳格な条件の下で取り扱われることから、センシティブな個人データの範囲が拡張されることによるデータ処理への萎縮効果を防ぐ趣旨なのではないかと思われる。

第２項　データの取り扱いの条件

センシティブな個人データの取り扱いについては、データ保護法の附則３で以下のように規定されており、データを取り扱うには、以下の10個の「センシティブな個人データ取り扱いに関する条件」の中の少なくとも１つを満たさなければならない。

１条　データ主体の明示的な同意（explicit consent）のある場合

２条（１）項　データの取り扱いが、雇用に関するもので、データ管理者に付与された権利の行使または課せられた義務の履行のために必要な場合

（２）項　主務大臣の命令によって

(a)（１）項の適用を排除する特定の場合、または

(b) 命令の中で明記された更なる条件が満たされない限り、（１）項の条件が満たされたとはみなされないことを規定している場合

３条 (a)（ｉ）データ主体またはその代理人の同意を得ることができないか、（ii）データ主体の同意を得ることができないとデータ管理者が考える合理的な理由があるが、データ主体または他の者の重要な利益（vital interests）を保護するためにデータの取り扱いが必要な場合、または

(b) データ主体またはその代理人の同意が不当に留保されている状況

下で、他人の重大な利益を保護するためにデータの取り扱いが必要な場合

4条(a)情報の取り扱いが、非営利で政治・哲学・宗教・労働組合の目的によって設立された団体の適法な活動の中で実施され、
(b)データ主体の権利や自由を適切に保護するために取り扱われ、
(c)団体のメンバーである個人か、団体の目的との関係で定期的に連絡を取る個人のいずれかの者のみに関係するものであり、
(d)データ主体の同意なく第三者に個人データを開示することを含まない場合

5条　データ主体の慎重な措置の結果として公知された個人データに含まれる情報である場合

6条(a)データの取り扱いが、法的手続の目的で、または法的手続に関して必要な場合、
(b)法的なアドバイスを得るために必要、または
(c)法的権利を確立、行使、または防御するために必要である場合

7条(1)項　データの取り扱いが、
(a)司法の運営のために必要
(aa)貴族院か庶民院のいずれかの権能の行使のために必要
(b)制定法によって人に与えられる権能の行使のために必要、または
(c)国王、大臣または省の権能の行使のために必要である場合

(2)項　主務大臣が命令によって、
(a)(1)項の適用を排除する特定の場合、または
(b)命令の中で明記された更なる条件も満たされない限り、(1)項の条件が満たされたとはみなされないことを規定している場合

7A条(1)項
(a)(i)詐欺防止機関(anti-fraud organisation)の構成員である個人

による、もしくは、そのような機関によってなされた取り決め（arrangements）に基づくセンシティブデータが開示された場合、または

（ⅱ）その個人（筆者注：詐欺防止機関に属する個人）または他の個人によってそのように開示（筆者注：（ⅰ）所定の開示）されたセンシティブデータが、開示以外のあらゆる方法によって取り扱われた場合、かつ

（b）データの取り扱いが詐欺または特殊な種類の詐欺の予防目的のために必要な場合

（２）項　本条において「詐欺防止機関」は、次のものを意味する。

詐欺または特殊な種類の詐欺を防止するための情報共有を行う、もしくは情報共有を容易にする法人格のない団体、法人、あるいはその他の個人

または、団体や個人の複数の目的もしくはそれらの目的の中の一つとして、詐欺防止の機能のあらゆるものを有している団体や個人

８条（１）項　情報の取り扱いが医療目的のために必要であり、

（a）健康に関する専門職が、または

（b）それと同等の守秘義務を負う者が引き受けた場合

（２）項　この項において、「医療目的」は、予防医療、医学診断、医学研究、ケアの提供と治療、ヘルスケアサービスの運営の目的を含む

９条（１）項　情報の取り扱いが

（a）人種的または民族的出自に関する情報を含むセンシティブな個人データに関するもので、

（b）異なる人種的または民族的出自を持つ人々の間における機会または待遇の均等を促進または維持する目的のために必要であり、そして

（c）データ主体の権利と自由に対する適切な保護のために行われる場合

（２）項　主務大臣は命令によって、（１）項（a）と（b）の範囲内で行われているデータの取り扱いが、（１）項（c）の目的において、データ主体の権利と自由のための適切な安全措置に基づいて扱われているか否かという状況について詳述することができる

10条　このパラグラフ（附則３）の目的のために主務大臣によって下された命令で明記された状況下で、個人データが扱われる場合

以上が、センシティブな個人データを取り扱うための条件である。一般的なデータの取り扱いに関する附則２よりも条件が具体的で厳格である。そして、センシティブな個人データを取り扱うには附則２の条件と附則３の条件の両方を満たすことが要求される[43]。ここからは、附則３に挙げられた条件のうち、附則２との相違が顕著である主要な条件について検討する。

まず、附則３の１条ではデータ主体の「明示的な同意」の必要性が明記されている。一般的なデータの取り扱いのための条件を規定する附則２では、「データ主体がデータの取り扱いについて同意している」ことが条件の１つとして挙げられており、明示的でなくても同意があればよいとされているのに対して、データの重要性に鑑みて明確な同意が必要であるとされている。

附則３の１条は、書面による同意でなければ無効であるとするものではないので、明確であれば口頭での同意も認められる。しかし、「明示的な」という言葉は「明らかで不明瞭なところがない（clear and unambiguous）」という意味で解釈される傾向にあるので、同意が不明確であるという批判を回避するために、データ管理者は書面によって同意の存在を示すことが多い[44]。

情報コミッショナーによって2001年10月に出されたLegal Guidanceは、「明示的な」という文言から、「データ主体の同意が絶対的に明白（absolutely clear）なものでなければならないことが示唆される。適切なケースにおいて、同意はデータの取り扱いについての具体的な項目（specific detail of the processing）、扱われるデータの特定の種類（the particular type of the to be processed）、取り扱いの目的（the purposes of the processing）、個人に影響を与えるデータの取り扱いの特別な状況のあらゆること（any special aspects of the processing which may

[43] Carey, supra note 5, at 84.

[44] Jay, supra note 12, at 212.

affect the individual）をカヴァーするべきである」[45]と述べている。このことから、情報コミッショナーも書面による同意を絶対的に要求してはいないが、データ主体が自らのデータを処理されることにつき、その種類や目的といった詳細について認識した上で、一切の曖昧なところのない明白な同意をしていることを要求していると言える。

続いて、附則３の３条（a）では「データ主体または他の者の重大な利益の保護」について規定されている。情報コミッショナーによると、「重大な利益」は生死に関わる状況（life and death situations）であると解釈されている[46]。一般的な個人データの取り扱いの条件を定める附則２の４条にも、「データ主体の重大な利益の保護のためにデータの取り扱いが必要であること」という類似の規定がある。しかし、附則３の３条は附則２の４条とは異なり「データ主体以外の者」という文言が加えられていることから、共同体の利益に資するという性質も有している[47]。例えば、データ主体が伝染病に罹患しており、他の者にも伝染する危険がある場合、データ主体の健康状態に関するデータを用いることは附則３の３条によって正当化され得る。データ主体が意識不明または所在が不明の場合、データ主体がデータの取り扱いについて同意をすることはできないので、本条によって関連するデータを開示することが可能になる。データ主体が単に開示を拒否している場合にも、健康に関する権限を持つデータ管理者も、附則３の３条に基づいてデータ開示をすることができる[48]。附則３の３条が、医療目的のためのデータの取り扱いについて規定する附則３の８条といかなる関係にあるのかということについては明らかではないが、後述の附則３の８条はデータの取り扱いが健康に関する専門職によって行われることを要求している一方で、３条はそのような限定をしていないという相違が見られる[49]。

---

[45] http://ico.org.uk/~/media/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf,30.

[46] Morgan et al, supra note 39,at 133.

[47] Carey, supra note 5,at 86.

[48] Carey, supra note 5,at 86.

[49] Carey, supra note 5,at 86.

続いて、附則３の７条は司法運営等のための取り扱いについて規定している。附則２の５条の規定と類似しているが、附則２の５条（d）が定める「公共の利益のために運営され、公的な性質を有する機能の行使（for the exercise of any other functions of a public nature exercised in the public interest by any person）」という項目が附則３には存在しない。このような規定が欠けていることで、公共の利益を追求する慈善団体やその他の機関は、附則３の７条の下でセンシティブな個人データの取り扱いを正当化されない[50]。このように、附則３の７条の下でセンシティブな個人データを扱う目的が司法の運営、議会の運営といった、範囲が比較的明確なものに限定することにより、データの扱いによってデータ主体の利益が損なわれる危険性を低減しようとしているものと思われる。

附則３の８条は、医療の目的によるデータの取り扱いに関する条文である。本条にいう「医療目的」の例が８条（２）項に列挙されているが、医療に関するその他の目的も含まれる[51]。データを取り扱う主体である「健康に関する専門職」には、医師、歯科医師、看護師、薬剤師等の幅広い職業の者が該当する。

附則３の９条は、人種的または民族的出自に関するセンシティブな個人データについての規定である。本条は、異なる人種的または民族的出自を有する者同士の機会と待遇の均等を促進・維持するためにデータが取り扱われることに限定しているが、データが他の目的よりも、そのような機会と待遇の均等のために用いられていることをデータ管理者はどのように明らかにするのかという問題がある。本条の違反を回避するためには、そのような目的で人種的または民族的出自に関するデータが取り扱われているか否かを、データ管理者が注意深く吟味することが求められる[52]。

附則３の10条は、主務大臣の発布した命令によってデータが取り扱われる場合についての規定である。本条を根拠として発布された命令として、センシティブな個人データの取り扱いに関する2000年データ保護命

[50] Morgan et al, supra note 39,at 135.

[51] Carey, supra note 5,at 88.

[52] Jay, supra note12, at 228.

令（Data Protection (Protecting of Sensitive Personal Data) Order 2000 SI 2000/417）がある。2000年データ保護命令は10条から成り、センシティブデータの取り扱いのための条件を規定している。この命令で規定されている条件には、データの取り扱いが犯罪を予防したり見つけたりするのに必要である場合、一定の政治的機関による政治的意見についての情報を取り扱う場合、データの取り扱いがデータ主体に影響がなく、調査のために必要な場合等がある。2000年データ保護命令に規定されている条件のいずれかを満たしていれば、1998年データ保護法における附則３の10条を遵守したということになり、センシティブデータの取り扱いが正当化される。

第５節　小括

本章では、イギリス1998年データ保護法における個人データの不法取得等の犯罪の意義と、情報保護のための第三者機関である情報コミッショナーの刑罰に対する考え方、実際の実務と、センシティブな個人データの意義とその取り扱いのための条件について検討してきた。

まず、データ保護法55条は個人データを不正に取り扱う行為を広く処罰している。55条のように違反者を直接処罰する規定を設けるに至った背景には、第２節の第１項で挙げたような個人データ関係の事件があり、それが社会問題に発展したことがある。特に、ブラッギングの手法を用いたり、数名の仲介者や私立探偵を使ったりすることで情報を不正に入手することも多く、情報の不正取引は悪質化・組織化している。犯罪は故意犯処罰が原則であるが、イギリス社会のこのような実態に鑑みると、処罰のための主観的要件を故意のみならず無謀にまで拡大することは一つの規制方法として考えられる。一方、日本でも情報漏洩の事件が多発しており、過失によって情報が漏洩するケース[53]のみならず、何らかの

[53] 例えば、学校教員が、生徒の成績等の個人情報の入力されたUSBメモリー等を紛失する事例が数多く発生しており、紛失したUSBメモリー等が他人に入手された場合、過失によって情報が漏洩したことになる。

原因によって漏洩した情報が転売されるケース[54]も発生している。情報が転売される等、情報侵害が故意に行われた場合はもちろんのこと、過失であっても大量の情報が漏洩した場合には被害は甚大であるので、過失による情報漏洩等を処罰対象とすべきであるか否かは検討の余地がある。

イギリス刑法における「無謀」は日本刑法における「過失」と同義であるとは必ずしも言えないものの、刑法の原則から見れば、過失犯の処罰を可能にするのは生命や身体等の重大な法益の侵害があった場合に限られるので、日本法において認識ある過失または認識のない単純な不注意による過失で情報漏洩が発生した場合に刑罰を発動させるためには、更なる根拠が必要となる。

次に、イギリス1998年データ保護法では、女王・政府から独立した第三者機関である情報コミッショナーがデータ保護のための監督を行っている。情報コミッショナーは、犯罪の捜査や訴追、法改正についての提言も行っており、その権限は広い。2010年４月からは、データ保護原則の重大な違反に対して金銭的制裁を科す権限も付与された。情報の不正取得や違反以外の一般的な刑事事件を訴追する検察官ではなく、情報についての専門機関である情報コミッショナーが捜査や訴追を行うという制度には、情報侵害の実態に即した訴追や処罰（あるいは訴追や処罰を行わないこと）が可能になるという意義がある。また、民事的制裁ではあるものの、金銭的制裁制度も違反に対する抑止力となっていると考えられる。

そして、このような権限を与えられているのみならず、毎年報告書を提出することを義務付けられることで、情報コミッショナーが実務を適切に行っているか否かがチェックされている。イギリスの情報コミッショナーのような専門の第三者機関を設けて一定程度の権限を付与する法制度が日本にも必要か否かは、情報の保護に関する既存の機関の実務

[54] 大規模なものとしては、株式会社ベネッセコーポレーションから760万件（流出した個人情報は最大でおよそ2070万件に上る可能性があるとみられている）の顧客情報が漏洩し、複数の名簿業者の間で転売が繰り返された後、IT 事業者の「ジャストシステム」に渡り、顧客にダイレクトメールが発送されたことによって漏洩が発覚したという事例がある（2014年７月）。

の現状に鑑みて検討する必要があるが、イギリスの情報コミッショナーの制度には一定の意義がある。また、情報コミッショナーの報告書にも記載されていたように、情報コミッショナーは個人データの保護のための厳罰化に対して積極的な姿勢を採っている。イギリスでは個人データの不正取扱に対して刑罰を発動することについて、日本ほどの抵抗感がないように思われるが、イギリスで発生している個人データの不正取扱の事件が立法事実となり、刑罰を用いることに対して説得力を持たせているのであろう。そして、専門機関である情報コミッショナーが、現状分析や調査を行った上で厳罰化の提言をしていることが、刑罰への更なる後押しとなっている。

続いて、イギリス1998年データ保護法では、センシティブな個人データが一般的な個人データと区別されている。センシティブな個人データは、健康状態、思想的信条、人種的または民族的出自といった、それが侵害されたり不当に取り扱われたりした際にプライヴァシーの侵害の程度が大きいとされるデータであり、データ保護法附則３所定の条件は、附則２に規定されている一般的な個人データの取り扱いの条件よりも多く、厳格である。

イギリス1998年データ保護法では、データの重要性によって一般的な個人データとセンシティブな個人データを区別しているものの、センシティブな個人データを不正に取り扱う行為をそれ以外の個人データの場合に比べて重く処罰する旨の規定は存在しない。また、センシティブな個人データを取り扱うにあたり、データ管理者は附則３と附則２の条件のうち１つ以上を満たす義務があり、その義務に違反した場合にはデータ保護原則１条違反となるので、情報コミッショナーからの是正通知を受けることになる。是正通知についても、センシティブな個人データについて違反があった場合には一般的な個人データの違反の場合に比して厳しい通知を行うといった区別はデータ保護法上ではなされていない。イギリス1998年データ保護法が、センシティブな個人データという概念を設け、一般的な個人データより厳格に保護されるべきものとして位置づけている一方で、刑罰の加重や、データ管理者の違反に対する通知の種類等に差異が設けられていない理由は定かではないが、違反や情報の不正取得が行われた後の制裁よりも、センシティブな個人データが不当

に扱われることに対する事前の予防に重点を置くのがデータ保護法の趣旨ではないかと思われる。

前述の通り、センシティブな個人データを取り扱う際には附則３の条件と附則２の条件をそれぞれ１つ以上満たすことが要求される。データ主体の明示的な同意があれば、附則３の１条と附則２の１条の要件を両方満たすことが可能になるが、データ主体が同意していない、または拒否している場合はデータの取り扱いが困難になる。例えば、附則３の７条に規定されている司法運営のためにデータを取り扱う場合には、附則３の７条と附則２の５条の内容が重なり合うので、附則３の条件を満たす場合には同時に附則２の条件も満たすことが可能になろう。しかし、センシティブな個人データを取り扱おうとする理由や目的がより抽象的になればなるほど、両方の条件を満たすことは困難となり、安易なデータの取り扱いに対する抑止力が働く。このように、センシティブな個人データについては、データ管理者の負担を重くすることで不正な取り扱いや違反の予防を図っているのではないかと考えられる。

確かに、データ取り扱いのための条件を厳格化することは、違反を抑止するのに一定の効果があるだろう。しかし、情報コミッショナーの第１報告書には個人データの不正取引を抑止し、個人のデータに対する有効な保護を行うためにはデータ保護法55条違反の罪の法定刑を引き上げ、拘禁刑を設けるべきであると記載されていた一方で、センシティブな個人データについては特段の言及がなかったことには疑問がある。予防のために厳罰化をすべきであるというのであれば、侵害や違反があった場合により重大なプライヴァシー侵害につながるセンシティブな個人データの不正取得の罪の法定刑を一般的な個人データの場合に比して重くするという発想にならないのはなぜだろうか。個人情報の不正取得等を直接的に処罰する規定の在り方を検討する際には、客体がセンシティブな個人データである場合と、それ以外の一般的な個人データである場合とで法定刑の差を設けるべきか否かが問題となるだろう。

［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。