Ⅱ．主要各国における個人情報保護法制と第三者機関の実態

ⅰ　イギリス

１．個人情報保護法制について

（１）個人情報保護制の概要

①法律名

イギリスの個人情報保護法は、1998年データ保護法(Data Protection Act 1998)である[1]。イギリスには、1984 年データ保護法(Data Protection Act 1984)があったが、1995 年の EU データ保護指令(EU Directive on Data Protection)[2]に従い、1998 年データ保護法（以下、イギリスについては、「1984 年データ保護法」又は「1984 年法」、「1998 年データ保護法」又は「1998 年法」というように表記することにする。）が制定された。女王の裁可を得たのは、1998 年 7 月 16 日である。施行は、2000 年 3 月 1 日であった。

伝統的にはコモン・ローを発展させたイギリスにおいて、アメリカの方式とは異なる体系的なデータ保護法が制定されていることに注目する必要がある。

②目的

日本の個人情報保護法は 1 条に目的を掲げているが、イギリスの 1998 年法にはそれに相当する規定はない。その長称が「個人データの取得、保有、利用又は提供を含む、個人に関する情報の取扱いの規制のために新たな規定を設けるための法律」(An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information)となっており、これが目的であるともいえる。

③適用範囲

ア)個人データ

1984 年法は、自動処理データのみに適用されていたが、1998 年法は、それ以外に「関連するファイリングシステムの一部として記録される情報」(relevant filing system)をも対象としている(１条)。法律上は、「個人データ」という概念を使っているが、情報コミッショナー事務局(Information Commissioner's Office, ICO)の文書は「個人情報」(personal information)を使っている場合がかなり見かけられる。これらについては後述参照。

イ)公的部門と民間部門

1998 年法は国の行政機関、地方公共団体などの公的部門と民間部門の双方に適用される(1984 年法も同様であった)。

④規制・権利の内容

個人情報の取扱いの全般を規制し、また、データ主体の権利を広く認めている。その一端については、1998 年法の全体像を見ることである程度知ることができる。

ア)1998 年データ保護法の構成

1998 年法は、次のような各章及び各節(日本の法律の形式でいえば「節」に当たるものをこのように呼ぶことにする)並びに附則からなっている。

第Ⅰ章　序則(1 条―6 条)
第Ⅱ章　データ主体の権利その他(7 条―15 条)
第Ⅲ章　データ管理者による通知(16 条―26 条)
第Ⅳ章　適用除外(27 条―39 条)
第Ⅴ章　執行(40 条―50 条)
第Ⅵ章　雑則及び総則(51 条―75 条)
　　コミッショナーの権能(51 条―54 条)
　　個人データの不法な取得等(55 条)
　　データ主体のアクセス権に基づき取得された記録(56 条・57 条)
　　コミッショナー又は審判所に提供される情報(58 条・59 条)
　　違反に関する総則的規定(60 条・61 条)
　　1974 年消費者信用法の改正(62 条)
　　総則(63 条―75 条)
　　附則 1―16

イ)データ保護原則

附則 1 に規定されているデータ保護原則(Data Protection Principles)の要約は、ICO によると、次のようになっている。日本の法律と異なり、附則に重要な事項が規定されていることに注意する必要がある(本稿では、Schedule を「附則」と訳しているが、日本の法律の附則とは異なることに注意されたい。イギリスの制定法の特徴である)。

第 1 原則　公正かつ適法な取扱い(Fairly and lawfully processed)
第 2 原則　限定された目的のための取扱い(Processed for limited purposes)

第３原則　目的適合性(Adequate, relevant and not excessive)
第４原則　正確性・最新性(Accurate and up to date)
第５原則　必要期間限定性(Not kept for longer than is necessary)
第６原則　データ主体の権利適合的取扱い(Processed in line with your rights)
第７原則　安全性確保(Secure)
第８原則　十分な保護のない第三国への移転制限
(Not transferred to other countries without adequate protection)

⑤監督・登録制度

公的部門と民間部門の双方を監督する情報コミッショナーが設けられている。また、1984年法で設けられた登録制度は、1998年法では、登録(registration)ではなく、通知(notification)という概念で存在している。1998年法は、コミッショナーによる諾否の返答を要しないこと及び登録抹消通知の存在しないことが、1984年法とは異なっている。

通知については、次のような制度となっている。データ管理者は、個人データを取り扱うに当たって、通知事項(氏名、住所、代表者、個人データのカテゴリ、取扱目的、データの提供先、情報を欧州経済地域外へ移転させる場合の国名)、及び、第７データ保護原則(情報の安全保護)遵守のための措置を、情報コミッショナーに通知しなければならず、情報コミッショナーは、通知を行った者の登録簿を保持しなければならない。データ管理者は、情報コミッショナーの登録簿に記載されなければ、個人データを取り扱ってはならない。

通知件数は、2003年頃までの間は、おおよそ約20万件前後で推移していたが、2003年から2004年にかけて、25万件を突破した。2007/2008年次報告書では、30万4000件を超えた旨が明らかにされており、そのうち、3万7776件が新規通知、26万5766件は更新又は維持された数である[3]。

⑥主な適用除外

様々な場面で適用除外が設けられている。詳しくは、後述参照。

⑦主な自主規制

いくつかの分野で実務規範(code of practice)が策定されている。例えば、個人情報の共有に対する実務規範の枠組み(Framework code of practice for sharing personal information)[4]、監視カメラ実務規範(CCTV code of practice)[5]、雇用実務規範(Employment Practices Code)[6]がある。また、プライバシー通知実務規範(Privacy Notices Code of Practice)が策定途中である(2009年２月21日現在)。

⑧その他

イギリスのデータ保護法には日本の個人情報保護法と異なる特徴がいくつかある。例えば、個人データの取扱いについて、通知に基づく登録制をとっていて、通知を義務付けられているデータ管理者が無登録で個人データを取り扱うことは､データ保護法違反となる。また、公的部門と民間部門の双方について監視する独立の機関として情報コミッショナーが女王によって任命されている。

（２）個別の検討課題

①いわゆる「過剰反応」(誤解)に対応した第三者提供制限の例外事由

[現状について]

イギリスを含め「過剰反応」という概念は理解され難いと考えられているが、データ保護法が「誤解」された事例として、ソーハム殺人事件(Soham Murder)[7]及びブリティッシュ・ガス事件(British Gas, BG)を取り上げる[8]。

前者は、問題人物であるイアン・ハントレー(Ian Huntley)という男のデータを、ハンバーサイド(Humberside)警察が削除していたというものである。ハントレーは、以前、ハンバーサイドに住み、数度にわたり性犯罪の容疑で逮捕されたという経歴を持っていた。ただし、有罪判決を下されたことはなかった。後に、ハントレーは、南方へ移り、ソーハムの学校で、偽名を使って働き始めた。学校は、男の経歴を調べたが、ハンバーサイド警察がデータを消去していたため、問題人物であることを発見できなかった。ハントレーは、2003 年 12 月 17 日、ジェシカ・チャプマン(Jessica Chapman)及びホリー・ウェルズ(Holly Wells)という２名の女児を殺害した罪で有罪判決を受けた。

ハンバーサイド警察の長官であるデイビッド･ウエストウッド(David Westwood)氏は、第 5 データ保護原則に基づいて消去した旨を発表し、データ保護法を批判した。

内務大臣(Home Secretary)は、事件の翌日、警察がハントレーの経歴に関する情報を処理した方法、及び、ハントレーを地方の学校に最終的に雇用するに至った身元調査の方法について、独立の調査を行う旨を発表した。その調査チームの長として、教育雇用省(Department for Education and Employment)の前政務次官であるサー・マイケル・ビシャード(Sir. Michael Bichard)を長に任命した。

ビシャード審問(Bichard Inquiry)は、2004 年１月 13 日より、同年３月 30 日まで、計 17 回にわたって実施され、同年７月 14 日、内務大臣への報告が行われた。報告書は同年７月 22 日に公開されている。報告の中で、ビシャード氏は、データ保護法には責任がなく、ハンバーサイド警察のミスであったことを明らかにした。

警察は、解釈の誤りを認め、上記発表を撤回している。

後者は、2003 年 12 月頃に発生した。

２人の老人がガス代を支払えなかったため、ガスの元栓を切られた。BG は、元栓を切った事実を、政府の社会福祉事業(Social Service)に報告しなければならないこととなっている。しかし、BG は報告を怠り、その結果、２人の老人は死亡した。BG は、データ保護法に基づき情報を提供しなかったと主張し、この事件はマスコミでも大きく取り上げられた。最終的に、BG は公表事実を撤回した。

ICO のホームページでは、「データ保護の俗説と本当の対応」(Data Protection myths and realities)と称し、事業者が慎重になりすぎて情報を提供しない５つのケースについて、概ね後掲のような内容で、あるべき対応が掲載されている。これら以外にも多々あるが、公表しているのはこれらのみであるとのことである(後掲１.(２)⑮イ)の「図表 個人情報保護の取扱いにおける「俗説」と「本当の対応」の概要」参照)。

[制度について]

ア)附則１「データ保護原則」の第１原則―公正かつ適法な取扱い

個人情報保護法 23 条(第三者提供の制限)1 項(事前の同意と例外)に直接的に相当する規定はない。

関連するものとしては、附則１第１章の「データ保護原則」(data protection principles)の第１原則を挙げることができる。

このデータ保護原則について、４条は、この法律でデータ保護原則というのは附則１第１章に明文化されているものである((１)項)とし、それらのデータ保護原則は、附則１第２章に従って解釈される((２)項)と規定している。また、４条は、データ保護原則を遵守するのはデータ管理者(「個人情報」の定義の項参照)の義務であるとしている((４)項)。

第１原則は、次のようになっている。

「個人データは、公正かつ適法に取り扱われなければならず、特に、(a)少なくとも附則２に掲げる条件の１つが満たされ、かつ、(b)センシティブな個人データについては少なくとも附則３に掲げる条件の１つが満たされる場合を除き、取り扱われてはならない。」

センシティブな個人データについては、後掲１．(2)④の「センシティブ情報に関する規定」で見ることにする。

イ)附則２「第１原則：個人データ取扱いの目的に関する条件」

附則２は、「第１原則：個人データ取扱いの目的に関する条件」(Conditions relevant for purposes of the first principle: processing of any personal data)と題されている。

その附則２は、次のような６つの条件を掲げている。

１．データ主体が当該取扱いに同意した。

２．当該取扱いが、(a)データ主体が当事者である契約の履行のため、又は(b)契約を締結する目的でデータ主体の要請に基づき手段を講ずるために、必要である。
３．当該取扱いが、契約によって課せられる債務以外で、データ管理者が従う法的義務を遵守するために必要である。
４．当該取扱いが、データ主体の重要な利益を保護するために必要である。
５．当該取扱いが、次に掲げる場合のために必要である。
(a)司法のため
(b)法規によりある者に付与された権能の行使のため、
(c)国王、国王の大臣若しくは政府省庁の権能の行使のため、又は
(d)ある者によって 公益のために行使される公的性格のその他の権能の行使のため

６．(1)　当該取扱いがデータ管理者によって追求される適法な利益(legitimate interests)のために必要である(この部分は要約)。
(2)　主務大臣がこの条件が満たされるために要求されるべき又は要求されるべきではない特定の状況を命令により明確にすることができる。この命令は、まだ定められていない(2009 年２月 21 日現在)。

個人データの取扱いは、ここに示した、附則２の条件の１つを満たすことができれば可能であるので、一般的には、広く行われている。

[制度の運用について]
データ保護法の的確な理解が必要であり、ICO は、ホームページで啓発活動を行っているばかりでなく、各種パンフレットの発行、研修会の開催などを行っている。また、ICO は、ソーハム殺人事件やブリティッシュ・ガス事件の教訓として、指導文書に法律用語を使わず、単純かつ分かり易く説明することを、さらに心がけるようになったとのことである。

②自治会や同窓会等の取扱い

[現状について]
データ保護法の適用除外は、事業者が取り扱う個人情報の量によっていない。適用除外は複雑であるが、一般的にいって、民間部門については、「ジャーナリズム、文学及び芸術」(journalism, literature and art)や家庭内利用目的(domestic purposes)の個人情報の取扱いは、適用除外される(第Ⅳ章)。日本でいう「自治会」に１対１で対応するものはないといえるが、そのような組織が個人情報を取り扱う場合には、データ保護法が適用される。また、現地調査で聞く限りでは、同窓会は存在するが、現在は、日本で伝統的に存在した同窓会

名簿はない場合が多いといえるけれども、何らかの形で(例えば、データベース)作成されるときには、データ保護法の適用があるとのことである。

[制度の運用について]

イギリスでは、自治会や同窓会については以下のような状況であるとのことである。

・イギリスにも「隣人監視組織」(neighbourhood watch)は存在し、また、家主が店子のリストを保有しており、その店子が集まって会議を行うような場合もあるということである。この場合、組織の性質にかかわらず、個人情報を取り扱う組織は法の規則を遵守する必要があり、自治体も自主的な組織も取扱いは同じであるということである。
・同窓会名簿については、「個人情報の掲載拒否を希望する場合は、掲載を停止することとすれば、作成できる。しかし、同窓会組織から名簿を大学側に渡す際に、その趣旨が大学にうまく伝わらず、大学で利用する際に不適切な取扱いをする場合があるということである。実際に、ある大学が同窓会名簿を売って金儲けをしたことがあり、問題になったことがある」ということである。

③「個人情報」の定義

ア)1998 年データ保護法の規定

1998 年データ保護法の 1 条は、基本的な解釈規定(Basic interpretative provision)であって、「データ」、「関連するファイリングシステム」又は「個人データ」について、次のように規定している。

(ア)データ

「データ」(data)とは、「(a)当該目的のために与えられる指示に応じて自動的に動作する装置によって処理されている情報、(b)当該装置によって処理されるべきことを意図して記録される情報、(c)関連するファイリングシステムの一部として又は関連するファイリングシステムの一部を構成すべきことを意図して記録されている情報、又は(d)上記(a)、(b)又は(c)の各号には該当しないが 68 条によって定義されるアクセス可能な記録の一部を構成する情報をいう」(1 条(1)項)と定義されている。

1984 年法では、自動処理されるデータのみが法律の対象となっていたにすぎないが、1998 年法では、上記のように、(c)関連するファイリングシステムの一部として又は関連するファイリングシステムの一部を構成すべきことを意図して記録されている情報も対象となる。

ここに出てくる「関連するファイリングシステム」についても、その定義を掲げるならば、次のようになる。

(イ)関連するファイリングシステム

「関連するファイリングシステム」(relevant filing system)とは、「情報が当該目的のために与えられる指示に応じて自動的に動作する装置によって処理されないにもかかわらず、個人への照会又は個人に関する基準への照会によって、特定の個人に関する特別の情報が容易にアクセスできるような方法でその一連の情報が構築されている限度における、個人に関する一連の情報をいう」(１条(１)項)と定義されている。

EU データ保護指令では、「『個人データ・ファイリングシステム』(「ファイリングシステム」)とは、機能的又は地理的な基準に照らして、集約化されているか、集約化されていないか、又は分散されているかどうかにかかわらず、特定の基準に基づいてアクセスすることができる構築された一連の個人データをいう」(２条(c)号)となっているので、イギリスの 1998 年法の定義はより詳細になっている。

(ウ)個人データ

「個人データ」(personal data)とは、「(a)当該データから、又は(b)データ管理者(data controller)が保有し、又は保有することになる可能性のある当該データその他の情報から、識別できる生存する個人に関するデータであって、かつ、当該個人に関する意見の表明及び当該個人についてデータ管理者その他の者の意図の表示を含む」(１条(１)項)と定義されている。

1984 年法では、「意図の表示」(any indication of the intentions)は「個人データ」には含まれていなかったが、1998 年法では、これも個人データの一部とされている。

例えば、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」である。

「個人データ」に関する控訴院の解釈は、ドュラント対 FSA 事件をめぐって議論が交わされている(後掲２.(３)②参照)。

イ)運用上の一般的な解釈

イギリスでは、個人情報について運用上、次のように解釈しているとのことであった。何が個人情報に当たるかという判断は難しいが、それが取り扱われる状況によるところが大きいということである。それが公共性のあるものなのか、真にプライベートのものなのかも重要であるとされる。

当該個人が特定される情報が個人情報であるが、例えば車のナンバーは、それだけでは個人情報ではないが、個人と関連づけられると個人情報になる。

④センシティブ情報に関する規定

[制度について]

1998 年データ保護法の規定では、センシティブ情報については、「２条 センシティブな

個人データ」(sensitive personal data)に規定されており、具体的には、「人種的・民族的出自、政治的意見、宗教的信条、労働組合への加入、健康状態、性生活、犯罪の前科・容疑、犯罪・容疑の手続・処分・判決」と定義されている。

センシティブな個人データの取扱いは、少なくとも附則３に掲げる条件の１つが満たされなければならない。附則３は、「第１原則：センシティブな個人データ取扱いの目的に関する条件」(Conditions relevant for purposes of the first principle: processing of sensitive personal data)であって、10 の条件を掲げている。そのうちの１つである「データ主体の同意」は、「明示の」(explicit)同意でなければならない。これは、一般の個人データの取扱いとは異なる点である。

人種に関する個人データは、例えば、企業の人事ファイルに個々人別に記録することはできないが、データ主体の明示の同意を得て統計目的で収集することはできる。また、政治的見解も人事ファイルに記録できない。

宗教に関する個人データについては、雇用関係においてイギリスの中でも北アイルランドでのみ収集・保管できる。これは、1989 年公正雇用(北アイルランド)法(Fair Employment (NI)Act 1989)[9]によるものである。

[制度の運用について]

イギリスでは、例えば、健康に関する情報はセンシティブであるが、利用目的と状況によって判断すべきだとする考え方もあるようである。この点について、以下のようないくつかの例が示された。

子どもが風邪をひいて学校を休むことについて、学校がコンピュータに入力した場合は、法律上センシティブ情報として取り扱われることになるが、本当にセンシティブ情報になるのかという疑問が残る。また、国民は信用情報を最も保護すべき情報と考えているが、イギリス法の定義では信用情報は必ずしもセンシティブ情報とはされていない。

また、イギリスでは組合の加入状況は、組合の権利が法で定められているため、センシティブ情報には入らないが、労使が敵対している他のヨーロッパ諸国ではセンシティブ情報になっている場合があるという指摘もあった。

さらに、例えば、Jones はウェールズ人の名前であるというように、名前からは特定の民族グループに属することがわかる場合があり、名前だけの利用であれば問題ないが、これを個人の趣味嗜好を知るために使う場合などは、センシティブ情報として取り扱われるということである。

⑤小規模事業者の取扱い

[現状について]

イギリスでは、小規模事業者は個人情報保護意識が不足しがちであると考えられている

ようである。例えば、従業員の医療情報などの取扱いについても十分に配慮していないし、具体的な例としては、ある新聞購読者が２週間配達を止めているという情報は、本人がその期間留守にしていることがわかってしまうにもかかわらず、小規模な新聞配達店などでは適切に取り扱われていない場合もあるとのことである。

[制度について]

1998 年データ保護法では、「データ管理者」(data controller)とは、「(４)項の規定に従い、(単独又は共同で又は他の者と協力して)何らかの個人データが取り扱われ又は取り扱われることになる目的及び態様を決定する者をいう」(１条(１)項)とされている。

1984 年法では、「データ・ユーザー」(data user)という言葉が使われていた。データ管理者は、それに相当するものであるといえる。

EU データ保護指令では、「『管理者』とは、単独又は他と協力して、個人データの取扱いの目的及び手段を決定する自然人、法人、公的機関、機関又はその他の団体をいう。取扱いの目的及び手段が国内法又は共同体法又は規則によって決定される場合には、管理者又はその指名に関する特定の基準は、国内法又は共同体法で定めることができる」(２条(d)号)とされている。

データ管理者には規模による相違はない。

[制度の運用について]

イギリスでは、保有リストの届出義務がないことを除き、小規模事業者だからといって特に適用除外はないとのことである。

小規模事業者は、企業活動に対する規制が多すぎると感じており、個人情報保護法も規制の1つと考えられていて歓迎されていないようである。小規模事業者向けの標準規約(Code of Conduct)を作成したが、対応しきれない内容であるという批判があり、もう少し簡素化したものにするべきではないかという議論がなされているとのことである。

⑥マス・メディアへの対応に関する規定とその内容

ジャーナリズムがデータ主体のプライバシーを侵害した場合は、ICO ではなく、プレス苦情委員会(Press Complaint Commission)が対応している。同委員会は、苦情を受けた際、当該行為が、自ら制定した行動規範に違反したか否かを確認し、対処する。訴訟に発展した有名な事件としては、キャンベル対 MGN 社事件(Campbell v. MGN Ltd)[10]、ダグラス対ハロー！社事件(Douglas v. Hello!)[11]がある。

なお、前掲１.(２)②のとおり、民間部門については、「ジャーナリズム、文学及び芸術」や家庭内利用目的の個人情報の取扱いは、適用除外される。ICO は、表現の自由に配慮して、ジャーナリズムに対しては特別扱いをしており、柔軟に対応している。1998 年データ

保護法が成立した際には、特にジャーナリズムからの反対はなかったとのことである。

⑦個人情報の目的外利用の防止措置

[制度について]

1998 年データ保護法の規定では、個人情報の目的外利用は、前掲の第２原則(限定された目的のための取扱い)によって制限されている。

附則１に規定されている、８つのデータ保護原則のうちの第２原則は、次のようになっている。

「個人データは、１つ又は２つ以上の特定のかつ適法な目的のためにのみ取得されなければならず、また、その目的又はそれらの目的と適合しない態様でさらに取り扱われてはならない。」

[制度の運用について]

イギリスでは、個人情報を使ってダイレクト・マーケティングを行う場合は、本人にダイレクト・マーケティング目的に使用してよいのかどうかの確認を取る必要がある。

一般的には、20～25%の個人は、ダイレクト・マーケティングに利用することに同意するが、質問を変えて、マーケティングに利用してほしくないか、と聞いても、20～25%の反応があるため、ダイレクト・マーケティング協会はオプトアウトを好む傾向があるということである。一方で、電子商取引法はダイレクト・マーケティングを実施する場合、媒体によっては、オプトイン方式を採用するように改正されたということである。

個人情報は生活の中で、必ず提供する場面があるので、二次利用については取得時の目的に照らして許容されるかどうかが重要になる。利用目的の範囲については、定義が非常に難しく、EU 各国でもばらつきがあるのが実際だという。国によっては完全に一致することまで求める国もあるが､そうでない国もあり､イギリスでも ICO が一部例示しているが、きりがないため、例示には限界があるということである。

そもそも、目的外利用は、本人の同意を取得した場合を除き、原則として禁止されている。目的外利用かどうかは、その情報が利用される状況と目的によって判断される。例えば､芝刈り機を買った顧客の情報を“芝の種”のマーケティングに使用することは許容されるが、CD の販促を行うのは明らかな目的外利用に当たる。

⑧市販の名簿の管理

[制度について]

1998 年データ保護法には、名簿(directory)に関する明文の規定はない。

[制度の運用について]

イギリスでは、市販の名簿も法律の規制対象になっているとのことである。そのような名簿への掲載のために個人情報を提供した時点で、一般に公表されることは前提になっていると考えられることが理由である。したがって間接取得した事業者は、利用目的が当初の目的と同じかどうかを判断する必要があるとのことである。

電話帳など、市販のリストの個人情報をコンピュータに取り込んだ時点で、法律に基づく取扱いが必要となるため、本人に利用目的を通知することが必要となる。印刷してある電話帳をそのまま利用する場合は、本人への通知は不要であると理解されているということである。

また、このような市販の名簿に関しては、類似の事例や対応について、以下のような状況があるとのことである。

・以前は、投票登録名簿(選挙人名簿に該当)がマーケティングに頻繁に利用された。若い夫婦や老夫婦が住む地域、金持ちの多い地域、職人が住む地域といった、地域による特性を明らかにするため、世論調査などにも利用されたようである。
・投票登録名簿については、2000 年の法改正(Representation of People Act 2000)[12]により、データベース登録の際に商用利用を拒否する場合は印が付けられることになったが、多くの国民は印を付けていないようである。
・事業者はリストブローカーから名簿を借りる場合があるが、この名簿には、賞品のプレゼント企画やコンテスト企画によって収集した個人情報が多く存在している。情報収集に当たっては、個人情報の利用目的を明確化する必要がある。また、第三者に提供する際には、本人の同意が必要である。
・広く頒布されているリストを利用したマーケティング活動については、オプトアウトの機会が提供されている。
・このような規制を回避するために、名前をつけずに郵便物を特定の地区等の郵便受けに入れる手法がとられているようである(いわゆるポスティング)。
・電話帳については、法律上、本人に掲載の可否を選択する権利が認められている。
・電話業界には、複数の民間事業者が存在しているが、電話帳の掲載可否については、一度選択を行えば、すべての電話会社が同じ対応をとることになっている。掲載は認めるが商用利用は拒否するという選択もできる(Telephone Preference Service, TPS)。
・苦情のほとんどは、マーケティング関係である。最近はマーケティング協会(Direct Marketing Association, DMA)と緊密に連絡をとって対応していることもあり、以前ほど問題は起こっていない。
・イギリスにも名簿事業者は存在している。数は少なくないが、多くは DMA のメンバーである。

・すべての組織は個人情報を適切に取り扱わないといけないので、電話帳でも安全に取り扱う必要がある。銀行、税関、郵便局では、リストはシュレッダーにかけたり、処理業者に委託する必要がある。捨てられているリストを入手し、商用利用した事例もあった。
・企業年鑑などのように、公開され、一般に入手可能な個人情報については、それを利用する企業の社員などはセキュリティに特に気をつける必要はない。道端に捨てても問題はない。一般に公開されているものは、誰でもどこでも容易に入手できるため、特別な配慮は不要という考え方である。

⑨個人情報の取得元の開示に関する措置

[現状について]
イギリスでは、取得元の開示についての請求は多いはずであるが、請求は個人からデータ管理者に直接行くため、統計は整備されていないとのことである。

[制度について]
前述のように、1998 年法の第Ⅱ章は、「データ主体の権利その他」として、日本の個人情報保護法でいう「本人」に様々な権利を認めている。その１つとして、７条で、個人データへのアクセス権が規定されている。その中で個人情報の取得元についても開示を請求することができることを明文化している(７条(１)項(c)号)。
これは、取得元にさかのぼって個人情報の停止などを要求する必要があるので、取得元についてはできる限り多くの情報を提供することが求められている。

[事業者の対応について]
イギリスでは、取得元の開示については、事業者は情報主体の信頼を得るために、可能な情報は提供することになるはずであるという指摘があった。
また、コンピュータにより、情報の取得元を割り出すことが容易になったことも影響を与えているようである。リストを購入する際は、取得元を必ず教えてもらうようにしており、リストブローカーもビジネスとして情報の取得元を明確にする必要がある。また、郵送した場合なども、情報の取得元について問い合わせが来る場合があるため、回答を用意しておく必要があると認識されているようである。

⑩個人情報の利用停止・消去に関する措置

[現状について]
ダイレクト・マーケティングへの利用を拒否したいイギリス人国民は、多くは禁止サービス(suppression service)に登録しているとのことである。約半数の世帯は、電話選好サー

ビス(TPS)に登録し、約８分の１は氏名と住所について、郵便選好サービス(Mail Preference Service, MPS)に登録しているとのことである。

[制度について]

上記⑧と同じく、1998 年法の第Ⅱ章「データ主体の権利その他」(７条―15 条)の一環として、個人情報の利用停止・消去に関する措置にかかわる規定がある。その他の規定も含め、「第Ⅱ章　データ主体の権利その他」の 10 条以下の条文見出しを掲げると、次のようになる。

10 条　損害又は苦痛を与えるおそれのある取扱いを停止させる権利
11 条　ダイレクト・マーケティングの目的のための取扱いを停止させる権利
12 条　自動決定に関する権利
13 条　一定の要件を満たさないことに対する賠償
14 条　修正、封鎖、削除及び破棄
15 条　管轄権及び手続

[事業者の対応について]

イギリスでは、ある大手のダイレクト・マーケティング企業では、消費者サービスの部署で、毎年数千件の利用停止などの請求を受け付けているということである。

⑪国際的な情報移転に関する措置

[制度について]

ア)1998 年データ保護法の規定

附則１「データ保護原則」の第８原則は、十分な保護のない第三国への移転制限に関する規定である。

第８原則は、「個人データは、ヨーロッパ経済地域以外の国又は地域が個人データの取扱いに関しデータ主体の権利及び自由について十分なレベルの保護を確保している場合を除き、その国又は地域に移転してはならない」とするもので、十分な保護のない第三国への移転を制限している。

1998 年法は全体として EU データ保護指令を国内法化するものであるが、特にこの第８原則はイギリス所在の日系の企業が日本に個人データを移転する際に問題となり得る。

イ)1998 年データ保護法の例外規定

一般の企業がその個人データを第三国に移転する場合には、上記のデータ保護原則の第８原則によって、第三国が「十分なレベルの保護」を確保していないときは、その個人デー

タを移転することができない。このことは、特に多国籍企業の場合には深刻である。第８原則に対する例外が附則４に規定されているので、それを見ることにする。

附則４「第８原則が適用されない事例」は、次のような場合を掲げている。

１条　データ主体がその移転に同意している場合。

２条　その移転が(a)データ主体とデータ管理者の間の契約を履行するため、又は(b)データ管理者と契約を締結する目的でデータ主体の要請により措置を講じるために必要である場合。

３条　その移転が(a)(i)データ主体の要請に基づき結び、又は(ii)データ主体の利益のためである、データ管理者とデータ主体以外の者との間の契約締結のために必要である、又は当該契約の履行のために必要である場合。

４条　(1) その移転が実質的な公益のために必要である場合。

(2) 主務大臣は、命令により、(a)実質的な公益のために必要とされる(１)項の目的のために移転が行われる状況、及び(b)法令により要求されない移転が実質的な公益のために必要とされる(１)項の目的のために行われるべきではない状況を定めることができる。

５条　その移転が、(a)何らかの法的手続(見込まれる法的手続を含む)の目的のため、又はその手続に関連して、必要であり、(b)法的助言を得る目的で必要であり、又は(c)その他法的権利を確立し、行使し、又は防御する目的のために必要である場合。

６条　その移転が、データ主体の重要な利益を保護するために必要である場合。

７条　その移転が公的な登録簿の個人データの一部にかかわり、その登録簿が閲覧に供される条件が移転後にデータが提供され又は提供され得る者によって遵守される場合。

８条　その移転がデータ主体の権利及び自由のために十分な保護措置を確保するものとしてコミッショナーにより承認される種類の条項に基づいて行われる場合。

９条　その移転がデータ主体の権利及び自由のために十分な保護措置を確保する態様で行われるものとしてコミッショナーにより認められている場合。

[法律以外の枠組みについて]

イギリスでは、現在の法律の下では EU 以外には情報の移転は原則禁止されている。そこで、多くの事業者は例外の１つである「契約」で対応しているということである。また、同一企業グループ間での国際的な個人情報移転に関しては、「拘束力のある企業ルール」(Binding Corporate Rules)も使われているということである。

また、多国籍企業の場合にはプライバシーポリシーを個々に申請して認証を得ることが必要である。EU の別の国を使う場合もあるとのことである。

ICO には、「拘束力のある企業間ルール」について、標準的なチェックリストを作成し、申請のあったルールのチェックを行っているということである。問題点としては、認証に

時間がかかる手続になっているという点が指摘された。

一方、「契約」については、EU に許可された標準的な契約様式を用いる方法がある。多岐にわたり、細かく規定されているため、ICO はチェックを行わない。標準的な契約様式を踏まえ、事業者が独自の契約様式を使用する場合についても、ICO が事前にチェックを行うことはないということである。問題が発生し、苦情が寄せられた場合にのみ ICO が対応するようにしているということである。「契約」には現在、３つの様式があるということである。

⑫EU データ保護指令に対する対応状況

EU データ保護指令は、1998 年 10 月 24 日にまでに対応するように構成国に求めていたので、イギリスは、形式的には対応していると見られている。

前述のように、1984 年法は、自動処理データのみに適用されていたが、EU データ保護指令が「個人データ・ファイリングシステム」も対象にしているので、1998 年法では、「関連するファイリングシステム」にも適用されるようになった。

⑬死者に関する個人情報の保護

[現状について]

死者に関する個人情報は、データ保護法では、保護の対象になっていないため、公開されたりすることがあり、問題になっている。また、ダイレクト・マーケティングの分野では、死者あてにメールが送られると、遺族が不快の念をいだくという問題などがある。

[制度について]

1984 年法で「生存する個人」(living individual)という概念が使われ、日本の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(1988 年)で取り入れた。1998 年データ保護法でも、同様の規定になっている。そのため、データ保護法の下では死者は何の権利も認められていないといえる。しかし、死者につながる生存する個人に関する情報は、保護の対象となる。

死者について規定しているのは、1990 年健康記録アクセス法(Access to Health Record Act 1990)[133] ３条である。同条は保健記録へのアクセス権に関する規定で、その(１)項は、次に掲げる者は保健記録の保有者に対してアクセスを請求することができるとして、(a)患者、(b)患者に代わって請求する権限を文書で付与された者、(c)記録がイングランド及びウェールズで保管され、かつ、患者が子どもである場合には、その患者の親権者、(d)記録がスコットランドで保管され、かつ、患者が生徒である場合には、その患者の親又は後見人、(e)患者が自己に関する事項を管理することができない場合には、裁判所により当該事項を管

理するよう任命された者、(f)患者が死亡した場合には、その患者の人格代表者(注・遺言執行者と遺産管理人の双方を含めてこのように称せられる)及び患者の死亡から発生する請求権を持ち得る者を挙げている。この最後の(f)が死者についての規定である。

[制度の運用について]

イギリスでは、ダイレクト・マーケティングの分野で、死者あてにメールが送られると、遺族が不快の念をいだくという問題などがあるばかりでなく、データ保護法で情報を正確かつ最新に保つことが求められ、コストもかかるという指摘があった。

そこで、ダイレクト・マーケティングを行うことが多いような団体では、ダイレクト・マーケティングのキャンペーン用の個人情報ファイルに含まれる死者情報については、スクリーニングを行うようにしている。そのことで、遺族の不興を買うことを避けるようにしているということである。

⑭直接処罰等の実効性担保の措置

[制度について]

1998 年データ保護法は、55 条で「個人データの不法な取得等」(unlawful obtaining etc. of personal data)について規定している。これは、違反者を直接処罰する規定である。
55 条(１)項は、次のように規定している。

「何人も、データ管理者の同意がなければ、故意又は認識ある過失で、(a)個人データ若しくは個人データに含まれる情報を取得し若しくは提供し、又は(b)個人データに含まれる情報について他の者に提供するようにさせることをしてはならない。」

この(１)項に違反した者は、罪を犯したことになる((３)項)。

法定刑は罰金で、データ保護法 60 条に規定がある。1991 年刑事裁判法(Criminal Justice Act 1991)[14]17 条によると、上限は 5,000 ポンドである。

歴史的にみると、1984 年データ保護法にはこのような規定はなかったが、個人データを権限がないのに取得しようとする動きが 1990 年代初頭から、明らかに拡大してきた。そこで、1994 年の刑事司法及び治安法(Criminal Justice and Public Order Act 1994)[15]の 161 条が、1984 年データ保護法５条の罰則を拡大した。161 条は、コンピュータで保有される個人情報を提供及び販売させること(procuring disclosure of, and selling, computer-held personal information)と題されていた。これをさらに個人データ一般を対象とし、個人データの不法な取得を処罰するようになったのが 1998 年データ保護法 55 条である。

これは、日本でも議論となった個人情報の窃盗・漏えいなどを直接処罰する規定の立法例である。それに加えて、1998 年データ保護法は、個人データの無登録取扱いを処罰する

こととしている(17 条)ため、情報コミッショナーの年次報告書では、訴追については、17 条違反及び 55 条違反の訴追の統計が出ている。2007/2008 年次報告書では、11 件の訴追が行われ、103 件の有罪認定が下された(うち、３件の訴追及び 90 件の有罪認定が 55 条違反である)。

[制度の運用について]

イギリスでは、データ保護法違反に関する情報を得ることが容易ではなく、情報提供を受けて捜査を開始することがしばしばあるということである。例えば、データ主体等からの苦情が端緒で訴追手続を始めることがある。しかし、苦情ばかりでなく、新聞等で 55 条違反関係の事件が取り上げられることにより、捜査が始まることもある。

これまでの具体的事件を見ると、次の３つに分けられるといえる。

ア)被用者型(employee 型)－銀行で働く、業務上顧客情報へのアクセス権のある従業者が、銀行の許可なく、顧客情報にアクセスして信用情報等(banking information)を入手するというもの。

イ)私立探偵型(private investigator 型)－私立探偵が、銀行を騙すもので、騙し方にはいくつかの方法があるが、電話で顧客と関係のある銀行などからなりすましで顧客情報を取得するもの。

ウ)自己利用型－金融サービスを提供している企業で働く職員が、退職する際、自分の新しいビジネスのためにこの顧客情報を持ち出して利用するもの。

⑮その他、特に留意すべき重要措置

ア)今後、個人情報保護に関してどのような取組が行われるか。

イギリスでは、20 年以上前の 1984 年に個人データを体系的に保護するデータ保護法が制定された。1984 年法で任命された初代のデータ保護登録官のエリック・ハウ(Eric Howe)氏も、２代目のエリザベス・フランス(Elizabeth France)女史も、データ保護法の普及啓蒙活動に誠心誠意努めてきた。

イギリス社会では、一方で、データ保護法が定着していると評価されているが、他方で、データ保護法についての誤解・無視・軽視なども見受けられる。

これは、データ保護法に特有な問題ではなく、法一般の問題でもある。

法に関する普及啓蒙活動は今後とも極めて重要であり、ICO は、データ保護法について今後ともそのような努力を続けていくことを強調している。

イ)「過剰反応」の例

以下のとおり、ICO は、マスメディアに取り上げられたものを含め、誤解を招き易い事

例をもとに、「俗説(myths)」として過剰な反応の事例を示し、「本当の対応(reality)」として、その俗説のような考え方、対応方法の問題点や正しい考え方を示している。

なお、俗説１から３について、ICO は実務指針(practical guidance)を出して対応している。

【図表　個人情報保護の取扱いにおける「俗説」と「本当の対応」の概要】[16]

	俗説(myths)	本当の対応(reality)
1	データ保護法は両親が学校で子どもの写真をとることを禁じている。	・純粋に私的な目的で撮影された写真は法の対象外である。 ・両親、友人、家族等は家庭用のアルバムを作る目的であれば、学校の行事に参加している子どもや友人の写真を撮影することが認められる。 ・データ保護法は、写真が学校や大学で公に利用される場合に適用される。例えば、通行証に用いるために、氏名のような個人の情報とともに画像を保存する場合などである。法律が適用される場合であっても、通常は撮影者が許可を求めることで足りる。
2	データ保護法は事業者が顧客の情報を第三者に提供することを一切禁じている。	・第三者でも個人情報にアクセスする権利を認められていれば、事業者がその者に個人情報を提供することは妨げない。 ・事業者は、顧客の情報を明らかにすることについて注意すべきである。個人情報の市場が存在しており、詐欺によって他者の情報を得ようとする不謹慎な者たちも存在する。 ・したがって、事業者は、銀行口座情報のように、従業者が顧客である個人の情報を開示するという決定を下す場合は、従業者の話している相手が、確実に自らの顧客又はその代理人(例えば、口座保有者が権限を与えた証拠がある場合)であるか否かを確かなものにするために適切な安全保護措置を講じなければならない。従業員は、個人情報を提供する現実的必要性があるか否かを考慮すべきである。 ・頻繁に他人の代理を行う者は、パスワード等により、第三者提供を受けられる代理人としての認証を受けるなどの方策をとることが、その企業で可能であるかどうかを確認すべきである。
3	データ保護法は両親が子どもの成績を見ることも	・データ保護法は、試験委員会が生徒やその母親に結果を渡すことを禁止していない。試験委員会は、当該生徒の自

	俗説(myths)	本当の対応(reality)
	禁止している。 これは、フルートの試験を受けた11歳の少女が自らの試験結果を確かめられなかったことが報道されたことに端を発する。	宅住所に送ることによって、正しい人物への情報開示を確実にすることができた。 ・この件で、生徒の母親があえて自分の娘の試験結果を開示するよう、情報主体のアクセス請求を出さなければならないというのは、明らかに不公正かつ不要である(ので、法はそこまで求めていないと理解すべきである)。しかし、少なくとも、アクセス権は、彼女が情報を得る権利を持つことを確実にした。
4	司祭が祈祷の途中で信者の名前を読み上げることは禁止されている。 これは、ローマカトリック教会で、司祭が、訴追をおそれて信者の名前の読み上げを取りやめたことが報道されたことに端を発する。	・データ保護法は、主にコンピュータ処理された個人情報を対象としている。地元教会の信者に関するこの類の情報は、コンピュータや複雑な紙のファイリングシステムには保存されないことが多く、そのため、このような形態の個人情報は規制の対象外である。 ・もしその情報が法律の適用対象であったとしても、本人が祈祷の最中に名前を読み上げられることについて歓迎していれば問題ない。しかし、もし本人が祈祷の最中に名前を呼ばれることを明示的に拒否している場合や、司祭が、信者が名前を読み上げられたくないことを察することができる場合には、その意思を尊重すべきである。
5	データ保護法は加害者の情報を被害者に教えることについて禁止している。 これは、車の損傷を受けた被害者が、警察に対して、加害者の情報の開示を求めたところ、拒否されたことが報道されたことに端を発する。	・警察が、要注意の加害者の情報について1998年データ保護法を理由に被害者に教えないことは、誤った対応である。 ・民事訴訟が予定されている場合に、関係者の個人情報を提供しないことまで法は予定していない。警察は個人情報の公開については常に注意する必要があるが、内務省から「どのような個人情報は提供してよいか」ということについて明確なガイドラインを示されている。 ・情報コミッショナーは本件について警察庁と交渉し、個人情報の提供を行わせた。

２．第三者機関について

（１）第三者機関の実態

①制度の概要

1998 年データ保護法は、第Ⅰ章　序則(1 条―6 条)の中の 6 条で、コミッショナー及び審判所(The Commissioner and the Tribunal)を置くと規定している。コミッショナー及び審判所のうち、個人情報保護に関する、直接的な監督機関は、コミッショナーである。コミッショナーは、1984 年法の定めるデータ保護登録官を引き継ぎ、データ保護コミッショナーとしてスタートした。その後、2000 年情報自由法(Freedom of Information Act 2000)[17]の運用にも当たるようになったことから、2001 年 1 月 30 日、情報コミッショナー(Information Commissioner)に名称を変更した。1998 年法成立時の情報コミッショナーは、エリザベス・フランス氏であったが、2002 年 11 月 30 日以降は、リチャード・トーマス(Richard Thomas)氏が務めている。

情報コミッショナーは、開封勅許状(Letters Patent)(権限付与のための文書で、他人が確認しやすいように開封されているので、このように呼ばれている)により女王によって任命される(６条(２)項)。

また、情報コミッショナーの職務・権能については、第Ⅵ章　雑則及び総則(51 条―75 条)の中で、51 条から 54 条までの規定がある。

一般的な職務については、「データ管理者が善良な実務を守ることを促進し、また、とりわけ、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」と定められている(51 条(１)項)。

個別の業務については、以下のとおりである。

・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)。未登録によるデータの取扱いは犯罪を構成し(17 条、21 条)、登録事項は無料公開される(19 条(６)項)。
・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達する(40 条)。
・評価請求に基づき情報提出通知を送達する(42 条、43 条)。
・特別の情報提出通知を送達する(44 条)。
・裁判所の令状に基づき立入検査権を行使する(50 条、附則９)。
・善良な実務や自らの権限等について、国民に対して情報提供を行う(51 条(２)項)。
・善良な実務に関する指針のための実務規範の策定及び配布を行う(同条(３)項)。
・両議院への年次報告を行う(52 条(１)項)。
・違反者に対して訴追する(60 条(１)項)。

その他、情報コミッショナー、その職員、代理人等は、原則として、取得した情報の機密性を守らなければならず(59 条(１)項(２)項)、故意又は認識ある過失により、これに違反して情報を提供した場合は、有罪となる(同条(３)項)。また、特別目的のための取扱い(アクセス権等)について、訴訟当事者になりそうな個人は、コミッショナーに援助を申請することができる制度(53 条)や、コミッショナーが、EU データ保護指令を遵守するためのイギリス国内での監視当局となること(54 条(１)項)等の制度が存在する。

附則５は、コミッショナーの地位、任期、俸給等について規定する。その特徴は、女王から独立し、議会に対して責任を負うという点に見られる。

・単独法人である(附則５第１章１条(１)項)。
・女王から独立した法執行機関である(附則５第１章１条(２)項)。
・開封勅許状により女王陛下から任命される(６条(２)項)。
・任期は５年以内、再任可(附則５第１章２条(１)項(４)項)。
・定年は 65 歳に達する日の属する職務年度の満了時又は 15 年の勤務を満了した時(附則５第１章２条(４)項)。
・自ら辞職する場合(附則５第１章２条(２)項)のほか、両議院の解任請求に伴い、女王から解任されることがある(附則５第１章２条(３)項)。
・俸給や年金の支給は、庶民院の決議で指定される(附則５第１章３条)。
・必要経費は議会が主務大臣に付与した額から支払われる(附則５第１章８条)。
・コミッショナーは、会計帳簿及び決算報告書を策定し、会計検査官は、決算報告書の写しに自らの報告書を付して、各議院に提出しなければならない(附則５第１章 10 条)。

②オフィスの実態

ICO は、マンチェスター郊外に本部事務所を構えるほか、北アイルランド、ウェールズ、スコットランドにも地域事務所を置いている。

ICO は、1998 年データ保護法のみならず、2000 年情報自由法、2003 年プライバシー及び電子通信(EC 指令)規則(Privacy and Electronic Communications (EC Directive) Regulations 2003)[18]、2004 年環境情報規則(Environmental Information Regulations 2004)[19]に基づく任務を担っている。権限拡大に伴い、毎年スタッフを増員し、組織を拡大させているとのことである。

2007/2008 年次報告書によれば、2007 年度に情報コミッショナーと常勤契約を締結しているスタッフは245名､情報コミッショナーの定める目的遂行に従事するスタッフは16名、合計 261 名となっている。前年度は、常勤契約が 243 名、その他スタッフが 19 名、合計 262 名であったことから、ほぼ横ばいである。

ICO は、質問と苦情が多く、その対応に時間をとられているため、もう少し人数が欲し

いと感じているということである。

ICO の運営は、データ管理者が毎年支払う 35 ポンドの登録料で行われている。2000 年３月１日の制度導入時から値上げは行われていない。2007 年度に受け取った手数料は、10,817,621 ポンドであり(延滞分を調整すると 10,592,887 ポンド)、営業利益総額は、10,613,117 ポンドであった。一方、スタッフに支払われた人件費は、8,616,009 ポンド、その他の営業経費が 7,088,324 ポンド、減価償却及び評価損が 1,252,241 ポンド、総額 16,956,574 ポンドの支出となった。その結果、ICO は、6,343,457 ポンドの営業損失を出している。この赤字分は、主に司法省からの補助金でまかなわれている。2007 年度の補助金は、5,050,000 ポンドであった。

③リソース確保に関する現状と問題点

情報コミッショナー(以前はデータ保護登録官、データ保護コミッショナー)は、1984 年法の時代から、独立の法執行機関としての職務を担っており、20 年以上の歴史を持つ。

しかし、第三者機関である情報コミッショナーに対する外部からの評価としては、以下のような見方も示されている。

情報コミッショナーは機能のバランスがよく、一定の役割は果たしていると考えられるが、権限が小さいことが課題である。例えば、令状なしに家宅捜査などを行う権限はない。この権限は国会により厳格に管理されており、警察しか保持していないものである。したがって、情報コミッショナーが家宅捜査を行いたいと主張した場合があったが、議会から阻止されたこともあったということである。

また、ICO には、そもそも各企業を個別に調べるための人員が不足しているという点も指摘された。実際には、苦情が寄せられれば、その都度対応しており、苦情があった場合、その問題がこじれないように、うまく解決していると考えられているようである。ただし、ICO は大企業に介入することがほとんどであり、小規模企業までは介入できていないということである。

資金面では、前掲２.(１)②のとおり、ICO は情報自由法の執行活動に基づく営業利益を持たないため、登録費用だけでは活動費をまかなうことができない。そのため、政府の補助金が重要な役割を果たしている。

④広報の実態

国民に対する情報提供や実務規範の公表は、情報コミッショナーの職務に含まれる。詳しくは、後掲２.(２)③を参照。

データ主体及びデータ管理者ともに、法律への関心度は非常に高いが、データ管理者の中には、消極的な反応を示す者もある。その場合、ICO は、当該データ管理者とミーティ

ングを行い、データ保護法を守ることによって評判を高め、事業にもプラスの効果を与える、データ保護法は新しい対応を求めるものではなく、例えばデータの正確性は、従来の対応を継続してもらえば良い等と説明し、懸念を払拭している。実際に、法律に基づく執行を行うこともあるが、可能な限り話し合いによってデータ保護法の理解を求めている。

データ管理者の法に対する認知度は、概ね９割を越える数字となっており、非常に高い値を示している。一方、データ主体(日本の法律でいう「本人」に該当する。)の認知度は、施行年である 2000 年の段階では３割弱という数字であったが、徐々に上昇し、2002 年から2003年の時期に７割を超すに至った。2006/2007年次報告書では、データ管理者は94%、データ主体は 82%、2007/2008 年次報告書では、サンプル数 1,223 件のうち 90%のデータ主体が自らの権利を認識しているという結果が公表されている。

また、2006/2007 年次報告書では、情報コミッショナーのサービスの満足度が公表されている。データ管理者については、128 事業者のうち、素晴らしい(Excellent)が９%、とても良い(Very Good)が 23%、良い(Good)は 34%、まあまあ(Fair)が 20%、悪い(Poor)が 15%、知らないが０%であった。個人については、202 人を基準としており、それぞれ、14%、22%、20%、12%、28%、３%となっている。

（２）第三者機関の活動状況

①第三者機関の国内での活動状況

ICO は、主に国内における問題を取り扱っており、主な活動状況については、ホームページや年次報告書に、その概要が掲載されている。

最近の活動の中で特筆すべきは、個人情報取引産業の取締りとの関係で、ICO が、2006年５月 10 日、議会に「プライバシーとは一体何でしょう？」(What price privacy?)という報告書を提出し、不法な個人情報の取得、売買を働いた者に対して拘禁刑を科すべきであると主張したことである。1998 年データ保護法 52 条(2)項は、「コミッショナーは適宜、議会の各院に、自らが適切と判断した権限に関して、他の報告書を提出することができる」との定めを置くが、それに基づく初めての報告書である。

55 条は、情報を保有する組織の同意なくして、個人データを故意又は認識ある過失で取得したり提供したりする行為を犯罪としているが、現在の法定刑は罰金のみであり、治安判事裁判所では 5,000 ポンドまで、刑事裁判所では上限なく刑事罰を科すことができる。しかし、機微な個人情報を組織的な取引の対象とする者には有効ではなく、事件を追いかける記者や、負債者を追跡する金融機関が情報を買い、一方の情報を売る側には私立探偵が必ずと言ってよいほど関係している。したがって、仮に違反者を訴追したとしても、5,000ポンドを超える罰金を受けるのはごくわずかな数であり、実効性が薄い。そこで、報告書では、大法官に対し、55 条違反の者に対する罰則を引き上げ、最大２年までの拘禁刑若し

くは罰金又はその併科、また、陪審によらない有罪判決については、最大６ヶ月までの拘禁刑若しくは罰金又はその併科を提案すべきである旨を要請した。
また、同年12月には、「プライバシーとは一体何でしょう？その後」(What price privacy now?)という第２報告書を発表した。この報告書では、司法省その他の関係団体との協議結果等がまとめられている[20]。

ICO の提案は法案提出へとつながり、2008 年刑事司法及び入国管理法(Criminal Justice and Immigration Act 2008)[21]が、2008 年５月８日、女王の裁可を受けて成立した。この法律の 77 条は、個人データの不法な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)を定めており、1998 年データ保護法を改正するものである。

77 条(１)項及び(２)項の規定は、次のようになっている。

「(１) 主務大臣は、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、次に掲げる責任を負わせる旨を定めることができる。
(a) 陪審によらない有罪判決に基づき、所定期間以内での拘禁刑、若しくは、法定上限額を超えない金額での罰金に処し、又はこれを併科する。
(b) 正式起訴状に基づく有罪判決により、所定期間以内での拘禁刑、若しくは、罰金に処し、又はこれを併科する。
(２) (１)項(a)号及び(b)号の定める『所定期間』は、命令により定められる期間をいうが、次に掲げる期間を超えてはならない。
(a) 陪審によらない有罪判決の場合、12 ヶ月(又は、北アイルランドは６ヶ月)、及び、
(b) 正式起訴状に基づく有罪判決による場合、２年」

この規定はまだ施行されていない(2009 年２月 20 日現在)。

ICO は、法律成立の翌日、プレスリリースを発表し、改正を歓迎する旨の声明を明らかにしている。

②第三者機関の国際的な活動状況

情報コミッショナーは、EU データ保護指令 29 条に基づき設置される「個人データの取扱いに係る個人の保護に関する作業部会」(通称 29 条委員会)に参加し、国際的な個人情報保護のための取組、越境執行協力に関する活動について、年４～５回の割合で検討している。

情報コミッショナーは、2006 年 11 月２日から３日にかけて、監視社会をテーマとして、第 28 回データ保護・プライバシー・コミッショナー国際会議(International Conference of Data Protection and Privacy Commissioners)をロンドンで主催した。2006/2007 年次報告

書によると、2007 年３月には、ヨーロッパで最も優れたデータ保護コミュニケーターとして支持された。

2007/2008 年次報告書によると、2007 年 12 月、情報コミッショナーは、上記プライバシー・コミッショナー国際会議のフォローアップ会議を主催し、プライバシー影響評価(privacy impact assessment)ハンドブックの策定に着手した。作業部会は、2007 年３月以降、14 の文書を採択しており、その中には、個人データの定義、及び、搭乗者名簿登録に関するアメリカの合意や EU の提案に対する意見を述べた文書も含まれる。

また、情報コミッショナーは、EU データ保護機関及びアジア太平洋経済協力(Asia Pacific Economic Co-operation, APEC)地域との間における、越境プライバシー原則の制度をめぐる協議を進めることにも関与し、データ保護コミュニケーターの国際ネットワークの発展の指導的な役割を果たしている。

その他、ICO は、ユーロポール及び関税情報システム(Europol and the Customs Information System)、ユーロダック(Eurodac)(亡命希望者を特定するためだけに設計されたヨーロッパの指紋データベース)及びユーロジャスト(Eurojust)(EU の共同司法機関)の監督活動にも参加している。

③教育・啓蒙、普及・広報活動等の現状

ICO は、データ保護法を普及させるため、キャンペーン、宣伝活動、定期的な会合、講演、実務規範その他指導文書の配布など、実に様々な試みを行っている。2007 年度は、情報自由法関連をあわせ、25 の指針の公表又は改定を行った。ICO が最近出したものとしては、CCTV の実務規範、及び、雇用実務規範があり、前者は2008年に改定された(後掲３.(１))。情報コミッショナーは、プレスリリースを公表し、インターネットに掲載するほか、関連事業者への送付、週刊誌への掲載などを行っている。

ICO のホームページのうち、「ドキュメント・ライブラリー」(Document Library)の中の「データ保護」のページには、実例集(Practical application)、専門家向け詳細ガイド(Detailed specialist guides)等の項目の中に、実務指針など多数の関連文書が挙げられている。この中に「データ保護の俗説と本当の対応」も掲載されている(前掲１.(２)⑮)。

その他、ICO は、年に 300 回程度の研修会を開いているとのことである。

④第三者機関と外部機関等との関係

特定分野に関して監督権限を有する組織がある場合、情報コミッショナーは、当該組織と共同して法の執行を行っている。

金融分野では、FSA(Financial Services Authority)が、2000 年金融サービス市場法(Financial Services and Markets Act 2000)[22]に基づき行政処分を下す権限を有しており、

ICO よりも強力な執行権限を行使している。具体的には、住宅組合がコンピュータを紛失した事例において、FSA は、98 万ポンドの罰金に処した。

通信分野では、OFCOM(Office of Communications)が、2003 年通信法(Communications Act 2003)[23]に基づき、イギリス国内の通信事業者を監督している。迷惑電話、迷惑ファックス、迷惑メールについては、ICO がデータ保護法並びにプライバシー及び電子通信規則に基づいて執行を行う際に、OFCOM と共同で対応している。

消費者保護の関係では、OFT(Office of Fair Trading)が所管しており、1998 年競争法(Competition Act 1998)[24]や 1974 年消費者信用法(Consumer Credit Act 1974)[25]等の監督を行っている。

（３）苦情・紛争処理の実態

①苦情・紛争処理の概況

1984 年法は苦情処理制度を設けていたが、1998 年データ保護法では、個人データの取扱いによって影響を受ける者の評価請求に基づき、情報コミッショナーが当該取扱いを評価するという制度となっている。

苦情/評価請求の受付件数は、年によって異なるが、1984 年法の時代から見てみると、1999 年頃までは、概ね、2,000 件台から 4,000 件台で推移し、1999 年から 2000 年の時期に、約 5,000 件へと達した。その後は急速な伸びを示し、2000 年から 2001 年は約 9,000 件、その後 2004 年頃までは 11,000 件から 12,000 件程度、2004 年から 2005 年は約 20,000 件、それ以降は、22,000 件から 24,000 件程度となっている。2007/2008 年次報告書によると、24,851 件の評価請求を受け付け、25,592 件（前年度未処理の件数を含むと考えられる）を処理し、1,237 件の処理を進めているという結果が公表されている。評価請求のあった事業分野は、金融が 33%、一般事業者が７%、電気通信が５%、警察及び刑事記録関係が５%、中央政府が５%、地方政府が４%、医療が４%、ダイレクト・マーケティングが４%、インターネットが３%であった。苦情の理由としては、アクセス権関連(47%)、データの正確性(13%)、個人データの提供(９%)、迷惑勧誘電話(リアルタイムが５%、自動が３%)、安全性(５%)、電子メール(４%)、ファックス(２%)、SNS(２%)等となっている。

処理内容は、助言及び指針の提供が 40%、違反の可能性が高いと評価したものが 30%、評価基準に適合しないと判断したものが 17%、違反の可能性は低いと評価したものは８%、その他が５%である。

処理に要する時間は、30 日以内が 60%、90 日以内が 85%、180 日以内が 97%であり、ほぼ目標に達している。

情報コミッショナーの権限の１つとして、執行通知の送達が認められている。しかし、ICO は、違反行為を認めても、まずは、電話、手紙、会合の実施といった手段によって、デー

タ管理者に対して改善を求めており、データ管理者は、これらの緩やかな手段によって、対応することが多い。執行通知は、法律上の権限の１つとして認められているものの、これらの手段によっても改善が認められない場合に、最後の手段として行使される。したがって、年間に発せられる執行通知の件数は、多くて５件程度である。また、執行通知の前に、準備的執行通知が発せられることもある。2006/2007 年次報告書によれば、ICO は、2006 年 12 月５日、同意なく勧誘電話をかけていた５社に対して、執行通知を発したとのことである。2007/2008 年次報告書では９件の執行通知が発せられた。なお、執行通知に不服のある管理者は、審判所へ申し立てる権利を持つ。不服を申し立ててから実際に審問が行われるまでに、２ヶ月程度を要するようである。執行上時間がかかるという点は課題とされている。

1998 年データ保護法の有罪認定件数(犯罪数で計算)は、1998-1999 年が 55 件、1999-2000 年が 130 件、2000-2001 年が 21 件、2001-2002 年が 33 件、2002-2003 年が 80 件、2003-2004 年が 45 件、2004-2005 年が 55 件、2005-2006 年が 31 件、2006-2007 年が 53 件、2007-2008 年が 103 件となっている。平均すると約 50 件程度である。被告人の数は 10 人から数十人程度だが、１人が多くの違反行為を犯している場合には、有罪認定件数も増加する。

2007/2008 年次報告書によると、2007 年４月１日から 2008 年３月 31 日までの間で、11 名の者に対して訴追を行い、103 件の有罪認定が下された。この年の報告書では、そのうち、ピーター・グリーンハル(Peter Greenhalgh)というソリシタが、通知義務違反で罰金を受けたことや、インフォファインド(Infofind)という私立探偵会社が、職員を語って雇用年金局から情報を引き出し、多くの人の現住所を聞きだして、金融機関への延滞者の追跡に使ったという事例で、44 件の違反行為を犯し、罰金を受けたことなどが取り上げられている。また、違反行為は、概ね、未通知による保有・取扱い(17 条)や、個人データの不法な取得(55 条)等で占められている。

②具体的ケース

未無登録による取扱いや個人データの不法な取得等のほかに、イギリスでは、アクセス権関連の訴訟の中でデータ保護法の解釈が示され、議論を呼んだ。

・ドュラント対金融サービス局事件(Durant v. the Financial Services Authority)[26]
2003 年 12 月８日、控訴院民事部判決。
・ジョンソン対医療防衛連合事件(Johnson v. Medical Defence Union Ltd.)[27]
2004 年２月　高等法院大法官部判決。
・スミス対ロイヅ Tsb 銀行事件(Smith v. Lloyds Tsb Bank plc)[28]
2005 年２月 23 日、高等法院大法官部判決。

ドュラント事件は、控訴院が「個人データ」や「関連するファイリングシステム」の解釈を示した点で注目を集めた。

マイケル・ジョン・デュラント(Michael John Durant)は、データ保護法７条に基づき、FSA に対し、バークレーズ銀行から取得した書類の開示を求めた。FSA は、控訴人の要求に応じてある種の情報を開示したが、控訴人は、より多くの情報の開示を求めた。

エドモントン・カウンティ裁判所(Edmonton County Court)は、2002 年 10 月 24 日、デュラントの訴えを退けた。その控訴審判決が本件であり、控訴院民事部は、2003 年 12 月８日、全員一致でドュラントの控訴を棄却した。

判断の概要は次のとおりである。

ア)「個人データ」とは何か。

７条の目的は、データ主体において、データ管理者の当該取扱いが違法にそのプライバシーを侵害しているか否かを確認できるようにすることである。「個人データ」への該当性は、個人識別性ではなく、個人に「関する」か否かによる。そして、それは「個人の私生活又は家族生活、ビジネス又は専門職業的資格であるか否かを問わず、「個人の」プライバシーに影響を与える情報である」場合に該当する。その際の考慮事項としては、次の２点が挙げられる。

第１は、重要な意味において、その情報が個人の経歴に関するものであるか否かである。すなわち、何ら私的な意味を持たない事柄又は出来事、その人物のプライバシーが損なわれたと言い得ないものに関する人生の出来事を越えて、データ主体と推定される人物に関する記録がなされることである。

第２は、争点の１つである。当該情報について、その人物が関与したかもしれない他の者、又は、その人物が加わり又は関与したかもしれない何かしらの取引若しくは出来事－例えば、本件では、他の何らかの個人若しくは団体の行動の調査で、その人物が行ったかもしれないものーよりもむしろ､データ主体と推定される人物を中心に捉えるべきである。本件の事情に鑑みて、ドュラントが開示を求めた情報は、法が意味するところの「個人データ」ではない。

イ)「関連するファイリングシステム」とは何か。

次に掲げるものに限定される。

・７条に基づく個人の請求に関する個人データを意味し得る特定情報が、そのシステム内に保持されているか否か、また、もしそうである場合、その中にファイルが保持されているか否かについて、調査の最初で明示的に特定するという方法で、システムの一部を形成するファイルが構成され又は参照されること、及び、
・システムが、それ自身の構造又は参照する仕組みの一部として、個人のファイルの中に、

申立人に関する特定の基準又は情報が容易に示され得るか否か、またその場所を、容易に特定するに足る精緻かつ詳細な方法を持つこと。

本件で問題となったファイルはこれらの要件を満たさない。

この判決に対して、イギリスでは、“控訴裁判所の解釈は狭すぎる”という評釈が目立つようである。これは、データ保護法よりも狭い解釈であり、EU データ保護指令に基づく個人データの定義から外れるような場合があるとのことである。そうであるならば、イギリスの 1998 年データ保護法は EU データ保護指令に違反することにもなる。

ICO は、2003 年及び 2004 年の年次報告書でこの判決を取り上げており、裁判所の判断を狭いと評価した。特に、控訴院判決については、裁判所が、個人識別性ではなく、個人に「関する」点に焦点を当てたことに着目している。

また、ICO は、「『ドュラント』事件と 1998 年データ保護法の解釈に対するその影響」(The 'Durant' Case and its impact on the interpretation of the Data Protection Act 1998)と題するコメントを出している[29]。

最近のケースとしては、2007 年 11 月に、英国歳入関税局(Her Majesty's Revenue and Customs)から 2 枚のコンピュータディスクが紛失し、児童手当の対象となる 16 歳以下の子ども及びその家族に関する 2500 万人分について、氏名、住所、生年月日、銀行口座の詳細を含む個人情報の漏えいする事件が発生している[30]。

３．その他の動向

（１）新たな課題への取組

①RFID

ICO は、2006 年８月９日、「無線 IC タグに関するデータ保護技術指針」(Data Protection Technical Guidance Radio Frequency Identification)[31]を公表し、RFID 技術を用いる者に対し、データ保護法に則った対応等について記している。

具体的には、RFID 技術の利用者に対し、次のようなことを提案した。

・個人データは、できうる限り収集又は蓄積すべきではない。
・製品や読取機に RFID タグが存在する旨を通知し、その意味を説明しなければならない。消費者に対しては、収集される個人情報の内容、収集者、収集目的を伝えなければならない。場合によっては、消費者に対して、商品の購入後にタグを無効化又は取り外す方法を伝えることも必要である。また、個人に対し、タグのシリアル番号が個人情報と結びつき、個人データになることを伝えなければならない。
・RFID の展開に当たって、予測不可能な目的による利用(function creep)に注意すべきである。
・個人データの正確性及び最新性を確実にし、システムの目的にとって必要でない個人情報は収集されるべきではない。
・個人情報は、特定された目的に必要な期間を超えて保持されるべきではない。
・無権限アクセスを防止し、情報の安全性を確実にしなければならない。セキュリティの確保は、RFID をめぐるデータ保護の問題の中で、とりわけ重視されている。

その他、ICO は、オイスターカード(Oyster Card)によって人々の移動を追跡できること、RFID の装着を義務づけられた従業者の行動を監視できること、消費者の購買履歴を収集蓄積し、分析できることなどを指摘し、技術的な解決策を推奨している。

②バイオメトリクス

イギリスでは、2006 年３月 30 日、ID カード法(Identity Cards Act 2006)[32]が成立した。これは第１段階の法律であって、その目的は、不法移民、不法就労、組織犯罪、テロリズム、身元詐称、例えば不法移民が公共サービスを詐欺的に利用することを防止し、人々の身元を認証するより信頼できる手段を確実にすることにある。

具体的には、イギリスに３ヶ月以上在住する 16 歳以上の者(外国人を含む)を対象に、顔、

虹彩、指紋といった生体情報(biometrics data)を搭載した個人情報のデータベース「国民識別登録簿」(National Identity Register, NIR)を設置し、あわせて、かかる情報を搭載したID カードを発行するための法的枠組みを定めている。この法律には、国家 ID 事業コミッショナー(National Identity Scheme Commissioner)の制度が設けられており、登録の審査を行うことを職務とする。コミッショナーは、主務大臣により任命される。また、同法に基づく規則や命令が 10 件以上提案されており、多くは 2009 年秋の実施を予定している。

2008 年 11 月には、外国人向け ID カードの発行が開始された。2009 年には、イギリス国民向けの ID カードの発行が予定されている。

2008 年 11 月 24 日、内務省(Home Office)の身分及び旅券サービス局(Identity and Passport Service)(2006 年 ID カード法の執行機関)が諮問文書を公表した。第２段階の立法では、ID カードを発行するための詳細な手続の制定権限を政府に付与し、手数料や ID カードに搭載する情報等を新規立法の制定なくして可能とするための手続を定めることとしている。

ID カードの最終的な制度の完成は 2013 年を予定している。

ICO は、以前から、身分カードが１枚に集約されることや国家 ID 登録簿の設置に対する懸念を表明しており、2006 年 ID カード法は、その懸念に配慮した形で制定されたと評価しつつも、政府が収集・保有する情報の範囲及びその取扱いにはなお注意を払っている。具体的には、カード情報を確認することを通じてデータの追跡が可能となり、私生活の詳細を集積できることや、政府が国家ID登録簿を国民情報プロジェクト(Citizens Information Project)(中央及び地方政府が国民の情報を共有し、公的資金の節約や公的サービスの向上を図るプロジェクト)に流用しようとしているように、データベースに搭載された情報が予想外に利用される危険性の存在することなどを指摘している[33]。

③ゲノム

ア)国家 DNA データベース[34]

内務省は、国家 DNA データベース(National DNA Database)を所管している。

国家 DNA データベースは、犯行現場や拘禁中の人物から採取した DNA サンプルの情報を保管する世界最大規模のデータベースである。データベースは、過去５年の間に顕著な拡大傾向を示しており、2005 年末で 340 万人であった登録者数は、2007 年６月時点で約 400 万人、全人口の約５％を占める。プライバシーとの関係で、内務省は、侵害行為により得られる利益と比較衡量すべきだという立場に立ち、2005 年から 2006 年にかけて、殺人・過失致死や強姦罪を含む４万 5000 件の犯罪行為が、DNA データベースの記録と適合したこと等を述べている。一方、ジーン・ウォッチ(Gene Watch)(後掲３.(２)①ウ)は、このデータベースについて、犯罪捜査目的にとどまらず、犯罪予防の目的でも利用されており、目的外利用や不正利用の問題が深刻であると指摘している。

1984 年警察及び犯罪証拠法(Police and Criminal Evidence Act 1984, PACE)[35]は、警察当局における指紋及び細胞の強制的な採取を認める(指紋については 61 条、細胞については 63 条)。

また、PACE64 条(３)項は、嫌疑の晴れた人物については、DNA サンプル及び指紋を破棄しなければならない旨を定めていたが、2001 年刑事司法及び警察法(Criminal Justice and Police Act 2001)[36]82 条(４)項は、その規定を廃し、当該犯罪捜査の目的を達成した後にも指紋及び細胞を保存できることとした。

2003 年刑事司法法(Criminal Justice Act 2003)[37] 9 条及び 10 条は、さらに PACE を改正し、警察が、記録化され得る犯罪を犯して警察署に身柄を拘束されている人物から DNA 及び指紋を同意なくして得られる規定を設けた。

なお、指紋や DNA のデータベース保存に関しては、「2006 年警察全国コンピュータにおける微細な記録の保存指針」(Retention Guidelines for Nominal Records on the Police National Computer 2006)[38]が作成されている。

一方、国家 DNA データベースをめぐっては、S 及びマーパー対イギリス政府事件(*S. and Marper v. the United Kingdom*)[39]において、ヨーロッパ人権裁判所が注目すべき判決を下した。

２名のイギリス人(S 及びマーパー)が犯罪の嫌疑を受け、警察によって指紋及び細胞のサンプルを採取されたが、その後 S は無罪判決を受け、マーパーは和解して訴訟を終了させた。しかし、警察当局は、国家 DNA データベースの中に、S 及びマーパーの指紋、細胞のサンプル、DNA 分析データを保持し続けたため、両者は、国内の裁判所に司法審査を申し立てた。イギリス国内の裁判所は、その主張を認めなかった。そこで、両者は、ヨーロッパ人権裁判所に対して不服申立てを行い、警察当局の保存行為はヨーロッパ人権条約８条(私生活及び家庭生活を尊重される権利)及び 14 条(差別の禁止)に違反すると主張した。同裁判所は、2008 年 12 月４日、８条違反を認める判決を下している。

イ)バイオバンク計画[40]

イギリスでは、バイオバンク計画が推進されている。

バイオバンクは、独立(in its own right)の登録慈善団体であり、大規模な医学調査活動を行っている。

バイオバンク計画は、1998 年に立ち上げられたプロジェクトであり、医学研究会議(Medical Research Council)、ウェルカム・トラスト(Wellcome Trust)、保健省(Department of Health)等から支援を受け、6100 万ポンドの資金をもとに進められている。この計画は、45 歳から 69 歳までのイギリス国民男女の最大 50 万人を対象に、血液・尿その他の生体試料、病歴、生活習慣情報を含む環境情報を収集し、最低 10 年は経過を観察し、健康上の変化を追跡するものである。これらの各要因が、人生後半における、ガン、心臓病、糖尿病、関節炎、さまざまな形の認知症を含む、深刻かつ生命の危険のある広範な病気の発生に対して、ど

のように影響しあうかに関する原因究明を行うことを目的とする。

バイオバンク計画は、特定の病気に罹患する遺伝情報領域を調べ、予防、診断、治療につなげられると考えられている。こうした医療を実現するためには、膨大な量の遺伝情報・病歴情報・生活習慣情報を収集し、構築されたデータベースを利用して研究を進める必要性がある。

一方で、DNA 情報の活用・漏えいに関する疑問のみならず、もろもろの点で批判があるにもかかわらず、強行されているという批判も存在する。ジーン・ウォッチは、プロジェクトと病気への罹患との関連が十分に実証されていないことを批判している。その他、科学的根拠がきちんと示される前に予算がついたことなどが指摘されている[41]。

④監視カメラ[42]

イギリスは、監視カメラ先進国として有名であり、CCTV(Closed-circuit Television)の設置台数は、イギリス全土で 400 万台を超える。イギリス人 1 人あたりに換算すると、14 人につき 1 台の CCTV が設置され、ロンドンに住めば 1 日に 300 回もカメラに撮られると言われている。内務省は、防犯予算の約 8 割を CCTV に費やしているとのことである。

CCTV は、主に警察が犯罪防止目的で利用しており、街中や公共交通機関等に設置されている。ドメスティック・バイオレンスや児童虐待の証拠をつかむために、自宅内に設置されることもある。民間においても、商店、職場、学校などで用いられている。国民は、一般的には CCTV の設置に理解を示しているとのことだが、犯罪防止目的以外の設置・利用については議論がある。また、CCTV が犯罪率を減少させたとの統計もあるが、信頼性が低いとの批判も存在する。

情報コミッショナーは、監視カメラによって、一般の人々の日常生活が侵害的方法で監視下に置かれることになり、データ保護及びプライバシーの問題を増大させていることを懸念している。そこで、CCTV を用いる事業者を対象として、2000 年に、監視カメラ実務規範を策定し、データ保護法を遵守するための条件を明らかにしている。その後、2008 年には改訂版を公表した。

実務規範では、CCTV の設置を人々に周知すること、鮮明な映像で撮影すること、システム運営の責任者を置くこと、CCTV システムの画像のセキュリティを確保し、アクセス制限をかけること、映像の保存は目的達成に必要な期間にとどめること、録音機能付 CCTV は犯罪捜査目的等の例外的な場合にのみ認めることなどが記されている。

⑤公共の安全（テロリズム）への対応

イギリスでは、2005 年のロンドン地下鉄爆破テロによる被害を受けたことなどから、テロ対策を重視している。その方法としては、CCTV やバイオメトリクス技術の利用が有効

であると考えられている(詳細は前掲３.(１)参照)。

（２）プライバシー保護団体や世論の動向について

①プライバシー保護団体の動向や見解

ア)リバティ(Liberty)[43]

リバティは、市民的自由のための全国協会(National Council for Civil Liberties)といい、1934 年に設立された組織である。超党派、非党派の会員で構成される。この組織は、キャンペーン、テストケース訴訟、議会のロビー活動、政策分析、助言と情報を無料で提供することなどを通じて、市民的自由及び人権に関する指導的な活動を行っている。
2008 年は、DNA サンプルのデータベース保存、ID カード計画などへの意見表明を行っている。

また、リバティは、2008 年８月、司法省の諮問を受け、ICO の善良な実務、コンプライアンスの確保、資金調達に関し、次のような答申を公表した。

・51 条(７)項は、善良な実務に照らして個人データの取扱いを評価する際に、データ管理者の同意を要件としている。善良な実務の評価は、データ管理者に利点をもたらす場合も多いが、管理者に同意を勧めることが問題になり得る。そこで、データ管理者が登録時に同意できるようにするとともに、同意撤回に３ヶ月の周知期間を設ける制度を認める。それによって、評価が差し迫ったところで同意を撤回する問題を回避できる。あわせて、評価に同意した者に対して、罰金を科さないように強い推定を置くことで、より極端な悪しき実務に対して ICO が処罰できる余地を許容しつつ、データ管理者が同意するインセンティブも維持する。
・43 条の情報提出通知において、重要事項のみならず、時間及び場所のような情報提出の態様も含める。例えば、通常の業務時間内、データ管理者が適切にアクセスできる場所などを示した網羅的でないリストを示すのも適切である。
・附則９の立入調査権限を強化し、①無作為抽出による検査を行う際にも、令状発布を認める、②証拠ではなくリスク評価に基づき違反を疑った場合においても、情報コミッショナーは令状申請にあたって根拠を持つべきである、③立入調査の際に、捜索、調査、差押えを行う附則９の権限を拡大すべきであり、また、データアクセス取得時のスタッフ支援を要求する権限、手続、データ入手先、データ提供先などに関する情報提供を求める権限も認めるべきである。

イ)プライバシー・インターナショナル(Privacy International, PI)[44]

PI は、1990 年創設の人権擁護団体で、政府や企業による監視行為及びプライバシー侵害に対する反対活動等を行っている。本部はイギリスのロンドンにあり、アメリカのワシントン DC にも事務所が置かれている。プライバシー及びデータ保護との関連では、ID カード、国境及び渡航の監視(ヒースロー空港で行われていた指紋認証)、通信の監視(データマイニング等)、DNA 及び遺伝情報の取扱い等の問題に関心を寄せている。

PI は、データ保護及びプライバシー法に関しては、EU データ保護指令を実現する法律、外国や企業による同指令の遵守、及び、国際的なデータ移転にも注目している。また、PI は、欧州の市民のために、十分な保護レベルに達しない国に情報を移転することで、欧州のプライバシー原則に違反する企業を相手取り、訴訟を遂行する方針を取っている。あわせて、世界各地のプライバシー規制の発展も調査している。

最近の具体的な活動としては、ヒースロー空港の指紋採取に異議を唱えたケースが存在する。PI は、ヒースロー空港が、指紋採取を 2008 年 3 月 27 日から開始するという方針を打ち出したことに対し、同年 3 月 9 日、情報コミッショナーに対し、「(指紋採取)計画は、イギリスのデータ保護法に基づく必要性と均衡性の基本的基準に違反している」との苦情を申し立てた。情報コミッショナーは、苦情が処理されるまで、「抗議しながら」指紋押捺を受け入れるよう乗客に助言した。結局、イギリス空港運営会社の British Airport Authority (BAA)は、3 月 26 日、ヒースロー空港ターミナルの指紋採取計画を棚上げすると発表している。

また、PI は、「世界の監視社会マップ」(Map of Surveillance Societies around the world)を公表している(2007 年 12 月 28 日現在)。これは、プライバシー保護体制を基準に地図を色分けしたものであり、それぞれは、青：一貫して人権基準を維持、濃緑：重要な保護及び予防手段を講じている、薄緑：濫用に対する適切な予防手段を講じている、黄：多少の予防手段を講じているが、保護は弱い、赤：予防手段を維持する上で、制度的欠陥(systemic failure)がある、桃：広範な監視社会、黒：地域特有の監視社会となっている。イギリス、アメリカ、ロシア、中国は黒、カナダは黄、オーストラリア、ニュージーランド、日本は赤と評価されている。最も高い評価はギリシャの薄緑である。

さらに、PI は、海外の動きにも着目している。最近では、カナダのトロント市交通委員会(Toronto Transit Commission, TTC)が、2007 年に、1,800 万ドルをかけて、バス、路面電車、地下鉄に 1,2000 台のカメラを設置する計画を打ち出したことに対し、カナダの情報コミッショナーに異議を述べたケースが存在する。

ウ)ジーン・ウォッチ[45]

ジーン・ウォッチは、遺伝子技術をめぐる諸問題に対して様々な問題提起を行う非営利団体である。具体的には、イギリス警察による国家 DNA データベースの問題、遺伝情報の利用とマーケティングの問題、遺伝子組み換え技術による植物の栽培等を取り扱っている。

前記ア)からウ)のいずれの組織においても、S 及びマーパー対イギリス事件を取り上げ、

好意的な見解を表明している。PI は、この事件に訴訟参加している。

②プライバシー関連諸問題についての世論の動向

最近の調査結果によると、次のような結果が明らかとなった。

You Gov 社及びデイリー・テレグラフ社は、2006 年 11 月、約 2,000 人を対象に、監視社会に対する調査を行った[46]。いくつかの結果を紹介すると、次のとおりである。

1　イギリスが「監視社会」と表現されることは正しいか。
正しい。　79%
正しくない。　16%
知らない。　5％
2　データベースの正確性及び信頼性
完全に正確で信頼できる。　2％
大部分は正確で信頼できる。　41%
相当部分が不正確であり、信頼できない。　37%
大部分が不正確であり、信頼できない。　11%
知らない。　9％
3　すべての政府機関がデータベース上の情報に関する秘密を守っていると信じているか。
信じている。　11%
信じていない。　66%
分からない。　23%
4　詳細な個人情報が国家データベースに記録されることをどう思うか。
非常に満足している。　6％
かなり満足している。　35%
かなり不満だ。　25%
非常に不満だ。　27%
知らない。　7％
5　ID カードの導入への賛否。
賛成　50%
反対　39%
知らない。　11%
6　ID カードのチップを用いて個人を追跡することの可否。
賛成　16%
反対　70%
どちらでもない。　14%

7　監視カメラによって、自分が偵察されていると感じるか。

よく感じる。　11%

時々感じる。　26%

めったに感じない。　35%

全く感じない。　27%

知らない。　１%

調査会社であるICMは、2006年８月から９月にかけて、約1,000人を対象に、IDカード法に対する世論調査を行った。この時点では、50%が「賛成」、49%が「反対」、１%が「制度を知らない」という結果であった[47]。その後、2008年２月に、同じく約1,000人を対象に行った調査によれば、IDカード計画を「非常に悪い構想」だと考える人が25%(2007年９月の17%から上昇)、「非常によい構想」であると考える人が12%、過半数を占める52%の人々は、１つの政府機関が保管していた情報を他の機関と共有することを快く思わないという評価を下している[48]。反対者が増えた背景には、2007年11月に英国歳入関税局から2,500万人分の個人情報が漏えいした事件の影響があると見られている(前掲２.(３)②)。

---

1 Data Protection Act 1998, c 29.

2 Council Directive 95/46, 1995 O.J. (L 281) 0031-0050 (EC).

3 情報コミッショナーの年次報告書については、ICO のホームページから見ることができる(http://www.ico.gov.uk/about_us/what_we_do/corporate_information/annual_reports.aspx)。

4 http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/pinfo-framework.pdf.

5 http://www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspx.

6 http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/employment_practices_code.pdf.

7 Information Commissioner, *Annual Report* (2004) p. 31. ビシャード審問については、以下のウェブ・サイト(http://www.bichardinquiry.org.uk/)参照。

8 石井夏生利『個人情報保護法の理念と現代的課題－プライバシー権の歴史と国際的視点』(頸草書房、2008年)404頁以下。

9 Fair Employment (NI)Act 1989, c 32.

10 *Campbell v. MGN Ltd.* [2004] UKHL 22.
キャンベル事件、ダグラス事件についての解説は、ジョン・ミドルトン「イギリスの1998年人権法とプライバシーの保護」一橋法学第４巻第２号(2005年)37頁以下。

11 *Douglas v. Hello !* [2005] EWCA Civ 595, [2005] 2 F.C.R. 487.

12 Representation of the People Act 2000, c 2.

13 Access to Health Record Act 1990, c 23.

14 Criminal Justice Act 1991, c 53.

15 Criminal Justice and Public Order Act 1994, c 33.

16 http://www.ico.gov.uk/upload/documents/library/data_protection/introductory/data_protection_myths_and_realities.pdf.

17 Freedom of Information Act 2000, c 36.

[18] Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003 No. 2426).
[19] Environmental Information Regulations 2004 (S.I. 2004 No. 3391).
[20] 各報告書については、以下のウェブ・サイト(http://www.ico.gov.uk/about_us/news_and_views/current_topics/what_price_privacy_now.aspx)参照。
[21] Criminal Justice and Immigration Act 2008, c 4.
[22] Financial Services and Markets Act 2000, c 8.
[23] Communications Act 2003, c 21.
[24] Competition Act 1998, c 41.
[25] Consumer Credit Act 1974, c 39.
[26] *Durant v. Financial Services Authority* [2003] EWCA Civ 1746.
[27] *Johnson v. Medical Defence Union Ltd.* [2004] EWHC 2509 (Ch).
[28] *Smith v. Lloyds Tsb Bank plc* [2005] EWHC 246 (Ch).
[29] 指針については、以下のウェブ・サイト(http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf)参照。
[30] 以下のウェブ・サイト(http://www.guardian.co.uk/politics/2007/nov/21/immigrationpolicy.economy3)等を参照。
[31] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/radio_frequency_indentification_tech_guidance.pdf.
[32] Identity Cards Act 2006, c 15. ID カード計画については、内務省のウェブ・サイト(http://www.homeoffice.gov.uk/passports-and-immigration/id-cards/)のほか、岡久慶「2006年 ID カード法－国民情報の総合管理」外国の立法 229 号(2006 年)158 頁以下等。
[33] http://www.ico.gov.uk/about_us/news_and_views/current_topics/identity_cards.aspx.
[34] http://www.homeoffice.gov.uk/science-research/using-science/DNA-database/.
[35] Police and Criminal Evidence Act 1984, c 60.
[36] Criminal Justice and Police Act 2001, c 16.
[37] Criminal Justice Act 2003, c 44.
[38] http://www.acpo.police.uk/asp/policies/Data/Retention%20of%20Records06.pdf.
[39] *S. and Marper v. the United Kingdom* [2008] ECHR 1581.
[40] http://www.ukbiobank.ac.uk/.
[41] http://www.guardian.co.uk/science/2006/feb/23/health.society.
[42] 寺西香澄「英国における CCTV 等の取扱い及びオランダにおけるマネー・ロンダリング対策」立法と調査 282 号(2008 年) 3 頁以下、青柳武彦『情報化時代のプライバシー研究－「個の尊厳」と「公共性」の調和に向けて－』(NTT 出版、2008 年)263 頁以下のほか、後述するプライバシー・インターナショナルのホームページも情報を掲載している。
[43] http://www.liberty-human-rights.org.uk/.
[44] http://www.privacyinternational.org/.
[45] http://www.genewatch.org/.
[46] http://www.yougov.com/archives/pdf/TEL060101024_3.pdf.
[47] http://www.icmresearch.co.uk/pdfs/2006_november_no2id_id_card_survey.pdf#search="ID card".
[48] http://www.guardian.co.uk/uk/2008/feb/06/politics.idcards.

ⅱ　フランス

１．個人情報保護法制について

（１）個人情報保護制度の概要

個人情報保護に関する一般法は、情報処理、情報ファイル及び自由に関する 1978 年１月６日の法律第 78-17 号（以下、「1978 年法」とする）である。同法は、2004 年８月６日の法律第 2004-801 号で大きく改正された。この改正は、1995 年の EU データ保護指令に対応するための改正を多数含むものであった[1]。以下、引用条文は、特に断らない限り、1978 年法のそれである。また、2004 年改正以前の同法については、旧法と称することがある。

①目的

1978 年法第１条は、同法の目的を、以下のように定める。

> 情報処理は、市民のそれぞれに奉仕するものでなければならない。その促進は、国際協力の枠内で行われなければならない。情報処理が、人間のアイデンティティや人権、私生活、さらには、個人的又は公的な自由を侵害するものであってはならない。

②適用範囲

1978年法は、個人情報について、「自然人に関するあらゆる情報のうち、識別番号(numéro d'identification ）又は個人に固有の一若しくは複数の要素を参照することで、直接又は間接に個人を識別し又は識別可能なもの」と定義したうえで（２条）、個人情報処理責任者(responsable d'un traitement de données à caractère personnel)がフランス領内に在住しているか、あるいは、フランス領内に設置された処理手段を用いている場合であって（５条）[2]、かつ、以下のいずれかの処理のうち、専ら個人的行為を行うことを目的とする処理を除いたものを、同法の適用範囲とする（２条）[3]。なお、公的機関か否かによる区別はない。

ⅰ）個人情報(données à caractère personnel)の自動処理(traitements automatisés)
ⅱ）情報ファイルに記載されているか、記載を予定されている個人情報の非自動処理(traitements non automatisés)

「個人情報処理責任者」とは、処理の目的と方法を決定する個人、あるいは、公的な機

関又は部局若しくは組織を意味する。ただし、法令の規定が、個人情報処理責任者を明らかしている場合は、その定めに従う（第３条Ⅰ）。

「個人情報処理」とは、個人情報に対して行われる一つのあるいは一連の作業を意味し、その手段を問わない。個人情報についてなされる作業(opération)について 1978 年法第２条は、収集(collecte)、記録(enregistrement)、編集(organisation)、蓄積(conservation)、修正(adaptation) 又は変更(modification) 、復旧(extraction)、参照(consultation)、利用(utilisation)、移転(transmission)や周知(diffusion)その他のあらゆる形態の開示(communication)、結合(rapprochement) や相互接続(interconnexion)、利用停止(verrouillage)、消去(effacement)、削除(destruction) と定める（２条）[4]。この規定は、EU データ保護指令２条(b)に対応するため、旧法よりも「個人情報処理」の範囲を拡張する方向で、2004 年に改正された。

③適用除外

ア)インターネットプロバイダーがプロキシサーバにアクセスした際に生じる一次的情報のコピー等は、本法の適用を除外される（４条）[5]。これは、インターネット上の特殊性、とりわけ、キャッシュに伴う問題に配慮したもので、2000 年６月８日「情報社会における諸役務及び電子商取引に関する EU 指令 2000-31 号（電子商取引指令)」第 13 条に対応するため、2004 年法改正で制度化された[6]。

イ)専ら医療研究のための自動処理は、情報処理・自由全国委員会(Commission nationale de l'informatique et des libertés: 以下、「CNIL」とする)への事前届出や、CNIL による許可（後述 97 頁参照)、及び、収集時の本人通知（後述 87 頁参照)、本人による処理拒否（後述 86 頁参照）に関する制度の適用を除外される（53 条)。

④内容

ア)収集・処理

（１）以下の原則の遵守が求められる（６条)。

ⅰ)公正かつ適法な収集・処理

ⅱ)収集の目的が、特定され、明白であり、かつ、正当なもので、この目的と相容れない手法での収集後処理がされないこと[7]。なお、処理目的は、CNIL への届出や許可申請、意見申請の際に明記されなければならない（後述 97 頁参照)。

ⅲ)収集目的と事後利用目的に照らし、情報が適切かつ妥当で、過剰なものではないこと。

ⅳ)情報が正確かつ完全であり、必要に応じて最新なものであること。収集又は処理の

目的に照らし、不正確あるいは不完全な情報が消去又は訂正されるよう、適切な措置がとられること。

ⅴ)情報が、収集又は処理の目的に照らし、必要な期間を超えない期間、当該個人の識別が可能な形で保存されること。

旧法は、詐欺的又は背信的な収集、あるいは、違法手段を用いた収集を禁止し、被収集者は、一定の場合に収集を拒否できるとしていたに過ぎなかったが、EU データ保護指令 6 条に対応するため、2004 年法改正で上記のように改正された。

（2）センシティブ情報の収集については、後述 90 頁参照。

（3）犯罪、有罪判決及び保安処分に関する個人情報の処理は、以下の場合に限り、許される（9 条)。

ⅰ)司法補助者(auxiliaire de justice)[8]が法律の定める任務を遂行するに当たってする必要最小限の処理。

ⅱ)知的財産法典 L321-1 条及び L331-1 条の定める法人が、自ら管理する権利の資格者として実施する処理。又は、同法典第Ⅰ、Ⅱ及びⅢ部Ⅱが定める権利の防御を確保するため、あるいは、当該権利を侵害された被害者のために実施する処理。

ⅲ) 裁判所、公的機関、及び、公役務を管理する法人が、その法的権限内において実施する場合。

（4）個人情報を処理する場合は、本人の同意を得るのが原則とされる。ただし、それ以外にも、以下の要件の一を満たしていれば、処理が許される（7 条)。

ⅰ)処理責任者に課せられる法的義務が遵守されていること。

ⅱ)本人の生命を保護する目的であること。

ⅲ)処理責任者又は個人情報の取得者(destinataire)[9]が担当する公役務の任務を遂行するためのものであること。

ⅳ)本人が当事者である契約の締結や、本人の要求に基づく契約前措置の遂行のためであること。

ⅴ)処理責任者や取得者が追求する正当な利益の実現に資するもので、本人の利益や基本的権利自由を害さないものであること。

旧法は、センシティブ情報の収集（後述 90 頁参照）を除き、本人同意を収集要件としてはいなかったが、EU データ保護指令 7 条に対応するため、2004 年法改正で上記の原則が盛り込まれた。ただし、EU データ保護指令 2 条(h)が「データ主体の同意」を定義し、また、同 7 条(a)が、「明確に」同意することを条件とするのに対し、本法は、

同意を定義しておらず、かつ、同意の明確さを問わない点で、EU データ保護指令よりも詳細さを欠くとの評価がある[10]。

（5）個人情報処理責任者又はその代表者は、本人から直接的に情報を収集する場合、収集対象者に対し、以下の事項を、事前若しくは収集時に通知しなければならない（32条Ⅰ）。

ⅰ)処理責任者又はその代表者の身元
ⅱ)処理目的
ⅲ)回答の任意性
ⅳ)回答拒否の場合の影響
ⅴ)取得者の名称又は取得者の範疇
ⅵ)アクセス権(後述 88 頁参照）などの権利
ⅶ)場合によっては、EU 域外への情報移転の可能性

・本人から直接収集する場合の通知については、旧法にも一定の規制があったが、EU データ保護指令 10 条に対応するため、2004 年法改正で、通知事項が追加された。
・電子通信網のあらゆる利用者は、処理責任者あるいはその代表者から、クッキーや接続証明の目的、及び、それらの取得を拒否しようとする場合に取り得る手段を、明確かつ完全な形で通知されなければならない（32 条Ⅱ）[11]。

以上の規制は、以下の場合に適用を除外される。

ⅰ)事前に CNIL が、本法の定めに則すことを承認した短期間の匿名化処理（32 条Ⅳ）
ⅱ)犯罪の予防や捜査、立証、起訴のための処理（32 条Ⅴ）。

（6）個人情報が当該情報の本人から直接に収集されるわけではない場合（間接収集）、当該処理の責任者あるいはその代表者は、当該情報を記録したときは、速やかに、直接収集の場合と同じ情報を当該本人に通知しなければならない。第三者への開示を予定されている場合には、遅くとも、当該情報の最初の処理の前に通知されなければならない（32 条Ⅲ）。

旧法には、間接収集の際の通知に関する規制がなかったところ、EU データ保護指令 11 条に対応するため、2004 年法改正で上記の規制が導入された。

イ)安全保護管理義務

個人情報処理責任者は、個人情報の安全を確保するため、とりわけ歪曲、破損、又は、無許可の第三者アクセスを排除するため、あらゆる有効な予防措置を講じなければならな

い（34 条）。

ウ)本人アクセス権

すべての自然人は、情報処理を拒否する権利（前述 86 頁参照）の他、処理責任者への質問権、自己情報の複写請求権、自己情報の訂正・利用停止・消去請求権を認められている。

（1）質問権

何人も、自己の身元を証明した上で、個人情報処理責任者に対し、以下の事項を明らかにするための質問をする権利がある（39 条Ⅰ）。

ⅰ)自己の個人情報が、当該処理の対象となっているかどうかの確認
ⅱ)当該処理の目的や、処理される個人情報の種類、それら個人情報が開示される第三者あるいはその種類についての情報
ⅲ)必要があれば、EU 非加盟国在住の取得者に対する個人情報移転についての情報
ⅳ)自己の個人情報、及び、その取得元に関して個人情報処理責任者が保有しているすべての情報に関するアクセス可能情報の提供。
ⅴ)自己に対して法的効果を有する決定が、自己の個人情報の自動処理に依拠してなされた場合に、当該自動処理の基礎となった論理を知悉し、かつ、異議申立てを可能にするような情報。ただし、当該個人に知らされる情報は、著作権法典第Ⅰ部及び第Ⅲ部第 4 章の規定に反して著作権を侵害するものであってはならない。

なお、請求の数や反復性、体系性から、濫用請求であることが明らかであれば、処理責任者は要求を拒否できる。濫用の明白性は、処理責任者が証明しなければならない（39 条Ⅱ）。

（2）複写請求権

何人も、個人情報処理責任者に対し、自己の個人情報の複写を求めることができる。複写拒否事由は列挙されていないが、請求の数や反復性、体系性から、濫用請求であることが明らかであれば、処理責任者は要求を拒否できる(39 条Ⅰ)。濫用の明白性は、処理責任者が証明しなければならない（39 条Ⅱ）。処理責任者は、実費を超えない範囲で、複写交付の費用を徴収できる（39 条Ⅰ）。

（3）質問権と複写請求権の例外

質問権と複写請求権に関する定めは、当該個人情報の保存が、請求者のプライバシーを侵害する危険が全くないことが明らかな形態で、かつ、もっぱら統計作成や学術歴史研究のために必要な期間を超えない期間においてなされた質問・複写請求には適

用されない（39 条Ⅱ）。

（４）訂正・利用停止・消去請求権

一般的な訂正・利用停止・消去請求権については、後述 92 頁参照。死者の個人情報の訂正については、後述 94 頁参照。

以上の(１)から(４)のアクセス請求が、国家の安全や国防、治安に関する個人情報処理に関してなされる場合は、処理責任者ではなく、CNIL に設置された委員会になされる。当該処理が含まれている情報を開示しても、その目的、あるいは、国家の安全や国防、治安を侵害しないものであると CNIL が認め、かつ、個人情報処理責任者が同意すれば、当該情報は請求者に開示される(41 条)。このようなアクセスは、犯罪の予防や捜査、立証、あるいは、租税調査や徴収といった任務が委託された私法人が保有する個人情報についても同様である(42 条)。

エ）監督・登録制度

CNIL による監督等の制度については、後述 96 頁以下参照。

（２）個別の検討課題

①いわゆる「過剰反応」（誤解）に対応した第三者提供制限の例外事由

第三者提供に的を絞った制度は存在しない。ただし、第三者に個人情報を提供する場合にも、収集・取扱いについての諸原則(前述 85 頁以下参照）の遵守が求められる。

なお、フランスでは、過剰反応(誤解）に相当する事案はみられないとの指摘がある[12]。

②自治会や同窓会等の取扱い

フランスでは、自治会名簿に相当する名簿は存在せず、仮にそのような名簿を作成・配布する場合でも、他の情報ファイルと同様、本人の同意が必要とされること、同窓会名簿についても、特別扱いはされていないこと、ただし、企業は同窓会名簿を販売促進のために使いたがっていること、以上のような指摘がある[13]。

③「個人情報」の定義

前述 84 頁のとおり。

④センシティブ情報に関する規定

ア)定義

人種や民族的起源、政治的、哲学的又は宗教的意見、労働組合への所属が直接又は間接的に明らかになる個人情報、あるいは、健康若しくは性生活に関する個人情報（８条Ⅰ）とされる。

なお、人種や民族的起源が明らかになる個人情報について、CNIL は、差別の発見やその内容の計測に関する学術的調査との関係で、いくつかの問題があることを指摘している（後述 108 頁以下参照）。

イ)規制内容

以下の場合を除き、収集・処理が禁止される（８条Ⅱ）。

ⅰ)本人の明示的同意がある処理

ⅱ)個人の生命を保護するために必要な処理で、当該個人が、法的無能力や物理的不能により、同意をすることができない場合

ⅲ)非営利や宗教、哲学、政治、あるいは、労働組合活動上の団体その他あらゆる組織による処理であって、

－－当該団体その他の組織の目的に則したもので、ア)の情報のみの処理であり、

－－当該団体あるいは当該組織の構成員や、これらの者の活動の範囲内でこれらの者と定期的な接触を維持している人々に関する処理であって、

－－当該本人が明示的に同意しない限り、第三者には提供されないような処理

ⅳ)当該個人によって公開されている個人情報についての処理

ⅴ)裁判における立証活動や、権利の行使あるいは防御のために必要な処理

※なお、警察や全国憲兵隊が収集した捜査情報については、STIC や JUDEX といった特別の処理システムが存在する（後述 107 頁以下参照）。

ⅵ)予防医療、医療上の診断、診療又は治療のための投薬、健康サービスの管理のために必要であり、かつ、保健衛生に関わる職業に携わる者、その他、職務の性質上、刑法典によって職業上の秘密保守義務を課された者による処理

ⅶ)統計に関する義務及び連携並びに秘密に関する 1951 年 6 月 7 日の法律第 51-711 号を遵守し、統計情報国家評議会(Conseil national de l'information statistique)の意見を経て、かつ、本法第 25 条の定める条件の下で、国立統計経済研究所(Institut national de la statistique et des études économique: INSEE)又は各省統計関係部局の一が実施する統計処理

ⅷ)医療分野における研究に必要な処理で、第９章に定める方式に従う処理

ウ)その他、以下のような例外も用意されている。

ⅰ)CNIL が本法の定めに適合すると事前に承認した、短期の匿名処理を目的とする処

理（８条Ⅲ）（後述 98 頁参照）
ⅱ)公益上の必要が認められ、かつ、CNIL が許可した処理（８条Ⅳ）（後述 98 頁参照）

エ)センシティブ情報を処理する場合は、事前に、コンセイユ・デタ（国務院）[14]の議を経るデクレ(décret en Conseil d'Etat)[15]による許可を要するところ、この許可は、CNIL の意見を経て下される。この意見は、許可と同時に公表される（26 条Ⅱ）（後述 99 頁参照)。

オ)旧法では、センシティブ情報の収集は、事前に本人による明示の同意があった場合に限って認められていたが、EU データ保護指令８条に対応するため、上記のような規制に改正された。

⑤小規模事業者の取扱い

法制度上、特に別扱いはされていない。
なお、小規模事業者による個人情報保護への対応は必ずしも十分ではない場合があること、中には、個人情報保護についてほとんど知識がない事業者もいること、小規模事業者への監督の充実が CNIL の課題の一つであること、以上のような指摘がある[16]。

⑥マス・メディアへの対応に関する規定とその内容

報道目的及び文学芸術目的での個人情報処理については、以下の制限が免除される（66 条)。

ⅰ)保存期間の制限(前述 86 頁参照）
ⅱ)センシティブ情報の収集禁止原則（前述 90 頁参照）
ⅲ)犯罪関係情報の収集禁止原則（前述 86 頁参照）
ⅳ)CNIL への事前届出・許可制度（後述 97 頁以下参照）
ⅴ)収集時の通知原則（前述 87 頁参照）
ⅵ)本人アクセス（前述 88 頁参照）
ⅶ）EU 非加盟国への個人情報移転に対する制限（後述 93 頁参照）

⑦個人情報の目的外利用の防止措置

2004 年法は、個人情報処理の適法要件の一つとして、「情報が、特定かつ明白で正当な目的で収集され、かつ、収集後にこの目的と相容れない手法では処理されていないこと」を求める。ただし、事後の処理で統計作成や学術若しくは歴史研究を目的とするものは、同法の定める手続を遵守し、かつ、当該個人に対する決定のために利用されるものでなけれ

ば、情報収集の当初の目的と整合するものとみなされる（6条②）。

また、情報が、収集又は処理目的に照らし、必要な期間を超えない期間内、当該個人の識別が可能な形で保存されていることも、個人情報処理の適法要件の一つであるところ（6条⑤）、保存期間を超えて保存されている個人情報について、目的外利用が許されるのは、以下の場合に限定される（36条）

ⅰ)歴史的、科学的あるいは統計処理上の目的による処理の場合

ⅱ)本人の明示的同意がある場合

ⅲ)CNILが許可した場合

ⅳ)センシティブ情報を、医療分野における研究目的や、公益上必要な目的で処理する場合

⑧市販の名簿の管理

法制度上、特に規制はない。通常の個人情報処理と同様の規制に服する。

⑨個人情報の取得元の開示に関する措置

法39条Ⅰ④は、「あらゆる人は、自己の個人情報の取得元に関して個人情報処理責任者が保有している情報につき、アクセス可能な情報提供を得るために、当該責任者に質問することができる」とする（前述88頁参照）

⑩個人情報の利用停止・消去に関する措置

現行法40条は、「何人も、自己の身元を証明した上で、情報処理責任者に対し、不正確、不完全、不明確、あるいは、保存期間が徒過していたり、収集や利用、提供あるいは保存が禁止されている自己の個人情報につき、状況に応じ、その訂正、修正、更新、利用停止、あるいは、消去を求めることができる」とする。

この請求を関係者が実際にした場合、処理責任者は、請求者に費用を負担させない形で、必要な処理を実施したことを証明しなければならない。

争いが生じた場合、当該情報が請求者によって提供されたものであるか、同人の同意の下に提供されたことが証明された場合を除き、証明責任は、アクセス権を行使された処理責任者の負担となる。

以上につき、前述88頁参照。

⑪国際的な情報移転に関する規定

現行法は、情報処理責任者が EU 非加盟国に個人情報を移転できる場合を、対象国が、個人情報処理に関し、プライバシーや基本的権利に対する十分な水準の保護を確保している場合に限定している（68 条)。ただし、以下の場合は、例外が認められる（69 条)。

ⅰ)本人の明示の同意があった場合
ⅱ)当該個人の生命を保護する目的の場合
ⅲ)公益の保護を目的とする場合
ⅳ)犯罪の立証や刑罰の執行、あるいは、裁判における権利擁護を目的とする場合
ⅴ)法令の規定が公衆への情報提供を定めており、かつ、あらゆる人の閲覧に供されるものとされている記録簿の適正な閲覧の場合
ⅵ)当該処理責任者と当該本人との間で締結された契約を執行する目的の場合
ⅶ)当該処理責任者と第三者の間で締結された契約の執行、あるいは、予定された契約の締結を目的とし、かつ、当該本人の利益を損なわない場合

旧法でも、国外への情報移転は、コンセイユ・デタの議を経るデクレが定めるところにより、事前の許可を要するものとされていたが（旧法 24 条)、許可条件を定めるデクレが制定されなかったため、実質的には機能していなかった[17]。2004 年改正法は、EU データ保護指令 25 条に対応するため、上記のような制度を整備した。

⑫EU データ保護指令に対する対応状況

1978 年法は 2004 年に大きく改正されたが、これは、EU データ保護指令に対応することを目的の一つとしていた。主たる改正点は、以下の通りである。

ⅰ）個人情報の定義において、個人識別可能手段のすべてについて言及すべきとした（２条）――EU データ保護指令前文（26）に対応(前述 84 頁参照)。
ⅱ）個人情報処理の範囲を拡張（２条）――EU 指令２条(b)に対応（前述 84 頁以下参照)。
ⅲ）適用対象機関の定義を明記(３条Ⅰ）――EU 指令２条(d)(e)に対応（前述 86 頁参照)。
ⅳ）取得者の定義を明記(３条Ⅱ）――EU 指令２条(g)に対応（85 頁以下参照)。
ⅴ）個人情報処理に関する諸原則を明示（６条）――EU 指令６条に対応（前述 85 頁参照)。
ⅵ）本人の同意があることを、個人情報処理実施の原則的要件とした（７条）――EU 指令７条に対応（前述 86 頁参照)。
ⅶ）センシティブ情報の収集につき、例外的に収集可能な場合を明記した（８条Ⅱ）

－－EU 指令８条に対応（前述 90 頁参照）。

viii）本人から直接に個人情報を収集する際（直接収集）における本人通知事項を追加（32 条Ⅰ）－－EU 指令 10 条に対応（前述 87 頁参照）。

ix）本人から直接に個人情報を収集するわけではない場合（間接収集）における本人通知制度を整備（32 条Ⅲ）－－EU 指令 11 条に対応（前述 87 頁参照）。

x）処理に対する事前規制が、公的部門と民間部門の場合で明確に区別されていたが、一部を共通化（22 条～29 条）－－EU 指令 18 条に対応（後述 97 頁以下参照）。

xi）EU 非加盟国への情報移転に対する規制制度を整備－－EU 指令 25 条に対応（前述 93 頁参照）。

⑬死者に関する個人情報の保護

法制度上、以下のような規制がある。

ⅰ)死亡原因を証明するために作成された情報を含め、死者に関する情報は、当該個人が、生前に書面で拒否した場合を除き、情報処理の対象となりうる（56 条）。

ⅱ)訂正請求の一環として、死者の相続人は、死者に関する情報を更新するよう情報処理責任者に請求することができる。この請求があった場合、情報処理責任者は、必要な措置をとったことを無料で請求者に証明しなければならない（40 条）。

なお、2002 年３月４日の法律４条は、死者についての医療上の秘密であっても、死者の被扶養者で相続人である者に対し、死因を知ること、あるいは、死者の名誉を守ること、相続人の権利を守ることを可能にするために必要な限り、開示されるとする。ただし、当該死者が、知らせないことについて生前に明確な意思表示をしていた場合は除かれる（公衆衛生法典 L1110-4）[18]。

⑭直接処罰等の実効性担保の措置

刑事罰と CNIL（後述 100 頁参照）による制裁がある。刑事罰については、以下のとおり。

ⅰ)CNILの職務遂行を妨害する行為;同委員会が発した文書提出命令を拒否する行為、同命令に対し虚偽情報を提出した行為は、１年の拘禁及び 1,5000 ユーロの罰金（51 条）

ⅱ）処理前に必要な届出や許可を怠った者；過失の場合を含めて、５年の拘禁及び 30 万ユーロの罰金（刑法典 L226-16 条１項）

ⅲ）CNIL による処理中断命令（後述 100 頁参照）に違反した者；５年以下の拘禁及

び 30 万ユーロ以下の罰金（刑法典 L226-16 条２項）

iv)簡易届出をした者で簡易化基準を遵守しなかった者等；５年の拘禁及び 30 万ユーロの罰金（刑法典 L226-16-1-A）

ｖ）個人識別全国名簿に登録されている個人登録番号を含んだ情報を許可なく処理する行為；５年の拘禁及び 30 万ユーロの罰金（刑法典 L226-16-1）

vi）安全確保のための有効な予防措置を講じないまま、処理を実施又は実施させる行為；５年の拘禁及び 30 万ユーロの罰金（刑法典 L226-17）

vii）詐欺的あるいは不誠実、不正な手段で個人情報を収集する行為；５年の拘禁及び 30 万ユーロの罰金（刑法典 L226-18）

viii）市場調査、とりわけ営業目的のために、本人が拒否したにもかかわらず処理を実施する等の行為；５年の拘禁及び 30 万ユーロの罰金（刑法典 L226-18-1）

ix）正当な理由に基づく拒否権行使の不遵守；５年の拘禁及び 30 万ユーロの罰金（刑法典 L226-18-1）

ｘ）センシティブ情報を明示的な本人同意がないまました処理；５年の拘禁及び 30 万ユーロの罰金（刑法典 L226-19）

ｘｉ）医学研究のための処理であって、当該本人に対し予めアクセス権等につき告知することなく、あるいは、本人や遺族が明示的に拒否しているにもかかわらずなされる行為；５年の拘禁及び 30 万ユーロの罰金（刑法典 L226-19-1）

ｘ ii）法令又は許可が定める期限を超えて情報を保存する行為で、統計処理や学術・歴史研究目的ではない行為；５年の拘禁及び 30 万ユーロの罰金（刑法典 L226-20 条）

ｘ iii）届け出られた目的とは異なる目的での利用；５年の拘禁及び 30 万ユーロの罰金（刑法典 L226-21）

ｘ iv）十分な個人情報保護制度を整備していない EU 非加盟国への情報移転；５年の拘禁及び 30 万ユーロの罰金（刑法典 L226-22－1）

ｘ ｖ）拒否リストに掲載されている個人情報を直接販売する目的で利用した場合；750 ユーロ以下の罰金（刑法典 L131－13）

２．第三者機関について

（１）第三者機関の実態

①制度の概要

ア)フランス個人情報保護法の特色は、独立行政委員会(autorité administrative indépendante)である CNIL（情報処理・自由全国委員会)[19]に、強力な規制権限を認める点にある[20]。1978 年法は、CNIL が独立行政委員会であることを明記し（11 条)、委員はその権限行使に当たり、いかなる機関の指揮も受けないと定める（21 条１項)。

イ)CNIL は、以下の委員（計 17 名）で構成される(13 条Ⅰ)。いずれも任期５年で再任が可能である（13 条Ⅱ)。委員は、委員会が認めた支障がある場合を除き、解任されない(13 条Ⅱ)。なお、2009 年２月４日に、新委員が、前任者の任期切れとともに、新たに任命されている[21]。

ⅰ）上下院議院各２名
ⅱ）経済・社会評議会(Conseil économique et social)[22]の委員２名
ⅲ）コンセイユ・デタ（国務院）の現職又は元裁判官２名
ⅳ）破毀院(Cour de cassation)[23]の現職又は元裁判官２名
ⅴ）会計院(Cour des comptes)[24]の現職又は元裁判官２名
ⅵ）有識者 15 名

その他、首相が指名する政府委員(commissaire du gouvernement)、及び、複数の政府委員補佐[25]も存在する。政府委員は、CNIL のすべての会議について、他の委員と同じ条件で招集される。出席できない場合は、政府委員補佐が代理出席する（1978 年７月 17 日のデクレ 78-774 号４条)。CNIL の説明によれば、会議における政府委員の役割は、処理の実態についての、政府や各省庁の方針を説明することにある[26]。政府委員は、制裁に関する場合を除き、第二回の審議を招集することができ、これは、第一回審議から 10 日以内に開催されなければならない(18 条)。また、各省庁には、情報処理・自由監督官(correspondant informatique et libertés)が置かれるが、政府委員は、これらの監督官と連絡を取り合うことで、1978 年法律の適用を調整する任務を担う（1999 年３月 12 日の首相通達)。
委員には秘密保守義務が課せられる(20 条)。

ウ)CNIL の具体的権限は、事前規制、義務違反行為に対する制裁、苦情処理、違法行為についての告発、調査及び物件収集、政府及び民間団体への助言等である(11 条)。さらに、

権利や自由に対する重大かつ急迫の侵害があると認める場合、委員長は、管轄裁判所に対し、仮処分手続(référé)をもって、当該権利自由の擁護に必要なあらゆる安全保護措置(mesure de sécurité)を、場合によっては罰金強制(astreinte)付で命じるよう求めることができる(45 条Ⅲ)。

(1)事前規制権限

(1)-1　対象

以下の個人情報処理は、事前規制の対象外である。

ⅰ)法令の定めによって、専ら公衆への情報提供を目的とし、かつ、公衆若しくは正当な利益を理由としたあらゆる人への閲覧に供される登録簿の管理をもっぱらの目的とする処理（22 条Ⅱ①)。

ⅱ)センシティブ情報の処理のうち、前述１④(２) ④ⅲ）に該当する処理（22 条Ⅱ②)(前述 90 頁参照)。

ⅲ)文学及び芸術目的の処理(67 条①)

ⅳ)報道活動のための処理で、職業倫理規範を尊重する範囲内でのもので(67 条②)、処理責任者が監督者を指名している場合（67 条)。

(1)-2　内容

(1)-2-1　届出

(1)-2-1-1　原則的な届出

個人情報処理のうち、許可（後述(1)-2-2、(1)-2-3 参照）を要するもの以外は、原則として、CNIL への届出の対象となる（22 条Ⅰ)。ただし、例外として、処理責任者が、本法の定める諸義務の尊重を独立に確保することを責務とする個人情報保護監督者を選任した場合は、届出義務が免除される（EU 非加盟国在住の情報取得者に個人情報を移転することが企図されている場合を除く)。監督者の選任は、CNIL に通知されなければならない[27]。

届出はオンラインでもすることができる(23 条Ⅰ)。届出を受理した CNIL は、遅滞なく受理証を交付する。届出者は、受理証を受領してから処理を実施しなければならない（23 条Ⅰ)。複数の個人情報処理であっても、同一目的で同種の個人情報を処理し、情報取得者が同一あるいは同範疇であるものは、単一の届出で構わない（統合届出(déclaration unique)。23 条Ⅱ)。

(1)-2-1-2　簡易届出(déclaration simplifiée)

ごく日常的な個人情報処理であり、かつ、その実施が、プライバシーや個人の自由に影響を与える可能性がないものは、簡易届出制度の対象となる。これは、CNIL が簡易届出の対象となる処理の種類を示す簡易化基準(normes simplifiées)

を公示し、その一に合致すると思料した処理責任者がその旨を届け出れば、処理が可能になるという制度である。いわば、CNIL による認証制度とイメージできよう。この場合も、統合届出が可能である（24 条Ⅱ）。

簡易化基準は、以下のことを明らかにする（24 条Ⅰ）。

ⅰ）簡易届出の対象となる処理の目的

ⅱ）処理される個人情報の種類

ⅲ）関係する個人の種類

ⅳ）当該個人情報の開示を受ける取得者の種類

ⅴ）個人情報の保存期間

なお、CNIL は、処理される個人情報の目的や、当該情報の取得者の種類、保存期間や関係個人の種類を考慮した上で、簡易届出を免除される処理を指定できる。

(1)-2-2　許可

以下の処理は、アレテ[27]許可又はデクレ許可(後述(1)-2-3)の対象になるものを除き、CNIL による許可を要する(25 条Ⅰ)。この場合も、統合許可が可能である(25 条Ⅱ)。

ⅰ)センシティブ情報の処理のうち、国立統計経済研究所又は各省統計関係部局の一が実施する統計処理(前述 90 頁参照）に該当する処理。自動処理か否かを問わない(25 条Ⅰ①)。

ⅱ)センシティブ情報の処理のうち、短期匿名処理の対象となるもの(8 条Ⅲ)。自動処理か否かを問わない(25 条Ⅰ①)。

ⅲ)センシティブ情報の処理のうち、公益を理由とするもの(8 条Ⅳ)。自動処理か否かを問わない(25 条Ⅰ①)。

ⅳ)遺伝情報の自動処理。ただし、医師や生物学者によってなされる処理で、予防医療、医療上の診断、診療又は治療のための投薬を目的とするものを除く(25 条Ⅰ②)。

ⅴ)自動処理か否かを問わず、犯罪や有罪判決、保安処分に関する処理。ただし司法補助者が関係個人を弁護する任務の必要に基づく場合を除く処理(25 条Ⅰ③)

ⅵ)処理の性質、範囲及び目的から、法的利益や給付の利益、契約上の利益を個人からはく奪するものではあるが、法令の規定が欠如しているような自動処理(25 条Ⅰ④)

ⅶ)以下を目的とする自動処理

――公役務を管理する一又は複数法人に属するファイルで、目的が異なる公益に係るものとの相互接続

――別法人に属するファイルであって、主たる処理目的が異なるものとの相互接続(25 条Ⅰ⑤)

viii)個人識別全国名簿における個人登録番号を記載した個人情報にかかる処理、及び、個人登録番号を含まないが同名簿への参照を必要とする処理(25 条Ⅰ⑥)
ix)個人の社会的困窮に対する評価を含む情報の自動処理(25 条Ⅰ⑦)
x)個人の調査に必要なバイオメトリクス情報を含む自動処理(25 条Ⅰ⑧)

(1)-2-3　デクレ許可やアレテ許可に関する事前意見

(1)-2-3-1　デクレ許可の場合

以下の処理は、コンセイユ・デタの議を経るデクレによる許可を要する。同デクレは、事前に CNIL の意見を経てから制定される。この意見は、理由を付して公表される。この場合も、統合許可が可能である(26 条Ⅳ、27 条Ⅲ)。

i)国によるセンシティブ情報の処理で、国家の安全や国防、治安に関わるもの、及び、犯罪予防や捜索、立証あるいは刑事訴追、刑罰や保安処分の実施を目的とするもの(26 条Ⅱ)
ii)国家、公法人、あるいは、公役務を管理する私法人による個人情報処理で、個人識別全国名簿上の個人登録番号を記載した個人情報にかかるもの(27 条Ⅰ①)
iii)国家による個人情報処理で、個人の認証や特定のための検査において必要なバイオメトリクス情報の処理にかかるもの(27 条Ⅰ②)

(1)-2-3-2　アレテ許可の場合

以下の処理は、大臣アレテによる許可を要する。同アレテは、事前に CNIL の意見を経てから制定される。この意見は、理由を付して公表される。この場合も、統合許可が可能である(26 条Ⅳ、27 条Ⅲ)。

i)国による処理で、国家の安全や国防、治安に関わるもののうち、センシティブ情報の処理を含まないもの(26 条Ⅰ①)
ii)国による処理で、犯罪予防や捜索、立証あるいは刑事訴追、刑罰や保安処分の実施を目的とするもののうち、センシティブ情報の処理を含まないもの(26 条Ⅰ②)
iii)国家や公法人による処理のうち、センシティブ情報又は犯罪情報の処理を含まず、かつ、異なる複数の公益に関連する処理やファイルの間での相互接続を生じさせないもの　(27 条Ⅱ②)
iv)国勢調査に関する処理(27 条Ⅱ③)
v)国家、公法人、あるいは、公役務を管理する私法人による個人情報処理で、電子行政の電気通信サービスの一つを行政利用者(usagers de l'administratinon)（市民）に利用させるためのものであって、かつ、個人識別全国名簿上の個人登録番号か、自然人を他のものから識別するような個人情報が記載された個人

情報の処理(27 条Ⅱ④)

(2)義務違反行為に対する制裁権限

本法の定めに反する行為は、刑事罰の対象となるほか(50 条、51 条)、以下のような CNIL による制裁の対象となる。

(2)-1　通常の制裁

ⅰ)警告(45 条Ⅰ)

ⅱ)処理中止の指示(45 条Ⅱ)

ⅲ)指示に従わない情報処理責任者に対する制裁として、

(a)過料(45 条Ⅰ①)。過料額は、15 万ユーロあるいは 30 万ユーロ以下、あるいは、30 万ユーロを上限とした総売上額の最大5%(47 条)

(b)届出の対象となる処理の中止命令(45 条Ⅰ②)

(c)CNIL による許可(前述2(1)①(1)-2-2)がなされている場合はその取消し(45 条Ⅰ)

(2)-2　緊急の制裁

ⅰ)当該処理が国家によるもので、デクレ許可やアレテ許可(前述2(1)①(1)-2-3)の対象ではないもの;最長3か月までの処理中断命令(45 条Ⅱ①)

ⅱ)当該処理が、26 条Ⅰ及びⅡに定める処理(前述2(1)①(1)-2-3-1 ⅰ)、2(1)①(1)-2-3-2 ⅰ)及びⅱ))に属さない場合、処理された個人情報のうち一定のもの;最長3か月までの利用停止(45 条Ⅱ②)

ⅲ)デクレ許可(前述2(1)①(1)-2-3-1)を要する処理のうちⅰ)に該当するもの、及び、アレテ許可(前述2(1)①(1)-2-3-2)を要する処理のうちⅰ)ⅱ)に該当するもの;違反行為中断措置をとるよう首相に通知(45 条Ⅱ③)

これらの制裁のうち、決定に値するものに不服のある者は、コンセイユ・デタに訴訟を提起できる(46 条)。

(3)出訴

CNIL 委員長は、権利や自由に対する重大かつ急迫の侵害があると認める場合、管轄裁判所に対し、仮処分手続をもって、当該権利自由の擁護に必要なあらゆる安全保護措置を、場合によっては罰金強制付で命じるよう、求めることができる(45 条Ⅲ)。

(4)アクセス権行使への対応

何人も、個人情報処理責任者に対し、質問する権利、自己情報の複写請求権(39 条)、自

己情報の訂正・利用停止・消去請求権（40 条）を有するが、国家の安全や国防又は治安に関する処理についての場合は、CNIL に請求する（間接請求）。

この請求は、CNIL 委員のうち、現役あるいは元裁判官（コンセイユ・デタ、破毀院、会計院）で構成される委員会に対してなされる。同委員会が、当該処理が含まれている情報を開示しても、その目的、あるいは、国家の安全や国防、治安を侵害しないものであると、処理責任者の同意を得て認めたときは、当該情報が請求者に開示される。

(5)その他

その他、CNIL は以下の権限を行使する。

ⅰ)個人情報の本人や処理責任者に対し、それらの者の権利及び義務について、情報提供（11 条①）

ⅱ)苦情処理（11 条②c)）

ⅲ)公的機関や裁判所からの意見要求への回答、個人情報の自動処理を実施しているか、あるいは、実施しようとしている人々及び組織への助言（11 条②d)）

ⅳ)共和国検事に対し、刑事訴訟法典 40 条に従い、委員会が知り得た犯罪行為を告発し、刑事手続において意見を述べる（11 条②e)）。

ⅴ)個人情報処理に関する調査、情報の複写の取得（11 条②f)）

ⅵ)職業団体あるいは主として情報処理責任者によって構成された団体の要求に基づき、職業上の倫理規範(règlges professionnelles)の素案について、及び、個人情報処理や個人情報匿名処理から倫理規範に服する個人を保護するための手法や手続について、本法の定めへの適合性に関する意見を述べる（11 条③a)）。

ⅶ)本法の定めに適合していると既に承認した職業上の倫理規範が定める保障について、個人の基本権尊重の観点から評価する（11 条③b)）。

ⅷ)倫理規範が本法の定めに適合すると認めた場合に、証票を交付する（c)）。

ⅸ)委員会は､自動処理からの個人の保護に関する法律又はデクレのあらゆる草案につき、意見を述べる（11 条④a)）。

ⅹ)政府に対し、自由の保護を、情報の処理と技術の進展に適合させるための法令制定を提案（11 条④b)）

ⅹⅰ)他の独立行政機関からの求めに応じ、情報保護について協力（11 条④c)）

ⅹⅱ)首相の求めに応じ、個人情報保護の分野における国際的交渉の場でのフランスの方針の準備及び確定作業に参画し、かつ、この分野を管轄する国際組織や共同体組織におけるフランス代表に参加（11 条④d)）

以上の任務を遂行するために、委員会は、勧告をすることができ、かつ、本法の定める場合には、個別の決定、あるいは、規則を定める決定を下すことができる（11 条)。

委員会は、毎年、共和国大統領、首相、及び、国会に対し、自らの任務の遂行について報告するための公式報告書を提出する（11 条）。

②オフィスの実態

CNIL委員長は、CNILの職員を任命する（19条）。2008年３月１日現在の職員の職(poste)は 120 であり、前年から 15 ポスト増えている。なお、2004 年段階では 80 であった[28]。

委員会職員にも秘密保守義務が課せられる（20 条）。

CNIL は、その任務の達成に必要な予算を与えられる。これら予算の管理について、財政統制に関する 1922 年８月 10 日の法律の定めは適用されない。委員会の会計は、会計院の統制に服する（12 条）。2008 年時における予算は 11,400,000 ユーロであり、前年から 1,500,000 ユーロの増である。なお、2004 年時は 6,500,000 ユーロであった[29]。

③リソース確保に関する現状と問題点

現時点で特筆すべき情報は入手できていない。

④広報の実態

2007 年以来、ラジオ局の一つであるフランス・インフォ(France Info)が、CNIL の広報番組を続けている[30]。

CNIL は、2004 年以来、1,000 人の市民を対象に、CNIL の認知に関する調査を行っている。「あなたは CNIL という名前を知っていますか？」という問いに対し、「はい」と答えた人の割合は、2004 年６月で 32%、2005 年 12 月で 37%、2006 年 12 月で 39%、2007 年 11 月で 50%という結果となっている[31]。

（２）第三者機関の活動状況

①第三者機関の国内での活動状況

CNIL の委員や職員は、シンポジウムやセミナー等に参加しており、2007 年の参加数は 155 である[32]。

②第三者機関の国際的な活動状況

CNIL は、情報が瞬時にヨーロッパ規模で、さらには世界規模で移動することから、様々

な作業部会において、ヨーロッパにおける、制度上のあるいは非正規の類似機関と協働しているとする。また、1995 年の EU データ保護指令 29 条によって設置された作業部会の委員長は、2008 年２月以来、CNIL の委員長が務めている[33]。

③教育・啓蒙、普及・広報活動等の現状

現時点で特筆すべき情報は入手できていない。

④第三者機関と外部機関等との関係

他政府機関との関係については、デクレ許可及びアレテ許可についての、前述 99 頁参照。なお、CNIL は、2007 年において、法律あるいはデクレの案について、６つの意見を述べている[34]。

（３）苦情・紛争処理の実態

①苦情・紛争処理の概況

ⅰ）2007 年における事前規制権限の行使[35]
届出･･･56,404 件。1978 年以来の届出総数は 1,216,404 件。
許可数･･･214 件　不許可･･･26 件　統合デクレ・アレテ許可･･・４件
センシティブ情報にかかる意見･･･22 件　統合許可への意見･･･２件
ⅱ）2007 年における制裁権限の行使[36]
警告･･･５件　　処理中止の指示･･･101 件　過料･･･９件(総額 175,000 ユーロ[37])
ⅲ）アクセス権行使への対応
間接請求･･･2,660 件（前年比 67%増）[38]。このうち、STIC（後述 107 頁以下参照）への請求は 1,259 件、JUDEX（後述 107 頁以下参照）への請求は 2,458 件[39]である。
ⅳ）その他
苦情申立ての受理件数･･･4,455 件（前年比 25%増加）[40]
2007 年における STIC と JUDEX（後述 107 頁以下参照）への査察･･･2,458 件[41]

②具体的ケース

2007年のCNIL年次報告書は、信用販売に関する主要ファイル(fichier central de credit)の問題を取り上げている。これは、諸個人の経済状況、とりわけ未払いの有無などに関する情報を集めたファイルのことである。信用販売に関する支払の付帯事項(incidents)を集

めたに過ぎないネガティブ・ファイル(fichier négatif)に対し、ポジティブ・ファイル(fichier positif)と呼ばれるのが通常である[42]。

CNIL は、かかるポジティブ・ファイルを、クレジット会社や住宅賃貸会社が利用して、弁済不能の危険に関する諸個人の情報を保有し得るようになることは、個人を社会的に排除する危険があるとして、2005 年 1 月の「ポジティブ・システム(centrales positives)について報告書」や、同年の年次報告書において、適法であることの承認を拒否している。それらによれば、クレジット産業におけるポジティブ・ファイルの有用性を承認し、かつ、かかるデータベースの目的と内容を措定できるのは立法者のみであるから、法律で認められない限り、ポジティブ・ファイルの導入は許されないとする。

同様の理由から CNIL は、2007 年 3 月 18 日、ポジティブシステム導入に関するエクスパリアン社の許可（1978 年法 25 条 I ④）申請を退けた(délibérations 2007-044)。この不許可について、CNIL の P.ノグリ(Nogrix)委員（当時）は、以下の 3 つの理由を挙げる。

ⅰ)銀行秘密という法的に保護されるべき秘密に含まれる情報が、法律上の根拠を欠いたまま、銀行法不適用のゆえに銀行秘密に関する諸規範に服さない企業に移転するおそれがあること。

ⅱ)顧客は、銀行秘密の解除条項に署名したことの効果について、十分な条件で告知されていないおそれがあること。

ⅲ)クレジット審査の際に、過去 3 年以内の支払情報が、極めて詳細なレポートの形でシステム参加企業に移転することは、個人の経済的プロファイリングを可能にし、かつ、これらの情報を、クレジット審査とは別の商業目的で利用させるおそれを生ぜしめる。

他方、CNIL は、2005 年と 2006 年に、同一銀行グループ内の複数消費者金融会社間における、不払い予防のための債務者情報交換システムを許可している。これらが許可されたことにつき、ノグリ委員は、以下の 5 つの条件をクリアーしたことを挙げる。

ⅰ)詐害行為や不払いの予防という目的が正当であること。

ⅱ)同一銀行グループ内での情報交換であるから、情報の流通範囲が限定されていること。

ⅲ)消費者金融会社における情報は、銀行秘密に属すること。

ⅳ)同一銀行グループ内であれば、金融上の危険について、利益が共通すること。

ⅴ)情報共有について、顧客が明示的に同意していること。

３．その他の動向

（１）新たな課題への取組

CNIL は、2007 年の年次報告書で、バイオメトリクス、RFID、監視カメラの問題を取り上げている。

①RFID

CNIL によれば、フランスにおいて、RFID や NFC といった技術を用いた IC チップは、パリ地下鉄の電子乗車券であるナヴィゴパス(NAVIGO)や電子マネーのように、交通や流通の分野において、特に多用されているという。その他の例として、電子パスポート、建物への出入証[43]等が挙げられている。そして、CNIL は、近い将来、さらに多様な分野で電子チップが用いられることになると予測したうえで、大要、以下のように述べる。

IC チップに組み込まれた情報は、それ自体が個人情報であることもあるし、そうではなくても、他のデータベースとの照合により、個人情報足りうるものがある。チップそれ自体からは、そこに含まれている情報を認識することはできないが（不可視性)、読み取り機器さえあれば、誰でも、他人の日常生活を、個人を識別した上で把握することが、しかも、遠隔地から可能である。以上のことが、個人情報保護の問題に新しい論点を生ぜしめている。

たしかに、今日において、RFID のシステムが、個人を継続的に監視する機能を有しているとまではいえない。例えば、ナヴィゴパスの利用は、利用者の地下鉄乗降駅を知らしめるに過ぎず、当該利用者の移動経路までをも把握させるものではない。なお、CNIL は、ナヴィゴパスから得られる情報の保存期間を２日間に限定し、かつ、当該情報の利用目的を、不正行為検知に限定するよう勧告している[44]。

RFID と私生活を調和させるためには、例えば、交通機関における利用の場合、自己を識別されることなく移動し続けることを可能にするシステムが存在し続けなければならない。流通機関の場合、例えば、スーパーマーケットの商品に備え付けられた IC チップは、レジ通過の際に、その内容が自動的に消去されるようにされなければならない。

RFID の広範囲にわたる普及、そこに含まれる情報の個人識別可能性、その不可視性、個人のプロファイリングの危険性といったことから、CNIL は、この新しい技術について、特別の警戒心をもって関心を寄せている。

RFID 技術の発展は、個人情報保護における主要原則－－合目的性、相当性、透明性、安全性－－に強く関わることについて、留意すべきである。

RFID を含んだ装置が、個人を直接的又は間接的に識別するものであれば、それは、1978 年法の適用対象となる。したがって、RFID を規制するための特別な法律は必要ない。しか

し、1978 年法の適用にあたり、特別の配慮は必要だろう。そして、この法律の適用状況次第では、同法の改正が必要になるかもしれない。CNIL に設置される作業部会において、この点が検討されることになる[45]。

②バイオメトリクス情報

個人の調査に必要なバイオメトリクス情報を含む自動処理については、国家がそれをする場合はデクレ許可が（前述 99 頁参照）、私人がする場合は CNIL の許可が必要となる（前述 99 頁参照）。後者の許可の申請数は、2005 年が 39 件（許可が 34 件、不許可が 5 件）、2006 年が 360 件（許可が 351 件、不許可が 9 件）、2007 年が 515 件（許可が 494 件、不許可が 21 件）[46]と、急増している。その多くは、事業場における労働者管理を目的としたものである[47]。

2007 年 7 月 10 日、CNIL は、外国人居住者のビザにバイオメトリクス情報を含めることを制度化しようとしたデクレの案について、内務相から諮問を受け、積極的な意見を公表している(délivération n.2007-195)。ビザに埋め込まれることになった情報は、デジタル処理化された顔写真と指紋（10 指）であった[48]。この意見を受けて、VISABIO というシステムが、2007 年 11 月 2 日のデクレ 2007-1560 号で制度化された。

また、同年 11 月 11 日には、2009 年 6 月 28 日までに、パスポートにバイオメトリクス情報を含めることを制度化しようとしたデクレ案について、やはり内務相から諮問を受けた。同デクレ案によれば、パスポートに埋め込むことを予定していたバイオメトリクス情報は、デジタル処理化された顔写真と指紋（２指）であった。このデクレは、内務省におけるパスポート管理ファイルシステム（DELPHINE）において、上記の情報に加え、デジタル処理化された 8 指の指紋をも登録することとしていたところ、CNIL はこの点を問題視し、かかるデジタル情報のデータベースは過剰なものであるとして、消極的な意見を公表した(délivération n. 2007-368)[49]。同意見の要旨は以下の通りである。

・DELPHINE システムは、行政上の目的に合致した、初めてのバイオメトリクス情報のデータベースである。
・かかる情報の自動的かつ集約化された処理は、公の秩序や治安といった要請によって正当化されない限り、許されない。
・確かに、パスポートの詐取防止という目的そのものは正当である。しかし、８指の指紋を国家的に保持することを正当化するほどの理由とはならない。かかる情報の集積は、個人の自由に対する過剰な侵害である。
・かつ、このように重要な問題を、デクレという行政立法で制度化することは問題である[50]。

③監視カメラ

2007 年現在、フランスには、9 万台の監視カメラが設置されており[51]、その多くは、複数のカメラを一カ所に設置するものだという。

CNIL によれば、監視カメラに関する届出（前述 97 頁参照）は、2002 年以降、コンスタントに増加し続けており、2006 年におけるそれは、2003 年のほぼ 20 倍の件数に上るという。2007 年における届出数は 1,317 件であり、前年までのそれと合算すると 2,980 件となる。他方、苦情申出も増加しており、2006 年には 114 件、2007 年には 121 件を数える。苦情申立の対象となったものは、事業場における労働者監視用カメラについてが最も多く（2007 年で 70 件)、共同住宅におけるものが 20 件、地方公共団体や市町村警察が設置するものについてが 13 件、学校におけるものが 3 件、その他が 15 件となっている。CNIL は、2007 年 11 月 22 日に、内務大臣からのヒアリングにおいて、監視カメラについての苦情申立が増加していることについて注意を喚起している。

監視カメラ設置についての法律は、安全に関する 1995 年 1 月 21 日の指針及びプログラム法律 95-73 号である。これによれば、国防関係のものを除き、監視カメラは、県地方長官(représentant de l'Etat)の許可を得て設置することができる（同法 10 条Ⅲ)。しかし、同時に CNIL への届出も必要なため、CNIL は、法制度が不明瞭でわかりづらくなっているとし、設置規制を含めた監督権を CNIL に集中すべきことを提言している。また、CNIL は、監視カメラ設置の根拠法律が、1995 年という、カメラによる録画が磁気テープへのアナログ録画時代のものであることを指摘し、その後の技術の進歩に併せた法改正の必要性を指摘する[52]。

（２）警察情報の利用について

フランスにはいくつかの治安・警察関係の情報システムがある。その代表例は、調書作成犯罪に関する情報処理システム（ système de traitement des infractions constatées: STIC ）と、文書及び情報処理についての司法システム(système judiciaire de documentation et d'exploitation: JUDEX)である。

STIC とは、被疑者や犯罪被害者について、刑事手続きの開始後に、国家警察の警察官や国家憲兵隊等によってもたらされた調査報告に基づく情報の集合であり、犯罪の認知や証拠収集、捜査の促進を狙いとする個人情報情報処理システムである。2001 年 7 月 5 日のデクレ 2001-583 号で制度化された[53]。内務省の国家警察総局が管轄する（2001 年デクレ 1 条、２条)。JUDEX は、後述の 2003 年法で制度化された。国防省の国家憲兵隊総局が管轄するものだが、その内容は、STIC と異ならない (2006 年 11 月 20 日のデクレ 2006-1411 号 1 条、２条)。

2008 年 12 月現在、STIC には、37,911,000 の犯罪行為、5,552,312 名の被疑者、28,325,976 名の被害者、10,000,000 の物(objets)についての情報がある[54]。

STIC が制度化された当初は、司法警察目的でのみ利用されていたが、日常の安全に関する 2001 年 11 月 15 日の法律 2001-1062 号 28 条が、その利用範囲を拡大した。つまり、治安や国防に関する許認可決定や、一定の区域への侵入許可、危険物に関する許可等について、当該部局の職員が、これらの決定をする前に、利用できることが認められた。その後、国内の安全に関する 2003 年 3 月 18 日の法律 2003-229 号 21 条Ⅳが、さらにその範囲を拡張する。具体的には、フランス国籍獲得要求、外国人の入国や滞在についての資格交付・更新等における利用が認められたのである[55]。2003 年法は、STIC を法律上の制度とし、かつ、JUDEX を新設した点でも重要である。

他方、2003 年法 21 条Ⅲは、事後の司法判断等により情報の内容が変更された場合、共和国検事は、当該情報の消去や補完、訂正を求めなければならないとし、同条Ⅴは、両システムの対象や、情報の保存期間等に加え、関係当事者がアクセス権を行使するための条件を、CNIL の意見を経たうえで、コンセイユ・デタの議を経るデクレで定めるものとする。

これを受けて、STIC については 2006 年 10 月 14 日のデクレ 2006-1258 号が、JUDEX については同年 11 月 20 日のデクレ 2006-1411 号が、それぞれ制定された。両者の内容に異なるところはない。両デクレは、証拠不十分による不起訴や免訴決定、無罪判決が確定したものは、両システムの情報を更新するよう、処理責任者に要求でき、また、この要求は、共和国検事に対して直接に、あるいは、CNIL を通じてなし得るものとする（2006-1258 号 3 条、2006-1411 号 3 条）。2007 年において、CNIL を通じた要求は 2,660 件であり、前年よりも 67%増加している[56]。

（3）CNIL 年次報告書について

ア)2007 年の CNIL 年次報告書は、2007 年のハイライトの一つとして、多様性の発見に関する 10 の勧告を挙げる。その内容は、以下のとおりである[57]。

①統計データベースや財務管理ファイルへのアクセスを、研究者に、より広く開放すべき。
②多様性を測定するための調査においては、諸個人のルーツに関する「客観的な」情報（国籍及び／又は両親の出生地）を用いるべき。
③諸個人のルーツについての情報を、企業や行政の有する（職員や顧客）ファイルに記録すべきではない。
④差別「感」(<< ressenti >> des disctriminations)についての研究を進めるべき。そこには、諸個人の身体的外観についての情報の集合が含められる。
⑤現実に生じる差別を発見するためには、一定の状況の下で、姓と名を分析することを認めるべき。
⑥センシティブ情報をより適切に保護するために、研究者の科学性を保障し、かつ、研究ファイルの管理手続を整備しつつ、情報処理、情報ファイル及び自由に関する法律を改

正すべき。
⑦現状では、民族人種学的な国籍測定システム(référentiel national ethnoracial)を創設すべきではない。
⑧多様性発見の検討を進めるため､信頼できる第三者としての鑑定者の利用を促進すべき。
⑨匿名化技術の利用により、秘密性と匿名性を保障すべき。
⑩情報についての権利と自由の実効性を、透明性の確保によって保障すべき。

イ)2007 年の CNIL 年次報告書は、1978 年法が良い法律であり、かつ、これまで、諸外国の法制に影響を与えてきたと自画自賛するが、同時に、同法には修正すべき点もあることを認める。具体的には、届出手続が複雑であることや、EU 非加盟国への個人情報移転に対する規制が不十分であること、より実効的かつ迅速な行動を可能にする制度運用を可能にする手段が検討されるべきこと等が挙げられている。その他、前述した RFID 問題への対応を含め、CNIL は、2008 年夏、これら諸課題を検討し、30 年後の法改正を目指した作業部会を設置している[58]。

（４）プライバシー保護団体や世論の動向について

前述の 2001 年法制定の際、警察以外の行政機関も STIC を利用できるようにすることにつき、CNIL は一貫して批判していたことに関し、STIC に批判的な市民グループは、CNIL の姿勢を評価していたようである[59]。

---

[1] 同改正については、清田雄治「フランスにおける個人情報保護法制の現況」愛知教育大学社会科学論集 42＝43 号（2005 年）277 頁、市川直子「フランスにおける個人データ保護法制」城西大学経済経営紀要 23 巻（2005 年）37 頁参照。改正以前の法制については、多賀谷一照「フランス」比較法研究 43 号（1981 年）49 頁、多賀谷一照「フランスにおけるプライバシー保護法制」ジュリスト増刊『情報公開・個人情報保護』（1994 年）293 頁、江藤英樹「フランスの個人情報保護法とプライヴァシーの保護」明治学院大学法学研究論集 6 号（1997 年）71 頁参照。
[2] 旧法は、対象機関を定義していなかったが、EU データ保護指令２条(d)及び(e)に対応するため、2004 年改正法で、本文のようが置かれた。
[3] 旧法は、適用対象外の個人情報処理を、ごく私的な処理に限定していたが（45 条）、2004 年改正法は、1995 年の EU 指令第３条に対応するため、本文のような定めを用意した。v. Laffaire (M. -L), Protection des données à caractère personnel, Edition d'Organisation, 2005, p.36.
[4] ２条のこの部分の内容は、EU データ保護指令２条(b)とほぼ同内容であるため、本文における紹介は、堀部政男「欧州連合(EU)個人情報保護指令の経緯」新聞研究 578 号(1999 年）18 頁の翻訳に依拠した。
[5] ４条は以下のように定める。「本法の定めは、デジタル通信網にアクセスするための情報の転送や供給の技術的行為の枠内で、他の顧客に対し、伝達された情報への最良のアクセ

ス可能手段を提供することを目的とした、自動的、過渡的、暫時的保存するための一時的コピーには適用されない」。

[6] v. Laffaire, op. cit., p. 39.

[7] ただし、事後の処理で統計作成や学術若しくは歴史研究を目的とするものは、処理に関する手続を遵守し、かつ、当該情報に含まれた個人を名宛人とする決定に利用されないものであれば、情報収集の当初の目的と整合するものとみなされる。

[8] 司法補助者とは、訴訟手続の進行及び裁判の正常な運営を助けることを任務とする法律家のことで、裁判所書記官、執行吏、公証人等の裁判所職員のほか、弁護士や鑑定人等も含む。

[9] 「取得者」とは、「当該個人情報の開示を受ける権限を有する者で、当該個人、処理責任者、受託者及び職務上当該情報を処理する任務にある人々を除くすべての者」と定義されている(３条Ⅱ)。旧法には、取得者を定義する明文規定がなかったところ、EU データ保護指令２条(ｇ)に対応するため、本文のような規定が置かれた。

[10] Laffaire, op. cit., p. 72.

[11] 32 条Ⅱは、以下のように定める。「電子通信網(réseaux de communications électroniques)のあらゆる利用者は、処理責任者あるいはその代表者から、以下の事項を、明確かつ完全な形で通知されなければならない。」

[12] 「諸外国等における個人情報保護制度の運用実態に関する検討委員会・報告書」（平成 19 年）（以下、「平成 19 年報告書」という）51 頁。

[13] 同 52 頁。

[14] 行政裁判の最上級裁判所。本文で後述するように、政府の準備する法令案などについて、諮問に応じて意見を発する権限がある。

[15] デクレには、共和国大統領若しくは首相による規範制定行為である一般規制デクレ(décret réglementaire)と、個別行政行為である個別デクレ(déctet individuel)がある。それぞれにつき、特に手続の規制がない一般デクレ(décret simple)の他、閣議を経るデクレ(décret en conseil des ministres)と、コンセイユ・デタの議を経るデクレがある。

[16] 平成 19 年報告書 55 頁。

[17] v. Laffaire, op. cit., p. 232.

[18] 井上禎男「フランスにおける個人情報保護第三者機関の機能と運用－－2004 年改正 1978 年個人情報保護法と CNIL の実務－－」名古屋市立大学人間文化研究５号（2006 年）182 頁参照。

[19] 2004 年法改正後の CNIL については、清田雄治「フランスにおける個人情報保護法制と第三者機関――CNIL による治安・警察ファイルに対する統制 」立命館法学 300＝301 号（2006 年）145 頁、井上・前掲 155 頁。同改正以前の CNIL については、多賀谷一照「フランスにおける「情報処理と自由全国委員会」の最近の動向」ジュリスト 760 号（1982 年）34 頁。

[20] 独立行政委員会については、Ｐ．ウェール＝Ｄ．プイヨー(兼子仁＝滝沢正訳)『フランス行政法－－判例行政法のモデル』(三省堂、2007 年）36 頁以下参照。

[21] http://www.CNIL.fr/index.php?id=2538&tx_ttnews[tt_news]=427&tx_ttnews[backPid]=17&cHash=e0dfe91b94.

[22] 第五共和国憲法により組織され、主として経済的社会的問題について政府の諮問に答える機関（憲法 69～71 条)。

[23] 民事及び刑事裁判の最上級裁判所。

[24] 公会計に関する一般的裁判管轄権を有する行政裁判所。

[25] CNIL の 2007 年年次報告書によれば、政府委員補佐は１名である(CNIL, 28e Rapport d'activité 2007, p. 91.)。

[26] http://www.cnil.fr/index.php?id=1499.

[27] CNILの2006年報告書によると、監督者は600名となっている。
[27] アレテとは、わが国の省令に相当する行政立法である。
[28] Rapport, op. cit., p. 96.
[29] ibid.
[30] Rapport, op. cit., p. 38.
[31] Rapport, op. cit., p. 39.
[32] ibid.
[33] Rapport, op. cit., p. 51.
[34] Rapport, op. cit., p. 94.
[35] Rapport, op. cit., p. 94.
[36] Rapport, op. cit., p. 94.
[37] Rapport, op. cit., p. 47.
[38] Rapport, op. cit., p.34 et p. 94.
[39] Rapport, op. cit., p. 33.
[40] Rapport, op. cit., p. 32 et p. 94.
[41] Rapport, op. cit., p. 36.
[42]藤原靜雄「個人情報保護の現在－－2008年9月・施行から3年余を経て－－」法律のひろば2008年9月号17頁。
[43] CNILの2007年年次報告書は、出入証システムの例として、郵便局での利用から発展したVIGIKを例示する。Rapport, op. cit., p. 27. VIGIKについては、http://www.VIGIK.com/参照。
[44] Rapport, op. cit., p. 27.
[45] Rapport, op. cit., p. 28.
[46]宮下紘「諸外国等における個人情報の保護の動向」法律のひろば2008年9月号46頁参照。
[47] Rapport, op. cit., p.18.
[48] ibid.
[49]
http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000019796136&fastReqid=1094268300&fastPos=
[50] Rapport, op. cit., p. 19.
[51] Rapport, op. cit., p. 25.
[52] Rapport, op. cit., p.25.
[53] その制定過程や内容については、清田・前掲「フランスにおける個人情報保護法制と第三者機関」154頁以下が詳しい。
[54] http://www.cnil.fr/index.php?1813
[55] http://www.cnil.fr/index.php?1813
[56] Rapport, op. cit., p. 94.
[57] Rapport, op. cit., p. 13 et s., p. 94.
[58] Rapport, op. cit,. p. 75.
[59]清田・前掲「「フランスにおける個人情報保護法制と第三者機関 」177頁。