

## 意見書

2015年2月5日  
隼あすか法律事務所弁護士  
明治大学法学部教授

夏 井 高 人

東京地方裁判所平成26年（ワ）第1415号債務不履行（情報開示）請求事件同年9月10日判決（以下「原審判決」という。）に対する東京高等裁判所平成26年（ネ）第5348号債務不履行（情報開示）請求控訴事件（以下「本件」という。）について、村田・若槻法律事務所弁護士村田雅夫氏から意見書の作成・提出を依頼されたので、個人情報の保護に関する法律（平成15年法律第57号・以下「個人情報保護法」という。）の制定過程に実際に関与した者として、かつ、JIS Q 15001（以下、制度を指す場合には「プライバシーマーク制度」という。）の運用実務に携わる者として、かつ、法情報学、情報法及びサイバー法の領域における研究者として、同法の立法事実及び立法趣旨を踏まえ、下記のとおり意見を述べる。

### 記

#### [目次]

1	検討依頼事項	2頁
2	検討の方法・手順	2頁
2. 1	本件の請求に関する理解	2頁
2. 2	JIS Q 15001 との整合性	3頁
2. 3	個人情報保護法 25 条との整合性	4頁
2. 4	小括及び本意見書における検討対象	5頁
3	検討結果	6頁
3. 1	条文上の文言について	6頁
3. 2	マネジメントシステムの考え方	9頁
3. 3	個人情報保護法 25 条 1 項違反行為の法律効果	11頁
3. 4	JIS Q 15001 に反する管理の法律効果	13頁
3. 5	EU 個人データ保護指令との関係	13頁

3. 6	行政機関個人情報保護法における開示請求との相違	18 頁
3. 7	裁判例	19 頁
3. 8	裁判上の請求権性を否定する学説	21 頁
4	まとめ	23 頁
4. 1	個人情報保護法 25 条 1 項の裁判規範性	23 頁
4. 2	JIS Q 15001 の裁判規範性	23 頁
	[注記]	24 頁

[本文]

## 1 検討依頼事項

個人情報保護法 25 条 1 項又は JISQ15001 各所定の保有個人データの開示の求めに関する条項には裁判規範性があるか。

## 2 検討の方法・手順

### 2. 1 本件の請求に関する理解

原審判決の「請求」の欄には、1 として「被告は、原告が平成 25 年 10 月 14 日に作成し被告に対し送付した、個人情報の開示等の請求書に依り生じた債務につき、被告が準拠を公表している JISQ15001 に従い、被告の所有する原告の個人情報について、原告が為したコンプライアンス通報に関する調査資料をはじめとした個人情報を追加して開示せよ」とあり、また、2 として「被告は、上に示す個人情報の開示等の請求書における不開示内容について、個人情報の保護に関する法律 25 条を根拠として“業務の実施に著しい支障をきたすおそれがある”との記載のみで一律に不開示とするのではなく、JISQ15001 3.4.4.5 項に規定の通り、理由を説明の上、できる限りの情報を開示せよ」とある。

原審は、諸般の事情を熟慮の上、原審原告（控訴人）の訴状にある請求の趣旨をそのまま原審原告の請求として判決に記載したものと推定される。

後述するとおり、個人情報保護法 25 条 1 項の開示の求めは、個人情報取扱事業者が現に保有する保有個人データに関する開示の求めを規定するものであり、個人情報取扱事業者が所有する個人情報の開示を求めるものである限り、そもそも同法 25 条 1 項の適用は全くないと考えるが、この点は一応措くこととする。

原審判決に示された原審原告（控訴人）の請求を論理的に解析してみると、原審原告（控訴人）が請求 1 において「原告が平成 25 年 10 月 14 日に作成し被告に対し送付した、個人情報の開示等の請求書に依り生じた債務」と述べる部分は、請求 1 における「JIS Q 15001 に

従い、被告の所有する原告の個人情報について、原告が為したコンプライアンス通報に関する調査資料をはじめとした個人情報を追加して開示せよ」との請求部分及び請求2における「JIS Q 15001 3.4.4.5 項に規定の通り、理由を説明の上、できる限りの情報を開示せよ」との部分の論拠を述べているもので、訴訟法的には請求を基礎づける事実または攻撃防御方法の記載に該当すると解すべきである。

そして、請求1における「JIS Q 15001 に従い、被告の所有する原告の個人情報について、原告が為したコンプライアンス通報に関する調査資料をはじめとした個人情報を追加して開示せよ」との請求部分及び請求2における「JIS Q 15001 3.4.4.5 項に規定の通り、理由を説明の上、できる限りの情報を開示せよ」との部分との関係について検討してみると、請求2における「JIS Q 15001 3.4.4.5 項に規定の通り、理由を説明の上、できる限りの情報を開示せよ」との部分は、請求1における「JIS Q 15001 に従い」との部分をより正確に記述するものであり、また、請求1における「被告の所有する原告の個人情報について、原告が為したコンプライアンス通報に関する調査資料をはじめとした個人情報」との部分は開示を求める情報を特定する趣旨と解される。

以上から、結局、原審原告（控訴人）の請求は、「原告が為したコンプライアンス通報に関する調査資料をはじめとした個人情報」を「JIS Q 15001 3.4.4.5 項に規定の通り、理由を説明の上」開示することを求める趣旨と解される。

## 2. 2 JIS Q 15001 との整合性

一般に、プライバシーマーク制度<sup>1</sup>は、JIS Q 15001 所定の要件に適合するとの評価を受けプライバシーマークの認証を受けた個人情報取扱事業者について、その保有する全ての保有個人データの取扱いを規律するものではない。

プライバシーマーク制度は、特定の個人情報取扱事業者がその保有する個人情報中の特定の種類のものについて個別に管理策を明示して認証申請することを前提としている。認証機関である JIPDEC は、申請された事項（管理対象となる個人情報、その取得方法等）に限定して評価と認証を行い、申請外の事項については何らの評価も認証も行わない。これは、個人情報の種類により管理策が異なることになる結果、認証機関が個別に審査をすることを要し、そのように個別に審査した対象についてのみ認証を与えるしかないという技術的限界によるものである<sup>2</sup>。

そして、被控訴人（原審被告）が JIPDEC から JIS Q 15001 に適合するものとしてプライバシーマークの認証を受けた事項を検討すると、被控訴人（原審被告）の常務としての従業員管理に必要な個人情報の通常の管理策については認証を受ける事項として掲記されているものの、本件におけるような企業の危機管理情報中にたまたま従業員情報が含まれる場合については認証事項として掲げられていない。

具体的に示すと、被控訴人（原審被告）が JIPDEC から JIS Q 15001 に基づくプライバシ

一マークの認証を受けている事項中で被控訴人（原審被告）の従業員に関する事項は、項目12であり、そこでは、個人情報の種類として「業務遂行上必要な従業員、派遣社員、販社・ビジネスパートナー従業員などの個人情報を取扱う業務」とあって全ての種類の従業員の個人情報であることは認められるものの、その取得方法に関しては、「Web サイト他により従業員等から日立が直接個人情報を取得（直接書面取得）」の場合のみである<sup>3</sup>。要するに、被控訴人（原審被告）が JIPDEC からプライバシーマークの認証を受けた個人情報<sup>4</sup>は、被控訴人（原審被告）が従業員本人以外の第三者から取得した個人情報や被控訴人（原審被告）自身の判断結果・評価結果として生成される情報を含まない。

ところが、原審原告（控訴人）が開示を求めている個人情報は、被控訴人（原審被告）が第三者から取得した情報及び被控訴人（原審被告）自身が自己の判断作用の結果として生成した情報なのであって、原審原告（控訴人）から直接に取得した個人情報ではない。

そして、JIS Q 15001 所定の開示手続は、プライバシーマークの認証を受けた事項についてのみ適用される<sup>5</sup>。プライバシーマークの認証が存在しない個人情報に関しては、制度上、JIS Q 15001 所定の手続に基づく開示もあり得ない。

結局、原審原告（控訴人）が開示を求める個人情報に関する限り、JIS Q 15001 所定の個人情報の開示手続が適用されることはあり得ない<sup>6</sup>。

## 2. 3 個人情報保護法 25 条との整合性

個人情報保護法 25 条 1 項は、個人情報取扱事業者が取得した全ての個人情報について規定するものではなく、保有個人データのみを開示対象としている。

ところで、本件において原審原告（控訴人）が開示を求めている個人情報は、被控訴人（原審被告）の危機管理情報の中に含まれているものであり、その性質上、同法 25 条 1 項 2 号所定の例外事由に該当し得る場合が一般的に多いという点を一応措くとしても、その個人情報としての性質及び数量<sup>7</sup>等からして、個人情報の保護に関する法律施行令（平成 15 年政令 507 号）2 条及び 3 条<sup>8</sup>所定の個人情報データベースを構成しない個人情報または保有個人データに該当しない個人情報と解すべきものと推定される<sup>9</sup>。

また、容易照合性（個人情報保護法 2 条 1 項）の点についても、危機管理情報は、通常の従業員管理用データベース等からは切断され、全く別のものとして管理されるのが通例である。本件の原審原告（控訴人）が開示を求める情報もまた、そのようにして管理されているもので、容易照合性が欠如しているか乏しいものと推定される。容易照合性が欠如しているために個人情報データベース（同法 2 条 2 項）を構成しない個人情報は、個人情報データベースの構成要素である個人データ（同法 2 条 4 項）に該当することはなく、無論、保有個人データ（同法 2 条 5 項）に該当することもない。

更に付言すると、一般に、危機管理情報については、容易照合性の解釈においても、また、個人情報保護法 25 条 1 項に基づく保有個人データの開示の求めにおける開示を拒否するこ

とのできる例外事由の判断においても、特段の考察と検討を要する。それは、当該情報が危機管理情報であるがゆえに、原則として<sup>10</sup>、当該危機管理情報の管理主体において格段に機密性の高いものとして管理・保有される必要性があるからである。

そして、原審原告（控訴人）が開示を求める情報が保有個人データに該当しない場合には、そもそも個人情報保護法 25 条 1 項所定の開示を求めることのできる「保有個人データ」に該当しないことになる<sup>11</sup>。

## 2. 4 小括及び本意見書における検討対象

原審原告（控訴人）が現在の請求の趣旨を維持する限り、個人情報保護法の適用はないし、JIS Q 15001 に基づく手続処理に乗ることもないと解される。

しかしながら、世間には、個人情報保護法の真の立法事実及び立法趣旨を全く知らず、個人情報保護の実務について知識・経験を全く有せず、単なる観念論のみを根拠として、「どのような場合においても個人情報の開示を求めることができる」と誤解されかねない論述を示す注釈書や概説書の類が存在することは事実である。

正義を守り、法の適切・妥当な解釈・適用・執行を職務とする裁判所がそのような根拠のない学説等によって判断を左右されることなど決してあり得ないこと信ずる。しかしながら、従来の学説等の中で誤りがあるものに関して、公刊されている書籍・論文等の中で当該学説における誤りの根本原因について詳細に触れているものが比較的少ないことも事実である。それゆえ、裁判所の判断形成において公正・公平さが担保されるよう、その判断形成の基礎となるべき資料として、適切な情報提供がなされなければならないと判断した。

他方で、本件で原審原告（控訴人）が開示を求めている情報は、法的性質としては被控訴人（原審被告）の危機管理情報の一種として認識・理解すべきものではあるが、部分的にせよ被控訴人（原審被告）の従業員管理のための常務において取扱われる個人情報（保有個人データ）ではないかとの疑いをもたれることはあり得ると考える。そのような疑いのある場合について、個人情報保護法 25 条の立法趣旨等について正確な理解を前提とした判断がなされるべきことは言うまでもない。

そこで、本意見書においては、個人情報保護法 25 条における開示の求めの法的性質（特に裁判規範性の有無）について一般的な法解釈論を提供することを求められた経緯に鑑み、一般的な法情報論及び法解釈論の範囲内において、個人情報保護法の母法的な存在となっている EU 個人データ保護指令（European Parliament and Council Directive 95/46/EC 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 [Official Journal L 281 of 23.11.1995]）<sup>12</sup>及び OECD プライバシー保護ガイドライン（OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data）<sup>13</sup>との整合性についても留意しつつ<sup>14</sup>、必要に応じていわゆる「自己情報コントロール権」<sup>15</sup>なる概念との関連についても触れながら、新たに検討を加え、その検討結果

を述べることとする。

なお、重複を避けるため、過去に論説等<sup>16</sup>で論じた点については、必要最小限の引用・参照にとどめ、基本的に省略する。

### 3 検討結果

#### 3. 1 条文上の文言について

個人情報保護法 25 条 1 項柱書本文は、「個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの開示（当該本人が識別される保有個人データが存在しないときにその旨を知らせることを含む。以下同じ。）を求められたときは、本人に対し、政令で定める方法により、遅滞なく、当該保有個人データを開示しなければならない」と規定している。

ここに「求められたときは」と規定し、「請求されたときは」と規定しなかったことの原因について、明確に文字化された公式資料（行政文書等）は存在しない。しかし、立法過程に現実に関与した者（最高裁判所の命により出向した判事を含む。）の間では、情報公開請求権の存在を前提とする情報公開請求とは異なるものであることを示すため、意図的に「求め」としたとの理解が存在していた。そのため、同法 25 条の呼称についても、明文では単に「開示」と項目名を示すにとどまり、一般には「開示の求め」と呼称するのが妥当であり、「開示請求」とは呼ばないとするのが了解事項となっていた。これもまた、開示の求めの法的性質に関して、情報公開法等に基づく情報公開請求権との混同を避けるという趣旨である<sup>17</sup>。

このような立法担当者間における理解に基づく用語の使い分けは、個人情報保護法案の基礎となった情報通信技術（IT）戦略本部個人情報保護法制化専門委員会「個人情報保護基本法制に関する大綱」（平成 12 年 10 月 11 日・以下「大綱」という。）の中でも示されている。

大綱では、「開示」に関する解説として、「『開示等に必要な手続』の内容は、開示、訂正等及び利用停止等における本人関与の実施に当たって必要となる事項であり、本人が行う求めの方法、本人の確認方法、実施に必要な期間、手数料を徴収する場合の額等が考えられる」（12 頁）と記され、また、「『透明性の確保』の観点から、個人情報取扱事業者が保有する個人データについて本人が開示を求められる仕組みを整備するものである。訂正等及び利用停止等とも合わせ、これらの仕組みにより、個人情報の適正な取扱いが当事者間で実効性をもって担保されることが期待される」（13 頁）と記されている。いずれも「求め」であって「請求」ではないこと、そして、その求めに対応するのはあくまでも個人情報取扱事業者であって、その求めに対応する際に要する手続等も個人情報取扱事業者がなすべき手続であり、裁判所の訴訟手続ではないことを明確にしている。そして、このような「開示」を

含む現行個人情報保護法の基本的な枠組みについて、大綱は、「基本原則実現のための具体的な方法は、取扱者の自主的な取組によるべきものである」（3頁）と明確に記している。

これは、後述のマネジメントシステムを骨格とする宣言的法規範<sup>18</sup>という従来の古典的な法規範にはあまりみられない法型式を採用することにより、事業者の自主性・自主管理体制を国家が支援することを目的として個人情報保護法が制定されたのであり、訴訟による請求権の行使と裁判所における紛争解決という伝統的・典型的な法規範とは異なるタイプの法制度であることを示しているということ認識・理解するのに十分だと思われる。このことと関連する政府答弁がある。平成14年4月25日開催の衆議院本会議における個人情報保護の保護に関する法律案外4案の審議において、当時の内閣総理大臣・小泉純一郎氏は、山内功氏の法案撤回要求に対し、「基本原則実現のための具体的な方法は、取扱者の自主的な取組によるべきものである」との大綱の記述を引用しつつ「政府においてはこの考え方をもとに立法化を行い、基本原則は、報道目的を含めた個人情報の有用性に配慮しつつ、個人情報を取り扱うすべての者が、個人情報の適正な取り扱いを行うよう、自主的に努力すべきことを求めるものとしています。すなわち、基本原則は、これに基づいて具体的な義務が課されるものではなく、公権力の関与や罰則を一切ありません」と明確に答弁している<sup>19</sup>。この内閣総理大臣答弁は、直接的には基本原則（個人情報保護法3条）に関するものであり、保有個人データの開示（同法25条1項）に関するものではない。しかし、個人情報保護法における個人情報取扱事業者の義務の法的性質を包括的に説明する答弁である以上、その答弁の中には開示の求めに応ずる義務の法的性質に関する部分も含まれていると理解するのが妥当である<sup>20</sup>。

更に、個人情報保護法の法案段階での国会（本会議、個人情報の保護に関する特別委員会等）の審議内容について、官報によって公開されている議事録を精査すると、質問者である議員（委員）からは開示を請求することのできる具体的な権利（裁判規範）であることを前提とする質問がなされている例が多々見受けられることは事実である。しかし、答弁者である大臣や政府委員等による答弁内容においては、ごく一部の例外を除き、一貫して「開示の求め」との表現が用いられている。質問者である議員が「請求権」との前提（法解釈）を政府が是認したと認識・理解したか否かについては想像の域を出ない。しかしながら、政府答弁において用いられている用語が一貫して「開示の求め」との表現であることは、立法過程における政府の認識・理解（法解釈）を考える上で極めて重要なことである。質問者と答弁者双方の用語が一致していないことについては、多様な解釈や批判があり得るものと予想される。しかしながら、当時の政府としては、具体的な権利としての請求権ではないということを示すために、意識的に用語を使い分けていたと考えるのが妥当である。

このように、立法過程から推測されることからすると、開示の「求め」は裁判規範としての「請求権」ではない<sup>21</sup>。それは、個人情報取扱事業者の自主的な努力としての任意の開示を期待するもので、その不開示が著しく不適切である場合や管理権の濫用的な状況が認められる場合には、業界団体等による自主管理的な措置（同法37条～47条参照）や主務大臣

の事後的な行政監督権の行使としての措置命令及び命令違反の場合の罰則の適用等（同法 32 条～36 条、56 条～58 条参照）<sup>22</sup>により是正するというのが法の基本構造である<sup>23</sup>。念のために付言しておく、個人情報と関連する何らかの法的利益が違法に侵害された場合には、民法 709 条に基づく損害賠償請求をなし得ることは当然のことであるし、また、機密性の高い重要な通信・情報・データ等に関しては、個人情報保護法以外の関連する特別法に基づき、しかるべく罰則の適用がある<sup>24</sup>。

日本国の個人情報保護法 25 条がこのような基本構造をもっていることは、EU の個人データ保護指令に基づく EU 加盟各国の個人データ保護法制<sup>25</sup>においても基本的には同じである。なお、EU 個人データ保護指令との適合性の観点からは、立法形式それ自体は法律であることが求められていないので、法律という法形式を採用する場合と行政規則という法形式を採用する場合とがある。

このように、個人情報保護法 25 条 1 項の開示の「求め」は裁判規範としての「請求権」を認めるものではないとの了解があった。この了解と異なる法解釈論が存在していることは、事実であるが、それは、主として立法過程に現実に参加しなかった研究者（名目的な政府委員等となっても実質的には何も関与していなかったのも同然に立法学や法情報論上の基本原則に則った検討をしたことのない研究者を含む。）によって提示されているもので、了解それ自体を知らないことに起因し、または、自己の法解釈論を有利に展開するために意図的に了解事項を無視していることに起因するものと推定される。

個人情報保護法制定の後、今日に至るまで、真の立法経緯を無視し、「自己情報コントロール権」なる概念<sup>26</sup>が一人歩きし、個人情報保護法 25 条 1 項について、開示の求めではなく開示請求権を法定したものとする全く根拠のない法解釈論が（少なくとも大学法学部等においては）横行していることは、まさに立法担当者が危惧した事態が発生していると評価することができる。

しかしながら、個人情報保護法の施行に際し、日本国政府は、「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・平成 20 年 4 月 25 日一部変更・平成 21 年 9 月 1 日一部変更）を定めている。この基本方針は、網羅的かつ非常に詳細なものであり、日本国政府としての個人情報保護法の解釈・運用上の基本方針（個人情報保護法 7 条、3 条）を国民に対して示すものである。そして、この基本方針に基づき、関連各省庁の個人情報保護ガイドラインが策定されている。

この基本方針中には、民事訴訟に関する事項が全く含まれていない<sup>27</sup>。これは、個人情報保護法 25 条 1 項等に基づく個人情報の本人の請求権なるものの存在を認めていないことを明瞭に示している。この基本方針は、後述のマネジメントシステムの考え方を基本とする公法（行政法）上の法規範として個人情報保護法が制定されたということを当然の前提とするものとする以外にない。少なくとも、この基本方針全体を読めると、個人情報保護法が個人情報の本人に訴訟上の請求権を与える趣旨で立法されたものだということを前提にして国政が運営されたことは一度もないことを理解できる。そして、個人情報保護法案は、

議員立法ではなく内閣提出法案だったので、このような日本国政府の意思が同法の立法意思であるとする以外にはない<sup>28</sup>。

### 3. 2 マネジメントシステムの考え方

一般に、ある社会的病理現象に対処するための方策には①法的対応、②技術的対応及び③自主管理（マネジメント）による対応の3つを考えることができる。それぞれ長所と短所がある<sup>29</sup>。

また、②と③を支援するための法制度が存在し得るし、①と③を支援するための技術が存在し得る。同様に、それぞれについて一定の基準を満たしているかどうかを判定し認証するための第三者認証制度が存在し得る。

個人情報保護法は、個人情報と関連する社会的病理現象に対処するための自主管理（マネジメント）による対応を支援しその実効性を確保するための法制度の一つである。そして、JIS Q 15001 は、個人情報と関連する社会的病理現象に対処するための自主管理（マネジメント）による対応が、国際的に承認された水準で達成されているかどうかを評価し認証するための第三者認証制度において用いられる判定基準の一種である<sup>30</sup>。

マネジメントシステムは、自主管理または自己管理の思想を基本としている。それは、基本方針（ポリシー）を定め、そのポリシーを実現するための手段・管理策（コントロール）<sup>31</sup>を決定し、その手段・管理策（コントロール）を実際に運用し、その運用結果を評価して改善するという組織運用方式の一種である<sup>32</sup>。

マネジメントシステムは、自主管理・自己管理のための宣言的な手法なので、そのような手法を採用したということだけで、他者との間で自動的に何らかの契約関係等を生ずるといった法的性質をもたない<sup>33</sup>。

わかりやすい例で説明すると、例えば、店舗の経営者（管理主体）が「その店舗を清潔に保つ」という基本方針（ポリシー）を定めたと仮定すると、この場合、ポリシーは管理主体である店舗経営者に対する自己羈束を有するものではあっても、その顧客に対する何らかの契約関係を自動的に生成するものではない。管理主体である店舗経営者は、次に、管理策（コントロール）を策定する。管理策は、どのようなものであっても良いので、例えば、「毎朝、店舗の店先を箒ではいて掃除する」という管理策だけを定めるものであってもよい。この場合、管理主体である店舗経営者と潜在的な顧客である未来の来店者との間に、「経営者が掃除をすべき義務」を内容とする何らかの契約関係が発生することはあり得ない。更に、管理主体である店舗経営者が管理策（コントロール）を現実に実施できるかどうかは全く別問題である。例えば、何年か経過した後、老齢のため毎朝店舗の店先を掃除することが体力的に無理になったというような事例を考えると、この管理策は運用することができない管理策になったことになる。この場合、再評価をし、管理策を変更しなければならない。例えば、新たな管理策（コントロール）として、店舗経営者自身ではなく、その息子に対し

て毎朝店先を箒ではいて掃除するように命じ、それを実行させるといったようなことを想定することができる。この場合においても、新たな管理策（コントロール）の策定により、将来の顧客との間において、店舗経営者が息子に対して清掃を命ずべき義務または店舗経営者の息子が命令に従って清掃すべき義務を内容とする何らかの契約関係が自動的に生成されるわけではない<sup>34</sup>。

つまり、マネジメントシステムにおいては、あくまでも、管理主体の自主管理・自己管理のために基本方針（ポリシー）を宣言し、その実施のための管理策（コントロール）を設計して運用・実施し、その結果を評価するということを繰り返すだけのことである。一般にこのようなサイクルのことを PDCA サイクルと呼んでいる。

マネジメントシステムの歴史的由来については、諸説あるけれども、標準的な考え方によれば、英国の工業規格（British Standard: BS）がその方式を標準化し、それが世界各国に普及し、日本国では日本工業規格（Japan Industrial Standard: JIS）においても採用された<sup>35</sup>。ただ、従来の物質を前提とする工業規格ではなく組織の自主的な運営方法に関する規格であるため、JIS では、それがマネジメントシステムの類型に属するものであることを明確にするため、JIS の類型コードを「Q」として識別できるようにしてある。それゆえ、プライバシーマーク制度の根拠となっている日本工業規格も JIS Q 15001 として、識別コード「Q」が付されているのである<sup>36</sup>。

このマネジメントシステムにおける基本構造は、JIS Q 15001 とプライバシーマーク制度や日本国の個人情報保護法のような個人情報（個人データ）の管理手法に関するマネジメントシステムの実装例でも全く同じように採用されている。

一般に、国家の立法機関が、個人情報（個人データ）の保護のための管理策（コントロール）の一種として、立法という手段を用いることがある。個人情報保護法は、その一例であるが、個人情報保護法には、管理策（コントロール）の基本部分しか定めていない。

ところで、一般に、立法により個人情報の本人（個人データ主体）による個人情報取扱事業者（個人データ管理主体）の管理（コントロール）に対する関与の方法を設定する場合、その関与をどのような態様・内容・程度のものとするかについては、あくまでも立法政策の問題である。日本国の個人情報保護法が個人情報の本人について請求権を認める趣旨で立法されたものでないことは既述のとおりである。

また、法律ではない任意の行為規範である工業規格という管理策（コントロール）を策定する場合でも同様である。日本工業規格である JIS Q 15001 は、具体的な管理策として、司法解決（訴訟上の請求権の行使）に関連する事項を一切規定していない。

この個人情報保護法と JIS Q 15001 とは、相互に全く無関係のもののように誤解されている。けれども、個人情報保護法制定当時において、EU 個人データ保護指令との適合性が否定された場合に備えて、個人情報保護法における規律よりもはるかに強力に個人情報の本人（個人データ主体）の利益を保護するように企図して国際標準に適合するように JIS Q 15001 が設計されたことは周知のとおりである。例えば、個人情報保護法においては、機微

な個人情報 (sensitive personal information) の取得に関しては特に明確な制限を設けていないが、JIS Q 15001 の 3.4.2.3 は、特定の機微な個人情報の取得、利用及び提供の制限を規定している<sup>37</sup>。これは、EU の個人データ保護指令にある同種の要件に対応するものである。

本来、全ての個人情報取扱事業者 (個人データ管理主体) が JIS Q 15001 によって提供される行動基準を尊重して個人情報 (個人データ) の取扱いをすることをそれぞれの管理策 (コントロール) の基本とすることが望ましいといえる。しかしながら、特に重要性を有しない個人情報をごく少量だけ保有している事業者に対しても厳格な管理を要求することは国策上好ましくないとの判断、そして、国家が主務大臣による監督を通じて事業者に対して公権力を行使するというかたちで遵守させることが望ましい行動基準は個人情報 (個人データ) の安全・適正な管理にとって不可欠な重要な個人情報 (個人データ) に限定し、私人である事業者の自由の領域が不当に抑圧されないようにすべきであるという国家権力の謙抑性の観点をも考慮に入れて、国家制度としてのマネジメントシステムは構築されなければならないと考えられた。その結果、訴訟における請求権の行使を含め、個人情報の本人 (個人データ主体) の権利を明確に法定することは見送られたのである。

このような立法政策が正しいものであったのかどうかについては、当然、批判もあり得ることである。現に、昨今の EU における個人データ保護の強化の動向を冷静に検討しながら、内閣府を中心として個人情報保護法の改正作業が進められている。そして、議決機関である国会が個人情報の本人 (個人データ主体) に訴訟上の請求権を認めるべきであると判断するときは、従来の立法政策を変更し、請求権を行使し得るような改正がなされることであろうし、これに伴って多数の関連法令の整備が実施され、新たに最高裁判所規則<sup>38</sup>が制定され、主務大臣である関連各省庁のガイドラインが全面改定されることになるであろう。

しかし、現行法の解釈論としては、個人情報保護法 25 条 1 項の現行の条文のまま「訴訟上の開示請求権を認めるべし」との見解は、立法論に属するものであって解釈論の範疇から大きくはみ出ていると理解するしかない。

以上を要するに、個人情報を保護するための国家による管理策 (コントロール) としての個人情報保護法においても JIS Q 15001 においても、訴訟上の請求権 (裁判規範性) を保留し、強いて言えば、将来の課題として検討を重ねるといふペンディングの状態とすることにしたと理解するのが正しい<sup>39</sup>。

### 3. 3 個人情報保護法 25 条 1 項違反行為の法律効果

個人情報保護法 25 条 1 項所定の開示の求めに対し当該開示を求められた保有個人データを保有する個人情報取扱事業者が、法定の除外事由がないのに、任意の開示をしなかったときは、個人情報取扱事業者の義務に違反する行為をしていることになる。

この義務は、本来は自主管理のためのマネジメントシステム上の行為規範でありながら、その重要性から特に法律によって行為規範として導入することが義務付けられているもの

である。これをマネジメントシステムの側面だけから見ると、予め設定された法定の管理策（コントロール）の不実施ということになる。

マネジメントシステムの基本的な考え方では、管理策を実施しなかった場合の対応策も管理策（コントロール）の一部として予め講じておくのが通例である。例えば、企業内において内部統制というマネジメントシステムが導入されている場合、内部統制上の管理策の一種である内部規律（社内規則、指示等）に反して従業員が適切に対応しなかった場合には、管理主体である経営者によって人事上の措置（懲戒処分等）が実施されることにより、本来期待されていた管理策の実施を実効的なものとするのが期待されている。ところが、個人情報取扱事業者は、個人情報（個人データ）の管理主体そのものであり、管理主体である個人情報取扱事業者を管理する上位の管理主体というものが存在しない。そのため、管理主体自身に管理策実施の懈怠や欺瞞等があるときは、管理主体である個人情報取扱事業者による自己管理・自主管理として管理策の実施を期待することができない<sup>40</sup>。

そのため、個人情報保護法は、公権力主体である主務大臣による是正という方策を国家システム上の管理策として導入している。具体的には、「主務大臣は、この節の規定の施行に必要な限度において、個人情報取扱事業者に対し、個人情報の取扱いに関し報告をさせることができる」ものとされ（個人情報保護法 32 条）、また、「主務大臣は、この節の規定の施行に必要な限度において、個人情報取扱事業者に対し、個人情報の取扱いに関し必要な助言をすることができる」（同法 33 条）、「主務大臣は、個人情報取扱事業者が第 16 条から第 18 条まで、第 20 条から第 27 条まで又は第 30 条第 2 項の規定に違反した場合において個人の権利利益を保護するため必要があると認めるときは、当該個人情報取扱事業者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができる」（同法 34 条 1 項）、「主務大臣は、前項の規定による勧告を受けた個人情報取扱事業者が正当な理由がなくてその勧告に係る措置をとらなかった場合において個人の重大な権利利益の侵害が切迫していると認めるときは、当該個人情報取扱事業者に対し、その勧告に係る措置をとるべきことを命ずることができる」（同法 34 条 2 項）、加えて、「主務大臣は、前 2 項の規定にかかわらず、個人情報取扱事業者が第 16 条、第 17 条、第 20 条から第 22 条まで又は第 23 条第 1 項の規定に違反した場合において個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認めるときは、当該個人情報取扱事業者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべきことを命ずることができる」ものとされている（同法 34 条 3 項）<sup>41</sup>。これらの条項中で個人情報保護法 25 条 1 項違反行為と関連するものは、同法 32 条、同法 33 条、同法 34 条 1 項及び 2 項である。そして、同法 34 条 2 項違反の行為（同法 56 条）及び同法 32 条違反の行為（同法 57 条）には罰則が適用される。しかしながら、主務大臣が個人情報の本人に代わって原告となり、個人情報取扱事業者を被告として、当該開示を求められている保有個人データの開示請求をすることのできる制度や主務大臣が個人情報の本人等に代わって原告となり、個人情報取扱事業者を被告として、損害賠償請求をすることのできる制度等は全く設けられていない（EU 加盟各

国においては、官庁である個人データ保護官がそのような個人データ主体を代理して開示請求をする権限を有することが加盟各国の個人データ保護法によって明定されている。) 42。

要するに、個人情報保護法違反行為の法律効果は、主務大臣による行政権の発動である。違反行為があれば、個人情報の本人について開示請求権が発生するというものではない。

### 3. 4 JIS Q 15001 に反する管理の法律効果

既述のとおり、JIS Q 15001 は、事業者<sup>43</sup>が自己管理・自主管理として個人情報（個人データ）を管理する際に用いる標準的な行動規範を定めるもので、その規範を自己の行動基準とする基本方針（ポリシー）を宣言し、JIS に定める管理策（コントロール）を自己の管理策として導入することとしても、そのことのみによって事業者の顧客や従業員等との間で何らかの契約関係が自動的に生成されるものではない。

このことは、JIS Q 15001 に従うことを基本方針（ポリシー）として宣言した事業者が、JIS Q 15001 所定の管理策に従わなかった場合、または、JIS Q 15001 に準拠して自己の管理策を実施することに失敗した場合でも同様である。JIS Q 15001 に従うものとして自己決定をしたというだけでは当該事業者の顧客や従業員等との間で何らかの契約関係も自動的に生成されるわけではない以上、当該顧客や従業員等との間で何らかの債権債務関係が成立することはないし、その債務不履行が生ずることもあり得ない。

事業者が JIS Q 15001 に違反した場合またはその遵守に失敗した場合、それだけでは何らの債務も生じないことは自明であるが、当該事業者が JIPDEC の審査を受けプライバシーマークの認証を受けている場合、当該事業者の失敗について JIPDEC から不適合の評価を受けると、プライバシーマーク認証の取消または保留の処分を受けることがある。これは、JIS Q 15001 それ自体から発生する法律効果というよりは、JIPDEC との間の認証申請にかかる契約関係に起因して発生するものと理解すべきである<sup>44</sup>。そして、当該事業者が JIPDEC によってプライバシーマーク認証の取消または保留の処分を受けたとしても、そのことのみによって当該事業者とその顧客または従業員との間で何らの債権債務も発生しないこともまた自明である。

### 3. 5 EU 個人データ保護指令との関係

日本国の個人情報保護法 25 条 1 項の規定する開示の求めが請求権性を有するか否かについての議論の中で、EU 個人データとの適合性が論じられるのが通例である。立法当時においても、この点についてかなり深い検討がなされた。

検討がなされた理由は 1 点に尽きる。それは、EU 個人データ保護指令 25 条 1 項が、次のように定めていたからである。

## Article 25 - Principles

1. Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

(ECOM プライバシー問題検討 WG による仮訳)

### 第 25 条 原則

1. 加盟国は、処理されている、又は後に処理される予定の個人データの第三国への移動は、当該第三国が適切なレベルの保護を提供している場合に限られることを規定するものとする。但し、本指令に従って採択された国内規定に対する遵守を害しないことを条件とする。

立法当時、日本国の個人情報保護法が EU の個人データ保護指令に定める個人データ保護の要件と同等の法的保護を与えるものでなければ、同指令 25 条 1 項の第三国移転禁止条項の適用により、EU 域内（EU 加盟国）と日本国（EU から見て第三国）との間の個人データのやりとりができなくなる危険性があるとの危惧感が高まった。

政府部内では、全ての分野にわたって綿密な検討が加えられたが、その中には司法救済に関する条項も含まれていた。EU 個人データ保護指令は、個人データ主体の権利が侵害された場合の司法救済について、下記のように規定している。

## Article 22 - Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

## Article 23 - Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

## Article 24 - Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

(ECOM プライバシー問題検討 WG に基づく仮訳・一部修正)

## 第 22 条 救済

法当局への照会の前に、とりわけ第 28 条に示す監視機関によって規定される行政的救済を害することなく、加盟国は、データ処理に適用される国内法が保証する権利の全ての侵害に対して、司法的救済を受ける権利をあらゆる者に与えるものとする。

## 第 23 条 責任

1. 加盟国は、遵法な処理作業、又は本指令に従って採択された国内規則に反する行為によって損害を被った全ての者に、管理者から損害賠償を受け取る権限を与えるものとする。

2. 管理者は、損害の原因となった事態に対して責任を有しないことを証明すれば、この責任の全部又は一部から免除されることができる。

## 第 24 条 制裁

加盟国は、本指令の条文の完全な実施を確保するために、適切な措置を採択するものとし、特に本指令に従って採択された国内規定の違反に対して課される制裁に関して規定するものとする。

EU 個人データ保護指令 25 条 1 項の要件との関係で検討課題となったのは、同指令 22 条に規定する権利である。そこには、「the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question」と規定されていた。この権利は、加盟国の法令によって個人データ主体に与えられた権利の侵害に対する「司法救済を得る権利」を意味し、加盟国は、そのような権利を保障する国内法を制定しなければならず、また、EU 加盟国と個人データのやりとりをする第三国もまた同等の立法をする必要があった。

ここで問題となるのは、「a judicial remedy for any breach」の意義である。

この表現は多義的である。そのため、当時、そのような理解の可否は別として、日本国の立法担当者の間では、損害賠償請求制度があれば足りると解釈した上で、民法 709 条に基づく損害賠償制度が既に明治時代から存在している以上、特に新規立法をすることを要しないとの意見が大勢を占めていたのである。

このような理解は、ひとり第三国である日本国だけではなく、EU 加盟国の中にもあった。そのため、EU 個人データ保護指令に基づく加盟各国の個人データ保護法が施行され、また、日本国でも個人情報保護法が施行された後、開示請求権、利用停止請求権、消去請求権などのような強い訴訟上の請求権による司法救済を求める人々からは、単に損害賠償請求しかできないとする解釈や立法に対する批判が起きることとなった。

このような議論を踏まえて、EU の個人データ保護規則案 (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) Brussels,

25.1.2012) は、かなり強い権利の保障を定めるものとしてとされていた。それは、規則案の 75 条である。同規則案の司法救済に関する部分及びその総務省訳は、下記のとおりである。

#### Article 75 Right to a judicial remedy against a controller or processor

1. Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority as referred to in Article 73, every natural person shall have the right to a judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.
2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has its habitual residence, unless the controller is a public authority acting in the exercise of its public powers.
3. Where proceedings are pending in the consistency mechanism referred to in Article 58, which concern the same measure, decision or practice, a court may suspend the proceedings brought before it, except where the urgency of the matter for the protection of the data subject's rights does not allow to wait for the outcome of the procedure in the consistency mechanism.
4. The Member States shall enforce final decisions by the courts referred to in this Article.

(総務省による仮訳)

#### 第 75 条 管理者もしくは処理者に対して司法救済を求める権利

1. 第 73 条の監督機関への不服申し立ての権利を含むあらゆる行政救済を毀損することなく、各自然人は、本規則に準じない個人データの処理によって本規則に基づく自らの権利が侵害されたと考える場合、司法救済を求める権利を有するものとする。
2. 管理者または処理者に対する訴訟は、管理者もしくは処理者が施設を有する加盟国にて提起されるべきものとする。管理者が公権力を行使する公的機関である場合を除き、当該訴訟をデータの対象者が住まう加盟国にて提起しても良い。
3. 同様の措置、決定または実施に関する訴訟が第 58 条の整合性機構においても係争中である場合、データの対象者の権利を保護する上で、整合性機構の手順の結果を待つことができないほど緊急の場合を除き、裁判所は訴訟を保留することができる。
4. 加盟国は本条における裁判所による最終判決を履行するものとする。

この条項案とは別に、規則案 77 条は、損害賠償請求について規定している。この 77 条 3 項は、過失の立証責任を転換している点で極めて重要なものである。

#### Article 77 Right to compensation and liability

1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.
2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.
3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.

(総務省による仮訳)

#### 第 77 条賠償を受ける権利と法的責任

1. 違法な処理操作もしくは本規則に適合しない活動の結果により損害を受けた者は、受けた損害に対し、管理者もしくは当該被害を引き起こした処理者から賠償を受ける権利を有するものとする。
2. 当該処理に 2 人以上の管理者もしくは処理者が関与する場合、各管理者もしくは処理者は被害総額に対する連帯責任を負うものとする。
3. 管理者もしくは処理者がその損害を引き起こした事象に対して責任がないことを証明する場合、同者はその一部もしくは全ての法的責任を免れる。

この規則案 75 条は、は、損害賠償請求（規則案 77 条）とは別に規定されているところから、通常は、損害賠償請求とは別の請求権を意味すると解されている。しかし、77 条は、直接の加害者だけではなく関連する者の間での連帯責任と証明責任に関する特則を定めるものであり、75 条の責任が損害賠償責任以外の責任のみを意味するものではないと解釈する余地を残していると言えないわけではない。これは、EU 域内においても、損害賠償責任よりも強い何らかの行為請求権を認めることについて消極的な意見があることの反映であり、いかようにも解釈可能にしてあると推定することは可能である。

しかしながら、EU 個人データ保護指令における司法救済規定の定め方と比較すると、より強力な請求権を法定すべき要求が高まっているという事実を反映していることは明らかである。

このことから、立法論としては、現行の個人情報保護法を改正しなければならない国際的圧力が高まっているということを否定することはできないと考える。しかしながら、翻って考えてみると、EU の個人データ保護指令が制定された当初においては、基本的には損害賠償請求のみで十分であるという考え方が主流で、そのような考え方に対する批判の高まりを受けて個人データ保護規則案の提案に至っているということ是可以する。

それゆえ、結局、個人情報保護法 25 条 1 項が、立法当初から裁判規範性を有していたのではなく、日本国の個人情報保護法の立法の時点では民法 709 条による損害賠償請求で足

りと考えられていたところが、その後の EU 域内における社会情勢の変化に伴い、より強い請求権の法定を求める声が高まっているのが現状だと判断するのが妥当である。

### 3. 6 行政機関個人情報保護法における開示請求との相違

行政機関の保有する個人情報の保護に関する法律（平成 15 年法律第 58 号・以下「行政機関個人情報保護法」という。）12 条 1 項は、「何人も、この法律の定めるところにより、行政機関の長に対し、当該行政機関の保有する自己を本人とする保有個人情報の開示を請求することができる」と規定し、国（行政機関）の保有する国民の保有個人データについて、開示請求権の存在を認めている。

法哲学的には、国が保有する国民の個人情報（個人データ）は、本来主権者である国民自身が保有する情報財の一種であり、それを国が信託的に譲渡を受けて管理しているのに過ぎないと理解することができる。米国においてはこのような考え方が特に強く、米国連邦政府が保有する公文書等の公開に関する基本原則は、本来国民の財産であるべき公文書について一定の公開制限を設けつつも、所定の期間経過と同時に制限を解除し、本来の権利者である国民が自由にその情報を入手し利用することができるようにすべきであるとの民主主義の理念に基礎を置くものである。米国連邦の公文書館である国立公文書記録管理局（United States National Archives and Records Administration）と米国連邦議会図書館（Library of Congress）は、そのための重要な政治的・歴史的役割を担ってきたし、米国連邦最高裁の判例は、国民の情報公開の権利を確保するために最大限の司法的・歴史的役割を果たしてきた。

このことは、日本国の法制及び日本国の裁判所でも基本的には同じである。日本国の行政機関の保有する情報の公開に関する法律（平成 11 年法律第 42 号・以下「情報公開法」という。）は、そのような米国におけるのと同じ民主主義の理念に基づいて制定されたのであり、また、日本国の裁判所は、国や地方自治体等の管理する公文書の情報公開について大きな役割を果たすことによって、日本国の民主主義の実質化に大いに寄与してきた。これは、まさに法の支配（rule of law）を象徴するものだと言える。

ところで、純理論的には、情報公開法に基づき、国民が請求者となって、国に対し、国が保有する当該国民の個人データの開示を請求することができるはずである。個人データもまた電子化された公文書として存在しているからである。しかしながら、個人データは、当該個人データによって識別可能な個人（国民）にとっては情報公開を求める利益が原則として正当かつ適法なものとして認められるべきものである一方、他方では、当該国民以外の第三者に無制限で公開されると、当該国民とそれ以外の第三者である者との間でプライバシー侵害や名誉棄損等の紛争が生ずるおそれのあるものが多々含まれること大いに予想されることから、開示請求権の存在それ自体については特に異論がないにしても、開示請求権者の範囲及び開示する情報（データ）の範囲・内容について一定の制限を設けないと、却って

公益に反する結果となることがあり得る。

行政機関個人情報保護法 12 条 1 項所定の開示請求権は、以上のような趣旨から、理論的には、情報公開法の特別法としての位置づけを有すると解することができる。

したがって、私人間の法律関係における個人情報（個人データ）の管理に関する基本的な行動規範を自主管理・自己管理のための行動規範として定め、その違反行為について、公権力である主務大臣の監督によって行動規範としての実効性を担保すべく制定された個人情報保護法における基本構造とは全く異なるものだと理解することができる。行政機関個人情報保護法に基づき開示を求めることのできる情報は、本来（民主主義の理念上では）、開示請求者自身のものであり、それを国が信託的に管理しているだけであるので、いわば寄託物の返還請求に近い論理構造をもっている。

これに対し、私人間においては、本来（思想信条の自由、財産権の自由にに基づき）、私人である個人情報取扱事業者が自己のものとして保有・管理する個人情報（個人データ）に対し、当該個人情報取扱事業者からみると他人であり同等に私人である個人情報の本人による関与を部分的に認めるものであり、その意味では、私有財産権に対する一定の制限を認めるための法制であると理解することもできる。そのような個人情報取扱事業者が保有する私有財産である個人情報（個人データ）の使用・収益・処分等に一定の制限が加えられることは、形式的には基本的人権の侵害を構成するものではあるが、そのような制限を加えることが国際協調主義の建前からも個人情報の本人の側の人権保障の観点からも公益に適ったものとして国会により承認された結果、公共の福祉による制限の一種として妥当なものとして個人情報保護法上によって規律される法律上の義務として存在していると考えられるのである。

このように、行政機関個人情報保護法 12 条 1 項における保有個人データの開示請求権と個人情報保護法 25 条 1 項における開示の求めとは、その法哲学的根拠を全く異にするものである。以上のことは、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（平成 15 年法律第 59 号）の場合も同じであり、行政機関個人情報保護法に準じて考えることができる。各地方自治体が制定している個人情報保護条例及び情報公開条例についても、同じである。

これらの開示請求権と開示の求めを一律に解し、全て「自己情報コントロール権」なる概念で一元的に理解しようとする説は、現実に存在した立法の経緯や立法事実という歴史的事実と完全に相反するというだけではなく、理念的にも基本的な誤謬や誤解を含むものであり、全く考慮に値しないと断言することができる<sup>45</sup>。

### 3. 7 裁判例

個人情報保護法 25 条 1 項に基づく開示の求めについて裁判規範性が争われた事案の裁判例として、東京地裁平成 19 年 6 月 27 日判決・判例タイムズ 1275 号 323 頁がある。同判決

は、個人情報保護法 25 条 1 項に基づく裁判上の開示請求の可否(裁判上の請求権性の有無)について、次のように判示して、消極の立場を明らかにしている。私見としては、判旨に賛成である。

(1) 原告らは、法 25 条 1 項について、本人が個人情報取扱事業者に対して保有個人データの開示を裁判上請求する権利を有することを規定したものであると主張する。

(2) しかしながら、前記法令の定めによれば、法は、25 条 1 項による開示の求め等に関する苦情の処理については、個人情報取扱事業者、業界団体による自主的な紛争解決を期待しており、そのために、本人が裁判外の各種の方法によって苦情の解決を求められる仕組みを設けるとともに、そのような自主的解決が期待できない場合の主務大臣による関与の仕組みを設けているものといえる。

すなわち、法は、広汎で多種多様な保有個人データの取扱いに関する苦情を第一次的には当事者間の自主的解決にゆだねる趣旨で、個人情報取扱事業者自身が、窓口等を設けて個人情報の取扱いに関する苦情の適切かつ迅速な処理をし、この目的を達成するために必要な体制の整備をする責務を努力義務として負っている旨を規定しつつ(法 31 条)、認定個人情報保護団体が、本人等から対象事業者の個人情報の取扱いに関する苦情について解決の申出があったときは、その相談に応じ、申出人に必要な助言をし、その苦情に係る事情を調査するとともに、当該対象事業者に対し、その苦情の内容を通知してその迅速な解決を求めなければならないと規定している(法 42 条 1 項)。

そして、法は、このような個人情報取扱事業者や認定個人情報保護団体による自主的解決が期待できない場合には、主務大臣において、個人情報取扱事業者から個人情報の取扱いに関して報告を徴収し、必要な助言をすることができるほか、個人情報取扱事業者が法 25 条等の規定に違反した場合において、個人の権利利益を保護するために必要があるときは、違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができ、個人情報取扱事業者が正当な理由がないのにその勧告に係る措置をとらなかった場合において個人の権利利益の侵害が切迫していると認めるときは、当該個人情報取扱事業者に対し、その勧告に係る措置をとるべきことを命ずることができるとしている(法 32 ないし 34 条)。さらに、法は、それらの主務大臣の措置の実効性を確保するために、法 32 条の報告徴収に違反した者は 30 万円以下の罰金に、法 34 条 2 項の命令に違反した者は 6 月以下の懲役又は 30 万円以下の罰金に処するものとしている(法 56、57 条)。なお、主務大臣は、認定個人情報保護団体に対しても、報告の徴収(法 46 条)、命令(法 47 条)、認定の取消し(法 48 条)という監督手段を行使することができるものとされている。

このような法の規定にかんがみると、法は、個人情報取扱事業者が法 25 条等の規定に違反した場合には、当該個人情報取扱事業者や認定個人情報保護団体による自主的解決及び主務大臣による行政上の監督によって、個人の権利利益を保護することとしているものと解される。

仮に、本人が、法 25 条 1 項に基づいて個人情報取扱事業者に対する保有個人データの開示を裁判手続で請求することができるかと解すると、法が上記のとおり定めた当事者間における自主的解決手段や主務大臣による紛争解決手段によるよりも裁判上の請求の方が直裁であるとして、法の定めた紛争解決手段によることなく、直接裁判上の開示請求がされることになり、紛争解決手段に関する法の規定が空文化することにもなりかねない。

(3) また、前記の法令の定めのとおり、個人情報取扱事業者は、法 25 条 1 項の開示の求め等に関し、その求めを受け付ける方法を定めることができる（法 29 条 1 項）上、当該開示の実施に関し、手数料を徴収することもできる（法 30 条）。ところが、本人が法 25 条 1 項に基づき個人情報取扱事業者に対する保有個人データの裁判上の開示請求ができるとなると、このような規定も適用の余地がなくなるが、法は、このような事態が生ずることを予定していないというべきである。

(4) さらに、法 25 条 1 項は、その標題が「開示」とされ、個人情報の開示を専ら個人情報取扱事業者の義務として規定し、本人が開示請求権を有することを規定していないことからすると、同項は、文言上も、行政機関（主務大臣）に対する義務として個人情報取扱事業者の開示義務を規定しているものであって、本人が開示請求権を有する旨を規定しているものではないと解される。

(5) 以上によれば、法 25 条 1 項が本人に保有個人データの開示請求権を付与した規定であると解することは困難であって、本人は、同項の規定に基づき、個人情報取扱事業者に対し、保有個人データの開示を裁判手続により請求することはできないというべきである。

そうすると、争点(2)及び(3)について判断するまでもなく、原告らの請求のうち、本件各診療録の開示を求める部分は理由がない。

この判決における個人情報保護法の基本構造の理解は、個人情報取扱事業者（個人情報管理主体）による自主管理を基本とするマネジメントシステムの考え方を法規範の形式で形成したもののだとの考え方を基礎としている。そして、このような理解は、同法の立法経緯及び立法事実とも正確に適合するもので、裁判所の判決理由中の説示としては、これ以上のものを望むことができない非常に高いレベルに達していると評価することができる。

この判決に対する批判的な見解も散見されるが<sup>46</sup>、いずれも学術的価値の乏しいものであり、考慮に値しない<sup>47</sup>。

### 3. 8 裁判上の請求権性を否定する学説

学説上、請求権性（裁判規範性）を否定する見解は多数あり、実質的には優勢な見解だと考える<sup>48</sup>。また、司法的救済に関して不法行為（民法 709 条）に基づく損害賠償請求をなし得ることに触れる程度で、積極的な行為請求権（開示請求、利用停止請求等）については全く触れていない学説が圧倒的に多い<sup>49</sup>。推測としては、消極説の立場にたちつつも諸般の事

情を考慮して意図的に触れていない場合が非常に多いのではないかと推察される。

個人情報保護法案のとりまとめにあたり大綱を確定する作業の責任者であった堀部政男氏が否定説であることは言うまでもない<sup>50</sup>。

世界各国の個人データ保護法制及びプライバシー保護法制の比較法的研究において重要な研究業績を多数著してきた石井夏生利氏は、現行の個人情報保護法の制定過程を綿密に調査した上、他の関連法令との条文構造上の相違を重視し、前掲東京地裁平成19年6月27日判決の判旨に賛成し、個人情報保護法25条1項の開示の求めの裁判規範性について否定説の立場を明らかにしている。なお、同氏は、個人情報開示請求権の必要性を否定するものではなく、あくまでも現行法の解釈論としては、個人情報保護法25条1項が裁判規範としての請求権を認めたものと解釈するのは無理だとの立場を採っている<sup>51</sup>。

長年にわたり JIPDEC 及び JISA におけるプライバシーマーク制度の確立・運用・再評価に関与し、現在でも内閣府等の個人情報保護と関連する重要な業務に従事している鈴木正朝氏は、他の法令に基づく情報開示請求の場合と比較して個人情報保護法25条1項の開示の求めでは開示手続に関する条項が全くなく、その執行方法も不明であることや、安易に裁判規範性を肯定することによる弊害が大きいこと（特に利益考量の余地がなくなる危険性が高いこと）、前掲東京地裁平成19年6月27日判決が消極的な見解を示していることなどを考慮に入れた上で、肯定説の論拠が薄弱であることを指摘し、個人情報保護法25条1項の開示の求めの裁判規範性について否定説の立場を明確にしている<sup>52</sup>。

一般社団法人電子情報技術産業協会情報政策委員会（JEITA）「EU データ保護指令改定に関する調査・分析報告書」（2012年3月）43頁は、EU 個人データ保護規則案の75条が個人データの管理者（日本国における個人情報取扱事業者に相当）に対して訴訟を提起し司法救済を受ける権利を明記していることと日本国の個人情報保護法及び JIS Q 15001 との対応関係について、「個人は、個人情報取扱事業者や認定個人情報保護団体に対して個人情報の取扱いに関する苦情を申し出ることができる（第31条、第42条）が、事業者における個人情報の取扱いに対して個人が当該事業者に対する訴訟を行う等の、司法手続による救済については同法上で規定されていない」、また、「JIS Q 15001 では、司法手続による救済については規定されていない」としている。すなわち、明白に完全否定説の立場をとっている<sup>53</sup>。この見解は、裁判所における訴訟という解決方法を法定する場合のモデルを EU の個人データ保護指令及び個人データ保護規則案に求めた上で、条文構成の比較検討の上で形成されたもので、学術的には比較法的検討の結果というべきもので、十分に傾聴に値する論拠が示されていると認めるべきである<sup>54</sup>。

私見は、開示を求める請求権の必要性は認めるがそれは立法論なのであり、現行の個人情報保護法25条1項の規定の法解釈論としては、「開示の求め」の請求権性（裁判規範性）について否定説の立場を採ってきた<sup>55</sup>。裁判規範として機能する請求権を確立するという立法政策を是とする場合<sup>56</sup>には、その執行方法に関する手続条項等を含め、請求権として機能し得るような法律要件及び法律効果を明確に示す条項として構成されなければならないし、

請求権行使の対象等について妥当な範囲とするための十分な事前検討を要すると解する。現行の個人情報保護法 25 条 1 項の規定のままでは、法律要件及び法律効果が曖昧である。そしてまた、単純に請求権性を肯定すると、その請求権の無条件な行使を認めると、そのことによる社会的な弊害があまりにも大きすぎる。それゆえ、現行法のままでは裁判規範性を認めることができない。

## 4 まとめ

以上の検討を踏まえると、本検討課題に対する検討結果は、次のとおりである。

### 4. 1 個人情報保護法 25 条 1 項の裁判規範性

個人情報保護法 25 条 1 項所定の開示の求めに裁判規範性はない。

個人情報の本人は、同法 25 条 1 項に基づき、開示を求める保有個人データを保有する個人情報取扱事業者に対し、民事訴訟によってその開示を求める請求権を有すると解することはできない。

同法 25 条 1 項の義務の違反行為がある場合、その違反によって開示請求権が発生すると解すべき余地もない。

同条 25 条 1 項の違反があった場合の法律効果は、主務大臣による行政監督権の行使である。そして、その行政監督権に対して個人情報取扱事業者が従わない場合には、罰則の適用があり得る。

このような行政法上の公権力の行使によって、マネジメントシステムとしての個人情報取扱事業者における保有個人データの取扱いの適正を確保しようとするのが個人情報保護法の基本構造である。

### 4. 2 JIS Q 15001 の裁判規範性

JIS Q 15001 は、自己管理・自主管理のための行動規範に過ぎず裁判規範性はない。

個人情報の本人は、JIS Q 15001 に基づき、個人情報を保有する事業者に対し、民事訴訟によってその開示を求める請求権を有すると解することはできない。

JIS Q 15001 に準拠した管理策を導入した事業者は、その導入によって、または、導入した管理策の審査を経て JIPDEC からプライバシーマークの認証を受けたことによって、当該事業者以外の者（顧客や従業員等）との間で自動的に何らかの契約関係が発生するというとはあり得ない。

JIS Q 15001 の遵守に関する失敗があった場合でも、そのことのみによって当該事業者以外との間で何らかの契約上の債務不履行関係が生ずることはあり得ない。JIS Q 15001 所定

の管理策の不順守やその実施の失敗がある場合、そのことによって開示請求権が発生すると解すべき余地もない。

プライバシーマーク制度は、プライバシーマークの認証を受けておりながら JIS Q 15001 の定める行動規範に反する事業者について、その違反行為を JIPDEC が事後評価することによって、プライバシーマーク認証について取消または留保の処分をすることにより、その実効性が担保されている。しかし、そのことによって、当該事業者とその顧客または従業員との間で自動的に何らかの債務が生ずるということとはあり得ないことである。

以上

---

[注記]

<sup>1</sup> 夏井高人・岡村久道・掛川雅仁編『Q&A インターネットの法務と税務』（新日本法規、2001）543～570ノ5 [2014年10月30日加除版]

<sup>2</sup> 例えば、電子的な処理を一切行わず、紙の書面に記載または印刷された個人情報のみを取り扱う事業者については、物体としての紙の汚損・滅失・盗難等を物理的に防止するための管理策（例：耐震・防水・耐火性のある堅牢な金庫の適切な使用等）が明示され実施可能であるか否かが認証審査の対象となる。これに対し、電子的な処理のみを行う事業者については、電磁的記録の改変・消去・無権限アクセス（不正アクセス禁止法2条4項所定の不正アクセス行為に該当しない無権限アクセス行為を含む。）等を電子的に防止するための情報セキュリティを重視した管理策（例：アクセス管理技術、監視技術、ファイアウォール技術、暗号化技術の適切な使用等）が明示され実施可能であるか否かが認証審査の対象となる。他方において、例えば、顧客情報、医療受診者情報、従業員情報ではそれぞれ法的性質が異なり、顧客情報では消費者契約法（平成12年法律第61号）4条に規定する「重要事項」の明示の要件との関連で、仮にそれが契約の意思表示の要素となっていない場合であっても、条理上、契約の付随義務の一種として（契約に基づく債務の一種として）顧客の個人情報の開示が認められる場合があり得る（最高裁平成17年7月19日判決・民集59巻6号1783頁参照）。これに対し、医療受診者情報では、無条件で情報を開示することにより医療の円滑・合理的な遂行に著しい支障が生ずることがあり得るため、診療契約の付随義務としても情報開示義務が比較的制限的にとらえられるべき場合があり得る（東京地裁平成19年6月27日判決・判例タイムズ1275号323頁参照）。また、労働契約においては、労働契約法（平成19年法律第128号）に所定のとおり、基本的には労働基準局が関与してその妥当性が基礎づけられる労働協約及び就業規則の規律する集団的な合意から法解釈により導き出される付随義務を抽象的に観念することは可能であるものの、労働関係は使用者の企業経営のための手段の一つとして存在しており（例えば、使用者以外には全てロボットが業務を担当しており、人間の従業員が存在しない事業所では労働関係がそもそも一切成立しない。これは、ロボットは人間ではないため、人間である労働者を必須の構成要素とする労務管理が存在しないことによる。そして、人間である労働者を用いて事業を遂行するか、人間ではない機械装置であるロボットを用いて事業を遂行するかは、単に経営者の経営判断と経営手段の選択の自由の領域に属する。）、か

---

つ、労働契約の本質上、労働者は使用者の指揮命令に従って労務を提供すべきものであり、使用者の指揮命令に関する重要事項については機密性の高いものがあり、また、それを無条件で開示することにより事業全体の遂行に著しい支障を発生させ得る場合がある。このように、契約上の義務（条理上の付随義務）として情報開示請求権を承認する場合であっても、個々の契約類型の特質に対応した個別の検討に基づき当事者の合理的な意思等を推測し、または、当該契約類型に即した適切な条理を推知すべきものである。換言すれば、個々の契約類型の特質を無視して一律に適用されるようなものとしては、付随義務としての開示請求を認めることはできない。現に、内外の裁判例もそのような一律の請求権なるものの存在を全く認めていない。

<sup>3</sup> 被控訴人（原審被告）の認証項目 12 に「直接書面取得」との括弧書きがあるのは、個人情報保護法 18 条 2 項本文所定の「本人との間で契約を締結することに伴って契約書その他の書面（電子的方式、磁気的方式その他の知覚によっては認識することができない方式で作られる記録を含む。以下この項において同じ。）に記載された当該本人の個人情報取得する場合その他本人から直接書面に記載された当該本人の個人情報取得する場合」に限定する趣旨と解釈するのが妥当である。すなわち、同条 2 項ただし書に規定する場合を含め、直接書面取得以外の取得については、JIS Q 15001 に基づくプライバシーマーク認証を受けておらず、プライバシーマーク制度における審査・認証機関である JIPDEC が一切関知するものではないことになる。

<sup>4</sup> JIS Q 15001 の 3.4.4.5 は、「保有個人データ」ではなく「個人情報」と規定している。ここで「個人情報」とあるのは、個人情報保護法 2 条 1 項に定義する「個人情報」と同義ではない。JIS Q 15001 の 3.4.4.5 の「個人情報」は、個人情報の管理主体が取得し、管理している個人データの中で、開示や第三者提供等の処分をすることのできる権限を有するものに限定される。このことは、管理者にとって開示権限のないデータについては、法的には開示不能であるので、自明と思われる。その結果、JIS Q 15001 の 3.4.4.5 の「個人情報」は、個人情報保護法 2 条 5 項及び同法 21 条 1 項所定の「保有個人データ」と同義と解釈するのが正当である。JIS Q 15001 においては、管理権限のある者の管理のための基本指針と管理策としての標準的な行動指針を提供しているので、取得した個人情報であっても管理対象外として個人情報データベースに格納されていない非個人データについては適用がないし、また、個人情報データベースに格納され個人データとして扱われるものであっても開示や第三者提供の権限を有しないものについては、「開示や第三者提供のような処分行為をしないようにすること」を適正に実施するための管理策が適用されることになる。

<sup>5</sup> 一般に、プライバシーマークの更新の申請があった場合、認証者である JIPDEC は、認証した事項について、JIS Q 15001 所定の基準に従った個人情報の管理がなされているか否かだけを審査し、その審査の結果として適合性が肯定されれば、認証の更新がなされる。このことは、プライバシーマーク制度に限ったことではなく、全ての種類の認証制度について妥当することであり、認証としての社会的意義を有するのは、認証の対象として限定された事項についてのみである。認証された事項以外の事項についても JIS Q 15001 所定の基準を安易に類推適用すると、その負担に耐えることができず認証を辞退する事業者が続出し、他方では、認証機関においても認証していない事項や申請されていない事項についての審査や評価をせざるを得なくなるが、そのようなことは物理的に全く不可能なことなので、認証業務それ自体を廃止せざるを得なくなり、結果的に、認証制度それ自体が全面的に崩壊することが確実に予想される。それは、社会秩序全体に対して大きな脅威と不安定要素をもたらすものである。それゆえ、安易な類推適用は決して許されることではない。

<sup>6</sup> プライバシーマーク制度における審査・評価・運用の基本的事項については、財団法人日本情報処理開発協会プライバシーマーク推進センター編『JIS Q 15001: 2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン（第 2 版）』（日本規格

協会、2010)、堀部政男監修(鈴木正朝・新保史生・齊藤雄一・太田克良)『JIS Q 15001: 2006 個人情報マネジメントシステム要求事項の解説』(日本規格協会、2006)が参考になる。なお、財団法人日本情報処理開発協会(JIPDEC)プライバシーマーク推進センターのWebサイト上では、プライバシーマーク制度の概要説明が公開されている。

<sup>7</sup> JIS Q 15001 の認証取得事項において「Web サイト他により従業員等から日立が直接個人情報を取得(直接書面取得)」の場合のみに限定されているのは、それが常務としての従業員管理情報であるからに他ならない。危機管理情報の多くは、第三者からの苦情等によって不定期に取得されるものであり、あるいは、そのような第三者から提供された情報に基づく経営主体の調査結果・考察・評価・判断の結果等を記録したものである。そのような危機管理情報は、その中に従業員の個人情報が含まれることがあっても、通常の個人情報(個人データ)とは全く異なる取扱いがなされる。

<sup>8</sup> 個人情報の保護に関する法律施行令2条所定の個人情報数の数量要件については、合理性がないものとして法改正により撤廃すべしとの意見があるが、現段階では立法論にとどまる。なお、同条の適用に際しては、個人情報の種類毎に分割して考察するのが妥当である。例えば、6か月以上の期間にわたり常時5000件を超える数量の顧客情報を有する事業者は、当該顧客情報に属する個人情報に関しては個人情報データベースを構成する個人データを保有していることとなり得る。しかし、当該事業者の友人が非常に少ない場合には、当該友人の個人情報について同施行令2条所定の個人情報データベースが存在しているとは言えない。このような場合、当該友人の個人情報を合算した上で、全ての種類の個人情報について個人情報取扱事業者として扱われるわけではない。それゆえ、一般に、危機管理情報が常に僅少にしか存在しない場合、当該危機管理情報に含まれる個人情報については、同施行令2条所定の除外事由に該当し得ることになるので、当該危機管理情報について個人情報取扱事業者となるわけではない。

<sup>9</sup> 行政文書の情報公開請求をする場合に、当該公開を求める文書の存在については、請求者である原告が主張・立証すべきものと判断した裁判例として、最高裁平成26年7月14日判決・判例タイムズ1407号52頁がある。なお、個人情報保護法の解釈・適用上の問題としては、同法25条に基づく開示の求めがあった場合において、当該保有個人データが存在しない場合には、当該求められた個人情報取扱事業者は、当該求めている者に対し、単に「存在しない」との事実を通知すれば足りる(同法25条1項柱書本文括弧書)。そのため、「存在しない」と通知を受けた場合には、当該保有個人データが存在することを前提にしてその開示を求める者は、上記最高裁平成26年7月14日判決に示されている判旨に従い、当該保有個人データの存在を主張・立証すべきであると解する。

<sup>10</sup> 企業における粉飾決算事例や詐欺事例にみられるような企業または会計監査法人等によって秘匿された書類等(いわゆる裏帳簿と呼ばれる会計書類や帳票類、財産隠匿や粉飾決算のための指示書等)については、その適法・違法の観点を度外視すると、当該企業にとっての危機管理情報の一種であり得るし、秘匿の要請の最も高いものであり得るかもしれない。しかし、このような犯罪事例では、当該書類を秘匿することについて正当な法的利益を認めることがあり得ない。それどころか、そのような犯罪を構成する物件は、犯罪組成物件または犯罪供用物件として没収の対象とされるべき場合があり、また、当該犯罪の立証のための証拠として押収・差押の対象とされるべきものである。その点で、このような粉飾決算等と関連する危機管理情報は、通常の業務を遂行している健全な企業において適正・適法に管理されている危機管理情報とは全く異なる法的評価を受けるべきものだという事に留意すべきである。

<sup>11</sup> 個人情報保護法25条1項が請求権の発生を認める条項であるとの解釈論を前提とする場合、その請求権の発生原因となる法律要件に該当する事実の主張・立証責任は、その請求権の存在によって利益を受ける開示請求者にあると解することになる。したがって、開示を求める情報が個人情報保護法25条1項所定の「保有個人データ」に該当することの主張・立証責任もまた、開示請求者にあると解することになる。そして、その請求権の

発生要件の一つである「保有個人データ」の要件の充足性が認められない限り、具体的な請求権としては何も発生していないことになるのは当然のことである。

<sup>12</sup> EUにおける個人データまたはプライバシー保護法制の最近の動向については、Serge Gutwirth, Ronald Leenes, Paul de Hert, Yves Poullet (eds.), *European Data Protection: Coming of Age*, Springer, 2014、Serge Gutwirth, Ronald Leenes, Paul de Hert (eds.), *Reforming European Data Protection Law*, Springer, 2014、ENISA, *The right to be forgotten – between expectations and practice*, October 2011、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未来像』(勁草書房、2014) 43～202 頁が参考になる。

<sup>13</sup> OECD のガイドラインは、2013 年に改正された。その詳細及び日本国法に対する影響については、堀部政男・新保史生・野村至『OECD プライバシーガイドライン－30 年の進化と未来』(JIPDEC、2014)、前掲『個人情報保護法の現在と未来－世界的潮流と日本の未来像』12～42 頁が詳しい。

<sup>14</sup> 世界各国の個人データ保護法及びプライバシー保護法並びにその最近の動向等については、前掲『個人情報保護法の現在と未来－世界的潮流と日本の未来像』、消費者庁「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」(平成 20 年 3 月)、消費者庁「個人情報保護における国際的枠組みの改正動向調査報告書」(平成 26 年 3 月 28 日)、宮下紘「個人情報保護の執行制度に関する比較法的考察」電気通信に関する政策、法律、経済、社会及び産業面等からの研究調査報告書 27 号 62～77 頁、堀部政男・石井夏生利・高木浩光・坂本団・小向太郎「パネルディスカッション：個人情報保護法制のグローバルダイナミズム」情報ネットワーク・ローレビュー13 卷 1 号 154～167 頁、Solove Schwartz, *Information Privacy Law* (3d edition), Aspen Publishers, 2009, pp.995-1071 が参考になる。

<sup>15</sup> 理念としての自己情報コントロール権の主張の当否及び自己情報コントロール権の考え方が米国の自己申告型プライバシー保護認証業者 TRUSTe (トラストイー) のような特定の業者の商業宣伝広告のために主に商業利用されてきたという歴史的事実が存在すること、自己情報コントロール権なる考え方が比較法という観点から世界的に考察してみた結果として優性な理論であるとは到底認められないこと、以上のようなあまり感心できない諸事情が存在したという歴史的事実はさておき(これらの諸点については、本意見書の本来的目的から逸脱することになりかねないので、詳論を割愛する。)、あくまでも要件事実論的に考察した場合、自己情報コントロール権なる理論は、請求権の発生の有無について全く影響を与えることがないという意味で理論的には無意味な考え方である。このことについては、前掲「労働災害と関連する保有個人情報の開示請求と開示拒否事由」でごく簡単に触れたとおりである。なお、現時点において、自己情報コントロール権という考え方が世界的に承認されているか否かという点について付言しておく、明確に否である。日本国においては、憲法学者を中心に肯定説が強い。しかし、これは、日本国だけに限定されたかなり奇妙な現象だと評価するしかない。米国においては、プロッサーのプライバシー理論(いわゆる 4 類型説)がリスティメントやモデル法等を通じて完全に定着しており、プロッサーの理論の延長線上で裁判実務が運営されている(新保史生『プライバシーの権利の生成と展開』(成文堂、2001)、石井夏生利『個人情報保護法の理念と現代的課題－プライバシー権の歴史と国際的視点』(勁草書房、2008) 121～205 頁、佐々木秀智「パブリシティ権とアメリカ合衆国憲法修正第 1 条」法律論叢 84 卷 2・3 合併号 331～364 頁参照)。英国においては、独自の判例理論が存在し、自己情報コントロール権という概念を用いていない。ドイツにおいては、法理論としては人格権の理論が顕著に優性であり(この理論は、EU における基本的人権としての個人データに関する権利の理論との親和性が最も高い。米国の判例法においては財産権としての理論的位置づけが濃厚であることと対照的である。)、実定法の解釈論としては「個人データに関するデータ主体の権利」との概念で確定しており、関連書籍や裁判例等をつぶさに調査してみても「自己情報コントロール権」との用語が出現する例を見出すことは極めて困難である(ドイツの連邦個人データ

保護法における「情報の自己決定権 (Recht auf informationelle Selbstbestimmung)」は、「自己情報コントロール権」と似た印象を受ける用語であるが、制度的に異なるものを概念内容としており、ドイツの個人データ保護法領域における学説上では、ドイツ連邦憲法 2 条 1 項に規定する人格権または人格的権利 (Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit) に由来するものと解するのが通説である。普通の私人にとって自己決定できる場面は限られており、せいぜい秘匿している私的秘情報情報を他者に提供するかどうかの意思決定の場面くらいに限定されている。それゆえ、自己決定のための決定的な場面として、EU の法制では、提供に際しての事前の承諾 (Consent) の重要性が認識され、明確に法制化されているのである。なお、ドイツ連邦憲法上の基本権としての人格権または人格的権利は、日本国憲法では、13 条に規定する自由権と同様の権利を意味するものとして理解することができる。また、同様の理念は、日本国の個人情報保護法 3 条の「個人情報とは、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることにかんがみ、その適正な取扱いが図られなければならない」との規定に反映されていると考えることもできる。すなわち、同条にいう人格的利益は、日本国憲法 13 条の自由権と同様または類似する法的性質を有すると解することができる。日本国の研究者の中には語としての形式的な類似性だけにとらわれ、いわゆる「自己情報コントロール権」なるものと完全に同義のものとして扱っている者もあるが、基本的に研究不足に起因する誤りであるので、注意を要する。)。フランスでは、単純に、EU 個人データ保護指令に基づいて制定された法令上の文言を用いて学説・判例が形成されており、著名な学術書や論文等の中で特に意識して「自己情報コントロール権」を用いている例はない (市川直子「フランスにおける個人データ保護法制」城西大学経済経営紀要 23 巻 37~66 頁、清田雄治「フランスにおける個人情報保護法制と第三者機関-CNIL による治安・警察ファイルに対する統制」立命館法學 300・301 号 145~181 頁が参考になる。)。更に、インターネット上で「自己情報コントロール権」を英語で表現したものと推定されるものの出現率を調査してみても、日本人の誰かが英語で無理に表現したものと推定されるコンテンツ等は散見されるものの、英語で書かれた正規の学術論文等として自己情報コントロール権なるものを承認するものを見出すことはできない。日本国において「自己情報コントロール権」として知られている概念の元となった英語表現は、「the basic attribute of an effective right of privacy is the individual's ability to control the circulation of information relating to him」(Arthur R. Miller, Assault on Privacy: Computers, Data Banks, & Dossiers, University of Michigan Press, 1971, p.25) である。そこで用いられている用語は能力または機会を意味する「ability」なのであって、法的権利を意味する「right」ではない。それゆえ、英語表現による「自己情報コントロール権」と関連する論文等を探してもほとんど存在しないのと同然なのは、当然の結果といえることができる。概念内容としては、「自己に関連する情報の流通について関与することのできる能力 (関与する機会の確保)」を意味する。このような関与する機会の確保は、OECD のプライバシー保護原則の中でも承認されているものである。しかし、OECD のガイドラインにおいては、法的権利 (訴訟上の請求権) として確立することまでは求めておらず、任意のマネジメントシステムの構築・運用や行政措置などの手法を含め、何らかの方法で関与の機会を設けることを求めるものである。2013 年に改訂された現行の OECD ガイドラインは、「個人参加の原則」として、個人データの本人が「(a) 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について、データ管理者又はその他の者から確認を得ること」についての権利及び「(b) 自己に関するデータを保有している者に対し、当該データを、合理的な期間内に、必要がある場合は、過度にならない費用で、合理的な方法で、かつ、本人が認識しやすい方法で、自己に知らしめられること」を求める権利を承認しつつも、「上記 (a) 及び (b) の要求が拒否された場合には、その理由が説明されること及びそのような拒否に対して異議を申立てることができること」を確保すべきことまでしか求めておらず、異議の方法は、各国の法制の相違に応じて、行政庁の一種であるデータ保護官 (プライバシーコミッショナー) に対する苦情申立てと行政権限の発動を求めることでも

十分であると解するのが一般的である。OECD が個人データの開示を求めるための訴訟上の請求権を絶対視するような考え方を採用したことは（客観的な事実の問題として）歴史上一度もないし、今後もないだろうと予測される。結局、日本国における「自己情報コントロール権」なるものの主張は、法理論というよりも、単なる理念のようなものに過ぎないのだと評価することができる。それゆえ、日本国の大学法学部等に在籍する賢明な研究者は、必要やむを得ない場合を除き、「プライバシー権」や「個人情報保護法上の権利」等と表現することはあっても、「自己情報コントロール権」なる用語を安易に用いることを慎重に避けてきたのである。

<sup>16</sup> 夏井高人「サイバー犯罪の研究（二）—フィッシング（Phishing）に関する比較法的検討」法律論叢 85 巻 4・5 合併号 179～236 頁、同「サイバー犯罪の研究（三）—通信傍受に関する比較法的検討」法律論叢 85 巻 6 号 363～420 頁、同「個人情報保護法第 50 条（適用除外）に関する要件事実論的検討」判例タイムズ 1131 号 68～74 頁、同「トレーサビリティシステムと個人情報保護上の問題点」情報ネットワーク・ローレビュー 3 号 113～138 頁、同「労働災害と関連する保有個人情報の開示請求と開示拒否事由」判例地方自治 387 号 97～101 頁、同「情報化社会における個人情報保護と情報公開」地方議会人 2001 年 2 月号 20～22 頁、夏井高人・新保史生『個人情報保護条例と自治体の責務』（ぎょうせい、2007）、松本恒雄・齋藤雅弘・町村泰貴編『電子商取引法』（勁草書房、2013）76～116 頁[分担執筆・第 3 章本人認証]、夏井高人監修『IT ビジネス法入門—デジタルネットワーク社会の法と制度』（Tac 出版、2010）、笠原久嗣・大河内智秀・副島聡監訳『CISSP 認定試験公式ガイドブック』（NTT 出版、2005）899～983 頁[分担監修・第 10 章]

<sup>17</sup> 前掲「個人情報保護法第 50 条（適用除外）に関する要件事実論的検討」では、この点を意識して「請求」と「求め」を明瞭に書き分けている。

<sup>18</sup> 比較的近似した立法例として、日本国憲法 25 条 1 項をあげることができる。通説・判例によれば、同条同項に規定する「健康で文化的な最低限度の生活を営む権利」は、国民の具体的な権利ではなく、訴訟において、国を被告として、具体的な経済的利益を得るために何らかの給付を求めることのできる根拠という意味での裁判規範ではない（最高裁昭和 42 年 5 月 24 日判決・民集 21 巻 5 号 1043 頁参照）。同条同項の規定は、日本国が自主的な努力により達成すべき目標を設定した宣言的な法規範として理解することが可能である。

<sup>19</sup> 関連する質疑については、前掲「個人情報保護法第 50 条（適用除外）に関する要件事実論的検討」で触れたとおりである。

<sup>20</sup> 論者の中には、個人情報保護法の立法趣旨について、自己情報コントロール権を肯定し、その権利の行使等について法定するものだと趣旨の主張をする立場がある（三宅弘『Q&A 個人情報保護法解説（第 2 版）』（三省堂、2005）など）。しかし、現実にあった立法の過程という歴史的事実に照らすと、個人情報保護法案が審議されていた当時、野党 3 党により自己情報コントロール権を明記する法案が提案されたことがあるけれどもその内容が現行の個人情報保護法に取り込まれることはなかった。すなわち、法案審議の時点で自己情報コントロール権について様々な議論が交わされたことは事実ではあるけれども、明瞭に否定されたものと認識・理解するのが正しい。にもかかわらず、現行の個人情報保護法が自己情報コントロール権を法律によって承認し規範化したものだとする主張は、全く根拠がなく、そのように解釈したいという主観的願望を法解釈論のかたちで投影しているだけのことに過ぎない。事実としては、国会審議によって否定されているので、そのような見解は、現行の個人情報保護法の法解釈論としては否定されるべきである。

<sup>21</sup> 仮に請求権構成（裁判規範構成）を絶対視した場合、極論すると、通りすがりの者（スマートフォン等を用いて周囲の状況を常時録音または録画している可能性がある。しかし、そのような録音・録画は、通りすがりの行人の単なる自由の範疇に属することが多い。）、たまたま立ち寄った店舗の経営主体（個人または法人・店舗内の状況や来店者等を盗難防止用の監視カメラで撮影している可能性がある。しかし、そのような監視カメラに

よる撮影は、店舗管理者の所有権または管理権の行使に過ぎない場合が多い。) その他およそ個人情報保護法の立法者が想定していないような偶発的に共通の社会関係に入った者を被告として、いつでも不意打ち的に保有個人情報の開示請求訴訟を提起し得ることとなる。そのような開示請求訴訟の勝敗は全く別として、そのような訴えの提起それ自体は常に適法と解するしかなく、結果的に、個人の自由や経営者の業務遂行に対し、単なる私人が合法的に侵害または阻害し得ることにもなる。この点に関して、藤原静雄『逐条解説個人情報保護法』(弘文堂、2003) 98頁は、「立法者のような考え方とは異なるが、権利性を認めることで弊害は生じないのではないかと思われる」と述べている。しかし、全く賛成できない。国民対国民の関係においては、精神的自由権の侵害となり得る危険性が甚だしく、また、正当に保護されるべき経営者の財産的権利を不当に侵害するような結果を招くような場合が多々想定される。したがって、他の諸利益との比較考量を一切度外視し、開示の求めの法解釈について請求権構成(裁判規範構成)を絶対視することは、著しく妥当性を欠くものと言える。なお、岡村久道『個人情報保護法』(商事法務、2004) 253頁は、個人情報保護法25条1項の「開示しなければならない」の意義について、「個人情報取扱事業者の開示義務を負わせるにとどまらず、個人情報取扱事業者に対する開示請求権を本人に付与する趣旨である」、「本法はプライバシーの権利もしくは自己情報コントロール権そのものを保護するものではないから、本条の開示請求権の法的性質も、これらの権利にかかる人格権に直接基づいた請求権ではなく、その意味では、本法が新たに創設した法定の請求権であると解すべきである」としている。プライバシー権または自己情報コントロール権に基づく開示請求権であることを明確に否定している点では裁判規範性否定説と理解することができるが、個人情報保護法によって創設された法定の請求権であると解する点では肯定説となっており、自己情報コントロール権説とは明確に異なる独自の法解釈論上の立場を示している。しかし、立法者の意思または立法事実の問題としては、立法者がそのような法定の請求権を創設しようとしたことは歴史上一度もないし、そのような請求権の可能性について委員会や国会において議論・審議がなされたこともない。あくまでも理論構成としての可能性を示すのにとどまるものと思われる。また、右崎正博・多賀谷一照・田島泰彦・三宅弘編『新基本法コンメンタール 情報公開法・個人情報保護法・公文書管理法—情報関連7法』(日本評論社、2013) 218~226頁[小町谷郁子・三宅弘]は、肯定説の立場を明らかにしている。しかし、その論拠として、主として自己情報コントロール権をあげている点で明らかに失当である。

<sup>22</sup> 前掲『Q&A インターネットの法務と税務』508ノ2~508ノ8[2014年10月30日加除版]

<sup>23</sup> 宇賀克也『個人情報保護法の逐条解説[第4版]』(有斐閣、2013) 126頁は、「立法意思は、開示の求めを拒否された場合、裁判による救済を求めることができるとするものであったことは明確である」としている。多義的な表現であり一義的明確とは言い難いが、仮に裁判上の開示請求権を承認する趣旨であるとすれば、明らかに立法事実及び立法過程に関する誤認を示すものであることにならざるを得ない(藤原静雄氏の前掲『逐条個人情報保護法』における立法者意思に関する論述内容とも明らかに矛盾する。)。しかし、宇賀克也氏が立法過程についてそのような単純な判断ミスまたは誤認・誤解をするはずがない。そこで推測すると、ここでいう「裁判による救済」とは、民事訴訟上の損害賠償請求を意味すると解するか、または、「立法過程では裁判による救済の可否に関する議論が交わされたことがある」との事実を示す程度のことと解するのが妥当である(歴史上の事実の問題として、そのような議論がなされたことは間違いないことで、国会の本会議及び専門委員会の議事録等にもそのような討議がなされた記録が残されている。しかしながら、大筋としては、裁判上の請求権性を否定する見解が優位を保っていたのであり、そのような見解に基づいて大綱及び法案が起草され、可決されたという歴史的事実を動かすことはできない。ただ、当時の政府が法案の可決を最優先課題にしたことから、リップサービス的なものを含め曖昧な答弁がなされたことがあるというのも事実であり、そのために今日に至

るまで議論を引きずってしまったと理解することもできる。)。他方、同書 126 頁は、「主務大臣による監督措置である命令は、その要件が厳格であり、これまで 1 件も発動されたことがなく」と指摘している。しかし、この指摘は明らかに事実誤認である。個人情報保護法上の主務大臣としての措置命令ではなく、消費者庁長官による消費者保護法上の措置命令として是正勧告や業務停止命令等がなされた事例は数多く存在するし、電気通信事業法等の違反事例として総務大臣により措置命令がなされた事例も多数ある。これは、個人情報（個人データ）の不適切な取扱いが単に個人情報保護法違反行為となるだけでなく関連する複数の法令にまたがって重畳的な違反行為として出現することが非常に多いことに起因している。例えば、西日本電信電話株式会社に対する総務大臣による業務改善命令等に関しては、平成 22 年 2 月 4 日付けをもって、「NTT 西日本、NTT 西日本一兵庫及び株式会社 NTT 西日本一北陸（以下「NTT 西日本一北陸」）の従業員が、NTT 西日本の顧客管理システムから、他社の DSL 役務利用に関する情報等を利用目的の達成に必要な範囲を超えて取り出し可能であったこと並びに個人情報の提供の手段及び方法に関する内部規程の運用及びチェック体制が不十分であったことは、個人情報の保護に関する法律（以下「保護法」）第 20 条及び電気通信事業における個人情報保護に関するガイドライン（以下「ガイドライン」）第 11 条第 1 項に規定する安全管理措置義務に違反するものであると認められます。NTT 西日本の従業員が、他社への電話番号移転に関する情報を取り出し、同情報を NTT 西日本一兵庫の従業員に利用目的の達成に必要な範囲を超えて提供したことは、保護法第 21 条並びにガイドライン第 12 条第 1 項、第 2 項及び第 5 項に規定する従業者の監督義務に違反するものと認められます。さらに NTT 西日本一兵庫及び NTT 西日本一北陸の従業員による個人情報の不適切な取扱いがあったことは、保護法第 22 条並びにガイドライン第 12 条第 3 項及び第 4 項に規定する委託先の監督義務に違反するものであったことが認められます。したがって NTT 西日本に対し文書による厳重注意を行うとともに、再発防止策及びその取組状況について報告を求めました」との内容が総務省の Web サイト上で公表されている。その他、類似の措置命令事例が多数存在するが、詳論は避ける（電気通信事業法や特定電子メール適正化法とからんだ事案についての措置命令事例については、夏井高人「サイバー犯罪の研究（六）－違法な電子メールに関する比較法的検討－」法律論叢 86 巻 6 号 181～243 頁で詳論したとおりである。）。換言すると、個人情報保護法違反のみを理由とする措置命令だけを調べ検討するのみでは、行政庁としての真の行政姿勢・行政実態を知ることが不可能である。また、個人情報保護法違反による措置命令が現実になされた事例も多数ある。要するに、行政庁としては行政権の過剰な干渉との批判を避けるため比較的謙抑的に行政権を発動しているというだけのことであって、措置命令をすべき重大事案についてはしかるべく対処してきたと評価するのが妥当である。

<sup>24</sup> 特別法に基づく罰則の適用に関しては、前掲「サイバー犯罪の研究（二）」及び「サイバー犯罪の研究（三）」において、比較法的な検討を踏まえて詳論したとおりである。

<sup>25</sup> EU 加盟国が個人データ保護指令に基づいて制定した法制中で最も厳格な個人データ保護法令は、ドイツの連邦個人データ保護法である。同法の注釈書等は多数出版されているが、Simitis, Bundesdatenschutzgesetz 8. Auflage, Nomos, 2014 及び Martin Eßer, Philipp Kramer, Kai von Lewinski, Auernhammer BDSG - Bundesdatenschutzgesetz und Nebengesetze 4. Auflage, Carl Heymanns Verlag, 2014 が詳しい。ドイツの連邦個人データ保護法 6 条 1 項は、個人データ主体の権利（Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35)）を規定し、同法 19 条は、個人データ主体が個人データ管理者に対して①個人データ的内容及び当該データの入手元（die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen）、②個人データの提供先（die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden）、③個人データ記録の目的（den Zweck der Speicherung）に関する情報を、請求することによって得ることができると規定し、これと対応するように、同法 34 条は、個人データ管理者が個人データ主体に対して、①個人データ的内容及び当該データの入手元、

②個人データの提供先及び③個人データ記録の目的に関する情報を提供すべき義務を規定している。つまり、①個人データの内容及び当該データの入手元、②個人データの提供先及び③個人データ記録の目的に関する情報の開示については、個人データ主体が権利者で個人データ管理者が義務者という当事者構造になっていることが条文上からも明らかにされているのである。同法6条の権利は、EU個人データ保護指令10条に規定する個人データ管理者の個人データ主体に対する情報提供義務を国内法化した条文である。前掲 Simitis の *Bundesdatenschutzgesetz* 1054 頁は、このような権利の法的性質について、「情報の自己決定をする権利 (Recht auf informationelle Selbstbestimmung)」の一種として位置付けている (前述のとおり、この理念はドイツ連邦憲法2条1項に由来する。)。同書94頁においても、この権利の発生根拠について、ドイツ連邦憲法上の権利 (基本的人権) の一種として位置付けている (ただし、同書中では、他人が保有・管理する情報に対して何らかの干渉をする行為が別の意味での人権侵害を構成する可能性については、特に詳しく論じられているわけではないので、注意を要する。すなわち、ドイツ法においても、個人データ主体の権利とデータ管理者の権利とが対等なものとして衝突する場面においては、利益考量による合理的な判断がなされなければならないのであり、個人データ主体の権利が常に個人データ管理者の権利に優越するわけではない。)。また、同書1055頁は、その目的を「自己情報の保護 (Selbstdatenschutz)」として位置付けている。この自己情報の保護は、EU個人データ保護指令において示されている理念に由来するものである。これらの条項は、個人情報そのものの権利としてではなく個人情報取扱事業者の義務として規定する日本国の個人情報保護法25条1項とは全く異なる立法形式を採用するものである。この日本国法とドイツ連邦法の条文構造の相違は、日本国とドイツ連邦とでその立法意思が明瞭に異なっていること、憲法上の基本的人権として情報に関する権利が一般に承認されるレベルに達しているか否かといった国情の違いに起因するものと考えられる (基本的人権の一種である自由権の尊重に関する国民の認識・理解の程度及びその内容について、EU域内においてさえ、例えば、ドイツとフランスとではかなり異なる部分があり、一律に論ずることができない。)。このような基本的人権の一種としての理解に関しては、Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, 2014 が参考になる。更に付言すると、ドイツの現行の連邦個人データ保護法は、個人データ主体を原告とし個人データ管理者を被告とする民事訴訟による紛争解決 (司法的解決) の手続については特別条項を置いておらず、通常の民事訴訟法の関連条項の解釈・適用に依拠している。そのため、今後、EU個人データ保護規則等の確定の動きに合わせて、逐次法改正が実施される可能性が高い。

<sup>26</sup> 自己情報コントロール権を主張する研究者・弁護士は決して少なくないが、弁護士の多くは大学においてそのように学んだためにそのように主張しているだけのことで、この概念それ自体の由来や理論としての健全性を検証した上で主張しているわけではない。理論としての「自己情報コントロール権」が流布されるに至ったことについて最も大きな力となったのは、いずれも昭和45年(1970年)に公表された佐藤幸治氏の「プライバシーの権利(その公法的側面)の憲法論的考察—その比較法的検討(1)」法律論叢86巻5号1~53頁、「プライバシーの権利(その公法的側面)の憲法論的考察—その比較法的検討(2)」同87巻6号1~40頁だと考えられる。これらの論文は、その後、佐藤幸治『現代国家と人権』(有斐閣、2008)に収録された。そして、「自己情報コントロール権」なる理論の米国における発展を根拠づけるべく William M. Beaney の「The Right to Privacy and American Law」が引用されている。その出典として記載されている「31 Law and Contemporary Problems 253 (1966)」とは、米国 Duke University Law School の紀要 (学術雑誌) である Law and Contemporary Problems の Volume 31, Number 2 (Spring 1966) を指すものと思われる、その253~271頁には確かにその題名の論文が掲載されている。しかしながら、この論文中には、日本語の「自己情報コントロール権」に対応するような英語表現が全く含まれていない。この論文の内容を要約すると、それは、警察による犯罪捜査の過程で私人のプラ

イバシーが侵害されるおそれを極小化するために、米国における連邦憲法上の適正手続の保障（due process）を強化すべきとするものである。少なくとも私人間のプライバシー侵害に関する論文ではないので、文脈上、私人である個人データ主体から私人である個人データ管理者に対するコントロール権が問題となり得る余地がない。また、自己決定権の問題としても、警察による違法捜査の文脈では自己決定が機能する余地が全くなく、侵害があった場合の事後救済（私法上では損害賠償請求・公法上では違法収集証拠としての証拠排除）を論ずるしかないのは当然のことである。それゆえに、同論文では、刑事手続における適正手続の保障を強化すべきだとの主張がなされているのである。同様に、佐藤幸治氏は、Charles Friedの「Privacy」と題する論文を根拠として引用している。この論文は、米国Yale大学の紀要（学術雑誌）であるYale Law JournalのVolume 77, Number 3, January 1968の475～493頁に掲載されている。その内容の要旨は、電子機器類や情報技術の発展に伴い他人間の秘密通信を盗聴することが非常に容易になったという社会的事実を踏まえ、米国における連邦憲法上の自己負罪の禁止原則（Self-incrimination doctrine）が事実上反故にされてしまっているという問題意識からはじめて、プライバシー概念の本質を社会心理学的な観点を加味しつつ哲学的に深く考察した上で、プライバシーの利益とされてきた諸利益の中でも特に私人に関する知識や情報の秘密性ないし秘匿性という価値の重要性を強調するものである。すなわち、この論文においてもまた、自己情報コントロール権に対応するような英語表現を見出すことはできない。これらWilliam M. BeaneyとCharles Friedの論文の主要課題は、要するに、公権力による私人間の通信に対する侵襲すなわち通信の秘密の侵害を論ずるものだとすることに尽きる（このようにプライバシー保護の問題と通信の秘密の問題とは極めて密接な歴史的・論理的関連性を有しているので、前掲「サイバー犯罪の研究（三）」においても、日本国法上の通信の秘密に重点を置いて詳論することとした。）。要するに、佐藤幸治氏が主張するような「自己情報コントロール権は米国に由来する」との主張は、何も根拠づけられているわけではなく、佐藤幸治氏がそのようなのだと「述べている」というだけのことに過ぎない。学術論文ではない本意見書の性質と目的上、この点に関する詳論は避けるが、佐藤幸治『現代国家と人権』及びその元となった論文に示されているその他の論拠（米国の学術論文や判例等）についても、全ての原典に直接にあたってつぶさに精査してみると、佐藤幸治氏が述べていることの論拠は必ずしも明確なものではないということを知ることができる。しかし、佐藤幸治氏は、極めて高名な憲法学者であるし、司法改革の旗手であり、法科大学院という専門教育制度の産みの親の一人である。そのために、同氏の言説が「確たる論拠のあるものだ」と考え、その主張が正しいと信じた学徒の数は万単位に及ぶものと推定される。

<sup>27</sup> 個人情報保護法25条1項の開示の求めとの関連では、基本方針6(1)①の「事業者が行う措置の対外的明確化」において、「事業者の個人情報保護に関する考え方や方針に関する宣言（いわゆる、プライバシーポリシー、プライバシーステートメント等）の策定・公表により、個人情報を目的外に利用しないことや苦情処理に適切に取り組むこと等を宣言するとともに、事業者が関係法令等を遵守し、利用目的の通知・公表、開示等の個人情報の取扱いに関する諸手続について、あらかじめ、対外的に分かりやすく説明することが、事業活動に対する社会の信頼を確保するために重要である。」と規定されているのみである。

<sup>28</sup> 理論的には、立法者意思が法理論を拘束することはないので、いかようにも法理論を構築することが可能である。しかし、立法者意思とは異なる法解釈論を前提として実務を改めることは非常に困難または不可能に近い。これを改めるためには、法改正案を策定し、国会において審議し、個人情報の本人と個人情報取扱事業者と監督官庁（主務大臣）との利害関係を合理的に調整し、必要な妥協を経て、新たなルールを確立し、その新たなルールに基づいて新たな基本方針を確定し、その新たな基本方針に基づいて関係各省庁の多数のガイドラインを改訂し、関連する訴訟法上の法令や最高裁判所規則を定め、それを周知するという手順を踏むのでなければ、社会的混乱を招くだけで、良い結果を産むことがな

---

いと考える。

<sup>29</sup> 前掲『IT ビジネス法入門』263～273 頁、484～499 頁参照

<sup>30</sup> 個人情報保護のための自主管理（マネジメント）を達成するための技術的方策について情報セキュリティという技術的側面からの対応が国際的に承認された水準で達成されているかどうかを評価し認証するための第三者認証制度の一つとして、情報セキュリティマネジメントシステム（ISMS）がある。日本国では、JIPDEC がその認証機関となっている。このほか、個人データまたはプライバシー保護のための技術的要素に関しては、堀部政男・JIPDEC 編『プライバシー・バイ・デザイン』（日経 BP 社、2012）、橋本誠志『電子的個人データ保護の方法』（信山社、2007）、FTC, internet of things, January 2015、ENISA, Privacy and Data Protection by Design – from policy to engineering, December 2014、Michael A. Caloyannides, Privacy Protection and Computer Forensics (Second edition), Artech House, 2004、Udaya Parampalli, Philip Hawkes (eds.), Information Security and Privacy, Springer, 2011、Robert F. Smallwood, Safeguarding Critical E-Document, Wiley, 2012、Serge Gutwirth, Yves Pouillet, Paul De Hert, Ronald Leenes (eds.), Computers, Privacy and Data Protection: an Element of Choice, Springer, 2011、Conrad Grützmacher, Recht der Daten und Datenbanken im Unternehmen, Otto Schmidt, 2014 が参考になる。

<sup>31</sup> 私人間の法律関係を前提とする限り、個人データの管理（コントロール）をすることができるのは個人データ管理主体（日本国の個人情報保護法では個人情報取扱事業者）のみであり、個人情報の本人（個人データ主体）が管理権（コントロール）を有することは理論的にあり得ないことである。それゆえ、個人情報の本人（個人データ管理主体）が保有する個人データについて、個人情報の本人（個人データ主体）が自己情報の管理権（自己情報コントロール権）を有することも理論的にあり得ないことである。例えば、A の友人 B が A との交際について B が所有する日記帳に日記として書き記したという事例を想定してみると、当該日記帳の所有権が B に属する以上、その日記帳に記載された情報の管理権も B のみに属し、A には一切の管理権がない。もし B が A との交際内容を世間に暴露し、公然と事実を適示したとすれば名誉棄損に基づく民事・刑事上の法的責任が生ずることはあり得ることではある。しかし、このことは、B が所有・管理する日記帳及びそれに記録された情報に対する A の管理権に基づくものではなく、全く別の法理に基づくものである。A が B の所有物や占有・管理物について管理権を有することはあり得ない。単に、契約や法令に基づいて何らかの「関与」をなし得ること場合があるという程度のことである。仮に、B が所有・管理する日記帳及びそれに記録された情報について A が管理権を有すると解するとすれば、極論すれば、例えば、B の脳内にある情報に対しても A が管理権を及ぼすことができなければならないことにならざるを得ないが、おそらく、そのような論理的帰結を必然的にもたらすような法理を承認・是認する法学説は存在しないのではないかと思われる。

<sup>32</sup> より抽象度を高めた考察が許されるとすれば、国家も組織の一種である以上、憲法をポリシーと理解し、ポリシーである憲法に基づく法令の体系をコントロールと観念し、それらの法令を根拠とする行政権の発動をコントロールの運用と考え、裁判所による行政権運用の適否の判断を運用に対する評価として位置付けるもまた可能である。

<sup>33</sup> 消費者が関与する取引関係においては、消費者保護の目的で、条理上、単なる宣言が契約上の付随義務として認められることはあり得る。これは、消費者と事業者との間の力関係が圧倒的に異なっており、社会的には付合契約（付従契約）しかないという法社会学的な実態を踏まえた解釈論の一種である。消費者が全国統一的な労働組合のような組織を構成し、経営者団体と団体交渉をするといった事態を想定することは不可能である。それゆえ、特殊な例外的事象として、裁判所の関与により、消費者の利益を保護するため、付随的義務という法概念による契約意思の補充・補正がなされてきた。そのような裁判例については既述のとおりである。ただし、ここで大事なことは、付随的義務の元となる何らかの契約（金銭消費貸借契約、売買契約等）が消費者と事業者との間で締結されているとい

う事実である。何も契約が存在しない場面では、付随的義務を観念することができない。なお、労働契約においては一定の特殊性が認められることは事実である。しかし、労働契約に関する限り、労働基準法に基づき、労働者の代表と使用者との間の基本合意に基づく集団的契約関係によって規律するのが日本国の法制度上の基本となっているので、労働契約について消費者契約と全く同じように考察・判断することはできない。労使間の団体交渉等によって解決できない場合に対する制度的な支えとしては、労働審判制度等が設けられている。

<sup>34</sup> 管理策の一つとして顧客との間で何らかの契約を締結するということはあり得る。この場合、締結される契約は、管理策の実施の結果として発生するものであり、管理策そのものではないこと、そして、管理策が策定されれば顧客との間での契約関係が自動的に生成されるわけではないことに留意すべきである。

<sup>35</sup> 情報セキュリティの領域においては、BS と互換性のある世界標準に準拠する日本国の工業規格として JIS Q 27000 が定められている。この JIS Q 27000 に基づく認証制度は、一般に、情報セキュリティマネジメントシステム (Information Security Management System: ISMS) と呼ばれており、情報システムを用いて業務を遂行する企業や官庁等によって広く導入されている。この ISMS の場合でも、例えば、システム管理者 (企業) と顧客との間に自動的に何らかの契約関係が生成されるわけではない。もし ISMS に基づくシステム管理に失敗し、不正アクセス等により顧客に損害が発生した場合には、ISMS に基づく契約違反 (債務不履行) が問題となるのではなく、当該企業と顧客との間のシステム利用契約等の個別具体的な契約における債務不履行 (過失) が論ぜられるべきである。契約関係のない第三者との関係では、不法行為 (民法 709 条) における法益侵害及び過失の有無が問題となり得るだけである。

<sup>36</sup> 世界各国の工業規格の認証機関は、相互認証をすることがある。例えば、BS と JIS との関係を考えてみると、日本国の JIS Q 15001 の認証 (プライバシーマークの付与) が BS による認証と互換性のあるものとして国家間または認証機関相互間で合意が成立している場合、日本国の JIS Q 15001 による認証を受けた企業は、その認証を受けた項目 (事項) に関する限り、英国においても BS に基づく認証を受けたのと同じ扱いを受けることができる。この例では、当該企業は、英国においても、当該認証項目 (認証事項) に関する限り、BS に規定する規格に適合する企業として扱われることになる。そして、英国と日本国とでプライバシーや個人情報 (個人データ) に関する法制が全く異なっているにもかかわらず、この工業規格の相互認証システムによる互換性が維持されている限り、日本企業は、当該認証項目 (認証事項) を含むビジネスについては、英国においても適法に企業活動を行うことになるのである。日本国の個人情報保護法は、オーストラリアの個人データ保護法と同様、EU の個人データ保護指令に全く適合するものではないが、それでも欧州・日本・オーストラリアの間で何らの法的支障もなく貿易や取引が実施可能となっているのは、このような工業企画ベースでの相互認証制度が存在し、有効に機能しているからである。このような実務は、経済産業省を主体として維持・継続されてきたもので、国際取引を必須の経営内容とする企業の間では公知のことである。しかし、国際取引に疎い憲法学者等の間では、空疎な観念論は存在してもマネジメントシステムの相互認証による法補完的な国際取引支援実務の実際に関する知識が乏しいかまたはこれを欠如しているのが通例なので、JIS の運用にも関与している例外的な研究者を除いては、基本的に、明確に意識されることが滅多にない。このことは、日本国内の訴訟実務しか経験のない弁護士でも全く同じことである。

<sup>37</sup> 前掲『個人情報保護マネジメントシステム実施のためのガイドライン[第2版]』80頁

<sup>38</sup> 現在の EU では個人情報の開示を求める場合の手数料を無償とするというのが原則的な考え方となっている。同様の条項を設置するように日本国の個人情報保護法を改正することは可能である。しかし、日本国において開示請求権を認める場合、その手数料の中に訴訟費用や弁護士費用等を含むかどうかについては明確な定めがない (そもそも訴訟上の

請求権を認めない前提で立法されたので、その関連の条項が一切存在しない。)。このような問題があるため、仮に開示請求権を認める法改正がなされたとしても、手数料の負担に関する規律が法律によって明確に定められるまでは訴訟費用等と関連する最高裁判所規則を制定することができない道理であるし、裁判所の訴訟指揮の範囲内の問題として扱うこともできないという深刻な課題を抱えてしまうことになるのである。なお、個人情報保護法とは無関係に、人格権その他の権利を根拠として開示請求権を是認することは、法解釈論上としてはあり得ることである(当事者間の契約に基づき開示義務が給付内容となっている場合、本体的な債務の履行を求めるものとしての請求権を是認すべきことも当然のことである。個人情報保護法 25 条 1 項に基づく開示の求めの法的性質は、あくまでも特別法上の請求権の存否に関するものであって当事者間の合意の合理的な解釈の問題とは全く別次元の事柄であることに留意しなければならない。)。費用負担が問題となるのは、仮に肯定説を前提とした場合、個人情報保護法に基づく特別法上の開示請求権だからこのことである。特別法上の請求権である以上、その根拠となる EU 個人データ保護規則との整合性を保つように、費用負担を含め関連諸規定全部について、法律上の文言とは異なっても整合性のある解釈論を全てワンセットのものとして提供した上で請求権性を是認するのでなければ、無責任との誹りを拒むことができないと思われる。

<sup>39</sup> 本文で述べたような自主管理(マネジメントシステム)という手法は、英国や米国では既に一般化しているし、裁判官、法学者、弁護士を含む法律家のほぼ全員がそのような理解に基づいて法解釈論を展開している。しかし、日本国の法律家の中で、古典的な「法規範」という概念しか知らないような法学者等にとっては全く理解しがたい手法であるかもしれない。このような時代の変化に対応した新たな国家的統制手法が既に立法及び工業規格として導入されているということを認識・理解する能力に欠けているところに、開示請求権をめぐる日本の憲法学等における混乱の根本原因があるとも考えることもできる。

<sup>40</sup> この問題は、一般に、「神の神はいない」という問題として知られている。

<sup>41</sup> この主務大臣による報告徴収と措置命令は、公法学上の自由裁量行為としての性質を有するものと解する。

<sup>42</sup> 国会における審議等の経過に照らすと、個人情報保護法案の可決に反対した野党は、個人情報の本人による請求権を強く求める一方で、主務大臣の権限強化には明瞭に反対の態度をとり続けたことが窺われる。その結果、EU の法制では認められた個人情報の本人による訴訟上の請求権も主務大臣による代理請求も、そのいずれもが法律の条文上では認められないという結果になったというのが真相である。

<sup>43</sup> 前述のとおり、一定数量の個人情報を取り扱う事業者は個人情報保護法所定の個人情報取扱事業者となるが、所定の数量に満たない少数の個人情報しか取り扱わない事業者は個人情報保護法所定の個人情報取扱事業者とはならない。JIS Q 15001 は、事業者が個人情報保護法所定の個人情報取扱事業者に該当すると否とを問わず、また、JIS Q 15001 に準拠しているとの審査を経て JIPDEC からプライバシーマーク認証を受けていると否とを問わず、誰でも自己の行動規範として採用することができ、これを自己のマネジメントシステムにおける基本方針(ポリシー)及び管理策(コントロール)とすることができる。このことは、個人情報の本人でも全く同様であって、顧客及び従業員が全く存在しない者が、自己の保有する自分自身の個人情報の管理のために JIS Q 15001 に従うことを宣言し、これを基本方針(ポリシー)及び管理策(コントロール)とすることもできるのであるが、そのように宣言すれば自動的に勤務先との間で何らかの契約関係が発生するなどということとはあり得ないことである(JIPDEC の審査・認証を受けていない場合には、JIPDEC との関係でも審査手数料や認証手数料等の支払に関する債権債務が発生することもないことは、自明である。)。この個人情報の本人が JIS Q 15001 に準拠して自分自身の個人個人情報を管理することを宣言する事例をみれば容易に理解することができるように、JIS Q 15001 は、それを導入することそれ自体によっては、本人以外の誰かとの関係において、何らの債権債務関係を発生させるものではない。いわば、本人が「正義に従って生きる」

---

と宣言しただけでは何らの法律関係も発生しないと全く同じである。およそマネジメントシステムというものは、すべからくそのような論理構造を有するものである。

<sup>44</sup> プライバシーマークの認証を受けた事業者と JIPDEC との間の認証審査契約関係に基づく契約上の制裁的行為の一種と解することができる。JIS Q 15001 所定の行動規範に反する行為または結果があれば JIPDEC による制裁として認証の取消等を受けることが債務の本旨として認証契約の中に約定されているという側面を重視すれば、解釈論上、単なる給付として理解することが可能である。他方で、認証の付与行為には条件付の取消権が留保されており、認証を受けた事業者に違反行為があれば条件の成就したことになり、JIPDEC に具体的な認証取消権が発生し、その取消権が JIPDEC によって行使されると認証が取り消されることになるとの解釈論も成立可能である。この場合、取消権が発生していてもそれを行使するかどうかは JIPDEC の裁量に任されているので、違反行為があれば JIS Q 15001 によって自動的に認証が取り消されるといったような法律関係が発生することもあり得ない。いずれにしても、これらは、認証を受けた事業者と JIPDEC との間の認証審査契約の締結という事実が必須の要件になっていることから、JIS Q 15001 そのものの法律効果と考えることはできない。

<sup>45</sup> 高橋滋・斎藤誠・藤井昭夫編『条解行政情報関連三法—公文書管理法・行政機関情報公開法・行政機関個人情報保護法』（弘文堂、2011）は、情報公開法や行政機関個人情報保護法等の理念について自己情報コントロール権で説明している。しかし、その説明文を「自己情報コントロール権」から「民主主義の理念」等に単純に置き換えても全体として無理なく意味の通る解釈論が提示されているところからすると、特に深く検討せずに「自己情報コントロール権」という流行語を使用しているのに過ぎないと解される。事実、行政機関個人情報保護法 12 条 1 項に関する注釈を読むと、自己情報コントロール権と関連する記述はいわゆる余事記載の一種ようになっており、その記述を全部削除しても同法 12 条 1 項の注釈としての完全性と有用性を些かも損なうことがないということからも、このことを理解することができる。

<sup>46</sup> この判決に対する批判的な見解を示す判例評釈として、宇賀克也「1.個人情報保護法 25 条 1 項に基づく訴訟による個人情報の開示請求の可否(消極) 2.個人情報保護法 25 条 2 項に違反した事業者が慰謝料の賠償責任を負わないとされた事例(東京地判平成 19.6.27)」判例時報 1990 号(判例評論 589 号) 164～170 頁、二関辰郎「個人情報保護法に基づく開示請求の権利性—裁判規範性を否定した東京地裁判決の批判的検討」自由と正義 59 卷 4 号 140～146 頁、三宅弘「判例研究 個人情報保護法 25 条の本人情報開示請求権の法的性格—東京地裁平成 19.6.27 判決の批判的検討」獨協ロー・ジャーナル 4 号 155～169 頁がある。なお、宇賀克也氏の判例評論は、後に宇賀克也『個人情報保護の理論と実務』（有斐閣、2009）95～111 頁に再録され同書の第 6 章として公刊されている。

<sup>47</sup> 宇賀克也氏の判例評論における問題点は、前述の宇賀克也『個人情報保護法の逐条解説 [第 4 版]』について述べたところと全く同じである。同氏は、実質的に同一内容の原稿を何度も単純に使いまわし、別の論考として公刊しているので、同じ誤謬が何度も単純に繰り返される結果となっている。

<sup>48</sup> 堀部政男編『プライバシー・個人情報保護の新課題』（商事法務、2010）61～91 頁[鈴木正朝分担執筆・第 2 章]に網羅的にまとめられている。

<sup>49</sup> 例えば、小向太郎『情報法（第 2 版）』（NTT 出版、2011）178～179 頁がそうである。同書では、個人情報取扱事業者の「義務」のみが説明され、裁判所による紛争解決としては「個人情報の不適正な利用に対しては、プライバシー侵害として不法行為責任に基づく損害賠償請求等が請求しうる場合がある」ことのみが示されている。ここで「プライバシー侵害として」と明記されていることは極めて重要である。これは、①「個人情報保護法が行政法の領域に属する法規範」であって、②個人情報保護法に定める個人情報取扱事業者の義務とは、「主務大臣に対する義務であり、個人情報の本人に対する私人間の義務ではない」という行政法学分野における通説的理解を前提としているのである。その結果、

個人情報保護法違反行為があっても、その違反は主務大臣に対する行政法上の違反に過ぎず、個人情報の本人との間の私法上の関係については何ら影響を与えない（私法上の法益侵害を構成しない）という行政法学上の法解釈論が確固たるものとして形成されてきた。このことは、板倉陽一郎「個人情報保護法違反を理由とする損害賠償請求に関する考察」情報ネットワーク・ローレビュー11巻1～12頁によって更に鮮明にされているところである。なお、前掲『ITビジネス法入門』296～297頁は、「行政規範としての個人情報保護法による個人情報取扱事業者に対する行政監督という公法上の社会統制とは全く別に、個人情報それ自体をプライバシーの一種またはそれに類する法的に保護される利益としてとらえ、その侵害に対する法的救済（不法行為としての損害賠償請求や名誉回復の措置、人格権としての差止請求など）を検討しなければならない」としている。このような見解に対する反対論として、加藤隆之「個人情報保護制度の遵守とプライバシー権侵害—個人情報の第三者提供に関する判例を中心として」亜細亜法學46巻1号19～127頁は、個人情報保護法が自己情報コントロール権を実定法上明らかにした法規範であるとの前提で、個人情報保護法上の権利の侵害による不法行為の成否を論じている。しかし、その立論の前提に誤りがあることは既に述べたとおりである。

<sup>50</sup> 前掲『プライバシー・個人情報保護の新課題』80頁

<sup>51</sup> 前掲『個人情報保護法の理念と現代的課題—プライバシー権の歴史と国際的視点』500～503頁

<sup>52</sup> 鈴木正朝（堀部政男監修）『個人情報保護法とコンプライアンス・プログラム』（商事法務、2004）233頁、前掲『プライバシー・個人情報保護の新課題』81～89頁

<sup>53</sup> 少なくとも、同報告書のとりまとめをした担当者は、日本国における学説の状況について、消極説が圧倒的に有力であるとの認識・理解を有するに至ったことだけは間違いないと認めることができる。

<sup>54</sup> 現在の政府部内における個人情報保護法及び関連諸法例の改正作業は、現行法がEUの個人データ保護指令及び個人データ保護規則案の求める要件にほとんど適合していないということを当然の前提とするものである。とりわけ、EU個人データ保護規則案が求める訴訟上の請求権（司法的救済）に関しては、日本国の個人情報保護法がそのような裁判規範性を有する権利を発生させる根拠法規たり得ないということを改正作業担当者間での共通認識とした上で、その検討作業が進められている。その意味で、個人情報保護法25条1項の開示の求めの法的性質に関する従来の裁判規範説（肯定説）は、憲法学説史的には、EUと米国の基本法制とその立法事実を十分に咀嚼・理解しないまま安易に提出された時代的かつ泡沫的な産物だったと評価することも可能である。

<sup>55</sup> 前掲「個人情報保護法第50条（適用除外）に関する要件事実論的検討」参照

<sup>56</sup> EUの個人データ保護法制との適合性を確保すべきであるという前提にたつと、国家政策上の重要課題の一つとして、個人データに関する訴訟上の請求権を肯定するための適切な法改正作業が必須のものとなる。ただし、そのような法改正のためには、様々な利害調整を含む慎重な検討が必要なのであり、法解釈論だけで肯定的に解決すればそれで全部足りるというような単純な問題ではないということを明確に認識すべきだと考える。なお、反対の立場（EUの法制との適合性を至上命令としない立場ないしEUの法制と完全に横並びである必要はないとする立場、あるいは、EU統合の失敗という未来像の可能性を見据えた全く別の立場等）も当然あり得る。例えば、米国は、EUとは異なるやり方でプライバシー保護（裁判所における司法的解決の場合を含む。）を図ってきた。英国は、場合によってはEUからの離脱を含め、米国と歩調を合わせつつも独自の政策論を選択するかもしれない。しかも、これらの問題全てが、法的にはTRIPsやACTAのような国際取引に関する国際合意と密接に連動するものであり、経済的には各国の国際収支やGDPの状況等によって大きく左右される可能性が高く、政治的には中東やアフリカにおける深刻な軍事的紛争や西側諸国と中国・ロシア等との間のサイバー戦による影響を直接に受けるような要素を含んでいる。そして、今後の日本国政府がどのような政策論に基づいて国際協調を

---

図るかについては全く予測できない。前掲『個人情報保護法の現在と未来－世界的潮流と日本の未来像』479頁は、「OECDは利害調整の役割を果たし、EUはデータ保護基本権による手厚い保護措置を求め、CoEは欧州ルールに則って、EU規則提案に足並みを揃える形で条約の現代化を進め、米国は自主規制ベースの制度設計を崩さず、APECも自主規制を基本に越境データ流通に関する制度を運用しており、それぞれの立場は異なる」としている。預言者でない限り未来のことは誰にもわからないが、法制度もまた文化現象の一種である以上、近未来の世界において個人データ保護の枠組みについて根幹からの変動があると予測することが無謀であることは誰も否定できないのではないかと考えられる（これらの点を考える上での基礎資料としては、前掲 *Reforming European Data Protection Law* が参考になる。）。日本国の法制に関して、個人情報（個人データ）の管理・保護に関して個人情報の本人（個人データ主体）の関与をどの程度まで認めるかについては、内閣府を中心として、EUにおける近時の議論や立法動向も踏まえた上で、慎重な検討が重ねられている渦中にある。その検討対象の一つであるEU内においても、様々な問題について賛否両論があり、米国の法制との関係もあって（EUのデータ保護官と米国のGoogle、Facebook及びAppleとの間の極端な見解の相違がその適例である。例えば、EUの個人データ保護法制におけるいわゆる忘れられる権利（Right to be forgotten）をめぐる昨今の動向がそうである。）、個人データ主体の個人データ管理者に対する請求権を単純に認めることについて明確なコンセンサスが存在し容易に実行可能な状態にあるとは思われない（従来、個人データ主体の個人データ管理者に対する請求権の有無について明確な理論と実務がEU域内において存在しなかったからこそ、EU個人データ規則案75条等において司法的解決の明確化を図らざるを得ない状況となっていることには特に留意すべきである。このような個人データ保護規則案75条等の制定の動きが存在するという事実から、日本国の個人情報保護法制定当時の時点においては、日本国においてもEUにおいても、個人データ主体の請求権なるものが必ずしも自明のものではなかったということを理解すべきである。）。土壇場に至って、いわば「梯子を外すような事態」が絶対に発生しないとは誰も断言できないのである。そして、国際的なテロ問題や国家諜報機関による他国の企業秘密や軍事機密に対する防諜活動等の問題もあり、単純に個人データ保護を考えるのみでは国家の安全性を損なう危険性があることが次第に認識されるようになってきた。慎重な配慮と検討を要するということを重ねて強調したい。