

情報活用と情報管理

リスクは企業活動につきものである。相応のリスクをとり、これをマネジメントしていくことで経営は成り立つ。これを情報セキュリティマネジメントに当てはめると、企業に求められるものが情報セキュリティリスクへの防御だけではないことが浮かび上がってくる。このことについて情報セキュリティが対象とする「情報」に注目しながら整理していく。

リスクマネジメントと情報

リスクマネジメントは経営そのものである。一般に、リスクをとらない以上リターンも見込めないというのが習わしだ。企業価値の最大化と利益の創出というリターンを求める企業経営において投資はリスクであるし、多くの従業員を抱えることもまた、リスクである。

しかし、従業員を組織し、合理的な投資を行っていかなくては企業の発展は見込めないものであり、リスクをマネジメントしていくことなくして企業経営は成り立たないのである。

今日、情報の取り扱いに関するリスクは、企業が直面する重大な問題のひとつとして強く認識されるようになっていく。

世の中を騒がしている個人情報の漏えいは、見舞金、訴訟費用、広報費用、株価・格付けの下落といった、直接的コストを発生させるだけではない。カスタマーロイヤリティの失墜など、大きな痛手となって、長期にわたり企業に跳ね返る。

個人情報を例にとっただけでも、その取り扱い如何によって損失を招くことは明らかであるが、技術情報、合併や買収に関する情報な

ども、ひとたび漏えいや改ざんに遭えば、多大な損失をこうむることになる。こうした問題は、企業が扱う他の多くの情報にも共通である。

情報の取り扱いが企業の対峙するリスクのひとつであるからには、それへの対処についてもリスクマネジメントの枠組みで考えていくことが基本となる。

情報セキュリティマネジメントでは、企業の経営方針やセキュリティに関する基本方針に基づき、まず対象となる情報資産の洗い出しとリスクの評価を行う。その上で、対策内容を決定し、それぞれの対策を実施。その後、内部者による評価や時には外部からの監査を受け、問題点を明らかにする。そして、それを元に作成された改善案を用いて、再び情報資産の見直しから始まるマネジメントサイクルを継続運用していくことで、情報セキュリティ対策を網羅的で質の高いものにできる。

リスクコントロールとリスクファイナンス

リスク対策の実施には、リスクコントロールとリスクファイナンスがある。

まず、リスクコントロールはリスクの影響度を軽減もしくは発生頻度を抑制する対策であり、回避、予防・防止、移転に対策の性質



を分けられる（表1参
照）。

そして、リスクコン
トロールを行っても、
なお残存するリスクに
対して、資金的な用意
をしておくのがリスク
ファイナンスである。

リスクファイナンスには保有と保険が存在す
る。ちなみに、情報セキュリティ分野でも、
現在個人情報保護法に対応させた保険商品が
いくつか発売されている。

個人情報保護関連5法の全面施行を前に、
ほぼすべての事業者は、2005年4月までに何
らかの「安全措置」の構築を迫られている。
しかし、担当者は、「セキュリティ対策が業
務の利便性を阻害する」と、現場から不満の
声上がることを危惧している。

一般的に、セキュリティの強化は利便性の
低下を伴うイメージを抱かせる。このため、
実際に従来のシステムを利用した業務を変更
させないよう、とりあえず、2005年4月まで
の対策としてログ収集だけを実施したいと考
える担当者も少なくない。

しかし、個人情報の漏えいや改ざん防止を
おもな目的とするなら、ログ収集だけでは目
的を達しえないことは明かだ。いま、企業
は業務で情報を扱う上での利便性とセキュリ
ティ強化のバランス感覚をもった情報管理対
策を求められていると言えよう。

表1 情報セキュリティ分野でのリスクコントロール例

回避	必要以上の情報を収集・保有しない。
予防・防止	各種のセキュリティ対策 物理的対策（入退室管理、電源対策ほか） 技術的対策（H/Wの冗長化、暗号化、認証、ウィルス対策ほか） 人的対策（教育・啓蒙ほか） ※なお予防・防止の中には、分散と結合という考え方も含まれる。 災害時の可用性確保のためのデータセンターの分散は前者の例。
移転（保険以外）	開発委託業者と結ぶ契約における瑕疵担保責任条項は、契約によ る移転の例。先々のシステムトラブル発生可能性というリスクを 他社へ移転している。

リスクでありながら、積極的な活用が求 められる「情報」

たとえば、デジカメ、AV機器、PCなどの
分野においては、短いサイクルで次々に新モ
デルが投入される。そして、斬新なモデルを
投入する企業が現れると、他社もほぼ同時期
に同様の製品を市場に投入してくる。今日、
細かなクオリティの点で差はあったとして
も、機能的に大差ない製品を、他社がタイム
ラグなく製造できてしまうのである。

マーケットが成熟するなか、他社との差別
化は、ますます重要になってきている。しか
し、一方で、専門知識や技術の陳腐化のスピ
ードも加速している。今日、企業は他と差別
化できる新しい価値を、生み出し続けなくて
はならない。そこで、情報の活用が、重要な
役割を果たすことは間違いない。

概して、日本のこれまでのIT活用は、業
務の効率化を目的としたものが多かった。た
とえば、ナレッジマネジメントシステムにお
いても、紙文書の削減や検索の容易性、遠隔

地からのアクセスなどに重点を置くものが多い。これに対し、米国では、企業の成長や価値の創造に役立てようという考え方で利用されていると言われる。

これは、米国が、80年代の日本の成長要因を研究し、日本企業で日常的に行われているさまざまな知の共有の重要性に気づいたからである。米国のナレッジマネジメントシステムは、そこから発達を遂げた。日本の文化のなかでは、あらたまって認識されることのなかった価値創造のプロセスが、異なる文化の視点から評価されたのである。

サミュエル・ハンチントン（米国の政治学者。著書『文明の衝突』）は、米国と日本の文化を、どちらも「近代的」とした上で、「罪と恥」、「競争と協調」、「異質性と同質性」などの点でとくに異なると指摘した。「言わずもがな」の文化で育った日本人は、情報を積極的に開示するのが得意ではないようである。

しかし、日本企業は、企業内にある情報を可視化して関係者で共有し、擦り合わせていくことの重要性を再認識すべきである。新たな価値はそこから生まれるのであり、それのできる限り組織的に効率性の高い形態で実現させていくことが求められているのである。

10年以上前、世界は「知識社会」に入ろうとしていると言われた。しかし、「情報＝知識」の流出が企業や社会に及ぼす影響は大きい。このため、「知識＝情報」の流通量が増大する以上に、その資産としての重要さが認

識され、保護される社会に移行したように思われる。企業は情報資産の価値を見つめ直し、その取り扱いに真剣に取り組まなくてはならない局面にきていることは間違いない。

「情報管理」を念頭に置いたセキュリティ対策

野村総合研究所（NRI）が扱うセキュリティ関連製品に、「Webブラウザプロテクター」がある（図1参照）。これはWebブラウザに表示される情報の再利用や流出を防止する機能をもった製品で、Web環境で顧客情報や社内の重要情報を扱うシステムを利用する企業への導入が進んでいる。

これは、Web画面の中に用意された、入力フィールドやボタンなどのコントロールの操作を阻害することがないため、これを適用したことで利便性が低下するというような窮屈な事態を招かない。業務フローの中でどうしても印刷が必要になる画面については、その画面だけ保護機能の適用をオフにすること



図1 Webブラウザプロテクターの利用イメージ(合成)

もできる。また、運用面でもコンテンツやプログラムに対して特別なタグを埋め込む必要がなく、利用者側、提供者・運用者側双方が、業務スピードを鈍らせなくて済む。利便性と運用負荷に配慮したこの製品の適用は、セキュリティのみならず、情報活用も含めた企業の情報管理をサポートする好例と言えるだろう。

しかし、同じ情報が複数のシステムで別々に管理されていたり、クライアント側にも重要な情報が多く存在したりするケースでは、こういった製品の適用よりも、まず情報の一元管理化を図ることが重要となる。2005年4月までに間に合わなくとも、管理する情報をまとめておけば、情報流出対策が実施しやすくなる。加えて、情報の更新、一貫性の維持にも効果的であり、できる限り早く管理形態の一元化を進めるべきであろう。

たとえば、各種ダイレクトメールを送るサービス事業者の場合、参照されるユーザープロフィールがメールの発信元の部署ごとに異なり、オプトインの情報が共有されていないとすればどうなるだろう。ダイレクトメールの受け取りを拒否したユーザーに、誤ってメールが配信されてしまう事故につながる危険が容易に予想されるはずだ。

情報はDBMSなどで一元的に管理し、運用が容易なWebベースでのアクセスインタフェースを用意する。そして情報の流出事故を未然に防ぎたい重要情報の一覧画面などについて、適宜Webブラウザプロテクターのよ

うな機能を適用し、流出を防ぐ対策を施す。

これはひとつの例であるが、同様に情報活用という点で使い勝手がよくセキュリティも確保されるような情報管理対応が今後ますます必要とされるであろう。

まとめ

「情報」というドメインだけにフォーカスした場合にも、多くのリスクは存在する。それは個人情報の取り扱いに限らない。技術的ノウハウや販売情報のセキュリティが侵されると、それは、すぐさま自社の競争優位を脅かすことにつながる。しかし、だからといって、「情報」を有効活用せず、行き当たりばったりの製品開発や営業活動を行っていたのでは、プレーヤーとしてマーケットに参加し続けられない。情報資産は、企業活動の原動力となる金の卵であるとともに、これまでのリスクに対する企業の知識や経験では対応しきれないアキレス腱にもなっている。

したがって、「情報」に対して、単にセキュリティ面で防御するという発想だけで取り組んだのでは、不十分であると言える。本来の企業活動を積極的に推進していくことと表裏一体のものとしてとらえなくてはならない。持続的な成長のためには、リスクが伴う「情報」の収集や流通を促進しなくてはならないことを再認識し、その活用と保護の間で、バランスを考えながら、検討していくことが求められていると言えるだろう。 ■