4.1 情報を守る必要性

時代が物質的な産業資本主義から、情報そのものが生産・消費の対象として市場で膨大にやりとりされる高度情報資本主義に移行するにつれ、情報そのものが持つ社会的な価値は非常に大きくなってきました。

もちろん、工業製品自体の価値が下がった訳ではありません。例えば自動車の場合、手で触れられる物としての車よりも、その車の意匠（デザイン）、車に搭載されるエンジンの設計図、タイヤのゴムの化学的製法、その他、車に詰め込まれたハイテク機器やソフトウェアのソースコードなどの情報のほうが、はるかに大きな価値を持つようになりました。また、誰がどの車をいつ購入したのかといった顧客情報やマーケティング情報は、より価値の高い財産となっています。さらには、その車に付けられたブランド名や独自のロゴなども広い意味で情報と呼べ、これらも企業の重要な財産です。

こうした観点からみると、情報を守るということは製造業者がパーツを盗難から守ることと同様に、あるいはそれ以上に重要であることがわかります。

4.1.1　コンプライアンス

コンプライアンスとは応諾する、従順であるという意味の言葉ですが、近年、法令遵守という意味で使われることが多くなっています。特に企業の活動において、その活動が法律・条例に違反しないようにすることをコンプライアンスあるいはビジネス・コンプライアンスと呼んでいます。また、法令や条例に反していないまでも社会通念上好ましくない、あるいは不正だと判断されないようにすることを、企業倫理と呼びます。最近では、この企業倫理の領域までを含めてコンプライアンスと呼ぶ場合も多くなってきました。

情報技術の世界では、不正アクセス防止法（不正アクセス行為の禁止などに関する法律）、個人情報保護基本法（個人情報の保護に関する法律）、特定電子メール法（特定電子メールの送信の適正化などに関する法律）などの法律・条例に直接抵触する行為を避けることはもとより、倫理の領域に注意を払うことも必要です。刑事罰の対象とはならないまでも、民事的に賠償責任などが発生する行為も考えられます。たとえば以下の行為は、明らかに法律に抵触する行為です。

- Webサーバに侵入し、HTMLデータを書き換える。
- データベースサーバに侵入し、顧客データを不正に取得する。
- 広告であることを明記せず、無差別に広告メールを送りつける。

一方、以下の行為は、法律上は可罰的違法性がありませんが、得意先や取引先からの信頼を低下させ、場合によっては民事訴訟の対象となる恐れもあります。

- ウイルスに感染したコンピュータから、得意先や取引先に対して大量のウイルス添付メールが送信される。
- メールサーバが外部ドメインからのメールを転送許可する設定になっていたため、スパムメールの踏み台とされる。
- コンピュータに外部からワームが侵入し、特定のサーバに対して業務を妨害するためのDoS攻撃の踏み台にされる。

いずれにせよ、倫理的に好ましくない行為の芽を摘むことが重要です。

コラム：内部統制と日本版SOX法（J-SOX）

2001年、アメリカにおいて巨額の粉飾決済や不正監査、役員不正が多発したのを契機にして、資本市場に対し企業の健全性を開示させ、市場の信用を回復させるための法令として2003年4月にSOX法（サーベンス・オクスリー法）が制定されました。SOX法制定の背後には、「企業経営者の責任の明確化」、「監査人の独立性強化」、「財務情報の開示強化」という三つの大きな柱があり、これらを、内部統制と呼ばれるプロセス監査システムによって監視することが義務付けられました。内部統制とは企業内部において社員が違法な行為などを行なわず健全に企業活動を行なうように、業務プロセスを標準化・透明化して組織を統制していく仕組みのことです。内部統制は法令順守が絶対であるため、コンプライアンスを実現する1つの手段ともいえます。

日本では2006年6月に金融商品取引法いわゆる日本版SOX法（J-SOX）が成立しました。J-SOXは2008年4月から上場企業を対象として施行されています。

金融庁から出されている内部統制の基本的要素には目的を達成するために6つの要素があり、その1つに「ITへの対応」があります。元々、ITの世界においては内部統制とは違った観点で、セキュリティ管理などの概念がありましたが、単純化された業務プロセスを迅速かつ正確に、また処理記録が残るという点でITの重要性は更に高くなっています。

NOTE

スパムメール：不特定多数に宛てた広告メールなど、受け手が望まないのに送りつけるメールのことをスパムメールと呼びます。
DoS攻撃：特定のサーバに対して連続してpingパケットを送信したり、DNSリクエストを繰り返したりしてサーバの処理をオーバーフローさせる攻撃のことをDoS（Denial of Service）攻撃と呼びます。

4.1.2　情報管理

情報化の波は、社会生活を豊かにする反面、危険性も秘めています。例えば、悪意を持つ第三者の不正アクセスやコンピュータウイルスによる情報の漏洩や改ざん、消失などは、情報化された社会に深刻なダメージを与えます。企業内ネットワークなど、一見クローズドなネットワークであっても、通常はどこかにインターネットとの接点を持っていて、随時、情報が出入りしているものです。すなわち、非常に多くの情報が、常に第三者による不正利用や破壊などの脅威にさらされているといえます。悪意を持つ第三者ばかりではなく、悪意を持たない人たちでも、無意識のうちに情報を不適切に取り扱ってしまい、個人や企業の権利が侵害されてしまうこともあります。

また、インターネット上にはさまざまな情報があふれています。パソコンの編集機能により、インターネット上の情報を加工して別の情報として発信することも簡単に行なえるようになってきました。しかし、他人の作った文章や絵、写真などを勝手に利用することはできません。人が作ったものは知的財産権で保護されているからです。他人の情報を無断で流用することは、法律違反となり、企業の信頼性を損なうことにもなり得ます。

以上のように、企業は、自社の持つ情報を適切に管理・運用していくことが必要です。企業内で活用する情報を外部、内部問わず盗難や改ざんから守っていくこと、情報の利用に関するルールを併せて情報管理と呼びます。

図4.1に情報管理の位置付けを示します。

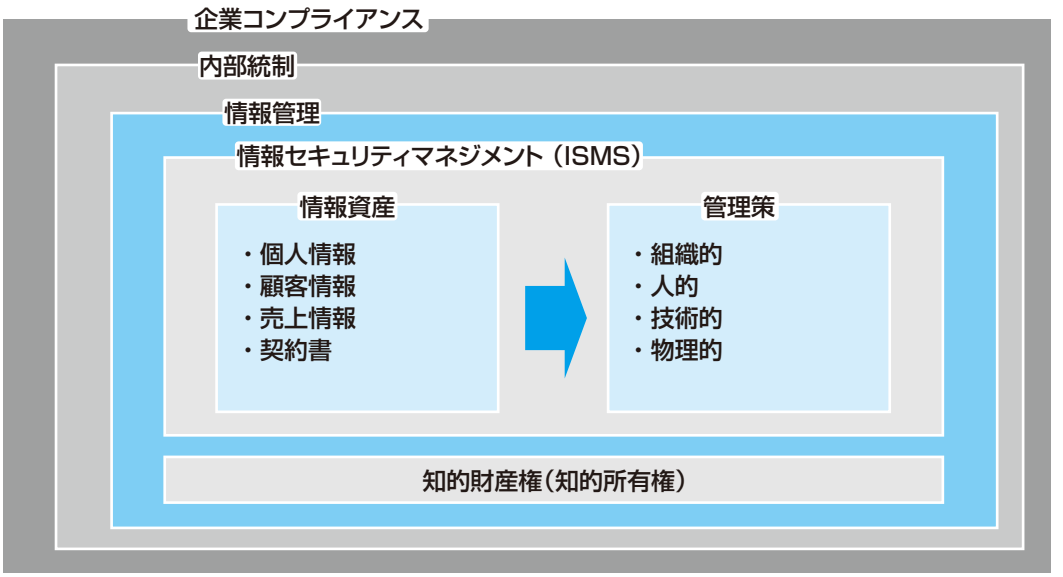

図4.1　情報管理の位置付け