企業に求められる情報セキュリティマネジメント

東京海上リスクコンサルティング㈱ リスクコンサルティング室 情報グループ
主任研究員 脇田 修二

企業において情報セキュリティの重要性が取り上げられるようになって久しいが、インターネット上のWebサイト改ざん、重要な情報システムのトラブル、関係者による情報の漏洩など、情報に関わるトラブルは未だ後を絶たない。一方で、企業が取り扱う情報は多様化、増加の一途を辿り、情報はいまや企業の活動に欠かせない経営資源の一つとなっている。同時に、情報に関するリスクも無視できない重大な存在となり、その顕在化は事業に致命的な影響を与えかねない。残念ながら、このような情報に対しても適切な保護管理がなされている企業は多くはなく、情報に関わるリスク対応の見直しが求められている。

企業が保護すべき情報とは

企業が保護すべき情報として最初に考えられるのが、顧客データベースや電子メールといった電子的な情報である。しかし、企業で取り扱われる情報は、紙に記録されることもあれば、印刷物として複製されることもあり、時には会話や噂として伝達される場合もある。これら電子的ではない情報も、企業にとって価値ある情報であれば保護しなければならない。情報の定義については意見の分かれるところだが、本稿では、紙、記憶、電子媒体など形態を問わず企業が価値を認める情報全般及びこれら情報の活用を補助するシステムやネットワークなどを「情報資産」と定義し、企業が保護すべき対象とする。

情報セキュリティの目的

情報セキュリティと言えば、クラッカー(ハッカー)と呼ばれる悪意ある第三者から情報システムを防御するための、ファイアウォールやウイルス対策のような技術的な対策との考えが未だ根強い。しかし、防衛は情報セキュリティの目的の一部にすぎない。

情報セキュリティに関する基本的なガイドラインである「ISO/IEC 17799」及び「JIS X 5080」では、情報セキュリティを「情報の機密性(Confidentiality)、完全性(Integrity)、可用性(Availability)を維持すること」と定めている。ここで、機密性、完全性、可用性は、そのアルファベットの頭文字からC.I.A.と略されることもあり、それぞれの意味は次のように定義されている。

- ●機密性…アクセスを認可された者だけが情報にアクセスできることを確実にすること
- ●完全性…情報及び処理方法が、正確であること及び完全であることを保護すること
- ●可用性…認可された利用者が、必要な時に、情報及び関連する資産にアクセスすることを確実にすること

つまり、情報セキュリティの目的は「利用を許可された者が(機密性)、矛盾なく正しい情報を(完全性)、利用したい時に利用できる(可用性)」環境を整備することであり、その結果情報資産を最大限に活用することが可能となるのである。

情報セキュリティマネジメント

企業の情報資産を取り巻く環境は流動的であり、事業方針の転換や法制度の変更、新たな技術や脅威の出現などにより、情報セキュリティに対する要求は常に変化している。したがって、一度構築された情報セキュリティ環境は、時間の経過と共にその効力が失われていくと考えられる。

そこで、情報セキュリティマネジメントシステム(ISMS)の構築により情報セキュリティを管理する体制を確立し、さらに図1に示すようないわゆるPDCA(Plan／Do／Check／Act)マネジメントサイクルの運用を通して情報セキュリティの継続的改善を実現することが望まれる。そして、ISMSを導入する目的は情報セキュリティの向上に止まらず、情報セキュリティを継続的に維持、改善できる組織体制の整備であり、ひいてはコーポレートガバナンス(企業統治)を確立することである。このような目的を認識した上で、企業における事業上のリスクを極小化する一連の統制がISMSなのである。

ISMSにおける情報リスクマネジメント

ISMSにより企業における事業リ

スクを極小化する上で重要となるプロセスが、情報リスクマネジメントである。情報リスクマネジメントは、情報資産に関するリスクの企業経営に与える影響を把握し、リスクがもたらす損失の極小化を図るもので、企業経営に対する影響の重大なリスクを合理的かつ経済的に管理するための経営管理手法である。つまり、企業にとってリスクが大きいと判断された情報資産に対して優先的に投資を行うことで、企業全体のリスクの総和を効率的に低減することが可能となる。

実際の情報リスクマネジメントは、具体的に次のような手順で実施される。

(1)情報資産の識別及び評価

企業の保有する情報資産を洗い出し、それぞれに資産価値を割り当てる。これらの価値は組織のビジネスに基づく資産の重要度であり、リスクの判定における重要な要因となる。例えば、顧客リストなどはビジネスが大きく依存する価値の高い情報資産だが、一般に配布されるパンフレットなどの資産価値は比較的低いと判断できる。

(2)リスク評価

リスクアセスメントとも呼ばれ、特に価値の高い情報資産に対して、①脅威の想定、②脆弱性の洗い出し、③資産価値に基づいた損失の想定を行い、リスクを評価する。図2に、顧客リストを対象としたリスク評価を例示する。リスク評価の手法は数多く開発されているが、全ての企業に適用できるような確立された手法は存在していない。従って、実際にリスク評価を実施する際には、これらの手法を比較検討の上、業務に応じてカスタマイズすべきである。

(3)リスク対応

リスク評価で識別されたリスクに対して、リスクの大きさと予算を考慮しながら適切な対応方法を決定する。リスクへの対応には、リスク保有、リスク移転、リスク回避、リスク低減の4つの方法がある。リスク保有は、リスクの存在を認識するが、特に対策を講じることなく財務上自己負担する資金的対策で、事業に対する影響が極めて小さいリスクなどに適用される。リスク移転は、保険会社などの第三者に資金的なリスクを移転する方法であり、自然災害や火災などある水準以上の対策に大きな投資が必要となるリスクに対して適用される。リスク回避は、リスク発生の要因を排除する方法である。例えば、ある業務の手順にリスクの存在を認識したが合理的な対策が見当たらない場合に、手順そのものを実施しないといった対応がこれに該当する。リスク低減は、4つの対応方法の中で最も優先されるべきものであり、リスクが顕在化しないように予防的な対策、または顕在化してもその損害を最小限に抑えるための対策を講じる方法である。一般的な情報セキュリティ対策は、リスク低減に該当する。

(4)結果の評価、見直し

リスク対応の効果を評価し、予想通りの結果が得られていなければ見直しを実施する。また、情報資産の価値、脅威、脆弱性といったリスク決定の要因は流動的に変化するため、定期的に評価、見直しを実施することで、適切な情報リスクマネジメントを維持する。

このように、情報リスクマネジメントは個別の情報セキュリティ対策の集合ではなく、経営判断に基づく企業全体の情報リスクの管理であるため、その活動には経営トップの参画が不可欠である。

まとめ

冒頭述べたように、情報セキュリティの必要性は認識されながらも、実効力のある情報セキュリティマネジメントを実践している企業は未だ多くない。その理由のひとつに、情報セキュリティに対する投資の効果が見えにくいことが挙げられる。しかし、これまで述べたようにISMSの導入が企業にもたらす恩恵は決して小さいものではない。また、企業の活動が情報資産に大きく依存する状況下での情報セキュリティを軽んじた経営は許されない。情報リスクが現実化して致命的な損害が発生した場合には、経営責任を問われることも考えられる。すなわち、適切なリスクマネジメントに基づく情報セキュリティマネジメントは企業における重要な経営課題であり、それゆえ経営者によりトップダウンで実施されるべきものなのである。

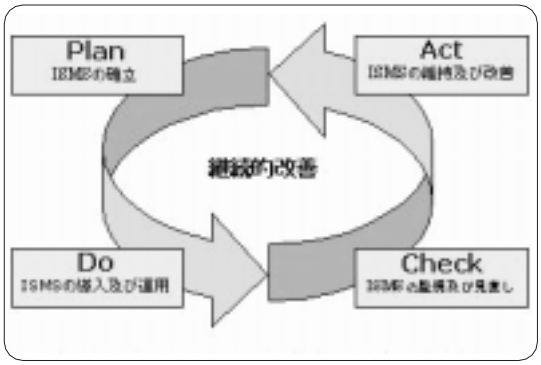

図1 PDCAマネジメントサイクルによるISMS の継続的改善
(c東京海上リスクコンサルティング㈱)

情報資産
顧客リスト

資産価値
◆業務に欠かせないデータで、漏洩すれば信用失墜や売上の低下などが発生 ◆個人情報であり、法的に保護が必要
脅　威
◆第三者による盗難 ◆職員による名簿業者への横流し
脆弱性
◆保管場所が施錠されていない ◆利用・持出しが記録されていない

↓

脅威が現実化する可能性が高く、その際の損失も大きい

↓

情報リスクが大きい

図2 顧客リストのリスク評価例
(c東京海上リスクコンサルティング㈱)

（安全と管理2003 7月号掲載）