TRC EYE Vol. 91

東京海上日動リスクコンサルティング（株）
情報グループ
主席研究員　　近森　健三

個人情報保護対策とリスクコントロール

第５回　リスクマネジメントと保険（最終回）

■リスクマネジメントの重要性

リスクマネジメントの国内規格である「JIS Q 2001」が策定されたのは今から約４年前であるが、当時から比べても「リスクマネジメント」という言葉がより一般的に使われるようになった感がある。この間、日本経済においては実質ＧＤＰの成長率はマイナスからプラスに転じ、不良債権の処理が進み、株式市場も底を打って上昇局面となり、史上最高益を達成する企業も続出している。一方で、大規模な震災や風水害の発生、ＢＳＥや新種ウィルスの発現、爆破テロ、企業会計不正、リコール、列車事故、アスベスト、詐欺事件や不祥事、そして個人情報の漏洩など、社会の安全・安心を脅かす事件・事故が国内外において絶えない。被害の程度や質がかなり深刻・悪質であるケースも多く、社会全体がリスクに対しより敏感になっている。企業にとっては、このような状況下においてリスク管理を一歩間違えると相当の打撃を受け、企業の存続をも脅かされることにもなりかねない。事業活動において収益とリスクが表裏一体である以上、事業活動に伴うリスクを認識し適切に管理すること、すなわちリスクマネジメントが極めて重要となる。

■リスクマネジメントとは

前述した「JIS Q 2001」によると、リスクマネジメントとは、「リスクに関して、組織を指導し管理する、調整された活動」であり、「一般的にリスク算定、リスク評価、リスク対応、リスク受容およびリスクコミュニケーションを含む」とされている。つまり、事業活動に伴うリスクを認識し、そのリスクが企業や組織にもたらす影響を評価したうえで、そのリスクへの対応策つまりリスクを取る（＝受容する）か取らないのかの判断、リスクを取る場合にはリスクの発生を減少させるための管理策を講じる。そして最も重要であるのは、この活動を一過性のものに終わらせるのではなく、常に経営層が評価・見直しを行い、継続的な改善を行うことである。この点については、本メルマガの第１回以降、折に触れて述べている通りである。

リスク対応の方法としては、「保有」、「低減」、「回避」、「移転」の４つの手段がある。そして、リスクの発生頻度とその損失規模の程度との兼ね合いで、取

るべき対応手段を選択する。高頻度かつ大規模なリスクについては極力「回避」、つまり事業から撤退すべきである。しかし、それができない場合は、損失規模と発生頻度の「低減」策を講じなければならない。高頻度だが比較的小規模なリスクについても「低減」が有効である。低頻度だが大規模なリスクについては損失規模の「低減」とともに、第三者にリスクを「移転」することが考えられる。この「移転」の代表的な方法が「保険」である。低頻度かつ小規模のリスクについては、「低減」や「移転」などの対策を講じたとしても、一定レベル以上はコストに見合うだけの損失低下が期待できない場合が多い。この場合は、特別な対策は取らずにリスクを「保有」し、万が一の発生に備えた対応のみ準備しておく。

■個人情報保護におけるリスクマネジメント

個人情報保護におけるリスクには、不正な情報取得、目的外利用など様々考えられるが、やはり最も留意すべきものは、個人情報の漏洩リスクであろう。第１回でも触れたが個人情報漏洩事故の発生件数は一向に減少する気配がない。個人情報漏洩事故は単なるプライバシー侵害に留まらず、オレオレ詐欺やクレジットカード詐欺、或いは幼児誘拐などの経済的被害や刑事事件に発展し、金銭的な損害賠償のみならず人命に係る恐れもある。従って、個人情報を取扱う企業や組織は、細心の注意をもって個人情報を管理することが求められている。

その際、リスクマネジメントの考え方が有効となる。具体的には、個人情報を取扱う業務について、業務フローを分析したうえでリスク要因を特定する。個人情報の取得から始まって、入力・加工、保管・保存、移送・送信、利用・提供、外部委託、廃棄・消去まで、個人情報のライフサイクルに従って、どのようなリスクがあるかを分析する。例えば、不正な情報を取得するリスク、不適切な保管のリスク、持ち出しのリスク、誤送信のリスク、誤廃棄のリスクなどが考えられる。次に、それらのリスクの発生頻度と影響の度合いを評価し、どのような対策を講じれば有効であるか――二重チェック、事前承認、台帳への記録、施錠管理、入退室管理、暗号化、持出禁止、ログの取得等々――を検討し、具体的かつ合理的な対策を講じる。そしてそれらの対策が実際に守られているか、効果的であるかどうかを常に点検し、必要に応じて見直しを実施する。

■個人情報保護漏洩リスクと保険

先に述べた通り、リスクへの対応方法の一つである「移転」において、最も一般的な手法が「保険」である。つまり、万が一個人情報漏洩事故が発生した場合において発生する種々の損失について、第三者である保険会社に一定程度転嫁する仕組みであり、保険会社各社から個人情報漏洩事故に特化した商品が提供されている。

実は、業務中に発生した個人情報漏洩によって本人の権利（プライバシー権など）を侵害し、結果的に法律上の損害賠償（慰謝料）を負担しなければなら

なくなった場合、この費用損害（賠償金や応訴費用）を補償する保険、いわゆる賠償責任保険は個人情報保護法の施行前から存在していた。ただし、対象業務が特定されていたり、使用人の悪意の情報持ち出し行為などが対象外（免責事項）になっていたりと限定的な内容となっているケースがあった。特に、後者の免責事項に関しては個人情報漏洩の大きな要因のひとつである従業員の故意による漏洩事件を対象外とするものでもあり、実質的には余り有益な保険ではなかったと言える。しかし従業員による個人情報漏洩事件が社会的な大きな問題として取り上げられるようになり、個人情報漏洩が普遍的なリスクとしてとらえられるようになると、こうした使用人の不正行為リスクなどの保険ヘッジニーズが顕在化してきた。そこで、個人情報漏洩リスクに特化し、あらゆる業務を対象として、使用人の不正行為も免責事項としない個人情報漏洩保険が開発されることになった。現在では、損害金の賠償や弁護士費用などに加えて、謝罪広告・会見費用、お詫び状の作成・発送費用、見舞金・見舞品購入費用、そして再発を防止するためのコンサルティング費用や個人からの問い合わせに対応するためのコールセンター費用などの関連費用もカバーできる商品もあるようだ。取扱う個人情報の種類と規模によっては、このような保険商品の活用も検討しておきたい。

■最後に

これまで５回にわたり、「個人情報保護対策とリスクコントロール」と題して個人情報保護に係るいくつかのテーマについて縷々述べてきた。我が国の現状を見るに、「個人情報保護法」の本格施行を前に有り合わせの対応を行って何とか２００５年４月１日を迎えたものの、実際の具体的な対策や定着化はまだまだこれからというところが多い。しかし一方では、個人の意識は確実に高まっており、また、被害も相次いで発生しているという事実がある。政府・自治体や企業にとっては、個人情報保護を図ることは社会的責任の一環であり、一人一人が安心して暮らせるよう、日々の改善が求められている。本メルマガがわずかでもその取り組みの参考となれば幸いである。最後に、紙幅の関係もあり、言葉足らずな点も多々あったと思うが、ご容赦頂ければと思う。

出典：特定非営利活動法人ネットワークリスクマネジメント協会発行
NRAメールマガジン『啓・警・契』第１０９号
URL：http://www.nra-npo.jp/

（第 91 号　2006 年 1 月発行）

