やっぱり間違いだらけのISO

第9回
「間違いだらけのISO／企業秘密と内部統制編」

DASジャパン株式会社 代表取締役
萩原 睦幸

個人情報の流出がマスコミに大々的に取り上げられ世間の注目を浴びているが、組織にはそれよりもはるかに重要な「企業秘密」に関する情報がある。この企業秘密に関しては、重要な新製品情報や研究開発データなどが知られているが、これらばかりではない。

顧客リスト、入札関連などの営業情報、仕入先からの購買に関する情報、それに各種議事録、定期的な社内報などはれっきとした機密情報である。さらに何気ない掲示物や組織変更に伴う人事情報なども、競合他社にとってはおいしい情報なのである(**図表1**)。

実はこれらの機密情報について意外と管理がずさんなところが少なくない。この際情報セキュリティの仕組みに先立ち、くまなく情報資産台帳などにリストアップし、各々の資産価値に応じた保護対策を講じる必要がある。

よく見かけるのは、電車内で重要な会議の議事録に人目も気にせず堂々と目を通していたり、パソコン内の重要な情報を回りの人にさらけ出している光景である。たまたま競合他社の人が近くにいたりすれば、それだけでも大きな脅威であり、かつ重要なヒントを与えることになってしまう。つい先日も、私の隣に座った中年社員は、パソコンに「社外持ち出し禁止」のラベルが貼ってあるにもかかわらず平気で使用しており、この行為は完全にルール違反である。また、最近はHPなどで自社をアピールしている企業が多いが、あまり検討せずに何もかもさらけ出すと競合他社に思わぬ足をすくわれることにもなる。海外の企業の中には、公開情報を意図的に偽っ

図表1　企業秘密として保護される条件

条件	内容
秘密管理性	当該情報が秘密対象として管理されていること
有用性	事業活動に有益な営業上または技術上の情報であること
非公知性	世間一般に公然と認知されていないこと

て競合他社を混乱させ、出し抜こうと考えている企業さえあるという。

そこで今注目を浴びつつあるのが、これらのさまざまな断片的な情報を収集・分析し、それらを競争情報として自社の戦略立案に生かす考え方である。欧米ではこのような企業が少なくなく、無防備な日本企業が狙われているという噂もある。これは旧来の産業スパイのように、重要な機密情報を盗んだり、会議室に盗聴マイクなどをしかけて貴重な情報を得るやり方とは違い、合法的に許される範囲の活動である。

情報セキュリティの仕組みの構築でも、「電子データの保護」ばかりに気をとられていると、思わぬ機密情報の流出につながりかねない。というのは、機密情報は電子データ以外のものもたくさんあるからだ。紙情報はいうに及ばず、社内での日常の何気ないやり取りやメモ、勤務を終え緊張感を失った社外での会話や行動など、機密情報が漏れる可能性はいたるところに存在する。某会社の秘書は仕事熱心で休日もいとわず働いてくれることで感謝されていたが、彼女の親戚に競合会社に勤務している人がいたという話もあり、いつどこで機密情報が漏れるかは分からない。

いずれにしても、自社として重要な機密情報は守る権利がある。競合他社を一歩でもリードしてこの厳しい競争社会を勝ち抜いて行かねばならないからだ。一方組織内の透明化やオープン化を求める声も強い。これからの組織は、両者のバランスをよく考えた上で、オープンにすべきものとそうでないものをきちんと区分し、社外にオープンな会社でありながら他社にない高い技術力を保持し得る企業を目指すべきであろう。

性悪説も時には必要

最近の情報漏洩や企業犯罪をみると、「まさかあの人が」という人が罪を犯していることに驚かされる。一見犯罪とは無縁なごく普通の人が犯罪に手を染めているからである。いわゆる「出来心」とか「魔がさした」といわれる類だが、人間は周囲にまったく監視の目がないと、ついよからぬことを考えるものである。

ところがわが国では、今まで他人を疑うのはタブーとされてきた。基本的に人間は善良であり、まず悪いことはしないものだという「性善説」に基づく考え方だ。今でこそ取引先と契約書を取り交わすようになってきたが、ひと昔前まではお互いの信頼関係だけで契約書ひとつなく、たとえあったとしてもその内容は通り一遍のあいまいな表現で済まされており、何か問題が起こったときのお互いの責任の取り方なども満足に記載されていないのが実態だった。そのくせ、ひとたび何かのトラブルでもあると、あいまいな契約書の内容に振り回され、結局は責任の擦り付け合いになり、今までの信頼関係があっという間に失われてしまうのである。

これを防ぐためには、当初から「人間は条件次第で悪事を働く」という性悪説に立ち、まさかのときに備えておくことも時には必要なのである。例えば、あらかじめ犯罪を想定して、その手口をあれこれ予測し、それを先回りし何らかの対策や取り決めをしておくことで犯罪や不正を未然に防止できるのである。

今までの日本人的な感覚からすると、当初から他人を疑うことに躊躇することも考えられるが、あらかじめ取り決めたルールに従っているかのチェックは、お互いに守るべき当たり前のことを確認しているに過ぎず、ヘタな遠慮などする必要はないのである。

人間系のセキュリティ対策

今までの情報セキュリティ市場は、ITが外部からのウイルスやスパムメールの攻撃にいかに耐えられるかに重点が置かれていたが、最近は企業の9割程度にウイルス対策ソフトが導入される時代を迎え、これらへの対策は一段落したとの見方が広まっている。

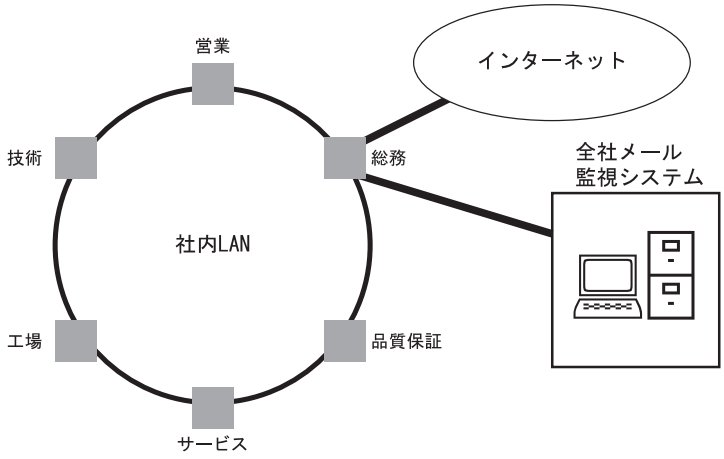
それよりもむしろ企業内からの情報漏洩や機密情報などの持ち出しが問題になっており、そちらの解決に軸足が移りつつある。その意味では、情報セキュリティの仕組みも、高度なセキュリティ技術を駆使した対策に加え、「人間系のセキュリティ対策」を強化する要求が出てきたといえよう。あらためて考えてみると、今日のIT技術のめざましい発展やさまざまな情報交換などはすべて人間が考え出したものであり、であれば逆に、人間の考え方や行動こそ、情報セキュリティにおける最大の脅威だという見方もできる。

前述の人間を「性悪説」として捉える考え方は、まさに人間の考え方や行動を

監視するものだが、人間の及ぼす脅威の脆弱性を少しでも取り除くためにも、何らかの取り決めは必要なのである。

例えば、社員の日常のメールの監視強化がある。どの所属の社員がいつ、誰と、どのような内容についてメールをやり取りしたのかを逐次監視し、何かの問題発生時には徹底的に調査できる仕組みの企業が出始めている(**図表２**)。また、すべての社内のパソコンをシンクライアントパソコンに入れ替え、情報やデータなどは端末にはいっさい保存できない仕組みに変えたところも増えつつある。さらに各種データへのアクセス制限も強化し、自分の業務に関係しないデータにはいっさいアクセスできないようにした企業もある。このように人間系に関するセキュリティもじわじわと規制される方向に動いている。

図表2　不正メールチェック



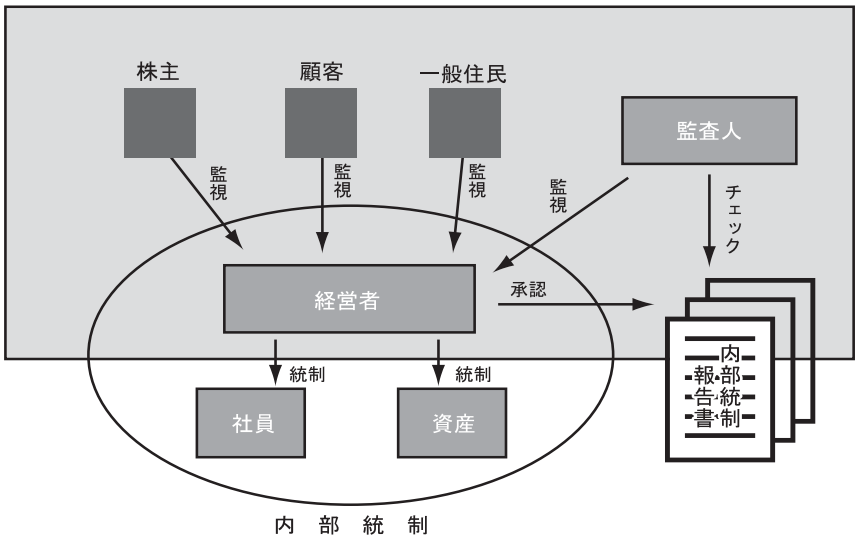
内部統制の時代

折りしも、来春から上場企業とその関連会社に「内部統制の仕組み」の導入が義務付けられる。

これは企業の財務会計の健全化を狙った法律だが、情報セキュリティと密接な関係がある。

「内部統制」という言葉は、一般の人にはあまりなじみがないが、従来から金融関係分野では財務報告の適切性の観点から用いられてきた。今やこの内部統制は、財務報告の健全性にとどまらず、広く企業内のコーポレートガバナンス(企業統治)までを意味する内容に変わってきている(**図表３**)。今回の上場企業に導入が義務付けられる内部統制は、昨今の相次ぐ粉飾決算の不祥事の防止を目的とした財務報告の健全性を狙ったものだが、この内部統制は、単なる財務報告にとどまらず、企業内の不正やミスの防止、それに業務の効率性も同時に実現できるという目論見もある。

図表3　コーポレートガバナンス(企業統治)



さて、現代の企業は日常業務そのものが大きくITに依存している。つまりこの内部統制の仕組みも組織内の業務プ

ロセスの整備ばかりではなく、日常のIT環境の統制まで行うことで、経営効率を上げる副次的効果も狙っている。

今や大手企業はいうまでもなく、中小や個人の零細企業にいたるまで、ITなしでは立ち行かない時代になりつつある。例えばちょっとした会計処理にしても、市販のアプリケーションソフトのおかげで簡単なパソコンへの入力処理だけで正しい処理ができてしまう。当初入力作業に慣れないと面倒な気もするが、慣れてしまうとITの便利さにかなうものはない。

ところで、このIT環境の整備・見直しには大きな意義がある。さまざまな業種の企業が目先の便利なITに飛びつき、後先も考えずにその場の思いつきで導入し、今日に至っている企業が少なくないのではないだろうか?

だからこそ、あちこちにITの脆弱性が生まれ、情報漏洩やデータ破壊の脅威にさらされているのだ。この内部統制という仕組みの導入をチャンスに、現状のITを基本からレビューし、業務に役立ちかつ社内外の情報アクセスの脅威から保護される強固なIT環境を、まさに構築するときではないか。

今後ITは企業内にとどまらず、広く一般の人々の暮らしに入り込んでくるのは間違いない。誰でもどこでもITが活用できる「ユビキタス社会」がいよいよ現実味を帯びてきている。となれば、内部統制の考え方を、組織内はもちろん、職場を離れた社外や家庭内にも広めていくことが必要になろう。というのは、社外や家庭から情報漏洩が起こるケースが少なくないからだ。

内部通報制度の効果

情報漏洩事故や企業犯罪を防止する上で大きな効果が期待できるものに、「内部通報制度」がある。過去のさまざまな企業不祥事は、社員からの内部告発により明るみに出た事件が少なくない。

内部通報制度とは、組織内の不正や違法行為の問題発生を抑止するために、通常の業務の連絡体制以外の報告ルートを構築し、未然に予防的対策をとり健全な企業風土を構築するものである。内部告発に踏み切る者は、現に世話になっている企業と目の当たりの不正・違法行為との間でジレンマに陥り悩んだ末の結論であろうが、それ相応の覚悟も持ち合わせている必要があろう。というのは、現在の内部通報制度はまだ未成熟なところもあり、保護されるべき通報者本人が保護されないケースが後を絶たないからだ。

内部告発の見返りとして人事の報復やさまざまな嫌がらせがあるというから、これでは企業内の不正を正すことができなくなってしまう。告発する通報者自身も、明らかに不正を正すという目的でなければならない。単なる経営者や特定の個人を追い込む目的などでの告発は正当なものとはみなされず、逆に通報者本人が不利益を被ることになる。

内部通報制度が健全に機能するためには、次のことが必要となろう。

(1) 経営者が十分この制度を理解していること

(2) 通報内容が適切に処理されること

(3) 通報者本人が保護されること

ここで重要なのは、組織全体に内部通報制度の意義や内容を正しく理解させる必要があり、これが不十分だと密告や裏切りといった、本来の不正を正すという趣旨を外れた行為になってしまう。逆に内部通報制度が正しく理解され社員に浸透してくると、不適切な行為は通報されるとの思いから、抑止効果が発揮される。つまり内部通報制度は、それが存在するだけで大きな意義を持つのである。▼

DASジャパン株式会社
代表取締役
萩原 睦幸

【プロフィール】2006年10月、英国系(UKAS)審査機関設立。組織に役立つ審査を理念に全国展開中。著書及び講演多数。『ISOが見る見るわかる』『間違いだらけのISO審査』『よくわかる日本版SOX法』他。著書は韓国語、中国語、タイ語にも翻訳されている。