2014～2015年度 教育研究高度化促進費 研究成果報告書「わが国の新たな情報法制の定立のための比較法研究と理解促進の取組」

著者	?野 一彦, 新保 史生, 河野 和宏, 新井 健介, 馬場口 登
発行年	2020
権利	第一論文 PHP研究所の許諾を得て公開しています。 第二論文 ミネルヴァ書房の許諾を得て公開しています。
URL	http://hdl.handle.net/10112/00021885

第二論文

髙野一彦「情報危機管理とビッグデーターわが国の個人情報保護法制への提言と企業コンプライアンスー」、関西大学社会安全学部編『リスク管理のための社会安全学』ミネルヴァ書房、2015 年、21〜46 頁

情報危機管理とビッグデータ

―わが国の個人情報保護法制へ提言と企業コンプライアンスのあるべき姿―

髙野一彦

Ⅰ．問題の所在

政府は2013年6月14日「日本再興戦略 -JAPAN is BACK-」を公表し、わが国の成長戦略の骨子を示した[1]。同書において政府は、ビッグデータによるイノベーションなどを通じた次世代産業の創出を成長戦略の主要施策として示し、そのためには、①データの利活用と個人情報・プライバシー保護を両立するルールの策定、②監督機関の設置を含む新たな法制度の定立、が必要であるとしている。

政府が「個人情報・プライバシー保護」を成長戦略の主要施策に据えた理由は２つ考えられる。

第一は、個人情報・プライバシー保護の国際的調和の問題である。EU（欧州連合）の「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1995年10月24日の欧州議会及び理事会の95/46/EC指令」（以下「EUデータ保護指令」という。）[2]において、わが国は「十分なレベルの保護（adequate level of protection）」を施している第三国として評価されておらず、同指令の適用を受けるEU加盟28か国および欧州経済領域（European Economic Area, EEA)構成国であるノルウェイ、リヒテンシュタイン、アイスランドのみならず、EUによりプライバシー保護の十分性を承認された11の国・地域[3]からわが国への個人データの移転が原則として禁止されている。世界からデータが集まらない状態で、わが国は国際的に展開するビックデータビジネスを創出することは困難である。従って国際水準の個人情報・プライバシー保護法制を定立し、データ移転制限を排することが、わが国の成長戦略に欠かせない。

第二は、ICTの発展に伴って顕在化した諸課題への対応の問題である。たとえば2013年7月、映画等レンタル事業C社は、顧客が薬局などで医薬品を購入する際に同社が運営するポイントカードを提示することで医薬品購入履歴情報を取得し、これをマーケティングデータとして利用していることについて社会的な批判を浴びた。さらに2014年7月には鉄道会社J社が運営する交通系ICカードによって取得した乗降履歴について、個人識別情報を削除し他社に販売したことが社会的非難を浴びた。このように「挑戦的」な個人情報の利用を行う企業も散見される一方、多くの企業は適法性判断が難しいため、保有する個人情報をビックデータとして利活用することに躊躇している。ビッグデータビジネスを次世代産業として創出するためには、企業がデータ利用時に適法性を判断できる基準、及びこれを担保する制度の定立が欠かせない要件である。

本稿は、このような問題意識を端緒として、国際的整合の観点からEUデータ保護指令、及びその改正提案である「個人データの取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の規則の提案」（2012年1月25日公表、以下「EU一般データ保護規則提案」という。）[4]との比較研究を行い、わが国の個人情報保護法の将来像を提言するとともに、企業の情報コンプライアンス・危機管理のあるべき姿を探究する。紙面の関係上、広い分野のすべてを詳細に論じることは不可能であるため、概括的に論じることをご容赦頂きたい。

２．国際的整合　―EU データ保護指令との比較を中心として―

（1）EU データ保護指令の規範としての効果

前述の EU データ保護指令は、プライバシーの保護と個人データの自由な流通の確保を目的とし、公共部門と民間部門の双方における個人データの処理（自動処理および一部のマニュアル処理）に対して適用される。指令(Directive)は、加盟国が指令に基づき国内法として立法義務を有する[5]。従って EU データ保護指令は、EU 加盟国および EEA 構成国に対して、同指令の規定に従った国内法の整備を求めている。

EU データ保護指令は「アジア・パシフィックにおいても多くの地域の立法の根拠として採用されている」[6]と評価されており、わが国において 2013 年 5 月 24 日に成立した「行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「行政手続番号法」という。）」においても個人情報保護の仕組みを検討する際の根拠となった[7]。

「多くの地域の立法の根拠として採用」されている理由は、EU データ保護指令における個人データの国際移転の制限規定による。同指令 25 条 1 項において、第三国が「十分なレベルの保護」を確保している場合に限ってデータの移転を行うことができることを規定し、十分でない第三国に移転する場合は同指令 26 条の規定により本人の同意を得るか、拘束的企業準則（Binding Corporate Rules, BCR）または標準契約（Standard Contractual Clauses, SCC）により、各国のデータ保護機関による事前の権限付与（authorization）を受ける必要がある。BCR の承認には 3 つのデータ保護機関のレビューが必要である。さらに原則としてデータ処理内容をデータ保護機関に通知する義務もある。

EU データ保護指令 25 条 1 項に規定された「十分性（adequacy）」の認定は、第三国の代表による公式な要請が欧州委員会（European Commission, EC）に提出された場合、EU データ保護指令第 29 条作業部会（Article 29 Data Protection Working Party）が評価を行い欧州委員会が最終判断を行う。わが国は「十分性」の認定手続きを申請していないため、EU にとってわが国は保護水準が不十分な第三国となる。したがって、EU 加盟国または EEA 構成国に所在する企業が日本に個人データを移転する場合は、同指令 26 条規定の例外的措置を利用することになるが、煩雑な手続きと多大な対応費用から、そもそも個人データを日本に移転せず、EU 域内で完結する場合も少なくない[8]。

グローバルに事業を展開する企業にとって、個人データの国際間の流通を規制されることは、事業の発展に多大な影響を及ぼすこととなる。たとえば、日本企業が EU 構成国の企業を買収した場合、原則として買収先企業の従業員の人事データを日本本社に送ることがでず、また消費者等のデータを送ることができない。そうなれば、買収した企業の管理を行うことはできず、単に財務諸表に売上利益を連結するにとどまるのである。これは EU 加盟国および EEA 構成国に限らず、EU によってデータ保護の十分性を評価された国・地域も国内法規に第三国へのデータ移転禁止条項を規定しているため、わが国のように十分性を認定されていない第三国にとって、いわば「包囲網」として機能することとなる。

このように個人データの移転に関する制限が第三国の経済や企業活動に及ぼす影響は大きく、これがわが国が立法の根拠として検討している理由である。

（2）EUデータ保護指令とわが国の個人情報保護法の相違

わが国では2003年5月23日、民間部門を対象とする「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。）、行政機関を対象とする「行政機関の保有する個人情報の保護に関する法律」、「独立行政法人等の保有する個人情報の保護に関する法律」の、いわゆる個人情報保護3法が成立し、同年5月30日に施行している。わが国は、これら個人情報保護3法を核とする個人情報保護法制について、欧州委員会に「十分性」評価を申請した場合、どのような評価を得るのであろうか[9]。

EUデータ保護指令の「十分性」判断の基準として、「個人データの第三国への移転：EUデータ保護指令25条及び26条の適用の実務文書（以下「実務文書」という。）」[10]が存在する。また、オーストラリアが欧州委員会に対して2000年プライバシー修正（民間部門）法（Privacy Amendment（Private Sector）Act 2000）の十分性の認定を申請し、これに対して29条作業部会は2001年1月26日に保護が不十分とする意見を、その理由とともに公表している（以下「オーストラリア意見書」という。）[11]。これらの文書を参考に、EUデータ保護指令の条文との突合せを行い、わが国の現行個人情報保護法制の「十分性」の検討を行った。その相違はつぎのとおりである。

第一は、開示請求の権利性である。わが国の個人情報保護法において、本人の開示請求に関する規定は、同法25条「開示」に規定されているが、本人等による開示の求めに対し、当該情報を開示することを事業者の義務としているに留まり、開示の求めを本人の出訴可能権として規定していない[12]。一方、EUデータ保護指令においては、アクセス権（right of access）としてデータ主体の権利を規定している（指令12条）。これは、データ主体が保存されているデータに関する情報を取得し、修正、消去することを「権利（right）」としており、「加盟各国は各データ主体に管理者から得る権利を保障しなくてはならない」ものとしている。またデータの主体に対し、与えられる権利として、異議申立権（指令14条）、自動処理された個人決定に服さない権利（指令15条）がある。さらに一部の例外を除いては、各国の監督機関に対し、データ処理の適法性に関する捜査請求をすることができる（指令28条4項）。このようにEUデータ保護指令は、開示請求などを本人の「権利」として規定している[13]。

第二は、独立した監督機関の存在である。EUデータ保護指令においては、監督機関の設置を規定している（指令28条）。この監督機関は公的部門および民間部門の双方を監督の対象としており、厳格な独立性が求められている。わが国の個人情報保護法では個人情報取扱事業者に対し、主務大臣が報告、助言、勧告、命令等により関与することになっているが、公的機関を監督する機関は存在しない。また独立性要件を満たさないため「個人情報保護法における主務大臣とは基本的に異なる」[14]機関である。

第三は、特別カテゴリーのデータの処理の規定である。EUデータ保護指令では「人種、民族、政治的意見、宗教又は思想における信条、労働組合への加盟、健康又は性生活に関するデータの処理」を、原則として禁止している（指令8条1項）。しかし、わが国の個人情報保護法における定義規定では、情報の内容や性格による取扱いの違いはない。

その他にも、十分性を認められないであろうと懸念されるいくつかの相違がある。たとえば5000件未満の個人データを保有する小規模事業者が個人情報保護法の適用を受けないこと、「十分なレベルの保護」でない第三国への情報の移転を制限していないことなど、情報の不正取得者への刑事罰を規定していないことなどが考えられる。国際的に自由な情報流通を行うためには、わが国における新しい個人情

報保護法の定立が必要であり、それはEUが求めるデータ保護の「十分性（adequacy）」の要件を充足するものでなければならないであろう。

３．企業から見たわが国の個人情報保護法の「有効性」の課題

（1）ECプライバシー研究報告における論点

2010年1月20日に欧州委員会が公表した「特に技術発展に焦点を当てた、新たなプライバシーの課題への異なるアプローチの比較研究」（以下「ECプライバシー研究報告」という。）[15]において、オーストラリアのニューサウスウェールズ大学のグレアム・グリーンリーフ（Graham Greenleaf）教授がわが国のデータ保護の十分性に関する調査を行っており、その調査結果は「Country Studies B.5-Japan」に記載されている[16]。同報告においてわが国は、個人情報保護法がインターネットにおいて適用されない場合があること、越境データ移動が制限されていないこと、開示請求などのデータ主体の権利行使が困難であること、独立した監督機関が存在せずデータ流出に関する通知や事業者の登録制度がないこと、などを主な理由として「日本の企業のデータ・コンプラインスが他の国の企業よりもより良いとする証拠はない」[17]と指摘し、これを根拠としてEUデータ保護指令におけるデータ保護の「十分性（adequacy）」を充足していると判断することは困難であると結論付けている[18]。

注目すべき点は、「私企業にとっては、法律違反による多額の罰金や集団訴訟よりも、風評リスクによる損害（risk of reputational damage）のほうが重要」であり、わが国の法律が有効であるとの根拠を見いだせないと指摘していることであろう。同調査結果を拝読して感じることは、データ保護の「十分性（adequacy）」は法律や制度の外形的要件と執行（enforcement）の状況も然ることながら、有効性（effectiveness）、すなわち企業においてルールがデータ処理の規範として有効に機能しているかどうかが要件として評価されていることである。

前掲「実務文書」の第1章「何が“十分な保護”を構成するか？（What constitutes “adequate protection”?）において、「手続/執行の仕組み（Procedural/ Enforcement Mechanisms）」の中に「ルールへの優れたレベルのコンプライアンス」（good level of compliance with the rules）があることが要件として示されている。しかし、前掲「オーストラリア意見書」においては、主に法律や制度の外形的要件と執行の状況に対する指摘であり、有効性についての指摘がほとんど見当たらなかった。

しかしグリーンリーフ教授によるわが国の調査結果からすると、わが国の新たなデータ保護法制を研究する場合、情報法分野の比較法研究による立法提案だけでは十分とはいえず、これらの法律を遵守する側の企業のコンプライアンスに関する研究と一体になり、どのような法や制度を設計すれば有効に機能するのか探求する必要があるのではないだろうか。

（2）コンプライアンスへの取組みの現状

企業がわが国の情報法をデータ処理の規範として尊重し、遵守するかどうかは、それぞれの企業が置かれている状況により違いがある。

第一は、企業法務におけるリスク評価の問題である。企業にはさまざまなリスクがあるが、限られた資源で対策を講じるためリスクに優先順位をつける。優先順位は一般に発生頻度と損失により評価する。したがって法的リスクは、当該分野の訴訟や行政行為などが、この2つの点で脅威かどうかにより企業の取組みに違いがでる。

第二は、経営者にかかる義務と責任の違いである。大会社や委員会設置会社は、会社法により内部統制システムの整備に関する事項の決定を義務付けられており、有価証券報告書提出会社は金融商品取引法により内部統制報告制度が義務付けられている。このような法律上の義務や株主のプレッシャーから解放され、経営上の選択肢を広げることが企業の発展に寄与するとの判断から上場を廃止する企業もある。

第三は、事業形態による違いである。法人顧客相手の事業と個人顧客相手の事業では、取組みに違いがでる。たとえば消費者に対して商品・サービスを提供する企業は、消費者の不信を招く情報の利用などが商品・サービスの不買運動につながることを恐れるが、インターネット広告のように法人顧客からの収入で成り立っている企業は消費者の信用低下を重要なリスクと捉える必要がないため、現行法制度の間隙をつく挑戦的なデータ利用を行う傾向がある。

① 企業法務におけるリスク評価の問題

企業法務の視点から、データ保護に関するリスク評価で考慮すべき事項はつぎの2つであろう。

第一は、主務大臣による行政行為である。個人情報保護法において、個人情報取扱事業者の義務違反に対する罰則は32条から35条に規定されており、主務大臣に対して行政上の義務の履行のために、「報告の聴取」「助言」「勧告」「命令及び中止命令」の権限を定めている。また主務大臣の命令に違反した場合における罰則も定めており、行為者のほか法人等をその対象とする両罰規定となっている。

消費者庁が公表した「平成24年度個人情報の保護に関する法律施行状況の概要」によると、2012年4月1日から翌年3月31日（平成24年度）の間に、地方公共団体及び国民生活センターに寄せられた個人情報に関する苦情相談は合計5,623件、事業者が公表した個人情報の漏えい事案件数は319件であったが、主務大臣等が行った勧告、命令及び緊急の命令は0件であった。またその前年度は、苦情相談5,267件、漏えい事案件数420件に対して主務大臣等が行った勧告、命令及び緊急の命令は同様に0件であった[19]。2005（平成17）年度の苦情相談の件数は14,028件、漏えい事案件数は5,267件であり、これと比較すると減少しているとはいえ、主務大臣による勧告、命令及び緊急の命令に至る可能性は極めて低い。

第二は、本人からのプライバシーの侵害を根拠とした訴訟である。京都府宇治市から住民基本台帳データ約22万人分が流出した事件で、宇治市民らが宇治市に対して起こした損害賠償請求訴訟において、大阪高等裁判所は2001年12月25日、プライバシーの侵害を認め1人あたり慰謝料1万円と弁護士費用5,000円の支払いを命じた[20]。また、1998年11月28日に早稲田大学が中国の江沢民主席の講演会を開催した際、参加希望学生の氏名、学籍番号等を記載した名簿を本人の同意なく警視庁に提出したことにつき、同大学の学生3人がプライバシーの権利の侵害を根拠に慰謝料を請求した事件の上告審において、最高裁判所は2003年9月12日、上告人らのプライバシーを侵害し、不法行為を構成するとして控訴審

判決を破棄し差戻した[21]。2004年3月23日、差戻し後の東京高等裁判所判決では慰謝料として1人あたり各5000円の支払いを命じたものの弁護士費用は認めなかった[22]。

この他にも数多くのプライバシーの権利の侵害に関する判例が存在するが、おおむね賠償額は数千円から数万円の間である。近年、名誉毀損事件の慰謝料が高額になる傾向があり、名誉棄損行為への抑止力としての効果を期待されているが、これと比較するとプライバシーの権利の侵害に関する損害賠償額は極めて低い。

企業には様々なリスクがあり、限られた資源で全てのリスクに対応することは不可能である。したがってリスク評価を行い、優先順位の高いリスクを中心に対応を行う。このリスク評価は一般に発生頻度と損失規模によって行う。個人情報保護法における主務大臣の権限行使の頻度の低さ、またプライバシー侵害訴訟における損害賠償額の低さは、企業における当該リスクの優先順位を低くしているのではないかと憂慮する。

②経営者にかかる義務と責任の違い

2005年6月29日に成立した会社法では、取締役会設置会社の場合、内部統制システムの内容は、取締役会の権限等（362条）として、「取締役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務の適性を確保するために必要なものとして法務省令で定める体制の整備（いわゆる「内部統制システム」）」（362条4項6号）につき、「大会社である取締役会設置会社においては、取締役会は、前項第6号に掲げる事項を決定しなければならない」（362条5項）としている[23]。

体制整備の内容は法務省令に委任されおり、2006年2月7日に公布された会社法施行規則100条1項「業務の適正を確保するための体制」の各号に、①情報の保存管理体制、②リスク管理体制、③効率性確保の体制、④使用人のコンプライアンス体制、⑤企業集団のコンプライアンス体制、の5項目が内部統制システムの具体的内容として規定されている。

特に、「使用人の職務の執行が法令及び定款に適合することを確保するための体制」（4号）、および「当該株式会社並びにその親会社及び子会社から成る企業集団における業務の適正を確保するための体制」（5号）は、自社のみならず企業グループのコンプライアンス体制の整備を親会社等の取締役の義務とした規定である。これは1993年の商法改正以降、増加傾向にあった株主代表訴訟を一層増加させ、また取締役の任務懈怠と損害との因果関係の要件を充足すれば、第三者に対する責任が問われる可能性もある。つまり会社に対する任務懈怠責任（423条）や、第三者に対する責任（429条）を根拠として株主又は第三者による違法行為の摘発を促し、これを抑止力として企業活動の適法性を確保するという法の目的の実現を意図していると解される。特に大会社及び委員会設置会社は「内部統制の基本方針」を取締役会で決議する必要がある。

一方、2006年6月7日に成立した金融商品取引法において、有価証券報告書提出会社に「内部統制報告制度」が義務付けられた。同法における「内部統制」は、財務報告の信頼性の確保および公正な情報開示を目的としている。同法における内部統制報告制度のプロセスは次のとおりである。まず有価証券報告書提出会社は、その記載内容が金融商品取引法に基づき適正であることを確認した旨を記載した「確認書」を内閣総理大臣に提出する（24条の4の2　第1項）。つぎに事業年度ごとに、財務報告の適正性

を確保するための体制を評価した「内部統制報告書」を、公認会計士又は監査法人の監査証明を受けた上で、内閣総理大臣に提出する（24条の4の4　第1項）。

その具体的な運用は、金融庁企業会計審議会内部統制部会が2005年12月8日に公表した「財務報告に係る内部統制の評価及び監査の基準」および2007年2月15日に公表した「財務報告に係る内部統制の評価及び監査に関する実施基準」による[24]。同実施基準において「事業活動に関わる法令等の遵守」の対象は、不正会計や有価証券報告書虚偽記載など財務報告に係る法規に限定にされておらず、事業活動を行っていく上で、遵守することが求められる国内外の法律、命令、条令、規則等、並びに組織の外部からの強制力をもって遵守が求められる規範、および組織が遵守することを求められ、又は自主的に遵守することを決定したもの、と規定している[25]。

したがって、金融商品取引法の「財務報告に係る内部統制」において遵守すべき対象の法令は、結果として会社法における内部統制システムが遵守の対象とする法令の範囲と大きな相違はないと考えられる。つまり企業における内部統制システムの構築は、会社法と金融商品取引法が「入口と出口」の関係にある。大会社および委員会設置会社は会社法に基づき取締役会において内部統制の基本方針を決定し、この方針に基づき内部統制システムを構築・運用する。ここで構築した内部統制システムは、有価証券報告書提出会社であれば金融商品取引法に基づき決算期に作成する内部統制報告書の「全社的な内部統制」として、監査人の評価を受けることとなる。なお会社法及び金融商品取引法は、海外に事業を展開するにあたっては、わが国のみならずその国の法令や規範への遵守も求めている[26]。

このように、大会社および委員会設置会社には会社法における内部統制システム構築義務が、また有価証券報告書提出会社には金融商品取引法における内部統制報告制度の義務がかかっており、これが経営者に対してコンプライアンス経営を促すモチベーションになっている。その一方で、非大会社、非公開会社の経営者にはこのようなモチベーションが殆どかかっていない。これは、いわゆる「中小企業」を中心とするカテゴリーであり、わが国においては約177.5万社、全会社数の99.3%を占めている[27]。

③事業形態による違い

事業形態が法人顧客相手なのか、または個人顧客相手なのかにより、企業のコンプライアンスへの取組みに違いが出る。家電製品や教育教材など、消費者に対して商品・サービスを提供する企業が消費者の不信を招く行為を行った場合、商品・サービスの不買運動につながる可能性がある。不買運動は事業の根幹を揺るがす重要なリスクである。したがって顧客の個人情報が蓄積し、膨大なデータベースを構築しても、社会受容性が低く顧客の不審を招く利用は避ける傾向がある。その一方でインターネット広告のように法人顧客からの収入で成り立っている企業は消費者の信用低下を重要なリスクと捉える必要がない。

このような事業形態の違いは、社内の運用ルールを法律の規定よりも厳しく設定するか、現行法制度の間隙をつく挑戦的な設定をするかの違いとして現れる。たとえば、個人情報保護法における第三者提供などの「同意」を約款の条項として記載する方法について、法的な有効性と社会受容性に乖離があるとの指摘がある。社会受容性を考慮するかは、事業形態の違いが少なからず影響を及ぼすものと考えられる。

（2）企業から見た「有効性」の課題

前述のように企業から見た「有効性」は、法律上の義務の有無、執行状況、消費者の影響により違いがある。検討結果を概括すると、わが国の個人情報保護法は主務大臣による権限行使の可能性が低く、また本人からのプライバシーの権利侵害を根拠とする訴訟も優先順位が高いリスクとして考慮する必要がない状況にある。加えて、非大会社または非公開会社であり、法人顧客対象の事業を行っている企業は「有効性」を担保するプレッシャーが全くかかっていないことになる。これは小規模事業者や、小資本で起業できて多額の設備投資が不要なため株式公開による資金調達や借入れの需要が少ないインターネットビジネスのような業態が該当することになる。しかしこれらの事業者は、国際的にみればデータ保護に関するルールが最も有効に機能して欲しい分野である。これが、グリーンリーフ報告におけるデータ保護の「有効性」に関するわが国の課題ではないかと思料する。

４．EU 一般データ保護規則提案への企業の対応

EU は欧州委員会によって 2012 年 1 月 25 日に EU 一般データ保護規則提案を公表し、2013 年 10 月 21 日に市民の自由・司法・内務委員会（Committee on Civil Liberties, Justice and Home Affairs, 以下「LIBE 委員会」という。）において修正案を可決した[28]。これはクラウドコンピューティングなどの情報通信技術の発展とグローバル化により顕在化した新たな問題への対応、多国籍企業への過度な負担の軽減などを目的とした改正である[29]。

EU 一般データ保護規則提案は本稿執筆時点（2014 年 9 月）で採択はされていないが、前述のようにデータ保護の十分性認証に関するフレームワークが個人データの国際流通に影響を与えることから、グローバル企業の情報コンプライアンス体制構築の際に考慮する必要があると思われるため、本項ではその論点に焦点をあてて検討する。

EU 一般データ保護規則提案は、第 1 条「対象事項及び目的」において、個人の保護と個人データの自由な移転の双方を目的とする旨の規定を定めている。現行の EU データ保護指令(Directive)は、加盟国の国内法の制定により実施されるため、加盟国間の法制度に違いが生じた。それに対して、規則（Regulation）はすべての加盟国において直接法的拘束力を有しているため、EU 加盟国及び EEA 構成国におけるデータ保護の基準が統一されることとなる。また「オンライン環境での信頼の構築は経済発展のカギである[30]」として、急速な技術発展により顕在化した新たな個人データ保護の課題に対応している。

企業における情報法コンプライアンスの視点で留意すべき点は、第 3 条「地域的な範囲」（Territorial scope）における域外適用（同条 2 項）及び第 25 条「欧州連合内に設立していない管理者の代理人」（Representatives of controllers not established in the Union）、第 7 条「同意の条件」（Conditions for consent）、第 17 条「忘れられる権利及び消去権」（Right to be forgotten and to erasure）、第 23 条「データ保護・バイ・デザイン、バイ・デフォルト」(Data protection by design and by default)、第 31 条「監督機関への報告」(Notification of a personal data breach to the supervisory authority)、

第79条「行政制裁」（Administrative sanctions）における監督機関による課徴金であろう。これらのうち、発効後の企業の情報コンプライアンス体制への影響が大きいと思われる条項について検討を行う。

第一は、明確な同意取得のスキームの確立である。データ主体の同意に関して、規約やポリシーなどの文書の中で示される場合は、その他の内容と区別して明示される必要がある（7条2項）。またデータ主体による同意の撤回の権利（7条3項）、データ主体と管理者の重要な立場のアンバランスがある場合に同意は法的な根拠を有しない事（7条4項）が規定されている。現在、わが国の企業は商品・サービスの申込の際に契約や約款の一部として同意を取得する場合があるがEU一般データ保護規則提案においては明確な同意を求めており、このような取得方法では要件を充足しないと思われる。

第二は、忘れられる権利及び削除権への対応体制の確立である。これは目的に照らして個人データが必要でなくなった場合、データ主体が同意を取り下げた場合など、自らの個人データを管理者に削除させる権利（17条1項）と規定している。管理者は、当該データが公表されていた場合、そのデータを取扱う第三者に対して、そのリンクや複製などを削除するための合理的な措置を講ずることを義務づけている（17条2項）。本条への故意または過失による違反は、最大50万ユーロまたは年間世界売上高の1%までの課徴金が科される（79条5項（c））ことから、企業は個人データの削除依頼の受付、削除対応及び第三者への削除要請の通知などの一連のプロセスを構築する必要がある。

第三は、クライシス対応の組織及びルールの確立である。個人データ違反（personal data breach）を発見した場合、不当に遅れることなく可能な範囲で24時間以内に監督機関に報告する義務があり、24時間を超えて報告を行う場合は正当な理由が求められる（31条1項）。また個人データ違反が、データ主体のプライバシー保護等への有害な影響が予測される場合に、不当に遅れることなくデータ主体に個人データ侵害の通知を行う（32条）ことを規定している。従って、企業は漏えいや不正使用などのネガティブ情報の収集と管理、経営者への報告、監督機関への報告、及び本人への連絡などの一連の対応を行う組織を確立し、手続きに関するルールを定立する必要がある。

第四は、罰則と域外適用である。本規則に違反した管理者や処理者に対して、最大1億ユーロまたは年間世界売上高の5%のいずれか大きい額の課徴金が科される（79条）[31]。またEU域内に設立されていなくとも域内のデータ主体の個人データを取扱う管理者が、EU域内のデータ主体に商品やサービスを提供する場合、または彼らの行動をモニタリングする場合に適用される（3条2項）。したがって、EU域内に所在し事業を行う企業が対象になること然ることながら、EU域外からインターネットを介して商品・サービスを提供する事業やクラウドなどの事業を行う企業も対象になる[32]。

５．新たな個人情報保護法への提言　―監督機関と法的制裁を中心として―

（1）監督機関に関するカナダ・オンタリオ州のプライバシー・コミッショナーからの示唆

EU一般データ保護規則提案において、欧州委員会が第三国又は国際機関の「保護レベルの十分性」(adequacy of the level of protection)を認定する場合、「独立した監視機関であり、データ保護ルールの遵守を確実にする責任を有し、欧州連合及び加盟国の監督機関が協力してデータ主体の権利行使を

支援し、又は助言を行う」存在が要件となることが明記された（41条2項(b)）。これは「独立監視機関の設置を第三国にも求める」ものとして注目されている[33]。

筆者は2011年8月、カナダ・オンタリオ州トロントを訪問し、プライバシー・コミッショナー（Privacy Commissioner）制度の設計と運用に関する調査を行った[34]。カナダでは、プライバシー保護に関する監視と紛争処理機関として、プライバシー・コミッショナー（Privacy Commissioner）を、また情報公開における同様の機関として情報コミッショナー（Information Commissioner）を置いている。カナダにおけるコミッショナーはオンブズマンであり、政府から独立した公務員として議会に対して責任を負って官民双方を監視する。所掌事務は、法の遵守監視と執行、国民への情報提供と教育啓発、事業者の相談、およびプライバシー影響評価と検査などである。

オンタリオ州においては、「Privacy by Design」の提案者であるアン・カブキアン博士（Dr. Ann Cavoukian）が、情報とプライバシーの双方のコミッショナー（Information and Privacy Commissioner: IPC）を務めている。コミッショナーは強制調査権を有しており、市民からの不服申立に関する調査を行い、勧告により紛争解決を図るが、市民からの不服申立がなくとも自己付託（incidents）として調査を行い、勧告により解決しない場合は自ら提訴し、または訴訟参加者（Intervener）として第三者の訴訟に参加する権限がある。

オンタリオ州IPC事務局は約140人の職員のうち約70人は情報公開、残り70名はプライバシーを担当している。年間の予算は14億円程度であり、そのほとんどは職員の人件費である(2010-2011年度)[35]。

運用事例として東オンタリオ小児病院（The Children’s Hospital of East Ontario：CHEO）のエルイーマム博士（Dr. Khaled El Emam）にヒアリングを行った。CHEOはオンタリオ州の新生児の登録情報データベースを新薬や治療技術の開発などに利用している。このデータベースのシステム構築、患者からの情報取得と研究者や製薬会社等への情報提供の一連のスキームに関して、初期段階からIPC事務局と相談を行いプライバシー保護の仕組みを導入し、プライバシー影響評価と複数回の検査を経てデータベースの運用を行っている。

エルイーマム博士は「システム構築と情報提供スキームの設計段階でのIPCとの相談は、事業者側にとっても時間と経費の低減につながり有益であった」、「コミッショナーによる監視と執行は事業者の意識を高め、オンタリオ州のプライバシー保護レベルを維持するために有効に働いている」旨の感想を語ってくれた。

監督機関による監視と執行、及び事業者へのコンサルテーション並びに市民への教育活動が、カナダ・オンタリオ州全体のコンプライアンス意識を高めている点は、小規模事業者やインターネットビジネスにコンプライアンス経営を促すプレッシャーが極めて低いわが国において、個人情報保護法制の「有効性」を高めるための示唆を含んでいると思われる。

（2）情報の不正取得者への法的制裁

EUデータ保護指令では、第24条「制裁」（Sanctions）に「加盟国は本指令の条文の完全な実行を確実にするために適切な措置を採択し、指令に従って採用された国内法規の条項の違反に対する制裁を規定する」と規定している。またEU一般データ保護規則提案では、第78条「刑罰」（penalties）が新た

に付加され、「加盟国は本規則の条項への違反に適用する刑罰をルールとして規定」し、「刑罰は効果的（effective）で均衡が取れ（proportionate）、そして抑止的（dissuasive）でなくてはならない」と規定している。

わが国においては、2013 年 5 月 24 日に成立した行政手続番号法の立法過程で、個人情報保護ワーキンググループにおいて国際的整合の観点から議論がなされた上で罰則規定が設けられており、不正取得行為等に対する抑止力として期待されている。その一方で、行政手続番号法の一般法としての個人情報保護法は個人情報の不正取得者への法的制裁を規定していない。これは主務大臣の関与の少なさと相俟って抑止力としての効果が期待できない上、EU 一般データ保護規則提案からみると「十分性（adequency）」の要件を充足しないこととなる。

わが国の刑法は有体物を中心とする体系を採ってきたため、無形の情報の不正取得行為等への刑事罰による対応が難しく[36]、不正競争防止法 21 条 1 項 1 号から 7 号に規定する営業秘密侵害罪による法的制裁を検討することが多い。その場合、客体となる情報が同法における営業秘密の要件を充足する必要がある。個人情報は「顧客リスト」などのかたちで多くの従業者が頻度高く利用しており、技術情報のようにアクセス制限や客観的認識可能性の要件を充足する管理は適さない。したがって、秘密管理性要件が厳格に問われる営業秘密侵害罪の適用は限定的である[37]。そもそも経済法に個人情報保護の役割を期待することの是非も考えられる。

一方、個人情報保護法の立法過程で罰則に関する議論がなされている。1999 年 10 月 20 日に開催された高度情報通信社会推進本部個人情報保護検討部会（座長：堀部政男中央大学教授、当時）の第 7 回部会において、「個人情報の保護について（骨子・座長私案）」[38]が示され、個人情報の不正取得者への罰則の加入を検討したが、分野横断的な罰則の創設は構成要件の明確化の観点から実現性に乏しいこと、広く薄く適用する罰則は抑止効果には限界があること、自由な事業活動の阻害要因となるおそれがあること、などの理由から見送られた経緯がある。

罰則が抑止効果を発揮するためには、監督機関による監視と執行が不可欠である。カナダ・オンタリオ州 IPC の事例では、監督機関は確実な執行を担保している。大会社・公開会社とそれ以外の会社、すなわち小規模事業者やインターネットビジネス事業者との間で情報コンプライアンス意識の差がますます拡大するわが国において、監督機関の設置と罰則の加入は、わが国のデータ保護の「有効性」を全体的に高める結果になるのではないかと思料する。

（3）匿名化情報の利用に関する判断基準

個人情報をビッグデータとして利用する際、個人情報保護法における個人情報、又は個人データの要件を充足しない匿名化（非識別化）情報に処理を施すことで適法に利用できることとなる。しかし、多くの企業は膨大な個人情報を保有しているにも関わらず、適法性判断が難しいためこれらの情報をビックデータとして利活用することに躊躇している。わが国は、匿名化（非識別化）情報の判断基準を示さなければ、ビッグデータビジネスによる次世代産業の創出は困難であろう。

欧米諸国では、匿名化（非識別化）情報について、どのような基準を示しているのであろうか。

EU 一般データ保護規則提案では、前文第 23 条に「匿名情報（anonymous data）」の定義を置き、「データ主体が識別できないような方法で匿名化されたデータ」について、データ保護の原則を適用せず利用が可能であるとしている。

アメリカにおいては公的部門と民間部門を統一的に規制する法律は存在せず、民間部門においては一部の分野に個別法が制定され[39]、その他は自主規制による「セグメント方式」を採用している。民間部門に法執行を行っている連邦取引委員会（Federal Trade Commission, FTC）は、2012 年 3 月に「急激に変化する時代の消費者プライバシー保護―企業と政策決定者への推奨（以下「FTC レポート」という。）」[40]を公表し、匿名化情報の取扱いに関する指針を示している。同レポートによると事業者が、①非識別化（de-identify）のための合理的な措置（reasonable measures）を施し、②再識別化（re-identify）しないことの約束を公表し、③データの受領者が再識別することを契約上禁止、している場合に「合理的に連結（reasonably linkable）できないデータ」であり、利用が可能であるとしている。

わが国では、高度情報通信ネットワーク社会推進戦略本部 パーソナルデータに関する検討会において、FTC3 要件をもとにわが国の匿名化情報の利用・管理ルールを策定してはどうかとの議論がなされたが、①合理的な措置（reasonable measures）が不明確、②「公的な約束」に反する場合、アメリカは FTC 法第 5 条「不公正・欺瞞的な行為」[41]として提訴可能だが、わが国に同様の法がない、③契約が履行される担保がない、などの課題が指摘されている[42]。

FTC レポートが示した 3 要件は、事業者が自ら公表した約束に反する行為があった場合、FTC 法 第 5 条における欺瞞的行為として法執行を行うことが制度上の担保となっている。

わが国においては、2004 年 4 月 2 日に閣議決定を行った「個人情報の保護に関する基本方針」の中で、「事業者が個人情報保護を推進する上での考え方や方針」（以下「プライバシーポリシー等」という。）の策定・公表を求めている[43]。会社法における「内部統制の基本方針」は、大会社・委員会設置会社においては取締役会で決議を行うことを求めているが、プライバシーポリシー等は企業における法的な手続きを経ず公表されることとなり、約束違反行為があった場合の法執行の根拠が明確ではない。

2014 年 6 月 24 日に公表された「パーソナルデータの利活用に関する制度改正大綱」では、「個人特定性低減データ」概念を採用し、「特定の個人が識別される可能性を低減したデータに加工したもの」について、本人の同意を得ずに第三者提供や目的外利用を行うことができるようにすると規定されている[44]。しかし情報通信技術の発展は目覚ましく、技術的基準をもって匿名化（非識別化）情報の基準を示すことは困難であると考えられる。

FTC3 要件のわが国への導入は、前述のように制度的担保の課題が指摘されたが、新たな個人情報保護法では、プライバシーポリシー等について取締役会の決議を経て公表することを事業者の義務とするとともに、公表内容への違反行為への行政的措置及び司法的措置を規定し、新設する監視機関にその執行権限を付与することを提言したい。またデータを受け取るものの再識別は、契約上の債務不履行責任のみならず、監督機関に執行権限を付与することで一貫した制度的担保が可能であろう。

欧米諸国においても、匿名化情報の利用に関する判断基準が明確に示されているとは言い難い現在、わが国においてその判断基準及び法執行の仕組みを先駆的に導入することは、ビッグデータにおける匿名化情報利用に関する標準化を先導することとなるり、有益な取組みであると考えられる。

（4）監督機関と法的制裁の必要性

わが国では、2013年9月2日から翌年6月19日までの間、12回にわたり高度情報通信ネットワーク社会推進戦略本部 パーソナルデータに関する検討会が開催された。その結果、2014年6月24日に「パーソナルデータの利活用に関する制度改正大綱」が公表され、2015年の通常国会に改正個人情報保護法案が提出される予定である。

本稿においては、同法案における最も重要な論点はデータ保護の国際的水準との整合であり、そのためには独立性の高い監督機関の新設と、違反者への罰則の明確化であることを主張した。これは一見「規制強化」であり、利活用の促進に寄与しない印象があるが、国際的水準のルール形成と執行により世界中からわが国に個人データが集積し、また監督機関による事業者とのコンサルテーションはファジーな分野に一貫した判断基準を提供できることから、わが国の成長戦略が求める「次世代産業の創出」に必要不可欠であると考えられる。

６．企業の情報コンプライアンス・危機管理

本稿では、データ保護の国際水準との整合が政府の成長戦略としての次世代産業の育成の根幹であること、ビッグデータへの情報の利用に際して顕在化した様々な課題への対応が必要であることから、わが国の個人情報保護法制が大きく変革していくであろうことを示し、その具体的な提言を行った。このような状況を踏まえ、グローバル企業はどのような判断基準で経営を行い、また情報コンプライアンス・危機管理体制を構築すれば良いのであろうか。

第一は、適法性判断を慎重に行うことである。現行法において法律の専門家でも判断が難しい事案が散見されるが、個々の経営判断について、法律家のみならず技術者、顧客などから広く意見を聴取し、様々な側面から適法性及び社会受容性を検討する必要がある。また、企業グループ内にチーフ・インフォメーション・オフィサー（Chief Information Officer：CIO）などの責任者と専任管轄部署を設置し、情報法の専門家を養成するとともに、個々の事案に対してグループ内で統一的な判断を行う必要がある。

第二は、新たな情報取扱規程の定立と運用である。わが国の現行個人情報保護法は、適法性と本人の納得感が乖離し、また国際的な基準とも乖離しており、現行法への「コンプライアンス」ではもはや不十分である。国際的視点から今後の法改正動向を把握し、国際水準と本人の納得感を判断基準として情報の取扱いに関する新たな企業グループ規程を定立し、前掲の責任者を中心にグループ横断的に運用を行う必要がある。

第三は、従業員等のモチベーションを高める経営である。情報通信技術の発展に伴って、内部者による情報の不正取得等の事案が散見されるようになった。企業は不正行為について、監督機関（現行法では主務大臣）への報告や本人等への通知を行う必要があるため、内部者の監視を強化する必要に迫られる。しかし監視は企業秩序定立権と従業者のプライバシー利の利益衡量の問題があり、また監視から受ける精神的苦痛は従業者の忠誠心を低減させることとなる。企業は万が一の場合に即時に対応を行えるように適正な監視を行うとともに、従業員等が働き続けたいと思う「モチベーション」を高めるための経営努力を行う必要がある。

このような「過渡期」において定立する情報管理に関する新たな仕組みが、企業の継続的成長の基盤となることを祈念している。

（たかの・かずひこ）

※本稿は科学研究費助成事業（学術研究助成基金助成金）基盤研究（C）、および関西大学教育研究高度化促進費の研究成果の研究成果として執筆した。誌面を借りて謝意を表したい。

---

[1] 首相官邸「日本再興戦略 -JAPAN is BACK-」（2013年6月14日）。（http://www.kantei.go.jp/jp/headline/seicho_senryaku2013.html 2014年9月17日確認）。

[2] European Commission, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 31995L0046, Official Journal L281, 23/11/1995 31- 50. EUデータ保護指令は、欧州委員会によって1995年10月24日に採択され、1998年10月24日に発効した。

[3] 石井夏生利『個人情報保護法の現在と未来―世界的潮流と日本の将来像―』勁草書房、2014年、89-90頁。2014年5月30日現在、スイス、アメリカ合衆国セーフハーバー・スキーム、カナダ、アルゼンチン、ガーンジー（Guernsey）、マン島（Isle of Man）、ジャージー（Jersey）、フェロー諸島（Faeroe Islands）、アンドラ、イスラエル、ウルグアイ、ニュージーランドが十分性の認定を受けたと紹介している。

[4] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation),* COM(2012) 11 final (Jan.25, 2012).

[5] 「規則（regulation）」は自動的に全加盟国の国内法の一部となり、「指令（directive）」は拘束力を持つものの加盟国が指令に基づき国内法として立法義務を有し、「決定（decision）」は特定の加盟国を拘束し、そして「勧告（recommendation）」「意見（opinion）」は加盟国に拘束力を有しない。

[6] Graham Greenleaf, Twenty-one years of Asia-Pacific data protection, *Privacy Laws & Business International*, Issue 101, Oct.2009, pp.21-24.

[7] 行政手続番号法は立法過程で、内閣官房・社会保障・税に関わる番号制度に関する実務検討会およびIT戦略本部企画委員会の下に設置された「個人情報保護ワーキンググループ」（座長・堀部政男一橋大学名誉教授）において、EUデータ保護指令や「プライバシー・バイ・デザイン」等の国際的なプライバシー保護の考え方に配慮した制度を検討し、導入した。

[8] 「国際移転における企業の個人データ保護措置調査 報告書」2010年3月、25-29頁。「(3)日系企業の対応状況」参照。

[9] 堀部政男「プライバシー・個人情報保護の国際的整合」堀部政男編著『プライバシー・個人情報保護の新課題』商事法務、2010、52頁。2009年4月23日に開催したブリュッセルのデータ保護会議において、欧州委員会・司法自由安全総局（European Commission Directorate-General-Justice, Freedom and Security）法務政策部（Legal Affairs and Policy）ユニットD５・データ保護（Unit D5-Data Protection）事務官（Desk Officer） ハナ・パチャコバ氏（Ms. Hana Pachackova）による「十分性認定手続（Adequacy finding procedure）」のプレゼンテーションにおいて、「日本は、個人の私生活にかかわる個人データ及び基本権に関して十分なレベルの保護を提供している国であるとは、EUによってまだ考えられていない」と述べたと紹介されている。

[10] European Commission, *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, 24 July 1998. 本実務文書 第1章では十分性審査の要件として、内容の原則（Content Principles）と手続/執行の仕組み（Procedural/ Enforcement Mechanisms）が記載されている。前者は(1)目的限定の原則、(2)データの内容と比例の原則、(3)透明性の原則、(4)セキュリティの原則、(5)アクセス、訂正と異議申立の権利、(6)受領者の再

移転制限、そして追加的な原則として(1)センシティブ・データ、(2)ダイレクト・マーケティング、(3)自動的な個人に関する決定が、そして後者は(1)ルールへの優れたレベルのコンプライアンスがあること（deliver a good level of compliance with the rules）、(2)データ主体の支援と援助を提供すること（provide support and help to individual data subjects）、(3)ルールが遵守されなかった際の被害者に適切な救済が提供されること（provide appropriate redress）が示されている。

[11] Article 29 Data Protection Working Party, *Article 29 Data Protection Working Party Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000*, (5095/00/EN WP40 final) Adopted on 26th Jan. 2001. 本意見書における指摘は、(1) 小規模ビジネス（年間の売上高が300万豪ドル以下）、被用者データが適用除外であること、(2) 法により要求または授権される場合には、二次的目的の利用・開示を認めていること、(3) データが一般に利用可能な公刊物として編集された場合はプライバシー原則が適用されないこと、(4) データの収集後に組織が個人に通知することを認めていこと、(5) ダイレクト・マーケティング用に個人データを利用する場合は個人の同意が不要であること、(6) センシティブ・データの収集のみに制限があり利用・開示に制限がないこと、(7) 永住権を持たないEU 市民はアクセス権・訂正権を行使できないこと、(8) オーストラリアから第三国への再移転を禁止していないこと、などである。

[12] ただし学説上、わが国の個人情報保護法25条1項の解釈は、開示等の求めに関する具体的権利性の肯定説と否定説がある。否定説としては、「個人情報取扱事業者の法律上の義務である」（園部逸夫『個人情報保護法の解説』ぎょうせい、2003年、156および159頁）、「裁判上の請求権を付与したものと解することはできない」（鈴木正朝「個人情報保護法とプライバシーの権利―「開示の求め」の法的性格」堀部政男編著『プライバシー・個人情報保護の新課題』商事法務、2010年、89頁）とする説などがあり、また肯定説としては、法案審議において細田国務大臣が立法者意思として権利を付与した旨を答弁していることなどを前提として「立法者意思に照らして具体的権利性を肯定すべきである」（岡村道久『個人情報保護法』商事法務、2009年、270頁）とする説などがある。なお、東京地方裁判所平成19年6月27日判決（判時1978号29頁）では開示の求めについて権利性を否定している。

[13] わが国においても、行政機関個人情報保護法、及び独立行政法人個人情報保護法は本人の開示請求権として権利構成しており、本人が情報開示を請求し、適切な開示が行われなかった場合には、行政不服審査法に基づく不服申立てを行うことができる。

[14] 堀部・前掲注(9)、44頁。

[15] European Commission, *Comparative Study on Different Approaches to New Privacy Challenges, In Particular in the Light of Technological Developments, Final Report*, 20 Jan. 2010.

[16] Graham Greenleaf, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Country Studies, B.5-JAPAN,* 13 (European Commission) May 2010.

[17] Graham Greenleaf id., at 28.

[18] ただし同報告では、わが国のデータ保護法制はOECDガイドラインやAPECプライバシー・フレームワークの基準を満たしていると言及している。

[19] 消費者庁「平成24年度個人情報の保護に関する法律施行状況の概要」2013年9月、5-6頁。なお平成24年度は主務大臣による報告の徴収8件、平成22年度は報告の徴収16件、助言1件であった。

[20] 大阪高判平成13年12月25日判例自治265号11頁。

[21] 最二小判平成15年9月12日判タ1134号98頁。

[22] 東京高判平成16年3月23日判時1855号104頁。

[23] 会社法では、取締役会設置会社を除く株式会社については、348条3項4号に取締役の職務執行の適法性・適正性を確保する体制の整備等の規定を設け、整備すべき体制は会社法施行規則98条に委任している。また委員会設置会社の取締役の権限として、416条1項1号ホに執行役に関する同様の規定を設け、整備すべき体制は会社法施行規則112条2項に委任している。本稿では取締役会設置会社について、その体制の整備に関する論を進めることとする。

[24] 2011年3月30日、金融庁 企業会計審議会は「財務報告に係る内部統制の評価及び監査に関する基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の改訂に関する意見書」を公表し、「財

務報告に係る内部統制の評価及び監査の基準」と「財務報告に係る内部統制の評価及び監査に関する実施基準」の一部を改訂している。

[25] 金融庁 企業会計審議会「財務報告に係る内部統制の評価及び監査に関する実施基準」2011 年3 月 30 日、3 頁。

[26] 大和銀行株主代表訴訟乙事件の大阪地方裁判所判決では「（商法は）事業を海外に展開するにあたっては、その国の法令に遵うこともまた求めている」と判示している。また金融庁 企業会計審議会・前掲注 13）、3 頁では遵守の対象を「事業活動を行っていく上で、遵守することが求められる国内外の法律・・規範」と規定している。

[27] 総務省「平成 21 年経済センサス‐基礎調査」2011 年6 月 3 日による、2009 年7 月 1 日時点の結果。

[28] European Commission, *LIBE Committee vote backs new EU data protection rules,* 2012. （http://europa.eu/rapid/press-release_MEMO-13-923_en.htm 2014 年9 月 20 日確認）。

[29] アメリカにおいては2012 年2 月 23 日、オバマ大統領が署名した政策大綱「ネットワーク社会における消費者データプライバシー：国際的デジタル経済におけるプライバシー保護とイノベーションを促進する枠組み」の中で、「消費者プライバシー権利章典」（Consumer Privacy Bill of Rights)が提言されている。White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (Feb.23, 2012) .

[30] European Commission *supra* note 4, at 2.

[31] 欧州委員会による当初の規則提案では、最大 100 万ユーロ、又は年間世界売上の 2%の課徴金が科される旨が規定されていたが「2013 年6 月の PRISM 問題により風向きが変わ」ったと指摘されている。石井・前掲注（3）：46 頁。

[32] EU 一般データ保護規則提案 第 25 条において、EU 域内に設立していない管理者（企業等）は、EU 域内に「代理人」を設立することを義務付けている。

[33] 石井夏生利「EU データ保護規則提案と消費者プライバシー権利章典」Nextcom Vol.10 2012 Summer、38 頁。

[34] プライバシー・コミッショナー制度の設計と運用、そしてプライバシー・バイ・デザイン(Privacy by Design；PbD）の具体的な運用の実態に関してヒアリング調査を行った。本調査では、オンタリオ州の情報・プライバシー・コミッショナー（Information and Privacy Commissioner, IPC）のアン・カブキアン博士 (Dr. Ann Cavoukian)、プライバシー担当のケン・アンダーソン副コミッショナー (Ken Anderson, Assistant Commissioner(Privacy))、アクセス担当のブライアン・ビーミス副コミッショナー（Brian Beamish, Assistant Commissioner(Access)）をはじめ、事務局の多くの方々と議論を行った。

[35] イギリスは ICO（Information Commissioner’s Office, ICO)であり、独立した法執行機関として 344 人、予算は約 30 億円（2017 万£）（2009-10 年）であったと紹介されている。石井夏生利「英国におけるインフォメーション・コミッショナーの組織と権限」2010 年8 月 21 日、17 頁。

[36]佐久間修『刑法における無形的財産の保護』成文堂、1991 年、1 頁、山口厚「企業秘密の保護」ジュリスト第 852 号、1986 年、48 頁。わが国では 1974 年に刑法に企業秘密漏示罪の加入が検討されたが、草案の段階から賛否両論が激しく対立した。消極論としては、刑法の謙抑性の観点から安易に刑法上の処罰規定を新設すべきでないこと、退職者に対する規定は職業選択の自由を害するおそれがあること、企業における内部告発を妨げる効果があることなどの意見があり、逆に積極論は、秘密が化体した媒体自体を侵害せず、情報のみを侵害する行為について、窃盗、業務上横領の成立を肯定することは困難であることなどの意見があったが、結果として同条は継続検討となった。

[37]経済産業省『営業秘密管理指針』2010 年4 月 9 日改定版、28 頁。わが国の営業秘密に関する裁判例のうち、秘密管理性について判断した 81 件の中で、秘密管理性を肯定したものは 23 件にとどまっている。

[38] 高度情報通信社会推進本部個人情報保護検討部会「個人情報の保護について（骨子・座長私案）」1999 年 10 月 20 日。

[39] 例えば、Health Insurance Portability and Accountability Act 1996 において医療情報を、また Children’s Online Privacy Protection Rule 2012 においてオンライン上での児童又はその児童の親に関する情報について規制を行っている。

[40] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change -Recommendations for Businesses and Policymakers* (March2012), iv.

[41] Federal Trade Commission Act of 1914, 15 U.S.C. §45(a)(2). FTCは商業活動に関する不公正な競争手段、不公正または欺瞞的な行為もしくは慣行について権限を行使することができる。

[42]森亮二「「FTC3要件」を参考にした匿名化について」パーソナルデータに関する検討会 技術検討ワーキンググループ、2013年11月、14-16頁。

[43]「個人情報の保護に関する基本方針」2004年4月2日閣議決定、2008年4月25日及び2009年9月1日一部変更、6頁。

[44]高度情報通信ネットワーク社会推進戦略本部「パーソナルデータの利活用に関する制度改正大綱」2014年6月24日、10頁。