企業の CISO 等やセキュリティ対策推進に関する実態調査

－調査報告書－

2020年3月25日

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

エグゼクティブサマリー

本調査は、企業のセキュリティ対策の実態や経営層・CISO 等[1]のセキュリティへの取組みの状況を把握することを目的として文献調査やインタビュー、アンケート調査を実施し、結果と得られた知見をまとめたものである。

調査結果

Ⅰ．経営層のセキュリティ認識

- 経営層のセキュリティに対する全般的なリスク認識は高まっている。
- 経営層はサイバーセキュリティに漠然と課題認識を有しているものの、具体的な課題を十分に理解できている経営層は少ない。
- 経営層は、日頃より CISO 等とコミュニケーションを図り、自らの考えや関心事項を伝達しておくことが必要である。CISO 等も経営層の経営・事業的な関心を把握することが求められる。

Ⅱ. CISO 等に求められる役割

- 専任の CISO 等を任命している企業が少ない。CISO 等の役割や責任が明確になっていないことも一因と考えられる。経営層には、CISO 等が主体的にセキュリティに関する取組みを進めることができるように、CISO 等の業務内容や責任を明確にし、業務執行に必要な権限を付与することが求められる。
- CISO 等に対して、技術的役割だけではなく、経営・事業的役割も担うことを期待している企業が多数存在する。多くの経営層がセキュリティの重要性を理解している。この点に関する限りは、多くの企業がサイバーセキュリティ対策を経営課題と捉えている。
- 経営層が求めるリスク評価や人材に関する情報を必ずしも CISO 等が報告できていない。この理由として人材に関しては CISO 等の役割定義の曖昧さ、リスク評価に関しては経営層と CISO 等とのコミュニケーション不足が一因であると考えられる。セキュリティ対策に必要なリソースを確保するためにも、CISO 等は、経営層の理解が得られる提案を行う必要がある。そのためには、CISO 等は日頃より経営層と接点を持ち、経営層の考えを理解しつつ、セキュリティ対策の必要性を説くことが重要である。
- セキュリティ人材の確保・育成が CISO 等の役割として重要視されている。
- セキュリティ人材が活躍できるようなキャリアパスの形成や、モチベーションを向上させる評価・報酬等の制度設計、組織文化の醸成などの取組みが求められる。

Ⅲ．CISO 等がサイバーセキュリティに関して重点的に取り組むべき課題

①サプライチェーンに対する具体的なセキュリティ対策

- サプライチェーンに対するセキュリティリスクへの理解度は高まっている。しかし、委託先の状況チェック等の対策が十分できていない企業が多い。
- 企業としては、サプライチェーンのパートナー企業等と責任範囲やセキュリティ対策に関する契約の締結や、定期的なチェックを通じた対策状況の把握等、まずは対応可能な範囲から、対策に着手することが求められる。

②PDCA サイクルの実践

- 多くの企業において、十分に PDCA サイクルの点検（Check）と改善（Act）を実施できているわけではない。
- サイバー演習のような実践の場においては、必ずしも緻密なシナリオを準備する必要はなく、実際に他社で発生したインシデント等が自社に起きた場合を想定し、対応方法を机上で検討する等の方法も有効と考えられる。

---

[1] 本報告書では、CISO（Chief Information Security Officer，最高情報セキュリティ責任者）または同等の責任者を「CISO 等」と定義する。

目次

1. はじめに

1.1. 調査背景・目的

近年、企業が、IT を積極活用した「攻めの経営」と、情報セキュリティのレベルを上げることによって情報資産を守る等の「守りの経営」とを高いレベルで両立するためには、経営層の示す経営方針に基づくセキュリティ対策の実践や、実務課題を踏まえた経営戦略の提示、企業内の総合調整や実務者層をリードできる人材が必要であるとされている。

また、独立行政法人情報処理推進機構（本報告書では、以下「IPA」と略記する）が実施した「CISO 等セキュリティ推進者の経営・事業に関する役割調査」(2018 年 3 月)[2]では、サイバーセキュリティ経営ガイドライン [3]等における、CISO 等及びサイバーセキュリティ対策を実施する上での責任者となる担当幹部の役割として、経営と事業貢献に関連する役割（本報告書では、以下「経営・事業的役割」と略記する）が重視されるとともに、その役割を実現させるための手引きや事例が求められていることを確認した。そして、「サイバーセキュリティ経営プラクティス作成」(2019 年 3 月)[4]では、経営ガイドラインを CISO 等が実践するための手引きや事例となるプラクティス集（本報告書では、以下「プラクティス集」と略記する）を作成した。こうした状況において、企業にはサイバーセキュリティ対策のための体制整備を含むリソース（人材・予算）の確保、経営層の意識改善、CISO 等の経営・事業的役割等の課題が山積している。

そこで、経営層を支える CISO 等の対策実践力を更に強化・支援し、国内企業のセキュリティに対する取組みのレベル向上に資することを目的として、サイバーセキュリティの脅威や対策の進化および、それらについての CISO 等の在り方や意識の変化等について調査を実施した。

なお、本報告書では、経営層が「CISO 等」を担うケースも想定されるが、本報告書においては、便宜上、「経営層」と「CISO 等」とを区別する。

---

[2] IPA「CISO 等セキュリティ推進者の経営・事業に関する役割調査」(2018 年 3 月)
[3] 経済産業省「サイバーセキュリティ経営ガイドライン Ver2.0」
[4] IPA「サイバーセキュリティ経営プラクティス作成」

1.2. 本調査の実施概要・本報告書の構成

本調査では、CISO 等の経営・事業的役割に関する実態や企業のセキュリティ対策の取組みを把握するために、文献調査、アンケート調査、有識者・企業インタビュー調査を実施した。

本報告書の構成は、本章を含め 7 章構成である。各章の関係性を以下に記載する。文献調査を通じて構築したサイバーセキュリティに関する国内企業の経営層や CISO 等の動向に対する仮説に対して、アンケート調査やインタビュー調査を通じて検証を行った。その結果を踏まえ、国内企業のセキュリティに対する取組のレベル向上に資するための検討を実施した。

- 第 2 章：文献調査
  国内外の公開レポートや書籍等を対象に、CISO 等の経営・事業的役割や、企業のセキュリティ対策の取組みに関する文献調査を実施した。
- 第 3 章：アンケート調査
  「文献調査」の結果を踏まえ、国内企業の CISO 等の経営・事業的役割に関する実態や企業のセキュリティ対策の取組み状況を把握するために、アンケート調査を実施した。
- 第 4 章：有識者インタビュー調査
  経営ガイドライン記載の指示項目 4,6,10 を中心に、サイバーセキュリティ経営に関する実践事例や既存の取組の成功要因等を把握する為に、CISO 等に関する有識者に対してインタビュー調査を実施した。
- 第 5 章：企業インタビュー調査
  「CISO 等セキュリティ推進者の経営・事業に関する役割調査」(2018 年 3 月)[5]では、CISO 等の経営・事業に関する役割を検討する企業の参考となる手引きや事例が必要とされている。これを受け IPA では、CISO 等またはその実際の活動を良く知る役職員（CISO 等の指揮下の職員、 情報セキュリティ部門長、リスク管理部門長等の部門長、これらの補佐役の職員等）に対してインタビューを実施し、得られた参考情報を 2019 年 3 月にプラクティス集として取りまとめて公表している。今回は、このプラクティス集の内容の拡充を図るため、改めて複数の企業に同様の趣旨のインタビューを実地した。
- 第 6 章：調査結果のまとめ
  「文献調査」、「アンケート調査」、「有識者・企業インタビュー調査」の結果から、企業や CISO 等の動向、サイバーセキュリティ対策に関する課題についての示唆をとりまとめた。

[5] IPA「CISO 等セキュリティ推進者の経営・事業に関する役割調査」(2018 年 3 月)

- 第 7 章：データ集
  参考資料として、文献調査の結果およびアンケート調査の集計結果を記載した。

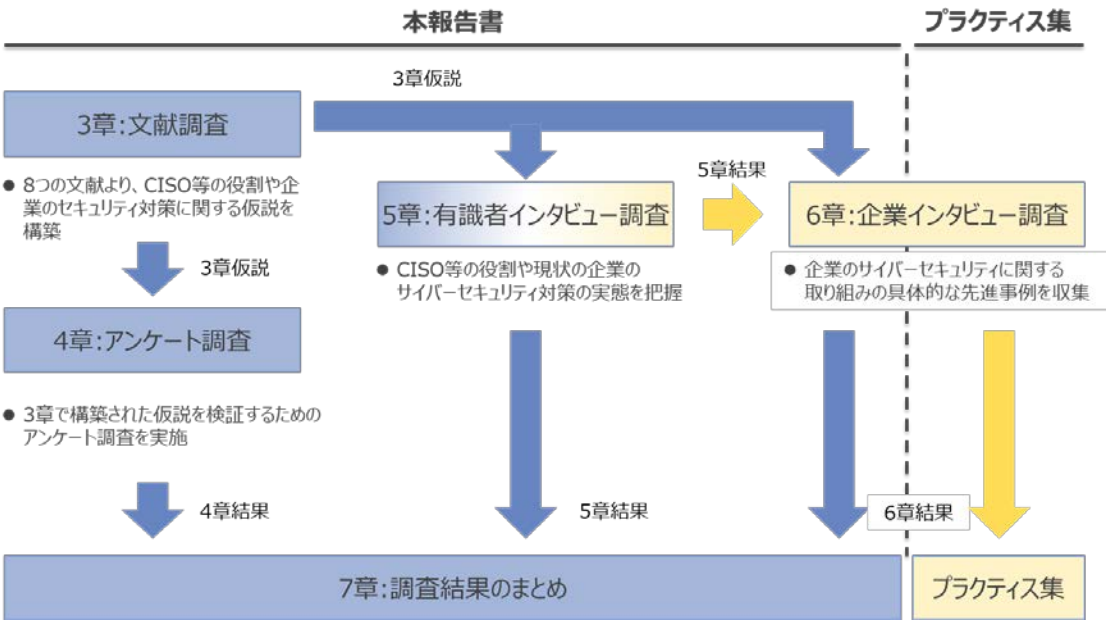

図 1-1 報告書の章構成

2. 文献調査

2.1. 調査概要

文献調査においては、下表に記載した 8 つの文献から、「サイバーセキュリティ経営ガイドライン Ver2.0」に定められている「サイバーセキュリティ経営の重要 10 項目」に準拠した上で、以下の 2 つの観点から情報を収集した。なお、各文献の概要および調査結果は 7 章データ集に記載する。

① CISO 等への期待や活動実態

② 経営層への期待や活動実態等のその他の有益な知見

表 2-1　調査文献一覧

文献番号	文献名	発行元
文献 1	CISO ハンドブック	日本ネットワークセキュリティ協会（JNSA）
文献 2	CybersecurityAssessmentTool	FFIEC
文献 3	CHIEF INFORMATION SECURITY OFFICER HANDBOOK	CIO Council
文献 4	FTSE 350 Cyber Governance Health Check 2018	Department for Digital, Culture, Media and Sport(UK)
文献 5	経営とサイバーセキュリティ -デジタルレジリエンシー	日経 BP 横浜 信一氏 著書
文献 6	LEVERAGING BOARD GOVERNANCE FOR CYBERSECURITY	Advanced Cyber Security Center
文献 7	NAVIGATING THE DIGITAL AGE	Palo Alto Networks
文献 8	Top CISO Trends	K logix

また、参考として、「サイバーセキュリティ経営ガイドライン Ver2.0」に定められている「サイバーセキュリティ経営の重要 10 項目及び、文献から情報を抽出する際の分類の視点について、以下に記載する。

表 2-2　サイバーセキュリティ経営の重要 10 項目 [6]

項目番号	重要項目	分類の視点
指示 1	サイバーセキュリティリスクの認識、組織全体での対応方針の策定	● 経営陣のサイバーセキュリティへの理解度の向上 ● 全社でのサイバーセキュリティ意識の向上 ● サイバーセキュリティにおけるリスクアペタイトの導入 ● 経営陣が定めるべきサイバーセキュリティに関する事項
指示 2	サイバーセキュリティリスク管理体制の構築	● CISO の役割の明確化 ● CISO が定めるべきサイバーセキュリティに関する事項
指示 3	サイバーセキュリティ対策のための資源(予算、人材等)確保	● 対応リソースの確保 ● 研修・育成
指示 4	サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	● リスク評価プログラムの客観性の確保 ● サイバーセキュリティリスクの定量化 ● IT・情報資産の棚卸し （リスクプロファイル）
指示 5	サイバーセキュリティリスクに対応する為の仕組みの構築	● リスクプロファイルを踏まえた技術的対策
指示 6	サイバーセキュリティ対策における PDCA サイクルの実施	● ポリシーの見直し ● リスク管理の見直し ● インシデント対応計画の見直し
指示 7	インシデント発生時の緊急対応体制の整備	● インシデント対応計画の整備 ● 演習・訓練の定期的な実施
指示 8	インシデントによる被害に備えた復旧体制の整備	● インシデント対応計画と BCP との連携 ● 利害関係者を含む社内外への連携
指示 9	ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	● 外部委託先の管理 ● データ・サービスの連携先の把握 ● オープンソースライブラリ等、製品に含まれる新たな脅威の認識
指示 10	情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	● 脅威情報の収集 ● 脅威情報の分析・評価 ● 内部・外部への共有

[6] 経済産業省「サイバーセキュリティ経営ガイドライン Ver2.0」

2.2. 文献調査の考察

2.2.1. 経営層がサイバーセキュリティにおいて果たすべき役割

2.2.1.1. サイバーセキュリティに対する人材の育成・確保

まず、経営層が果たすべき役割として、サイバーセキュリティに対する人材の育成・確保がある。現状の問題として、サイバーセキュリティについての予算が、人材ではなく技術投資に集中していることがあげられる。この点について言及している主な文献は、文献 7「NAVIGATING THE DIGITAL AGE」（以降、文献 7）である。文献 7 では、「サイバーセキュリティ予算はその全額を防御に充てるのではなく、侵入に成功した攻撃の識別（発見）と事後対応（レスポンス機能）に充てるべきである。また、テクノロジーに投資するだけではなく、従業員の教育・啓発活動（攻撃者の攻撃活動がどのようなものか等）にも予算を投入するべきである」や「経営陣は、予算の配分について、技術的投資に偏重しがちで、従業員教育や人材育成の分野をないがしろにしている」と記載されている。

多くの経営層は、サイバーセキュリティを経営上のリスクとして認識しており、サイバーセキュリティへの技術的な対策の投資を増やす傾向が強くなってきていると考えられる。サイバーセキュリティへの投資において、短期的に効果を発揮する技術的な投資が優先されることは自然な流れである。しかし、中長期的な目線のサイバーセキュリティ対策として、経営層はサイバーセキュリティに対する人材の育成・確保に注力していく必要がある。サイバーセキュリティに対する人材の育成・確保のためには、サイバーセキュリティ対策人材専用の新しい人材育成体系の構築や新たなキャリアパスの構築が必要と考えられる。

2.2.1.2. CISO 等との密な関係の構築

次に、CISO 等やセキュリティ担当者等との密な関係構築がある。現状の問題として、経営層と CISO 等との関係に溝があることがあげられる。この点について、言及している主な文献は、文献 6「LEVERAGING BOARD GOVERNANCE FOR CYBERSECURITY」（以降、文献 6）と文献 8「Top CISO Trends」（以降、文献 8）である。文献 6 では、「取締役会は、CIO や CISO、その他リスク管理を所管する経営幹部と距離がある」や「CISO は、経営陣と直接コミュニケーションをとる機会が少ない」、文献 8 では、「CISO と取締役会との距離が遠い、役員から認知を得ていない」と記載されている。

経営層と CISO 等やセキュリティ担当者等との関係に溝があると、現場からエスカレーションされる情報と、経営層が必要とする情報の観点や粒度（サイバー攻撃の事業へのインパクトや想定被害、他社の動向等）の間に大きな差が生じてしまう可能性がある。また、経営層がサイバーセキュリティに関する意思決定を行うために必要な情報が現場からエスカレーションされないことによって、意思決定が遅延し、インシデントに対して有効な対策が講じられないことも想定される。このような事態にならないためにも、常日頃より、経営層は CISO 等との密なコミュニケーションを図り、密な関係の構築を行うことが必要と考えられる。また、文献 1「CISO ハンドブック」（以降、文献 1）では、「リズム・オブ・ビジネスや

事業計画や目標の理解、数字、評価指標などを織り交ぜることにより共通言語での相互理解が望ましい」と記載されており、経営層と CISO 等は、一方通行ではなく、お互いを理解しあえる双方向のコミュニケーションを図ることが重要であると考えられる。

2.2.1.3. サイバーセキュリティを理解した上での意思決定

最後に、サイバーセキュリティへの投資や対策において、インシデントによる自社事業へのインパクトを把握した上で意思決定を行うことがあげられる。現状の問題として、経営層のサイバーセキュリティの理解度があまり高くない企業が存在していることと、インシデントによる自社事業へのインパクトを把握せずに、投資や対策の意思決定をしていることがあげられる。この点について言及している主な文献は、文献 3「CHIEF INFORMATION SECURITY OFFICER HANDBOOK」（以降、文献 3）、文献 4「FTSE 350 Cyber Governance Health Check 2018」（以降、文献 4）、文献 6、文献 7 である。文献 3 では、「現状のリスクと想定される攻撃を把握したうえで、その対策となるサイバーセキュリティソリューションを具体的に準備できている企業は少ない」、文献 4 では、「経営陣は、サイバー攻撃の被害想定（株価や営業損失など金銭的なリスク、レピュテーショナルリスク等）が十分に理解できていない」、文献 6 では、「サイバーセキュリティをデジタル戦略の一環としてとらえる風土が醸成されていないのではないか」、文献 7 では、「経営陣のサイバーセキュリティへの理解度が低い」や「経営陣は、サイバー攻撃により社内の各種資源が汚染された場合を想定していない」、「経営陣は、サイバーセキュリティに対処できる技術的な専門家を、経営メンバーに加えていない」、「経営陣は、社内外で発生しているサイバー攻撃事案に関する情報収集と自社へ波及する影響についての分析をおろそかにしている」と記載されている。

効果的なサイバーセキュリティ対策を行うためには、インシデントによる自社事業へのインパクトを把握したうえでその意思決定を行うことが重要である。自社事業へのインパクトを把握するためには、同業他社の動向やインシデント発生時のレピュテーショナルリスクや顧客サービスの提供停止に伴う機会損失、監督当局の指導・監督の動向、過去のセキュリティへの投資やセキュリティ対策の実績とその効果等を総合的に理解することが必要であると考えられる。

2.2.2.CISO 等がサイバーセキュリティにおいて果たすべき役割

2.2.2.1.情報収集やサイバーセキュリティ対策のための人的リソースの確保

まず、CISO 等がサイバーセキュリティにおいて果たすべき役割として、人的リソースを確保することがあげられる。現状の問題として、脅威情報の収集やその分析・評価、社内への共有を行うための十分な人的リソースが不足していることがある。この点について言及している文献は、文献 1「CISO ハンドブック」（以降、文献 1）と文献 3 である。文献 1 では、「脅威情報の収集を行うチャネルを確保する必要があるが、情報収集先や収集の手順が定義できていないケースがある」、文献 3 では、「人材不足の昨今、人的リソースをサイバーセキュリティに自由に振り分けられるほど余裕がある企業は少ない」と記載されている。

脅威情報の収集や分析は、人的リソースの多寡やその質によって、対応のレベルが大きく左右されるため、CISO 等は経営層に働きかけ、十分な人的リソースを確保することが求められる。

2.2.2.2.サプライチェーンのリスクの特定・対応策の構築

次に、経営層がサプライチェーンへのセキュリティ対策の必要性を認識している状況下で、CISO 等はサプライチェーンのリスクの特定とそれに対する対応策を実行することがあげられる。現状の問題として、委託先等のサプライチェーン上のパートナー企業等の管理や、そのリスクを把握できていないことがある。この点について言及している主な文献は、文献 2「Cyber security Assessment Tool」（以降、文献 2）と文献 4、文献 5「経営とサイバーセキュリティ- デジタルレジリエンシー -」（以降、文献 5）である。文献 2 では、「委託先のサイバーセキュリティを管理・分析するプロセスを整備することが求められている」、文献 4 では、「自社と直接契約関係にはないものの、自社サービスのサプライチェーンに関係する事業者に係るサイバーリスクについても認識する必要がある」、「自社サービスのサプライチェーンに影響する事業者、およびそのリスクについて特定できていない」と記載されている。また、文献 5 では、「情報システム・制御システム・委託先・調達先等それぞれに想定されるリスクを洗い出し、ビジネスの観点から優先順位付けを行う」と記載されており、社内システムだけではなく、サプライチェーン（委託先や調達先を含む）のリスクの洗い出しの必要性も示唆されている。

多くの CISO 等は、自社が取り扱う顧客情報や製品情報が、自社以外のどの外部組織へどのような形で保管されているのかを把握できていないことが想定される。サプライチェーンのサイバーセキュリティを強固なものにするためには、サプライチェーンのサイバーリスクの範囲（委託先、再委託先、クラウド、オープンソースソフトウェア、ウェブサイト構築事業者等）を特定し、自社のビジネスに応じた実効的な対応策の構築が必要であると考えられる。

2.2.2.3. サイバーセキュリティ対策における PDCA サイクルの実践

最後に、サイバーセキュリティ演習等を通じた、サイバーセキュリティ対策における PDCA サイクルを実践することがあげられる。現状の問題として、インシデント対応計画の精緻化ができていないことや、計画の点検（Check）と改善（Act）が実践できていないことがある。この点について言及している主な文献は、文献 1 と文献 4 である。文献 1 では、「CISO は、マネジメントサイクルを単なる改善だけではなく、企業としての学習と成長につなげていく。そのためにも情報セキュリティ計画を丹念に検討し、その評価を通じて事業部門・他部門・経営陣といったステークホルダーと協力を得ることが望ましい」、文献 4 では、「インシデント対応計画は事業計画に整合しているかを定期的に見直すべき」と記載されている。

サイバー攻撃は絶えず変化を続けるため、サイバーセキュリティ対策は常に改善していく必要がある。新たな脅威に対応するためには、絶えずサイバーセキュリティ対策の見直しと改善が必要であり、PDCA サイクルを強化していくことが求められている。

2.3. 調査結果

調査結果のまとめとして、8つの文献から「サイバーセキュリティ経営ガイドラインVer2.0」に定められている「サイバーセキュリティ経営の重要10項目」に準拠した上で、収集した情報（知見）を以下に整理した。なお、8つの文献から収集した詳細な情報は、7章データ集に記載した。

表 2-3　8つの文献から収集した主な情報（知見）

項目番号	CISO等への期待や活動実態	経営層への期待や活動実態等のその他の有益な知見
指示1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定	● リズム・オブ・ビジネスや事業計画や目標の理解、数字、評価指標などを織り交ぜることにより共通言語での相互理解が望ましい（文献1） ● 経営陣とのコミュニケーションの機会が少ない（文献6） ● CISOが役員から認知されていない（文献8）	● 取締役会とCISO等の経営幹部との間に距離がある（文献6） ● 経営陣は、サイバー攻撃の被害想定（レピュテーショナルリスク等）を十分に理解できていない（文献4） ● 経営陣のサイバーセキュリティへの理解度が低い（文献7）
指示2 サイバーセキュリティリスク管理体制の構築	● CISOには、企業・ビジネス全体のリスクを把握することと、社内各層に対するコミュニケーション能力が求められる（文献2） ● 技術部門と非技術部門の橋渡しをするための高いコミュニケーションスキルが必要である（文献7）	● サイバーセキュリティをデジタル戦略の一環としてとらえる風土が醸成されていない（文献2）
指示3 サイバーセキュリティ対策のための資源(予算、人材等)確保	● CISOには、セキュリティ人材を安定的に育成・供給する仕組みを構築する役割が求められる（文献8）	● テクノロジーへの投資だけではなく、従業員の教育・啓発活動にも予算を投入するべきである（文献7）
指示4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	● 情報システム・制御システムだけではなく、委託先・調達先等それぞれに想定されるリスクを洗い出し、ビジネスの観点から優先順位付けを行う（文献5）	● 現状のリスクと想定される攻撃を把握したうえで、具体的なソリューションを準備できている企業は少ない（文献3）
指示5 サイバーセキュリティリスクに対応するための仕組みの構築	● 個々のシステムのログではなく、総合的にログを収集管理できる管理基盤を構築すること(文献1) ● セキュリティに関する従業員の教育や注意喚起についての仕組みを構築すること（文献8）	● 経営陣は、技術的な専門家を経営メンバーに加えていない(文献7)
指示6 サイバーセキュリティ対策におけるPDCA	● CISOは、ITやリスク部門のみならず、他部門や経営陣を巻き込んで情報セキュリティ計画を精緻化していくことが求められるが、	● 事業計画の見直しと合わせた、定期的なインシデント対応計画の見直しができていない企業が多い（文献4）

項目番号	CISO 等への期待や活動実態	経営層への期待や活動実態等の その他の有益な知見
サイクルの実施	十分にコミュニケーションが取れていないケースがある（文献 1）	
指示７ インシデント発生時の緊急対応体制の整備	● 万一の場合（業務停止等）に備え、その際の意思決定プロセスを訓練しておくべきである（文献 5）	● 経営陣は、インシデント発生時にコミュニケーションをとる関連部門との関係性の構築と使用する各種ドキュメントの整備に注力する必要がある（文献 7）
指示８ インシデントによる被害に備えた復旧体制の整備	● インシデント発生時は、CISO が取締役会に報告を行い、意思決定する必要がある（文献 7）	● CSIRT にとどまらない、社内の複数部門と連携した利害関係者への対応をインシデント対応計画に盛り込むことが重要である（文献 1）
指示９ ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	● 自社と直接契約関係にはないものの、自社サービスのサプライチェーンに関係する事業者に係るサイバーリスクについても認識する必要がある（文献 4） ● 現状は、自社サービスのサプライチェーンに影響する事業者、およびそのリスクについて特定できていない（文献 4） ● 業務委託先等のセキュリティレベルを管理監督する必要がある（文献 5）	● 平時における情報収集にリソースを投入できていない（文献 6）
指示１０ 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	● サイバーキュリティ事象や脅威情報について、情報収集を行うリソースやチャネルを確保する必要があるが、規程等で情報収集先や情報収集手順が定義できていないケースがある（文献 1）	● 経営陣は、社内外のサイバー攻撃の情報収集と自社への影響の分析をおろそかにしている（文献 7）

3. アンケート調査

3.1. 調査概要

「文献調査」の結果を元に構築した仮説を踏まえ、企業の CISO 等の経営・事業的役割等に関する動向や企業のセキュリティ対策の取組み状況を把握するために、国内企業を対象にアンケート調査を実施した。本調査は、従業員数 301 人以上かつ CISO 等を任命している国内企業を対象とした。アンケート調査の概要を以下に記載する。

表 3-1　アンケート調査の概要

調査目的	「文献調査」の結果を踏まえ、国内企業の CISO 等の経営・事業的役割等に関する動向や企業のセキュリティ対策の取組み状況を把握する
調査対象	従業員数 301 人以上かつ、CISO 等を任命している国内企業
調査期間	2019 年 10 月 1 日～10 月 21 日
調査方法	ウェブアンケート調査およびアンケート票調査
回収結果	有効回答数 534 件
調査項目	● 回答企業の基本属性（業種、従業員数、CISO 等の任命状況等） ● セキュリティに関する会議体の実施状況やテーマ ● 経営層が必要とするサイバーセキュリティに関する情報 ● 経営層が CISO 等に求める・重視する役割 ● CISO 等に求められる重要なスキル・経験 ● サイバーセキュリティマネジメントの PDCA サイクル ● サプライチェーンに関する実践事例 ● インシデントレスポンスに関する実践事例 等　全 34 項目
データ精査	回答データに関して、下記の方針で精査し、該当したデータは、回答内容に不備や矛盾があり、信頼性に問題があると判断し、除外した ● 回答時間が 180 秒未満の回答 ● 10 問以上連続して同じ記号の選択肢を回答する不正な回答 ● 設問 34 まで回答がなされていない回答 ● 設問間で矛盾がある回答 ● 同一企業による重複回答

3.2. アンケート調査結果の考察

3.2.1. 経営層の動向

3.2.1.1. セキュリティ人材の育成・確保の重要度の理解

文献調査から、「中長期的な目線のサイバーセキュリティ対策として、経営層はサイバーセキュリティに対する人材の育成・確保が必要である」との示唆が得られた。

まず、セキュリティに関する会議体の実施状況を確認した設問（アンケート調査 Q9）では、「経営層が参加してセキュリティを議論する会議等はない」と回答した割合は 17.6%（図 3-6 参照）であり、約 80%以上の企業では、経営層によって、セキュリティに関する議論がなされていることが明らかになった。また、課題認識について確認した設問（アンケート調査 Q7）では、「経営層のリスク感度が低い」と回答した割合が 9.7%（図 3-2 参照）にとどまり、2017 年度の調査結果よりも減少している傾向が確認できた。

そして、セキュリティに関する会議体で付議された議題について確認した設問（アンケート調査 Q11）では、「サイバーセキュリティ人材の育成や採用に関する方針・計画」が付議されたと回答した割合が 19.5%（図 3-7 参照）であった。一方で、「インシデント発生時の組織的対策の方針・計画（52.9 %）」や「自社で発生したインシデントへの対応(61.2%)」（図 3-7 参照）等のインシデントに関して議論していると回答した割合が多かった。

以上の結果を踏まえ、経営層のセキュリティに対する全般的なリスク認識は高まってきていると考えられる。そして、経営層はセキュリティ人材の重要度は理解しているものの、人材に関するトピックが付議される割合がインシデント対応等の他のトピックよりも少ない傾向があるため、現状の優先度は低いと認識している可能性がある。CISO 等は、セキュリティに関する経営層が参加する会議体にて、セキュリティ人材の育成・確保の必要性を認識・理解してもらうための内容を盛り込んでいくことが今後の課題と考えられる。

3.2.1.2. 経営層と CISO 等とのコミュニケーション不足

文献調査から、「CISO 等との密な関係構築が必要である」との示唆が得られた。経営層と CISO 等との間の意思疎通の程度を図るために、「実際にセキュリティに関する会議体で議論された内容」（アンケート調査 Q11）と「経営層が求める情報」（アンケート調査 Q12）の結果を比較したところ、経営層が求める情報は「インシデントによる想定被害額等の定量的なサイバーリスク評価(54.5%)」（図 3-8 参照）や「定性的なサイバーリスク評価（46.8%）」（図 3-8 参照）である一方で、CISO 等が報告する割合は、それぞれ 16.5%、 34.4%（図 3-7 参照）にとどまっており、両者に差が見られる。[7]また、人材についても、37.8%（図 3-8 参照）の企業が、経営層が求める情報と回答しているにもかかわらず、実際に付議される企業は

[7] なお、アンケート調査 Q11 は、アンケート調査 Q9 にて経営層が参加するセキュリティに関する会議体があると回答した企業のみを対象に集計しているため、アンケート調査 Q12 と分母（n）が異なっている。

19.5%（図 3-7 参照）にとどまっている。この理由としては、経営層と CISO 等との間の日頃のコミュニケーション不足や CISO 等の経営・事業的な意識の不足が考えられる。経営層は、日頃より CISO 等とコミュニケーションを図り、自らの考えや関心事項を伝達しておくことが必要であると考えられる。一方で、CISO 等も経営・事業的な観点から経営層の関心を推し量る取組みが必要であると考えられる。

3.2.1.3. サイバーセキュリティが事業へ及ぼすインパクトを重要情報と認識

文献調査から、「経営層はサイバーセキュリティが自社へ与えるインパクトを理解した上で意思決定をすることが重要である」との示唆が得られた。経営層がサイバーセキュリティに関する意思決定を行う際に重視する情報を確認した設問（アンケート調査 Q13）では、端的に、「レピュテーショナルリスク（10.1%）」（図 3-9 参照）や「定量的なサイバーリスク評価(37.1%)」（図 3-9 参照）と回答した割合は小さい。一方で、「自社で発生したインシデントの内容(62.0%)」（図 3-9 参照）や「同業他社で発生したインシデントの内容（44.9%)」（図 3-9 参照）などインシデントに関する情報が重視されている。実際に発生したインシデントの情報は、そのインシデントが自社の事業に対して発生した場合にどのようなインパクトをもたらすかということの予測に活用できるため、事業へのインパクトを重視していると捉えることができる。

また、サイバーリスクの分析結果を事業リスク評価に役立てているかどうかを確認した設問（アンケート調査 Q8）から、50%以上（図 3-3 参照）の企業が、サイバーリスクの分析結果を事業リスク評価に役立てられていないことが明らかになった。なお、IT 依存度が高い企業ほど、サイバーリスクの分析結果を事業リスク評価に活用している傾向が確認できた。

以上を踏まえ、他社等のインシデント事例を重要な情報として認識し、自社事業へのインパクトを把握しようとしている経営層は多いものの、定量的・定性的にサイバーリスク評価を実施し、その結果を事業リスク評価に活用できている経営層は比較的多くはないと考えられる。

3.2.1.4. PDCA サイクルの更なる強化が必要

文献調査から、「サイバーセキュリティ演習等を通じた、サイバーセキュリティ対策における PDCA サイクルを実践することが重要である」との示唆が得られた。企業の PDCA の取組み状況を確認するための設問(アンケート調査 Q24)では、Check として、「演習/訓練」、「情報収集」、に取り組む企業はそれぞれ約 50%(図 3-10 参照)であった。Act として、「関係規定類の見直し」を実施する企業は約 50%程度(図 3-10 参照)であったが、「リスク評価の見直し」を実施する企業は約 40%(図 3-10 参照)、さらに「体制の充実化」を実施する企業は約 25%(図 3-10 参照)であった。サイバーセキュリティ対策における Check の手法は、自己評価と第三者評価に分類できる。自己評価は、自組織の現状のセキュリティ対策の効果や完成度を、演習や訓練、チェックリストを利用して実施できる。自社で実施するため、第三者による評価よりも手間や時間、費用の負担が少ない。一方で、第三者評価は、独立した専門家によって現状のセキュリティ対策に対する客観的な評価を実施することである。費用と時間を考慮し、自己評価と第三者評価を組み合わせて、自社のセキュリティ対策の向上に向けて活用していくことが有効である。そして、その評価を基に、現状のセキュリティ対策の問題を把握し、セキュリティ計画の見直しや体制の整備(人材の育成等)等の改善を行うことが必要である。サイバーセキュリティ対策は、特定の対策を実装・実施して完了するわけではない。サイバー攻撃は常に変化し、新たな脅威が発生する可能性を念頭に、定期的なセキュリティ対策の有効性の確認とその改善が求められる。

3.2.2.CISO 等の動向

3.2.2.1.サイバーセキュリティ人材の確保が課題

文献調査から、「サイバーセキュリティ対策のための人的リソースの確保が重要である」との示唆が得られた。CISO 等をサポートする人材の動向を確認するために、CSIRT の人員の配置状況を確認した設問（アンケート調査 Q31）では、平常時やインシデント発生時にかかわらず常に CSIRT 専任の人員が配置されている割合は 22.8%（図 3-14 参照）にとどまっていた。また、平常時に兼任として CSIRT に配置されている場合は、68.3%（図 3-14 参照）であった。そして、課題認識について確認した設問（アンケート調査 Q7）では、「担当者の専門知識が不足している」と回答した割合は、2017 年度の調査結果よりも増加している傾向が確認できた。平常時に兼任として人員を配置する企業が多いものの、専任の人員を配置している企業は多くはない（サイバーセキュリティ人材を十分に確保できていないと推察される）ため、サイバーセキュリティに関する脅威情報の収集やその情報の分析、リスク評価等への活用、分析結果の社内への共有等が十分に実施できている企業は少ないと推察できる。CSIRT の設置目的を確認した設問（アンケート調査 Q32）では、「インシデント発生時の被害の拡大防止」を設置目的と回答する企業が最も多かった（図 3-15 参照）。しかし、専任の人員が少ないことによって、いざインシデントが発生した際に、事業の内容に即した迅速かつ十分な初動対応ができない可能性も考えられる。

3.2.2.2.サプライチェーンのリスク認識は高いが対策は不十分

文献調査から、「サプライチェーンのリスクの特定・対応策の構築が重要である」との示唆が得られた。サプライチェーンのリスク認識について確認した設問（アンケート調査 Q25）では、サプライチェーンのリスクを「リスクと認識していない」と回答した割合は 2.8%（図 3-11 参照）、「わからない」と回答した割合は 3.9%（図 3-11 参照）にとどまり、企業のサプライチェーンに対するリスク認識は高まっていると考えられる。また、IT 依存度が高い企業ほど、サプライチェーンのリスク認識が高い傾向があることも確認できた。なお、「社外のクラウドサービス利用（70.8%）」（図 3-11 参照）や「重要情報の社外保管（61.8%）」（図 3-11 参照）等については、突出してリスク認識が高いことが確認できたが、「社内でのソフトウェア利用（36.1%）」（図 3-11 参照）や「社内で利用するソフトウェアへのオープンソースライブラリの取込み（23.8%）」（図 3-11 参照）のリスク認識は相対的に低かった。クラウドや委託先の管理に関するリスク認識は高いものの、社外から調達したソフトウェアやオープンソースの脆弱性等に対するリスクを認識している企業は多くはないと考えられる。

一方で、サプライチェーンセキュリティへの対策として、実施されている対策は「契約条項へのセキュリティ要求事項の追加（60.5%）」（図 3-13 参照）が主であり、「チェックシートによる委託先管理（35.4%）」（図 3-11 参照）や「技術的な対策（39.7%）」（図 3-13 参照）を実施している企業は相対的に少ない。また、「委託先からの納品時にセキュリティチェックを実施している」と回答した企業は約 15%（図 3-13 参照）に留まっている。すなわち、

多くの企業は、形式上、書面での契約にセキュリティの要求事項を盛り込む程度にとどまっており、実際にチェックシート等を通じたサプライチェーン上の企業のセキュリティ対策の管理や技術的対策を実施できている企業は少ない可能性がある。サプライチェーンを踏み台としたサイバー攻撃として、委託先等のサプライチェーン上の関連企業を狙った攻撃とソフトウェア製品のサプライチェーンの脆弱性を狙った攻撃等が想定される。いずれの攻撃に対しても、確実に防ぐことができる対策を実施することは困難であるが、重要情報へのアクセスの制限やネットワークの監視、最新のソフトウェアの利用、従業員への教育の実施、チェックシートやヒアリング等を活用した、サプライチェーン企業におけるセキュリティ対策状況の確認等の対策が求められる。

3.2.2.3. 経営・事業的な役割や、経営層等に対するコミュニケーションスキルが重要

CISO 等に期待する役割やスキルについて確認した設問から、期待される役割として、「経営・事業的な役割」や「セキュリティ人材の育成・確保」、スキルとして「コミュニケーションスキル」が求められていることが明らかになった。

まず、「経営・事業的な役割」については、CISO 等に対して「技術的な役割」のみを期待する割合が 2017 年度の調査結果よりも減少していることが確認できた。また、CISO 等の以前の所属を確認した設問（アンケート調査 Q17）では、約 60%（図 3-19 参照）が非 IT システム関連部門の出身であった。さらに、CISO 等に求めるスキルを確認する設問（アンケート調査 Q18）から、「IT スキル」を重要とする割合（図 3-20 参照）も 2017 年度の調査結果より減少していた。そして、CISO 等をサポートするメンバーの配置の理由を確認した設問（アンケート調査 Q29）では、「CISO 等がセキュリティの専門家ではなく、専門知識を持ったメンバーがサポートする必要がある」と回答した割合が、約 60%（図 3-22 参照）と最も高いことが確認できた。以上のことから、CISO 等に求められる役割が、IT やセキュリティ等の技術的な役割から、経営・事業的な役割にシフトしてきていると考えられる。

CISO 等に求められる役割の変化に伴い、CISO 等に任命されるキャリアパスについて、今後は、IT システム関連部門だけではなく、コーポレート部門や事業部門の出身者が CISO 等へ登用されるケースが増加することが予想される。

また、「セキュリティ人材の育成・確保」を、役割として CISO 等に求める企業は現状、11.4%（図 3-21 参照）にとどまるが、31.8%（図 3-21 参照）の企業が今後重視する役割として認識している。つまり、「人材の育成・確保」の役割を果たしている CISO 等は現時点では多くはないが、今後は CISO 等に必要とされる役割ということである。これらの結果より、サイバーセキュリティ人材の確保に課題認識を有している企業が多く存在していると考えられる。

最後に、「コミュニケーションスキル」については、経営層や他の関係者との関係を構築するために重要なスキルと考えられる。また、CISO 等に求めるスキルを確認する設問（アンケート調査 Q18）（図 3-20 参照）では、コミュニケーションスキルの重要性が、2017 年

度の調査結果よりも増加している傾向が確認できた。一方で、プレゼンテーションスキル（わかりやすい資料作成、説明力等）が求められる割合は、コミュニケーションスキル（経営層や現場、ステークホルダーとの折衝・交渉力等）よりも相対的に低く、経営層に対する対面での説得力のあるコミュニケーションが求められていると考えられる。

3.3. アンケート調査結果

3.3.1. 分析軸

今回の調査では、企業がサイバーセキュリティを経営・事業的リスクと捉えるかどうかは、各企業の事業がどの程度 IT を活用しているかに依存すると仮定し、「IT 依存度」という軸を設定して、分析を実施した。「IT 依存度」は、アンケート調査 Q6「事業の IT システム・IT サービスへの依存度」の回答を基に以下の通りに、カテゴリー1 とカテゴリー2、カテゴリー3、カテゴリー4 に分類した。「カテゴリー1 が最も IT 依存度が高く、カテゴリー4 が最も低い」と定義した。

表 3-2　IT 依存度のカテゴリー

分類	アンケート調査 Q6 の選択肢
カテゴリー1	IT システム・IT サービスが事業上 **必要不可欠な要素** であり、その停止は **事業全体または重要な事業の停止に繋がる**（金融、通販、ネット通販等）
カテゴリー2	顧客へのサービス提供や生産活動の **一部で IT システム・IT サービスを利用** しており、その停止は **事業の一部に大きく影響する**（重要インフラ業種等）
カテゴリー3	顧客へのサービス提供や生産活動の一部で IT システム・IT サービスを利用しているが、IT に依存しない代替手段等があるため、**一時的な停止であれば事業への影響は小さい**
カテゴリー4	IT システム・IT サービスは主に社内業務等に利用するのみで、その停止は **事業にあまり影響しない**

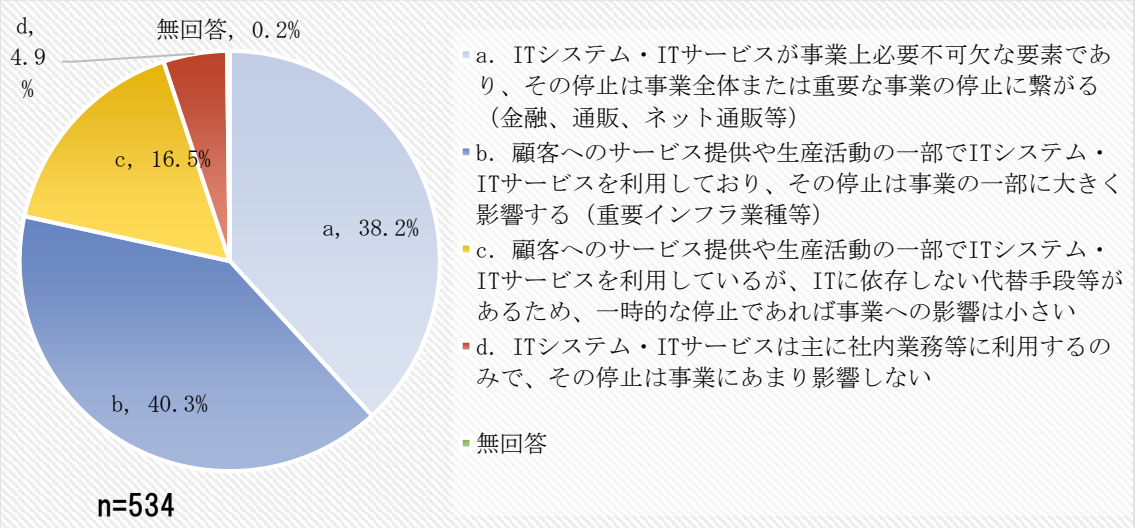
d, 4.9 %
無回答, 0.2%
c, 16.5%
a, 38.2%
b, 40.3%
n=534
a. ITシステム・ITサービスが事業上必要不可欠な要素であり、その停止は事業全体または重要な事業の停止に繋がる（金融、通販、ネット通販等）
b. 顧客へのサービス提供や生産活動の一部でITシステム・ITサービスを利用しており、その停止は事業の一部に大きく影響する（重要インフラ業種等）
c. 顧客へのサービス提供や生産活動の一部でITシステム・ITサービスを利用しているが、ITに依存しない代替手段等があるため、一時的な停止であれば事業への影響は小さい
d. ITシステム・ITサービスは主に社内業務等に利用するのみで、その停止は事業にあまり影響しない
無回答

図 3-1　IT 依存度

3.3.2. 調査結果

アンケート調査より、有意と判断した特徴的な調査結果を記載する。なお、先述した「IT依存度」の軸で分析をした調査結果の中でも、有意な差が確認できた調査結果のみを記載する。本パートで記載しない他のアンケート調査結果は、7 章データ集に記載した[8]。

3.3.2.1. サイバーセキュリティに関する経営層・企業の動向

① 課題認識（アンケート調査 Q7）

サイバーセキュリティに関する課題認識として、「リスクの見える化（45.7%）」や「インシデント発生に備えた準備（34.6%）」、「担当者の専門知識（30.0%）」を課題と認識する企業の割合が多い。一方で、「経営層のリスク感度が低い（9.7%）」や「経営層に IT やセキュリティの重要性を理解してもらえない（9.4%）」、「CISO 等の能力が不十分である（4.9%）」を課題と認識する企業の割合は少ない。

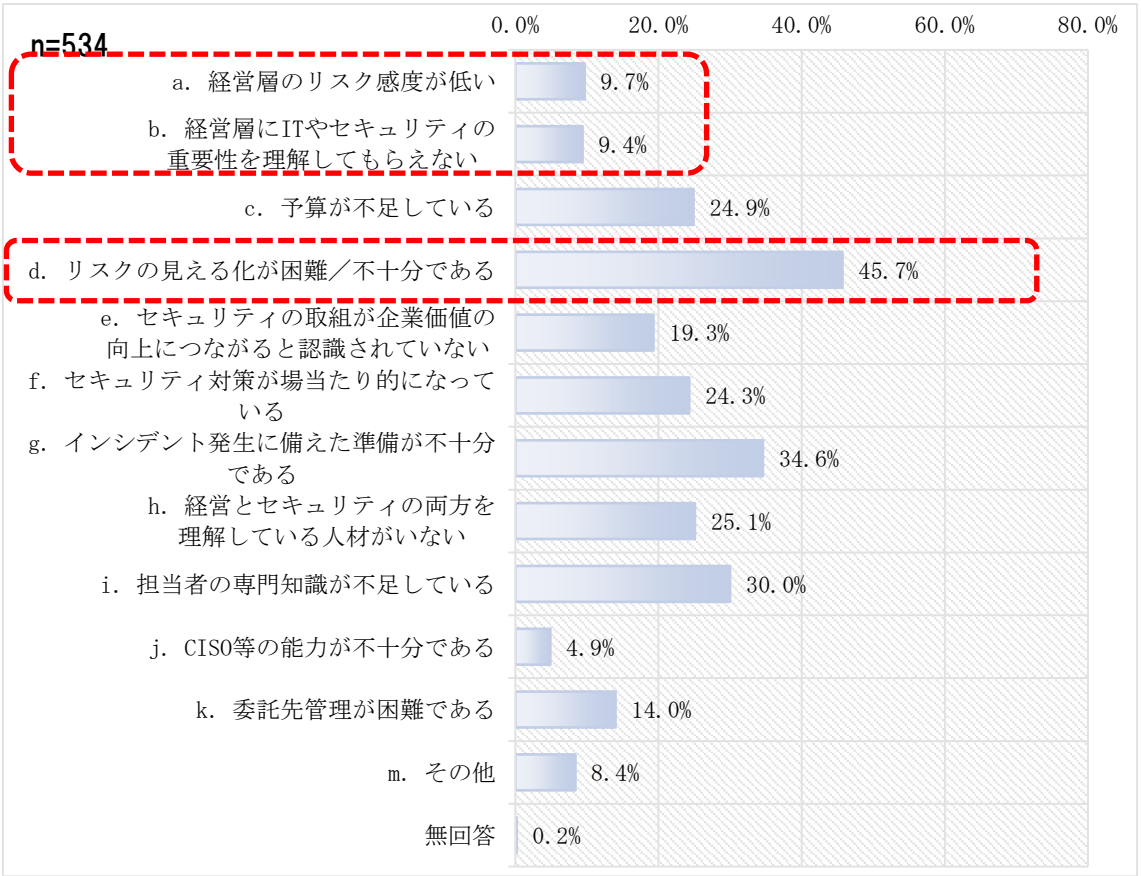

図 3-2 課題認識

[8] 構成比は小数点以下第 2 位を四捨五入しているため、合計しても必ずしも 100 とはならないグラフが存在する。

② セキュリティリスクの分析結果の事業リスクへの活用動向（アンケート調査 Q8）

情報漏洩やサイバー攻撃による社内システムの停止、サイバー攻撃による顧客サービスシステムの停止などのセキュリティリスクの分析結果について、経営層の事業リスク評価に役立てている企業は半数にも満たないことが明らかになった。情報漏洩を事業リスク評価に役立てている企業は 48.5%であったが、サイバー攻撃による社内システムの停止や顧客サービスシステムの停止を役立てている企業はそれぞれ 40.4%と 34.5%であった。

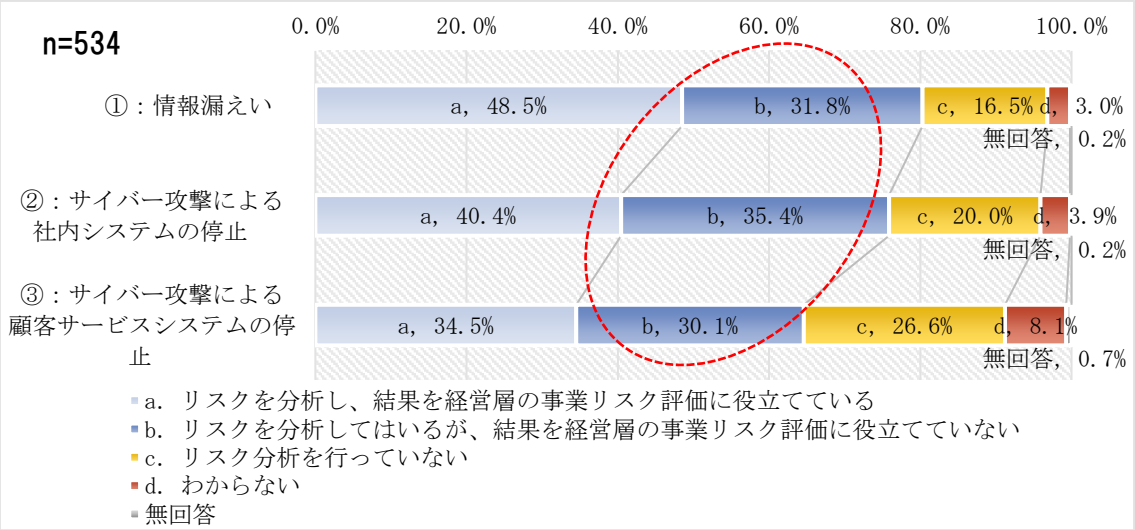

図 3-3 セキュリティリスクの分析結果の事業リスクへの活用の動向

また、CISO 等がいる組織においてもセキュリティに関する事業リスク評価が未実施である割合は 53.4%そのうち、リスク分析を行っていない組織の割合は 21.0%存在する。

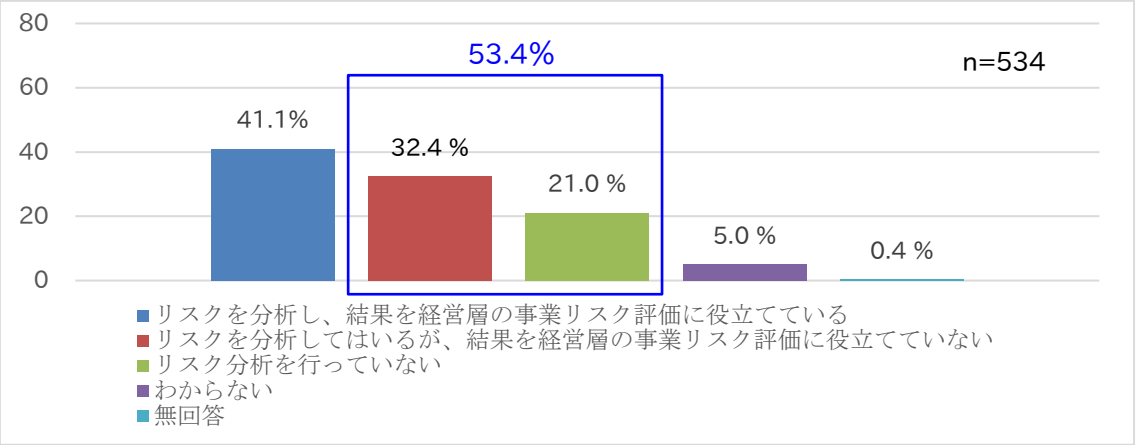

図 3-4　セキュリティリスクの分析結果の事業リスクへの活用

（図 3-3 において①,②,③の平均値を算出）

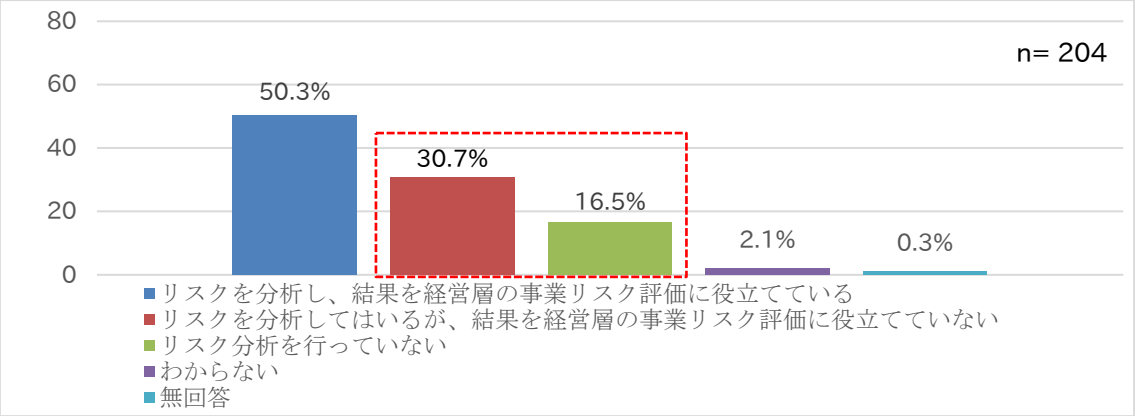

図 3-5　IT 依存度カテゴリー1 のセキュリティリスクの分析結果の事業リスクへの活用

（図 3-4 において IT 依存度カテゴリー1 の組織のみを抜粋）

さらに、「IT 依存度」の分析軸で比較すると、IT 依存度が高い企業であっても、セキュリティリスク分析を行っていない（16.5%）、またはリスク分析を行っていてもその結果を事業リスク評価に役立てていない割合は 30.7%であり、事業リスク評価につなげられていない企業が半数近く存在する。

③　セキュリティに関する会議体の実施状況（アンケート調査 Q9）

経営層が参加する会議等において、サイバーセキュリティに関する全社的な戦略や方針について議論されている会議体は、「役員会（10.1%）」や「サイバーセキュリティやリスク対応に特化した経営層が参加する会議（44.4%）」、「その他の経営層が参加する会議（23.6%）」が主な会議体であった。一方で、「経営層が参加してセキュリティを議論する会議等はない」と回答した割合は 18.6%であった。約 80%以上の企業では、経営層が参加する会議にてサイバーセキュリティについて議論を行っていることが明らかになった。

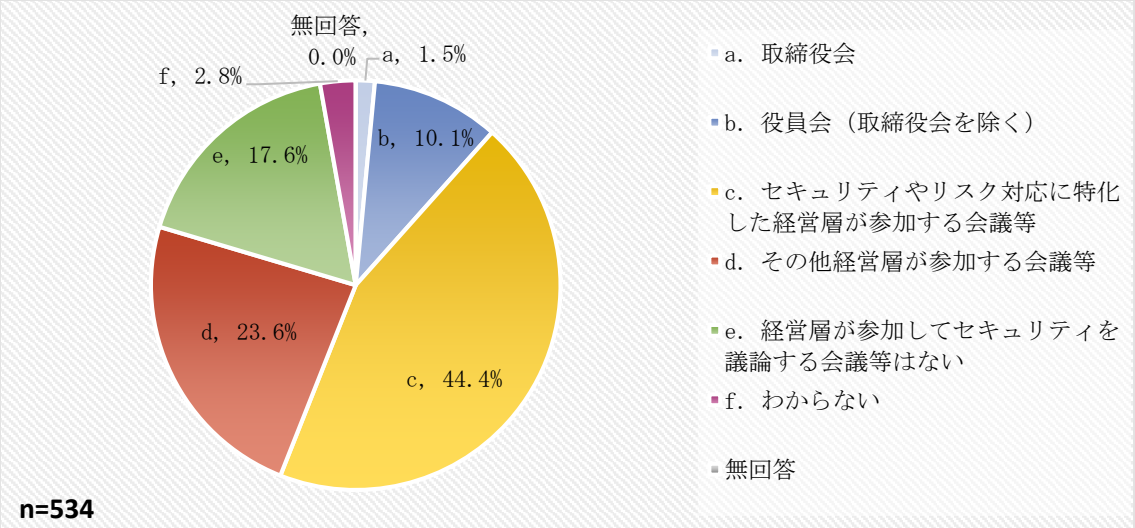

図 3-6　セキュリティに関する会議体の実施状況

④　セキュリティに関する会議体で議論された内容と今後報告が必要とされる内容
（アンケート調査 Q11・12）

経営層が参加するセキュリティに関する会議体で実際に取り上げられた内容として、「自社で発生したインシデントの対応（61.2%）」や「従業員のサイバーセキュリティの向上に向けた方針・計画（59.3%）」、「インシデント発生時の情報連携等の組織的対策の方針・計画（52.9%）」が上位を占め、「サイバーセキュリティ人材の育成や採用に関する方針・計画（19.5%）」や「インシデントによる想定被害額等の定量的なサイバーリスク評価（16.5%）」が付議される割合は低い。

一方で、経営層がサイバーセキュリティに関する意思決定を行うために、今後求める（報告を受ける必要がある）情報として、「インシデントによる想定被害額等の定量的なサイバーリスク評価（54.5%）」や「インシデント発生時の情報連携等の組織的対策の方針・計画（51.7%）」、「従業員のサイバーセキュリティ意識の向上に向けた方針・計画（50.7%）」への関心が高い。また、「インシデントによる定量的なサイバーリスク評価」や「サイバーセキュリティ人材の育成や採用に関する方針・計画」について、現在付議されている割合は、それぞれ 16.5%、19.5%である一方、今後報告が求められる割合は、それぞれ 54.5%、37.8%とギャップが見られた。

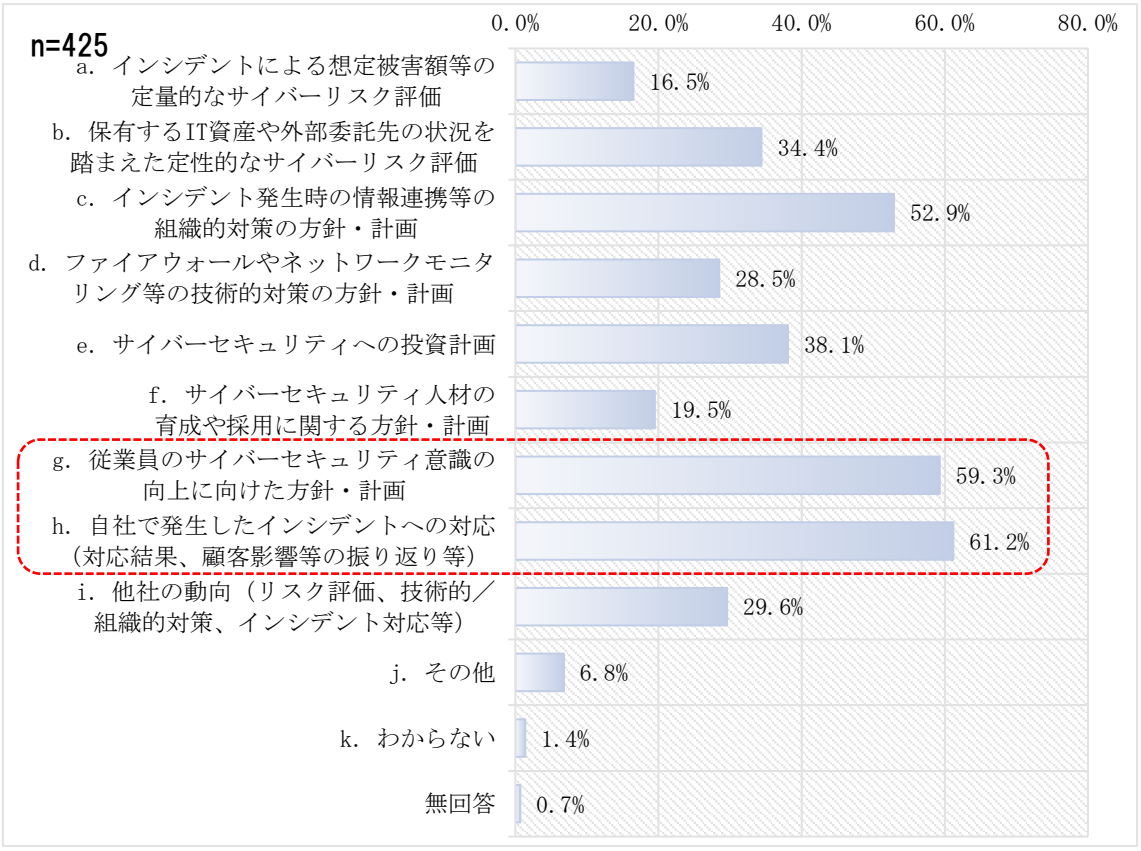

図 3-7　セキュリティに関する会議体で議論された内容

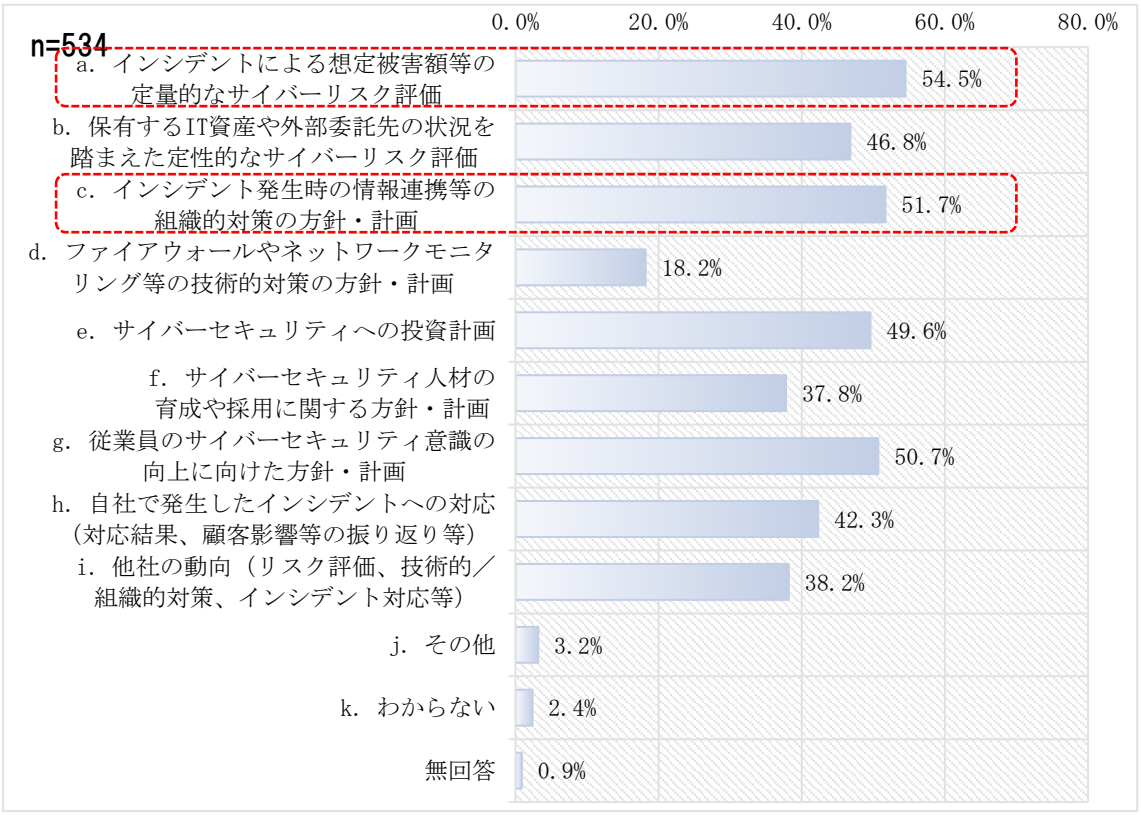

図 3-8　今後、経営層がセキュリティに関する会議体で求める情報

⑤　経営層がサイバーセキュリティに関する意思決定を行う際に重視する情報
（アンケート調査 Q13）

経営層は、サイバーセキュリティに関する意思決定を行うにあたり、「自社で発生したインシデントの内容（62.0%）」や「同業他社で発生したインシデントの内容（44.9%）」、「インシデントによる想定被害額等の定量的なサイバーリスク評価（37.1%）」を重視している。

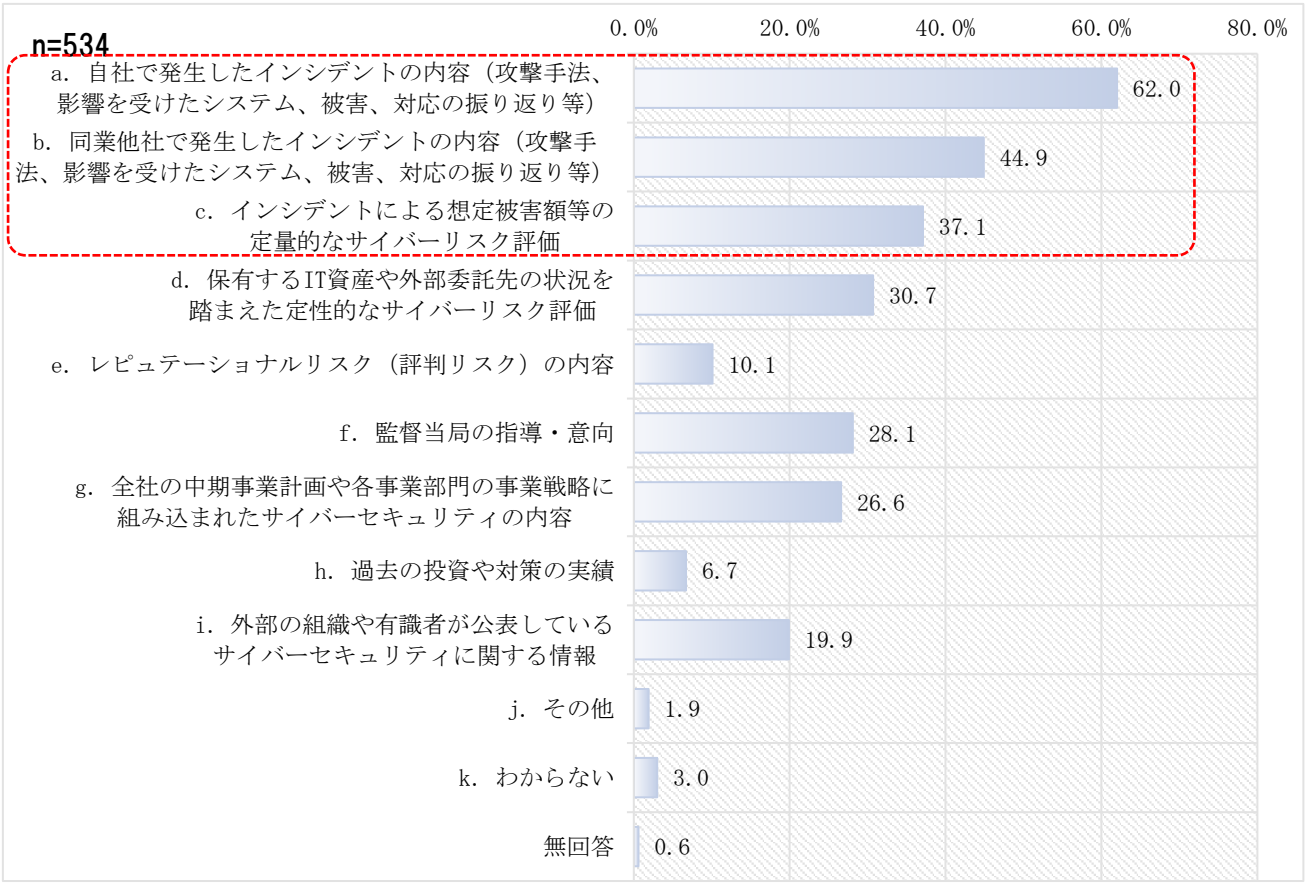

図 3-9　経営層がサイバーセキュリティに関する意思決定を行う際に重視する情報

⑥　PDCA サイクルにおける C と A の取組み（アンケート調査 Q24）

サイバーセキュリティ対策の PDCA サイクルを実践するために、Check の観点では、「脅威情報や脆弱性情報、インシデント情報の収集・分析（54.3%）」や「サイバーセキュリティ演習/訓練（49.6%）」に取り組んでいる企業は全体の約 5 割であった。その一方で、Act の観点では、「サイバーセキュリティ関係規定類の見直し（52.1%）」を実施する企業は 5 割以上見られたものの、「リスク評価の見直し（39.5%）」や「サイバーセキュリティ対応体制の充実化（26.2%）」に取り組む企業は相対的に少ない。

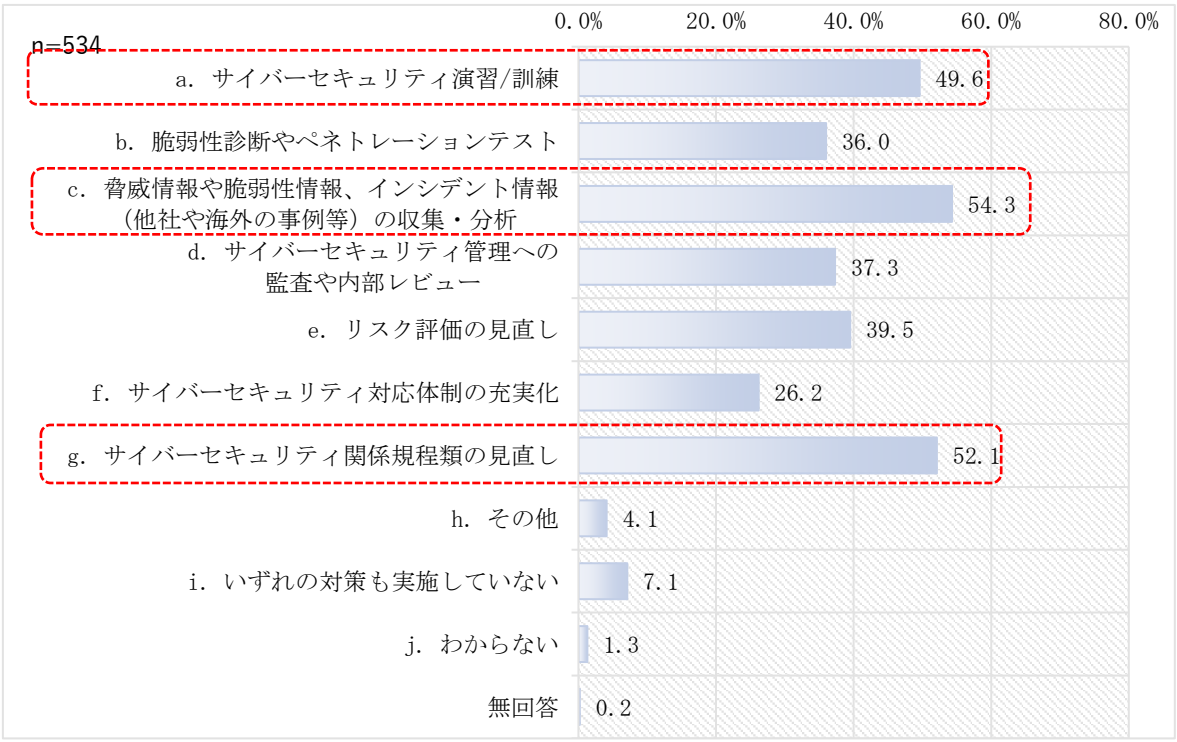

図 3-10　PDCA サイクルにおける C と A の取組み

⑦　サプライチェーンセキュリティのリスク認識（アンケート調査 Q25）

サプライチェーンのサイバーセキュリティリスクとして、「社外のクラウドサービス利用（70.8%）」や「顧客情報や限定提供データの社外保管（61.8%）」をリスクと認識している企業が多い。一方で、「社内で利用するソフトウェアへのオープンソースライブラリへの取組み（23.8%）」をリスクと捉える企業は相対的に少ない。

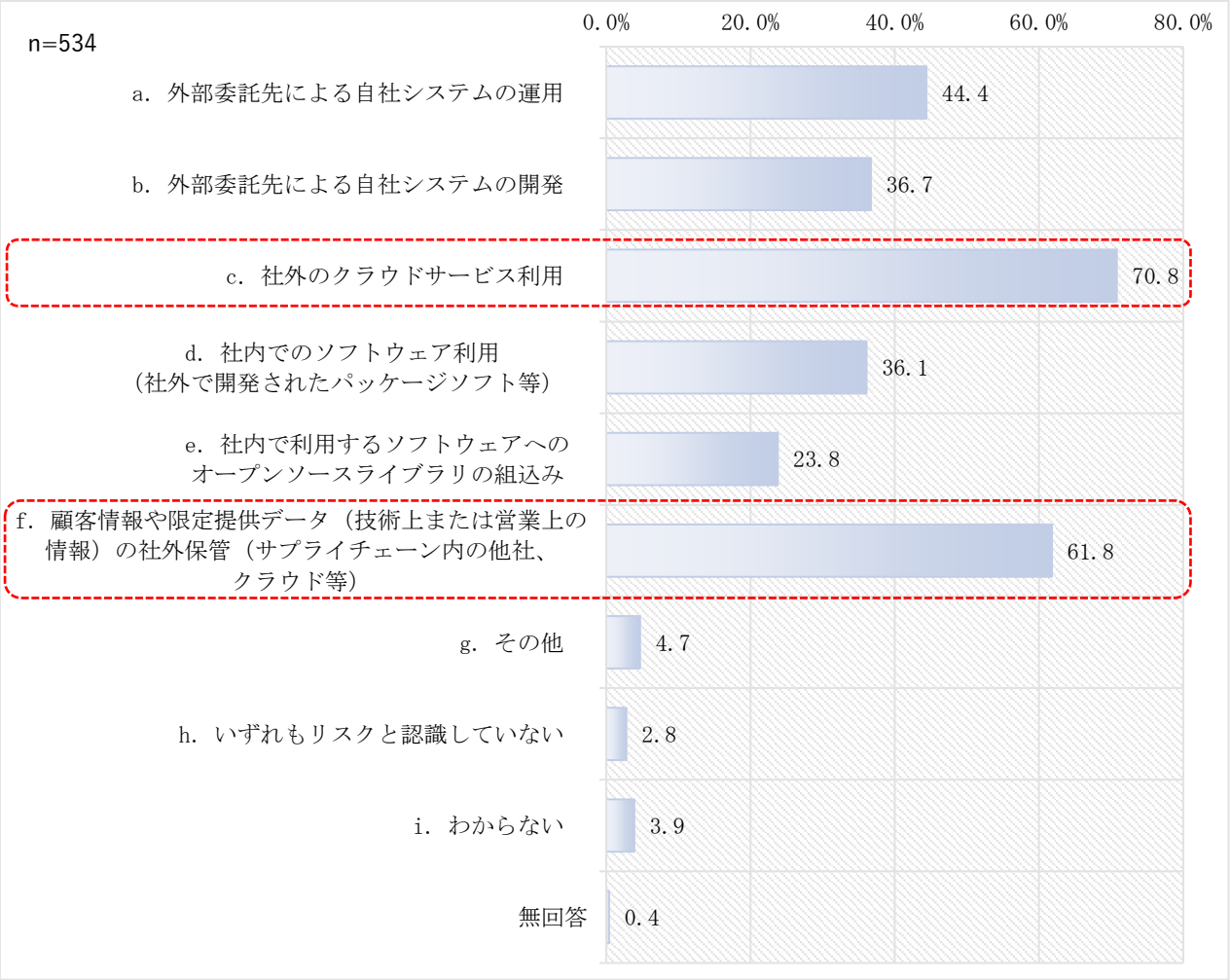

図 3-11　サプライチェーンセキュリティのリスク認識

また、「IT 依存度」[9]の分析軸で比較すると、IT 依存度が高い企業ほど、サプライチェーンのリスク認識が高い傾向がみられる。

[9] IT 依存度のカテゴリーの詳細な定義は、表 3-2 参照。「カテゴリー1 が最も IT 依存度が高く、カテゴリー4 が最も低い」と定義している。

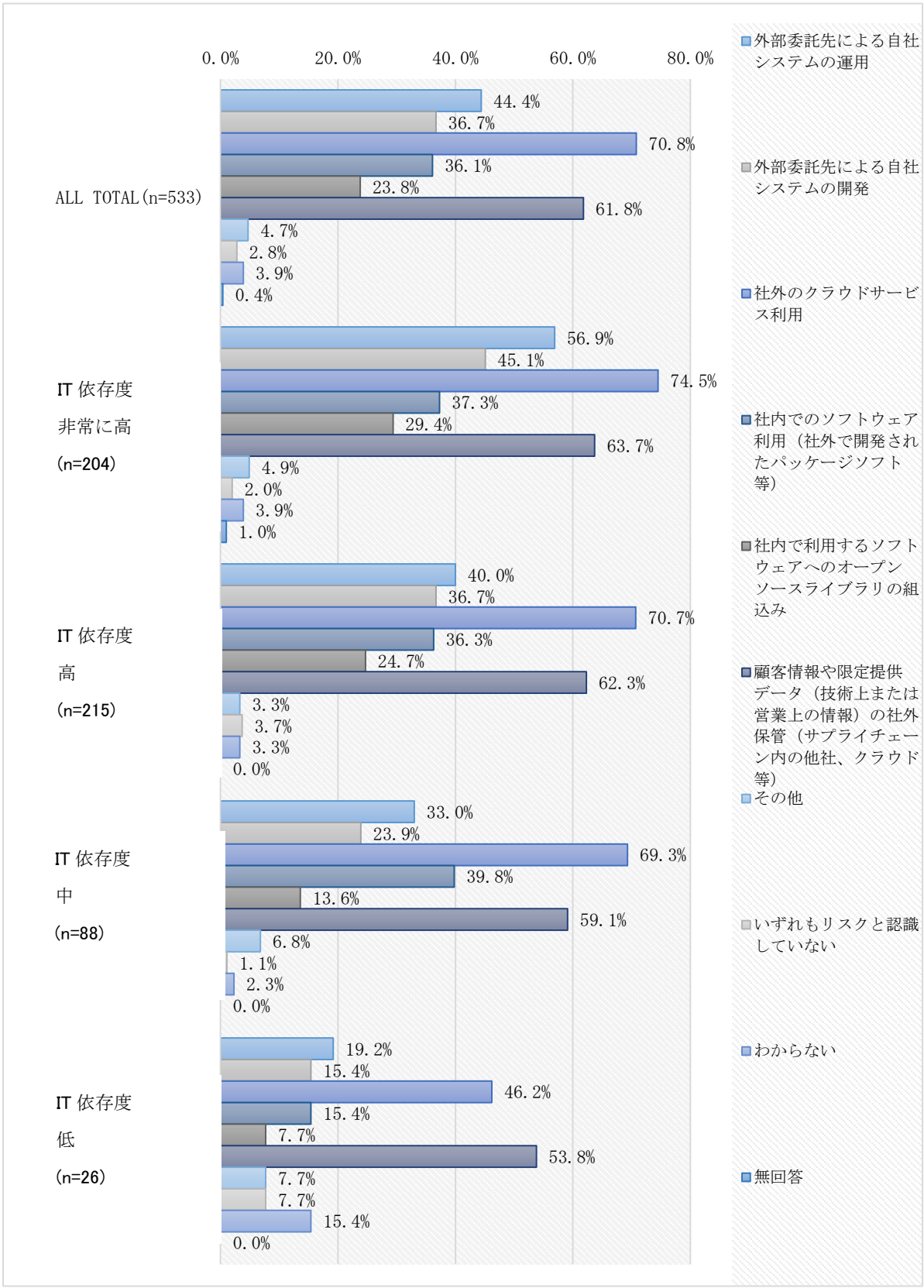

図 3-12　サプライチェーンセキュリティのリスク認識（IT 依存度）

⑧　サプライチェーンセキュリティへの対策（アンケート調査 Q26）

サプライチェーンセキュリティへの対策として、実施されている対策は「契約条項へのセキュリティ要求事項の追加（60.5%）」が主であり、「チェックシートによる委託先管理（35.4%）」や「技術的な対策（39.7%）」を実施している企業は相対的に少ない。また、「委託先からの納品時にセキュリティチェックを実施している」と回答した企業は 15.4%に留まっている。

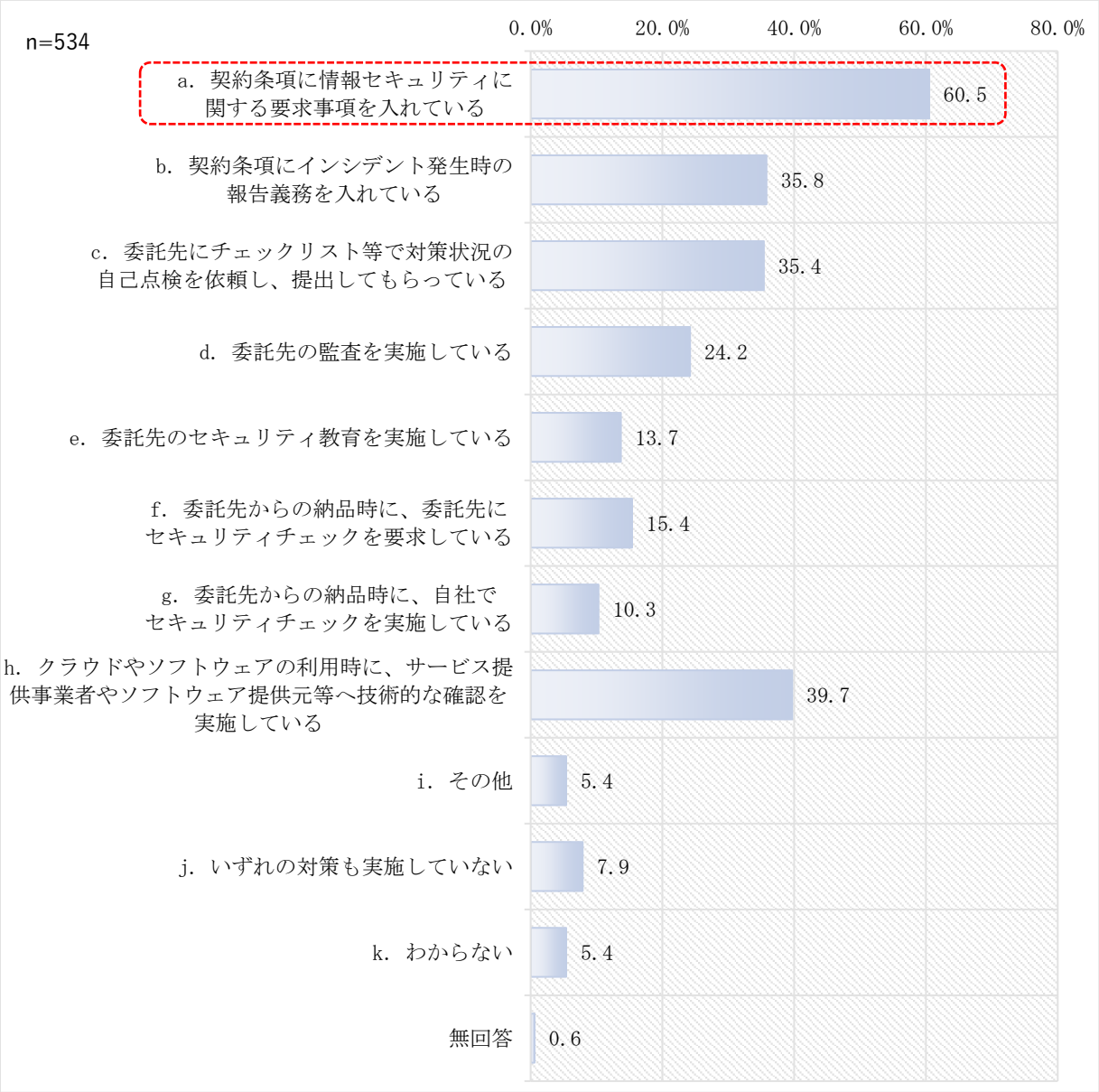

図 3-13 サプライチェーンセキュリティへの対策

⑨CSIRT の人員配置状況（アンケート調査 Q31）

CISO 等をサポートする CSIRT に、1 名以上の専任のメンバーを配置している企業は約 30%程度であり、専任のメンバーを配置していない企業は 68.9%である。一方で、1 名以上の兼任のメンバーを配置している企業は、約 70%程度である。インシデント発生時になると、内部と外部（外部委託先等）より兼任のメンバーを配置する企業が多い。

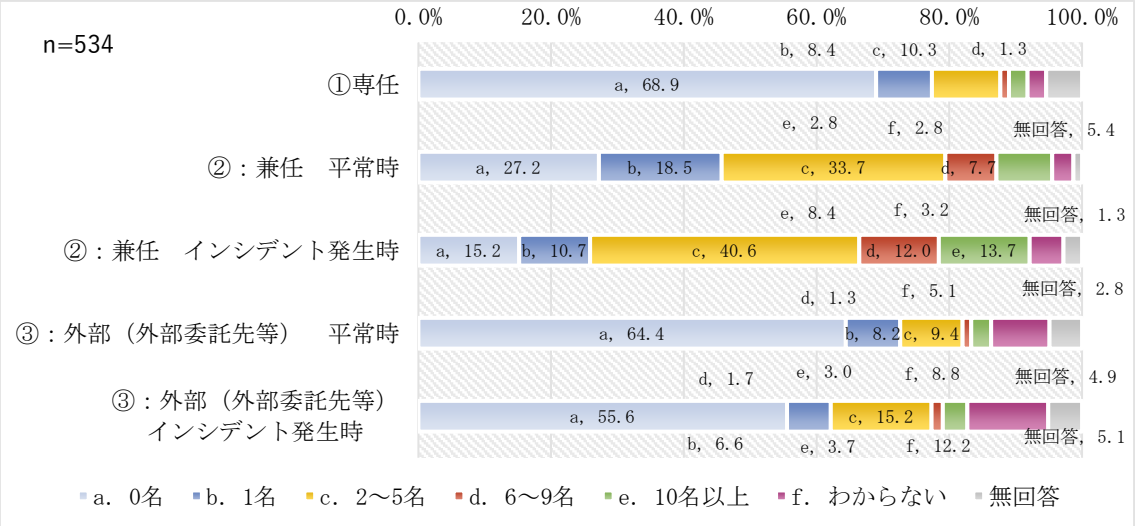

図 3-14　CSIRT の人員配置状況

⑩　CSIRT の設置目的（アンケート調査 Q32）

CSIRT の設置目的として、「インシデント発生時の被害の拡大防止」を回答した企業が、71.3%と最大であった。次いで、「インシデント発生及び被害の予防」を回答した企業は 60.9%であった。一方で、「インシデント対応計画の策定」や「インシデントの経験・知見に基づく改善策の実施」を回答した企業は 50%に満たなかった。

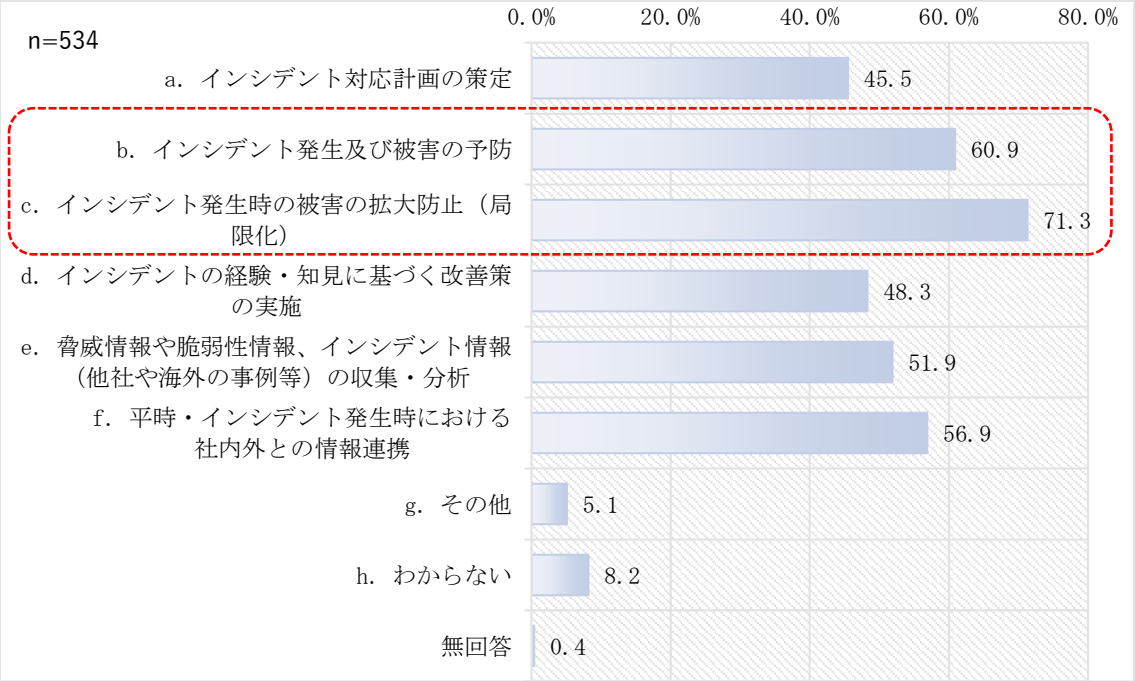

図 3-15　CSIRT の設置目的

3.3.2.2. CISO 等の動向

① CISO 等の設置状況（アンケート調査 Q2）

CISO 等の設置状況を専任・兼任別で比較すると、「専任」は 7.5%、「兼任」は 92.5%であった。

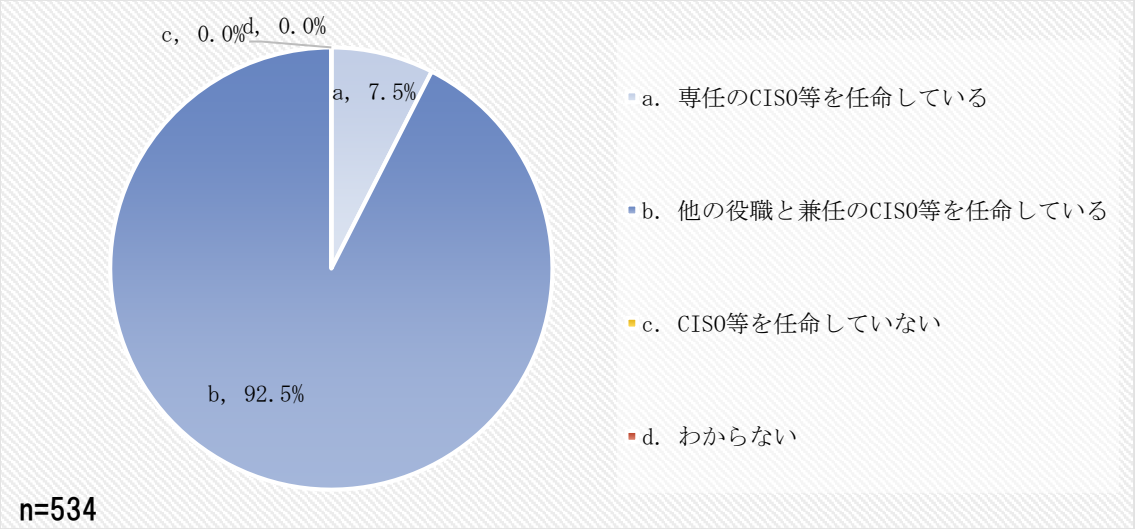

図 3-16 CISO 等の設置状況

②経営層が CISO 等に求める役割（アンケート調査 Q14）

経営層は、CISO 等に対して、「技術的役割」よりも「経営・事業的役割」を求めている。

経営層が CISO 等に対して「経営・事業的役割」を求める割合は 73%である（「b.経営・事業的役割（34.8%）」と「c.技術的役割と経営・事業的役割の両方（38.2%）の回答の合計」）。その一方で、CISO 等に「技術的役割」のみを求める割合は、6.7%にとどまる。

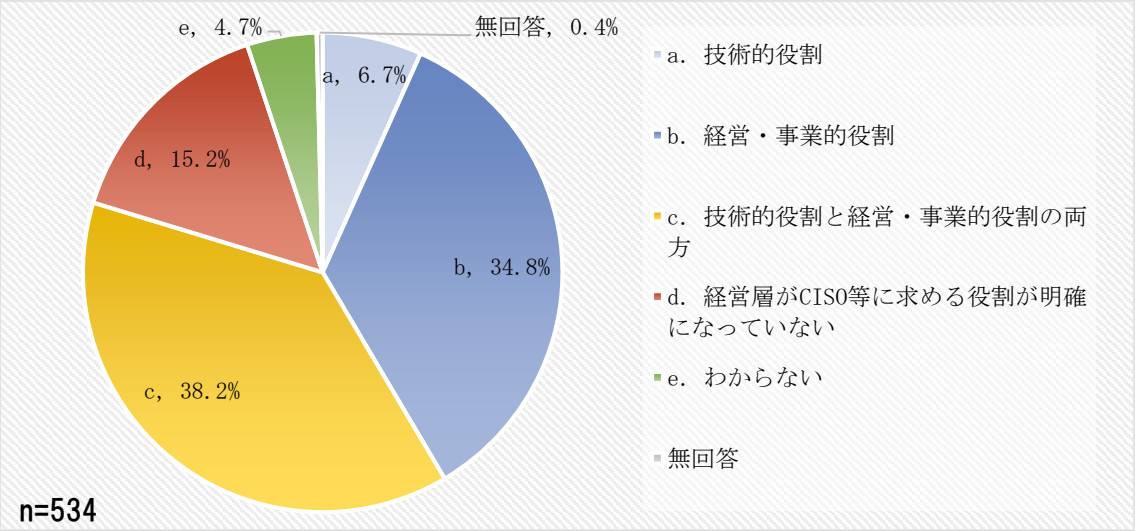

図 3-17　経営層が CISO 等に求める役割

また、「IT 依存度」[10]の分析軸で比較すると、IT 依存度が高い企業ほど、CISO 等に経営・事業的役割を求める傾向がみられる。カテゴリー1 の IT 依存度が高い企業は、経営・事業的役割を重視すると回答した割合は約 8 割、その他の IT 依存度が高くない企業（カテゴリー2～4）は、約 7 割以下にとどまっている。

[10] IT 依存度のカテゴリーの詳細な定義は、表 3-2 参照。「カテゴリー1 が最も IT 依存度が高く、カテゴリー4 が最も低い」と定義している。

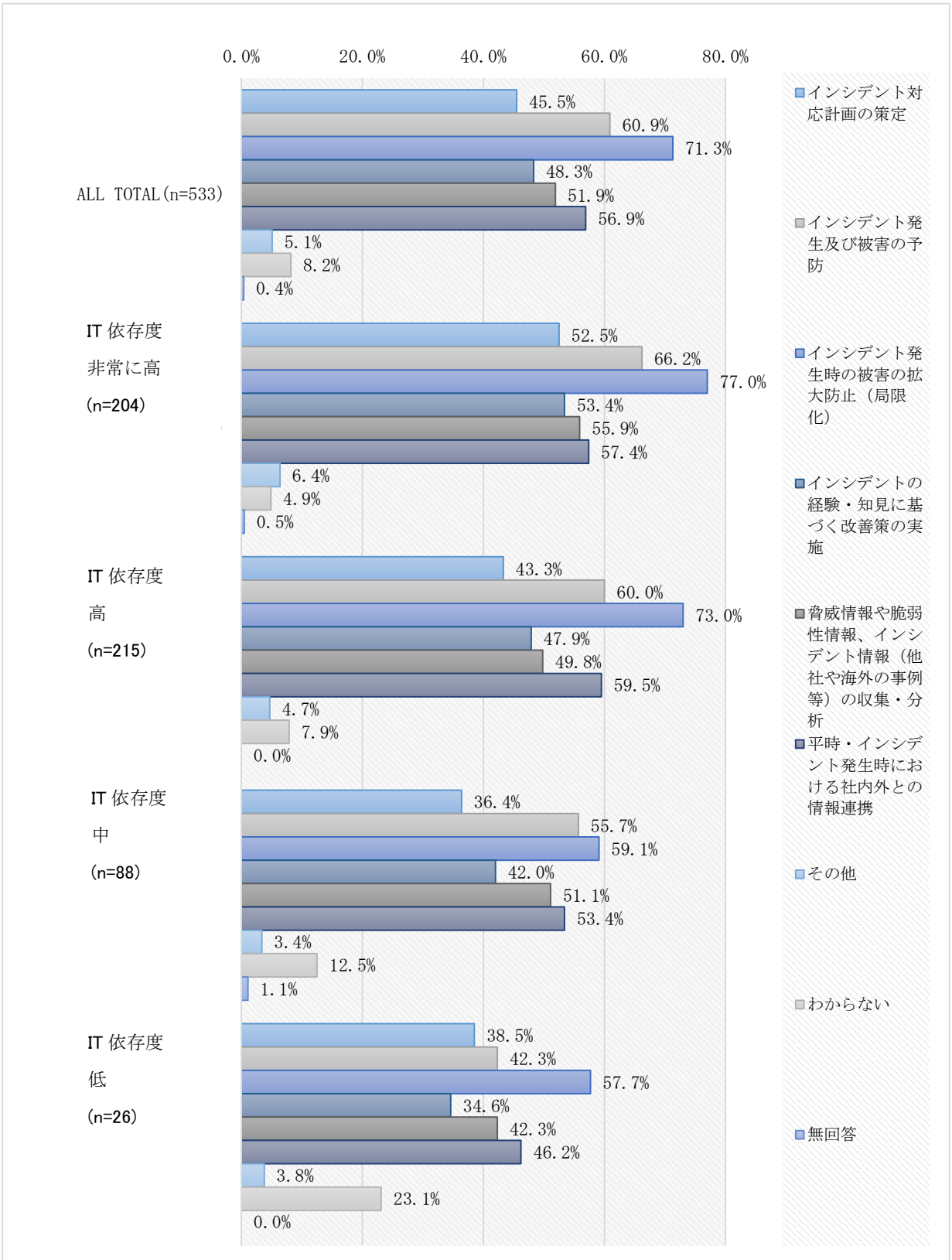

図 3-18　経営層が CISO 等に求める役割（IT 依存度）

③CISO 等の以前の所属（アンケート調査 Q17）

CISO 等が CISO 等に任命される以前の所属としては、IT システム関連部門は 23.8%、IT システム関連部門以外の非事業部門は 39.7%、事業部門（製品・サービス提供部門）は 18.2%であった。IT システム関連部門出身の CISO 等が少数派であることが確認できた。

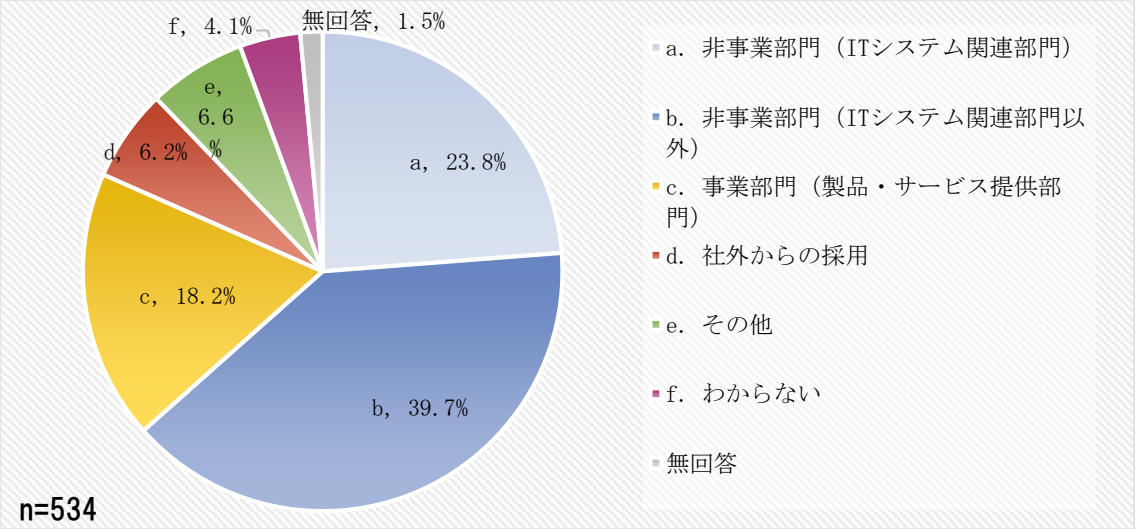

図 3-19　CISO 等の以前の所属

④CISO 等に重要なスキル・経験（アンケート調査 Q18）

CISO 等の役職を担う人材に、重要なスキルや経験として、「セキュリティ管理に関する知識（55.1%）」や「コミュニケーションスキル（52.4%）」が特に重視されている。一方で、「インシデント対応経験（10.1%）」や「実務経験（9.4%）」、「プレゼンテーションスキル（8.6%）」を求める企業は少ない。

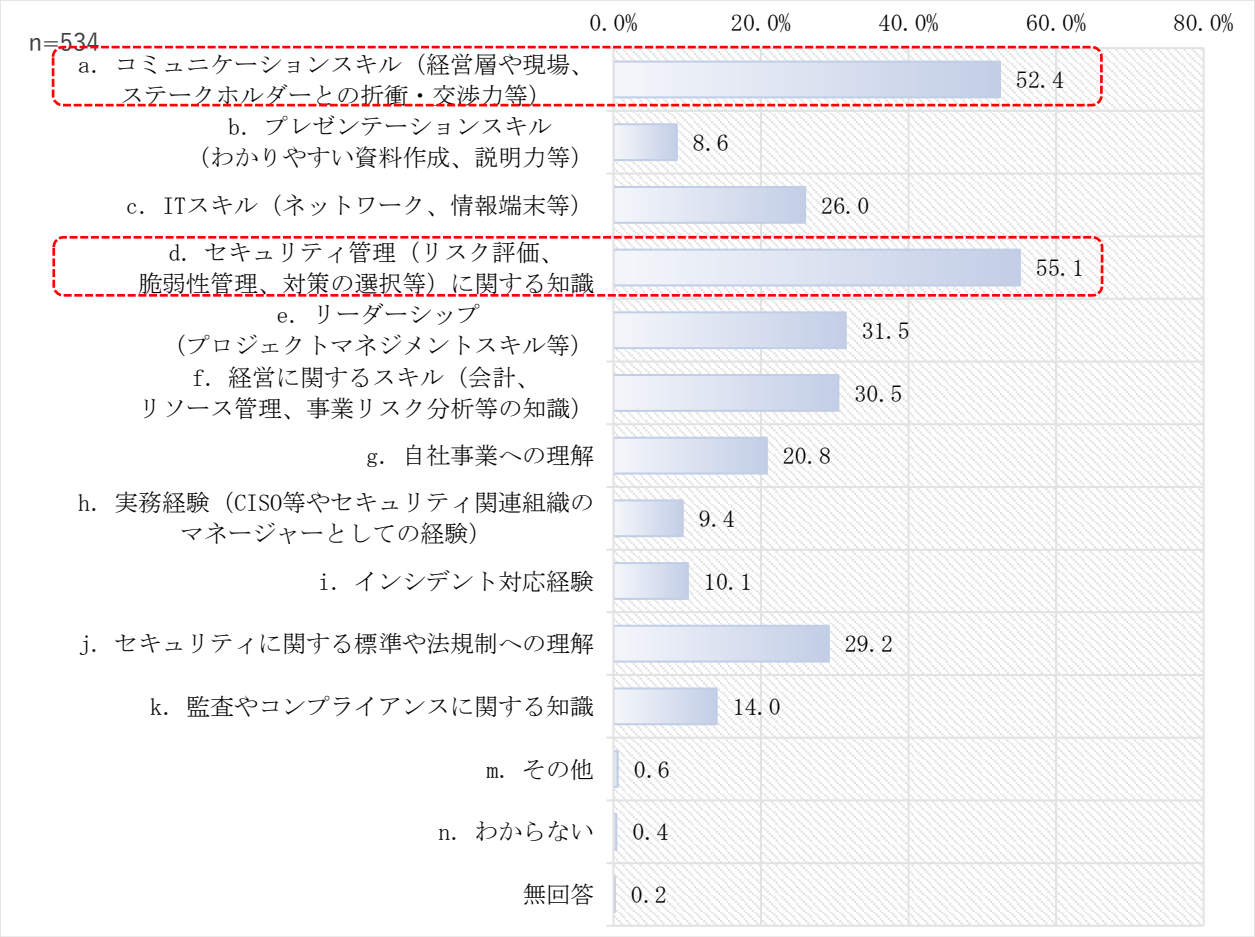

図 3-20　CISO 等に重要なスキル・経験

⑤重視している CISO の役割（アンケート調査 Q19・Q20）

CISO 等に求められる役割の「技術的役割」、「経営・事業的役割」から、更に CISO 等に求める具体的な役割を確認した。現在は、「経営層との橋渡し（45.5%）」や「セキュリティ対策の推進（45.3%）」が特に重視されている役割である。一方で、「セキュリティ技術分析・評価（9.2%）」や「CSIRT・SOC の管理監督（6.0%）」、「IT 導入におけるセキュリティ上の助言（7.7%）」、「外部組織との連絡・調整・発信（7.7%）」、「セキュリティ人材の育成・確保（11.4%）」の選択率が 10%前後にとどまっている。

また、今後重視される役割として、現在も重視されている「経営層との橋渡し（37.3%）」や「セキュリティ対策の推進（36.1%）」に加え、「セキュリティ目標・計画・予算の策定・計画（36.7%）」や「セキュリティ人材の育成・確保（31.8%）」と回答する割合が 30%を超えた。特に、「セキュリティ人材の育成・確保」は、現在重視されている割合（11.4%）と大きなギャップが見られ、今後、より重要視されていることが確認できた。

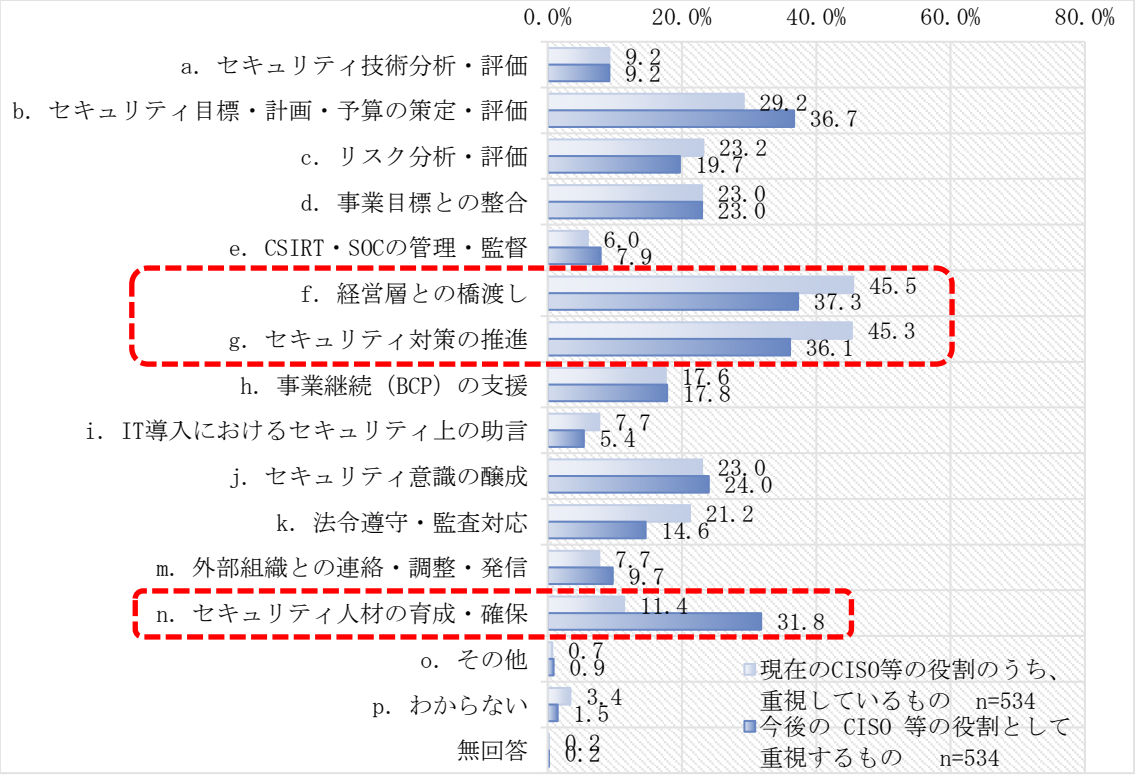

図 3-21　重視している CISO 等の役割

⑥CISO 等のサポートメンバーを配置する理由（アンケート調査 Q29）

CISO 等をサポートするメンバーを配置する理由として、「CISO 等がセキュリティの専門家ではなく、専門知識を持ったメンバーがサポートする必要があるため」と回答した企業が 60.8%と最も多かった。次いで、「CISO 等の業務所掌握範囲が広く、一人で対応するのが困難である」と回答した企業が 54.2%であった。一方で、「CISO 等がセキュリティの専門家であり、事業に関する知識等それ以外の専門知識を持ったメンバーがサポートする必要があるため」や「各部門が有する知見の共有と人材の育成ができるよう、各部門のメンバーを含めているため」と回答した企業はそれぞれ約 5%程度であった。

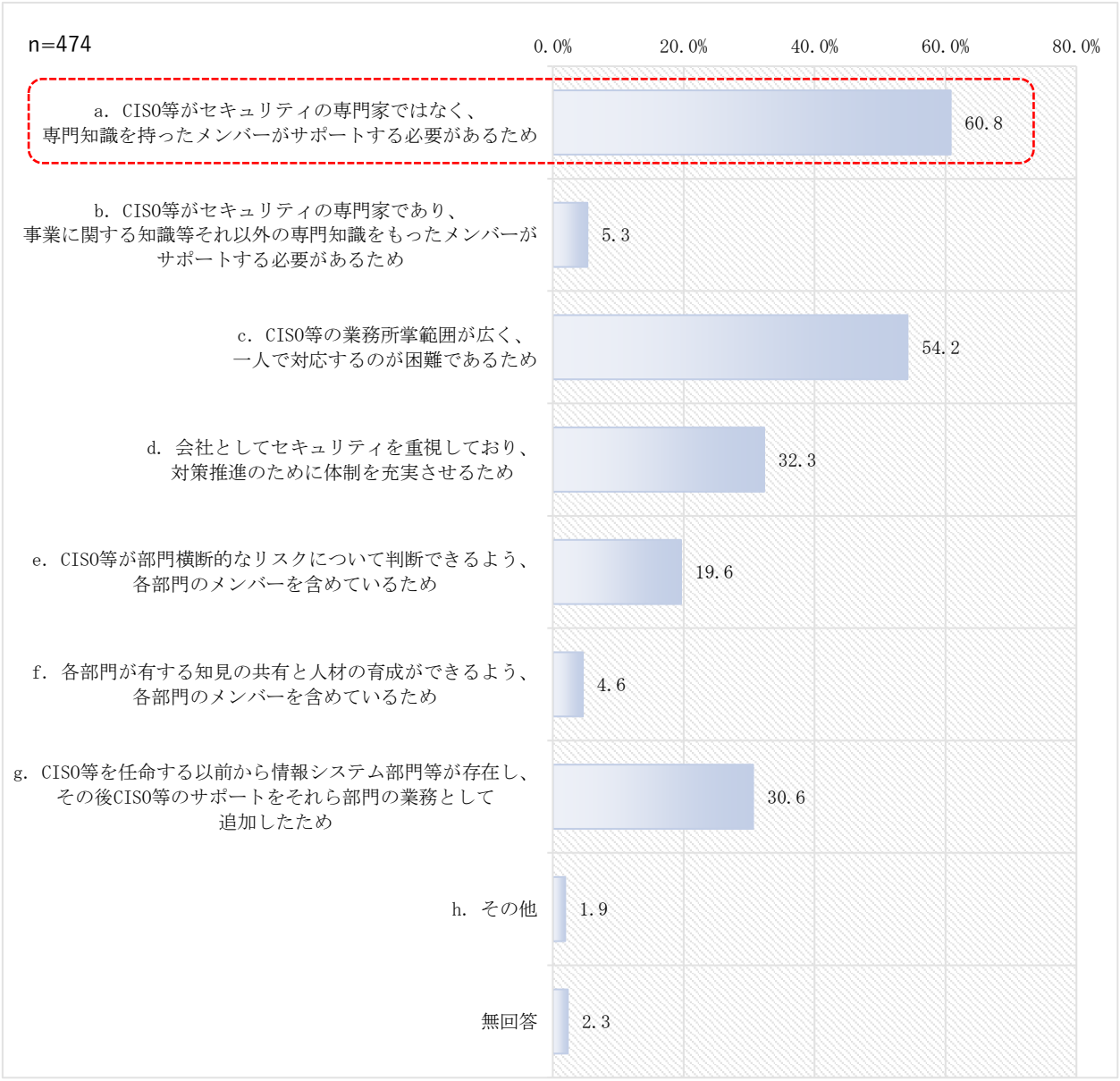

図 3-22　CISO 等のサポートメンバーを配置する理由

4. インタビュー調査

4.1. 調査概要

サイバーセキュリティ経営の豊富な知見を有する国内の有識者から、サイバーセキュリティ経営に関する国内企業の先進的な取組みや、その取組みの成功要因等についてインタビューを実施した。有識者インタビュー調査の概要を以下に記載する。

表 4-1　有識者インタビュー調査の概要

調査対象	● 国内有識者　3 名 ➢ グローバル IT 企業の CISO　1 名 ➢ セキュリティ関連の業界団体幹部　1 名 ➢ 複数企業における CISO 補佐官の経験者 1 名
調査期間	2019 年 8 月 27 日～8 月 30 日
主な質問事項	① サイバーセキュリティリスクの把握と組織全体での対応 ● サイバーセキュリティリスクの分析・評価手法 ● サイバーセキュリティへの対応方法 等
	② サイバーセキュリティ対策における PDCA サイクルの実施 ● サイバーセキュリティ管理の内部レビューや監査の定期的な実施 ● サイバーセキュリティ演習/訓練の定期的な実施　等
	③ 情報の収集・共有を通じたサイバーセキュリティの確保 ● 脅威情報・脆弱性情報等の入手先 ● 分析結果の内部共有、改善等に向けた活用方法及び体制の構築　等
	④ サイバーセキュリティ管理体制の構築 ● サイバーセキュリティ目標・計画・予算策定への助言 ● サイバーセキュリティ人材の育成・採用に関する提言・改善策　等
	⑤ サプライチェーンのサイバーセキュリティの確保 ● グループ企業や外部委託先のセキュリティ管理・対策を確認・改善する手法 ● サプライチェーンを通じた新たなサイバー攻撃手法の調査・対策　等

4.2.有識者インタビュー調査結果の考察

4.2.1.セキュリティリスク把握のための完璧を目指さないスモールスタートの取組み

サイバー攻撃の高度化に伴い、情報の窃取のみならず、システムの変更や停止等の正常な運用を妨害する攻撃が登場してきている。そのようなサイバー攻撃に対応するためには、既存の事業で保有している情報やシステムを把握し、経営戦略の観点から守るべき情報やシステムを特定することが重要である。そして、サイバー攻撃の脅威や影響度からサイバーセキュリティリスクを把握し、必要なリスク低減措置を講じなければならない。

しかし、「セキュリティリスクを経営戦略や事業から切り離して考えても効果が薄い」という見解があった一方で、3 章アンケート調査の結果も踏まえると、現時点ではまだ、セキュリティリスクと経営戦略・事業を紐づけて考えることができる企業は多くはないと考えられる。セキュリティリスクを把握する前に、CISO 等はまず、自社の経営戦略及び事業を十分に理解し、リスクの本質を理解することが重要である。自社の事業とサイバーセキュリティリスクを紐づけるためには、情報資産管理台帳や専用のソフトウェア等を活用することが有効である。しかし、初めからすべての情報資産やリスクを洗い出すことは、人的リソースの不足等の課題から、多くの企業にとって対応が容易ではない。また、サイバー攻撃の手法は日々進化しており、機動的な対応も求められる。そこで、まずは定性的なリスク評価等で、守るべき重要な情報資産を社内で共通理解することから始めるなど、初めから網羅性を目指さず、重要度の高い領域からスモールスタートで取組みを始めることが肝要である。

4.2.2.PDCA サイクル実践のための演習/訓練の重要性の高まり

新たな脅威の発生等サイバー攻撃のトレンドの変化や、セキュリティ製品等のセキュリティ対策の進化に対応し続けるためには、サイバーセキュリティ対策に係る PDCA サイクルを構築することが重要である。計画したサイバーセキュリティ対策の有効性を確認し、サイバーセキュリティ対策を従業員に理解・定着させ、改善に繋げるためには、演習や訓練の実施が効果的である。

演習や訓練の実施に関して、「独自のシナリオを検討し、演習を実施することが重要である」という意見があった。独自のシナリオによる演習の効果として、参加者の関心・主体性を高めることが期待される。外部のベンダ等から得たシナリオをそのまま利用するのではなく、ベンダの協力等も得ながら自社の業務に即した内容を加味することで、参加者の当事者意識の向上が期待される。また、こうした方法は、複数の部門や社外関係者を巻き込むシナリオなど、柔軟にシナリオを構築できることもメリットの 1 つである。社内外の関係者を巻き込んだシナリオの検討を通じて、外部のベンダの活用方法や社内の他部門のスタッフの顔や関心を把握できることは意義深いと考えられる。

また、必ずしも緻密なシナリオを準備して実施する必要はなく、実際に他社で発生したインシデント等が自社に起きた場合を想定し、インシデントへの対応方法を机上で検討することも、課題の発見等につながるため、有効的である。

4.2.3.情報共有活動および情報収集の為の外部コミュニティとの関係構築

脆弱性情報や他社で発生したインシデント情報等を収集し、それらの情報の活用によってインシデントを防止するために、外部のサイバーセキュリティに関する情報共有活動へ参加することが重要である。既に金融 ISAC や交通 ISAC 等、業種によっては、参加企業が双方でサイバーセキュリティに関する情報を共有する枠組みが存在している。しかし、「情報共有は自社と同業種だけに絞る必要はない」という見解があったように、セキュリティベンダのユーザー会等、同業者以外のコミュニティで情報共有を実施することも有用であると考えられる。様々な業種の企業が参加するコミュニティでは、業界固有のインシデント等だけではなく、広く一般的な課題や、利用するソフトウェア等の共通的な課題に関する情報の共有も可能である。また、普段の活動では出会うことができないセキュリティの専門家と関係を構築する機会も想定される。

そして、現場の担当者間の草の根のコミュニティを構築し、気軽に相談できる相手が外部にもいるという状態をつくることも重要である。脆弱性の情報を得た際など、自社では活用できない場合でも、外部の相談相手に相談したところ、活用方法を教えてもらえるというようなケースも想定される。

4.2.4.CISO 等に求められる役割（経営層との関係構築、予算の確保）

CISO 等に求められる重要な役割として、「経営層に対して情報共有ができる関係を構築すること」、「予算を確保すること」との見解があった。まず、日頃より経営層との関係性が構築されていなければ、会議にて課題を提案したところで、経営層に納得・理解してもらうことは難しいことが想定される。その場合、当然、セキュリティ予算を確保することも困難であり、その結果として、セキュリティ人材の確保やソリューションの導入ができず、検討したリスク対応の提案は画餅に帰してしまう。経営層に提案を納得・理解してもらうためには、セキュリティの観点だけではなく、経営・事業的な観点の要素を盛り込むことも必要である。しかし、一概に経営・事業的な観点といっても、経営層の関心が高い分野と低い分野があることが想定される。そのため、経営層に求める観点を盛り込むためには、CISO 等は日頃より経営層と接点を持ち、経営層のことを理解することが重要である。一部の企業では、役員ではない CISO 等でも、役員会議に参加できるように働きかけるなど、プロアクティブに経営層とコミュニケーションを図る事例も確認することができた。

4.3. 調査結果

4.3.1. サイバーセキュリティリスクの把握と組織全体での対応

まず、企業として、サイバーセキュリティリスクを経営上の重要なリスクとして認識することが重要である。そして、自社の守るべき情報を特定（サイバーセキュリティリスクを把握）したうえで、組織全体として対応方針を策定することが重要である。さもなければ、受容できないリスクが残存している場合、想定外の損失を被る可能性がある。そこで、有識者に対して、サイバーセキュリティリスクの分析・評価手法やサイバーセキュリティへの対応等についてインタビュー調査を実施した。

まず、セキュリティリスクの把握について、「セキュリティリスクを事業等と切り離して、単独で検討してもあまり意味がない」、「セキュリティリスクの無理な数値化はお勧めしない」との見解が得られた。

そして、サイバーセキュリティへの対応について、「リスクの洗い出し以前に、セキュリティアーキテクチャの整備」、「ベンダ等のサイバーセキュリティパートナーとの協力関係の構築」等の取組みが重要であるという見解が得られた。さらに、サイバーセキュリティ対応における CISO 等へ期待される役割として、「経営層への課題提案にとどまらない、セキュリティ対策の執行」や「サイバーリスクだけではない全般的なリスクマネジメントの習得」が求められるとの見解も得られた。

有識者の主な見解を以下に記載する。

（セキュリティリスクの把握について）

- セキュリティリスクを単独で考えても効果は薄い。理由としては、ジェネラルコントロールで対応できる範囲はとても小さいためである。サイバーセキュリティリスクを単独で考えてしまうと、例えば「ID コントロールと物理コントロールが連動していない」や「どのような事業を行っているか理解していないとリスクの本質が理解できない」等々様々な問題が発生する。
- セキュリティリスクの無理な数値化はお勧めしない。セキュリティリスクを数値化せずとも、感性をもって判断することが経営層の使命である。
- 経営層はサイバーセキュリティを一括りに考えている傾向があるため、情報漏洩だけではなく改ざん等の情報リスクやシステムリスクを含めた、リスクの一覧を提示して、教育することが重要である。

（サイバーセキュリティへの対応について）

- 基準を守るだけの取組では意義が薄い。チェックリストを満たすことが目的ではない。全部のリスクを洗い出す前にまず始めてみることが大事である。そのためにはアーキテクチャの整備が必要である。重要なリスクの少なくとも 70%を特定できたのであれば、まずはそれを守る対応を講じる。こうした考え方のベースとなるアーキテクチャが存在しない中で、セキュリティを考えても俊敏な対応は不可能である。

- 情報資産の洗い出しや整理等を行う前に、ベンダ等の信頼できるサイバーセキュリティパートナーの協力を仰ぐことが重要である。
- 大手のセキュリティベンダとの取引が難しい中小企業等は、仮に予算が少ない場合でも、企業の成長に応じて継続的に予算を確保していくという姿勢を見せていくことで、協力を仰げる可能性がある。
- リスクの把握の前に、リスクベースマネジメントの考え方を理解することが重要である。

（サイバーセキュリティへの対応における CISO 等の役割）

- CISO 等には、セキュリティの執行責任者としてリスク対応の枠組みを整備し、リソースの手当てを行うことが求められる。そのため、経営層に課題を提案して終わりではなく、「執行」まで実施することが求められる。
- リスクの定量化は困難である。リスク分析の専門家はリスクの定量化の手法を開発したというが、実態には即していない。そのため、CISO 等は、サイバーリスクに限定しない全般的なリスクマネジメントを学ぶことも大事である。

4.3.2. サイバーセキュリティ対策における PDCA サイクルの実践

サイバーセキュリティ対策を確実に実施し、また改善していくために、既存の PDCA サイクルの中でも特に Check に課題があると考えられる。有識者からは、PDCA サイクルを強化するために、PDCA サイクルの”C(Check)”について、業務に即したサイバーセキュリティ演習/訓練を組む込むことが必要であるとの見解が得られた。

またその他、「内部監査の徹底」、「アカウンタビリティの観点で、対応計画や体制を評価すること」や「仮想的に、実際に世間で起きたインシデントが自社で発生した場合の対応方針を検討すること」が重要であるという見解が得られた。

さらに、PDCA サイクルは一般的に”P(Plan)”・”D(Do)”・”C(Check)”・”A(Act)”の 4 ステップで検討されるが、「会社の状況等に応じて、4 ステップにこだわらず、さらに細分化してもよい」などの見解もあった。

有識者の主な見解を以下に記載する。

（Check について）

- 業務負荷は大きいが、内部監査を徹底することは効果がある。内部監査の結果を援用することによって、「対現場」「対経営層」両方に対して、施策を推進しやすくなるメリットがある。
- CISO 等が全てのシステムについて精通するのは不可能であるため、「インシデントが発生して顧客影響等が生じた際に、外部に説明するための材料がそろっているかどうか」という観点で、対応計画や体制を評価することは有効である。例えば、メールの誤送信の際に、「いつ」「どこで」「だれが」「どうして」そのような行動をとったのか、またその行動は「ポリシーとの関係においてどうか」、「再発防止策は定められているか」等の観点で内容が整理されている必要がある。
- 技術的対応、組織的対応それぞれの視点から一つひとつ論点を洗い出し、独自の演習シナリオを作ることが有用である。必ずしも「出来の良い」シナリオでなくてもよい。
- 抽象的な内容ではなく、業務に即した具体事例をベースに演習や訓練を行うと、参加者の関心が高まる。社内のメンバーが「うすうす気になっていること」に関するシナリオがよい。セキュリティ部門が単独で実施しても効果は低い。
- 世間を騒がせたインシデントが自社で生じた場合にどう対応するかを考えることが有効。「判断する人がわからない」「連絡手段が定まっていない」「（システム停止等を判断した場合の）判断した者の免責が定められていない」等の課題点が明らかになる。考えているだけの組織と、小規模でも実践している組織では対応力が全く違ってくる。

（PDCA サイクルの在り方）

- PDCA サイクルを 4 ステップではなく、会社の状況等に応じて、ステップを 10 個に分けてもよい。会社によっては、自社で重要情報を選んで、脆弱性を調べるよりも、有力なセキュリティパートナーを先に見つけることが PDCA サイクルの実践の第一ステップに場合もある。
- セキュリティベンダを複数利用し、双方を切磋琢磨させる企業も存在する。

4.3.3. 情報の収集・共有を通じたサイバーセキュリティの確保

最新のサイバーセキュリティを確保するためには、内部での調査だけではなく、積極的に外部からサイバー攻撃等に関する情報を収集し、その情報を内部で有効活用することが重要である。有識者に対して、脅威情報・脆弱性情報等の入手先や分析結果の内部共有、改善等に向けた活用方法及び体制の構築方法等についてインタビュー調査を実施した。

まず、脅威情報の収集・分析のための体制について、「情報を収集・共有できる枠組みや CSIRT 等の体制を構築すること」や「情報提供元のセキュリティベンダを使いこなせる人材の確保」が重要であるという見解が得られた。

また、情報収集のために、「業種に囚われない企業間の情報交換」や「現場の担当者の草の根のコミュニティの構築」が重要であるとの見解があった。

有識者の主な見解を以下に記載する。

（脅威情報・脆弱性情報の収集・分析のための体制）

- CISO 等は、脅威情報の収集・共有を実施できる枠組みや体制(CSIRT 等)を構築することに注力すべきであり、必ずしも CISO 等自身で対応する必要はない。CISO 等自身は、日頃より脅威情報へ感度を高め、状況に応じて CSIRT 等に状況を確認するという運用が良いだろう。
- セキュリティパートナーから情報を取得できる状況だとしても、そのようなセキュリティパートナーを使いこなせる人材を社内に確保することが重要である。

（情報収集のための企業間や草の根のコミュニティの重要性）

- 情報交換や相談を行う相手は、自社と同業種だけに絞る必要はない。例えば、ベンダのユーザー会は、課題認識を共有していることが多いため、様々な業種の企業が、情報交換のために参加している。
- 現場の担当者の草の根のコミュニティを作ることも重要である。担当者が一堂に集まる会議等を通じて、他のパフォーマンスユニットとの間でお互いに名前と顔が一致している状態を作るのが良いだろう。

4.3.4. サイバーセキュリティ管理体制の構築

組織としてサイバーセキュリティリスクの把握をし、サイバーセキュリティ以外のリスク管理体制との整合をとるためにも、サイバーセキュリティ対策を実施する目的の下、サイバーセキュリティリスクの管理体制を構築することは重要である。有識者に対して、サイバーセキュリティ目標・計画・予算策定への助言やサイバーセキュリティ人材の育成・採用に関する提言・改善策等についてインタビュー調査を実施した。

サイバーセキュリティ管理体制構築における CISO 等の役割として、「事業目標実現のための IT とセキュリティのアーキテクチャの整備」や「事業部門と協力して、IT の導入と運用を進めること」、「人材確保やシステム導入のための予算を確保すること」、「経営層とコミュニケーションできる関係を構築すること」が重要であるという見解が得られた。また、セキュリティ人材については、「セキュリティ人材が正当に評価されないこと」が問題であるとの指摘もあった。

有識者の主な見解を以下に記載する。

（管理体制構築における CISO 等の役割）

- CISO は、①事業目標実現のために IT とセキュリティに関するアーキテクチャを用意する、②アーキテクチャと整合するように事業部門と調整して IT の導入・運用をスムーズに進める必要がある。なお、CISO は必ずしもボードメンバーではないが、自身が経営会議のメンバーではない場合は、自身よりも一段上位の者を通じて①・②を経営会議に諮りながら、これらの業務執行に責任を持つ必要がある。
- CISO の最大の役割は、予算を確保することである。予算を確保できれば、人材の確保やシステムの導入等が可能である。
- CISO は、経営層と個人的に親しい間柄である必要はないが、直接報告し情報を共有できる関係を構築する必要がある。

（セキュリティ人材の確保について）

- サイバーセキュリティ人材の補強方法として ①時間はかかるが既存の人材を育成する、②外部から引き抜く、③予算を確保してコンサルティング企業を雇う、④CISO や CIO のシェアリングの 4 種類がある。
- セキュリティ人材が、正当に評価されないことは問題である。

（サイバーセキュリティ責任者の各組織への設置について）

- 共通言語で意思の疎通を行うことを可能にする為に、必ずしも専任者である必要はないが、パフォーマンスユニットごとにサイバーセキュリティ責任者を置くことが重要である。

4.3.5. サプライチェーン全体のサイバーセキュリティの確保

サプライチェーンのビジネスパートナー等を踏み台にした、自社へのサイバー攻撃の被害を防止し、委託先への委託業務などにおいて、自社と委託先でサイバーセキュリティ対策の漏れを防止する等の為にも、対策状況の把握等のサプライチェーン全体のサイバーセキュリティ対策は重要である。有識者に対して、グループ企業や外部委託先のセキュリティ管理・対策を確認・改善する手法やサプライチェーンを通じた新しいサイバー攻撃手法の調査対策等についてインタビュー調査を実施した。

まず、サプライチェーンのサイバーセキュリティを確保するために、「他社とルールや優先順位等の枠組みの策定」や「情報交換をできる関係を構築すること」が重要であるとの意見があった。そして、グローバルな会社においては、グローバルガバナンスを効果的なものにするために、「国によって文化が異なる点に留意すること」が重要であるとの見解が得られた。また、近年のクラウドの普及に伴い、「クラウドセキュリティが必須」との見解もあった。

有識者の主な見解を以下に記載する。

（サプライチェーンのサイバーセキュリティを確保するための他社との関係性）

- サプライチェーンのサイバーセキュリティについて、完璧に対応しようとするとキリがない。そのため、どういうタイミングでどこまでやるか、優先順位をどうするか等、「共通の枠組み」を決めておくことが最も重要である。
- サプライチェーンを構成する他社とお互いに情報を交換することは重要である。

（グローバルガバナンスにおける留意点）

- レピュテーションリスクについては、「あの事業者と仕事をするとデータが漏れる」と外部に思われてしまった時点で、自社の信用は完全に失墜する。システム的・技術的な対策は必須であるが、グローバル企業では国・地域によって文化が異なる点に留意する必要がある。例えばセキュリティポリシーを徹底しようにも、そもそもポリシーに注意を払わない文化もある。

（クラウドセキュリティの重要性）

- クラウドを活用する企業が増加しており、クラウドセキュリティが必須になってきている。サプライチェーンのリスクもクラウドに移行している。

5. インタビュー調査

5.1. 調査概要

「CISO 等セキュリティ推進者の経営・事業に関する役割調査」(2018 年 3 月)では、CISO 等の経営・事業に関する役割を検討する企業の参考となる、手引きや事例が必要とされている。これをうけ IPA では、CISO 等またはその実際の活動を良く知る役職員（CISO 等の指揮下の役職員、情報セキュリティ部門長、リスク管理部門長等の部門長、これらの補佐役の役職員等）に対してインタビューを実施し、得られた参考情報を 2019 年 3 月にプラクティス集として取りまとめて公表している。今回このプラクティス集の内容の拡充を図るため、改めて複数の企業に、同様の趣旨のインタビューを実地した。なお、本企業インタビュー等を基に作成したプラクティス集は別途参照されたい。

企業インタビュー調査においては、サイバーセキュリティ経営に関して豊富な経験を有する国内企業から、サイバーセキュリティ経営を実践するための主要な取組みや課題、その解決方法について、インタビュー調査を実施した。特に、サイバーセキュリティ経営ガイドラインの指示項目 4、6、10 およびセキュリティ担当者の悩みとその解決方法について、重点的にインタビューを実施した。企業インタビュー調査の概要を以下に記載する。

表 5-1　企業インタビュー調査の概要

調査対象	先進的なサイバーセキュリティ対策に取り組む国内企業　7 社
調査期間	2019 年 10 月 30 日～12 月 18 日
主な質問事項	① サイバーセキュリティリスクの把握とリスク対応に関する計画の策定 ● セキュリティリスクを特定・評価するための方法 ● 多様なステークホルダーとのポリシーの共有や具体的な監督の方法　等
	② サイバーセキュリティ対策における PDCA サイクルの実施 ● 多様なステークホルダーを巻き込んだ演習・訓練の実践内容 ● 演習・訓練や内部監査等を対経営層・現場で有効に活用するための工夫　等
	③ 情報共有活動への参加を通じた攻撃情報の入手と有効活用及び提供 ● 自社が主体となりコミュニティを形成している事例 ● 自主的なコミュニティで情報共有を実施している事例　等
	④ セキュリティ担当者の悩み ● サイバーセキュリティ対策を実践する際の具体的な悩み ● 悩みの解決方法やその成功要因　等

5.2.企業インタビュー結果の考察

5.2.1.サイバーセキュリティのリスク把握とリスク対応

経営戦略の観点から自社の守るべき情報を特定し、サイバー攻撃の脅威や影響度を評価した上で適切な対応を講じることが重要である。企業インタビューを通じて、セキュリティリスクの把握・対応のために、「リスクアセスメントの実践」が重要であるとの見解が得られた。具体的な「リスクアセスメントの実践」に関する取組として、「リスクアセスメント自体の精度を高めるのではなく、有効な対策の把握と実施に注力している」や「リスクベースアプローチを導入している」事例が見られた。本来であれば、自社の IT システムや IoT 機器、その他の情報資産をすべて洗い出し、それぞれの情報資産のセキュリティリスクと対応内容を明確化する必要がある。しかし、最初から全ての情報資産の洗い出しを実施できている企業は少ないと考えられる。そして、最初の入口（情報資産の洗い出し）がボトルネックとなり、セキュリティリスクへの対策が進まない企業も多いと想定される。そこで、網羅的な情報資産の洗い出しから取り掛かるのではなく、4.2.1 でも述べた通り、経営上のリスクの高い領域からスモールスタートで取組みを実施することが重要であると考えられる。取組みの事例として、「無償のアセスメントツールを使用する」や「リスクベースアプローチで早急にリスクが高い領域から優先的に対策を実装する」等が見られた。まずは、身近・手軽なツールを用いて、経営層や事業部門とのコミュニケーションを通じ、重要度が高い情報資産に対してリスクアセスメントを実施することから取り掛かることが効果的であると考えられる。

5.2.2.PDCA サイクルの実践

サイバーセキュリティ対策を確実に実施し、また改善していくために、PDCA サイクルの実践は重要である。企業インタビューを通じて、PDCA サイクルの実践のために、「Check を重視すること」や「柔軟に計画を見直すこと」が重要であるとの見解が得られた。まず、「Check」については、「自社で作成した独自シナリオによる演習の実施」や「演習を通じて判明した、セキュリティ意識が低い従業員(ダミーの標的型攻撃メールを開封する等)を教育している」などの事例が見られた。いずれの取組みも、演習や訓練が、従業員のサイバーセキュリティに関する意識の醸成・啓発の場となるように、工夫・有効活用をしていると考えられる。従業員に対して、意味のある演習・訓練を行うためには、演習・訓練を企画する部門の工夫が必要である。まず、自社独自のシナリオによる演習には、参加従業員の当事者意識を醸成する効果が期待できる。そして、業務の実態に即したリアルなシナリオを作成することができれば、インシデント時の予行演習としても効果的である。また、演習を通じてセキュリティ意識が低い従業員を抽出し、追加の教育を実施することによって、従業員のセキュリティ意識が高まり、最終的に、組織としてのセキュリティ対策強化が可能になる。

そして、「中期事業計画では期間が長すぎるため、年次計画とし、年に 2 回ほどセキュリティ計画の見直しを実施している」事例が見られた通り、演習・訓練を通じて発生した課題

を解決するために、年に 1 度だけの見直しではなく、必要に応じて随時、セキュリティ計画を見直すことができるような環境を CISO 等は整備することが重要であると考えられる。

5.2.3. 情報の収集・共有活動

サイバーセキュリティに関する有益な情報を取得するために、日頃の社内における机上リサーチや IT ベンダからの情報提供も効果的であるが、外部の情報共有活動への参加も効果的である。企業インタビューを通じて、サイバーセキュリティに関する情報を外部から収集するためには、「コミュニティの参加者との信頼関係を構築すること」が重要であるとの見解が得られた。また、経営層へ情報を効果的に共有するために、「平常時から情報共有をしておくこと」や「IT の専門用語ではなく、平易な表現を用いること」が重要であるとの見解もあった。

まず、情報収集について、外部のコミュニティ参加者と信頼関係を構築するためには、Give and Take の考え方が重要である。有益な情報を取得するためには、必ずしも高度な情報を提供する必要があるということではない。コミュニティの運営の支援やオフライン会議への参加など、どのような形であれ、自身が参加しているコミュニティへの貢献が必要であるということが考えられる。地道な貢献を積み重ねることによって、最終的に他の参加者から信頼を得ることができ、有益な情報の取得やセキュリティに関する相談ができるような関係の構築が可能になる。しかしながら、CISO 等やそのサポートメンバーは、人材不足の中でそもそも日々の業務に追われ、情報収集の為に外部のコミュニティへ参加・貢献をすることが容易ではないということが、現状の課題であると考えられる。

次に、経営層への情報共有について、「セキュリティに関する専門用語を、簡易な表現の使用や絵を用いるなどして“翻訳”している」や「インシデントが発生した時だけではなく、平時から情報共有をしている」事例が見られた。経営層にサイバーセキュリティに関して理解をしてもらうためには、経営層が理解しにくい専門用語を使用することは望ましくない。そのためには、経営層が理解できる表現や、理解しやすい手法（絵や図等を活用）して、“翻訳”することが効果的である。しかし、その“翻訳”をするためには、経営層の視点に立つことが重要である。その為には、CISO 等は、可能な限り経営層の思考の理解に努めることが重要である。例えば、サイバーセキュリティが事業にどのような影響を与えるか、なぜそのセキュリティ対策が重要であるか等の観点を報告等に盛り込むことが効果的であると考えられる。経営層の思考を理解するためには、平時よりコミュニケーションを図ることが必要である。

5.2.4. サイバーセキュリティ人材

サイバーセキュリティ対策を実施するためには、予算の確保もさることながら、対策を実施する人材の確保も重要である。企業インタビューを通じて、サイバーセキュリティ人材について、「人材の確保ができていない」、「インシデント対応等の日々の業務に追われ、サプ

ライチェーンのマネジメントや教育の優先順位が低い」との見解が得られた。いずれも、人材の量が不足していることが大きな原因であると考えられる。（なお、人材の質も当然重要であるが、高い能力や知識を有する人材が仮に確保できたとしても、日々の業務の遂行のためには、一定数の人材の量が必要であるため、ここでは人材の量に注目する）

人材確保の手段は、大きく「社外の人材の採用（ヘッドハンティング等）や利用（CISO シェアリング等）」、「社内の人材の育成」に分類できる。まず、人材を集めるためには、待遇面等のインセンティブを付与することが効果的である。また、人材確保のため現状の課題は、セキュリティ人材に求める要件が定義できていないということであると考えられる。セキュリティ人材の要件が定まっていないと、育成のための教育プログラムの構築やどのような人材を採用すればよいかということが曖昧になってしまうことが予測される。したがって、インセンティブ等の人事制度の整備やセキュリティ人材の要件の明確化が今後の課題であると考えられる。

5.2.5. サプライチェーンのサイバーセキュリティ対策

サイバー攻撃の多様化等に伴い、自社に対するサイバーセキュリティ対策だけではなく、サプライチェーンの委託先等に対するサイバーセキュリティ対策の実施が重要である。企業インタビューを通じて、サプライチェーンのサイバーセキュリティ対策について、「サプライチェーンマネジメントの重要性は認識しているものの、対応が進んでいない」との見解が得られた。

サプライチェーンのサイバーセキュリティ対策があまり進んでいない原因としては、「人材不足」と「具体的な対策方法が不明瞭であること」の 2 点が考えられる。まず、人材不足について、繰り返しになるが、緊急性が高い業務に人員が優先的に投入されており、サプライチェーンのサイバーセキュリティ対策に対応できる余力がある企業が多くはないと推察される。また、具体的な対策が不明瞭であることについて、「顧客情報等の重要な情報を委託先が管理しているため、どのようにアプローチすればいいのかわからない」との見解が得られた通り、情報資産の管理方法や IT システムの構造上の問題等によって、サプライチェーン全体のセキュリティ対策は一筋縄ではいかない。しかし、一ヵ所でも十分なセキュリティ対策が実施できていない委託先等が存在する場合、サプライチェーン全体のセキュリティ対策のレベルは下がってしまう。そこで、契約時に責任範囲を明確化する等の対応策もあるが、これだけでは不十分である。具体的な対策・アプローチが分からない企業が多数存在していることが想定されるため、「サプライチェーンのサイバーセキュリティ対策が十分にできていると判断するための基準」の策定が今後の課題であると考えられる。

5.3. 調査結果

5.3.1. サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

経営戦略の観点から自社の守るべき情報を特定し、サイバー攻撃の脅威や影響度を評価した上で適切な対応を講じることが重要である。そのために、豊富な経験を有する企業が既に実施している取組みについて、インタビュー調査を実施した。

セキュリティリスクの把握のために、「アセスメントの精度を高めるよりも、まずは無償のアセスメントツールを用いてリスクアセスメントを実施している」や「外部のセキュリティパートナーと隔週で情報共有をし、指示をもらっている」、「リスクアセスメントを監査ではなく点検という姿勢で実施することによって、現場から相談してもらえる信頼関係を構築している」などの取組みが見られた。また、リスク対応のために、「業界基準をベースに独自の基準を作成している」取組みや「時間や資源が限られているため、リスクベースアプローチの考え方で、リスクが高い領域に対策を優先的に実装している」という見解が得られた。

企業インタビューから得られた主な見解や取組みの事例を以下に記載する。

（セキュリティリスクの把握のための工夫）

- セキュリティに課題があることが公知になると、一気に信用を失い事業が消滅する可能性があるため、外部のセキュリティパートナーと 2 週間に 1 回程度定例のミーティングで情報を共有し指示を仰いでいる。
- リスクアセスメントのために、無償のアセスメントツールを使用している。IT 資産をすべて洗い出して管理することは困難であるため、リスクアセスメント自体の精度を高めるのではなく、「有効な対策を把握・実施すること」に注力している。
- リスクアセスメントは毎日やらないといけない業務だと考えている。現状は、すべて人で対応しているが、当面は AI での代替はできないと考えている。そのため、自社のシステムや情報資産がすべて頭に入っている経験のある人材の教育が必要である。
- リスクアセスメントは、監査ではなく点検という姿勢で実施している。その結果、現場から相談してもらえるような信頼関係を構築できている。
- 監査の名目で実施してしまうと、現場は不正や不都合な事実を隠すようになり、それが最終的に大きなインシデントにつながる可能性もある。

（リスク対応のための工夫）

- 業界団体が作成した情報開示認定制度の基準をベースに、ISMS の考え方を加味して、リスク対応の基準を作成している。
- IT 資産や情報資産の洗い出しといったリスクの評価作業は重要であるものの、時間と資源が限られているため、リスクベースアプローチの考え方の下、早急にリスクが高い領域から具体的な対策を実装することを優先した。具体的には、外部情報をもと

に、想定されるサイバー攻撃の手法を全て洗い出し、一つずつ自社の業務・システム環境で起こり得るかを検証した。

5.3.2. サイバーセキュリティ対策における PDCA サイクルの実施

サイバーセキュリティ対策を確実に実施して改善していくためには、PDCA サイクルの強化が重要である。PDCA サイクルを強化するために、サイバーセキュリティ対策に豊富な経験を有する企業の取組みについて、インタビュー調査を実施した。

まず、Plan について、「セキュリティ計画を年に 2 回見直している」、「必要に応じて、随時追加予算を確保している」、「生産拠点に向けては、グローバルポリシーをレベルダウンさせたポリシーを策定している」との取組みが見られた。

また、Check について、「PDCA サイクルの中でも特に Check を重要し、現場従業員への情報共有や教育に注力している」といった見解や、「外部シナリオを参考に作成した独自のシナリオの演習を実施している」、「既存のセンサーの有効性を確認するために、平時よりセンサーの数値を確認している」などの取組みが見られた。

企業インタビューから得られた主な見解や取組みの事例意見を以下に記載する。

（Plan のための工夫）

- サイバーセキュリティの領域では、中期事業計画では期間が長すぎるため、年次計画とし、年に 2 回ほど計画の見直しを実施している。イレギュラーの情報を入手したり、インシデントが発生したりした場合は、随時計画を見直し、追加予算の確保も行うこともある。
- サイバーセキュリティに関する中期計画を策定しており、毎年のレビュー結果に基づいてこれをアップデートしている。
- 生産拠点のセキュリティは重要であるが、情報セキュリティと同レベルのセキュリティを生産拠点に求めることは難しいため。グローバルポリシーを生産拠点向けにレベルダウンしたポリシーを策定している。

（Check のための工夫）

- 演習に限らず実際のインシデント時も同様であるが、何か起きた際は対処を優先するが、同時に対処に要した時間や対処の内容等の証跡を記録することを徹底している。
- PDCA サイクルの中でも、特に、日々の業務に追われるとついつい見逃してしまいがちなチェックを重要視している。チェックやチェックを基にした改善がどのような効果を発揮するか、現場従業員が理解できるように情報共有や教育に注力している。
- 全従業員対象に、標的型メール訓練を年に複数回実施している。開封した職員には再度のチェックを実施する。加えて、職層や階層別の研修時のコンテンツの 1 つとし

て、サイバーセキュリティ研修を実施しているほか、定期的な e ラーニングも実施している。
- 外部で受けた訓練シナリオ（NISC・金融庁の分野横断演習(DeltaWall)）等）を参考に、自社で独自のシナリオを作成して演習を実施している。
- 既存のセンサーの有効性を確認するために、継続的に平常時の数値を計測することが重要である。また、センサーの数値は毎月計測しており、数値や結果は経営層に対して情報共有している。

5.3.3. 情報共有活動への参加を通じた攻撃情報の入手とその有効活用

サイバーセキュリティに関する有益な情報を取得するために、日頃の社内における机上リサーチや IT ベンダからの情報提供も効果的であるが、外部の情報共有活動への参加も効果的である。外部への情報共有活動への参加や、取得した情報の有効活用の取組みについて、インタビュー調査を実施した。

外部のコミュニティ等の情報共有活動へ参加する際には、「参加企業が周囲の参加者の信頼を獲得し、情報を取得するためには、Give and Take の考え方が重要である」、「他の参加者からの信頼を集めるためには、オンラインの非対面な活動だけではなく、オフラインの対面での活動が必要である」、「勉強会や交流会の事務局等の手伝いを積極的にすることによって、外部人脈の構築が可能である」との見解が得られた。

また、情報の活用に関する課題として、「メールベースでの情報配信を行っている団体やコミュニティが多く、受け手は、全文を読んでから対応する必要があるため非効率である」や「事業者によって社内体制の構築度合いやセキュリティへの意識にバラつきが大きい」との見解が得られた。

そして、入手した情報を活用し、その結果を経営層へ報告する際には、「IT やセキュリティの言葉をそのまま使用せず、可能な限り平易な表現で伝える」や「平常時から情報共有を行い、経営層とも信頼関係を構築している」、「インシデントが発生したときにだけ報告しに来るというネガティブなイメージを経営層に抱かせない工夫も重要である」との見解が得られた。

企業インタビューから得られた、主な見解や取組みの事例を以下に記載する。

（外部との信頼関係の構築）
- コミュニティを通じて、参加企業が周囲の参加者の信頼を獲得し、情報を取得するためには、Give and Take の考え方は重要である。
- チャタムハウスルール（参加者は受け取った情報を自由に引用・公開することができるが、情報発信者や他の参加者を特定する情報は伏せなければならない）等の行動規範を定めた中で、やる気があり、コミュニティ内で中心となり活動する参加者は、信頼を集めている。

- 他の参加者からの信頼を集めるためには、オンラインの非対面な活動だけではなく、オフラインの対面の活動が必要である。そして、「相談を含めたコミュニケーション」、「情報共有」、「共助の関係が成立」という循環が形成される。
- 勉強会や交流会の事務局等の手伝いを積極的にすることによって、外部人脈の構築が可能である。
- 情報共有のコミュニティ等の取組では、Give and Take の精神がないと、情報を取得できないということを意識している。
- 共有する情報には、機微な情報も含まれるので、秘密保持契約を参加者間で交わした上で、情報共有時のルール（メールの暗号化等）を定めている。

（情報活用に関する問題）

- 日本の企業や組織の多くは、メールを用いて情報の収集や配信を行っているため、受け手が、大量のテキスト情報から有用な内容を取捨選択し、活用可能なフォーマットに転換する必要がある等、対応の負荷が高い。
- 事業者により情報の分析や活用を行うための社内体制の構築度合いやセキュリティに対する意識にバラつきが大きいため、共有する情報の内容やレベル感等の最適化が難しい。

（経営層への報告に関する工夫）

- 経営層とコミュニケーションを取る際は、IT やセキュリティの言葉をそのまま使用せず、可能な限り平易な表現で伝えるように工夫している。例えば“セキュリティに穴がある“等。また、有事の場合の業務や収益への影響等「インパクト」を伝えることに留意している。
- 経営層向けの「翻訳」のコツは、なるべく「絵を描く」ことや、起きたことの「影響」を伝えることに留意することである。後者は、事象のロジックを細かく説明するよりも有効である。
- 平常時から情報共有をしておくと、経営層とも信頼関係を構築することができる。インシデントが発生したときにだけ報告しに来るというネガティブなイメージを経営層に抱かせない工夫も重要である。

5.3.4. セキュリティ担当者の悩み

本企業インタビューでは、事前に準備した質問項目のほか、セキュリティ担当者が抱えている悩みについても調査を行った。結果として、「人材」、「情報共有活動」、「サプライチェーン」等についての悩みを確認できた。

まず、人材について、「セキュリティ人材が待遇面で優遇されることは少ないため、人が集まらず、育成も難しい」や「予算は十分にあるものの、IT と制御系の両方に精通した人材の絶対数が不足している」との見解が得られた。

また、情報共有活動について、「情報交換ができるコミュニティが不足している」や「人材不足の為、外部との情報交換・コミュニティへの参加が自由にできない」との見解が得られた。

最後に、サプライチェーンについて、「サプライチェーンに関するセキュリティリスクは認識しているが、対応に苦慮している」や「具体的なアプローチが不明」、「サプライチェーンマネジメントを十分に実践しているという基準が分からない」との見解が得られた。

企業インタビューから得られた、主な見解や取組みの事例を以下に記載する。

（人材について）

- セキュリティ人材が待遇面で優遇されることは少ないので、人が集まらない。また、育成も難しい。
- インシデント等が何もなければ業務的には暇ではあるが、足元が固まっていないため、サプライチェーンマネジメントや将来への教育が後回しになってしまっている。
- サイバーセキュリティの重要性については経営層も十分に理解しており、予算も十分にあるものの、IT と制御系の両方に精通した人材の絶対数が足りない。

（情報共有活動について）

- 情報交換ができるコミュニティは不足している。
- 外部との情報交換・コミュニティへの参加が自由にできない。そのため、欲しい情報が必要な時に得られないし、誰に聞けばいいのかもわからない。
- 外部の団体やコミュニティを作りたくても、日々のインシデント対応に時間を取られ、コミュニティ活動に時間を割くことは難しい。
- 情報共有活動に注力できるのは大企業だけであり、サプライチェーン上の中小企業は予算も人員も不足しているため、情報共有活動に取り組むことは難しい。

（サプライチェーンについて）

- サプライチェーンマネジメントを十分に実践しているという基準が分からない。
- サプライチェーンに関するセキュリティリスクは認識しているが、対応に苦慮している。委託契約を締結している場合は、まだ対処のしようがあるが、単発契約の場合はほとんど管理不可能である。
- サプライチェーンのリスク管理は認識しているものの、サービスの受け手としてどこまで効果的な対策が打てるかという意味で非常に悩ましい。対策を打つにしても、投資対効果の点でも整理が困難である。

6. 調査結果のまとめ

文献調査及びアンケート調査、有識者・企業インタビュー調査を通じて、国内企業におけるサイバーセキュリティの認識や取組みの状況、CISO 等の動向等を把握し、その課題を明らかにした。

本章では、サイバーセキュリティに関する企業の動向および課題について取りまとめる。

6.1. サイバーセキュリティに関する企業の動向

6.1.1. 経営層はサイバーセキュリティ課題認識を有している傾向

調査を通じて、多くの企業の経営層がサイバーセキュリティに課題認識を有していることが明らかになった。

まず、アンケート調査から、「経営層のリスク感度が低い」や「経営層に IT やセキュリティの重要性を理解してもらえない」と回答する企業はそれぞれ約 10%に留まり、CISO 等を任命している多くの企業の経営層は、サイバーセキュリティリスクやその対策に関心があり、サイバーセキュリティに課題認識を有していることが明らかになった。また、予算を課題と認識する割合は約 25%（次図参照）であった。

また、経営層が意思決定を行う上で重視している情報として、「自社や同業他社で発生したインシデントの情報」と回答した割合は 40%以上であったが、「レピュテーショナルリスク」と回答した割合は約 10%であった（図 7-13 参照）。さらに、インタビュー調査では、「経営層はサイバーセキュリティを一括りに考えている傾向がある」との見解が得られており、経営層はサイバーセキュリティの重要性を理解はしているものの、サイバーセキュリティが自社へ与える具体的な影響を十分に理解できている経営層はあまり多くはないと考えられる。

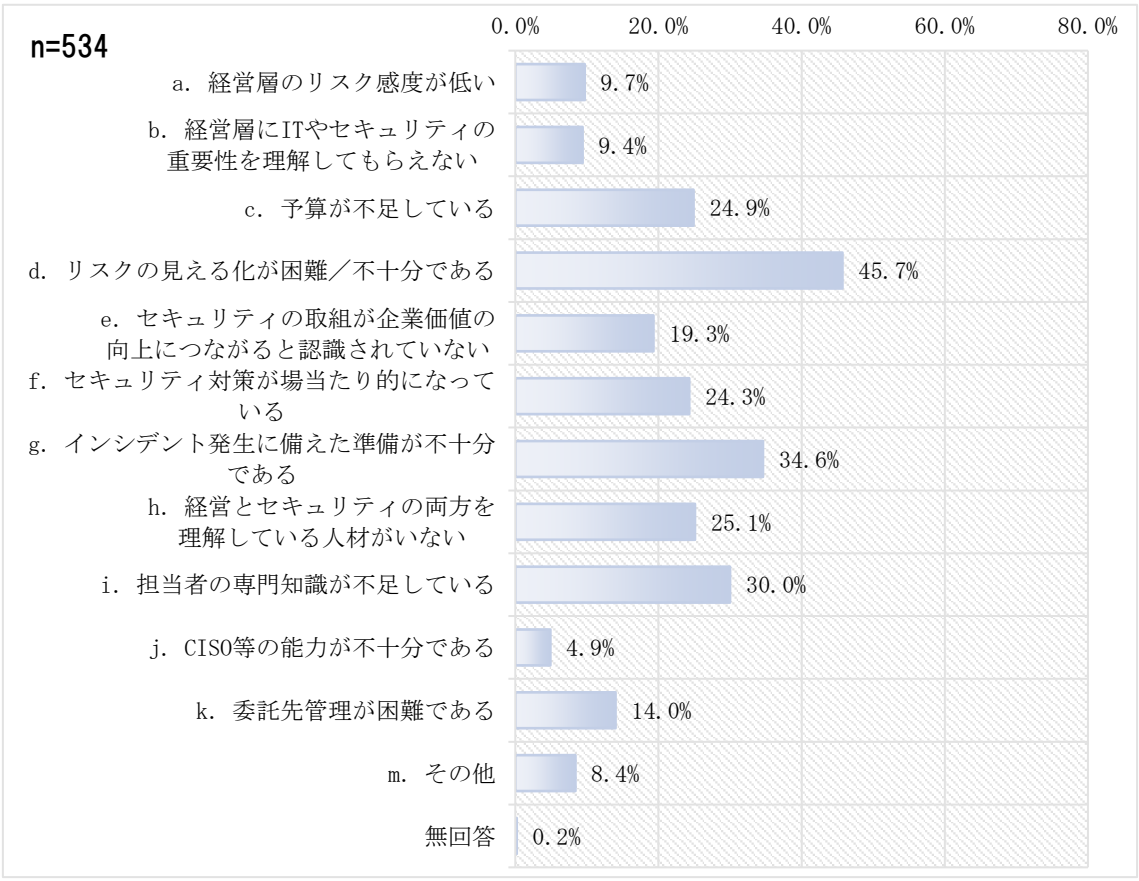

図 6-1　サイバーセキュリティに関する課題認識

6.1.2. 兼任の CISO 等の任命が主流

調査を通じて、専任の CISO 等を任命している企業が少ないことが明らかになった。アンケート調査では、「兼任の CISO 等を任命している」と回答した企業は約 90%（下図参照）であった。そして、インタビュー調査からも、「専任の CISO 等を任命している企業は多くはない」との見解が得られた。さらに、この背景として、「多くの企業において CISO 等の業務内容、権限、責任が明確に規定されていないこと」との見解も得られた。現状の CISO 等の役割は、ISMS の推進等にとどまっており、経営・事業的役割が明確になっていない企業が多いことが想定される。そのため、名目的に CISO 等のポジションを他のポジションと兼務させているという事態になっていると考えられる。また、そもそも専任の CISO 等を任命できるほどの人材を量的・質的に確保できている企業が多くはないということも要因の 1 つと考えられる。

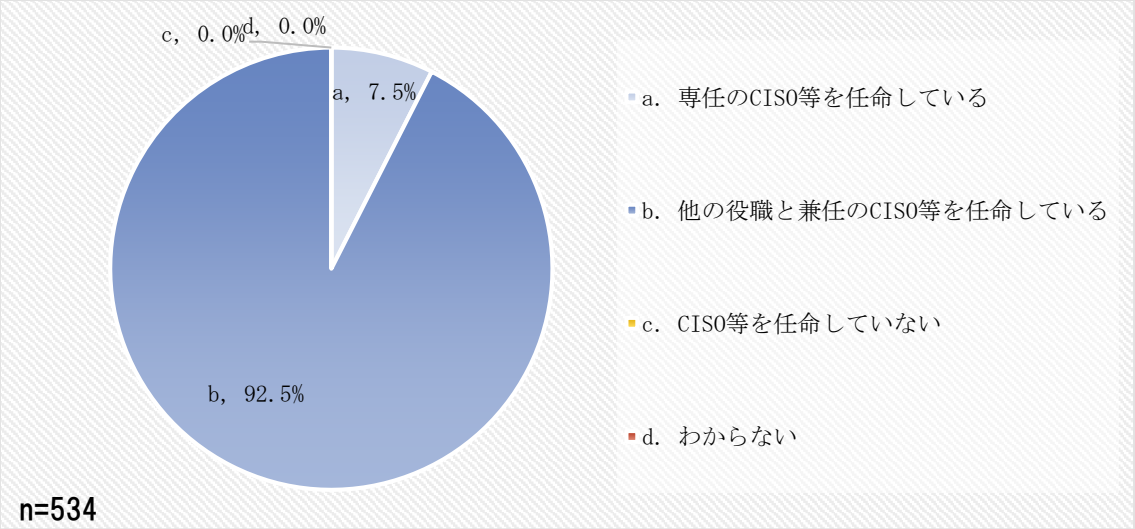

図 6-2　CISO 等の設置状況

6.1.3. CISO 等に期待される役割は、技術的役割と経営・事業的役割の両方

調査を通じて、CISO 等に対して、「技術的役割」だけではなく、「経営・事業的役割」も担うことを期待している企業が多数存在していることが明らかになった。

アンケート調査では、CISO 等に「技術的役割」のみを求める割合は 6.7%（下図参照）にとどまり、非 IT システム関連部門出身の CISO 等の割合が大きいことが明らかになった。また、インタビュー調査では、「CISO 等にはサイバーリスクに限定しない全般的なリスクマネジメントの学習が重要」との見解も得られた。

以上の結果を踏まえ、サイバーセキュリティ対策は、もはや「技術的な課題」ではなく、事業の停止や信用の失墜等のリスクに鑑み、「経営課題」と認識している企業が多数存在していると考えられる。

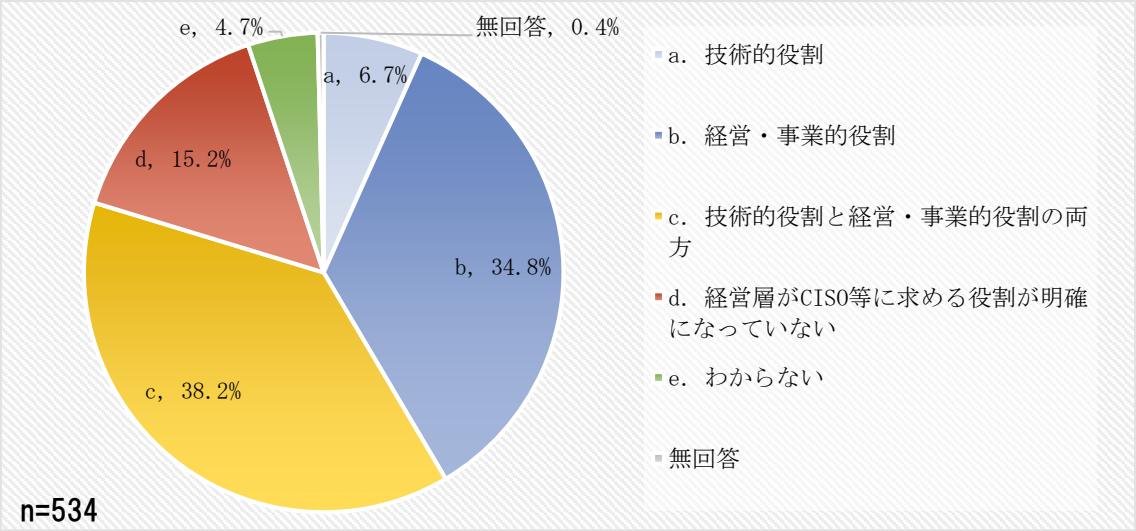

図 6-3　経営層が CISO 等に求める役割

6.2. サイバーセキュリティ対策の推進上の課題

6.2.1. CISO 等の業務内容や責任、権限の明確化

CISO 等が期待される役割を果たすためには、その業務内容や責任、付与する権限を明確に定義する必要がある。

調査を通じて、CISO 等に期待される役割は、大枠として「経営・事業的役割」であるが、詳細な役割として「予算の確保」、「人材の確保」、「コミュニケーションを通じて、経営層や関係者等のステークホルダーとの関係の構築」等が重要であることが明らかになった。一方で、CISO 等を兼任で任命している企業が多い背景として、CISO 等の業務内容や責任、権限が明確になっていないとの見解が得られた。

兼任で CISO 等を任命している企業では、CISO 等の役職が形骸化もしくは、名目的に設置されている可能性もあり、有効なサイバーセキュリティ対策が推進されていない可能性も推察される。IPA が実施した過去の調査「CISO 等セキュリティ推進者の経営・事業に関する役割調査」(2018 年 3 月)でも、「経営層が、CISO 等に必要な権限と責任を明確にし、与えるよう、啓発普及すること」と結論付けられており、CISO 等の形骸化を防ぎ、有効なサイバーセキュリティ対策を推進するためにも、企業および経営層には継続して、CISO 等の業務内容や責任、権限を明確にしていく取組みが求められる。

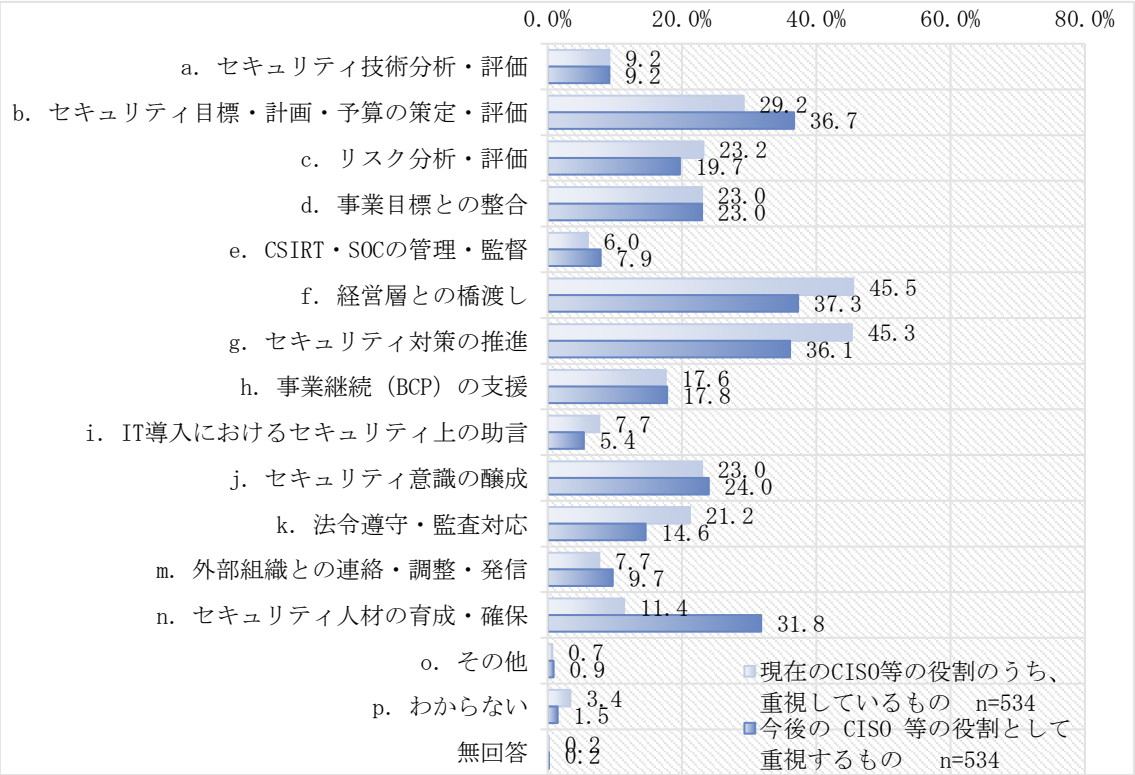

図 6-4　重視している CISO 等の役割

6.2.2. セキュリティ人材の確保

サイバーセキュリティ対策を推進するためには、CISO 等や CISO 等をサポートする人材を質的・量的に確保する必要がある。

調査を通じて、「予算はあるものの、人材が確保できていない」や「日々の業務が優先され、人材の育成に注力できていない」、「サイバーセキュリティ人材の要件が分からない」等、人材確保に苦労している企業が多数であることが明らかになった。

セキュリティ人材を育成もしくは確保するためには、セキュリティ人材のモデルを定義することが必要である。この点については、経済産業省を中心に検討が進められており、セキュリティ人材の全体像の可視化や育成・活躍促進のためのモデルの構築が進められてい

る[11]。また、企業としては、セキュリティ人材が活躍できるようなキャリアパスの形成や、評価・給与等の制度設計、セキュリティ人材のモチベーションが向上されるような組織文化の醸成、働きやすい環境の整備などの取組みが求められる。

そして、人材不足に伴う問題として、「脅威情報等の情報収集や収集した情報の活用が難しい」との意見が調査を通じて明らかになった。外部のコミュニティとの信頼関係を構築することによって、情報収集源を確保できるだけではなく、情報の分析の際に相談をできる人脈を形成できる可能性もある。情報の収集から分析までを自社で完結させるだけではなく、外部のコミュニティや人材を活用することも効果的であると考えられる。

6.2.3. サプライチェーンに対する具体的な対策の実行

事業の IT 化やグローバル化に伴い、サプライチェーンの複雑化が進む中、自社の情報システム等の特定機能の防御だけではなく、サプライチェーンの委託先等に対するサイバーセキュリティ対策の実行が必要である。

調査を通じて、「サプライチェーンのリスクを認識していない企業は少ない」や「重要性は認識しているものの具体的な対策はできていない」等、サプライチェーンに対するセキュリティ対策の重要性の理解度は高まっているものの、具体的な対策を実行できている企業は多くはないことが明らかになった。

サプライチェーンのセキュリティ対策を実行する上での問題は、「人材不足でサプライチェーンのセキュリティ対策まで手が回らないこと」や「具体的な対策がわからないこと」が想定される。企業としては、サプライチェーン上のパートナー企業等と責任範囲やセキュリティ対策に関する契約の締結や、定期的な監査を通じた対策状況の把握、サイバー保険への加入等が効果的と考えられる。また、通常のサイバーセキュリティ対策と同様に、まずは重要情報の特定に取り組むことが重要である。しかしながら、現時点では、サプライチェーンのセキュリティ対策を手探りで進めている企業が多い。そのため、サプライチェーンのセキュリティ対策の手引きや事例、最低限実施する必要がある対策の一覧等が整備されれば、サプライチェーンのセキュリティ対策に取り組もうとする企業に参考となると考えられる。

6.2.4. PDCA サイクルの実践のための Check の実施

セキュリティ対策を PDCA サイクルとして実施させるために、セキュリティ対策の実施の状況を確認し・評価する Check の取組みが必要である。

アンケート調査を通じて、セキュリティ対策の十分な Check（確認・評価）として、演習や訓練、情報収集を実施できている企業は約 50%（次図参照）、ペネトレーションテストや脆弱性診断を実施できている企業は約 40%程度（次図参照）であることが明らかになった。また、上記の Check の方法の中でも、インタビュー調査を通じて、「独自シナリオを作成し

[11] 経済産業省「事務局説明資料」（第 5 回産業サイバーセキュリティ研究会 WG2 資料）

て、演習を実施することが重要である」等、演習の重要性が明らかになった。演習には、従業員のサイバーセキュリティに対する意識の醸成や教育（サイバー攻撃発生時の対応等）の場としての効果が期待される。

企業としては、セキュリティ対策の有効性を確認するためにも、定期的な Check の取組みが求められる。また、Check の結果を基に、セキュリティ対策の Act（見直し・改善）まで実施し、サイバーセキュリティ対策を強化していくことが求められる。

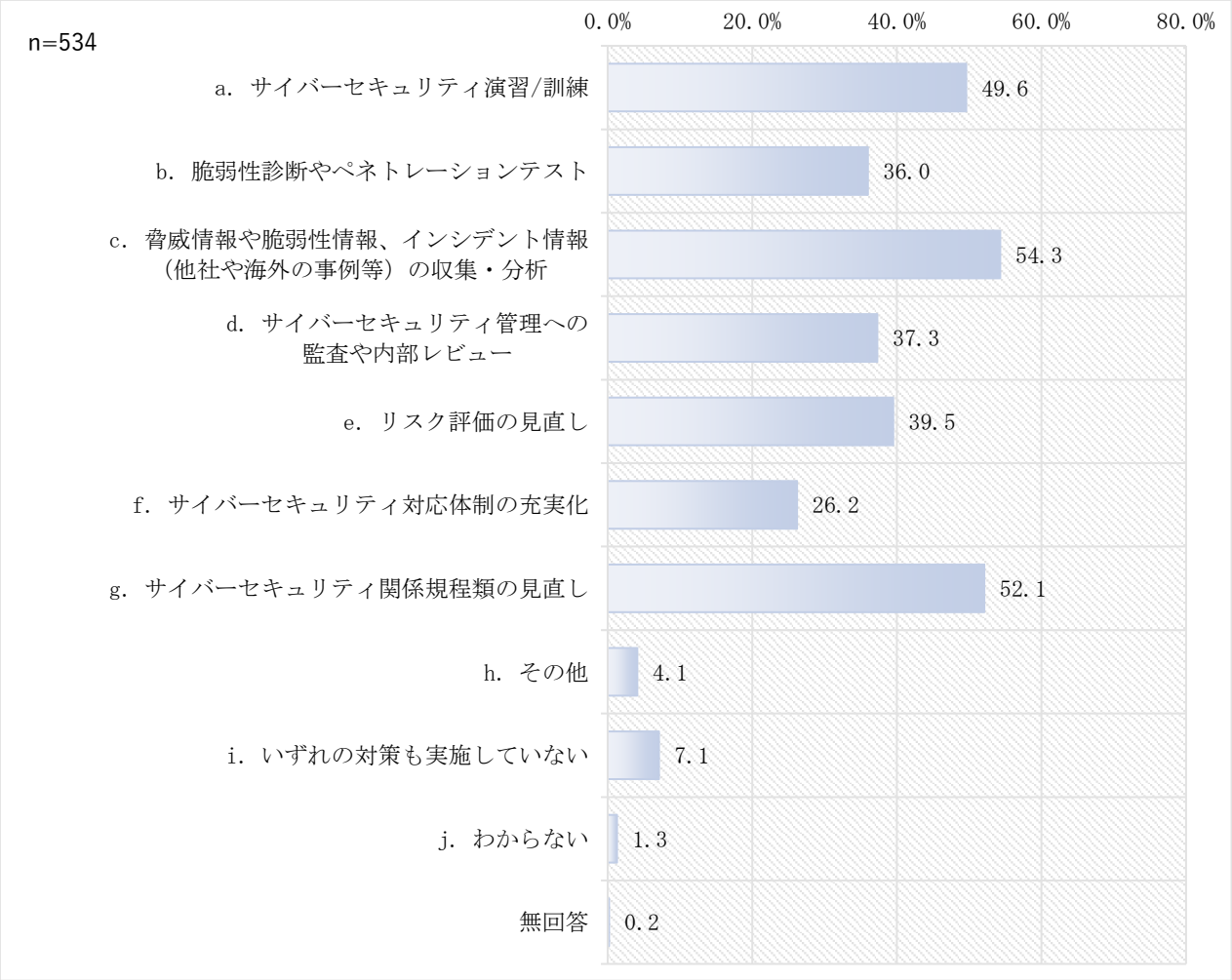

図 6-5　サプライチェーンセキュリティのリスク認識

7. データ集

7.1. 文献調査の結果

文献調査の結果を以下に記載する。

7.1.1. 文献 1：CISO ハンドブック [12]

「CISO ハンドブック」は、2018 年 5 月 11 日に、「CISO が経営陣の一員としてセキュリティ業務を執行する上で前提となる、ビジネス（経営）の基本的な枠組みを整理し、明確にすべき目標と指標、そして施策を評価する判断基準を提供することを目的」[12]として、日本ネットワークセキュリティ協会（JNSA)よって発行された文書である。

情報セキュリティの目的や課題、情報セキュリティマネジメントの基礎知識（ビジネスリスクと情報セキュリティの関係、経営サイクルと情報セキュリティ・マネジメントサイクル等)、経営陣としての CISO 等への期待（経営会議での報告、関係部門との連携等）等が記載されており、セキュリティ業務やビジネス、経営会議で議論される業務執行（CISO の役割と責任、業務）等を理解するための参考となる情報が整理されている。

本文献では、CISO 等に対して、事業計画の理解やリスクの分析・評価、ポリシーの策定、リスク管理の枠組みの見直し等多岐に渡る役割が期待されている。また、CSIRT に関しては、「復旧体制には、CSIRT にとどまらず社内の複数部門と連携した対応が必要であるが、こうした対応がインシデント対応計画に含まれていないことがあるのではないか」、「CSIRT の規模が会社の規模と整合していない企業があるのではないか」等の問題が提起されている。そして、情報共有に関しては、「脅威情報の収集を行うチャネルを確保する必要があるが、情報収集先や収集の手順が定義できていないケースがあるのではないか」等の問題が提起されている。

下表に、①CISO 等への期待や活動実態、②経営層への期待や活動実態等のその他の有益な知見の 2 つの観点から本文献より収集した主な情報（知見）を整理する。

---

[12] 日本ネットワークセキュリティ協会（JNSA)「CISO ハンドブック」https://www.jnsa.org/result/2018/act_ciso/

表 7-1　文献 1 から抽出した情報（知見）の整理 [13]

項目番号	CISO 等への期待や活動実態	経営層への期待や活動実態等の その他の有益な知見
指示 1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定	● リズム・オブ・ビジネスや事業計画や目標の理解、数字、評価指標などを織り交ぜることにより共通言語での相互理解が望ましい。	● サイバーセキュリティ対応方針の策定において、IT 部門やリスク部門の課題認識だけで実施している企業があるのではないか ● 組織全体のガバナンスの問題として、リスクを俯瞰して理解した上で、組織目標と整合性を持った内容を規定する意識が不足しているのではないか
指示 2 サイバーセキュリティリスク管理体制の構築	● CISO は、IT 環境の変化に応じた対策を計画、立案、実施できるような仕組みづくりを常に考慮することが望ましい ● CISO はセキュリティ施策を展開し維持するために、セキュリティ対策が自動的に適用され、計測が行える等正規版を構築することが望ましい	● サイバーセキュリティ管理体制を構築するにあたって、以下のようなステップを踏まえる必要がある • 事業計画の理解 • 経営環境・事業環境におけるサイバーセキュリティリスクの理解 • セキュリティポリシーの策定 • 不足するリソースの整理 • サイバーセキュリティリスクの変化の分析、リスク管理枠組みの見直し
指示 3 サイバーセキュリティ対策のための資源(予算、人材等)確保	● CISO は、役職（職位）に基づいた権限付与ではなく、ロール（職務）に基づいた権限を付与することで、人員の移動など役割の変更に一貫性を持った対応ができる仕組みづくりを構築すること	● サイバーセキュリティ対策において、専門的なノウハウを有する外部専門家の活用を進めている企業は少ないのではないか
指示 4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	● サイバーセキュリティ対策の検討において、IT 利活用の利便性との関係を定量的に比較・勘案する視点が不足しているのではないか	● サイバーセキュリティ対策の検討において、セキュリティアーキテクチャ（システムのセキュリティ機能自体を攻撃から守る仕組）や情報のライフサイクルの視点を加味できていない企業があるのではないか
指示 5 サイバーセキュリティリスクに対応するための仕組みの構築	● CISO は個々のシステムのログを単独で扱うのではなく、統合的に収集管理ができる統合ログ管理基盤を構築すること	● 情報セキュリティ対策において、個々の IT 資産のリスク評価、各人員のロールに着目した必要な ID 権限の設定・管理、統合ログ管理、計測可能なセキュリティ統制基盤の構築等基礎的な対策ができていない企業があるのではないか
指示 6 サイバーセキュリティ対策における PDCA サ	● CISO は、マネジメントサイクルを単なる改善だけではなく、企業としての学習と成長につなげていく。そのためにも情報セキュリ	

[13] 日本ネットワークセキュリティ協会（JNSA）「CISO ハンドブック」に基づき、NTT データ経営研究所にて作成

項目番号	CISO 等への期待や活動実態	経営層への期待や活動実態等のその他の有益な知見
イクルの実施	ティ計画を丹念に検討し、その評価を通じて事業部門・他部門・経営陣といったステークホルダーと協力を得ることが望ましい ● CISO は、IT やリスク部門のみならず、他部門や経営陣を巻き込んで情報セキュリティ計画を精緻化していくことが求められるが、十分にコミュニケーションが取れていないケースがあるのではないか	
指示７ インシデント発生時の緊急対応体制の整備		● CSIRT の規模が会社の規模と整合していない企業があるのではないか
指示８ インシデントによる被害に備えた復旧体制の整備	● 総務・人事部門は情報セキュリティの計画と実装、緊急対応など、セキュリティ対策全般において連携が必要な部門となる。それぞれの業務ドメインが違うため、同じ課題に対して異なる常識を持つことも考えられるため、目的と手段を明確にしながら、協力関係を構築することが望ましい ● 法務部門はコンプライアンス対応に不可欠な部門で、法令やガイドラインを相互に理解する必要がある。またセキュリティ侵害や事故が発生した際に対応を進める際にも、法務部門の協力が不可欠である。事前に緊急対応マニュアルを作成し、必要な対応を明確にしておくことが望ましい ● 広報部門とは緊急時だけではなく、定期的にコミュケーションを図り、緊急対応が必要なセキュリティ侵害や事故が発生した場合に、遅滞なく連携が取れることが望ましい	● 復旧体制には、CSIRT にとどまらず、社内の複数部門と連携した利害関係者への対応が必要であるが、こうした対応がインシデント対応計画に含まれていないことがあるのではないか （例） ・ 総務・人事部門：緊急的な人材の配置等 ・ 法務部門：法的解釈からみた対応の整理等 ・ 広報部門：外部への情報発信等
指示９		
指示１０ 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	●サイバーキュリティ事象や脅威情報について、情報収集を行うリソースやチャネルを確保する必要があるが、規程等で情報収集先や情報収集手順が定義できていないケースがある ●収集・分析した脅威情報に関して、ビジネスへのインパクトを社内へ報告する方法の整理、エスカレーションルートが規定等で定義できていないケースがある	

7.1.2. 文献 2：Cybersecurity Assessment Tool[14]

「Cybersecurity Assessment Tool」は、米国連邦金融機関検査協議会が、昨今のサイバー攻撃の脅威の拡大と高度化が進んでいることを受け、金融機関が自組織のサイバーセキュリティに対する取組みの成熟度を測定することを可能にするために、2015 年 6 月に公表したものである。

この「Cybersecurity Assessment Tool」は、FFIEC の情報技術検査ハンドブックの指針やサイバーセキュリティ関連の規制・ガイドライン、米国国立標準技術研究所のサイバーセキュリティフレームワークを含む他の業界で受け入れられているサイバーセキュリティ業界標準の概念が組み込まれている。

本文献は、金融機関がサイバーセキュリティの成熟度を測定するツールが主に記載されているため、CISO 等への期待や CISO 等の活動実績に関する特に明示的な記載は確認できなかった。しかし、「インシデントレスポンスに必要となる、対処・判断・連携に係る一連の手順、および、BCP との連携について定義が求められている」、「委託先のサイバーセキュリティを管理・分析するプロセスを整備することが求められている」等の知見を元に、「インシデント対応計画が未整備の企業がまだあるのではないか」、「サプライチェーンのサイバーセキュリティについて、対象とすべきサプライチェーンの範囲の特定（網羅的なリスク評価）や、サプライチェーンに応じた実効的な対応策の構築ができていない企業が多いのではないか」等の仮説が導かれた。

次表に、経営層への期待や活動実態等のその他の有益な知見の観点から本文献より収集した主な情報（知見）を整理する。

[14] FFIEC「Cybersecurity Assessment Tool」 https://www.ffiec.gov/cyberassessmenttool.htm

表 7-2 文献 2 から抽出した情報（知見）の整理[15]

項目番号	経営層への期待や活動実態等のその他の有益な知見
指示１ サイバーセキュリティリスクの認識、組織全体での対応方針の策定	● 組織全体での対応方針（サイバーセキュリティポリシー）の策定とともに、企業文化の醸成が求められており、全社的なサイバーセキュリティに対する理解が求められる ● 対応方針（サイバーセキュリティポリシー）には、CISO の責務にとどまらず、ボードメンバーの責任についても求められる
指示２ サイバーセキュリティリスク管理体制の構築	● 管理体制には CISO にとどまらずボードメンバーの役割、果たすべき責任を明確にすることが求められており、単に CISO の任命にとどまらない関与が求められる
指示３ サイバーセキュリティ対策のための資源(予算、人材等)確保	● 企業のリスクプロファイル（どの程度サイバーの脅威に晒されているか）に応じて、必要なリソースが変わるとの考えから、企業に必要とされるリソースを特定するためのプロセスそのものを整理することが特徴的となっている ● また育成プログラム、研修プログラムといった各種の計画も企業のリスクプロファイルに応じた必要な知識をベースとしたものを求めている
指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	● リスク管理プログラムとして、リスク評価（保有する IT 資産を起点とするもの)、分析結果に基づく改善については、記載レベルに大きな差異はない
指示５ サイバーセキュリティリスクに対応するための仕組みの構築	● リスク分析の結果として技術的な仕組みを導入する枠組みを構築することに加え、各種の防御・検知についての技術的対応についても一定程度のレベルが求められる
指示６ サイバーセキュリティ対策における PDCA サイクルの実施	● PDCA サイクルについての言及は、より上位概念でのみ語られており、以下の４つを定期的に実施することが求められている。 ・ サイバーセキュリティポリシーの策定 ・ ポリシーに基づくリスク管理 ・ ポリシーが順守されているかの監査・サイバーセキュリティ対策とポリシーが全社のリスクアペタイトステートメントと整合性が取れているかの監査 ・ 改善（脆弱性に係る内容が中心となっているもののポリシーについても同様のサイクルを想定）
指示７ インシデント発生時の緊急対応体制の整備	● インシデントレスポンスに必要となる、対処・判断・連携に係る一連の手順、および、BCP との連携について定義が求められている
指示８	
指示９ ビジネスパートナーや委託先等を含めたサプライチェーン全体の対	● 委託先管理、データ管理の２点からサプライチェーンを捕捉することを求めている 【委託先管理】 ● 委託先のサイバーセキュリティを管理・分析するプロセスを整備することが求められている。

[15] FFIEC「Cybersecurity Assessment Tool」に基づき、NTT データ経営研究所にて作成

項目番号	経営層への期待や活動実態等のその他の有益な知見
策及び状況把握	● また、契約書面でサイバーセキュリティを確保していること、インシデント発生時の報告等、既存の委託先管理にサイバーセキュリティの項目を付加して管理することが求められている 【データ管理】 ● データのサプライチェーンについてもネットワーク図等を利用したデータの流れを整理することが求められている
指示１０ 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	● 大きく３つの整理がなされている ・ 外部からの脅威情報の収集：情報共有機関、自社での検知等、脅威情報の収集について定めること ・ 脅威情報の分析・評価：個々の脅威情報が自社に与える脅威の有無を評価・分析すること。さらに傾向分析を基とした将来的な影響の予測、体制の整備に関する分析を実施すること。 ・ 内部への共有・他社への共有：分析した結果に関する社内関係者への共有のあり方情報共有機関への共有のあり方を定めること

7.1.3. 文献 3：CHIEF INFORMATION SECURITY OFFICER HANDBOOK[16]

「CHIEF INFORMATION SECURITY OFFICER HANDBOOK」は、米国の各府省の最高情報責任者による協議会 CISO Council が、既存もしくは新しく着任した CISO に対して、連邦政府のサイバーセキュリティにおける CISO の役割を教育するために、作成された文書である。

この「CHIEF INFORMATION SECURITY OFFICER HANDBOOK」には、CISO が、連邦政府機関がそれぞれの目標を達成できるように支援するためのリスク管理の原則を、責任をもって適用するための情報や、CISO が組織のサイバーセキュリティプログラムを開発もしくは改善する際に参考となる法律、ポリシー、ツールがまとめられている。

本文献では、CISO に対して、「自組織の任務とリソースをサイバーセキュリティの強化に向けること」、「資金調達の要求および情報セキュリティのためのその他の予算関連資料の処理と提出を行うこと」、「システムの構成要素に対する被害の潜在的な影響を理解すること」、「事件が起きた場合、すべての従業員が、被害を最小化するための自身の役割を理解している環境を確実に整えること」等の役割が期待されている。また、「人的リソースをサイバーセキュリティに自由に振り分けられるほど余裕がある企業は少ない」、「サイバーセキュリティのリスクを定量的に評価する手法を持つ企業は少ない」等の問題点も提起されている。

次表に、①CISO 等への期待や活動実態、②経営層への期待や活動実態等のその他の有益な知見の 2 つの観点から本文献より収集した主な情報（知見）を整理する。

[16] CIO Council 「CHIEF INFORMATION SECURITY OFFICER HANDBOOK」 https://www.cio.gov/resources/ciso-handbook/

表 7-3 文献 3 から抽出した情報（知見）の整理 [17]

項目番号	CISO 等への期待や活動実態	経営層への期待や活動実態等のその他の有益な知見
指示 1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定		● 大統領が発行した大統領令や予算管理局（OMB）によって発行された方針または指針を遵守する必要がある
指示 2 サイバーセキュリティリスク管理体制の構築	● CISO に対して、主な責務として組織全体の情報セキュリティを統括し、以下の役割を行うための適切な専門的資格を付与させること。 ・ 必要に応じてサイバーセキュリティソリューションを実行させること ・ 自社の任務とリソースを組織のサイバーセキュリティの強化に向けること ● CISO の責務として、権限、所掌について、サイバーの技術的な視点にフォーカスしすぎており、経営的な視点が不足している可能性はないか	
指示 3 サイバーセキュリティ対策のための資源(予算、人材等)確保	● 組織が予算をまとめた際、CISO は資金調達の要求および情報セキュリティのためのその他の予算関連資料の処理と提出を担当する	● 全従業員が情報セキュリティプログラムを理解している企業は少ないのではないか ● 人材不足の昨今、人的リソースをサイバーセキュリティに自由に振り分けられるほど余裕がある企業は少ない
指示 4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	● CISO は、システムの構成要素に対する被害の潜在的な影響を理解しなければならない。そして事件が起きた場合、すべての従業員が、被害を最小化するための自身の役割を理解している環境を確実に整えなければならない	● サイバーセキュリティのリスクを定量評価する手法を持つ企業は少ない ● 現状のリスクと想定される攻撃を把握したうえで、その対策となるサイバーセキュリティソリューションを具体的に準備できている企業は少ない
指示 5 サイバーセキュリティリスクに対応するための仕組みの構築	● 米国国立標準研究所（NIST）が公布した最低限のセキュリティ要件と標準を遵守する必要がある。	
指示 6		
指示 7 インシデント発生時の	● CISO は、システムの構成要素に対する被害の潜在的な影響を理	● インシデント発生時でも、安全を確認した上で、業務を継続で

[17] CIO Council「CHIEF INFORMATION SECURITY OFFICER HANDBOOK」に基づき、NTT データ経営研究所にて作成

項目番号	CISO 等への期待や活動実態	経営層への期待や活動実態等のその他の有益な知見
緊急対応体制の整備	解しなければならない。そして事件が起きた場合、すべての従業員が、被害を最小化するための自身の役割を理解している環境を確実に整えなければならない	きる計画と手順を整備できている企業は少ない ● インシデント発生時、被害を最小化させるために、従業員それぞれが自身の役割を理解している企業は少ない
指示８		
指示９		
指示１０		

7.1.4. 文献 4：FTSE 350 Cyber Governance Health Check 2018[18]

「FTSE 350 Cyber Governance Health Check 2018」は、英国のデジタル・文化・メディア・スポーツ省（Department for Digital, Culture, Media and Sport）が、ロンドン証券取引所に上場している企業のうち、時価総額上位 350 位の企業を対象としたサイバーセキュリティマネジメントに関する調査結果をまとめた文書である。2018 年の調査には、350 社中 94 社が調査に参加した。この調査への参加の可否の結果だけでも、サイバーセキュリティに対する意識の違いを確認することができる。

この「FTSE 350 Cyber Governance Health Check 2018」では、各企業の取締役会のサイバーセキュリティに対する理解度、取締役会のサイバーリスクに関する情報への関与度、取締役会のサイバーセキュリティインシデント管理への関与度、組織のサプライチェーンリスク管理について調査が実施されている。

本文献では、CISO に対して、「取締役会に対して CISO が直接、各種報告を実施するべきである」、「CISO が作成したサイバーセキュリティのインシデント対応手順は外部による監査をうけることも重要である」等の役割の期待や提言がなされている。また、「インシデント対応計画は、本来、事業内容の変更と合わせて見直しが必要であるものの、対応できていない企業が多い」、「自社サービスのサプライチェーンに影響する事業者、およびそのリスクについて特定できていない」等の知見を元に、「サイバーセキュリティ対策において PDCA サイクルを回せていない企業が多いのではないか」、「サプライチェーンのサイバーセキュリティについて、対象とすべきサプライチェーンの範囲の特定（網羅的なリスク評価）や、サプライチェーンに応じた実効的な対応策の構築ができていない企業が多いのではないか」等の仮説が導かれた。

次表に、①CISO 等への期待や活動実態、②経営層への期待や活動実態等のその他の有益な知見の 2 つの観点から、本文献より収集した主な情報（知見）を整理する。

[18] Department for Digital, Culture, Media and Sport 「FTSE 350 Cyber Governance Health Check 2018」 https://www.gov.uk/government/publications/cyber-governance-health-check-2018

表 7-4　文献 4 から抽出した情報（知見）の整理 [19]

項目番号	CISO 等への期待や活動実態	経営層への期待や活動実態等のその他の有益な知見
指示 1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定		● サイバーセキュリティ戦略について、取締役会に「報告して承認を得る」ことは定着しつつあるも、取締役会で「討議」を行っているケースはほとんどないのではないか ● ビジネスと整合的にリスクを把握し適切な予算確保を図るため、経営陣はリスクアペタイトを文書化した上で、それをスタッフと共有すべきではないか ● 経営陣は、自社の業務遂行に不可欠な情報や、自社で保有する情報資産・システム資産について十分に理解できていないのではないか ● 経営陣は、サイバー攻撃の被害想定（株価や営業損失など金銭的なリスク、レピュテーショナルリスク等）が十分に理解でていないのではないか ● 経営陣がサイバーセキュリティ演習に参加しているケースはまだまだ少ないのではないか（特に非金融分野）
指示 2 サイバーセキュリティリスク管理体制の構築	● 取締役会に対して CISO が直接報告を行うべきだ ● FTSE350 のうち、35%の企業が取締役会に対して CISO が直接報告を行っている ● CISO が役員でないケースが多いのではないか	
指示 3 サイバーセキュリティ対策のための資源(予算、人材等)確保		● 技術的なバックグラウンドを有するメンバーがいないため、取締役会では技術的なアジェンダが議論されることが少ないのではないか ● サイバーセキュリティ専用の予算を確保していないケースが多いのではないか ● サイバーセキュリティに関する技術的な知識やノウハウを有するメンバーが取締役会にいないケースが多いのではないか

[19] Department for Digital, Culture, Media and Sport 「FTSE 350 Cyber Governance Health Check 2018」に基づき、NTT データ経営研究所にて作成

項目番号	CISO 等への期待や活動実態	経営層への期待や活動実態等の その他の有益な知見
指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定		● サイバーセキュリティのインシデント対応手順は外部による監査をうけるべきだ ● FTS350 のうち 25%の企業しか外部監査を受けていない
指示５		
指示６ サイバーセキュリティ対策における PDCA サイクルの実施	● インシデント対応計画は事業計画に整合しているかを定期的に見直すべきだ ● FTSE350 のうち約半数の企業だけが定期的に見直しを行っている	● インシデント対応計画は収益計画と整合した内容になっていない（過度なリスクテイクまたは過度なリスク回避となっている）のではないか
指示７ インシデント発生時の緊急対応体制の整備	● サイバー攻撃に独立したインシデント対応手順を定義すべきだ ● FTSE350 のうち 45%がサイバー攻撃に独立したインシデント対応手順を定義できていない	● インシデント対応計画に基づくサイバーセキュリティ演習を実施している企業は少ないのではないか ● サイバー攻撃に独立したインシデント対応マニュアルが規定できていないのではないか（危機管理マニュアルの１パーツとして定義するにとどまっているのではないか） ● リスク管理部門やシステム部門が策定したインシデント対応計画は、業務部門と十分に連携が取れておらず、危機時において実効的な内容になっていないのではないか
指示８		
指示９ ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	● 自社と直接契約関係にはないものの、自社サービスのサプライチェーンに関係する事業者に係るサイバーリスクについても認識する必要がある（TSE350 のうち 23%未満しか認識できていない） ● 自社サービスのサプライチェーンに影響する事業者、およびそのリスクについて特定できていない	
指示１０ 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	● サイバーセキュリティへの 10 の対応ステップ等、NCSC 等政府機関の助言を取り入れるべきだ（FTSE350 のうち約 3/4 の企業が取り入れている）	● 外部機関より情報を収集して自社のリスクに結び付け対策を強化する一連の対応を、CSIRT の業務として定義していない会社が多いのではないか

7.1.5. 文献 5：経営とサイバーセキュリティ- デジタルレジリエンシー -[20]

「経営とサイバーセキュリティ–デジタルレジリエンシー–」は、NTT 持株会社でサイバーセキュリティのスポークスパーソンを務める横浜真一氏によって執筆された、サイバーセキュリティに関する経営層向けの経営書である。

本文献では、CISO に対して、「技術よりも企業全体やビジネス全体のリスクを理解していること」、「他の役員との折衝や社内各層に対する情報伝達がスムーズにできること」、「業務停止に関する判断が求められる事態に備え、万一の場合の意思決定プロセスを平時から定めて訓練しておくこと」等の役割が期待されている。また、「業務におけるヒトとシステムの関わりやシステムの構成等を正確に把握している企業は少ない」等のサイバーセキュリティリスクの把握に関する問題点や「インシデント時に経営幹部等へのエスカレーションが遅延することによって、外部への公表が遅れ、レピュテーションを棄損した事案」等の問題が提起されている。一方で、「大手企業がそのノウハウと人材を共同で出し合い、会員企業のサプライチェーンを構成する中堅中小企業向けの研修プログラムを作り、人材育成や研修を提供することを計画する動きがある」等のポジティブな動向も確認することができた。

下表に、①CISO 等への期待や活動実態、②経営層への期待や活動実態等のその他の有益な知見の 2 つの観点から本文献より収集した主な情報（知見）を整理する

[20] 横浜信一氏「経営とサイバーセキュリティ　デジタルレジリエンシー」https://www.nikkeibp.co.jp/atclpubmkt/book/18/265130/

表 7-5　文献 5 から抽出した情報（知見）の整理 [21]

項目番号	CISO 等への期待や活動実態	経営層への期待や活動実態等のその他の有益な知見
指示 1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定		● 取締役会が果たすべき役割は以下のとおり ・ サイバーセキュリティを企業横断のリスクマネジメント課題として理解する ・ サイバーリスクの法的意味合いを企業の状況に応じて理解する ・ セキュリティ専門家（ブレーン）にアクセスできるようにして、定期的に適切な時間を使ってサイバーリスクの管理について議論する必要がある ・ 経営陣に対し「適切な人員と予算を伴った企業横断のサイバーリスク管理の枠組みを持つべきだ」と働き掛ける ・ サイバーセキュリティのどのリスクを避け、許容し、緩和し、保険をかけるかを議論して、それぞれの具体策について議論する ● 取締役会での議論は、「何かが起こってからの対策」ではなく「何を守るべきか」にすべきだ。しかも自社のミッションに呼応する形で日常的に行うべき ● サイバーセキュリティが経営課題である理由は 3 点あると考えている。 ・ 事業継続性が脅かされる為 ・ ステークホルダーからのトラストを守る活動である為 ・ 企業成長の基盤作りである為 ● 諸外国では、企業のサイバーセキュリティへの取組を政府機関が評価し、認証を与える動きがある（認証が得られないと信用力が低下しビジネスに影響を及ぼす） ● 日本語は防御策にならない。攻撃は国境も言語も簡単に超える

[21] 経営とサイバーセキュリティ- デジタルレジリエンシー -に基づき、NTT データ経営研究所にて作成

項目番号	CISO 等への期待や活動実態	経営層への期待や活動実態等のその他の有益な知見
指示２ サイバーセキュリティリスク管理体制の構築	● CISO 本人には、技術よりも企業全体やビジネス全体のリスクを理解していることや、他の役員との折衝や社内各層に対する情報伝達がスムーズにできるコミュニケーション能力が求められる ● サイバーセキュリティ対策においては、CISO 個人の資質よりも、CSIRT チームとしてのケイパビリティが重要 ● 役員の啓発（サイバーセキュリティを議論する「共通の土台作り」）も CSIRT チームが担うべき重要な役割	
指示３ サイバーセキュリティ対策のための資源(予算、人材等)確保	● 自社ビジネスの特性を踏まえ、ビジネスに不可欠な「優先して守るもの」を定義してから、セキュリティ対策に係る資源配分を検討すべきだ	● 単にシステムの構成のみを以ってリスク評価を行っている可能性がないか
指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	● 情報システム、制御システム、委託先、調達先等それぞれに想定されるリスクを洗い出し、発生頻度や影響の大きさを定量評価したうえで、ビジネス観点から対策の優先順位付けを行う ● 優先して防御する対象の優先順位付けは、資産管理の視点からではなく、ビジネスの特徴・競争優位の源とその維持、今後の市場の動きなど経営的な視点から実施すべきだ	● 業務におけるヒトとシステムの関わりやシステムの構成等を正確に把握している企業は少ないのではないか
指示５ サイバーセキュリティリスクに対応するための仕組みの構築		● 発せられたアラートをヒトが無視してしまうような、技術的対策は機能しても人的要因により効果を発揮しないケースもある ● 開発段階を含め、データベースへのアクセス制限・アクセス管理は徹底する必要がある ● 新たなデバイスの登場がアクセス制限の抜け穴となるケースも想定されるため、技術的対処は絶えずにアップデートが必要
指示６ サイバーセキュリティ対策における PDCA サイクルの実施		● PDCA サイクルに代わって有効なのが、「戦略→実装→訓練→評価」のサイクルである。 ● PDCA サイクルはサイバーセキュリティにおいては当てはまりにくい。能動的な「Do」に該当するものが存在しないため

項目番号	CISO 等への期待や活動実態	経営層への期待や活動実態等のその他の有益な知見
指示７ インシデント発生時の緊急対応体制の整備	● 業務停止に関する判断が求められる事態に備え、万一の場合の意思決定プロセスを平時から定めて訓練しておく ● 攻撃事態は直接に事業継続性を脅かすものでなくても、攻撃を検知した後の対処や復旧を考えるうえで、事業運営への影響、場合によっては一時的な業務停止を決める必要	● インシデント時に経営幹部等へのエスカレーションが遅延することで、外部への公表が遅れ、レピュテーションを棄損した事案あり
指示８		
指示９ ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	● 業務委託先やシステム開発（運用）委託先のサイバーセキュリティレベルを管理・監督する必要がある	● NIST サイバーセキュリティフレームワークに対してのパブリックコメント（意見書）のうちサプライチェーンに関する内容 • 自社として何を守るのかという問いの一部として考える • 契約関係の有無とは関係なく、他社と何らかの相互依存関係があればサプライチェーンとして考える • 共通の用語を使うことが大切
指示１０ 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供		● 大手企業がそのノウハウと人材を共同で出し合って、会員企業のサプライチェーンを構成する中堅中小企業向けの研修プログラムを作り、人材育成や研修を提供することを計画する動きもある

7.1.6. 文献 6：LEVERAGING BOARD GOVERNANCE FOR CYBERSECURITY[22]

「LEVERAGING BOARD GOVERNANCE FOR CYBERSECURITY」は、米国の非営利団体 Advanced Cyber Security Center (ACSC)が、2019 年 1 月に、機密データの流出や企業の市場価値の失墜等の企業へ悪影響を与える、昨今の高度化されたサイバー攻撃の登場を受けて、サイバーセキュリティガバナンスにおける取締役会の役割に関するベンチマークを構築する目的で作成した文書である。ACSC メンバーの CISO や CIO 合わせて 20 人へのインタビューやオンライン調査を元に作成されている。

本文献では、CISO に対して、「自社のサイバーセキュリティ対策について、取締役会の信頼を構築する」、「取締役会の理解・専門知識のレベル向上を図るため、継続的なトレーニングの機会を提供する」、「サイバーセキュリティへの投資をデジタル戦略投資の一環としてとらえた上で適正な予算配分が図られるよう、社内関係者に働きかける」等の役割が期待されている。また、「サイバーセキュリティやテクノロジーに関する技術的な知識・ノウハウを有する役員の登用が進んでいない」、「取締役会は、CIO や CISO その他リスク管理を所管する経営幹部と距離がある」、「サイバーセキュリティを担当する部署が孤立し、関連部署と連携・協力を取り合う会議体や風土が不足している」等の、サイバーセキュリティリスクの認識や組織全体の対応に関する問題点や、「サイバーセキュリティ関係の予算が増えていることが、経営上の課題となっている」、「サイバーセキュリティ関係の予算が、IT 関連の予算として計上されていない」等の予算に関する問題点が提起されている。

下表に、①CISO 等への期待や活動実態、②経営層への期待や活動実態等のその他の有益な知見の 2 つの観点から本文献より収集した主な情報（知見）を整理する。

[22] Advanced Cyber Security Center 「LEVERAGING BOARD GOVERNANCE FOR CYBERSECURITY」 https://www.acscenter.org/blog/why-the-ciso/ciso-perspective-should-matter-to-corporate-boards/

表 7-6　文献 6 から抽出した情報（知見）の整理 [23]

項目番号	CISO 等への期待や活動実態	経営層への期待や活動実態等のその他の有益な知見
指示 1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定	● テクノロジーやサイバーセキュリティに関するテーマを取締役会に付議し、経営陣の理解を向上させる ● 自社のサイバーセキュリティ対策について、取締役会の信頼を構築する役割を担う ● 取締役会でサイバーセキュリティに関する議論が活発化するように、テーマ設定や付議内容を工夫する ● デジタル戦略やサイバーセキュリティに関する取締役会の理解・専門知識のレベル向上を図るため、継続的なトレーニングの機会を提供する ● テクノロジーやサイバーセキュリティに関するテーマをリスク委員会や監査委員会に付議する回数が少ない ● 経営陣と直接コミュニケーションをとる機会が少ない	● テクノロジーやサイバーセキュリティに関するテーマを取締役会に付議できていない ● サイバーセキュリティやテクノロジーに関する技術的な知識・ノウハウを有する役員の登用が進んでいないのではないか ● 取締役会は、CIO や CISO その他リスク管理を所管する経営幹部と距離があるのではないか ● サイバーセキュリティを担当する部署が孤立し、関連部署と連携・協力を取り合う会議体や風土が不足しているのではないか ● 取締役会のテーマとしてサイバーセキュリティが取り上げられることは、極めて稀なのではないか
指示 2 サイバーセキュリティリスク管理体制の構築	● CISO と CIO は、デジタル戦略とセキュリティに関する総合的な見解を示すために、取締役会に共同で出席すべきだ	● CIO と共同してデジタル戦略とセキュリティに関する統合的な戦略を立案し、取締役会に付議するような機会は少ない ● サイバーセキュリティをデジタル戦略の一環としてとらえる風土が醸成されていないのではないか
指示 3 サイバーセキュリティ対策のための資源(予算、人材等)確保	● サイバーセキュリティへの投資をデジタル戦略投資の一環としてとらえた上で適正な予算配分が図られるよう、社内関係者に働きかける ● サイバーセキュリティをデジタル戦略と分離して捉えて、予算の策定・執行を行えていない	● サイバーセキュリティ関係の予算が増えていることが、経営上の課題となっているのではないか ● サイバーセキュリティ関係の予算が、IT 関連の予算として計上されていないのではないか ● IT 戦略に関する予算を検討する過程において、サイバーセキュリティ関係の予算が議論の俎上に上がらないのではないか ● サイバーセキュリティをデジタルトランスフォーメーション戦略の一要素としてとらえる必要があるのではないか

[23] Advanced Cyber Security Center「LEVERAGING BOARD GOVERNANCE FOR CYBERSECURITY」に基づき、NTT データ経営研究所にて作成

項目番号	CISO 等への期待や活動実態	経営層への期待や活動実態等のその他の有益な知見
指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	● NIST 等の内外の関係機関が公表する情報を参考に、サイバーリスクの特定・評価・コントロールを行う手法を研究・試行錯誤すべきである	● サイバーリスクの特定・評価・コントロールに際し、いくつかの運用上の指標は確認しているものの、それらを複合的・総合的に勘案し、分析できるようなフレームを有していない
指示５		
指示６		
指示７		
指示８		
指示９ ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	● NIST 等内外の関係機関が公表する情報等から、サイバーリスク評価のためのフレームワーク構築に有用な情報を収集する	● 平時における情報収集に資源を投入できていないのではないか ● NIST 等海外を含む先進的な取組の事例を収集できていないのではないか
指示１０		

7.1.7. 文献 7：NAVIGATING THE DIGITAL AGE[24]

「NAVIGATING THE DIGITAL AGE」は、米国のサイバーセキュリティ民間企業 Palo Alto Networks が、デジタル時代における事業運営、特にサイバーセキュリティ関連する問題について、ビジネス、科学、技術、政治、学術、サイバーセキュリティ、法律の分野から総勢 50 人以上の有識者の寄稿を元に作成した文書である。サイバーセキュリティを取り巻く問題の中でも、特に、技術分野と非技術分野の役員の相互理解に焦点を当てられており、将来的な脅威とリスク、現状から得られる教訓、現状の対応に関する評価・問題点について各有識者の知見が集約されている。

本文献では、CISO に対して、「経営陣にサイバーセキュリティの重要性を理解させること」、「セールス部門からの信頼を構築すること」、「社内で、セイバーセキュリティーに関する活動をまとめた報告会や資料を作成し、セキュリティについての理解度や認知度を向上させること」等の役割が期待されている。また、「CISO は、社内外で発生しているサイバー攻撃事案に関する情報収集と、自社へ波及する影響についての分析をおろそかにしている」、「投資は技術的な対応に偏重しがちであり、教育等ヒトへの投資が進んでいないのではない」、「サイバーセキュリティ対策において、技術的な対処以上に、従業員一人一人の意識向上が肝要である」等の問題点が提起されている。一方で、「経営陣はサイバーセキュリティ対策に予算を確保する必要性について理解が進んできている」等のポジティブな動向も確認することができた。

下表に、①CISO 等への期待や活動実態、②経営層への期待や活動実態等のその他の有益な知見の 2 つの観点から本文献より収集した主な情報（知見）を整理する。

[24] Palo Alto Networks「Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers Second Edition」 https://www.securityroundtable.org/navigating-the-digital-age-2nd-edition/

表 7-7 文献 7 から抽出した情報（知見）の整理 [25]

項目番号	CISO 等への期待や活動実態	経営層への期待や活動実態等のその他の有益な知見
指示 サイバーセキュリティリスクの認識、組織全体での対応方針の策定	● 取締役会の役割（主にポリシー順守の監督）を定義する ● 経営陣にサイバーセキュリティの重要性を理解させる（会社の重要なデータにアクセスできる経営自身が攻撃のターゲットの対象になることもある） ● 最悪の事態に備えるために、危機管理、インシデント対応訓練、サイバーインシデントのシミュレーションは、取締役会を含めた全レベルで実施する必要がある	● 取締役会のメンバー自身がサイバーセキュリティポリシーを制定する必要はないが、どのようなポリシーが施行されているか、施行されたポリシーはきちんと監視されているか、どのように執行されているかについては把握していなければならない ● 経営陣のサイバーセキュリティへの理解度が低い。また、取締役会の役割が不明瞭である
指示２ サイバーセキュリティリスク管理体制の構築	● ビジネスを実現する権限を与えられた CISO は、ビジネスを理解し、ビジネスの基本的な活動と価値に精通していなければならない ● サイバーセキュリティ分野の基本タスクであるセキュリティ対策機器の管理、脆弱性スキャン、パッチ管理、アプリケーションのセキュリティ管理などは全て完璧にこなす必要がある ● リスクマネジメントについて語ることができるだけでなく、組織のためにリスクマネジメントとは何かを定義し、明確に表現できる必要がある ● 進歩するテクノロジーの行く先について予測と準備をする必要がある ● CISO は、組織のすべての側面をよく理解しておく必要がある ● CISO は、セールス部門からの信頼を構築しておく必要がある。それによって、インシデント発生時に、セールス部門が対峙する顧客に安心感を付与し、顧客流出を防止できる ● CISO には、技術部門と非技術部門を結束させ、協力関係を築いてチームプレイを実現するためのより高いビジネススキル、そしてより高いコミュニケーションスキルが必要である	● ビジネスを理解し、他部門と関係性を構築できている CISO は少ない ● CISO は、サイバーセキュリティに関する技術的な知見を備えてはいるが、その脅威がビジネス部門へ及ぼす影響に関して、専門用語を使用することなく、わかりやすく説明する努力を怠っているのではないか

[25] Palo Alto Networks「Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers Second Edition」に基づき、NTT データ経営研究所にて作成

項目番号	CISO 等への期待や活動実態	経営層への期待や活動実態等のその他の有益な知見
	● ビジネスを理解し、他部門と関係性を構築できている CISO は少ない	
指示３ サイバーセキュリティ対策のための資源(予算、人材等)確保	● CISO はセキュリティという領域から少し離れ、組織全体にどのような価値を与えられるかという観点（以下の４項目を中心に）でものを考える必要がある。 ・ どうすればサイバーセキュリティが収益の創出、保護、確保に役立つか ・ どうすればサイバーセキュリティが既存客の維持に役立つか ・ どうすればサイバーセキュリティが競合との差別化に役立つか ・ どうすればサイバーセキュリティが業務の効率と有効性を引き上げられるか ● サイバーセキュリティ予算はその全額を防御に充てるのではなく、侵入に成功した攻撃の識別（発見）と事後対応（レスポンス機能）に充てるべきである。また、テクノロジーに投資するだけではなく、従業員の教育・啓発活動（攻撃者の攻撃活動がどのようなものか等）にも予算を投入するべきである ● 「引きこもりがちでコミュニケーション下手」というセキュリティ部門と他のビジネス部門（営業、マーケティング、開発等）から賛同や支援を得られるような部門に進化させるのが難しい現状にある	● サイバーセキュリティ予算はその全額を防御に充てるのではなく、侵入に成功した攻撃の識別（発見）と事後対応（レスポンス機能）に充てるべきである。また、テクノロジーに投資するだけではなく、従業員の教育・啓発活動（攻撃者の攻撃活動がどのようなものか等）にも予算を投入するべきである ● 経営陣は、サイバーセキュリティに関する十分な予算を確保することの大切さを理解はしているが、その予算の使い方に関しては、攻撃の防御や検知、検知後の対応について、適切な予算配分を実施していないのではないか ● 経営陣は、予算の配分について、技術的投資に偏重しがちで、従業員教育や人材育成の分野に関しては、ないがしろにしているのではないか
指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	● CISO は、取締役会が進捗とサイバーセキュリティ対策の効果を把握できるようにするための、それを表現するための測定方法を開発する必要がある ● 侵害通知書の記載項目に回答できるような、インシデント対応計画を構築することが望ましい（技術的な問題だけではなく、リーダーシップや社内のコミュニケーションについても記載が必要）	● サイバーセキュリティの効果を定量化する手法は確立されていない
指示５ サイバーセキュリティ	● 対応力、テクノロジー、インフラ、物理空間をめぐる問題の対	● 経営陣は、サイバーセキュリティに対処できる技術的な専門家

項目番号	CISO 等への期待や活動実態	経営層への期待や活動実態等のその他の有益な知見
リスクに対応するための仕組みの構築	処計画を立てる（インシデントに対する対応力の有無や、そのためのテクノロジーの調達、インフラの修復やクリーンアップの可否、追加装置を設置する物理空間の有無等の確認が必要） ● DDoS 攻撃とランサムウェア攻撃への対策プランを必ず用意しておく必要がある	を、経営メンバーに加えていない ● サイバーセキュリティツール以前に、社内のサイバー衛生環境が整っていない ● インシデント発生時の対処計画を、既存の対応力、テクノロジーやインフラ、物理空間を考慮した上で、立案する必要がある ● 経営陣は、インシデントが発生した場合の対処計画の立案時に、社内に有する技術やシステムインフラやネットワークインフラを十分に考慮していないのではないか ● 経営陣は、サイバー攻撃により社内の各種資源が汚染された場合を想定していないのではないか
指示６		
指示７ インシデント発生時の緊急対応体制の整備	● 侵害通知書を事前に準備しておく ● 攻撃者による攻撃を探知した際に、すぐに被害を最小限にするように対応するべきではない。落ち着いて状況を把握し、しばらく攻撃者を泳がせ、攻撃者の行動や使用ツールを観測することによって、攻撃者のバックドア（ネットワークへアクセスするための入り口）を探知できる可能性や攻撃者を特定できる ● 平時のうちに特別委員会を設置しておくべきである。この委員会には明確に定義された意思決定手順を持たせ、有事の際にはただちに招集できるようにしておく必要がある	● 事前に通知書を準備することによって、実際に記入する際に直面する問題（記載項目等）を解決・整理することが可能 ● インシデントが発生した際に、連絡を取りあうセキュリティオペレーションセンターとの関係性の構築が重要 ● 経営陣は、インシデント発生時にコミュニケーションをとるべき関連部門との関係性や使用する各種ドキュメントの整備をおろそかにしているのではないか ● インシデント発生時に、スムーズに対応できる企業が少ない
指示８ インシデントによる被害に備えた復旧体制の整備	● 攻撃が見つかった場合に社内の誰が何をすればよいのかを明確にしておく必要がある（接続遮断の決定権をだれがもつのか、メディアや当局等へだれが情報展開をするのか等） ● インシデント発生時は、CISO が直接取締役会に報告を行うとともに、意思決定を行う必要がある	● インシデント発生時の対応手順が整備されていない ● インシデント発生時の社内対応プロセスを事前に準備しておく必要がある ● 経営陣は、インシデント発生時に社内各部門がとるべき行動基準を定めていないのではないか
指示９		
指示１０ 情報共有活動への参加を通じた攻	● 社内で、サイバーセキュリティに関する活動をまとめた報告会や資料を作成し、セキュリティ	● 新しく登場する攻撃に対して、十分にキャッチアップと情報のアップデートができていない

項目番号	CISO 等への期待や活動実態	経営層への期待や活動実態等のその他の有益な知見
撃情報の入手とその有効活用及び提供	についての理解度や認知度を向上させる ● 注目度や関連性の高いインシデントを調査し、それらが自組織の状況にどのように当てはまるかを理解しておく必要がある	● 日頃より、自社業務に関連性が高い、または、世間で話題になっているインシデントを調査・把握し、防止策等について検討を行う必要がある ● 経営陣は、社内外で発生しているサイバー攻撃事案に関する情報収集と自社へ波及する影響についての分析をおろそかにしているのではないか

7.1.8. 文献 8：Top CISO Trends[26]

「Top CISO Trends」は、米国のサイバーセキュリティ民間企業 K logix が、昨今のサイバーセキュリティのトレンドとサイバーセキュリティ業界の行く末を理解するために、CISO やセキュリティの専門家総勢 16 人に対して実施したインタビューを元に、2019 年 3 月に作成した文書である。有識者に、CISO の職務に効果的な特徴・能力や情報セキュリティの目標、その目標を妨げる課題等をインタビューし、その結果が取りまとめられている。

本文献では、米国の事例ではあるが、CISO に対して、「プライバシーやセキュリティに関する法規制の動向を把握すること」、「CISO にはセキュリティプログラムなど技術的な内容についても、内容を咀嚼して、その概観を的確に伝えるような「コミュニケーション力」が要請される」等の役割が期待されている。また、「CISO の業務成績のベンチマークが明確になっていない」、「CISO は、技術的な知識は豊富であるものの、ビジネスに精通していない」等の問題点が提起されている。一方で、「セキュリティ人材を安定的に育成・供給する仕組みの構築に取組み始めた企業がある」等のポジティブな動向も確認することができた。

下表に、①CISO 等への期待や活動実態、②経営層への期待や活動実態等のその他の有益な知見の 2 つの観点から本文献より収集した主な情報（知見）を整理する。

[26] K LOGIX「Top CISO trends」https://www.klogixsecurity.com/blog/top-ciso-trends

表 7-8　文献 8 から抽出した情報（知見）の整理 [27]

項目番号	CISO 等への期待や活動実態	経営層への期待や活動実態等のその他の有益な知見
指示 1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定	● CISO は自身の業務成績のベンチマークが明確になっていないのではないか（リスクをどれだけ減らしたかは実際にはわからない	● 良くも悪くも、経営層は主に重大な事件の発生の有無で CISO の業績を判断する
指示 2 サイバーセキュリティリスク管理体制の構築	● 自身の業務遂行において、必要に応じて取締役会へアクセスできるルートを確保する ● CISO としての自身の認知度および CISO の業務内容について、役員の認知を向上させる ● サイバーセキュリティ対策において強力なリーダーシップを発揮する ● ビジネスに精通し、調整役であることを自覚する ● プライバシーやセキュリティに関する法規制の動向を把握する ● CISO の役割は、知的財産、機密データ、およびビジネスの評判を保護すること。また、CISO がもっとビジネスの洞察力を持つことへの期待が高まっている ● 取締役会との距離が遠く、役員からの認知を得ていない ● 技術的な知識は豊富であるも、ビジネスに精通していない	● CISO は技術的な知識・バックグラウンドとビジネス全般への精通の両面が求められるのではないか ● CISO はセキュリティプログラムなど技術的な内容についても、内容を咀嚼して、その概観を的確に伝えるような「コミュニケーション力」が要請されるのではないか
指示 3 サイバーセキュリティ対策のための資源(予算、人材等)確保	● セキュリティ人材を安定的に育成・供給する仕組みを構築する	
指示 4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	● CISO はセキュリティベンダから同じような提案を多数受けている	● セキュリティベンダが提供する各種サービスについて、自社が真に必要とするものを峻別・判断する視点や知識が不足しているのではないか ● 数多くのセキュリティベンダのうち、どのベンダの経験が豊富で信頼できるか、判断に迷っているのではないか ● AI 等を活用したデータ主導型（ヒートマップや定性的な評価ではない）のリスク分析の手法について、関心が高まっているのでないか

[27] K LOGIX「Top CISO trends」に基づき、NTT データ経営研究所にて作成

項目番号	CISO 等への期待や活動実態	経営層への期待や活動実態等のその他の有益な知見
		● サイバーセキュリティに関して、防御からレジリエンス対策の重点が移ってきているのではないか ● 内部犯行への対策が進んできているのではないか
指示５ サイバーセキュリティリスクに対応するための仕組みの構築	● サイバーセキュリティに関する従業員教育・注意喚起についての仕組みの構築	● 基礎的なテーマであるが、CISO は ID 権限の付与やアクセス管理の方法についての関心が高い
指示６		
指示７		
指示８		
指示９ ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握		● IOT への脅威やサプライチェーンセキュリティに関する関心は年々高まってきているのではないか ● その一方で、アクセス制限や ID 管理等に関する従来のサイバーセキュリティのベストプラクティスを実装するのが困難である等、対応に苦慮しているケースが多いのではないか
指示１０ 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	● CISO は、自身の職務を超えて、セキュリティコミュニティに貢献することが求められる	● 同業他社等とセキュリティコミュニティの構築に取組み始めた企業があるのではないか

7.2. アンケート調査の結果

アンケート調査の設問及び単純集計結果を以下に記載する[28]。

7.2.1. 回答企業の属性情報

Q1.　総従業員数（有給役員,正従業員・正職員,準従業員・準職員,アルバイト等を含む）についてお聞きします。直近の会計年度の人数として、当てはまるものを 1 つお選びください。（単一選択）

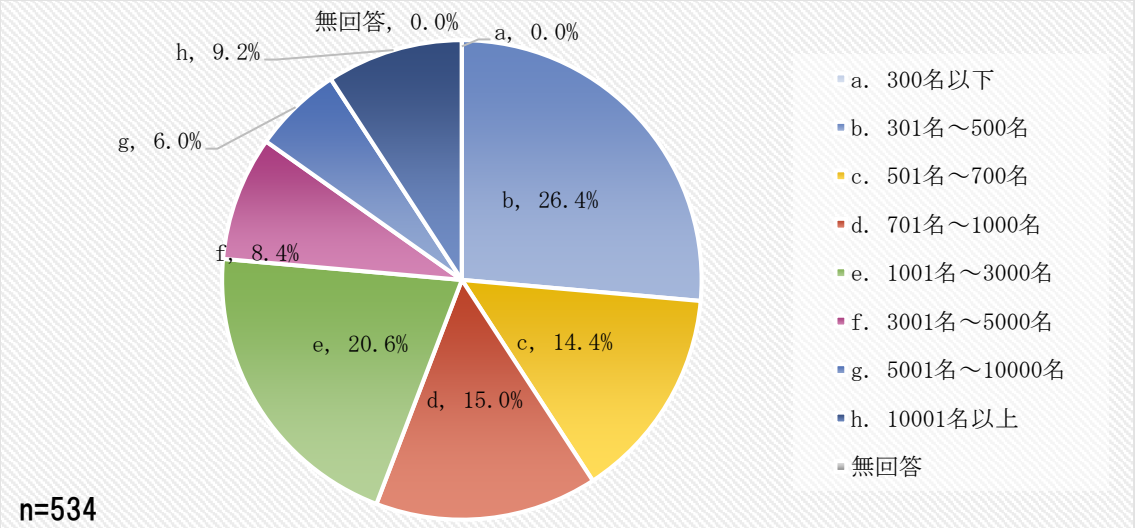

図 7-1　総従業員数

[28] 構成比は小数点以下第 2 位を四捨五入しているため、合計しても必ずしも 100 とはならないグラフが存在する。

Q2.　組織全体の情報セキュリティ対策を統括する CISO（Chief Information Security Officer，最高情報セキュリティ責任者）または同等の責任者（以下「CISO 等」という）を任命していますか。当てはまるものを 1 つお選びください。（単一選択）

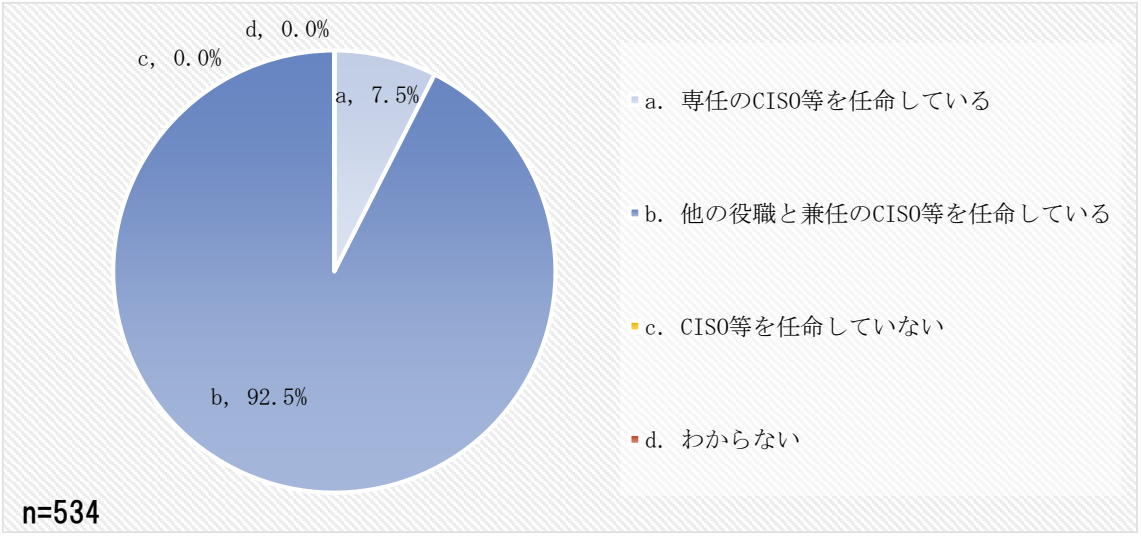

図 7-2　CISO 等の任命状況

Q3.　ご回答いただいている方ご自身の役職または立場として最も近いものを 1 つお選びください。（単一選択）

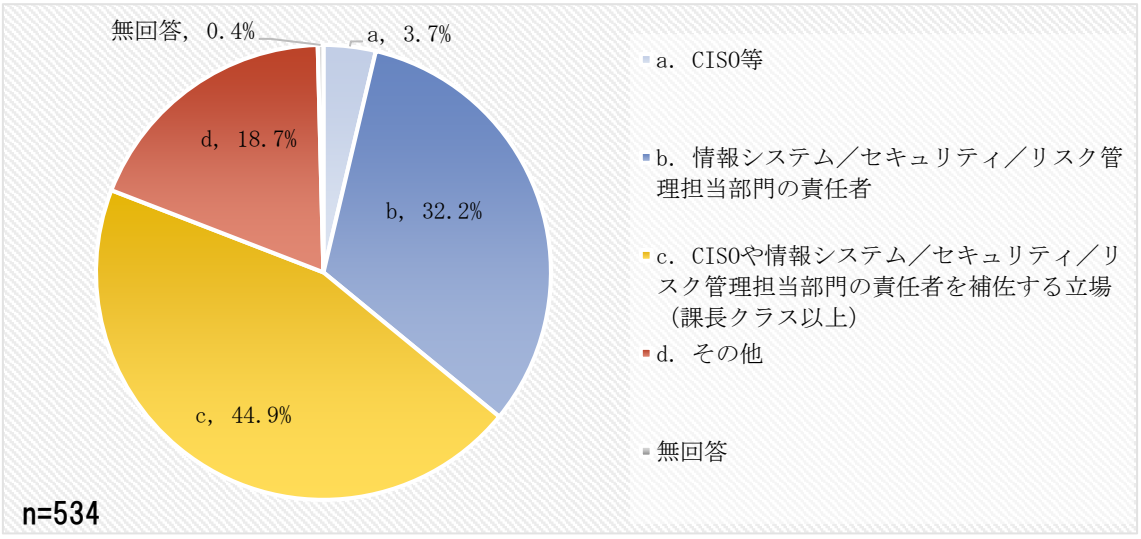

図 7-3　回答者の役職

Q4.　貴社の業種*を 1 つお選びください。（単一選択）*日本標準産業分類に基づく

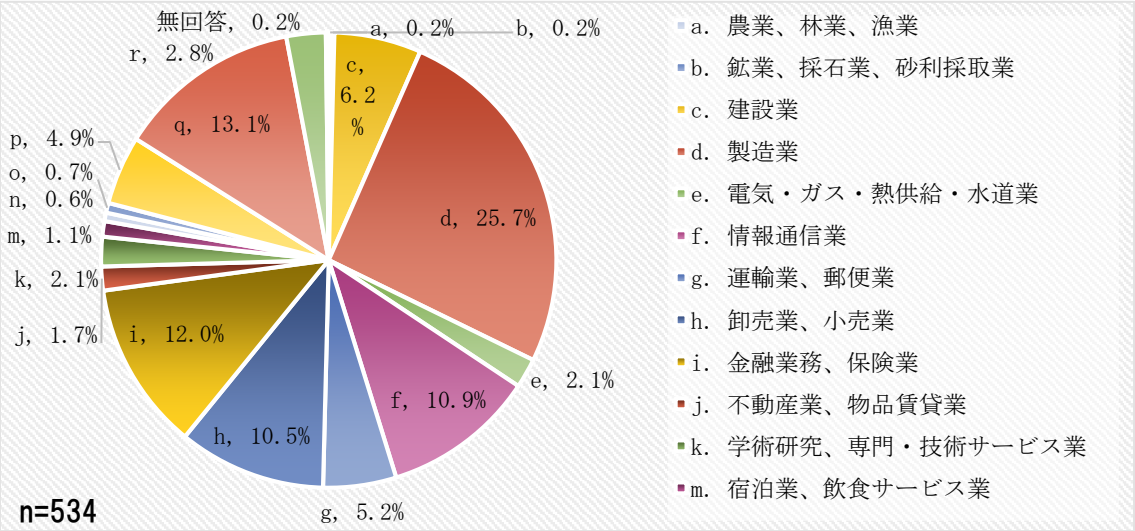

図 7-4　業種

Q5.　直近の会計年度の総売上高を 1 つお選びください。（単一選択）

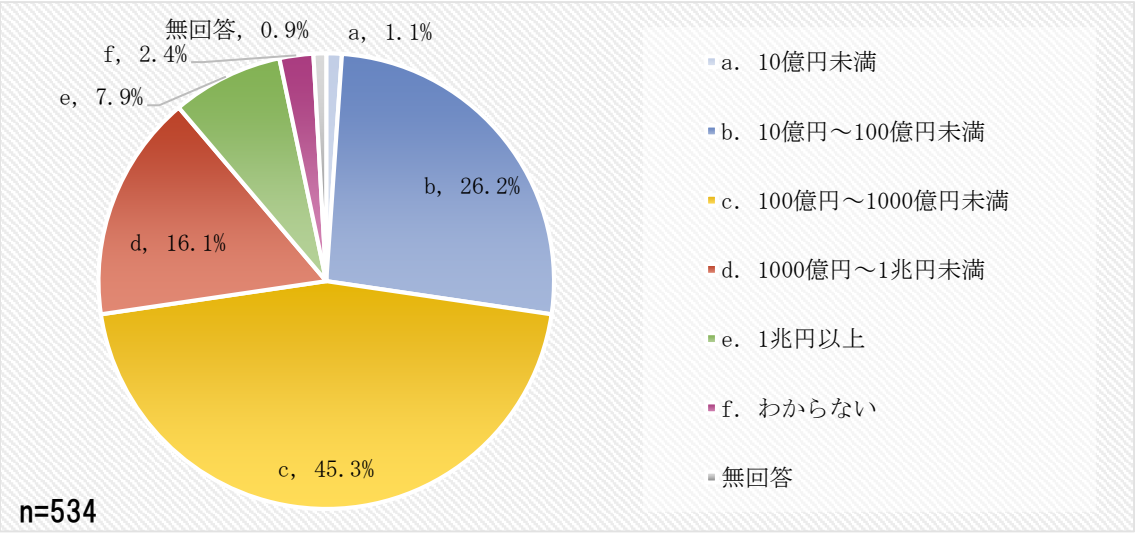

図 7-5　総売上高

7.2.2. IT 依存度

Q6.　事業の IT システム・IT サービスへの依存度について、最も近いものを 1 つお選びください。（単一選択）

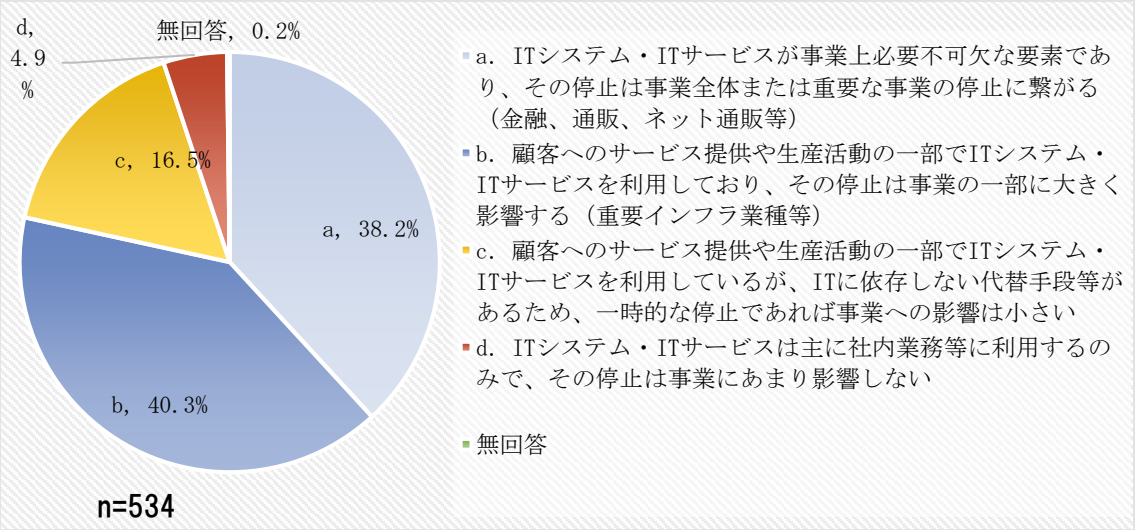

図 7-6　IT 依存度

7.2.3. セキュリティに関する課題認識

Q7. セキュリティ対策を推進する上で、特に課題と感じておられることを 3 つまでお選びください。(3 つまで複数選択可)

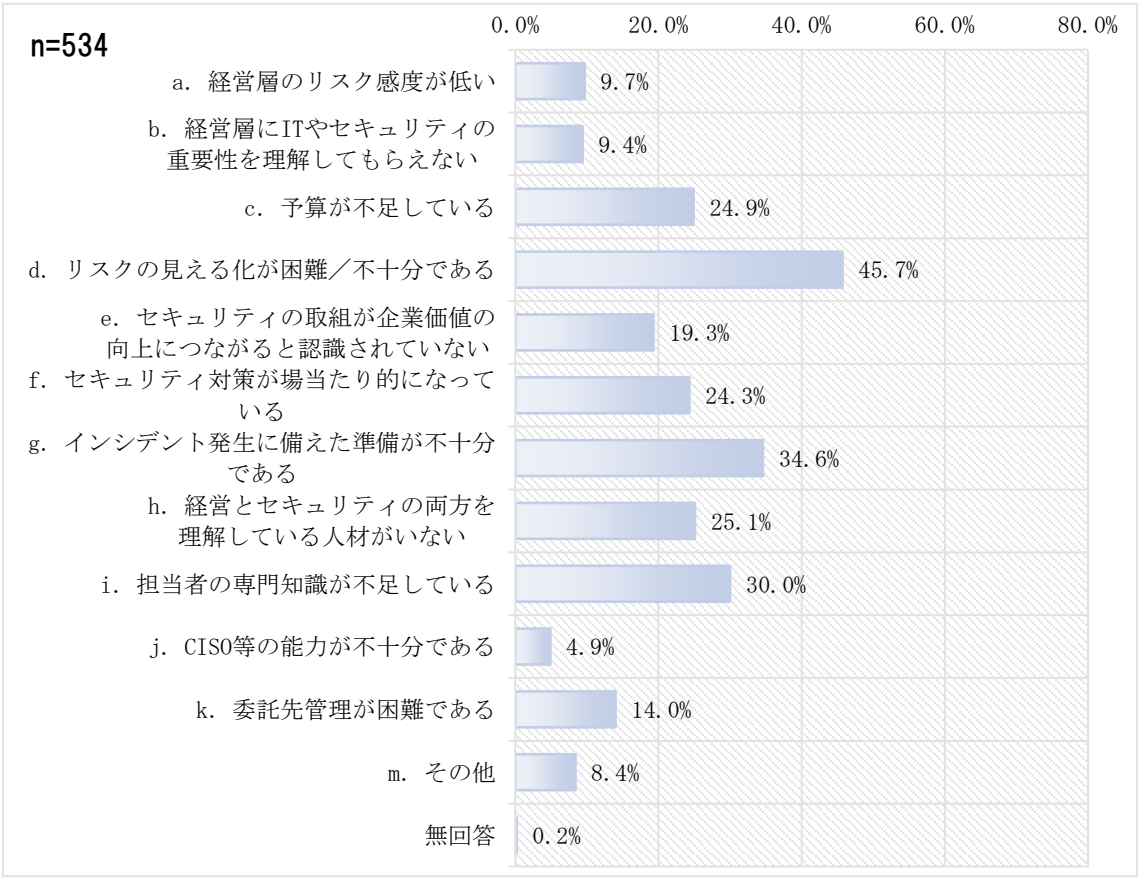

図 7-7 課題認識

7.2.4. セキュリティリスクの事業リスク評価への活用

Q8.　セキュリティリスク（情報漏えい、サイバー攻撃によるシステム停止等）の分析結果を経営層の事業リスク評価に役立てていますか。当てはまるものをそれぞれ１つずつお選びください。（単一選択）

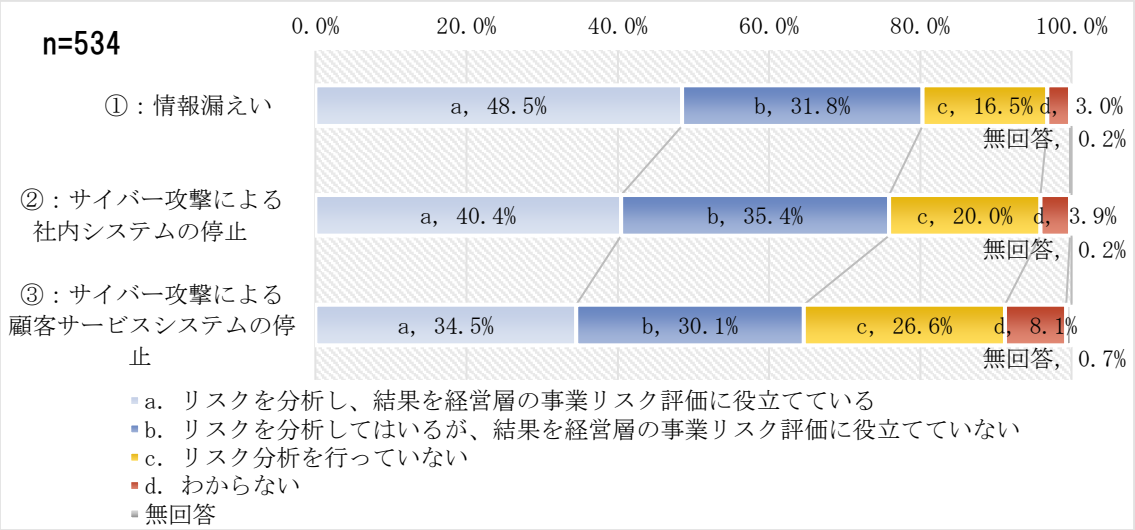

図 7-8　セキュリティリスクの事業リスク評価への活用

7.2.5. セキュリティに関する会議体

Q9.　経営層が参加する会議等のうち、セキュリティリスクの評価、インシデントへの対応方針、投資計画等のサイバーセキュリティの全社的な戦略・方針について、最もよく議論しているものを１つお選びください。（単一選択）

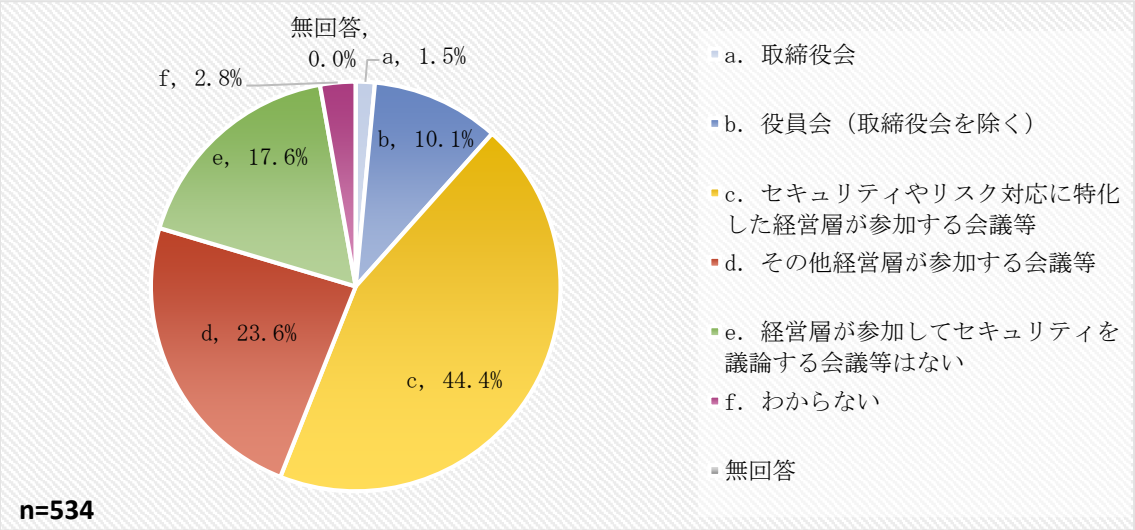

図 7-9　セキュリティに関する会議体（概要）

Q10　前問で回答いただいた会議の運営について、当てはまるものをそれぞれ 1 つずつお選びください。（単一選択）

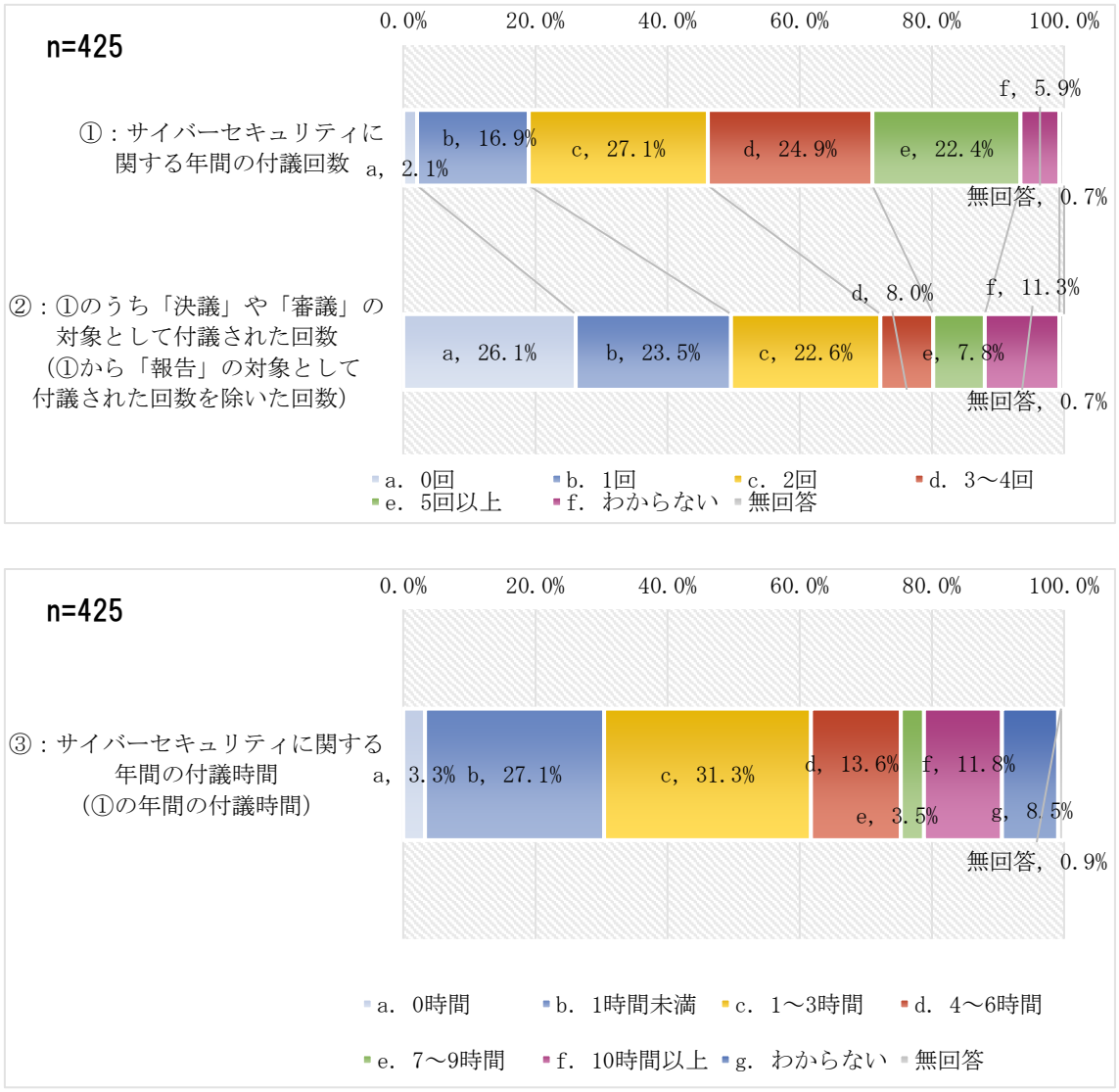

図 7-10　セキュリティに関する会議体（運営）

Q11.　Q9 で回答いただいた会議で実際に取り上げられた議題を全てお選びください。(複数選択可)

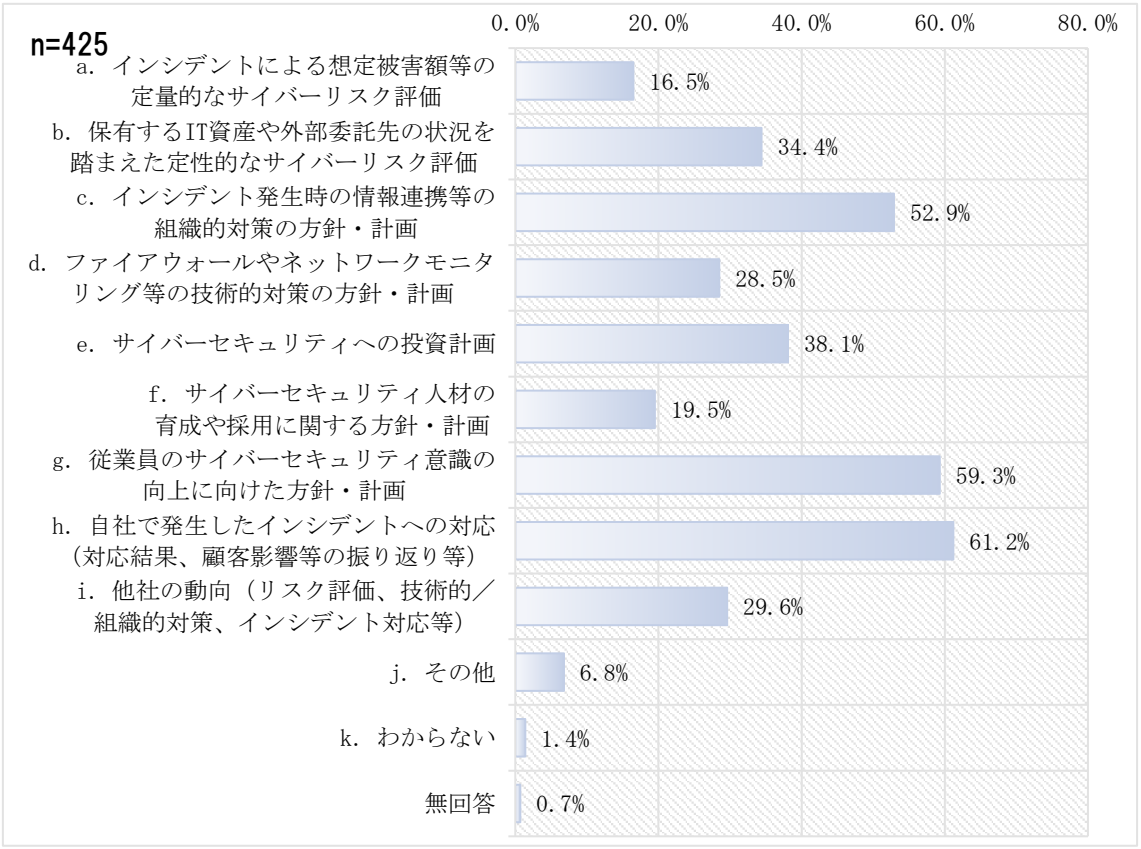

図 7-11　セキュリティに関する会議体（議題）

Q12.　経営層がサイバーセキュリティに関する意思決定を行うにあたり、今後、報告を受ける必要があると考えられる内容について、当てはまるものを全てお選びください。（複数選択可）

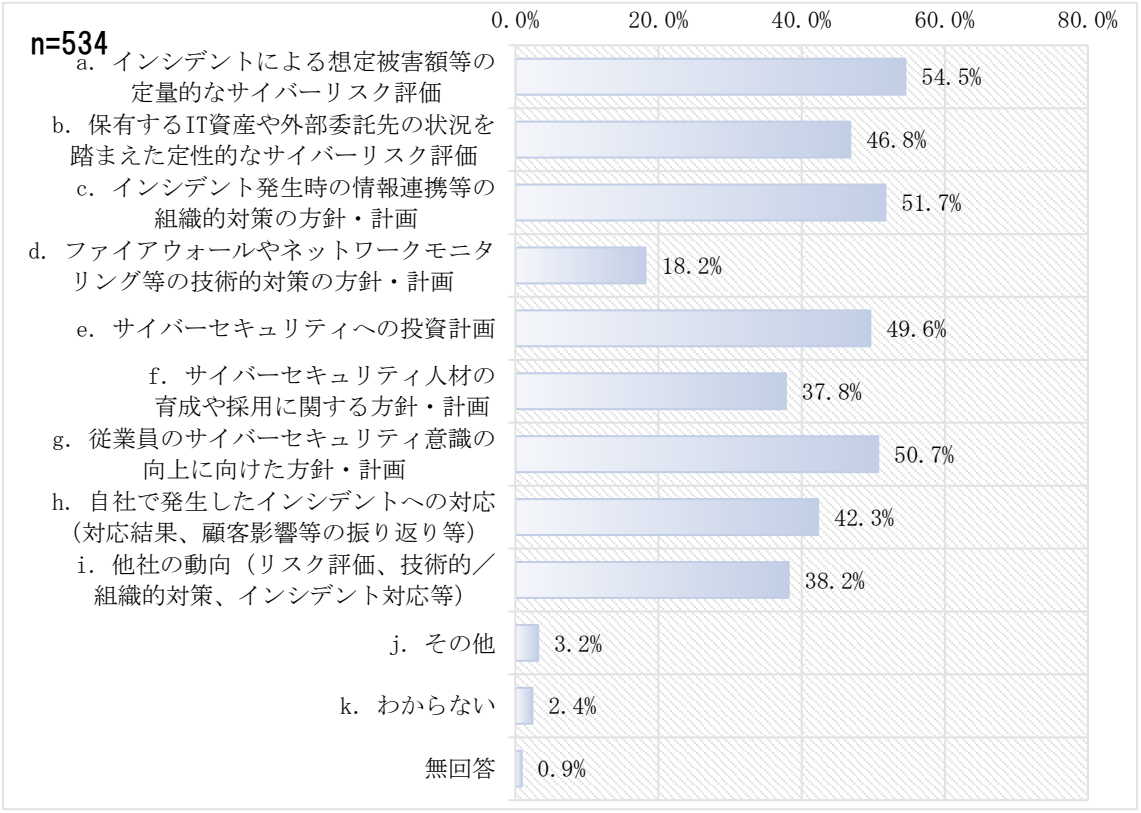

図 7-12　セキュリティに関する会議体（議題）経営層が今後報告を受けるべき内容

7.2.6. 経営層が重視する情報

Q13.　経営層がサイバーセキュリティに関する意思決定を行うにあたり重視する情報を3つまでお選びください。(3つまで複数選択可)

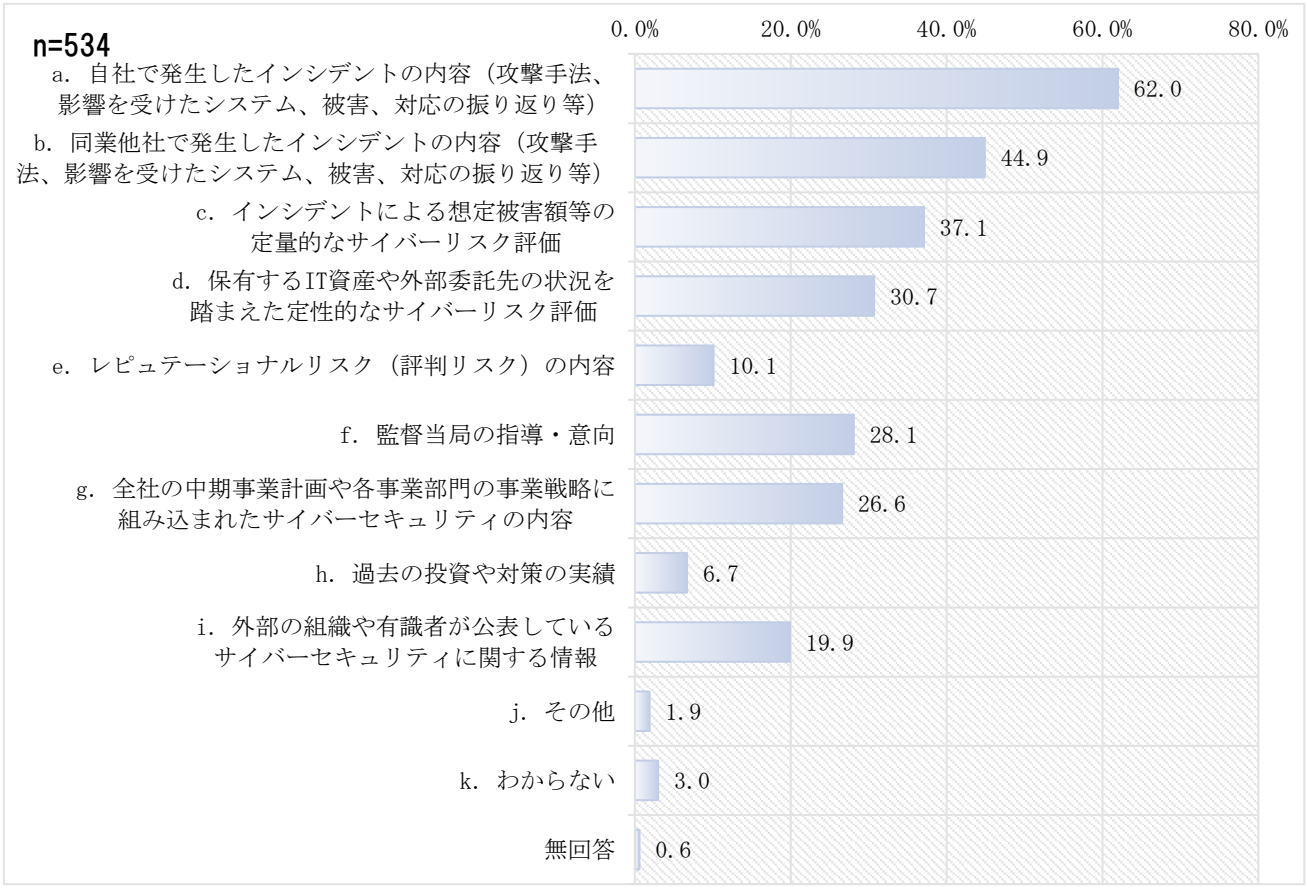

図 7-13　経営層が重視する情報

7.2.7. CISO 等に求める経営・事業的役割

Q14.　経営層が CISO 等に求める役割として重視しているのは、「技術的役割*」と「経営・事業的役割**」のどちらですか。当てはまるものを 1 つお選びください。（単一選択）

*技術的役割：システムやネットワーク構成を踏まえた対策の立案・実施、脆弱性診断やログの監視体制の構築等

**経営・事業的役割：サイバーセキュリティ目標・予算の策定や、事業リスク評価、経営層との橋渡し等

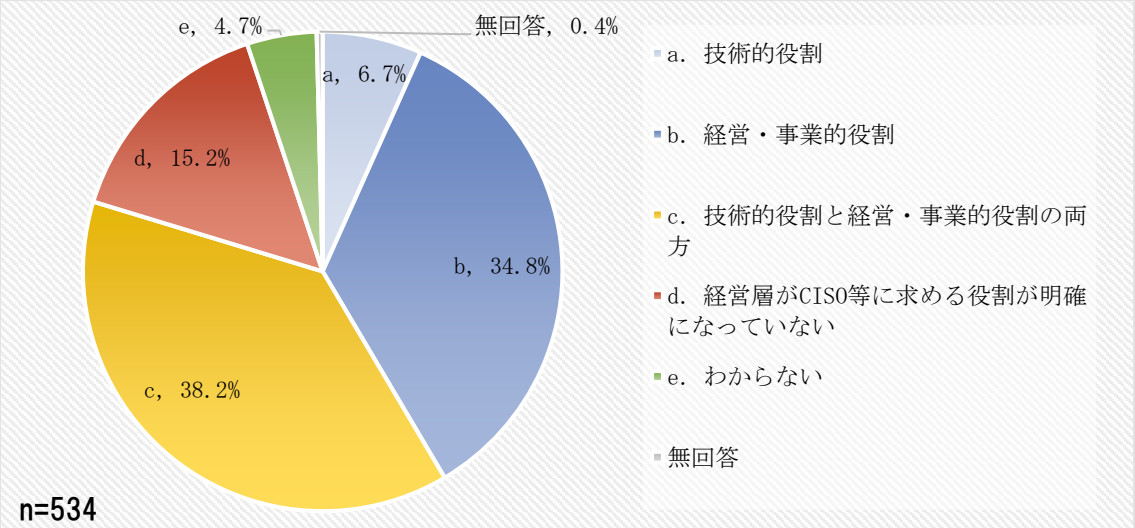

図 7-14　CISO 等に求める役割

Q15.　前問で「b,c」と回答いただいた方にお伺いします。経営層が「経営・事業的役割」を重視する理由を 3 つまでお選びください。(3 つまで複数選択可)

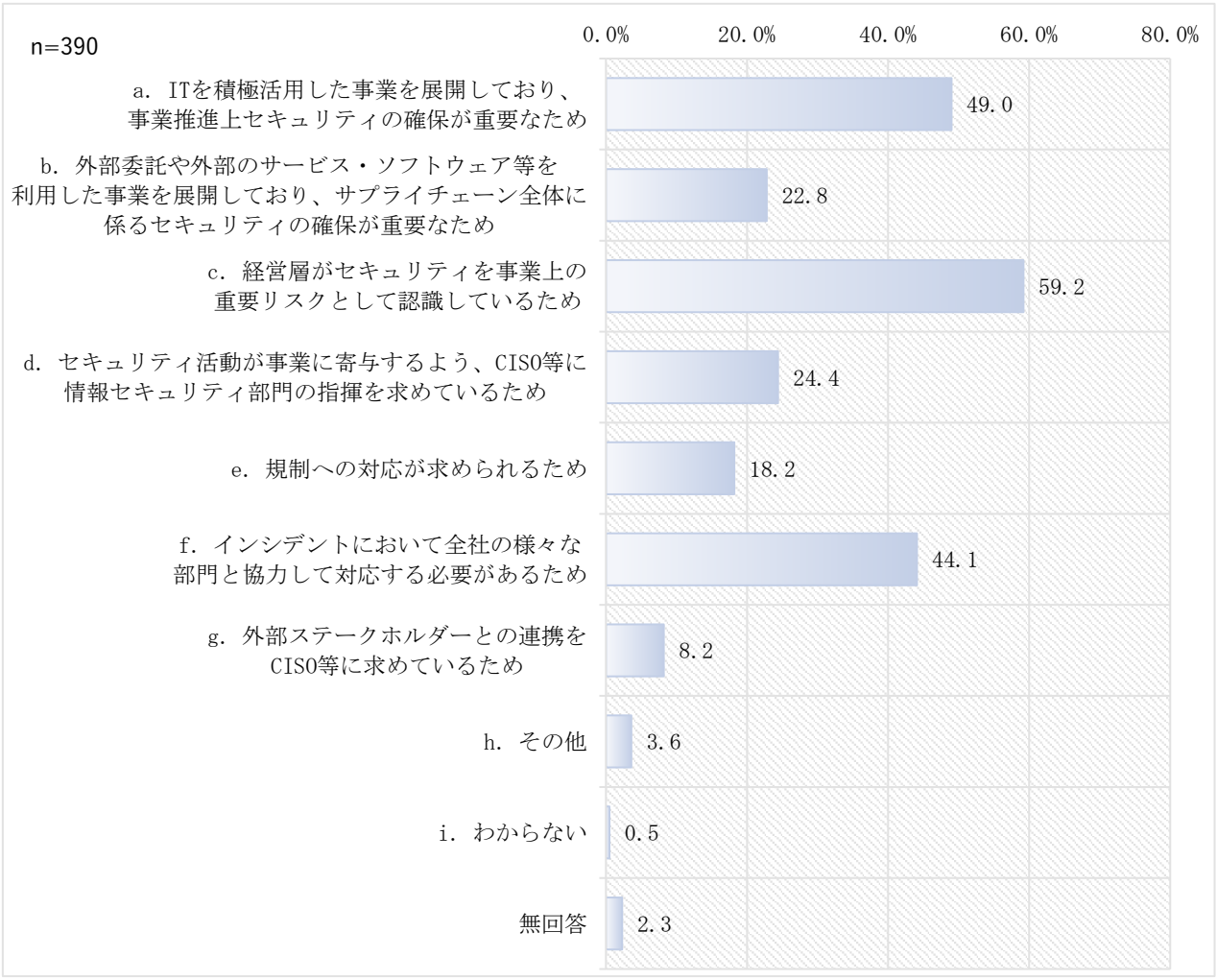

図 7-15　「経営・事業的役割」を重視する理由

Q16　Q14 で「a」と回答いただいた方にお伺いします。経営層が「経営・事業的役割」を重視しない理由を全てお選びください。（複数選択可）

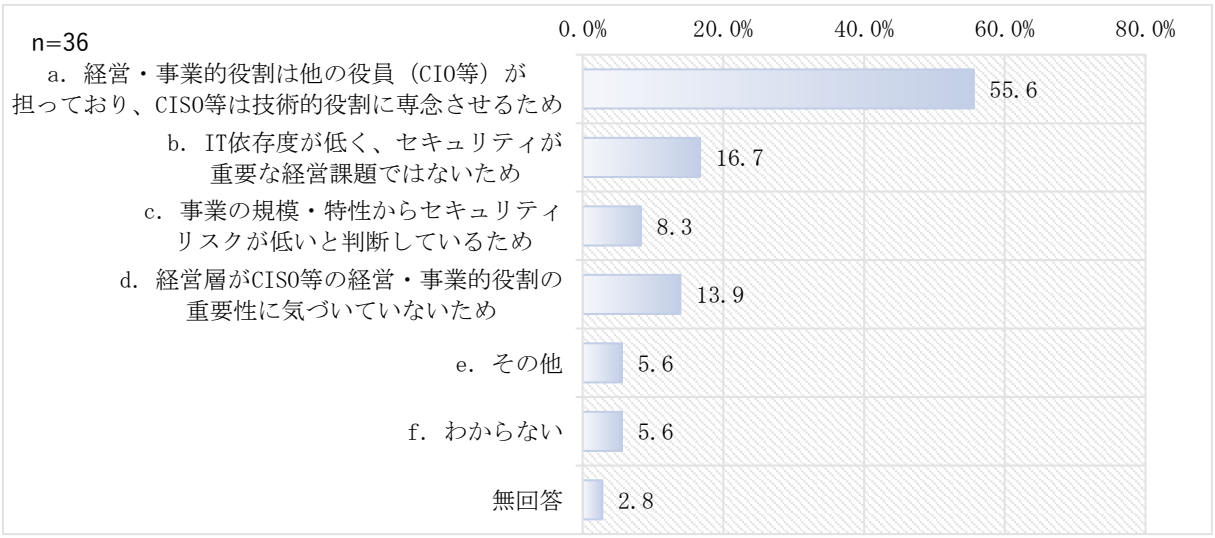

図 7-16　「経営・事業的役割」を重視しない理由

7.2.8. CISO 等の以前の所属

Q17.　現在の CISO 等が CISO 等になる以前の所属として当てはまるものを 1 つお選びください。（単一選択）

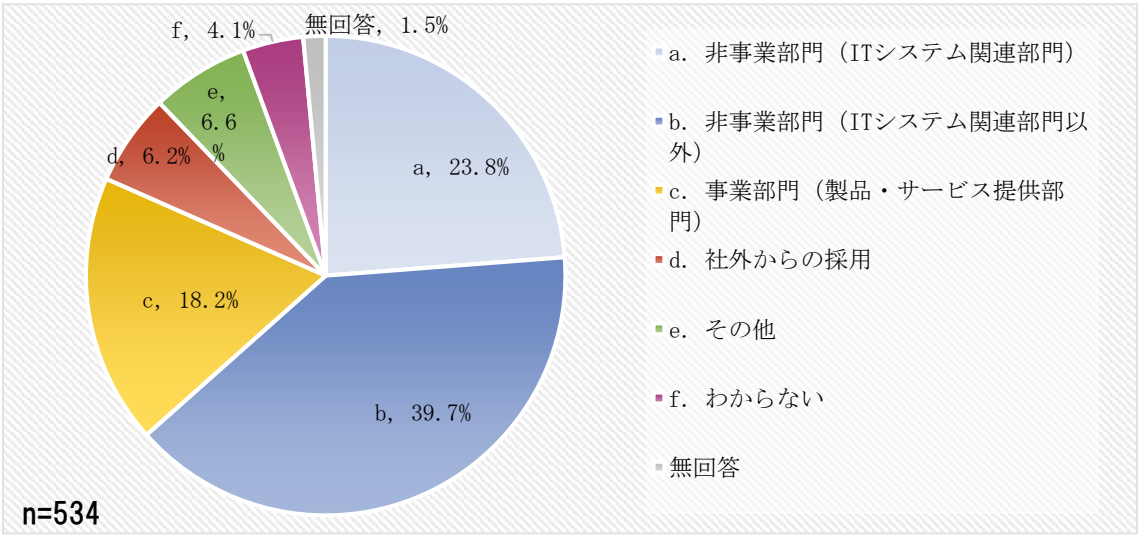

図 7-17　CISO 等の以前の所属

7.2.9.CISO 等に重要なスキル・経験

Q18.　CISO 等の役職にどのようなスキル・経験が重要であると考えていますか。重視するスキル・経験を 3 つまでお選びください。(3 つまで複数選択可)

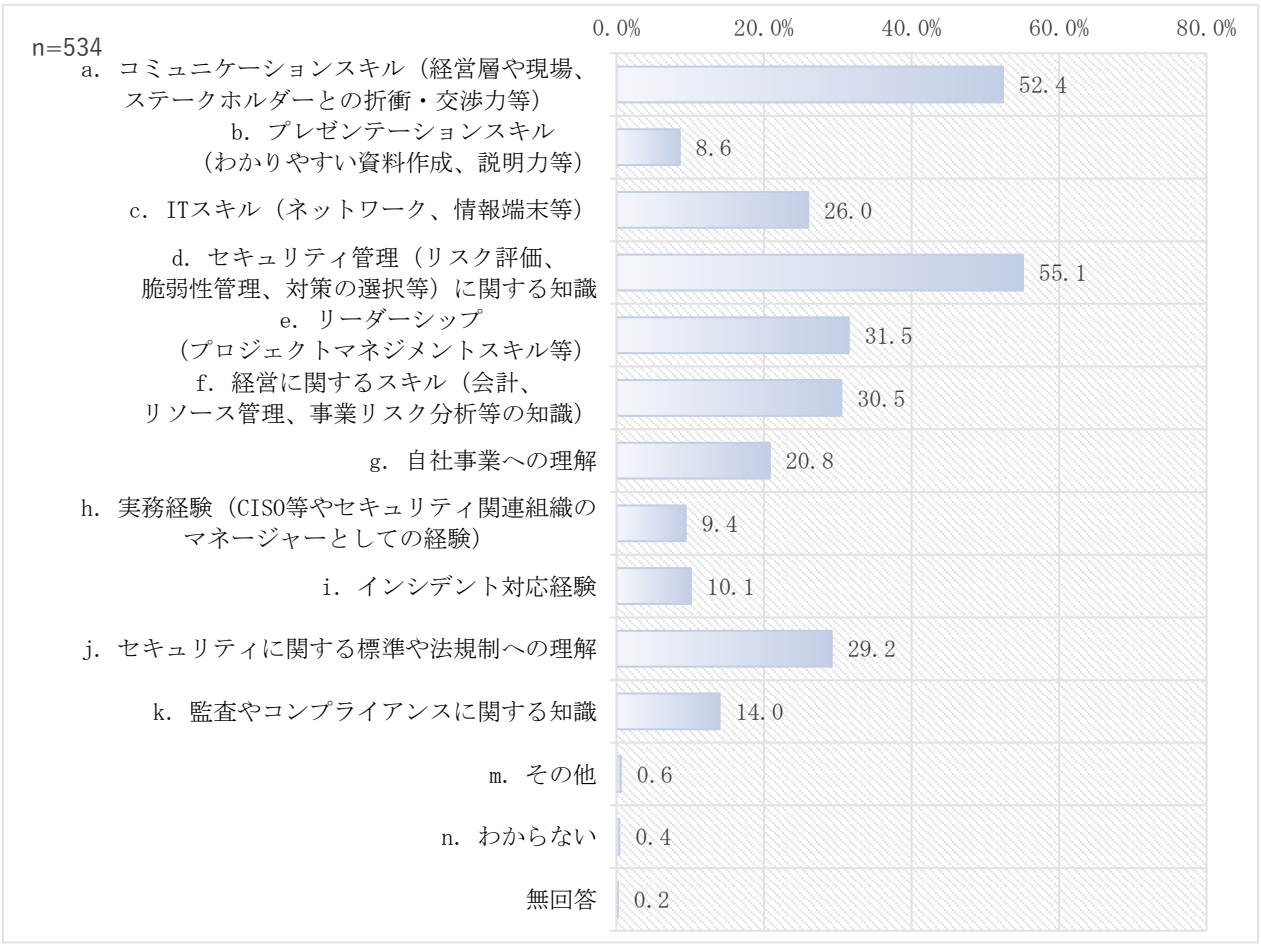

図 7-18　CISO 等に重要なスキル・経験

7.2.10. 重視している CISO 等の役割

Q19.　現在の CISO 等の役割のうち、重視しているものを 3 つまで選択してください。(3 つまで複数選択可)

Q20.　今後の CISO 等の役割として重視するもの 3 つまでお選びください。(3 つまで複数選択可)

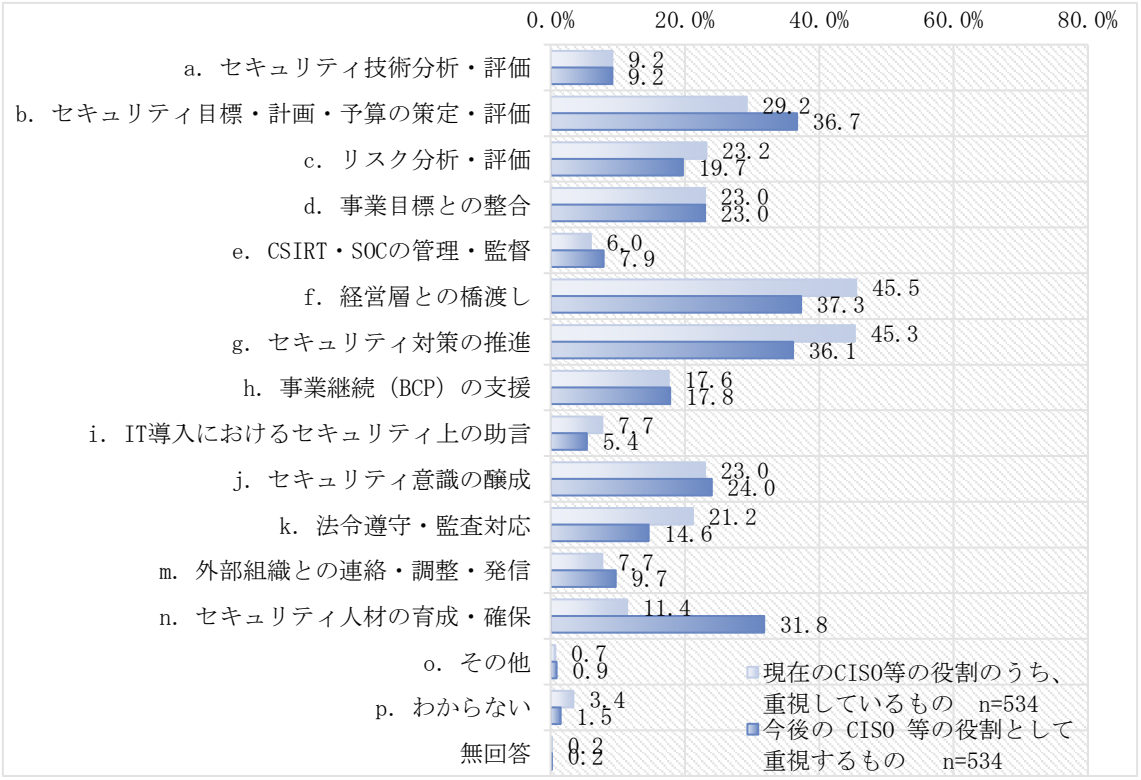

図 7-19　重視している CISO 等の役割

7.2.11. CISO 等の現状の取組み

Q21.　サイバーセキュリティリスク管理体制を構築するために、CISO 等が定めている社内ルールを全てお選びください。(複数選択可)

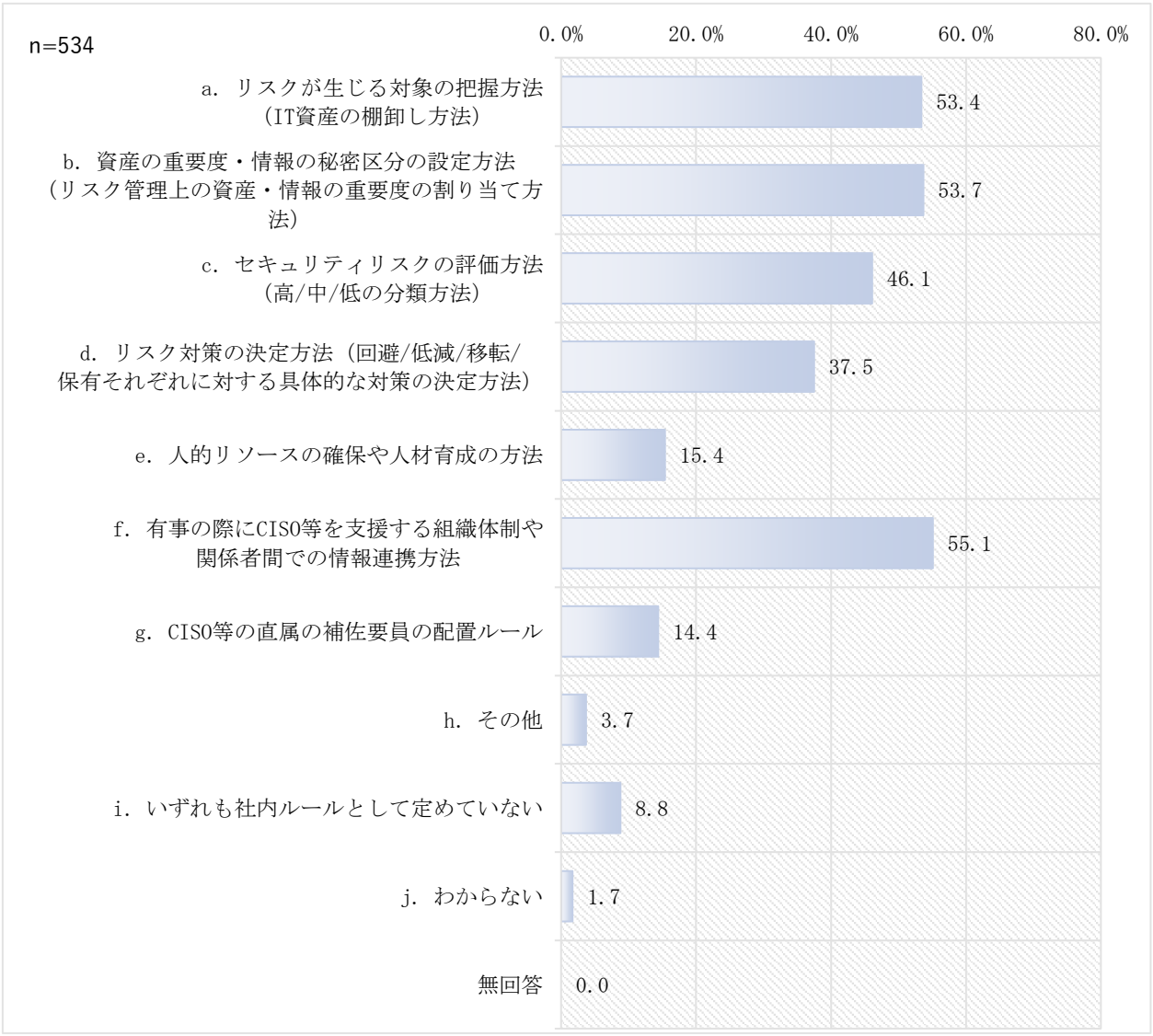

図 7-20　CISO 等が定める社内ルール

Q22.　CISO 等が、サイバーセキュリティ人材の育成・確保に関して、果たしている役割を全てお選びください。（複数選択可）

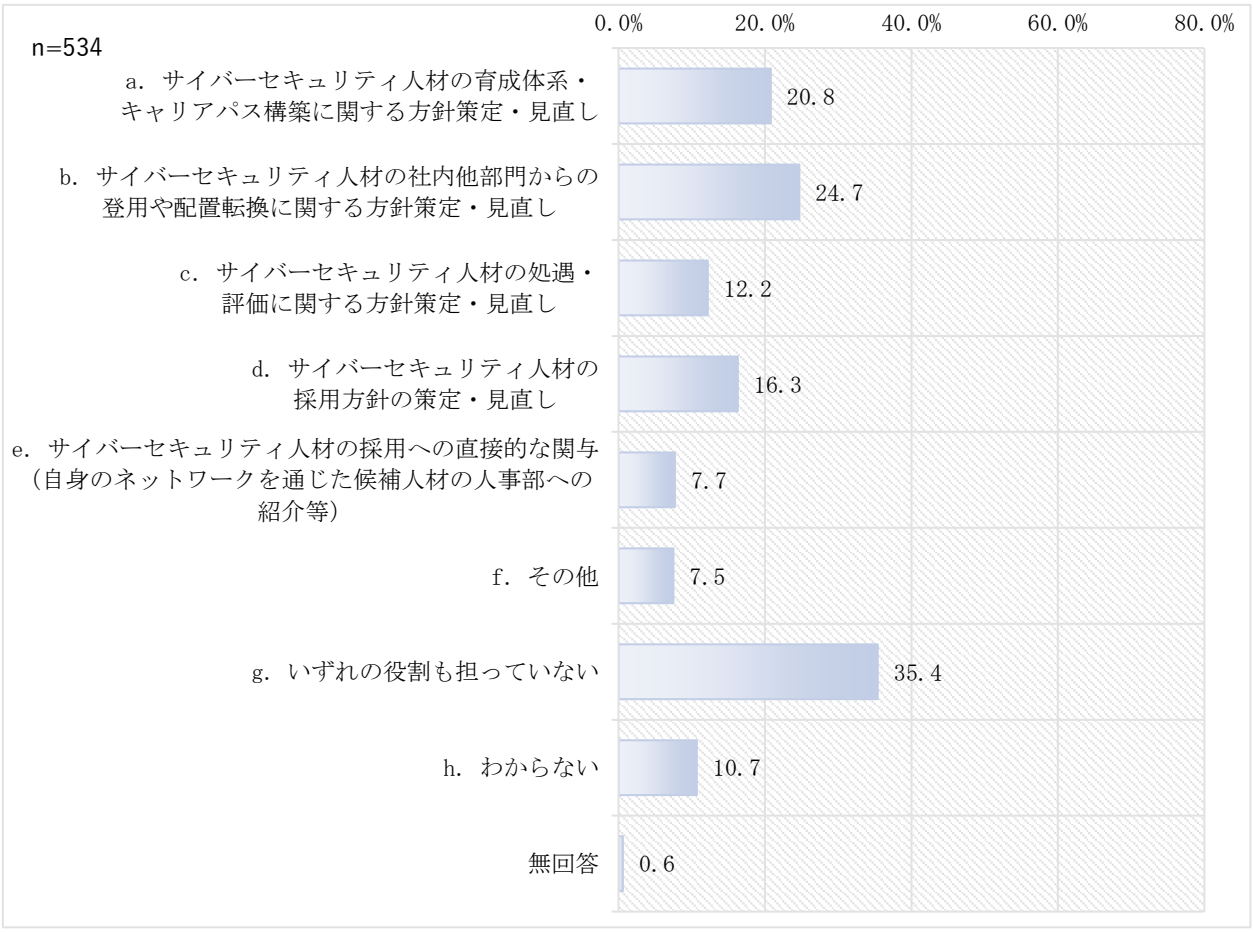

図 7-21　CISO 等が人材の育成・確保に果たしている役割

Q23　CISO 等が、CISO 等としての業務時間全体に対し、社内のマネジメントや社外との調整に費やす時間の割合について、最も当てはまるものをそれぞれ１つずつお選びください。（単一選択）

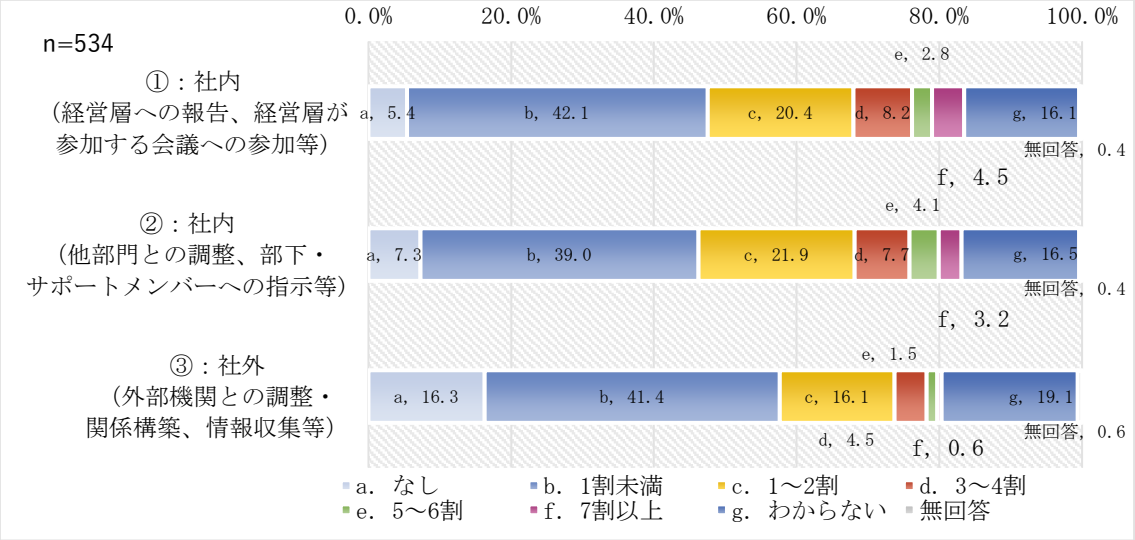

図 7-22　CISO 等の業務時間の配分

7.2.12. PDCAサイクルについて

Q24.　サイバーセキュリティマネジメントの PDCA サイクルにおいて、特に Check（診断、演習/訓練等）と Act（Check の結果を基とした改善）の実効性を高めるため、定期的に実施している対応を全てお選びください。（複数選択可）

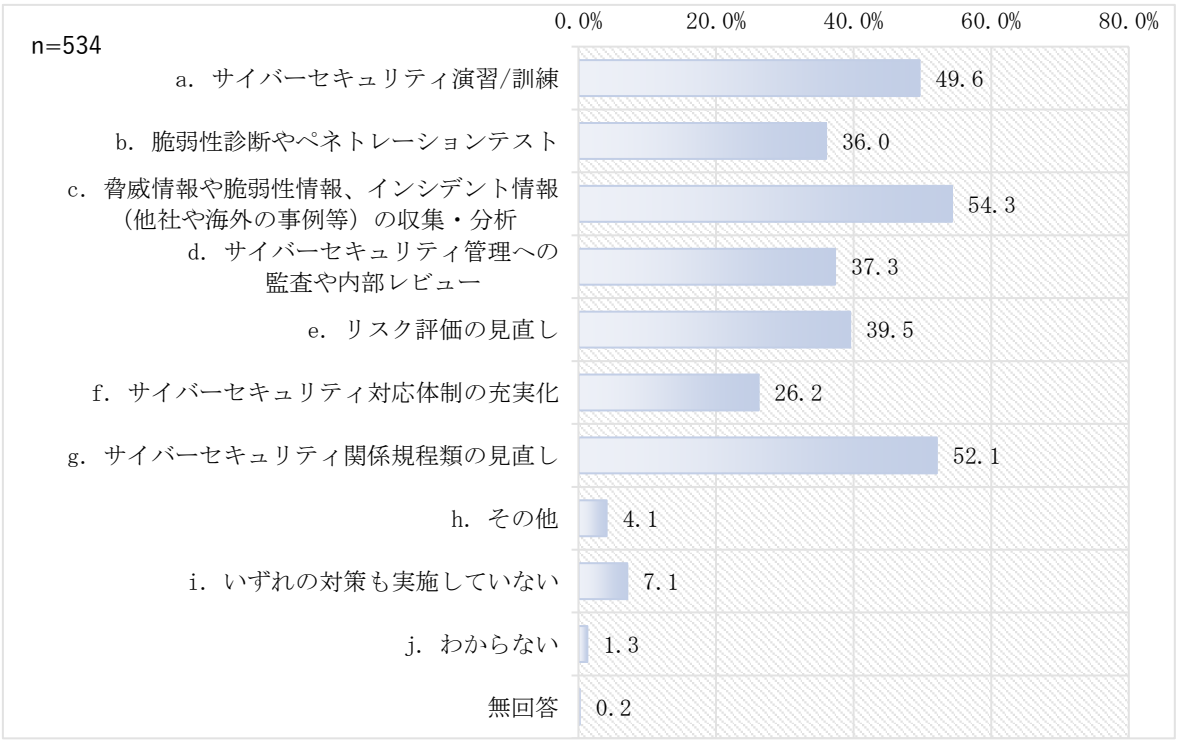

図 7-23　PDCA における C と A の取組み

7.2.13. サプライチェーンのセキュリティ

Q25.　サプライチェーンのサイバーセキュリティリスクについて、貴社でリスクと認識している範囲を全てお選びください。（複数選択可）

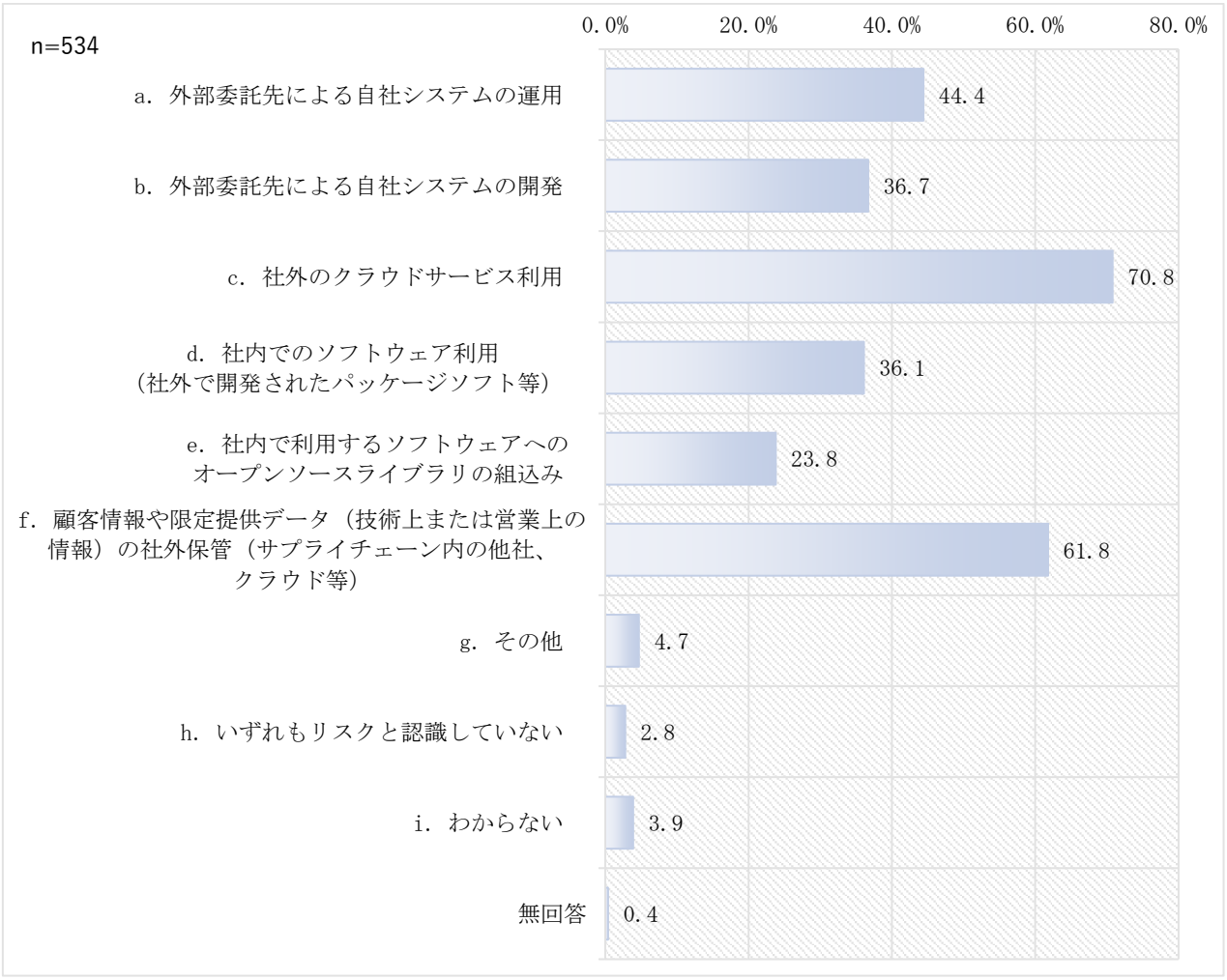

図 7-24　サプライチェーンセキュリティのリスク認識

SQ25.　前問でお選びいただいた項目のうち、特にリスクが高い項目について１番目から順番にお選びください。（それぞれ１つずつ）

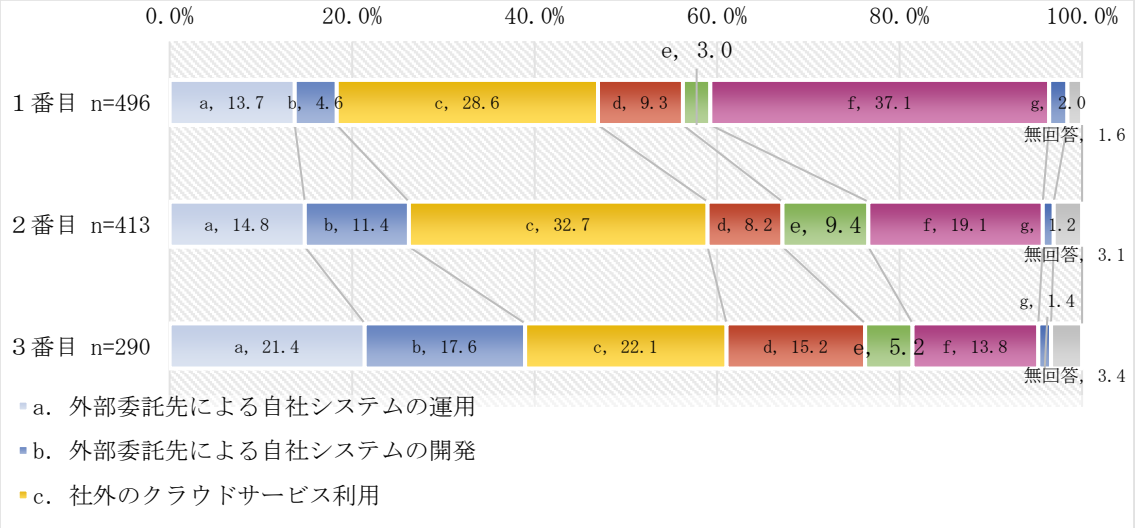

図 7-25　サプライチェーンセキュリティのリスク認識（特にリスクが高いもの）

Q26. サプライチェーンのサイバーセキュリティリスクに対応するため、実施している対策を全てお選びください。（複数選択可）

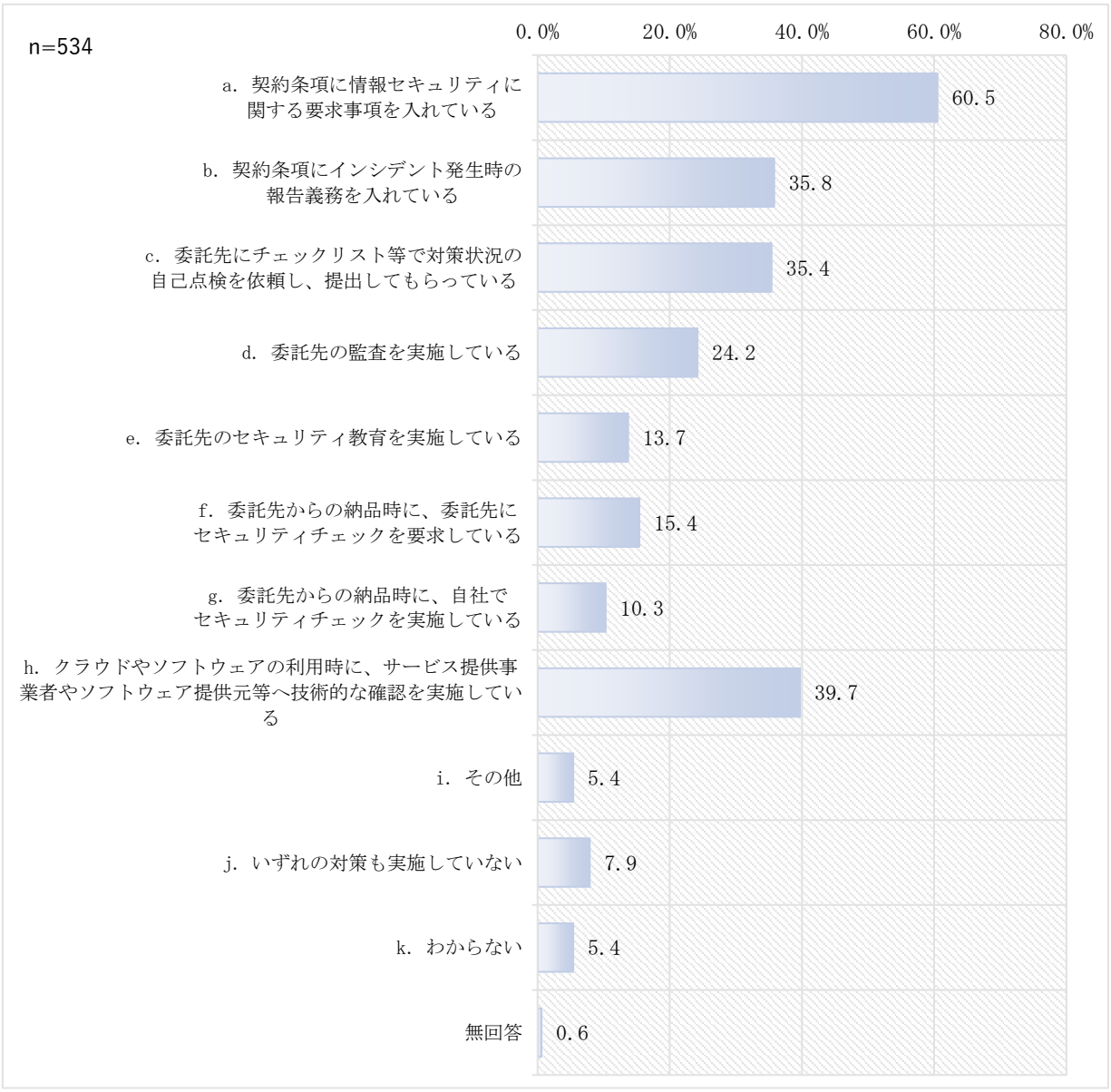

図 7-26 サプライチェーンセキュリティへの対策

7.2.14. 情報の収集と活用

Q27.　外部の脅威情報や脆弱性情報等について、情報収集、分析・評価、内部共有のそれぞれを実施していますか。当てはまるものをそれぞれ 1 つずつお選びください。(単一選択)

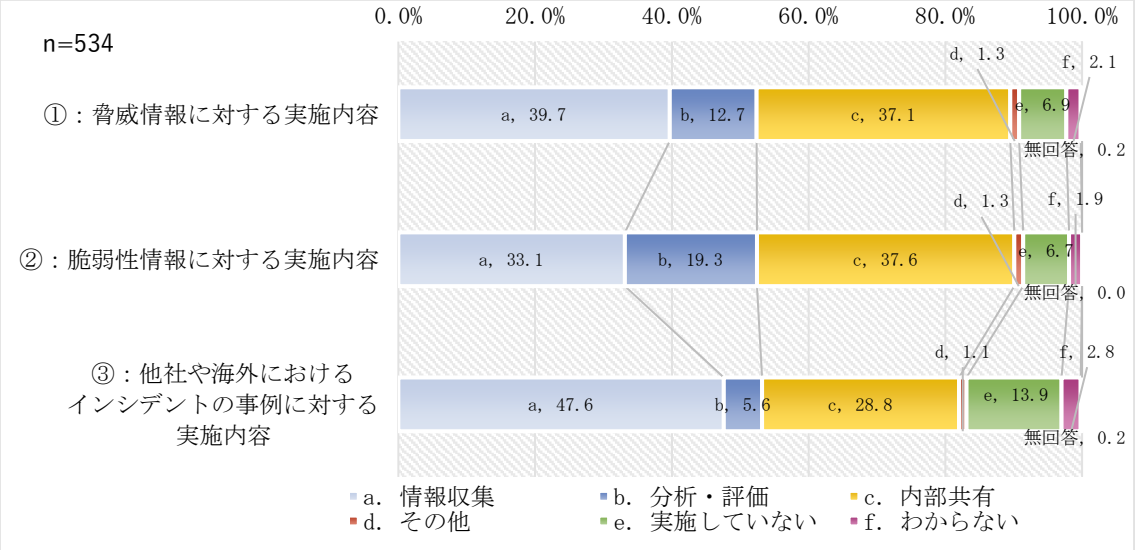

図 7-27　情報の収集と活用

7.2.15. CISO 等のサポートメンバー

Q28.　CISO 等が役割を遂行するにあたり、サポートするメンバーがいますか。当てはまるものを全てお選びください。(複数選択可)

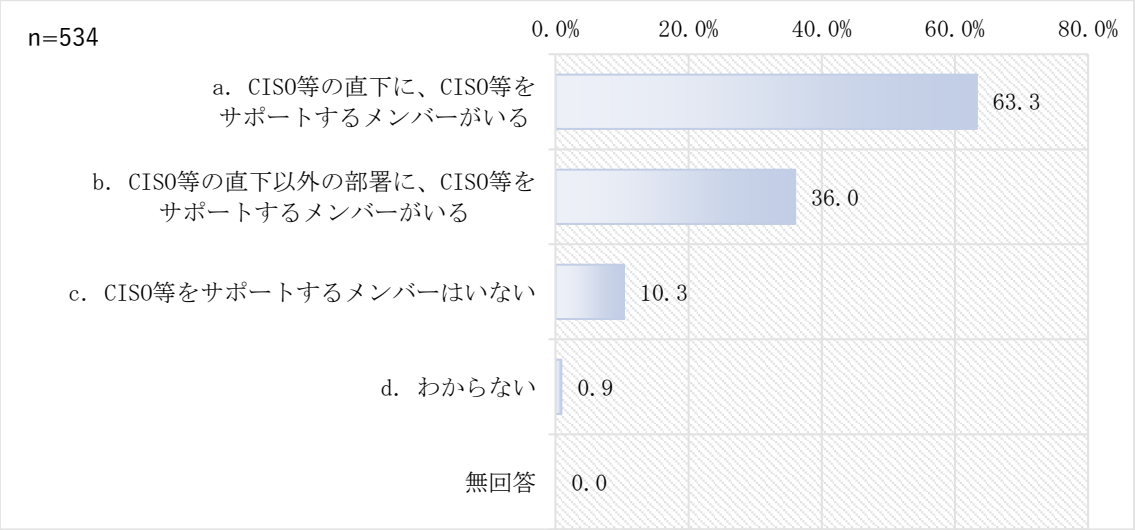

図 7-28　CISO 等のサポートメンバーの配置状況

Q29.　前問で「a.b」いずれか回答いただいた方にお伺いします。CISO 等をサポートするメンバーがいる理由を 3 つまでお選びください。（3 つまで複数選択可）

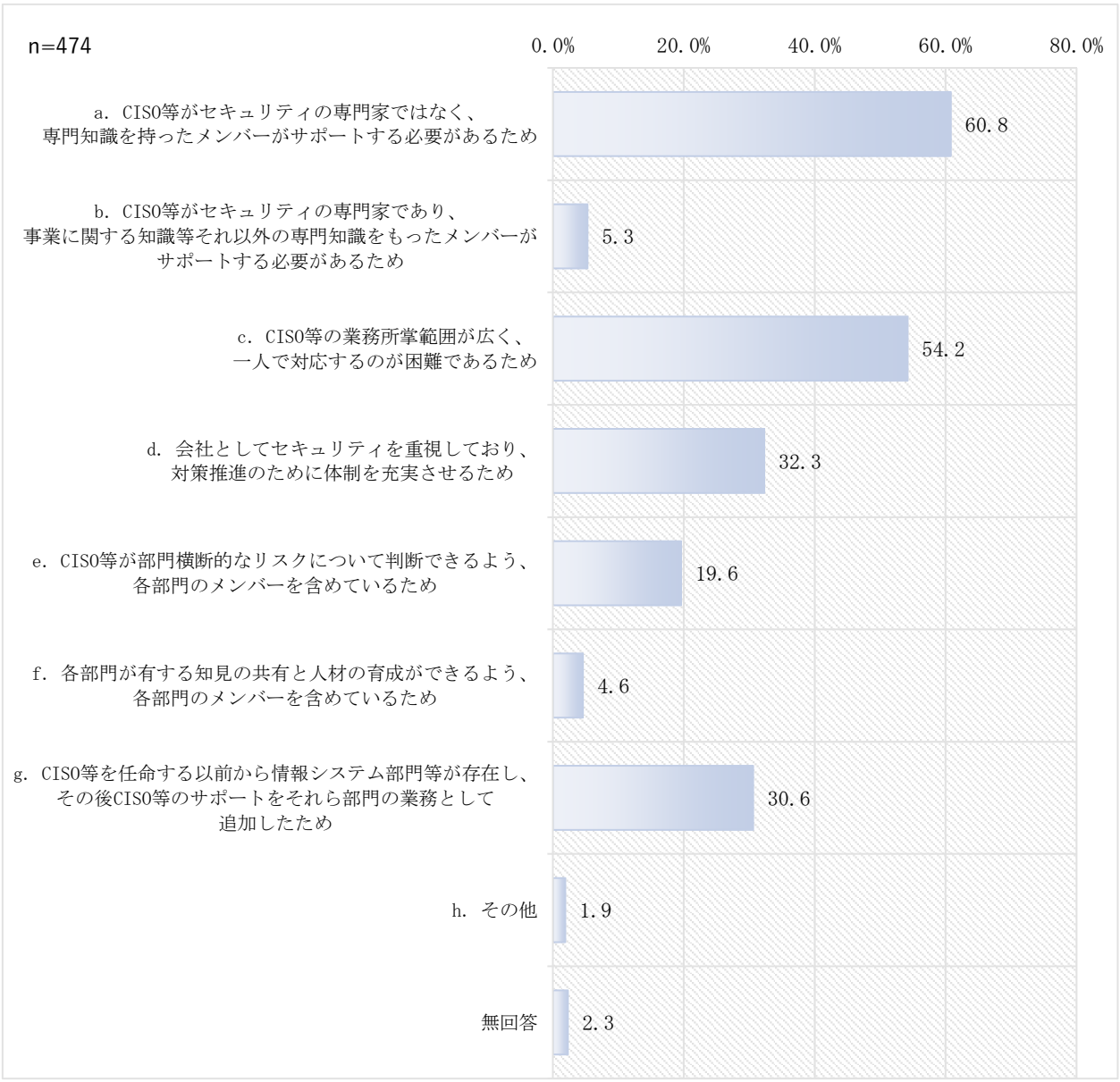

図 7-29　CISO 等のサポートメンバー（理由）

Q30.　Q28 で「a.b」いずれか回答いただいた方にお伺いします。CISO 等を支援するメンバーの所属部署について、当てはまるものを全てお選びください。（複数選択可）

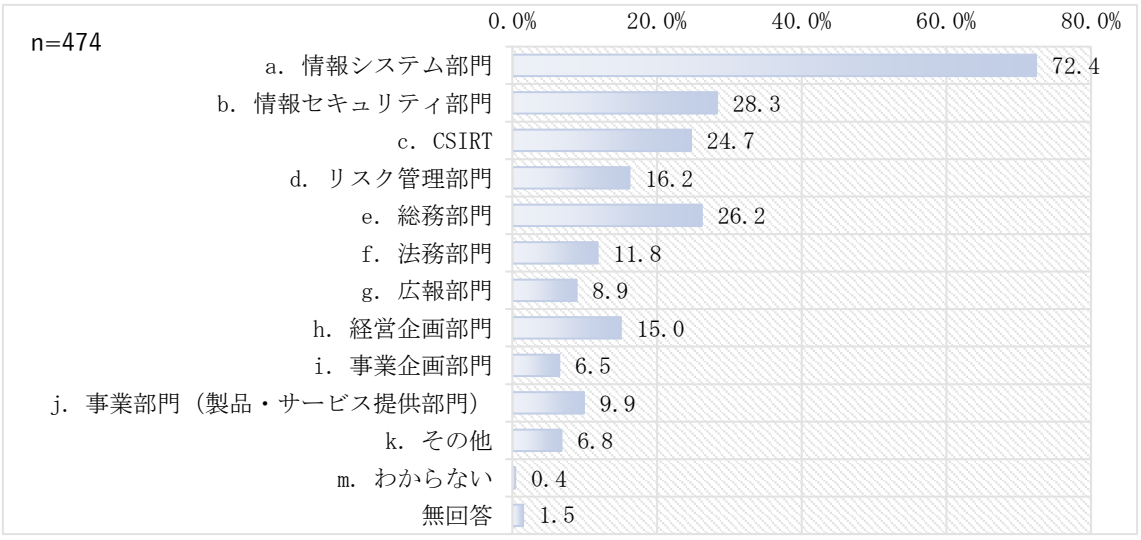

図 7-30　CISO 等のサポートメンバー（所属部署）

7.2.16. CSIRT

Q31.　CSIRT に配置されている人員について当てはまるものをそれぞれ 1 つずつお選びください。（単一選択）

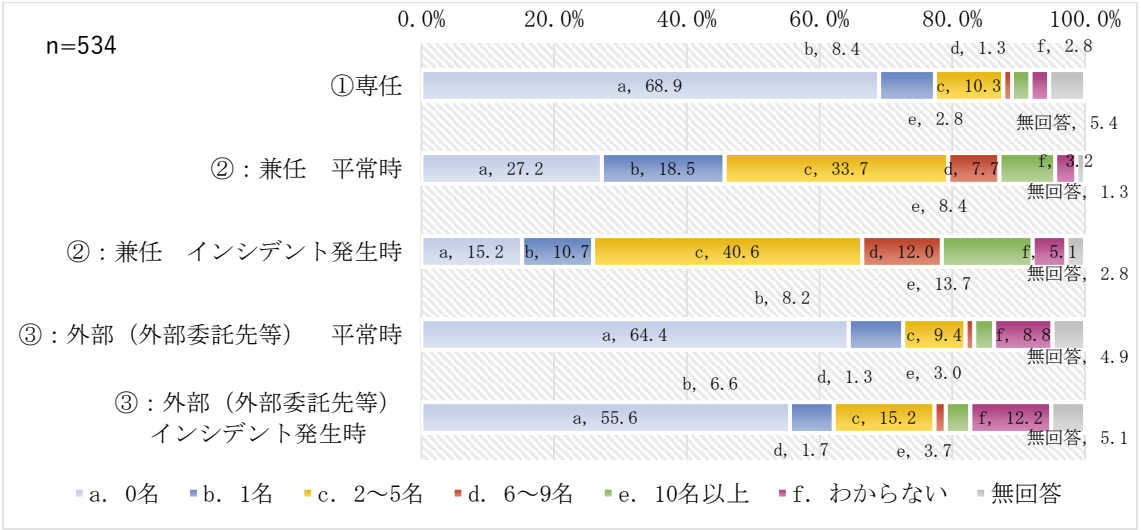

図 7-31　CSIRT（人員配置）

Q32.　CSIRT の設置目的（またはミッション）を全てお選び下さい。（複数選択可）

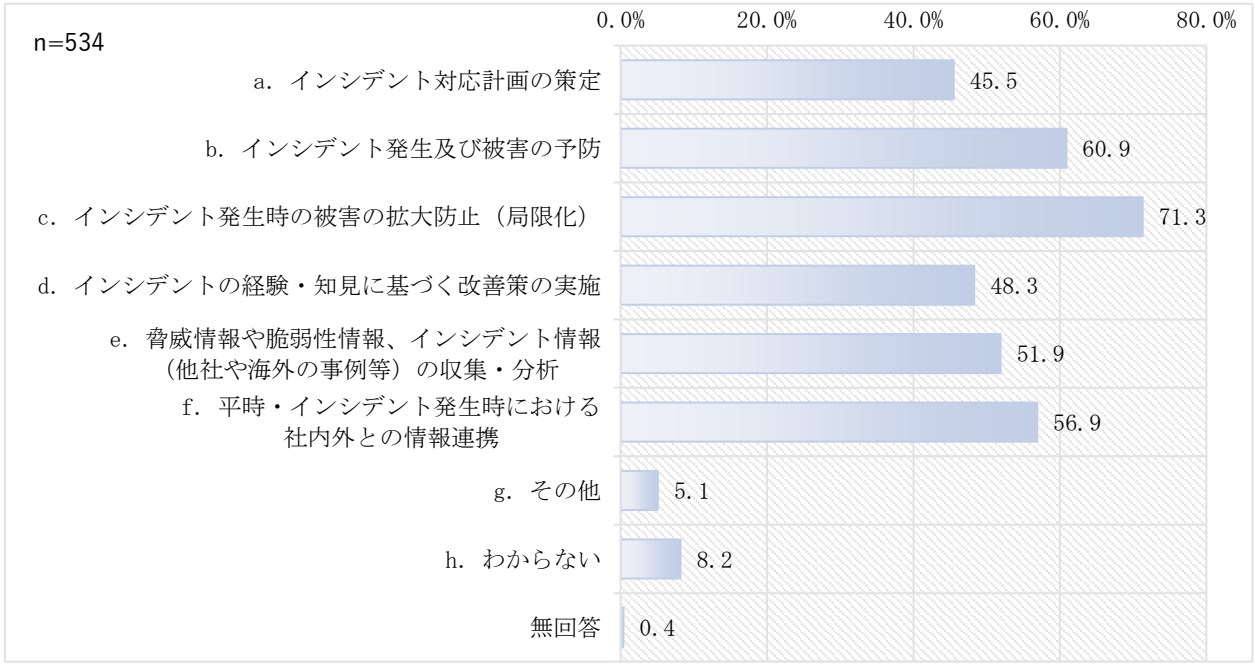

図 7-32　CSIRT（設置目的）

Q33.　CSIRT がインシデント対応にあたって有する権限（システム停止、ネットワーク遮断、調査等）を 1 つお選び下さい。（単一選択）

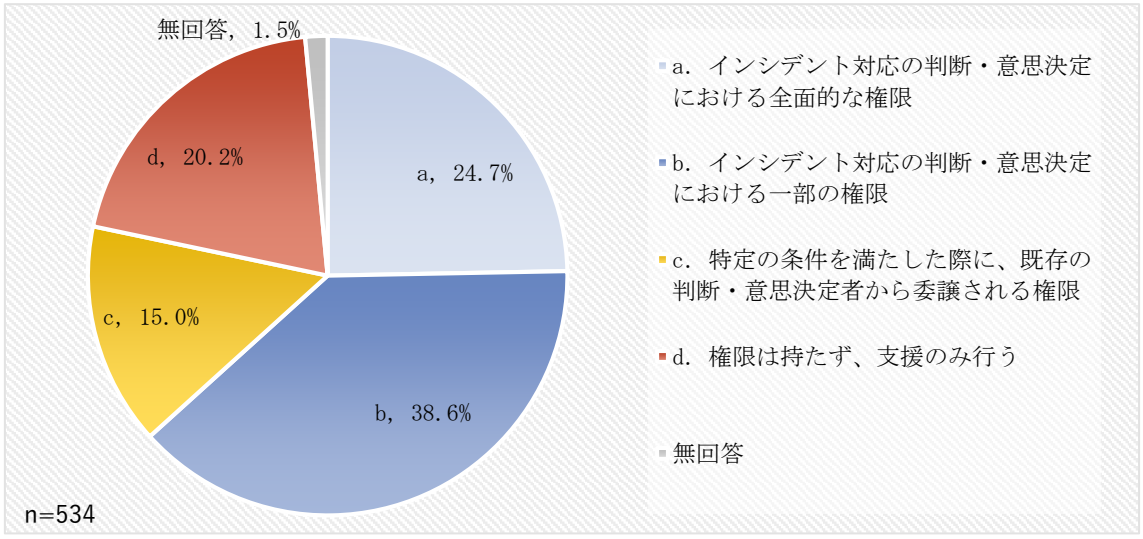

図 7-33　CSIRT（権限）

Q34.　CSIRT のメンバーに求められるスキル・経験を 3 つまでお選びください。（3 つまで複数選択可）

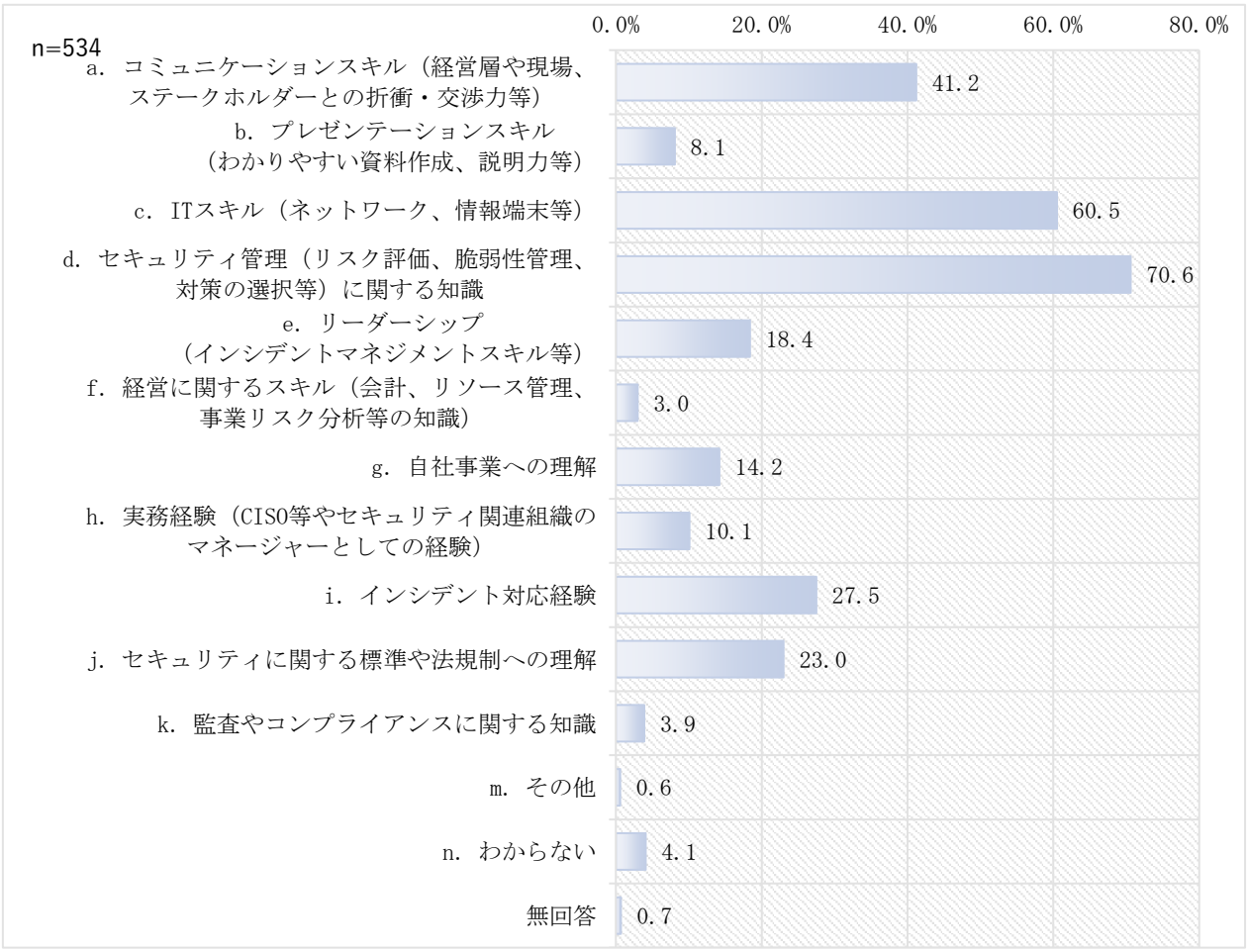

図 7-34　CSIRT（メンバーに求められるスキル・経験）