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

北　原　宗　律

（受付　2005 年 10 月 11 日）

1. は　じ　め　に

日本では，2005年４月から，いわゆる個人情報保護法が全面的に施行された。法律が動き出したからといって，問題が一挙に解決されたという経験は，未だかつてない。個人データをめぐる諸問題に関しても同様である。

個人データ処理は個人データをコンピュータで処理をするという意味である。そこで起こる問題が個人データの濫用である。そして，個人データの濫用の未然防止が個人データの保護ということである。個人データの保護を実現するためには，そのための人的設備の設置が不可欠である。データ保護のための物的設備の充実も重要な課題であるが，それ以上に，人的設備の充実が必要である。

イギリスの1998年データ保護法は，データ保護のための人的設備として，情報コミッシュナー，データ保護監査官，データ管理者およびデータ監査人の設置を規定する。これらの人的設備の役割と義務の履行を通して，データ保護法のコンプライアンス文化を醸成しようとするものである。すなわち，すべての組織におけるデータ保護法の遵守という文化である。

データ保護法は，情報コミッシュナーへの個人データ処理の「届出」を組織に義務づけている。そのため，組織は，個人データ処理および個人データの所在を詳細に把握しておかなければならない。その作業が「データ監査」である。データ監査は，届出のためだけに実施されるのではなく，組織のデータ保護方針の策定にも役立つものである。また，個人データ処理の透明性を保証する。

本小論において，データ保護のための人的設備について検討をする。データ監査人の役割と義務（2，3），データ保護監査官の役割と権限（4），データ管理者の役割と義務（5）について，検討する。

2. データ監査の導入

2.1 データ監査の役割と範囲

データの監査は，データ・ファイルのみに関わるのではなく，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明らかにさ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，そのことだけで，継続的なコンプライアンス（法律の遵守）を保証するものではないのである[1)]。

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得る。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関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得る。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。

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[2)]。

1） R. Morgan/R. Boardman, Data Protection Strategy, SWEET & MAXWELL, 2003, p. 33.
2） Ibid. p. 34.

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の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。

2.2 監査前の準備

コンプライアンスを容易にするための管理体制の整備ということがある。この主要な部分は，コンプライアンス戦略の推進のため，取締役会の全面的な支援を得る必要性があるということである。データ保護を管轄する既存の体制が取締役会から支援を得られるかどうか，監査手続きがその支援を享受できることを保証すべきである。その支援を得るだけで，データ監査人は個人データの取り扱いに関する真実を得ることができる。監査報告が組織にとって本当の価値をもつ唯一の方法は，監査結果が取締役会に向けられており，そして取締役会がその監査結果を全面的に受け容れることである。つまり，調査終了時での監査人の報告が取締役会によって閲覧・議論されるということを意味する。たとえその組織が，もちろん，監査人と日々関係をもっているデータ保護監査官をすでに設置してあっても，取締役会の究極的な責任はもっとも重いものである。

したがって，データ監査人が取締役会の支援を得られるならば，スタッフがデータ監査の目的とコンプライアンスの必要性を知らされなければならないだろう。スタッフは，前もって，監査の内容と目的について知らされ，すべての情報を監査人に速やかに提供するようにすべきである。組合の代表者やそのほかのスタッフとの相談機構も利用されるべきである。

現在あるすべてのデータ保護手続き，行動規準，戦略，規則，枠組み，ハンドブックのなかのスタッフ心得，イントラネットは，監査の前に，監査人に手渡しておくべきである。その他の関係文書には，コールセンターで使用されるマニュアル，組織の構成図，その他関係

部局等の構成図が含まれる。これらの文書のすべてが提供されるならば，監査人は，コンプライアンスの弱い部所を把握し，そのような部所が徹底的に調査されることを保証するものである。

他の外部のコンサルタントと同じように，監査人も組織内の必要なすべての設備が提供されなければならない。つまり，部屋，机，駐車場，組織のネットワークの利用などである。

3. データ監査の実施

3.1 記録と処理

監査の最初の作業は，組織が保有するすべての個人ファイルやデータを特定することだろう。コンピュータ・ファイルがすべてではない。CCTV，オーディオテープ，タコグラフレコード，いわゆるマニュアルレコードも監査作業の対象となる。いずれの組織においても，ファイル一つひとつを精査し，それがどのように処理されているのかを把握することは困難である。その代わり，監査人は，各種ファイルの代表的なサンプルを検証する必要があろう。データ保護法 1(1) において，「処理」は極めて広く定義されており，「検索，照会そして利用」と開示というような簡単なことから，ファイルの始まりであるデータの「獲得，記録または保持」，ファイルの終わりであるデータの「消去，破壊」まで定義されている。法律によって定義されていないもので，データに関してできることは，文字通り何もない。つまり，その定義において，処理のすべてのステップが網羅されている。

ファイルがすべての情報を表すことはできない。監査人は，ファイルを扱うすべての部所におけるスタッフ個人に，また組織の個人データを扱う契約者に問いかける必要がある。この場合，契約者はデータ処理者である。同じように，監査人は，組織が他の組織のために扱う個人データについても考慮しなければならない。この場合，当該組織はデータ処理者となり，他の組織がデータ管理者となる。いろいろな人間がデータを見たり，利用したり，修正したり，あるいは消去したりするので，データを，組織の一つ以上の部局を超えて追いかけることも必要である。ファイルがどのように処理されたかについて，監査人に提供される情報は，ファイル自体の正確性のために検査される必要がある。データ監査人は，データ保護八原則をひとつ一つを考慮しなければならないからである。

データ監査人は，個人データに関係する組織内での方針の存在と利用について検査すべきである。例えば，データの不適切な開示は，膨大な顧客データを保有する組織（例えば，コールセンター）にとって共通の関心事である。それは，安全性違反になるだけではなく，もし，データが組織の方針に違反して開示されたものならば，責任あるスタッフの一人はデータ保護法第55条の下で，個人的な責任を負うことになろう。つまり，個人データの違法な開示に

当たる行為である。もっと悪ければ，獲得データの売買という結果も想定できる。

データがどこに移送されるかを考慮することも必要だろう。つまり，個人データが，外部から組織内へか，あるいは，反対に，その組織から外部の個人・組織へかということを明らかにしなければならない。データ保護の第 8 原則は，海外へのデータの移送に関して一定の安全措置を要求する。しかし，データが海外へ移送されることなく，イギリス国内にとどまるか，特定の国への移送なのか，あるいは領土内であっても，開示は，データ保護法 1(1) の処理の定義に含まれるので，そのデータに誰がアクセスできるのか，つまり誰に開示されるのか，そしてその目的は何かということを監査人は知らなければならない。

最後に，データ監査人は，データ保護法における届出の除外について考えねばならない。

3.2 データ主体

組織において，「誰がデータ主体か」を考えることから始めるのがよい。組織がそのデータを保有し，処理する対象となる識別可能で生存する個人とは誰なのか。組織のスタッフがこれに入ることはほとんど間違いない。年金支給のための，または，ほかの目的のための退職者のリストも存在するだろう。それから，内定者，ボランティア，アルバイト従業員，パート従業員，公務員などもいる。学校には，校長，教員がいる。また，定義は難しいが，顧客や消費者もいる。学校の顧客は生徒かそれともその親か。

データ主体の各々の種類について，監査人は，以下のような問題を明らかにしなければならないだろう。どんなデータが，どんなデータの種類が存在するか，そのデータの目的は何か，それらのデータの各々の種類はどこから入手されたのか，どの範囲まで，データ主体が任意に提供し，そしてそれらのデータの処理を理解しているのか，それらのデータが他のデータとどのように接続されるのか，どのように編集されるのか，どのようにプリントアウトされたり，ディスプレイに表示され，さもなくば開示されるのか，誰に開示されるのか，また，そのデータはどのように時々訂正されたり修正されたりするのか，その組織の内外で，ほかの誰に移送されるのか，そして，データは最終的にどのように消去されるのか，ということである。

データが個人に関してではなく，もっぱら識別不能な集団について情報を記録していることが問題である場合には，人々に関するデータが処理される。これの例としては，意見の調査やセンサスが上げられる。イギリス・データ保護法では「個人データ」は以下のように定義されている。すなわち，「生存する個人に関するもので，(a) それらのデータから，(b) それらのデータとデータ管理者が保有しているか，これから保有するであろう他の情報から，その個人を識別できるもの」である。したがって，識別不可能な生存する個人のデータであるなば，そのデータは，法律上，個人データとはなりえないので，それゆえデータ保護法に

従わなくてもよい。そのようなデータに出くわした場合には，それは，事実，個人データでないということを保証するための細心の注意が払わなければならない。データが個人的かどうかを確定するためのチェック・ポイントは，データの獲得の方法とその後にどんな接合が起こりえるかを見極めることである 。

3.3 コンピュータ・ファイル

コンピュータ・ファイルがデータ監査の出発点であることにちがいない。コンピュータ・ファイルは，ほとんどの場合，その所在が明らかであり，ユーザをサポートする IT 部門にも熟知されているものである。また，IT 部門に知られているすべてのソフトウェア・アプリケーションのリストを IT 部門から入手することも容易である。そのリストによって，メイン・コーポレイト・ファイルや個々のファイルやアプリケーションの保有者が判明する。さらに，ファイルの所有者も判明する。気をつけなければならないことは，IT 部門が知らないファイルも存在するということである。これには，マニュアル・ファイルだけではなく，個人的に所有するパソコンで作成された私的ファイルも含まれる。この監査において，これまでの監査で発見されなかったいかなる私的ファイルも存在しなかったということを証明することが重要である。実用的な秘訣として，スタッフのモニタのアイコンを見れば，それが，IT 部門がサポートしていない，もしくは，私的ファイルのために使われていたソフトやファイルの私的な一部であると認めることができることがある。

電子メールについても問題が多い。メール・ファイルやメモ・ファイルが単独のファイルで存在するのではなく，組織のサーバ上にリンク・ファイルの形で保存されていることがある。そのため，電子メールはそのサーバ上に保存されたままになっている。ほとんどの組織では，かように保存されている多くの電子メールは，おそらく組織の業務用でなく，スタッフの個人メンバーの私的なものであるはずだ。そのような私的電子メールはスタッフの個人用のファイルやシステムに別個に保存するようにすべきである。監査目的のために，監査人は，一般的に組織が電子メールをどんな方式で保存するのかについての見解を示さなければならないだろう。サーバにそのまま保存するか，送信者別か，受信者別か，組織の方針として私的電子メールの扱い，すべての電子メールをモニタする場合にはどのような方法を用いるか，ということについての見解である。

3.4 データ処理

3.4.1 一般的処理

監査人は，データがどのように処理されたかを検査することになろう。コンピュータプログラムに関しては，「処理」は，データ入力，データ修正，データ消去，およびモニタやプ

リンタ上の表示を含むものである。表示については，監査人は，誰もがコンピュータでデータを見ることができるのかどうか，あるいは，権限のある者だけがそれを見たり修正できるようにパスワードなどによって保護されているのかどうかを検証することになろう。マニュアル・ファイルについては，データがどのように処理されたかを詳細に立証することは極めて困難である。というのは，マニュアル・ファイルの作成において，データを処理するための詳細に述べた特定のプログラム・コードは存在しないからである。そのことよりも，マニュアル・ファイルの場合には，誰がファイルのキャビネットを開けることができるのか，キャビネットに鍵がかけられているのか，無錠なら誰でもファイルを持ち出せるのかどうか，ということが問題となる。データが最終的に廃棄されるときには，時にはつまらない紙くず同然にただ紙くず籠に捨てられるのか。それとも，シュレッダにかけられるのか，さもなくば，完璧に消滅させられるのか。消滅が契約者によるものであるならば，そのセキュリティ協定とは何か。

3.4.2　海外でのデータ処理

海外でデータ処理が実施される場合には，特殊な問題が起こることが考えられる。例えば，コールセンターが海外に存在する場合が想定できる。

3.5　データ監査のためのチェックリスト

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[3)]。

・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）

3） Ibid. pp. 51–53.

・オーディオ（契約，教育，ボイスメール）
・バイオメトリック
・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
・スタッフか
・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組織に適合させるか。
・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。

3.6 監査結果の分析

監査人は，監査終了時に，前記質問に基づいた広範囲の情報を手に入れるだろう。その分析・解釈はデータ保護のコンプライアンスの問題に関わっている。そして組織は，データ保護原則や他の項目をその組織が保有するデータに適用するであろう。そしてこのことから，組織がどのようにしてコンプライアンスを確立し，改善し，維持するかを理解できる。

このように監査結果を検討することによって，監査人は，個人ファイルやデータ保護が一般的にどのように扱われるべきかということについての勧告のリストを作成すべきである。結論の主要部分は取締役会またはその他の役員会に提示されるべきである。その詳細な結論は，部局によって，または特定のファイルという方法で，組織に提示されなければならない。個別的な原則，または侵害された法律条項を理由にするより，その方がよい。なぜなら，行動リストは組織の各部局のために整理される必要があるからである。また，組織がその内部でコンプライアンスに弱い部所を特定することができようにするためでもある。

4. 個人データ保護法コンプライアンス

4.1 コンプライアンス戦略

組織がデータ保護監視を完成させたなら，戦略を策定し，監査によって明らかになるリスクが向けられることを確認する必要がある。組織のコンプライアンス戦略のキーポイントは，1）コンプライアンスに応えるために組織が実施しなければならない政策と手続を描くこと，2）必要な人材を任命すること，であろう。

コンプライアンス戦略は，組織が現行法に適合する（従う）ことを保証するのみならず，加えて，コンプライアンス文化が醸成されていることの保証を手続と点検のなかに盛り込むべきである。そうすることで，組織が実施するデータ処理におけるいかなる変化もデータ保護法に合致したものとなるであろう。

4.2 データ保護監査官

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，データ保護監査官の任命である。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[4)]。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

4） P. Carey, Data Protection, 2nd ed., OXFORD UNIVERSITY PRESS 2004, p. 215.

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，データ保護監査官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。

データ保護監査官は，必ずしも，専任でなくてもよい。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官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官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官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，データ保護監査官またはチーフ・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。

データ保護監査官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。データ保護監査官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，データ保護監査官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。データ保護監査官が誰に報告しようとも，データ保護監査官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官に必要な権限とデータ保護監査官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[4a)]。

組織はデータ保護監査官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官に対しても，特に何の責任を課していない。しかしながら，データ保護監査官は，他の会社の経営者と同様に，法律違反がデータ保護監査官の同意，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官に選任されて，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。

4a） R. Morgan/R. Boardman, ibid. pp. 58−59.

4.3 データ保護方針とコンプライアンス手続

4.3.1 データ保護方針

データ保護監査官の選任に続いて，組織はデータ保護に関する方針を整備し，組織内で十分に支持されるようにする必要がある。本法の下ではこのための要求事項は規定されていないが，方針が法律に合致していることを保証する原理・手続を記述した明文化された方針を採用することが組織にとって望ましい習慣である。それは，組織が真摯にデータ保護に取り組んでおり，最重要課題として支持することを組織内の全員に明確に知らしめることになるのである。法律に基づいて，データ主体によって苦情や請求を提起された場合でも，組織が明文化し，厳格なコンプライアンスのための手続を実施していたという証拠があれば，それが裁判において有利にはたらく。

方針および手続の文書は部門特定のもの，組織横断的なものなどの混在したものにならざるを得ない。例えば，ある組織は，データ保護原則（例えば，公正取得とデータの質について）に合致することを保証するために，各部門ごとの特定の手続を採用することもあろう。しかしながら，その方針の多くは，組織に横断的に通用するものである。データ主体の照会，セキュリティの問題，越境データ流通および電子メールなどの取扱方に関することである[5)]。

データ保護方針は以下の事項に向けられる。

- 方針の相手方――方針が誰に向けられるのか，誰に関係しているのか。
- 組織におけるデータ保護の重要性
- データ保護に関して，組織の最終目標の記述（例えば，法律の遵守あるいは法律以上のことを組織としては実施する）。
  - データ保護に関して取締役会の関与の記述
  - 法律への背景
    - データ保護方針の必要性
    - 法律の組織としての解釈
  - 他のデータ保護方針へのリンク（ISO9000，BS7999）
  - 組織の構成
    - 組織の構成図
    - データ保護監査官の詳細な紹介と連絡先
  - 組織の構成員に対するデータ保護教育の詳細な記録
  - 組織全体のおよび部門別の方針のリスト
  - 監査報告・評価手続

5） Ibid. pp. 59−60.

・方針に不服従のスタッフの取扱

・書類の作成者，改定手続，改訂版数などの管理

重要なことは方針を決めているだけではなくて，その完全な実施の戦略を立てていることである。つまり，組織内の誰もが，その方針を熟知して遵守していることを保証する戦略である。これを実現するために，確立した手続，契約の精査，方針の公布・普及（教育も含む），組織中の関連事項，手続の実施，ということが結合したものが要求される。

4.3.2　コンプライアンス手続

4.3.2.1　データ分析

データ監査は，まず，個人データを処理する者，または部局を特定しておかねばならないだろう。その各々のために，特定の方法の手続を決めておかねばならない。しかし，その各々に個別の手続は必ずしも必要ではないが，いかなる個人データ処理部局もその義務を実行するのには法律をいかに遵守するかについての明確なガイダンスなしにはやっていけない。そのようなグループには以下のものが含まれよう：

・顧客との接触をもつもの，セールス，アフタサービス，顧客関係，清算などを含む。

・将来の顧客との接触をもつもの，マーケッティングを含む。

・サプライヤとの接触をもつもの，アカウントを含む。

・一般消費者との接触をもつもの，セキュリティ，宣伝，インターネット。

・従業員，従業員内定者との接触をもつもの，人材，イントラネット。

・海外支店，海外取引企業に関係するもの。

・テレワークスタッフ。

・仕事として電子メールを利用またはアクセスする全スタッフ。

上の例は，これで言い尽くされているわけではない。組織によっては他にも考えられるものもあるだろう。これらのグループはいろいろなスタッフが入り交じった形になっている。直接対面的に，電話で，電子メールで，あるいはその他の手段でにデータ主体との接触をもつものもいれば，対面的にではデータ主体と接触するものもいる。しかし，いずれの場合も，データ主体の記録を扱うことには違いない。これらのグループおよびグループ内のスタッフのタイプは詳細な個人データの取扱方法を知らねばならないだろう。

データ監査において特定された個人データファイルの各々について，データ保護監査官は，監査報告およびその他の必要な情報に基づいて，十分に分析を実施し，データ保護原則と照らし合わさなければならない。その場合以下の諸点が考慮に入れられる[5a)]：

・個人データとは何か。

5a）Ibid. pp. 61–62.

・データ処理の各ステップにおいてそのデータを処理するものは誰か。
・そのデータには除外規定が適用されるのか。
・そのデータの出所はどこか，誰からか。
・データの取得において附則 2（個人データの処理）の条件の一つ以上に適合しているか。
・センシティブデータではないか。もしセンシティブデータなら，附則 3（センシティブデータの処理）の条件の一つ以上に適合しているか。
・適法に処理されたか。特に秘密情報の場合。
・どんな目的で処理されたか。
・データが誰に開示されるのか。
・その開示は目的に合致するか，目的外か。
・データは正確か，最新のものか，最新にするための手段は何か。
・データの貯蔵期間は。当初の貯蔵期間を超える場合の正当な理由は何か。
・データ主体の権利を侵害しない方法で処理が実施されているか。これに応えるために，さらに分析が必要である：
・どのような方法で，特定個人のデータが抽出されたか。
・必要な場合に，データは修正されたか，消去されたか，封鎖されたか。
・データ主体の要求に応じてデータのダイレクトマーケティングは遮断されたか。
・データは自動意思決定に利用されたか。もしそうならこのプロセスがデータ主体に知らせたか。もしデータ主体が要請したら，非自動的処理が可能だったのか。
・データを処理する関係者のデータのセキュリティ・アセスメントは実施されたことがあるのか。
・データ・プロセッサーはすべてのまたは一部の処理に利用されるのか。
・データは海外へ移転されるのか。もしそうなら，越境データ流通の条件に合致するのか。
・データは適法に第三者に移転されるのか。もしそうなら，そのデータの処理に係わる条件がその第三者に課せられるのか。

このような情報およびポリシーに基づいて，各データタイプを扱い，データ主体と直接的な接触をもつすべてのスタッフのために手続を工夫することが可能である。この最後の点は重要である。何となれば，例えば，コールセンターのスタッフは通常の業務として特定の個人のデータを扱うのではなく，特別な方法でデータを扱うよう電話をかけたその同じ個人と接触しているに過ぎないのだから。その手続が，何らかの方法でその問題を扱うことをそのようなスタッフに許可しているどうかについて，もしくは，手続がその問題を他の誰かに任せているかどうかについて決断しなければならないだろう。

スタッフの各グループのために，一連の手続が考えられる必要があろう。セキュリティ，顧客との接触方法のような他の要求事項を充足するための多くの手続がすでに存在しているので，この手続だけを別個に考えるのでは，他の手続との関連性を損なうことになる。理想的には，データ保護によって指示された手続がこれらの手続の補完的なものとすることであろう。そのため，データ保護監査人の任務の最初の仕事は，現存するスタッフのための手続の洗い直しにある。すなわち，これらの既存の手続が，データ保護ための要求事項に合致しているのかどうか，あるいは中立的なのかどうか，または矛盾しているのかどうか，ということについて検討しなければならない。これには，組織の他の部門との協議が欠かせないはずだ。つまり，セキュリティ部門，人事部門，IT 部門，並びに，特殊業務の営業担当者との協議である。その結果，データ保護のためのコンプライアンスが実施されることを保証するための交渉ということになろう。もちろん，データ保護監査人が猛烈な反対に出くわした場合には，監査人に必要な権限を付与するということを含んでいる。

4.3.2.2　データ保護監査人コード

この点について，情報コミッシュナーによって推奨された，いくつかの分野における，良き慣行を取り上げたい。法律第51条の下で，コミッシュナーには以下の義務が課せられる：

「データ管理者による良き慣行の次のものを推奨すること」

そして，特に，同業組合等との協議に従って行動規準を策定することである。良き慣行は法律51(9)条によって以下のように定義されている。すなわち，「個人データの処理において，データ主体の利益を考慮することでコミッシュナーに望ましいと写る慣行で，データ保護法の要求事項を遵守することを含む」。

それゆえ，それは，コミッシュナーのコードが法律を反映していなくて，法律に規定されていない事項を明らかに含む場合である。コードの遵守に関して，その他の重要なコードを守ることなく，データ管理者が十分に法律を遵守していない場合にちがいない。CCTV コードにおいては，コミッシュナーは，法律が要求する部分と法律を超える部分とをわかりやすく区別している。しかしながら，雇用慣行データ保護コードはこのような区別はしていない。

4.3.2.3　その他のコード

しかしながら，これでその歴史は終わったわけではない。というのは，データ保護監査官は，全体にしろ一部にしろデータ保護に向けられたり，コミッシュナーの推奨を得られないような他の行動規準が，それにもかかわらず，同業者組織によって，時にはコミッショナー事務局との協議によって考案されてきたという事実を注目しなければならないからである。しかし，一例として，イギリスセキュリティ産業協会の「秘密情報源の安全な破壊のための行動規準」について考えてもらいたい。これは，明確に，1998年データ保護法を遵守するように考案された行動規準である。警察署長協会もまた行動規準を策定した。明らかに，これ

らの行動規準は情報コミッシュナーの承認を得ていない。したがって，データ保護監査官は，法律についての自らの認識に反対する彼らの主張を検討しなければならない。しかし，これらの行動規準の内容に有益で実践的なものが多く含まれており，規準に記された産業標準への訴えの方が，単に組織のデータ保護方針に頼ることや法律への訴えよりも，コミッシュナーの理念を理解させるより容易な道であることがわかるであろう。

4.3.2.4　手続のチェック・リスト

データ保護監査官は以下のような情報から始めるべきである。

・データ監査の結果によるデータの種類

ここから，データ保護原則に照合した監査官独自のデータ分析の実施，つまり，以下のことを考慮しなければならない。

・組織のデータ保護方針
・組織内の下部のデータ保護方針
・情報コミッシュナーの関連行動規準
・関連するビジネス行動規準
・スタッフのひとつのグループによる処理タイプ，セキュリティ，コンシステンシーのために考案された従来の手続

これらのすべてに基づいて，データ保護監査官は，既存の手続を検証し，個人データを取り扱うスタッフのグループひとつ一つのための新しい手続を考案し，新しい手続をラインマネージャーに渡し，必要な場合には取締役会を通じてデータ保護委員会のサポートをとりつけるのである。

4.4 契　　約

4.4.1　契約と個人データ

個人データとその処理についての記述は，組織の契約のなかに現れる。これは，明らかに，データ処理契約にも当てはまるが，組織と顧客との契約関係のような，他の多くの契約にも当てはまる。もし，組織が個人データの処理に個人の同意を得ているということを保証することになっているとしても，ディレクト・マーケティングは特に複雑な手続の問題の多い方法である。データ保護監査官は，それゆえ，組織の法務担当者や関係する営業役員と共同して，DM に個人データが含まれているかどうかをみるために組織の契約関係を精査しなければならない。もし，個人データが含まれているならば，組織がそれらの個人データの合法的な処理を許可しているということに満足しなければならない。センシティブでない個人データの場合でも，附則 2 の 6(1)条に基づくだけでは十分ではない。同条は，データ管理者の利益に必要なデータ処理の範囲について言及することなく，「データ管理者によって追求され

た合法的な利益の目的のための」データ処理を許可しているからである。

データ処理契約に基づくのではなく，契約上の理由で，第三者にデータが移転される場合にも同じような考慮がなされなければならない。例えば，組織が，個人データを別のマーケティング会社に移転するという同意をその個人から得ており，同時に，処理契約上もデータの移転権限を適法に有している場合に，データを移転する当該組織は，データ受領組織によって如何に正確にデータが利用されているかについて照会すべきであって，受領者に対して契約上の制約を課すべきである[6)]。

4.4.2　データ処理契約

データ保護監査官の重要な任務は，データ処理契約に関わるものである。データ処理契約の種類として，つぎのようなものがあげられる。

・給与計算プログラムのような個人データを含む事務サービス
・オンライン診断システムで，ソフトウェアの問題解決を引き受ける診断会社が問題発生時に処理中の個人データを職務上みなければならない時がある。
・個人データを含む外注処理
・個人データの転換
・電子メール扱う ISP（インターネット・サービス・プロバイダ）契約
・機器保守契約，機器の診断やバグの修正において保守契約者が機器内のデータを見る立場にある。
・データ復旧サービス。契約者は，ディスク・クラッシュ，火災被害，その他の災害によって失われたデータの回復を求められる。
・バック・アップ契約，ホット・スタンドバイ契約。契約者は，セキュリティのため，個人データのファイルのコピーを頼まれる。他に方法がない場合の個人データ処理システムの入れ替え。
・プログラミング契約。将来のデータ処理のテストのために個人データを利用する。

データ処理契約に係わる第７原則が遡及的に適用される。そのため，データ保護監査官は，現在のならびに将来の契約すべてを知っておかなければならない。さらに，書面によらないで第７原則に違反する契約が存在することもあり得る。通常のビジネスにおいては，書面に基づかないような処理協定は多くはないと思われるが，データ変換，保守，プログラム開発においては，非公式の協約のようなものがあって，その場合には，ほとんどあるいはまったく書面が残されていない。データ保護監査官は正式な契約をもっと強調すべきである。

6）R. Morgan/R. Boardman, ib., p. 66.

4.5 公　　表

4.5.1 コンプライアンスの風土

今までにデータ保護法の影響はビジネス界を通して行き渡っている。法律に適合するために，組織はコンプライアンスがさまざまのレベルでスタッフによって理解されていることを保証する必要があり，コンプライアンスの風土が促進されることが肝要である。これを達成するためには，データ保護の使命があらゆるレベルでそしていろいろな方法でスタッフに行き渡っていることが要求されるだろう。その方法としては：

・組織によるスタッフの教育。

・スタッフの掲示板やイントラネットにデータ保護問題を掲示する。

・スタッフ用のハンドブックの配布。

・雇用契約に入れる。

これらの方法はそれぞれ以下の節で取り扱われることになろう。

4.5.2 教　育

個人データを扱ったり，データ主体と接触があると思われるスタッフは，教育を受ける必要があろう。一部には，これは部門別に特定された手続によって記述される。手続における教育は，データ保護の諸問題を扱うと同時に，安全性というようなその他の問題も扱うようになる。しかし，スタッフは，直面する新しい状況を正しく認識し，それに対処できるように，少なくとも，データ保護原則をある程度理解しているということが望ましいことである。また，スタッフ不足やその他の理由で，通常よりも教育を受ける機会が少ない責任をとらなければならないこともしばしばある。もし，スタッフがデータ保護原則をよりよく把握しておれば，データ保護の領域における危険の機会は大幅に減少するだろう。そこで，スタッフの特定の業務に適用される特別の手続における訓練の前に，データ保護原則の一般的な教育を受けることが推奨される。

4.5.3 スタッフハンドブック

その規模や複雑性にかかわらず，ほとんどの組織は，スタッフのためのハンドブックを作成している。それは，組織が，職員の昇進・昇格や，一定の技術的・法的・倫理的標準の維持のようなさまざまな良き慣行にかかわることを説明している。データ保護の説明についても，このハンドブックを使うのが理想的である。データ保護原則は簡単明瞭に表現されているので，そのまま字義通りにそのハンドブックに挿入しても違和感はない。組織はデータ保護原則の精神と字義に従って行動することを決定し，データ保護にかかわる問題を真摯に受け止めるというような意思表明を入れておく方がよい。さらに，ハンドブックにおいて，データ保護方針の実施に関する組織の姿勢を明きらかにしておかなければならない。

4.5.4　雇用契約

最後に，雇用契約に，組織のデータ保護方針で説明されたようなデータ保護原則に従う旨の一文を載せておかねばならないだろう。職場における秘密保持についても同様である。これは，当該組織がデータ保護に真摯に取り組んでいることをスタッフに印象づける目的である。また，組織がデータ保護原則を遵守していることを強調し，スタッフが退社後も組織についての事柄を秘密にしておくということも強調しておかねばならない。スタッフが雇用中に得た個人データを暴露した場合には，前述の条件の提示を怠っていたことは組織がデータ保護の第７原則（セキュリティ）違反の責任をおわなければならない。

4.6　実　　施

データ保護に関する方針の策定において，組織は，その方針の違反に対する制裁を考えておかねばならないだろう。重大な違反は解雇に値するといってもよい。国家警察コンピュータシステムを利用して個人データを不正取得した場合はデータ保護法第55条が適用される。組織は，法律違反について均衡感覚をもち，故意にデータ保護原則やデータ保護方針を侵害したスタッフに対する各種の制裁を用意しておかなければならない。

データ保護監査官の義務は，侵害を探すことであり，人材局に助言することである。さらに非難すべき侵害には以下のようなものが含まれる：

・組織を刑事裁判に引き込む。
・組織を民事裁判に引き込む。
・組織を情報コミッシュナーの実施警告または特別な告発警告にさらす。
・侵害により組織を事業停止に陥れる。
・顧客，サプライヤ，他のスタッフに損害または被害をもたらす。
・組織を社会的攻撃に陥れる。

どのような制裁措置が考えられようとも，重大な侵害は解雇という結果になり，そのような制裁には情状酌量の余地はないということを組織はスタッフに警告しておかなければならない。組織がデータ保護法にかかわっていることを公表するために選択されたさまざまな方法は，少なくとも，受けることができる処罰を与えるものでなければならない[7)]。

7）R. Morgan/R. Boardman, ibid., p. 70.

5. 届　　出

5.1 届出義務

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[8)]。

そこで，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。登録制度は，法律においては，「届出」（notification）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[9)]。

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[10)] 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。

5.2 届出免除

1984年データ保護法の下では，データ・ユーザ（1998年データ保護法の「データ管理者」と同じ意味である。）の登録が義務づけられていた。そして，データ登録官の権限の多くが登録されたデータ・ユーザに対してのみ行使されていた。したがって，届出の除外範囲も，1984年法の下では，極めて狭く考えられていた。

1998年法における状況はかなり異なっている。届出の除外は極めて広く適用され，多くの組織，とりわけ小規模な組織は，その処理の届出をする必要性が今では完全に例外的になっている。法律は，かなり広い範囲の除外を認めており，以下のように，さまざまな例外が規

8） http://www.informationcommissioner.gov.uk/
9） P. carey, Data Protection, 2nd ed., OXFORD UNIVERSITY PRESS, 2004, p. 127.
10） ヨーロッパ経済地域。European Economic Area の略。EU に，ノルウェー，アイスランド，リヒテンシュタインを加えた国々から構成される。

定されている[11)]。

・マニュアル・レコード
・データ処理者
・個人的，家族の，家庭内の目的のためのデータ処理
・人事管理，広告，マーケティング，PR，精算，記録保存のコアビジネスのための処理
・非営利団体によるデータ処理
・公的登録
・国家安全関係

5.2.1　マニュアル・レコード

もし組織が個人データの処理をコンピュータで実施していないのであれば，届出をすることはないように思われる。法律17条第２項では，届出を提出する義務は，１条１項のデータの定義のなかのサブ・パラグラフ（a）か（b）に該当する個人データにのみ適用される，と規定している。これらのサブ・セクションは，コンピュータ上で処理される情報か，未だコンピュータ上にはないが，あとでコンピュータに移転するつもりで作成されたマニュアル（紙）記録である情報に適用される。したがって，ほとんどのマニュアル・記録には登録の義務は生じない。情報自由法2000が発効したときに，1998年法の 1(1)(e) で定義された公権力の記録もまたそれ自身組織に届出を要求していない。

実際は，ほとんどの組織は，今は，少なくとも，一部のデータをコンピュータ上で処理をしているだろう。そのため，マニュアル記録を例外とすることは，完全な例外とはならない。組織は，コンピュータ上で処理する情報だけを届け出るということを決定できた。さもなければ，組織は，任意ではあるが，マニュアル記録の処理を届け出ることができた。このように，自主的な届出というメリットがあった。データ保護法第24条の下で，誰でも，マニュアル記録を登録していない組織に対して，マニュアル記録の処理に関する一定の情報を提供するよう求めることができる。この情報は開示要求の受領から21日以内に提供されなければならない。しかも，無料である。もし，組織がこの種の情報についての膨大な開示要求を受け取るならば，24条は，組織にとっては煩わしいものとなるであろう。しかしながら，現在まで，同条はほとんど注目されなかったし，広く利用されることはなかった[12)]。

5.2.2　データ処理者

組織は，それがデータ管理者か単なるデータ処理者かのいずれであるかを確定しなければならない。法律の下では，データ処理者には届出の義務はない。給与支払事務所のような組織は，それは，顧客のデータという観点からは，データ処理者であり，自己のデータという

11）R. Morgan/R. Boardman, Data Protection Strategy, SWEEET & MAXWELL, 2003, p. 72.
12）Ibid., p. 73.

観点からは，データ管理者でもあるといってよい。このような場合，自分のデータのみの処理を届け出る必要があろう。データ処理者が雇用されているところでは，データ処理者によって処理されたデータに関して届け出るのはデータ管理者の義務であって，データ処理者の義務ではない。

5.2.3　個人的，家族的および家庭内使用

データ保護法第36条の下で，広い例外がある。個人的，家族的目的によって処理された個人データに関しては，届出のみならず，すべての条項において広い例外がある。この例外は個人，すなわち生存する人間によって処理される個人データに適用される。有限会社や合資会社によってではない。さらに，個人商店は，個人データを個人的・家族的・家庭内目的ではなく，商売のために処理する場合には，この例外の恩恵を受けることはできない。しかしながら，この例外は，家庭にあるコンピュータでもっぱら個人的な電子メールを送ったり，クリスマスカードのリストやほかの住所リストを保存するものは同法の下での届出の義務を負うことはない。

5.2.4　ビジネスと非営利団体のデータ処理

17(3) 条は，国務大臣に対して，あるデータ処理が「データ主体の権利や自由を侵害する恐れがない」と判断すれば，中核的業務のためのデータ処理の一定のもののを例外とすることを認めている。届出規則（The Notification Regulations）は，この例外の仕組みを詳細に利用している。それらの例外は以下に掲げておく[13)]。組織は，ほとんどの場合，例外は関連する目的に「必要な」データ処理に限られているということを銘記すべきである。実際は，組織が成長するにつれて，例えば，スタッフ管理のために「必要な」データ処理だけでなく，便宜上データ処理を開始するであろう。したがって，例外が，中小企業やクラブに有利のように見えるが，大規模な組織にとってメリットはないように思われる。データ処理が中核業務の例外にはいるかどうか疑問に思うデータ監査官は，「届出ハンドブック」第4節，問4を参照すべきである。ここには情報コミッシュナー事務局が例外と見なさない，つまり，例外の範囲外のデータ処理のタイプがかげられている。目下，以下の目的の個人データ処理が例外とされている。

・私的調査
・健康管理・サービス
・警備
・犯罪防止と犯罪捜査
・法務関係

13） Ibid., pp. 74–78.

・教育
・調査
・司法
・コンサルタント事業
・フィナンシャル・アドバイス
・クレジット照会

5.3 届出方法

組織が届出を必要と判断したのであれば，その届出手続は極めて簡単である。情報コミッシュナーに，その旨を電話かウエブサイトから伝えるだけでよい。インターネット登録システムを利用する場合は，完全には自動的ではないので注意が必要である。一度届出が完全に終了していれば，その登録様式を印刷して情報コミッシュナー事務局に郵便で送付する必要がある。オンラインではできない。

届出に必要な情報

・組織名
・住所
・連絡先
・データ主体
・データの種類

5.4 届出の更新

重要なことは，組織が，法律との継続的なコンプライアンスを示すものとして，届出の最新性を維持することである。法律第20条と届出規則の規則12は，組織に対して，届出を，正確かつ完全な報告書にするように義務づけている。そのいかなる変更も，その事実の28日以内に届け出なければならない。これを怠った場合は犯罪となる。情報コミッシュナー事務局は，届出の変更に用いるための二つの標準様式を用意している。一つは，組織が新しい目的を届ける場合に用いるものと，もう一つは，その他の変更を届け出る場合に用いるものである。

組織は，また，届出を毎年更新することを保証しなければならない。1984年法の下では，登録は3年間有効であったが，1998年法の下では届出は1年間しか有効でない。組織が届出を完成させるときには，自動的に届出を更新する方法も選択することができる。これは，組織が届出の更新を不注意で看過しないようにするための賢明な方法である。しかしながら，更新料金の支払いは手続の一部にすぎないということを組織は覚えておかなければならない。

組織は，届出が正確で完全であるということをチェックするための協定を締結しなければならない。

情報コミッシュナー事務局の慣例はデータ管理者に届出更新の必要性を忘れないように連絡することである。しかしながら，これはコミッシュナーの法的な義務ではない。さらに，更新の連絡が常に時間通りに到着するとは限らないので，組織はこれに頼るべきではない。この更新の連絡が到着しないということは，法律上何の弁解にもならない。

6. お わ り に

イギリス・データ保護法は，すべての組織にとって，個人データの保護がいかに重要なものであるかを教えてくれる。情報社会にあって，「個人データの取り扱い如何」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ということを示唆している。

個人データの保護の実現は，結局のところ，人間の問題である。データそのものの処理は，もちろん，コンピュータという機械が実施するのであるが，データ処理の目的や方法を決定する人間，すなわち，データ処理管理者，個人データ処理を監視し，法律の遵守（コンプライアンス）を監視するデータ保護監査官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。

イギリス・データ保護法の特徴のひとつは，1984年法の「登録制度」と1998年法の「届出制度」にあらわれている。後者の届出制度は前者の登録制度を引き継いだ形になっている。その理念も踏襲されている。つまり，個人データ処理の「透明化」である。組織には，個人データ処理に関する「届出」が義務づけられている。すなわち，組織のデータ管理者がこの届出を履行しないと，個人データ処理を実施できないということになっている。

この届出は，個人データ処理に係わるほとんどすべての情報の種類を要求している。そのために，詳細かつ厳密なデータ監査が求められる。そのことはデータ監査のためのチェック・リストにもあらわれている。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。それは，組織にとっての個人データ処理の透明性の確保である。もうひとつは，データ監査の実施によって，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，当面の個人データ処理の必要性・正当性を関係する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，この個人データの処理の透明性が最も重要な意味をもつ。すなわち，個人のデータ保護の権利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，個人データへのアクセス権，修正権という権利を行使することを可能にする。

したがって，データ監査によって獲得された，個人データに関する情報を届出にすべて反映させることでなければ，真のデータ保護の実現は困難となる。