Vol.2009-CSEC-46 No.12
2009/7/2

ISMS 認証取得及びその継続における課題と解決策について

水沼 彩子[†] 澤近 俊輔[†] 新原 功一[†]
鈴木 宏幸[†] 宮本 智[†] 村上 靖[†] 大和田 竜児[†]
小野 康史[†] 星 智恵[†] 内田 勝也[†]

日本における ISMS 認証制度が始まって以来，多くの事業所が ISMS 認証を取得している．一方，ISMS 導入による問題点も指摘されている．
本稿は，ISMS 認証取得組織および ISMS 認証機関向けに行ったアンケート調査の結果を基に，ISMS 導入及び運用で発生している課題を把握し，その解決法について主に管理・運用面から考察を行うものである．これにより，ISMS 認証制度に関する課題と施策案を提案する．

Problems and Solutions of acquiring/maintaining ISMS Certification

Ayako MIZUNUMA [†] Shunsuke SAWACHIKA [†]
Koichi NIIHARA [†] Hiroyuki SUZUKI [†]
Satoshi MIYAMOTO [†] Yasushi MURAKAMI [†]
Ryuji OOWADA[†] Yasushi ONO [†] Tomoe HOSHI [†]
and Katsuya UCHIDA [†]

In Japan, many organizations and companies have acquired ISMS certification since the system started. But some experts pointed out some problems of ISMS implementation.

In this paper, we confirm some problems of ISMS implementation and operation from the result of the questionnaires for ISMS acquisition/certification organizations. Then we confirm some solutions in terms of mainly ISMS management and operation. From these researches, we propose some ideas of measures against ISMS certification system.

1. はじめに

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 認証制度という）は，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（以下，JIPDEC）によって運用されており，2009 年 3 月末時点で，3,000 を越える事業所[a]が認証を取得している．

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，といった声もある．

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〔1〕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．

今回はこの前回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て 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〔2〕を行った．前回調査と比較し，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，課題と解決策を考察した．

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．

2. 調査概要

2.1 認証取得組織向けアンケート調査

(1) 調査対象

2,092 事業所

（2008 年 10 月 30 日の時点で，JIPDEC の WEB サイトで住所等を公表していた ISMS 認証取得組織）

(2) 期間・回答数等

アンケート期間：2008 年 12 月 8 日～2009 年 2 月 27 日

† 情報セキュリティ大学院大学
Institute of Information Security

a)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．

回答数(回答率)：352 通(16.8%)

(3) 回答形式

回答は原則無記名・選択方式とした。また必要に応じ具体的な内容を記すための項目や自由記入欄を設けた.

(4) 質問項目

事業者（企業，公共団体等）の基礎情報，ISMS 認証取得報，ISMS 認証の運用に関連する課題，コンサルタント，ISMS 審査員，ISMS 認証の運用に関連する情報，ISMS に関連した教育・ルールなど，合計 61 項目.

2.2 認証機関向けアンケート調査

(1) 調査対象

23 団体

（2009 年 2 月 3 日現在，JIPDEC の WEB サイトで公表していた ISMS 審査機関）

(2) 期間・回答数等

アンケート期間：2009 年 2 月 3 日～2009 年 3 月 6 日

回答数(回答率)：7 通(30.4%)

(3) 回答形式

回答は記名・選択方式とした。また必要に応じ具体的な内容を記すための項目や自由記入欄を設けた.

(4) 質問項目

当該認証機関の ISMS が占める割合などの基礎情報，実際の審査活動における状況確認としての審査員への教育状況，審査時の指摘事項や ISMS 認証取得の動向など，合計 33 項目.

2.3 認証取得組織に対するインタビュー調査概要

2009 年 2 月に認証取得組織 2 社に対して，主に認証取得組織の現状等のインタビュー調査を実施.

2.4 認証機関に対するインタビュー調査概要

2009 年 3 月に ISMS 認証機関 3 団体に対して，審査機関の基礎情報，審査員，審査時の対応，受審側の対応，審査における付加価値，ISMS 認証取得の動向等のインタビュー調査を実施.

3. 認証取得組織に関する考察

3.1 組織の基本情報

- ISMS 認証取得組織の規模

昨今の経済状況を反映して，資金力の少ない企業ではセキュリティへの投資を回避する傾向が見られる.「1,000 万円以上 5 億円未満」の企業が前回同様，全体の 7 割を占めており，この規模の組織が ISMS 認証を取得する中心的な層である傾向は変わっていない.

組織の従業員数については,「100 人未満」の組織は，前回の 3 割から 4 割弱に増加しており，小規模の組織の ISMS の取得が進んでいることを示している．これは ISMS が事業所単位での取得が可能となっていることから，全社単位ではなく事業所ごとの取得が進んでいるものと思われる.

- ISMS 認証を取得している業種の割合

今回の調査でも，前回同様「情報通信業」が 4 割を占めており，最も大きな割合を占めている．これは経済産業省の安全対策基準をグローバル化して ISMS 第三者認証制度をスタートさせたことや，当初システム開発等の業務をしている組織を対象にしていた経緯が関係していると考えられる.

- アンケート記入者について

アンケート記入者の経験年数については,「1 年以上 3 年未満」で 6 割を超えているが，前回の調査に比べて 1 割前後減少している．一方,「3 年以上 5 年未満」,「5 年以上 7 年未満」,「7 年以上」とすべてのグループで前回調査より増加している．このように ISMS の担当者は異動のサイクルが比較的長く，少なくとも 3 年以上の在籍となるケースが増えている．これは ISMS が専門性を求められる業務であることとも関係していると思われる.

3.2 ISMS 認証取得関連

- 認証取得の体制について

2007 年以降も継続して ISMS を取得する企業が増加している．これは，ISMS 認証が認証取得組織自身にとって有効であり，これまで以上に ISMS が浸透していることを示している．事業者の規模についても，前回と同様に 300 人以下の規模での取得が多く，大規模組織での取得は少ない.

- 認証取得の目的・発案者等について

目的としては，営業活動への影響が最も高かった．これは，発注側の情報セキュリティ対策への関心の高さを示していると思われる．注目すべきは「会社業務の運営を ISMS 認証に基づいた方法にするため」が増加している点である．これは，企業における業務の改善に ISMS 手法を利用するケースが増えているためと思われる(図 1).

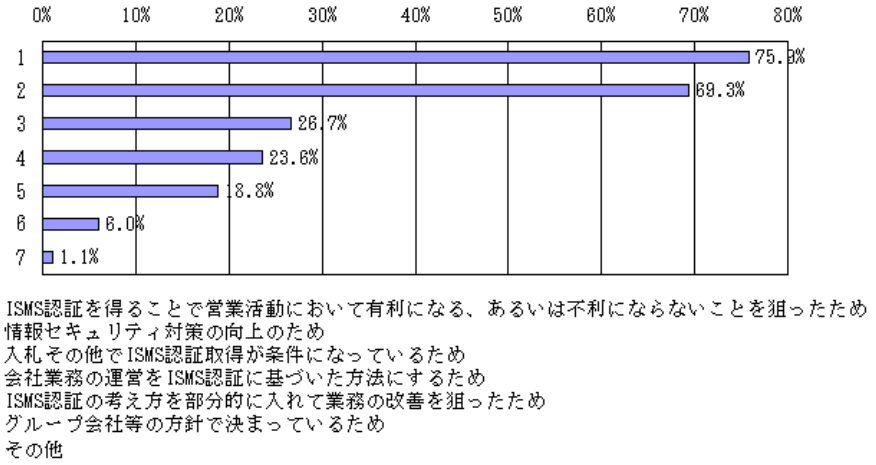

図 1　ISMS 認証取得の目的

認証取得の発案者は，規模に関わらず役員以上の割合が非常に高く，戦略的に ISMS 取得をトップダウン指示で実施しているケースが多いことがわかる．また運用責任者も同様に，役員以上の割合が高い傾向となっている．

3.3 ISMS 認証の効果・影響

● ISMS の効果

ISMS の効果として認証取得組織が感じているものは，「社員のセキュリティ意識の浸透と実践」，「情報資産の明確化と整理」であり，前回調査からは大きく変動していない．これは，ISMS 導入により狙っていた効果が結果として表れているためと思われる．

● ISMS 認証の想定外の影響

業務に悪影響を及ぼしていると考えている認証取得組織は，前回よりも若干減少している．これは自由記述の意見にもあるが，事前にある程度の影響を想定できているものと思われる．

業務量の増加については，「監査目的の資料作成」や「ISMS 事務局などからの直接業務に関係ない依頼作業」が前回同様に多く，PDCA サイクルを回すための作業への理解が，十分に理解されていないように思われる．

一方，業務上の制約としては，「機器の取り扱い」や「上長の承認」など，前回同様，ルールに関連した制約をあげる回答が多かった．これは，情報資産の取り扱いの強化に伴い，それらが直接制約となって表れていると思われる．

● ISMS 認証の運用上の負担，重点取り組み

前回同様，業務改善の継続を負担と感じることが多いことがわかった．また，重点的に取り組むものとしては，前回と同様に「一般社員の認識・理解の強化」が一番多かった．前回調査では，ISMS 取得後間もないことが影響していると考察したが，未だに一般社員への教育について認証取得組織は頭を悩ませていることがわかる．

● 実業務と ISMS の乖離

本問については，全体の約半分が「どちらともいえない」，または「乖離している」と回答している．前述の「監査目的の資料作成」や「ISMS 事務局などからの直接業務に関係ない依頼作業」に負荷がかかっていることからもわかる．ISMS 事務処理の影響で､本来のセキュリティ活動の実業務が十分でないケースも多くあると思われる．

● ISMS 維持のためのコスト

半数が妥当と回答している一方，4 割強が高いと回答している．認証取得組織にとって，ISMS 維持コストは負担となっている．

3.4 ISMS 認証に関連する体制

● 経営陣の関わり方

前回同様，経営陣が ISMS 認証に積極的に関わっていることが伺える．

● ISMS 事務局について

事務局の人数は，前回同様少人数で運営されている．これは，ISMS 認証取得組織の約 6 割が 300 人未満の比較的小さい組織であるため，事務局も少人数で運営されていると推測される．

また事務局メンバーのスキル習得については，外部から内部へとシフトする傾向がある．これは，スキルが内部に蓄積されつつあるとの解釈もされるが，調査全体を見る限りでは専門性があるとはいい難い傾向にあり，運用経費等の削減等のため内部で対応せざるを得ず、このような結果になったのではないかと考えられる。

3.5 コンサルタントについて

コンサルタントの能力や有効性に関する問題点を把握するための質問であり，回答は 10 段階評価を中心に行った．

● コンサルタントの利用について

コンサルタントの利用については，認証取得前に「利用した」「一部利用した」との回答の合計が 8 割を超えている一方，認証取得後「利用していない」との回答が 6 割を超えている．前回調査と同様に，認証取得前はコンサルタントを利用するが，取得後は自ら維持管理する傾向が伺える(図 2・3).

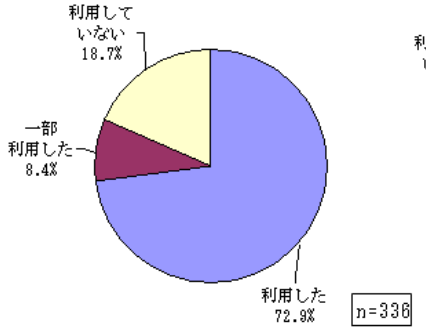

図 2　コンサルタント利用状況
（ISMS 認証取得前）

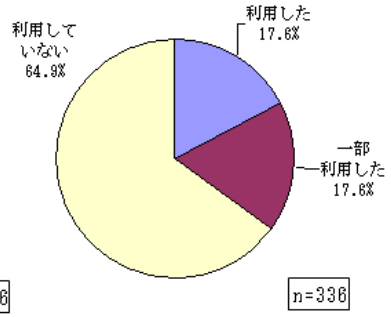

図 3　コンサルタント利用状況
（ISMS 認証取得後）

- ISMS 認証の要求事項，セキュリティ技術への理解度の平均点はそれぞれ 8.4，7.9 であり，おおむね理解度は高いと評価されている．
- 業務に対する理解度について

平均点は 6.9 であり，必ずしも高いとはいえない．5 以下を「比較的理解されていない業種」，6 以上を「比較的理解されている業種」として比較すると，理解されていない割合が比較的高い業種は，「大学以外の教育・学習支援業」，「金融・保険業」，「医療・福祉」．理解の割合が比較的高い業種は，「製造業」，「卸売・小売業」であった．このように，コンサルタントの理解度は業種による差がある (図 4).

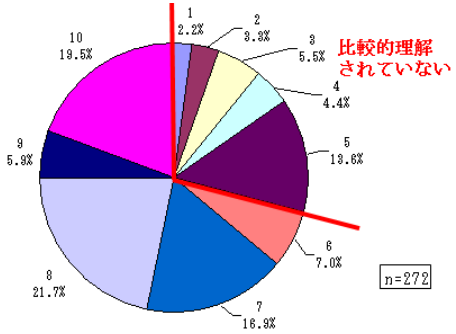

図 4　コンサルタントの業務に対する理解度(10 段階評価)

- コミュニケーション能力及びコンサルティングの有効性について

「コミュニケーション」，「実効性のある提案」，「確立した手法」，「一貫性」は，ともに平均 7 点台の評価を得ている．また，「ISMS 認証を取得する上で役に立ったか」については，平均 8.3 点台の評価を得ている．これらの結果から，コンサルティング能力，およびコンサルティングの有効性については高い評価を得ている．

業務に対する理解度が必ずしも高くないにもかかわらず，有効性の高い評価を得ている背景には，業務に対する理解度の低さを「ISMS に関する知識量やコミュニケーション能力で補っている」，「一部の業種では業務知識を期待されていない」と見ることもできる．

- コンサルティング費用について

「妥当」が高い比率を占めるが，「安い」と比較すると「高い」の割合が大きい．前述の「コンサルタントの利用」が認証取得後に低くなるのは，費用的な要因もあると考えられる．

- コンサルタントの選定理由，導入・選定の最終判断について

コンサルタント選定理由としては，「紹介」「関係会社・取引先」など人脈や組織上の関係が高い割合を占めている．コンサルテーションは形のないものだけに，人的・組織的な関係から選ばれる場合が多い (図 5).

導入・選定の最終判断は，経営陣が行っている割合が高い．これは人的関係の重視と，費用面での判断の双方から経営陣の意向が大きく関わっていると思われる．

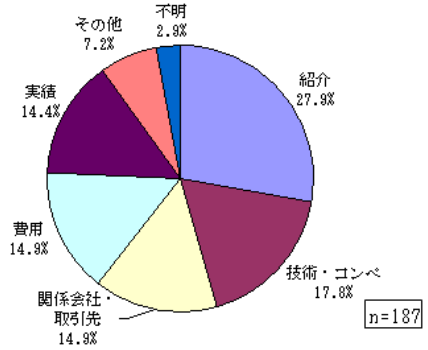

図 5　コンサルタントの選定理由

3.6 ISMS 認証審査及び審査員について

ISMS 認証審査における審査員の能力や審査の質に関して，ISMS 認証自体の質を把握するための質問．回答は 10 段階評価を中心に行った．

- ISMS 要求事項およびセキュリティ技術の理解度について

ISMS 認証の要求事項やセキュリティ技術に関する理解度については，平均点がそ

れぞれ 9.3，8.8 であり，高評価を得ている．

● 業務に対する理解度について

審査員の，組織の業務に対する理解に関する質問については平均 7.7 であったが，回答にばらつきがあり，6 以下の評価も約 21% あるなど，あまり理解されていないとの回答も少なくない．中でも，医療・福祉は業務理解が難しい分野があることが伺えた(図 5).

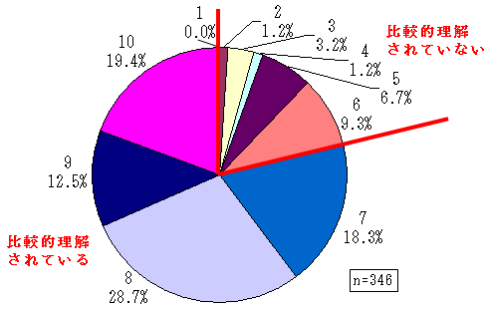

図 6　コンサルタントの業務に対する理解度(10 段階評価)

● コミュニケーション能力及び審査での指摘について

「審査員のコミュニケーション能力」「実効性のある指摘」「組織に対する効果や課題の確認」の平均はいずれも 8 点を超えており，高評価であった．ただし，先述の業務の理解度の結果を考慮すると，コンサルタントと同様に ISMS 審査員も，業務に対する理解度の低さを ISMS に関する知識量やコミュニケーション能力で補っていると見ることもできる．

今後 ISMS の更なる普及を進めるにあたり，審査員自身もが業務に対する理解を深めていくことが重要であると考えられる．

3.7 内部監査・マネジメントレビュー

● 内部監査体制について

前回調査と比べると，内部監査体制については常設の社内チームの構築が進んでいることが伺える．

● 内部監査指摘事項に対する改善について

内部監査指摘事項に対する改善作業は，約 9 割が実施しているとの結果になった．前回の調査では「事務局に改善作業を行う余力が無い」との回答が半数を超えていたが，指摘事項に対する改善は、「重欠点」と指摘される可能性もあるため、その重要性が理解され，改善作業が行われるようになったと考えられる．

● マネジメントレビューの実施方式

マネジメントレビューの頻度は「半年に 1 回」と「1 年に 1 回」の合計が約 92%を占めた．「3 ヶ月に 1 回」及びそれよりも短期間の頻度で実施している組織は，6%となった．この傾向は前回調査と大きな変化は無い．

3.8 教育

● 教育実施形態

いずれの職位においても，「集合研修」が上位に位置づけられている．特に一般社員向け教育では全体の 8 割以上を占める．また，「冊子の配布」や「OJT」が次に続くことから，集中教育と継続教育を併用して実施していると考えられる．

ただし，年間 1～2 度行う「集合研修」において集中して受講できるか，あるいは個人で受講する場合は最後まで理解できたかを確認することは困難であり，それぞれの実行にあたっての有効性を評価する手段については，検討の余地があると思われる．

「その他」の記述欄においては，外部研修を受ける旨の記述が目立った．これは各人のレベルに合わせた研修を選び，受講できる意味で非常に有効であると考えられる．

● 職位との関連

前回に続き，一般社員，情報セキュリティ管理者・推進者，経営陣の三階層についてアンケートを実施した．最も特徴的なのは「特に行っていない」割合が，階層が上がるにつれて増加している．このことは、情報セキュリティに対する経営陣自身の意識の低下が懸念される．なお，この傾向は前回調査でも同様であった．

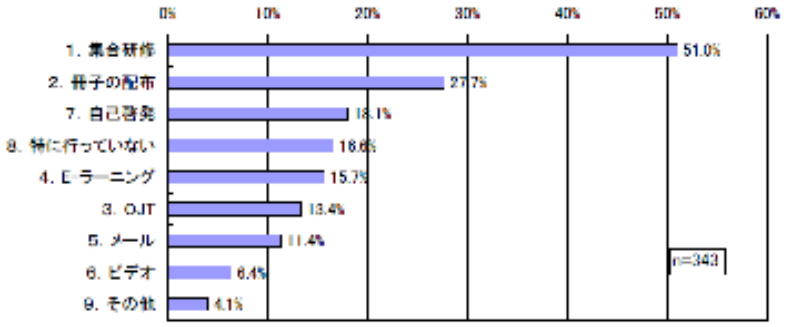

図 7　経営陣に対する教育機会

● 教育の担当部門とレベル

「情報セキュリティ担当部門」が最も多く，さらに「総務部門（人事・経理含む）」「情報システム管理部門」と続き，前回と類似した結果が得られた．

教育レベルは，全体の 6 割程度が概ね 7 点以上と判断しており，特に「社外」は高レベルであった．しかし，少数ではあるが，教育レベルが 1～3 点と判断しているケースもある．この場合，教育担当部門、教育内容等全体的な見直しを行う必要があるのではないかと思われる．

● 啓発活動

今回，啓発活動を行う場として「会議での通知」と「web コンテンツの掲載」を追加したが，それぞれ 57%，30%と高い回答があった．カリキュラムを組む集合研修とは別に，日常的に行う会議や， web の利用が啓発活動を行うのに適切であると考えられる．また，前回同様，啓発活動にはあまり費用をかけない傾向が見られる．

3.9 社内ルール

● 業務用 PC からの情報漏洩対策

業務用 PC からの情報漏洩対策として実施している対策は,「ログインパスワード認証」が約 95%,「ログインパスワードの定期的な変更」が約 81%という結果であり，広く浸透していると考えられる．

また，PC の盗難・紛失等のリスクに対する対策として,「保存ファイルの暗号化」,「BIOS パスワードの設定」,「ハードディスク暗号化」は約 3 割が対策を行っているが,「シンクライアント」の導入は 1 割にも満たなかった．

● PC，媒体の社外持出に関するルール

社外持出について定められたルールについては, PC と媒体の間に差はほとんどない．PC は約 88%，媒体は約 79%が「ルールあり（持出許可必要）」と回答している．

● 社内持込あるいは，利用制限

ノート PC，外部記録媒体共に，約 8 割が社内持込あるいは，利用を制限していた．また，携帯電話の持込制限は約 16%で，ノート PC，外部記録媒体から比べるとかなり低い．

3.10 自由意見欄

● 自由意見欄について

PDCA サイクルが回ってきたと手ごたえを感じているとの意見がある一方，負担増になっている，本来の目的が形骸化しているなどの意見も多く，導入年数や企業規模により，ISMS 取得による効果に対する意見には差がみられた．また，ISMS 取得によりセキュリティの向上は図られたが，今後は業務改善のツールとしても活用していくことが課題であるとの意見などから，業務改善に向けた取り組みへの努力が必要と感じている．さらに審査員同様，コンサルタントについての質のばらつきを指摘する意見も複数あった．コンサルタントの選択によっては ISMS 構築後の品質が左右される可能性がある．

● 意見の区分について

自由意見欄を区分すると，情報セキュリティに対する対策，監査，教育についての意見が多く見られた．特徴的な意見としては，審査員のレベルに差がある，意見の押し付けが見られる，尊大な態度の審査員がいるなど，審査員の資質に対する疑問を呈する意見も多い．これに関連し，審査員評価制度の確立が指摘されている．

● 他認証との関連について

セキュリティ関連として，プライバシーマークに関連したコメントが他認証に対するコメントの中で半数以上を占めた．QMS については取得組織が多く，認証の進め方・定常活動に類似点が多いため，同様の考え方で進めているというコメントが複数あった．

情報セキュリティに関する資格は，ISMS，プライバシーマーク，情報セキュリティ格付け制度など混在しており，担当者レベルでは 1 つを選択できないためか、これらの作業量が増えており統一化してほしいとの声も聞かれた．

3.11 アンケート全体からの分析

アンケートの結果から，ISMS に関連する組織や制度についての問題点として，主に以下の点を挙げることができる．

① 経営陣の情報セキュリティ，ISMS 推進等への関与が大きいことは望ましいが，経営陣の誤った考えで方向性が変わることもあり，経営陣への啓発活動も重要な課題である．

② 管理策への誤解が多い．認証取得組織の状況に応じて，管理策の適用除外や追加の管理策で更に高度なセキュリティを構築してもよいことを理解していない．ISMS 導入時の規格への誤解もあるが，コンサルタントの不適切な指導や審査員の不適切な審査などが原因と考えられる．ISMS 担当者は，時間の経過，環境の変化によるリスクを適切に把握し，適切な管理策を見直していく必要がある．

③ コンサルタントの利用も慎重に検討する必要がある．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ことがある．特に業種によっては理解度にばらつきが見られる傾向があった．コンサルタントは ISMS 知識を深めつつ，認証取得組織の業務を理解する能力を高めることも必要である．レベルの低いコンサルタントは，認証取得の障害になったり，認証制度の発展の阻害要因になる．コンサルタントの登録制の導入なども検討の余地がある．

④ 経営陣等との関係から，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．コンサルタントの決定については十分な事前調査を実施し，費用対効果も鑑みつつ信頼できるコンサルタント選びを行うべきである．

⑤ 認証機関や，審査員に問題があると感じている認証取得組織もある．コンサルタ

ントと同様，業種にもよるが認証取得組織は，十分な事前調査やコンサルタントとの相談を行い，慎重に認証機関を決定する必要がある．認証機関の決定を入札制度で行うことや，認証取得後も審査員，認証機関の変更や苦情を認証機関，認定機関に訴えることもできるので，これらの利用も考慮していくべきである．

3.12 インタビュー全体からの分析

インタビューの結果から，ISMS についての認証取得組織の取り組みかたとして，主に以下のような傾向があると考えられる．

① 認証取得のきっかけに関しては，経営陣の意向が大きく反映される傾向がある．
② いずれの認証取得組織もプライバシーマークの取得も検討していたが，最終的には経営陣の判断で，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い自組織での必要性を勘案したうえで，ISMS を導入する傾向があると考えられる．
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，審査の不十分さ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．

4. 認証機関に関する考察

4.1 アンケート全体からの分析

アンケートの結果から，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考えられる．

① 審査対象組織の専門性に関し，得意分野が存在する傾向がある．
② 審査活動向上の取り組みとして，審査員教育やその力量の指標について確認した．10 段階評価において，審査員が持つべき力量に関し，全ての項目に渡って重要度の高い 9～10 点を選択するケースと，一部の技術や知識については 5～6 点を選択するケースが見られた．認証機関によっては保有すべきと考える力量の分野にばらつきがあることがわかる．また，認証取得組織に対する情報発信はほとんどの認証機関が行っていたが，コンサルタントに対する直接の情報発信は半数以下に留まった．認証機関によっては，コンサルタントとの距離の置き方には差があるものと考えられる．
③ ほとんどの認証機関で審査が不適合であるとして，認証を保留しているケースがある．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．判定委員のメンバー構成については，内部のみ・外部のみ・それぞれ混在といったケースが均等にちらばり，目立った傾向はみられなかった．現時点では，認証取得組織に対して，認証保留，停止等があっても，公開されることがないため，その経緯が第三者にはわからない．業界として，統一的な仕組みの構築が必要と考える．
④ 今後の傾向として，今年以降の ISMS 認証取得要求度合いは，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．また，セキュリティ格付けについては半数が肯定的な見方であったが，抵抗も一部見られた．

4.2 インタビュー全体からの分析

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いうことができる．

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る．特殊な専門性を持った審査員の手配に腐心するというコメントも得られた．幅広く専門知識を持った審査員の育成にも注力していると考えられる．
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 内部メンバーのみで判定委員会を構成する場合は，ベテランを配置し公正を期しているとの回答であった．ただ、第三者認証制度の考えからは若干ずれがあるようにも感じる．
④ 公正な審査を行って適切にマネジメントシステムを運用させるため，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．
⑤ 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．

5. ISMS 認証制度の実効性を向上させる解決策について

3 章，4 章の考察を元に，ISMS 認証制度を導入・運用するときの実効性を向上させる解決策を検討する．

(1) 自組織に対する ISMS の意義の再認識

ISMS 認証取得について，取得自体を目的としているため，本来の目的が見えなくなってしまう傾向がある．

認証取得組織は ISMS 取得の意義を再認識した上で、社内の体制を確立するべきである．ISMS が正しく認識されないままであると本来の業務に悪影響を及ぼす矛盾が生じる可能性もある．認証取得組織は，必要に応じて管理策を更新するなど常に見直しを図る必要がある．更に,政府・自治体等は ISMS 認証取得を入札条件の一部に組み入れているが，QMS 等での弊害を考えると入札条件から外すべきであろう．

(2) コンサルタントの評価制度

ISMS 導入時にコンサルタントを利用する認証取得組織が多い．利用するコンサルタントの良否は，その後の ISMS の適用においても大きな影響があると思われる．しかし，このコンサルタントの情報やその評価の情報が十分共有できていない．認証取得組織側，特に，初めて ISMS 認証を取得しようとする組織は，コンサルタントの情報収集に苦労していると思われる．公平に評価されたコンサルタント情報を，認証取得を行う組織が容易に取得できるような仕組みが必要と思われる．

今後，ISMS 制度が普及するに従い，コンサルタントも淘汰され，認証取得組織に対し,適切なアドバイスのできるコンサルタントのみが生き残ることになるであろう．

(3) 認証機関のレベルアップ

認証機関については概ね適切であるとの回答を得ているが，不満のある認証取得組織もやや見られた．

これについては，認証機関と認証取得組織の双方に問題があるとも考えられる．業務に対する認識の相違や，認証取得組織側が ISMS 制度を誤解している場合，さらに認証機関によっては得意分野や経験豊富な業界等が存在するためである．しかし,「審査員によって指摘の内容や表現が違う」，といった意見もあり，統一性のある審査ができないという実態もあるようである．

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努めねばならない．また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と考えられる．

(4) 経営トップ層に対する教育，啓発

ISMS を維持・向上していく上で，教育および啓発は不可欠であると考えられる．

前回調査でも指摘したが，上位層ほど教育の機会が少なくなる傾向がある．経営陣は多忙であるが,ISMS 運用の成功の経営トップの十分な理解が必要であると言える．経営陣に情報セキュリティや ISMS に関する知識が不足していれば，効果的・効率的に ISMS の運用ができなくなる可能性がある．また，ISMS の実現によって内部統制を確立していくには，経営陣の高い意識・モラルの維持が重要になる．

6. おわりに

ISMS 認証制度は，ISMS 認証取得組織，コンサルタント，認証機関など，それぞれが，様々な課題を抱えている．今回、我々はアンケート調査及びインタビュー調査の結果を元に,ISMS 認証制度の実効性を高めることに寄与する施策案の提案を行った．

今後も調査を継続して実施し，データを蓄積することによって，時代にあった提言を行っていきたいと考えている．

謝辞

約 2,100 事業所にアンケートを発送し，350 余りの回答をいただいた．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いただいた認証取得組織に対し厚く御礼を申し上げたい．

また，インタビューを快諾いただいた認証取得組織 2 事業所，及び，認証機関 3 団体に対しても厚く御礼申し上げたい．

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 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．

参考文献

〔1〕 財団法人ニューメディア開発協会．
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」，平成 19 年 3 月

〔2〕 財団法人ニューメディア開発協会
平成 20 年度ニューメディアに関する調査研究事業「ISMS(情報セキュリティマネジメントシステム)第三者認証制度及びその実態調査」，平成 21 年 3 月