

情報セキュリティマネジメントシステム (ISMS)
認証事業者実態調査

Survey of Registered Organizations of Information Security
Management System (ISMS)

中 尾 宏 内 田 勝 也
Hiroshi NAKAO Katsuya UCHIDA

情報セキュリティマネジメントシステム (ISMS) 認証事業者実態調査

中尾 宏* 内田勝也**

企業や組織への情報セキュリティ対策は、経営層から利用者までの広範な人たちを巻き込んだ、全社的・包括的体制の構築が基本になる。国内では、2002年4月から「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」が本格運用され、2013年10月現在、約4,440事業者が認証取得をしている。2009年のISO調査では、全世界の43%を日本が占めている。しかし、他の認証制度と同様、認証取得効果への疑問、制度の誤解、制度運用の課題も浮上してきている。本稿は、今回で第4回目となる国内で唯一大規模なISMS認証事業者への調査を通して、制度、運用、推進等での課題を明確にし、その対応について考察した。

キーワード：情報セキュリティマネジメントシステム (ISMS)、ISO/IEC 27001、リスクアセスメント

Survey of Registered Organizations of Information Security Management System (ISMS)

Hiroshi NAKAO* and Katsuya UCHIDA**

Information security in business organization basically is to establish a comprehensive and corporate-wide system including from management executives to end-users.

In Japan, from April 2002, a Conformity Assessment Scheme for Information Security Management Systems (ISMS Conformity Assessment Scheme) had been operated officially. As of Oct. 2013, about 4,440 organizations have gotten the certification.

Moreover, Japan accounted for 43% of total world in the ISO Survey of 2009.

However, as with other certification systems, the doubt to the certification effect, misunderstanding of the system, issues of systems operation has also emerged.

The survey of the fourth to the ISMS certified organizations is the largest one in Japan. And we identify and discuss about the ISMS's system, and the implementation, the operation.

Keywords: information security management system (ISMS), ISO/IEC 27001, risk assessment

*東京情報大学 総合情報学部 環境情報学科

Tokyo University of Information Sciences, Faculty of Informatics, Department of Environmental Information

**情報セキュリティ大学院大学

Institute of Information Security

1. はじめに

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月に、ISO/IEC 27001/27002は、JIS Q 27001/27002: 2006として、日本規格（JIS化）になった。2013年10月7日現在、4,390の事業者¹が認証を取得している。

世界におけるISMS認証取得事業者数の半分以上²を日本が占めており、傑出した登録件数になっている。しかし、取得後に業務負荷が増大した、ISMSの考えが隔々まで浸透していないとの回答だけでなく、ISMS認証取得を維持するために二重帳簿的対応をしているという声まで聞こえてくる。このような認証制度的課題は、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者に対して適切でない、あるいは、審査員毎に異なる指摘内容に悩まされている事業者がある。さらに、審査費用が高いとの不満まである。

第3回の調査では、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が、今回の調査（第4回調査）は、平成24（2012）年12月末時点の全認証取得先を対象にした。第1回及び第2回の調査では、住所非公開事業者への送付は行なわなかったが、今回は、ウェブで認証取得を公開している住所非公開事業者を可能な限り調査し、アンケートを送付した。

今回の調査結果は、ISMS認証取得事業者や認証機関、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である。

2. アンケート調査内容

今回の調査では、住所非公開のISMS認証事業者を可能な限り調査し、約3,800事業者に、アンケートを郵送して、調査を行った。

質問項目については、前回（2010年度）の調

査に準じた項目にしたが、審査員が審査（審査/サーバランス）で確認する文書類を調査するため、「初回審査で確認した文書に関する質問（問40）」を追加した。また、2012年6月にISMS認証取得事業者による大規模なサーバ障害の事故が発生していることから、ISMSの認証取得の有効性を評価するために、「更新審査で確認した文書に関する質問（問41）」を追加した。

調査項目を大幅に変更すると、継続調査の特徴である比較調査が難しくなるため、以上のように基本的には前回の調査を踏襲した。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。新規項目は、前述した項目を追加した。このため、質問は67項目であるが、1項目で2つの内容⁴を聞いている項目がある。

質問は以下のグループに分けた。各グループの質問の概要は以下の通りである。

(1) 事業者、記入者の基礎情報の質問（7問）

事業者の組織規模（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

(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、提案者、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（9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 3 回と同様、回答を得た ISMS 認証取得事業者に訪問し、郵送のアンケート調査を補った。

なお、認証機関へのアンケート調査は実施しなかった。

3. アンケート調査について

3. 1 ISMS 認証取得事業者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 2012年12月20日

アンケート回答締め切り

2013年02月02日

注) アンケートは、3月31日(日)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 3,786事業者

2012年12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 認証取得事業者から、3,786事業者を選んで送付した。住所が非公開の事業者はウェブ等を調査し、認証取得事業者の ISMS 事務

局宛てに送付した。

(3) 有効回答数

最終的に回収した件数は、2013年3月31日時点で、453事業者から回答を得た。回答率は12.0%であった。

(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、国内事業者の中には、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いわれており、この調査も回答は無記名を原則⁵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。

(6) アンケートの特徴

アンケート全体としては以下の特徴がある。

- 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。本調査の回収率は、前回(2010年)22.1%(426事業者)、前々回(2008年)16.8%(352事業者)、初回(2006年)18.6%(264事業者)であった⁶が、今回は12.0%(453事業者)の回答があった。今回は最低の回収率だが、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高い回収率で、調査対象である ISMS 認証取得事業者にとって、本調査内容に対する関心が高いことを示している。

- 自由意見、記名回答の多さ

本調査は無記名方式であるが、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3,786事業者の

内、回答があった426事業者の内、企業名記入は258事業者 (60.6%)、記入者名記入は231名 (54.2%)、メールアドレス記入は198事業者 (46.5%) があった。回収した453事業者の半数が実名でアンケートに回答している。

必ずしも件数は多くないが、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)、審査員の「適用宣言書⁷」未確認等、ISMS運用上の課題について記名で指摘してきた事業者がある。

3. 2 ISMS認証取得事業者インタビューの概要

(1) インタビュー実施日

2012年4月25日 (木)～4月26日 (金) の2日間。

(2) インタビュー対象

認証取得事業者5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

各事業者の回答内容は、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。(※紙面の都合により本報告書には添付していない。)

(5) インタビュー

認証取得組織の現状、すなわち、ISMS事務局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、訪問・面談することにより、確認を行ってアンケート法による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 回答事業者組織の基本情報

(1) ISMS認証取得事業者の規模

今回の調査でも「1,000万円以上5億円未満」の事業者が、全体の7割以上 (78.1%)

を占め、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」の組織は調査を重ねる度に減少する傾向にあるが、依然全体の2割弱 (16.4%) を占め、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、毎回増加傾向にあった、従業員300人未満の事業者の割合が75.9%と前回比10%以上の増加となった。前回65.7%、前々回64.4%、初回58.9%であり、小規模な組織でのISMS認証取得の必要性が高まっていると考えられる。

(2) ISMS認証取得業種

今回の調査でも以前の調査と同様、「情報通信業」が40%以上を占めており、最大の割合になっている。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「情報システム安全対策実施事業者認定制度⁸」を廃止し、技術的な情報セキュリティと人間系の運用・管理面の情報セキュリティマネジメントを取り込み、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とが、情報通信業が大きな割合を占める理由と考えられる。

第2位は、「製造業」(9.3%)で、初回の3位から前々回、前回と2位に順位を上げたが、2位の変化はない。第3位は「複合サービス業」(9.1%)で前々回、前回と同じである。

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、公務 (政府・自治体)、以下、医療・福祉、金融・保険業、教育・学習支援、不動産、電気・ガス・水道となるが、前回、前々回とは1桁台での相違であり、大きな差異は無い。

(3) アンケート回答者の所属部門と役職

今回の調査では、前回同様、前々回に2位だった総務（含人事・経理）部門（133件、29.4%）が、前回同様2位の情報セキュリティ部門（80件、17.7%）を抑えて、トップになった。3位は、情報システム管理部門（52件、11.5%）で、前回、前々回と同様である。これら上位3部門で全体の約60%を占めた。理由は明確でないが、情報セキュリティ部門が組織化され定着してきた可能性がある。また、他の規格の認証取得している事業者が半数以上の57.3%あり、他の規格のダブル認証取得が、総務部門がトップになった理由と考えられる。

回答者の役職は、課長（24.1%）、部長（20.8%）、一般社員（15.0%）の順で、前回と同様で、上位3位の役職階層で全体の約60%（59.8%）を占める。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化がないが、会長・社長の割合が前回より高い。

前々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、前回と情報セキュリティ責任者（30.8%から34.2%に）、ISMS事務局責任者（37.9%から31.5%に）の順位が入れ替わり、三位にISMS事務局員（26.7%から28.4%に）の順となる。

記入者のISMS認証業務の経験年数は、今回の調査では、「1年～3年未満」が31.5%で、前回トップであった「3年～5年未満」の25.8%を上回ったが、3年以上の経験者が63.7%を占めており、前回と同様に経験豊富な担当者が多くを占めている。

4. 2 ISMS認証取得に関する事項

(1) ISMS認証取得年月

2006年の取得が最大（73件、16.5%）で最も多く、2015年（59件、13.3%）、2008年（54件、12.2%）、2009年と2011年が（51

件、11.5%）と続くが、以前の調査と大きな相違はない。

(2) ISMS認証取得事業者の従業員数

認証取得対象従業員数では、100人未満（309件、69.8%）、100～300人未満（92件、20.8%）の順で、この2つで全体の90.5%を占め、300人未満規模の事業者がISMS認証を取得している。

ISMS認証制度では、ISMS取得範囲は組織の一部分でも良く、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（309件）の3/4以上（229件、74.1%）は100人未満の組織が、12.6%（39件）を100人以上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人未満と回答した事業者がある。これは複数の企業（グループ企業と考えられる）でISMS認証を取得していると考えられ、他の人数でも同じ。

(3) 他の認証取得状況と取得年月

ISO 9000（127件、28.0%）、プライバシーマーク（122件、26.9%）、ISO14000（110件、24.3%）の順になっており、前年と2位、3位が入れ替わったが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（177事業者）、1つ取得（137事業者）、2つ取得（79事業者）、3つ取得（26事業者）、4つ取得（4事業者）、5つ取得（1事業者）となっており、アンケート回答事業者（453事業者）の内、276事業者（60.9%）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」（327件、72.2%）が最も高い結果で、次いで「情報セキュリティ対策向上のため」（288件、63.6%）と

っており、これらは過半数を超えている。前回に続き「業務改善」(203件、44.8%)が3位で「入札」(157件、34.7%)を上回った。ISMSが入札条件になっている官庁・自治体があるが、それらに入札するだけの規模・実績がないため、入札が必ずしも高くないと考えられる。

小規模事業者では、大企業等のSCM(サプライ・チェーン・マネジメント)に入ることが重要になる。

(5) 認証取得の提案者

ISMS認証取得の提案者は、会長・社長(262件、61.9%)やその他取締役(76件、18.0%)、管理職(76件、18.0%)となっており、トップダウンによることが分かる。

執行役員(20件、4.7%)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と考える。

(6) ISMS認証の運用責任者は？

前回、前々回と順位は同じで、その他取締役(158件、36.7%)、管理職(144件、33.4%)、会長・社長(79件、18.3%)の順である。

(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は、前回と前々回と順位は同じで、「変更予定なし」(314件、69.6%)が最も多い。ISMS認証はプライバシーマークと異なり、必ずしも組織全体を取得の単位としていないため、取得後にISMS認証範囲の組織拡大⁹を考える事業者がある。

なお、ISMS認証以外の認証を取得している事業者が約60%あるため、統合審査等を検討している事業者があると判断できる。

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？

上位は、以前と同じで、「社員のセキュリティ意識の浸透と実践」(400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%以上の割合になっている。

(2) ISMS認証取得での想定外の影響は？

「業務への影響はない」(116件、25.6%)との回答は、調査を重ねるたびに、増加している(初回：46件・17.4%、第2回：79件・22.4%、第3回：103件・24.2%)。しかし、「業務量の増加」(163件、36.0%)や対策コストの増加(147件、32.5%)、「組織・人が必要」(143件、31.6%)は「業務への影響ない」の回答より高くなっている。「業務上の制約の増加」(105件、23.2%)と「手続きの煩雑化」(89件、19.6%)が「業務への影響はない」より低くなっているが、20%前後の事業者が回答しており、依然としてISMS認証制度の定着化に苦勞している様子がうかがえる。

全体(453事業者)の内、半数近く(45.0%)の204事業者が、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、さらに、その内、117事業者(25.8%)が「監査目的のための資料作成」をその具体的な項目としてあげている。ISMS審査(更新審査やサーベイランス)や内部監査向けの資料作りが負担になっている。

また、105事業者(23.2%)が業務上の制約を増やしているが、92事業者(20.3%)が機器の取扱(持出・持込)の制約、58事業者(12.8%)が上長の承認の増加、54事業者(11.9%)が資料作成ルールと回答している。

(3) ISMS認証後の運用上の負担と重点的な取り組み

ISMS認証取得後の運用で負担になっていると感じている項目には、「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、41.5%)、

「リスクアセスメントの見直し」(180件、39.7%)、「情報資産台帳の見直し」(175件、38.6%)、「内部監査対応」(172件、38.0%)の順になっている。以前の調査でも、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」(291件、66.4%)が半数を超える回答があった。それ以降は、「教育研修の改善」(130件、29.7%)、「内部監査担当のスキル強化」(121件、27.6%)「管理者層の認識・理解の強化」(117件、26.7%)、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」(192件、42.7%)、「どちらとも言えない」(159件、35.3%)、「乖離はある」(99件、22.0%)となっている。なお、前回の調査では、「乖離はない」は、38.2%、「乖離はある」が26.5%で、今回の調査では、乖離を感じていない事業者が前回調査より増加、「乖離はある」の二倍近い回答を得ている。

(5) ISMS維持費用について

ISMS維持費用については、前回の調査とほぼ同じく、「高い」(250件、55.8%)との回答が「妥当」(193件、43.1%)との回答を上回った。景気の影響もあるが、一部には審査との兼ね合いで高いと回答している事業者もある。

4. 4 ISMS認証に関連する体制等について

(1) ISO 27002をどこまで取り入れたか

全体としては、前回、前々回と続けて大きな相違はなく、「参考程度」(186件、42.3%)、「十分に取り入れた」(153件、34.8%)としている。

(2) ISMSの継続的な運用のための経営陣のマネジメントレビュー以外の関与

経営陣のマネジメントレビュー以外の関わりについては、初回(2006年)以降毎回

80%前後の高い回答を得ている。今回も「関わっている」(361件、82.4%)、で、経営陣の積極的な関与がうかがえる。

(3) ISMS事務局

ISMS事務局の人数は、「4~6人」(133件、29.7%)、「2人」(112件、25.0%)、「3人」(81件、18.1%)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になるが、300人未満の認証取得対象従業員数の割合が約76%であることを考えると、事務局の人数としては妥当である。

ただし、1名のみで兼務が40事業者、2名で兼務が196事業者あり、ISMS業務が定着していない事業者では、事務局の人数を絞った人数となっている。

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」(163件、42.6%)、「50~70%未満」(23.2%)、「一人もいない」(47件、12.3%)の順になっており、半分以上(65.8%)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、52.9%)、「OJTによる習得」(197件、45.3%)、「外部講習によるスキル習得」(30.6%)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、社内教育も可能になる。

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が行われていないため、コンサルタントに関連する質問を前々回、前回に引き続き行った。

(1) コンサルタントを利用について

以前の調査と大きな相違はなく、認証取得までは、70%以上の事業者がコンサルタ

ントを利用しているが、認証取得後は逆に約70%の事業者が利用していないと回答している。認証取得時の知識・経験があれば、事業者独自にISMSの運用を行うことが可能である。

(2) コンサルタントの各種理解度

コンサルタントの評価については、全般的に低く、10段階評価で8以上がない。また、前回から比べると多少高くなっているが、誤差の範囲である。

コンサルタントの評価項目	今回 (2013年)	前回 (2010年)
(29) ISMSの理解度	7.87	7.85
(30) 情報セキュリティの理解度	7.92	7.79
(31) 認証取得事業者業務の理解度	6.73	6.62
(32) コミュニケーション能力	7.22	6.95
(33) 実効性のある提案	6.82	6.54
(34) 確立したコンサル手法	6.90	6.67
(35) 一貫性を持ったコンサルテーション	7.12	6.97
(36) ISMS認証取得に役立った	7.82	7.72

① 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。277事業者が回答している。「高い」(117件、42.2%)、「妥当」(131件、47.3%)とほぼ拮抗しているが、妥当が若干高くなっている。

② コンサルタント選定で最も重視した項目

コンサルタントの選定にあたり、上記(①～⑨、質問の29～37)のいずれを重視したかについては、327事業者が回答している。「⑧、36. 認証取得に役立った」(78件、23.9%)が最も多く、次いで、「⑦、37. 費用の妥当性」(51件、15.6%)、「⑤、33. 実効性のある提案」(50件、15.3%)となり、当然のことながら、認証取得に役立つコンサルタントを求めている。

③ コンサルタント導入の最終判断者は？

330事業者が回答しているが、トップダウンによる決定の感があり、「1. 会長・社長」(225件、68.2%)が最も多く、次いで、「2. その他取締役」(46件、13.9%)、「3. 執行役員」(18件、5.5%)である。

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。他の認証システムでも、従来から、一部の認証取得事業者の不満として、審査員の質や態度が挙がり、今回は新たに2問(初回審査及び更新審査で審査員が確認した文書類)を追加した。

① ISMS審査員が初回審査で確認した文書類は何か

ISMSの審査において、「適用宣言書」は認定取得事業者にとって、重要な文書の一つといえる。リスク軽減のために管理策の選択や追加を行い、事業者が事業への管理策の適用にあたって必要がないと判断すれば管理策を適用除外とする。事業者が取り組む管理策を外向きに宣言し、ISMSの運用にあたっての拠り処となるものである。しかし、ISMS審査員が、適用宣言書の重要性を認識せず適用宣言書を確認しないで、審査を実施していると、複数の事業者が回答している。

初回審査で審査員が確認した文書類について431事業者が回答した。「適用宣言書」(404件、93.7%)、「内部監査資料」(408件、94.7%)、「マネジメントレビュー議事録」(403件、93.5%)、「リスク対応計画書」(407件、94.4%)は、いずれも90%以上の高い回答を得ている。

② ISMS審査員が更新審査(サーベランス)で確認した文書類は何か

409事業者が回答し、「適用宣言書」(330件、80.7%)、「内部監査資料」(397件、97.1%)、「マネジメントレビュー議事録」(396件、96.8%)、「リスク対応計画書」(381

件、93.2%)は、更新審査では適用宣言書を確認していない事業者が初回審査よりさらに増え、79事業者(19.3%)ある。

事業者は、適用宣言書を確認しない5審査機関名を実名で挙げて回答している。この内、2審査機関は複数の事業者で回答していた。事業者名を記載しない回答の中には、適用宣言書を確認していないとの回答があり、さらに多くの審査機関が適用宣言書を確認していない可能性がある。

審査員の評価項目	今回 (2013年)	前回 (2010年)
(42) ISMSの理解度	8.90	8.65
(43) 情報セキュリティの理解度	8.60	8.31
(44) 認証取得事業者業務の理解度	7.43	6.98
(45) コミュニケーション能力	8.07	7.66
(46) 実効性のある指摘	7.89	7.39
(47) 効果や課題の確認能力	7.98	7.58

③ ISMS審査員について、最も重視する項目は何か。

422事業者が回答しており、「実効性のある指摘」(230件、54.5%)が前回と同じく半分以上を占めている。次いで、「貴組織の業務の理解度」(72件、17.1%)、「効果や課題を確認する能力」(38件、9.0%)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)

452事業者のうち「1年に1回」(344件、76.1%)を占めており、前回(77.1%)より若干低下しているが、長期的には増加傾向にある。年何回のサーベイランスを実施するかは、認定機関の基準に従い、受審側の負担や効率性を鑑みて、受審側事業者と認証機関との相互で定める。実際は年1度が多い。

(2) 内部監査体制について

内部監査体制については、以前は、非常設社内チームがトップであったが、前回に続き、今回の調査でも467事業者のうち、「常設社内チーム」(223件、47.8%)が約半数を占めている。それでも、「非常設社内チーム」(207件、44.3%)がまだ半分近くある。

(3) 指摘事項は改善されていますか？

初回の調査から「改善されている」との回答が連続して減少している。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41.1%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。したがって、ISMS審査員は次回以降のサーベイランス等で改善の状況を確認する必要がある。

(4) マネジメントレビューの実施頻度と形態

「年1回」(331件、73.1%)が70%以上を占めており、次いで、「半年に1回」(92件、20.3%)となっている。ISMSでは、年1回、実施することを要求しているが、インシデントの発生や大きなリスクの懸念がある場合は、その都度、マネジメントレビューを実施することが必要である。内部監査の実施やISMS審査等の時期に合わせて、マネジメントレビューを実施している場合が多い。

マネジメントレビューを「会議形式で行っている」(411件、90.7%)が、今回も90%以上あるが、次第に減少し、「会議とメールの組合せ」(33件、7.3%)が増大している。今後、TV会議等が一般化すれば、TV会議によるマネジメントレビューの開催も増大する可能性がある。

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、以前の調査とあまり大きな相違はなく、「集合研修」(362件、79.9%)が最大であり、次いで、「冊子の配布」(176件、38.9%)、「OJT」(128件、28.3%)、「E-ラーニング」(140件、30.9%)と続いている。しかし、継続的にISMS認証取得して事業者のうち、4事業者が教育を実施していないと回答した。そのような場合、審査員はどのような審査を行うのか疑問である。

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」(267件、60.8%)、「冊子の配布」(117件、26.7%)、「OJT」(106件、24.1%)、「Eラーニング」(76件、17.3%)の順になり、前回の順位の3、4位が逆転しているが、前々回と同じ回答を得た。まったく教育が行われいない事業者が、25事業者ある。

経営陣への教育については、「集合研修」(207件、47.2%)、「冊子の配布」(106件、24.1%)、「E-ラーニング」(75件、17.1%)、「メール」(58件、13.2%)の順となる。なお、75事業者(17.1%)で、教育が行われていないが、経営者自身のISMSの重要性の認識を高めるために何らかの教育・啓発が望まれる。

(2) 社員へのISMSの教育頻度について

以前は、年1回、半年に1回が多かった社員へのISMSの教育が、前回の調査では、「3ヶ月に1回」(43.1%)、「月1～2回」(26.0%)となり、頻繁に教育を実施している傾向が見られると分析したが、今回の調査では、「1年に1回程度」(186件、41.3%)の40%を超える回答を得た。情報セキュリティについては、技術的な対応だけでは限界があり、利用者への教育・啓発の必要性が増大している。回答では、「半年に1回程度」(118件、26.2%)が多く、前回の回答と同様の結果になった。

(3) ISMS教育の担当部門とレベル

「情報セキュリティ部門」(225件、50.1%)が最大で、「総務(含人事等)」(118件、26.3%)が続く、「情報システム管理部門」(74件、16.5%)となる。

担当部門のレベルでは、設問が適切でなかったためか、有効回答が少なかったが、全体的には前回、前々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の具体的な方法について

啓発活動では、「ポスター掲示」(94件、20.8%)が、前回(71.4%)から大きく減少し3位に後退、「会議での連絡・通知」(306件、67.7%)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」(107件、23.7%)が続いている。

(5) 教育以外に行っている啓発活動の有効性の評価方法について

前回に続き、教育・訓練等についての有効性測定としてどのよう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：227件、60.5%、E-ラ：118件、78.7%)が最も多い。

ただし、集合教育では、「アンケートの実施」(95件、25.3%)、「出欠確認」(69件、18.4%)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」(28件、18.7%)、「出欠確認」(12件、8.0%)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、アンケートは意識の向上や認識の程度を知るにはよいが、教育・訓練の理解度を測定するには効果的な方法ではない。また、出欠の確認だけでは教育効果を測定できない。

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ないが、ISMS認証取得事業

者がどのようなことを行っているかを調べた。

(1) 情報漏えい対策について

上位4項目は、前回と同様に50%を越えており、「2. ログインパスワード認証」(435件、96.7%)、「パスワードの定期的変更」(392件、86.7%)、「ファイルの暗号化」(311件、68.8%)、「外部媒体接続制限」(236件、52.2%)の順になった。

パスワード認証、パスワードの定期変更は当然行うものであるが、ファイルの暗号化(前回67.1%、前々回36.9%)が次第に一般的になってきた。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)の社外持出ルール

ノートPC及び、外部記録媒体の持出で「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、約10%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」(381件、88.6%)や「外部記憶媒体」(373件、86.7%)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」(94件、21.9%)等では、前回と同様により高い割合になっている。

(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」(336件、76.0%)との回答が最も多く、次いで、「感染あり」(96件、21.7%)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

取得事業者では、感染が半分程度の割合になっており、コンピュータウイルス対策が有効に機能していると判断できる。また、感染無しの割合が前回より約10%向上しており、ISMS認証取得の効果がでている。

感染原因として考えられるのは、前回と同様「ウェブ閲覧によるドライブバイダウンロード」(40件、41.7%)が最も多かったが、「パターン更新漏れ」(16件、16.7%)が前回の19.7%から減少する一方、「ゼロデイウイルス」(23件、24.0%)が前年(15.3%)より増加傾向にある。

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いうより、「トロイの木馬」とか「スパイウェア」と呼ばれるプログラムであり、ワクチンソフトで検出することが難しい。

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柄や疑問、課題等について自由な記入を求めた。

何らかのコメント(除「特になし」等)が記入されていたのは、111件、24.5%(有効回答数:453件)あった。主な記述は以下の通り。

- ① ISMS認証システムは、有効性が高いとの評価がある一方、JIS Q 27001: 2006/27002: 2006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が多い。
- ② ISMS認証とプライバシーマーク等、複数の認証取得事業者では、共通項目が多いので、統合審査が出来ないかという意見が多い。しかしながら、複数の認証取得事業者では、統合審査の対応に苦労している。
- ③ 認証取得が目的化してしまう傾向がある。
- ④ ISMS推進担当者が少なく、作業負荷が大きい事が課題になっている。また、推進担当者が少ない場合、ISMSのノウハウ等

が集中するため、異動／退職時等に課題を残している。

- ⑤ 従業員に対する教育が徹底していないため、情報セキュリティに対する意識向上・定着化が難しい。
- ⑥ 削減に努めているが、インシデントがなかなか減らない。また、逆にインシデントは発生していないが、ISMSが定着していない。
- ⑦ 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。
- 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は多い。
- ⑨ リスクアセスメントや有効性評価が十分に行われていない事業者も多い。
- ⑩ 審査員に対する評価では、毎回の指摘事項が適切といった高い評価がある一方、審査員が毎回異なり、各審査員の指摘が毎回異なる、あるいは、レベルが低いとの声も多い。
- ⑪ ISMS維持費用（含審査料）が高額で、最近の不況時にはかなり厳しい。また、審査料に見合う審査が行われていないという不満が一部にある。

4. 11 アンケートから見てくるもの

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課題になっている。

さらに、今回初めて実施した審査時、初回及び更新審査時やサーベイランス時において、審査員がどのような文書を確認しているかを聞いた

が、複数の審査機関・審査員が、「適用宣言書」を確認していないとの回答があった。これは、ISMS認証取得事業者において、大規模障害があり、また、巷間、審査が杜撰だとの指摘があったため、新たな質問項目を追加したが、当初の想像以上に審査機関／審査員が確認していないとの回答があった。

もちろん、認証取得側への質問で、審査員が確認しなかった理由等は明確でないが、審査時あるいは、サーベイランス時に重要な文書を確認していない。審査員の力量の不足や、審査機関の教育・訓練の不足の場合は、審査員の再教育や、審査機関の教育・訓練の仕組みの再構築が必要である。また、認定機関は、認定機関が定めたR100やR200に従って、認証機関が教育・訓練の仕組みを運用しているかを確認する必要がある。

- ① 経営者の関心度：経営層のコミットメントやメッセージが、各組織階層の管理職、一般社員の方針の周知徹底や理解を容易にし、ISMSの運用に大きな影響を与える。

経営者の関わりについては、ISMSや情報セキュリティの知識を持って、率先して対応に当たることが必要だと考える人たちがいる一方、ISMSの構築や運用において、経営層自らの参画が重要である。経営者の立てた方針が実現できているかを経営者自らが確認し、経営者が積極的に関与することで、従業員がISMSを積極的に推進でき、継続的に改善が可能となるとの回答もある。

- ② ISMSの課題：ISMSでの有効性評価に苦勞している。ISO/IEC 27004: 2009「情報セキュリティマネジメントー測定」の日本語訳¹¹が出版されているが、有効性評価は、苦勞している事業者が多い。
- ③ ISMSへの誤解：管理策について、全てを適用し、いわばチェックリストのように利用しなければならないと考えている認証、事業者や審査員がいる。ISMSは、組

織全体で取得しなくても良いため、取得範囲によっては、適用除外となる管理策がある、あるいは、追加の管理策を付加して、より高度な管理策を策定することが許されている。ただし、これらについて、どのような管理策の選択を行ったか「適用宣言書」に記述する。毎回の調査報告で、このことを記述しているが、ISMSの管理策が自社のセキュリティレベルに合致しない（レベルが低い）との指摘がある。ISMSの管理策を選択してリスク軽減の効果がなければ、追加の管理策を加えて、適用宣言書に記述すれば良いのだが、一部の事業者や審査員に適用宣言書の理解が不足している。

- ④ コンサルタントや審査員の問題：コンサルタントについて、①ISMSの理解度、②情報セキュリティの理解度、③認証取得事業者業務の理解度、④コミュニケーション能力、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テーション、⑧ISMS認証取得に役立ったの8項目の評価を10段階で行った。以前の調査より、若干高くなっているが、大幅な改善にはなっていない。8点以上の評価を得ている項目が1つもなく、事業者業務の理解度、実効性のある提案、確立したコンサル手法については、6点台の低さになっている。良いコンサルに巡り会わない、コンサル費用が低く、良いコンサルを採用できないのか不明であるが、もう少し高いレベルが望まれる。

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、事業者の業務理解度は、前回6点台だったが、7点台になっている。ただ、自由回答からは、審査員のレベル差があり、指摘事項については、審査機関内でバラバラだと感じると

いった指摘があり、ここに現れない課題もある。

さらに、ISMSの維持費用について56%が高いとしており、審査がマンネリ化しているとの指摘があり、費用に見合うメリットを感じていない。

4. 12 インタビューから見えてくるもの

以前の調査では2、3事業者へのインタビューであったが、今回は6事業者へ訪問し、インタビューを試みた。

全体的な印象は、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ていない。

(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場合、専任のISMS推進者を設けていない。このため、経営層の理解の程度等がISMSの推進に影響している。

また、ISMS推進担当者（含担当責任者）の専門性が高くなるにつれ、人事異動が難しいと考えている。ISMS推進担当者は、内部監査や外部審査に対応し立会いに参加する。実務を兼務しISMSの維持・管理を行っている場合、ISMS推進担当者の後任を探すのが難しい。

(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者が多いが、コンサルタントに問題があったと回答している事業者がいくつかある。

当該事業者の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ケースが多く、コンサルタントしての力量を十分に判断できないために、良い結果をもたらさない場合がある。コンサルタントの可否を判断するための何らかの客観的な情報が必要である。

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指摘もある。

ISMS推進者でなく、現場の責任者が外部審査のインタビューに対応する場合、ISMS審査の指摘が誤っていても、そのまま、指摘事項として認め、最終会議を終了し、審査報告書が指摘ミスのまま作成されたとの回答を事業者から回答を得た。審査員は、仮に指摘ミスがあれば、事業者からの指摘事項の取り下げや、最終会議での発言があると考えている。

また、審査員側に全く問題がないとの回答でも、実際には審査員・審査機関が事業者の業務内容を十分に把握していないために、指摘ミスとなったのではないかと考えた回答もある。

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事業者もあり、価格、審査機関の対応、審査員の力量等を含め、従来の審査機関・審査員で継続するか判断を行っている事業者もある。

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者がある。審査機関が審査員に対し、対象事業者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る。

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認証取得事業者調査を始めたが、今回の調査で、4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、本調査が最も広範囲に行っている。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を考察した。

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る。

- 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ISO 9000 (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⁾。韓国は日本より早く入札要件から外している。これは、QMS認証制度の問題ではなく、運用に問題があるためである。すなわち、入札要件にしたため「QMS認証を金で買う」事業者が出て、QMS認証取得が適切な品質確保には繋がらないことが判明した。

ISMSでも同じような問題がいわれており、今までの調査内容からも、ISMS認証の維持継続が目的化しており、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者が多々ある。

実際、実業務とISMSとの「乖離がない」と回答している事業者は40%以下で、「乖離あり」は約27%、4分の1以上になる。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、形骸化する。実際、「当社のレベルに比べ、あの事業者のISMS認証レベルは余りにも低すぎる」との声もある。

- 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る。ISO/IEC規格

に基づいた制度でも、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とは、「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事業者は、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者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大きな乖離があるとの回答がある。

コンサルタントがどのようなコンサルテーションを行うかについては、規制するものはないが、ISMS 認証制度に標準的なコンサルタント養成のスキームがあれば、コンサルタント自身のISMS 関連知識のレベルが向上し、ISMS 認証取得を計画している事業者にとっても、コンサルタントの選定に役立つと考えられる。

「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の存在が必要である。

5. 3 監査概念について

以前の調査等を含めて、非常に大きな問題として感じたのは、ISMS 認証システムは、「監査」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、取捨選択可能な文書である。

JIS Q 27002: 2006「0.2.5 管理策の選択」は、

(略) リスクを受容可能なレベルまで低減することを確実にするように、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)と規定している。

JIS Q 27001: 2006「4.2.1 ISMS の確立」は、

(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。

と規定している。

管理目的、管理策はチェックリストではなく、リスク低減を目的として、リスク分析の結果、明らかとなった対策を管理策として取捨選択するものである。

このことを、コンサルタント、審査員、ISMS 取得事業者、ISMS 推進者は十分に理解していることが必要である。

たとえば、派遣労働者に対する機密保持契約(NDA)を行うかにおいて、派遣先企業とのNDAは法的な面から締結が必要であるが、ISMS 基準に管理策としての規定がないため、派遣要員とのNDAは不要との指摘が、ISMS の外部審査員により指摘された。しかし、ISMS の基準に管理策の規定がなくても、リスクが大きいと判断すれば、適切な管理策を新たに追加(作成することを含める)することを要求している。おしなべて適用される一律の管理目的、管理策が各事業者適切に適用される限らない。事業者毎だけでなく、同一事業者の事業変化、新規事業等の環境変化を配慮する必要がある。

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回答がある。事業や環境が異なれば、リスクが変化しているが、審査員の力量のバラツキにより指摘に違いを生じる。しかし、指摘にあたっては、指摘ミスや審査員間で意見相違が発生しないように、審査の力量を高め、審査員間のコミュニケーションを図るべきである。

また、指摘にあたっては、事業者には指摘内容について十分な説明を行い、事業者を理解させることが必要である。

本調査は認証取得事業者側の意見を聴収し、審査機関側からの意見を聴収していないため、必ずしも公平な調査とはいえない。しかし、実名の認証機関名（審査員名）を挙げて、厳しい意見を主張する事業者の回答がある。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られる。

また、審査員には退職後の熟年者が多いが、専門家としての能力の維持・向上を目指す必要がある。

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える。

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となる。

しかし、調査から明らかとなる教育や啓発活動のいくつかの課題がある。

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。

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で分らないとしているが、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である。

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がある。

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、企業経営上どのような問題が発生するかを自問・自答する必要がある。経営層のISMS認証制度の必要性の理解を容易にする。

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ISMSの役割と責任を認識し、経営層自らがISMSに参画することが重要である。

② 集合研修での工夫

今回の調査では、e-ラーニングは約30%の事業者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者は集合研修中心である。集合研修では、17%が出欠確認のみで、19%程がアンケート実施である。

出欠確認だけでは、殆ど教育効果がなく、アンケートは従業員等、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の指摘もあり、アンケートを行う場合、その内容の工夫が必要である。

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いわれている。

さらに、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、個人指導的な教育・研修（コン
サルテーション）で適用されている。

ISMSや情報セキュリティ分野で、心理
学的な知見をつかった教育が実験的に行わ
れるようになってきた。

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5 A）＝その成果を収益金額に換算
 - ② 顧客満足度（レベル5 B）＝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・啓発に関しては、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が出現しており、従来の教育・啓発だけでは十分でないことがある。

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3,800のISMS認証取得事業者にアンケートを送付し、453事業者から回答を頂いた。情報セキュリティ関連の調査の回答率では、1桁の回答率といわれているが、毎回、高い回収率で、多くのISMS認証取得事業者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者の方々に厚くお礼を申し上げます。
以 上

【注】

- 1 ISMS認証制度では、適用システムごとにISMS認証を取得でき、事業部門ごとのISMS認証取得が可能である。また、適用システムが同一であれば関係した複数の組織にまたがって、グループ全体を一つの単位として認証取得ができる。したがって、本社、事業部、データセンター等の部門単位の取得やグループとして認証取得が可能であるため、件数を数える場合、取得単位の「事業者」とした。
- 2 2009年における全世界での取得件数は、12、934事業者で、日本は5,508事業者で、全体の約43%を占めている。（ISO（国際標準化機構：the International Organization for Standardization）の調査。なお、国内登録件数と異なるのは、国内の認定機関である一般財団法人 日本情報経済社会推進協会（JIPDEC）に認定されていない認証機関の審査により認証を取得した事業者があるため、JIPDECの認証事業者件数より多くなっている）<http://www.iso.org/iso/survey2009.pdf>（2013. 10. 20確認）
- 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。
- 4 問62では、①集合教育と②E-ラーニング、問64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。
- 5 ①会社名・団体名、②住所、③記入者名、④メールアドレスの4項目は、匿名も認めた。
- 6 前回、2010年は、発送数 2,000事業者、回答数 426事業者、回答率 21.3%、2008年は、発

送数 2,096事業者、回答数 352事業者、回答率 16.8%、2006年は、発送数 1,907事業者、回答数 264事業者、回答率 18.6%であった。

- 7 適用宣言書の定義：その組織のISMSに関連して適用する管理目的及び管理策を記述した文書。

注記 管理目的及び管理策は、組織の情報セキュリティに対する、次のものに基づく。

①リスクアセスメント及びリスク対応のプロセスの結果及び結論 ②法令又は規制の要求事項 ③契約上の義務 ④事業上の要求事項

JIS Q 27001: 2006「情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項」3.16より

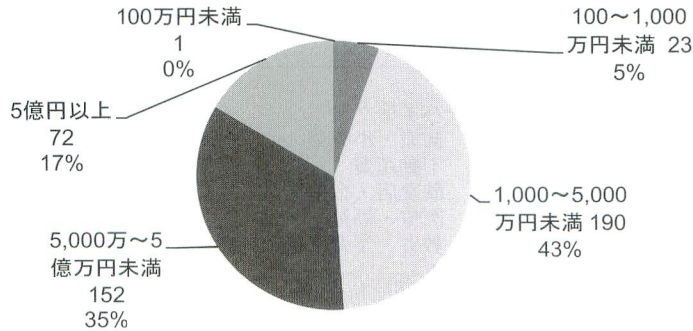
- 8 1981年（昭和56年）7月20日通商産業省告示342号による「情報システム安全対策実施事業者認定制度」が作られた。
- 9 ISMS認証制度では、企業・組織の部門単位での取得が可能で、その後、複数部門／全社に拡大することができる。
- 10 内田勝也、「ネット時評『情報セキュリティ認証制度、実態調査で見えてきた課題』」、日本経済新聞社、2007. 06. 28, http://www.nikkeidigitalcore.jp/archives/2007/06/post_109.html
- 11 ISO/IEC 27001: 2005等は、JIS Q 27001: 2006としてJIS化されているが、これはISO/IECの翻訳である。ただし、JIS化されたものと翻訳は、内容的にはあまり大きな相違はない。
- 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
- 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>

ISMS 認証事業所実態調査 [資料編]

組織／記入者について

1. 資本金 (択一)

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

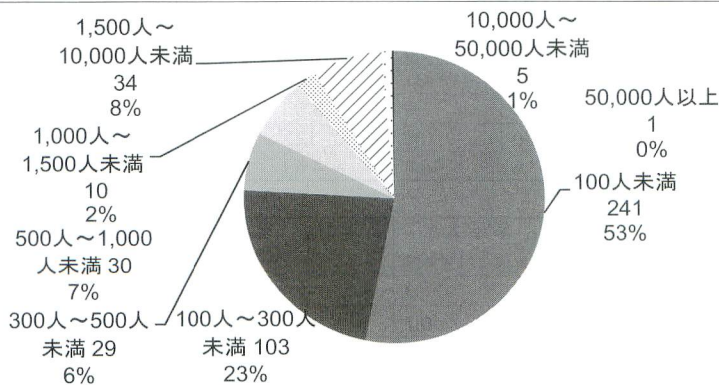


	有効 回答数	100 万円 未満	100～1,000 万円未満	1,000～5,000 万円未満	5,000 万～ 5 億円未満	5 億円以上
今回	438	1	23	190	152	72
2012 年	(%)	0.2	5.3	43.4	34.7	16.4
前回	415	3	7	144	182	79
2010 年	(%)	0.7	1.7	34.7	43.9	19
2008 年	339	1	4	109	149	76
	(%)	0.3	1.2	32.2	44.0	22.4
2006 年	258	2	8	75	115	58
	(%)	0.8	3.1	29.1	44.6	22.5

組織／記入者について

2. 従業員数 (択一)

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



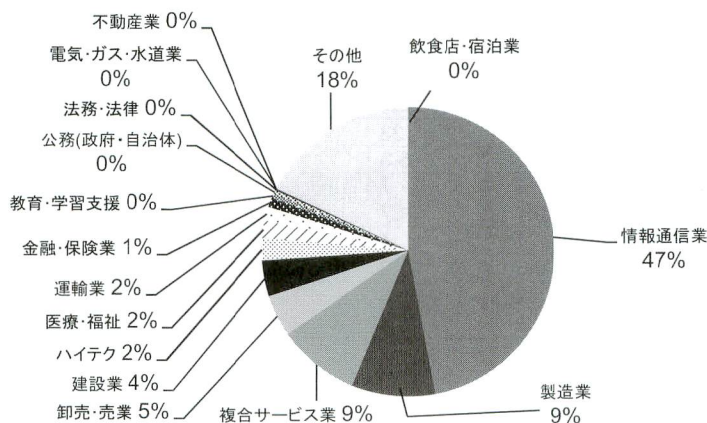
	有効 回答数	100 人 未満	～300 人 未満	～500 人 未満	～1,000 人未満	～1,500 人未満	～1 万人 未満	～5 万人 未満	5 万人 以上
今回	453	241	103	29	30	10	34	5	1
2012 年	(%)	53.2	22.7	6.4	6.6	2.2	7.5	1.1	0.2

前回	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
前々回	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
	263	84	71	28	28	11	32	8	1
2006 年	(%)	31.9	27	10.6	10.6	4.2	12.2	3	0.4

組織／記入者について

3. 組織の業種（択一）

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



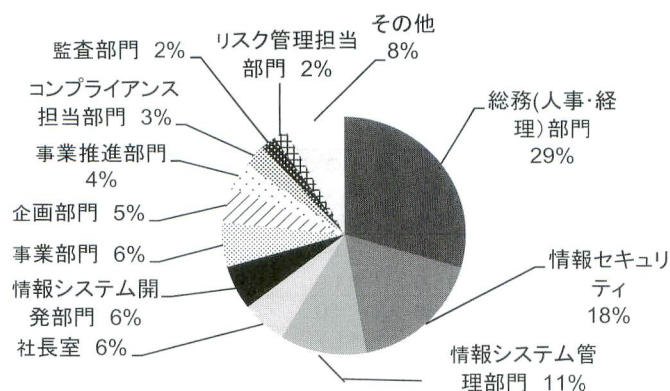
	有効 回答数	6. 情報 通信業	5. 製造業	13. 複合 サービス業	8. 卸売 小売業	1. 建設業	7. ハイテク	3. 運輸業	15. 公務 (自治体)
今回	453	213	42	41	21	18	9	7	7
2012 年	(%)	47.0	9.3	9.1	4.6	4.0	2.0	1.5	1.5
前回	425	172	50	45	27	15	9	7	7
2010 年	(%)	40.5	11.8	10.6	6.4	3.5	2.1	1.6	1.6
前々回	345	149	39	31	19	14	6	2	3
2008 年	(%)	43.2	11.3	9	5.5	4.1	1.7	0.6	0.9
	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

	11. 医療・ 福祉	4. 金融・ 保険業	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	3	4	3	2	1	1	0	79
2012 年	0.7	0.9	0.7	0.4	0.2	0.2	0.0	17.4
前回	3	4	3	2	1	1	0	79
2010 年	0.7	0.9	0.7	0.5	0.2	0.2	0	18.6
前々回	4	9	1	3	1	1	0	63
2008 年	1.2	2.6	0.3	0.9	0.3	0.3	0	18.3
	2	4	1	3	1	1	0	44
2006 年	0.8	0.9	0.4	1.1	0.4	0.4	0	16.7

組織／記入者について

4. 記入者の所属（最も近いものを1つ選択下さい）

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



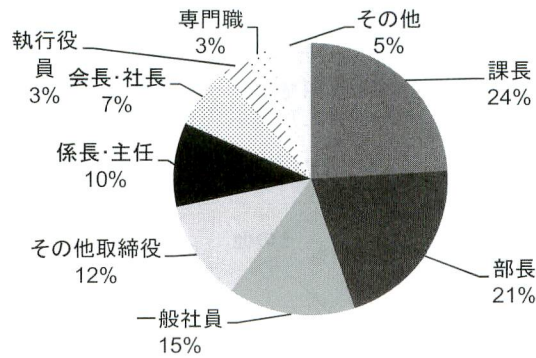
	有効 回答数	1. 総務(人事・経理)部門	6. 情報 セキュリティ	4. 情報 システム管理	2. 社長室	5. 情報 システム開発	7. 事業部門
今回	452	133	80	52	27	27	27
2012 年	(%)	29.4	17.7	11.5	6.0	6.0	6.0
前回	426	103	85	66	20	20	19
2010 年	(%)	24.2	20	15.5	4.7	4.7	4.5
前々回	346	64	93	48	7	19	19
2008 年	(%)	18.5	26.9	13.9	2	5.5	5.5
	263	29	76	38	10	13	22
2006 年	(%)	11	28.9	14.4	3.8	4.9	8.4

		3. 企画部門	8. 事業推進	9. コンプラ	11. 監査部門	10. リスク 管理	12. その他
今回		22	17	14	9	8	36
2012 年		4.9	3.8	3.1	2.0	1.8	8.0
前回		30	18	12	6	8	39
2010 年		7	4.2	2.8	1.4	1.9	9.2
前々回		36	6	5	6	11	32
2008 年		10.4	1.7	1.4	1.7	3.2	9.2
		26	—	8	6	2	33
2006 年		9.9	—	3	2.3	0.8	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 | 4. 部長 | 7. 専門職 |
| 2. その他取締役 | 5. 課長 | 8. 一般社員 |
| 3. 執行役員 | 6. 係長・主任 | 9. その他 |

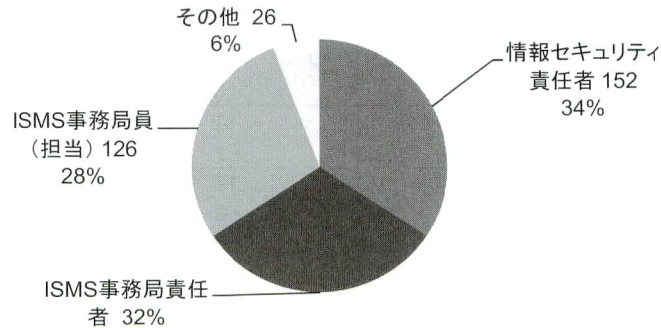


	有効 回答数	5. 課長	4. 部長	8. 一般 社員	2. その他 取締役	6. 係長・ 主任	1. 会長・ 社長	3. 執行 役員	7. 専門職	9. その他
今回	453	109	94	68	54	45	34	14	12	23
2012 年	(%)	24.1	20.8	15.0	11.9	9.9	7.5	3.1	2.6	5.1
前回	426	111	100	60	50	49	17	9	15	9
2010 年	(%)	26.1	23.5	14.1	11.7	11.5	4	2.1	3.5	2.1
前々回	338	79	99	49	28	34	11	12	18	8
2008 年	(%)	23.4	29.3	14.5	8.3	10.1	3.3	3.6	5.3	2.4
2006 年	264	69	66	32	—	27	35	17	12	6
	(%)	26.1	25	12.1	—	10.2	13.3	3	4.5	2.3

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 | 3. ISMS 事務局員 (担当) |
| 2. ISMS 事務局責任者 | 4. その他 |



	有効 回答数	1. 情報セキュリティ 責任者	2. ISMS 事務局 責任者	3. ISMS 事務局員 (担当)	4. その他
今回	444	152	140	126	26
2012 年	(%)	34.2	31.5	28.4	5.9
前回	419	129	159	112	19
2010 年	(%)	30.8	37.9	26.7	4.5
前々回	335	68	136	42	97
2008 年	(%)	34.6	38.2	24.2	3

組織／記入者について

前回	411	1	1	9	25	32	86	96	85	77				
2010 年	(%)	0.2	0.2	2.2	6.1	7.8	20.9	23.4	20.7	18.7				
前々回	345	1	1	6	13	31	67	80	84	63				
2008 年	(%)	0.3	0.3	1.7	3.8	9	19.4	23.2	24.3	18.3				
	264	1	1	11	24	39	79	108	1					
2006 年	(%)	0.4	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

2. 100 人～ 300 人未満

3. 300 人～ 500 人未満

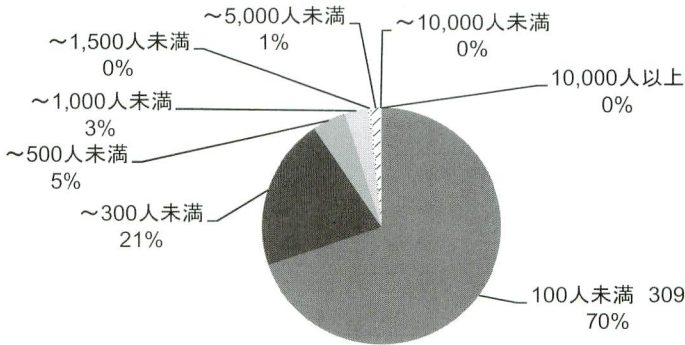
4. 500 人～1,000 人未満

5. 1,000 人～ 1,500 人未満

6. 1,500 人～ 5,000 人未満

7. 5,000 人～10,000 人未満

8. 10,000 人 以上



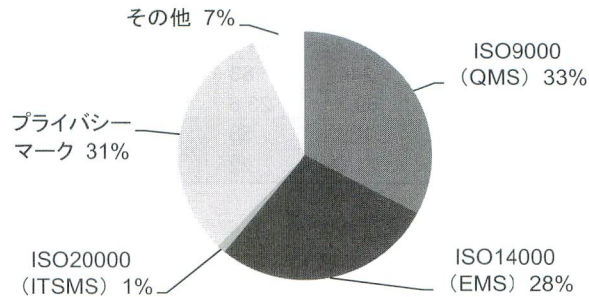
	有効 回答数	1. 100 人 未満	2. ~300 人未満	3. ~500 人未満	4. ~1,000 人未満	5. ~1,500 人未満	6. ~5,000 人未満	7. ~1 万 人未満	8. 1 万 人以上
今回	443	309	92	20	14	2	5	1	0
2012 年	(%)	69.8	20.8	4.5	3.2	0.5	1.1	0.2	0
前回	421	230	126	27	19	11	7	1	0
2010 年	(%)	54.6	29.9	6.4	4.5	2.6	1.7	0.2	0
前々回	345	205	84	19	20	8	5	1	3
2008 年	(%)	59.4	24.3	5.5	5.8	2.3	1.4	0.3	0.9
	261	154	71	16	8	2	5	2	3
2006 年	(%)	59	27.2	6.1	3.1	0.8	1.9	0.8	1.1

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	229	39	10	9	4	14	3	1	309
300 人未満	4	61	7	6	4	9	1	0	92
500 人未満	0	2	12	1	1	4	0	0	20
1,000 人未満	0	0	0	13	0	1	0	0	14
1,500 人未満	0	0	0	0	1	0	1	0	2
5,000 人未満	0	0	0	1	0	4	0	0	5
10,000 人未満	0	0	0	0	0	1	0	0	1
10,000 人以上	0	0	0	0	0	0	0	0	0
Total	233	102	29	30	10	33	5	1	

ISMS 認証取得に関して

10. 他の認証取得状況

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

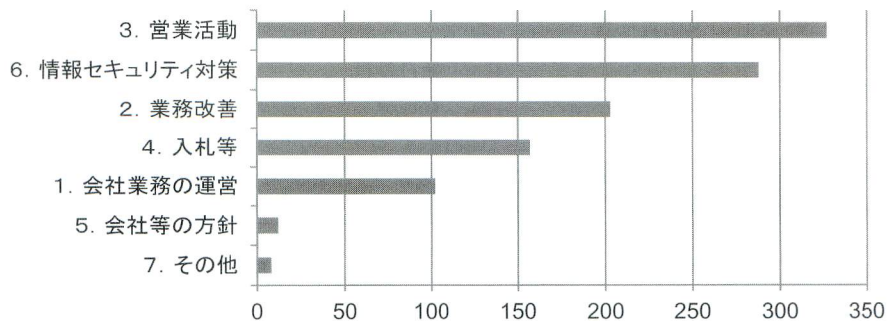


	有効 回答数	1. ISO9000 QMS	2. ISO14000 EMS	3. ISO20000 ITSMS	4. Pマーク	5. その他
今回	453	127	110	4	122	26
2012年	(%)	28.0	24.3	0.9	26.9	5.7
前回	421	163	131	17	118	19
2010年	(%)	36.4	29.2	3.8	26.3	4.2
前々回	352	130	112	16	104	
2008年	(%)	36.9	31.8	4.5	29.5	
2006年	265	110	81	11	68	
	(%)	41.5	30.6	4.2	25.7	

ISMS 認証取得に関して

11. 認証取得の主な目的（複数選択可）

- 会社業務の運営を ISMS 認証に基づいたものにするため
- ISMS の考え方を取入れ、業務の改善を狙ったため
- 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
- 入札等で ISMS 認証取得が条件になっているため
- グループ会社等の方針で決まっているため
- 情報セキュリティ対策の向上のため
- その他

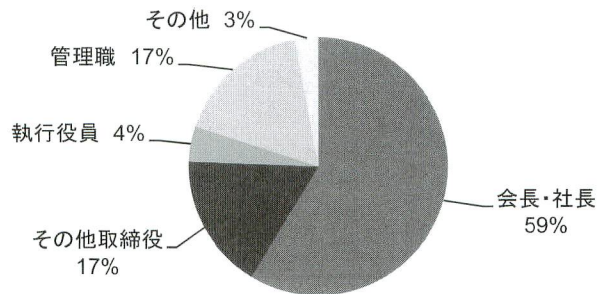


	有効 回答数	3. 営業 活動	6. セキュ リティ対策	2. 業務 改善	4. 入札	1. 業務 運営	5. 方針	7. その他
今回	453	327	288	203	157	102	12	8
2012 年	(%)	72.2	63.6	44.8	34.7	22.5	2.6	1.8
前回	423	318	280	189	159	106	26	10
2010 年	(%)	75.2	66.2	44.7	37.6	25.1	6.1	2.4
前々回	352	267	244	83	94	66	21	4
2008 年	(%)	75.9	69.3	23.6	26.7	18.8	6	1.1
2006 年	264	199	189	58	77	65	15	10
	(%)	75.4	71.6	22	29.2	24.6	5.7	3.8

ISMS 認証取得に関して

1 2. ISMS 認証取得の発案者

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



	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	447	262	76	76	20	13
2012 年	(%)	61.9	18.0	18.0	4.7	3.1
前回	423	220	88	72	19	24
2010 年	(%)	52	20.8	17	4.5	5.7
前々回	347	191	66	54	20	16
2008 年	(%)	55	19	15.6	5.8	4.6

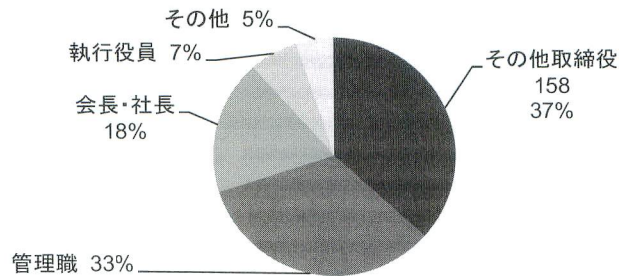
ISMS 認証取得に関して

1 3. ISMS 認証の運用責任者

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

	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	431	158	144	79	28	22
2012 年	(%)	36.7	33.4	18.3	6.5	5.1
前回	391	142	120	79	41	9
2010 年	(%)	36.3	30.7	20.2	10.5	2.3

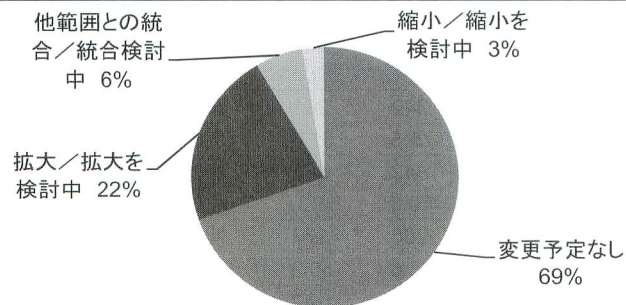
前々回	347	136	97	68	42	5
2008 年	(%)	39.1	27.9	19.5	12.1	1.4



ISMS 認証取得に関して

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

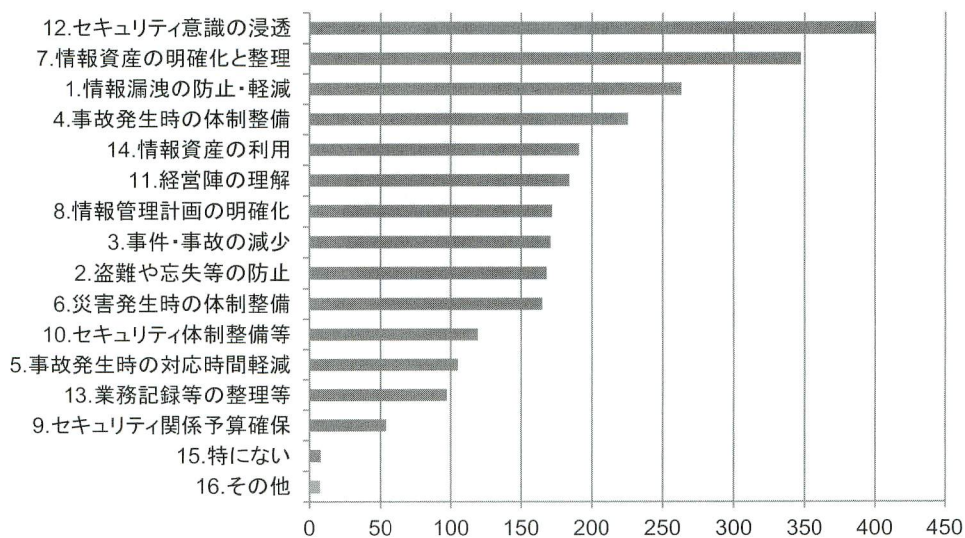


	有効 回答数	1. 縮小・ 縮小検討中	2. 拡大・ 拡大検討中	3. 他範囲と統合 統合検討中	4. 変更予定なし
今回	451	12	99	26	314
2012 年	(%)	2.7	22.0	5.8	69.6
前回	423	20	126	30	247
2010 年	(%)	4.7	29.8	7.1	58.4
前々回	348	13	114	19	202
2008 年	(%)	3.7	32.8	5.5	58

ISMS 認証取得に関して

1 5. 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. 特になし |
| 8. 情報管理計画の明確化と必要な対策の実施 | 16. その他 |



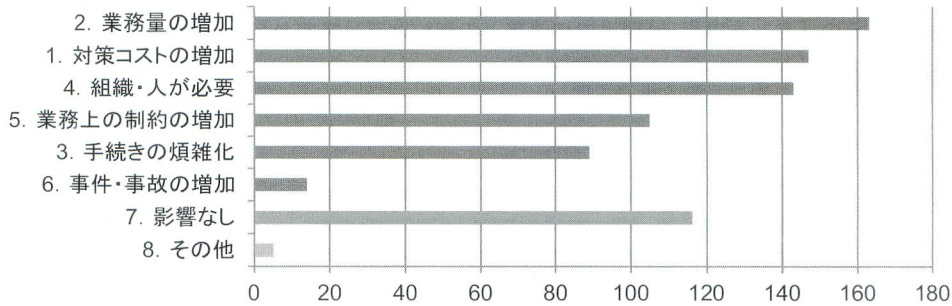
	有効 回答数	12. セキュ 意識	7. 情報 資産	1. 情報 漏えい	4. 事故 発生時	14. 情報 資産利用	11. 経営 理解	8. 情報 管理計画	3. 事件 事故減少
今回	453	371	342	261	262	194	210	179	205
2012 年	(%)	81.9	75.5	57.6	57.8	42.8	46.4	39.5	45.3
前回	426	371	342	261	262	194	210	179	205
2010 年	(%)	87.1	80.3	61.3	61.5	45.5	49.3	42	48.1
前々回	352	307	266	177	188	145	142	128	76
2008 年	(%)	87.2	75.6	50.3	53.4	41.2	40.3	36.4	21.6
2006 年		232	205	146	149	117	114	113	54
		87.9	77.7	55.3	56.4	44.3	43.2	42.8	20.5

	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	13. 業務 記録等	9. セキュ ティ予算	15. 特にな い	16. その他
	177	167	146	124	117	83	5	7
	39.1	36.9	32.2	27.4	25.8	18.3	1.1	1.5
	177	167	146	124	117	83	5	7
	41.5	39.2	34.3	29.1	27.5	19.5	1.2	1.6
	124	114	114	62	108	54	4	5
	35.2	32.4	32.4	17.6	30.7	15.3	1.1	1.4
	106	99	77	57	97	49	3	8
	40.2	37.5	29.2	21.6	36.7	18.6	1.1	3

ISMS 認証取得に関して

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かるコストの増加 | 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 |

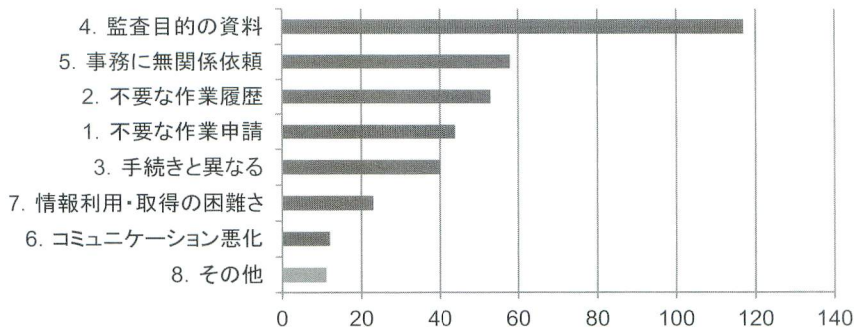


	有効 回答数	2.業務 量増加	1.コスト 増加	4.組織・ 人必要	5.制約 増加	3.手続 煩雑化	6.事件・ 事故増	7.影響 なし	8.その 他
今回	453	163	147	143	105	89	14	116	5
2012 年	(%)	36.0	32.5	31.6	23.2	19.6	3.1	25.6	1.1
前回	426	170	136	120	141	110	19	103	9
2010 年	(%)	39.9	31.9	28.2	33.1	25.8	4.5	24.2	2.1
前々回	352	131	102	110	109	78	7	79	7
2008 年	(%)	37.2	29	31.3	31	22.2	2	22.4	2
2006 年	264	105	91	97	97	61	9	46	6
	(%)	39.8	34.5	36.7	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
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

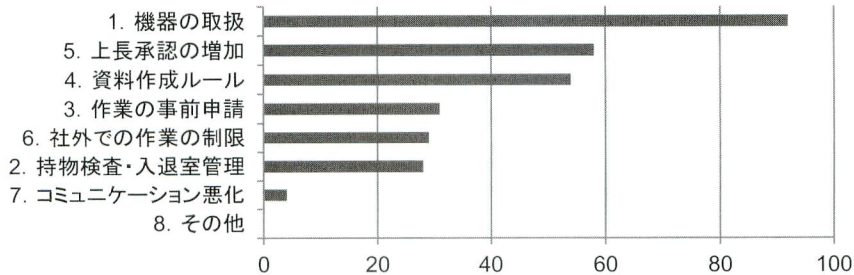


	有効 回答数	4. 監査 目的資料	5. 無関 係資料	2. 不要な 作業履歴	1. 不要な 作業申請	3. 手続 と異なる	7. 情報利 用困難	6. コミュー ニケーション悪化	8. その 他
今回	453	117	58	53	44	40	23	12	11
2012 年	(%)	25.8	12.8	11.7	9.7	8.8	5.1	2.6	2.4
前回	215	126	68	58	58	37	44	13	15
2010 年	(%)	58.6	31.6	24.7	27	17.2	20.5	6	7
前々回	162	87	55	41	35	24	20	6	19
2008 年	(%)	53.7	34	25.3	21.6	14.8	12.3	3.7	11.7
2006 年	264	64	55	31	30	18	20	12	20
	(%)	38.6	33.1	18.7	18.1	10.8	12	7.2	12

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



	有効 回答数	1. 機器 の取扱	5. 承認 増加	4. 資料 ルール	3. 事前 申請	6. 社外 作業限	2. 持物 検査等	7. コミュ ニケーション	8. その他
今回	453	92	58	54	31	29	28	4	0
2012年	(%)	20.3	12.8	11.9	6.8	6.4	6.2	0.9	0.0
前回	141	112	78	78	49	55	55	6	5
2010年	(%)	79.4	55.3	55.3	34.8	39	39	4.3	3.5
前々回	110	68	59	44	19	24	28	0	0
2008年	(%)	61.8	53.6	40	17.3	21.8	25.5	0	0
2006年	(%)	82.5	59.8	51.5	23.7	33	41.2	7.2	2.1

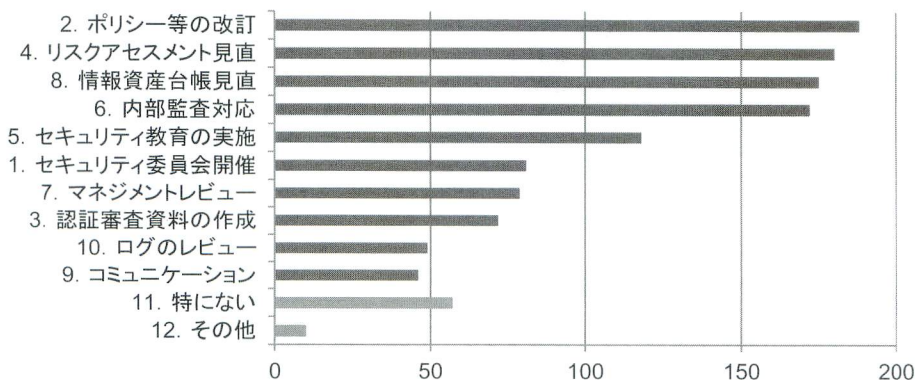
ISMS 認証取得の効果・影響

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 | 7. マネジメントレビューの実施 |
| 2. ポリシー等の改訂や記録などの更新作業 | 8. 情報資産台帳の見直し作業 |
| 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 | 9. 事務局と現場とのコミュニケーション |
| 4. リスクアセスメントの見直し | 10. ログのレビュー |
| 5. セキュリティ教育の実施 | 11. 特にない |

	有効 回答数	2. ポリシー 等の改訂	4. リスク アセスメント	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	453	188	180	175	172	118	81
2012年	(%)	41.5	39.7	38.6	38.0	26.0	17.9
前回	420	188	210	181	157	114	88
2010年	(%)	44.8	50	43.1	37.4	27.1	21
前々回	352	133	178	158	131	95	66
2008年	(%)	37.8	50.6	44.9	37.2	27	18.8
2006年	(%)	52.7	53.8	50	41.3	36	21.2
		7. マネジメ ントレビュー	3. 認証審査 資料の作成	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
		79	72	49	46	57	10
		17.4	15.9	10.8	10.2	12.6	2.2

76	85	45	47	51	12
18.1	20.2	10.7	11.2	12.1	2.9
45	62	43	36	36	9
12.8	17.6	12.2	10.2	10.2	2.6
45	36	45	29	17	6
17	13.6	17	11	6.4	2.3



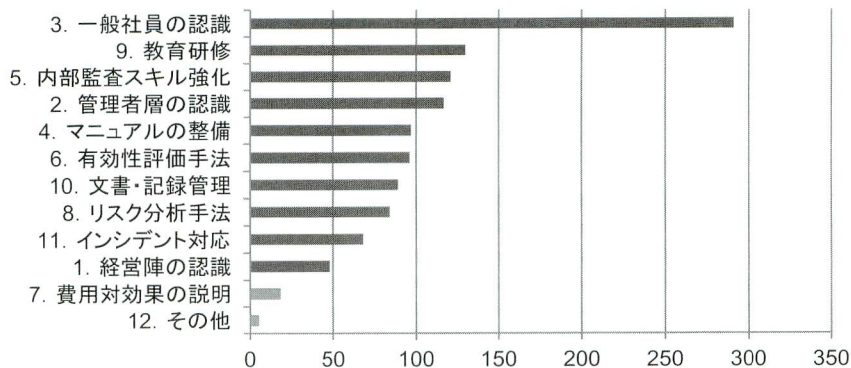
ISMS 認証取得の効果・影響

※はツール導入を含む

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）

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

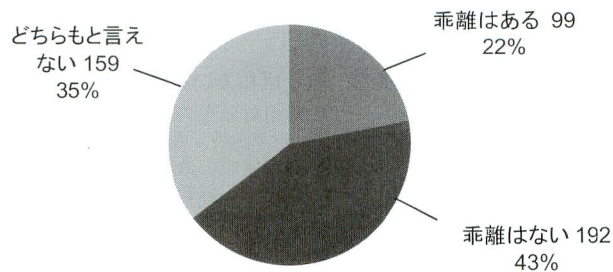
	有効 回答数	3. 一般社員 の認識	9. 教育研修 の改善	5. 内部監査 人スキル強化	2. 管理者 層の認識	4. マニユ アルの整備	6. 有効性 評価手法
今回	438	291	130	121	117	97	96
2012 年	(%)	66.4	29.7	27.6	26.7	22.1	21.9
前回	416	281	127	131	123	103	131
2010 年	(%)	67.5	30.5	31.5	29.6	24.8	31.5
前々回	352	220	102	91	76	79	112
2008 年	(%)	62.5	29	25.9	21.6	22.4	31.8
	264	183	95	61	76	83	108
2006 年	(%)	69.3	36	23.1	28.8	31.4	40.9
		10. 文書・ 記録管理	8. リスク 分析手法	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
		89	84	68	48	18	5
		20.3	19.2	15.5	11.0	4.1	1.1
		94	101	87	65	24	4
		22.6	24.3	20.9	15.6	5.8	1
		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

2 1. 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



	有効 回答数	1. 乖離はある	2. 乖離はない	3. どちらとも言えない
今回	450	99	192	159
2012 年	(%)	22.0	42.7	35.3
前回	422	112	161	149
2010 年	(%)	26.5	38.2	35.3
前々回	347	41	172	134
2008 年	(%)	11.8	49.6	38.6

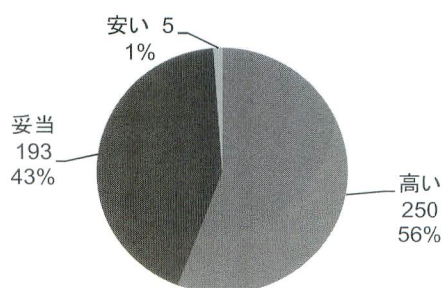
ISMS 認証取得の効果・影響

2 2. 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	448	250	193	5
2012 年	(%)	55.8	43.1	1.1
前回	422	236	185	1
2010 年	(%)	55.9	43.8	0.2

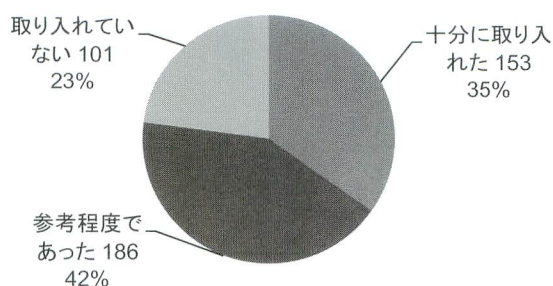
前々回	347	148	191	8
2008 年	(%)	42.7	55	2.3



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



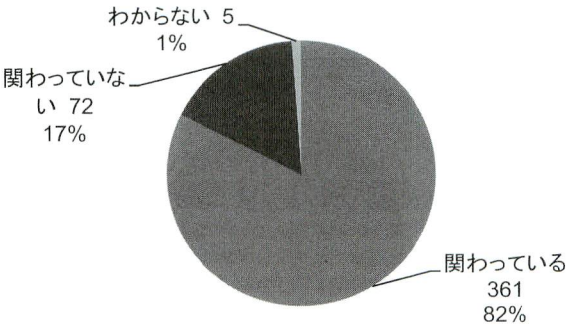
	有効回答数	1. 十分に取り入れた	2. 参考程度であった	3. 取り入れていない
今回	440	153	186	101
2012 年	(%)	34.8	42.3	22.9
前回	422	150	178	94
2010 年	(%)	35.5	42.2	22.3
前々回	348	125	157	66
2008 年	(%)	35.9	45.1	19

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？

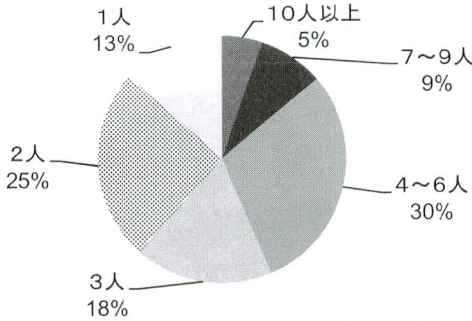
1. 関わっている 2. 関わっていない 3. わからない

	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	438	361	72	5
2012 年	(%)	82.4	16.4	1.2
前回	412	332	72	8
2010 年	(%)	80.6	17.5	1.9
前々回	344	262	77	5
2008 年	(%)	76.2	22.4	1.5
(2006 年)	259	213	41	5
	(%)	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()

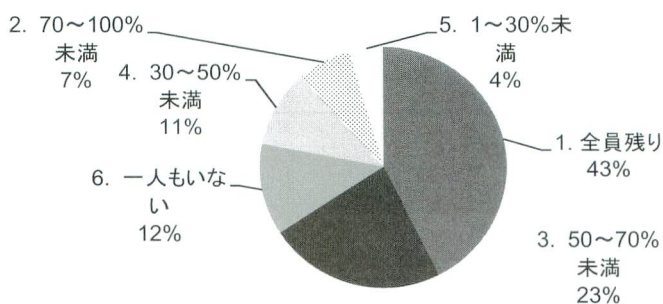


	有効 回答数	4. 4～6人	2. 2人	3. 3人	1. 1人	5. 7～9人	6. 10人以上
今回	448	133	112	81	60	38	24
2012年	(%)	29.7	25.0	18.1	13.4	8.5	5.3
前回	422	111	89	96	57	37	32
2010年	(%)	26.3	21.1	22.7	13.5	8.8	7.6
前々回	347	93	89	64	49	34	18
(2008年)	(%)	26.8	25.6	18.4	14.1	9.8	5.2
		64	67	63	29	28	13
(2006年)	(%)	24.2	25.4	23.9	11	10.6	4.9

	合計	専任	兼務	その他	専任+兼務+その他
一人の場合	60	19	40	1	60
二人の場合	112	25	196	3	224
三人の場合	81	23	214	6	243
4～6人の場合	133	82	547	12	641
7～9人の場合	38	48	232	15	295
10人以上	24	26	254	23	303

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)

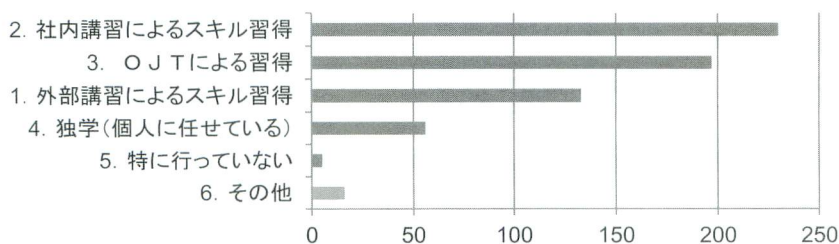


	有効回答数	1. 全員残り	3. 50~70%未満	6. 一人もいない	4. 30~50%未満	2. 70~100%未満	5. 1~30%未満
今回 (2012 年)	383	163	89	47	40	27	17
	(%)	42.6	23.2	12.3	10.4	7.1	4.4
前回 (2010 年)	413	87	87	81	46	53	59
	(%)	21.1	21.1	19.6	11.1	12.8	14.3

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 3. OJTによる習得 5. 特に行っていない
2. 社内講習によるスキル習得 4. 独学(個人に任せている) 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 (2012 年)	435	230	197	133	56	5	16
	(%)	52.9	45.3	30.6	12.9	1.1	3.7
前回 (2010 年)	415	230	220	163	59	27	23
	(%)	55.4	53	39.3	14.2	6.5	5.5
前々回 (2008 年)	352	219	168	113	38	13	8
	(%)	62.2	47.7	32.1	10.8	3.7	2.3
(2006 年)		184	110	85	19	7	12
	(%)	69.7	41.7	32.2	7.2	2.7	4.5

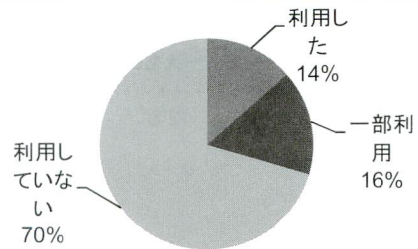
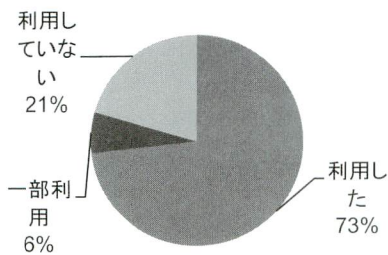
ISMS 認証取得の効果・影響

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

	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 (2012 年)	448	328	28	92
	(%)	73.2	6.3	20.5
前回 (2010 年)	416	296	32	88
	(%)	71.2	7.7	21.2
前々回 (2008 年)	347	253	29	65
	(%)	72.9	8.4	18.7
(2006 年)	263	182	29	52
	(%)	69.2	11	19.8

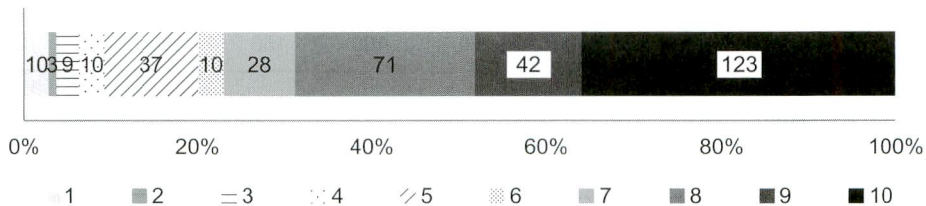
認証取得後

	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	443	60	71	312
	(%)	13.6	16.0	70.4
前回	401	53	71	277
	(%)	13.2	17.7	69.1
前々回	336	59	59	218
	(%)	17.6	17.6	64.9
	255	44	58	153
	(%)	17.3	22.7	60

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



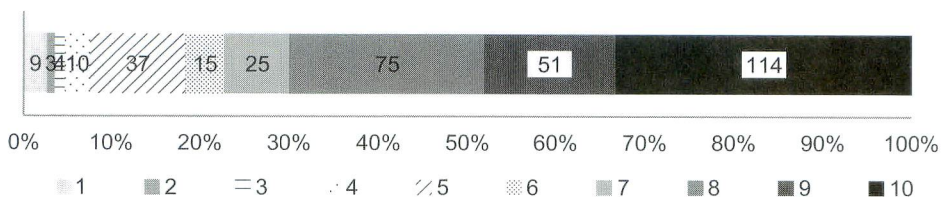
ISMS 理解度: 平均値: 7.87

	有効 回答数	1	2	3	4	5	6	7	8	9	10
今回 (2012 年)	343	10	3	9	10	37	10	28	71	42	123
	(%)	2.9	0.9	2.6	2.9	10.8	2.9	8.2	20.7	12.2	35.9
前回 (2010 年)	316	8	5	9	9	31	11	29	65	33	116
	(%)	2.5	1.6	2.8	2.8	9.8	3.5	9.2	20.6	10.4	36.7
前々回 (2008 年)	273	3	5	2	1	11	10	25	64	41	111
	(%)	1.1	1.8	0.7	0.4	4	3.7	9.2	23.4	15	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



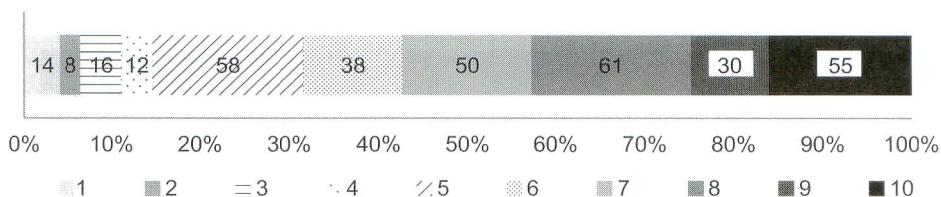
情報セキュリティの理解度: 平均値: 7.92

	有効 回答数	1	2	3	4	5	6	7	8	9	10
今回	343	9	3	4	10	37	15	25	75	51	114
(2012年)	(%)	2.6	0.9	1.1	2.9	10.8	4.4	7.3	21.9	14.9	33.2
前回	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	21.5	9.8	33.5
前々回	274	5	5	2	3	21	22	39	58	39	80
(2008年)	(%)	1.8	1.8	0.7	1.1	7.7	8	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



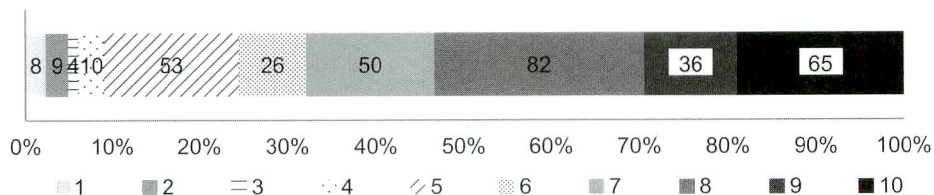
貴組織業務の理解度: 平均値: 6.73

	有効 回答数	1	2	3	4	5	6	7	8	9	10
今回	342	14	8	16	12	58	38	50	61	30	55
(2012年)	(%)	4.1	2.3	4.7	3.5	17.0	11.1	14.6	17.8	8.8	16.1
前回	316	6	9	15	19	43	36	70	68	19	31
(2010年)	(%)	1.9	2.8	4.7	6	13.6	11.4	22.2	21.5	6	9.8
前々回	272	6	9	15	12	37	19	46	59	16	53
(2008年)	(%)	2.2	3.3	5.5	4.4	13.6	7	16.9	21.7	5.9	19.5

コンサルタントについて

3.2. 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



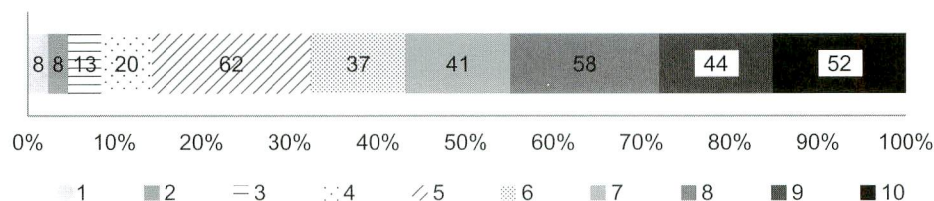
コミュニケーション： 平均値：7.22

	有効 回答数	1	2	3	4	5	6	7	8	9	10
今回	343	8	9	4	10	53	26	50	82	36	65
(2012年)	(%)	2.3	2.6	1.2	2.9	15.5	7.6	14.6	23.9	10.5	18.9
前回	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
前々回	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	26.6	9.9	29.6

コンサルタントについて

3.3. 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



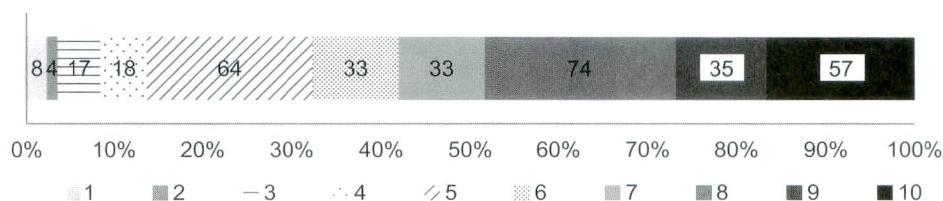
実効性のある提案： 平均値：6.82

	有効 回答数	1	2	3	4	5	6	7	8	9	10
今回	343	8	8	13	20	62	37	41	58	44	52
(2012年)	(%)	2.3	2.3	3.8	5.8	18.1	10.8	12.0	16.9	12.8	15.2
前回	316	6	7	22	28	39	37	51	68	28	30
(2010年)	(%)	1.9	2.2	7	8.9	12.3	11.7	16.1	21.5	8.9	9.5
前々回	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

3 4. 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



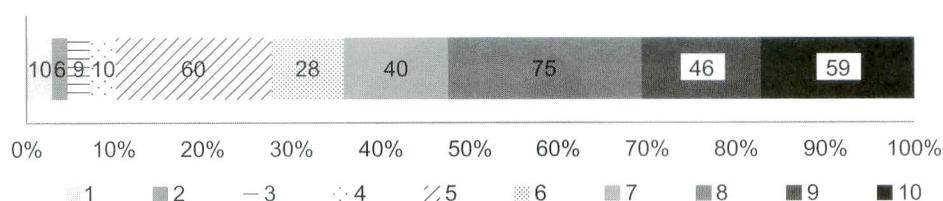
確立したコンサル手法: 平均値: 6.90

	有効 回答数	1	2	3	4	5	6	7	8	9	10
今回	343	8	4	17	18	64	33	33	74	35	57
(2012 年)	(%)	2.3	1.2	5.0	5.2	18.7	9.6	9.6	21.6	10.2	16.6
前回	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
前々回	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

3 5. 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



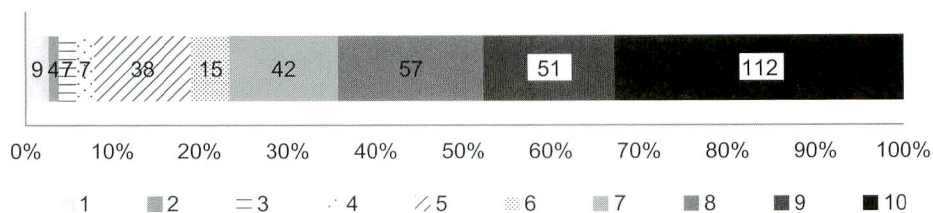
一貫性を持ったコンサルテーション: 平均値: 7.12

	有効 回答数	1	2	3	4	5	6	7	8	9	10
今回	343	10	6	9	10	60	28	40	75	46	59
(2012 年)	(%)	2.9	1.7	2.6	2.9	17.5	8.2	11.7	21.9	13.4	17.2
前回	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	24.2	10.8	13.1
前々回	272	4	6	11	8	21	14	41	65	29	73
(2008 年)	(%)	1.5	2.2	4	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

3 6. 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



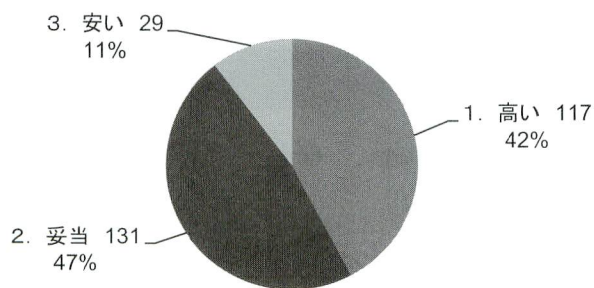
ISMS 認証取得に役立った: 平均値: 7.82

	有効 回答 数	1	2	3	4	5	6	7	8	9	10
今回 (2012 年)	342	9	4	7	7	38	15	42	57	51	112
	(%)	2.7	1.2	2.0	2.0	11.1	4.4	12.3	16.7	14.9	32.7
前回 (2010 年)	315	10	2	11	3	28	23	27	85	34	92
	(%)	3.2	0.6	3.5	1	8.9	7.3	8.6	27	10.8	29.2
前々回 (2008 年)	274	3	3	5	4	10	15	30	55	42	107
	(%)	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

3 7. 費用の妥当性

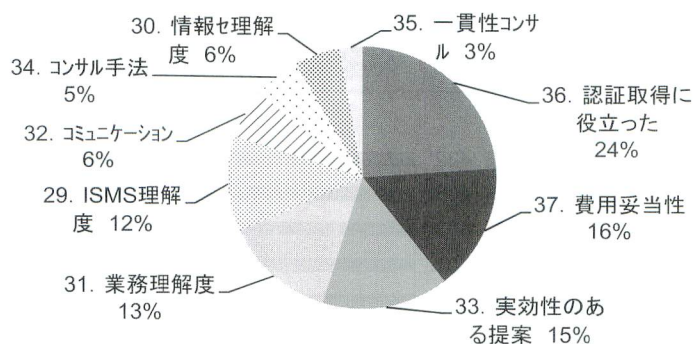
1. 高い 2. 妥当 3. 安い



	有効回答数	1. 高い	2. 妥当	3. 安い
今回 (2012 年)	277	117	131	29
	(%)	42.2	47.3	10.5
前回 (2010 年)	259	118	125	16
	(%)	45.6	48.3	6.2
前々回 (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)

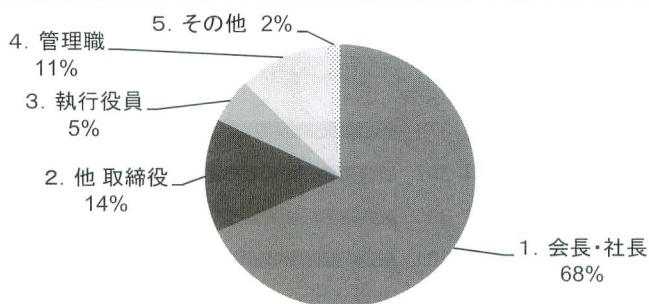


	有効 回答数	36	37	33	31	29	32	34	30	35
今回	327	78	51	50	44	39	20	18	18	9
(2012年)	(%)	23.9	15.6	15.3	13.5	11.9	6.1	5.5	5.5	2.7
前回	300	70	34	56	43	53	16	14	9	5
(2010年)	(%)	23.3	11.3	18.7	14.3	17.7	5.3	4.7	3	1.7

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

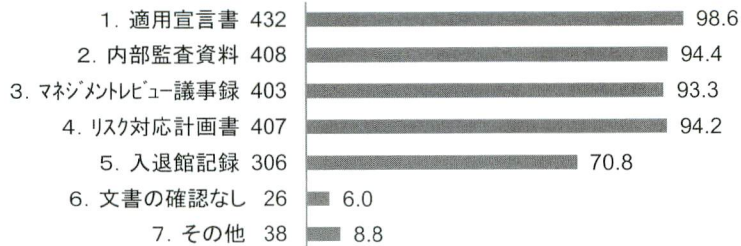


	有効 回答数	1. 会長・社長	2. 他 取締役	3. 執行役員	4. 管理職	5. その他
今回	330	225	46	18	36	5
(2012年)	(%)	68.2	13.9	5.5	10.9	1.5
前回	313	206	56	16	30	5
(2010年)	(%)	65.8	17.9	5.1	9.6	1.6
前々回	337	215	47	15	48	12
(2008年)	(%)	63.8	13.9	4.5	14.2	3.6

ISMS 審査員について

4 0. 審査員が初回審査で確認した文書類は？（複数選択可）

- | | |
|------------------|---------------|
| 1. 適用宣言書 | 5. 入退館記録 |
| 2. 内部監査資料 | 6. 文書の確認なし |
| 3. マネジメントレビュー議事録 | 7. その他（記入欄あり） |
| 4. リスク対応計画書 | |

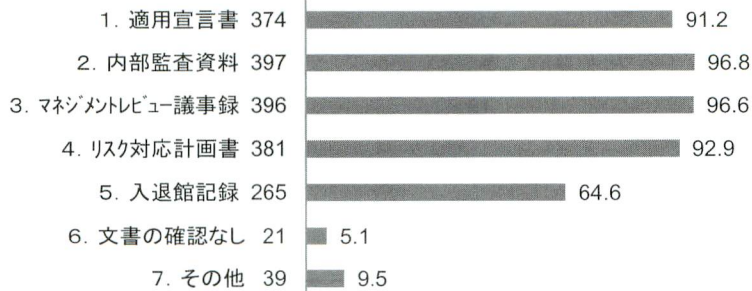


	有効 回答数	1. 適用 宣言書	2. 内部監査 資料	3. マネジメント レビュー議事録	4. リスク対応 計画書	5. 入退館 記録	6. 文書の 確認なし	7. その他
今回 (2012 年)	432	426	408	403	407	306	26	38
	(%)	98.6	94.4	93.3	94.2	70.8	6.0	8.8

ISMS 審査員について

4 1. 審査員が更新審査（サーペランス）で確認した文書類は？（複数選択可）

- | | |
|------------------|---------------|
| 1. 適用宣言書 | 5. 入退館記録 |
| 2. 内部監査資料 | 6. 文書の確認なし |
| 3. マネジメントレビュー議事録 | 7. その他（記入欄あり） |
| 4. リスク対応計画書 | |

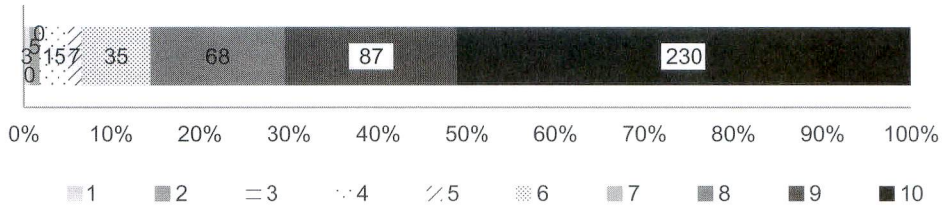


	有効 回答数	1. 適用 宣言書	2. 内部監査 資料	3. マネジメント レビュー議事録	4. リスク対応 計画書	5. 入退館 記録	6. 文書の 確認なし	7. その他
今回 (2012 年)	410	374	397	396	381	265	21	39
	(%)	91.2	96.8	96.6	92.9	64.6	5.1	9.5

ISMS 審査員について

4 2. 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



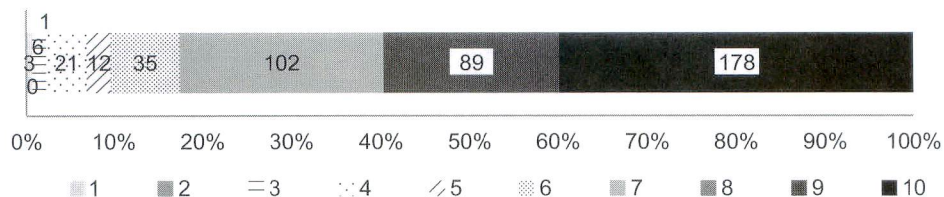
ISMS の理解度: 平均値:8.90

	有効 回答数	1	2	3	4	5	6	7	8	9	10
今回	450	3	0	5	0	15	7	35	68	87	230
(2012 年)	(%)	0.7	0.0	1.1	0.0	3.3	1.6	7.8	15.1	19.3	51.1
前回	417	4	2	3	4	22	7	33	76	79	187
(2010 年)	(%)	1	0.5	0.7	1	5.3	1.7	7.9	18.2	18.9	44.8
前々回	347	1	0	1	0	2	4	17	45	68	209
(2008 年)	(%)	0.3	0	0.3	0	0.6	1.2	4.9	13	19.7	60.6

ISMS 審査員について

4 3. 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



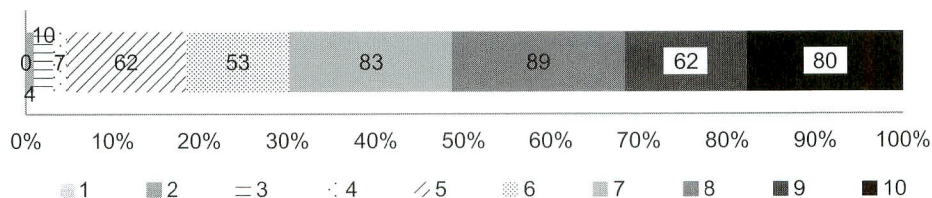
セキュリティ技術の理解度: 平均値:8.60

	有効 回答数	1	2	3	4	5	6	7	8	9	10
今回	447	3	0	6	1	21	12	35	102	89	178
(2012 年)	(%)	0.7	0.0	1.4	0.2	4.7	2.7	7.8	22.8	19.9	39.8
前回	417	2	4	5	5	27	18	42	83	90	141
(2010 年)	(%)	0.5	1	1.2	1.2	6.5	4.3	10.1	19.9	21.6	33.8
前々回	347	0	1	2	2	5	11	34	66	63	163
(2008 年)	(%)	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

4 4. 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



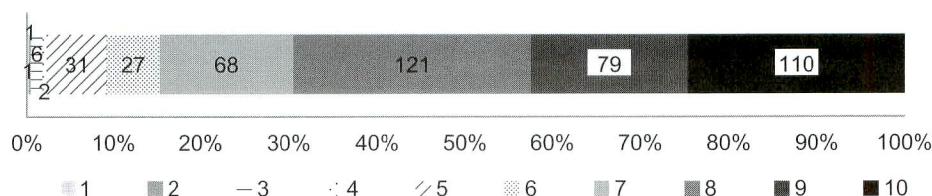
貴組織の業務の理解度： 平均値: 7.43

	有効 回答数	1	2	3	4	5	6	7	8	9	10
今回	450	0	4	10	7	62	53	83	89	62	80
(2012 年)	(%)	0.0	0.9	2.2	1.5	13.8	11.8	18.4	19.8	13.8	17.8
前回	417	4	2	18	15	58	59	69	109	42	41
(2010 年)	(%)	1	0.5	4.3	3.6	13.9	14.1	16.5	26.1	10.1	9.8
前々回	346	0	4	11	4	23	32	63	99	43	67
(2008 年)	(%)	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

4 5. 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



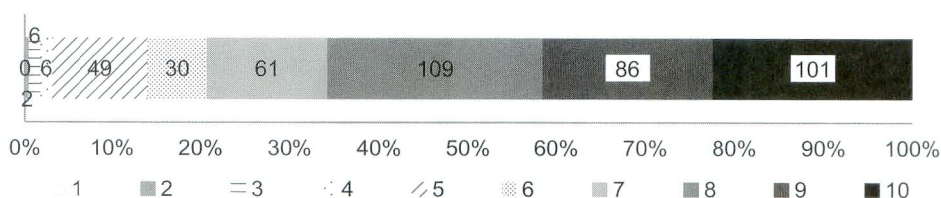
コミュニケーション： 平均値: 8.07

	有効 回答数	1	2	3	4	5	6	7	8	9	10
今回	446	1	1	6	2	31	27	68	121	79	110
(2012 年)	(%)	0.2	0.2	1.3	0.5	7.0	6.1	15.2	27.1	17.7	24.7
前回	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
前々回	347	1	2	3	7	13	21	32	101	62	105
(2008 年)	(%)	0.3	0.6	0.9	2	3.8	6.1	9.3	29.3	18	30.4

ISMS 審査員について

4 6. 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



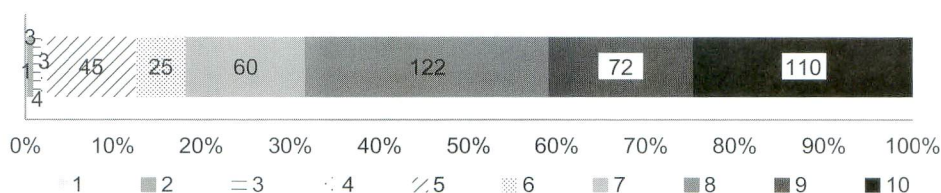
実効性のある指摘: 平均値: 7.89

	有効 回答数	1	2	3	4	5	6	7	8	9	10
今回 (2012 年)	450	0	2	6	6	49	30	61	109	86	101
	(%)	0.0	0.4	1.3	1.3	10.9	6.7	13.6	24.2	19.1	22.5
前回 (2010 年)	417	2	4	9	15	46	43	63	118	58	59
	(%)	0.5	1	2.2	3.6	11	10.3	15.1	28.3	13.9	14.1
前々回 (2008 年)	347	1	2	4	7	16	21	46	92	62	96
	(%)	0.3	0.6	1.2	2	4.6	6.1	13.3	26.7	18	27.8

ISMS 審査員について

4 7. 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

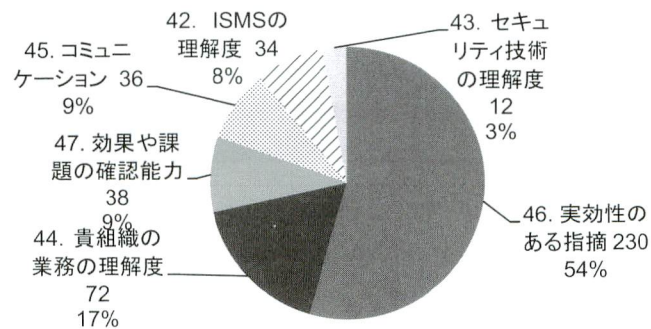


効果や課題を確認する能力: 平均値: 7.98

	有効 回答数	1	2	3	4	5	6	7	8	9	10
今回 (2012 年)	445	1	3	4	3	45	25	60	122	72	110
	(%)	0.2	0.7	0.9	0.7	10.1	5.6	13.5	27.4	16.2	24.7
前回 (2010 年)	417	5	2	6	11	39	38	61	120	69	66
	(%)	1.2	0.5	1.4	2.6	9.4	9.1	14.6	28.8	16.5	15.8
前々回 (2008 年)	346	1	1	3	3	19	14	37	92	59	117
	(%)	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

48. 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？

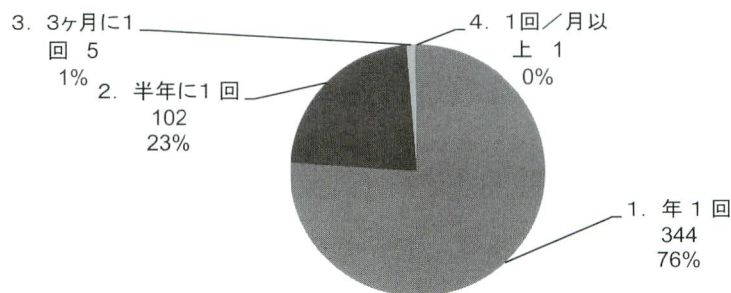


	有効 回答数	46	44	47	42	45	43
今回 (2012 年)	422	230	72	38	34	36	12
	(%)	54.5	17.1	9.0	8.1	8.5	2.8
前回 (2010 年)	396	202	66	49	42	30	7
	(%)	51	16.7	12.4	10.6	7.6	1.8

内部監査について

49. 内部監査の実施頻度（除 自己点検）

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

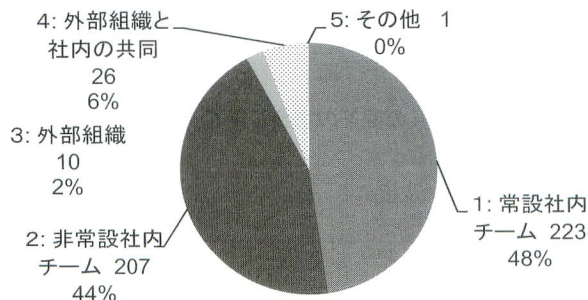


	有効 回答数	1. 1 年 に 1 回	2. 半年に 1 回	3. 3 ヶ月に 1 回	4. 毎月 1 回以上
今回 (2012 年)	452	344	102	5	1
	(%)	76.1	22.6	1.1	0.2
前回 (2010 年)	423	326	86	7	4
	(%)	77.1	20.3	1.7	0.9
前々回 (2008 年)	348	252	92	3	1
	(%)	72.4	26.4	0.9	0.3
(2006 年)	264	171	88	2	3
	(%)	64.8	33.3	0.8	1.1

内部監査について

50. 内部監査体制について

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

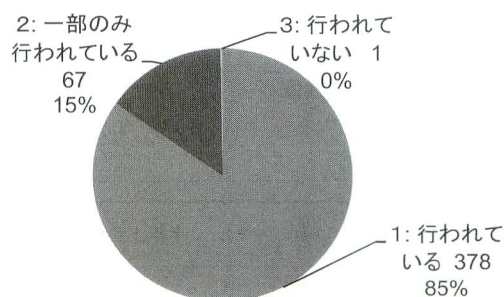


	有効 回答数	1. 常設 社内チーム	2. 非常設 社内チーム	3. 外部組織	4. 外部と 社内の共同	5. その他
今回	467	223	207	10	26	1
(2012 年)	(%)	47.8	44.3	2.1	5.6	0.2
前回	445	218	189	11	19	8
(2010 年)	(%)	49.0	42.5	2.5	4.3	1.8
前々回	359	156	175	11	15	2
(2008 年)	(%)	44.3	49.7	3.1	4.3	0.6
	275	101	151	7	14	2
(2006 年)	(%)	36.7	54.9	2.5	5.1	0.7

内部監査について

51. 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



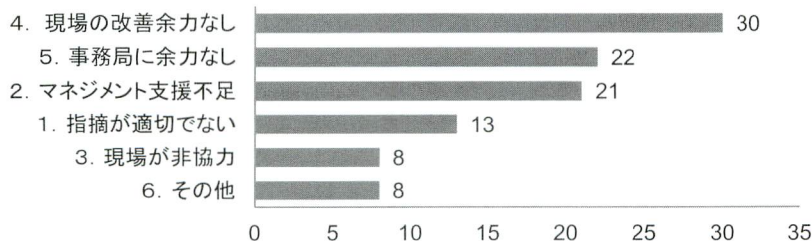
	有効回答数	1. 行われている	2. 一部のみ	3. 行われていない
今回	446	378	67	1
(2012 年)	(%)	84.8	15.0	0.2
前回	420	358	61	1
(2010 年)	(%)	85.2	14.5	0.2

前々回	345	305	40	0
(2008 年)	(%)	88.4	11.6	0
	264	239	25	0
(2006 年)	(%)	90.5	9.5	0

内部監査について

5 2. 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 |



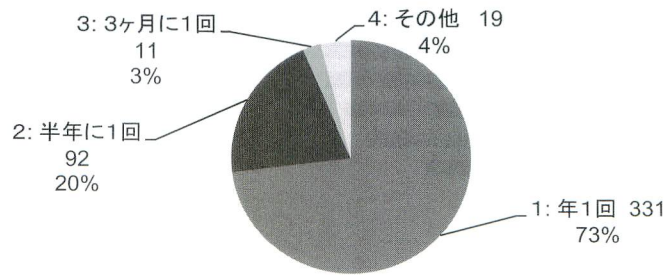
	有効 回答数	4. 現場の 改善余力なし	5. 事務局に 余力なし	2. マネジメン ト支援不足	1. 指摘が 適切でない	3. 現場が 非協力	6. その他
今回	73	30	22	21	13	8	8
(2012 年)	(%)	41.1	30.1	28.8	17.8	11.0	11.0
前回	85	27	15	14	16	11	23
(2010 年)	(%)	31.8	17.6	16.5	18.8	12.9	27.1
前々回	40	25	14	9	9	9	3
(2008 年)	(%)	62.5	35	22.5	22.5	22.5	7.5
	25	13	13	7	5	3	3
(2006 年)	(%)	52	52	28	20	12	12

マネジメントレビューについて

5 3. マネジメントレビューの実施頻度

- | | |
|------------|--------------|
| 1. 年 1 回 | 3. 3 ヶ月に 1 回 |
| 2. 半年に 1 回 | 4. その他 |

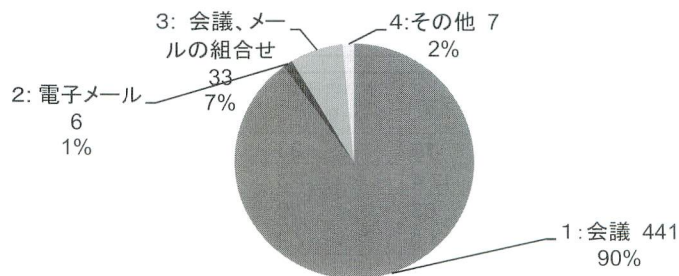
	有効 回答数	1. 年 1 回	2. 半年 1 回	3. 3 ヶ月 1 回	4. その他
今回	453	331	92	11	19
(2012 年)	(%)	73.1	20.3	2.4	4.2
前回	423	299	86	15	23
(2010 年)	(%)	70.7	20.3	3.5	5.4
前々回	346	239	78	9	20
(2008 年)	(%)	69.1	22.5	2.6	5.8
	264	163	77	8	16
(2006 年)	(%)	61.7	29.2	3	6.1



マネジメントレビューについて

5 4. 実施形態

- | | |
|----------|---------------|
| 1. 会議 | 3. 会議、メールの組合せ |
| 2. 電子メール | 4. その他 |

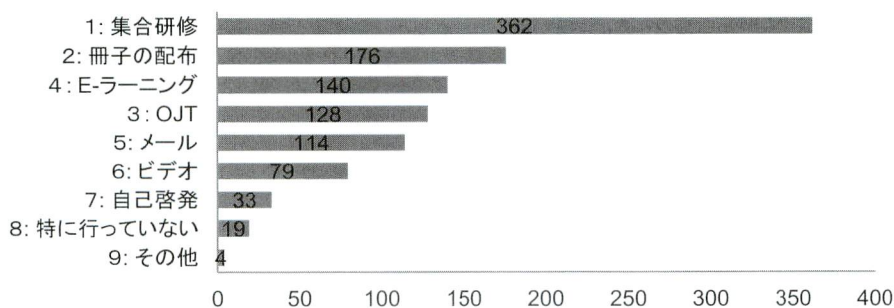


	有効 回答数	1. 会議	2. 電子メール	3. 会議、 メールの組合せ	4. その他
今回 (2012 年)	453 (%)	411 90.7	6 1.3	33 7.3	7 1.5
前回 (2010 年)	432 (%)	392 90.7	5 1.2	28 6.5	7 1.6
前々回 (2008 年)	347 (%)	321 92.5	3 0.9	17 4.9	6 1.7
(2006 年)	264 (%)	255 96.6	0	7 2.7	2 0.8

教育について

5 5. 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. O J T | 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: O J T	4: E ラー ニング	5: メール
今回	453	362	176	128	140	114
(2012 年)	(%)	79.9	38.9	28.3	30.9	25.2
前回	423	347	180	140	128	107
(2010 年)	(%)	82	42.6	33.1	30.3	25.3
前々回	295	146	118	110	75	
(2008 年)	(%)	84.8	42	33.9	31.6	21.6
	264	243	124	80	64	61
(2006 年)	(%)	92	47	30	24.2	23.2

6: ビデオ	7: 自己啓 発	9: その他	8: 行って いない
79	33	19	4
17.4	7.3	4.2	0.9
63	30	24	3
14.9	7.1	5.7	0.7
50	36	21	0
14.4	10.3	6	0
33	20	21	1
12.5	7.6	8	0.4

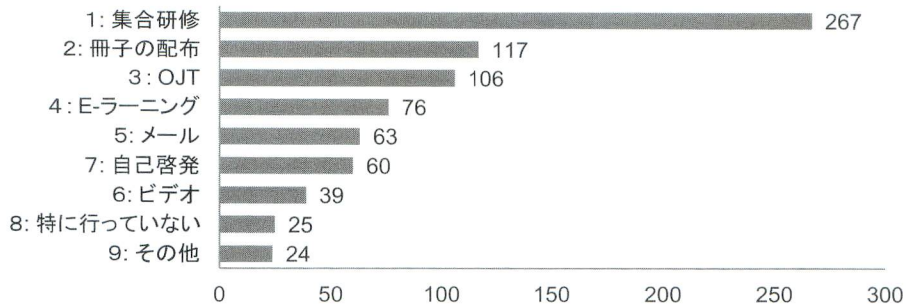
教育について

56. 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 | 4. E-ラーニング | 7. 自己啓発 |
| 2. 冊子の配布 | 5. メール | 8. 特に行っていない |
| 3. O J T | 6. ビデオ | 9. その他 |

	有効 回答数	1. 集合研 修	2. 冊子の配 布	3. O J T	4. E ラーニ ング	5. メール
今回	439	267	117	106	76	63
(2012 年)	(%)	60.8	26.7	24.1	17.3	14.4
前回	420	252	129	136	73	53
(2010 年)	(%)	60	30.7	32.4	17.4	12.6
前々回	231	91	115	63	39	
(2008 年)	(%)	67.2	26.5	33.4	18.3	11.3
	264	197	98	60	41	44
(2006 年)	(%)	74.6	37.1	22.7	15.5	16.7

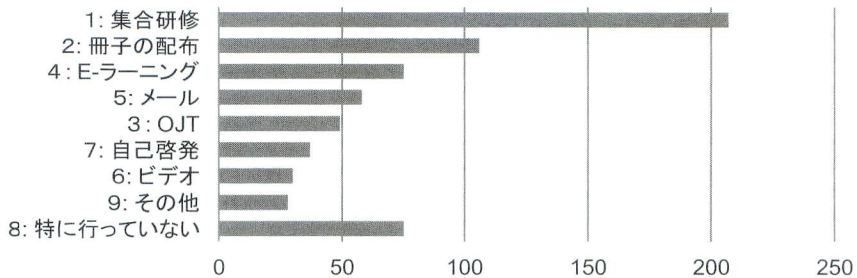
		7. 自己啓発	6. ビデオ	8. 行っていない	9. その他
今回		60	39	25	24
(2012 年)		13.7	8.9	5.7	5.5
前回		100	35	34	28
(2010 年)		23.8	8.3	8.1	6.7
前々回		92	22	15	24
(2008 年)		26.7	6.4	4.4	7
		33	18	16	25
(2006 年)		12.5	6.8	6.1	8.4



教育について

5 7. 経営層への教育方法は？ (複数選択可)

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



	有効 回答数	1: 集合 研修	2: 冊子 の配布	4: Eラー ニング	5: メール	3: OJ T
今回	439	207	106	75	58	49
(2012 年)	(%)	47.2	24.1	17.1	13.2	11.2
前回	415	160	120	75	45	55
(2010 年)	(%)	38.6	28.9	18.1	10.8	13.3
前々回		175	95	54	39	46
(2008 年)	(%)	51	27.7	15.7	11.4	13.4
	264	141	92	35	38	34
(2006 年)	(%)	53.4	34.8	13.3	14.4	12.9

		7: 自己 啓発	6: ビデ オ	9: その 他	8: 行っ ていない
今回		37	30	28	75
(2012 年)		8.4	6.8	6.4	17.1
前回		45	24	16	99
(2010 年)		10.8	5.8	3.9	23.9
前々回		62	22	14	57
(2008 年)		18.1	6.4	4.1	16.6
		20	14	22	46
(2006 年)		7.6	5.3	8.4	17.4

教育について

58. 社員への ISMS の教育頻度は？

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

	有効 回答数	6. 年 1回	5. 半年 1回	4. 3ヶ 月1回	3. 月 1～2回	1. 毎日	2. 週 1～2回	8. その 他	7. 未実 施
今回	450	186	118	68	51	10	6	25	4
(2012 年)	(%)	41.3	26.2	15.1	11.3	2.2	1.3	5.6	0.9
前回	420	16	2	181	109	46	61	3	2
(2010 年)	(%)	3.8	0.5	43.1	26	11	14.5	0.7	0.5
前々回	336	127	82	64	43	6	3	17	1
(2008 年)	(%)	37	23.9	18.7	12.5	1.7	0.9	5	0.3
		72	59	41	37	4	8	39	4
(2006 年)	(%)	27.3	22.3	15.5	14	1.4	3	14.8	1.5

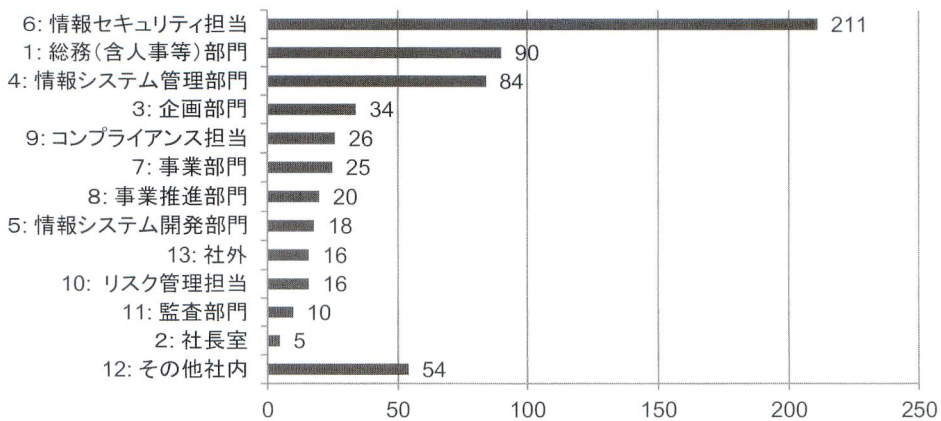
教育について

59. 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	7. 事業部 門	5. 情報シ ステム開発	3. 企画	9. コンプライ アンス
今回	449	225	118	74	28	27	26	20
(2012 年)	(%)	50.1	26.3	16.5	6.2	6.0	5.8	4.5
前回	420	211	90	84	25	18	34	26
(2010 年)	(%)	50.2	21.4	20	6	4.3	8.1	6.2
前々回	349	146	78	53	24	19	29	14
(2008 年)	(%)	41.8	22.3	15.2	6.9	5.4	8.3	4
		134	55	39	24	10	22	12
(2006 年)	(%)	50.8	20.8	14.8	9.1	3.8	8.3	4.5

		2. 社長室	8. 事業推進	10. リスク管理	11. 監査	13. 社外	12. その他社内
今回		19	16	12	11	9	38
(2012年)		4.2	3.6	2.7	2.4	2.0	8.5
前回		0.9	0.8	0.6	0.5	0.4	1.9
(2010年)		1.2	4.8	3.8	2.4	3.8	12.9
前々回		7	8	16	11	17	77
(2008年)		2	2.3	4.6	3.2	4.9	22.1
		6	—	4	9	40	40
(2006年)		2.3	—	1.5	3.4	15.2	15.2



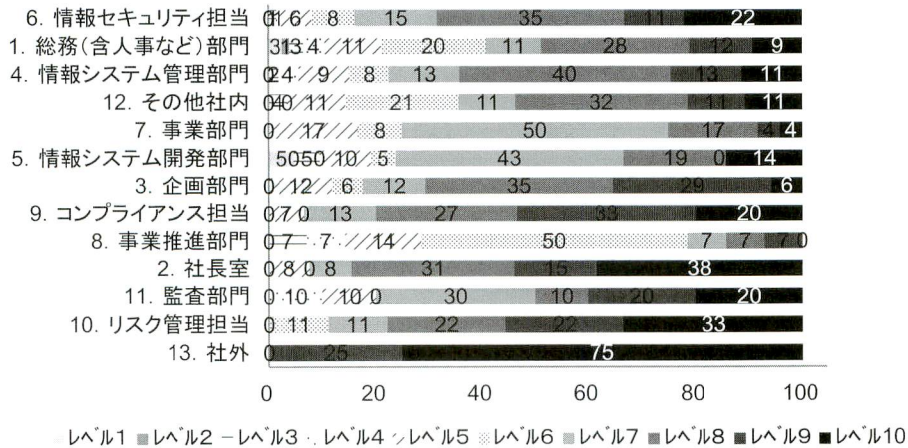
教育について

60. 問59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 | 6. 情報セキュリティ担当 | 11. 監査部門 |
| 2. 社長室 | 7. 事業部門 | 12. その他社内 |
| 3. 企画部門 | 8. 事業推進部門 | 13. 社外 |
| 4. 情報システム管理部門 | 9. コンプライアンス担当 | |
| 5. 情報システム開発部門 | 10. リスク管理担当 | |

	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	7. 事業部門	5. 情報システム開発	3. 企画	9. コンプライアンス
今回	回答数	136	76	53	24	21	17	15
(2012年)	平均値	8.0	6.9	7.5	7.0	6.9	7.8	8.4
前回	回答数	112	43	44	15	9	22	14
(2010年)	平均値	8	7	8	6.7	8	7.3	8.2
前々回	回答数	136	75	51	22	20	27	12
(2008年)	平均値	7.6	6.3	7.5	6.9	7.2	7.1	7.3
		8. 事業推進	2. 社長室	11. 監査	10. リスク管理	13. 社外	12. その他社内	
今回	回答数	14	13	10	9	4	28	
(2012年)	平均値	5.9	8.6	7.6	8.6	9.8	7.3	
前回	回答数	11	2	4	8	6	22	
(2010年)	平均値	7.4	10	7.5	7.6	9.3	7.2	

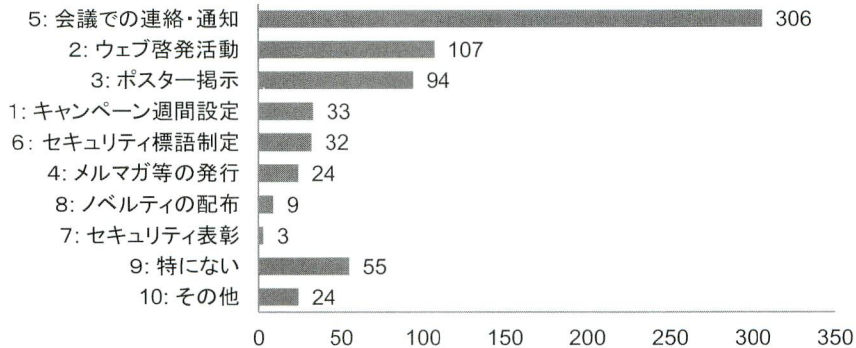
前々回 (2008 年)	回答数	8	7	10	15	15	70
	平均値	6.8	7.9	8	8.2	8.9	6.9



教育について

6 1. 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 |



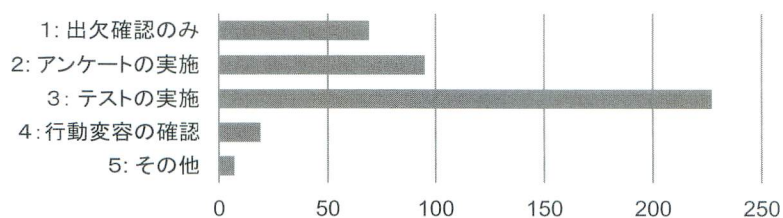
	有効 回答数	5: 会議での 連絡・通知	2: ウェブでの 啓発活動	3: ポスター掲 示	1: キャンペー ン週間の設定	6: セキュリテ ィ標語の制定
今回	452	306	107	94	33	32
(2012 年)	(%)	67.7	23.7	20.8	7.3	7.1
前回	420	290	100	300	44	44
(2010 年)	(%)	69	23.8	71.4	10.5	10.5
前々回		194	102	105	45	42
(2008 年)	(%)	56.6	29.7	30.6	13.1	12.2
				86	17	29
(2006 年)	(%)			32.6	6.4	11

		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
今回	452	24	9	3	55	24
(2012年)	(%)	5.3	2.0	0.7	12.2	5.3
前回	420	35	16	14	50	21
(2010年)	(%)	8.3	3.8	3.3	11.9	5
前々回		43	28	13	63	25
(2008年)	(%)	12.5	8.2	3.8	18.4	7.3
		38	15	5	93	47
(2006年)	(%)	14.4	5.7	1.9	35.2	17.8

教育について

62-①. 問55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 3. テスト／レポート提出 5. その他
2. アンケートの実施 4. インタビュー等による行動変容の確認



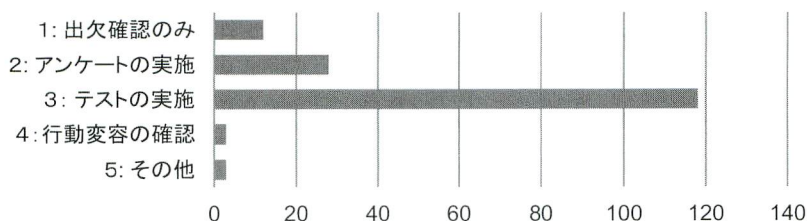
	有効回答数	1. 出欠確認	2. アンケート	3: テスト	4. 行動変容	5. その他
今回	375	69	95	227	19	7
(2012年)	(%)	18.4	25.3	60.5	5.1	1.9
前回	365	62	69	209	22	3
(2010年)	(%)	17	18.9	57.3	6	0.8

教育について

62-②. 問55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 4. インタビュー等による行動変容の確認
2. アンケートの実施 5. その他
3. テスト／レポート提出

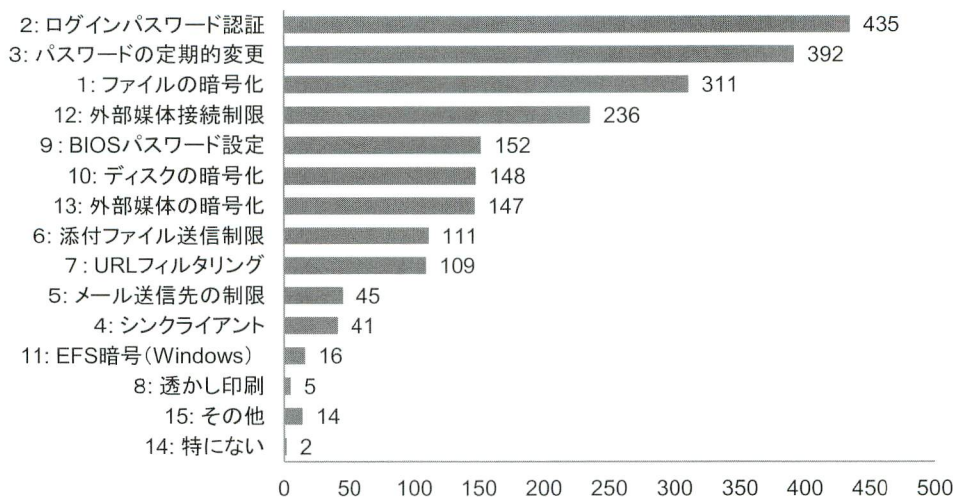
	有効回答数	1. 出欠確認	2. アンケート	3: テスト	4. 行動変容	5. その他
今回	150	12	28	118	3	3
(2012年)	(%)	8.0	18.7	78.7	2.0	2.0
前回	133	4	14	110	3	2
(2010年)	(%)	3	10.5	82.7	2.3	1.5



教育について

6 3. 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 | |



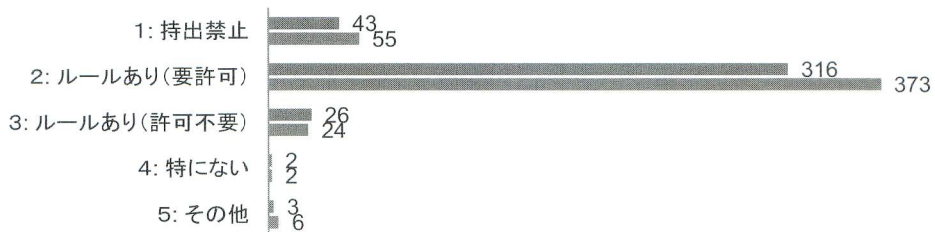
	有効 回答数	2. パスワ ード認証	3. パスワ ード変更	1. ファイル の暗号化	12. 外部媒 体接続制 限	9. BIOS パスワード	10. ディス クの暗号化	13. 外部媒 体の暗号 化
今回	452	435	392	311	236	152	148	147
(2012 年)	(%)	96.2	86.7	68.8	52.2	33.6	32.7	32.5
前回	422	402	368	283	239	138	148	163
(2010 年)	(%)	95.3	87.2	67.1	56.6	32.7	35.1	38.6
前々回	352	333	286	130	57	108	115	178
(2008 年)	(%)	94.6	81.3	36.9	16.2	30.7	32.7	50.6

	6. 添付ファイル制限	7. URL フィルタリング	5. メール送信先制限	4. シンククライアント	11. EFS 暗号	8. 透かし印刷	15. その他	14. ない
今回	111	109	45	41	16	5	14	2
(2012 年)	24.6	24.1	10.0	9.1	3.5	1.1	3.1	0.4
前回	117	139	55	58	17	5	20	1
(2010 年)	27.7	32.9	13	13.7	4	1.2	4.7	0.2
前々回	96	94	34	26	9	1	10	1
(2008 年)	27.3	26.7	9.7	7.4	2.6	0.3	2.8	0.3

社内ルールなど

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

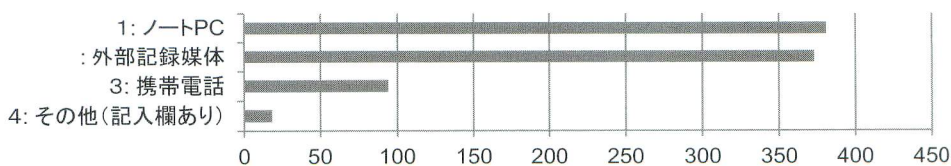


PC 持出	有効 回答数	1. 持出禁 止	2. ルールあり (要許可)	3. ルールあり (許可不要)	4. 特にな い	5. その他
今回	452	55	373	24	2	6
(2012 年)	(%)	12.2	82.5	5.3	0.4	1.3
前回	420	53	345	16	5	1
(2010 年)	(%)	12.6	82.1	3.8	1.2	0.2
前々回	343	25	300	15	0	3
(2008 年)	(%)	7.3	87.5	4.4	0	0.9
媒体持出	有効 回答数	1. 持出禁 止	2. ルールあり (要許可)	3. ルールあり (許可不要)	4. 特にな い	5. その他
今回	385	43	316	26	2	3
(2012 年)	(%)	11.2	82.1	6.8	0.5	0.8
前回	362	34	305	14	8	1
(2010 年)	(%)	9.4	84.3	3.9	2.2	0.3
前々回	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

65. 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P C	2. 外部記憶 媒体	3. 携帯電話	4. その他
今回	430	381	373	94	18
(2012 年)	(%)	88.6	86.7	21.9	4.2
前回	398	356	341	86	25
(2010 年)	(%)	89.4	85.7	21.6	6.3
前々回	352	274	274	57	9
(2008 年)	(%)	77.8	77.8	16.2	2.6

社内ルールなど

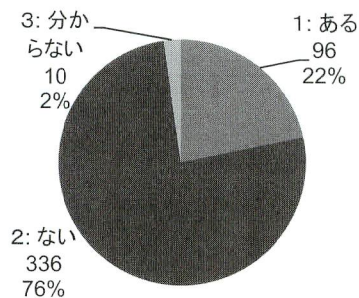
66／67. コンピュータウイルス感染の有無／感染原因は？

66. ウイルスの感染の有無

1. ある
2. ない
3. 分からない

67. 問 66 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



ウイルス感 染	有効回答 数	1. ある	2. ない	3. 分から ない
今回	442	96	336	10
(2012 年)	(%)	21.7	76.0	2.3
前回	422	137	280	5
(2010 年)	(%)	32.5	66.4	1.2

ウイルス感 染	有効 回答数	5. ウェブ 閲 覧	4. ゼ・ロ・デ・イ ウイルス	3. パ・タ・ン 更新漏	1. ワ・ク・チ ン未導入	2. ワ・ク・チ ン期限切	6. 不明
今回	96	40	23	16	12	3	1
(2012 年)	(%)	41.7	24.0	16.7	12.5	3.1	1.0
前回	137	71	21	27	15	1	29
(2010 年)	(%)	51.8	15.3	19.7	10.9	0.7	21.2