業務改善による個人情報の活用

2005 年 3 月 30 日
弁護士　牧野 二郎

【要旨】
個人情報の保護対策が進められているが、どちらかといえば、利用規制の方向が強く打ち出されているのではないか。個人情報の活用という視点が見出せないと、今後のビジネスがいびつになってしまうだろう。ここでは、個人情報保護の本質を考慮したうえで、如何に活用するか、安全な活用の視点と方向性を展開したい。

【キーワード】
個人情報保護、個人情報の活用、業務改善、コンプライアンス、業務監視、監査体制
第三者機関による監査、危険因子、マニュアル、シリアル番号、データベース分割、
情報力、個人情報保護法、ガイドライン

【目次】
1　個人情報保護の本質
2　管理責任と違反行為の関係
3　保護対策と利用規制
4　業務改善としての保護対策
5　コンプライアンスの失敗事例
6　業務改善の視点からのコンプライアンス対策
7　監査の実をあげる対策
8　新しいビジネスシーン
9　情報セキュリティ、情報力の拡大に向けて

１　個人情報保護の本質

（１）個人情報保護の必要性

わが国においては個人情報の保護の必要性はこれまであまり認識されてこなかった。1980 年にＯＥＣＤ（ヨーロッパを中心に先進国 30 カ国が参加する「経済開発機構」という国際機関）から、「プライバシー保護と個人データの国際流通についてのガイドラインに関するＯＥＣＤ理事会勧告」がだされ、強く認識されるようになるが、わが国では個人情報、プライバシーという認識が極めて低かった。

その８年後である 1988 年（昭和６３年）12 月 16 日になって、ようやく「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」が公布となった。しかし、この時点で民間事業者などの個人情報の利用に関する規制は現実化していなかった。

さらに 1995 年にはＥＵ（ヨーロッパ経済機構）から、個人情報保護に関する指令（ディテクティブ）がだされ、個人情報の保護に関する強力な実施計画がだされ、ヨーロッパ各国は一斉に個人情報保護対策を推し進めることになった。

わが国では、1999 年（平成 11 年）住民基本台帳法の改正議論が行われ、住民基本ネットワークの構築に関連して、住民のプライバシーの保護対策が強く認識され、行政部門は当然の対象としつつ、あわせて、民間部門におけるプライバシー保護、個人情報保護の必要性が議論の対象とされた（住民基本台帳法改正法案審議（第１４５回国会）・参議院本会議における小渕内閣総理大臣答弁参照)。

（２）個人情報保護の制度化

平成 11 年 7 月高度情報通信社会推進本部「個人情報保護検討部会」初会合が開かれ、個人情報保護の基本方針が議論されるなど本格的な議論が進められた。検討部会会長であった堀部正男教授が中心となり、11 月 19 日「我が国における個人情報保護システムの在り方について（中間報告)」がまとめられた。我が国の個人情報保護システムの中核となる基本原則等を確立するため、全分野を包括する基本法を制定することが必要であるなど、基本骨格が作られた。その後、平成 12 年専門家会議が開かれ、法制化に向けた議論が行われ、13 年には法案が策定され、14 年審議未了により 1 度廃案となり、15 年に成立したという経緯がある。

この間、報道機関、ジャーナリストらから、個人情報保護法は「治安維持法」であるとの批判が相次ぎ、法律家の中からも基本的人権を侵害するものであるとの主張がなされるなど、法案をめぐって厳しい対立が繰り返された。

当初基本法と個別法の総合したものとして考えられてきたが、立法対応の中で、政府はこれを一本化し、全産業を対象とし、重要産業に関しても当面法律を作らず、ガイドラインで対応するといった形で対応する選択をした。

（３）情報化社会と個人情報

インターネットを中心とした電子商取引や、情報サービスが急速に普及するに従って、個人に関する情報が大量に提供され、利用されるようになった。個人から提供を受けた事業者は、これを我が物として自由に利用するといった傾向があることが問題とされ、事業者は費用をかけて収集した情報資産は企業に属する資産であると考え、個人の情報の取扱いに関するコンセンサスはなかなか確立されなかった。

インターネット利用者などに対するアンケート調査などの結果、個人情報の漏えいが不安であるとする調査結果が多数出された。こうした不安が広まることは、情報化や電子商取引の阻害要因となることは明らかであることから、そうした阻害要因の除去、対応のためにも、個人情報の保護の制度を求める動きも強まった。こうした事情も背景として、個人情報保護の政策が進められた。

（４）個人情報保護のポイント

現在の保護法制度の特徴は、事業者による管理の適正化による保護の実現である。

個人情報を盗んだり、不正に流用し、販売するなどした個人、職員に対しては個人情報は対応しない。そうした逸脱行為を放置したり、管理していない事業者を処罰するという間接的な規制を採用したのである。

最近でも、個人情報を漏えいした個人を処罰する法制度を作るよう求める声もあり、関係省庁も議論を進めているとの話もあるが、その正確な状況は今のところ不明である。

個人情報保護法は、事業者による個人情報の適正管理を求めるものであり、事業者規制法としての性格を基本とするが、その実質は利用禁止などではない。むしろ、適正な利用促進であり、不適切な濫用を規制するという趣旨のものである。

従って、個人情報保護対策は、個人情報を活用することにより、事業者から国民へ提供される各種のサービスが、充実、発展することを視野に入れて、そうした発展を促進し、決して阻害することがないように組み立てられなければならない。

２　管理責任と違反行為の関係

情報化社会における安全対策の基本が、行為処罰から、管理責任重視へと傾斜しつつあることが認められるようだ。これまでは、刑法などの犯罪処罰の体系は、行為責任論（犯罪行為を問題として、行為の特徴が予定した行為類型に当てはまることを処罰の根拠とする考え方）に基づいたものとなっており、それで逸脱行為のほとんどがカバーできた。管理責任が問われるのは、業務上の管理責任が明確なものに限定され、被害が重大なものに限定されてきた（業務上過失致死、過失致傷など）。

ところが、情報の流通の高速化、広範囲への情報流布の危険性を考慮した場合、一つ一つの行為を処罰するのでは犯罪防止の実効性はなく、被害の拡大、被害の継続を食い止め

られないことが明確になってきた。必要な対応は、重要な情報を持つものが的確な管理を行うことであって、情報資産の散逸防止を確実に行うことで、犯罪の発生そのものを防止、規制するということが求められた。

こうして、行為責任に基づく行為の規制とともに、そうした犯罪の原因を作るずさんな管理(犯罪の温床を作るようなずさんな管理)を規制するという意味での管理規制が必要となったのである。

３　保護対策と利用規制

（１）利用と保護

個人情報の保護とは何を意味するのか。保護といっても、単なる安全な保管を意味するのではないことは言うまでもない。利用することが前提となっており、ここでの保護とは、安全な利用の確保、ということである。安全とは、情報提供者にとって、提供の趣旨に従って利用されるという意味での安全と、事業者にとっても情報資産が予想外の逸脱利用がなされないこと、自らの管理権限の枠を外れないということでの資産としての利用の面で安全という意味も含むものである。

（２）需要に応じたサービス提供

個人情報は、本人に対するサービスや商品の提供を行う場合に、より充実したサービスなどを提供するために必要なものである。本人の情報があれば、その本人の要望を正確に理解して、本人の個別の必要に応じた、きめ細かなサービスを提供することができるようになる。そうした個人情報がない場合には、汎用的な、規格化された一般的サービスや既製品の提供をするほかない。

こうした観点では、本人が最適のサービスを求めるためには、サービス提供者である事業者(専門事業者)に対して、その事業者が必要とする情報を提供することが必要となるが、本人には、どのような情報が必要であり、不要であるかの判断は困難なことがある。事業者側からすれば、サービスの特性や機能、限界などを考慮したうえで、本人の特性、行動様式などを踏まえた総合的判断が必要となる場面も存在するだろう。

当職のような弁護士業務を実施する場合も、本人の希望するところや、家族関係、さまざまな環境を知る必要がある。また、問題事象に沿って、さまざまな情報を聴き取り、その中から、必要なものを取捨選択することもが多い。正確な情報を、可能な限り提供してくれるように求めることが多いし、本人には証拠としての重要性がにわかに判断できないことが多く、本人の取捨選択を認めてしまうと、重要証拠が隠れてしまうことも多い。従って、法律上の守秘義務を説明して、本人に不利な情報も含めて事件に関連するすべての情報の提供を求めるようになる。こうして本人は、弁護士の求めに応じて、次々と情報を提供することになる。

（３）事業者の優位性を規制すること

本人の最も適したサービスを提供するためには、事業者の専門性に即した情報収集、情報利用が必要であるとすれば、本人はその事業者、専門事業者の求めに応じて、求められたすべての情報を提供するほかない。そうした場合、本人の立場はどうなるのか。本人は、当該部分の専門的知識を持ち合わせていない場合には、事業者の言うがままに、すべての情報を提供しなければならないのか。

ここから、専門性の規制、透明性の確保という要請が出てくるのである。専門性を持ち、優位性を有する事業者に対して、その専門性、専門性に基づく判断を、本人に明確に示すことを求め、専門性のベールの裏に隠し事を持たせない工夫が必要となる。こうした観点から、事業者が本人から情報を収集する場合には、事業者がどのような事業活動、サービスを行うのか、それを目的として特定して、表示することが必須となる。これが個人情報保護法で求める利用目的の特定と表示の問題である。

事業者は、自ら掲げた利用目的に必要な範囲でのみ、情報収集しなければならず、目的の達成の範囲を超えた収集を行うことは規制される。また、収集した情報は、やはり利用目的の範囲で利用するのみであって、それ以外に利用することは許されない。特に、収集した情報を、無断で第三者に提供することなどは本人の意思を裏切り、予想外の事を行うことにもなるので、強く規制される。即ち第三者提供に関しては、事前の同意かオプトアウトの制度を採用する必要があるとされている。このように、事業者の優位性に対する的確な規制が設けられており、本人の無知に乗じた専横は規制されるものとなった。

４　業務改善としての保護対策

個人情報の利用・活用を視野に入れるといっても、利用・活用によって漏えいの危険性は限りなく高まることになる。ノートＰＣに入れて、顧客先を回るなどして持ち歩くことは、ノートＰＣの紛失、盗難などの危険性を伴う。事務所で利用していた場合でも、事務所荒らしなどの盗難にあう危険もある。また、従業者が、自宅作業のため、持ち帰り、あるいは個人のメールアドレス宛に必要な個人情報ファイルを送信し、紛失し、あるいは誤送信し、漏えいしてしまうこともある。こうした漏えいを故意に引き起こす従業員の存在も予想する必要がある。

こうして、業務に伴う多くの危険な場面が存在することを率直に認める必要がある。その上で、その業務に内在する危険な作業や、危険因子（危険の原因となる要素）を明確にして、その排除を進める必要がある。即ち、個人情報取扱いを基本として、その一連の作業における危険作業を排除し、あるいは安全作業となるように、業務の改善を図る必要がある。

業務改善を進めることで、事業活動を進めながら、その業務から危険な部分が除去され、事故の発生する可能性が極めて小さくなることが期待できる。

具体的に業務改善はどのように行うべきか。たとえば、勧誘や、サービス説明などのため顧客回りを必要とし、その際顧客のデータを利用する必要があるといった場合を想定しよう。その際に顧客の過去のデータなどを利用して、様々なシュミレーションをすることもあろう。これまではそうした要請のために、ノートＰＣに数百人分の顧客データを保持し持ち歩いていたと思われる。これではあまりに多くの危険性を内包する。そこで、業務改善策としては次のように考える。まず、顧客データは、事業所のサーバに置き、持ち出さず、ＷＥＢベースで見られるように設定しておき、外回りの従業員はサーバーに入るためのパスワードやＰＫＩのアクセスキーを持つのみとする。顧客回りをしている従業員は、空のノートＰＣを持ち、客先でインターネットを利用して、アクセスする。顧客先で、サーバーに入って、必要なデータをサーバー内で操作し、情報を見せて勧誘する、といった方法が考えられる。記録を残せないノートＰＣであれば、その後の紛失の危険もないためさらに安全である。従業員が大量のデータを持ち歩かない分、安全といえる。こうした方法は、シンクライアント、サーバーベースオペレーティングといった呼称で呼ばれている形式のものが提供され始めている。

また、何らかの理由からどうしても持ち歩く必要がある場合には、訪問予定の顧客のデータのみを、絶対に身体から離さない構造にした記憶端末、ＵＳＢメモリなどに、その都度記録して、携帯する方法も考えられる。

こうした業務手順や、環境を改善することで、危険な作業や危険因子を排除することが可能となり、作業担当の従業員はきわめて安全な環境で業務を遂行できるようになり、事業者のみでなく、従業者にとっても安心な業務となる。

５　コンプライアンスの失敗事例

（１）コンプライアンスの困難性

コンプライアンス（法令順守）が求められており、各企業はコンプライアンス部を創設して、さまざまな対策を実施している。企業では、行動基準を明確にし、研修会をこまめに実施し、業績評価を行い、細かなルール作りを行い、監視体制をとるなどの工夫がなされている。ところが、そうした体制をほぼ完成させたはずの有名企業で、次々とコンプライアンス違反事案が発見され、社会問題とされている。

これらの事象は、コンプライアンス(法令順守)の困難性を示すとともに、これまでの手法では不十分であることを証明しているともいえる。法令順守を求めることが困難である理由は明らかである。法令が存在するということは、違反事実がはびこる危険があるため規制するのであって、もともと犯され、破られる危険があるのが法律なのであって、法律を守るというのはそう簡単なことではないのである。利益を求め、違法行為までもが横行するのは、世の常である。法律は基準を示して、違法判断し、処罰するのだが、残念なことに違法行為は常に一定量存在しつづける。

コンプライアンスの実現のためには、こうした本質的な困難性を明確にした上で、その根源を断つ姿勢で臨む必要がある。

（２）透明性の確保

現時点でのコンプライアンス違反事例の多くが、事故隠し（食品メーカー、自動車メーカーなど）であり、告知すべき事実を隠した取引（マンション販売、ディーゼルエンジン販売など）をしている事例である。いずれにしても事実の隠蔽がその原因となっているといえる。従って、まず企業に求められるのは「透明性」の確保である。別の言葉で言えば説明責任といってもいいだろう。説明責任は事業者の立場や対消費者との関係で発生することが多いようだが、透明性の確保はさらに広く、企業自体の社会的存在を意識して、広く投資家や、未来の投資家、さらには影響する社会全体に対して、自らの活動の全貌を広く開示してゆくことを意味している。こうすることで、企業は常に社会の目、他人の目を意識し、業務遂行の姿勢が正されることになる。よどみ、隠され、見えない中で犯罪が仕組まれ、実施されることを考えれば、透明性を確保することの重要性は明らかだろう。

６　業務改善の視点からのコンプライアンス対策

より徹底したコンプライアンスの実現は、業務改善によって実現すべきである。既に述べたように、個人情報保護もまた法令遵守の一つであるから、個人情報保護対策はコンプライアンス対策そのものといっていい。

コンプライアンスの場面で、独自に考慮すべき問題がある。それは、企業ぐるみ犯罪であり、経営者、管理者の犯罪という点である。大型のコンプライアンス違反事件は、企業経営者の手によるものである。

そこに必要なことは、経営者をも規律し、その違法行為によっても破綻しない仕組みを持つことである。この場合、行動規範や監督体制はほとんど機能しない。それ自体は従業員監督には一定の有効性があるとしても、監督する側（経営陣）には機能しないことが多い。では、経営者でも手を触れられないものとはなにか。時間である。時間の流れを変えることは誰にもできないため、これをデータに埋め込むこと（タイムスタンプ）で、変造できない証拠が完成する。すべての記録に対してタイムスタンプを押すことが偽造変造を防止する方法となる。しかし、作成記録そのものを破壊し、隠匿するなどの行為が行われることもある。こうした行為に対しては、そうした破壊、隠匿の事実が表示されるシステムを必要とする。

結局、必要な対応とは、明確な業務手順を定めて、手順に従った記録を機械的に取れるようにシステムを構成し、かつ、明確なルールを定める。その上で、記録したものに対して偽造、変造防止のためのタイムスタンプを義務化し、連続した情報として記録し保管する。

コンプライアンス対策の場合には、経営者などによる証拠隠しなども、重大な危険因子となる。従って、業務改善の一つとして、業務の危険因子を排斥するとともに、その一環として、業務記録を機械的に行って、順次タイムスタンプを付して証拠化するということで、偽造変造、記録隠しなどに対抗するということである。

７　監査の実をあげる対策

業務監査の厳格な実施など、言われるほど易しいものではない。毎日、担当業務を遂行する人間ならば、その業務の問題点や自らのミスなどを認識することが可能かも知れなしが、日常的にその業務に従事していないものが、業務監査を行うのは不可能というべきである。業務の詳細を知らない上、ヒアリング程度しか情報収集ができないとなれば、業務担当者の言うなりになるほかない。違反事実を摘発することなど、おおよそ無理ということになる。

監査の実を挙げ、適正業務を確保するというのであれば、既に述べた業務改善が必要である。即ち、業務改善行為によって危険因子が排除されていること、即ち、その業務の重要な部分の業務記録（受付原簿、破棄原簿、業務報告、業務記録、アクセスログなどの記録）が完全にとられ、それらがタイムスタンプによる時間の証明がなされ、偽造検出を可能としているといった状況があること、こうしたチェックポイントが客観的に確保されているのであれば、監査対象が明確になる。

加えて、監査人、監査機関に調査権限があることが必要である。こうした記録相互の照合によって、業務のズレや逸脱などが判明するとしても、その原因を明確にして、対策を立てるためには事案の真相究明が必須である。従って、そうした観点からは監査人の調査権限が保障されなければならない。

現在のところ、こうした業務改善行為も調査権限の付与もない中で、企業の多くは企業外部の専門家による監査を求めようとしている。しかし、業務は内部の作用であるのだから、外部の人間にその実際がわかるはずもなく、外部の人間に調査権限が与えられることもまず考えられない。従って、外部専門家による監査機関というのは、内部の監査体制が既に述べたように業務改善や記録保管が実施され、それを基礎に内部監査の実が挙がっていることを確認し、点検するといった意味を持つだけであり、それ以上の機能を期待することはできない。

こうして、コンプライアンスもまた、業務改善行為に依存することになる。

８　新しいビジネスシーン

以上は、従来型の業務を基礎に、その業務を改善するという視点で立論を試みたものである。しかし、既に別の視点から、業務の本質的な見直し行為が試みられている。ここで

は新しいビジネススキームを検討したい。

個人情報保護の観点からは、究極の業務改善は、個人情報を使わないビジネスを考案することである。即ち個人情報に代わる情報を利用し、事業活動を進めることである。即ち事業者が、個人を識別できる情報を持たないで、なおかつ特定の個人に対して各種のサービス提供を可能にすることである。

① リーチ情報の利用（匿名直接型）

既に一部研究者の方々から、個人情報とは区分できる情報として、「リーチ（Reach）情報」という概念が提唱されている。その趣旨は、本人の識別ができる情報ではないため、個人情報とはならない性格のものではあるが、確実に本人の手元に情報が提供され、本人が受領可能な状態になる、という特徴を持つ情報である。電子メール情報などは、それ自体に氏名が埋め込まれているものは個人情報となるといわれるが、アトランダムに設定されたＩＤなど、個人が識別できないＩＤは多数存在する。こうした情報のみを保持して、他に照合できるような氏名情報などを持たないという条件下では、事業者はメールアドレスと個人名などを容易に照合できないため、個人情報とはいえないことになる。具体的には、匿名で作成できるＷＥＢメールなどであれば、実在の存在確認をしない上、各自が自由に設定ができること、そのアドレスを自身のものとして表示すれば、以後事業者はそのアドレスを対象としてサービスを開始できるのであって、必ずしも事業者は個人名、実在の氏名を持たずとも良いことになり、この場合のＷＥＢメールのアドレスは、個人情報とはされない。従って、個人情報保護法の適用対象とはならないという点がポイントとなる。

こうした「リーチ情報」には、次のものが当たると思われる。

電子メールアドレス
携帯メールアドレス
電話番号、携帯電話番号
私書箱（郵便局私書箱、私設私書箱）

ただ、こうしたリーチ情報だけでは、決済に関しては支払い義務者の特定ができないため、一定の限界があるのも事実である。従って、決済機能は別に持ち、利用することが必要となる。プリペイドカード方式や登録時一括して支払いを済ませる方式、会員番号など特定のための符号を付して送金先を指定して、送金者として表示された会員番号などによって、利用者からの支払いを確認した場合に情報や、物品を提供する方法も考えられる。

② 仮名情報の利用（匿名間接型）

次に、事業者が把握するのは、個人情報ではなく、一定の一意の符号であって、その符号に対して送付することが可能となる仕組みで、たとえば、宅配事業者、配送センタ

ーなどの中間介在機関があり、その機関に実名登録及び符号（ハンドルネームや呼称、他と重複しないニックネームなど）の登録があり、その機関で、実名と符号や呼称との接合機能を果たす方式である。

この方式は、既に日本ＩＢＭの研究者から公表された方式であって、事業者は個人を識別することなく、事業活動を行うことが可能であることを示した点で興味深い。従って、事業者には個人情報保護法の適用はない。ただ、中間に介在する配送センターなどが両方の接合を行うことから、個人情報取扱い事業者となるとともに、その機関がきわめて重要な存在となる。

決済に関しても、事業者は本人情報を持たないことから、中間に介在する配送センターなどを介した決済情報を保有することになり、訴訟を提起するなどの場合には、新たに中間事業者に対して開示請求を行うことが求められる。従って、事業者のサービスを受ける前に、利用者との間で、開示を認める一定の契約、約款などによる合意の形成が必要となると思われる。

③　プロファイル・ポータビリティ・システムの利用

松下電器、ピアなどの事業者が中心となって、ＰＫＩシステムを利用した、プロファイル・ポータビリティのシステムが提案されている。

今回のフォーラムにおいて、担当者からその詳細について解説がなされる予定であるが、このシステムは、①の「リーチ情報」の概念を発展させ、なおかつ②の中間介在方式を活用することで、より広範な事業者の利用可能な構造を提案するものであり、新しい事業スキームを提案するものとして注目される。

詳細は、当日の解説を参照されたい。

個人情報は、その個人そのものの唯一の情報を、ビジネスの際の本人との間のサービス提供や物品の送付、請求、決済に利用するものであって、ビジネスのすべての局面で相当慎重な対応が求められる。ところが、情報提供サービスや、オンラインビジネスなど、比較的小額で、大量の取引を行う業種のもの、現実的な決済を中心に行い、情報共有を中心に行う業種などにあっては、個人情報といった貴重な情報を扱うことなく、より合理的な処理を可能にすることが求められる。その方法が見出されている以上、その活用が望ましいのは言うまでもない。

事業者にとって、取引の相手が、佐藤さんであるか、鈴木さんであるかはさほど重要ではない。むしろ、取引対象となる相手としての存在が重要であり、最低限支払いが確保されれば良いとも言える。信頼関係が確立されてゆく中では、相手の呼称が重要になることはあっても、それ以上本名を求めることはない。結婚して戸籍を入れるなどの特段のことがない限り本籍に表示された本名など、必要もないし、求めることもない。

この事実を客観的に見た場合、相互のリーチ情報の交換と、決済手段の確保によって、

ビジネスは可能となってくるものと思われる。

9　情報セキュリティ、情報力の拡大に向けて

個人情報保護法は、個人情報の取り扱いについて、管理責任を問題とする法律制度ではあるが、その 20 条の定める安全管理措置は、さらに多くの課題を内包する。20 条の定めは茫漠としており、必要かつ適切な措置の内容が明らかでないため、その具体的に求められる措置の内容は、各行政機関が定めるガイドラインによって明記されることになる。なお、この仕組みは、法律の安定性の観点からは、法律が必要事項を規定していないとも考えられ、白紙委任的であるということもできるものであり、いささか疑問ではあるが、現在のガイドラインを見る限り、法の趣旨に従った解釈の範囲にあるものと思われ、具体的な疑問を持つものではない。

主にガイドラインによって明らかにされている安全管理措置は、個人情報の保護という範囲をカバーするものではあるが、そこに記載された各種の措置は、個人情報保護にとどまらず、より広く活用される性格のものとなっている。組織的対策、人的対策、物的環境対策、技術的対策のいずれをとっても、情報システム、情報資産の保護にとっても欠くことのできない仕組みが求められているということができる。個人情報という情報資産を守る仕組みは、個人情報資産だけでなく、法人情報や各種の機密情報を守る上でも十分活用できるものとなっている。

こうして個人情報保護対策は、広く情報資産や情報システムを守り、情報関連の安全利用を確保するための制度整備の側面を持つものでもあり、今求められている「情報力」を装備するための重要なポイントとなる。個人情報保護対策は、一過性のものではなく、今後の企業の情報分野における競争力をつけるものであり、まさに情報を的確に利用し、かつ安全に保管管理する力、即ち「情報力」をつけるものとなっている。

我々は、目の前の個人情報保護という問題に目を奪われることなく、5 年先、10 年先の情報社会における競争力を鍛え上げてゆく過程として、現在の対策を考え、大きな展望の中で捉えなければならない。