「2012 情報セキュリティマネジメント実態調査報告書」

ISACA東京支部 CISM委員会

平成24年12月

情報セキュリティを確保し維持するためにはその中核を担う情報セキュリティマネージャー（ISM）の存在が重要です。特に昨今の新たな情報セキュリティの脅威や各種のモバイル端末の出現に対して対策の難しさと組織目的達成のためにICTの利活用から得る利得とのバランスをいかに取るかについて的確な判断が求められており、企業経営者を支えるISMの役割は重要性を増しています。しかしながら例えば、日本国内ではセキュリティの専門家、システム監査あるいは情報セキュリティ監査の専門資格がありますが、ISMについてはISACAのCISMが唯一であり、その数は未だ400名に届いていない状況にあります。ISACA東京支部CISM委員会では、国内の情報セキュリティマネジメントに関する人材が今後とも重要性を増すことが予想されるなかで、実態を把握することが情報セキュリティの専門家や企業にとって参考になると考え、当調査を行いました。

当調査は国内のISACA各支部会員とJASA日本セキュリティ監査協会会員に対して行ったものです。当調査における設問は大きく対象母集団のプロファイルを把握する設問、情報セキュリティ体制と人材に関する設問、そしてISACAで定める情報セキュリティマネージャーのタスクを基にしたセキュリティマネジメントの運用調査を確認する設問に分かれています。

1. 調査母集団のプロファイル

1−1 回答者の所属団体

当調査はISACA国内各支部とJASA 日本セキュリティ監査協会会員を対象として電子メールで協力をお願いし行ったものです。電子メールの配信対象は全体で約4000名、Webでのアンケートに回答していただいた数は356件です。なお6件はJASAとISACA会員の双方であると回答しています。

いずれの回答者も情報セキュリティに関する知識を有し、実務に直接的または間接的に関係している方々であると想定されます。情報セキュリティの

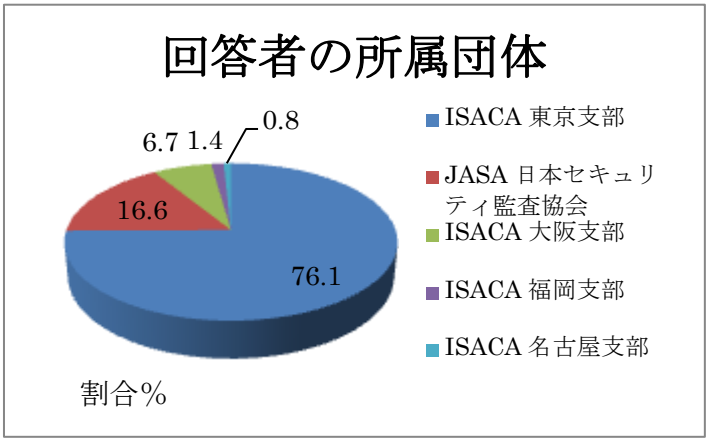

図 1 回答者の所属団体

専門家の関わる企業が対象となることから、母集団の企業は国内の平均的な企業というよりも、セキュリティマネジメントに関して比較的意識の高い企業と推定されます。

1-1-1　対象組織の産業分野

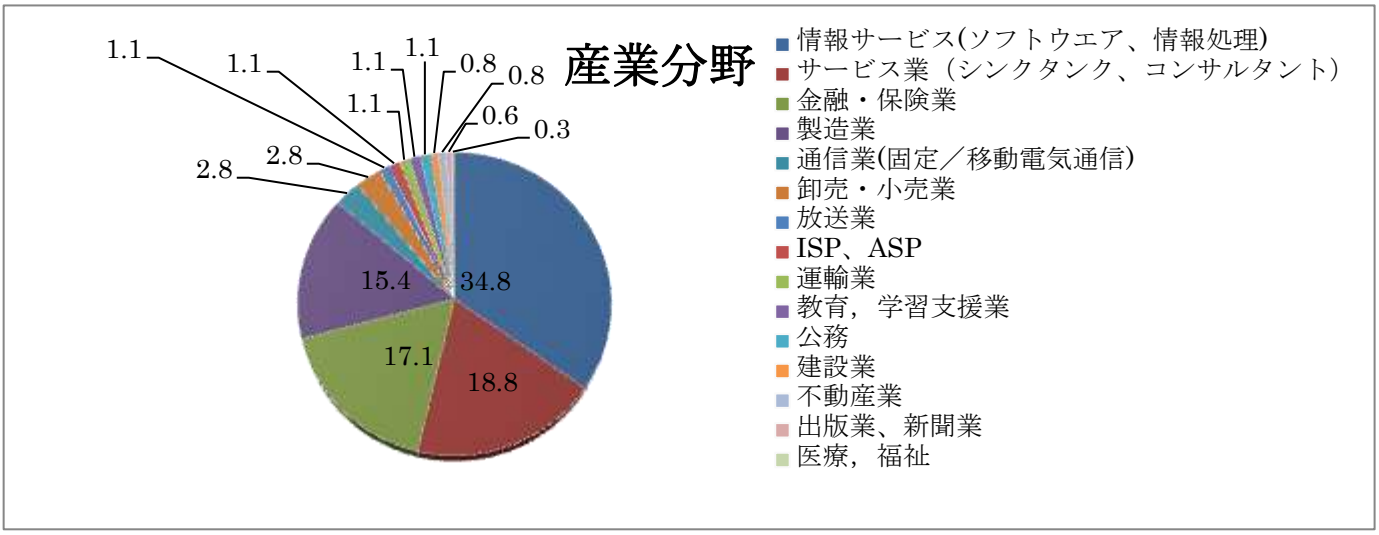

図 2　対象企業の産業分野

対象となる企業の産業分野は情報サービス業、サービス業、金融・保険業、製造業の企業数が上位の86.1%を占めており、この調査の主要な対象となっています。

1-1-2　従業員規模

企業規模は大企業が相対的に多く、中小規模の企業まで比較的一様に分布しています。

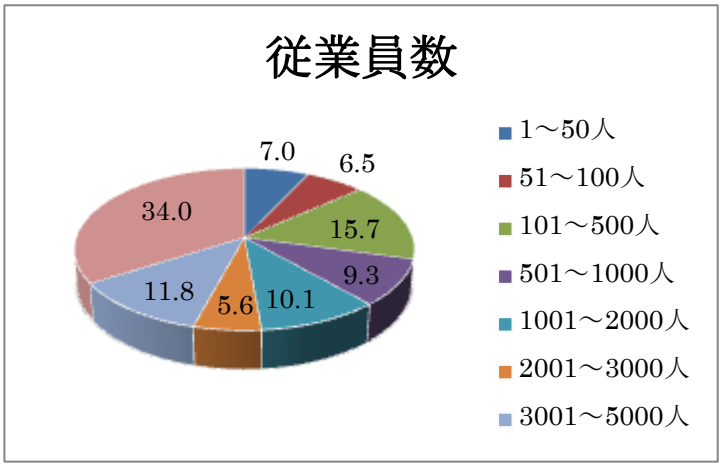

図 3　企業規模の分布

1-1-3　回答者の組織内での所属

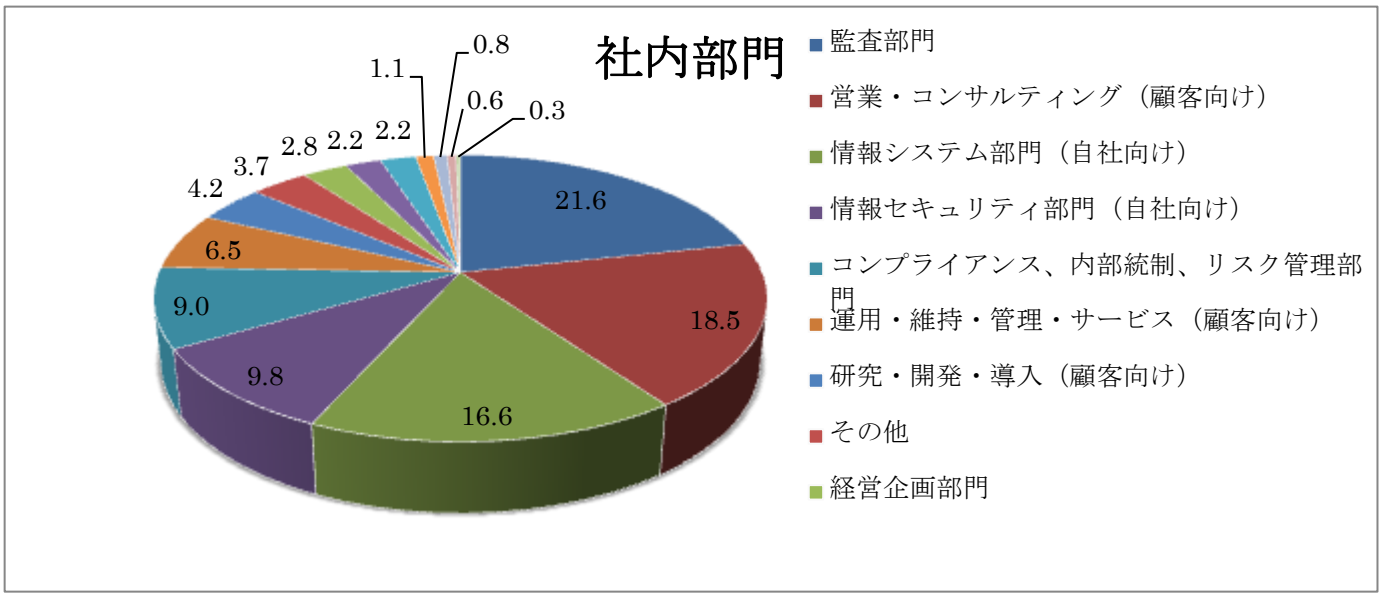

図 4　回答者の社内部門

回答者の所属は情報セキュリティ部門が約10%であることから、直接情報セキュリティに携わっている割合は比較的小さいことが分かります。

1-1-4 回答者の職位

回答者の約半数が企業内の管理職（部長、課長クラス）であり、ISMの職位に相当する職位の方々となっています。

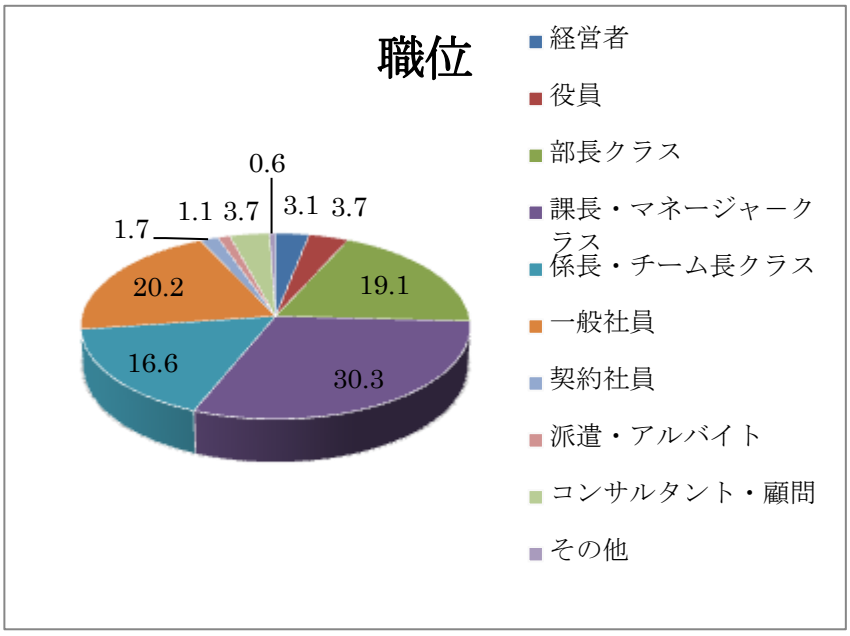

図 5　回答者の職位

2. 情報セキュリティの体制と人材

2-1-1 キュリティマネジメントを主管している部門

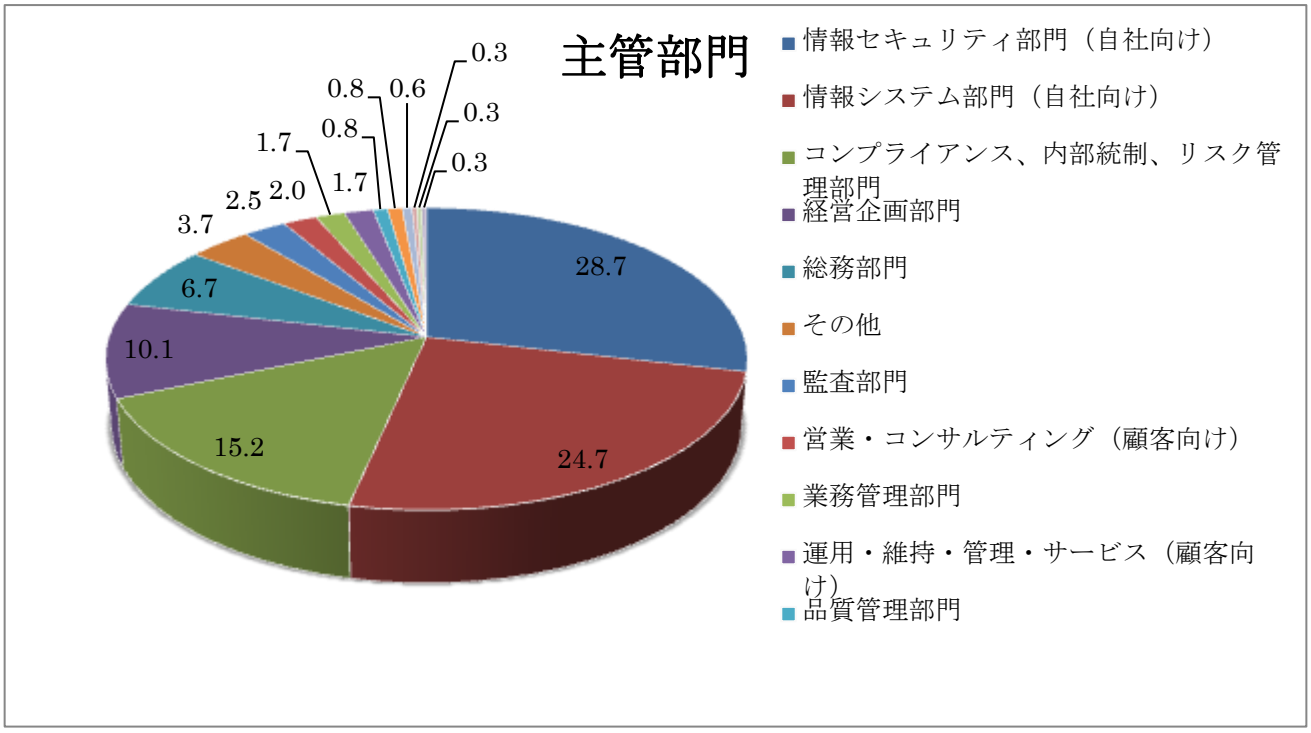

図 6　情報セキュリティマネジメントを主管する部門

情報セキュリティを主管する部門として、多くの企業では専門の対応部署（情報セキュリティ部門、情報システム部門、コンプライアンス、内部統制、リスク管理部門）で対応しています（68.6%）が、それ以外では情報セキュリティの担当として必ずしも相応しくない部門で担当しています。

2-1-2 情報セキュリティマネージャ（ISM）は存在しているか

約70%でISMの実務を担当する人材が配置されています。「知らない／わからない」が19%であるのは、ISMの配置を明確にしていないことであろうと思われます。

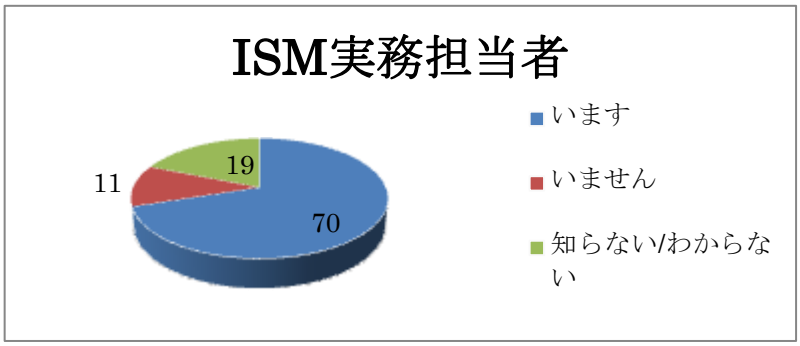

図 7　ISMの配備状況

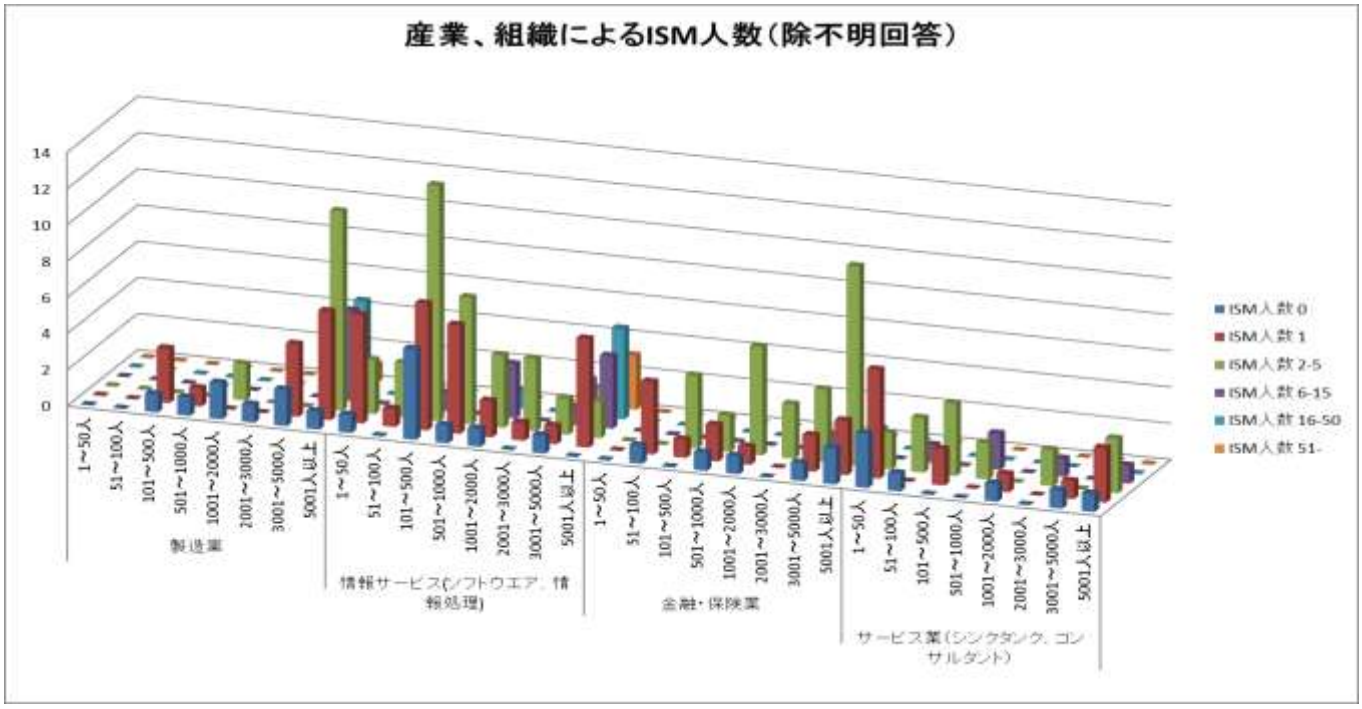

図 8　ISMの人数

図8は４つの産業分野における企業規模別のISMの人数分布を示しています。製造業では中小規模で対応が進んでおらず、また大企業でも対応の進んでいる割合は小さくなっています。情報サービス業ではISMの配備状況は比較的進んでいます。金融・保険業では特に大企業で対応する人数が少ない傾向にあります。

2-2-1 ISMの能力

図9にあるように、ISMの能力に関して十分な能力があると判断した割合は34%であり、それ以外は不十分と判断されています。43.2%が能力不足と判断しており、人材育成の重要性が高いことが分かります。

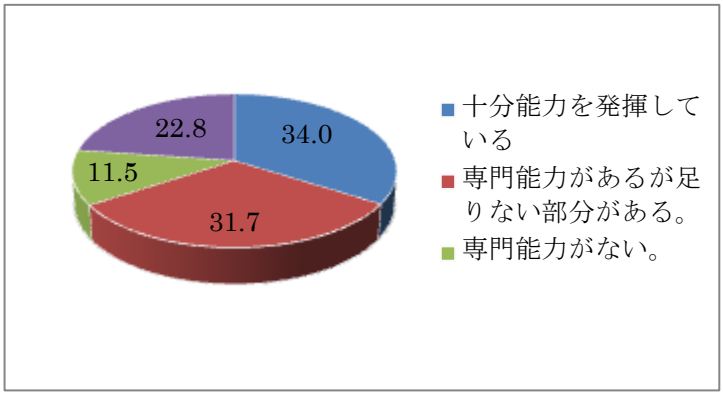

図 9　担当者の能力

2-2-2 ISMに足りない専門能力

ISMに不足している専門能力として、専門知識を挙げる割合が多く、ISMが新たな脅威に対して十分対応できていない可能性があります。

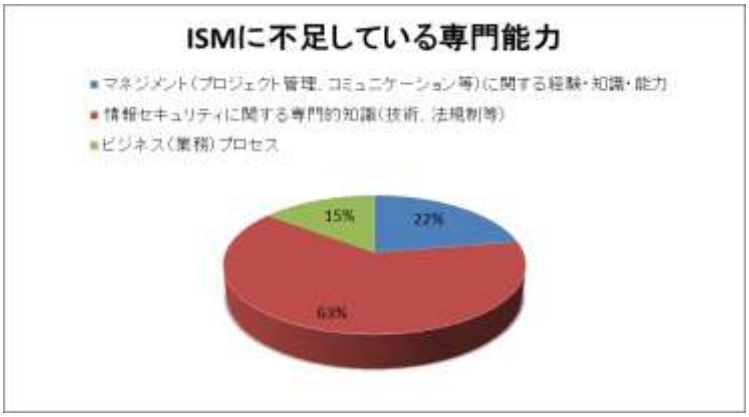

図 10　不足している専門能力

2-2-3 ISMの育成のための第一歩は

ISMを育成するために推奨する事項として、以下の４つが高い比率で回答されています。

- セミナー・研修などに参加して知識を習得する
- セキュリティ関連知識を学びCISM（ISACA）などの資格を取得する。
- システム開発･運用の現場でセキュリティ対策の経験を積む
- セキュリティインシデントの対応を経験する

ISMには経験と最新の知識のふたつが求められています。

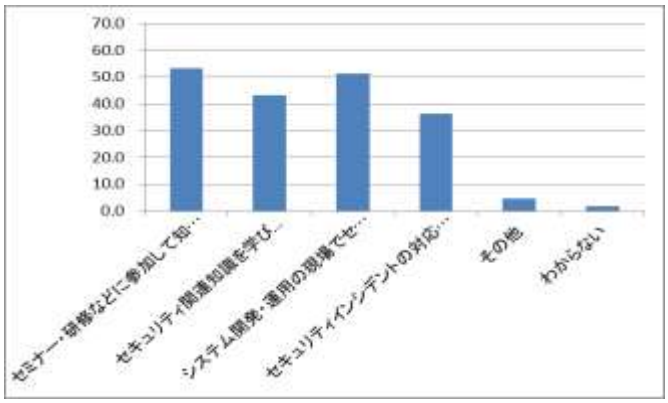

図 11　ISMの育成方法

2-3-1　資格取得に対するインセンティブ

人材確保のための有効な手段と考えられる資格取得への支援は約半数の企業であるものの、その割合は大きくありません。

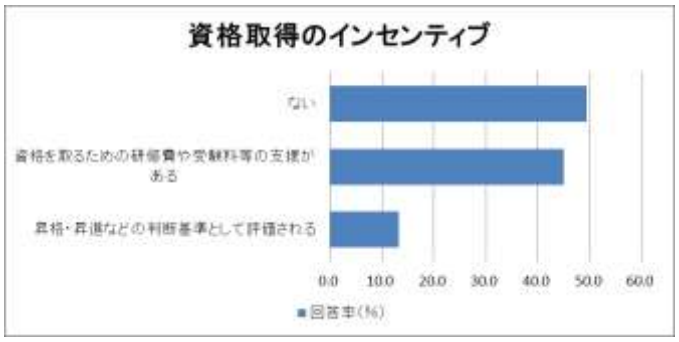

図 12　資格取得のインセンティブ

2-3-1a 資格取得の報奨金

資格取得後の報奨金については、77.8%で報奨金がないと回答しています。人材育成、人材確保の目標の具体的方法が企業で認識されていないことが分かります。

また、給与に加算される資格手当は97.8%で考慮されておらず、人材確保についての配慮が進んでいないと判断できます。

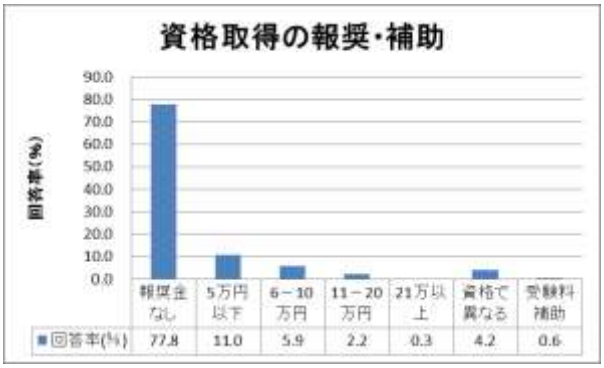

図 13　資格取得への報酬

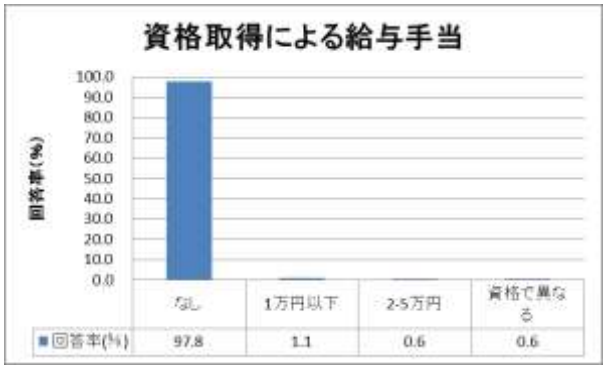

図 14　資格取得での給与手当

2-3-2 ISMの有する資格

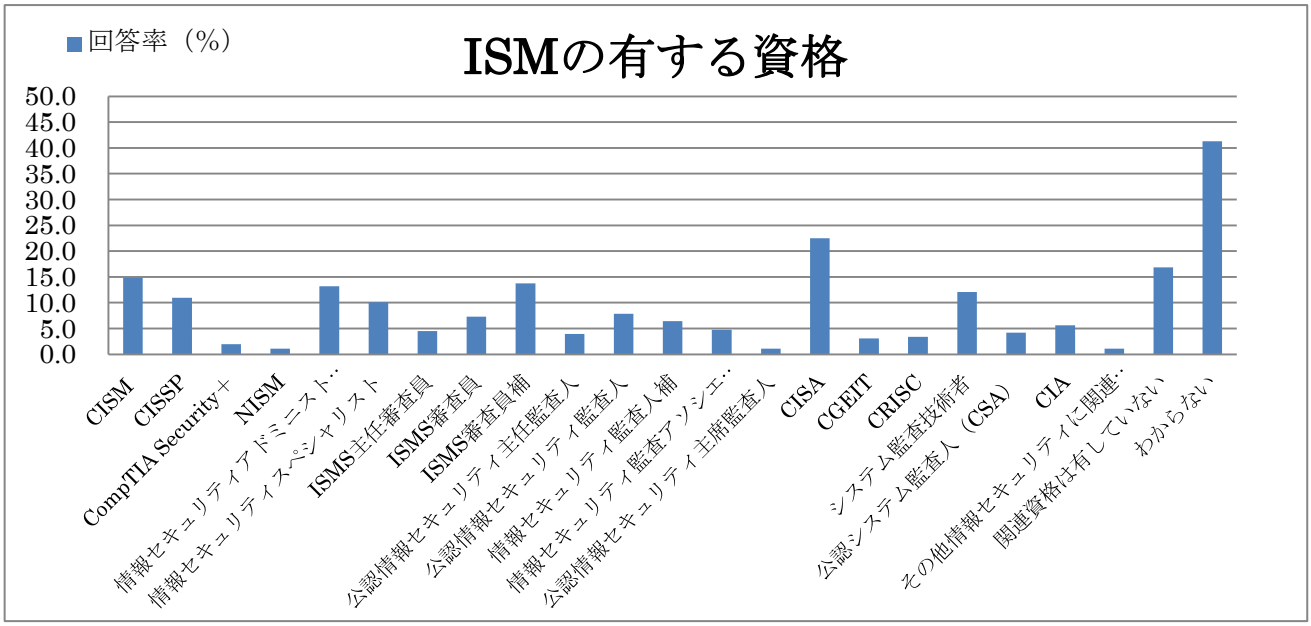

図 15 ISMの有する資格

図15はISMが有する資格の分布であり、セキュリティの専門資格の他に監査資格の有資格者が多くなっています。これは、回答者の集団がISACAとJASAであることに原因するかもしれません。監査の有資格者が情報セキュリティマネジメントを担当しているのは人材の流動性を示していると思われます。また、ISMの資格であるCISMの有資格者の割合が低く、今後CISMを含めてISM関連資格の取得者増加の余地があると期待できます。

2-3-3 回答者の有する資格

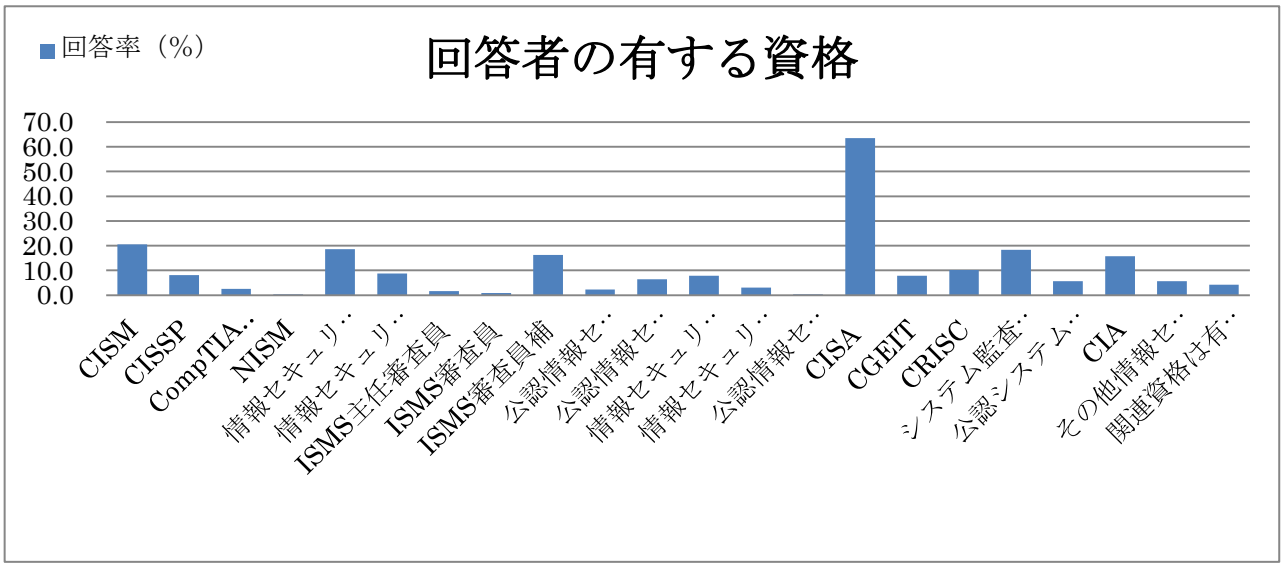

図 16　回答者の有する資格

本調査がISACAの会員とJASAの会員を対象としたため、回答者はISACAの主要な資格であるCISAの有資格者の割合が多くなっています。

3 セキュリティマネジメント運用調査

セキュリティマネジメントの実態調査としての設問は、以下のように４つの領域における対応状況と総合的な評価に関するものです。

項番	情報セキュリティガバナンスに関する設問
3-1-1	確立された情報セキュリティガバナンスフレームワークと、これにより支えられる組織目標と目的に調和した情報セキュリティ戦略がある。
3-1-2	情報セキュリティ方針が確立されていて、経営陣の指示・伝達のもとで、基準、手順などが策定されている。
3-1-3	情報セキュリティの役割と責任が規定（明文化）されており、組織全体に説明責任と権限が確立している。
3-1-4	情報セキュリティ戦略の有効性を測定基準に従い監視・評価し、報告するプロセスが確立しておりそれを経営陣が把握している。
	情報リスク管理とコンプライアンスに関する設問
3-2-1	情報資産のランク付けのプロセスがあり、資産の重要度に応じた対策が取られている。
3-2-2	法規制、組織、及びその他の条件を把握し、組織として遵守すべき状況を把握している。
3-2-3	リスク評価、脆弱性評価、および脅威分析が定期的に行われ、組織の情報資産に対するリスクが把握できている。
3-2-4	情報セキュリティ管理策の適切性とリスクが許容水準に効果的に低減しているかを定期的に評価している。
3-2-5	情報リスク管理を事業とITの各プロセス(開発、調達、プロジェクト管理、合併・買収など)に組み込み、一貫性のある包括的な情報リスク管理プロセスを組織全体で推進している。
3-2-6	既存のリスクを監視し、不遵守や情報リスクの変化について経営陣が把握しており、リスク管理の意思決定プロセスに役立てている。
	情報セキュリティプログラムの開発と管理に関する設問
3-3-1	情報セキュリティプログラムは情報セキュリティ戦略と調和しており、他のビジネス機能(人事、経理、調達、IT等)との間で整合性があり、ビジネスプロセスへの組み込みが考慮されている。
3-3-2	情報セキュリティの基準、手順等の文書を確立、伝達、および維持し、情報セキュリティ方針が遵守されている。
3-3-3	情報セキュリティの周知と研修のためのプログラムがあり、セキュリティで保護された環境とセキュリティ文化を維持している。
3-3-4	情報セキュリティ要件を組織の各種プロセス(変更コントロール、合併および買収、開発、事業継続、災害復旧など)に組み込んでいる。
3-3-5	情報セキュリティ要件をサードパーティ(合弁会社、委託業者、ビジネス・パートナー、顧客など)の契約と活動に組み込でいる。
3-3-6	セキュリティプログラムの管理と運用上の測定基準があり、監視と定期的な報告により情報セキュリティプログラムの有効性と効率が把握されている。
	情報セキュリティのインシデント管理に関する設問
3-4-1	情報セキュリティインシデントを組織として正確に把握し対応できている。
3-4-2	インシデント対応計画があり、情報セキュリティインシデントに即座に対応できている。
3-4-3	情報セキュリティインシデントを調査し記録するプロセスがあり、法規制、および組織の要件に準拠して適切に対応し原因究明ができるようにしている。
3-4-4	インシデントのエスカレーションと通知のプロセスがあり、該当する利害関係者がインシデント対応管理に確実に参加できるようになっている。
3-4-5	コミュニケーションの計画とプロセスがあり、内部および外部とのコミュニケーションが管理されている。
3-4-6	インシデントの事後レビューを実施し、インシデントの根本原因を特定し、是正処置を策定し、リスクを再評価し、対応の有効性を評価し、適切な対策が実施できている。
3-4-7	インシデント対応計画、災害復旧計画、および事業継続計画は統合されている。
	総合的な評価に関する設問
3-5-1	あなたが関係する企業・組織における効果的な情報セキュリティマネジメントの運用は以下のどれに最も該当しますか。

このうち3-4-1,3-4-2,3-4-3以外の回答の選択肢は同じであるので「対応できている」の割合の大きいものから順に図17に示しています。

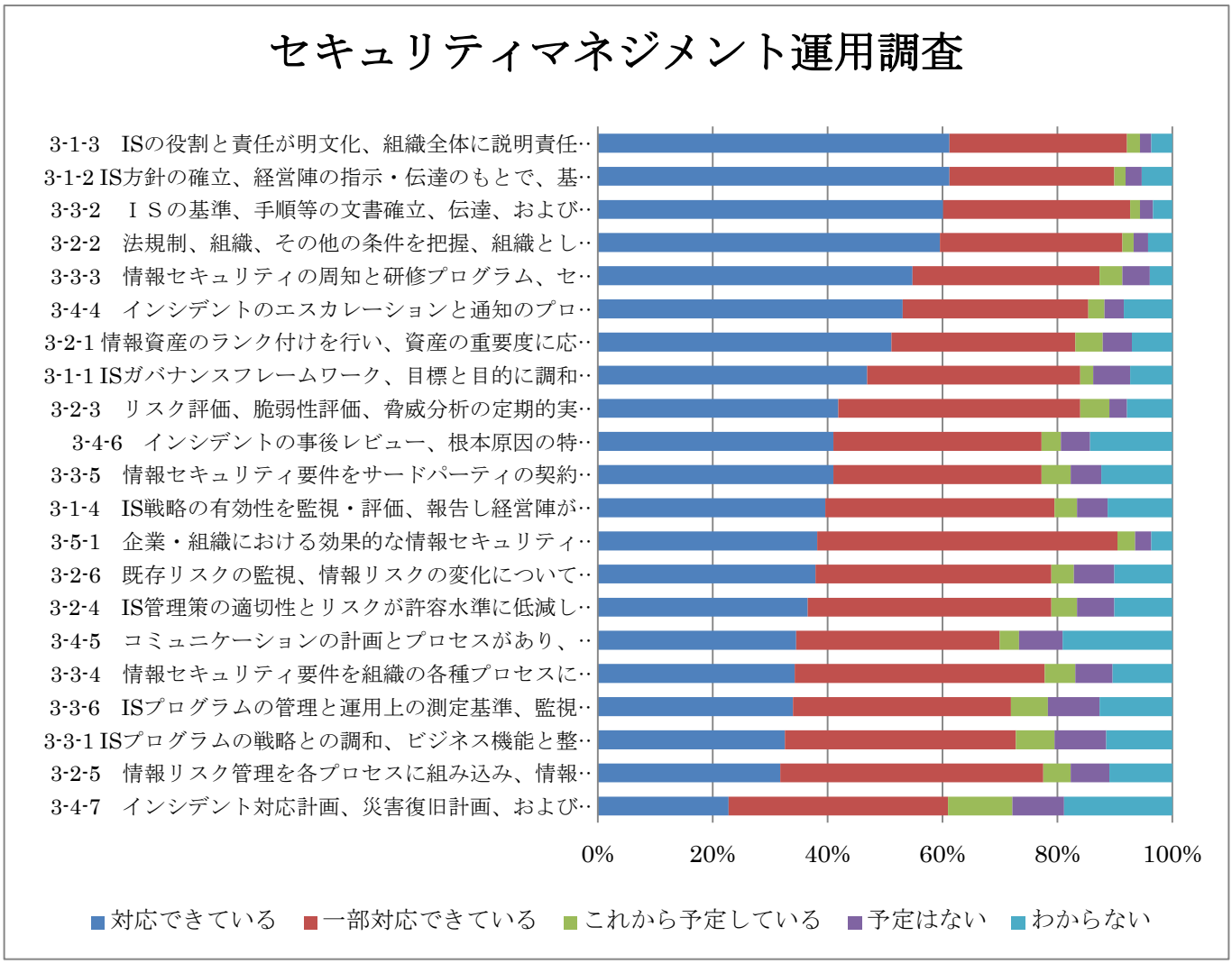

図 17　情報セキュリティマネジメントの実態

情報セキュリティガバナンスの各項目の対応状況から、例えば3-1-3, 3-1-2からは組織に方針がありそして内部規定や推進体制が文書化されている点で「対応できている」「一部対応できている」組織が多く、情報セキュリティマネジメントシステム（ISMS）が既に導入されていることを意味しています。ところが、3-1-1セキュリティ戦略がある、そして3-1-4戦略の有効性の評価となると次第に「対応できている」ポイントが低下しています。

情報リスク管理とコンプライアンスに関しては、3-2-2 法規制の把握のポイントが高く、ついで3-2-1 資産のランク付に対応できています。しかし、3-2-3 リスクや脅威分析の定期的な実施ではポイントが低下し、3-2-6 リスクの監視やリスクの変化への対応、そして3-2-4の管理策の評価、3-2-5のリスク管理の各プロセスへの組み込みにおいてポイントが低下しています。

情報セキュリティプリグラムの開発と管理に関しては、3-3-2 基準や手順の確立、3-3-3 研修の実施で「対応できている」比率が高く、3-3-5 契約への組み込み、さらに3-3-4 各種プロセスへの組み込みでポイントが下がります。3-3-6 セキュリティプログラムの評価への対応と3-3-1 セキュリティ戦略と調和したビジネスプロセスへの組み込みへの対応では更にポイントが低下しています。

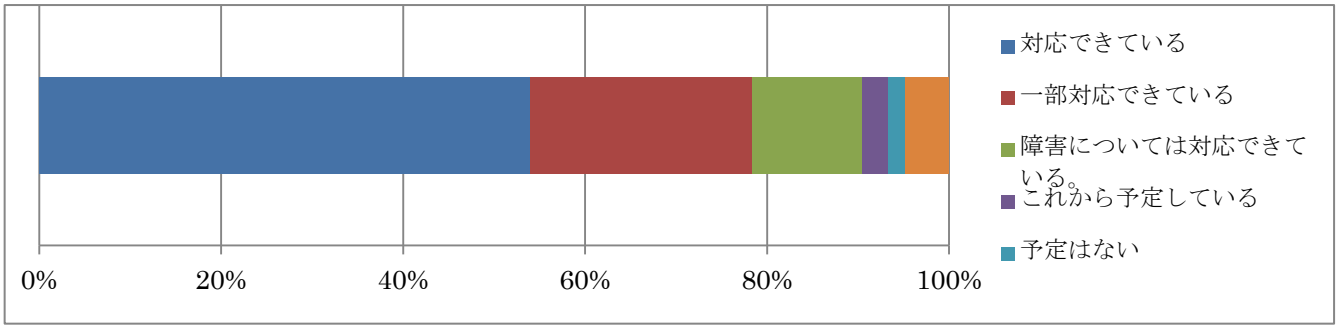

図 18　3-4-1 情報セキュリティインシデントを組織として正確に把握し対応できているか。

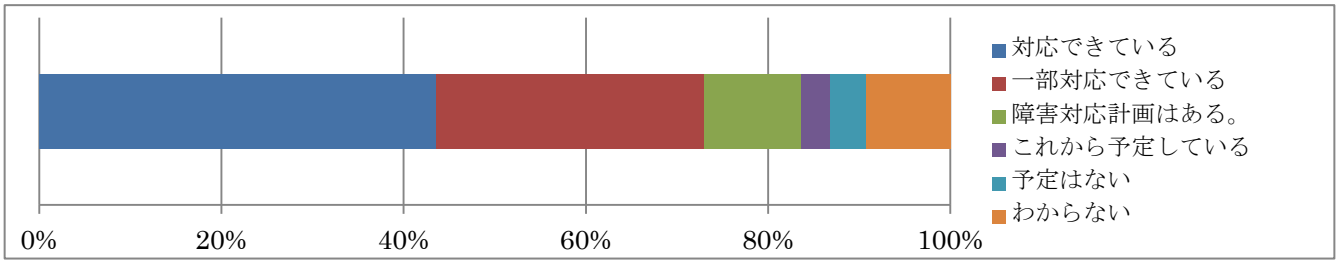

図 19　3-4-2 インシデント対応計画があり、情報セキュリティインシデントに即座に対応できているか。

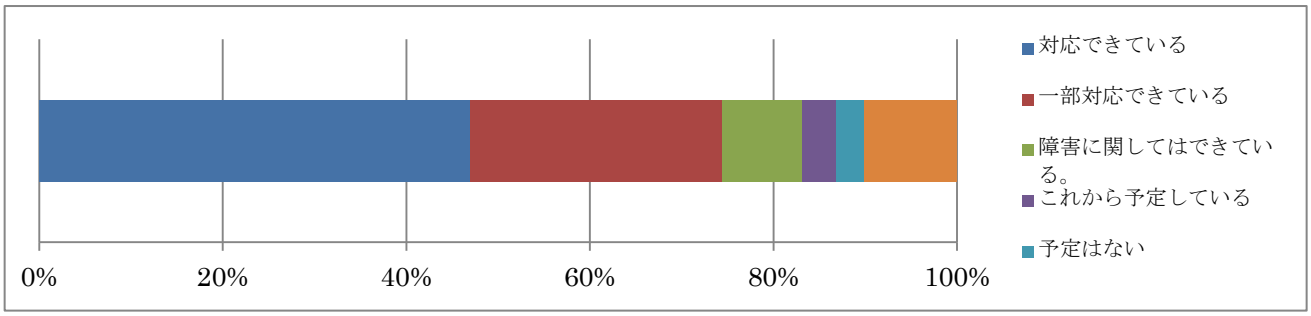

図 20　3-4-3 情報セキュリティインシデントを調査し記録するプロセスがあり、法規制、および組織の要件に準拠して適切に対応し原因究明ができるようにしているか。

設問3-4-1, 3-4-2, 3-4-3はインシデントに関する設問であり、夫々図18、19、そして20に対応しています。3-4-4 インシデントのエスカレーションプロセスがあり、3-4-1 インシデントの把握に対応できているが、3-4-6 インシデントの事後レビューではポイントが下がります。3-4-5 内外のコミュニケーションの管理でさらにポイントが下がります。今回の調査で最も対応状況の悪いのは 3-4-7 インシデント対応計画、災害復旧計画、および事業継続計画の統合への対応でした。

3-5-1は総合的な評価であり、「対応できている」の割合は38.2%と他の設問と比較して平均的な値です。しかし、「一部対応できている」の割合が52.2%と最も高く、多くの回答者はセキュリティマネジメントの有効性が不十分であると認識しています。

3.　4 総合評価

以下、まとめますと；

1. 情報セキュリティマネージャー(ISM)の配備が不十分である企業が多い。
2. ISMの約３分の２は、専門知識等が足りないと判断されており、知識の獲得や経験を積むことが求められている。
3. 企業では専門領域における資格獲得者への支援が不十分であるところが多い。
4. 情報セキュリティマネジメントシステムの導入は対象企業で進んでおり、効果的な運用ができていると判断しているのは約40%であり、約50%は対応が不十分であると考えている。
5. 情報セキュリティマネジメントシステムの計画段階に実施する部分への対応比率は高いものの、ビジネスプロセスや対外的な関係の中でのセキュリティ管理の組み込み、情報セキュリティ戦略やセキュリティプログラムの有効性の評価、包括的な情報リスク管理への対応ができていない傾向にある。
6. インシデント対応計画、災害復旧計画、および事業継続計画の統合への対応が遅れている。

最近国内でもAPT攻撃など新しい型の攻撃が脅威となっており、企業は既に情報セキュリティマネジメントシステム（ISMS）を導入しているものの、外的環境からの脅威の変化に追従できているのでしょうか。新しい型の攻撃に対しては既存の対策の見直しと包括的な情報リスク管理が必要となっていますが、当調査結果からはいずれにおいても対応できていない企業がかなりあるという傾向があります。当調査結果は個別企業のセキュリティ対策に役立つものではありませんが、企業経営者、情報セキュリティ担当者や情報システム担当者が情報セキュリティマネジメントの運用において陥りやすい傾向を把握する上で参考になるものと期待しています。