情報セキュリティ認証制度を考える
～ 認証取得企業調査から ～

はじめに

2002 年 4 月に本格運用が始まった ISMS（情報セキュリティマネジメントシステム）は、2007 年 6 月 22 日現在、2,226 事業所が認証を取得している。本格運用から既に 5 年以上が経過しており、QMS（品質マネジメント、94 年運用開始）の約 43,400 事業所や EMS（環境マネジメント、96 年運用開始）の 19,800 件に比較し、事業所の取得件数は遙かに少ないが、確実に増加している。

一方では、プライバシーマーク、ISMS 認証取得事業所において、大規模な個人情報漏えいも発生しており、認証取得制度に関する疑問も呈されている。

このような状況から、認証取得事業所の実態を調べるため、20007 年 2 月に ISMS 認証取得企業に対して、実態調査を行った。

調査は、2007 年 1 月現在、ISMS 認証を取得した 1,907 事業所のうち、住所を公開している 1,422 事業所を対象とし、郵送によるアンケートを実施し、264 事業所（回答率 18.6%）から回答を得た。認証取得は事業所単位であるため、一法人が複数の認証を取得している場合、原則として全ての事業所に送付した。

ISMS 認証制度と同様なものに、QMS（品質マネジメントシステム）、EMS（環境マネジメントシステム）があるが、これらの認証取得事業所の一部を対象に実施した調査[注1]はあるが、認証取得事業所全体を対象に行った調査は、今回が最初だと思われる。

分析結果から

アンケート全体を分析する限りにおいて、以下のよう事が明らかになった。

① 経営者の情報セキュリティ、ISMS 推進等の意識の高低が大きく影響している
② ISMS への誤解。特に管理策への誤解が多い。
③ コンサルタントの問題。認証取得や情報セキュリティシステムの構築の支援を求めた一部のコンサルタントのレベルの低く、ISMS 認証取得に悪い影響があった
④ 審査機関、審査員の問題。審査員のレベルが低いため、苦労しているも見うけられる
⑤ ISMS 独自の問題。ISMS が ISO/IEC27001 への移行があり、移行期間が短かったため、本来業務の停滞がみられた

これらについて少し詳細にみていくと、ISMS 推進にあたっていくつかの課題がわかる。

（１）「② ISMS への誤解」では、管理策への誤解が多いが、ISMS 等のマネジメントシステムには、監査の考え方が根底に流れている。　しかしながら、この点の理解がない事業所や審査機関（審査員）が多いように思われる。ISMS の管理策で決められている内容が唯一絶対のものであるとの考えがちであるが、監査の考え方は、管理策

で決められているものが不十分であれば追加すればよく、対象外の管理策があれば、その理由を明確にし､削除できる｡このことはISMSの要求事項にも明記してあるが、これを理解していないと、いわゆる「日本版SOX法への対応は、ISMSでは不十分である」とか､「当社が目標とする情報セキュリティマネジメントには、ISMSの管理策のレベルは低すぎる」と言った誤解が発生する。また、外部委託をしていない事業所では、外部委託に関連する管理策は不要であることも理解できる。

（2）「③ コンサルタントの問題」では、本調査だけでなく、筆者が関係している審査機関の「審査判定委員会」においても、認証対象事業所の審査状況報告でも、ISMSが理解できていないコンサルタントが一部にいるために審査での指摘事項が非常に多いとの報告がある。

取引先企業や親会社から、ISMS認証取得を迫られて、内部にISMS等の知識を持った社員がいないため、十分な検討もせずにコンサルタントに半ば「丸投げ」せざるを得ないためかも知れない。　この様なケースの場合、認証取得に長期間必要になることも多く、社員がISMSの知識を習得し、信頼できるコンサルタントに委託（必要な部分のみの委託が望ましい）することが結果的に良い結果をもたらしているケースが多い。

コンサルタントの格付け制度を創設してはどうかとの意見もあるが、誰が、どの様に行うかと言った方法論の問題だけでなく、格付け制度を作ることの是非も議論する必要があろう。

（3）「④ 審査員、審査機関の問題」では、最近は比較的良くなってきたとの話もあるが、一部の審査員のレベルの低さを指摘する声もある。私見であるが、古い時代のQMS審査しか知らない審査員がISMS審査員になったケースがある。審査員資格として、① 監査の考え方、② 情報システム、情報セキュリティの知識、③ 審査事業所の業務知識、業界知識、を持っていることが望まれるが、必ずしも十分な知識がない審査員が一部にいると感じられる。

最近は、審査員教育の充実を求めているため、レベルの低い審査員は少なくなっているようであるが、一層の努力が求められる。

（4）「⑤ 移行の問題」であるが、ISO/IEC27001が制定され、従来、ISO/IEC17799を基に実施されていた認証制度の内容が更新されることになった。審査は認証取得後、１年ごとに行われるため、18ヶ月の移行期間では、ISO/IEC27001実施直前に認証取得した事業所は短期間に新システム（ISO/IEC27001）への移行を与儀なくされた。もう少し余裕を持って移行期間を設定して欲しいとの要望である。

（5）「① 経営者の意識」については、取引先や親会社等の外部からの要請により ISMS認証取得を短期間に求められた事業所では、低レベルのコンサルタントに丸投げし、認証取得が目的化し、認証取得後は経営者が関心を示さなくなってしまうと、ISMSの維持管理がうまくいかないことが多いようである。更に、ISMS 認証取得・維持の

ためには、何でもありと言った考えに陥り易く、現場での作業との乖離が発生したりするため、推進事務局が苦労している様子が伺われる。

経営者の意識が高いことが､結局はISMSの成功に結びついている様子がうかがえる。日本ではボトムアップ的な経営と言われているが、ISMS 認証取得等では経営トップの関心の高さが、成功要因の１つであると感じられる。

認証取得について

昨年来、ISO9001やプライバシーマーク取得事業所において、不祥事がマスコミを騒がしているが、本調査やISMSの調査・研究や某審査機関で審査判定委員会委員長を拝命している者として、最近の不祥事等から、以下のようなことを感じている。

（１）ISMSやISO9001等では、マネジメントシステムの構築が十分に行われているかを審査するものであり、マネジメントシステムが完全であることを保証するものではない。もっとも、企業のマネジメントシステムが 100%問題ないことを保証することは、どの様な分野でも不可能である。　色々な製品でリコールや人身事故の発生を完全になくすことができないこととなんら変わりはない。

（２）ISMSやISO9001等の認証取得事業所において、不祥事が発生すると事業所自体だけ問題になることが多いが、審査が適切に行われたのかについても検証が必要と思われる。　ISO9001認証取得をしていた食品工場の不祥事では、マニュアル等の不備が指摘されたが、ISMS やISO9001 では文書作成・更新は重要な項目の１つであり、ISO9001の審査員が確認していなければならないはずであるが、維持審査・更新審査時点で確認をしていなかったのだろうか？

認証取得事業所において、関連する事件・事故が発生しないことを保証している訳ではないが、審査機関、審査員が適切な審査をしていたかの検証は必要と思われる。認証取得事業所の大規模な事件・事故については、第三者による、いわゆる「事故調査委員会」による検証が必要ではないかと考えている。

不適切な審査をした審査機関、審査員には何等お咎めのなくても良いと考えるのであれば、不適切な会計処理を認めた経営者や会計事務所が何故罰を受けたかを考えてみて欲しい。

なお、上記食品工場では、事故後にISO9001認証の取得が認められなかったが、事故前後で大きな変化があったのだろうか？　単に、問題点が顕在化しただけである。　それを見つけられなかった事故前の審査機関には、説明責任があるのではないか？

（３）今回、始めてこの様な調査を行ったが、調査側での課題もあり、費用の工面ができれば、今後とも実施し、ISMS 等の認証制度をより良いものにして行きたいと考えている。

本調査は、(財）ニューメディア開発協会の資金援助にて実施した。また、多くの認証取

得事業所の協力に対して厚く御礼申し上げます。

なお、調査の詳細は、同協会のウェブ（http://www.nmda.or.jp/）を参照いただきたい。

注１： 主なものとしては、以下のようなものがある。

- （財）日本適合性認定協会（http://www.jab.or.jp/）、2006 年 1 月「ISO9001 に対する適合組織の取組み状況
  （http://www.jab.or.jp/library/Report_Survey-QMS_2005.pdf）」
- （社）日本印刷技術協会（http://www.jagat.or.jp/）、2001 年 5 月「ISO9000 運用アンケート調査（http://www.jagat.or.jp/story_memo_view.asp?StoryID=4688）」
- 日本海事検定キューエイ株式会社（http://www.nkkkqa.co.jp/）2006 年 10 月「EMS アンケート調査結果
  （http://www.nkkkqa.co.jp/docs/topics/200610_EMS_Question-report.pdf）」、2006 年 7 月「QMS アンケート調査結果
  （http://www.nkkkqa.co.jp/docs/topics/200607_QMS_Question-report.pdf）」