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

平成 23 年 3 月

はじめに

筑波大学法科大学院　藤原　靜雄

個人情報保護制度の監督機関について、我が国個人情報保護法は主務大臣制を採用し、個人情報保護を所管する特別な機関は置かれていないが、諸外国等においては個人情報保護制度について独立した監督機関がおかれていることが多いこと等から、個人情報保護法を執行する中立的な第三者機関の設置は「国際的な整合性も踏まえ、中長期的課題として検討する」とされている（個人情報保護に関する取りまとめ（意見）（平成 19 年 6 月 29 日国民生活審議会））。

国内における個人情報保護制度の監督機関に関する議論については、平成 22 年 8 月に設置されている消費者委員会個人情報保護専門調査会における委員からの発言でも触れられているほか、内閣官房における「社会保障・税に関わる番号制度」の検討の中でも「番号制度に係る個人情報保護法制の円滑な執行と適切な運用を担保するために設置される第三者機関の在り方について、具体的検討を行う。設置に当たっては、監視機能を実効あらしめるべく、どのように独立性を担保しどのような権限を持つべきかという観点から、責任主体、設置形態（単独府省にするか三条委員会にするか等）、人事（人員構成）、調査権限、規模等の論点について、諸外国の事例も踏まえながら、十分に検討する。」（平成 23 年 1 月 31 日「社会保障・税に関わる番号制度についての基本方針」）とされており、同基本方針を受けて設置された個人情報保護ワーキング・グループの中で独立性を持った監督機関の在り方が議論されている。

社会保障・税に関わる番号制度で設置が予定される監督機関はあくまで「番号に係る個人情報」を対象とするものになると考えられ、個人情報保護制度全般に関する監督機関については、なおその在り方等について議論が必要である。一方、諸外国等における個人情報保護の監督機関については、過去の調査（内閣府「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」平成 21 年 3 月）等によりある程度我が国においても紹介がされてきたが、その具体的な制度状況（憲法・行政組織法上の位置づけ、個人情報保護法以外の所管法令、具体的な執行権限等）や運用状況（予算規模、職員の採用・人事・給与・キャリアパス、他の規制機関との協働状況、苦情の受付状況・内訳、執行状況等）などの実践的な観点からは、十分な情報が集積されているとはいえない状況であった。

そこで、本委員会においては、個人情報保護制度の監督機関において特徴を持つ国であるイギリス、フランス、ドイツ、スウェーデン、アメリカ、カナダ、オーストラリア及び韓国について、特に上記のような制度状況及び運用状況につき、実地調査及び文献調査を行った。なお、アイルランドについては、当初の予定には含まれていなかったが、担当委員のご尽力により、監督機関からの質問票への回答の形で収録を果たしている。

最後に、ご多忙の中、貴重な時間を割いていただいた各担当委員と適切かつ周到な情報提供をしてくださった板倉陽一郎　個人情報保護推進室　政策企画専門官（弁護士）に感謝申し上げたい。

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

委員名簿・執筆分担

○藤原　靜雄	筑波大学法科大学院教授 （平成 23 年 4 月より中央大学法科大学院教授） はじめに・あとがき執筆、ドイツにつき監修、全体につき査読
尹　龍澤	創価大学法科大学院教授 韓国につき執筆
六川　浩明	弁護士・成城大学法学部講師・首都大学東京産業技術大学院大学講師 オーストラリアにつき執筆
加藤　隆之	亜細亜大学法学部准教授 イギリス・ドイツ・アイルランドにつき執筆
宮下　紘	駿河台大学法学部准教授 フランス・スウェーデンにつき執筆
河井　理穂子 （井上）	国立情報研究所特任助教 （平成 23 年 4 月より埼玉工業大学人間社会学部専任講師） アメリカ・カナダにつき執筆

（○は委員長）

目次

I.　諸外国等における個人情報保護制度の監督機関の概要

i.　欧州

（1）イギリス概要

1　個人情報保護法制の概要

イギリスの個人情報を保護する法律名は「1998 年データ保護法（Data Protection Act1998）」。1984 年データ保護法を EU データ保護指令に対応すべく改正して成立。

公的部門・民間部門双方に適用され、自動処理データに限らない「個人データ」を対象とする。小規模事業者に対しても義務の免除はない。権利義務規定のほか、データ保護原則を定めている。届出制度を採用しており、登録料が課される（大規模事業者は 500 ポンド、それ以外は 35 ポンド）。

2　監督機関の制度概要

イギリスにおける監督機関は情報コミッショナー（Information Commissioner）である。「データ管理者が善良な実務を守ることを促進し、本法に基づく義務をデータ管理者が遵守することの促進に関し、本法のもと自らの役割を果たす」ことを職務とする（データ保護法 51 条（1））。マンチェスターに本部を構えるほか、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。情報コミッショナーは政府から指名される。

事務局は主に 5 つの部署に分かれており，スタッフは 327 名（うち常勤スタッフ 311 名。2009/2010 年年次報告書）。予算は登録料と補助金をあわせて 18,692,000 ポンド（同）。

情報コミッショナーを女王から独立した単独法人で、議会に対して責任を負う。任期は 5 年であり、再任可能だが 3 回目以降は例外的。

3　監督機関の運用実態

苦情処理や紛争解決の数は上昇傾向。2009/2010 年年次報告書によると、苦情及び助言は 33,234 件、そのうち 32,714 件が処理された。執行通知が 15 件、監査が 5 件、訴追が 2 件行われた（情報コミッショナーは自ら法廷において検察官として活動することが可能）。2010 年 4 月より上限 50 万ポンドの金銭的制裁の権限が加わり、実際に 2 件が科せられた（それぞれ 60,000 及び 1,000 ポンド）。

4　監督機関の課題等

地位や権限について法改正が予定されている（任期を 7 年に延長、主務大臣の同意が必要とされていた複数の事案について同意不要とするものなど）。また、EU データ保護指令との関係で、欧州委員会がイギリスのデータ保護法の運用の多くの点を疑問視している。

（2）フランス概要

1　個人情報保護法制の概要

「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」につき、2004 年に大幅な改正が行われ、2009 年 5 月 12 日にも改正されて現在に至る。

公的部門・民間部門を問わず適用される。主な権利・義務に関する内容として，基本原則（法 6 条)、個人情報の処理における本人の同意（法 7 条)、情報処理の拒否権、処理責任者への質問権、自己情報の複写請求権、訂正・利用停止・消去請求権（法 39 条)、安全管理義務（法 34 条）などの条項を備えている。

2　監督機関の制度概要

フランスにおける監督機関は「情報処理及び自由に関する全国委員会（Commission nationale de l’informatique et des libertes（CNIL))」。CNIL はフランスにおける初の独立行政委員会である（1978 年成立)。17 名の委員により構成される（裁判官 6 名､国会議員 4 名､経済･社会評議会委員 2 名､上院･下院議長任命の IT 専門家 2 名、首相任命の IT 又は市民的自由専門家 3 名)。任期は 5 年で再選は可能だが 10 年を超えてはならない。事務局には約 150 名のスタッフがいる。CNIL はパリにあり、地方部局は存在しない。予算は 2010 年で 14,700,000 ユーロ。

CNIL の執行権限は 2004 年法により強化され、官民両部門において通知と事前の意見表明を行うことができるようになり、また法律違反の際は法令遵守通知の発出を行い、服従しない場合は上限 150,000 ユーロの罰則、反復違反の場合は上限 300,000 ユーロを課すことができる。

3　監督機関の運用実態

2010 年には 4800 件の苦情処理を受け付けており、毎週 150 通程度の手紙を返している。2010 年は検査が 310 件、罰金を科したのが 34 件（合計 555,400 ユーロ)。

4　監督機関の課題等

近年は，監視カメラ・バイオメトリクス・位置情報などに検査の力を注いでいる。また，拘束的企業準則（BCR）の利用を促進している。将来的な課題として、Privacy by Design、グローバル化における一定の水準の設定などが挙げられる。

（3）ドイツ概要

1　個人情報保護法制の概要

ドイツにおける中心的な法律は連邦データ保護法（Bundesdatenschutzgesetz（BDSG））である。最も直近の改正は 2009 年。同法の目的は個人データの取り扱いにおける個人の人格権権侵害からその個人を保護することにある（1 条 1 項)。公的部門及び民間部門を包括的に規定している。また近年ではインターネットに対応すべく通信役務個人情報保護法（1997 年）およびテレコム法（2004 年）なども個人情報保護の個別法として重要視。

2　監督機関の制度概要

公的部門の法の運用については、連邦データ保護・自由監察官（「連邦監察官」）の役割が大きく、民間部門の法の運用については、各州の監督官庁（州の監察官ないし内務省の担当部局）が重要な役割を果たしている。

現在、連邦監察官オフィスの職員数は 91 名である。連邦監察官オフィスはボンにあり、ベルリンに「連絡室」を設けている。2011 年の予算はおよそ 8,800,000 ユーロ。

連邦監察官の独立性はデータ保護法によって合理的に確保されている（22 条及び 23 条参照)。同法では連邦監察官が連邦議会によって選任されること、そして職務遂行に当たってはその独立性を尊重し、法にのみ従うことが定められている。

3　監督機関の運用実態

2009 年から 2010 年にかけて、文書により 11,153 件、電話により 14,204 件の要望を受けた。2010 年には、6,087 件の苦情処理を行っている。

連邦データ保護法 24 条により、公的部門に対し、質問検査、立入権限が存在し、勧告や公表を行うこともできる(同 25 条､26 条)。ただし､他の行政機関に対して指示や命令､罰則を科すことは出来ない。民間部門に対しては、行政罰や直罰を科すことが可能。

4　監督機関の課題等

現在、連邦監察官が抱えるデータ保護に関する大きな課題のひとつは、州のコミッショナーの独立性に関する欧州委員会との対立である（2010 年の欧州司法裁判所判決では「完全な独立性」を満たさないとされた)。連邦監察官オフィスでは、州コミッショナーが、独立性要件を充足するか否かについて引き続き議論している。

（4）スウェーデン概要

1　個人情報保護法制の概要

スウェーデンにおける中心的な法律は「個人データ法（Personuppgiftslag（1998:204））」である（補足的な規則として，個人データ施行令（全 14 条）」。同法は個人データの処理による個人の人格の侵害に対する保護（第 1 条）を目的としている。国レベルにおいて世界で最も早い 1973 年に制定され、1998 年、2007 年にそれぞれ大規模な改正が行われた。

公的機関・民間機関双方を対象としており、個人データ管理者の義務を定めるほか、事業者にはデータ保護検査院（後述）への登録が義務付けられている。

2　監督機関の制度概要

スウェーデンのデータ保護機関はデータ保護検査院（Datainspektionens）であり，オンブスマンに類似する独立行政機関の一つとして理解されている（同様の第三者機関はスウェーデン全体で約 250 存在する）。本部のみで，地方機関や支部は存在しない。個人データ法、債務回復法、クレジット情報法の 3 つの法分野の法執行を監視しており、立法に対する提言を行ってきたことを最大の功績ととらえている。

データ保護検査院委員会は 5 名から構成され、国会議員 2 名、大学教授 1 名、IT 専門家 1 名、地方議員 1 名からなる。機関のスタッフは 43 名である（執筆時）。事務局は局長の他、4 つのチームから構成され、チームごとに実質的な業務が行われている。予算は 36,100,000 クローナ。

3　監督機関の運用実態

苦情処理・相談対応につき、2010 年にはメール相談が約 2,100 通、電話応対が約 5300 回。正式な苦情処理については 2010 年は 322 件。同じく、立入検査、呼び出し検査につき、それぞれ 64 件開始、52 件終了及び 98 件開始、83 件終了。これまで罰金を科した例はない。

4　監督機関の課題等

リズボン条約以降、EU 内ではデータ保護がますます重要になってきており、EU の他の加盟国との調和をどのようにとっていくかが今後問題となるだろうと思われる

（5）アイルランド概要 ＜補節＞

1　個人情報保護法制の概要

アイルランドにおける個人情報保護に関する法律はデータ保護法（Data Protection Act）である。1987 年と 1988 年に議会で審議された上ですべての政党の賛成により成立した。

欧州評議会の第 108 条約を基礎としており、EU データ保護指令制定後に改正された。

2　監督機関の制度概要

データ保護コミッショナーが監督機関の地位にある。データ保護法附則第 2 では、データ保護コミッショナーが「職務遂行に際して、独立しているべきである」ことを定めている。最高 5 年の任期で指名され、再指名されることもできる。地位及び給与が保障されていること、省庁とは切り離されており、大臣の命令に従う必要がないこと、などの点で独立性が確保されている。公的部門・民間部門をいずれも監視している。

現在 22 名の職員がおり、全員公務員である。地域支部等は特に存在しない。予算は 2011 年度で 1,458,000 ユーロ。

コミッショナーは執行通知を出す権限を有し、この執行通知に従わない場合、コミッショナーによる提訴が可能であり、罰金刑が科される（自由刑は存在しない）。

3　監督機関の運用実態

苦情受付数は 2008 年度－ 1,031 件、2009 年－ 914 件、2010 年－ 783 件、となっている。多くの苦情は公式な調査を経ずに処理されている。2 名の職員が交代で電話応対にあたり、コミッショナーを含め全職員がこの職務にあたっている。

4　監督機関の課題等

今後、広くデータ保護法違反を犯罪と構成し、権限を広げていきたいと考えている。

2002 年 EU 電子プライバシー指令においてはデータ保護違反届出に関する定めを置くことが加盟国に義務付けられているが、この届出は電子プライバシー規制法にのみおかれることとなっており、これに該当しないデータ保護法違反行為に対し、事実の告知義務が課せられないことは問題であると考えている。

ii.　北米

（1）アメリカ概要

1　個人情報保護法制の概要

米国は個人情報保護をセクトラル方式で行っているため、包括的な法律は存在しない。公的部門に関しては連邦政府が保有する個人情報を対象にした連邦プライバシー法（1974 年）が制定されており、民間部門については個別法がある。また連邦国家である米国の性質上、州法における多様な個別対応が存在している。そして個人情報保護を規定する法律ごとに監督する機関が規定されている。民間部門に対しては FTC を中心に、その他司法省（Department of Justice)、商務省（Department of Commerce）なども監督機能の一部を担う。

2　監督機関の制度概要

連邦取引委員会（FTC）は独立行政委員会であり、コミッショナーには職権行使の独立性が認められている。委員会は 5 人のコミッショナーで形成されており、大統領によって指名され、上院で承認されてから就任する（任期 7 年)。本部は Washington DC にあり、全米を 7 つのエリアに分けて業務を行っている。FTC 全体では 1,100 人の職員がいる。この中で主に個人情報保護関係の法律を扱っているのが消費者保護局である。

なお、公的部門を監督する第三者機関は存在しない。この理由については、合衆国憲法の第 2 条に違反するからであるとの見解が存在する。

3　監督機関の運用実態

FTC は違反などを自ら探し出し、立入検査、令状による命令を含む調査権限がある。また、FTC 法 Section5 に基づく法執行として排除措置や同意命令を発することができ、また相手方が争う場合には行政審判を行う。

FTC では一件一件の苦情処理を行わないが、データベースに記入された数としては 2009 年度で 3,300,000 件とされている。

4　監督機関の課題等

FTC では現在、ソーシャルネットワーク、クラウドコンピューティング、オンライン広告、携帯マーケティングなどについての対策、そして国際的な他国間との法執行の連携、また金融関係の消費者保護に関わる法律への対策、また、消費者や企業に対する個人情報保護･プライバシー保護教育の強化と、政策提言に力を入れていくということである。

（2）カナダ概要

1　個人情報保護法制の概要

カナダには公共部門と民間部門の個人情報保護に関し別々の法律が存在する。連邦の公的部門に係る法律が連邦プライバシー法であり、民間部門に係る法律が個人情報保護及び電子文書法（PIPEDA）である。Privacy Act では、情報の収集への同意、同意を得た目的以外の利用の禁止、個人情報の開示請求等の規制を定めている。PIPEDA は商業活動の過程で個人情報を収集・利用又は提供するあらゆる組織に適用される。連邦レベルでは，両法について Office of Privacy Commissioner が法執行を管轄しており、州レベルでは、州の公的部門のほか、PIPEDA と「実質的に同様」な州法が存在する場合は民間部門についても州のプライバシーコミッショナーが法執行を担うことになる。

2　監督機関の制度概要

Office of the Privacy Commissioner of Canada（OPC）は議会に直接責任を負う独立した機関である（オンブズマンの一種)。コミッショナーは 7 年の任期を持ち、議会より指名される。

州政府のプライバシーコミッショナーは、オンタリオ州を例に採ると、任期が 5 年であり、3 政党の合意で任命される。州議会の承認によっては何度でもその地位を更新できる。州政府から独立した機関であり、同様に独立した機関はオンタリオ州に 5 つ存在する。

3　監督機関の運用実態

連邦レベルでは、2009 年度に OPC の公的部門に寄せられた問い合わせ･苦情は全部で 2,572 件（うち不服申立てと認められたのは 665 件)。この間不服申立てへの判断（Findings）を明らかにしたのは 1,154 件。2009 年度民間 (PIPEDA 対象) 部門で 2,538 件 (うち不服申立てと認められたのは 231 件)。この間判断を明らかにしたのは 587 件。

これに対しオンタリオ州では、個人情報に関する開示請求は 2009 年度 14,678 件である。

4　監督機関の課題等

OPC では PIPEDA を改正し、現在、情報流出に関する報告義務を民間企業に義務づける法案が議論されている。これは米国カリフォルニア州等に設けられている法律と同様のものである。

オンタリオ州プライバシーコミッショナーは、PHIPA において、政府機関に対して行う情報開示請求の際にかかる費用を統一的に規定するべきであると考えている。

iii. オセアニア

オーストラリア概要

1　個人情報保護法制の概要

オーストラリアでは 1987 年、National ID Card 議論において、国民のプライバシー保護に懸念が生じたことを契機に 1988 年連邦プライバシー法（Privacy Act 1988:Act No.119 of 1988 as amended）を制定した。連邦プライバシー法は当初、公的部門のみを対象とする法律だったが、2001 年 12 月から民間部門も対象とする National Privacy Principle が連邦プライバシー法第 3 附則（Schedule 3）に設けられている。

2　監督機関の制度概要

従来，連邦プライバシーコミッショナー（及び事務局）による体制であったが，2010 年 11 月には以前より存在した連邦プライバシーコミッショナーに加えて The Australian Information Commissioner（連邦情報コミッショナー)、連邦 FOI コミッショナー及び統一的な事務局として The Office of Australian Information Commissioner（OAIC 連邦情報コミッショナー事務局）が設置されている。連邦情報コミッショナーは連邦 FOI コミッショナー及び連邦プライバシーコミッショナーの上位機関であり、連邦政府による情報管理についての戦略的役割を担うとされる。

3 名のコミッショナーのうち連邦プライバシーコミッショナーは、連邦プライバシー法に基づき、個人のプライバシー保護についての役割を担う（AIC 法第 4 条)。その他、現在オーストラリアはさらなる法改正の途中にあり、上述した Privacy Principles の統合など随所に改善を施す見込みである。

事務局は Compliance 部、Policy 部、Operation 部から構成されており、各コミッショナーから指示を受けて業務を遂行する。3 名の各コミッショナーの任期は 5 年以内である（AIC 法第 15 条)。2010 年 10 月における連邦プライバシーコミッショナー事務局の職員数は 60 名であり、予算は 2010 年 6 月までの 1 年間、収入ベースで 7,622,000 豪ドルである。

3　監督機関の運用実態

連邦プライバシーコミッショナーにおける 2009 年から 2010 年までの相談受付件数は電話相談が 20,935 件、郵便・メール・ファックスが 1,909 件である。苦情申立は 1,201 件であった。Determination（決定）に至ることはまれで、施行後 8 件を数えるのみである。

4　監督機関の課題等

2008 年 5 月の連邦プライバシー法改革のための提言書には連邦プライバシーコミッショナーの権限強化と明確化に向けた提案が多数なされている。本稿執筆時点において、連邦プライバシー法改革のたの公開草案の一部が公表されている。

iv.　アジア

韓国概要

1　個人情報保護法制の概要

2004 年から議論されてきた法の制定が公共・民間に分かれていた個人情報保護に関する法律を統合するという形で 2011 年 3 月 29 日から「個人情報保護法」（法律第 10465 号）として公布される。そして 9 月から全面施行されることになった。

現時点では公共部門の一般法が公共機関個人情報法であり、民間部門の一般法的位置を有しているのが情報通信網法（厳密にいえば情報通信分野のみを規律）である。

新しい法律（一般法）は“個人情報処理者”などの用語を再定義することでその適用対象を公共・民間部門すべての個人情報処理者に拡大し、コンピューターによる処理情報の他に手書き文書も保護範囲に含む、としている。なお、今後も個別法は並存する。

2　監督機関の制度概要

現行の公共機関個人情報保護審議委員会は公共機関で電子計算機処理される個人情報の保護に関する事項を審議する。個人情報紛争調停委員会は情報通信網法に基づき設置・運営され、個人情報に関する紛争について調停を行う。韓国インターネット振興院（KISA）は、個人情報侵害申告センターの運営、個人情報紛争調停委員会の運営、政府部署実態調査に対する技術支援などを遂行している。

新法においては個人情報保護委員会（大統領所属、新設)、行政安全部、中央行政機関の三者に主要な機能を置くとされている。特に個人情報保護委員会は基本計画等の審議、公的機関への是正勧告等を担うこととされている。この際、EU における独立的個人情報保護機構の基準を満たすように留意して制度設計を行った。

3　監督機関の運用実態

個人紛争調停委員会が扱う調停件数は 2009 年度で 144 件である。韓国インターネット振興院が年間に受け付けた申告数は 2010 年度で 1,788 件、相談は 53,044 件に上った。

4　監督機関の課題等

現在、行政安全部は、法律で委任事項を具体化するための規則の制定、法律施行のための分野別指針の制定、関連制度・法令の改善、対国民キャンペーンなどの準備を進めている。また、新設される個人情報保護委員会の事務局構成は、最初の問題になりそうである。

II. 諸外国等における個人情報保護制度の監督機関の制度状況及び運用状況

i. イギリス

1 個人情報保護法制の概要

（1）法律名

イギリスにおける個人情報を保護する法制度の中心は、1998 年データ保護法（Data Protection Act 1998）である。

イギリスには、1984 年データ保護法（Data Protection Act 1984）が存在したが、1995 年の EU データ保護指令（EU Directive on Data Protection 95/46EC）に従う内容で、1998 年データ保護法（以下、単にデータ保護法という場合には、1998 年データ保護法を指す）が制定された。女王の裁可を得たのは、1998 年 7 月 16 日であり、その施行は、2000 年 3 月 1 日であった。

現在、このデータ保護法の改正法案である、自由の保護法案（Protection of Freedoms bill）が議会に提出されている。

（2）目的

日本の個人情報保護法は 1 条にその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。

（3）適用範囲

①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) も対象とされている（1 条）。

デュラント事件では、この「個人データ」や「関連するファイリング・システム」の解釈について争われたが、控訴院の解釈（Durant v. Financial Services Authority [2003] EWCA Civ 1746）に対して欧州委員会が懸念を有していることについては、「4 監督機関の課題等」の「（2）EU データ保護指令との関係」を参照していただきたい。

②公的部門と民間部門

1984 年法と同様、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。

（4）適用除外

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依拠していない。それゆえ、小規模事業者であっても、データ保護法の義務の免除はない。適用除外の内容は、これを認める目的によって、除外対象となる条文が異なるため、少々複雑である。

たとえば、国家安全（National security、28 条）、犯罪及び課税（Crime and taxation、29 条）、健康、教育及び社会活動(Health, education and social work、30 条)、規制的活動(Regulatory activity31 条)、ジャーナリズム、文学及び芸術（journalism, literature and art、32 条)、研究、歴史及び統計（Research, history and statistics、33 条）家庭内利用目的（domestic purposes、36 条)、さらには付則 7 及び 8 などにおいても、特別な扱いを認める適用除外に関する詳細な定めをおいている。

（5）権利・義務規定に関する内容

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。

① 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　データ主体の権利等（7 条―15 条）
第Ⅲ章　データ管理者による届出（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限（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

②データ保護原則

データ保護原則（Data Protection Principles）は、附則 1 の第 1 章に示されている（4 条（1））。その要約は、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　保有期間の限定（Not kept for longer than is necessary）
第 6 原則　データ主体の権利に対する適合的取扱い（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）

（6）届出制度

1984 年法で設けられた登録制度であるが、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。この制度では、小規模事業者を除き、データ管理者は、以下の事項（18 条（2）（a）（b）、16 条（1））を情報コミッショナーに届出なければならず（18 条（1））、情報コミッショナーは、この届出を行った者の登録簿を保持しなければならない（19 条）。また、データ管理者は、届出事項に変更があった場合などにその届けをなす義務が課されている（20 条）。なお、この登録事項は、合理的な時間に無料で公開される（19 条（6）（a））。

・データ管理者の氏名及び住所
・本法のためにデータ管理者が代表者を定めた場合、その者の氏名及び住所
・データ管理者によって又はその者のために処理されている又はその予定である個人データ及び個人データが関連するデータ主体のカテゴリー
・個人データの取扱目的
・個人データの提供先
・個人データを欧州経済地域外へ移転させる場合の提供先又は国名や地域
・データ管理者が公的機関である場合、その事実の摘示
・17 条（1）で禁止されている状況下で処理されている又は処理が予定されている個人データが、同条（2）又は（3）によって適用が除外され、届出義務がそれらのデータには適用されない場合、

その事実の摘示

・第 7 データ保護原則（個人データに対する安全措置）遵守のための措置に関する一般的記述

かつては、この登録制度において、一律 35 ポンドの登録料が課されていたが、2009 年 10 月 1 日より、大規模事業者に対しては、500 ポンドの登録料が課されることとなった（18 条（5）参照)。その大規模事業者とは、1 年に 25,900,000 ポンド以上の売り上げのあること、若しくは、250 人以上の従業員を有していること、又は、250 人以上の職員を有する公的機関であることである。500 ポンド払う企業は、全体の 5 パーセント程度である。35 ポンド支払う必要のない、極めて小規模の事業者も存在するが、その数や割合を ICO では把握していない。この届出制度の適用がない以上、その数を把握しようがないからである。このような 2 段階の登録料制度は、規模にかかわらず一律としていた場合の不公平を解消するものである。つまり、大規模事業者の方が、ICO の職務遂行に関し費用がかかることを反映させたのである。

届出件数は、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、304,000 件を超えた旨が明らかにされており、そのうち、37,776 件が新規通知、265,766 件は更新又は維持された数である。2009/2010 年次報告書では、それまでの数から 15 パーセント上昇し、328164 件に達したことが記されている。そのうち、292,200 件が届出の更新であり、42,000 件強が新規届出であるという。また、その新規届出のうち、3907 件が、ICO から会計士、ソリシタ（事務弁護士)、人材派遣会社、個人の医療コンサルタントへの働きかけによるものである。ICO では、今後も届出のなされていない業界への働きかけをしていく予定である。

2 監督機関の制度概要

（1）設置の経緯

個人情報保護に関する直接的な監督機関は、情報コミッショナーである。情報コミッショナーは、1984 年法の定めるデータ保護登録官（Data Protection Registrar）を引き継ぎ、データ保護コミッショナー（Data Protection Commissioner）としてスタートした。その後、データ保護コミッショナーは、2000 年情報自由法(Freedom of Information Act 2000)についても所管するようになり、同法 18 条(1)によって、2001 年 1 月 30 日から、情報コミッショナー（Information Commissioner）に名称が変更となった。

1984 年法で任命された初代のデータ保護登録官は、エリック・ハウ（Eric Howe）氏であり、2 代目はエリザベス・フランス (Elizabeth France) 氏であった。さらに、1998 年法成立時の情報コミッショナーも、フランス氏であったが、2002 年 11 月 30 日に、リチャード・トーマス（Richard Thomas）氏がその地位を引き継いだ。その後、2009 年 6 月 29 日に、クリストファー・グラハム氏（Christopher Graham）氏が、その地位を引き継ぎ、現在に至っている。

（2）制度の概要

①所掌事務

情報コミッショナーの職務・権能については、第VI章 雑則及び総則の 51 条において、一般的な職務が定められている。そこでは、「データ管理者が善良な実務（good practice）を守ることを促進し、かつ、とりわけ、本法に基づく義務をデータ管理者が遵守することの促進に関し、本法のもと自らの役割を果たすこと」であると定められている（51 条（1））。善良な実務とは、個人データの取扱いに際して、データ主体などの利益を考慮して、情報コミッショナーにとって望ましいと考えられるものであり、かつ、本法で要求されていることを遵守していることを含む（但しそれに限られない）ものであることを意味する（51 条（9））。

また、主な個別の職務内容については、次のようなものがある。

- データ管理者からの届出事項を登録簿に記録する（19 条）。
- データ保護原則に違反した又は違反しているデータ管理者に対して、執行通知（Enforcement notices）を送達する（40 条）。
- 個人データの取扱いによって直接影響を受けている又は受けていると考えられる者が、その処理の適法性の評価を請求した場合（Request for assessment、42 条（1））、その請求者にとって適切であることが認識できる形で評価を行う（42 条（2）、また 42 条（3）も参照）。また、このような請求を受けたコミッショナーは、評価を行うか否かなどについて、その請求人に対して通知しなければならない（42 条（4））。なお、評価通知（Assessment notices）については、41A-C 条として定められるが、今後施行されることになっている。
- 42 条の評価請求を受けた場合又はデータ管理者がデータ保護原則を遵守しているか判断する目的で情報を求めることが合理的である場合には、データ管理者に情報提供の時期などを示した通知（情報通知、Information notices）を送達できる（43 条）。
- 42 条の評価請求を受けた場合又は 32 条によってデータの取扱いが延期されると疑われる合理的な理由のある場合、当該個人データが特定の目的にのみ利用されていることを示すなどの情報を提供するよう通知（特別情報提出通知、Special information notices）を送達できる（44 条）。
- 巡回裁判官又は地方裁判所裁判官（District Judge）（治安判事裁判所）の令状に基づき立入検査権を行使する（50 条、附則 9）。
- 同法の解釈、善良な実務、本法における職務の範囲内におけるその他の事柄について、国民に対して情報提供することが、情報コミッショナーにとって便宜であると自らが考える情報の提供を行い、これらの事項についていかなる者に対しても助言を与える（51 条（2））。
- 主務大臣が命じた場合又は情報コミッショナーがそうすることが妥当であると考えた場合、適切であると思われる者との協議の上、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（51 条(3)）。また、このような実務規範の策定や構成員へのその配布などを商業組合に奨励する（51 条（4）（a））。

・本法における情報コミッショナーの職務・役割に関して両議院への年次報告書を提出する（52 条（1））。適当と考えられる場合、これらの職務・役割に関する他の報告を両議院へ提出する（52 条（2））。また、51 条（1）又は（2）の報告書で含まれていない、主務大臣の指示に従い 51 条（3）の下で策定された実務規範を両議院へ提出する（51 条（3））。なお、データ共有規範（Data-sharing code）については、52A-E 条として定められているが、今後施行されることになっている。
・イングランド、ウェールズでは、情報コミッショナーによる又は公訴局長官による若しくはその同意を得て、北アイルランドでは、情報コミッショナーによる又は北アイルランド公訴局長官による若しくはその同意を得て、データ保護違反者に対して訴追手続を行う（60 条（1））。

②組織体制

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 年プライヴァシー及び電子通信（EC 指令）規則（Privacy and Electronic Communications（EC Directive）Regulations 2003）、2004 年環境情報規則（Environmental Information Regulations 2004）に基づく任務を担っている。このような権限及び日常的な業務の拡大に伴い、ICO のスタッフは、毎年を増加している。

情報コミッショナーのもと、主に 5 つの部署に分かれている。それらは、人事や社内教育などを所管する総務部（Director of Organisational Development）、情報公開などを所管する情報の自由部（Deputy Commissioner and Director FOI）、プライヴァシー保護・個人情報保護を所管するデータ保護部（Deputy Commissioner and Director DP）、事業者への法執行を所管する執行部（Director of Operations）、法人担当部（Director of Corporate Affairs）である。なお、データ保護部の副コミッショナー（コミッショナーと呼称されているが、情報コミッショナーのような採用手続は必要なく、通常の職員としての採用手続による）は、ディヴィド・スミス氏（David Smith）である。

また、法的に要求されたものではないが、情報コミッショナーは、マネージメント・ボードによって支えられている。このボードでは、ICO の戦略やその遂行における監督経過の発展、その組織のガヴァナンス及び ICO への信頼の確保に対して責任を負っている。このボードは、3 ヶ月に 1 回、会合を開き、その構成メンバーは、ICO の執行メンバー 5 名と外部の専門家等 6 名からなる。このボードは、公平な組織運営を行っているという外部に対するアピールの面も有している。

③人事制度

情報コミッショナーは議会でなく、政府から指名される。その指名者を確定するために、政府が公開競争（open competition）の手続を行う。そこでは、司法省が担当組織（sponsoring department）となって、候補者リスト（short list）を作成し、面接を行う。その際には、利害関係者（stakeholders）によって構成されるパネルを組織し、そこで議論を行うが、このパネルをチェックする第三者の機関も存在する。

その後、このパネルが、候補者を総理大臣に推薦するが、総理大臣はこれを拒否することも可能である。もっとも、実際に拒否したケースはない。だが、現在の情報コミッショナーについては、議会で疑義が出され、議会は、この人事に関し介入する権限はないものの、議会の一般的な権限を行使して、現在のコミッショナーを召喚し質問している。なお、最後は、もちろん形式的な手続であるが、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））。

情報コミッショナー以外のスタッフは、同コミッショナーに人事権があることになっており（附則 5 第 1 章 4 条（1）（1A））、雇用契約はこの組織と結ぶことになっている。給与等については、コミッショナーによって決定される（附則 5 第 1 章 4 条（2）（3））また、その雇用契約は、任期制ではなく、すべて定年制の正規職員である。採用の契約主体は、情報コミッショナー・オフィスであるため、他の行政組織へと異動することもない。また、情報コミッショナーが変わったとしても、理由なくスタッフを解雇することはできない。その意味では、情報コミッショナーが人事権を有するとは、新しい職員を採用する際に、その権限を行使できるという方が正確である。

④職員数

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。2008/2009 年次報告書によれば、2008 年度は、常勤スタッフが 268 名、目的遂行のためのスタッフが 14 名の合計 282 名である。

さらに、2009/2010 年次報告書によれば、2009 年度は、常勤スタッフが 311 名、目的遂行のためのスタッフが 16 名の合計 327 名である。なお、2010 年末現在では、合計 352 名のスタッフが在籍しているという（現時点では、内訳は不明）。

このように、ICO の職員数は、ここ数年、増加傾向にあるといえる。

⑤予算

ICO の運営費は、データ管理者が毎年支払う登録料と司法省（政府）からの補助金で賄われている。

登録料は、前年比 16.6 パーセント増加の 13,192,000 ポンドであった。その増加分のうち、13 パーセントの 1,474,000 ポンドが高額な登録料（500 ポンド）によるものであり、残りの 3.6 パーセントの 408,000 ポンドが低額な登録料（35 ポンド）によるものである。ICO と司法省との合意文書の条件に従い、登録料の 3 パーセントを限度して、翌年へこれを繰り越すことが認められているが、2009/2010 年度には、1.3 パーセントの 169,000 ポンドが繰り越された。

司法省からの補助金は、2009/2010 年度で、前年度と同額の 5,500,000 ポンドであった。これも登録料と同様に、ICO と司法省との合意文書の条件に従い、補助金の 2 パーセントを限度して、翌年へこれを繰り越すことが認められているが、2009/2010 年度に繰り越されたものはない。

このように、具体的には、ICO の予算は、事業者の登録料により 70 パーセント強をカバーできてい

る。残りの30パーセント弱の予算は、政府からの補助金で賄われているが、政府からもらっている以上、独立性に疑問符がつくので、この財源をどうすべきかについては、継続的に内部で議論しているという。なお、この登録料によって、プライヴァシーの分野については予算的にすべてカバーできているが、このオフィスは、情報の自由についても所管しており、その部分について予算が分けられているわけではないため、同制度による収入は、そちらのほうへも割り当てられている。

（3）法的位置づけ

情報コミッショナーの法的根拠は、1998年のデータ保護法に求められる。同法では、第Ⅰ章序則の6条（1）（3）で、情報コミッショナー及び審判所（The Commissioner and the Tribunal）を設置することが定められている。

附則5第1章では、情報コミッショナーの地位、任期、俸給などについて規定している。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みられる。

- 単独法人である（1条（1））。
- 情報コミッショナー及びその職員は、女王の下にある機関とはみなされない（1条（2））。
- 任期は5年以内であり、再任も可能であるが、3回目以降の再任は、特別な状況の理由によって、それが公共の利益にとって望ましくない限り、なされるべきではない（2条（1）（5））。
- 定年は65歳に達する日の属する勤務年度の満了時、又は、それより早い年齢の場合には、15年の勤務を満了した時（2条（4））。
- 自ら辞職する場合（2条（2））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（2条（3））。
- 俸給及び年金の支給は、庶民院の議決で指定される（3条（1））。
- 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（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（10条）。

通常、イギリスの独立した行政機関は、公平性を保つため5,6人のメンバーで構成される委員会制度を採用している。コミッショナー1人に権限を集中させているICOの組織は特殊であるといえる。ICOは、EU指令から直接独立性確保が要求されているため、強い独立性が国内法によって確保されているのである。

すなわち、ICOの組織の位置づけをひとことでいうと、国家の統治上の（governmental）組織とはいえるが、政府（government）の一部の組織ではないということになる。つまり、いずれかの省庁のもとにあるわけではない。そのため、大臣などの命令に服することがない。それが、独立した監視機関の意味の中核である。

なお、予算の面をみればわかるように、あらゆる面において、政府から完全に独立した組織という

ものは存在しないが、他の独立した組織と比較すると、ICO はその独立性が高いといえるようである。

ところで、イギリスでは、周知のように成文化された憲法は存在しないが、議会の権限が広く解されているため、このような独立性のある機関を議会が定めることに、憲法上の疑義があるとは考えられていないようである。

（4）番号制度との関係

イギリスでは、2006 年 3 月 30 日、ID カード法（Identity Cards Act 2006）が成立した。この法律の制定経緯などについては、石井夏生利・堀部政男「イギリス」「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」（消費者庁、2009 年）を参照していただきたい。

この法律では、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、指紋といったバイオメトリクス・データ（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枠組みを定めている。

また、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、このコミッショナーは、主務大臣により任命されるものとなっている。このコミッショナーは、情報コミッショナーとは別に、同制度の運用及びその監視をするためにおかれた。

そして、2009 年 10 月 1 日に、ジョセフ・ピリング卿が、初めてのアイデンテティ・コミッショナーに指名された。2010 年 2 月 25 日には、同コミッショナー・オフィスの設立経緯や概要、同コミッショナーの職務内容や今後の計画などを示した最初の年次報告書も出されている。

実際、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 カードの発行が開始された。

ところが、その後、労働党から、保守党と自由民主党の連立政権に変化したことによって、2010 年 5 月に、ID 文書法案（Identity Documents Bill）が庶民院に提出された。この法案は、ID・カード法の廃止と、それに伴い、アイデンテティ・コミッショナーの制度の廃止することなどが盛り込まれている。そして、2010 年 12 月 21 日に女王の裁可を得て ID 文書法（Identity Documents Act）が成立した。その結果、アイデンテティ・コミッショナーのポストは消滅し、そのオフィスも閉鎖された。

3 監督機関の運用実態

（1）苦情処理・紛争解決

ICO は、国内における問題を中心として取り扱っており、その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記載されている。2009/2010 年次報告書によると、苦情処理や紛争解決などの数は、上昇傾向にあり、ICO の役割が大きくなっていることがわかる。

苦情や質問などの受付件数は、年によって異なるが、1984 年法の時代からみてみると、1999 年頃までは、概ね、2,000 件台から 4,000 件台で推移し、1999/2000 年次に、約 5,000 件へと達した。その後は急速な伸びを示し、2000/2001 年次は、約 9,000 件、その後、2004 年頃までは、11,000 件から 12,000 件程度、2004/2005 年次は、約 20,000 件、2005/2006 は、22,059 件、2006/2007 年次は、23,988 件である。2007/2008 年次は、24,851 件を受け付け、25,592 件（前年度からの繰越件数が含まれているため、受付件数を超えている）を処理し、1237 件が処理中である。2008/2009 年次は、25,509 件を受け付け、23,406 件を処理し、6442 件が処理中となっていた。

さらに、2009/2010 年次報告書によると、データ保護分野において苦情や助言などが求められた数は、過去最高の 33,234 件であり、前年比 30 パーセント以上の増加となった。そのうち、32,714 件が処理され、この処理件数は、前年比 40 パーセントの増加となった。その結果、2010 年 3 月末現在、データ保護違反の紛争の未処理数（処理中の件数）は、7,251 件となっており、前年の 2009 年 4 月 1 日時点の 6,680 件から 9 パーセントの増加となっている。

ICO は、紛争処理に係る時間短縮に努めており、1 年以上の処理期間のかかった紛争は 58 件であり、これは処理中の紛争の 1 パーセントにも満たない。6 ヶ月を超える紛争数は 1,315 件から 960 件に減少し、これは 27 パーセントの減少である。そして、75 パーセント近くの紛争が、90 日以下で処理されている。

ところで、2009/2010 年次報告書によると、ICO へ相談の電話が寄せられた数は 212,000 件を超えて、前年比 6 パーセント以上の増加となったという。ただ、この数字は、届出に関するものや情報提供など、文字通り「苦情」とはいえないものの処理にかかわる電話も含まれている。また、この数は、データ保護関係に関するもののみならず、情報開示など情報の自由に関するものも含まれている。

なお、実践的な助言を電話で提供することや情報豊かなウェブサイトの構築により、根拠のない苦情の数は 9 パーセント減少したという。

（2）データ保護法違反行為とその制裁・処罰

データ保護法違反行為の類型としては、以下の①～⑥のようなものがあるが、情報コミッショナー・オフィスでの聞き取り調査によると、具体的なプライヴァシー違反の事件としては、民間では、詐欺的に情報を得るなどのブラギング（bragging）行為（55 条）に関するものが多く、他方、公的組織では、適切な管理体制や措置などに関するものが多いという。

①届出義務違反

データ管理者は、届出義務があることから、19 条によって求められている情報コミッショナーの登録がなされていない段階で、個人データを取り扱ってはならず（17 条（1））、これに違反すると有罪となる（21 条（1））。また、届出事項の変更義務に関する 20 条（1）のために定められた届出規則（notification regulations）によって課された義務に違反する者も、有罪となる（21 条（2））。

②評価前取扱い禁止義務違反

22 条（2）で示す届出が情報コミッショナーに対してなされた際（22 条（2）は、コミッショナーの届出に対する評価義務について定める）、当該届出を情報コミッショナーが受領してからから 28 日（若しくは、（4）に該当する場合には、この期間が（4）のもと延長される）（22 条（4）では、特別な状況下における理由がある場合には、この期間の延長ができる旨を定める）が経過するか、又は、その期間の最終日（若しくは延長されたその期間）までにその処理に関して（3）に基づくコミッショナーからの通知をデータ管理者が受領した場合を除き（22 条（3））では、コミッショナーの 28 日以内の回答義務について定める）、評価対象となるいかなる取扱いもしてはならない（22 条（5））。この規定に違反したデータ管理者は有罪となる（22 条（6））。

③情報開示義務違反

個人データが 17 条（2）（3）のため同条（1）が適用されずに処理された場合、又は、データ管理者がその処理に関する届出事項を 18 条に基づいて届出ていないにもかかわらずそれが処理された場合、データ管理者は、私人からの文書による要請を受領後 21 日以内に、その者に文書で関連する届出事項を無料で入手可能な状態にしなければならない（24 条（1））。これに違反するデータ管理者は有罪となる（24 条（4））。

④通知義務違反

執行通知、情報提供通知又は特別情報提供通知に従わなかった者は、有罪となる（47 条（1））。さらに、情報提供通知又は特別情報提供通知に従おうとする際に、内容が虚偽であることを知りつつ文書を作成、又は、内容が虚偽を含む文書を認識ある過失（recklessly）によって作成した者も有罪となる（47 条（2））。

⑤海外情報制度の検査妨害

情報コミッショナーは、シェンゲン情報制度（ヨーロッパの国家間において国境検査なしで国境を越えることを許可する協定に基づく制度）、ユーロポール情報制度及び税関情報制度に記録されている、いかなる個人データも検査することができる（54A 条（1））。故意にこの検査権限の行使を阻害した者、又は、この権限を行使する者に対して、合理的な理由なく、合理的に要求された援助を怠った者は有罪とする（54A 条（6））。

⑥個人データの不法な取得等

55 条（1）では､個人データの不法な取得等（unlawful obtaining etc. of personal data）について、次のように定められている（55 条（2）では適用除外について定める)。

「何人も、データ管理者の同意なく、故意又は認識ある過失（recklessly）によって、

(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若しくは公開、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。」

そして、同規定に違反した者は、有罪とすると定められている（55 条（3))。また、同規定に違反して個人データを取得した場合にそのデータを販売する者は有罪とすると定められている (55 条 (4))。さらに、同規定に違反して個人データを取得した場合又はその後、同規定に違反してそのデータを取得した場合に、個人データを販売する申出をした者は有罪となると定められている（55 条（5))。

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）の 161 条が、1984 年データ保護法 5 条の罰則を拡大した。同法 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、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。

⑥法定刑

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

なお、2008 年 5 月 8 日、女王の裁可を受けて成立した刑事司法及び入国管理法（Criminal Justice and Immigration Act）の 77 条は、個人データの不法な取得等に関する処罰の変更権限（Power to alter penalty for unlawfully obtaining etc. personal data）について定めており、1998 年データ保護法の処罰に比べると、拘禁刑を含むという厳格な形で改正している（77 条（5）参照)。

77 条（1）(2）の規定は、次のように定められている。

(1) 主務大臣は、命令により、1998 年データ保護法 55 条の罪を犯したものに対し、以下の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、所定期間内での拘禁刑若しくは法定の上限額を超えない金額での罰金を科し、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、所定期間内での拘禁刑若しくは罰金を科し、又はこれを併科する。

(2) (1) (a) (b) に定める「所定期間」は、その命令により定められる期間を意味するが、以下に定め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 月（北アイルランドでは 6 月)、また、

(b) 正式起訴状に基づく有罪判決による場合、2 年

この規定に従い、主務大臣が命令を制定する際には、情報コミッショナー、また、主務大臣が適当と考えるメディア組織及びその他の人々と協議しなければならない（77 条（4））。

（3）権限行使

①執行通知

情報コミッショナーの権限のひとつとして、データ保護法違反を解消するように命じる内容の執行通知の送達（Enforcement Notices）が認められている（40 条）。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、それほど多くない。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 年次報告書によると、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いう。2007/2008 年次報告書によると、5 つの警察組織や Marks & Spencer などに対して、9 件の執行通知を発したという。2008/2009 年次報告書によると、自治局（Department for Communities and Local Government）や防衛省（Ministry of Defense）などに対して、6 件の執行通知を発したという。さらに、2009/2010 年次報告書によると、グラスゴー市議会のほか、エンジニア会社、建設会社、鉄道会社、石油・ガス会社などに対して、15 件の執行通知が発せられたという。

なお、執行通知に不服のあるデータ管理者は、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。

②監査

ICO では、定期的に、事業者がデータ保護法を遵守しているか検査するため、その同意を得て、監査（consensual assessment, audit）を行っている。2009/2010 年次報告書によると、ICO では、16 の政府、地方、厚生に関わる公的機関及び私的な組織に対して、立入による法令遵守の監査を実施したと記されている。なお、これらの監査に対する反応は、総じて肯定的なものであり、問題のある部分に対処する計画について合意（undertakings）がなされたという。

ICO では、よりリスクを基礎とした（risk-based）監査報告を提供するため、この監査能力の向上に努めており、監査方法を修正している。

なお、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たことを受けて、首相がICOに対して、政府機関への抜き打ち検査（spot check）権限を認めた。このため、ICOでは、2008/2009年次には、労働及び年金局（Department for Work and Pensions）と運転免許証付与機関（the Driver and Vehicle Licensing Authority）に対してこの権限を行使した。

③訴追

データ保護違反があった場合、情報コミッショナーは、法廷において、検察官として活動することが可能である(60条(1))。もっとも、訴追は最終的な手段である。法律上は、検察官又はプライヴァシー・コミッショナーが訴訟を追行するものとなっているが、現実には、検察官にお願いすることはほぼない。情報コミッショナーの権限を行使すれば、証拠を収集することは可能であるし、それに関与し事件を良く知る情報コミッショナーが訴訟を追行した方がより合理的だからである。ちなみに、ICOの執行部（Enforcement Section）には、もと警察官も採用している。但し、スコットランドでは、検察官がすべて法廷に立って訴訟を追行している。

2007/2008年次報告書では、11件の訴追が行われ、103件の有罪認定がなされた。このうち、3件の訴追及び90件の有罪認定が55条違反である。2008/2009年次報告書では、届出義務違反に対して、10件の訴追がなされた。そのうち、6件がソリシタに対するもので、4件が会計士に対するものである。2009/2010年次報告書では、これまでに、データ管理者としてICOへの届出を怠った7つの私人や組織に対して起訴していることが記されている。

2009/2010年次における2つのケースでは、刑事法院（Crown Court）で起訴され、そのうちのひとつでは、5,000ポンドの罰金刑が科された。もうひとつのケースでは、支配人（director）が法人と共に処罰されたという。また、ICOでは、執行通知に対応しなかった2つの機関を起訴しところ、いずれも有罪と判断されたという。ひとつは個人であり、その者は、届出義務違反でも起訴され、刑事法院で審理されたが、もう1つでも有罪とされ、計5,200ポンドの罰金刑を受けている。

2008/2009年次の間、ICOは、建設業界で秘密のブラックリストが出回っているとの疑惑を調査した。このリストは、組合活動などの理由で、同業界で働くことが不適であると考えられる人々の詳細を明らかに含むものであった。ICOの調査の結果、コンサルティング協会（Consulting Association）といわれる組織が、そのようなデータベースの管理者であることが明らかとなった。その結果、Ian Kerr（コンサルティング協会の代表している）事件は、2009年7月に、治安判事が彼らの刑の宣告権限では不十分と考えたため、Knutsford刑事法院へと委ねられた。被告人は、5,000ポンドの罰金と裁判費用1,187ポンド20ペンスの支払いが命じられた。この事件は、その起訴後、テレビや一流紙などからの多くの注目を集めたようである。

④金銭的制裁

(a) 制度概要

2008年の刑事司法及び入国管理法144条（1）で新しく導入されたものであり、2010年4月6日

より施行されている、情報コミッショナーによる金銭的制裁の制度が重要である（55A 条、55B 条）。司法手続きを経ずに、情報コミッショナーが、重大なデータ保護法違反に対して、高額の金銭的制裁を科すことを認めるものであり、今後重要な役割を果たすと考えられるからである。

この制度の運用の指針を示すものとして、データ保護法 55C 条（1）のもと、解釈指針（Statutory Guidance）が設けられており、それは ICO のウェブサイトでも掲載されている。また、2010 年のデータ保護（金銭的制裁と通知）規則（Data Protection（Monetary Penalties and Notices）Regulation）及び同年のデータ保護（金銭的制裁）命令（Data Protection（Monetary Penalties）Order）も参照すべきである。

情報コミッショナーは、4 条（4）（データ管理者のデータ保護原則遵守義務）の重大な違反行為があった場合、又は、違反行為が実質的な財産的損害若しくは精神的損害を引き起こす可能性の高い場合であり、かつ、以下の要件を充足する場合に、金銭的制裁通知（a monetary penalty notice）をデータ管理者へ送達することができる（55A 条（1））。その要件とは、当該違反行為が故意によるものであり、当該違反行為が生じる危険性のあったこと、及び、その行為が実質的な財産的損害又は実質的精神的損害をもたらす虞の高い類のものであったことをデータ管理者が知り若しくは知るべきであったにもかかわらず、その違反行為を阻止するための合理的な措置をとらなかった場合である（55A 条（2）（3））。

この金銭的制裁通知とは、データ管理者へ情報コミッショナーが決定した金銭の額を、この通知で定められた期日までに、同コミッショナーへ支払うことを求める通知である（55A 条（4）（6））。このコミッショナーによって決められる額は、定められた額を超えてはならないが（55A 条（5））、その上限は、500,000 ポンドと高額である。なお、指定された期日までに支払いをすれば、20 パーセントまでの減額措置がなされる。そして、同条の下コミッショナーによって受領された金銭は、統合基金（Consolidated Fund）へと支払われる（55A 条（8））。

金銭的制裁通知を送達する前に、情報コミッショナーは、データ管理者に対して目的を示した通知（a notice of intent）を送達しなければならない（55B 条（1））。この通知は、情報コミッショナーが金銭的制裁通知を送達する予定であるということを示す通知である（55B 条（2））。

ところで、支払われた金銭はすべて国庫に納められるため、ICO の予算の一部となるわけではない。とすれば、国庫から与えられた予算で活動する公的組織のお金からプライヴァシー違反の支払いをなし、そのお金がまた国庫に戻るということになる。これでは、公的組織に対する支払い命令をしても意味がないのではないかという指摘もある。しかし、事実上、その組織では、予算が縮減されることになるし、その組織の評判も傷つくことになるため、IOC では、このような制度に十分意味があると考えている。

また、ICO が有効に金銭的制裁を科すことができるようになったメリットとして、プライヴァシー違反に対する一貫した措置をとることができるようになったことがあげられる。たとえば、以前は、銀行が顧客情報を流失した場合、監督官庁から金銭的制裁が科されていたが、病院がそうした場合、法の定めがなかったため、監督官庁から金銭的制裁を科されることはなかった。しかし、現在では、すべての組織に対して、ICO が一貫して、金銭的制裁を科すことができる。

なお、この支払命令に応じれば、事件は終結したものとして処理され、その後、刑事事件として裁判所へ訴えられることはない。

（b）具体的な制裁措置

情報コミッショナーは、2010 年 11 月 24 日に、深刻なデータ保護法違反をした 2 つの組織に対して、初めて金銭的制裁を科した。

まずひとつ目は、Hertfordshire 郡議会の職員が極めてセンシティヴな個人情報を誤った相手先にファックスしたという 2 つの深刻な事件を理由として、同議会に対して 100,000 ポンドの金銭的制裁が科された。第一事件は、児童の性的虐待を含むものであり、法定で審理された。第二事件は、児童保護手続（child care proceedings）の詳細を含むものであった。

ふたつ目は、Hull と Leicester において地域の法律助言センターを利用した 24,000 人に関する個人情報を含む匿名化されていないラップトップを紛失したことを理由として、雇用サーヴィス会社 A4e に対して、60,000 ポンドの金銭的制裁を科した。

その後も、ICO では、2011 年 2 月 8 日に Ealing 議会に対して 80,000 ポンド、また、Hounslow 議会に対して 70,000 ポンドの金銭的制裁を科している。いずれのケースも、個人情報を含む匿名化されていないラップトップの紛失について責任が問われた。さらに、2011 年 5 月 10 日には、およそ 6,000 人のセンシティヴ情報を適切に保管していないという理由で、元ソリシタ法律事務所 ACS Law として開業していた Andrew Jonathan Crossley 氏に対して、1,000 ポンドの金銭的制裁を科した。

（4）国際連携

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・出席している。この部会では、EU 域内のプライヴァシー保護の取組、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などについて検討されており、年 4 ～ 5 回の会合が開かれるほか、特定のプロジェクトのため、サブグループが構成されることもある。

ICO は、EU 以外に関与している国際会議として、コミッショナー会議とベルリングループによる会議を重要視している。後者は、ベルリンのコミッショナーが始めたことから通称でそのように呼ばれているが、正式には、テレコミュニケーションにおけるデータ保護に関する国際的作業部会（International Working Group on Data Protection in Telecommunication）という。

その他にも、OECD の WPISP（Working Party on Information Security and Privacy）にも出席しているが、ご存知のとおり、OECD は原則として政府関係者のみ出席するものであるから、その関係者（情報セキュリティの担当者）と共に行って、必要な場合に ICO がコメントするという形をとっている。また、欧州評議会も以前は積極的に関与していたが、近年は、政府が関与していることから、ICO はあまり関心を有していない。

さらに、ICO は、ユーロポール（the Europol Information System）、関税情報システム（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（54 条（1）参照)。

4 監督機関の課題等

（1）法改正の動向

情報コミッショナーの地位やその権限については、現在大幅な法改正が予定されている。その法案の名称は、自由の保護法案であり、同法案では、指紋及び DNA プロファイルの保管や破棄、監視カメラ、不均衡な執行行為からの財産の保護、傷つきやすい集団への保護、犯罪記録の保護など幅広い内容が盛り込まれている。そして、情報コミッショナーについては、主に次のような改正が予定されている。

・任期を 5 年から 7 年に延長（101 条（1））
・両議院の勅語奉答文（the Address）に従い、女王によって解任されるが（データ保護法附則 5 第 1 章 2 条（3））、議院でその動議を出す要件を明記（101 条（2））
　たとえば、情報コミッショナーが少なくとも 3 ヶ月間その職務を遂行しないこと、指名の条件に従わないこと、犯罪者として有罪判決を受けることなどが要件とされている。
・65 歳の定年年齢及び再任の規定の削除（101 条（3））
・主務大臣（Secretary of State）の承認（approval）が必要とされていた評価通知に関する実務規範、データ共有の規範、罰金通知に関する指針について、基本的に、その協議（consultation）で足りるとすること（102 条）
・一般的な権限としての費用を課す権限（データ保護法 51 条）を行使する際に必要とされている主務大臣の同意を不要とすること（103 条（1））
・職員数や条件などに関して必要とされている主務大臣の同意を不要とすること（104 条（3））

情報コミッショナーの任期に関して、ICO としては、5 年では長期的な視野にたった運営・執行を行うことができないことから、任期を 7 年とするよう主張している。つまり、再任不可という法案には賛成しているが、5 年では短いと考えている。

また、コミッショナーの解任については、政府がこれを単独ですることはできず、厳格な要件のもと、両議院の同意が必要とされているが、同法案では、この要件をより厳格とすることが求められている。

さらに、コミッショナーの定年制度は、年齢による差別が問題とされている。欧州では、このように差別禁止を根拠として、あらゆるポストで定年制度を廃止する傾向にある。

なお、同法案には、指紋や DNA のデータを保管する制度に関しても、重要な修正が含まれている。たとえば、責任のある警察署長（chief officer of police）にとって、指紋の取得や DNA プロファイルの由来するサンプルの取得が違法、または、逮捕に伴うそれらの取得に際してその逮捕が違法若しく

は人違いに基づくものであると考えられる場合、それらの情報は削除されなければならないと定められている（1 条（2））。

また、同法案では、主務大臣は、保管とバイオメトリクス（生体認証）素材の利用のためのコミッショナー（the Commissioner for the Retention and Use of Biometric Material）を指名することが求められており（20 条（1））、その権限や役割についても定められている（20 条（2）- （7）、21 条、22 条（4））。

このコミッショナー制度は、監視カメラについても（the Surveillance Camera Commissioner）求められている（34 条（1））。また、その権限や役割についても定められている（34 条（2）- （4）、35 条）。

なお、現在の政権は、プライヴァシー保護に対する関心が高く、IOC では、この法案が通過する可能性が高いと考えている。

（2）EU データ保護指令との関係

イギリスは、これまで、EU データ保護指令と整合的に対応していると考えられてきた。ところが、2010 年 10 月 6 日、欧州オンブズマンは、欧州委員会の委員長であるバロッソ（Barroso）氏に対して、イギリスの EU 保護指令への対応の問題点に関する同オンブズマンの勧告草案について、同委員会の意見を求める文書を提出した。

このオンブズマンの勧告は、クリス・パウンダー（Chris Pounder）博士からの不服申立に基づくものである。それに対して、同委員会は、2011 年 2 月 14 日に、その勧告草案に対する次のような意見を同オンブズマンへ送達している。

Ⅰ 事実関係・経緯の背景・要約

欧州委員会は、当初の不服と欧州オンブズマンが不服申立人へ送達したそれに対する見解、不服申立人によって示された追加的要望・意見、不服申立人によって示された要望・見解への回答を同委員会に求める同オンブズマンの要望、より詳細な情報への要望に関する同委員会の意見、同オンブズマンの友好的な解決の提案及びそれに対する同委員会の回答について言及する。同オンブズマンは、既に分析を行い、結論を出している。

Ⅱ 欧州オンブズマン勧告

同オンブズマンは、同委員会が、イギリスの違反手続に関して求められた情報の要約を不服申立人に提供すること、または、それが不可能な説得的な理由を送達することを勧告している。

Ⅲ 欧州オンブズマンの事実認定や提案に対する欧州委員会の意見

欧州司法裁判所が Petrie 事件で確認し、また、オンブズマンの質問のための DG コーディネーターの半期に一度の第二回目会合が 2010 年 11 月 30 日に行われた際に、同オンブズマン事務所の法務部の長である M. ジョアオ・サンタナ（Joao Sant'Anna）氏が認めたように、同委員会は、違反手続の処理、その調査の目的のための、また、適正手続の利益となる関連する職務に関し秘密を保持する義務に服する。このような義務は、要約された情報の提供を排除するものではないが、この手続において、個々の主張を詳細に述べるべきではない。

IV 結論

2010 年 12 月 16 日付の文書によって（コピー添付)、同委員会は、不服申立人に対してより詳細な情報を送達した。しかしながら、同委員会は、それが先例となるとは考えていない。

添付：2010 年 12 月 16 日付の欧州委員会からクリス・パウンダー（Chris Pounder）博士宛の文書

この文書では、「イギリスの指令 95/46/EC の実施状況」と題して、イギリスに対する違法手続に関する要約された情報について記されている。そして、イギリスが違反しているのではないかと疑われている指令 95/46/EC の条文は、第 2、3、8、10、11、12、13、22、23、25、28 条であることが指摘されている。各条との関係における具体的な問題点は次のとおりである。

- 第 2 条に関する問題は、指令の定義よりも狭いように思われるファイリング・システムの定義及びデュラント事件判決におけるこの定義の解釈に関するものである。
- 第 3 条に関する問題は、イギリスのデータ保護法が、単なる家庭での活動（household activity）よりも広いように思われる娯楽（recreational）目的を含む表現を含むことにに関するものである。
- 第 8 条に関する問題は、刑事犯罪に関するデータを他のセンシティヴ・データと異なる取り扱いをしているか否かということについてである。
- 第 10 条及び 11 条は、データ管理者がデータ主体に対して提供すべき情報を明示しているが、この情報が、データ主体から得たものか、それ以外のところから収集したか否かによっても異なる。データ保護法は、データ管理者が公開を義務付けらテレいるデータに対して、この義務を解除しているように思われる。
- 第 12 条は、データ主体に対して自らのデータの正確性を調査し、そのデータが最新のものであることを確保し、必要であれば、そのデータを修正、削除若しくはブロックしてもらう権利を与えている。しかしながら、データ保護法は、この点に関して、データ主体による申出を容認又は拒絶する裁量を裁判所に与えているように思われる。
- 第 13 条に関する問題は、データ保護法においてデータ主体が秘密事項にアクセスする権利を除外することに関するものである
- 第 22 条は、司法的救済について定め、第 23 条は、加盟国に対し、データ処理違法なデータ処理の結果生じた損害に対する賠償を認めることを求めている。データ保護法は、非物理的損害（non-material damage、非財産的損害）の範囲を狭めているように思われる。
- 第 25 条に関する問題は、イギリスのデータ管理者が、個人データを第三国へ移転する場合の保護水準の十分性評価について監視される程度に関するものである。
- 第 28 条に関する問題は、イギリス監視機関の調査権限の十分性に関するものである。

以上のように、欧州委員会は、第三者期間としてのイギリスの情報コミッショナーの権限のみならず、イギリスのデータ保護法とその運用全般に疑問を呈していると考えられ、今後の不服申立手続の動向を注視する必要がある。

＜参考文献＞

・石井夏生利「個人情報の窃取・漏えいと刑事罰」堀部政男編『プライバシー・個人情報保護の新課題』（商事法務、2010 年）93 頁。

・石井夏生利・堀部政男「イギリス」「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」（消費者庁、2009 年）

＊ イギリスのデータ保護法の制度やその運用については、ICO のホームページが充実しており、大変参考になる（www.ico.gov.uk）。本稿も、上記文献のほか、これを基礎に作成している。

ii. フランス

本章を執筆するにあたり、平成 23 年 3 月に行われたヒアリング調査において、情報処理及び自由に関する全国委員会（Commission nationale de l'informatique et des libertés）（以下、「CNIL」という。）Pascale Raulin-Serrier（欧州・国際担当）、Christophe-Alexandre Paillard（法・国際・IT 担当）、Norbert Fort（苦情処理担当）、Emmanuelle Bartoli（欧州・国際担当）、政策研究財団 Jean-Francois Daguzan（主任研究員）、Frederic Coste（研究員）、Jean-François Clair（元仏内務省国土監視局次長）から詳細な回答をいただいた。ここに協力していただいた方々に謝意を記す。

1　個人情報保護法制の概要

（1）法律名

「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」

2004 年 8 月 6 日の法律第 2004 － 801 号（以下、「法」という。）で大幅な改正が行われた[1]。2009 年 5 月 12 日にも法改正が行われた。

（2）目的

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、人権、私生活、又は個人の自由ないし公的な自由を侵害するものであってはならない。（法第 1 条）

（3）適用範囲

個人情報を「自然人に関するあらゆる情報のうち、識別番号または個人に固有の一もしくは複数の要素を参照することによって、直接または間接に個人を識別しまたは識別可能なもの」と定義している（法第 2 条）。

なお、IP アドレスを個人データに該当しないと判断した 2007 年 4 月 27 日[2] と同年 5 月 15 日[3] の控訴院の判決の後、2009 年 1 月 13 日、フランス破棄院（Cour de cassation）がインターネット接続業者を特定するための IP アドレス（本件では固定アドレスか可変的なアドレスであるかの区別の検討をしていない。）については CNIL への事前届け出をしない旨の判決[4] を下した。

1　同法の紹介については、「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」（内閣府・平成 21 年 3 月）（フランス：下井康史）をもとにしている。

2　Cour d'appel de Paris, 13ème chambre, section B Arrêt du 27 avril 2007.

3　Cour d'appel de Paris 13ème chambre, section A Arrêt du 15 mai 2007.

4　Cour de cassation Chambre criminelle Arrêt du 13 janvier 2009.

しかし、フランス上院においてはEUデータ保護指令に照らし、IPアドレスが個人情報に該当することを断言する旨の提言として出され[5]、結局、2009年5月15日の知的財産法の改正[6]により、IPアドレスを含むインターネット通信へのアクセス権限が規定され、IPアドレスを用いた事業についてはCNILへの届け出が必要となった。

（4）内容

主な権利・義務に関する内容としては、次のような規定がある。

・公正かつ適法な収集・処理、収集の目的の特定・正当性、情報の正確性、目的に必要な期間のみの情報の収集・処理等の基本原則が定められている（法6条）。個人情報の処理には、本人の同意を得ることが原則とされている（法7条）。

・すべての自然人は情報処理を拒否する権利のほか、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・消去請求権が認められている（法39条）。

・個人情報処理責任者は、安全管理義務を履行しなければならない（法34条）。

（5）監督・登録制度

法においては、電子処理ファイルを作成・保有する場合に、CNILへの簡易届出が必要な場合、CNILへの許可が必要な場合、CNILによって発議され表明された意見に対する所管の大臣のアレテによる許可が必要な場合、などの指定がなされている。

事前手続の概要については、下記のとおりになっている[7]。

あらゆる事前手続を必要としない場合（法22条2項、同3項）	非営利目的、および宗教的、哲学的、政治的、労働組合的な性格を有する結社等によって処理される場合など
CNILへの簡易手続が必要な場合（法24条1項）	私生活または自由への侵害のおそれを生じない処理が行われる、個人情報の通常の類型
CNILによる許可が必要な場合（法25条）	遺伝情報を対象とする一定の自動処理や犯罪、刑罰、または保安上の措置にかかわる情報を対象とする自動処理もしくは非自動処理など
CNILによって発議され表明された意見に対する所管大臣のアレテによる許可が必要な場合（法26条1項）	国家の保安、国防、または公の安全に関する情報の処理など

5 Par M. Yves DETRAIGNE et Mme Anne-Marie ESCOFFIER, Rapport D' Information n °441 (2008-2009) La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information 98.

6 L.331-37 du Code de la propriété intellectuelle.

7 詳細については、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」人間文化研究5号（2006）168頁、参照。

CNIL によって発議され表明された意見に対するコンセイユデタの議を経たデクレによる許可が必要な場合（法 27 条 1 項・26 条 2 項）	一定のセンシティブ情報や住民登録全国台帳における個人登録記載者の情報につき、国、公法人または公役務を管理する私法人のために行われる個人情報の処理など
CNIL によって発議され表明された意見に対する、アレテによる許可もしくは、公施設法人または公役務を管理する私法人につきその審議機関の決定によって当該法人のための処理が行われる場合（法 27 条 2 項）	フランス本国及び海外領土での国勢調査に関する処理など
CNIL への届出が必要な場合（法 22 条 1 項）	上記してきた特別な処理の場合を除き、個人情報の自動処理

（6）その他

○プライバシー権について

1970 年に新設されたフランス民法第 9 条[8]には私生活を尊重される権利の保障が規定されており、データ保護は 1789 年の人権宣言第 2 条[9]とそれを受けた憲法によって間接的に保障されている。1978 年情報の処理・ファイル・自由に関する法律（2004 年改正）は、「人間のアイデンティティ…、私生活…を侵害してはならない」（1 条）と規定され、また「アクセス権の行使（droit d'accés)」が規定されていることから、いわゆる「自己情報コントロール権」が保障されていると理解されてきた[10]。

○主な憲法院判決[11]

・自動車検問に関する判決（1977 年 1 月 12 日）

司法警察員などに自動車検問に関する広範な権限を与える法律の条文は、個体の自由の基礎にある本質的原理を侵害し、したがって憲法に適合しないものである。

・自動車のビデオ監視に関する判決（1995 年 1 月 18 日）

私生活尊重件を無視することは、個体の自由を侵害するという性質をもちうる。

主な破棄院判決[12]

・氏名・私生活：映画内容の部分的削除（1985 年 2 月 13 日）

ある映画において、有名な犯罪者がある親子の実名をフルネームで登場させた事件において、その親子の実名を使用しながら家族の日常生活、家庭生活をあからさまにしており、また一部分はフィ

---

8 フランス民法（1970 年 7 月 17 日）9 条「何人もその私生活を尊重される権利を有する」。

9 フランス人権宣言第 2 条「全ての政治団体の目的は、人の、生れながらにして侵すことのできない権利を守ることにある。ここで言う権利とは自由、所有、安全、そして暴虐への抵抗の権利のことである。」

10 内野正幸『表現・教育・宗教と人権』（弘文堂・2010）87 頁。

11 内野・前掲。

12 皆川治廣『プライバシー権の保護と限界論』（北樹出版・2000）45 頁以下、参照。

クション化が行われているものの、関係者の同意なくして実名を使用したことを私生活の侵害になりうると判示した。

なお、フランスにおいては、アメリカで使用されるプライバシーに相当する言葉は用いられず、私生活を尊重される権利の中においてプライバシー権が議論されてきた[13]。この点、フランスにおける私生活を尊重される権利は、人間の尊厳を基礎として、性生活、医療、死生観に関する事柄まで含むため、アメリカのプライバシー権よりも広く保障されるという指摘もある[14]。

○フランスのデータ保護に関する一般的な考え方

政策研究財団 Daguzan 氏からのヒアリングによれば、フランスにおけるデータ保護の一般的な考え方は次のとおりである。

・Big Brother に象徴されるように、われわれは常に政府のデータの作成に対しては懐疑的である。商業目的のデータベースの作成はそれほど大きな問題ではないが、防衛・警察によるデータベースの作成に疑いの目を持っている。防衛・警察・税務当局が保有するデータは相互関連付けが行われてきたことが深刻な問題となっている。そのため、CNIL のチェック機能の強化が期待されてきた。
・国家のデータベース作成に懐疑的であるのは、第二次大戦中における権威主義的な体制が歴史的要因となっている。フランスでは特にこの傾向が強い。同じ EU でもイギリスは監視カメラ（CCTV）が街のあらゆるところに設置されており、データベース作成に対する国民意識は異なる。
・哲学的な背景としては、強力な政府、すなわち、大統領権限の集中や中央政府によるデータ監視に対しては、右派からも左派（特にフランスではジャコバン派）からも懐疑的である。

2　監督機関の制度概要

本章は特に断りのない限り、CNIL でのヒアリング結果及び CNIL の年次報告書（2009 年）をもとにまとめている。

（1）制度の概要

・名称

情報処理及び自由に関する全国委員会（Commission nationale de l'informatique et des libertés）（以下、「CNIL」という。）

---

13 佐藤雄一郎「フランス憲法における私生活尊重権について」東北法学 24 号（2004 年）55 頁、北村一郎「私生活の尊重を求める権利」北村一郎編『現代ヨーロッパ法の展望』（東京大学出版会・1998）215 頁、参照。

14 See Jeanne M. Hauch, Protecting Private Facts in France: The Warren & Brandeis Tort Is Alive and Well and Flourishing in Paris, 68 TUL. L. REV. 1219 (1994).

（2）設置の経緯

1970 年代初頭「サファリ（SAFARI）（Système automatisé pour les fichiers administratifs et le répertoire des individus）」[15] プロジェクトの下、国家統計局（Institut national de la statistique）が社会保障番号（Numéro d'Inscription au Répertoire（通称 NIR））を個人識別のための排他的な道具として用い、教育、軍隊、医療、税、雇用等に関係する他の行政機関とのデータ・マッチングを可能とさせることとなった。このような行政機関が保有する個人のファイルの自動処理の進展に伴い個人の自由が脅かされるという国民の危惧が高まり、スウェーデンのオンブズマンをモデルにして、1978 年の情報処理、情報ファイル及び自由に関する法律の制定とともに新たな機関として CNIL が設立された。

CNIL はフランスにおいて初めての独立行政機関（Autorité administrative indépendante）である。そもそも、CNIL のような独立行政機関が設置された背景には、1945 年に創設された番号制度に対する議会における強い反対論があった。番号制度については、私的自由を侵害するため右派と左派との間で独立行政機関の必要性に関するコンセンサスがあった。

近年、この 20 年間で独立行政機関が多く作られすぎた（約 40 の機関がある）ことから、独立行政機関の再組織化が必要となり、統合化されてきた。なお、番号制度にも関連して、CNIL は行政文書へのアクセスに関する独立行政機関（Commission d'Accès aux Documents Administratifs）（以下、「CADA」という。）と協働することがしばしばある。

（3）法的地位（委員会、人員、予算、人事、権限、他機関・地方との関係）

①独立行政委員会について

そもそも独立行政委員会（autorité administrative indépendante）は、「本質的に基本的人権と経済活動にかかわる部門において、独立規制の組織を設置するという要請に応えたもの」であり、「独立性を理由として、行政内部で特別な地位を占めている」[16]。これらの独立行政機関は、後見的なものであれ（一般的に法人格を有していないため）、階層的なものであれ（独立であるため）、古典的な統制を免れていることから、「政府は、行政…を司る」[17] と規定する 1958 年憲法 20 条 2 項の合憲性が問題となる。この点、憲法院は職権で憲法 20 条 2 項の適合性を審理するのを自制しており、憲法院の

15「フランス人狩り」とも呼ばれ、行政による個人情報保護侵害の危険性が指摘された。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」立命館法学 2005 年 2・3 号（2005）146 頁。

16 P. ウェール /D. プイヨー著、兼子仁・滝沢正訳『フランス行政法』（三省堂・2007）36-37 頁。

17 初宿正典・辻村みよ子『新解説世界憲法集〔第 2 版〕』（三省堂・2010）243 頁〔フランス第 5 共和国憲法・辻村みよ子訳〕。

判例から少なくとも明示的に独立行政委員会の違憲性の判断を導くことはできないと理解されている[18]。また、(Décision n° 2004-499 DC du 29 juillet 2004) CNIL[19]

また、フランスにおいて初めて設置された独立行政機関としての CNIL に対しては、独立性と決定権限の現実的運用に対する懐疑的な立場と、その権限行使の正当性に対する問題視する見解があった[20]。前者については、CNIL には効果的な介入を行うための手段を欠いている、というものである。政策研究財団 Jean-Francois Daguzan 研究員に対する今回のヒアリングにおいても、CNIL の権限の実効性を疑問視する指摘がされた。実際に、CNIL がこれまで介入してきた領域は介入を特に必要とする新たな分野が多く、また、CNIL の権限行使は市民に受け入れられやすい調整を行うなど、全般的に消極的であった。

他方、CNIL の権限行使の正当性については、フランスの政治的思考において主権と公の意思を称える民主政を採ってきているため、選挙によって選出されていない委員による金権政治や賢者による統治といった批判はもっともなものであった。同じく独立して権限を行使する裁判官については、憲法上の正当性が一定程度認められるのに対し、独立行政機関については伝統的にも憲法上もその正当性を裏付けるものはない。

CNIL に対してはこれらの批判があり、行政、立法、司法という三権に基づくフランスの政治・法的伝統にもかかわらず、CNIL は制度改革をもたらした「専門化された第四権力」としての地位を維持し、長年の実績から一定の敬意を払われる機関となった。いかなる独立性も、既存の権力・体制を犠牲にしない限りはそのような機関としての地位に相当しないのであって、しだいに自分の居場所を見つけ、他の機関からも受容されてきた。このように、CNIL は「自由の協会（Academy of liberties)」として存続してきた。

②委員会について

17 名の委員で構成される。6 名の裁判官、4 名の国会議員、2 名の経済・社会評議会委員、2 名の上院・下院議長任命の IT 専門家、3 名の首相任命の IT または市民的自由の専門家から成る。委員長と 2 名の副委員長は委員会委員の選挙によって選出される。任期は 5 年で、再選可能であるが 10 年を超えてはならない。ただし、議員の場合は、議員任期終了まで。委員に対する報酬は CNIL から一切支出されていない。

週 1 回、毎週木曜に総会が開催される。総会では 1 回につき通常は 2 つの事例について審議される。各省庁の担当官や民間の事業者が呼び出され、審議が行われる。総会には、法律や技術の専門家が呼ば

18 清田雄治「フランスにおける『独立行政機関 (les autorité administrative indépendante)』の憲法上の位置」立命館法学 2008 年 5・6 号（2008）130 頁。

19 本判決の紹介については、清田雄治「フランスにおける個人情報保護の憲法的保障」政策科学 13 巻 3 号（2006）45 頁、参照。

20 Andre Vitalis, France, in GLOBAL PRIVACY PROTECTION 124-5 (JAMES B. RULE & GRAHAM GREENLEAF eds., 2008).

れ、意見を述べることがある。議事録がとられているが、審議内容は公にならす、結論のみが公にされている。たとえば、本調査の直近の期日では Google 社が呼ばれ、ストリートビューに関するヒアリングが行われた。

総会のほかに、分科会があり、そこでは懲罰について議論されたり、各委員の専門性に応じて審議が行われることがある。

③人員、人事

約 150 名のスタッフ（現在リクルート中であり、夏までに 150 名のスタッフになる。2009 年の人員は 132 名である。）がいる。

4 人の課長のもと、4 つの課（法・国際・IT 専門課（43 名）、ユーザー・検査課（65 名）、研究・イノベーション･将来動向課（8 名）、行政･財務･IT 課（29 名）が置かれ、以上のほかに事務局長付き（10 名））の部署がある。2010 年 12 月に組織再編を行い、研究・イノベーション・将来動向課はそこで新たにつくられたものである。

スタッフは、省庁からの出向者はごくまれである。スタッフは、ソリスターや IT 専門家のほか経済専門家、裁判官、警察官、財務・人事関係者などから成っている。短期契約や長期契約などがあり、ほとんどのスタッフが25～35歳の若い人たちから成る。エンジニアなどは6年間の雇用が限界であり、退職後は Google 社などへ再就職した者がいる。法律関係者は退職後裁判官になった者もいる。このような再就職については、その存在が公になっていることや CNIL はあくまで仕事を中立的に遂行しているため CNIL としては問題がないと考えている。

CNIL の建物は 6 階建てであり、課長は個室があり、その他は概ね２～３名につき 1 部屋割り当てられている。

④予算

予算は、2010 年 14,700,000 ユーロ（約 22 億円）、2009 年 13,000,000 ユーロ（約 19.5 億円）となっており、2004 年から 5 年間でおよそ 2 倍になった。

	2004	2005	2006	2007	2008	2009
人員	80	85	95	105	120	132
予算（百万ユーロ）	6.5	7.2	9.0	9.9	11.4	13.0
人員費	4.2	4.7	5.3	6.0	7.2	3.3
運営費	2.3	2.5	3.7	3.8	4.2	4.7

表 1　CNIL の予算

⑤権限

1978 年法は 2004 年法になり、CNIL の執行権限が強化された。

改正前は、民間部門における通知と公的部門における事前の意見を表明するにとどまっ

ていた。しかし、2004 年法の制定に伴い、官民両部門において通知と事前の意見表明を行うことができることとなった。同時に、官民両部門においてセンシティブデータの処理や国際データ移転をする場合などの事前の認証を要求し、認証は委員会の総会で承認されなければならない。近年、バイオメトリックに関するデータ処理を行う事業者が多く CNIL に訪問し、事前に説明を行い、許可をもらいにくる。現在、CNIL では認証制度（label）を検討しており、EU データ保護指令の改正の動きに向けて国内でも本格化していく予定である。プライバシー影響評価についてはこれまで行ってきていないが、認証制度と同時に話を進めていく予定である。

また、2005 年以降、法律違反があった場合、「係争処理部 (Formation contentieuse)」より警告と法令遵守通知の発出を行っており、これらに服従しなかった場合は上限 150,000 ユーロの罰則だが、反復違反の場合は上限 300,000 ユーロの罰則を科すことができる。このほかに、データ処理の中止命令を出すことができ、緊急時には 3 ヶ月間の処理中止とデータ保護を命令することができる。このような措置に対する不服がある場合は、コンセイユデタに訴えることができる。これまで CNIL がコンセイユデタに訴えられたことは一度もない。

⑥他機関・地方との関係

CNIL はパリにあり、地方部局等は存在しない。

CADA との協働をしばしば行うことがヒアリングの結果分かった。また、地方自治体に対しても立ち入り検査等の権限行使を行うことがある。

3　監督機関の運用実態

（1）施行状況

主な統計は次のとおりである。

・CNIL へのデータファイル宣言：140 万回（1978 年以降）
・認証（2009 年）：544
・バイオメトリックに関する認証：900
・ビデオ監視に関する認証：3054
・認証の拒否：5
・センシティブデータ（危険性の高いデータ処理）への意見：35
・警察記録の提出要求：2217
・法令遵守通知：446（2009 年は 91 回）
・警告：25（2009 年は 4 回）

（2）苦情処理・紛争解決

○苦情処理の実態

13 人のスタッフで 3 つの系統に分かれて、苦情処理に当たっている（①銀行、クレジット、債務整理、税金、地方、市民的自由、②ビジネス、販売、テレコム、保険、エネルギー、郵便、不動産、③雇用、健康、社会保障、教育、交通）。

苦情に対する直接の回答は 25％程度であり、事業者との対話（手紙・メールを書くなど）が 75％程度となっている。

2010 年には 4800 件の苦情処理を受付ている。苦情の分野としては、雇用（20％）、銀行・クレジット（20％）、ビジネス・販売（20％）、健康・社会保障（5％）などとなっている。苦情の内容としては、異議申立の権利（50％）、違法なデータ収集（15％）、アクセス権（10％）、訂正権（10％）、安全管理措置（5％）となっている。

2010 年 6 月からは苦情処理をホームページで受けつけるサービスを開始した。

○苦情処理と権利論

苦情処理のほとんどが権利に関するものであり、”e-right” がかかわってくる。「忘れられる権利（the right to be forgotten）」は、インターネット上における個人情報の消去を求めるものであり、CNIL としては情報処理、ファイル、及び自由に関する 1978 年 1 月 6 日の法律第 78-17 号第 48 条で保障された権利であると考えている。「忘れられる権利」について、アメリカでは個人の識別情報は変化するものであって、その意味で「忘れられる」というものであるが、ヨーロッパでは 18 歳のときに残された個人情報が雇用などの場面で 40 歳になっても左右することがあり、「過去の情報を消去する」ことを意味する。

また、CNIL としては、E メールアドレスであろうと IP アドレスであろうと、すべて個人データに該当するものとして対応してきている。

○ダイレクト・マーケティング

郵便法 33 条 4 項 1 号によれば、ダイレクト・マーケティングのために個人データを用いる場合、本人の事前の同意が必要とされている。また、電子メールのみならずショート・メッセージ・サービスやマルチ・メッセージング・サービスによるマーケティングについても規制の対象となっている。もっとも、人以外の自動的にダイヤルができる機械による電話に対しては、いわゆるオプト・アウト方式が採られている。ダイレクト・マーケティングの規制に違反した場合は、5 年以下の懲役または 300,000 ユーロ以下の罰金（刑法典 b226-18 条 1 項）[21] ないし不法なメールにつき 750 ユーロの罰金（郵便法 10 条 1 項）に処せられる。

---

21 欺瞞的、不正な又は不法な手段を用いて、個人が異議を申し立てているにもかかわらず、個人に関するデータ処理を継続することは、…5 年以下の懲役又は 300,000 ユーロ以下の罰金に処する。

○対応例

苦情に対して、毎週 150 通程度の手紙を書いてきている。通常であれば 15 日程度で手紙を書くようにしているが、複雑な事案については２～３か月程度かかることがある。

近年、多重債務処理を目的として、銀行・金融機関が利用している個人に対する信用貸付事故に関する国内ファイル / データベース（FICP：Fichier national des incidents de remboursement des crédits aux particuliers）について特に問題が多く、苦情処理が増加している。

○データ保護担当者（Correspondant Informatique et Libertés）

2009 年末時点で 6000 の組織において、データ保護担当者が置かれている（法 22 条）。そのうちの約 90%が民間企業であり、CNIL は公的機関にも担当官を任命するよう呼びかけている。データ保護担当者の役割は組織のデータ保護法の順守を監督し、CNIL に担当者を登録しておくことで CNIL が行う研修等に参加することができることとなっている。2009 年には 23 回の研修が行われ、350 名のデータ保護担当官が出席している。

（3）権限行使（立ち入り検査・罰則）

CNIL は、2 日前に通知をすれば、直接訪問をして他省庁が保有している文書の開示を求めることができ、必要があれば、文書を押収することができる。特に金融関係の省庁や機関におけるコントロールが多くなっている。この役割は警察と変わらない。

Google 社のストリートビューについては、2010 年 5 月に事前通知を行い、まずはグーグル・カメラを押収し、CNIL 内の技術専門家により分析を行った。その後、CNIL に Google 社を呼び出し、委員会においてストリートビューの問題点を追及した。その結果、Google 社は、Wi-Fi データの収集やストリートビュー・サービスなどについてこれまで性的志向や政治的思想にかかる個人情報を収集していたことが判明し、罰金を科すこととなった（2011 年 3 月 21 日付け）。なお、Google の技術的問題については未解決な部分があり、今後とも調査を行っていく予定である。このほかに注目を集めた事例として、2006 年 6 月に CNIL は銀行 Credit Lyonnais に対して情報システムの立ち入り検査の協力を拒んだことを理由に 45,000 ユーロの罰金を課したものがある。

主な統計は次のとおりである。

・検査：310（2010 年）270（2009 年）（2001 年は 14 回）
　→検査は増加傾向にある
・罰金：34（合計金額 555,400 ユーロ）

○ CNIL の権限行使の実態について

・公的には強力な権限を行使する機関であると見られてきているが、実際の執行面は弱い。特に人員と財政の不足が問題である。

○検査・罰則の運用実態

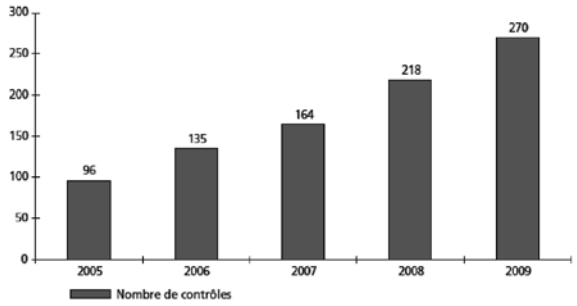

表 2　検査件数の推移

年次定期検査	31%
苦情に基づく立ち入り検査	25%
通知による法令遵守チェック	11%
その他（バイオメトリック検査）	33%

表 3　2009 年検査の内訳

＊ 2009 年 11 月 6 日コンセイユデタが CNIL による検査に対しては、異議申立の権利があらかじめ告知されなければならないという判決を下したため、以降、CNIL は事前に異議申立の権利を告知し、異議申立があった場合は、立ち入り検査を実施するために裁判所に審査をしてもらうこととなった。

販売サービス業	35%
医療	16%
行政、地方自治体	12%
テレコム・インターネット	10%
銀行	5%
その他	22%

表 4　CNIL 懲罰委員会が審査した主なテーマ

顧客・ユーザー・会員の管理	32%
バイオメトリックス	20%
社会保障番号の不法利用	10%
マーケティング	9%
ビデオ監視	9%
請求書の収集	5%
人事	3%
銀行記録	3%
スパム報告	3%
その他	6%

表 5　CNIL 懲罰委員会が審査した主な分野

事前手続（届出・許可）	33%
データアクセス、異議申立	19%
第三者提供	11%
安全管理措置	10%
データ更新	9%
違法なデータ収集	8%

表 6　CNIL 懲罰委員会が認定した違反類型

2009 年における罰則の実態

・91 通の法令遵守に関する正式通知

・5 件の罰金、総額 75,000 ユーロ

・4 件の警告

2009 年執行事例

・2009 年 1 月

Keolis Rennes：警告（理由）都市交通社の匿名パスの不適切な運用

・2009 年 2 月

Directannonces：罰金€40,000（理由）民間の不動産広告用の個人情報の不公正な収集

・2009 年 3 月

公的機関（未公表）：警告（理由）電子投票の安全管理措置違反

・2009 年 3 月

公的機関（未公表）：警告（理由）電子投票の安全管理措置違反

・2009 年 4 月

Societe Jean-Marc-Philippe：罰金€10,000（理由）労働者の継続的なビデオ監視

・2009 年 5 月

Optical Center：罰金€5,000（理由）マーケティングに関する異議申立権利に関する違反

・2009 年 7 月

Groupement d’huissiers：罰金€10,000（理由）安全管理措置違反

・2009 年 7 月

SCP Huissiers：罰金€10,000（理由）債務者に関する侮辱的なコメントの履歴保存

・2009 年 7 月

SCP Huissiers：罰金€10,000（理由）債務者に関する侮辱的なコメントの履歴保存

○防衛・警察機関への検査

Jean-François Clair(元仏内務省国土監視局 Directeur adjoint)からのヒアリングをもとに執筆した。

・CNIL は、職権又は、個人からの請求を受けて、警察・セキュリティ関連の行政機関が保有する秘密（secret)・機密（confidentiel）のファイルを閲覧 (consulter) することができる。行政機関が保有する文書の分類は大別して、秘密・機密・保護なしの 3 種となっている。

・自分に関するファイルが当局によって作成されているのではないか知りたがる市民は多い。しかし、実際、多くの場合、当該個人のファイルは存在しない。
・秘密 / 機密に分類されたファイルも、一定期間（30 ～ 35 年程度）を経過するなどの条件を満たすと、国立公文書館（Archive Nationale）に移管され、個人が直接閲覧できるようになる。
・CNIL が閲覧したファイルに問題が見つかった場合の対応：① CNIL が問題個所を修正するよう勧告する、②個人が裁判所に提訴し、当該文書の合法性を問い、又は問題個所の修正を求める。

CNIL の警察機関等へのファイル間接アクセス数[22]

2009 年、CNIL は 2217 件の間接アクセス権の要請を受け、内務省と防衛省へのファイルアクセスを行い、5712 件のファイル検証を行った。

	検証数	割合
内務省	4279	75%
防衛省	1433	25%

表 7　内務省・防衛省に対する検証数及び割合

このほかに、2009 年、諜報ファイルへの検証は 1236 件、内務省警察記録（STIC）への検証は 1385 件となっている。

○ STIC に対する検査

・2007 年 6 月から 2008 年 11 月にかけて CNIL は「調書作成犯罪に関する情報処理システム（Systeme de traitement des infractions constatees）」（以下、「STIC」という。）に対する検査を初めて行った。その結果、警察データファイルの利用の目的とそれを用いる手段・方法との関係性の不十分さが明らかになったところがあり、CNIL は 11 項目にわたる提案を行った[23]。

（内務省）

－データ入力機械の安全確保に向けた手続の実施
－省庁別の犯罪に関する文書の異なる取り扱いの統一化
－地方のデータベースにおけるデータ保存期間の法令順守
－アクセス管理の厳格な運用
－警察情報へのアクセス履歴追跡の強化
－行政の調査のために用いた人物像に関する法令順守

（法務省）

－司法の決定に関する情報について、内務省に転送する際、特定のソフトウェアの利用

22 CNIL, 30e Rapport D’ Activite 2009, p.37.

23 CNIL, 30e Rapport D’ Activite 2009, p. 10-11.

○ CNIL と監視機関の関係

・内務省国土監視局（Direction de la Surveillance du Territoire）（以下、「DST」という。）は、従来 DST と中央情報総合局（Direction centrale des renseignements généraux：RG）（以下、「RG」という。）に分かれていたころ、DST が保有するファイルは CNIL に存在が知らされていた（été déclarées）ので CNIL との関係では問題がなかった。RG が保有するファイルは、CNIL に存在が知らされているもの（たとえばテロ関係）と、そうではないもの（たとえば政治的志向に関するもの）があったので統合により、問題が生じ始めた。

（4）CNIL 以外の第三者機関の活動について

・犯罪に関する個人情報文書の管理システムとしては、警察組織である STIC、司法憲兵隊（JUDEX gens d'armerie）（以下、「JUDEX」という。）、司法府（Casier judiciaire）においてそれぞれ保有されている。2009 年 1 月に司法憲兵隊（もともと軍系列）が内務省の管轄下に移ったため、今後、STIC と JUDEX が統合される可能性があるかもしれない。

・このような情報管理について、CNIL 以外の個人情報保護に関連する独立行政機関（どちらも諮問機関。国家機関に対して拘束力のある決定をとる力はない）がある。

① セキュリティ上の通信傍受の統制の国家委員会（CNICIS：Commission nationale de contrôle des interceptions de sécurité）

・セキュリティ上の通信傍受を望む機関は、まず自身を管轄する省の大臣に許可を求める。大臣は、首相に許可を求める。首相は CNICIS の意見を踏まえて許可・不許可を決定する権限を有する。運用上、ほとんどの場合（9 割以上）、首相は CNICIS の勧告に従っている。

・委員会は、コンセイユデタの構成員（法案等の作成において政府に助言、フランスの行政裁判所の最高機関、行政活動の監督の３つが主な任務とされる）あるいはその出身者、裁判官（あるいは出身者）、議員（上下院）から構成される。裁判官に多くの権限を与える国もあるが、フランスでは構成員の出身の多様性が判断の適切さを担保することになるという考えに立った仕組みを採用している。

・フランスでは通信傍受に２種類あり、一つは司法的理由による盗聴（interception judiciaire）、もう一つはセキュリティ上の理由によるもの (interception de sécurité)。この委員会は、そのうちセキュリティ上の盗聴に関する諮問機関として機能してきた。

②秘密・機密に分類された文書への裁判官によるアクセスの統制を担当する委員会（CCSDN：Commission consultative du secret de la défense nationale）

大統領府に設置された対テロ機関（1982 年）による文書閲覧システムの濫用への対応として 1991 年に設置された。

○旅客機の乗客名簿の共有について

・搭乗者名記録の外国への提供は、捜索ないし法的状況に関する措置の対象となっている全員の目録を作成することにより、司法・軍事・行政当局の要請にもとづいて警察・司法憲兵隊がおこなう捜索を円滑なものとするのに役立つ。

・同姓や同名を理由として予約や搭乗の段階で無関係の人が移動を封じられる一方で、テロ行為は繰り返されている。すべての乗客名簿の共有は不必要であり、現状の制度には問題がある。

→ 2005 年 10 月 10 日の意見において、CNIL はデータ処理が商業目的で集められたデータにもとづいており、人の移動の自由とプライバシーが侵害される危険性や本人が知らないうちに身元を管理される危険性があることを強調した。そして、このような措置を永続させないような所要の措置を講ずることと特定の目的地に向かう乗客のデータに限定することを要求したが、法案に生かされることはなかった[24]。

③国際連携

○国際対応の現状

CNIL の Bartoli によれば、クラウド・コンピューティングやアウトソーシングに関する問題が増加してきているため、近年 CNIL としても国際問題に力を入れてきている。EU レベルにおいては、29 条作業部会の分科会での文書草案に携わってきている。また、欧州評議会 108 条約を国際標準のモデルにしたいと考えている。アメリカがこの条約への署名を拒否しており、残念だが、オバマ政権になり、姿勢が変わりつつあり、姿勢を共有しつつある。データ保護プライバシー・コミッショナー会議においては、昨年からコミッショナー間での情報交換をするため、決議採択の数を増やしていきたいと考えている。

OECD においては GPEN が開始されているが、まずは情報共有のレベルである。各国主権を維持したいと考えており、現状では執行協力にまではいたっていない。カナダのコミッショナーを中心とした Google Buzz に関する 10 か国の共同声明を出したことは大きな功績であると考えている。

今年、CNIL はアメリカ合衆国 FTC と 2 回ほど意見交換を行ったが、今後も議論の数を増やしたい。セーフハーバー制度については問題が多く、その実効性に多くの苦情が寄せられてきており、改善を図っていきたい。

ISO との協働も重要であり、データ主体の意識向上になるとともに、セキュリティの向上につながると考えている。

CNIL は年間 40 通程度の国際会議への招待状をいただいているが、お金と時間の関係で 2010 年は 24 回の会議に出席したにとどまる。CNIL はビジネスの現実に無知であるという批判があるため、可能な限りビジネス界の声も聞くことができるよう、ビジネス界からも出席がある会議に出席するようにしてきている。

---

24 高山直也「フランスのテロリズム対策」外国の立法 228 号（2006）124 頁。

○国際標準について

2009 年データ保護プライバシー・コミッショナー国際会議において、いわゆるマドリッド宣言が採択されたが、欧州評議会 108 条約も有力な候補であり、どの文書を国際標準の基礎にするかは今後の問題である。重要なことは現状のソフトローを拘束力あるものにしていきたい。拘束力があるとは条約を意味している。実現に向けて国際会議を開催していきたい。政治・経済問題に関わるが、最終調整は政府(外務省)にもお願いすることになるであろう。今年 5 月にパリで開催される G20 においては、首脳宣言に International Consultation of Data Protection という項目が入れられることなり、非常にうれしく思う。

（5）広報・啓発活動

○ CNIL の知名度

	04 年 6 月	09 年 12 月
CNIL を知っている	32	42
CNIL を知らない	68	58

表 8　CNIL の知名度

○広報啓発活動

127 回（2009 年）シンポジウム、セミナー、会議、研修等に参加

○助言活動

7 件の法案・デクレに関する意見提出

4　監督機関の課題等

○ 2004 年法改正に伴う変化と近年の取組

1978 年法では民間部門においてデータ処理に関する通知を受け、公的部門において事前の意見表明を行っていたのみであったが、2004 年法改正に伴い、官民両部門において通知の原則が適用されることになったほか、センシティブデータの処理やデータの第三国移転等について CNIL の事前認証が要求されることになったことなど、権限が拡大した。また、2004 年 9 月以降、制裁小委員会が設置され、2005 年以降、警告または法令順守の通知を発出してきている。

CNIL は、一定の要件を満たした安全保障に関する文書を除き、いかなる専門的な文書にもアクセスでき、必要な文書のコピーを要求することができる。このような検査体制が CNIL の非常に重要な役割となってきている。近年は、監視カメラ、バイオメトリクス、位置情報について検査の力を注いできている。また、EU 域外へのデータ移転については、「拘束力ある企業ルール（Binding Corporate Rules)」の利用を促進してきた。

○将来の課題

CNIL は、技術的な課題につき、Privacy by Design などの問題に取り組んでいる。Facebook や Google の問題は今後も検討していくであろう。同時に、グローバル化について一定の水準を設けることも重要である。これまで CNIL の副委員長とアメリカ合衆国 FTC との間での交渉を重ねてきている。2011 年 5 月に G20 がフランスで開催されるが、その中でも私生活の保護に関する共通の基準を設けていきたいと考えている。サルコジ大統領は、インターネットの著作権の問題を論題として意欲的に取り上げるつもりでいる。この会議によって、デジタル科学技術の発達が直面する個人情報保護の重要なステップを乗り越え、フランスが果たす重要な役割を明確にすることが期待される。

・その他の動向

○ソーシャル・ネットワークと忘れられる権利

・世論調査 2009 年 12 月調査（18 歳以上 1000 人）
　43％の国民がソーシャル・ネットワークのプライバシー保護が不十分と回答

・主要なソーシャル・ネットワークに関する調査結果
　―データ管理の利用ツールへのアクセスが困難である。
　―非会員の個人がサイト上の集団写真に写っていることが知らされていないことがある。
　―異議申立ができないままユーザーの年齢、性別、IP アドレスに基づくターゲット広告がされている。
　―データ保存期間が体系的に明確化されておらず、長期間保存されることもある。
　―ユーザーからの消去の要請はしばしば考慮に入れられている。

○番号制度

・歴史的経緯[25]

25 高山憲之「諸外国における社会保障番号制度と税・社会保険料の徴収管理」海外社会保障研

社会保障番号は当初、紙媒体で管理されていたが、ポンピドー大統領時代の 1973 年にコンピュータ化に取り組み始めた。その計画は「サファリプロジェクト」と呼ばれ、個人の自由と権利を侵害するという批判を浴びた。1978 年に CNIL が設置され、同委員会の下で社会保障番号の使用を規制することになったが、1998 年 11 月、詐欺対策のためすべての税金データベースとのデータ・マッチングを認めるようになった。このように、全省庁を横断して普遍的に利用しないことが基本方針とされていたが、税金の分野においては紐付けすることが認められている。

＜社会保障番号（１５桁の数字）の構成＞

最初の１桁：性別（男性が１、女性が２）

次の４桁：生年月

次の２桁：県番号

次の３桁：地方自治体（コミューン）番号

次の３桁：同一地方自治体内における同年同月生まれの人の届出順番

最後の２桁：行政上の確認キー番号

⇒フランスの番号制度は、必ずしもランダムな番号の組み合わせではなく、番号自体からも一定の形で個人像が浮かび上がってくることに注意が必要である。

ヒアリングにおいては政策研究財団 Daguzan 氏が実際の社会保険カードを見せてくれた。番号のほか、氏名、生年月日、生まれた場所、住所、写真、自筆サインの情報が含まれている。身分証明書として銀行や EU 域内の交通機関（乗車の際の ID 提示）に用いることができる。医療カードは別にあり、税金に関するカードはない。現在のカードには生体情報が含まれていないが、一般に生体情報の利用にはフランス国民の抵抗が強い。

○国民社会保障台帳（Répertoire National de la Protection Sociale）

2006 年 12 月 21 日法によれば、すべての社会保障機関、医療保険機関、及び国の労働機関に対し、社会保険番号、保険加入者の住所、保険形態、保険の恩恵などを含む国民社会保障台帳の創設を義務づけた。この台帳には、①社会保険加入者の書式を単純化させること、②行政の効率を向上させること、③詐欺撲滅政策の促進という目的があった。2009 年 4 月 30 日、この法令の見直しが行われ、CNIL は、①データの安全性と機密性を確保するために、アクセスの追跡を可能とし、利用機関による監視が必要であること、②アクセス及び訂正の権利をデータ本人に告知されること、③台帳の年次報告書を CNIL に提出することを内容とする意見を公表している。また、2009 年 11 月 12 日、CNIL は税務当局が運用する ”Evafisc” というデータベースの運用状況について審査を行った。CNIL は、このデータベースの導入は詐欺対策の政策を目的とされていることが正当であると判断した。その上で、CNIL は、データの正確性の維持（同姓同名などを理由とした間違いが生じていないかどうか）と保存期間（10 年間）が経過した場合のデータ削除について要請を行った。

究 172 号（2010）12 頁、参照。

○テロ対策とデータ保護

フランスにおけるテロ対策とデータ保護について、政策研究財団 Daguzan 氏と Coste 氏からのヒアリングによると次のような回答があった。

・9・11 テロ後には市民の人権を保護する重要性が増してきており、CNIL の強化が望まれる。EU ではデータ保護は基本的人権の問題であり、テロ対策との間で緊張関係にある。

・データ・マッチングは、テロリズム対策と防衛以外では禁止されてきている。数年前からテロリスト容疑者のデータベースが内務省の所管で作成されてきた。このデータベースには、データの区分がなされているが、個人の政治的思想、宗教、労働組合加入状況、人種、金融取引といったセンシティブデータが含まれていたため問題とされた。

・CNIL は内務省が所管するデータベースの利用をチェックすることができる最終チェック機能を有しているが、財政面と調査に時間を要することから実際にはチェックがおろそかになっている。現状では、このようなデータベースを作成するための内務省から CNIL への届出が必要なだけとなっている。

・アメリカやドイツは連邦制を採用しているため、中央政府によるテロリズム対策はフランス以上に難しくなっている。しかし、フランスは中央集権型であるため、データの一元化とともにテロリズム対策が行われてきている。

○日本の新機関に対する CNIL のコメント

社会保障と税という２分野に特定した第三者機関というのは、ヨーロッパの目から見て、データの国際移転におけるデータとは「あらゆるデータ」を指していることから、社会保障と税の２分野のみを監督するのは十分とはいえない。クラウド・コンピューティングやソーシャル・ネットワーキング・サービス等における問題に対処すべきであり、問題は社会保障と税に限ったものではない。いずれにせよ、官民両部門と全分野について監督できる機関が望ましく、同時に高級レベルでの国際対話が必要である。

・まとめ

フランスのデータ保護機関である CNIL は「EU においてもっとも強力かつ効果的な機関の 1 つである」[26] と評価される。そして、「多くの分野において非常に詳細な手引きを示してきており、同時に「拘束力ある企業ルール」をはじめとして規制問題において緊密に取り組んできている」[27] と指摘される。

CNIL の本来の役割は行政機関が保有する個人ファイルのデーマッチング等による個人の自由の侵害を防止するための監視であった。もっとも、1978 年当時の法が想定していた行政機関に対する脅威の監視のみならず、現在ではソーシャル・ネットワーキング・サービス等のパソコンを用いた日常生活における個人データの流通に付随する個人の人格や選好に対する危険をどのように未然に防止するかという課題が重要になってきている。フランスにおけるデータ保護の主題は、いわゆる ”Big Brother”（巨大な機関による監視や検閲）から ”Little Sisters”（万人によるあらゆる形態の監視という比喩）へと変容したと言われる [28]。

CNIL からのヒアリング結果でも明らかになったように、近年、人員・予算が拡大傾向にあり、同時に立ち入り検査等の実施状況が増加傾向にある。権限行使の実効性と正当性に対する懐疑的な見解も存在するが、30 年以上にわたる実績から、国民の信頼を得た機関となっており、ヒアリング結果からは CNIL の役割がますます期待されている様子がうかがえた。

---

26 European Commission, Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, A3- France (May 2010) at 54.

27 Id.

28 Vitalis, supra note 20, at 122.

iii. ドイツ

1　個人情報保護法制の概要

（1）法律名・目的

ドイツにおけるデータ保護に関する一般法は、連邦データ保護法（Bundesdatenschutzgesetz (BDSG)、Federal Data Protection Act）である。同法のもっとも最近の改正は、2009 年 8 月 14 日に行われ、同年の 9 月 1 日に施行されている。この改正案は、2008 年 7 月 30 日に閣議決定されていた。

同改正では、主に、個人信用情報に関して、個人信用調査会社へのデータの提供（28a 条）及びいわゆるスコーリング（28b 条）についての規律の新設、また、当事者の開示請求権の強化（6 条、6a 条、34 条）を意図している。

さらに、この連邦データ保護法のほか、ドイツでは、個別法としておよそ 40 本の法律が存在する。その中には、国勢調査判決以降見直しを受けているものが多い。とくに治安関係、社会保障関係（詳細である）は従来行政規則レベルで対応していたものが法令のレベルになっているという特徴がある。また、インターネット対応といわれる通信役務個人情報保護法（1997 年）及びテレコム法（2004 年）なども個人情報保護の個別法として重要視されている。さらに、近年、「インターネットにおける個人情報の保護―人格権に対する重大な侵害からの保護のための法律案」が連邦議会に提出された。

同法の目的は、個人データの取扱いにおける個人のプライヴァシー権侵害からその個人を保護することにある（1 条 1 項）。

（2）制度の特色

①ドイツ法は、2001 年の改正法により、第 1 章が公的部門・民間部門に共通する総則規定、第 2 章が公的機関、第 3 章が民間部門に関する規律、第 4 章が特別規定（守秘義務に服する個人データの提供の要件、学術研究の特則、メディア条項等）となっている。制定当初の立法では公的部門に対する規律が厳しかったが、情報化社会の進展とともに民間部門（非公的機関と公法上の競争企業を併せて民間部門と呼んでいる）の規律が重要という意識が高まってきている。それが最新の法改正にも現れている。

② 2001 年法は、EU 指令転換法（EU 指令の国内法化）であるが、その主たる改正点としては、公的部門・民間部門を問わず、ⅰ）データ処置システムの選択及び構築に際してのデータ回避・データ倹約の原則、匿名化・仮名化優先の原則が採用されたこと（3a 条）、ⅱ）本人の同意の内容と手続が詳細に定められたこと（4a 条）、ⅲ）個人データの第三国等への提供の要件が定められたこと（4b 条）、ⅳ）データ保護の責任者を設置と自動処理の届出及びその免除の要件が定められたこと（4d 条、4e

条、4f 条)、ｖ）ヴィデオ監視等についての明文の規定が置かれたこと（6a 条)、vi）センシティヴデータの考え方が採用されたこと（3 条 9 項、ただし、公的部門と民間部門で取扱いの要件が異なる）等をあげることができる。

③開示等の権利で特徴的なのは次の点である。ｉ）当該個人に関して蓄積されたデータ及び当該データの情報源に関するデータ、ii）データが提供される受領者または受領者の範疇、及びiii）蓄積目的が請求権の対象となっている（19 条)。自己に関する情報がどこから来て、どこに行くかを、本人が追えるようになっていると言い換えてもよい（19 条から 20 条、34 条及び 35 条)。第三者提供等の例外規定が詳細である分、本人の権利は強いと言える。

④独立した横断的データ保護庁を有する（EU の標準として有しなければならないというのが正確）のがヨーロッパの法制であるが、ドイツの個人情報保護法制にあっては、監督機関が 3 層に分かれている。すなわち、連邦の公的部門と民営化された鉄道・郵便・通信を連邦データ保護・情報自由監察官（以下、単に「連邦監察官」と略す）が、州の公的部門は州のデータ保護（情報公開法を有している州では、データ保護・情報自由）監察官（シュレスヴィッヒ・ホルシュタイン州の場合には、個人情報保護のための州独立センターという委員会）が、そして州の民間部門は監察官等又は内務省の下にある監督官庁が所管している。わが国の分担管理の監督とは決定的に異なる点である。

⑤セキュリティに関連して、行政機関の場合には、Das Bundesamt für Sicherheit in der Informationstechnik（BSI:情報技術における安全のための連邦官庁、連邦情報安全庁と呼ばれる）が存在し、セキュリティについて啓蒙活動を行ったり、あるいは、セキュリティの大部かつ詳細なガイドラインを示している。ガイドラインであって法的義務ではないが、州のデータ保護当局の中には、これを抜粋する形で参考にしているところがある（ヘッセン州等)。

（3）適用範囲

連邦データ保護法は、公的部門と民間部門を包括的に規制している。

（4）適用除外

適用除外の内容は、これを認める目的によって、除外対象となる条文が異なり、これらを網羅的に挙げることは困難である。特別な取扱いを一定の主体に認める場合としては、次のようなものがある。

専門的又は特別な公式の秘密保持の義務のもとでのデータ処理（39 条)、研究機関による個人データの処理（40 条)、メディアによるデータ処理（41 条）などについて、個人データの特別な扱いが認められている。なお、メディアによるデータ処理に関する 41 条の成立経緯やその内容については、藤原靜雄「ドイツ」「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」（消

費者庁、2009 年）が詳しいので参照していただきたい。

また、小規模事業者についても、データ保護法上、特別な取扱いが認められている。個人データを自動化して収集、処理又は利用する事業者は、データ保護担当者を任命しなければならず、それ以外の方法による取扱い等についても、20 人以上がそれに従事する場合には同様であるが、個人データの取扱い等に従事する者が 9 人以下の事業者については、この義務が免除される（4f 条 1 項）。2006 年の法改正により、人数要件が 4 人から 9 人に緩和されたものである。さらに、2006 年の法改正により、データ保護担当者を設置が困難な小規模事業者は、事業主自身が担当者となることが許されるようになっている。

なお、小規模事業者の届出義務の免除については、以下（6）の届出制度を参照していただきたい。

（5）権利・義務規定に関する内容

6 条 1 項では、データ主体のアクセス、修正、削除、ブロックの権利が、法的取り扱いによって排除されることや制限されてはならない旨を規定している。

また、データ主体の個人情報の利用停止・消去に関する措置については、35 条が詳細に定めており、34 条が、自己に関して蓄積されたデータの情報源に関するデータについての開示請求権を認めているが、2010 年 4 月 1 日から施行されている改正連邦データ保護法では、当事者の開示請求権を強化する規定がおかれたことが重要である（6 条 3 項、6a 条、34 条）。その概要は次のとおりである。

・6 条では、データ主体の権利について定めているが、新たに 6 条 3 項が追加された。そこでは、「連邦データ保護法又はその他のデータ保護規定に基づくデータ主体の権利行使に関する個人データは、その権利行使から生じるデータ管理者の義務を履行するためにのみ利用される」と定められている。
・6 a 条では、自働的個人評価に関して定めている。そして、同条 1 項では、「自然人によらない内容評価に基づく判断は、自働処理のみに基づくものとする」という規定が加えられた。また、同条 1 項が適用されない場合として、同条 2 項 2 号の規定が改正された。
・34 条 1 項では、従来から、データ主体の求めによりデータ管理者が次のような情報を提供することが定められている（文言形式は、データ主体の権利からデータ管理者の義務の形式に改正されている）。
  a データの情報源に関する情報を含む、データ主体に関して記録されたデータ
  b データが移転された相手方又は相手方のカテゴリー
  c データを記録する目的

また、スコーリング（28b 条）についての規律が新設されたことに伴い、同条の場合には、その判断に責任を有する組織は、データ主体の求めに応じて、以下の情報を提供すべきことと定められた（34 条 2 項）。

a 情報提供の要求を受ける 6 ヶ月前以内における最初の計測された又は記録された推定評価（probability value）

b 推定評価を計測するために利用されたデータの種類
c 当該個人のケースに言及し、一般的に理解できる用語によって、推定評価やデータ主体の重要性をいかに計測したか

さらに、34 条 3,4 項では、個人データを移転する目的で記録、収集などする組織に対しても、データ主体への情報提供義務のあることが新たに定められた。

（6）届出制度

民間のデータ管理者は所管官庁に、また、連邦若しくは郵便・テレコミュニケーション企業のデータ管理者は連邦監察官に対して、個人データの自動処理取扱い前に届出る義務を有する（4d 条 1 項)。

とはいえ、データ管理者がデータ保護の担当者を指定している場合には、この義務が免除される（4d 条 2 項)。民間部門において、10 人以上の者が個人データの収集、処理、利用に携わる企業では、個人情報保護の担当者を置かなければならないというシステムが定着している（4f 条)。既に 1997 年にはこの制度が公的部門にも組織的に取り入れられている[1]。

これは、ドイツではデータ保護担当者に、より現場に近いところで個人情報保護のマネジメントを行わせるのが、監督官庁への届出制度よりも個人情報保護にとって実効的であると考えられているためである。

また、この自動化された処理方式を監督機関へ届け出る義務も、個人データの処理等に従事する者が 9 人以下で、かつ、当事者の同意が存在するか又は処理等が本人との契約関係若しくは契約類似の信頼関係に資する場合には、免除される（4d 条 3 項)。この 9 人という要件については、終身雇用（permanently employed）の者という要件が付け加えられ、2010 年 4 月 1 日より施行されている。

1　1997 年の内務大臣命令による。

2　監督機関の制度概要

（1）設置の経緯

連邦監察官の設立は、1977 年法の制定の際に、特に議論された。コミッショナーが議会から選任されるべきか、首相又は大臣から指名されるべきか、そのオフィスをいずれの組織に帰属させるべきか、各部署の長が、コミッショナーのように独立しているべきかなどについて議論があったが、その設立は、すべての政党から受け入れられた。

連邦監察官の設立にあたっては、既存の組織を改変するのではなく、新たに組織を創設した。内務省（Ministry of the Interior）が、コミッショナーの最終決定を受け入れる形で、連邦監察官オフィスの人員を新たにリクルートし、その人員は内務省の所属とされた。

（2）制度の概要

①所掌事務

(a) 公的部門の法の運用については、連邦監察官の役割が大きい。日常の業務において、関係機関が連邦監察官に法の解釈運用について事前の相談をすることは多い。監察官は、わが国における行政監察のような形で行政機関の個人情報保護の体制・運用について監察を行う。

(b) 民間部門の法の運用については、各州の監督官庁（州の監察官ないし内務省の担当部局）が重要な役割を果たしている。各州の監督官庁は、行政規則、ガイドラインの制定を通じて多様な活動を行っているが、特記すべきは、ディッユセルドルファー会同(Dusseldorfer Kreises)と呼ばれる、各州の最上級監督庁の集まりである。ここで、特定の事業者あるいは事業者団体との申し合わせがなされ、これが、事業者団体の自主規制に繋がっている。

なお、職能団体（弁護士会、研究者、世論調査専門家等）については、個人情報保護に関する行動基準の案を所管の監督官庁に示し、監督官庁がこれを審査するという仕組み（法 38a 条）も一定の役割を果たしている。

(c) 非公的機関の監督官庁については法 38 条が定める。

監督官庁は、この法律及びデータ保護に関する他の法規定の実施について、監督する。監督官庁は、この法律又はデータ保護に関する他の法規定に対する違反を確認した場合には、これについて本人に知らせ、訴追又は処罰する権限を有する機関に違反を告発し、及び重大な違反の場合には、これを営業監督官庁に営業法上の措置の実施のために知らせる権限を有する。監督官庁は、定期的に、遅くとも 2 年ごとに、活動報告書を公表する（38 条 1 項）。

何人も、非公的機関による自己の個人データの収集、取扱い又は利用に際して、自己の権利を侵害されたと考える場合には、監督官庁に助力を求めることができる（38 条 1 項による 21 条 1 文の準用）。

監督官庁は、届出義務のある自動処理（4d 条）の登録簿を作成管理する。何人も、この登録

簿を閲覧することができる（38 条 2 項)。

監督に服する機関及びその機関の管理を委託された者は、求めに応じて、監督官庁に対し、監督官庁の任務の遂行のために必要な開示を遅滞なく行わなければならない（38 条 3 項)。

監督官庁により監督を委託された者は、監督官庁に託されている任務の遂行のために必要な限りで、営業及び業務時間内に、当該機関の敷地及び事務所に立ち入り、そこで審査及び検査を行なう権限を有する（38 条 4 項)。

この法律及びデータ保護に関する他の法規定に従ったデータ保護を保障するために、監督官庁は、9 条（技術的・組織的措置）に基づく要求の範囲内で、確認された技術的若しくは組織的な瑕疵の除去のための措置がとられるよう命じることができる（違反に対しては過料が定められている)。監督官庁は、データ保護担当者がその任務の遂行のために必要な専門知識及び信頼性を有していない場合、データ保護担当者の解任を求めることができる（38 条 5 項)。

州政府及び州政府によって権限を与えられた機関は、本章の適用範囲内におけるデータ保護の実施の監督を管轄する監督官庁を定める（38 条 6 項)。

②組織体制

ここでは、連邦レベルについてであるが、そこでは、連邦監察官のもと、次長（Leading Officer）がおかれており、そのもとに 9 つの課がおかれている。

第 1 課　総務部、非公的部門（6 名）
第 2 課　法執行機関、金融及び労働行政、善意目的の非軍事的サーヴィス、国家行政（たとえば、外国人に関する法律）（15 名）
第 3 課　社会及び健康サーヴィス、被用者及び賃金労働者に関するデータ保護（7 名）
第 4 課　テレマティックス、応用情報学プロジェクト（7 名）
第 5 課　警察、情報機関、刑法、欧州及び国際的レヴェルにおける警察と司法の協力（6 名）
第 6 課　科学技術上のデータ保護、情報テクノロジー、データ・セキュリティ（10 名）
第 7 課　欧州又は国際問題、前 GDR の国家安全省によって集積された文書の再評価、国家行政（たとえば、登録事項）（7 名）
第 8 課　テレコミュニケーション、テレメディア、郵便事業、電子健康カードとのプロジェクトグループ（9 名）
第 9 課　情報の自由（4 名）

この他に中枢の機能を支える部署(Central Functions)に 13 名の職員がいる。また報道担当者(Press) 2 名が連邦監察官のもとにいる。

また、連邦監察官オフィスはボンに置かれているが、ベルリンにもある連邦議会や政府と緊密な関係を維持する必要があるため、ベルリンも「連絡室」(laison office）を設けている。

③人事制度

連邦監察官は、連邦議会（Bundestag）によって 5 年の任期で選任される（22 条 1、3 項）。2 期目の選任も可能であるが 3 期目の選任はできない（22 条 3 項）。また、選任時に☒なくとも 35 歳以上でなければならない（22 条 1 項）。同監察官は、任期満了の場合を除くと、終身雇用の裁判官の解雇が正当化される場合と同じ根拠を有する場合にのみ解任される（23 条 1 項）。また、同監察官は、連邦政府各省の部局長クラスである格付け B9 の給与を毎月受け取る（23 条 7 項参照）。

連邦監察官オフィスの職員は、定期的に研修に参加することが求められている。新しくオフィスの職員となった者は、データ保護問題に関する特別な研修を受けることが必須である。職員は、他の公務員と同様の地位にあるため、平均して 3 年から 5 年で他の部署（連邦監察官オフィスに限られない）へ異動する。

④職員数

連邦監察官オフィスの現在の職員数は、91 名である。その多くが、公務員（政府による終身雇用）であるが、26 名の職員は任期付き又は任期の定めのない採用によるものである。これらの者は、より容易に解雇されるなど通常の公務員と異なる扱いがされている。

現在では、91 名の職員のうち、より高い行政サーヴィスの職務を担う 35 名に対しては、大学の学位又は修士号を要求している。非常勤職員の数は変動するが、現在のところ約 10 名である。

⑤予算

2011 年の予算は、およそ 8,800,000 ユーロである。そのうち、6,200,000 ユーロを人件費に、2,200,000 ユーロをオフィスでの経費や旅費に（外部からの IT 援助のための 500,000 ユーロを含む）、400,000 ユーロを新しいコンピュータや技術的な設備にあてている。

なお、予算以外の収入源は存在しない。

（3）法的位置づけ

連邦レベルでのプライヴァシー執行機関（連邦監察官、連邦コミッショナー）の独立性は、データ保護法によって十分合理的に確保されている（22 条及び 23 条を参照）。連邦監察官が連邦議会（Bundestag）によって選任されること、および、その職務遂行に当たって独立しており、法にのみ従うべきことが定められている（22 条 4 項）。さらに、連邦監察官には、スタッフと予算を備えたオフィスが与えられている。

他方､以下の「4　監督機関の課題等」でみるように､州レベルでのコミッショナーについては､近年、欧州データ保護指令 95/46/EC の 28 条で求められている「完全な独立性」を有しないという、欧州司法裁判所（European Court of Justice）の判決があった。

（4）番号制度との関係

連邦監察官は、連邦金融機関の税金 ID 番号の利用を監視している。

しかし、国民 ID 制度はない。国民 ID などと呼ばれているものは存在するが（ドイツ国民であること又はドイツ在住であることを証明するため)、それは、地方公共団体のうち、もっとも小さな行政単位で作成してもらうものである。その情報については、他のより大きな地方公共団体及び政府もアクセスすることが可能であるが、合理的な理由がなければならない。また、そのような基礎的情報を政府（国家）が集約して保管するということはない。この点については、様々な議論があったが、現在のところ、反対意見が強く、政府による一括管理には至っていない。

3　監督機関の運用実態

(1) 施行状況の概要

施行状況調査等は行われていないが、問題状況は、連邦監察官が 2 年に一度、連邦議会に義務的に提出する報告書に掲載されている（26 条 1 項)。連邦監察官（州のデータ保護監察官等も同じ）は、いわば専門のデータ保護庁であるので、各省・各分野別に問題点を網羅している。

その第 23 回活動報告書 2009 － 2010 年は既に発行されており、そのドイツ語版は、連邦監察官のホームページで閲読することができる。しかし、英語版については作業中であり、本稿執筆時点では、未だ発刊されていない。

そこで、連邦監察官が、同報告書の主要な内容について記者発表をした際の英語版が存在するので、その内容を紹介する。

・自分たちの日常的行動が、記録、監視されているということに同意していない人々は増加している。よって、私（連邦監察官）は、連邦政府とドイツ議会に対して、この市民の意思を真剣に受け止め、公表されたデータ保護計画を実行に移すよう求めていく所存である。
・連邦政府によって昨年提出された被用者データ保護に関する法案は、つまるところ、長年に渡って知られている欠点に決着をつける意図を明らかにしたものである。同法案は、雇用者と被用者とにより大きな法的確実性を与えようとするものであるが、私の見解では、たとえば、被用者に対するオープン・ヴィデオ監視カメラが拡大されることなどに対して批判されるべきである。この法案に対する議会の議論が早期に行われ､職場におけるデータ保護の大きな向上に至ることを望んでいる（No.12.1)。
・マイクロソフト・ストリート・サイドやグーグル・ストリート・ヴューのようなストリート・ヴュー・サーヴィスやソーシャル･ネットワークに関する最近の議論によって、国際企業は、ドイツや欧州データ保護法を遵守しなければならないということが明らかとなっている。企業が、利用者の事前の同意なく、インターネットによる相当な収益を上げることができるという事態は容認できない。このような状況に対して、レッド・ライン法（red-line-law）というキー・ワードのもとに、連邦政府から意見以上のものは何も表明されておらず、議論の価値のある法案すら提出されていないというのは残念である（No.4.1.3)。

・レッド・ラインは、治安機関（security authorities）においても必要である。数週間前に、SWIFT合意の実施に関して明白な瑕疵が明らかとなったが、最近、制度的な、無期限の、かつ、科学技術的に実質的な審査なく、同盟国から反テロの立法拡大することを求められている（No.7.1.1）。
・連邦憲法裁判所が、政府による包括的監視に対する明確な限界を繰り返し（最近のものでは、データ保持に関する判決において）示していることを失念している人もいるようである。包括的な監視は、ドイツ連邦共和国の憲法のアイデンテティと両立しないだろう。欧州及び国レベルの連邦政府が、いずれも、この判決に従うことを期待している（No.6.1）。
・3年以上も前に、連邦憲法裁判所は、連邦政府に対して、納税者の納税機関に対する無条件のアクセス権を早急に実施するよう命じた。にもかかわらず、依然として、データ主体が「正当な利益」(legitimate interest）を証明した場合に限って、財政機関がその保存するデータに関する情報をデータ主体に提供しているということについては受け入れることができない。私は、連邦政府が最終的にこの要件を充足することを期待する（No.9.4）。
・欧州司法裁判所は、データ保護機関の独立性について明確な指針を示した。ドイツは、この判決を期限内に実施しなかったため、数千万ユーロという罰金を支払わなければならないだろう。この判決は、正式には、ランド（州）のデータ保護監視機関に対して適用されるものであるが、同様の法規定は国レベルでも尊重されなければならない。すなわち、たとえば、私には、テレコミュニケーションや郵便サーヴィス事業によってなされたデータ保護違反に対して、罰金を科す権限が与えられなければならない。残念なことに、現在まで、連邦政府は、繰り返しこれらの提言を拒絶している（No.2.1)。
・また、将来的なデータ保護組織は、財政や職員の点で独立したものでなければならない。政府は、この組織が保証された地位に基づいて、この仕事を始められる条件を作り出すべきである（No.2.5)。
・州のデータ保護コミッショナーと共に、データ保護法の近代化に関する具体的な意見を提出した。データ保護に関するドイツと欧州の法的枠組みは、データ保護が急速な科学技術の発展についていくことを確保しなければならない（No.1、13.2)。
・今日、法的規範によってデータ保護を保障することは、これまで以上に難しくなってきている。データ保護技術は、データに対するコントロールを回復させるようにしなければならない。デジタル消去者（digital eraser）に関する議論は、このことがいかに困難であるかを表している（No.1.6)。

より多くの不服、新しい任務、より多くの市民の不服

・本報告書に示された期間では、30の不服が申し立てられた。2007年から2008年に関する報告書では、10の不服が申し立てられていた。連邦データ保護法（BDSG）の第25条に基づいて、連邦データ保護・情報自由監察官は、連邦データ保護法や他のデータ保護の規定の違反、または、個人データの処理や処理に対して他の問題点を発見した場合、不服を申し立てることができる。
・2009年から2010年にかけて、連邦データ保護・情報自由監察官事務局は、市民から数多くの要望を受けた。つまり、文書による11,153の要望と電話による14,204の要望である。2007年から2008年と比較すると、文書の要望がおよそ47パーセントの増加であり、電話の要望がおよそ10パー

セントの増加である。

・これに加えて、私の事務局には、さまざまな新しい任務を与えられた。2011 年 1 月から、連邦監察官は、それまで州のデータ保護コミッショナーによって遂行されてきたものであるが、全国 335 の労働センターに助言を与え、これを管理する権限が与えられている。現在までのところ、その任務を遂行するために必要とされる 15 のポストが満たされておらず、一時的なスタッフで賄われているに過ぎない（No.11.5.1）。ELENA[2] 手続の主要な管理の仕事（No.11.1.3.2）や De メールのサーヴィス提供者の認証（No.3.3）によって、より多くの職務が与えられた。

第 23 回活動報告書のその他の項目

国勢調査 2011（No.8.1.1）

・国勢調査のために収集されたデータについて、明文による目的制限及び高い水準のデータ・セキュリティが保障されなければならない。とりわけ、個人情報が行政に戻ることは許されてはならない。私にとっては、個人の国勢調査の遂行に必要とされる個人データが匿名化され、必要性がなくなり次第、直ちに削除されることが重要である。ある特定の問題としては、住民登録において移転の障壁（barrier）が創設されていた者のデータ保護の取扱いである。ランドのデータ保護コミッショナーと共に、統計局の職務を緻密に検査し、明文化されたデータ保護要求を遵守していることを確保するつもりである。

2　独立行政法人労働政策研究研修機構のホームページでは、ドイツが導入した ELENA について説明している。その概要は次のとおりである（http://www.jil.go.jp/foreign/jihou/2010_2/german_01.htm）。
経営者は、2010 年 1 月 1 日から全ての従業員の賃金や諸手当等に関する情報を毎月 ELENA（Eleketronischer Entgeltnachweis）と呼ばれる中央データベースにオンラインで報告することが義務づけられることになった。 ELENA は、各種証明書に関する事務処理の軽減や紙書類の削減を目指して、2008 年 6 月 26 日の閣議で導入が決定し、これまで準備が進められてきた。ドイツ全土で働く約 4000 万人の労働者が対象になる。今後は各人に順次 IC チップ付のカードが支給され、2012 年以降は紙による証明書の発行が不要となる。
一方、労働組合や個人情報保護を訴える市民団体は、この運用に関して強い懸念を示している。公共国際放送メディアのドイチェ・ヴェレは、賃金や諸手当に関する情報に加え、不就業の実績も報告義務となっていることから、当該労働者がストライキに参加したかどうかの情報まで記録に残ってしまう可能性があることを指摘している。フランク・ブジルスケ統一サービス産業労組（Ver.di）委員長は、メディアのインタビューに対して「この巨大なデータベースは、誤用可能性など多くの問題がある」との懸念を表明している。
また、EU レベルに目を向けると、欧州委員会が 2005 年に発表・採択した「i2010 ～成長と雇用に向けた欧州の情報社会」で述べられている通り、将来的には ELENA のようなデータベースを EU 加盟国間で相互運用する構想も出ている。これが実現すると、今後は EU 域内の国際的な労働力移動の管理などに活用される可能性もある。

反テロデータベースにおけるデータ処理

・私は、連邦や州の警察及び情報機関と共に保存されている反テロデータベースに関して、憲法保護のための連邦局（the Federal Office for the Protection of the Constitution, BfV）のデータ処理を検査した際、重大な問題点を発見した。BfV では、削除すべきデータを反テロデータベースに依然として保存していた。それに加えて、隠密になされた通信傍受活動から得られたデータは、法で要求された特別の表示も付さずに保存されていたが、それは明文の規則に反するものである。反テロデータベースの他の利用者にとって、これらのデータが法によって特に保護されているということが分かるものではなかった。BfV はこれらの問題点を修正することを約束した。

反テロリストとのデータ・マッチ（No.13.7）

・私は、関税行政によって要求されている「認定経済事業者」（Authorized Economic Operator）としての認証における EC 反テロリストとの一般的な照合（match）に対して批判的な立場をとっている。ともあれ、セキュリティ関連の分野で働くスタッフのデータのみ照合されるということを達成するために、その照合の基礎となっている指示（instruction）の修正は、企業にとって、より大きな法的明確性をもたらすには至っていない。

ドイツの空港における身体スキャナー（No.7.3.1）

・2009 年の後半における攻撃は失敗に終わったが、それは、ドイツにおいても、裸のスキャナー（nude scanners）の導入に関する議論に火をつけた。同スキャナーの利用に関して私が創案した要件は、連邦内務省（the Federal Ministry of the Interior）によって取り上げられた。私の要件によれば、この導入の条件は、これらのデータを処理し、移転する際に、真の安全性確保の証明、データ保存の放棄、人間の尊厳の保護を求めるというものである。これに対応するハンブルグ空港における実践のテストが、連邦内務省によって拡大して、実施されている。

De メール：将来の安全なコミュニケーション？（No.3.3）

・De メール計画の目的は、安全で信頼できる電子コミュニケーションの確立である。しかし、同計画は、データ保護法や選択的エンド・ツー・エンド暗号化（optional end to end encryption）のような科学技術に関連する重要な要件の遵守にもかかわらず、依然として残された問題がある。それは、安全性、データ保護、処理の透明性、市民による De メールの受容について明らかになっていくだろう。

スマートメーター－知的な電子計器（No5.1）

・製造と消費の知的な一体化は、スマートメーターといわれている電子計測機器の設置を求めている。その機器は、とりわけ、実際の消費を計測し、そのデータを外部の組織に送るのである。この過程で収集されたデータは、非常にセンシティヴなものである。なぜなら、それらの機器が、個人の生活習慣に関する詳細な情報を入手することを可能にするからである。このことによって、スマートメーターに関する科学技術上のデータ保護や IT セキュリティに対する拘束的な基準が不可欠となっている。

関係する企業の自発的な取組では、不十分である。

クラウド・コンピューティング―クラウドにおけるデータ保護（No.5.6）

・インターネットにおける分散化したデータ処理（クラウド・コンピューティング）は、極端な場合には、誰によってデータが処理される処理されるのか、また、IT システムがいずれの国に存在するのかについてさえ分からない状況下で、いかにデータ保護及びデータ・セキュリティを図るのかという問題を生じさせている。仮に、個人データが、EU 又は EC 域外で処理されるのであれば、データ保護の観点から、クラウド・コンピューティングへのアプローチは、直ちにその限界に至るだろう。

欧州レベルにおける RFID-PIA（No.5.9）

・RFID チップは、より一層、服、店舗のカード、ID に統合されるようになっている。欧州レベルで採択された文書では、そのデータ保護の重要性と危険性について指摘している。RFID チップの利用に際しては、遡及的（upstream）リスク分析（プライヴァシー影響評価、PIA）が、データ保護に寄与するだろう。RFID チップが利用される前に、産業貿易業界からの PIA 報告書がデータ保護執行機関に提出されなければならない。

長旅の終わり―EU テレコミュニケーション指令の採択（No.4.4）

・2009 年の終わりに採択された電子コミュニケーションに関する EU 指令（ePrivacy Directive）の改正では、テレコミュニケーション・サーヴィスの利用者の権利が強化されている。よって、データ保護違反に際して、データ主体のプライヴァシー侵害が予期される場合、テレコミュニケーション・サーヴィスのプロヴァイダーは、監視機関及びデータ主体に対して、その旨を通知しなければならない。利用者の同意を得たプロファイリングについては、クッキーやその他の識別子（identifier）に記憶することのみが許されている。しかしながら、同指令の改正を実施するために向けられた現在の立法手続は検討されていない。私は、この ePrivacy 指令によって向上されたデータ保護の要件から、ドイツのインターネット利用者が利益を受けるために、テレメディア法（Telemedia Act）の修正が不可欠であると考えている。

彼らはあなたがどこにいるのか知っているので―時間と共に変化するローケイション・サービス（No.6.2）

・テレコミュニケーション法（Telecommunications Act）の現在の改正が、ネットワーク管理者による携帯電話の不公平な「古典的」（classical）場所に対する保護を促進させている。たとえば、契約者が、自身の場所を突き止めるものと偽って、そのパートナーや第三者によって利用されている携帯電話の場所を把握している。他方、増加する GPS や WLAN の位置情報を利用したスマートフォンの重要な場所に対する適切な保護は、依然として欠いている。

口座スクリーニング手続の統制（No.9.8）

・私は、国家機関による会計のマスター・データの自動検索が着実に上昇していることに懸念を有している。2010 年には、金融機関及び社会保障局が、58,000 件についてより多くのデータを求めた（2009 年は 44,000 件）。この要望数は、ここ 5 年だけでも 5 倍以上に増加している。また、警察、関税局、検察局による犯罪起訴のための銀行口座の自動検索の数も増加している。2010 年には、105,000 件の検索が行われ、前年比 15 パーセントの増加となった。よって、私の見解では、口座データの自動検索の力をテストすることが不可欠であると思う。

電子給与明細（Electronic remuneration statement、No.11.1.3）

・長い議論を経て 2009 年春に制定された ELENA 手続法によって、社会保障の分野における最大のデータ処理プロジェクトのひとつが、法で規制されることになった。2010 年の初期から、3300 万人以上被用者データが、ELENA 手続に保存されている。この手続の将来については、議論が多く、憲法上の不服申立の対象ともなっている。電子給与明細の方法の修正は、データ保護や情報セキュリティのために保障された明文の要件を下げるものであってはならない。

電子健康カード（No.3.4）

・2010 年春に、電子健康カード（e 健康カード）の実施に参加する利害関係人の責任と任務が再分配された。これは、できれば今年に実効的な実施を開始させる意図によってなされた。この電子健康カードの導入の遅れは、データ保護法に関する問題を引き起こしている。たとえば、現在までのところ、情報セキュリティに関する連邦部局によって認証された第一世代の健康カードの暗号化技術は、2015 年までしかその利用を許されていないのである。保険対象の人々のデータ保護のための立法規制の発効日も遅れている。私は、このプロジェクトを引き続き監視し、この分野におけるとりわけ繊細なプライヴァシーの利害関係を守るよう主張していくつもりである。

民間の追加的保険を提供する際の健康保険事業による違反行為（No.15.7）

・法定の健康保険事業 2 社が民間の健康保険事業と協同した際、極度に深刻なデータ保護法の違反行為が行われたため、私は、その当該法定健康保険事業 2 社の従業員及び前述の民間の健康保険事業の従業員に対して、権限ある検察局と共に起訴をした。その法定の健康保険事業は、その協力関係にある民間の健康保険事業に対して、彼らの保険対象者に関する一部非常にセンシティヴなデータにアクセスすることを認めていた。そして、その起訴後 3 年の間に、アウリッヒ（Aurich）とオルデンブルク（Oldenburg) の検察局との間で、何回かの予備的調査がなされたものの、現在ではそれがなくなった。なぜなら、時間の経過によって訴追の維持が困難となり、それが取り下げられたからである。このように、公的な訴追の活動が不活発なことが、情報の自己決定に対する基本的権利の侵害となることがある。

民間のコール・センターによる義務遂行の際のお粗末なデータ保護（No.11.1.4）

・法定健康保険事業において、私は、深刻なデータ保護違反を発見した。健康保険事業は、顧客とのコミュニケーションのため社内にコール・センターを設けているが、24 時間のサーヴィス提供を求める保険対象者の要求に沿うため、その保険事業は、その業務をある民間企業に委託した。そして、その民間会社と提携している企業が個人の相談員に対して、非常にセンシティヴな健康データを含む保険対象者のすべてのデータベースにアクセスすることを認めていた。この点について、私は、データ保護の確保、とりわけセンシティヴデータに関しては、幹部職員（chief executive）によって取扱われるべきであり、それを従業員、契約受諾者（contract acceptors）又は他の契約当事者に委ねることはできないと指摘している。

（2）苦情処理・紛争解決

連邦監察官オフィスでは、特別の相談室をもっていない。2010 年には、6087 件の国民からの苦情を処理した。なお、電話対応のための特定の職員はおらず、個々の質問は、能力のある職員によって回答されることになっている。

（3）権限行使

連邦データ保護法 24 条 1 項は、連邦の公的機関が本法や他のデータ保護規定を遵守しているかについて、連邦監察官が監視すると定めている。よって、連邦の公的機関は、連邦監察官とその職員がその職務を遂行する際に協力する義務がある。とりわけ、連邦監察官には、次の権限が与えられなければならない。

・質問に対する情報、および、あらゆる文書、とりわけ、同条 1 項の監視に関連する記録されたデータやデータ処理プログラムを検査する機会

・いついかなる場合であっても、敷地内への立入（24 条 4 項）

相手方行政機関による個人データの違法、不当な処理等を確認したら異議を唱え、相手方の見解の表明を求めるということになる（25 条）。場合によっては､連邦監察官は改善勧告を行う（26 条 3 項）。勧告に従わなければ、活動報告書の中で公表し（26 条 1 項）、連邦議会における質問の対象となる可能性を探る。議会質問があれば、所管大臣に答弁の必要が生じることになるからである。

このように、連邦監察官は、連邦の他の公的機関に対し、法の遵守を監視し、助言を提供し、データ保護法違反を発見した場合、苦情を申し立てることもできる。しかし、他の行政機関に対して指示や命令を出す権限や直罰を科す権限はない。

なぜなら、同監察官は、いずれの組織のもとにも属さず、上下関係が存在しないからである。行政組織内部で処罰を科すには、自らの組織が上級行政庁である必要があるとドイツでは考えられている。

なお、連邦監察官の権限や能力は、連邦の公的機関によって広く認知されているものの、これらの権限を行使する際に、とりわけ、連邦の金融機関や情報機関との間で問題が生じることが稀にある。

他方、私的部門を所掌するデータ保護監督機関は、データ保護法違反を発見した場合、その民間事業者に対する行政罰（43 条)、刑罰（44 条）という直罰規定を利用できる。行政罰の過料の上限は、軽微なデータ保護違反である 43 条 1 項の場合には、5,000 ユーロであるが、重大なデータ保護法違反である場合には、300,000 ユーロである（43 条 3 項)。他方、刑罰については、2 年以下の懲役又は罰金となっている（44 条 1 項)。

（4）他の機関との連携

連邦監察官は、連邦ネットワーク庁、連邦情報セキュリティ室などと協力し、データ保護措置の発展に努めている。

（5）国際連携

EU の加盟国であるから、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･出席している。また、ケース･バイ･ケースで外国のカウンターパートと協力している。通常、連邦監察官は、春に開催される欧州データ保護会議（European Data Protection Conference）及び秋に開催される国際データ保護・プライバシー・コミッショナー会議（International Conference of Data Protection and Privacy Commissioners）には出席している。

4　監督機関の課題等

現在、連邦監察官が抱えるデータ保護に関する大きな課題のひとつは、州のコミッショナーの独立性に関する欧州委員会との対立である。

具体的には、州レベルのデータ保護機関（コミッショナー）が欧州データ保護指令 95/46/EC の 28 条 (1) による「完全な独立性」（complete independence）を有するかに関して欧州委員会からドイツに対して疑義が出され（具体的には、バイエルン等ドイツ 16 州のうち半分の 8 つの州で内務省の下にある監督官庁が民間部門を所管している点について)、ドイツがその要件の解釈を争った結果、2010 年に欧州司法裁判所でドイツの主張を否定する判断がなされたということである。

この判決を受けて、連邦監察官オフィスでは、州コミッショナーが、独立性要件を充足するか否かについて引き続き議論しているという。同判決の概要は以下のとおりである。

ドイツの州データ保護機関の独立性に関する欧州司法裁判所大法廷判決

（2010 年 3 月 9 日）

（Case C-518/07）

European Data Protection Supervisor v. Federal Republic of Germany

判決

1. 欧州委員会（the Commission of the European Communities）は、その申出により、当裁判所に対して以下のことを宣言するよう求めている。すなわち、ドイツ連邦共和国は、それぞれの州における公的部門以外の個人データの処理を監視する責任を有する機関を州の監視に服させることによって、また、その結果、そのデータの保護を確保する責任を有する監視機関の「完全な独立性」という要件を不正確に解釈することによって、個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令 95/46/EC（データ保護指令）の第 28 条 (1) 第 2 文に定められている義務を履行していないというものである。

法的文脈

2. 「監視機関」と題された指令 95/46/EC 第 28 条では、次のように定めている。

(1) 各加盟国は、ひとつ以上の公的機関が、本指令に従って当該加盟国が制定した規定のその領域内における適用を監視する責任を有することを定めるものとする。

これらの機関は、与えられた職務の遂行に際して、完全に独立して活動するものとする。

(2) 各加盟国は、個人データの処理に関する個人の権利や自由の保護に関係する行政措置を策定又は行政立法を定める場合には、監視機関に相談すべきことを定めるものとする。

(3) 各監視機関は、とりわけ、以下の権限を付与されるものとする。

・処理作業の目的物となるデータへのアクセス権限や監視の職務遂行のために必要なあらゆる情報の収集権限を含む調査権限。

・たとえば、処理作業が実施される前に、第 20 条に従った勧告権限とその勧告の適切な公開を確保する権限、データのブロック化、消去又は破壊を命じる権限、仮又は確定的に処理の禁止を命じる権限、管理者を警告又は譴責処分に付す権限、問題点を国会又はその他の政治機関に付託する権限などの実効的な介入権限。

・本指令に従って制定された国内法が侵害された場合に、法的手続きに関与する又はこのような違反行為を司法当局へ通知する権限。

監視機関による決定に対して不服のある者は、裁判所へ訴えることができる。

(4) 各監視機関は、個人又は個人を代表する組織から申し立てられた個人データの処理に係る個人の権利及び自由の保護に関する請求を審理するものとする。関係する個人は、その申立ての結

果に関して通知を受けるものとする。

とりわけ、各監視機関は、本指令の第 13 条に従って制定された国内法が適用される場合に、データ処理の適法性の調査に関する申立ての請求を審理する。当該個人は、少なくとも、調査が行われたことについての通知を受けるものとする。

(5) 各監視機関は、その活動に関する報告書を定期的に作成するものとする。その報告書は公開されるものとする。

(6) 各監視機関は、問題となっている処理に対していかなる国内法が適用されるかに関わらず、自らの加盟国の領域内において、第 3 項に従って与えられた権限を行使することができる。各監視機関は、その他の加盟国の監視機関によって、その権限行使を求められることがある。

監視機関は、とりわけ、あらゆる有用な情報を交換することによって、その職務の遂行に必要な範囲で、お互いに協力するものとする。

(7) 加盟国は、監視機関の構成員及び職員が、雇用の終了後であったとしても、アクセスした秘密情報に関して、職務上の秘密保持義務を負うことを定めるものとする。

3. 個人データの処理に係る個人の保護について、ドイツ法では、その処理が公的機関によってなされるか否かによって違いを設けている。

4. よって、公的機関によるデータ保護に関する規定の遵守の監視について責任を有する機関と、非公的機関や公法によって規律される市場で競争する事業によるデータ保護の遵守の監視について責任を有する機関との間で違いがある。

5. 公的機関によるデータの処理は、連邦レベルにおいては、個人データの保護及び情報の自由に対して責任を有する連邦の代表者（連邦監察官）によって、また、地方レベルにおいては、地域のデータ保護に責任を有する代表者によって監視される。それらの代表者は、それぞれの議会に対してのみ責任を負い、通常、彼らの監視の客体である公的機関からのいかなる検査、指示又は他の影響に服することはない。

6. 他方、非公的機関によるデータの処理について責任を有する機関は、州によって異なる。しかし、州レベルのすべての法律は、その監視機関が州の検査に服することを明示している。

訴訟前手続

7. 非公的機関が個人データの処理にかかる個人の保護に関する規定を遵守することの確保責任を有する機関（データ保護機関）が、州の検査に服することは、指令 95/46/EC の第 28 条 (1) 第 2 文に反するものと考えられ、すべてのドイツの州がその場合に該当するため、欧州委員会は、2005 年 7 月 5 日に、ドイツ連邦共和国に対して正式な通知文書を送達した。ドイツ側は、2005 年 9 月 12 付けの文書で回答し、そこでは、関連するドイツの監視制度が当該指令の要求に従っていると主張していた。そこで、欧州委員会は、2006 年 12 月 12 日に、ドイツ連邦共和国に対し理由付きの意見書を送達し、以前になした主張を繰り返した。それに対する 2007 年 2 月 14 日の回答では、ドイツ連邦共和国がその従来の立場を変えなかった。

8. 以上のような状況において、欧州委員会は、2007 年 11 月 22 日に、本件訴訟を提起した。
9. 2008 年 10 月 14 日の決定により、本裁判所の長（President）は、欧州データ保護監視機関（European Data Protection Supervisor）に対して、欧州委員会が求める決定形式を支持して、本ケースへ介入することを許可した。

訴訟

両当事者の主張

10. 本紛争は、指令 95/46/EC の第 28 条 (1) 第 2 文における「完全に独立して」という文言及び個人データの処理にかかる個人の保護に関する監視機関の権限行使に対する、欧州データ保護監視機関によって支持されている欧州委員会とドイツ連邦共和国の 2 つの異なる解釈に関するものである。
11. 「完全に独立して」という文言の広義の解釈に依拠する欧州委員会及び欧州データ保護監視機関の見解においては、監視機関がその職務を完全に独立して行うという要件は、監視機関が、他の機関又は行政外の機関によって行使される影響であろうとも、いかなる影響も受けてはならないという意味に解釈されるべきである。ドイツにおいて、公的部門以外で個人データの処理に係る個人の保護に関する規定の遵守を確保する責任を負う機関が、州の検査に服することは、その要件に違反するものである。
12. これに対して、ドイツ連邦共和国は、「完全に独立して」という文言について狭義の解釈を提案し、指令 95/46/EC の第 28 条 (1) 第 2 文は、監視機関が監視下に置く公的機関から独立していなければならず、外部の影響にさらされてはならないという意味で機能的な独立性をもつことを求めていると主張している。とすれば、ドイツ連邦共和国の見解においては、ドイツの州において行使される州の検査は、このような外部の影響とはならず、むしろ、監視機関と同様の行政機関に与えられた権限によって行使され、また、監視機関のように指令 95/46 の目的を達成するために要求された組織の内部監視構造であることになる。

当裁判所の事実認定

監視機関の独立性に関する要件の範囲

13. 本件訴訟の実体の評価は、指令 95/46/EC 第 28 条 (1) 第 2 文に含まれる独立性の要件の範囲、つまり、その規定の解釈にかかっている。その意味で、その規定の文言そのもの及び指令 95/46 の目的や構造を考慮に入れなければならない。
14. 第一に、指令 95/46/EC 第 28 条 (1) 第 2 文の文言に関してであるが、「完全に独立して」という文言が同指令によって定義されていないため、その通常の意味を考慮することが必要である。公的機関との関係では、「独立性」という用語は、通常、当該機関が、いかなる指示又は圧力の下にも置かれずに、完全に自由に活動できることが確保されている状態を意味する。
15. ドイツ連邦共和国の見解とは異なり、独立性の要件が監視機関とその監視に服する機関との間の関係にのみ関するものであると示唆するものはない。それどころか、独立性という概念は、「完全に」

という形容詞が付されており、このことは、監視機関への直接又は間接的な外部の影響から離れた決定権限であることを含意している。

16. 第二に、指令 95/46 の目的についてであるが、個人データの処理に係る個人の保護に関する国内法の調和を通じて、同指令は、加盟国間のこうしたデータの自由な流通を主に確保しようとしていること、それは、14 条 (2)EC の意味における域内市場の確立や機能にとって必要であることが、その前文第 3,7,8 文から明らかである。

17. しかしながら、個人データの自由な流通は、私的な生活に対する権利を侵害する可能性が高いことが、とりわけ、ECHR（欧州人権条約）の第 8 条及び EC 法の一般原則において認められている。

18. こうした理由から、指令 95/46 の前文第 10 文及び第 1 条から明らかなように、後者（ECHR の第 8 条及び EC 法の一般原則）は、既存の国内法によって保障されている保護を弱めようとするものではなく、反対に、EC において、個人データの処理に関する基本的な権利や自由の高い水準の保護を確保しようとするものである。

19. よって、指令 95/46/EC 第 28 条によって設置された監視機関は、これらの基本的な権利や自由の庇護者であり、加盟国におけるその存在は、指令 95/46 の前文の第 62 文に明記されているように、個人データの処理に係る個人の保護における必須の組織であると考えられる。

20. その保護を確保するために、監視機関は、一方では、私的生活に対する基本的な権利の保護と、他方では、個人データの自由な流通を求める利益との妥当なバランスを確保しなければならない。さらに、指令 95/46/EC 第 28 条 (6) では、それぞれの国の監視機関が互いに協力することを求められており、必要な場合には、他の加盟国の監視機関からの要請により、その権限を行使することさえしなければならないことになっている。

21. 国家の監視機関の独立性の保障は、個人データの処理に係る個人の保護に関する規定の遵守の監視の実効性及び信頼性を確保しようとするものであり、その目的に照らして解釈されなければならない。それは、それらの機関や職員に特別な地位を付与するためではなく、彼らの判断によって影響を受ける個人や組織の保護を強化するために設立されたものである。よって、監視機関がその職務を遂行する際には、客観的かつ公平に活動しなければならない。その目的のため、監視機関は、監視対象である機関の影響のみならず、国家や州からの直接又的又は間接的影響を含む外部からの影響を受けてはならないのである。

22. 第三に、指令 95/46 の構造であるが、それは、EC286 条及び Regulation No 45/2001 と同義に理解されなければならない。後者は、EU 組織や機関による個人データ処理及びそのデータの自由な流通に関するものである。指令 95/46 も、それらの目的を達成しようとするものであるが、加盟国におけるそのようなデータの処理に関するものである。

23. 監視機関が国家レベルで存在することと同様に、個人データの処理に係る個人の保護に関するルールの適用を確保する責任を有する監視機関は、EC レベルでも定められている。すなわち、欧州データ保護監視機関である。規則 No 45/2001 の 44 条 (1) に従って、その機関は、完全に独立してその職務を遂行することになっている。そこで、44 条 (2) では、その職務遂行に際して、欧州デー

タ保護監視機関が、いかなる者にも指示を求め又はいかなる者からも受けることはないと付け加えることによって、独立性の概念を明らかにしている。

24. 規則 No 45/2001 の 44 条及び指令 95/46/EC 第 28 条が同じ一般的な概念を基礎としていることに鑑みると、これら 2 つの規定は、同様に解釈されるべきであり、その結果、欧州データ保護監視機関の独立性のみならず、国家の監視機関の独立性も、その職務遂行に関するいかなる指示も受けないことが含まれることになる。

25. 指令 95/46/EC 第 28 条 (1) の第 2 文の文言そのもの、その目的、また、同指令の構造に依拠することによって、その第 28 条 (1) 第 2 文の明確な解釈に達することが可能である。よって、同指令の制定経緯を考慮すること、また、この点について意見が対立している同委員会やドイツ連邦共和国によって提出された主張について判断することは必要ではない。

26. 以上のことに鑑みると、指令 95/46/EC 第 28 条 (1) の第 2 文は、公的機関以外の個人データの処理を監視する責任を有する監視機関が、外部の影響を受けずにその職務を遂行できるという独立性を享受しなければならないという意味に解釈されることになる。その独立性は、監視対象の機関によって行使されるあらゆる影響のみならず、直接的又は間接的かに関わらず、私的な生活に対する権利の保護と個人データの自由な流通の妥当なバランスを図るという職務の監視機関による遂行に疑問が生じうる他のいかなる外部的な影響を排除するものである。

州の検査

27. 次に、ドイツにおいて監視機関が服する国家の検査が、上記に定義した独立性の要件と整合的であるか否かについて評価することが必要である。

28. この州の検査は、いかなる形で行われるものであれ、原理的には、個々の州政府やその政府に服する行政機関に対して、直接又は間接的に監視機関の決定に影響を与えること、その例としては、おそらく、その決定を取消し又は変更することを許容するものである。

29. 確かに、ドイツ連邦共和国の主張するように、州は、監視機関の活動が国内法及び EC 法を遵守することを確保しようとしているに過ぎず、それゆえ、これらの監視機関に対して、個人データの処理に係る個人の保護や基本的な権利と整合しない政治的目的を潜在的に追求することをこれらの機関に義務付けようとしているわけではないということは、ア・プリオリに認められなければならない。

30. しかしながら、一般的な行政の一部であり、それゆえ、それぞれの州の政府の統治下にある監視機関を検査することは、監視機関が個人データの処理に関する規定を解釈、適用する際に客観的に活動することを妨げる。

31. 欧州データ保護監視機関がその見解の中で主張したように、関係する州の政府は非公的機関による個人データの処理が問題となっている場合に、そのデータの保護に関する規定の不遵守に関する利害を有するだろう。たとえば、公私の共同事業や私的部門との公的契約のように、その政府が実際に又は潜在的に参加していた場合、その政府自身がその処理に関して利害関係を有する当

事者である。また、その政府は、とりわけ、課税や法執行の目的において、一定のその職務を遂行するためにデータベースにアクセスするのに必要である又は有用であるという場合には、特定の利害関係を有するだろう。さらに、その政府は、州や地域にとって経済的に重要な一定の企業によるデータ処理に係る個人の保護に関する規定の適用に際して、経済的な利益を尊重する傾向にあるだろう。

32. これに加えて、監視機関を検査することが、監視機関の決定に政治的な影響を及ぼすという危険性のみによっても、その機関の職務を独立して行うことを妨げるのに十分であることが指摘されるべきである。第一に、欧州委員会が主張したように、監視機関の意思決定慣行を検査することに鑑みると、これらの機関の側に「事前遵守」(prior compliance) というものが存在している可能性がある。第二に、私的生活に対する権利の庇護者としての監視機関によって決められた役割の目的のためには、その機関の決定、すなわちその機関自身がいかなる公平性を疑われるものであってはならない。

33. 以上の考察に鑑みると、公的部門以外の個人データの処理を監視する責任のあるドイツの監視機関に対して行使される州の検査は、独立性の要件と整合的とはいえない。

ドイツ連邦共和国によって主張された EC 法の原則

34. ドイツ連邦共和国は、加盟国に対し、公的部門以外の個人データの処理に関する監視機関に対する試験的な検査制度を廃止するよう義務付けていると指令 95/46/EC 第 28 条 (1) の第 2 文における独立性の要件を解釈することは、EC 法の様々な原則に反する妥当と主張している。

35. 第一に、その加盟国の意見では、とりわけ、民主主義の原理が独立性要件の広義の解釈を排除するという。

36. この原則は、ドイツの憲法のみならず、EU6 条 (1) にも明記されており、行政は、議会に対して責任を負う政府の指示に服することを求めている。よって、市民や事業者の権利への介入の適法性は、所掌の大臣の検査に服する。個人データの処理に係る個人の権利の保護に対して責任を有する監視機関は、指令 95/46/EC 第 28 条 (3) のもと、公的機関以外の市民や事業者へ一定の介入権限を有するのであるから、その活動の適法性に対しては、その適法性や内容を監視する制度などによってより高い検査が間違いなく必要である。

37. 民主主義の原理は、EC 法の一部を構成しており、EU6 条 (1) で欧州連合の基礎として明記されていることに留意すべきである。加盟国に共通した原理のひとつであるから、それは、指令 95/46/EC 第 28 条のような 2 次的な法律の立法を解釈する際にも考慮に入れられなければならない。

38. この原則は、古典的な階層的行政の外にあり、多かれ少なかれ政府から独立している公的機関の存在を排除していない。加盟国におけるこのような監視機関の活動の存在と条件は、法律によって規制されており、ある加盟国では、憲法によって規制されている。そして、これらの監視機関は、その法律を遵守し、権限のある司法の審査に服することが求められている。ドイツの司法制度に

おいて存在するように、このような独立した行政機関は、法律に従うことを求められ、権限のある司法の審査に服するが、しばしば規制的な役割を有しており、政治的な影響を受けてはならない職務を遂行する。データの保護に関する監視機関の職務に関しては、まさにこのことがあてはまる。

39. 確かに、これらの機関に対する議会の影響の欠如は考えられない。しかしながら、指令 95/46 が、加盟国に対して、このような議会の影響という義務の欠如をなすものでは全くないことが指摘されるべきである。

40. よって、まず、監視機関の管理者が、議会又は政府によって指名される。次に、制定者はその機関の権限を画定する。

41. さらに、制定者は、監視機関の活動を議会へ報告するよう、これに義務を課すことができる。この点、各監視機関が定期的にその活動に関する報告書を作成し、それを公にする旨について定める指令 95/46/EC 第 28 条 (5) と比較できるだろう。

42. 以上のことに鑑みると、公的部門以外の個人データの処理に係る個人の保護について責任を有する監視機関に対して、一般的な行政として独立した地位を与えることは、それ自体で、民主的な正当性をその機関から奪うことにはならない。

43. 第二に、これもドイツ連邦共和国による主張であるが、EC5 条第一文で明記され与えられた権限の原則が、欧州共同体に対して、それに与えられた権限及び EC 条約で定められた目的の範囲内で活動することを義務付けている。

44. この点に関し、ドイツ連邦共和国は、より高い行政機関に関する監視機関の独立性は、指令 95/46 の法的基礎として機能する EC 条約の 100A 条を根拠として要求されていないと主張している。

45. その規定は、欧州共同体の立法者に対して、域内市場の確立とそれが機能する状態を向上させる措置をとる権限を与えており、その立法者は、純粋にその目的を有し、EC 条約によって保障された経済的自由の障害の除去に寄与しなければならない。

46. 既に指摘したように、監視機関の独立性は、彼らの決定に影響を与える可能性のある外部の影響から自由でなければならない範囲において、指令 95/46 の目的に照らして必要な要素である。

47. その独立性は、すべての加盟国において、個人データの保護の同質的な水準を作り出し、その結果、域内市場の確立とそれが機能するために必要とされるデータの自由な流通に寄与するために必要である。

48. 以上のことに鑑みると、監視機関の独立性の要件に対する広義の解釈は、指令 95/46 の法的基礎として機能する EC 条約の 100A 条の下で欧州共同体に与えられる権限の範囲を超えていることにならない。

49. 第三に、ドイツ共和国連邦は、EC5 条の第 2,3 文における、従属性（subsidiarity）と均衡性（proportionality）の原則及び、EC10 条に明記されている、加盟国と欧州共同体の組織との誠実な協力の原則について指摘している。

50. 同国は、とりわけ、従属性と均衡性について、EU 条約及びアムステルダム条約による EC 条約に付加されたプロトコール第 7 文に着目している。それによれば、EC 法を侵害することなく、確立された国内の取り決め及び加盟国の法制度の組織や機能に対して配慮するよう注意が払われるべきであるという。

51. ドイツ連邦共和国に対して、その法秩序とは異質の制度の採用を義務付けること、つまり、国家のレベルを超えてデータの保護に関する立法のモデルとして活動し、ほぼ 30 年間近く設立されてきた実効的な監視制度をあきらめることを義務付けることは、その要件と整合的ではないという。

52. これらの主張は、受け入れられない。これまで指摘したように、指令 95/46/EC 第 28 条 (1) の第 2 文で明記されている独立性の要件の解釈を州の検査を排除する意味と解することは、EC 条約の目的を達成するのに必要なことを超えるものではない。

53. 以上のすべての考察に鑑みると、それぞれの州において、非公的機関や公法によって支配されている市場で競争する事業者による個人データの処理に関する監視について責任を有する監視機関を州の検査に服させることによって、また、その結果、これらの監視機関が「完全に独立して」職務を遂行するという要件を誤って解釈することによって、ドイツ連邦共和国は、95/46/EC 第 28 条 (1) 第 2 文の義務を履行していないと判示されなければならない。

＊ 本稿におけるドイツの法制度の概要については、藤原靜雄「ドイツ」「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」（消費者庁、2009 年）に依拠している。本稿では、それを基礎として、その後のドイツの動きを付加したものであるが、筆者が英語文献のみ解読可能であるため、英語に翻訳された原文を参考にしていること（固有名詞などがドイツ語ではなく英語になっている点など）について、ご了解いただきたい。

参考文献

藤原靜雄「個人情報保護法制の国際比較 ドイツ」比較法研究 64 号（2002 年）16 頁。

同 「ドイツにおける個人情報保護の実際〜わが国の過剰反応問題を考える一視座」
筑波大学法科大学院創設記念『融合する法律学（上)』(2006 年、信山社）134 〜 159 頁。

同 「資料 改正 連邦データ保護法 (2001 年 5 月 23 日施行)」季刊行政管理研究 99 号
(2002 年）76 頁。

iv. スウェーデン

本章を執筆するにあたり、平成 23 年 3 月に行われたヒアリング調査において、スウェーデン・データ保護検査院 Gaby Borglund（Legal Adviser）及び Birgitta Abjornsson（International Legal Adviser）から有益な資料とともに詳細な回答をいただいた。ここに協力していただいた方々に謝意を記す。

1　個人情報保護法制の概要

（1）法律名

個人データ法（Personuppgiftslag（1998:204））[1]

（1998 年 10 月 24 日施行：1973 年データ法を全面改正）

なお、個人データ法の補足的な規則として、個人データ施行令（全 14 条）がある。

（2）目的

個人データの処理によって個人の人格（personal integrity）の侵害に対する個人の保護（第 1 条）

（3）適用範囲

個人データは「生存する自然人に直接的に又は間接的に帰属するあらゆる種類の情報」と定義される（第 3 条）

2005 年 6 月 8 日、データ保護検査院は、スウェーデン反海賊団体が用いていた IP アドレスを個人データに該当するという決定を下した[2]。他方で、街や通りの名前、髪や目の色に関する人の一般的な描写、パソコンの閲覧履歴は個人データに当たらないとされてきた[3]。

1　スウェーデンの個人データ法に関する紹介としては、平松毅『個人情報保護－理論と運用』（有信堂・2009）、参照。また、法制度については、CHRISTINE KIRCHBERGER, CYBER LAW IN SWEDEN (2011) を参考にした。個人データ法の翻訳としては、菱木昭八朗「スウェーデン個人情報保護法」新聞研究 582 号（2000）86 頁以下、参照。

2　Decision by the Data Inspection Board, 8 June 2005, nr 503-2005. See also Decision by the Administrative Court of Appeal (Kammarrätt), 8 June 2007.

3　Decision by the Supreme Administrative Court (Regeringsrätten), 11 October, 1999.

・適用除外

自然人が行う純粋に私的な性格の活動については法が適用されない。(第 6 条) また、報道の自由と表現の自由と矛盾する限りにおいて法が適用されない。(第 7 条)

2001 年 6 月 12 日、スウェーデン最高裁判所は、報道目的のためにインターネット上に個人情報を公表することは個人データ法上の第三国移転には該当しないという判決を下している[4]。

(4) 内容 (権利・義務規定に関する内容)

・個人データの管理者 (個人データの処理の目的と手段を決定する者) は次の義務を履行しなければならない。(第 9 条)

ⅰ) 個人データ処理の合法性
ⅱ) 正確な，かつよい慣行による処理
ⅲ) 特定かつ明確化された目的のもとでの個人データの取扱い
ⅳ) 情報が収集された利用目的と一致しない処理の禁止
ⅴ) 処理の目的に関連して相当かつ関係する限りでの処理
ⅵ) 目的に関して必要な限りでの個人データの処理
ⅶ) 個人データの正確性と最新化
ⅷ) 不正確・不完全な個人データの訂正・削除
ⅸ) 処理の目的を超える期間の個人データの保持の禁止

(5) 監督・登録制度

監督機関は、ⅰ) 処理された個人データへのアクセス、ⅱ) 個人データの処理及び処理の安全性に関する情報及び文書、ⅲ) 個人データの処理に関連するその他の前提となる文書等へのアクセスを要請する権限を有する (第 43 条)。この要請に従わない場合、個人データの管理者に対し、個人データの処理を禁止することができる。(第 44 条)

また、データ処理を行う事業者はデータ保護検査院に対して事前に書面で通知をしなければならない (第 36 条)。データ処理とは、収集、記録、体系化、蓄積、適合化、修正、修復、集計、使用、開示、移転等の自動処理で行われるかどうかに関わりなく、個人データに関する処理を行ういかなる機能も意味することとされている (第 3 条)。また、マニュアル処理であっても、登録のため体系化され、検

---

4 Public Prosecutor v. Ramsbro, Decision of 12 June 2001, no B 293-00.
また、Bodil Lindqvist 判決において、欧州司法裁判所は、サーバーからインターネット利用者に対して自動的に情報が送信されていないこと、またインターネットのサーバー上に個人データをアップロードさせる個人と、当該サーバー上で個人データにアクセスした個人とのあいだに直接的な個人データの移転があったとは言えないことなどを理由として、スウェーデンに拠点のあるインターネット・サーバー上に示された個人データが EU データ保護指令 25 条にいう「国際移転」には該当しないと判断した。Bodil Lindqvist, Case C-101/01 [2003] ECR Ⅰ -12971.

索可能な状態であれば、そのような処理も法の義務対象となる。

例外として、①データ保護検査院に対して事業者があらかじめ指名した個人データ監督官を登録している場合、②他の法令で別途定められている場合、③線形テキストにおいて個人データが処理される場合、④ NPO によって個人情報が処理される場合、⑤登録された個人が処理に同意している場合がある。

（6）その他

○ 1998 年法全面改正

1973 年データ法は、数回の改正が行われたものの、時代の変化とともに 1980 年代後半には法の大部分が現状を反映していなかった。そのため、1989 年政府にデータ保護に関する委員会が設置され、4 年間の検討を経て 1993 年に最終報告書が公表された。当時スウェーデンは EC に加盟していなかったものの、1994 年に EU に加盟するとともに、1995 年 EU データ保護指令との整合性を保つことができるよう 1997 年に全面改正案が公表された。1998 年に全面改正されたデータ保護法が施行されると、インターネット上の個人データの公表について「私のインターネットに干渉するな」というスローガンのもとメディアやインターネット利用者からの抗議の声があがった。これに対し、議会は、次の 3 段階の行動計画を示してきた。すなわち、短期的には、インターネット上の個人データの公表を促進するために法改正の検討を行うこと、中期的には、法改正による影響が日常的なデータの取り扱いではなく、個人データの乱用を防止するものとすべきこと、長期的には、EU データ保護指令の改正への働き掛ける、というものであった。すでに短期的な計画として、個人データの第三国移転については、2000 年 1 月 1 日の法改正で対処されている。また、中期的な課題として、個人データの乱用防止に向けた調査を行い、2004 年に報告書が示され、個人データの乱用防止に向けた公的機関と企業における対策が取られてきた[5]。長期的な計画として、スウェーデンにおけるデータ保護に関する諸問題を契機とする EU データ保護指令の改正の提案についてはすでに加盟国の中でも賛同が見られ、2010 年から本格化した EU データ保護指令の改正に向けた検討が行われている。

---

5 Sören Öman, Implementing Data Protection in Law, Scandinavian Studies in Law vol. 47 (2004) at 391.

○ 2007 年法改正

2007 年 1 月 1 日の個人データ法一部改正において、体系化されていない個人データの取り扱いについて新たな条項(第 5 条 a)が設けられた。法改正前までは、デジタルカメラで撮影された写真をインターネット上に公表することがデータの処理に該当するとされてきた[6]。しかし、今回の法改正によって、音、画像、電子メール、インターネット上のテキスト等の体系化されていない個人データについては、個人データ処理の基本要件、データ処理の届出、登録された個人への告知、第三国移転の規定が適用されないこととなった。もっとも、体系化されていない個人データについては、不適切な目的の処理の禁止、合理的な理由なく大規模なデータデータ処理の禁止、個人データの訂正、名誉毀損の禁止、秘匿性の確保といった義務がガイドラインとして示されている。

また、ソーシャル・メディア等におけるインターネット上の個人データの取扱いは、ソーシャル・メディアのサービスを提供する事業者のみならず、それを利用するユーザーもまた一定の義務が課されることなっている（たとえば、Twitter のアカウント所有者は自らのつぶやきについて個人データ処理の管理者となる）[7]。

○関連法

個人データ法のほかに、個人データの保護に関連する法律としては、次のものがある。

・電子通信法（2003 年）Lag (2003:389) om elektronisk kommunikation
　電子通信分野における個人データの処理に関する規則を定めている。
・公共カメラ監視法（1998 年）Lag (1998:150) om allmän kameraövervakning
　公共の場における監視カメラの使用の許可や公衆への周知等を要件として定めている。
・クレジット情報法（1973 年）Kreditupplysningslag(1973:1173)
　クレジット情報を取り扱う事業者に対してデータ保護検査院への事前の許可を規定している。

○個人登録番号制との関係

個人登録番号（Person Nummer）制は、1947 年に導入の後、住民登録制度のコンピューター処理に伴い 1967 年の住民登録令 7 条及び住民登録告示 4 条を根拠として行われており、スウェーデンに住民登録している者は、すべて識別のため個人登録番号＊を有する。

6　Decision by the Data Inspection Board, 20 Sep. 2005 no. 763-2005.

7　Sören Öman, Trends in Data Protection Law, Scandinavian Studies in Law vol. 56 (2010) at 219.

現在、国税庁が個人登録番号に関する業務を所掌している。なお、個人登録番号については、民間の利用に供する目的で創設されたSPARという機関において、国税庁から一部の情報が提供されている。

個人データ法22条にも個人識別番号に関する次の規定がある。

「個人識別番号に関する情報または分類番号は、同意のない場合、a) 処理の目的、b) 安全な認識の意義、またはc) その他特別の理由によって明確に正当化されるときのみ取り扱うことができる」

データ保護検査院は番号制度に関連して社会保障分野の監視について特に力を入れている。特定の児童の行動を市が知りたいという場合、その児童の行動、たとえば、買春したか、刑務所にいたことがあるかといったセンシティブ・データを用いることの帰結は何であるか、をチェックしてきている。番号制度に関する立法がより適切に執行されるように促してきた。

他方で、近年は減少傾向にあるが、個人登録番号が盗難にあう事例[8]が多く、データ保護検査院はこのような個人登録番号の誤用を防止するために行政機関や企業が保有するファイルをチェックするとともに、このような個人登録番号の盗難に対しては特別法による罰則によって対処されることとなっている。

＊個人登録番号について[9]

個人番号は10桁の番号であり、3つの要素から構成されている。ある地域で2011年4月1日に生まれた男性を例（110401-3234）にとって説明する。まず、最初の6桁は生年月日である。次の3桁は生誕番号（birthnumber）であり、男性は奇数、女性は偶数となっている。3桁の数字は乱数的に付番され、特別の意味を有していない。性別で生誕番号が異なるため，性転換者は性転換時に番号が変わる。最後の1桁はチェック番号を表している。データベース化される情報は、①氏名、②住所、③婚姻の有無、④家族関係、⑤出生地、⑥国籍、⑦移民であるかどうか、⑧住民登録からの離脱原因、⑨死亡地などの情報が含まれる。

個人番号はあらゆる行政手続および民間の取引において広範に使用されている。住民登録、納税、社会保険、雇用・失業、病院、徴兵、運転免許、パスポート、郵便、不動産登記、警察、教育、選挙、統計調査など。民間では銀行取引、保険手続など。統一された個人番号の使用頻度は高く、誰もが自分の個人番号を覚えている。1998年6月8日に可決した年金法案についても、労働市場への参加形態、

---

8 麻薬乱用者が、警察や病院、社会福祉機関に対して別人の名前と個人登録番号を告げていたことから、個人情報登録番号の本人に対して社会福祉機関から麻薬の乱用者であるため、彼女の子どもを児童保護命令の対象とする旨の本人が了知しない手紙が届いた事例、将来を約束されたボクサーが、ある犯罪者が彼の氏名と個人識別番号を利用したことから、ナショナルボクシングチームにおける地位を失いかけた事例、脱税目的の企業監査役として、本人の知らないところで、その公認会計士の氏名と個人識別番号が用いられていた事例がある。アニタ・ボンデスタム「スウェーデンの個人識別システム」法学セミナー578号（2003）52頁。

9 スウェーデンの個人登録番号制については、平松・前掲注1，358頁以下、高山憲之「諸外国における社会保障番号制度と税・社会保険料の徴収管理」海外社会保障研究172号（2010）5頁、鈴木雅人「スウェーデンにおける住民登録番号制度と個人情報保護制度の現状」法学セミナー578号（2003）50頁、参照。

参加期間、参加濃度も多様化しつつ、公正と平等を確保するために、整備されたパーソナル・ナンバー制度を備えているため、ライフスタイルの多様性には十分対応できている。他方で、平等なサービスを提供するために国民総背番号制度などが導入され、それが管理社会化を促進している、という批判が度々行われてきている[10]。

○労働者のプライバシー

従業員の位置情報について GPS を用いて確認する企業があるため、その運用実態とプライバシー侵害の程度について調査を始めている。2011 年 2 月に公表された職場における位置情報技術に関するチェックリスト（Positioning Technology in Working Life）では、次の点について留意することを示されている。

① 個人データ法の適用があることを常に念頭に置くこと
② 誰が個人データの管理者であるかを明確化させること
③ 労働者は必ずしも通常どおり同意することができないこと
④ 個人データ処理の目的を明確にすること（書面による利用目的の特定）
⑤ 必要以上の期間データを保有しないこと
⑥ 労働者に対する明確な情報を提供すること
⑦ 個人データの保護に万全を期すこと

10 岡沢憲芙『スウェーデンの政治』（東京大学出版会・2009）x 頁、参照。

2　監督機関の制度概要

以下の記述は、データ保護検査院におけるヒアリング及び 2010 年次報告書（Datainspektionen, Arsredovisning 2010）を基にしている。

（1）データ保護機関の背景

・名称

データ保護検査院（Datainspektionens）

（2）設置の経緯

・歴史的経緯

1973 年から 1974 年にかけ，データの自動処理やコンピューター等の機械の出現に対して議論が高まり、データ法が成立した。メディアと政党はこれらの新たな現象に対して議論をしたが、コンセンサスの必要性を認めていた。そして、監督制度が必要であるという議論が高まり、データ保護検査院が設置された。

国レベルにおいて個人データ保護法が世界で初めて制定されたのがスウェーデンである。この背景については、次のような事情が考えられる[11]。第 1 に、スウェーデンでは、公文書公開の原則が実践され、個人は当局の端末を利用して希望する公の情報を自身で検索することができることとなっていたが、その適用除外の一つにプライバシー保護（秘密保護法）[12] があり、この具体化が必要であった。第 2 に、1946 年以来，個人登録番号制が採用され、個人情報がどのように利用されるかという危惧に対して特別の配慮が必要であった。第 3 に、行政機関から民間分野に大量の個人情報が移転していることに伴い、プライバシー侵害への統制が必要となった。第 4 に、国勢調査をめぐるトラブルにより個人情報ファイルの処理の仕方をめぐる世論の反発があった。第 5 に、コンピューター技術の発達に対応できる法制度の準備を促す欧州評議会の勧告をスウェーデンの立法者も認識していた。

・EU との関係

スウェーデンは 1995 年に EU に加盟し、同年に制定された EU データ保護指令に基づき 1998 年 4 月 29 日に個人データ法を改正し、1998 年 10 月 24 日に施行した。また、電子通信におけるデータ保護に関する 2002 年 EU 指令については、2003 年 7 月 25 日に電子通信法として国内法化された。

2011 年 3 月、EU データ保全指令（Data Detention Directive）－テロリズム対策の観点からインター

---

11 平松・前掲注 1, 356-358 頁、参照。

12 個人データ法とは別途、1980 年に公布された秘密情報（Sekretesslagen）に関する一般法である秘密保護法がある。同法の紹介については、福本歌子『スウェーデンの公文書公開と言論表現権』（青木書店・1997）123 頁以下、参照。

ネット・プロバイダ事業者が電子メールのIPアドレスや送受信者データを6か月以上保全することを義務付けることなどを内容とする指令―の国内法での実施を延長したことについて欧州委員会からスウェーデン政府に対して1億5000万クローナ（約19億5000万円）の罰金が課されることとなった。社会民主党や緑党といったリベラル派が長期間の保全に抵抗したためである。また、スウェーデンでは、2009年に監視社会に防止する法制度が整備され、スパイ社会やBig Brother社会に対する抵抗があることも国内法での実施延長の背景にある。

（3）法的地位

①組織について

データ保護検査院は政府に財政面などで依存しているが、独立して活動してきている。このような第三者機関はスウェーデンに約250存在する（公的機関それ自体は約400存在する[13]）。その多くが監督機関としての地位である。データ保護に関する監督機関は、データ保護検査院のみである。

・憲法上の位置づけ

スウェーデン憲法は、立憲君主制を採用し、権力分立制（separation of power）ではなく、役割の分担（a separation of function）という仕組みをとっている[14]。したがって、日本における立法、行政、司法という三権分立の構造がそのままあてはまるわけではない。スウェーデン憲法では、統治構造（Regeringsform）、政体の継続法（Successionsordning）、プレスの自由法（Tryckfrihetsfororddning）、表現の自由に関する基本法（Yttrandefrihetsgrundlag）の大きく分けて4つの事項について規定を設けている。

憲法においてプライバシーという文言はないが、“integritet”：「personal integrity」という言葉が用いられ、実質的にプライバシー権の保障をしている。憲法第2章3条2項において、「すべての市民は、自動データ処理の手段によって個人情報の登録から生じた個人の人格へのいかなる侵害に対しても保護される」と規定されている。昨年秋に憲法修正が行われ、個人の状況を調べることによって生じる侵害に対処するため”personal integrity”の強化がされた。スウェーデンにおけるプライバシー権の実質的な意味での保障は、国家からの消極的な防御権としてではなく、国家に一定の作為を求める権利として理解されてきた[15]。

いわゆる第三者機関であるデータ保護検査院の存在について、憲法上の論点は存在しない。また、デー

---

13 Kirchberger, supra note 1, at 23.

14 LAURA CARLSON, THE FUNDAMENTALS OF SWEDISH LAW 25 (2009).

15 榎原猛『プライバシー権の総合的研究』（法律文化社・1991）295頁。

タ保護検査院が唯一のデータ保護機関である。スウェーデンの統治制度では、21 の郡（landsting）と 290 のコミューン（kommuner）があるが、地方に類似の機関や支部は存在しない。

データ保護検査院はオンブズマン * に類似する独立行政機関のひとつとして理解できる。スウェーデン憲法においても立法過程における関係機関から情報の収集と意見聴取が規定されている。国民の声を聴く機関が最重要とされており、第三者機関もそのような機関であると認識している。また、スウェーデンにおいては、「二元的な行政組織」と言われるように、各省とは別に、具体的な行政の執行、重要事項以外の政策決定については、内閣の外局である独立行政機関または地方政府に委任されている。このような二元的な行政組織については、①政策立案と具体的執行とを分化することにより、行政の効率化が図られていること、②個別の政策遂行について上級官庁等からの介入を受けないため、責任の所在が明確になること等の利点があると評されている [16]。

＊スウェーデンにおけるオンブズマンについて [17]

特に重要な役割を果たしてきたのが議会オンブズマン（Riksdagens Justitieombudsman）と司法官（Justitiekanslern）である。1809 年、民主憲法を制定した際に憲法 96 条で一人のオンブズマンを設置することが制度化された。スウェーデン新憲法（1974 年制定）は、第 2 章 6 条において、「国会は、国会が定める規則にしたがって、公務における法令の適用を監視するために、一ないし数人のオンブズマンを選出するものとする。オンブズマンは、規則で指示された事件に対して、法律上の手続を発動することができる。」と規定されている。

オンブズマンは、市民からの苦情の申立て、または職権によって活動を開始するが、その職務を開始する契機となるのは、マスコミの報道、裁判所や行政機関への視察などである。オンブズマンの調査権については、オンブズマンが裁判所、行政機関の審議に出席することができ、また裁判所、行政機関の記録等の文書も利用できることとなっている。いかなる裁判所、行政機関、国、自治体の公務員もは、オンブズマンに要求された情報及び報告を与えなければならない。具体的な権限としては、大臣訴追の国会の決議に基づき、その訴訟を遂行すること、公務員が公務に課せられた義務に反し犯罪を犯した場合に特別検察官として訴追することなどがある。

16『衆議院 EU 憲法及びスウェーデン・フィンランド憲法調査議員団報告書』（平成 16 年 12 月）22 頁。

17 園部逸夫・枝根茂『オンブズマン法〔新版〕』（弘文堂・1997）122 頁以下、参照。

②委員会について

データ保護検査院委員会は 5 名から構成される。政府とは異なる機関であるが、公務員としての身分である。委員長の報酬は 1,052,486 クローナ(約 13,700,000 円)。4 年ごとに選挙がおこなわれるが、通常は再選される。

現在の構成としては、国会議員 2 名、大学教授 1 名、IT 専門家 1 名、地方議員 1 名となっている。

データ保護検査委員会は、政府からデータ保護に関連する照会について 2010 年に 74 項目の検討を行った。

	2010 年	2009 年	2008 年
検討件数	７４	１１６	９７
受付件数	７４	１０７	１１１

表 1　政府からの照会事項に対するデータ保護検査委員会の検討状況（2010 年）[18]

③人員、人事

現在、43 名のスタッフ（うち 26 名が女性）がおり、約 20 名が法律専門家、3 名が IT 専門家、その他が行政部門などの担当である。設置当初は 15 名のスタッフであったが、現在は 43 名まで増員された。

6 か月間の試用期間があり、任期付き雇用がほとんどとなっている。2010 年には 2 名が辞職した。専門性を有した人材の確保が重要であり，この点は 2010 年の年次報告書でも指摘されている。法律専門家はほとんど弁護士資格を有しており、修士号を有したスタッフも 3 名いる。

事務局長のほか 4 つのチームから構成され、チームごとに実質的な業務が行われている。

①医療・研究・教育チーム
②事業者対策チーム
③法執行チーム
④サービス（総務、人事、広報）チーム

建物はストックホルムの繁華街にあるビルの 5 階を使っている。

18 Datainspektionen, Arsredovisning 2010, p.13.

④予算[19]

予算は議会の議決を経て司法省から受け取っている。その金額は下記のとおりとなっている。その他、講演会、セミナー、会議による収入がある。小さな予算でやりくりをしてきているとの認識である。

年	総額	活動費（人件費・家賃等を除いた金額）
2010 年	36,100,000 クローナ（約 4 億 7000 万円）	4,432,000 クローナ（約 5700 万円）
2009 年	3,526,700 クローナ（約 4 億 6000 万円）	4,349,000 クローナ（約 5600 万円）
2008 年	3,342,200 クローナ（約 4 億 3000 万円）	4,141,000 クローナ（約 5400 万円）

表 2　データ保護検査院の予算推移

⑤権限

個人データ法、債務回復法、クレジット情報法の 3 つの法分野の法執行を監視している。また、立法過程においてデータ保護に関する意見を議会に対して述べることができる。

ヒアリングにおいて指摘されたこととして、データ保護検査院の最大の功績は、立法に対して提言を行ってきたことである, ということがある。2010 年には法案審議の過程において 17 回の提言を行ってきた。これは憲法の一部である「統治構造」の第 7 章の 2 において、政府の任務については関係する機関から情報と意見を聴取することが定められていることに基づく権限行使である。このような提言が法律に反映されることでデータ保護が実現されてきた。具体的な功績をあげるのであれば、クレジットカード情報に関する法的諸問題が 2003 年から議会で議論されてきたところ、データ保護検査院が 7 年間かけて提案をしてきたことが、最終的に法案に盛り込まれた，というものが挙げられる。

⑥他機関・地方との関係

政府機関（金融情報当局、技術部署、警察等）と情報共有を頻繁に行っている。具体的には、昨年、テロ資金流用対策として債権整理問題について協力し、児童への啓発目的で消費者庁及び児童オンブズマンと意見交換を行ったほか、情報セキュリティ分野の意見交換のために IT セキュリティ機関などと協働してきた。

---

19 Datainspektionen, Arsredovisning 2010, p.33.

また、議会オンブズマンと協働して進めてきたものであるが、データ保護が立法に適切に組み込まれることが重要である。また、執行面でも、議会に対して苦情を申し出た個人の氏名を議会が公表した事件について、議会オンブズマンと協働して対処した。

地方に支部などは存在しない。

3　監督機関の運用実態

（1）苦情処理・紛争解決

・苦情処理の実態

相談件数としては、毎週 200 件程度の電話と 60 ～ 70 通程度のメールを受け付け、対応している。2010 年には約 2100 通（2009 年は約 3100 通）のメールによる相談（通常 3 営業日以内に返答)、電話による約 5300 回の相談対応を行ってきた。通常２人（多忙期は 3 人）の法律専門家が電話とメールの対応を行っており、スタッフは必ず 1 月に 1 回は全員が対応することとなっている。

苦情処理の件数は、下記の表のとおり年間 200 ～ 300 件程度となっている。具体的には、個人からの苦情を受けて、違反の疑いのある事業者に対して手紙などを書いている。

	件数
2010 年	３３２件
2010 年	２３３件
2010 年	２７９件

表 3　苦情処理件数の動向 [20]

また、2010 年 5 月・11 月にグーグル社からデータ保護検査院に対し、WiFi 情報が偶然収集しうる状況にあったことについて情報提供があり、データ保護検査院がこの情報を調査し、意見を公表したという事例があった [21]。

・ダイレクト・マーケティング

法 11 条は「個人データの管理者に対して登録された個人がダイレクト・マーケティングの処理に書面で異議を唱えている場合、ダイレクト・マーケティングに関する目的をもって個人データを処理しており、いわゆるオプト・アウトのアプローチが採られている。

---

20 Datainspektionen, Arsredovisning 2010, p.19.

21 Datainspektionen, Integritetsåret 2010, pp.10-11.

（2）権限行使（立入検査・罰則）

・立入検査

立入検査権限が個人データ法 43 条の下で認められている。この検査には二通りあり、事前に手紙・質問状を書いた上で、データ保護検査院に呼んで検査する場合と、現地に訪問して検査する場合である。このほかに質問状のみを送付して調査する場合がある。

現地に訪問する場合は事前に質問状等を送付することとなっている。検査の実施については IT 専門家が行うことがほとんどである。検査をする場合は、新聞やテレビに出ている問題について行うことが多い。省庁等の公的機関に対しても、行う権限があるが、立法に関する意見を提出する程度のことしかしていない。

センシティブ･データ（人種･民族[22]、政治的思想、宗教･哲学上の信念、労働組合の構成員、医療情報、性的志向（13 条））の取扱いに伴う苦情が多くなってきている。今後、センシティブ・データを利用する金融機関等について必要が生じれば事前通知なしで立入検査を行う計画もないわけではない。

立入検査の結果概要は以下のとおりである[23]。

	2010 年	2009 年	2008 年
開始	６４	４１	５３
終了	５２	４４	２９

表 4　現地立入検査の件数表 5 呼び出し検査の件数

	2010 年	2009 年	2008 年
開始	７４	７９	６０
終了	７４	６６	６５

表 5　呼び出し検査の件数

22 政府の報告書によれば、氏名・使用言語から個人の人種・民族が間接的に識別しうる場合があるため、センシティブ・データに該当すると指摘している。Government Official Report SOU 2001:32 , Domstolarnas register och personuppgiftslagen- En rättslig anpassning 124.

23 Datainspektionen, Arsredovisning 2010 p.15.

	2010 年	2009 年	2008 年
開始	５２	２９	0
終了	７５	0	0

表 6　質問状による調査の件数

・罰則

これまで罰金を科した事例はない。

法 13 条から 21 条におけるデータ管理者に課された義務規定に違反した場合、データ管理者は罰金を科せられ又は 6 か月以下の懲役に処せられることになる。なお、軽微な違反は刑事罰の対象とはならない。

立入検査の拒否や検査の結果不法なデータ処理が発覚した場合は、是正を求めるが、是正にも応じない場合、罰金を科すことができる。データ保護検査院側は罰則を最初から課すつもりで検査をしているわけではなく、法令順守の徹底を促し、正しいことをしてもらいたい、という意図がある。罰則を科すことになった場合、データ保護検査院は、行政裁判所に提訴し、同裁判所が罰則を課すこととなっている。罰則に対する不服申し立ては行政裁判所に提訴できることになっている。

（3）事前届出と検査

個人データを処理しようとする事業者は、データ保護検査院に対しあらかじめ書面で届出をしなければならない（法第 36 条 1 項)。また、各事業者が個人データ担当者を置く場合又は辞任させる場合、その旨をデータ保護検査院に届け出なければならない（法 36 条 2 項)。

センシティブ・データの処理については、3 週間前に事前に届出をする必要がある（法 41 条)。データ保護検査院は 3 週間の間で複雑な技術検査を行い、限られた時間の中でセンシティブ・データの可否について決定を下している。

	2010 年	2009 年	2008 年
研究分野	３１１	２９４	２１１
警察	３１	２９	1
警備・防衛	2	2	2

表 7　事前届出と検査の状況 [24]

24 Datainspektionen, Arsredovisning 2010 p.19.

もっとも、データ保護検査院の決定（decision）には強制力がなく、また決定に不服がある場合は行政裁判所へ提訴することができる。損害が生じうる事案や罰則を科すべき事案になるとデータ保護検査院単体で強制力のある決定を下すことはできず、行政裁判所において審理されることになっている。実際には、データ保護検査院がデータ処理を認めないという決定をする場合、事業者は技術的に足りない部分を修正するなどしており、これまで決定を無視された事例は 1 件もない。

近年、医学・疫学研究に関する事前届出が増加の傾向にある[25]。センシティブ・データの処理には本人の同意が必要であるが、法 19 条 1 項によれば、「データが処理されることによる個人の人格の侵害に比べて研究または統計におけるデータ処理が社会の利益にとって必要である場合」には医学・疫学研究における個人データの処理が認められることとなっている。また、法 19 条 2 項は、研究倫理委員会による承認があった場合には、前記の社会的な利益があるものとみなしている。データ保護検査院は、2002 年 12 月、遺伝子研究個人データの処理について報告書[26]を公表し、事前届出における審査項目等を示している。

また、法 21 条によれば、犯罪等の法令違反に関する個人データの処理が公的機関以外において行われることを禁止しているが（1 項)、データ保護検査院を含む政府からの禁止免除の決定が行われれば、このような個人データの処理が認められることとなっている。具体的には、企業内部における犯罪等について、公益通報に関する個人データの処理が多くなっている。

2010 年	2009 年	2008 年
7 6	6 2	4 1

表 8　犯罪等の法令違反に関する個人データの処理の事前届出の状況[27]

25 遺伝データについては、遺伝子プライバシー法（Genetisk integritet (Lag (2006:351)）がある。

26 Datainspektionen, Rapport: Personuppgifter i genforskning 2002:4.

27 Datainspektionen, Arsredovisning 2010 p.12

（4）広報啓発活動

・一般的な活動

データ保護検査院では、広報啓発活動に力を入れており、パンフレット・雑誌（定期刊行誌「Integritet」）を発行している。2010年時点で6268人（2009年5474人）（企業のプライバシー担当者、弁護士、ジャーナリスト、公務員等が主な読者層と考えられるとの回答があった。）が雑誌を定期購読している。2010年には325,409回のホームページへのアクセス数があったほか、67回（2009年54回）のプレスリリースを行い、データ保護に関する広報啓発活動を行ってきている。また、ソーシャル・メディアの問題に取り組んできており、セミナー等を通じて若者にプライバシー・リスクを教えてきているほか、専用のホームページを公表するなど違反通報のホームページ窓口を設けている。

2010年には講演会やセミナーを49回（2009年48回）、事業者向けの研修セミナーを8回（2009年8回）行ってきている[28]。

・事業者向けガイドライン

2010年10月、個人データ法における基本原則をまとめたガイドライン（Ansvaret för personuppgifter som hanteras i system för whistleblowing）を公表した。

2009年1月時点では、6,100以上の事業者において個人データ保護担当者が設置され、データ保護検査院に届出がされている。個人データ保護担当者の役割は、①個人データの処理が合法かつ正しい方法で処理されているかを保証するため独立して活動すること、②もし個人データ管理者が不法な個人データ処理を行っている場合などにはデータ保護検査院に通知しなければならないこと、③個人データの処理について個人データ法の適用について疑義が生じた場合はデータ保護検査院に相談することである。（法38条1項～3項）。

・青少年保護対策

近年、データ保護検査院はソーシャル・メディアの利用における青少年保護に精力的に取り組んできた。“青少年とプライバシー2011年（Ungdomar och integritet 2011）”という統計報告を含むパンフレットを作成し、学校等へ配布しプライバシー啓発教育に利用している。

統計対象となった15－18歳の青少年のうち、23%は両親の目の行き届く範囲でパソコン利用をしているが、46%は両親の知らないところでオンライン接続を行っている。これらの青少年の60%以上が、インターネット利用に関するプライバシー問題について考えたことがあると回答し、年々増加傾向にある。そして、統計の結果によれば、青少年の非常に多くがソーシャル・ネットワーキング・サイトを閲覧していることが明らかになった。

---

28 Datainspektionen, Arsredovisning 2010 pp.8-10.

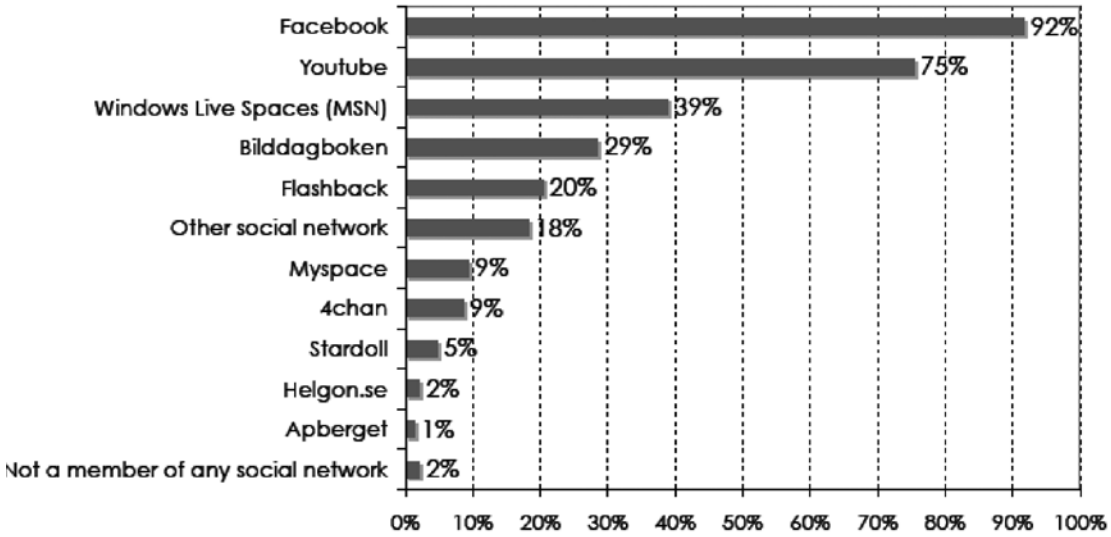

表 9　1 週間に 1 回以上閲覧するソーシャル・ネットワーキング・サイト

青少年がインターネットにおける被害等の状況については次のとおりになっている（下段括弧内の数値は 2007 年時の統計との比較)。

ネット上で自身に対する不親切な記述が書き込まれた	５６％ （＋１％）
ネット上で自身に対する嘘が書き込まれた	５４％ （＋１％）
他人から不快なメールが送られてきた	４２％ （＋１７％）
ネット上に意思に反して写真を公開された	３７％ （＋７％）
ネット上で性的に嫌がらせをさせられた	２３％ （－２％）
ネット上で他人が自分になりすまされた	２２％ （－５％）

表 10　青少年のインターネットにおける被害等の状況

（5）チェック体制

年次報告書を毎年会計検査院へ提出している。議会や他の政府機関にも年次報告書を公表することとなっている。最終的には議会オンブズマンによって適切な執行が行われているかチェックされる仕組みになっている。

（6）国際協力

法第 33 条において、個人データの第三国移転をする場合には、当該国が個人データの十分の保護水準を満たしていない限り、データの移転が禁止されている。しかし、第三国に個人データを移転することについて同意している場合、ないしそれが一定の条件を満たし必要とされる場合（法 34 条）、または政府が認可した場合（法 35 条）についてはデータの移転が認められる。

これまで、データ保護の執行に関して、他国の機関との具体的な協働実績はない。

データ保護プライバシー・コミッショナー会議、北欧諸国が参加する会議、ヨーロッパでの様々な会議、欧州委員会 29 条データ保護作業部会、通信分野におけるデータ保護国際作業部会（いわゆるベルリン・グループ）等への出席をしてきており、他国の動向に注視しているとのことである。2010 年には第 29 条作業部会における「技術分科会」、「執行タスクフォース分科会」、「プライバシーの未来分科会」、「主要な規定分科会」に積極的に関与してきた。

4　監督機関の課題等

・データ保護検査院は設立以降多くの変化が生じたが、全体的にみて、国民からの大きな尊敬の念を持って支えられてきた機関であると自負している。重要な役割として，国民に情報提供をし，法律家による相談を受け付けてきた。データ保護検査院はこのように国民の声を聴くことのできる機関であり，国民の声は聴き続けることが大切である。

・リズボン条約[29] 以降、データ保護がますます重要になってきており、EU 他の加盟国との調和をどのようにとっていくか、またデータ保護機関の役割と権限をどのように強化していくかが今後問題となってくるであろう。

---

29 リズボン条約（2009 年 12 月 1 日発効）により、従来の「欧州共同体（EC)」、「共通外交・安全保障政策（CFSP)」、「警察・刑事司法協力 (PJCC)」の 3 本柱による枠組みが廃止され、EU の権限強化がされるとともに、「個人データ保護」が新たな政策課題として明記された。

・まとめ

スウェーデンは、約 930 万人からなる国であり、比較的早くから全国民に番号制度が普及しやすい人口数であると見ることもできる。そして、スウェーデンが IT 国家になった背景には、地理的要因と社会経済的要因も指摘されている[30]。すなわち、スウェーデンは国土の約 3 分の 1 が北極圏で、暗い冬は人々を街から孤立させる。このような地理的条件から携帯電話やインターネットが早くから日用品となった。また、資源に乏しい小国が高い生産性と生活水準を維持するためには、全国民に高い教育サービスを充実させることが必要であった。そのため、情報化の推進は幼児教育から始まり、情報通信産業を発展させていった。このような背景があり、個人データ保護法が世界で最も早く国レベルにおいて制定されてきた。

2009 年時点、スウェーデンでは、人口の 83%がインターネット利用をしている[31]。62%が電子メールのチェック、ニュース購読、その他実用的な情報入手のために日常生活においてインターネットを利用している。また、16 歳から 74 歳までの人の中で 63%がインターネットで商品の購入をしたことがあると回答している。旅行代金やチケット予約を含まない電子商取引の売り上げは 2008 年において約 2,652 億円（20,400,000,000 クローナ）となっており、実質的な電子商取引による売上金額ははるかにそれを超える。公的部門においても、スウェーデンは電子政府を推進してきており、1998 年に情報技術委員会（IT-komissionen）を設置し、情報通信技術の効果を分析してきた。

このようにヨーロッパ諸国において、情報通信技術の発展が顕著であったスウェーデンにあっては、データ保護検査院もまた世界で最も歴史の古い個人情報保護の監督機関としてその役割を果たしてきた。ヒアリングの結果からは、オンブズマン制度が、独立した監督機関という発想の背景にあるものとして理解できた。そのため、データ保護検査院は、民間部門のみならず、地方公共団体に対しても電子政府の推進に関するガイドラインを公表してきた[32]。

ヒアリングの結果、データ保護検査院は確かに立入検査等を行っているが、むしろ広報啓発活動に力を入れ､市民の間でデータ保護が適切に運用される役割を果たしてきたことを把握できた。また､データ保護検査院における最大の功績は立法過程におけるデータ保護に関する意見提出であるとの回答を得た。このような独立行政機関の位置づけと役割はスウェーデンにおける特有の統治構造に起因するものであるが、データ保護の運用実態として参考になるものである。

---

30 島田達巳「e-Japan 戦略としての電子政府の検討－スウェーデンとの比較において―」大阪市立大学経営研究 52 巻 4 号（2002）4 頁、参照。

31 Kirchberger, supra note 1, at 36.

32 Datainspektionen, Vägledning för kommuner: Personuppgifter och e-förvaltning

v. アイルランド＜補節＞

1 監督機関設置の経緯

（1）個人情報保護に対する国民感情・世論はどのようなものか？

（強く保護すべきという考えか、企業活動のために有益に使われるべきであるという考えか等）そのような国民感情・世論が形成された理由・歴史的背景は何か？

最も新しい国民調査は、2008 年に行われた。EU によって行われたユーロ指標（Eurobarometer）によると（http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf)、アイルランドの国民は、その他の EU の国々よりも一般的にデータ保護により関心を有していることが示されている。

データ保護に関する個人の関心	EU 平均（%）	アイルランド（%）
関心がある	63.8	70.5
関心がない	34.8	28.2
わからない・回答なし	1.4	1.3

また、コミッショナーによって行われた 2008 年の調査によると、プライヴァシーの保護は、アイルランドの国民にとって、比較的重要であることが示されている。

項目	とても重要であると考える国民の割合（%）
優れた健康サーヴィス	89%
犯罪防止	87%
個人情報のプライヴァシー	84%
消費者の権利保護	77%
公的組織の倫理	77%

（2）監督機関設置の際の、国内世論、マスコミの論調はどのようなものであったか？設置に反対する団体はあったか？（「設置に反対する団体」があった場合）どのようにして反対意見を説得し、監督機関設置の決定に踏み切ったか？

データ保護コミッショナー・オフィスを設立したデータ保護法案は、1987 年と 1988 年に議会で審議されたが、すべての政党がこの法案に賛成した。1988 年のデータ保護法（Data Protection Act）は、同法の執行を監視するデータ保護コミッショナーを政府が任命することを定めていた。

この法律は、欧州評議会のデータ保護条約（第 108 条約）を基礎としていた。他の多くの EU 諸国がデー

タ保護法を制定していたことも役に立った。同法は、EU のデータ保護指令 96/46/EC の要求に合致するように 2003 年に改正された。EU 諸国においては、EU 指令に従うことが義務だからである。

（3）監督機関設置の方法について、既存の組織を改変して設置したのか、全く新たに組織を創設したのか？人員の調達はどのようにおこなったか？（全く新たに組織を創設した場合、多数の人員をどこから持ってきたのか）

1988 年データ保護法が新たに、データ保護コミッショナーについて規定した。また、同法は、権限を有する大臣（司法大臣）が、同コミッショナーの職員となる公務員を指名すると定めていた。

（4）その他、設置に至るまでに苦労した点は？

特に存在しない。

2　監督機関の制度状況

（5）憲法に、「プライヴァシーの権利」、「権力分立」、「地方自治」の規定はあるか？また、憲法の規定監督機関にどのような影響を与えているか？

アイルランド憲法は、プライヴァシーに関する特別な規定を有していない。しかしながら、裁判所は、憲法 40.3.1 の規定が（国は、市民としての個人の権利を法律において尊重し、かつ、法律によって可能な限り保護することを保障する）、プライヴァシーの権利を保障していると解釈している。

（6）監督機関の「独立性の程度」はどの程度担保されているか？その理由は？

データ保護法附則第 2 では、データ保護コミッショナーが、「その職務遂行に際して、独立しているべきである」ことを定めている。同コミッショナーは最高 5 年の決められた任期で指名され、再指名されることもできる。再任されなくとも、公務員に戻ることが可能であり、さらに、従前（コミッショナー当時）の地位及び給与が保障されていること、省庁とは切り離されており、大臣の命令に従う必要がないこと、などの点でその独立性が確保されていると考えられる。

また、同コミッショナーは、明文で示された非行又は病気によりその職務の遂行が事実上できなくなった場合にのみ失職する。なお、同コミッショナーは、報酬を伴う他の役職につくことや被用者となることは許されない。

（7）監督機関と「法的位置づけ」が同様の政府機関は他にあるか？それとも、監督機関のような組織は特殊で唯一のものであるか？

他にも同様の法的根拠を有する組織は存在する。たとえば、情報コミッショナー（information commissioner）がそうである。同コミッショナーは、公共サービス（public service）のオンブズマンをも兼任している。その他にも、年金オンブズマンが、民間の年金制度について独立した機関として権限を有している。

（8）監督機関の組織体制、職員数はどうなっているか？（できる限り詳細を伺う）

現在 22 名の職員がいる。全員、終身雇用の公務員である。

これらの公務員は、司法省（公務員の人事について所管している）からの指名により、コミッショナー・オフィスの構成員となる。これらの公務員は、他の公務員と同様、他の行政組織に異動する可能性がある。また、彼らが昇進するためには、他の行政組織の空席ポストに応募することが原則として必要である。

この職員の指名については、コミッショナーに拒否権はなく、司法省から送られてきた人を受け入れるしかない。もちろん、非公式な相談は可能であるが、制度として拒否する権限はない。

（9）地方支部等は存在するか？（存在する場合）地方支部の数、地方支部と地方政府との関係はどうなっているか？

特に存在しない。

（10）監督機関は個人情報保護以外の業務も所掌しているか？（所掌している場合）個人情報保護関係業務と他の業務の比率は？

個人情報保護以外の業務は所管していない。

（11）監督機関にどのような権限が与えられているか？（普及啓発、苦情処理、相談受付、報告徴収、立入検査、命令、指導、勧告、助言等）従わない場合，どの程度の強制力があるか？

コミッショナーは、これらすべての権限を有する。仮に、人々が従わない場合、コミッショナーは、執行通知(Enforcement Notice)を出す権限を有する。この執行通知に従わないことは罪となる。仮に、これに従わない場合、コミッショナーは、彼らを裁判所に訴えることができる。この場合、拘禁刑はないが罰金刑が科される。

（12）コミッショナー又は委員会委員の人事制度はどうなっているか？（選任手続、任期、再任、解任、定年、俸給、年金）

コミッショナーの定年は、現在のところ、65 歳である（この定年制度が廃止される法案が提出されている）。また、データ保護法によって、コミッショナーの給与と年金については、（司法省の）大臣が、財務省の同意を得て決定することが定められている。

私（Billy Hawks）は 4 代目のコミッショナーであるが、私を含めてこれまでのコミッショナー全員が官僚出身である。このコミッショナーの地位については、もっと低くても良いと主張する者もいるが、他の行政組織を監視し、国民の信頼を獲得するには、ある程度の地位にいなければならないと一般には解されている。

現在のところ、コミッショナーの給与と年金は、次長（Assistant Secretary-General）の水準と同じである。官庁によるが、このポジションは、事務官としては 2 番目から 3 番目の地位である。すなわち、相当大きい組織では、事務次官の次に事務次官代理（Deputy Secretary）という地位があるが、ほとんどの組織では、事務次官の次が、この次長になる。給与は、およそ 148,000 ユーロである。また、退職後の年金は、退職時の給与の 50 パーセントの額である。

なお、政府（Government）から、コミッショナーが選任されるということなどは、データ保護法附則第 2 で定められているが、これは公平に行われていると一般に考えられている。なぜならその選任（高級官僚選抜制度（senior selection system））は、常設の特別な委員会における競争手続（competitive procedure）によって行われるからである。この選抜は、極めて中立的なものと解されていて、そこに、党派的なものが入り込む余地はない。場合によっては、民間人が審査のメンバーに数名入ることもある。この制度の信頼性は、アイルランドでは非常に高い。

また、公務員は、いかなる政党に入ることも許されていないから、国民からも中立的な立場と考えられている。他の多くの EU 諸国では、議会の指名であることは承知している。よって、政府からの指名では独立性に懸念があるとの指摘がなされ得ると考えられるが、これまでのところ、幸い、この点が指摘されたことはない。

もっとも、ドイツの州コミッショナーの独立性が議論された際に、彼らが、アイルランドの制度もみてくれといっていたとはきいている。だが、そもそも、指名を中立的に行う完璧な制度は存在しないように思われる。

（13）監督機関と他の行政機関との力関係はどのようになっているか？他の行政機関に対して指導・命令を行うことは可能か？また、地方公共団体に対して指導・命令を行うことは可能か？従わない場合，どの程度の強制力があるか？

コミッショナーは、公的組織と民間組織のいずれも監視する権限を有し、執行通知などの権限を含め、両者の権限の範囲に相違はない。公的組織に対しても、事前の許可を得ずに立入検査を行う権限を有しているため、衝突することが稀にある。ただ、多くの場合には、コミッショナーの役割やその権限を理解しているため、他の行政組織との関係は基本的に良好である。

（14）監督機関と他の行政機関が協働して、業務を行う例はあるか？

ある。たとえば、情報の自由を監視する情報コミッショナー、消費者庁、人権委員会などとである。

（15）監督機関が適正に業務を行っているかについて、監視を行う制度はあるか？（第三者評価など）

コミッショナーのあらゆる決定に対して、裁判所へ訴える権利がある。

（16）監督機関は、「国民 ID」、「SSN」といったような番号制度も管理・監督しているか？管理・監督していないのであれば、どの機関が行っているか？　当該機関と監督機関の関係はどうなっているか？

国民番号制度のようなものはないが（よってその ID カードもない）、アイルランドでは、生まれるとすぐに番号が与えられ、住所や性別などのデータ・セットという情報と共に、それを社会保障省（Department of Social Welfare）が管理する。これは、あくまでも社会保障制度の実施のために行われるため、必ずしも、アイルランド国民に限らずそのデータが収集されている。なお、税収確保のため、国税省もその情報を共有することが認められている。

しかし、これらの制度とデータ保護コミッショナー・オフィスとは特に関係がない。

3　監督機関の運用状況

（17）予算額とその内訳はどのようになっているか？

どの経費が一番高額となっているか？（人件費、調査費、事務費等）

2011 年度の予算は、1,458,000 ユーロである。その使途の大部分は、人件費であり、その額はおよそ 1,300,000 ユーロである。

（18）予算以外に収入源はあるか？得られた収入の使途は？

予算以外の収入源は存在しない。データ管理者やデータ処理者による届出料の総額は、毎年およそ 600,000 ユーロにもなるが、それは中央政府（財務省）へと納入される。

（19）監督機関職員について、学位（修士・博士）及び法曹資格を取得している職員の割合は？また、任期付職員、非常勤職員は何名ほど勤務しているか？

数名の職員が修士号を持っている。法曹資格取得者はいない。また､すべての職員が終身雇用である。

（20）職員の専門性はどのように確保されるか？人事異動の頻度、人事ローテーションはどのようになっているか？

定期的に社会内及び社外の研修が行われる。新しく組織の一員となったすべての者に対して、基礎的な研修が行われた後に、実地研修が行われる。組織内部での配置換えはアド・ホックになされる。。

（21）監督機関が実際に行う業務について、具体的にどのような業務があり、それぞれの業務を何名の職員が担当しているか？

調査部、監査部、届出・行政部、教育部、国際部の 5 つの部に分かれて、22 名の職員が働いている。

（22）監督機関の権限行使の状況、罰則等の運用状況はどのようになっているか？（報告徴収、勧告、命令、立入検査の件数等）

コミッショナーの権限として、データ保護法違反の行為があった場合に、その行為をやめるように命じることができる。この命令に違反して初めて、裁判所に訴えることができるが、多くの事件ではこの命令に従う形で解決がなされている。第 1 審の裁判所では（アイルランドも日本と同じく 3 審制を採用している)､コミッショナーが検察官として法廷に立つ。通常は､被告人が罪を認めることが多い。第 2 審以降は、通常の検察官が法廷に立つ。

（23）監督機関が重大な処分を下した例としてどのようなものがあるか？また、監督機関が行政機関に対して処分を下した例はあるか？

罰金という形式での処罰は、データ保護法及び電子プライヴァシー規制法（Electronic Privacy Regulation）に定められた罪に違反した場合に、裁判所によってのみ科される。この罰金が科された多くの事件は、求められていない電子マーケティング（unsolicited electronic marketing）のメッセージを送ったというものである。

データ保護法における罪は次のとおりである。

・コミッショナーによって出された通知に従わないこと

・法よって届出が要求されているにもかかわらず、それを怠ったこと、または、登録条件に従わなかったこと

第一審の裁判所では、罰金刑の通常の上限は 3,000 ユーロである。上訴審では、100,000 ユーロまで罰金を科すことができるが、現在までのところ、上級審まで争われたケースは

ない。

このデータ保護法とは別に、電子プライヴァシー規制法の罪が規定されている。そこでは、求められていない電子マーケティング行為 1 回につき 5,000 ユーロまでの罰金を第一審で科すことができる。また、上級審で争われたケースはないが、上級審では、より高い罰金刑を科すことができる。

（24）苦情相談窓口の数、苦情処理受付件数はどうなっているか？苦情の件数が膨大で困っていないか？電話対応等の相談員の数は？

苦情受付数

2008 年	1,031 件
2009 年	914 件
2010 年	783 件

多くの苦情は、公式な調査を必要とせず、非公式に処理されている。2 名の職員が、交代で電話対応にあたっている。コミッショナーを含め全職員が、この職務にあたっている。

（25）個別の相談に対してどのような解決が図られるケースが多いか？「助言」のみの対応となるケースは、全体の何割程度になるか？また、相談を聞いた結果、監督機関への正式な「申立」を相談者に勧めるケースはどの程度あるか？

ほとんどの苦情が、友好的に処理されている。たとえば、当該組織が謝罪や何らかの形での埋め合わせを提供するという形である。多くの苦情が電話で処理されており、その場合、基本的な情報を提供又は助言を与えている。

（26）これまで監督機関が行った活動の中で、大きな成果・効果があったものは何か？

データ保護法の新法の内容を考慮するよう政府に説得したこと、及び、様々な部門におけるデータ保護の水準を向上させるために我々の権限を行使したことである。

（27）海外の関係機関との連携は盛んに行われているか？国際会議等への参加はどの程度行っているか？

国際的な協力や活動は、とりわけ 29 条委員会を通じて、主に EU のプライヴァシー保護執行機関と共に行っている。この委員会の全体会合は、年に 5 回開催され、それ以外にも同委員会が、特定のテーマについてサブグループを作り、議論することも多い。そのため、年に何度もブリュッセルに行っている。その他、コミッショナー会議や IPPA 会議など主要な会議にも出席している。

4　今後の課題

（28）監督機関設置前と比べて、監督機関設置後、大きく世の中が変わったと言えるか？

そのように言えると思う。

（29）監督機関が設置されたことによって生じた弊害、マイナス面はないか？

データ保護のルールは、マーケティングのような営利活動や個人データの共有などの政府の活動を時折抑制してしまうことがある。

（30）現在の監督機関の制度にはどのような課題があるか？

特に存在しない。

（31）法執行をする際にどのような課題があるか？

電子プライヴァシー規制法では、違法行為＝犯罪である。たとえば、営業のために、同意のない E メールを送信することは同法に違反するため、犯罪となる。なお、同法は「電子」となっているが、電話での勧誘なども規制の対象となっている。電話勧誘は E メールよりもはるかに迷惑な行為と考えられている。

ところが、この電子プライヴァシー規制法とデータ保護法とを比較すると、後者の場合には、一旦コミッショナーが命令を出し、それに違反しない限り起訴することができない点で迂遠である。その

ため、電子取引のみならず、広くデータ保護法違反を犯罪と構成し、コミッショナーの権限を広くしたいと考えているが、現在のところ成功していない。

データ保護法にのみ違反する場合には、いかに重大な違反行為であったとしても、執行命令に違反しない限り犯罪とならないというのではバランスを失している。もちろん、悪意のない軽微な情報流失などは、許されるべきであるし、実際そうされている。ただ、コミッショナーとしては、電子プライヴァシー規制法と同様の権限を与えられれば、とり得る選択肢が増えるという意味で望ましいと考えている。

電子プライヴァシー規制法は、2002 年の電子プライヴァシー EU 指令（Electronic Privacy Directive）に基づき定められたものであるが、同指令により、今年の 5 月までにデータ保護違反届出（Data Breach Notification）に関する定めを置くことが加盟国に義務付けられた。これに対応して、アイルランドでは、データ保護違反届出義務を定めた規定を電子プライヴァシー規制法におくこととなったが、データ保護法には、この定めをおく予定が現在のところない。つまり、電子プライヴァシー規制法に該当しないデータ保護違反行為に対しては、その事実の告知義務が課されていないことが問題である。

（32）国民が期待する監督機関の役割にはどのようなものがあると考えているか？

データ保護に関する国民の権利が保障されるように確保することである。

（33）今後、監督機関の制度を改正するような動きはあるか？

情報の自由に関するオフィスと併合すべきという意見が出ている。

（34）その他

仮に、日本政府がコミッショナー制度を創設する場合、一部の権限をコミッショナーに委譲し、それが他の国家組織をも監視するという点をクリアーできるかが課題であるように思われる。

ただ、アイルランドのような制度は、従来の行政組織をもっとも破壊しない（the least destructive）形であるように思われるので、日本でも同制度の採用は可能ではないかと思う。極論すれば、独立性は、コミッショナー 1 人にしか確保されていない。コミッショナーは官僚出身であるし、その職員も、他の行政組織と変わらず配置されるに過ぎない。とすれば、コミッショナーというポストさえ設置すれば、それ以上の人的及び財政的行政コストがふくらむわけではない。

＜参考文献＞

・萩原聡央「アイルランドの個人情報保護制度」季報情報公開・個人情報保護 33 号（2009 年）17 頁。

vi. アメリカ

1　個人情報保護法制の概要

（1）個人情報保護に関連する法律

米国は、個人情報保護に関してセクトラル方式を採用している。幾度にも渡る包括的個人情報保護法の提案にもかかわらず、現時点において、包括的に個人情報を保護する法律は存在しない。この状況は、公的機関、民間機関に共通している。

＜公的部門＞

公的部門については、Privacy Act（1974 年）が制定されており、連邦政府が保有する個人情報が対象となっている。

＜民間部門＞

民間部門については、個別法、判例法又は自主規制による規則が存在する。個別法は、一部の気密性の高度な情報を扱う分野（信用情報、医療情報等）については、問題の発生が契機となって制定されている。

＜州法による多様性＞

米国は連邦国家であるため、州法における多様な個別対応が存在する。例えば、カリフォルニア州は漏洩時の本人に対する告知義務、ミネソタ州は ISP の二次的使用に対するユーザーによる事前承認、ジョージア州は個人情報を含む文書、記録媒体の廃棄禁止などを定めている。

＜個別法＞

主な個別法は以下に記述しておく。

・公正信用報告法（Fair Credit Reporting Act, FCRA）
・金融サービス近代化法、（Gramm–Leach–Bliley Act, GLBA）
・児童オンラインプライバシー保護法（Children's Online Privacy Protection Act, COPPA）
・スパム対策法（CanSPAM Act）
・Telemarketing and Consumer Fraud and Abuse Prevention Act（DoNotCall）
・家庭教育プライバシー法（Family Educational Rights and Privacy Act, FERPA）
・金融プライバシー権法（Right to Financial Privacy Act）
・プライバシー保護法（Privacy Protection Act, ECPA）

・ビデオプライバシー保護法（Video Privacy Protection Act, VPPA）
・電話加入者保護法（Telephone Consumer Protection Act）
・医療保険の相互運用性及び説明責任に関する法律
（Health Insurance Portability and Accountability Act, HIPAA）
・電気通信法（Telecommunications Act）

・US SAFE WEB Act of 2006

個人情報保護に直接関わるものではないが、FTC の権限を広げ、国際社会における他国とプライバシー保護のための情報共有をしやすくした法律が、US SAFE WEB Act of 2006 である。国境を越えた国際的な消費者に対する詐欺や欺瞞（fraud and deception）が世界的な課題となったことに対応し、2006 年 12 月 9 日に上下院で US SAFE Web Act of 2006 が可決された。この法律では、次の 4 つの点で FTC の国際的な消費者に対する詐欺や欺瞞に対する対策、活動を強化したといえる。1. 外国の協力機関との連携を容易にした、2. 消費者に被害を与えるスキームに関する情報収集を容易にした、3. 国際的なケースの情報を強化した､4. FTC の国際的な執行プロジェクトとネットワークを強めた｡また、新しく Consumer Financial Protection Bureau (Department of Treasury にあるが、独立する) を設立するための法律も規定された。

（2）監督機関

米国は、個人情報保護を規定する法律ごとに監督する機関が存在する。民間部門に対しては、FTC が中心となって消費者保護の一環として個人情報保護に関するさまざまな法律の執行を担っている。その他、Department of Justice、Department of Health and Human Services（HHS）の中にある Office of Civil Rights（OCR）や Department of Commerce、Federal Communication Commission（FCC）なども監督機関とされている。

2　監督機関の制度概要

（1）設置の経緯・歴史

米国には、個人情報やプライバシーに関して、全般的に所轄する統一的な第三者機関は存在しない。個人情報保護に関しては分野別（setorial）に個別の法律が定められているため、監督機関も各個別法の規定によってそれぞれ定められている。

＜民間部門＞

民間部門の監督機関として代表的なものは、Federal Trade Commission（FTC）である。FTC の Consumer Protection 部門は、およそ 46 の法律の執行に関わる業務を行っており、個人情報保護関係だけでもおよそ 8 の法律の執行を担当する。さらに、FTC は特に調査（investigation）と法執行（law enforcement）の場面においては、他の省庁からの情報を重要なリソースとしており、他省庁との連携が盛んに行われている。FTC が調査に着手する端緒となるメインリソースは、他省庁からの情報（referral）である場合も少なくない。[1]

また、各個別法においては Department of Health and Human Services（HHS）の中にある Office of Civil Rights や Department of Commerce、Federal Communication Commission（FCC）なども監督機関とされている。これらは、FTC と協調して監督機関の役割を一部担っている。

さらに、2011 年 7 月には、Consumer Financial Protection Bureau（現在、Department of Treasury にある）が独立をして、新しい独立第三者機関となる[2]。現在 FTC の管轄である金融系の法執行に関わるものについては、この新しい機関へ移管される予定である。しかし、privacy に関わる部分の多くは FTC に残るということである[3]。

1　筆者の FTC ヒヤリング調査による（2011 年 3 月 16 日）

2　http://www.consumerfinance.gov/

3　前掲 1 に同じ

以下に具体的な監督機関の設置経緯を記述する。

・Federal Trade Commission

FTC の歴史は、1915 年 3 月 16 日にその始めの日を迎えた。Commerce Department の Bureau of Corporations が独立をして、Federal Trade Commission となった。Department の配下にある Bureau と違い、独立した機関である FTC は、行政判断をすることができるようになった。その主たる業務は、不正な競争方法（unfair methods of competition）の規制であった（シャーマン・クレイトン法を改正した）。1938 年に議会は、不正な競争方法の規制に加えて、不公正・欺瞞的な行為・慣行（unfair and deceptive acts or practices）の規制監視にまで FTC の権限を広げた。それ以来、FTC は広い範囲の消費者保護に関する法律の監督機関となった。またさらに、FTC 法 Section5 で、命令において民事罰（civil penalty）を課すことができるようになった。さらに、1969 年に、仮差止めと差止めを裁判所に対して求めることもできるようになった。そして、1975 年、議会は FTC に産業界別の規則を制定する権限を与え、さらにそれらに違反した者に民事罰を課すことができるようになった。

FTC が個人情報保護、プライバシー関係の法律に関する執行に携わるようになったのは、1970 年以降が中心である。FTC（Federal Trade Commission）は、1970 年に施行された Fair Credit Reporting Act（FCRA）の執行機関となったことを発端として、クレジット、雇用、保険などに利用される消費者の個人情報に関する保護の法執行役を務めている。この FCRA の執行を通して、FTC はユニークな専門性を展開していくこととなった。1990 年代中盤になると、FTC は FCRA 以外のプライバイシーに関わる法律も執行するようになった。それ以来、プライバシー保護は FTC の重要な業務の一つとなっていった。

・Department of Commerce

EU/US Safe Harbor について担当するが、実際の執行は FTC が行っており、DOC は特に Safe Harbor 原則の策定等、民間部門への取り組み組支援、関係業界への適切な対応の働きかけなどを行っている。また、Privacy Framework に適合している企業を審査して登録する作業を行っている。Department of Commerce は米国とが EU の交渉の過程でこの登録作業について担当することとなったものである。

・Federal Communication Commission（FCC）

FCC は Federal Radio Commission に取って代わる機関として 1934 年通信法によって設立された。周波数帯（ラジオ及びテレビジョン放送を含む）を使用するすべての非政府組織、すべての州間電気通信及びアメリカ合衆国内で発信または着信するすべての国際通信を規定して管理を行っている。個人情報保護の分野においては特に、Telephone Consumer Protection Act を担当している。一般的な行政権のほか、事業者に対して、免許の交付、更新の可否の決定をする裁定権、放送通信に関する規則を制定する準立法権を有する。周波数オークションの採用で政府に莫大な利益をもたらした。

・Office for Civil Rights（OCR）,Department of Health and Human Services（HHS）

HHS は主に Health Insurance Portability and Accountability Act（HIPAA：医療保険の相互運用性と説明責任に関する法律）の法執行に携わっている。

＜公的部門＞

公的部門には、統括的な監督機関は存在しない。それぞれの Agency や Department に、Inspector General（IG）が存在し、インターナルなチェックを行っている。この点については、「（２）法的位置づけ」において、公的部門に対して、総括的な第三者監督機関を置くことができない理由について述べる。

また、クリントン政権時代には、Office of Management and Budget に Privacy Office をおいて、政府機関に対してある程度統括的なプライバシーに関する管理を行った[4]。しかし、政権が代わってからは、そのようなポジションは作られなくなったようである[5]。

（２）制度の概要

ここでは、民間部門の主要監督機関である FTC について記述をする。

・Federal Trade Commission

① 組織、人事など

FTC は独立した機関であり、その業務の議会への報告義務がある。５人のコミッショナーで形成される[6]。５人は、大統領によって指名され、上院で承認されて就任し、任期はそれぞれ７年である。これら５人のうちからチェアマンが選出される（FTC 法 41 条）。また、３人以上は必ず同じ政党から選ばれてはならない。現在のチェアマン、Jon Leibowithz は、2009 年３月２日にオバマ大統領に指名された。コミッショナーは、任務懈怠、在職中の不正行為等の場合を除き、自らの意に反して罷免されることはなく、職権行使の独立性が認められている。

その他事務総長、局長クラス４人および地方事務所８か所（アトランタ、シカゴ、サンフランシスコ、ダラス、シアトル、クリーブランド、ニューヨーク）号が設けられている。

FTC には、３つの部局（bureau）が存在する。The Bureau of Consumer Protection、The Bureau of Competition、そして Bureau of Economics である。

4　この Office は、HIPAA 法の施行に一役かったという。

5　Peter Swire 教授に対する聞き取り調査による。Peter Swire 教授は、Ohio State University の教授であり、クリントン政権時代、Chief Counselor for Privacy in the Office of Management and Budget であった。現在は、Privacy Office という名称の Office は存在していない。

6　Edith Ramirez、William E. Kovacic、Jon Leibowithz（chairman）、J.Thomas Rosch、Julie Brill の５人である（本稿執筆時点）。

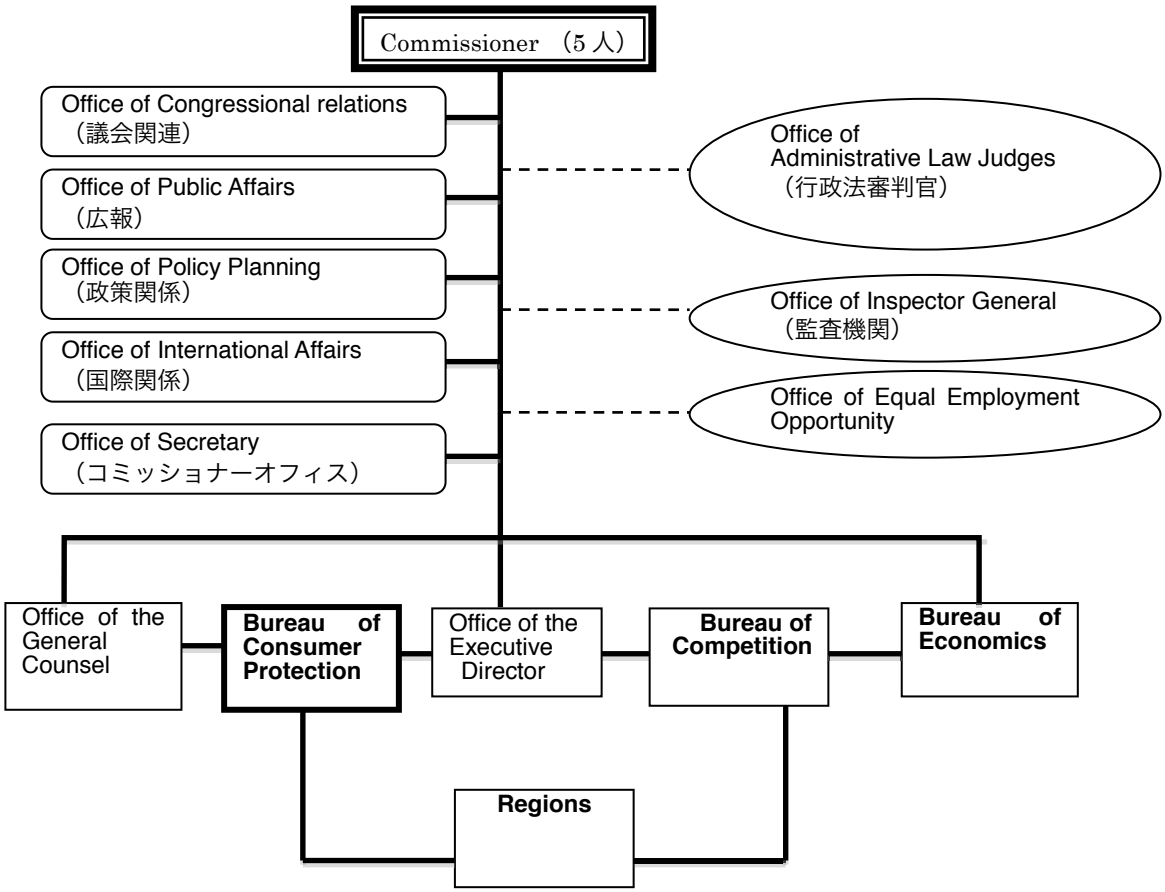

図 1　Federal Trade Commission の組織図[7]

本部は、Washington DC にあり、全米を 7 つのエリアに分けて業務を行っている。FTC 全体では、およそ 1100 人の職員がおり、そのうち弁護士が 600 人、エコノミストが 8 0 人、マネージメントが 42 人、その他が 461 人となっている（2010 年度）[8]。

主に個人情報保護関係の法律を扱っているのは、Bureau of Consumer Protection である。その中には division が存在し、特に Division of Advertising Practices、Division of Financial Practices、Division of Marketing Practices、Division of Privacy & Identity Protection の 4 つが主に Consumer Protection 分野の法執行にあたっている。

7　http://www.ftc.gov/ftc/ftc-org-chart.pdf

8　“Federal Trade Commission Performance and Accountability Report FY 2010”, p.6

各 Division の規模は、比較的小さく、例えば Division of Privacy & Identity Protection は、弁護士が 22 人、マネージャーが 3 人、調査員が 2 人、技術知識のエキスパート（フルタイムではなく、ハーフタイム)、事務スタッフ 2 人のおよそ 30 人である。平均すると各 Division は、40 人くらいの人数の規模である[9]。

下記に Bureau of Consumer Protection の組織図を掲載する。

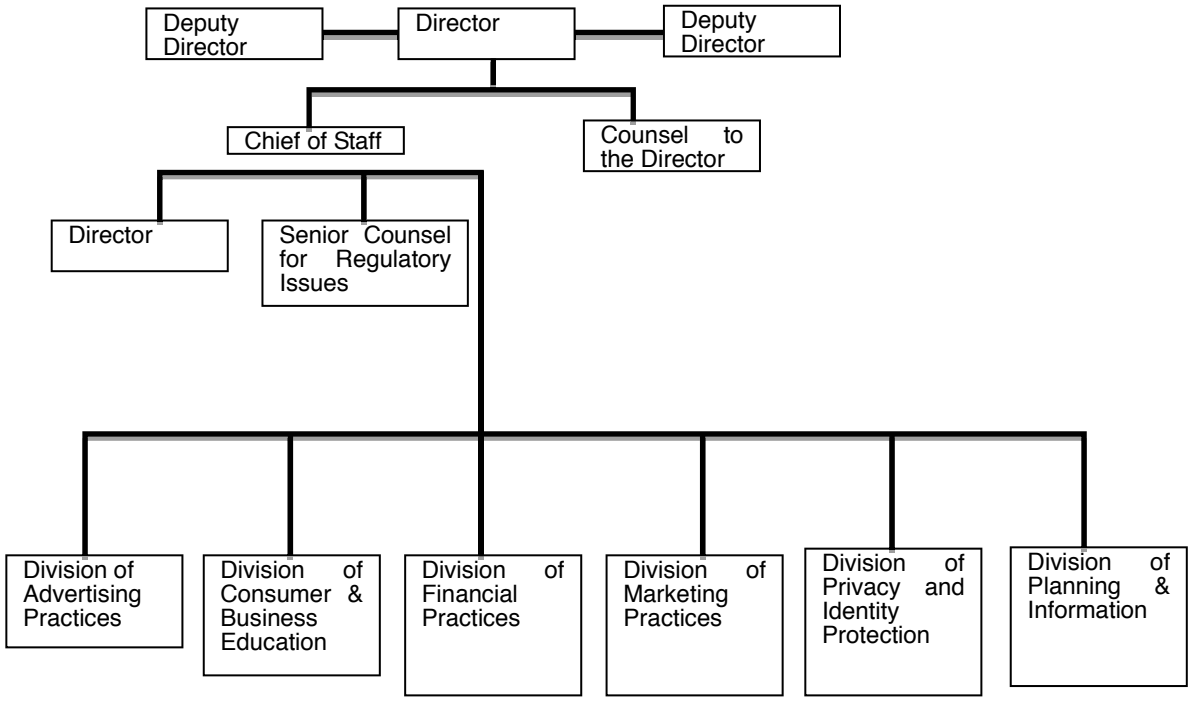

図 2　Bureau of Consumer Protection の組織図

職員の勤務状況であるが、ケースを持つと急に忙しくなることもあるが、基本は 9 時–17 時の生活（定時）であるという。また、研究調査[10]によると、アメリカの小さい政府機関の中では働きたい場所 Top10 の中に入るという。実際、ヒヤリングでは、FTC に一度就職すると、他の政府機関と比べて離職率が低い気がするという意見があった。10 年以上勤務しているのは普通であるという。これは、アメリカの民間企業などと比べてかなり一つの場所に勤める勤続年数としては長いほうであると考えられる。

9　前掲 1

10 Partnership for Public Service and American University's Institute for the Study of Public Policy Implementation (ISPPI)

また、給与については、実際の給与金額の情報は得ることはできなかったが、米国の公務員給与形態にのっとって給付されており、コミッショナーの給与は、大臣並みということではないようである。むしろ、コミッショナーより、Bureau of Consumer Protection や Bureau of Competition などの Director の給与の方が高いという。もちろん、職員の給与形態も、国家公務員の給与形態にのっとっているが、弁護士資格を持っている者は等級が真ん中より上からはじまるという。

② 予算

FTC 全体の予算は大きく分けて、消費者保護（Protecting Consumer）分野と公正競争の保持（Maintain Competition）の２つの目的についてそれぞれ予算割り振られている。

個人情報保護、プライバシー保護に関わりのある、消費者保護目的の予算について、2007 年～2011 年分を以下に掲載した[11]。

11 Federal Trade Commission FY 2008, 2009, 2010, 2011, 2012 Congressional Budget Justification Summary

表１消費者保護（Protect Consumer）分野の予算額とその FTE

Strategic Goal 市場における消費者に対する詐欺、欺瞞その他の不公正な慣行の防止	FY 2007 FTE	FY 2007 Amount	FY 2008 FTE	FY 2008 Amount	FY 2009 FTE	FY 2009 Amount
1. 消費者に対して重大な被害(injury)を及ぼす Identity fraud, 欺瞞、不正な慣行に対する対策	92	$24,416	94	$27,400	96	$24,827
2. 詐欺、欺瞞、不公正、その他の違法行為に対する法執行	397	$84,038	403	$90,523	419	$102,042
3. 消費者教育を通して消費者の被害を抑えること	50	$11,157	49	$14,420	49	$12,351
4. アメリカ国民を国際競争社会において保護するため、他国に対して消費者保護に関する政策、技術的な助言をする	30	$6,780	35	$7,603	37	$9,083
合計	569	$126,391	581	$139,946	601	$148,303

Strategic Goal 市場における詐欺、不正な企業活動の防止	FY2010 FTE	FY2010 Amount	FY2011 FTE	FY2011 Amount
1. 消費者に対して重大な被害(injury)を及ぼす Identity fraud, 欺瞞、不正な慣行に対する対策	94	$21,950	91	$22,548
2. 詐欺、欺瞞、不公正、その他の違法行為に対する法執行	443	$113,271	448	$113,824
3. 消費者教育を通して消費者の被害を抑えること	50	$18,147	50	$16,063
4. アメリカ国民を国際競争社会において保護するため、他国に対して消費者保護に関する政策、技術的な助言をする	7	$2,900	7	$2,959
5. リサーチ、報告書、ルールメイキング、擁護（advocacy）を通して消費者の保護を強化すること	40	$10,317	44	$11,049
合計	634	$166,585	640	$166,443

FTE（Full-Time Equivalents）というのは、フルタイムの職員が年間を通して何人必要かという試案である。例えば、2010 年は「詐欺、欺瞞、不公正、その他の違法行為に対する法執行」を実行するために、443FTE 必要である。

2007 年～ 2009 年までは、消費者保護を 1 ～ 4 までの実施事項にさらに分けて予算を割り振っている。2010 年以降はさらに 1 つ実施要項が増えて、1 ～ 5 となった。「4. アメリカ国民を国際競争社会において保護するため、他国に対して消費者保護に関する政策、技術的な助言をする」に関する予算

がかなり減り、その分、「5. リサーチ、報告書、ルールメイキング」の項目が追加されている。それらを通して FTC の役割を強化しようという狙いがあるようである。

さらに、下記に、Consumer Protection の予算について、上記表の 1 ～ 5 の実施事項ごとに、具体的な分野にどの程度 FTE を割り振っているのかを以下に示した。

表 2 実施施策毎の Consumer Protection の予算

	2011					
	Objective Number					Total FTE
	1	2	3	4	5	
Financial Practices	5	90	4	0	6	105
Privacy and Identity Protection	6	33	2	0	9	50
Marketing Practices	5	87	2	0	3	97
Advertising Practices	5	48	1	0	6	60
Enforcement	3	48	1	0	1	53
Planning and Information	39	8	3	0	0	50
Consumer and Business Education	0	0	20	0	1	21
Economic and Consumer Policy Analysis	0	1	1	0	3	5
Management	5	15	3	0	4	27
Support	23	118	13	7	11	172
合計	91	448	50	7	44	640

いわゆる個人情報保護、プライバシー保護は全ての分野に横断的に関わっているであるが、特に Privacy and Identity Protection、Marketing Practices、Advertising Practices の 3 分野は、個人情報保護、プライバシー保護の方執行に関わる事案を扱っていると考える。これらの FTE を足すと 207 であり、これは全体の 32%ほどである。

③役割と業務

FTC の中心業務は、法執行、政策立案のイニシアティブ、消費者、企業などに対してのプライバシー問題に関する教育普及などである。FTC は、プライバシーに関する業務を通して、現在未来におけるプライバシー保護の重要性と同時に、ビジネスにおけるテクノロジーのイノベーションの重要さを痛感しており、その２つのバランスをとるため、柔軟かつ革新的なプライバシー保護のアプローチが変動する市場において必要であると考えている。

FTC は、FTC 法 Section5 のもと、欺瞞・不公正な行為、慣行に対してアクションを取る。ここでいう、不公正な行為とは、「消費者自身によっては合理的に回避することが出来ず、かつ、その行為・慣行が消費者又は競争にもたらす利益を上回るような実質的損害を消費者に与える又は与えるおそれがある行為・慣行」を意味する。また同時に FTC は、様々な分野の個人情報保護、プライバシー保護に関わる法の執行も任されている。例えば Gramm-Leach-Bliley Act(GLB Act)、the Children's Online Privacy Protection Act (COPPA)、The Can-Spam Act、さらには Telemarketing and Consumer Fraud and Abuse Prevention Act などがある。Telemarketing and Consumer Fraud and Abuse Prevention Act は、Do not Call Rule というものを FTC が規定している。Do not Call Registry に消費者が登録をすると、セールスなどの不要な電話がかかってこないようになるというものである。一定の効果が得られているという。

その他 FTC は、プライバシー関連の政策立案のイニシアティブ、消費者、企業などへのプライバシー問題に関する教育普及を担当している。

さらに、FTC は、苦情の情報などを Consumer Sentinel Network (CSN) に登録を行っている。また、FTC はこのデータベースに、The Internet Crime Complaint Center、Better Business Bureaus、the Identity Theft Assistance Center、the National Fraud Information Center、そして 2011 年からは The North Carolina Department of Justice、The Minnesota Department of Public Safety、The Lawyers' Committee for Civil Rights、The Center for Democracy and Technology、Publishers Clearing House、MoneyGram International and Privacy Star からの苦情情報も登録している。これらの情報は、あらゆる米国内の政府機関、州政府、そして外国の法執行機関に提供され共有されている。

（2）法的位置づけ

＜民間部門に対する監視機関について＞

民間部門を関する第三者機関の存在については、特に違憲性の疑いはない。独立した機関として議会に対して報告義務がある。また今日においてはこのような第三者機関に関する論争もなく、先に述べたように 2011 年 7 月にはまた新しく Consumer Financial Protection Bureau が Department of Treasury から独立する。現在、民間部門を監督する第三者監督機関に関して法的な問題点は存在していないといってよい。

＜公的部門に関して＞

公的機部門を監督する第三者監督機関というものは、存在しない。憲法違反となるからである。合衆国憲法の Article II は “The executive power shall be vested in a President of the United States of America” と規定しており、大統領に執行権が授けられているからである。大統領の管轄の外に、その執行権を監視する機関を設けるのは憲法違反となるとされる [12]。これが、公的部門を監督する FTC のような監督機関を設けるのは難しいとされる一因である。そのためか、FTC も民間部門に法施行を行う権利あるが、公的部門に対しては権利がない。

公的部門における個人情報保護やプライバシー保護はどのように遵守されているのか。

まずは、国民には表現の自由が保障されている。これにより、国民は自分のプライバシーがどのようにそしてひどく政府によって侵害されたか、いくらでも表現していくことができる。そして、国民は訴訟を自由におこすことができる。次に、議会は執行部を監督する権限があり、その執行に問題がある場合は、調査を行うことができる。また、議会は法律を改正する、新しく追加するなどして、政府機関における個人情報保護の取り扱いに関する規定を厚くすることができる。

以上の点により、アメリカにおいては公的部門に対して第三者監督機関を置くことができない、また置く必要がないと考えられている。

---

12 前掲 5

3　監督機関の運用実態

（1）施行状況の概要

FTC の最大の業務は、管轄する法に関する違反に対する調査と法執行（Investigation and law enforcement）である、以下に FTC におけるこれらの手続きを説明する。

①調査

FTC は、所管している FTC 法 Section5 に基づく違反などを自ら探し出すことから始める。その主な情報源はニュースであり、また他省庁からの情報（referral）である。違反をしている企業の競合企業からの告発などが情報源となる場合もしばしば見受けられる。

FTC は、その情報源に基づき、対象になった会社や個人などに対して立入検査、令状による命令を含む調査を行う権限がある（FTC 法 Section 9）。また、文書提出命令、証人関門等の民事審査請求を行うことができる。さらに、FTC は、特別年間報告書を提出させる権限もあり、これに従わない場合は裁判所で遵守することを命令してもらうことができる。また一定期間置いて従わない場合は罰金（民事罰）を科すことも出来る。

②法執行

（a）Adjudication

FTC は、不公正又は欺瞞な行為、慣行に対して FTC 法 Section 5 に基づいて法執行を行うことができる。さらに、その他の FTC 所管法令に基づいて、法執行を実施する。

（b）排除措置と同意命令（consent order）

FTC は、排除措置を命じることが相当であると判断した場合に、改善について同意を求める。もし、相手方が同意に応じれば FTC は同意命令(consent order)を下し､相手方はその措置に従うこととなり、事件は終了する。しかしこの同意はあくまで相手方の自発的な行為に基づくものであり、同意をしたくない場合はしなくてもよい。また、同意命令は、違反事実を法的に認定したも

のではなく、違法性を法的に確定するものではない。

（c）行政審判

相手方が争うと決めた場合は、今度は行政法審判官（Administrative Law Judge）のもとで争われ、立会審査官が原告、被審人が被告となり、審判が開始することとなる。対審構造の審判手続きが行われ､違反事実の存否について審理が行われる。そして､ALJ が仮決定（initial decision）を下す。なお、審判開始決定後であっても同意命令手続きを行うことは出来る。

もし、立会審査官か、または被審人がこれに不服の場合は、コミッショナー５人のフルコミッショ

ンに再度審査を請求することができる。そして、これに対してコミッションの最終的な決断が下される。この判断に不服の場合は、控訴裁判所に控訴することができる。そしてその判断は裁判所の判決となる。もし、その判決に不服があれば、最高裁判所に上告することができる。

もし、コミッションの最終判断に従わない場合は、地方裁判所において民事罰を求められる。また地方裁判所は必要的差止め（mandatory injunctions）をすることも出来る。

また、コミッションはさらに消費者自身に損害賠償についても告発された側に求めていくことができる。

排除措置を命じられた側は同意命令に応じることも多く、裁判所（行政審判を含む）まで争われるケースはそこまで多くはない。

（d）取引規制規則の制定（Rulemaking）

上記の Adjudication に加えて、産業規模の不公正又は詐欺的取引慣行を防止するため、取引規制規則（Trade Regulation Rules）を制定することができる（FTC 法 18 条）。これにより、FTC は、訪問販売におけるクーリング・オフに関する規則、テレマーケティング販売に関する規則等、消費舎取引に関するさまざまな規則を制定している。

FTC が規則を制定するには、関係者に非公式なヒヤリングを行い、特定の者が不利益を被らないようにしなくてはならない。規則が公表されると、そのルールに違反する者に対して、FTC は、地方裁判所に$11,000 を上限として罰金（民事罰）をその違反行為ごとに課すことを求めることができる[13]。また、そのルールに違反したものは、そのルール違反によって生じる消費者の損害に責任を持たなくてはならない。FTC は、このような場合消費者のために損害賠償を裁判所に求めることができる。

13 http://www.ftc.gov/ogc/brfovrvw.shtm

（e）司法手続き

上記のいずれの場合も、FTC は罰金を課すこと、損害賠償請求を行うためには裁判所に求めなければならない。しかし、FTC は命令を下したり、規則を制定したりすることができる他、命令を下さないで直接裁判所に訴えを起こすことができる。FTC 法 13 条では、FTC を執行する法に違反する行為を行っている場合又は今まさに行おうとしていると信じるに足る場合、仮差止めを裁判所に直接求めることができる。これは、審判中の事件に関しても行うことができる。また、事件によっては、差止め請求も出来る。

現在は、同意命令（consent order）から行政審判に行くケースより、直接地方裁判所に FTC が請求をして行くケースが増えている。仮差止めと賠償金請求が一度に出来るので、効率が良いからである。

もちろん、行政審判にも利点がある。この場合、FTC は事実関係について最初に認定をしていくこととなる。裁判においてもこの事実関係に関する FTC の判断について、その証拠が信用できるものであれば、裁判所は FTC の判断に従わなければならない。また、FTC の FTC 法やその他の法律に関する解釈を尊重しなければならない。そのため、FTC は新しい種類の法解釈や事実を含む場合は、行政裁判を好む傾向にある。

（2）苦情処理・紛争解決（体制・仕組み、件数等）

基本的には、FTC では苦情処理は行っていない。ただし、苦情受付は常におこなっている。FTC は、苦情を統計や調査の補助資料として使用するのみである。下記に、苦情を受付して Consumer Sentinel Network Data Book というデータベースへ記入したものの数を記載する。

表 3　FTC で受け付けた苦情件数

	FY 2006	FY 2007	FY 2008	FY 2009
件数	1,011,000	1,100,000	3,050,000	3,300,000

また、このデータベースに登録された情報は、世界中のあらゆる個人情報保護やプライバシー保護に関わる法執行機関が、閲覧することができ、グローバルな個人情報保護、プライバシー保護に一役買っている。

（3）権限行使（罰則・命令・勧告・立ち入り検査の件数等）

Consumer Protection の分野では、2010 年度、57 ケースを地方裁判所で争い、また 102 の判決を得ることができた。そして、$560 million の損害賠償を被害者に支払わせ、$11.4 million を民事罰として支払わせた。また、Department of Justice へ送られた（request）ケースでは、11 の民事罰を課すことができ、$21 million の金額を得た。また、FTC は、新しく 9 の行政審判を行い、16 の行政命令を下した。ほとんどのケースにおいて、FTC は他の法執行機関と連携をして行った。ただし、これらの数字は、クレジットカード詐欺やローンに関するものが多く含まれており、個人情報保護まわりの純粋な数字ではない[14]。

以下に個人情報保護、プライバシー保護まわりの 2010 年の代表的なケースを示す[15]。

【Safe Harbor Cases】

2010 年 1 月､現在までの 6 つの会社[16] に対して排除措置の通告を行い､同意命令に至った。いずれも、EU/US Safe Harbor の基準を満たしていないのにも関わらず、消費者を欺瞞して満たしているように見せかけていた。これに対し、同意命令を発した。

【US Search】

2010 年 9 月には、オンラインデータブローカーの US Search が、自己の個人情報に関して、他人が見たり買ったり出来ないようにするために課金を消費者に対して行うという欺瞞的な行為を行っていた。これに対し、課金された金銭を 5000 人の消費者へ返還するとともに、Web サイトの改善を命じた。

---

14 “The FTC in 2010”, p.25

15 “Protecting Consumer Privacy in an Era of Rapid Change Proposed Frame work for Businesses and Policy makers, Preliminary FTC Staff Report”, FTC (Dec. 2010)

16 World Innovators, ExpatEdge Parteners, In the Matter of Onyx GraphicsInc., Directors Desk, Progressive Gaitways, Collectify

【Social Networking Service –Twitter–】

Twitter に対し、利用者の個人情報を適切に保護することができず、プライバシー侵害のリスクにさらしたことについて、排除措置を命じ、同意命令に達した。

【Data Security】

FTC は 2010 年 12 月、100 近くの団体が自己のコンピュータネットワークにおいて保有する、消費者や被雇用者の個人情報などが、P2P ファイルシェアリングネットワーク上に漏洩しているという警告の手紙を送った。Dave & Busters, Inc. は、排除措置に応じ、保有している消費者のクレジットカード、デビットカードの情報を道理にかなった適切な方法で保護することにした。

【州とのジョイントケース–LifeLock–】

2010 年 3 月、35 の州と協力し、FTC は LifeLock に対し、同社が行う ID 詐欺防止のサービスについて欺瞞的な抗告を行ったとした。同社は同意命令に応じ、消費者に$11 million そして、州に$1 million を支払った。

【Computer Security】

FTC は 2010 年 2 月、コンピュータセキュリティソフトに関して、スパイウェアやウィルスをスキャンするという 1 万件もの嘘の広告を行ったとして、$163,167,539 の判決を得た。

また、FTC は 2010 年 4 月、地方裁判所において、3FN というインターネットプロバイダーをシャットダウンし、$1.08 million の賠償金を得た。このプロバイダーは、スパムや児童ポルノ、その他のデジタルコンテンツの配信に関わってきていた。また、リモートキーロガープログラムを売り、他人に知られることなく他人のコンピュータにそれらをインストールする方法を公表していた FTC は Cyberspy Software, LLC にストップをかけた。

【Telephone Services】

2010 年 3 月、FTC は、DOJ を代理し、さらカリフォルニア、イリノイ、オハイオ、ノースカロライナ政府とともに、衛星テレビ会社の Dish Network を連邦裁判所に訴えた。この会社は、Do Not Call Registry に登録されている消費者に対して電話で営業を行った。

【子供のオンラインプライバシー】

2009 年 11 月、IconixBrand Group, Inc. は、$250,000 を罰金として支払った。これは、保護者の承諾を得ずに 1000 人ほどの子供の個人情報を収集、保持していたことによるものである。

表 4　Privacy 関連の主要 Case 一覧（2007 年以降）[17]

＊ 裁判所で争われたものだけでなく、同意命令も含む

年度	ケース名
2006 年度	US v. Choice Point
	消費者保護（FCRA）のケースで民事罰の最高額（罰金 $10 million と被害者への賠償金 $5 million）
	In the Matter of Zango
	アドウェアに関する初のケース
	US v. Xanga
	COPPA で最高額の民事罰（ $1 million）
	In the Matter of CardSystems Solutions
	金融情報の最大級の漏洩に対する同意命令（settling charges)
2007 年	US v. American United Mortgage Company
	DisposalRule がはじめて適用された
	FTC v. Various (dba AdultFriendFinder)
	アダルト向けのソーシャルネットワークにおける、利用者に選択の余地のない性的画像のポップアップに関する同意命令
2008 年	US v. Value Click
	CAN-SPAM の最高額の民事罰（ $2.9 million ）
	In the Matter of Reed Elsevier and Seisent
	データブローカーの LexisNexis に対する顧客情報の流用

17 前掲 15

	In the Matter of TJX Companies
	データブローカーの TJXに対する顧客情報の流用
2009 年	In the Matter of CVS Caremark
	雇用者情報の保護に関する初のケース
	In the Matter of World Innovators
	EU-US Safe Harbor に関するケース
	In the Matter of ExpatEdge Parteners
	EU-US Safe Harbor に関するケース
	In the Matter of Onyx Graphics
	EU-US Safe Harbor に関するケース
	In the Matter of Directors Desk
	EU-US Safe Harbor に関するケース
	In the Matter of Progressive Gaitways
	EU-US Safe Harbor に関するケース
	In the Matter of Collectify
	EU-US Safe Harbor に関するケース
2010 年	In the Matter of Twitter
	初のソーシャルメディアに対するデータセキュリティのケース
	FTC v. Pricewert
	ISP をシャットダウンしたケース
	FTC v. ControlScan
	Online seal provider に対するデータセキュリティのケース
	FTC v. Innovative Marketing
	スパイウェアに関する最高額の賠償金ケース（$163 million ）
	FTC v. Lifelock
	FTC と州が協力した最大級のプライバシーケース
	Sweep against companies for exposure of employee and/or customer data on peer-to-peer (P2P) file-sharing networks
	いろんな P2P ファイルに関するデータセキュリティについて様々な企業を一斉調査(sweep)し、意見書を対象の会社に送った

4　監督機関の課題等

FTC は特に消費者のプライバシー保護、データセキュリティについて強化をしている。特に、現在はソーシャンルネットワーク、クラウドコンピューティング、オンライン広告、携帯マーケティング、データブローカーの情報収集とその利用についてについてどのように今後対応をしていくべきか、直近の課題として検討をされている。

また、技術の革新次々と行われ、とりまく状況が刻々と変化をする個人情報保護、プライバシー保護の分野では、特に以下の３つのことを特に企業と政策担当者に対して指導をして行きたいと FTC は考えている。

■ Privacy by Design

企業は、消費者の個人情報保護、プライバシー保護を企業全体として強化し、新しい製品、サービスなどの開発段階のどのステージにおいても、消費者の個人情報保護、プライバシー保護を織り込んで行かなければならない。データセキュリティ、道理にあったデータ収集の制限、データの正確性などに特に注意しなければならない。

■ Simplified Choice

消費者の個人情報保護に関する選択肢を簡潔にする。企業は、慣行的に行われてきた個人情報の収集については消費者の同意を得る必要がない。しかし、選択が必要な場面においては、企業は、消費者が正しい選択を出来るタイミング、文脈において選択肢を提供いなければならない。

■ Greater Transparency

情報の取り扱いについて透明性を保つ必要がある。個人情報の注意事項に関しては、短く明確に、そしてより一般的な標準に合致したものでなければならない。収集した個人情報に関しては、その情報に対して道理にかなったアクセスを提供し、さらに個人情報を収集した際と異なった目的で個人情報をしようする場合は、特別に公表して利用の合意を得なければならない。また、情報を取り扱う者は、常に消費者に対して商業的な個人情報の利用に関して教育を行わなければならない。

さらに、FTC の課題としては、国際的な個人情報保護の連携を他国の法執行機関と行うことがまず重要である。さらに、FTC が現在管轄している金融関係の消費者保護に関わる法律が、新しい独立第三者機関に移行するので、それに対する対策が必要であるといえる[18]。また、より消費者や企業に対する個人情報保護、プライバシー保護の教育の強化と、政策提言に力をいれていくということである。

---

18 前掲 1

vii. カナダ

1　個人情報保護法制の概要

（1）法律名、目的、適用範囲、適用除外、内容（権利・義務規定）

①概要

カナダは、10 州と 3 準州からなる連邦国家である。公的部門に関する個人情報保護法と民間部門に関する個人情報保護法は、分離されている。連邦の個人情報保護に関する法律は、公的部門に係る法律である Privacy Act と民間部門に係る法律である Personal Information Protection and Electronic Documents Act（PIPEDA）である。

10 州全てが州の公的機関に係る個人情報保護法を個別に 持っており、州の公的機関に対しては連邦法の Privacy Act は適用されない（州の中の市や町などの機関にもこのそれぞれの州法が適用される）。一方、民間部門に係る法律は、連邦法の PIPEDA が州内の取引にも適用される。ただし、各州が連邦と「実質的に同様」（substantially similar）な立法を行っている場合には、連邦法の適用から除外され、州法が適用される。現在、この「実質的に同様」の認定を受けているのは、4 州だけである。ただし、例えばオンタリオ州のように Personal Health Information Protection Act（PHIPA、医療個人情報保護法）という医療に係る個人情報についてのみ個別に個人情報保護法が州レベルで存在する場合もある。この場合、州内の医療関係の個人情報はこの法律が適用される。

このようにカナダの個人情報保護法は連邦と州の法律が複雑に混在する形となっている。

②目的と適用範囲

カナダの個人情報保護法は、「識別可能な個人に関する情報」を保護対象とするものであり、この点で 1980 年の OECD ガイドラインと方向を同じくする。連邦法上の公的機関に係る法律である Privacy Act はプライバシー保護一般だけを目的とはしておらず、「政府機関が保有する個人情報に関し、当該個人のプライバシーを保護し、また当該情報につき当該個人にアクセス権を認める既存のカナダ法を拡張することを目的」（第 2 条）としている。よって、Privacy Act は、プライバシーだけではなく情報へのアクセス権も保護する。

・Privacy Act

Privacy Act では、個人情報を「その形態のいかんを問わず、識別可能（identifiable）な個人に関する情報」（3 条）であると定義、a ～ i 号において 9 つのタイプを列挙し、その後に続く j ～ m 号で特定の条項の関係で個人情報として取り扱われない情報の種類が列挙されている。個人情報の収集、保持、破棄については、4 条～ 6 条、利用、公開については、7 条～ 8 条に規定されている。これらの条項は、カナダ国民だけではなく、国籍にかかわらず全ての人に適用される。公的機関はその業務に係る個人

情報のみ収集することができ、その個人の同意なしの公的機関同士での個人情報の共有は禁止されている。また、収集に際して、その個人情報収集の目的について明らかにし、同意を得なければならない。政府によって収集された個人情報は一定期間（最低２年）保持されなければならない。さらに、個人情報は、その情報が常にその個人に関する最新の情報であるようにしなければならないとされている。政府機関の長に対し、その管理する個人情報を原則として Personal Information Bank（個人情報バンク）に登録するとともに、データバンクの概要を示す情報を一般に公開しておくことが要求される（10条)。さらに、政府機関の管理下にある情報で個人情報バンクに登録されていないものに関して、破棄については機関ごとに個別に規則が定められてその規則に従わなければならない。機関ごとの個別規則は、The Library and Archives of Canada Act に準じたフレームワークを採用している。また、本人に同意を得た目的以外の個人情報の利用は許されない。個人情報の開示については、本人の同意がない限り、第三者に対しては開示されてはならず（8 条)、一方で本人の求めに応じて開示しなければならない（12 条 1 項)。また､本人は自己の情報に誤りがあった場合などは訂正を請求することができ、訂正がなされなかった場合には、訂正の請求があった事実を当該情報に付記することを求める権利が定められている。ただし、この本人の同意なく個人情報を開示してはならないという原則については、この原則を定める 8 条にその例外が規定されている。

また、個人情報の開示請求については適用除外があり、69 条、70 条において規定されている。国立図書館・国立博物館等の収蔵資料、政府機関以外により、又は政府機関以外のために国立図書館等に寄託された資料、Queen’s Privy Council for Canada（中枢院）機密文書などは、Privacy Act が適用されない。さらに、外国政府や外国機関、国際機関、州政府、州政府によって設置された地方団体などから秘密を条件として取得した個人情報、連邦騎馬警察が州又は地方公共団体のために警察活動中に取得した個人情報で、当該州または地方公共団体の要請に基づきカナダ政府が非開示としたものなどは、開示請求があっても応じてはならないことになっている。一方で、連邦州間問題に関する個人情報、国際関係又は国防に関する個人情報、法執行や犯罪捜査に関する個人情報、受刑者から刑務所等の施設に開示請求がなされた個人情報などは、政府の裁量によって開示できるとされている。

• PIPEDA

PIPEDA は、「プライバシー権」と「諸組織が個人情報を収集、利用開示するにつき、合理的人間が当該状況に照らして妥当と認める必要性」のバランスをとって、「個人情報の収集、利用及び開示」を規律する準則を定めることを目的とする。商業活動 (commercial activities) の過程で個人情報を収集、利用又は開示する全ての組織（organization)、連邦レベルで活動、事業またはビジネスを行うにつきその従業員の個人情報を収集、利用又は開示するすべての組織が適用対象になる。OECD ガイドラインを実定法化しており、8 原則に対応する 10 原則を定めている。適用除外について、PIPEDA 全体にかかる適用除外として、Privacy Act が適用される政府機関、個人情報を私的なあるいは家庭内の目的をもって収集、利用又は開示するにすぎない個人、報道や、芸術、文学の目的の場合、ある組織

の従業員についての､氏名､職位､勤務先住所､電話番号などがある。さらに､個人情報の収集や利用､

開示に関する本人への告知･同意原則が排除されるという形での適用除外が存在する(4 条および 7 条)。

州レベルの法律に関しては、それぞれ 10 州全てが連邦政府以外の公的機関に関する個人情報保護の法律を持っており、州によっては民間機関に対する PIPEDA にかわる法律がある州、さらに医療に関する個人情報に対してのみ州独自の法律を持つものなど様々である。

（2）監督・登録制度

上記の Privacy Act、PIPEDA 両法については、Office of Privacy Commissioner（OPC）が法執行を管轄する。州政府などの公的機関に関する法律、州が PIPEDA に「実質的に相当」する法をもっている場合はその法律などについては、州の管轄となり、それぞれの州に存在する Privacy Commissioner に法執行がまかされている。本報告では、州レベルの法についてはオンタリオ州を例に記述する。

2　監督機関の制度概要

（1）設置の経緯

① Office of the Privacy Commissioner of Canada（OPC）

カナダ連邦の個人情報保護に関する監視・紛争処理機関（第三者機関）は、Office of the Privacy Commissioner（OPC）である。1982 年の Privacy Act により設置されたものであり、Privacy Act（公的部門）と Personal Information and Electronics Documents Act（PIPEDA、民間部門）の双方の運用に関して担当をする。OPC は一般的に、不服申立（complaint）に対する判断が法的拘束力を有さないため、オンブズマンとして理解されている。Commissioner は、Officers of Parliament（国会に仕える役人）であり、Privacy Commissioner と同様の地位にある機関としては、他に Auditors General、Chief Electoral Officers、Commissioners of Official Languages、Information Commissioners、Conflict of Interest and Ethics Commissioners、Public Sector Integrity Commissioner、Commissioner of Lobbying がある。

Commissioner の中心的な役割は、二つの法の執行である。個人からの問い合わせ・苦情をもとに、不服申立の案件を扱う。これは通常のオンブズマンの職務と同様であるが、これに加えて Commissioner は、自己付託によって強制調査を行い、不服申立を自らすることもできる。その点で Privacy Commissioner は他のオンブズマンと異なる特徴を持つ。また、プライバシーや個人情報保護をめぐる諸問題、例えば新規の立法などについて、調査を行い、公的に意見を発することも行う。それらの面でも、通常のオンブズマンの権限を超えたプライバシーと個人情報に関する全般的な業務を行っている。

②州政府の Privacy Commissioner

–Information and Privacy Commissioner, Ontario Canada（IPC）を例として –

カナダは、10 州と 3 準州からなる連邦制度構造をとっている。そのため、一部の個人情報保護に関する分野は、州の管轄となっている。州や市の公的機関については、州の法律が適用される。10 州全てに連邦法の Privacy Act と同様の法律が存在する。

オンタリオ州にも Privacy Commission が存在し、Information and Privacy Commissioner（IPC）と呼ばれる。Commissioner の Ann Cavoukian は、”Privacy by Design” の提案者として有名である。Privacy by Design (PbD) は、プライバシー保護の概念を、デザイン仕様書、ビジネスの慣行、物理的な基盤に埋め込む考え、すなわちプライバシー保護を、デザイン仕様書や新たなシステムを作るうえでの構造やその手順にあらかじめ組み込んでいくという考え方である。Ann Cavoukian の精力的な活動が高く評価され、オンタリオ州の Information and Privacy Commissioner, Ontario Canada（IPC）は、州レベルの機関であるにもかかわらず、世界的に注目を浴びている。

オンタリオ州の公的部門の個人情報保護に関する法律としては、まず Ontario’s Freedom of Information and Protection of Privacy Act（FIPPA）という法律がある。Information and Privacy Commissioner（IPC）は、この法律に基づいて 1988 年 1 月 1 日に設置された。この FIPPA は、州の政府だけではなく、その他の州の公的機関、例えば大学などにも適用される。もう一つの公的部門に関する法律は、The Municipal Freedom of Information and Protection of Privacy Act（MFIPPA）と呼ばれる。MFIPPA は名前の通り、地方の市、警察、図書館、学校などに適用される。

民間部門に関しては、基本的には連邦法（PIPEDA）が適用されるが、個人の病気や疾患、通院の記録など健康上の記録が医療施設の中において収集、利用、公開される場合については、州独自の法律である The Personal Health Information Protection Act (PHIPA) が適用される。この PHIPA には、個人が自己の健康に関する情報の開示請求を出来る権利も含まれる。

オンタリオ州には、IPC 以外にも、IPC と同様に独立した地位にある機関が 5 つ存在する。The Auditor、The Ombudsman、Environmental Commissioner、Conflict of Interest Commissioner、The Chief Election Officers の 5 つである。これらの機関は、行政からも独立をしており、また自発的に管轄する法に関連する問題について調査でき、場合によっては法的拘束力のある命令を出せる場合もある。

（２）制度の概要（所掌事務、組織体制、人事制度、職員数、予算等）

① Office of the Privacy Commissioner of Canada（OPC）

OPC は、議会（Parliament）に直接責任を負う独立した機関である。職員は公務員としての待遇にあり、Commissioner は、各省次官相当とされている。Assistant Commissioner が２名おり（一人は、Privacy Act（公共部門）担当、もう一人は PIPEDA（民間部門）担当)、さらにその下に各部門が置かれている。Commissioner は、7 年任期であり、議会から指名される。

以下に、簡単に各部門の説明を記す[1]。

a）Investigations and Inquiries Branch（調査・審査部）

Privacy Act 29 条（公的部門）と PIPEDA 11 条（民間部門）に基づいて、個人から寄せられた不服申立（complaints）[2] に関して調査を行い、Commissioner が最終的に判断を下す（Findings)。また、その他あらゆる情報源からの情報に基づいて、個人情報の取り扱いの管理に問題があるケースについて独自の調査を行う（incident investigation)。調査後､Commissioner が判断（Findings）を下し、不服申立者と不服申立をされた政府機関や民間機関（被不服申立者）に対して判断（Findings）のレポートを送付する。申立が認容されれば、申立をされた側に対して勧告（recommendation）も行う。不服申立の調査、判断の手順等についての詳細は後述する。

b）Audit and Review Branch（監査・評価部）

監査・評価部では、公的機関、民間機関が、二つの個人情報に関する連邦法を遵守しているかについて評価する。公的機関は、Privacy Impact Assessment Reports（PIAs）を提出する義務がある。民間部門について義務はないが、PIAs を提出し個人情報に関する連邦法を遵守していることを広く示す努力をすることが望まれている。

c）Communication Branch（渉外部）

渉外部は､主に広報に対する戦略的なアドヴァイスとサポートを行う。また､メディアなどをモニターして、OPC の教育活動に対する評価や世論などを分析して、OPC のイベント等を企画していく。

d）Research, Education and Outreach Branch（研究、教育、社会事業部）

研究、教育、社会事業部は、プライバシー、技術などに関わる課題を研究し、OPC の政策展開、調査、評価、教育活動をサポートする。国際的な関係者との社会事業にも関わっている。

1　http://www.priv.gc.ca/aboutUs/au_org_e.cfm#contenttop

2　個人によって苦情・問い合わせ（inquiry）として OPC へ提出されたものの中から、登録官（register）が不服申立（complaints）を構成することができるか判断する。不服申立と認められたもののみ調査（investigation）の段階に進む。不服申立を構成しない場合（例えば OPC の管轄ではない場合なども含む)、苦情・問い合わせを行った個人に対しアドヴァイスがされる。

e) Legal Services, Policy and Parliamentary Affairs Branch（法サービス・政策・議会対策部）

法サービス・政策・議会対策部は、OPC に対して、カナダ国内又は国際的にプライバシーに関してこれから課題となると考えられる事項に関する法的戦略を提案する。また、訴訟当事者として参加をするプライバシーに関する訴訟について担当をする。また、Commissioner に対して、Privacy Act と PIPEDA の解釈に関する法的なアドヴァイスも行う。一般的な法的アドヴァイスも他の部に対して行う。Commissioner の議会に対する説明責任についてもサポートを行う。

f) Human Resources（人事部）

人事部は、人事に関して広範な管理の責任を行う。

g) Corporate Services（総務部）

組織の管理を主に行い、また財務に関する管理も行う。

②州政府の Privacy Commissioner
–Information and Privacy Commissioner, Ontario Canada（IPC）を例として –

オンタリオ州 Commissioner（IPC）は、連邦政府の Commissioner（OPC）と異なり、情報に対するアクセスとプライバシーの両方に関して担当する。プライバシー部門には 22 人の職員がおり、IPC 全体では 98 人の職員が働いている。プライバシー部門、情報に対するアクセス部門それぞれに Assistant Commissioner がいる [3]。

オンタリオ州には主な政党が３つあり、最終的にはその３政党の合意で Commissioner が任命される。Commissioner は、5 年任期で、再任を希望し、州議会が承認すれば次の 5 年間また Commissioner をつとめることができる。州議会さえ承認すれば、Commissioner は何度でも 5 年単位でその地位を更新していくことができる。

管轄する法律は前述の通り、州の公的機関に適用される法律 Freedom of Information and Protection of Privacy Act（FIPPA)、市や市の警察、学校などに適用される法律（The Municipal Freedom of Information and Protection of Privacy Act（MFIPPA))、健康上の記録の医療施設における収集、利用、公開に関する法律（The Personal Health Information Protection Act (PHIPA)) の３つである。もちろん、この３つの法律が適用される機関に対しては、連邦法の Privacy Act と PIPEDA は適用されない。

2009 年度の支出は、13,028,602 カナダドルで、そのうち職員の給料等が、10,219,722 カナダドルであり、支出のほとんどが人件費である。参考までに 2009 年度の Commissioner Ann Cavoukian の給料は、203,791.12 カナダドル、Assistant Commissioner（Privacy）Ken Anderson は、210,969.58 カナダドルである [4]。

---

3 筆者の IPC ヒヤリング調査による（2011 年 3 月 15 日）

4 Office of the Information and Privacy Commissioner 2009 Annual Report : Financial Statement

3　監督機関の運用実態

（1）Office of the Privacy Commissioner of Canada（OPC）

① 施行状況の概要

（a）Privacy Act（公的部門）

Privacy Act には、連邦政府機関の個人情報の取り扱いが規定されている。その法執行を OPC は担っている。

基本的に、個人の問い合わせ・苦情をベースに、調査やそのケースの Findings を出している。ただし、Findings には法的拘束力はない。また、Privacy Act（公的部門）におけるケースについては、本人の自己情報開示請求以外の案件については、Commissioner は、連邦裁判所に出訴できない。ただし、PIPEDA（民間部門）に関するケースにおいては、Commissioner は連邦裁判所に出訴することができる。これにいては後述する。

以下に、OPC における問い合わせ・苦情の受付、不服申立、勧告（Findings）について手順を記載する[5,6]。

Inquiry

個人が OPC に対して、手紙また電話、来所によって（メールなどによる苦情・問い合わせは受け付けていない）政府機関の Privacy Act 違反に関する苦情・問い合わせを行う。2 つの部門合わせて 6 人の受付係で対応を行っている。電話、来所によって苦情・問い合わせを行った者は、後日文書に提出をしなければならない。1 日に 80 ～ 100 件の苦情・問い合わせがある。

↓

Initial Analysis

登録官は、Inquiry に関して、それらが Privacy Act に違反する可能性があるかを判断する。個人は、個人情報に関するあらゆる政府機関の取り扱いについて苦情を申し立てることができる。自己の個人情報へのアクセスの拒否・遅滞、情報へのアクセスが個人情報法の不正収集、不正利用・公開、不明確な利用や公開などに関する申立が認められる。

5　Annual Report to Parliament 2009-2010(Report on Privacy Act), Office of Privacy Commissioner of Canada

6　著者の OPC に対するヒヤリング調査の際に配布された資料。Investigations and Inquiries Branch (Arthur Dunfee, Director General, Investigations and Inquiries Branch)

↓

Complaint

苦情・問い合わせ（Inquiry）が Privacy Act に違反する可能性がある場合、それは不服申立（Complaint）として認められ、調査（Investigation）が開始される。

ケースによっては、Complaint として認められても、調査が開始される前に当事者の合意によって解決する場合もある。この場合、Early Resolution と呼ばれ、Early Resolution Officers がこの合意による解決に協力する。通常は、Early Resolution が 45 日以内に決まらない場合は、調査（Investigation）の段階へ送られる。

可能性がないと判断された場合は、その苦情・問い合わせを提出した個人宛にアドヴァイスを送付する。

↓

Investigation

調査では、Commissioner が個人の権利が公的機関において侵害されているかどうかについて判断するための基礎事実に関する情報を提供する。調査官は、各公的機関に対して不服申立の概要を提出し、申立者、被申立機関の両方に対して、事実に関する証拠等を収集、証人へのインタビュー、書類調べなどを求めることができる。また、Commissioner 又はその代理人を通して、調査官は独自に証拠収集、立ち入り検査などの権限が与えられている。不服申立に対する調査においては、強制調査権を有する。

調査の間に、申立者が不服申立を取り下げた場合、申立者が消息不明などの場合は、調査は打ち切られる。

↓ OR

↓

Settled

調査を続ける過程で、申立者と被申立者が何らかの和解に至る場合は、そこで調査は打ち切られる。基本的に OPC は、この和解を推奨する立場である。調査中のケースでも、常に調査官もこの和解を支援する。

↓

Analysis

調査官は、事実関係を整理して、Commissioner への報告書（recommendation）を用意する。また、どのような報告書を Commissioner に提出するかについて、この時点で両当事者に通知がされる。そこで、もう一度証拠や意見などを提出する機会が両者に与えられる。

この時点で和解になる場合もある。その場合、調査は打ち切られる。

Findings

Commissioner は、調査官の報告書をレビューし、査定をする。そして、調査官ではなく Commissioner が不服申立に対する最終判断（Findings）を下す。そして、両当事者に判断を文書にて送付する。そこには不服申立の概要、適切な事実関係の概要、分析、そして公的機関に対する Recommendation が記載されている。場合によっては、Commissioner は、公的機関に対して、相当の期間内に改善案を提出させることもある。

Commissioner の判断（Findings）には、以下の４種類がある。

1. Not Well-Founded
   公的機関による申立者の権利侵害が認められるに足る証拠が十分ではない。
2. Well-Founded
   公的機関による申立者の権利侵害が認められる。
3. Well-Founded, Resolved
   調査において十分な侵害の証拠が見受けられ、被申立者である公的機関は、問題点について改善を行うことを約束した。
4. Resolved
   申立者に対する権利侵害が認められたが、被申立者である公的機関が、OPC が納得できるだけの改善を具体的に約束した場合。

Findings の後…

公的部門の案件においては、連邦裁判所へ訴訟提起をすることが出来る範囲が非常に狭い。本人情報の開示請求の拒否の事例のみ、連邦裁判所へ訴訟提起をすることが出来る。この場合は、申立者が訴訟提起することも出来るが、OPC が訴訟提起をすることも出来る。

一方、民間部門ではその他の事項についても連邦裁判所に訴訟提起を出来るため、公的部門に対する OPC の権力は民間部門に対するそれと比べて、かなり限定されているといえるであろう。

■ Incidents（自己付託）について

義務ではないが、公的機関は個人情報の漏洩についての報告を OPC にすることとなっている。このことは、OPC の調査を大変効率的なものとし、さらに OPC はこれらの漏洩報告について、自己付託(incidents）として調査を行い、Findings を出すことができる。この点、漏洩報告を義務化してほしいと云う声が OPC では数多くあった。

（b）PIPEDA（民間部門）[7]

民間部門についても、公的部門と同様に、苦情･問い合わせは登録官によって登録される。登録後は、調査の段階に進む。そして調査後は、Commissioner は、両者は少々違う手順に進む。 Commissioner は、仮報告書を事前に送り、被申立者である民間機関に対して、申立に対してどのように対応するべきか recommendation を行い、一定期間の間にそれに従って改善を行うよう伝える。その後、最終報告書が両当事者に送られる。最終報告書では、申立、事実の分析、被申立者である民間企業の recommendation への対応、そして調査の結果に対する判断が記載される。これには、公的部門と同様に、Well-Founded、Well-Founded and Resolved、Resolved、Not-Well-Founded の 4 種類がある。

（c）公的部門と民間部門の大きな違い

調査と Commissioner の判断（Findings）の後において､公的部門と民間部門には大きな違いがある。民間部門では、不服申立の内容について、不服申立者又は Commissioner が連邦裁判所に訴訟を起こすことができる。ここで裁判所は改善命令を下し、さらに申立者に対して法的救済を与えることも出来る。これは、公的部門との大きな違いである。

②州政府の Privacy Commissioner
–Information and Privacy Commissioner, Ontario Canada（IPC）を例として –

（a）Ontario’s Freedom of Information and Protection of Privacy Act（FIPPA）、The Municipal Freedom of Information and Protection of Privacy Act（MFIPPA）の法執行

FIPPA、MFIPPA（公的機関）の法執行に際して、苦情・問い合わせの受付から、調査、早期解決、和解、勧告のプロセスを以下に示す[8]。

Intake

まず登録官、分析官が苦情・問い合わせをスクリーニングし、IPC の管轄外、プライバシーに関する申立ではないものを排除する。ここで不服申立と認められたものに関して、分析官は申立者に問い合わせし､問題点を明確にし､IPC のプライバシー申立に関するプロセスを説明する｡そして､問題となっている公的機関に現在の状況を伝え、解決の可能性があるか問い合わせる。

---

7 著者の OPC に対するヒヤリング調査の際に配布された資料 (2011 年 3 月 14 日)。Investigations and Inquiries (PIPEDA), Trevor Yeo, Acting Manager Investigations(PIPEDA)

8 http://www.ipc.on.ca/english/Resources/IPC-Corporate/IPC-Corporate-Summary/?id=473

Intake Resolution

登録官は、正式な調査の段階（investigation）の前に非公式な解決（resolution）にもっていけないかどうか判断をする。

Investigation

非公式な解決が望めない場合は、いよいよ調査の段階となる。調査官は、申立を明確にし、自ら情報を集めて和解を目指す。和解が望めないときは、仮のプライバシー申立のレポート（申立の概要、調査中に収集した情報、結論、両当事者に対する勧告）を送る。そして、レポートに関して事実関係の修正、削除を両当事者に認める。そして、Commissioner の承認を得て最終報告書を両当事者に送る。さらに、両当事者が勧告に関して改善を行っているか事後審査を行う。

FIPPA、MFIPPA の申立に対しては、IPC は一部の場合を除いて法的拘束力を持つ命令を発することができない（PHIPA の場合は、法的拘束力を持つ命令を発することができる）。

IPC は、調査段階で最終報告又は命令までいったケースについて、通常実名で公表を行っている。これは、連邦の Privacy Commissioner（OPC）に比べて特徴的であり、そして IPC の法執行力をより影響力のあるものとしている。OPC にはこれは認められていない。このように被申立者を和解に応じることを促すことを促進する上で、名前を公表することは、かなりの効果があるという評価を学者等からも受けている[9]。

☆ Personal Health Information Protection Act（PHIPA）の法執行

上記の二法とほぼ同様であるが、PHIPA に関しては IPC は法的拘束力を持つ命令を発することができる。この命令に違反すると、IPC は裁判所へ行きその執行を請求することができるが、現在までに命令違反で裁判所までいった例は見られないという。

9　トロント大学教授 Lisa Austin に対するインタビュー調査より（2011 年 3 月 15 日）

（2）苦情処理・紛争解決（体制、しくみ、件数等）、権利行使（罰則・命令・勧告・立ち入り検査の件数等）

① Office of the Privacy Commissioner of Canada（OPC）

（a）Privacy Act（公的部門）

前述にあるが、Commissioner の Findings は、命令ではないので、法的拘束力を持たない。Findings を受けた後、申立者によって連邦裁判所に訴訟を起こす場合はあるが、基本的に OPC は命令をすることができない。さらに、基本的には（特別に事案の公共性が高いなどで、被申立者である機関の名前を公表することはあるが）具体的な被申立者の名前を明らかにしない。

2009 年 4 月 1 日～ 2010 年 3 月 31 日の期間で、公的部門のプライバシーに関する問い合わせ・苦情は全部で 2,572 件であった。そしてそのうち、不服申立として認められたのものが、665 件となる。以下に不服申立として認められた事案内容の内訳は以下となる。

不服申立の種類	件数	合計
開示請求	239	開示請求 251
訂正	10	
手数料	2	
時間制限	264	時間制限 292
時間制限の延長	28	
収集	17	プライバシー 122
利用、公開	98	
保有、破棄	7	
合計	665	665

表 1　公的機関に対する不服申立の種類（2009 年）[10]

この期間に Commissioner が調査の結果の不服申立に対する判断（Findings）を明らかにした件数は、1,154 件であった。

不服申立に対する判断結果と申立の種類に関して、以下にデータを掲載する。

---

10 前掲 5

不服申立の種類					その他		合計
		Well-Founded 不服申立認容	Not-Well Founded 政府側が判断支持された	Resolved	調査の過程での解決又は和解	打ち切り	
ACCESS	Access 開示請求	64	263	27	90	86	530
	Correction/notation 訂正	0	5	1	7	3	16
	Fees 手数料	0	0	0	1	0	1
	Language 言葉使い	0	1	0	1	0	2
Time Limits	Time Limits 時間制限	253	15	0	13	13	294
	Correction/Time Limits 訂正時間	2	0	0	0	0	2
	Extension Notice 時間制限の延長	11	6	0	0	1	18
Privacy	Collection 収集	3	18	1	9	6	37
	Retention and Disposal 保有・破棄	4	4	2	2	2	14
	Use and Disclosure 利用・公開	119	39	6	38	38	240
合計		456	351	37	161	149	1154

表 2　公的機関に対する不服申立に対する判断結果と申立の種類（2009 年）[11]

（b）PIPEDA

前述にもあるが、公的部門と同様 Commissioner の判断（Findings）は、命令ではないので、法的拘束力を持たない。調査の結果 Recommendation を受けた後、申立者によっては連邦裁判所に訴訟を起こす場合はあるが、基本的に法的拘束力をもった命令ではない。さらに、公的部門と同様に基本的には具体的な被申立者の名前を明らかにしない。

2009 年度は、問い合わせ・苦情は、PIPEDA 部門で 2,538 件であった。そのうち、申立と認められて、調査段階に入ったのが、231 件であった。

以下に、PIPEDA 部門のどのような種類の申立が多いのかを表にした（2009 年度）。

11 前掲 5

	件数
開示請求	64
利用・公開	59
収集	33
本人の同意	22
セキュリティ	21
説明責任	10
明確性	10
個人情報保護ポリシー	9
保有期間	4
時間制限	3
法令順守	3
訂正	2
手数料	1
その他	0
合計	231

表 1　公的機関に対する不服申立の種類（2009 年）[10]

一番申立が多かったのは、アクセスである。アクセスというのは、主に情報の開示請求（request）に民間機関が応じなかった、または十分な情報を提供しなかったというものである。特に 2009 年度は、保険部門においてアクセスに関する申立が多く見られた。いくつかのケースは、弁護士が個人の代理で申立を起こしているものであった。次に多かったのが、利用・公開である。これは、民間機関の個人情報の目的外利用、第三者への無断公開である。

申立が調査段階を経て、Findings として出された件数は、587 件であった。Findings の種類別、また業界別の件数について、以下に記載する。

12 Annual Report to Parliament 2009: Report on the Personal Information Protection and Electronic Documents Act, Office of Privacy Commissioner of Canada

	打ち切り	早期解決	管轄外	申立認められず	レポートなし	解決	和解	申立認容	申立認容、解決	合計
金融	17	31	8	30	0	12	14	5	26	143
保険	27	9	2	32	3	5	5	4	7	95
販売	42	9	6	10	0	6	6	5	6	91
通信	8	15	2	15	1	6	6	3	1	91
交通	6	2	7	15	1	6	6	3	1	63
接客（保育所、美容室など）	5	1	4	12	0	1	1	8	3	38
その他	3	5	2	4	0	6	6	4	7	34
会計士、弁護士など	5	1	1	7	0	3	3	7	2	27
医療	1	2	2	14	0	0	0	1	1	19
サービス	4	1	1	3	0	6	6	3	0	19
環境	0	0	0	1	0	3	3	1	0	5
レンタル	0	0	0	0	0	0	0	0	1	1
合計	118	76	35	142	4	55	55	45	61	587

表 4　判断（Findings）の種類、業界別件数（2009 年）[13]

② Information and Privacy Commissioner of Ontario（IPC）

（a）FIPPA、MFIPPA（公的機関）

オンタリオ州の公的機関は、情報開示請求について（一般的事項と個人情報に関する開示請求の 2 種類がある）そのリクエストの件数と応じた件数を報告する義務がある。

個人情報に関する開示請求は、2009 年度は 14,678 件である。そのうち市や町などの公的官（Municipal）は、10,895 件、州レベルの公的機関（Provincial）は、3,783 件である。開示請求とその対応について、公的機関は IPC に対して報告の義務があり、IPC では全ての開示請求に対して、請求された公的機関の応対率（response rate）を公的機関の実名で全て公開をしている。

開示請求がなされても公的機関が応対せず、または請求者が満足しない場合は、IPC に対して申立をすることができる。

IPC が 2009 年度に受け付けた申立は、個人情報の開示請求について 353 件、プライバシーに関して 264 件であった。

また、2009 年に終了した個人情報の開示に対する申立は、329 件であり、以下の表の通りである。最終的な決定が出される前に、仲裁（mediation）の段階で解決されるものが多い。

13 前掲 12

全体半分ほどが仲裁段階で終了し、さらに全体の４分の１ほどが命令段階まで進む。

	Intake 採用段階	Mediation 仲裁段階	Adjudication 命令段階	%	合計
解決	31	151	5	56.9	187
命令 *	1	1	69	21.6	71
取り下げ	21	4	7	9.7	32
申立として 認められない	27	0	0	8.2	27
破棄	5	2	2	2.7	9
調査が 行われず	0	0	3	0.9	3
合計	85(25.83%)	158(48.0%)	86(26.1%)	100%	329

表５　各段階においてケースが終了した件数とその種類[14]

さらに、個人情報の開示請求について調査を経て命令までいったケースにおいては、その判断は以下である。ほとんどの場合申立が認められている。[15]

判断	Provincial Orders	Municipal Orders	合計	%
申立容認	12	18	30	42.3
申立一部容認	12	9	21	29.6
その他	5	5	10	14.1
申立を認めず	5	5	10	14.1
合計	34	37	71	100.0

表６　個人情報の開示請求について調査を経て命令にまで達したケース

次に、プライバシーに関する申立の件数と intake と investigation の段階で、どのような形態でその申立が終了したかについて示す[16]。

14 Access & Privacy A time for Innovation, Information & Privacy Commissioner of Ontario, 2009 Annul Report

15 前掲 14

16 前掲 14

	Intake 採用段階	Investigation 調査	%	合計
解決	168	6	174	76.7
申立として 認められない	25	0	25	11.0
取り下げ	18	1	19	8.4
報告書	0	3	3	1.3
破棄	4	0	4	1.8
命令	0	2	2	0.9
合計	215	12	227	100.9

表 7　プライバシーに関する申立の件数と申立の終了形態

ほとんどのケースが調査段階まで進まず、申立受付後、何らかの形で合意の解決をしている場合が74%ほどとなる。さらに調査に進んでからも当事者同士の間の和解というものがはかられ、最後の命令までたどり着いたのは、プライバシーのケースではわずか２件である。このように、IPC はまずは和解での解決を進めるように努力している。また、調査段階までいくと、その調査の存在は一般に公表され、その中で被申立者名も公表される。そのため、調査段階までいかないよう被申立者側も努力するというのが現状である。

最後に、PHIPA に基づいた申立の現状を記述する。PHIPA の申立は大きく分けて、開示請求（訂正も含む）と収集・利用・公開の二つがあり、申立の 2009 年の合計は 248 件であった。開示請求は、79 件であり全体の 32%、個人からの収集・利用・公開に対する申し立ては、55 件で全体の 22%、さらに医療機関等が自らの情報流出を報告する場合が 101 件と全体の約半数、IPC が独自に調査を行ったものが 13 件で 5%である。

（3）具体的な活動例（行政機関に対する処分例、重大な処分を下した例、裁判例）
連邦法の Privacy Act、PIPEDA に関する処分例などを以下に記述する。

① Privacy Act

2009 年に Privacy Act 部門において調査、判断（Findings）を行った例について数件紹介する [17]。

※ 通常は、OPC は、被申立者の名前を明らかにしない。だが、以下の例は公共性の高さなどをかんがみて明らかにしている）

■ Human Resources and Skills Development Canada が個人の収入情報に関する書類を間違って本人ではない人に送ってしまった例

Human Resources and Skills Development Canada（HRSDC）は、個人の収入に関する書類について、印刷、封筒に封入する段階で複数の個人を取り違え、本人ではない人に収入書類を送ってしまった。44 件の取り違えが報告された。その書類には、名前（配偶者がいる場合は配偶者の名前も）、住所、ソーシャルインシュアランスナンバーが記載されていた。この印刷、封入作業は機械で行われていたが、この機械担当者は、複数枚の書類が 1 つの封筒に間違えて封入されたのを見て、少し機械を調整して、またそのまま作業を続けた。彼は、間違って封入された書類を見つけようとせず、マネージャーにもその報告をしなかった。OPC は、この申立を認容した。

HRSDC は、独自の調査を行い、その書類を封筒に挿入する機械を改善し、さらに品質管理の手順を強化した。このケースでは機械担当者による人的なミスが個人情報を取り違えて配布してしまった大きな原因である。このような人的ミスが個人情報の不正公開において重要な役割を担ってしまったことについて、OPC は HRSDC に対して、職員に個人情報保護に関するセキュリティの重要性を認識させることが必要であると勧告した。HRSDC は、職員の Privacy Act に関する知識を再教育し、その周辺のポリシーや手順について改善をした。

■ Correctional Service Case

The Canadian Association of Elizabeth Fry Societies（女性の権利保護団体）は、この団体に属する女性の代わりに、Correctional Service of Canada（更正保護施設）に対して彼女の個人情報の開示請求を行った。この女性は、The Canadian Association of Elizabeth Fry Societies に対して、彼女の犯罪歴に関する個人情報開示請求の代理を認めていた。

Correctional Service は、60 日以内という期限以内に請求に応じず、2 回目の請求がなされた。はじめの請求がなされてから 123 日後、その女性は監獄で自殺をした。その後、The Canadian Association of Elizabeth Fry Societies は、再度彼女の個人情報の開示を求めたところ、Correctional Service of Canada は、この請求は Privacy Act22 条の適用除外に当てはまり、開示に応じる必要がないとした。本件の場合、OPC の調査では、Correctional Service of Canada に対して 22 条は適用されず、この申立は認容されるという判断を下した。その後も、Correctional Service of Canada は、開示請求に応じず、本件は連邦裁判所で争われた。裁判所は、Correctional Service of Canada には 22 条は適用されないとし、The Canadian Association of Elizabeth Fry Societies の開示請求を認めた。

---

17 前掲 5

② PIPEDA

2009 年度の勧告について、具体的に 2 件の例を示す [18]。

■ Facebook

2009 年、PIPEDA 部門は、Facebook に対する調査を行った。Facebook は、ソーシャルネットワーキングサービスを運営し、アメリカのカリフォルニア州にある民間企業である。カナダ国外の企業に対しても、その企業がカナダ国民に対して現実的に重要なかかわりを持つ場合は、PIPEDA は、適用される。

OPC は、多量の Facebook に対する申立を受けて調査を開始し、複数の個人情報保護に関する問題点を指摘した。一番大きな問題点は、第三者であるゲームやクイズのアプリケーション制作会社が、利用者の個人情報を必要以上に多く共有できていることである。何万とあるアプリケーション制作会社に対して、利用者の個人情報を提供する過程で、Facebook は必要以上の個人情報の共有が行われないような、十分な技術的措置を採っていないとされた。もう一つの問題点は、Facebook から利用者に対して、自己の個人情報がどのように扱われているのかに関して説明が足りないという点である。例えば、個人情報の deactivation（被活性化、個人情報は利用者から見えなくなる、Facebook サーバー上には残る）の場合と deletion（消去、完全にサーバー上からも消される）の区別が利用者にとってわかりにくいことが挙げられる。

調査後、Facebook は、プライバシー保護に関して多くの改善を行うことを約束した。最大のものは、個人情報を取得するアプリケーションを利用する場合、利用者は個人情報のひとつひとつのカテゴリーに対して、その都度どのアプリケーションにどの個人情報が提供されているのか把握することができるようになるという改善である。また、それぞれのアプリケーションの制作者がどのようにその個人情報を利用するかの説明へリンクが張られることとなった。OPC は 1 年ほどでこの技術的な改善措置が行われると期待している。また、Facebook は、利用者へ個人情報がどのように扱われているのか、説明をわかりやすく修正するという約束もした。これらの改善について、Facebook は、現在も対応中であるという報告書を OPC へ送ってきている。

■ Landlord Organization 賃借人の情報を許可なく共有

いわゆる悪い賃借人、賃料の支払いが滞り気味の者のリストをインターネットのサイトでメンバーに公開している賃貸人協会に対して、OPC は調査を行った。メンバーだけに公開をしているとするが、一部についてはインターネット上で誰でもアクセス可能となっていた。申立者は、個人情報が同意なしに、収集、公開されているとした。

OPC は、賃貸人と賃貸人協会が用意していた、賃借人に対する個人情報に関する説明書類が不十分だとした。彼らの個人情報がどのように利用・公開されるかについて、またインターネット上でその情報が公開されるかについてなど、有効な同意を得ていないと OPC は判断をした。協会は、賃借人に

---

18 前掲 12

対して同意を得ることを賃貸人に伝えることを怠っていたとして、協会に会員規約に、賃借人への同意を義務づけること、賃貸契約に個人情報に関する同意項目を加えること、賃借人からの同意が得られるまでは、リストを取り下げることなどを勧告した。その後、この協会は存続しておらず、OPC はフォローアップできていない。

（4）他機関との連携

① OPC

OPC は、オンタリオ州の Privacy Commissioner をはじめ、州レベルの Privacy Commissioner と緊密に連携を取って業務を行っている。OPC によせられる苦情・問い合わせのうち、連邦 Commissioner の管轄ではなく州 Commissioner の管轄である場合が相当数あり、その場合は直接州 Commissioner へケースがまわされる。

② IPC

IPC は、様々な州の機関、市の機関と協力をして個人情報保護、個人情報の開示請求に応じている。上述の通り、命令の段階まで進むどころか調査の段階の前で申立が和解になるという事実の背景には、この協力関係の緊密さがある。個人情報の保護に関して、保護の責務を担うそれぞれの公的機関が、まず開示請求を受けた場合にはその数とその対応を IPC に報告する義務があり、IPC に報告することにより、開示請求に対する対応が常にある程度監視されている状態にある。IPC は、個人情報が何らかの形で侵害される前に事前に公的機関と連携としてそれらを防ぎ、さらに個人情報が侵害された場合は、なるべく和解などで早期解決ができるようつとめている。

4　監督機関の課題等

（1）現在の問題・課題、今後の動き

① OPC

現在、PIPEDA を改正して、情報流出（Data Breach）に関する報告義務を民間企業に義務づけるという法案が議論されている（C-29 bill）。これは、アメリカのカリフォルニア州においてはじめに規定された、企業に情報流出の報告義務を求めるという法律と同様のもので、カナダ版について検討が進められていることになる。この報告が義務づけられればincident（自己付託）で調査を行えるケースが増え、より調査を充実させ、カナダ国民の個人情報保護を手厚く行えるということで、OPC はこれを強く望んでおり、法案が通ることが期待されている[19]。

19 著者の OPC ヒヤリング調査による（2011 年 3 月 14 日）

② IPC

IPC は、情報へのアクセス法も管轄しており、個人情報の開示請求はプライバシー部門で扱っているが、一般の情報開示請求のケースも扱う。2009 年度は、一般的な情報開示請求、個人情報開示請求を合わせて、37,090 件の請求が公的機関に対してなされた。また、PHIPA（医療情報に関する個人情報保護の法律）部門についても多数の請求が行われている。この際問題となるのは、政府機関に対して行う情報開示請求の際にかかる費用がまちまちであることである。2009 年の公的機関（州政府）に対する個人情報の公開請求は、9.47 カナダドルであり、一般情報に関しては 39.66 カナダドルである。特に、PHIPA においては州で統一的に、開示請求の際にかかる費用を規定するべきであり、それがオンタリオ州民の個人情報の開示請求に対する壁を低くするということにつながると、Commissioner Ann Cavoukian は述べており、これらに関する法律の改正が必要とされている。

viii. オーストラリア

1　個人情報保護法制の概要

（1）豪州連邦憲法にはプライバシー権は規定されていないが、豪州が加盟している国際人権規約（B規約）（International Covenant on Civil and Political Rights）第 17 条（「何人も、その私生活、家族、住居若しくは通信に対して恣意的若しくは不法に干渉され又は名誉及び信用を不法に攻撃されない。」）に基づき、豪州国民はプライバシー権を有するとされている。

豪州では、1987 年に連邦政府が National ID Card を導入しようとした際、国民のプライバシー保護に懸念が生じたことを直接の契機として、1988 年、連邦プライバシー法（Privacy Act 1988: Act No. 119 of 1988 as amended）が成立した。

National ID Card 制度は国民の多数の反対により導入されなかった。これは、豪州はもともと犯罪者収容地であったが、なかには無実の者もおり、また不当に重罪を課せられた者もいたことから、歴史的に豪州国民は反権力指向が根強いことが背景にあるようである。

連邦プライバシー法第 6 条に定める様々な定義条項のなかには、“privacy” の定義条項は存在しないものの、“personal information”、“sensitive information”、“health information” 等の定義条項が存在している。

連邦プライバシー法は成立当初、公的部門のみを対象とする法律であったため、連邦プライバシー法第 3 章第 2 節（第 14 条乃至第 16 条）に定められている Information Privacy Principles（以下「IPPs」という）は agencies（公的部門）のみを対象とするものとして規定されている。

しかしながら、その後、連邦プライバシー法について、民間部門における個人情報の取扱いも規制対象とする法改正がなされ、2001 年 12 月 1 日からは、organizations（民間部門）を対象とする個人情報保護原則である National Privacy Principles（以下「NPPs」という）が、法の第 3 附則（Schedule3）に設けられている。

（2）2010 年 5 月、豪州連邦議会において The Australian Information Commissioner Act 2010（以下「AIC 法」という）及び Freedom of Information Amendment（Reform ）Act 2010 が成立し、これにより連邦プライバシーコミッショナーの上位機関として Information Commissioner が新設されることとなり、2010 年 11 月 1 日から The Australian Information Commissioner（連邦情報コミッショナー）及び The Office of Australian Information Commissioner（OAIC 連邦情報コミッショナー事務局）が設置されている。Information Commissioner という制度は、英国、カナダ、アイルランドをモデルにしたものであるが、このような統合的体制を採用することにより、業務の効率性とコスト削減をも図っている。その際、情報公開を執務する Freedom of Information Commissioner も新設されている。

これにより現行の連邦情報コミッショナー事務局は次のような体制となっている。

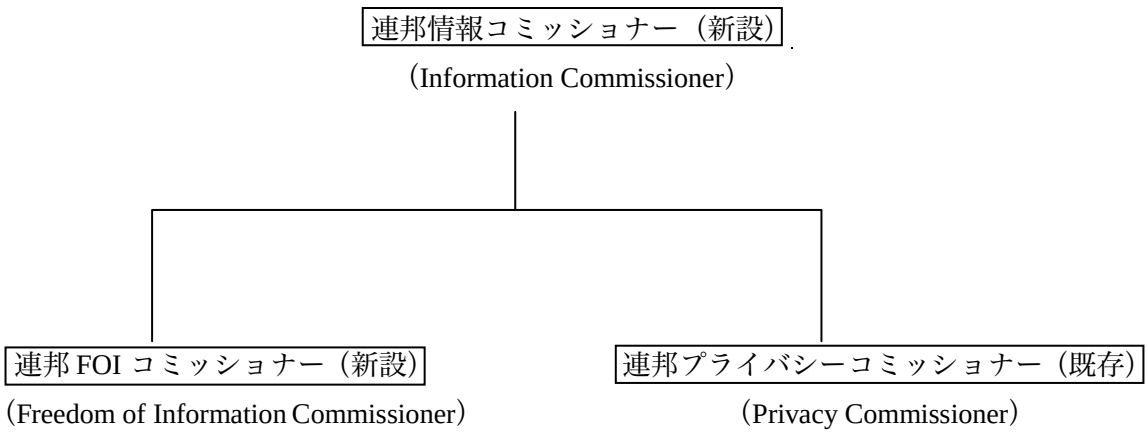

図 1　連邦情報コミッショナー事務局の体制

・連邦情報コミッショナーは、連邦 FOI コミッショナー及び連邦プライバシーコミッショナーの上位機関である（AIC 法第 4 条）。
・連邦情報コミッショナーは、連邦政府による情報管理について戦略的役割を担う（AIC 法第 4 条）（連邦情報コミッショナーの権限は後述する）。
・連邦 FOI コミッショナーは、Freedom of Information Act（1982 年）に基づき、豪州国民の豪州連邦政府に対する情報開示についての役割を担う（AIC 法第 4 条）（連邦 FOI コミッショナーの権限は後述する）。
・連邦プライバシーコミッショナーは、連邦プライバシー法（1988 年）に基づき、個人のプライバシー保護についての役割を担う（AIC 法第 4 条）（連邦プライバシーコミッショナーの権限は後述する）。
・連邦情報コミッショナーのみが連邦情報コミッショナーの役割を遂行することができるが（AIC 法第 4 条）、他方 3 名の連邦コミッショナーは連邦 FOI コミッショナーと連邦プライバシーコミッショナーの役割を遂行することができる（AIC 法第 4 条）。

AIC 法第 9 条によれば、連邦プライバシーコミッショナーは “privacy functions” に関する権限を有することと定められている。“privacy functions” とは、(1) 個人のプライバシーに関する事柄、及び、(2) 1988 年連邦プライバシー法第 4 章第 2 節（Functions of Commissioner：第 27 条乃至第 29 条）、1914 年連邦刑法第 7 章 C 第 5 節、1990 年連邦データマッチング法第 12 条乃至第 14 条及び附則、1953 年国民医療法、1997 年連邦電気通信法第 309 条に定める権限である。

2010 年 5 月に成立した AIC 法に基づき、連邦プライバシー法が 2011 年 3 月に改正され、連邦プライバシー法に規定されている “Commissioner” については、従来の連邦プライバシーコミッショナーではなく、連邦情報コミッショナーを意味することとなった（連邦プライバシー法第 6 条）。そこで、上位機関である連邦情報コミッショナーと連邦プライバシーコミッショナーとの権限関係が問題とな

る。AIC 法第 12 条によれば、連邦プライバシーコミッショナーは privacy functions を有するとはいうものの、連邦プライバシー法に関するガイドラインの起案・公表・改訂、連邦政府への報告書の提出、determination の決定等について、連邦情報コミッショナーの同意を得ることが必要とされている（AIC 法第 12 条第 4 項）。

（3）さらなる連邦プライバシー法改正の動向

① 2008 年 5 月 30 日、The Australian Law Reform Commission（ALRC：豪州法改革委員会）は、連邦プライバシー法を改革するための約 2600 頁に及ぶ「REPORT 108：For Your Information: Australian Privacy Law and Practice」という提言書を、司法大臣に提出した。この提言書には連邦プライバシー法改正に関する 295 個の提言が含まれている。このなかには、例えば、“personal information” の定義を、現状の “information or an opinion（including or an opinion forming part of a database）, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion”（「情報又は意見（データベースの一部を構成する意見を含む）であって、真実であるか否かにかかわらず、又は媒体に記録されているか否かにかかわらず、当該情報又は意見から個人が識別でき、又は合理的につきとめられるもの」）から “information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual”（「情報又は意見であって、真実であるか否かにかかわらず、又は媒体に記録されているか否かにかかわらず、識別でき、又は合理的に識別し得る個人に関するもの」）と改正すべきとする提言も含まれている（Recommendation6-1）。

②これを受けて豪州連邦政府は、連邦プライバシー法改正作業を 2 つのステージに分けて着手することを決定した。

第 1 ステージは、豪州法改革委員会が連邦プライバシー法改正案として提言する 295 個の提言のうち、197 個の提言に関する対応として、以下の改正作業を行おうとするものである。

・2 つの Privacy Principles（IPP 及び NPP）を 1 つの Privacy Principle に統合
・連邦プライバシー法全体の再構成
・プライバシーに対する新技術による影響についての規定
・連邦プライバシーコミッショナーの権限の強化と明確化
・Credit reporting に関する保護の強化
・医療情報及び遺伝情報の保護の強化、公共利益の調査を促進するための個人情報の利用

第 2 ステージは、豪州法改革委員会が連邦プライバシー法改正案として提言する 295 個の提言のうち（第 1 ステージで対応する 197 個を除いた）98 個の提言に対する対応として、以下の改正作業を行おうとするものである。

・連邦プライバシー法に定める適用除外条項の再検討
・重大なプライバシー侵害に対する損害賠償責任条項の導入
・重大なデータ漏洩に関する通知
・児童及びその法定代理人に関するプライバシーについての規定
・1997 年豪州連邦電気通信法に基づく個人情報の取扱い
・各州プライバシー法との調和

③豪州連邦政府は、2009 年 10 月、第 1 ステージに関する対応書を公表した（“Enhancing National Privacy Protection：Australian Government First Stage Response to the Australian Law Reform Commission Report 108”）。これは、197 個の提言のうち 141 個の提言を受け入れるというものである。

④豪州連邦政府は 2010 年 6 月 24 日、統一 Privacy Principles 草案（Exposure Draft of unified Privacy Principle）を公表した。

豪州連邦プライバシー法のなかで最も重要な意味を有するプライバシー原則の変遷は次のとおりである。

(a) もともと連邦プライバシー法（1988 年）は agencies（公的部門）を対象とする法律であったため、連邦プライバシー法第 3 章第 2 節（第 14 条乃至第 16 条）に定められている “Information Privacy Principles”（IPPs）は公的部門を対象とするものとして定められおり、その内容は次のとおりである。

原則 1　個人情報の取得方法及び目的
原則 2　本人からの個人情報の取得
原則 3　個人情報の取得一般
原則 4　個人情報の保有及びセキュリティ
原則 5　記録保持者が保持する情報
原則 6　個人情報が含まれる記録へのアクセス
原則 7　個人情報が含まれる記録の変更
原則 8　利用にあたっての記録保持者による正確性の確認他
原則 9　関連する目的の範囲内における個人情報の利用
原則 10　個人情報の利用制限
原則 11　個人情報の公開制限

(b) 連邦プライバシー法が 2000 年改正により organisations（民間部門）をも適用対象とすることに伴い、連邦プライバシー法の第 3 附則（Schedule3）に、民間部門を対象とする連邦プライバシー原則 “National Privacy Principles”（NPPs）が定められるに至ったがその内容は次のとおりである。

原則 1　取得
原則 2　利用及び公開

原則 3　データ内容の正確性及び最新性
原則 4　データの安全管理
原則 5　公開性
原則 6　アクセス及び訂正
原則 7　識別子
原則 8　匿名性
原則 9　域外へのデータの流通
原則 10　センシティブ情報

(c) 豪州法改革委員会は、2007 年、2 つのプライバシー原則の統合版である統合プライバシー原則案 (Proposed Uniform Privacy Principles、UPPs) を提示した (ALRC Discussion Paper 72: Review of Australian Privacy Law)。
原則 1　匿名性 (Anonymity and Pseudonymity)
原則 2　取得 (Collection)
原則 3　通知 (Specific Notification)
原則 4　公開性 (Openness)
原則 5　利用及び開示 (Use and Disclosure)
原則 6　ダイレクトマーケティング (Direct Marketing) (民間部門のみに適用)
原則 7　データ内容の正確性及び最新性 (Date Quality)
原則 8　データの安全管理 (Data Security)
原則 9　アクセス及び訂正 (Access and Correction) (民間部門のみに適用)
原則 10　識別子 (Identifiers)
原則 11　域外へのデータ移転 (Transborder Data Flows)

(d) 豪州連邦政府は 2010 年 6 月 24 日、統一プライバシー原則の公開草案 (Exposure Draft : Australian Privacy Principles) を公表し、その内容は以下のとおりであるが、必ずしも豪州法改革委員会による上記 2007 年 UPPs 提案には沿っていない。

Part A-Australian Privacy Principles

Division I-Introduction

Division 2-Consideration of personal information privacy

2　Australian Privacy Principle I-open and transparent management of personal information
3　Australian Privacy Principle 2-anonymity and pseudonymity

Division 3-Collection of personal information

4　Australian Privacy Principle 3-collection of solicited personal information
5　Australian Privacy Principle 4-receiving unsolicited personal information
6　Australian Privacy Principle 5-notification of the collection of personal information

Division 4-Dealing with personal information

7 Australian Privacy Principle 6-use or disclosure of personal information

8 Australian Privacy Principle 7-direct marketing

9 Australian Privacy Principle 8-eross-border disclosure of personal information

10 Australian Privacy Principle 9-adoption, use or disclosure of government related identifiers

Division 5-Integrity of personal information

11 Australian Privacy Principle 10-quality of personal information

12 Australian Privacy Principle 11-security of personal information

Division 6-Access to, and correction of, personal information

13 Australian Privacy Principle 12-access to personal information

14 Australian Privacy Principle 13-correction of personal information

Part B-Other relevant provisions

15 Definitions

16 Meaning of agency

17 Meaning of organisation

18 References to the Australian Privacy Principles

19 Extra-territorial operation of this Act etc

20 Acts and practices of overseas recipients of personal information

21 Commissioner may make rules relating to certain matters

22 Regulations

⑤近年中に公表される予定の改正連邦プライバシー法公開草案は、

Ⅰ Privacy Principles, Ⅱ Credit Reporting, Ⅲ Health Information（医療情報）, Ⅳ連邦情報コミッショナーの機能と権限、の４つの章を中心に構成される予定である[1]。

1 Department of the Prime Minister and Cabinet（内閣府、キャンベラ）における平成 23 年 3 月 21 日付インタビューによる。

2　監督機関の制度概要

（1）連邦情報コミッショナー事務局

①コミッショナー体制

既述のとおり、2010 年 5 月に AIC 法が成立したことに伴い、2010 年 11 月 1 日から次のような体制となっている。Compliance 部、Policy 部、Operation 部は、各コミッショナーから指示を受けて業務を遂行する体制となっている。

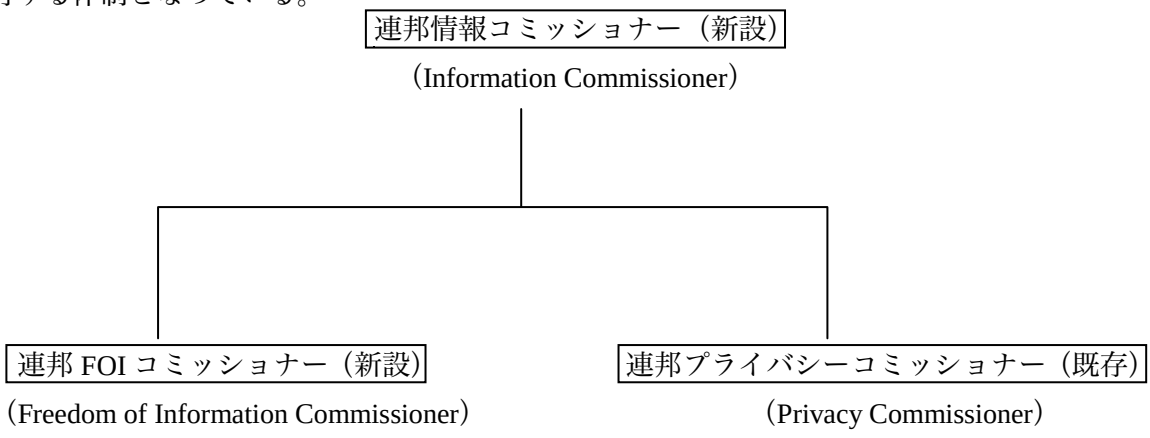

図 2　連邦情報コミッショナー事務局の各コミッショナー及び各部の関係

②3 名の各コミッショナーの関係と役割

既述のとおりである。

③任命と任期

3 名の各コミッショナーの任命権者は、Governor-General（豪州総督）である（AIC 法第 14 条)。うち FOI コミッショナーについてのみ、資格要件として、大学で法律の学位を得たことが必要である(AIC 法第 14 条)。3 名の各コミッショナーの任期は 5 年以内である（AIC 法第 15 条)。

④報酬

3 名の各コミッショナーの報酬は、Remuneration Tribunal Act 1973 に基づき，Remuneration Tribunal (豪州連邦政府の重要な公務員の報酬を決定する独立行政機関) が決定する (AIC 法第 17 条)。

⑤職員

連邦情報コミッショナー事務局に勤務する職員は、Public Service Act 1999 に従って職務に従事する（AIC 法第 23 条)。

⑥権限委託

3名の各コミッショナーは連邦情報コミッショナー事務局の職員に対して権限を委託することができる。但し、次に定める権限を委託することはできない（AIC法第25条)。

・内閣への報告
・年次報告の作成
・ガイドラインの公表
・Freedom of Information 法第55条H・第55条K・第55条Q・第73条・第86条・第89条・第89条A・第89条Kに定める権限
・ガイドラインの公表（連邦プライバシー法第17条）
・Determinationを下す権限（連邦プライバシー法第52条）

⑦年次報告

情報コミッショナーは、年次報告を内閣に提出しなければならない（AIC法第23条)。

⑧体制と人員

(a)2010年10月当時における連邦プライバシーコミッショナー事務局の体制は次のとおりであった[2]。

・職員合計60名（女性38名、男性22名）
・管理職5名（Commissioner 1名、Deputy Commissioner 1名、Assistant Commissioner 1名、Executive Assistant 2名）
・Compliance部30名（Director 2名、Deputy Director 4名、Compliance Officer 15名、Assistant Compliance Officer 4名、Enquiries Officer 4名、Administrative Assitant 1名）
・Policy部16名（Director 1名、Deputy Director 4名、Policy Officer 10名、Administrative Assistant 1名）
・Corporate and Public Affairs 8名（Director 1名、Deputy Director 2名、Corporate and Public Affairs Officer 3名、Corporate and Public Affairs Officer 2名）

(b) 2011年現在における連邦情報コミッショナー事務局の体制は次のとおりである[2]。

・職員合計77名
・管理職9名（Commissioner 3名 , Assistant Commissioner 3名 , Executive Assistant 3名）
・Compliance部36名（Director 6名、Deputy Director 7名、その他職員23名）
・Policy部20名（Director 3名、Deputy Director 4名、Administration Assistant 1名 , Policy Adviser 12名）
・Operations部12名（Director 2名、Deputy Director 3名、Office Manager 1名、Corporate and Public Affairs Officer 1名、Corporate Affairs Officer 2名、Training Manager 1名、その他2名）

---

2 The Office of Australian Information Commissioner（OAIC 連邦情報コミッショナー事務局、シドニー）における平成23年3月23日付インタビューの際に受領した資料による。

（2）権限

① 連邦プライバシー法

前述の通り、2011 年 3 月における連邦プライバシー法の改正により、連邦プライバシー法における “Commissioner” とは従来の連邦プライバシーコミッショナーに代わり連邦情報コミッショナーを意味することとなった。

連邦プライバシー法第 4 章 “Functions of the Information Commissioner” のうち、第 27 条乃至第 28A 条には連邦情報コミッショナーが有する多数の機能が列挙されており、重要な機能として、苦情処理、連邦プライバシー法違反に対する調査、公的機関及び民間部門の法令遵守を確認するための監査の実施、連邦プライバシー法に関する事項について公的機関及び民間部門に対する助言の提供等が定められている。

同法第 5 章 “Investigations”（第 36 条乃至第 70 条 B）には、プライバシー侵害に関する相談や苦情申立（Complaints）が持ち込まれたときの Preliminary inquiries（予備的調査、第 42 条）、Investigations（第 40 条、第 43 条）に加え、自主調査権限（own motion investigations：第 40 条第 2 項）等の対応方法等が規定され（第 1 節）、一定の法的判断である Determination について規定し（第 2 節）、Enforcement（第 3 節）について規定している。

Determination とは、コミッショナーにおいて相手方（respondent）が申立人（complainant）のプライバシーを侵害しており相手方は当該侵害行為を再び行ってはならない等の宣言（declaration）を出すこと（その宣言には、個人情報の訂正指令等を含む。第 52 条第 3 項）、又は、苦情申立を decline（拒絶）する判断を言う（第 52 条第 1 項）。

一方、Enforcement に関する諸規定をみると、相手方（respondent）は当該 determination に従わなければならないという遵守規定が設けられているものの（第 55 条）、determination には法的拘束力がないから（第 52 条第 1 項 B）、determination を法的に強制的に履行させるためには、申立人（complainant）又はコミッショナーが、連邦裁判所において法的手続を開始しなければならない（第 55 条 A）。連邦裁判所は、Interim injunction（暫定的差止命令）を発することも可能である（第 55 条 A）。

連邦プライバシー法第 6 章（第 71 条乃至第 80 条 E）“Public interest determinations and temporary public interest determinations” においても determination を規定しているから、連邦プライバシー法全 101 条のうち、第 27 条乃至第 80 条 E が連邦情報コミッショナーの機能・権限・判断等に関する規定で占められている。

② AIC 法

2010 年 5 月に成立した Australian Information Commissioner 法（AIC 法）においても、3 名の各コミッショナーの機能と権限が定められている。即ち、連邦情報コミッショナーは情報開示及びプライバシー保護に関する機能を有する（AIC 法第 7 条第 10 条）。連邦 FOI コミッショナーは、Freedom of Information Act（1982 年）に基づき、豪州国民の豪州連邦政府に対する情報開示についての役割

を担い（AIC 法第 4 条)、連邦プライバシーコミッショナーは連邦プライバシー法（1988 年）に基づき個人のプライバシー保護についての役割を担う(AIC 法第 4 条)とされているが､連邦 FOI コミッショナーと連邦プライバシーコミッショナーは、情報開示機能とプライバシー機能を共有する（AIC 法第 11 条第 2 項及び第 12 条第 2 項)。

AIC 法には、各コミッショナーの基本的な機能、任命、報酬、事務局のスタッフ等に関する諸規定が定められているのみであり、各コミッショナーの権限に関する enforcement に関する規定はない。

③改正提言

したがって、プライバシー保護のための連邦情報コミッショナー及び連邦プライバシーコミッショナーの権限の強化に関する問題は、連邦プライバシー法の改正内容に係ることとなる。

豪州法改革委員会による連邦プライバシー法改正提言である 2008 年 5 月付提言書（“REPORT 108：For Your Information: Australian Privacy Law and Practice”）には連邦プライバシーコミッショナー権限の強化と明確化に向けた関連提案が多数に上っているが、それらのうち、連邦プライバシーコミッショナー権限の強化と明確化に向けた直接的提案は、“Part F-Office of the Privacy Commissioner”(pp.1513-1554)に掲載されている合計 31 の提案であり(Recommendation 46-1 〜5、47-1~8、48、49-1~13、50-1~4)、例えば次のような提案がなされている[3]。

・連邦情報コミッショナーが作成して公表するガイドラインは、法的拘束力をもたせるべく、“guidelines” という用語ではなく “rules” という用語を使用すべきである（Recommendation 47-2)。
・公的部門が個人情報に重大な影響を与える新規プロジェクトを実施する場合、連邦情報コミッショナーは、当該公的部門に対し、プライバシー影響評価（PIA）を実施するよう指示することができるようにすべきである（Recommendation47-4)。
・連邦情報コミッショナーは、豪州プライバシー影響評価ガイド（2006 年）を、民間部門がより利用しやすくするために改訂すべきである（Recommendation 47-5)。
・民間部門が保有している個人情報記録における Privacy Principle その他の法令への適合性を確認すべく、当該個人情報記録に対する Privacy Performance Assessments（プライバシー実施評価）を実施することができる権限を連邦情報コミッショナーに付与するべきである（Recommendation 47-6)。

3　なお、2008 年 5 月付提言書（“REPORT 108：For Your Information: Australian Privacy Law and Practice”）が公表された時点では 2010 年 AIC 法が成立していなかったことから、同提言書では「連邦プライバシーコミッショナー」という用語が使用されているが、2010 年 AIC 法が成立した影響により、連邦プライバシー法における “Commissioner” とは連邦情報コミッショナーを意味することとなったことから（2011 年 3 月改正連邦プライバシー法第 6 条)、2008 年 5 月付提言書における主体を以下では「連

邦情報コミッショナー」と表現している。

・連邦情報コミッショナーの権限行使の効率化を図るべく、苦情申立が外部の紛争解決制度によって取り扱われているか、又は、連邦情報コミッショナーが外部の紛争解決制度によって当該苦情申立を解決することが適当であると判断した場合は、当該苦情申立を decline（拒絶）する権限を付与すべきである（Recommendation49-2)。

・現行の連邦プライバシー法に記載されている連邦情報コミッショナーの権限は不明確であるから、これを明確化して定めるべきである（Recommendation 49-4)。

・現行の連邦プライバシー法に記載されている conciliation（調停）手続は不明確であるから、これを明確化して定めるべきである。例えば､conciliation（調停）が不調となったとき､連邦情報コミッショナーに、determination を行う権限、苦情申立を拒絶する権限、investigation をさらに実施する権限等を付与すべきである（Recommendation 49-5)。

・連邦情報コミッショナーに、苦情申立ての相手方に対する preliminary inquiries（予備的調査）に加え､第三者に対する preliminary inquiries を実施する権限を付与するべきである（Recommendation 49-10)。

・現行の連邦プライバシー法 42 条は、連邦情報コミッショナーが正式な自主的調査権限（own motion investigation）を実施する前に、予備的調査をすることを許容すべく改正されるべきである（Recommendation49-10)。

・連邦情報コミッショナーが、連邦裁判所に、必要な文書若しくは情報を保有している個人に対して当該文書若しくは情報を提出することを命令することを要求する権限、又は、必要な会議に出席することを命令することを要求する権限を付与すべきである（Recommendation 49-11)。

・苦情処理をする過程において、連邦情報コミッショナーが、苦情申立人でない個人に関する個人情報を取得することを許容すべきである（Recommendation 49-12)。

・連邦情報コミッショナーが公的部門若しくは民間部門がプライバシー侵害をしていると判断した場合、当該公的部門若しくは民間部門に対して、連邦プライバシー法を遵守するよう通告を発する権限を付与すべきであり、また、連邦裁判所で当該通告の遵守命令を得ることを申し立てる権限を付与すべきである（Recommendation 50-1)。

・重大若しくは反復されるプライバシー侵害が発生している場合、連邦情報コミッショナーが、連邦裁判所に対し、civil penalty（民事制裁金）を求める権限を付与すべきである（Recommendation 50-2)。

・連邦情報コミッショナーが civil penalty を求める制度が設けられる場合、enforcement guidelines を設けるべきである（Recommendation 50-3)。

なお、本稿執筆時点においては、連邦プライバシー法に関する公開草案のうち、プライバシー原則の公開草案のみが公表されているにとどまり、連邦情報コミッショナーの権限強化に関する公開草案は公表されていない。

3　監督機関の運用実態（2009 年 7 月～ 2010 年 6 月）

連邦プライバシーコミッショナー事務局における 2009 年 7 月から 2010 年 6 月までの運用実態は次のとおりである[4]。

① 相談・申立受付件数

電話相談 20,935 件（1 日あたり 78 件）

郵便、電子メール、ファックスでの相談 1,909 件

苦情申立（Complaints）1,201 件

②自主的調査権限（Own motion investigation）を実施した件数（連邦プライバシー法第 40 条 2 項）

117 件

③ Case notes

連邦プライバシーコミッショナー事務局が取り扱った事件のうち特に重要な 27 の事例を、HP に掲載している。

④講演

連邦プライバシーコミッショナーは，26 件の講演を実施した。

⑤ Policy Advices

連邦プライバシーコミッショナーは、公的機関及び民間部門から助言を求められた際、198 件の助言を提供した。

⑥ Information Sheet の作成と公表

連邦プライバシーコミッショナー事務局は、民間部門や公的機関がプライバシー侵害の結果を招来しないための Information Sheet（個人情報の取り扱いに関する啓蒙的説明文書）を作成して公表している。

民間部門に対し、2010 年、クラブやパブで運転免許証等の個人情報をスキャン等する際に、クラブやパブの事業者が遵守すべき啓蒙的説明文書を作成して公表し（Information Sheet（private sector）30 号―2010：ID scanning in clubs and pubs)、2009 年には遺伝情報の取り扱いに関する Information

4　Office of the Privacy Commissioner, Australian Government, “The Operation of the Privacy Act Annual Report 1 July 2009-30 June 2010”

Sheet（private sector）29 号 —2009：Use or disclosure of genetic information in the private health sector を作成公表した[5]。

⑦苦情処理【1】電話相談

・電話相談件数 20,935 件
・無料で相談に応じている。
・連邦プライバシーコミッショナー事務局が、当事者間の和解のための会議室等を提供することはない。当事者に対する連絡は、全て電話又は電子メールで行う。
・プライバシーコミッショナー事務局が、和解契約書案を提供することはなく、加害企業側が和解契約書案を被害者に提供することが殆どであるということである。

個人	17,667 件
Health service providers	391 件
連邦政府	382 件
法律事務所・会計事務所等	253 件
不動産業	224 件
州政府	178 件
金融	151 件
公益団体	123 件
小売	75 件

表 1　電話相談者の内訳

5　連邦プライバシーコミッショナーは、2009 年 7 月～ 2010 年 6 月期以前にも、多くの啓蒙的説明文書を作成公表している。
2009 年（7 月以前には）、Information Sheet（private sector）28 号—2009：NPP3 Date Quality を作成・公表した。
また 2008 年には、Information Sheet（private sector）27 号 —2008：A step-by-step guide to internal investigations of privacy complaints by organisations（企業におけるプライバシーに関する苦情の内部調査のためのガイド）、Information Sheet（private sector）26 号—2008：Interaction between the Privacy Act and the Spam Act（連邦プライバシー法及び SPAM 法の関係）、Information Sheet（private sector）25 号—2008：Sharing health information to provide a health service（医療サービスのための医療情報共有）、Information Sheet（private sector）24 号—2008：Disclosure of health information and impaired capacity（医療情報の開示と医療資格の喪失）、Information Sheet（private sector）23 号—2008：Use and disclosure of health information for management, funding and monitoring of a health service（医療サービスの経営、資金調達及びモニタリングのための医療情報の利用及び開示）、Information Sheet（private sector）22 号—2008：Fees for access to health information under the Privacy Act（連邦プライバシー法における医療情報へのアクセスのための手数料）、Information Sheet（private sector）21 号—2008：Denial of access to health information due to a serious threat to life or health（生命又は身体への深刻な危険を理由とした医療情報へのアクセスの拒否）を作成公表した。
2007 年には、Information Sheet（private sector）20 号—2007：Scanning ‘Proof of Identity’ Documents（スキャンによる「同一性証明」のための文書）、Information Sheet（private sector）19 号—2007：The Prescription Shopping Information Service（PSIS）and The Privacy Act（処方箋購入情報サービスと連邦プライバシー法）を作成公表した。）

電話相談の内容

(a) 民間部門に関するもの

取得（NPP1 条）	1,427 件
利用と開示（NPP2 条）	2,670 件
データ内容の正確性及び最新性（NPP3 条）	268 件
データの安全管理（NPP4 条）	732 件
公開性（NPP5 条）	130 件
アクセス及び訂正（NPP6 条）	1,301 件
識別子（NPP7 条）	8 件
匿名性（NPP8 条）	35 件
域外へのデータ移転（NPP9 条）	135 件
センシティブ情報（NPP10 条）	1,692 件
適用除外条項	1,102 件
一般的問い合わせ	75 件
合計	9,510 件

表 2　民間部門の電話相談の内容

(b) それ以外に関るもの

Credit Reporting	862 件
Surveillance	376 件
Data-matching	21 件
IPPs	731 件
Spent Convictions	115 件
納税申告番号	105 件
プライバシー一般	2,281 件
マネーロンダリング	12 件
Do not call register	74 件
合計	4,577 件

表 3　それ以外の電話相談の内容

(c) プライバシーに関連性のないもの 6,848 件

⑧ 苦情処理【2】電子メール，郵便，ファックスによる相談

・相談件数は、1,909 件。

・うち、71％は、NPP（民間部門に適用される個人情報保護原則）に関するもの。

⑨苦情処理【3】書面による苦情申立（Complaints）

・書面による苦情申立受理件数は、1,201 件

・内容に関する内訳は次のとおりである。

NPP に関するもの	53％
Credit Reporting に関するもの	19％
IPP に関するもの	11％
納税申告番号[6] に関するもの	0.4％

表 4　書面による苦情申立ての内容

・争点別の内訳は次のとおりである。

NPP 原則に定める利用又は開示	28.1％
Credit Reporting	22.7％
IPP 原則	18.1％
NPP 原則に定める取得	15.1％
NPP 原則に定めるデータ安全管理	12.7％
NPP 原則に定めるアクセス及び訂正	11.3％
NPP 原則に定めるデータ内容の正確性及び最新性	9.6％
その他の NPP 原則	0.9％
納税申告番号[6]	0.5％

表 5　書面による苦情申立ての争点

6　豪州国民であるか外国人であるかを問わず、豪州で労働する人々は Tax File Number（TFN）を取得する必要があり、更に労働開始時に企業にこの番号を報告する必要がある。Tax File Number（TFN）を有していないと、給与に対する源泉徴収ができないうえ、給与に対して約 50%の課税がされてしまう。

・苦情を申し立てられた業界は次のとおりである。

金融	210 件
クレジット・債権回収・賃借人データベース	152 件
連邦政府	147 件
医療健康業	108 件
電気通信事業	95 件
小売業	51 件
個人事業者	45 件
州政府	38 件
保険	31 件

表 6　書面による苦情申立ての相手方業界

・苦情申立を受けた後の処理手続の概要は次のとおりである。

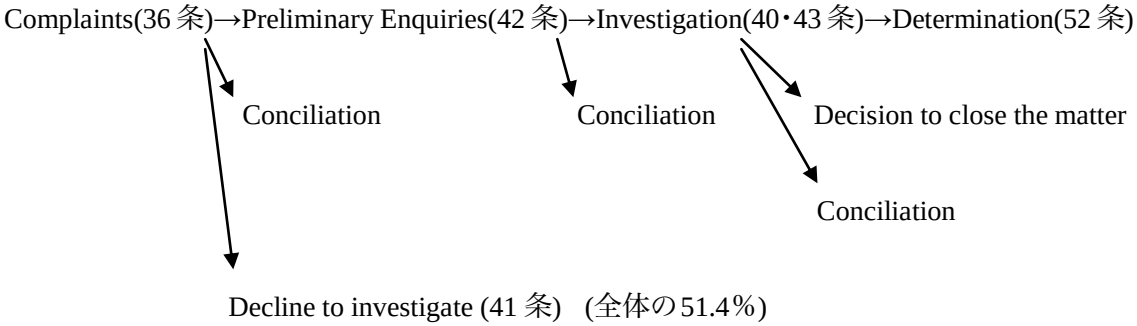

図 3　苦情申立後の処理手続

・連邦プライバシーコミッショナーが自主的調査権限を行使する場合もある。(own motion investigation 第 40 条第 2 項)
・苦情申立を受理後、12 ヶ月以内に終結させることを目標としているが、平均的には 6 ヶ月で終結させている。
・苦情申立を終了させた段階は次のとおりである。

Investigation の段階で終結したもの	15.4%
Preliminary Enquiries（予備的調査）の段階で終結したもの	33.2%
Decline to investigate として終結したもの	51.4%

表 7　苦情申立の終了段階

・ほとんどの Complaints は determination まで行くことはない。Determination（決定）について、連邦プライバシーコミッショナーは、①苦情申立を拒絶する Determination（決定)、又は②苦情申立に理由があることを認めて相手方（respondent）に対して連邦プライバシー法違反を停止し損害

賠償を支払うよう求めるDeterminationを発することができる（連邦プライバシー法第52条1項）。但し、このDeterminationは相手方に対して法的拘束力がないから（同法第52条1B項）、このdeterminationを法的に執行する（enforce）ためには、コミッショナー又は申立人が、連邦地方裁判所に、determinationを執行するための法的手続を開始しなければならない（同法第55条）。

連邦プライバシー法が施行された1989年以降、1993年に2つ、2003年に1つ、2004年に5つ、合計8つのdeterminationが出されているのみである[7]。

・苦情申立受理後、Investigationを経て当事者間に十分な協議がなされた結果の救済として、NPP原則に関連したものをみると、次のように分類されている。

個人情報記録の修正	9件
謝罪の書簡を送付する	24件
手続を変更したという書簡を送付する	10件
情報開示	23件
スタッフの教育	8件
他の救済	9件
損害賠償（AUD1000まで）	6件
損害賠償（AUD1001-5000）	7件
損害賠償（AUD5001-10000）	1件
損害賠償（AUD10001以上）	0件

表8　NPP原則に関する救済

⑩収支報告（2009年7月～2010年6月）

収入の部	
政府からの歳入	AUD6,470,000
商品販売，サービス提供	AUD1,130,000
その他の収益	AUD22,000
収入合計	AUD7,622,000
支出の部	
人件費	AUD5,272,000
備品費	AUD2,324,000
減価償却費	AUD39,000
支出合計	AUD7,635,000

表9　連邦プライバシーコミッショナー事務局の収支報告（2009年7月～2010年6月）

7　これらの8つの事例は、http://www.privacy.gov.au/materials/types/determinations?sortby=55に掲載されている。

4　New South Wales 州におけるプライバシー監督機関の運用実態（2009 年 7 月～ 2010 年 6 月）

①電話及び電子メールでの苦情受付

合計 1,227 件（内訳 電話 1,032 件、電子メール 190 件）

②書面による苦情申立（complaints）の相手方

州政府	41 件
民間部門	15 件
個人	8 件
市政府	1 件

表 10　NSW 州プライバシーコミッショナーにおける書面における苦情申立ての相手方

③プライバシーに関する助言の提供

開示に関するもの	41 件
アクセスに関するものもの	23 件
取得に関するもの	22 件
プライバシー原則に関する	17 件
利用	10 件

表 11　NSW 州プライバシーコミッショナーにおけるプライバシーに関する助言の内容

④連邦プライバシーコミッショナー事務局との管轄に関する問題

例えば、New South Wales 州民が、同州内の民間企業により自己のプライバシーが侵害されたことを理由として苦情を申し立てる場合、当該州民は、連邦情報コミッショナー事務局と NSW 州プライバシーコミッショナー事務局のいずれに苦情を申し立てるべきであるかが問題となる。

この管轄に関する規定は設けられておらず、NSW 州民は、いずれの事務局にも苦情を申し立てることができるとのことである[8]。

8　Office of the NSW Privacy Commissioner 事務局（シドニー）における平成 23 年 3 月 23 日付インタビューによる。

＜参考文献、ヒアリング先＞

・Australian Law Reform Commission “Report 108: For Your Information: Australian Privacy Law and Practice”Volume1-3
・Office of the Privacy Commissioner, “The Operation of the Privacy Act 1 July 2009-30 June 2010”.
・Privacy NSW 2009-2010 Annual Report
・Australian Government “Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108: For Your Information: Australian Privacy Law and Practice”
・Exposure Draft “Australian Privacy Principles”
・ヒアリング先は次のとおりである。内閣府（キャンベラ、平成 23 年 3 月 21 日）、Information Integrity Solutions 社（シドニー、平成 23 年 3 月 22 日）、連邦情報コミッショナー事務局（シドニー、平成 23 年 3 月 23 日）、New South Wales 州プライバシーコミッショナー事務局（シドニー、平成 23 年 3 月 23 日）。

ix 韓国

1　現行の個人情報保護法の体系

韓国においては、公共部門と民間部門に分かれている個人情報保護に関する法律を統合した法律の制定を目指して、2004 年から論議がなされてきた。本年（2011 年）3 月 29 日，ついに「個人情報保護法」(法律第 10465 号) が制定・公布され、2011 年 9 月 30 日から全面施行されることになった。

そこで、本稿では、まず個人情報保護法施行以前である現時点での現行の個人情報保護法制の概略と監督機関について述べた後に、新たに制定され、これから施行される個人情報保護法の主要内容と監督機関について、現時点で分かる範囲内で、紹介することにする。

（1）憲法的根拠

個人情報保護制度の憲法的根拠については、「情報の自己決定権」にあるとされる。憲法裁判所は、その判決で、情報の自己決定権とは、「自身に関する情報が、いつ誰にどの範囲まで知られ、また、利用されるようにするのかを、その情報主体が自ら決定することのできる権利、すなわち情報主体が個人情報の公開と利用に関して自ら決定する権利」（헌재 2005.7.21,2003 헌마 282）と定義している。

このような情報の自己決定権の憲法的根拠については、学説は、憲法 17 条の私生活の秘密と自由に関する条項に置くものと、10 条の人間の尊厳と価値規定に置くもの、両者を含めるものとに大きく分かれている。これに対して、判例の見解は、大法院と憲法裁判所で分かれている。大法院（最高裁判所）は、10 条及び 17 条にその根拠を求めるのに対して（대판 1998.7.24,96 다 42789)、憲法裁判所は、情報の自己決定権は独自的な基本権であり、憲法に明示されない基本権であると解している（헌재 2005.5.26,99 헌마 513,2004 헌마 190(병합))。

（2）法的体系

韓国においては、個人情報保護に関する法律として、まず、1993 年に「公共機関の個人情報保護に関する法律」（以下、公共機関個人情報保護法と称する）が制定され、1995 年 1 月 8 日から施行されている。この法律は、文字通り、公共部門の個人情報のみをその対象としたものである。

一方、民間部門における個人情報保護に関する一般法は、制定されてこなかった。情報通信網（インターネット）上の個人情報保護については、「情報通信網利用促進及び情報保護等に関する法律」（以下、情報通信網法と称する）22 条から 29 条及び「個人情報保護方針」で、信用情報については「信用情報の利用及び保護に関する法律」で規律している。また、「金融実名取引及び秘密保障に関する法律」(4 条 1 項、4 項)、「位置情報の保護及び利用等に関する法律」では、それぞれ当該分野における秘密漏洩禁止や情報の不当な使用禁止を規定している。

現行の韓国における個人情報保護のための立法体系を概観すれば、下の表 1 の通りである。

表１　韓国の個人情報保護立法体系

区分	関連法規	規制内容
公共部門	公共機関の個人情報保護に関する法律	○国・公共機関保有の個人情報保護 ○収集・処理・利用過程上の情報主体と公共機関の権利・義務規律
	公共機関の情報公開に関する法律	○個人情報の非公開、部分公開
	住民登録法	○住民登録の閲覧又は謄・抄本の交付、住民登録電算情報資料の利用等
	統計法	○統計作成過程時の個人、団体法人の秘密保護
	国政監査及び調査に関する法律	○私生活侵害目的の監査、調査の制限
	国家公務員法	○業務上知りえた秘密の保護
通信部門	情報通信網利用促進及び情報保護等に関する法律	○情報通信サービス提供者による個人情報収集、処理規制 ○旅行業、ホテル業、航空運送事業、塾等の事業者の個人情報保護
	通信秘密保護法	○郵便物の検閲、電気通信の盗聴等の通信関連の私生活の保護
	通信制限措置の許可手続及び秘密維持に関する規則	○犯罪捜査・国家安保のための通信制限措置の許可手続
	電気通信事業法	○個別利用者に関する情報の公開及び流用の禁止等
	位置情報の保護及び利用等に関する法律	○位置情報の収集・提供の範囲、誤・濫用の防止
医療部門	保健医療基本法	○保健医療関連の私生活の保護
	医療法、伝染予防法、後天性免疫欠乏症予防法	○業務上秘密漏洩禁止
	生命倫理及び安全に関する法律	○遺伝子情報の保護等
金融部門	信用情報の利用及び保護に関する法律	○民間部門による個人信用情報の処理の規制 ○信用情報主体の閲覧および訂正請求等
	金融実名取引及び秘密保障に関する法律	○金融取引の秘密保障
	証券取引法	○情報の提供、漏洩の禁止
その他	保険業法、弁護士法、外国為替取引法、法務士法、公証人法等	○業務上知りえた秘密の保護

出 処 :http://www.kidi.or.kr/pdf/%EC%97%B0%EA%B5%AC%EC%9E%90%EB%A3%8C/%EC%97%B0%EA%B5%AC%EB%B3%B4%EA%B3%A0%EC%84%9C/080117_2/200.pdf

このように、これまで韓国の個人情報保護法の体系は、おおむね、①公共部門の法律と②民間部門のうちの情報通信部門及び信用部門の主要法律、そして、③その他の個別の法規で構成されていると理解されてきた。

以下、この章においては、現行の個人情報保護法制度、すなわち、①公共部門の一般法である公共機関個人情報保護法と、②事実上、民間部門の一般法的位置を有している情報通信網法 (もっとも、この法律は厳密に言えば民間部門のうちの情報通信分野に限って規律したものにすぎない) が規定する個人情報保護の内容及びその保護機構について、簡単に概観することにする。

2　現行の個人情報保護法制の概観

（1）公共機関個人情報保護法の内容

①個人情報保護の基本原則

公共機関個人情報保護法は、個人情報の基本原則として、ⅰ) 公共機関の長は、個人情報を収集する場合、その目的を明確にしなければならないし、目的に必要な最小限の範囲内で適法かつ正当に収集しなければならず、目的外の用途に活用してはならないこと（3 条の 2 第 1 項)、ⅱ) 公共機関の長は、処理情報の正確性及び最新性を保障して、その保護の安全性を確保しなければならないこと（2 項)、ⅲ) 公共機関の長は、個人情報の収集・活用等、個人情報の取扱いに関する事項を公開しなければならず、個人情報処理において処理情報の閲覧請求権等、情報主体の権利を保障しなければならないこと（4 項）を定めている。

②保護の対象となる個人情報

公共機関個人情報保護法の保護対象となるものは、「公共機関のコンピュータ・閉鎖回路テレビジョン等の情報の処理又は送・受信機能を有する装置により処理される個人情報」（1 条）である。「公共機関」とは、国家行政機関・地方自治団体その他の公共団体のうち大統領令で定めるものをいう。「個人情報」とは、生存する個人に関する情報で、当該情報に含まれている氏名・住民登録番号等の事項により当該個人を識別することのできる情報（当該情報のみでは特定個人を識別できなくても、他の情報と容易に結合して識別することのできるものを含む）をいう（2 条 2 項)。

③個人情報の収集・保有の制限

(a) 個人情報の収集制限

公共機関の長は、思想・信条等、個人の基本的人権を著しく侵害するおそれのある個人情報を収集してはならない。ただし、情報主体の同意があるか、または、他の法律に収集対象個人情報が明示されている場合には、この限りではない（4 条 1 項)。

(b) 個人情報ファイルの保有制限

公共機関は、所管業務を遂行するために必要な範囲内で個人情報ファイルを保有することができる（5 条)。

(c) 事前協議

公共確保の長が、個人情報ファイルを保有しようとする場合（他の公共機関から処理情報を提供されて保有しようとする場合を除く）には、行政安全部長官と協議しなければならない（6条1項）。

(d) 個人情報ファイルの公告

行政安全部長官または関係中央行政機関の長は、事前協議した事項を大統領令の定めるところにより、年1回以上、官報またはインターネットホームページ等に掲載して公告しなければならない（7条）。

(e) 個人情報ファイル台帳の作成

保有機関の長は、当該機関が保有している個人情報ファイル別に所定の事項を記載した台帳を作成して一般人が閲覧できるようにしなければならない（8条）。

(f) 個人情報の安全性確保等

公共機関の長は、個人情報を処理したり個人情報ファイルを「電子政府法」による情報通信網によって送受信する場合、個人情報が紛失・盗難・漏洩・変造または棄損されないよう、安全性確保に必要な措置を講じなければならない（9条、9条の2）。

(g) 閉鎖回路テレビジョンの設置等

公共機関の長は、犯罪予防及び交通取締など公益のために必要な場合、行政手続法の規定による公聴会など、大統領令で定める手続を経て、関係専門家及び利害関係人の意見を収斂した後に、閉鎖回路テレビジョンを設置することができる（4条の2第1項）。

④処理情報の目的外利用及び提供の制限

(a) 処理情報の保有目的外の利用及び提供の禁止

保有機関の長は、他の法律に基づいて、保有機関の内部または保有機関の外部の者に対して利用させたり提供する場合を除いては、当該個人情報ファイルの保有目的以外の目的で処理情報を利用させたり提供してはならない（10条1項）。保有機関から処理情報を提供された者は、保有機関の同意なく当該処理情報を第三者に利用させたり提供してはならない（10条5項）。

ただし、一定の場合には、処理情報の保有目的外の利用及び他の機関への提供も例外的に許される(10条3項)。保有機関の長は、法律が定めた例外規定に基づいて、処理情報を情報主体以外の者に利用させたり提供しようとするときには、処理情報を受領した者に対して、使用目的・使用方法その他必要な事項に対して制限したり処理情報の安全性確保のために必要な措置を講じるよう要請しなければならず、このような要請を受けた情報受領者は処理情報の安全性確保のための措置をとらなければならない（10条4項）。

保有機関から提供された処理情報を利用する機関は、提供機関の同意なしに当該処理情報を他の機関に提供してはならない（10条5項）。個人情報の処理を行う公共機関の職員や公共機関から個人情報の処理業務を委託されて業務に従事する者等は、職務上知り得た個人情報を漏洩し、または権限なく処理するなど、不当な目的のために使用してはならない（11条）。

(b) 提供の制限

保有機関の長は、保有目的にしたがって処理情報を利用または提供する場合であっても、業務遂行に必要な最小限の範囲に、その利用または提供を制限しなければならない (10 条 2 項)。保有機関の長は、公共機関個人情報保護法の規定 (10 条 3 項 2 号～ 5 号、7 号) により保有目的外の目的に利用または提供する場合には、その利用または提供の法的根拠・目的及び範囲などに関して必要な事項を情報主体が容易に確認できるように官報またはインターネットホームページなどに掲載しなければならない (10 条 6 項)。

(c) 個人情報ファイルの破棄

保有機関の長は、他の法律により保存しなければならない場合を除いて、個人情報ファイルの保有目的達成など、当該個人情報ファイルの保有が不必要になったときには、当該個人情報ファイルを、遅滞なく、破棄しなければならない (10 条の 2)。

⑤処理情報の閲覧・訂正・削除等

(a) 情報主体の閲覧請求権

情報主体は、法律で制限された場合を除いて、個人情報ファイル台帳に記載された範囲内において文書で本人に関する処理情報の閲覧を保有機関の長に請求することができる (12 条 1 項)。本人の処理情報を閲覧した情報主体は、保有機関の長に文書でもって当該処理情報の訂正または削除を請求することができる (14 条 1 項)。

(b) 不服請求

閲覧・訂正・削除の請求に対して公共機関の長が行った処分または不作為によって権利または利益が侵害された者は、行政不服申立てまたは行政訴訟を提起することができる（15 条)。

⑥個人情報保護方針の制定・公告

保有機関の長は、一定の事項を盛った個人情報保護方針を定めなければならない (20 条 1 項)。

⑦個人情報管理責任官の指定

公共機関の長は、所管処理情報の保護及び管理のために、個人情報管理責任官を指定しなければならない。その資格要件・指定および運営等に関して必要な事項は、大統領令で定める (20 条の 2)。

（2）情報通信網法の個人情報保護規定

情報通信網法に規定されている個人情報保護義務は、表 2 のとおりである。

情報通信網法が定める、個人情報の収集・利用の同意手続、個人情報破棄義務などの基本原則及び手続的規定は、国際的水準に達している。個人情報保護規定は、OECD の個人情報保護ガイドラインを忠実に反映しており、同意手続の細分化などは、むしろ EU 国家よりも詳細であるともいえよう。しかし、義務違反の事業者に対する制裁手段は脆弱であり、事業者の個人情報保護の認識の強化及び投資を誘引するための制度的装置は不十分であり（技術的・管理的保護措置の未履行に対する制裁は過料 1000 万ウォン)、また、事業者には個人情報を侵害したときに利用者に侵害事実を伝える法的義務がないために、利用者にとっては迅速な被害予防及び権利救済が困難であると指摘されている。

表 2　情報通信網法の個人情報保護内容

区分	主要内容	罰則
個人情報収集	・同意のない個人情報収集 (22 条)	罰則 (5 年以下の懲役又は 5,000 万ウォン以下の罰金及び課徴金)
	・機微な個人情報収集 (23 条)	
	・法定代理人の同意のない児童の個人情報収集 (31 条)	
	・必要最小限の個人情報以外の情報を未提供であるという理由でのサービス提供の拒否 (23 条)	過料 (3,000 万ウォン以下)
	・住民登録番号以外の会員加入方法を未措置 (23 条の 2)	
個人情報利用及び提供	・同意を得た目的と異なる目的で個人情報を利用 (24 条)	罰則 (5 年以下の懲役又は 5,000 万ウォン以下の罰金及び課徴金)
	・利用者の同意のない個人情報の第三者提供 (24 条の 2)	
個人情報取扱委託	・利用者の同意のない個人情報の取扱の委託 (25 条)	罰則 (5 年以下の懲役又は 5,000 万ウォン以下の罰金及び課徴金)
	・個人情報の取扱委託事実の未公開 (25 条)	
営業譲受による個人情報の移転	・営業譲渡等の未通知 (26 条①)	過料 (2,000 万ウォン以下)
	・営業譲受者等が当初の目的と異なる目的で個人情報を利用・第三者提供 (26 条③)	罰則 (5 年以下の懲役又は 5,000 万ウォン以下の罰金及び課徴金)
個人情報の管理	・個人情報管理責任者の未指定 (27 条) ・個人情報取扱方針の未公開 (27 条の 2)	過料 (2,000 万ウォン以下)
	・技術的・管理的措置の未履行 (28 条)	是正措置
	・技術的・管理的措置の未履行による漏洩 (28 条)	罰則 (2 年以下の懲役又は 1,000 万ウォン以下の罰金及び課徴金 (1 億ウォン以下)
	・個人情報取扱者の個人情報棄損・侵害・漏洩 (28 条の 2)	罰則 (5 年以下の懲役又は 5,000 万ウォン以下の罰金)
個人情報の破棄	・個人情報の未破棄 (29 条)	過料 (3,000 万ウォン以下)
利用者の管理	・利用者の同意撤回・閲覧・訂正要求の未措置 (30 条③ , ④)	過料 (3,000 万ウォン以下)
	・個人情報の誤謬訂正要請に対する必要措置を履行する前に個人情報の第三者提供・利用 (30 条⑤)	罰則 (5 年以下の懲役又は 5,000 万ウォン以下の罰金)
	・利用者の同意撤回・閲覧・訂正要求を個人情報の収集方法よりも困難にする (30 条⑥)	過料 (3,000 万ウォン以下)

3　韓国における個人情報保護監督機関

韓国における現行の個人情報保護監督機関の現状は、表３の通りである。

表３　韓国における個人情報保護機構の構成及び運営状況

機関名	構成現況	機関長任命	機関の役割及び根拠法	運営現況
個人情報紛争調停委員会	・委員会 (総 15 人) - ４人の法律家 - ６人の教授 - ３人の関連機関専門家 - ２人の消費者、事業者団体代表 ・事務局	行政安全部長官	民間部門の被害救済（情報通信網法）	・委員会を支援する事務局を韓国インターネット振興院で運営する
放送通信委員会	行政機関 (政府省庁)	大統領	民間の情報通信分野の監督（情報通信網法）	・個人情報保護業務を専門に担当する個人情報保護倫理課がある ・個人情報侵害申告受付、相談などの業務を担当する個人情報 侵害申告センターを、行政安全部、放送通信委員会と共同で運営
公共機関個人情報保護審議委員会	・委員会 (総 10 人) - 委員長１人を含む 10 人の委員で構成 - 委員長 : 行政安全部次官 - 委員 : 国務総理が任命又は委嘱	国務総理	公共部門の審議機構（公共機関個人情報保護法）	・公共部門でコンピュータによって処理される個人情報の保護に関する主要事項の審議
行政安全部	行政機関 (政府省庁)	大統領	公共部門の監督 (公共機関個人情報保護法) と民間部門のうち百貨店・ホテル・旅行社など（情報通信網法）	・個人情報保護業務を担当する部署がある ・公共機関個人情報保護に関する事項を審議する個人情報保護審議委員会運営

出典 : 이창범 / 윤주연『각국의 개인정보피해구제제도 비교연구』2003 년 12 월、개인정보분쟁조정위원회、277 頁を基に一部加筆修正した

ここでは、公共機関個人情報保護法が規定する公共機関個人情報保護審議委員会と、情報通信網法が定める個人情報紛争調停委員会、そして、情報通信網法に基づいて設立された放送通信委員会傘下の特殊法人であり、個人情報侵害申告センターの業務を担当している韓国インターネット振興院（KISA）[1]について説明することにする[2]。

（1）公共機関個人情報保護審議委員会

①公共機関個人条保護審議委員会の概要

公共機関のコンピュータ等によって処理される個人情報の保護に関する事項を審議するために国務総理所属下に公共機関個人情報保護審議委員会を置く (公共機関個人情報保護法 20 条 1 項)。しかし、委員会の構成・運営及び人事・行政上の支援などは、国務総理室ではなく、行政安全部が担当している。

委員会は、①個人情報保護に関する政策及び制度改善に関する事項、②処理情報の利用及び提供に対する公共機関間の意見調整に関する事項、③行政安全部長官から審議要請を受けた事項、④他の法律で定められた所管業務を遂行するための処理情報の目的外利用または提供に関する事項、⑤その他個人情報の保護に関して大統領令で定める事項について、審議する (2 項)。

委員会は、委員長 1 人を含む 10 人以内の委員で構成し (3 項)、委員長は行政安全部次官が、委員は公共機関の所属職員及び個人情報に関する学識と経験が豊富な者の中から委員長の推薦で国務総理が任命または委嘱する (4 項)。委員の任期は、2 年であり (5 項)、その他委員会の組織及び運営に関して必要な事項は大統領令で定めるとされている (6 項)。委員は、当然職 5 名と委嘱職 5 名で構成されているが、当然職 5 名は政府省庁の公務員である。

②公共機関個人情報保護審議委員会の運用実態

このような構成のために、国家人権委員会は、公共機関個人情報保護審議委員会について「個人情報保護審議委員会は行政安全部次官が委員長を任されており、委員は委員長が推薦する構造である。個人情報保護審議委員会の役割は、諮問機能以上を果たし得ず、別途の事務局も存在しないので、行政安全部から全く独立し得ておらず、2005 年から 2009 年の上半期までの会議開催が総 6 回に止まるなど、実効性のある役割をしていると見ることは困難である[3]」とまことに厳しい評価を下している。

1　2009 年 7 月に、政府の公共機関先進化政策により放送通信委員会傘下の韓国情報保護振興院 (KISA)、韓国インターネット振興院 (NIDA)、情報通信国際協力振興院 (KIICA) の 3 つの機関が統合して新たにスタートした機関である。

2　国家人権委員会も、その決定の中で、「現行法上、個人情報保護を担当する機構としては、公共部門を担当する公共機関の個人情報保護に関する法律に基づいた個人情報保護審議委員会と、民間部門を担当する情報通信網利用促進及び情報保護等に関する法律上の個人情報紛争調停委員会及び個人情報侵害申告センターがある」(国家人権委員会常任委員会決定 [3 개개인정보보호법률안 (이혜의원대표발의안 , 변재일의원대표발의안 , 정부발의안) 중 개인정보보호기구 관련 조항에 대한 의견](2009.12.24)6 頁) と述べている。

3　国家人権委員会常任委員会、前掲決定 (2009.12.24)6 頁。

（2）個人情報紛争調停委員会

①個人情報紛争調停委員会制度の概要

個人情報紛争調停委員会は、情報通信網法 33 条乃至 40 条に基づいて設置・運営されている[4]。

(a) 構成

紛争調停委員会は、委員長 1 名を含む 15 名以内の委員で構成され、そのうちの 1 名は常任とする（33 条 2 項)。常任委員は、事務局の指揮監督と委員会の議決の支援を行う。

委員は、次の①から⑥のいずれかの資格を有する者の中から、行政安全部長官が任命または委嘱するが、委員の分布を多様にするためにそれぞれの資格要件に該当する者を 1 名以上含まなければならない（3 項)。その資格とは、①大学または公認された研究機関で副教授級以上またはこれに相当する職にあるかあった者で個人情報保護関連分野を専攻した者、②４級以上の公務員またはこれに相当する公共機関の職にあるかあった者で個人情報業務に関する経験のある者、③判事・検事または弁護士の資格のある者、④情報通信サービス利用者団体の役職にあるかあった者、⑤情報通信サービス提供者または情報通信サービス提供者団体の役職にあるかあった者、⑥非営利民間団体支援法第 2 条による非営利民間団体で推薦した者の 6 種である。なお、情報通信網法には、委員の欠格事由についての定めはない。

一方、委員は、次の各号の一に該当するときは、当該紛争調停請求事件の審議・議決から除斥される（35 条 1 項)。すなわち、①委員またはその配偶者であった者が当該事件の当事者になるか、その事件に関して共同権利者または共同義務者の関係にある場合、②委員が当該事件の当事者と親族関係にあるかあった場合、③委員が当該事件に関して証言や鑑定をした場合、④委員が当該事件に関して当事者の代理人または役員として関与した場合、の４つの場合である。さらに、当事者は委員に審議・議決の公正を期待するのが困難な事情があるときは、紛争調停委員会に忌避を申し立てることができる。この場合、紛争調停委員会は忌避の申立てが妥当であると認めるときは、忌避の決定をする (2 項)。また、委員が除斥・忌避に該当するときは、自らその事件の審議・議決を回避することができる (3 項)。

なお、委員長は、委員の中から行政安全部長官が任命する (33 条 5 項)。

---

4 現在の個人情報の監督の実際の流れは、韓国インターネット振興院（KISA）で個人情報侵害の申告を受け付けて、その事案に従い各部署に渡している。例えば、紛争調停事件は個人紛争調停委員会に渡し、個人情報侵害事件で刑事事件の場合は行政安全部を経て捜査当局に移行しているが、しかし、個人情報保護法が施行されれば、個人情報保護に関する事項は、個人情報保護委員会を中心に扱われることになり、紛争調停事件は行政安全部傘下の個人情報紛争調停委員会で扱われることになるであろうということである。2011 年 3 月 25 日に行った個人情報紛争調停委員会委員長である金洙謙・東国大学法学部長へのインタビューでの発言。

(b) 委員の任期及び身分保障

委員の任期は 3 年であり、連続して任命することができる (33 条 4 項)。委員は、資格停止以上の刑を宣告され、または、心身上の障害で職務を遂行できない場合を除いては、その意思に反して免職または解嘱されない (34 条)。

(c) 業務支援組織

紛争調停委員会の業務を支援（紛争調停案件の事実調査、委員会の議決の支援など）するために、韓国インターネット振興院 (KISA) に事務局を置く (33 条 6 項)。また、紛争の調停業務を効率的に遂行するために紛争調停委員会に 5 名以下の委員で構成される調停部を置いている (33 条の 2 第 1 項)。

(d) 調停対象紛争の範囲と調停手続

調停対象は、個人情報に関する紛争である (33 条 1 項)。ここで個人情報とは、生存する個人に関する情報で、氏名・住民登録番号等によって個人を識別することができる符号・文字・音声・音響及び映像等の情報 (他の情報と容易に照合することができることによって特定の個人を識別することができる情報を含む) をいう (2 条 6 号)。

情報通信網法には、申請人の資格についての規定はないが、個人情報紛争調停委員会の設置目的が「個人情報に関する紛争を調停」するものである以上、申請人は個人情報に関する紛争に対して調停を申請しようとする者であると解される。代表者や代理人に関する規定はない。また、申請書に記載しなければならない要件、申請期間、調停費用などについての規定もない。

紛争の調停申請を受け付けた紛争調停委員会は、申請を受けた日から 60 日以内に審査して調停案を作成しなければならない。ただし、やむを得ない事情がある場合には、紛争調停委員会の議決によって、その期間を延長することができる (36 条 2 項)。期間を延長する場合には、期間延長の事由などの事項を申請人に知らせなければならない (3 項)。

紛争調停委員会は、紛争調停のために必要な資料の提供を紛争当事者に要請することができる。この場合、その紛争当事者は正当な事由がない限り要請に従わなければならない (37 条 1 項)。

紛争調停委員会は、調停申請を受け付けた後、当事者にその内容を通知して、調停前の合意を勧告することができる (19 条)。

(e) 調停の効力

紛争調停委員会は調停案を作成したときは、遅滞なく、各当事者に提示しなければならない (38 条 1 項)。この場合、調停案を提示された当事者は、提示された日から 15 日以内に調停案の受諾の可否を紛争調停委員会に通知しなければならない (38 条 2 項)。当事者が調停案を受諾すれば、紛争調停委員会は直ちに調停書を作成しなければならず、委員長及び各当事者はその調停書に記名捺印しなければならない (3 項)。当事者が調停案を受諾して調停書に記名捺印すれば、当事者間に調

停書と同一の内容の合意が成立したものとみなす (4 項)。金融紛争調停委員会や環境紛争調停委員会とは異なり、裁判上の和解と同じ効力は有しない。

②個人情報紛争調停委員会制度の運用実態[5]

(a) 年間紛争調停件数

個人紛争調停委員会が年間に扱う調停件数は、表 4 のとおりである。

表 4　年間紛争調停件数　（単位 : 件）

調停内容			2007 年	2008 年	2009 年
紛争調停決定	認容決定	調停成立	13	32	68
		調停不成立	4	4	12
	棄却決定		2	2	3
調停前当事者合意			75	41	61
合計			94	79	144

※現行の委員会の調停による合意は、民事上の和解の効力を有しており、一方の不履行または成立・効力要件に瑕疵がある場合には、裁判所に損害賠償の提起が可能である。

(b) 紛争調停委員会の業務量

紛争調停事件の事実調査、委員会の開催、結果報告などのために、月 2 回の委員会を開催し、月平均 12 件の証拠収集及び調査結果の措置を行っている。また、事務局の指揮監督、紛争調停改善方案の点検などのために、月 2 回の会議出席、事務局の運営監督、紛争調停分析を行っている。しかしながら、「民事部門の個人情報紛争調停委員会は行政安全部長官が委員会の委員長と委員を全て任命して、予算もやはり韓国インターネット振興院を通じて支援されており、機能もまた紛争調停に局限されている[6]」という限界があることは否定できない。

（3）韓国インターネット振興院 (KISA)

①韓国インターネット振興院の役割[7]

個人情報保護法制定までは、韓国は情報通信網法などに基づいて個人情報保護を規律してきた。情報通信網法は情報通信網における個人情報保護、安全性確保、電子メール (スパムメール) 規制などを規定する法律であり、個人情報保護については、その第 4 章 (22 条〜 40 条) で規定している。

5　個人情報紛争調停委員会の運用実態については、행정안전부『개인정보보호법 심사참고자료』(2010.12)、43 頁を参照。

6　国家人権委員会常任委員会、前掲決定 (2009.12.24)6 頁。

7　韓国インターネット振興院 (KISA) の役割及び運用実態についての記述は、2011 年 3 月 24 日の KISA 情報保護本部のパック・グァンジン（박광진）本部長、3 月 25 日の KISA 情報保護本部のキム・ミンソプ（김민섭）責任研究員へのインタビューと、その後に提供された資料に基づく。

情報通信網法には別途の個人情報保護監督機構に関する規定は存在しないが、放送通信委員会および行政安全部が事業者に対する規制・監督権限を行使することを規定している。放送通信委員会は情報通信サービス分野を、行政安全部は情報通信サービス分野以外の産業分野 (旅行業、観光業、ホテル業、塾など 24 個分野、情報通信網法 67 条) をそれぞれ管轄し、その主要な規制・監督権限としては、個人情報保護に関する施策の準備 (4 条)、事業者に対する資料提出要求権、現場検査権、是正命令権 (64 条)、課徴金賦課権 (64 条の 3)、法違反行為に対する過料賦課権 (76 条) などである。

個人情報保護法が制定された後も、情報通信網法などの個別法律がある場合には当該個別法律がまず適用されるので (個人情報保護法 6 条)、放送通信委員会が担当する情報通信サービス分野の個人情報保護規制・監督権限は今後も維持されることになる。

韓国インターネット振興院は、情報通信網法 52 条に基づいて、個人情報侵害申告センターの運営、個人情報紛争調停委員会の運営、政府部署の実態調査に対する技術的諮問及び支援などの業務を委託されて遂行している。個人情報保護法の施行以後は、同法による「専門機関」に指定される場合には、個人情報侵害申告センターの運営、個人情報紛争調停委員会の運営、流出事故発生時の申告受付、その他政府が委託する個人情報関連業務を遂行する予定である。

②韓国インターネット振興院の運用実態

韓国インターネット振興院が運営する個人情報侵害センターが年間に受け付けた申告数は、表 5 のとおりであり、年々増加していることが明らかである。

また、表 6 は、それらの内容を類型別に分析したものである。住民登録番号の不正利用が最多であり、これは韓国において絶対的な身分証明書の地位を占める住民登録番号が安易に利用されている現状をよく示すものでもある [8]。

表 5　受付現況

区分	2006 年	2007 年	2008 年	2009 年	2010 年	'11 年 3 月
申告	740	847	988	2,139	1,788	242
相談	22,593	25,118	38,823	33,028	53,044	9,436
合計	23,333	25,965	39,811	35,167	54,832	9,678

※申告は違法事実の是正などの処理が行われた苦情申立てをいう。相談は関連情報の提供や案内などで終結した苦情申立てをいう。

8　住民登録法に基づく住民登録番号制度は、本来は、行政機関がその管轄区域内に住所を置く住民を統一的に登録して、住民の居住状況と移動実態を把握して、もって行政事務の円滑な処理を目的とするものであるが、導入のもう一つの理由が国防を目的としたものであることは否定できない事実である。1962 年の住民登録法の制定に基づき、当初は希望者のみの登録として開始されたが、1968 年の同法改正によって、住民個々人に番号が付与され、18 歳以上の住民に住民登録証の発給を行うようになった。その後、1975 年の改正で住民登録証の発給対象者を 17 歳に引き下げ、1977 年の改正で指紋をはじめとする個人の身上情報がすべて登録されるようになり、1980 年の改正で住民登録証の所持義務が規定されることで、ここに住民登録証が ID としての役割を果たすようになった。韓国では、絶対的な地位を有する身分証明書ということができ、あらゆるところで住民登録番号が求められている実情である。詳しくは、自治体国際協会編『各国の電子自治体の推進状況』(自治体国際協会（CLAIR)、2006 年）134 ～ 135 頁、を参照。

表 6　個人情報侵害申告及び相談の類型別現況

受付類型	2007 年	2008 年	2009 年	2010 年	2011 年 (3 月)
合計	25,965	39,811	35,167	54,832	9,678
利用者の同意なき個人情報収集関連	1,166	1,129	1,075	1,267	232
個人情報収集時の告知または明示義務関連	7	6	15	75	8
過度な個人情報収集	51	87	115	146	58
目的外利用または第三者提供関連	1,001	1,037	1,171	1,202	234
個人情報取扱者による毀損・侵害等	123	125	158	158	23
個人情報処理委託時の告知義務	2	6	6	25	5
営業の譲受けなどの通知義務	14	9	6	22	8
個人情報管理責任者関連	10	26	10	21	3
技術的・管理的措置不備関連	522	1,321	819	1,551	317
収集または提供された目的達成後の個人情報未破棄	146	294	294	323	51
同意撤回・閲覧または訂正の要求関連	865	949	680	826	99
同意撤回、閲覧・訂正を収集よりも容易にすべき措置	461	503	603	630	154
児童の個人情報収集	14	27	19	35	21
住民登録番号など他人情報の毀損・侵害・盗用	9,086	10,148	6,303	10,137	2,905
情報通信網法適用対象外関連 (信用情報関連の問合せなど)	12,497	24,144	23,893	38,414	5,560

4　新しい個人情報保護法の制定―統合的な基本法としての個人情報保護法

（1）法制定の背景及び経緯

盧武鉉政権時代の第 17 代国会 (2004 ～ 2008 年) においては、「その当時、多くの個人情報保護法案が提出され、いわゆる個人情報保護に関する百家争鳴の時代に入った。その当時の論議は、個人情報保護のために、より“望ましい”法を探し求める過程であったし、結局、これは個人情報の“保護”と“利用”の間の関係をどのように設定するべきかに対する個人情報保護それ自体についての哲学的悩みを持っていたのである[9]」といえる。しかし、これらの個人情報保護法案は、いずれも 17 代国会の任期満了により自動廃棄された。

個人情報保護法の制定・改正は、新たに出帆した李明博政権において、ますますその必要性を増すことになった。

第一の理由は、大規模個人情報侵害事故の頻発による国民の不安感の急増である。最近の個人情報侵害は、大型化・知能化・多様化しており、インターネット・ショッピングモールなどでの 6,950 万人の流出事故 ('10.3 ～ 5) をはじめとして、2007 年から 2010 年までに延べ約 1 億人の個人情報侵害事故が発生していることである。また、2005 年から 2007 年までの個人情報被害規模は、10 兆 7000 億ウォンと推計されている。第二に、個人情報保護法の一般法が制定されていないために、法適用の死角地帯が発生していることである。公共機関個人情報保護法、情報通信網法などの個別法の体系を採っているために、オフライン事業者、非営利機関などが法適用対象から除外されており、たとえば、2009 年の個人情報侵害申告 35,167 件のうち、68.1% の 23,948 件が法適用除外事業者であった（表 6 参照)。また、個別法の間での保護原則、処理基準及び推進体系が相違しているために、国民の間で混乱が生じてもいる。そして、第三に、世界各国との FTA の対策、また、IT 強国としての位相を確保する必要に迫られていることである。世界各国との FTA 締結によって相互間の個人情報の交流増大が予想され、国際水準の個人情報保護体系の構築が必要とされたのである[10]。

そこで、李明博政権の第 18 代国会 (2008 ～ 2012 年) においては、行政安全部が 2008 年 3 月に「個人情報保護法制定プロジェクト」を設立して検討を開始したし、国会においても、李惠薫議員案 (08.8.3)、卞在一議員案 (08.10.27) をはじめ多くの関連法案が国会に発議された。政府は、これまでの検討を踏まえて、2008 年 11 月 28 日に、「個人情報保護法」の政府案を提出した。しかし、国会の法案審査小委員会は、国会上程中の個人情報に関連した 13 件の法律案を総合審査した結果、いずれも本会議に付議しないことにして、これらを統合・調整した国会行政安全委員会の代案を提案することで一致した (2010.9.28)。

9　김일환「개인정보보호법 제정의 주요 쟁점」『“정보인권의 법적보장과 그 구체화”공동학술세미나』(국가인권위원회인권정책과、2010 年)92 頁。

10 행정안전부『개인정보보호법심사참고자료』(2010.12)1 ～ 2 頁、を参照。

国会行政安全委員会は、法案審査小委員会の審査結果を受け入れて、委員会としての代案を作成して、委員会を通過させた (2010.9.30)。この時点で、事実上、与野党合意の法案は確定したのであるが、2011 年度予算案を巡る与野党の場外闘争のあおりを受けて、この法案の国会本会議上程は予定よりも大幅に遅れることになった。すなわち、本年（2011 年）3 月 10 日に至ってやっと法制司法委員会全体会議を通過、翌 11 日に、最後の関門である国会の本会議を、在籍議員 221 名中、賛成 219 名、棄権 2 名で通過して、3 月 29 日に公布、9 月 30 日に施行されることになった。個人情報保護法は、日の目を見るまでに実に 2004 年から議論されて 7 年の歳月を費やしたのである。

（2）個人情報保護法の構成

個人情報保護法は、本則 9 章 75 条及び附則で構成されている。

その概略を示せば、第 1 章「総則」では、法律の目的、用語の定義 (適用範囲)、個人情報保護原則、情報主体の権利、他の法律との関係など、第 2 章「個人情報保護政策の樹立等」では、個人情報保護委員会の構成･機能、個人情報保護の基本計画及び施行計画の樹立、実態調査、個人情報保護指針、自主規制の促進施策、国際協力についてそれぞれ規定している。

続く､第 3 章は 2 節からなっている。第 1 節「個人情報の収集､利用､提供等」では､個人情報の収集･利用の基準、提供の基準及び収集の制限、目的外の利用・提供の制限、個人情報の破棄、同意を受ける方法について、第 2 節「個人情報の処理制限」では、機微情報と固有識別情報の処理制限、映像情報処理機器の設置・運営の制限、業務委託にともなう個人情報処理の制限、営業譲渡などの移転制限についての定めが置かれている。

第 4 章「個人情報の安全な管理」では、安全措置義務、個人情報処理方針の樹立・公開、個人情報保護責任者の指定、個人情報ファイルの登録及び公開、個人情報影響評価、個人情報の流出通知など、第 5 章「情報主体の権利保障」では、個人情報の閲覧要求権、訂正・削除要求権、処理停止要求権、権利行使の方法及び手続、損害賠償責任について規定している。第 6 章「個人情報紛争調停委員会」では、設置・構成、委員の身分保障、除斥・忌避・回避、調停の申請、処理期間、資料の要請、調停前合意の勧告、紛争調停、調停の拒否および中止、集団紛争調停など、第 7 章「個人情報団体訴訟」では、訴訟の対象、専属管轄、代理人選任、訴訟許可要件、確定判決の効力など、第 8 章「補則」では、適用の一部除外、禁止行為、秘密維持義務、意見提示及び改善勧告、侵害事実の申告、資料提出要求及び検査、是正措置、告発及び懲戒勧告、結果の公表、年次報告、権限委任・委託などについての規定があり、そして、第 9 章「罰則」では、罰則、過料及び両罰規定が置かれている。

この個人情報保護法の制定によって、現行の「公共機関の個人情報保護に関する法律」の全部と「情報通信網利用促進及び情報保護等に関する法律」の一部条項 (第 33 条～ 40 条、第 66 条第 1 号および第 67 条) は、吸収されて廃止されることになる。

（3）個人情報保護法の主要内容

①用語の定義及び個人情報保護義務の適用対象

(a) 用語の定義

用語の定義は、次のように規定されている（2 条)。すなわち、「“ 個人情報 ” とは、生存している個人に関する情報で、氏名、住民登録番号及び映像等を通じて個人を識別できる情報（(当該情報のみでは特定個人を識別できなくても、他の情報と容易に結合して識別することのできるものを含む)）をいう」(1 号）とし、「“ 個人情報ファイル ” とは、個人情報を容易に検索できるように一定の規則に従い体系的に配列または構成した個人情報の集合物をいう」(4 号）と定義する。したがって、個人情報ファイルには、電子的に処理するデータベースだけでなく書類などの記録も含むことになる。

また、「“ 個人情報処理者 ” とは、業務を目的として個人情報ファイルを運用するために、自らまたは他のものを通じて、個人情報を処理する公共機関、裁判所、団体及び個人等をいう」(5 号）と定義している。したがって、裁判所・国会等の憲法機関、営利・非営利法人はもちろん、オフライン事業者も含むことになる。

個人情報保護法は、その適用対象を、公共・民間部門のすべての個人情報処理者に拡大しただけでなく、コンピュータ等によって処理される情報のほかに手書き文書をも保護範囲に含めている。これによって、オフライン事業者、非営利団体、国会・裁判所・中央選挙管理委員会の行政事務を処理する機関など、これまで個人情報保護関連法律の適用を受けなかった死角地帯が解消されるとともに、個別法律の間で異なっていた処理基準も基本的に共通されることになり、国家社会全般の個人情報保護水準が向上するものと期待されている。政府の説明によれば、個人情報保護法の制定によって、これまで適用対象外であった約 300 万個の機関・事業者（死角地帯）が新たに対象に加わることになり、適用対象は約 350 万個のすべての公共機関と事業者になるといわれている [11]。

(b) 他の法律との関係

個人情報保護法は、「個人情報保護に関しては、情報通信網利用促進及び情報保護等に関する法律、信用情報の利用及び保護に関する法律等、他の法律に特別の規定がある場合を除いては、この法律の定めるところによる」(6 条）と定めて、この法律が一般法であると同時に、今後も個別法律が併存することを明らかにしている。

②個人情報保護委員会の設置と個人情報紛争調停委員会の拡大

個人情報保護の基本計画の樹立、個人情報保護に関する法令及び制度の改善など、個人情報に関する主要事項を審議・議決するために、新たに大統領所属下に「個人情報保護委員会」を構成して、個人情報保護と関連した重要事項に対する意思決定の慎重性・専門性・客観性の確保に努めるとともに、従来の「個人情報紛争調停委員会」の規模と機能をも拡大・充実させた。この点は本稿執筆の主たる目的でもあるので、詳細は、章を改めて、後述することにする。

---

11 행정안전부보도자료 2011 년 3 월 30 일「개인정보보호 2.0 시대의 개막 “ 개인정보보호법 제정 · 공포 ”」1 頁。http://news.mopas.go.kr/govnews/branch.do?act=newsView&id=200000657&currPage=1

③個人情報の処理原則

(a) 個人情報の収集・利用、第三者提供及び破棄

個人情報は、情報主体の同意や法律の規定に基づくときなど、一定の場合に限ってのみ、収集することができ、収集目的の範囲内でのみ利用ができる（15 条 1 項)。

同意を得るときには、①個人情報の収集・利用目的、②収集項目、③個人情報の保有及び利用期間などを明確に告知しなければならない（2 項)。

個人情報の目的外の利用・提供は、原則的に禁止されるが（18 条 1 項)、別途の同意の獲得、法律の規定の存在、犯罪捜査、裁判業務の遂行など一定の場合には例外を許容している（2 項)。

個人情報の収集・利用目的の達成などで不必要になったときには、遅滞なく、個人情報を破棄しなければならない（21 条)。

このように、これまで個別法律の間で相違していた処理基準を統一するとともに、個人情報の収集、利用、提供、破棄に至る各段階別に個人情報処理者が遵守しなければならない処理基準を具体的に規定した。

(b) 同意を得る方法

個人情報の目的外利用・提供、固有識別情報などに対する同意手続を強化した。すなわち、契約の締結等のための必須的同意事項と選択的同意事項とを区分して、情報主体がこれを明確に認知できるような方法で同意を得なければならないとしている（22 条)。

④個人情報の処理制限

(a) 固有識別情報の処理制限

住民登録番号など法令によって個人を固有に区別するために付与された固有識別情報は原則的に処理を禁止して（24 条 1 項)、別途の同意を得るかまたは法令による場合などに限って制限的に例外を認める一方、大統領令で定める基準に該当する個人情報処理者はホームページを通じた会員加入を募るときには、住民登録番号以外の方法を必ず提供するように義務化している（2 項)。固有識別情報の処理が例外的に許される場合についても、①情報主体の別途の同意、②法令で具体的に固有識別情報の処理を要求または許容している場合（24 条 1 項各号）に厳しく限定している。

これは、本来、行政目的のために導入された住民番号であったが、その個人を証明する精度の高さ (価値) からハッキングの対象になるなどの副作用が大きくなってきたので、民間では住民番号を使用せず、代わりに「I-PIN」などの代替手段を用いるようにしたものである [12]。

12　2011 年 3 月 25 日に行った行政安全部個人情報保護課のキム・サングァン (김상광) 書記官へのインタビューでの発言。

(b) 個人情報処理の委託

個人情報処理を委託する場合には、情報主体が受託者及び委託業務の内容をつねに容易に確認できるように、大統領令で定める方法により公開しなければならない（26 条 2 項）。マーケッティング目的で個人情報処理を委託する場合には（業務内容や受託者の変更の場合を含む）、大統領令で定める方法により、業務の内容と受託者を情報主体に必ず知らせなければならない（3 項）。また、委託者の受託者に対する監督義務及び賠償責任を規定するとともに（4 項、6 項）、受託者が、委託された業務の範囲を超えて個人情報を利用または第三者に提供することを禁止した（5 項）。

⑤映像情報処理機器の設置制限

映像情報処理機器運営者は、法律で具体的に許容されている場合のほか、犯罪予防及び捜査、施設の安全及び火災の予防、交通の取締、交通情報の収集・分析及び提供のために必要な場合に限って、一般的に公開された場所に、映像情報処理機器を設置できると規定した（25 条 1 項）。また、その際には、情報主体がその設置を容易に認識できるように、案内板の設置などを義務付けた（4 項）。刑務所や精神保健施設等を除いては、浴場、化粧室、サウナ室、脱衣所等、私生活を著しく侵害するおそれのある場所の内部には設置・運営を禁止し（2 項）、さらに、設置目的外での操作の禁止、録音機能の使用禁止などを定めている（5 項）。

⑥個人情報の安全な管理

(a) 技術的・管理的保護措置の強化

個人情報処理者は、個人情報の紛失・盗難・流出または毀損防止のために、内部管理計画の樹立、接続記録の保管など、大統領令の定めるところに従い、安全性確保に必要な技術的・管理的及び物理的措置を講じなければならないとの、安全性確保義務を規定した（29 条）。また、個人情報処理者は、個人情報処理目的、処理・保有期間、第三者提供・委託、情報主体の権利・義務及びその行使方法などを記載した「個人情報処理方針」を樹立して、それを公開しなければならない（30 条）。

個人情報処理者は、個人情報の処理に関する業務を総括して、その責任を負う、「個人情報保護責任者」を指定しなければならない（31 条）。

(b) 公共機関の特例

公共機関の長は、当該機関が保有する個人情報ファイルについて、その目的・根拠・期間等、一定の事項を行政安全部長官に登録しなければならず（32 条 1 項）、行政安全部長官は、これを公開しなければならない（4 項）。

⑦個人情報影響評価制度の導入

公共機関は、個人情報ファイルの運用によって情報主体の個人情報を侵害するおそれがある場合には、必ず個人情報影響評価を行わなければならない（33 条 1 項）。公共機関以外の個人情報処理者に

ついては、個人情報ファイルの構築・拡大などが個人情報保護に影響を及ぼすおそれが大きいと判断される場合には、「影響評価をするために積極的に努力しなければならない」と規定している（6 項）。

⑧個人情報流出事実の通知・申告制度の導入

被害の拡散防止及び情報主体の効果的な権利救済のために、個人情報処理者は、個人情報流出事実を認知した場合、遅滞なく、当該情報主体に関連事実を通知するとともに (34 条 1 項)、被害を最小化するための必要な措置をとらなければならない (2 項)。大統領令で定める一定規模以上の個人情報が流出したときには、個人情報処理者は、流出事実の通知及びその措置結果を、遅滞なく、行政安全部長官または専門機関に申告しなければならない (3 項)。

⑨情報主体の権利保障

情報主体に個人情報の閲覧請求権、訂正・削除請求権、処理停止要求権などを付与して、その権利行使方法などを規定した（35 条〜 39 条）。いうまでもなく、これは、個人情報処理者が保有中である個人情報の正確性及び最新性を担保して、情報主体の自己情報決定権を強化するためのものである。

⑩集団紛争調停制度の導入

個人情報紛争調停委員会の調停決定に裁判上の和解の効力を付与するとともに、個人情報被害が大部分の場合、大量・少額事件である点を考慮して、集団紛争調停制度を導入した（49 条）。

⑪団体訴訟の導入

個人情報処理者をして個人情報の収集・利用・提供などに対する遵法精神と警戒心を高めるとともに、同一・類似の個人情報訴訟に伴う社会的費用を節減するために個人情報団体訴訟制度を導入した。訴訟を提起できる者は、①消費者基本法上の消費者団体、②非営利民間団体支援法上の非営利民間団体である（51 条 1 号、2 号）。ただし、濫訴の弊を避けるために、集団紛争調停を経ること（55 条）、また、団体訴訟の対象は権利侵害行為の中断・停止請求訴訟に限られる（51 条柱書き）ことを定めている。

⑫補則

(a) 法適用の例外

統計法により収集される個人情報、国家安全保障に関連した情報分析のために収集される個人情報、公共の安全と安寧のために緊急に必要とされ一時的に処理される個人情報、言論・宗教・政党の固有活動のために収集される個人情報などは、適用除外される (58 条)。

(b) 個人情報侵害事実の申告

個人情報処理者によって権利または利益を侵害された者は、行政安全部長官にその侵害事実を申告することができ (62 条 1 項)、行政安全部長官は申告の受付け及び業務処理の支援のために個人

情報侵害申告センターを設置・運営する (2 項)。これは、個人情報侵害事実の申告・相談の窓口を用意して、情報主体の迅速な権利救済と苦情処理に寄与しようとするものである。

(c) 改善勧告・資料提出の要求・検査

行政安全部長官または関係中央行政機関の長は、個人情報保護のために必要と認めるときは、個人情報処理者に処理実態の改善を勧告し、その措置結果を報告させること (61 条 2 項、3 項)、個人情報保護法違反の嫌疑または申告などがあるときには、個人情報処理者に関係資料の提出を要求し、立入検査すること (63 条)、また、個人情報が侵害されかつ放置すれば回復の困難な被害が発生するおそれがあると認めるときには、個人情報保護法に違反した者に対して、侵害行為の中止、個人情報処理の一時的停止、その他必要な措置を命じられること (64 条)、個人情報処理者に個人情報法規違反の犯罪嫌疑があると認めるときには管轄捜査機関に告発し、また、法規違反に責任ある者を懲戒するようその所属機関・団体などの長に勧告できること (65 条)、そしてこれらの改善勧告、是正措置命令、告発・懲戒勧告のほか、過料の内容について、公表できること (66 条) を規定している。

⑬罰則

業務妨害目的の個人情報の変更・抹消、機微情報の無断処理、個人情報の無断利用・提供などの重大な法益侵害には、懲役または罰金を科している (70 条〜 74 条)。一方、個人情報管理責任者の未指定、個人情報取扱方針の未公開などの手続的義務違反に対しては過料を科している (75 条)。

（4）個人情報保護法の制定で変更される事項

個人情報保護法の制定によって、従前と異なるようになる点を表の形式で一覧にすると、次の表７のとおりである。

表７　個人情報保護法による変更点

区分	現行	個人情報保護法
規律対象	○公共機関、情報通信事業者、信用情報提供・利用者など分野別個別法がある場合に限って個人情報保護義務適用	○公共・民間統合規律で法適用対象拡大 : 現行法の適用を受けなかったオフライン事業者、医療機関、協会･同窓会など非営利団体、国会・裁判所・憲法裁判所・中央選挙管理委員会などに拡大
保護範囲	○公共機関はコンピュータなどによって処理される個人情報ファイルだけを保護対象にする	○公共団体への苦情処理申請書類などの紙文書に記録された個人情報も保護対象に含む
収集・利用及び提供基準	○公共、情報通信など分野別個別法に基づく処理基準存在	○公共・民間を網羅する個人情報処理原則と基準を提示
固有識別情報処理制限	○住民登録番号など固有識別情報の民間使用を事前に制限する規定なし	○原則的処理禁止 : 情報主体の別途同意、法令の根拠がある場合などは例外許容
	○インターネット上での住民登録番号以外の会員加入方法提供義務化 (情報通信サービス提供者限定)	○インターネット上での住民登録番号以外の会員加入方法提供義務化の対象拡大 (情報通信サービス提供者→公共機関、一部民間分野個人情報処理者) ※大統領令で義務化対象を規定
		○住民登録番号など固有識別情報処理時に暗号化など安全措置確保義務明示

映像情報処理機器規制	○公共機関が設置・運営する閉回路テレビ (CCTV) に限って規律 : 犯罪予防及び交通取締りなど公益のために必要な場合、専門家及び利害関係人の意見収斂を経て設置 ○録音機能、任意操作禁止	○公開された場所に設置・運営する映像情報処理機器規制を民間まで拡大 : 公開された場所であるデパート・アパートなどの建物駐車場、商店内・外部などに映像情報処理機器を設置するときには法令、犯罪予防・捜査、施設安全及び火災予防、交通取締りなどのために設置可能 ○規律対象を既存の ‘ 閉鎖回路テレビ (CCTV)’ からネットワークカメラも含む
		○公衆トイレ・浴場・更衣室など私生活侵害のおそれが大きい場所は設置禁止
テレマーケッティングなど規制	○「情報通信網法」によって情報通信サービス提供者に限って規制 : マーケティング目的で個人情報取扱いを委託する場合、情報主体の同意を受けること	○マーケティングのために個人情報処理に対する同意を受けるときには他の個人情報処理に対する同意と一まとめにして同意を受けないように明示的に規定 : 情報主体が分かりやすいように告知して同意を受けること ○すべての個人情報処理者はマーケティング業務の委託時、情報主体に委託業務内容及び受託者を告知すること (情報通信サービス提供者→すべての個人情報処理者に規制対象拡大)
個人情報ファイル登録・公開及び影響評価	○公共機関が個人情報ファイル保有時に行政安全部長官と事前協議	○公共機関が個人情報ファイル保有時に行政安全部長官に登録
	○行政安全部長官は事前協議ファイル官報公告	○行政安全部長官は登録事項公開

		○公共機関は大規模個人情報ファイル構築など侵害の危険が高い場合には事前影響評価実施を義務化 (民間は自律施行)
流出通知	関連制度なし	○大規模個人情報流出時には関係機関の政策樹立及び積極的な事後措置のために関係機関への申告義務規定
委員会	○国務総理所属の公共機関個人情報保護審議委員会 : 公共部門政策審議	○大統領所属の個人情報保護委員会設置 : 公共・民間部門個人情報保護政策審議・議決機構
	○個人情報紛争調停委員会 : 民間分野紛争調停	○個人情報紛争調停委員会の機能拡大 :(現行) 15 人以内 (民間限定) → (拡大) 20 人以内 (すべての公共・民間含む)
	○団体訴訟、集団紛争調停未導入	○団体訴訟導入 : 権利侵害の中止・停止の団体訴訟導入 ○集団紛争調停導入 : 多数・少額の個人情報流出などの被害が多いので一括的な紛争調停ができるように情報主体の被害救済強化

행정안전부『개인정보보호법 심사참고자료』2010.12、20 ～ 21 頁。

5 個人情報保護法の監督機関

（1）監督機関をめぐる議論の過程

盧武鉉政権下で提出された議員法案では、個人情報保護の適用対象などについては争いがあったものの、監督機構については、調査・諮問機能を超えた是正勧告、告発などの執行及び準司法機能を有すべきであるという点では共通していた[13]。

また、李明博政権下で提出された、すべての議員法案も、その監督機構は、調査、諮問機能にとどまらず、是正勧告、告発などの執行及び準司法機能を持つ独立した行政庁としての委員会を提示した[14]。それにもかかわらず、当初提出された政府案だけは、国務総理所属に置かれる審議委員会の形式を提示して、その審議委員会では主要な事案を審議するだけで、各部処（省庁）が執行を担当し、行政安全部がそれを総括するというものであった。

独立監督機構を置くことについては、行政安全部は、別途の機構を設置することに伴う費用の増大は「小さい政府」を標榜する現政権の政策と相反すること、情報化と個人情報保護業務の連携の必要性、各部処の個人情報保護政策と衝突・重複するおそれ、個人情報保護政策の執行力の脆弱と意思決定の遅延のおそれなどを理由に、否定的であり、自らが担当すべきであるという意見であった[15]。しかし、法案審査の過程で、野党、国家人権委員会、市民団体などの問題提起を受けて、個人情報保護委員会を大統領所属に格上げするとともに、委員会の機能に議決機能を追加すること、委員の選出を国会・大法院・大統領が各々５人ずつ推薦すること、さらに、個人情報保護委員会に常任委員と事務局[16]を新設することなど、その独立性を高める規定を追加することで、野党などと妥結するに至った。

---

13 もっとも、そもそも個人情報保護機構が公共部門と公共民間部門をすべて管掌すべきか否か、その機構の権限が諮問（勧告）、調停の役割に限定されるべきか、それとも制定された個人情報保護法のように執行機能などを有する強力な権限を付与すべきかについては、その当時も議論があった。김일환、前掲論文、99 頁。

14 김일환、前掲論文、104 頁。

15 김일환、前掲論文、107 頁。

16 個人情報保護委員会の業務を支援するための事務局は、主務官庁の行政安全部からの派遣される公務員と、別途に専門知識を有している人材を契約職公務員として採用することで運営することになるものと予想される。2011 年 3 月 25 日に行った金洙謙・個人情報紛争調停委員会委員長へのインタビューでの発言。

これらの案を比較すれば、表８のとおりである。

表８　監督機関の法案別比較

区分	李惠薫議員案	卞在一議員案	政府案	個人情報保護法
名称	個人情報委員会	個人情報保護委員会	個人情報保護委員会	個人情報保護委員会
所属	国務総理	大統領	国務総理	大統領
性格	政策樹立・執行	政策樹立・執行	政策審議	政策審議・議決及び執行
構成	9名(常任1)	9名(常任1)※国会3、大統領3、法院3	15名	15名(常任1)※国会5、大統領5、法院5
	任期3年	任期3年	任期2年	任期3年
機構	事務処設置	事務処設置	—	事務局設置

김상광「개인정보보호법 제정 쟁점 토론자료」『“정보인권의 법적보장과 그 구체화”공동학술세미나』국가인권위원회인권정책과、2010年、125頁

（2）個人情報保護委員会

(a) 個人情報保護委員会の機能

個人情報保護委員会、行政安全部、中央行政機関の三者の主要な機能は、次のとおりである。

まず、個人情報保護委員会は、個人情報保護政策の審議・議決が主たる機能であり、具体的には、①個人情報保護基本計画・施行計画の審議・議決、②公共機関の目的外利用・提供の審議・議決、③中央行政機関・自治団体に対する是正勧告、④国会に対する年次報告書の提出、⑤影響評価結果・改善勧告などの審議・議決などである（詳細は後述）。

これに対して、行政安全部は、個人情報保護業務の総括・調整が主要な機能であり、具体的には、①基本計画の樹立･施行、②標準個人情報保護指針の制定、③個人情報処理方針作成指針の制定･勧告、④個人情報流出通知の運営、⑤法違反行為の調査、是正勧告・命令、過料の賦課、⑥個人情報ファイル登録の受付け及び現況の公開、⑦自主規制の促進及び支援施策、⑧個人情報影響評価の管理運営などである。

そして、中央行政機関の主たる機能は、その所管分野及び個別法の個人情報保護業務の遂行であり、具体的には、①所管分野の個人情報保護の施行計画の樹立、②法違反行為の調査、是正勧告･命令、過料の賦課などである[17]。

17 행정안전부『개인정보 침해사례 및 개인정보보호법 [안] 소개 2010.11.23』25頁。
www.csokorea.org/news/download.asp?idx=4232

したがって、「個人情報保護委員会の性格は、諮問機構と行政機構の両者の性格を有している。同委員会は、各中央行政機関を統合調整して、各中央行政機関はその所属機関に対して監督するという、いわば『分散統合型』の構造ということができる。同委員会は、司法府と立法府に対しては三権分立の原則から強制はできないが、是正勧告はできる[18]」ものである。

(b) 個人情報保護委員会の構成

個人情報保護委員会は、委員長 1 名、常任委員 1 名を含む 15 名以内の委員で構成するが、大統領、国会、大法院長[19]がそれぞれ選出・指名する 5 名ずつの委員を大統領が任命または委嘱することになっている（7 条 2 項、4 項 1 号）。委員長は、委員の中から公務員でないものを大統領が委嘱する（3 項）。

委員になる資格を有する者は、①個人情報保護と関連した市民社会団体または消費者団体から推薦を受けた者、②個人情報処理者で構成された事業者団体から推薦を受けた者、③その他、個人情報に関する学識と経験が豊富な者のいずれかでなければならない（4 項 2 号）。

委員長と委員の任期は 3 年であり、1 回に限って再任することができる（5 項）。

(c) 個人情報保護委員会と個人情報紛争調停委員会の分離

個人情報保護委員会と個人情報紛争調停委員会とを分離したが、両者の関係が不明であるとして、個人情報紛争調停委員会を個人情報保護委員会に統合するか、その傘下の委員会として構成すべきであるとの意見もある。

(d) 独立性の保障

「[個人情報] 保護委員会は、その権限に属する業務を独立して遂行する」（7 条 1 項後段）と定めてはいるが、独立的な活動を具体的に保障する規定はない[20]。

---

18 2011 年 3 月 25 日の行政安全部個人情報保護課のキム・サングァン (김상광) 書記官へのインタビューでの発言。個人情報保護法は、その 64 条 4 項で、「保護委員会は、中央行政機関、地方自治団体、国会、裁判所、憲法裁判所、中央選挙管理委員会が、この法律に違反したときには、当該機関の長に、第 1 項各号に該当する措置 [個人情報侵害行為の中止・個人情報処理の一時的停止・その他個人情報保護のために必要な措置……筆者注] を勧告することができる。この場合、勧告を受けた機関は、特別の事由がない限り、これを尊重しなければならない」と規定している。

19 国家機関のうちで最も民主的正当性の弱い大法院長がいかなる制限もなしに委員を 5 名指名することに対しては、否定的な意見もある。

20 この点は、すでに国家人権委員会から改善すべきとの意見が表明されている。すなわち、国家人権委員会は、国会行政安全委員長に、政府が発議した個人情報保護法律案は、個人情報保護機構が十分に機能を遂行するのに必要な独立性の要素が不備であり、この法案を中心とした立法は望ましくないという意見を表明した。また、ハンナラ党の李恵薫議員が代表発議した個人情報保護法律案と民主党の卞在一議員が代表発議した個人情報保護法律案についても、委員の免責特権関連規定と委員任命過程での国会の関与を高める方案、組織・予算上の独立性を高める方案を積極的に補完する必要があると明らかにした。特に政府案に対しては、「3 個の法案のうち政府が発議した案は個人情報保護機構が有さなければならない核心的機能である調査機能がなく独立性要件を深刻に欠如している」し、「また、委員が全員非常任委員で専門性が劣るおそれもある」と厳しく指摘していた。国家人権委員会常任委員会、前掲決定 (2009.12.24) 12 ～ 13 頁。

(e) 委員会の業務と権限

個人情報保護委員会が審議・議決する事項は、①基本計画及び施行計画、②個人情報保護と関連した政策、制度及び法令の改善に関する事項、③個人情報の処理に関する公共機関間の意見調整に関する事項、④個人情報保護に関する法令の解釈・運用に関する事項、⑤個人情報を目的外の用途に利用しまたは第三者に提供しなければ他の法律で定める所管業務を遂行できないとして、個人情報保護委員会に個人情報の利用・提供の審議・議決を求める事項、⑥行政安全部長官が影響評価結果に対して意見を提示しようとするときに必要とされる事前の審議・議決を求める事項、⑦個人情報保護に影響を及ぼす内容の法令や条例に対して行政安全部長官が関係機関に意見を提示しようとするときに必要とされる事前の審議・議決を求める事項、⑧中央行政機関、地方自治団体、国会、裁判所、憲法裁判所、中央選挙管理委員会が個人情報保護法に違反したときに、当該機関の長に、個人情報侵害行為の中止、個人情報処理の一時的停止その他の必要な措置をとるように勧告する事項、⑨行政安全部長官が行う改善勧告、是正措置命令、告発・懲戒勧告、過料の賦課の処理結果の公表についての事項、⑩個人情報保護施策の樹立及び施行に関する年次報告書の作成・提出に関する事項、⑪個人情報保護と関連して大統領または個人情報保護委員会委員長または委員２名以上が会議に付した事項、⑫その他、法令によって個人情報保護委員会が審議・議決する事項である（8条1項)。

そして、以上の事項を審議･議決するために必要な場合には、関係公務員、個人情報保護の専門家･社会団体、関連事業者に対して意見を聞き、関係機関等に対して資料などの提出を要求することができる（2項)。

(f)EU 基準による独立性の検討

個人情報保護法の制定において、EU の独立的個人情報保護機構の設立という基準を満たすか否かは、一つの大きな課題であった。そこで、「前 EU 適合性評価審査官に内部検討を受けた結果、この法案の推進体系[監督体系]がEUの監督機構独立性評価基準に適合しており『模範的な個人情報法制』であるとの評価を受けた」（2010 年 9 月）し、外交通商部が「法案は、韓 -EU・FTA の基本趣旨に違背せず、通商摩擦の可能性はないことを公文で確認した」[21]。EU 基準による推進体系独立性の検討の主要な項目及びその結果は、次の表 9 のとおりである。

21 행정안전부『개인정보보호법심사참고자료』(2010.12)31 頁。

表９　EU 基準による推進体系独立性の検討

EU 独立性基準	個人情報保護法	検討	
		卞 在 一 議員案	個人情報保護法
1. 監督機構の法的設立根拠	大統領所属の審議・議決機構である個人情報保護委員会（7 条）	○	○
2. 独立調査権保有	委員会が侵害行為の是正勧告、公表、意見聴取等（8 条）	○	○
3. 任期保障	委員長及び委員３年、１度に限り再任可能（7 条）	○	○
4. 免職条件明示	委員推薦、任期規定 (7 条)、紛争調停委員の免職制限（41 条）	○	○
5. 職務関連民事訴訟に対する免責特権	—	×	×
6. 国会による任命	国会５人推薦、大法院長５人指名を大統領が任命 (7 条)	○	○
7. 行政府と独立的な行政及び支援の確保 (人事、予算)	部処 (省庁) と独立した大統領所属で、人事、予算は別途（7 条）	○	△
8. 国会に対する定期報告義務	国会年次報告 (67 条)	○	○
9. 独立監督官の兼職禁止	常任委員任命 (7 条)	○	○

행정안전부『개인정보보호법심사참고자료』2010.12、31 頁。

（3）個人情報紛争調停委員会

①機能

従来の個人情報紛争調停委員会は、民間分野の紛争調停のみをその対象としており、また、調停の効力も民事上の和解にとどまっていた。これに対して、個人情報保護法では、その機能を、公共・民間にまで拡大するとともに、紛争調停の内容は、①侵害行為の中止、②原状回復・損害賠償その他必要な救済措置、③同一または類似の侵害の再発を防止するために必要な措置に関して調停案を作成し(47 条 1 項)、その調停内容が当事者によって受諾されたときには、裁判上の和解の効力を認めた（47 条 5 項)。

また、情報主体の被害・権利侵害が多数の情報主体に同じような類型で発生したときには、紛争調停委員会に、一括的な紛争調停 (集団紛争調停) を依頼・申請することができることを定めている（49 条)。

なお、迅速な紛争解決のために、紛争調停の申請を受け付けたときに、当事者にその内容を提示して調停前の合意を勧告することができる（46 条）。

公共機関は、相手方から紛争調停の通知を受けたときは、特別な事情がない限り紛争調停に応じなければならない（43 条 2 項）。

調停の処理期間は、原則として調停申請を受けた日から 60 日以内であり、やむを得ない事情がある場合には紛争調停委員会の議決で処理期間を延長することができる（44 条）。

②構成

個人情報紛争調停委員会は、従来よりも人数を増やして、委員長 1 名を含む 20 名以内とし、そのうちの 1 人は常任委員とする（40 条 2 項）。

委員は、次の各号の一に該当する者の中から行政安全部長官が任命または委嘱する。すなはち、①個人情報保護業務を管掌する中央行政機関の高位公務員団に属する公務員またはこれに相当する公共部門および関連団体の職にあるかまたはあった者で、個人情報保護業務の経験がある者、②大学または公認された研究機関で副教授以上またはこれに相当する職にあるかまたはあった者、③判事・検事または弁護士の職にあるかまたはあった者、④個人情報保護と関連した市民社会団体または消費者団体から推薦を受けた者、⑤個人情報処理者で構成された事業者団体の役員の職にあるかまたはあった者（3 項）である。委員長は、公務員でない委員の中から行政安全部長官が任命する（4 項）。

委員の任期は 2 年であり、一回に限って再任することができる（5 項）。紛争調停委員会は、紛争調停業務を効率的に遂行するために必要な場合には、調停事件の分野別に、5 人以内の委員で構成される調停部を置くことができ、調停部が紛争調停委員会から委任されて議決した事項は紛争調停委員会で議決したものとみなす（6 項）。

委員は、資格停止以上の刑を宣告されるか、心身の障害によって職務を遂行できない場合のほかは、その意に反して免職・解職されない（41 条）。また、委員の除斥・忌避・回避（42 条）についても規定して、その公正性を保障している。

6　個人情報保護法施行に向けての準備と今後の課題

（1）施行に向けての準備

個人情報保護の施行に向けて、現在、行政安全部は、次のような準備を進めている[22]。

---

22 행정안전부보도자료 2011 년 3 월 30 일、3 頁。

第一に、法律で委任している事項を具体化する施行令と施行規則の制定である。第二に、大統領所属に置かれる個人情報保護委員会及び同委員会の業務支援のための事務局設置の準備である。第三に、法律が定める新規制度の施行のための分野別指針・告示の制定、すなわち、個人情報処理に関する標準個人情報処理、機微情報・固有識別情報処理、個人情報流出通知制運営、公共機関個人情報影響評価運営、集団紛争調停制度運営などに関する個別指針の制定である。第四に、関連制度・法令の改善、自主規制及び教育･広報の活性化などを含む３年単位で樹立される個人情報保護基本計画 (行政安全部) と、毎年樹立される施行計画 (中央行政機関) の準備である。第五に、個人情報保護法の制定によって現在と変化するであろう点についての対国民キャンペーン活動の展開、具体的には、法令解説書の普及、公共機関・事業者に対する特別教育などである。そして、第六に、個人情報保護法制定後の後続措置を支援するために、個人情報の政策と技術の専門家で構成された「個人情報保護研究会」をこの４月に発足する予定である。

（2）監督機関の課題

個人情報保護法の制定経緯で見たように、監督機関の性格をどのようにするのかこそが、個人情報保護法制定の最大の難関であった。それこそが、今後の課題でもある。もっとも、監督機関として新設された個人情報保護委員会の業務と権限が未だ不明確であるために、その姿は現時点では、いまだ可変的である。

たとえば、個人情報保護委員会は、各部処 (省庁) が持っている調査権を持っていないだけでなく、紛争調停は紛争調停委員会が担当し、資料提出要求権は行政安全部長官が有しているのである (11 条)。

たしかに、もともとの政府案では、国務総理所属の審議委員会として構想され、その機能は主要事案を審議することであり、執行は各部処 (省庁) が担当し、行政安全部がそれを総括するという仕組みであったが、野党等との協議の過程で、個人情報保護委員会を大統領所属に格上げして、また、委員会の機能に議決機能を追加するとともに、年次報告書の国会提出という一部の執行機能も追加した。しかし、そのためにかえって、個人情報保護機構としての機能と役割に体系性がなくなり、その基本的な機能が不明確になってしまったことは否定できない。このために、「代案に規定されている個人情報保護委員会の場合、国際的基準やこれまで議論してきた水準に比べれば、保護機構の独立性と権限は不足している。独立性保障や権限などで見れば、個人情報保護のための独立した機構として十分な機能を果たすのは困難であると判断されるし、体系的かつ一貫した形態の個人情報保護機構と見るのも困難であるので、それは“妥協の産物”といわざるをえないものである[23]」とも評されている。

---

23 김일환、前掲論文、116 頁。彼は、望ましい個人情報保護委員会の形態と役割について、公共部門と民間部門の個人情報保護機構は、その対象と手段が多くの点で異なるので、「公共部門の個人情報保護監督機構は“大統領傘下の独立行政庁としての委員会 (合議制)”の組織形式をとるのが望ましく、民間部門の場合には当該民間領域で自立規制を施行させると同時に行政安全部をはじめとする処分権と裁決権などは当該部処の長が行使するシステムが最も適合的である」と主張している (김일환、前掲論文、116 頁)。

これに対して、法案の担当者は、次のように反論している。

すなわち、「委員会の独立性の問題は、行政府と委員会の関係の問題に置換することができ、日常化している個人情報侵害の侵害問題を解決するために、力量を何処に結集するかという選択の問題である。新たに出帆する個人情報保護委員会が行政府の政策力量を活用できずに、部処（省庁）と対立・統制するようになる場合、国家社会の侵害対応力は非常に弱まるであろう。政府における個人情報保護業務が占める政策の優先順位、資源の配分における非常に貧弱な水準（政府部処予算約 200 億、人数約 40 名）を考慮すれば、初期の個人情報保護委員会と行政安全部、各部処の関係は、共生と協力の基調を維持しなければならない。……国家公権力による個人の私生活保護、安全な生活確保を最優先課題と見る場合には、推進体系は行政府から独立した独自的な意思決定権と規制権を持つ独立行政官庁の形態と権限を整えることが急務ではあるが、一方、毎日繰り返される事業者の個人情報保護が最優先課題になる場合には、個人情報侵害の事前予防と事後処罰の効率的業務処理が鍵になる。……個人情報保護業務の大部分が部処中心の政策樹立・執行を主として推進（17 の部処、38 の法律）されている現実を勘案するとき、既存の体系を補強する次元から推進体系を設計して、既存制度の経路の依存性を最大限活用しなければならない。個人情報保護委員会が基本的に政策決定及び執行の一部機能を重点的に遂行するようになると、これと関連して、紛争調停、被害救済機能をどのように有機的に結合させるべきかが新たな論点になりうる。紛争調停は、準司法的判断を基本としているので、現行のように委員会及び行政安全部から独立性を備えるようにしている[24]」と説明している。

少なくとも現時点では、①民間部門における自主規制強化のシステム化の問題、②個人情報保護法と個別法律との間の整合性の問題[25]、③個人情報保護委員会と個人情報紛争調停委員会との関係及び協力の問題については、今後も検討する必要があることだけは明らかに指摘できるであろう。

---

24 김상광「개인정보보호법 제정 쟁점 토론자료」『“ 정보인권의 법적보장과 구체화 ” 공동학술세미나』(국가인권위원회인권정책과、2010 年)125 ～ 126 頁。

25 2011 年 3 月 24 日に行った国会立法調査処のチョ・ギボム（조규범）立法調査官へのインタビューにおいて、チョ立法調査官は、「個人的な見解として、まず、個人情報の保護は、基本的な法律と細部的な法律が並行してこそ成果があり、大統領所属の監督機関が設置されても、これと有機的に連結される様々な分野で個人情報を担当する機構が存続してはじめて効果的に機能するであろう」と述べたが、将来において再度、韓国における個人情報保護制度の監督機関に関する調査を行うときには、この観点からの総合的な調査が必要となるであろう。

7　結びにかえて

本稿を執筆するために、3 月 23 日から 26 日まで韓国の地で、個人情報保護についての専門家に対するインタビュー調査を行った。

インタビューした相手は、個人情報保護法の立案制定に直接かかわった行政安全部個人情報保護課のキム・サングァン (김상광) 書記官、その法案の審査などを担当した国会立法調査処のチョ・ギボム（조규범）立法調査官、韓国における個人情報保護制度の監督機関の一つである個人紛争調停委員会委員長をしている金洙謙・東国大学法学部長、現時点では事実上、個人情報保護の監督に関する業務を一手に引き受けている韓国インターネット振興院 (KISA) 情報保護本部のパック・グァンジン（박광진）本部長とキム・ミンソプ（김민섭）責任研究員、そして外部の中立的な有識者として、前 KISA の主任研究員で、現在は韓国ハッキング協会事務局長である朱徳奎博士である。

この人選は、韓国における個人情報保護制度の監督機関の実態について調査研究するためには、考えられる最高の人選に近いものであったといえよう。しかしながら、インタビュアー自身の学識不足と韓国語能力の未熟さもさることながら、韓国の個人情報保護法が国会を通過したばかりで、未だ施行令もできていない段階でのインタビューであったために、今回の調査の目的である監督機関の実態については、時期的な限界を強く感じざるを得なかった。当然、新設される個人情報保護委員会の事務局もいまだ構成されていないだけでなく、インタビューに応じていただいた方々は、いずれも個人情報保護法の施行に向けて精力を傾けざるを得ない立場にあるので、まさに多忙極まりない時期であった。

そのため、今回のインタビューは必ずしも本稿に十分に反映することができなかったことをお許しいただくとともに、貴重な時間を割いていただいた方々に心より御礼を申し上げる次第である。

今回の韓国での調査において献身的な協力をしてくれた朱徳奎博士は、「個人情報保護委員会は、大統領所属の機関で、独立性を有していると見ることができるものの、国会、大法院からそれぞれ 5 人を推薦して大統領が任命するという委員の選出方法を見るとき、放送通信委員会などと比べて専門性を担保するよりは政治性を帯びる可能性が大きい。このような機構は、経験則上、円滑な行政執行が困難になりやすので、委員会の専門性を担保するためには、事務局の役割が大変重要になる。また、個人情報保護法は、その 40 条で、行政安全部長官は、個人情報紛争調停委員会の事務局運営などの業務を支援するために、大統領令で定めるところにより、専門機関を指定することができると規定している。現在の個人情報紛争調停委員会の業務支援の事務局は、韓国インターネット振興院（KISA）に置かれているが、そもそも、KISA は情報通信網法に基づいて民間の事業者を規制するために設置された専門機関であるので、今のままの体制では、公共機関及び手記情報に対する個人情報保護業務にまで拡大された個人情報保護法上の専門機関の役割を果たすには不十分であろう」と語ったが、新設される個人情報保護委員会が個人情報保護制度の監督機関としての役割を十分に発揮するためには、その事務局がどのような形で構成されるのかが、最初の関門になりそうである。

あとがき

筑波大学法科大学院　藤原　靜雄

1　本調査の目的と個人情報保護制度の監督機関

個人情報保護の問題は、経済、人権、地方自治等、様々な側面から検討することが必要であるが、地球規模でのネットワーク社会の進展と経済のグローバルな展開の中で、国際的な協調が求められていることもあり、わが国の制度について他国に理解してもらうとともに、他国の制度を正確に理解することがますます重要な課題となっている。

国際社会における個人情報保護制度の相互理解という観点からは、EU 諸国における個人情報保護に係る第三者機関（いわゆるプライバシー・コミッショナー）やカナダ、オーストラリア、ニュージーランド等のプライバシー・コミッショナーが重要な役割を果たしているが、他方、アメリカのようにコミッショナー制度を持たない国もある。また、韓国のようについ最近の法改正でコミッショナー制度を導入した国もある。わが国では、第三者機関については「国際的な整合性も踏まえ、中長期的課題として検討することが必要」とされている（「個人情報保護に関する取りまとめ（意見）（平成 19 年 6 月 29 日国民生活審議会)」）ところであるが、わが国でも、社会保障・税に関わる番号制度における個人情報保護の第三者機関の設置が議論されているおりでもあり、諸外国の制度の運用の実態にまで踏み込んだ研究が必要なように思われる。第 1 章、第 2 章は、そのような角度から、わが国の監督機関の在り方を考える上で有益であると思われる国々について、実務の実態を知るという観点を重視し、調査研究を行ったものである。

2　各国の監督機関の特色と本調査研究

本調査研究で取り上げた国々の監督機関の特色は、筆者の個人的な印象であるが、単純化して言えば以下のようなものである。

イギリスの個人情報保護に関する直接的な監督機関は、情報コミッショナーである。これは、データ保護コミッショナーが情報自由法についても所管するようになったことによる名称変更である。イギリスの監督機関にかかる制度も他の EU 諸国とほぼ同じであるが､情報コミッショナーが議会でなく､政府から指名され､その手続（コミッショナー候補者の公募、利害関係者（stakeholders）によって構成されるパネルでの候補者の絞り込み等）に特徴がある。

フランスは、EU の諸制度に係る議論をリードする国と言ってよいと思われるが、この国には、個人情報保護にかかる第三者機関として、情報処理及び自由に関する全国委員会（Commission nationale de l'informatique et des libertés)、略称クニール（CNIL）が存在する。クニールはフランスにおける初めての独立行政機関でもあり、権限の強い行政機関として著名である。

フランスと同様、EU の個人情報保護施策に大きな影響力をもつドイツは、個人情報保護を重視する国であるが、連邦制をとる国であり、公的部門の法の運用については、連邦監察官が大きな役割を演じ、民間部門の法の運用については、各州の監督官庁（州の監察官ないし内務省の担当部局）が重要な役割を果たしている。

国レベルにおいて世界で初めて個人情報保護法を制定したスウェーデンでは、第三者機関としてデータ保護検査院が存在するが、これはスウェーデンを発祥の地とするオンブズマン制度の一つ、すなわち分野別オンブズマンとして理解すべきものである。

米国には、個人情報やプライバシーに関して、全般的に所轄する統一的な第三者機関は存在しない。個人情報保護に関しては分野別に個別の法律が定められているため、監督機関も各個別法の規定によってそれぞれ定められている。これが米国の特色である。ただ、そのような仕組みの中でも、民間部門の監督機関としてのFTC（Federal Trade Commission）を、代表的な監督機関としてあげることができる。

カナダは連邦制をとる国であるが、連邦レベルの監督機関はプライバシーコミッショナーであり、これは公的部門と民間部門の両方の法律を所管する。コミッショナーは、カナダ連邦の個人情報保護に関する監視・紛争処理機関であり、個人からの問い合わせ・苦情をもとに、不服申立ての案件を扱うとともに、自己付託によって強制調査を行い、不服申立てを自らすることもできる。この点がプライバシーコミッショナーの特徴であるとされている。なお、カナダには、オンタリオ州等、特色ある監督機関をもつ州が存在する。

オーストラリアは、情報公開と個人情報保護の両者を統括する連邦インフォメーションコミッショナーの下に、連邦プライバシーコミッショナーと連邦情報自由（FOI）コミッショナーをそれぞれ置き、現在、プライバシー保護法の改正を進めている最中である。

韓国では、2004年以来続いてきた長い議論に1つの区切りを付ける形で、本年（2011年）3月29日に、公的部門・民間部門を通じての個人情報保護にかかる一般法である「個人情報保護法」（2011年9月30日から全面施行される予定）が制定された。監督機関の在り方が、法制定過程の最大の争点であったが、同法で設置されることとなった個人情報保護委員会は、大統領府に属する独立性の高い機関として位置づけられ、主として、個人情報保護政策の審議、議決を任務とする。ただし、個人情報保護業務の総括・調整は行政安全部が行い、個別法の執行業務は個別法を所管する各中央行政機関が遂行する。なお、韓国には、救済機関として別に個人情報紛争調停委員会が存在する。

以上みてきたように、各国はそれぞれの法的、文化的、歴史的事情を背景に、各自の個人情報保護法制を発展させ、その中での監督機関の在り方を模索してきたと言える。EU、英連邦諸国といった枠組みでの共通点もあるが、EUの中でさえ、微妙な差異が存在する。しかし、他方で多くの共通点が存在することも事実である。

3　わが国の議論への示唆

わが国としても、国際社会の一員として、また、わが国の利益を確保するために、わが国から情報の発信をし、個人情報保護にかかる国際ルールの形成に参加する必要性があると思われるが、その際には、主要先進諸国には独立した第三者機関が存在するという事実を正面から受け止める必要があろう。情報の権利分立という考え方からは、利用と監視は分離することが望ましいと言えるからである。

わが国でも、今後、税・社会保障を超えた一般的な第三者機関の在り方について検討を進めていく必要があろうが、その際には、わが国の主務大臣制の下でいかに制度を構築するかという論点（韓国での議論の経緯の分析の必要性）、憲法構造との関係での議論（オンブズマン制度の1つであるスウェーデンの議論との比較の必要性）、第三者機関の長（あるいは委員）の選任手続の在り方（イギリスの透明性を模索する手続の実態分析の必要）、国と地方との関係（連邦制を採用する国と採用しない国の制度の比較）、第三者機関が有すべき権限の問題（フランスやカナダの制度の運用の実態）、他の救済機関との関係（韓国の制度の分析の必要性）など、議論を深めるべき論点は多い。

本調査研究が今後議論を深化させていくための一助になれば幸いである。

諸外国等における監督機関の比較

	法律名 （制定年）	主な監督機関名 （設置年）	事務局職員数	予算 （百万円）	法的位置付け	委員数 委員構成	他機関との協働	相談･苦情処理 受付数･回答数 方法	検査･捜査 立入検査件数 根拠	救済･制裁 命令･勧告･報告徴収等	救済･制裁 罰則 根拠	救済･制裁 不服申立 司法救済	法案等への意見提出	国際協力
イギリス	1998 年データ保護法（1984 年データ保護法を改正）	情報コミッショナー（2001 年、前身は 1984 年）	３５２ (2010年末)	２，４００	女王から独立した単独法人	１	n/a	３３，２３４件 ３２，７１４件 回答（苦情） ２１２，０００件（電話）	１６件 （監査）	執行通知１５件 金銭的制裁２件	訴追７件 有罪２件	執行通知に対して審判所に申し立てる権利		情報コミッショナーが国際連携を行っている
フランス	情報処理、情報ファイル及び自由に関する法律（1978年/2004年改正）	情報処理及び自由に関する全国委員会（1978 年）	１５０	１，６９０	独立行政委員会	１７	特に行政文書へのアクセスに関する委員会との協働	４，８００件	３１０件	法令遵守通知 ４４６件 警告 ２５件	３４件の罰金	行政裁判所への申し立てが可能	７件	法・国際・IT 専門課が担当
ドイツ	連邦データ保護法（2009年最終改正）	連邦データ保護・情報自由監察官（1977 年）	９１	１，００３	連邦議会によって選任され、法にのみ従う	１	連邦ネットワーク庁，連邦情報セキュリティ室などと協力	６，０８７件 （2010 年）	n/a	n/a	n/a	n/a	n/a	29 条委員会、欧州データ保護会議、国際データ保護・プライバシーコミッショナー会議等に参加
スウェーデン	個人データ法（1973年/1998年改正）	データ保護検査院 （1973 年）	４３	４７０	独立行政委員会 （オンブズマン制度に類似）	５ 国会議員、大学教授、IT専門家、地方議員	政府の他機関との情報共有	約２，１００通 （メール） 約５，３００件 （電話） ３３２件回答	２１４件開始 ２１０件終了	—	０件	行政裁判所への申し立てが可能	１７件	国際法律専門官が担当
アメリカ	連邦プライバシー法（1974 年） 公正信用報告法（FCRA） 金融サービス近代化法（GLBA） 児童オンラインプライバシー保護法（COPPA）等	中心的なのは、連邦取引委員会（FTC） （1915 年） ＊その他 Office for Civil Rights(OCR), Department of Health and Hu-man Services (HHS) など多数の機関が関わっている	およそ３０ （プライバシー及び個人識別保護局のみ）	１３ （個人情報保護、プライバシー保護関係のみ）	独立行政委員会	5	州との協力など	3,300,000件 （2009 年度）	n/a	判決　１０２件 （消費者保護） 民事罰　１１件 行政命令１６件	N/A	n/a	３８（議会担当オフィスの議会での testimony の数、2009-2010（第 111 国会）	他国の法執行機関と連携
カナダ	連邦プライバシー法 個人情報保護及び電子文書法（PIPEDA 法）	プライバシーコミッショナー （1982 年）	１５８ （フルタイムの人数に換算）	１，８１１	特殊オンブズマン	１	州のプライバシーコミッショナー、他の連邦機関と連携	５，１１０件 （問い合わせ･苦情） ８９６件 （不服申立て） （公的･民間合計）	N/A	判断（Findings） １，７４１件 （公的･民間合計）	n/a	n/a	法案のレビュー　１０ 議会委員会への出席　１４	コミッショナーの直下にある国際担当部門が担当
オーストラリア	連邦プライバシー法 （1988年） 連邦情報コミッショナー法 （2010年）	連邦情報コミッショナー（2010年）、連邦プライバシーコミッショナー（1988年）	７７ （2011年）	６４０	豪州総督が任命	３ （コミッショナーは３名だが互いに独立）	n/a	２０，９３５件 （電話） ６，８４８件 （苦情申立）	n/a	n/a	n/a	n/a	n/a	APEC Data Privacy Pathfinder, OECD, Asia Pacific Privacy Authorities, International Conference of Data Protection and Privacy Commissioners に出席し協力している。
韓国	個人情報保護法（2011年）	個人情報保護委員会 （2011年）	未設立	未設立	諮問機構と行政機構の両者の性格を有する	１５ 大統領･国会･大法院長が5名ずつ選出･指名	未設立	未設立	未設立	未設立	未設立	未設立	未設立	未設立