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

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

～　目次　～

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、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、とい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] 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　アンケート調査の内容

認証取得組織向けのアンケートについては、先に述べた本調査の目的に沿って質問項目を設定した。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、最後に組織の中でどのように 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、前回の調査に加え、コンサルタントや ISMS 審査員に関する質問を追加し、第三者認証制度の問題点の洗い出しに努めるとともに、運用面から情報資産の持ち出しについても、新たに質問を加えた。

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いるが、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。

以上の考え方から、調査については、前回の調査との比較を重視する質問はそのまま残し、新たな問題として調査が必要であると考えられる質問を追加し、合計61 項目についてアンケートを行った。また、アンケート回答のみでは得られない、認証取得組織の現状を把握するため、本調査後にいくつかの事業所に対してインタビューを行った。

質問は 7 つのグループからなっている。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、本調査を回答いただく担当者の部門、役職などの属性情報等の質問を 7 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11 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等の質問を 9 問実施した。

(4)　コンサルタントに関する情報

コンサルタント利用の有無、コンサルタントの理解度、費用の妥当性、選定方法等の質問を 12 問実施した。

(5)　ISMS 審査員に関する情報

審査員の ISMS の理解度、審査員の業務の理解度、コミュニケーション、実効性のある指摘を行ったか等の質問を 5 問実施した。

（6）　ISMS 認証の運用に関連する情報

内部監査の実施頻度、内部監査の体制、マネジメントレビューの実施頻度などに関する質問を 6 問実施した。

（7）　ISMS に関連した教育・ルール

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、社外持出ルール等の質問を 10 問実施した。

今回はさらに、日本に所在する全認証機関（計 24 団体）に対するアンケートを実施した。質問として当該認証機関の 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について、合計 33 項目についてアンケート調査を行った。

また、いくつかの認証機関に対して、アンケートと並行してインタビュー調査を行った。質問は、主に以下の 7 つのグループに分けられる。

(1) 審査機関の基礎情報

ISMS が占める割合、審査を行う上での得意領域、認証組織を理解するための方法などについて質問した。

(2) 審査員

審査員としての資質、審査員教育の方法、力量を測定するための方法などについて質問した。

(3) 審査時の対応

クレームの有無、コンサルティングを求められたときの対応について質問した。

(4) 受審側の対応

受審側に望む姿勢や有効性の評価などについて質問した。

(5) 審査における付加価値

受審側に興味深いと思われる付加価値について質問した。

(6) ISMS 認証取得の動向

不況の影響や今後の動向などについて質問した。

(5) その他

認証取得の適正規模やプライバシーマークとの関連などについて、自由な意見を伺った。

３　アンケート調査について

(1) 認証取得組織向けアンケート調査の概要

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）までに返送いただいた回答を集計した。

② 調査対象

アンケート発送数　　2,096 件

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 2,092 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。

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 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あった場合は、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。さらに、それらの回答とは別に、アンケート回答用紙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。

⑥ アンケートの特徴

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

前回調査では、回答率は、18.6％という回答率であったが、今回は若干低い

16.8%という回答率となった。

しかし、過去に本学などで行っているセキュリティ関係のアンケート調査の回答率が 10%程度だったのに比べると、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、回答した企業の約 4 割が意見もしくは連絡先を記入する結果となり、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。

  意見の中には、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。

(2) 認証機関向けアンケート調査の概要

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)までに返送いただいた回答を集計した。

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 回答形式

認証機関による傾向の違いを把握するため、回答は記名方式とした。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。

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、アンケート回答用紙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。

⑥ アンケートの特徴

アンケート全体の特徴としては、回答率が 3 割と高かったことや、自由記述欄への回答が多かったことから、認証機関としても ISMS 認証に対する関心が高いことが伺える。

また、アンケートの設問や実施方法へのリクエストも目立っており、次回実施の際には検討する必要がある。

(3) 認証取得組織に対するインタビュー調査概要

① インタビュー実施日

2009 年 2 月 18 日(水)
2009 年 2 月 26 日(木)

② 調査対象

認証取得組織　2 社

③ 回答形式

予め定めた分野別の設問につき、インタビュアーが順次質問を行い、回答いただいた。

④ 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。

⑤ インタビューの特徴

認証取得組織の現状について、インタビュー調査を行った。実際の現場での担当者の意見や、認証機関、コンサルタントに対する要望など、アンケート調査では得られない、貴重な意見が得られた。

(4) 認証機関に対するインタビュー調査概要

① インタビュー実施日

2009 年 3 月 5 日(木)、2009 年 3 月 6 日(金)
2009 年 3 月 13 日(金)

② 調査対象

ISMS 認証機関　3 団体

③ 回答形式

予め定めた分野別の設問につき、インタビュアーが順次質問を行い、回答いただいた。

④ 結果の取り扱い

集計結果については、個別機関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。

⑤ インタビューの特徴

各審査機関からは、審査員・営業・広報担当の方々に、受審側とは異なる ISMS の考え方について 1 時間～1 時間 45 分にわたってインタビューを行った。

4 総合的な考察（認証取得組織）

(1) 組織の基本情報

▪ ISMS 認証取得組織の規模

今回の調査では、資本金が 1,000 万円未満の組織の割合は前回調査の半数となった。昨今の経済状況を反映して、資金力のない企業では、セキュリティへの投資を回避する傾向が出ていると考えられる。「1,000 万円以上 5 億円未満」の企業が前回同様、全体の 7 割を占めている。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。また資本金「5 億円以上」の組織は前回同様 2 割前後であり、大規模な組織が積極的に ISMS 認証を取得している傾向も、変わっていない。

続いて組織の従業員数についてであるが、今回の調査で前回調査よりも増加したのは、従業員数が「100 人未満」の組織と「50,000 人以上」の組織である。中でも「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ことが考えられる。

▪ 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。また、「情報通信業」は前回より割合が微増している。

次に多いのは「製造業」である。前回の調査の 3 番目から 2 番目に順位を上げた。これは、製造業での機密情報保護への関心の高まりが背景にあると考えられる。3 番目は前回の 2 番目から順位を落とした「複合サービス業」である。その他の業種では前回同様の結果となった。

▪ アンケート回答者の所属部門と役職

前回調査と同様に、一番多かったのは 3 割を占める「情報セキュリティ担当部門」である。ただし、前回調査より微減している。逆に、今回最も増加したのは「総務部門」である。前回調査の約 1 割から今回調査では約 2 割と増加した。これは、セキュリティについて、これまでは情報セキュリティ担当部門だけの対応であったものが、全社的な対応へ変化してきたと考えられる。また、前回調査と同様、「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 2 割を占めている。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。

アンケート回答者の役職で最も多かったのは、前回同様、部長、課長クラスの中間管理職で、合計で 5 割を占めている。また係長・主任を加えると 6 割を占め、組

織を動かす実務者が担当していることがわかる。この傾向は、前回調査と変わっていない。また、会長・社長・役員や執行役員を合わせると 1 割を超えており、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組織が多いことも、前回同様である。アンケート回答者の役職に関しては、全体的に前回同様の結果となった。

さらに今回調査の新規調査項目である、記入者の ISMS 運用における役割では、ISMS 事務局（責任者及び担当者）が 6 割を超えており、実務に携わっている人が多く、情報セキュリティ責任者などマネジメント層が回答するケースは少ないことが伺える。

今回のアンケート記入者の経験年数については、調査の結果、「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とが考えられる。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。

(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(ISO27001)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 が浸透してき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が増えていない。

また、他のマネジメントシステムの取得については QMS だけでなく、EMS も前回より増加している。これは近年の環境経営への注目度の高さを示しているものと思われ、これら 3 つのマネジメントシステムは、CSR 活動の基本柱となっている企業も多い。一方、2 年前より本格的に運用を開始した ITSMS は微増となっている。

・ 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いという結果になった。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。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。

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。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。

また、認証取得後の認証範囲の変更などの今後の展望については「変更予定なし」が最も多く、まずは運用定着化を図っている企業が多いことがわかる。一方、規模拡大を検討している企業も多くなっており、他組織への拡大を検討するケースが増加していると思われる。

(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、多い順に「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」となっており、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きている。これは、自由記述の意見にもあったように、認証取得時に、ある程度の影響を想定することができるようになってきているのが要因と思われる。一方、想定外の回答の中では、やはり業務量の増加や制約等、直接影響が出るものが多い傾向となっている。

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」が前回同様多く、PDCA サイクルを回すための作業への理解が、未だに浸透していないことがわかる。

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、前回同様、「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。また、「内部監査担当のスキル強化」が前回よりも増加している。ここから、認証取得組織が、取得後の内部監査対応時に苦労していることが伺える。

- 実業務と ISMS の乖離

実業務と ISMS の乖離（ダブルスタンダードの発生）についての質問であったが、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。これは、ISMS 認証の想定外の影響でも述べた、「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」に負荷を取られてしまい本来のセキュリティ対策活動に影響する事を実業務と ISMS の乖離と捉えているケースが多くあることが想定される。

- 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。やはり認証取得

組織にとって、ISMS 維持コストは負担となっていると考えられる。

(4) ISMS 認証に関連する体制

▪ 経営陣の関わり方

前回同様、引き続き経営陣が ISMS 認証に積極的に関わっていることが伺える。しかし、回答は、若干減少傾向にあり、ここ 1、2 年に取得した事業者において経営陣が関わらないケースもあった。

▪ ISMS 事務局について

人数構成については、引き続き少人数で運営されている実態が明らかとなった。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できているのではないかと推測される。初回認証取得メンバーが残っているかという問いについては、「一人もいない」が増加した。これは、認証取得から時間が経過しており、メンバー交代が増えていることを示している。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している傾向があり、スキルが内部に蓄積されつつあると考えられるのであればいいのだが、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ないのではないかと思われる。

(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、前回調査の項目である「コンサルタントの利用」以外の質問について、新規に質問を追加した。回答は、10 段階評価を中心とした。

▪ 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。

▪ ISMS 認証の要求事項・セキュリティに関する技術に対する理解度について

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」として比較したところ、理解されていない割合が比較的高いものとして「大学以外の教育・学習支援業」「金

融･保険業」「医療・福祉」、理解されている割合が比較的高いものとして「製造業」「卸売･小売業」が見られた。このように、コンサルタントの理解度は業種による差がみられた。

- 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」「確立したコンサルティング手法」「一貫性を持ったコンサルティング」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と見ることもできる。業務に対する理解度を高めることで、より有効なコンサルティングが行えると考えられ、業務の理解度を高めることが、今後の課題ではないかと思われる。

- 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のではないかと考えられる。

- 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と考えられる。また「技術・コンペ」「実績」など業務能力、「費用」が同等の割合で見られるが、いずれも認証取得組織側に、コンサルタントの能力や費用対効果の評価が求められるものである。コンサルタントを継続利用する組織は、評価する能力も向上していくと思われるが、前述のように認証取得前にのみコンサルタントを利用し、認証取得後には利用しない組織の割合が高い。今後も認証取得前にのみコンサルタントを利用する傾向が続くのであれば、評価能力が求められる項目の割合が大きく変化することはないのではないかと思われる。

導入・選定の最終判断については、社長・会長、その他の取締役、執行役員等の経営陣、トップが行っている割合が高いといえる。選定理由に続き、関係の重視と、費用面での判断の双方からトップ層の意向大きく関わっていると思われる。

(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 認証システム自体の質に関わる重要な事項であるとの認識から、今回、新たに質問を追加した。回

答は、10 段階評価とした。

- 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（平均 9.3）やセキュリティ技術（平均 8.8）に関する理解度については、それぞれ高い値を示していた。今回のアンケート回答者の所属の約半数が情報システム、情報セキュリティ以外の部門である事を考慮すると、技術的な知識量には違いがあることから、当然の結果であるともいえる。

- 業務に対する理解度について

審査員が組織の業務を理解しているかとの質問については、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感じている回答も少なくなかった。そこで、比較的理解されていないと感じている回答者の業種割合を見たところ、上位から 4 番目に「医療・福祉」があった。しかし、アンケート全体の業種割合では 9 番目であることを考慮すると、医療・福祉は業務理解が難しい分野があることが伺える。

- 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については、平均 8.3 であった。また、「実効性のある指摘」「組織に対する効果や課題の確認」の平均がそれぞれ、8.1、8.4 であった。結果としては、比較的高い値であるといえる。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、審査員が本質的な指摘や組織が抱える課題への気づきを事業者に与えていくためには、審査員自身が業務に対する理解を深めていくことが肝要ではないかと考えられる。

(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、「常設の社内チーム」の割合が増加しており、「非常設の社内チーム」は減少している。このことから、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認証取得組織は皆無であったが、約 1 割弱の認証取得組織は、改善は「一部のみ行われている」と回答している。その理由として、「現場に改善作業を行う余力が無い」を選択した認証取得組織が多かった。

しかし、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、今回は 3 分の 1 程度に減少しており、事務局には改善作業に従事するための余裕が出てきたことも伺える。

- 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。

また、実施形態についての傾向も前回調査とは変わらず、「会議での実施」が 9 割以上を占める結果となった。

(8) 教育

- 教育実施形態

選択肢は、「集合研修」「E-ラーニング」等の集中して行う教育と、「冊子配布」「OJT」等の継続して行う教育に分類される。まず、これらをどのように教育を行っているかについて、職位別に質問を行った。なお、本設問は複数選択を可としている。

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、集中して行う教育と継続して行う教育を併用して実施していると考えられる。また、個人で受講できる「メール」や「E-ラーニング」などにもついても積極的に行われているようである。

ただし、年間 1～2 度のペースで行う「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どう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。

なお、選択肢で、「集合研修」として、「ビデオ」を見る場合、回答者の選択が一意でなかった可能性がある。次回調査では、質問内容を明確にしたい。

- 職位との目立った関連性

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ている。最も特徴的であったのは「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とである。一般的に情報セキュリティはトップダウンで行う方が有効であるといわれているが、経営陣に対する教育機会が少なくなっているとすれば、今や経営スキームの一角である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

に見られた。
また、情報セキュリティ管理者・推進者には「OJT」「自己啓発」が 2 番目、3 番目に多かった。さらに、「その他」で外部研修と回答したケースが三階層とも最も多かったことから、情報セキュリティ管理者・推進者には業務や様々な機会を通し、自発的に学ぶことを期待する経営陣の意思が見て取れる。

・ 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。また、「社内その他」が全体の 2 割を占めているが、今回のアンケートでは記載できるスペースを準備しなかったために詳細は把握できていない。準備した選択肢の他にどのような部門が教育を行ったかを調査することで、興味深い結果が得られるかもしれない。
それぞれのレベルについては、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」は高レベルであることがわかる。しかし、少数ではあるが 1～3 点といった否定的とも取れる判断を下したケースも見られた。この場合、教育を行うこと自体の意味合いが薄れるとも考えられ、改善する必要性が高いともいえる。

・ 啓発活動

今回のアンケートでは、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」を追加したところ、大きな反応が見られた。カリキュラムを組む集合研修とは別に、日常的に行う会議での発言や、誰もが参照できる web での表現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。

(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、「外部媒体の接続制限」は約半数の認証取得組織が実施しているが、「外部媒体のデータ移動時強制暗号」は約 16%にとどまっている。このことから、外部媒体のリスクは認識しているものの、コストが必要となる対策はあまり進んでいないことがわかる。
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」を導入している認証取得組織は 1 割にも満たないという結果であった。

▪ 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かった。傾向としては、PC の場合は約 88%、媒体の場合は約 79%の認証取得組織が「ルールあり（持出許可必要)」と回答している。また、社外持出を全面禁止している認証取得組織は、PC の場合は約 7%、媒体の場合は約 9%であった。

ただし、「特になし」と回答した認証取得組織は、PC については無かったが、外部媒体については少ないが存在した。

- 社内持込もしくは利用を制限したもの

ノート PC、外部記録媒体については、約 8 割が社内持込もしくは利用を制限していた。また、携帯電話を制限していると答えた認証取得組織は約 16%にとどまり、少数派であるように見受けられる。

(10)自由回答欄

- 自由回答欄について

自由記述欄の記載について、一番多かったのは ISMS 制度に対する意見であったが、その次には ISMS への感想が多かった。また、PDCA サイクルが回ってきているとの手ごたえを感じているとの意見がある一方で、負担増となっている、認証取得が目的化しており、本来の目的が形骸化しているなど、うまく機能していないとの意見も多く、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。

- 意見の区分について

自由意見欄をその性質により、組織・予算・監査・教育・対策・事故・対応・その他に区分すると、多い順に、情報セキュリティに対する対策、監査、教育の順番となった。ISMS 関係者の関心の順番とイコールであると考えられる。特徴的な意見としては、順位の 2 番目の監査について、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が多く見られた。また、審査員の評価制度の必要性も指摘されている。

- 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。次点では QMS の関連が多かった。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。複数社から各認証との統合の必要性は指摘されており、今後の課題であると考えられる。

なお、QMS、EMS、ISMS、ITSMS 等については、統合審査が可能であるが、一部の

審査機関では、統合審査に積極的でない所もあるとの話もある。

- 自由回答欄の内容について

自由意見欄の内容から、意識・プロセス・コスト・有効性・監査・コンサル・審査員・リスクアセスメント・J-SOX・PDCA・ポリシーに分類すると、プロセス、有効性、意識が上位を占める。この結果から、ISMS 活動を通して自組織のセキュリティ、業務プロセスを改善していく上でのコメントが多数寄せられていることがわかる。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、業務改善に向けた取り組みへの努力を図っている認証取得組織が多く見られた。また、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。認証取得組織によっては、コンサルタントに ISMS 取得を依存しているところもあり、その選択の良し悪しが ISMS の構築後の品質に直結する可能性がある。

(11)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。

このようなケースは、経営者層が誤った認識を持っている場合、間違った方向に進む可能性があるため、経営者への啓発活動に重点を置くべきである。

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。これは、本来の ISMS 制度の理解が正しくできていないため、導入の効果が現れていないためと考えられる。

本来の ISMS 取得の目的を誤って理解している認証取得組織は、再度、自組織にとっての必要性を考え直す必要がある。

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。

ISMS 導入作業時のコンサルタントの不適切な指導や、審査に通ることを優先した認証取得組織の対応の結果とも考えられる。ISMS 担当者はその組織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。

特に業種によって理解度にばらつきが見られる。ISMS 知識を深めることは当然のことながら、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。認証取得組織の状況に応じた臨機応変な支援ができず、型通りの指摘しかできないコンサルタントの存在は、ISMS 認証制度の発展の阻害要因とも成りうることから、コンサルタントの登録制の導入なども今後の課題としてあげられる。

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。

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組織へのヒアリング、コンサルタントとの面接などを実施し、費用対効果も勘案した上で、信頼できるコンサルタント選びを行うべきである。

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。

コンサルタントと同じように、業種にもよるが、認証取得組織は、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、慎重に認証機関を決定する必要がある。また、取得後も認証機関を変更したり、苦情を訴えることもできる制度が確立されていることから、これらの利用も考慮していくべきである。

(12) インタビューからの分析

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いうことができる。

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。

５　総合的な考察（認証機関）

(1) アンケート全体からの分析

・　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。後日行ったインタビューによると、情報セキュリティのライフサイクルに沿って廃棄物業界でも ISMS 認証を取得するケースが見られ、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があった。審査領域にも不得手とされる領域があり、事前に理解するために注力しているものと思われる。

・　審査活動向上の取り組みについて

審査員教育やその力量の指標について確認した。今回は 10 段階の指標を用いたが、認証機関によっては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。また、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。

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。

・　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。

また、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。後日行ったインタビューでは、内部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す旨、コメントがあったが、ISMS 等のように第三者認証制度の最終段階でベテランとはいえ、社員だけの判定委員会で良いかの疑問は残る。

判定委員会での差し戻しもあるとのこと、ひとつの審査に対し、多くのチェックがなされていることがわかる。

なお、現時点では、認証取得組織に対して、認証保留、認証停止等があっても、公開されることがないため、認証の継続を諦めたのか、何らかの問題があったため、認証保留、認証停止等があったかは、第三者からはわからない。　業界として、統一的な仕組みの構築が必要ではないだろうか。

・ 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。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、「格付け」に対する抵抗も一部見られた。

(2) インタビューからの分析

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。

6 ISMS 認証制度の実効性を向上させる施策案について

4 章、5 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) ISMS 制度の再認識

本来の ISMS 制度の取得について、取得することが目的となってしまい、何故、何のために導入するのか、その組織として何が目的なのか、が見えなくなってしまう傾向がある。

認証取得組織は、まず、社内の体制を確立するべきである。経営層が過度に現場に介入したり、また、経営層に ISMS への知識が足りなかった場合、内部の運用がうまく回らない。本来は、事業推進のための一つの策としての ISMS が、それ自体の取得が目的となってしまい、本来業務に影響を及ぼすというような、矛盾が生じる可能性がある。したがって、認証取得組織は、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

ISMS の認証について、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。導入後にこの比率は低くなるが、更新時には、再度、コンサルタントを利用する認証取得組織も多い。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、コンサルタントは、ISMS に関する知識の取得をさらに行うことで、コンサルタント自身のレベルが上がるはずである。

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と考えられる。

(3) 認証機関のレベルアップ

認証機関については、アンケートの中からも様々な意見があがっている。おおむね、適切であるとの回答を得ているが、認証機関に対して大いに不満を述べている認証取得組織も多かった。

これについては、一概に認証機関だけの問題であるとも言えない。相互に認識が違っている場合や、認証取得組織側が、ISMS 制度を誤解している場合もあるからである。また、認証機関によって、それぞれに得意な分野や経験豊富な

ケース等がある。

しかし、「審査員によって指摘の内容や表現が違う」、といった意見も多く、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。

したがって、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と考えられる。

(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。しかし、認証取得組織内の全構成員に周知を図ることは難しいものである。そこで、いくつかの課題を述べる。

①上層部に適切な教育を実施する。

前回調査でも指摘されていたが、上位層、役員層ほど、教育自体の機会が少なくなる傾向がある。

確かに、役員層は多忙ではあるが、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。なぜなら、ISMS は企業活動の一側面であり、結果的に、業務をうまく展開させるための一つの策に過ぎないからである。また、ISMS の実現によって内部統制を確立していくには、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が重要である。往々にして、経営者層がルールを守らないことは多く、そのために制度が成り立たなくなるケースが多い。

②集合研修について工夫をこらす。

今回調査によると、集合研修は多く行われていた。しかし、工夫を行っていると回答した認証取得組織はほとんどなかった。

集合研修は、人数が多い分、一人ひとりの自覚が足りなくなる可能性もある。また回数だけを開催すればよいというものではない。多くの人に周知・理解させ、実際の行動に結び付けてもらえなければ、研修を行う意味がない。

このため、研修実施後にテストを実施し理解度を図るなどの工夫が必要である。

③継続的な教育・啓発活動

ISMS においては、継続的に PDCA サイクルを回していくことが重要である。教育・啓発に関しても、繰り返し、継続していくことが重要である。教育の機会が多ければ多いほど、それに触れる構成員も増える。繰り返し行うことにより、大きな効果も得られると考えられる。

7 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。

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質問の６グループの概要は以下のとおりである。

１．事業者（企業、公共団体等）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	７問
質問項目	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

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に関する情報を得る
質問数	１１問
質問項目	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

３．ISMS 認証の運用に関連する課題

目的	事業者が実際にISMS認証を取得した際に生じた課題および生じている課題に関する情報を得る
質問数	９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

４．コンサルタントに関する情報

目的	事業者がISMS認証取得にあたって利用しているコンサルタントに関する情報を得る
質問数	１２問
質問項目	コンサルタント利用の有無、コンサルタントの理解度、費用の妥当性、選定方法

５．ISMS 審査員に関する情報

目的	事業者がISMS認証取得にあたって利用しているコンサルタントに関する情報を得る
質問数	５問
質問項目	審査員の ISMS の理解度、審査員の業務の理解度、コミュニケーション、実効性のある指摘を行ったか

６．ISMS 認証の運用に関連する情報

目的	ISMS 認証に基づいた内部監査、マネジメントレビューに関する情報を得る
質問数	６問
質問項目	内部監査の実施頻度、内部監査の体制、マネジメントレビューの実施頻度

７．ISMS に関連した教育・ルール

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	１０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、社外持出ルール

付録　B．アンケートの配布資料

今回のアンケートで使用した質問および回答などの資料は、以下のとおりである。

（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）アンケート回答用紙　　（3ページ）

（4）審査機関向けアンケート表紙　（1ページ）

（5）審査機関向け回答用紙　　（3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 20 年 11 月現在、約 2,900 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ってきてい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。

質問は別紙となっております。**回答用紙（本紙）にご回答頂き、回答用紙のみ、同封の封筒にてご返送ください。**

また、回答は、電子メールでお送りいただくことも可能です。以下のページにアクセスしていただき、回答用エクセルシートを回答先までお送りください。

［ＵＲＬ］ http://lab.iisec.ac.jp/~uchida_lab/enq/isms/2008/index.html

［回答先］ uchida@iisec.ac.jp

なお、回答は平成 20 年 12 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。

なお、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 21 年 1 月 31 日(土)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。

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

質 問 票　回答用紙にご記入ください（本質問票のご返却は不要です）

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

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（択一）

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（択一）

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（択一）

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. 総務部門(人事・経理含む)	2. 社長室	3. 企画部門	4. 情報システム管理部門
5. 情報システム開発部門	6. 情報セキュリティ担当部門	7. 事業部門	8. 事業推進部門
9. コンプライアンス担当部門	10. リスク管理担当部門	11. 監査部門	12. 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	2. その他の取締役	3. 執行役員	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 運用における役割

1. 情報セキュリティ責任者	2. ISMS 事務局責任者	3. ISMS事務局員(担当)	4. その他

7. 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

貴組織の ISMS 認証取得についてお聞きします

8. ISMS 認証を取得した年月をお答えください（ISMS 認証を取得した年月を西暦、月でご記入ください）。

9. 認証組織の従業員数をお答えください。（択一）

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	

10. 他の認証の取得状況と取得後年数をお答えください。（複数選択可）

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（　　）	

11. 認証取得の主な目的をお答えください。（複数選択可）

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ため	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ため	
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のため	7. その他

12. 認証取得の発案者をお答えください。（択一）

1. 会長・社長	2. その他の取締役	3. 執行役員	4. 管理職	5. その他

※問12・13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。

13. 認証の運用責任者をお答えください。（択一）

1. 会長・社長	2. その他の取締役	3. 執行役員	4. 管理職	5. その他

14. 認証取得後の認証範囲の変更と検討状況についてお答えください。（択一）

1. 縮小または縮小検討中	2. 拡大または拡大検討中	3. 他範囲との統合または統合検討中	4. 変更予定なし

質 問 票　回答用紙にご記入ください（本質問票のご返却は不要です）

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

15. 得られた効果をお答えください。（複数選択可）

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. 経営陣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

16. 想定外の影響をお答えください。（複数選択可）

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. ISMS を担当する組織・人が必要になった	5. 業務上の制約の増加	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（記入欄あり）	

17. 問16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。具体的にはどのようなものでしょうか（複数選択可）

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	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（記入欄あり）	

18. 問16で「5. 業務上の制約が増加」を回答された方に質問します。現場における業務上の制約をお答えください。（複数選択可）

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. 社外での作業の制限
7. 他部門とのコミュニケーションの悪化	8. その他（記入欄あり）	

19. ISMS 認証取得後の運用で負担になっている作業をお答えください。（複数選択可）

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. 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
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. 情報資産台帳の見直し作業	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. 特になし	12. その他（記入欄あり）

20. 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、あるいは取り組む予定のあるものをお答えください。（複数選択可 ・ ※はツールの導入なども含みます）

1. 経営陣の認識・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（記入欄あり）

21. 実業務と ISMS の乖離（ダブルスタンダードの発生）はありませんか？（択一）

1. 乖離している	2. 乖離していない	3. どちらとも言えない

22. ISMS を維持するためのコストは妥当と感じますか？（択一）

1. 高い	2. 妥当	3. 安い

23. ISO27002（情報セキュリティマネジメントの実践のための規範）はどこまで取り入れましたか？（択一）

1. 十分に取り入れた	2. 参考程度とした	3. 取り入れていない

24. 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ますか？（択一）

1. 関わっている	2. 関わっていない	3. 不明

25. ISMS 事務局のメンバーは何人ですか？

1. 専任（　　人）	2. 兼務（　　人）	3. その他（　　人）

26. 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ますか？（択一）

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

27. 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いましたか？（複数選択可）

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. 特になし	6. その他（記入欄あり）

質 問 票　回答用紙にご記入ください（本質問票のご返却は不要です）

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

認証取得時・運用時のコンサルタントについてお聞きします

28. コンサルタントを利用しましたか？（択一）

認証取得まで	1. 利用した	2. 一部利用した	3. 利用していない
認証取得後	4. 利用している	5. 一部利用している	6. 利用していない

問28で3･6の両方を選択された方は、問39にお進みください。

29. コンサルタントは、ISMSを理解していましたか？（択一）

理解していない ←	1	2	3	4	5	6	7	8	9	10	→ 理解していた

30. セキュリティに関する技術について理解していましたか？（択一）

※ 問28の回答選択肢からお選びください。

31. あなたの組織の業務について理解していましたか？（択一）

※ 問28の回答選択肢からお選びください。

32. コミュニケーションをうまく取ることができましたか？（択一）

できなかった ←	1	2	3	4	5	6	7	8	9	10	→ できた

33. 実効性のある提案を行っていましたか？（択一）

行っていない ←	1	2	3	4	5	6	7	8	9	10	→ 行っていた

34. 確立したコンサルティング手法を持っていましたか？（択一）

持っていない ←	1	2	3	4	5	6	7	8	9	10	→ 持っていた

35. 一貫性を持ったコンサルティングを行っていましたか？（択一）

行っていない ←	1	2	3	4	5	6	7	8	9	10	→ 行っていた

36. ISMS認証を取得する上で役に立ちましたか？（択一）

役に立たなかった ←	1	2	3	4	5	6	7	8	9	10	→ 役に立った

37. 費用は妥当でしたか？（択一）

1. 高い	2. 妥当	3. 安い

38. どのような手段でコンサルタントを選定したか、ご自由にお書き下さい。

39. コンサルタント導入の最終判断はどなたでしたか？（択一）

1. 会長･社長	2. その他の取締役	3. 執行役員	4. 管理職	5. その他

ISMS審査員についてお聞きします

40. ISMS審査員は、ISMSを理解していましたか？（択一）

理解していない ←	1	2	3	4	5	6	7	8	9	10	→ 理解していた

41. セキュリティに関する技術について理解していましたか？（択一）

※ 問40の回答選択肢からお選びください。

42. あなたの組織の業務について理解していましたか？（択一）

※ 問40の回答選択肢からお選びください。

43. コミュニケーションをうまく取ることができましたか？（択一）

できなかった ←	1	2	3	4	5	6	7	8	9	10	→ できた

44. 実効性のある指摘を行っていましたか？（択一）

行っていない ←	1	2	3	4	5	6	7	8	9	10	→ 行っていた

45. 効果や課題を確認する能力を持っていましたか？（択一）

持っていない ←	1	2	3	4	5	6	7	8	9	10	→ 持っていた

内部監査についてお聞きします

46. 実施頻度をお答えください。ただし、自己点検は除きます。（択一）

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

47. 体制をお答えください。（複数選択可）

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. 外部機関と社内チームの共同体制	5. その他（記入欄あり）	

48. 指摘事項に対する改善は行われていますか？（択一）

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

49. 問48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。その理由をお答えください。（複数選択可）

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（記入欄あり）

マネジメントレビューについてお聞きします

50. 実施頻度をお答えください。（択一）

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（記入欄あり）

51. 実施形態をお答えください。（複数選択可）

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（記入欄あり）

教育・社内ルールについてお聞きします

52. ISMS の維持に必要と思われる社員教育の手段をお答えください。（複数選択可）

1. 集合研修	2. 冊子の配布	3. OJT	4. E-ラーニング	5. メール
6. ビデオ	7. 自己啓発	8. 特に行っていない	9. その他（記入欄あり）	

53. 同じく、情報セキュリティ管理者・推進者教育の手段をお答えください。（複数選択可）

※ 問52の回答選択肢からお選びください。

54. 同じく、経営陣教育の手段をお答えください。（複数選択可）

※ 問52の回答選択肢からお選びください。

55. ISMS に関する教育の年間の頻度をお答えください。（択一）

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. なし	8. その他（記入欄あり）

56. ISMS に関する教育の担当部門をお答えください。（複数選択可）

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

57. 問56の教育担当者の情報セキュリティに関するレベルを、問56で選択した部門それぞれについてお答えください。

レベル低 ←	1	2	3	4	5	6	7	8	9	10	→ レベル高

58. 教育以外の啓発活動がある場合はお答えください。（複数選択可）

1. キャンペーン週間などの設定	2. web コンテンツの掲載	3. ポスターの掲示	
4. ニュースレター・メルマガの発行	5. 会議での通知	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（記入欄あり）

59. 業務用 PC からの情報漏洩対策として実施している対策をお答えください。（複数選択可）

1. 保存ファイルの暗号化	2. ログインパスワード認証	3. ログインパスワードの定期的変更
4. シンクライアント	5. メールの送信先制限	6. メールの添付ファイル送信制限
7. URL フィルタリング	8. 透かし印刷	9. BIOS パスワードの設定
10. ハードディスク暗号化	11. EFS 暗号化(Windows)	12. 外部媒体のデータ移動時強制暗号
13. 外部媒体の接続制限	14. 特になし	15. その他（記入欄あり）

60. 以下の情報資産を社外持出する際のルールをお答えください。（択一）

【業務用ノート PC】・【業務用外部記録媒体】

1. 持出全面禁止	2. ルールあり（持出許可必要）	3. ルールあり（持出許可不要）
4. 特になし	5. その他（記入欄あり）	

61. 社内持込もしくは利用を制限したものをお答えください。（複数選択可）

1. ノート PC	2. 外部記録媒体	3. 携帯電話	4. その他（記入欄あり）

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。

貴組織・ご記入者について

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　【　　】(1～12)
5. ご記入者の役職　【　　】(1～9)
6. ご記入者の ISMS 運用における役割【　　】(1～4)
7. ご記入者の経験年数【　　】(1～5)

ISMS 認証取得について

8. ISMS 認証を取得した年月　【西暦 ……年……月 】
9. 認証組織の従業員数【　　】(1～8)
10. 他の認証の取得状況と取得後年数【 1.(　　年) 2.(　　年) 3.(　　年) 4.(　　年) 5.(　　年) 】
11. ISMS 認証を取得する主な目的は？【 1.　2.　3.　4.　5.　6.　7. 】
12. ISMS 認証取得の発案者は？【　　】(1～5)
13. ISMS 認証の運用責任者は誰ですか？【　　】(1～5)
14. 認証取得後の認証範囲の変更と検討状況は？【　　】(1～4)
15. 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.　】
16. 想定外の影響は？【 1. 2. 3. 4. 5. 6. 7. 8.(……)】
17. 問16の回答「2.」「3.」のみ　【 1. 2. 3. 4. 5. 6. 7. 8.(……)】
18. 問16の回答「5.」のみ　【 1. 2. 3. 4. 5. 6. 7. 8.(……)】
19. 負担になっている作業は？
【 1.　2.　3.　4.　5.　6.　7.　8.　9.　10.　11.　12.(……)】
20. 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.(……)】
21. 実業務と ISMS の乖離はありますか？【　　】(1～3)
22. ISMS 維持のコストは妥当ですか？【　　】(1～3)
23. ISO27002 はどこまでとりいれましたか？【　　】(1～3)
24. 経営陣はマネジメントレビュー以外に関わっていますか？【　　】(1～3)
25. 事務局のメンバーは？【 1. 専任(……人) 2. 兼務(……人) 3. その他(……人)】
26. 最初のメンバーの割合は？【　　】(1～5)
27. 新しいメンバーへの教育は？【 1. 2. 3. 4. 5. 6.(……)】

コンサルタントについて

28. コンサルタントを利用しましたか？　認証取得まで【　　】(1～3)　認証取得後【　　】(1～3)
29. コンサルタントは ISMS を理解していましたか？【　　】(1～10)
30. コンサルタントはセキュリティ技術について理解していましたか？【　　】(1～10)
31. コンサルタントは貴社の業務について理解していましたか？【　　】(1～10)
32. コンサルタントはコミュニケーションをうまく取ることができましたか？【　　】(1～10)
33. コンサルタントは実効性のある提案を行っていましたか？【　　】(1～10)
34. コンサルタントは確立したコンサルティング手法を持っていましたか？【　　】(1～10)
35. コンサルタントは一貫性を持ったコンサルティングを行っていましたか？【　　】(1～10)
36. コンサルタントは ISMS 取得上、役に立ちましたか？【　　】(1～10)
37. コンサルタントの費用は妥当でしたか？【　　】(1～3)
38. コンサルタント選定手段を教えてください。(……)
39. コンサルタント導入の最終判断はどなたでしたか？【　　】(1～5)

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。

ISMS 審査員について

40. ISMS 審査員は ISMS を理解していましたか？【　　】(1～10)
41. ISMS 審査員はセキュリティ技術について理解していましたか？【　　】(1～10)
42. ISMS 審査員は貴社の業務について理解していましたか？【　　】(1～10)
43. ISMS 審査員コミュニケーションをうまく取ることができましたか？【　　】(1～10)
44. ISMS 審査員は実効性のある指摘を行っていましたか？【　　】(1～10)
45. ISMS 審査員は、効果や課題を確認する能力を持っていましたか？【　　】(1～10)

内部監査について

46. 内部監査の実施頻度は？【　　】(1～4)
47. 内部監査の体制は？【 1. 2. 3. 4. 5. (　　)】
48. 内部監査指摘事項の改善は？【　　】(1～3)
49. 問48で「2. 」「3. 」を回答した方のみ【 1. 2. 3. 4. 5. 6. (　　)

マネジメントレビューについて

50. マネジメント・レビューの頻度は？【 1. 2. 3. 4. 5. (　　)】
51. マネジメント・レビューの実施形態は？【 1. 2. 3. 4. (　　)】

教育・社内ルールについて

52. 社員教育の手段は？【 1. 2. 3. 4. 5. 6. 7. 8. 9. (　　)】
53. 管理者、推進者教育の手段は？ 【 1. 2. 3. 4. 5. 6. 7. 8. 9. (　　)】
54. 経営陣教育の手段は？【 1. 2. 3. 4. 5. 6. 7. 8. 9. (　　)】
55. ISMS 教育の頻度は？【 1. 2. 3. 4. 5. 6. 7. 8. (　　)】
56. ISMS の教育担当部門は？ 【 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 】
57. 教育担当者のレベルは？【 1. (　) 2. (　) 3. (　) 4. (　) 5. (　) 6. (　) 7. (　)
8. (　) 9. (　) 10. (　) 11. (　) 12. (　) 13. (　) 】(1－10)
58. 教育以外の啓発活動は？ 【 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. (　　)】
59. 業務用PCの情報漏洩対策は？【 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14.
15. (　　) 】
60. 社外持出のルールは？ 業務用ノートPC【 1. 2. 3. 4. 5. (　　)】
業務用外部記録媒体【 1. 2. 3. 4. 5. (　　)】
61. 社内持ち込み、利用制限したものは？【 1. 2. 3. 4. (　　)】

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

平成 21 年 2 月 3 日

情報セキュリティ大学院大学

内田研究室　内田勝也

ISMS 認証取得及びその継続の課題を探るためのアンケートご協力のお願い

拝啓

貴社ますますご清栄のこととお慶び申し上げます。

平成 20 年 12 月現在，約 2,900 の事業所・部門が ISMS の第三者認証（ISO/IEC27000 シリーズによる認証）の取得がなされております。

これは，企業の事業活動，社会全般の必要不可欠な取組みとして情報セキュリティの重要性への理解が進み，各組織が情報セキュリティに取り組むにあたって，ISMS という考え方を導入し，管理するという考え方が一般的になってきたことの現われであるとも考えられます。

しかしながら，一方ではセキュリティ対策，認証取得に対する負荷の増加に対する効果の実感などについて課題を感じるという声を耳にします。

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の研究を行なっております。ISMS 認証取得及びその後の運用で発生する課題を抽出することを目的として，平成 19 年 1 月に認証取得組織を対象としたアンケート調査を実施いたしました。その結果，取得組織の運用実態とともに審査機関や審査員に対する意見が多く寄せられました。そこで，ISMS 認証取得審査の実態の把握と整理を行なうためアンケート調査を実施いたします。

つきましては，皆様におかれましても，本調査の趣旨を御了察の上，本件アンケート調査にご協力くださいますよう，何卒よろしくお願いします。

ご多忙のところ誠に恐縮ですが，別紙のアンケート調査表を，**平成 21 年 2 月 20 日（金）**迄に，同封の封筒にてご投函くださいますようお願いいたします。ご回答いただいた内容については，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は，本研究に関連することのみに利用し，それ以外の用途で利用することはありません。

調査票を Excel 形式のファイルで入手し，電子的に記入していただくことができます。その場合は，以下の URL から Excel 形式のファイルをダウンロードしてご利用ください。ただし，データ保護のために，回答のご提出は紙ベースでお願いいたします。

http://lab.iisec.ac.jp/~uchida_lab/enq/isms/2008/index.html

期限までにご回答くださいますよう，重ねてご協力をお願いいたします。

敬具

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　℡ 045－410－0238

電子メール uchida@iisec.ac.jp　携帯電話 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，ご連絡の際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。

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

ISMS認証取得及びその継続の課題を探るためのアンケート

2009/ 2/ XX

情報セキュリティ大学院大学
内田研究室　内田　勝也

本調査について

ISMS認証取得及びその継続の課題を探るための審査機関対象調査にご協力をいただきありがとうございます。

本調査は、ISMS審査機関を対象として、審査員教育や認証登録に関する設問を中心に構成されております。

本調査票が、本件対象データの所管部署以外に送達された場合は、恐れ入りますがご担当部署にご回送くださいますようお願いします。

回答期限

平成21年2月XX日(X)までに、返信用封筒にてご投函ください。

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 tel:03-3519-6440
電子メール: uchida@iisec.ac.jp　携帯電話: 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の際は電子メールまたは携帯電話までいただければ幸いです。

貴組織プロフィールについて

1 貴組織、ご回答者についてお尋ねいたします。

(1)企業名				
(2)所在地 [本社]	〒			
(3)回答 ご担当者	**所属部署:**			
	氏名:		**お役職:**	
	ご住所: **(上記と異なる場合)**			
	電話番号:		**メール アドレス:**	

2 貴組織の認証体制についてお尋ねいたします。以下の設問についてご記入ください。

(1)設立年(西暦)　　年

(2)貴社においてISMS認証の開始年(西暦)　　年

(3)ISMS認証に関わる審査員の人数と構成。

専属(社員)	(人)	契約	(人)

記入欄	

(4)貴組織でISMSと統合審査が可能なISO等認証を以下のリストから選択してください。(複数選択可)

1	2	3	4	5	6	7	8
ISO9000	ISO14000	ISO20000	ISO22000	ISO10002	PCI DSS	BCMS	その他(　　)

(5)昨年1年間のISO/IEC27001認証審査件数　※基準年は2008年1月～2008年12月となります

1	新規	⇒	件
2	継続・更新	⇒	件

(6)審査対象組織の業種、分野への専門性について。得意とする業種はありますか。1～4のうち最も当てはまるもの1つに○をつけてください。また、ご意見があれば記入欄にご記入ください。

1	2	3	4
無い	どちらかといえば無い	どちらかといえば有る	有る

記入欄	

審査活動向上の取組みについて

3 所属する審査員に対する教育の状況についてお尋ねいたします。以下の設問についてご記入ください。

(1)審査員に対して教育を提供する組織がありますか。1～4のうち最も当てはまるもの1つに○をつけてください。また、特記事項があれば記入欄にご記入ください。

1	2	3	4
無い	兼任組織がある	専任組織がある	その他(　　)

記入欄	

(2)審査員に対する年間教育目標時間の設定がありますか。 以下のいずれか1つに○をつけてください。また時間数をご記入ください。

1	無い
2	ある

⇒ 時間/年

(3)成果基準(テスト、インタビュー等による評価)を持つ教育は実施されていますか。以下の1～4のうち昨年1年間の実績のある方式に○をつけてください。(複数選択可)

1	2	3	4	5
実施していない	教材資料配布	E-ラーニング	集合研修	その他(　　)

(4)ISMS審査員の力量で重要と考える項目はどれですか。1～6の項目ごとに最も当てはまるもの1つに○をつけてください。

A.ISO27001,要求事項

1	2	3	4	5	6	7	8	9	10
重要度低 ←									→ 重要度高

B.セキュリティ技術

1	2	3	4	5	6	7	8	9	10
重要度低 ←									→ 重要度高

C.監査の原則、監査手法、技法

1	2	3	4	5	6	7	8	9	10
重要度低 ←									→ 重要度高

D.管理(マネジメント)と意思疎通(コミュニケーション)能力

1	2	3	4	5	6	7	8	9	10
重要度低 ←									→ 重要度高

E.関連法令、規則の知識

1	2	3	4	5	6	7	8	9	10
重要度低 ←									→ 重要度高

F.その他(　　)

1	2	3	4	5	6	7	8	9	10
重要度低 ←									→ 重要度高

(5)受審組織からのフィードバック等から、ISMS審査員の力量項目の中で現状として最も当てはまるもの1つに○をつけてください。

A.ISO27001,要求事項

1	2	3	4	5	6	7	8	9	10
満足度低 ←									→ 満足度高

B.セキュリティ技術

1	2	3	4	5	6	7	8	9	10
満足度低 ←									→ 満足度高

C.監査の原則、監査手法、技法

1	2	3	4	5	6	7	8	9	10
満足度低 ←									→ 満足度高

D.管理(マネジメント)と意思疎通(コミュニケーション)能力

1	2	3	4	5	6	7	8	9	10
満足度低 ←									→ 満足度高

E.関連法令、規則の知識

1	2	3	4	5	6	7	8	9	10
満足度低 ←									→ 満足度高

F.その他(　　)

1	2	3	4	5	6	7	8	9	10
満足度低 ←									→ 満足度高

(6)審査員の力量を測定するための独自の指標がありますか。 以下のいずれか1つに○をつけてください。 また測定指標の概要をご記入ください。

1	無い
2	ある

⇒

記入欄	

4 受審組織やコンサルタントなどの外部組織を対象とした教育活動についてお尋ねします。以下の設問についてご記入ください。

(1)取得事業者を対象とした教育活動として主催していることはありますか。1～4のうち最も当てはまるもの1つに○をつけてください。また、特記事項があれば記入欄にご記入ください。

1	2	3	4	5
実施していない	出版刊行物	Webサイト	教育・研修	その他(　　)

記入欄	

(2)コンサルタントを対象とした教育活動として定期的に主催していることはありますか。1～4のうち最も当てはまるもの1つに○をつけてください。また、特記事項があれば記入欄にご記入ください。

1	2	3	4	5
実施していない	出版刊行物	Webサイト	教育・研修	その他(　　)

記入欄	

認証・認定活動実績について

5 ISMSの審査から認定までの指摘事項の状況についてお尋ねします。 以下の設問についてご記入ください。

（1）ISMSの新規取得の前に予備審査は必要だと思いますか。また、理由を記入欄にご記入ください。

1	不要	⇒	記入欄	
2	どちらかといえば不要			
3	どちらかといえば必要	⇒	記入欄	
4	必要			

（2）新規および継続/更新審査において不適合として是正処置条件付合格、または判定保留となる事例はありますか。以下のうちで最もよく当てはまるものに○をつけてください。 調査対象基準年は2008年1月～2008年12月までとします。

1	2	3	4
0件	10%以下	10%以上30%未満	30%以上

6 認証登録判定委員会の活動状況についてお尋ねします。 以下の設問についてご記入ください。

（1）認証登録判定委員会委員の機関内部、外部メンバ構成の状況について、以下のうちで最も当てはまるものに○をつけてください。また、特記事項があれば記入欄にご記入ください。

1	2	3	4
内部メンバのみで構成	過半数を内部メンバで構成	過半数を外部メンバで構成	外部メンバのみで構成

記入欄	

（2）認証登録判定委員会の指摘によるフォローアップ審査の事例はありますか。以下のうちで最も当てはまるものに○をつけてください。調査対象基準年は2008年1月～2008年12月までとします。

1	2	3	4
0件	10%以下	10%以上30%未満	30%以上

（3）継続・更新審査における審査員のアサインの際の考慮について、以下のうちで最もよく当てはまるものに○をつけてください。また、その理由についても記入欄にご記入ください。

1	2	3	4
同じ審査員を優先する	受審組織からの要望による	別の審査員を優先する	その他（　　）

記入欄	

ISMS認証取得動向について

7 最後に、ISMS認証取得の今後の動向について質問をさせていただきます。以下の設問についてご記入ください。

（1）今年（2009年）以降のISMS認証取得の要求度合いは、どのように変化するとお考えでしょうか。以下の1～5のうち最も当てはまるもの1つに○をつけてください。また、特記事項が有る場合には記入欄にご記入ください。

1	2	3	4	5
減少	微減	変化なし	微増	増加

記入欄	

（2）企業の情報セキュリティ対策の促進として、セキュリティ格付けや情報セキュリティ監査制度などの第三者認証が実施、実施を予定されています。これらの動きについて、以下の1～3のうち最も当てはまるもの1つに○をつけてください。また理由を記入欄にご記入ください。

1	2	3	4	5
歓迎できない	どちらかといえば歓迎できない	特になし	どちらかといえば歓迎できる	歓迎できる

記入欄	

（3）今後ISMS認証の更なる普及と充実のために「付加価値のある審査」とは、どのようなものだとお考えでしょうか。ご自由にご意見をご記入ください。

記入欄	

（3）本アンケート全般についてお気づきの点やご感想がございましたら、ご自由にご意見を記入ください。
また、調査集計後（2月末～3月上旬）に追加調査（インタビュー形式を予定）にご協力をいただける場合には、以下にご記入ください。

記入欄	

※ 追加調査にご協力をいただけると回答いただいた場合は、ご連絡に設問1の個人情報を使用させていただきます。

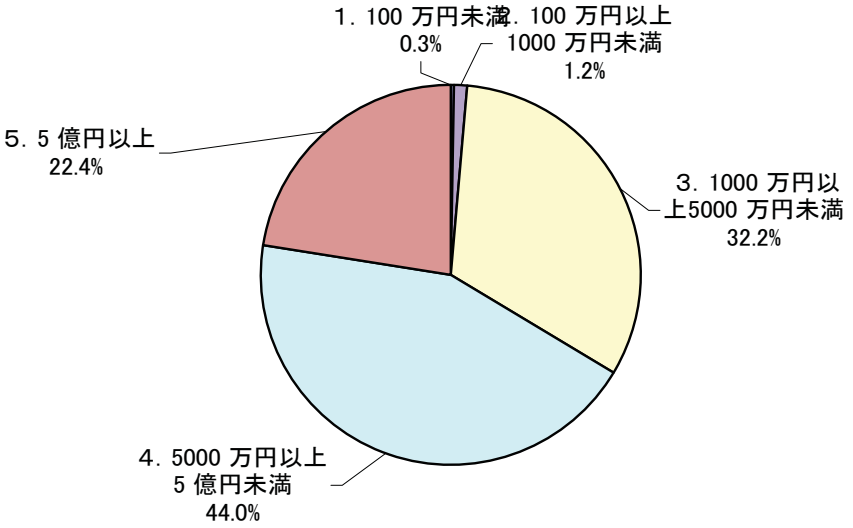
以上でアンケート設問は終了です。　ご協力をいただき、誠にありがとうございました。

本調査票は、同封の返信用封筒をご利用いただき、2月XX日（XX）までに投函をいただきますよう重ねてお願い申し上げます。

組織、記入者について

1．資本金（択一）

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



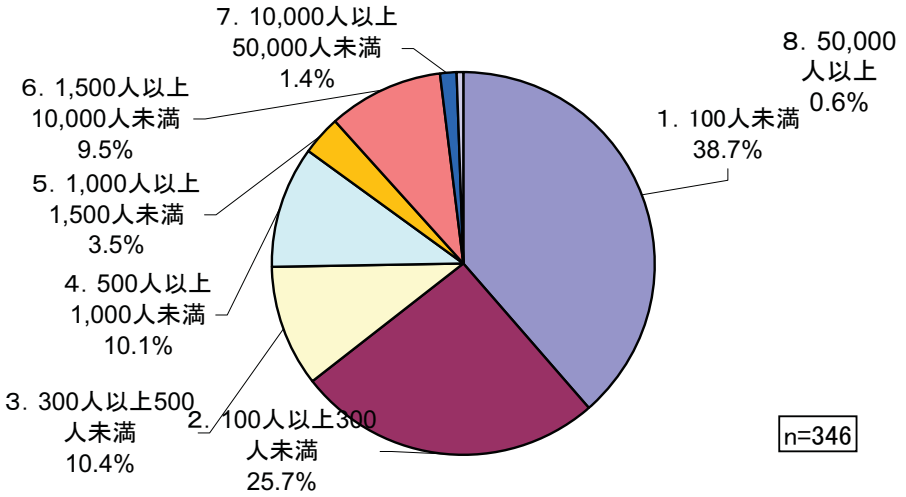
資本金（択一）　（単位：社数・%）

	有効回答数	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
今回	339	1	4	109	149	76
	100%	0.3%	1.2%	32.2%	44.0%	22.4%
前回	258	2	8	75	115	58
	100%	0.8%	3.1%	29.1%	44.6%	22.5%

今回の調査では資本金1000万円以上5億円未満の企業が76.1%で、前回の73.7%を上回った。引き続きこの規模の事業者がISMS認証を取得する中心的な層であることは変わらない。また、5億円以上が22.4%であり、全体として前回調査とほぼ同じ結果を示している。

組織、記入者について

2. 従業員数(択一)
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



(単位:従業員数・%)

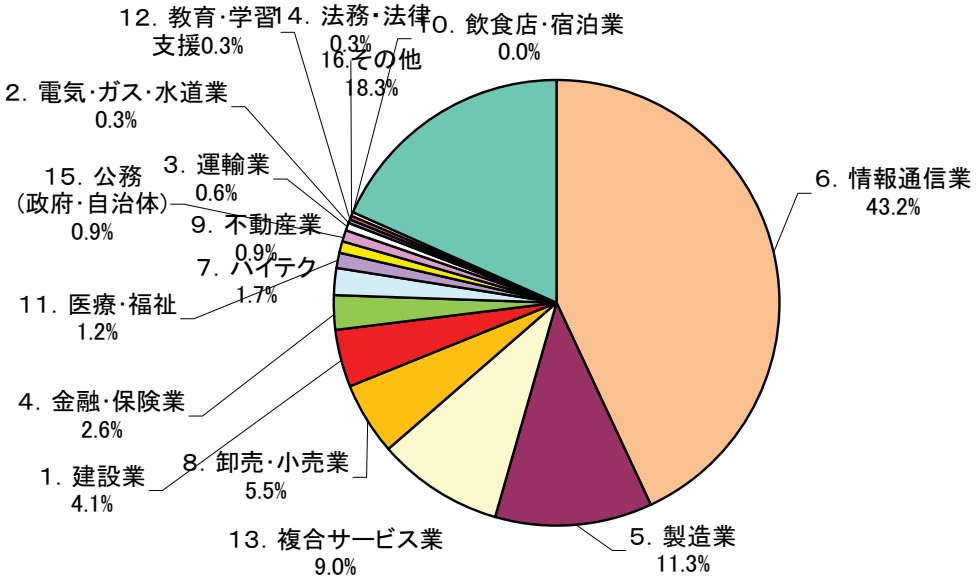
	有効回答数	1. 100人未満	2. 100人以上300人未満	3. 300人以上500人未満	4. 500人以上1,000人未満	5. 1,000人以上1,500人未満	6. 1,500人以上10,000人未満	7. 10,000人以上50,000人未満	8. 50,000人以上
今回	346	134	89	36	35	12	33	5	2
	100%	38.7%	25.7%	10.4%	10.1%	3.5%	9.5%	1.4%	0.6%
前回	263	84	71	28	28	11	32	8	1
	100%	31.9%	27.0%	10.6%	10.6%	4.2%	12.2%	3.0%	0.4%

全体としての傾向は前回同様であるが、100人未満が38.7%であり、前回の31.9%より増加しており、小規模な組織での取得が増えている。なお、本アンケート調査では会社全体の人数で回答している組織とＩＳＭＳを取得している部署ごとの人数で回答している組織があると考えられる。

組織、記入者について

3. 該当する業種(択一)

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



n=345

該当する業種(択一)　　(単位:社数･%)

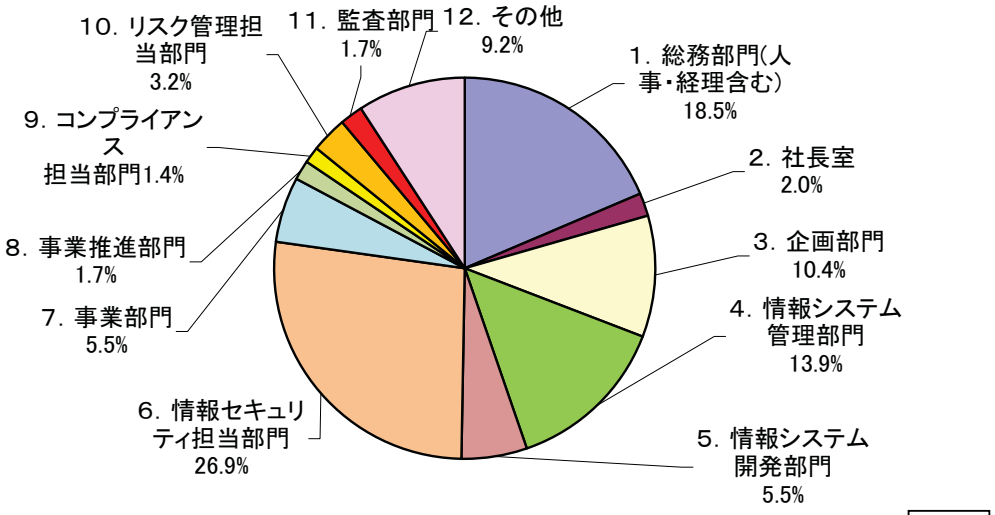
今回	有効回答数	6. 情報通信業	5. 製造業	13. 複合サービス業	8. 卸売･小売業	1. 建設業	4. 金融･保険業	7. ハイテク	11. 医療･福祉
	345	149	39	31	19	14	9	6	4
	100%	43.2%	11.3%	9.0%	5.5%	4.1%	2.6%	1.7%	1.2%
前回	有効回答数	情報通信業	製造業	複合サービス業	卸売･小売業	建設業	金融･保険業	ハイテク	医療･福祉
	345	108	20	39	12	15	4	6	2
	100%	41.1%	7.6%	14.8%	4.6%	5.7%	1.5%	2.3%	0.8%
今回		9. 不動産業	15. 公務(政府･自治	3. 運輸業	2. 電気･ガス･水道業	12. 教育･学習支援	14. 法務･法律	10. 飲食店･宿泊業	16. その他
		3	3	2	1	1	1	0	63
		0.9%	0.9%	0.6%	0.3%	0.3%	0.3%	0.0%	18.3%
前回		不動産業	公務(政府･自治体)	運輸業	電気･ガス･水道業	教育･学習支援	法務･法律	飲食店･宿泊業	その他
		3	3	4	1	1	1	0	44
		1.1%	1.1%	1.5%	0.4%	0.4%	0.4%	0.0%	16.7%

今回の調査で一番減少幅の大きかった業種は複合サービス業で、前回14.8%から9.0%と激減した。業界自体の景気の低迷を反映して、セキュリティ対策へのコストを削減していることが予想できる。逆に、製造業で前回の7.6%から11.3%と増加しており、製造業の機密情報の保護への関心が高まりが背景にあると考えらえる。

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



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）　（単位：社数・%）

今回	有効回答数	1. 総務部門(人事・経理含む)	2. 社長室	3. 企画部門	4. 情報システム管理部門	5. 情報システム開発部門	6. 情報セキュリティ担当部門	7. 事業部門
	346	64	7	36	48	19	93	19
	100%	18.5%	2.0%	10.4%	13.9%	5.5%	26.9%	5.5%
前回	有効回答数	総務	人事	経理	社長室	企画部門	情報システム管理部門	情報システム開発部門
	263	26	1	2	10	26	38	13
	100%	9.9%	0.4%	0.8%	3.8%	9.9%	14.4%	4.9%

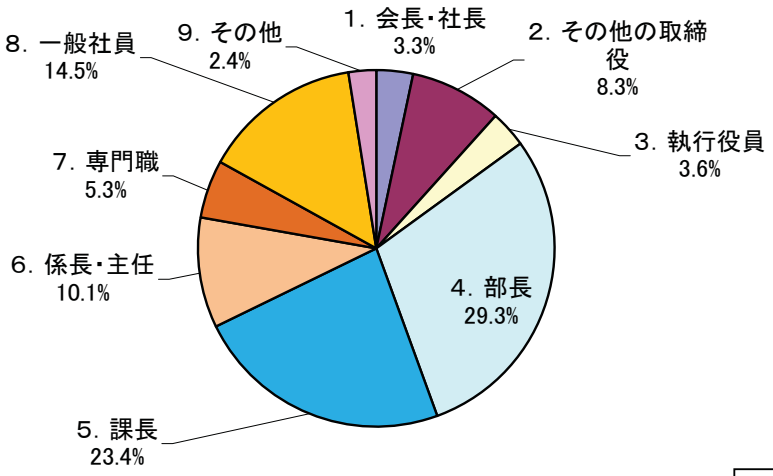
今回	8. 事業推進部門	9. コンプライアンス担当部門	10. リスク管理担当部門	11. 監査部門	12. その他	
	6	5	11	6	32	
	1.7%	1.4%	3.2%	1.7%	9.2%	
前回	情報セキュリティ担当部門	事業部門	コンプライアンス担当部門	リスク管理担当部門	監査部門	その他
	76	22	8	2	6	33
	28.9%	8.4%	3.0%	0.8%	2.3%	12.5%

情報セキュリティ担当部門が前回の28.9%より26.9%と減っており、逆に総務部門が前回（総務及び人事）の10.3%より18.5%と増えている。
これはセキュリティについて、情報セキュリティ担当部門だけの対応であったものが、全社で対応するように変化してきていることが考えられる。

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
2.その他の取締役
3.執行役員
4.部長
5.課長
6.係長・主任
7.専門職
8.一般社員
9.その他



ご記入者の役職(ご自身の役職で最も近い役職を1つ選択してくださし　(単位:社数・%)

	有効回答数	1. 会長・社長	2. その他の取締役	3. 執行役員	4. 部長	5. 課長	6. 係長・主任
今回	338	11	28	12	99	79	34
		3.3%	8.3%	3.6%	29.3%	23.4%	10.1%
		会長・社長・役員	執行役員	事業部長	部長	課長	係長・主任
前回	264	35	8	9	66	69	27
		13.3%	3.0%	3.4%	25.0%	26.1%	10.2%

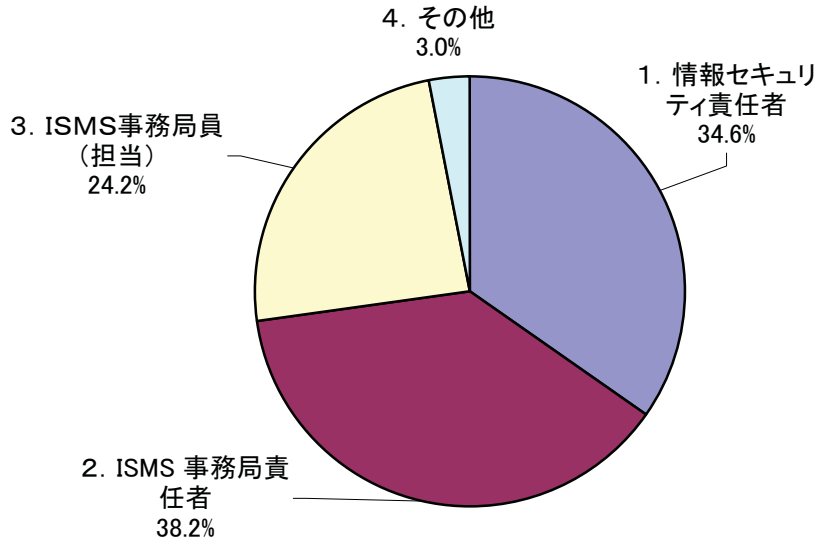
	7. 専門職	8. 一般社員	9. その他
今回	18	49	8
	5.3%	14.5%	2.4%
	専門職	一般社員	その他
前回	12	32	6
	4.5%	12.1%	2.3%

今回の調査では前回の選択肢と変更しているが、傾向としては前回と大きな変化は無かった。部長、課長は前回が51.1%で、今回は52.7%となっており、ほぼ半数を占めている。また、会長社長、取締役、執行役員は15.1%となっており、前回の会長・社長・役員、執行役員の16.3%とほぼ同じ割合である。

組織、記入者について

6. ご記入者のISMS運用における役割

1.情報セキュリティ責任者
2.ISMS事務局責任者
3.ISMS事務局員（担当）
4.その他



n=335

（単位：社数・%）

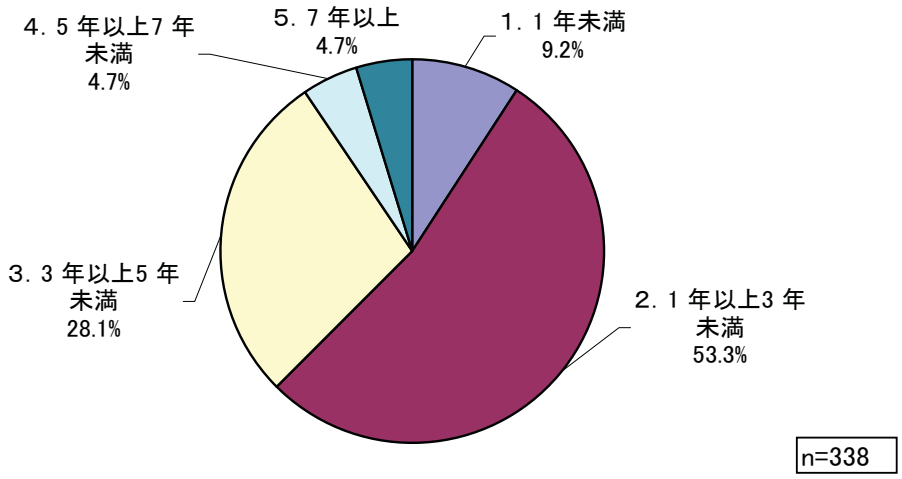
有効回答数	1. 情報セキュリティ責任者	2. ISMS事務局責任者	3. ISMS事務局員（担当）	4. その他
335	68	136	42	97
100%	34.6%	38.2%	24.2%	3.0%

本質問は今回調査で新規項目である。ISMS事務局（責任者+担当者）が62.4%となっており、質問に回答しているのは事務局が中心となっていることが考えられる。

組織、記入者について

7. 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



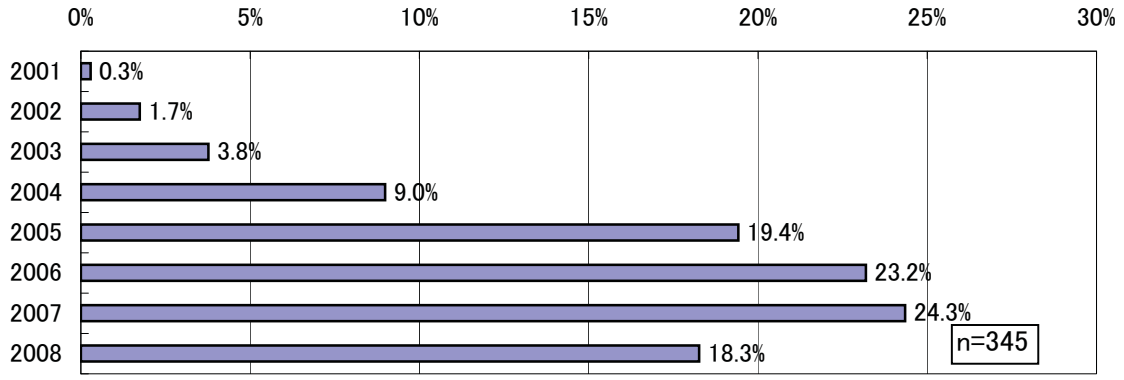
（単位：社数・%）

	有効回答数	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
今回	338	31	180	95	16	16
	100%	9.2%	53.3%	28.1%	4.7%	4.7%
前回	263	38	152	54	11	8
	100%	14.4%	57.8%	20.5%	4.2%	3.0%

1年未満3年未満が最も多く62.4%だが、前回の72.2%より減っている。逆に3年以上5年未満は28.1%、7年以上は4.7%と前回の結果に比べて増えている。
このことから、ISMS担当者は異動のサイクルは比較的長く、少なくとも3年以上の在籍となっている可能性が高い。

ISMS認証に関連する体制

8. ISMS認証を取得した年月をお答えください
（ISMS認証を取得した年月を西暦、月でご記入ください）。



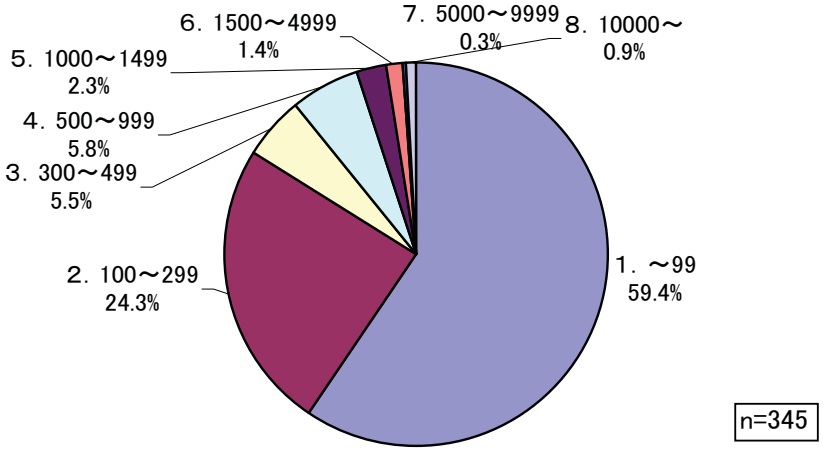
（単位：社数・%）

	有効回答数	2001	2002	2003	2004	2005	2006	2007	2008
今回	345	1	6	13	31	67	80	84	63
	100%	0.3%	1.7%	3.8%	9.0%	19.4%	23.2%	24.3%	18.3%
前回	264	1	11	24	39	79	108	1	
		0.4%	4.2%	9.1%	14.8%	29.9%	40.9%	0.4%	

前回調査と比較して、2007年、2008年も取得会社が増えている。
但し、本調査は2008年度は12月までの調査の為、さらに増加する可能性がある。

ISMS認証に関連する体制

9. 認証組織の従業員数をお答えください。(択一)
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



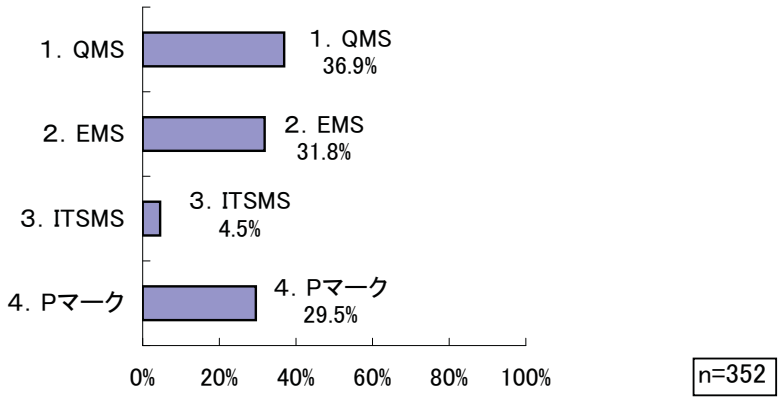
(単位:従業員数・%)

	有効回答数	1. ～99	2. 100～299	3. 300～499	4. 500～999	5. 1000～1499	6. 1500～4999	7. 5000～9999	8. 10000～
今回	345	205	84	19	20	8	5	1	3
		59.4%	24.3%	5.5%	5.8%	2.3%	1.4%	0.3%	0.9%
前回	261	154	71	16	8	2	5	2	3
		59.0%	27.2%	6.1%	3.1%	0.8%	1.9%	0.8%	1.1%

前回とほぼ同様の傾向として、「100人未満」が57%、「100人以上300人未満」が24%で、300人未満の組織での取得が全体の83.8%をしめている。

ISMS認証に関連する体制

10. 他の認証の取得状況と取得後年数をお答えください。(複数選択可)
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(　　)



(単位:社数)

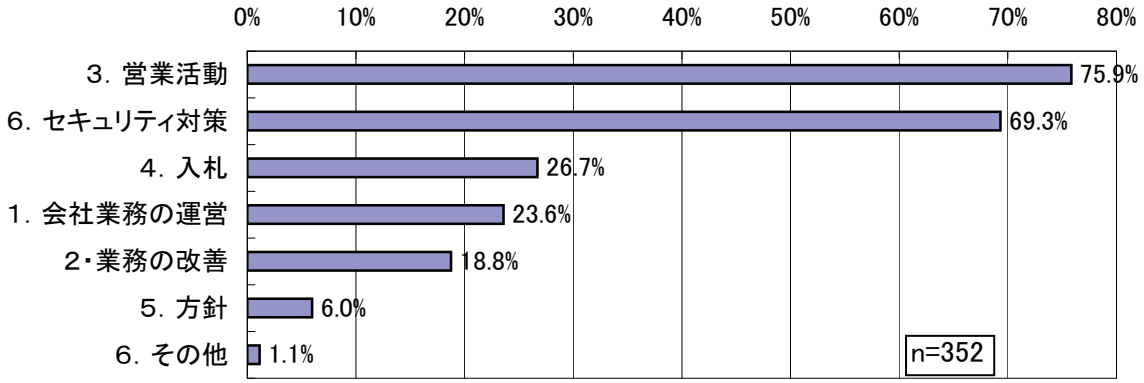
	有効回答数	1. QMS	2. EMS	3. ITSMS	4. Pマーク
今回	352	130	112	16	104
		36.9%	31.8%	4.5%	29.5%
前回	265	110	81	11	68
		41.5%	30.6%	4.2%	25.7%

前回同様、「QMS」取得が36.9%と多いが、「EMS」や「Pマーク」も増加している。
2年前に本格運用した「ITSMS」についても16社が実施している。

ISMS認証取得について

11. 認証取得の主な目的をお答えください。(複数選択可)

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ため
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ため
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のため 7. その他



(単位:社数・%)

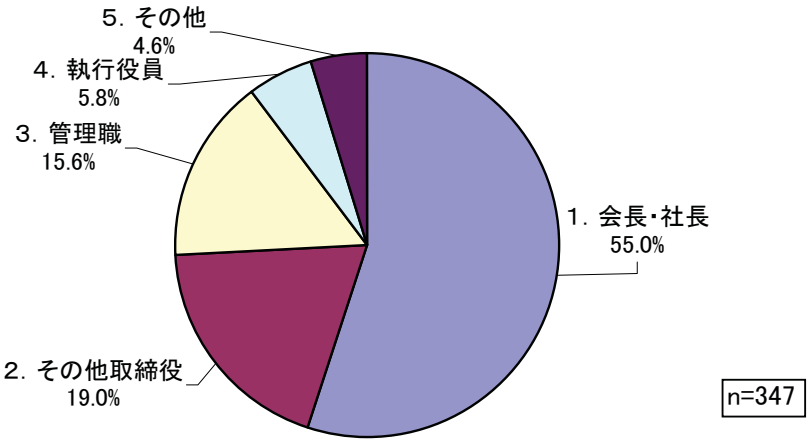
	有効回答数	3. 営業活動	6. セキュリティ対策	4. 入札	1. 会社業務の運営	2・業務の改善	5. 方針	6. その他
今回	352	267	244	94	66	83	21	4
		75.9%	69.3%	26.7%	18.8%	23.6%	6.0%	1.1%
前回	264	199	189	77	65	58	15	10
		75.4%	71.6%	29.2%	24.6%	22.0%	5.7%	3.8%

前回同様、「営業活動に有利」や「情報セキュリティ対策」が多くなっている。
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ためが75.9%、など前回と同じ傾向になっている。
注目すべきことは、「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。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。

組織、記入者について

12. 認証取得の発案者をお答えください。(択一)

1. 会長・社長
2. その他の取締役
3. 執行役員
4. 管理職
5. その他
※問12・13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。



(単位:社数・%)

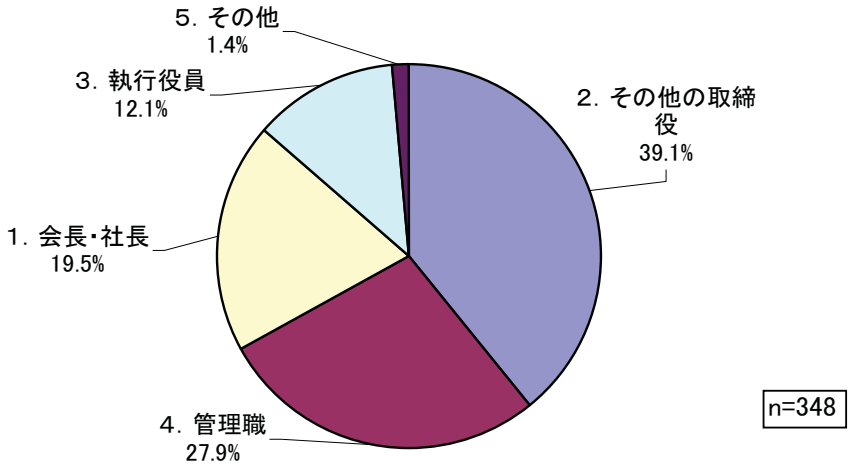
有効回答数	1. 会長・社長	役	3. 管理職	4. 執行役員	5. その他
347	191	66	20	54	16
	55.0%	19.0%	5.8%	15.6%	4.6%

役員以上の割合が79.8%と非常に高く、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。

組織、記入者について

13. 認証の運用責任者をお答えください。(択一)

1. 会長・社長
2. その他の取締役
3. 執行役員
4. 管理職
5. その他



(単位:社数・%)

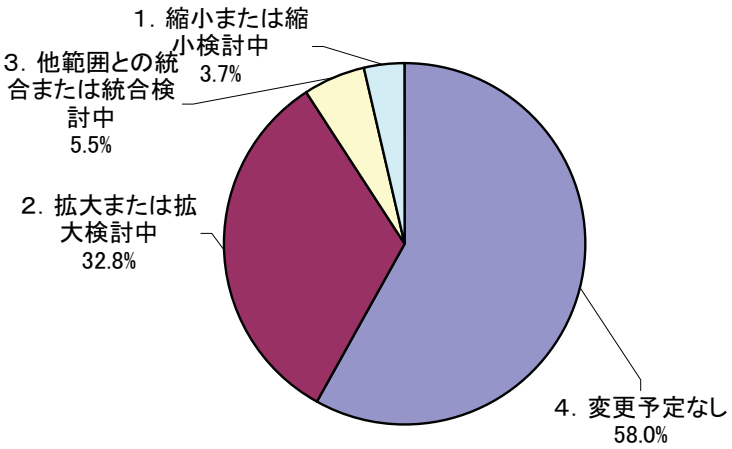
有効回答数	1. 会長・社長	2. その他の取締役	3. 執行役員	4. 管理職	5. その他
348	68	136	42	97	5
	19.5%	39.1%	12.1%	27.9%	1.4%

役員以上の割合が70.7%と非常に高く、認証の責任者もトップダウン体制で運用しているケースが多いことがわかる。

組織、記入者について

14. 認証取得後の認証範囲の変更と検討状況についてお答えください。(択一)

1. 縮小または縮小検討中
2. 拡大または拡大検討中
3. 他範囲との統合または統合検討中
4. 変更予定なし



n=348

(単位:社数・%)

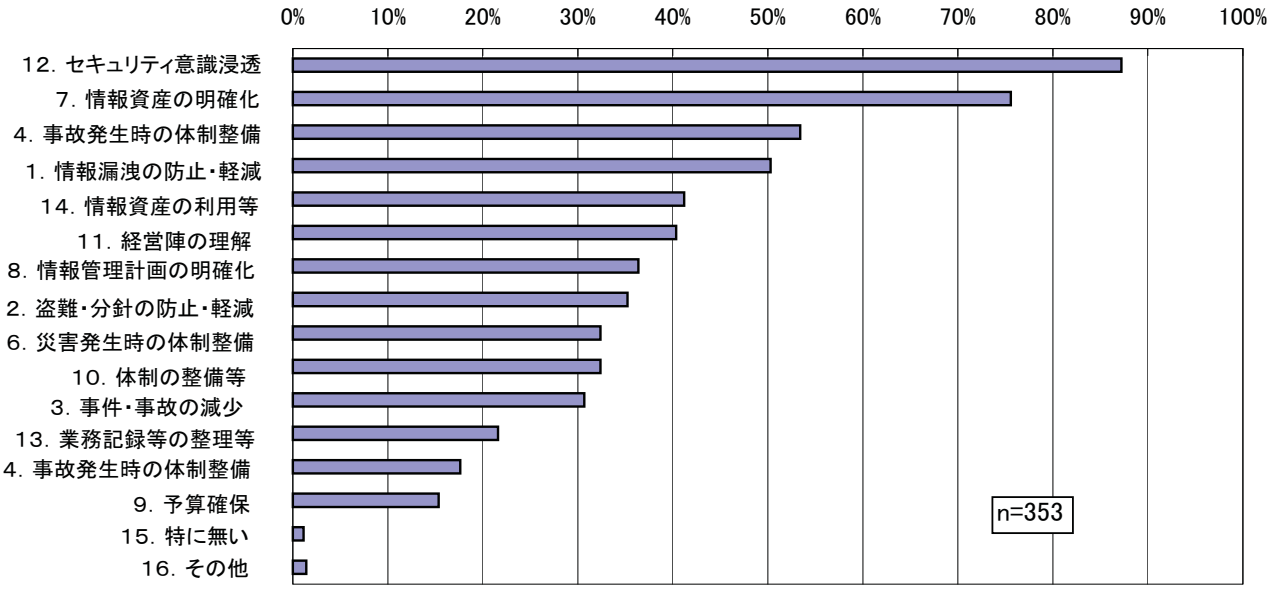
有効回答数	1. 縮小または縮小検討中	2. 拡大または拡大検討中	3. 他範囲との統合または統合検討中	4. 変更予定なし
348	13	114	19	202
	3.7%	32.8%	5.5%	58.0%

認証取得後の範囲の変更は58.0%が「変更予定なし」との回答であった。
しかし、「範囲の拡大および検討中」も32.8%と高い割合を示しており、他組織への拡大を検討するケースが増加していると思われる。また、「他範囲との統合」も少ないながら5.5%となっている。

ISMSの効果

15. 得られた効果をお答えください。(複数選択可)

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. 経営陣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



(単位:社数・%)

	有効回答数	12. セキュリティ意識浸透	7. 情報資産の明確化	4. 事故発生時の体制整備	1. 情報漏洩の防止・軽減	14. 情報資産の利用等	11. 経営陣の理解	8. 情報管理計画の明確化	2. 盗難・分針の防止・軽減
今回	352	307	266	188	177	145	142	128	124
		87.2%	75.6%	53.4%	50.3%	41.2%	40.3%	36.4%	35.2%
前回	264	232	205	149	146	117	114	113	106
		87.9%	77.7%	56.4%	55.3%	44.3%	43.2%	42.8%	40.2%

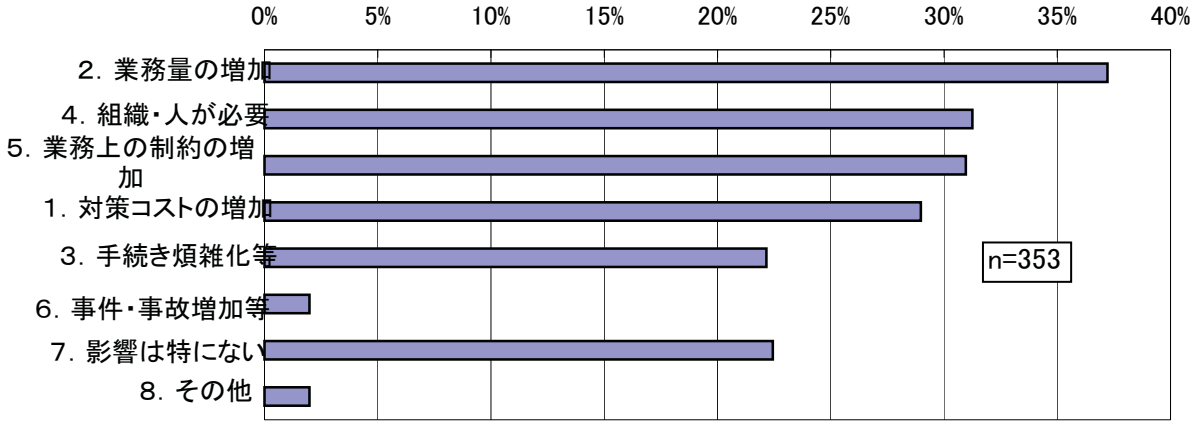
6. 災害発生時の体制整備	10. セキュリティ体制の整備等	3. セキュリティ事件・事故の減少	13. 業務記録等の整理等	4. 事故発生時の体制整備	9. セキュリティ関係予算確保	15. 特に無い	16. その他
114	114	76	108	62	54	4	5
32.4%	32.4%	21.6%	30.7%	17.6%	15.3%	1.1%	1.4%
99	77	54	97	57	49	3	8
37.5%	29.2%	20.5%	36.7%	21.6%	18.6%	1.1%	3.0%

前回調査とほぼ同様の傾向となっている。
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。
1事業者あたり平均5.7個の効果を選択しており、これも前回同様である。

ISMSの効果

16. 想定外の影響をお答えください。(複数選択可)

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. ISMSを担当する組織・人が必要になった
5. 業務上の制約の増加
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(記入欄あり)



(単位:社数・%)

	有効回答数	2. 業務量の増加	4. 組織・人が必要	5. 業務上の制約の増加	1. 対策コストの増加	3. 手続き煩雑化等	6. 事件・事故増加等	7. 影響は特にない	8. その他
今回	352	131	110	109	102	78	7	79	7
		37.2%	31.3%	31.0%	29.0%	22.2%	2.0%	22.4%	2.0%
前回	264	105	97	97	91	61	9	46	6
		39.8%	36.7%	36.7%	34.5%	23.1%	3.4%	17.4%	2.3%

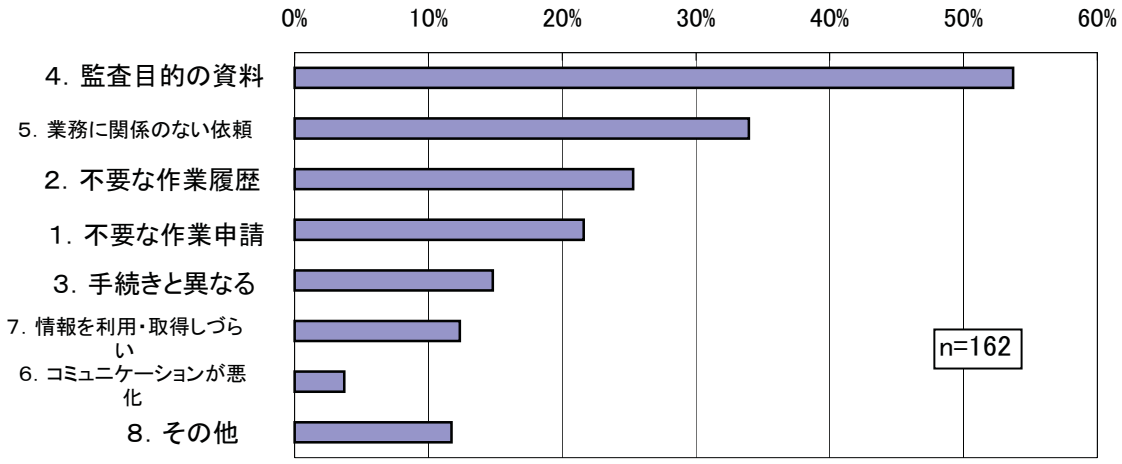
その他詳細
想定内(6件)
会社が理解していない(1件)

「業務への影響はない」が22.4%となっており、影響があるは77.6%に達している。
また影響を受けている項目も平均1.5個選択されている。

ISMSの効果

17. 問16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。具体的にはどのようなものでしょうか（複数選択可）

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
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（記入欄あり）



（単位：社数・%）

	有効回答数	4. 監査目的の資料	5. 業務に関係のない依頼	2. 不要な作業履歴	1. 不要な作業申請	3. 手続きと異なる	7. 情報を利用・取得しづらい	6. コミュニケーションが悪化	8. その他
今回	162	87	55	41	35	24	20	6	19
		53.7%	34.0%	25.3%	21.6%	14.8%	12.3%	3.7%	11.7%
前回	166	64	55	31	30	18	20	12	20
		38.6%	33.1%	18.7%	18.1%	10.8%	12.0%	7.2%	12.0%

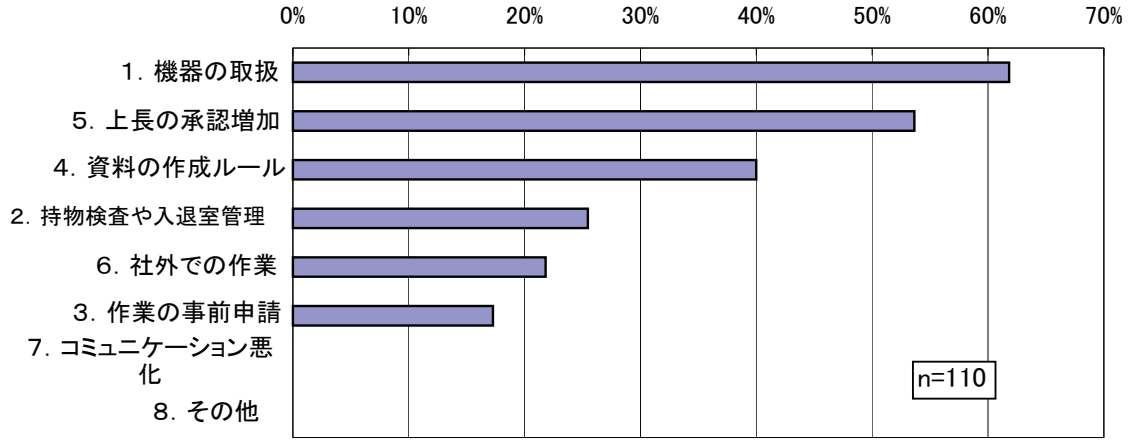
その他詳細
必要な申請・手続きの増加（11件）
記録の増加（5件）
工数の増加（3件）

問16の2、3を選択した162名が回答している。
「監査目的の資料作成」がもっとも多く53.7%をしめている。
「ISMS事務局からの作業依頼」など、間接的な作業が増加していることがわかる。

ISMSの効果

18. 問16で「5. 業務上の制約が増加」を回答された方に質問します。現場における業務上の制約をお答えください。（複数選択可）

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. 社外での作業の制限
7. 他部門とのコミュニケーションの悪化
8. その他（記入欄あり）



（単位：社数・%）

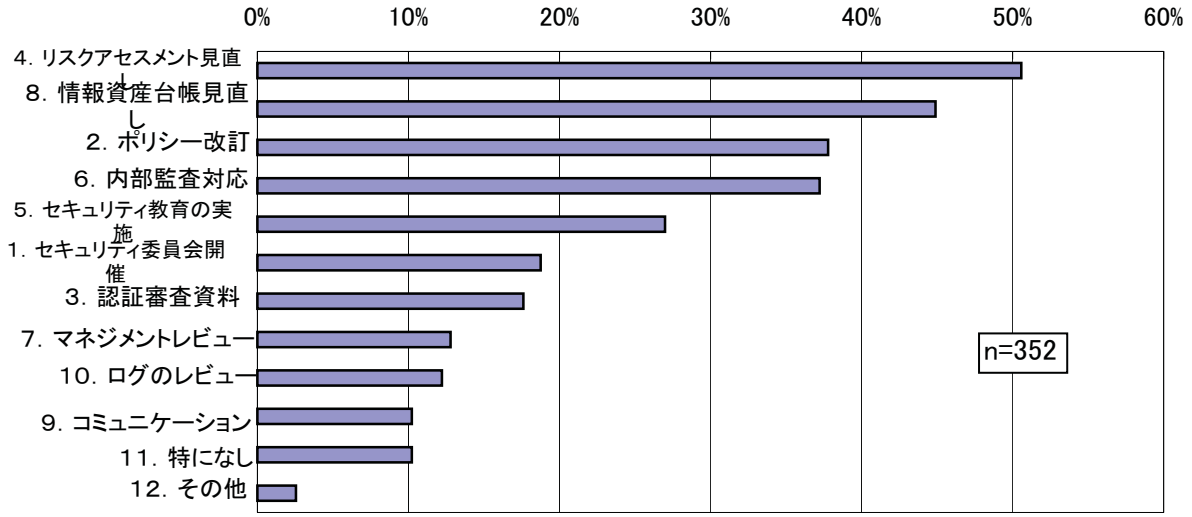
	有効回答数	1. 機器の取扱	5. 上長の承認増加	4. 資料の作成ルールの指定等	2. 持ち物検査や入退室管理	6. 社外での作業	3. 作業の事前申請	7. コミュニケーションの悪化	8. その他
今回	110	68	59	44	28	24	19	0	0
		61.8%	53.6%	40.0%	25.5%	21.8%	17.3%	0.0%	0.0%
前回	97	80	58	50	40	32	23	7	2
		82.5%	59.8%	51.5%	41.2%	33.0%	23.7%	7.2%	2.1%

問16の5を選択した110名が回答している。
「機器の取り扱い」に関する制約が61.8%と最も多い。「上長の承認」の増加や「資料のルール」も多くなっている。
平均2.2個を選択しているが、前回3.0個であったことから、制約があると感じているケースが減少している。これはルールが浸透してきていることを示していると思われる。

ISMSの効果

19. ISMS認証取得後の運用で負担になっている作業をお答えください。(複数選択可)

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. 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
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. 情報資産台帳の見直し作業
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. 特になし
12. その他(記入欄あり)



	有効回答数	4. リスクアセスメント見直し	8. 情報資産台帳見直し	2. ポリシー改訂	6. 内部監査対応	5. セキュリティ教育の実施	1. セキュリティ委員会開催	3. 認証審査資料
今回	352	178	158	133	131	95	66	62
		50.6%	44.9%	37.8%	37.2%	27.0%	18.8%	17.6%
前回	264	142	132	139	109	95	56	36
		53.8%	50.0%	52.7%	41.3%	36.0%	21.2%	13.6%

7. マネジメントレビュー	10. ログのレビュー	9. コミュニケーション	11. 特になし	12. その他
45	43	36	36	9
12.8%	12.2%	10.2%	10.2%	2.6%
45	45	29	17	6
17.0%	17.0%	11.0%	6.4%	2.3%

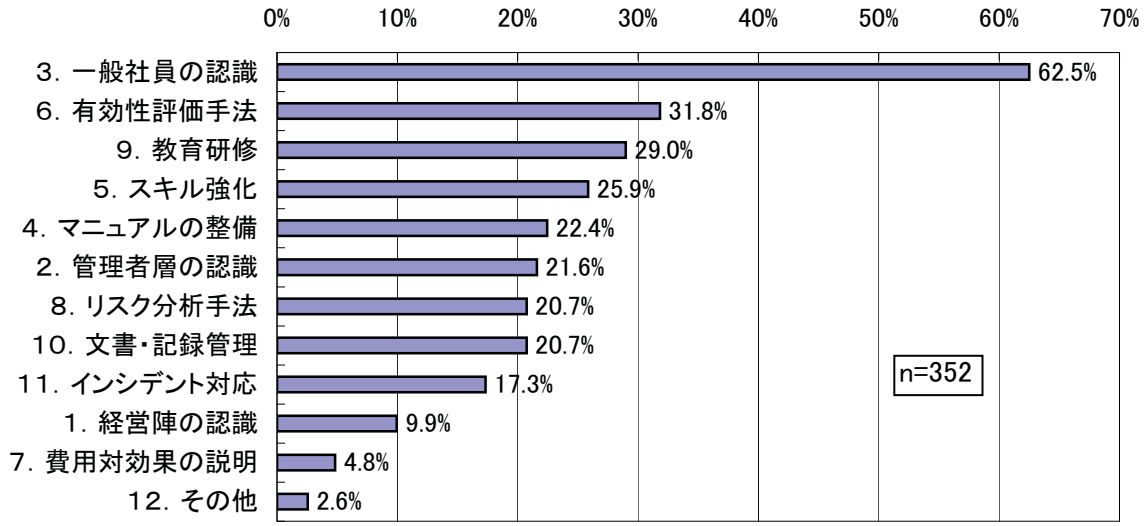
その他詳細
事務局運営(2件)
負担ではない(2件)
有効性評価の検討(2件)
教育・訓練(2件)
立会い(1件)

いずれも高い割合になっているが、注目は「情報資産台帳の見直し作業」である。
重要ではあるが負担になっていることがわかる。

ISMSの効果

20. 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、あるいは取り組む予定のあるものをお答えください。
（複数選択可 ・ ※はツールの導入なども含みます）

1. 経営陣の認識・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（記入欄あり）



（単位：社数・%）

	有効回答数	3. 一般社員の認識	6. 有効性評価手法	9. 教育研修	5. スキル強化	4. マニュアルの整備	2. 管理者層の認識	8. リスク分析手法
今回	352	220	112	102	91	79	76	73
		62.5%	31.8%	29.0%	25.9%	22.4%	21.6%	20.7%
前回	264	183	108	95	61	83	76	62
		69.3%	40.9%	36.0%	23.1%	31.4%	28.8%	23.5%

10. 文書・記録管理	11. インシデント対応	1. 経営陣の認識	7. 費用対効果の説明	12. その他
73	61	35	17	9
20.7%	17.3%	9.9%	4.8%	2.6%
62	54	27	12	4
23.5%	20.5%	10.2%	4.5%	1.5%

その他詳細

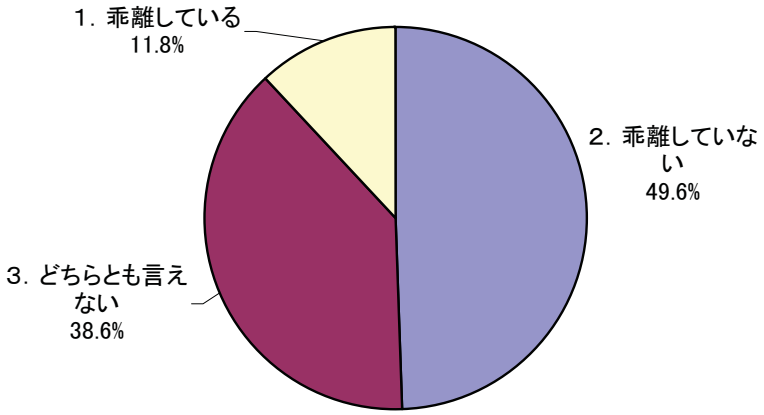
インフラ整備（2件）	ライセンス管理	BCP
業務フロー整備（2件）	他マネジメントシステムとの統合	予定なし

前回同様、「社員の認識・理解の強化」が62.5%と最も高い。
「有効性評価手法の改善」は前回のISO27001移行時と比較すると低下している。
また、「費用対効果の説明手法」については4.8%と前回同様低く、まだ浸透していない。

ISMSの効果

21. 実業務とISMSの乖離(ダブルスタンダードの発生)はありませんか？(択一)

1. 乖離している
2. 乖離していない
3. どちらとも言えない



(単位:社数・%)

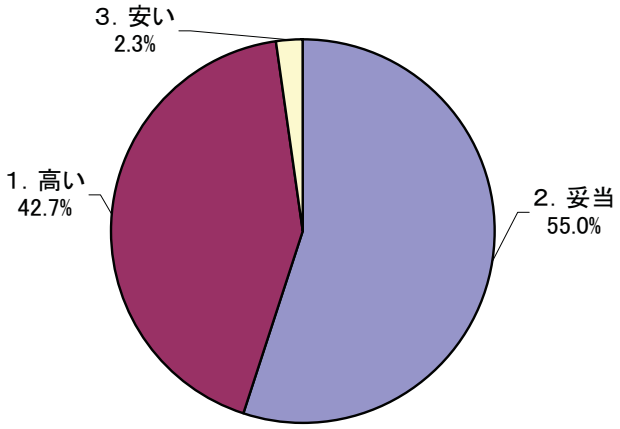
有効回答数	2. 乖離していない	3. どちらとも言えない	1. 乖離している
347	172	134	41
	49.6%	38.6%	11.8%

今回新規追加の設問である。
全体の49.6%が「乖離していない」と回答しているが、「どちらとも言えない」、あるいは「乖離している」も合計50.4%となっている。現場では、乖離してしまう、あるいはわからないようなケースがあることがわかる。

ISMSの効果

22. ISMSを維持するためのコストは妥当と感じますか？（択一）

1. 高い
2. 妥当
3. 安い



n=347

（単位：社数・%）

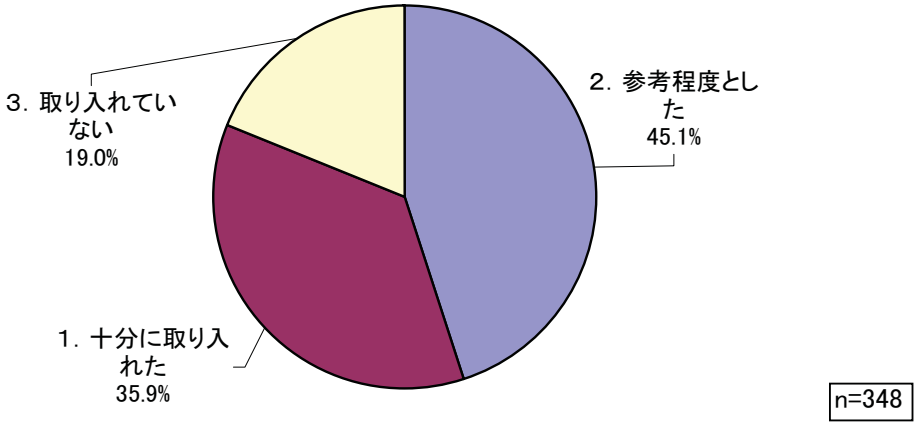
有効回答数	2. 妥当	1. 高い	3. 安い
347	191	148	8
	55.0%	42.7%	2.3%

今回新規追加の設問である。
「妥当」と回答したのが55.0%に対し、「高い」が42.7%と高い割合となっている。
「安い」と回答したのは2.3%に過ぎず、ISMS維持コストは企業にとって負担となっていることがわかる。

ISMSの効果

23. ISO27002(情報セキュリティマネジメントの実践のための規範)はどこまで取り入れましたか？(択一)

1. 十分に取り入れた
2. 参考程度とした
3. 取り入れていない



(単位:社数・%)

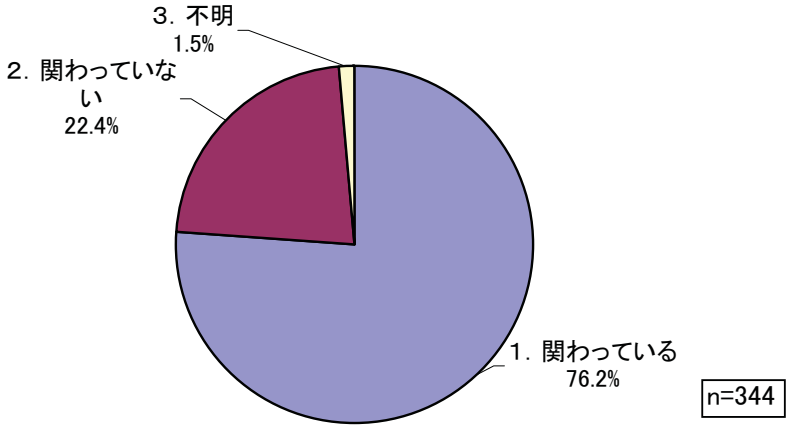
有効回答数	2. 参考程度とした	1. 十分に取り入れた	3. 取り入れていない
348	157	125	66
	45.1%	35.9%	19.0%

今回新規追加の設問である。
「十分に取り入れた」、あるいは「参考にした」は合計で81.0%と高い割合を示しているが、
「取り入れていない」も19.0%となっている。

ISMS認証に関連する体制

24. 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ますか？（択一）

1. 関わっている
2. 関わっていない
3. 不明



（単位：社数・%）

	有効回答数	1. 関わっている	2. 関わっていない	3. 不明
今回	344	262	77	5
		76.2%	22.4%	1.5%
前回	259	213	41	5
		82.2%	15.8%	1.9%

前回と比較して、経営陣の関与が約6%減少している。
取得部門にてマネジメントレビューをするケースが増えていることを表していると思われる。

ISMS認証に関連する体制

25. ISMS事務局のメンバーは何人ですか？

1. 専任（　　人）
2. 兼務（　　人）
3. その他（　　人）

図1:事務局の人数

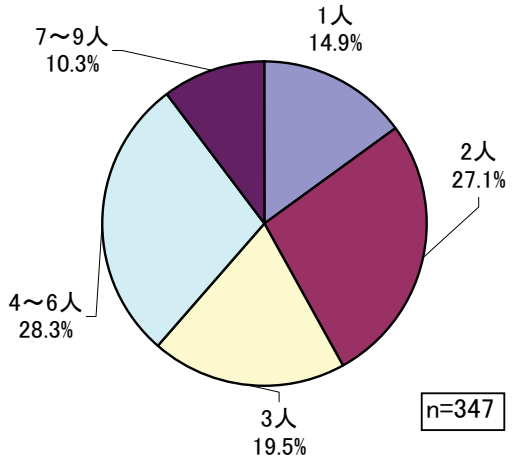
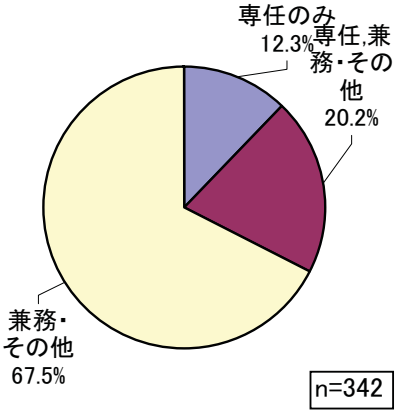


図2:事務局の体制



	有効回答数	1人	2人	3人	4~6人	7~9人	10人以上
今回	347	49	89	64	93	34	18
		14.1%	25.6%	18.4%	26.8%	9.8%	5.2%
前回	264	29	67	63	64	28	13
		11.0%	25.4%	23.9%	24.2%	10.6%	4.9%

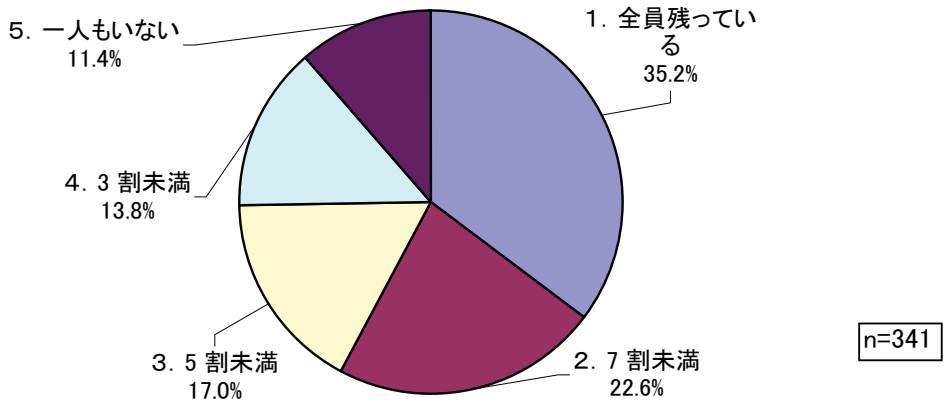
	有効回答数	専任のみ	専任＋兼務・その他	兼務・その他のみ
今回	342	42	69	231
		12.3%	20.2%	67.5%
前回	264	37	50	177
		14.0%	18.9%	67.0%

事務局の人数は「3人以下」と回答した企業が58.2%を占めており、前回同様の結果となっている。
「専任」の担当者を置いている企業は32.4%と前回同様、兼務体制で運営されているケースが多いことがわかる。

ISMS認証に関連する体制

26. 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ますか？（択一）

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



（単位:社数・%）

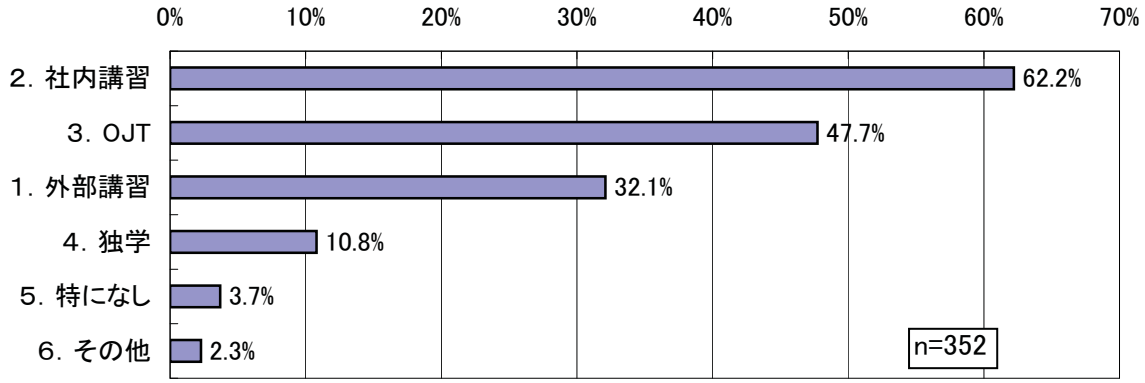
	有効回答数	1．全員残っている	2．7 割未満	3．5 割未満	4．3 割未満	5．一人もいない
今回	341	120	77	58	47	39
		35.2%	22.6%	17.0%	13.8%	11.4%
前回	263	142	50	20	32	19
		54.0%	19.0%	7.6%	12.2%	7.2%

52%が「全員残っている」と回答している反面、「一人もいない」が11.4%と前回よりも高くなってきている。これは認証取得から時間が経過しており、メンバー交代が増えていることを示している。

ISMS認証に関連する体制

27. 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いましたか？（複数選択可）

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. 特になし
6. その他（記入欄あり）



（単位：社数・%）

	有効回答数	2. 社内講習	3. OJT	1. 外部講習	4. 独学	5. 特になし	6. その他
今回	352	219	168	113	38	13	8
		62.2%	47.7%	32.1%	10.8%	3.7%	2.3%
前回	264	184	110	85	19	7	12
		69.7%	41.7%	32.2%	7.2%	2.7%	4.5%

その他詳細
コンサルタントの活用（2件）
新メンバーなし（5件）
審査員資格取得

「社内講習」、および「OJT」という社内リソースを利用したスキル取得が多い。
「外部」が減っていることから、スキルが内部に蓄積されてきたと思われる。

コンサルタント

28. コンサルタントを利用しましたか？（択一）

認証取得まで
1. 利用した
2. 一部利用した
3. 利用していない

認証取得後
4. 利用している
5. 一部利用している
6. 利用していない

図1. 認証取得まで

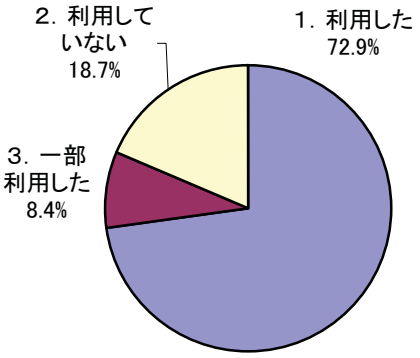


図2. 認証取得後

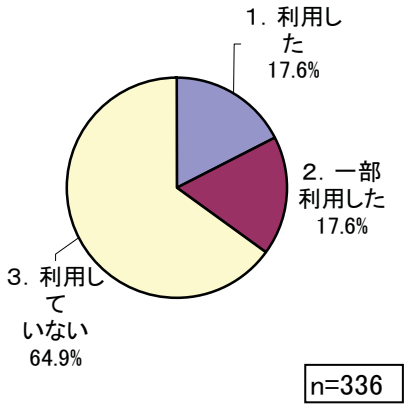


図1. 認証取得まで （単位：組織数・%）

	有効回答数	1. 利用した	2. 一部利用した	3. 利用していない
今回	347	253	29	65
	100%	72.9%	8.4%	18.7%
前回	263	182	29	52
	100%	69.2%	11.0%	19.8%

図2. 認証取得後 （単位：組織数・%）

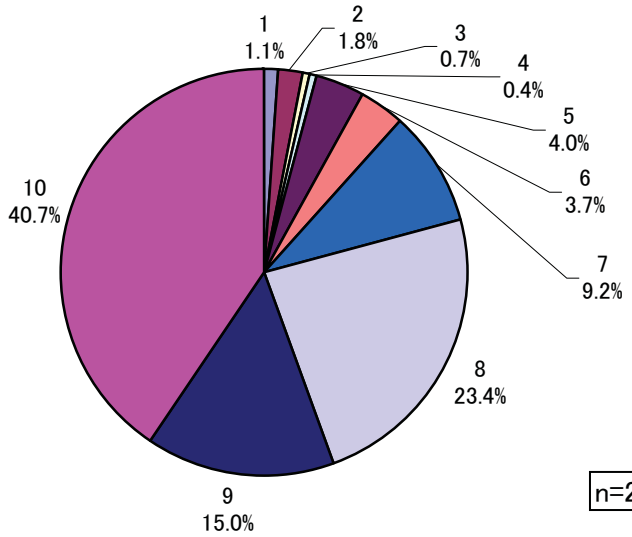
	有効回答数	1. 利用した	2. 一部利用した	3. 利用していない
今回	336	59	59	218
	100%	17.6%	17.6%	64.9%
前回	255	44	58	153
	100%	17.3%	22.7%	60.0%

外部コンサルタントの利用については、認証取得前に「利用した」「一部利用した」との回答の合計が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事業所が多いことが伺える。一方、認証取得後「利用していない」との回答が60%を超えており、認証取得後の維持管理については自ら実施する傾向が見て取れる。これらは、前回調査とほぼ同様の傾向を示している。

コンサルタント

29. コンサルタントは、ISMS 認証の要求事項を理解していましたか？（ 択一）

理解していない ← | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | → 理解していた



（単位：組織数・%）

有効回答数	1	2	3	4	5
273	3	5	2	1	11
100%	1.1%	1.8%	0.7%	0.4%	4.0%
	6	7	8	9	10
	10	25	64	41	111
	3.7%	9.2%	23.4%	15.0%	40.7%

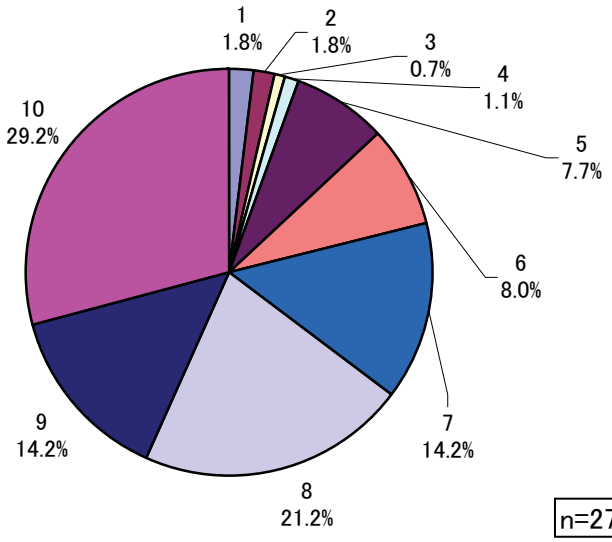
平均
8.4

10段階評価において、7点以上を約80%、9点以上を過半数が占めていることから、コンサルタントのISMS 認証要求事項理解度は高いと評価している事業所が多い傾向がみられる。

コンサルタント

30. セキュリティに関する技術について理解していましたか？（択一）

理解していない ← | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | → 理解していた



（単位：組織数・%）

有効回答数	1	2	3	4	5
274	5	5	2	3	21
100%	1.8%	1.8%	0.7%	1.1%	7.7%
	6	7	8	9	10
	22	39	58	39	80
	8.0%	14.2%	21.2%	14.2%	29.2%

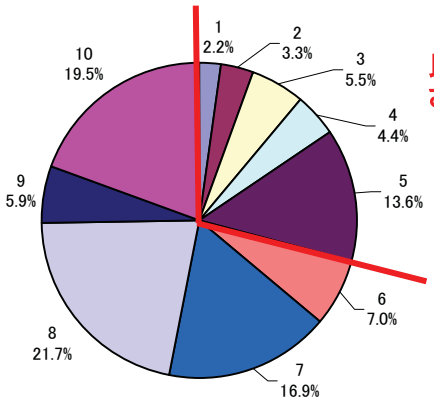
平均
7.9

10段階評価において、6点以上を約80%、9点以上を過半数が占めていることから、コンサルタントのISMS 認証要求事項理解度は高いと評価している事業所が多い傾向がみられる。

コンサルタント

31. あなたの組織の業務について理解していましたか？（択一）

理解していない ← | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | → 理解していた



（単位：組織数・%）

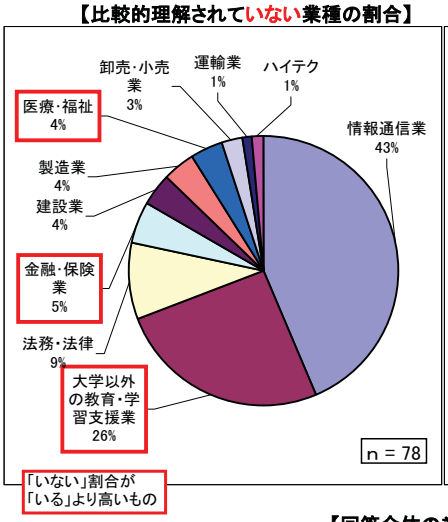
有効回答数	1	2	3	4	5
272	6	9	15	12	37
100%	2.2%	3.3%	5.5%	4.4%	13.6%

6	7	8	9	10
19	46	59	16	53
7.0%	16.9%	21.7%	5.9%	19.5%

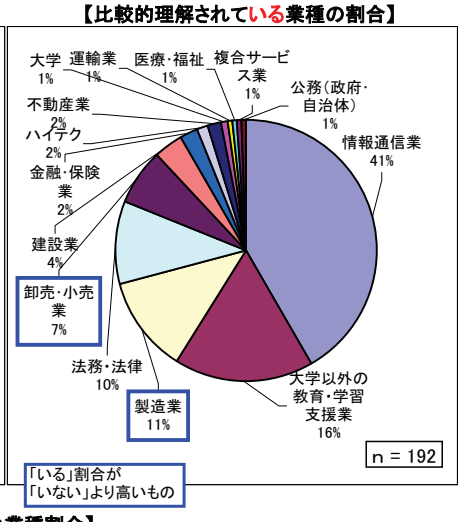
平均
6.9

10段階評価において、5点以下を約30%が占めていることから、コンサルタントの事業所の業務に対する理解度は必ずしも高くないと思われる。10段階評価の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」として比較した。理解されていない割合が比較的高いものとして「大学以外の教育・学習支援業」「金融・保険業」「医療・福祉」、理解されている割合が比較的高いものとして「製造業」「卸売・小売業」が見られた。

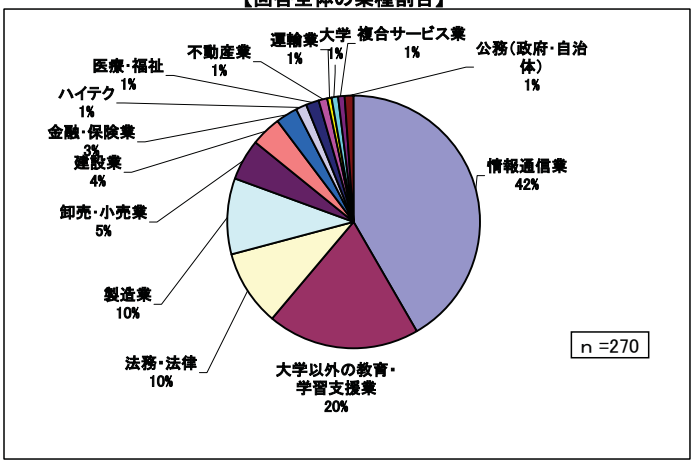
【比較的理解されていない業種の割合】



【比較的理解されている業種の割合】



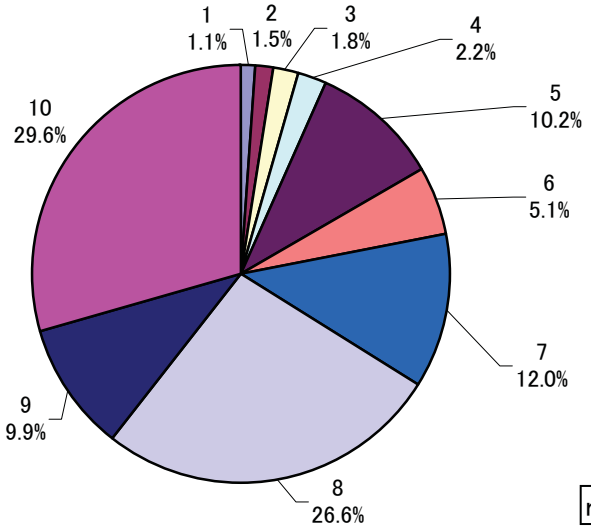
【回答全体の業種割合】



コンサルタント

32. コミュニケーションをうまく取ることができましたか？（択一）

理解していない ← | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | → 理解していた



（単位：組織数・%）

有効回答数	1	2	3	4	5
274	3	4	5	6	28
100%	1.1%	1.5%	1.8%	2.2%	10.2%
	6	7	8	9	10
	14	33	73	27	81
	5.1%	12.0%	26.6%	9.9%	29.6%

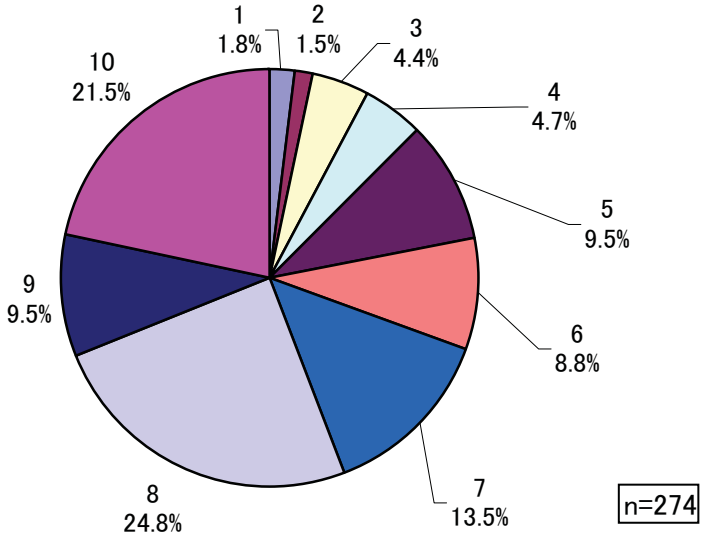
平均
7.8

10段階評価において、7点以上を約80%が占めていることから、コンサルタントのコミュニケーション能力は高いと評価している事業所が多い傾向がみられる。

コンサルタント

33. あなたの組織にとって実効性のある提案を行いましたか？（択一）

理解していない ← | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | → 理解していた



（単位：組織数・%）

有効回答数	1	2	3	4	5
274	5	4	12	13	26
100%	1.8%	1.5%	4.4%	4.7%	9.5%
	6	7	8	9	10
	24	37	68	26	59
	8.8%	13.5%	24.8%	9.5%	21.5%

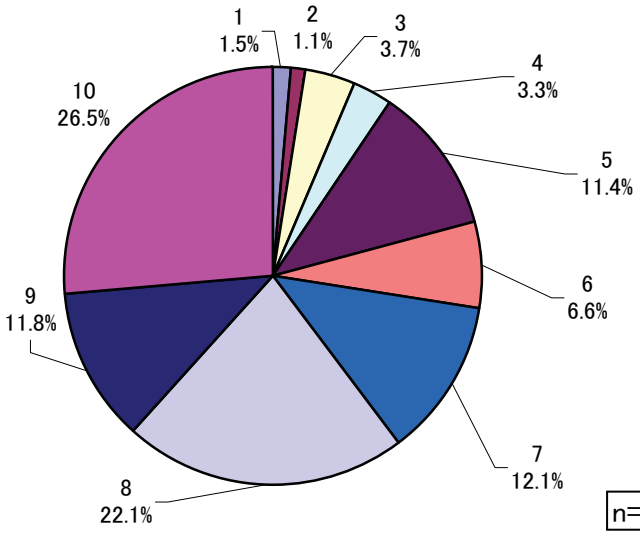
平均
7.3

10段階評価において、7点以上を約60%が占めていることから、コンサルタントは審査を受けた事業所にとって実効性のある提案を行ったと評価している事業所が比較的多い傾向がみられる。

コンサルタント

34. 確立したコンサルティング手法を持っていましたか？（択一）

理解していない ← | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | → 理解していた



（単位：組織数・%）

有効回答数	1	2	3	4	5
272	4	3	10	9	31
100%	1.5%	1.1%	3.7%	3.3%	11.4%
	6	7	8	9	10
	18	33	60	32	72
	6.6%	12.1%	22.1%	11.8%	26.5%

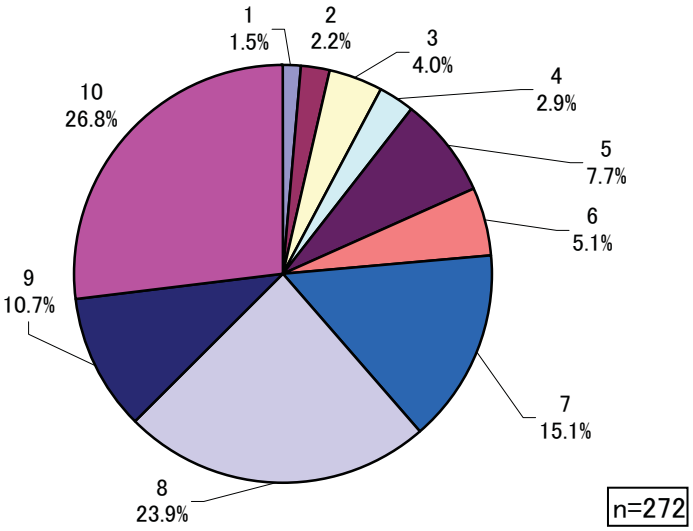
平均
7.6

10段階評価において、7点以上を70%が占めていることから、コンサルタントは概ね確立したコンサルティング手法を持っていたと評価している事業所が多い傾向がみられる。
また、4人に一人は5点以下の評価となっている。

コンサルタント

35. 一貫性を持ったコンサルティングを行いましたか？（択一）

理解していない ← | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | → 理解していた



（単位：組織数・%）

有効回答数	1	2	3	4	5
272	4	6	11	8	21
100%	1.5%	2.2%	4.0%	2.9%	7.7%
	6	7	8	9	10
	14	41	65	29	73
	5.1%	15.1%	23.9%	10.7%	26.8%

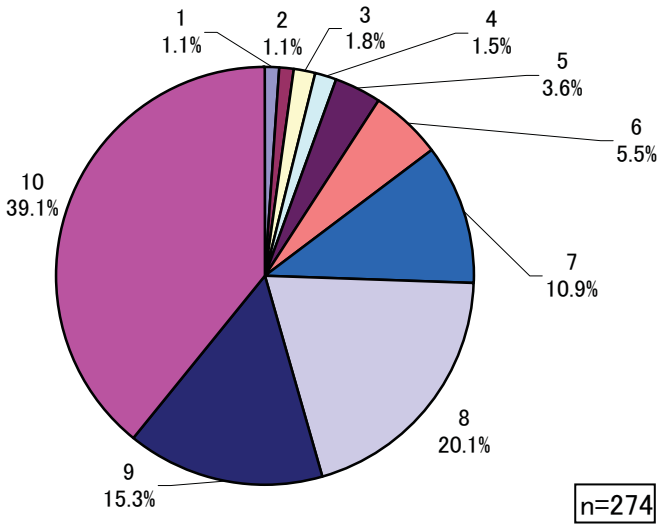
平均
7.6

10段階評価において、7点以上を約75%が占めていることから、コンサルタントは一貫性を持ったコンサルティングを行ったと評価している事業所が多い傾向がみられる。
また、5人に一人は5点以下の評価となっている。

コンサルタント

36. ISMS 認証を取得する上で役に立ちましたか？（択一）

理解していない ← | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | → 理解していた



（単位：組織数・%）

有効回答数	1	2	3	4	5
274	3	3	5	4	10
100%	1.1%	1.1%	1.8%	1.5%	3.6%
	6	7	8	9	10
	15	30	55	42	107
	5.5%	10.9%	20.1%	15.3%	39.1%

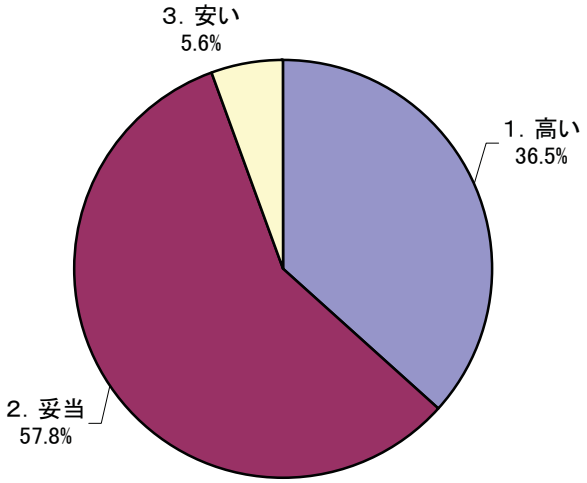
平均
8.3

10段階評価において、7点以上を約85%が占めていることから、コンサルタントはISMS 認証を取得する上で有効な活動を行ったと評価している事業所が多い傾向が見られる。

コンサルタント

37. 費用は妥当でしたか？（択一）

1. 高い 2. 妥当 3. 安い



n=249

（単位：組織数・%）

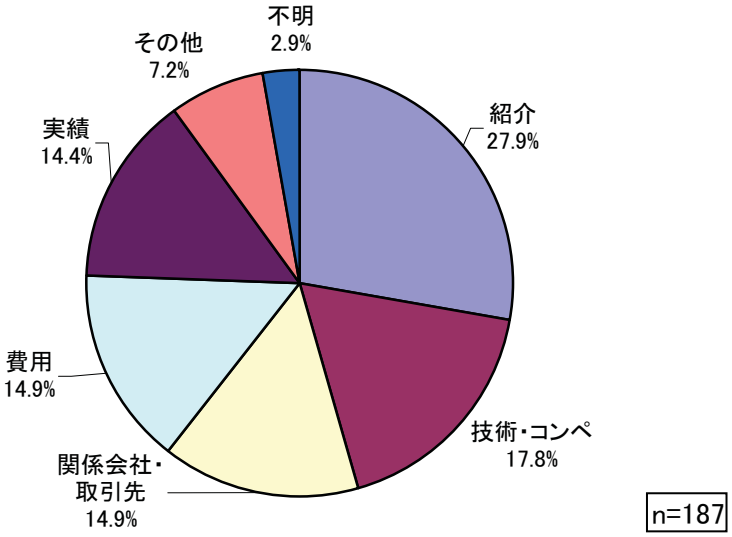
有効回答数	1. 高い	2. 妥当	3. 安い
249	91	144	14
100%	36.5%	57.8%	5.6%

コンサルタントの費用については、約60%の事業所が「妥当」と評価している。また、30%以上が「高い」としており、「安い」とした割合は低い傾向が見られた。

コンサルタント

38. どのような基準・手段でコンサルタントを選定したか、ご自由にお書き下さい。

（自由意見を分類。複数の内容を含むものは複数計上。）



（単位：組織数・%）

総数	紹介	技術・コンペ	関係会社・取引先	費用	実績	その他	不明
187	58	37	31	31	30	15	6
100%	31.0%	19.8%	16.6%	16.6%	16.0%	8.0%	3.2%

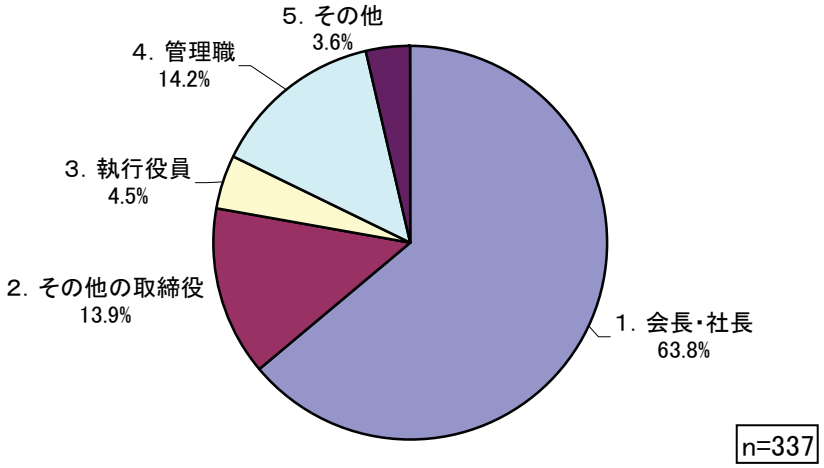
コンサルタント選定理由としては、「紹介」、「関係会社・取引先」など人脈や組織上の関係が高い割合を占めている。また「技術・コンペ」「実績」など業務能力、「費用」が同等の割合で見られる。

回答例
・紹介　：　グループ会社の紹介、社長の知人、取引先の紹介
・技術・コンペ　：　3社によるコンペ、提案資料、業務内容の理解
・関係会社・取引先　：　グループ会社、ビジネス上のパートナー関係にあった為
・費用　：　コンサルティング費用、相見積り
・実績　：　9001 14001 と同じコンサル、同業社の取得事例が多いこと

コンサルタント

39. コンサルタント導入・選定の最終判断はどなたでしたか？（択一）

1. 会長・社長 2. その他の取締役 3. 執行役員 4. 管理職 5. その他



（単位：組織数・%）

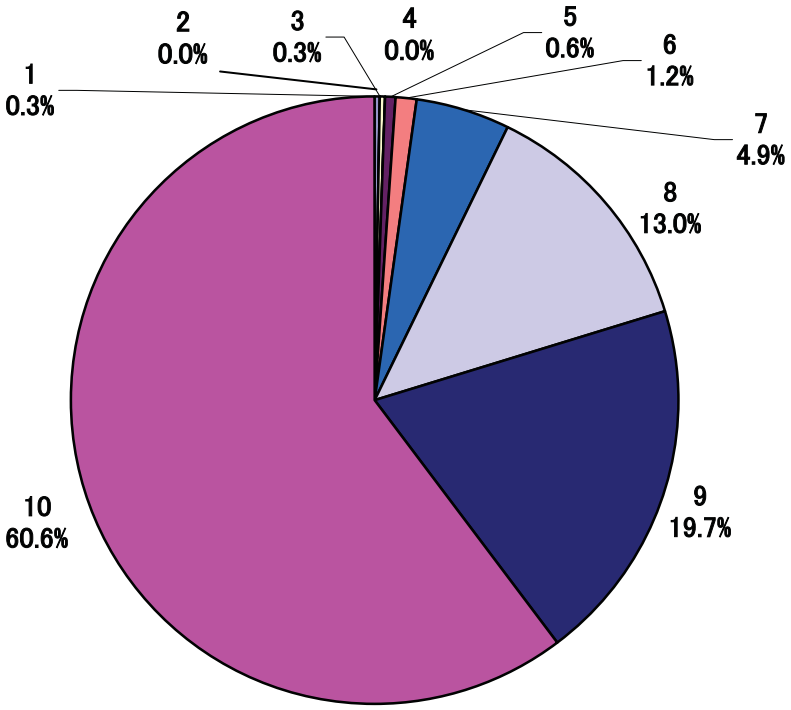
有効回答数	1. 会長・社長	2. その他の取締役	3. 執行役員	4. 管理職	5. その他
337	215	47	15	48	12
100%	63.8%	13.9%	4.5%	14.2%	3.6%

コンサルタント導入・選定の最終判断は社長・会長、その他の取締役、執行役員等の経営陣、トップが行っている割合が高い傾向が見られる。

ISMS認証審査及び審査員

40. ISMS 審査員は、ISMS 認証の要求事項を理解していましたか？（ 択一）

理解していない ← | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | → 理解していた



（単位：社数・%）

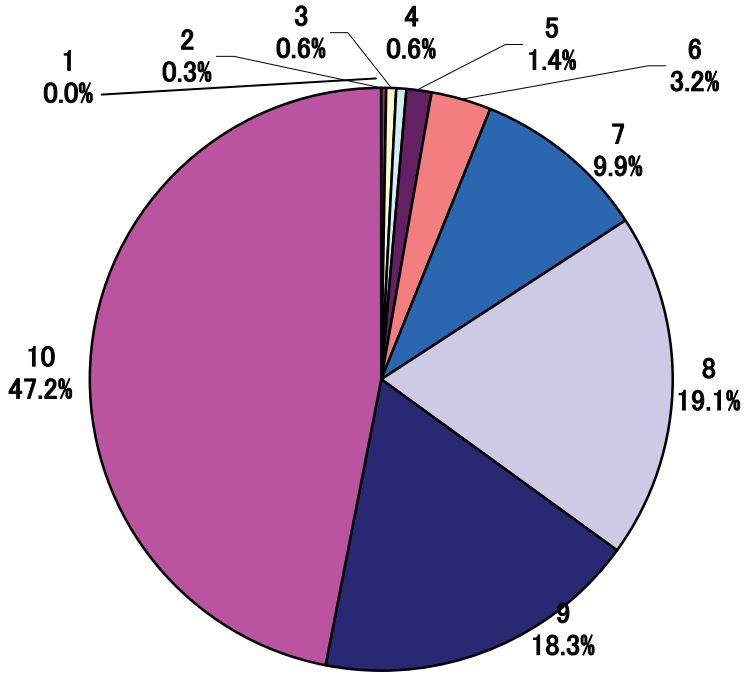
有効回答数	1	2	3	4	5
347	1	0	1	0	2
100%	0.3%	0.0%	0.3%	0.0%	0.6%
	6	7	8	9	10
	4	17	45	68	209
	1.2%	4.9%	13.0%	19.7%	60.6%

平均
9.3

審査員がISMS認証の要求事項を理解しているかどうかについて尋ねた所、理解度8以上の回答が、約93%あった。この事から、組織内のISMS担当者は、審査員がほぼ理解していると感じている事が言える。

41. セキュリティに関する技術について理解していましたか？（択一）

理解していない ← | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | → 理解していた



n=347

（単位：社数・%）

有効回答数	1	2	3	4	5
347	0	1	2	2	5
100%	0.0%	0.3%	0.6%	0.6%	1.4%
	6	7	8	9	10
	11	34	66	63	163
	3.2%	9.9%	19.1%	18.3%	47.2%

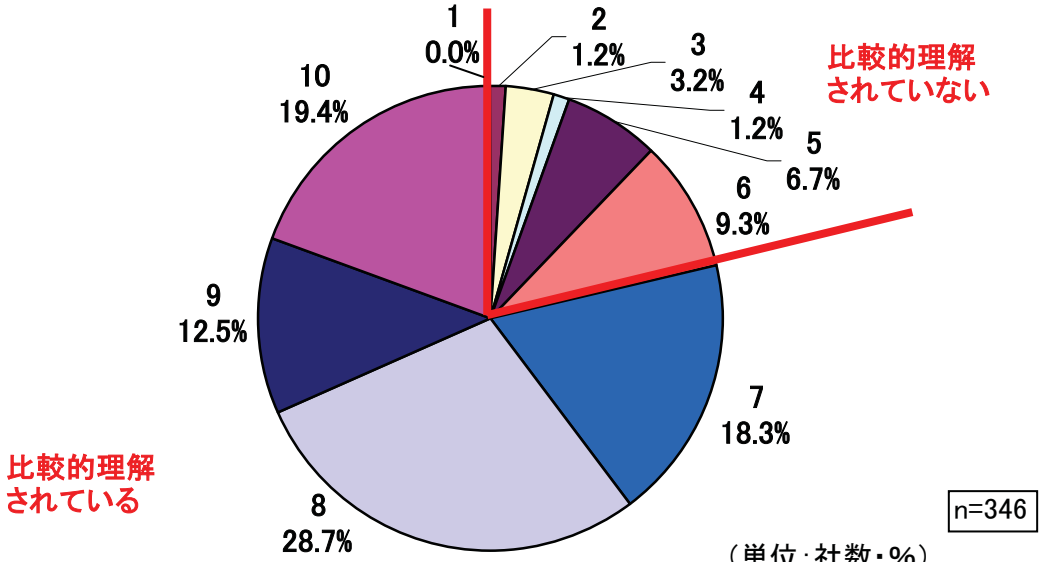
平均
8.8

次に審査員が情報セキュリティ技術について理解していたと思うかを尋ねた。此方も、理解度8以上が全体の約85%を占めており、審査員の技術レベルについては、あまり問題ないと感じている人が多い。

ISMS認証審査及び審査員

42. あなたの組織の業務について理解していましたか？（択一）

理解していない ← | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | → 理解していた



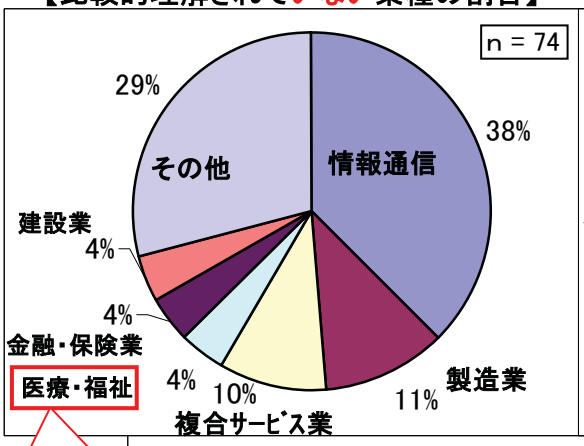
（単位：社数・%）

有効回答数	1	2	3	4	5
346	0	4	11	4	23
100%	0.0%	1.2%	3.2%	1.2%	6.7%
	6	7	8	9	10
	32	63	99	43	67
	9.3%	18.3%	28.7%	12.5%	19.4%

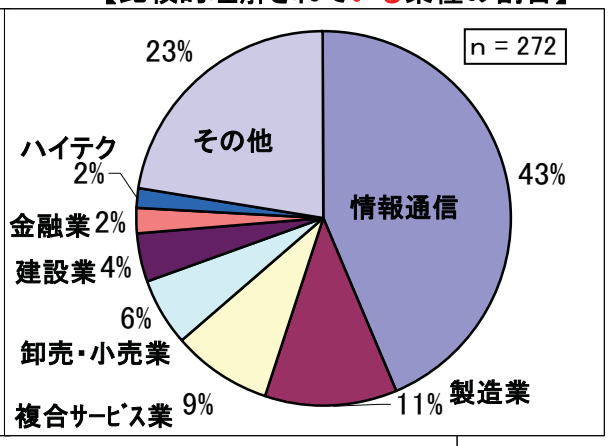
平均
7.7

ISMS審査員が、対象組織の業務内容をどの程度理解してくれていると感じているかを尋ねた。概ね、概ね理解してくれていると感じているが若干ばらつきがある。理解度が6以下である審査員も全体で約21%存在している。そこで、比較的理解されている/いないで二分し、業種に特徴があるかを更に分析した。

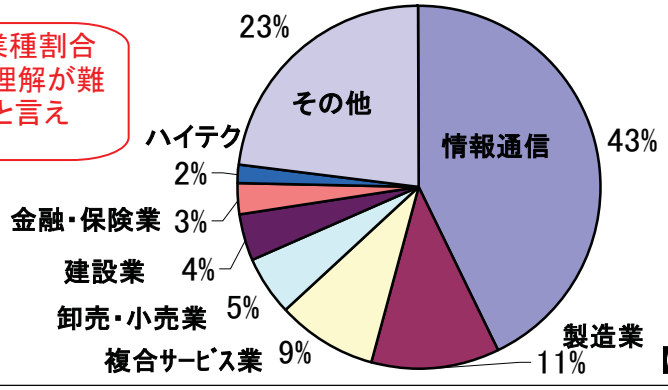
【比較的理解されていない業種の割合】



【比較的理解されている業種の割合】



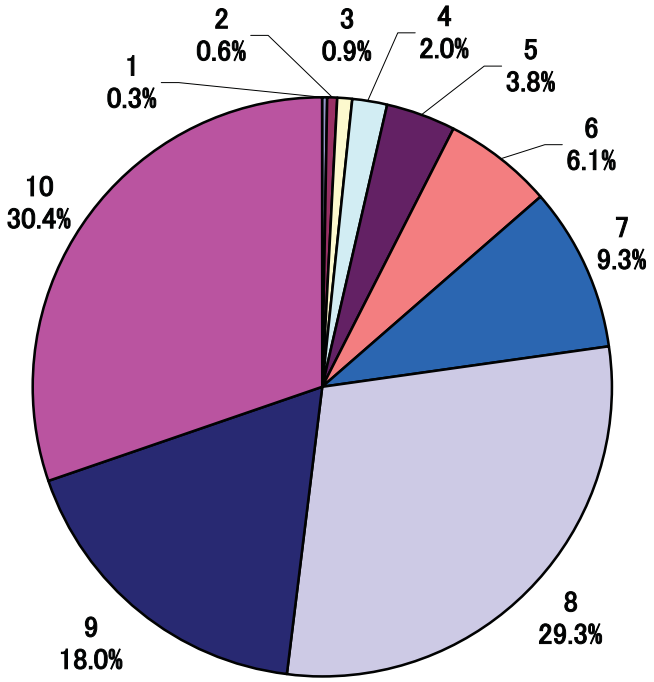
回答者全体の業種割合と比べて多い。理解が難しい業種であると言える。



【回答者全体の業種割合】

43. コミュニケーションをうまく取ることができましたか？（択一）

理解していない ← | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | → 理解していた



（単位：社数・%）

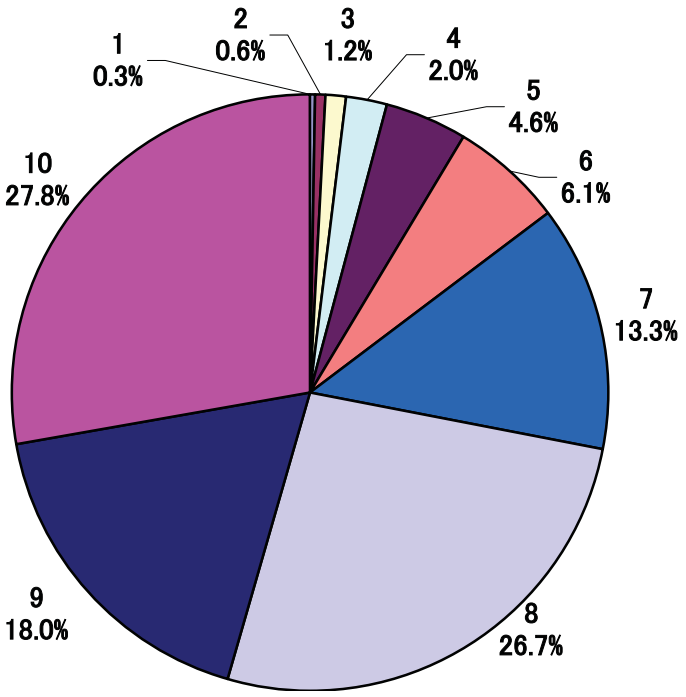
有効回答数	1	2	3	4	5
347	1	2	3	7	13
100%	0.3%	0.6%	0.9%	2.0%	3.8%
	6	7	8	9	10
	21	32	101	62	105
	6.1%	9.3%	29.3%	18.0%	30.4%

平均
8.3

ISMS審査員のコミュニケーション能力について尋ねた。此方も、理解度8以上が全体の約78%を占めており、全体としてはコミュニケーションが問題無くとれていると見ることができる。問32でコンサルテーションとのコミュニケーションに関するの回答があるが、審査員の方がコミュニケーションがとれたと回答している方が多い。一方で少数だが、コミュニケーションが取れていないと感じる担当者も中には存在している。

44. あなたの組織にとって実効性のある指摘を行いましたか？（択一）

理解していない ← | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | → 理解していた



n=347

（単位：社数・%）

有効回答数	1	2	3	4	5
347	1	2	4	7	16
100%	0.3%	0.6%	1.2%	2.0%	4.6%
	6	7	8	9	10
	21	46	92	62	96
	6.1%	13.3%	26.7%	18.0%	27.8%

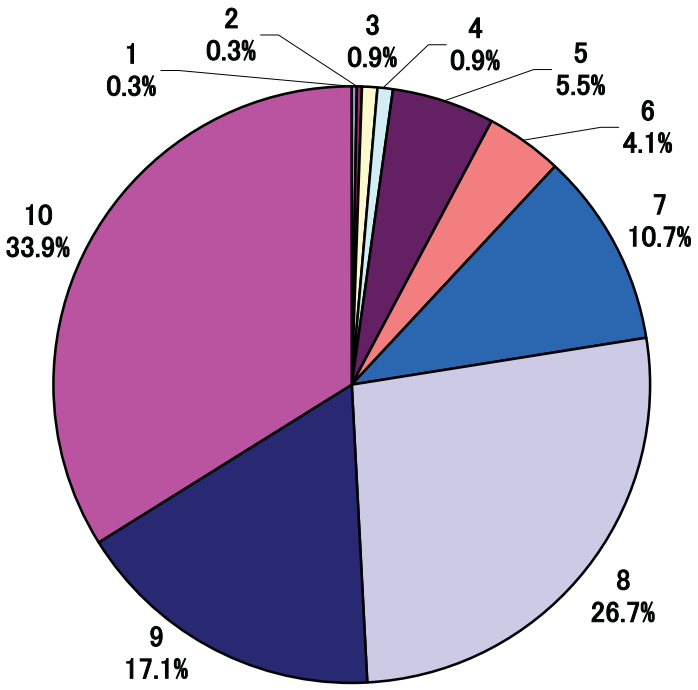
平均
8.1

ISMS審査員が行った指摘が実効性をともなっていたかどうかについて尋ねた。全体としては、実効性が伴った指摘を受けていると感じている組織が大半を占めている（8以上が、約73%）。一方で、5以下を選んだ回答が全体の約9%を占めていることは、少ない数値では無いと思われる。

ISMS認証審査及び審査員

45. あなたの組織にとって効果や課題を確認する能力を持っていましたか？（択一）

理解していない ← | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | → 理解していた



（単位：社数・%）

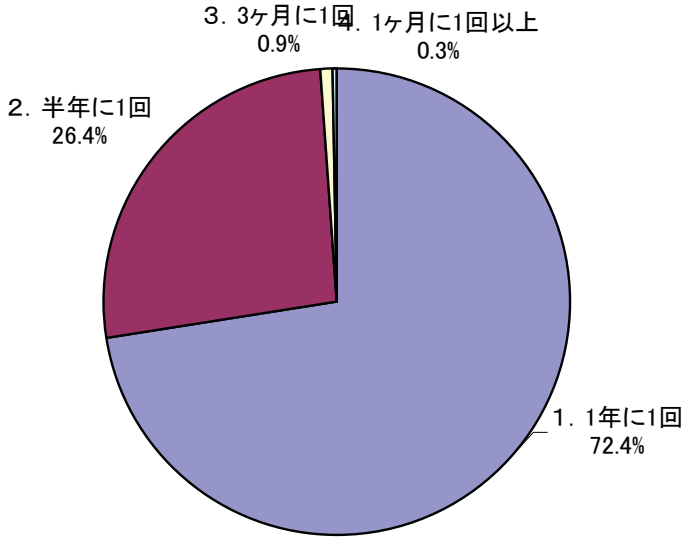
有効回答数	1	2	3	4	5
346	1	1	3	3	19
100%	0.3%	0.3%	0.9%	0.9%	5.5%
	6	7	8	9	10
	14	37	92	59	117
	4.1%	10.7%	26.7%	17.1%	33.9%

平均
8.4

ISMS審査員が行った指摘が実効性をともなっていたかどうかについて尋ねた。全体としては、実効性が伴った指摘を受けていると感じている組織が大半を占めている（8以上が約78%）。一方で、5以下を選んだ回答が全体の約8%を占めていることは、少ない数値では無いと思われ、審査員の業務理解と合わせて、実効性を持った指摘を行う事が更に求められる結果となった。

内部監査について

46. 実施頻度は？（択一）
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



n=348

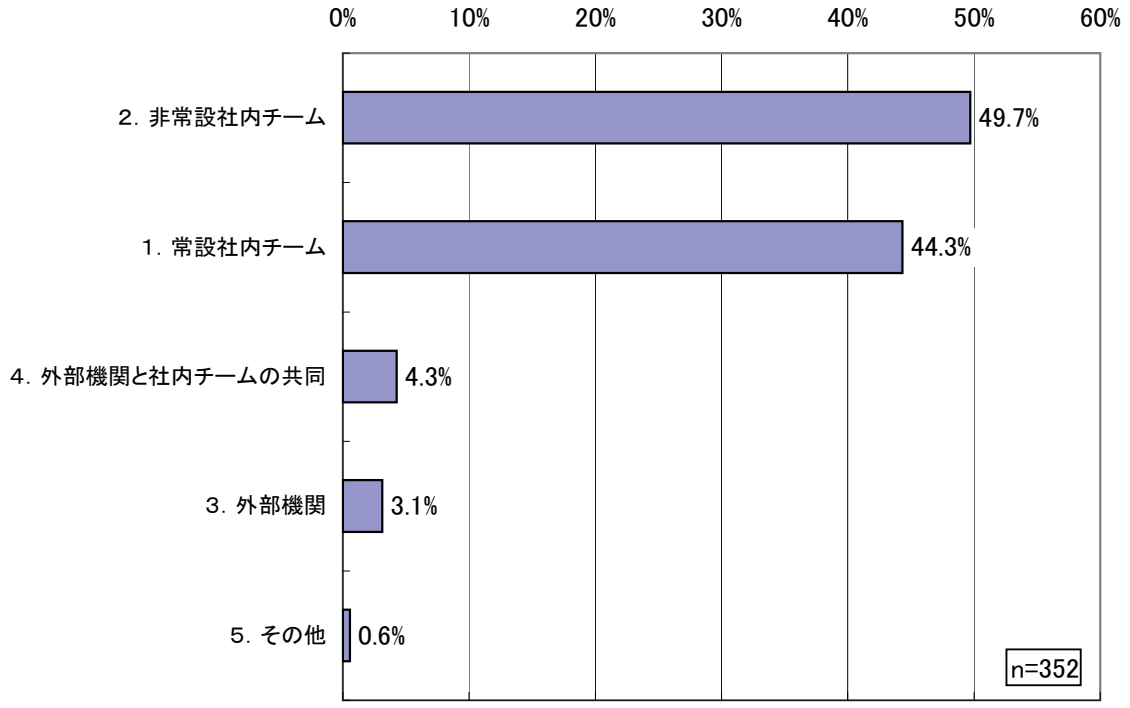
内部監査の実施頻度は？　（単位：社数・%）

	有効回答数	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回以上
今回	348	252	92	3	1
	100.0%	72.4%	26.4%	0.9%	0.3%
前回	264	171	88	2	3
	100.0%	64.8%	33.3%	0.8%	1.1%

「1年に1回」及び「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約98%となり大半を占めている。逆に「3ヶ月に1回」と答えた企業は全体のわずか1%弱に止まっている。この傾向は前回調査と変化は無い。
また、前回の調査では「1ヶ月に1回以上」実施していた企業が3社あったが、今回は1社に減少している。

内部監査について

47. 内部監査の体制は？（複数選択可）
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. 外部機関と社内チームの共同体制
5. その他（記入欄あり）



内部監査の体制は？　（単位：社数・%）

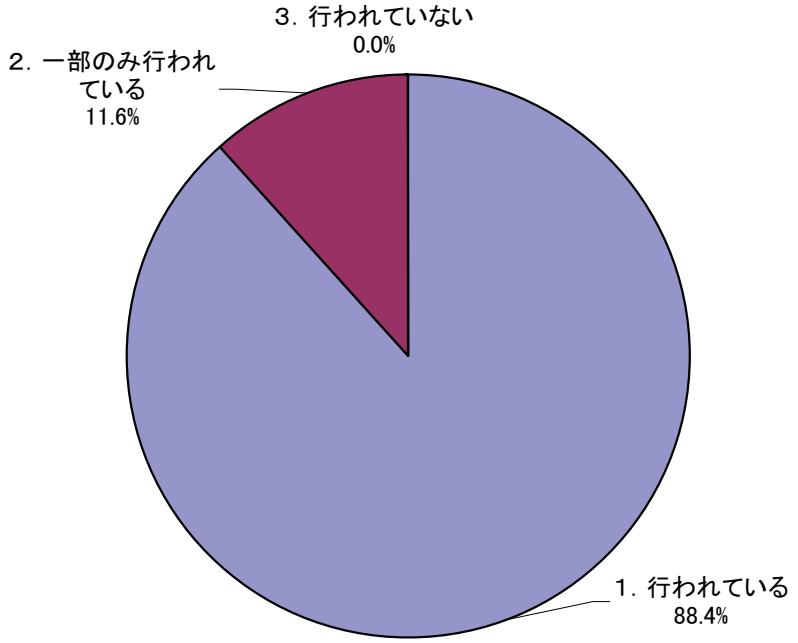
	有効回答数	1. 常設社内チーム	2. 非常設社内チーム	3. 外部機関	4. 外部機関と社内チームの共同	5. その他
今回	359	156	175	11	15	2
		44.3%	49.7%	3.1%	4.3%	0.6%
前回	264	101	151	7	14	2
		38.3%	57.2%	2.7%	5.3%	0.8%

その他詳細
事務局員（1件）
部外に依頼（1件）

「常設の社内チーム」及び「非常設の社内チーム」との回答が大半を占めており、全体の約94%に及んでいる。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。
前回調査と比べると、常設の社内チームの割合が6%増加しており、非常設の社内チームは7.5%減少している。このことから、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。

内部監査について

48. 指摘事項に対する改善は行われていますか？（ 択一）
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



n=345

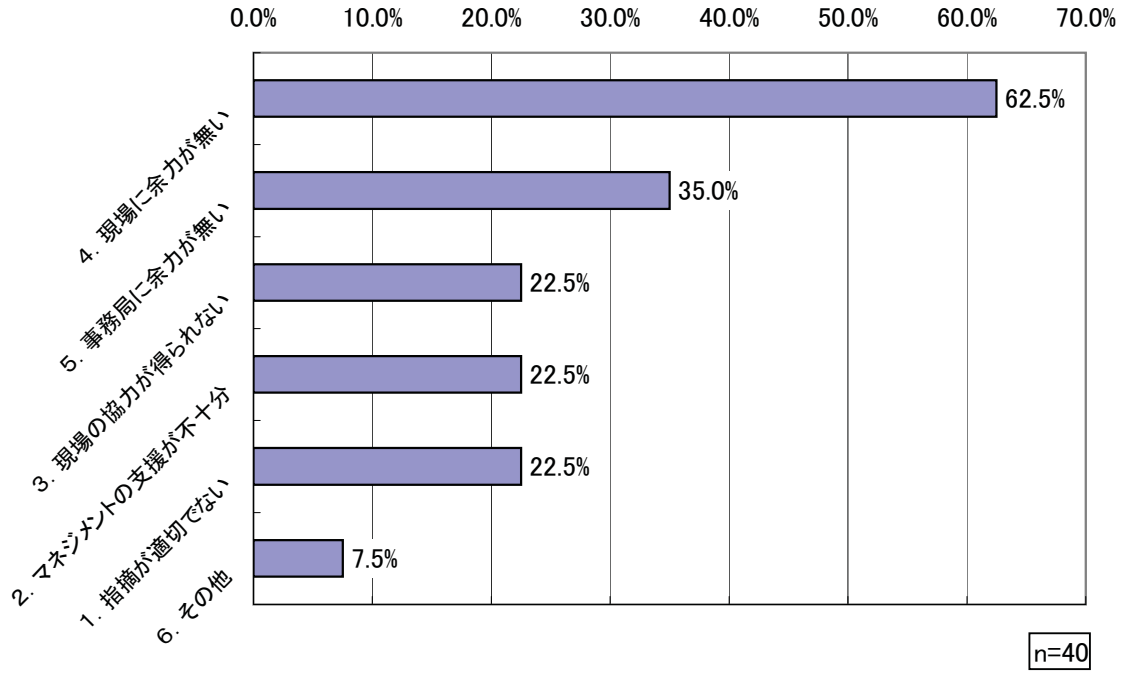
指摘事項に対する改善は行われていますか？　　（ 単位：社数・%）

	有効回答数	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
今回	345	305	40	0
	100.0%	88.4%	11.6%	0.0%
前回	264	239	25	0
	100.0%	90.5%	9.5%	0.0%

「行われている」が全体の約88%を占めている。また、「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想定される。
前回の調査と比べて特に傾向の変化は無い。

内部監査について

49. 問48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。その理由をお答えください。(複数選択可)
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(記入欄あり)



(単位:社数・%)

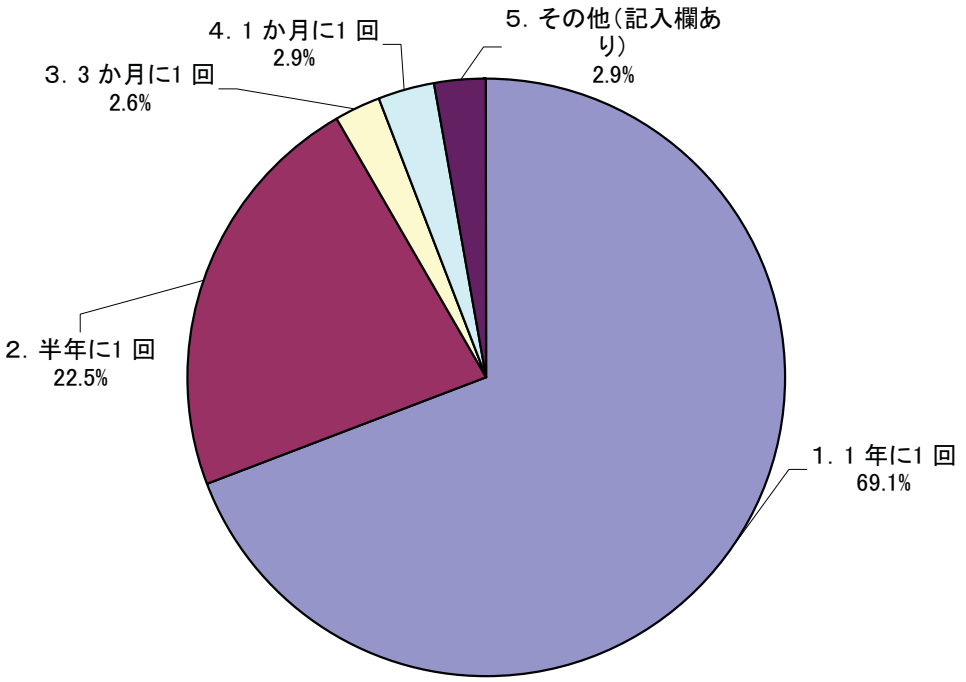
	有効回答数	1. 指摘が適切でない	2. マネジメントの支援が不十分	3. 現場の協力が得られない	4. 現場に余力が無い	5. 事務局に余力が無い	6. その他
今回	40	9	9	9	25	14	3
	100.0%	22.5%	22.5%	22.5%	62.5%	35.0%	7.5%
前回	25	5	7	3	13	13	3
		20.0%	28.0%	12.0%	52.0%	52.0%	12.0%

その他詳細
費用の問題(1件)
不要、不可能なものを除外(1件)
内部監査のスキル向上が必要(1件)

「現場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、半数以上が回答を選択している結果となった。また、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、今回は17%減少しており、事務局には改善作業に従事するための余裕が出てきたことが伺える。
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、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想定される。

マネジメントレビューについてお聞きします

50. 実施頻度をお答えください。(択一)
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(記入欄あり)



n=338

マネジメントレビューの実施頻度は？ (単位:社数・%)

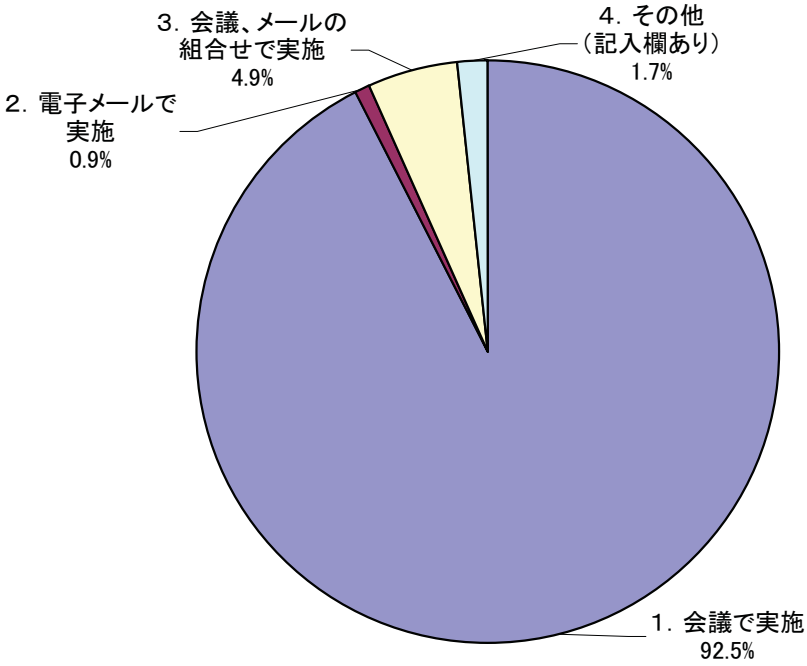
	有効回答数	1. 1 年に1回	2. 半年に1回	3. 3 か月に1 回	4. 1 か月に1 回	5. その他(記入欄あり)
今回	346	239	78	9	10	10
	100.0%	69.1%	22.5%	2.6%	2.9%	2.9%
前回	264	163	77	8	11	5
	100.0%	61.7%	29.2%	3.0%	4.2%	1.9%

その他詳細
毎週の定例MTGをMRとしている(2件)
2ヶ月に1回(1件)
4ヶ月に1回(2件)
年に2回(1件)
定期年1回と必要に応じて(3件)
必要に応じて(1件)

「1年に1回」との回答が全体の約69%を占めており過半数となっている。さらに、「半年に1回」と回答した企業を含めた場合は全体の約92%に達している。また、「3ヶ月に1回」および「1ヶ月に1回」は全体の3%、3%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分かる。この傾向は前回調査と大きな変化は無い。

マネジメントレビューについてお聞きします

51. 実施形態をお答えください。(択一)
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(記入欄あり)



n=340

マネジメントレビューの実施形態は？ (単位:社数・%)

	有効回答数	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(記入欄あり)
今回	347	321	3	17	6
	100.0%	92.5%	0.9%	4.9%	1.7%
前回	264	255	0	7	2
	100.0%	96.6%	0.0%	2.7%	0.8%

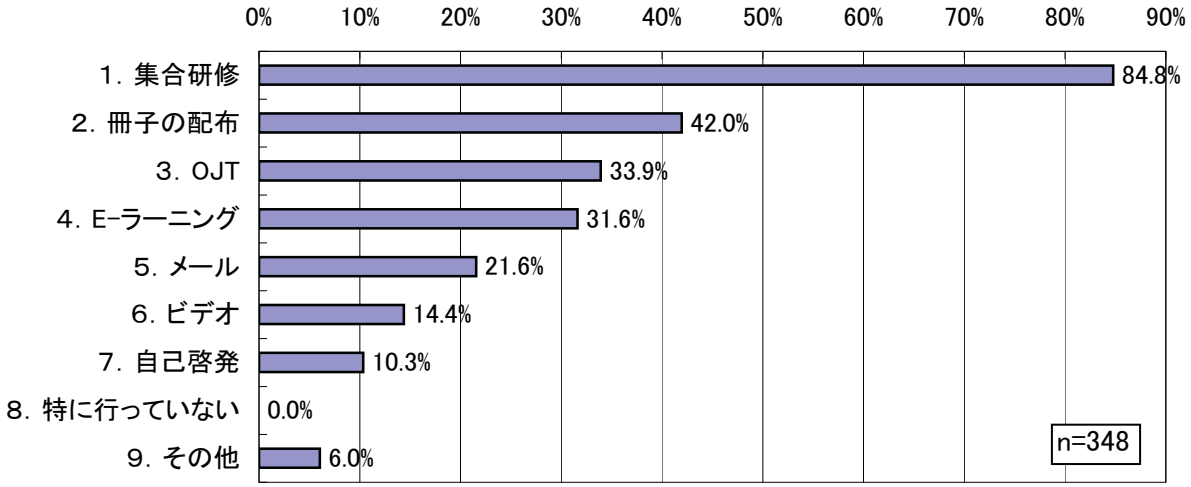
その他詳細
報告書(3件)
実質実施していない(1
未回答(2件)

「会議で実施」と回答した企業が全体の約92%を占めており大多数である。前回と比べると、「会議、メールの組合せで実施」の回答をしている企業が10社増えており、関係者へメール等を送信することで会議実施の証跡を残す組織が多くなっているように見受けられる。

教育・社内ルール

52. ISMSの維持に必要と思われる社員教育の手段についてお答え下さい（複数選択可）

1：集合研修
2：冊子の配布
3：OJT
4：E-ラーニング
5：メール
6：ビデオ
7：自己啓発
8：特に行っていない
9：その他（記入欄あり）



	有効回答数	1. 集合研修	2. 冊子の配布	3. OJT	4. E-ラーニング	5. メール	6. ビデオ
今回	851	295	146	118	110	75	50
		84.8%	42.0%	33.9%	31.6%	21.6%	14.4%
前回	647	243	124	80	64	61	33
		92.0%	47.0%	30.0%	24.2%	23.2%	12.5%

7. 自己啓発	8. 特になし	9. その他
36	0	21
10.3%	0.0%	6.0%
20	1	21
7.6%	0.4%	8.0%

その他詳細

外部研修（3件）
回覧（2件）
掲示板（2件）
朝礼・会議等（3件）
web・メール（2件）
定期チェック（2件）
テスト（2件）
他（5件）

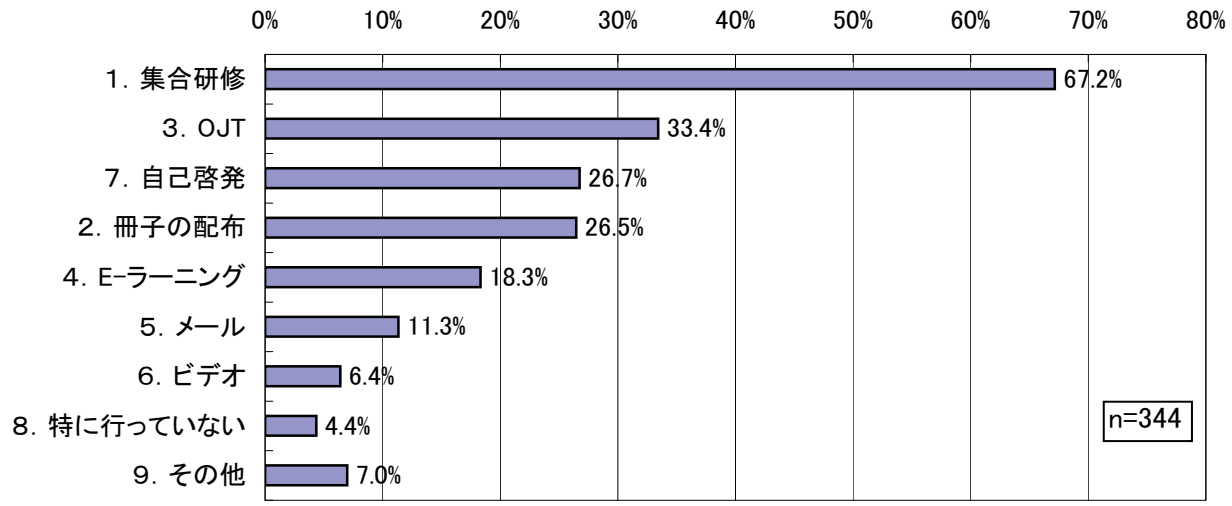
前回と同様、講師による集合研修が多数を占め、その他の項目にも順位に変動は見られなかった。集合研修に加え、冊子配布やビデオなどの個人学習が行われている。

全従業員に対し同レベルの集合教育を実施することで一斉にボトムアップを図ろうとした結果であり、個人学習においてその補完を行うのが一般的な教育方法であると考えられる。

教育・社内ルール

53. 同じく、情報セキュリティ管理者・推進者教育の手段についてお答え下さい（複数選択可）

1:集合研修
2:冊子の配布
3:OJT
4:E-ラーニング
5:メール
6:ビデオ
7:自己啓発
8:特に行っていない
9:その他（記入欄あり）



	有効回答数	1. 集合研修	3. OJT	7. 自己啓発	2. 冊子の配布	4. E-ラーニング	5. メール
今回	692	231	115	92	91	63	39
		67.2%	33.4%	26.7%	26.5%	18.3%	11.3%
前回	532	197	60	33	98	41	44
		74.6%	22.7%	12.5%	37.1%	15.5%	16.7%

6. ビデオ	8. 特になし	9. その他
22	15	24
6.4%	4.4%	7.0%
18	16	25
6.8%	6.1%	8.4%

その他詳細
外部講習・研修（17件）
他（7件）

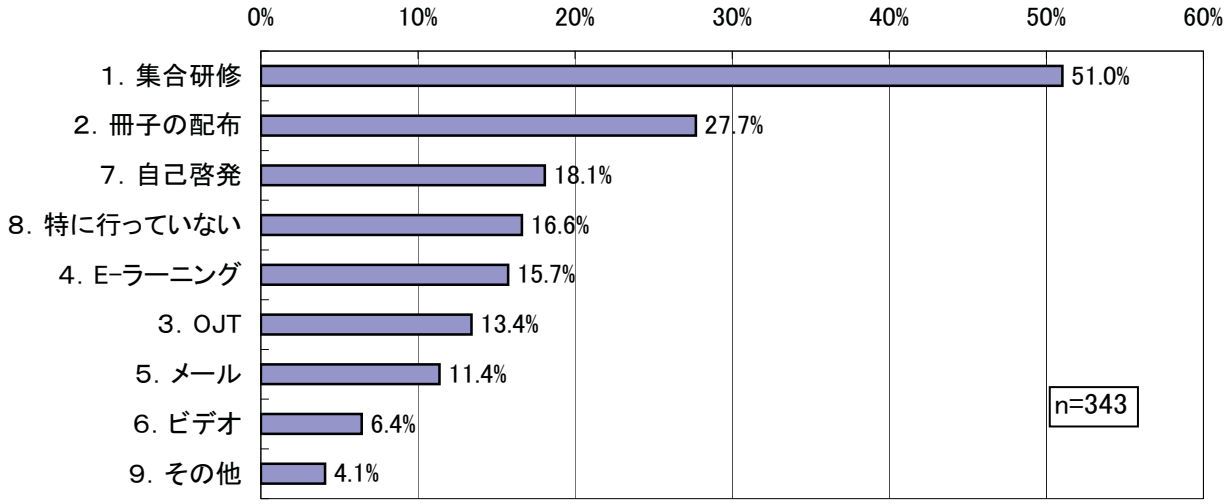
一般社員と比較して情報セキュリティ管理者・推進者に対しては、前回は比較的少なかった「自己啓発」「OJT」による教育方法の増加が目立つ。管理者としての自覚を高めるためと考えられる。

また、その他に「外部研修」の記述が増えていることから、自社外でスキルを身につけ、活用するフローがあることが想定される。

教育・社内ルール

54. 同じく、経営陣教育の手段についてお答え下さい（複数選択可）

1:集合研修
2:冊子の配布
3:OJT
4:E-ラーニング
5:メール
6:ビデオ
7:自己啓発
8:特に行っていない
9:その他（記入欄あり）



	有効回答数	1. 集合研修	2. 冊子の配布	7. 自己啓発	8. 特になし	4. E-ラーニング	3. OJT
今回	564	175	95	62	57	54	46
		51.0%	27.7%	18.1%	16.6%	15.7%	13.4%
前回	442	141	92	20	46	35	34
		53.4%	34.8%	7.6%	17.4%	13.3%	12.9%

5. メール	6. ビデオ	9. その他
39	22	14
11.4%	6.4%	4.1%
38	14	22
14.4%	5.3%	8.4%

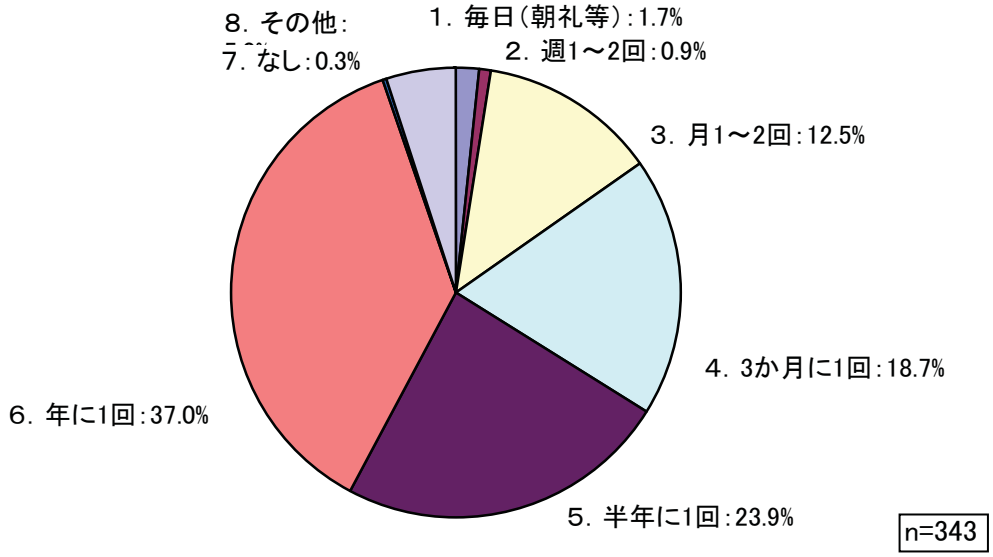
その他詳細
個別研修（5件）
会議（2件）
外部研修（2件）
他（5件）

一般社員らと比較すると、「特に行っていない」ケースが大きく増加している。経営陣に対しては教育が行いづらいことが想定される。また、前回と比較すると「自己啓発」に増加傾向が見られることから、経営陣自らの行動が求められていることがわかる。

一般的にはトップダウンで行う情報セキュリティにおいて、経営陣に対する教育機会が消極的であることについては改善の機会があると考えられる。

教育・社内ルール

55, ISMSに関する教育の年間の頻度をお答え下さい（択一）
1：毎日（朝礼等）　6：年に1回
2：週1～2回　7：なし
3：月に1～2回　8：その他（記入欄あり）
4：3か月に1回
5：半年に1回



	有効回答数	1．毎日（朝礼等）	2．週1～2回	3．月に1～2回	4．3か月に1回
今回	336	6	3	43	64
		1.7%	0.9%	12.5%	18.7%
前回	264	4	8	37	41
		1.4%	3.0%	14.0%	15.5%

5．半年に1回	6．年に1回	7．なし	8．その他
82	127	1	17
23.9%	37.0%	0.3%	5.0%
59	72	4	39
22.3%	27.3%	1.5%	14.8%

その他詳細
必要に応じて実施（9件）
レベルによって実施回数が変化(4件）
他（4件）

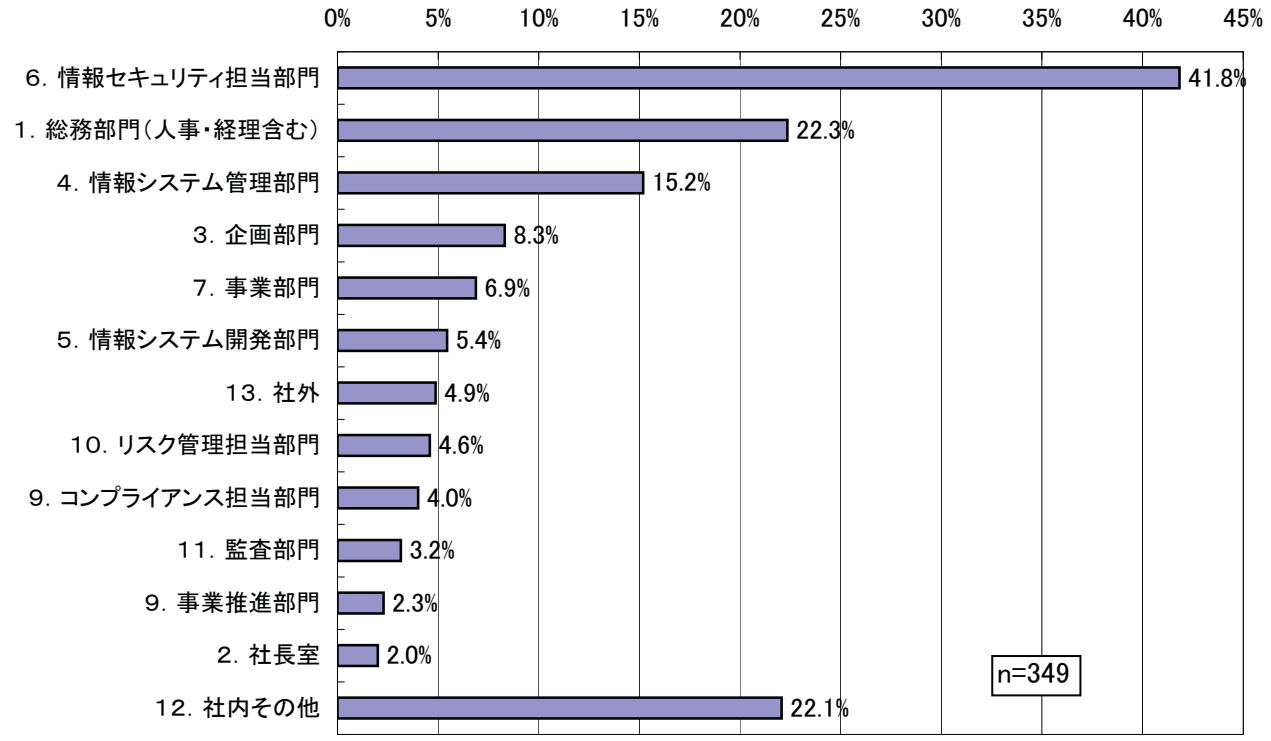
年間1～2回が半数以上を占め、前回とほぼ同じ傾向が見られる。これは、カリキュラムを定めた講義形式での実施であると考えられる。また少数ではあるが毎日～週数度実施しているケースもあるが、これは日々気づいたことなどを少しずつ継続的に実施しているものと考えられる。

教育としては、この両方を行うことでより意識付けが強く行われるものと思われる。

教育・社内ルール

56. ISMSに関する教育の担当部門をお答え下さい（複数選択可）

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



	有効回答数	6. セキュリティ	1. 総務部門	4. 情シス管理	3. 企画部門	7. 事業部門	5. 情シス開発	13. 社外
今回	499	146	78	53	29	24	19	17
		41.8%	22.3%	15.2%	8.3%	6.9%	5.4%	4.9%
前回	355	134	55	39	22	24	10	(40)
		50.8%	20.8%	14.8%	8.3%	9.1%	3.8%	(15.2%)

10. リスク管理	9. コンプライアンス	11. 監査部門	9. 事推部門	2. 社長室	12. 社内その他
16	14	11	8	7	77
4.6%	4.0%	3.2%	2.3%	2.0%	22.1%
4	12	9	―	6	(40)
1.5%	4.5%	3.4%	―	2.3%	(15.2%)

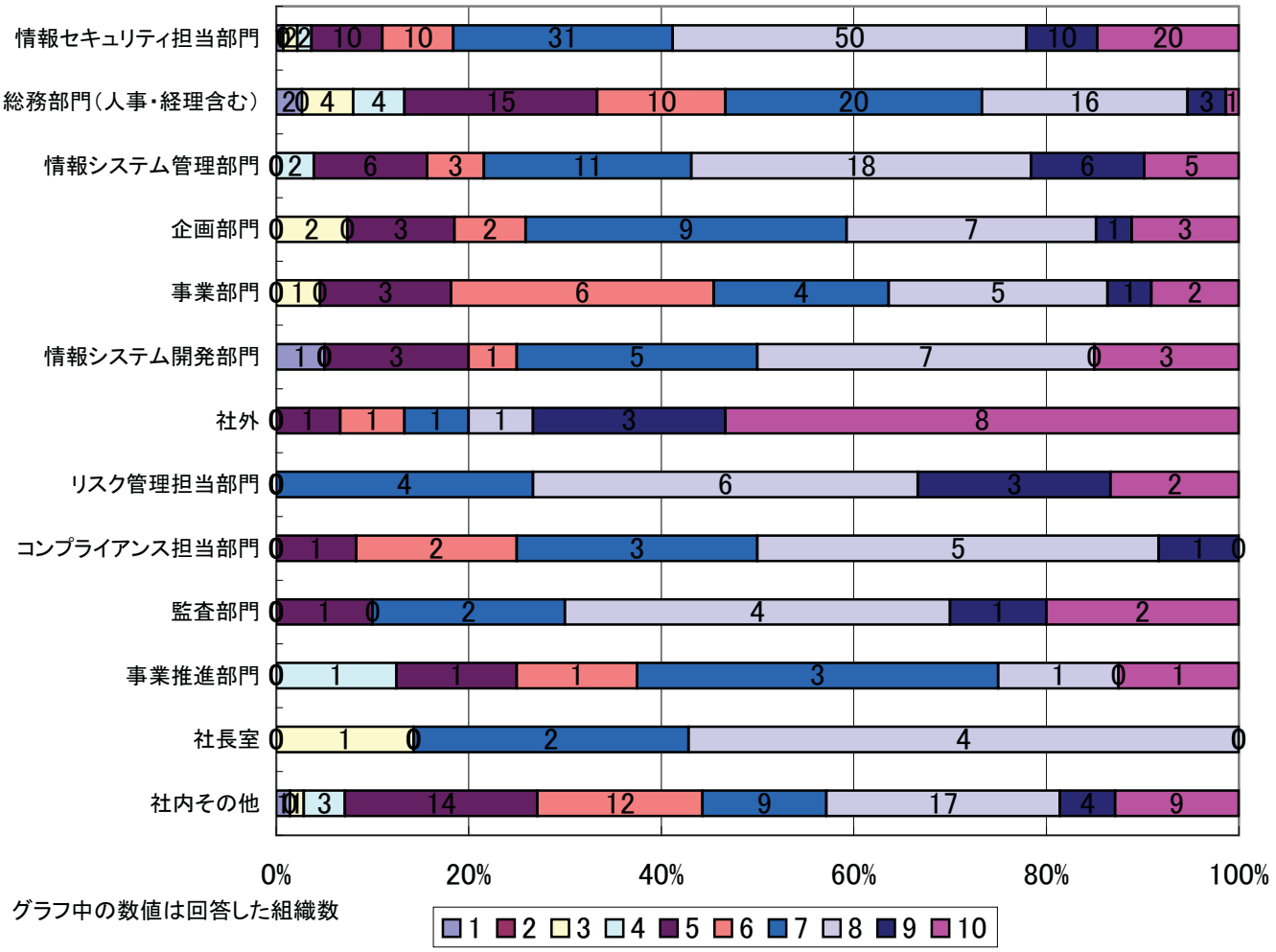
今回も情報セキュリティ部門による実施が目立つ。その他も前回と同様な傾向が得られた。
社内その他部門についても相当数の回答があったが、部門名を記載させるアンケート形式にしなかったため内容は不明である。

なお、前回は「その他」に社内・社外の区分を行っていなかったため、上記の一覧では便宜上括弧をつけて記載している。

教育・社内ルール

57. 問56の教育担当者の情報セキュリティに関するレベルを、問56で選択した部門それぞれについてお答え下さい

レベル低	1	2	3	4	5	6	7	8	9	10	レベル高



グラフ中の数値は回答した組織数

有効回答数	セキュリティ	総務部門	情シス管理	企画部門	事業部門	情シス開発	社外
468	136	75	51	27	22	20	15
平均	7.6	6.3	7.5	7.1	6.9	7.2	8.9

リスク管理	コンプライアンス	監査部門	事推部門	社長室	社内その他
15	12	10	8	7	70
8.2	7.3	8.0	6.8	7.9	6.9

今回新規設問。

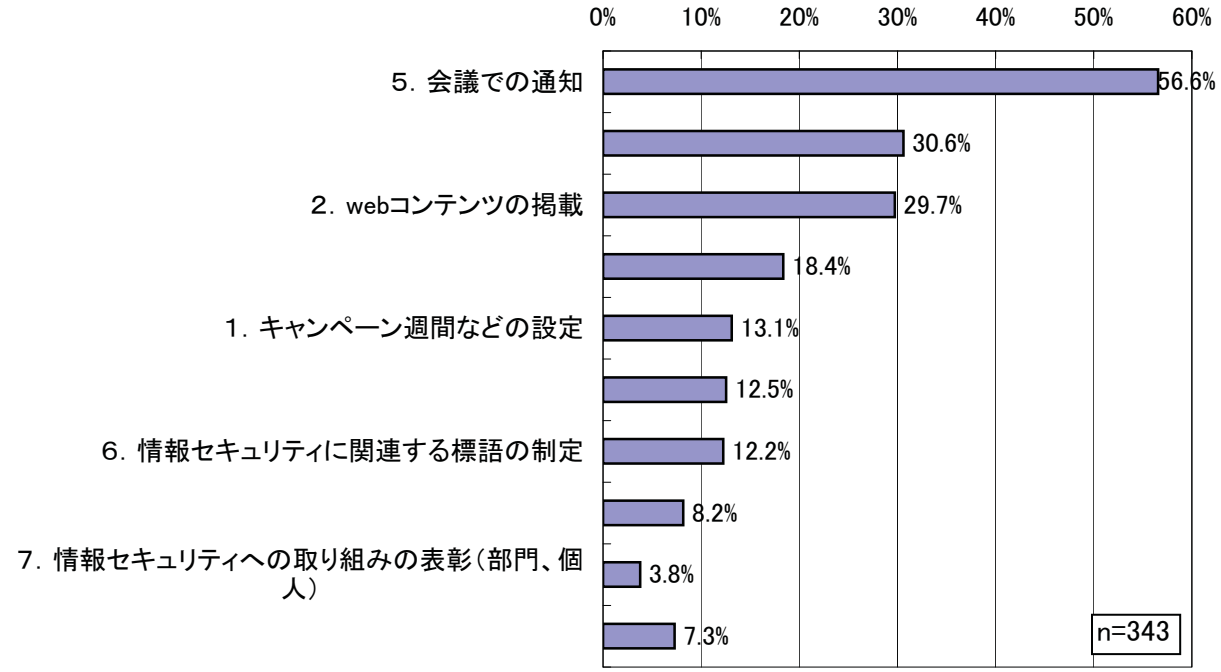
情報システム部門を中心に概ね7点以上、また社外に依頼する場合は半数以上が10点とするなど、講師側の情報セキュリティに関するレベルは高いと考えられる。しかし1～3点といった否定的とも取れる判断も数件ではあるが存在しており、教育自体の意義が問われる。

なお本問につき問56との有効回答数の差分は、教育担当組織の記載はあったがレベルまでは記載されていなかったケースである。

教育・社内ルール

58. 教育以外の啓発活動がある場合はお答え下さい（複数選択可）

1：キャンペーン週間などの設定
2：webコンテンツの掲載
3：ポスターの掲示
4：ニュースレター・メルマガの発行
5：会議での通知
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（記入欄あり）



	有効回答数	5．会議	3．ポスター	2．web	9．特になし	1．キャンペーン	4．メルマガ	6．標語
今回	660	194	105	102	63	45	43	42
		56.6%	30.6%	29.7%	18.4%	13.1%	12.5%	12.2%
前回	330	―	86	―	93	17	38	29
		―	32.6%	―	35.2%	6.4%	14.4%	11.0%

8．ノベルティ	7．表彰	10．その他
28	13	25
8.2%	3.8%	7.3%
15	5	47
5.7%	1.9%	17.8%

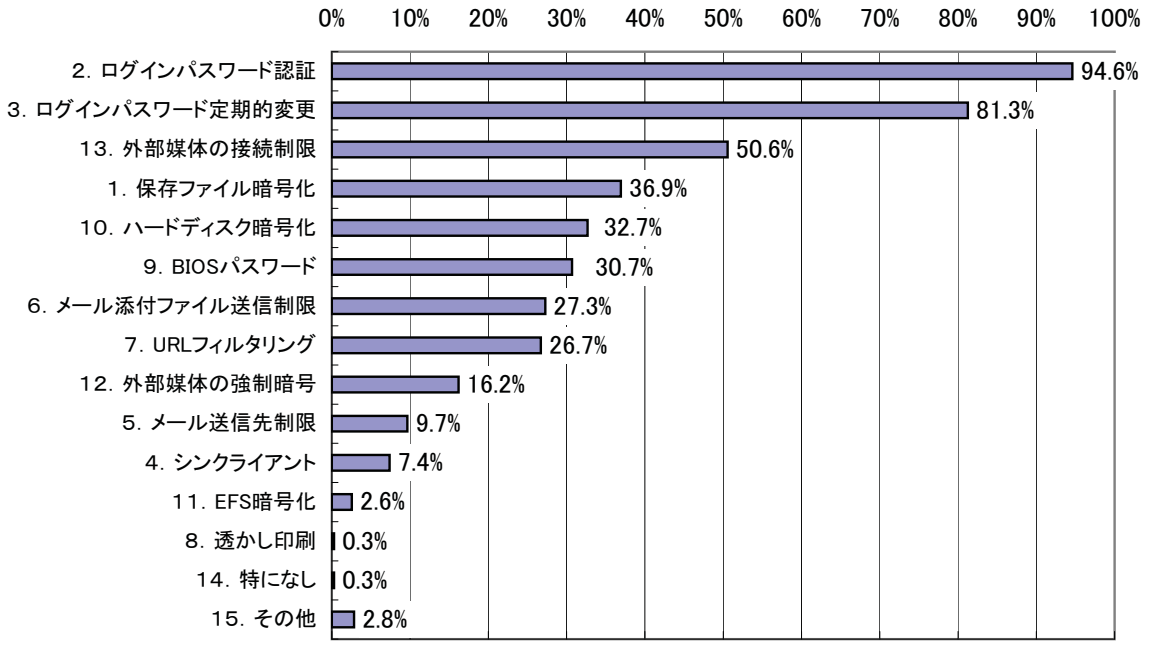
その他詳細
メール発信（6件）
テスト実施（2件）
定期チェック（4件）
各種フォーラムへの参加（2件）
社内報、掲示で通知（3件）
他（8件）

今回選択肢として追加した「会議での通知」に多数の回答が寄せられている。会議において上位からセキュリティに関する講話などが行われ、それに加えてwebやポスターなどによる通知が行われているものと考えられる。

啓発に関してはあまり費用はかけない傾向が見られる。

59. 業務用PC からの情報漏洩対策として実施している対策をお答えください。(複数選択可)

1. 保存ファイルの暗号化
2. ログインパスワード認証
3. ログインパスワードの定期的変更
4. シンクライアント
5. メールの送信先制限
6. メールの添付ファイル送信制限
7. URL フィルタリング
8. 透かし印刷
9. BIOS パスワードの設定
10. ハードディスク暗号化
11. EFS 暗号化(Windows)
12. 外部媒体のデータ移動時強制暗号
13. 外部媒体の接続制限
14. 特になし
15. その他(記入欄あり)



(単位:社数・%)

n=351

有効回答数	1. 保存ファイル暗号化	2. ログインパスワード認証	3. ログインパスワード定期的変更	4. シンクライアント	5. メール送信先制限	6. 添付ファイル送信制限
352	130	333	286	26	34	96
100.0%	36.9%	94.6%	81.3%	7.4%	9.7%	27.3%

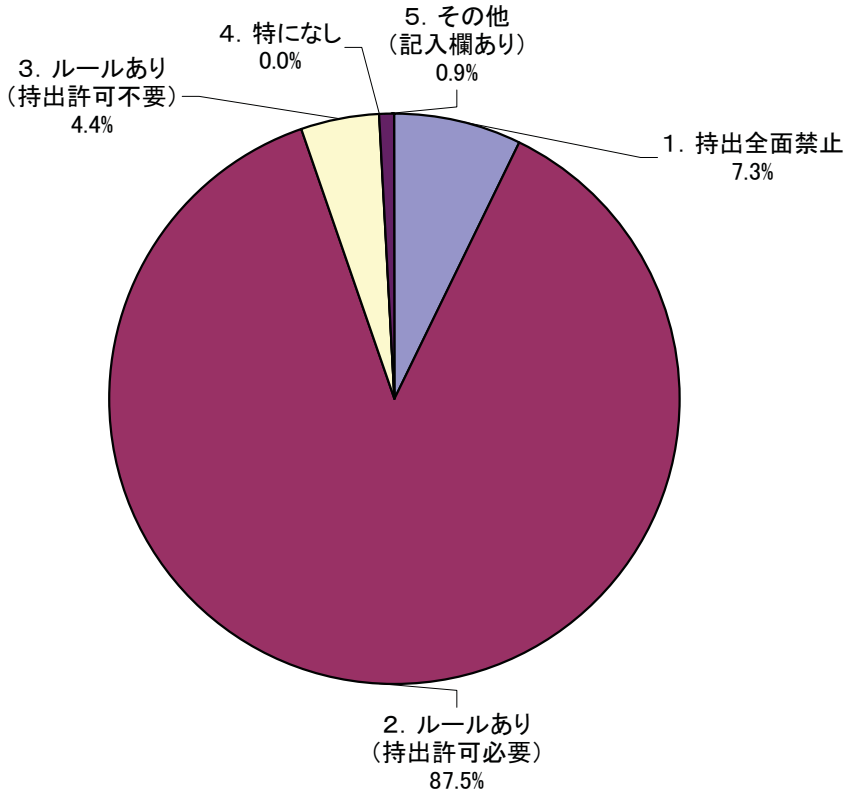
7. URLフィルタリング	8. 透かし印刷	9. BIOSパスワード	10. ハードディスク暗号化	11. EFS暗号化	12. 外部媒体の強制暗号
94	1	108	115	9	57
26.7%	0.3%	30.7%	32.7%	2.6%	16.2%

13. 外部媒体の接続制限	14. 特になし	15. その他
178	1	10
50.6%	0.3%	2.8%

その他詳細
持出禁止(1件)
監視ソフトの導入(1件)
ユーザーIDの極小化(1件)
ローカルに極力データを残さない(3件)
機密レベル毎に項目6, 9, 10を実施(1件)
未回答(3件)

「ログインパスワード認証」、「ログインパスワードの定期的な変更」については、大多数の企業が実施していることが分かった。また、「外部媒体の接続制限」は約半数の企業が実施しているが、「外部媒体のデータ移動時強制暗号」は16%にとどまっていることから、外部媒体のリスクは認識しているもののコストが必要となる対策はあまり進んでいないことがわかる。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割の企業が対策している。

60. 以下の情報資産を社外持出する際のルールをお答えください。(択一)
【PC持出について】
1. 持出全面禁止
2. ルールあり(持出許可必要)
3. ルールあり(持出許可不要)
4. 特になし
5. その他(記入欄あり)



(単位:社数・%)

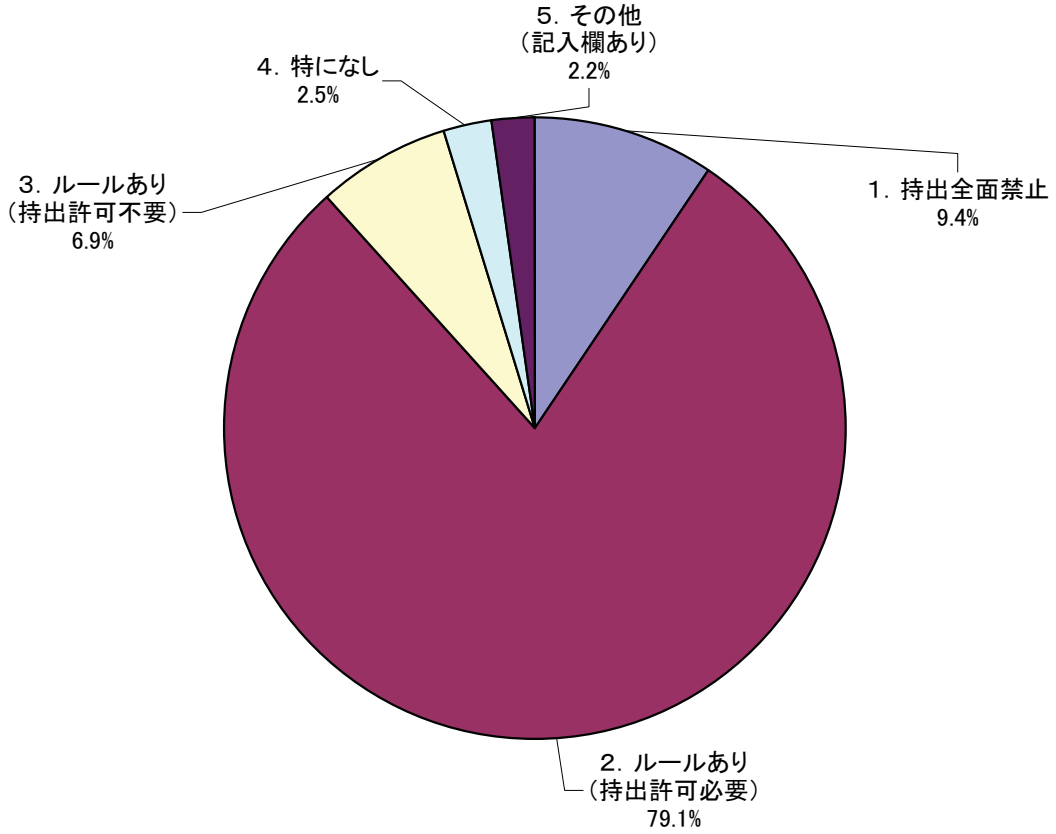
n=343

有効回答数	1. 持出全面禁止	2. ルールあり(持出許可必要)	3. ルールあり(持出許可不要)	4. 特になし	5. その他(記入欄あり)
343	25	300	15	0	3
100.0%	7.3%	87.5%	4.4%	0.0%	0.9%

その他詳細
持出用は常時暗号化(1件)
PCに機密情報を入れたら持出許可必要(1件)
PCは配備しない(1件)

「ルールあり(持出許可必要)」としている企業が大多数を占めており、ルールを定めていない企業は無かった。
このことから、社外持出する際のルールを定めているが、社外持出を全面禁止している企業は少数派であると考えられる。

60. 以下の情報資産を社外持出する際のルールをお答えください。(択一)
【外部媒体持出について】
1. 持出全面禁止
2. ルールあり(持出許可必要)
3. ルールあり(持出許可不要)
4. 特になし
5. その他(記入欄あり)



(単位:社数・%)

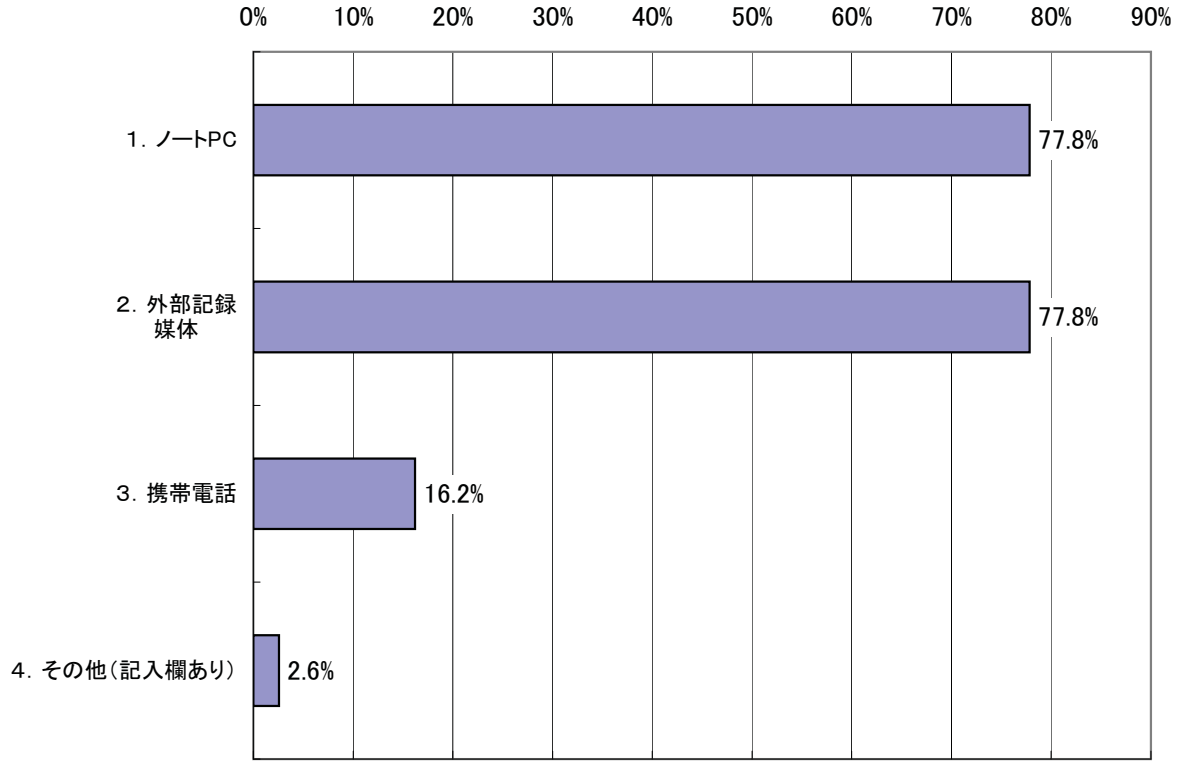
n=277

有効回答数	1. 持出全面禁止	2. ルールあり(持出許可必要)	3. ルールあり(持出許可不要)	4. 特になし	5. その他(記入欄あり)
277	26	219	19	7	6
100.0%	9.4%	79.1%	6.9%	2.5%	2.2%

その他詳細
管理部門が提供したUSBメモリのみ利用可能
暗号化USBメモリのみ利用可能(1件)
機密情報を入れたら持出許可必要(1件)
日をまたぐ場合は、持出許可(1件)
使用禁止(1件)
その他(1件)

「ルールあり(持出許可必要)」としている企業が約8割を占めている。ルールを定めていない企業も7%存在することが分かった。
このことから、社外持出する際のルールを定めているが、社外持出を全面禁止している企業は少数派であると考えられる。

61. 社内持込もしくは利用を制限したものをお答えください。(複数選択可)
1. ノートPC
2. 外部記録媒体
3. 携帯電話
4. その他(記入欄あり)



(単位:社数・%)

n=352

有効回答数	1. ノートPC	2. 外部記録媒体	3. 携帯電話	4. その他(記入欄あり)
352	274	274	57	9
100.0%	77.8%	77.8%	16.2%	2.6%

その他詳細
個人所有のノートPC(5件)
USB接続機器(1件)
カメラ(1件)
特になし(1件)
その他(1件)

ノートPC、外部記録媒体については、約8割の企業が社内持込もしくは利用を制限していることが判明した。
また、携帯電話を制限している企業は少数派であることが考えられる。

付録D　認証取得組織へのインタビュー内容

分野	設問/回答
1.組織概要	出席者の担当業務
	・情報システム管理部門とセキュリティ組織の事務局を兼任 ・ISMS認証取得時の事務局を担当。現在は事務局を離れ、オブザーバ的役割
	事務局の構成
	・出席者他2名 ・4名構成
	セキュリティ委員会の構成
	・CISOは、情報システム関連を管掌する役員（常務）。他に部門長で構成 ・委員会のトップは、社長代行。委員会は、2～3ヶ月に1回程度開催
2.認証取得	認証範囲の概要
	・本社及びグループ会社2社 ・当初は全社。徐々に縮小傾向。適用範囲の中心はコールセンター
	取得からの年数
	・2005年認証取得、2008年更新審査受審
	認証取得の背景，動機
	・経営陣からの指示。Pマークも検討したが、業務形態を考慮してISMSを選択 ・顧客情報保護の重要性を考え、Pマークも検討したが、上層部の判断でISMSを選択
	認証取得の効果
	・顧客や取引先に評価してもらえる ・社内文書や連絡体制が整備された
	継続の課題
	・業務効率とセキュリティ対策のトレードオフ ・対策の費用対効果 ・（一般論として）認証取得自体の目的化への傾向を危惧している ・PDCAのうちAを実行するのが困難 ・審査員の指摘が「～望ましい」という表現になっており、現場の改善行動につながらない
	内部統制、J-SOXなどの取組みはISMS活動に影響したか
	・J-SOXの影響はなかった
	力を入れているところはあるか
	・セキュリティは最終的には「人」であるため教育が重要 ・PDCAのCをしっかりやっている
	認証範囲外組織の社内別部門からの理解は得られているか
	・認証範囲外組織も、セキュリティ対策には取組んでいる ・窓口となるメンバーに対して、シミュレーション形式での教育を行うことで、セキュリティ意識の徹底、不明時の相談等の連絡体制を周知している ・各部署にエリア責任者（課長クラス）を配置 ・現場にはまだ浸透しきれていないが、継続が必要
	新たなセキュリティ対策の導入などにおいて、マネジメントシステムのトップである経営陣の理解は得られているか
	・CISOの知識が深く、常に的確な指示がある
3.コンサルタント	コンサルタントを使用したか
	・適宜スポットで相談、支援を受けている ・人からの紹介を採用 ・毎年利用している
4.審査制度	審査員、審査機関の対応には満足しているか
	・大きな不満はない。但し、審査員と事務局の間で、適用宣言書の解釈の違いが生じたことがあった ・予備審査の受診により課題が明らかになり、適用範囲の拡大審査がスムーズに行えた ・指摘事項や審査内容の不満はない

付録D　認証取得組織へのインタビュー内容

分野	設問	A組織	B組織
1.組織概要	出席者の担当業務	情報システム管理部門、セキュリティ組織の事務局を兼任	2005年7月にISMSを取得した際の事務局を担当。 現在、事務局は別の部署が担当しているが、出席者はISMS審査員補の資格があり、オブザーバ的役割を担っている
	事務局の構成	事務局は、出席者他2名　（認証取得当時の担当者は退社したが引継ぎが適切に実施された）	4名構成
	セキュリティ委員会の構成	情報システム関連を管掌する役員（常務）をCISOとして部門長で構成	委員会は、2～3ヶ月に1回程度開催。委員会のトップは、社長代行
2.認証取得	認証範囲の概要	認証範囲は、以下のとおり ・本社管理本部、情報通信管理部 ・子会社A（ISP事業を担当） ・子会社B（コールセンター業務を担当） 社員は、本社で採用され、各子会社に配属される形態をとる	2005年7月当初は全社で取得、500人規模。 その後、徐々に範囲を縮小。 本社にコールセンターがあり、そちらが適用範囲の中心。 企画部門は、徐々に範囲から外す方向
	取得からの年数	－	2005年7月に取得、2008年に更新審査を受けた
	認証取得の背景，動機	経営陣からの指示。 Yahoo等の情報漏えい事件をきっかけとして、セキュリティ対策の必要性を認識してISMS認証取得に取組む。 Pマークも検討したが、より業務形態に合致する認証としてISMSを選択	顧客情報の保護が必要と考え、Pマークも検討したが、上層部の判断でISMSを選択
	認証取得の効果	通り一遍の教育ではなく、具体的な行動につなげることの出来る教育手法として、事例やシミュレーションを採用。 （例）「USBメモリ内のデータを社内システムに読み込む」というオペレーションの是非を考えてもらうため、実際にメモリを手渡して、「どうするのが正しいか」などを問いかけるようなカリキュラムを考案	顧客や取引先（特に大手）に「ISMS認証を取得しています」と説明すると、評価してもらえる。 社内における各種手順や連絡体制が整備された
	継続の課題	業務効率とセキュリティ対策のトレードオフ。 厳密な管理が、業務効率の低下に影響することがないか。 コールセンターの効率化など、ITILなども意識した運用を考えながら、対策への投資対効果について検討していきたい	一般的に、認証取得自体が目的化している傾向を感じているが、取得後にPDCAを回していくことこそが大事なのではないか。 自らの経験としては、PDCAのA(改善)を実行するのが難しい。 審査員から指摘もあるが、審査員は「～するのが望ましい」というだけなので、現場では「気をつけます」ということで終わってしまう。改善行動につながらない。 また、P（リスクアセスメント）が弱いと感じている。リスクアセスメントはかなり大変で、負荷になっている。 年ごとに資産価値が変わるはずだが、現場では昨年と同じ対応をしている
	内部統制、J-SOXなどの取組みはISMS活動に影響したか	－	J-SOX法の影響はない。規程の見直しなどは発生するが、ISMSと関係するものではなかった。 IT導入が内部統制とイコールではないと考えている。トップが悪いことができないように委員会を組織するというのが、本来のSOX法の主旨ではないか
	力を入れているところはあるか	最終的にはセキュリティは「人」だと考えるので、教育はしっかりやっていきたいと考えている	PDCAのC（チェック）は、他社と比較してもかなりできていると考えている。 教育は、内部の社員が行っている。 リスクアセスメントにマジックポリシーを利用しており、その保守に約30万円ほどかかるが、その他の費用はあまりかけていない
	認証範囲外組織の社内別部門からの理解は得られているか	認証範囲外の組織であっても、セキュリティ対策には適宜取り組んでいる。 範囲外であっても、より機微な情報を取り扱う組織もある。 範囲外組織に対しても窓口となるメンバーに対して、シミュレーション形式で具体的な教育を行うことで、セキュリティ意識の徹底と、不明時の相談などの連絡体制を周知させることができているのではないかと感じている。（例）セキュリティ委員が各部門を訪問して、機密書類の保管を目の前で実践するなど	各部署にエリア責任者（課長クラス）を配置している リスクアセスメントを、現場にやらせている。部署のことは、自分達が一番良く知っているはずなので 現場にはまだまだ浸透していないが、言い続けていくことが必要と考えている
	新たなセキュリティ対策の導入などにおいて、マネジメントシステムのトップである経営陣の理解は得られているか	CISOは、情報システム全般に関する知識が深いため、新しい技術の採用について相談をすると、投資対効果や自社の業態などを鑑み時期などについて常に的確な指示がある	－
3.コンサルタント	コンサルタントを使用したか	構築、認証取得ならびに継続運用について適宜スポットで相談、支援を受けている	コンサルタントは、人からの紹介を採用。 認証取得、継続運用について毎年利用している。 金額については、最初にコンサル担当を利用する場合、どのくらいが妥当な金額なのかわからない
4.審査制度	審査員、審査機関の対応には満足しているか	審査では、直接的なコンサルティングをされることはない。一般論として、他社対策の例などを紹介されることはある。 指摘事項や審査内容に関する大きな不満はないが、適用宣言書の中の「電子商取引」業務を実施業務として適用することについての解釈の違いは発生したことがある。しかし、特段の不満ではない。 拡大審査の際など、事前に予備審査を受審し、指摘をされたことで、範囲の拡大に関する課題を明らかにすることができ、認証範囲の拡大をスムーズに行うことができた	指摘事項や審査内容に関する不満はない。意見に納得できないことはあるが、事務局側の対応にも問題があるかもしれない。 今年、理由もなく契約金額が上がったが、別会社に変える動きは特にない。 昨年の更新時には、金額が100万円を超えた。 133の管理策について、毎年資産が変われば、適用宣言書も毎年変わると思うが、審査員はそこまで確認しない。例えば、対象部署がなくなったとしても、チェックしない。これでよいのか疑問

付録E　認証機関へのインタビュー内容

分野	設問/回答
1. 認証機関	審査を行う上で得意な業種はあるか
	・ある。IT関連産業になじみ深い。 ・不得意分野はなくすよう努力している。
	幅広い業種の場合、どのようにして組織の概要を把握するのか
	・事前の調査票記入、web等の公開情報確認 ・NACEコード、独自コードの運用による
	審査機関はISMS認証の普及を目的としているか
	・目的としている。ISMSの推進を行っている。 ・目的とはしない。ISMSは「社会財」としてとらえる必要があり、件数は問題ではない
	判定委員会の構成
	・全て内部（ベテラン含む） ・過半数が外部
2. 審査員	審査員としての資質とは何か
	・コミュニケーション力が最も重要 ・スキルは最低限、向上心や好奇心、経験も重要
	審査員教育はどのようにして行うか
	・OJT、全国合同回儀、グループ討議の実施、QMSとの連携勉強会、外部講師による最新IT技術研修等
	審査員の力量を測定する指標はあるか
	・一般的な資格に加え、定例会議への参加、審査時の実地確認、クラス分けの実施等
	審査員のレベル、判断の差について
	・同じ項目を指摘で厳しく判断することはあるが、その内容は社内で共有している。
	審査員の外部人材活用
	・社員と同様の研修の後、活用している。
3. 審査時の対応	審査に対するクレームはあるか
	・審査員の意見の強要、聞く耳を持たないとの指摘あり ・経営陣前での指摘がクレームとなるケースもある。
	コンサル的な指摘を求められることがあるか。またその場合はどう答えるか。
	・あまりそのような希望はない。 ・解決法は投げず、着地点のすり合わせなどを行う。
4. 受審側の対応	受審側に望む姿勢とは
	・ありのままを見せてほしい、認証機関には守秘義務がある。 ・考え方が異なる場合は顧客になりえない。
	審査時のその場しのぎ対応はあるか
	・つじつまのあわないケースは見られる。
	有効性の評価について、具体的にどう考えるか
	・どこが改善につながるかを計れる数値を出すのが重要 ・認証機関として明言することはできない ・施策実施率などはひとつの尺度に過ぎず、全てを判断するのは困難。管理策・マネジメントの双方ともに永遠の課題。
5. 付加価値のある審査	付加価値のある審査とは
	・本人たちが見つけられない問題を見つけ出すこと。 ・業務のパフォーマンスが上がっていないところを受審側が気づくこと。 ・付加価値が認証取得組織によって異なるため、一概には言えない。
6. 今後の動向	貴機関におけるISMS認証取得の割合
	・いずれも10%以下
	不況の影響は受けているか
	・QMSやEMSほどの影響はない。 ・いずれ頭打ちとなる
	ISMSの今後の動向
	・取得企業が増えることを期待するが、IT産業以外では取得は少ない。 ・世界的に考えれば、必ずしも認証取得は必要ない。 ・コンサルタントの役割が重要である。
	ISMS全体について
	・ISMS認証取得が目的になってはいけない。また重過ぎるマネジメントシステムは会社にとって負担となるだけ。 ・審査員のビジネスモデルができていないことから馴れ合いの審査となり、自己が起きる。受審側がどう考えるかが重要。
7. その他	認証取得の適正規模
	・小さい組織から広げるケースが多い。身の丈にあったISMSを運用してほしい。
	Pマークとの関連
	・ISMSに比べて「安く早く」といった風潮がある。認証機関は、正しく情報を伝える必要がある。
	ISO/IEC27006・17021について
	・特に意識する必要はない。 ・17021は認証機関の「よくない」事例が書かれているので、参考になる。 ・27001は現実とかけなはれている場合がある。どう圧かを考慮する必要がある。

付録E　認証機関へのインタビュー内容

分野	設問	A機関	B機関	C機関
1. 認証機関	審査を行う上で得意な業種はあるか	ISMS審査員にはIT産業経験者が多いため、ITに馴染み深い。	全ての分野を担当した訳ではないが、不得意領域をなくすよう努力している。	サービス業が多いQMS登録者からISMSを取得させているため、結果としてサービス業が多いことはあり得る。
	幅広い業種の場合、どのようにして組織の概要を把握するのか	事前の調査票への記入、およびNACEコードを参考とする。	事前の調査票への記入、認証取得希望組織への訪問、NACEコードに加え、独自のコードを利用する。	独自のコード体系と経験を重視し、審査員を配置する。
	審査機関はISMS認証の普及を目的としているか	目的としている。普及活動はあるが、少ない。	ITは変化の激しいため、目的とはしない。ISOを利用してレベルを上げ、規格を返上して自分でマネジメントするのでも構わない。ISMSをツールとして取り入れて、セキュリティが向上すれば良いと考える	ISMSは「社会財」である必要があり、件数をやみくもに増やせばいいというものではない。
	判定委員会の構成	資格のあるベテランのパートナーを含め、3名で構成される。	過半数を内部メンバで構成	内部1名，外部4名
2. 審査員	審査員としての資質とは何か	日常の業務の進め方からも、コミュニケーション力を重視する。	公平性を含んだスキルは最低限であり、向上心、好奇心ではないかと考える。ISMSの様々なケースを審査しつつ、経験を積む必要がある。	―
	審査員教育はどのようにして行うか	審査員をクラス分けし、最下位審査員は最上位審査員からOJTで指導を受ける。また、年に5回の審査上の問題点を情報共有する勉強会、グループ討議の場を設けている。 技術教育は外部のセキュリティ専門家に依頼している。 教育については、ベテランと新人を一緒に組ませ、互いに啓発させている。	年に30時間の講習を行い、さらに隔月で別の教育を行う。また外部から講師を呼びセキュリティの技術と知識の乖離を埋める努力をしている。それらは文書化して情報共有を行っている。	審査員技術会議や他のマネジメントシステム関連の会議もあり、通算で年間10回程度の会議が行われている。内容としてはISO27006の理解、不具合事例の検証などを行っている。
	審査員の力量を測定する指標はあるか	品質審査員資格を持っていることと、2ヶ月に1回の審査委員会議への出席。 暫定審査委員時にはさらに厳密な指標がある。	基本的な資格に加え、ISMS審査の履歴や教育の履歴を自動的に記録する社内システムを用い、自動的に各個人の力量テーブルを作成、共有している。	基本的な資格に加え、組織内でさらに細分化したクラス分けを行っている。技術会議などを通じて彼らの技術は収斂していく。
	審査員のレベル、判断の差について	―	同様な指摘において、規格の解釈などでのブレはないと考えている。ただし、一見異なった指摘でも内容は同じ(例えば認証パスワードの設定レベルの差)であるケースは想定される。こうした指摘内容について、社内で共有している。	―
	審査員の外部人材活用	―	外部の人材に審査に加わってもらう場合は、2か月に1回の研修への参加などを条件としている。	―
3. 審査時の対応	審査に対するクレームはあるか	ある。審査員が意見を強要した、話をいっさい聞かなかった、というクレームが出ることもある。あるいは審査員が、経験に基づき前の会社の事例を言うことがあるかもしれない。	ある。相性があわない場合は何でもクレーム扱いされてしまう。また、規格の解釈を間違うケースもあり、それを経営陣の前で指摘すればクレームとなる。	ある。審査後のアンケートによるフィードバックでいろいろと意見を得ている。
	コンサル的な指摘を求められる場合はどう答えるか	そのような希望はあまりない。ISMSはコンサル等に指導してもらい、審査機関を選ぶのは最後の取得審査の段階だと思われる	―	コンサルは行わないが面倒は見る必要があると考える。受審組織には脆弱性に気づき、直してほしい。規格が問題ではなく、どのように説明するかが問題である。ISMSは認証組織と受審組織のコミュニケーションが重要である。
4. 受審側の対応	受審側に望む姿勢とは	事前の整理は必要なく、ありのままを見せて欲しいという。意識的に隠されてしまうと、本来の審査にならない。改善指摘事項は嫌がることはないし、指摘がないと審査員の力量を疑われるケースもある。認証を維持することは目的ではなく、改善することが重要。要は、経営者がどう考えるかによるようだ。気付きを得てもらえると審査する側としても嬉しい。	我々には守秘義務があるので、情報開示をしてほしいが、強制力はない。よって、受審企業に断られたらそれ以上は求めない。	ISO17021の記載内容をベースに考慮している。事前に審査時の要求事項を基本ガイドとして配布している。考え方が違っていると、そもそも顧客にはなり得ない。
	審査時のその場しのぎ対応はあるか	―	監査すればすぐにわかる。ただし日銀のように抜き打ち検査はできない。不適合が多いと彼ら自身の評価につながる。本人の思いもくみ取る必要がある。	つじつまの合わないこと、あるいはコンサルタントに丸投げしていることが見受けられる。コンサルタントと受審組織、認証組織は適正に三位一体である必要がある。
	有効性の評価について、具体的にどう考えるか	大事なのは事故0件のために、何をするかである。会議を行うにしても、その数のどこが改善につながるのかを測定できる数値を出すことが重要。 型にはめることを目標としている会社も多いが、その会社によって目的は異なるので慎重に考えるべき。審査員のコメントに自社の意識を加味する必要がある。	審査に通るのはあくまでも出発点であり、それをどう経営に結びつけるかが問題である。審査機関としての具体的なが有効性の評価についてのコメントは避ける。	ISMSの難しさは、規格そのものが（組織によって異なるため）目標を明確に定めていない。それらの施策実施率はひとつの尺度に過ぎない。当団体では「やっているかやっていないか」でまず判断する。組織の大きさにもよるが、有効性の評価は永遠の課題であると考える。
5. 付加価値のある審査	付加価値のある審査とは	価値も会社によってそれぞれ違うため、一概には言えない。 ユーザが何をすればよいかが現場でわかるように伝えることが大事。業務のパフォーマンスが上がっていないのはどこか？ということを受審側が気付くような審査を目指している。また、ユーザが気付かない場合には、再度、別の表現で伝えている。	当該組織が見つけられない問題を見つけること、また、期待されている効果を出せるよう指摘をすることが重視する。セキュリティマネジメントの場合、経営にどう直結するのかが見えにくい。限られた予算の中でどうIT投資を節約するのか、その手がかりを示す必要性、時代の要請も考慮する必要性がある。経営者が持っている期待にこたえることが大事である。	年に1度審査を行っただけで、規格適合性をすり合わせてなにをアウトプットとできるか、脆弱性を明確にできるか、経営にどの程度役立てるかを明示することは困難である。付加価値が認証組織の目的によって異なるため、一概には言えないと思われる

分野	設問	A機関	B機関	C機関
6. 今後の動向	貴団体におけるISMS認証取得の割合	JIPDECのwebでは3000件を超えたようだが、5000件で頭打ちとなると思われる。	10%以下。	10%程度で頭打ちの可能性もある。
	不況の影響は受けているか	ISO自体が各企業で経費削減の対象になった。ただし、EMSなどは、認証取得しなくても実施的に行うようになってきている。ISMSは、QMS・EMSほど影響は受けていない。	―	ある程度IT関連の組織にISMSが回ったため、落ち着いてきたと見られる
	ISMSの今後の動向	内部統制とのかかわりで、情報セキュリティに移行してくるのではないかと考えている。取得企業が増えることを期待しているが、IT産業以外の一般の会社の取得が少ない。	現在は増加傾向、今後も地方を中心に拡大すると思われる。	ISMS認証取得に携わるコンサルタントには同じ方向を見てほしい。ISMS認証を取得することはメリットではない。取得する目的を明確にしないと却って重荷になってしまう。そのためにも、認証取得組織・認証機関・コンサルタントの三位一体の考え方が必要である。ただし、マーケットとしては大きいに越したことはない。
	ISMS全体について	身の丈に合ったISMSを運用して欲しい。重すぎるマネジメントは、会社にとって負担になるだけである。ISMS認証取得は目的とするべきではない。	日本では英国に比べ審査員のビジネスモデルができていない。慣れ合いの監査をするからISMS取得企業で事故が起こる。今後、受審企業が増えると安かろう悪かろうの風潮が広がらないかと危惧している。だが、結局、そうなってしまうかどうかは受審企業がどう考えるかにかかっていると考える。	―
7. その他	認証取得の適正規模	Pマークのように全社でというしばりはないので、小さな組織から取得して拡大していくという会社が多い。そういう意味から、最初に経営者の意志は最初に確認している。	―	―
	Pマークとの関連	―	―	2006年度版（ISO15001）が公布されて以降、Pマーク自体が取引条件に含まれたケースが多い。ISMSに比べて「安く早く」といった風潮は好ましいものとは言えず、認証機関は新規顧客を中心に正しく情報を伝える必要があると考える。ISMSは社会財であるという考え方に従うと、ISMSはビジネスとしてとらえるべきではない。審査時には目先の利益だけにとらわれず、長期的にどの審査機関を使うか判断すべき。その意味で、受審組織にも責任はあると考える。
	ISO/IEC27006・17021について	受審側は、手順およびチェックリストを確認すればよい。	苦情やクレームの要件は27001にはないが、それは仕組みの問題なので受審企業に問題はない。 27001はすべてカバーしているわけではなく、現状とかけ離れている項目はある。やりにくいというよりはどう扱うかということが重要である。	同規格の顧客への要求事項は徐々に強くなっている。特にISO17021にはその「よくない」例について書かれているので参考とされたい。

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）

ＵＲＬ：www.nmda.or.jp