ISMS 適合性評価制度に関する

調査報告書

2024 年 7 月

一般社団法人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、厚く御礼申し上げます。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。

情報セキュリティマネジメントシステム（ISMS）の国際規格である ISO/IEC 27001 に基づく ISMS 適合性評価制度は、2002 年の本格運用開始以降、急速な IT 化の進展及びこれに伴う組織の情報セキュリティリスクの増大を背景に順調に認証取得組織数を伸ばし、2024 年 3 月末には認証取得組織数が 7,700 件を突破しました。

皆様方におかれましては、昨今のクラウド、IoT、AI 等の新たな IT 技術の急激な発展や標的型攻撃やランサムウェア等のサイバー攻撃の進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、深く感謝申し上げます。

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 4 回にわたり ISMS 適合性評価制度の実態把握や、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。

このたび、前回調査から 7 年が経過し、認証取得組織数も約 2,000 件増加したことから、現時点での ISMS 適合性評価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、アンケート調査を実施しました。なお、今回のアンケートでは、生成AIブーム等で話題になっているAIシステムに関して、新たな設問項目を設けました。

当センターといたしましては、今回の調査結果を踏まえて、ISMS 適合性評価制度の信頼性の更なる確保とその活用度の一層の向上を通じて、我が国の情報セキュリティの底上げのインフラとして機能するよう、努めてまいる所存です。

本報告書が、ISMS に携わる皆様にとっての課題を検討、改善する際の一助となれば幸いです。

2024 年 7 月

一般社団法人情報マネジメントシステム認定センター

（ISMS-AC）

調査概要

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

調査を開始した 2024 年 2 月時点で、本調査の対象は、当センターが認定した ISMS 認証機関から ISMS 認証を取得し、登録情報を公開している 6,790 組織（海外組織及び所在地非公開組織は除く）。

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

2024 年 3 月 11 日～3 月 26 日

調査対象数：6,790

有効回答数：1,704

回 答 率：25.1%

基本情報について

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」(53.3%)が突出しており、以下「その他サービス業」(19.3%)、「卸売・小売業」(4.7%)、「分類不明」(4.0%)、「建設業(エンジニアリングを含む)」(3.8%)が続いている(図 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。

表 1 法人の業種(集計)

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	0	0.0	13	建設業(エンジニアリングを含む)	65	3.8
2	衣服・天然素材繊維製品の製造業	1	0.1	14	廃棄物処理業・再生業	11	0.6
3	木材・木製品・パルプ・紙等の製造業	6	0.4	15	電力・ガス・熱・水道供給業	6	0.4
4	出版・印刷業	51	3.0	16	卸売・小売業	80	4.7
5	化学薬品・化学製品(化学繊維を含む)・医薬品の製造業	2	0.1	17	金融・保険・不動産業	33	1.9
6	石油・石炭・ゴム・プラスチック等の製造業	2	0.1	18	情報技術	909	53.3
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	8	0.5	20	医療関係	32	1.9
9	機械・機器の製造業	23	1.3	21	その他サービス業	329	19.3
10	電気/電子機器・光学的装置製造業	33	1.9	22	公共・行政・教育機関	19	1.1
11	輸送機器製造業	3	0.2	23	分類不明	69	4.0
12	その他の製造業	21	1.2		合計	1,704	100

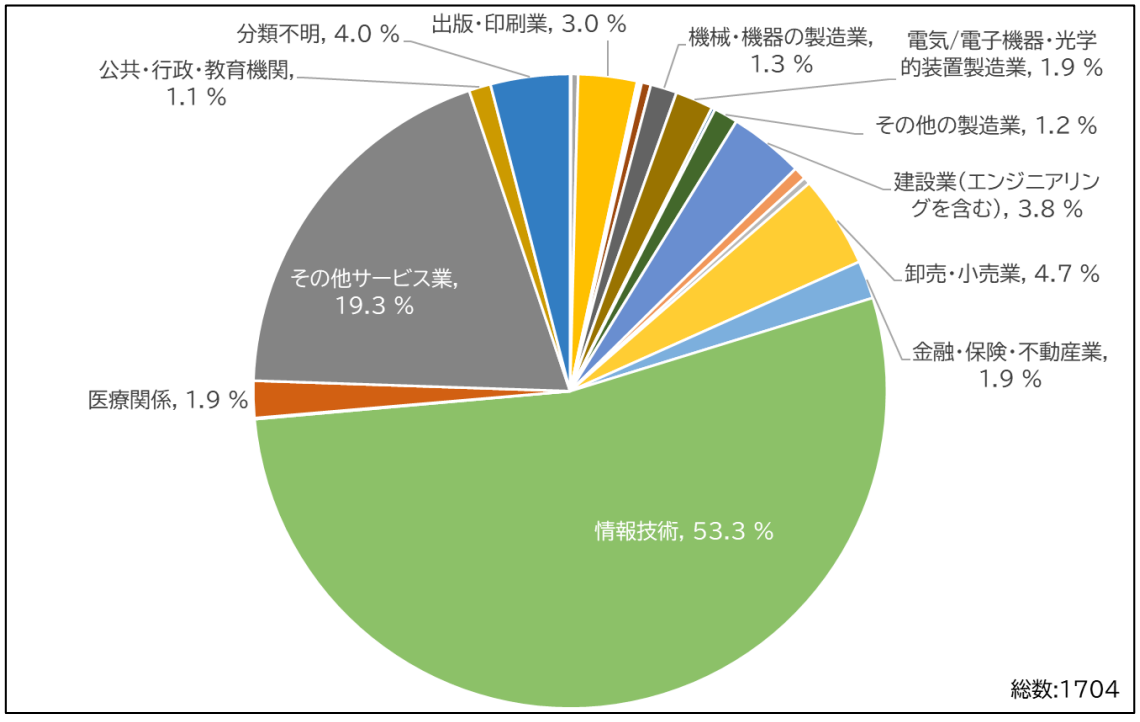

図 1 法人の業種

「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」(34.2%)、「システムインテグレーション業」(24.4%)、「ソフトウェアウェアプロダクト業」(19.8%)で 8 割を占めており、以下「インターネット附随サービス業」(5.5%)、「通信業」(4.4%)の順となっている(図 2)。

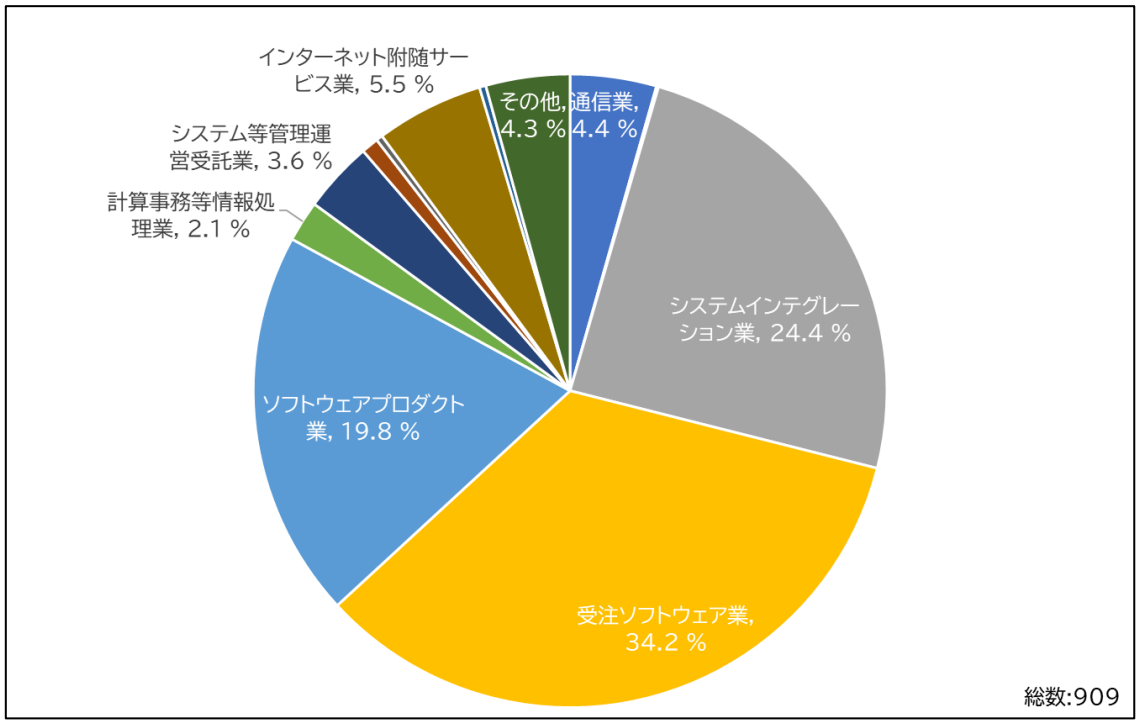

図 2 情報技術の内訳

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 万円超、5000 万円以下」(34.9%)が最も多く、「5000 万円超、1 億円以下」(21.0%)、「1000 万円以下」(19.4%)、「3 億円超」(14.5%)」、「1 億円超、3 億円以下」(6.5%)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されたい。

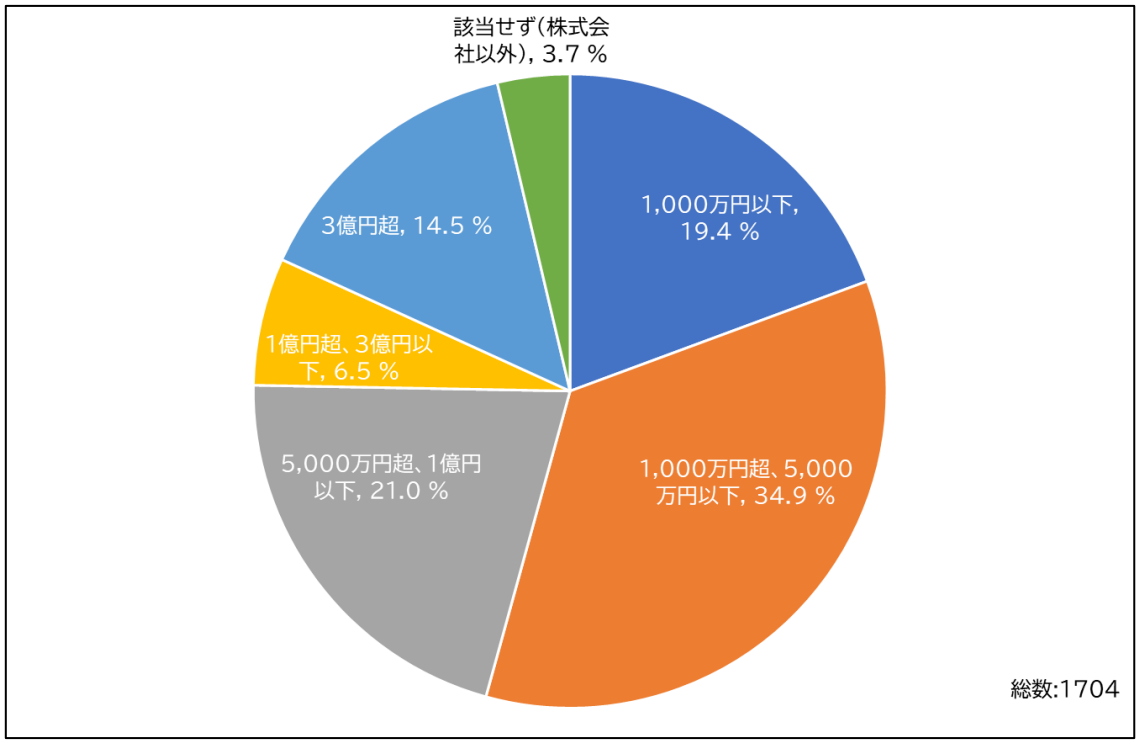

図 3 資本金

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」(23.0%)が最も多く、「20 人超、50 人以下」(21.9%)、「50 人超、100 人以下」(18.7%)の順となっている(図 4)。

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。

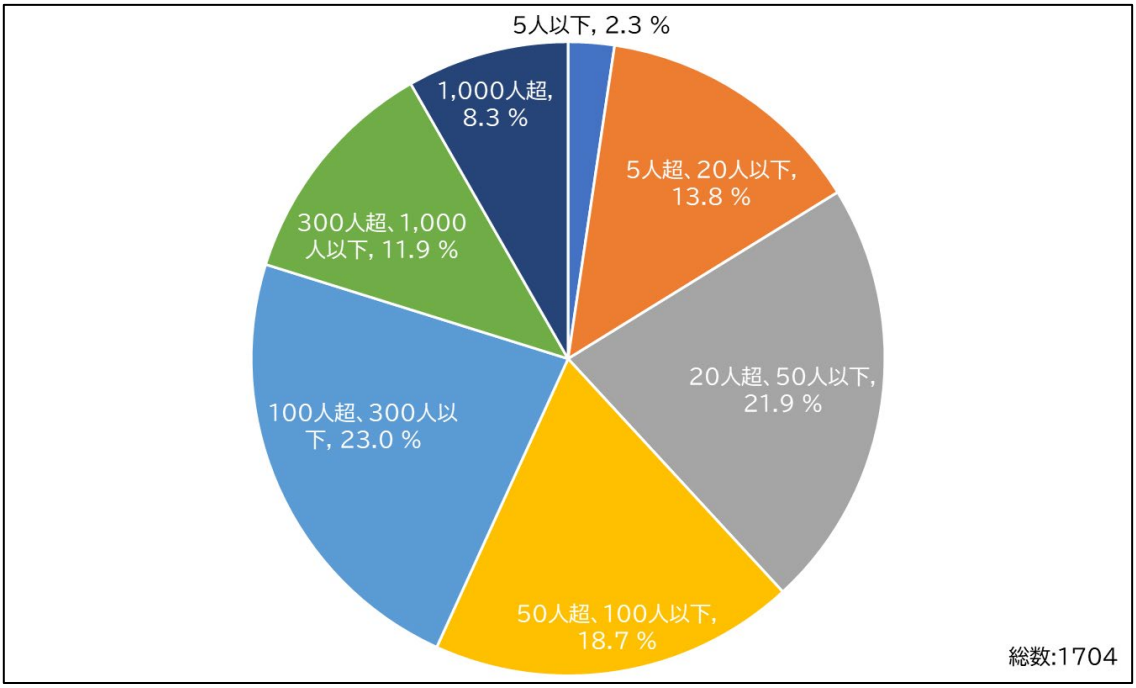

図 4 従業員数

4. ISMS 取得の認証範囲について

(1)ISMS 認証範囲の割合

ISMS 取得の認証範囲の従業員数について、全社から見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 5)。

表 2 認証範囲の割合(集計)

		回答件数(件)	割合(%)
1	全社	889	52.2
2	全社の 75%以上	259	15.2
3	全社の 25%～75%	271	15.9
4	全社の 25%未満	285	16.7
合計		1,704	100.0

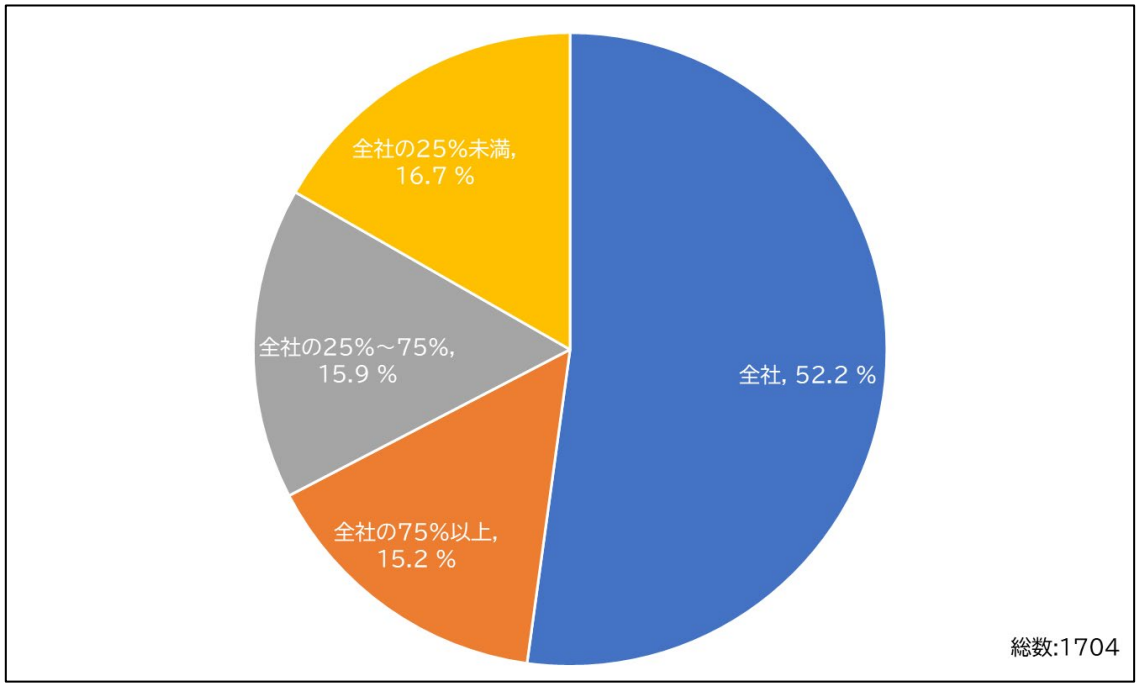

図 5 認証範囲の割合

(2)ISMS 認証範囲の従業員数

認証範囲の従業員数について尋ねたところ、「20 人超、50 人以下」(26.5%)、「5 人超、20 人以下」(23.8%)、「100 人超、300 人以下」(18.8%)、「50 人超、100 人以下」(18.2%)の順となった(図 6)。

表 3 認証範囲の従業員数(集計)

		回答件数(件)	割合(%)
1	5 人以下	63	3.7
2	5 人超、20 人以下	405	23.8
3	20 人超、50 人以下	452	26.5
4	50 人超、100 人以下	310	18.2
5	100 人超、300 人以下	320	18.8
6	300 人超、1,000 人以下	120	7.0
7	1,000 人超	34	2.0
合計		1,704	100.0

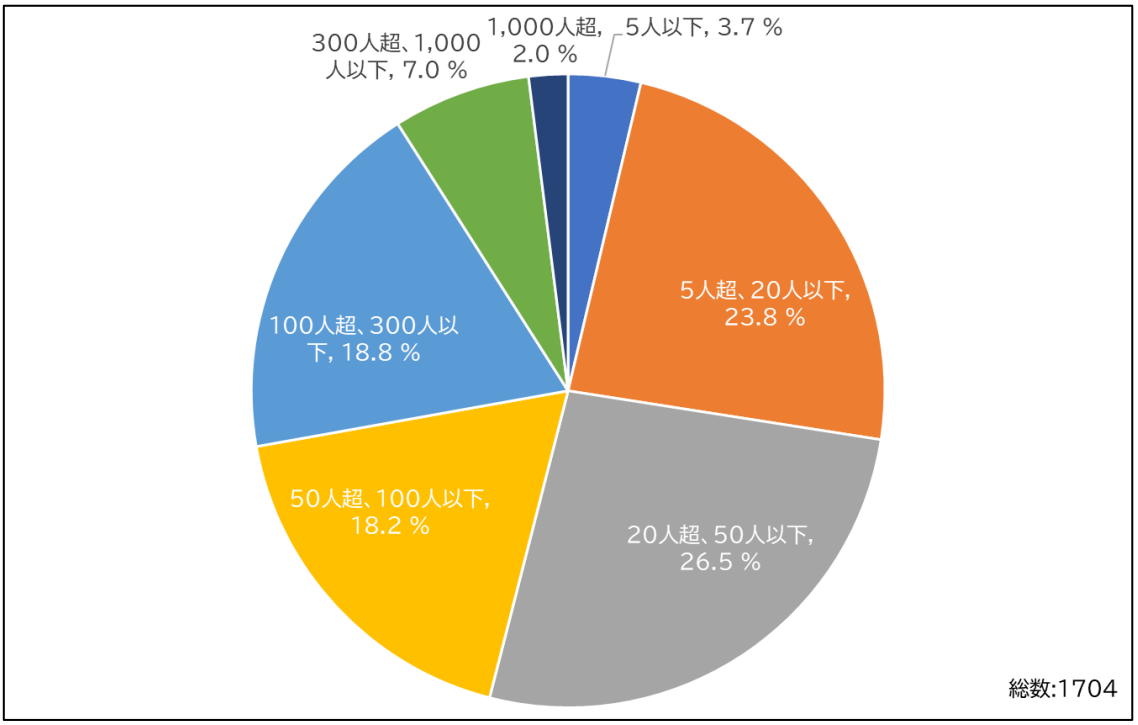

図 6 認証範囲の従業員数

ISMS 認証の運用実績等について

1. 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 段階に分類した。その結果、「10 年超」(43.2%)、「5 年超、10 年以下」(23.1%)、「1 年超、3 年以下」(14.6%)、「3 年超、5 年以下」(12.6%)、「1 年以下」(6.5%)の順となった(図 7)。

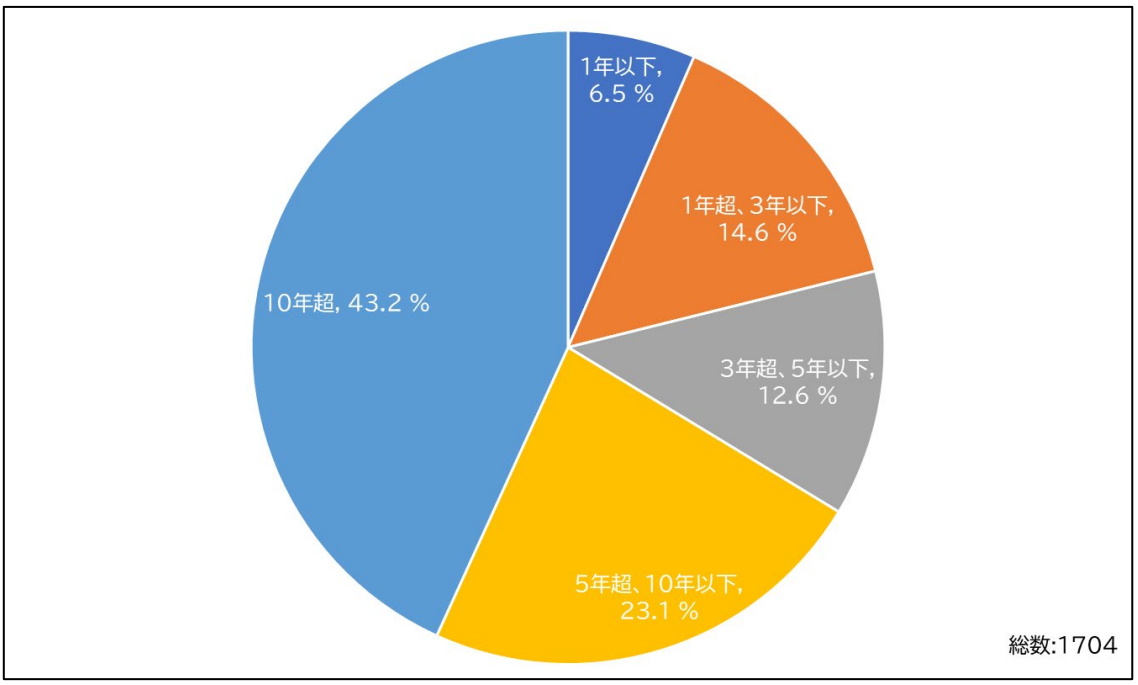

図 7 経過年数

2. 他のマネジメントシステム認証

(1)現在取得している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システム認証取得をしているかを尋ねた結果、「プライバシーマーク」(56.4%)、「ISO 9001(品質)」(48.2%)、「ISO 14001(環境)」(25.2%)、「ISMS クラウドセキュリティ認証(クラウドサービスプロバイダ及びクラウドサービスカスタマ)」(8.5%)、「ISO/IEC 20000(IT サービス)」(5.0%)の順となった(図 8)。

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。

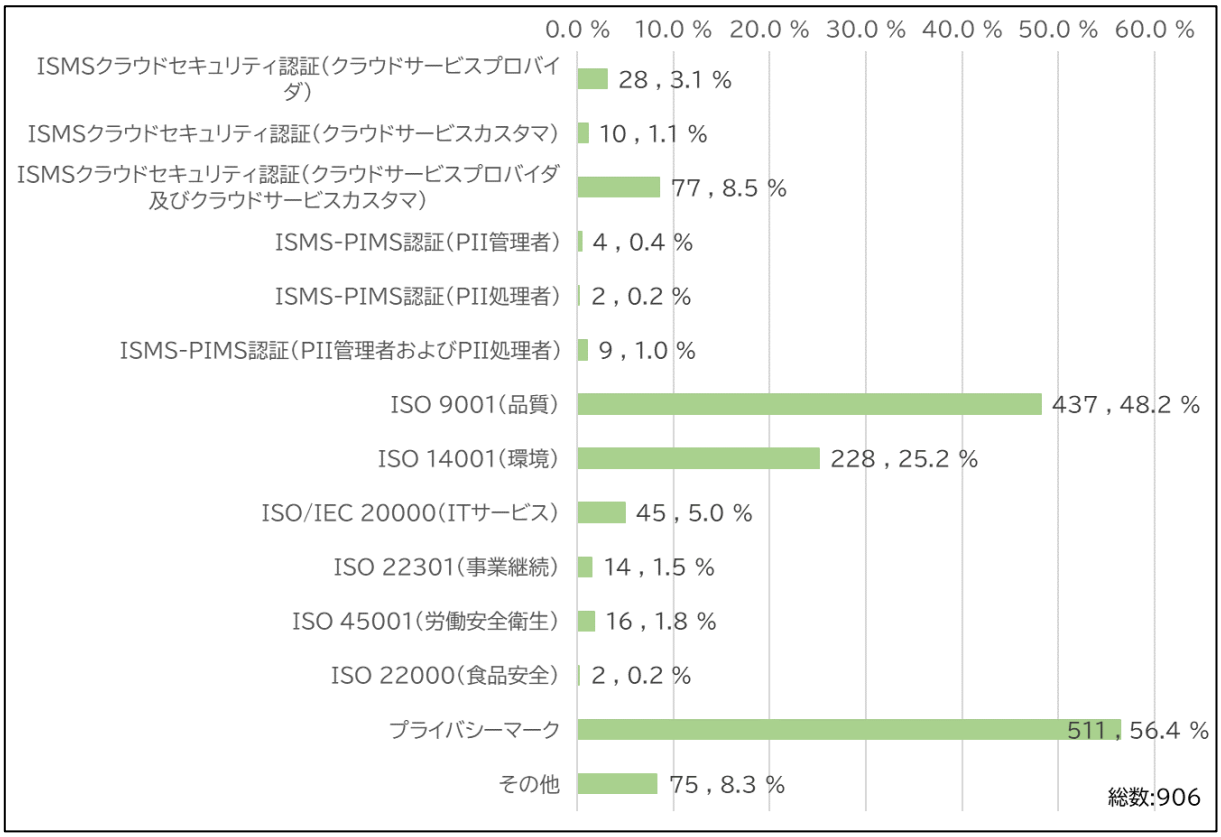

図 8 他のマネジメントシステム認証

(2)過去に取得していた他のマネジメントシステム認証

過去にマネジメントシステム認証を取得していて、現在は取得していないマネジメントシステム認証はあるかを尋ねた結果、「プライバシーマーク」(53.5%)、「ISO 9001(品質)」(27.7%)、「ISO 14001(環境)」(21.3%)であった(図 9)。

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。

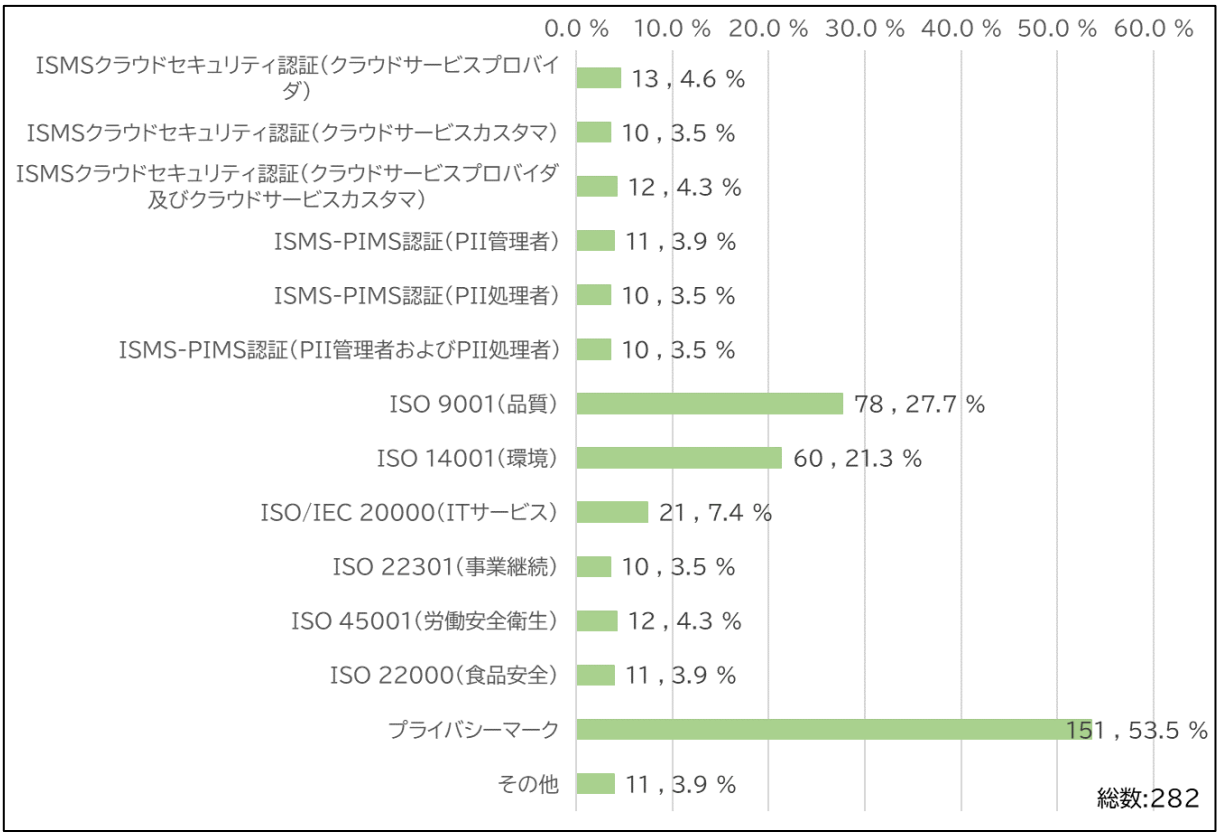

図 9 過去に取得していた他のマネジメントシステム認証

3. 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」(70.0%)、「変更を考えたが、実行していない」(12.6%)、「1 回変更した」(15.9%)、「2 回以上変更した」(1.5%)となった(図 10)。

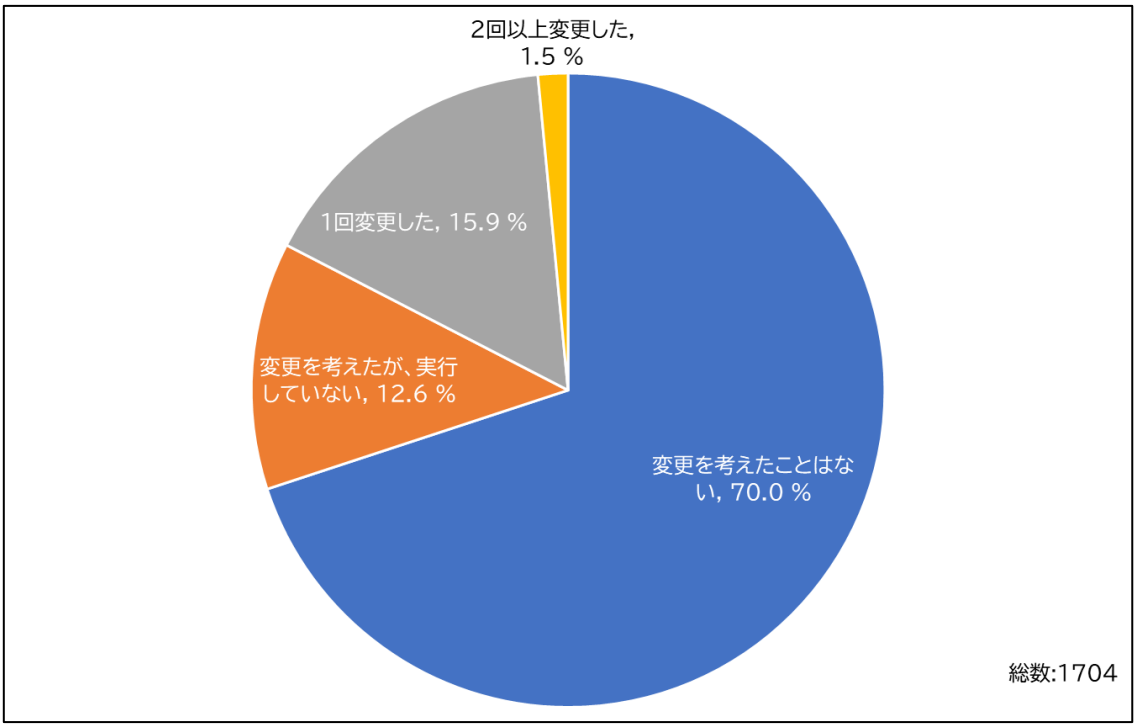

図 10 認証機関の変更

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 512 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 61.3%を占めた。

表 4 認証機関の変更に関する理由

		回答件数(件)	割合(%)
1	審査内容(深さや指摘内容等)が不満	57	11.1
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	41	8.0
3	審査料金の比較	314	61.3
4	その他	100	19.5
合計		512	100.0

ISMS の導入及び認証取得の効果等について

1. 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 11 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「顧客からの信頼を確保するため」(84.7%)で、「組織の情報セキュリティ対策の強化のため」(81.2%)、「組織の情報セキュリティ管理体制の強化のため」(80.3%)が続く。一方、「該当する」の回答が最も少ないものは「同業他社との差別化、営業上の優位性の確保のため」(51.9%)であった。

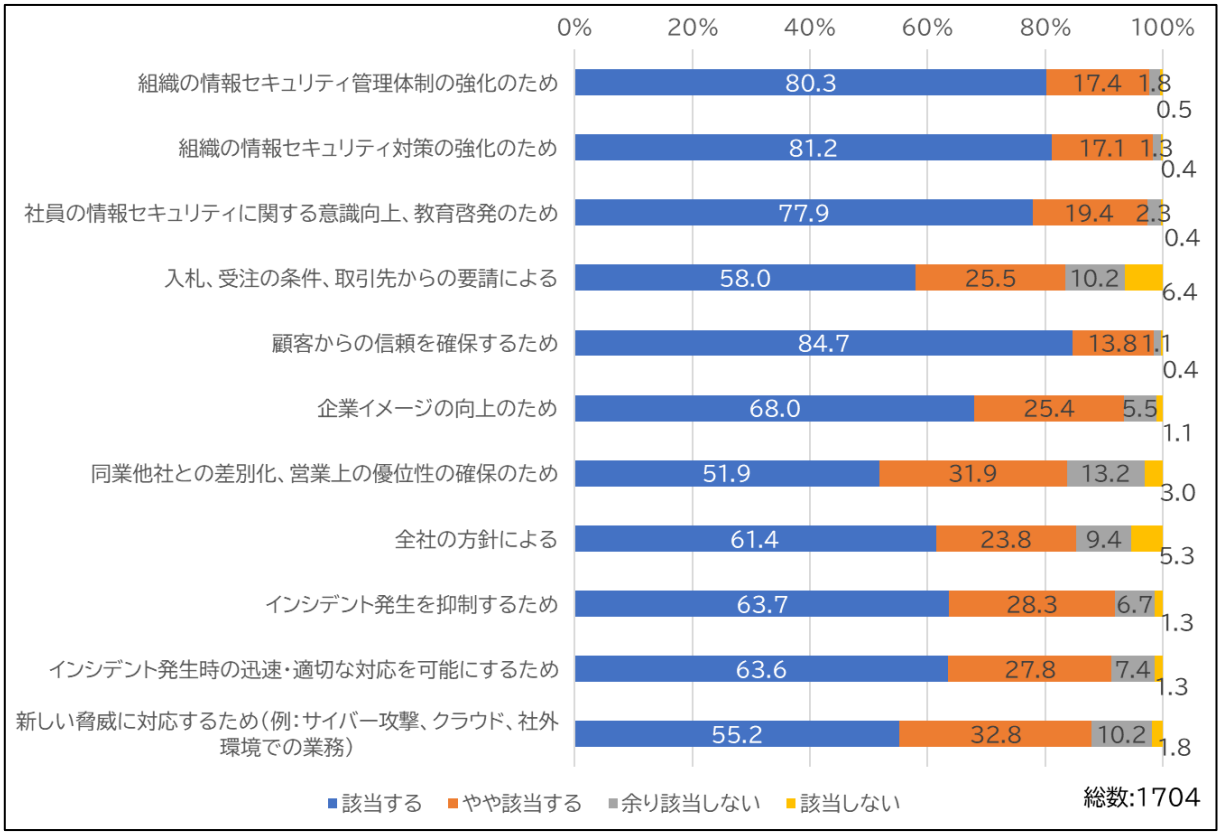

図 11 導入の目的又は動機

前問の各項目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。

- コンプライアンス、内部統制の強化のため。
- 定期的に認証機関の審査と情報セキュリティチェックが入ることで、マネジメントシステムの維持向上を効果的に実行できるため。
- 社員の意識改革、情報セキュリティに関するリテラシーの向上のため。
- 個人情報(顧客情報)保護の観点から、情報漏洩事件・事故を起こさないため。
- 情報資産をあらゆる脅威から守り、事業継続を確実にするため。

2. 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 12 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「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」(71.6%)、僅差で「組織の情報セキュリティ管理体制が強化できた」(70.5%)、「組織の情報セキュリティ対策が強化できた」(70.2%)が続き、次いで「経営者の情報セキュリティに対する関与が深まった」(57.2%)となった。一方、「該当する」の回答が最も少ないものは「営業上、同業他社に対する優位性の確保に貢献した」(34.7%)、「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」(36.4%)となった。

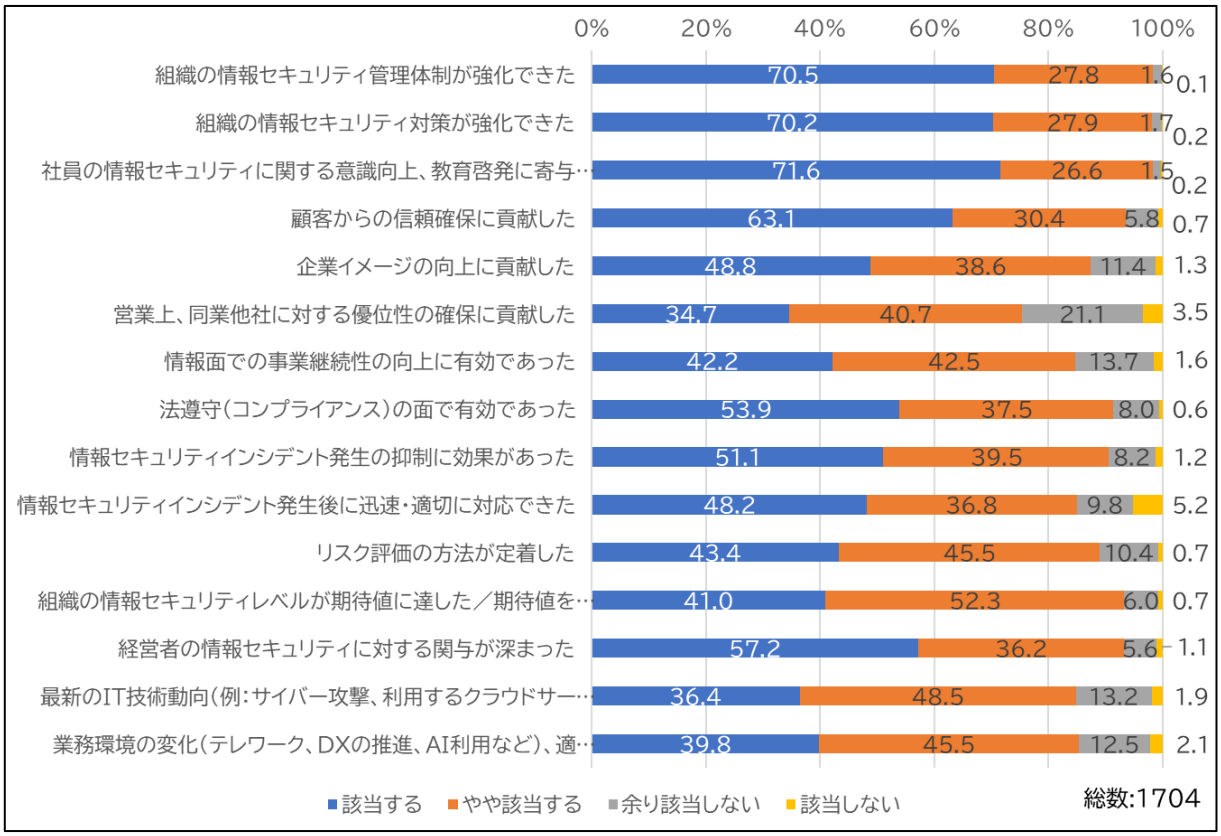

図 12 ISMS 導入の効果

前問の各項目で「該当する」を選択した場合、また各項目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。

- 内部、外部の要求事項を満たす為にどういう活動を行う必要があるのかを考えて行動することができるようになった。常に新しい脅威の情報を社内に展開できるようになり、結果大きなインシデントに発展するリスクを低減できている。 トップマネジメントで経営層が指示したセキュリティ対策や教育についての定量的なレポートを受け取れるようになったため、セキュリティ投資への理解も深まっている。
- リスクアセスメントの意識が非常に高まり、それに対する管理策や対策を自発的に考えられる組織になった。またトラブルを未然に防ぐ取組みも各個人が責任を持って対応できているため、これまでセキュリティ事故

が発生した事象もない。

- 顧客からの信頼確保という点で、セキュリティ要求が上がる昨今に認証取得が大きく貢献していると感じる。
- 情報セキュリティに関する環境整備が推進され、また社員教育や内部監査の実施により社員の意識向上につながった。
- 審査を通して審査員からの指摘等により、より効果的な情報セキュリティ環境構築を向上できた。
- 体制の整備と対策の強化として、ISMS 推進事務局を組織し、部署年度目標を立て、インシデント発生防止のための教育、状況把握等を行い再発防止に繋げている。
- ISMS を通じて確立された情報セキュリティのノウハウが、就業規則の改訂等を通じて他部署にも良い影響を与えている。
- ISMS を導入することによって、当社の情報セキュリティ管理体制と安全対策の強化や、セキュリティインシデント発生の抑制、社員の情報セキュリティに関する意識の向上を実現することができました。最新の IT 技術動向、業務環境の変化（クラウドサービス、AI の利用など）に応じられるセキュリティ対策の策定、そして人材の育成・確保などは今後の課題と認識しています。
- 社内にて情報セキュリティの体制が整っていたため、セキュリティインシデント発生時にも、どのように対応すべきかが明確であり、迅速に対処することができました。
- 情報面を含めて広義に事業継続性を検討し、災害やパンデミックに備えてきた結果　新型コロナウイルス感染症の流行時も適時適切な対応を展開できた。

3. 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（登録証）の他に要求されたことがあるかを尋ねたところ、図 13 に示す結果となった。

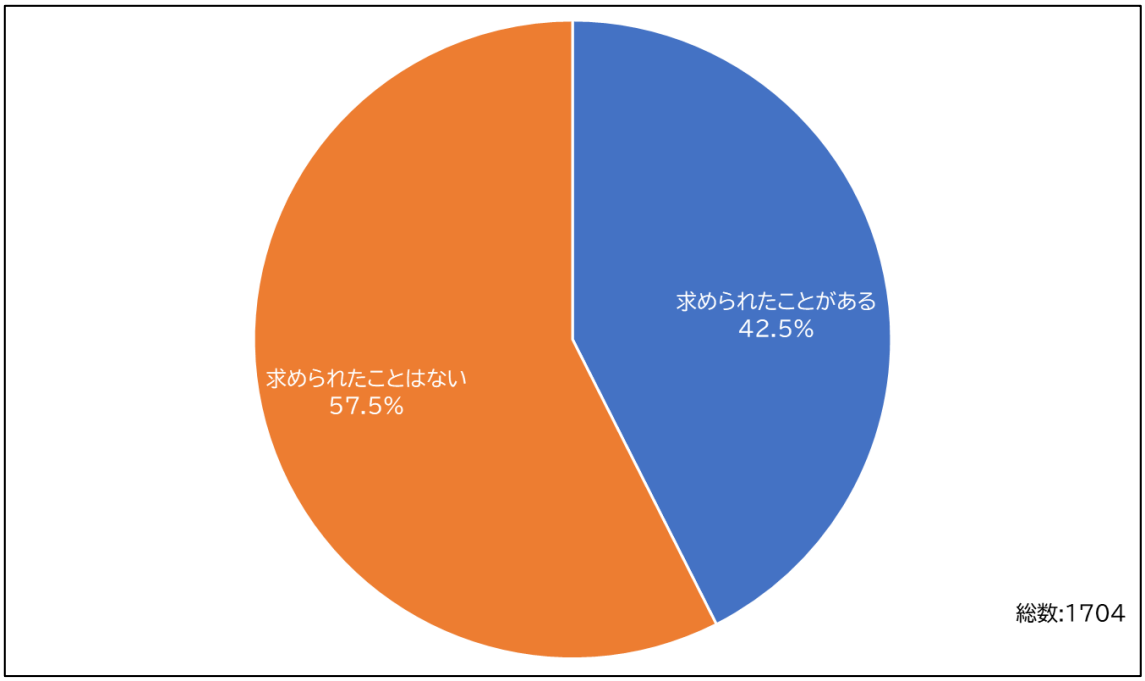

図 13 登録証以外に求められた経験

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図 14 のとおり。

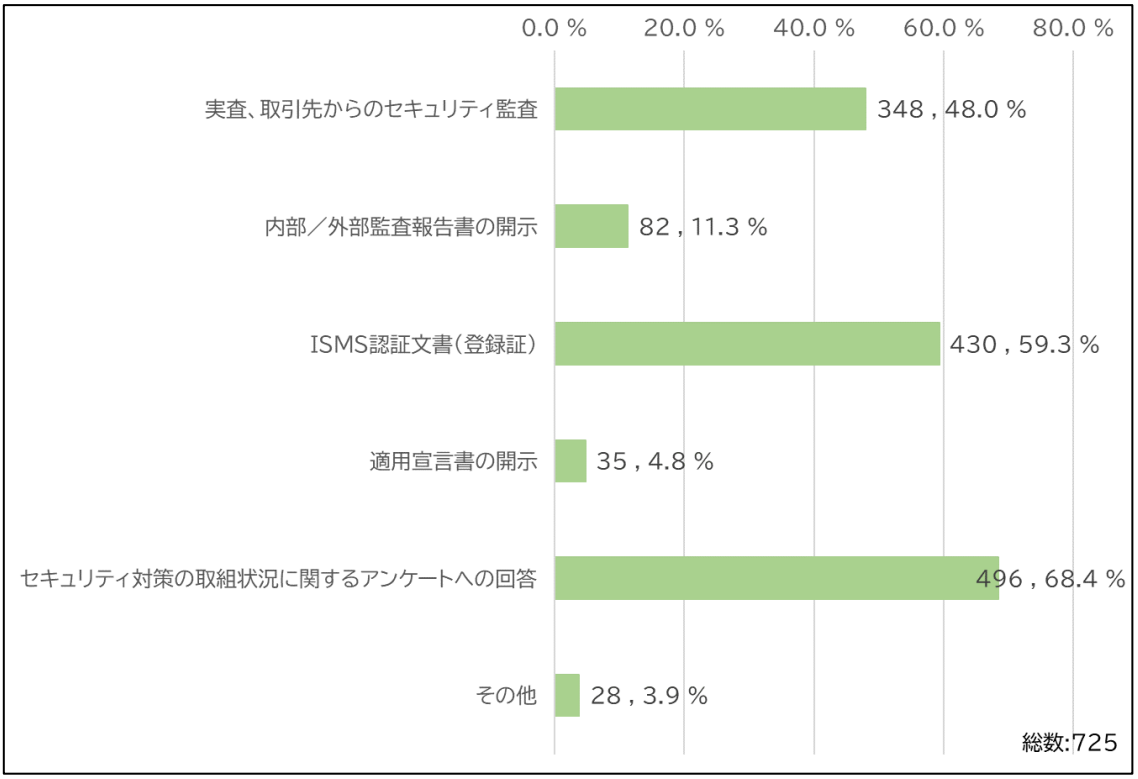

図 14 要求された項目

4. 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、「人材の確保、育成」(54.2%)、「マンネリ化・形骸化」(50.8%)、「組織内の情報セキュリティ教育・意識向上」(46.7%)の順となった(図 15)。

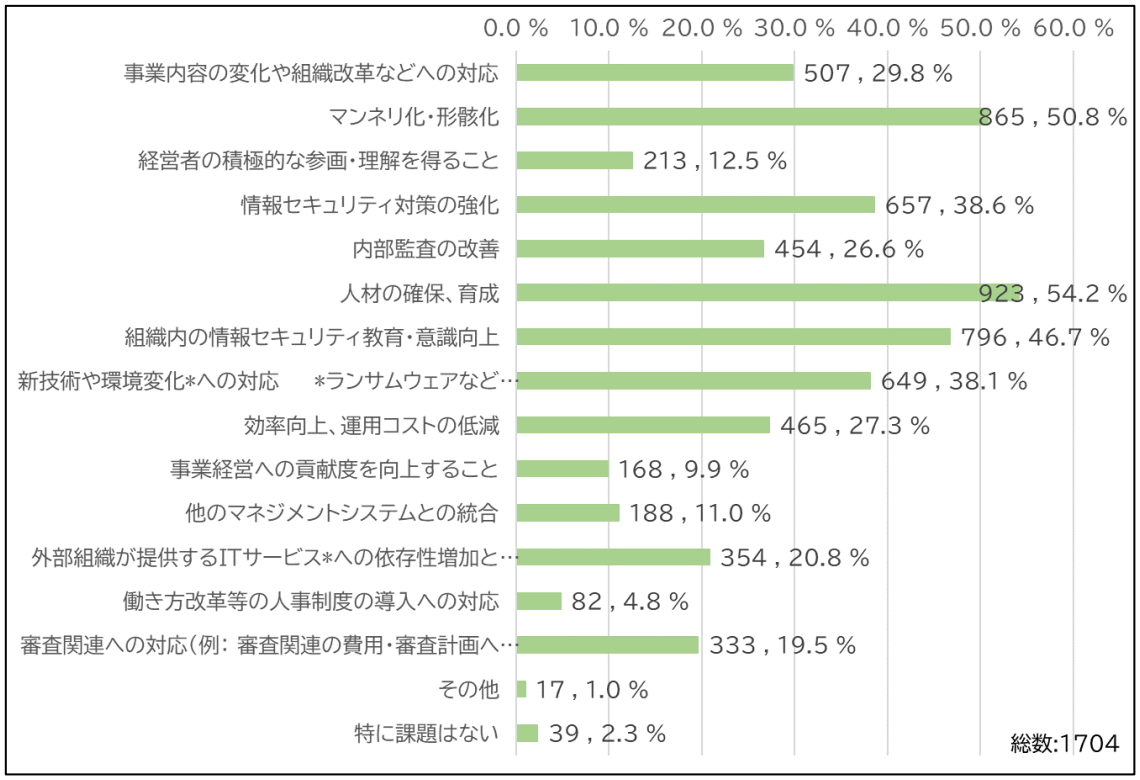

図 15 ISMS に関する今後の課題

上位3項目の主な内容は次のとおり。回答例の後ろにカッコ書きがある場合は、回答者の所属部署・役職を示す。

(1)人材の確保、育成

ISMS の運用に携わる要員については、第一に ISMS 専任者の不足、後任者の育成、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く見られた。

この課題を認識している組織の回答者としては、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であった。

回答例を次に示す。

- ISMS のみならずセキュリティレベルを向上させるための人材が不足しており、採用が急務。
- ISMS の運営として、専任をつけるのは難しく、極めて一部で行っている状況がある。現状はそれで足りているが、将来的には不安がある。
- ISMS を推進する担当者や事務局の体制を維持する人員の確保や、後進の育成が課題。
- セキュリティ人材が不足しており、確保も難しい状況。

(2)マンネリ化・形骸化

マンネリ化・形骸化における具体的内容に関する記述では、ISMS の運用を行ういわゆる「事務局」に関するものが多い状況であった。その中でも「事務局要員の固定化・業務の属人化」、「業務の定型化」、「事務局の高齢化」などが多く見られた。次に、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「慣れによる関係者の意識の低下」、「ISMS の運用の固定化」という意見も多く見られた。

さらに、要員の定期的な教育・訓練は実施してきたが、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、新しい技術や情報の入手が滞っているという意見や認証取得の為の活動となってしまっているなどの意見がみられた。

これらの課題を認識している組織の回答者としては、ISMS 運営事務局が最も多く、その他、関連部署、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る。

回答例を次に示す。

- 認証取得してから 18 年が経過したが、ISMS 運営事務局の運営メンバーが初期メンバーのまま固定化・高齢化しており、最近の IT 技術の進歩やクラウドサービスなどの導入に、対応できていない。(ISMS 運営事務局)
- 少人数の組織であるため、ISMS 運営事務局のメンバーが限られてしまい、マンネリ化を招いている。
- ISMS 運営事務局は、情報資産の管理が形骸化していることを認識し、管理方法の見直しを行っている。
- 運営自体が毎年同じでマンネリ化している。特に教育は毎年変化を付けるのに苦労する。(ISMS 運営事務局)
- リスクアセスメント手法が一定の為、新しい脅威が出てこない。(ISMS 委員会)
- セキュリティ教育の部分ではレポート配信とセキュリティテストの実施を行っているが 効果を具体的に実感することは難しく、また継続するにつれてマンネリ化を感じる。
- 認証を維持するためではなく、本来的な目的達成のために、規格移行に合わせて、運営事務局の刷新を図る。

(3)組織内の情報セキュリティ教育・意識向上

組織内の情報セキュリティ教育においての課題は、まず、その対象となる範囲として、全社教育を課題とされる意見が多く見られた。また、経営層、ISMS 事務局要員、情報システム部門、一般社員などの役割、所属部門毎に必要と思われる情報の入手・提供についてや、それぞれに必要な力量を満たす教育の実施方法などの課題も多くあった。

また、ほとんどの回答において、定期的になんらかの教育を実施されているが、その教育のコンテンツの整備、教育の実施頻度・タイミングなどを課題とされている回答が多くあり、かつ、教育実施後における効果測定方法や理解度の差についての課題が多い結果である。

この課題を認識している組織の回答者としては、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。

- 全社施策であるセキュリティ教育のほかに、認証範囲のサービス部門においても別途業務に特化したセキ

ュリティ教育を実施している。

- 新卒、キャリア採用者の入社時は一時的なレベルの低下が起きる懸念があり、各組織内での教育、あるいは全社教育計画に則り、一定のレベル感を維持する必要はある。
- 事業部門において、インシデント管理・資産管理・リスクアセスメントなどの活動において、適切な力量を有したスタッフの教育育成や自らの事業部門における取組の向上・改善に課題がある。
- 何度教育を繰り返しても標的型メール訓練で一定以上の開封者が出ており、セキュリティ意識が根付かない。
- 教育を行っていてもインシデント時に報告が滞る事態があったため深度化を図る必要がある。（ISMS 運営事務局）
- 情報セキュリティに関する社内研修を１回/年に実施しているが、なかなか意識の向上に繋がっていない部分がある。
- 情報を取り扱うことに関連するリスクについて、従業員の理解や認識はいまだに不足していると考えられる。セキュリティ運用を当たり前に実施してもらえるように、教育や意識向上のための仕組みづくりを推進していきたい。

審査員の力量及び審査の質について

1. 審査員の力量

(1)最近受審した審査での審査員の力量

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 16 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、「マネジメントシステムに関する知識及び業務経験」(74.2%)、次いで「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」(72.5%)、「コミュニケーション能力」(70.5%)、「審査技術」(70.5%)、「改善課題を指摘する能力」(68.1%)、「受審組織の業務に対する理解」(63.0%)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。

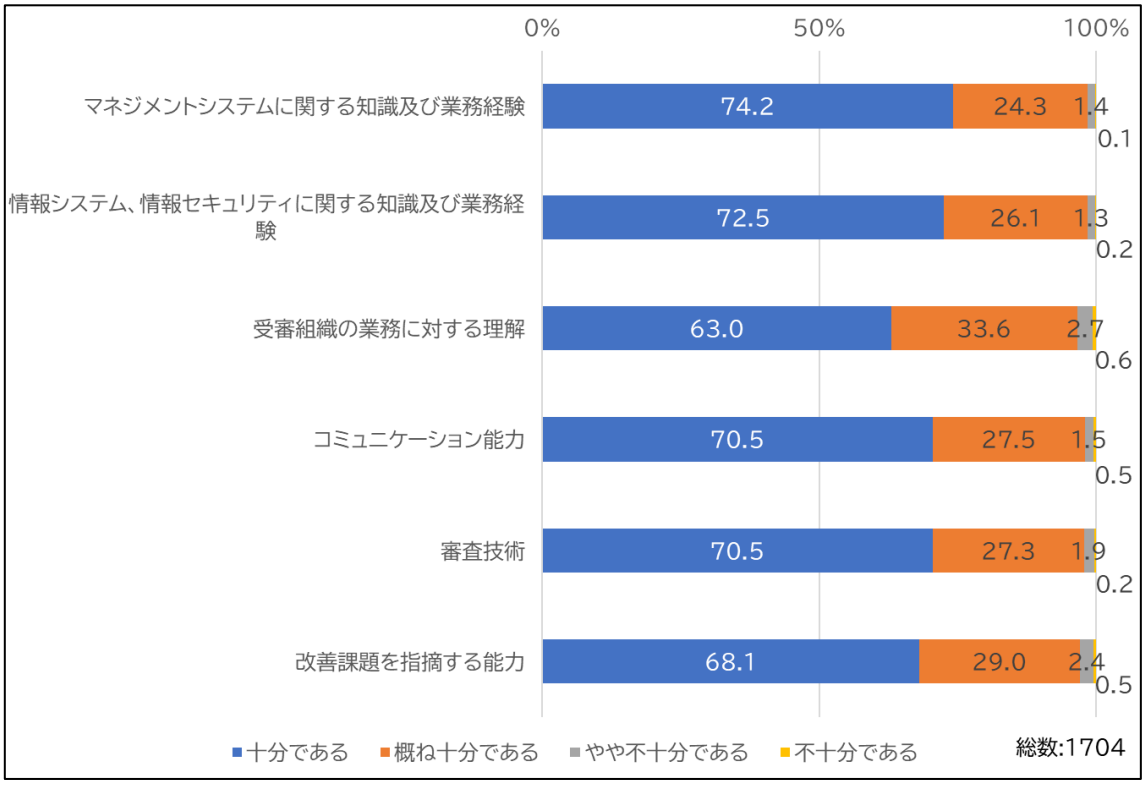

図 16 審査員の力量

(2)経過年数とのクロス集計

審査員の力量に関する6つの項目の評価結果について、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。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。その傾向は、特に「マネジメントシステムに関する知識及び業務経験」、「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」、「審査技術」の項目において顕著に表れている。

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。ISMS 認証を取

得してから 10 年を超える組織が 4 割を超えている中で、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。

(a)マネジメントシステムに関する知識及び業務経験

マネジメントシステムに関する知識及び業務経験について、ISMS 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 17 に示す。

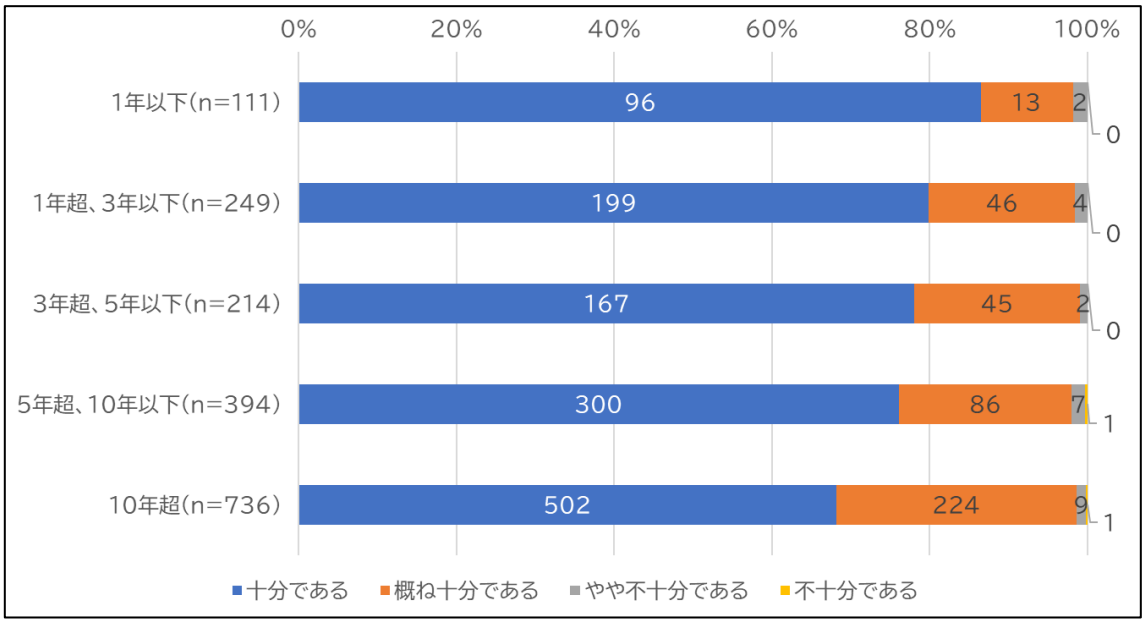

図 17 マネジメントシステムに関する知識及び業務経験と経過年数

(b)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

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について、ISMS 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 18 に示す。

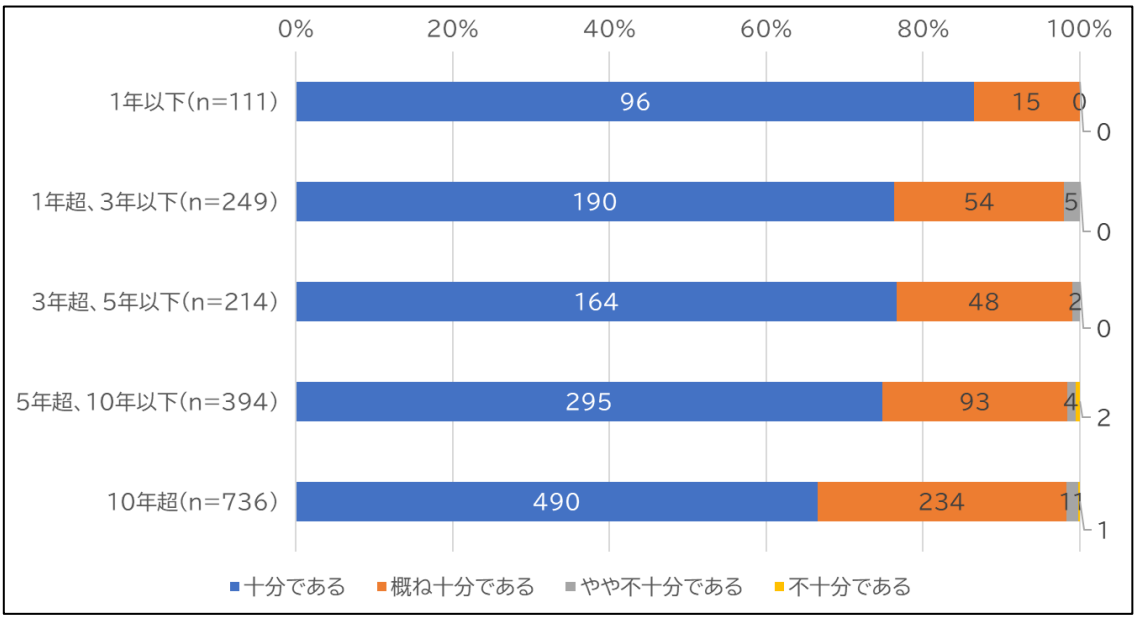

図 18 情報システム、情報セキュリティに関する知識及び業務経験と経過年数

(c)受審組織の業務に対する理解

受審組織の業務に対する理解について、ISMS 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 19 に示す。

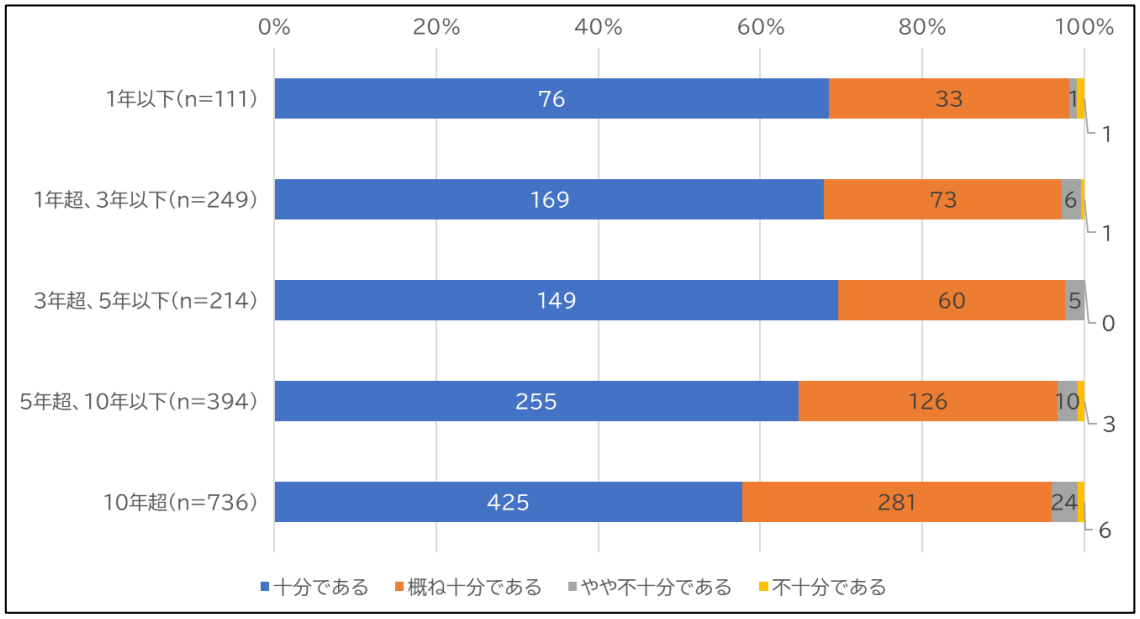

図 19 受審組織の業務に対する理解と経過年数

(d)コミュニケーション能力

コミュニケーション能力について、ISMS 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 20 に示す。

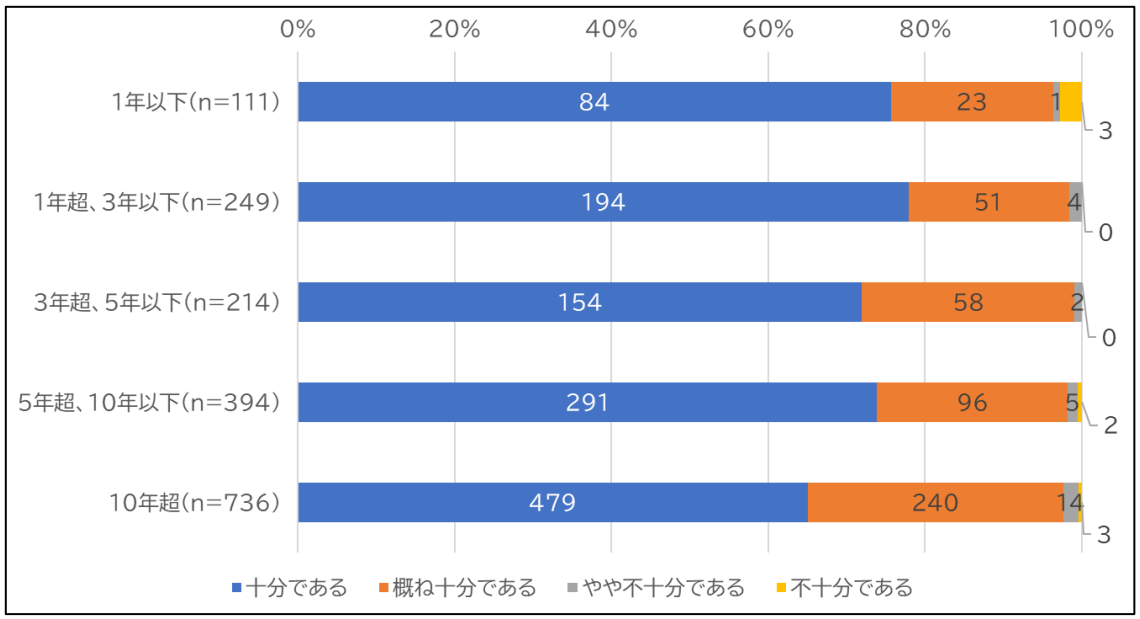

図 20 コミュニケーション能力と経過年数

(e)審査技術

審査技術について、ISMS 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 21 に示す。

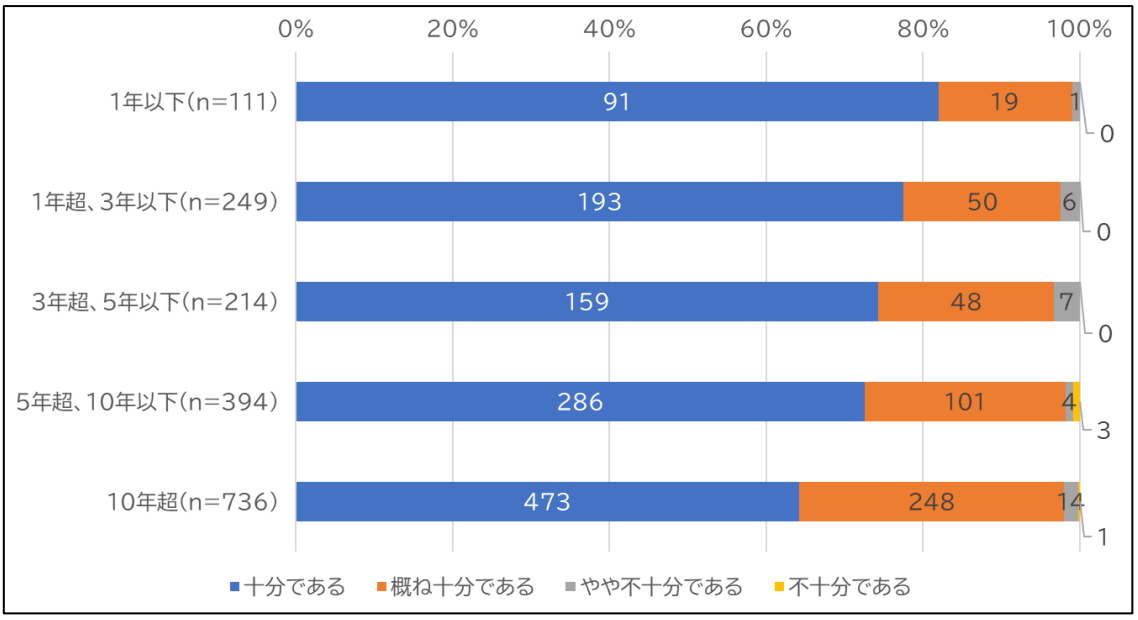

図 21 審査技術と経過年数

(f)改善課題を指摘する能力

改善課題を指摘する能力について、ISMS 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 22 に示す。

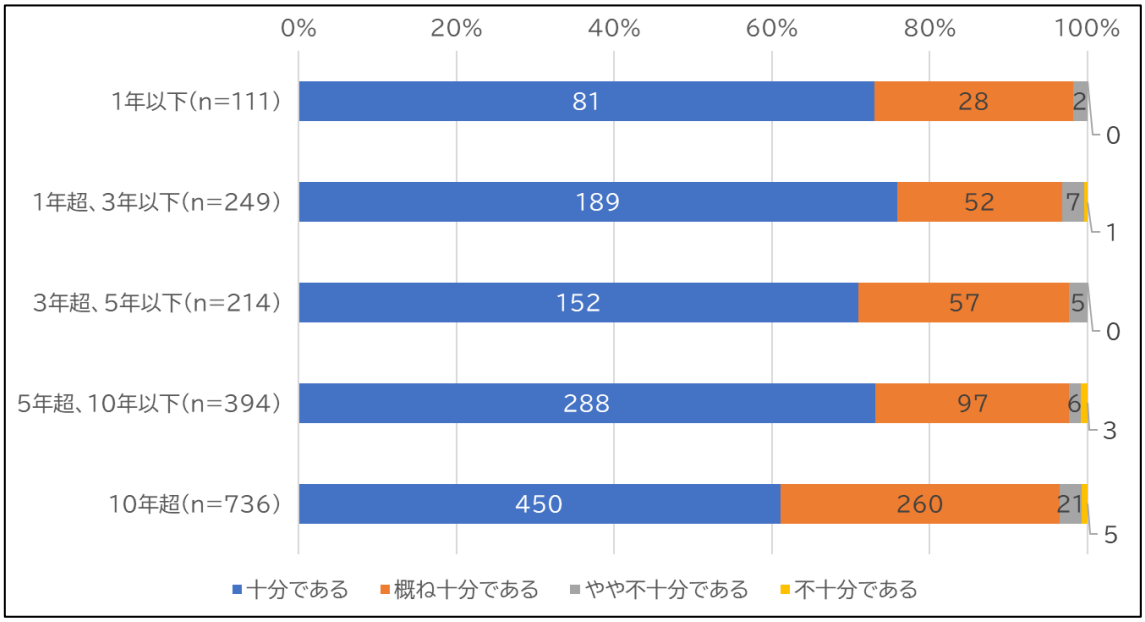

図 22 改善課題を指摘する能力と経過年数

2. 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

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の評価は、「満足」(76.8%)、「やや満足」(21.5%)、「やや不満」(1.4%)、「不満」(0.4%)であった(図 23)。

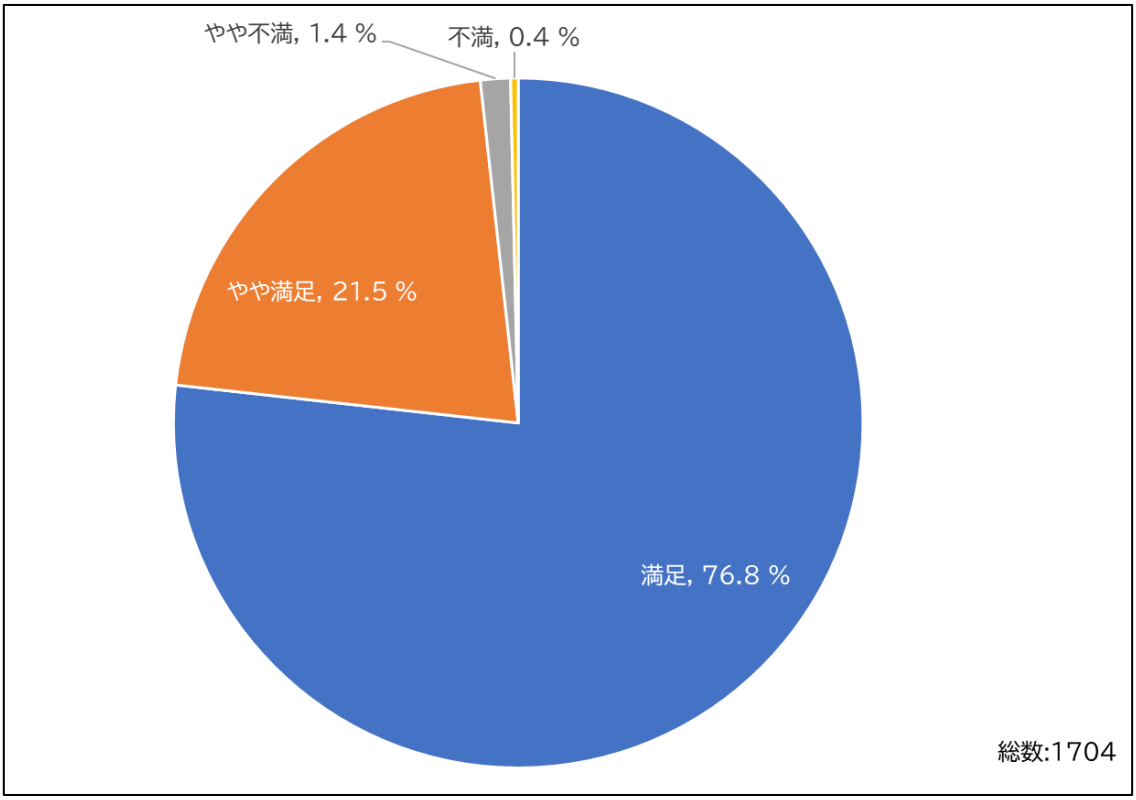

図 23 審査の内容(規格適合性)

「やや不満」、「不満」な点として指摘されたものの回答例は、次のとおり。

- QMS、EMS との複合審査の中で ISMS が埋没している。
- 限られた時間内のサンプリングなので困難とはいえ、潜在的な課題・問題点の追求に至っていないと思われる。
- 文書審査が中心。
- 情報セキュリティの視点だけでなく、事業プロセスから来るマネジメントプロセスとしての観点で審査して欲しい。
- 当社の事業分野、事業内容を、MS 運用体制を理解されて審査されているのか、疑わしいところがある。
- 指摘事項に対して十分な説明がされなかった。

・ JIS 規格の言葉の記載にとらわれすぎた指摘で、当社の業務上実体のないものまでマニュアル等に記載する必要があるのか疑問点があった。
・ 複数の部門に対するヒヤリング内容に一貫性が無く、場当たり的に質問しているように感じた。
・ 審査期間中のヒヤリングや確認が十分でなく、後日、メール等によって確認がおこなわれた。

(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」(76.2%)、「やや満足」(22.3%)、「やや不満」(1.3%)、「不満」(0.1%)の順であった(図 24)。

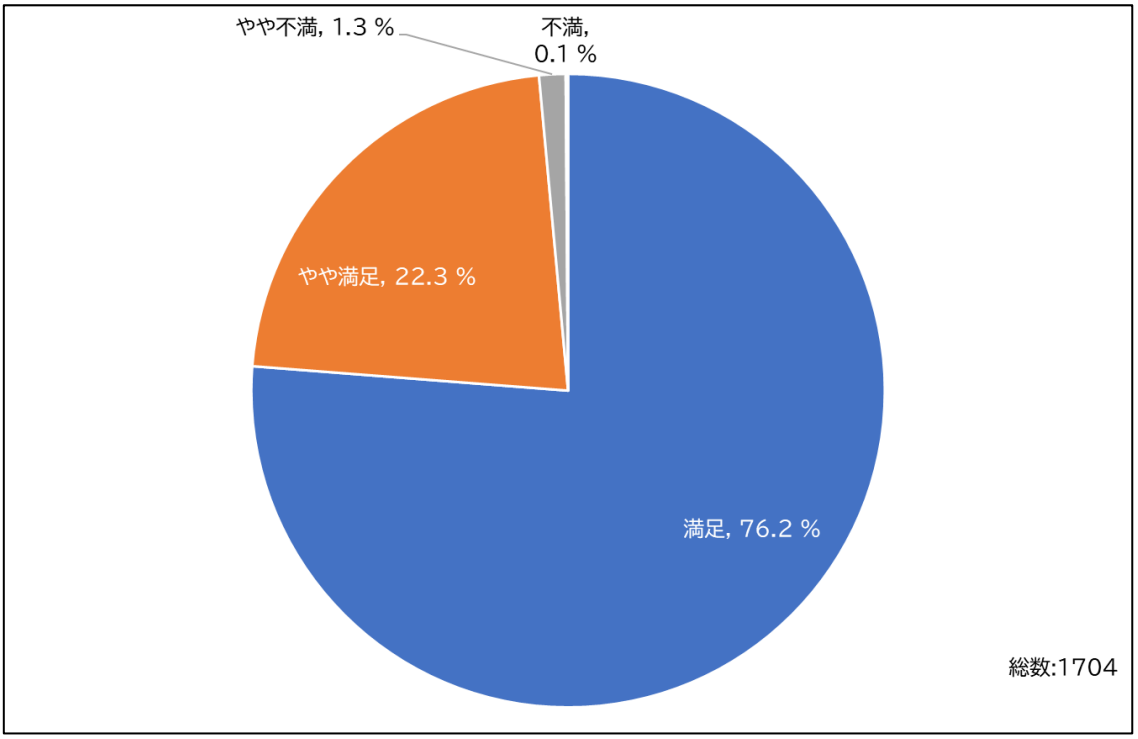

図 24 審査の内容(管理策)

「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。
・ 管理策個々への踏み込みが足りない。
・ 審査員によって、規格の解釈や指摘事項が異なる点や、改善課題の指摘内容について、情報セキュリティ面よりも、品質向上面(ISO9001)に偏っている指摘を受けることがあった。
・ あまり有用な指摘が上がっていない。
・ 企業規模や実態にそぐわない管理策を提案されることがある。
・ 弊社の主張について、審査員の意見を押し付ける。
・ 規定類等の書類審査重視であり、実務的な審査ではなかった点。
・ 審査員の力量の差が大きい場合があり、年度によっては不満が大きい場合もあった。
・ サーベランス審査の審査員が毎年同じ方でマンネリ化している。

(2)審査の時間

審査の時間の評価は、「適切」(79.6%)、「長い」(14.4%)、「短い」(0.8%)、「何とも言えない」(5.2%)であった(図 25)。

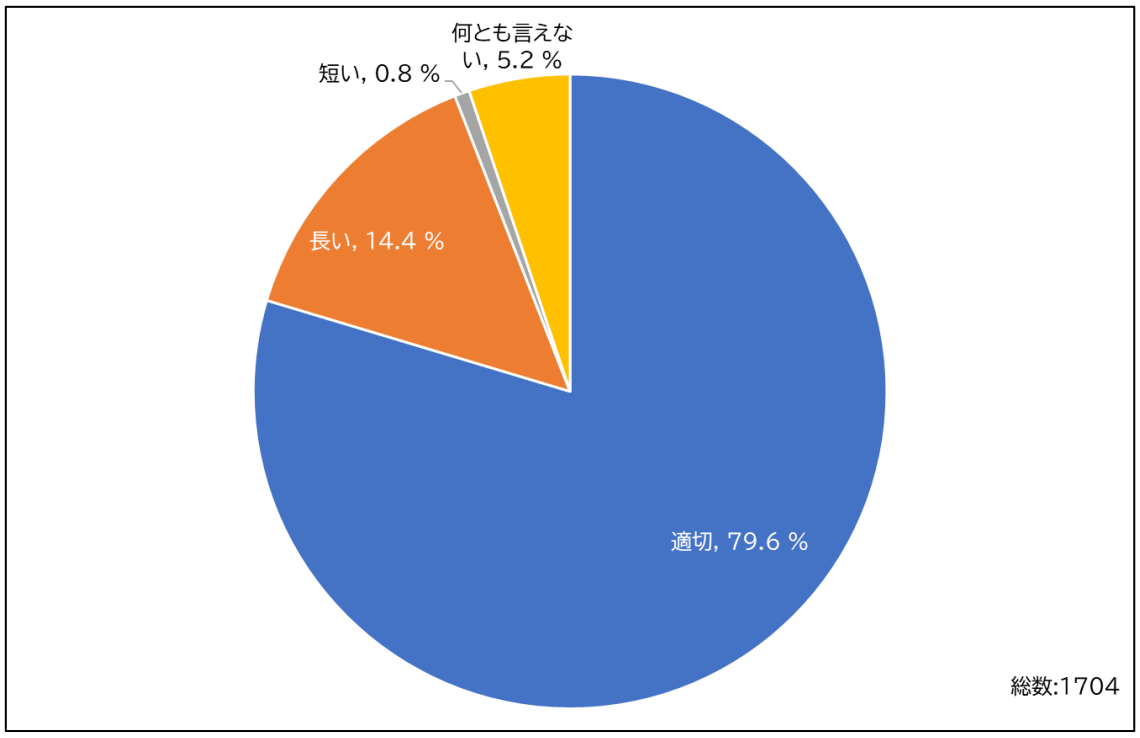

図 25 審査の時間

(3)審査の所見・指摘の有効性

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」(54.0%)、「大いに役立った」(44.3%)、「あまり役立たなかった」(1.5%)、「役立たなかった」(0.1%)であった(図 26)。

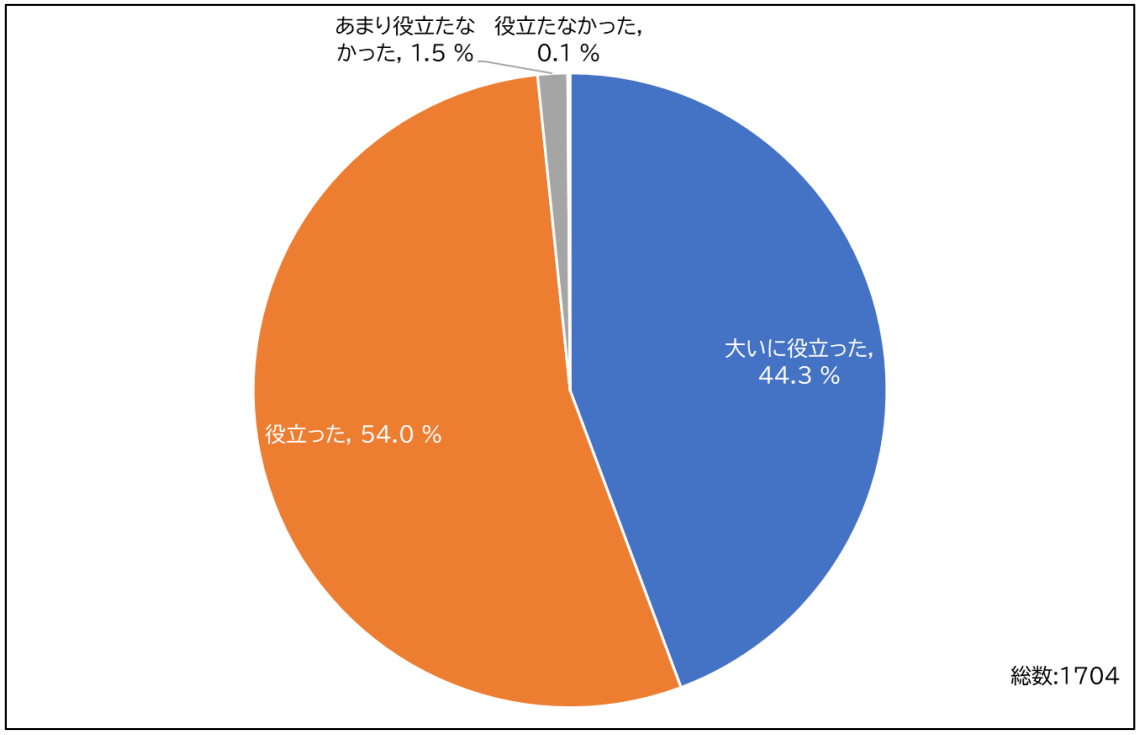

図 26 審査の所見・指摘

「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。

- 審査員によって審査員の出したい不適合ありきで、審査されているように感じることが多くある。
- 何かしらの観察事項を指摘しなければならないから指摘している感じがする。
- 杓子定規な審査、指摘事項だった。
- 情報セキュリティ面での指摘ではなく、業務品質向上に関する指摘を受けることがあった点。
- 指摘事項が不明確。
- 指摘事項に本人の思い込みがあり説得力にかける。
- 指摘された観察事項のほとんどが、改善すべき課題にならなかった、当社業務のための指摘ではなく、ISMS のための指摘。
- 規程類等の書類審査重視だったため書類の整備にかかる指摘が多く、実務的な運用にかかる指摘はなかった点。
- 審査員の指摘(推奨)する管理レベルまで必要と判断していない。
- セキュリティに重きがあり、やや古い審査に感じました。業務毎(プロセス毎)に沿った ISMS の活用を希望していたため。

(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」(77.4%)、「やや満足」(21.0%)、「やや不満」(1.4%)、「不満」(0.2%)の順であった(図27)。

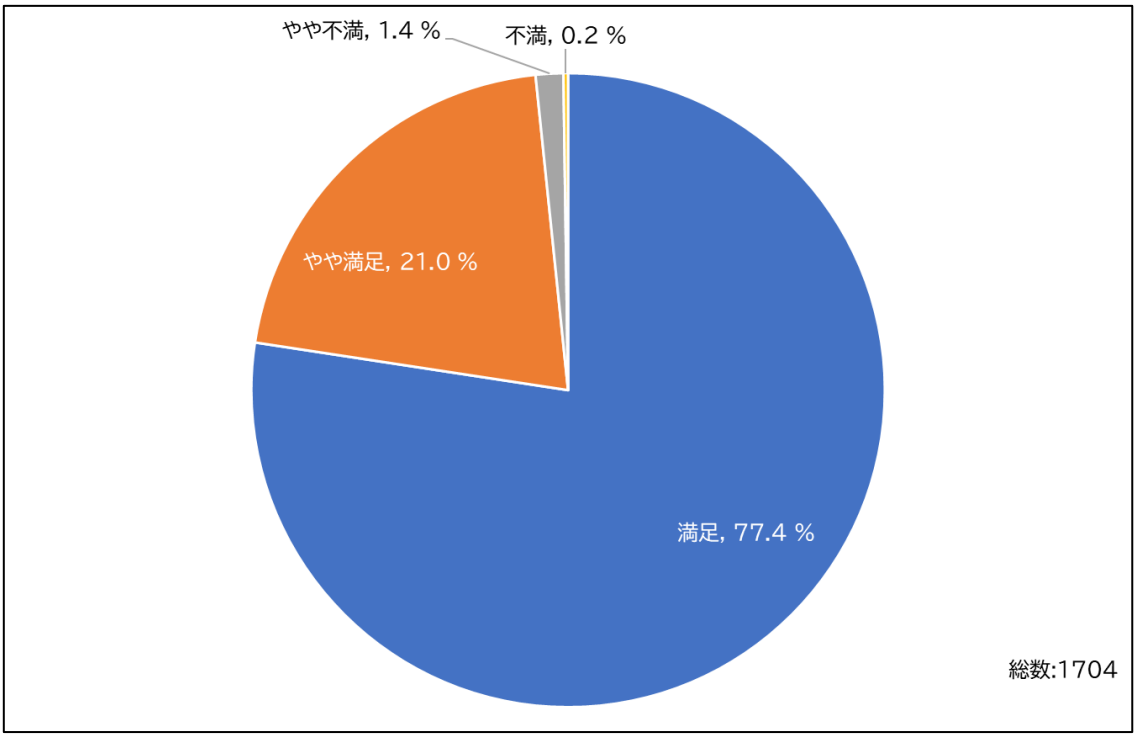

図 27 審査の質に対する総合評価

「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。

- ISMS に割く時間が少ない。
- 審査員のレベルに高低差が大きい。
- IT 関連の知識がやや古いように感じた。
- 業務内容を理解していないので、審査内容も浅い。
- 監査結果が組織の向上に役立つものではなかった。
- 審査が長時間かつ、指摘事項が不明確。
- 規程類等の書類審査重視であり、実務的な審査ではなかった点。
- 当社の事業分野、事業内容を、MS 運用体制を理解されて審査されているのか、疑わしいところがある。
- コロナ終息後も審査にリモートが導入されたこと。
- 審査以外の部分で、事前調整と事後フォローの質が低い。
- 指摘事項について、明確な指摘ではなく、審査員の個人的な意見と感じられた。

(5)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、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(図 28)。

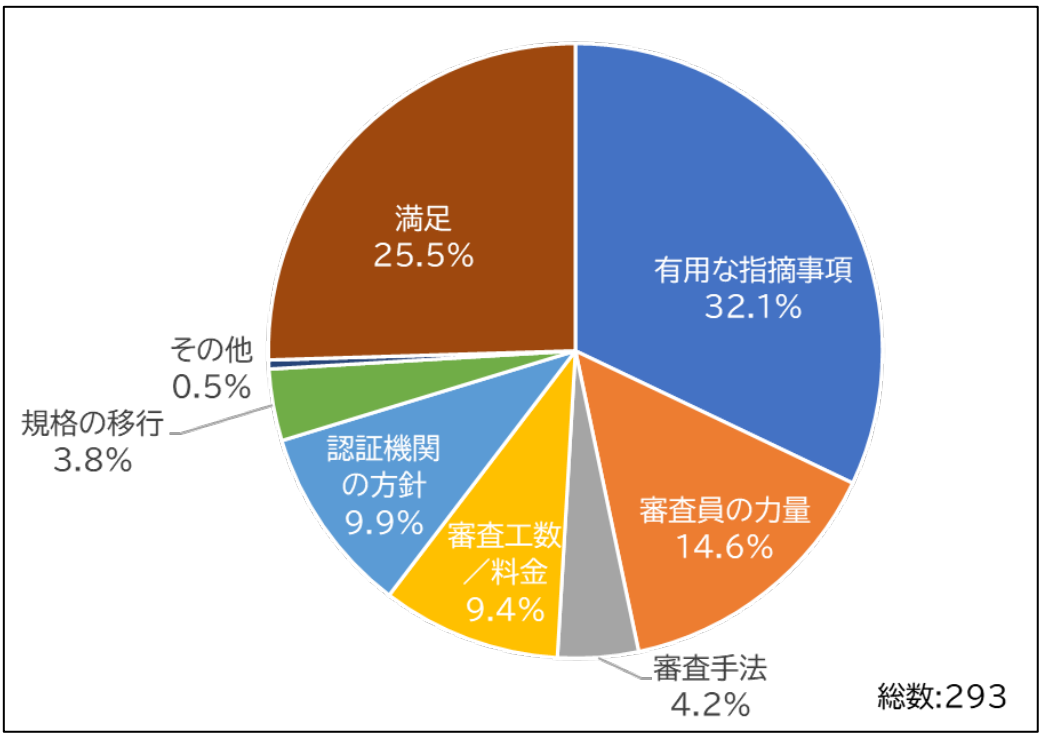

図 28 認証審査および審査員に対するご意見・ご要望

- 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。改善課題となり得る回答例を以下に記す。

- PDCA に役立つ気づきをご指摘いただきたい。
- ISMS でセキュリティなど強化しつつ、ISMS を利用して、社内体制および経営層含めた全従業員の意識改革を起こす審査を行っていただきたいです。
- マネジメントシステムが形だけでなく、実務に伴った形で有用化していくという観点からは、運用面等で実務に即した指摘やヒントが改善に繋がるような審査となればよい。
- 何かしら指摘されるとマネジメントシステム運用の負荷が増える場合が多いが、負荷が増えると手が回らなくなる部分も出て来て、全体として効果が上がらないか下がる事も危惧されるので、運用負荷の妥当性についても指摘してもらえると助かる。
- 業務と組織の規模に合わせた指摘になるとなおよい。
- 現在の規格内容に合った内容で、不要なものを削減したりコンパクトにする等のご指摘をいただきたいです。
- 弱点を見つけ出し具体的な指摘をしてほしい。
- 情報セキュリティに関する社会的要請が高まる中で、対応に関する最新の情報をアドバイスしていただければありがたい。

- 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。

- 弊社の業務と規格項目の関連の本質的な理解、関係ない無意味な作業を求めないように力量を高く保ってほしい。
- 審査する企業が属す業界の会社運営状況などなるべく詳しく調査理解した上で審査してほしい。
- 審査員の方の勉強会をもっと行っていただき規定を満たすだけの ISMS にしないでほしいです。
- 審査員の質にバラつきがあるように感じる。審査では、専門知識や経験豊富な審査員を要望している。
- 審査員毎の主観で審査をしているよう感じるため、審査機関で基準を統一してほしい。
- 情報セキュリティだけでなく、他のマネジメントシステムのスキルを身に着けて欲しい。
- 経験も大事ですが、新技術、社会の時流と当社の事業を理解して頂いて審査して欲しい。
- 若手の審査員の意見も聞いてみたい。

- 審査手法

この分類項目は、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。

- オンライン審査を特例ではなく前提での運用としていただきたい。（サイト訪問も現物保管は減少しているためあまり効果的ではないと考えます）。
- 新型コロナの時期にリモート審査で対応していただいた時期があったが、当社および審査員の移動を考慮すると、「移動時間の低減（経費削減）」や「審査部門のスケジュール調整」にメリットがあるので、リモート審査オプションがあるとよいと考える。
- 審査にかかる時間を短くしたい。 審査ドキュメントやワークフローには 改善の余地があると思う。
- 小規模事業者はトップマネジメントと総務部長などを兼ねていたりもするため、メンバーが変わらないのであれば、最後の報告は 1 回で十分。結果審査時間を 1 時間ほど減らしても問題がなかった。

- 審査工数/料金

全回答のうち、5．5％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。

- 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。

- 審査日程（工程）について事前にもっと詳細打ち合わせが必要と思われた。
- 業務内容の理解を深めてから審査計画を立てた方が効率的であったと思います。
- 連絡のレスポンスをもう少し早くしていただけると助かります。
- 組織の状況を深く理解していただきたいので、 可能な限り同じ審査員を派遣して欲しい。
- 審査員の対応には満足していますが、審査組織バックオフィスから画一的な応答しか得られないことは残念に感じています。

・　最終の審査報告書の記載ミス等があるので、推敲をしっかりお願いしたい。

● 規格の移行

この分類項目は JIS Q 27001:2023(ISO/IEC 27001:2022)への移行に関するもので、回答例を以下に示す。

・　新規格への移行審査に係る情報提供をお願いします。
・　規格の改訂時に注意すべき点のレクチャー、他社事例の紹介。
・　2022 年版への移行に際してアドバイスがあり、非常に有益であった。
・　移行を 2025 年に計画しており、そのための準備を行っているが、規程を素直に具体化した場合、情報セキュリティに関する設備導入にかなりの費用が掛かるように感じている。 企業経営に影響を与える可能性もある為、ある程度投資を妥協しなければならない部分も出てくるように感じるので、審査の際は、その背景を踏まえた判断をしていただくことを望む。

● 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。

・　余談やコンサルで時間を費やす審査員がいる中で、今回(直近)の審査員の方は非常に誠意を以て対応して頂けた感があります。
・　弊社の業務内容を理解していただいている審査員の方に担当してもらっているため、業務説明などのイニシャル工数がかからず助かっている。
・　審査員は数年固定でご担当いただけており、審査員が変更になる年の前年には引継ぎで二人来られていたので、審査を受ける側としてはコミュニケーションの構築等の負担が少なく助かりました。
・　現在弊社をご担当いただいている審査員様は、弊社の実状を理解しつつ、「どのような指摘をすることが、この会社にとって、より有効であるか」を非常に熟考されていると感じます。机上論だけでなく、こちらの心情や内情にも寄り添った上で、厳しくご指摘をいただけるような審査員様が今後も誕生することを、個人的には祈っております。

認証機関の認定の信頼性について

1. 認定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」(40.9%)、「やや重視した」(23.3%)、「多少は考慮した」(17.0%)、「まったく考慮しなかった」(18.8%)の順となった(図29)。

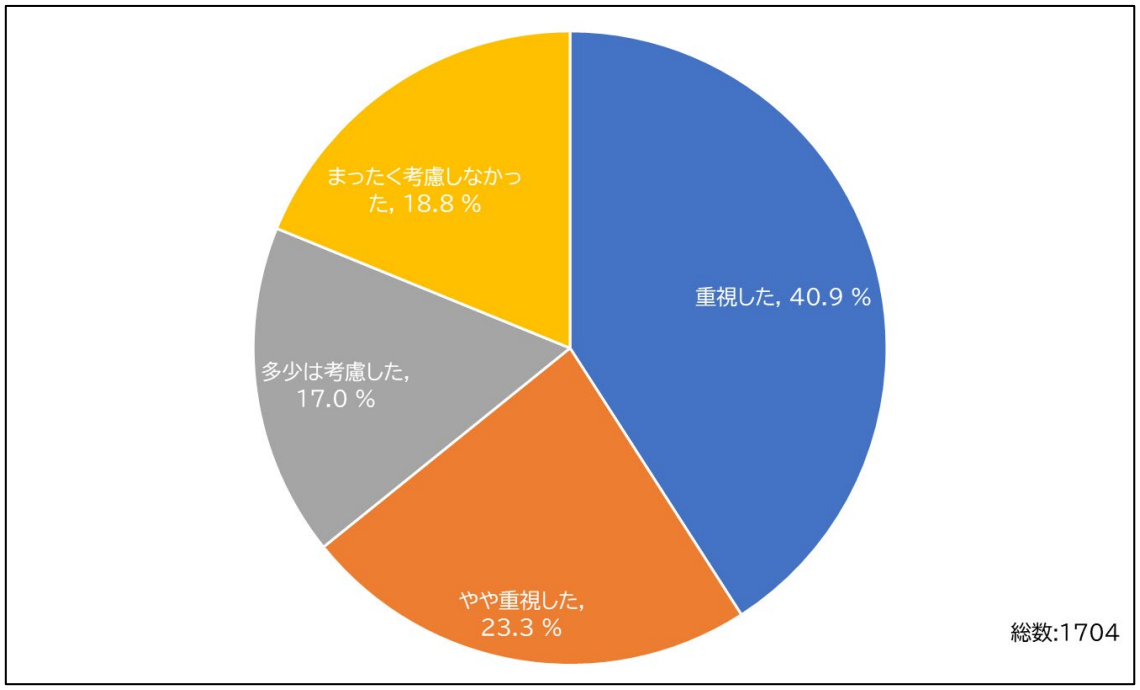

図 29 認証審査の認定の有無

(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」(37.6%)、「やや重視した」(19.6%)、「多少は考慮した」(19.2%)、「全く考慮しなかった」(23.6%)の順となった(図 30)。

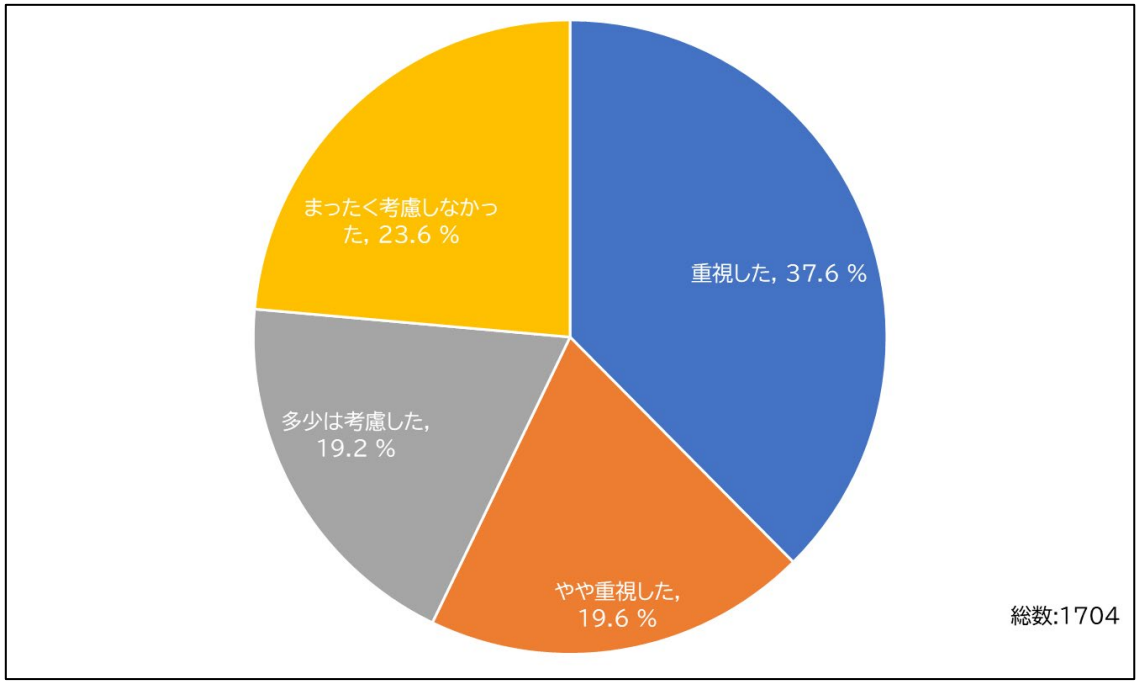

図 30 国内認定機関による認定

(3)認定シンボルの利用

名刺等で認証マークと併せて認定シンボル*を利用しているか尋ねた結果、「利用している」(75.6%)、「利用していない」(24.4%)となった(図 31)。

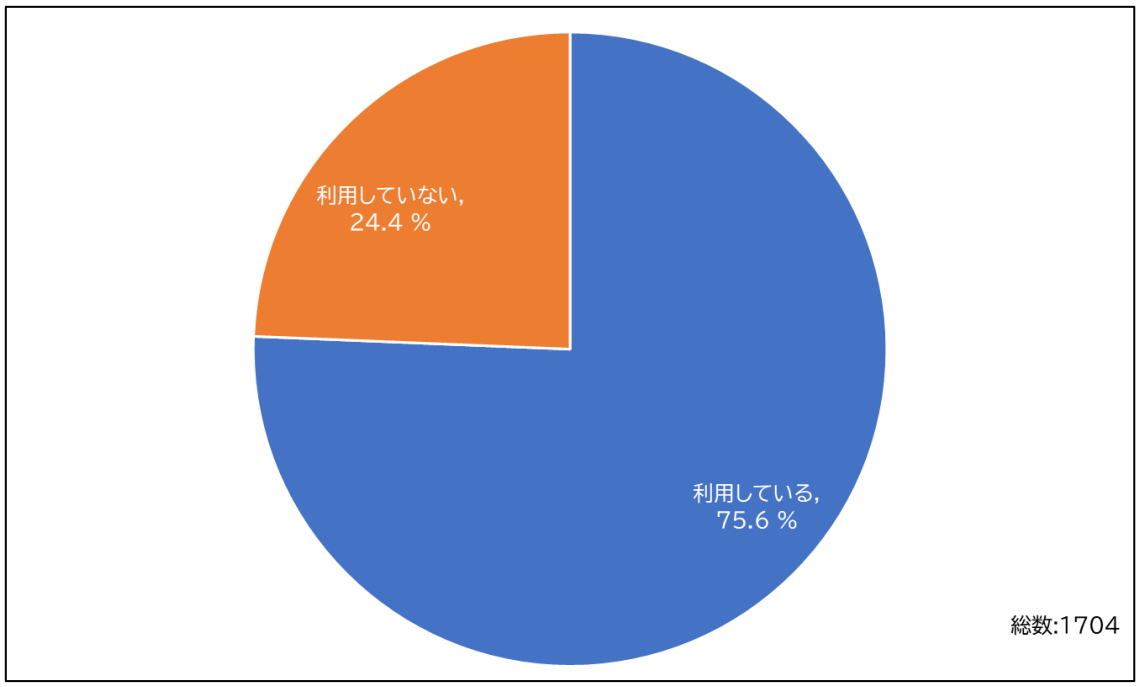

図 31 認定シンボルの利用

【*認定シンボル】

制度全般に対するご意見等

1. 調達先への要求

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」(46.3%)、「確認のみ実施したことがある」(35.3%)、「確認したことはない」(18.4%)の順となった(図 32)。

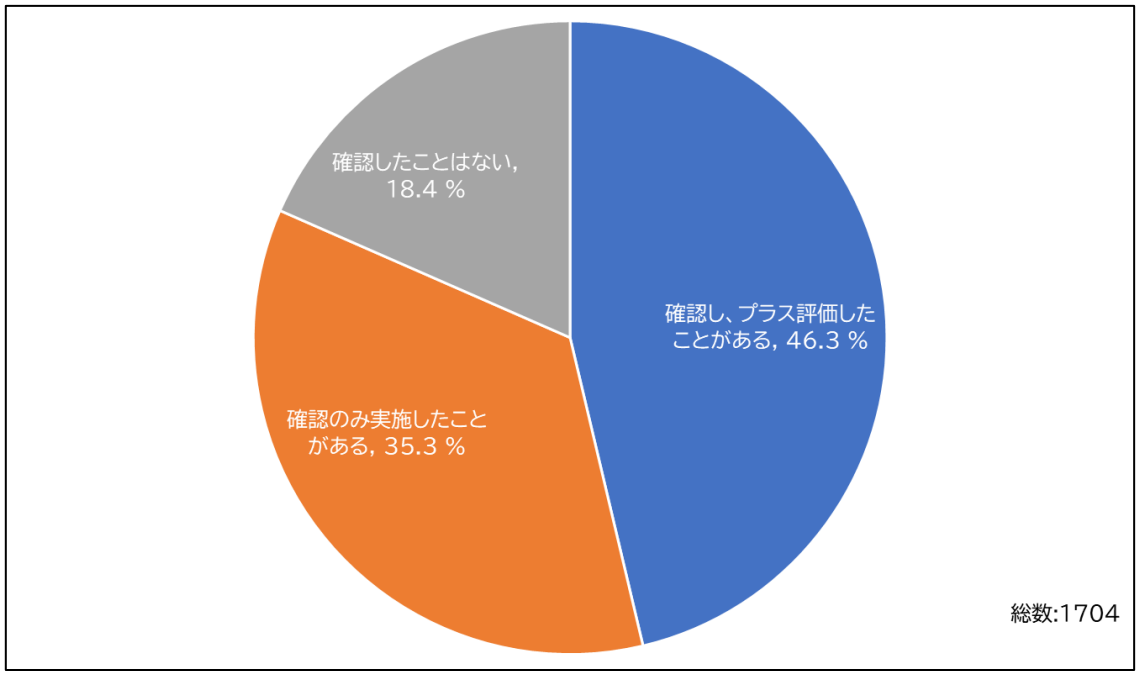

図 32 調達先への要求

2. 海外展開

(1)海外展開の有無

海外展開の有無について尋ねたところ、「海外展開している」(13.1%)「海外展開していない」(86.9%)となった(図 33)。

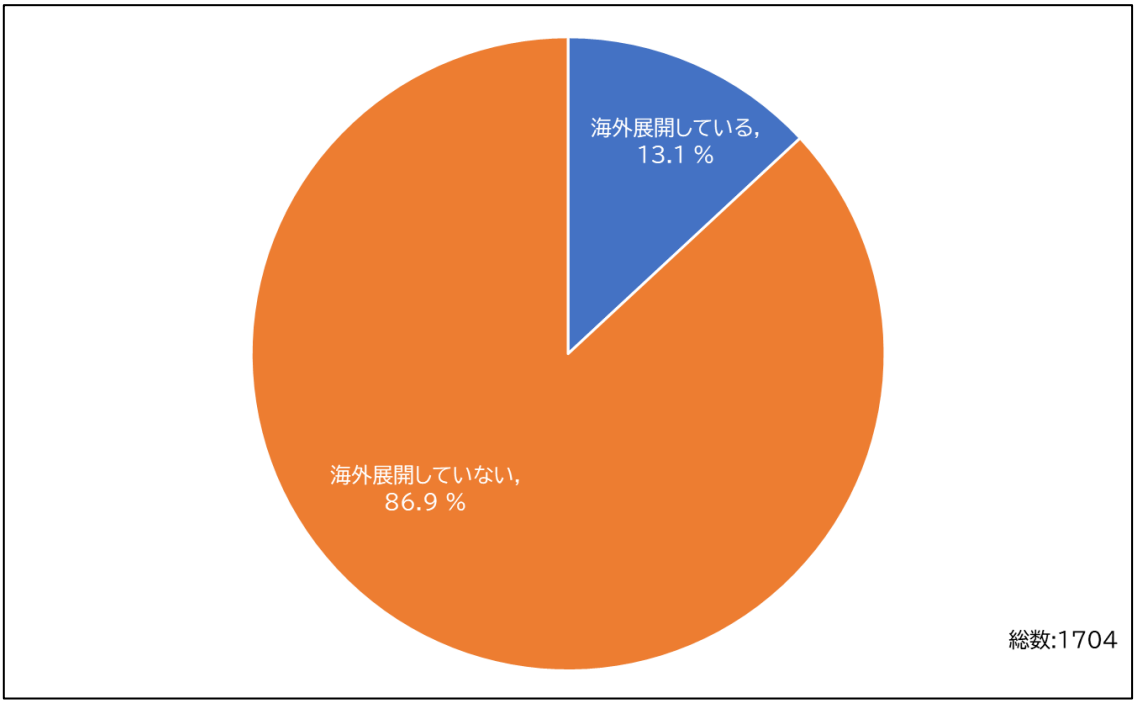

図 33 海外展開の有無

(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りし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」(65.0%)、「確認され、プラス評価されたことがある」(20.2%)、「確認されたことがあるが、プラス評価されたことはない」(14.8%)の順 となった(図 34)。

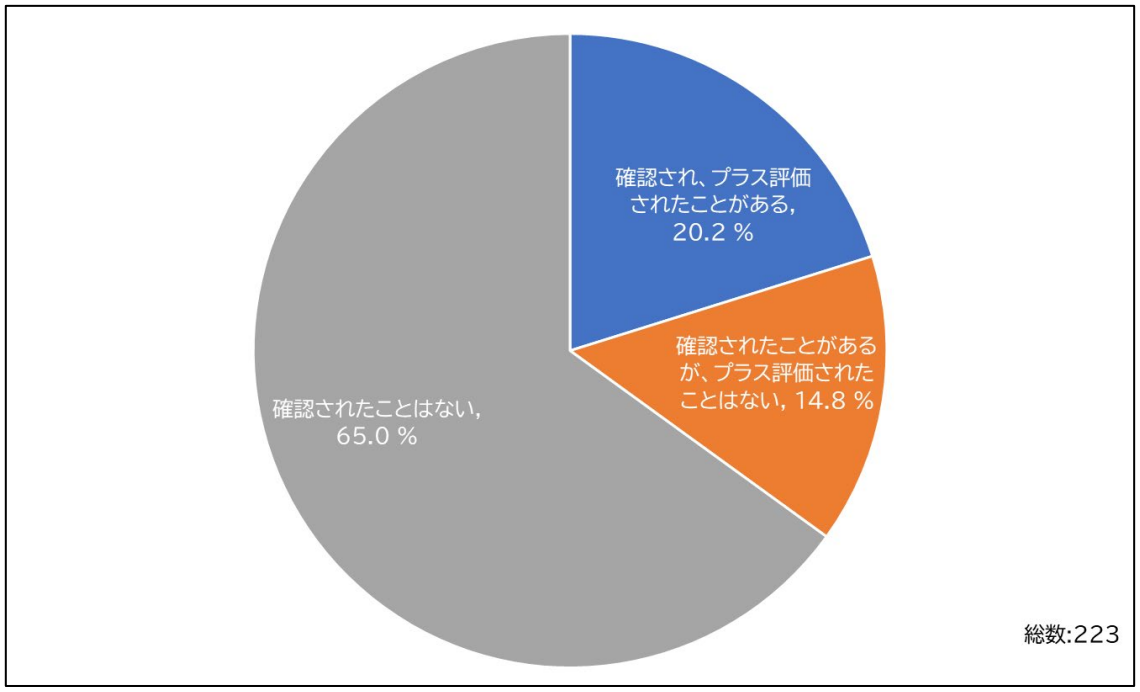

図 34 海外パートナーからの ISMS 認証の確認と評価

3. AI システムの利用

(1)AI システムの利用の有無

事業活動において AI を活用しているかを尋ねたところ、「AI を活用していない」(59.6%)、「AI 利用者(AI システム又は AI サービスを利用する事業者)」(27.1%)、「AI 提供者(AI システムをアプリケーションや製品もしくは既存のシステムやビジネスプロセス等に組み込んだサービスとして AI 利用者、場合によっては業務外利用者に提供する事業者)」(8.6%)、「AI 開発者(AI システムを開発する事業者)」(4.8%)の順となった(図 35)。

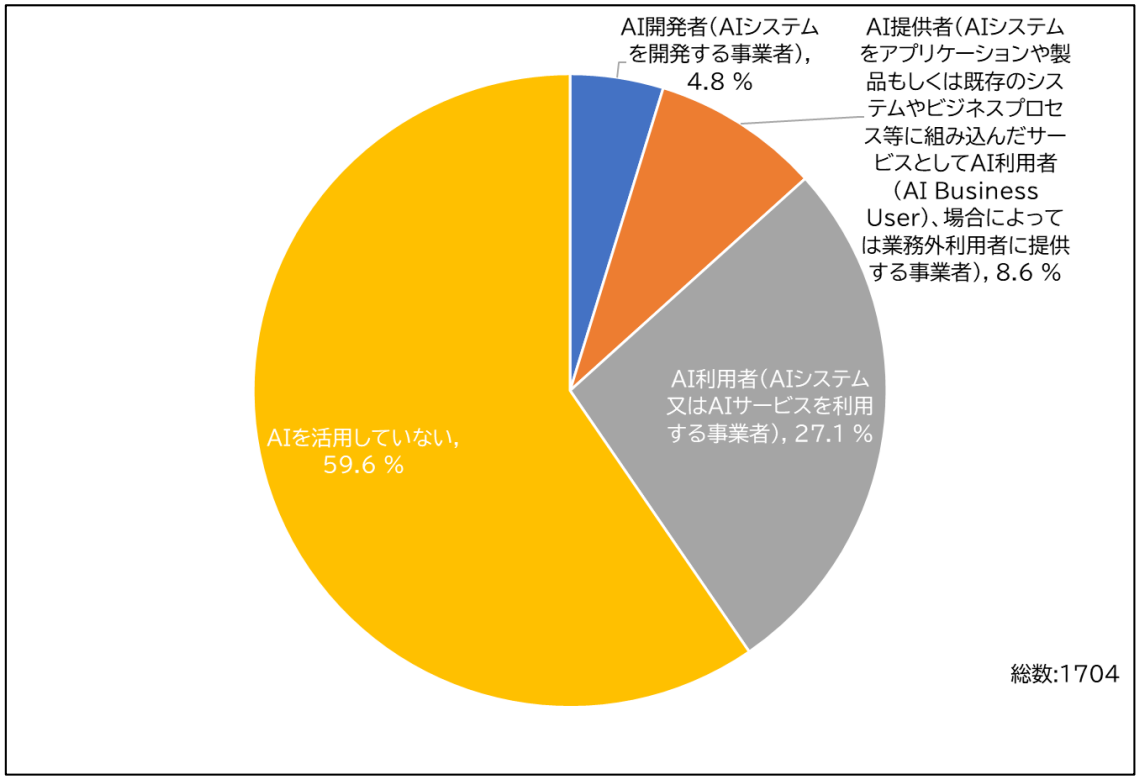

図 35 AI システムの利用

(2)AI マネジメントシステムへの関心

上記で、「AI 開発者」、「AI 提供者」、「AI 利用者」のいずれかを選択した組織に対して、ISO/IEC 42001 (AI マネジメントシステム)について尋ねたところ、「概要をよく知らないが、関心がある」(60.8%)、「概要をよく知らないし、関心はない」(23.9%)、「取得予定はないが、概要は知っている」(14.1%)、「今後取得予定」(1.0%)の順となった(図 36)。

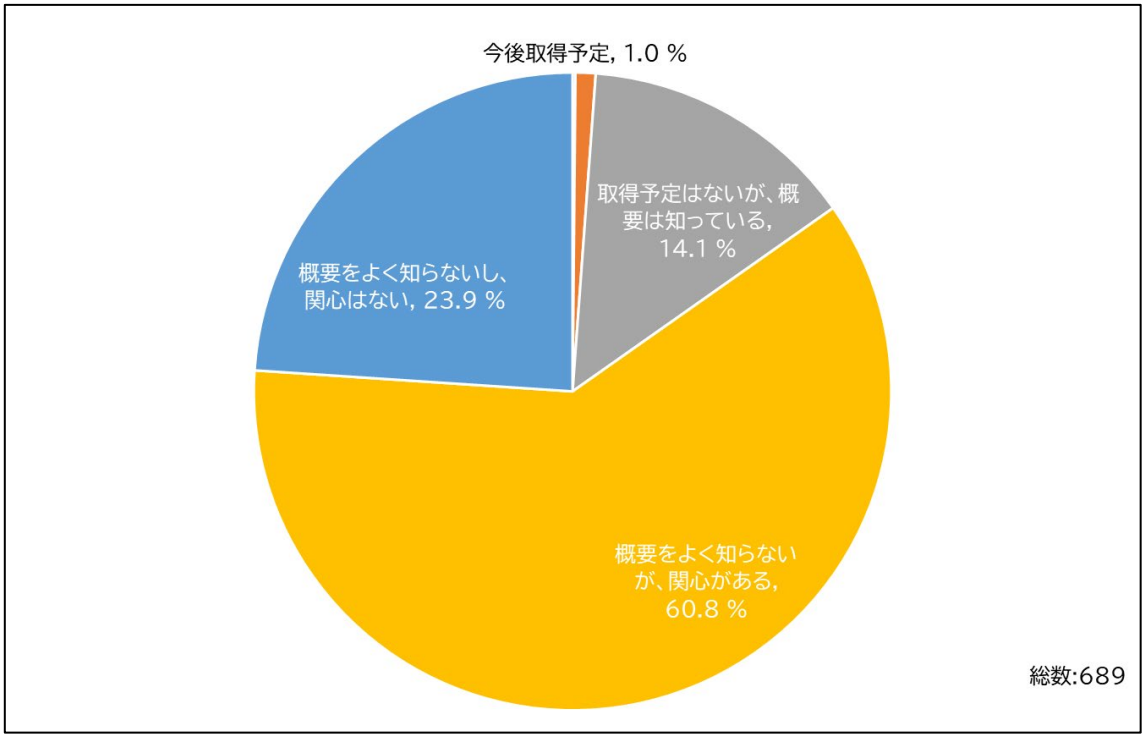

図 36 AI マネジメントシステム認証の認知

4. 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 37 のとおりである。

「研修・セミナーの実施」（52.0%）、「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）」（50.5%）、次いで「制度の認知度向上（普及・広報）」（44.7%）の要望が主にあげられた。

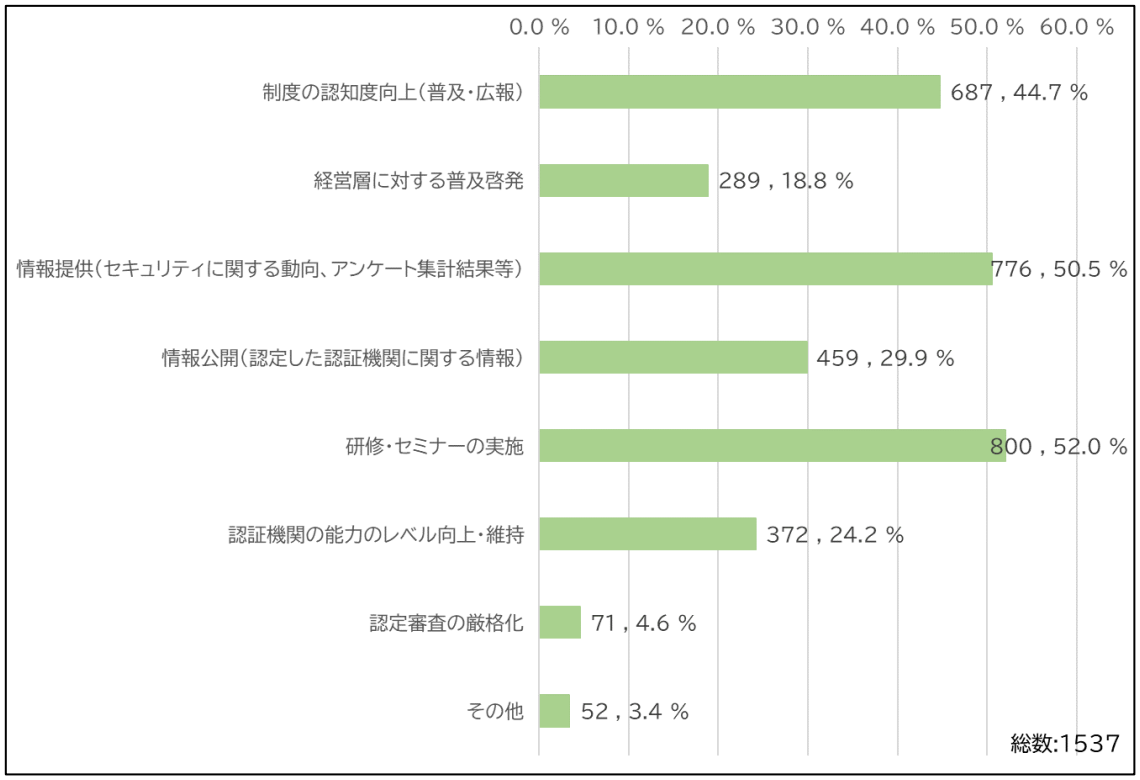

図 37 本センターへの期待

5. ISMS 適合性評価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は以下のとおりである。

［制度の認知度改善、制度推進］

ほとんどが ISMS 適合性評価制度の認知度向上の要望であった。ISMS クラウドセキュリティ認証や ISMS-PIMS 認証に関する制度の認知度向上の要望についても多く頂戴した。主な回答例を以下に示す。

- 10 年以上取得してから経過していますが、前項で述べたとおり、全く認知度の向上が進んでいない。従事者、利害関係者様を含めて現状を改善する気がないのではないかと？私たちは考えています。今後は危機感を持って取り組んでもらいたい。
- ISMS 認証の必要性と重要性は疑いの余地なしであり、当社は今後も維持し続けたいと考えている。 ただし ISMS の社会的認知度はまだまだ低いと思う。
- 広く世間一般での ISMS の認知度向上に取り組んでいただければと思います。
- もっと社会的評価を高めていただきたい。
- ISO/IEC 27001 取得の重要性をアピールしていただきたい。
- ISMS-PIMS 認証制度も広く認知されるようにしてほしい。
- ISO/IEC 27017 の有用性向上のため、認知度向上に取り組んでほしい。
- ISMS-AC 自ら、いま以上に積極的な広報活動を実践してください。

［ガイドライン・規格］

ISO/IEC27001:2022 の発行から日本語版や JIS の発行までの期間に対するご意見を多くいただいた。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。

- ISMS に関わる改訂等、情報発信を行って欲しい。
- 規格が変わった際に、どのように対応すればよいかの資料が少ない。
- ISO 改訂発刊から JIS 規格化までの期間が長いため、もう少し早く JIS 規格化できるよう対応を進めていただきたい。
- 規格改訂時の日本語版の提供を迅速にしてほしい。
- 規格改訂時の移行認証に関して、企業に対して、具体的な移行作業・方法を判り易く解説する機会を増やして欲しい。
- ISMS 認証は、大切な取組みと考えています。 情報セキュリティの動向や、個人情報保護法、医療情報管理などの動向情報の共有（セミナー、動画など）をお願いしたい。 ISMS 認証と、業務バランスがとれるような審査対応と業務への落とし込みのヒントなどの情報公開をお願いしたい。
- 解説やベストプラクティスなどの情報公開をしてほしい。
- 規則が多く覚えるのが大変なので、噛み砕いた説明書のような公式情報があると助かります。
- 情報セキュリティに関するテキストや教材を公開してほしい。

［制度の信頼性の維持・向上］

回答例を以下に示す。

- デジタル化の進展で ISMS 適合性評価制度の重要性が高まっているので、制度の更なるレベルアップをお願いしたい。

・　現在もされていると思うが、今後も認証機関の能力のレベル向上・維持を十分担保できるようにしてほしい。
・　認証機関によって認証難度に大きな差が無いか確認してほしい。
・　審査機関毎の特性や、各業界への精通具合等が判るような資料を公開して欲しい。

［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。

・　2023 年 7 月に共同開催された ISO/IEC27001：2022 移行セミナーを拝聴させて頂き、大変参考になりました。今後もこのような情報発信頂けると幸いです。
・　評価制度自体には意見はありませんが、年度末の業務繁忙時期におけるアンケート調査は避けて頂けましたら幸いです。
・　回答する時間がかかりすぎたので、もう少し簡素化してもよいように思います。ただ、いろいろ振り返ることができたので、今後、役に立つと思います。

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。

新型コロナ禍を経て在宅勤務を含むテレワークが急速に広まるとともに、クラウド、IoT、AI 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にとって一層大きな経営課題の一つとなっています。

ISMS の導入は、その対策として有効と評価され、この 2～3 年は認証数の増加率向上が続いています。

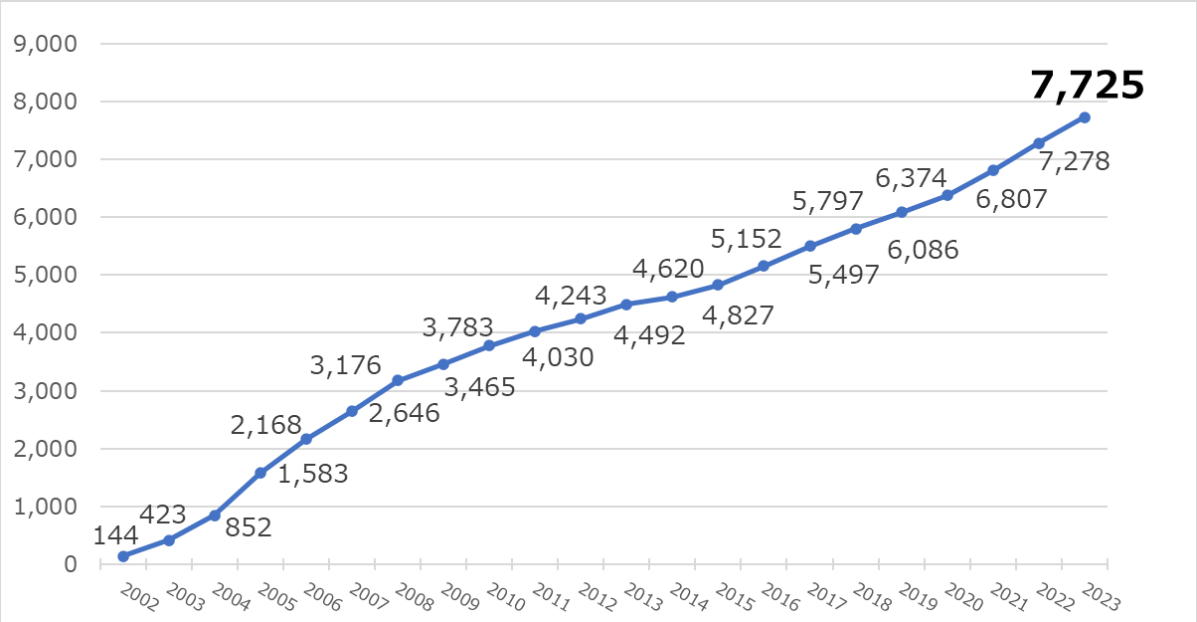

図 38 ISMS 認証取得組織数の推移 （数値は各年度末）

アンケートでは、ISMS を取得されている組織は、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が得られていると回答されました。

ただし一方では、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 10 年を超える組織が 4 割を超える中、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も増加していることが示されました。

ISMS は、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。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が、ISMS の構築・運用をコストとしてではなく、企業活動存続への投資と捉える考えも広がっているように感じられ、その結果として認証取得件数も伸びていると思われます。

さらに今回は、最近利用が急速に拡大している AI システムに関して、新たな設問を加えました。具体的には、

ISMS 認証取得組織における AI の活用状況に加えて、AI システムの開発、利用、提供に関するマネジメントシステムの国際規格である ISO/IEC 42001:2023（AI マネジメントシステム）への関心を尋ねました。

その結果、ISMS 認証取得組織の約 4 割は、AI システムを何らかの形で利用しており、その開発、利用、提供に関するマネジメントシステムへの関心が高いことが分かりました。また、AI マネジメントシステムの認証については 「AI 開発者」、「AI 提供者」又は「AI 利用者」である組織のうち、14.1％が「取得予定はないが、概要は知っている」、60.8％が「概要をよく知らないが、関心がある」と回答され、関心の高さが示されました。

当センターといたしましては、今回のアンケート調査結果を最大限に活用して、ISMS 適合性評価制度の信頼性の更なる確保とその活用度の一層の向上に努めてまいるとともに、ISO/IEC 42001:2023 を認証基準とした「AIMS 適合性評価制度」（仮称）の認定スキームを構築する予定です。

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

2023 年度

ISMS 適合性評価制度に関するアンケート調査書

2024 年 3 月

一般社団法人情報マネジメントシステム認定センター（ISMS-AC）

2023 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 4 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 7 年が経過し、認証取得組織数も約 2,000 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。

今回のアンケート調査について

【アンケートの調査主体及び調査実施機関】
本調査は、一般社団法人情報マネジメントシステム認定センター（ISMS-AC）が株式会社帝国データバンクに委託して実施するものです。

【アンケート調査の対象】
本調査の対象は、当センターが認定した ISMS 認証機関から ISMS 認証を取得し、登録情報を公開している全組織（海外組織及び所在地非公開組織は除く）といたします。

【回答内容の取扱いについて】
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とともに、ISMS 認証の取得又は利用を検討されている組織へ適切な情報提供を行うために使用します。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。

【回答期限】
以下の期日までにご回答をお願いいたします。
回答期日：2024 年 3 月 21 日　23：59

【連絡先】
一般社団法人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

Q1. 貴法人名及び回答者の所属部署について記入してください。

法人名:_____

所属部署:_____

Q2. ご回答者の役職について記入してください。

- 役員
- 管理職
- 技術職(情報システム関連等)
- 一般社員/職員
- ISMS 担当部署
- その他(_____)

Q3. 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。

- 食料品・飲料・タバコ等の製造業
- 衣服・天然素材繊維製品の製造業
- 木材・木製品・パルプ・紙等の製造業
- 出版・印刷業
- 化学薬品・化学製品(化学繊維を含む)・医薬品の製造業
- 石油・石炭・ゴム・プラスチック等の製造業
- ガラス・セラミック・コンクリートの製造業
- 鉄鋼・非鉄金属業・金属製品の製造業
- 機械・機器の製造業
- 電気/電子機器・光学的装置製造業
- 輸送機器製造業
- その他の製造業
- 建設業(エンジニアリングを含む)
- 廃棄物処理業・再生業
- 電力・ガス・熱・水道供給業
- 卸売・小売業
- 金融・保険・不動産業
- 情報技術
- ホテル・レストラン業
- 医療関係

・ その他サービス業
・ 公共・行政・教育機関
・ 分類不明（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

Q4. 「その他製造業」を選択された方へ

詳しい業種を記載ください。

Q5. 「その他サービス業」を選択された方へ

詳しい業種を記載ください。

Q6. 「情報技術」を選択された方へ

下記のうち該当するものを選択してください。

・ 通信業
・ 放送業
・ システムインテグレーション業
・ 受注ソフトウェア業
・ ソフトウェアプロダクト業
・ 計算事務等情報処理業
・ システム等管理運営受託業
・ データベースサービス業
・ 各種調査業
・ インターネット附随サービス業
・ 映像・音声・文字情報制作業
・ その他（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

Q7. 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。

・ 1,000 万円以下
・ 1,000 万円超、5,000 万円以下
・ 5,000 万円超、1 億円以下
・ 1 億円超、3 億円以下
・ 3 億円超

・　該当せず（株式会社以外）

Q8.　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。

・　5 人以下
・　5 人超、20 人以下
・　20 人超、50 人以下
・　50 人超、100 人以下
・　100 人超、300 人以下
・　300 人超、1,000 人以下
・　1,000 人超

ISMS 取得の認証範囲について

Q9.　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。

・　全社
・　全社の 75%以上
・　全社の 25%～75%
・　全社の 25%未満

Q10.　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。

・　5 人以下
・　5 人超、20 人以下
・　20 人超、50 人以下
・　50 人超、100 人以下
・　100 人超、300 人以下
・　300 人超、1000 人以下
・　1000 人超

Q11.　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

Q12.　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をお答えください。

- 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

Q13.　貴組織における認証登録番号を記載ください。

認証登録番号（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

Q14. 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。

- ISMS クラウドセキュリティ認証（クラウドサービスプロバイダ）
- ISMS クラウドセキュリティ認証（クラウドサービスカスタマ）
- ISMS クラウドセキュリティ認証（クラウドサービスプロバイダ及びクラウドサービスカスタマ）
- ISMS-PIMS 認証（PII 管理者）
- ISMS-PIMS 認証（PII 処理者）
- ISMS-PIMS 認証（PII 管理者及び PII 処理者）
- ISO 9001（品質）
- ISO 14001（環境）
- ISO/IEC 20000（IT サービス）
- ISO 22301（事業継続）
- ISO 45001（労働安全衛生）
- ISO 22000（食品安全）
- プライバシーマーク
- その他（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

Q15. 貴組織では、過去にマネジメントシステム認証を取得していて、現在は取得していないマネジメントシステム認証はありますか。

複数ある場合は、その全てを選択してください。

- ISMS クラウドセキュリティ認証（クラウドサービスプロバイダ）
- ISMS クラウドセキュリティ認証（クラウドサービスカスタマ）
- ISMS クラウドセキュリティ認証（クラウドサービスプロバイダ及びクラウドサービスカスタマ）
- ISMS-PIMS 認証（PII 管理者）

- ISMS-PIMS 認証(PII 処理者)
- ISMS-PIMS 認証(PII 管理者及び PII 処理者)
- ISO 9001(品質)
- ISO 14001(環境)
- ISO/IEC 20000(IT サービス)
- ISO 22301(事業継続)
- ISO 45001(労働安全衛生)
- ISO 22000(食品安全)
- プライバシーマーク
- その他(_____)

Q16. 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。

- 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

Q17. 「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。

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

ISMS の導入及び認証取得の効果等について

Q18. 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。

項目	該当する	やや該当する	余り該当しない	該当しない
組織の情報セキュリティ管理体制の強化のため				
組織の情報セキュリティ対策の強化のため				
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				

入札、受注の条件、取引先からの要請による				
顧客からの信頼を確保するため				
企業イメージの向上のため				
同業他社との差別化、営業上の優位性の確保のため				
全社の方針による				
インシデント発生を抑制するため				
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				
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）				

Q19. 前問の各項目以外に、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。

Q20. 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。

項目	該当する	やや該当する	余り該当しない	該当しない
組織の情報セキュリティ管理体制が強化できた				
組織の情報セキュリティ対策の強化できた				
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				
顧客からの信頼確保に貢献した				
企業イメージの向上に貢献した				
営業上、同業他社に対する優位性の確保に貢献した				
情報面での事業継続性の向上に有効であった				
法遵守（コンプライアンス）の面で有効であった				
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				
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				
リスク評価の方法が定着した				
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				

経営者の情報セキュリティに対する関与が深まった				
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				
業務環境の変化（テレワーク、DXの推進、AI利用など）、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。				

Q21. 前問の各項目で「該当する」を選択された場合、また各項目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。

Q22. 顧客から、貴組織の情報セキュリティ対策の実施状況の把握のため、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。

- 求められたことがある
- 求められたことはない

Q23.「求められたことがある」を選択された方へ

具体的にどのようなものを求められましたか（複数可）。

- 実査、取引先からのセキュリティ監査
- 内部／外部監査報告書の開示
- ISMS 認証文書（登録証）
- 適用宣言書の開示
- 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
- その他（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

Q24. 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）。

- 事業内容の変化や組織改革などへの対応
- マンネリ化・形骸化
- 経営者の積極的な参画・理解を得ること
- 情報セキュリティ対策の強化
- 内部監査の改善
- 人材の確保、育成
- 組織内の情報セキュリティ教育・意識向上
- 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
- 効率向上、運用コストの低減

- 事業経営への貢献度を向上すること
- 他のマネジメントシステムとの統合
- 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
- 働き方改革等の人事制度の導入への対応
- 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)
- その他
- 特に課題はない

Q25.「事業内容の変化や組織改革などへの対応」を選択された方へ

可能でしたら差し支えない範囲で具体的な内容(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

Q26.「マンネリ化・形骸化」を選択された方へ

可能でしたら差し支えない範囲で具体的な内容(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

Q27.「経営者の積極的な参画・理解を得ること」を選択された方へ

可能でしたら差し支えない範囲で具体的な内容(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

Q28.「情報セキュリティ対策の強化」を選択された方へ

可能でしたら差し支えない範囲で具体的な内容(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

Q29.「内部監査の改善」を選択された方へ

可能でしたら差し支えない範囲で具体的な内容(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

Q30.「人材の確保、育成」を選択された方へ

可能でしたら差し支えない範囲で具体的な内容（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

Q31.「組織内の情報セキュリティ教育・意識向上」を選択された方へ

可能でしたら差し支えない範囲で具体的な内容（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

Q32.「新技術や環境変化への対応 」を選択された方へ

可能でしたら差し支えない範囲で具体的な内容（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

Q33.「効率向上、運用コストの低減」を選択された方へ

可能でしたら差し支えない範囲で具体的な内容（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

Q34.「事業経営への貢献度を向上すること」を選択された方へ

可能でしたら差し支えない範囲で具体的な内容（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

Q35.「他のマネジメントシステムとの統合」を選択された方へ

可能でしたら差し支えない範囲で具体的な内容（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

Q36.「外部組織が提供する IT サービスへの依存性増加と管理 」を選択された方へ

可能でしたら差し支えない範囲で具体的な内容（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

Q37.「働き方改革等の人事制度の導入への対応 」を選択された方へ

可能でしたら差し支えない範囲で具体的な内容（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

Q38.「審査関連への対応 」を選択された方へ

可能でしたら差し支えない範囲で具体的な内容（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

Q39.「その他 」を選択された方へ

可能でしたら差し支えない範囲で具体的な内容（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

審査員の力量及び審査の質について

Q40. 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。

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
マネジメントシステムに関する知識及び業務経験				

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				
受審組織の業務に対する理解				
コミュニケーション能力				
審査技術				
改善課題を指摘する能力				

Q41. 最近受審された ISMS 認証審査の質を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の観点で評価してください。

- 満足
- やや満足
- やや不満
- 不満

Q42. 「不満」「やや不満」を選択された方へ

不満な点を具体的に記載ください。

Q43. 最近受審された ISMS 認証審査の質を管理策に関する審査内容の観点で評価してください。

- 満足
- やや満足
- やや不満
- 不満

Q44. 「不満」「やや不満」を選択された方へ

不満な点を具体的に記載ください。

Q45. 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。

- 適切
- 長い
- 短い
- 何とも言えない

Q46．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評価してください。

- 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

Q47．「あまり役立たなかった」「役立たなかった」を選択された方へ

役立たなかった点を簡潔に記載ください。

Q48．総合的に見た審査の質を、総合評価してください。

- 満足
- やや満足
- やや不満
- 不満

Q49．「不満」「やや不満」を選択された方へ

不満な点を具体的に記載ください。

Q50．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

Q51．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。

- 重視した
- やや重視した
- 多少は考慮した
- まったく考慮しなかった

Q52．前問の回答の理由について具体的に記載ください。

Q53．　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。

- 重視した
- やや重視した
- 多少は考慮した
- まったく考慮しなかった

Q54．前問の回答の理由について具体的に記載ください。

Q55．貴社のウェブサイト、名刺等で認証マークと併せて選択肢にある認定シンボルを利用していますか。

- 「認定シンボル」を利用している
- 利用していない

Q56．前問の回答の理由について具体的に記載ください。

制度全般に対するご意見等

Q57．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。

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

Q58．貴組織は事業活動を海外展開されていますか。

- 海外展開している
- 海外展開していない

Q59．「海外展開している」を選択された方へ

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。

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

Q60．貴組織は事業活動において AI を活用していますか。

- AI 開発者（AI システムを開発する事業者）
- AI 提供者（AI システムをアプリケーションや製品もしくは既存のシステムやビジネスプロセス等に組み込んだサービスとして AI 利用者（AI Business User）、場合によっては業務外利用者に提供する事業者）
- AI 利用者（AI システム又は AI サービスを利用する事業者）
- AI を活用していない

Q61．「AI 開発者」「AI 提供者」「AI 利用者」を選択された方へ

ISO/IEC 42001（AI マネジメントシステム）について、最も当てはまると思うものをご回答ください。

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

Q62．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。

- 制度の認知度向上（普及・広報）
- 経営層に対する普及啓発
- 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）
- 情報公開（認定した認証機関に関する情報）
- 研修・セミナーの実施
- 認証機関の能力のレベル向上・維持
- 認定審査の厳格化
- その他（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

Q63．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。