個人データ処理と人的設備

――データ管理者・データ監査人・データ保護監査人――

北　原　宗　律

（受付　2007 年 5 月 10 日）

要　　旨

データ保護とは，個人データ処理におけるデータ主体の人格権の保障である。この領域における人格権は「情報的自己決定権」と呼ばれるものである。この情報的自己決定権は，この権利をめぐる法律規定とその法律の中に盛り込まれるところの「データ保全」，すなわち，データ処理に関わる技術的・組織的措置によって実現される。この組織的措置が個人データ保護のための人的設備ということである。個人データの濫用，とりわけ，データの流出事故はこの人的設備に原因があると思われる。

人的設備として，「データ監査人」，「データ管理者」，および「データ保護監査人」が挙げられる。データ監査人は，個人データの「一生」を実証・把握する任務がある。データ管理者は，データ保護法の規範名宛人として同法のコンプライアンス文化を醸成し，データ保護のための技術的・組織的措置を実施する義務がある。データ保護監査人は，個人データ処理全体を監視するとともに，データ保護コンプライアンス監視も行わなければならない。個人データ濫用の程度により，データ処理システムの封鎖・廃棄を勧告する権威も授権されている。監督機関としての「情報コミッシュナー」もこの人的設備である。

キーワード　データ保護，データ管理者，データ保護監査人，データ監査，人的設備

1. は　じ　め　に

個人データの濫用の問題は，個人データをコンピュータで処理する以前から現実化していた。それは，個人データを紙のファイルに記録し，そのデータをもっぱら人間の手で処理をしていた時代である。個人データの濫用とは，個人データを誤って記録したり，収集目的以外の目的のために個人データ処理をすることである。それによって，憲法で保障されている個人の人格権の侵害という結果を導くことになる。個人データは人格データであり，その人格データによって当該個人の人格像が形成される。誤ったデータ処理によって本人とは別の人格像が形成される，というのがこの問題の本質である。ペーパー・ファイルとデータ・ファイルにおいても，問題の本質は何ら異なることはない。ただ，データ・ファイル，すなわち，コンピュータ処理の場合には，その侵害の拡大の速度と範囲に計り知れないものがある。

したがって，データ保護とは，個人データ処理におけるデータ主体の人格権の保障という

ことになる。つまり，「個人データ処理」という限定された範囲における個人の権利の保障という意味しか持たない。1983年12月，ドイツの連邦憲法裁判所は，「情報社会においては，個人は，『情報的自己決定権』を有する」という判断を示した[1)]。その情報的自己決定権（Recht auf informationelle Selbstbestimmung）という権利は，「データ保護の権利」（Recht auf Datenschutz,The Right of Data Protection）であると，その判旨から推察できる。それ以外の範囲については別の問題である（例えば，いわゆる「プライバシーの権利」の侵害，自由権の侵害など。）。また，データ保護の対象となる「個人データ」は，当該データ主体の手から離れた，つまり，データ主体の守備範囲には存在しない「データ」である。それらの個人データは，組織に保有される場合が多い。保有個人データは，自己の個人データではあるが，データ主体としては，それらのデータをどうすることもできない状況下に置かれている。個人データが自己の支配下にある場合には，データ保護の問題は生じないように思われる。

さて，データ保護の矛先が向けられるのは，もっぱら，データ主体の手から離れ，そして，組織が保有する「個人データ」に対してである。したがって，組織は，「善良なる管理者の注意をもって」，この個人データを管理しなければならない。この場合の「管理」は，「データ処理」という意味である。

組織において，個人データ処理にかかわる人的設備として，「データ処理者」「データ管理者」「データ監査人」「データ保護監査人」および「情報コミッショナー」と呼ばれる者が存在する。昨今の個人データの濫用事件，とりわけ，個人データの流出事件をみると，これらの人的設備がその本来の役割を果たしていないのではないだろうか思われる節がある。それらの人的設備は，直接的には，「個人データ処理」に関わっているのであるが，「適法に」個人データ処理を実施する義務，個人データ処理が「適法に」実施されることを監視する義務をそれぞれ負っているのである。ということは，これらの人的設備は，個人データ保護のための人的設備である。本小論では，これらの人的設備の役割と権限について検討することにする。

本小論において，まず，データ保護の概念を明らかにし（2），個人データ処理の透明化に資するデータ監査について述べる（3）。つぎに，法律の実効性を確保するための個人データ処理の実施手続について検討し（4），データ保護監査のための人的設備に言及する（5）。

2. データ保護（広義）の概念

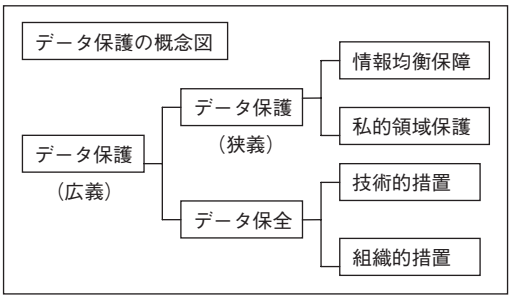
データ保護は，「データ保護」（狭義）と「データ保全」からなる。（狭義の）データ保護

1） BVerfGE 65, 42. なお，この判決の概要については，参照，北原宗律，「データ保護法の研究」，広島修道大学研究叢書，第98号，1997年，pp. 83–91.

は，権力間の「情報均衡の保障」と個人の「私的領域の保護」からなる。データ保全は，データの盗難・破壊等を防止するための技術的措置と不正なデータ処理を防止するための組織的措置からなる[2)]。

2.1 データ保護（狭義）

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する。データを保護するための法としてのデータ保護法は，データ主体（当該データが帰属する当事者），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。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）」が保護さるべきかということが問題である。データ保護は直接に法的措置によって達成される。



2.2 データ保全

他方，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」保護さるべきかということが問題である。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

2） 北原「データ保護法の研究」，pp. 119–122.

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。

3. データ監査

データ監査は，個人データ処理の実態を把握するために実施されるものである。とりわけ，組織内の「個人データ」の取扱方について，詳細かつ厳密な方法で，明らかにしなければならない。そのためには，上層部の支援体制，情報提供等が不可欠である。また，データ監査報告書に基づいて，個人データ処理の「届出」「登録」申請書が作成される。この報告書は，データ保護監査人による監査の資料としては最も重要な意味を持つ。

3.1 データ監査の実施

データの監査は，データ・ファイルのみに係わるのではなく，データ保護法およびデータ保護原則がいつでも遵守されているということを保証するための組織内の機構もその視野に入れなければならない。

識別可能な個人（データ主体）についてのさまざまなデータ・ファイルが合法的に処理されていることを保証する唯一の方法は，データを実証することである。個人データを含むすべてのファイルは特定されなければならない。そして，それらのデータはどこから来たのか，データはどのようにして収集されたのか，データはどのように処理されたのか，データはどのように修正されたのか，データはどのように開示されたのか，データはどこに提供されたのか，データはどのくらいの期間保存されているのか，そしてデータは何時どのような方法で最終的に消去されたのか，というようなことが問われなければならない。データ監査は，他の監査と同じように，ある特定の時間における組織の瞬間的活動にすぎない。つまり，データ監査は，それによって違法な事実を何も発見できなくても，それだけで，継続的なコンプライアンスを保証するものではない[3)]。

3） R. Morgan/R. Boardman, ‘Data Protection Strategy’, SWEET&MAXWELL, 2003, p. 33.

3.2　データ監査の範囲

データ監査は，その性格上，組織のあらゆる部所にまで入り込む必要がある。ひとつの部門で完璧にかつ正確に取り扱われる個人データが，別の部門ではかなりいい加減に利用されるといったことだってありえる。たとえば，販売チームは顧客の個人データを扱うに際してデータ保護原則に従うのであるが，他方，マーケティング・チームはデータ保護法に全面的に係わっていることに気がつかず，無謀にもデータ保護原則を無視することだってありうる。すべてのデータがコンピュータ・ファイルやウエブ上の情報でなくてもそういうことが起こりうる。データに何が起こっているのかを検証する際には，組織外へのデータの移送，サプライヤー，ディーラー，配給業者のような取引相手，規制機関，政府機関，その他のマーケティング会社および一般公衆のことも考慮しなければならない。また，コンピュータ・ファイルで，ウエブで，電子メールで，普通郵便で，電話のような内線通話でデータを移送するのかどうかということも考慮しなければならない。さらに，国内だけの移送なのか，海外における契約者，支店，取引相手への個人データの移送なのかも考慮の対象になる。

3.3　データ監査のチェック・リスト

ある組織および組織が保有するデータを検証する監査人は，そのデータについて，以下の項目をチェックすべきである[4)]。

・監査の範囲
　・組織において，どんな部局，ファイル，システムがこれまで監査の対象になったか。そして，その理由。
　・組織の全体的なコンプライアンスの指示が十分であるかどうか。
・データ監査の種類
　・コンピュータ？
　・電子メール？
・その他の通信文やメモ書き
　・インターネット？
　・イントラネット？
　・マニュアルファイル（ファイリング・システム）
　・ビデオ（CCTV，写真，フィルム）？
　・オーディオ（契約，教育，ボイスメール）？
　・バイオメトリック？

4）　Ibid. pp. 51–53.

・その他（例えば，タコグラフ）？
・個人データの種類
・個人データか他のデータか？
・個人データなら，センシティブ・データか？
・アクセス可能なデータか？
・そのデータには秘密データ（医療・金融情報）が含まれるか？もし，そうなら，この結果は何か？この結果について個人は何を知らされるのか？
・クッキーは入っているのか？もし，入っているなら，それはどのように使われるのか？
・データ主体の種類
・職員か？
・一般人か？
・顧客か？
・取引先か？
・データの「保有者」
・誰か？
・「私的」ファイルか？
・私的な電子メールはどのように扱われるのか？
・あるとすれば，データ処理者によってデータのどの部分が処理されるのか？
・当該組織は，データ処理者として，他の組織のためにデータ処理を実施するのか？
・データ処理の目的
・どんな方法で，どんな理由で，データが収集されるのか？
・データ収集について，個人にどんな情報が提供されるのか？どうのように？いつ？
・データの利用がデータ収集時の目的に十分適合しているか？
・DM を実施しているか？実施しているなら，どんな方法か？
・趣向サービスに同意を求めているか？データの正確性を保証する措置は？誰がそれを保証するか？
・データが不正確の場合の結果は？
・最新性はどのように維持されるのか？
・どのくらいの期間保有されるのか？
・データが利用されなくなったときはどういうことが起こるのか？
・データの安全性
・物理的安全性

・スタッフの安全性
・システムの安全性――パスワード，ファイアウオールなど。
・データ処理者による安全性
・データ処理者の選任は？
・データ処理者の安全性のチェックは？
・どのように記録として残されるのか？
・継続中のテストプロセスはあるのか？

・EEA の外部への移送
・ファイルは？
・電子メールは？
・インターネット情報は？
・イントラネット情報は？

・アクセスの容易性
・データのなかの特定個人の識別はどの程度容易なのか？

・処理と手続
・いかなる産業組合・同業組合の指針が利用可能か？
・個人データに関して公刊されたプロセスと手続が存在するか？
・どのようにしたらそれらをスタッフ等に気づかせることができるか？
・どのように実施するか？
・どのように最新なものにするか？
・誰が責任を負うか？
・どのようにして，その責任者を組織の機構に適合させるか？

・データ保護の届出
・組織は届出を実施したか？
・実施していなければ，なぜその例外と考えるのか？
・届出は監査によって認証された個人データと矛盾しないのか？
・その目的は？
・届出は最新のものか？
・どのようにして届出の最新性を維持するか？

・データ主体の権利に基づく請求に応える手続が実施されているか？
・情報コミッシュナーの行動規準（CCTV や雇用に関する）は守られているか？
・組織は CCTV 用の小冊子を用意しているか？

3.4 データ監査人

データ監査は組織のすべての部門で行うことになる。しかも，監査を実施する外部の専門機関を利用するのが最善である。外部の機関を利用するメリットは，次のようなものである[5)]。

1. 外部機関は監査業務の経験が豊富であり，データ保護法のデータ保護原則を熟知している。

2. その作業は一回限りで，ある特定の時間の寸見が要求される。おそらくすでに何年間も同じ仕事に従事している通常のスタッフではこの作業を瞬時にこなせないだろう。もし，その作業がだらだら続くのであれば，それぞれの時間で組織のそれぞれの部局で寸見は不可避的にぼやけ，不正確なものとなってしまう。

3. 外部の監査人は，それまで組織の人間ではなかったし，公平な目でその作業を続けられる。

4. 外部の監査人は守るべき特権をもっていない。

5. 外部の監査人は組織の一員ではないから，隠し事をされたりすることはないし，困らせたり，脅迫されたりすることは覚悟している。

監査人の作業の最終的な報告書は，どの範囲で組織がコンプライアンスに適合していないか，そしてどうすればコンプライアンスを達成し，継続できるか，ということについての分析結果となる。

4. 個人データ処理の実施手続

個人データ処理システムの設置もしくはその実施のために，監督機関への手続が必要である。その手続を踏まなければ，個人データ処理の実施はできない。その手続として，「許可制」と「届出制」がある。一般的には，許可制の方が届出制よりも厳格な規制を課すことが可能である。したがって，個人の権利に重大な侵害の危険をもたらす可能性のあるシステムに対しては許可制が，他方，明らかにそういう危険の可能性がないか，もしくは常時定型的なデータ処理のみを目的とするシステムに関しては届出制がとられている。

4.1 個人データ処理

データ処理形態の種類について，自動的（電子的）処理と非自動的（マニュアル）処理に大別される。法律による規制対象をマニュアル処理にまで拡大すれば，法律の実効性を弱める危険がある。自動的処理についても，同様の危険性があるが，規制対象とする個人データ

5） 北原，前掲「データ保護法の研究」，p. 146.

処理の範囲を確定するために，個人データ処理の実施について，「届出」もしくは「登録」制度を設ける必要がある。個人データ処理システムの設置または実施の手続は，データ保護監査対象のシステムを確定することに資するのである。

4.2 個人データ処理の届出

データ保護の下での主要な原則の一つは，透明性ということである。すなわち，個人が，自己についての個人データの処理をどの組織が実施しているかを，容易に見つけ出すことができる方法がある，ということである。この目標を推進するために，EU のデータ保護指令は，加盟国に対して，個人データを処理する組織の登録制度を設立するよう求めている。イギリスにおいては，この登録制度は情報コミッシュナーの下で行われる。登録文書は，公式文書となり，コミッシュナーのウエブサイトで探すことができる。

そこで，1998年イギリス・データ保護法第17条は，データ管理者は，これに登録されていなければ，個人データ処理を実施することはできないと規定する。1984年イギリス・データ保護法の登録制度が，1998年法においては，「届出」（notification）制度と呼ばれている。届出違反は刑法的犯罪である。最高5,000ポンドの罰金が科せられる。つまり，届出の手続をせずに個人データ処理を実施した場合である。

因みに，フランス法およびスウエーデン・データ法は，許可制と届出制を併用して導入し，アメリカ法は新規システムの設置についてのみ事前に議会および行政予算庁への通知制度を導入している。また，ドイツ法は各機関の任務・業務の合法的遂行である限りシステムの設置を制限していない[6)]。

届出義務は，データ処理の目的と方法を決定する各組織に課せられる。その義務が各組織に課せられるということは，グループ会社は，グループ内の各々の会社が届出をしなければならないということである。したがって，グループ内のすべての会社を覆うような「包括的」届出ということはあり得ない。また，届出はイギリス国内の組織のデータ処理にしか適用されない。そのため，EEA の複数加盟国に設立されている組織は，各国の届出要求事項に従わなければならない。

4.3 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。データ処理作業を行うのはデータ処理者であるが，データ処理者の違法行為についても，データ処理を監督する立場から，データ管理者の責任となるのである。データ管理者には，個人データ保護

6） ドイツ・連邦データ保護法（BDSG）第 9 条の附則を参考にした。

法の規範名宛人として，データ処理の正当なる遂行と法律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。

データ管理者の責任となる違反行為とは，個人データの収集，記録，貯蔵，分類，伝達，編集というようなデータ処理のすべての操作段階において行われる違法行為や個人データの漏洩，すなわち，不特定多数者へのデータの不正開示の行為である。データ保護法に個人データ処理システムの設置または実施手続が規定されているならば，その手続違反についても，データ管理者の責任が問われる。

また，データ管理者が講ずべき「データ保全措置」とは，つぎの10項目である[7)]。

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） 北原宗律，「イギリス・データ保護法におけるデータ監査とコンプライアンス」，経済科学研究，第9巻第2号，2006年，pp. 200–201.

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。

5. データ保護監査設備

データ保護法の実施を促進し，法律の遵守を監視する人的設備の設置が必要である。すなわち，個人データ処理におけるコンプライアンスの監視者である。その設備には，「データ保護受託官」制度，オンブズマン制度，行政組織というような形態がある。監視方法には，「他者監視」と「自主監視」，「外部監視」と「内部監視」がある。それらのすべてを組み合わせた，いわゆる「ハイブリット方式」が最も効果的であると思われる。この人的設備には，独立的地位と最強の権限が与えられなければならない[8)]。

5.1 データ保護監査人

コンプライアンス戦略における第一歩は，組織が最高度のレベルのデータ保護方針を採用することである。しかしながら，実際には，データ保護に全責任を負う人的設備を任命することから始めるのが最もよい。すなわち，データ保護監査人の任命である。つぎに，その最初の任務の一つは，データ保護委員会において承認されるような必要な方針案と手続案を策定することである。組織ひとつ一つにデータ保護に全責任を負う人的設備を配置することは重要なことであるが，その組織が大規模か，膨大な個人データを保有するか，もしくは複雑な個人データ処理を実施している場合には，データ保護監査人を補佐する人的設備を組織内に任命することが必要であろう。

データ保護監査人は，必ずしも，専任なくてもよい。つまり，法務部門や情報部門に所属する者がデータ保護監査人となることも通常のことである。また，個人データの収集がビジネスにとって批判的である場合には，データの収集と処理に詳しい者がデータ保護監査人の役割を援助することは理解できよう。例えば，クレジット照会ビジネスや DM ビジネスを運営する組織にとっては，ビジネス開発部長がデータ保護監査人として行動するのが得策である。データ保護は情報部門が行う特別のことではなく，その組織内ではより広い重要性をも

8） 北原宗律，「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――」，経済科学研究，第 8 巻第 1 号，2004年，pp. 97–101.

つことであることをその組織に知らせることも有用である。ある組織は，データ保護監査人またはチーフ・プライバシー・オフィサーの選任を開始している。この傾向はアメリカ資本の企業に最も共通しているが，それらの組織は必ずしもアメリカのプライバシー法に従わなくてもよい。

データ保護監査人はその責任と義務が明確に規定されていることを保証する必要がある。データ保護監査人の報告方法と権限も特定されるべきものである。ある組織が「コンプライアンス」部門を持っている場合には，この部門がデータ保護の責任をとることもある。この場合，データ保護監査人はコンプライアンス監理者，会社秘書または法務部長（取締役会メンバー）に報告することになる。データ保護監査人が誰に報告しようとも，データ保護監査人は取締役会のメンバーとなり，データ保護の問題を最高度の課題として提起することができる。この領域における実質的な失敗は取締役会が真摯にデータ保護責任をとることを保証すべきである。取締役会メンバーはデータ保護監査人に必要な権限とデータ保護監査人の進言が最高度レベルで承認され，かつ実施されることを保証する「権威」が与えられるべきである。

組織はデータ保護監査人を任命すべきことを勧めるが，現行法はそのことを規定していない。従って，法律はデータ保護監査人に対しても，特に何の責任を課していない。しかしながら，データ保護監査人は，他の会社の経営者と同様に，法律違反がデータ保護監査人の同意，黙認または懈怠に基づくものであるならば，同法の下で個人的な責任を引き受けることになることは当然知っているはずである。そのことにより，ある個人がデータ保護監査人に選任されて，その問題についてほとんど初歩的な知識しか持ち合わせていないならば，このリスクを最小限にするために適切な教育を受けることを申し出るようにアドバイスされてしかるべきである。そのような教育は取締役会メンバーにまで広げられることが望ましい。

5.2 データ保護監査人の権限

データ保護監査人は組織に所属しているものの，その地位は独立している。極めて重大な責任が負わされるのであるから，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，所属組織の個人データ処理システムの一時的な封鎖もしくは廃止を勧告するものである。

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[9)]。

（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組織に対して，直接的な監査と立ち入り

9） Reinhard Voßbein, Die Organisation der Arbeit des betrieblichen Datenschutzbeauftragten, DATAKONTEXT, 1977, SS. 47ff.

権限

(3) 組織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

6. ま と め

多くの業界で監査制度が導入されている。しかし，ここ数年の間で，その制度の破綻を示すような事件が日常的に起こっている。もちろん，業界全体に及ぶ事件ではなく，ある業界の数社に限られているのだが。そのなかで，監査法人自体の解体に発展したという事件もあった。

「個人データ処理」の業界においては，その危惧はまったくないのであろうか。

情報社会において，「個人データの取扱い如何」が，組織の存亡にかかわるのみならず，組織に所属する構成員の存亡，すなわち，解雇・辞職という結果を引き起こすこともあり得る。

個人データ保護の実現は，結局のところ，人間の問題である。データ処理の目的や方法を決定する人間，すなわち，データ管理者，個人データ処理を監視し，コンプライアンスを監視する人間，すなわち，データ保護監査人，これらのデータ保護のための人的設備の資質と権威が問われている。

個人データ処理が不可欠な組織（情報社会においてはすべての組織）においては，さまざまな方法と機会を利用して，すべての構成員にコンプライアンス文化を浸透させなければならない。

「データ監査」や「届出制度」の導入は，個人データ処理の「透明化」のひとつの方策である。これらの方策は，個人データ処理に関わるほとんどすべての情報（メタ・データ）を要求している。データ監査を実施することによって，組織が，どんな種類の個人データを保有し，処理し，利用し，提供しているかを把握することができる。つぎに，この透明化によって，個人データ処理にかかわる説明責任を果たすことができる。つまり，個人データ処理の必要性・正当性をデータ主体に説明し，納得させることができるのである。

すべてのデータ主体にとっても，この個人データ処理の透明性が最も重要な意味をもつ。すなわち，情報的自己決定権行使の踏台となるのである。つまり，個人が自己についての個人データ処理を，どの組織が，どの部所が実施しているかを容易に見つけ出すことができるのである。さらに，個人データのアクセス権や修正権という権利を行使することを可能にする。