平成１８年度ニューメディアに関する調査研究事業

「ＩＳＭＳの維持管理における実態調査」

調　査　報　告　書

《概要版》

平成１９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 目的

ここ数年、情報漏洩事故を起こした企業や組織の管理責任が問われるなど、社会的に情報セキュリティへの関心が高まっている。このような背景の中で、２００２年に始まったISMS第三者認証制度は急速に普及し、２００７年４月９日現在で２,０８４事業所[1]が取得している。

その様な状況の中で、ISMS 認証取得後に業務負荷が増加しただけだとか、ISMS の考え方が組織内に浸透しないと言った問題を指摘されるようになってきた。しかし、これらが一部の認証取得事業所のみの問題なのか、ISMS 認証制度全体の問題なのか、は必ずしも判然としていない。

現時点ではこれらに関連する ISMS 認証取得企業等の調査・研究が行われていないように思われる。

このような状況を考えると、現状を正確に把握することが大切であろう。そこで、ISMS認証取得事業所に対してアンケート調査（以下、本アンケート）を行い、実態を調査することにした。

本アンケートの目的は、問題点の有無を含め、ISMS 認証取得事業所が抱えている問題を明確にすることとした。また、もし問題点が有るならば、それに対する対策案を検討・実施する場合に必要となる情報収集としても考えた。

1.2 アンケートについて

(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 4 つのグループ分析の基礎となる

① 事業所の基礎情報

② ISMS 認証取得作業

③ 認証の運用に関する質問。さらに本アンケートの目的にある問題点を探るために、ISMS 認証の効果を問う質問と想定外の影響や作業増加など回答者が感じる負の部分を尋ねる質問

④ 教育・啓発活動について

これらの質問は、質問ごとの回答を分析することを想定した。また、各種のクロス集計による分析も視野に入れて行った。

(2) 質問項目の概要

質問は３５項目に集約し、回答率の向上を目指した。また、本アンケートだけでなく、

[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。

いくつかの事業所に対してインタビューを予定した。
なお、質問の４グループの概要は以下の通りである。
① 事業者（企業、公共団体等）の基礎情報
事業者の組織の規模（従業員数、資本金）、業種、本アンケートを回答頂く担当者の部門、役職などの属性情報等の質問を 6 問実施した。
② ISMS 認証取得に関連する情報
取得した ISMS 認証の対象範囲（ISMS 認証は事業者の部門単位での取得が可能）、他のマネジメントシステムの導入経験の有無、ISMS 認証の取得目的、取得年数、ISMS 導入によって得た効果・業務への影響等の質問を１０問実施した。
③ ISMS 認証の運用に関連する課題
業務上の負担感、効果を高めるための重点施策、マネジメントレビュー以外の運用に対する経営層の関与、ISMS 事務局の体制・教育、コンサルティング、内部監査に関する事項などの情報の質問を１３問実施した。
④ ISMS に関連した教育
教育の手段、経営層、管理者、一般職員に対する教育の方法、教育頻度、教育を担当する部門、教育以外の啓発活動等の質問を 6 問実施した。

(3) 回答について
回答は選択方式を採用し、回答は原則として無記名にした。また、任意で ISMS 認証に関連する自由形式のコメントの記入も依頼した。

(4) 実施概要
① 期間
２００７年２月の約１ヶ月を回答期間としたが、集計は３月９日（金）までのものを含めた。
② 調査対象
２００７年１月１０日現在、（財）日本情報処理開発協会の WEB に公開されていた 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事業所を対象とした。
一法人で、複数の認証取得している場合は、全取得部門に送付した。ただし、小事業所で宛名が同一の場合は集約した。
③ 回答形式
回答は原則として選択方式であるが、具体的な内容を記す項目も一部にあった。また、自由記入欄を設け、回答者に意見・コメントを求めた。
④ 有効回答数
２６４事業所からの回答を得ることができた。回答率は１８.６％になった。

また自由形式のコメントあるいは回答者の氏名の記入が予想以上の１６２事業所からあった。自由形式のコメント欄は選択肢のアンケート項目を補い、選択肢の回答からは見えない部分を考慮して考えた。

本アンケートの回答数も事前には 10%前後と予想していたが、18%以上の回答があり、通常の情報セキュリティアンケートより遙かに高い回答率になった。

２．回答結果

調査結果から、事業者の基本情報と ISMS の効果に関連した質問の回答結果を示す。

2.1 事業者の基本情報

(1) 資本金

図１に示したが、事業者の資本金額を聞いたもので、自治体や特殊法人等の無回答が７事業所あった。

資本金が 1,000 万円未満の事業者はすくない。資本金 1,000 万円から 5,000 万円未満が 29%、5,000 万円から 5 億円未満が 45%、5 億円以上が 22%となった。

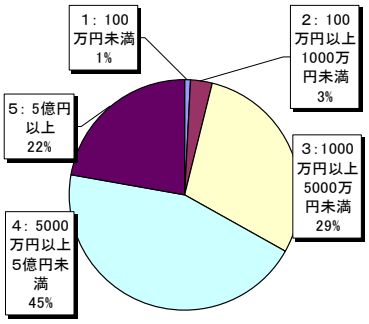

図１　事業者の資本金

(2) 従業員数

図２に示したが、事業者の従業員数は、100 人未満が 33%、300 人未満が 27%で、300 人未満の事業者が 60%となった。1,000 人以上の事業者が 19%あり、ISMS 認証取得事業者は少人数の組織から大規模な組織まで多岐に及んでいる。

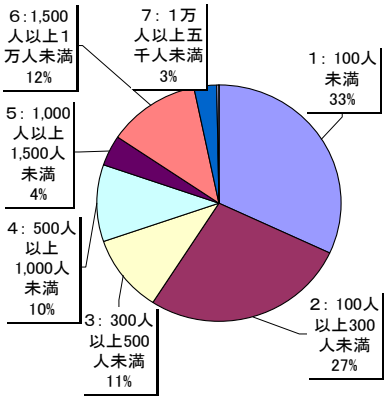

図２　従業員数

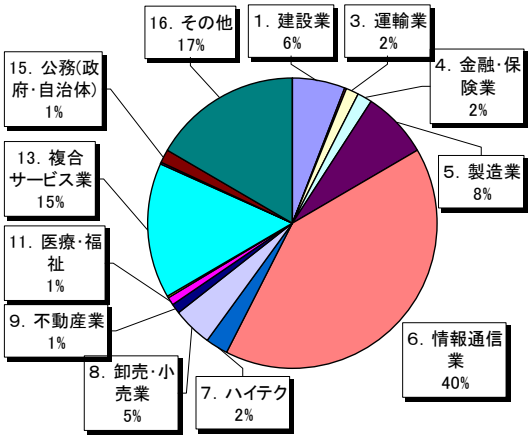

図 ３　事業者の業種

(3) 事業者の業種

図 3 に示したが、情報通信業が 40%を占めており、システム開発やデータ事業などの情報を扱う業務を中心に導入が進んでいる。これは当初、ISMS 第三者認証制度が、情報

サービス産業を対象とした経済産業省「情報処理サービス業情報システム安全対策実施事業所認定制度（「安対基準」と呼ばれていた）」をグローバル化する目的から生まれたことが影響していると思われる。実際には、2002 年 4 月の本格運用からはすべての業種を対象範囲とした。次に多いのが複合サービス業で 13%。複合サービス業は何らかのサービス提供を行うため、個人情報や法人の情報を扱うケースの多いことから ISMS 認証を取得していると考えられる。

(4) 回答者の所属

本アンケートでは、事業所の ISMS 担当者に回答を依頼した。その回答者の所属部門別の割合を図 4 に示した。　情報セキュリティ担当部門が 28%と最も多く、続いて、情報システム管理部門（15%）と情報システム開発部門（5%）を合わせた、システム部門が 20%あった。

情報セキュリティやシステム部門を除く他の部門が 52%を占めており、ISMS 担当は情報システム関連以外が多いことがわかる。

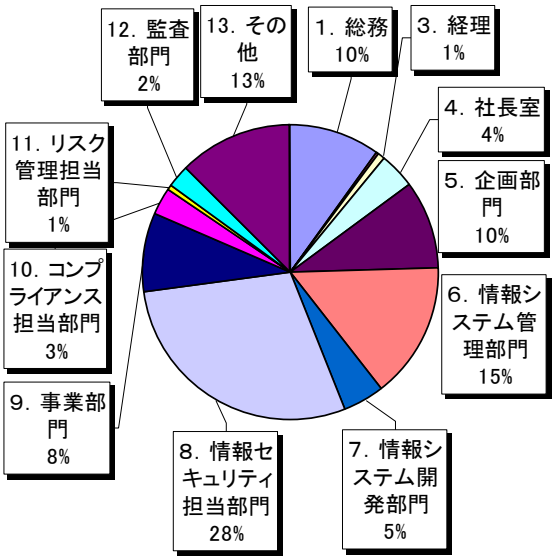

図 4　アンケート回答者の所属部署

2.2 事業所の業務に与える影響

(1) ISMS 認証取得によって得られた効果

1．情報流出や漏洩の防止・軽減
2．盗難や忘失などの防止・軽減
3．セキュリティ事件・事故の減少
4．事故発生時の体制・計画の整備
5．事故発生時の対応時間の軽減・短縮
6．災害発生時の体制・計画の整備
7．情報資産の明確化と整理
8．情報管理計画の明確化と必要な対策の実施
9．セキュリティ関係予算の確保
10. セキュリティ体制の整備と人員確保
11. 経営層のセキュリティへの理解と実践
12. 社員へのセキュリティ意識の浸透と実践
13. 業務記録等の整理と検索性の向上
14. 情報資産の利用・保存状況の改善
15. 特に無い
16. その他

標本数 264

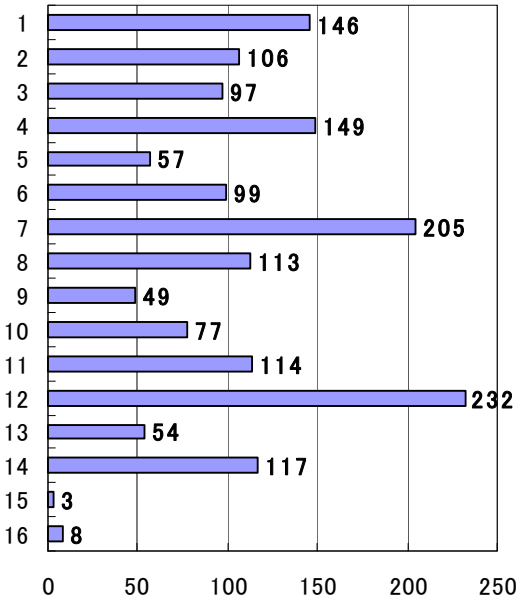

図 5　ISMS 認証取得によって得られた効果

全体的には、ISMS 認証取得の効果を感じている担当者が多いと思われる。

最も多いのは「12. 社員のセキュリティ意識の浸透と実践」の 88%で、次いで、「7. 情報資産の明確化と整理」の 78%となっている。

(2) ISMS 認証取得で発生した想定外の影響

ISMS 認証の想定外の影響について聞いたもので、「1. 情報セキュリティ対策にかけるコストの増加」、「2. 業務量の増加」、「4. 業務上の制約の増加」、「5. ISMS を担当する組織・人が必要になった」が、34～40%の回答率となった。ISMS 認証取得後、日が浅い事業所における運用面での課題が現れているものと思われる。

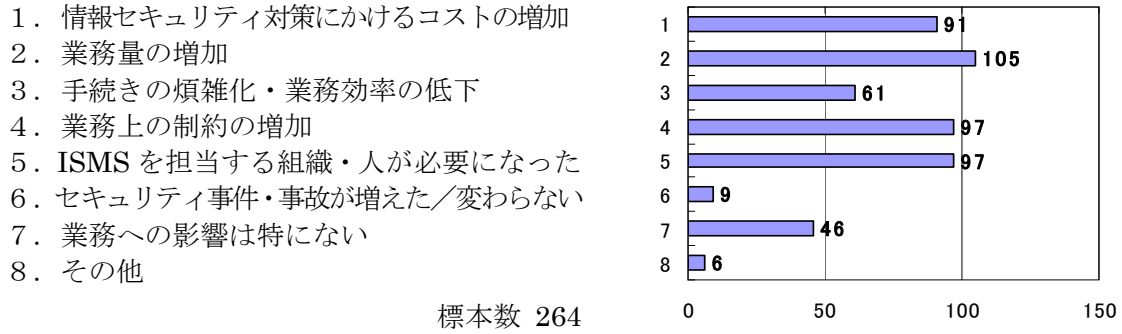

図 6 ISMS 認証で発生した想定外の影響

(3) 上記(2)の設問で、２、３を回答した事業所に、以下のどれが該当するか

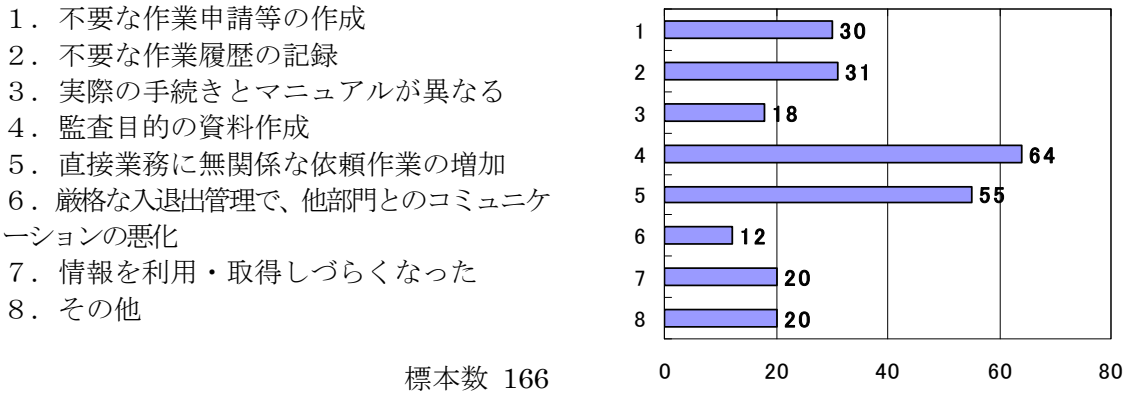

図 7 ISMS 認証による業務量増加･効率低下

上記(2)で、作業量の増加、および手続きの煩雑化・業務効率の低下、を選択した回答者 166 名が回答した。

「4. 監査目的の資料作成」が 38%、「5. ISMS 事務局などからの直接業務に関係な依頼作業の増加」が 33%となっている。内部監査やその他の間接的な業務負担の大きさが感じられる。

(4) 上記(2)で４を選択した場合、ISMS の導入で現場における業務上の制約は？

上記(2)で４を選択した 97 名が回答した。

83%の回答者が「1. 機器の取り扱いに関する制約」をあげている。機器を自由に使えない不便さを感じている。　次に、「5. 上長の承認の増加」が 60%、「4.資料の作成ルール」が 52%と高い回答率で続いている。　これらの項目は組織の管理体制に直接関連しており、また認証取得時に必要であるとして、情報資産管理策を策定したが、実運用で ISMS 担当者がこのように感じているところは興味深い。

１．機器の取扱（含持出･込）上の制約
２．厳格な持ち物検査や入退室管理
３．作業の事前申請
４．資料の作成ルールや保存場所等の指定
５．上長の承認の増加
６．社外での作業の禁止
７．他部門とのコミュニケーションの悪化
８．その他

標本数 97

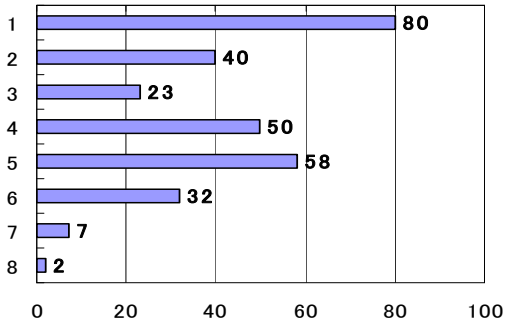

図 8　ISMS 認証による業務上の制約の増加

(5)　ISMS 認証取得後の運用で負担になっている作業

１．セキュリティ委員会の開催
２．ポリシー（含 規定類、マニュアル等）の改訂や記録などの更新作業
３．情報資産台帳の見直し作業
４．リスクアセスメントの見直し
５．セキュリティ教育の実施
６．内部監査対応
７．マネジメントレビューの実施
８．業務とマニュアルの乖離等に起因する認証審査資料の作成
９．事務局と現場とのコミュニケーション
１０．ログのレビュー
１１．特に無し
１２．その他

標本数 264

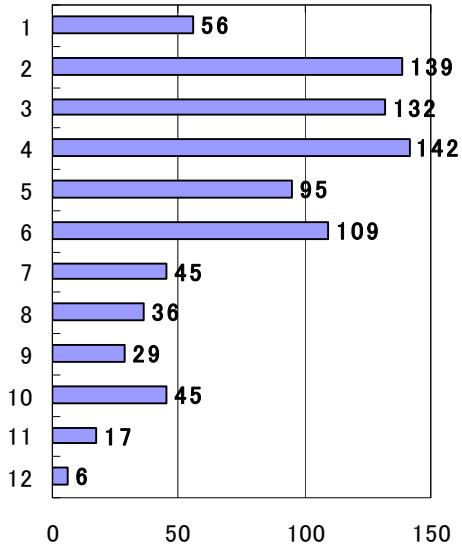

図 9　ISMS 認証後の運用で負担になっている作業

ISMS 認証の運用で、どの様な作業を負担と感じているかを聞いた。いずれの項目も必須なものである。

「2. ポリシーの改訂や記録などの更新作業」、「3. 情報資産台帳の見直し」、「4. リスクアセスメントの見直し」、「5. セキュリティ教育」、「6. 内部監査対応」については、36～54%が回答しており、と高い割合で負担を感じている。

特に、「4. リスクアセスメントの見直し」は 54%と最高の回答となっている。その理由として考えられるものとしては、リスクアセスメントに不慣れ、作業量が大きい、現場に作業を依頼する必要がある等が考えられる。

３．アンケート全体の考察

今回のアンケート調査は、一部の ISMS 認証取得企業から、ISMS を取得したが情報セキュリティ対策との乖離があるとの問題提起があった。　また、ISO9000 等の取得を支援しているコンサルタント等の「ISO 不要論」（内容を精査すると、必ずしも不要論を述べていはいない）的な書籍の出版等から、ISMS の第三者認証制度を客観的に調査することにより、認証取得事業所にとって、ISMS が真に有用なものになるためになすべきことを調べてみた。

アンケートを分析する限りにおいては、おおよそ以下のように分類できる。

① 経営者の情報セキュリティ、ISMS 推進等に非常に高い意識を持っており、事務局（常勤、兼務を問わず）も積極的に推進している事業所
② 経営者の情報セキュリティ､ISMS 推進等への関心がないまたは低い｡このため、推進事務局の努力が報われていない事業所
③ ISMS への誤解。管理策への誤解が多い。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、ISMS を理解していないために、認証取得時に苦労した事業所
⑤ 審査機関、審査員の問題。　審査機関に依存することが多いようであるが、審査員のレベルが低いため、苦労している事業所
⑥ ISMS 独自の問題。　ISMS が JIS Q 27000 シリーズに移行があり、移行期間が短かったため、本来業務の停滞がみられた事業所

この他に、文書化があまり行われていない事業所では、膨大な文書化に苦労している。但し、一過性であり、一度きちんと作成した文書は更新があるが、それでも認証取得時からみると、格段に少なくなっていると回答している事業所も多い。

回答が 20%弱であるが、当初想像した程、多くの問題点を抱えている事業所は多くないように思われる。　これは、比較的うまく運営している事業所からの回答が多かったとか、前向きに回答したとも考えられるが、審査機関において、「審査判定委員会」[2] で

[2] 審査員が審査した内容の報告を受け、認証取得を認めるかを判定する委員会

の状況とそれ程大きく異なる感じは受けない。

４．ISMS 認証制度の実効性を向上させる施策案

考察を基に、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の概要を述べる。

(1) 資料作成の負担を軽減するための施策

①日常的に行う作業の中で、必要な書類が作成・蓄積されるように業務を見直す。
②業務見直しの中で、作成書類についても見直しを行い、不要な書類については積極的にはずしていく。
③計画的な書類作成について、監査を行うタイミングだけでなく、定期的な確認を行い、確実なリマインドをする。

(2) ポリシーやルールによる制約を改善するための施策

①ISMS 認証を取得して期間が浅い場合は、組織に ISMS が浸透するための時間は十分に確保するとともに、普及・啓発活動を並行して実施するべきである。
②計画策定時に十分に現場の意見を吸収する。
③一定期間経過、制約となるようなルールについては、リスクアセスメントの結果を尊重しながら見直しを行う。

(3) コンサルタントの評価制度

①コンサルタントの評価制度を設け、認証取得事業所が参考に出来る様にする。

(4) 教育、普及啓発などについて

①全階層における系統的な研修・教育、啓発機会の確保
②集合研修についての改善とより現場に浸透した研修の実施
・実施する集合研修自体のトータルな実施方法の工夫
・小規模な研修の高頻度の実施の組み合わせ
③普及啓発活動によって情報セキュリティに「親しみやすさ」を持ち込む

５．今後の課題

今回は、ISMS 認証取得事業所の実態調査を中心に行ったが、今後更に、共通の課題を抱えている事業所への対応策等を考えることが可能であれば、実施して行きたいと考えている。

なお、約 1,400 事業所にアンケートを発送し、260 余りの回答を頂き、この種のアンケ

ートにしては、非常に高い回収率になり、ご協力頂いた事業所に対し厚く御礼を申し上げたい。

また、ヒアリングを快く受諾して頂いた 2 社に対しても厚く御礼申し上げたい。

最後に、この調査は、財団法人 ニューメディア開発協会の競輪の補助金によって行うことができましたことを御礼申し上げます。

発行日　平成１９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 内田研究室
住　所　〒221-0835　横浜市神奈川区鶴屋町 2-14-1

平成１８年度ニューメディアに関する調査研究事業
「ＩＳＭＳの維持管理における実態調査」

《概要版》

ＵＲＬ：www.nmda.or.jp