ISMS 適合性評価制度に関する

アンケート調査報告書

2009 年 3 月

財団法人 日本情報処理開発協会
情報マネジメント推進センター

目　　次

はじめに 1

調査の概要 2

基本情報について 3

ISMS 認証の運用実績等について 9

審査員の力量及び審査の質について 13

制度全般に対するご意見等 27

おわりに 34

付録　ISMS 適合性評価制度に関するアンケート調査書

はじめに

このたびは、ご多忙の中、ISMS 適合性評価制度(以下、ISMS 制度)に関するアンケート調査にご協力を賜り、厚く御礼申しあげます。おかげさまで、多数の組織様から、貴重なデータとともに、数多くの有益なご意見、ご要望等を頂戴することができました。調査結果につきましては、本書で概要をご報告するとともに、今後の制度の運営に積極的に活用させていただく所存です。

ISMS 適合性評価制度は、民間主体の制度として導入され、本協会が立ち上げ時点から主導的な立場で推進してまいりました。本制度は、2001 年度にスタートし、約１年間のパイロット運用を経て、2002 年 4 月から本格運用に入り、今日に至っております。

この間、数多くの情報セキュリティ事故が発生し、それらへの対応や経済産業省によるガイドラインの制定等を契機にして、情報セキュリティ管理の重要性についての認識は、格段に高まってまいりました。

このような背景のもと ISMS 制度は着実に社会に根付いてまいりましたが、本制度も本格運用開始以来５年が経過したことから、制度の信頼性をより高めるためにも、制度全体を点検すべき時期に来ているとの認識のもとに、このたびのアンケート調査を実施する運びになりました。

調査の目的は、ISMS 制度の実態を把握し、ISMS 制度の更なるスパイラルアップを図ることにあります。中でも、ISMS 認証審査は、組織様の ISMS 改善に大きな影響を与えますので、認証審査員の力量及び認証審査の質の現状を把握することを、今回のアンケート調査の主眼点にいたしました。

本報告書で調査結果の概要をご報告するとともに、今後、調査結果に対して更に分析、検討を進め、皆様にとってなお一層有効で、活用度の高い制度にするために、必要な対応策を講じていく所存です。

また、関連機関、関係者がそれぞれの立場、視点で、調査結果を ISMS 制度の改善のためにご活用いただければ幸いです。

2009 年 3 月

財団法人 日本情報処理開発協会
情報マネジメント推進センター

調査の概要

調査内容
付録の「ISMS 適合性評価制度に関するアンケート調査書」を参照。
調査項目は以下のとおり。
・組織の基本情報
・ISMS 認証の運用実績に関する情報
・審査員の力量及び審査の質に関する評価
・制度全般に対するご意見、ご要望

調査対象
調査開始の 2008 年 10 月時点で、本協会が認定した ISMS 認証機関から ISMS 認証を取得した組織のうち登録情報を公開している 2,683 組織。

調査方法
郵送した調査書の質問（選択形式及び記述形式）に回答、返信していただく。

調査期間
2008 年 10 月下旬～11 月末日。ただし、回答希望日以降の到着分も集計した。

有効回答数、回収率
有効回答数　　1,161 件
回収率　　43.3%

基本情報について

質問１　法人の業種

23 種類の業種区分について尋ねたところ、「情報技術」(59.7%)が突出しており、以下「その他サービス」(12.7%)、「製造業」(7.2%)、「卸売・小売業」(5.0%)が続いている（図 1-1）。なお、この質問の集計結果は、同一法人の中の複数の部門が個別に認証を取得している場合、同一法人の情報を重複して集計したものであることに注意。

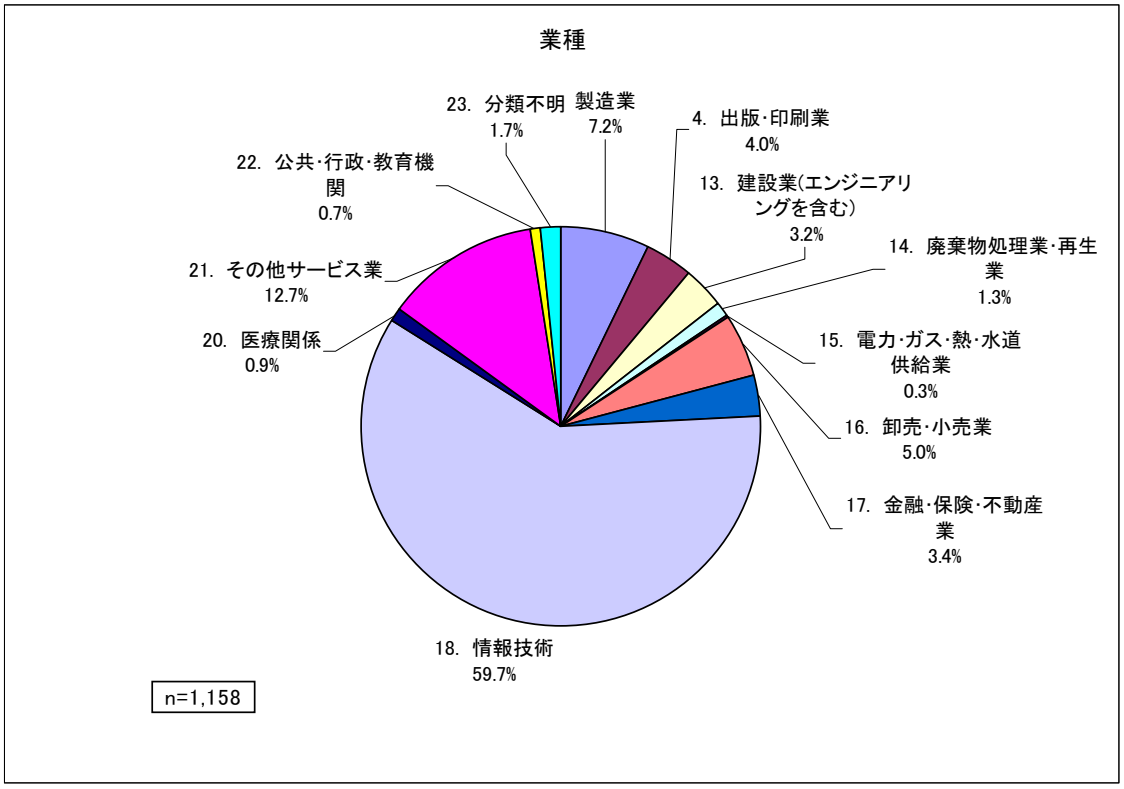


図 1-1　法人の業種

「製造業」の内訳は図 1-2 に示すとおりとなっている。最も多いものが「電気／電子機器・光学的装置製造業」(54.2%)、以下「その他の製造業」(16.9%)、「機械・機器の製造業」(12.0%)の順となっている。

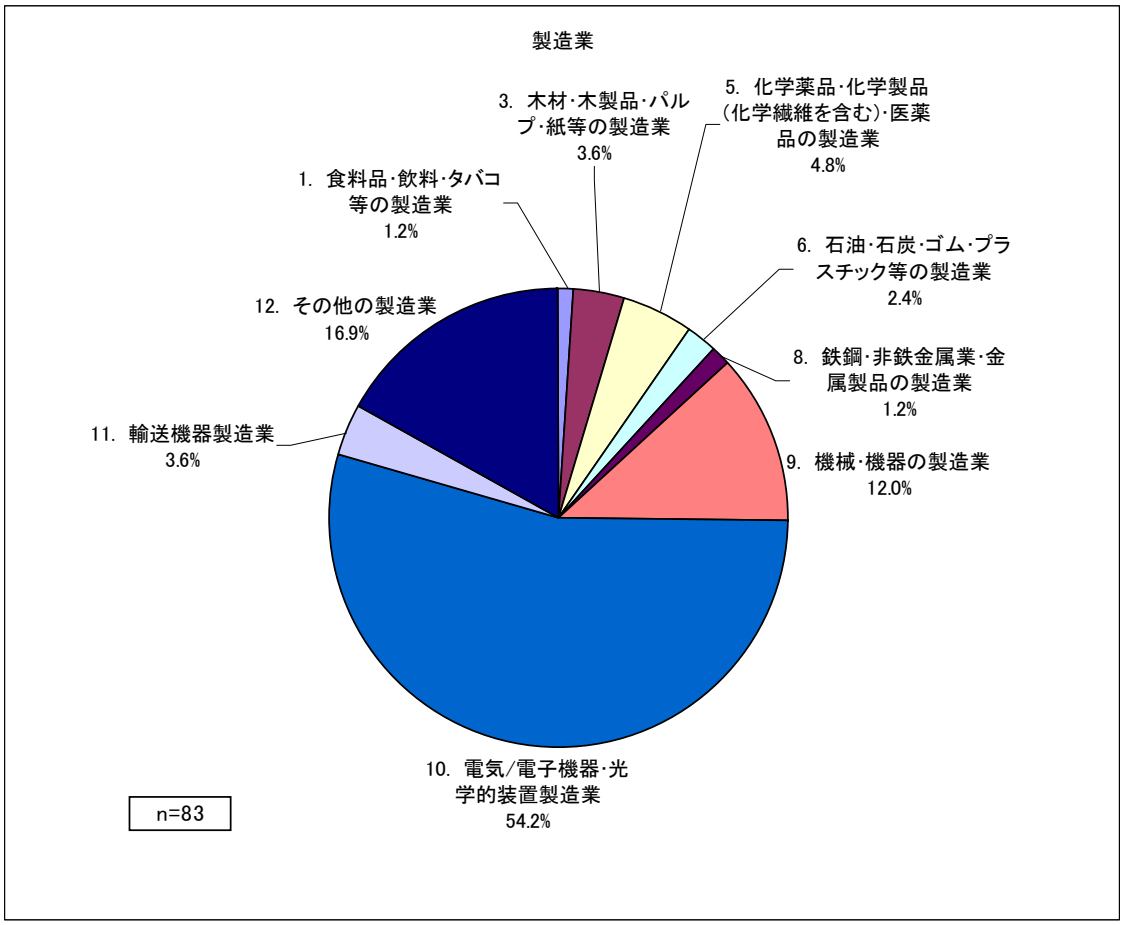


図 1-2　製造業の内訳

「情報技術」の内訳として 11 件の小区分を尋ねたところ、「受注ソフトウェア業」(28.8%)、「システムインテグレーション業」(26.7%)で過半数を占め、以下「システム等管理運営受託業」(9.2%)、「通信業」（8.0%）の順となっている（図 1-3)。

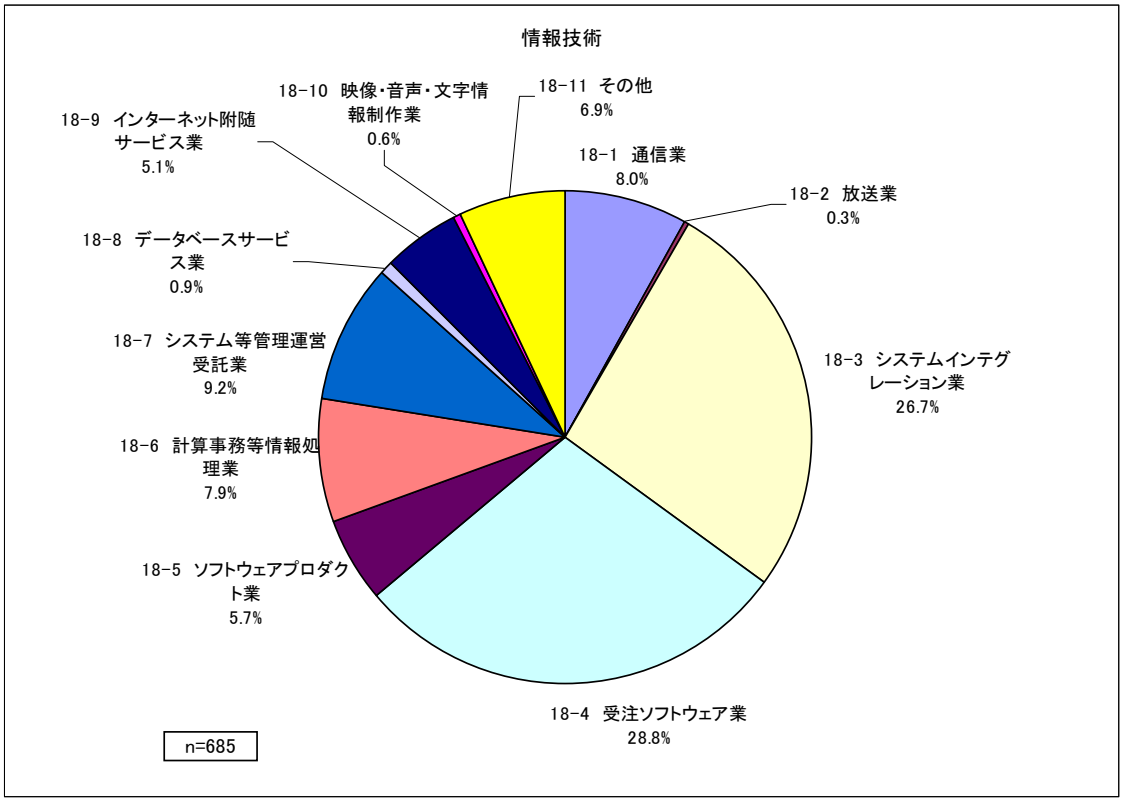


図 1-3　情報技術の内訳

質問２　資本金

法人が株式会社の場合、資本金を尋ねたところ、「5000 万円以下」(35.9%)が最も多く、対極の「3 億円超」(35.1%)　が小差で続き、以下「5000 万円超、1 億円以下」(15.8%)、「1 億円超、3 億円以下」(13.2%)となっている（図 2)。

なお、この質問の集計結果は、同一法人の中の複数の部門が個別に認証を取得している場合、同一法人の情報を重複して集計したものであることに注意。

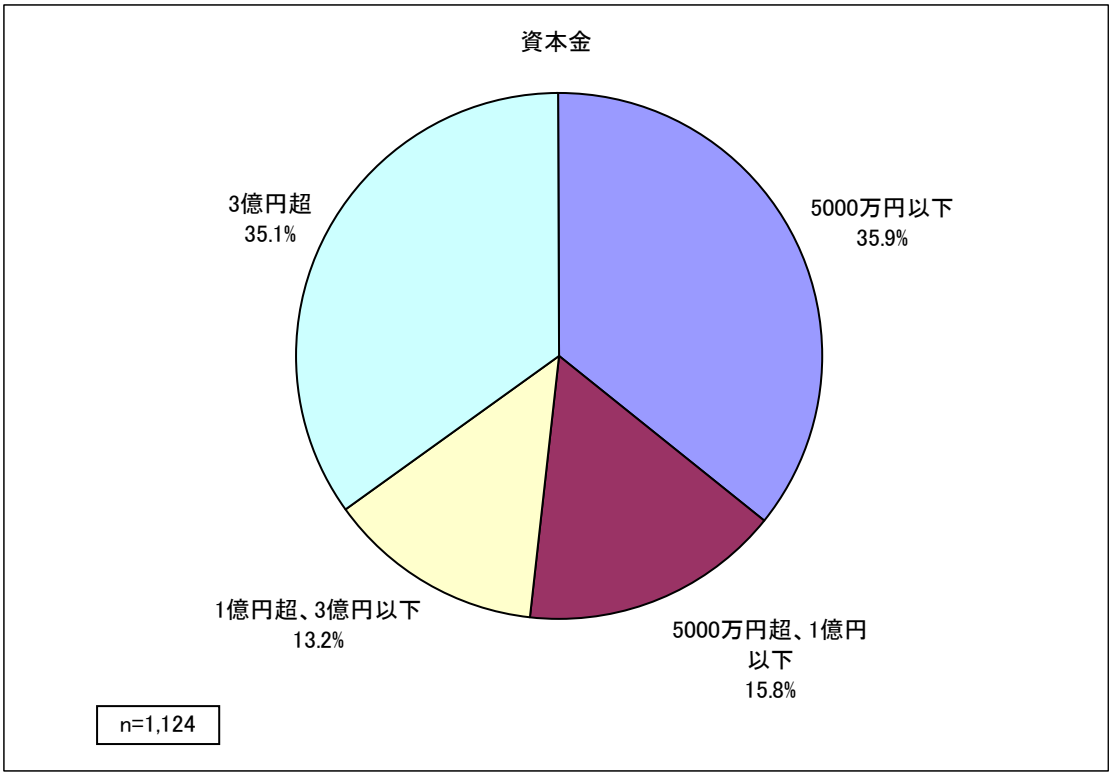


図 2　資本金

質問３　従業員数

法人が常時使用する従業員の数については、「300 人超」(40.2%)が最も多く、「100 人超、300 人以下」(22.1%)、「50 人超、100 人以下」(15.5%)の順となっている（図 3)。

なお、この質問の集計結果は、同一法人の中の複数の部門が個別に認証を取得している場合、同一法人の情報を重複して集計したものであることに注意。

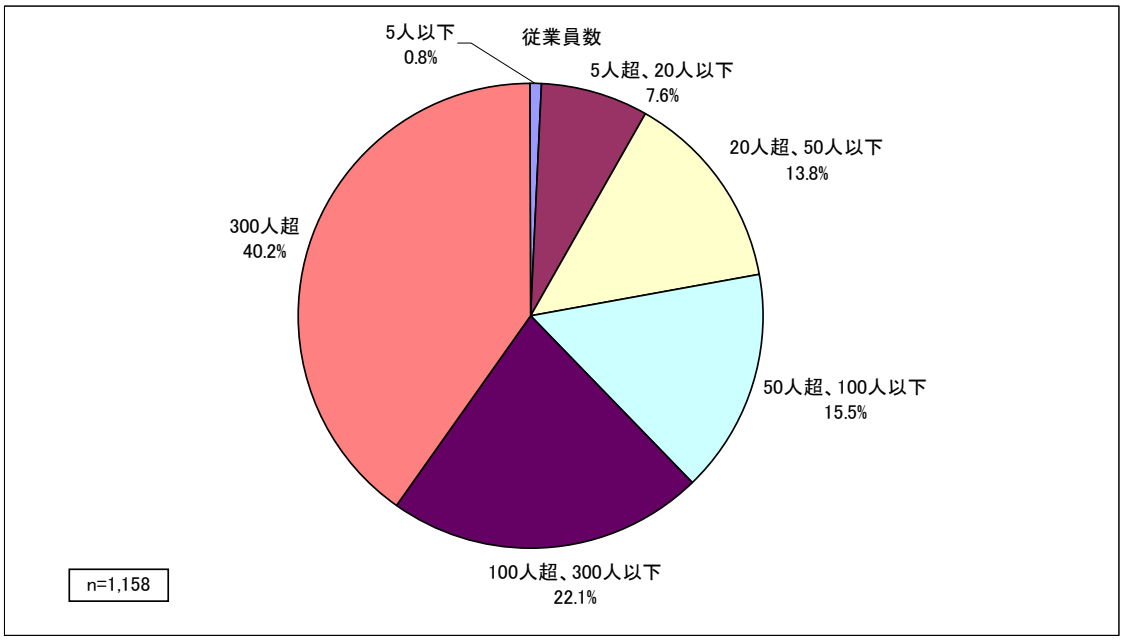


図 3　従業員数

質問４　認証範囲の従業員数

認証範囲の従業員数を実数で尋ねた結果を、質問３と同一の区分で分類したところ、「20 人超、50 人以下」(23.9%)、「100 人超、300 人以下」(22.7%)、「50 人超、100 人以下」(20.9%)の順となった。区分の中間値は「50 人超、100 人以下」となっている（図 4)。

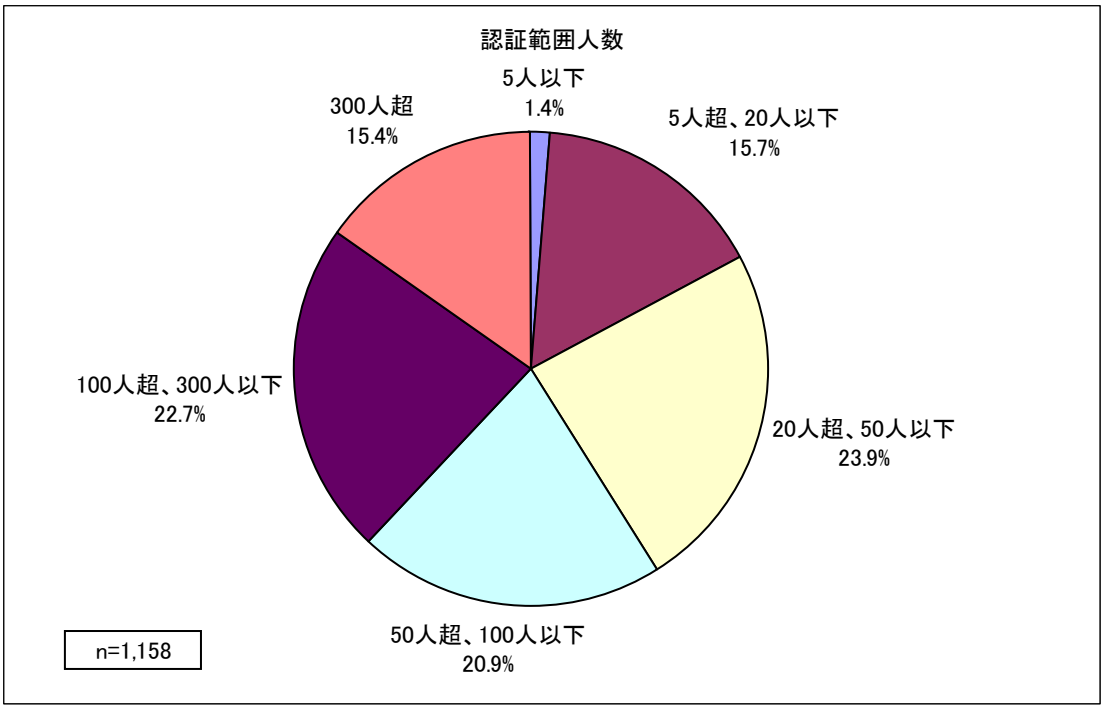


図 4　認証範囲の従業員数

ISMS 認証の運用実績等について

質問５　経過年数

ISMS 認証取得後の経過年数を年月数で尋ねた結果を、「１年以下」「１年超３年以下」「３年超５年以下」「５年超」の４階級に区切って度数を調べた。

「１年超３年以下」(42.7%)、「３年超５年以下」(28.7%)の順となった（図 5)。

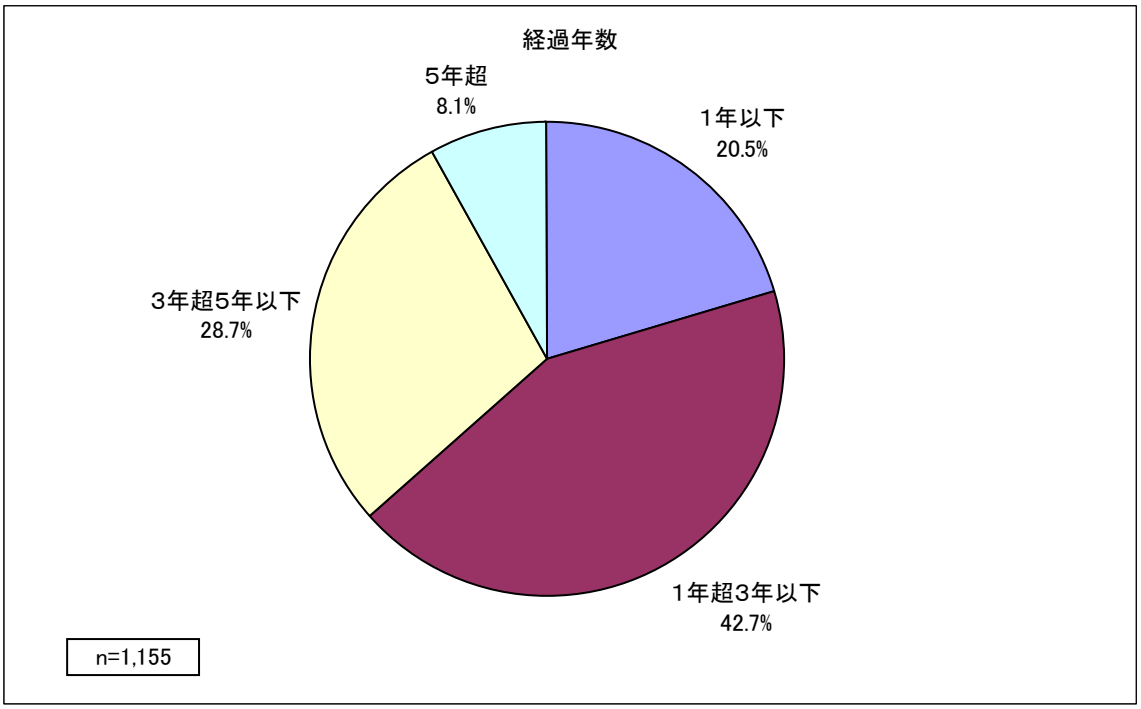


図 5　経過年数

質問６　導入の目的又は動機

ISMS 導入の目的又は動機について、８つの項目に「該当する」「やや該当する」「余り該当しない」「該当しない」の４段階で尋ねた結果は図 6 のとおりとなった。

全項目のうち、「該当する」の回答が最も多いものは「2 組織の情報セキュリティ対策の強化のため」(81.1%)、僅差で「5 顧客の信頼性確保のため」(79.7%)、「1 組織の情報セキュリティ管理体制の強化のため」(78.9%)が続く。「該当する」の回答が最も少ないものは「4 入札、受注の条件、取引先からの要請による」(34.5%)であった。

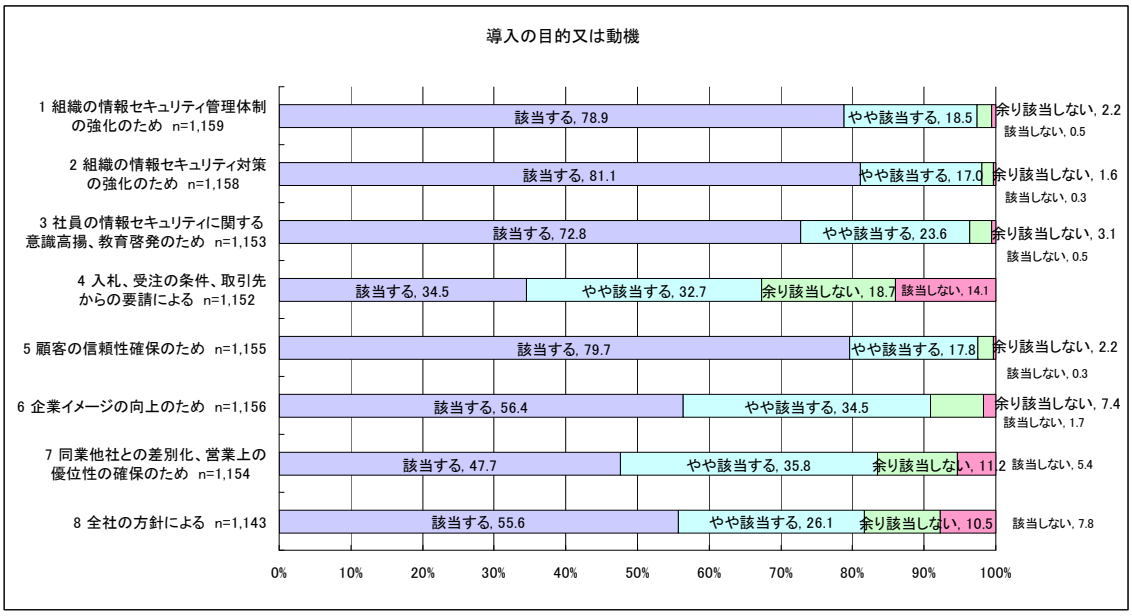


図 6　導入の目的又は動機

項目 No.1 から項目 No.8 以外の導入の目的又は動機のうち、主な事項を以下に記す。

・経営ツール、BPR、業務改善等
・法令順守(コンプライアンス)
・グループ企業としての取組み
・安全対策事業所制度の終了

質問７　導入の効果

ISMS 導入の効果について、８つの項目に「該当する」「やや該当する」「余り該当しない」「該当しない」の４段階で尋ねた結果は図 7 のとおりとなった。

全項目のうち、「該当する」の回答が最も多いものは「2 組織の情報セキュリティ対策が強化できた」(75.0%)、僅差で「1 組織の情報セキュリティ管理体制が強化できた」(74.9%)が続き、次いで「3 社員の情報セキュリティに関する意識高揚、教育啓発に寄与した」(69.8%)となった。

「4 顧客の信頼性確保に貢献した」(52.0%)、「5 企業イメージの向上に貢献した」(41.4%)及び「6 営業上、同業他社に対する優位性の確保に貢献した」(26.7%)の「該当する」の回答比率は、導入の目的又は動機で「該当する」とした回答比率に比べて、15%から 28%低下している。

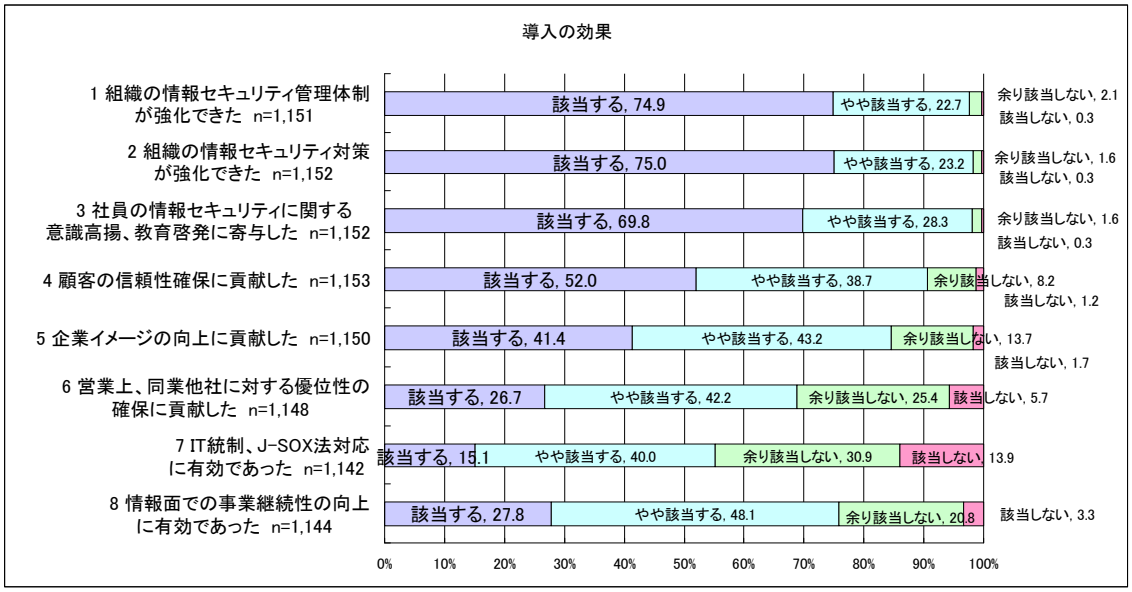


図 7　導入の効果

項目 No.1 から項目 No.8 以外の効果のうち、主な事項を以下に記す。

・情報セキュリティを考慮したシステムの導入、構築ができた(No.2 に関連)。
・利害関係者からの情報セキュリティ対策、体制等の調査に自信をもって対処できようになった。
・社内の業務フロー、規則等が明確になり、明文化できた。
・副次効果として、書類、データ等の整理、整頓に役立った。

質問８　ISMS に関する今後の課題

回答件数は 794 件

回答内容を下記のように分類した結果は図 8 のとおりである。なお、１件の回答に複数の分類項目に該当する内容があれば、各々を分けて分類した。

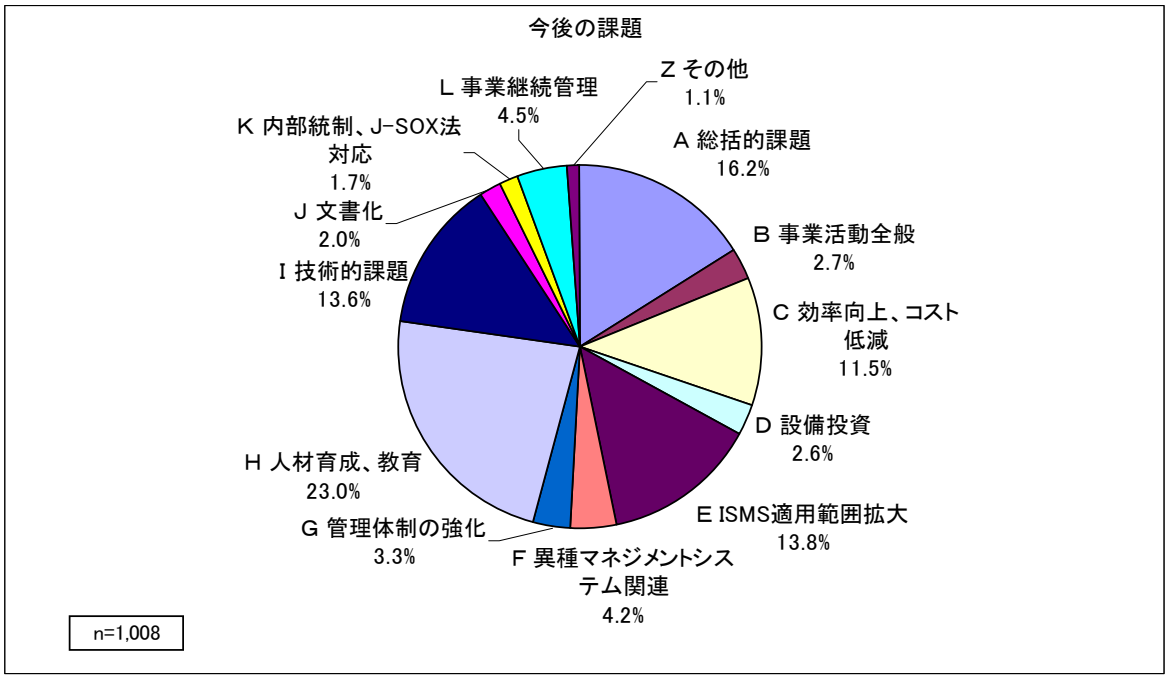


図 8　ISMS に関する今後の課題

A　総括的課題：マネジメントシステムの継続改善、形骸化の防止、運用の定着化など

B　事業活動全般：経営、事業への反映、営業活動、顧客要求への対応など

C　効率向上、コスト低減：運用効率の向上、運用コスト低減、情報セキュリティと利便性のバランスなど

D　設備投資：システム化、ツール導入を含む

E　ISMS 適用範囲の拡大：部門への適用から全社、グループ会社への適用拡大など

F　異種マネジメントシステム(プライバシーマークを含む)との統合、他のマネジメントシステム認証取得など

G　管理体制の強化：ISMS の運用、管理体制の強化

H　人材育成、教育：ISMS 推進要員の育成、社員の教育、意識高揚など

I　技術的課題：リスクアセスメントの強化、管理策の強化、有効性評価など

J　文書化：契約、規定、手順などの見直し

K　内部統制、J-SOX 法対応：内部統制、J-SOX 法対応への活用、連携

L　事業継続管理：事業継続計画の策定、事業継続管理の推進

Z　その他

審査員の力量及び審査の質について

質問９　審査員の力量

最近受審した審査での審査員の力量について、６つの項目に「十分である」「概ね十分である」「やや不十分である」「不十分である」の４段階で評価していただいた結果は図 9-1 のとおりとなった。

全項目のうち、「十分である」の回答が最も多いものは「1 マネジメントシステムに関する知識及び業務経験」(74.7%)、次いで「2 情報システム、情報セキュリティに関する知識及び業務経験」(70.1%)、「5 審査技術」(65.5%)、「4 コミュニケーション能力」(65.5%)の順となっている。「6 改善課題を指摘する能力」(60.9%)、「3 受審組織の業務に対する理解」(50.6%)はやや少なかった。

「十分である」及び「概ね十分である」の回答を加算したものの比率は、いずれの項目についても 95%を上回る高い値を示している。

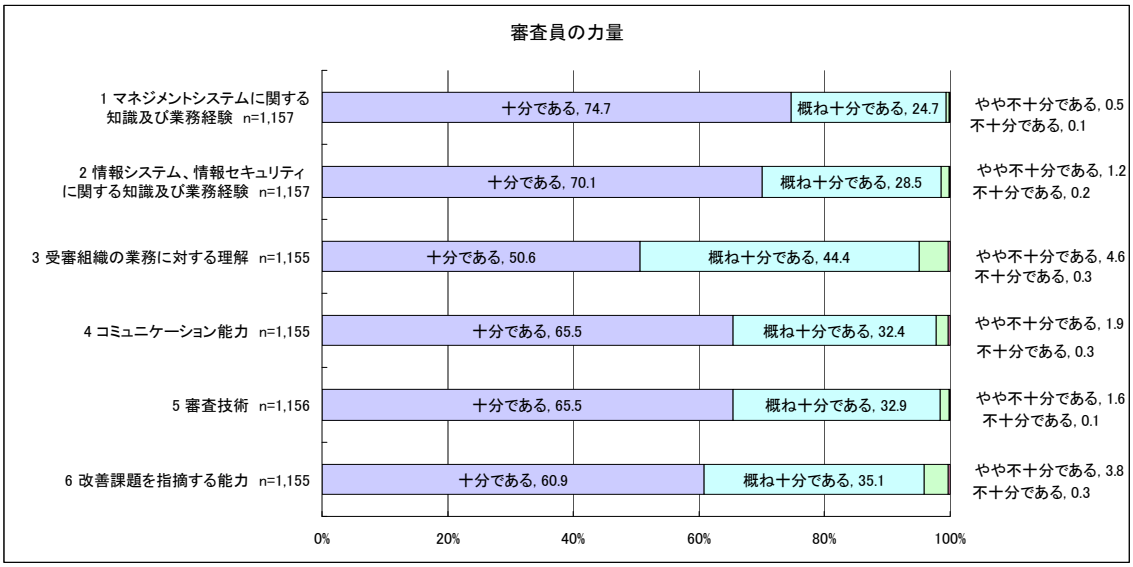


図 9-1　審査員の力量

質問９と質問５とのクロス集計

審査員の力量に関する６つの項目の評価結果のうち、「十分である」の比率を、ISMS 認証取得後の経過年数の４階級ごとにクロス集計した結果を、図 9-2 に示す。

項目によって、若干の差異があるものの、ISMS 認証取得後の経過年数を経るにしたがって、「十分である」の比率が減少する傾向がみられる。特に、経過年数が３年を境にして、階段的に減少する傾向にある。

これは、受審側で ISMS の運用、改善の実績を積むに従い、審査に対する要求度、期待度が高くなるのは当然として、審査側の対応が受審側の要求、期待に応えきれていないことを示すものと思われる。特に、受審組織にとって ISMS 取得３年後に再認証審査を受けることが、審査に対する要求度が高まる契機になっているようである。

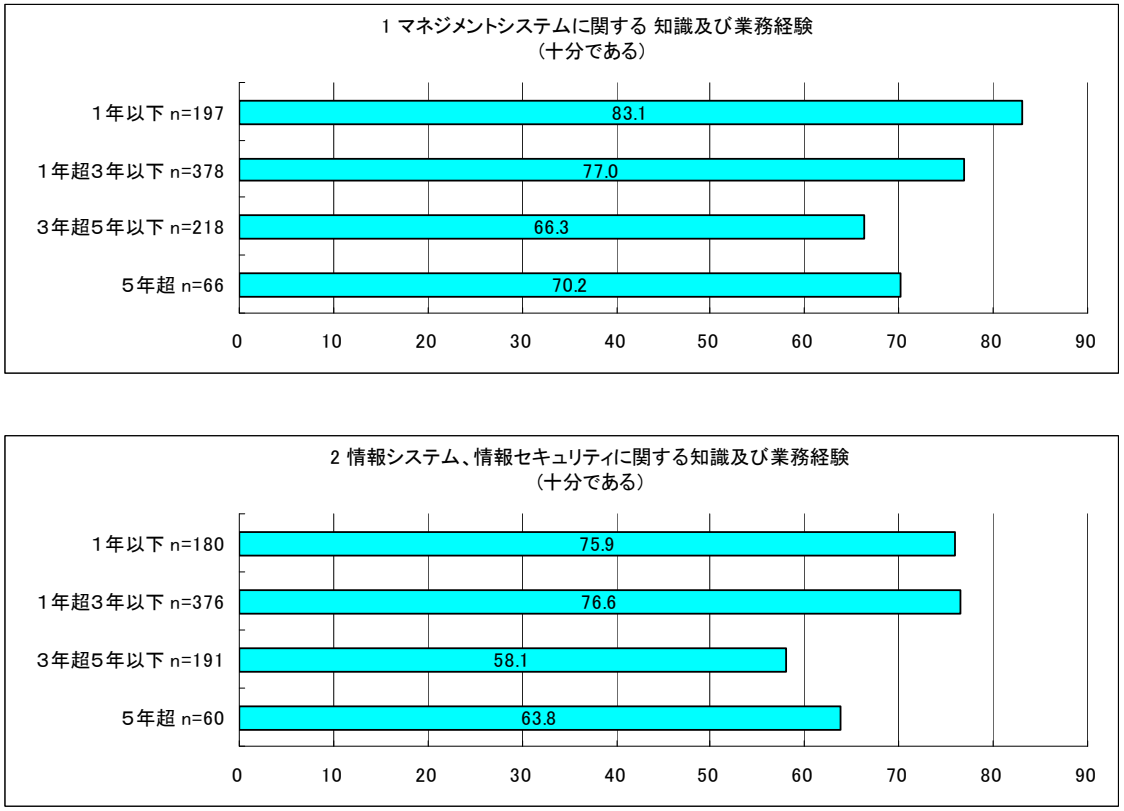
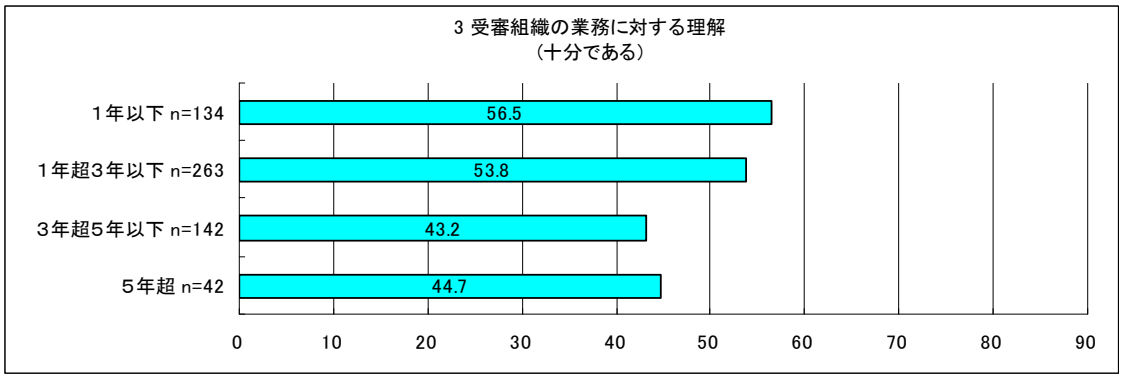
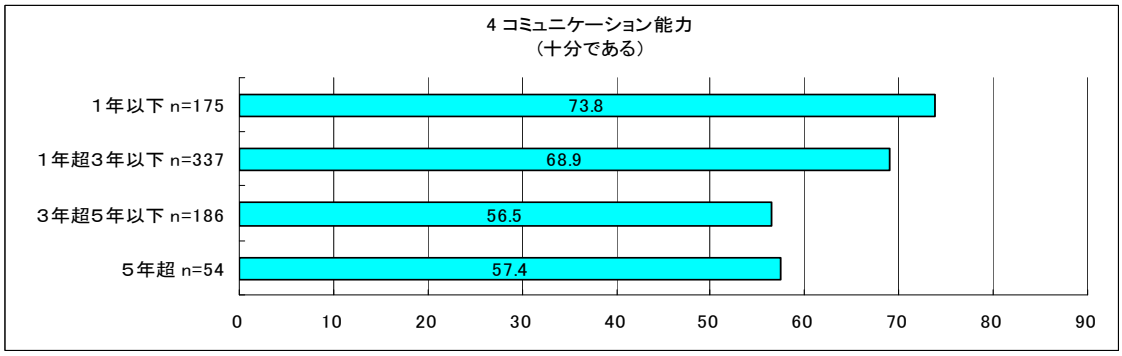
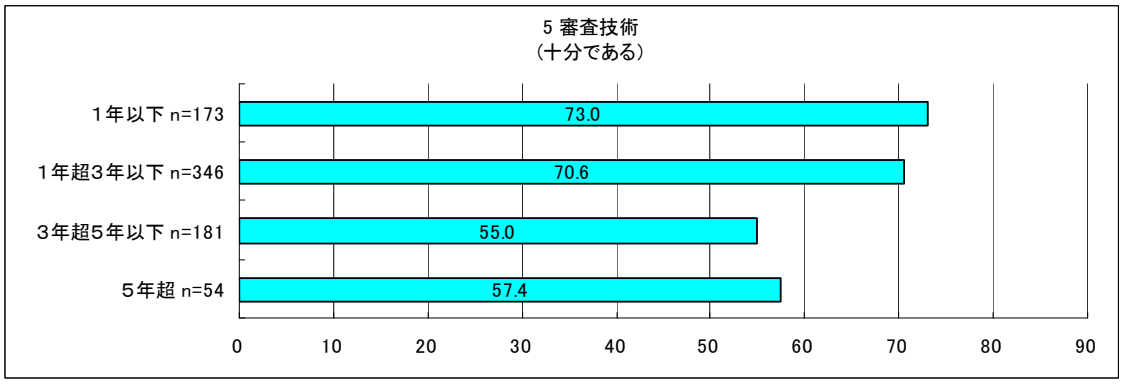


図 9-2　経過年数区分と審査員の力量







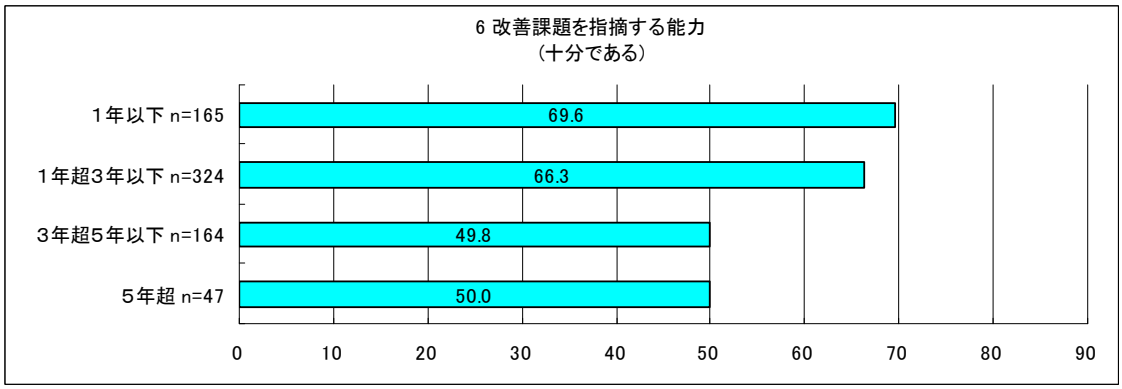


図 9-2　経過年数区分と審査員の力量（続き）

質問１０　審査の質

最近受審した審査の質について、審査の内容、審査の時間、審査の所見・指摘、審査に対する総合評価の４つの観点で評価していただいた。

(1)審査の内容

審査の内容に関しては、規格適合性及び管理策の２つに分けて、「満足」「やや満足」「やや不満」「不満」の４段階で評価していただいた。

(a)規格適合性に関する審査内容の評価は、「満足」(69.6%)、「やや満足」(28.1%)、「やや不満」(2.0%)、「不満」(0.3%)であった（図 10-1）。

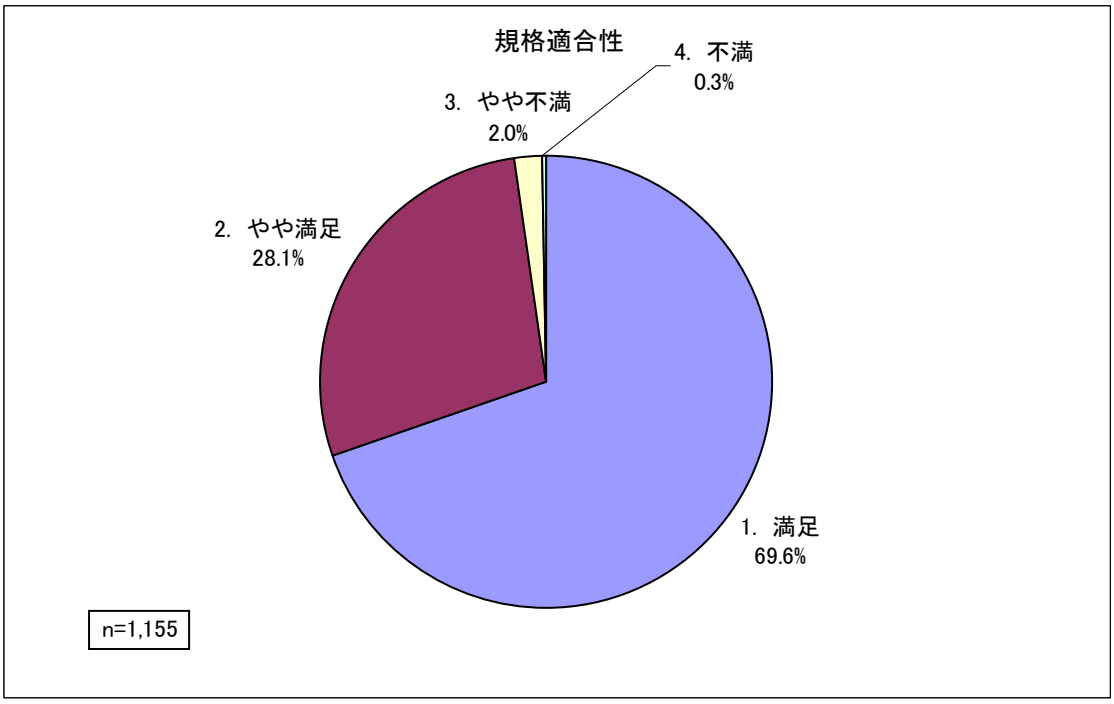


図 10-1　審査の内容（規格適合性）

「やや不満」及び「不満」な点として指摘されたものの例示

・規格の性格上、あいまいさが残る事項について、審査員の主観によるところがあり、見解の相違があった。
・取組みが実施され、記録が残されていればＯＫというようなことがあった。
・前回と審査員が異なり、改善事項の評価が考え方の違いとなって再度指摘を受けたことがあった。
・専門家は当然理解できる内容でも、受審側にとって意味不明のまま終わることがある。

(b)管理策に関する審査内容の評価は、「満足」(62.4%)、「やや満足」(34.7%)、「やや不満」(2.8%)、「不満」(0.2%)の順であった（図 10-2)。

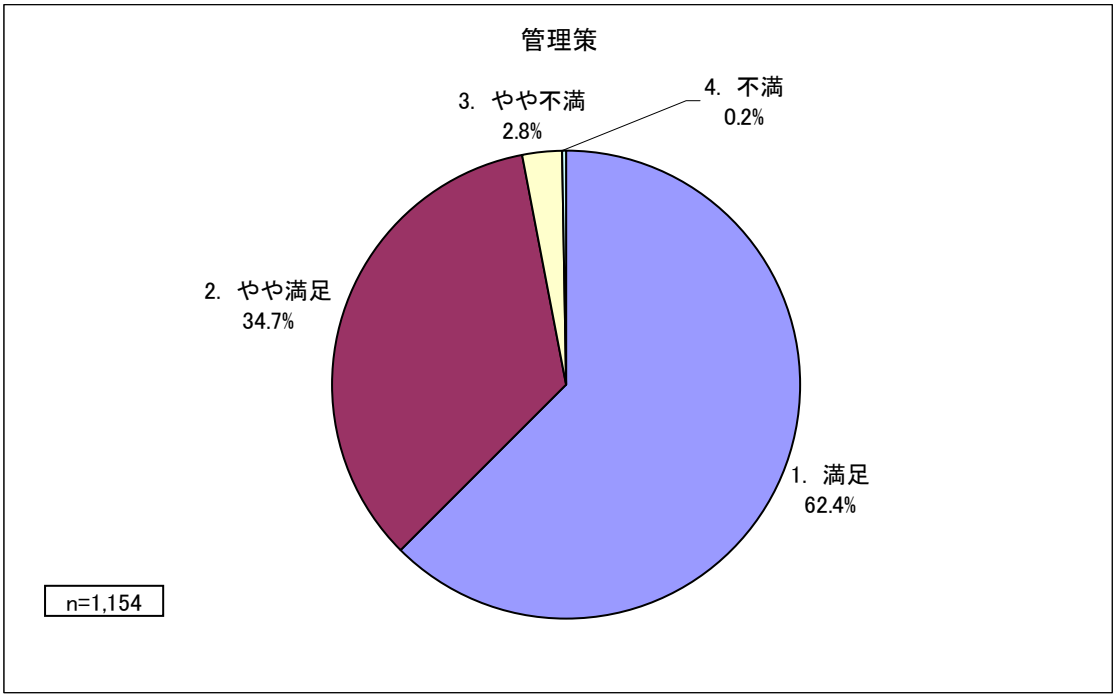


図 10-2　審査の内容（管理策）

「やや不満」及び「不満」な点として指摘されたものの例示

・本社では実施していない綿密なレベルのセキュリティ対策を実施している委託先に、観察事項の指摘を受けたこと。
・ISMS というより、事業継続性評価のような指摘が多く、従来の ISMS の概念を拡大していると思われる。
・ISO 27004 が未発行なのに、要求事項に書かれていない指摘があった。
・それぞれの資産の利用方法や重要度に応じた管理が実施されているかの視点での審査が少ない。
・管理策の解釈が審査員によって異なり、規格に要求されていないことを指摘されることがある。
・管理策の検証が不十分と思われた。
・業種特有のリスク、業種では考えなくてよいリスク等の識別が不十分である。
・業務改善の実施を主眼に審査されるため、個々の管理策に対する有効性の評価が不鮮明である。

(2)審査の時間

審査の時間に関しては、審査の信頼性の観点から、「適切」「長い」「短い」「何とも言えない」の４項目で評価していただいた。

評価は、「適切」(71.9%)、「長い」及び「何とも言えない」(12.4%)、「短い」(3.3%)の順であった（図 10-3)。

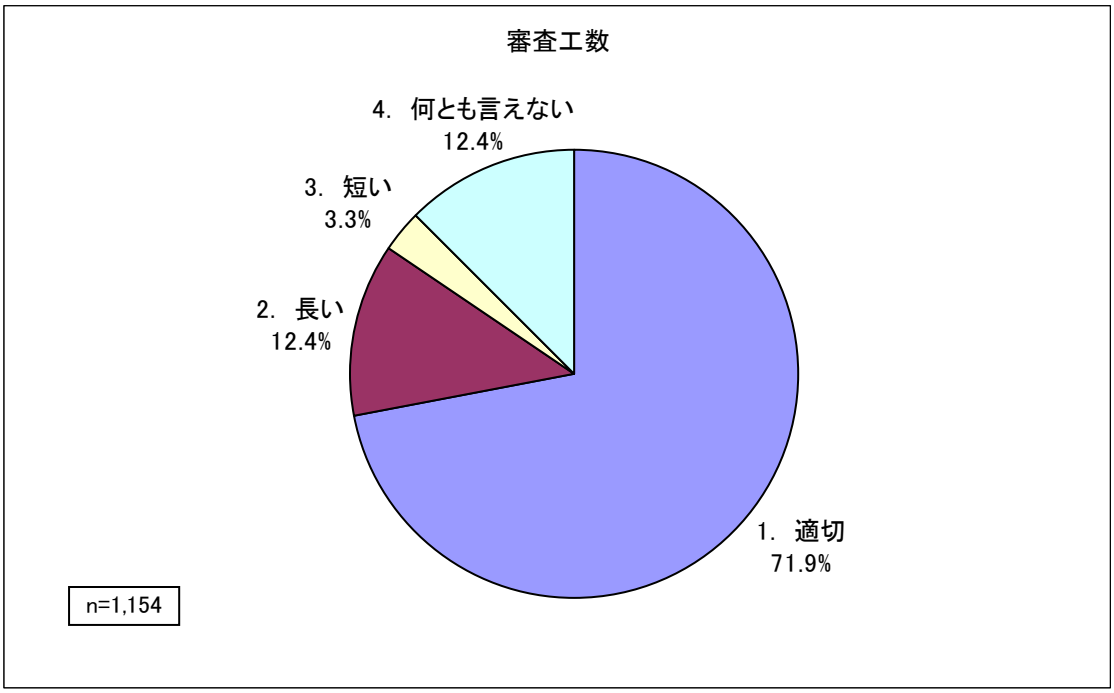


図 10-3　審査の時間

(3)審査の所見・指摘

審査の所見・指摘の有効性を、「大いに役立った」「役立った」「あまり役立たなかった」「役立たなかった」の４段階で評価していただいた。

評価は、「役立った」(63.2%)、「大いに役立った」(34.3%)、「あまり役立たなかった」(2.4%)の順であった。「役立たなかった」の評価はゼロであった（図 10-4)。

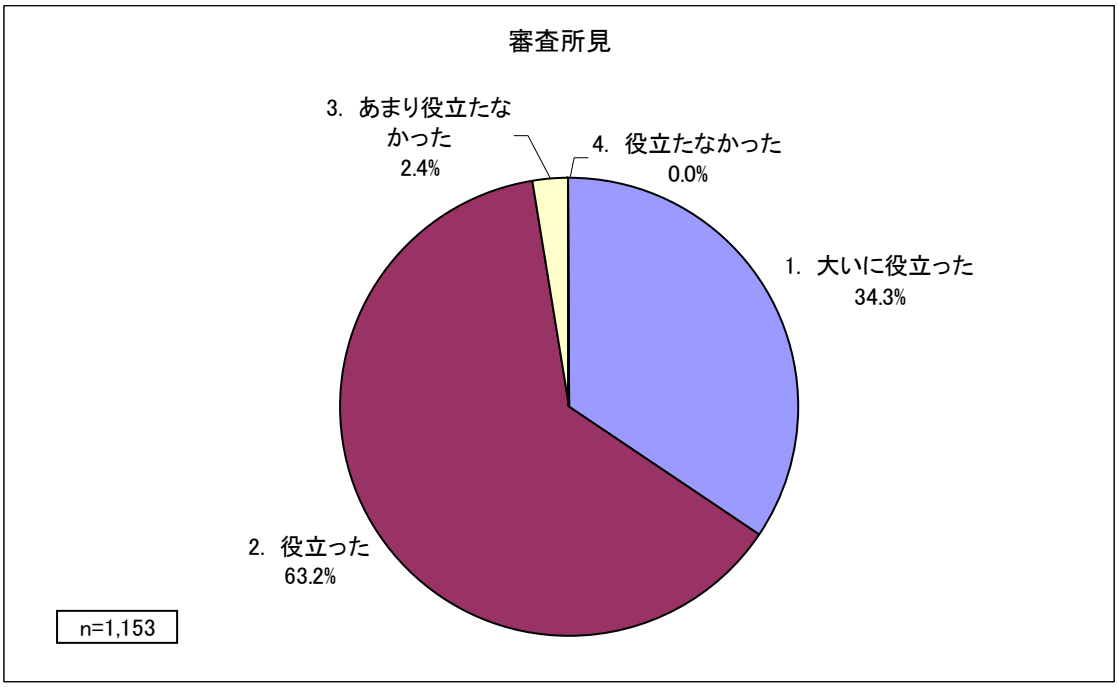


図 10-4　審査の所見・指摘

「あまり役立たなかった」点として指摘されたものの例示

・マネジメントパフォーマンスや ISMS 自体への有効性に対する審査が不十分であった。
・維持する上では役立っているが、スパイラルアップにはつながっていない。
・有効性評価が受審者として具体的に理解できない。
・当社の企業としての方針に触れる指摘が一部にあり、認証機関と意見が合わなかった。
・業務に関する業界の情報セキュリティ動向を考慮した指摘があればよかった。
・資産の洗い出しから適用宣言書策定までのステップに対してコメントを頂いたが、効率的な運営と徹底の観点からの議論が必要と感じた。

(4)審査の質に対する総合評価

審査の質に対する総合評価として、「満足」「やや満足」「やや不満」「不満」の４段階で評価していただいた。

評価は、「満足」(69.8%)、「やや満足」(27.0%)、「やや不満」(2.9%)、「不満」(0.3%)の順であった（図 10-5)。

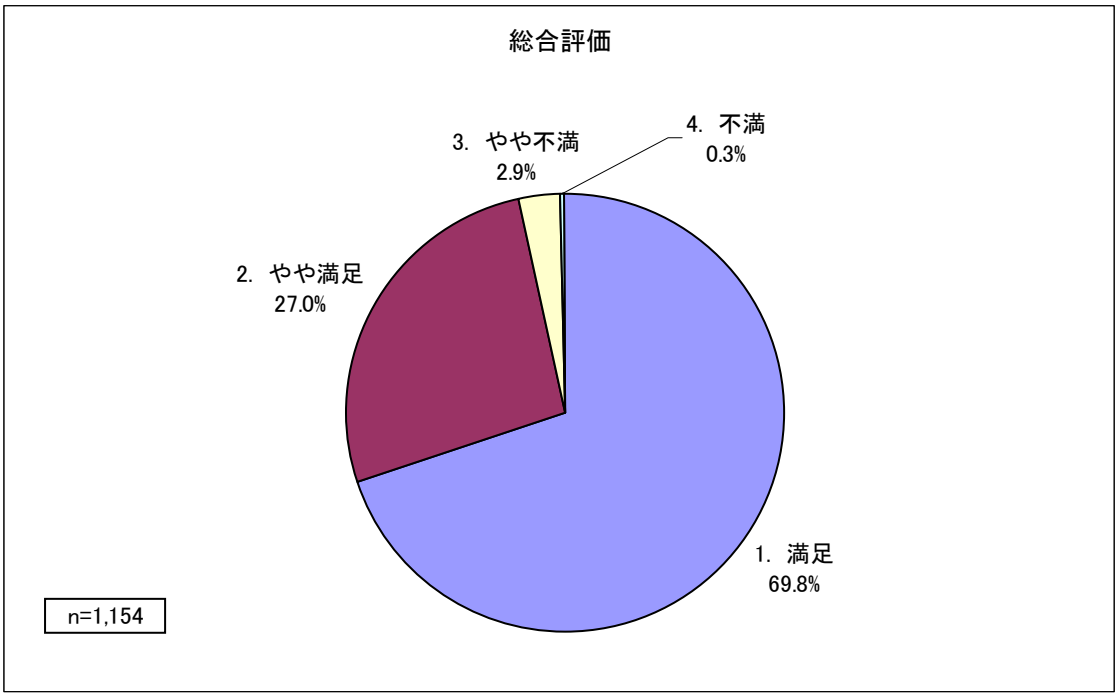


図 10-5　審査に対する総合評価

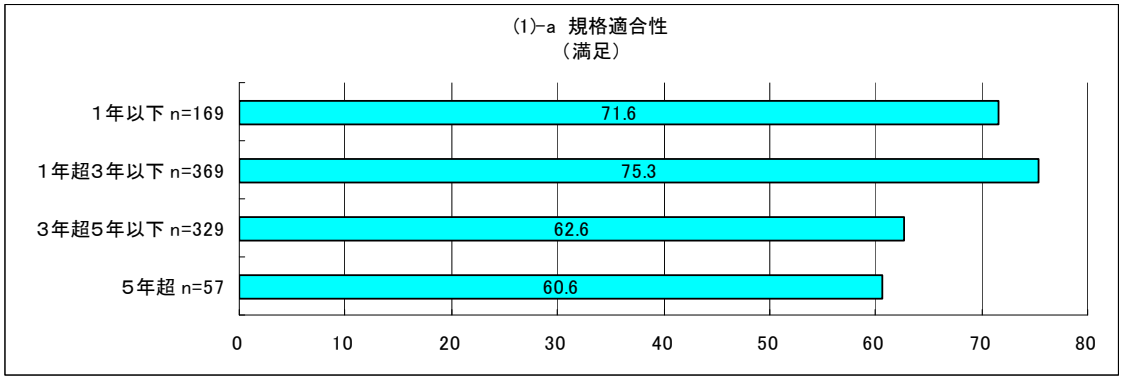
「やや不満」及び「不満」な点として指摘されたものの例示

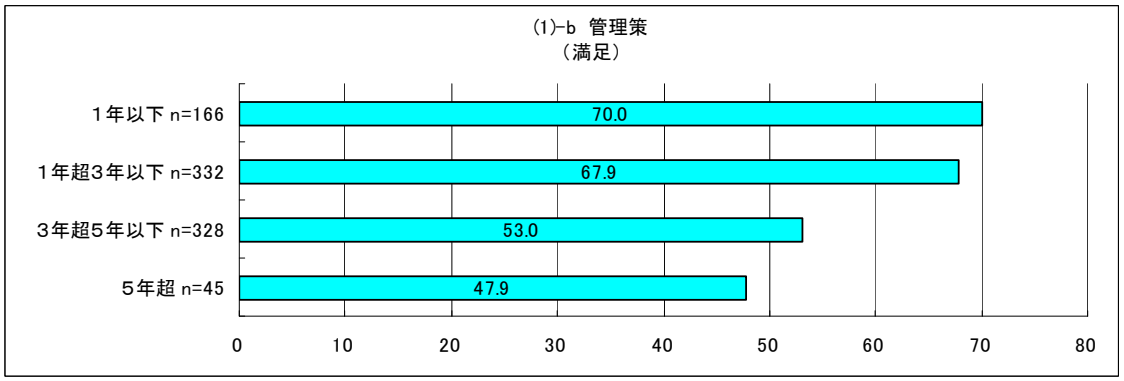
・情報セキュリティの改善につながる指摘になっていないことがあった。
・ISMS の審査であるはずが、審査員の方が QMS の審査と勘違いしている様にみえる状況があった。
・審査員から当社の更なる改善ポイントを見出そうとする意欲に乏しかった。
・企業レベルに応じない、理想論的な指摘がある。
・審査員が毎回異なるので、組織の特徴を理解して審査するには時間が不十分と思われる。
・審査員によって力量の差が大きいと感じた。
・審査時に課題を深掘りして、本質を見極めようとする姿勢が見られないケースがあった。

質問１０と質問５とのクロス集計

審査の質に関する５つの項目の評価結果のうち、各項目の選択肢の「1」(「満足」、「適切」又は「大いに役立った」)を選んだ比率を、ISMS 認証取得後の経過年数の４階級ごとにクロス集計した結果を、図 10-6 に示す。

項目によって、若干の差異があるものの、「質問９と質問５とのクロス集計」の場合と、概ね同様の傾向がみられる。





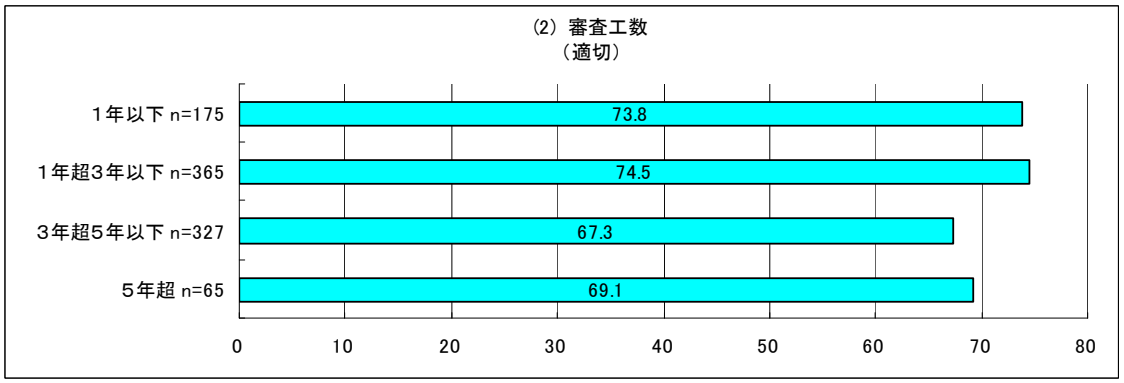
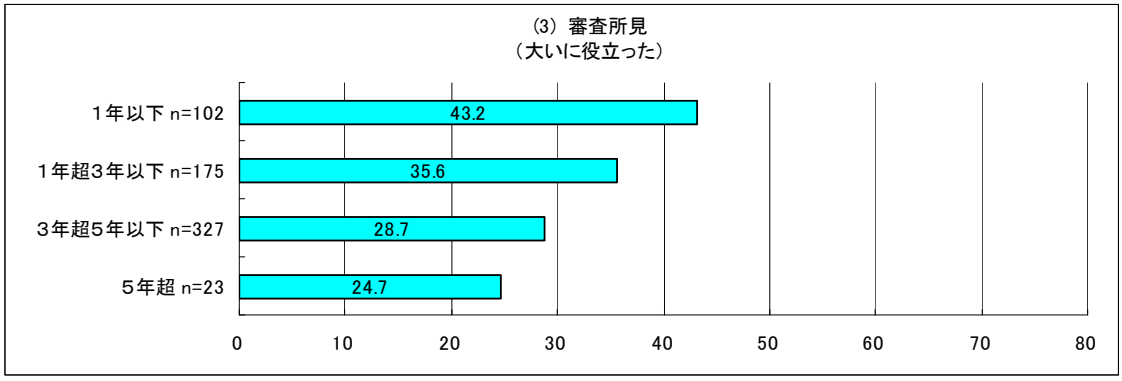


図 10-6　　経過年数区分と審査の質



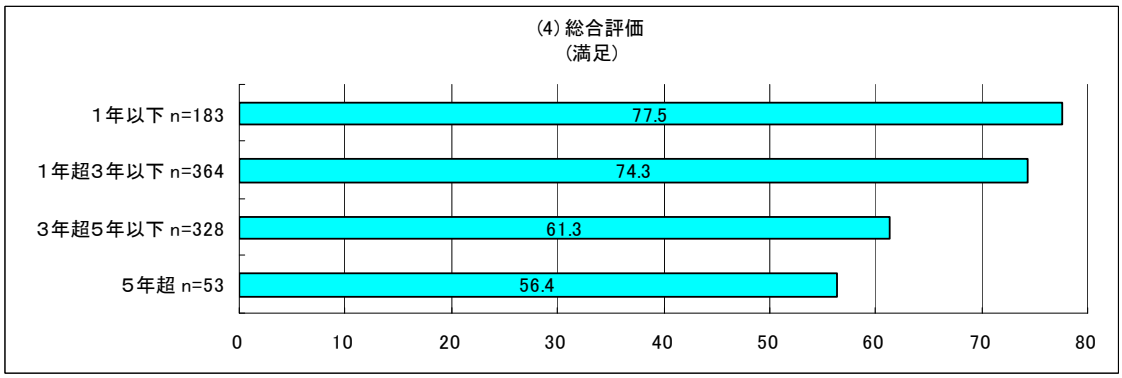


図 10-6　　経過年数区分と審査の質（続き）

質問１１　認証審査及び審査員に対するご意見・ご要望

回答件数は 295 件

回答内容を下記のように分類した結果は図 11-1 のとおりである。なお、１件の回答に複数の分類項目に該当する内容があれば、各々を分けて分類した。

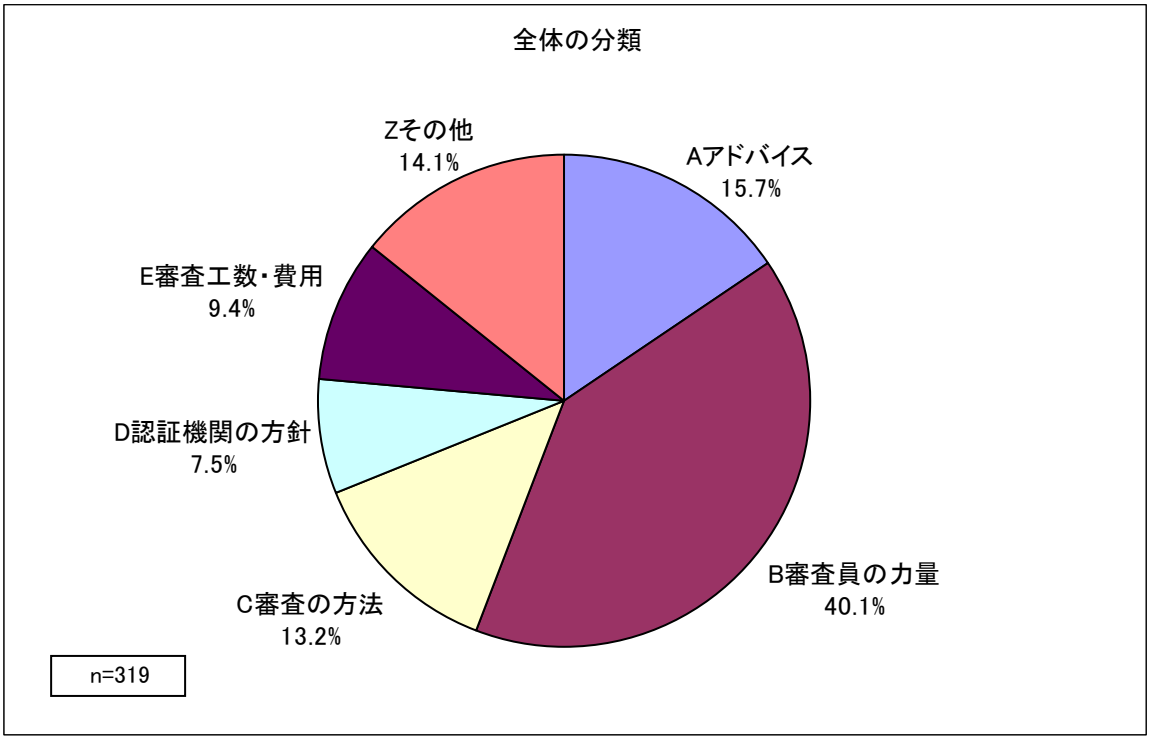


図 11-1　認証審査及び審査員に対するご意見・ご要望

分類項目ごとの回答内容の傾向について分析した結果を述べる。

Ａ　アドバイス、コミュニケーション

この分類項目に該当する意見、要望の多くは、審査において、受審組織にとってより有益な指摘、情報提供を求めるものであり、コンサルティングを受けることに相当する可能性のある内容である。

審査ではコンサルティングを提供することはできないが、「例えば、特定の解決策の提示を含まない、審査中に明らかになった改善の機会の明示」(JIS Q 27006:2008　5.2.1 f)参照)はコンサルティングとみなされない。この種の意見、要望があることを念頭において、審査においてより高い価値を付加することが課題と考える。回答例を以下に記す。

・受審組織のマネジメントシステム改善につながる他社事例の紹介
・ISMS を経営のツールとして活用するためのヒントや有効性の改善に結び付く手掛かりの提供
・データと数値を使った、管理策のリスクと効果の説明
・同業(同規模)他社と比較した、受審組織のセキュリティレベルの提示
・受審組織のスパイラルアップについての議論

B　審査員の力量

この分類項目については、小分類項目に細分割して、分類、集計した結果を図 11-2 に示す。

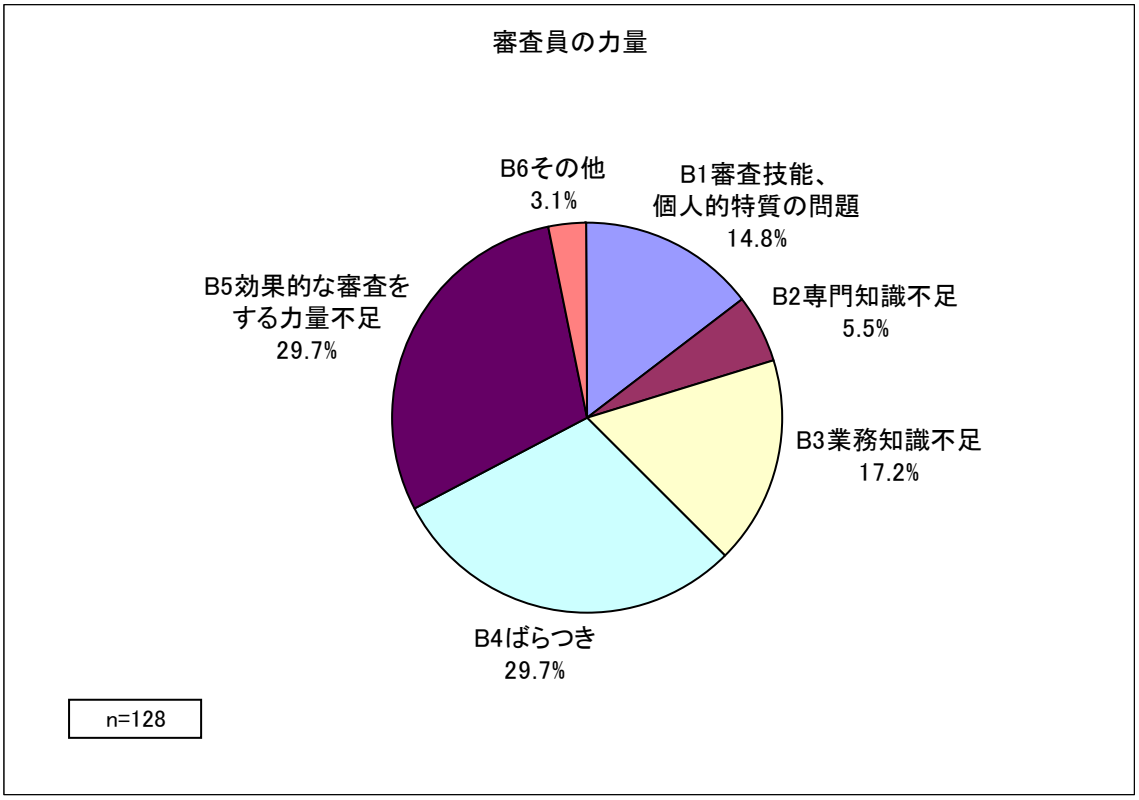


図 11-2　認証審査及び審査員に対するご意見・ご要望（審査員の力量）

以下に、小分類ごとの回答例を示す。

B1　審査技能、個人的特質の問題

・理解しにくい言葉や規格用語での質問、指摘がある
・説明能力、コミュニケーション能力不足が感じられる
・報告書の文章が不正確なものや理解し難いものがある
・得意分野に集中した審査となっている

B2　専門知識不足

・最新セキュリティ技術、知識の理解不足
・IT 系、システム関係には強く、マネジメントシステムの知識、経験が不足
・技術・知識レベルの一層の向上に期待(仮想化技術、グリーン IT、SaaS 等の技術面でのリスク)

B3　業界、業務等の知識不足

・情報技術分野に偏重しているため、審査員の業務区分の拡充を希望

・企業個々の状況（規模、業種等）に合った審査を希望
・受審組織の業務への認識が不足

B4　審査員間のばらつき
・力量のばらつき
・ISMS の要求事項及び管理策に関する見解の濃淡
・審査の深さ、広さの違い
・審査の基準、評価のばらつき

B5　効果的審査をする力量不足
・ISMS が経営に役立つツールとして機能しているかの観点からの審査を希望
・業務が有効に機能しているかの観点での審査を希望
・管理策の実施状況や問題点等（有効性）を中心とした審査を希望
・規格との整合性にばかり拘る審査員がいる

B6　その他
・慢性的な企業体質の改善のきっかけになるよう、時には辛辣な指摘を希望
・事故のない状況を作り出すため、検出事項は厳しく指摘してほしい

C　審査の方法
この分類項目は、審査員個人の方針に関わると思われる審査の方法に関するものである。回答例を以下に示す。
・事前の調査やヒアリングシート等により効率的な審査をしてほしい
・指摘事項（観察事項）の改善内容を定期審査で確認してほしい
・管理策の有効性を現場で見てほしい
・審査を徐々に厳しくしてほしい
・審査スケジュール調整を早めに、フレキシブルにしてほしい
・受審側の規模、実態に合わせた審査日数、時間としてほしい

D　認証機関の方針
この分類項目は、認証機関の方針によると思われるものでC以外のものである。回答例を以下に示す。
・同じ審査員による継続的な審査を希望
・QMS、EMS 等との複数認証における統合審査の実施
・サンプリングロジックの説明
・外部へ公開可能な報告書の作成

Ｅ　審査工数、費用

ほとんどが審査時間の短縮、審査費用の低減に関する要望であったが、審査日程を長くしてじっくり審査してほしいとの要望も若干あった。

Ｚ　その他

満足している旨の回答がかなりあった。その他アンケート調査に関する回答、意図が把握できなかった回答などがここに含まれる。

制度全般に対するご意見等

質問１２　海外のパートナーとの制度の活用

事業活動を海外展開している組織に対して、海外のパートナーとの制度の活用状況に関する調査結果を記す。

(1)海外のパートナーから ISMS 認証の取得を確認されたり、貴組織が ISMS 認証を取得していることをプラスに評価されたことがありますかとの質問に対して、「1 確認され、プラス評価されたことがある」「2 確認されたことがあるが、プラス評価されたことはない」「3 確認されたことはない」の３つの選択肢に答えていただいた結果、項目の回答比率は、「3 確認されたことはない」(68.3%)、「1 確認され、プラス評価されたことがある」(20.8%)、「2 確認されたことがあるが、プラス評価されたことはない」(10.8%)の順となった（図 12-1)。

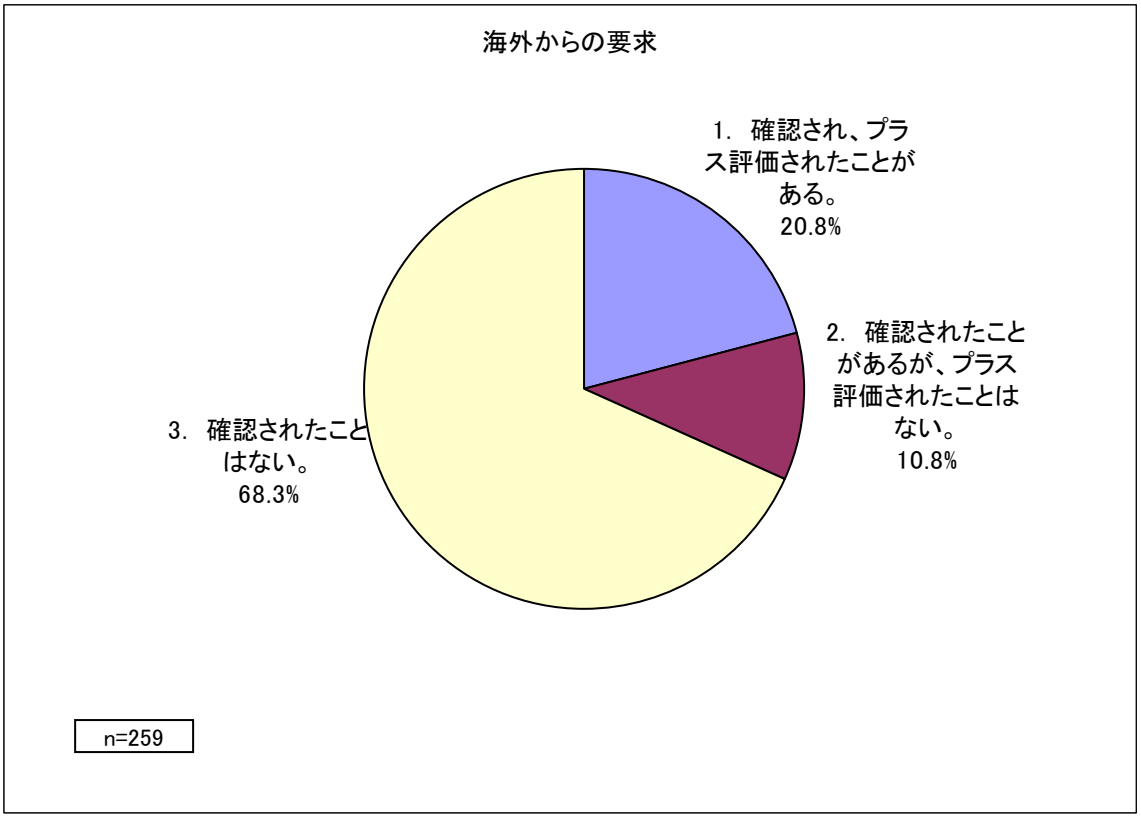


図 12-1　海外のパートナーとの制度の活用（海外からの要求）

(2) 海外のパートナーに ISMS 認証の取得を要求したり、海外のパートナーが ISMS 認証を取得する必要性を感じたりしていますかとの質問に対して、「1 要求している」「2 要求していないが、必要性を感じている」「3 要求していないし、必要性も感じていない」の３つの選択肢に答えていただいた結果、項目の回答比率は、「2 要求していないが、必要性を感じている」(58.1%)、「3 要求していないし、必要性も感じていない」(33.7%)、「1 要求している」(8.1%)の順となった（図 12-2)。

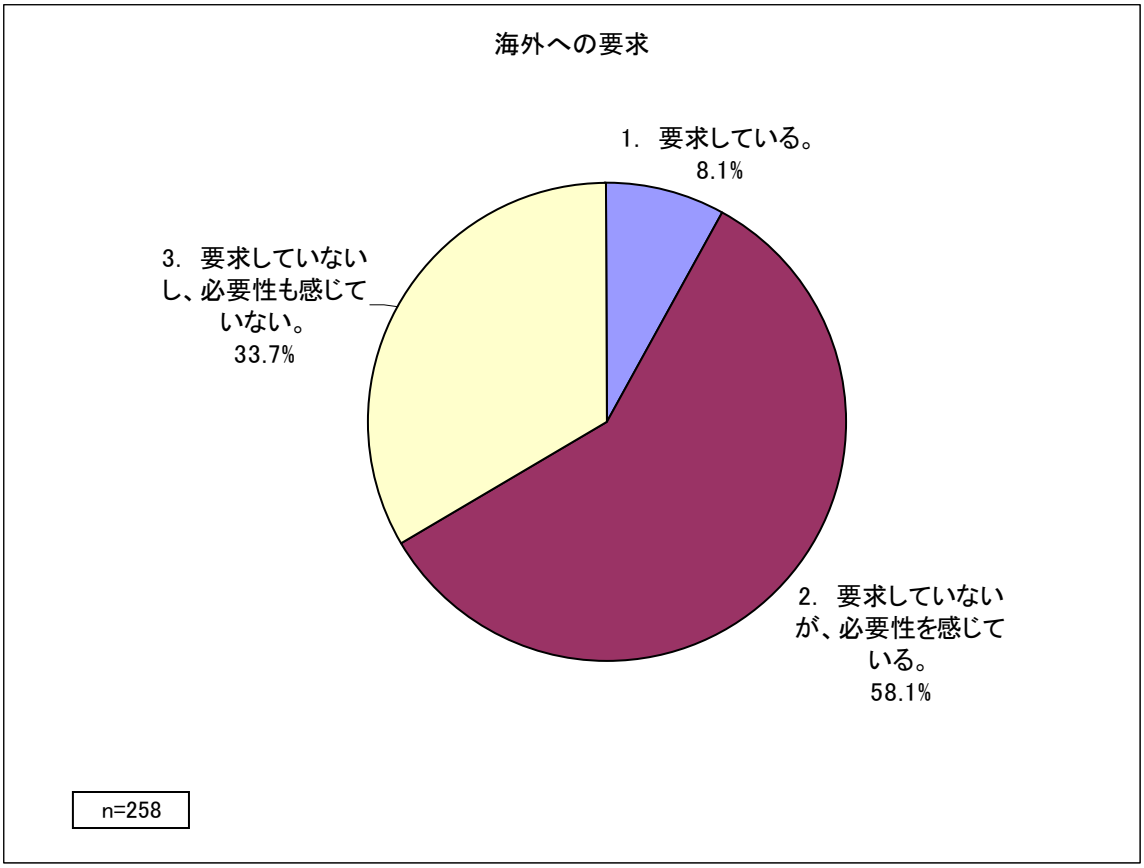


図 12-2　海外のパートナーとの制度の活用（海外への要求）

質問１３　本協会への期待

回答件数は 210 件

回答内容を下記のように分類した結果は図 13 のとおりである。なお、１件の回答に複数の分類項目に該当する内容があれば、各々を分けて分類した。

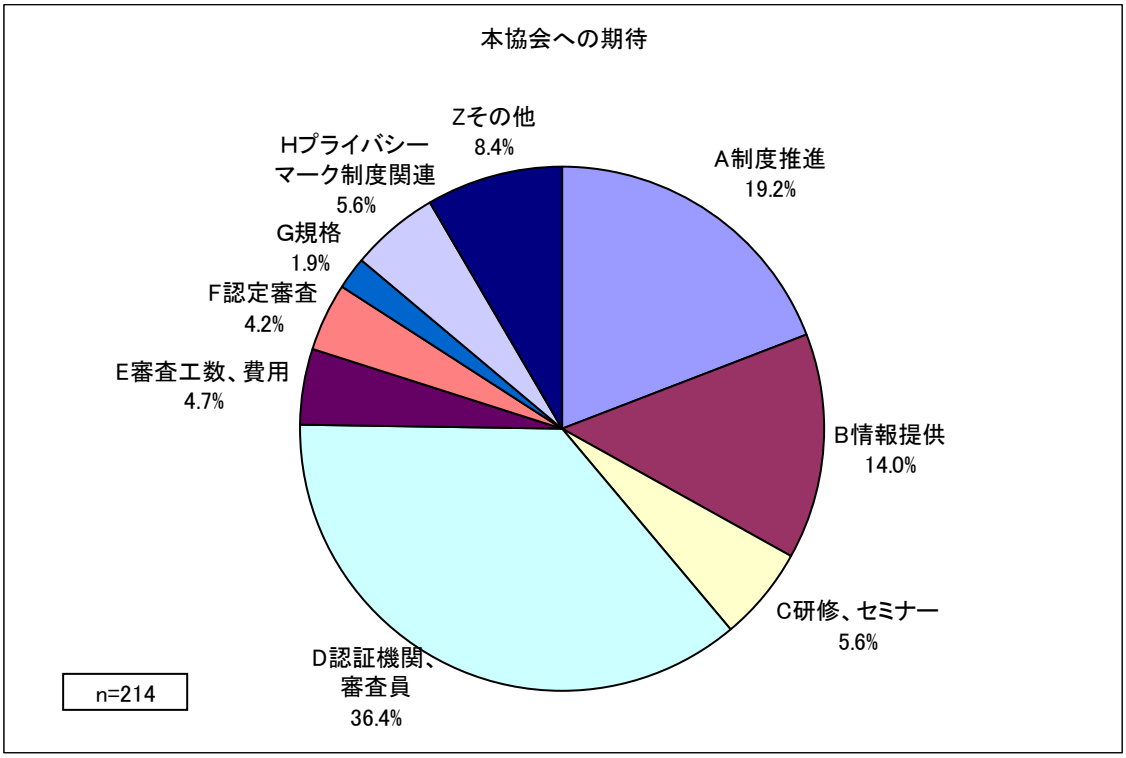


図 13　本協会への期待

分類項目ごとの回答内容の傾向について分析した結果を述べる。

Ａ　制度の認知度改善、制度推進

この分類項目は、制度の広報、普及、運営推進、制度の活用に関するものである。回答例を以下に示す。

・ISMS 認証の意義を社会全体に認識されるような活動を強化していただきたい。
・専門知識がない人でも理解できるよう、規格や管理策の解説をしてほしい。
・情報の重要性のレベル分け及び保護水準の標準化の推進をお願いしたい。
・中小企業向けの運用ガイドラインを作成してほしい。

Ｂ　情報提供

この分類項目は、分類項目Ａの手段としての情報公開に関するものである。回答例を以下に示す。

・情報セキュリティに関する有益な情報を提供し続けて頂きたい。
・認証機関との情報交換の場における、役立つ情報を提供してほしい。

・認証機関を比較検討するための情報をより充実していただきたい。
・認証取得組織による世間で話題になった不祥事について、事後の対応を公開してほしい。

C　研修、セミナー

この分類項目は、研修、セミナーの実施に関するものである。要望のあったテーマの例を以下に示す。

・ISO/IEC 27001 に関するセミナーで、例えば内部監査人のスキルアップ、是正・予防処置の演習など
・最近のセキュリティに関する各種動向の定期的な教育、指導
・認証取得している情報セキュリティに取り組む他社情報の交流や、スキルアップのためのセミナー
・認証取得組織に対する定期的な研修会で、他社におけるリスク対応の事例などの聴講

D　認証機関、審査員

この分類項目は、審査員の力量、認証機関の能力、方針、営業活動に関するものである。回答例を以下に示す。なお、審査員の力量に関するものは、質問１１の回答に関する分類項目Ｂと重複、類似するものが多いので回答例は省略する。

・審査員のみならず、認証機関によっても要求事項の解釈が違っている場合がある。少しでも足並みがそろうような活動を期待する。
・認証機関の審査レベルの差をなくす取り組みに期待する。
・認証機関を変更しても、認証取得日が更新されないようにしてほしい。
・最近、認証機関による「認証機関乗り換え」営業が多くある。認証という性格上、営業競争はなじまないと思う。何らかの指導が必要と思う。

E　認証審査工数、費用

この分類項目では、審査費用、登録・維持費用の低減に関する要望が多かった。

F　認定審査

この分類項目での回答例を以下に示す。

・認証機関の審査員の教育が定期的に行われ、審査員の能力向上が図られているかを確認してほしい。
・認証機関の数が多くなり過ぎて質が低下するようなことがないよう、慎重な認定を期待する。

G　規格

この分類項目は、規格、基準の制定、改訂に関するものである。

・業界別の認証基準を作成してほしい。
・現在、審査は毎年行うことになっているが、内部監査を毎年確実に行っていることにより、審査間隔をもう少し広げてもよいのではないか(例えば２年ごと)。

H　プライバシーマーク制度との関連

この分類項目での回答例を以下に示す。
・プライバシーマーク制度との統合審査
・プライバシーマークとダブルで規格を運用しているが、審査員の質、指摘内容に差がある。それらの統一、平準化に向けて改善してほしい。
・ISMS とプライバシーマークを認証取得しているが、用語、解釈が違う場合があり、併用運用構築に手間がかかった。できれば、両規格の共用性を高めてほしい。

Z　その他

満足している旨の回答、意図が把握できなかった回答などである。

質問１４　制度全般に対するご意見・ご要望

回答件数は 232 件

回答内容を質問１３と同じ分類項目で分類した結果は図 14 のとおりである。なお、１件の回答に複数の分類項目に該当する内容があれば、各々を分けて分類した。

質問１３及び質問１４の回答について、分類項目ごとの構成比を比較した結果、質問１３に対して質問１４は、分類項目Ａで大きく増加し、分類項目Ｄでは逆に大きく減少していることが分かる。質問１３及び質問１４の個々の回答内容に関しては、重複、類似したものが相当数あった。

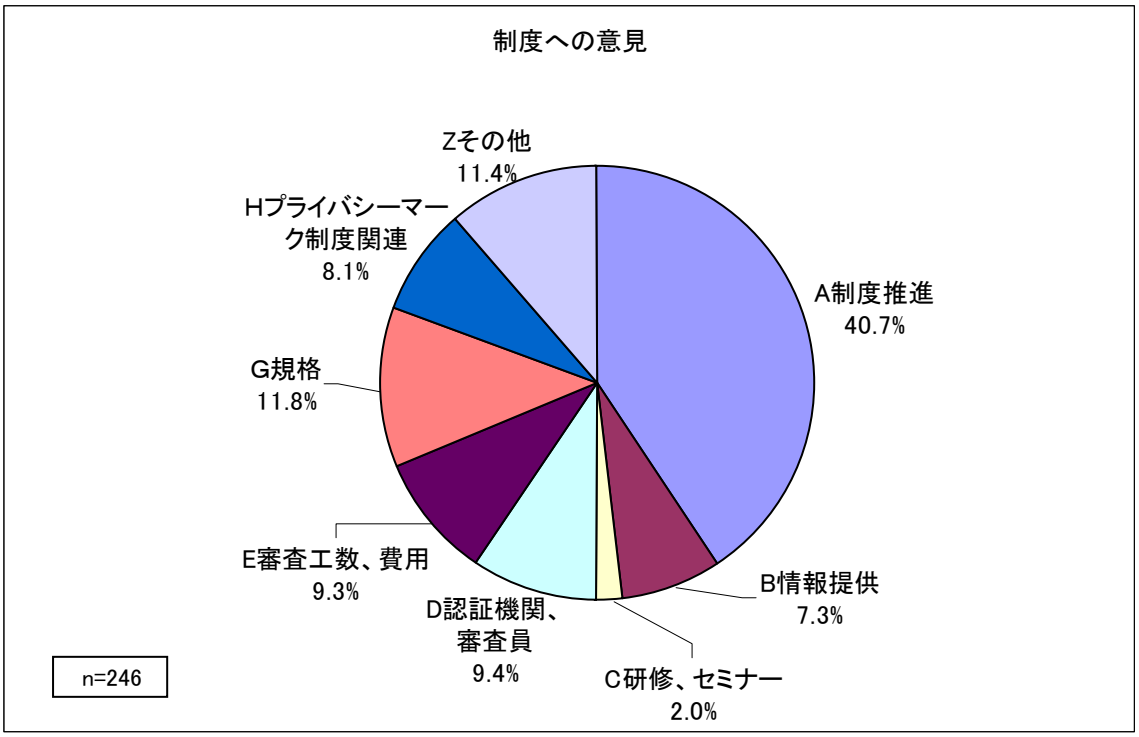


図 14　制度全般に対するご意見・ご要望

分類項目ごとの回答内容の傾向について分析した結果を述べる。

Ａ　制度の認知度改善、制度推進

ISMS 制度の認知度向上の要望が、分類項目Ａ全体の 36%を占めている。

ガイドラインや解説書の作成に関する要望も多く、その内容として次のようなものがある。

・業種や事業規模別のリスク分析についてのシンプルなガイドライン
・管理策の分解能と有効性評価測定について、セキュリティの時代の変化に沿った指導、解説
・リスク受容についての最低レベルの基準

このほか、制度の活用として ISMS 認証と入札取引条件の関連付け、他のマネジメントシステムとの整合性向上の要望などがあった。

Ｂ　情報提供

質問１３の場合と同様、ISMS に関する有益な情報を、他社事例や最新の規格の動向などを含めて情報公開する要望が多かった。

経済産業省の「マネジメントシステム規格認証制度の信頼性確保のためのガイドライン」に対する、本協会としての取り組み、方向性を提示の要請もあった。

Ｃ　研修、セミナー

回答内容は、質問１３と類似していた。

Ｄ　認証機関、審査員

回答内容は、質問１３と重複、類似が多かったが、それらを除いた以下の回答例を以下に示す。

・認証サイクルの基点（有効期限）が、初回審査の判定日でなく更新審査後の再認証の判定日となるため、審査時期が前へ少しずつずれて来るのが不都合になっている。

・ISO/IEC 27004 のガイドラインにあるとおり、審査方法も人によるチェック中心からの脱却を望む。

Ｅ　認証審査工数、費用

質問１３の場合と同様、審査費用、登録・維持費用の低減に関する要望が多かった。

Ｇ　規格

回答内容は、規格の日本語が分かりにくいという意見が多く、この分類項目の大半を占めた。他に、規格の要求事項の中に、技術的に古いものがあるとの内容の指摘が複数件あった。

Ｈ　プライバシーマーク制度との関連

質問１３の場合と同様、ISMS 制度とプライバシーマーク制度との調和、統合を求める意見が多かった。

Ｚ　その他

満足している旨の回答、意味不明の回答などのほかに、今回のアンケート調査に関する意見、要望が数件あった。

おわりに

ISMS 制度のユーザーである組織と本協会とが直接情報交換する機会は、制度の説明会、セミナーなどの制度の普及、広報活動の場や、Web による情報提供、Q&A に限られていましたが、今回、アンケート調査により、数多くの組織から生の声を聞くことができ、大変有意義な結果を得られました。

ISMS 制度は、QMS、EMS などに比べると歴史が浅く、認証を取得して間もない組織が多い。組織のマネジメントシステムと同様、制度自体も発展途上にあります。このことがアンケート調査結果に反映されており、組織のマネジメントシステムを改善するための具体策に尽力されていることがうかがえ、これが審査や制度推進に対する具体的な要望となって表現されています。

また、マネジメントシステムを構成する人的側面の重要性を認識されており、これが人材育成、教育を今後の主な課題としている組織が多いことで示されています。

一方、技術的な側面に関しての具体的な課題も多く、組織にとって役に立つ情報を提供することが求められています。

ISMS は、将来起こり得るリスクに備えるための仕組みであり、日常の事業活動のアウトプットに必ずしも直結しないため、費用対効果を説明しにくいという特質がありますが、これが、経営者の ISMS に対する投資を消極的にさせる要因の一つになっているものと思われ、今回の調査でも、審査、登録、維持に対する費用の低減を求める意見が多く見られました。

ISMS 制度を運用する側の認定機関、認証機関の役割は、審査の信頼性を高め、組織の ISMS の価値を高めることにあります。このためにも、今回のアンケート調査結果を最大限に活用させていただく所存です。

本報告書は、本制度に関する様々な立場の関係者に読んでいただき、各々の立場で課題の解決に尽力されることを願いまして結びとします。

付録　ISMS 適合性評価制度に関するアンケート調査書

次頁以降は、今回使用したアンケート調査書の内容です。

ISMS 適合性評価制度に関するアンケート調査書

はじめに

アンケート調査に回答いただく前に、下記の回答情報の取扱方針に対して、記入者の同意をいただくことにしております。同意いただける場合は、下記のチェック個所に記入いただき、本ページを含めて返送してください。
本アンケート調査では回答者の所属、氏名、連絡先等の情報を記入いただくことにしております。これらの個人情報を含む回答情報は、財団法人日本情報処理開発協会の個人情報保護方針*に基づいた下記の方針にしたがって利用させていただきます。

注*　http://www.jipdec.or.jp/ov/kojin.pdf

［個人情報管理者］
本アンケート調査業務における個人情報管理者は下記のとおりです。
財団法人 日本情報処理開発協会 情報マネジメント推進センター ISMS 制度推進室長
［個人情報の取扱いについて］
弊センターでは、回答欄に記入いただいた個人情報を、本アンケート調査内容に関するご確認及びアンケート調査結果のご報告のために使用いたします。弊センターは、これらの業務を含むアンケート調査に関わる業務の一部を外部委託いたします。外部委託事業者は、十分な保護水準を満たしており、契約等により適切な処置を講じています。
弊センターが取得した個人情報は、法令等による場合を除いて第三者に提供することはありません。
弊センターが取得した個人情報の安全管理のために、必要かつ適切な措置を講じます。
弊センターが取得した個人情報は、本人からの開示、訂正、削除、利用停止等の要請に対して遅滞なく対応いたします。
［回答内容全体について］
回答情報は、ISMS 適合性評価制度全般の運用状況を把握し、今後同制度を改善するために使用します。貴組織名を特定した回答情報は公開いたしません。
［集計・分析結果について］
回答情報を集計・分析した結果は報告書にまとめ、弊センターの HP で公開いたします。

上記の方針に同意いただけるでしょうか。□内にチェック印を記入してください。

□同意する
□同意しない

同意いただける場合、以下のアンケート調査にご協力ください。

記入要領

質問項目は全部で、14 問です。回答は、該当する番号に○印を付けていただくものと、回答情報を記入していただくものとがあります。

調査書の返送について

調査書は、同封の返信用封筒に入れて、郵送していただくか、又は下記の連絡先に FAX 送信してください。
回答希望期日：２００８年１１月末日までにご回答をお願いいたします。

連絡先

財団法人　日本情報処理開発協会　情報マネジメント推進センター
電話番号：０３（３４３２）９３８６
FAX 番号：０３（３４３２）６２００

質問及び回答

基本情報について

貴法人名及び回答者の所属、氏名、連絡先等について記入してください。

法人名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

回答者

所在地：〒＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

所属、役職：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

氏名：＿＿＿＿＿＿＿＿＿＿＿＿

連絡先：E-Mail＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

TEL＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

質問１　貴法人の業種を、下記の業種区分から選択してください。複数業種に関連する場合は、主力業種１つのみ選択してください。12、21 又は 23 を選択した場合、(　)の中に業種を記入してください。18 を選択した場合、さらに 18-1 から 18-10 から該当するものを１つのみ選択してください。18-10 を選択した場合、(　)の中に業種を記入してください。

1. 食料品･飲料･タバコ等の製造業
2. 衣服･天然素材繊維製品の製造業
3. 木材･木製品･パルプ･紙等の製造業
4. 出版･印刷業
5. 化学薬品･化学製品(化学繊維を含む)･医薬品の製造業
6. 石油･石炭･ゴム･プラスチック等の製造業
7. ガラス･セラミック･コンクリートの製造業
8. 鉄鋼･非鉄金属業･金属製品の製造業
9. 機械･機器の製造業
10. 電気/電子機器･光学的装置製造業
11. 輸送機器製造業
12. その他の製造業（＿＿＿＿＿＿＿＿）
13. 建設業(エンジニアリングを含む)
14. 廃棄物処理業･再生業
15. 電力･ガス･熱･水道供給業
16. 卸売･小売業
17. 金融･保険･不動産業

18. 情報技術
    18-1 通信業
    18-2 放送業
    18-3 システムインテグレーション業
    18-4 受注ソフトウェア業
    18-5 ソフトウェアプロダクト業
    18-6 計算事務等情報処理業
    18-7 システム等管理運営受託業
    18-8 データベースサービス業
    18-9 インターネット附随サービス業
    18-10 映像・音声・文字情報制作業
    18-11 その他（＿＿＿＿＿＿＿＿＿＿）
19. ホテル･レストラン業
20. 医療関係
21. その他サービス業（＿＿＿＿＿＿＿＿＿＿）
22. 公共･行政･教育機関
23. 分類不明（＿＿＿＿＿＿＿＿＿＿）

質問２　貴法人が株式会社の場合、貴法人の資本金について、下記のうち該当するものを選択してください。

1. 5000 万円以下
2. 5000 万円超、1 億円以下
3. 1 億円超、3 億円以下
4. 3 億円超

質問３　貴法人が常時使用する従業員の数について、下記のうち該当するものを選択してください。

1. 5 人以下
2. 5 人超、20 人以下
3. 20 人超、50 人以下
4. 50 人超、100 人以下
5. 100 人超、300 人以下
6. 300 人超

質問４　認証範囲の従業員数を概数でお答えください。

約（＿＿＿）人

ISMS 認証の運用実績等について

質問５　貴組織が ISMS 認証を取得してから現在までの経過年数及び認証登録番号をお答えください。

経過年数（＿＿年＿＿か月）　　認証登録番号（＿＿＿＿＿＿）

質問６　ISMS 導入の目的又は動機について、下記の各項目が該当するか否かをお答えください。

No.	項　　目	該当する	やや該当する	余り該当しない	該当しない
1	組織の情報セキュリティ管理体制の強化のため	1	2	3	4
2	組織の情報セキュリティ対策の強化のため	1	2	3	4
3	社員の情報セキュリティに関する意識高揚、教育啓発のため	1	2	3	4
4	入札、受注の条件、取引先からの要請による	1	2	3	4
5	顧客の信頼性確保のため	1	2	3	4
6	企業イメージの向上のため	1	2	3	4
7	同業他社との差別化、営業上の優位性の確保のため	1	2	3	4
8	全社の方針による	1	2	3	4

上記 1～8 以外に、目的又は動機として意識している事項がありましたら、記入してください。

質問７　ISMS 導入の効果について、下記の各項目が該当するか否かをお答えください。

No.	項　　目	該当する	やや該当する	余り該当しない	該当しない
1	組織の情報セキュリティ管理体制が強化できた	1	2	3	4
2	組織の情報セキュリティ対策が強化できた	1	2	3	4
3	社員の情報セキュリティに関する意識高揚、教育啓発に寄与した	1	2	3	4
4	顧客の信頼性確保に貢献した	1	2	3	4
5	企業イメージの向上に貢献した	1	2	3	4
6	営業上、同業他社に対する優位性の確保に貢献した	1	2	3	4
7	IT 統制、J-SOX 法対応に有効であった	1	2	3	4
8	情報面での事業継続性の向上に有効であった	1	2	3	4

上記 1～8 以外に、効果として特記すべき事項がありましたら、記入してください。

質問８　貴組織の ISMS に関する今後の主な課題について、差し支えない範囲で記入してください。

審査員の力量及び審査の質について

質問９　最近受審された ISMS 認証審査において、審査員の力量を下記の観点で評価してください。

No.	項　　　目	十分である	概ね十分である	やや不十分である	不十分である
1	マネジメントシステムに関する知識及び業務経験	1	2	3	4
2	情報システム、情報セキュリティに関する知識及び業務経験	1	2	3	4
3	受審組織の業務に対する理解	1	2	3	4
4	コミュニケーション能力	1	2	3	4
5	審査技術	1	2	3	4
6	改善課題を指摘する能力	1	2	3	4

質問１０　最近受審された ISMS 認証審査の質を下記の観点で評価してください。

［審査の内容］

(1)-a　マネジメントプロセス、マネジメント文書の規格適合性に関する審査内容を、下記の４段階で評価してください。３又は４を選択された場合は、不満な点を簡潔に記入してください。

1. 満足
2. やや満足
3. やや不満＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
   ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
4. 不満＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
   ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

(1)-b　管理策に関する審査内容を、下記の４段階で評価してください。３又は４を選択された場合は、不満な点を簡潔に記入してください。

1. 満足
2. やや満足
3. やや不満＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
   ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
4. 不満＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
   ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

［審査の時間］

(2)　組織の ISMS の有効性を含む実施状況の評価に関する審査時間を、審査の信頼性の観点から、下記の項目で評価してください。

1. 適切
2. 長い
3. 短い
4. 何とも言えない

［審査の所見・指摘］

(3)　審査所見・指摘の、マネジメントプロセス、マネジメント文書、管理策、及びそれらの運用を改善するうえでの有効性を、下記の４段階で評価してください。３又は４を選択された場合は、役立たなかった点を簡潔に記入してください。

1. 大いに役立った
2. 役立った
3. あまり役立たなかった＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

   ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
4. 役立たなかった＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

   ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

［審査に対する総合評価］

(4)　総合的に見た審査の質を、下記の４段階で総合評価してください。３又は４を選択された場合は、不満な点を簡潔に記入してください。

1. 満足
2. やや満足
3. やや不満＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

   ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
4. 不満＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

   ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

質問１１　今後の認証審査及び審査員に対して、ご意見、ご要望等がございましたら、記入してください。

制度全般に対するご意見等

質問１２　貴組織が事業活動を海外展開されている場合のみ、ご回答ください。

(1)　海外のパートナーから ISMS 認証の取得を確認されたり、貴組織が ISMS 認証を取得していることをプラスに評価されたことがありますか。

1. 確認され、プラス評価されたことがある。
2. 確認されたことがあるが、プラス評価されたことはない。
3. 確認されたことはない。

(2)　海外のパートナーに ISMS 認証の取得を要求したり、海外のパートナーが ISMS 認証を取得する必要性を感じたりしていますか。

1. 要求している。
2. 要求していないが、必要性を感じている。
3. 要求していないし、必要性も感じていない。

質問１３　認定機関として、認証機関を認定する立場にある弊センターに期待することがございましたら、記入してください。

質問１４　ISMS 適合性評価制度全般に対して、ご意見、ご要望等がございましたら、記入してください。

以上

アンケートにご協力いただき、ありがとうございました。