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

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

～　目次　～

1 はじめに

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、ISMS認証は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等の話が課題として出てくるようになった。しかしこれらが一部事業所のみの局所的な話であり全体としては特に問題ではないのか、逆に実は ISMS 取得企業の多くが何らかの同じような問題に直面しているのかは判然としない。

現時点ではこれらに関連するような課題の調査や研究はほとんどみられない。そこで、ISMS 認証取得事業所に対してアンケート調査（以下、本調査）を行うことにした。

本調査の目的は、ISMS 認証取得及び運用に関連して何か課題が発生しているのか、そうならば、それはどのような課題なのかを明確に把握することである。さらに課題が有るならば、それに対する対策案を検討するために、本調査の情報を活用したいと考えた。

本調査では、ISMS 認証取得企業を対象に、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、技術だけでなく、管理・運用面からの考察を行い、課題と施策案を述べる。

ISMS 第三者認証制度についていろいろな議論が有る中、本調査の結果から抽出した課題とその解決策は、ISMS 第三者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る。

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　アンケート調査の調査内容

先に述べた本調査の目的に沿って質問項目の作成を行った。質問は分析の基礎となる事業所の基礎情報を最初に置き、次に ISMS 認証取得に関連する作業への質問、続いて認証の運用作業に関連する質問が続き、最後に組織のなかでどのように ISMS についての教育・啓発活動を行っているかの質問とした。

さらに調査の目的にある課題を探るために、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を加えた。

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て作成してあるが、さらに基礎情報と認証維持作業に関する回答を組み合わせるなどのクロス集計による分析も可能である。

検討段階では質問数が100項目近くになった。質問を合体したり削除したりすることで、質問数を35に集約・削減した。この質問数削減の狙いは回答率向上であり、必須の作業であったが、その結果、細部を問う質問がなくなった。これを補うために本調査後にいくつかの事業所に対してインタビューを予定することにした。

質問は4つのグループに分けることが出来る。それらの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

事業所の組織の規模（従業員数、資本金）、業種、本調査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 認証は事業所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 アンケート調査について

(1) 概要

① 期間

アンケート発送　　2007年1月31日（水）
アンケート回答締め切り　　2007年2月28日（水）
※実際には3月9日（金）までに戻ってきた回答を集計した。

② 調査対象

2007年1月10日において、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 認証を取得した1907事業所を対象とした。

これらの事業所の情報を精査し、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1422事業所を選別して最終的な調査対象とし、その事業所の ISMS 担当者宛てに送付した。うち1通が宛名不明で返送されたため、最終的には1421事業所となった。

③ 有効回答数

最終的に計上した2007年3月9日時点で、264通の回答を得た。回答率は18.6%であった。

④ 回答形式

アンケートの質問がセキュリティに係わる分野であることなどから、回答者にとって答えにくい部分が含まれていると考え、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有った場合は、未回答または不明として処理した。

回答は原則として選択方式であるが、必要に応じ具体的な内容を記す項目も一部に設けた。それらの回答とは別に、アンケート解答用紙裏面には自由記入欄を設け、回答者に意見・コメントを求める形式とした。

⑤ 結果の取り扱い

集計結果については、個別企業名や担当者名の特定ができないよう配慮しまとめることとした。また、連絡のために記載された企業所在地、担当者名などは公表しないこととした。

(2) 特徴

アンケート全体としては以下のような特徴が見られた。

- 高い回答率

  これまでに中央大学などで行ったセキュリティ関係のアンケート調査においては、回答率は10％程度の回答率のものが多かったのに比して本調査の回答率は、18．6％という高い回答率となった。

  これは、調査対象とした ISMS 認証を取得している事業所にとって、本アンケート調査が扱っている課題への関心が高いものであることを示しているとも考えられる。

- 自由意見及び記名付き回答の多さ

  今回のアンケートは無記名方式としたが、アンケート裏面には、自由意見欄を設けるとともに、回答内容についての問い合わせやインタビューの依頼などの連絡用として任意での、氏名及びメールアドレス欄を設けた。

  最終的には、回答した企業の過半数（約 61%）が意見もしくは連絡先を記入する結果となり、やはりアンケートで取り上げた課題への関心の深さを表している。

  意見のなかには、フィードバック等を求める声も多く、何らかの改善策を求めている企業の多さを物語っているともいえる。

4 総合的な考察

(1) 組織の基本情報

- ISMS 認証取得事業者の組織の規模

資本金が1000万円未満の事業者3．9%と少ない。1000万円から5000万円未満が29%、5000万円から5億円未満が45%で合計74%となった。この規模の事業者が ISMS 認証を取得する中核的な層をなしている。また資本金5億円以上の事業者は22%となり、大規模な事業者も積極的に ISMS 認証を取得しているといえる。 地方自治体や法人などは7事業者であった。

続いて事業者の従業員数についてである。従業員数が100人未満の事業所が33%、300人未満が27%となり、合計で60%が300人未満の事業者となった。一方では1000人以上の従業員をかかえる事業者も合計で19．5%もいる。

資本金と従業員数でその事業者の規模がおおよそ推測できる。資本金と従業員数の情報から、ISMS 認証は事業者の規模を問わず取得されていると考えられる。

- ISMS 認証を取得している業種の割合

調査の結果で特徴的なのは情報通信業が40%を占めていることだ。これは経産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と当初システム開発等の業務をしている事業所を対象にしていたためと考えられる。なお現在、ISMS は業種を問わず適用できる。

次に多いのは13．複合サービス業で、これは個人情報を扱うことの多い業務を含んでいると考えられる。その他の業務は多少の差はあるものの、ほぼ平均的に散らばっている。

- アンケート回答者の所属部門と役職

一番多かったのは情報セキュリティ担当部門の28%で、ISMS 事務局を含む情報セキュリティの専任者の割合が読み取れる。また、情報システム管理部門と情報システム開発部門を併せると20%となり、システムの管理、開発に携わる人員が ISMS 認証の管理に関わっていることを示している。これも ISMS 第三者認証制度の経緯が影響していると考えられる。

これ以外では企画部門と事業部門がそれぞれ10%、8%となり、若干割合が高い。それ以外の部署は概ね分散している。情報セキュリティ選任でもシステム関連でもない部署が担当する割合を合計すると52%と約半数を占める。

アンケート回答者の役職で最も多かったのは、部長、課長クラスの中間管理職で合計が52%をしめた。また係長・主任を加えると62%を占め、組織を動かす実務者が担当していることがわかる。特徴的なのは、1．会長・社長・役員、2．執行役員を合わせると16%を占めていることで、ISMS 認証の責任者として役員クラスも積極的に参画している事業所も多いことを示している。

それでは認証制度が開始されて5年目の ISMS であるが、今回のアンケート回答者はどのくらいの経験を持っているだろうか。調査の結果、主力は2．1年以上3年未満で、58%に達した。ISMS 第三者認証制度が2002年に始まったことから上記のように経験年数の短い担当者

が多いのだろう。また企業の人事異動の影響受けて、担当者が定期的に交代している可能性も高い。一方5年以上担当している人の合計も7%となり、長年担当が固定になっている事業所も見受けられる。

(2) ISMS認証取得関連

- 認証取得の範囲について

認証取得範囲の従業員数と基本情報である全社従業員数を比較した際に、100 人以下の規模での認証取得と運用がされているとの回答が多数である。これは、ISMS(ISO27001)の認証取得の特徴である、認証取得の範囲を取得目的にあわせた明確な境界を定義することで、取得事業所自身で範囲組織、範囲業務を定義することができるためであると考えられる。

リスクアセスメントや運用マニュアルの策定などの実運用上は、範囲を特定して構築、運用ができることはメリットがあるが、同企業、組織内の適用範囲外組織との運用上のギャップなどが、インタビューやアンケートの記述式回答の結果からも伺える。

認証取得範囲内でセキュリティ対策を十分に行ったとしても、適用範囲外との情報の交換時が、ある種のセキュリティ・ホールとなってしまう可能性もあり、範囲外の組織に対してもセキュリティ基本方針の理解や、具体的なセキュリティ運用手順遵守の理解を求めていくことが肝要であると考えられる。

- ISMS 取得の目的と発案者

2005 年 4 月の個人情報保護法の完全施行も追い風となり、情報セキュリティ対策の必要性が企業や組織に浸透しはじめたことから、企業のビジネス戦略のひとつとして情報セキュリティ・マネジメント・システムへの取り組みをトップダウンで指示した企業が数多く存在したことが取得年数や発案者、運用責任者に関する設問の回答から伺える結果となった。

- 他認証の取得状況について

半数以上の企業、組織が品質、環境などの他認証を取得しており、マネジメントシステムを活用することによる営業戦略上の業務改善への期待が高いことが伺える。

ただし、企業内にマネジメントシステムが複数存在することによる、審査対応などの業務負荷も課題としてあげている企業も存在し、今後のマネジメントシステムの統合などを進めることでの負荷軽減などへの取り組みが求められると考えられる。

さらには、個人情報の保護を目的としたプライバシーマーク認証を同時に取得している企業も全体の 25 パーセント存在することから、認証を取得した目的に相違があるのか、構築アプローチ、マネジメントシステム運用上の課題の有無などは、今後の調査として興味深い点である。

(3) ISMS認証の効果・影響

- ISMS の効果

ISMS の効果はどの程度出ているのだろうか。調査で、一番多かったのは社員のセキュリテ

ィ意識の浸透と実践、次いで情報資産の明確化と整理、となった。これらは一般的な ISMS の効果の印象と合致する。また多くの認証取得事業所が複数の ISMS の効果を感じていると回答しており、情報セキュリティ体制の確立という観点から ISMS にはその効果があると考えてよいだろう。

- ISMS 認証の想定外の影響

ISMS 認証を取得したことによって、業務に何らかの良くない影響を受けていると考えている事業所は8割強に達する。これからISMS認証の取得によって全体に作業量が増える、業務上の制約が増える等の状況が実際に起きていることを示している。

原因については別途詳細な検討が必要だが、例えば認証取得作業中に取得後の運用の検討が十分なされていなかった可能性が考えられる。取得時にはコンサルティングを受けるケースが多いが、コンサルタントがこれらの状況について適切に説明、検討を行っているか確認する必要もあるだろう。

それでは具体的にISMS認証に絡んだ作業量の増加、および手続きの煩雑化などはどのような作業で感じるのであろうか。調査では「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」などの指摘が非常に多い。

これらは PDCA を回すための作業であり、ISMS 認証を取得することで新たに発生した作業を負担と感じるケースが多いようだ。ISMS の理解を組織に浸透させるとともに、PDCA を回す作業負荷を軽減する対策を検討したい。

また、業務上の制約が増加したケースでは、8割を超える事業所が「機器の取り扱いに関する制約」を指摘した。機器を自由に使えない不便さは日頃業務を進める中で直接感じることが多いのであろう。

他にも多くの制約の指摘があったが、ISMS 認証取得後の期間が短い事業所も多いことを考えると、「慣れ」ることで解消される可能性も高い。それでも解消されない制約はルールの見直しやシステムの導入など効率向上の対策を取るべきであろう。

- ISMS 認証の運用上の負担感

一旦取得した ISMS 認証はその運用を通じて PDCA 活動を推進し、業務の改善を続ける必要がある。この ISMS の運用についても負担と感じる事業所が多い。

運用に関連する作業として、「ポリシーの改訂や記録などの更新作業」、「情報資産台帳の見直し」、「リスクアセスメントの見直し」、「セキュリティ教育」、「内部監査対応」について、いずれも作業項目として必須のものばかりだが、負担感が高いという結果になった。

- ISMS 関連作業で重点的に取り組んでいる項目

各事業所で ISMS の効果を高めるために重点的に取り組んでいる作業を聞いた。最も多かったのは、「一般社員の認識・理解の強化」である。続いて「有効性評価手法の改善」であった。これは ISMS が ISO/IEC27000 にかわり有効性評価が厳しくなるとの話に対応した動きといえよう。

ISMS 認証を取得して、時間が経っていない企業も多いことから、一般社員への教育は定番として取り組んでいる様子であるが、次の一手は各事業所によってばらついているといえる

だろう。

逆に少ないのは「費用対効果の説明手法」で、ほとんど取り組まれていない。ISMS 関連費用の経営陣への説明は難しいのではと考えていたので、この結果は意外であった。

また「経営者の認識・理解の向上」についても平均以下の取り組みであった。経営陣の認識向上は重要で有るはずだが、これについては教育についての質問結果と合わせて今後考察していきたい。

(4) ISMS認証に関連する体制

- 経営陣の関わり方

ISMS 認証を維持するためには経営陣の協力が必要不可欠であるが、多くの企業で経営陣の積極的な関わりがあることが確認された。これは ISMS 認証の運用責任者の 77%が役員以上であることからもわかるように、ISMS の取組みが経営課題の一部として認識されていることを示している。

- ISMS 事務局について

ISMS 認証の事務局の人数は 3 人以下が約 6 割を占めており、全体的に少人数で運営されている実態が明らかになった。また事務局の体制としては、兼務担当者が中心に構成されており、専任担当者のみで運営されている企業は全体の 14%に留まった。

特に小規模な事業所は、予算等の都合により専任の組織・担当者を配置することができず、事務局担当者（兼務者）の負荷増大を懸念する声もある。中には「事務局担当者（全員が兼任）の負荷が高く、ISMS の質が低下する恐れがある」との意見もあり、事務局の要員確保が ISMS 認証を維持する上での課題になっていることが伺える。

- コンサルタントについて

外部コンサルタントの利用については、認証取得までに「利用した」と回答した企業が全体の 8 割を占めており、多くの企業が ISMS 認証を取得するためにコンサルタントを利用したことがわかる。

とりわけ、認証取得範囲内の自社要員に IT 技術者がいない場合や、専任担当者を配置することができない小規模の会社では、コンサルタントを利用しないと認証取得そのものが難しいという意見もあり、コンサルタントの必要性が高くなっている現状が伺える。しかし一方では「コンサルタント費用の負担が重い」、「コンサルタントのレベルが低く、システム作りが大変だった」などの意見もあり、必ずしもコンサルタントを利用した方が良い結果を生むわけではないようである。

(5) 内部監査・マネジメントレビュー

- マネジメントレビューと内部監査の実施頻度の相関関係について

マネジメントレビューの頻度と内部監査の実施頻度を比較した場合、回答の分布がほぼ一致していることが判明した。

マネジメントレビューと内部監査の実施頻度については、1 年に 1 回という頻度が半数以上となり、半年に 1 回以上を含めると大多数を占めた。逆に 3 ヶ月以内の短期間は少数派である。

- 内部監査体制について

内部監査体制は大多数が社内チームで構成されており、外部機関を利用するのは少数派となった。その中で過半数を占めたのが非常設の社内チームである。これから内部監査の担当者は兼務者が多いことが伺える。

- 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、9割以上が実施されているという結果になった。さすがに、改善作業を行っていないという事業所は皆無であったが、一割弱の事業所は、改善作業を一部のみ行っていると回答した。その理由として、現場や事務局に改善作業を行う余力が無いという点が指摘されている。

- マネジメント・レビューの実施方式

マネジメント・レビューの実施は電子メールを用いて実施することはなく、担当者が集合する会議形式が中心となっていることが判明した。このことから、マネジメント・レビューの重要性を企業は認識しており、電子メールという簡素化した形式ではなく、手間が発生する会議形式の実施として回答に反映されているといえる。

会議の実施は電子メールでの実施より運用や管理など人的な負担は大きいといえる。しかし、人的負担が多くなっても、会議形式の重要性からほぼ全ての企業が実施しているといえる。

(6) 教育

- ISMS 認証維持のための教育

ISMS 認証の維持において行われている教育については、一般的と思われる集合研修が、いずれの職位においても上位を占める。

2 番目に多かった冊子の配布は、少々興味深い結果ではあるが、教育頻度について、年に 1 回から 2 回が全体の半分程度を占めることを考えると、集合研修によって、きっかけを作り、冊子などの配布によって継続的な効果を狙うというシナリオが考えられる。

また、集合研修が多いことは、その実施のしやすさや、業者などによる対応がしやすいこととともに、外部の講師を招くとしても、費用対効果が高く、実施の成果を人数で表現できるからであろうと考えられる。しかし、一方で、各個人のレベルにあった研修がしにくく、その場限りもしくは短期的な効果のみにとどまると言った集合研修のデメリットについては特に工夫が見られていない。

自由記述欄においては、そのデメリットを効果的に補完するような取り組みの記述を期待したが、残念ながらそのような記述は見られなかった。これは、実際に多く行われている集合研修に改善の余地があることを示している。集合教育の効果を上げられれば、教育自体の実効

力をあげることができるということにもなる。

- 職位別の教育状況

職位別の教育状況の把握において、特徴的が出たのは、職員、管理職、役員と職位があがるにつれ、教育の手段総数も、それを行っていないという回答数も増加していることだ。

半ば予測された結果ではあるが、情報セキュリティ教育は、質的な差を設ける必要こそあるが、その機会においては、どの職階にも必要なものであると考えられる。特に、ISMS の実施においては、職階が高ければ高いほど、その意識や倫理性も高くなっていかなければならない。多忙な管理職、役員に対する教育の方法についてはさらに検討の余地がある。

また、管理職においては、自己啓発を選択した割合が他のものに比して若干高い。管理職に対する教育方法についても一考の余地が有りそうだ。

- 教育関係の担当部門

教育関係の担当部門は情報系部門が圧倒的に多い。確かに、「情報セキュリティ」に関してのものであることから、この結果は当然のものでもあるが、これは、裏返せば、一般的な教育ではなく、専門的なものであるという認識なのではないかとも考えられる。

社員として情報セキュリティに関する知識や倫理観を備えていなければならないならば、研修を主に行う総務、人事部門が行う比率がもう少し高くなっても良いように思うが、むしろ少数である。今後変化するのだろうか。

- 啓発活動

普及啓発の方法については、意外にも3割程度が行っていないという回答であった。通常の教育はほとんどの事業所で行っているのに対して、継続的な意識の維持に効果があると考えられる普及啓発は、まだまだ浸透していないと考えられる。

方法についても、ポスターの掲示や、ニュースレター、メルマガ、標語など旧来の手法が目につき、親しみやすいアプローチである、マスコットやノベルティ、表彰などはまだ少数派で、ここにも工夫がありそうである。

セキュリティと言うと、何か大変で、堅苦しい、やっかいなものというイメージがつきまとうが、実は当たり前のことを継続的に行うものであるということから考えると、今後、親しみやすさというものを一つのキーワードにしても良いのではないかと考える。

(7) アンケート全体からの分析

アンケートの回答とコメントを読み込むと、ISMS に関連する組織や制度についての問題点を以下のように6通りに分類することが出来る。

① 経営者が情報セキュリティ、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。

この経営者が ISMS に関心を示さないケースは、営業上の目的などで形式的に ISMS を取得する事業所などが該当する。この場合は、先ず何よりも経営者への啓発活動に重点を置くべきである。

③ ISMS への誤解。管理策への誤解が多い。管理策で必要ないものは適用除外したり、または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。
ISMS 導入作業時のコンサルタントの不適切な指導や事業所が審査に通ることを優先した事業所の対応の結果とも考えられる。ISMS 担当者はその事業所に合う適切な管理策とは何かを自発的に構築しなければならない。

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。
今回のアンケートではコンサルタントについて問題視するコメントが寄せられた。ISMS 認証取得時のコンサルタント決定については、十分な事前調査、すでに認証を取得した事業所へのヒアリング、コンサルタントとの面接などを実施し信頼できるコンサルタント選びを行うべきである。

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。
コンサルタントと同じように、こちらも十分な事前調査や他の ISMS 認証取得事業所へのヒアリング、コンサルタントとの相談を行い、慎重に審査機関を決定する。

⑥ ISMS 独自の問題。２００６年、ISMS が JIS Q 27000 シリーズに移行したが、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。
ISMS から JISQ27000 に移行する期間が１年と限られたことから、ISMS 認証を取得した事業所が継続審査時に JISQ27000 に移行する作業をしなければならなくなった。ISMS 認証を取得したばかりの事業所にとっては、審査を続けざまに受けることになり負担が高まった。移行期間が短いことと移行に関する情報不足がこの問題に拍車を掛けたようだ。

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] での状況とそれ程大きく異なる感じは受けない。

[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

５　ISMS認証制度の実効性を向上させる施策案について

4章の総合的な考察を元に、ISMS 認証制度を導入・運用するときの実効性を向上させる施策案を述べる。

(1) 資料作成の負担を軽減するための施策

内部監査や継続審査で必要な書類の作成を負担に思っている事業者は多く。また、一般的には、導入前に比べて ISMS の導入後、作成資料は多くなる傾向にある。この原因は主に以下のような点であると考えられる。

①これまでに本来当然に必要である書類を作成していなかった。または、定められた書類の作成を怠っていた。
②計画的な作成が求められているにもかかわらず、それを実施していなかった。
③監査対応のために、通常不要な書類を作成している。またはつじつま合わせのような作業を行っている。
④不要と考えられる書類であるにもかかわらず、作成を続けている。

こういった書類作成の負担を減らすために施策として、以下の事を提案したい。

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。

監査を、非日常の物としてとらえるのではなく、日常の延長線上でとらえ、そのための資料作りを行わないようにする。特に、情報資産台帳のような書類についても、その更新が経常的な業務の中で行われるように工夫することで、負担を分散でき、結果として、業務の集中化を避けることができる。

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。

不要な書類については遠慮せず作成物からはずしていくべきで、決まっているから作成しなければならないということではない。ISMS の目的は、書類作成ではないことを関係者全員が確認していくことも重要である。

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、定期的に確認することで失念を防止する。

必要書類について、計画的な作成や工夫がされていても、それを実施しなければ意味がない。日常業務に忙殺されてつい後回しにするのではなく、適切なタイミングで作成できるよう、管理職、担当者が相互に確認する工夫をしておくことで、忘れがち、後回しにしがちな書類作成を適切に行うことができる。

(2) ポリシーやルールによる制約を改善するための施策

ISMS の導入により、利用する電子機器の制約やセキュリティの強化による制約の発生について「不便である」「業務に影響がある」と感じる事業者は多い。それらについての対応及び留意点について以下のように考えた。

ISMS 認証を取得して期間が浅い場合は、まず、策定したルール、ポリシーになれていないということが原因としてあげられよう。効果についてあまり性急に求めると、よい計画や、ポリシーであっても成果が出ないということになりかねない。組織に ISMS が浸透するための時間は十分に確保する必要があるとともに、そのための普及・啓発について並行して実施するべきである。

また、計画策定時に十分に現場の意見を吸収することが重要である。事業を行う目的を十分ふまえた上でポリシーやルールを策定していかないと、現実的でないポリシーやルールとなってしまい、結果としてそれ自体が守られないといった状態になってしまう。

ISMS のために事業をやっているわけではないのであるから、そこを十分に認識してポリシー、ルールの設定を行うよう心がけるべきである。

一定期間経過、障害となるようなルールについては、継続運用の中で、目的を違えないように確認し、方向性のぶれがないようにした上で、見直しを行うべきであろう。

(3) コンサルタントの評価制度

ISMS の認証について、導入時にコンサルタントを利用する事業者は多い。導入後にこの比率は低くなるのだが、企業において導入時に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。

しかしながら、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。実際には、その情報収集に苦労している事業者が多いのではないかと想像される。

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

(4) 教育、普及啓発などについて

ISMS の効果を継続的に維持し向上していく上で、教育および普及啓発は不可欠かつ非常に重要であると考えられる。アンケートにおいて各事業者の状況を確認した中から、いくつかの問題点が浮かび上がった。

①各職位に平均した適切な教育が実施されていない。

ある程度想定していた問題の一つではあったが、やはり上位、つまり役員層になるほど、教育自体の機会が少なくなる傾向がある。

②もっとも実施されている集合研修についての目立った工夫がない。

集合研修はどの階層においても多く行われているが、記述欄などをみても目立った工夫を行っていると回答した事業者はほとんどなかった。

③普及啓発について従来手法に依存され、工夫が少ない。

手法としてはポスター掲示や標語の作成などが多く、従来型の手法にとどまっている傾向が見て取れる。

こういった問題点を改善するための施策として以下のようなことを提案したい。

①全階層における系統的な研修・教育、啓発機会の確保

多忙な役員層ではあるが、ISMS の成功の鍵は、企業の経営に関わるトップ層の十分な理解を得ることにあると言ってもよい。ISMS の実現にあわせ、内部統制のことを考えるときにも、役員など経営者層の高い意識・モラルを維持していくことは重要である。内部統制の崩壊要因としてあげられるものに、それら経営者層自身のモラルハザードや犯罪があげられているからである。

つまり、役員など上位の階層については、高い倫理観を維持し、ISMS の実現に向けて対応をしてもらう必要があり、そのこと自体、ISMS 導入が成功するか否かの大きな要因であるといえる。

一方で、各階層における教育内容についてはそれぞれに対応した適切なものを選択する必要がある。役員、経営層であれば、より倫理的な感覚を醸成する教育である必要があるだろうし、社員であれば、具体的な業務において、どのような対処を行えばよいかといった内容が中心になるであろう。

また、教育、研修計画については、専門部署だけで内容を決定するのではなく、各事業者において、全体の研修、人材育成を担当している部署と共同で進めていくことに留意する必要がある。

そのような部署と共同して教育、研修計画を検討していくことで、人材育成との関係を整理しながら計画を検討することが可能であろうし、これまでの教育ノウハウの吸収とともに、より全社的な対応が実現するだろう。

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

調査の中、多くの事業者において集合研修が行われていることはわかったが、その実施回数は、年に１－２回といったものでそれほど頻繁に行われているわけではない。

この部分について、２つの観点からの改善を提案したい。

一つは、実施する集合研修自体のトータルな実施方法の工夫である。

内容について、職位に応じたものを工夫していくのはもちろんだが、ここで指摘したいのは、研修自体とともに、その前後の募集、通知、効果測定などを合わせてトータルに考えて検討し、実施すべきであるということだ。

もう一つは小規模な研修の高頻度の実施を組み合わせることである

集合研修については、大人数であればあるほど、開催回数は多くできないと

いうのが一般的な状況であろうと想像できる。

そこで、必ず職場単位、グループ単位の小規模研修を組み合わせて、高頻度に定期的なタイミングで研修（もちろん朝礼や、係や課単位の打ち合わせの中で実施するようにしてもよい）を組み合わせて実施することを提案したい。

多くの企業が ISMS の効果を高めるために取り組んでいる点として「一般社員への認識・理解の強化」をあげているにもかかわらず、結果としてはそのような教育を行っていることは顕著に表れていない。この提案は、まさにその点を改善するためのもので、次に述べる普及啓発の改善とともに取り組むべきではないかと思う。

小規模で短時間のものであっても、高頻度で対応できれば、全体的な研修で行った内容などについて、適時リマインドすることができ、効果の向上が期待できるはずである。

③普及啓発について

ポスター掲示や、標語については一定の取り組みが見られる。それらの手段について効果がないと考えているわけではなく、むしろ積極的に実施すべきであるが、ここに「親しみやすさ」を導入することを提案したい。

ISMS について、社内で実施する際「きまったことだから」「セキュリティ確保のために必要だから」といって進めていくのでは、社内への周知は難しいと思われる。

それに起因して一定の緊張感が生まれることはデメリットばかりではないが、そこに「親しみやすさ」を持ち込むことで、社員のちょっとした話題になるなど、より印象深く認識してもらうことが可能なのではないだろうか。

たとえば、分別収集において仙台市が分別収集を進めるために設定したキャラクターである「ワケル君」が人気を博したり、suica や pasmo にそれぞれキャラクターが設定されていたりという状況は、行政が行う「分別収集」という一見そのようなものと無縁かと思われることでも、イメージ戦略が可能なことを示しているし、「かわいいから」といった理由でキャラクターグッズを求めたりという状況が発生し、それがカード自体の認識を高めたりと、それぞれ効果的であることを示しているのではないだろうか。

そこで、普及啓発においては、従来手法に加え、特にノベルティやマスコットなどの活用を積極的に行うことを提案したい。また、キャラクターなどの設定については、デザイナーなどに依頼するような方法をとるのではなく、社内において公募等を行うといった方法を利用するなど、より社員の参加意識を醸成していく方法を併用するとより効果的だと考える。

６　今後の課題

今回は、ISMS 認証取得事業所の実態調査を元に検討を行い、その結果は考察にまとめたとおりである。しかしながらこのアンケートの回答について、もう一段時間をかけて検討を行いたいと考えている。そうすることで、今回の回答が持つさらなる情報を引き出したいと考えている。

また同時に ISMS 認証を取得、運用する際に発生する課題に対して具体的な対応策について検討したい。これらの課題を抱えている事業所と協力することで、その対応策を実施、検証したいと考えている。

７　謝辞

約 1,400 事業所にアンケートを発送し、260 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事業所に対し厚くお礼を申し上げたい。

また、ヒアリングを快諾頂いた 2 社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18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。

以上

付録　A. 質問項目の切り口と設問

今回実施したアンケートの質問の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

目的	事業者の組織の大きさや業種、回答記入者の属性を見る。
質問数	６問
質問 項目	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

２．ISMS 認証取得に関連する情報

目的	事業者が実際に ISMS 認証を取得した際の情報および ISMS 認証取得によって得た効果、生じている課題に関する情報を得る。
質問数	１０問
質問 項目	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

３．ISMS 認証の運用に関連する課題

目的	ISMS 認証に基づいた日常的な運用や内部監査、マネジメントビューに関する情報を得る。
質問数	１３問
質問 項目	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

４．ISMS に関連した教育

目的	ISMS 認証に関する教育の実施状況の情報を得る。
質問数	６問
質問 項目	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

付録　B．アンケートの配布資料

今回のアンケート調査で使用した質問及び回答などの資料は次の通りである。

(1) アンケート表紙　　（１ページ）
(2) アンケート質問用紙　　（４ページ）
(3) アンケート回答欄　　（１ページ）
(4) アンケート回答記入欄　　（１ページ）

ISMS 認証取得及びその継続における課題を探るためのアンケートへのご協力のお願い

皆様方にはますますご健勝のこととお喜び申し上げます。

平成 19 年 1 月現在、1,900 余りの事業所・部門で ISMS 認証（ISO/IEC27000 シリーズによる認証を含む）の取得がなされております。これは、情報セキュリティへの関心の高さを示すとともに、セキュリティという広範なものに対して、一定の基準を導入し管理しようという考え方が一般的になりつつあることの現れとも考えられます。

しかしながら一方で、認証取得後、思ったような効果が上がらない、経費に見合った効果を実感できない、現場で行っていることと基準が乖離しているなどの問題を感じるという声も耳にします。

私ども情報セキュリティ大学院大学内田研究室では、情報セキュリティマネジメントシステムについて研究を行っております。本アンケートでは、研究の一環として ISMS 認証取得及びその後の運用で発生している事柄や課題を抽出したいと考えております。更に、アンケート結果を踏まえ ISMS 認証の効果をより高めるための施策についての検討を行っていく予定です。

この趣旨をご理解頂き是非ともご回答頂きますよう、お願い申し上げます。

次ページ以降に質問がございます。別紙の回答用紙にご回答頂き、同封の封筒でご返送ください。

回答は平成 19 年 1 月 1 日現在あるいは、直近の数値をご記入ください。また、ご記入頂く方については ISMS 認証のご担当者様を想定させて頂いております。

アンケートにつきましては、全ての項目について貴社名、ご記入者名等の個別属性を公開することはありません。また、ご記入いただいた内容については、本研究に関連することのみに利用し、それ以外に利用することはありません。

また、アンケートの集計および分析結果につきましては、上記に配慮した上で本研究室 WEB に公開する予定です。ご希望の方にはご連絡致します。

大変お忙しいことと存じますが、アンケートは平成 19 年 2 月 28 日(水)までにご投函いただきますよう、重ねてお願い申し上げます。

ご質問・お問い合わせ先
情報セキュリティ大学院大学　内田研究室　内田勝也
〒221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1　TEL045-410-0238
電子メール uchida@iisec.ac.jp　携帯 090-1050-3206

研究室に在室していることが少ないため、お手数ですが、ご連絡は電子メールあるいは携帯電話までいただければ幸いです。

質 問 票	回答用紙にご記入ください

貴組織・ご記入者についてお聞きします（不明項目は 未記入で構いません）

1. 資本金（1つを選択）

1：100 万円未満	2：100 万円以上 1000 万円未満	3:1000 万円以上 5000 万円未満
4：5000 万円以上 5 億円未満	5：5 億円以上	

2. 従業員数（1つを選択）

1：100 人未満	2：100 人以上 300 人未満	3：300 人以上 500 人未満
4：500 人以上 1,000 人未満	5：1,000 人以上 1,500 人未満	6:1,500 人以上 10,000 人未満
7：10,000 人以上 50,000 人未満	8：50,000 人以上	

3. 該当する業種（1つを選択）

1. 建設業	2. 電気・ガス・水道業	3. 運輸業	4. 金融・保険業
5. 製造業	6. 情報通信業	7. ハイテク	8. 卸売・小売業
9. 不動産業	10. 飲食店・宿泊業	11. 医療・福祉	12. 教育・学習支援
13. 複合サービス業	14. 法務・法律	15. 公務(政府・自治体)	16. その他

4. ご記入者の所属（所属されている部門が最も近い部門を1つ選択してください）

1. 総務	2. 人事	3. 経理	
4. 社長室	5. 企画部門	6. 情報システム管理部門	
7. 情報システム開発部門	8. 情報セキュリティ担当部門	9. 事業部門	
10. コンプライアンス担当部門	11. リスク管理担当部門	12. 監査部門	13. その他

5. ご記入者の役職（ご自身の役職で最も近い役職を1つ選択してください）

1. 会長・社長・役員	2. 執行役員	3. 事業部長	4. 部長	
5. 課長	6. 係長・主任	7. 専門職	8. 一般社員	9. その他

6. ご記入者の ISMS 認証業務に関する経験年数（ご自身のご経験年数を1つ選択してください）

1. 1 年未満	2. 1 年以上 3 年未満	3. 3 年以上 5 年未満
4. 5 年以上 7 年未満	5. 7 年以上	

貴社の ISMS 認証取得についてお聞きします

7. ISMS 認証を取得した年月（ISMS 認証を取得した年月を西暦、月でご記入ください）

8. ISMS 認証対象組織の従業員数（1つを選択）

1. 100 人未満	2. 100 人以上 300 人未満	3. 300 人以上 500 人未満
4. 500 人以上 1,000 人未満	5. 1,000 人以上 1,500 人未満	6. 1,500 人以上 5,000 人未満
7. 5,000 人以上 10,000 人未満	8. 10,000 人以上	

9. 他の認証の取得状況と取得後年数は？（いくつでも）

1. ISO9000（QMS）（ 年）	2. ISO14000(EMS)（ 年）	3. ISO20000(ITSMS)（ 年）
4. プライバシーマーク（ 年）	5. その他（ ）	

10. ISMS 認証を取得した主な目的は？（いくつでも）

1. 会社業務の運営を ISMS 認証に基づいた方法にするため	2. ISMS 認証の考え方を部分的に入れて業務の改善を狙った	3. ISMS 認証を得ることで営業活動において有利になるあるいは不利にならないことを狙った	
4. 入札その他で ISMS 認証取得が条件になっているため	5. グループ会社等の方針で決まっているため	6. 情報セキュリティ対策の向上を狙った	7. その他

11. 一番初めに ISMS 認証取得について発案したのは誰か？（どれか1つ）

1. 代表取締役	2. 専務、常務	3. その他役員	4. 管理職	5. その他

※問11，12において自治体などの場合は、1. 長、2. 助役・収入役、3. 局・行政区長、4. 部長・課長、と読み替えてご回答ください。

12. 現時点で、ISMS 認証の運用責任者は誰か？（どれか1つ）

1. 代表取締役	2. 専務、常務	3. その他役員	4. その他

質 問 票	回答用紙にご記入ください

13. ISMS 認証取得によって得られた効果は？（いくつでも）

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

14. ISMS 認証取得で発生した想定外の影響は？ （いくつでも）

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	3. 手続きの煩雑化・業務効率の低下
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	6. セキュリティ事件・事故が増えた又は変わらない
7. 業務への影響は特にない	8. その他（記入欄有り）	

15. 問14で「2. 業務量の増加」、「3. 手続きの煩雑化・業務効率の低下」を回答された方に質問します。
それらはどのようなものか？（いくつでも）

1. 不要な作業申請等の作成	2. 不要な作業履歴の記録	3. 実際の手続きとマニュアルが異なる
4. 監査目的の資料作成	5. ISMS 事務局などからの直接業務に関係のない依頼作業が増加した	6. 厳格な入退出管理で、他部門とのコミュニケーションが悪化
7. 情報を利用・取得しづらくなった	8. その他（記入欄有り）	

16. 問14で「4. 業務上の制約が増加」を回答された方に質問します。
ISMS の導入で現場における業務上の制約は？（いくつでも）

1. 機器の取扱（含む持出・込）に関する制約	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（記入欄有り）	

17. ISMS 認証取得後の運用で負担になっている作業は？（いくつでも）

1. セキュリティ委員会の開催	2. ポリシー（含む規定類、業務マニュアル等）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（記入欄有り）

18. 現在、ISMS の効果を高めるために重点的に取り組んでいる（含む予定）ものは？（いくつでも）

1. 経営者の認識・理解の向上	2. 管理者層の認識・理解の強化	3. 一般社員の認識・理解の強化
4. マニュアルの整備	5. 内部監査担当のスキル強化	6. 有効性評価手法の改善
7. 費用対効果の説明手法の明確化	8. リスク分析手法の改善（※）	9. 教育研修の改善（※）
10. 文書・記録管理の改善（※）	11. インシデント対応の向上（※）	12. その他（記入欄有り）

※含むツールの導入など

19. ISMS の継続的な運用のために経営陣はマネジメント・レビュー以外に関わっているか？（どれか1つ）

1. いる	2. いない	3. 不明

20. 事務局のメンバーは何人か？

1. 専任（　　人）	2. 兼務（　　人）	3. その他（　　人）

21. 現在の事務局には初回認証取得の際のメンバーが、どのくらいの割合で残っているか？（どれか1つ）

1. 全員残っている	2. 7 割未満	3. 5 割未満
4. 3 割未満	5. 一人もいない	

質 問 票 回答用紙にご記入ください

22. 新しいメンバーに対して、どのような形で ISMS に関連したスキル習得を行ったか？（いくつでも）

1. 外部講習によるスキル習得	2. 社内講習によるスキル習得	3. OJT による習得
4. 独学（個人に任せている）	5. 特に無し	6. その他（記入欄有り）

23. 外部コンサルタントの支援は？（どれか1つ）

認証取得まで	1. 受けている	2. 一部受けている	3. 受けていない
認証取得後	1. 受けている	2. 一部受けている	3. 受けていない

24. 内部監査の実施頻度は？（どれか1つ） ※ここでは更新取得審査作業は内部監査に含まないとします。

1. 1年に1回	2. 半年に1回	3. 3か月に1回	4. 1か月に1回以上

25. 内部監査体制は？（いくつでも）

1. 常設の社内チーム	2. 非常設の社内チーム	3. 外部機関
4. 外部機関と社内機関の共同体制	5. その他（記入欄有り）	

26. 内部監査指摘事項に対する改善は行われているか？（どれか1つ）

1. 行われている	2. 一部のみ行われている	3. 行われていない

27. 問26で「2. 一部のみ行われている」「3. 行われていない」と回答された方に質問します。その理由は？（いくつでも）

1. 内部監査の指摘が適切でない	2. 改善対策に対するマネージメントの支援が不十分	3. 現場の協力が得られない
4. 現場に改善作業を行う余力が無い	5. 事務局に改善作業を行う余力が無い	6. その他（記入欄有り）

28. マネジメント・レビューの頻度は？（どれか1つ）

1. 1年に1回	2. 半年に1回	3. 3か月に1回
4. 1か月に1回	5. その他（記入欄有り）	

29. マネジメント・レビューは、どのような形で実施されているか？（いくつでも）

1. 会議で実施	2. 電子メールで実施	3. 会議、メールの組合せで実施	4. その他（記入欄有り）

30. ISMS の維持に必要な社員教育の手段は？（いくつでも）

1. 集合研修	2. 冊子の配布	3. OJT	4. Web 学習
5. ソフトウェア	6. メール	7. ビデオ	8. 自己啓発
9. 通信教育	10. 特に行っていない	11. その他（記入欄有り）	

31. それでは管理者教育は？（いくつでも） ※ 問30の回答選択肢からお選びください。

32. 同じく役員教育は？（いくつでも） ※ 問30の回答選択肢からお選びください。

33. ISMS に関連した教育の頻度はどの程度か？（どれか1つ）

1. 毎日（朝礼等）	2. 週1～2回	3. 月に1～2回	4. 3か月に1回
5. 半年に1回	6. 年に1回	7. 不定期	8. 無し

34. ISMS の教育担当部門は？（いくつでも）

1. 総務	2. 人事	3. 経理	4. 社長室	
5. 企画部門	6. 情報システム管理部門	7. 情報システム開発部門	8. 情報セキュリティ担当部門	
9. 事業部門	10. コンプライアンス担当部門	11. リスク管理担当部門	12. 監査部門	13. その他

35. 教育以外の啓発活動は？（いくつでも）

1. キャンペーン週間などの設定	2. マスコットの制定	3. ポスターの掲示	
4. ニュースレター・メルマガの発行	5. 啓発ビデオの作成	6. 情報セキュリティに関連する標語の制定	
7. 情報セキュリティへの取り組みの表彰（部門、個人）	8. セキュリティの標語などを書いたノベルティの配布	9. 啓発活動は特に行っていない	10. その他

ありがとうございました。

以上でアンケートは終了です。**回答用紙の裏面**をご確認ください。

回 答 票

回答で、【　　】(1～6)等の場合には、1から6までの数字を、【　】内にご記入ください。
【 1. 2. 3. 4. ・ ・ 】の場合は、該当する数字全てに○印をつけてください。
記入式の回答欄が狭い場合は回答票裏面の記入欄にお書きください。

1. 資本金　【　　】(1～5)
2. 従業員数　【　　】(1～8)
3. 該当する業種　【　　】(1～16)
4. ご記入者の所属　【　　】(1～13)
5. ご記入者の役職　【　　】(1～9)
6. ご記入者の ISMS 認証に関する経験年数　【　　】(1～5)
7. ISMS 認証を取得した年月　【西暦 ＿＿＿＿年＿＿月 】
8. ISMS 認証対象組織の従業員数　【　　】(1～8)

9. 各認証の取得後の年数は？【 1.（　　年） 2.（　　年） 3.（　　年） 4.（　　年）
5.（＿＿＿＿＿＿＿＿＿＿＿＿） （　　年） 】
10. ISMS 認証を取得する主な目的は？　【 1.　2.　3.　4.　5.　6.　7. 】

11. ISMS 認証取得の発案者は？　【　　】(1～5)
12. 現時点で、ISMS 認証の運用責任者は誰ですか？　【　　】(1～4)
13. 認証によって得られた効果は？
【 1.　2.　3.　4.　5.　6.　7.　8.　9.　10.　11.　12.　13.　14.　15.　16.　】
14. 想定外の影響は？　【 1. 2. 3. 4. 5. 6. 7. 8.（＿＿＿＿＿＿＿＿＿＿＿＿）】
15. 問 14 の回答「2.」「3.」のみ【 1. 2. 3. 4. 5. 6. 7. 8.（＿＿＿＿＿＿＿＿＿＿＿＿）】
16. 問 14 の回答「4.」のみ　【 1. 2. 3. 4. 5. 6. 7. 8.（＿＿＿＿＿＿＿＿＿＿＿＿）】
17. 負担になっている作業は？
【 1.　2.　3.　4.　5.　6.　7.　8.　9.　10.　11.　12.（＿＿＿＿＿＿＿＿＿＿＿＿）】
18. 重点的に取り組んでいる（含む予定）ものは？
【 1.　2.　3.　4.　5.　6.　7.　8.　9.　10.　11.　12.（＿＿＿＿＿＿＿＿＿＿＿＿）】
19. 経営陣の関わりは？　【　　】(1～3)
20. 事務局のメンバーは？　【 1. 専任（＿＿＿＿人）　2. 兼務（＿＿＿＿人）　3. その他（＿＿＿＿人）】

21. 最初のメンバーの割合は？　【　　】(1～5)
22. 新しいメンバーへの教育は？　【 1. 2. 3. 4. 5. 6.（＿＿＿＿＿＿＿＿＿＿＿＿）】
23. 外部コンサルタントの支援　認証取得時まで【　　】(1～3)　認証取得後【　　】(1～3)
24. 内部監査の実施頻度は？　【　　】(1～4)
25. 内部監査体制は？　【 1. 2. 3. 4. 5.（＿＿＿＿＿＿＿＿＿＿＿＿）】
26. 内部監査指摘事項の改善は？　【　　】(1～3)
27. 問２６で「2.」「3.」を回答した方のみ【 1. 2. 3. 4. 5. 6.（＿＿＿＿＿＿＿＿＿＿＿＿）】
28. マネジメント・レビューの頻度は？　【 1. 2. 3. 4. 5.（＿＿＿＿＿＿＿＿＿＿＿＿）】
29. マネジメント・レビューの実施方法は？【 1. 2. 3. 4.（＿＿＿＿＿＿＿＿＿＿＿＿）】

30. 社員教育の手段は？【 1.　2.　3.　4.　5.　6.　7.　8.　9.　10.　11.（＿＿＿＿＿＿）】
31. 管理者教育は？　【 1.　2.　3.　4.　5.　6.　7.　8.　9.　10.　11.（＿＿＿＿＿＿）】
32. 役員教育は？　【 1.　2.　3.　4.　5.　6.　7.　8.　9.　10.　11.（＿＿＿＿＿＿）】
33. 主要な教育の頻度は？　【　　】(1～8)
34. ISMS の教育担当部門は？【 1.　2.　3.　4.　5.　6.　7.　8.　9.　10.　11.　12.　13. 】
35. 教育以外の啓発活動は？　【 1.　2.　3.　4.　5.　6.　7.　8.　9.　10.　】

裏面に続きます

回 答 票

貴社で ISMS 認証に基づく運用をされている中で感じておられる事項や疑問、課題などがございましたら、ご記入ください。

情報セキュリティ大学院大学内田研究室は、マネジメントシステムに関連した情報セキュリティについて研究しています。ご回答内容の確認や研究に関するご案内・ご連絡をさせて頂いてもよろしければ、以下の項目のご記入をよろしくお願い致します。

貴社名

会社ご住所

ご記入者のお名前

ご記入者の E-MAIL アドレス

ご記入頂いた貴社名、会社ご住所、ご記入者のお名前および E-MAIL アドレスは情報セキュリティ大学院大学内田研究室の ISMS 関連研究に関するご連絡以外には使用致しません。

ご記入ありがとうございました。
この回答用紙を、郵送にて返送頂きますよう、よろしくお願い致します。

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

付録　C．アンケート結果のまとめ

質問は全部で３５問である。それらの質問の集計結果を以下に示す。

(1) 内容

１つの質問についての以下の内容を１ページにまとめた。

- 質問
- 回答を集計したグラフ
- 回答の集計数値（表）
- 質問ごとの考察

である。

(2) 質問項目一覧

事業者（企業、公共団体等）の基礎情報

１．　資本金
２．　従業員数
３．　該当する業種
４．　ご記入者の所属
５．　ご記入者の役職
６．　ご記入者の ISMS 認証業務に関する経験年数

ISMS 認証取得に関連する情報

７．　ISMS 認証を取得した年月
８．　ISMS 認証対象組織の従業員数
９．　他の認証の取得状況と取得後年数は？
１０．　ISMS 認証を取得した主な目的は？
１１．　一番はじめに ISMS 認証取得について発案したのは誰か？
１２．　現時点で ISMS 認証の運用責任者は誰か？
１３．　ISMS 認証取得によって得られた効果は？
１４．　ISMS 認証取得で発生した想定外の影響は？
１５．　問１４で「２．業務量の増加」「３．手続きの煩雑化・業務効率の低下」を回答された方に対して、それらはどのようなものか？
１６．　問１４で「４．業務上の制約が増加」を回答された方に質問します。ISMS の導入で現場における業務上の制約は？

ISMS 認証の運用に関連する課題

１７．　ISMS 認証取得後の運用で負担になっている作業は？

１８．　現在、ISMS の効果を高めるために重点的に取り組んでいるものは？
１９．　ISMS の継続的な運用のために経営陣はマネジメントレビュー以外に関わっているか？
２０．　事務局のメンバーは何人か？
２１．　現在の事務局には初回認証取得の際のメンバーが、どのくらいの割合で残っているか？
２２．　新しいメンバーに対して、どのような形で ISMS に関連したスキル習得を行ったか？
２３．　外部コンサルタントの支援は？
２４．　内部監査の実施頻度は？
２５．　内部監査体制は？
２６．　内部監査指摘事項に対する改善は行われているか？
２７．　問２６で「２．一部のみ行われている」「３．行われていない」と回答された方に対して、その理由は？
２８．　マネジメント・レビューの頻度は？
２９．　マネジメント・レビューは、どのような形で実施しているか？

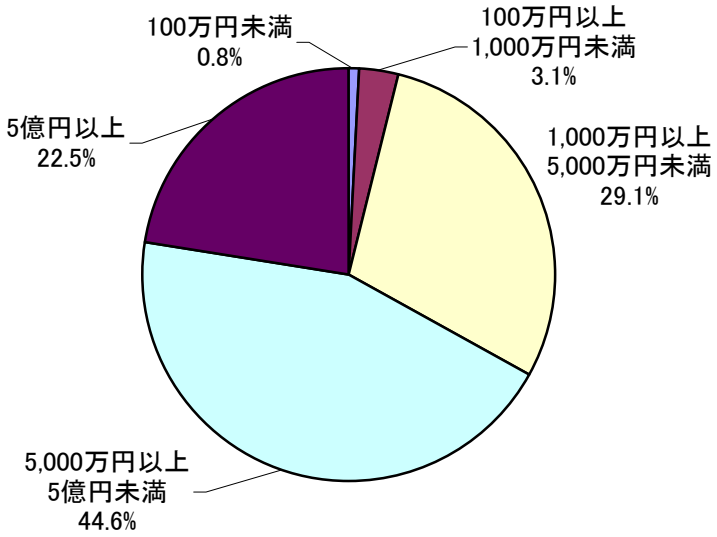
ISMS に関連した教育

３０．　ISMS の維持に必要な社員教育の手段は？
３１．　それでは管理者教育は？
３２．　同じく役員教育は？
３３．　ISMS に関連した教育の頻度はどの程度か？
３４．　ISMS の教育担当部門は？
３５．　教育以外の啓発活動は？

組織、記入者について

１．資本金（１つを選択）

１．　100万円未満
２．　100万円以上1,000万円未満
３．　1,000万円以上5,000万円未満
４．　5,000万円以上5億円未満
５．　5億円以上



（単位：社数・%）

総数	100万円未満	100万円以上1000万円未満	1000万円以上5000万円未満	5000万円以上5億円未満	5億円以上
258	2	8	75	115	58
100%	0.8%	3.1%	29.1%	44.6%	22.5%

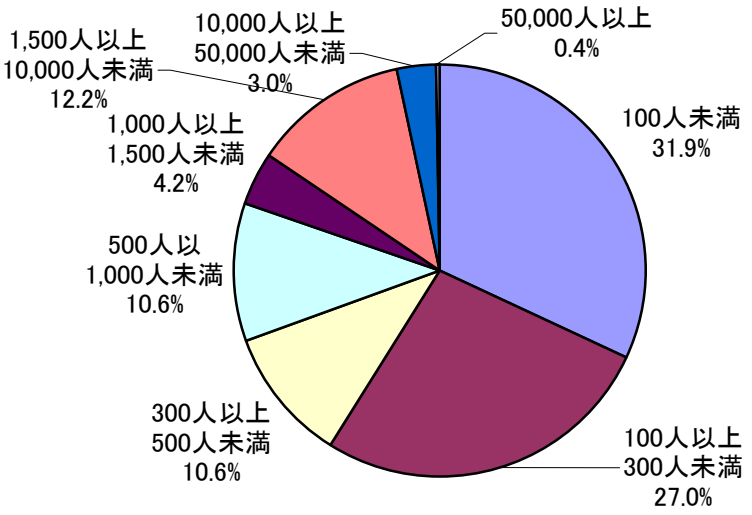
資本金が1,000万円未満の事業者は3.9%と少ない。1,000万円から5,000万円未満が29%、5,000万円から5億円未満が45%で合計74%となった。この規模の事業者がISMS認証を取得する中核的な層をなしている。

資本金5億円以上の事業者は23%となり、大規模な事業者も積極的にISMS認証を取得しているといえる。
事業者の資本金を問う質問なので、地方自治体や法人などは無回答となった。総計が258であることから、無回答は6事業者であった。

組織、記入者について

２．従業員数（１つを選択）

１．　100人未満
２．　100人以上300人未満
３．　300人以上500人未満
４．　500人以上1,000人未満
５．　1,000人以上1,500人未満
６．　1,500人以上10,000人未満
７．　10,000人以上50,000人未満
８．　50,000人以上



n=263

（単位：社数・%）

総数	100人未満	100人以上 300人未満	300人以上 500人未満	500人以 1,000人未満	1,000人以上 1,500人未満
263	84	71	28	28	11
100%	31.9%	27.0%	10.6%	10.6%	4.2%

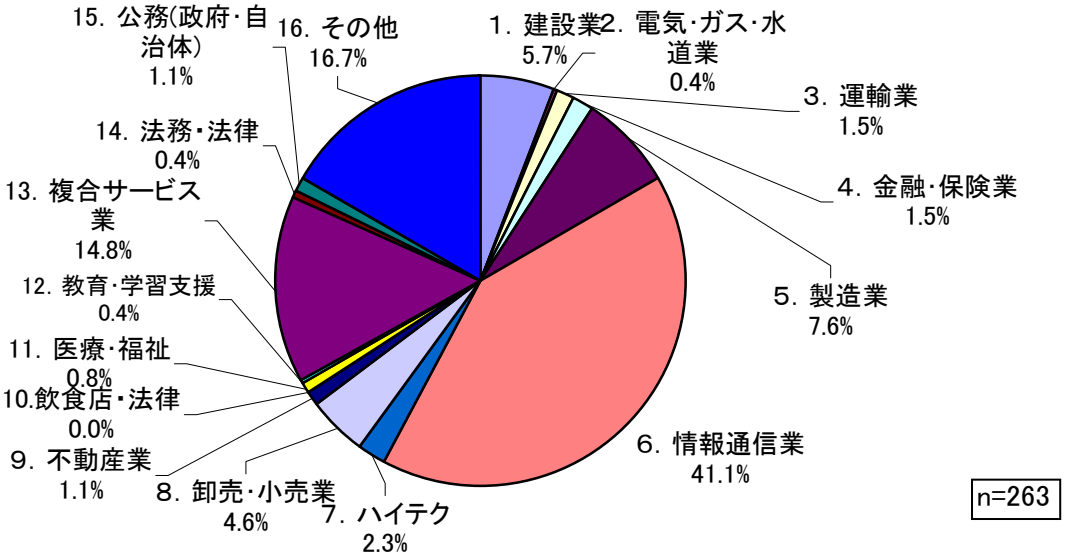
1,500人以上 10,000人未満	10,000人以上 50,000人未満	50,000人以上
32	8	1
12.2%	3.0%	0.4%

事業者の従業員数で、100人未満が32%、300人未満が27%となり、合計で約60%が300人未満の事業者となった。一方では1,000人以上の従業員をかかえる事業者も合計で約20%もいる。このことよりISMS認証は事業者の規模を問わず取得されていると考えられる。

組織、記入者について

３．　該当する業種（１つを選択）

１．建設業	２．電気・ガス・水道業
３．運輸業	４．金融・保険業
５．製造業	６．情報通信業
７．ハイテク	８．卸売・小売業
９．不動産業	１０．飲食店・宿泊業
１１．医療・福祉	１２．教育・学習支援
１３．複合サービス業	１４．法務・法律
１５．公務（政府・自治体）	１６．その他



（単位：社数・%）

総数	1. 建設業	2. 電気･ガス･水道業	3. 運輸業	4. 金融･保険業	5. 製造業	6. 情報通信業
263	15	1	4	4	20	108
100%	5.7%	0.4%	1.5%	1.5%	7.6%	41.1%
	7. ハイテク	8. 卸売･小売業	9. 不動産業	10.飲食店･法律	11. 医療･福祉	12. 教育･学習支援
	6	12	3	0	2	1
	2.3%	4.6%	1.1%	0.0%	0.8%	0.4%
	13. 複合サービス業	14. 法務･法律	15. 公務(政府･自治体)	16. その他		
	39	1	3	44		
	14.8%	0.4%	1.1%	16.7%		

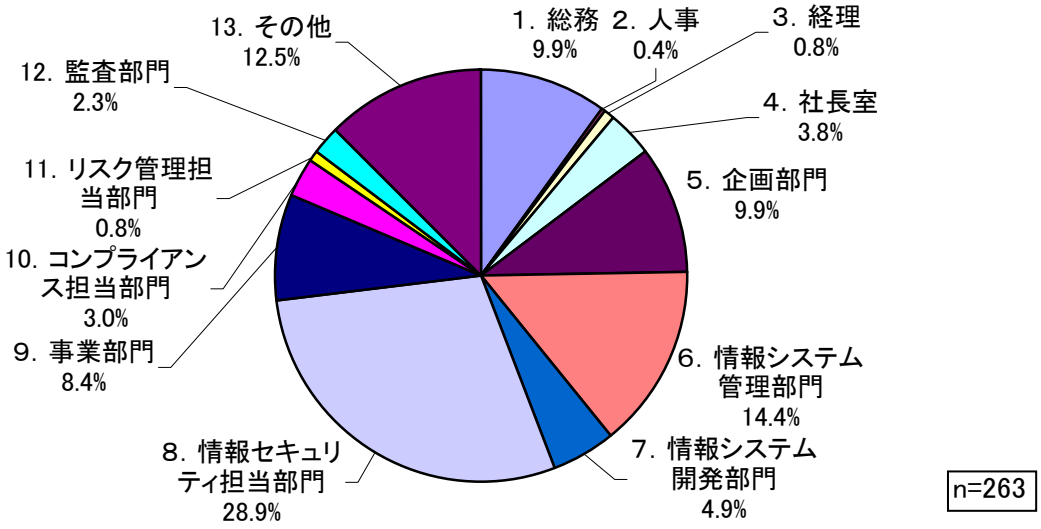
特徴的なのは「6．情報通信業」が約40%を占めていることだ。これは経済産業省の安全対策基準をグローバル化してISMS第三者認証制度をスタートさせたことと当初システム開発等の業務をしている事業者を対象にしていたためと考えられる。なお現在はISMSは業種を問わず適用できる。

次に多いのは「13．複合サービス業」で、これは個人情報を扱うことの多い業務を含んでいると考えられる。その他の業種は多少の差はあるものの、ほぼばらついている。

組織、記入者について

４．ご記入者の所属（所属されている部門が最も近い部門を１つ選択してください）

１．総務	２．人事
３．経理	４．社長室
５．企画部門	６．情報システム管理部門
７．情報システム開発部門	８．情報セキュリティ担当部門
９．事業部門	１０．コンプライアンス担当部門
１１．リスク管理担当部門	１２．監査部門
１３．その他	



（単位：社数・%）

総数	1. 総務	2. 人事	3. 経理	4. 社長室	5. 企画部門	6. 情報システム管理部門
263	26	1	2	10	26	38
100%	9.9%	0.4%	0.8%	3.8%	9.9%	14.4%

7. 情報システム開発部門	8. 情報セキュリティ担当部門	9. 事業部門	10. コンプライアンス担当部門	11. リスク管理担当部門	12. 監査部門	13. その他
13	76	22	8	2	6	33
4.9%	28.9%	8.4%	3.0%	0.8%	2.3%	12.5%

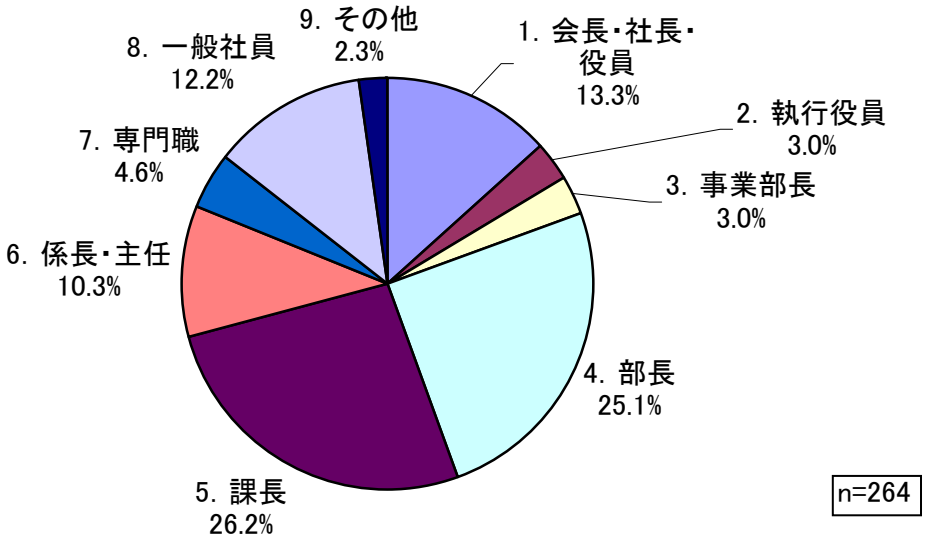
一番多かったのは情報セキュリティ担当部門の約29%で、ISMS事務局を含む情報セキュリティの専任者の割合が読み取れる。また、情報システム管理部門と情報システム開発部門を併せると約19%となり、システムの管理、開発に携わる人員がISMS認証の管理に関わっていることを示す。これは経済産業省の安全対策基準をグローバル化する目的でISMS第三者認証制度を開始した経緯もあり、このようになっていると考えられる。

これ以外では企画部門と事業部門がそれぞれ約10%、約8%となり、若干割合が高い。それ以外の部署は概ね分散している。情報セキュリティ専任でもシステム関連でもない部署（6，7，8以外）が担当する割合を合計すると52%と約半数を占める。

組織、記入者について

５．　ご記入者の役職（ご自身の役職で最も近い役職を１つ選択してください）

１．会長・社長・役員
２．執行役員
３．事業部長
４．部長
５．課長
６．係長・主任
７．専門職
８．一般社員
９．その他



（単位：社数・%）

総数	1. 会長･社長･役員	2. 執行役員	3. 事業部長	4. 部長	5. 課長	6. 係長･主任
264	35	8	9	66	69	27
100%	13.3%	3.0%	3.4%	25.0%	26.1%	10.2%

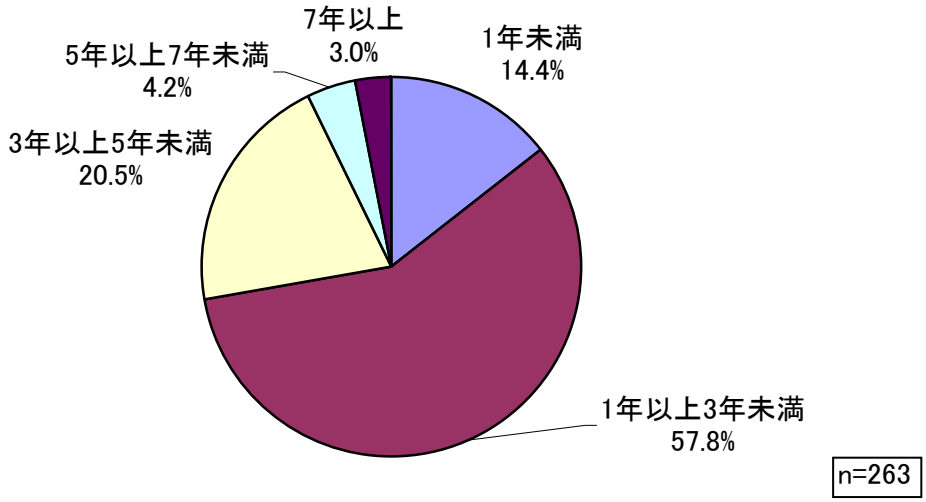
7. 専門職	8. 一般社員	9. その他
12	32	6
4.5%	12.1%	2.3%

「4. 部長」、「5. 課長」の中間管理職が合計で51%をしめた。「6. 係長・主任」を含めると62%を占め、組織を動かす実務者が担当していることがわかる。
特徴的なのは、「1. 会長・社長・役員」、「2. 執行役員」を合わせると約16%を占めていることで、ISMS認証の責任者として役員クラスも積極的に参画している事業者も多いことを示している。

ISMS認証に関連する体制

６．　ご記入者のISMS認証業務に関する経験年数
（ご自身のご経験年数を１つ選択してください）

１．１年未満
２．１年以上３年未満
３．３年以上５年未満
４．５年以上７年未満
５．７年以上



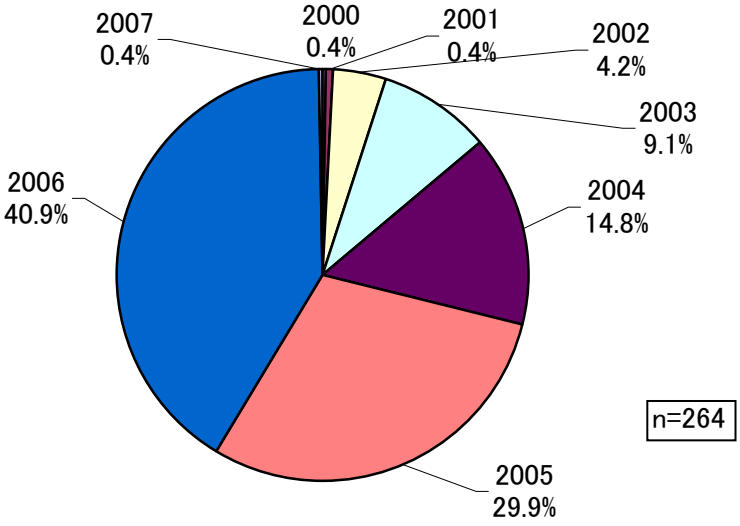
（単位：社数・%）

総数	1年未満	1年以上3年未満	3年以上5年未満	5年以上7年未満	7年以上
263	38	152	54	11	8
100%	14.4%	57.8%	20.5%	4.2%	3.0%

主力は「２．1年以上3年未満」で、約58%に達した。
ISMS第三者認証制度が2002年に始まってから数年しか経過していないので、上記のように経験年数の短い担当者が多いと考えられる。
5年以上担当している人の合計も7%を超え、長年担当が固定されていると想像できる事業者も見受けられる。

ISMS認証取得関連

７．　ISMS認証を取得した年月（ISMS認証を取得した年月を西暦、月でご記入ください）



（単位：社数・%）

総数	2000	2001	2002	2003	2004
264	1	1	11	24	39
100%	0.4%	0.4%	4.2%	9.1%	14.8%

2005	2006	2007
79	108	1
29.9%	40.9%	0.4%

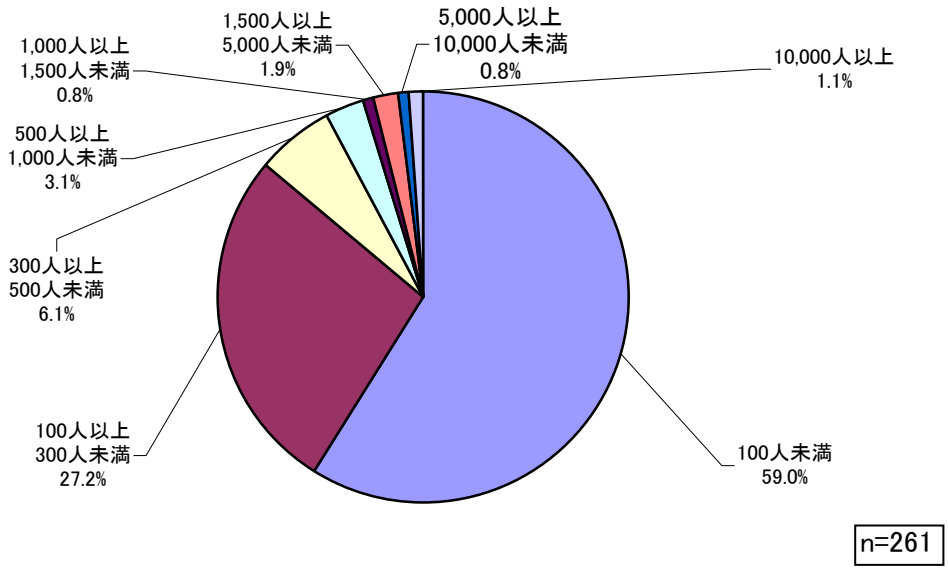
今回のアンケート回答組織の認証取得年数の内訳によると2005年および2006年に取得と回答した企業が187件と数多いが、（財）日本情報処理開発協会（JIPDEC）が公表している取得事業者数の推移と比較しても同様の傾向となっている。

さらには、回答者数の半数以上が1年以上のISMSの継続運用を行った実績がある。うち14%にあたる37件の組織は、ISMSの更新審査のタイミングである3年を超える実績がある。

ISMS認証に関連する体制

８．ISMS認証対象組織の従業員数（１つを選択）

１．100人未満
２．100人以上300人未満
３．300人以上500人未満
４．500人以上1,000人未満
５．1,000人以上1,500人未満
６．1,500人以上5,000人未満
７．5,000人以上10,000人未満
８．10,000人以上



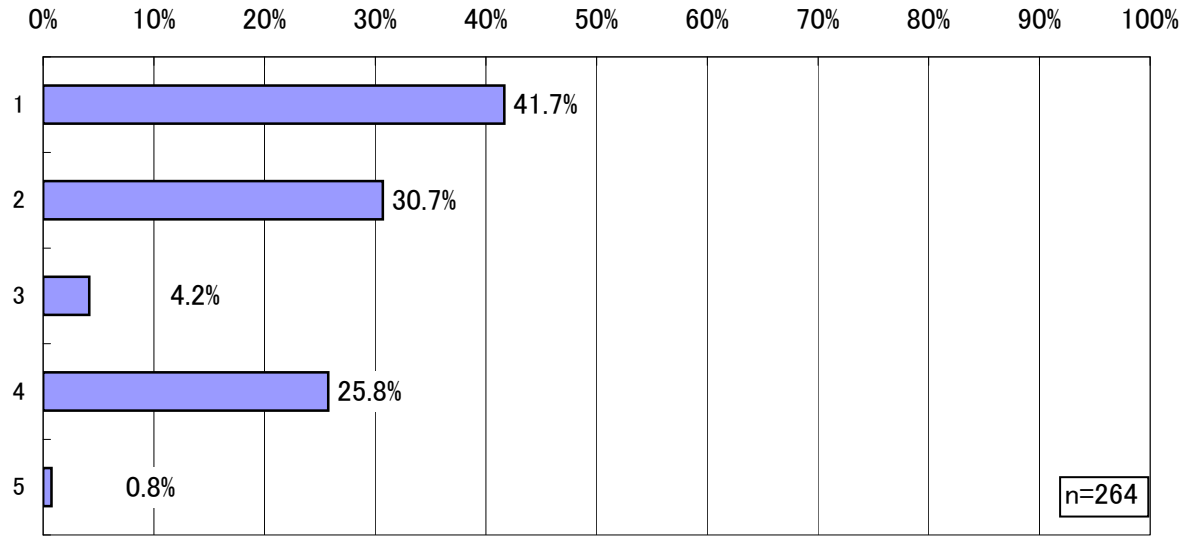
（単位：社数・%）

総数	1	2	3	4	5	6	7	8
261	154	71	16	8	2	5	2	3
100%	59.0%	27.2%	6.1%	3.1%	0.8%	1.9%	0.8%	1.1%

アンケート回答数のうち適用範囲の従業員数が100人未満の比率が59%、100人以上300人未満の組織が27%となり、300人未満の組織で取得したと回答した組織は全体の86%を占める。

９．他の認証の取得状況と取得年数は？（いくつでも）

１．ISO9000(QMS)
２．ISO14000(EMS)
３．ISO20000(ITSMS)
４．プライバシーマーク
５．その他



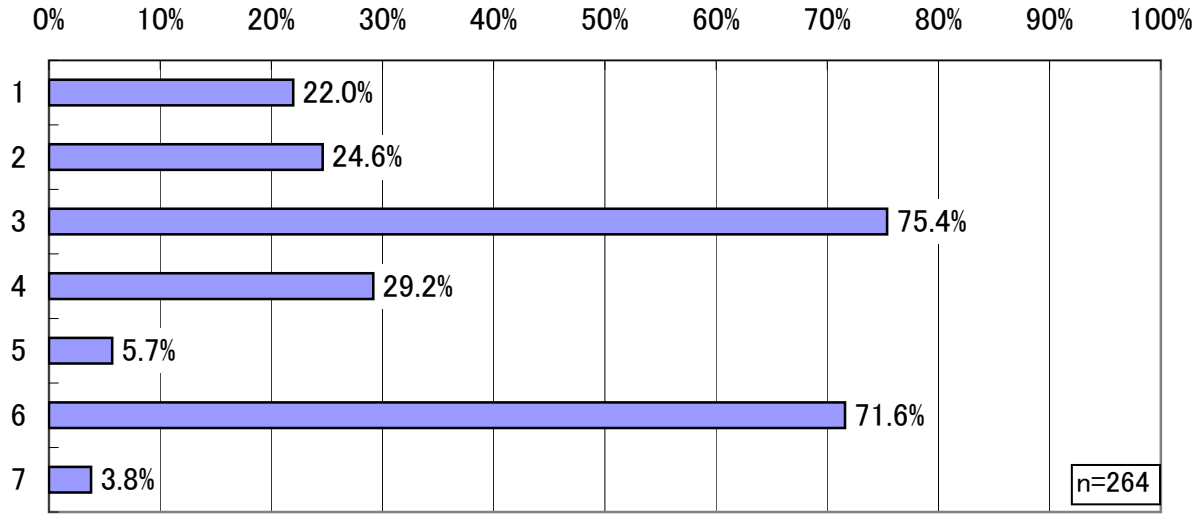
（単位：回答数・%）

総数	1	2	3	4	5
265	110	81	11	68	2
	41.7%	30.7%	4.2%	25.8%	0.8%

ISMS以外の認証取得のケースとしては、品質マネジメントシステムが比較的多いが、個人情報の保護に関するマネジメントシステムであるプライバシーマークの認証を取得していると答えた企業が全体の25%存在する。
また、最近パイロット運用から本格運用に移行したばかりのISO20000(ITSMS)認証取得を回答した企業が、11社存在するが、この結果はISO20000のもととなったBS15000あるいはITILの運用についての回答も含まれていると考えられる。

１０．　ISMSを取得した主な目的は？（いくつでも）

１．会社業務の運営をISMS認証に基づいた方法にするため
２．ISMS認証の考え方を部分的に入れて業務の改善を狙った
３．ISMS認証を得ることで営業活動において有利になるあるいは不利にならないことを狙った
４．入札その他でISMS認証取得が条件になっているため
５．グループ会社等の方針で決まっているため
６．情報セキュリティ対策の向上を狙った
７．その他



（単位：回答数・%）

総数	1	2	3	4	5	6	7
264	58	65	199	77	15	189	10
	22.0%	24.6%	75.4%	29.2%	5.7%	71.6%	3.8%

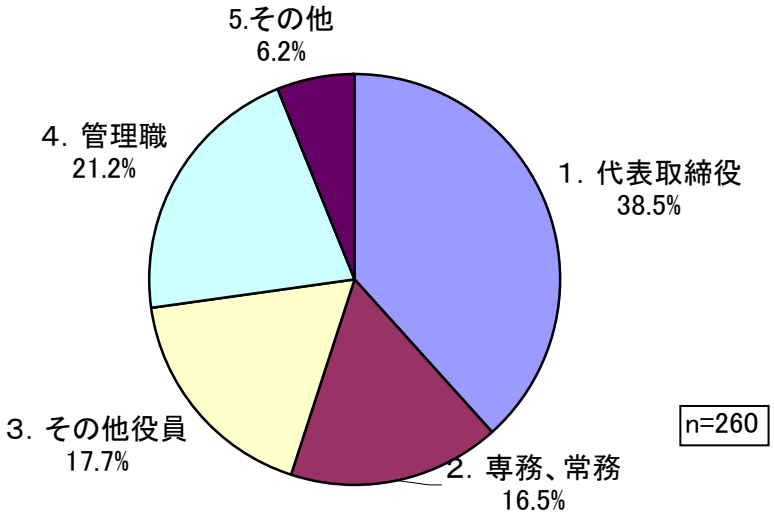
「1．会社業務の運営をISMS認証に基づいた方法にするため」、あるいは「2．ISMS認証の考え方を部分的に入れて業務の改善を狙った」に表されるようなISMSのマネジメントシステムとしての側面からの採用よりも、「3．ISMS認証を得ることで営業活動において有利になるあるいは不利にならないことを狙った」ないし「4．入札その他でISMS認証取得が条件になっているため」で記載される企業、組織の営業戦略上の事由による目的をあげる組織が多い。

また、目的として情報セキュリティ対策の向上をあげた組織、企業が次いで多いことから、ISMSを自組織におけるセキュリティ対策実施状況の基準とすることも取り組みにおいて期待されていたことがうかがえる。

ISMS認証取得関連

１１．一番初めにISMS認証取得について発案したのは誰か？（どれか１つ）

１．代表取締役
２．専務、常務
３．その他役員
４．管理職
５．その他



（単位：社数・%）

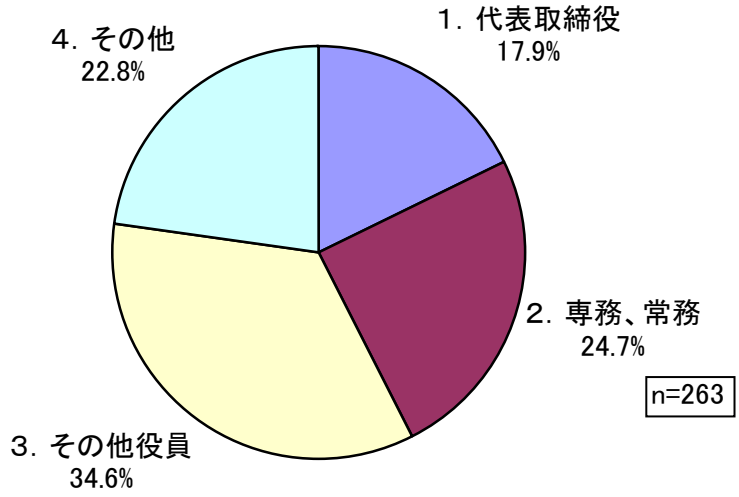
総数	1．代表取締役	2．専務、常務	3．その他役員	4．管理職	5.その他
260	100	43	46	55	16
100%	38.5%	16.5%	17.7%	21.2%	6.2%

「1．代表取締役」と回答した企業が全体の38.5%を占め、その他の回答からも経営資源の投入のデシジョンのできる役員以上の役職からの発案が全体の7割を超えており、ISMSの認証取得をビジネス上の戦略としてとらえ、認証の取得をトップダウンで指示している傾向が明らかになった。

組織、記入者について

１２.現時点で、ISMS認証の運用責任者は誰か？（どれか１つ）

１．代表取締役
２．専務、常務
３．その他役員
４．その他



（単位：社数・%）

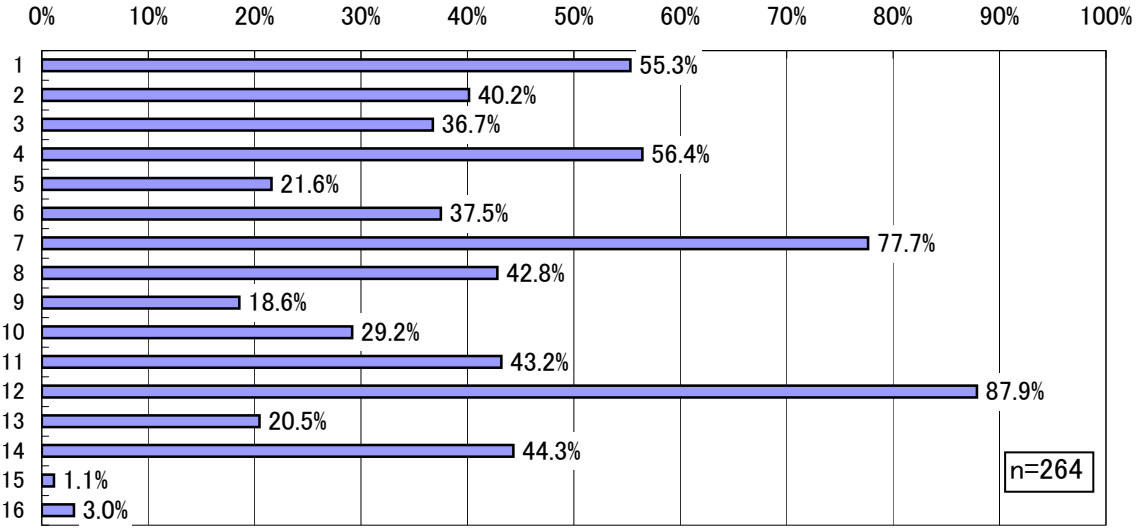
運用責任者	総数	１．代表取締役	２．専務、常務	３．その他役員	４．その他
社数	263	47	65	91	60
%	100.0%	17.9%	24.7%	34.6%	22.8%

問11の質問の発案者の回答が、代表取締役や専務、常務役員クラスが比較的多かったことに比較すると、実運用の責任者となっているのは範囲を管掌する役員であるように見受けられる。これは、ISMSの適用範囲が全社単位ではないことも影響していると考えられる。

ISMSの効果

１３．ISMS認証取得によって得られた効果は？（いくつでも）

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



総数	1	2	3	4	5	6
264	146	106	97	149	57	99
	55.3%	40.2%	36.7%	56.4%	21.6%	37.5%
	7	8	9	10	11	12
	205	113	49	77	114	232
	77.7%	42.8%	18.6%	29.2%	43.2%	87.9%
	13	14	15	16		
	54	117	3	8		
	20.5%	44.3%	1.1%	3.0%		

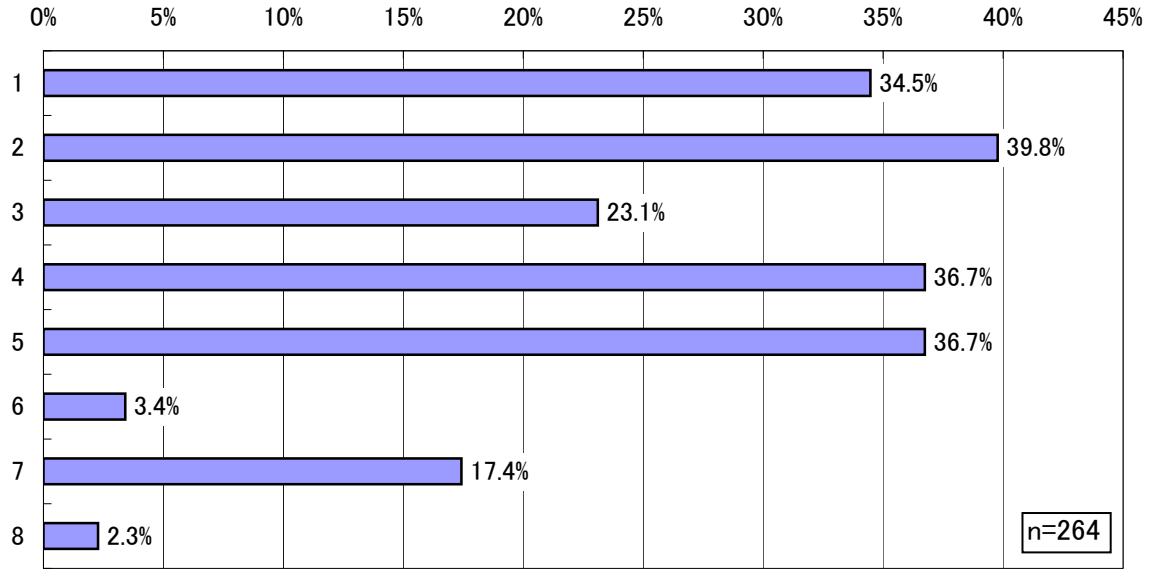
ISMS認証を取得し運用を開始した事業者は、様々な効果を得ていると考えられる。この質問はどのような効果を得ていると考えているか、確認する目的を持っている。
回答のうち、一番多かったのは社員のセキュリティ意識の浸透と実践、2番目が情報資産の明確化と整理、となった。これらは一般的なISMSの効果の印象と合致する。

全体でみると、1事業者あたり平均約6.2個の回答を選択している。また、逆に効果が特になかったという回答は3件のみで非常に少ない結果となった。
これらより、ISMS認証取得事業者はISMSの効果を感じており、情報セキュリティ体制の確立という観点からはISMSにはその効果があると考えてよいだろう。

ISMSの効果

１４．ISMS認証取得で発生した想定外の影響は？　（いくつでも）

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
３．手続きの煩雑化・業務効率の低下
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
６．セキュリティ事件・事故が増えた又は変わらない
７．業務への影響は特にない
８．その他（記入欄有り）



総数	1	2	3	4	5	6
264	91	105	61	97	97	9
	34.5%	39.8%	23.1%	36.7%	36.7%	3.4%

7	8
46	6
17.4%	2.3%

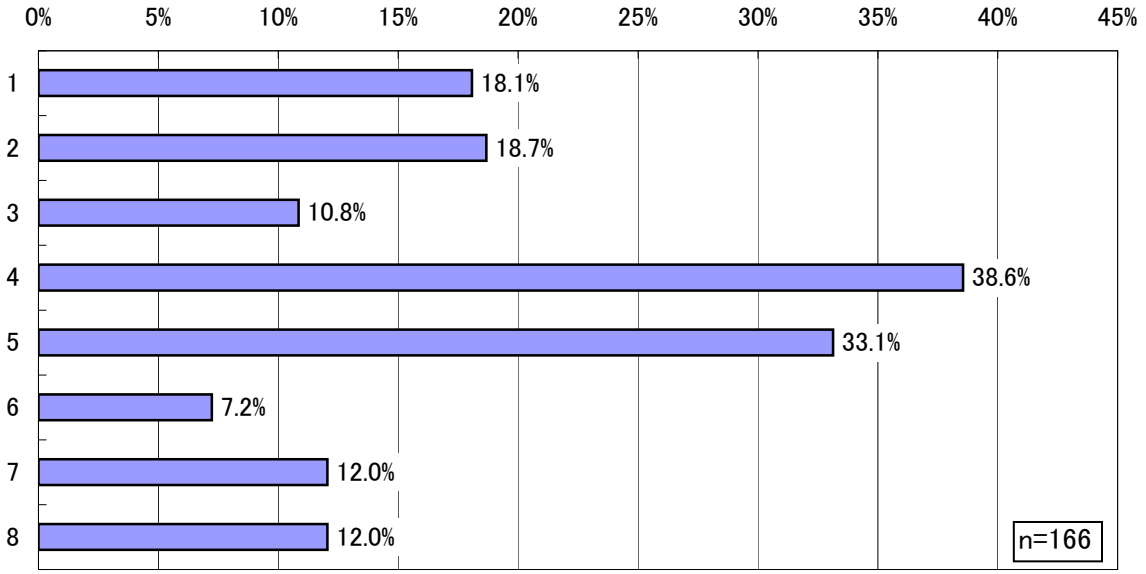
ISMS認証の想定外の影響についての設問だが、「7．業務への影響は特にない」、が17．4%となり、業務に何らかの影響を受けていると考えている事業者は82.6%になる。
何らかの影響を受けていると感じている事業者は、1事業者あたり平均2.1個を選択している。

「6．セキュリティ事故・事件が増えた又は変わらない」、が少ないことからインシデントの発生頻度は低下していると考えている担当者が多いことが伺えるが、実際にインシデントが発生していない可能性も高い。

ISMSの効果

１５．問１４で「２．業務量の増加」、「３．手続きの煩雑化・業務効率の低下」を回答された方に質問します。それらはどのようなものか？（いくつでも）

１．不要な作業申請等の作成
２．不要な作業履歴の記録
３．実際の手続きとマニュアルが異なる
４．監査目的の資料作成
５．ISMS事務局などからの直接業務に関係のない依頼作業が増加した
６．厳格な入退出管理で、他部門とのコミュニケーションが悪化
７．情報を利用・取得しづらくなった
８．その他（記入欄有り）



総数	1	2	3	4	5	6
166	30	31	18	64	55	12
	18.1%	18.7%	10.8%	38.6%	33.1%	7.2%

7	8
20	20
12.0%	12.0%

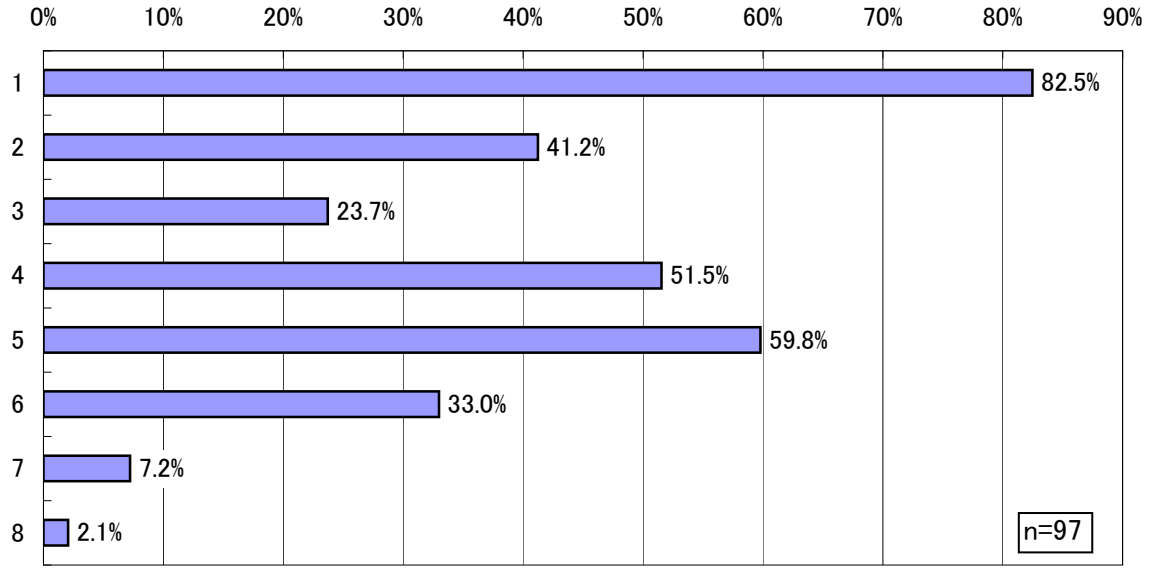
問14．で「作業量の増加」および「手続きの煩雑化・業務効率の低下」を選択した回答者166名がこの設問に回答した。
回答「4．監査目的の資料作成」が38.6%、「5．ISMS事務局などからの直接業務に関係な依頼作業が増加した」、が33.1%とこの2つの回答率が高かった。
1事業者あたり、平均1.5個の回答を選択している。

他の回答項目も低いながらも回答されているところから、ISMS認証のオーバーヘッドを感じている事業者が多いことが伺える。

ISMSの効果

１６．問１４で「４．業務上の制約が増加」を回答された方に質問します。
ISMSの導入で現場における業務上の制約は？（いくつでも）

１．機器の取扱（含む持出・込）に関する制約
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（記入欄有り）



総数	1	2	3	4	5	6
97	80	40	23	50	58	32
	82.5%	41.2%	23.7%	51.5%	59.8%	33.0%

7	8
7	2
7.2%	2.1%

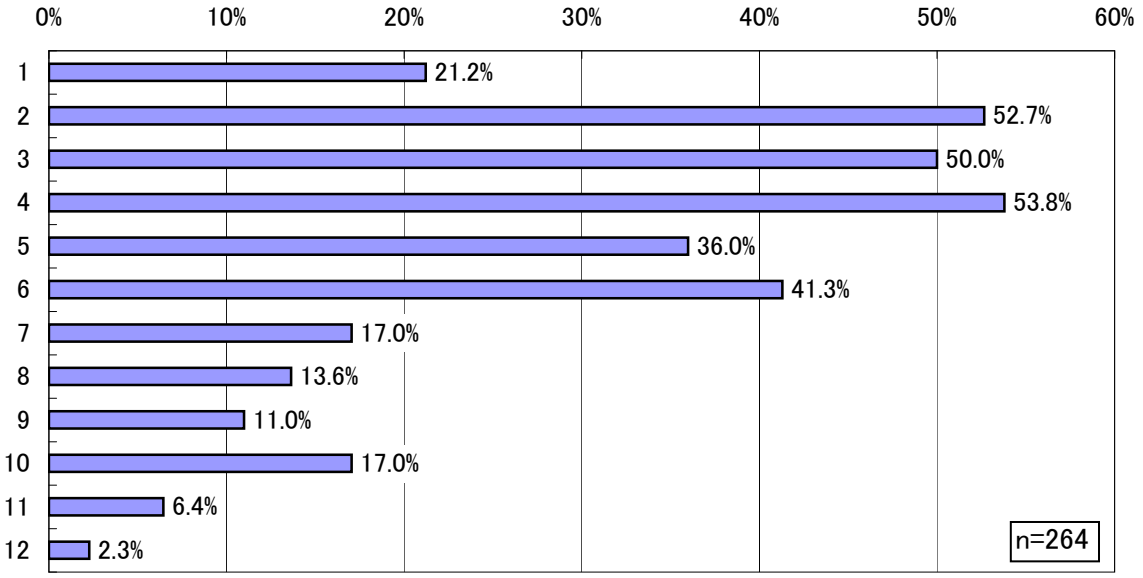
問14で「4．業務上の制約が増加」、と回答した97名が、この設問に回答した。このなかで、8割を超える回答者が「1．機器の取り扱いに関する制約」、をあげている。機器を自由に使えない不便さが制約の原因の一つになっているようだ。また「4．資料の作成ルールや保存場所の指定」、「5．上長の承認の増加」、なども高い割合で制約と感じている。

平均すると1事業者あたり3個の回答を選択している。
この質問の回答選択肢はいずれも重要な情報セキュリティ対策を含むものである。これらの施策は認証取得段階のリスクアセスメントの結果を受けて決定されているはずである。ここで業務上の制約と感じるとすれば、過剰な制約を含むルールになっている、ルールの趣旨が十分に浸透していない、等の理由が考えられる。

ISMSの効果

１７．ISMS認証取得後の運用で負担になっている作業は？（いくつでも）

１．セキュリティ委員会の開催
２．ポリシー（含む規定類、業務マニュアル等）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（記入欄有り）



総数	1	2	3	4	5	6
264	56	139	132	142	95	109
	21.2%	52.7%	50.0%	53.8%	36.0%	41.3%
	7	8	9	10	11	12
	45	36	29	45	17	6
	17.0%	13.6%	11.0%	17.0%	6.4%	2.3%

ISMS認証を運用していくにあたって、負担と感じる作業項目を問うている。
いずれの項目も作業項目として必須のものばかりだが、回答したISMS担当者は負担に感じている割合が高い。特に、「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」、はいずれも高い割合で負担を感じるとなった。

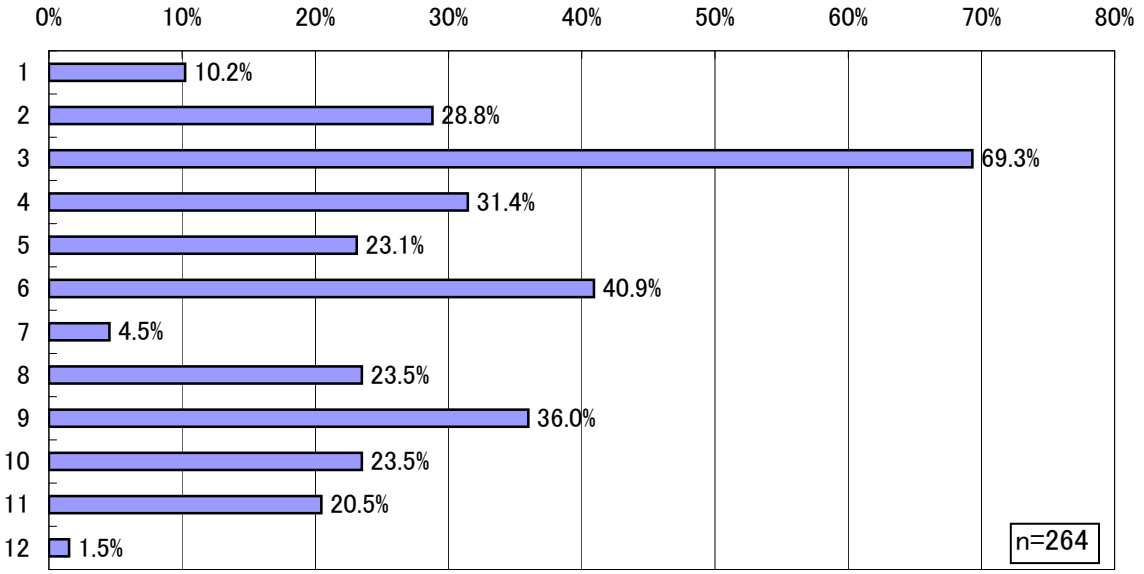
これらの作業は一般的に作業量が大きく、また現場の協力が必要となる項目である。さらにISMSではこれらの作業を定期的に行うことが求められており、それが負担と感じる一因となっていると考えられる。

ISMSの効果

１８．現在、ISMSの効果を高めるために重点的に取り組んでいる（含む予定）ものは？（いくつでも）

１．経営者の認識・理解の向上	２．管理者層の認識・理解の強化
３．一般社員の認識・理解の強化	４．マニュアルの整備
５．内部監査担当のスキル強化	６．有効性評価手法の改善
７．費用対効果の説明手法の明確化	８．リスク分析手法の改善（※）
９．教育研修の改善（※）	１０．文書・記録管理の改善（※）
１１．インシデント対応の向上（※）	１２．その他（記入欄有り）

※ツールの導入を含む



総数	1	2	3	4	5	6
264	27	76	183	83	61	108
	10.2%	28.8%	69.3%	31.4%	23.1%	40.9%
	7	8	9	10	11	12
	12	62	95	62	54	4
	4.5%	23.5%	36.0%	23.5%	20.5%	1.5%

ISMSの効果を高めるために重点的に取り組んでいる作業は、「3．一般社員の認識・理解の強化」が飛び抜けて多い。「6．有効性評価手法の改善」はISMSがISO/IEC27000にかわり有効性評価が厳しくなるとの話に対応した動きといえよう。

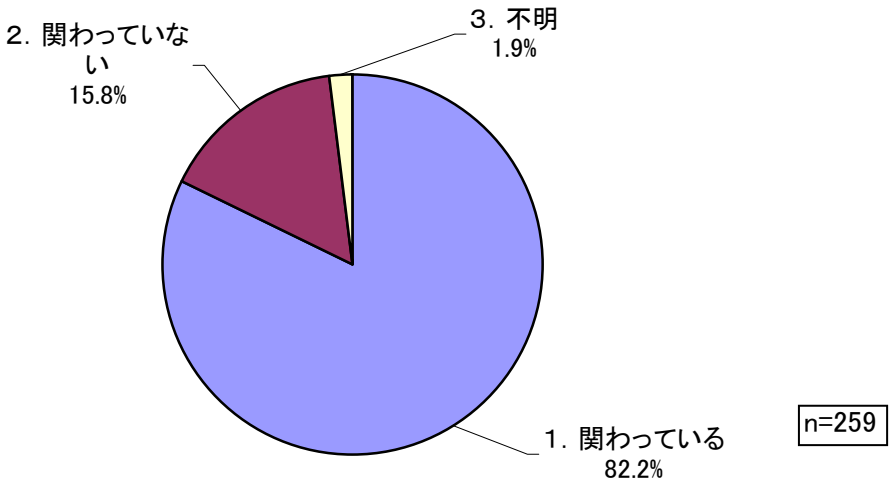
次に 「9．教育研修の改善」と続くがこれらの項目には大きな差がない。1事業者あたり3.1個の回答を選択している。ISMS認証を取得して、時間が経っていない企業も多いことから、一般社員への教育は定番として取り組んでいる様子であるが、次の一手は各事業所によってばらついているといえるだろう。

少ないのは「7．費用対効果の説明手法」、でこれについてはほとんど取り組まれていないと言って良い状況である。また「1．経営者の認識・理解の向上」についても平均よりも小さな値となった。

ISMS認証に関連する体制

１９．ISMSの継続的な運用のために経営陣はマネジメントレビュー以外に関わっているか？
（どれか一つ）

１．関わっている
２．関わっていない
３．不明



（単位：社数・%）

総数	１．関わっている	２．関わっていない	３．不明
259	213	41	5
100%	82.2%	15.8%	1.9%

ISMSの実効性を高め、継続的な活動を実施するためには経営陣の積極的な関与が必要不可欠であることから、認証規格で求められているマネジメントレビュー以外の経営陣の関わり方について調査した。その結果、80%超の企業が「１．関わっている」と回答しており、経営陣がISMSの取組みに積極的に関与していることが見て取れる結果となった。一方、「２．関わっていない」、「３．不明」と回答した企業も17.7%（46社）あった。

ISMS認証に関連する体制

２０．事務局のメンバーは何人か？

１．専任　（　　人）
２．兼務　（　　人）
３．その他（　　人）

図1.事務局の人数

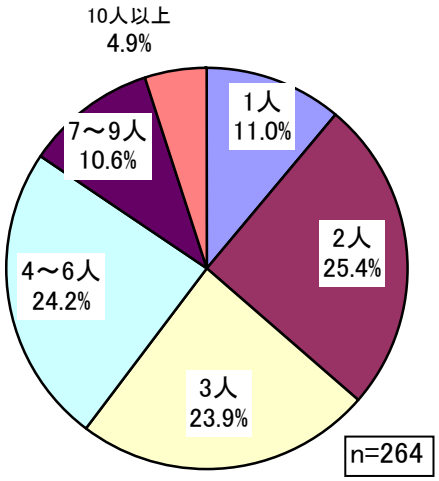


図2.事務局の体制

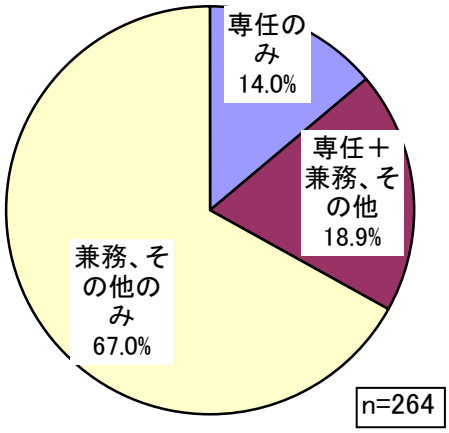


図1.事務局の人数　（単位：社数・%）

総数	1人	2人	3人	4～6人	7～9人	10人以上
264	29	67	63	64	28	13
100%	11.0%	25.4%	23.9%	24.2%	10.6%	4.9%

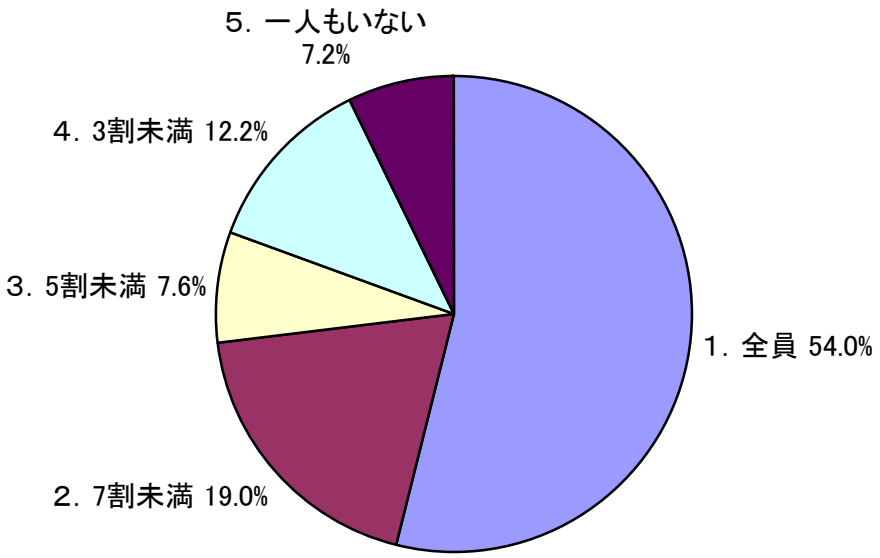
図2.事務局の体制　（単位：社数・%）

総数	専任のみ	専任+兼務、その他	兼務、その他のみ
264	37	50	177
100%	14.0%	18.9%	67.0%

事務局の人数は3人以下と回答した企業が60%を占めており、全体的に少人数で運営している傾向が見て取れる（図1.）。また、事務局の体制としては、専任担当者を置いている企業は全体の33%に過ぎず、大半の企業が兼務体制で運営していることが伺える。今回のアンケートの意見にも、「予算的に専任部署を設置できず、結果として事務局メンバー（兼務担当者）の負荷が高くなっている」という意見もあり、いかに事務局を運営するかが課題になっていると言える。

ISMS認証に関連する体制

21. 現在の事務局には初回認証取得の際のメンバーが、どのくらいの割合で残っているか？（どれか1つ）
1:全員残っている
2:7割未満
3:5割未満
4:3割未満
5:一人もいない



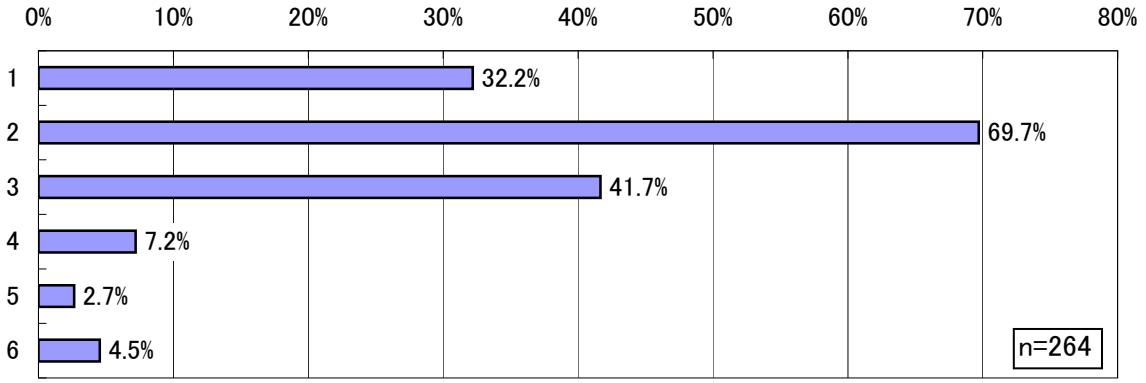
総数	1. 全員	2. 7割未満	3. 5割未満	4. 3割未満	5. 一人もいない
263	142	50	20	32	19
	54.0%	19.0%	7.6%	12.2%	7.2%

全体の約5割強の企業が「1. 全員残っている」と回答した。さらに「2. 7割未満」を含めると、全体の約7割以上となり、認証取得時のメンバーが中心となって事務局を運営している実態が明らかになった。この傾向は、今回のアンケートに回答した事業者の7割以上が2005年以降に認証を取得しており、認証取得後間もないことが影響していると考えられる。

ISMS認証に関連する体制

２２．新しいメンバーに対してどのような形でISMSに関連したスキル習得を行ったか？（いくつでも）

１．外部講習によるスキル習得
２．社内講習によるスキル習得
３．ＯＪＴによる習得
４．独学（個人に任せている）
５．特に無し
６．その他



総数	1	2	3	4	5	6
264	85	184	110	19	7	12
	32.2%	69.7%	41.7%	7.2%	2.7%	4.5%

新メンバーに対する教育方法としては「2．社内講習によるスキル習得」と回答した企業が69.7%（184社）あり、OJTと合わせて社内の教育プログラムを通じてスキル習得を行っていることが伺える。ただし外部講習と回答した企業も32.2%（85社）あり、自社の教育プログラムの不足を外部講習で補っているものと思われる。また「6．その他」の記述回答で多かったのは「新メンバーは入ってない」というものであった。

ISMS認証に関連する体制

２３．外部コンサルタントの支援は？（どれか一つ）

認証取得まで
１．受けている　　２．一部受けている　　３．受けていない

認証取得後
１．受けている　　２．一部受けている　　３．受けていない

図1.認証取得まで

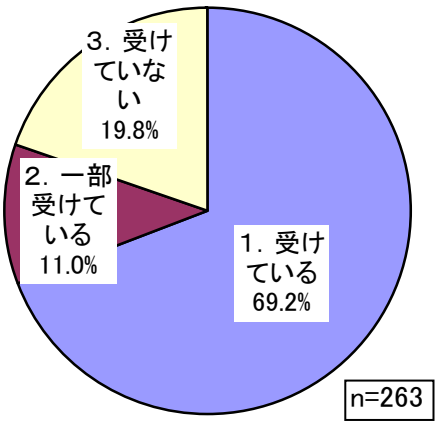


図2.認証取得後

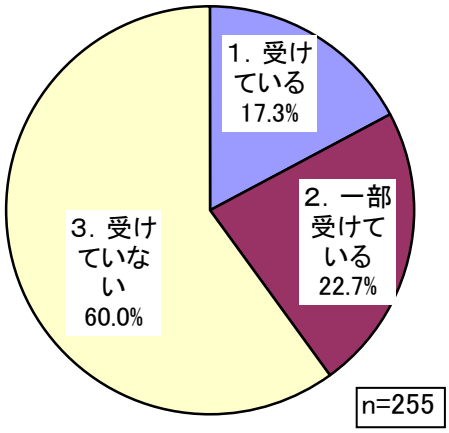


図1.認証取得まで　　（単位：社数・%）

総数	1．受けている	2．一部受けている	3．受けていない
263	182	29	52
100%	69.2%	11.0%	19.8%

図2.認証取得後　　（単位：社数・%）

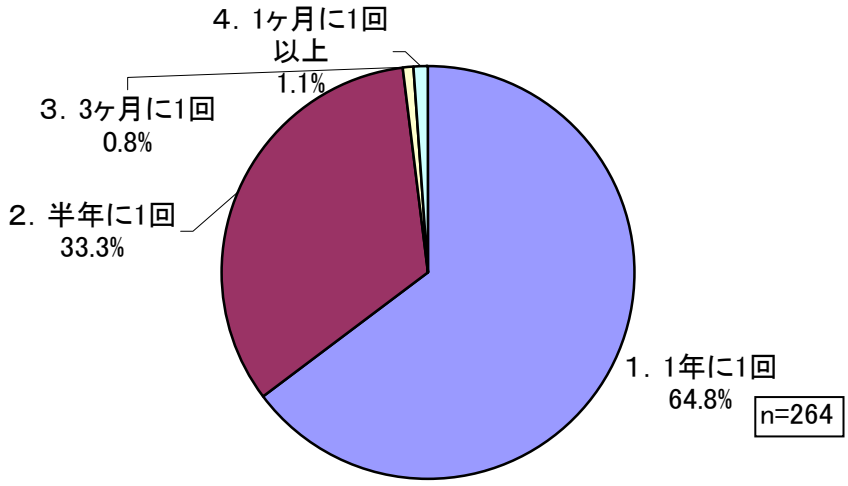
総数	1．受けている	2．一部受けている	3．受けていない
255	44	58	153
100%	17.3%	22.7%	60.0%

外部コンサルタントの利用については、認証取得前に「1．受けている」「2．一部受けている」と回答した企業が80%を超えており、認証を取得するために外部コンサルタントを利用した企業が多いことが伺える。一方、認証取得後は60%の企業が「3．受けていない」と回答しており、認証取得後の維持管理については自社で実施する傾向が見て取れる。

内部監査・マネジメントレビュー

２４．内部監査の実施頻度は？（どれか１つ）

１．１年に１回
２．半年に１回
３．３ヶ月に１回
４．１ヶ月に１回以上



（単位：社数・%）

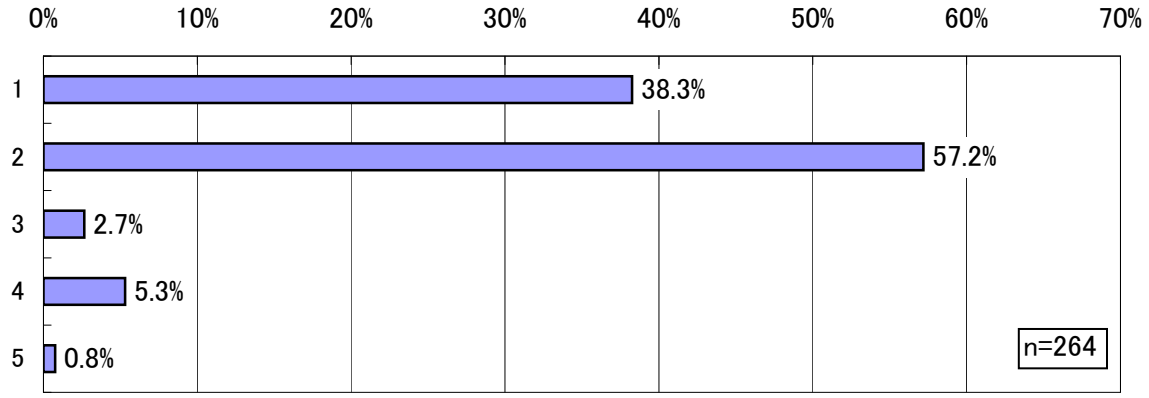
総数	１．1年に1回	２．半年に1回	３．3ヶ月に1回	４．1ヶ月に1回以
264	171	88	2	3
100%	64.8%	33.3%	0.8%	1.1%

「１．1年に1回」及び「２．半年に1回」など半年に1回以上と回答した企業が全体の98%以上となり大半を占めている。逆に「３．3ヶ月に1回」及び「４．1ヶ月に1回以上」と答えた企業は全体のわずか2%に止まっている。
このことから、内部監査の実施頻度は半年以上が大半であり、3ヶ月以内の短期間での実施は少数派であることが判明した。

内部監査・マネジメントレビュー

２５．内部監査体制は？（いくつでも）

１．常設の社内チーム
２．非常設の社内チーム
３．外部機関
４．外部機関と社内機関の共同体制
５．その他（記入欄あり）



総数	1	2	3	4	5
264	101	151	7	14	2
	38.3%	57.2%	2.7%	5.3%	0.8%

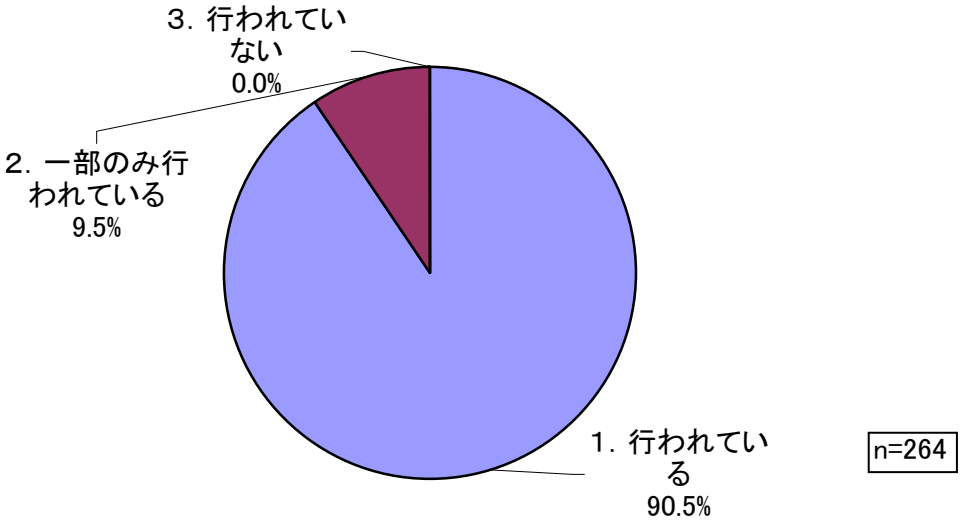
「2．非常設の社内チーム」の回答が最も多く、全体の約57.2%を占めている。また、「1．常設の社内チーム」及び「2．非常設の社内チーム」との回答が大半を占めており、全体の95.5%に及んでいる。

このことから、内部監査体制はほとんどが社内チームで構成されており、外部機関を利用するのは少数派となっていることが判明した。

内部監査・マネジメントレビュー

２６．内部監査指摘事項に対する改善は行われているか？（どれか１つ）

１．行われている
２．一部のみ行われている
３．行われていない



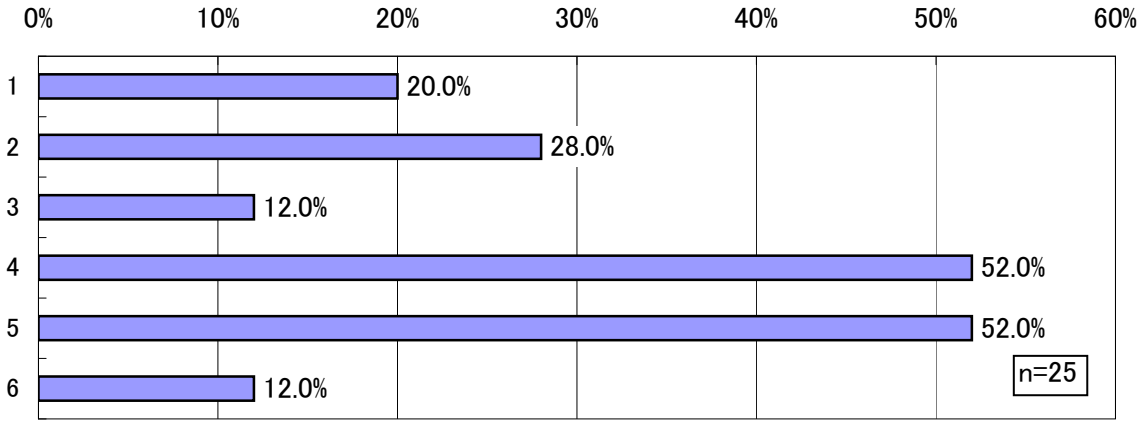
総数	1．行われている	2．一部のみ行われている	3．行われていない
264	239	25	0
100%	90.5%	9.5%	0.0%

「1．行われている」が全体の約91%を占めている。また、「3．行われていない」と回答した企業はなかった。
このことから、改善が行われているのが大多数である。また、一部のみ行われているを含めて、内部監査指摘事項に対する改善はすべて行われているということが判明した。

内部監査・マネジメントレビュー

２７．問２６で「２．一部のみ行われている」「３．行われていない」と回答された方に質問します。その理由は？（いくつでも）

１．内部監査の指摘が適切でない
２．改善対策に対するマネージメントの支援が不十分
３．現場の協力が得られない
４．現場に改善作業を行う余力が無い
５．事務局に改善作業を行う余力が無い
６．その他（記入欄有り）



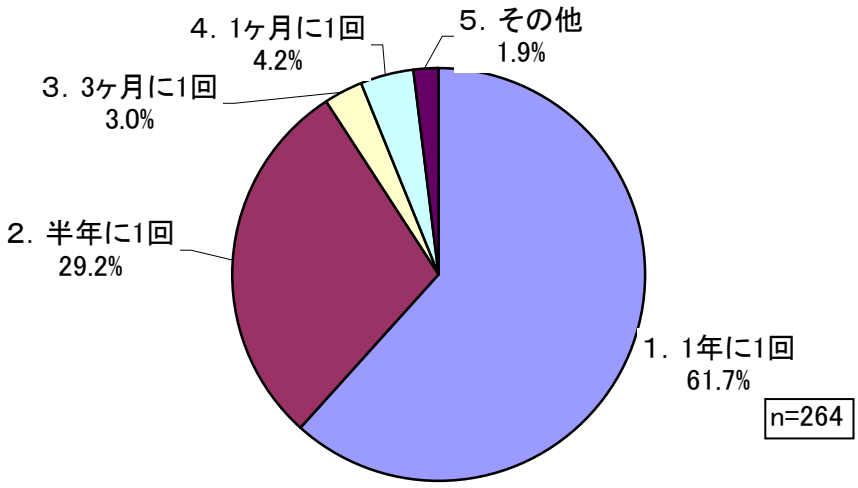
総数	1	2	3	4	5	6
25	5	7	3	13	13	3
	20.0%	28.0%	12.0%	52.0%	52.0%	12.0%

「４．現場に改善作業を行う余力が無い」、「５．事務局に改善作業を行う余力が無い」という回答が最も多い結果となり、それぞれ半数以上が両回答を選択している結果となった。逆に「３．現場の協力が得られない」との回答は最も少なかった。
　このことから、内部監査の指摘事項に対する改善が行われない理由としては、事務局や現場に改善作業を行う余力が無いことが大きな割合を占めていることが判明した。

内部監査・マネジメントレビュー

２８．マネジメントレビューの頻度は？（どれか１つ）

１．１年に１回
２．半年に１回
３．３ヶ月に１回
４．１ヶ月に１回
５．その他（記入欄有り）



（単位：社数・%）

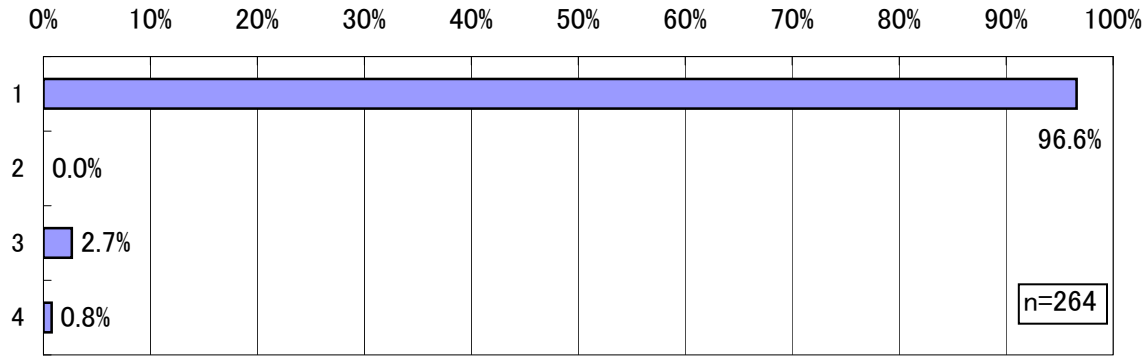
総数	１．1年に1回	２．半年に1回	３．3ヶ月に1回	４．1ヶ月に1回	５．その他
264	163	77	8	11	5
100%	61.7%	29.2%	3.0%	4.2%	1.9%

「１．1年に1回」との回答が全体の約62%を占めており過半数となっている。さらに、「２．半年に1回」と回答した企業を含めた場合は全体の約91%に達している。また、「３．3ヶ月に1回」および「４．1ヶ月に1回」は全体の3%、4%となり少数派となっている。
このことから、マネジメントレビューの頻度は半年以上が大多数あり、3ヶ月以内の短期間での実施は少数派であることが判明した。

内部監査・マネジメントレビュー(6)

２９．マネジメント・レビューはどのような形で実施されているか？
（いくつでも）

１．会議で実施
２．電子メールで実施
３．会議、メールの組み合わせで実施
４．その他（記入欄有り）



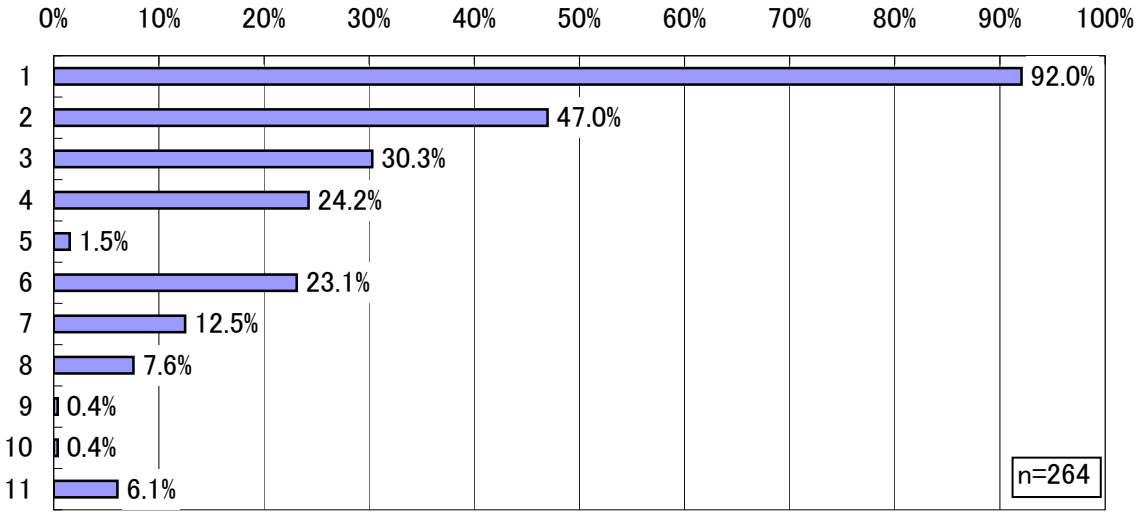
総数	1	2	3	4
264	255	0	7	2
	96.6%	0.0%	2.7%	0.8%

「1．会議で実施」と回答した企業が全体の約97%を占めており大多数である。また、「2．電子メールで実施」と回答した企業はなかった。
このことから、マネジメントレビューは会議で実施するのが大多数となっており、電子メールだけで実施しているケースは存在しないことが判明した。

教育

３０．ISMSの維持に必要な社員教育の手段は？（いくつでも）

１．　集合研修	２．　冊子の配布
３．　ＯＪＴ	４．　Web学習
５．　ソフトウェア	６．　メール
７．　ビデオ	８．　自己啓発
９．　通信教育	１０．特に行っていない
１１．その他（記入欄有り）	



総数	1	2	3	4	5	6
264	243	124	80	64	4	61
	92.0%	47.0%	30.3%	24.2%	1.5%	23.1%
	7	8	9	10	11	
	33	20	1	1	16	
	12.5%	7.6%	0.4%	0.4%	6.1%	

教育手段のうち、最も多いのが集合研修であり、そのほかの項目とあわせ、ほとんどの企業が何らかの形で取り組んでいる。また、複数の手段を組み合わせている企業も比較的多い。

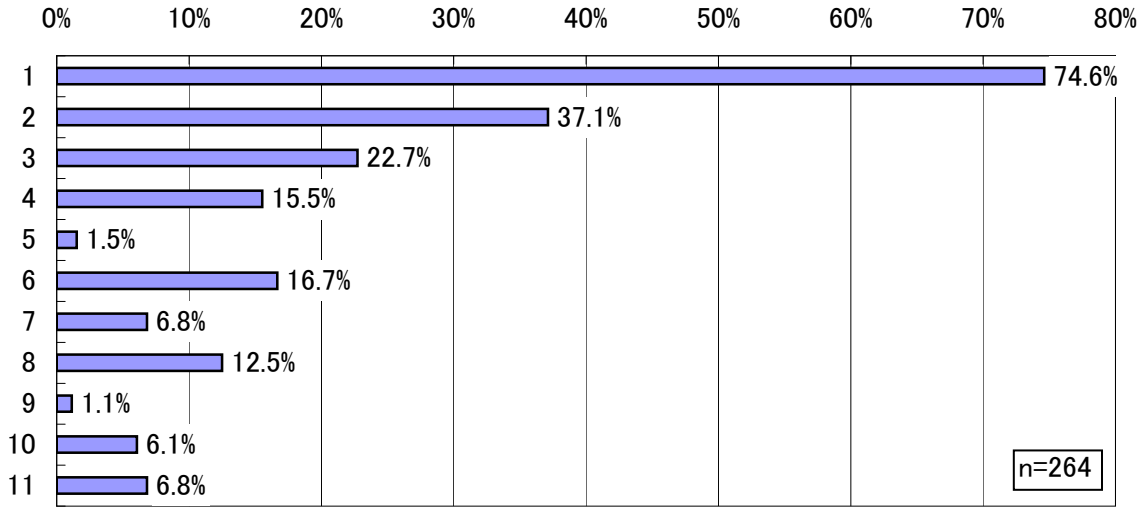
ISMSにおいて、教育の重要性が指摘されている事に連動しての結果と思われる。

多くの企業にとって集合研修は取り組みやすいものであると同時に、集合研修一般において、個々のレベルに最適化した研修が行いにくいという欠点がある。その点を改善し、集合研修の効果を上げることは、ISMS及びセキュリティの普及啓発に対して効果的であるとも考えられる。

教育

３１．それでは管理者教育は？（いくつでも）

１．　集合研修	２．　冊子の配布
３．　ＯＪＴ	４．　Web学習
５．　ソフトウェア	６．　メール
７．　ビデオ	８．　自己啓発
９．　通信教育	１０．　特に行っていない
１１．その他（記入欄有り）	



総数	1	2	3	4	5	6
264	197	98	60	41	4	44
	74.6%	37.1%	22.7%	15.5%	1.5%	16.7%
	7	8	9	10	11	
	18	33	3	16	18	
	6.8%	12.5%	1.1%	6.1%	6.8%	

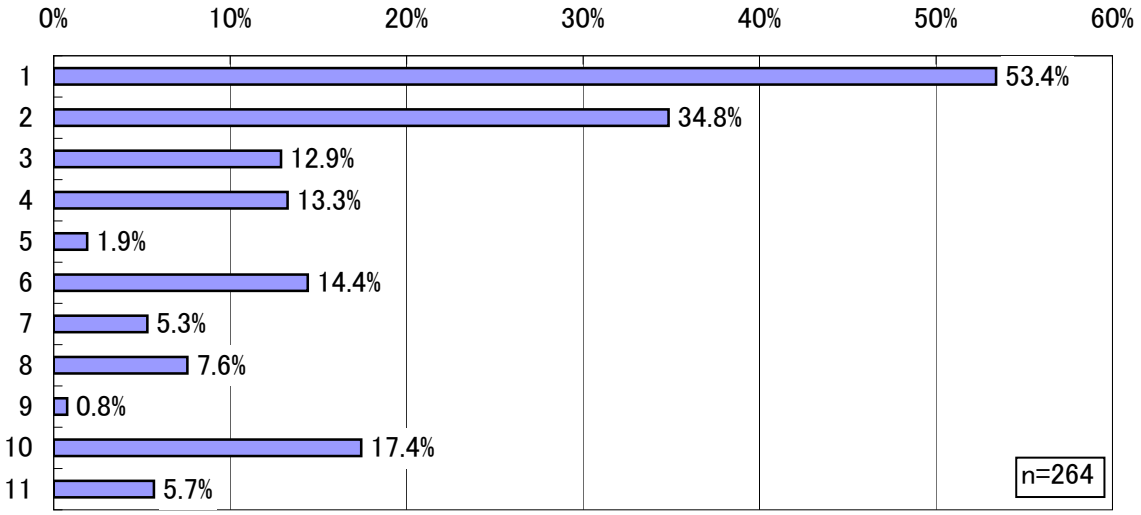
管理職になると、一般社員においてはほとんどなかった「１０．特に行っていない」という企業が増加、また、全体に件数が減少している様子が見て取れる。
さらに、集合研修についての件数も減少している。

管理職と一般社員の研修に温度差があり全体に管理職の研修が少なくなっている。
ISMSの効果向上において、管理職の理解は重要だが、単にマネジメント層ということでその頻度が減少しているとすると、改善の余地があるとも考えられる。

教育

３２．それでは役員教育は？（いくつでも）

１．　集合研修	２．　冊子の配布
３．　ＯＪＴ	４．　Web学習
５．　ソフトウェア	６．　メール
７．　ビデオ	８．　自己啓発
９．　通信教育	１０．　特に行っていない
１１．その他（記入欄有り）	



総数	1	2	3	4	5	6
264	141	92	34	35	5	38
	53.4%	34.8%	12.9%	13.3%	1.9%	14.4%
	7	8	9	10	11	
	14	20	2	46	15	
	5.3%	7.6%	0.8%	17.4%	5.7%	

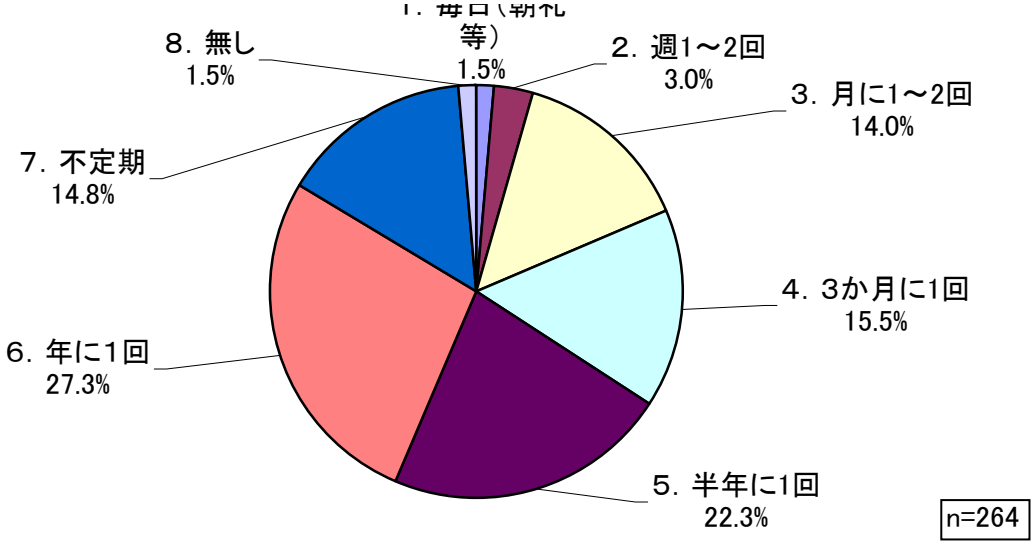
一般社員、管理職に比べて「１０．特に行っていない」がさらに増加している。
全体の傾向として、職位が上位のものほど、教育機会が少なく、対処されていない状況となっている。

現実的に多忙な役員について、なかなか教育機会を設けられないのは、やむを得ないことかもしれないが、内部統制などの効果を考えると、全体としての効果を維持する為には、どの階層においても教育は重要なはずである。このアンバランスは改善すべき対象ではないかと考えられる。

教育

３３．ISMSに関連した教育の頻度はどの程度か？（どれか１つ）

１．毎日（朝礼等）
２．週１～２回
３．月に１～２回
４．３か月に１回
５．半年に１回
６．年に１回
７．不定期
８．無し



（単位：社数・%）

総数	1．毎日（朝礼等）	2．週1～2回	3．月に1～2回	4．3か月に1回	5．半年に1回
264	4	8	37	41	59
100%	1.5%	3.0%	14.0%	15.5%	22.3%
	6．年に1回	7．不定期	8．無し		
	72	39	4		
	27.3%	14.8%	1.5%		

教育の頻度を聞いた質問だが、比較的短期間（毎日～3ヶ月）については、全体の34%、年に1-2回というレベル(不定期を含む）では、約64%となっている。

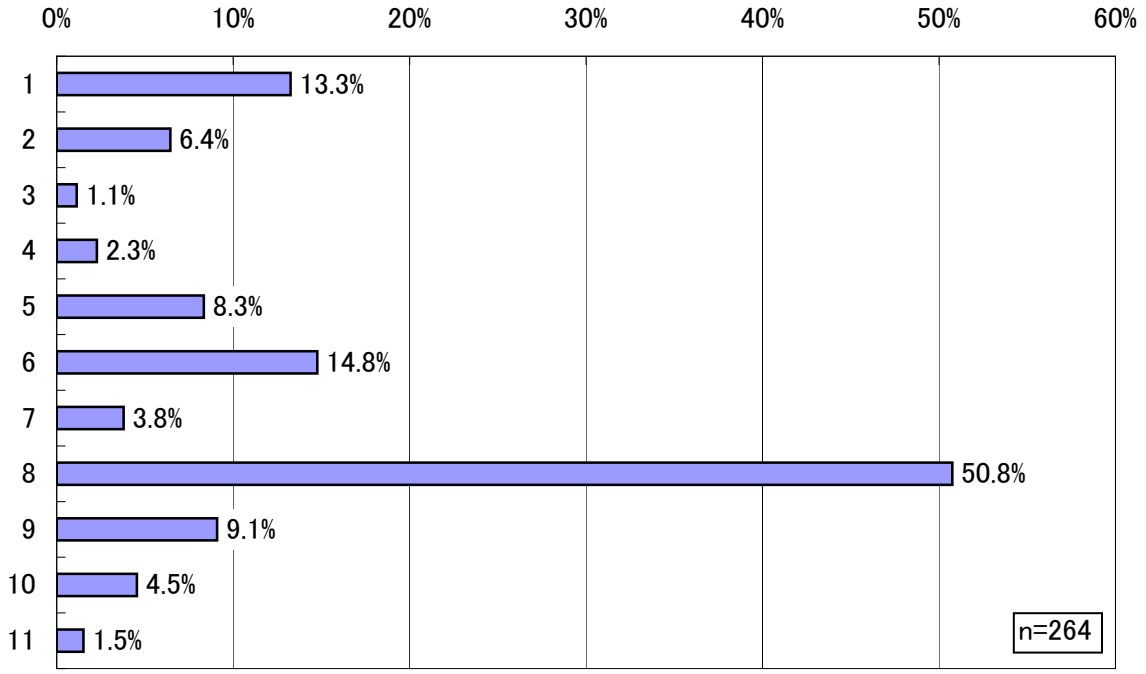
教育自体ある程度反復して行うことが効果的であるにもかかわらず、それを実践している企業はまだ多いとは言えない。

研修などを行うことは、ある意味、経費と負担が求められるため、回数を増やせない事情もあると思うので、あまり負担の重くない手段で、効果を継続できルような手段が必要とされているのではないかとも考えられる。

教育

３４．ISMSの教育担当部門は？（いくつでも）

１．総務
２．人事
３．経理
４．社長室
５．企画部門
６．情報システム管理部門
７．情報システム開発部門
８．情報セキュリティ担当部門
９．事業部門
１０．コンプライアンス担当部門
１１．リスク管理担当部門
１２．監査部門
１３．その他



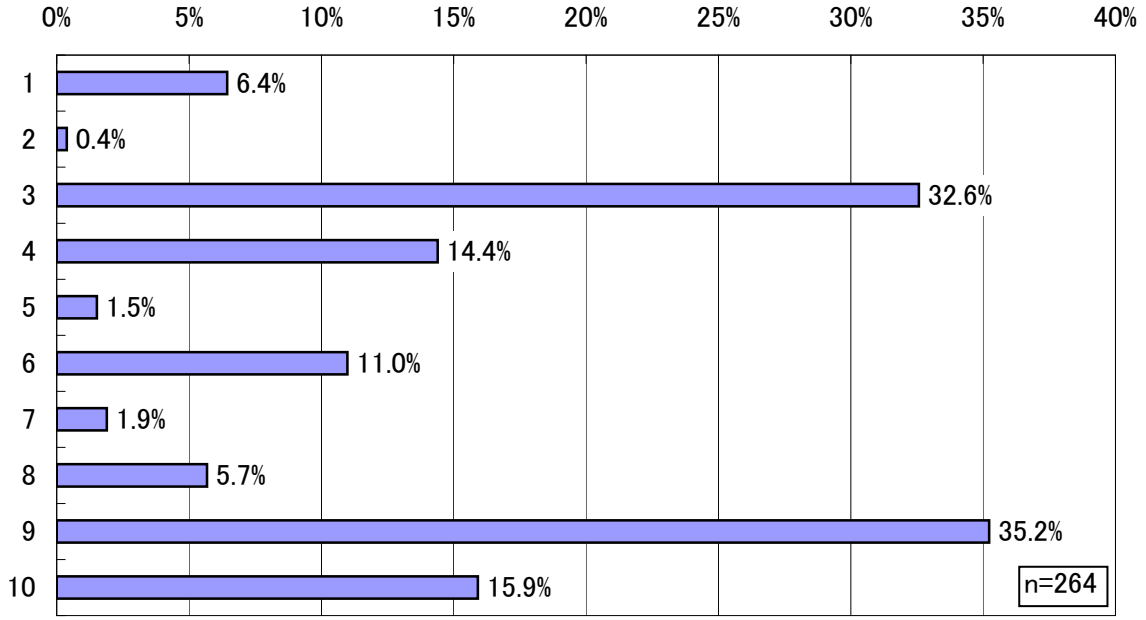
総数	1	2	3	4	5	6	
264	35	17	3	6	22	39	
	13.3%	6.4%	1.1%	2.3%	8.3%	14.8%	
	7	8	9	10	11	12	13
	10	134	24	12	4	9	40
	3.8%	50.8%	9.1%	4.5%	1.5%	3.4%	15.2%

ISMS自体を担当している部門との比較が必要だが、最も多いのは情報セキュリティ部門で、当然とも言える結果が出ている。
そのほかの総務・管理部門が担う場合は一般的な研修の対応として行われているのかもしれない。
企業規模などに応じ、部門などの構成に特徴があるのかもしれない。。

教育

３５．教育以外の啓発活動は？（いくつでも）

１．キャンペーン週間などの設定　　**２．マスコットの制定**
３．ポスターの掲示　　**４．ニュースレター・メルマガの発行**
５．啓発ビデオの作成　　**６．情報セキュリティに関連する標語の制定**
７．情報セキュリティへの取り組みの表彰（部門、個人）
８．セキュリティの標語などを書いたノベルティの配布
９．啓発活動は特に行っていない　　**１０．その他**



総数	1	2	3	4	5	6
264	17	1	86	38	4	29
%	6.4%	0.4%	32.6%	14.4%	1.5%	11.0%
	7	8	9	10		
	5	15	93	42		
	1.9%	5.7%	35.2%	15.9%		

「9．特に行っていない」という回答が全体の約35%を占めている一方で、そのほかの企業については、教育以外に何らかの啓発活動を行っている状況であることがわかる。
少なからず、効果を向上させるために、教育とは別の対応を行っている企業が多いということになる。

ただ、手段については、社員などが積極的に関与するメルマガや表彰といったものは多くはなく、最も多いのはポスターの掲示などで、あまり積極的なものではない。
啓発手段についても、さらに、改善が必要であると考えられる。

付録D　ISMS認証取得事業者へのインタビュー

(1) A社へのインタビュー

訪問した事業者　　A 社
日　時　　2007 年3月中旬
場　所　　首都圏
出席者　　情報セキュリティ専門部署の部長　1名

概　要

① 出席者の担当業務

- 出席者は、ISMS、P マークなどの事務局を担当する情報セキュリティ専門部署に専任で所属している。ISMS 関連では内部監査やマネジメントレビューの開催など情報セキュリティ関連業務の中核的な役割を担っている。

② ISMS対象人数

- A 社全社で ISMS 認証を取得している。全社の従業員は約150名で、別に外注の運用オペレータが多数存在する。

③ ISMS導入の背景

- 社長による取得指示により認証取得の作業が始まった。

④ ISMS導入の目的

- まず ISMS 認証取得ありきであり、取得だけが目標だった。また当時は認証の継続を考えていなかった。

⑤ ISMS導入の効果

- （課題を中心に話を聞いたため、特に回答無し）

⑥ ISMS導入の課題

- 「業務量の増加」、「人が必要になった」を感じている。その理由は、運用業務別に異なる組織であるため継続審査の準備等において人的応援が得られにくいということからである。事務局も兼務者が多く負担の軽重差があり、兼務者へのスケジュール調整が難しい、などの問題がある。
- 親会社のシステム運用の請負が主業務であるため親会社のポリシーに従うことが多く、A 社で制定しているセキュリティポリシーや運用ルールが適用されないケースが多い。A 社から親会社に働きかけるところまでは至っていない。
- 認証取得時に負担になったのは、コンサル会社が提示した「ISMS を取得する為の 400 の要求事項」への対応だった。この要求事項については予防対策が少ない印象だった。

- リスクアセスメントの見直しについては、当初はコンサルからの指摘が500～600カ所程度有り、100あまりの対策を打った。業務の変化が少ないこともあり、2～3年目以降はやるべきことが少なくなった。このことを審査時にうまく説明できないで困惑する。
- 内部監査時に指摘事項をたくさん出すと現場が困るために、政策的にその量を少なくすることがある。また長期継続的な対策の継続をする体制が明確でないため、指摘事項が長期的な課題だとその後の扱いが難しい。
- 事務局と現場のコミュニケーションに課題がある。現場はローテーション職場なので同じ話を複数回実施する必要性があり事務局専任者の負担が大きい。また事務局兼務者は現場優先で作業をしがちで ISMS を第一に考えていないため、これも専任者の負担が増える要因となっている。これは事務局兼務者に人事権限を持つ管理職クラスが入っていないために作業量の調整が柔軟に行われていないことも大きな要因である。

⑦ その他

- ISMS 認証を継続するために全社的に業務量が増加した。これは本で勉強しても事前にはわからなかったし、認証を継続するための話が取得時には無かった。会社の幹部も理解が不足していたのではと思う。コンサルは継続するための作業について十分に強調しなかった。
- セキュリティポリシーやルールの明確化は倫理を明文化しただけで、そもそも必要な事だったと思う。そう言うことから、ISMS 認証取得によって「制約の増加」が起きたとは感じていない。教育の充実や環境の整備が一番重要な要素であり、投資が必要と考える
- PDCA が大切で ISMS にこだわる必要はないと感じている。ただ ISMS を導入したのだから、これを使って組織の目標と現実の差異をつぶす必要ある。人事権限を持つ管理職クラスが担う必要があるのではないか。
- 長期計画の計画終了後の結果の検証、評価を行っていないため、PDCA がうまく機能せず同心円上を回っている様な気がする。
- マネジメントレビューは年に1回、セキュリティ委員会は6～7回行っている。しかし出席者の ISMS に対する理解度が低く、教育の必要性を感じる。
- 教育の手段はいくらもある。重要なのは理解できるかどうかである。事務局の兼務者は ISMS 認証審査委員補の資格を取得することになっている。人作りが大切である。
- ISMS 認証の継続審査に対するプレッシャーが大きくなってきている。

(2) B社へのインタビュー

訪問した事業者　B 社
日　時　2007 年3月中旬
場　所　首都圏
出席者　システムデータセンタ担当　中間管理職クラス　4名

概　要

① 出席者の担当業務

- 出席者は、データセンターのバッチ業務、小売業向けシステム、社内ネットワーク、データセンター設備等を担当されている。この4名がISMS事務局員。全員兼務で、現在も事務局で活動中。

② ISMS対象人数

- B 社及び協力会社を含め、約 100 名が ISMS 認証の対象業務に従事している。

③ ISMS導入の背景

- 3年程前にコンサル企業から情報システム担当役員にトップセールスがあった。
- P マークは取得済みで、P マーク審査員からは ISMS も十分カバーしていると言われた。
- 半年後位に、役員から再度 ISMS 認証取得についての検討指示がおりた。
- 出席者4名とも ISMS については全く知識が無い状態からのスタートであった。
- 当初、限定された範囲として、取得することを考えたが、社長から話がありデータセンター全体での取得を目指すことになった。
- 5年程前に、改めて役員会で承認され構築作業を開始した。組織を直接管掌する担当役員は、当初、ISMS 取得検討を指示した役員ではなかったが経営トップの考えは変化がなかった。

④ ISMS導入の目的

- 他社の情報セキュリティ事故・事件から、情報セキュリティの向上の必要性を感じた。個人情報の管理に対する取り組みはPマークの取得運用の過程で理解していたが、その他の情報についても情報セキュリティの向上の必要性を感じた。
- データセンターの価値向上（イメージアップ）を目指した。基本的には業務に ISMS を取り込む事を想定して、認証取得を目指した。

⑤ ISMS導入の効果

- 事務局（自分達）の情報セキュリティへの理解が深くなった。
- まだ完全ではないが、取得後は社員の情報セキュリティへの理解が深まり、全社員へ浸透してきた。
- リスクアセスメントについて、問題点が明確になり、トップダウンで行えるため、ISMS

導入以前より、やりやすくなった。

- ベースラインアプローチによって、問題点が明確化されることもあり、業務改善のきっかけを作ることができるようになった。
- 情報セキュリティ予算の獲得しやすくなった。また経営層の理解も得られ易くなった（質問 13 の 9 & 11）。
- 従来は、事故・事件の原因究明は責任追及を行うことになると考えがあり、行えなかったが、ISMS 導入後は原因究明が行いやすくなった。

⑥ ISMS導入の課題

- ISMS 認証の範囲外の部門とのコミュニケーションにおいて、セキュリティ要求依頼の理解を得ること。
- 導入後、1 年程度しか経過していないため、規程類の作成に時間を取られている。ただ、これも時間が解決してくれると考えている。
- 今年度は運用に重きを置き、運営を事務局中心から現場に広げることとした。事務局は監査や有効性の評価手法などの見直しに注力する必要性を感じている。
- 業務上発生した制約としては、個人情報保護の観点による障害時ログ解析への制約が大きい。また、ログ解析には復旧と原因解析とのジレンマがある。
- 複数の役員が同一場所にいないことが多いため、ISMS 書類等の更新を行う時に承認の押捺が非常に面倒になっている。電子承認システムの導入の必要性を感じているが、予算等の関係からできていない。
- 質問 17「運用上の負担」については、「1.セキュリティ委員会の開催」が一番大きな負担になっている。それ以外では、「3.資産台帳の見直し」、「4.リスクアセスメント」、「7.マネジメントレビュー」、「8.業務とマニュアルの乖離」（変更管理が十分にできていない）、「10.ログのレビュー」等が負担になっている。またログレビューに関しては、非常に時間を取られている。

⑦ その他

- 教育は、P マークと ISMS の両方で行っている。P マークで年2回、ISMS で年 1 回の合計3回行っているため比較的浸透していると思われる。
- 会社全体の取り組みとして、職務上のポジションと連係したセキュリティ教育の体系化の整備を始めている。

以上

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
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」

ＵＲＬ：www.nmda.or.jp