資料２－１

諸外国等における個人情報保護制度の運用実態に関する検討委員会･報告書

平成 19 年 1 月

はじめに

平成 17（2005）年 4 月に個人情報の保護に関する法律（以下「個人情報保護法」という）が全面施行されてから 2 年近くが経過した。この間、いわゆる「過剰反応」と報ぜられた問題をはじめ、国民、事業者のこの法律に対する反響にきわめて大きいものがあったのは周知のところである。この法律は、わが国ではじめて、民間部門における個人情報の取扱いを包括的に規律するものであり、いわば新たな地平に足を踏み入れたものである。その結果、わが国の国民の個人情報保護意識を著しく高めるとともに、これまで意識されてこなかった新たな問題を浮かび上がらせることとなった。過剰反応と呼ばれる現象にも実はこのようなものが多いように思われるが、まずは、法の施行状況の正確な把握が肝要である。

個人情報保護法の成立を受け、同法 7 条 1 項に基づき策定された「個人情報の保護に関する基本方針」（平成 16 年４月２日閣議決定）では、内閣府は、法の施行状況について、全面施行後３年を目途として検討を加え、その結果に基づいて必要な措置を講ずること、このため、国民生活審議会は、法の施行状況のフォローアップを行うこと、とされている。これらを踏まえ、第 20 次国民生活審議会個人情報保護部会（部会長：野村豊弘学習院大学大学院法務研究科教授）では、現在、平成 19 年夏の取りまとめに向けて、個人情報保護法の施行状況の評価及び個人情報保護制度に関する検討を行っている。本検討委員会は、同審議会の検討に資するため、審議会での主な検討課題に即して、諸外国等の個人情報保護制度の運用実態を明らかにするために設けられたものである。

本検討委員会では、わが国の問題を考える一助にするために、国民生活審議会が既に公表している検討課題の項目を中心に、イギリス、フランス、ドイツ、アメリカに加え、OECD、EU、APEC について調査を行った。調査国・機関、ヒアリングの項目等は上記の目的を意識して選択したものである。報告書の記述の順序及び内容もその旨を意識したものとなっている。報告書の分担は執筆分担に記載のとおりであるが、どの国・機関の記述についても、全委員による検討を経ている。また、報告書全体の内容の検討を、堀部顧問と調整しつつ、藤原が行っている。

各委員及び堀部顧問には、ご多忙の中、集中的に議論に参加し、報告をまとめていただいたことに深謝する次第である。また、比較的短期間に豊富な内容の調査、議論を行えるような環境を設定していただいた、内閣府個人情報保護推進室、（株）野村総合研究所のスタッフの方々にもこの場を借りて御礼申し上げたい。

本報告書が、わが国の問題意識を踏まえた実態調査として、国民生活審議会等の場で活用されることを祈念するものである。

平成 19 年 1 月

検討会委員長
筑波大学法科大学院教授　藤原静雄

諸外国等における個人情報保護制度の運用実態に関する検討委員会

委員名簿・執筆分担

（敬称略　50 音順）

下井　康史	新潟大学大学院実務法学研究科助教授 フランス、OECD について執筆
中原　茂樹	大阪市立大学大学院法学研究科助教授 ドイツ、EU について執筆
野口　貴公美	法政大学社会学部、同大学大学院政策科学研究科助教授 アメリカ、APEC について執筆
○藤原　靜雄	筑波大学法科大学院教授 全編について査読
※堀部　政男	中央大学大学院法務研究科教授 イギリスについて執筆、及び全編について査読

（○は委員長、※は顧問。）

目　次

諸外国等における個人情報保護制度の運用実態（概要）

Ⅰ.諸外国

１．イギリス

（１）個人情報保護制度の概要

イギリスでは、1984 年に公的部門と民間部門の双方を対象とする「データ保護法」が制定された。1998 年には、1995 年の EU データ保護指令の要求事項に対応するため、現在の「1998 年データ保護法」が新たに制定された。公的部門と民間部門の双方を監督する独立した機関として、情報コミッショナーが設置されている。

（２）「個人情報保護に関する主な検討課題」関連項目に即した状況

① いわゆる「過剰反応」（誤解）に対応した第三者提供制限の例外事由

個人データは、原則として、次の条件の一つが満たされる場合を除き、取り扱ってはならないこととされている。

ｱ)データ主体が当該取扱いに同意

ｲ)データ主体を当事者とする契約のために必要

ｳ)法的義務の遵守に必要

ｴ)データ主体の重要な利益の保護のために必要

ｵ)司法のため及び法規等による権能の行使のために必要

ｶ)データ管理者の適法な利益のために必要

イギリスでは、現在でも「過剰反応」が見られる（現地での聞き取り調査による）。このため、監督機関では、具体例と正しい考え方をホームページで公表するなど、法律の的確な理解に向けて啓発活動を行っている。

② 自治会や同窓会等の取扱い

地域社会や同窓会についても、個人情報の取扱いに関する義務は同様に適用される。イギリスでは、近隣住民の組織や同窓会が名簿を作成することはある（現地での聞き取り調査による）。

③ 「個人情報」の定義

「個人データ」は、「(a) 当該データから、又は (b) データ管理者が保有し、又は保有することになる可能性のある当該データその他の情報から、識別できる生存する個人に関するデータであって、かつ、当該個人に関する意見の表明及び当該個人につ

いてデータ管理者その他の者の意図の表示を含む」と定義されている。

④ センシティブ情報に関する規定

センシティブ情報は、「人種的・民族的出自、政治的意見、宗教的信条、労働組合への加入、健康状態、性生活、犯罪の前科・容疑、犯罪・容疑の手続・処分・判決」と定義されている。

センシティブな個人データの取扱いに当たっては、少なくとも 10 の条件のうちの 1 つが満たされなければならず、そのうちの 1 つである「データ主体の同意」は、「明示の」同意でなければならないとされている。

⑤ 小規模事業者の取扱い

小規模事業者であっても、個人情報の取扱いに関する義務は同様に適用される。小規模事業者の個人情報保護の取組は遅れている（現地での聞き取り調査による）。

⑥ 個人情報の目的外利用の防止措置

個人データは、特定のかつ適法な目的のためにのみ取得されなければならず、その目的と適合しない態様でさらに取り扱われてはならないとされている。目的外利用かどうかは、その情報が利用される状況と目的によって判断される（現地での聞き取り調査による）。

また、本人は、損害又は苦痛を与えるおそれのある取扱いを停止させる権利、及びダイレクトマーケティングの目的のための取扱いを停止させる権利を有するとされている。個人情報を使ってダイレクトマーケティングを行う場合は、事前に本人の確認を取ることが求められる場合もある（現地での聞き取り調査による）。

⑦ 市販の名簿の管理

広く頒布されている名簿については、法律上、他の個人情報の取扱いと同様に規制されている。ただし、電話帳に記載されている情報は、本人から公開を前提として収集されているため、電話帳については、運用上、特段の管理は必要とされていない（現地での聞き取り調査による）。

⑧ 個人情報の取得元の開示に関する措置

1998 年データ保護法では、本人のアクセス権が規定されている。その中で、個人情報の取得元についても、本人は開示を請求できることとされている。

⑨ 個人情報の利用停止・消去に関する措置

1998 年データ保護法では、本人のアクセス権が規定されており、その中で、損害又

は苦痛を与えるおそれのある取扱いを停止させる権利、及びダイレクトマーケティングの目的のための取扱いを停止させる権利等を有するとされている。

⑩ 国際的な情報移転に関する規定

原則として、十分な保護水準を確保していない第三国へのデータ移転が制限されている。具体的には、「個人データは、ヨーロッパ経済地域以外の国又は地域が個人データの取扱いに関しデータ主体の権利及び自由について十分な水準の保護を確保している場合を除き、その国又は地域に移転してはならない」との原則が規定されている。

⑪ EU データ保護指令に対する対応状況

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

⑫ 第三者機関の概要

官民双方を監督する独立した監督機関として、情報コミッショナーが設置されている。2005～2006 年度における全職員数は、245 人である（データ保護以外の担当者を含む）。同コミッショナーの機能は、①情報の適切な取扱いの推進、②データ保護に関する啓発、③データ管理者の行動規範の作成・承認、④情報の届出の管理、⑤法令遵守の調査、⑥法令違反に対する通知の発出、⑦犯罪の起訴、⑧議会への報告等を行うことである。

⑬ 死者に関する個人情報の保護

1998 年データ保護法では、「生存する個人」という概念が使われているため、本法上、死者は何の権利も認められていないといえる。

1990 年保健記録法では、死者の保健記録に関するアクセス権について規定されている。同規定では、患者が死亡した場合、その患者の遺言執行者や遺産管理人等は、保健記録の保有者に対してアクセスを請求することができるとされている。

⑭ 直接処罰等の実効性担保の措置

1998 年データ保護法では、個人データの不法な取得等について、「何人も、データ管理者の同意がなければ、故意又は認識過失で、（a）個人データ若しくは個人データに含まれる情報を取得し若しくは提供し、又は（b）個人データに含まれる情報について他の者に提供するようにさせることをしてはならない。」とされている。これは違反者を直接処罰する規定であり、法定刑は上限 5,000 ポンド（約 115 万円）の罰金である。2005～2006 年度では、個人データの不法な取得に関する 6 件を含め、16 件の訴追が行われた。

２．フランス

（１）個人情報保護制度の概要

公的部門と民間部門の双方を監督する独立行政委員会として、情報処理及び自由に関する国家委員会（CNIL）が設置されている。

フランスでは、EU データ保護指令に対応するため、公的部門と民間部門の双方を対象とする「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」が、2004 年に大きく改正された。

（２）「個人情報保護に関する主な検討課題」関連項目に即した状況

① いわゆる「過剰反応」（誤解）に対応した第三者提供制限の例外事由

個人情報を取り扱う場合は、本人の同意を得るのが原則とされている。ただし、次の要件の一つが満たされる場合は、原則として取扱いが許される。

ｱ)取扱責任者の法的義務の遵守　ｲ)本人の生命を保護する目的

ｳ)公役務の任務の遂行　　ｴ)本人が当事者である契約のために必要

ｵ)正当な利益の実現に資するもので、本人の利益や基本的権利自由を害さない

フランスでは、「過剰反応」が見られるとの情報は得られなかった（現地での聞き取り調査による）。

② 自治会や同窓会等の取扱い

義務の対象である「個人情報取扱責任者」は、「法令の規定が明示的に定める場合を除き、処理の目的と方法を決定する個人、又は、公的な機関又は部局若しくは組織」と定義されている。

地域社会や同窓会についても、個人情報の取扱いに関する義務は同様に適用される。

③ 「個人情報」の定義

「個人情報」は、「自然人に関するあらゆる情報のうち、識別番号又は個人に固有の一若しくは複数の要素を参照することで、直接又は間接に個人を識別し又は識別可能なもの」と定義されている。

なお、「個人を識別し得るか否かを判定するには、取扱責任者その他すべての人々が保有している手段、又は、アクセス可能な個人識別可能手段のすべてについて考慮すべき」とされている。

④ センシティブ情報に関する規定

センシティブ情報は、「人種・民族的起源、政治的、哲学的又は宗教的意見、労働組合への所属が直接又は間接的に明らかになる個人情報、又は、健康若しくは性生活に

関する個人情報」と定義されている。

センシティブ情報の収集・取扱いは、原則として禁止されているが、本人の明示的同意がある場合等は例外とされている。

⑤ 小規模事業者の取扱い

小規模事業者であっても、個人情報の取扱いに関する義務は同様に適用される。小規模事業者の個人情報保護の取組は遅れている（現地での聞き取り調査による）。

⑥ 個人情報の目的外利用の防止措置

情報処理、情報ファイル及び自由に関する法律では、個人データは、収集の目的が特定され、明白・正当であるとともに、収集後にこの目的と相容れない手法で取り扱われないことが原則であるとされている。

また、本人は、情報取扱責任者に対し、保存期間が徒過していたり、収集や利用が禁止されている自己の個人情報について、状況に応じ、その利用停止・消去を求めること等ができるとされている。

業界団体で作成されている「ダイレクトメールの送信を拒否することを明示した者」のリストが目的外利用防止に一定の役割を果たしている（現地での聞き取り調査による）。

⑦ 市販の名簿の管理

広く頒布されている名簿については、法律上、他の個人情報の取扱いと同様に規制されている。ただし、電話帳に記載されている情報は、本人から公開を前提として収集されているため、電話帳については、運用上、特段の管理は必要とされていない（現地での聞き取り調査による）。

⑧ 個人情報の取得元の開示に関する措置

情報処理、情報ファイル及び自由に関する法律では、「あらゆる人は、自己の個人情報の取得元に関して個人情報取扱責任者が保有している情報につき、アクセス可能な情報提供を得るために、当該責任者に質問することができる」とされている。

⑨ 個人情報の利用停止・消去に関する措置

情報処理、情報ファイル及び自由に関する法律では、「何人も、自己の身元を証明した上で、情報取扱責任者に対し、不正確、不完全、不明確、又は、保存期間が徒過し、収集や利用、提供又は保存が禁止されている自己の個人情報につき、状況に応じ、その訂正、修正、更新、利用停止、又は、消去を求めることができる」とされている。

⑩ 国際的な情報移転に関する規定

情報処理、情報ファイル及び自由に関する法律では、情報取扱責任者がEU非加盟国に個人情報を移転できる場合は、原則として、対象国が、個人情報の取扱いに関し、プライバシーや基本的権利に対する十分な水準の保護を確保している場合に限定されている。

⑪ EUデータ保護指令に対する対応状況

EUデータ保護指令に対応するため、主に以下の点について改正が行われた。

ｱ)個人情報の定義において、個人識別可能手段のすべてを考慮すべきとした

ｲ)個人情報取扱いの範囲を拡張

ｳ)個人情報の取扱いに関する諸原則を明示

ｴ)個人情報収集に当たっては、原則として本人の同意を取得

ｵ)センシティブ情報を例外的に収集できる場合を明記

⑫ 第三者機関の概要

官民双方を監督する独立行政委員会として、情報処理及び自由に関する国家委員会（CNIL）が設置されている。同委員会は17名の委員で構成されており、2006年12月現在の職員数は85人である。同委員会の機能は、①情報の取扱いの届出・許可の管理、②義務違反に対する制裁、③苦情処理、④助言、⑤違法行為の告発、⑥調査及び物件収集、⑦政府及び民間団体への助言、⑧重大・急迫時の裁判所への安全保護措置の命令要求等を行うことであり、強力な規制権限を有している点が特色である。

⑬ 死者に関する個人情報の保護

情報処理、情報ファイル及び自由に関する法律では、死亡原因を証明するために作成された情報を含め、死者に関する情報は、当該個人が、生前に書面で拒否した場合を除き、情報処理の対象となり得るとされている。また、訂正請求の一環として、死者の相続人は、死者に関する情報の更新をするよう情報取扱責任者に請求することができ、この請求があった場合、情報取扱責任者は、必要な措置をとったことを無料で請求者に証明しなければならないとされている。

基本的人権は生存する人間だけに適用されるため、死者の情報は保護の対象外である（現地での聞き取り調査による）。

⑭ 直接処罰等の実効性担保の措置

情報処理、情報ファイル及び自由に関する法律では、詐欺的又は不誠実、不正な手段で個人情報を収集する行為については、5年の拘禁及び30万ユーロ（約4,650万円）の罰金の刑事罰が定められている。

個人情報の漏洩が、本人の尊厳や私生活における静穏を侵害した場合については、5年の拘禁及び30万ユーロの罰金（故意によらない場合は軽減）の刑事罰が定められている。

また、違反があった場合、情報処理及び自由に関する国家委員会は、取扱責任者に対し、警告を発することや、違法な取扱いの中止を指示することができ、この指示に従わない者には、30 万ユーロを上限とした総売上額の最大 5%等の過料を科すことができる。

2005年からの18ヶ月間では、116件の注意、94件の勧告、7件の制裁が行われた（現地での聞き取り調査による）。

３．ドイツ

（１）個人情報保護制度の概要

ドイツでは、1977 年、公的部門及び民間部門の双方を対象とする「連邦データ保護法」が制定され、1990 年、2001 年に大幅な改正が行われている。連邦制が採用されているため、連邦の制度とは別に、各州においても個人情報保護に関する法制度が整備されている。連邦レベルでは、連邦の公的機関及び鉄道、郵便、情報通信分野の民間事業者を監督する機関である、データ保護監察官が設置されている。州レベルでは、州の公的機関及び一般の民間企業の監督が行われているが、その仕組みは州によって多様である。

（２）「個人情報保護に関する主な検討課題」関連項目に即した状況

① いわゆる「過剰反応」（誤解）に対応した第三者提供制限の例外事由

個人データの提供等は、原則として、次のいずれかの場合に許されるとされている。

ｱ)本人との契約や類似の信頼関係に資する場合
ｲ)責任機関の正当な利益を守るために必要な場合
ｳ)データが一般にアクセス可能か、公表が許されている場合
ｴ)第三者の正当な利益を守るために必要な場合
ｵ)危険の防止等に必要な場合
ｶ)宣伝や市場調査、世論調査のために限られたデータが取り扱われる場合（ただし、本人が異議を申し立てた場合は、提供等は許されない）
ｷ)研究施設の利益のために、学術研究の実施について必要な場合

ドイツでは、1977 年に連邦データ保護法が施行された際、「過剰反応」が見られた。これについては、個別の事案ごとに議論が行われ、解決が図られた（現地での聞き取り調査による）。

② 自治会や同窓会等の取扱い

同窓会についても、個人情報の扱いに関する義務は同様に適用される。ドイツでは、同窓会が名簿を作成することはある（現地での聞き取り調査による）。

なお、ドイツでは、個人情報の個人的・家庭的な利用は法律の規制の対象外とされている。

③ 「個人情報」の定義

「個人データ」は、「特定の又は特定され得る自然人（本人）の人的又は物的状況に関する個々の言明」と定義されている。

④ センシティブ情報に関する規定

「特別な種類の個人データ」は、人種的及び民族的出自、政治的意見、宗教的又は哲学的な信条、労働組合への加入、健康又は性生活に関する事項とされている。

「特別な種類の個人データ」が収集され、取り扱われ、又は利用される限り、同意は、さらに明示的に、当該データと関連付けられなければならないとされており、このような同意がない場合は、一定の例外を除き、データの収集等は許されていない。

⑤ 小規模事業者の取扱い

小規模事業者であっても、個人情報の取扱いに関する義務は同様に適用される。小規模事業者の個人情報保護の取組は遅れている（現地での聞き取り調査による）。

⑥ 個人情報の目的外利用の防止措置

連邦データ保護法では、個人データの収集に当たっては、データが取り扱われ、利用される目的が具体的に確定されなければならないとされている。

宣伝活動や市場調査、世論調査の目的のため、集団の構成員に関する限定されたデータが取り扱われる場合は、原則として、目的外利用が許されているが、本人が責任機関に異議を申し立てた場合は許されないとされている。

また、本人が、責任機関に異議を申し立て、かつ、本人の保護に値する優越的な利益がある場合、個人データの利用は許されないとされている。

⑦ 市販の名簿の管理

データが一般にアクセス可能である場合については、本人の保護に値する利益が明らかに優越する場合を除き、以下の取扱いが可能とされている。

ｱ)自己の業務目的の遂行のための収集、蓄積、変更、提供及び利用

ｲ)自己の業務目的の遂行のための収集時に特定された目的外での提供・利用

ｳ)信用調査機関、名簿取引、市場調査及び世論調査に役立つ場合、提供を目的とする、業務上の収集、蓄積及び変更

⑧ 個人情報の取得元の開示に関する措置

連邦データ保護法では、本人は、自己に関して蓄積されたデータの情報源や、データが譲渡される受領者又は受領者の範疇、蓄積の目的について、開示を求めることができるとされている。

⑨ 個人情報の利用停止・消去に関する措置

連邦データ保護法では、個人データは、原則として、いつでも消去又は利用停止（封鎖）することができるとされており、当該データの蓄積が許されない場合等は、原則

として消去されなければならないとされている。

また、本人が、責任機関に異議を申し立て、かつ、本人の保護に値する優越的な利益がある場合、個人データの利用は許されないとされている。個人データの正確性が本人によって争われ、かつ、正確かどうかが確定できない場合は、原則として、利用停止等が行われなければならないとされている。

なお、本人は、事業者が広報活動を目的とする場合等において、自身の個人情報の利用停止・消去の請求の権利を有している（現地での聞き取り調査による）。

⑩ 国際的な情報移転に関する規定

連邦データ保護法では、欧州共同体法の適用を受ける活動の枠内において、他の EU 構成国内にある機関等以外の機関に個人情報を提供することは、当該機関に適切なデータ保護水準が存在しないときであっても、例外的に許される場合があるとされている。

⑪ EU データ保護指令に対する対応状況

EU データ保護指令へ対応するため、2001 年に連邦データ保護法が改正された。主な改正点は、①個人データの取扱いを収集段階から規制し、同意原則を適用したこと、②個人に関する自動的判断の規制を設けたこと、③「特別な種類のデータ」についての規制を設けたことである。

⑫ 第三者機関の概要

ドイツでは、以下の監督体制をとっている（左は監督機関名、右は監督対象）。

① 連邦データ保護監察官：連邦の公的機関及び民営化された一部事業者
② 州のデータ保護監察官：州の公的部門
③ 州のデータ保護監察官又は内務省の下の監督官庁：一般の民間事業者

民間部門についての監督機関の機能は、①法律違反についての本人への通知、訴追又は告発、②データ処理の届出の管理、③事業者に対する情報開示請求、④立入検査の実施、⑤技術的・組織的措置の実施命令等を行うことである。

⑬ 死者に関する個人情報の保護

連邦データ保護法には、死者の個人情報に関する規定は設けられていない。

死者の個人情報については、民法上の人格権を根拠に遺族が保護を求めることができるようである。また、憲法裁判所においても、死者の人格権は死後も保護されるべきである旨の判決がある（現地での聞き取り調査による）。

また、カルテの第三者への開示については、開示先が遺族の場合には、民法上の解釈により開示でき、開示先が遺族以外の第三者の場合には、刑法上の医者の守秘義務との

関係で、原則として開示できない（現地での聞き取り調査による）。

⑭ 直接処罰等の実効性担保の措置

連邦データ保護法では、故意又は過失により、次の行為等を行った者は、25 万ユーロ（約 3,875 万円）以下の過料を科される旨が定められている。

ｱ)権限なく、一般的にはアクセスできない個人データの収集、取扱いを行うこと

ｲ)権限なく、一般的にはアクセスできない個人データの入手や提供を行うこと

ｳ)一般的にはアクセスできない個人データを不正な申告により受け取ること

ｴ)第三者への譲渡を通じて、提供されたデータを他の目的に利用すること

これらの行為を、対価を得て、又は、自己若しくは他人の利得を図ることを意図して、又は他人を害することを意図して、故意に行った場合には、2 年以下の自由刑又は罰金に処すとされている。

監督機関には、強制的な立入権限が認められているほか、違反があった場合、まずは書面で改善指導を行い、従わなかった場合には利用停止措置をとることとなる（現地での聞き取り調査による）。

ベルリン州の非公的機関については、過料は年約 10 件である（現地での聞き取り調査による）。

４．アメリカ

（１）個人情報保護制度の概要

アメリカでは、公的部門と民間部門の双方を対象とする包括的な個人情報保護法は存在しない。公的部門については、連邦政府の保有する個人情報の取扱いについて、1974年に制定されたプライバシー法が制定されている。一方、民間部門については、判例法による保護があるほか、自主規制に委ねられているところもあるが、信用情報や医療情報など一部の機密性の高い情報を扱う分野においては、分野ごとに個別法が制定されている。

（２）「個人情報保護に関する主な検討課題」関連項目に即した状況

①いわゆる「過剰反応」（誤解）に対応した第三者提供制限の例外事由

情報の提供については、分野ごとに個別法で規定されている。例えば、個人の健康情報に係るプライバシー規則（医療保険の相互運用性と説明責任に関する法律（HIPAA）プライバシールール）では、情報の提供には原則として本人の同意又は許可が必要であるが、次の場合は例外とされている。

ｱ)法律の規定がある場合　　ｲ)公的健康業務に用いる場合
ｳ)ネグレクトやDVの被害者情報の公開　　ｴ)監督に用いる場合
ｵ)司法・行政手続のための公開　　ｶ)法執行目的
ｷ)死者情報が葬儀業者等に開示される場合　ｸ)移植手術等に用いられる場合
ｹ)調査目的　　ｺ)健康・安全への深刻な脅威がある場合
ﾀ)特別な政治的理由がある場合

また、医療機関と提携する会社は、当該医療機関との間で守秘義務契約を結ぶ必要がある。

アメリカでは、「過剰反応」が見られる（現地での聞き取り調査による）。このため、監督機関では、ガイドブックやインターネットを活用した啓発活動により、理解を促している。

②自治会や同窓会等の取扱い

アメリカでは、特定の分野ごとにプライバシー法が制定されているため、分野ごとに固有の義務の対象が定義されている。

自治会や同窓会における個人情報の取扱いを直接規制する連邦法は存在しない。

③個人情報の定義

アメリカでは、特定の分野ごとにプライバシー法が制定されているため、分野ごとに固有の個人情報の定義がされている。

金融サービス近代化法（GLBA）が対象とする個人情報は、「非公開個人情報」であり、「個人を識別でき、かつ、一般に入手可能でない金融情報全般」とされている。

公正信用報告法（FCRA）が対象とする個人情報である「消費者報告」は、「消費者個人の信用度、信用に対する評価、信用枠、特性、社会的評判、身上事項、生活様式に関する消費者報告機関による情報の伝達であって、信用若しくは保険、雇用目的等のために、消費者の適格性を判断するに当たり用いられ又は収集されるもの」とされている。

個人の健康情報に係るプライバシー規則（医療保険の相互運用性と説明責任に関する法律プライバシールール）が対象とする個人情報は、「個人の識別が可能な医療情報」とされている。

④センシティブ情報の取扱い

「消費者報告」（信用情報）のうち、被報告者の友人等に対する個人的な面接によって得られる、当該被報告者の性質等の情報を指す「消費者調査報告」については、特に要保護性の高い情報であると考えられることから、その開示が厳格に制限されている。

医療情報は、原則として本人（患者）の同意がない限り利用・提供は許されない（保護された保健情報（PHI）の利用・提供は必要最小限のものに限られている）ほか、医精神科治療記録など特に配慮を要する情報については、特段の保護が図られている。

⑤小規模事業者の取扱い

公正信用報告法では、小規模事業者であっても、個人情報の取扱いに関する義務は同様に適用される。

医療保険の相互運用性と説明責任に関する法律では、従業員 50 人以下の自己運営管理医療プランは適用除外とされているため、同法のプライバシールールについても、同様に適用除外となる。小規模事業者の中には、同ルールの遵守が困難な事業者もある（現地での聞き取り調査による）。

⑥個人情報の目的外利用の防止措置

公正信用報告法では、消費者報告機関は、消費者報告の提供を法で定めた目的に限定するため、目的外利用を防止するための合理的な手続に従わなければならないとされており、この規定は、民事上の損害賠償責任により担保されている。

個人の健康情報に係るプライバシー規則（医療保険の相互運用性と説明責任に関する法律プライバシールール）では、原則として、個人情報の利用・公開には本人の許可を得る必要があるとされている。

⑦市販の名簿の管理等

民間部門の名簿や住所録については、個別分野の規制に委ねられている。法の適用対象となる情報であれば、当該情報が市販されている名簿に載せられている場合にも、他の媒体の情報と同様に当該法律の規制対象となる。

⑧個人情報の取得元の開示に関する措置

金融サービス近代化法では、個人情報の取得元の開示を義務付ける規定は設けられていない。

公正信用報告法の解釈においては、消費者に対する開示の際は、消費者ファイルに記載されている全項目の内容を開示することとされているため、消費者報告機関は、原則として、情報源についても開示する必要がある。

個人の健康情報に係るプライバシー規則（医療保険の相互運用性と説明責任に関する法律プライバシールール）では、個人情報の取得元の開示を義務付ける規定は設けられていない。金融サービス近代化法及び医療保険の相互運用性と説明責任に関する法律には個人情報の取得元の開示を義務付ける規定は置かれていない。

⑨個人情報の利用停止・消去に関する措置

公正信用報告法では、消費者から情報の正確性について争いが提起された場合、消費者報告機関は再調査を行い、情報を訂正・削除することとされている。

個人の健康情報に係るプライバシー規則（医療保険の相互運用性と説明責任に関する法律プライバシールール）では、訂正請求権は認められているが、利用停止や消去については定められていない。

⑩国際的な情報移転に関する措置

個人の健康情報に係るプライバシー規則（医療保険の相互運用性と説明責任に関する法律プライバシールール）や金融サービス近代化法など、法律によっては、海外の事業者に情報が提供される場合に、国内法の規定が適用されることを明示するものがある。

また、EU データ保護指令の第三国移転条項への対応として、2000 年に EU とセーフハーバー協定を締結したことにより、商務省がプライバシー原則に基づき認証した企業については、十分性を付与されることとなった（2006 年 11 月時点で認証を受けている企業は 1,045 社）。

【セーフハーバー協定の概要】

適用範囲：セーフハーバーに加入した事業者が EU の事業者と通商や情報の流通を行う際に適用される。加入は任意である。

監督制度：事業者がセーフハーバー原則に違反している場合、商務省から告知を受け

る。違反行為等については、連邦取引委員会（FTC）により調査や停止命令、民事罰等の制裁措置が行われる。

⑪EU データ保護指令に対する対応状況

特定の認証基準を設け、その認証を受けた企業ごとに十分性を付与する「セーフハーバー原則」について、EU と協定を締結している。この協定により、DOC が作成するプライバシー原則を企業が遵守することにより、EU データ保護指令違反とはならないことが約されている。

⑫第三者機関の概要

連邦取引委員会は、諸外国の監督機関ほど政府から独立しているわけではないが、消費者及び事業者の啓発に当たっている。FTC の機能は、①連邦取引委員会法に基づく、企業の個人情報の取扱いに関する不正・欺瞞の監視、②金融サービス近代化法に基づく、ｱ)金融のプライバシー通知に関する規則の実施、ｲ)個人情報の事務的、技術的及び物理的保護、ｳ)詐欺に対する執行、③公正信用報告法及びこどもオンラインプライバシー保護法に基づく、消費者のプライバシー保護を行うことである。なお、信用情報については、違反行為者を被告とする民事訴訟の提起権限を有する。

⑬死者に関する個人情報の保護

個人の健康情報に係るプライバシー規則（医療保険の相互運用性と説明責任に関する法律プライバシールール）は、死者の個人情報についても適用されることを明示的に規定している。

具体的には、死者の情報の取扱いについて、

- 対象機関は、検死官又は医療検査官に対し、死者の同定、死因の決定等の義務を履行することを目的として、医療情報を提供することができる
- 対象機関が、検死官又は医療検査官の義務をも同時に履行している場合、定められた目的のために自ら医療情報を利用することができる
- 対象機関は、葬儀施主に対し、その業務に必要な限りにおいて、法に定めるところにより情報を提供することができる

といった規定がある。

⑭直接処罰等の実効性確保の措置

公正信用報告法では、消費者報告機関から消費者についての情報を故意に虚偽の名目で取得した者に対し、5,000 ドル（約 60 万円）以下の罰金若しくは 1 年以下の懲役又は併科が定められている。このほか、連邦取引委員会は第三者による定期的監査を求めることもある（現地での聞き取り調査による）。

個人の健康情報に係るプライバシー規則（医療保険の相互運用性と説明責任に関する法律プライバシールール）では、本人の同意を得ずに情報を入手、提供した者には、5万ドル（約600万円）以下の罰金等が定められている。2006年12月までに、同法の違反者に対する罰金処分の例はない（現地での聞き取り調査による）。

Ⅱ．国際機関

１．OECD

（１）個人情報保護制度の概要

プライバシー保護と個人データの国際流通についてのガイドラインに関するOECD理事会勧告（OECDプライバシー・ガイドライン、1980年9月23日採択。）

目的：加盟国間の情報の自由な流通を促進すること、及び、加盟国間の経済的社会的関係の発展に対する不当な障害の創設を回避すること。

対象：OECD加盟国

拘束の程度：OECD加盟国は、OECD理事会からガイドラインに準じた対応を採ることが勧告されるが、その遵守を義務付けられてはない。

（２）「個人情報保護に関する主な検討課題」関連項目に即した状況

①「個人情報」の定義

「個人データ」は、個人に関する情報であって、個人が識別され又は識別され得る情報のすべてとされている。OECDプライバシー・ガイドラインが適用されるのは、個人データのうち、公的又は私的部門において、取扱方法又は性質若しくは利用状況からみて、プライバシーと個人の自由に対する危険を含んでいるものすべてとされている。

② センシティブ情報に関する規定

センシティブ情報に関する規定は設けられていない。センシティブ情報の定義は多様であり、普遍的にセンシティブなデータと整理されるものを定義することは、不可能であろうとされている。

③ 個人情報の目的外利用の防止に関する規定

OECDプライバシー・ガイドラインでは、利用制限の原則として、個人データは、データ主体の同意がある場合又は法律に基づく場合を除き、目的明確化原則により明確化された目的以外の目的のために、開示、利用その他の使用に供されるべきではないとされている。

目的明確化の原則では、個人データの収集目的は、遅くともデータ収集時には明確化されるべきであり、事後の利用は、当該収集目的の達成と、目的変更時に明確化された目的の達成の場合に限定されるべきとされている。

また、個人は、自己に関するデータについて異議申立を行う権利、及び異議が認められた場合に当該データを消去させる権利を有すべきとされている。

④ 個人情報の取得元の開示に関する規定

OECD プライバシー・ガイドラインでは、個人情報の取得元の開示に関する規定は明記されていない。

ただし、個人参加の原則として、個人は、自己に関するデータについて提供される権利を有すべきであるとされている。

⑤ 小規模事業者の取扱い

小規模事業者であっても、個人情報の取扱いに関する義務は同様に適用される。

⑥ 個人情報の利用停止・消去に関する規定

OECD プライバシー・ガイドラインでは、個人参加の原則として、個人は、自己に関するデータについて異議申立を行う権利、及び、その異議申立が認められた場合には、当該データを消去、訂正、完全化及び補正させる権利を有すべきであるとされている。

⑦国際的な情報移転に関する規定

OECD プライバシー・ガイドラインでは、国際的な情報移転について、加盟国は、①他の加盟国に及ぼす影響について配慮すべきこと、②国際流通が阻害されることなく、安全になされることを確保するための手段を講ずべきこと、③他の加盟国による本ガイドラインの未遵守等の場合を除き、国際流通の制限を控えるべきこと、④国際流通の障害となる必要以上の法律や政策、運用を回避すべきことが規定されている。

⑧ 第三者機関に関する規定

OECD プライバシー・ガイドラインでは、監督機関に関する特段の規定は設けられていない。採るべき実効性担保の仕組みは、各国の法体系等によって変わり得るため、監督機関の設置等は各国の判断に委ねられている。

⑨ 死者に関する個人情報の保護

OECD プライバシー・ガイドラインでは、死者に関する個人情報の保護に関する規定は設けられていない。

⑩ 直接処罰等の実効性担保に関する規定

OECD プライバシー・ガイドラインでは、加盟国は、諸原則の国内実施に際し、個人データに関するプライバシーと個人の自由を保護するための手続や制度を整備すべきであり、不遵守に対する適切な制裁や救済手段を提供することとされている。

⑪その他、特に留意すべき重要事項（今後の取組の予定等）

1998 年の電子商取引に関する OECD 閣僚会議では、同ガイドラインに沿って、開かれたグローバルネットワークを構築すべきことを確認した、「グローバルネットワークでのプライバシー保護に関する宣言」が採択された。最近では、2006 年 7 月 24 日に「プラバシーに関する通知文の簡素化-OECD による報告及び勧告-」が公表されたほか、プライバシー法執行の越境的な課題を検討するため、同年 10 月 26 日、「プライバシー法の越境的な執行協力に関する報告書」が公表された。

２．EU

（１）個人情報保護制度の概要

個人データの取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令（EU データ保護指令、1995 年 10 月 24 日指令。）

目的：個人データの取扱いに対する自然人の基本的権利及び自由、特にプライバシー権の保護。

対象：EU 構成国。ただし、第三国への個人データの移転を規制する、いわゆる第三国条項を通じて、EU 構成国以外の国にも大きな影響を与える。

拘束の程度：EU 構成国は、指令を国内法化する義務を負う。

（２）「個人情報保護に関する主な検討課題」関連項目に即した状況

①「個人情報」の定義

「個人データ」は、「識別された又は識別され得る自然人（データ主体）に関するすべての情報」とされている。識別され得る個人とは、「特に個人識別番号、又は肉体的、生理的、精神的、経済的、文化的若しくは社会的アイデンティティに特有な 1 つ又は 2 つ以上の要素を参照することによって、直接的又は間接的に識別され得る者」とされている。

② センシティブ情報に関する規定

構成国は、原則として、人種又は民族、政治的見解、宗教的又は思想的信条、労働組合への加入を明らかにする個人データの取扱い、及び健康又は性生活に関するデータの取扱いを禁止しなければならないとされている。

③ 個人情報の目的外利用の防止に関する規定

EU データ保護指令では、構成国は、個人データについて、原則として、特定された明示的かつ適法な目的のために収集され、それに続いてこれらの目的と相容れない方法で取り扱われないことを確保しなければならず、管理者はこの遵守を確保しなければならないとされている。

④ 個人情報の取得元の開示に関する規定

EU データ保護指令では、構成国は、すべてのデータ主体に対して、管理者から、①関係するデータの種類や開示されたデータの取得者に関する情報、②取り扱われているデータ及びその情報源に関する入手可能な情報のデータ主体への通知、等を取得する権利を保障しなければならないとされている。

⑤ 小規模事業者の取扱い

小規模事業者であっても、個人情報の取扱いに関する義務は同様に適用される。なお、小規模事業者を個人情報保護制度の適用除外とすることについては、EU から問題視されることがある。

⑥ 個人情報の利用停止・消去に関する規定

EU データ保護指令では、構成国は、すべてのデータ主体に対して、管理者から、原則として、①不完全又は不正確なデータの修正、消去又は封鎖、②既にデータが開示されている第三者に対する、これらの修正、消去又は封鎖の通知、等がなされる権利を保障しなければならないとされている。

⑦国際的な情報移転に関する規定

EU データ保護指令では、構成国は、個人データの第三国への移転は、当該第三国が十分なレベルの保護措置を確保している場合に限って、行うことができることを定めなければならないとされている。

また、その十分性は、データの性質、取扱いの目的・期間、発信国・最終目的国、当該第三国の一般的及び分野別の法規範並びに専門的規範及び安全保護対策措置等、データ移転に関するあらゆる状況にかんがみて、評価されなければならないとされている。

さらに、構成国は、十分なレベルの保護を保障しない第三国に対する移転が例外的に可能な場合を定めなければならないとされている。

このため、構成国は第三国移転の例外事由を設けており、これに基づき、本人が明確に同意した場合のほか、①拘束力のある企業ルールを定め、監督機関に申請して認証を得た場合、②EU の定めた標準契約条項を利用する場合、③セーフハーバー原則による場合等は移転が可能になっている。

⑧ 第三者機関に関する規定

EU データ保護指令では、各構成国は、各国の規定の適用に関し、完全に独立して監督する公的機関を定めなければならないとされている。

監督機関の機能は、①調査、②介入、③法的手続の開始、違反の司法機関への通知、④個人の主張の聴取、⑤定期的な活動報告書の作成を行うこととされている。

⑨ 死者に関する個人情報の保護

EU データ保護指令は、死者のデータについてはあえて言及していないというのが関係者の一致した解釈である。閣僚理事会、EU 委員会とも、「個人情報」に死者のデータを含めるか否かは、加盟各国の立法政策に委ねるということで合意している。

⑩ 直接処罰等の実効性担保に関する規定

EU データ保護指令では、構成国は、同指令の完全な実施を担保するために適合的な措置を講じ、同指令に基づく規定に対する違反がある場合に加えられる制裁について、特に定めなければならないとされている。

⑪その他、特に留意すべき重要事項（今後の取組の予定等）

2006 年 1 月現在、EU から十分な保護水準を確保していると認められた国・地域は、スイス、カナダ、アルゼンチン、ガンジー島、マン島の 5 つである。なお、カナダは、連邦政府部門対象の法律、民間部門対象の法律、州政府対象の州法等、複数の法律を組み合わせることにより、ほぼすべての機関を対象とした法的枠組みを形成し、十分性を認められた。

また､アメリカ､オーストラリアの EU データ保護指令への対応状況は以下のとおり。

①アメリカ：包括法がないため、特定の認証基準を設け、その認証を受けた企業ごとに十分性を付与するセーフハーバー協定を 2000 年に EU と締結。

②オーストラリア：包括法である「プライバシー修正法」を 2000 年に施行したが、ｱ)小規模事業者が規制対象外、ｲ)一般に利用可能なデータが規制対象外、ｳ)データの第三国移転が規制対象外等の理由により、保護水準が不十分とされた。

３．APEC

（１）個人情報保護制度の概要

APEC プライバシーフレームワーク（APEC フレームワーク、2004 年 10 月 29 日採択。国際的実施の部分は 2005 年 11 月 16 日承認。）

目的：APEC 加盟エコノミーにおける整合性のある個人情報保護への取組を促進し、情報流通に対する不要な障害を取り除くこと。

対象国：APEC 加盟エコノミー

拘束の程度：APEC 加盟エコノミーに対して適用を推奨。適用に際しては、加盟エコノミーにおける個別事情を考慮すべきであるとされている。

（２）「個人情報保護に関する主な検討課題」関連項目に即した状況

①「個人情報」の定義

「個人情報」は、「個人が識別される、又は識別可能なすべての情報」とされている。

②センシティブ情報に関する規定

センシティブ情報の定義及びその取扱いについての規定は設けられていない。

ただし、情報の安全管理は、「情報のセンシティブ性の程度」に見合ったものでなければならないとされている。また、業務上の機密情報については、個人のアクセスが制限される場合があるとされている。

③個人情報の目的外利用の防止に関する規定

APEC フレームワークでは、収集された個人情報は、①本人の承諾を得た場合、②本人から求められたサービス等を提供する必要がある場合、③法律の権限等による場合を除き、収集目的及びそれに矛盾しない又は関連する目的を履行するためだけに、使用されなければならないとされている。情報の収集、利用、公開に当たって、個人に対して選択権を付与する仕組みが用意されるべきであるとされている。

また、個人は、可能かつ適切であれば、情報を消去させることができるべきとされている。

④個人情報の取得元の開示に関する規定

APEC フレームワークでは、個人情報の取得元の開示については、特段の規定は設けられていない。

ただし、開示・訂正の原則として、個人は、自己の個人情報について知らされるべきとされている。

⑤小規模事業者の取扱い

小規模事業者であっても、個人情報の取扱いに関する義務は同様に適用される。義務の対象である「個人情報管理者」には、別の個人・組織から指示された機能を実践する個人・組織は含まれない。また、自身の個人、家族又は家計に関する事柄と関連する個人情報を収集、保持、取扱い、又は利用する個人も含まれない、とされている。

⑥個人情報の利用停止・消去に関する規定

APEC フレームワークでは、個人は、可能かつ適切であれば、情報を修正、補完、改訂、消去させることができるべきとされている。

⑦国際的な情報移転に関する規定

APEC フレームワークでは、個人情報管理者が個人情報を第三者に提供する場合、国内・国外を問わず、個人から同意を得るか、又は提供先が当該情報を同フレームワークに則って保護することを確認できる手続を踏まなければならないとされている。

⑧第三者機関に関する規定

APEC フレームワークでは、監督機関に関する特段の規定は設けられていない。損害防止のため、制度の実施の仕組みを整備すべきとされている。

⑨死者に関する個人情報の保護

APEC フレームワークでは、死者の個人情報については特段記述されていない。

⑩直接処罰等の実効性担保に関する規定

APEC フレームワークでは、罰則については特段記述されていないが、各加盟エコノミーが同フレームワークを国内で適用する際は、適切な救済の制度化も含まれるべきとされている。また、加盟エコノミーは、損害防止のための適切な措置として、制度の実施体制を整備すべきとされている。

⑪その他、特に留意すべき重要事項（今後の取組の予定等）

APEC 電子商取引運営グループ（ECSG）では、APEC フレームワークの適用に関するセミナーの開催や会議を通じ、域内諸国の多様な実情を考慮しつつ、①各国における APEC フレームワークの適用、②越境的なプライバシールールの構築、③情報共有や調査・執行の越境協力に向けた検討等を行っている。

Ⅰ.諸外国

１．イギリス

（１）個人情報保護制度の概要

①法律名

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

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

②目的

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

③適用範囲

ア）個人データ

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

イ）公的部門と民間部門

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

④規制・権利の内容

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

ア）1998 年データ保護法の構成

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

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

イ）データ保護原則

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

第 1 原則　公正かつ適法な取扱い（Fairly and lawfully processed）
第 2 原則　限定された目的のための取扱い（Processed for limited purposes）
第 3 原則　目的適合性（Adequate, relevant and not excessive）
第 4 原則　正確性・最新性（Accurate and up to date）
第 5 原則　必要期間限定性（Not kept for longer than is necessary）
第 6 原則　データ主体の権利適合的取扱い（Processed in line with your rights）
第 7 原則　安全性確保（Secure）

第 8 原則　十分な保護のない第三国への移転制限(Not transferred to other countries without adequate protection)

⑤監督・登録制度

公的部門と民間部門の双方を監督する情報コミッショナーが設けられている。また、1984 年法で設けられた登録制度は、1998 年法では、登録（registration）ではなく、通知（notification）という概念で存在している。

⑥主な適用除外

様々な場面で適用除外が設けられている。詳しくは、後述参照。

⑦主な自主規制

3 つの分野で実施規範（code of practice）が策定されている。例えば、監視カメラ実務規範（CCTV code of practice)、雇用実務規範（Employment Practices Code）がある。

⑧その他

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

（2）「個人情報保護に関する主な検討課題」関連項目に即した状況

①いわゆる「過剰反応」（誤解）に対応した第三者提供制限の例外事由

[現状について]

事前に提出した質問票でいう「過剰反応」という概念は、理解され難かった。また、現地調査でも、同様な状況であったが、具体例な例を挙げると、そのような現象は見られるということであり、情報コミッショナー事務局は、後掲のような具体例をホームページで公表している。これら以外にも多々あるが、公表しているのはこれらのみであるとのことである（後掲（２）⑮イ）の「図表　個人情報保護の取扱いにおける「俗説」と「本当の対応」の概要」参照)。

[制度について]

ア）附則 1「データ保護原則」の第 1 原則―公正かつ適法な取扱い

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

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

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

第 1 原則は、次のようになっている。

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

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

イ）附則 2「第 1 原則：個人データ取扱いの目的に関する条件」

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

その附則 2 は、次のような 6 つの条件を掲げている。

1. データ主体が当該取扱いに同意した。
2. 当該取扱いが、(a) データ主体が当事者である契約の履行のため、又は (b) 契約を締結する目的でデータ主体の要請に基づき手段を講ずるために、必要である。
3. 当該取扱いが、契約によって課せられる債務以外で、データ管理者が従う法的義務を遵守するために必要である。
4. 当該取扱いが、データ主体の重要な利益を保護するために必要である。
5. 当該取扱いが、次に掲げる場合のために必要である

(a) 司法のため

(b) 法規によりある者に付与された権能の行使のため、

(c) 国王、国王の大臣若しくは政府省庁の権能の行使のため、又は

(d) ある者によって 公益のために行使される公的性格のその他の権能の行使のため

6. (1) 当該取扱いがデータ管理者によって追求される適法な利益（legitimate interests）のために必要である（この部分は要約)。

(2) 主務大臣がこの条件が満たされるために要求されるべき又は要求されるべきで

はない特定の状況を命令により明確にすることができる。この命令は、まだ定められていない。

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

[制度の運用について]

データ保護法の的確な理解が必要であり、情報コミッショナー事務局は、ホームページで啓発活動を行っているばかりでなく、各種のパンフレットなどを発行している。また、年に 300 回くらい研修会などを開いている。

②自治会や同窓会等の取扱い

[現状について]

データ保護法の適用除外は、事業者が取り扱う個人情報の量によっていない。適用除外は複雑であるが、一般的にいって、民間部門については、「ジャーナリズム、文学及び芸術」（journalism, literature and art）や家庭内利用目的（domestic purposes）の個人情報の取扱いは、適用除外される。日本でいう「自治会」に 1 対 1 で対応するものはないといえるが、そのような組織が個人情報を取り扱う場合には、データ保護法が適用される。また、現地調査で聞く限りでは、同窓会は存在するが、現在は、日本で伝統的に存在した同窓会名簿はない場合が多いといえるけれども、何らかの形で（例えば、データベース）作成されるときには、データ保護法の適用があるとのことである。

[制度の運用について]

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

・イギリスにも「隣人監視組織」（neighbourhood watch）は存在し、また、家主が店子のリストを保有しており、その店子が集まって会議を行うような場合もあるということである。この場合、組織の性質にかかわらず、個人情報を取り扱う組織は法の規則を遵守する必要があり、自治体も自主的な組織も取扱いは同じであるということである。

・同窓会名簿については、「個人情報の掲載拒否を希望する場合は、掲載を停止することとすれば、作成できる。しかし、同窓会組織から名簿を大学側に渡す際に、その趣旨が大学にうまく伝わらず、大学で利用する際に不適切な取扱いをする場合があるということである。実際に、ある大学が同窓会名簿を売って金儲けをしたことがあり、問題になったことがあるということである。

③「個人情報」の定義

ア）1998 年データ保護法の規定

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

(ア)データ

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

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

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

(イ)関連するファイリングシステム

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

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

(ウ)個人データ

「個人データ」(personal data) とは、「(a) 当該データから、又は (b) データ管理者 (data controller) が保有し、又は保有することになる可能性のある当該データ

その他の情報から、識別できる生存する個人に関するデータであって、かつ、当該個人に関する意見の表明及び当該個人についてデータ管理者その他の者の意図の表示を含む」(1 条 (1) 項) と定義されている。

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

例えば、特定の者が「怠け者である」というのは、「当該個人に関する意見の表明」であり、「怠け者であるから、解雇する」というのは、「意図の表示」である。

イ)「個人データ」に関する控訴裁判所の解釈

控訴裁判所民事部(Court of Appeal (Civil Division))が、Durant v. Financial Service Authority [2003] EWCA Civ 1746 において、「個人データ」、「関連するファイリングシステム」、その他の概念について、解釈を示したことから、それをめぐって議論が交わされている。

控訴人マイケル・ジョン・デュラント (Michael John Durant) は、1998 年データ保護法 7 条に基づいて、金融庁 (Financial Service Authority, FSA) が自己について保有している個人データの開示を求めた。FSA は、控訴人の要求に応じてある種の情報を開示したが、控訴人は、より多くの情報の開示を求めた。

控訴人の請求を退けた、2002 年 10 月 24 日のエドモントン・カウンティ裁判所(Edmonton County Court) の判決に対する控訴が本件である。

本件において、控訴裁判所は、前掲の「個人データ」の定義の中の「個人に関する」の「関する」(relate to) について解釈し、データが「個人の個人的又は家族的生活、ビジネス又は専門職業的資格であるか否かを問わず、「個人の」プライバシーに影響を与える情報である」場合に、データは「個人に関する」ということになると解釈した。

ウ) 評釈例

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

エ) 運用上の一般的な解釈

イギリスでは、個人情報について運用上、次のように解釈しているとのことであった。

何が個人情報に当たるかという判断は難しいが、それが取り扱われる状況によるところが大きいということである。それが公共性のあるものなのか、真にプライベートのも

のなのかも重要でであるとされる。

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

④センシティブ情報に関する規定

[制度について]

1998 年データ保護法の規定では、センシティブ情報については、「2 条 センシティブな個人データ」（sensitive personal data）に規定されており、具体的には、「人種的・民族的出自、政治的意見、宗教的信条、労働組合への加入、健康状態、性生活、犯罪の前科・容疑、犯罪・容疑の手続・処分・判決」と定義されている。

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

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

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

[制度の運用について]

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

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

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

さらに、例えば、Jones はウェールズ人の名前であるというように、名前からは特定の民族グループに属することがわかる場合があり、名前だけの利用であれば問題ないが、

これを個人の趣味嗜好を知るために使う場合などは、センシティブ情報として取り扱われるということである。

⑤小規模事業者の取扱い

[現状について]

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

[制度について]

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

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

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

データ管理者には規模による相違はない。

[制度の運用について]

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

小規模事業者は、企業活動に対する規制が多すぎると感じており、個人情報保護法も規制の一つと考えられていて歓迎されていないようである。小規模事業者向けの標準規約（Code of Conduct）を作成したが、対応しきれない内容であるという批判があり、もう少し簡素化したものにするべきではないかという議論がなされているとのことである。

⑥個人情報の目的外利用の防止措置

[制度について]

1998 年データ保護法の規定では、個人情報の目的外利用は、前掲の第 2 原則（限定さ

れた目的のための取扱い）（Processed for limited purposes）によって制限されている。

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

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

[制度の運用について]

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

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

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

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

⑦市販の名簿の管理

[制度について]

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

[制度の運用について]

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

電話帳など、市販のリストの個人情報をコンピュータに取り込んだ時点で、法律に基

づく取扱いが必要となるため、本人に利用目的を通知することが必要となる。印刷してある電話帳をそのまま利用する場合は、本人への通知は不要であると理解されているということである。

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

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

・企業年鑑などのように、公開され、一般に入手可能な個人情報については、それを利用する企業の社員などはセキュリティに特に気をつける必要はない。道端に捨てても問題はない。一般に公開されているものは、誰でもどこでも容易に入手できるため、特別な配慮は不要という考え方である。

⑧個人情報の取得元の開示に関する措置

[現状について]

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

[制度について]

前述のように、1998 年法の第Ⅱ章は、「データ主体の権利その他」として、日本の個人情報保護法でいう「本人」に様々な権利を認めている。その１つとして、7 条で、個人データへのアクセス権が規定されている。その中で個人情報の取得元についても開示を請求することができることを明文化している（7 条（1）項（c）号)。

これは、取得元にさかのぼって個人情報の停止などを要求する必要があるので、取得元についてはできる限り多くの情報を提供することが求められている。

[事業者の対応について]

イギリスでは、取得元の開示については、事業者は情報主体の信頼を得るために、可能な情報は提供することになるはずであるという指摘があった。

また、コンピュータにより、情報の取得元を割り出すことが容易になったことも影響を与えているようである。リストを購入する際は、取得元を必ず教えてもらうようにしており、リストブローカーもビジネスとして情報の取得元を明確にする必要がある。また、郵送した場合なども、情報の取得元について問い合わせが来る場合があるため、回答を用意しておく必要があると認識されているようである。

⑨個人情報の利用停止・消去に関する措置

[現状について]

ダイレクトマーケティングへの利用を拒否したいイギリス人国民は、多くは禁止サービス（suppression service）に登録しているとのことである。約半数の世帯は、電話選好サービス（TPS）に登録し、約 8 分の 1 は氏名と住所について、郵便選好サービス（MPS）に登録しているとのことである。

[制度について]

上記⑧と同じく、1998 年法の第Ⅱ章「データ主体の権利その他」（7 条―15 条）の一環

として、個人情報の利用停止・消去に関する措置にかかわる規定がある。その他の規定も含め、「第Ⅱ章　データ主体の権利その他」の 10 条以下の条文見出しを掲げると、次のようになる。

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

[事業者の対応について]

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

⑩国際的な情報移転に関する措置

[制度について]

ア）1998 年データ保護法の規定

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

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

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

イ）1998 年データ保護法の例外規定

一般の企業がその個人データを第三国に移転する場合には、上記のデータ保護原則の第 8 原則によって、第三国が「十分なレベルの保護」を確保していないときは、その個人データを移転することができない。このことは、特に多国籍企業の場合には深刻である。第 8 原則に対する例外が附則 4 に規定されているので、それを見ることにする。

附則 4「第 8 原則が適用されない事例」は、次のよう場合を掲げている。

(ア)データ主体がその移転に同意している場合。

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

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

(エ)

〈1〉その移転が実質的な公益のために必要である場合。

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

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

(カ)その移転が、データ主体の重要な利益を保護するために必要である場合。

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

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

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

[法律以外の枠組みについて]

イギリスでは、現在の法律の下では EU 以外には情報の移転は原則禁止されている。そこで、多くの事業者は例外の一つである「契約」で対応しているということである。また、同一企業グループ間での国際的な個人情報移転に関しては、「拘束力のある企業ルール」（Binding Corporate Rules）も使われているということである。

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

情報コミッショナー事務局には、「拘束力のある企業間ルール」について、標準的なチェックリストを作成し、申請のあったルールのチェックを行っているということである。問題点としては、認証に時間がかかる手続になっているという点が指摘された。

一方、「契約」については、EU に許可された標準的な契約様式を用いる方法がある。多岐にわたり、細かく規定されているため、情報コミッショナー事務局はチェックは行わない。標準的な契約様式を踏まえ、事業者が独自の契約様式を使用する場合についても、情報コミッショナー事務局が事前にチェックを行うことはないということである。問題

が発生し、苦情が寄せられた場合にのみ情報コミッショナー事務局が対応するようにしているということである。「契約」には現在、3つの様式があるということである。

⑪EU データ保護指令に対する対応状況

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

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

⑫第三者機関の概要

[制度について]

1998 年データ保護法は、第Ⅰ章　序則（1 条―6 条）の中の 6 条で、コミッショナー及び審判所（The Commissioner and the Tribunal）を置くと規定している。コミッショナー及び審判所のうち、個人情報保護に関する、直接的な監督機関は、コミッショナーであり、2000 年情報自由法（Freedom of Information Act 2000）の運用にも当たるので、2000 年情報自由法で、「情報コミッショナー」という名称になった。ここでは、コミッショナーについて見ることにする。

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

また、コミッショナーの権能については、第Ⅵ章　雑則及び総則（51 条―75 条）の中で、51 条から 54 条までの規定があり、具体的には、①情報の適切な取扱いの推進、②データ保護に関する啓発、③データ管理者の行動規範の作成・承認、④情報の届出の管理、⑤法令遵守の調査、⑥法令違反に対する通知の発出、⑦犯罪の起訴、⑧議会への報告等を行うこととされている。

また、附則 5 は、コミッショナーの地位、任期、俸給等について規定している。例えば、コミッショナー及びそのスタッフは公務員ではなく、またコミッショナーの任期は 5 年であると定められている。その他、関連する規定の中にコミッショナーが出てくる。

[制度の運用について]

現在のコミッショナーであるリチャード・トーマス（Richard Thomas）氏は、2002 年 11 月 30 日に任命された。コミッショナーは、1998 年データ保護法、2000 年情報自由法などの関連法令の執行の責任を負う独立の機関で、議会に対して直接報告する立場にある。

情報コミッショナー事務局によると、270～280 人の職員が勤務しており、うち約 70 人

が個人情報保護担当であるとのことである。情報コミッショナーの「2005-2006 年年次報告書」では、情報コミッショナーと常雇い契約を締結しているスタッフ 230 人、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 15 人、合計 245 人となっているので、事務局の説明は、それ以外の勤務者も含めた数であると見ることができる。質問と苦情が多く、その対応に時間をとられているため、もう少し人数が欲しいと感じているということである。

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

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

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

⑬死者に関する個人情報の保護

[現状について]

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

[制度について]

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

死者について規定しているのは、1990 年保健記録法（Access to Health Record Act 1990）3 条である。同条は保健記録へのアクセス権に関する規定で、その（1）項は、次に掲げ

る者は保健記録の保有者に対してアクセスを請求することができるとして、(a) 患者、(b) 患者に代わって請求する権限を文書で付与された者、(c) 記録がイングランド及びウェールズで保管され、かつ、患者が子どもである場合には、その患者の親権者、(d) 記録がスコットランドで保管され、かつ、患者が生徒である場合には、その患者の親又は後見人、(e) 患者が自己に関する事項を管理することができない場合には、裁判所により当該事項を管理するよう任命された者、(f) 患者が死亡した場合には、その患者の人格代表者（注・遺言執行者と遺産管理人の双方を含めてこのように称せられる）及び患者の死亡から発生する請求権を持ち得る者を挙げている。この最後の (f) が死者についての規定である。

[制度の運用について]

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

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

⑭直接処罰等の実効性担保の措置

[制度について]

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

55 条 (1) 項は、次のように規定している。

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

この (1) 項に違反した者は、罪を犯したことになる ((3) 項)。

法定刑は、罰金でデータ保護法 60 条に規定がある。1990 年治安判事裁判法 (Magistrate Court Act 1990) によると、上限は 5,000 ポンドである。

歴史的にみると、1984 年データ保護法にはこのような規定はなかったが、個人データを権限がないのに取得しようとする動きが 1990 年代初頭から、明らかに拡大してきた。そこで、1994 年の刑事司法及び治安法 (Criminal Justice and Public Order Act 1994) の 161 条が、1984 年データ保護法 5 条の罰則を拡大した。161 条は、コンピュータで保有される個人情報を提供及び販売させること (procuring disclosure of, and selling,

computer-held personal information）と題されていた。これをさらに個人データ一般を対象とし、個人データの不法な取得を処罰するようになったのが 1998 年データ保護法 55 条である。

これは、日本でも現在議論になっている個人情報の窃用・漏えいなどを直接処罰する規定の立法例であるが、イギリスのデータ保護法は、個人データの無登録取扱いを処罰することとしている（第 17 条）ので、情報コミッショナーの年次報告書では、訴追については､17 条違反及び 55 条違反の訴追の統計が出ている｡2005-2006 年年次報告書では、16 件の訴追が報告されている（うち、6 件が 55 条違反と関係している)。

[制度の運用について]

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

これまでの具体的事件を見ると、次の 3 つに分けられるといえる。

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

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

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

⑮その他、特に留意すべき重要措置

ア）今後、個人情報保護に関してどのような取組が行われるか。

イギリスでは、20 年以上前の 1984 年に個人データを体系的に保護するデータ保護法が制定された｡1984 年法で任命された初代のデータ保護登録官のエリック･ハウ(Eric Howe)氏が、データ保護法の普及啓蒙活動に誠心誠意努めてきたことは、当時から交流のあった者として認識している。2 代目のエリザベス・フランス（Elizabeth France）女史も、同様であったことも知っている。

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

これは、データ保護法に特有な問題ではなく、法一般の問題でもある。

法に関する普及啓蒙活動は今後とも極めて重要であり、情報コミッショナー事務局はデータ保護法について今後ともそのような努力を続けていくことを強調している。

イ）「過剰反応」の例

イギリスでも、以下のような例が情報コミッショナー事務局におけるホームページで過剰反応の例として示されている。「俗説（myths）」として過剰な反応の事例が示されており、「本当の対応（reality）」として、その俗説のような考え方、対応方法の問題点や正しい考え方が示されている。

図表　個人情報保護の取扱いにおける「俗説」と「本当の対応」の概要

	俗説（myths）	本当の対応（reality）
1	個人情報保護法は、両親が学校で子どもの写真をとることを禁じている	・私的な目的で撮影された写真は法の対象外である。 ・両親、友人、家族等は家庭用のアルバムを作る目的であれば、学校の行事に参加している子どもや友人の写真を撮影することが認められる。
2	個人情報保護法は事業者が顧客の情報を第三者に提供することを一切禁じている	・第三者でも個人情報にアクセスする権利を認められていれば、事業者がその者に個人情報を提供することは妨げない。 ・銀行や電話会社が自分の近親者の口座情報を教えないことについて情報コミッショナーに苦情が寄せられることがあるが、事業者は詐欺的な個人情報の取得に備えて注意することが求められているので仕方のない対応であると考える。 ・頻繁に他人の代理を行う者は、第三者提供を拒否されないようにパスワード等により、第三者提供を受けられる代理人としての認証を受けるなどの方策をとることが、その企業で可能であるかどうかを確認すべきである。
3	個人情報保護法は両親が子どもの成績を見ることも禁止している	・法は、試験実施者が生徒とその母親に成績を送付することを禁止していない。 ・母親があえて自分の娘の成績を開示するように請求するというのは不公正かつ不要である（ので、法はそこまで求めていないと理解すべきである）。
4	司祭が祈祷の途中で信者の名前を読み上げることは禁止されている	・法は主にコンピュータ処理された、ファイリングシステムに載せられた個人情報を対象としており、このような形態の個人情報は規制の対象外である。 ・もし対象だったとしても、本人が祈祷の最中に名前が読み上げられることについて歓迎していれば問題はない。しかし、もし本人が祈祷の最中に名前を呼ばれることを拒否していることが特に明言されている場合や、司祭が、信者が名前を読み上げられるたくないことを察することができる場合には、その意思を尊重すべきである。
5	個人情報保護法は、加害者の情報を被害者に教えることについて禁止している	・警察が、加害者の情報について個人情報保護法を理由に被害者に教えないのは誤った対応である。 ・民事訴訟が予定されている場合に、関係者の個人情報を提供しないことまで法は予定していない。警察は個人情報の公開

	俗説（myths）	本当の対応（reality）
		については常に注意する必要があるが、内務省から「どのような個人情報は提供してよいか」ということについて明確なガイドラインを示されている。 ・情報コミッショナーは本件について警察庁と交渉し、個人情報の提供を行わせた。

（出所）情報コミッショナー ホームページより

２．フランス

（１）個人情報保護制度の概要

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 78-17 号(Loi n ° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)。

同法は、2004 年 8 月 6 日の法律 2004-801 号（以下「2004 年法」という。）で大きく改正されている[1]。この改正は、1995 年の EU データ保護指令に対応するための改正を多数含んでいる。

②目的

情報の取扱いは、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。情報の取扱いが、人間のアイデンティティや人権、私生活、さらには、個人の又は公的な自由を侵害するものであってはならない（1 条)。

③適用範囲

個人情報取扱責任者（responsable d'un traitement de données à caractère personnel ）がフランス領内に在住しているか、又は、フランス領内に設置された取扱い手段を用いている場合（5 条）[2]、以下の取扱いに本法が適用される（2 条)。ただし、専ら個人的行為を行うことを目的とする場合を除く[3]。

ア）個人情報(données à caractère personnel)の自動処理(traitement automatisé)

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

2004 年の法改正以前は、対象機関についての定義がなかったが、EU データ保護指令 2 条(d)及び(e)に対応するため、2004 年改正法でこのような定めが置かれた。

---

[1] 本節における条文の引用は、特に断らない限り、2004 年に改正された「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」のものを示す。

[2] 5 条は、本法の適用につき、以下のいずれかがたされていることを求める。

（a）取扱責任者がフランス領内に在住していること。フランス領内で定住して活動している取扱責任者は、その法的形態がいかなるものであれ、在住しているとみなされる。

（b）取扱責任者が、フランス領内にも、他の欧州連合加盟国内にも在住していないが、フランス領内に設けられた処理手段を用いていること。ただし、その利用が、フランス領内又は他の欧州連合加盟国への情報移転のみを目的とする場合は除外される。

[3] 2004 年法改正以前は、適用対象外の個人情報取扱いを、ごく私的な取扱いのみに限定していたが（45 条)、2004 年改正法は、1995 年の EU データ保護指令第 3 条に対応するため、本文のような定めを用意した。v. Laffaire (M. -L), Protection des donneées a caractère personnel, Edition d'Organisation, 2005, p.36.

「個人情報取扱責任者」とは、法令の規定が明示的に定める場合を除き、取扱いの目的と方法を決定する個人、又は、公的な機関又は部局若しくは組織を意味する（3 条Ⅰ）。

「個人情報の取扱い」とは、個人情報に対して行われる作業(opération) 、又は、一連の作業を意味し、その手段を問わず、特に、収集(collecte)、記録(enregistrement)、編集(organisation)、蓄積(conservation)、修正(adaptation) 又は変更(modification) 、復旧(extraction)、参照(consultation)、利用(utilisation)、移転(transmission) や周知(diffusion) その他のあらゆる形態の開示(communication)、結合(rapprochement) や相互接続(interconnexion)、利用停止(verrouillage)、消去(effacement)、削除(destruction) を意味する（2 条）[4]。この規定は、EU データ保護指令 2 条(b)に対応するため、旧法よりも「個人情報の取扱い」の範囲を拡張する方向で、2004 年法により改正された。

④規制・権利の内容

ア）収集・取扱い

(ア)以下の原則の遵守が求められる（6 条)。

〈1〉公正かつ適法な収集・取扱い

〈2〉収集の目的[5]が、特定され、明白であり、かつ、正当なもので、更には、収集後にこの目的と相容れない手法で取り扱われないこと[6]。

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

〈4〉情報が正確かつ完全であり、必要に応じて最新のものであること。収集又は取扱目的に照らし、不正確又は不完全な情報が消去又は訂正されるよう、適切な措置がとられること。

〈5〉情報が、収集又は取扱目的に照らし、必要な期間を超えない期間、当該個人の識別が可能な形で保存されること。

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

---

[4] 2 条のこの部分の内容は、EU データ保護指令 2 条(b)とほぼ等しいので、同条の翻訳は、堀部政男「欧州連合(EU)個人情報保護指令の経緯」新聞研究 578 号(1999 年) 18 頁の翻訳に依拠している。

[5] 収集目的は、情報処理及び自由に関する国家委員会への届出や許可申請、意見申請の際に明記しなければならない（後述 2⑫ｳ)(エ)〈2〉参照)。

[6] ただし、事後の処理で統計作成や学術若しくは歴史研究を目的とするものは、取扱いに関する手続を遵守し、かつ、当該情報に含まれた個人を名宛人とする決定に利用されないものである限り、情報収集の当初の目的と整合するものとみなされる（6 条 2 °ただし書)。

(イ)センシティブ情報の収集については、後述(2)④参照。

(ウ)犯罪、有罪判決及び保安処分に関する個人情報の取扱いは、以下の場合に限り、許される（9条）。

〈1〉司法補助者(auxiliaire de justice)[7]が法律の定める任務を遂行するに当たってする必要最小限の取扱い。

〈2〉知的財産法典L321-1条及びL331-1条の定める法人が、自ら管理する権利の資格者として実施する取扱い。又は、同法典Ⅰ、Ⅱ及びⅢ部が定める権利の防御を確保するため、又は、当該権利を侵害された被害者のために実施する取扱い[8]。

(エ)個人情報を取り扱う場合は、本人の同意を得るのが原則だが、本人同意がなくても、以下の要件の一を満たしていれば認められる（7条）。

〈1〉取扱責任者に課せられる法的義務が遵守されていること。

〈2〉本人の生命を保護する目的であること。

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

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

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

2004年法改正以前は、センシティブ情報の収集（後述(２)④参照）を除き、本人同意は収集条件とされていなかったが、EUデータ保護指令7条に対応するため、2004年法改正で上記の原則が盛り込まれた。ただし、EUデータ保護指令2条(h)が「データ主体の同意」を定義し、また、同7条(a)は、「明確に」同意することを条件とするのに対し、本法は、同意の定義と、同意の性質を問わない点で、EUデータ保護指令よりも詳細さを欠くとの評価がある[10]。

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

〈1〉取扱責任者又はその代表者の身元

〈2〉取扱目的

---

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

[8] その他、公的部門にのみ許される場合として、裁判所、公的機関、及び、公役務を管理する法人が、その法的権限内において実施する場合がある。

[9] 「取得者」とは、「当該個人情報の開示を受ける権限を有する者で、当該個人、処理責任者、受託者及び職務上当該情報を処理する任務にある人々を除くすべての者」と定義されている(3条Ⅱ)。2004年法改正以前、取得者を定義する明文規定はなかったところ、EUデータ保護指令2条(ｇ)に対応するため、上記の規定が置かれた。

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

〈3〉回答の任意性
〈4〉回答拒否の場合の影響
〈5〉取得者の名称又は取得者の範疇
〈6〉アクセス権(後述（２）④エ)参照）などの権利
〈7〉場合によっては、EU 域外への情報移転。

・本人から直接収集する場合の通知については、2004 年法改正以前から一定の規制があったが、EU データ保護指令 10 条に対応するため、2004 年法改正で、通知事項が増加された。

・電子通信網のあらゆる利用者は、取扱責任者又はその代表者から、クッキーや接続証明の目的、及び、それらの取得を拒否しようとする場合に取り得る手段を、明確かつ完全な形で通知されなければならない（32 条Ⅱ）[11]。

以上の規制は、以下の場合に適用を除外される。

〈1〉事前に「情報処理及び自由に関する国家委員会（Commission nationale de l'informatique et des libertés, CNIL)」が、本法の定めに即すことを承認した短期間の匿名化処理（32 条Ⅳ）

〈2〉犯罪の予防や捜査、立証、起訴のための取扱い（32 条Ⅴ）。

(カ)個人情報が当該情報の本人から直接に収集されるわけではない場合(間接収集)、当該取扱いの責任者又はその代表者は、当該情報を記録してからすぐに、直接収集の場合と同じ情報を当該本人に通知しなければならない。第三者への開示を予定されている場合には、遅くとも、当該情報の最初の取扱いの前に通知されなければならない（32 条Ⅲ)。

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

イ）安全保護管理義務

個人情報取扱責任者は、個人情報の安全を確保するため、とりわけ歪曲、破損、又は、無許可の第三者アクセスを排除するため、あらゆる有効な予防措置を講じなければならない（34 条)。

ウ）第三者提供制限

特に第三者提供に的を絞った法制度は存在しない。ただし、第三者への提供についても、前述ア)(ア)の諸原則が適用される。

---

[11] 32 条Ⅱは、以下のように定める。「電子通信網(reseaux de communications électroniques) のあらゆる利用者は、処理責任者又はその代表者から、以下の事項を、明確かつ完全な形で通知されなければならない。
－接続端末設備に保存されている情報に電子伝達手段を用いたあらゆるアクセスの目的、又は、同様の手段を用いて接続端末設備に情報を記録するすべての行為の目的
－以上のことを個人が拒否しようとする場合にとり得る手段

エ）本人アクセス権

すべての自然人は、情報の取扱いを拒否する権利（前述ア）（エ）参照）の他、取扱責任者に質問する権利、自己情報の複写請求権、自己情報の訂正・利用停止・消去請求権を認められている[12]。

(ア)質問権

何人も、自己の身元を証明した上で、以下の事項を明らかにする目的で個人情報取扱責任者に質問する権利がある（39 条Ⅰ）。

〈1〉自己の個人情報が、当該取扱いの対象となっているかどうかの確認

〈2〉当該取扱いの目的や、取り扱われる個人情報の種類、それら個人情報が開示される第三者又はその種類についての情報

〈3〉必要があれば、EU 非加盟国在住の取得者に対する個人情報移転についての情報

〈4〉自己の個人情報、及び、その取得元に関して個人情報取扱責任者が保有しているすべての情報について、アクセス可能な情報の提供（後述（２）⑧参照）。

〈5〉自己に対して法的効果を有する決定が、自己の個人情報の自動処理に依拠してなされた場合に、当該自動処理の基礎となった論理を知悉し、かつ、異議申立を可能にするような情報。ただし、当該個人に知らされる情報は、知的財産法典Ⅰ部及びⅢ部 4 章の規定に反し、著作権を侵害するものであってはならない。

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

(イ)複写請求権

取扱責任者は、実費を超えない範囲で、複写交付の費用を徴収できる（39 条Ⅰ）。複写拒否事由は列挙されていないが、請求の数や反復性、体系性から濫用請求であることが明らかであれば、取扱責任者は要求を拒否できる。濫用の明白性は、取扱責任者が証明しなければならない（39 条Ⅱ）。

(ウ)質問権と複写請求権の例外

質問権と複写請求権に関する定めは、当該個人情報の保存が、請求者のプライバシーを侵害する危険が全くないことが明らかな形態で、かつ、専ら統計作成や学術歴史研究のために必要な期間を超えない期間においてなされている場合は適用されない（39 条Ⅱ）。

(エ)訂正・利用停止・消去請求権

後述（２）⑨参照。死者の個人情報の訂正については、後述（２）⑬参照。

(オ)監督・登録制度

後述（２）⑫ウ）参照。

---

[12] その他、特別のアクセス制度として、国家の安全や国防、治安に関する個人情報処理に関する各請求は、処理責任者ではなく、情報処理及び自由に関する国家委員会に設置された委員会になされるものがある(41 条)。

⑥主な適用除外

ア）インターネットプロバイダーがプロキシサーバにアクセスした際に生じる一次的な情報のコピー等は、本法の適用を除外される（4 条）[13]。これは、インターネット上の特殊性、とりわけ、キャッシュに伴う問題に配慮したもので、2000 年 6 月 8 日「情報社会における諸役務及び電子商取引に関する EU 指令 2000-31 号（電子商取引指令)」13 条に対応するため、2004 年法改正で導入された[14]。

イ）専ら医療研究のための自動処理は、情報処理及び自由に関する国家委員会への事前届出・許可（後述（２）⑫ウ)参照)、及び、収集時の本人通知（前述（１）④(オ)(カ)参照)、本人による処理拒否（前述（１）④ア)(ウ)参照）に関する制度の適用を除外される（53 条)。

ウ）報道目的及び文学芸術目的での個人情報取扱いについては、以下の制限が免除される。

(ア)保存期間の制限

(イ)センシティブ情報の収集禁止原則（後述（２）④参照）

(ウ)犯罪関係情報の収集禁止原則（前述(１)④ア)(ウ)参照）

(エ)情報処理及び自由に関する国家委員会への事前届出・許可制度（後述（２）⑫ウ)参照）

(オ)収集時の通知原則（前述（１）④(オ)(カ)参照）

(カ)本人アクセス（前述（１）④エ)参照）

(キ)EU 非加盟国への個人情報移転の原則（後述（２）⑩参照）

⑦主な自主規制

[制度について]

法律に自主規制に関する法制度はない。

[実態について]

・フランス銀行連盟においては、情報処理及び自由に関する国家委員会の指導により、消費者向けに個人情報保護に関する小冊子を作成している。この小冊子は国内の銀行に広く配布しており、ホームページにも掲載している。

・情報処理及び自由に関する国家委員会によると、自主規制の事例としては、ダイレクトマーケティング協会（Fevad）と通信販売協会の 2 つの事例があるとのことであ

[13] 4 条は以下のように定める。「本法の定めは、デジタル通信網にアクセスするための情報の転送や供給の技術的行為の枠内で、他の顧客に対し、伝達された情報への最良のアクセス可能手段を提供することを目的とした、自動的、過渡的、暫時的保存するための一時的コピーには適用されない」。

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

る。

・ダイレクトマーケティング協会には、1993 年に策定された自主規制としてのガイドラインがある。1997 年にマーケティングの大キャンペーンがあり、約 200 の質問に応えると関連したダイレクトメールが大量に送付されてくるという事件があった。その際、消費者から多数の要望があり、情報処理及び自由に関する国家委員会の指導の下、自主規制で問題を解決したという事例がある。

・一方で、情報処理及び自由に関する国家委員会は、各業界向けに対し、ガイドラインを作成するよう指導しているが、例えば鉄道・輸送業界では必ずしも作成していないというように、対応は様々である。

⑧その他

フランス個人情報保護法の特色は、独立行政委員会である情報処理及び自由に関する国家委員会に、強力な規制権限を認める点にある。この点については、後述（２）⑫参照。

（２）「個人情報保護に関する主な検討課題」関連項目に即した状況

①いわゆる「過剰反応」（誤解）に対応した第三者提供制限の例外事由

[現状について]

・情報処理及び自由に関する国家委員会へのヒアリングによると、フランスで「過剰反応」に相当する事案は聞いたことがないとのことであった。通常、個人情報の取得時に、第三者提供（取得者）についても通知しなければならないため（前述（１）④ア）（オ）（カ）参照)、第三者提供時に「過剰反応」のような問題は起こらないはずであるとの指摘があった。

・フランスでは、例えば、病院に対する安否確認については、病院ではなく警察が対応しており、緊急事態であれば、警察が家族に伝えるのが通常である。怪我をした人がいれば、その人のバッグなどから連絡先を探し、家族に連絡を取ろうとするのが普通の対応である。家族に言えないような事情があれば、連絡しないかもしれないが、それは特殊なケースであるとのことである。

・国に提供するのは、法律に根拠がある場合か、本人の同意を得た場合に限られる（前述（１）④ア）（エ）〈3〉参照)。各主体は個人のプライバシー保護に配慮しながら、状況に応じて対応しているとのことであった。

・フランスでは、医療情報についても医療関連の法律で厳格に保護されているとのことである。医療関係の個人情報保護は 200 年以上の伝統があるので、現在では混乱はない。診療情報の医療研究への提供については関心も高く、特別の同意が必要である。インターネットで収集する医療情報については、商用目的での譲渡を制限するように

呼びかけているとのことである。
・また、個人情報を統計目的で利用する場合は、目的を記載した上、調査後にはファイルを消去するため、あまり問題は起きないとのことである。
・また、ダイレクトマーケティング協会へのヒアリングにおいては、警察から、クレジットカード犯罪等に関する情報提供依頼は頻繁にあるとのことであったが、義務であるため、提供は拒否していないとのことであった。銀行も警察から口座情報の提供依頼を受けることがあるが、提供は拒否していないとのことである（前述（１）④ア)(エ)〈3〉参照)。
・また、フランス国営鉄道でもフランスで「過剰反応」に相当する事案は聞いたことがないとの回答が得られた。目的外利用の場合については、罰則が厳格に定められているので（後述（２）⑭ア)(ス)参照)、問題は無いと考えられるとのことである。
・例えば、死傷者に関して家族から安否確認があっても、これに応ずる権限があるのは警察と軍だけであるため、列車事故が発生し、家族から問い合わせがあっても、国鉄は手助けを行うだけで、積極的な関与はしておらず、そもそも、チケットに名前などは記載されていないので問題は無いという認識であった。

[制度について]
第三者への提供制限に特化した規制はない。収集や利用に関する制限についての法律の定めがこの点を規制することになる（前述（１）④ア)(ア)参照)。

②自治会や同窓会等の取扱い

[制度について]
情報処理及び自由に関する国家委員会へのヒアリングによると、フランスには自治会名簿や地域の名簿は存在せず、仮にそのような名簿を作成・配布する場合でも、本人の同意が必要であり、法律による規制の対象となるということである。

[制度の運用について]
・情報処理及び自由に関する国家委員会へのヒアリングによると、企業が従業員名簿を組合に渡すことは原則として禁止されているとのことである。児童名簿をテニス協会のような組織に渡すことも同様である。
・同窓会事務局も、情報処理及び自由に関する国家委員会への届出が必要とのことであり、特別扱いはされていない。ただし、企業は同窓会名簿を販売促進のために使いたいと思っているようであるとの指摘があった。

③「個人情報」の定義

ア）現行法は、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（numéro d'identification）又は個人に固有の一若しくは複数の要素を参照することで、直

接又は間接に個人を識別し又は識別可能なもの」と定義する（2 条）。

なお、「個人を識別し得るか否かを判定するには、取扱責任者その他すべての人々が保有している手段、又は、アクセス可能な個人識別可能手段のすべてを考慮すべき」とされている（モザイク・アプローチ）（2 条）。これは、EU データ保護指令前文（26）に対応するため、2004 年法で改正された点である。

イ）個人情報のうち、特定の指標に従ってアクセスできるように構成され安定した体系となっているものを、個人情報ファイル(fichier de donées à caractère personnel) という（2 条）。

情報処理及び自由に関する国家委員会へのヒアリングによれば、情報の種類は問わず、私生活の情報も、医師が職業上作成した診断書も対象となり、媒体も問わず、紙も絵も対象で、性質も問わず、車のナンバーも電話番号も対象であるとのことである。

なお、年齢、性別、生活する場所、職業など、４～5 つの情報をテレビで流せば、概ね個人が特定できるという指摘もなされているということである。

④センシティブ情報に関する規定

[制度について]

ア）現行法は、センシティブ情報を、「人種や民族的起源、政治的、哲学的又は宗教的意見、労働組合への所属が直接又は間接的に明らかになる個人情報、又は、健康若しくは性生活に関する個人情報」と定義する（8 条Ⅰ）。

イ）現行法は、センシティブ情報の収集・取扱いを、原則として禁止するが、以下の場合を例外とする（8 条Ⅱ）[15]。

(ア)本人の明示的同意がある場合

(イ)人の生命を保護するために必要であり、かつ、本人が法的無能力又は物的不可能性のため、同意を与えることができない場合。

(ウ)宗教、哲学、政治又は労働運動に関する非営利の結社その他組織が実施する取扱いで、当該結社・組織の目的に即した情報を対象とし、その構成員や定期的に当該結社等と接触がある個人のみに関わるもので、しかも、本人の明示的同意なしには第三者に伝達されない情報の取扱いの場合。

(エ)当該本人が公表している個人情報の取扱い

(オ)裁判上の権利の証明、行使又は防御に必要な取扱い

(カ)医療専門職、又は、職業上の秘密保守義務(obligation de secret professionnel) が課せられている人々（刑法典 226-13 条）が実施する予防医療、診断、看護若しくは処置の管理や、厚生役務の管理に必要な取扱い

[15] 本文で列挙したものの他、公的部門に特有のものとして、国立統計経済研究所(Institut National de la Statistique et des Études économiques: INSEE)や各省統計関係部局の一が実施する統計処理がある。

(キ)医療研究に必要な取扱いで、一定の方式に従うもの

ウ）その他、公益上の取扱いが認められ、かつ、情報処理及び自由に関する国家委員会が本法の定めに適合すると事前に承認した、短期の匿名での取扱いを目的とする取扱いも例外的に認められる(後述（２）⑫ウ）（ウ）参照)。

エ）センシティブ情報を取り扱う場合は、事前に、コンセイユ・デタ（国務院）[16]の議を経るデクレ(décret en Conseil d'Etat)[17]による許可を要するところ、この許可は、情報処理及び自由に関する国家委員会の意見を経て下される。この意見は、許可と同時に公表される（26 条Ⅱ）（後述（２）ウ)(エ)参照)。

2004 年法改正以前、センシティブ情報の収集が認められるのは、事前に本人による明示の同意があった場合に限定されていたが、EU データ保護指令 8 条に対応するため、上記のような規制に改正された。

[制度の運用について]

・情報処理及び自由に関する国家委員会へのヒアリングにおいては、差別・偏見につながり得るものがセンシティブ情報とされているが、センシティブ情報の内容は状況によって変化するとの指摘があった。また、フランスでは組合活動は政治的な活動として捉えられており、組合の管理職は選挙によって選ばれるので、企業も幹部の情報は知りえるが、組合の一般の構成員については知りえない状況であるということである。
・なお、社員の健康情報については、会社の担当医師は知りえるが、会社の役員や管理職はアクセスできないとのことである。なお、この点に関連して、従業員は病気になっても会社に報告する義務は無いと考えられているとのことである。信頼関係があれば、任意で報告することはあるという。管理職が担当医師などの第三者から健康情報の提供を受け、何らかの対応を行うことはできないとのことである。
・また、同僚であっても個人の信条などについて質問することは、原則として禁止される。
・民族的な出自は移民の問題があるため、議論になっている。企業はアジア系、アフリカ系といった、出自地域別の管理職数などを把握するため、社内の民族構成の統計を取ろうとすることがあり、現在は国籍、生まれた場所だけが統計として取られている。これ以上の情報を統計にするのであれば、民族の分類などの点で、大議論になることが想定されるとのことである。移民問題は本来国会で扱われるような内容であり、情

[16] 行政裁判の最上級裁判所。政府の準備する法令案などの諮問に対する答申も発する。

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

報処理及び自由に関する国家委員会が解決方法を提案するかどうかは検討中である。民族的出自は国籍と誕生地、両親の誕生地以外は踏み込めないのではないかと感じているとのことであった。

・もちろん、特定の場面では、これらのセンシティブ情報の利用が必要になることもあることについても指摘が為された。

⑤小規模事業者の取扱い

[現状について]

・情報処理及び自由に関する国家委員会へのヒアリングによると、小規模事業者は個人情報保護に必ずしも十分な対応を行っていない場合もあるということであった。

・中には、個人情報保護についてほとんど認識がないような事業者も存在しており、小規模事業者に対して個人情報保護法の周知を進めることが重要であるという認識も示された。

・また、ダイレクトマーケティング協会へのヒアリングによると、Web サイトなどで個人情報保護に取り組んでいることを掲載している小規模事業者も多いが、事業者自身が個人情報保護法をほとんど理解していないことが多いとのことである。

・例えば“収集拒否”の申出ができることを記載していても、実際に申出があったときの対応方法を準備していない場合があるとのことである。大企業には個人情報保護担当の専門家が配置されているが、小規模事業者では社長が独自に法律を解釈して対応している場合もあるようである。

・ダイレクトマーケティング業界は個人情報保護に対する認識が高いので、どのように小さな事業者であろうと対応をしているはずである。個人情報保護法のは進化に現場が追いついておらず、小規模事業者の場合にはこの傾向が顕著であるとのことである。小規模事業者向けの簡素でわかりやすい法律が必要ではないかという指摘があった。

[制度について]

法制度上、特別な扱いはされていない。

[制度の運用について]

・情報処理及び自由に関する国家委員会へのヒアリングにおいては、小規模事業者の監督は課題であるという指摘があった。業界団体に属している企業には比較的目が届くものの、それ以外の事業者については監督が難しく、今後は公認会計士や弁護士を通じての監督などを検討していく必要があるという認識が示された。

・ただし、小規模事業者でスパムメールを送った場合に、勧告や制裁を実施したこともある（フランス国内のスパムメール送信者は世界全体の 3%程度であり、割合は少ないとのこと。）とのことであり、運用上も問題のあるケースは小規模事業者であっても実効力を伴う監督を実施しているとのことである。

・個人情報保護に対する事業者の認知度を高めるために、商工会議所を通じ、年間 300 回のカンファレンスを開催したり、個人情報保護の重要性を取り上げた児童向けのゲームを作成している他、大学などと連携して、卒業生すべてに情報処理及び自由に関する国家委員会の活動を周知するような活動も実施しているとのことである。

⑥個人情報の目的外利用の防止措置

[現状について]

・ヒアリングによると、目的外利用も一部では見られるようである。
・ダイレクトマーケティング協会へのヒアリングによると、目的外利用ではないが、事業者間で名簿の交換を行っているとのことである。性別、子どもの有無、ダイレクトマーケティング購入履歴などが含まれている名簿が交換されているそうである。
・また、事業者から顧客情報を収集し、新たな名簿の作成・編集を行う事業者が存在するとのことである。ダイレクトマーケティングを行う企業は、こうした事業者にデータの整理をしてもらっているが、「利用目的」を契約に記載しているため、名簿作成・編集事業者による目的外利用は発生しないのが通常であるとのことである。なお、名簿作成、編集事業者への情報開示の可否については、情報収集時に本人から確認を取っているとのことである。
・名簿作成・編集事業者とは別に、リストブローカーも 100 社程度存在している。名簿を集める会社と、それを調製する会社に分かれている。例えば結婚の公示や、家の新築許可の公示情報を収集する会社もあるとのことである。納税者番号も公示されるが、これは政府からリストブローカーに販売されるとのことである。
・同窓会、同好会の名簿も収集され、販売・貸与されているとのことである。貸与はキャンペーンのような場合の一時的利用のために行われるが、この場合はダイレクトメールの発送は名簿事業者が行うため、実際に名簿そのものが貸与を受ける事業者に提供されるわけではないとのことである。

[制度について]

現行法は、「収集の目的が、特定され、明白であり、かつ、正当なもので、更には、収集後にこの目的と相容れない手法で取扱われないこと」との原則により、目的外利用を制限している（6 条Ⅰ②）（前述(１)④ア）参照)。

また、「情報が、収集又は取扱目的に照らし、必要な期間を超えない期間、当該個人の識別可能な形で保存されること」との原則により、利用目的に照らして不必要な情報の保存を制限している（６条Ⅰ⑤）（前述(１)④ア）参照)。

法制度上、保存期間を超えて保存されている情報の目的外利用が許されるのは、以下の場合に限定されている（36 条）

ア）歴史的、科学的又は統計処理上の目的による取扱いの場合

イ）本人の明示的同意がある場合

ウ）情報処理及び自由に関する国家委員会の許可がある場合

なお、情報処理及び自由に関する国家委員会へのヒアリングよると、情報の利用は、取得した際の目的に縛られ、利用目的を変えるときには再度同意を取らなければならない（上述の（２）⑥イ）参照）とのことである。

[制度の運用について]

・ダイレクトマーケティング協会でのヒアリングによると、フランスには、「ダイレクトメールの送信を拒否することを明示した者」のリストが目的外利用防止に一定の役割を果たしているようである。そのようなリストは、ダイレクトマーケティング協会等の業界団体で作成し、会員に配布している。イギリスでは、電話など営業媒体ごとに「送付拒否者リスト」が存在しているが、フランスにはまだないとのことである。
・なお、プリペイド式の携帯電話について、“偽りのプリペイド番号を作成して通話だけ行い、支払いが行われない”、という事態が発生したことを受け、クレジットカード会社と携帯電話会社がブラックリストを交換しようとしたことがある。その際、情報処理及び自由に関する国家委員会がリスト作成停止を求め、その後、ブラックリスト作成時の規則を作成し、その範囲内で作成・交換することを許可した事例がある（後述（２）⑫ウ)(ウ)〈4〉参照）とのことである。

⑦市販の名簿の管理

[現状について]

・情報処理及び自由に関する国家委員会へのヒアリングによると、フランスにも市販の名簿は多数あるが、流通量や名簿に掲載されている人数による規制の区別は無いとのことである。
・ダイレクトマーケティング業界へのヒアリングによると、CD-ROM などで名簿が売られていることはあるが、広く一般的に購入できるような名簿はあまり存在しないとのことである。市販の CD-ROM については機密情報として取り扱っており、一般ゴミとして道端に捨てるようなことは考えられないとのことである。
・無差別に抽出したリストは販売して良いが、一定の目的で抽出したリストは販売してはいけないことになっているとのことである。
・電話帳はダイレクトマーケティングを行う際には頻繁に使用するが、その際、電話帳に公開されている情報をそのまま利用するのではなく、フランステレコムに対象者を絞った名簿を作成してもらい、購入しているとのことであった。
・一方で、インターネットの電話帳から勝手に情報名簿を作成し、販売している違反事業者もいるとのことである。
・なお、フランス国営鉄道へのヒアリングによると、外部の名簿を利用したことはなく、個人情報は自社で直接取得しているとのことである。また、鉄道はほとんどの国民が

利用するものであるため、電話帳などを使ってこちらから売り込みを行うことはないということである。

[制度について]

法制度上、特に規制はない。通常の個人情報の取扱いと同様の規制に服する。

[制度の運用について]

・情報処理及び自由に関する国家委員会へのヒアリングによると、法律上は電話帳もほかの名簿などと全く区別されていない。
・この点、市販の名簿作成者は、本人から個人情報を取得する際、市販される可能性があることを示しているはずであり、電話帳の個人情報は公開が前提となっているので、企業が電話帳を道端に捨てても、責任は問われないという取扱いをしているとのことであった。
・電話帳を捨てた方は問題ないが、拾って使用した方が責任を問われることになるとのことである。
・なおフランステレコムは、情報処理及び自由に関する国家委員会の指導により、掲載拒否者のリスト（レッドリスト）を作成している。これにより、20%の国民は電話帳に名前を掲載していない。また、商業的利用拒否者リスト（オレンジリスト）も作成されている。
・電話帳については電話事業の民間開放の進展により、複雑な問題がでてきているとのことである。例えば、電話会社を変更すると、その度に名前を掲載するかどうかを判断しなくてはならないが、これに対する理解が進んでいないため、啓蒙が必要である。また、フランスレコム以外の電話帳にはオレンジリストの目印がないため、企業は各電話会社に高額の手数料を支払って、商業利用の可否を照会しなくてはならないとのことである。
・他にフランスで問題になっているのは、百貨店や航空会社のクラブメンバーの個人情報であるという。家族の情報なども詳細に掲載されているため、厳格に取り扱うべきだという議論があり、消費者のプロフィールは、センシティブ情報（前述（２）④参照）として取り扱う方向で議論が進んでいる。なお、メンバーズカードはグループ企業内だけで利用されるものであり、グループ外への提供事例は報告されていない。
・フランスには、「一般に利用可能」（Public Avairable）という概念は無い。EU データ保護指令の作成時に、そのような概念は認められなかった。
・商業的利用を拒否したにもかかわらず商業的利用をされた場合、当該個人は、情報処理及び自由に関する国家委員会に苦情を申し立てることになる（後述（２）⑫ア）参照）。

・ダイレクトマーケティング協会でのヒアリングによると、フランステレコムは、オレンジリストを作成しているが、他の電話会社には影響力がないため、実効性に問題が

あるとのことである。

⑧個人情報の取得元の開示に関する措置

[現状について]

・フランス銀行連盟へのヒアリングによると、取得元に関する顧客からの質問請求数などは把握していないとのことであった。顧客からは、“（取得元開示の）要望の申出先の担当者が分かりにくい”という声があるとのことである。

・一方、情報処理及び自由に関する国家委員会へのヒアリングによると、取得元の開示に関しては、週に 20 件程の問合せがあるとのことであった。

・また、ダイレクトマーケティング協会へのヒアリングによると、消費者から、どのようにして自分の住所を知ったのかなど、取得元に関する問い合わせが来ることはあるが、件数はそれほど多くないとのことである。

・また、フランス国営鉄道からのヒアリングによると、取得元に関する開示請求について、集計は行っていないが、非常に少ないという感触があるとのことであった。開示請求等については、個人情報保護監督者（後述(２)⑫ウ)(ア)参照）が対応しているが、職員総数は約 16 万人にもかかわらず、この監督者は１人であることが、請求の少なさを示唆しているとの指摘がなされた。

[制度について]

現行法は、「あらゆる人は、自己の個人情報の取得元に関して個人情報取扱責任者が保有している情報につき、アクセス可能な情報提供」を得るために、当該責任者に質問することができる」としている（39 条Ⅰ④）（前述(１)④エ)参照)。

[制度の運用について]

・情報処理及び自由に関する国家委員会へのヒアリングにおいて、取得元が分かりにくい場合は、情報処理及び自由に関する国家委員会が本人に代わって開示を求めることがあるとのことである。

・ダイレクトメールにコード番号が書いてある場合は、情報処理及び自由に関する国家委員会が問い合わせを行うと、その情報がどこから来たのかが追跡できるケースがあるとのことである。

・情報処理及び自由に関する国家委員会の認識によると、取得元を記録する義務はないが、取得元を開示する義務があるため、通常は作成しているはずであるとのことである。

・個人情報保護法の理解が進んできたので、自分で利用停止請求などを行う事例が増えてきているとの見解が示され、最初に情報を収集した事業者に対する消去の要望が多いとのことであった。

[事業者の対応について]

・ダイレクトマーケティング協会へのヒアリングによると、法律上、取得元の記録は義務ではないが、マーケティング上はデータの有効性が重要であるから、ビジネス上の必要性から取得元を記録しているとのことであった。
・なお、取得元を開示する場合は、具体的な事業者名を明示するとのことである。
・また、フランス国営鉄道からのヒアリングによると、直接取得がほとんどであるとのことである。支払いまでの間は、「Web で取得した」、「窓口で取得した」といった取得元情報を保管しているが、支払終了後に削除するようにしている。したがって、取得元に関する問い合わせがあった場合、「自社で取得したものである」ということしか本人に伝えないとのことであった。

⑨個人情報の利用停止・消去に関する措置

[現状について] [18]

・フランス銀行連盟からのヒアリングによると、実際の請求件数は把握していないとのことである。
・また、ダイレクトマーケティング協会へのヒアリングによると、消費者から協会に対し、ダイレクトメールが多数寄せられるので停止して欲しい、又は、自分の名簿を売らないで欲しいといった要望が寄せられることがあるとのことである。最近の傾向としては、Ｅメールによる広告の受け取りを拒否したいという要望が寄せられるようになってきており、電話による案内・調査を拒否したいという要望もあるとのことである。
・利用停止の請求件数は、名簿掲載者の 1%以下である。感覚的には、“ 100 万人にダイレクトメールを送って、100 件の請求が来るかどうか ” である、とのことである。

[制度について]

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

この請求を関係者が実際にした場合、取扱責任者は、請求者に費用を負担させない形で、必要な取扱いを実施したことを証明しなければならない（40 条）。

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

[18] 情報処理及び自由に関する国家委員会が 2006 年に公表した年次報告書 <http://www.ladocumentationfrancaise.fr/rapports-publics/064000317/index.shtml>によると、同委員会に対するアクセス権行使は、2004 年で 1,970 件、2005 年で 1,760 件となっているが、これはいずれも、国家の安全や国防、治安に関する個人情報処理に関する各請求である。前掲注（13）参照。

取扱責任者の負担となる（40 条)。
以上につき、前述（１）④エ)参照。

[制度の運用について]
・情報処理及び自由に関する国家委員会からのヒアリングによると、個人情報の保管期間として、2 回ダイレクトメールを発送して消費者から反応がなかった場合は、リストからその情報を削除するよう指導しているとのことである。
・法律上の義務ではないが、2 回反応が無ければ、利用価値が無いといえるのではないかと考えられており、事業者もコストを削減できると考えているとのことである。

〔事業者の対応について〕
・ダイレクトマーケティング協会へのヒアリングによると、販売促進目的の電話はオプトアウト方式であるため、電話がかかってきた時点で拒絶する者が多いというのが実態であるとのことである。
・個人情報の利用停止・消去をすぐに行わないと、情報主体から情報処理及び自由に関する国家委員会に対して苦情が寄せられるので、企業はすぐに対応するのが通常であるとのことである。
・利用停止・消去の請求について、多くの場合は利用停止のみで対応しているとのことである。通常、消費者は複数の事業者に個人情報を提供しているため、一箇所で消去しても解決にならないことが背景にあり、リスト上では利用を望まない者に印を付けてその旨を明確にするとともに、第三者に開示する場合は、印を付けたままで開示しているとのことである。
・また、国営鉄道へのヒアリングによると、利用停止・消去については国営鉄道のホームページ上で本人自ら操作できるようになっているとのことであり、顧客が販促情報を受け取りたくないという申出をすれば、販促対象者から削除するとのことである。

⑩国際的な情報移転に関する規定

[制度について]
現行法は、情報取扱責任者が EU 非加盟国に個人情報を移転できる場合を、対象国が、個人情報の取扱いに関し、プライバシーや基本的権利に対する十分な水準の保護を確保している場合に限定している（68 条)。ただし、以下の場合は、例外が認められる（69 条)。
（ア）本人による明示の同意があった場合
（イ）当該個人の生命を保護する目的の場合
（ウ）公益の保護を目的とする場合
（エ）犯罪の立証や刑罰の執行、又は、裁判における権利擁護を目的とする場合
（オ）法令の規定が公衆への情報提供を定めており、かつ、あらゆる人の閲覧に供さ

れるものとされている記録簿の適正な閲覧の場合
（カ）当該取扱責任者と当該本人との間で締結された契約を執行する目的の場合
（キ）当該取扱責任者と第三者の間で締結された契約の執行、又は、予定された契約の締結を目的とし、かつ、当該本人の利益を損なわない場合

2004 年法改正以前も、国外への情報移転は、コンセイユ・デタの議を経るデクレが定めるところにより、事前の許可を要するものとされていたが（旧法 24 条）、許可条件を定めるデクレは制定されることがなかったため、実質的には機能していなかった[19]。2004 年改正法は、EU データ保護指令 25 条に対応するため、上記のような制度を整備した。

[法律以外の枠組みについて]
・情報処理及び自由に関する国家委員会へのヒアリングによると、個人情報の第三国移転に対する規制としては、法律以外にも、「契約」による場合と、「拘束力のある企業ルール」による場合があるということである。

[国際移転に関する問題]
・フランス銀行連盟へのヒアリングによると、銀行間の送金のために作られる SWIFT コードを含む名簿が、アメリカの国家安全保障法に基づき、フランスの銀行からアメリカに流れたことがある。情報提供ができないと日常業務に支障が出るが、顧客に一切通知が無かったため大問題となり、情報処理及び自由に関する国家委員会からも厳しく追及されたケースがあるとのことである。
・外国の銀行の場合でも、本社の所在地にかかわらず、フランス国内に所在する支社はフランス法の適用を受けるため、フランスの支店から顧客情報をアメリカや日本にある本社に提供できるかどうかが問題になるとのことである。この点についても、情報処理及び自由に関する国家委員会は非常に厳しく規制しているとのことである。
・情報処理及び自由に関する国家委員会は EU データ保護指令 25 条を根拠にしている。また、情報処理及び自由に関する国家委員会は、法 68 条に基づき、厳格な指導を行っているとのことである。
・銀行のリスク管理のために、マネーロンダリング対策も含め、銀行間での国際的な顧客情報の交換に関する規制緩和が議論になっており、EU データ保護指令や法律の改正が必要だと感じているとのことである。
・また、ダイレクトマーケティング協会へのヒアリングによると、フランス語圏の国にコールセンターなどを設置する企業が多いが、個人情報をチュニジアやモロッコ、インドなどに移転した場合、移転先の国が個人情報保護に取り組んでいないことから、フランス企業が一切責任を取らないことが多いという問題があることが指摘された。

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

⑪EU データ保護指令に対する対応状況

現行年法は 2004 年に大きく改正されたものだが、この改正は、EU データ保護指令に対応することを目的の一つとしていた。主たる改正点は、次のとおり。

ア）個人情報の定義において、個人識別可能手段のすべてについて考慮すべきとした（2 条）－EU データ保護指令前文（26）に対応（前述（２）③参照)。

イ）個人情報取扱いの範囲を拡張（2 条）－EU データ保護指令 2 条(b)に対応（前述（１）③参照)。

ウ）適用対象機関の定義を明記(3 条Ⅰ）－EU データ保護指令 2 条(d)(e)に対応（前述（１）③参照)。

エ）取得者の定義を明記(3 条Ⅱ）－EU データ保護指令 2 条(g)に対応（脚注 10 参照)。

オ）個人情報取扱いに関する諸原則を明示（6 条）－EU データ保護指令 6 条に対応（前述（１）④ア)(ア)参照)。

カ）個人情報収集にあたり、本人の同意があることを原則とした（7 条）－EU データ保護指令 7 条に対応（前述（１）④ア)(エ)参照)。

キ）センシティブ情報の例外的収集につき、例外的に収集可能な場合を明記した（8 条Ⅱ）－EU データ保護指令 8 条に対応（前述（２）④イ）ウ)参照)。

ク）本人から直接に個人情報を収集する際（直接収集）における本人通知事項を増加（32 条Ⅰ）－EU データ保護指令 10 条に対応（前述（１）④ア)(オ)参照)。

ケ）本人から直接に個人情報を収集するわけではない場合（間接収集）における本人通知制度を整備（32 条Ⅲ）－EU データ保護指令 11 条に対応（前述（１）④ア)(カ)参照)。

コ）取扱いに対する事前規制が、公的部門と民間部門の場合で明確に区別されていたのが、情報取扱いの種別による区別に変更（22 条～29 条）－EU データ保護指令 18 条に対応（後述（２）⑫ウ）参照)。

サ）EU 非加盟国への情報移転に対する規制制度を整備－EU データ保護指令 25 条に対応（前述（２）⑩参照)。

ダイレクトマーケティング協会へのヒアリングによると、EU データ保護指令の内容については、現時点では要望を出してはいないが、EU データ保護指令の改正論議も出始めているとのことである。

⑫第三者機関の概要

[制度について]

ア）フランス個人情報保護法の特色は、独立行政委員会である情報処理及び自由に関する国家委員会に、強力な規制権限を認める点にある。

現行法は、同委員会が独立行政委員会であることを明記し（11 条)、委員はその権限行

使に当たり、いかなる機関の指揮も受けないと定める（21 条 1 項)。

同委員会の具体的権限としては、事前規制権限と（ウ)以下)、義務違反行為に対する制裁権限（後述⑭イ)参照）の他、苦情処理、助言、違法行為についての告発、調査及び物件収集、政府及び民間団体への助言等の権限（11 条）がある。さらに、権利や自由に対する重大かつ急迫の侵害があると認める場合、委員長は、管轄裁判所に対し、仮処分手続(référé)をもって、当該権利自由の擁護に必要なあらゆる安全保護措置(mesure de sécurité)を、場合によっては罰金強制(astreinte)付で命じるよう求めることができる(45 条Ⅲ)。

イ）同委員会は、以下の委員（計 17 名）で構成される(13 条Ⅰ)。いずれも任期 5 年で再任が可能である（13 条Ⅱ)。

(ア)上下院議院各 2 名

(イ)経済・社会評議会(Conseil Économique et Social)[20]の委員 2 名

(ウ)コンセイユ・デタの現職又は元裁判官 2 名

(エ)破毀院(Cour de Cassation)[21]の現職又は元裁判官 2 名

(オ)会計院(Cour des Comptes)[22]の現職又は元裁判官 2 名

(カ)有識者 5 名

ウ）情報取扱責任者は、情報の取扱いにあたり、文化財法典 2 編に従った古文書の長期保全のみを目的とした取扱い（36 条）を除き、原則として、情報処理及び自由に関する国家委員会に対し、事前に届け出るか、又はその許可を得なければならない[23]。

2004 年法改正以前における情報処理及び自由に関する国家委員会の事前規制は、公的部門と民間部門で全く異なる内容であったところ、EU データ保護指令 18 条に対応するため、2004 年法改正により官民共通の規制が導入された。

(ア)個人情報を自動処理する場合、原則として、情報処理及び自由に関する国家委員会への届出が義務付けられる（22 条Ⅰ)。届出がされると、情報処理及び自由に関する国家委員会が受領証を交付し、これによって取扱いが可能になる（23 条Ⅰ)。

届出義務が除外されるのは、次のとおり。

〈1〉公衆一般の閲覧に供することを専らの目的とした登録簿の取扱い（22 条Ⅱ②）

---

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

[21] 民事及び刑事裁判の最上級裁判所。

[22] 公会計に関する一般的裁判管轄権を有する行政裁判所。

[23] 本文で紹介する届出及び許可制度の他、公的部門による処理に対する特有の規制として、情報処理及び自由に関する国家委員会の意見を経て大臣アレテ(省令）(arêté)の形式で下される許可の制度がある(26 条Ⅰ)。

〈2〉収集後、事前に情報処理及び自由に関する国家委員会の承認を受けた匿名化方式による処理に遅滞なく付されるセンシティブ情報の取扱い(22条Ⅱ②)(前述(2)④参照)

〈3〉取扱責任者が、本法の定める諸義務の尊重を独立に確保することを責務とする個人情報保護監督者(correspondant à la protection des données à caractère personnel)を選任した場合[24]。ただし、EU非加盟国に在住する取得者に個人情報を移転することが企図されている場合を除く(22条Ⅲ)。

(イ)ごく日常的な個人情報の取扱いであり、かつ、その実施が、プライバシーや個人の自由に影響を与える可能性がないものは、簡易届出(déclaration simplifiée)制度の対象となる。これは、情報処理及び自由に関する国家委員会が簡易届出の対象となる取扱いの種類を示す簡易化基準(normes simplifiées)を公示し、その一に合致すると思料した取扱責任者がその旨を届け出れば、取扱いが可能になるという制度である。いわば、情報処理及び自由に関する国家委員会による認証制度とイメージできる。

簡易化基準は、以下のことを明らかにする(24条Ⅰ)。

〈1〉簡易届出の対象となる取扱いの目的

〈2〉取扱われる個人情報の種類

〈3〉関係する個人の種類

〈4〉当該個人情報の開示を受ける取得者の種類

〈5〉個人情報の保存期間

例えば、情報処理及び自由に関する国家委員会は、簡易化基準の一つとして、人事管理に関する個人情報の取扱を簡易届出の対象としている(2005年1月13日公示[25])。

さらに、情報処理及び自由に関する国家委員会は、取り扱われる個人情報の目的や、当該情報の取得者の種類、保存期間や関係個人の種類を考慮した上で、簡易届出さえも免除できる取扱いを指定することができる(24条Ⅱ)。例えば、被用者への給与支払いに関する個人情報の取扱いがその例である(2004年12月9日公示[26])。

---

[24] 監督者の選任は、情報処理及び自由に関する国家委員会に通知される(22条Ⅲ2項)。

[25] この簡易化基準は、公的部門の人事管理も対象としている。Norme simplifiée n° 46, Délibération n° 2005-002 du 13 janvier 2005 portant adoption d'une norme destinée à simplifier l'obligation de déclaration des traitements mis en œuvre par les organismes publics et privés pour la gestion de leurs personnels <http://www.cnil.fr/index.php?id=1231>。

[26] Dispense de déclaration n° 1, Délibération n° 2004-096 du 9 décembre 2004 décidant la dispense de déclaration des traitements de gestion des rémunérations mis en œuvre par l'Etat, les collectivités locales, les établissements publics et les personnes morales de droit privé gérant un service public<http://www.cnil.fr/index.php?id=1749>。この指定は、公的部門の人事管理も対象としている。

(ウ)以下の場合、原則として、事前に情報処理及び自由に関する国家委員会の許可を要する（25 条Ⅰ[27]）。

〈1〉センシティブ情報を遅滞なく匿名化した取扱い、及び、公益上の必要が認められるセンシティブ情報の取扱い（前述（２）④参照）

〈2〉遺伝情報に対する自動処理であって、医師や生物学者によってなされ、かつ、予防治療や診断、医療目的の処理ではない場合。

〈3〉自動処理か否かを問わず、犯罪や有罪判決、保安処分に関する取扱い。ただし、司法補助者が関係個人を弁護する任務に必要な場合を除く。

〈4〉法的利益や契約上の利益を個人からはく奪する自動処理であるが、法令による保護が欠如している自動処理

〈5〉別法人に属するファイルを、主たる目的が異なるファイルと相互接続するための取扱い（25 条Ⅰ⑤）[28]

〈6〉個人識別全国名簿(répertoire national d'identification des personnes physique)[29]記載の登録番号が含まれている取扱い。

〈7〉個人の社会的困窮に対する評価を含む情報の自動処理。

〈8〉個人の調査に必要な生体統計学的情報を含む自動処理。

許可申請があった場合、情報処理及び自由に関する国家委員会は、原則として、申請から 2 か月以内に諾否の応答をしなければならない。この期間は、委員長の理由付決定があれば、一回まで延長できる。期間内に委員会が諾否の応答をしない場合は、許可申請は拒否されたものとみなされる(25 条Ⅲ)。

委員会が許可をする際、以下の諸事項が明らかにされる（29 条)。

〈1〉取扱いの名称と目的

〈2〉委員会による制裁処分（後述⑭イ)参照）の前に行われる聴聞手続が実施される部署

〈3〉登録される個人情報の範疇

〈4〉当該情報の開示を受けることができる取得者又はその範疇

(エ)センシティブ情報の取扱いについては、事前に、コンセイユ・デタの議を経るデクレの形式で下される許可を要する[30]。この許可は、情報処理及び自由に関する国家委員会

[27] 本文で紹介するものの他、公的部門による一定の取扱いについても、情報処理及び自由に関する国家委員会の事前許可が必要になることがある（25 条Ⅰ）。

[28] 25 条Ⅰ⑤は、公的部門に特有のものとして、公役務を管理する一又は複数法人に属するファイルで、目的が異なる公益に係るものの相互接続を目的とする取扱いも挙げている。

[29] 国立統計経済研究所(INSEE)が作成する名簿。

[30] 本文で紹介するものの他、公的部門による一定の取扱いについても、情報処理及び自由に関する国家委員会の意見を経て下される、コンセイユ・デタの議を経るデクレによる許可が必要な場合がある(27 条)。

の意見を経て下される。この意見は、許可と同時に公表される（26 条Ⅱ）（前述 2④エ））。

情報処理及び自由に関する国家委員会は、申請から 2 か月以内に意見を表明しなければならない。ただし、この期間は、委員長の理由を付した決定に基づき、1 度まで延長できる（28 条Ⅰ）。取扱いに対して委員会に求められた意見が、期間内に表明されなければ、許可に同意したものとみなされる（28 条Ⅱ）。

(オ)届出者・許可申請者は、以下の事項を明らかにして届出若しくは申請をしなければならない（30 条Ⅰ）。

〈1〉取扱責任者の身元と住所
〈2〉取扱目的
〈3〉場合によっては、相互接続や結合、又は他の取扱いと関係を有する場合のその態様
〈4〉取扱対象となる個人情報、当該情報の収集元、取扱いに関係する個人の範疇
〈5〉取り扱われる情報の保存期間
〈6〉取扱担当者・組織
〈7〉情報の開示を受け得る情報取得者又は取得者の範疇
〈8〉アクセス権行使の担当部局又は権利行使手段
〈9〉取扱いの安全性や、法律によって保護される秘密保持、下請を利用する場合において取扱受任者への指示等を確実なものにするための定め
〈10〉場合によっては、EU 域外諸国への個人情報の転送

届出及び簡易届出は、Web 上からすることができる[31]。

[制度の運用について]

・調査権の行使について、情報処理及び自由に関する国家委員会からのヒアリングによると、事前通告なしの立入調査の頻度は高くないが、調査を受け入れない場合は、警察に支援を頼み、調査を強制的に実施することができるとのことである。
・法律違反が疑われる事案につき、情報処理及び自由に関する国家委員会が調査を実施した場合、企業は情報処理及び自由に関する国家委員会の求めたすべての情報の提出が義務付けられているとのことである。
・情報処理及び自由に関する国家委員会は非公式に警告を発することがある。企業から意見を聞くこともあるということである。
・情報処理及び自由に関する国家委員会は、事前規制によって個人情報の取扱いを管理することが重要な目的であると認識しており、例えば個人情報を利用する商品を作る場合は、情報処理及び自由に関する国家委員会が商品やその製造過程を認証し、シー

31 http://www.cnil.fr/index.php?id=6

ルを発行することを検討しているとのことである。
・また、情報処理及び自由に関する国家委員会は苦情処理も行っているが、同組織の関与により、95%の苦情が解決しているとのことである。
・このほか、情報処理及び自由に関する国家委員会には国際交渉の実施や、新技術のフォローといった役割も担っており、特に新技術については、RFID やナノテクノロジーなどの動向をレポートにまとめているとのことである。
・監督者設置について、情報処理及び自由に関する国家委員会は厳しく指導しており、現在は約 600 名の監督者が設置されているということである（情報処理及び自由に関する国家委員会調べ)。
・また、取扱いに関する許可を情報処理及び自由に関する国家委員会が決定することになっているが、許可の要件に関する詳細な規定がない一方、許可を取るのが非常に難しいため、問題になっているということもあるようである。
・一方で、情報処理及び自由に関する国家委員会の調査はもっと行われても良いはずだが、実際には調査し切れていないのが実情であり、課題になっているとの話も聞かれた。情報処理及び自由に関する国家委員会は年ごとに特定の業界を特に対象として、監査などを実施しているようである。

⑬死者に関する個人情報の保護

[現状について]
・情報処理及び自由に関する国家委員会へのヒアリングによると、フランスでは死者情報に関して今まであまり問題が発生していないとのことであり、死者については、死因についてのみ議論がある。死因については相続人以外は知ることはできないとのことである。
・ダイレクトマーケティング協会へのヒアリングによると、消費者から、死亡した親族や、痴呆が進んだ高齢者に対してダイレクトメールが送付されないようにするため、情報を更新して欲しいという要望が多く寄せられているようである。

[制度について]
法制度上、以下のような規制がある。
ア)死亡原因を証明するために作成された情報を含め、死者に関する情報は、当該個人が、生前に書面で拒否した場合を除き、情報取扱いの対象となり得る（56 条)。
イ)訂正請求の一環として、死者の相続人は、死者に関する情報の更新をするよう情報取扱責任者に請求することができる。この請求があった場合、情報取扱責任者は、必要な措置をとったことを無料で請求者に証明しなければならない（40 条)。

[制度の運用について]
情報処理及び自由に関する国家委員会へのヒアリングによると、基本的人権は生きて

いる人間だけに適用されるため、死者の情報は保護の対象外であるとの指摘があった。

⑭直接処罰等の実効性担保の措置

[制度について]

ア）刑事罰

（ア）情報処理及び自由に関する国家委員会の職務遂行を妨害する行為、同委員会が発した文書提出命令を拒否する行為、同命令に対し虚偽情報を提出した行為は、1 年の拘禁及び 15,000 ユーロの罰金（51 条）

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

（ウ）情報処理及び自由に関する国家委員会による取扱中断命令（後述イ)参照）に違反した者は、5 年以下の拘禁及び 30 万ユーロ以下の罰金（刑法典 L226－16 条 2 項）

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

（オ）個人識別全国名簿に登録されている個人登録番号を含んだ情報を許可なく取り扱う行為は、5 年の拘禁及び 30 万ユーロの罰金（刑法典 L226-16-1）

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

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

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

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

（コ）センシティブ情報を明示的な本人同意がないまました取扱いについては、5 年の拘禁及び 30 万ユーロの罰金（刑法典 L226-19)

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

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

（ス）届け出られた目的以外の利用は、5 年の拘禁及び 30 万ユーロの罰金（刑法典 L226-21）

（セ）個人情報の漏洩が、本人の尊厳や私生活における静穏を侵害した場合は、5 年の拘禁及び 30 万ユーロの罰金（刑法典 L-226-22 第 1 項。ただし、当該行為が、軽率さや怠慢のように、故意によらない場合は、3 年の拘禁及び 10 万ユーロの罰金（刑法典 L-226-22 第 2 項）。以上についての訴追は、被害者による告訴が必要とされる（刑

法典 L226-22 第 3 項）

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

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

イ）情報処理及び自由に関する国家委員会による制裁

本法に定める義務違反があった場合、情報処理及び自由に関する国家委員会は、取扱責任者に対し、警告を発することができる。

必要があれば、委員会の定める期間内に違法な取扱いを中止するよう指示することができ、この指示に従わない者には、過料(sanction pécuniaire)を科すことができる。

過料額は、15 万ユーロ又は 30 万ユーロ以下、又は、30 万ユーロを上限とした総売上額の最大 5%である。この場合、届出(前述（２）⑫ウ)(ア)参照）の対象となる取扱いであれば取扱停止命令(injonction de cesser le traitement)を、許可された取扱いであれば（前述（２）⑫ウ)(ウ)参照）許可取消しの処分をすることもできる（45 条)。

これらの決定に不服のある者は、コンセイユ・デタに訴訟を提起できる（46 条)。なお、緊急の場合は、取扱実施の中断(interruption)を命ずることもできる（45 条Ⅱ)。

[運用について]

・フランス銀行連盟へのヒアリングによると、情報処理及び自由に関する国家委員会による制裁について（上記イ）参照)、2006 年 6 月 28 日、クレディリヨネ（Credit Lyonnais）が情報処理及び自由に関する国家委員会の調査に非協力的だったとして（前述（２）⑫ア)参照)、約 4.5 万ユーロの罰金を課されたことがあったとのことである[32]。15～30 万ユーロ若しくは売上の最大 5%が過料額の上限であるため、比較的緩やかな制裁と考えていると言うことであった。

・このケースについては、フランスでは銀行は顧客の債務情報をフランス銀行（Banque de France）に提供するとともに、照会することができるようになっているところ、クレディリヨネは 2002 年 2 月に登録した債務情報につき、更新データを 2004 年 9 月 16 日に登録したが、同年 12 月にフランス銀行担当者がこのデータに不正確な情報が含まれていることを発見したことで、発覚したということである。実際、顧客の中には、債務を返済したにもかかわらず、借入れができなくなった者もいた。

・このような事態について、2004 年 12 月 15 日、情報処理及び自由に関する国家委員会は、クレディリヨネに質問を送付したところ十分な回答がなく、さらに 2005 年 3 月 24 日に再度質問状を送付したところ一切回答がなかったため、これが過料の対象とされたということである。

・銀行連盟としては過失によるものと考えており、過去の顧客情報の保有を制限するよ

[32] http://www.cnil.fr/index.php?id=2104&news[uid]=381&cHash=20ea8ddf3c

う、加盟銀行に通達を出した経緯がある。
・マスコミがこの問題を大きく取り上げたため、情報処理及び自由に関する国家委員会の制裁権限が周知されたという効果もあったと認識されているようである。
・なお、情報処理及び自由に関する国家委員会へのヒアリングにおいては、2005 年からの 18 ヶ月間で 116 件の注意、94 件の勧告、7 件の制裁が行われており、制裁が行われた 7 件のうち、6 件については実際に制裁が課されたということが確認できた。2 件はデータ取扱いの差止めであり、4 件は事案の公開で対処されていると言うことである。残りの 1 件はヒアリング時にはまた対応が実施されていないということであった。

⑮その他、特に留意すべき重要措置

・情報処理及び自由に関する国家委員会へのヒアリングによると、今のところ、法改正の必要性は感じていないとのことであった。しかし、今後、新技術に対応して法律を見直すことはあり得るという見解が示された。また、条文中に参照箇所が多くなり、複雑になってしまっているので、簡略化の必要性はあるかもしれないという指摘もあった。
・なお、情報処理及び自由に関する国家委員会の組織人員体制については、法律上、権限は充実しているが、職員が 85 人であり、人員不足であると感じているという指摘があった。ドイツやイギリスの第三者機関は人員も充実しているとのことである。適切に法律を運用する上では、2 倍（160 人規模）の人員は必要だと感じているということである。助言を求める人が多いが、対応しきれていないのが問題点として指摘された。

・ダイレクトマーケティング協会へのヒアリングによると、大企業ではオプトインとオプトアウトの使い分けや違いに対する認識は高まってきているが、多くの企業には未だ浸透してないということである。ダイレクトマーケティング協会では、情報処理及び自由に関する国家委員会に相談しながら、特に小規模事業者に向けて、オプトインを使用する際のガイドラインを作成したとのことであった。
・オプトインとオプトアウトの両方を記載したり、承諾・不承諾のいずれの場合もチェックをするようにしているため、混乱が生じていることを問題視しているとのことである。例えば、オンライン確定申告の際に、テレビを「保有していない」場合にチェックをすることとなっていたにもかかわらず、多くの人が「保有している」場合だと誤解し、30%程度が誤った申告を行った事例があったとのことである。
・ダイレクトマーケティング目的で名前と住所だけの個人情報を取り扱う場合につき、義務を緩和するよう情報処理及び自由に関する国家委員会に要望したところ、通達で受け入れられたということがあったとのことである。

３．ドイツ[33]

（１）個人情報保護制度の概要

①法律名

・ 連邦データ保護法（Bundesdatenschutzgesetz）

②目的

・ 個人データの取扱いによる人格権侵害から個人を保護すること（1 条 1 項）

③適用範囲

・ 公的機関（連邦の公的機関及び連邦法を執行する州の公的機関）：個人データ
・ 非公的機関：自動処理される個人データ、又はデータファイル（同質的に構成され、一定の基準に従ってアクセスすることができ、分析し得る個人データの集積）内の個人データ

※第 1 章に両部門に共通の規定、第 2 章に公的機関、第 3 章に非公的機関に関する規定が置かれている。EU データ保護指令が両部門を区別していないことの影響で、2001 年の改正法では、両部門に共通の規定が増えている。

④規制・権利の内容

・ 収集：個人データは、原則として、本人から収集しなければならない（4 条 2 項）。
・ 通知：個人データが本人から収集される場合、責任機関から、①責任機関の名称、②収集、取扱い、利用の目的、③第三者提供の範囲、について通知されなければならない（4 条 3 項）。
・ 利用目的による制限（14 条、28 条）
・ 第三者提供の制限（15 条、29 条）
・ 安全管理措置：データ保護担当者（4f 条）、秘密保持（5 条）、技術的・組織的措置（9 条）、委託による収集、取扱い又は利用（11 条）
・ 本人への開示（19 条、34 条）
・ 訂正・消去・利用停止（20 条、35 条）

⑤監督・登録制度

・ 監督：公的機関は連邦データ保護監察官――連邦議会の選挙によって選出。任期 5 年（22 条）。非公的機関は各州の監督官庁（38 条）。

---

33 当節で引用している法文の日本語訳は、藤原静雄「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, No. 99, 2002 年 9 月）に掲載されている日本語訳を参考にしている。

・ 登録制度：個人データのコンピュータ処理については、その開始前に、非公的機関は監督機関に、連邦機関はデータ保護監察官に、届け出なければならない（4d 条）。ただし、①データ保護担当者を任命している場合、②データの収集、取扱い又は利用に従事する者が 9 人以下で一定の要件を満たす場合には、届出義務が免除される。

⑥主な適用除外

・ 州は立法において、もっぱら自己の報道・編集上の又は文学的な目的のための個人データの収集、取扱い及び利用については、5 条（秘密保持）、9 条（技術的・組織的措置）及び 38a 条（自主規制）に相当する規律、ならびにこれに関する 7 条（損害賠償）の責任規律が適用されることを定めなければならない（41 条 1 項）。＝それ以外の規制は適用されない。
・ 連邦法上の放送局の報道によって、自己の人格権を侵害される場合は、蓄積されたデータの開示を請求できる。ただし、取材源の秘匿に関わる場合は、開示を拒否できる（41 条 3 項）。連邦法上の放送局には、連邦データ保護監察官に代わるデータ保護監督者が置かれる（42 条）。

⑦主な自主規制

・ データ保護監査（9a 条）
・ 責任機関の一定のグループを代表する職業団体及びその他の団体は、「データ保護法上の規制の実施を促進するための行為基準」の案を所轄の監督官庁に提示して説明することができる（38a 条 1 項）。監督官庁は、提出された案と適用法との適合性を審査する（同条 2 項）。――ただし、この規定は実際にはほとんど運用されていないようである。

（2）「個人情報保護に関する主な検討課題」関連項目に即した状況

① いわゆる「過剰反応」（誤解）に対応した第三者提供制限の例外事由[34]

[現状について]

・ 前連邦データ保護監察官事務所職員へのヒアリングによると、1977 年にドイツではじめて連邦データ保護法が施行されたときには、日本のような混乱はドイツにもあった。国勢調査判決が連邦憲法裁判所によって出され、個人情報保護法が国民の注目を浴びた際にも同様の議論があった[35]。以下に具体例を示す。

---

[34] 藤原静雄「ドイツにおける個人情報保護法の実際－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』118 頁以下による。

[35] 1983 年 12 月に、国勢調査の項目が余りにも詳細であるということで、連邦憲法裁判所によって違憲判決が出された。この判決は「情報の自己決定権」（自己情報コントロール権と同等のもの）を認め、従来の立法・行政実務における個人情報の取扱いのあり方の再検討を迫った。

- 最初に議論になったのが、誕生日リスト問題である。ドイツでは、公的部門でも民間部門でも、部門の長が部下の誕生日を把握しておいて、電話をかけて祝ったりするのが慣例であり、電話等をもらった方も喜ぶ。連邦データ保護法が施行されたときに、これが許されないのではないか、すなわち、本人の同意なく収集することの是非が問題となった。そのため、旧法のデータファイル概念の適用を受けないように手書きのリストを作成する等の工夫がされたが、無駄なことではないかという議論があった。現在、多くの組織では、月と日のみを本人の同意の下に収集している（生年を知られることには抵抗がある人が多いため）。
- 幼稚園や学校の名簿が作れないという議論もあった。一定数の児童・生徒の親が同意を与えなかったからである。この問題は、教育が州の事務であるので、部分的には州の教育関係法規の改正で対処されることとなった。
- 私的な団体（スポーツ倶楽部、音楽同好会等）の会員情報の第三者への提供（チケットの案内等のため）についても議論が起きたが、団体の規約に提供等の条件をきちんと書くことで対処した。
- 法施行後まもなく、外務省、又は国防軍のアメリカ担当部署では、パーティなどの招待客のリストが問題となった。食の好みや席順（誰と誰とを一緒にしない等）といった個人情報を保有することの是非が問題とされたからである。これも、法の適用を逃れるべく単なる手書きのリストにする等の議論がされたことがある。
- 国勢調査判決の直後に、民間でも公的部門でも、執務室の入口に公務員又は従業員の名前を掲示することの是非が議論されたことがある。労働法と個人情報保護の関係は、今も難しい問題の一つである。
- 同意の解釈についても制定時議論があった。国防軍などで社会学者の調査に協力するに際して、兵士の同意がないのではないかということが議論された。軍は、一室に兵隊を集めて同意しない者は退出するという方式をとろうとしたが、これも上官の前では任意性がないとの指摘が出た。これは国防軍側が押し切った。
- 連邦議会の議員でボンと自分の郷里（選挙区）との間を、誰が国防軍の飛行機を使って飛んでいるかという質問に対して、拒否理由に個人情報保護が利用されたことがあり、プレスとの間で議論となった。
- 国勢調査判決以降、社会保障の分野で目的拘束が非常に厳しくなった。そのため、不法に社会給付を受けている人間の把握を警察がすることが難しくなっている。これも批判の的となっている。
- 制定後まもなく、国防軍の中で、兵士の射撃成績を掲示することについて、成績は評価情報であり保護されるべき個人情報であるから、本人の同意が要るのではないかが問題とされた。この問題をめぐって、個人情報保護の行き過ぎが議論された。

[制度について]

(1) 自己の業務目的の遂行のための手段として、個人データを収集、蓄積、変更若しくは提供し、又はそれを利用することは、以下のいずれかの場合に許される（28 条 1 項）。

1　それが本人との契約関係若しくは契約類似の信頼関係の目的に資する場合

2　責任機関の正当な利益を守るために必要で、かつ、取扱い若しくは利用をさせないことについての本人の保護に値する利益が存在しない場合

3　データが一般にアクセス可能であるか、又は、責任機関がそれを公表することが許されている場合。ただし、責任機関の正当な利益と比較して、取扱い若しくは利用をさせないことについての本人の保護に値する利益が明らかに優越する場合は、この限りでない

個人データの収集の際、データが取り扱われ、利用される目的が具体的に確定されなければならない。

(2) 他の〔＝データ収集の際に特定された目的以外の〕目的のためには、個人データは、(1)2 及び 3 の要件のもとでのみ提供され、又は利用されることが許される（28 条 2 項）。

(3) 他の〔＝データ収集の際に特定された目的以外の〕目的のための提供又は利用は、次のいずれかの場合にも許される（28 条 3 項）。

1　第三者の正当な利益を守るために必要な場合

2　国家及び公共の安全にとっての危険の防止並びに犯罪行為の追及のために必要な場合

3　宣伝、市場調査又は世論調査の目的のため、人的集団の構成員に関して、限定された項目（①当該人的集団への本人の所属に関する記載、②職業、部署又は業務の名称、③氏名、④称号、⑤学位、⑥住所及び⑦生年）につき名簿の形で又はその他の方法でまとめられたデータが取り扱われる場合で、かつ、本人が提供又は利用させないことについての保護に値する利益を有すると推定する理由がない場合

4　研究施設の利益のために、学術研究の実施について必要な場合。ただし、研究計画の実施についての学術上の利益が、目的変更をさせないことによる本人の利益に著しく優越し、かつ、他の方法では研究目的が達成できないか又は過度の出費を要するときに限る。

(4) 上記(3)3 の目的のための個人データの利用又は提供は、本人が責任機関に異議を申し立てた場合には、許されない。本人は、すでに第三者にデータが提供されている場合、この第三者に異議を申し立てれば、第三者はそのデータを利用停止（封鎖）しなければならない（28 条 4 項）。

② 自治会や同窓会等の取扱い

[制度について]

・　同窓会については、次項に掲げるように、大学（ドイツの大学は基本的に国立である）

の同窓会の存在を確認できた。連邦及び州の個人情報保護制度上、同窓会が特に適用除外とされていないことから、規制の対象となる。

・ なお、ドイツでは、個人情報の個人的・家庭的な利用は法律の規制の対象外とされている。

[制度の運用について]

ベルリン州データ保護監察官へのヒアリングによると、同窓会のような非営利の団体における個人情報の取扱いと、事業者における個人情報の取扱いとの間には、区別がなく、同じように監督され、罰則を科せられるとのことである。

ベルリン・フンボルト大学データ保護担当者へのヒアリングによると、ドイツにも「同窓会」は存在し、大学とは別の組織としてベルリン州データ保護法の対象となっている。同窓会名簿（大学が管理する同窓会データベースへの登録を承諾した卒業生についての名簿データ）は、次のとおり取り扱われている。

・ 同窓会名簿は大学の学生簿とは別のデータベースとして管理されており、名簿への登録は任意である。寄付金の募集、雇用の促進等の利用目的の他、住所ブローカーに渡さない、データは厳重に管理するといった諸条件を事前に説明し、同意した場合のみ登録してもらう仕組みになっている。
・ 利用については厳しい制約があり、外部からデータベースに直接アクセスすることはできない。大学からもベルリン州データ保護監察官からも独立した立場にあるデータ保護担当者が仲介となり、外部からのアクセスに対する本人の同意を確認する。なお、アクセス許可申請件数は次のとおりである。
  - 民間団体からの申請： 550～650 件／年
  - 研究関連の申請： 150～200 件／年
  - 上記外にも警察からの申請が時々ある。
・ このデータベースは 6 年前（2001 年）に構築された。当初はデータの取扱いに関する不安から、卒業生の 60%がデータベースへの掲載を拒否したが、徐々にデータベースのメリットと厳格な管理のルールについて理解が広がり、現在の拒否率は 25%である。卒業生にとってのデータベースに登録することのメリットとしては、大学関係のイベントの通知やビジネスパートナーの紹介を受けられること等がある。
・ 名簿の掲載項目は次のとおりである。
  ：氏名、旧姓、生年月日、現住所、出身地住所、就職先の連絡先、学位の種別、卒業年、国籍、大学からの案内を送付して良いか（掲載する項目の限定可）

③ 「個人情報」の定義

[制度について]

・ 個人データ（personenbezogene Daten）とは、特定の又は特定され得る自然人（本人）

の人的又は物的状況に関する個々の言明（Einzelangabaen）をいう（3 条 1 項）。

④ センシティブ情報に関する規定

[制度について]

(1)「特別な種類の個人データ」とは、人種的及び民族的出自、政治的意見、宗教的又は哲学的な信条、労働組合への加入、健康又は性生活に関する事項をいう（3 条 9 項）。

(2)「特別な種類の個人データ」が収集され、取り扱われ、又は利用される限り、同意は、さらに明示的に、当該データと関連付けられなければならない（4a 条 3 項）。

(3) 自己の業務目的のための、「特別な種類の個人データ」の収集、取扱い及び利用は、本人が上記(2)により同意しないときは、以下のいずれかに該当する場合に、許される（28 条 6 項）。

1 本人又は第三者の死活にかかわる利益の擁護のために必要であり、そして当事者が、肉体的又は法的な理由から、同意を与えることができる状態にない場合

2 本人が公にしたことが明白であるデータが問題になっている場合

3 法律的な請求権の主張、行使又は防御のために必要であり、収集、取扱い又は利用を排除することについての本人の保護に値する利益が優越することを推定させる根拠が存しない場合

4 学術研究の遂行のために必要であり、研究計画の遂行における学術的な利益が、収集、取扱い又は利用を排除することについての本人の利益より著しく優越し、かつ、研究目的が他の方法で達成できないか又はその達成に均衡を欠く過度の出費を要する場合

(4)「特別な種類の個人データ」の収集は、さらに、これが、健康への配慮、医学上の診断、健康管理又は公衆衛生業務上の取扱い若しくは公衆衛生業務のために必要であり、かつ、これらのデータの取扱いが、医師又はその他これと同等の守秘義務に服する者によって行われる場合に、許される。上記の目的のためのデータの取扱い及び利用は、上記の医師等に適用される守秘義務規定に従う（28 条 7 項）。

(5)「特別な種類の個人データ」は、上記(3)及び(4)以外の目的のためには、上記(3)の 1 から 4 まで又は上記(4)の要件のもとでのみ、提供又は利用することが許される。提供又は利用は、これが、国家及び公共の安全にとっての危険の防止並びに著しく重大な犯罪行為の追及のために必要な場合にも許される（28 条 8 項）。

(6) 政治的、哲学的、宗教的又は労働組合的な傾向を有し、収益目的を追求しない組織は、それが組織活動にとって必要である限り、「特別な種類の個人データ」の収集、取扱い又は利用を許される。このことは、その構成員又はその組織の活動目的との関連で、その組織と定期的に接触する者の個人データにのみ適用される。この個人データの組織外の者又は機関への提供は、上記(2)の要件のもとでのみ許される（28 条 9 項）。

(7) 匿名化された形で提供するために、個人データが業務上収集及び蓄積される場合にも、

上記(3)から(6)までが準用される（30 条 5 項）。

(8) 「特別な種類の個人データ」又は犯罪行為若しくは秩序違反に関するデータが問題となっており、かつ、その正確性を責任機関が証明できない場合は、個人データは消去されなければならない（35 条 2 項 2 号）。

[制度の運用について]

ベルリン州データ保護監察官へのヒアリングによると、センシティブ情報は、次のとおり取り扱われている。

- 各個人情報がセンシティブ情報に当たるか否かは、利用目的など情報が扱われる状況によって左右されるものなので、一概には言えない（例えば、ドイツでは、名前によって国籍や出身地が判別できるので、単なる氏名であっても、状況によってはセンシティブな情報になり得る）。国勢調査判決を含む連邦憲法裁判所の判決においても、個々の個人情報がセンシティブ情報に当たるか否かは利用方法などによるとされている。
- センシティブ情報の取扱いが許される法的根拠としては、明示的な同意が必要とされており、（一般的な）契約だけでは不十分である。センシティブ情報の取扱いは当事者の承諾がある場合だけ処理を認める 28 条 6 項～9 項があり、これらが優先する（契約に 4a 条 3 項のような明確な条項があればよいが、その条項を盛り込むことが難しい）。
- データ保護監察官には、センシティブ情報に関する解釈・指針を拘束力のあるガイドラインの形で示す権限はないが、民間に対して考え方（解釈の提案）を示すことはあり得る。議会承認を受けている年次報告書に掲載することで、普及に努めている。

⑤ 小規模事業者の取扱い

[現状について]

ドイツ商工会議所本部（DIHK）へのヒアリングによると、個人情報保護に関する小規模事業者の取組の現状は、次のとおりである。

- 厳格な意味で、連邦データ保護法に規定されたとおりにデータ保護担当者を設置している小規模事業者は少ない。理由としては、小規模事業者には、予算的にも人員的にも、専門家を設置する余裕がないことが考えられる。
- 小規模事業者に対するデータ保護担当者設置義務の基準緩和（次項[制度について]を参照）は、DIHK から働きかけを行った要請の一つである。

[制度について]

- 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――※注：2006 年の改正により、4 人から 9

人に緩和されたものである)。さらに、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)。

・ データ保護担当者を設置できない（設置する余裕のない）事業者は、事業主が担当者となることが、2006 年 8 月の法改正によって、認められている。

[制度の運用について]

ベルリン州データ保護監察官へのヒアリングによると、小規模事業者に関する個人情報保護制度の運用は、次のとおり行われている。

・ 法改正により、データ保護担当者を設置する事業者の規模の基準を 4 人から 9 人に緩和した背景には、小規模事業者において同規定の遵守が実質上難しかったということがあった。
・ 法遵守が不十分である原因の１つとして、各事業者の法に関する知識不足が考えられるため、担当者を置いていない事業者を発見した場合、まずは当局から設置するよう指示を出し、従わない場合に勧告を行うなど、段階的に対応している。
・ 当局からの支援、アドバイスの他、GDD、TÜF といった民間団体が小規模事業者におけるデータ保護の取組に対する支援を行っており、重要な役割を担っている。

⑥ 個人情報の目的外利用の防止措置

[現状について]

・ ドイツ商工会議所本部（DIHK）へのヒアリングによると、連邦データ保護法に抵触する非合法的な名簿事業者は多数存在し、多くの事業者がこの名簿を使用している実態はある。
・ ベルリン州データ保護監察官へのヒアリングによると、個人情報の目的外利用がどのくらい行われているかについて、統計はないが、大きな問題であり、苦情は非常に多い。消費者はオプトイン方式を望むことが多い一方で、事業者はオプトアウト方式を好んで用いているとのことである。また、事業者は、事前に受け取り拒否を示している人に対しても、ダイレクトメールを送付することが、しばしばあるようである。

[制度について]

(1) 自己の業務目的の遂行のための手段として、個人データを収集、蓄積、変更若しくは提供し、又はそれを利用することは、以下のいずれかの場合に許される（28 条 1 項)。
　1　それが本人との契約関係若しくは契約類似の信頼関係の目的に資する場合
　2　責任機関の正当な利益を守るために必要で、かつ、取扱い若しくは利用をさせないことについての本人の保護に値する利益が存在しない場合

3　データが一般にアクセス可能であるか、又は、責任機関がそれを公表することが許されている場合。ただし、責任機関の正当な利益と比較して、取扱い若しくは利用をさせないことについての本人の保護に値する利益が明らかに優越する場合は、この限りでない

個人データの収集の際、データが取り扱われ、利用される目的が具体的に確定されなければならない。

(2) 他の〔＝データ収集の際に確定された目的以外の〕目的のためには、個人データは、(1)2及び3の要件のもとでのみ提供され、又は利用されることが許される（28条2項）。

(3) 他の〔＝データ収集の際に確定された目的以外の〕目的のための提供又は利用は、次のいずれかの場合にも許される（28条3項）。

1　第三者の正当な利益を守るために必要な場合

2　国家及び公共の安全にとっての危険の防止並びに犯罪行為の追及のために必要な場合

3　宣伝、市場調査又は世論調査の目的のため、人的集団の構成員に関して、限定された項目 a)当該人的集団への本人の所属に関する記載、b)職業、部署又は業務の名称、c)氏名、d)称号、e)学位、f)住所及び g)生年につき名簿の形で又はその他の方法でまとめられたデータが取り扱われる場合で、かつ、本人が提供又は利用させないことについての保護に値する利益を有すると推定する理由がない場合

4　研究施設の利益のために、学術研究の実施について必要な場合。ただし、研究計画の実施についての学術上の利益が、目的変更をさせないことによる本人の利益に著しく優越し、かつ、他の方法では研究目的が達成できないか又は過度の出費を要するときに限る。

(4) 上記(3)3の目的のための個人データの利用又は提供は、本人が責任機関に異議を申し立てた場合には、許されない。本人は、すでに第三者にデータが提供されている場合、この第三者に異議を申し立てれば、第三者はそのデータを利用停止（封鎖）しなければならない（28条4項）。

(5) データが提供された第三者は、これを、それが提供された目的を遂行するために取扱い、又は利用することが許される。他の目的のための取扱い又は利用は、上記(2)及び(3)の要件のもとでのみ許される（28条5項）。

[制度の運用について]

・ ベルリン州データ保護監察官へのヒアリングによると、明らかに違法な目的外利用が行われている場合には、まず書面での指導を行い、最終的に過料や技術的な利用停止を課す場合もある。

⑦ 市販の名簿の管理

[現状について]

ベルリン州データ保護監察官によると、原則として、市販の名簿は、他の個人情報と同様の安全管理措置をとることとされているとのことである。

ベルリン・フンボルト大学データ保護担当者へのヒアリングによると、市販されている教員名簿は、次のとおり取り扱われている。

- 教員名簿には印刷物として広く市販されるものと、インターネット／イントラネットで提供されるものとの2種類があり、印刷物は学期ごとにおよそ1万部が印刷されている。
- 印刷物の教員名簿は市販されているものではあるが、学内においては他の個人情報と同様に取り扱っている。
- 教員名簿には、学長、副学長、幹部、教授に関する情報が掲載されており、大学が教授とその研究テーマによって成り立っているという考え方により、教授等は掲載を拒むことはできない。また、掲載項目は、氏名、肩書き、研究テーマ、執務室の電話番号、FAX番号、電子メール、住所、各人のホームページのリンク（オプション）である。

[制度について]

(1) データが一般にアクセス可能である場合には、自己の業務目的の遂行のために、個人データを収集、蓄積、変更若しくは提供し、又はそれを利用することができる。ただし、責任機関の正当な利益と比較して、取扱い若しくは利用をさせないことについての本人の保護に値する利益が明らかに優越する場合は、この限りでない。個人データの収集の際、データが取り扱われ、利用される目的が具体的に確定されなければならない（28条1項3号）。

(2) データが一般にアクセス可能である場合には、自己の業務目的の遂行のために、個人データの目的外〔＝データ収集の際に確定された目的以外の〕提供・利用が許される。ただし、責任機関の正当な利益と比較して、取扱い若しくは利用をさせないことについての本人の保護に値する利益が明らかに優越する場合は、この限りでない（28条2項）。

(3) データが一般にアクセス可能である場合には、提供を目的とする、個人データの業務上の収集、蓄積若しくは変更は、とりわけこれが信用調査機関、名簿取引、又は市場調査及び世論調査に役立つ場合は、許される。ただし、蓄積又は変更を排除することについての本人の保護に値する利益が明らかに優越する場合は、この限りでない（29条1項2号）。

⑧ 個人情報の取得元の開示に関する措置

[現状について]

ベルリン州データ保護監察官へのヒアリングによると、個人情報の取得元の開示に関する苦情は多くよせられているとのことである。

[制度について]

(1) 本人は、以下のものについて、開示を求めることができる。

1　自己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

2　データが譲渡される受領者又は受領者の範疇

3　蓄積の目的

本人は、開示されるべき個人データの種類を詳細に示さなければならない。個人データが業務上、提供目的で蓄積される場合は、企業秘密を守ることの利益が優越しないときに限り、本人は情報源及び受領者に関する情報の開示を求めることができる。この場合、情報源及び受領者に関する情報の開示は、当該記載事項が蓄積されていない場合でも、なされるものとする（34 条 1 項）。

(2) 本人は、個人データを、業務上、開示する目的で蓄積している機関に対しては、データが自動処理されておらず、又は自動化されていないデータファイルに蓄積されていない場合でも、個人データに関する情報の開示を求めることができる。企業秘密を守ることの利益が優越しない限り、本人は、情報源及び受領者に関する情報の開示を求めることができる（34 条 2 項）。

[制度の運用について][36]

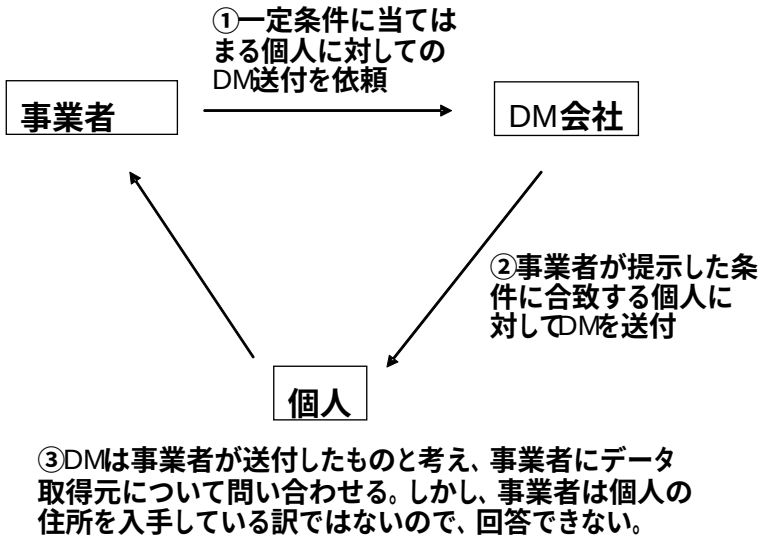
・ 信用調査機関（Auskunftei）について、個人情報の取得元及び受領者に関する情報の開示が行われない、又は不十分であるとして、苦情を訴える請求者が多いが、監督官庁の求めに応じて、速やかに是正されることがしばしばである。ただし、いくつかのケースでは、信用調査機関が、企業秘密を守ることの利益が優越すると主張して、開示を拒絶している。信用調査機関の顧客が、本人に知られないことを最重要視するケースや、本人が信用調査機関に対して、開示を求める理由を十分に示さないケースなどである。個別のケースにおける監督官庁と信用調査機関との交渉により、多くの場合、最終的には、自分に関する経済的情報を誰が入手したかについて、本人が知ることができた。それ以外の少数のケースにおいては、データ受領者に関する情報を信用調査機関が開示しないことが正当と認められたが、その場合、少なくとも、監督官庁の中立的な審査により、濫用的事例と認める根拠がないということは、本人に通知された。最近、信用調査機関の団体と最上級データ保護監督官庁との間で協定が結ばれ、今後は、本人がデータ受領者を知ることについて正当な利益を有することを主張できる場合、又は、データ受領者が、信用調査機関を使っていることが一般に知られている分野（通信販売業者、情報通信企業、銀行等）に属している場合には、具体的なデータ受領者が本人に通知される。それ以外の場合には、信用調査機関が個別に判断する。

[36] バイエルン非公的部門データ保護監督庁 2002 年/2003 年活動報告書 35～36 頁による

[事業者の対応について]

ドイツの大手民間事業者へのヒアリングによると、個人情報の取得元の開示について、以下のような対応がなされている。

- 例えば、企業グループ内で親会社から子会社への個人情報が提供されている状況で顧客から子会社の保有する個人情報について情報の取得元に関する問い合わせがあった際には、親会社と回答するなど、顧客からの開示請求には基本的に応じている。
- 広告を受け取った人から、個人情報の入手元について問い合わせが来ることがあるが、アドレスブローカー（DM 会社）から送付している場合は、送付を依頼した事業者が住所を把握しているわけではないので、回答できない（次図参照）。ただし、アドレスブローカーから発送しているかどうかは分かるので、問い合わせした個人に対して、その説明をする。なお、アドレスブローカーから個人データを購入してもよいことは、28 条 3 項 3 号に規定されている。
- ドイツの法律（UWG：不正競争禁止法）では、電話、ファックス、電子メールによる広告の送付は、本人の承諾がない限り、してはならないこととされている。書簡による消費者への広告のみが認められている



⑨ 個人情報の利用停止・消去に関する措置

[現状について]

- ベルリン州データ保護監察官へのヒアリングによると、個人情報の利用停止・消去に関する苦情は、目的外利用や取得元の開示に関するものよりは少ない。苦情が少ない理由としては、当事者がデータを保持されていること自体を知らない場合が多いことが考えられる。
- ベルリン・フンボルト大学データ保護担当者へのヒアリングによると、個人情報の利用

停止・消去の請求は、15 年間で 2 件のみであった。

[制度について]

ベルリン州データ保護監察官によると、本人は、一定の条件のもと（特に事業者が広報活動を目的とする場合）で、自身の個人情報の利用停止・消去の請求の権利をもっている。法文の詳細は次のとおりである。

(1) 個人データは、下記(2)1 及び 2 の場合を除いては、いつでも消去することができる。個人データは、次のいずれかの場合には、消去されなければならない（35 条 2 項）。
   1 当該個人データの蓄積が許されない場合
   2 「特別な種類の個人データ」又は犯罪行為若しくは秩序違反に関するデータが問題となっており、かつ、その正確性を責任機関が証明できない場合
   3 個人データが自己目的のために取り扱われており、当該データを知ることが蓄積目的の実現のために必要でなくなったとき
   4 個人データが業務上の提供目的で取り扱われ、かつ、当該データの最初の蓄積を始期として 4 年が経過した時点での審査の結果、それ以上の継続的な蓄積が必要でないと判明した場合
(2) 次のいずれかの場合には、消去の代わりに利用停止（Sperrung：封鎖）が行われる（35 条 3 項）。
   1 上記(1)3 の場合に、法律、約款若しくは契約上の保管期限のため消去ができないとき
   2 消去によって保護に値する本人の利益が侵害されるおそれがあるという推定に理由があるとき
   3 特殊な方法の蓄積であるため消去が不可能又は不均衡に高額の費用を要するとき
(3) 個人データの正確性が本人によって争われ、かつ、正確であるとも不正確であるとも確定できない場合は、以後、利用停止がなされなければならない（35 条 4 項）。
(4) 本人が、責任機関に異議を申し立て、かつ、審査の結果、本人の保護に値する利益が、本人の特別な個人的事情のゆえに、責任機関の収集、取扱い又は利用に対する利益に優越することが判明した場合、個人データは、自動処理又は自動化されていないデータファイル内の取扱いのために、収集、取扱い又は利用をすることを許されない（35 条 5 項）。
(5) 提供目的で業務上データを蓄積する場合、不正確な個人データ又はその正確性が争われている個人データは、それが一般にアクセス可能な情報源から入手され、かつ、記録目的で蓄積されているときには、上記(1)の 2 の場合を除き、訂正、利用停止又は消去されない。蓄積期間中は、本人の要求に基づいて、当該データには、本人の反論を添付するものとする。この反論を添付せずにデータを提供することは許されない（35 条 6 項）。
(6) 不正確なデータの訂正、正確性が争われているデータの利用停止、及び蓄積が許されて

いないことを理由とした消去又は利用停止をした場合には、均衡を欠く過度の出費を要せず、かつ、本人の保護に値する利益と対立しない限り、蓄積のために当該データが送付されている機関に対して、通知がなされなければならない（35 条 7 項）。

(7) 利用停止されたデータは、以下の場合にのみ、本人の同意なしに、提供又は利用することが許される（35 条 8 項）。

1　学問上の目的のために、現存の立証困難を解消するため、又は、責任機関若しくは第三者の重大な利益のためになる理由から、不可欠であり、かつ

2　利用停止されていなかったとしたら、データがそのために提供され又は利用されることが許されるであろう場合

[制度の運用について]

・ ベルリン州データ保護監察官へのヒアリングによると、違反者に対して過料を科すことは、法律上は可能であるが、ほとんどのケースは当局からの指導によって解決する。

・ ベルリン・フンボルト大学データ保護担当者へのヒアリングによると、利用停止・消去の請求があった場合には、まず関連するデータについて暫定的に利用停止措置をとった上で、利用停止・消去の必要性と情報の利用の必要性について評価し、請求に応じるか否かを判断することとしている。

[事業者の対応について]

・ ドイツの大手民間事業者へのヒアリングによると、顧客からの個人情報の利用停止・消去の請求は寄せられている。請求があった場合でも、他の法律に基づきデータを一定期間保存しておくことが義務付けられている場合、その期間内は物理的にデータを消去することはできないため、例えば、顧客から物理的にデータを消去せよとの要求があった場合には、応じられない事情を説明するようにしている。

⑩ 国際的な情報移転に関する規定

[制度について]

(1) その全部又は一部が欧州共同体法の適用を受ける活動の枠内において、4b 条 1 項に掲げられている（他の EU 構成国内にある機関、他の欧州経済圏に関する条約締結国内にある機関、又は欧州共同体の組織及び施設）以外の機関に個人情報を提供することは、当該機関に適切なデータ保護水準が存在しないときであっても、以下のいずれかの場合に限り、許される。

1　本人が同意した場合

2　提供が、本人と責任機関との間の契約の履行のために必要であるか、又は本人の指示に合致した契約の予備的な措置の遂行に必要である場合

3　本人のために責任機関によって第三者と結ばれたか、結ばれるような契約の締結又

は履行のために提供が必要な場合

4　重要な公益の確保のため、又は、法廷における法的請求権の主張、行使又は擁護のために提供が必要な場合

5　提供が本人の死活に関わる利益の確保のために必要である場合

6　公衆に対する情報であり、かつ、個別事例において法律上の条件が満たされている場合に、何人でも又は正当な利益を証明できるすべての者が閲覧可能な登録簿から提供が行われる場合

データが提供される機関に、提供されたデータの目的外利用は許されないことを指示しなければならない（4c 条 1 項）。

(2) 上記(1)に関わらず、責任機関が人格権及びそれと結びついた諸権利の行使の保護に関して、十分な保証を示すならば、所管の監督官庁は、4b 条 1 項に掲げられた機関以外に個別の個人データの提供又は個人データの特定の態様の提供を許可することができる。この保証は、とりわけ契約条項又は拘束力ある企業ルールから明らかになる（4c 条 2 項）。

[法律以外の枠組みについて]

ドイツの大手民間事業者へのヒアリングによると、以下のような枠組みを用いた対応がなされている。

・ 拘束力のある企業ルール（Binding Corporate Rules）として、標準規約（Code of Conduct）を定めることで、国際的な情報移転を図ることとしている。ただし、標準規約については、作成後、監督官庁及び EU 委員会から承認を受けなくてはならず、手続が煩雑という問題がある。

・ EU 委員会は、標準契約条項（Standard contractual clauses for the transfer of personal data to third countries）を定めているが、これを遵守するのは難しい。このため、標準規約の作成を進めている。

・ セーフハーバー協定については、関係する外国企業が協定に加盟しているアメリカ企業のみであれば活用できるが、それ以外の企業とも関係している場合には使えない。

⑪ EU データ保護指令に対する対応状況

[現状について]

・ EU データ保護指令の国内法化のため、2001 年に連邦データ保護法が改正された。主な改正点は、次のとおり。

(1) 個人データの取扱いを収集段階から規制し（4 条）、同意原則を適用（4a 条）――EU データ保護指令 2 条 b、7 条 a に対応

(2) 公的部門・民間部門を通じて、届出義務（4d 条）は、データ保護担当者（4f 条）を任命した場合、原則として免除される（4d 条 2 項）――EU データ保護指令 18 条に

対応

(3) 個人に関する自動的判断の規制（6a 条）――EU データ保護指令 15 条に対応

(4)「特別な種類のデータ」（3 条 9 項、いわゆるセンシティブ情報）についての規制――EU データ保護指令 8 条に対応

(5) 公的機関についても、第三者からのデータ収集の場合の本人への通知を原則として義務づけた（19a 条）――EU データ保護指令 11 条に対応

(6) データ保護法上の規制の実施を促進するための行為基準について、規定が置かれた（38a 条）――EU データ保護指令 27 条に対応

⑫ 第三者機関の概要

[制度について]

ドイツでは、以下の監督体制をとっている（左は監督機関名、右は監督対象）。

④ 連邦データ保護監察官：連邦の公的機関及び民営化された一部事業者（鉄道、郵便、情報通信分野の事業者）

⑤ 州のデータ保護監察官：州の公的部門

⑥ 州のデータ保護監察官又は内務省の下の監督官庁：一般の民間事業者

非公的機関の監督官庁について、以下に述べる。

(1) 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）。

(2) 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）。

(3) 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）。

(4) 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）。⇒違反に対する過料（43 条 1 項 10 号）

(5) 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う権限を有する（38 条 4 項）。⇒違反に対する過料（43 条 1 項 10 号）

(6) 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（⇒違反に対する過料：43 条 1 項 11 号)。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)。

(7) 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)。

⑬ 死者に関する個人情報の保護

[制度について]

・ 連邦データ保護法には、死者の個人情報に関する規定はない。なお、ベルリン州データ保護監察官へのヒアリングによると、公的機関に対するベルリン州のデータ保護法には、死者の個人情報に関する規定がある（4 条 1 項)。

[制度の運用について]

ベルリン州データ保護監察官へのヒアリングによると、死者の個人情報について、以下のような運用がなされている。

・ 死者の個人情報について、民法上の人格権を根拠に遺族が保護を求めることができる。憲法裁判所においても、死者の人格権は死後も保護されるべきである旨の判決が出されている。
・ また、死者の情報が同時に遺族に関する情報である場合もある（例えば、死者の財産の情報は相続者の情報でもあり、データ保護の対象となる)。
・ カルテの第三者への開示について、開示先が遺族の場合には、民法上の解釈により開示できる。開示先が遺族以外の第三者の場合には、刑法上の医者の守秘義務との関係で、原則として開示できない。

⑭ 直接処罰等の実効性担保の措置

[制度について]

(1) 故意又は過失により、

1 権限なく、一般的にはアクセスできない個人データを、収集する者又は取り扱う者
2 権限なく、一般的にはアクセスできない個人データを、自動処理方法を用いていつでも呼び出せるようにする者
3 権限なく、一般的にはアクセスできない個人データを呼び出し、又は、自動処理により又は自動化されていないデータファイルから自ら入手し若しくは他者に入手させる者
4 一般的にはアクセスできない個人データの提供を、不正な申告により受ける者

5　第三者に譲渡することを通じて、提供されたデータを他の目的のために利用する者、又は

6　匿名化された個人データ（30 条）について、個々の記載事項とメルクマールとを不正に結合した者は、25 万ユーロ以下の過料を科される（43 条 2 項）。

(2) 上記(1)の行為を、対価を得て、又は、自己若しくは他人の利得を図ることを意図して、又は他人を害することを意図して、故意に行った場合には、2 年以下の自由刑又は罰金に処す。犯罪行為は告発に基づいてのみ訴追される。告発権限のある者は、本人、責任機関、連邦データ保護監察官又は監督官庁である（44 条）。

[制度の運用について]

ベルリン州データ保護監察官へのヒアリングによると、罰則等について、以下のような運用がなされている。

・　過料が科される事例は、ベルリン州の非公的機関については、およそ 10 件/年である。また、2006 年度に入ってから刑事告発を行った件数は、公的機関・非公的機関あわせて、20 件程度である（11 月時点）。自由刑については、把握している限りでは、これまでに科された事例はない（執行猶予の例はある）。

・　明らかな法律違反があった場合、まずは書面で改善指導を行い、従わなかった場合、技術的に利用の停止措置を執る（38 条 5 項）。

・　38 条 4 項で、一定の条件下における強制的な立入権限が認められており、データ処理設備の確認や資料閲覧を実施している。データ保護監察官のスタッフ全員が実施権限をもっており、比較的頻繁に行われている。なお、立入対象には個人の家は含まれない。

４．アメリカ

はじめに

・アメリカの個人情報保護法の制度は、オムニバス方式ではなく、必要に応じて、領域ごとに個別法を設ける「セクトラル方式」を採用しており、分野ごとに多数の法律が存在する。アメリカには全般的なプライバシー保護法はなく、部門ごとにプライバシーを保護する形をとっている。1974 年制定のプライバシー法(Privacy Act)は、連邦政府の保有する個人情報について適用されるものである。
・民間分野については、民間の自主規制を基本とした対応を行っている。法規制よりも自主規制・自己統制という伝統が強固であるとされる。
・一部の機密性が高い情報を扱う分野では法律による規制が行われている。個別法において、保護されるべき情報の範囲は分野ごとにその特性に応じて定められている。
・アメリカの個別法の制定は、「現実に問題が発生したことを受け、議会が規制にのりだすもの」として行われることも多い。必ずしも、情報保護の必要性の高さを一義的にあらわしているわけではない。
・アメリカにおける個人情報保護制度はセクトラル方式をとるため、制度（とりわけ民間分野の法制度）の実情を考察するためには、個別法の規定に遡って考察する必要が生じる。しかしながら本稿において個別法を網羅的にすべて取り扱うことは不可能である。以下においては、個別法における制度の概要について考察するため、信用情報分野（公正信用報告法（FCRA））、金融情報分野（金融サービス近代化法（GLBA））、並びに医療情報分野（医療保険の相互運用性及び説明責任に関する法律（HIPAA）及びその規則（HIPAA プライバシールール））の法制度を中心に紹介する。

（１）個人情報保護制度の概要

①法律名

・公正信用報告法（1970 年）（Fair Credit Reporting Act, FCRA)。信用情報。
・家庭教育の権利とプライバシーに関する法(1974 年)（ Family Educational Rights and Privacy Act, FERPA)。連邦の資金援助を受けている学校の教育情報。
・金融プライバシー権法(1978 年) (Right to Financial Privacy Act)。金融機関の保有する金融情報。
・プライバシー保護法（1980 年）(Privacy Protection Act)。報道機関の保有する情報。
・ケーブル通信政策法（1984 年）(Cable Privacy Protection Act)。有線テレビ事業者情報。

・電子通信プライバシー法（1986 年）（Electric Communicarions Privacy Act)。通信メディアの利用に関わる個人情報。
・電子消費者保護法（1986 年）（Electric Consumers Protection Act,ECPA)。
・ビデオ・プライバシー保護法（1988 年）（Video Privacy Protection Act,VPPA)。ビデオレンタル顧客情報等。
・金融記録プライバシー法（1988 年）（Financial Records Privacy Act)。
・ポリグラフ使用からの従業員保護法（1988 年）（Employee Polygraph Protection Act)。ウソ発見器の雇用情報としての利用規制。
・電話加入者保護法（1991 年）（Telephone Consumer Protection Act)。通話記録。
・運転免許プライバシー保護法（1994 年）（Drivers' Privacy Protection Act)。自動車登録記録。
・医療保険の相互運用性及び説明責任に関する法律（1996 年）（Health Insurance Portability and Accountability Act,HIPAA)。プライバシーに関して、2002 年 策定の、個人の健康情報に係るプライバシー規則（HIPAA プライバシールール,45 C.F.R. 164(SECURITY AND PRIVACY))。
・こどもオンラインプライバシー保護法（1998 年）（Children's Online Privacy Protection Act)。13 歳未満のこどもからのインターネット上での個人情報収集。
・金融サービス近代化法(1999 年)(Financial Modernization Act ,Gramm-Leach-Bliley Act, GLBA)。
・未承諾のポルノグラフィー及びマーケティング攻撃に対する規制法（2003 年）（Controlling the Assault of Non-Solicited Pornography and Marketing Act,CAN-SPAM-Act)。スパムメール規制。

②目的

・法律ごとに、法の目的、個人情報保護の目的が述べられている。
・FCRA によれば、法の目的は、個人消費者報告（信用報告、調査報告）の取扱いの規制（FCRA,602(b))。消費者報告機関が、消費者信用、人事、保険その他の情報に対する商業的需要を満たすために、情報の機密性、正確性、的確性と適切な利用に関し、消費者にとって公正かつ公平な方法で対応すべく、相当な手続を定めることを求めるものとされる。
・HIPAA プライバシールールは、医療保険関連情報、個人情報に関する安全保護措置とプライバシールールの確立のため、個人情報保護の基準、要請、解釈の細目を示すことをその内容としている。

③適用範囲

・法律ごとに、法の適用範囲（対象事業者、対象となる情報の範囲）が定められている。
・FCRA の対象事業者は、消費者報告機関（FCRA, 603(f))。第三者に対し消費者報告を提供

する目的で、消費者信用情報又はその他の消費者についての情報を収集又は評価することを通常業務の全部又は一部とする者で、消費者信用報告を提供する可能性のある者すべて。

・FCRA の対象となる情報は、「消費者報告」(FCRA,603(d))。「消費者報告」とは、消費者個人の信用度、信用に対する評価、信用枠、特性、社会的評判、身上事項、生活様式に関する消費者報告機関による情報の伝達であって、信用若しくは保険、雇用目的、又は 604 条で認められているその他の目的のために、消費者の適格性を判断するに当たり用いられ又は収集されるもの。このうち、「消費者調査報告」とは、消費者報告又はその一部分であって、消費者の性質、社会的評判、身上事項又は生活様式についての情報が、被報告者である消費者の隣人、友人、仲間、知人、又はこれらの事項の情報につき知っていると思われる者に対する個人的な面接によって得られるもの（FCRA,603(e)）をいう。

・HIPAA プライバシールールの対象となる事業者（covered entity）は、医療保険組合などの医療保険者（health plan）・医療保険支払い業務担当業者などの医療情報交換事業者（health clearing house）・病院や医師などの医療提供者（healthcare provider）で、電子的に医療情報を取り扱う者（45 C.F.R. 164.103)。

・HIPAA プライバシールールの対象となる情報は、個人の識別が可能な医療情報（Individually Identifiable Health Information）及び保護された保健情報（Protected Health Information)、をさす（45 C.F.R. 164.501)。これは、治療情報や医療機関で利用される情報を含む個人の健康状態を記したもので、「①医療提供者、医療保険者、雇用者又は医療情報交換事業者によって作成され、又は受け取られたもので、②個人の過去、現在、若しくは将来にわたる身体的・精神的な状態、医療に対する支払い、又は過去、現在、将来にわたる医療に対する支払いに関連するもの」で、当該個人を識別可能、又は当該情報を用いて個人を識別することができると信じるにつき相当の根拠があるとされるもの。

④規制・権利の内容

・それぞれの分野ごとに、情報主体のコントロール権を中心に定められている。

＜FCRA の定める規制・権利の内容＞

・提供制限：消費者報告の提供が許容される場合の限定（FCRA,604)。

・収集制限：一定期間経過後の情報報告の禁止（FCRA,605)。消費者報告機関は、消費者調査報告がなされることを開示しない限り、消費者調査報告を入手ないし作成してはならない（FCRA.606)。消費者報告機関の手続は、情報を利用しようとする者に対し、その身分を証明させ、またその目的以外には用いないことを確保させるものでなければならない。消費者報告機関は、消費者報告を提供するに先立ち、その者の身分の証明及び用途を確認するために合理的な努力を払わなければならない（FCRA.607)。

・本人からの請求：消費者が求めた場合、消費者報告機関は、消費者に関する情報ファイル（医療情報を除く）の実質的内容、情報源、消費者報告の受取人などを開示する義務を

負う（FCRA.609）。ファイルに記載された情報の完全性又は正確性について消費者から異議申立があった場合に、消費者報告機関は情報について再調査する義務を負う（FCRA.611）。

＜HIPAA プライバシールールの定める規制・権利の内容＞

・提供制限：原則として、個人の許可を必要とする（45 C.F.R. 162.508）。同意なく利用できる場合として、TPO（①診療時、②支払時、③医療業務管理時）に用いる場合（45 C.F.R. 162.506、同意をとるかどうかは選択制）、例外として個人の許可を必要としないもの（45 C.F.R. 162.512）。

・収集制限：目的のための必要最小限（45 C.F.R. 162.502(b)）。

・通知：各医療機関は、医療情報の取扱い方針について患者に通知する義務（notice requirement）を有する（45 C.F.R. 162.520）。

・本人からの請求（開示・訂正・報告請求権）：患者は、①開示請求権（45 C.F.R. 162.524）、②訂正請求権（45 C.F.R. 162.526）、③医療記録利用・提供状況に関する記録告知を受ける権利（45 C.F.R. 162.528）、を有する。

⑤監督・登録制度

・それぞれの分野ごとに、個別法において定められている。

・FCRA（信用情報）について、法律に基づく規制・取締りは連邦取引委員会（Federal Trade Commission, FTC）が行う（FCRA,621）。

・FTC は、諸外国の監督機関ほど政府から独立しているわけではないが、消費者及び事業者の啓発に当たっている。FTC の機能は、①連邦取引委員会法に基づく、企業の個人情報の取扱いに関する不正・欺瞞の監視、②金融サービス近代化法に基づく、ｱ)金融のプライバシー通知に関する規則の実施、ｲ)個人情報の事務的、技術的及び物理的保護、ｳ)詐欺に対する執行、③公正信用報告法及びこどもオンラインプライバシー保護法に基づく、消費者のプライバシー保護を行うことである。また、監督機関として違反行為者を被告とする民事訴訟の提起権限も認められている。 登録制度に関する規定は置かれていない。

・HIPAA プライバシールール（医療情報）においては、事業者内に、プライバシー保護担当者（privacy officer）の設置が義務付けられている（職員研修の実施の要請、文書によるプライバシー関連手続の整備など）（45 C.F.R. 162.530(a)(1)）。登録制度に関する規定は置かれていない。

⑥主な適用除外

・それぞれの分野ごとに、その特性に応じて定められている。

・FCRA によれば、消費者報告には、「単に消費者とその報告をする者との間の取引又は経験に関する情報を内容とする報告」、「クレジットカード又はそれと類似の証票の発行者による直接又は間接の特定の信用供与の授権又は承認」、「第三者から直接又は間接に、ある消

費者に特定の信用供与をするよう要求されていた者が、その要求に関して自己の決定を伝える報告」は含まれない（FCRA,603(d)）。

⑦主な自主規制

・多様な自主規制、ガイドラインが存在している。医療情報については、アメリカ医師会医療倫理規定（American Medical Association, Code of Medical Ethics,2002）がある。金融情報については GLBA への準拠指針を業界団体（全米住宅ローン・ブローカー協会（National Association of Mortgage Brokers）及び全米自動車販売協会（National Association of Auto Dealers)）が FTC と共同で作成している。法律の規定がない分野においても、雇用情報についての「社内プライバシー規則」などが存在する[37]。
・アメリカには、政府が事業者団体に認証機能を委託する制度はない。存在する認証制度やシール付与制度はいずれも民間企業の自主的な取組。
・アメリカ政府による自主規制の奨励として、商務省（Department of Commerce, DOC）はセーフハーバー原則（Safe harbor principles）の策定など民間部門の取組みを支援するとともに、関係業界に適切な対応を強く働きかけている。FTC は、事業者がオンライン上で、自ら掲げたプライバシーポリシー（当該事業者の顧客のプライバシーをどのように扱うかについての方針の宣言）に違反していた場合、不公正又は詐欺的取引として摘発する任務を担う。
・民間部門の包括的個人情報保護制度の欠陥を補う産業界の自主的取組としては、①企業のプライバシーポリシー、②BBBOnline、TRUSTe、CPA WebTrust 等によるプライバシー・シール（マーク）、③W3C の個人情報交換規格（P3P）など。TRUSTe は、企業の Web サイトのプライバシーに関する方針の監督・認定を行っている他、セーフハーバー協定への参加を考慮しているアメリカ企業に対し、有料のプログラムを提供したり、カウンセリングを行ったりしている[38]。

（2）「個人情報保護に関する主な検討課題」関連項目に即した状況

①いわゆる「過剰反応」（誤解）に対応した第三者提供制限の例外事由

[現状について]

・FTC へのヒアリングによれば、過剰反応のような現象はみられており、FTC では金融機関や消費者から情報開示についてよく問い合わせを受けているとのことであった。
・保健福祉省（Health and Human Services, HHS）へのヒアリングによれば、HIPAA プライ

37　アメリカ自由人権協会「プライバシーの権利　情報化社会と個人情報保護」、127 頁（教育資料出版会、1994）。

38　http://www.truste.org/pdf/EUDataSheet.pdf.

バシー規則についても、施行後、規則の理解不足に起因する過剰反応がみられたとのことであった。例えば、患者の「保護された医療情報」(Protected health Information, PHI)を他の医療機関又は患者の友人や家族と共有することを拒否する事態など（45 C.F.R. 160.510a-b)。

[制度について]
・それぞれの分野ごとに、個別法において定められている。
・GLBA プライバシー規則によれば、金融機関の提供の例外事由について、「詐欺や不正取引等の防止」の場合、「民事、刑事、行政規制調査手続等に応じる場合等」について定められている（16 C.F.R. 313.13-15）
・HIPAA プライバシールールによれば、情報の提供には本人の同意又は許可があることが原則とされるが、例外としてどちらも必要なく情報が利用できる場合が定められている（45 C.F.R. 162.512)。a,法律の規定がある場合、b,公的健康業務(public health activities)に用いる場合、c,ネグレクトや DV の被害者情報についての公開、d,監督(health oversight activities）に用いる場合、e,司法手続、行政手続のための公開、f,法執行目的、g,死人についての情報開示が葬儀業者などに開示される場合、h,移植手術等の目的に用いられる場合、i,調査目的、j,健康・安全への深刻な脅威がある場合、k,特別な政治的理由がある場合。いずれの場合にも、例外事由については詳細に列挙されている。また、医療機関と業務提携をする会社に対しては、守秘義務契約を結ぶ必要がある（45 C.F.R. 164.532)。

[制度の運用について]
・FTC には、GLBA をはじめとする FTC の規制に対して質問のある企業や消費者のために、問い合わせ窓口が設けられている。法律上の許容性について、各企業及び消費者は窓口に電話で問い合わせることができる。
・FCRA については、FTC、連邦議員下院銀行・金融及び都市問題に関する委員会（消費者問題及び通貨制度に関する小委員会)、連邦準備制度理事会（Federal Reserve Board, FRB）は、各々消費者や消費者報告の利用者向けに Q&A 方式のガイドブックを作成しており、消費者等の理解の促進を図っている。これらは、「消費者のプライバシーと金融システムの効率的な機能の両者を確保するために、必然的に生じる数々の問題とそれらへの対処法、さらには最善の解決法を導く手掛かり」として参照されている[39]。
・HHS では、適用機関が HIPAA プライバシー規則を理解する手助けとして、HHS の市民権局（Office of Civil Rights, OCR）のウェブサイトや講演などで情報提供を行っている。

②自治会や同窓会等の取扱い

[制度について]

[39] 江夏健一監修『個人信用情報と訴訟』169 頁（文眞堂、1993 年)。

・自治会・同窓会における個人情報の取扱いについて、これを直接規制する連邦レベルの立法は存在しない（自治会や同窓会が主に取り扱う個人情報の種類について特別に定められた個別法は存在せず、FCRA、HIPAA などの既存の法律の適用範囲内にそれらの組織が区分されることがない限り、それらの組織が法の遵守を義務付けられることはない）。

③個人情報の定義

[制度について]

・アメリカには、包括的なプライバシー法は存在せず、特定の分野ごとに法律が作成されている。このため、プライバシー法ごとに各々固有の個人情報の定義がされており、その分野に限って規制が適用される仕組みとなっている。

・GLBA の対象とする個人情報は、「非公開個人情報」（nonpublic personal information）（16 C.F.R. 313.3）。これは、「個人を識別でき、かつ、一般に入手可能でない金融情報全般」をさす。

・FCRA の対象とする個人情報となる「消費者報告」とは、消費者個人の信用度、信用に対する評価、信用枠、特性、社会的評判、身上事項、生活様式に関する消費者報告機関による情報の伝達であって、信用若しくは保険、雇用目的、又は 604 条で認められているその他の目的のために、消費者の適格性を判断するに当たり用いられ又は収集されるもの（FCRA,603(d)）。このうち、「消費者調査報告」とは、消費者報告又はその一部分であって、消費者の性質、社会的評判、身上事項又は生活様式についての情報が、被報告者である消費者の隣人、友人、仲間、知人、又はこれらの事項の情報につき知っていると思われる者に対する個人的な面接によって得られるもの（FCRA,603(e)）をいう。

・HIPAA プライバシールールの対象となる情報は、「個人の識別が可能な医療情報（individually identifiable health information）」（45 C.F.R. 164.501）。これは、治療情報や医療機関で利用される情報を含む個人の健康状態を記したもので、「①医療提供者、医療保険者、雇用者又は医療情報交換事業者によって作成され、又は受け取られたもので、②個人の過去、現在、若しくは将来にわたる身体的・精神的な状態、医療に対する支払い、又は過去、現在、将来にわたる医療に対する支払いに関連するもの」で、当該個人を識別可能、又は当該情報を用いて個人を識別することができると信じるにつき相当の根拠があるとされるもの（「PHI」と表現されている）。

④センシティブ情報に関する規定

[制度について]

・それ自体センシティブな情報であると考えられる消費者報告（信用情報）のうち、消費者調査報告についてはさらに要保護性の高い情報であると考えられることから、その開示が厳格に制限されている（FCRA,606）。

・収集制限：FCRA においては、一定期間の経過した古い情報（10 年以上経過した破産宣告

についての報告、7 年以上経過した訴訟・判決、 7 年以上経過した租税先取特権、7 年以上経過した信用取引勘定に関する報告、7 年以上経過した逮捕・正式起訴又は有罪判決の記録、その他消費者に不利益な情報であって、報告の時までに 7 年を経過しているもの。）については、消費者報告に含めてはならない（FCRA,605)。消費者報告機関が消費者調査報告を作成する場合には「その報告の中の消費者に不利益な情報（公的記録に係る情報を除く）を、後の消費者報告の内容としてはならない」（FCRA,614．3 ヵ月以内に入手されたものでなければ、不利益な情報は消費者報告に記載できない)。

・飲酒癖、生活水準、支持政党、性生活、夫婦仲などといった他人に知られたくないような私事を含む報告については、FCRA は規制の対象としていない。

・それ自体センシティブな情報であると考えられる医療情報は、原則として本人（患者）の同意がない限り利用・提供は許されない（PHI の利用提供は必要最小限のものに限られている)。HIPAA プライバシールールは医精神科治療記録（psychotherapy notes）になど特に配慮を要する情報について、別途規定をおく（45 C.F.R.　164.508)。

[制度の運用について]

・ヒアリングにおいては、講じられている具体的な措置に関する回答は得られなかった（例えば GLBA については、情報の取扱いに関しては諸規則（16 C.F.R.　313.10-12）が定められ、これに基づいて運用されている、との回答に留まった)。

⑤小規模事業者の取扱い

[現状について]

・DOC へのヒアリングによれば、セーフハーバー協定への参加者のうち、約 35%が小規模事業者であるとのことであった。

・HHS へのヒアリングによれば、HIPAA プライバシー規則の適用機関には、小規模事業者も含まれている（小規模事業者にも大規模事業者同様に規則が適用されるが、概ね問題なく導入されている）とのことであった。

[制度について]

・それぞれの分野ごとに、個別法において定められている。

・FCRA には、人数や規模による事業者の差別化規定は存在しない。法の対象となる事業者には、「消費者報告を第三者に提供する目的をもって消費者の信用情報その他の消費者に関する情報を収集し、又は評価することを通常業務の全部又は一部とする者で、消費者信用報告を提供する可能性のある者すべて」が含まれる（FCRA,603(f).)。

・HIPAA プライバシールールによれば、「従業員 50 人以下の自己運営管理医療プラン」は HIPAA の適用除外となるため、プライバシールールからも適用が除外される（160.103.もっとも、この適用除外規定は小規模事業者への配慮というより、HIPAA の目的が医療情報

の電子化であることから認められた適用除外規定であると考えられる)。

[制度の運用について]

・DOC では、セーフハーバー協定への参加におけるカウンセリングサービスが提供されている。DOC へのヒアリングで得られた回答によれば、協定の参加を申請している企業のうち、小規模事業者は組織内に法律部門がないため、協定に参加するためにどのような手続を経る必要があるのかを理解するために、コンサルティングなどの支援をより多く必要とする場合がある、とのこと。

・HHS は規則の制定の際、小規模事業者も無理なく適用できる内容に配慮したとのことであったが、小規模事業者の中には独自の法律部門を持たないなどの理由から、規則の遵守が難しい場合があるようである。

⑥個人情報の目的外利用の防止措置

[制度について]

・個別法ごとに規定が設けられている。

・信用情報については、消費者報告機関に対して目的外利用の制限の規定を設け(「いかなる消費者報告機関も・・消費者報告の提供を 604 条に列挙された目的に限定するために、合理的な手続に従わなければならない。この手続は、情報利用者に対し、その身分を証明させ、またその情報を求める目的及びその情報をそれ以外の目的には用いないことを保証させるものでなければならない」(FCRA,607))、この規定は、直接的には罰則により担保されている(故意又は過失で法に違反した場合には、当該消費者報告機関又は情報利用者は、消費者に対する民事上の損害賠償責任を負う(FCRA,616-617.))。

・HIPAA プライバシールールは、原則として、個人情報の利用・公開には本人の許可を得る必要があると定めている(45 C.F.R. 164.508)。医療機関による医療個人情報が適切に管理されているかは、プライバシー保護担当者により監督される(45 C.F.R. 164.530(a)(1))。もっとも、患者から許可を得て対象機関以外の第三者に情報が提供された後は、HIPAA による規制は及ばないことになる。

[制度の運用について]

・個人情報の濫用防止を含めた HIPAA の法執行の適正性の確保のために、外部機関による教育プログラム、非営利の医療認定組織による HIPAA 適用認定事業が設けられている[40]。アメリカ病院連盟 (American Hospital Association, AHA), アメリカ医療連盟 (American Medical Association, AMA), ヘルスケア情報管理システム (Healthcare

[40] 真野俊樹編著『医療機関の個人情報保護対策』57-58 頁(中央経済社、2005 年)。HHS へのヒアリングでは、業界団体の JCAHO (Joint Commission of the Accreditation of Healthcare Organization)の認定プログラムの紹介があった(ただしこれは JCAHO 独自のもので、HHS の OCR が関与するものではないとのこと)。

Information Management system, HIMSS)といった業界団体は、各々の会員に対して HIPAA 遵守方法についてガイダンスを提供している。
・FTC へのヒアリングによれば、目的外利用防止のために定められている規則に基づく規制を実際に施行することは（FTC にとって）非常に困難である、とのことであった（例えば GLBA の運用において、マーケッターが GLBA の規定外の情報源から消費者の情報を入手したり、金融機関が規制対象外である非金融機関との事業の一環で情報を収集している場合に、GLBA の規制対象行為となるかどうかの判別が難しい点など）。

⑦市販の名簿の管理

[現状について]
・民間部門の名簿、住所録に関しては、個別分野の規制に委ねられる。アメリカには、調査業を特別に対象とした規制はない。
・法の適用対象となる情報であれば、当該情報が市販されている名簿に載せられている場合にも、他の媒体の情報と同様に当該法律の規制対象とされる。

[制度について]
・FCRA において、消費者報告とは消費者の適格を判断するにあたり、役立てる目的を持つものとされる。従って、氏名・住所・配偶者の有無等内容が限定的な人名録、電話帳、当座預金口座をもつ個人名簿、事業者名簿などはそれのみでは「消費者報告」とはならない。
・金融情報について、GLBA は個人を識別できる個々の消費者に関する金融情報と、金融情報から派生している複数の消費者に関する金融情報のリストに関する取扱いを特別に区別していないため、法の対象とされる非公開個人情報には、複数の消費者に関する情報リストも含まれることがある。GLBA においては、「名簿」に関する独自の規定はない。
・HIPAA プライバシールールは、対象機関が保有する情報であれば名簿に含まれる医療情報についても適用がある。規則では、医療業務に携わるもの以外の利用については規制できないことが一つの限界であると指摘されている[41]が、HHS へのヒアリングによれば、HHS はこれを問題とは考えていないとのことであった（後に述べる「匿名化」の手続を利用することによって、対処できるとの回答）。
・教育情報（学校記録）のうち、当該校が連邦教育省から資金を受けている場合には、家庭教育の権利とプライバシーに関する法（FERPA）の適用を受ける。FERPA における名簿情報とは、生徒の名前、住所、電話番号、生年月日、出生地、専攻、クラブ活動や生徒会活動への参加状況、出席状況、卒業資格と賞、出身校等である（20 U.S.C. 1232g(a)(5)(A). 45 C.F.R. 99.32.）。名簿情報は、生徒又は親が開示してはならないと指示している場合には開示できないが、異議申立のなかった名簿情報については自由に開示することができ

[41] 開原成允・樋口範雄編「医療の個人情報保護とセキュリティ（第 2 版）」67 頁（有斐閣、2005 年）

る（20 U.S.C. 1232g(a)(5)(A)and(B). 45 C.F.R. 99.37)。

[制度の運用について]

・HIPAA プライバシー規則に定められる「匿名化(De-identification)」(45 C.F.R. 160.514)による対応が可能となる。匿名化とは、規則（45 C.F.R. 160.514）に定められる 18 の識別肢（Identifier）を取り除くことによって医療情報を匿名情報とすること。匿名化された医療情報は、広範囲にわたって配布されるリストに公表することができる。

⑧個人情報の取得元の開示に関する措置

[制度について]

・GLBA には開示を義務付ける規定は置かれていない。

・FCRA の解釈においては、消費者に対する開示の際には、消費者報告機関は消費者ファイルに記載されている全項目の内容を開示することとされている[42]。消費者報告機関は情報源についても開示しなければならないが、「単に消費者調査報告の作成にのみ利用され、その他の目的には利用されていない情報源はこの限りではない」と規定されている。

・HIPAA プライバシー規則には開示を義務付ける規定は置かれていない。

[制度の運用について]

・FTC へのヒアリングによれば、金融機関に対して個人情報の取得元の開示を義務付ける規定をおかない GLBA の運用において、開示請求への対応は各金融機関の自主性に委ねられているとのことであった。

[事業者の対応について]

・DOC へのヒアリングによれば、この問題はセーフハーバー協定の 7 原則の一つ（管轄外への情報転送（Onward Transfer)）の中で対応されるもの（協定の参加企業はこの原則を含む諸原則の遵守が義務付けられている）とのことであった。

⑨個人情報の利用停止・消去に関する措置

[制度について]

・個別法ごとに、調査請求権や個人情報の利用停止請求権について規定される場合がある。

・調査請求権として定められているもの：FCRA においては、消費者から情報の正確性について争いが提起された場合には、消費者報告機関は合理的な期間内に再調査し、情報を訂正することが要求される（FCRA,611)。調査によっても争いが解決しない場合には、消費者には文書提出権が認められる（FCRA611(b)）。争いについての文書が提出された場合、消費者報告機関は以降の消費者報告に、その旨を注記し、文書又はその要約を添付するこ

[42] 江夏健一編『FTC vs.FCRA』255 頁（文眞堂、1991 年)。

ととされる（FCRA611(c)）。調査の結果、不正確とされた情報については消費者報告機関により削除される。この場合、情報利用者に対しては、情報が削除されたことについての通知が送付される。

・訂正請求権として定められているもの：HIPAA プライバシールールにおいては、訂正請求権（45 C.F.R.　162.526）が認められているが、利用停止や消去については定められていない。

[制度の運用について]

・HIPAA プライバシールールでは、PHI の利用停止や消去に関する要件を規定していないが、HHS へのヒアリングによれば、これは医療機関ごとの判断、州法の規定に委ねるとの趣旨によるもの、とのことであった。

⑩国際的な情報移転に関する措置

[制度について]

・法律によっては、海外の事業者に情報が提供される場合に、国内法の規定が適用されることについて明示するものがある。

・HIPAA プライバシールールは、国防総省によって運営される海外の医療ケア施設には適用される（45 C.F.R. 164.501（c）など）。

・アメリカで取引を行っている金融機関、及びアメリカの通商に影響力のある金融機関には、GLBA の遵守が義務付けられている。

[法律以外の枠組みについて]

・EU データ保護指令への対応として、セーフハーバー条項への対応が行われている（⑪を参照）。

⑪EU データ保護指令に対する対応状況

[現状について]

・民間の自主規制を尊重し、セグメント方式で法整備を進めるアメリカにおいては、法制による EU データ保護指令への準拠は困難である。このため、特定の認証基準を設け、その認証を受けた企業ごとに十分性を付与する「セーフハーバー原則」について、2000 年に協定を締結している。この協定により、DOC が作成するプライバシー原則（Privacy Principles）を企業が遵守することにより、EU データ保護指令 25 条違反とはならないことが約されている。

・DOC へのヒアリングによれば、現在、セーフハーバー協定に参加している企業数は 1,045 社、セーフハーバー協定に対する業界の反応は好意的であるとのこと。また、セーフハーバー協定における条項を改善する予定などはない、とのことであった。

［セーフハーバー協定の概要について］

・セーフハーバー原則における個人情報とは、「識別された、又は識別可能な個人のデータであって、EU データ保護指令の対象内で、アメリカのある組織が EU から受け取り、記録されるもの」である。セーフハーバー原則においては、①第三者に提供する場合、②当初目的と合致しない目的のために個人情報を利用する場合にはオプトアウトの機会を与えなければならない、とされる。センシティブ情報（医療・健康状態、人種、民族的出自、政治的意見、宗教的・哲学的信条、労働組合の組合員であることを特定する情報、性生活を特定する情報）が第三者に提供される場合、又はオプトインにより承認された目的以外に利用される場合、積極的又は明示のオプトインが与えられなければならない、とされる。

・適用範囲：セーフハーバーに加入した事業者が、EU の事業者と通商や情報の流通を行う際に適用される。セーフハーバーへの加入は任意である。

・「原則」の内容：告知原則、選択原則、データ移転の原則、セキュリティの原則、データの完全性の原則、アクセスの原則、仲裁の原則。

・監督・登録制度：セーフハーバー原則の遵守事項に違反している場合には、商務省から告知を受ける。違反行為が認められた場合（セーフハーバー原則に違反した企業等）には連邦取引委員会（FTC）が連邦取引委員会法 5 条に基づき調査、「不公正又は欺瞞的な行為」に該当すると判断された場合には民事罰等の制裁措置が行われる。FTC は停止命令を出すこともできる。

⑫第三者機関の概要

[制度について]

・個別法の規定に委ねられている。

・FCRA については、FTC の消費者保護局（Bureau of Consumer Protection, BCP）が、第三者機関として、苦情を受け付けている。ただし、政府からの独立性という観点からは、他国の第三者機関ほどの独立性は無く、個人情報に関する苦情の専門機関でもない（個人情報保護に特化しているわけではない）。

・HIPAA プライバシールールの苦情は、HHS の OCR で受け付けているが、専門機関ではない。

[制度の運用について]

・FTC へのヒアリングによれば、現在アメリカにおいては、医療・金融機関を含む様々な分野の企業が効果的な個人情報の取扱説明（Privacy Notice）をどのように策定することができるかについて調査するための省庁間ワーキンググループが招集されているとのこと。このワーキンググループにおいて、各省庁は共同で、効果的な個人情報保護規定について検討を行っている。

⑬死者に関する個人情報の保護

[制度について]

・規定されている法律と、規定されていない法律がある。

・HIPAA プライバシールールは、死者に関する個人情報についても適用されることを明示的に規定している（45 C.F.R. 164.502(f)）。

・死者の情報の取扱いについては、「対象機関は、検死官又は医療検査官に対し、死者の同定、死因の決定その他の法的義務を履行することを目的として、医療情報を提供することができる。対象機関が、検死官又は医療検査官の義務をも同時に履行している場合、本条に定める目的のために自ら医療情報を利用することができる」（45 C.F.R. 164.512(g)(1)）、「対象機関は、葬儀施主に対しその業務に必要な限りにおいて、法に定めるところにより情報を提供することができる」（45 C.F.R. 164.512(g)(2)）といった規定がある。

⑭直接処罰等の実効性確保の措置

[制度について]

・個別法ごとの規定に委ねられている。

・FCRA においては、故意又は過失による義務規定の不履行について、消費者報告機関又は情報利用者は、民事上の責任を負う（FCRA,616-617）。消費者報告機関から消費者についての情報を、故意に虚偽の名目で得たものは、5,000 ドル以下の罰金若しくは 1 年以下の懲役又は併科（FCRA,619）。

・FTC へのヒアリングによれば、FTC は法の定める罰金の他、違反企業が独立した第三者による定期的監査を受けることを求めることもある（GLBA 違反の企業につき、情報セキュリティプログラムの実施と 2 年ごとの監査を今後 20 年受けるための費用を負担する旨を命じた例がある）[43]。

・HIPAA は、プライバシールールを遵守しない情報の取扱いについて罰則を設けている（HIPAA,1177）。民事罰（1 件あたり 100 ドル、1 人あたり年間 2 万 5 千ドルまで）。本人の同意無しに情報を入手、提供したものには 5 万ドル以下の罰金及び 1 年未満の懲役刑。意図的な虚偽を用いて入手した場合には 10 万ドル以下の罰金及び 5 年未満の懲役、さらに営利目的や被害を与える意図がある場合には 2 万 5 千ドル以下の罰金と 10 年未満の懲役。法執行は HHS の OCR が行う。

[制度の運用について]

・HHS へのヒアリングによれば、2006 年 12 月までに HIPAA の違反者に対する罰金処分の例

[43] FTC の取締りと一例として、不動産会社である National Title Agency 社が GLBA 規定を侵害していた事例など（FTC Press Release,Real Estate Service Company Settles Privacy and Security Charge, http://www.ftc.gov/opa/2006/05/20060510-3.htm）。

はないとのこと。

⑮その他、特に留意すべき重要措置

［今後の取組の動向について］

・ブッシュ大統領は、2006 年 5 月 10 日、ID 盗難対策タスクフォースを設置している。このタスクフォースは、個人の ID 保護対策への提言を各省庁に行うことになっている[44]。

・アメリカ議会は、個人情報侵害通知法（Data Breach Notification Act）について審議を行っていたが、可決には至らなかった（この法案は、顧客の個人情報の安全性に問題が発生した場合、企業は、顧客にそれを通知することを義務付けることを内容とするもの)。同法案に関する大統領タスクフォースは、個人情報盗難防止のために各省庁が講じることのできる措置について提言を策定中である。

・HHS の OCR は、(ハリケーンなどの)緊急事態後の医療ケア提供手法、電子カルテ(Electronic Health Record, EHR）への規定の拡張などについてのイニシアティブに参画している。

［州法との関係、その他について］

・州法について、アメリカの個人情報保護制度は、連邦法による保護のみならず、州レベルでも様々な法律が制定されている。州においても連邦と同様に、個人情報保護に関する法律はセクトラル方式がとられている。

・州法との関係を法文中に規定するものもある（「消費者についての情報の収集、配布又は利用に関する州法を、無効とし、変更し・・適用を免除するものではない」（FCRA,622）など)。FCRA と州法の規定が抵触する場合には FCRA の規定が優先する。幾つかの州法では、連邦法より厳しい制限が課されることがある。例えば、ニューヨーク州では、裁判が係争中でない限り、有罪とされなかった刑事訴追又は逮捕の記録を消費者報告機関が報告することを禁止している。また、人種、宗教、肌の色、家柄などに関する情報や、入手目的が不明瞭な情報についても取扱いを禁止している。

・医療分野に適用される個人情報保護に関する規制は HIPAA プライバシールールの他にも存在する。公的機関についてはプライバシー法の適用対象となる。アルコール、薬物濫用に関しては、薬物乱用防止・治療・リハビリ法（Drug Abuse Prevention,Treatment and Rehabilitation Act）や総合アルコール乱用及びアルコール依存症防止・治療・リハビリ法 （ Comprehensive Alcohol Abuse and Alcoholism Prevention,Treatment, and Rehabilitation Act）など。多くの州は、精神健康、HIV、性感染病など特定の種類の医療情報におけるプライバシーを保護するために独自の法律を制定している。州法が HIPAA よりも弱い効力のものである場合を除いて、HIPAA プライバシールールではなく州のプライバシー法が適用される。

---

[44] White House, Exective Order,Strengthening Federal Effects to Protect Against Identity Theft(2006.5.10).

Ⅱ．国際機関

１．OECD[45]

（１）個人情報保護制度の概要

①制度名

・プライバシー保護と個人データの国際流通についてのガイドラインに関するOECD理事会勧告（OECD Recommendation of the Council concerning the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ）（以下「OECD プライバシー・ガイドライン」という。）

・OECDプライバシー・ガイドラインは1980年9月23日に採択された。

②目的

・加盟国間の情報の自由な流通を促進すること、及び、加盟国間の経済的社会的関係の発展に対する不当な障害の創設を回避すること（前文)。

③適用範囲（規制の対象、対象国及び拘束の程度を含む）

・規制の対象：個人に関する情報であって、個人が識別され又は識別され得るあらゆる情報(個人データ)（1条b）のうち、公的又は私的部門において、取扱方法又は性質若しくは利用状況からみて、プライバシーと個人の自由に対する危険を含んでいるもののすべて（2条)。

(注)個人データにおいて識別され又は識別可能な個人は、「データ主体」とされる(1条ｂ))。

・対象国：OECD加盟国。

・拘束の程度：OECD加盟国は、OECD理事会からガイドラインに準じた対応を採ることが勧告されるが、その遵守を義務付けられているわけではない。前文は、以下のことを求めている。

1. 加盟国は、本勧告の主要部分である勧告付属文書のガイドラインに掲げているプライバシーと個人の自由の保護に係わる原則を、その国内法の中で考慮すること。
2. 加盟国は、プライバシー保護の名目で、個人データの国際流通に対する不当な障害を除去すること、又は、そのような障害の創設を回避することに努めること。
3. 加盟国は、勧告付属文書に掲げられているガイドラインの履行に協力すること。

---

[45] 当節で引用しているガイドラインの日本語訳は、「外務省ホームページ：http://www.mofa.go.jp/mofaj/gaiko/oecd/privacy.html（2006年12月)」による日本語訳を用いている。

4. 加盟国は、このガイドラインを適用するために、特別の協議・協力の手続についてできるだけ速やかに同意すること。

さらに、6 条は、「本ガイドラインは、最低基準であって、プライバシーと個人の自由を保護することを目指す別の諸措置で補完されるものとみなされるべき」としている。

④規制・権利の内容

ア）収集制限の原則（7 条）

・個人データの収集制限を設けるべきである。

・いかなる個人データも、適法かつ公正な手段によって、かつ、必要に応じて、データ主体に告知するか、若しくは、その同意を得た上で収集するものとすべきである。

イ）データ内容の原則（8 条）

・個人データは、その利用目的に沿った内容であるべきである。

・当該利用目的に必要な範囲内において、正確、完全であり最新のものに保たれるべきである。

ウ）目的明確化の原則（9 条）

・個人データの収集目的は、遅くともデータ収集時には明確化されるべきである。

・事後の利用は、以下の場合に限定されるべきである。

-当該収集目的の達成

-当該収集目的とは別目的ではあるが、目的変更時に明確化された目的の達成

エ）利用制限の原則（10 条）

・個人データは、目的明確化原則により明確化された目的以外の目的のために開示、利用その他の使用に供されるべきではない。ただし、以下の場合を除く。

a)データ主体の同意がある場合、又は

b)法律の規定に基づく場合

オ）安全保護の原則（11 条）

・個人データは、その紛失若しくは不当なアクセス・破壊・使用・修正・開示等の危険に対し、合理的な安全保護措置により保護されるべきである。

カ）公開の原則（12 条）

・個人データに関する開発、運用及び政策の透明性を確保するための一般的な政策を実施すべきである。

・個人データの存在、性質、その主要な利用目的、さらには、当該個人データのデータ管

理者の身元とその通常の所在地を特定できる手段を容易に利用できるべきである。
(注)データ管理者とは、国内法の下で、個人データの内容及び利用に関する決定権限を有する者を意味する。その際、当該データの収集、保存、取扱い、提供が、当該管理者によってされているのか、当該管理者の名の下でその職員によっているのかは問わない(1条 a))。

キ）個人参加の原則（13 条）
・個人は以下の権利を有すべきである。
a)データ管理者その他の者から、データ管理者が自己に関するデータを保有しているか否かの確認を得ること
b)自己に関するデータを
ⅰ)合理的な期間内に
ⅱ)必要があれば、過度にならない費用で
ⅲ)合理的な手段で
ⅳ）自己にわかりやすい形で
自己に提供されること
c)上記 a)及び b)の請求が拒否された場合に、その理由が提示されること、及び、当該拒否に対して異議申立ができること
d)自己に関するデータについて異議申立ができること、及び、その異議申立が認められた場合には、当該データを消去、訂正、完全化及び補正させること

ク）責任の原則（14 条）
・あらゆるデータ管理者には、上記諸原則を実施するための措置を講ずる責任を負わせるべきである。

⑤監督・登録制度
・OECD プライバシー・ガイドラインには、監督・登録制度を直接に定める規定は存在しない。
・各国が整備すべき具体的な法制度は、国ごとに異なり得ることから、第三者機関の設置や登録制度の実施についても国ごとに多様であることが前提となる。なお、前述③及び後述⑦ア）参照。

⑥主な適用除外
・適用除外についての定めはない。
・各国が整備すべき具体的な法制度は、国ごとに異なり得ることから、適用除外ついても国ごとに多様であることが前提となる。なお、前述③及び後述⑦ア）参照。

⑦その他

ア）第 4 部「国内実施」19 条は、以下のように定める。

「第 2 部及び第 3 部に定める諸原則の国内実施に際し、加盟国は、個人データに関するプライバシーと個人の自由を保護するための、法的、行政的その他の手続又は制度を整備すべきである。特に、加盟国は以下の点に努めるべきである。

a）適切な国内法を制定する。

b）行動規準その他の形式による自主規制システム整備を奨励し、支援する。

c）個人にその権利を行使するための合理的な手段を提供する。

d）第 2 部及び第 3 部の諸原則の実施措置を遵守しない場合における適切な制裁及びそれに対する救済手段を提供する。

e）データ主体に対する不当な差別がないようにする。」

・19 条について、説明覚書 69 条は、以下のように述べる。「本ガイドライン第 2 部及び第 3 部の具体的な実施手段(implementation, modalités)を整備するのは、まずもって、各加盟国である。これらの実施手段が、様々な法的制度・伝統によって多様であることは当然であり、したがって、19 条は、本ガイドラインを適用させるにあたり検討されるべき国内制度の種類について、大まかに示した一般的枠組みを設定しようと努めたものに過ぎない。冒頭の文章（前文）は、一般的な問題、更には統制手段に関する問題につき、各国が着手するための手段を複数示したものである（例えば、特別な監督機関の創設や、裁判所その他の公的機関といった既存の統制手段の利用等）。

・さらに、説明覚書 70 条によれば、19 条各号は、以下のように理解される。

a）19 条(a)は、各国に対し、適切な国内法を制定するよう求めるが、この<<適切な>>という言葉は、立法的解決の適切性は各国が判断することを意味している。

b）19 条（b）は、主としてコモン･ロー国家を念頭に置くもので、これらの国においては、法律以外の制度による本ガイドラインの実施が、立法行為を補完することになる。

c）19 条（c）は、データ管理者からの意見や、法的援助や支援といった制度を予定している。また、刑事罰や、民事及び行政上の制裁を念頭に置いている[46]。

d）19 条(d)は、統制機関が多様であり得ることを示す。つまり、特別の監督機関を設けるのか、裁判所その他の公的機関等、既存の統制手段を利用するのか。

e）19 条(e)は、差別に関わるもので、不平等な取扱いを排除しようとするものだが、たとえば、被差別集団を支援するためといった、<<良性の差別(benign discrimination)>>を認める可能性は残される。排除されるのは、国籍や居所、性別、民族、信教、労働組合所属等による差別である。

イ）「第 5 部　国際協力」は、以下のように定める。

20 条「加盟国は、求めに応じて、本ガイドラインで定められた諸原則を適用するための具

[46] この一文は、本ガイドラインの仏語版にのみ存在する。

体的な実施手段を、他の加盟国に示すべきである。また、加盟国は、個人データの国際流通や、プライバシー及び個人の自由の保護に関する手続が、簡明であり、かつ、本ガイドラインに適合する他の加盟国の手続と矛盾しないものとすべきである。」
21 条「加盟国は、以下の点を容易にする手続を定めるべきである。
・本ガイドラインに関する情報の交換、及び
・手続や調査に関する相互支援」
22 条「加盟国は、個人データの国際流通に適用される法を制度化するために、国内的及び国際的な原則を策定するよう努力すべきである」

（２）「個人情報保護に関する主な検討課題」関連項目に即した状況

①「個人情報」の定義

・個人に関する情報であって、個人が識別され又は識別され得る情報のすべてが、個人データ(個人情報)とされる （1 条ｂ)）。本ガイドラインが適用されるのは、個人データのうち、公的又は私的部門において、取扱方法又は性質若しくは利用状況からみて、プライバシーと個人の自由に対する危険を含んでいるものすべてである（2 条）(前述（１）③参照)。

② センシティブ情報に関する規定

・OECD プライバシー・ガイドラインには、センシティブ情報に関する規定は明記されていない。
・説明覚書 6 条は、センシティブ情報の定義は多様であるとし、説明覚書 19 条 a）は、普遍的にセンシティブなデータといったものを定義することは、おそらく不可能であるとしている。

③ 個人情報の目的外利用の防止に関する規定

・10 条は、個人データが、「目的明確化原則により明確化された目的以外の目的のためには開示、利用その他の使用に供されるべきではない」としつつ、以下の場合を例外とする。
a)データ主体の同意がある場合、又は
b)法律の規定に基づく場合（前述（１）④エ)）
・なお、9 条が、「個人データの収集目的は、遅くともデータ収集時には明確化されるべき」とし、事後の利用を、当該収集目的の達成と、当該収集目的とは別目的ではあるが、目的変更時に明確化された目的の達成の場合に限定し、目的明確化の原則を定めている（前述（１）④ウ)）。

④ 個人情報の取得元の開示に関する規定

・OECD プライバシー・ガイドラインに、個人情報の取得元の開示に関する規定は明記されていない。

⑤ 小規模事業者の取扱い

・OECD プライバシー・ガイドラインに、小規模事業者を特別扱いする旨の規定はない。

⑥ 個人情報の利用停止・消去に関する規定

・13 条が、個人に認められるべき権利の一つとして、「自己に関するデータについて異議申立ができること、及び、その異議申立が認められた場合には、当該データを消去、訂正、完全化及び補正させる」権利を明記している（前述（１）④キ）参照)。

⑦国際的な情報移転に関する規定

・「第 3 部　国際的適用における基本原則－自由な流通と合法的制度」において、国際的な情報移転に関する規定が、以下のように定められている。

15 条「加盟国は、個人データの国内での取扱いとその再移出が、他の加盟国に及ぼす影響について配慮すべきである。」

16 条「加盟国は、加盟国の一の通過を含めた個人データの国際流通が、阻害されることなく、かつ、安全になされることを確保するために、合理的かつ適切な手段のすべてを講ずるべきである。」

17 条「加盟国は、自国と他の加盟国との間における個人データの国際流通を制限することを控えるべきである。ただし、後者が、実質的に本ガイドラインをまだ遵守していない場合、又は、当該データの再移出が自国のプライバシー保護規制を免れようとする場合であれば、この限りでない。また、加盟国は、自国のプライバシー法制が、当該データの性格を理由に特別の規制を設けており、かつ、他の加盟国が自国と同等の保護を課していないようなある種の個人データについては、その流通を制限することができる。」

18 条「加盟国は、プライバシーと個人の自由の保護という名目で、これらの保護に必要な程度を超え、かつ、個人データの国際流通に対して障害を創設することになるような法律や政策及び運用を回避すべきである。」

⑧ 第三者機関に関する規定

・OECD プライバシー・ガイドラインに、第三者機関に関する規定は明記されていない。

・各国の法体系等によって、採るべき実効性担保の仕組みは変わり得るため、第三者機関の設置や登録制度の内容は、国ごとに異なり得ることから（説明覚書 6 条）と記述され、第三者機関については、各国の判断に委ねられている（前述（1）③、(1）⑦ア）参照)。

⑨ 死者に関する個人情報の保護

・OECD プライバシー・ガイドラインに、死者に関する個人情報の保護に関する規定は明記されていない。

⑩ 直接処罰等の実効性担保に関する規定

・第 4 部 19 条は、「第 2 部及び第 3 部に定める諸原則の国内実施に際し、加盟国は、個人データに関するプライバシーと個人の自由を保護するための、法的、行政的その他の手続や制度を整備すべき」とし、そのうえで、加盟国が特に留意すべき点として、「(d) 第 2 部及び第 3 部の諸原則の実施措置を遵守しない場合における適切な制裁及びそれに対する救済手段を提供する」としている（前述（１）⑤ ⑦ア）参照)。

⑪ その他、特に留意すべき重要事項（今後の取組の予定等）

本ガイドライン以外に、以下のような動きがある。

・1992 年 11 月 26 日､「情報システムのセキュリティのためのガイドライン」が採択された。

・1997 年 3 月 27 日、「暗号政策ガイドライン」が採択された[47]。

・1998 年、オタワで開催された電子商取引に関する OECD 閣僚会議において、「グローバルネットワークでのプライバシー保護に関する宣言」が採択。OECD プライバシー・ガイドラインに沿って、国家と民間部門が協力して、開かれたグローバルネットワークを構築すべきことが確認された。

・2002 年 7 月 25 日、「情報システム及びネットワークのセキュリティのためのガイドライン:セキュリティ文化の普及に向けて」が、セキュリティ・ガイドラインの改定として、採択された[48]。

・2006 年 7 月 24 日に「プライバシーに関する通知文の簡素化-OECD による報告及び勧告-」が公表された.

・2006 年 10 月 26 日、プライバシー法執行の越境的な課題を検討するため、「プライバシー法の越境的な執行協力に関する報告書」が公表された。

[47] これについては、堀部政男「OECD の情報セキュリティ・プライバシー関係専門家会合の活動とガイドラインの策定（上)」季報情報公開・個人情報保護 18 号（2005 年）2 頁参照。

[48] これについては、堀部政男「OECD の情報セキュリティ・プライバシー関係専門家会合の活動とガイドラインの策定（下)」季報情報公開・個人情報保護 19 号（2005 年）2 頁参照。

２．EU[49]

（１）個人情報保護制度の概要

①制度名

個人データの取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令（以下「EU データ保護指令」という）

②目的

個人データの取扱いに対する自然人の基本的権利及び自由、特にプライバシー権の保護（1条 1 項）

③適用範囲（規制の対象、対象国及び拘束の程度を含む）

- 規制の対象：全部又は一部が自動的な手段による個人データの取扱い、及び、ファイリングシステムの一部である、又はファイリングシステムの一部とすることを意図している個人データの非自動的な取扱い（3 条 1 項）
- 対象国：EU 構成国。ただし、第三国への個人データの移転を規制する、いわゆる第三国条項（25 条・26 条）を通じて、EU 構成国以外の国にも大きな影響を与える。
- 拘束の程度：EU 構成国は、指令を国内法化する義務を負う。

④規制・権利の内容

(1) データ内容に関する原則（6 条）
(2) データ取扱いの正当性の基準（7 条）
(3) 特別な種類のデータの取扱い（8 条・9 条）
(4) データ主体に提供されなければならない情報（10 条・11 条）
(5) アクセス権（12 条）
(6) データ主体の拒否権（14 条・15 条）
(7) 取扱いの秘密保持及び安全（16 条・17 条）
(8) 監督機関への通知等（18 条・19 条）
(9) 司法的救済、責任及び罰則（22 条～24 条）
(10)第三国に対する個人データの移動（25 条・26 条）
(11)行動規約（27 条）
(12)監督機関及び作業部会（28 条～30 条）

[49] 当節で引用している法文の日本語訳は、堀部政男「欧州連合（EU）個人情報保護指令の経緯」（新聞研究，No．578，1999 年 9 月）に掲載されている日本語訳を参考にしている。

⑤監督・登録制度

18 条　監督機関への通知義務

1.構成国は、管理者又はその代理人がいる場合はその者が、1 つの目的又は複数の関係する目的を達成することを意図した全部又は一部の自動処理作業を実施する前に、28 条に規定された監督機関に通知しなければならないことを定めなければならない。

2.構成国は、次に掲げる場合に、かつ次に掲げる条件に基づいてのみ、通知の簡略化又は適用除外を定めることができる。

－取り扱われるデータを考慮しつつ、データ主体の権利及び自由に制約的な影響を与えるおそれが低い種類の取扱作業に関して、管理者又はその代理人が取扱いの目的、取り扱われるデータ又はデータの種類、データ主体の所属、データの開示を受ける取得者又は取得者の所属、及びデータが保存される期間を特定した場合。及び／又は、

－管理者が、管理者を規律する国内法に従って、特に次に掲げる事項に関して責任を有するデータ保護担当役員を任命した場合。

－この指令に基づいて制定された国内法の規定を、それぞれの方法でもって、内部的適用を行うことを確保すること。

－21 条 2 項に定められた情報に関する事項を含む管理者が行う取扱作業の記録を保管すること。

これによって、取扱作業がデータ主体の権利及び自由に制約的な影響を与えるおそれがないよう保証すること。

3.構成国は、法律又は規則に従って、情報を公衆に提供することが予定されている、及び公衆一般又は正当な利益を証明する者のいずれかによる閲覧のために公開されている記録の保管を唯一の目的としている取扱いには、1 項の規定を適用しないことを定めることができる。

4.構成国は、8 条 2 項(d)に規定された、政治、思想、宗教又は労働組合の目的を有した財団、協会又はその他の非営利団体による、適切な保証の下での正当な活動の過程において行われる取扱作業の場合に、通知義務の適用除外又は通知の簡略化を定めることができる。

5.構成国は、個人データを含む一定の又はすべての非自動的取扱作業が通知されなければならないことを明記し、又はこれらの取扱作業には簡略化された通知が必要であることを定めることができる。

⑥主な適用除外

・　この指令は、次に掲げる個人データの取扱いには適用してはならない（3 条 2 項）。

－欧州連合条約第Ⅴ章及び第Ⅵ章に規定されているような共同体法の適用範囲外の活動中に行われるもの、及び公安、防衛、国家安全保障(取扱作業が国家安全保障問題にかかる場合には国家の経済的安定を含む)又は刑事法の分野における国家の活動に関するすべての取扱作業。

－自然人によって、純粋に個人的な又は家庭内での活動中に行われるもの。

・ 構成国は、プライバシー権と表現の自由に関する準則とを調和させる必要がある場合に限り、ジャーナリズム目的又は芸術上、文学上の表現目的のためにのみ行われる個人データの取扱いについて、本章（Ⅱ章）、第Ⅳ章及び第Ⅵ章の規定の適用除外及び例外を定めなければならない（9 条）。

（2）「個人情報保護に関する主な検討課題」関連項目に即した状況

①「個人情報」の定義

「個人データ」とは、識別された又は識別され得る自然人（以下「データ主体」という。）に関するすべての情報をいう。識別され得る個人とは、特に個人識別番号、又は肉体的、生理的、精神的、経済的、文化的若しくは社会的アイデンティティに特有な 1 つ又は 2 つ以上の要素を参照することによって、直接的又は間接的に識別され得る者をいう（2 条 a）。

② センシティブ情報に関する規定

8 条　特別な種類のデータの取扱い

1. 構成国は、人種又は民族、政治的見解、宗教的又は思想的信条、労働組合への加入を明らかにする個人データの取扱い、及び健康又は性生活に関するデータの取扱いを禁止しなければならない。

2. 1 項の規定は、次のいずれかに該当する場合には、適用されない。

(a) データ主体が前項に定められたデータの取扱いに対して明示の同意を与えた場合。ただし、構成国の法律がデータ主体の同意によっても 1 項の禁止を解除し得ないことを規定している場合は、この限りではない。

(b) 取扱いが、労働法の分野において、管理者の義務の履行、及び特定の権利の行使の目的のために必要な場合。ただし、十分な保護措置を定めている国内法により、権限を与えられている場合に限る。

(c) データ主体が物理的に又は法的に同意を与えることができない場合に、データ主体又はその他の者の重大な利益を保護するために、取扱いが必要である場合。

(d) 政治、思想、宗教又は労働組合の目的を有した財団、協会又はその他の非営利団体によって、適切な保障のもとでの正当な活動の過程で、取扱いが行われる場合。ただし、その取扱いが当該団体の構成員又は団体の目的に関して団体と定期的に接触している者のみに関係していること、及び、当該データがデータ主体の同意を得ないで第三者に開示されないことを条件とする。

(e) データ主体によって明示的に公開されたデータに関する場合、又は法的な請求の確定、行使、若しくは防御のために必要な場合。

3.　1項の規定は、データの取扱いが予防的医療、診断、看護若しくは治療の提供又は健康管理サービスの運営の目的のために必要な場合、並びに、国内法又は国の管轄機関が定めた規則により、職業上の守秘義務を負う医療専門家によって、又は同様の守秘義務を負うその他の者によってデータが取り扱われる場合には、適用されない。

4.構成国は、適切な保護措置を定める場合に、重要な公共の利益を理由として、国内法又は監督機関の決定により、2項の規定に加えて、適用除外を定めることができる。

5.犯罪、刑事事件の有罪判決又は安全保障に関するデータの取扱いは、公的機関の管理の下でのみ行わせることができる。また、国内法に適合的な特定の保護措置が定められている場合には、その措置を定めた国内規定に基づいて、構成国により認められる例外に従って取り扱うことができる。 ただし、有罪判決の完全な記録は、公的機関の管理のもとでのみ保存することができる。

構成国は、行政的制裁又は民事訴訟に関するデータについても、公的機関の管理の下で取り扱われなければならないことを定めることができる。

6.　4項及び5項に規定されている第1項の規定の例外は、委員会に通知されなければならない。

7.構成国は、国内の個人識別番号又はその他の一般的に適用されている識別データの取扱いに関する条件を定めなければならない。

③ 個人情報の目的外利用の防止に関する規定

6条

1.構成国は、個人データが以下の条件を満たすことを確保しなければならない。

(a)公正かつ適法に取り扱われること。

(b)特定された明示的かつ適法な目的のために収集され、それに続いてこれらの目的と相容れない方法で取り扱われないこと。ただし、歴史的、統計的又は科学的な目的のために引き続き行われる取扱いは、構成国が適切な保護措置を定めている場合には、これと相容れないものとはみなされない。

(c)そのデータが収集され、及び／又は、それに続いて取り扱われる目的に照らして、適切であり、関連性があり、かつ過度でないこと。

(d)正確であり、かつ必要な場合にはデータを最新のものに保つこと。データが収集され、又はそれに続いて取り扱われる目的に照らして、不正確又は不完全なデータが消去又は修正されることを確保するために、あらゆる合理的な手段が講じられなければならない。

(e)データが収集される、又はそれに続いて取り扱われる目的に照らして必要とされる期間内に限り、データ主体の識別が可能な形態で保存されること。構成国は、歴史的、統計的又は科学的な利用のために長期間保存される個人データに関して適切な保護措置を定めなければならない。

2.管理者は、1項の遵守を確保しなければならない。

④ 個人情報の取得元の開示に関する規定

12 条　アクセス権

構成国は、すべてのデータ主体に対して、管理者から次に定めるものを取得する権利を保障しなければならない。

(a)合理的な間隔で制約なしに、過度の遅れ又は費用を伴うことなく、

―データ主体に関するデータが取り扱われているか否かの確認、及び少なくとも取扱いの目的、関係するデータの種類、開示されたデータの取得者又は取得者の所属に関する情報。

―取り扱われているデータ及びその情報源に関する入手可能な情報の理解可能な形式でのデータ主体への通知。

―少なくとも 15 条第 1 項に規定された自動的な決定の場合には、データ主体に関するデータの自動処理に係る論理についての知識。

⑤ 小規模事業者の取扱い

EU データ保護指令には、特別扱いする旨の規定はない。小規模事業者を個人情報保護制度の適用除外とすることについて、問題視されることがある（第三国に対する保護水準の審査におけるオーストラリアの例―-後述）。

⑥ 個人情報の利用停止・消去に関する規定

12 条　アクセス権

構成国は、すべてのデータ主体に対して、管理者から次に定めるものを取得する権利を保障しなければならない。

(a) 略

(b) 適切な場合には、特にデータの不完全又は不正確な性質のために、この指令の規定に従わないで取り扱われたデータの修正、消去又はブロック。

(c) データがすでに開示されている第三者に対する(b)に従って行われた、修正、消去又はブロックの通知。ただし、これが不可能であり又は過度の困難を伴う場合は、この限りではない。

⑦国際的な情報移転に関する規定

IV章　第三国への個人データの移転

25 条　原　則

1.構成国は、取り扱われている又は移転後に取扱いが予定されている個人データの第三国への移転は、この指令に従って採択された国内規定の遵守を損なうことなく、当該第三国が十分なレベルの保護措置を確保している場合に限って、行うことができることを定めな

ければならない。

2.第三国によって保障される保護のレベルの十分性は、一つのデータ移転作業又は一連のデータ移転作業に関するあらゆる状況にかんがみて、評価されなければならない。特に、データの性質、予定されている取扱作業の目的及び期間、発信国及び最終の目的国、当該第三国において有効である一般的及び分野別の法規範、並びに当該第三国において遵守されている専門的規範及び安全保護対策措置が考慮されなければならない。

3.構成国及び委員会は、第三国が 2 項の規定の意味における十分なレベルの保護を保障していないと考えられる事例について、相互に情報提供しなければならない。

4.構成国は、31 条 2 項に規定する手続に基づいて委員会が、第三国が本条 2 項の規定の意味における十分なレベルの保護を保障していないと認定した場合には、当該第三国への同一タイプのデータの移転を阻止するために必要な措置を講じなければならない。

5.委員会は、適切な時期に、4 項に基づく認定によってもたらされる状況を改善することを目的として交渉を開始しなければならない。

6.委員会は、31 条 2 項に規定する手続に基づいて、第三国が私生活、個人の基本的な自由及び権利を保護するための当該第三国の国内法、又は特に本条 5 項に規定された交渉の結果に基づいて締結した国際公約を理由として、2 項の規定の意味における十分なレベルの保護を保障していると認定することができる。

構成国は、委員会の決定を遵守するために必要な措置を講じなければならない。

第 26 条　例外

1.構成国は、25 条の例外として、及び特別な場合を規律する国内法に別段の定めがある場合を除いて、25 条 2 項の規定の意味における十分なレベルの保護を保障しない第三国に対する個人データの移転又は一連の移転は、次に掲げる条件を満たした場合に行うことができることを定めなければならない。

(a)データ主体が、予定されている移転に対して、明確な同意を与えている場合。

(b)移転が、データ主体と管理者との間の契約の履行のために、又はデータ主体の請求により、契約締結前の措置の実施のために必要である場合。

(c)移転が、データ主体の利益のために、管理者と第三者との間で結ばれる契約の締結又は履行のために必要である場合。

(d)移転が、重要な公共の利益を根拠として、又は法的請求の確定、行使若しくは防御のために必要である場合、又は法的に要求される場合。

(e)移転が、データ主体の重大な利益を保護するために必要である場合。

又は、

(f)法律又は規則に基づいて情報を一般に提供し、及び公衆一般又は正当な利益を証明する者のいずれかによる閲覧のために公開されている記録から、閲覧に関する法律に規定された条件が特定の事例において満たされる範囲内で、移転が行われる場合。

2.構成国は、1 項の規定を損なうことなく、管理者が個人のプライバシー並びに基本的な権利及び自由の保護、並びにこれらに相当する権利の行使に関して、十分な保護措置を提示する場合には、25 条 2 項の規定の意味における十分なレベルの保護を保障しない第三国への個人データの移転又は一連の移転を認めることができる。このような保護措置は、特に、適切な契約条項から帰結することができる。

3.構成国は、2 項の規定によって付与された許可を、委員会及び他の構成国に通知しなければならない。

一つの構成国又は委員会が、個人のプライバシー並びに基本的な権利及び自由の保護を含む正当な理由に基づいて異議申立を行った場合には、委員会は、31 条 2 項に規定された手続に基づいて、適切な措置を講じなければならない。

構成国は、委員会の決定を遵守するために必要な措置を講じなければならない。

4.委員会が 31 条 2 項に規定された手続に従って、一定の標準契約条項が本条 2 項によって要求される十分な保護措置を提供していると決定する場合には、構成国は、委員会の決定を遵守するために必要な処置を講じなければならない。

⑧ 第三者機関に関する規定

28 条　監督機関

1.各構成国は、1 つ又は 2 つ以上の公的機関が、この指令に従って構成国が採択した規定の範囲内で、その適用を監督する責任を負うことを定めなければならない。

この機関は、委任された職権を遂行するうえで、完全に独立して活動しなければならない。

2.各構成国は、個人データの取扱いに係る個人の権利及び自由の保護に関する行政措置又は規則を制定する際に、監督機関に諮ることを定めなければならない。

3.各監督機関は、特に次に掲げる権限を与えられなければならない。

―取扱作業の対象を構成するデータにアクセスする権限、及び監督職務の遂行に必要なすべての情報を収集する権限等の調査権限。

―例えば、20 条の規定に従って取扱作業の実施前に意見を述べ、及びこの意見の適切な公開を保障する権限、データのブロック、消去又は破壊を命じる権限、取扱いの一時的又は確定的な禁止を命じる権限、管理者を警告又は懲戒する権限、問題点を国会又はその他の政治機関に照会する権限等の介入権限。

―この指令に従って採択された国内規定への違反があった場合に、法的手続を開始する権限、又はこの違反を司法機関に通知する権限。

監督機関の決定に不服がある場合は、裁判所に対して訴訟を提起することができる。

4.各監督機関は、個人データの取扱いに係る個人の権利及び自由の保護に関して、個人又は個人を代表する協会からなされる主張を聴取しなければならない。その個人は、主張の結果についての情報を提供されなければならない。

5.各監督機関は、定期的に活動報告書を作成しなければならない。この報告書は、公開されなければならない

6.各監督機関は、当該取扱いに関してどの国内法が適用されるかにかかわらず、当該構成国の領域内においては、本条3項の規定に従って与えられた権限を行使することができる。

各監督機関は、他の構成国からこの権限の行使を求められることがある。

監督機関は、特にすべての有用な情報を交換する等、職務の遂行に必要な範囲内で、相互に協力しなければならない。

7.構成国は、監督機関の構成員及び職員が、退職後であっても、アクセスした機密情報に関して職業上の秘密義務を負うことを定めなければならない。

⑨ 死者に関する個人情報の保護

EU データ保護指令は、死者のデータについてはあえて言及していないというのが関係者の一致した解釈である。閣僚理事会、EU 委員会とも、「個人情報」に死者のデータを含めるか否かは、加盟各国の立法政策に委ねるという事で合意している。

⑩ 直接処罰等の実効性担保に関する規定

24条　制　裁

構成国は、この指令の規定を完全に実施することを担保するために適合的な措置を講じ、及びこの指令に従って定められた規定に対する違反がある場合に課される制裁について、特に定めなければならない。

⑪ その他、特に留意すべき重要事項（今後の取組の予定等）

2006年1月現在、EUから十分な保護水準を確保していると認められた国・地域は、スイス、カナダ、アルゼンチン、ガンジー島、マン島の5つである。

このうち、カナダは、2001年に1月に「個人情報保護及び電子文書法」(PIPEDA) を施行。2004年までに3段階に分けて民間事業者の対象範囲を広げ、2004年1月に全面施行となった。2001年12月20日の欧州委員会決定で、適切な保護水準の国と認められる。セグメント方式では、初めてEUデータ保護指令に準拠した事例。連邦政府部門対象の「連邦プライバシー法」、民間部門対象のPIPEDA、州政府対象の州法等、複数の法律を組み合わせることにより、ほぼすべての機関を対象とした法的枠組みを形成した。

また、アメリカ、オーストラリアのEUデータ保護指令への対応状況は以下のとおりである。

(1)アメリカ：民間の自主規制を尊重し、またセクトラル方式で法整備を進めるアメリカにおいては、法制による EU データ保護指令への準拠は困難である。このため、特定の認証基準を設け、その認証を受けた企業ごとに十分性を付与する「セーフハーバー原則」のための交渉を1998年より実施し、2000年に協定を締結

している。アメリカ企業がセーフハーバーに参加することは任意であるが、参加可能な企業は連邦取引委員会（FTC：Federal Trade Commission）及びアメリカ運輸省の管轄にある企業に限られており、連邦準備理事会（FRB）管轄の金融機関や、コモンキャリア、航空会社、貨物及び倉庫会社は含まれていない。2004 年末の EU 委員会の監査においては問題点が多く指摘され、①原則遵守の意思表明の必要性、②連邦政府（商務省）の強力な指導とモニタリングの必要性、③違反者に対する強力な影響力の行使の必要性などが連邦政府に要請された。

(2)オーストラリア：1988 年施行の「プライバシー法」の適用範囲を民間事業者にまで広げた「プライバシー修正法」を 2000 年に施行。これにより、法形式はセクトラル方式からオムニバス方式へと改変された。（ⅰ）年商 300 万豪ドル未満の小規模事業者及び被雇用者のデータが規制対象外とされたこと、（ⅱ）一般に利用可能な個人データが規制対象外とされたこと、（ⅲ）データ取得時の本人への通知が困難な場合には、事後に通知してもよいとされたこと、（ⅳ）ダイレクトマーケティングが主目的のデータ利用について、オプトアウトが認められていないこと、（ⅴ）センシティブデータの規制が収集のみで、利用や開示についての規制がないこと、（ⅵ）EU 市民の個人データについて、本人の訂正請求権が認められていないこと、（ⅶ）EU から取得した個人データをオーストラリアから第三国へ移転することが規制されていないこと等を理由に、保護水準が不十分とされた。

なお、EU においては、治安関係を中心に個人情報保護との衝突が深刻な問題として意識されてきている。

３．APEC

（１）個人情報保護制度の概要

①制度名

・APEC プライバシーフレームワーク(APEC Privacy Framework)（2004 年 10 月 29 日採択）（以下「APEC フレームワーク」という。）
・その内容には、項目ごとにナンバーがつけられている（以下「項」という。）。各項ごとに解説が付記されている（以下、条項の訳出は暫定的なものである）。

②目的

・APEC 加盟エコノミーにおける整合性のある個人情報保護への取組を促進し、不要な情報流通に対する障害を取り除くこと。

③適用範囲

・APEC 加盟エコノミーに対して、APEC フレームワークの適用を推奨しているもの。
・APEC フレームワークの適用に関しては、加盟エコノミーにおける個別事情を考慮すべきであると述べられている（6 項、12 項など）。

④規制・権利の内容（APEC フレームワークにおける諸原則）

・Ⅰ．損害の回避（14 項）
・Ⅱ．通知（15～17 項）
・Ⅲ．収集の制限（18 項）
・Ⅳ．個人情報の利用（19 項）
・Ⅴ．選択の機会提供（20 項）
・Ⅵ．個人情報の正確性確保（21 項）
・Ⅶ．安全管理措置（22 項）
・Ⅷ．開示・訂正（23～25 項）
・Ⅸ．説明責任（26 項）

⑤監督・登録制度

・APEC フレームワークには、監督・登録制度を直接に定める規定は存在しない。
・14 項には、加盟エコノミーにおいて損害の防止のために必要な措置をとることが規定され、その措置としては様々な方法が想定されている。

⑥主な適用除外

・12 項。原則の適用に当たっては加盟エコノミーごとの調整が可能とされる。
・13 項（適用除外)。国家主権、国家の安全、公共の安全、公共政策に関する情報について。

⑦主な自主規制

・APEC フレームワーク以外に、自主規制に関するガイドライン等は策定されていない。
・31 項によれば、フレームワークの実行化の一つの方法として「自主規制」という形が有り得ることが述べられている。

⑧その他

・APEC フレームワークには、加盟エコノミーにおける適用のためのガイダンス（part IV, A Guidance For Domestic Implementation)が記載されている（27 項)。

（２）「個人情報保護に関する主な検討課題」関連項目に即した状況

①「個人情報」の定義

・9 項（個人情報)。個人情報は、「個人が識別される、又は識別可能なすべての情報」とされる。

②センシティブ情報に関する規定

・22 項（安全管理措置）に、情報の安全管理は「情報のセンシティブ性の程度」に見合ったものでなければならない、と規定されている。
・23-25 項の解説部分に、業務上の機密情報（confidential commercial information）については個人のアクセスが制限される場合があると述べられている。
- 22 項　個人情報管理者は、紛失又は個人情報への不正アクセス、又は個人情報の不正な破壊、使用、変更又は開示、又はその他の誤用のようなリスクに対し、適切な安全管理により、個人情報を保護しなければならない。そのような安全管理は、想定される被害の可能性及び程度、情報のセンシティブ性の程度、及び保持の程度に応じたものでなければならない。また、定期的な見直し及び再評価を行わなければならない。
- 23 項　個人は、以下についての権利を有する。

a）個人は、個人情報管理者が、自身の個人情報を保持しているかどうかを確かめることができる。
b）個人は、本人確認の後、ⅰ.合理的な期間で、ⅱ.過度にならない費用で、ⅲ.合理的な方法で、ⅳ.わかりやすい形で、自らの個人情報について知ることができる。
c）個人は、情報の正確さを確認することができる。可能であり、かつ適当な場合には、

情報の修正、消去等を行うことができる。
- 24 項　（23 項に定める情報へのアクセス、修正が除外される場合）
- 25 項　23 項 a/b/c の請求が否定された場合、当該個人はその拒否の理由が示され、かつその拒否を争い得えなければならない。

③個人情報の目的外利用の防止に関する規定

・18 項に収集目的の原則、19 項に収集された個人情報は収集目的及びそれに矛盾しない又は関連する目的を履行するためだけに使用されなければならないことが定められている。
・19 項の解説によれば、加盟エコノミーに明確な法律がなくとも、虚偽による情報の収集は不公正とみなされるべきであるとされる。
・20 項にオプトイン・オプトアウトの仕組みを用意すべきことが定められている。
- 18 項：個人情報の収集は、収集目的に照らし妥当なものに限定される。そのような情報は、合法的かつ公正な方法であるとともに、可能な場合には関連する個人に通知し、又は同意を得た上で取得しなければならない。
- 19 項：収集された個人情報は、収集目的及びそれに矛盾しない又は関連する目的を履行するためだけに使用されなければならない。ただし、以下の場合はその例外である。
  a）収集された個人情報の当人の承諾を受けた場合
  b）個人により求められたサービス又は製品を提供する必要がある場合
  c）法律又は他の正当な手段の権限、法的効力を有する声明及び宣言による場合
- 20 項：情報の収集・利用・公開にあたって、個人に対して選択権を付与する仕組みが用意されるべきである。

④個人情報の取得元の開示に関する規定

・APEC フレームワークには、個人情報の取得元の開示について特段の規定はない。

⑤小規模事業者の取扱い

・10 項（個人情報管理者）には、小規模事業者に関する例外的取扱いは存在しない。
・「個人情報管理者」には別の個人又は組織により指示された機能を実践する個人又は組織は含まれない。また、自身の個人、家族又は家計に関する事柄と関連する個人情報を収集、保持、取扱い、又は利用する個人も含まれない、とされる。

⑥個人情報の利用停止・消去に関する規定

・23 項 c)。「可能かつ適切であれば」情報の修正、補完、改訂、消去についての権利が認められるべき、とされる。
・個人からの請求が拒否された場合にはその理由が明らかにされるべき（25 項）とされる。

⑦国際的な情報移転に関する規定

・APEC フレームワークは、APEC 域内において、個人情報に関する一環的な取組が必要との認識から制定されたものである。加盟エコノミー間のデータの移転を前提とし、「APEC 加盟エコノミーにおけるデータの収集、アクセス、使用、又は処理を行う国際組織が、組織内での個人情報への国際的なアクセス及び使用のために均一のアプローチを提示・実行できるようにすること」等の認識に基づいて定められている。

・26 項には、個人情報を第三者に提供する場合、「国内・国外を問わず」フレームワークの諸原則に即して保護するための手続を設けなければならない、とされる。

・ANNEX1 には、国際的な情報移転に関してのガイダンスが定められるべきことが述べられている。

・26 項　個人情報管理者は、個人情報を第三者に提供する場合、国内・国外を問わず、個人から同意を得て、又は提供を受けた個人又は組織が当該個人情報を本フレームワークの諸原則に則って保護することを確認できる合理的な手続を踏まなければならない。

⑧第三者機関に関する規定

・APEC フレームワークでは、第三者機関については特段の規定はない。

・14 項の解説では、損害防止のための適切な措置として、制度の実施機構（enforcement mechanisms）を整備すべきと述べられている。

⑨死者に関する個人情報の保護

・APEC フレームワークには、死者の情報については特段の記述はない。

⑩直接処罰等の実効性担保に関する規定

・APEC プライバシーフレームワークでは、罰則については規定されていない。

・38 項において、加盟エコノミーでの適用の際に、適切な救済の制度化も含むべき、と述べられている。

・14 項の解説において、加盟エコノミーは損害防止のための適切な措置として、制度の実施機構（enforcement mechanisms）を整備すべき、とされる。

⑪その他、特に留意すべき重要事項（今後の取組の予定等）

・27 項で言及するガイダンス（A Guidance For Domestic Implementation）の内容は次のとおり。

Ⅰ.個人情報保護の利潤の最大化（28～30 項）。

Ⅱ.APEC フレームワークの実行化（31～34 項）

Ⅲ.国内のプライバシー保護の教育と広報（35, 36 項）

Ⅳ.官民セクターの協力（37 項）

Ⅴ.プライバシー保護違反があった場合の適切な救済について（38 項）

Ⅵ.APEC フレームワークの適用状況についての APEC への報告（39 項）

・2005 年以降、APEC の ECSG（電子商取引運営グループ/Electronic Commerce Steering Group）は、APEC フレームワークの域内諸国での適用のためのアシスタントセミナー（技術支援会議）を開催し、域内諸国の多種多様な実情を考慮しつつ、①各国における APEC フレームワークの適用、②越境的なプライバシールールの構築、③情報共有や調査・執行の越境協力に向けた検討等を行っている。また、ECSG のデータ・プライバシー・サブグループの会合では、プライバシー影響評価（Privacy Impact Assessment/PIAs）について検討が行われ、加盟エコノミー間での理解と活用を進めるため、共同実施の可能性が表明されている。