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４回　個人情報漏洩時の対応

■事故発生を想定した対策

ミスや事故というものはどれだけ注意していたとしても完全には防ぐことができない。最も陥りがちであるのは、「事故はあってはならない。」という意識が強すぎて現実を直視せず、事故への対応が遅れることである。実際に事故が起きた際に、これは事故ではないと解釈したり、事故を隠そうとしたりすると、結局は被害が拡大してしまうことになる。「事故は起きるものである。」と想定し、万が一の場合に適切な対応がとれるよう備えておくことが重要である。そのためには、事故の早期発見のための事前準備策、発生後の二次被害防止と早期沈静化のための緊急時対応、そして類似の事故の再発を防ぐための再発防止策の３つ観点から考えると良い。

■事故対応の事前準備策について

事故対応において何よりも重要なのは早期発見・早期対応ができるための仕組み作りである。個人情報漏洩対応というと、損害賠償や謝罪文等のことを考えがちであるが、火事や盗難などと同じように、まずは発生の事実を早期に検知することが被害拡大防止の第一歩である。そのためには、情報システムへの不審なアクセス・操作を検知するツールの導入等システム的な対策に加え、①何が個人情報漏洩に該当するのかの判断基準の明確化や、②発見した際の連絡方法の明確化など、運用面のルール整備も必要となる。

①判断基準について

故意に事故やミスを隠そうとしなくても、例えば、取引先の情報を入れていた USB メモリが１週間見当たらない場合や、お客様から情報が漏れているのではないかという問い合わせの電話があった場合について、当事者が「事故に該当しないだろう。」と勝手に判断してその事実を放置していると対応が遅れる可能性がある。法律やガイドライン上では個人情報の定義は規定されているが、何が漏洩事故に該当するのかについてまでは明記されていないため、各人の判断がまちまちとなる恐れがある。従って、どのような事実が漏洩事故や漏洩事故の兆候であるのかについて予め定めておく必要がある。例えば、以下のような事象が考えられる。

 ©東京海上日動リスクコンサルティング株式会社　2006

・ 顧客や社外より、個人情報が流出している、インターネット上でアクセス可能な状態になっている等の問い合わせを受けた。
・ 個人情報を含む書類、媒体、パソコン等を紛失した。
・ 個人情報を含む書類、媒体、パソコン等が盗難にあった。
・ 個人情報を含む書類、媒体、パソコンに不審者がアクセスした形跡があった。
・ 個人情報を含む業務システム、サーバ等へ不正アクセスの履歴があった。
・ 個人情報へのアクセスを制御する部屋・キャビネット・机などの鍵、権限者のＩＤ・パスワード、身分証明書等が紛失・盗難にあった。
・ 報道機関、監督官庁、捜査当局などから個人情報漏洩に関する問い合わせを受けた。
・ 組織内より、個人情報が漏洩している、不適切に取り扱われているとの通報を受けた。
・ インターネット掲示板等に、個人情報漏洩に関するうわさ等の書き込みがあることを発見した。
・ 自組織保有のものと思われる個人情報が名簿業者やインターネットで売買されていることを発見した。
・ 自組織保有のものと思われる個人情報を保有しているという不審な連絡を受けた。
・ 委託事業者や取引先より同様の事案が発生した旨、報告を受けた。

②連絡方法について

上記のような事象を検知した場合、担当者レベルで安易に対応するのではなく、確実に個人情報の管理責任者に伝える必要がある。従って、直属の情報管理責任者が不在の場合に備えて、所定の代行者などの緊急連絡先も定めておくと良い。その際、確認すべき事項の漏れを防ぎ、事故管理を確実に実施するために、専用の報告書様式を定めておく方が良い。もちろん、事象発生時には迅速な対応が求められるため、まずは電話やメール等で第一報を行ったうえで、後で報告書に記載し回付すればよい。

■緊急時対応について

情報漏洩事故や事故の恐れがある事象が発生した場合、まず行うべきは被害拡大の防止である。この際、原因究明や責任問題に関心が行きがちであるが、自組織の立場で考えるのではなく、あくまでも顧客サイド被害者サイドの視点に立った対応が求められる。事実関係をまず押さえ、影響度合いを見極めた上で、被害者の被害拡大の防止策を最優先に行う。特に、件数が多い場合、経済的被害が発生している場合もしくはその恐れがある場合、法令違反の恐れがある場合などは、全組織的な緊急対応が必要である。具体的には、以下のような対応を実施する。

① 対応体制の立ち上げ
・ 関係者および業務、事務、ＩＴに詳しい専門家（社内社外とも）の召集
・ 調査委員会の発足

 ©東京海上日動リスクコンサルティング株式会社 2006

② 事実関係の調査、証拠保全
・ 漏洩日時、漏洩した情報・件数、漏洩先、漏洩の形態・方法、漏洩原因、二次被害の可能性および発生状況等の事実確認
・ 入退出記録、アクセスログなどの証拠保全
③ 社外関係機関との連携
・ 所管官庁、所轄警察などへの報告
・ ハイテク犯罪の場合、コンピュータ緊急対応センター（ＪＰＣＥＲＴ）、情報処理振興事業協会（ＩＰＡ）への報告
・ 顧問弁護士への報告、相談
④ 拡大防止対策の実施
・ 個人情報の流出該当者などへの連絡、臨時問い合わせ窓口の設置
・ 被害拡大防止措置（例えばネット掲示板に掲載されている個人情報の削除等）
⑤ メディア対応
・ ホームページによる経緯および調査結果の逐次公表
・ ニュースリリース、記者会見などによる経緯および調査結果の逐次公表
・ お詫び広告（社告）
・ 従業員への情報の共有化
⑥ 事後対応
・ 被害者からの損害賠償請求対応
・ 被害者に対する見舞金　　など

事故が発生した場合、いかに素早く、誠実に、透明性のある対応ができるかどうかが重要である。適切な対応を行うことができれば、架空請求などの二次被害を食い止めることができ、信用の失墜を最小限にとどめることができるが、逆に対応に失敗すると、本人の被る被害が拡大し、組織全体の信用を大きく損なうことにもなりかねない。

■再発防止策について

緊急時対応が落ち着いた時点で、類似の事故の再発を防止するための対策を検討し実施する。その際、事故発生の直接的な原因のみならず、根本的な原因まで調査したうえで対策を講じる必要がある。例えば、委託先が原因で事故が発生した場合、当該委託先への改善要求や契約解除などにとどまるのではなく、委託先業務全般について、選定基準の見直しや管理状況の点検、監督方法の見直しも実施する。さらに、組織内の従業員に対して、社内規程やルールの変更箇所について、その趣旨や内容について徹底すべく再教育を実施する。局所的、場当たり的な対応にとどまるのではなく、抜本的、徹底的な対策を講じることが重要である。

また、大事には至らなかったミスやトラブルが発生した場合においても、この再発防止策を十分に検討し確実に実施しておくことが重要である。その積み重ねが、より大きな事故の発生防止につながる。

 ©東京海上日動リスクコンサルティング株式会社　2006

最終回（第五回）は、リスクマネジメントと保険というテーマを取り上げたい。

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108号
URL：http://www.nra-npo.jp/

□ 本文は、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の許可を得て、原文のまま掲載しています。他への転載や二次使用には本協会の承諾が必要です。

（第 90 号　2006 年 1 月発行）

 ©東京海上日動リスクコンサルティング株式会社　2006