平成２０年度ニューメディアを基礎とする調査研究事業

情報セキュリティに関するマネジメントシステムの維持管理についての管理・運用面に関する調査研究

調　査　報　告　書

《概要版》

平成２１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。
URL：http://keirin.jp

１　はじめに

1.1 調査の目的

2001 年 7 月から翌年 2 月までのパイロット期間を経て、2002 年 4 月から本格運用が始まった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 認証制度と言う）は、2006 年 5 月に、JIS Q 27001／27002 を適用することになり、2009 年 3 月末時点で、3,000 を越える事業所[1]が認証を取得している[2]。

多くの事業所が ISMS 認証を取得しているが、ISMS 認証取得後に業務負荷が増加した、ISMS の考え方が組織内に浸透しない、と言った声が聞こえるようになった。このような認証制度の課題は、他の認証制度、ISO 9001（品質マネジメントシステム： QMS: Quality Management System）では、以前から雑誌や書籍で指摘されてきた。

このような課題が一部の認証取得組織のみの問題であり、全体として大きな問題ではないのか、あるいは、多くの ISMS 認証取得組織に同じような問題があるのか、といったことを把握するため、平成 18 年度に、ISMS 認証取得組織に対してアンケート調査を行った。この前回調査では、ISMS 認証取得及び運用に関連してどのような課題があるかについて調査した。

今回の調査では、この前回の調査の結果を踏まえ、さらに新たな問題点を探ることを目的とし、ISMS 認証取得組織及び ISMS 認証機関を対象にアンケート調査を行った。これにより、2 年前の前回調査と比較しながら、ISMS 導入及び運用で発生している課題を把握し、それに対する解決方法について、主に管理・運用面からの考察を行い、課題と施策案を述べることとする。

ISMS 認証取得組織が増えていく中で、本調査の結果やその解決策は、ISMS 適合性認証制度だけでなく、他の認証制度の実効性を高めることに寄与することが出来ると考えている。

1.2 本調査の構成について

本調査では、以下の 4 つの方法により現状の把握と課題の抽出を行った。

① 認証取得組織へのアンケート調査
② 認証機関へのアンケート調査
③ 認証取得組織へのインタビュー調査
④ 認証機関へのインタビュー調査

---

[1] 事業者が複数の事業所（本社、事業部門、データセンター等）で ISMS 認証を取得していることがあるため、「事業所」とした。なお基礎情報に関連するところでは事業者を用いた。
[2] 2009 年 3 月 27 日現在、3,092 事業所が ISMS 認証を取得している。

２　調査結果の概要

2.1 認証取得組織へのアンケート調査

（１）質問項目の構成について

本アンケートの目的に沿って、質問項目を作成した。

質問は以下の７つのグループからなる。

① 事業者（企業、公共団体等）の基礎情報

② ISMS 認証取得に関連する情報

③ ISMS 認証の運用に関連する課題

④ コンサルタントに関する情報

⑤ ISMS 審査員に関する情報

⑥ ISMS 認証の運用に関連する情報

⑦ ISMS に関連した教育・ルール

（２）回答について

回答は無記名方式とした。集計に当たって得られた回答に不明確な部分があった場合は、未回答または不明として処理した。

（３）アンケートの概要

①　期間

アンケート発送　　2008 年 12 月 8 日（月）

アンケート回答締め切り　2009 年 1 月 31 日（土）

※実際には 2 月 27 日（金）までに戻ってきた回答を集計した。

②　調査対象

2008 年 10 月 30 日の時点で、財団法人日本情報処理開発協会情報マネジメントシステム推進センターが同 WEB サイトで公表している ISMS 認証を取得した 2,650 事業所のうち、住所が公開されており、アンケート資料が正しく郵送されると判断した 2,092 事業所調査対象とした。

③　有効回答数

最終的に計上した 2009 年 2 月 27 日時点で、352 通の回答を得た。回答率は 16.8%であった。

（４）アンケート結果の分析

アンケートの回答から、ISMS に関連する組織や制度についての問題点として、主に以下の 6 点を挙げることができる。

① 経営者の情報セキュリティ、ISMS 推進等への関与が大きい。このため、経営

層の意向で方向性が変わることが想定される。

② ISMS 制度そのものへの誤解がある。ISMS 導入の予想外の影響として、業務量の増加や監査向け資料作成の増加を挙げている認証取得組織が多い。

③ 管理策への誤解が多い。認証取得組織の状況に応じて、管理策の中で必要ないものは適用除外したり、追加の管理策で更に高度なセキュリティレベルを構築してもよいことを理解していない。

④ コンサルタントの問題。認証取得や更新のために情報セキュリティシステムの構築の支援を求めたコンサルタントが業務を理解していないために、適切な支援ができない。

⑤ 経営者等との関係から、コンサルタントを決定する認証取得組織も多い。結果として、人的、組織的な要因からコンサルタントが選定されるため、適切な支援が行われない。

⑥ 認証機関、審査員の問題。審査員の業務の理解度が低いと感じている事業所もある。

2.2 認証機関へのアンケート調査

（1）質問項目について

本調査の目的に沿って、質問項目を作成した。

（2）回答について

回答は無記名方式とした。集計に当たって得られた回答に不明確な部分があった場合は、未回答または不明として処理した。

（3）アンケートの概要

① 期間

アンケート発送　　2009 年 2 月 3 日（火）

アンケート回答締め切り　　2009 年 2 月 20 日（金）

※実際には 3 月 6 日（金）までに戻ってきた回答を集計した。

② 調査対象

2009 年 2 月 3 日現在、財団法人日本情報処理開発協会情報マネジメントシステム推進センターが同 WEB サイトで公表していた ISMS 審査機関 23 団体を対象とした。

③ 有効回答数

最終的に計上した 2009 年 3 月 6 日時点で、7 通の回答を得た。回答率は 30.4%であった。

（4）アンケート結果の概要

① 認証機関の基本情報について

認証機関の規模にもよるが、ISMS 審査員は正社員よりも契約社員の方が多い傾向が見られる。

また、審査対象組織の専門性に関し、ほとんどの認証機関が得意とする業種が「どちらかと言えばある」「ある」を選択していた。

② 審査活動向上の取り組みについて

認証機関が考える力量の重要性と認証取得組織からのフィードバックから得られる力量の重要性では、若干ではあるが後者のほうが評価は低かった。認証取得組織側との認識に差があるとも考えられる。

③ 認証・認定活動実績について

認証機関の母数にもよるが、ほとんどの認証機関で不適合として判定を保留しているケースが見られた。ISMS 審査が単純に認証を与えるだけの審査ではないことがわかる。

④ 認証・認定活動実績について

今年以降の ISMS 認証取得要求度合いとしては、半数が微増から増加、一部では微減といった回答が得られた。ISMS の重要性に対する考え方と昨今の不況が影響していると思われる。

2.3 認証取得組織へのインタビュー調査

インタビューの結果から、ISMS 認証制度についての認証取得組織の取り組み方として、主に以下のような傾向があると言うことができる。

① 認証取得の契機に関しては、経営層の意向が大きく反映される傾向がある。また、いずれの認証取得組織も、個人情報の漏洩防止対策として ISMS 認証を取得していた。

② いずれの組織も、プライバシーマークの取得も検討していたが、最終的には経営層の判断で、業務形態に合致する ISMS 認証を選択している。このことから、他の認証制度とも比較を行ったうえで、自組織の必要性を勘案したうえで、ISMS 導入する傾向があるのではないかと考えられる。

③ アンケート調査でも、同様の結果が得られたが、認証機関に対しての大きな不満はなかった。ただし、個々の指摘においての解釈の違いや、意見の違いはあるようである。指摘については、大いに歓迎されており、むしろ、情報資産に変更があっても審査員が管理策の変更まで確認しなくてよいのかなど、指摘が少ないことに対する不満の意見があった。

④ 組織の内部への展開や、職員の教育を重要視している傾向がみられた。また、PDCA サイクルの中で、改善点のチェックまではできても、改善を実行することは難しい、との意見もあった。

2.4 認証機関へのインタビュー調査

インタビューの結果から、ISMS 認証制度についての認証機関の姿勢として、主に以下のような傾向があると言うことができる。

① いずれの認証機関にも審査を行う上での得意領域があり、幅広く専門知識を持った審査員の育成に注力している。

② 審査員の資質として専門領域のスキルに加え、コミュニケーション能力を重視している。またカリキュラムを組んで教育活動を行い、審査員としての力量を保持している。

③ 公正な審査を行って適切にマネジメントシステムを回すため、認証取得組織のありのままの状態の開示を希望している。

④ 付加価値のある審査としては、認証取得組織に規格適合性の観点からの「気づき」を与え、改善のためのトリガーとしてほしいと考えている。また認証取得組織・コンサルタント・認証機関の三位一体の取り組みが必要であるという考え方もできる。

3　ISMS 認証制度の実効性を向上させる施策案

調査結果を元に、ISMS 認証制度を導入・運用するときの実効性を向上させる施策案を述べる。

(1) ISMS 制度の再認識

認証取得組織は、社内の体制を確立し、自らが対応できる範囲で、必要に応じて管理策を構築するなど、常に見直しを図る必要がある。

(2) コンサルタントの評価制度

コンサルタント情報について、実際に認証取得を行う組織が容易に取得できるような評価制度が必要と思われる。

これにより、コンサルタント自身のレベルが上がり、コンサルタントも淘汰されていき、認証取得組織に対して、適切なアドバイスのできる優良なコンサルタントのみが生き残ることになる。

(3) 認証機関のレベルアップ

認証機関は、認証取得組織の理解に努め、一定以上のレベルを保ち審査が行えるように、しておかなければならない。認証取得組織を理解し、内容を納得させるためにも、コミュニケーション能力は、審査員として必須の能力である。

(4) 教育、普及啓発などについて

①上層部に適切な教育を実施する。

②集合研修について工夫をこらす。

③継続的な教育・啓発活動

4 おわりに

約 2,100 事業所にアンケートを発送し、350 余りの回答を頂いた。この種のアンケートにしては、非常に高い回収率であり、このことに対してご協力頂いた認証取得組織に対し厚くお礼を申し上げたい。

また、インタビューを快諾頂いた認証取得組織 2 事業所、及び、認証機関 3 団体に対しても厚く御礼を申し上げたい。

本調査は、財団法人ニューメディア開発協会の平成 20 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た。ここに感謝の意を表す。

発行日　平成２１年３月
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5号　新目白ビル６Ｆ
電　話　03-5287-5034　ＦＡＸ　03-5287-5029

調査事業者　情報セキュリティ大学院大学
住　所　〒221-0835　横浜市神奈川区鶴屋町2-14-1

平成２０年度ニューメディアを基礎とする調査研究事業
（情報セキュリティに関するマネジメントシステムの
維持管理についての管理・運用面に関する調査研究）

《概要》

ＵＲＬ：www.nmda.or.jp