内部統制と個人情報漏えいリスク

個人情報保護監査研究会　蓮見節夫（会員 no.9）

１．内部統制規準における個人情報漏えいリスクの位置づけ

経営者が企業を経営するに当って内部統制が必要であることは、経営のイロハのようなものですが、法的責任について明確にされたのは 2000 年９月に示された大和銀行事件への大阪地裁判決によります。経営者は、従業員のすべての行為を見張っていることはできないので、従業員が不正を起こさないよう、又不正が行われた場合、早く発見し対処できるよう、健全な会社経営が営む事業の規模、特性に応じたリスク管理体制（いわゆる内部統制システム）を構築しなければいけないということが示されました。

その後も財務報告にからむ不正事件がいくつか発覚し、2007 年２月に企業会計審議会から「財務報告に係る内部統制の評価及び監査に関する実施規準の設定について（意見書)」（以下、略して「内部統制規準」とする）が公表されました。

内部統制規準は、「Ⅰ内部統制の基本的枠組み」「Ⅱ財務報告に係る内部統制の評価及び報告」「Ⅲ財務報告に係る内部統制の監査」の３部から構成されています。

内部統制の基本的枠組みでは、内部統制は、基本的に、企業等の４つの目的（①業務の有効性及び効率性、②財務報告の信頼性、③事業活動に関わる法令等の遵守、④資産の保全）の達成のために企業内のすべての者によって遂行されるプロセスであり、６つの基本的要素（①統制環境、②リスクの評価と対応、③統制活動、④情報と伝達、⑤モニタリング、⑥ＩＴへの対応）から構成されています。

今、問題にしようとしている個人情報漏えいリスクは、基本的要素の一つである「リスクの評価と対応」の中に位置づけられるリスクの一つです。もちろん、他の要素とも関連を持ちます。

２．個人情報の情報資産としての価値

多数の個人情報を扱う事業者は、個人情報漏えいリスクを常に背負っています。2005 年４月に全面施行された個人情報保護法においても、個人情報取扱事業者の義務を定めています。法的にも、個人情報の取扱いにおける安全管理義務、従業員への監督責任、委託先の監督責任などの義務を負っていることを知らなければなりません。

個人情報の資産価値はどの程度のものでしょうか。過去の判例では、宇治市住民基本台帳漏えい事件で、宇治市の外部委託先への監督責任が問われ、１人につき１万 5000 円（慰謝料１万円＋弁護士費用 5000 円）の損害賠償が課されました。平成 19 年５月の大阪地方裁判所では、Yahoo!BB の顧客情報流出事件で BB テクノロジーに対して、１人につき 6000 円（慰謝料 5000 円＋弁護士費用 1000 円）の支払いを命じました。別に、ソフトバンク BB は、Yahoo!BB 全会員に金券 500 円を配り謝罪しています。

仮に１件２万円の価値とすると、10 万件の個人情報があれば、20 億円となります。当然、

個人情報も、信用情報や機微情報を含めば、その何倍もの情報資産価値を持つものとなります。

一人の営業マンが、自分の顧客情報 1000 件を持ち歩いたとすると、2000 万円の資産価値のものを持ち歩いていることになります。多くの人は、2000 万円の現金を持ち歩いた場合は、怖くて歩けなくなるのではないでしょうか。しかし、小さな磁気媒体に入ってしまうと、自分が 2000 万円の資産価値のあるものを持ち歩いていることに気が付かない事が多いのです。そこにリスクがあります。

３．個人情報漏えいのリスク対策

個人情報漏えいのリスク対策としては、内部統制の仕組みを考える場合、プライバシーマーク認定取得を考えるのが一番手っ取り早い方法といえます。プライバシーマーク制度は、「JIS Q 15001 個人情報保護マネジメントシステムー要求事項」に基づいて、マネジメントシステムを整備し運用されていることを審査し認定するものです。

「JIS Q 15001 個人情報保護マネジメントシステムー要求事項」はマネジメントシステムの一つでもあり、Plan,Do,Check,Act のマネジメントサイクルを廻します。組織体制としては、個人情報保護管理者や個人情報保護監査責任者を任命します。運用面では、個人情報の特定、個人情報取得時の利用目的の明示と本人の同意、特定した個人情報の取扱いの流れに沿ったリスク分析、リスクに対する適切な安全対策の実施、従業者の監督と教育、委託先の監督、日常点検、などが必要です。

これらの結果として、リスクが許容範囲に抑えられ、漏えい問題等を起こさない状態にあれば、個人情報漏えいリスクに対する内部統制としては、合格と言えるでしょう。