平成 22 年度ニューメディアを基礎とする調査研究事業

ISMS 第三者認証制度をより有効なものにするための
ＩＳＭＳ 認証事業所調査
調 査 概 要 報 告 書

平成２３年３月

財団法人 ニューメディア開発協会

この事業は、競輪の補助金を受けて実施したものです。
http://ringring-keirin.jp

１．本調査について

国内における情報セキュリティマネジメントシステム適合性評価制度（以下、ISMS 認証制度）への関心は高く、2010 年末に 4,522 事業所が認証取得しており、世界の半数以上[1]を占める。しかし、ISMS が必ずしも業務遂行に役立たないとの声もあり、他の認証制度、ISO9001（品質マネジメントシステム、QMS）でも指摘[2]されている。しかし、ISMS 認証制度に対する調査は本調査以外なく、実態を調査し、ISMS 認証システムの維持・継続を目指して本調査を実施した。

１．１　アンケート概要

（１）　**期間及び回答数**： 2010 年 12 月 24 日にアンケートを発送し、2011 年 1 月 31 日を回答期限とし、2 月 14 日までに返送分を集計した。426 事業所から回答を得、回答率は 22.1%であった。

（２）　**アンケート調査対象**： 2010 年 11 月時点で、（財）日本情報処理開発協会 ISMS 推進センターが公表している ISMS 認証取得事業所の内、取得年月が古い順に 2,000 事業所に送付した。

（３）　**アンケート調査項目**： 今回の調査では、前回調査に準じ、①事業所、記入者の基礎情報の質問（7 問）、②ISMS 認証取得に関連する質問（11 問）、③ISMS 認証運用に関連する質問（9 問）、④コンサルタントに関する質問（12 問）、⑤ISMS 審査員に関する質問（7 問）、⑥ISMS 認証の重要運用項目に関する質問（6 問）、⑦教育・社内ルールに関する質問（8 問）、⑧その他の質問（5 問）の 8 グループに分けられる。

１．２　インタビューの概要

インタビューは、2011 年 3 月 3 日より、3 月 7 日の 3 日間に回答事業所の内、6 事業所に対して実施し、あらかじめ定めた設問に対して回答を得たが、回答内容については個別企業名や面談者を特定できないように配慮した。

２．調査結果概要

２．１　アンケート結果の概要

- 資本金「1,000 万円以上 5 億円未満」の企業が約 8 割ある。
- 約 70%の事業所が従業員 300 人未満で、認証対象従業員 300 人未満が約 85%。
- 情報通信業が 40%以上で、製造業：約 12%、複合サービス業：約 11%だった。
- QMS：約 36%、EMS：約 30%、P マーク：約 26%で、約 57%が ISMS 以外の認証を取得。
- 取得目的は、営業活動に有利：約 75%、情報セキュリティ対策向上：約 66%。
- 社員のセキュリティ意識の浸透と実践:約 87%、情報資産の明確化と整理:約 80%、

[1] 全世界で7,058事業所の内、日本は3,720事業所で、全体の約53%を占めている。(International Register of ISMS Certificates の 2010 年 12 月の調査。 国内での登録件数とは異なる件数になっている) http://www.iso27001certificates.com/

[2] 日経コンストラクション「ISO を入札要件から外す」日経 BP 社 2004 年 6 月 11 日号

事故発生時の体制・計画の整備：約 62%、情報流出や漏洩の防止・軽減：約 61%が導入効果だが、想定外の影響は、業務量増加：約 40%、業務上の制約増加：約 33%、対策コスト増加：約 32%、組織・人が必要：約 26%で定着化に苦労し、半数以上が業務量の増加や手続きの煩雑化・効率低下と回答。資料作成が負担であり、約 33%が業務上の制約を増やしている。

- 実業務と ISMS の乖離では、「どちらとも言えない」(149 件、35.3%)、「乖離はある」(112 件、26.5%) だが、前回調査の 2 倍以上が乖離を感じている。
- コンサルタントは、ISMS 認証取得までは 70%以上が利用したが、取得後は 70%弱が利用してない。10 段階評価で 7.14 と厳しい評価をしている。
- 審査機関・審査員も、前回より厳しい評価（7.76）で、「実効性のある指摘」等、基本部分の評価が低い。
- 社員教育の方法は、集合研修：約 82%、E-ラーニング：約 30.3%で、約 43%が 3 ヶ月に 1 回教育を実施。集合研修では出席確認：17%だけの事業所もある。
- 情報漏えい対策は、パスワード認証：約 95%、パスワードの定期変更：約 87、ファイルの暗号化：約 67%、外部媒体接続制限：約 57%で、50%を越えた。
- ノート PC や外部記憶媒体の持出ルールはともに「要許可」が 80%以上であった。
- ウイルス感染は、感染なし： 約 66%で、感染あり：約 33%で、他のセキュリティ調査と比較し、感染ありは半分程度で認証取得効果があると言える。
  感染原因はウェブ閲覧によるドライブバイダウンロードが半分以上で、トロイの木馬、スパイウェアと見られ、ワクチンソフトでの検出は難しい。
- 自由回答欄は、131 件、30.8% （全回収数：426 件）の記入があった。主な物とし、①制度的な問題： JIQ27001/27002 の規格書が分かり難い。P マークとの統合を望む。②審査機関・審査員の問題： 指摘が毎回異なる。レベルが低い。費用対効果が悪い。③運用上の問題： リスク評価、有効性評価が難しい。 作業負荷。従業員教育・周知が不十分。インシデントが減らない。 ISMS 担当者の交代が難しい。

２．２　インタビュー結果の概要

- 大規模事業所でなく、兼務者が多く、専門性が高く人事異動が難しい。経営層の理解等が ISMS 推進に影響。
- コンサル利用は、ISMS 関連レベルが分からず失敗も。客観的情報が必要であろう。
- 審査員は問題ないが多いが、適切な ISMS 審査ができない審査員が多い感じはある。

３．ISMS 認証制度の実効性向上のための提案

3 回目（2 年毎実施）で、本調査が最も広範囲に実施。ISMS 認証制度の考察を行った。

３．１　ISMS 制度の見直し／第三者機関の設置

- ISMS を国･自治体の入札要件[3]から外す。QMS では、官庁・自治体の入札要件のため、

[3] （財）日本情報処理開発協会「FAQ1: 制度一般」http://www.isms.jipdec.jp/faq/faq1.html

「認証を金で買う」事業所が増え、適切な品質確保ができなくなった。ISMS も同じで、セキュリティマネジメントの向上にならない事業所が多々ある。実業務と ISMS の「乖離なし」は 40%以下で、「乖離あり」が約 27%、4 社に 1 社以上ある。第三者機関の設置を設置し、認定機関、認証機関、審査員研修機関等の運営体制を監査する仕組みが必要であろう。制度が良くても、運用体制が悪ければ制度全体が揺らぐ。

３．２　コンサルタントの評価制度

多くの事業所はコンサルを利用している。コンサルの情報・評価が共有できていない。認証審査時に審査員とコンサルとの乖離があるとの回答もある。コンサルがどの様なコンサルテーションを行うかは自由だが、ISMS 関連の教育、経験等の情報公開で、関連知識レベルの向上や認証取得事業所のコンサルの選定にも役立つ。

３．３　監査概念（リスクマネジメント主体の考え）について

監査あるいは、リスクマネジメントの欠如が問題と感じる。管理策は取捨選択するもの。 JISQ27001「4.2.1 ISMS の確立」や JISQ27002「0.2.5 管理策の選択」を知らないコンサル、審査員、推進者等が ISMS 推進の妨げになっている。

ISMS は管理策がなくても、リスクが大きいと判断すれば、適切な管理策を作成する必要がある。環境・時間の変化でリスクは変わる。情報資産の見直し理由はリスクの変化。組織・システム変更等で、情報資産リスクの再評価が必要。

３．４　認証機関、審査員の質的向上

審査員により指摘が異なる。リスクの変化があれば、指摘も異なるが、説明は必要。指摘事項を認証取得事業所に説明し、誤解があれば、訂正が必要。意見相違はあるが、丁寧な説明をする必要がある。

認証機関･審査員に厳しい意見を記名で書いている事業所があることを認証機関、審査員は真剣に考えて欲しい。審査機関は審査員の質的向上に努めることが認証システムの普及に繋がる。

３．５　教育、普及啓発について

ISMS 認証システムの維持・向上に教育･普及啓発は最重要なものの１つ。 特に、ISMS 認証制度は、情報セキュリティを対象としたマネジメントシステムの確立である。関係者全てに周知し、推進することが大切である。しかし、調査から見える教育や啓発活動にいくつかの課題がある。

① 経営層などへの適切な教育の実施

ISMS 成功の鍵の１つは、経営層の関心の高さ。 ICT システムの数日間停止や個人情報･機密情報の漏えいが企業経営に及ぼす影響を考えて欲しい。ISMS 認証システムの重要性が理解できるであろう。　ICT システムや ISMS 認証システムに、関心を示さないことが大きな問題になる。

② 集合研修での工夫

e-ラーニングの実施は約 30%だったが、80%以上は集合研修。集合研修で 17%

が出欠確認のみで、19%程がアンケート実施。

カーク・パトリックは研修評価・効果測定の評価モデルを提言している[4]。最近の心理学や行動科学等の知見を利用した教育では、成果達成、投資収益率まで考えた教育・研修が行われている。

③ 継続的な教育・啓発活動

新たな技術などへの対応を含め、継続的な教育を行うことが大切になる。

4. 謝辞

約 2,000 の ISMS 認証取得事業所にアンケートを送付し、426 件の回答を頂きました。非常に高い回収率で、多くの ISMS 認証取得事業所の方々のご協力に深く御礼を申し上げます。

また、お忙しい中、インタビューを快諾頂いた認証取得事業所にも厚くお礼を申し上げます。

今回のアンケート調査は、財団法人ニューメディア開発協会の平成２２年度ニューメディアに関する調査研究事業の一環として実施しました。　ここに感謝申し上げます。

以　上

[4] （独）雇用・能力開発機構「公共能力開発施設の行う訓練効果測定」６章
http://www.tetras.uitec.ehdo.go.jp/download/kankoubutu/a-114-07.pdf

発行日　　平成 23 年 3 月 31 日
作　成　　財団法人ニューメディア開発協会
住　所　　〒112-0014
　　東京都文京区関口 1 丁目 43 番地 5 号　新目白ビル６階
電　話　　(03) 5287-5034
ＦＡＸ　　(03) 5287-5029

調査者　　中央大学 研究開発機構　内田勝也研究室
住　所　　〒112-8551　東京都文京区春日 1 丁目 13 番地 27 号

平成 22 年度 ニューメディアを基礎とする調査研究事業
（ISMS 第三者認証制度をより有効なものにするための
ISMS 認証事業所調査）

URL　http://www.nmda.or.jp