iii　ドイツ

１．個人情報保護法制について

（１）個人情報保護法制の概要

①法制の歴史

ア)ドイツにおける個人情報保護の法制化のもっとも大きな要因は、他の比較的早くから個人情報保護法制を有しているヨーロッパ諸国と同様、1960 年代に進展した情報化、言い換えればコンピュータの発達である。簡単に言えば、コンピュータという情報処理の武器が登場したが、再び独裁者あるいは国家権力が市民の権利を脅かすことがないように、個人情報保護法制を構築する必要があるというものである。個人情報保護法制の狙いは、国家権力から国民を保護することにあったと言える。

イ)このような考え方を受けて、連邦制の国家であるドイツでは、ヘッセン州が早くも 1969 年に世界ではじめての個人情報保護法を制定した。そして、1977 年には連邦政府が個人情報保護法を制定し、翌 1978 年から施行された。施行当初はわが国と同様の混乱があった[1]。

ウ)その後、1983 年 12 月に連邦憲法裁判所によりいわゆる国際調査判決[2]が出され、これがドイツの個人情報保護法制の分岐点になったと言われている。すなわち、この判決は「情報上の自己決定権」（日米で自己情報コントロール権と言われているものとほぼ同内容）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のである。その影響は極めて大きく、一方では、1990 年の個人情報保護法の改正につながり、他方では、多くの個別法（とくに治安、社会保障関係）の改正を促すこととなった。

エ)さらに、1995 年の EU 指令を受けて、ドイツは、2001 年、指令の水準に合わせた改正を行っている[3]。これは、メディアとの確執もあり、本来の国内法化の期限より３年遅れたものであった。

オ)そして近時の小改正として、2005 年 11 月末に成立した大連立政権（キリスト教民主同盟・キリスト教社会同盟と民主党）が、2006 年８月から施行された「とくに中規模企業経営における官僚的障壁を除くための第一次法」（７a)の中で、小規模事業者及び自営業者に対して、個人データを自動処理するに際しての監督官庁への届出義務も内部の個人情報保護責任者の設置も除外した。

カ)最新の立法状況としてあげるべきは、2008 年 7 月 30 日に新たな連邦データ保護法改正案が閣議決定されたこと、及び、2008 年 12 月 10 日に「データ保護監査の規律及びデータ保護法の改正のための法律」[4]が閣議決定されたことである。前者は、個人信用情報に関するもので、個人信用調査会社へのデータの提供（28a 条）及びいわゆるスコーリング（28b 条）についての規律の新設、当事者の開示請求権の強化（６条、６a 条、34 条）を意図するものであり、後者は、データ保護監査の規律のための個別法を制定し（データ保護監査に関する９a 条は削除)、28 条（非公的機関等の自己目的のためのデータ収集、処理及び利用)、29 条（提供目的でする業務上のデータの収集及び蓄積）等を改正するものである。後者には、2008 年のデータスキャンダルと呼ばれる、ドイツテレコム等の民間部門で相次いだ不祥事が影響しているようである（３．その他の動向参照)。

②個人情報保護法の国内法体系上の位置づけ

ア)連邦個人情報保護法は、公的部門と民間部門を包括的に規制している。

イ)個別法として 40 本近い法律[5]が存在する。その中には、国勢調査判決以降見直しを受けているものが多い。とくに治安関係、社会保障関係（詳細である）は従来行政規則レベルで対応していたものが法令のレベルになっているという特徴がある。また、近年では、インターネット対応といわれる通信役務個人情報保護法（1997 年）及びテレコム法（2004 年）なども個人情報保護の個別法として重要視されている。

ウ)情報公開法制との関係でドイツの特色としてあげることのできるのは次の点である。すなわち、ドイツでは個人情報保護法制が先行し、EU 諸国の個人情報保護法制のあり方に影響を与えるほどの議論の蓄積があるのに対し、連邦のレベルでの一般的情報公開法はようやく昨年 2005 年に成立し、2006 年１月１日から施行されている。これを、個人情報を保護する思想が情報の自由、情報の流通の思想（例えば、北欧諸国、アメリカ合衆国）よりも優位にあったとみることもできよう。

エ)国際文書との関係では、ドイツを含めヨーロッパの法制は、1981 年の個人データの自動処理の際の個人の保護に関する条約及び 1995 年の EU 指令を規準として構成されているという点が重要である。ドイツの実務家からの意見聴取でも、OECD 理事会勧告（1980 年）よりもヨーロッパ条約の方を重視しているとの回答を得ている。また、EU 指令は 81 年の条約よりもさらにレベルが高くなっていることに注意する必要がある。

③法制の特色

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

イ)2001 年法は、EU 指令転換法（EU 指令の国内法化）であるが、その主たる改正点としては、公的部門・民間部門を問わず、ⅰ）データ処置システムの選択及び構築に際してのデータ回避・データ倹約の原則、匿名化・仮名化優先の原則が採用されたこと（３a 条)、ⅱ）本人の同意の内容と手続が詳細に定められたこと（４a 条)、ⅲ）個人データの第三国等への提供の要件が定められたこと（４ｂ条)、ⅳ）データ保護の責任者を設置と自動処理の届出及びその免除の要件が定められたこと（４d 条、４e 条、４f 条)、ⅴ）ヴィデオ監視等についての明文の規定が置かれたこと（６a 条)、ⅵ）センシティヴデータの考え方が採用されたこと（３条９項、ただし、公的部門と民間部門で取扱いの要件が異なる）等をあげることができる。

わが国の過剰反応問題との関係で言えば、第１に、EU 指令（第３条２項）を受けて、民間部門については「データの収集、処理又は利用が、もっぱら個人的なあるいは家庭的な活動のために行われる場合を除く」こととされている。例えば、家庭の PC に私的なアドレスや誕生日データを入力する場合が典型例であるとされる。国家による個人情報保護が必要とされるのは、第三者の基本権の保護と抵触するようなデータ処理の場合であって、全くの個人的な利用の場合にはその必要がないからである。逆に、広域ネットワークの一部であるメールボックスに、第三者の情報を蓄積する場合のように、私人が公的な情報の流れの中に身を置いた場合にはこの要件を充たさなくなるとされる。

第２に、目的外利用・第三者提供規定について以下のような特徴がある。国勢調査判決を受けて大改正がなされた 1990 年法で、公的部門、民間部門の双方について、目的外利用・第三者提供に関する規律が詳細化されたが、これが 2001 年改正法ではさらに徹底されている。公的機関から公的機関への個人データの提供、公的機関から非公的機関への個人データ提供、非公的機関から他の（公的・非公的）機関への提供の関連条文は、わが国の問題を考えるのにも参考になる。

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

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

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

漏洩事故等については、行政機関も民間企業もこれを連邦や州のデータ保護当局に届け出る法的義務はない。しかし、公的部門、民間部門に置かれたデータ保護担当者が事故情報、政府の方針、新しい事例等について、常にその属する組織に情報を提供するというシステムを採用している。

④法制の運用上の特色

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

なお、ドイツにおいては、開示請求や不服申立てについての統計は、連邦レベルでも州レベルでも存在しない。聴き取り調査によれば、連邦レベルで E-Mail による照会も含めて年間 3000 件程度[6]（連邦監察官事務所）の苦情・不服があるとのことである。

また、現行法では、漏洩事故等を行政機関が連邦データ保護・情報自由監察官に、民間企業等が監督官庁に届ける義務はない。

イ)公的部門の法の運用については、連邦監察官の役割が大きい。日常の業務において、関係機関が連邦監察官に法の解釈運用について事前の相談をすることは多い。監察官は、わが国における行政監察のような形で行政機関の個人情報保護の体制・運用について監察を行う。この場合の監察官の権限は比較的強く、質問検査、書類閲覧、立入検査などの権利を与えられている（24 条)。担当者に対する立入拒否がないわけではないという問題が指摘

されているが、その場合には、監察官自らが電話等で直接のやりとりをすることになる。相手方行政機関の違法、不当な処理等を確認したら異議を唱え、相手方の見解の表明を求めるということになる（25 条)。場合によっては、連邦監察官には改善勧告を行う（26 条３項)。勧告に従わなければ、活動報告書の中で公表し（26 条１項)、連邦議会における質問の対象となる可能性を探る。議会質問があれば、所管大臣に答弁の必要が生じることになるからである。

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

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

エ)民間部門については、わが国の認定個人情報保護団体のような制度はないが、個人情報保護のコンサルタント業とでもいうべき幾つかの民間団体が存在する。その代表的なものが GDD（Gesellschaft fÜür Datenschutz und Datensicherung）と呼ばれる、1977 年、ドイツ連邦データ保護法の成立とともに設立された団体である。GDD は、EU 委員会・連邦政府・州政府等の活動情報を収集し、これを会報（かなり専門的な問題や具体的事例が取り上げられている）を通じて会員に提供し、また、個人情報保護法上生ずる問題について講習会、研修会を実施している。民間部門において監督官庁の業務を補完する存在であると言ってよいと思われる。

なお、民間部門について、シュレスヴィッヒ・ホルシュタイン州が、国家（州）によるマーク制度の試みをはじめているが、他の州は現在のところあまり関心を寄せていないようである。その結果、現状では、この制度はドイツ・ヨーロッパ単位で活動する企業にとっては魅力のないものとなっている。しかしながら、前述１－（１）－①－カ）の「データ保護監査の規律及びデータ保護法の改正のための法律」によれば、ドイツでも、データ保護シール（わが国で言えばマーク）を民間事業者に付与する制度が創設されることになっている。法律が成立すれば、この制度は 2010 年７月１日から運用される予定である。これにより、ドイツの自主規制制度も新たな局面を迎えることになると思われる。

（２）個別の検討課題

①いわゆる「過剰反応」（誤解）に対応した第三者提供制限の例外事由

ドイツでもいわゆる「過剰反応」は生じている。過剰反応事例は、1977 年の制定時と 1983 年の国勢調査判決の直後に多くみられる。国民の個人情報保護意識（プライバシー意識）が高まったのは、法制定時よりもむしろ国勢調査判決によってのようである。しかしながら、過剰反応によって第三者提供の例外事由規定が影響を受けたという事実はない。

②自治会や同窓会等の取扱い

わが国でいう自治会に相当するものが存在するかどうかは不明である[7]。同窓会については、大学（ドイツの大学は基本的に国立（正確に言えば州立）である）の同窓会等がある。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。

各州の個人情報保護法の問題となるが、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）の取扱いは大要次のようなものである。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。大学の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。ベルリンフンボルト大学の例では、データベースは 2001 年に構築された。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、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）とのことである。

③「個人情報」の定義

個人データ（personenbezogene Daten）とは、特定の又は特定されうる自然人（本人）の人的又は物的状況に関する個々の情報（Einzelangabaen）をいう（３条１項)。

④センシティブ情報に関する規定

ｉ）「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)。

ⅱ）「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)。

ⅲ）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４a 条３項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)。

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

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

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

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

ⅳ）「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なわれる場合に、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)。

ⅴ）「特別な種類の個人データ」は、上記(ⅲ)及び(ⅳ)以外の目的のためには、28 条６項の１から４まで又は上記(ⅳ)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)。

ⅵ）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(ⅱ)の要件のもとでのみ許される（28 条９項)。

ⅶ）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(ⅲ)から(ⅵ)までが準用される（30 条５項)。

ⅷ）「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)。

なお、センシティブ情報という概念を自国法の概念に導入することについては、95 年 EU 指令の国内法化の過程で議論のあったところである。

⑤小規模事業者の取扱い

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)。１-（１）-⑤で述べた 2006 年の法改正により、人数要件が４人から９人に緩和されたものである。さらに、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)。また、2006 年の法改正により、データ保護担当者を設置が困難な小規模事業者は、事業主自身が担当者となることが許されるようになっている。

⑥メディアとの関係

ｉ）現行法に至る経緯

ア)ドイツのメディア特権に関する規定は、既に 1977 年法に定められている（１条３項）が、これが 1990 年法 41 条（メディアによる個人情報の利用）に受け継がれ、さらに、EU 指令９条の国内法化を通じ、現行の 2001 年法となったものである。

90 年法の 41 条１項は、「個人データが、報道関係又は映画関係の企業又は補助企業、若しくは放送関係の補助企業によって、もっぱら自己の報道・編集上の目的で、処理又は利用される場合、この法律の５条及び９条のみが適用される」と定めていた。

イ)現行法の政府草案作成過程での議論

1999 年７月６日に公表された内務省の草案では、41 条は、「メディアによる個人データの収集、処理及び利用」の表題の下、「州は、立法において、報道関係の企業もしくは補助企業、又は放送関係もしくは映画関係の補助企業による、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、処理及び利用に対して、４f 条、４g 条、５条、６a 条、７条、９条、31 条、38a 条、41 条２項及び３項、ならびに 44 条１項第５号及び条２項の規定に準じる規律が適用されることを定めなければならない」となっていた。

メディア分野での連邦と州のデータ保護の規律の統一性を図るために連邦立法による大綱法としたこと、収集の段階からの規制であること、EU 指令の要請に忠実に、履行義務及

び制裁規定（７条の立証責任を伴う損害賠償、44 条の過料規定）を 41 条の規律に含めたこと、38a 条の行為規範の要請、⑤表現の自由と情報の自己決定権の調整規定として、４f 条・４g（企業のデータ保護担当者）、６a 条（自動化された決定）、41 条２項及び３項（反論、開示･訂正権）、31 条（特別の目的拘束）が適用されることが特色である。

これは、EU 指令に忠実な転換であり政府としては従前の方針を変更したわけではないという見方もできるが、メディア側にとっては、現行法の規制と比較した場合、かなりの規制の強化であるといってよい。そのため、これが明らかになると、メディアの側とくにプレスが激しく反発をした。

ウ）ドイツ報道評議会の反論　右の草案が公表されて間もない 1999 年８月 31 日に、ドイツ報道評議会[8]はこれに対する見解（20 頁の詳細な逐条的反論書）を示した。

そこでは、州と連邦の管轄の問題とともに、41 条の規定に対して強い批判がなされている。これを要約すれば、①31 条の特別の目的拘束には問題はないし、秩序罰を編集上の作業には及ぼしていないことを歓迎するが、②その他の規定については、収集概念の採用及びその関連規定への拡張、編集上のデータ保護担当者の任命に関する規定等を削除すべきことを求める、③また、これまで連邦法上の放送局（ドイッチェ・ヴェレ）に対してのみ課せられていた反論の蓄積、開示訂正権の承認も認められない、④行為規範については自主規制の観点からこれを歓迎するが、規範の策定を監督官庁が審査することには反対である、というものである。とくに、②の編集上のデータ保護担当者（ドイツの個人情報保護法の特徴である企業内データ保護担当者）の設置は、負担の大きさとともに、データ保護担当者の罷免要求を通じての監督官庁の関与（４f 条３項）との関係で警戒を呼んだようである。

エ）議論の背景　このように議論が対立した背景の一因として、ドイツ報道協議会のこれまでの活動対する評価が割れていることを挙げることができる。すなわち、報道の自由と情報の自己決定権の調整をメディアの自主規制に委ねるとしても、報道協議会は「歯のない虎」と揶揄されるように制裁を担保する手段のない自主規制であること（これはスウェーデンと異なる点として強調される）、また、もっとも強い内部的制裁である「公開の叱責（öffentliche Rügen；叱責を媒体上に掲載する倫理的義務がある）」を掲載しない新聞や雑誌が存在[9]することに対する消極的評価が存在するのである。そのため、自主規制は、発行者が司法手続を回避するための制度で公衆利益を考えて作った制度ではないとの批判もあるところである。

いずれにせよ、このような立法当局とプレスの議論の対立は政治問題化し、最終案の確定も数ヶ月遅れたのである。

ⅱ）現行法

紆余曲折を経て成立した現行法の 41 条は以下のとおりである。

【第 41 条】メディアによる個人データの収集､処理及び利用

（1）州は、立法において、報道関係の企業もしくは補助企業による、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､処理及び利用に対して、これに関連する第７条に相当する責任規定を含む、第５条、第９条、第 38ａ条の規定に相当する規律が適用されることを定めなければならない。

（2）連邦法上の放送局による個人データの報道･編集上の収集、処理又は利用が、当事者の反論の表明にいたる場合には、この反論が蓄積データに含められ、かつ当該データ自体と同じ期間保存されなければならない。

（3）何人も、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、報道の基礎となった自己に関して蓄積されたデータに関して開示を要求することができる。当該データから、編集部分の、記事、資料及び報告の執筆者、寄稿者又は情報提供者個人を推し量ることができる場合に限り、開示は拒否できる。当事者は、不正確なデータの訂正を要求することができる。

（4）その他、連邦法上の放送局には、この法律について、５条、７条、９条、及び 38ａ条が適用される。行政上の事務が問題となっている場合には、24 条から 26 条に代わって、42 条が適用される。

すなわち、90 法に、①７条の責任（ただし、５条と９条違反に限定)、②38a 条の行為規範が加わったという形になったのである。プレスの要求を容れた形での妥協で、自主規制の重視への方向転換したといってよい。ただし、行為規範は 41 条という法的枠組み規定の具体化であるということになる。これを受けて報道協議会は、情報主体に、プレス内部のデータの流れを審査する可能性を開くような、行動原則、勧告、苦情手続を有する行為規範を策定しなければならない。

ⅲ）現状

以上に見てきたように、ドイツの個人情報保護法の改正はプレスの優位を認める方向で決着が付いたといえる。独自の監察官の存在を前提として、賠償、秘密の保持、セキュリティなど最低の枠組みが存在する中に、当該法的枠組みの一環としての自主規制が加わるという形になった。もっとも、このことがプレスを法的枠組みの外に完全に置いたということではない。メディアとの関係は、５条、７条、９条、38a 条を基準として、各州の立法者に委ねられたことになる[10]。また、報道評議会に対して、これまでとは違った実効性ある取組を要求しているとみることもできる。

⑦個人情報の目的外利用の防止措置

公的部門については、法 14 条が一般的な前提要件を定め、15 条が公的機関への、16 条が非公的機関への提供について定めている。目的外利用が詳細に定められていること、特別な種類のデータ（いわゆるセンシティブデータ）についての過重要件があること、が公的部門から公的部門、公的部門から民間部門への提供の特徴である。

わが国では個人情報保護法が規律する民間部門についても、以下のような詳細な定めがある。

【第 28 条】　自己の目的のためのデータ収集､処理及び利用

（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、変更もしくは提供し、又はそれを利用することは、以下の各号に掲げる場合に許される。

1　それが本人との契約関係も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、かつ処理もしくは利用させないことについての本人の保護に値する利益が優越すると推定させる理由が存在しない場合

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、処理もしくは利用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処理され､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）他の目的のためには、個人データは第 1 項第 1 文第 2 号及び第 3 号の要件のもとでのみ提供され､又は利用することが許される。

（3）他の目的のための提供又は利用は､以下の各号に定める場合にも許される。

1　第三者の正当な利益を守るために必要な場合、又は、

2　国家の､及び公共の安全にとっての危険の防止ならびに犯罪行為の追及のために必要な場合、又は、

3　宣伝又は市場もしくは世論調査の目的のため、人的集団の構成員に関して、以下に限定された項目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存在しない場合

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

4　研究施設の利益のために、学術研究の実施のために必要な場合、研究計画の実施に

ついての学術上の利益が、目的変更の排除に対する本人の利益に著しく優越し、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とき

第１文第３号の場合、契約関係又は契約類似の信頼関係の目的の範囲内で蓄積された以下の項目に関連したデータが提供されることとなる場合には、提供をさせないことについての保護に値する利益が存在すると推定される。

１　犯罪行為

２　秩序違反ならびに

３　使用者によって提供がなされる場合に労働法上の法律関係

（４）本人が、責任機関に、宣伝又は市場もしくは世論調査の目的のための当該本人の情報の利用又は提供について異議を申し立てる場合、この目的のための利用又は提供は許されない。本人は、宣伝又は市場もしくは世論調査の目的のための請求については、責任機関、データの出所、及び第１文に基づく反論権について知らされるものとする。請求者が、本人の知らない機関に蓄積されている本人の個人データを利用するときは、請求者は、本人が当該データの出所について知ることができるようしなければならない。本人が、第三項に従ってデータが提供された第三者に、宣伝又は市場もしくは世論調査の目的のための利用又は提供について異議を申し立てる場合、第三者はこの目的のためのデータを封鎖しなければならない。

（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処理し又は利用することが許される。他の目的のための処理又は利用は、非公的機関は第２項及び第３項の要件のもとでのみ、ならびに公的機関は、第 14 条第２項の要件のもとでのみ許される。提供機関は、第三者にそのことを告知しなければならない。

（６）自己の業務目的のための、特別な種類の個人データ（第３条９項）の収集、処理及び利用は、本人が第４ａ条第３項により同意しないときは、以下の各号の場合に許される

１　本人又は第三者の死活的な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、処理又は利用を排除することにおる本人の保護に値する利益が優越するということを推定させる根拠が存しない場合、又は

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、処理又は利用を排除することによる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

（７）特別な種類の個人データ（第３条９項）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行政のため

に必要であり、かつ、これらのデータの処理が、医師又はその他これと同様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。第１文に挙げられた目的のためのデータの処理及び利用は、第１文に挙げられた者に適用される守秘義務規定に従う。

第一文に挙げられた目的のために、健康に関するデータが、その職務の遂行が病気の確認、治癒若しくは鎮静、又は薬の製造若しくは販売をもたらすが、刑法 203 条１項及び３項に挙げられている職業ではない職業の関係者によって収集、処理又は利用される場合には、これらは、医師自らがこれについて権限を有するであろう場合と同一の条件の下でのみ許される。

（８）特別な種類の個人データ（第３条９項）は、他の目的のためには、第６項第１号から第４号までの要件の下でのみ提供、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犯罪行為の追及のために著しい重要性を有する場合のために必要な場合にも許される。

（９）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（第３条９項）の収集、処理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、第４ａ条第３項の要件のもとでのみ許される。第３項第２号が準用される。

【第 29 条】提供目的でする業務上のデータの収集及び蓄積

（１）提供を目的とする、個人データの業務上の収集、蓄積もしくは変更、特にこれが興信所、名簿取引、又は市場及び世論調査に役立つ場合は、以下の各号に掲げる場合に許される。

１　収集、蓄積又は変更を排除することに対する保護に値する利益を本人が有すると推定する理由が存在しない場合、又は、

２　データが、一般にアクセス可能な情報源から入手可能なものであり、又は責任機関がそれを公表することにつき許されている場合、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先する場合はこの限りでない。第 28 条第１項第２文が適用されるものとする。

（２）第一項による目的の範囲内での提供は、以下の場合に許される。

１ａ）　データが提供される第三者が、当該データを知ることについて正当な利益を疎明する場合、又は、

ｂ）　第28条第３項第３号に従って名簿の形でもしくはその他の方法でまとめられた、宣伝又は市場もしくは世論調査の目的で提供されるとされるデータが取り扱われる場合で、かつ、

２　提供を排除することについての保護に値する利益を本人が有していると推定する理

由が存しない場合

第 28 条第 3 項第 2 文は準用される。第 1 号 a に従った提供の場合、正当な利益の存在の根拠及びその疎明の方法は、提供機関によって記録されるものとする。自動化された呼出処理方式で提供される場合、記録義務はデータが提供される第三者に課される。

（3）本人の反対の意思が、基礎となる電子的又は印刷された記録ないし登録簿から明白な場合、電子的な又は印刷された住所録､電話番号簿、業種別名簿若しくは同様の記録簿への個人情報の採録は行われてはならない。データの受領者は、受け取りの際に、電子的又は印刷された記録簿ないし登録簿からの証明が、記録又は登録簿に載せられることを保証しなければならない。

（4）提供データの処理又は利用には、第 28 条第 4 項及び第 5 項が準用される。

（5）第 28 条第 6 項から第 9 項までが準用される。

【第 30 条】匿名化された形での提供目的のためにする業務上のデータの収集及び蓄積

（1）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、特定のもしくは特定しうる自然人の人的もしくは物的関係に関する個々の記載事項を関連づける指標は分離して蓄積されなければならない。この指標は、これが蓄積の目的を遂行するため又は学術目的のために必要である限りでのみ、個々の記載事項と結合することが許される。

（2）個人データの変更は次の各号に掲げる場合に許される。

1　変更の排除について保護に値する利益を本人が有していると推定する理由が存在しない場合、又は、

2　変更の排除について、本人の保護に値する利益が明らかに優越しない限りで、データが一般にアクセス可能が情報源から入手可能なものであるか、又は責任機関がそれを公表することを許されている場合

（3）個人データは、その蓄積が許されないものである場合、消去されなければならない。

（4）第 29 条は適用されない。

（5）第 28 条第 6 項から第 9 項までが準用される。

【第 31 条】　特別の目的拘束

個人データが、もっぱらデータ保護の監督、データセキュリティ、又はデータ処理施設の適正な運営を確保する目的で蓄積される場合、個人データはこれらの目的のためにだけ用いられることが許される。

コンピュータ処理データベースの規制を主眼に、利用と保護のバランスについて詳細に規律しているのがドイツ法の特色であるが、既に述べたように、2008 年 12 月に閣議決定された法案（注 3 参照）では、28 条及び 29 条は権利保護の方向での規制強化が図られることが予定されている。法案の成否は予断を許さない状況にあるが、要点のみ触れておくと、

第１に上記28条３項３号のリスト特権は廃止され個人データの提供についての本人の同意義務が強化されること、第２に個人情報の紛失（漏洩）の場合に届出義務が課せられたこと、第３に過料の額が引き上げられたこと、第４に企業におけるデータ保護管理者の権限が消費者保護の方向で拡充されたことである。

⑧市販の名簿の管理

現行の連邦データ保護法28条は、目的外利用が許される場合として、いわゆる「リスト特権」を認めているが、近時ドイツで問題となった、民間部門における不透明な名簿取引の実態に鑑みて、⑥で述べたように、マーケティングや世論調査のためのリストデータは、今後、本人の同意の下でのみ、利用・提供することができるのが原則となる。

⑨個人情報の取得元の開示に関する措置

法34条が、自己に関して蓄積されたデータの情報源に関するデータについての開示請求権を認めている。

⑩個人情報の利用停止・消去に関する措置

法35条が詳細に定めている。

⑪国際的な情報移転に関する規定

法４ｂ条（個人データの外国並びに超国家的又は国家的機関への提供）が詳細に定めている。

⑫EU データ保護指令に対する対応状況

2001年の改正法で対応済みである。

⑬死者に関する個人情報の保護

連邦データ保護法上は解釈の問題となっている。有力なのは、カルテ、統計、税法上の守秘義務のように個別法の規定で死者の個人データが保護されている場合があるが、連邦データ保護法のような一般法には拡張できない、とする考え方である。ただし、州法の中に公的部門について規定する例がある。（ベルリン等）

⑭直接処罰等の実効性担保の措置

法 43 条、44 条が直罰規定として存在する。なお、2008 年改正法案では、過料の上限は現行の 25,000 ユーロから 300,000 ユーロに引き上げられることが予定されている。

２．第三者機関について～民間部門

（１）第三者機関の実態

①制度の概要

非公的機関の監督官庁については法 38 条が定める。

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

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

監督官庁は、届出義務のある自動処理（４d 条）の登録簿を作成管理する。何人も、この登録簿を閲覧することができる（38 条２項）。

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

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

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

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

2006 年当時、ドイツに対しては、民間部門（非公的機関と公法上の競争企業を併せて民間部門と呼んでいる）について、一部の州（バイエルン等ドイツ 16 州のうち半分の８つの州）で内務省の下にある監督官庁が所管している点について、EU 委員会から独立性のある

第三者機関の設置という点において、EU 指令を忠実に国内法に転換したとは言えないのではないかという批判があった。

②オフィスの実態

個人情報・情報公開監察官事務所として、ドイツの旧首都であるボンに独立のオフィスを構えている。予算規模は、2006 年度で、369 万ユーロ（日本円で約 4 億 7 千万）であり、スタッフは 70 人（ただし、情報公開・個人情報保護監察官事務所全体である)。このうち執行部門担当職員数は 56 人である。

③リソース確保に関する現状と問題点

スタッフには専門知識を有する専門家が多い。事務所での聴取りによれば、スタッフ数は十分ではないということであった。

④広報の実態

法の実効性を高める試みとして、データ保護監察官は、次のような活動を行なっている。ⅰ）各種の冊子を市民向けに発行している。各州もトピックごとに同種の冊子を発行するなどして啓蒙活動に努めている。ⅱ）ヨーロッパの先行国に共通のことであるが、HP の充実に努めている。ⅲ）Newsletter を発行し、外国をはじめ希望者に PDF ファイル等の形で発送している。ⅳ）個人情報保護意識を国民の間に醸成すべく、時事問題に対する見解の発表を頻繁に行なっている。

（２）第三者機関の活動状況

①第三者機関の国内での活動状況

個人情報保護上重要と考えられる問題が生じたとき、あるいは個人情報保護に係わる立法作業が行なわれるときには、かならず監察官が意見を表明する。連邦の各州との間で定期的な会合がもたれている。民間企業からの相談業務も多い。

②第三者機関の国際的な活動状況

EU 諸国の場合、コミッショナー会議が定期的に開催されており、そこで国際的な問題が議論される。と同時に、EU 指令 29 条の作業部会による情報交換が重要な役割を果たして

いる。ドイツはフランスとともに先導的な役割を果たしている。

③教育・啓蒙、普及・広報活動等の現状

（１）④広報の実態で述べたような活動を行なっている。州レベルでは、シュレスヴィッヒ・ホルシュタイン州が、個人情報保護の研修（データ保護アカデミィという名前で催される）として、企業や市民向けの講座を有料で提供している。

④第三者機関と外部機関等との関係

特に目立った民間部門との人事交流、民間企業への業務委託等はないようである[11]。なお、個人情報保護のセキュリティの（安全管理措置）の側面、とくに IT 技術に関しては、１－（１）－③－オ）で触れたように、Bundesamt für Sicherheit in der Informationstechnik (BSI)（連邦情報技術庁）が大きな役割を果たしている。

（３）苦情・紛争処理の実態

①苦情・紛争処理の概況

連邦レベルで E-Mail による照会も含めて年間 3,000 件程度（連邦監察官事務所）の苦情・不服があるとのことである。なお、訴訟を提起するのは個人の権利であるので、苦情処理とは関係なく訴訟は提起されている。

②具体的ケース

ここでは、2008 年５月に発覚し、現在もなおドイツを揺るがしている、「個人情報保護スキャンダル」と呼ばれる一連の事件を紹介しておく。2008 年７月 30 日、個人信用情報機関等への個人情報の提供及びその後の利用を透明化することを眼目とする個人情報保護法改正案が閣議決定されたのであるが、改正案が成る直前の同年５月末に、シュピーゲル紙によって、ドイツテレコムが管理者や監査人の通話記録を内部監査において利用していたということが報じられていた。これが「テレコム事件」の発端である。

内務大臣自らテレコム会長と会談し、テレコムが自主的な規制に努める等の結論が出されたのであるが、その直後に、2006 年に、約 1,700 万人分の携帯電話所有者の個人情報がテレコムグループのＴ－モバイルから流出していたことが発覚した。中には著名人の情報も含まれていると報じられた。

同年８月には、連邦中央消費者保護連盟（Verbraucherzentrale Bundesverband）が、

600 万人分の個人情報（400 万人分は住所氏名のみならず口座情報が付いている）がブラックマーケットで取り引きされ、電話による勧誘等に利用されていると報じた。

そして、12 月には、週刊誌（Wirtschaftswoche：週間経済）が 2100 万人分の口座情報等がブラックマーケットで取り引きされていると報じた。同じく、12 月に、ベルリン州立銀行がクレジットカード情報を大量に紛失した。

このような状況の中で、2008 年 12 月のさらなる個人情報保護改正法が閣議決定されたのである。

一連の事件は、2009 年になっても続き、2009 年 1 月には、ドイツ連邦鉄道が不正防止のためという理由で、約 22 万人の従業者の個人情報（住所、氏名、身分証番号、電話番号、配偶者の氏名、口座情報、税情報等）を外部の興信所に提供していたことが報じられた。この事件によって、個別法としての被用者個人情報保護法の必要性が話題に上っている。

この間、連邦データ保護監察官は、終始、積極的に意見を表明している。

３．その他の動向

（１）新たな課題への取組[12]

①RFID

RFID については、個人識別の可能性、その不可視性、（遠隔地からも）個人のプロファイリングの可能性（危険性）という観点から、個人情報保護の問題であると認識されている。すでに、2006 年に EU 委員会が RFID の可能性と危険性の問題を取り上げたことから、ドイツでも 2006 年 10 月の第 72 回連邦・州データ保護監察官会議で決議がなされている。決議のポイントは、民間事業者に、消費者利益の観点からの拘束力ある自主規制ルールを定めることを求めていることである。ルールに盛り込まれるべき考慮事項は、透明性（すべての当事者に、チップを利用していること、利用目的、内容について情報が与えられること）、表示義務、秘密裡のプロファイリングの禁止、無権限者による読取りの禁止、利用目的を達した場合のチップの非活性化、である。

②ビデオ監視

ドイツでは、ビデオ監視は、今日、我々の生活の一部となってしまったという事実認識の下、議論がされている。警察法、州の集会法などにこれを正面から規定するものがある。個人情報保護法としては、連邦データ保護法６ｂ条に規定がある。

【６b 条】光学的電子的設備による、公然と入り得る空間の監視
光学的電子的設備による公然と入り得る空間の監視(ビデオ監視)は、これが、

１．任務の遂行のため、
２．住居権の行使のため、
３．具体的に確定された目的のために正当な利益を行使するために、
必要であり、かつ、本人の保護に値する利益が優越するとの根拠がない場合に限り、許される。

（２）監視の状況及び責任機関が、適切な措置により、認識可能にならねばならない。
（３）第１項により収集されたデータの処理及び利用は、当該目的の達成のためにこれが必要であり、かつ、本人の保護に値する利益が優越するとの根拠がない場合に限り、許される。
（４）ビデオ監視により収集された特定の者のデータが分類される場合には、この者に対し、第 19a 条及び第 33 条に準じて、処理及び利用について通知がされなければならない。

（５）データが、目的の達成のために必要でないか、又は本人の保護に値する利益が、更なる蓄積と矛盾する場合は、データは遅滞なく消去されなければならない。

ドイツでは、収集された個人データの安全管理措置（法９条）の重要性が指摘されている。

③生体認証

多様な（指紋、光彩、顔等）な生体認証が利用されている。個人情報保護の観点からは、認識の安定性に応じた手続、濫用を禁止する組織的・技術的措置、全体としての目的拘束及び比例原則の観点からの検討を経ることが必要である、とされている。

（２）公共の安全（テロリズム）への対応

公的部門の話であるが、警察・法務分野での国際協力の強化は著しい。自由・安全・権利の３本柱（ハーグ・プログラム）が推進役である。オイロポール、シェンゲン条約、SIS Ⅱ、税関情報システム等の拡張・充実政策がとられている。ビザ情報システムも稼働間近である。

９．11 事件以降、アメリカと EU 諸国のデータ保護当局との間に緊張関係がある。PNR 協定事件（当初の情報：【PNR 記録コード、予約日、飛行予定日、名前、PNR における他の名前、住所、支払いの形態、支払住所、電話番号、当該 PNR の全旅程、複数の飛行の登録、旅行社、担当者、PNR 内でのコード割当情報、旅客の旅行上の身分、予約の分割に関する情報（＊）、Ｅメールアドレス、航空券の発行に関する情報、一般的特記事項（＊）、航空券番号、座席番号、発券日、未搭乗の履歴、荷札番号、予約なしで航空券を所持している旅客、特別なサービスの要求、委託者に関する記録、PNR 記録の変更のすべて、PNR 内の旅行者の数、座席の等級、片道切符の航空券、緊急時の APIS 情報、ATFQ-Felder（自動的料金問い合わせ）】等 34 項目）、SWIFT 事件（正式名称は Society for Worldwide Interbank Financial Telecommunication。1973 年に設立された、ベルギーのブリュッセルに本拠を置くベルギー法上の協同組合。電信による送金サービス等を行い、世界の 7800 以上の金融関係会社が接続しているという。ヨーロッパとアメリカに計算センターがある。2006 年６月末に、SWIFT の計算センターのデータへのアクセスについてアメリカの捜査機関及び財務当局との間に秘密の取り決めが存在することが、メディアによって暴露され、ヨーロッパ各国のデータ保護当局が、ヨーロッパの個人情報保護法に違反する不適法なものであると批判した事件）等が起きている。前者については、EU 当局とアメリカとの間で 2007 年７月に新たな協定が締結され、ヨーロッパ発アメリカ行きのすべての旅客機の乗客の個人情報をほぼ無制限にアメリカの関係当局が利用できることとなった。各国のデータ

保護当局はなお批判的である。後者は、今後、アメリカの当局は、ヨーロッパ内の情報の処理についてはアクセス権限を有しないということになり、各国のデータ保護当局の勝利という形で決着した。

（３）プライバシー保護団体や世論の動向について

①プライバシー保護団体の動向や見解

2008年に相次いだ漏洩等の事故に際して、連邦データ保護監察官とVerbraucherzentrale Bundesverband (vzbv)、連邦刑事公務員連合（BDK）が、個人情報保護は消費者保護であると共同声明を出している。

②プライバシー関連諸問題についての世論の動向

2008 年２月の調査（EUrobarometer）によれば、ドイツの消費者の 86%が個人情報保護の実務を信頼していないという結果（BFDI の HP による）が示されている[1][3]。

---

[1] 藤原静雄「ドイツにおける個人情報保護の実際～わが国の過剰反応問題を考える一視座」筑波大学法科大学院創設記念『融合する法律学（上)』(2006, 信山社）134～159 頁参照。
[2] 藤原静雄・鈴木庸夫「西ドイツ連邦憲法裁判所の国勢調査判決」ジュリスト 817 号 64 頁以下、同 818 号 76 頁以下。
[3] これが本稿で取り上げる現行法であるが、その翻訳として、藤原静雄「資料 改正 連邦データ保護法(2001 年５月 23 日施行)」季刊行政管理研究 99 号（2002 年）76 頁以下がある。本稿で条項の示した条文の内容については、この翻訳を参照されたい。
[4] Gesetz zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften.
[5] 連邦データ保護・情報自由監察官（BfDI）の HP には 36 本の個別法が挙げられている。
[6] 連邦監察官事務所での聴取りによる。
[7] おそらく、わが国でいう自治会的なものはなく、それに相当する機能を果たしているとすれば教会の教区ではないかと推測される。
[8] 自主規制を目的とし、スウェーデンとイギリスの新聞評議会をモデルに、1956 年、ジャーナリスト及び新聞発行者の主要な団体によって設立されている。評議会は、４つの主要団体、すなわちドイツ新聞発行者協会、ドイツ雑誌発行者協会、ドイツジャーナリスト協会、メディア労働組合の代表によって構成される。運営経費の約 55%をこの４団体が、残りの 45%は内務省の補助金で賄うが、内務省は使途について影響を行使しないとされる。72 年には内部に苦情処理委員会が設置され、73 年（96 年改訂）には、プレスコードが定められている。これは、法的枠組みではなく、プレスの職業倫理の維持を目的とする記者と発行者のためのガイドラインである。
[9] 例えば、若干旧い統計であるが、1999 年度では、15 件（456 件の苦情の申し出）が公開

の叱責に相当すると判断されたが、実際に掲載されたのは 10 件である。
[10] ブレーメンのプレス法 5 条が連邦法を基準として個人情報保護規定を置いているが、すべての州でこの規定の立法化がなされているかは不明である。
[11] 聴取りの結果であるが、統計的なものまではできなかったことをお断りしておく。
[12] これらの課題はすべて、連邦データ保護監察官第 21 次報告（2005～2006）に取り上げられている。以下の記述もそれに依拠している。
[13] なお、EU 構成国としてのドイツについては、後掲の OECD、APEC、EU の取組の項（宮下紘専任講師担当）の統計を参照。

ⅳ　アメリカ

１．個人情報保護法制について

（１）個人情報保護法制の概要

①米国の個人情報保護制度の特徴

ア）セクトラル方式

個人情報保護について、領域・業種ごとに個別法により規制し、包括的な個人情報保護法（オムニバス方式）は存在しない。

イ）公的部門

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

ウ）民間部門

民間部門については、個別法、判例法又は自主規制による規制が存在するが、自主規制・自己統制が基本である。

一部の機密性の高度な情報を扱う分野（信用情報、医療情報等）においては、問題の発生が契機となって、個別法が制定されている。

エ）州法による多様性

米国は連邦国家であるため、州法の多様性に対する個別対応が存在する。

例えば、以下の州では、独自の制度が設けられている。

・カリフォルニア州：　漏えい時の本人に対する告知義務
・ミネソタ州：　ISP の二次使用に対するユーザーによる事前承認
・ジョージア州：　個人情報を含む文書、記録媒体の廃棄禁止

②歴史的経緯

ア）伝統的プライバシー権

19 世紀後半に、伝統的プライバシー権が提唱された。

Samuel D. Warren / Louis D. Brandeis は、“The Right to Privacy”（Harvard Law Review, 1890）において、プライバシー権を「一人にしておいてもらう権利（the right to be let alone）」とした。

プライバシーの保護は、コモンローの下で発達した。

不法行為法（Torts）におけるプライバシー侵害は、以下の４点にまとめられる。（Restatement Sec. 652B, C, D, E 1970）

（ⅰ） 個人の/私的な情報の公表（Public Disclosure of Private Facts）

（ⅱ） 外界から遮断された個人の/私的な空間への侵入（Intrusion upon Seclusion）

（ⅲ） 事実誤認・虚偽情報の公表（False Right）

（ⅳ） 氏名等の盗用・不正使用（Appropriation）

イ）現代的プライバシー権

20 世紀後半になると、現代的プライバシー権が提唱された。

Alan F. Westin は、“Privacy and Freedom”（1967）において、プライバシー権を「自己に関する情報の流れをコントロールする個人の権利（individual's right to control the circulating of information relating to oneself）」（自己情報コントロール権）として、定義づけた。

ウ）プライバシー保護調査委員会報告書

1977 年 7 月 12 日付のプライバシー保護調査委員会報告書では、「情報社会における個人のプライバシー」（Personal Privacy in an Information Society）に関して、以下のプライバシー法の８原則が掲げられている。

（ⅰ） 公開の原則（Openness）

（ⅱ） 個人アクセスの原則（Individual Access）

（ⅲ） 個人参加の原則（Individual Participation）

（ⅳ） 収集制限の原則（Collection Limitation）

（ⅴ） 使用制限の原則（Use Limitation）

（ⅵ） 提供制限の原則（Disclosure Limitation）

（ⅶ） 情報管理の原則（Information Management）

（ⅷ） 責任の原則（Accountability）

③連邦法と州法

ア）連邦法と州法との関係

（ア）専占（Preemption）の法理

最高法規条項（Supremacy Clause、米国憲法６編２項）により、連邦法の州法に対する優位が定められている。

連邦法と州法とが黙示的に抵触する場合においても、専占により、連邦法が州法に優位

する。

連邦法の存在又は不存在が州法による規制を許さない場合か否かのメルクマールとして、以下の基準が挙げられる。

（ⅰ） 全国統一の規律の要否

（ⅱ） 伝統的に州の権能に属する分野か否か

（ⅲ） 連邦法の包括性・網羅性

（イ）連邦の各個別法と州法との関係

州レベルにおける個人情報保護は、連邦と同様に、セクトラル方式で、個別法により規制されている。

連邦の各個別法と州法との関係についても、専占の法理が適用されるが、連邦法によっては州法との関係を規定していることがある。例えば、以下のとおりである。

・公正信用報告法（FCRA）

州法の適用を排除しないが、FCRA と州法が抵触する場合はFCRAの規定が優先される。

・医療保険の相互運用性及び説明責任に関する法律（HIPAA）プライバシー・ルール

州法が HIPAA よりも効力が弱い場合を除き、州のプライバシー法が優先される。

（ウ）判例

米国銀行協会（ABA） v. カリフォルニア州司法長官（American Bankers Association v. Gould, 412 F.3d 1081, 2005 WL 142260、C.A.9 (Cal.), June 20, 2005）において、ABA は、カリフォルニア州法が金融信用情報の関連会社間での利用、非関連会社への提供につき規制していることは、FCRA の専占、憲法の最高法規条項に反し、認められない旨の主張を行った。

これに対して、連邦裁判所は、①FCRA に専占条項があり、一定範囲での連邦法の専占が認められていること、及び②専占の範囲は、関連会社間での情報の利用・提供に限られることを判示し、カリフォルニア州法における専占の範囲外の部分の有無、当該部分の適用の有効性を判断するため、第一審に差戻した。

イ）Data Breach Notification Laws

Data Breach Notification Laws は、カリフォルニア州から始まり（2003 年）、現在 26 州で施行されている。

同法では、個人データを保有・管理する事業者がデータベースの破壊、不正アクセス、紛失等の事実を認識した際には、直ちに当該本人にその旨を告知する義務が規定されているが、暗号化されたデータについては適用除外が認められている。

現在、連邦法化が検討されている。

④情報保護と情報公開

個人情報保護に関連して、情報保護ないし情報公開に関連する連邦法として、以下の法令がある。

・情報公開法（Freedom of Information Act、５ U.S.C. 552）
・プライバシー法（Privacy Act of 1974、５ U.S.C. 552a）
・議会の情報公開法（Government in the Sunshine Act、５ U.S.C. 552b）

⑤公的部門における個人情報の保護

公的部門において個人情報の保護を定めるものとして、プライバシー法（Privacy Act of 1974、５ U.S.C. 552a）（1975 年 9 月 27 日施行）がある。

プライバシー法においては、以下の事項が規定されている。

（ⅰ） 連邦政府機関の記録の誤用から個人のプライバシーを保護
（ⅱ） 連邦政府機関が保有する個人情報に対する本人によるアクセス
（ⅲ） プライバシー保護調査委員会の設置

⑥民間部門における個人情報の保護

民間部門を対象として個人情報の保護を定める連邦法においては、各個別法ごとに以下のような事項が規定されている。

- 法・個人情報保護の目的
- 法の適用範囲
- 対象事業者、対象となる情報の範囲
- 規制の内容
- 情報主体の権利（コントロール権）の内容
- 監督・登録制度
- 適用除外

主な連邦の個別法としては、以下の法令がある。これらについては、後に詳述する。

(a) 公正信用報告法（FCRA）
(b) 家庭教育権・プライバシー法
(c) 金融プライバシー権法
(d) プライバシー保護法

(e) ケーブル通信政策法
(f) 電子通信プライバシー法
(g) ビデオ・プライバシー保護法
(h) ポリグラフ使用従業員保護法
(i) 電話加入者保護法
(j) 運転免許プライバシー保護法
(k) 医療保険の相互運用性及び説明責任に関する法律（HIPAA）
(l) 電気通信法
(m) 児童オンラインプライバシー保護法
(n) 金融サービス近代化法（GLBA）

⑦自主規制

ア）多様な自主規制・ガイドライン

米国においては、多様な自主規制、ガイドラインが存在する。

例えば、以下のようなガイドラインが挙げられる。

- 医療情報： 米国医師会倫理規定
- 金融情報： GLBA への準拠指針
- 雇用情報： 社内プライバシー規則

イ）認証機能委託制度

米国には、政府による認証機能委託制度は存在しないが、民間企業による認証制度、シール付与制度が存在する。

ウ）政府による自主規制の奨励

米国では、政府が自主規制を奨励している。

商務省（DOC）は、セーフハーバー原則の策定を行い、また、関係業界による適切な対応の推奨を行っている。

連邦取引委員会（FTC）は、オンライン上のプライバシー・ポリシー違反の摘発を行っている。

エ）民間企業による自主的取組

民間企業による自主的取組の例として、プライバシー・ポリシーの策定、プライバシーシール（マーク）（BBBOnline、TRUSTe、CPA WebTrust 等）の取得、W３C（個人情報交換規格（P３P））の取得等が挙げられる。

（２）個別の検討課題[1]

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

ア）個別法による対応

個人情報の第三者提供については、分野ごとに個別法で規定されている。

(ア) 医療保険の相互運用性及び説明責任に関する法律（HIPAA）の「HIPAA プライバシー規則」

個人情報の提供には原則として本人の同意又は許可ないしそれらを与える機会の付与が必要であるが、次の場合は例外とされている（45 C.F.R. 164.512）。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。

(a) 法律の規定がある場合
(b) 公衆の健康に係る業務に用いる場合
(c) 虐待、ネグレクト又は DV の被害者に関する情報の開示
(d) 健康に関する監視業務に用いる場合
(e) 司法・行政手続のための開示
(f) 法執行目的の場合
(g) 死者に関する情報の検視官、葬儀業者等に対する開示
(h) 臓器提供、移植手術等に用いられる場合
(i) 調査目的の場合
(j) 健康・安全への深刻な脅威を回避するために必要な場合
(k) 特殊な政府機能（軍隊、国家安全保障等）のために必要な場合

また、医療機関と提携する企業は、当該医療機関との間で守秘義務契約を締結し、当該契約に従って個人情報を利用することが必要である（45 C.F.R. 164.532）。

(イ) 金融サービス近代化法（GLBA）の「GLBA プライバシー規則」

金融機関の提供の例外事由について、詐欺、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）。

イ）過剰反応に関する現状

米国では、現地での聞き取り調査によれば、「過剰反応」が見られる。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。

関係機関へのヒアリングの結果によれば、以下のような現状がみられる。[2]

・連邦取引員会（FTC）へのヒアリングによれば、過剰反応のような現象がみられ、FTC

では金融機関や消費者から情報開示について頻繁に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 プライバシー規則についても、施行後、同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があった（45 C.F.R.　160.510a-b）。

ウ）制度の運用における過剰反応への対応

・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。法律上の許否について、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。

・公正信用報告法（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）等は、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[3]。

・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

自治会・同窓会における個人情報の取扱いを直接規制する連邦レベルの法令は存在しない。従って、FCRA、HIPAA などの既存の法律の適用範囲内にそれら自治会・同窓会等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

米国には、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ため、プライバシーに関する法律ごとに各々固有の個人情報の定義がなされており、当該法律の定める個人情報の定義の範囲において、当該法律による規制が適用される仕組みとなっている。

ア)FCRA

FCRA の対象とする個人情報となるのは、消費者報告（consumer report）で、これは、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提供であって、信用、保険、雇用目的その他の目的のために、消費者の適格性を判断する際に使用・収集されるものである（15 U.S.C. 1681a (FCRA Sec. 603(d))）。対象となる事業者は、消費者報告機関（consumer reporting agency）で、消費者報告機関とは、第三者に対し消費者報告を提供する目的で、消費者信用情報その他の消費者についての情報を収集・評価することを通常業務とする者で、消費者報告を提供する可能性のある者とされている（15 U.S.C. 1681a (FCRA Sec. 603(f))）。

イ)HIPAA プライバシー規則

HIPAA の対象とするのは、特定の個人を識別可能な健康情報（individually identifiable health information、IIHI）である（42 U.S.C. 1320d）。これには、以下の情報が含まれる。

（ⅰ） ヘルスケアサービスの提供者、ヘルスプランの立案者、雇用者、又はヘルスケア情報センターが作成・取得した情報

（ⅱ） 過去・現在・将来の個人の身体的・精神的状態、個人に対するヘルスケアの提供、又は個人に対するヘルスケアの提供に係る支払に関する情報（個人識別可能又は個人の特定に利用されうると信ずる合理的な根拠がある場合）

保護された健康情報（protected health information、PHI）は、特別に定められた状況を除き、使用・開示が禁止される（45 C.F.R. 164.502）。

ウ)GLBA

GLBA の対象とする個人情報は、「非公開個人情報」（nonpublic personal information）である。これは、個人を識別できる金融関連情報で、一般に入手可能でない金融情報に基づく情報全般を意味する（16 C.F.R. 313.3(n)）。

④センシティブ情報に関する規定

ア）FCRA

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（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（15 U.S.C. 1681a (FCRA Sec. 603(e))）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（15 U.S.C. 1681d (FCRA Sec. 606)）。

一定期間を経過した古い情報（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とされている（15 U.S.C. 1681c (FCRA Sec. 605)）。また、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とされ、当該報告の作成過程で事実であることが立証されたもの、又は 3 か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（15 U.S.C. 1681l (FCRA Sec. 614)）。

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。

イ）HIPAA

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る（45 C.F.R. 164.502）。HIPAA プライバシー規則においては、精神・心理療法記録（psychotherapy notes）等、特に配慮を要する情報について、本人の同意を必要とするなど別途規定が置かれている（45 C.F.R. 164.508）。

ウ）GLBA

情報の開示、利用、共有等の制限に関して、諸規定が定められている（16 C.F.R. 313.10-12）。

⑤小規模事業者の取扱い

それぞれの分野ごとに、個別法において定められている。

ア）FCRA

FCRA には、人数や規模により事業者を格別に取り扱う規定は存在しないから、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。

FCRA の対象となる消費者報告機関には、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、及び消費者報告を作成又は提供する目的をもって州際取引に係る方法・施設を利用する者すべてが含まれる（15 U.S.C. 1681a (FCRA Sec. 603(f))）。

イ）HIPAA プライバシー規則

「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、HIPAA

プライバシー規則からも適用が除外される（45 C.F.R. 160.103）。

ウ）セーフハーバー

商務省（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、組織内に法律部門がない小規模事業者は、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である。

⑥マス・メディアへの対応に関する規定とその内容

プライバシー保護法（Privacy Protection Act）（1980 年）は、報道機関の保有する情報の保護を目的とし、報道機関の保有する情報へのアクセスを求める際の法的手続を定めている。

規制の内容としては、州・連邦の職員による報道機関が保有する著作物、文書資料に対する捜索、差押の禁止が規定され、これらの情報にアクセスするためには裁判所の召喚状が必要とされている。この原則に対する限定的な例外規定は、国家安全保障関連情報、報道機関による犯罪の証拠、証拠隠滅等である。

⑦個人情報の目的外利用の防止措置

それぞれの分野ごとに、個別法に規定が設けられている。

ア）FCRA

信用情報については、消費者報告機関に対する目的外利用の制限の規定が設けられ、いかなる消費者報告機関も消費者報告の提供を法定の一定の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ものとされ、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とされている（15 U.S.C. 1681e (FCRA Sec. 607)）。この規定は、直接的には罰則により担保されているが（15 U.S.C. 1681q-1681r (FCRA Sec. 619-620)）、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（15 U.S.C. 1681n-1681o (FCRA Sec. 616-617)）。

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る。

イ）HIPAA プライバシー規則

原則として、個人情報の利用・開示には本人の許可を得る必要があり、当該利用・開示は、許可の内容に従ったものでなければならない旨定められている（45 C.F.R. 164.508）。医療機関等は、医療個人情報に関するポリシー及び手続の策定、実施に対する責任者や苦情を受け付ける担当者を任命しなければならない（45 C.F.R. 164.530(a)(1)）。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。

⑧市販の名簿の管理

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。米国では、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。

ア）FCRA

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提供であって、信用、保険、雇用目的その他の目的のために、消費者の適格性を判断する際に使用・収集されるものである（15 U.S.C. 1681a (FCRA Sec. 603(d))）。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。

イ）HIPAA プライバシー規則

HIPAA プライバシー規則は、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される。ただし、HIPAA プライバシー規則では、医療業務に携わる者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が[4]、保健福祉省（HHS）へのヒアリングによれば、HHS はこれを問題とは考えておらず、匿名化の手続を利用することによって対処できるとのことであった。すなわち、HIPAA プライバシー規則の下では、個人を識別せず、個人を特定するために利用できると考えられる合理的な理由のないものとして「匿名化（De-identification）」された健康情報は、特定の個人を識別可能な健康情報（IIHI）に該当しない（45 C.F.R. 164.514）。医療情報をの匿名化の要件は、(ⅰ)一般に認められている特定個人を識別できない統計的・科学的原理や方法に通じている者が特定個人を識別するために利用しうるリスクが極めて小さいと判断し、その判断の正当性を書面化している場合、又は(ⅱ) 18 の識別子（Identifier）（①氏名、②地理情報、③個人に直接関連する日付の要素、④電話番号、⑤ファックス番号、⑥電子メールアドレス、⑦社会保障番号、⑧医療記録番号、⑨ヘルスプラン受益者番号、⑩アカウント番号、⑪認

証・ライセンス番号、⑫車両・製造番号、⑬機器・製造番号、⑭URL、⑮IP アドレス番号、⑯生体認証、⑰顔写真画像、⑱その他の特有の識別番号等）を取り除くことである。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。

ウ）GLBA

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等に関する取扱いを特別に区別していないため（16 C.F.R. 313.3(n)）、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。

エ）家庭教育権・プライバシー法（FERPA）

教育情報（学校記録）のうち、当該学校が連邦教育省から資金を受けている場合には、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、体育会系チームのメンバーの体重・身長、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る（20 U.S.C. 1232g(a)(5)(A)and(B)）。

⑨個人情報の取得元の開示に関する措置

ア）FCRA

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（15 U.S.C. 1681g (FCRA Sec. 609(a)(1))）[5]。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については開示される必要はない旨規定されている（15 U.S.C. 1681g (FCRA Sec. 609(a)(2))）。

イ）HIPAA プライバシー規則

HIPAA プライバシー規則には、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。

ウ）GLBA

GLBA 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。

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 の運用においては、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。

⑩個人情報の利用停止・消去に関する措置

個別法によっては、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。

ア）FCRA

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、その結果に基づいて情報を訂正することが要求される（15 U.S.C. 1681i (FCRA Sec. 611)）。調査によっても争いが解決しない場合には、消費者には争いの本質について記載した文書を提出することができる（15 U.S.C. 1681i (FCRA Sec. 611(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ととされる（15 U.S.C. 1681i (FCRA Sec. 611(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、その要請に基づいて、情報が削除されたことについての通知が送付される（15 U.S.C. 1681i (FCRA Sec. 611(d))）。

イ）HIPAA プライバシー規則

HIPAA プライバシー規則においては、訂正請求権（45 C.F.R. 164.526）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。ただし、PHI の利用停止や消去に関する要件を規定していないことについて、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。

⑪国際的な情報移転に関する措置

個別法によっては、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。

ア）HIPAA プライバシー規則

HIPAA プライバシー規則は、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）。

イ）GLBA

米国で取引を行っている金融機関及び米国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。

ウ）セーフハーバー

EUデータ保護指令に対して､セーフハーバー協定による対応が行われている(⑫を参照)。

⑫EU データ保護指令に対する対応状況

ア）EU データ保護指令

EU データ保護指令（個人データ処理に係る個人の保護及び当該データの自由な移動に関する EC 指令、1995 年 10 月 24 日）は、①全部又は一部が自動的に処理される個人情報、及び②マニュアル処理でファイリングシステムに蓄積されている個人情報を適用範囲とする。

EU データ保護指令 25 条では、EU 構成国は、個人情報の第三国への移転を、当該第三国が十分なレベルの個人情報保護を確保している場合に限って、行なうことができる旨定められ、その例外として、国家に十分なレベルの保護体制がない場合においても、企業・組織が当該保護体制を保有していれば、当該企業・組織に対しては個人データの移転が可能であるとされている（EU データ保護指令 26 条)。

イ）セーフハーバー（Safe Harbor）

米国は、EU データ保護指令への対応として、セーフハーバー協定（Safe Harbor Agreement）（2000 年 5 月）を締結し、米国商務省が作成するセーフハーバー 原則（2000 年 7 月公表）を産業界が遵守していれば、EU 指令 25 条違反にならない（十分なプライバシー保護を行なうとみなされる）というセーフハーバーを設定することとした。

セーフハーバーの適用対象は、EU から米国へ流通する個人情報であり、EU の国民からデータを収集し、そのデータを米国に持ち込むすべての企業が適用対象となる。

実務的手続としては、米国企業がセーフハーバーへの参加を決定し、商務省に確約書を提出すると、商務省は参加リスト・確約書を保存して、これをウェブサイトに掲載する。

セーフハーバー原則の内容は、以下のとおりである。

① 告知： 利用目的等
② 選択： opt-out（目的外使用、第三者提供)、opt-in（センシティブ情報）
③ アクセス： 開示、訂正、変更、削除請求
④ セキュリティ： 不正行為等に対する予防措置
⑤ 第三者への提供： 通知・選択
⑥ データの完全性： 利用目的との関連性、データの信頼性、正確・安全・最新性
⑦ 実施・施行： 商務省・FTC による監督（違反に対する告知、調査、停止命令）

⑬死者に関する個人情報の保護

個別法により、規定されている法律と規定されていない法律がある。

HIPAA プライバシー規則では、死者に関する個人情報についても適用されることが明示的に規定されている（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、検視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、検視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)）。また、対象機関は、葬儀業者等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)）。

⑭直接処罰等の実効性確保の措置

個別法ごとの規定に委ねられている。

ア）FCRA

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（15 U.S.C. 1681n-1681o (FCRA Sec. 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者、又は個人情報をその受け取りが許されていない第三者に機関保有のファイルから故意に提供した消費者報告機関の役職員は、刑法の規定に基づく罰金若しくは２年以下の懲役・禁錮又はそれらの併科に処せられる（15 U.S.C. 1681q-1681r (FCRA Sec. 619-620)）。

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）[6]。

イ）HIPAA プライバシー規則

HIPAA は､プライバシー規則を遵守しない情報の取扱いについて民事罰（１件あたり 100 ドル、１人あたり年間２万５千ドルまで)、本人の同意なしに情報を入手、提供したものには５万ドル以下の罰金、１年以下の懲役・禁錮又はこれらの併科、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、５年以下の懲役・禁錮又はこれらの併科、さらに営利目的や被害を与える意図がある場合には 25 万ドル以下の罰金、10 年以下の懲役・禁錮又はこれらの併科を設けている（42 U.S.C. 1320d-6 (HIPAA Sec. 1177)）。法執行は HHS の OCR が行う。

（３）個人情報保護に関する個別法

①公正信用報告法

公正信用報告法（Fair Credit Reporting Act, FCRA）（1970 年）は、信用情報の取扱いについて規定している。

ア)目的

目的は、信用情報の利用、信用情報機関の規制である。

信用情報機関が取り扱う消費者の信用、人事、保険その他の情報の機密性、正確性、適切な利用等に関し、消費者にとって公正・公平な方法で対応するための相当な手続を定め、公正・衡平（fair and equitable）な利用を図っている。

イ)適用範囲

対象情報は、消費者報告（consumer report）で、これは、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提供であって、信用、保険、雇用目的その他の目的のために、消費者の適格性を判断する際に使用・収集されるものである。

対象事業者は、消費者報告機関（consumer reporting agency）である。ここで、消費報告機関とは、第三者に対し消費者報告を提供する目的で、消費者信用情報その他の消費者についての情報を収集・評価することを通常業務とする者で、消費者報告を提供する可能性のある者とされている。

ウ)規制の内容

規制の主な内容は、以下のとおりである。

（ⅰ） 消費者報告の提供制限

- 一定の要件の充足
- 一定期間経過後の情報報告の禁止
- 情報提供者による正確な情報の提供

（ⅱ） 消費者報告の手続・利用

- 消費者調査報告実施に関する開示（消費者に不利益な取扱いを行う場合等）
- 消費者報告機関による報告提供前の身分証明・用途確認のための合理的努力
- 情報の正確性を確保するための手続
- 一定の場合における利用者による報告利用の消費者に対する事前通知

（ⅲ） 本人からの請求に対する消費者報告機関の対応

- 消費者に関する情報ファイルの実質的内容、情報源、消費者報告の受取人等

の開示
- 情報の完全性・正確性に関する異議申立に対する再調査、訂正等

エ)監督機関

監督機関は、連邦取引委員会（FTC）である。

オ)適用除外

適用除外の対象は、以下のとおりである。
- 単なる消費者・報告者間の取引・経験に関する情報を内容とする報告
- クレジットカード等の証票の発行者による特定の信用供与の授権・承認
- 第三者からの信用供与の要求に対する自己の決定を伝える報告

カ)救済措置

法律違反は訴訟の対象となる。

違反に対する懲罰的損害賠償が規定されている。

キ)改正法

FCRA 改正（消費者信用報告改正法）（1996 年）により、関連会社（資本の共同関係その他支配関係を共通する事業者）への情報提供の自由が認められた。

②家庭教育権・プライバシー法

家庭教育権・プライバシー法（Family Educational Rights and Privacy Act, FERPA）（1974 年）の目的は、学生の学歴記録の機密保持である。

適用範囲は、小中学校の教育機関で、連邦の資金援助を受けている学校が対象となる。

規制の内容としては、教育機関が保有する記録の開示について、生徒又は両親（生徒が年少）の書面による同意が要件とされている。例外として、進歩・確認・標準テストの運営を助け、学生の支援プログラムを管理し、授業の改善をするためが挙げられている。

法に従わない教育機関に対しては、政府助成金が制限される。

不服申し立ては、教育機関の長を通じて教育長官になされる。

③金融プライバシー権法

金融プライバシー権法（Right to Financial Privacy Act）（1978 年）の目的は、個人の財務情報の連邦政府に対する開示の際の規制で、財務情報の開示に関する厳格なガイドラインを定め、通知、異議申立についての法的手続を定めている。

適用範囲は、連邦政府に対する開示で、民間企業への財務情報の開示の規制ではない。

規制の内容としては、金融機関による顧客の口座記録に記載されている内容の複写の政府機関に対する開示・提供について、以下の要件が定められている。

① 顧客の承認
② 行政機関の召喚状・出頭命令
③ 裁判所の召喚状・捜索令状
④ その他の公的な正式文書による特別の手続（外国諜報活動等）

法的命令に対する救済、賠償、懲罰的賠償が規定されている。

④プライバシー保護法

プライバシー保護法（Privacy Protection Act）（1980 年）の目的は、報道機関の保有する情報の保護で、報道機関の保有する情報へのアクセスを求める際の法的手続が定められている。

規制の内容としては、州・連邦の職員による報道機関が保有する著作物、文書資料に対する捜索、差押の禁止が規定され、これらにアクセスするためには裁判所の召喚状が必要とされている。

限定的な例外規定は、国家安全保障関連情報、報道機関による犯罪の証拠、証拠隠滅等である。

⑤ケーブル通信政策法

ケーブル通信政策法（Cable Communications Policy Act）（1984 年）の目的は、ケーブル通信加入者の個人情報の保護である。

規制の内容としては、①ケーブル通信加入者に対するプライバシー権に関する文書による通知（1 年に 1 度以上）（収集する情報の種類、使用方法、開示先、保存期間、アクセス方法、事業者の義務の明記）、②個人情報の収集・開示前に、加入者から文書・電子データによる同意書（正当業務に必要な場合等は不要）、③加入者の権利としてのデータへのアクセス、訂正請求、④個人情報が不要となった場合の破棄等が定められている。

⑥電子通信プライバシー法

電子通信プライバシー法（Electronic Communications Privacy Act、ECPA）（1986 年）の目的は、①電子通信の傍受からの保護、②権限のないアクセス・開示からの電子データ、通信内容の保護で、ワイヤレス通信、電子メール、デジタル通信を介した会話や事業者・顧客間のデータ送信を保護するものである。

規制の内容としては、①傍受の禁止、②政府が適切な法的手続きなく通信業者に対して電子通信の開示を要求することの禁止（社内メールシステムには適用なし）、③ユーザーからの授権に基づく電子情報へのアクセス、④発信者・受信者の同意に基づく電子情報の公表等が定められている。

⑦ビデオ・プライバシー保護法

ビデオ・プライバシー保護法（Video Privacy Protection Act, VPPA）（1988 年）の目的は、ビデオレンタル顧客情報等の保護である。

規制の内容としては、①個人情報を含むレンタルビデオの貸出記録の開示の禁止、②情報開示が認められる場合の限定（(ⅰ)本人に対して開示する場合、(ⅱ)本人の文書による同意がある場合、(ⅲ)令状等による場合、(ⅳ)開示対象が氏名・住所のみである場合、(ⅴ)本人に対して開示を禁止する機会が付与されている場合、(ⅵ)通常の営業の範囲内における開示の場合）、③個人情報を含む記録の特定期間経過後の破棄等が定められている。

⑧ポリグラフ使用従業員保護法

ポリグラフ使用従業員保護法（Employee Polygraph Protection Act（1988 年）の目的は、うそ発見器の雇用情報としての利用規制である。

規制の内容としては、①雇用者による、(ⅰ)被雇用者、雇用予定者に対する嘘発見器の使用、(ⅱ)嘘発見器の結果の使用、(ⅲ)嘘発見器使用を拒否した被雇用者等に対する雇用に関するアクションの禁止（適用除外は雇用者のビジネスに経済的損失等を与える事件についての調査）、②労働長官による禁止事項の説明の告知、③労働長官が違反防止の権限、④被験者の異議申し立て中、テスト中、テスト後の権利、⑤嘘発見器を使用する試験者の資格等が定められている。

⑨電話加入者保護法

電話加入者保護法（Telephone Consumer Protection Act）（1991 年）の目的は、電話加入者のプライバシーの保護である。

規制の内容としては、①自動ダイヤル通話システムにより、着信側が同意なく電話料を負担する架電の禁止、②ファクシミリ、コンピュータその他の機器を使用した受け手が求めない広告の送信の禁止、③連邦通信委員会（Federal Communication Commission、FCC）による規則の制定等が定められている。

⑩運転免許プライバシー保護法

運転免許プライバシー保護法（Drivers' Privacy Protection Act）（1994 年）の目的は、個人の自動車記録に含まれる個人情報の保護である。この個人情報には、運転者の氏名、住所、電話番号、SSN、ID 番号、写真、身長、体重、性別、年齢、医療・障害情報等が含まれるが、交通違反、運転免許証の状態、事故情報は対象外とされている。

規制の内容としては、陸運局による運転者の個人情報の開示には、運転者の文書による同意が必要であるとされている。

⑪医療保険の相互運用性及び説明責任に関する法律

医療保険の相互運用性及び説明責任に関する法律（Health Insurance Portability and Accountability ACT、HIPAA（Kennedy-Kassebaum Act））（1996 年）は、医療情報の取扱いについて規定している。

ア)HIPAA の目的

HIPAA の目的は、転職後の健康保険の継続及び健康保険の請求・支払における医療記録のコンピュータ（電子）化にある。

ところが、電子化された医療情報の使用増加によるプライバシー侵害の可能性が生じたため、「HIPAA プライバシー規則」（45 C.F.R. 164 (Security and Privacy)）（2002 年）が制定され、個人の健康情報に係るプライバシー保護に関する包括的な連邦規則となった。

イ)HIPAA の対象情報

HIPAA の対象とするのは、個人を特定識別可能な健康情報（individually identifiable health information、IIHI）である。これには、以下の情報が含まれる。

・ヘルスケアサービスの提供者、ヘルスプランの立案者、雇用者、ヘルスケア情報センターが作成・取得した情報
・過去・現在・将来の個人の身体的・精神的状態、医療に対する支払に関する情報（個人識別可能又は個人の特定に利用されうると信ずる合理的な根拠がある場合）

保護された健康情報（protected health information、PHI）は、特別に定められた状況を除き、使用・開示が禁止される。

ウ)HIPAA プライバシー規則の目的・対象事業者

HIPAA プライバシー規則の目的は、健康保険関連情報、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に、個人情報保護の基準・要請・解釈の細目を示す

ことである。

その対象事業者は、健康保険事業者、医療・健康情報交換事業者、医療提供者で、電子的に医療・健康情報を取り扱う者である。

エ)HIPAA プライバシー規則の規制内容

HIPAA プライバシー規則の規制の内容は、以下のとおりである。

・情報提供には、個人の許可・同意を必要とする。この制限の例外として、許可・同意を必要としない場合には、診療時、支払時、医療業務管理時に使用する場合等が挙げられている。
・情報収集は、目的のため必要最小限に限られる。
・医療・健康情報の取扱い方針の患者への通知が必要である。
・個人情報の保護措置として、①対象事業者は、保護された健康情報の保護のために、適切な管理、技術、物理的な措置を講ずること、②プライバシー保護担当者（Privacy Officer）を設置すること、③職員研修、プライバシー関連手続に関する文書の整備を行うこととされている。
・本人からの請求については、開示・訂正請求、医療記録利用・提供状況に関する記録告知が認められている。

⑫電気通信法

電気通信法（Telecommunications Act）（1996 年）は、1934 年通信法を改正したもので、電気通信事業者による消費者固有のネットワーク情報（consumer proprietary network information、CPNIzzxcvbn）の機密性の保護が定められている。

CPNI には、電気通信サービス加入者の通信パターン、請求記録、電話帳未記載の電話番号、自宅住所等が含まれる。

電気通信法の対象事業者は、電気通信業者である。

規制の内容としては、①CPNIは、電気通信サービス提供目的でのみ使用することができ、マーケティング目的での使用を禁止すること、②消費者からの指示時、消費者へのサービス提供時にのみ、個人を特定できる CPNI を使用、開示、アクセスの許可をすること等が定められている。

なお、Wireless Communication and Public Safety Act（1999 年）では、緊急通報、携帯電話利用における位置情報の使用の限定が定められている。

⑬児童オンラインプライバシー保護法

児童オンラインプライバシー保護法（Children's Online Privacy Protection Act、COPPA）

（1998 年）の目的は、13 歳未満の児童の個人情報の保護である。

適用対象は、13 歳未満の児童に向けられた商業ウェブサイト、及びその事実を知りながら自動から個人情報を収集する一般ウェブサイトである。

COPPA の規制の内容は、以下のとおりである。

・13 歳未満の児童について両親の事前の承諾なく個人情報の収集、他者への個人情報の開示することの禁止
・プライバシー・ポリシーの掲示義務
・FTC による規則の制定
・FTC によるサイト運営者の自己規制策定の促進

COPPA に関連して、連邦取引委員会により児童オンラインプライバシー保護規則（Children's Online Privacy Protection Rule、COPPR）が定められている。COPPR では、ウェブサイト運営者等がプレイバシーポリシーに含めるべき事項、保護者からの同意取得の時期・方法等について詳細に規定されている。

⑭金融サービス近代化法

金融サービス近代化法（Financial Modernization Act, Gramm-Leach-Bliley Act、GLBA）（1999 年）の目的は、証券・銀行・保険業務の一本化を認容である。

そこで、系列・関連企業間での顧客情報の共有、情報の集中、多角的利用に関して、総合金融サービスにおける個人情報の保護が求められることとなった。

GLBA の規制の内容は、以下のとおりである。

・金融機関による個人情報保護の体制・手続の設定
・機密財務情報への不正なアクセスの防止
・金融機関が収集する顧客情報の種類、使用について、プライバシー・ポリシーの通知・開示（個人情報保護体制の説明、関連会社・非関連会社への情報提供）
・個人情報取得の際の真実でない詐欺的文言の使用禁止
・非関連会社への情報提供についての顧客の個人情報提供拒否権（opt out）

⑮その他

その他、個人情報保護に関する規定を含む法令として、以下のようなものがある。

・税制改革法：Tax Reform Act（1976 年）
・債務取立法：Debt Collection Act（1982 年）
・電子消費者保護法：Electric Consumers Protection Act（ECPA）（1986 年）
・コンピュータ安全保護法：Computer Security Act（1988 年）

・金融記録プライバシー法： Financial Records Privacy Act（1988 年）
・スパムメール規制法： Controlling the Assault of Non-Solicited Pornography and Marketing Act、CAN-SPAM-Act（2003 年）
・事務処理削減法：Paperwork Reduction Act（1980 年）（政府の個人情報収集の削減）

２．第三者機関について

（１）第三者機関の実態

①制度の概要

米国には、個人情報全般を所轄する統一的な第三者機関は存在しない。
分野別の個人情報に関する第三者機関は、各個別法の規定に委ねられている。

②連邦取引委員会

ア）FTC の法的位置づけ

米国の連邦取引員会（Federal Trade Commission、FTC）は、諸外国の第三者機関ほど政府から独立しているわけではないが、消費者のプライバシー保護については、消費者保護に関する職務・権限を担う独立の機関として機能している。

FTC は、５人の委員（コミッショナー）によって統括されており、これらの委員は上院の承認を経て、大統領によって指名・任命され、各委員の任期は７年である。これら５人の委員のうち１名が委員長として選出される（FTC 法 41 条)。委員は、任務懈怠、在職中の不正行為等の場合を除き、自らの意に反して罷免されることはなく、職権行使の独立性が認められている。

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

イ）FTC の職務・権限

FTC の職務・権限は、以下のとおりである[7]。

（ア）不公正な競争方法の規制（FTC 法５条(a)）

本規制の目的は、シャーマン法・クレイトン法に違反する行為（取引制限、独占行為、合併等企業結合等）を不公正な競争方法として規制するとともに、これらの行為・慣行をその初期段階において規制することにある。

（イ）不公正・欺瞞的な行為・慣行の規制監視（FTC 法５条(a)）

ここで、不公正な行為とは、消費者自身によっては合理的に回避できず、かつ、その行為・慣行が消費者又は競争にもたらす利益を上回るような実質的損害を消費者に与え又は与えるおそれがある行為・慣行を意味し（FTC 法５条(n)）、ここにおいて、FTC は、消費

者保護も所管することとなっている。

（ウ）取引規制規則の制定

FTC は、産業規模の不公正又は欺瞞的取引慣行を防止するため、取引規制規則（Trade Regulation Rules）を制定することができる（FTC 法 18 条）。これにより、FTC は、訪問販売におけるクーリング・オフに関する規則、テレマーケティング販売に関する規則等、消費者取引に関する多数の規則を制定している。

（エ）消費者保護法令の執行

FTC は、信用機会平等法（Equal Credit Opportunity Act）、貸付真実法（Truth-in-Lending Act）、公正信用報告法（Fair Credit Reporting Act）等の消費者保護法令の執行機関であり、これら消費者保護法令の違反行為は、不公正・欺瞞的な行為・慣行（FTC 法 5 条(a)）を構成するものとされている。

（オ）金融関連の個人情報の保護

金融関連の個人情報に関して、FTC は、①金融のプライバシー通知に関する規則の実施、②個人情報の事務的・技術的・物理的保護、③詐欺に対する執行を行う（金融サービス近代化法）。

（カ）消費者のプライバシー保護（FCRA、COPPA）

公正信用報告法（FCRA）や児童オンラインプライバシー保護法（COPPA）は FTC を通じて施行される。

（キ）経済実態、企業活動等に関する調査（FTC 法 6 条）

FTC は、経済実態、企業活動等に関する調査権限を有する。

ウ）消費者保護局

FTC の消費者保護局（Bureau of Consumer Protection、BCP）が、不正・欺瞞的慣行から消費者を保護する役割を担っており、消費者保護局の傘下には、プライバシー・本人性保護課がある。

エ）FTC の事件処理手続

（ア）審査手続

FTC の職員の中から指定された審査官が、立入検査、令状による命令を含む調査を行い（FTC 法 9 条）、また、文書提出命令、証人喚問等の民事審査請求を行う（FTC 法 20 条）。

（イ）同意命令

FTC は、審査手続の結果、法的措置をとることが相当であると判断したときは、相手方に審判開始決定書及び排除措置命令を通告し、次いで、当該命令案の内容についての交渉を通じて合意に達したときは、一般人からの意見申出期間経過後に、同意命令を出す。

同意命令は、違反事実を法的に認定したものではなく、違法性を法的に確定するものではない。

（ウ）審判手続・審決

FTC は、同意命令に至らないときは、審判手続を開始する。審判手続では、審査官が原告側、被審人が被告側となる対審構造の下、行政法審判官（米国内における７年間以上の弁護士資格を有し、かつ、訴訟、行政機関での正式な聴聞を主宰するなどの行政法審判官となるに相応しい経験を７年間以上有する者から任命される。行政法審判官は行政庁により任命されるが、行政庁には罷免する権限はなく、独立性と身分保障が認められている。）が審判を主宰し、仮決定を行う。仮決定は、被審人が異議申立てを行わない場合に、最終的な審決として確定する。仮決定に対する異議申立てがあった場合は、FTC は、仮決定を再検討して最終的な審決を行う。

なお、審判開始決定後であっても、同意命令の手続を行うことができる。

（エ）不服申立て

被審人が審決に不服があるときは、連邦控訴裁判所に審決取消請求訴訟を提起することができる。但し、裁判所は、FTC の専門的機関としての判断を尊重することが求められており、FTC の認定事実が実質的証拠に基づいている場合は、その事実認定が裁判所を拘束する（実質的証拠の原則）（FTC 法５条(c)）。

（オ）仮差止命令

FTC は、審決の確定前に裁判所に対して仮差止命令を求めることができる（FTC 法 13 条）。

オ）苦情・紛争処理

FTC の消費者保護局（BCP）が、第三者機関として、苦情を受け付けている。但し、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なく、個人情報に関する専門機関でもない。

FTC は、信用情報については、違反行為者に対する民事訴訟を提起することができる。

③その他

ア）保健福祉省市民権局

保健福祉省（Health and Human Services、HHS）の市民権局（Office of Civil Rights、OCR）では、HIPAA プライバシー・ルールの苦情を受け付けている。但し、専門機関ではない。

イ）商務省

商務省（Department of Commerce、DOC）は、セーフハーバー原則の策定等、民間部門の取組の支援、関係業界への適切な対応の働きかけなどを行っている。

３．その他の動向

（１）新たな課題への取組

①9.11 のプライバシーへの影響

ア)USA 愛国者法

USA 愛国者法（USA Patriot Act）（2001 年 10 月）は、国土安全保障名目の個人情報収集を目的とする。

情報収集の対象・種類・方法が不明確であることが問題視されている。

情報提供者による提供事実の秘匿が認められている。

イ)国土安全保障法

国土安全保障法（Homeland Security Act）（2002 年 11 月）においては、情報共有の手続が定められている。

プライバシー担当官（政府)、情報セキュリティ・プライバシー諮問委員会に関する規定がある。

②ID カードシステム

監視・追跡システムについては、情報収集目的の不明確性、不正使用の危険性が指摘されている。Radio Frequency Identification（RFID）について、データの収集、利用、管理に関する法的規制が検討されている。

埋め込み型 ID チップ等については、不正使用・濫用の危険性が問題となる。

エンターテインメント技術については、データ収集・利用における危険性が問題となる。

③インターネットとプライバシー

インターネット関連では、インターネットの監視、GPS（Global Positioning System）の監視への利用、ビデオカメラによる監視、携帯電話・ワイヤレス通信技術における通信の傍受が問題となっている。

④その他の動向

ア)ID 盗難対策タスクフォース

ID 盗難対策タスクフォースが、個人の ID 保護対策を検討している。

イ)個人情報侵害通知法

個人情報侵害通知法案では、個人情報の安全性に関する問題発生を顧客に通知する義務が規定されていたが、同法案は、成立しなかった。

ウ)保健福祉省市民権局

保健福祉省市民権局は、緊急事態（自然災害等）後の医療ケア提供方法、電子カルテ等について検討している。

（２）2008 年 FTC 報告書（消費者・競争への力）

消費者のプライバシー及びデータ・セキュリティは、連邦取引委員会（FTC）の消費者保護の使命の中心をなすものである。

2008 年 FTC 報告書によれば、FTC は、個人情報に対するテクノロジーによる脅威から消費者を保護すべく、意欲的に闘ってきたとされている[8]。

具体的には、以下の活動実績が報告されている。

①データ・セキュリティに対する執行

FTC のデータ・セキュリティに係る執行は、個人データの収集、保存、利用及び廃棄を含む個人データのライフ・サイクル全般を保護しようとするものである。

今まで、FTC は、消費者の機微なデータを取り扱っている企業による不十分なセキュリティに対して、17 件の執行活動を行った。

2007 年 12 月、FTC は、American United Mortgage Company が、機微な個人情報を含む消費者ローンの文書をセキュリティのない収納箱その他顧客情報の保護がなされていない場所に放置していたことに対して、50,000 ドルの民事制裁金で和解した旨を発表したが、これは、FTC 廃棄規則違反の最初のケースである。

その他のデータ・セキュリティに関する FTC による執行としては、①2004 年から 2006 年にかけて、機微な消費者ローン情報について合理的なセキュリティを施さず、違反に至った件（Goal Financial、2008 年３月）、②電子商取引事業者がオンラインで消費者から収集したクレジットカード情報を暗号化し、機微な顧客情報を保護するのに適切な措置を講じたと偽った件（Value Click、2008 年３月）、③小売業者が顧客のクレジットカード情報に対するセキュリティを怠り、プライバシー・ポリシーに違反するとともに不正な業務を行った件（Life is Good、2008 年１月）がある。

②携帯メール

FTC は、消費者の秘密の電話番号や財務記録を売買するための携帯メールの利用その他の違法なビジネスに対して執行活動を継続している。

Information Search, Inc.（2007 年 3 月）、Eye in the Sky Investigations, Inc.（2007 年 6 月）、及び CEO Group, Inc.（2007 年 12 月）の件では、FTC は、オンライン・データのブローカーが、消費者の認識又は同意なしに、電話記録を取得・販売したことに対して、命令により、消費者の電話記録の販売を禁止し、また、260,000 ドルの罰金を科した。

③スパイウェア・アドウェア

FTC は、消費者の認知・同意なしに、消費者のコンピュータにインストールされ、当該コンピュータのモニタリングや管理、棄損又は無秩序な大量の広告を送付するために用いられるスパイウェアやアドウェアのプログラムに対して執行活動を継続している。

DirectRevenue LLCがアイテムをダウンロードするとアドウェアがインストールされて、検出し除去することが困難なポップアップ広告が配信されることを十分に開示せずに、消費者に無償のコンテンツ・ソフトウェアとして提供したことに対して、FTC は、150 万ドルの同意命令とともに、2005 年 10 月 1 日より前にコンピュータにインストールされたアドウェアによる広告の配信、消費者の明示の同意のないアドウェアのダウンロード及びセキュリティの脆弱性の悪用に対する禁止等を命令した（2007 年 6 月）。

④CAN-SPAM

CAN-SPAM 法は、一般的に、商業的電子メールにおける詐欺的送信及び件名コンテンツを禁じ、消費者に将来の商業的メールによる宣伝に対するオプトアウトの権利を付与しているが、FTC は、CAN-SPAM 法の積極的な法執行を継続している。

FTC は、1997 年に迷惑メールないし Spam に対する最初の執行を行って以来、250 の個人及び企業に対して、93 件の法執行を行ってきたが、そのうち、30 件は、CAN-SPAM 法の違反に対するものであった。

近時の事例として、Adteractive、Member Source Media 及び Value Click が無償ではないのに無償のギフトを提供するとの広告を配信したことに対して、FTC は、合計約 400 万ドルの民事制裁金を科した。このうち、Value Click に対する 290 万ドルの制裁金は FTC の CAN-SPAM 法に関する制裁金としては最高額である。

⑤児童のプライバシー・セキュリティ

FTC は、13 歳未満の児童から個人情報を収集、利用し又は開示させる前にその保護者から同意を得ていない、児童向け及び一般向けのセブサイトの運営者に対して、民事罰の請

求を提起することにより、COPPA を積極的に執行している。

1998 年の COPPA の制定以来、FTC は、13 件の執行を行い、合計 190 万ドル以上の民事制裁金を科してきた。

Imbee.com が、最初に両親の同意を得ずに 10,500 人以上の子どもから個人情報を収集して保有したこと、包括的なプライバシー・ポリシーを掲げていなかったこと、及び両親への直接の通知においてウェブサイトでの情報収集手続を明示的かつ完全に開示しなかったことによって COPPA に違反したことに対して、FTC は、130,000 ドルの民事制裁金を科し、また、COPPA の遵守と包括的な子どものプライバシー・ウェブサイト及びソーシャル・ネットワーキングの教育的素材へのリンクを求めた（2008 年 1 月）。

⑥Do Not Call 執行

電話販売ルールの「Do Not Call（DNC）」規定は、全国 Do Not Call 登録簿に電話番号を掲載している消費者に対してほとんどの商業的テレマーケティングを行うことを禁じ、また、消費者が 2 秒以内に生のオペレーターに繋げられない「abandoned call」を禁じているが、FTC は、精力的に DNC 規定の執行を継続している。

2003 年 10 月以来、FTC は、個人 68 人及び企業 93 社に対して、36 件の執行を行った。これらのうち 31 件について、FTC は、1,600 万ドル以上の民事制裁金と 800 万ドル以上の消費者救済を行った。

---

1 本項全般について、「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）12～16 頁、94～104 頁。

2 前注 1 、94～95 頁。

3 江夏健一監修『個人信用情報と訴訟』169 頁（文眞堂、1993 年）。

4 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）。

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

6 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を参照（FTC Press Release,Real Estate Service Company Settles Privacy and Security Charge, http://www.ftc.gov/opa/2006/05/20060510-3.htm）。

7 公正取引委員会ホームページ（www.jftc.go.jp）。

8 “The FTC in 2008: A Force for Consumers and Competition” Federal Trade Commission, March 2008, p.42 – p.45.