TRC EYE Vol. 87

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１回　個人情報保護を取り巻くリスクと対策のポイント

■減少しない個人情報漏洩事件

個人情報保護法が本格的に施行された２００５年４月１日以降も個人情報漏洩事件は一向に減る傾向にはない。政府・監督当局の指導もあり、これまで内部で処理していた漏洩事件についても、新聞やホームページにおいて外部公表をしていることが件数を押し上げているとも思えるが、例えば、行政機関における個人情報漏洩事故の件数（新聞等への発表ベース）は、２００４年１０月から２００５年３月までの半年間では２４件、２００５年４月から８月の５ヶ月間で４３件となっている。仮に積極的開示という背景を考慮しても、昨年を上回るペースで個人情報漏洩事件が発生していることになる。一事件あたりの漏洩件数についても１万件以上の個人情報が漏洩した事例(不明分を除く)は、同様の期間の比較で、1件から４件に増加している。(尚、行政機関を含む全体では、同様の期間の比較で、総件数は１２６件から１９２件となっている。以上筆者調べ。)

行政機関や企業においては、２００５年４月１日をXデーとして、それこそ駆け込みでの対応を行った例も多いのではないだろうか。筆者は、情報セキュリティマネジメントのコンサルティングを実施しているが、個人情報保護に関しては、「とにかく２００５年３月中に形だけでも何とかしたい。」という声を良く耳にした。当初、２００３年５月に個人情報保護法が交付された時点においては、法律の条文だけでは趣旨は理解できるが具体的には何をすれば良いのかが必ずしも明らかではなかった面もある。このため、行政や企業等の実務者の対応は、関係各省庁からガイドラインや実務指針が出され始めた２００４年９～１０月頃より本格的に開始されたところも多い。そして、４月１日までの約半年間は、ガイドラインや実務指針の要求事項に即した内部規程を策定するという作業に追われ、従業者への周知、ルールの徹底、内部でのチェック体制の構築まで手が回らなかったというのが実態ではないだろうか。その事が、個人情報漏洩事件の多発につながっていると考えられる。

■個人情報漏洩事件の発生原因

行政機関における情報漏洩の場合、２００５年４月～８月の４３件についての発生原因をみると、管理不備等による紛失が１０件、文書の誤廃棄・記憶媒体の消去漏れ等の廃棄に係るものが８件、車上あらしが５件、郵送・メール・ファックス等の誤送付が５件、ウィルスやファイル交換ソフト「Winny」に起因するものが４件、内部者の無許可持ち出し・不正使用等が４件、盗難が４件、外部からの不正アクセスが２件、外部委託先での管理不備が１件となっている。このように個人情報漏洩の発生原因は様々ではあるが、実は従業者の不注意に起因するものが多い。この例でも、盗難や不正アクセスなどの外的な要因によるものは少なく、管理不備による紛失、誤廃棄、無許可持ち出し、誤送付・誤送信や車上あらしなど、個人情報を取扱う者が十分に注意していれば防ぐことができたものが大多数を占めている。この傾向は、民間の企業でも同様である。この他、これは行政機関の事例ではないが、４月以降個人情報保護法に則った開示請求を受けた際に、定められた手続きに従って処理をしたにも係らず、他人の情報を誤って開示してしまったという事例もある。個人情報を管理しているシステムや事務所に対して、外部からの不正侵入等を防御するための対策を怠ってはならないのはもちろんであるが、実際には、内部の日常業務の中に情報漏洩のリスクが多く潜んでおり、少しでも気を許すと事件につながるというのが現実である。

■厳格な内部ルールとの現実とのギャップ

考えてみると、個人情報保護についての基本方針を定め、責任体制も定め、現場での管理者も設置し、種々の規程類も作成したはずである。個人情報の洗い出しも行い、全ての取り扱い手順について適切な個人情報保護が図れるよう、ルールも整備しているはずである。しかしこのルールが遵守できない事例が発生してしまうのは何故であろうか。

ひとつには、ルール自体に問題があるということが考えられる。個人情報保護法やガイドラインの定めることをそのまま規程に反映しても、実務における個人情報の取得・加工・利用・提供・委託・送付・保管・廃棄等の一連の業務フローに即していなければかえって使いづらものとなり、結果的に、普段の動作として身に付かない恐れがある。また、人間心理としては、自分が漏洩事件を引き起こしてしまうという最悪の事態が発生することを無意識に思考回路から外し、「少しくらい（今日だけ、今だけ）守らなくても大丈夫だ。」という根拠のない安心感から不用意な取り扱いをしがちであり、適切なルールがあっても機能しないという側面もある。さらに、組織内においては日々新たな業務が発生し、業務の流れが変わり、人の入れ替わりもある。個人情報を取り巻く環境の変化に応じて、そこに潜むリスクも変化し、気が付かないうちに内部ルールと現実とのギャップが拡大することもある。このようなギャップは完全に埋めることは困難であるが、少しでも小さくすることは可能である。

■個人情報保護のためのポイント

個人情報保護をより確実なものとするためには、内部のルールをいかに実際の業務に即したものとするか、それをいかに徹底していくか、そして日々変化するリスクにいかに追随し対応するか、ということがポイントとなる。このためには、日々の点検と教育、監査、見直しというプロセスが特に重要となる。また、この点は自組織内のみならず外部委託先に対しても同様であるが、自組織のコントロールが当然には直接及ばない外部委託先に対しては、実効性を担保するため工夫が必要となる。また、種々の策を講じたとしても、不幸にも漏洩事故が発生する場合がある。事故が発生した場合には、個人情報の保護を図るために、いかに早く適切な対応を行い被害の拡大を食い止めるかも重要である。そして、個人情報保護のための内部統制の仕組みが新たなリスクに対応できるようにするためには、常にリスクを認識し、評価し、対策を見直すというリスクマネジメントの考え方が有効となる。

第２回以降は、「教育・監査」「外部委託先の管理」「漏洩時の対応」「リスクマネジメントと保険」というテーマを取り上げながら、個人情報保護対策とリスクコントロールについて考えてみたい。

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１０５号
URL：http://www.nra-npo.jp/

（第 87 号　2006 年 1 月発行）

