資　料

個人情報漏洩のリスクマネジメントと保険について

—— FPとしての視点 ——

Leakage Risk Management of Personal Information and Insurance

—— Viewpoint from FP ——

長崎県立大学　赤堀　勝彦/*Katsuhiko AKABORI*

〈キーワード〉

個人情報漏洩リスク	リスクマネジメント	保険
leakage risk of personal information	risk management	insurance

〈要　約〉

近年、民間企業や行政による情報漏洩事件が相次いで発生しており、個人情報の保護に対して社会的にも注目が集まってきている。ITが高度に発達したネットワーク社会において、事業者は情報漏洩という新たなリスクに直面していることから個人情報を保護するための厳しい管理体制が求められている。そうした中で、2003年５月に成立し、その一部が施行された「個人情報の保護に関する法律」（個人情報保護法）が2005年４月より全面施行され、実際に個人情報取扱事業者の義務規定、罰則規定等が適用されることとなった。

個人や家計のパーソナル・ファイナンスにかかわるFPは、法律で求められている内容を理解することは当然のことであるが、この法律の施行にかかわらず、個人情報の取り扱いはFPの倫理要件の代表的なものとなっていることを踏まえて、個人情報の取り扱いに対しては十分な認識と注意が必要である。

一方、FPを消費者としての視点から捉えると、情報が氾濫する中で、自分の情報は自分で守るという意識を持って行動する必要がある。すなわち、消費者自身による個人情報流出防止に努めるなどリスクマネジメントを徹底することが重要である。」

また、最近は個人情報漏洩に対して、第三者への損害賠償やブランド価値の毀損の防止・縮減を補償する個人情報漏洩対応保険が発売されている。保険は、リスク・ファインシングの観点から有効と考えられるが情報漏洩リスクのすべてが保険で補償されるわけではない。その意味でも、今後、個人情報取扱事業者は単に法律を遵守するだけではなく個人情報保護法ガイドラインを踏まえた、機能的な安全管理措置を実践していくことが不可欠である。

１．はじめに

最近、個人情報の大量漏洩・流出事件が頻繁に報道されている。個人情報の漏洩元は、官庁から病院、インターネット接続会社、通販会社など様々である。また、銀行、保険会社、信販会社など金融機関からの流出も相当数ある。従来も情報漏洩が報じられたことはあるが、近年の情報漏洩は、件数も多く、１件あたりの情報の量が多いのが特徴である。

そのような中で、個人情報の適正な取扱い方法等をルール化した「個人情報の保護に関する法律」（以下、個人情報保護法という）が2003年５月に制定され、その一部が施行されていたが、2005年４月１日より全面施行されることとなった。

個人情報保護法は、「個人情報の適正な取扱い」を基本理念として、国や地方公共団体の責務等を規定しており、個人情報保護、個人の権利・利益を保護することを目的とした法律である。また、個人情報保護法は、個人情報保護の基本法としての性格と、民間部門の個人情報保護の一般法としての性格を併有する。この一般法の適用を受けるのは、個人情報取扱事業者(1)であるが、営利事業を行うことは、個人情報取扱事業者の要件ではなく、NGO等も含まれ得る。個人情報取扱事業者の数は数百万人に上ると予想されており、その影響は極めて大きいといえる。

個人や家計のパーソナル・ファイナンスにかかわるFPは、法律で求められている内容を理解することは当然のことであるが、この法律の施行にかかわらず、個人情報の取り扱いはFPの倫理要件の代表的なものとなっていることを踏まえて、守秘義務を遵守し、個人情報の適切な保護と利用が求められる。すなわち、FPは自ずと顧客のプライバシーにかかわる情報を知り得る立場にあることから、その情報が顧客の意に反して漏れた場合、顧客とFPとの関係が破綻するばかりでなく、損害賠償責任を負うことになる場合もある。ひいてはFP全体に対する信頼の失墜につながるため、職務遂行上、十分に留意する必要がある。

したがって、個人情報漏洩を職務上のリスクと捉え、個人情報漏洩リスクに対する適切なリスクマネジメント体制を構築することが重要である。

本稿は、相次ぐ個人情報漏洩事故に対するリスクマネジメントおよび個人情報漏洩対応保険について、FPとしての視点から考察することとする。

2．個人情報漏洩リスクとリスクマネジメント

2.1　個人情報漏洩による賠償責任リスク

⑴　民事上の責任追及リスク

個人情報の漏洩者に故意・過失がある場合、漏洩者は、本人に対しプライバシー権侵害に基づく不法行為責任を負い、漏洩者の雇用者や委託元である事業者は、使用者責任（民法715条）に基づく損害賠償請求を受けることになる。

プライバシー権は、その内容について様々な捉え方があるが、ここでは損害賠償の前提となる人格権としてのプライバシー権が問題であり、一般に「私生活を意に反して公開されない権利」、「そっとしてもらう権利」として捉えることが可能である。

また、漏洩者が不明であっても、本人から契約によって個人情報を取得して個人データとした個人情報取扱事業者は、本人に対して契約上の安全管理義務を負担しており、個人データの安全管理（個人情報保護法（以下、単に「法」という）20条～22条）に不備があった場合には、債務不履行責任（民法415条）に基づく損害賠償請求を受ける可能性がある。この債務不履行責任は不法行為と同様過失責任であるから、事業者自身に個人情報の漏洩について過失がなければ責任を負うことはない。しかし、例えば従業員が個人情報を取り扱う上で故意または過失によって第三者に漏洩した場合、その従業員の過失は、信義上事業者自身の過失と同視されることになる。

さらに、漏洩事件により事業者に損失が発生した場合には、取締役・監査役は、株主代表訴訟（商法267条）により、事業者に対する損害賠償責任（商法266条、280条）や、本人に対する損害賠償責任（商法266条の３，280条）を追求される可能性がある。

⑵　個人情報保護法上の行政処分リスク

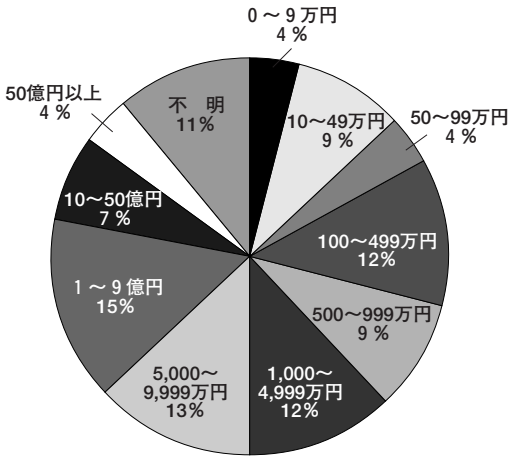
政府の個人情報の保護に関する基本方針（2004年４月２日閣議決定）では、「大規模な個人情報の漏洩等個別の事案が発生した場合、各省庁は、各事業等分野における個人情報の適正な取り扱いを確保するため、必要な情報の収集に努めるとともに、当該個別の事案の被害の広がりや社会的な影響を踏まえ、迅速に法第4章の規定に基づく措置[2]等の検討を行う」としている。

なお、命令には、勧告を先行させる通常の命令（法34条２項）と勧告を先行させない緊急命令（法34条３項）との二種類があるが、命令に違反した場合、行為者は、６ヶ月以下の懲役または30万円以下の罰金を科され（法56条）、事業者は、両罰規定により30万円以下の罰金を科される可能性がある（法58条）。また、報告を怠ったり、虚偽の報告をしたりした場合には、行為者と事業者は、それぞれ30万円以下の罰金を科される可能性がある（法57条、58条）。

以上のとおり、個人情報漏洩事件が起きた場合、事業者には債務不履行、不法行為に基づく損害賠償責任が発生することもあり得る。また、損害賠償以外にも、謝罪広告やお詫び状の郵送による費用の支出が必要な場合が考えられる。近時の個人情報漏洩事案においては、数十万人から数百万人分の個人データが漏洩した事案が見られるが、この場合郵送費用だけでも膨大な金額となることが予想される。さらに、適切な対応がとられない場合、顧客を軽視し、コンプライアンス意識が低いという印象を社会に植え付けてしまう可能性がある。その結果、信用が大きく悪化する他、顧客の離反や新規採用、株価、格付けの低下、資金調達コストの増加など事業者の経営にも広く悪影響を及ぼす可能性がある。いったん損なわれた信用を再び回復するには、個人情報保護に関する本格的な取組みによる十分な保護レベルの確立が不可欠であるが、それを対外的に周知させるための広告費用も見逃すことのできないものである。

なお、2003年度（１月～12月）における情報漏洩一件あたりの損害賠償額は、NPO日本ネットワークセキュリティ協会の調査によると、賠償損害額１億円以上の事件が26%となっている。その損害賠償額の合計は全体の約97%にあたり、損害賠償額が高額とされる事件が発生している（図１）。

図１　情報漏洩一件あたりの損害賠償額



出所：NPO日本ネットワークセキュリティ協会「2003年度情報セキュリティインシデントに関する調査報告書」2004年３月31日、18頁。

表１　情報漏洩の原因

要　素	原　因	2003年の比率(％)	原因の内容
技術的	人為ミス	46	設定ミス､誤操作､管理ミス
	対策不足	11	バグ・セキュリティーホール、不正アクセス
非技術的	人為ミス	2	置き忘れ
	犯　罪	25	内部犯罪、情報持ち出し、盗難
その他		11	
不　明		5	－

出所：NPO日本ネットワークセキュリティ協会「2003年度情報セキュリティインシデントに関する調査報告書」2004年３月31日、12頁。

表２　情報漏洩の経路

要　素	経　由	2003年の比率(％)
インターネット	Web経由	20
	Email経由	17
	FTP経由	2
媒　体	紙媒体	14
	FD等可搬記録媒体	14
	パソコン本体(DISK等可搬記録媒体)	11
その他		4
不　明		18

出所：NPO日本ネットワークセキュリティ協会「2003年度情報セキュリティインシデントに関する調査報告書」2004年３月31日、14頁。

2.2　個人情報漏洩の原因

最近の漏洩発生の原因あるいは動機の一つとして、個人情報の場合、それを買う者が現れたことが挙げられる。また、入手した情報を架空請求等に利用することもあるといわれている。すなわち、個人情報の価値が上がり、自らが利用しなくても他者に売るために不正に情報を入手するケースが増加しているか、あるいは、漏洩のリスクが高まっているといえる。

個人情報漏洩の事例では、その原因や影響も個々の事例により異なるが大きく分けると、次の３つのタイプに分類できる。

① 外部からの浸入（事務所外から立ち入った第三者が、事務所内に保管している書類、記録媒体、パソコン等の個人情報を違法に持ち出す。あるいは、車上あらし、成りすまし等も含まれる）

② 内部者の故意の持ち出し（内部者が事務所内に保管している個人情報を意図的に持ち出す。また、内部者の中でも委託先や派遣者が関与したものも含まれる）

③ 内部者の過失によるもの（内部者が、事務所内に保管している個人情報を営業上の理由その他の目的で事務所外に持ち出して喪失する場合や、置き忘れ、誤送信等によるものも含まれる）

上記の中で、細部にわたってみると、例えば侵入自体が違法な場合や、合法的に立ち入って違法に個人情報を持ち出した場合、事務所内で個人情報にアクセスする権限があった場合となかった場合、持ち出した個人情報をどこかに置き忘れた場合と第三者に窃取された場合など、事例によって様々な相違がある。

NPO日本ネットワークセキュリティ協会による2003年度の情報漏洩の原因と経路の調査結果は、表１および表２のとおりである。

情報漏洩の原因について、前年度（2002年度）と比較すると、前年度は非技術的要素の人為ミス・犯罪が７％であったのに対し、2003年度は27%と、約４倍に増加しているのが目立つ。一方、前年度は技術的要素の人為ミス・対策不足が全体の88%を占めており、情報漏洩原因の大部分を占めていたのに対し、2003年度の技術的要素の人為ミス・対策不足は、全体の57%であり、情報漏洩の原因の半数強に減少している。

2.3　個人情報漏洩のリスクマネジメント

本項では、事業者および消費者の両面から考察することとする。

⑴ 事業者としての個人情報の適切な管理の重要性

個人情報の適切な管理には、安全保護管理だけではなく、個人情報の取得から、廃棄、苦情対応まで広範な対応が必要となる。情報システム部を中心とした対応だけでなく、全社的な対応が必要とされる点に難しさがある。

個人情報漏洩をはじめとして、個人情報の不適切な管理による事故を個人情報保護リスクと捉え、リスクマネジメントの枠組みの中でリスク対策として個人情報保護対応を進めていくことが有効と考えられる。

具体的な手順としては、対応策の立案（Plan）、対応策の実施（Do）、対応策の実施状況の見直しと改善活動（Act）というサイクルを継続的に回していく必要がある。そのための重要な要素は、リスクの変化を反映した、対応策や対応の仕組み・体制の見直しを適時行うことである。

また、個人情報保護法を遵守するためのコンプライアンス体制を事務所内に構築しておくことが重要である。個人情報保護法を遵守するためのチェックポイントの例は表３のとおりである。

さらに、個人情報保護法の個別の義務に従うことだけでなく、違法行為を防止すると同時に発見・是正するための取り組みを恒常的に行っていくことが本来的には必要である。このような見地から、プライバシーマーク[3]を取得することとかISMS[4]を導入すること等の対応が重要とされる。これらの取得・導入には、一定の人的・物的資源を投入することが不可欠であるが、個人情報保護

表３　個人情報保護法遵守のためのチェックポイント（例）

個人情報の把握	□何が個人情報に該当するのかについて具体的に検討しているか □どのような個人データを保有しているのかを具体的に洗い出しているか □個人データのうち、保有個人データに該当するものが何かについて具体的に洗い出しているか □個人情報について、だれが管理責任者であるかが明確になっているか
個人情報の取得	□取得している個人情報について利用目的を特定しているか □利用目的の明示は適切に行われているか □利用目的の通知、公表等の手段が具体的に定められているか（特に第三者から取得する場合） □利用目的の変更等が想定される場合、その利用目的の変更時の通知、公表の手続きを定めているか
安全管理措置	□個人データの情報セキュリティ対策について、セキュリティポリシーや関連規程、ルール、手順を定めているか □従業員に対して、個人データの安全管理についての教育を行っているか □個人データの処理等を外部委託している場合、どこに委託しているかを把握しているか □外部委託先との契約の有無、契約内容（特に機密保持、再委託の制限について）を確認しているか □外部委託先の管理状況を把握しているか
第三者提供	□第三者提供を行っている場合、あらかじめ本人の同意を得ているか □同意を得ていない場合、本人の求めに応じて個人データの第三者への提供を停止する仕組みができているか □同意を得ていない場合、第三者へ利用目的とすること、第三者に提供される個人データの項目、第三者への提供の手段又は方法等についてあらかじめ本人に通知し、又は容易に知り得る状態に置いているか
共同利用	□共同利用する旨、共同利用する個人データの項目、共同利用する者の範囲、利用する者の利用目的、共同利用する個人データの管理責任者の氏名等をあらかじめ、本人に通知、又は容易に知り得る状態に置いているか
開示、訂正等、利用停止等	□開示請求の求めのための窓口を定めているか □開示請求の求めのための手段を定めているか □開示請求者の求めに利用する書面の様式等を定めているか □訂正等を行い、本人にその旨を通知するための手段を定めているか □利用停止等を行い、本人にその旨を通知するための手段を定めているか □請求時における本人確認の方法について定めているか □手数料について定めているか □手数料を徴収する場合、徴収方法を定めているか
苦情処理	□苦情対応のための窓口を定めているか □苦情対応のための体制は整えているか

出所：丸山満彦「コンプライアンス体制の構築」『企業リスク』第１巻第２号（通巻第２号）トーマツ企業リスク研究所、31頁。

に高い価値観を持って取り組んでいることを示すことができるメリットも存在する。なお、すべての事業者がこうしたマネジメントシステムの構築に着手しなければならないというわけではないが、業種上の特性や、個人情報の量、取扱実態、法令抵触リスクの大きさ等を考慮に入れつつ、取り組みの必要性について検討しておくことが重要である。

その一方で、事業者は万一の事態に対処するため、日常から危機管理計画を立てておき、個人情報漏洩対応保険等に加入しておくことにより、適正なリスクの分散を図っておくことが必要である。

⑵ 事業者としての個人情報漏洩事故への対策

個人情報漏洩事故の原因について増加割合が高い盗難、紛失についての基本的な対策をまとめると以下のとおりとなる。

1）盗難に対する基本的な対策

① 施錠管理の徹底、警備体制の強化等を行い、来訪者の入室管理を徹底するとともに、事務所等への侵入防止対策を強化する
② 事務所内で来訪者に応対する際は、所定の場所に限定して対応する
③ 重要な情報にはパスワードを設定して保管する
④ 車上荒らし対策としては、僅かな時間でも、また、施錠の有無にかかわらず、車内に個人情報を放置しないことである

2）紛失に対する基本的な対策

① 個人情報が記載されている資料やFD・MOなどの電子データ媒体の保管ルールを明確に定め、ルールを遵守する
② 電子データ類は、パスワードを設定し、不要なデータは取得・保有しない[5]など必要なセキュリティ対策を講じておく
③ 不必要なコピーやプリントアウトを制限する
④ 事務所外への個人情報の持ち出しについては「禁止する」、あるいは、「許可制にする」など、一定のルールを定めたうえで遵守する
⑤ 従業員宅への個人情報持ち帰り禁止などのルールを作り[6]、ルールを遵守する
⑥ 外出先では、個人情報は僅かな時間でも放置せずに常に携行する

⑶ 消費者としての個人情報漏洩事故への対策

基本的な対策としては、上述の事業者としての対策と類似しているものがあるが、特に生活者として留意すべきことをまとめると以下のとおりである。

1）流出に対する基本的な対策

① ホームページに載せる個人情報に注意する
② クレジットカード番号等の入力に注意する
③ クレジットカードの利用明細（カード売上票（控）、カード利用表）を処分するときには注意する
④ インターネットカフェを利用する際に注意する
⑤ アンケート調査・懸賞募集に注意する

2）セキュリティ対策

① ユーザーIDとパスワードの管理を徹底する
② 外部からの不正なアクセスを遮断したり、無用のデータを他に送信させないためファイウオールの設定をする
③ ウイルス検知ソフトを導入する。また、最新のデータに更新しておく
④ 不審なメールは開かないことと不要なメールは送らないことにする
⑤ 不安を感じた場合は、事業者に対して利用停止請求を行う

⑷ 今後の課題

国民生活センターの「個人情報流出事故に関する事業者調査結果」[7]（2005年３月25日公表）によると顧客の氏名や住所など個人の情報を流出させた事業者の約７割が、管理責任者の配置など流出の防止策を講じていたにもかかわらず、流出事故を起こしていたことが判明した。調査では2003年～2004年に情報を流出させた事業者94社を対象に、44社、45件の事故について回答を得ている。45件の事故で流出した個人情報は名前、連絡先、性別、年齢、生年月日といった個人識別情報の他に生命保険の設計書や、口座番号と暗証番号が記載されたクレジットカードの入会申込書など被害に直結する情報が含まれていた。

また、流出事故当時の事業所内における管理体制は、45件の内34件（76%）が「プライバシーポリシーを策定していた」、「規定やルール等を整備していた」、「保護管理者等を設置していた」、「情報システムへのアクセス制御を行っていた」など何らかの措置を講じていた。しかし、「規定が不十分であった」、「個人情報へのアクセスが容易であった」、「従業員に対する教育が不十分であった」など、管理体制上の問題を事故原因とした事例は33件（73%）あり、規定等は整備されていたが運用において事業所内の管理体制が不十分であったといえる。一度流出した情報の流出を防ぎ止めることは困難であることを踏まえ、個人情報取扱事業者は個人情報流出問題の重要性を十分に認識する必要がある。

なお、流出先が判明した事故の概要は、表４のと

表４　流出先が判明した事故（12件）の概要

	流出先	流出先での利用	流出先への対応	事故の概要
A社	暴力団関係者と名乗る人物	流出先での利用事実はない	弁護士に委任し原本の回収を行った、裁判所に対して営業機密に係る情報の不正使用禁止等を求める仮処分の申立を行った	従業員による持ち出し
B社	信用調査会社	社内データとして利用していた	流出先から現物を回収するとともに、情報を外部にもらさないという誓約書をとった	従業員による持ち出し
C社	名簿業者	架空請求、電話による商品先物取引などのセールス	名簿の買い戻し、名簿の再利用禁止、データ削除	従業員による持ち出し
D社	名簿業者	不明	流出先から回収し、データ削除されたことの証明書を取得した	委託先従業員による持ち出し
E社	漏洩仲介業者（ブローカー）	不明	連絡が取れず警察に任せた	従業員による持ち出し
F社	金融ブローカー	流出先から興信所に情報が流れ、企業の採用情報の判断材料として利用された可能性がある	警察に届出、個人信用情報機関への報告	従業員による持ち出し
G社	インターネット上で売買	インターネット通販で利用された	被害拡大防止のため、モニタリングを実施した	委託先従業員による持ち出し
H社	名簿業者	回収したとの報告を委託先から受けている	回収をしたため対応はしていない	委託先（人物は特定できず）からの持ち出し
I社	名簿業者	NA	NA	従業員による持ち出し
J社	顧客	NA	NA	メールをCCで送信した
K社	取引先	悪用は認められなかった	返却してもらった	誤送付
L社	一般個人	利用はされていない	回収した	個人情報が記録された記録媒体を残したままパソコンを処分

出所：国民生活センター「個人情報流出事故に関する事業者調査結果」2005年３月25日、３頁。

おりである。

国民生活センターの上記調査結果を踏まえ、個人情報漏洩のリスクマネジメントの今後の課題を挙げれば、先ず、事務所内等においては個人情報の安全管理措置を徹底すると共に従業員等の監督を徹底することである。さらに、情報処理会社や配送会社などすべての個人情報取扱経路について、委託先の管理体制の確認や契約条項の見直し等、具体的な委託先の管理を徹底することが重要である。また、現在、個人情報の漏洩・流出事故が発生しても、その事実すら消費者は把握できない可能性があり、被害回復等の方法が塞がれてしまう恐れがあり、架空請求等の二次的被害の防止という観点からも、漏洩・流出事故の関係機関への報告・通知・公表についての統一的なルールの整備が必要である。最後に、内部の従業員の持ち出し等により個人情報が外部に流出したというケースが目立つことから個人情報保護の実効性を確保するためにも、従業員の重大な過失による情報の流出を含めた情報窃盗の刑罰化の是非について早急に検討する必要があると考える。

一方、消費者の立場からは、自らの個人情報が大切なものであることを十分認識して、むやみに情報を提供しないことと信頼できる事業者だけに提供するといった心構えが求められる。

3．個人情報漏洩に対応する賠償責任保険

3.1　個人情報漏洩対応保険の特徴

個人情報の漏洩事故が発生した場合、当事者である事業者は、損害賠償金の支払いを余儀なくされる可能性があるだけでなく、長年をかけて築いてきた信用や消費者からの信頼を失いかねない。かかる事故が発生した際には、信頼を回復すべくアカウンタビリティ（説明責任）の遂行や広報宣伝活動を行う必要がある。個人情報漏洩対応保険は、こうした事業者が負担する損害賠償金や各種費用を補償することにより、事業活動を支援することを目的としている。この保険は、賠償責任保険に属し、その担保範囲としては、法的な賠償責任に関する部分から争訟に応じるための弁護士費用等、謝罪広告やお詫び状郵送に関する費用に至るまでの広範な損害を補償する。

補償内容は一般に保険会社が定めた一定のパターンから選択できる。また、保険料の算定にあたっては、会社の規模、取り扱う個人情報の件数および内容等から一般的な算定式に基づく査定を行ったうえで、プライバシーマークやISMS適合性評価制度等における認証を受けていることなど個人情報保護体制の確立状況に応じて保険料を減額する扱いにしている場合が多い。

3.2　個人情報漏洩対応保険の概要

個人情報漏洩に対応する賠償責任保険には、個々の事業者向けの保険の他に日本商工会議所などの会員向けの団体保険[8]がある。ここでは、個々の事業者向けの保険の概要を紹介することとする[9]。

⑴　保険の補償内容

①　他人から訴えられた場合に生じる損害

偶然な事由により個人情報[10]を漏洩したこと、またはその恐れがあることに起因して、保険期間中に日本国内において損害賠償請求がなされたことにより、被保険者が法律上の損害賠償金と弁護士費用等の争訟費用を負担することによって被る損害について保険金が支払われる。

②　個人情報漏洩発生時の対応に必要となる費用

被保険者が取り扱う個人情報が流出したまたはその恐れがある場合において、被保険者が保険会社に事故を通知した日以降に発生した公（広）告費用[11]、通信費用、コンサルティング費用[12]、見舞費用、マスコミ対応費用、臨時対応費用[13]、事故原因調査費用、損害賠償請求費用のうちあらかじめ保険会社が同意したものに対して保険金が支払われる。

⑵　契約例および保険金支払例[14]

①　契約例

保険金額：賠償責任　3億円、費用　3,000万円
免責金額：賠償責任　設定なし、費用　設定なし
縮小填補割合：賠償責任　100%、費用　95%

②　保険金支払例

損害賠償金および争訟費用：2,000万円
謝罪広告費用：1,000万円
信頼回復広告費用：500万円
通信費用：1,000万円

上記の場合、支払われる保険金は以下のとおり4,375万円となる。

2,000万円＋｛(1,000万円＋500万円＋1,000万円)×95%｝＝4,375万円

⑶　保険金が支払われない主な場合（賠償損害・費用損害共通）

次に掲げる事由のいずれかに起因する損害に対しては、保険金は支払われない。

①　保険契約者または被保険者の故意
②　保険契約者または被保険者が法令に違反することを認識しながら行った行為に起因する事故
③　被保険者に対して行政機関からの指導または個人情報の保護に関する法律第34条（勧告および命令）の規定による勧告もしくは命令（以下「指導等」という。）がなされた場合において、当該指導等がなされてから被保険者が必要または適切な措置等を完了するまでの間に発生した、当該指導等の対象となった個人情報の取り扱いに起因する事故
④　被保険者の使用人等または個人情報共同利用者等が被保険者のためにその事務を処理するにあたり、または自己の職務上の地位を利用して行った窃盗、強盗、詐欺、横領、背任行為または複製の作成[15]
⑤　戦争、外国の武力行使、革命、政権奪取、内乱、武装反乱その他これらに類似の事変または暴動
⑥　情報漏洩が客観的に確認できない場合
⑦　偽りその他不正な手段により取得した個人情報に生じた事故
⑧　被保険者の使用人等の個人情報の流出
⑨　個人情報以外の情報の流出

4．おわりに

情報化社会の発展を背景に、多量の個人情報が漏洩する事件が頻発している。このような事態を踏まえ、2005年4月1日より個人情報保護法が完全施行され、個人情報が漏洩した際の事業者の罰則が強化されることとなった。

家族構成から勤務先、資産、金融機関からの借入れなど、個人の重要な情報が蓄積されている個人情報取扱事業者において個人情報が漏洩した場合、個人情報保護法に基づく罰則の適用、監督当局の行政処分を受ける他、被害者本人からの損害賠償請求、マスコミ等の報道による社会的失墜などを避けることができず、ひいては事業そのものを揺るがしかねない、といっても過言ではない。

個人情報の流出を防ぐ方法としては、情報へのアクセスや事務所外持出しを必要最小の範囲に限定するという物理的な側面と、従業員の個人情報の管理に対する意識を深めるという心理的な側面がある。物理的な側面としては、個人情報へのアクセスを限定する方法と、事務所外への持出しを限定または禁止する方法が考えられる。故意に漏洩するような場合でなくても、従業員が漏洩でき

る情報は本人がアクセスできる情報に限られるであろうから、この範囲を営業上必要な範囲に限定しておけば、過失により漏洩される恐れのある情報はその範囲にとどまることになる。

また、最近は個人情報漏洩に関して、第三者への損害賠償やブランド価値の毀損の防止・縮減を補償する個人情報漏洩対応保険が発売されている。保険は、リスク・ファイナンシングの観点から有効と考えられるが情報漏洩リスクのすべてが保険で補償されるわけではない。その意味でも、今後、事業者は広範な社会的責任を果たし社会の期待に応えていくために、単に法律を遵守するだけではなく個人情報保護法ガイドラインを踏まえた、機能的な安全管理措置を実践していくことが不可欠である。

一方、消費者の立場からは、情報が氾濫する中で、自分の情報は自分で守るという意識を持って行動し、消費者自身による個人情報流出防止に努めるなどリスクマネジメントを徹底することが重要である。

注

(1) 個人情報保護法が適用される「個人情報取扱事業者」とは、個人情報データベース等を事業の用に供している者と定義され（同法２条３項)、その取り扱う個人情報の量、利用方法から個人の権利利益を害する恐れが少ないものとして政令で定める者は除外される（同法２条３項５号)。事業、すなわち一定の目的をもって反復継続して遂行される同種の行為であって、かつ一般社会通念上事業と認められるものであれば営利であると非営利であるとを問わず、また、個人であっても個人情報取扱事業者に該当することになる。そして、政令２条では、取り扱う個人情報が5,000人を超えない場合は、個人情報取扱事業者に該当しないとされている。

この5,000人を超えるか否かの判断においては、その事業所において管理するすべての個人情報データベース等を構成する個人情報を基礎に判断するから（重複分を除く)、個人情報を扱うほとんどの事業所は個人情報取扱事業者に該当することになると考えられる。

(2) 「法第４章の規定に基づく措置」としては、次のものがある。

① 報告の徴収（法32条）
② 必要な助言（法33条）
③ 個人情報取扱事業者の義務違反行為の中止その他違反を是正するために必要な措置を取るべき旨の勧告（法34条１項）
④ 正当理由なく個人情報取扱事業者が上記勧告に関わる措置をとらず、かつ個人の重大な権利利益の侵害が切迫していると認められる場合の、勧告に関わる措置をとるべき旨の命令（法34条２項）
⑤ 個人情報取扱事業者が個人情報または個人データの取り扱いに関する義務（利用目的の通知・公表（法18条）を除く）に違反し、かつ個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認められる場合の、義務違反行為の中止その他違反を是正するために必要な措置をとるべき旨の命令（法34条３項）

(3) プライバシーマーク制度は、個人情報の取り扱いについて適切な保護措置を講ずる体制を整備している民間事業者等に対し、その旨を示すマークとしてプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認容する制度で、1998年４月１日より運用を開始した。この制度は、個人情報の保護に関する個人の意識の向上を図ること、民間事業者の個人情報の取り扱いに関する適切性の判断の指標を個人に与えること、民間事業者に対して個人情報保護措置へのインセンティブを与えることを目的としており、日本情報処理開発協会（略称JIPDEC）が付与機関となって運用する。現在（2005年12月13日現在）のプライバシーマー使用許諾事業者は、2,635社である（http://privacymark.jp/list/clist)。

プライバシー制度の利用は、単に個人情報保護法に対応できる体制・仕組みを構築するための助けになるだけでなく、顧客、取引先等からの信頼性の向上や第三者機関によるお墨付きを受けることによる同業他社との差別化、さらに認証取得というゴールが明確なことによる従業員のモチベーションの向上などそれを利用する企業に様々な効果をもたらすことが期待される（岡崎史寛「プライバシーマーク取得のポイント」『企業リスク』第１巻第２号（通巻第２号)、トーマツ企業リスク研究所、2003年、36頁)。

(4) ISMSとは、情報セキュリティマネジメントシステム（Information Security Management System）のことで、個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用することである（http://www.isms.jipdec.jp/isms/index.html, 2004年３月３日)。ISMSに関する認証制度には、「ISMS適合性評価制度」と「BS7799－2の認証制度」の２つがあるが、認定・認証機関が異なるだけで

内容的には同じである。いずれの認証制度も、ISMS認証基準（Ver2.0）とBS7799-2:2002に適合したマネジメントシステムを整備し、情報資産の取り扱いを適切に行っている事業者を第三者機関が認証する制度である。ISMSにおいて、情報セキュリティとは、情報の機密性（Confidentiality）、完全性（Integrity）および可用性（Availability）をバランス良く維持し改善することとされており、単に情報漏洩（機密性の喪失）を防止するだけでなく、情報の改竄や消失、あるいは利用停止といった事態から、効率的かつ有効に情報を保護することをマネジメント・システムとして行うことが要求されている（石井秀明「ISMS・プライバシーマーク認証取得の現場から」『企業リスク』第２巻第１号（通巻第５号）、トーマツ企業リスク研究所、2004年、23頁）。

⑸ 例えば、６ヶ月以内に消去されるものは、保有個人データに該当しない個人データとされ、開示等の義務が課されない（施行令４条）ことから不要なデータはできるだけ６ヶ月以内に消去するように保有期間を事務所内規定で定めることによって、個人情報保護法違反のリスクを回避することも重要である。

⑹ 例えば、通勤途中の紛失事故の内、飲酒後の事故が多いことから事務所内ルールに従って持ち帰る場合にも、厳格なルール作りが必要である。

⑺ 国民生活センターの「個人情報流出事故に関する事業者調査結果」の調査対象は、「内閣衆質159号第120号個人データ流失に関する質問に対する答弁書」の別表4および新聞社告をもとに抽出した94社で、調査時期は2004年12月～2005年１月である。回収数（回収率）は50社（53.2%）、内有効回答数は44社（46.8%）である。ただし、１社で２件の事故を回答した事業者もあったため、合計45件の事故について分析したものである。

⑻ 日本商工会議所の個人情報漏洩賠償責任保険制度は、全国524商工会議所の会員企業を加入資格者に、補償期間を2005年３月１日より１年間として、国内損害保険会社12社（2005年３月末現在）が保険を引受けるものである。保険契約形態は、日本商工会議所と引受保険会社で保険契約を締結する形となる。保険金支払対象となるのは、

商工会議所会員企業が所有・使用・管理する（していた）個人情報が漏洩し、保険期間中に、法律上の損害賠償責任を負担することによって被る損害賠償金や訴訟費用などの賠償損害、および事故解決のために要した法律相談費用、事故対応費用、広告宣伝活動費用、コンサルティング費用、見舞金・見舞品購入費用などの費用損害となる。また、オプションとして、コンピュータ・ウイルスの感染による他人に対する損害など情報システム・ネットワークに関連する事故による損害を対象とすることも可能である（http://www.jcci.or.jp/sangyo/rouei-hoken/sub_win.html）。

⑼ 個人情報漏洩対応の保険は、損害保険各社がこれを取り扱っているが、具体例として、本稿では日本興亜損害保険社の「個人情報漏洩対応保険」（個人情報漏洩危険担保特約条項・個人情報漏洩対応費用担保特約条項付き総合賠償責任保険）の概要を説明することとする。なお、この保険の名称は損害保険会社により異なることがある。例えば、AIU保険社や東京海上日動火災保険社は「個人情報漏洩保険」、損害保険ジャパン社は「個人情報取扱事業者保険」、三井住友海上火災保険社は「個人情報漏洩事故対策保険」（個人情報プロテクター）などとなっているが、基本的な補償内容については大きな差異はない。

⑽ 本保険でいう「個人情報」とは生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日、その他の記述等により特定の個人を識別することができるものをいい、被保険者（会社）の役員、使用人等の個人情報は含まない。

⑾ 公（広）告費用とは、事故の状況説明、信頼回復のための広告掲載等を行うのに要する費用等をいう。例えば、事故の事実公表や謝罪のための社告、業務再開を公告するための社告等である。

⑿ コンサルティング費用とは、事故の事実についての確認または調査を行うため、または事故対応の方法を策定するために起用したコンサルタントに支払うべき手数料および費用をいい、法律事務所または弁護士に支払う法律相談費用を含む。

⒀ 臨時対応費用とは、事故対応のために記名被保険者が支出する臨時雇入費用、使用人に対して支払う超過勤務手当、交通費および宿泊費用をいう。

⒁ 契約例および保険金支払例は、日本興亜損害保険社の「個人情報漏洩対応保険のご案内」〈2004年11月版〉より引用した。なお、保険金支払限度額その他補償内容は、損害保険会社により異なる。

⒂ ④に対しては、追加保険料が支払われることにより保険の対象とすることができる。ただし、

当該使用人等または個人情報共同利用者等に対しては損害保険会社から求償を行う。

参考文献

⑴ AIU社「個人情報漏洩保険」（2004年）ホームページ：http://www.actfor.co.jp/AIU/johorei/joho_top.htm

⑵ 受川忠広「個人情報保護法の解説と企業が取るべき対応」『RMFOCUS』第８号、三井住友海上火災保険社・インターリスク総研、2005年、９頁。

⑶ 岡村久道『個人情報保護法』商事法務、2004年。

⑷ 経済法令研究会編『金融機関のための個人情報保護コース』（第１分冊および第２分冊）経済法令研究会、2004年。

⑸ 国民生活センター「個人情報流出事故に関する事業者調査結果」2005年３月25日。

⑹ 損害保険ジャパン社「個人情報取扱事業者保険のご案内」2004年。

⑺ 田島正広『個人情報保護法と金融機関』経済法令研究会、2004年。

⑻ 谷口博一「情報漏洩事件の原因究明の現場から」『企業リスク』第２巻第１号（通巻第５号），トーマツ企業リスク研究所、2004年、28－32頁。

⑼ 日新火災海上保険社「Safety Information」vol. 65、2005年。

⑽ NPO日本ネットワークセキュリティ協会「2003年度情報セキュリティインシデントに関する調査報告書」2004年３月31日。（注）なお、同協会の算出モデルによると、2003年における個人情報漏洩事件の被害賠償額は総額280億6,936万円で、１件当たりの平均損害賠償額は５億5,038万円である。情報漏洩の被害者全員が、損害賠償訴訟を起こすとは限らないが、損害賠償金額および情報漏洩事件によるブランドイメージの低下等による売上げに対する影響を考慮すれば、情報漏洩を未然に防ぐためにセキュリティ面へ投資することが必要であることがわかる。

⑾ 日本興亜損害保険社『個人情報保護法に関するガイドラインの解説と企業の実務対応～経済産業分野~』2005年。

⑿ 日本プライバシーコンサルタント協会編『個人情報保護体制は万全かープライバシーコンサルタントによる体制構築のための処方箋―』ぎょうせい、2004年。

⒀ 三井住友海上火災保険社「個人情報プロテクターのご案内」2004年。

⒁ 森山満『顧客情報漏えいの予防プログラム』商事法務、2004年。

⒂ 脇田一郎「個人情報保護とリスク・マネジメント」『企業リスク』第２巻第１号（通巻第５号）、トーマツ企業リスク研究所、2004年、18頁。

⒃ 渡部喬一『個人情報保護法のしくみと実務対策』日本実業出版社、2004年。