個人データ処理における企業倫理

——ビジネスにおける個人データ処理とデータ保護について——

北　原　宗　律

（受付　2004年5月10日）

1. はじめに

ビジネスのためにあらゆる機会をとらえて個人データが収集されている。個人（消費者として，顧客として）は，金融，消費，行政，教育，娯楽などさまざまなサービスを享受するために，契約上，個人データを提供しなければならない。個人データはデータ主体の人格データでもある。人格データはその人のプロフィルである。つまり，人格データによってその人の「人格像」が形成されるのである。しかも，この人格像の形成こそ，本人でしかなし得ない憲法上の権利である。これは，自己の「個人データの処分権」，もしくは「情報的自己決定権」と呼ばれる権利である。いわゆるプライバシーの権利とは異質なものである。個人データの濫用がプライバシーの権利の侵害の契機となることもあるが，両者は同じものではない。個人データが本人（データ主体）の同意なしに社会に流出し，その流出した個人データによって，その人の別の「人格像」が形成される危険性がある。誤った，あるいは，古くなった個人データによっても，そういうことが起こる危険性がある。このような危険性を一切排除するということが「データ保護」という考え方（概念）である。

ところで，そのような個人データの企業サイドにおける誤登録・不正流出・不正利用・不正提供・不正売買が日常的に行われているふしがある。顧客あるいは消費者の個人データ保護がビジネス倫理・企業倫理のひとつであることが忘れられている。環境倫理については，その遵守の様子が目に見えて誰からも理解されるが，データ保護という企業倫理については，その遵守の様子が外部からはなかなかわかりずらい。皮肉なことに，個人データ流出事件が明るみになって，倫理的な個人データ処理をやっていない会社であったと評価される。すなわち，データ保護という企業倫理が守られていなかったということになる。倫理違反を犯した企業は，顧客や消費者，社会全般から厳しい評価を受け，最悪の道筋として，企業崩壊ということに結びつく。日本においてインターネット・ビジネスがもうひとつ盛んにならないのは，この個人データの保護が確保されていないことにも原因がある。

企業の「顧客情報」，「顧客名簿」あるいは「顧客データ」が社外から流出する事件が後を

絶たない。つい最近では，インターネット接続会社から，そのユーザの個人データ，450万人分が流出した事件があった。この事件では，当時は，従業員の誰もが個人データを貯蔵してあるデータバンクにアクセスできるようになっており，心無いものが，故意に個人データのリストを持ち出したということである。同社は被害に遭った人に，謝意を表して，500円を送付した。これだけでも，約40億円の損害を蒙ったということである。

ここでいう「データ保護」とは，各企業が，個人の情報的自己決定権に基づいて個人データ処理を行うということである。日本では，この権利は法律でも判決でも正式には認められてはいない。だが，この権利は人格権から派生する権利として，情報社会における人間固有の権利といってよい。法律上正式に認められていない権利だからといって，企業はこの権利を全く無視するわけにはいかない。そこにこそ，企業のビジネス遂行における倫理性が要請されているのである。企業が個人データ処理を実施する場合には，必ずデータ主体の同意を獲得しなければならない。

個人データ処理を主管業務とする企業はもちろん，他の主管業務のために個人データ処理を必要とする企業も，この権利を最大限に尊重して業務の展開に当たらなければ，その存亡の危機に直面するであろう。海外では，データ保護担当の CEO が存在する時代である。

日本の場合，個人データ処理について，それを監視するための強力な権限のある監査人制度（外部・内部）がないから，個人データの濫用が日常的に発生しているのではないだろうか。個人データの濫用事件が発生しても，企業の代表者らしき者が謝罪の弁明を行うことで終わりになってしまう。その代表者が問題となった個人データ処理をすべて把握しているわけではない。それならば，企業の個人データ処理をすべて把握し，監視できる人的設備を設置しなければならない。個人データ濫用が発生した場合には，その責任はその人的設備にある。その代わり，その人的設備については，その資格を厳格にし，企業から独立した地位を与え，かつ，強力な権限を付与しなければならない。民間企業のみならず，公的機関においてもこのような人的設備が必要である。だが，日本の個人情報保護法も JIS 規格も，そのような制度を求めていない。

本稿では，まず，個人データの収集・利用の問題点を指摘し（2），個人データの濫用の態様を紹介する（3）。つぎに，企業における個人データの濫用によるリスクを検討し（4），JIS 規格における個人データの収集・利用制限に関する規定について検討する（5）。最後に，データ保護のための設備について（6），データ保護のための人的設備について（7），それぞれ検討する。

2. 個人データの収集と利用

2.1 個人データの収集

企業はさまざまの方法で個人データを収集する。各種契約書類から，アンケート調査から，商品モニターから，懸賞広告から，あるいは，いわゆる名簿屋からである。高校や大学という教育機関からの場合もある。

最近では，インターネットの普及によって，携帯電話またはパソコン上での懸賞広告による個人情報の収集が多くなってきている。「豪華景品」をちらつかせて，懸賞に応募させることは二次的な目的で，実は，解答応募には関係のない個人データを入力させて，それらの個人データを収集することが第一の目的なのである。

ファミリーレストランや居酒屋では，テーブルにアンケート用紙が用意してある。誕生日や結婚記念日のための割引優待券との引き換えに，氏名，住所，電話番号，家族構成，誕生日，結婚記念日，E メールアドレスなどを記入したアンケート用紙を渡す。そういう方法で収集された個人データについて，どのように管理されているのか，どこに提供されるのか，どこに貯蔵されているのか，詳しいことはわからずじまいである。顧客に対するサービス向上ということだけでは割り切れない。

デパートやスーパー，ガソリンスタンドやホームセンターなども会員カードを発行している。そのカードを利用するたびにポイントがたまり，その分の値引きをしたり，商品券を発行したりする。そのような特典が会員に与えられるのは結構なことではあるが，その時々の購買行動が逐一記録されている。これらも個人データである。

インターネットのブラウザに忍び込ませている Cookie やスパイウェアという個人データ収集用のプログラムも大いに活用されている。Cookie については，ユーザがある程度操作して，登録された個人データを消去したり，プログラムそのものを動かなくすることもできる。しかし，Cookie を停止したままにしておくと，ブラウザの動きが悪くなるという警告メッセージが発せられる。ただ，スパイウェアについては，ユーザが手を出すことはできないそうである。

サイトは Cookie を使用してユーザの過去のアクセスに関する情報を得ることができる。たとえば，あるユーザが現地の天気予報を検索し，オンラインで書籍を購入した場合，そのサイトは Cookie を使ってユーザの住んでいる都市や好きな作家を記憶し，次回にユーザがサイトにアクセスしたときにその情報を活用したりする。

「スパイウェア」はインターネットに接続されたパソコンからネットの閲覧状況や頻度，傾向などを盗み出すソフトの総称である。ネットで配布されるソフトを組み込んだり，ネッ

ト上で広告を閲覧した場合に組み込まれる場合がある。利用者が知らないうちに組み込まれている例も少なくない。これは，利用者がどういうページを閲覧しているか，どのくらいの頻度で特定のページを閲覧しているのかなどを「監視」する機能を持っている。閲覧頻度やネットショッピングの金額，回数などを集めれば，利用者の趣味や商品，サービスに対する好き嫌いや所得水準，消費性向などが分かり，マーケティングに有効である。

さらには，「Web ビーコン」といわれるタグを活用することもある。Web ビーコン（Web バグとも呼ばれる）とは，Web ページや HTML メールなどに埋め込まれるタグで，受け取ったユーザーの Web アクセス行動のデータ取得やユニークユーザー計測，HTML メールの開封調査といった機能を実現する。Web ページのアクセスログ解析などに比べ，複雑で高度な計測を可能にする反面，1 ピクセル四方の透明 gif などユーザー側はまず気がつかない形をとっていることが多いため，個人データの濫用を引き起こす懸念がある。

このような方法で個人データを収集することは，JIS 規格や法律よって規定されている「データ主体の同意」を得るということに，違反する恐れがある。JIS 規格は，個人情報の収集について，まず，収集目的を明確に定め，その目的の達成に必要な限度において行うものと定め（4.4.2.1），収集方法も，適法，かつ公正な手段で行うものとしている（4.4.2.2）。さらに，「特定の機微な個人情報」の収集を禁止する（4.4.2.3）。この「機微な個人情報」の収集・利用・提供についても，情報主体の明示的な同意がある場合には，それらの処理ができるとされている（4.4.2.3）。

2.2 個人データの利用

個人データの必要性が急速に高まるのは，企業が多様な価格，品質，表示に対する消費者の反応を正確に評価できる度合いを高めることによって，市場でのパフォーマンスを改善しようとする時である[1)]。製品がある価格で，ある特定の宣伝広告に反応し，1 年間のある時期に売れた，という事実に関するデータを集めるだけでは，もはや十分ではない。企業はますます，どのようなタイプの人物が購入し，どのようなタイプの人物が購入しなかったかについて，より多くの個人データを要求するようになってきている。そして，データベース・マーケティング技術を利用すれば，企業は，自社のアピールに最も注意を向けそうな顧客に，その宣伝活動の的を絞ることができる。企業がまだ知らない潜在的顧客に関する情報は，増え続ける個人的な顧客情報への需要の中でも，とりわけ重要な側面を有している[2)]。

顧客と接する機会のあるすべての部門で顧客情報とコンタクト履歴を共有・管理し，マーケッティング，商品・サービスの勧誘，申込，商品・サービスの提供，アフターケアのあら

1） O・H・ガンジーJr，個人情報と権力，同文館1997年，46頁。
2） 同上。

ゆる時点での個人データを収集・蓄積できるシステムが導入・活用されている[3]。それが「顧客関係管理システム（CRMS）」である。CRMSは，顧客の満足度の向上による収益の拡大化を図ることを目的とするところから，企業は常時顧客とのコミュニケーションを図り，顧客個人の価値観や商品・サービス嗜好等を把握することが肝要となる。また，CRMSは，顧客データバンクシステム（CDS），営業情報システム（SFAS），コンピュータ電話統合システム（CTIS）などから構成されている。

3. 個人データ濫用の態様

3.1 個人データの濫用

個人データの濫用とは，データ主体の許諾を得ることなく，データの収集目的以外に処理・利用・提供することである。個人データの濫用は個人データ処理のすべての段階で発生する[4]。すなわち，個人データの収集から，入力，登録，編集，照合，接続，送信，利用，提供，修正，削除，消去に至るまでのあらゆる段階で，個人データの濫用が起こり得ると考えられる。個人データは，それらが接続されることによって，人格プロフィルを形成する。また，誤った，または過去の古くなった個人データに基づいて，各種サービスが提供されるのであれば，当然，そのデータ主体は不利益を被ることになる。

以下に，これまでに明らかにされた個人データ濫用の態様を紹介する。このような事例が頻繁に発生するのはどこに問題があるのだろうか。

3.2 個人データの誤登録

個人信用情報センターで，氏名が同音異字であったために，機械製造会社社長が既に破産宣告を受けた土建会社社長の氏名と取り違えて登録されたため，金融機関からの融資を拒否されたという事例がある。これは同センターの入力オペレータが官報から土建会社社長の氏名を登録する際に，注意深く確認作業を行うか，登録後に本人確認を実行していれば，防ぐことができたはずである。また，警察庁では，コンピュータのプログラムミスで，ドライバー23人に「免許停止」と誤通報し，うち5人が実際に「免停」処分になっていた。これも，「プログラムミス」というように，あたかもコンピュータが悪いという印象を与えるが，人間がミスを犯していたことに間違いない。

3） 北岡弘章，漏えい事件，Q & A に学ぶ個人情報保護と対策，日経 BP 社2003年，52頁。
4） 北原宗律，情報社会の情報学（改訂版），西日本法規出版2003年，113頁。

3.3 個人データの不正流出

古くは，就職情報会社が全国の大学から求人用として入手した学生名簿を企業側に売り渡していたり，生命保険会社数社から大量の契約者の個人データが流出し，民間情報サービス会社で販売されていたという事例がある。また，消費者金融会社社員が支店の端末機を使用して本社のホストコンピュータから20万人分の顧客データを引き出し，300万円で売り渡していたという事件があった。社員なら，誰でも，顧客の個人データバンクにアクセスし，個人データをダウンロードできる仕組みになっていたことが伺われる。

さらに，国際電話会社の代理店から利用者名簿が流出したり，NTT の社員が顧客の個人情報を漏洩したり，ビデオレンタル店が延滞客名簿をネット上で売買したり，ある市の住其ネット用住民データ22万人分がネット上で販売されたという事例もある。人材派遣会社の登録者9万人分の個人データが同社に派遣されていたシステム開発会社の社員によって持ち出され，ネット上で販売されていたということもあった。

また，大手コンビニエンスストアの会員カードの個人情報が社外に流出していたということもあった。この事件では，その1年前から流出していたことが明らかになり，会員登録のみに使用していた住所にダイレクトメールが届いたのがきっかけで流出が発覚した。

2004年2月20日には，消費者金融の三洋信販の顧客データ32万3,820人分が外部に流出していたことが判明した。この個人データには，氏名，生年月日，住所，性別，未婚・既婚の別，職場の連絡先などが含まれていた。同社によれば，コンピュータ管理している顧客情報は約200万人で，そのすべての流出の可能性を認めている。

インターネット接続サービス会社から，450万人分の個人情報が漏れていた。460万人分の

顧客情報紛失・流出事件

企 業 名	発覚時期	流出規模	顧客への対応
ローソン	03年6月	約56万人	500円の商品券
アプラス	03年8月	約8万人	1000円の商品券
日本信販	03年8月	約2400人	謝罪文
JCB，UFJ カード	03年8月	約7000人	1000円の商品券
ファミリーマート	03年11月	約18万人	1000円のカード
NTT データ	03年12月	約4300人	謝罪文
三洋信販	04年1月	約32万人	相談受付
ソフトバンク BB	04年2月	約451万人	500円の金券
ジャパネットたかた	04年3月	約30万人	販売自粛
アッカ・ネットワーク	04年3月	30万人以上	電話相談受付

（朝日新聞2004年3月26日より）

契約者情報の入ったDVDとCDを保有する男が統括会社のソフトバンクから20億～30億円を脅し取る計画をしていたことから，この流出が明らかになった。仲間の一人の派遣社員がヤフーBBのサポートセンターに勤務し，苦情処理を担当し，契約者情報を閲覧できる立場にあったという。この時点で，すべての契約者670万人分の情報を保存したデータバンクにアクセスが認められていたのは，合計135のIDを与えられたシステム開発担当者や委託業者らだった。

3.4 個人データのネット流出

これは，個人データをインターネット利用者なら誰でも閲覧できるような状態にしたものである。

1998年1月には，大手派遣会社テンプスタッフの登録者名簿約9万人分のデータがネット上に流出したという事件がおきた。ネット上で売られていた名簿には，住所，氏名，電話番号，生年月日などに加え，容姿ランクがABCの3段階でつけられていた。犯行は，テンプスタッフに派遣されていた28歳のシステム開発会社の元社員によるものである。この事件では，テンプスタッフを相手にプライバシーの侵害などを理由とした損害賠償の訴訟がおこされる事態に発展している（「Mainichi DIGITAL トゥディ」より）。

人材派遣大手のパソナが運営する障害者の雇用支援のウェブサイトで行われていたオンライン署名に参加した人の名前や住所，電話番号などの個人情報105人分が外部から閲覧できる状態になっていた。個人情報はサイトが開設され署名が始まった2年4カ月前から誰でも見られる状態だった。問題の個人情報には，住所，氏名，電話番号のほか，メールアドレスや障害の有無，性別，年代も含まれていた（「Mainichi DIGITAL トゥディ」より）。

3.5 個人データの誤送信

新しいサービスや商品の紹介メールを送信した際，誤って一部の顧客の個人データを全顧客に送信してしまうというものである。

2000年10月25日，ソニー・クリエイティブプロダクツが顧客3000人に新製品を告知する電子メールを，誤って，送信先の3000人分全員のメールアドレスが掲載された一覧表を送信してしまった。電子メール作成担当者が本来添付すべきファイルではなく，誤って電子メールアドレスを掲載したファイルを添付して送信したということである（「Mainich DGITAL トゥデイ」より）。これは担当者の初歩的な不注意によって起こったものであるが，電子メールアドレスも個人データと考えられており，個人データの重要性の認識がないものと思われる。

2000年10月30日，ハウステンボスジェイアール全日空ホテル（長崎県佐世保市）が顧客1500人に同社の新サービスを告知する電子メールを送信したところ，誤って顧客の氏名と電

子メールアドレスが本人を含めて全顧客にも見える状態のまま送信していた。同ホテルには同日までに60件以上の苦情のメールや電話が殺到。同ホテルでは2回にわたり電子メールで全員に謝罪した。同ホテルではメールを使った告知サービスは当分の間，見合わせる方針。同ホテルによると，1500人は同ホテルが運営するインターネットを利用した予約サービス向けの登録会員。28日午後6時50分ごろ，担当者が同ホテル内にあるレストランの新メニューと宿泊プランを組み合わせた新サービスを告知しようとしたところ，誤って1500人分のアドレスを宛て先（to：）に登録。1500人は200－250人ごとに6回に分けて送信したが6通とも宛先に登録してしまった，という。本番送信前にテスト送信などは行っていなかった。同ホテルは，午後7時過ぎになって電子メールを受け取った顧客からの苦情電話でミスに気付いた。同ホテルでは同日深夜に電子メールで謝罪。翌日改めて原因とアドレスの削除を求める電子メールを送った。同ホテルでは「顧客には大変申し訳ないことをした。マニュアルの作成など必要なシステムが整備されるまではメールによる告知は自粛したい」と話している（「Mainichi DIGITAL トゥデイ」より）。

4. ビジネスと個人データ処理

4.1 個人データ流出による企業のリスク

ネット・ビジネスが拡大しない理由のひとつが，その際に必要な個人データの管理・利用に，消費者や顧客が不安を抱いていることである。ある統計でも，ネット利用者の70%がプライバシー情報が漏れることに危惧を抱いて，ネットショッピングの利用に二の足を踏んでいる，という結果が出ている。

収集した顧客の個人データについて，どれだけの意識をもって，それを管理・利用しているのか疑わしい。個人データといえども，企業にとっては，「情報財産」である。これまでの個人データの流出事件において，1人当たり，500円ないし1000円のカードや金券でもって，謝罪したということである。ソフトバンクは，今回の事件では40億円の損害を被った。

個人データの流出事件によって企業にどのような影響があるのか。一般的には以下のようなことが考えられよう[5)]。①マスコミの報道によって多くの個人，関連メディアや取引企業などから問い合わせが殺到し，状況説明などに追われる。さらに，行政当局の状況調査が入る可能性もある。②取引先から取引停止，改善通告，出入り禁止を受ける。③業界団体から締め出されたり，労働団体から調査を受ける。④行政機関からの改善命令に対応しなければならない。⑤被害者弁護団による謝罪・賠償要求や，株主からの株主代表訴訟などに対応し

5) 日本ネットワークセキュリティ協会編『個人情報保護法対策セキュリティ実践マニュアル』インプレス2003年，21頁。

なければならない。⑥会社への帰属意識，モチベーションが低下した社員の退職。⑦株価の下落。⑨業績の悪化。⑩倒産。

4.2 企業活動と個人データ処理

情報社会において，すべての企業にとって，個人データ処理が必要不可欠なものとなっている。消費者および顧客の個人データを処理したり，企業の構成員の個人データを処理することもある。個人データ処理を必要としない企業は存在しない。そして，誤った個人データ処理を行えば，企業そのものの存在が危うくなるという時代である。

個人情報保護法もJIS規格も企業の個人データ処理そのものを禁止しているのではない。個人の権利・利益を侵害しないような方法でのデータ処理は認められている。これまで，個人データ保護，すなわち，個人データの濫用防止のために，人的設備および物的設備に投資してこなかっただけのことである。もちろん，企業の個人データ保護についての認識がなかったということには大いに問題がある。

個人データ処理を不可欠とする企業にとっては，個人情報保護法やJIS規格が個人データ処理を制約するものとして受け止められているのだろう。果たしてそうだろうか。これまで，野放図にできた個人データ処理について，個人の権利・利益を保護する方法で実施する。それが，結局は企業の利益になるということではないだろうか。

5. 個人情報保護に関するJIS規格と法律

5.1 JIS規格等による収集制限

JIS規格とは，1999年3月に制定された，「JIS Q 15001『「個人情報に関するコンプライアンス・プログラムの要求事項』」のことである。その4.4.2において，「個人情報の収集に関する措置」が規定されている。個人情報の収集の原則として，収集目的を明確に定め，その目的の達成に必要な限度において個人情報を収集することが義務づけられている。4.4.2.4には，情報主体から直接収集する場合の措置が規定されている。それによれば，情報主体に対して，少なくとも，事業者内部の個人情報管理者の氏名・職名等，収集目的，提供先の受領者の氏名・職名等，預託先，収集応諾の任意性と収集拒否の不利益，閲覧請求権・修正権の説明を書面等で通知し，情報主体の同意を得なければならないとされている。また，4.4.2.5においては，情報主体以外から間接的に収集する場合の措置が規定されている。それによれば，直接収集の場合と同様の事項について情報主体に通知しなければならないと規定されている。

問題は，直接および間接収集の場合に，必要事項を収集のどの時点で通知するかというこ

とである。収集拒否の不利益の説明があることから，収集の事前に必要事項を通知しておかなければならないということであろう。対面的に個人情報の収集が行われる場合には，情報主体に示す用紙の前段部分にこれらの通知事項の記載があり，後段部分に個人情報の記載スペースがあるという形式になる。Web においても，この形式は守られるべきである。

そうすると，Cookie，スパイウェア，あるいは Web ビーコンを使用しての個人情報の収集は，「適切，かつ，公正な」手段による収集行為とは呼べないだろう。法律においても，個人データの取得目的，利用目的を特定し，データ主体に通知しなければならないとしているので，これらのソフトウェアを使用して個人データを取得することは違法となるものと思われる。

5.2 JIS 規格等による利用・提供制限

コンプライアンス・プログラムの 4.4.3 において，個人情報の利用及び提供に関する措置が規定されている。それによれば，データ主体が同意を与えた収集目的の範囲内で行われなければならないとされている（4.4.3.1）。

この規定が，最近，企業が導入・運用を進めているいわゆる「顧客関係管理システム（CRMS）」に適用されると，データ保護の観点から問題視されるのではないかと指摘されている[6]。法律のもとでは，個人データを取得する際には，必ずしも同意をとる必要はないが，利用目的を通知，公表する必要がある。反対に，利用目的を通知，公表することによって，この CRMS の活用が可能となる。ただ，ユーザー登録，顧客登録，修理登録，アンケート登録などで別個に収集した個人データを，顧客に対するサービスのために，他の目的にそのまま利用できるかどうか問題なしとはしない。

6. データ保護のための設備

6.1 データ保護の概念

データ保護（広義）は，その保護の客体と方法の観点から，データ保護（狭義）とデータ保全という二つの概念によって形成される[7]。データ保護（Datenschutz）は，「個人」の保護を，データ保全（Datensicherung）は，「データ」の保全をそれぞれ主眼とする。また，データ保護は，個人データ処理という限られた範囲内での個人の人格データの保護ということでもある。

データ保護は，主としてデータ処理における個人とその私的領域の保護という目的に由来

6） 北岡弘章，前掲書。
7） 北原宗律，データ保護法の概念，法とコンピュータ，No. 1，1983年，75頁。

する。データを保護するための法律やJIS規格は，データ主体，データ管理者およびデータ利用者というデータ処理にかかわる三者の間の権利と義務の複雑な接合部分の諸関係を規律することになる[8)]。データ主体とデータ管理者との関係においては，データ保護から導き出されるべきデータ主体の「権利」とデータ管理者の「義務」が中心となる。データ主体とデータ利用者との間にも同様の権利義務関係が存在する。データ管理者とデータ利用者との関係においては，データ管理者には，データ主体の権利の保障のための利用者の義務の履行を監視する権限が与えられている。この概念の下では，「何が（誰が）」が保護されるべきかということが問題である。データ保護はJIS規格のような法的措置によって達成される。

6.2 データ保全

データ保全は，データ自体の保護を意味し，データが記録されるデータ媒体の保護をも含む。この概念の下では，データが「どのように」保護されるべきかということが問題となる。データ保全は，とくに，データの盗難，破壊，変造，不正利用を防止するための措置によって実現される。したがって，それは，データの破壊，変造などを防止するためのあらゆる技術的な措置と，不正なデータ処理を防止するためのあらゆる組織的な措置によって達成される。データ保全の中心点に，すべてのデータファイルおよびプログラムを含めたコンピュータ支援システムの維持が考えられている。データ媒体の盗難・破壊対策としては，媒体収納庫自体の自然災害に対する安全措置および収納庫の出入りの厳重な管理などがあげられる。その他，記憶媒体の劣化対策，ソフトウェアによる破壊対策などの措置がある。また，データの不正利用や誤操作を防止する対策としては，データに対する権限関係を明確にしておくとともに，暗号化や暗唱符号の設定によって利用しうるデータを制限する方策がとられる。データ保全は，直接的には技術的・組織的措置によって達成され，法律は間接的にこれを支援する。なお，データ保護がデータ処理における濫用からの個人データの保護であり，他方，データ保全は，データ処理における濫用から個人データを保護するための技術的・組織的措置であることは上述の通りであるが，データの濫用が私的領域への侵害となる範囲において，「データ保全は，同時に，データ保護措置でもある」。すなわち，データ保全は，データ保護の実現の方法であると同時に，データ保護の前提でもあるのである。

上述したところのデータ保護とデータ保全との関係を踏まえると，「データ保護法は，『データ保護』を『データ保全』によって実現する法的措置の総体である」ということができる。これが，データ保護法の形式的概念である。

有効なデータ保護は相応のデータ保全措置を前提とするが，データ保護法がデータ保全の

8) 北原宗律，データ保護法の研究，広島修道大学研究叢書98号，広島修道大学総合研究所1997年，121頁。

方法のみで覆われるのであれば，データ保護の意義が失われてしまうことになりかねない。これらの相互依存関係を明確にするとともに，両者の特質，すなわち，データ保護は「なにを」保護すべきかということに，そしてデータ保全はこの保護を「どのように」実現すべきかということにかかわることを常に銘記していなければならない。

6.3 データ管理者

データ管理者とは，データ処理の運営管理に関して全責任を負う者をいう。ここでは，データ管理者には，個人データ保護法及び JIS 規格の規範名宛人として，データ処理の正当なる遂行と法律等の遵守のために極めて重大な注意義務が課せられる。したがって，データ処理の全責任を負う者として，その違反行為および秩序違反は個人データ保護法およびその他の法規の罰則によって処罰され，場合によっては損害賠償の責を負うべきである。データ管理者には，データ主体，監督機関に対する義務と自己の職務上の義務が帰属する。

まず，データ主体に対しては，主として，データ主体の権利に対応する義務を負う。データ主体のアクセス権行使のための個人に関するデータについての情報を提供する義務である。すなわち，貯蔵個人データの種類，内容等をデータ主体に知らせなければならない。また，データの誤りが発見された場合には，当該個人の修正権に基づきデータの修正，消去あるいは封鎖の措置を講じなければならない。

つぎに，監督機関に対しては，その立ち入り調査への協力義務および調査活動に必要な記録，データ，資料などの提出義務がデータ管理者に課せられる。このほか，個人データ処理システムの設置の際の許可あるいは届出の要件の実施について監督機関もしくは監督官庁へ報告する義務が課せられる。

最後は，データ管理者の職務上の義務である。データ管理者は，職務上，データの誤りを発見した場合には，職権によってその誤りを修正するか，誤りを含む全データを消去または封鎖しなければならない。また，不正確な，あるいは無効なデータを第三者に提供した場合には，その旨を第三者に通知する義務がある。さらに，データ保護のための技術的・組織的措置としての「データ保全」措置を講じなければならない。このデータ保全措置については，次節で述べる。

6.4 データ保全措置

データ保全 (Datensicherung) は，データ，データファイル，およびプログラムを含むコンピュータ・システムの保存ならびに防御を意味する。データ保全という概念の下に，データの破壊，変造，盗難を防止するためのあらゆる技術的措置と，不正なデータ処理を防止するためのあらゆる組織的な措置が含まれる。

データ保全の具体的・個別的な措置の実際の運用に際しては，比例原則（Grundsatz der Verhältnismeßigkeit）が適用されるべきである。すなわち，これらの措置は，必要とする費用と保護目的とが適切に釣り合う場合にのみとられるような措置で十分であるということである。データ保全措置の具体的規制については，次のとおりである。

①立ち入り規制（Zugangskontrolle）：権限の無い者が個人データ処理施設に接近することを防止する。

②紛失規制（Abgangskontrolle）：データ媒体がその処理区域から権限の無い者によって持ち出されることを防止する。

③貯蔵規制（Speicherkontrolle）：権限の無い者がデータを貯蔵することを防止し，貯蔵データが知られることを防止する。

④利用規制（Benutzerkontrolle）：権限の無い者が自動的データ処理システムを利用することを防止する。

⑤アクセス規制（Zugriffskontrolle）：権限の無い者がデータにアクセスすることを防止する。

⑥提供規制（Übermittlungskontrolle）：データの提供先を精査し，明示すること。

⑦入力規制（Eingabekontrolle）：データの入力日時と入力者を明示すること。

⑧委託規制（Auftragskontrolle）：データ処理を委託する場合，委託者の指示によってのみデータ処理が実施されることが保障される。

⑨移送規制（Transportkontrolle）：データ媒体を輸送する際の不正読み取り，変更，消去を防止する。

⑩組織規制（Organizationskontrolle）：データ保護の要請に適した組織作りが行われること。

7. データ保護の人的設備の問題

7.1 JIS 規定と法律

個人データの濫用として紹介したような事故を防止しなければならない。まず，それがデータ保護の目的である。そして，個人データ濫用事故が個人データ処理において発生しているということを鑑みれば，個人データ処理の責任者・管理者およびそれらの監視・監督体制に大いに問題が存在しているのではないだろうか。

コンプライアンス・プログラムでは，事業者の代表者は，この規格の内容を理解し実践する能力のある管理者を事業者内部から指名し，コンプライアンス・プログラムの実践及び運用に関する責任及び権限を他の責任にかかわりなく与え，業務を行わせなければならない，

と規定する（4.4.1）。しかし，このたびの個人情報保護基本法には，個人データ処理管理者についての規定はおかれていない。

ある地方自治体では，データ保護責任者・データ保護管理者・総括データ保護管理者という主官業務に応じた階層的なデータ保護のための人的設備を設けている。いずれも専従ではないが，各課の課長をデータ保護責任者，各局の局長をデータ保護管理者，総務局長を総括データ保護管理者に，それぞれ当てるという方法をとっている。

データ保護責任者は，まず，データ，プログラム及び記録媒体の適正管理が義務づけられ，通信回線等による伝送データの利用制限措置，不必要なデータの消去措置などの義務が課せられている。

また，個人情報について新たなデータ処理を行うときは，事前に，データ保護管理者がその届出を総括データ保護管理者にしなければならない。この届出に当たっては，事前に両者の協議を必要としており，その際，個人情報保護審議会の意見を尊重しなければならないとしている。

7.2 データ保護のための内部監査と外部監査

データ保護のための監督機関の組織形態としては，いわゆるオンブズマン制度から行政組織に至るまでさまざまの形態が考えられる。現状においては，行政機関としての性格をもつ形態が多い。スウェーデンにおいては，それは，「データ検査院」（Datainspektionen:The Data Inspection Board）と呼ばれている。データ検査院は，中央機関のひとつであり，他の機関と同様独立した機関である。検査院は，データ法の実施監督業務の他，一般国民のオンブズマン的役割を持っている。フランスの「情報処理および自由に関する国家委員会」（CNIL）もまた，独立した行政機関であって，いかなる階級的組織的な権限にも監督権限にも従う必要はない。ドイツの場合には，連邦法（BDSG）によって，ただ一人の「データ保護受託官」（Bundesbeauftragter für den Datenschutz, BfD）が任命され，連邦内務省に所属すること，および連邦データ保護受託官は「自己の職務遂行に当たっては何人からも独立しており，法律にのみ服する」ことが規定されている。データ保護のための監督機関は，どこからも指揮監督を受けないという独立性，公正・中立性がまず要求されるのである。

監督機関の監視方法としては，「他者監視」（Fremdkontrolle）と「自主監視」（Selbstkontrolle），つまり，「外部監視」（externe Kontrolle）と「内部監視」（interne Kontrolle）という形態が考えられる。外部の特別の機関によって公的・私的データ処理の統一的な監視体制をとるか，もしくは，自己責任の原則に基づいて内部的に段階的な監視体制をとるかは，規制対象となるデータの範囲および他の法制度との関連で決定されるべきである。

ドイツ連邦法案（EBDSG）は，官庁およびその他の公的機関のために基本的には自主監

視の方法をとっていた。ところが，この方法に対して強い批判が浴びせられた。公的分野，とりわけ行政府において私的領域の侵害の危険性が高く，データ収集などにおいて行政府の命令の拘束が強いことを考慮するならば，この領域における最も効果的な監視方法を得るためには，監督機関が一般的な決定機関から独立したものでなければならない。民間部門においても，営業の自由や私的自治の原則に任せた内部監視の方法だけでは十分とはいえない。

そこで，より実効性のあるデータ保護の監視のためには「他者監視か自主監視か」という二者択一の方法ではなく，その二つの形態の結合，すなわち，「他者監視と自主監視」という方法が必要である。

監督機関は，通常，「データ保護法の諸条項の遵守を監視する」ことをその第一義的な任務とする。その任務と権限が及ぶ範囲は，マニュアル処理を含むすべての個人データの保護にまで拡大されるのではなく，原則として，「自動的」データ処理の個人データの保護に限定されるべきである。監視の任務を非自動的データファイルにまで拡大する場合には，その種のデータファイル（いわゆる文書情報）が膨大な量にのぼり，かつ広範囲に散在するために，その任務を適切に実行できないものと考えられる。したがって，監督機関の監視の範囲は，個人データ処理システムの設置の際の許可あるいは届出によって登録されているものに限られる[9]。

7.3 データ保護監査人制度

7.3.1 個人データ流出の要因

これまでに明らかになった個人データの濫用事件における個人データの流出原因等から，個人データの流出の要因を以下のようにまとめることができよう[10]。

①不正持出し：自社での個人データ処理および外部委託による個人データ処理の関係者が個人データを不正に持ち出す場合である。それらの関係者は，処理段階ではすべての個人データを閲覧できる立場にある。しかし，個人データをメディアにダウンロードできないようにしなければならない。たとえ，ダウンロードできたとしても，そのメディアが持ち出されることができないような仕組みを考えなければならない。出入り口にメディアの検知器を設置する。

②メールによる誤送信：担当者のメール送信時での操作ミスによって，本人以外に他人の個人データを送りつけてしまうものである。メーリングリストや同報通信を使用する場合によく起こる。

---

9) 北原宗律，わが国の「個人情報保護法」の問題点――その基本的構成をめぐって――，法とコンピュータ No. 8，1990年，74頁。

10) 稲垣隆一編著，個人情報保護法と企業対応，清文社2003年，265頁以下。

③システム不備：会社の Web サイトのシステムの不備または設計ミスによって，インターネット利用者に会社保有の個人データが閲覧可能な状態になってしまう。

④アクセス管理の不備：個人データへのアクセス権限のない者がアクセス管理の不備から個人データにアクセスできたことが契機となって，自制心を失い，ついつい個人データを持ち出してしまう場合がある。

⑤不正アクセス：インターネット等のネットワークを通じてシステムに不正に侵入し，個人データをダウンロードする。

⑥コンピュータウイルス：個人データを収集するウイルスも考えられるが，多くのウイルスは不正アクセスの準備をする。

⑦ソーシャルエンジニアリング：システムや Web サイトへの不正アクセスに必要な他人の ID やパスワード，システム管理者情報を不正に取得する行為である。

⑧運用管理の不備：個人データ処理のための，個人データの移送，配信，送信，送付といった個人データの移動におけるデータ管理のリスクから個人データの流出が発生する。

⑨ゴミあさりと廃棄物からの復元：ゴミや廃棄物のなかから個人データを復元する。入力済みのアンケート用紙など焼却されずに拾われることもある。

⑩窃盗：ネットワークから個人データを盗む，あるいは事務室に侵入してハードコピーした個人データを盗む，コンピュータを盗んだら，そのディスクに個人データが記録されていた，ということもある。

⑪委託先：個人データ処理を委託したときに，委託先がデータ保護の人的・物的設備が不十分な場合には，個人データの流出事件が発生する頻度が高いといえる。

7.3.2 データ保護監査人

個人データの濫用を防止するためには，まず，データ管理者の義務を明確に，権限を強化しなければならない。つぎに，個人データ処理を監視・監督する人的設備を設けることである。JIS 規格にも法律にもこの人的設備は規定されていない。

個人データ処理を実施する企業は，個人データ処理の監督者として，データ保護監査人を配置しなければならない。データ保護監査人に企業の個人データ処理の監督に当たらせる。企業からは独立した地位を与えられるが，重大な個人データの濫用を引き起こした場合には，個人データ処理を封鎖できるような強力な権限をも与えなければならない。

国に「データ保護庁」を設置し，そこに国の「データ保護監査人」を配置する。自治体には「データ保護局」を設置し，そこに自治体の「データ保護監査人」を配置する。個人データ処理を実施する企業にも「データ保護監査人」の配置を義務づける。

7.3.3 データ保護監査人の資格

データ保護監査人（Data Protection Commissioner）の資格制度を設ける必要がある。つまり，データ保護監査人は，その任務遂行のため，法律的知識および技術的知識を十分兼ね備えた人格者でなければならない[11]。個人データの流出の要因から，その流出を防止するためには，それらの要因を除去することが最も効果的なデータ保護のための方策であるはずである。したがって，個人データ処理および個人データの濫用を監視する「データ保護監査人」には，多岐にわたる法律的・技術的・経営的知識が要求されるのである。

まず，法律的知識としては，いわゆる「個人情報保護法」全般にわたる知見が要求される。自治体の個人情報保護条例についての知識も要求される。個人データの海外移動が頻繁に行われる場合には，関係諸外国のデータ保護法についての知見も要求される。その他，個人情報保護のための「JIS 規格」「ガイドライン」や「指針」というものについても熟知していなければならない。

つぎは，データ保全に係わる技術的知識およびデータ保全措置の具体的方策に係わる知識を具備していなければならない。すなわち，個人データ処理システム，コンピュータ・ネットワークおよびネットワークセキュリティに係わる専門的・技術的知識である。データ入力・出力装置および周辺機器，データ転送装置およびデータ転送メディア，外部データ貯蔵ユニットおよびデータ貯蔵メディア（データバックアップ），コンピュータネットワークおよびネットワークトポロジー，ネットワークへの脅威およびネットワークの保護に係わる技術的知識などである。

7.3.4 データ保護監査人の権限

データ保護監査人は企業に所属するものの，地位は独立している。極めて重い責任が負わされるのあるから，その権限は非常に強固なものとならざるを得ない。最強の権限としては，所属企業の個人データ処理の一時的な封鎖もしくは廃止までもできるものである。

データ保護監査人の一般的な権限として，以下のものが考えられる。

①データ保護のための専門的知識・技術の適用権限

②データ保護とデータ保全のためにすべての企業に対して，直接的な監査と立ち入り権限

③企業首脳部に対するデータ保護とデータ保全の問題についての勧告権限

④疑惑的問題についての監督官庁への告発権限

11） Reinhard Voßbein, Die Organisation der Arbeit des betriblichen Datenschutzbeauftragten, DATAKONTEXT 1997, SS. 47ff.

8. お わ り に

情報社会において企業が拡大・発展を目指すのであれば，顧客，消費者の個人データの保護が肝要である。個人データ処理が経営上不可欠なものであるならば，まず，個人データの保護措置を完璧なものにしなければならない。それが企業倫理でもある。

本小論においても，「個人データ」と「個人情報」とを何の区別なく使用してきた。わが国の個人情報保護法においては，「データ」と「情報」とが別々の意味に用いられているが，データ保護の議論あるいは個人情報保護の議論において，両者を区別する実益はないものと思われる。ちなみに，諸外国においても，このような区別に出会ったことがない。

いずれにしても，個人データであれ，個人情報であれ，これらは企業の「情報財産」の一部である。個人データの重要度については，それぞれの企業において違いがあるのかもしれない。業務に不可欠な膨大な個人データ群，つまり，個人データバンクそのものが「企業秘密」のはずである。個人データ以外のデータや情報でも，一端公表されると，それはもう企業秘密ではなくなってしまう。企業秘密といわれるためには，秘密扱いに足るだけの厳密な管理が前提となっている。このような社会であるにもかかわらず，「データ窃盗」罪という規定がないのも，何か時代遅れの感がしないでもない。

データ主体の立場からいえば，一端，個人データが流出してしまえば，どのような救済措置，損害賠償を講じようとも，完璧な回復，つまり，元に戻すということはあり得ないのである。それこそ情報の性質のせいである。1980年代初頭，最初の個人情報保護法案が国会で議論されたことがあった。「まだ，問題が現実化していない。法律の必要性を感じない。」ということで，審議未了，次々と廃案になってしまった。個人データ保護については，問題が現実化してしまっては，データ保護の意義が失われてしまうのである。個人データ保護は，個人データ濫用の「未然防止」に意味がある。個人データの濫用を起こさないというところにデータ保護の目的がある。そのような観点から，個人情報保護法も JIS 規格も考えられたはずである。もし，そうなら，個人情報保護法および JIS 規格の完全実施によって，個人データ濫用という事件は皆無になるはずである。

データ保護においても，やはり，最後には，そのための人的設備の問題が残される。法律や JIS 規格の完全実施という場合にも，それを監視する人的設備が必要である。個人データ処理の内部告発的役割を担うデータ管理者，そして，外部告発的役割を担うデータ保護監査人というような，人的設備が配置されて初めて完全なデータ保護が実現されるのである。