

企業が理解すべき 個人情報保護法の意味と とるべき対応

稲垣隆一 氏 ISMS主任審査員 / 日本弁護士連合会コンピュータ委員会副委員長 / 弁護士

個人情報保護法が内在する意味を企業はどのように理解し、受け止めるべきか。電子ネットワークのセキュリティと企業防衛を専門とし、日本弁護士連合会コンピュータ委員会副委員長を務める弁護士の稲垣隆一氏に持論を展開していただいた。

民間企業にとってのリスク

まず、個人情報の保護をめぐる状況認識についてうかがいたいと思います。

稲垣 現実、法文化、情報セキュリティ技術、それらすべてが大きく変化し、その動きが国民一般の意識に浸透しつつある。今はそのような変化の時期にあるのだと理解しています。

現実において、ネットワークが社会に、広く、深く浸透しており、ユビキタス社会¹の実現が目前に迫っています。そこでは、セキュアな状態が確保されていなければ、私が私でなくなる脅威が存在する。既にそれは、なりすましや架空請求といったかたちで現れ出した。そのような状況の中、「個人情報の保護に関する法律(以下、個人情報保護法)」が成立しました。これをもって、日本で初めて民間企業に一般的に適用される法律上の義務として情報セキュリティの確保が規定されたわけですが、何より重要なことは、それが、個人情報のとらえ方の枠

組みそのものが変わった、との宣言であったことです。旧来の個人情報の議論といえば、その情報がプライバシーとしてどれほどの価値があるのかということが焦点でした。住基ネットの議論に際しても、氏名、生年月日、性別、住所の「住基4情報」は果たしてそれほど厚く保護すべき対象なのか、という論争があった。氏名は公開情報ではないか。性別など見れば分かるではないか、と。これらのことから分かるように、伝統的に、公開性、非公開性が保護の対象か否かの重要な判断基準とされていた。ところが今回の法律は、それを一蹴して個人の特定情報や属性情報といった公開された情報も保護の対象する価値がある。なぜならマッチングのキーになるから、とするわけです。

その個人情報保護法は企業にどのようなリスクをもたらすのでしょうか。

稲垣 個人情報保護関連5法²は、直接の法律上の

効果としてリーガルリスクを発生させるものではありません。しかし、個人情報保護法には、損害賠償や差止請求といった民法上の効果の根拠になるとは書かれていませんから、企業にとってのリスクは、民法なり商法なりの規定を通じて具体化されることとなります。ただ、この立法がリーガルリスクなり経営上のリスクなりを確実に高めることは紛れもない

¹ ユビキタス社会：いつでもどこでも、利用者が意識せずとも、情報通信技術を活用できる環境が実現されている社会のこと。

真実です。かつて、個人情報の保護は限られた人の限られた主張と受け取られていましたが、今回、保護の内容が具体的なかたちで国民一般に示されました。企業にとっては、安全管理のための諸々の義務が課せられ、規範内容が設けられ、リーガルリスクは、それらがなかった時代とは比較にならないほど高まっています。企業はそのリスクに鈍感であってはなりません。一連の不祥事で、顧客情報の流出のお詫びとして500円分の商品券を配る企業があり、住民基本台帳のデータが外部に漏れた京都府宇治市のケース³でも、慰謝料額(の下限)は1万円でした。それを先例と見なし、高を括るのはとんでもない誤りです。いずれのケースでも具体的被害は生じていませんが、今後、精神的被害が認定されれば、そのような金額で収まらないことは明らかです。特に信用情報、医療、介護、投薬歴、教育などのセンシティブな情報にまつわる紛争なら、相当高額の賠償を覚悟しなければなりません。さらに、情報漏洩にからみ、そのうちの一人が刑事事件の被害者になれば、企業は、悪いのは刑事事件の加害者だ、と言い逃れることはとても無理でしょう。

そもそも企業は、個人情報保護をめぐり、法廷で争うことはできないと知るべきです。極めて稀なケース、つまり被害者と称する者の主張にまるで理がない。争うこと自体に社会的な価値があり、社会が支持する。そういったケースでもない限り、まともな企業はまず争えません。何しろ争点は人格的利益です。企業が個人に対して、お前の人格はこのように扱う、と主張する。しかも、社会から見て両論争うような案件について、最高裁まで何年間もかけて徹底的に争うのか。その間、延々と、われわれはそのような企業だ、と宣伝し続けるのか。逆に言えば、そ

れだけの広報的価値を見出させる案件でしか争えないということです。企業は、個々人を差別なく扱うこと、社会的責任を果たすことが求められる時代になっていることを考えればなおさらのことです。ビジネスモデルとしても、CRM(Customer Relationship Management)⁴のよう的一对一の関係を大事にするのが本来の企業のあり方だ、という認識が社会に広がっています。その中で、個人情報をめぐる訴訟を起こされ、あの会社は人格を大切にしない、となれば、大衆資金を集める年金基金などは投資を控えるかもしれない。また、個人情報の保護が、コンプライアンスの問題と見なされるようになっていくことにも留意していただきたい。株式市場からの眼差しが強くなれば、個人情報に関する過ちは、株主の議決権行使にも影響を与え、選改任議案が通らなくなったり、報酬基準を減額する基準をつくれ、といった動きにつながったりすることも十分考えられます。

株主代表訴訟の可能性も想定すべきでしょうか。

稲垣 怖いところは、個人情報保護法に主務大臣の関与が規定されている点です。勧告や命令があったとき、適切な行動をとらなかったとなれば、株主代表訴訟が現実になる可能性があると言えます。監督権の行使がある中での違法行為ならば論を待ちません。

情報セキュリティの限界性

日本的雇用慣行の変質、雇用の流動化といった環境変化もリスクを高めるのでは。

稲垣 指摘されるように、そのような変化は忠誠心といった従業員のメンタリティに影響を与えているのでしょうか。また、現実的利益としてキャリア形成ということも

あります。わが社への貢献か、正義の実現か。戦国武将さながら、自分のキャリアにいつそう貢献するのはいずれか秤にかける。そして、滅私奉公で証拠湮滅を図るより、正々堂々と内部告発をして、事件発覚の端緒をつくったのは自分だとカミングアウトする。そのような行動により高い価値を見出す従業員が増えているのではないかと思います。

「個人情報の保護に関する基本方針(以下、基本方針)」も指摘するところですが、アウトソーシングの進展など、経営手法の変化によって個人データのコントロールが難しくなっているようです。**稲垣** つまり、インターネットとよく似た状況が企業社会に出現しているということです。インターネットの世界は、誰が管理者なのかは定かではありません。その本質は、参加者の協働による効率性の追及であり、利益の調和です。そして、企業のワークフローもそれに類似したかたちに変質しつつあります。一本化されていた管理権限のピラミッドが崩れ、雇用形態が多様化し、あるいは分社化が進み、独立した個々が納得した上で協働するかたちになっている。そのような状況がリスク管理をいっそう困難なものにしています。

この変化は、おそらく情報セキュリティのあり方にも影響を及ぼします。管理者不在のネットワークにおけるセキュリティのために大事なものは、個々の参加者の意思であり、その自由な働きを保証する自己表明と立証、そして責任です。まず、ネットワークへの参加を希望する者が、私はこういう者であり、こういうことをしたい。セキュリティのレベルはこうです、と意思を明示する。それに対して、既にネットワークに参加している側が承諾を与える。リスクを承知した自己責任とアイデンティティの証明。その評価と合意。世の

2 個人情報保護関連5法：個人情報に関する法律(基本法)、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、情報公開・個人情報保護審査会設置法、行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律(整備法)の5法。

3 1999年5月、京都府宇治市の住民基本台帳データ約22万人分が漏洩した事

件。宇治市が当該データを利用した乳幼児検診システムの開発を企図し、その開発業務を民間業者に委託したところ、再々委託先のアルバイト従業員が当該データを不正にコピーして名簿業者に販売したケース。

4 CRM[Customer Relationship Management]: 顧客の購入・利用履歴だけでなく、苦情や意見なども含めた企業とのあらゆる接点における情報を統合管理する経営手法のこと

中に、そのような流れができてつあります。情報セキュリティの仕組みであるISMS (Information Security Management System)⁵ 適合性評価制度や情報セキュリティ監査制度⁶も同じ思想的基盤を持つものです。それらが最近、注目され出したのは、単なる流行ではなく、確実な時代的根拠があるからではないか、私はそのように見えています。

民間企業はいかに対処すべきでしょうか。

稲垣 願いとしては、社会の隅々にまでデータ保護のシステムが普及して、社会がより安全になることですが、それが実態を無視した言い方であることも承知しています。ISMSや情報セキュリティ監査、JISQ15001:1999⁷などのコンプライアンス・プログラム、各種のガイドライン、それらのシステムに実際に取り組むのは企業です。当然、中には、そこまでの人手と労力を掛けて守る価値はない、そのような経営判断を下す経営者も当然いるでしょう。日本の株式会社のうち上場企業は1,200社程度に過ぎません。株式公開の大企業には、社会的な責務があり、メリットもある。しかし、数としては閉鎖会社の方が圧倒的に多く、コントロールより業績だ、と言い張るオーナーがいれば、その説得は一筋縄ではいきませんが、それでも、それぞれの会社には体力に応じてできる限りのことをしていただきたいと申し上げたい。方策を講じる上で単独では無理なら、数社で共同するという方法もあります。できることから取り掛かり、次第に充実させるという発想でよいのです。セキュリティ監査制度もそのような発想に基づくものです。総体としての評価のISMSが難しい会社も、基準をつくり、監査を実行できる。いわば松竹梅の梅コースだけれど、体力に応じた責任を果たせるという仕組みです。そこまで言っても、

なおメリットがない、という会社には、民間関係であれこれ言ってもどうにもなりません。そこから先は政治のmatterでしょう。

消費者側の意識が低ければ、無責任な企業を野放しにしてしまいますね。

稲垣 かといって、鋭敏に反応し過ぎて、右往左往して欲しくありません。住基ネットについて、片山虎之助総務大臣(当時)は「セキュリティは万全を期しているから大丈夫」と発言されました。霞が関界限では「万全を期す」とは「できるだけのことをする」という意味かもしれませんが、社会には「大丈夫」というところを鵠呑みにする人が多かった。また、意図的にそう喧伝する者もいた。しかし、セキュリティ対策は想定され得る脅威に対しては設計上の力を発揮するが、残念ながら想定外の外力には無力です。また、保証される安全はあくまで設計上のもので、それが設計通りにつくられたものか否かは蓋然性の問題となります。つまり、万全の対策を講じても、理論上、大丈夫ではないのです。そのような社会的なコンセンサスが求められます。では、やっても仕方がないではないか、という声が上がるともかもしれませんが、それは違う。重要なことは責任をまっとうすることです。コストを負担し、人手を割き、リスクに理論的に立ち向かう企業があれば、それに対する正当な評価が必要であり、それは消費者の役割です。だからこそ、企業は形式的な紛い物のシステムをつくるべきではありません。下手をすれば一種の湮滅工作です。情報開示の不手際が会社の存亡を招く時代であり、情報保護に関する浅薄な認識が命取りにつながりかねないことを、ぜひご理解いただきたいと思います。

万全な対策がないとすれば、改善が重要な意味を持つてくるということ

でしょうか。

稲垣 その意味で、ISOのマネジメントシステムの論理の枠組みはよくできています。人間には限界があり、完全はないという前提から、改善を繰り返して高めていくことを求めるものであり、まず事実を見よ、というものです。そして、リスクを洗い出し、方針を決め、対処する。それは法律家がリスクを扱うときの論理の枠組みに実によく似ており、普遍的な考え方です。

事実を踏まえながら修正を積み重ねていくと。

稲垣 さすがに狩猟民族の考えた仕組みと言いますか、綿密に計画し、理詰めで追い詰める。少しでもよく、とにかく前へ。ISMSにそのような雰囲気を感じます。ただ、私には個人情報保護がセキュリティとは対称的なものに見えます。セキュリティは、脅威を徹底的に洗い出すものです。人の化けの皮を剥ぎ、切り刻んで真実を見ようとする。あらゆる角度から光を当て、細部まで知ろうとするデジタル世界のもので。一方、そのようなことは嫌だ、というレジスタンスがある。人間とは矛盾に満ちた存在であり、影の部分もある。それを認めるべきだ。それが個人情報保護の叫びです。そこにはアナログ的というか、いい加減さを守ろうとする志向がある。そして、その二つを同じ人が同時に言っているところが興味深い。狩猟民族も、やはり理詰めの世界だけに生きるのは息苦しいのかもしれない。

データのオーナーは誰か

個人情報の有用性と保護のバランスについて、企業はどのように認識すべきでしょうか。

稲垣 かつて実業界には、ビジネスを阻止しない限度において個人情報の保護

5 ISMS[Information Security Management System]: 企業や組織が自身の情報セキュリティを確保・維持するために、技術対策のみならず、組織のマネジメントとして、ルール(セキュリティポリシー)に基づいたセキュリティレベルの設定やリスクアセスメントの実施などを継続的に運用する枠組みのこと。ISMSをその組織が保持しているかどうかを第三者が認定する「ISMS適合性評価制度」が、2002年4月1日から運用が開始された。

6 情報セキュリティ監査制度: 昨年発表された、JIS x 5080をベースとして情報資産へのセキュリティマネジメントを監査する制度。国、自治体での採用をはじめとして全国に広がりつつある。

7 JISQ15001:1999: 個人情報保護に関するコンプライアンスプログラムの要求事項。全社的な計画、実施、監査、改善によって個人情報保護の実効性を高める。プライバシーマークの準拠基準となっている。

を図っていく、という意識がありました、今年4月、基本方針が示されたとき、それがもろくも崩れ去りました。この法は、保護と利用の両方に目を配り、調整を図ろうというのですが、その方法論は個人情報の保護に万全を期すことこそが重要で、天秤ではなく個人情報保護の底上げによれ、と明言しているわけです。私もこれは妥当な見解だと思います。そのような視点で改めて法の条文を読み返せば、利用に対して圧倒的に劣位にある保護の地位を回復することで対等化を図る、という立法者の意図を読み取れるはず。最近、識者の方々が法の解説書などで同様の認識を示されています。これは単純な比較衡量ではない。おとしめられた個人の地位を回復して対等化を図るものである、そのような論陣を張られているのを知り、私も意を強くしました。

その思想は、現実の企業社会に十分理解されているとお考えですか。

稲垣 残念ながら、未だに法の「企業に重大な影響を与える場合」といった例外規定に安易に飛び付こうとする企業人が多い。それはなぜか。この法律の本当の恐ろしさが分かっていないためです。個人情報保護法は、データのオーナーは誰かという根本的な認識に変更を迫る意味において、とてつもなく重大な法律です。この法がコントロールの対象とするのは個人データであり、それは会社がコストと時間をかけてつくり上げたものです。保護法前夜、会社はプログラマーを雇い、情報を加工しているのですから、個人データのオーナーは会社だ、と考えるのが常識だった。ところが、そのデータをネットワークで回す時代になった途端、情報主体の側から、そんな使い方にはけしからん、オーナーは私だ、という反応が出てきた。そして、法もそれを是



認した。それが法律の権利者対応の規定に現れています。会社にすれば、具体的な脅威もないのに、利用目的を公表する、間違っている、直せ、使わない、なぜあれこれ言われるのか、と困惑するかもしれません。事態を理解するには、データも情報主体たる本人がオーナーだ、という認識が必要です。そう考えて初めて、この法律を読み解けます。別の言い方をすれば、システム構築の現場にいる弁護士としては、そのように見なければ、やり遂げるエネルギーが沸きません。ある石油会社と仕事をしたときのこと、全世界で数何千万枚ものカードを発行しているという。全員に通知するコストの総額を耳にしたときは、さすがに私も怯みそうになりました。例外的保護という考えでは、その負担は到底承服し難いということになるでしょう。それでも、オーナーが誰かを勘違いして、例外に寄り掛かることの恐ろしさを、ぜひご理解いただきたい。

通信の秘密やインターネットにおける匿名性などの議論が熱を帯びており、法律家の活躍が望まれていると思われます。

稲垣 法律家が前面に出る社会は発

展途上国、という言い方もありますが、ことITについては世界中が発展途上にあるわけです。法律家の仕事は、正義や公平などそれ自体は実利に結び付かないことを扱い、それをもって社会にクサビを打ち込むことです。であれば、実体に一步遅れて出番が来て当然であり、むしろ望ましいかたちなのでしょう。確かに法律家の活動領域が広がっており、積極的関与が求められます。辛いのは、あまたの法律家に、ITの特性への拒絶反応からの脱却が第一歩だ、と説かなければならないことです。

ISMS主任審査員

日本弁護士連合会コンピュータ委員会副委員長 / 弁護士

稲垣 隆一(いながき りゅういち)

早稲田大学法学部卒業、東京地方検察庁検事等を経て、1990年第二東京弁護士会弁護士登録。法務省法制審議会刑事法部会幹事(サイバー犯罪関連)、総務省地方自治体における情報セキュリティ監査の在り方に関する調査研究会委員、経済産業省情報セキュリティ監査研究会委員、警察庁総合セキュリティ対策会議委員・警察大学校講師、JIPDECシステム監査基準検討委員会委員等を歴任。主な著書に、『株主制度の運用と実務』(新日本法規出版・1998)、『株主対策実務ハンドブック』(第一法規・2003)、『個人情報保護法と企業対応』(清文社・2003)ほか多数。

読者の皆様のご意見・ご感想をお寄せください。

h-bunka@lec-jp.com

**個人情報保護法の
全面施行に向けて**
~ 求む! 世界最先端の個別法 ~