# ISMS 適合性評価制度に関する
# 調査報告書

2018 年 3 月

情報マネジメントシステム認定センター（ISMS-AC）

目次

## はじめに

このたびは、ご多忙の中、ISMS適合性評価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。

2002年に本制度の本格運用を開始してから約15年になります。その間、弊センターはISMSの認定機関として、わが国の情報セキュリティ全体の向上に貢献するとともに、諸外国からも信頼を得られる情報セキュリティレベルを達成することを目的として、認証機関の認定及びISMSの普及啓発活動を実施してまいりました。おかげさまで3月現在、認証取得組織数は約5,500件となり、なお着実に増加しております。

皆様方におかれましては、昨今のクラウド、IoT等の新たなIT技術の急激な普及やサイバー攻撃等の高度化する脅威に直面する中、ISMSの構築、運用、維持及び改善に多大なご尽力を続けられておられますこと、深く感謝申しあげます。

このたび、前回調査から3年が経過し、認証取得組織数も5000件を超えたことから、ISMS認証を取得されている組織様を対象としたアンケート調査を再度実施することに致しました。今回のアンケートの目的は、近年の新たな脅威への対応も含むISMSの有効性を検証するとともに制度の改善点・運用状況を把握することであり、それに基づいて今後も皆様にとってなお一層有効で、活用度の高い制度にしていく所存です。

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。皆様方からお寄せいただいた有益な情報をもとに、ISMS導入の有効性を検証するとともに課題点を確認し、更なる制度の充実と改善に取り組んでまいりたいと存じます。

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。

2018年3月

情報マネジメントシステム認定センター

## 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。

・基本情報について

・ISMS認証の実績等について

・ISMSの導入及び認証取得の効果等について

・審査員の力量及び審査の質について

・認証機関の認定の信頼性について

・制度全般に対するご意見等

調査対象

調査開始の2018年1月時点で、本センターが認定した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5,130組織。

調査方法

郵送でアンケートの案内をし、WEB上から質問（選択形式及び記述形式）に回答していただく。

調査期間

2018年1月10日～1月29日

| | | |
|---|---|---|
| 有効回答数 | : | 1,180 |
| 回答率 | : | 23.0% |

## 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」（58.2%）が突出しており、以下「その他サービス業」（16.8%）、「建設業(エンジニアリングを含む)」（4.2%）、「卸売･小売業」（3.8%）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されたい。

| 業種区分 | 組織 | (%) | 業種区分 | 組織 | (%) |
|---|---|---|---|---|---|
| 1 食料品･飲料･タバコ等の製造業 | 1 | 0.1 | 13 建設業(エンジニアリングを含む) | 50 | 4.2 |
| 2 衣服･天然素材繊維製品の製造業 | 0 | 0.0 | 14 廃棄物処理業･再生業 | 11 | 0.9 |
| 3 木材･木製品･パルプ･紙等の製造業 | 3 | 0.3 | 15 電力･ガス･熱･水道供給業 | 2 | 0.2 |
| 4 出版･印刷業 | 28 | 2.4 | 16 卸売･小売業 | 45 | 3.8 |
| 5 化学薬品･化学製品(化学繊維を含む)･医薬品の製造業 | 4 | 0.3 | 17 金融･保険･不動産業 | 16 | 1.4 |
| 6 石油･石炭･ゴム･プラスチック等の製造業 | 2 | 0.2 | 18 情報技術 | 687 | 58.2 |
| 7 ガラス･セラミック･コンクリートの製造業 | 0 | 0.0 | 19 ホテル･レストラン業 | 1 | 0.1 |
| 8 鉄鋼･非鉄金属業･金属製品の製造業 | 4 | 0.3 | 20 医療関係 | 18 | 1.5 |
| 9 機械･機器の製造業 | 11 | 0.9 | 21 その他サービス業 | 198 | 16.8 |
| 10 電気/電子機器･光学的装置製造業 | 37 | 3.1 | 22 公共･行政･教育機関 | 12 | 1.0 |
| 11 輸送機器製造業 | 2 | 0.2 | 23 分類不明 | 32 | 2.7 |
| 12 その他の製造業 | 16 | 1.4 | 合計 | 1180 | |

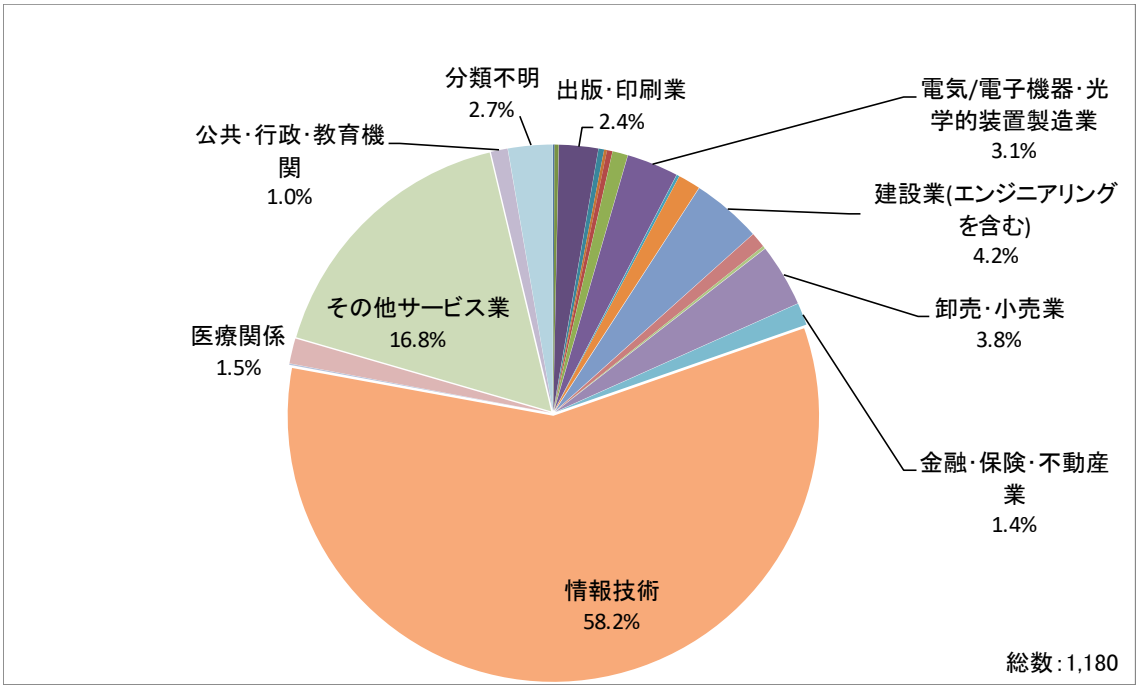
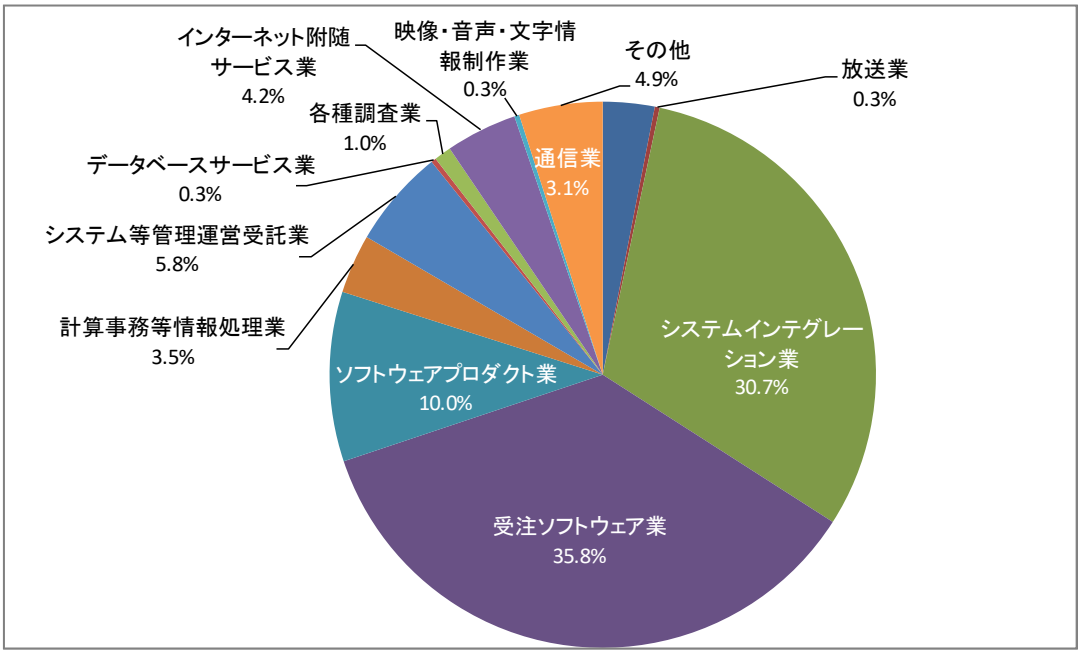



**図1-1 法人の業種**

「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」(35.8%)、「システムインテグレーション業」(30.7%)で過半数を占め、以下「ソフトウェアプロダクト業」（10.0%）、「システム等管理運営受託業」(5.8%)の順となっている（図1-2）。

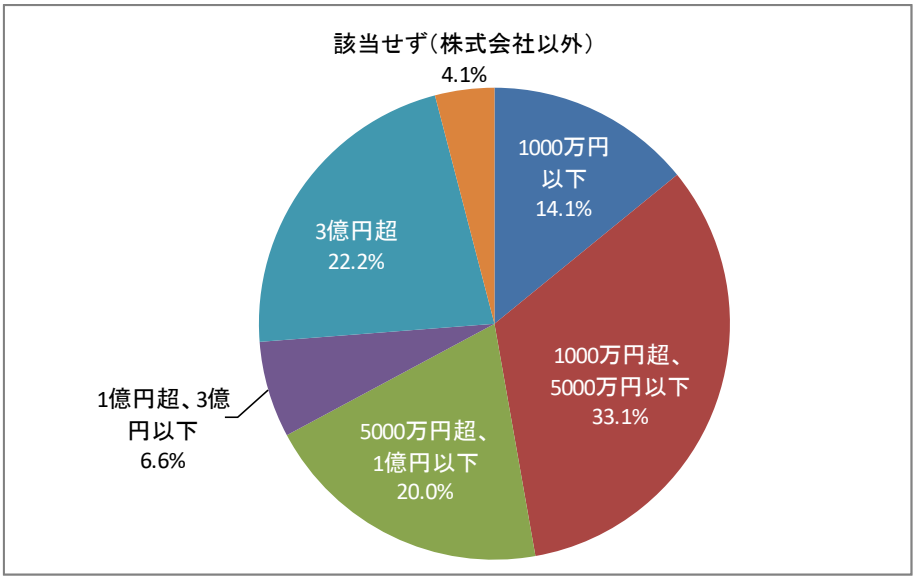



総数：687

**図1-2 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、「1000万超、5000万円以下」(33.1%)が最も多く、対極の「3億円超」(22.2%)で続き、以下「5000万円超、1億円以下」(20.0%)、「1000万円以下」(14.1%)、「1億円超、3億円以下」(6.6%)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されたい。

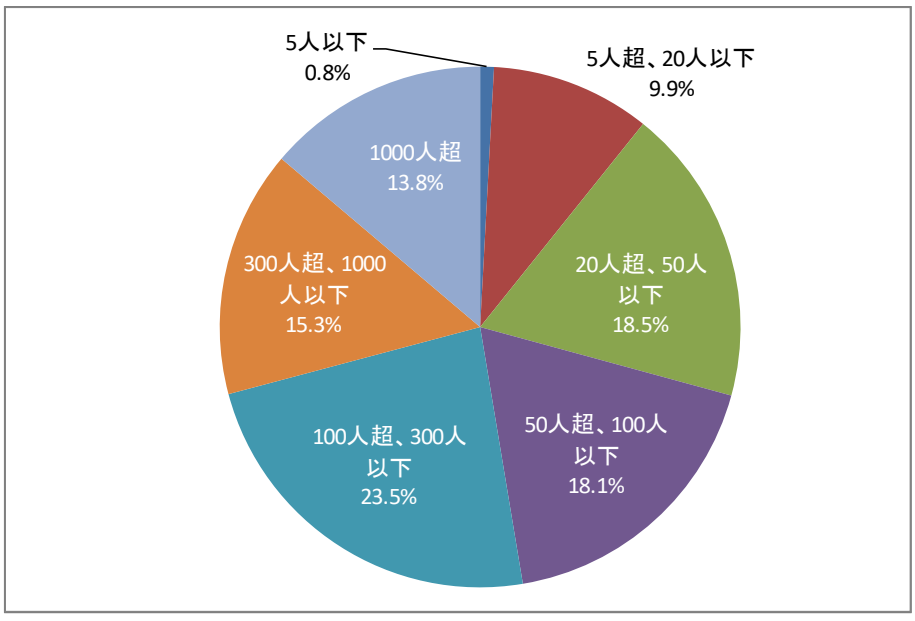



総数:1,180

**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、「100人超、300人以下」(23.5%)が最も多く、「20人超、50 人以下」(18.5%)、「50人超、100人以下」（18.1%）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されたい。




総数:1,180

**図3 従業員数**

### 質問4 ISMS取得の認証範囲について

認証範囲の従業員数について、全社からみた割合について尋ねた結果を分類したところ、下記の結果が得られた。

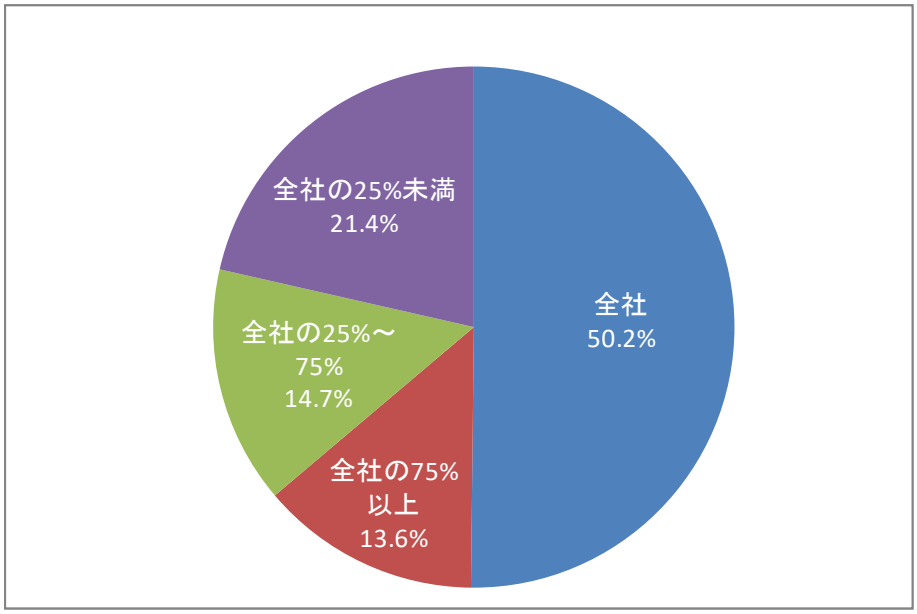



**図4　　ISMS取得の認証範囲について**　　総数：1,180

| 有効回答数=1,180 | 件数 | (%) |
|---|---|---|
| 1　全社 | 592 | 50.2% |
| 2　全社の 75%以上 | 161 | 13.6% |
| 3　全社の 25%～75% | 174 | 14.7% |
| 4　全社の 25%未満 | 253 | 21.4% |

また、認証範囲の従業員について尋ねたところ、「20人超、50人以下」(26.4%)、「5人超、20人以下」(19.9%)、「100人超、300人以下」（19.5%）、「50人超、100人以下」（19.1%）の順となった。

| 有効回答数=1,180 | 件数 | (%) |
|---|---|---|
| 1　5 人以下 | 25 | 2.1% |
| 2　5 人超、20 人以下 | 235 | 19.9% |
| 3　20 人超、50 人以下 | 311 | 26.4% |
| 4　50 人超、100 人以下 | 225 | 19.1% |
| 5　100 人超、300 人以下 | 230 | 19.5% |
| 6　300 人超、1000 人以下 | 114 | 9.7% |
| 7　1000 人超 | 40 | 3.4% |

**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１０年以下」、「１０年超」の５段階に分類して度数を調べた。その結果、「５年超１０年以下」(33.7%）、「１０年超」(31.6%)、「１年超３年以下」(16.3%)の順となった（図5）。

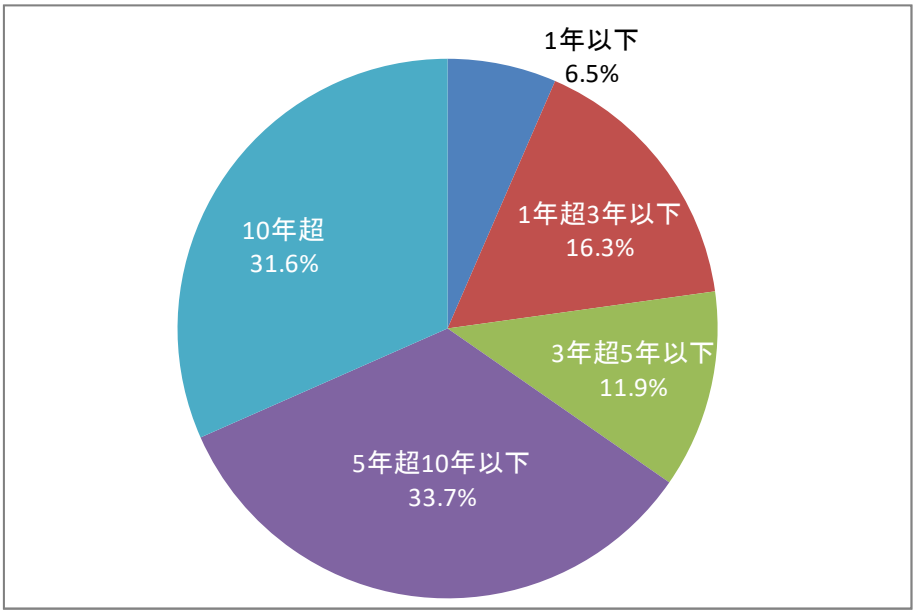


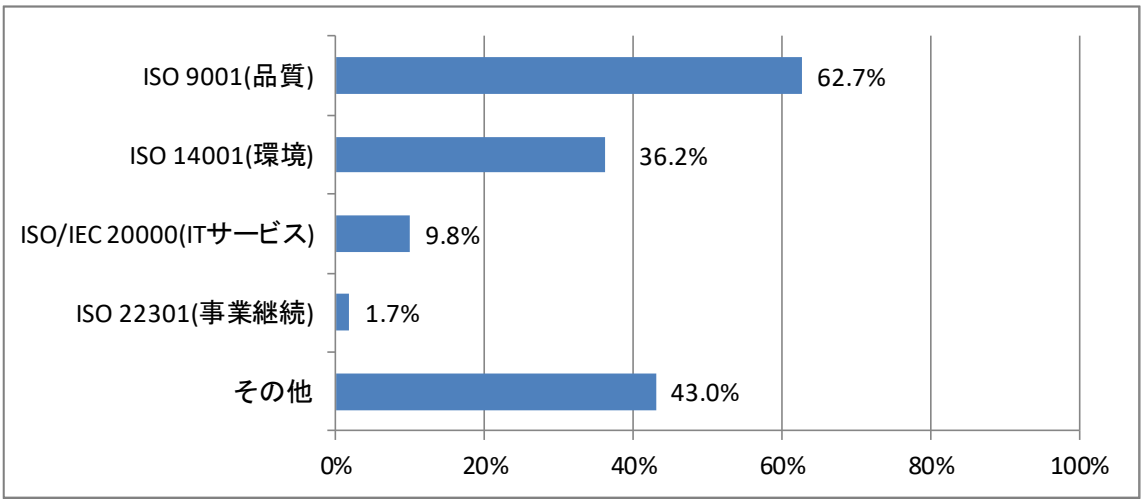

**図5 経過年数**

総数:1,180

### 質問6 他のマネジメントシステム認証

ISMS認証取得以外にどのようなマネジメント認証取得をしているかを尋ねた結果を、「ISO 9001（品 質）」、「ISO 14001（環境）」、「ISO/IEC 20000（ITサービス）」、「ISO 22301（事業継続）」、「その他」に分類して調べた。その結果、「ISO 9001（品質）」（62.7%）、「ISO 14001（環境）」(36.2%)、「ISO/IEC 20000（ITサービス）」(9.8%)、「ISO 22301（事業継続）」（1.7%）の順となった（図6）。

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されたい。

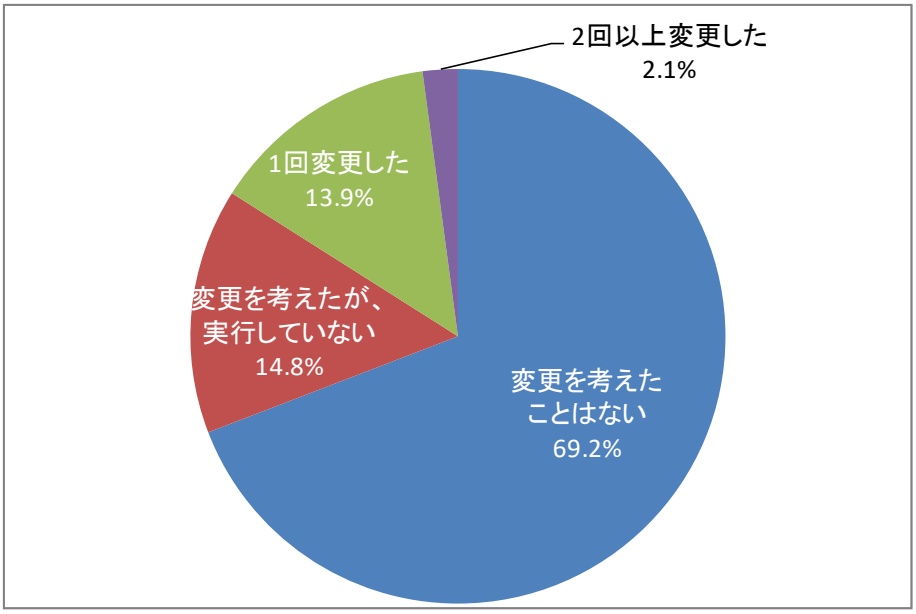



総数:630

**図6 他のマネジメントシステム認証**

### 質問7 認証機関の変更

ISMS認証取得後から現在に至るまでに、認証機関（審査機関）を変更した、または検討したことを尋ねた結果を、「変更を考えたことはない」、「変更を考えたが、実行していない」、「1回変更した」、「2回以上変更した」に分類して度数を調べた。その結果、「変更を考えたことはない」（69.2%）、「変更を考えたが、実行していない」(14.8%)、「1回変更した」(13.9%)、「2回以上変更した」（2.1%）の順となった（図7）。




総数:1,180

**図7　　認証機関の変更**

また、上記で「変更を考えたが、実行していない」、「1回変更した」、「2回以上変更した」と回答した364組織に対して、その理由として最もあてはまるものを回答してもらった結果、以下のように、「審査料金の比較」とした組織が62.9%を占めた。

| 有効回答数=364 | | 件数 | (%) |
|---|---|---|---|
| 1 | 審査内容（深さや指摘内容等）が不満 | 48 | 13.2 |
| 2 | 認証機関のサービス（情報提供等）や対応（手続き等）に不満 | 26 | 7.1 |
| 3 | 審査料金の比較 | 229 | 62.9 |
| 4 | その他 | 61 | 16.8 |

ISMSの導入及び認証取得の効果等について

## 質問8 導入の目的又は動機

ISMS導入の目的又は動機について、１１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8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「5. 顧客からの信頼を確保するため」(81.0%)、僅差で「2. 組織の情報セキュリティ対策の強化のため」(80.8%)、「1. 組織の情報セキュリティ管理体制の強化のため」(80.4%)が続く。一方、「該当する」の回答が最も少ないものは「11. 新しい脅威に対応するため」(41.7%)であった。

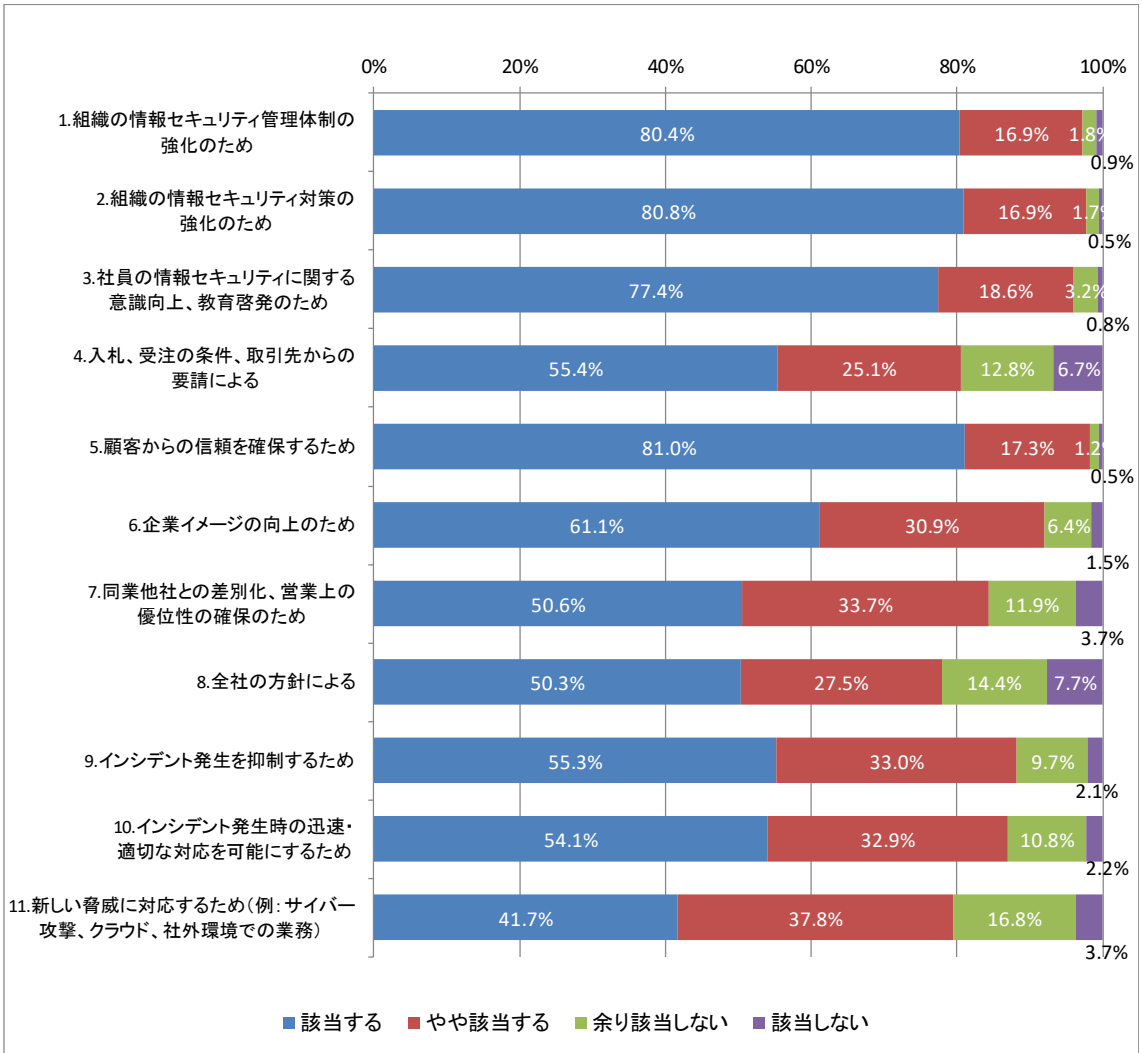



**図8 導入の目的又は動機**

総数:1,180

項目No.1から項目No.11以外の導入の目的又は動機のうち幾つかの事項を以下に記す。

・お客様情報の情報漏洩事件・事故を起こさないため。
・セキュリティ強化を契機にITの統制の整備を促進するため。
・従業員に対するマネジメントの一環としてISMSの運用を利用。
・情報セキュリティ技術を弊社の成長戦略の一つのアイテムと考えているため。
・審査機関による組織の情報セキュリティチェック及び改善アドバイスを受けるため。

## 質問9 ISMS導入の効果

ISMS導入の効果について、15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9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「3. 社員の情報セキュリティに関する意識向上、教育啓発に寄与した」（71.8%）、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」(70.6%)、「2. 組織の情報セキュリティ対策が強化できた」(69.3%)が続き、次いで「4.顧客からの信頼確保に貢献した」(56.4%)となった。一方、「該当する」の回答が最も少ないものは「15.業務環境の変化（在宅勤務、BYODなど）、適用法令に対応する上で、社内ガバナンスに効果があった」(21.1%)、「14.最新のIT技術動向（例：サイバー攻撃、利用するクラウドサービスの事故）に対応した対策が図れた」(25.0%)となった。

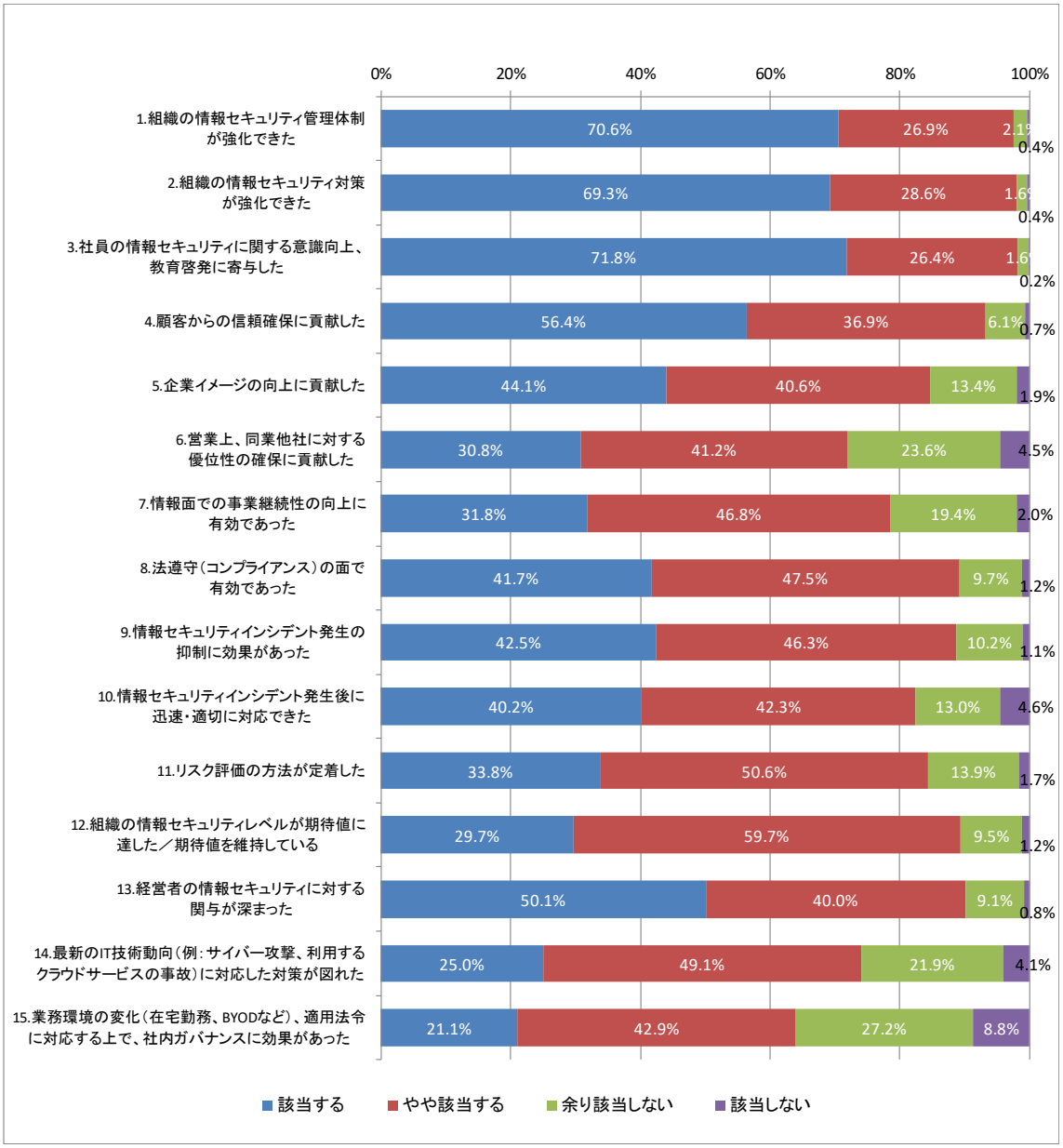



**図9 ISMS導入の効果**　　総数：1,180

上記項目№1～15で1(該当する)を選択した場合、又は№1～15以外に効果として特筆すべき事項がある場合にその具体的な内容や例について尋ねた結果、得られた回答（記述式）の幾つかを以下に記す。

・情報セキュリティを推進する社内体制が確立できた。社員がISMSを意識して顧客情報を取り扱うようになった。顧客からISMS認証を持っていることに対して好印象をもたれた。

・属人的な情報のバラ付き、アプローチの仕方がスタンドプレーが多かった状態から各々担当者をつけることにより情報取扱いが統一管理が適切に行われ始めた。

・ISMS基準で情報資産の取り扱いが定められたことで、 各自が順守する（できる）体制が整った。 また、その行動から意識が変わった。 よって、社内環境と社員意識の良化が当社の大きな変化（効果）であった。

・社員の情報セキュリティへの意識が高まったとともに、コンプライアンス、ガバナンスの意味でも社員全体の意識やモラルが高まった。

・クライアント（官公庁）の信頼性が高くなり、社員の意識向上が大きかった。

・ISMS取得に向けて取り組んだ結果、PC・ネットワーク関係のセキュリティが強化され、ウィルス感染等の被害を水際で防げている。

・パートナー企業のセキュリティの意識も高まった。

・情報セキュリティ犯罪が増加する中で、ある程度の事前防護策の策定・実施に役立っている。

・インシデント発生時の連絡体制を明文化し周知することで、問題発生時に落ち着いて行動することができた。

・情報セキュリティに関する設備投資について承認されやすくなった。

・マネジメントレビューにおけるトップマネジメントからの指摘、指示事項等を通じて、上位方針との連携が強化できている。

### 質問10 顧客からの要求

顧客から、組織の情報管理リスクの把握のため、ISMS認証文書（登録書）の他に要求されたことがあるかを尋ねたところ、図10に示す結果となった。

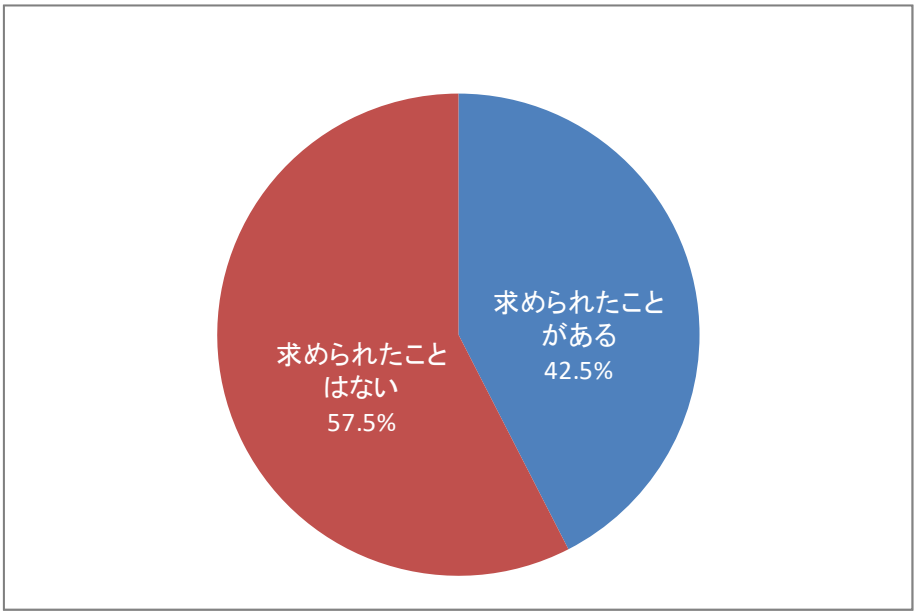



**図10 登録証以外に求められた経験** 総数：1,180

顧客から、組織の情報管理リスクの把握のため、要求された項目の代表的なものは以下のとおり。

| 有効回答数=502 | | 件数 | (%) |
|---|---|---|---|
| 1 | 実査、取引先からのセキュリティ監査 | 294 | 58.6 |
| 2 | 内部／外部監査報告書の開示 | 88 | 17.5 |
| 3 | 適用宣言書の開示 | 34 | 6.8 |
| 4 | セキュリティ対策の取組状況に関するアンケートへの回答 | 371 | 73.9 |
| 5 | その他 | 51 | 10.2 |

## 質問11 ISMSに関する今後の課題

自組織のISMS認証取得、維持に関する今後の主な課題について尋ねたところ、「2.マンネリ化・形骸化」(63.6%)、「6.人材の確保、育成」(57.1%)、「7.組織内の情報セキュリティ教育・意識向上」(52.5%)の順となった（図11）。

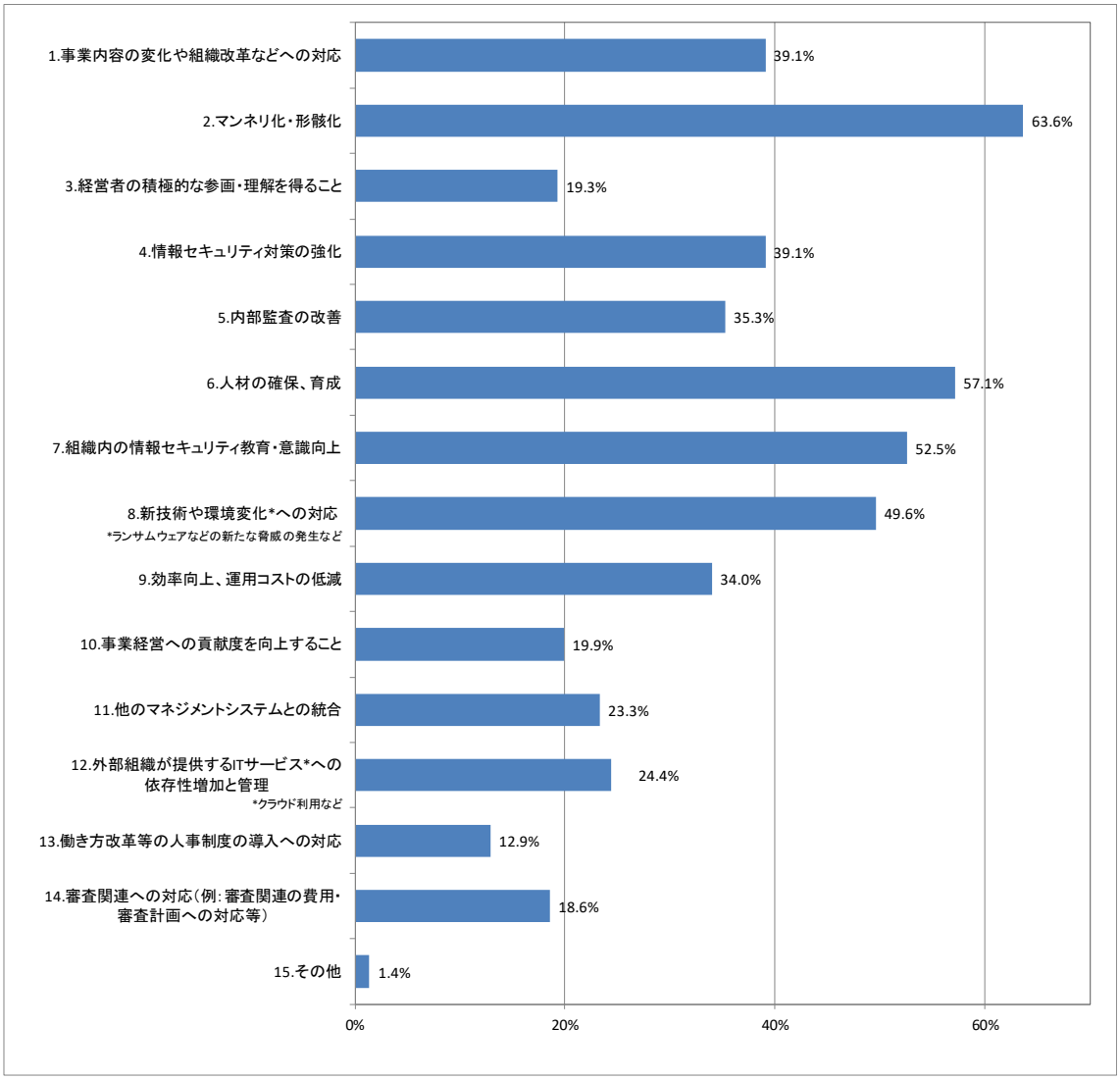



**図11 ISMSに関する今後の課題**　　総数：1,180

各項目ごとの主な内容は次のとおり。

### [1.事業内容の変化や組織改革などへの対応]

主な意見として、事業内容の変化や組織変更・人事異動が多いため、それに合わせたISMS活動範囲の見直し、規定・ルールの改訂、それに伴うシステム対応や要員への周知を迅速に行うことが難しく、工数・費用面からも課題となっているということが多くあげられた。この課題を認識している組織については、回答として経営陣、ISMS運営事務局、情報セキュリティ管理者、情報システム担当などが挙げられた。回答例を次に示す（課題を認識している組織の記載がある場合には、カッコ書きで示す）。

・ISMSの活動単位が組織変更の度に変更となり運用が困難。
・組織改革などで引継が十分行われず、後任が一から勉強しなおす必要がある。
・事業内容の変革とICT技術等の進化に伴って、対応すべきリスク内容が変わってくるが、タイムリーかつ適切に対応しきれていない。
・経営環境、事業内容、組織の変化が激しい中、ルールの改訂や周知が追い付かない。
・ISMS運営事務局 事業内容や組織の変化が速く、現場とのかい離が起きやすい。
・ビジネスの変化や、顧客幅の拡がりへの対応（管理責任者・事務局）。
・全組織で認証していないため、組織変更時の効率的な対応。
・新規事業を始めたときのリスクアセスメントやマニュアル改訂の対応。

**[2.マンネリ化・形骸化]**

ISMS認証を取得してから5年を超える組織が6割を超えている中、ISMSが定着したことでインシデント発生が減少した反面、改善につながりにくくいという意見や、新たなリスクの発見も難しく、マネジメントシステムも固定化、形骸化が進んできているという意見が多かった。また、定着化により、規定・ルール等の本来の目的に対する理解が薄れてきているという意見もあった。

要員の点からは、定期的な教育・訓練によりISMSは定着してきたが、人・時間の不足等により教育内容について刷新が難しくマンネリ化しているという意見、慣れによって要員のセキュリティ意識が薄れてきているという意見などが多くみられた。

この課題を認識している組織としては、ISMS運営事務局・委員会が最も多く、その他、経営陣、情報セキュリティ管理者、情報システム担当などが挙げられた。回答例を次に示す（課題を認識している組織の記載がある場合には、カッコ書きで示す）。

・ISMSが定着したことでインシデントが抑制された反面、緊張感が薄れている。
・やることが当たり前になりインシデントも減ったが、経験しないことで危機感が不足していないか心配になる。
・ルールが定着したが、何のためにそのルールになっているのか理解されていないことがある。
・変化に対して現場の拒否反応があり、マンネリ化の課題がある。
・社員はやらされている感がある。定期的に自己診断を行い、形骸化しないような施策を打ってきているが、施策に限界が感じられる。
・ある程度マネジメントシステムが定着したが、内部監査項目等が固定化され形骸化してきている。

**[3.経営者の積極的な参画・理解を得ること]**

情報セキュリティは費用対効果が見えにくいこともあり、経営陣についてはセキュリティを保護する必要という認識はあるものの、ISMSへの理解を得る時間がとりづらく積極的な参画・理解を得ることが難しいという意見や、セキュリティ強化等のための資源についての理解・確保が課題であるといった意見が多かった。この課題を認識している組織としては、主にISMS運営事務局が挙げられた。回答例を次に示す（課題を認識している組織の記載がある場合には、カッコ書きで示す）。

・経営陣が多忙なため理解を得る時間がとりづらい。
・コスト意識がビジネスへ直結した投資ではないため、予算獲得が困難。
・セキュリティ強化等の資源の理解、確保が難しい。
・経営陣については利便性を求める傾向が強く、セキュリティを保護する必要がある認識はあるものの、取組に対して積極的とは言い難い。
・大きな問題が発生していないことが原因か、ISMS活動の有効性が過少評価されているように感じる。
・経営課題が多すぎて、情報セキュリティの重要性を認識しつつも後回しになりがちである。

**[4.情報セキュリティ対策の強化]**

この課題は、主に情報システム担当、ISMS運営事務局において認識されており、課題としてはクラウドサービスなどの新技術活用における情報セキュリティ対策強化のための予算・コストの調整が困難、新たな脅威の情報収集と情報セキュリティ対策の強化が必要だが迅速な対応が困難といった意見が多かった。回答例を次に示す（課題を認識している組織の記載がある場合には、カッコ書きで示す）。

・全社レベルでのセキュリティ対策強化における、予算の確保及び、実施コストの調整。
・クラウドサービス活用における情報セキュリティ対策の強化。
・ITインフラの技術向上によるモバイル化対応。
・新たな脅威や環境に対応しなければならない点（情報システム担当）。
・対策強化による従業員の負担増。
・事業を取り巻く状況と規格要求事項の解釈の変化対応情報がなく、対応策に苦慮することがある。
・特に大きな事故が起こっていないので、強化というより維持になっている。
・発生したインシデントに対する是正処置の的確な対応。

**[5.内部監査の改善]**

内部監査員の育成、質の向上、増員などが必要という意見、内部監査の有効性の改善が必要という意見、内部監査の手法や内容がマンネリ化が進んでいるという意見などがISMS運営事務局から多く寄せられた。この課題を認識している組織としては、主にISMS運営事務局、内部監査責任者が挙げられた。回答例を次に示す（課題を認識している組織の記載がある場合には、カッコ書きで示す）。

・指摘や改善が出にくくなっており、今までとは違う視点での監査ができるよう、教育が必要と考えている。
・監査員のレベルの統一。
・内部監査員のシステムに関する知識が足りない。
・構成人数が少ないため、監査・被監査のメンバーが同じになりやすく、監査も変化に乏しくなる。
・効果的な監査をするには高度な内部監査員の知識や経験が必要で、それに関する教育

費用や時間がかかる。
・業務効率向上に寄与できない点、余計な仕事が増えるととらえがちになるところ。
・経営者、ISMS運営事務局から見て、内部監査から積極的な成果・効果を得ることが少ない。
・毎年監査項目の変更が少ないため、真の改善につながる監査になっていないことを懸念。
・ISMSのPDCAと業務運用稼働とのバランスが難しい。
・内部監査にかかる労力の削減と効果の向上。

**[6.人材の確保、育成]**

ISMSの運用に携わる要員については、固定化・属人化を解消するための後任の育成、兼務による負担集中の軽減などが具体的な課題として多く挙げられた。また、知見のあるシステム管理者、情報セキュリティ管理者の確保、内部監査員の育成・確保が難しいという意見も多かった。この課題を認識している組織としては、ISMS運営事務局、経営陣、情報セキュリティ管理者、情報システム担当などが挙げられた。回答例を次に示す（課題を認識している組織の記載がある場合には、カッコ書きで示す）。

・ISMSを維持管理する上で次の世代の育成が急務。
・ISMSを理解し実行できる要員が限られている。ISMSの理解が全社員に浸透していない。
・ISMS運用メンバーが長年固定化し後継の育成ができていない。（ISMS委員会）。
・ISMSを社内横断プロジェクトで推進しており、プロジェクトメンバーは兼務のため経験不足のメンバーの負荷が大きい。
・セキュリティスキルを保持する人材の確保及び育成に関わるコスト（経営陣)。
・情報セキュリティ、IT、ネットワーク等の知識を持った管理・運用を行える人材の確保・育成が容易でない（管理責任者）。
・全従業員(代表含む)への本当の意味での浸透を考えたい。
・新しく入社された方への教育及び、関係者の人手不足。
・人事異動が頻繁にあるため、管理職の交代も多く、各部署で意識が根付かない。
・中小企業で、社内で情報セキュリティ・ＩＴに精通している人材を育成・確保することが困難。

**[7.組織内の情報セキュリティ教育・意識向上]**

要員のセキュリティ意識を維持することは重要だが、リソース（コスト）不足による教育内容の固定化もあり、マンネリ化、形骸化が課題となっているという意見が多かった。また、マンネリ化を防止するための教育内容の刷新への対応に苦慮しているとの意見も多かった。その他、新たな脅威・リスクに対応するための教育内容の見直しなども挙げられた。

この課題を認識している組織としては、ISMS運営事務局、情報セキュリティ管理者、情報システム担当、経営陣などが挙げられた。回答例を次に示す（課題を認識している組織の記載がある場合には、カッコ書きで示す）。

・ISMS運営事務局から見て、組織の構成員全員の意識向上が難しい。
・どのような教育を行っていくべきかの選択と実施のコスト。
・教育にかける時間がそのままコストに繋がった。
・上位者から内容の簡易・簡略化を指示される。
・マンネリ化を打破する為に繰り返しの教育は実施しているが、教育自体にも慣れてしまって新鮮さが無くなって来る事が課題（情報システム担当）。
・入退者が多く従業員へのセキュリティ教育は十分とは言えない。
・意識向上は継続的な運用が大切であるため、働きかけの方法には苦慮している。
・社員のISMSに対する「やらされ感」。
・新たな脅威に対するセキュリティ教育・啓蒙（ISMS委員会）。
・業務内容に沿った教育カリキュラムの確立。
・横展開するにあたり、別部署の理解を得る。
・いくらシステムでセキュリティ対策を行っても最後は人的要素が大きいため、教育・意識向上は欠かせないと考えている。
・認証範囲内の教育・意識向上よりも、全社における認証範囲外の教育・意識向上が課題と捉えている。認証範囲外の組織と業務上連携することがあるが、双方に情報セキュリティに対する共通の認識が必要と考えている。

**[8.新技術や環境変化*への対応]**　　*ランサムウェアなどの改め脅威の発生など

クラウドなどの新技術の活用における新たなリスク対応や、ランサムウェア・サイバー攻撃の高度化等による外部環境の変化に対応するための情報収集・人材確保・コストが課題として多く挙げられた。特に、日々新たな技術・脅威が発生するのに対して迅速な対応を行うことが課題という意見が多かった。この課題を認識している組織としては、ISMS運営事務局、情報セキュリティ管理者、経営陣などもみられたが、特に回答として多かったのは情報システム担当である。回答例を次に示す（課題を認識している組織の記載がある場合には、カッコ書きで示す）。

・ランサムウェア、標的型攻撃メール等、外部からの脅威に対する耐性強化（事務局）。
・クラウドへの進出による新たなリスクへの対応と、外部の脅威の高まりへの対応（管理責任者・事務局）。
・サイバー攻撃の高度化等、外部環境の変化への対応に伴う技術面の習得・人材確保・育成コスト（経営陣、開発責任者）。
・モバイル端末や私物端末の業務利用対応（情報システム室、ISMS委員会）。
・新たなリスクに対応する人材の確保ができない、対策コストを負担できない。
・最近は脆弱性の発見が多く、対象アプリのアップデートが頻発し、注意喚起やアップデートフォロー・確認に手間を取られる（管理責任者）。
・脅威のリスク評価と投資計画を長期的に計画する力量が不足している。
・常に情報を収集していないと見逃す恐れ。
・現在のマニュアルで想定していない環境が発生した場合にいかに迅速に対応出来るかが課題（情報システム担当）

・日々変わる情勢への対応方法やその作業時間の確保が容易ではない。
・新技術や環境変化によるマネジメントシステムへの反映等について具体例などを提示してほしい。
・様々な新技術はあるが、業務の効率化とセキュリティ向上は裏腹になる場合がある。

**[9.効率向上、運用コストの低減]**

事務局等の運用コスト・負担の削減が課題といった意見や、自動化・シンプル化して効率化するためにはコストがかかることが課題、認証維持のための審査費用が課題といった意見が多かった。また、費用対効果が明確に掴めないことが課題といった意見も多かった。この課題を認識している組織としては、経営陣、ISMS運営事務局が回答として多くあげられた。回答例を次に示す（課題を認識している組織の記載がある場合には、カッコ書きで示す）。

・ISMS専属の担当部署がないため、ISMS関連業務が本務を 圧迫し効率も低下させている（経営陣）。
・ISMS活動の実効性向上及び効率化（経営層及びISMS事務局が組織全体の課題として認識）。
・リスクアセスメント等、ISMS運用に対するコスト（作業工数）が負担。
・高コストになりがちなセキュリティ管理を、問題ないレベルまで低コスト化することも重要な課題。
・新技術や新たな脅威に対する対策、ISMS審査費用などの負担を低減したい。
・様々なセキュリティ対策の運用コストや運用担当者の作業効率化。
・ISMSの打合せ・進捗報告等をISMS以外の定期的な打合せに組み込む。
・運用負担がある割にはコストメリットが少ない。
・適性コストが分かりにくい。
・新たな脅威への対応、インシデントの適切な抑制のために、ルールが増加する傾向にある。運営する事務局・対応する社員の工数は年々増加している。できるだけ効率的・効果的なルール設定にし、セキュリティの担保と運営効率を両立させたい。

**[10.事業経営への貢献度を向上すること]**

セキュリティについては事業経営への貢献度を数値化・可視化することが難しく、貢献度が見えづらいことが課題であるという意見が多くみられた。また、事業経営への一体化が必要という意見もみられた。一方で、受注の機会損失を防げたという意見もあった。この課題を認識している組織としては、ISMS運営事務局、経営陣の他、事業部門、営業部門などが挙げられた。回答例を次に示す（課題を認識している組織の記載がある場合には、カッコ書きで示す）。

・貢献度を数量化できず、効果が分かりにくい。
・投資効果の把握・可視化が難しい（経営者、ISMS運営事務局）。
・セキュリティに関しては事業経営への貢献度が見えづらい。
・セキュリティは出来て当たり前というところに留まっており、経営への貢献までには

至っていないと思う。
・事業経営への、真の一体化（管理責任者）。
・マンネリ化・形骸化と関連するが、理解して実施することにより貢献度も増すと考える。
・売上やお客様満足度への貢献の見える化。
・顧客に対しての啓発・周知、ISMS取得会社が業務を受注することの顧客側メリットを分かりやすく伝える工夫。
・受注の機会損失を防げた貢献度は大きい。

**[11.他のマネジメントシステムとの統合]**

この項目では、特にISO 9001、PMS（プライバシーマーク）、ISO 14001との統合が課題として多く挙げられた。認証範囲の違いや各マネジメントシステムの性質の違いから統合が難しいという意見がある一方で、ISOによるマネジメントシステム統合を機に共通化を図るという意見もみられた。この課題を認識している組織としては、ISMS運営事務局が最も多く、その他、経営陣、ISO推進室などが挙げられた。回答例を次に示す（課題を認識している組織の記載がある場合には、カッコ書きで示す）。

・ISO 9001との統合が必要になるが、認証範囲に違いがあるため、統合が進まない。
・QMS、EMSとの性質の違いが大きく、理想の統合形態が見出せない状況（マネジメントシステム運営担当者）。
・品質、環境のリスク評価手法と整合が取れない。事務局が分離していることにも課題がある。
・PMSとの重複する部分が多いが、審査が別機関のため対応が大変。
・ISO 9001と14001を取得しており、HLS※も統一されたことから共通化できる部分については共通化を図ることを課題としている。
・QMS、ISMSについて、内部監査やマネジメントレビューなどを統合して行えた方が効率がよいと考える。
・ISO 20000を取得予定。効率的な運用を目指したい。
・ISO 22301との統合。

※ ISOが規定しているマネジメントシステム規格共通の構成・用語・テキストのこと。

**[12.外部組織が提供するITサービス*への依存性増加と管理]** *クラウド利用など

クラウドサービスに関する意見が多かった。そのなかには、今後のクラウドサービス利用の検討が必要という意見から、クラウドサービスの利用におけるリスク対応（セキュリティ対策）・ルール整備や、クラウドサービス利用拡大に伴う管理が課題といった意見があり、多くの組織でクラウドサービスの各導入段階におけるセキュリティ対策が課題として挙げられていた。また、クラウドサービス利用においては、リスクアセスメント、リスク責任の切り分け、自社で管理が及ばない範囲の増加に伴う運用の整理を課題として挙げる意見もみられた。この課題を認識している組織としては、ISMS運営事務局、情報システム担当、経営陣などが挙げられた。回答例を次に示す（課題を認識している組織の記載がある場合には、カッコ書きで示す）。

・クラウドサービスへの対応（27017対応の検討を含む）（管理責任者・事務局）。
・クラウドは社内IS部門が推奨するもののみ利用可としているが、他を利用したいという要望もある。規程を整備しないといけないが、ISMS事務局及び担当者の知識が追い付いていない。
・クラウド環境の利用によるリスク責任の切り分けが難しくなる。
・クラウド環境への移行が進んでいるが、それに対するリスク分析が弱くなっている。
・クラウド利用の審査基準の明確化。
・外部クラウドサービス利用の増加によるリスクアセスメント徹底の必要性（全社）。
・外部サービスの利用が増加しており、当社として手が届かない範囲が増えているため、どこまでかを整理して運用することは課題の一つと認識している。
・外部共有サービスを利用する場合、サービス事業者側のルールに準拠する必要がある。利用サービスに合わせられるよう、自社のルールに弾力性を持たせる必要がある。
・業務上のサーバーなどがクラウド環境になりつつある。そのときの安全性や使いやすさなど、用途用途で考えなければならない。
・社外勤務者のモバイル機器対応。
・新しい技術のリスク度を測ることに苦慮するケースが増えている。

**[13.働き方改革などの人事制度の導入への対応]**

テレワーク（在宅勤務）などの新しい働き方への将来的な対応が課題として多く挙げられた。この課題を認識している組織としては、経営陣が最も多く、その他、総務部門、システム担当、ISMS運営事務局などが挙げられた。回答例を次に示す（課題を認識している組織の記載がある場合には、カッコ書きで示す）。

・将来的な話ですが、自宅勤務によるテレワーク等、現在考えられていない働き方に対応する仕組みを迅速に対応する事が課題（経営陣、情報システム担当、ISMS担当）。
・在宅勤務及びBYOD対応への仕組み構築とルール整備。
・新たなインフラ環境の運用開始に伴うセキュリティ対策に関係する検討範囲が多岐に渡り運用面、費用対効果等大変である。

**[14.審査関連への対応（例：審査関連の費用・審査計画への対応等）]**

認証維持のための定期的な審査費用を課題としてあげる意見が多かった。また、審査時の対応のための要員への負担や実業務への影響も課題として挙げられた。この課題を認識している組織としては、ISMS運営事務局、経営陣、管理責任者などが挙げられた。回答例を次に示す（課題を認識している組織の記載がある場合には、カッコ書きで示す）。

・審査関連費用の負担軽減。
・認証範囲の人員が兼務しているため、審査対応が負荷となっている。
・審査費用が実績向上につながっているか判断できておらず、費用対効果を経営陣に十分説明できない。
・QMS、EMSは同時審査にしているので、ISMS審査も統合していきたい。
・経営層から見る、審査費用と質問の内容、指摘事項、ＭＳの活用度合いのギャップが大きい。

## 審査員の力量及び審査の質について

### 質問12 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つの項目に対して「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段階で尋ねた結果は、図12-1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」(73.6%)、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」(68.6%)、「4.コミュニ ケーション能力」(66.3%)、「5.審査技術」(65.9%)、「6.改善課題を指摘する能力」(60.5%)、「3.受審組織の業務に対する理解」(58.2%)の順となっている。「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。

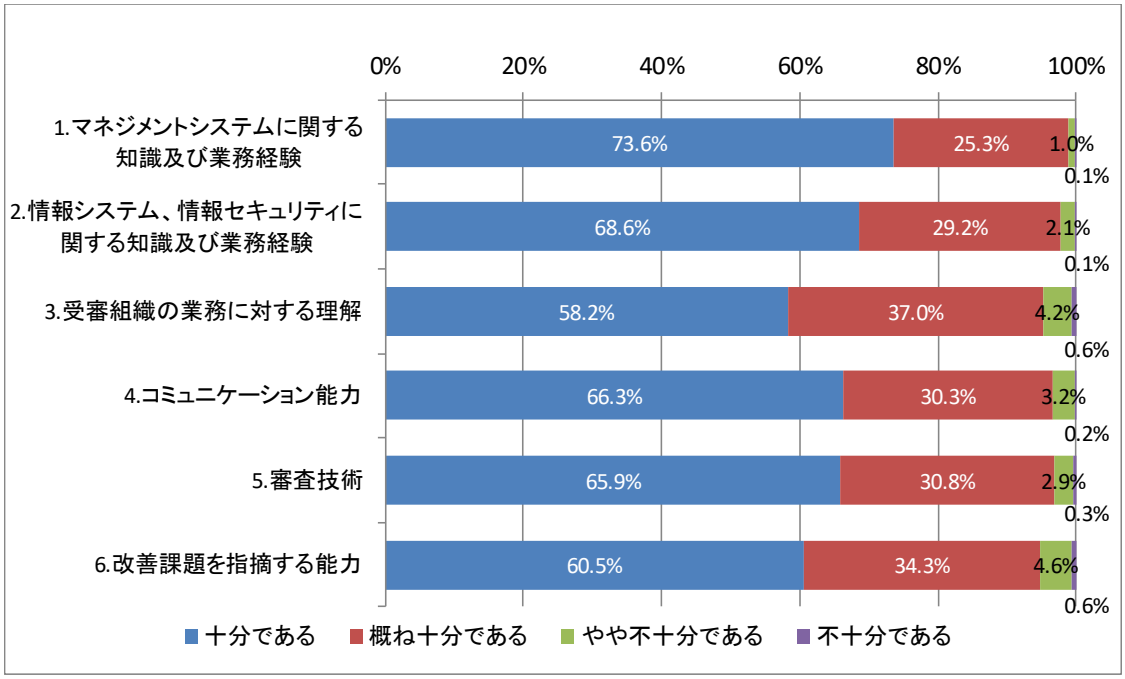



**図12-1 審査員の力量**

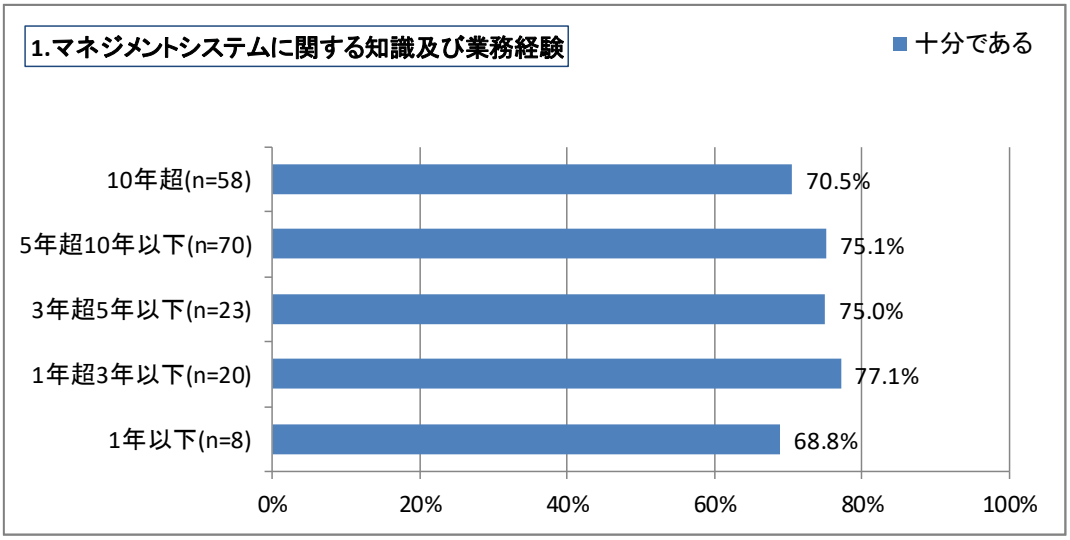
総数:1,180

### 質問12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５段階ごとにクロス集計した結果を、図12-2に示す。

回答の組織数が少ないところもあるが、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。



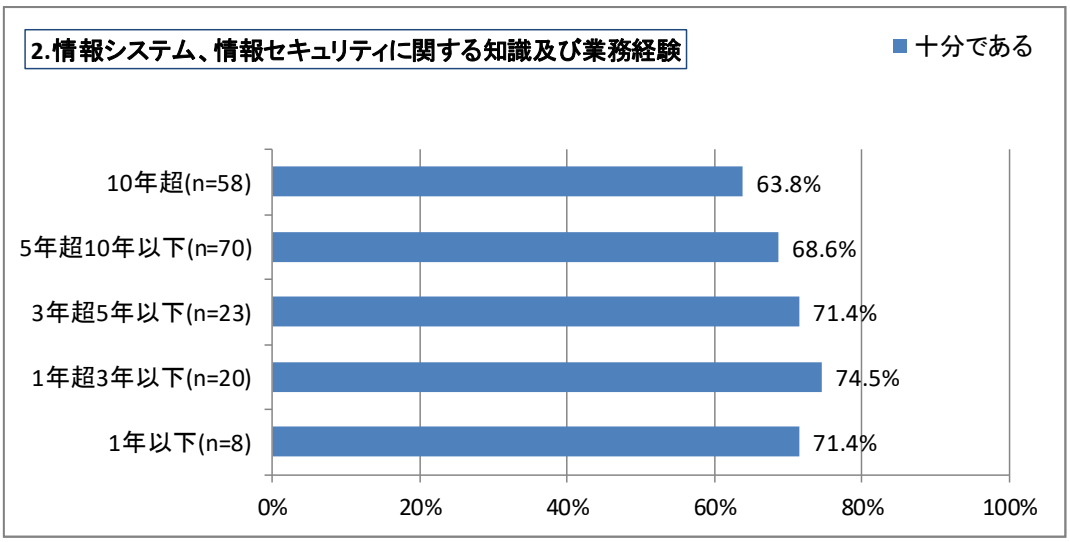
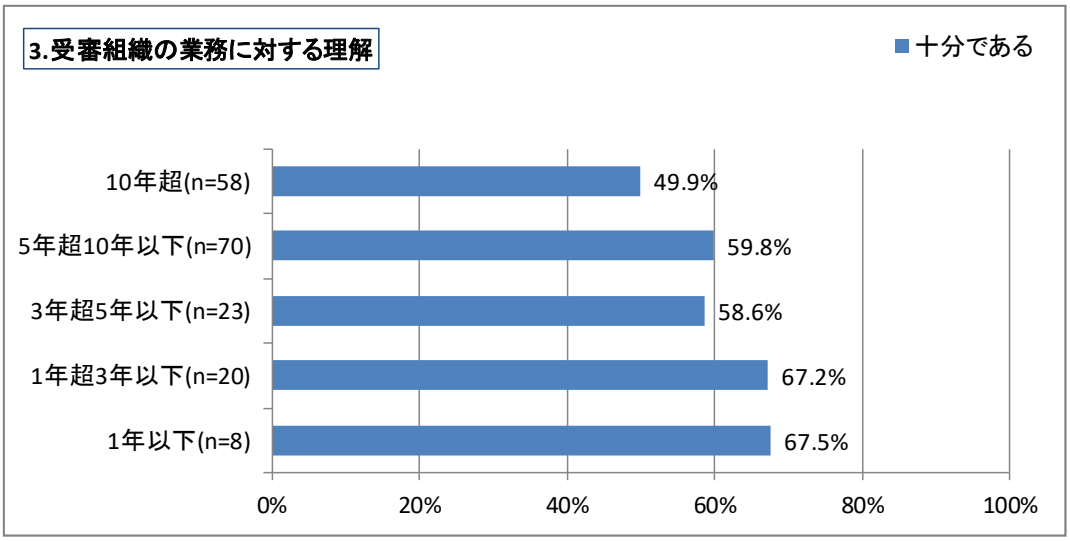




**図12-2 経過年数区分と審査員の力量(1/3)**



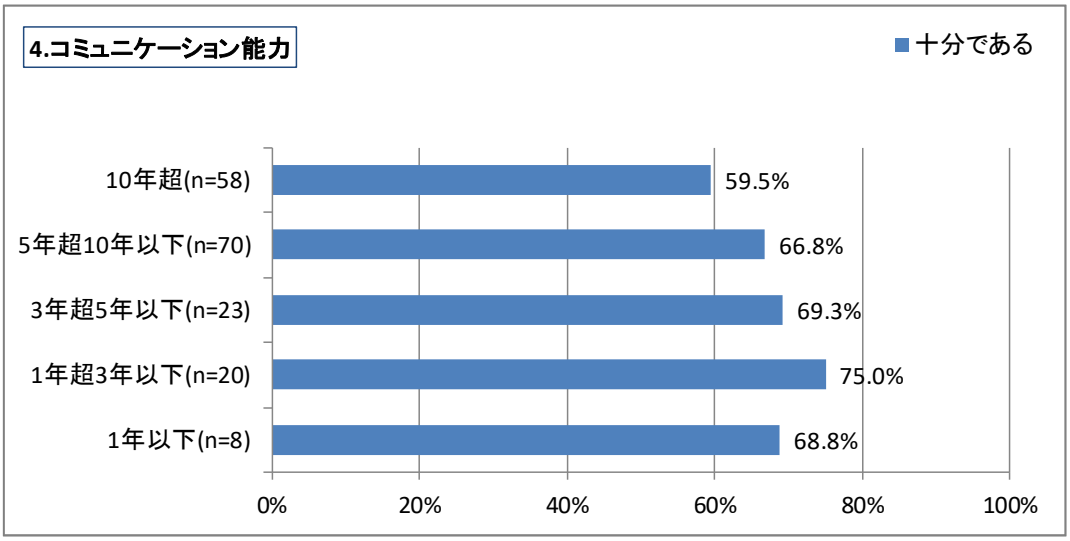
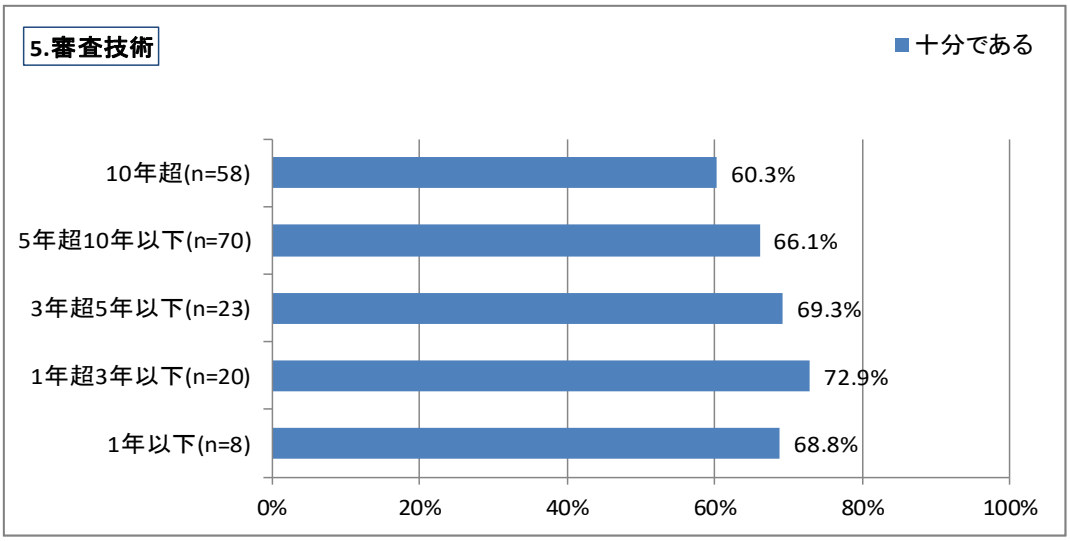




**図12-2 経過年数区分と審査員の力量(2/3)**



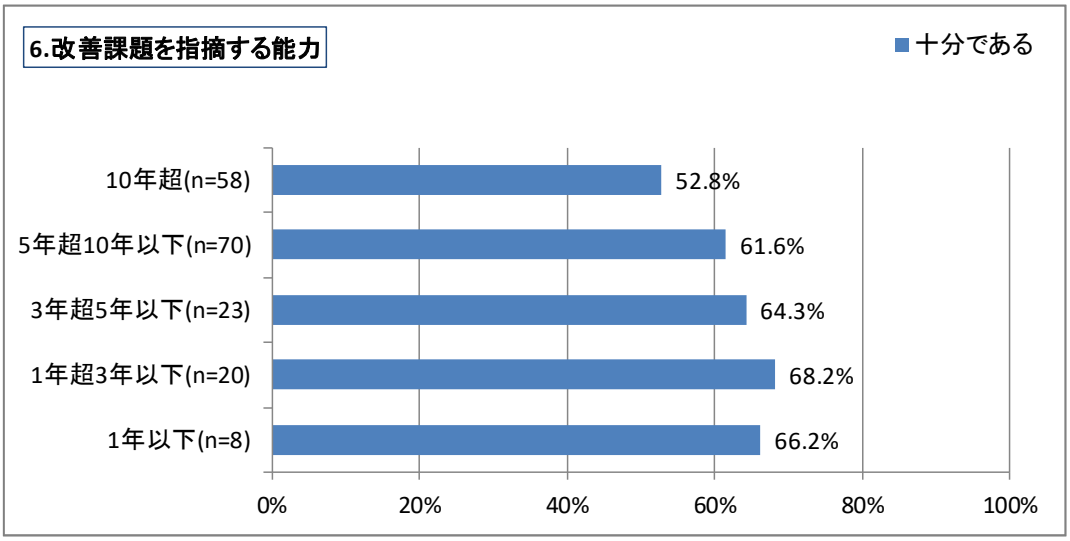




**図12-2 経過年数区分と審査員の力量(3/3)**

**質問13 認証審査の質**

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段階で尋ねた。

a)規格適合性に関する審査内容の評価

規格適合性に関する審査内容の評価は、「満足」(65.0%)、「やや満足」(33.6%)、「やや不満」(1.3%)、「不満」(0.2%)であった（図13-1a）。

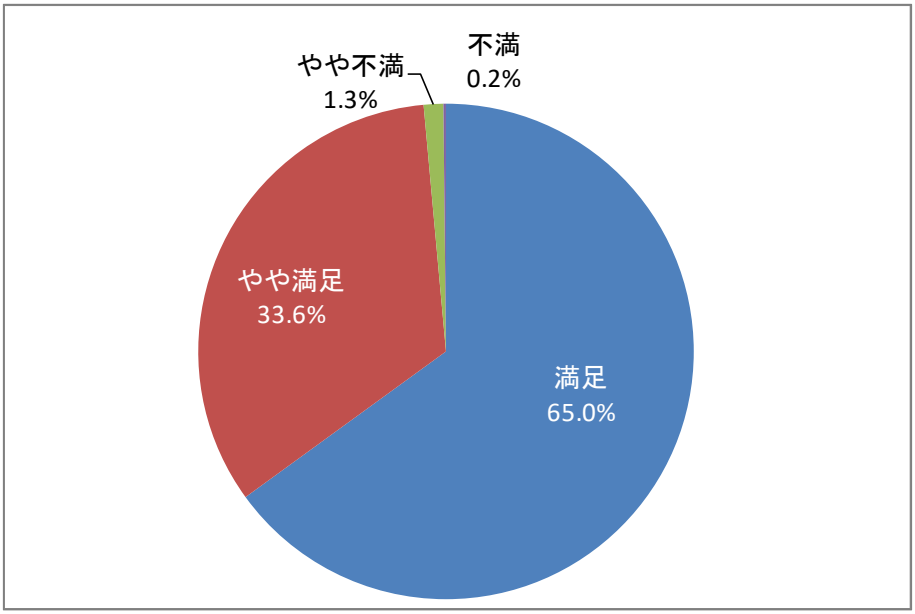



**図13-1a 審査の内容(規格適合性)** 総数:1,180

「やや不満」、「不満」な点として指摘されたものの例は、次のとおり。

・拘束時間が長すぎる。
・指摘の内容が口頭と文書でずれがある。
・細かすぎる。
・画一的に見られる。
・過去との継続性。
・自社の改善につながらない。
・自己判断が多い。
・弊社のマネジメント文章の意図を聞こうとせず、不適合を出すための審査を行っているように感じた。

(b)管理策に関する審査内容の評価

管理策に関する審査内容の評価は、「満足」(63.6%)、「やや満足」(33.9%)、「やや不満」(2.2%)、「不満」(0.3%)の順であった（図13-1b）。

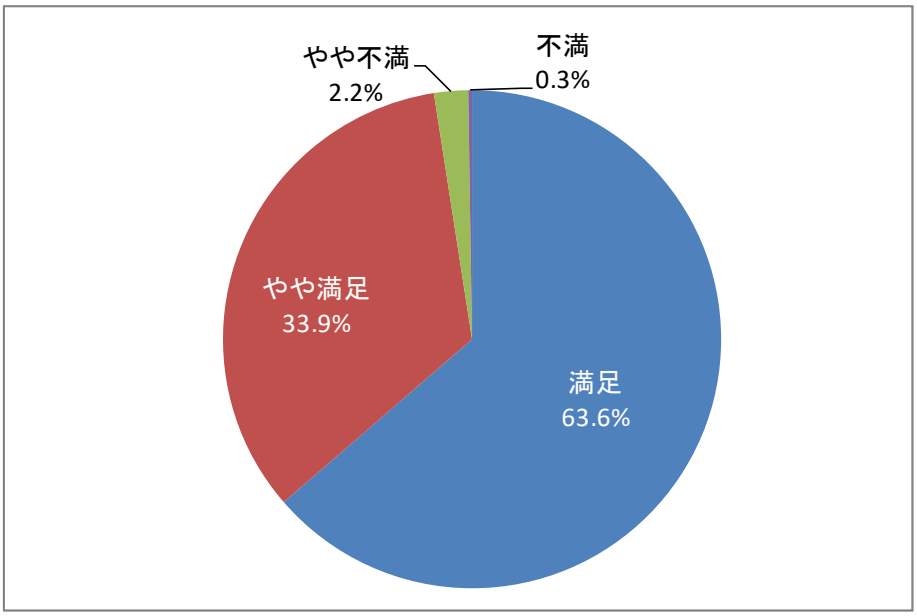



**図13-1b　審査の内容（管理策）**　　総数：1,180

「やや不満」、「不満」な点として指摘されたものの例は、次のとおり。

・審査員によって判断基準が異なる。
・重箱の隅のようなことを指摘する。
・問題の本質に対する指摘をいただけない。
・量が多くて見切れない。
・指摘がない。

**(2)審査の時間**

審査の時間の評価は、「適切」(74.0%)、「長い」(13.1%)、「短い」(2.5%)、「何とも言えない」(10.3%)であった（図13-2）。

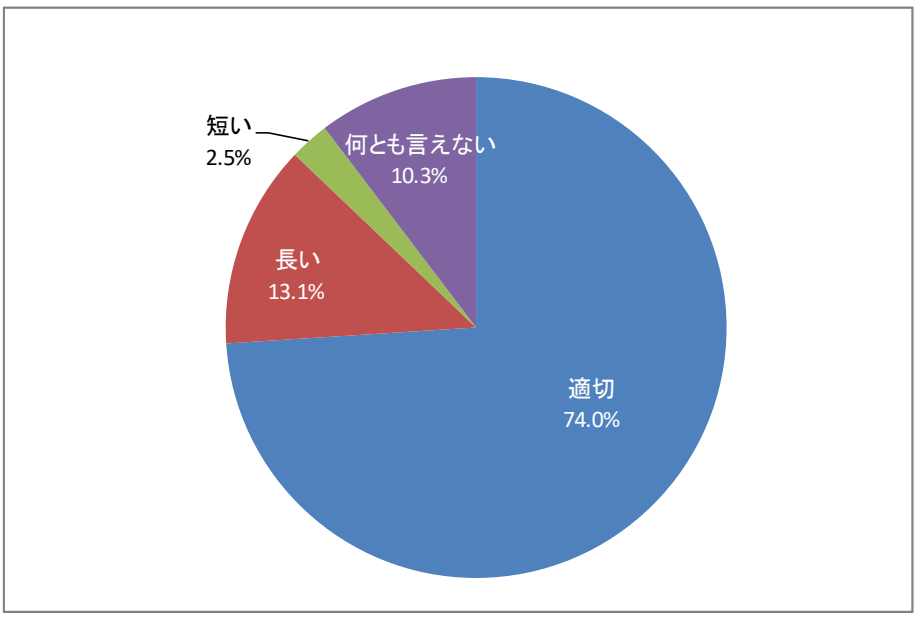
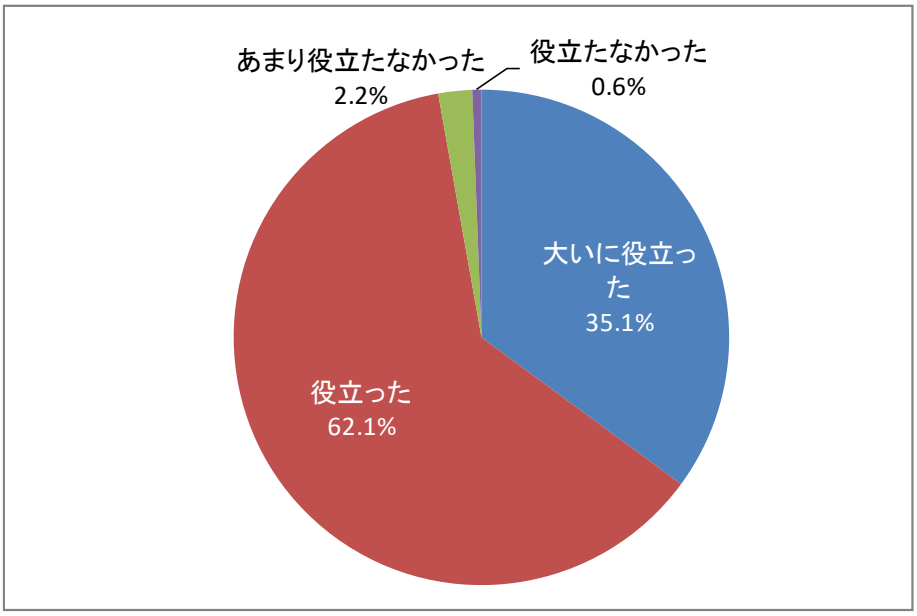



**図13-2　審査の時間**　　総数：1,180

### (3)審査の所見・指摘の有効性

(3) 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段階で尋ねた。

評価は、「役立った」(62.1%)、「大いに役立った」(35.1%)、「あまり役立たなかった」(2.2%)、「役立たなかった」(0.6%)であった（図13-3）。




総数:1,180

**図13-3 審査の所見・指摘**

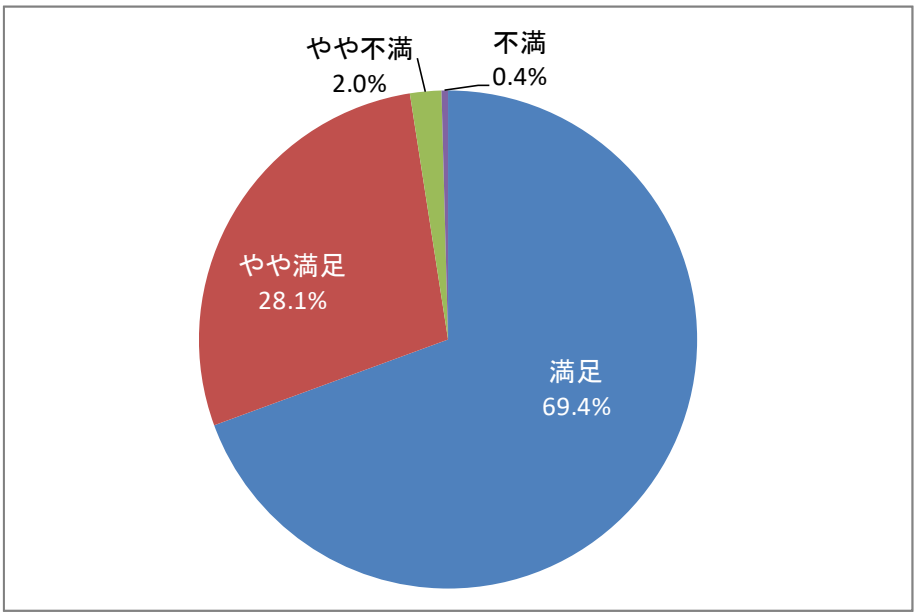
「あまり役立たなかった」、「役立たなかった」点として指摘されたものの例は、次のとおり。

・技術知識の不足。
・認識していることが多かった。
・具体性がない。
・指摘があまりなかった。
・弊社マネジメント、管理策について理解しようとせず、審査員の持論から指摘を行っているので弊社には合わない指摘であった。
・審査員の力量により大きく左右される。必要以上に厳しいのも困りものだが、当たり障りのないのもどうかと思う。
・無理に所見を考えている。

### (4)審査の質に対する総合評価

審査員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」(69.4%)、「やや満足」(28.1%)、「やや不満」(2.0%)、「不満」(0.4%)の順であった（図13- 4）。




総数:1,180

**図13-4 審査の質に対する総合評価**

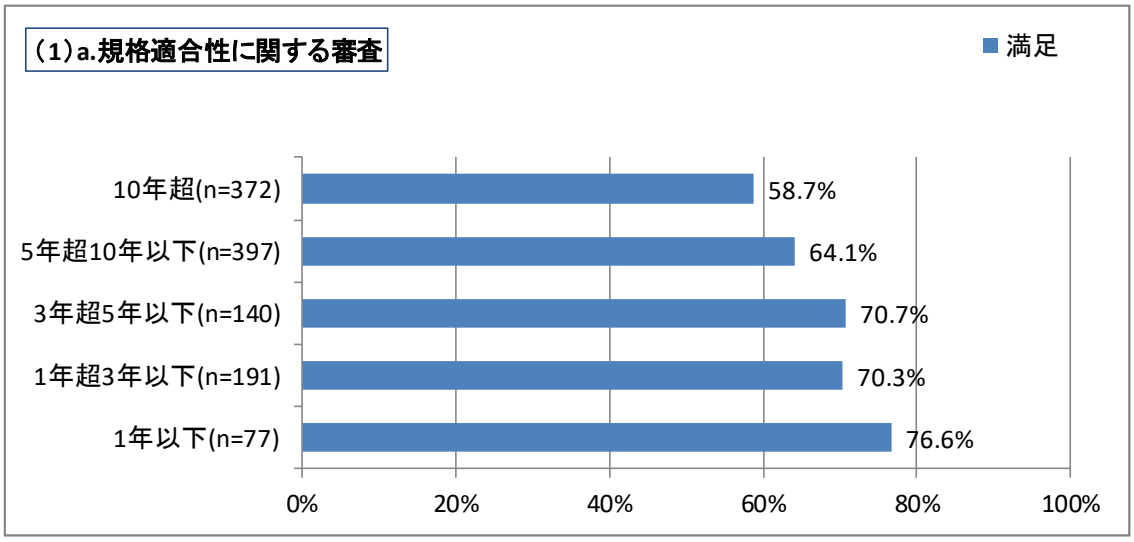
「やや不満」、「不満」な点として指摘されたものの例は、次のとおり。

・もっと実質的な我々が気が付かない有効な改善の機会が欲しかった。
・より厳しい審査を期待する。
・指摘の視点が限定的。
・問題の本質に対する指摘をもらえない。
・ノルマとして指摘事項をあげているのではないかと感じる。
・量的に見切れていないと感じる。
・審査員によってバラつきが見受けられる。
・当社の企業形態を前提とした審査となっていない。
・拘束時間が長すぎる。

### 質問13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５段階ごとにクロス集計した結果を、図 13-5に示す。

(1) は、経過年数とともに下がる傾向にある。(2)～(4)は、項目によって若干の差異があるものの、「質問１２と質問５とのクロス集計」の場合と概ね同様、ISMS 認証取得3年の再認証審査時期を境として、評価が段階的に下がる傾向がみられる。



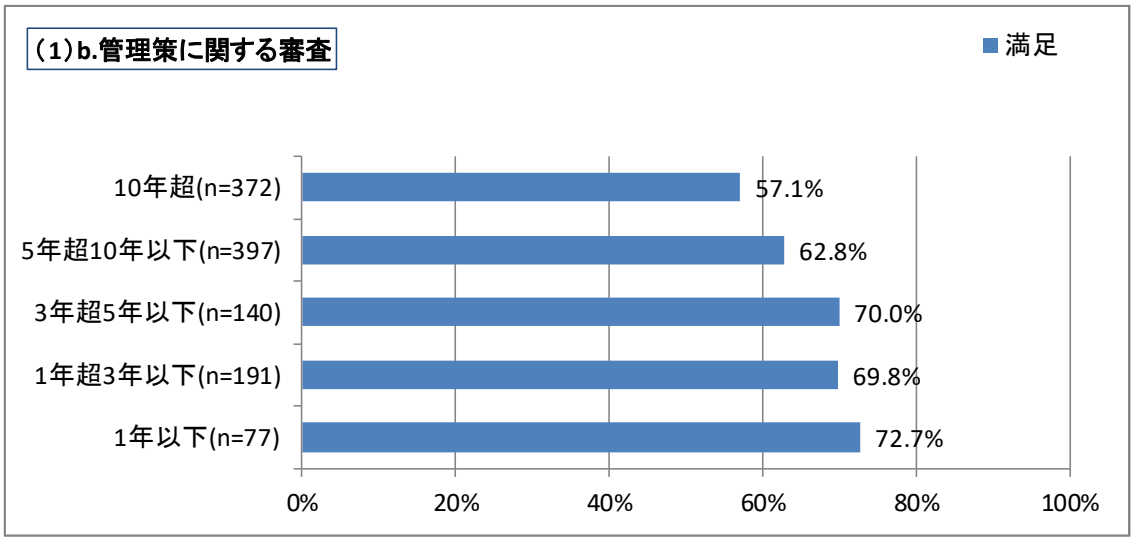
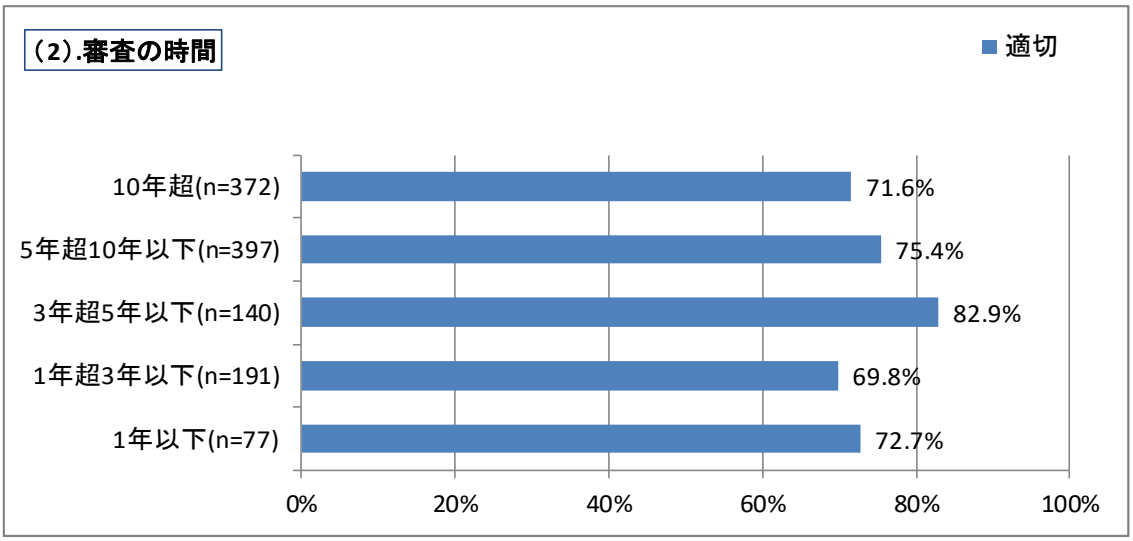
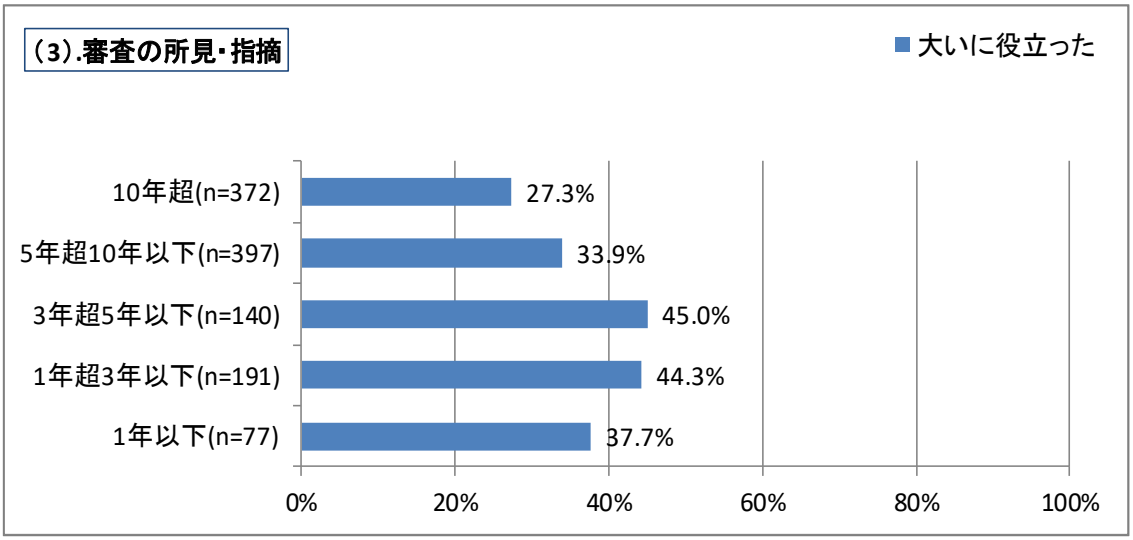




**図13-5 経過年数区分と審査の質(1/2)**



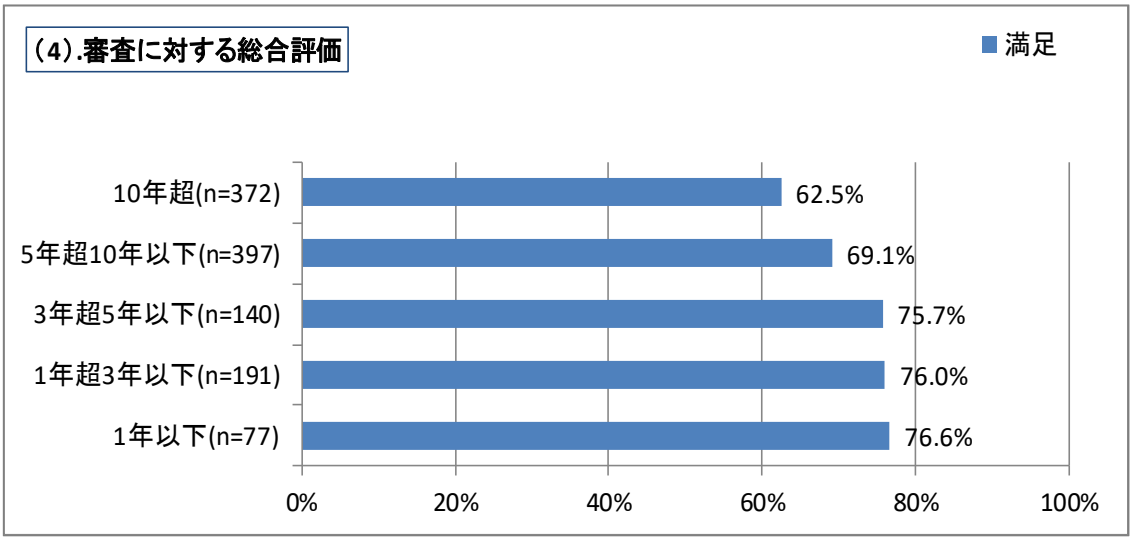
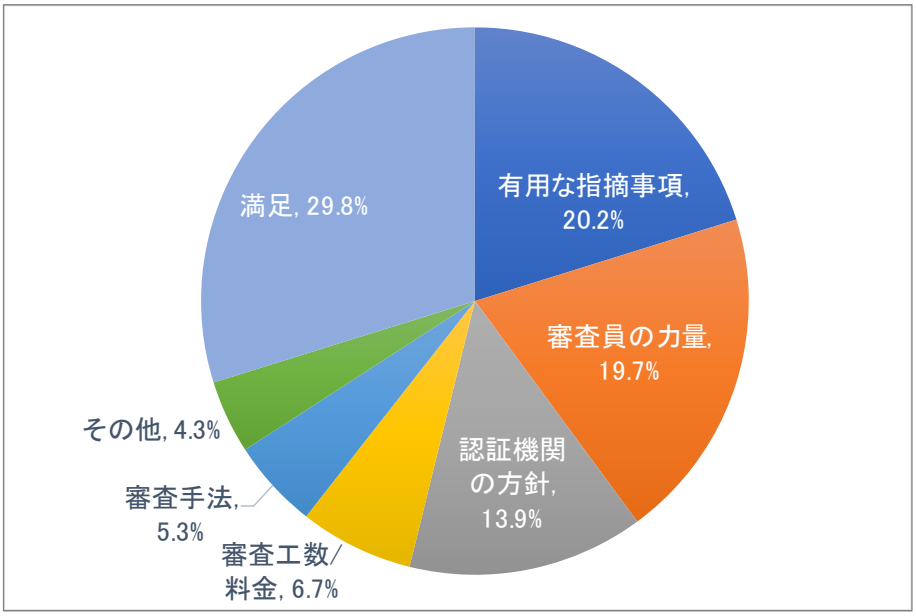




**図13-5 経過年数区分と審査の質(2/2)**

### 質問14 認証審査および審査員に対するご意見・ご要望

認証審査および審査員に対するご意見・ご要望の内容（記述式）を分類した結果は、図14のとおりである。




総数：208

**図14 認証審査およ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は、次のとおり。

**・有用な指摘事項**

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、今後の改善活動に活かそうとする内容である。回答例を以下に記す。

・改善に繋がる指摘は厳しくてもしてほしい。
・我々が認識できていない課題等の指摘がほしい。
・本質的なリスク改善につながる指摘をしてほしい。
・受審企業の特性に沿った審査および指摘をしてほしい。
・情報セキュリティの観点から経営改善に役立つ提案などが増えるとよい。
・コンサルにならない程度で構わないのですが、観察事項や改善の機会をいただいた時には、他組織での事例など、ヒントを交えて指摘をしてほしい。

**・審査員の力量**

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、審査員の力量のばらつきや審査員によって見解が違う指摘事項となることがあるため、均一でかつ有益な情報の提供を求めるものである。また、組織の業務内容等の理解や最新の技術に対する知見を求めるものある。回答例を以下に記す。

・審査員により意見が違う。 問題ないと以前審査員に言われたことが、指摘事項として

ピックアップされることがあった。

・審査員の質のバラツキが大きい。 適合性だけを求められても企業活動に意味はなく、有効性評価を中心に審査してもらいたい。

・審査実施中に担当審査員の解釈が、やや固定観念に縛られ柔軟性がないと感じられたことがあった。

・被審査組織の業種・事業の特徴など、理解の広さ・深さを期待する。

・事業規模にあった合理的な判断、新技術に対する知見を高めてほしい。

**・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、回答例を以下に示す。

・過去の経緯なども理解できると思うため、できれば同じ審査員による継続的な審査を希望。

・規格の改訂情報について、早目の情報提供を希望。

・審査の実施計画の作成において，審査報告書の作成及び確認時間を考慮し，計画段階で十分な時間を確保できるよう留意してほしい。

・昨今のデータねつ造等により、審査や認証への価値が下がってしまっていることもあり、簡単に審査がクリアできることや、形式的な進め方も問題と感じている。

**・審査工数/料金**

ほとんどが審査期間の短縮、審査費用の低減に関する要望であった。

**・審査手法**

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手法に関するものである。なお、審査員による判断のばらつきについては、「審査員の力量」に分類した。

・審査員、弊社事務局とのコミュニケーションを重視した審査を行ってほしい。

・審査時に難しい言葉があるのは仕方ないと思うが分かりやすく説明してほしい。

・運用について、当たり前のことが当たり前に実施できていることを審査してほしい。

・管理策の強化という観点で、もう少し細かく 審査をしてほしい。

**・その他**

アンケート調査に関する回答や意図が把握できなかった回答などがここに含まれる。

**・満足**

審査が改善に役立っているという意見、審査員への感謝の意見や審査に満足しているという意見も多く寄せられた。回答例を以下に示す。

・単に規格要求に対する合否を確認するだけでは無く、マネジメントが求める本質を説明して頂けるため、今後の運用や改善に役立っている。

・業務内容等をご理解した上で、今後の活動に大変役立つ審査をしていただいている。

・外部の視点からの指摘事項は、社内では気付かなかったこともあり、とても有用な指摘だった。単なる認証取得・維持のための審査ではなく、弊社に内在する問題点やリ

スクをご指摘頂き感謝している。

・継続的に運用するにあたり当社の実態に合わせた実際的な考え方を適切に説明していただいた。また、ニュートラルな立場で親切に対応いただいた。

・指摘事項が明確で非常に良かった。

・短い時間の中で、合理性のある指摘をいただき、気づきの部分を含めて、客観的に指摘をいただけるので非常に有効と感じている。

・当社の実情を認識し、コミュニケーションも豊富に、わかりやすく審査・指摘をいただいた。

・自社内への評価のみでなく，業界の傾向また他業界の例なども示していただき，セキュリティ活動の改善に大変役立っております。

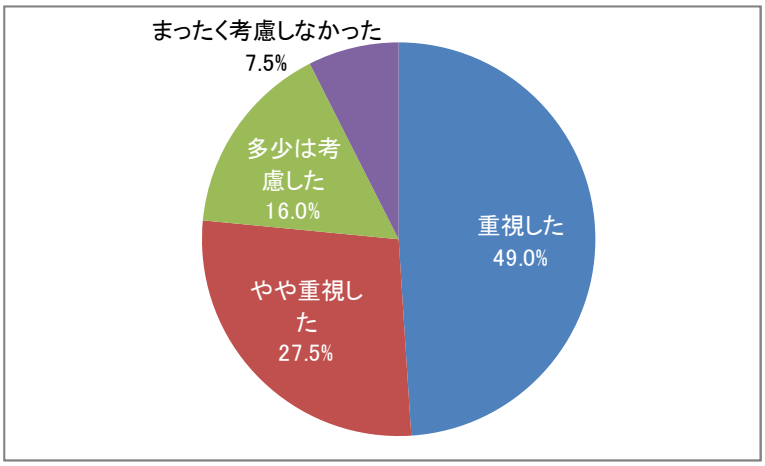
認証機関の認定の信頼性について

**質問15 認証機関から認定を受けた認証機関の信頼性**

認定機関から認定を受けた認証機関の信頼性について、認定の有無、国内の認定機関の２つの観点で評価していただいた。

**（1）認定の有無**

信頼性の判断材料の一つとして、認定の有無を4段階で評価していただいた結果、「重視した」（49.0%）、「やや重視した」（27.5%）、「多少は考慮した」（16.0%）、「まったく考慮しなかった」（7.5%）の順となった（図15-1）。

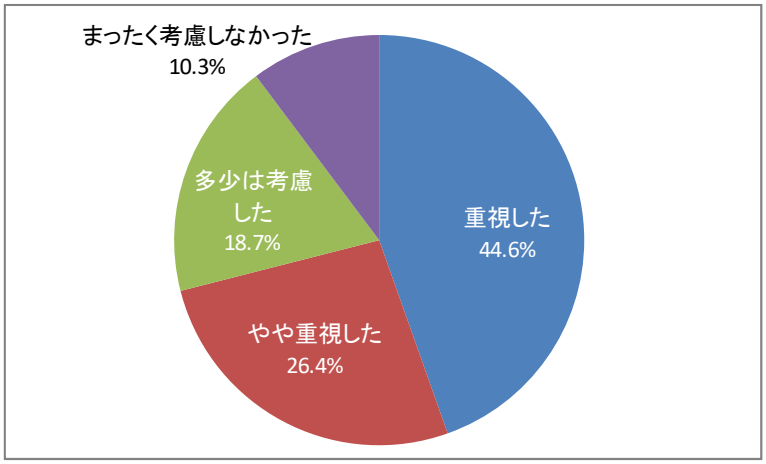



総数:1,180

**図15-1 認証機関の認定の有無**

**（2）国内認定機関による認定**

認定機関が国内の認定機関から設定を受けていることに関する意識を４段階で評価していただいた結果、「重視した」（44.6%）、「やや重視した」（26.4%）、「多少は考慮した」（18.7%）、「全く考慮しなかった」（10.3%）の順となった（図15-2）。



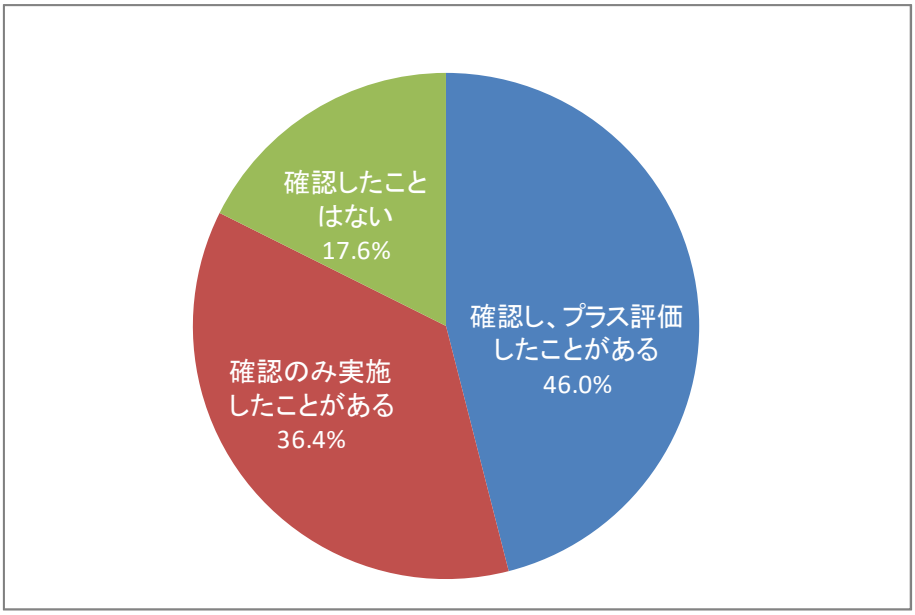

総数:1,180

**図15-2 国内認定機関による認定**

制度全般に対するご意見等

### 質問16 調達先からの要求

調達先がISMS認証を取得しているか確認したこと、また、その取得をプラスに評価したことがありますか、との質問に対して、回答は「確認し、プラス評価したことがある」（46.0%）、「確認のみ実施したことがある」（36.4%）、「確認したことはない」（17.6%）の順となった（図16）。

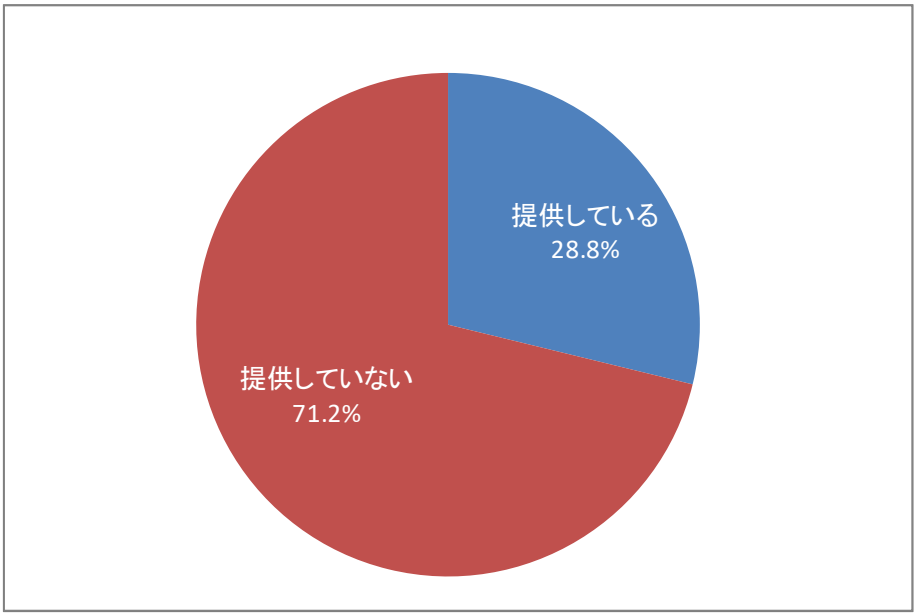



総数：1,180

**図16 調達先からの要求**

### 質問17 クラウドサービスの提供有無

クラウドサービスの提供有無について尋ねたところ、「提供している」（28.8%）、「提供していない」（71.2%）となった（図17-1）。

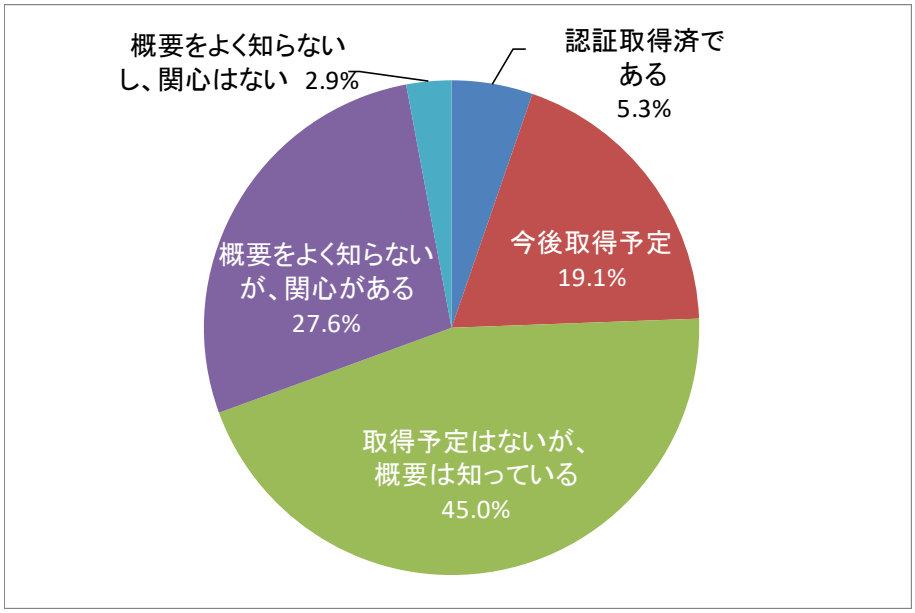



総数：1,180

**図17-1 クラウドサービス提供有無**

### 質問17-2 ISMSクラウドセキュリティ認証

上記で「はい」を選択した組織に対してISMSクラウドセキュリティ認証について取得状況を尋ねたところ「取得予定はないが、概要は知っている」（45.0%）、「概要をよく知らないが、関心がある」（27.6%）、「今後取得予定」（19.1%）の順となった（図17-2）。

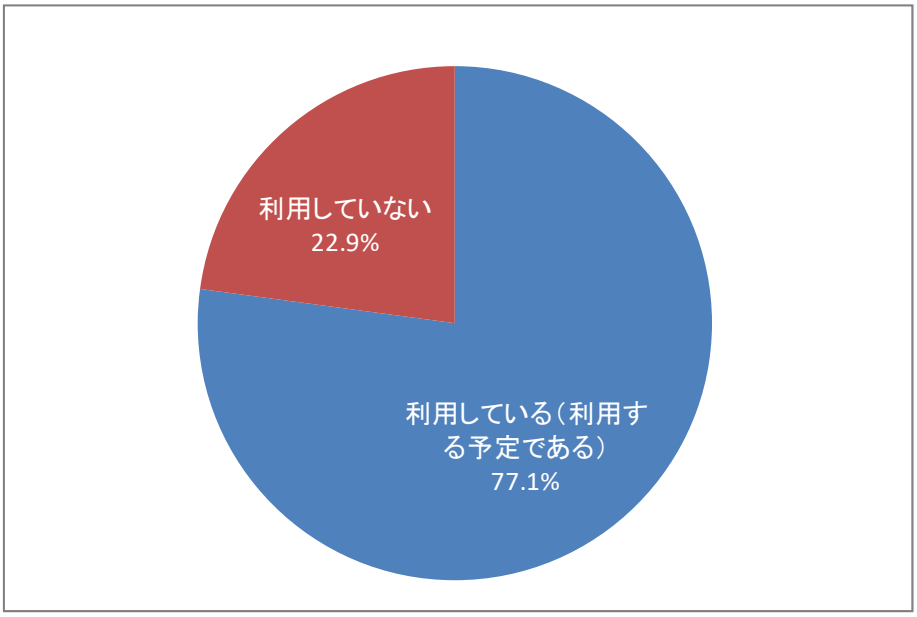



総数：340

**図17-2 ISMSクラウドセキュリティ認証の認知（提供側）**

### 質問18 クラウドサービスの利用有無

クラウドサービスの利用有無について尋ねたところ、「利用している（利用する予定である）」（77.1%）、「利用していない」（22.9%）となった（図18-1）。

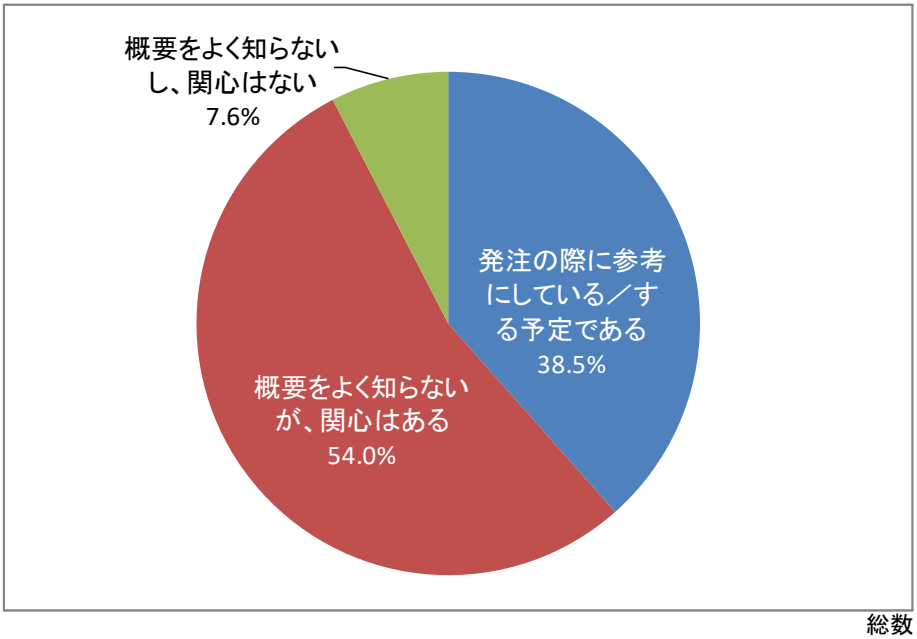



総数：1,180

**図18-1 クラウドサービス利用有無**

### 質問18-2 利用のISMSクラウドセキュリティ認証

上記で「はい」を選択した組織に対してISMSクラウドセキュリティ認証について尋ねたところ「概要をよく知らないが、関心はある」（54.0%）、「発注の際に参考にしている／する予定である」（38.5%）、「概要をよく知らないし、関心はない」（7.6%）　の順となった（図18-2）。

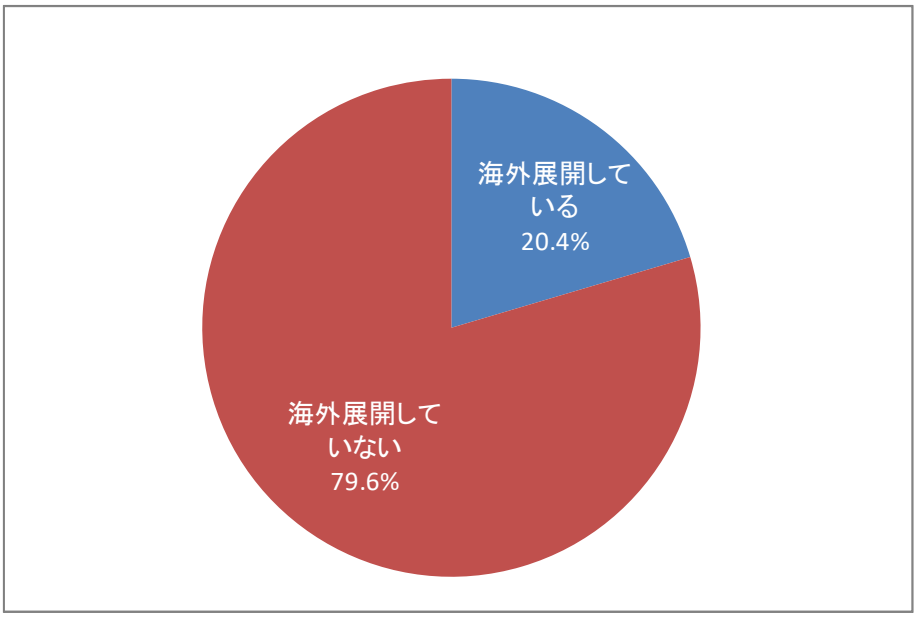



総数：910

**図18-2 ISMSクラウドセキュリティ認証の認知（利用側）**

### 質問19 海外展開有無

海外展開有無について尋ねたところ、「海外展開している」（20.4%）「海外展開していない」（79.6%）となった（図19-1）。

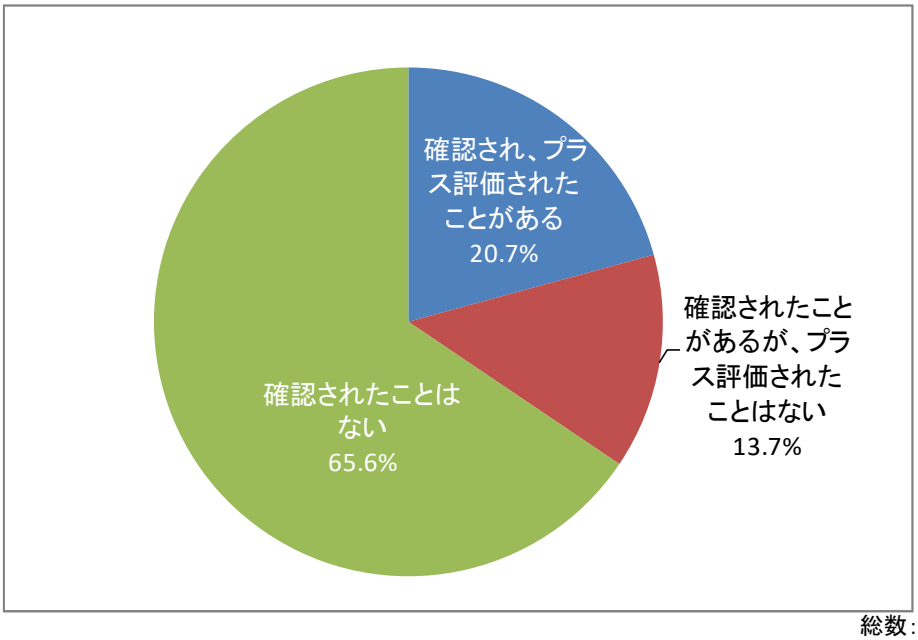



総数：1,180

**図19-1 海外展開有無**

### 質問19-2 海外のパートナーからのISMS認証の確認と評価

上記で「はい」を選択した組織に対して海外パートナーからISMS認証の取得を確認されたり、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、回答は「確認されたことはない」（65.6%）、「確認され、プラス評価されたことがある」（20.7%）、「確認されたことがあるが、プラス評価されたことはない」（13.7%）の順 となった（図19-2）。

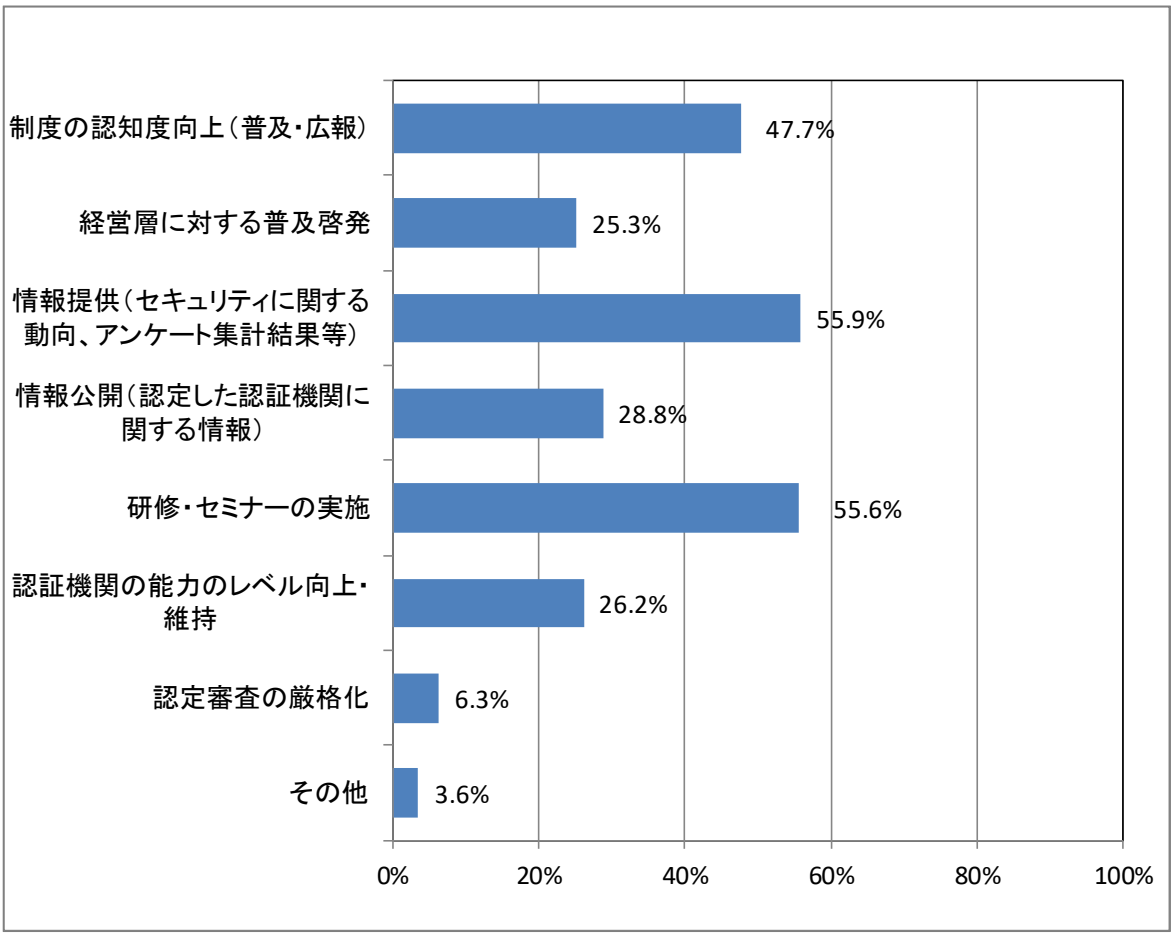



総数：241

**図19-2 海外のパートナーからのISMS認証の確認と評価質問20 本センターへの期待**

制度全般に対するご意見・ご要望（記述式）を分類した結果は、図20のとおりである。

「情報提供（セキュリティに関する動向、アンケート集計結果等）」（55.9%）、「研修・セミナーの実施」（55.6%）、次いで「制度の認知度向上（普及・広報）」（47.7%）の要望が主にあげられた。




総数：1,180

**図20 本センターへの期待**

### 質問21 制度全般に対するご意見・ご要望

分類項目ごとの主な回答内容の傾向について分析した結果を述べる。

**[制度の認知度改善、制度推進]**

ほとんどがISMS制度の認知度向上の要望であった。主な回答例を以下に示す。

・ISMSの認知度がもう少し上がってほしい。
・ISMSの有効性一般に認識されることを望む。
・ISMSがISOであることを認識していない方が多いため、ISMS＝ISOであることの認識を広めてほしい。

**[ガイドライン・規格]**

規格の日本語がわかりにくいという意見が多く、また具体的な事例や手引書の要望もあった。主な回答例を以下に示す。

・要求事項、解説等、翻訳が分かりにくい。もう少し、普通の日本語でお願いしたい。
・自由度の高い規格のため裁量範囲は広いが、何をどのくらいやれば、という指標がわかりにくい。もちろん各社で決めるべきことなのだが、もう少し他社事例とか、その手の参考類があればよいと思う。
・業務のプロセスベースのリスクアセスメント手法に関する手引書／ベストプラクティスがあるとよい。

**[制度の信頼性の維持・向上]**

回答例を以下に示す。

・審査を受けることにはリソースが必要ですが、結局は適合性評価があることで、社内のセキュリティ意識が高まるとともに、客観的な評価を頂ける機会となるため、引き続き制度の維持をお願いします。
・ISMSは認証取得より維持していく方が大変だと痛感しています。 特に、単なる認証維持では意味がなく、新技術や環境の変化に合わせ、会社としても社員一人一人のレベルでも常にPDCAを回し、技術的にもモラルやコンプライアンス、ガバナンスの意味でも「これで終わり」になることがない永続的な取り組みであることに大変さを感じております。 それだけにISMS適合性評価制度についても時代の情勢や新技術・環境変化に合わせて変化・進化して欲しいと考えております。

**[その他]**

満足している旨の回答、今回のアンケート調査に関する意見、要望のほか、以下のような回答があった。

・情報セキュリティマネジメント上、必須の制度であると考えています。
・良い制度であると思うが、ISOはヨーロッパの考え方が中心である。日本独自の考え方も付加した制度があっても良いのではないかと思う。
・国際規格でありながら本当に国際的に通用するのか不安である。日本だけが飛びぬけてこれを利用しているように見える。（特に27001）

## おわりに

このたびのアンケート調査により、ISMSの認証取得組織様から生の声を数多く聞くことができ、大変有意義な結果を得られました。ご多忙の中、本調査にご協力頂きました組織の皆様に改めて深く御礼申し上げます。

昨今はクラウド、IoT等の新しい技術の普及や標的型攻撃等による攻撃への備え等、情報セキュリティの確保は組織の大きな経営課題の一つとなっています。ISMSを取得されている組織では、社員のセキュリティ意識の向上、管理体制の強化等の効果は得られているが、最新技術動向への対応等に課題があり、具体的な対応事例を求めていることがうかがえました。

また、ISMSの認証取得期間が長い組織では10年を超える組織が出始め、情報セキュリティ教育・意識の維持面でのマンネリ化や、次世代の人材育成を課題として挙げている組織が多いことも示されています。

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制度における認定機関、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

平成29年度

# ISMS適合性評価制度に関するアンケート調査書

2018年1月10日

情報マネジメントシステム認定センター（ISMS-AC）

平成29年度

# ISMS適合性評価制度に関するアンケート調査書

## はじめに

ISMS 適合性評価制度（以下、ISMS 制度）は民間主体の制度として 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、コンピュータ処理への依存度の高まりやインターネットの爆発的な広がりとともに、それに比例して情報資産への脅威も増大し、システムや人的な脆弱性を突いたセキュリティ事故も件数、規模ともに増加してきました。また、最近では、標的型攻撃やランサムウェアなどのサイバー攻撃の進化や、クラウド・IoT などの急激な発展による新たな脅威にも早急に対応することが求められるようになってきており、ISMS の効果的な運用が益々重要になってきていると認識しております。

情報マネジメントシステム認定センター（以下、「当センター」）では、これまで過去 3 回にわたり ISMS 制度の実態把握や、制度の信頼性向上を目的としてアンケートを実施し、そこから得られた課題については、認証機関に対する認定活動及び組織一般に対するユーザーズガイド配布やセミナー開催等の普及啓発活動を通じて対応してまいりました。

前回調査から 3 年が経過し、認証取得組織数も約 1,500 件増加したことから、現時点での ISMS 制度の状況を再確認するとともに、上記の情報セキュリティ環境の変化に対する ISMS の有効性を検証し、関連する課題を明確にすることを目的として、本アンケートを実施させて頂くこととしました。皆様方から頂く情報の分析結果を基に、更なる制度の充実と改善に取り組んでまいりたいと思います。

## アンケート調査にお答えいただく前に

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いた上、本ページを含めてご返送ください。

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、一般財団法人日本情報経済社会推進協会(JIPDEC)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*　https://www.jipdec.or.jp/privacypolicy.html

**［個人情報保護管理者］**

本アンケート調査業務における個人情報保護管理者は下記のとおりです。

一般財団法人日本情報経済社会推進協会(JIPDEC) 総務担当役員

**［個人情報の取扱いについて］**

当センターでは、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。当センターは、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。
当センターが取得した個人情報は、上記によるものの他、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。
当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。
当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、当センターの 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。<br>□同意頂ける方のみ進みください。　URL の下に記載の ID と PW を入力の上アンケートにご協力お願いいたします。 |

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。

## 回答要領

質問項目は全部で、22 問です。回答は、該当する番号を選択していただくものと（選択式）、回答情報を入力していただく（記述式）ものとがあります。

## 回答期限について

以下の期日までにご回答をお願いいたします。
回答期日：２０１８年1月２９日（月）

## 連絡先

情報マネジメントシステム認定センター（ISMS-AC）
電話番号：03(5860)7570
FAX番号：03(5573)0564

## 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：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

所属：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

役職：［役員、管理職、技術職（情報システム関連等）、一般職、ISMS担当部署、その他（　　）］（ひとつだけ選択）

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18-12から該当するものを１つのみ選択してください。18-12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　各種調査業
18-10　インターネット附随サービス業
18-11　映像・音声・文字情報制作業
18-12　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. 1000万円以下
2. 1000万円超、5000万円以下
3. 5000万円超、1億円以下
4. 1億円超、3億円以下
5. 3億円超
6. 該当せず（株式会社以外）

**質問３**　貴法人が常時使用する従業員（全社）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、1000人以下
7. 1000人超

**質問４**　ISMS取得の認証範囲についてお答えください。

(1)　貴組織における認証範囲（一部認証の場合は従業員数の割合）をお答えください。

1. 全社　　2. 全社の75%以上　　3. 全社の25%～75%　　4. 全社の25%未満

(2) 認証範囲の従業員数を概数について、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、1000人以下
7. 1000人超

(3) 認証範囲に特筆すべき特徴（例えば「グループ企業による取得」、「海外サイトを含む」等）があれば記入してください。

| |
|---|
| |

**ISMS認証の実績等について**

**質問５** 貴組織がISMS認証を初めて取得してから現在までの経過年数及び現在の認証登録番号をお答えください。

経過年数

1. 1年以下
2. 1年超、3年以下
3. 3年超、5年以下
4. 5年超、10年以下
5. 10年超

認証登録番号（＿＿＿＿＿＿＿＿＿＿）

**質問６** 貴組織では、ISMS以外にどのようなマネジメントシステム認証を取得していますか。複数取得されている場合は、その全てを選択してください。

1. ISO 9001(品質)　　2. ISO 14001(環境)
3. ISO/IEC 20000(ITサービス)　　4. ISO 22301(事業継続)
5. その他

（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

**質問７**　貴組織がISMS認証を初めて取得してから現在までの間に認証機関(審査機関)を変更した、または変更することを検討されたことがあるかお答えください。

1. 変更を考えたことはない
2. 変更を考えたが、実行していない
3. 1回変更した
4. 2回以上変更した

上記で2～4（認証機関の変更を考えたことがある、あるいは実際に変更した）を選択された方は、その理由として最も当てはまるものをお答えください。

1. 審査内容（深さや指摘内容等）が不満
2. 認証機関のサービス（情報提供等）や対応（手続き等）に不満
3. 審査料金の比較
4. その他

（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

## ISMSの導入及び認証取得の効果等について

**質問８**　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向上、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 | 顧客からの信頼を確保するため | 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 |
| 9 | インシデント発生を抑制するため | 1 | 2 | 3 | 4 |
| 10 | インシデント発生時の迅速・適切な対応を可能にするため | 1 | 2 | 3 | 4 |
| 11 | 新しい脅威に対応するため（例：サイバー攻撃、クラウド、社外環境での業務） | 1 | 2 | 3 | 4 |

上記1～11以外に、目的又は動機として意識された事項がありましたら、記入してください。

| |
|---|
| |

**質問９**　ISMSを導入し認証を取得された効果について、また認証を取得し運用を継続している効果について、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向上、教育啓発に寄与した | 1 | 2 | 3 | 4 |
| 4 | 顧客からの信頼確保に貢献した | 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 | 情報面での事業継続性の向上に有効であった | 1 | 2 | 3 | 4 |
| 8 | 法遵守（コンプライアンス）の面で有効であった | 1 | 2 | 3 | 4 |
| 9 | 情報セキュリティインシデント発生の抑制に効果があった | 1 | 2 | 3 | 4 |
| 10 | 情報セキュリティインシデント発生後に迅速・適切に対応できた | 1 | 2 | 3 | 4 |
| 11 | リスク評価の方法が定着した | 1 | 2 | 3 | 4 |
| 12 | 組織の情報セキュリティレベルが期待値に達した／期待値を維持している | 1 | 2 | 3 | 4 |
| 13 | 経営者の情報セキュリティに対する関与が深まった | 1 | 2 | 3 | 4 |
| 14 | 最新のIT技術動向（例：サイバー攻撃、利用するクラウドサービスの事故）に対応した対策が図れた | 1 | 2 | 3 | 4 |
| 15 | 業務環境の変化（在宅勤務、BYODなど）、適用法令に対応する上で、社内ガバナンスに効果があった。 | 1 | 2 | 3 | 4 |

上記項目№1～15で1(該当する)を選択された場合、また№1～15以外に効果として特筆すべき事項がありましたら、その具体的な内容や例を差し支えない範囲で記入してください。

**質問１０**　顧客から、貴組織の情報管理リスクの把握のため、例えば実査、監査報告書の開示など、ISMS認証文書（登録証）の他に求められたことがありますか。

1. 求められたことがある
2. 求められたことはない

上記で１を選択した場合、どのようなものを求められましたか。

1. 実査、取引先からのセキュリティ監査
2. 内部／外部監査報告書の開示
3. 適用宣言書の開示
4. セキュリティ対策の取組状況に関するアンケートへの回答
5. その他（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

**質問１１**　貴組織のISMSを運用し、認証を維持していく上での主な課題について、該当するものを選択してください（複数可）。可能でしたら、その項目について差し支えない範囲で内容（課題を認識した主な組織*を含めて）を記入してください。

＊例：経営陣、情報システム担当、ISMS運営事務局、関連部署の事業責任者など

1. 事業内容の変化や組織改革などへの対応
2. マンネリ化・形骸化
3. 経営者の積極的な参画・理解を得ること
4. 情報セキュリティ対策の強化
5. 内部監査の改善
6. 人材の確保、育成
7. 組織内の情報セキュリティ教育・意識向上
8. 新技術や環境変化*への対応　*ランサムウェアなどの新たな脅威の発生など
9. 効率向上、運用コストの低減
10. 事業経営への貢献度を向上すること
11. 他のマネジメントシステムとの統合
12. 外部組織が提供するITサービス*への依存性増加と管理　*クラウド利用など
13. 働き方改革等の人事制度の導入への対応
14. 審査関連への対応（例：　審査関連の費用・審査計画への対応等）
15. その他

| 項目 | 内容 |
|---|---|
| | |
| | |
| | |

## 審査員の力量及び審査の質について

質問１２　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１３　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］

⑵ 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］

⑶ 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］

⑷ 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１４　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。

| |
|---|
| |

## 認証機関の認定の信頼性について

**質問１５**　認定機関から認定を受けた認証機関によるISMS認証の信頼性について、最も当てはまると思うものをご回答ください。また(1)～(2)については、その理由を簡潔に記入してください。

(1)　認証機関の信頼性の判断材料の一つとして、認定の有無を考慮しましたか。

1. 重視した　2. やや重視した　3. 多少は考慮した　4. まったく考慮しなかった

| (理由) |
| --- |
| |

(2)　認証機関が、国内の認定機関から認定を受けていることを意識しましたか。

1. 重視した　2. やや重視した　3. 多少は考慮した　4. まったく考慮しなかった

| (理由) |
| --- |
| |

## 制度全般に対するご意見等

**質問１６**　調達先がISMS認証を取得しているか確認したこと、また、その取得をプラスに評価したことがありますか。

1. 確認し、プラス評価したことがある。
2. 確認のみ実施したことがある。
3. 確認したことはない。

**質問１７(1)** 貴組織はクラウドサービスを提供していますか。

1.提供している　2.提供していない

上記(1)で1を選択した場合のみ、ご回答ください。

(2) ISMSクラウドセキュリティ認証について、最も当てはまると思うものをご回答ください。

1. 認証取得済である。
2. 今後取得予定。
3. 取得予定はないが、概要は知っている。
4. 概要をよく知らないが、関心がある。
5. 概要をよく知らないし、関心はない。

**質問１８(1)** 貴組織はクラウドサービスを利用していますか。

1.利用している　2.利用していない

上記(1)で1を選択した場合のみ、ご回答ください。

(2) ISMSクラウドセキュリティ認証について、最も当てはまると思うものをご回答ください。

1. 発注の際に参考にしている／する予定である。
2. 概要をよく知らないが、関心はある。
3. 概要をよく知らないし、関心はない。

**質問１９**（1）貴組織は事業活動を海外展開されていますか。

1.海外展開している2.海外展開していない

上記(1)で1を選択した場合のみ、ご回答ください。

(2)　海外のパートナーからISMS認証の取得を確認されたこと、あるいは貴組織が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。

**質問２０**　認定機関として、認証機関を認定する立場にある当センターに期待することがございましたら、該当するものを選択するか（複数可）、その他の欄に記入してください。

1. 制度の認知度向上（普及・広報）
2. 経営層に対する普及啓発
3. 情報提供（セキュリティに関する動向、アンケート集計結果等）
4. 情報公開（認定した認証機関に関する情報）
5. 研修・セミナーの実施
6. 認証機関の能力のレベル向上・維持
7. 認定審査の厳格化
8. その他

| |
|---|
| |

**質問２１**　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。

**質問２２**　今後、ISMS適合性評価制度改善のためのヒアリングを検討しておりますが、その際にご協力いただくことは可能でしょうか。

1. はい
2. いいえ

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。