平成 22 年度ニューメディアを基礎とする調査研究事業

ISMS 第三者認証制度をより有効なものにするための
ＩＳＭＳ 認証事業所調査
調　査　報　告　書

平成２３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。
http://ringring-keirin.jp

～ 目　　次 ～

１．はじめに 1
２．アンケート調査の内容 2
３．アンケート調査について 4
３．１　ISMS 認証取得事業所向けアンケートの概要 4
（１）　アンケート期間 4
（２）　アンケート調査対象 4
（３）　有効回答数 4
（４）　回答形式 4
（５）　結果の取扱い 4
（６）　アンケートの特徴 5
３．２　ISMS 認証取得事業所インタビューの概要 5
（１）　インタビュー実施日 5
（２）　インタビュー対象 5
（３）　回答形式 5
（４）　結果の取扱い 5
（５）　インタビューの特徴 6
４．総合的な考察 7
４．１　回答事業所組織の基本情報 7
（１）　ISMS 認証取得事業所の規模 7
（２）　ISMS 認証取得業種 7
（３）　アンケート回答者の所属部門と役職 7
４．２　ISMS 認証取得に関するもの 8
（１）　ISMS 認証取得年月 8
（２）　ISMS 認証取得事業所の従業員数 8
（３）　他の認証取得状況と取得年月 8
（４）　ISMS 認証の取得目的 9
（５）　認証取得の発案者 9
（６）　ISMS 認証の運用責任者は？ 9
（７）　認証取得後に認証範囲の変更／変更の検討 9
４．３　ISMS 認証の効果・影響について 9
（１）　ISMS 認証取得で得られた効果は？ 9
（２）　ISMS 認証取得での想定外の影響は？ 9
（３）　ISMS 認証後の運用上の負担と重点的な取組み 10
（４）　実業務と ISMS の乖離 10

（５）　ISMS 維持費用について 10
４．４　ISMS 認証に関連する体制等について 11
（１）　ISO27002 をどこまで取り入れたか 11
（２）　ISMS 事務局 11
４．５　コンサルタントについて 11
（１）　コンサルタントを利用について 11
（２）　コンサルタントの各種理解度 11
４．６　ISMS 認証審査及び審査員について 13
４．７　内部監査、マネジメントレビューについて 13
（１）　内部監査の実施頻度（除、自己点検） 13
（２）　内部監査体制について 14
（３）　指摘事項は改善されていますか？ 14
（４）　マネジメントレビューの実施頻度と形態 14
４．８　教育について 14
（１）　教育方法について 14
（２）　社員への ISMS の教育頻度について 15
（３）　ISMS 教育の担当部門とレベル 15
（４）　教育以外に行っている啓発活動について 15
（５）　教育以外に行っている啓発活動について 15
４．９　社内ルール等について 16
（１）　情報漏えい対策について 16
（２）　可搬媒体（①ノート PC、②外部記録媒体）の社外に持出ルール 16
（３）　社内持込や利用制限機器について 16
（４）　コンピュータウイルス感染の有無と感染原因 16
４．１０　自由回答欄について 17
４．１１　アンケートから見えてくるもの 18
４．１２　インタビューから見えてくるもの 19
（１）　ISMS 推進担当者と経営層の理解 19
（２）　コンサルタント、審査機関・審査員について 19
５．ISMS 認証制度の実効性向上のための提案 21
５．１　ISMS 制度の見直し 21
５．２　コンサルタントの評価制度について 22
５．３　監査概念について 22
５．４　認証機関、審査員の質的向上 23
５．５　教育、普及啓発について 23
６．　謝辞 26

付録Ａ　アンケート調査配布資料 27
　１．アンケートご協力のお願い 27
　２．アンケート質問用紙 28
　３．アンケート回答用紙 32
付録Ｂ　アンケート結果のまとめ 35
付録Ｃ．ISMS 認証取得組織へのインタビュー 101
付録Ｄ．自由意見欄について 107

１．はじめに

８ヶ月のパイロット期間を経て、2002 年 4 月より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 月からは、ISO/IEC 27001/27002 の日本語版である JISQ27001/27002 を適用することになった。　2010 年末には、(財)情報処理開発協会への登録が 3,744 件、(公益財）日本適合性認定協会への登録が 778 件あり、合計 4,522 事業所[1]が認証取得している。

世界における ISMS 認証取得事業所数の半分以上[2]を日本が占めており、傑出して登録件数になっている。しかしながら、取得後に業務負荷が増大した、末端まで ISMS の考えが浸透していないと言う声だけでなく、ISMS 認証取得を維持するために、二重帳簿的な対応をしていると言った声まで聞こえてくる。　このような認証制度の課題については、他の認証制度、ISO9001（品質マネジメントシステム、QMS）でも、指摘[3]されてきた。

また、審査員の指摘が必ずしも認証取得事業所に対して適切でない、あるいは、審査員毎に異なるケースに悩まされているケースもある。　更に、審査費用が高いとの不満もある。

前 2 回の調査では、ISMS 認証取得事業所全てにアンケートを送付し、回答も求めたが、今回は認証取得の古い順に 2,000 社を選択し、アンケートを送付した。　この 2,000 社は、2008 年 10 月までに ISMS 認証を取得した事業所で、ISMS 取得後、2 年以上経過しており、情報セキュリティマネジメントシステムの定着化が、前 2 回の調査より、進んでいるかについてもみていきたい。

今回の調査結果が、ISMS 認証取得事業所や認証機関、認定機関等、ISMS 認証制度に関係する人たちだけでなく、他の認証制度に対しても有用なものになると考えている。

---

[1] ISMS 認証制度では、場所、特性等により、企業・団体で複数の ISMS 認証を取得できる。このため、本社、事業部、データセンター等での取得が可能であるため、件数を数える場合、「事業所」とした。

[2] 全世界で 7,058 事業所の内、日本は 3,720 事業所で、全体の約 53%を占めている。（International Register of ISMS Certificates の 2010 年 12 月の調査。 国内での登録件数とは異なる件数になっている）http://www.iso27001certificates.com/

[3] 日経コンストラクション「ISO を入札要件から外す」日経 BP 社 2004 年 6 月 11 日号　QMS の課題、特に官庁等の入札要件の問題点を韓国での事例等を含めて解説している

2. アンケート調査の内容

今回の調査では、予算等の制約もあり、ISMS 認証取得事業所の全てに対する調査を断念し、2,000 社に絞ってアンケートを送付した。

（財）日本情報処理開発協会の ISMS 適合性評価制度に登録されている「ISMS 認証取得組織」に公開されている事業所から、認証取得年月の古い順に、2,000 事業所を抜き出し、郵送による調査を行った（但し、所在地等が非公開になっている事業所は除いた)。

質問項目については、原則、前回（2008 年度）の調査に準じた項目にしたが、追加した項目もある。

主なものとしては、「教育効果の測定（問 60)」、「コンピュータウイルスの感染の有無（問 64)」、「感染原因（問 65)」等がある。

教育効果測定の目的は、本来、教育・訓練を行う場合、教育実施側に対し、教育効果があったかを確認させると共に、受講者に有益なものであるかを測定する必要があると考えている。特に集合教育の場合、複数の受講者に対して、１、２名のインストラクターで行うことが多いが、効果のない教育・訓練は大きな損失になる。

また、ISMS 認証取得に直接関係しないが、コンピュータウイルスに関する質問を追加した。情報セキュリティ分野への取組みが行われているが、インシデントがなかなか減らないとの話やコンピュータウイルス感染被害は、国内外が調査[4] [5] をみても、コンピュータウイルス感染が上位を占めており、その理由はあまり明確でない。このため、感染原因を調べることがインシデント削減にも役立つものと考えた。

以上のように、基本的には前回の調査を踏襲した。調査内容を大幅に変更することは、調査の継続を考えると前回との調査比較が難しくなる可能性もあり、質問項目自体に問題がないかぎり、前回の質問を継続した。新規項目については、前述したような項目を追加した。　このため、今回の質問は 65 項目となったが、１項目で 2 つの内容[6]を聞いている項目もある。

質問は以下のようなグループに分けられ、各グループの質問概要は以下のようになっている。

(1) 事業所、記入者の基礎情報の質問（7 問）

事業所の組織規模（資本金、従業員数)、業種、記入者の所属部門、役職、ISMS 運用での役割、経験年数

---

[4] 鈴木宏幸他「2009 年情報セキュリティ調査から見た日米の比較」日本セキュリティ・マネジメント学会 第 23 回全国大会

[5] Computer Security Institute「2010 / 2011 CSI Computer Crime and Security Survey」http://www.gocsi.com/

[6] 問 60 では、①集合教育と②E-ラーニング、問 62 では、①業務用ノート PC と②業務用外部記録媒体について同一の質問を行っている

(2) ISMS 認証取得に関連する質問（11 問）
ISMS 取得年月、対象従業員数、他の認証取得年月、ISMS 認証取得目的、発案者、運用責任者、取得範囲の変更の有無、ISMS 認証取得による効果、想定外の影響、

(3) ISMS 認証運用に関連する質問（9 問）
ISMS 認証取得後の運用上の負担、ISMS の効果増進のための取組み、ISMS と実務の乖離の有無、維持費用について、ISO27002 の取組み方、経営者のマネジメントレビューへの関与、現在の事務局人数、当初要員の残留率、事務局員の教育等

(4) コンサルタントに関する質問（12 問）
コンサルタントの利用の有無、コンサルタントの理解度、費用の妥当性、コンサルタントの選定重視項目等

(5) ISMS 審査員に関する質問（7 問）
ISMS 審査員の各種理解度、指摘事項の妥当性、審査員に対する重視項目等

(6) ISMS 認証の重要運用項目に関する質問（6 問）
内部監査の実施頻度、体制、指摘事項の改善の有無とその対応、マネジメントレビューの実施頻度、実施形態

(7) 教育・社内ルールに関する質問（8 問）
社員、情報セキュリティ管理者、経営層等への教育方法、社員に対する教育頻度、教育担当部門と各担当部門の情報セキュリティレベル、教育以外の啓発方法、教育（集合、e-ラーニング）の評価方法

(8) その他の質問（5 問）
実施している情報漏えい対策、可搬型ＰＣ・記録媒体の持出ルールの有無、社内持込ルール、コンピュータウイルスの感染の有無と感染原因

郵送によるアンケート調査以外に、前 2 回と同様、回答を頂いた ISMS 認証取得事業所に対して訪問を行って、郵送のアンケート調査を補った。

なお、前回（第 2 回目）では、認証機関に対してアンケート調査を行ったが、今回は実施しなかった。

３．アンケート調査について

３．１　ISMS 認証取得事業所向けアンケートの概要

（1） アンケート期間

アンケート発送　　2010 年 12 月 24 日

アンケート回答締め切り　　2011 年 01 月 31 日

注）アンケートは、2 月 14 日（月）までに返送があった回答を集計した

（2） アンケート調査対象

アンケート発送数　　2,000 事業所

2010 年 11 月時点で、(財) 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ウェブで公表している ISMS 認証取得事業所の内、取得年月が古いものから、2,000 事業所を選んで送付した。　なお、2,000 事業所は、住所が公開されている事業所を選択したため、住所等が非公開の事業所は取得年月日が古くても除き、事業所の ISMS 担当者宛てに送付した。

認証取得時期としては、2008 年 10 月 24 日が最新の取得年月日となっている（10 月 24 日の取得事業所は複数あったため、一部は送付されていない)。

（3） 有効回答数

最終的に回収した件数は、2011 年 2 月 14 日時点で、426 事業所から回答を得た。回答率は 21.3%であった。

実際には、2,000 通の送付の内、70 件が転居等のため、実質の回答率は、22.1%になる。

（4） 回答形式

本調査は、情報セキュリティマネジメントシステムの調査であるが、国内事業所の中には、情報セキュリティに関する調査では、匿名を希望したり、回答を控える傾向が強いと言われている。このため、今回も回答は無記名を原則[7]とした。

（5） 結果の取扱い

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。

[7] ①会社名・団体名、②住所、③記入者の名前、④メールアドレスの４項目についての記入については、匿名も可とした。

（6） アンケートの特徴

アンケート全体の特徴としては、以下のようなものが見られた。

- 回収率の高さ

一般的に情報セキュリティ関係の調査では回収率が低いことが多い。本調査でも、前回は 16.8%（352 事業所）、前々回は 18.6%（264 事業所）であった[8]が、今回は 22.1%（426 事業所）の回答があった。　郵送による情報セキュリティのアンケート調査としては非常に高い回収率であり、調査対象である ISMS 認証取得事業所にとって、本調査内容に対する関心が高いことを示していると思われる。

- 自由意見、記名回答の多さ

本調査は無記名方式となっているが、アンケートには自由記入欄（ISMS 認証の維持・運用での疑問、課題等を自由に記入）を設け、回答内容の確認、インタビュー依頼等のため、連絡先が記入できるようになっている。

アンケートを受領した 1930（送付は 2,000）事業所の内、無回答事業所が 78%近く(1,504 事業所)あったが、回答があった 426 事業所の内、企業名記入は 258 事業所（60.6%）、記入者名記入は 231 名（54.2%）、メールアドレス記入は 198 事業所（46.5%）あった。　回収した 426 事業所の半数が実名でアンケートに回答している。

必ずしも多くの件数ではないが、審査員のレベル・技量や審査のバラツキ(指摘事項が審査員によって異なる）等、ISMS 運用上の課題について記名での指摘もある。

３．２　ISMS 認証取得事業所インタビューの概要

（1）インタビュー実施日

2011 年 3 月 3 日（木）～3 月 7 日（月）の 3 日間

（2）インタビュー対象

認証取得事業所　6 社に対して実施した

（3）回答形式

あらかじめ定めた設問について、インタビューにより回答を得た。

（4）結果の取扱い

各事業所の回答内容は、個別企業名や面談者が特定できないように配慮してまとめた。

---

[8] 前回、2008 年は、発送数 2,096 事業所、回答数 352 事業所、回答率 16.8%であった。
前々回 2006 年は、発送数 1,907 事業所、回答数 264 事業所、回答率 18.6%

（5）インタビューの特徴

認証取得組織の現状について、インタビューによる調査を行った。ISMS 担当者の考え方や認証機関、コンサルタントに対する要望、情報セキュリティインシデント等について、アンケート調査だけでは得られない、貴重な意見が得ることができた。

４．総合的な考察

４．１　回答事業所組織の基本情報

（１）ISMS 認証取得事業所の規模

今回の調査でも「1,000 万円以上 5 億円未満」の企業が、全体の 7 割以上（78.6%）を占めており、この規模の組織が ISMS 認証取得を行う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」の組織は前回より少し減っているが、2 割弱（19.0%）であり、大規模な組織も積極的に ISMS 認証を取得している傾向は変わっていない。

次に、組織の従業員数については、従前の調査と大きな差はない。65.7%の組織が従業員 300 人未満となっている。前回 64.4%、前々回 58.9% と比べ、若干増加している。小規模な組織での ISMS 認証取得の必要性が高いことを示していると考えられる。

（２）ISMS 認証取得業種

今回の調査でも従前の調査と同様、「情報通信業」が 40%以上を占めており、最も大きな割合を占めている。これは経済産業省が情報サービス業の情報システムが十分な安全対策を実施しているかを認定する制度として「情報システム安全対策実施事業所認定制度[9]」があった。この認定制度を廃止し、技術的な情報セキュリティと人間系の運用・管理面を取り込み、グローバル･スタンダードとして ISMS 第三者認証制度をスタートさせた。このため、情報通信業が大きな割合を占めている。

第 2 位には、「製造業」（11.8%）、である。前々回 3 位から前回 2 位に順位を上げたが、今回も 2 位であった。第 3 位は「複合サービス業」（10.6%）で前回と同じだった。

中位クラス以下の順位が前回等とは多少異なる。今回は、6 位：ハイテク、7 位：運輸業、8 位：公務（政府・自治体）、以下、金融･保険業、医療･福祉、教育･学習支援、不動産、電気･ガス･水道となっているが、前回は、6 位：金融･保険業、7 位：ハイテク、8 位：医療･福祉等と続いている。　ただ、1 桁台での相違であり、大きな相違ではないと考えている。

（３）アンケート回答者の所属部門と役職

今回の調査では、前回 2 位だった総務（含人事・経理）部門（103 件、24.2%）が、前回の情報セキュリティ部門（85 件、20.0%）を抜いて、トップになった。3 位は、情報システム管理部門（66 件、15.5%）で、前回と同様であった。これら上位 3 部門で全体の約 60% を占めた。　明確な理由は不明だが、今回の調

[9] 1981 年（昭和 56 年）7 月 20 日通商産業省告 示 342 号による「情報システム安全対策実施事業所認定制度」が作られた

査では ISMS 認証取得後、2 年以上経過している事業所を対象としていることがあるのではないかと考えている。　また、他の認証を取得している事業所は、半数以上の 57.3% あった。このことも関係しているようにも考えられる。

回答者の役職では、課長（26.1%）、部長（23.5%）、一般社員（14.1%）の順で、従前とは異なるが、上位 3 クラスで全体の 60%以上(63.7%)を占めており、係長・主任まで含めると 75%を越えている。取締役が ISMS 認証取得に関係していることは前回とあまり変わらないが、会長・社長の割合は低くなってきた。

前回から追加した質問の記入者の ISMS 運用における役割についての質問では、前回と同じで、ISMS 事務局責任者(37.9%)、情報セキュリティ責任者(30.8%)、ISMS 事務局員（26.7%）の順になっている。

今回の調査では、「3 年～5 年未満」が 38.2%を占め、「1 年～3 年未満」の 27.7%を押さえた。また、3 年以上の経験者が 65.5%を占めており、前回の 37.5%、前々回の 27.7% と比べると遙かに経験豊富な傾向が強い。

４．２　ISMS 認証取得に関するもの

（１）ISMS 認証取得年月

2006 年の取得が最大（96 件、23.4%）で、2005 年（86 件、20.9%）、2007 年（85 件、20.7%）、2008 年（77 件、18.7%）と続いているが、従前と大きな相違はない。ただ、2008 年取得事業所については、526 件ある事業所の約 26%（138 件）にはアンケートを送付していないため、2008 年取得事業所全てにアンケートを送付していれば、もう少し増えた可能性は考えられる。

（２）ISMS 認証取得事業所の従業員数

認証取得対象従業員数では、100 人未満（230 件、54.6%）、100～300 人未満（126 件、29.9%）の順で、この 2 つで全体の 84.5%を占めており、300 人未満規模の事業所が ISMS 認証を取得していることが分かる。

ISMS 認証制度では、ISMS 取得範囲は組織の一部でも可能なため、企業の従業員数と認証対象従業員数のクロス集計を行ってみた。

100 人未満の認証取得対象従業員数(230 件)の半数以上（148 件、64%）は、100 人未満の組織が、20%（46 件）を 300 人未満の組織取得している。なお、認証取得対象従業員数が 100～300 人未満と回答しているが、従業員数は 100 人未満と言った回答があるが、これは複数の企業で ISMS 認証を取得しているケースと考えられ、他の人数でも同じと考えられる。

（３）他の認証取得状況と取得年月

ISO9000（163 件、36.4%）、ISO14000（131 件、29.2%）、プライバシーマーク（118 件、26.3%）の順になっており、前年とあまり大きな相違はない。

なお、ISMS 以外に取得している認証制度の数では、取得していない（182 事業所)、１つ取得（105 事業所)、２つ取得（81 事業所)、３つ取得（52 事業所)、４つ取得（5 事業所)、５つ取得（１事業所）となっており、アンケート回答事業所（426 事業所）の内、244 事業所（57%余り）が ISMS 以外の認証を取得している。

（４）ISMS 認証の取得目的

「営業活動に有利になる」（318 件、75.2%）が最も高い結果になったが、次いで「情報セキュリティ対策向上のため」（280 件、66.2%）となっており、これらは過半数を超えている。前回は入札が３位であったが、今回は「業務改善」（189 件、44.7%）が入札を上回った。

（５）認証取得の発案者

ISMS 認証取得の発案者は、会長・社長（200 件、52.0%）やその他取締役（88 件、20.8%)、管理職（72 件、17.0%）となっており、トップダウンによるものであることが分かる。 執行役員（19 件、4.5%）は最低の数値になっているが、これは、執行役員制度がない企業が多いためだと思われる。

（６）ISMS 認証の運用責任者は？

前回と順位は同じで、その他取締役（142 件、36.3%)、管理職（120 件、30.7%)、会長・社長（79 件、20.2%）の順になっている。

（７）認証取得後に認証範囲の変更／変更の検討

認証取得後の認証範囲の変更については、前回と同じで、「変更予定なし」（247 件、58.4%）が最も多い。ISMS 認証はプライバシーマークと異なり、組織全体で取得する必要がないため、取得後に ISMS 認証範囲の拡大を考える組織もある。

なお、ISMS 認証以外の認証を取得している事業所が 60%近くあるため、統合審査等を検討している事業所もあるものと思われる。

４．３　ISMS 認証の効果・影響について

（１）ISMS 認証取得で得られた効果は？

上位には、従前と同じで、「社員のセキュリティ意識の浸透と実践」（371 件、87.1%)、「情報資産の明確化と整理」（342 件、80.3%)、「事故発生時の体制・計画の整備」（262 件、61.5%)、「情報流出や漏洩の防止・軽減」（261 件、61.3%）の順になっている。今回は、上位４項目が 61%以上の値になっている。

（２）ISMS 認証取得での想定外の影響は？

「業務への影響はない」（103 件、24.2%）との回答が前回（79 件、22.4%)、前々回（46 件、17.4%）より増加しているが、「業務量の増加」（170 件、39.9%)、

「業務上の制約の増加」(141 件、33.1%)、「対策コストの増加」(136 件、31.9%)、「組織・人が必要」(120 件、25.8%)、「手続きの煩雑化」(110 件、25.8%) の割合は「業務への影響ない」の回答より高くなっている。

ISMS 認証制度の定着化には、苦労している様子がうかがえる。

全体 (426 事業所) の内、半数以上の 216 事業所が、業務量の増加や手続きの煩雑化・効率低下と回答しており、更に、その内、126 事業所 (58.6%) が「監査目的のための資料作成」をその具体的なものとしてあげている。ISMS 審査(更新審査やサーベイランス) や内部監査のための資料作りが負担になっているものと思われる。

また、141 事業所(33.1%)が業務上の制約を増やしているが、112 事業所(79.4%)が機器の取扱 (持出・持込) の制約、78 事業所 (55.3%) が資料作成ルール、上長の承認の増加 (55.3%) 等と回答している。

(3) ISMS 認証後の運用上の負担と重点的な取組み

ISMS 認証取得後の運用で負担になっていると感じているものとしては、「リスクアセスメントの見直し」(210 件、50.0%)、「ポリシー (含規定類、業務マニュアル等) の改訂や記録などの更新作業」(188 件、44.8%)、「情報資産台帳の見直し」(181 件、43.1%)、「内部監査対応」(157 件、37.4%) の順になっている。従前の調査でも、これら４項目が上位にきている。

重点的な取組みでは、「一般社員の認識・理解の強化」(281 件、67.5%) が半数を超える回答があった。それ以降は、「有効性評価手法の改善」(131 件、31.5%)、「内部監査担当のスキル強化」(131 件、31.5%)、「教育研修の改善」(127 件、30.5%) と続いている。

(4) 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) については、「乖離はない (161 件、38.2%)」、「どちらとも言えない」(149 件、35.3%)、「乖離はある」(112 件、26.5%) となっている。なお、前回の調査では、「乖離はある」は、約 12%足らずであり、今回の調査では、乖離を感じている事業所が前回調査より２倍以上になる。

(5) ISMS 維持費用について

前回の調査では、半数以上が「妥当」と回答していたが、今回は、「高い」(236 件、55.9%) との回答が「妥当」(185 件、43.8%) を上回った。景気後退の影響もあるが、一部には審査との兼ね合いで高いと回答している所もある。

４．４　ISMS 認証に関連する体制等について

（１）ISO27002 をどこまで取り入れたか

全体としては、前回と大きな相違はなく、「参考程度」（178 件、42.2%）、「十分に取り入れた」（150 件、35.5%）としている。

（２）ISMS 事務局

ISMS 事務局の人数は、「４～６人」（111 件、26.3%）、「３人」（96 件、22.7%）、「２人」（89 件、21.1%）の順になっている。適切な事務局人数を決めるのは業務内容等を考慮して決めることがなるが、300 人未満の認証取得対象従業員数の割合が約 85%であることを考えると、この程度の事務局の人数であろうと考えられる。

但し、１名のみで兼務が 45 事業所、２名のみで兼務が 69 事業所あり、ISMS 業務が定着していない事業所では、厳しい人数ではないかと思われる。

初回認証取得時の事務局メンバーがどの程度残っているかでは、「全員残っている」（87 件、21.1%）、「50～70%未満」（21.1%）、「一人もいない」（81 件、19.6%）の順になっており、半分以上（55%）が、初回認証時の半数以上のメンバーが残っていると回答している。

事務局の新規メンバーに対する ISMS 関連スキル教育では、「社内講習によるスキル習得」（230 件、55.4%）、「OJT による習得」（220 件、53.0%）、「外部講習によるスキル習得」（39.3%）と続いている。事務局メンバーに対する教育をどの様に行うかは、メンバーが完全に交代するのでなければ、社内での教育も可能であると思われる。

４．５　コンサルタントについて

ISMS 認証取得のために、コンサルタントの利用があるが、必ずしも適切なコンサルテーションを行っていないケースもあり、コンサルタントについて、いくつかの質問を前回から行っている。

（１）コンサルタントを利用について

従前の調査と大きな相違はなく、認証取得までは、70%以上の事業所が利用しているが、認証取得後には 70%弱の事業所が利用していない。認証取得時の知識・経験があれば、自社だけで ISMS の運用を行っているものと思われる。

（２）コンサルタントの各種理解度

① ISMS の理解度

316 事業所が回答しているが、平均値が 7.85 となっている。

② 情報セキュリティの理解度

316 事業所が回答しているが、平均値が 7.79 となっており、前回の 7.9 か

らは若干低くなっている。

③ 認証取得組織の業務への理解度

316 事業所が回答しているが、平均値が 6.62 となっており、前回の 6.9 から更に低くなっている。

④ コミュニケーション

315 事業所が回答しているが、平均値が 6.95 となっており、前回の 7.8 から更に低くなっている。

⑤ 実効性のある提案をしているか

315 事業所が回答しているが、平均値が 6.54 となっており、前回の 7.3 から更に低くなっている。

⑥ 確立したコンサル手法

314 事業所が回答しているが、平均値が 6.67 となっており、前回の 7.6 から更に低くなっている。

⑦ 一貫性を持ったコンサルテーション

314 事業所が回答しているが、平均値が 6.97 となっており、前回の 7.6 から更に低くなっている。

⑧ ISMS 認証を取得する上で役に立ちましたか？

315 事業所が回答しているが、平均値が 7.72 となっており、前回の 8.3 から更に低くなっている。

⑨ 費用の妥当性

コンサルタント費用についての質問であるが、259 事業所が回答しているが、「高い」（118 件、45.6%）、「妥当」（125 件、48.3%）とほぼ拮抗しているが、妥当が若干高くなっている。

⑩ コンサルタント選定で最も重視した項目は、上記（29～37）のどれですか？

300 事業所が回答しているが、「36.認証取得に役立った」（70 件、23.3%）が最も多く、次いで、「33.実効性のある提案」（56 件、18.7%）、「29.ISMS の理解度」（53 件、17.7%）となっており、当然のことながら、認証取得に役立つコンサルを求めている。

⑪ コンサルタント導入の最終判断者は？

313 事業所が回答しているが、トップダウンによる決定の感があり、「１．会長・社長」（206 件、65.8%）が最も多く、次いで、「2. その他取締役」（56 件、17.9%）、「4. 管理職」（30 件、9.6%）となった。

４．６　ISMS 認証審査及び審査員について

コンサルタントと同様、ISMS 審査員についての調査を行った。他の認証システムについても、従前から、審査員の質や態度について一部の認証取得事業所から不満もでてきており、今回も調査を行った。

① ISMS 審査員は ISMS を理解していましたか？

417 事業所が回答しているが、平均値は 8.65 で、前回 9.3 から低くなっている。審査員の ISMS 理解度が必ずしも十分でないとの評価が増えている。

② ISMS 審査員のセキュリティ技術の理解は？

417 事業所が回答しているが、平均値は 8.31 で、前回は、8.8 であり、評価の低落傾向は変わらない。

③ ISMS 審査員の認証取得組織業務への理解度

417 事業所が回答しているが、平均値は 6.98 で、前回は、7.7 であり、評価の低落傾向は変わらない。 審査員は原則的には、審査対象業界の経験があることが前提になっているが、他業界からの審査員の知識等が十分ではないのではないかと思われる。

④ コミュニケーションについて

417 事業所が回答しているが、平均値は 7.66 で、前回は、8.3 であり、コミュニケーション能力が低い審査員が見受けられる。

⑤ 実効性のある指摘

417 事業所が回答しているが、平均値は 7.39 で、前回は、8.1 であり、認証取得事業所が審査員に対して厳しい見方をしていることがわかる。

⑥ 効果や課題を確認する能力

417 事業所が回答しているが、平均値は 7.58 で、前回は、8.4 であり、認証取得事業所が審査員に対して厳しい見方をしていることがわかる。

⑦ ISMS 審査員について、最も重視する項目

396 事業所が回答しており、「実効性のある指摘」（202 件、51.0%）が半分以上を占めている。次いで、「貴組織の業務の理解度」（66 件、16.7%）、「効果や課題を確認する能力」（49 件、12.4%）と続いている。

４．７　内部監査、マネジメントレビューについて

（１）内部監査の実施頻度（除、自己点検）

傾向としては、「年１回」（326 件、77.1%）が増えている。 ただ、リスクを考えると、高リスク部門の頻度を増やすことも１つの方法である。更新審査やサーベイランスが年１回のため、年１度と考えている事業所もあるが、ISMS

認証制度上では、年１回以上、実施しても問題はない。

（２）内部監査体制について

内部監査体制については、従前では、非常設社内チームがトップであったが、今回の調査では、424 事業所からの回答があり、「常設社内チーム」（218 件、51.4%）が過半を占めているが、それでも、「非常設社内チーム」（189 件、44.6%）もまだ半分近くある。

（３）指摘事項は改善されていますか？

従前からみると、改善されているとの回答が少し減ってきている。また、その理由として、「現場に改善余力がない」との回答が約 32%あり、「現場が非協力」や「マネジメントの支援不足」等、ISMS 認証システムの維持に問題になりそうな理由が上位に並んでいるが、審査員（審査機関）は次回審査で問題（指摘事項）にすべきであろう。

（４）マネジメントレビューの実施頻度と形態

「年１回」（288 件、70.7%）が 70%以上を占めており、次いで、「半年に１回」（86 件、20.3%）となっている。ISMS では、年１回実施すれば良いのだが、大きなリスク要因などがあれば、その対応のためにマネジメントレビューを行うことを妨げるものではない。内部監査の実施や ISMS 審査等に合わせて行っている。

マネジメントレビューを会議形式で行っているのが、今回でも 90%以上に達しているが、次第に減る傾向にあり、「会議とメールの組合せ」（28 件、6.5%）が増えてきている。　今後、TV 会議等が更に一般化すれば、TV 会議等での対応も考えられる。

４．８　教育について

ISMS に関する組織内での普及・啓発に重要なものの１つに教育があるが、教育について、いくつか質問を行った。

（１）教育方法について

社員への教育方法については、従前の調査とあまり大きな相違はなく、「集合研修」（347 件、82.0%）が最も行われており、次いで、「冊子の配布」（180 件、42.6%）、「ＯＪＴ」（140 件、33.1%）、「E-ラーニング」（128 件、30.3%）と続いている。ただ、継続的に ISMS 認証取得を行っている組織でありながら、３事業所が教育を行っていないとの回答があるが、審査員はどの様な審査を行っているのだろうか？

情報セキュリティ管理者・推進者への教育方法では、「集合研修」（252 件、60.0%）、「ＯＪＴ」（136 件、32.4%）、「冊子の配布」（129 件、30.7%）、「自己啓

発」(100 件、23.8%) の順になっており、前回の順位の３，４位が逆転しているが、前々回と同じになっている。　全く教育が行われていないケースが 34 事業所ある。

経営陣への教育については、「集合研修」(160 件、38.6%)、「冊子の配布」(120 件、28.9%)、「E-ラーニング」(75 件、18.1%)、「ＯＪＴ」(55 件、13.3%) の順になっている。ここでも、９９の事業所 (23.9%) で、教育が行われていないが、経営者への認識を高めるためにも何らかの教育・啓発が望まれる。

（２）社員への ISMS の教育頻度について

従前では、年１回、半年に１回が多かったが、今回の調査では、「３ヶ月に１回」(181 件、43.1%)、「月１～２回」(109 件、26.0%) となっており、頻繁に教育を実施している傾向が見られる。情報セキュリティについては、技術的な対応だけでは限度があり、利用者への教育・啓発が重要になってきている。

（３）ISMS 教育の担当部門とレベル

「情報セキュリティ部門」(211 件、50.2%) が最も多く、「総務 (含人事等)」(90 件、21.4%) が続いており、「情報システム管理部門」(84 件、20.0%) になっている。

担当部門のレベルでは、設問が適切でなかったため、有効回答が非常に少なかったが、全体的には前回の調査よりレベルが高くなっている。

（４）教育以外に行っている啓発活動について

啓発活動では、「ポスター掲示」(300 件、71.4%) と「会議での連絡・通知」(290 件、69.0%) が他の活動に比べ高い割合を示している。次いで、「ウェブ啓発活動」(100 件、23.8%) が続いている。前回は、会議、ポスター、ウェブの順であるが、会議が他の２つの項目より高い割合を示している。

（５）教育以外に行っている啓発活動について

今回、始めて教育・訓練等についての有効性測定としてどの様な方法を採用しているかを尋ねた。集合教育、E-ラーニングとも、「テストの実施」(集合：209 件、57.3%、E-ラ：110 件、82.7%) が最も多い。

但し、集合教育では、「アンケートの実施」(69 件、18.9%)、「出欠確認」(62 件、17.0%) が比較的高い割合を示しているが、E-ラーニングでは、「アンケートの実施」(14 件、10.5%)、「出欠確認」(4 件、3.0%) は、余り大きな割合にはなっていない。

教育・訓練の有効性測定では、アンケートはあまり役立たないと言われており、出欠の確認だけでは殆ど教育効果が見られないのではないかと思われる。

４．９　社内ルール等について

最後の質問グループとして、社内ルール（個別のセキュリティポリシー）やコンピュータウイルスに関する内容について聞いた。ISMS 認証維持に直接関係するものではないが、ISMS 認証取得事業所がどの様なことを行っているかについて調べてみた。

（１）情報漏えい対策について

上位４項目は 50%を越えており、「２．ログインパスワード認証」（402 件、95.3%）、「パスワードの定期的変更」（368 件、87.2%）、「ファイルの暗号化」（283 件、67.1%）、「外部媒体接続制限」（239 件、56.6%）の順になった。前回は３位と４位が逆で、また、上位３項目のみが 50%を越えていた。

パスワード認証、パスワードの定期変更は当然行うべきものになっているが、ファイルの暗号化（前回は 36.9%）が次第に一般的になってきている。情報漏えいが発生しても、ファイルが暗号化されていれば、情報が悪用される可能性は少ない。

（２）可搬媒体（①ノート PC、②外部記録媒体）の社外に持出ルール

ノート PC の場合も外部記録媒体の場合も、「ルールあり（要許可）」が、80%以上の回答でトップであった。次いで、「持出禁止」で、10%前後の割合であった。

持出禁止を基本としている場合、何らかの理由（ポリシー違反であるが）で、持ち出されてしまった場合の対応を考えておく必要がある。例えば、ファイルの暗号化等が必要になる。適切な暗号化を行っていれば、ポリシーに違反して、持ち出されても、情報漏えいになる可能性は低い。

（３）社内持込や利用制限機器について

「ノート PC」（356 件、89.4%）や「外部記憶媒体」（341 件、85.7%）の持込・利用制限は非常に多くの組織で制限をしているが、「携帯電話」（86 件、21.6%）等についても前回より高い割合になってきている。

（４）コンピュータウイルス感染の有無と感染原因

「感染はない」（280 件、66.4%）との回答が最も多く、次いで、「感染あり」（137 件、32.5%）になっている。　通常のセキュリティ調査などでは、感染ありが、回答者の 60%以上であることが多いが、ISMS 認証取得事業所では、感染が半分程度の割合になっている。　ISMS 認証取得効果がでていると言えるであろう。

感染原因として考えられるものでは、「ウェブ閲覧によるドライブバイダウンロード」（71 件、5.18%）が最も多く、次いで、「パターン更新漏れ」（27 件、19.7%）、「ゼロディウイルス」（21 件、15.3%）と続いている。

一般的には、ウェブ閲覧による有害プログラム（マルウェア）は、コンピュータウイルスと言うより、「トロイの木馬」とか「スパイウェア」と呼ばれるものが多く、ワクチンソフトで検出することが難しいと思われる。

４．１０ 自由回答欄について

回答者に ISMS 認証の維持・運営を行っている中で感じている事項や疑問、課題等について自由な記入を求めたもの。

何らかのコメント（「特になし」等は除いた）が記入されていたものは、131 件、30.8% （全回収数：426 件）あった。　主な記述は以下の通り。

① ISMS 認証システムについて、有効性の高いものだとの評価がある一方で、JISQ27001／27002 等の規格書がわかり難い、英訳が日本語として熟れていないとの不満も多い。

② ISMS 認証とプライバシーマーク等、複数の認証取得事業所では、共通項目が多いので、統合して出来ないかの意見も多い。　複数の認証システムを取得している事業所では、そのための対応に苦労している。

③ ISMS 推進担当者が少なく、兼務等の場合、作業負荷も大きい事が課題になっている。

④ 従業員に対する教育が徹底していないこともあり、情報セキュリティに対する意識向上・定着化が難しい。

⑤ 削減に努めているが、インシデントがなかなか減らない。

⑥ 新しい情報機器の出現のため、それらの管理手順等の対応が後手に回り勝ちになっていることが多い。

⑦ 情報資産の見直し、リスク評価等、定期的に行う ISMS の作業がマンネリ化してきている。

⑧ セキュリティ対策と業務効率のバランスの難しさを指摘する声も多い。

⑨ リスクアセスメントや有効性評価について、必ずしも十分に行われていない事業所も多い。

⑩ ISMS 推進担当者の専門性が高くなり、人事異動が難しくなっている。

⑪ 審査員に対する評価も、毎回の指摘事項が適切だと言った高い評価がある一方、審査員の指摘が毎回異なる、レベルが低いと言った声も多い。

⑫ ISMS 維持費用（審査料も含め）が高額になっており、最近の不況時にはかなり厳しくなっている。　また、審査料に見合う審査が行われていないという不満も一部にある。

⑬ 費用対効果等に面から、ISMS 認証システムの維持を返上する考えの所がでてきている。

４．１１ アンケートから見えてくるもの

アンケートへの回答や自由記入欄からいくつかのことが見えてくる。

第１回目の調査実施後に、認証制度の課題をマスコミのウェブに寄稿[10]したが、指摘した内容は、①経営者の関心度の高低、②ISMS への誤解、特に管理策への誤解、③コンサルタントの問題、④審査機関、審査員の問題、⑤ISMS 独自の問題（短期間での移行）の５項目であった。最後の項目は、この時、独自の課題であったが、他の４項目は、今回の調査でも同じような課題となっている。

① 経営者の関心度: 経営トップが情報セキュリティを無視する態度が、管理職、一般社員への波及し、ISMS の運用に大きな影響を与える。　逆に、経営者が積極的であればある程、継続的改善も可能になるとの回答もある。

② ISMS の課題： ISMS での有効性評価に苦労している。ISO/IEC27004:2009「情報セキュリティマネジメントー測定」の日本語訳[11]も出版されているが、有効性評価について苦労している事業所が多い。

③ ISMS への誤解: 特に管理策についての誤解は、認証取得事業所だけでなく、審査員の一部にもある。

「JISQ27001:2006　情報セキュリティマネジメントシステムー要求事項」の 1.2 適用には、『この要求事項は、汎用的であり、形態、規模及び事業の性質を問わず、全ての組織に適用できることを意図している。（中略） 管理策の適用を除外する場合は、（中略）適用除外を正当とする理由と、責任ある者が関連するリスクを受容したことを示す証拠が必要である。』としている。このため、認証取得事業所は管理策の取捨選択することが可能としている。しかしながら、管理策を「唯一絶対的なもの」と考えているため、業務との乖離や二重帳簿的な仕組みを構築している回答がある。

④ コンサルタントや審査員の問題: コンサルタントや審査員に対しての評価を 10 段階で行ったが、従前の調査より、両方とも低くなっている。　特に、コンサルタントに対する評価は、①ISMS の理解度、②情報セキュリティの理解度、③業務の理解度、④コミュニケーション力、⑤実効性のある提案、⑥確立したコンサル手法、⑦一貫性を持ったコンサル、⑧ISMS 取得に役立ったについての評価で、８以上の評価を得たものが一つもなかった。特に、③から

---

10 内田勝也,「ネット時評『情報セキュリティ認証制度、実態調査で見えてきた課題』」, 日本経済新聞社, 2007.06.28, http://www.nikkeidigitalcore.jp/archives/2007/06/post_109.html

11 ISO/IEC27001 等は、JISQ27001 として JIS 化されているが、これは ISO/IEC の翻訳である。ただし、経験から言えば、JIS 化されたものと翻訳とは、内容的にはあまり大きな相違はない。

⑦については、平均が6点台の評価となっている。

また、審査員の評価では、①ISMSの理解度、②セキュリティ技術の理解度、③業務の理解度、④コミュニケーション、⑤実効性のある指摘、⑥効果・課題を確認する能力について評価したが、③は6点台となっており、④から⑥も7点台であった。　本来、審査員はその業界の理解が必要であり、原則的には、その業界出身者が望ましいのだが、その業界での経験が少なければ、何らかの教育・研修が必要になるのだが。　また、一部の審査員に、審査員としての資質に欠けるとの批判もある。認証取得事業所からのコメントだけで判断するのは適切でないが、審査員の立場、即ち、受審事業所とは対等の立場であることを忘れている審査員がいる。

更に、ISMSの維持費用について56%が高いと評価しており、審査がマンネリ化しているとの指摘もあり、費用に見合うメリットを感じていないのではないだろうか。

４．１２ インタビューから見えてくるもの

従前の調査では2、3事業所へのインタビューであったが、今回は6事業所への訪問、インタビューを試みた。

全体的な印象としては、アンケート調査で課題として指摘されている事柄から大きく離れるものではない。

（1）ISMS推進担当者と経営層の理解

企業規模やISMS認証取得範囲があまり大きくないこともあり、専任でISMS推進を行っていない。このため、経営層の理解の程度等がISMS推進に影響している感じを受けた。

また、ISMS推進担当者（担当責任者も含め）の専門性が高くなるにつれ、人事異動が難しくと感じている。内部監査を担当したり、審査員審査に立会したりする必要があり、兼務でISMSの維持・管理を行っている場合には、後任を探すのが大変なのであろう。

（2）コンサルタント、審査機関・審査員について

コンサルタントを利用している事業所が多いが、コンサルタントに問題があったと回答している事業所もいくつかある。

多くの場合、自社業界の関係者の紹介やセミナー等の講師をコンサルタントとして、依頼しているが、レベルかが分からないため、良い結果に繋がらないこともある。

何らかの客観的な情報が必要なのであろう。

審査員については、比較的恵まれているとの回答が多いが、審査員、審査機関に問題があるとの回答もある。

ISMS 推進者でなく、現場の責任者が対応する場合等では、ISMS 審査での指摘事項等に対して、指摘事項が誤解に基づくものであっても、それを現場責任者が説明しないこともあるようで、審査報告書が作成された後に問題になると言ったこともあると言った回答もあった。審査員としては、誤解での指摘であれば事業所側からの説明があると考えている可能性があるのではないかと感じている。

また、審査員に全く問題がないとの回答でも、実際には審査員・審査機関に対する課題が見えていないのではないかと感じた回答もあった。

なお、更新審査時に、ISMS 審査に対して複数から見積もりを取得している所もあり、価格、審査機関の対応、審査員の技量等を含めて、従来の審査機関・審査員で継続するかの判断を行っている事業所もある。

コンサルタント、審査員については、自社業務の知識やコミュニケーション能力に若干課題があると感じている事業所もある。審査機関として、審査員に対して、対象事業所の業務知識やコミュニケーション能力をどの様に高めるかを考える必要があろう。

５．ISMS 認証制度の実効性向上のための提案

2006 年に第１回の ISMS 認証取得事業所調査を始めたが、今回の調査で、3 回目になる。　現在、情報セキュリティマネジメントシステムに関連する調査は、本調査が現在まで最も広範囲に行ってきた。今回の調査を含め、ISMS 認証制度の実効性向上のため、何を行う必要があるか考察した。

５．１　ISMS 制度の見直し

- ISMS のパイロット期間からそろそろ 10 年になるが、一度、ISMS 認証制度全体の見直しを行うことが大切であろう。

- 認証制度の意義は、企業間取引において情報資産を適切に管理・運用しているかを、関係する取引先毎に調査するのは容易ではない。しかし、第三者がある基準に従って、情報資産を管理する仕組みが構築されているかを判断し、適切であれば、「認証」（お墨付き）を与える。　この認証を獲得した企業であれば、安心して情報のやり取りを行うことが可能であると判断することができる。

- ISMS が、国や自治体の入札要件[12]になっているが、本当に適切なのだろうか？　品質管理マネジメントシステムである ISO9000（QMS）認証システムは、国土交通省が 2000 年から入札条件にしていたが、2004 年 4 月以降は入札条件から外すことにした[13]。韓国でも日本より早く入札要件から外している。これは、QMS 認証制度でなく、QMS の運用の問題である。即ち、入札要件にしたために「QMS 認証を金で買う」事業所が出てきており、QMS 認証取得をしているから適切な品質を確保できているとは限らないことが判明している。

  ISMS でも同じような問題が言われており、今までの調査内容からも、ISMS 認証の維持継続が目的となっており、セキュリティマネジメント体制のレベル向上に繋がっていない事業所が多々あることを感じる。

  実際、実業務と ISMS との「乖離がない」と回答している事業所は 40%もなく、はっきり「乖離あり」としているのは約 27%、4 社に 1 社以上ある。情報セキュリティ推進に役立つ制度であるが、目的が不明確になれば、制度に対する不信感が高まり、形骸化してしまう。実際、「当社のレベルに比べ、あの事業所の ISMS 認証レベルは余りにも低すぎる」と言った声もある。

- 第三者機関の設置を設置し、認定機関、認証機関、審査員研修機関等の運営体制を監査する仕組みが必要であろう。　ISO/IEC 規格に基づいた制度であ

---

[12] （財）日本情報処理開発協会「FAQ1: 制度一般（ISMS）」
http://www.isms.jipdec.jp/faq/faq1.html

[13] 日経コンストラクション「ISO を入札要件から外す」2004.6.11 号 日経 BP 社

っても、運用体制が十分でなければ、ISMS 認証制度全体が揺らいでしまう可能性がある。　身内での運用体制が長く続けば、問題が顕在化するのは、「国技」だけではない。

５．２　コンサルタントの評価制度について

ISMS 認証等の取得を考える場合、他の認証取得経験がない等の事業所では、コンサルタントの利用を考える組織が多い。ISMS 等の認証取得後には、コンサルタントの利用は少なくなるが、それでも一部の事業所では継続して利用している。

しかしながら、コンサルタントについての情報やその評価については、十分共有できていないため、ISMS 認証取得目的でコンサルタントを利用したが、認証審査時に、審査員とコンサルタントとの乖離に愕然とすることがあると言う回答もある。

コンサルタントがどの様なコンサルテーションを行うかについては、自由であるが、ISMS 認証制度の標準的な教育を受講しているか等の情報があれば、コンサルタント自身の ISMS 関連知識のレベル向上になり、また、ISMS 認証取得を計画している事業所にとっても、コンサルタントの選定に役立つと思われる。

「安かろう、悪かろう」でなく、良質なサービスを提供するコンサルタントがもっとでてきて欲しい。

５．３　監査概念について

従前の調査等を含めて、非常に大きな問題として感じていたのは、ISMS 認証システムは、「監査」だという考えの欠如である。

管理目的、管理策はチェックリストでなく、取捨選択可能なものである。

実際、JISQ27002 では、「0.2.5 管理策の選択」において、

> （略）リスクを受容可能なレベルまで低減することを確実とするように，管理策を選択し実施することが望ましい。管理策は，この規格又は他の管理策集から選択することが可能であり，また，固有の要求に合わせて新しい管理策を適切に設計することも可能である。セキュリティ管理策の選択は，リスク受容基準，リスク対応における選択肢，及び当該組織が採用している全般的なリスク管理の取組み方を基に下した組織的な判断に依存するものであり，すべての関連する国内外の法令及び規制にも従うことが望ましい。(後略)

と述べており、JISQ27001 でも、「4.2.1 ISMS の確立」において、

> (g) リスク対応のための，管理目的及び管理策を選択する。
>
> 管理目的及び管理策は，リスクアセスメント及びリスク対応のプロセスにおいて特定した要求事項を満たすために選択し，導入しなければならない。
>
> この選択には，法令，規制及び契約上の要求事項と同じく，リスク

受容基準も考慮しなければならない。

と述べており、管理目的、管理策がチェックリストでなく、リスクを考慮して取捨選択するものであることが分かる。

この点についての理解がないコンサルタント、審査員、ISMS 取得事業所推進者等が ISMS 推進の妨げになっていることは明確である。

実際、ISMS 認証制度ではないが、派遣者に対する機密保持契約（NDA）を行うかの議論において、派遣先企業との NDA は法的な面から締結が必要であるが、チェックリストに規定がないため、派遣要員との NDA は不要だとの見解があると指摘された。しかしながら、ISMS では、管理目的、管理策に規定がなくとも、リスクが大きいと判断すれば、適切な管理策を新たに作成する必要がある。全ての管理目的、管理策が各事業所に適切とは限らない。事業所毎だけでなく、同一事業所でも環境の変化、時間の経過によりリスクは変わる。

リスク中心の考えが大切であり、情報資産を見直す最大の理由はリスクの変化を確実に把握することである。組織変更やシステム変更等があれば、情報資産のリスクを再評価する必要がある。

５．４　認証機関、審査員の質的向上

審査員によって、指摘が異なるとの意見がある。時間の経過や環境が異なれば、リスクが変化し、審査員の指摘も以前と異なる可能性があるが、指摘が異なる点を審査員に説明をさせる指導をすべきであろう。認証の審査やサーベイランスは、監査業務の一つと考えられ、指摘事項については、その理由を被監査部門（認証取得事業所）に説明する必要がある。　指摘事項については、審査員の誤解や意見相違が発生することもあり、100%完全に認証取得事業所を納得させることはできないこともあるが、指摘事項を説明する必要がある。

本調査は認証取得事業所からの意見を主に聞いており、審査機関側からの意見を聞いていないため、必ずしも適切な判断とは言えないが、それでも、認証機関（審査員）に対して、厳しい意見を記名で書いてくる事業所もあることを認証機関、審査員の方々はぜひ考えて欲しい。

審査機関は審査員の質的向上に努めることが、ISMS 認証システムの普及に繋がると考えている。

また、審査員も「老後のアルバイト」的な考えを捨て、専門家としての能力の維持・向上を目指して欲しい。

５．５　教育、普及啓発について

ISMS 認証システムを維持・向上する上で、教育や普及啓発は非常に重要であると考えている。

特に、ISMS 認証制度は、情報セキュリティに関するマネジメントシステムの構築を目的としている。　このため、ISMS 認証制度システムに関係する全ての者に

周知を図り、推進することが大切になる。

しかしながら、調査から見えてくる教育や啓発活動の課題もいくつか存在する。

① 経営層などへの適切な教育の実施

経営層、管理層ほど、教育自体の機会が少なくなる傾向がある。

経営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の十分な理解を得ることにあると言える。

経営トップは情報通信（ICT）システムや情報セキュリティ等は、専門的過ぎて分からないと言うことが多いが、情報セキュリティや ISMS 認証制度に関心を持つことが大切だと思われる。

また、経営トップ自らが、セキュリティポリシーを順守しないため、それが ISMS 認証制度を崩壊させる原因になるとの回答もある。

経営層は、自社の ICT システムが数日停止した場合や保有する個人情報や機密情報が漏えいした場合、企業経営上どの様な問題が発生するかを自問・自答して欲しい。ISMS 認証制度の重要性が理解できるのではないだろうか。

ICT システムや ISMS 認証制度が理解できないこと以上に、経営層が関心を示さないことが大きな問題であることを自ら考えて欲しい。

② 集合研修での工夫

今回の調査でも、e-ラーニングは約 30%の事業所で実施されているが、80%以上が集合研修であり、まだまだ多くの事業所では集合研修が中心である。集合研修では、17%が出欠確認のみであり、19%程がアンケート実施である。

出欠確認では、殆ど教育効果がなく、アンケートも従業員等、組織内の人々を対象にしたものはあまり実態を反映しないと言われている。

カーク・パトリックは、研修評価・効果測定に関して、4 段階の評価モデルを提言している[14]。　一般的には、教育・研修は、行動変容を起こすような教育・研修を行うことが必要であると言われている。

更に、最近の心理学や行動科学等の知見を利用した教育では、成果達成、投資収益率まで考えた教育・研修が可能であると考えられており、個人指導的な教育・研修（コンサルテーション）では実際に行われている。

ISMS や情報セキュリティ分野でも、心理学的な知見をつかった教育も実験的に行われるようになってきている。

参考： カーク・パトリックの 4 段階評価モデルにジャック・フィリップスが 5 段階目の評価を追加した、5 段階評価モデル

１．研修満足度：受講直後のアンケート調査等による受講者の研修に

[14] （独）雇用・能力開発機構「公共能力開発施設の行う訓練効果測定」 6 章
http://www.tetras.uitec.ehdo.go.jp/download/kankoubutu/a-114-07.pdf

対する満足度の評価。ある基準と比較して望ましい研修が行なわれたかを評価

2．学習到達度：　筆記試験やレポート等による受講者の学習到達度の評価。研修受講の結果、受講者という個人に与えた効果（学習到達）を測定

3．行動変容度：受講者自身へのインタビューや他者評価による行動変容の評価。　研修受講の結果、受講者という個人に与えた効果（行動変容）を測定

4．成果達成度：　研修受講による受講者や職場の業績向上度合いの評価。　受講者個人の行動がもたらした組織への影響

5．投資収益率：　効果測定は、効果を収益に換算し、収益を教育研修への投資額との比較ではじめて有意義になる（ジャック・フィリップス（Jack J. Phillips）の提案)。

① 収益貢献度（レベル 5A）= その成果を収益金額に換算

② 顧客満足度（レベル 5B）= 顧客の満足に与えた成果を見たもの

③　継続的な教育・啓発活動

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。情報通信システムや情報セキュリティでの新しい技術や考え方も出現している。従来の教育・啓発だけでは十分でないこともある。

新たな技術などへの対応を含め、継続的な教育を行うことが大切になる。

６．謝辞

約 2,000 の ISMS 認証取得事業所にアンケートを送付し、426 件の回答を頂いた。前２回に比べても、また、情報セキュリティ関連の調査の回答率からみても、非常に高い回収率で、多くの ISMS 認証取得事業所の方々のご協力に深く御礼を申し上げます。

また、お忙しい中、インタビューを快諾頂いた認証取得事業所の方々に厚くお礼を申し上げます。

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２２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ました。　ここに感謝申し上げます。

以　上

付録Ａ　アンケート調査配布資料

１．アンケートご協力のお願い

中央大学
研究開発機構 内田研究室

「ISMS 第三者認証制度をより有効なものにするための ISMS 認証事業所調査」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 22 年 11 月現在、約 3,700 の事業所・部門で ISMS 認証が取得されております。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、情報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広く普及してきた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、現場と ISMS 基準が乖離しているなどの問題を感じるとの回答もあります。更に、昨今の厳しい経済状況のため、ISMS 認証取得の継続を断念した企業・団体もでてきております。

私ども中央大学 研究開発機構 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。本アンケートは、平成 18 年、20 年に続き、3回目になりますが、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も行っております。

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。

質問は別紙にありますが、**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://www.uchidak.com/isms/

［回答先］ uchidak@tamacc.chuo-u.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、ご記入者名を含め、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、WEB に公開します。 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 23 年 1 月 29 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
中央大学 研究開発機構 内田研究室 教授 内田勝也
〒112-8551 東京都文京区春日 1-13-27
電子メール uchidak@tamacc.chuo-u.ac.jp　携帯 090-1050-3206

なお、本調査研究は、(財)ニューメディア開発協会 平成 22 年度の調査研究事業の一環として実施しています。

２．アンケート質問用紙

質問票	回答用紙にご記入下さい （本質問票の返却は不要です）

中央大学
研究開発機構 内田研究室

貴組織／ご記入者についての質問です（不明な項目は未記入でも構いません）

１．資本金 （択一）

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

２．従業員数（択一）

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

３．貴組織の業種（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: 政府･自治体	16: その他

４．ご記入者の所属（最も近い部門を１つ選択して下さい）

1: 総務(人事･経理)部門	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	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（最も近い役職を１つ選択して下さい）

1: 会長･社長	2: その他取締役	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 認証業務の経験年数（ご自身の経験年数を１つ選択して下さい）

1: 1年未満	2: 1年～3 年未満	3: 3 年～5 年未満	4: 5 年～7 年未満	5: 7年以上

ISMS 認証取得に関して

８．ISMS 初回認証取得年月は？ 西暦＿＿＿＿＿年＿＿＿月

９．認証取得対象従業員数

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

10．他の認証取得状況と取得（西暦）年月

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

11．認証取得の主な目的（該当するものは全て選択して下さい）

1: 会社業務の運営を ISMS 認証に基づいたものにするため	2: ISMS の考え方を取入れ、業務の改善を狙ったため	3: ISMS 認証取得が営業活動に有利になる、あるいは不利にならないことを狙った	
4: 入札等で 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．認証取得の発案者は？（択一）

1: 会長･社長	2: その他取締役	3: 執行役員	4: 管理職	5: その他

13．ISMS 認証の運用責任者は？（択一）

1: 会長･社長	2: その他取締役	3: 執行役員	4: 管理職	5: その他

14．ISMS 認証取得後に認証範囲について変更／変更検討を行っていますか？（択一）

1: 縮小／縮小を検討中	2: 拡大／拡大を検討中	3: 他範囲との統合／統合検討中	4: 変更予定なし

質問票 回答用紙にご記入下さい（本質問票の返却は不要です）

中央大学 研究開発機構 内田研究室

15. ISMS 認証取得で得られた効果は？（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: 特にない ｜16: その他

16. 想定外の影響はありましたか？（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・事故の増加／減少しない
7: 業務への影響は特にない	8: その他（記入欄あり）	

17. 問 16 の「２」、「３」を選択した方 ⇒具体的にどのようなものですか？（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: 事務局等からの業務に無関係な依頼作業の増加	6: 厳格な入退出管理で他部門とのコミュニケーションの悪化
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 の「５」を選択した方 ⇒ 現場での業務上の制約がありますか？（複数選択可）

1: 機器の取扱（含持出・込）の制約	2: 厳格な持ち物検査や入退室管理	3: 作業の事前申請
4: 資料の作成ルールや保存場所等の指定	5: 上長の承認の増加	6: 社外での作業の制限
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: 特にない	12: その他（記入欄あり）

20. ISMS の効果を高めるため重点的に取り組んでいる／予定があるものは？（複数選択可・※はツール導入を含む）

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）はありますか？（択一）

1: 乖離はある	2: 乖離はない	3: どちらとも言えない

22. ISMS の維持費用は妥当だと思いますか？（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: 参考程度であった	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: わからない

25. 現在の 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. 現在の事務局に初回認証取得時メンバーが残っている割合は？ （ ） % （100% 全員←→0%誰もいない）

27. 事務局新メンバーに対する ISMS 関連スキル教育について（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: 特に行っていない	6: その他（記入欄あり）

質問票	回答用紙にご記入下さい （本質問票の返却は不要です）

中央大学
研究開発機構 内田研究室

外部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？（各項目で択一）

認証取得まで	1: 利用した	2: 一部利用した	3: 利用しなかった	⇒ 3、6の両方を選択した方は、問４０にお進み下さい
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	

コンサルタントの以下の項目を 10 段階で評価して下さい（１：低い ⟷ 10：高い）

29. ISMS の理解度	1	2	3	4	5	6	7	8	9	10
30. 情報セキュリティの理解度	1	2	3	4	5	6	7	8	9	10
31. 貴組織の業務の理解度	1	2	3	4	5	6	7	8	9	10
32. コミュニケーション	1	2	3	4	5	6	7	8	9	10
33. 実効性のある提案	1	2	3	4	5	6	7	8	9	10
34. 確立したコンサル手法	1	2	3	4	5	6	7	8	9	10
35. 一貫性を持ったコンサル	1	2	3	4	5	6	7	8	9	10
36. ISMS 認証取得に役立った	1	2	3	4	5	6	7	8	9	10
37. 費用の妥当性	1：高い			2：妥当			3：安い			

38. コンサルタント選定で最も重視した項目は、上記（29～37）のどれですか？（択一）＿＿＿＿＿＿＿＿

39. コンサルタント導入の最終判断者は？（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

	低い ←									→ 高い
40. ISMS の理解度	1	2	3	4	5	6	7	8	9	10
41. セキュリティ技術の理解度	1	2	3	4	5	6	7	8	9	10
42. 貴組織の業務の理解度	1	2	3	4	5	6	7	8	9	10
43: コミュニケーション	1	2	3	4	5	6	7	8	9	10
44: 実効性のある指摘	1	2	3	4	5	6	7	8	9	10
45: 効果や課題を確認する能力	1	2	3	4	5	6	7	8	9	10

46. ISMS 審査員について、最も重視する項目は、上記（40～45）のどれですか？（択一）＿＿＿＿＿＿＿＿

内部監査について

47: 実施頻度（除 自己点検）

1：年１回	2：半年に１回	3：３ヶ月に１回	4：１回／月 以上

48. 体制について回答下さい（複数選択可）

1: 常設社内チーム	2: 非常設社内チーム	3: 外部組織	4: 外部組織と社内の共同	5: その他(記入欄あり)

49. 指摘事項は改善されていますか？

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

50. 問４９で、「２」または、「３」と回答された方に、その理由を回答下さい（複数選択可）

1: 内部監査の指摘が不適切	2: 改善対策への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: 現場に改善を行う余力がない	5: 事務局に改善を行う余力がない	6: その他(記入欄あり)

マネジメントレビューについて

51: 実施頻度	1：年１回	2：半年に１回	3：３ヶ月に１回	4:その他（記入欄あり）
52: 実施形態（複数選択可）	1：会議	2：電子メール	3: 会議 メールの組合せ	4:その他（記入欄あり）

質問票	回答用紙にご記入下さい （本質問票の返却は不要です）

中央大学
研究開発機構 内田研究室

教育・社内ルールなどについて

53. ISMS の維持に必要な社員への教育方法を回答ください。（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）	

54. 情報セキュリティ管理者・推進者への教育方法は？（複数選択可） *** 選択肢は問５３と同じです ***

55. 経営層への教育方法は？ ・・・・・・・・・（複数選択可） *** 選択肢は問５３と同じです ***

56. 社員への ISMS の教育頻度を回答ください。（択一）

1: 毎日	2: 週 1～2回	3: 月に1～2回	4: 3ヶ月に1回程度
5: 半年に1回程度	6: 年に1回程度	7: 行っていない	8: その他（記入欄あり）

57. ISMS の教育の担当部門を回答ください。（複数選択可）

1: 総務(含人事など)部門	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	7: 事業部門	8: 事業推進部門	
9: コンプライアンス担当	10: リスク管理担当	11: 監査部門	12: その他社内	13: 社外

58. 問５６で選択したそれぞれの教育担当部門の情報セキュリティレベルを回答ください。

低い ←	1	2	3	4	5	6	7	8	9	10	→ 高い

59. 教育以外の啓発活動について回答下さい(複数選択可)

1: キャンペーン週間等の設定	2: ウェブでの啓発活動	3: ポスター掲示	4: メルマガ等の発行
5: 会議での連絡・通知	6: セキュリティ標語の制定	7: セキュリティへの取組への表彰(部門・個人)	
8: 標語等を書いたノベルティの配布		9: 特にない	10: その他(記入欄あり)

60. 問５３で、①【集合教育】及び②【E-ラーニング】を行っている場合、各評価方法を回答下さい。（択一）

1： 出欠確認のみ	2： アンケートの実施	3： テストの実施／レポート提出
4 ：インタビュー／他者評価による行動変容の確認		5： その他（記述あり）

61. 情報漏えい対策として実施している対策を回答下さい(複数選択可)

1: ファイルの暗号化	2: ログインパスワード認証	3: パスワードの定期的変更	4: シンクライアント
5: メール送信先の制限	6: 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 パスワード設定	10: ディスクの暗号化	11: EFS 暗号(Windows)	12: 外部媒体接続制限
13: 外部媒体の暗号化		14: 特にない	15: その他(記入欄有り)

62. ①【業務用ノート PC】、②【業務用外部記録媒体】を社外に持出す場合のルールを回答下さい。（択一）

1: 持出禁止	2: ルールあり(要許可)	3: ルールあり(許可不要)	4: 特にない	5: その他(記入欄あり)

63. 社内持込あるいは、利用制限があるものを選択して下さい。（複数回答可）

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)

64. コンピュータウイルス感染の有無（択一）

1: ある	2: ない	3: 分からない／知らない

65. 64 で「１：ある」と回答された方。感染原因は？(複数回答可)

1: ワクチンソフト未導入	2: ワクチンソフト期限切れ	3: パターンファイル更新漏れ	4: ゼロディウイルスのため
5: ウェブ閲覧によるウイルスのダウンロード(ドライブ・バイ・ダウンロード)による			6: 不明

ありがとうございました。
なお、回答用紙には、裏面に自由記入欄等がありますので、こちらもご回答頂けると幸いです。

３．アンケート回答用紙

中央大学
研究開発機構 内田研究室

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をご利用下さい。

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 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 初回認証取得西暦年月　＿＿＿＿年＿＿月

9 認証取得対象従業員数　【　】（１～８）

10 他認証取得 西暦年月　1：＿＿＿＿年＿＿月　2：＿＿＿＿年＿＿月　3：＿＿＿＿年＿＿月
4：＿＿＿＿年＿＿月　5：＿＿＿＿年＿＿月

11 認証取得目的は？　【1．　2．　3．　4．　5．　6．　7．】

12 発案者は？　【　】（１～５）　13 運用責任者は？　【　】（１～５）

14 認証範囲の変更等　【　】（１～４）

15 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 回答２，３のみ　【1.2.3.4.5.6.7.8.】＿＿＿＿＿＿＿＿＿＿

18 問 16 回答５のみ　【1.2.3.4.5.6.7.8.】＿＿＿＿＿＿＿＿＿＿

19 負担な作業は？
【1．2．3．4．5．6．7．8．9．10．11．12．】＿＿＿＿＿＿＿＿＿＿

20 重点的に取り組んでいる（含予定）のものは？
【1．2．3．4．5．6．7．8．9．10．11．12．】＿＿＿＿＿＿＿＿＿＿

21 実務との乖離は？　【　】（１～３）　22 維持費用は妥当か？　【　】（１～３）

23 27002 の取り入れ程度　【　】（１～３）　24 経営層の関わり　【　】（１～３）

25 事務局メンバーは？　1．専任（　　）人　2．兼務（　　）人　3．その他（　　）人

26 初期メンバーの割合　【　】％　（100% 全員残っている←――→0%誰もいない）

27 新メンバーの教育？　【1.2.3.4.5.6.】＿＿＿＿＿＿＿＿＿＿

コンサルタントについて

28 コンサルの利用は？　取得まで【　】（１～３）　取得後【　】（４～６）

29 ISMS の理解度？	【　】（１～10）	30 セキュ技術の理解度？	【　】（１～10）
31 貴社業務の理解度？	【　】（１～10）	32 コミュニケーション？	【　】（１～10）
33 実効性のある提案？	【　】（１～10）	34 確立したコンサル手法？	【　】（１～10）
35 一貫性を持って実行？	【　】（１～10）	36 ISMS 取得に役立った？	【　】（１～10）
37 費用は妥当でしたか？	【　】（１～３）		
38 選定での重視項目は？	【　】（29～37）		
39 決定の最終判断者は？	【　】（１～５）		

中央大学
研究開発機構 内田研究室

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をご利用下さい。

審査員について

40 ISMS の理解度？　【　】（1～10）
41 セキュ技術の理解度？　【　】（1～10）
42 貴社業務の理解度？　【　】（1～10）
43 コミュニケーション？　【　】（1～10）
44 実効性のある指摘？　【　】（1～10）
45 効果･課題の確認能力？　【　】（1～10）
46 重視した項目は？　【　】(40～45)

内部監査について

47 実施頻度(除 自己点検)？　【　】（1～4）
48 内部監査体制は？　【 1.2.3.4.5.（　　）】
49 指摘事項の改善は？　【　】（1～3）
50 問 48 で 2/3 を回答した方　【 1.2.3.4.5.6.（　　）】

マネジメントレビューについて

51 開催頻度は？　【　】1～4.（　　）
52 実施形態は？　【 1.2.3.4.（　　）】

教育･社内ルールについて

53 社員の教育手段？　【 1.2.3.4.5.6.7.8.9.（　　）】
54 管理者･推進者の教育手段？　【 1.2.3.4.5.6.7.8.9.（　　）】
55 経営層の教育手段？　【 1.2.3.4.5.6.7.8.9.（　　）】
56 社員の教育の頻度は？　【 1.2.3.4.5.6.7.8.（　　）】
57 教育担当部門は？　【 1．2．3．4．5．6．7．8．9．10．11．12．13．】
58 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)
59 教育以外の啓発活動は？　【 1.2.3.4.5.6.7.8.9.10.（　　）】
60 ① 集合教育の評価方法？　【 1.2.3.4.5.（　　）】
②E-ラーニングの評価方法は？　【 1.2.3.4.5.（　　）】
61 PCの情報漏えい対策は？　【 1.2.3.4.5.6.7.8.9.10.11.12.13.14
15.（　　）】
62 社外持出しルールは？　ノートPC【 1.2.3.4.5.（　　）】
外部記録媒体【 1.2.3.4.5.（　　）】
63 社内持込、利用制限は？　【 1.2.3.4.（　　）】
64 ウイルス感染の有無？　【　】（1～3）
65 ウイルス感染原因は？　【 1.2.3.4.5.6. 】

裏面（自由記述欄）に続きます

中央大学
研究開発機構 内田研究室

回答票

貴社でISMS 認証の維持・運用を行っている中で感じている事項や疑問、課題等がございましたら、ご記入ください。

情報セキュリティマネジメントや人間を中心とした「情報セキュリティ心理学」等の研究を行っております。
ご回答内容の確認等についてご連絡をさせて頂いてもよろしければ、以下の項目をご記入下さい。

貴社名	
ご住所	
ご記入者のお名前	
電子メールアドレス	

（無記名でも構いません）

＊ご記入頂いた貴社名やご住所、ご記入者のお名前、電子メールアドレスは本調査研究及び関連イベント以外に使用致しません。

ご記入ありがとうございました。

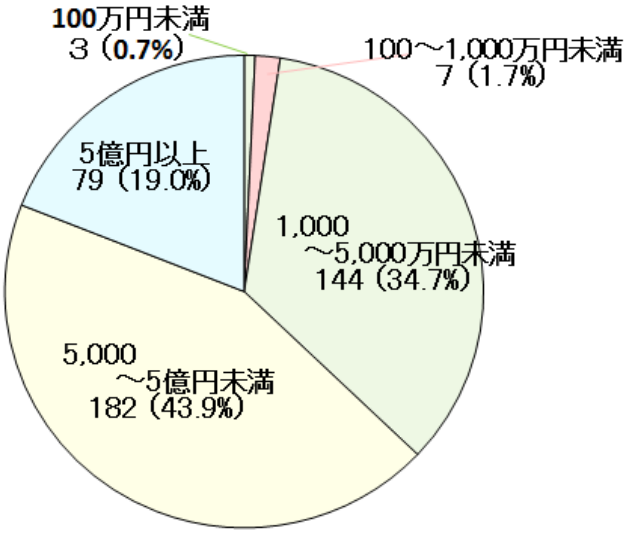
本解答用紙を郵送にて返送頂きますようお願い致します。

付録Ｂ　アンケート結果のまとめ

組織／記入者について

１．資本金（択一）

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



n=415

	有効回答数	100 万円未満	100～1,000 万円未満	1,000～5,000 万円未満	5,000 万～5 億円未満	5 億円以上
今回	415	3	7	144	182	79
（2010 年）	(%)	0.7	1.7	34.7	43.9	19.0
前回	339	1	4	109	149	76
(2008 年)	(%)	0.3	1.2	32.2	44.0	22.4
前々回	258	2	8	75	115	58
(2006 年)	(%)	0.8	3.1	29.1	44.6	22.5

1,000 万円以上の事業所が全体の 97.6% を占めており、前回は 98.6%、前々回は 96.2%となっている。

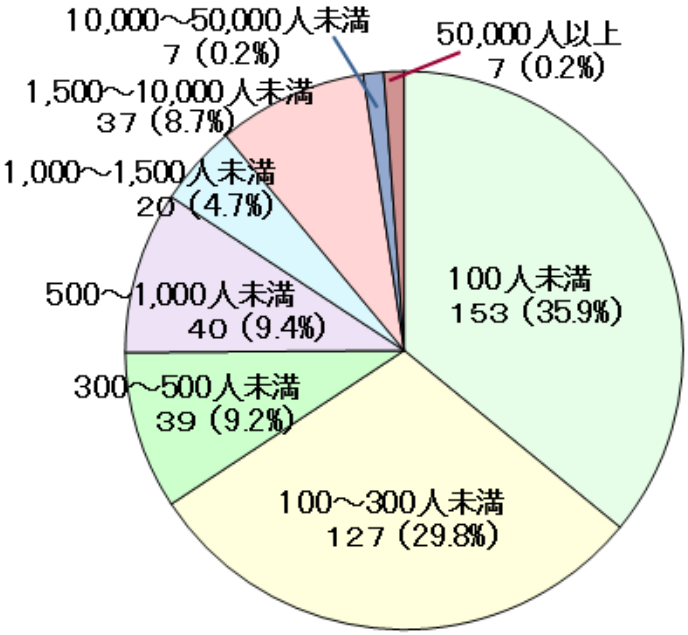
1,000 万円～5 億円未満が、それぞれ、78.6%、76.2%、73.7% となっており、資本金はこの辺りに集中している。

なお、無回答（11 事業所）には、政府・自治体、教育・学習支援、その他等が含まれている。

組織／記入者について

２．従業員数（択一）

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



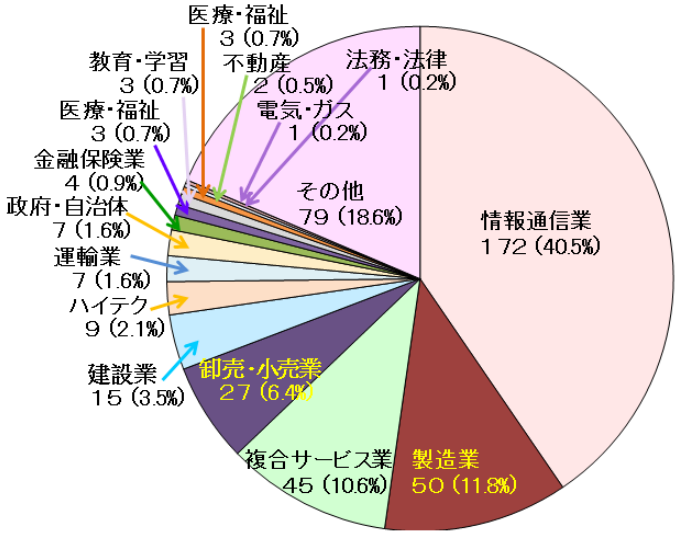
n=426

	有効回答数	100人未満	100～300人未満	300～500人未満	500～1,000人未満	1,000～1,500人未満	1,500～10,000人未満	10,000～50,000人未満	50,000人以上
今回	426	153	127	39	40	20	37	5	5
(2010年)	(%)	35.9	29.8	9.2	9.4	4.7	8.7	1.2	1.2
前回	346	134	89	36	35	12	33	5	2
(2008年)	(%)	38.7	25.7	10.4	10.1	3.5	9.5	1.4	0.6
前々回	263	84	71	28	28	11	32	8	1
(2006年)	(%)	31.9	27.0	10.6	10.6	4.2	12.2	3.0	0.4

全体の傾向としては、従前の調査と大きな差はない。65.7%の組織が従業員 300 人未満となっている。前回 64.4%、前々回 58.9% と比べると若干増加している。
小規模な組織での ISMS 認証取得の必要性が高いことを示していると考えられる。

組織／記入者について

３．貴組織の業種（択一）			
１．	建設業	９．	不動産業
２．	電気・ガス・水道業	１０．	飲食店・宿泊業
３．	運輸業	１１．	医療・福祉
４．	金融・保険業	１２．	教育・学習支援
５．	製造業	１３．	複合サービス業
６．	情報通信業	１４．	法務・法律
７．	ハイテク	１５．	公務（政府・自治体）
８．	卸売・小売業	１６．	その他



n=425

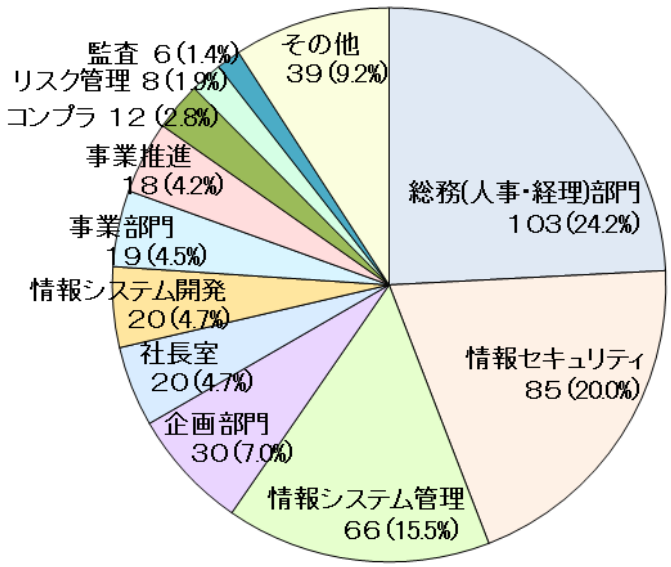
	有効回答数	6. 情報通信業	5. 製造業	13. 複合サービス業	8. 卸売小売業	1. 建設業	7. ハイテク	3. 運輸業	15. 公務（自治体）
今回	425	172	50	45	27	15	9	7	7
(2010 年)	(%)	40.5	11.8	10.6	6.4	3.5	2.1	1.6	1.6
前回	345	149	39	31	19	14	6	2	3
(2008 年)	(%)	43.2	11.3	9.0	5.5	4.1	1.7	0.6	0.9
前々回	345	108	20	39	12	15	6	4	3
(2006 年)	(%)	41.1	7.6	14.8	4.6	5.7	2.3	1.5	1.1

		4. 金融・保険業	11. 医療・福祉	12. 教育・学習支援	9. 不動産	2. 電気・ガス・水道	13. 法務・法律	10. 飲食宿泊業	16. その他
今回		4	3	3	2	1	1	0	79
(2010 年)		0.9	0.7	0.7	0.5	0.2	0.2	0.0	18.6
前回		9	4	1	3	1	1	0	63
(2008 年)		2.6	1.2	0.3	0.9	0.3	0.3	0.0	18.3
前々回		4	2	1	3	1	1	0	44
(2006 年)		0.9	0.8	0.4	1.1	0.4	0.4	0.0	16.7

組織／記入者について

４．ご記入社の所属（最も近いものを１つ選択下さい）

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



n=426

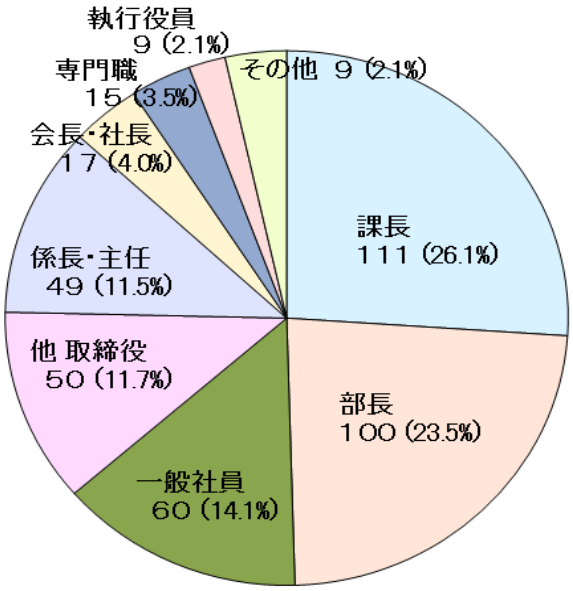
	有効回答数	1. 総務(人事･経理)部門	6. 情報セキュリティ	4. 情報システム管理	3. 企画部門	2. 社長室	5. 情報システム開発
今回(2010年)	426	103	85	66	30	20	20
	(%)	24.2	20.0	15.5	7.0	4.7	4.7
前回(2008年)	346	64	93	48	36	7	19
	(%)	18.5	26.9	13.9	10.4	2.0	5.5
前々回(2006年)	263	29	76	38	26	10	13
	(%)	11.0	28.9	14.4	9.9	3.8	4.9

		7. 事業部門	8. 事業推進	9. コンプラ	10. リスク管理	11. 監査部門	12. その他
今回(2010年)		19	18	12	8	6	39
		4.5	4.2	2.8	1.9	1.4	9.2
前回(2008年)		19	6	5	11	6	32
		5.5	1.7	1.4	3.2	1.7	9.2
前々回(2006年)		22	ー	8	2	6	33
		8.4	ー	3.0	0.8	2.3	12.5

組織／記入者について

５．記入者の役職（択一）

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



n=426

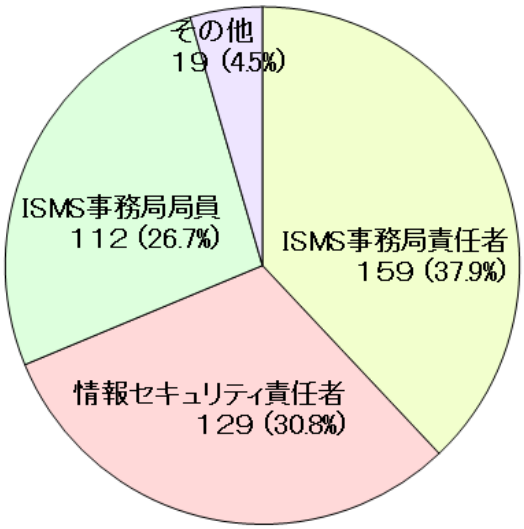
	有効回答数	5. 課長	4. 部長	8. 一般社員	2 その他取締役	6. 係長・主任	1. 会長・社長	7.専門職	3.執行役員	9. その他
今回	426	111	100	60	50	49	17	15	9	9
(2010 年)	(%)	26.1	23.5	14.1	11.7	11.5	4.0	3.5	2.1	2.1
前回	338	79	99	49	28	34	11	18	12	8
(2008 年)	(%)	23.4	29.3	14.5	8.3	10.1	3.3	5.3	3.6	2.4
前々回	264	69	66	32	―	27	35	12	17	6
(2006 年)	(%)	26.1	25.0	12.1	―	10.2	13.3	4.5	3.0	2.3

注）前々回：「会長・社長」には役員も含まれ、「執行役員」には、事業部長も含まれる

組織／記入者について

６．記入者の ISMS 運用における役割（択一）

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



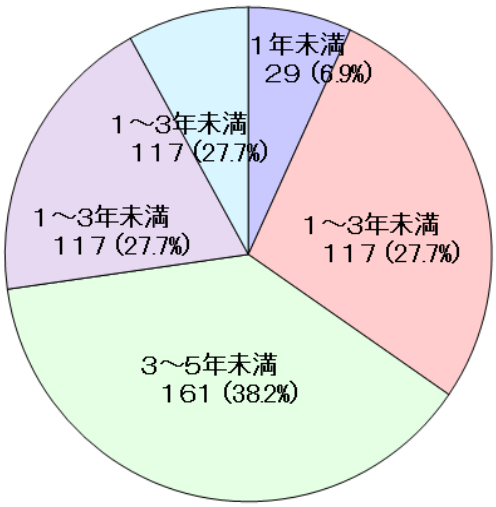
n=419

	有効回答数	2. ISMS 事務局責任者	1. 情報セキュリティ責任者	3. ISMS 事務局員（担当）	4. その他
今回（2010 年）	419	159	129	112	19
	(%)	37.9	30.8	26.7	4.5
前回（2008 年）	335	136	68	42	97
	(%)	38.2	34.6	24.2	3.0

組織／記入者について

７．記入者の ISMS 認証業務の経験年数

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



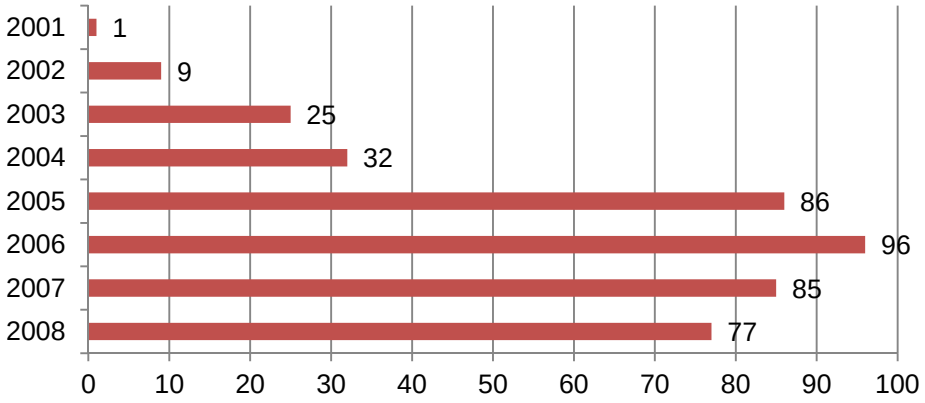
n=422

	有効回答数	1. 1年未満	2. 1年～3年未満	3. 3年～5年未満	4. 5年～7年未満	5. 7年以上
今回	422	29	117	161	81	34
(2010 年)	(%)	6.9	27.7	38.2	19.2	8.1
前回	338	31	180	95	16	16
(2008 年)	(%)	9.2	53.3	28.1	4.7	4.7
前々回	263	38	152	54	11	8
(2006 年)	(%)	14.4	57.8	20.5	4.2	3.0

ISMS 認証取得に関して

８．ISMS 初回認証取得年月は？

（ISMS 認証を取得した年月を西暦年月で、記入して下さい）



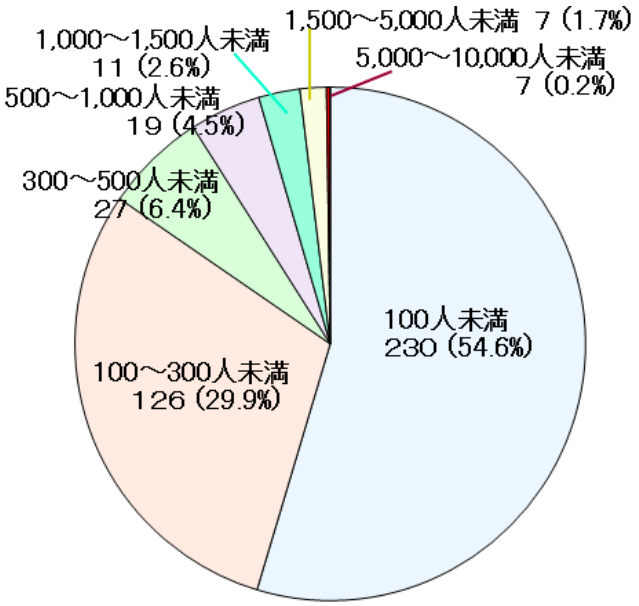
n=411

	有効回答数	2001 年	2002 年	2003 年	2004 年	2005 年	2006 年	2007 年	2008 年
今回	411	1	9	25	32	86	96	85	77
(2010 年)	(%)	0.2	2.2	6.1	7.8	20.9	23.4	20.7	18.7
前回	345	1	6	13	31	67	80	84	63
(2008 年)	(%)	0.3	1.7	3.8	9.0	19.4	23.2	24.3	18.3
前々回	264	1	11	24	39	79	108	1	
(2006 年)	(%)	0.4	4.2	9.1	14.8	29.9	40.9	0.4	

ISMS 認証取得に関して

９．認証取得従業員数

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



n=421

	有効回答数	1. 100 人未満	2. 100～300 人未満	3. 300～500 人未満	4. 500～1,000 人未満	5. 1,000～1,500 人未満	6. 1,500～5,000 人未満	7. 5,000～10,000 人未満	8. 10,000 人以上
今回	421	230	126	27	19	11	7	1	0
(2010 年)	(%)	54.6	29.9	6.4	4.5	2.6	1.7	0.2	0.0
前回	345	205	84	19	20	8	5	1	3
(2008 年)	(%)	59.4	24.3	5.5	5.8	2.3	1.4	0.3	0.9
前々回	261	154	71	16	8	2	5	2	3
(2006 年)	(%)	59.0	27.2	6.1	3.1	0.8	1.9	0.8	1.1

ISMS 認証取得に関して

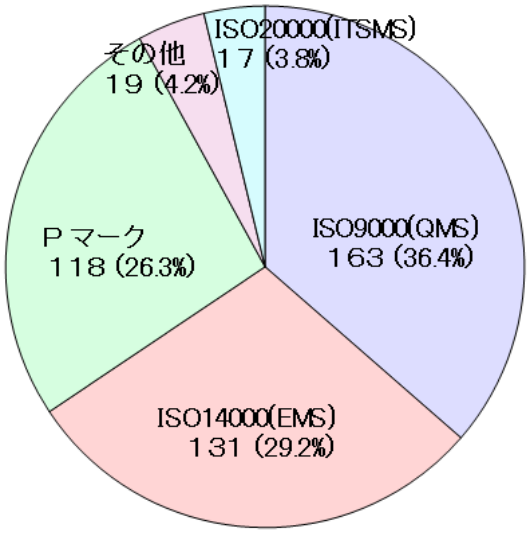
従業員⇒ 認証対象者	100 人未満	300 人未満	500 人未満	1,000 人未満	1,500 人未満	5,000 人未満	10,000 人未満	10,000 人以上	Total
100 人未満	148	46	9	12	5	7	2	1	230
300 人未満	3	75	12	9	3	18	2	1	126
500 人未満	0	1	18	4	2	2	0	0	27
1,000 人未満	0	0	0	13	3	3	0	0	19
1,500 人未満	0	0	0	1	7	3	0	0	11
5,000 人未満	0	0	0	0	0	4	1	2	7
10,000 人未満	0	0	0	0	0	0	0	1	1
10,000 人以上	0	0	0	0	0	0	0	0	0
Total	151	125	39	39	20	37	5	5	

認証対象従業員数と組織の従業員数を比較したもの。
横軸に「従業員数」、縦軸に「ISMS 認証取得対象者数」をとった。
従業員より、認証取得対象者数が多いものが一部にあるが、これは複数の企業が ISMS 認証を取得している場合と考えられる。

ISMS 認証取得に関して

１０．他の認証取得状況

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



n=421

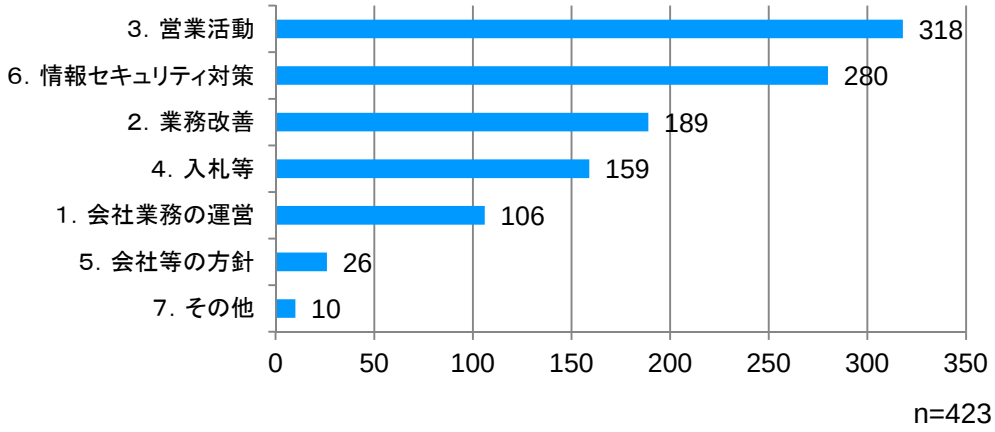
	有効回答数	1. ISO9000 QMS	2. ISO14000 EMS	3. ISO20000 ITSMS	4. Pマーク	5. その他
今回	421	163	131	17	118	19
(2010年)	(%)	36.4	29.2	3.8	26.3	4.2
前回	352	130	112	16	104	
(2008年)	(%)	36.9	31.8	4.5	29.5	
前々回	265	110	81	11	68	
(2006年)	(%)	41.5	30.6	4.2	25.7	

ISO9000(QMS)、ISO14000(EMS)、Pマークを取得しているISMS認証事業所が多い。

ISMS 認証取得に関して

１１．認証取得の主な目的（複数選択可）

１．　会社業務の運営を ISMS 認証に基づいたものにするため
２．　ISMS の考え方を取入れ、業務の改善を狙ったため
３．　ISMS 認証取得が営業活動に有利になる、あるいは不利にならないことを狙った
４．　入札等で 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

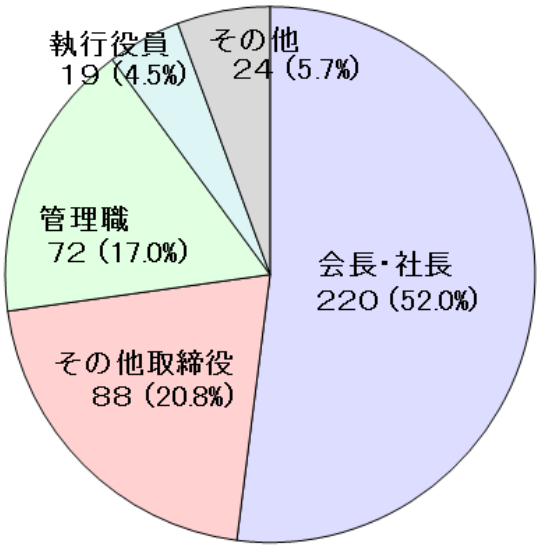


	有効回答数	3. 営業活動	6. セキュリティ対策	2. 業務改善	4. 入札	1. 業務運営	5. 方針	7. その他
今回	423	318	280	189	159	106	26	10
(2010 年)	(%)	75.2	66.2	44.7	37.6	25.1	6.1	2.4
前回	352	267	244	83	94	66	21	4
(2008 年)	(%)	75.9	69.3	23.6	26.7	18.8	6.0	1.1
前々回	264	199	189	58	77	65	15	10
(2006 年)	(%)	75.4	71.6	22.0	29.2	24.6	5.7	3.8

ISMS 認証取得に関して

１２．ISMS 認証取得の発案者は？

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



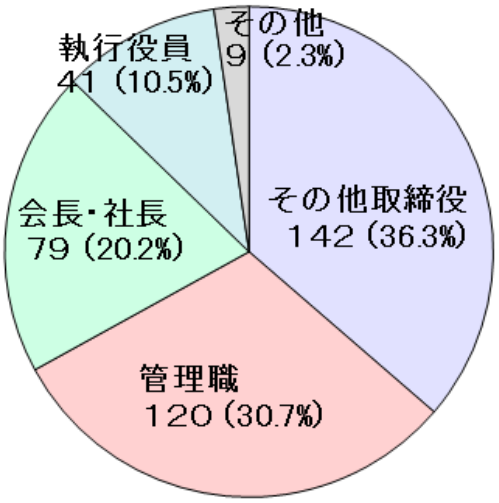
n=423

	有効回答数	1. 会長・社長	2. 他 取締役	4. 管理職	3. 執行役員	5. その他
今回	423	220	88	72	19	24
(2010 年)	(%)	52.0	20.8	17.0	4.5	5.7
前回	347	191	66	54	20	16
(2008 年)	(%)	55.0	19.0	15.6	5.8	4.6

ISMS 認証取得に関して

１３．ISMS 認証の運用責任者は？

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



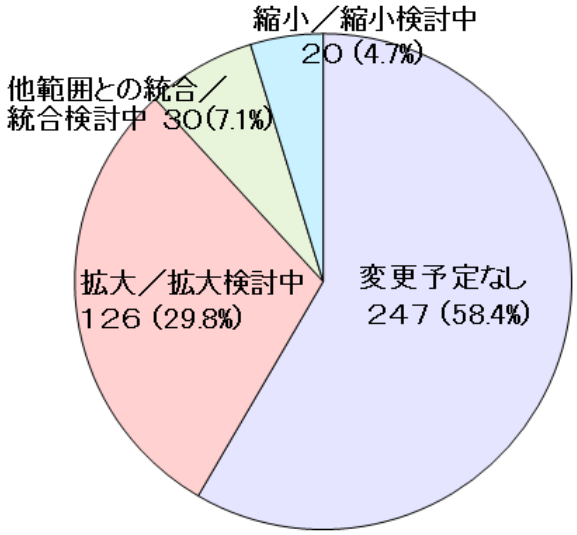
n=423

	有効回答数	2. 他 取締役	4. 管理職	1. 会長・社長	3. 執行役員	5. その他
今回 (2010 年)	391	142	120	79	41	9
	(%)	36.3	30.7	20.2	10.5	2.3
前回 (2008 年)	347	136	97	68	42	5
	(%)	39.1	27.9	19.5	12.1	1.4

ISMS 認証取得に関して

１４．ISMS 認証取得後に認証範囲の変更／変更の検討を行っていますか？

１．　縮小／縮小を検討中
２．　拡大／拡大を検討中
３．　他範囲との統合／統合検討中
４．　変更予定なし

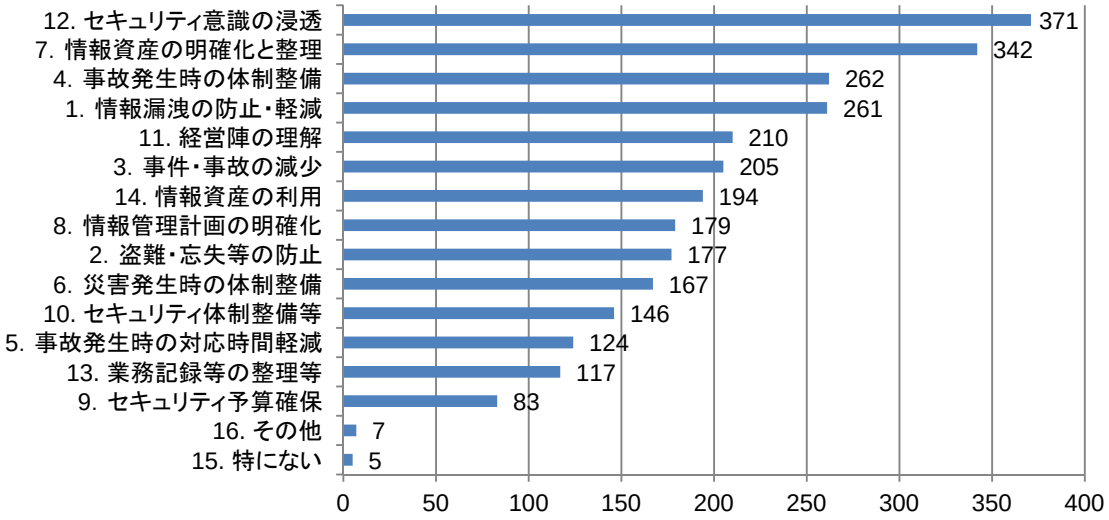


n=423

	有効回答数	1. 縮小・縮小検討中	2. 拡大・拡大検討中	3. 他範囲と統合 統合検討中	4. 変更予定なし
今回 (2010 年)	423	20	126	30	247
	(%)	4.7	29.8	7.1	58.4
前回 (2008 年)	348	13	114	19	202
	(%)	3.7	32.8	5.5	58.0

ISMS 認証取得の効果・影響

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

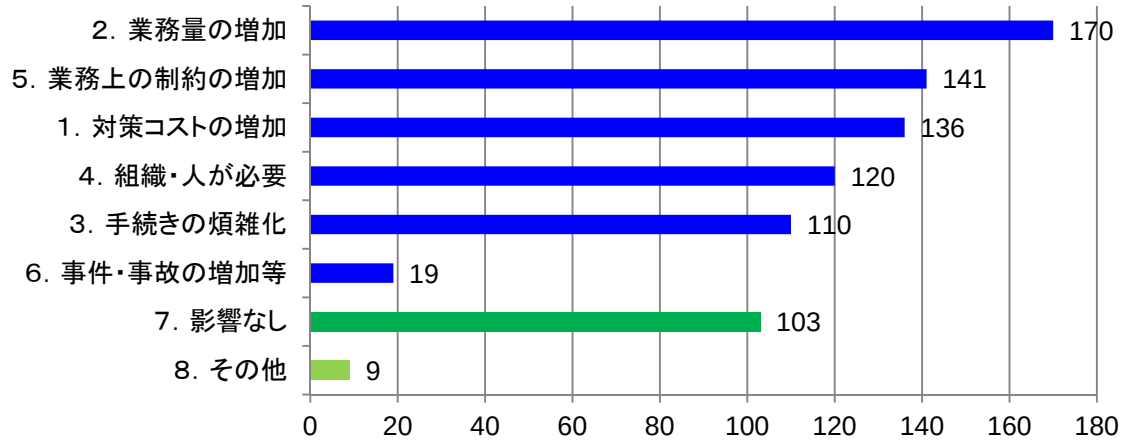


	有効回答数	12. セキュ意識	7. 情報資産	4. 事故発生時	1. 情報漏えい	11. 経営の理解	3. 事件事故減少	14. 情報資産利用	8. 情報管理計画
今回	426	371	342	262	261	210	205	194	179
(2010 年)	(%)	87.1	80.3	61.5	61.3.	49.3	48.1	45.5	42.0
前回	352	307	266	188	177	142	76	145	128
(2008 年)	(%)	87.2	75.6	53.4	50.3	40.3	21.6	41.2	36.4
前々回		232	205	149	146	114	54	117	113
(2006 年)		87.9	77.7	56.4	55.3	43.2	20.5	44.3	42.8

2. 盗難防止	6. 災害発生時	10. セキュリティ体制	5. 事故対応時間	13. 業務記録等	9. セキュ予算	16. その他	15. 特にない
177	167	146	124	117	83	7	5
41.5	39.2	34.3	29.1	27.5	19.5	1.6	1.2
124	114	114	62	108	54	5	4
35.2	32.4	32.4	17.6	30.7	15.3	1.4	1.1
106	99	77	57	97	49	8	3
40.2	37.5	29.2	21.6	36.7	18.6	3.0	1.1

ISMS 認証取得の効果・影響

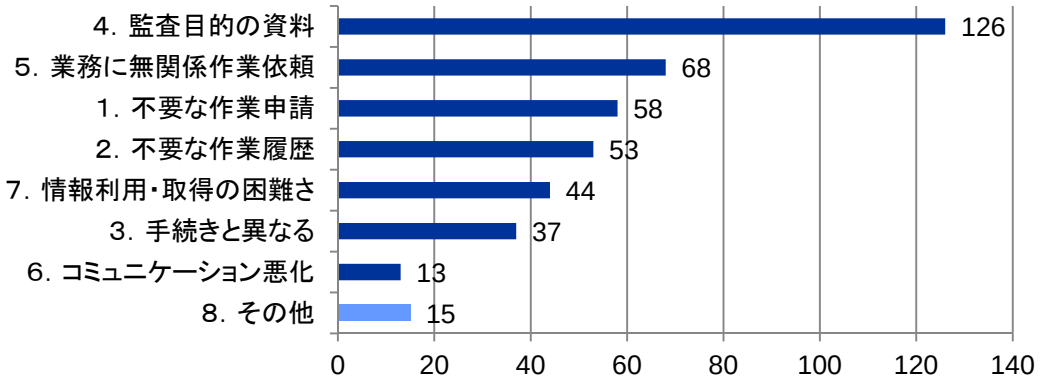
１６．ISMS 認証取得での想定外の影響は？　（複数選択可）	
1.　情報セキュリティ対策にかけるコストの増加	5.　業務上の制約の増加
2.　業務量の増加	6.　セキュリティ事件・事故の増加／減少しない
3.　手続きの煩雑化・業務効率の低下	7.　業務への影響は特にない
4.　ISMS を担当する組織・人が必要になった	8.　その他



	有効回答数	2. 業務量の増加	5. 制約の増加	1. 対策コスト増加	4. 組織・人が必要	3. 手続き煩雑化	6. 事件・事故増加	7. 影響なし	8. その他
今回	426	170	141	136	120	110	19	103	9
(2010 年)	(%)	39.9	33.1	31.9	28.2	25.8	4.5	24.2	2.1
前回	352	131	109	102	110	78	7	79	7
(2008 年)	(%)	37.2	31.0	29.0	31.3	22.2	2.0	22.4	2.0
前々回	264	105	97	91	97	61	9	46	6
(2006 年)	(%)	39.8	36.7	34.5	36.7	23.1	3.4	17.4	2.3

ISMS 認証取得の効果・影響

１７．問 16 の「２」、「３」を選択した⇒具体的な内容は？　（複数選択可）	
1.　不要な作業申請等の作成	5.　事務局等からの業務に無関係な依頼作業の増加
2.　不要な作業履歴の記録	6.　厳格な入退出管理で他部門とのコミュニケーションの悪化
3.　実際の手続きとマニュアルが異なる	7.　情報を利用・取得しづらくなった
4.　監査目的の資料作成	8.　その他

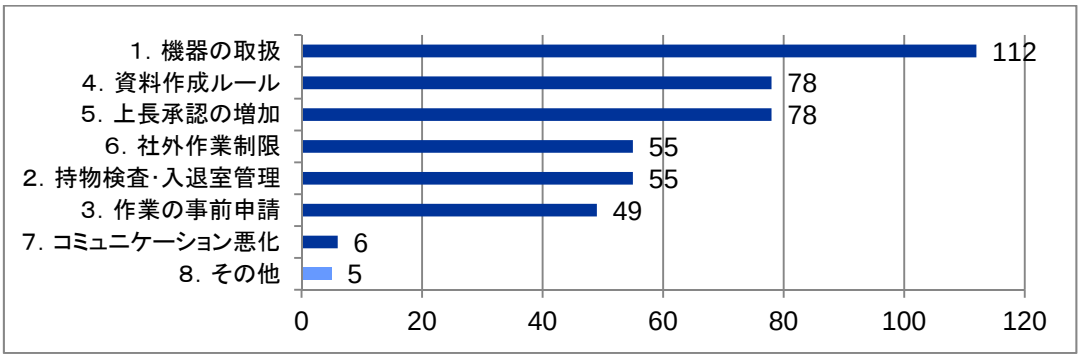


	有効回答数	4. 監査目的資料	5. 業務無関係資料	1. 不要な作業申請等	2. 不要な作業履歴	7. 情報利用の困難さ	3. 手続きと異なる	6. コミュニケーション悪化	8. その他
今回	215	126	68	58	58	44	37	13	15
(2010 年)	(%)	58.6	31.6	27.0	24.7	20.5	17.2	6.0	7.0
前回	162	87	55	35	41	20	24	6	19
(2008 年)	(%)	53.7	34.0	21.6	25.3	12.3	14.8	3.7	11.7
前々回	264	64	55	30	31	20	18	12	20
(2006 年)	(%)	38.6	33.1	18.1	18.7	12.0	10.8	7.2	12.0

ISMS 認証取得の効果・影響

１８．問 16 の「５」を選択 ⇒現場での業務上の制約はありますか？ （複数選択可）

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

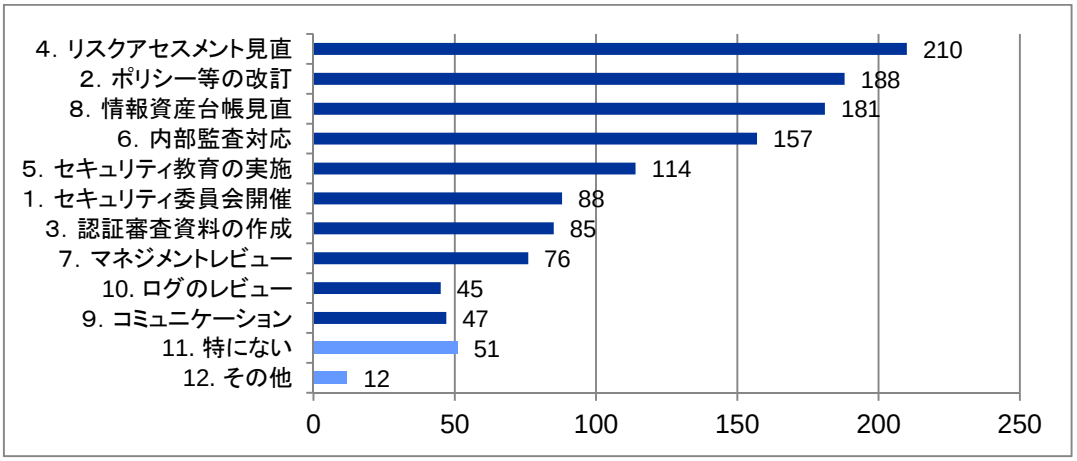


	有効回答数	1. 機器の取扱	4. 資料作成 ルール	5. 上長の承認増加	6. 社外作業の制限	2. 持ち物検査等	3. 作業の事前申請	7. ｺﾐｭﾆｹｰｼｮﾝ悪化	8. その他
今回	141	112	78	78	55	55	49	6	5
(2010 年)	(%)	79.4	55.3	55.3	39.0	39.0	34.8	4.3	3.5
前回	110	68	44	59	24	28	19	0	0
(2008 年)	(%)	61.8	40.0	53.6	21.8	25.5	17.3	0.0	0.0
前々回		80	50	58	32	40	23	7	2
(2006 年)	(%)	82.5	51.5	59.8	33.0	41.2	23.7	7.2	2.1

ISMS 認証取得の効果・影響

１９．ISMS 認証取得後の運用で負担になっている作業は？　（複数選択可）

1. セキュリティ委員会の開催
2. ポリシー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. 特にない
12. その他



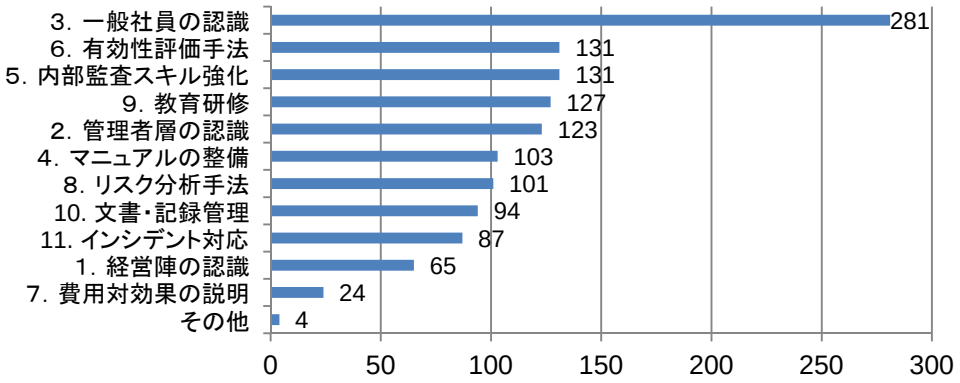
	有効回答数	4. リスクアセスメント	2. ポリシー等の改訂	8. 情報資産の見直し	6. 内部監査対応	5. セキュリティ教育	1. セキュリティ委員会
今回	420	210	188	181	157	114	88
(2010 年)	(%)	50.0	44.8	43.1	37.4	27.1	21.0
前回	352	178	133	158	131	95	66
(2008 年)	(%)	50.6	37.8	44.9	37.2	27.0	18.8
前々回	264	142	139	132	109	95	56
(2006 年)	(%)	53.8	52.7	50.0	41.3	36.0	21.2

3. 認証審査資料の作成	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. 特にない	12. その他
85	76	45	47	51	12
20.2	18.1	10.7	11.2	12.1	2.9
62	45	43	36	36	9
17.6	12.8	12.2	10.2	10.2	2.6
36	45	45	29	17	6
13.6	17.0	17.0	11.0	6.4	2.3

ISMS 認証取得の効果・影響

２０．ISMS の効果を高めるため重点的に取り組んでいるものは？（複数選択可）
※はツール導入を含む

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

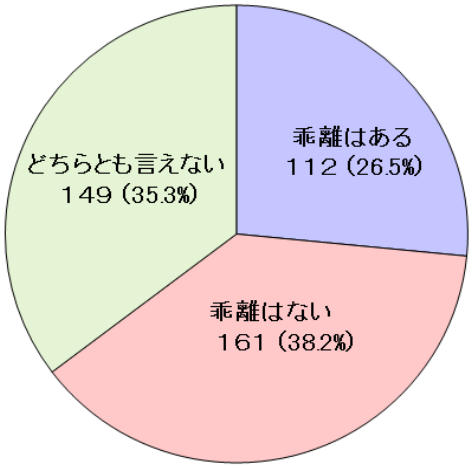


	有効回答数	3. 一般社員の認識	6. 有効性評価手法	5. 内部監査人スキル強化	9. 教育研修の改善	2. 管理者層の認識	4. マニュアルの整備
今回	416	281	131	131	127	123	103
(2010 年)	(%)	67.5	31.5	31.5	30.5	29.6	24.8
前回	352	220	112	91	102	76	79
(2008 年)	(%)	62.5	31.8	25.9	29.0	21.6	22.4
前々回	264	183	108	61	95	76	83
(2006 年)	(%)	69.3	40.9	23.1	36.0	28.8	31.4

8. リスク分析手法	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	12. その他
101	94	87	65	24	4
24.3	22.6	20.9	15.6	5.8	1.0
73	73	61	35	17	9
20.7	20.7	17.3	9.9	4.8	2.6
62	62	54	27	12	4
23.5	23.5	20.5	10.2	4.5	1.5

ISMS 認証取得の効果・影響

２１．実業務と ISMS の乖離（ダブルスタンダードの発生）はありますか？（択一）
1. 乖離はある
2. 乖離はない
3. どちらもと言えない

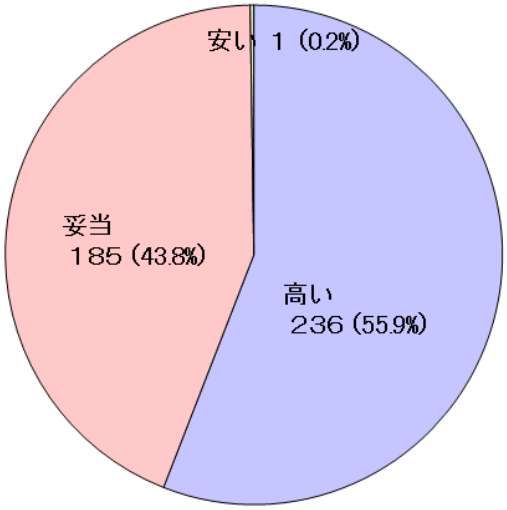


	有効回答数	1. 乖離はある	2. 乖離はない	3. どちらもと言えない
今回（2010 年）	422	112	161	149
	(%)	26.5	38.2	35.3
前回（2008 年）	347	41	172	134
	(%)	11.8	49.6	38.6

ISMS 認証取得の効果・影響

２２．ISMS の維持費用は妥当だと思いますか

1. 高い
2. 妥当
3. 安い

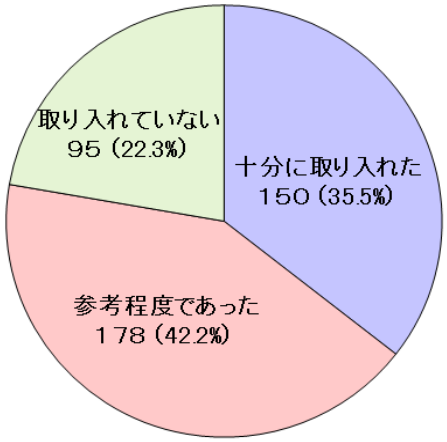


	有効回答数	1. 高い	2. 妥当	3. 安い
今回 (2010 年)	422	236	185	1
	(%)	55.9	43.8	0.2
前回 (2008 年)	347	148	191	8
	(%)	42.7	55.0	2.3

ISMS 認証取得の効果・影響

２３．ISO27002 はどこまで取り入れましたか？

1. 十分に取り入れた
2. 参考程度であった
3. 取り入れていない

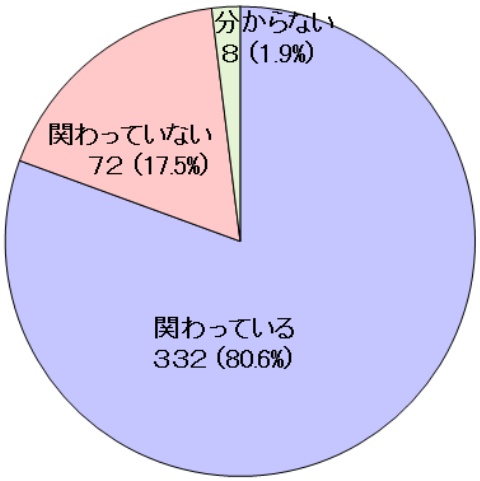


	有効回答数	1. 十分に取り入れた	2. 参考程度であった	3. 取り入れていない
今回（2010 年）	422	150	178	94
	(%)	35.5	42.2	22.3
前回（2008 年）	348	125	157	66
	(%)	35.9	45.1	19.0

ISMS 認証取得の効果・影響

２４．ISMS の継続的な運用のため、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. 関わっている
2. 関わっていない
3. わからない

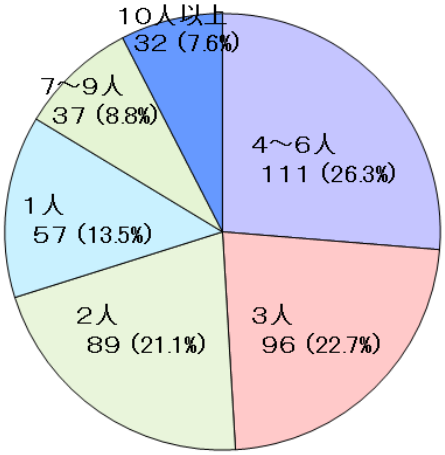


n=412

	有効回答数	1. 関わっている	2. 関わっていない	3. わからない
今回	412	332	72	8
(2010 年)	(%)	80.6	17.5	1.9
前回	344	262	77	5
(2008 年)	(%)	76.2	22.4	1.5
前々回	259	213	41	5
(2006 年)	(%)	82.2	15.8	1.9

ISMS 認証取得の効果・影響

２５．現在の 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（　）

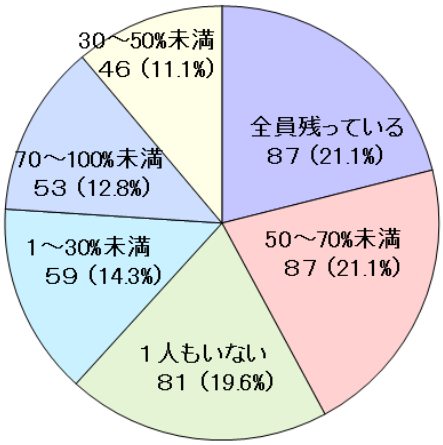


	有効回答数	4. 4～6人	3. 3 人	2 2 人	1. 1 人	5. 7～9人	6. 10人以上
今回	422	111	96	89	57	37	32
(2010 年)	(%)	26.3	22.7	21.1	13.5	8.8	7.6
前回	347	93	64	89	49	34	18
(2008 年)	(%)	26.8	18.4	25.6	14.1	9.8	5.2
前々回		64	63	67	29	28	13
(2006 年)	(%)	24.2	23.9	25.4	11.0	10.6	4.9

	合計	専任	兼務	その他	専任+兼務+その他
一人の場合	57	12	45	0	0
二人の場合	89	6	69	0	14
三人の場合	96	7	73	1	25
4～6人の場合	111	9	76	1	25
7～9人の場合	37	0	28	0	9
10 人以上	32	0	22	0	10

ISMS 認証取得の効果・影響

２６．現在の事務局に初回認証取得時メンバーが残っている割合は？
（　　）%（100%:全員残っている ←→0%:誰も残っていない）

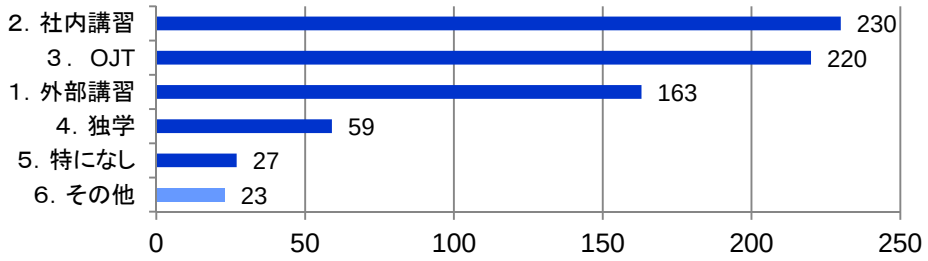


	有効回答数	1. 全員残り	3. 50～70%未満	6. 一人もいない	5. 1～30%未満	2. 70～100%未満	4. 30～50%未満
今回	413	87	87	81	59	53	46
(2010 年)	(%)	21.1	21.1	19.6	14.3	12.8	11.1

ISMS 認証取得の効果・影響

２７．事務局新メンバーに対する ISMS 関連スキル教育について（複数選択可）

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

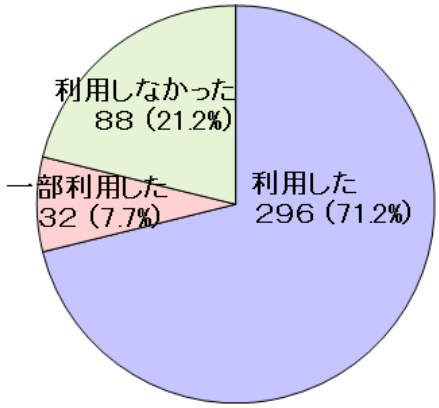


	有効回答数	2. 社内講習	3. OJT	1. 外部講習	4. 独学	5. 特になし	6. その他
今回	415	230	220	163	59	27	23
(2010 年)	(%)	55.4	53.0	39.3	14.2	6.5	5.5
前回	352	219	168	113	38	13	8
(2008 年)	(%)	62.2	47.7	32.1	10.8	3.7	2.3
前々回		184	110	85	19	7	12
(2006 年)	(%)	69.7	41.7	32.2	7.2	2.7	4.5

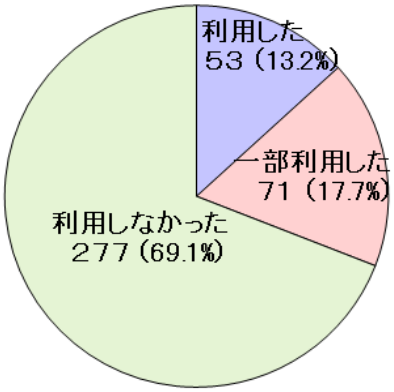
ISMS 認証取得の効果・影響

２８．コンサルタントを利用しましたか？　（択一）

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



認証取得まで



認証取得後

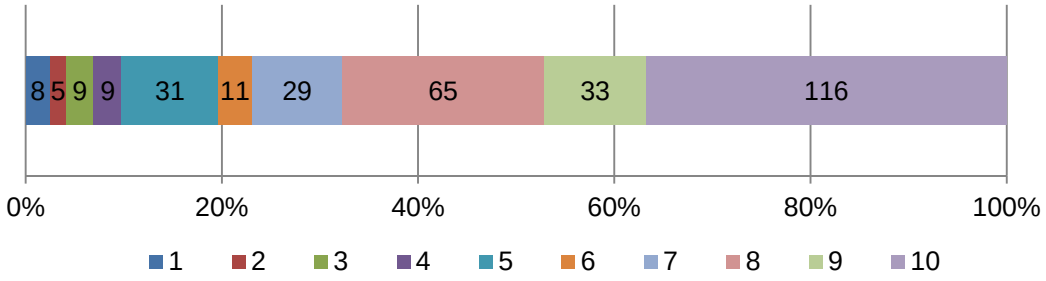
	有効回答数	1. 利用した	2. 一部利用	3. 利用しなかった
今回	416	296	32	88
(2010 年)	(%)	71.2	7.7	21.2
前回	347	253	29	65
(2008 年)	(%)	72.9	8.4	18.7
前々回	263	182	29	52
(2006 年)	(%)	69.2	11.0	19.8

有効回答数	1. 利用した	2. 一部利用	3. 利用しなかった
401	53	71	277
(%)	13.2	17.7	69.1
336	59	59	218
(%)	17.6	17.6	64.9
255	44	58	153
(%)	17.3	22.7	60.0

コンサルタントについて

２９．ISMS の理解度を 10 段階で評価して下さい。　（１：低い ←→ 10：高い）

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



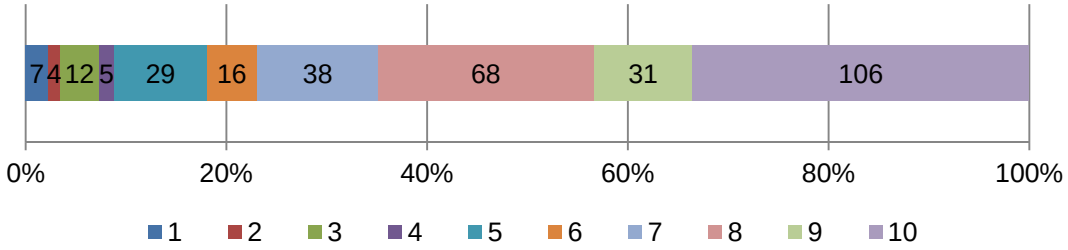
ISMS 理解度：平均値：7.85

	有効回答数	1	2	3	4	5	6	7	8	9	10
今回	316	8	5	9	9	31	11	29	65	33	116
(2010 年)	(%)	2.5	1.6	2.8	2.8	9.8	3.5	9.2	20.6	10.4	36.7
前回	273	3	5	2	1	11	10	25	64	41	111
(2008 年)	(%)	1.1	1.8	0.7	0.4	4.0	3.7	9.2	23.4	15.0	40.7

コンサルタントについて

３０．情報セキュリティの理解度。　（１：低い ←→ 10：高い）

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



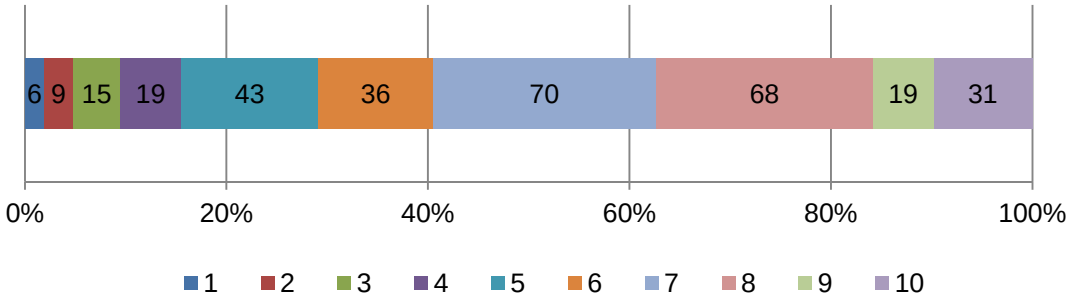
情報セキュリティの理解度：　平均値：7.79

	有効回答数	1	2	3	4	5	6	7	8	9	10
今回	316	7	4	12	5	29	16	38	68	31	106
(2010年)	(%)	2.2	1.3	3.8	1.6	9.2	5.1	12.0	21.5	9.8	33.5
前回	274	5	5	2	3	21	22	39	58	39	80
(2008年)	(%)	1.8	1.8	0.7	1.1	7.7	8.0	14.2	21.2	14.2	29.2

コンサルタントについて

３１．貴組織業務の理解度。　（１：低い ←→ 10：高い）

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



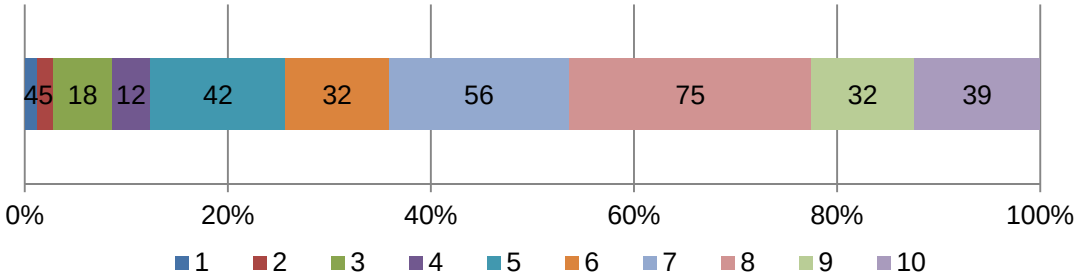
貴組織業務の理解度：　平均値：6.62

	有効回答数	1	2	3	4	5	6	7	8	9	10
今回	316	6	9	15	19	43	36	70	68	19	31
(2010年)	(%)	1.9	2.8	4.7	6.0	13.6	11.4	22.2	21.5	6.0	9.8
前回	272	6	9	15	12	37	19	46	59	16	53
(2008年)	(%)	2.2	3.3	5.5	4.4	13.6	7.0	16.9	21.7	5.9	19.5

コンサルタントについて

３２．コミュニケーション　（１：低い ←→ 10：高い）

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



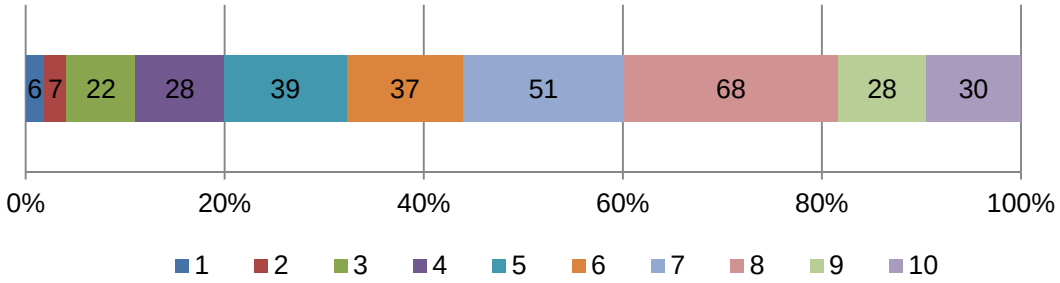
コミュニケーション：　平均値：6.95

	有効回答数	1	2	3	4	5	6	7	8	9	10
今回	315	4	5	18	12	42	32	56	75	32	39
(2010年)	(%)	1.3	1.6	5.7	3.8	13.3	10.2	17.8	23.8	10.2	12.4
前回	272	3	4	5	6	28	14	33	73	27	81
(2008年)	(%)	1.1	1.5	1.8	2.2	10.2	5.1	12.0	26.6	9.9	29.6

コンサルタントについて

３３．実効性のある提案　（１：低い ←→ 10：高い）

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



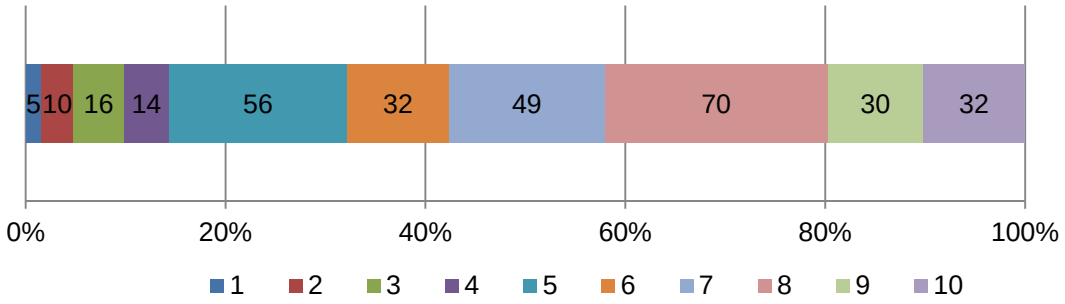
実効性のある提案：　平均値：6.54

	有効回答数	1	2	3	4	5	6	7	8	9	10
今回	316	6	7	22	28	39	37	51	68	28	30
(2010年)	(%)	1.9	2.2	7.0	8.9	12.3	11.7	16.1	21.5	8.9	9.5
前回	273	5	4	12	13	26	24	37	68	26	59
(2008年)	(%)	1.8	1.5	4.4	4.7	9.5	8.8	13.5	24.8	9.5	21.5

コンサルタントについて

３４．確立したコンサル手法　（１：低い ←→ 10：高い）

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



確立したコンサル手法：　平均値：6.67

	有効回答数	1	2	3	4	5	6	7	8	9	10
今回	314	5	10	16	14	56	32	49	70	30	32
(2010年)	(%)	1.6	3.2	5.1	4.5	17.8	10.2	15.6	22.3	9.6	10.2
前回	272	4	3	10	9	31	18	33	60	32	72
(2008年)	(%)	1.5	1.1	3.7	3.3	11.4	6.6	12.1	22.1	11.8	26.5

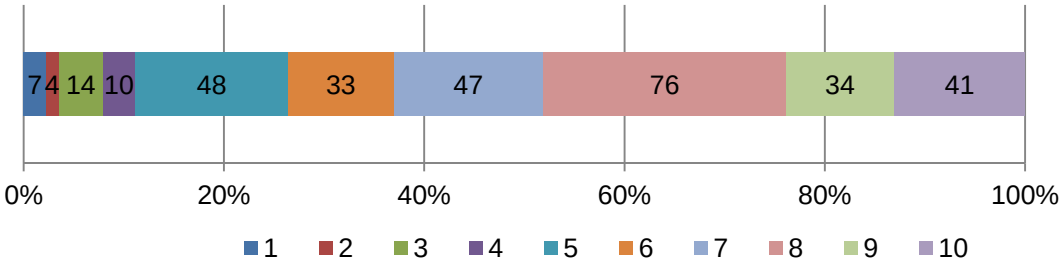
コンサルタントについて

３５．一貫性を持ったコンサルテーション　（１：低い ←→ 10：高い）

理解していない ←

1	2	3	4	5	6	7	8	9	10

→ 理解していた



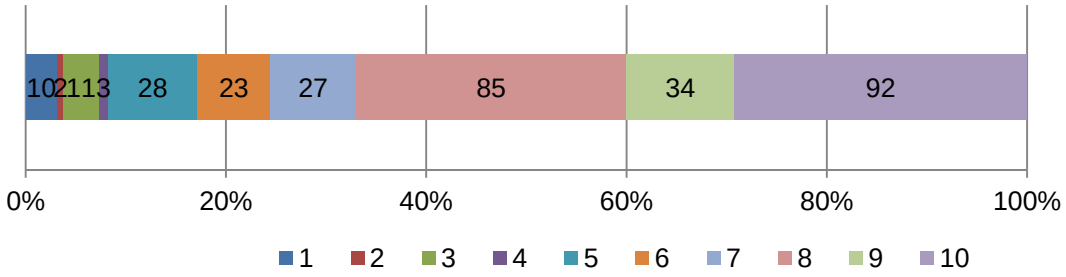
一貫性を持ったコンサルテーション：　平均値：6.97

	有効回答数	1	2	3	4	5	6	7	8	9	10
今回	314	7	4	14	10	48	33	47	76	34	41
(2010年)	(%)	2.2	1.3	4.5	3.2	15.3	10.5	15.0	24.2	10.8	13.1
前回	272	4	6	11	8	21	14	41	65	29	73
(2008年)	(%)	1.5	2.2	4.0	2.9	7.7	5.1	15.1	23.9	10.7	26.8

コンサルタントについて

３６．ISMS 認証取得に役立った　（１：低い ←→ 10：高い）

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



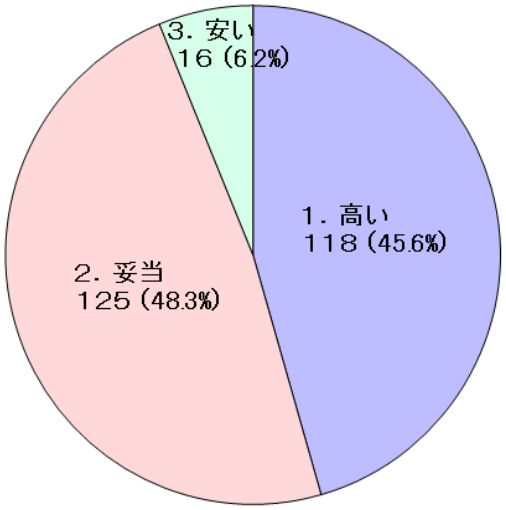
ISMS 認証取得に役立った：　平均値：7.72

	有効回答数	1	2	3	4	5	6	7	8	9	10
今回	315	10	2	11	3	28	23	27	85	34	92
(2010 年)	(%)	3.2	0.6	3.5	1.0	8.9	7.3	8.6	27.0	10.8	29.2
前回	274	3	3	5	4	10	15	30	55	42	107
(2008 年)	(%)	1.1	1.1	1.8	1.5	3.6	5.5	10.9	20.1	15.3	39.1

コンサルタントについて

３７．費用の妥当性

１．高い　　２．妥当　　２．安い

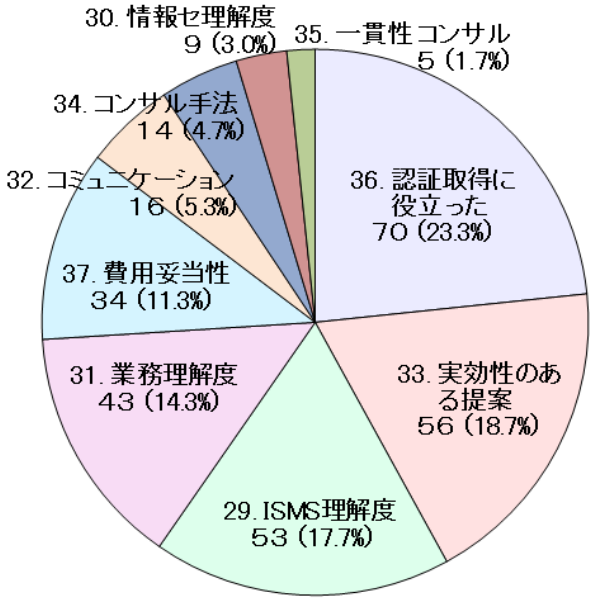


費用の妥当性：平均値：

	有効回答数	1．高い	2．妥当	3．安い
今回（2010年）	259	118	125	16
	(%)	45.6	48.3	6.2
前回（2008年）	249	91	144	14
	(%)	36.5	57.8	5.6

コンサルタントについて

３８．コンサルタント選定で最も重視した項目は、上記（29～37）のどれか？（択一）
（29～37）



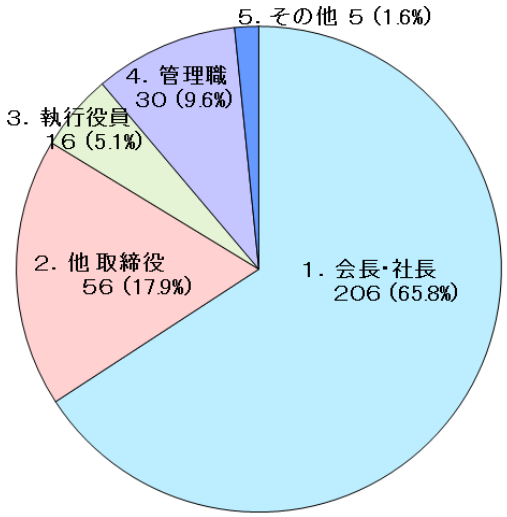
n=300

	有効回答数	36	33	29	31	37	32	34	30	35
今回	300	70	56	53	43	34	16	14	9	5
(2010年)	(%)	23.3	18.7	17.7	14.3	11.3	5.3	4.7	3.0	1.7

コンサルタントについて

３９．コンサルタント導入の最終判断者は？（択一）

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

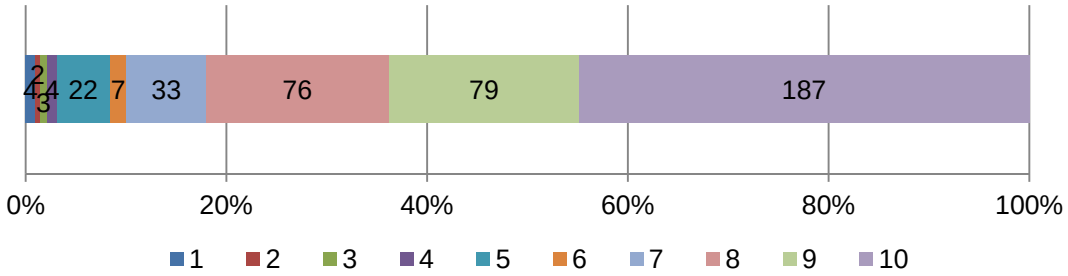


	有効回答数	1. 会長･社長	2. 他 取締役	3. 執行役員	4. 管理職	5. その他
今回	313	206	56	16	30	5
(2010 年)	(%)	65.8	17.9	5.1	9.6	1.6
前回	337	215	47	15	48	12
(2008 年)	(%)	63.8	13.9	4.5	14.2	3.6

ISMS 審査員について

４０．ISMS の理解度　（１：低い ←→ 10：高い）

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



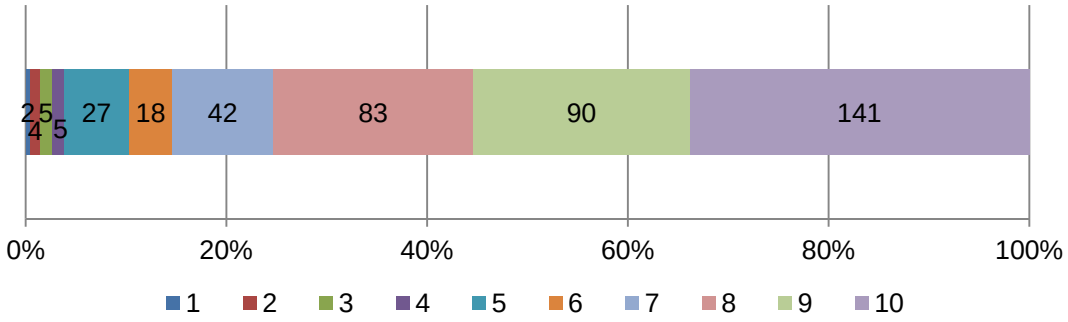
ISMS の理解度：　平均値：8.65

	有効回答数	1	2	3	4	5	6	7	8	9	10
今回	417	4	2	3	4	22	7	33	76	79	187
(2010 年)	(%)	1.0	0.5	0.7	1.0	5.3	1.7	7.9	18.2	18.9	44.8
前回	347	1	0	1	0	2	4	17	45	68	209
(2008 年)	(%)	0.3	0.0	0.3	0.0	0.6	1.2	4.9	13.0	19.7	60.6

ISMS 審査員について

４１．セキュリティ技術の理解度　（１：低い ←→ 10：高い）

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



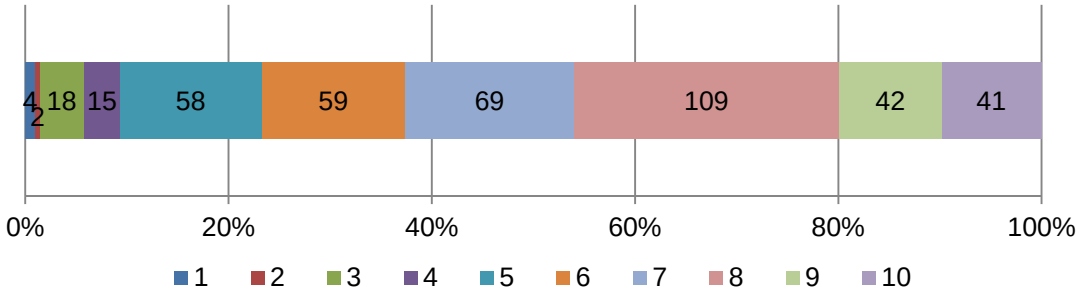
セキュリティ技術の理解度：　平均値：8.31

	有効回答数	1	2	3	4	5	6	7	8	9	10
今回	417	2	4	5	5	27	18	42	83	90	141
(2010 年)	(%)	0.5	1.0	1.2	1.2	6.5	4.3	10.1	19.9	21.6	33.8
前回	347	0	1	2	2	5	11	34	66	63	163
(2008 年)	(%)	0.0	0.3	0.6	0.6	1.4	3.2	9.9	19.1	18.3	47.2

ISMS 審査員について

４２．貴組織の業務の理解度　（１：低い ←→ 10：高い）

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



貴組織の業務の理解度：　平均値：6.98

	有効回答数	1	2	3	4	5	6	7	8	9	10
今回	417	4	2	18	15	58	59	69	109	42	41
(2010 年)	(%)	1.0	0.5	4.3	3.6	13.9	14.1	16.5	26.1	10.1	9.8
前回	346	0	4	11	4	23	32	63	99	43	67
(2008 年)	(%)	0.0	1.2	3.2	1.2	6.7	9.3	18.3	28.7	12.5	19.4

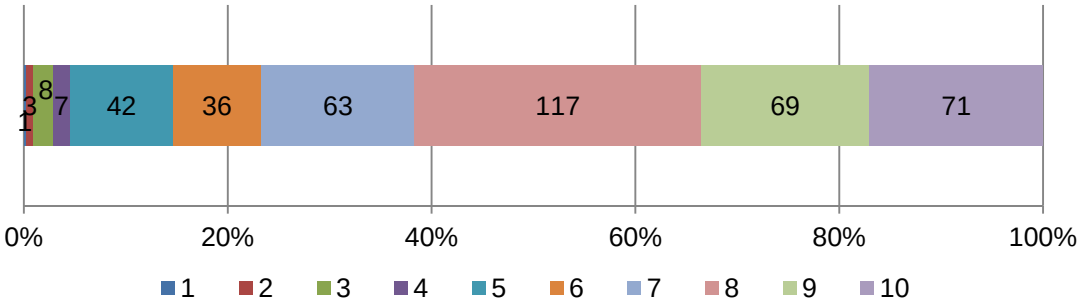
ISMS 審査員について

４３．コミュニケーション　（１：低い ←→ 10：高い）

理解していない ←

1	2	3	4	5	6	7	8	9	10

→ 理解していた



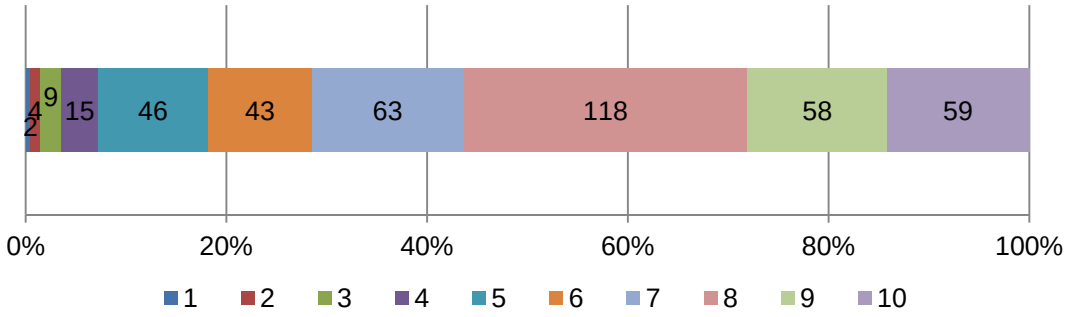
コミュニケーション：　平均値：7.66

	有効回答数	1	2	3	4	5	6	7	8	9	10
今回	417	1	3	8	7	42	36	63	117	69	71
(2010 年)	(%)	0.2	0.7	1.9	1.7	10.1	8.6	15.1	28.1	16.5	17.0
前回	347	1	2	3	7	13	21	32	101	62	105
(2008 年)	(%)	0.3	0.6	0.9	2.0	3.8	6.1	9.3	29.3	18.0	30.4

ISMS 審査員について

４４．実効性のある指摘　（１：低い ←→ 10：高い）

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



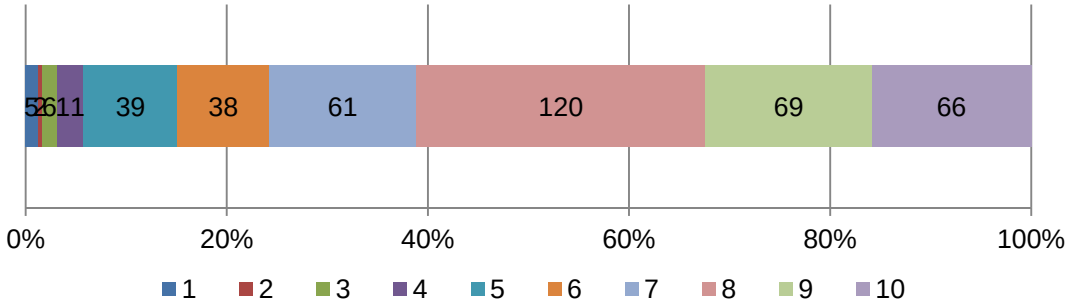
実効性のある指摘：　平均値:7.39

	有効回答数	1	2	3	4	5	6	7	8	9	10
今回	417	2	4	9	15	46	43	63	118	58	59
(2010年)	(%)	0.5	1.0	2.2	3.6	11.0	10.3	15.1	28.3	13.9	14.1
前回	347	1	2	4	7	16	21	46	92	62	96
(2008年)	(%)	0.3	0.6	1.2	2.0	4.6	6.1	13.3	26.7	18.0	27.8

ISMS 審査員について

４５．効果や課題を確認する能力　（１：低い ←→ 10：高い）

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

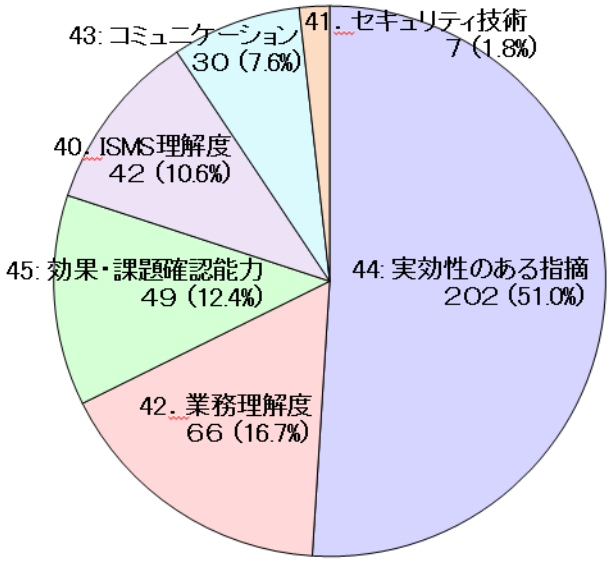


効果や課題を確認する能力：　平均値：7.58

	有効回答数	1	2	3	4	5	6	7	8	9	10
今回	417	5	2	6	11	39	38	61	120	69	66
(2010 年)	(%)	1.2	0.5	1.4	2.6	9.4	9.1	14.6	28.8	16.5	15.8
前回	346	1	1	3	3	19	14	37	92	59	117
(2008 年)	(%)	0.3	0.3	0.9	0.9	5.5	4.1	10.7	26.7	17.1	33.9

ISMS 審査員について

４６．ISMS 審査員について、最も重視する項目（上記 40～45）のどれですか？

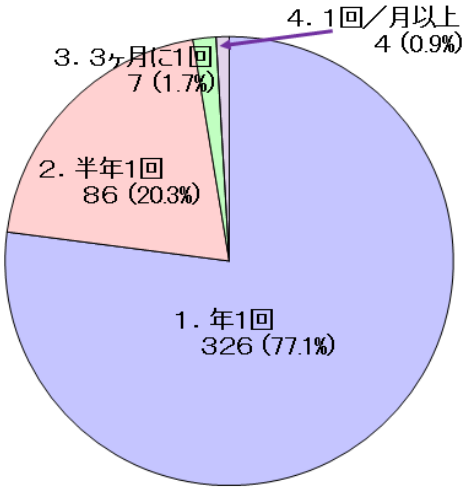


	有効回答数	44	42	45	40	43	41
今回	396	202	66	49	42	30	7
(2010 年)	(%)	51.0	16.7	12.4	10.6	7.6	1.8

内部監査について

４７．内部監査の実施頻度（除 自己点検）

１．　年１回
２．　半年に１回
３．　３ヶ月に１回
４．　１回／月以上

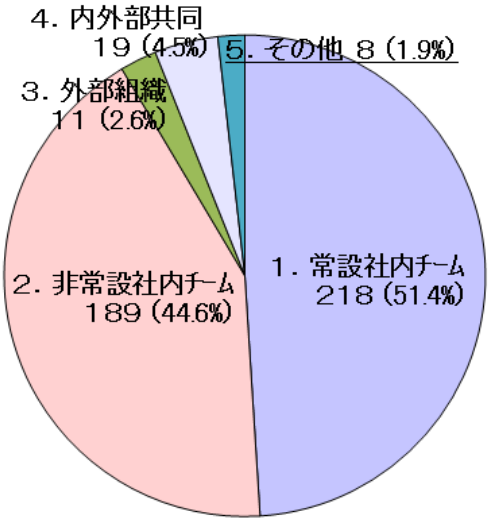


	有効回答数	１．　年　１　回	２．　半年に１　回	３．　３ヶ月に１　回	４．　１回／月以上
今回	423	326	86	7	4
(2010 年)	(%)	77.1	20.3	1.7	0.9
前回	348	252	92	3	1
(2008 年)	(%)	72.4	26.4	0.9	0.3
前々回	264	171	88	2	3
(2006 年)	(%)	64.8	33.3	0.8	1.1

内部監査について

４８．内部監査体制について

１．　常設社内チーム	４．　外部組織と社内の共同
２．　非常設 社内チーム	５．　その他
３．　外部組織	

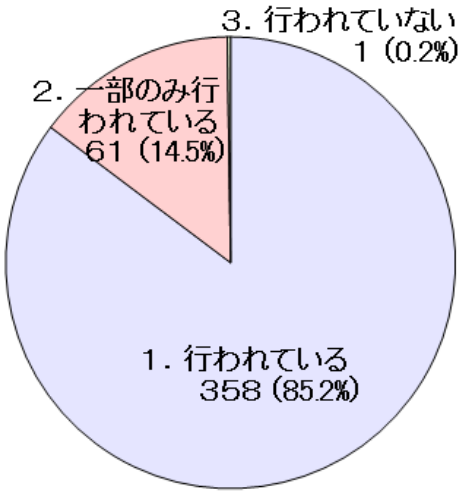


	有効回答数	1．常設社内チーム	2．非常設社内チーム	3．外部組織	4．外部と社内の共同	5．その他
今回	424	218	189	11	19	8
(2010 年)	(%)	51.4	44.6	2.6	4.5	1.9
前回	359	156	175	11	15	2
(2008 年)	(%)	44.3	49.7	3.1	4.3	0.6
前々回	264	101	151	7	14	2
(2006 年)	(%)	38.3	57.2	2.7	5.3	0.8

内部監査について

４９．指摘事項は改善されていますか？

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

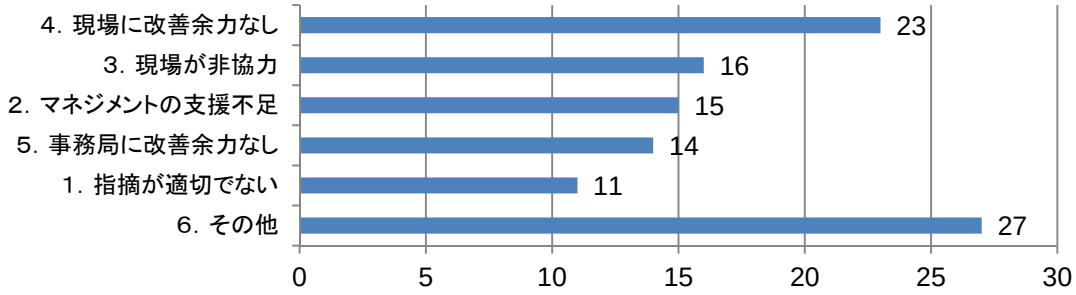


	有効回答数	1．行われている	2．一部のみ行われている	3．行われていない
今回 (2010 年)	420	358	61	1
	(%)	85.2	14.5	0.2
前回 (2008 年)	345	305	40	0
	(%)	88.4	11.6	0.0
前々回 (2006 年)	264	239	25	0
	(%)	90.5	9.5	0.0

内部監査について

５０．前問で、「２」または、「３」の回答の場合、その理由は？

１．　内部監査の指摘が不適切	４．　現場に改善を行う余力がない
２．　改善対策へのマネジメントの支援が不十分	５．　事務局に改善を行う余力がない
３．　現場の協力が得られない	６．　その他

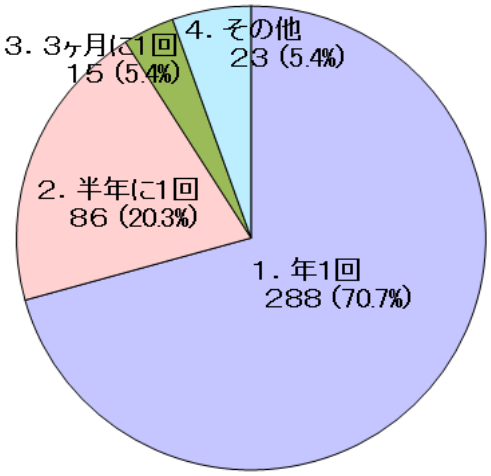


	有効回答数	4．現場の改善余力なし	3．現場が非協力	2．マネジメント支援不足	5．事務局に余力なし	1．指摘が適切でない	6．その他
今回	85	27	11	14	15	16	23
(2010 年)	(%)	31.8	12.9	16.5	17.6	18.8	27.1
前回	40	25	9	9	14	9	3
(2008 年)	(%)	62.5	22.5	22.5	35.0	22.5	7.5
前々回	25	13	3	7	13	5	3
(2006 年)	(%)	52.0	12.0	28.0	52.0	20.0	12.0

マネジメントレビューについて

５１．マネジメントレビューの実施頻度

１．　年１回
２．　半年に１回
３．　３ヶ月に１回
４．　その他



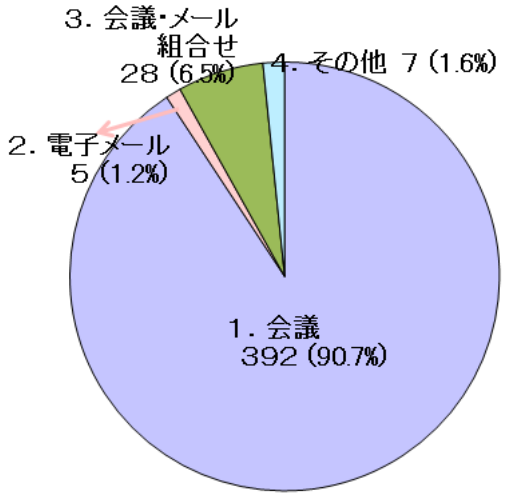
n=423

	有効回答数	１．年１回	２．半年に１回	３．３ヶ月に１回	４．その他
今回	423	299	86	15	23
(2010 年)	(%)	70.7	20.3	3.5	5.4
前回	346	239	78	9	20
(2008 年)	(%)	69.1	22.5	2.6	5.8
前々回	264	163	77	8	16
(2006 年)	(%)	61.7	29.2	3.0	6.1

マネジメントレビューについて

５２．実施形態

１．　会議
２．　電子メール
３．　会議、メールの組合せ
４．　その他

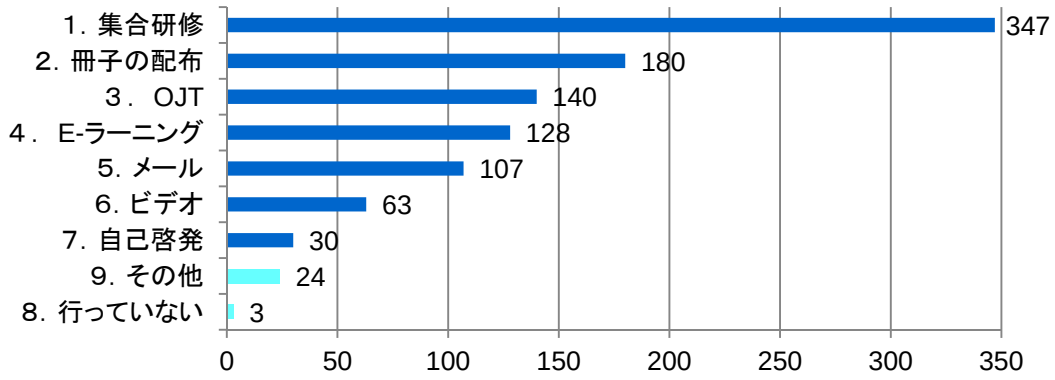


	有効回答数	1. 会議	2. 電子メール	3. 会議、メールの組合せ	4. その他
今回	432	392	5	28	7
(2010 年)	(%)	90.7	1.2	6.5	1.6
前回	347	321	3	17	6
(2008 年)	(%)	92.5	0.9	4.9	1.7
前々回	264	255	0	7	2
(2006 年)	(%)	96.6	0.0	2.7	0.8

教育について

５３．ISMS の維持に必要な社員への教育方法を回答ください。（複数選択可）

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



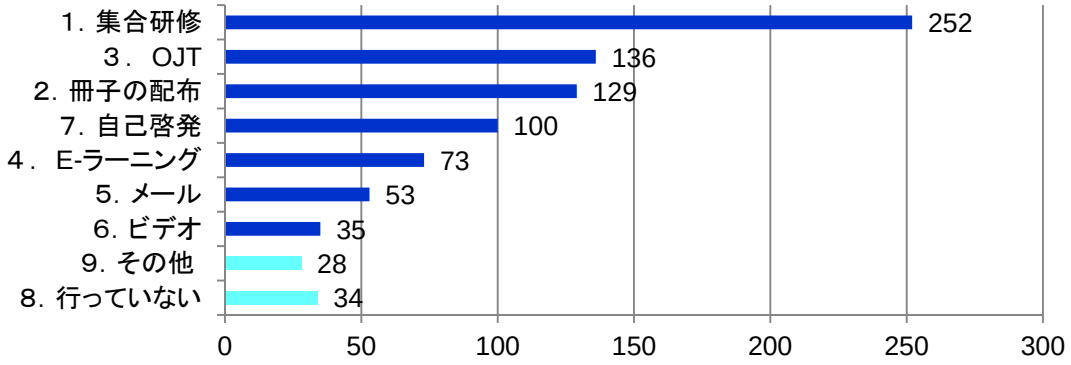
	有効回答数	1：集合研修	2：冊子の配布	3：ＯＪＴ	4：E ラーニング	5：メール
今回	423	347	180	140	128	107
(2010 年)	(%)	82.0	42.6	33.1	30.3	25.3
前回		295	146	118	110	75
(2008 年)	(%)	84.8	42.0	33.9	31.6	21.6
前々回	264	243	124	80	64	61
(2006 年)	(%)	92.0	47.0	30.0	24.2	23.2

6：ビデオ	7：自己啓発	9：その他	8：行っていない
63	30	24	3
14.9	7.1	5.7	0.7
50	36	21	0
14.4	10.3	6.0	0.0
33	20	21	1
12.5	7.6	8.0	0.4

教育について

５４．情報セキュリティ管理者・推進者への教育方法は？（複数選択可）

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



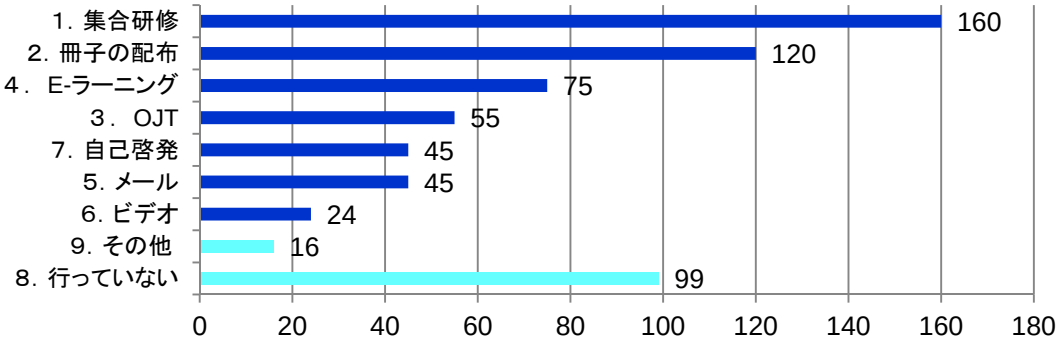
	有効回答数	1. 集合研修	3. ＯＪＴ	2. 冊子の配布	7. 自己啓発	4. E ラーニング
今回	420	252	136	129	100	73
(2010 年)	(%)	60.0	32.4	30.7	23.8	17.4
前回		231	115	91	92	63
(2008 年)	(%)	67.2	33.4	26.5	26.7	18.3
前々回	264	197	60	98	33	41
(2006 年)	(%)	74.6	22.7	37.1	12.5	15.5

5. メール	6. ビデオ	9. その他	8. 行っていない
53	35	28	34
12.6	8.3	6.7	8.1
39	22	24	15
11.3	6.4	7.0	4.4
44	18	25	16
16.7	6.8	8.4	6.1

教育について

５５．経営層への教育方法は？　（複数選択可）

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



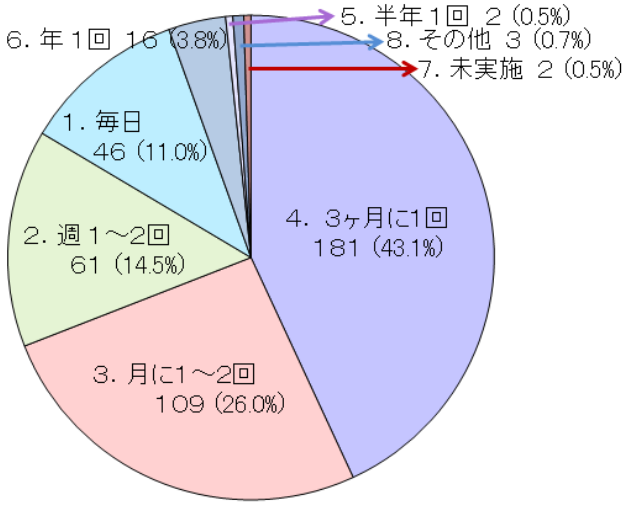
	有効回答数	1：集合研修	2：冊子の配布	4：E ラーニング	3：ＯＪＴ	7：自己啓発
今回	415	160	120	75	55	45
(2010 年)	(%)	38.6	28.9	18.1	13.3	10.8
前回		175	95	54	46	62
(2008 年)	(%)	51.0	27.7	15.7	13.4	18.1
前々回	264	141	92	35	34	20
(2006 年)	(%)	53.4	34.8	13.3	12.9	7.6

5：メール	6：ビデオ	9：その他	8：行っていない
45	24	16	99
10.8	5.8	3.9	23.9
39	22	14	57
11.4	6.4	4.1	16.6
38	14	22	46
14.4	5.3	8.4	17.4

教育について

５６．社員への ISMS の教育頻度は？

１．　毎日	５．　半年に１回程度
２．　週　１～２回	６．　年に１回程度
３．　月　１～２回	７．　行っていない
４．　３ヶ月に１回程度	８．　その他（記入欄あり）

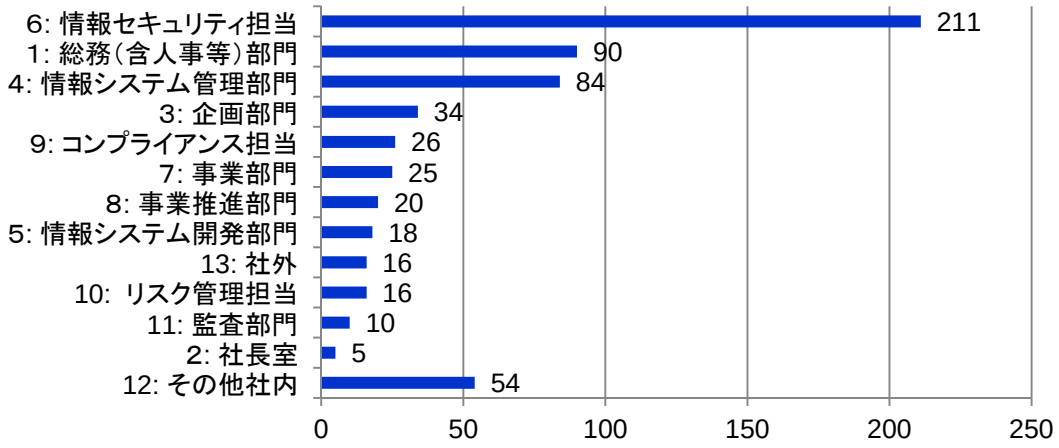


	有効回答数	4. 3ヶ月 1 回	3. 月 1～2回	2. 週 1～2回	1. 毎日	6. 年 1 回	5. 半年 1 回	8. その他	7. 未実施
今回	420	181	109	61	46	16	2	3	2
(2010 年)	(%)	43.1	26.0	14.5	11.0	3.8	0.5	0.7	0.5
前回	336	64	43	3	6	127	82	17	1
(2008 年)	(%)	18.7	12.5	0.9	1.7	37.0	23.9	5.0	0.3
前々回		41	37	8	4	72	59	39	4
(2006 年)	(%)	15.5	14.0	3.0	1.4	27.3	22.3	14.8	1.5

教育について

５７．ISMS の教育の担当部門を回答ください。（複数選択可）

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



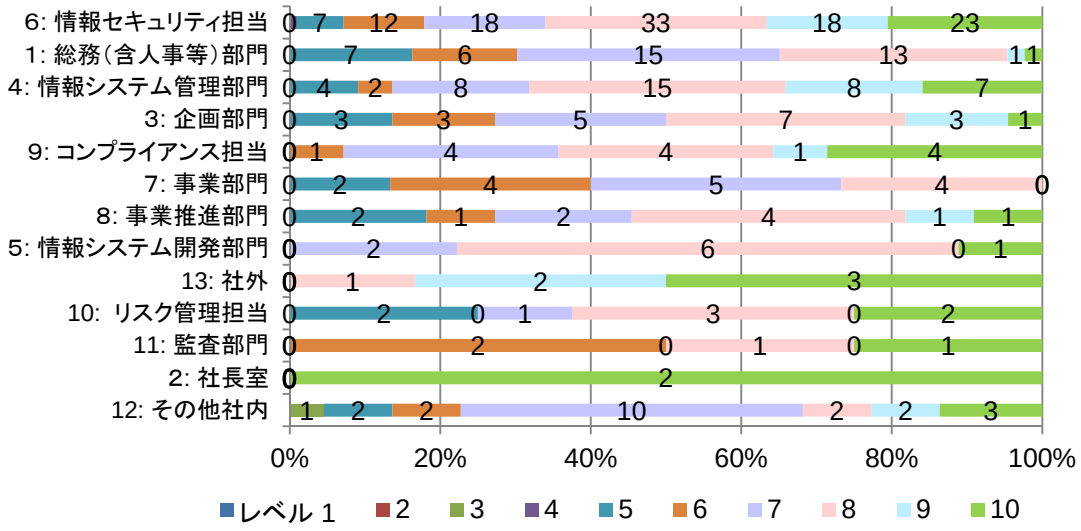
	有効回答数	6．情報セキュリティ	1．総務（含人事）	4．情報システム管理	3．企画	9．コンプライアンス	7．事業部門	8．事業推進
今回	420	211	90	84	34	26	25	20
(2010 年)	(%)	50.2	21.4	20.0	8.1	6.2	6.0	4.8
前回	349	146	78	53	29	14	24	8
(2008 年)	(%)	41.8	22.3	15.2	8.3	4.0	6.9	2.3
前々回		134	55	39	22	12	24	―
(2006 年)	(%)	50.8	20.8	14.8	8.3	4.5	9.1	―

5．情報システム開発	13．社外	10．リスク管理	11．監査	2．社長室	12．その他社内
18	16	16	10	5	54
4.3	3.8	3.8	2.4	1.2	12.9
19	17	16	11	7	77
5.4	4.9	4.6	3.2	2.0	22.1
10	40	4	9	6	40
3.8	15.2	1.5	3.4	2.3	15.2

教育について

５８．問 57 で選択した各教育担当部門の情報セキュリティレベルは？

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



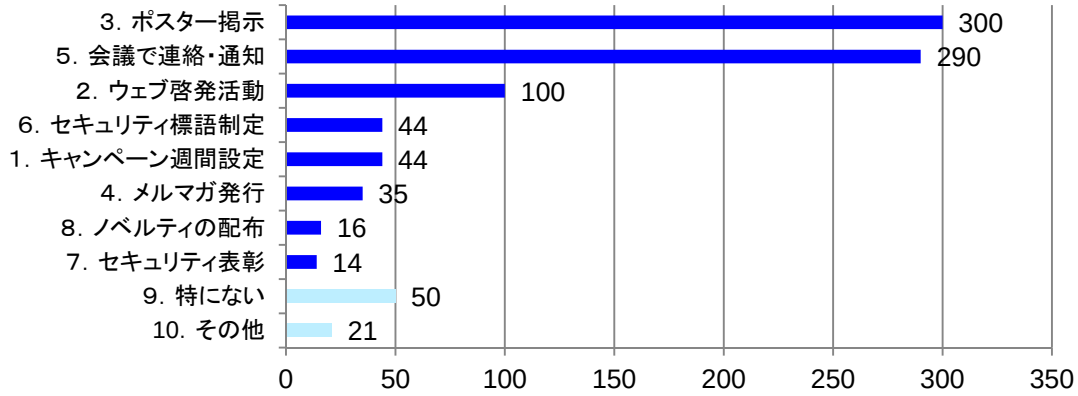
	有効回答数	6．情報セキュリティ	1．総務（含人事）	4．情報システム管理	3．企画	9．コンプライアンス	7．事業部門	8．事業推進
今回 (2010 年)	回答数	112	43	44	22	14	15	11
	平均値	8.0	7.0	8.0	7.3	8.2	6.7	7.4
前回 (2008 年)	回答数	136	75	51	27	12	22	8
	平均値	7.6	6.3	7.5	7.1	7.3	6.9	6.8

5．情報システム開発	13．社外	10．リスク管理	11．監査	2．社長室	12．その他社内
9	6	8	4	2	22
8.0	9.3	7.6	7.5	10.0	7.2
20	15	15	10	7	70
7.2	8.9	8.2	8.0	7.9	6.9

教育について

５９．教育以外の啓発活動について回答下さい（複数選択可）

１．	キャンペーン週間等の設定	６．	セキュリティ標語の制定
２．	ウェブでの啓発活動	７．	セキュリティ取組の表彰（部門・個人）
３．	ポスター掲示	８．	標語等を書いたノベルティの配布
４．	メルマガ等の発行	９．	特にない
５．	会議での連絡・通知	10．	その他



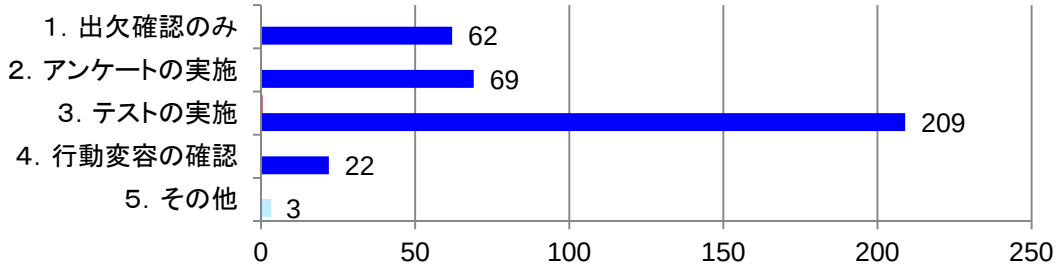
	有効回答数	3：ポスター掲示	5：会議での連絡・通知	2：ウェブでの啓発活動	6：セキュリティ標語の制定	1：キャンペーン週間の設定
今回	420	300	290	100	44	44
(2010 年)	(%)	71.4	69.0	23.8	10.5	10.5
前回		105	194	102	42	45
(2008 年)	(%)	30.6	56.6	29.7	12.2	13.1
前々回		86			29	17
(2006 年)	(%)	32.6			11.0	6.4

4：メルマガ等の発行	8：ノベルティの配布	7：セキュリティ表彰	9：特にない	10：その他
35	16	14	50	21
8.3	3.8	3.3	11.9	5.0
43	28	13	63	25
12.5	8.2	3.8	18.4	7.3
38	15	5	93	47
14.4	5.7	1.9	35.2	17.8

教育について

６０-①. 問 53 で【集合教育】を行っている場合の評価方法は？

１． 出欠確認のみ
２． アンケートの実施
３． テスト／レポート提出
４． インタビュー等による行動変容の確認
５． その他

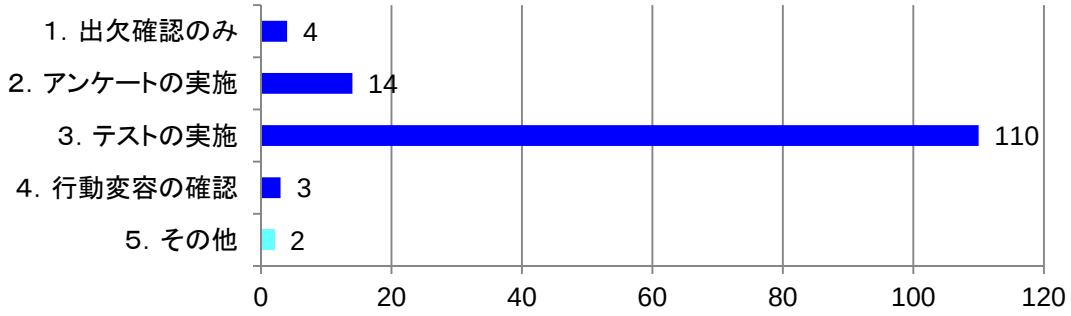


	有効回答数	1．出欠確認	2．アンケート	3：テスト	4．行動変容	5．その他
今回	365	62	69	209	22	3
(2010 年)	(%)	17.0	18.9	57.3	6.0	0.8

教育について

６０-②. 問 53 で【E-ラーニング】を行っている場合の評価方法は？

１． 出欠確認のみ
２． アンケートの実施
３． テスト／レポート提出
４． インタビュー等による行動変容の確認
５． その他

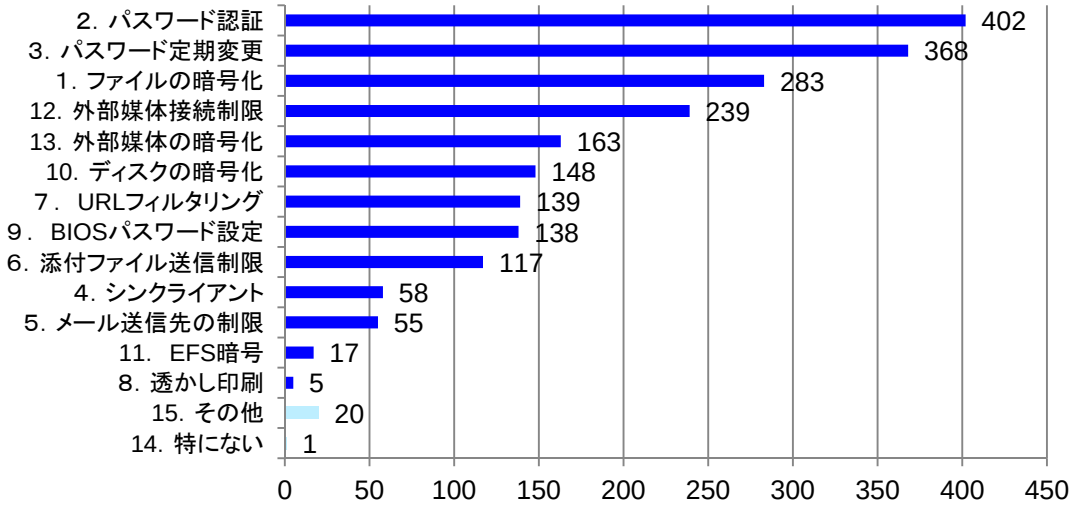


	有効回答数	1．出欠確認	2．アンケート	3：テスト	4．行動変容	5．その他
今回	133	4	14	110	3	2
(2010 年)	(%)	3.0	10.5	82.7	2.3	1.5

教育について

６１．情報漏えい対策として実施している対策を回答下さい(複数選択可)

１． ファイルの暗号化	９． BIOS パスワード設定
２． ログインパスワード認証	10． ディスクの暗号化
３． パスワードの定期的変更	11． EFS 暗号（Windows）
４． シンクライアント	12． 外部媒体接続制限
５． メール送信先の制限	13． 外部媒体の暗号化
６． 添付ファイル送信制限	14． 特にない
７． URL フィルタリング	15． その他
８． 透かし印刷	



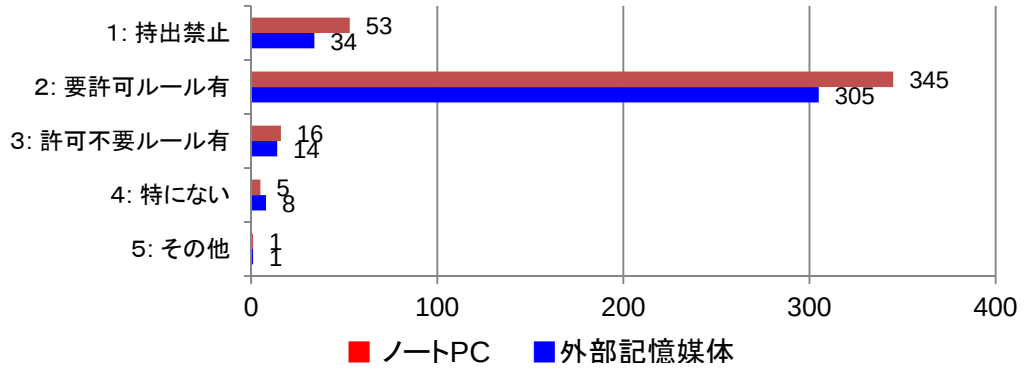
	有効回答数	2. パスワード認証	3. パスワード変更	1. ファイルの暗号化	12. 外部媒体接続制限	13. 外部媒体の暗号化	10. ディスクの暗号化	7. URL フィルタリング
今回	422	402	368	283	239	163	148	139
(2010 年)	(%)	95.3	87.2	67.1	56.6	38.6	35.1	32.9
前回	352	333	286	130	57	178	115	94
(2008 年)	(%)	94.6	81.3	36.9	16.2	50.6	32.7	26.7

9. BIOS パスワード	6. 添付ファイル制限	4. シンクライアント	5. メール送信先制限	11. EFS 暗号	8. 透かし印刷	15. その他	14. ない
138	117	58	55	17	5	20	1
32.7	27.7	13.7	13.0	4.0	1.2	4.7	0.2
108	96	26	34	9	1	10	1
30.7	27.3	7.4	9.7	2.6	0.3	2.8	0.3

社内ルールなど

６２．①【ノート PC】、②【外部記録媒体】の社外持出ルールを回答下さい。（択一）

１．　持出禁止
２．　ルールあり（要許可）
３．　ルールあり（許可不要）
４．　特にない
５．　その他



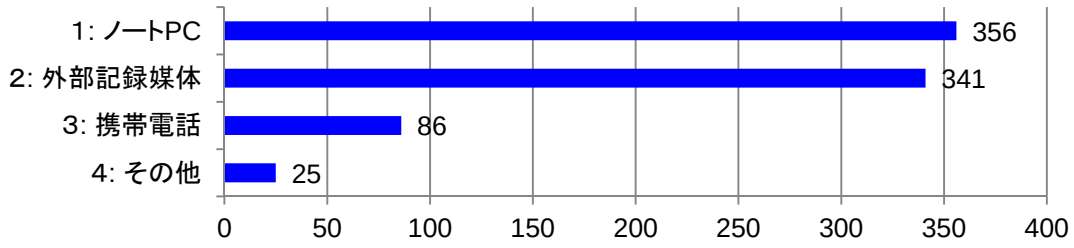
PC 持出	有効回答数	1．持出禁止	2．ルールあり（要許可）	3．ルールあり（許可不要）	4．特にない	5．その他
今回	420	53	345	16	5	1
(2010 年)	(%)	12.6	82.1	3.8	1.2	0.2
前回	343	25	300	15	0	3
(2008 年)	(%)	7.3	87.5	4.4	0.0	0.9

媒体持出	有効回答数	1．持出禁止	2．ルールあり（要許可）	3．ルールあり（許可不要）	4．特にない	5．その他
今回	362	34	305	14	8	1
(2010 年)	(%)	9.4	84.3	3.9	2.2	0.3
前回	277	26	219	19	7	6
(2008 年)	(%)	9.4	79.1	6.9	2.5	2.2

社内ルールなど

６３．社内持込あるいは、利用制限があるものを選択して下さい。（複数回答可）

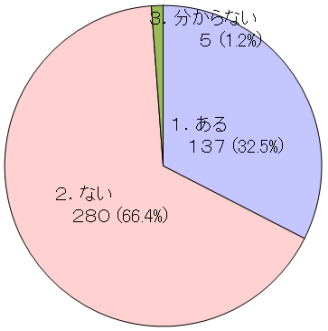
１．　ノートＰＣ
２．　外部記憶媒体
３．　携帯電話
４．　その他

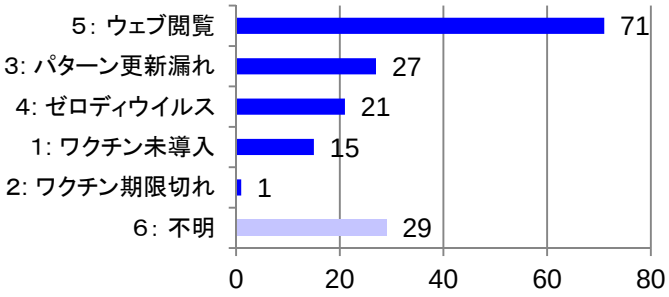


PC 持出	有効回答数	１．ノートＰＣ	２．外部記憶媒体	３．携帯電話	４．その他
今回	398	356	341	86	25
(2010 年)	(%)	89.4	85.7	21.6	6.3
前回	352	274	274	57	9
(2008 年)	(%)	77.8	77.8	16.2	2.6

社内ルールなど

６４／６５．コンピュータウイルス感染の有無／感染原因は？	
64．ウイルスの感染の有無 １．　ある ２．　ない ３．　分からない	65．問 64 で「1」の場合、感染原因は？ １．　ワクチンソフト未導入 ２．　ワクチンソフト期限切れ ３．　パターンファイル更新漏れ ４．　ゼロディウイルスのため ５．　ウェブ閲覧による（ドライブバイダウンロード） ６．　不明





PC 持出	有効回答数	1．ある	2．ない	3．分からない
今回	422	137	280	5
(2010 年)	(%)	32.5	66.4	1.2

PC 持出	有効回答数	5．ウェブ閲覧	3．パターン更新漏れ	4．ゼロディウイルス	1．ワクチン未導入	2．ワクチン期限切れ	6．不明
今回	137	71	27	21	15	1	29
(2010 年)	(%)	51.8	19.7	15.3	10.9	0.7	21.2

一般の情報セキュリティ調査では、内外共にコンピュータウイルス（マルウェア：Malicious Software）被害は、50%以上あるが、本調査では 30%余りで、通常より半分程度になっている。ISMS 認証取得効果がでているのかも知れない。
また、感染原因では、「ウェブ閲覧」が 52%近くで最も多い。国内外に同種の調査を見いだせなかった。　この「ウェブ閲覧」は、多くのワクチンソフト（アンチウイルスソフト）で、発見、削除することは難しい「トロイの木馬」、「スパイウェア」と呼ばれているもの。このため、セキュリティ対策ソフト等で、ウェブフィルタリング等の総合的セキュリティ対策を考える必要があるのではないだろうか？

付録Ｃ．ISMS 認証取得組織へのインタビュー

ヒアリング（１）

分野	設問／回答
１．組織概要	
(1) 出席者の担当業務	• 課長として、ISMS を推進している
(2) 事務局の構成	• 専任が 1 名であるが、
(3) セキュリティ委員会の構成	• 社長、役員以下、約 20 名で構成している
２．認証取得	
(1) 認証範囲の概要	• 基本的には全社でやっている
(2) 取得からの年数	• 2007 年に取得しており、3 年以上経過している
(3) 認証取得の背景	• 2005 年にセキュリティ事故があり、それを機会に取得を目指した。個人情報を持っていないので、P マークを取ることは考えていなかった。 • また、親会社の基本的な考えが、安全・安心を目指していることもある。
(4) 取得の効果	• ISMS での考え方は情報セキュリティ確保に役立っている
(5) 継続の課題	• 事務局の属人化、ヒューマンエラー対策等の課題はある
(6) 内部統制、J-SOX 等の取組みは ISMS 活動に影響したか？	• ISMS の取得は非常に役立っている
(7) 特に力をいれているところ	•
(8) 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	• 得られている
(9) 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	• 親会社を含め、グループ全体で安全・安心対応については、十分な理解を得ている
３．コンサルタント	
(1) コンサルタントを利用したか？	• 取得時及び、現在も部分的には利用している。比較的に良い結果に繋がっている
４．審査制度	
(1) 審査員、審査機関の対応について	• 審査員には恵まれており、高い評価を与えられる
５．その他	
(1) インシデント対応について	• ISMS 認証取得後には、大きなインシデントもなく、また、件数も少ない
(2) ウイルス感染について	• ウイルスの検出はあるが、感染はない

ヒアリング（２）

分野	設問／回答
１．組織概要	
(1)	出席者の担当業務 • 管理本部長と課長で、管理本部長はマネジメントシステム等全ての責任を負っており、課長は、ISMS 事務局責任者。
(2)	事務局の構成 • 上記(1)の管理者（本部長）と課長、他１名で運用、実業務は２名で行っている
(3)	セキュリティ委員会の構成 • 上記３名に各部門からで構成されている。月１回の頻度で開催
２．認証取得	
(1)	認証範囲の概要 • 全社にて実施している
(2)	取得からの年数 • 2005 年に取得した
(3)	認証取得の背景 • QMS を比較的早い時期に取得しており、個人情報保護法施行時に、Ｐマークと ISMS をほぼ同時に取得することを目指した。非常に大変であったが、取得することができた
(4)	取得の効果 • グループ会社で唯一 ISMS 認証を取得しており､最近の IT 統制等への対応では､ISMS の管理策が非常に役立った。他のグループ会社から比較してもうまく対応できた
(5)	継続の課題 • 他のマネジメントシステムとの重複項目が多いが、それらの統合化、また、内部監査要員の技量向上が難しい。情報システム管理との兼務者はあまり問題がないが、他の部門からの監査要員の技量向上についても課題の１つと認識している
(6)	内部統制、J-SOX 等の取組みは ISMS 活動に影響したか？ • (4)で述べたように、グループ企業での IT 統制への対応などでは非常に役立った
(7)	特に力をいれているところ • 他のマネジメントシステム等との統合化等
(8)	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 • 特に問題はない
(9)	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 • 得られている。　ただ、企業全体として緊縮予算になっている
３．コンサルタント	
(1)	コンサルタントを利用したか？ • 認証取得時には利用したが、最初のコンサルタントは非常にレベルが低かったため、初回更新審査時に変更した。　現在は利用していない。 • 両方のコンサルタント（企業）は、紹介であった
４．審査制度	
(1)	審査員、審査機関の対応について • 特に問題になるようなことはなく、審査員の指摘事項等も適切である
５．その他	
(1)	インシデント対応について • 件数も少なく、大きな問題になるようなことはない
(2)	ウイルス感染について • ウイルスの検出はあるが、感染はない

ヒアリング（３）

分野	設問／回答
１．組織概要	
(1)	出席者の担当業務 • 課長職であるが、兼務で、非常に忙しい
(2)	事務局の構成 • ４名が兼務している
(3)	セキュリティ委員会の構成 • 30 名程度で委員会を構成しており、2 週間に 1 回開催している
２．認証取得	
(1)	認証範囲の概要 • 現在は本社とデータセンターだけの対応であるが、新たに担当部門のできたので、今後、拡張される可能性はある
(2)	取得からの年数 • 2005 年から取得しており、初期の頃から取得している
(3)	認証取得の背景 • 社長からの発案で ISMS 取得を目指した。個人情報もあるが、重点は企業営業であり、P マークの取得はあまり考えなかった • 3 月より、新たな組織ができ、そこでの対応することになる。現在は、全く関係のない部門で対応しているので、今後は更に発展して行くことになる
(4)	取得の効果 •
(5)	継続の課題 • 特にない。　ISMS 対応組織ができ、より以上のことが可能になると思われる
(6)	内部統制、J-SOX 等の取組みは ISMS 活動に影響したか？ • していない
(7)	特に力をいれているところ •
(8)	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 • 得られている
(9)	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 • 得られている
３．コンサルタント	
(1)	コンサルタントを利用したか？ • 利用したようであるが、当時、担当していなかったため、明確でない
４．審査制度	
(1)	審査員、審査機関の対応について • コミュニケーションや業務理解度等に若干問題がある
５．その他	
(1)	インシデント対応について • 業務上の対応のため、全く問題がない訳ではないが、大きな問題は発生していない
(2)	ウイルス感染について • ウイルスの検出はあるが、感染はない • ISMS 範囲ではないが、ウェブ閲覧での感染経験があるが、報告がないので、発見理由は現時点で不明

ヒアリング（４）

分野	設問／回答
１．組織概要	
(1)	出席者の担当業務 • 部長として、兼務で ISMS を推進する責任者（兼務）
(2)	事務局の構成 • 兼務が 4 名で構成している
(3)	セキュリティ委員会の構成 • 社長、役員以下、20 数名で構成している
２．認証取得	
(1)	認証範囲の概要 • 全社でやっている
(2)	取得からの年数 • 2005 年に取得している
(3)	認証取得の背景 • 取引先からの進めや同業者での事故が引き金になり、ISMS の取得を目指した。個人情報はないため、P マークの取得は考えなかった
(4)	取得の効果 • ISMS での考え方は情報セキュリティ確保に役立っている
(5)	継続の課題 •
(6)	内部統制、J-SOX 等の取組みは ISMS 活動に影響したか？ •
(7)	特に力をいれているところ •
(8)	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 • 得られている
(9)	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 • 得られている
３．コンサルタント	
(1)	コンサルタントを利用したか？ • 比較的良いコンサルタントに恵まれた。ただ、特殊な業界であったため、業務の理解度は多少問題があったが、仕方ないと考えていた
４．審査制度	
(1)	審査員、審査機関の対応について • 審査員には比較的恵まれたが、業務の理解をさせるのに苦労した
５．その他	
(1)	インシデント対応について • 現時点まで、大きな問題は発生していない
(2)	ウイルス感染について • ウイルス感染はあったが、パターンファイルの更新漏れで発生した

ヒアリング（５）

分野	設問／回答
１．組織概要	
(1)	出席者の担当業務 • 部長で、他の業務と兼務で ISMS を推進している
(2)	事務局の構成 • 兼務が 2 名と幹部監査人がいる
(3)	セキュリティ委員会の構成 • 月１回の部長会がセキュリティ委員会の役割を果たしている • マネジメントレビューは２回／年行っている
２．認証取得	
(1)	認証範囲の概要 • 基本的には全社でやっている
(2)	取得からの年数 • 2006 年に取得した
(3)	認証取得の背景 • 外部からの取得要請や自社製品にセキュリティ関係のものがあるため、ISMS 認証取得が必要であると考えた
(4)	取得の効果 • 営業的にも ISMS 取得は役立っている
(5)	継続の課題 • 現在の担当者が当初から変わらないが、今後数年で、退職者がでることになり、ISMS 業務のスキルをどの様に継承していくかが課題になっている
(6)	内部統制、J-SOX 等の取組みは ISMS 活動に影響したか？ •
(7)	特に力をいれているところ • クリア PC の実施を行っている
(8)	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 • 得られている
(9)	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 • 得られている
３．コンサルタント	
(1)	コンサルタントを利用したか？ • 取得時及び、現在も部分的には利用している。提案能力の点では若干問題があった • 取得後は年１回相談をするかどうかである
４．審査制度	
(1)	審査員、審査機関の対応について • 審査員には恵まれており、高い評価を与えられる
５．その他	
(1)	インシデント対応について • 大きな問題は発生していない
(2)	ウイルス感染について • 感染はない

ヒアリング（６）

分野	設問／回答
１．組織概要	
(1)	出席者の担当業務 • 部長クラスで、兼務で ISMS 推進を担当している
(2)	事務局の構成 • ２名が兼務している
(3)	セキュリティ委員会の構成 • 部長会がその役割を担っている
２．認証取得	
(1)	認証範囲の概要 • 全社を対象にしている
(2)	取得からの年数 • 取得後、4 年以上経過している
(3)	認証取得の背景 • 当時、既に EMS を取得しており、情報セキュリティの確保のため、社長からの指示で ISMS の取得を行った
(4)	取得の効果 • 社員のセキュリティ意識の向上等はあるが、業務上の制約が多く、若干、現場業務との乖離もある
(5)	継続の課題 •
(6)	内部統制、J-SOX 等の取組みは ISMS 活動に影響したか？ •
(7)	特に力をいれているところ •
(8)	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 •
(9)	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 • 部長会での報告などもあり、トップの理解は得られている
３．コンサルタント	
(1)	コンサルタントを利用したか？ • 利用したが、当社の方針とややミスマッチな部分があり、認証取得には役だったが、全体的には問題があったと言わざるを得ない
４．審査制度	
(1)	審査員、審査機関の対応について • 審査員の考え方が、特に出先の責任者に十分理解をさせた指摘がない
５．その他	
(1)	インシデント対応について • 大きな問題はない
(2)	ウイルス感染について • アンチウイルスソフトが導入されていない PC があったため、感染したことがある

付録Ｄ．自由意見欄について

ISO27001 は ISO9001 に比べ客先から取得を要請されるケースが多い。 ISMS は事故が発生して当たり前で運用のモチベーションを維持するのが難しい リスクアセスメントを行い、自社にあった ISMS を構築しても審査を繰り返してゆくと、性悪説の立場を取ると結局全ての対策を取らざるを得なくなる
現在、当社では ISO9000、ISO27001、ISO１４０００を取得しており、更にＰマークも取得予定です（社長より）
弊社が ISMS を取得した動機は、社会情勢で情報セキュリティが重要視される中、体制を構築するノウハウ・人材が社内に存在しなかった。そこで、外部コンサルタントの力を借りて情報セキュリティ体制を構築し、ISMS 取得に至った。　認証取得から５年経過した今では ISMS 要求事項をベースに情報セキュリティ体制も整い、PDCA も動いており日々改善を行っている。 また、近年グループ全体で行っている IT 統制の対応項目において、既に ISMS の調査年で対応済みの項目が多く、対応にかかる工数が最小限で済んだことも利点としてあげられる。 情報セキュリティ上の脅威が日々変化している現在、ISMS 審査員からの指摘事項は、維持・運用活動の中で漏れていたリスクを認識できるという意味で貴重なものだと認識している。 現在の弊社のおける課題は下記のものがある。 【課題１：情報セキュリティ管理効率化】 ISMS、プライバシーマーク、IT 統制の３つを管理しているが、重複する項目が多く、同じような内容の規程類・記録類が多数存在する。　情報セキュリティ管理の効率化を目的に統合化が課題となっている。 【課題２：内部監査員の技量向上】 ISMS は専門知識を必要とするため、通常業務と関連性のある ISO9001 に比べて内部監査員の技量向上が難しい側面がある。　内部監査員と情報システム管理と兼務している者は問題がないが、それ以外の者の技量向上策が課題
弊社は、一部門での認証のため、全社ルールとの差分調整が運用で発生してしまう。 （例）報告書が２部必要。　これらを現在改善中
①カメラ付き携帯電話の取扱い　②電子メールによる情報漏えい制限、等が現時点での課題となっている
日常業務以外に ISMS 認証のための業務を行うため、時間的に制約があり、作業負担になる点　(ISMS 自体は良い取組だが、ISMS 自体では利益を生む企業活動とは直結しない)
情報の電子化が進む現状において管理策のレベルアップが益々必要になっている。 特に IT 関連の体制強化、整備が課題となっている
専任者で推進する程の余裕がないため、作業量が多く大変。本来業務を優先するため、すべてのことが後回しになってしまう。 費用対効果がどれほどのものか疑問 中身をきちんと理解していないために、余計なことまでやってしまっていると考えられる
ISMS の推進により、作業や管理が増える一方、セキュリティを高める有効な手段の導

入がやりやすく（予算がとりやすい)、弊社ではとても意味のあるものになっている。外部監査では自分たちでは気づかない点の指摘があり、改善につなげていくことができとても良いものになっている
①携帯電話リスク対応　②ファイル暗号化のマニュアル化、等が現時点での課題
全ての認証は不景気になると相手にされなくなる（笑)。　但し、組織は強くなる気がしている。　２つの ISO で高額な費用のため、小さな会社では負担になっている
①社員１人１人のセキュリティに関する意識レベルの向上、②ルールありきとなり、社員の自ら考える力の不足、③「事務局だけで対応すれば良い」という意識の払拭、等が現時点での課題
セキュリティ確保の手順やルールを整備しても､社員個人のモラルに依存してしまう。モラルを高め､維持するには､社員満足度向上（給与や福利厚生関連の諸施策を含む)、長期的な雇用の維持などを整備し、確実に実施し、改善して行く必要があると感じている。 「今の会社に定年まで勤務したい」という、安心感を感じられるような事業の推進や適切な処遇が重要だと感じる
2010 年 12 月を持って、認証を取り下げた。　ISMS 認証の維持・管理に頼らなくても、部門内の情報セキュリティ意識レベルを維持できると判断したため
社員全員で活用できる仕組み作りが大切だと考えている
″ISMS 認証は現時点で１番有効性が高い規格であると認識している。ただ、問題点として、 １．プライバシーマークと共通化を進めて欲しい。日本ではプライバシーマークの認知度が高く、取得企業も多いが、実業務としては、ISO に比較すると非現実的な要求が多い。　ただし、プライバシーマーク側は JISQ15001 になり、ISO と同様のリスク分析手法を利用するようになっているが、独自路線を進んでいるため、ダブルスタンダードになる一因と思われる。 ２．審査基準となる事例を知りたい。ISO 規格は大枠抑えられているが、細かい点は取得先に任せすぎな点が気になる
ISMS 認証システムについて以下のことを感じている ① 規格（ISO27001/27002）があいまい ② 規格の解釈は組織によって異なるはず（異なってもいいはず）だが、審査員の見解によって、NG になることも多い ③ 規格の中にでてくる用語を、どうやって解釈しようか迷うことが多すぎる（調べても明確な答えを得られたためしがない) ④ 規格が曖昧なので、実際の企業活動においても浮世離れしすぎて、ダブルスタンダードを発生させているのではないか？ ⑤ JISQ15001 の方が具体的になっているので、普及しているのではないか？（費用も安い) ⑥ ISMS 構築時、JIPDEC のガイドラインでは、難しすぎて（否定されすぎて)、導入しても二重規則で効果がでないのではないか？　最初に「今でも OK」､「改善要」に分類し､導入前からちゃんとやっていたことを認めるようにしないと､一瞬に形骸化してしまう
認証取得・維持に割かれるエネルギーは本来の業務を脅かす程のものがある。このジ

レンマを如何に乗り越えつつ、ISMS を自分たちの組織の血肉にしていけるかが課題となっている。 この課題に正面から取り組まない限り、ISMS が組織にとっての『業務の邪魔者』の地位に留まらざるを得ないと考える
有効性評価の手法がイマイチである
一般社員の意識の定着化が難しい。人間は忘れる。他社のインシデント事例等を紹介して、危機意識を低下させない仕組みが必要
兼任の事務局は業務的にきつい
取得時に得意先より認証の有無が、仕事の発注に影響するとの話だったが、現在は費用が優先され、維持費用に合わなくなっている
情報セキュリティの運用開始時は、ルールが面倒で事務局での事務処理が増え、やる気がなかった。 しかし、５年経過し、現在では ISMS を行っていてよかったと思っている。 内部統制や J-SOX 等に有効であり、助かっている
通常業務と兼務のため、維持・運用が負担となる場合がある。 《回答内容についての補足》 ① 問１９：11 としたが、ISMS 構築時の予定としては負担がない意味。上記の如く、通常業務と兼務となる場合は、全てにおいて作業内容が負担となっている。 ② 問３８，４６： コンサルの選定：前提として ISMS を理解されていない方は困りますので、この回答とした。 ③ 問５７： ISMS 教育は事務局が行うので、その他とした。 ④ 問６３： 記入の仕方が不明でした。 私物 PC、外部記録媒体は社内持込禁止、携帯は可となります。 私物の持込の件と理解しました
ITSMS、BCMS は廃止して、ISMS に統合すべき
セキュリティレベルを上げることが一番効果的だが、コスト面を考えるとなかなか手が届かない。 ① 入退管理システムを導入するには費用が高い ② 審査は年１回だが、内容を考えて審査をしてくれると良いと思うことがある ③ 教育には悩まされる。 外部研修を受けさせるにも結構、費用が掛かるので、全員と言う訳にはいなないが、教育については指摘されることが多い しかし、ISMS をやった事によって、情報の大切さは（管理する必要性など)、ずいぶん、浸透したように思える
ISMS は便利なものと言うだけでなく、自身を守るためにも必要と考えています
入館証や携帯電話の紛失事故が無くならない
コスト削減のため、部門を統合した審査を行っているが、組織が大きくなるほど、末端まで共通したコントロールが難しい。 ISMS に適した組織の大きさがあるように思われるが、それがどれ位なのかはよく分からない。 ISMS は自分たちが決めたルール通り活動していることを確認できればよいが、CMMI のように何らかの客観的指標でレベル付けがあってもよいのではないかと考えている
記録作業の合理化ができないか思案中
専門知識が必要で言語（日本語）の言い回しが難しい。 また、外国語での表現が多いので教育レベルの問題もあり、教育をレベル毎にしなくてはならない
ISMS 導入当初はセキュリティ管理を確立するために役立ったが、現在の規格ではセキ

ュリティを向上させることは出来ないと感じている
ISO27001 の認証の取得・維持自体が目的化している例は他にも多いと思う。　決して無意義な活動ではないが、現状の規格通りに運用しようとすると、一企業として負担が大きすぎると感じる。　今後は無駄を省き、社員各自のセキュリティ意識向上が課題である
現在、ISMS だけでなく、EMS も同時に取得しているが、更にコンプライアンスや内部統制も含め、全て当社の CSR の考え方を基盤とした、BCMS(事業継続マネジメントシステム）の中で運用し、既存の業務とは別の運用にならないように行っている。 最初は別のシステムとしてとらえ、運営し、かなりの負担があったが、現在は矛盾なく進んでいます
ノート PC や記録媒体、書類などの目に見えるものは管理・監視しやすいが、人間の頭の中にある情報の管理（守秘）は難しい。 電車の中や飲食店での会話に会社情報を出さない等は教育・啓発頼り
長年、運用していても費用対効果が低い。　ISO 全般にいえるが、認証は対外的に必要であって、内部では不要論が多い
教育、指導の下、会社全体で ISMS 運用がうまく回って行くにつれて、日常的に行いすぎて、それが何の為にやっているか（対策など）を忘れてしまいがちになる。 定期的に声をだすことで、各自が再考できる環境を構築しているが、組織が大きくなるとどこまで浸透するかという疑問がある。 大企業との付き合いが多いが、末端の社員は全く情報セキュリティへの意識が低いことが多々ある。　そのことを反面教師として、運用していきたいと考えている
審査機関に対する費用をもう少し安くできないか？　審査機関毎に審査費用に大幅な差があるのはなぜか？
① ISMS の要求事項と弊社の業務内容に相違があり、形式的に取り組んでいる規定がある ② セキュリティの強化と合理化（利便性）が反比例している
ISO9000 と異なり、「抜け穴」が多く、有名無実化しやすい。　マネジメントが有効に機能していない組織では導入・運用は厳しいものとなる
″当社では認証は一部のサービスのであるが、ISO27001 に基づいた情報資産の管理の仕組みは全社的に展開しており、そういった意味で実効性のあるものとなっている。 元々は、認証取得が目的ではなく、ISO27001 ベースの仕組みを構築していく中で、特定のサービスに限定した認証をたまたま取得したような形である。 このような活動を行っていく上で、重要なのは TOP の意識であり、うまくいくも、いなないも TOP の気持ち次第である。　ボトムアップではどうしても形だけの仕組みになりがちである。″
適用宣言書作成において、リスク分析が必要とあるが、必要ないと考える。　「適用宣言書は全て満たされるべき」と、どちらにしろ要求されるので、それであれば、最初から全て満たすことをすれば十分と思う
毎年策定する当該年度の「セキュリティ目的」をどの様に決定すべきか困惑している
《更新維持費用について》 ① 年に１回のサーベイランス、３年に１回の更新審査での審査料として、高額を請求

されるが、これは不当に高い金額である。中には規格の理解度が高くないにもかかわらず、些末な事にこだわって是正要求をする審査員もいる ② ISMS 審査員の知識領域の広さと深さは、弁護士や公認会計士に比べれば半分にも満たないものだが、審査料の単価は同額である ③ 第三者機関が足並みをそろえて、せめて半額に値下げすべきである ④ このアンケートを集計・公表するに当たり、貴研究室から審査機関に対して、審査料の実効的値下げを是非働きかけて頂きたい
① 社内教育の際、教材の入手に大変苦労している ② 最近の審査ではリスク対応計画の内容がどのリスクアセスメント寄りの対応なのか審査員の質問を受ける（明確な結びつけがない）
昨年、維持・運用を行うためにコスト（含人件費）を算出してみた。 この作業の中で、作業項目等の洗い出しを行ったが、外部審査に関わる以外の部分は弊社にとって必要なことが分かった
① ISMS 認証取得メリットが社会的に大きいとは言えないのが現状であり、この点を改善するよう働きかけてもらいたい ② サーベイランス審査もあり、毎年対応することは、良いスパイスと言えているが、少々日程（審査員稼働）が多めであると感じている。 P マーク審査と合わせてももっと少ない日程で実施していかないと長続きしない ③ 企業が取り組んでいる技術的な対策を評価して入札等で P マークと別に考慮すべきである
P マークと統合して欲しいと感じる。　＊どちらも JIPDEC の認定なので
ISMS 認証システムを７年以上、旧通産省の「安対認定」を入れると１６年位、維持・運用しているとある程度安定する。 安全な状態を維持しているだけなら、毎年かなりの金額をかけて、外部審査をいれる必要性があまりない様に思う。　毎年、審査が入る事により、無理に指摘事項を作られて、その対応にかなりの時間を使っているような気がする。　ISMS をもっと広めるためには、この辺りの審査の方法も見直さないとやめていく企業が増えるのでは・・・（実際に減ってきているが）
ISMS 導入後、６年になるが、導入時に社内規定を厳しく（細かく）しすぎてしまった部分もあり、運用するうちに、実体（実運用）とルール（規定）に差異が生じている。また、部門（ISMS 事務局以外の他部門）は、ISMS を「やらされている」感が強く、難しさを感じる
① 社内業務と ISMS に関する業務の工数増加に伴い、 • 一時的にセキュリティレベルが下がる 特に、「経営者の判断」と称して行われる指示が、情報セキュリティ・ISMS を考慮されてなく、不十分である事がある ② 可用性・機密性・完全性のバランスを維持することができる知見者が少なく、ISMS 運用はその少数の知見者が担うことになる • 負荷が上がる（想定内の事象であるが・・・） ③ ISO を「営業ツール」としてしか捕らえられていない経営陣・幹部が多い。 また、ISO27001 を「情報セキュリティ」のみに特化したものと認識し、「業務効率化」、「業務改善」などの ISO の考え方に至っていない
アンケートの集計結果を知らせて欲しい

審査員の質に疑問がある。　規格の解釈に主観をいれて時間を費やすだけになっている

16-8： QMS、OH&SMS とあわせて認証が４つになったため、IMS(統合マネジメントシステム）に移行することになった。
各種マネジメントシステムが並立する場合、例えば、内部監査も年４回巡ってくるなど、現場の負担も大きい。日本の事業会社は QMS、EMS を取得している場合が多いので、こうした企業に ISMS を普及させる場合、最初から IMS に繋げることを考えた方が良いと思う
一般的には、情報システム系の会社が認証取得する例が多いと思うが、特に技術開発を行う企業では、競争力の源泉である技術情報をどう守か、どう使うか、という点で ISMS 認証を取得する意義は十分あると思われ、こうした企業に ISMS の認知度を上げることも検討すべき課題と思う

〃認証取得以降、基本的な方針は変わらないが、現場の対策やマニュアルは随時見直しを行っている。 内部監査や委員会等の実施で PDCA はしっかり回っていると思うが、情報を守ることに執着しすぎて発行する様式（承認）が増え、現場の作業が煩雑になっていると感じる。
事故を未然に防止することも大事だが、機密性と可用性をバランスよくカバーし、「当社にあった仕組みを効率よく」作りあげたいと感じている

対象要員が拡散したり、スコープを広げる検討をしているが、認証審査の費用等を考えると二の足を踏んでしまう。要員数が多ければ、１人当たりの費用は少なくなるが、10 名位までの小所帯となると難しい問題となる

有効性の評価方法、法規制に関する見直しが難しい

① ISMS 摘要の形骸化（PDCA 及びスパイラルアップの為の対策）
② 他の ISO(9000、14000）との統一化及び統合化
③ ISO9000 及び 14000 の維持運用が安全品質管理部なのに対し、ISMS は情報部門ということで、別運用／管理となっている（情報セキュリティ≒システム関連という認識）
④ 発注先との契約及び要求が年々厳しくなる中、施工など現場レベルでの ISMS 定着の悪さ
⑤ ISO27001 の要求にある有効性評価に関わる要求（ISO27004)の不明確さ（JIS 化されない理由等）
⑥ 個人情報保護法と ISMS の統一化や差分、運用方法が別になっている
⑦ ISMS 維持運用（含 内部監査）の工数・費用について対費用効果が計りにくい
⑧ ISMS にて様々なルールや様式を決めているが、発注先からの要求で別の様式やルールについても社内展開しないといけない
⑨ 内部統制（J-SOX)や ISO20000 等、一部 ISMS と共通する部分がある場合に、どの様に取り組んでいくかが不明なこと
⑩ 子会社や協力会社の情報セキュリティ監視の範囲や程度(特に個人情報保護法による対応)
⑪ 情報セキュリティ自体が何か会社に対して生産性を生むものではないという事で、ISMS 事務局として、どこまで踏み込んで良いかの判断（何か事件・事故が起きたら太変と思う立場とそんなに出来ないという現場との立場をどの様に近づけるか）

過去数年で情報セキュリティに対する社内のリテラシーは向上していると感じるが、

ISMS 運用に引き続き専門性が求められる現実は変わっていない。もっと自律的に運用できる組織にするにはどうしたらよいのか？
ISMS 認証取得後５年目頃から、当社の業務にあった、また、身の丈にあった運用ができるようになった。従来は、コンサル会社が「このような記録が必要」と提示してきた記録簿に記入することで精一杯だったのが、必要な内容を取捨できるようになった PDCA サイクルを回していくことが最も大切だが、最も困難。 社長を含めて、４～５人の会社なので、一人で何役もこなしている。　「認証」取得・維持のたえのコストがかかり過ぎると感じる
第三者認証機関の契約社員として審査業務を担当している。　以前は規格適合性を中心に審査することが主流だったが、最近は、付加価値の高い審査、業務、事業に有効な審査にフォーカスしている。　審査業務ではコンサルはできなことから付加価値という点ではどこまでコメントできるのかという難しさがあるが、経営に役立つ審査という点で、第三者認証の質も変わりつつあるとではないかと感じている。 受審企業はマーク維持のために、漠然と受審されるのではなく、どの辺りをキーに審査して欲しいのかを審査側との意識合わせを通じて、行うことが大切なのではないかと思う
① 社内への意識向上、ルールの徹底が課題 ② 情報セキュリティに対する設備投資が十分にできない
① 事務局の属人化（要員のローテーションができない、専門化している） ② ヒューマンエラー対策（ISMS、ツール等全て″人″であり、無くならない） ③ ISMS 維持費用（費用対効果の有効性が減少）
事務局として、管理等大変だが、ISMS の取得をして情報資産の整理・整頓ができ、良かったと感じる。 いつも思うのは JIS の要求事項は表現がわかり難い！ 英語を日本語に訳しただけからだと思う
ISMS はマネジメントサイクルを最も重視しており、一定の PDCA サイクルが確立した後、現場レベルの更なる向上が難しい
維持・運用に多くの時間（特に書類作成）と費用がかかる。その割に効果を実感できない。　極論だが、セキュリティ事故は仕組みだけでは防げない。起きる時は起きてしまう。99%は出来ても、100%は出来ない。100% 防げないなら意味がないと感じる
外部委託先の管理（特に再委託先までを含む）負担が大きくなっているのが課題
規格についての意見であるが、 ① 付属書 A が実質 Shall になっており、要求が細かすぎる ② プロセスが無駄なものがあり、「効果の測定評価」等、内部監査、マネジメントレビューで十分では？
外部審査での指摘事項の改善を行っているが、費用が掛かりすぎ、困難な状況にある
セキュリティのルール強化は可能だが、実業務を阻害、さらには高コスト体質を生みかねない。　結局、安全・安心と業務効率とのバランスが大事となり、取引先による縛りも大きく影響する
この調査で、情報セキュリティの実態を改めて見直す良い機会となり、進化するウイルス感染や事故･事件に現状対策では不十分ではないか？ との検証視点を変えてみる事にした。

中小企業に適合した認証システムが必要と感じている。　大企業とは違うため、人的コスト、時間をかけられない。　そうした先行事例があれば興味ある
事業部で認証取得をしているが、全社での取得でないため、会社規則に従いつつ、独自規則を作っている。　規則の階層が深いため、従業員からみると複雑になっている。 セキュリティ監査は事業部の内部監査で兼ねているが、全社で取得しているPマークについての監査は別途必要になるため現場は負担を感じている
ISMS認証という一つの枠組みで扱われる中に、事業継続はそれ程必要としないものもあるが、画一的に扱われる事に疑問がある
外部コンサル及びISMS審査会社の費用が高すぎる。　当社が利用している審査会社は審査員の交通費、宿泊費までも当社負担となっている
ISMS審査において、審査員の指摘がバラつく。　正反対のことを言われることもあり、どこまで対応すべきか迷うことがある
情報セキュリティの活動・重要性を末端の社員まで浸透させるのに苦労している。　多くの社員に係わってもらうため、内部監査員の増員や事務局担当もローテーションで行うことを検討している
ISO14001(環境ISO)も認証取得している。　また、小職はその他、ISO9001、OHSAS18001も前勤務先で取得に関係していた。　これらISOに比べ、ISMSは規格の要求事項を満たすためにマニュアルや運用帳票以外に付属の文書類が多く必要であり、これらをごく一部の従業員しか熟読（理解）していないのが実情である。 規格と照らし会わせて、できるだけ文書を軽減（できれば削減）したいと常々思案しているが、審査時に不適合を受ける懸念が排除できず、悶々とした状態が続いている
課題：　セキュリティ意識の個人差がある。　例：引き出しの施錠忘れなど
維持していくために、本来であれば専門部署が欲しいがそこまでは行えず、個人の負担が大きい。　スタート時に全社ベースで取得したが、そろそろ考え直す時期にきているかも知れない
ISMS認証の維持・運用に費用とマンパワーがかかり過ぎる。　もっと楽にとれたら良いと思われる
社員への啓発活動と平行し、協力会社社員に如何に情報セキュリティ意識を高めてもらうかが課題となっている。　５年近くの活動を通じ、社員へはISMSが浸透しているが、協力会社メンバーの意識はまだまだ低く、問題も発生しており、この改善が課題になっている
現在、一部部局のみISMSの認証取得を受けているが、セキュリティ対策は全体で取り組むべき課題と考えている。 しかし、ISMS認証取得では業務に直接関係しない審査のための書類作成が必要になることがある。　全体にISMSの活動を広げるにあたり、このような作業は避けたいと考えている。 現在は、認証取得を受けていない部局でも有効なセキュリティ対策の実施が担保できるような取組を検討中です
情報セキュリティは仕組みが必要であることは間違いないが、どんな仕組みを構築したとしても、""ひやり""、""はっと""は防げても、悪意を持った人間やソーシャルエンジニアリングに対抗できない。　セキュリティ事故の要因が組織内の人間にあるケ

ースが最も多いことから考えれば、個々人の倫理観を高めることが最も重要なのか？ 問１６： その他： コスト増、業務量の増は発生しているが、想定したもの
他社が ISMS の取組で、どの様な工夫をされているかが気になる
① 事務局の負荷（準備・調査事項、もしくは改善事項）が大きいため、今後改善をし、効率化することが必要と考えている ② 複数のデータセンターで、リスク評価や管理策にバラツキがあり、均質な適用を図っていくことが重要と考えている ③ 133 の管理策について有効性測定方法を自ら定義し、測定値を求めることはかなりの労力となる ④ 情報漏洩事故に対して、有効な管理策を行うことは難しいが、重要であると考えている
① 必要と思われる事柄の洗い出しが不十分なため、ルールを作成しても短期間で変更しなければならない ② １つの事柄に対し、リスク分析が必要なものが多く時間が取られる ③ ISO27001 に関しての情報交換や事務局等の同じ立場の人のコミュニケーションが欲しいと思った時期もあったが、会社それぞれの ISMS なので参考にならないのではないかと思っている ④ 業務を洗い出し、必要なものを資産として登録するルールを作る。 リスクを洗い出し、是正や予防すべて事項を明確にしなければいけないが、１つ１つに時間がかかる上に、是正、予防をなかなか理解してくれない ④ トップダウンであるにもかかわらず、トップがルールを勝手に変えるので、管理職もそれにならいはじめ、一般社員への示しがつかない。 ⇒ 効果測定ができない
認証取得当初はコンサルと審査員の意見の違いに愕然とすることもあったが、コンサルに頼らない、審査員に振り回されない独自の ISMS を目指し、かなり改善された 従業員の理解と協力は難しいし、審査のための書類作成は大きな負担となっている。 何よりトップが意欲的に参加しないと形骸化し、審査のための ISMS となってしまう 現在はどう本業に活かせる ISMS を築けるかを課題に取り組んでいる
① メールのご送信、かばんの紛失などへの有効な対策が見あたらない ② 本社のみが現在では ISMS の認証範囲となっているが、地方支店への展開はハードルが高い（料金、業務、運用的に） ③ 最低限の ISMS 運用はできていると思うが、これ以上の踏み込んだ ISMS の取組と効果が疑問
① 全社的な取組を行っているが、参加者の積極性には温度差がある ② 元々、セキュリティ事故を起こした事のない社風や仕事への取組方だと思うが、管理策を取り入れて、マネジメントシステムを導入する事で、意識の面でも実務の面でも確実にセキュリティレベルが高くなったと思う ③ ISO27001 の取得が圧倒的に日本の企業が多いというのは少し不安。 海外から別のスタンダードが入ってきて、振り回されなければよいが
ISMS の普及・展開は QMS、EMS 等に比べ難しい。 頭から毛嫌いしている社員が多い
要求事項や実践のための規範が現在の ICT の技術進歩と乖離しつつある。 セキュリティの精神を守って、どの様に守るかの具体的な対策は各社の裁量で行うのが良いと感じている

″弊社では、今月認証を返上した。 何か協力できることがありましたら気軽にご連絡下さい。 中央大学 OB として調査に協力させて頂いた″
内部監査の監査内容のマンネリ化と監査を行う時間を取ることが難しい。 ISMS 推進部門と社員の教育ができていない（教育内容と時間）
① 教育に関する設問では、ISMS 教育と情報セキュリティ教育の使い分けが悩ましかった。 当所では以下のように切り分けている。 • ISMS 教育・・・リスク分析等の手法等 • 情報セキュリティ教育・・・事故事例や規則、運用の解説 ② ISMS マニュアルや ISMS 文書で関連規則との関係付けを行っているが、それが足かせとなり、煩雑化や規則の整備が出来ない（反映を洩らせば指摘される）と言った本末転倒も生じている
2002 年 6 月に BS7799 の認証を取得して 9 年目になる。ISMS の導入時に網羅的にリスクと管理策を検討するのは有意義であるが、維持管理、スパイラルアップは難しい。審査員の質問は本質的には毎年同じで、新鮮味が薄れているが、事故・トラブルがなくなることはない ISO9001、14000、27001、その他、マンネリを感じつつ、何がいつまで有効か、マネジメントシステムは重要と思うが、認証維持は必要か等々、一度総括する必要がある このアンケートや情報セキュリティ心理学の研究で分かったことをフィードバックして欲しい
JISQ27001:2006 と JISQ15001:2006 の統合（社内規定、帳票）を進めている。 両規格に従って作成した社内規定にそれぞれ従っているため、強い方の規程に合わせると実情に合わなくなってきた。 例： 外部訪問者の記録・・・ISMS では情報資産が会議室になければ記録不要、PMS では社内に第三者が入れば必ず記録
現状は特に大きな問題はない。取得３年目の更新審査が終わり、従業員も変わらず、最低限のセキュリティ体制はできている。 引き続き、業務効率を下げずに、かつ、しっかりとした体制が保てるよう努めるだけ
① 外部審査について、サンプリング審査なので仕方ない面もあるが、審査員により、指摘されたり、されなかったりする ② サーベイランスと更新では工数にかなりの開き（約２倍）があり、これが経費に直接跳ね返ってくるので厳しいところがある
① 審査員の受信側セキュリティレベルの理解が必要。 ISMS 認証取得企業のセキュリティレベルを明確にした方が良い。 工数計算時のようにレベルを明示できれば審査員とのコミュニケーションも円滑に進められると思う ② 有効性を強調する余り、適合性を疎かにする審査員も目につく。 ISMS の適合性評価は他の規格より重要であると思う
ISMS の認証継続にあたり、当社では一般従業員の業務に大きく負荷をかけることはないように ISMS 事務局でほとんどの業務を実施している。 貴研究室で実施した前回調査報告で、当初の事務局員が少なくなって世代交代ができている企業も見受けられるが、当社では未だ事務局員が当初から交代せず通常業務と兼務で担当している。 世代交代できた企業は、どのように ISMS の運用スキルを継承したのか？ 世代交代後、以前と変わりなく ISMS が運用できているのか？ 以前の事務局員が一人もいない企業は、以前の事務局員が全くサポートもせず運用されているのか？ 当初の事務局員は

ISMS の構築から体で身に付けたと思うが、現在の事務局員の意識は？（やらされ意識など受け身になっていないか？）等、今後の調査報告でこの辺りが記述されていると、これらの調査に回答している意義がでてくる。 今回の調査から、この辺りに新たな疑問が湧いた次第です
マネジメントシステムそのものや、各施策の実施に対する有効性評価をどういう観点でどう評価していくかが難しいと感じている
本回答が何かしらの成果に結びつけばいいと思っている。 宜しくお願い致します
問 65 で、中国から帰国した出張者が電子記録媒体（ＵＳＢメモリ）を介して日本国内の工場のＰＣに感染させた。 ＰＣのワクチンソフトは最新のパターンファイルになっていたがアラームが出ず防げなかった
ISMS 維持・運用の専任部署はないため、そのリソースに関して各部で限りがあり事務局として十分に機能していないという課題がある。しかし、現状では、できる限りの対応を行っている。 ノート PC について持ち出しルールは業務上の制約があるため制限を設けることはできないが、メールチェックのみであるならば、Blackberry の利用の推進などで対応している。(パスワードが必要なため紛失時に対する情報漏えいのリスクの軽減を図ることが可能)　　また、ソフトウエアについては、グローバルで定義されたソフトウエアのみ使用可能であるため近年ウイルス感染に関する被害は軽減している。しかし、海外出張時にウイルス感染する事例があり、ウイルス対策については、社員に認知されている
全社での問題報告、改善提案がなかなか集まらず、維持レベルが少しづつ低くなってしまう
ISMS 認証と P マーク認証の両立について、 ① 両立できる効率的運用方法はどの様にするのか？　特に、両認証の適用範囲が異なる場合 ② 対外的（グローバルな視点も含む）な効果としてどの様に考えられるのか？　例：入札条件等
① ISMS の維持活動が定着し、社内での PDCA や、内部監査等からの改善が図られる一方、審査員から実効性のある指摘が少なくなり、今後、審査にかかる負担の軽減または、有効性を向上させるための施策を検討していく必要がある ② 情報漏洩事件を切っ掛けに、それらを教訓とした都度チェックが頻繁かつ迅速に行われているのに対し、従来の定期的な情報資産の洗い出し、リスク評価、分析から発見されるリスクは軽微かつ限定的なものが多く、定期的な作業に対してのモチベーション維持が課題である
① 認証から年月が経つにつれて、マンネリ感がある。管理職層の再教育が急務 ② スマートフォンなど新技術の導入に際し、手順等の対応が追いつかず、セキュリティレベルが落ちているのではないかという不安がある ③ セキュリティを強固にすることと、業務の便利さは反比例するものであり、弊社のような SI 事業を行っている場合、新技術を利用したシステムを調査・開発する（試作的なもの）という行為とセキュリティを強固にするということが、両立できないことがあり、板挟みである
管理策の有効性測定に課題を感じている。 現在、セキュリティ対策の実施状況をサンプリング測定して、対策の有効性を評価しているものもあるが、多くは、セキュリテ

ィ対策の実施状況は部門で自己評価した結果をそのまま有効性評価しており、一応、定性的な評価になっている。 負荷をかけず、管理策の有効性を定量的に評価できる方法を模索している
リスク分析、管理策の決定において、考え過ぎな面を気にする人が生じ、業務効率とリスク対策のバランスの良い管理策の合意に難しい点がある（バランスの良い管理策のアドバイスが早く出ると良い）
年１回の審査ではなく、半年に１回くらいの審査でよいのではないか。 アンケートは担当者でなく、会社に送付して欲しい
情報セキュリティの観点から、P マーク認証の要求事項を ISMS 体制に統合することを検討している（個人情報は ISMS 上で追加管理策として定義し、独自に ISO15001 要求事項を満たす管理策を維持する。　P マークは得られないが致し方ない)。 理由は、個人情報も含めてセキュリティについては単一のマネジメントシステムにて管理したい。 自社業務が直接顧客情報は扱わない（従業員の個人情報のみ)。　認証維持に関わるコストが大きい、等があげられる。 両者に共通するのはリスク対策部分のみで、範囲は異なる点も多いが、個人情報も情報資産であり、ISMS の拡張で個人情報保護をフルにカバーできると考えている
問１は、会社全体の資本金を示す。　問 10-2、10-4 は会社全体で取得しているもの
① 現状が「正しい」のか「あるべき姿」なのかの確証が持てないため、基準・運用が右往左往する ⇒新たにコンサルタントを選定し、再構築を開始した ② ISMS と P マーク（PMS)の２重運用が非効率に思える ③ 規格の要求事項とポリシー類が合致しているのか、精緻に付け合わせできているとは言えない ④ 弊社は「セキュリティ委員会」と「同事務局」で合計 12 名の人的コストをかけているが、コストに見合った成果が上がっているとは言い難い ⑤ 外部審査・内部監査における指摘への対策が不十分、もしくはどこまで対応すればよいかが不明 ⑥ リスクアセスメントからの一連の文書が効果測定の指標となり得ていない
財政難による予算の削減や、運用面の乖離等により平成２２年４月をもって、ＩＳＯ２７００１認証取得を取り下げた。 それ以後は、自主運用に切り替え運用がし易いよう規程類の見直しを行ない実施している
当社はコンサルタントを用いず自社独自の取り組みで認証の取得、維持を行っている。そのため、認証取得以前にあった情報セキュリティ関連ルールをベースにマネジメントシステムを構築し、ルールの有効性の評価と継続的改善に利用しているため、運用上の違和感は少なく、むしろルールの形骸化、形式化を防ぐための良い仕組みであると感じている。 ISMS とはセキュリティに関する管理策やルールそのものではなく、経営陣を含む組織の中で継続的改善を図る営みのことであると理解している。そのため経営陣を始め、組織の管理職の積極的な関与が重要であると考えている。 しかしながら最初は、マネジメントシステムの構築よりも個別の施策が先決になってしまう傾向もあり、これを理解して貰うことが課題です。 コンサルタントを入れて実施されているところは、どのように対処されているのか興味がある。　今後とも、是非情報交換をさせて欲しい
現在適用範囲の拡大を考えているが、各部署への教育方法を検討する必要がある

当社は廃棄物処理業務を行っており、ISMS の 30%しか意味がない。 しかしながら大手企業の廃棄物を適正に処理するための一つの方法であり、信用おけるものとして取得している。　ただ、審査費用等があまり高度すぎては意味がない
対象機器の拡大、スマートフォンやタブレット端末も今後は対象とせざるをえないと考えている。　内部監査やアセスメントが現場に与える負荷。　個人情報の管理を重点とするプライバシーマーク取得の方が負荷が軽い。　運用については行動ベースでシンプルにまとめたい
ISMS の維持・運用を行うことで、情報資産に対するリスクは低減するが、実際にリスクアセスメント等の作業部門の負担は小さくない。　そのためいかにセキュリティレベルを下げずに効率的な ISMS 活動に改善していくことができるか、等が ISMS 維持・運用を行う上での課題だと考えている
① 「行った」という確証を審査時に必ず要求されるが、確証が必ず残るものばかりではない。 しかし、部門としては説明がしやすいため、「審査のための確証」を準備する傾向がある（その分コストが発生する） ② 一度認証を取ってしまうと、もうやめられないのでは？　と思う。　何かがあった時、「認証をやめたせいだ！」と言われるかねないので、誰も言い出せないと思う。 ※「情報セキュリティ心理学」非常に興味がある。連絡を頂ければご協力させて頂く
情報セキュリティサービス会社として、サービスを提供する社員がまずは高いセキュリティに対する意識を持つことが求められるが、日常業務の忙しさから、ルールを守らないということが頻発している。　些細な内容のことでも重大なインシデントにつながる可能性があるので、情報セキュリティ運営組織を中心に内部監査（簡易なもの）を多く実施することで意識の向上を続けている
ISMS の維持では、情報セキュリティに対する設備投資が必要になる。 中小企業にとっては、金額面の負担が大きく、難しい。 ISMS に係わらずとも顧客要求事項として対応せざるを得ない部分ではあるが、資金、人材をも十分とは言えない中、厳しいものがある
① ISMS 教育を実施しているが、従業員１人１人にまで意識がまわらない ② 認証取得してから、４年経つが、リスク分野の手法に限界を感じている
ISMS の事務局として、組織が作成した年間スケジュールに従い、決められた活動が実践されているか、つくられるべき成果物が作成されているか等を管理するツールがあると、便利だと思う また、先進的な ISMS 活動を実践している組織事例（情報を公開できる範囲で）等を紹介頂けると有り難い 今回のアンケートが有意義なものとなりますことを期待している
社員の情報セキュリティレベルを一定にするのに大変苦心している
現時点での課題は以下の通り ① 効果的なリスクアセスメント手法の採用 ② 有効性の測定指標の開発
ISMS を含む各マネジメントシステムと従業員の作業負荷とのバランスを取ることが重要だと認識している
人、物、金の限られたリソースをどこまで投資して有効性を確保するか常に考えている。　リスク分析、事業継続分析等難しいと感じている。　また、社員への意識付け

も定期教育等で実施しているが、どこまで理解しているか、実践できるか、等が課題と考えている

（注）今回の ISMS 調査に直接関係ないコメントや記入組織、記入者を判断できないように一部のメッセージの表現を多少変えてある。

発行日　　平成 23 年 3 月 31 日
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 番地 5 号　新目白ビル６階
電　話　　(03) 5287-5034
ＦＡＸ　　(03) 5287-5029

調査者　　中央大学 研究開発機構　内田勝也研究室
住　所　　〒112-8551　東京都文京区春日 1 丁目 13 番地 27 号

平成 22 年度 ニューメディアを基礎とする調査研究事業
（ISMS 第三者認証制度をより有効なものにするための
ISMS 認証事業所調査）

URL　http://www.nmda.or.jp