CISO 等セキュリティ推進者の
経営・事業に関する役割調査

－調査報告書－

2018年3月28日

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

目 次

1. はじめに

1.1 調査背景・目的

近年、企業活動における IT の積極活用は、企業の成長や事業の発展、グローバル化に対応した経営変革のために必須であるとされている。一方で、IT 活用を進めるほどセキュリティ上のリスクは高まり、インシデントが企業活動に与えるインパクトは増大する。事実、企業の事業継続を脅かすセキュリティインシデントの発生は後を絶たない。IT を積極活用した攻めの経営と、インシデントによるインパクトを最小限に抑える守りの経営を高いレベルで両立するには、経営層がセキュリティを経営戦略として捉え、主体的に取組むことが大切であるとの指摘がなされている。

また経営層による主体的取組の推進には、経営層の示す経営方針に基づくセキュリティ対策を実践し、実務課題を踏まえた経営戦略を提示し、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。さらに、「サイバーセキュリティ経営ガイドライン」におけるサイバーセキュリティ対策を実施する上での責任者である担当幹部や、NISC「サイバーセキュリティ人材育成プログラム」における橋渡し人材（以下、CISO 等セキュリティ推進者、あるいは単に CISO 等と省略する）の役割として、企業のセキュリティへの取組みが経営と事業に貢献するようマネジメントする役割の重要性が指摘されているところである。

セキュリティへの投資が、優先的に対策すべきセキュリティリスクへの対処となるようマネジメントする役割や、あるいはセキュリティ対策が事業運営の現実から遊離して形骸化しないように、社内の関係部門と十分に連携した上で対策策定する役割など、セキュリティの取組みを経営と事業の観点で意味あるものにする主導的な役割が求められている（本調査では以降、「経営・事業に関する役割」あるいは単に「経営・事業的役割」と略記する）。

しかしながらこうした指摘に関わらず、経営層とセキュリティ部門との橋渡しを行う役割や、セキュリティ対策と事業目標との整合を取る役割等を、CISO 等の役割として重視する当事者・関係者の割合はまだ少ない[1]。多くの CISO 等の役割は技術そのものに関するものであり、上記「経営・事業に関する役割」を十分に担っていない可能性がある。CISO 等が経営・事業に関する役割を担うことを阻害している要因は何か、そうした役割を果たす上で課題となるのはどのようなことか等を調べることが必要である。

1.2 本調査の概要

本調査は、CISO 等の経営・事業に関する役割について、複数の側面から調べる。すなわち、CISO 等に求められる経営・事業に関する役割とは具体的にはどのような内容か、どのくらいの CISO 等がそうした役割を担っているか、経営・事業に関する役割を担う上で阻害要因はなにか、あるいは経営・事業に関する役割の課題はなにかといった点である。

本報告書の構成は、以下の通りである。

[1] IPA「企業の CISO や CSIRT に関する実態調査 2017」 p34-p35

1. 文献調査（第 2 章）：国内外の公開レポート、書籍等を対象に CISO 等の経営・事業に関する役割の文献調査を行う。
2. 有識者調査（第 3 章）：海外を含めた、大学、セキュリティ関連団体、企業等に所属する、CISO 等に関する有識者を対象にインタビュー調査を行う。
3. アンケート調査（第 4 章）：「文献調査」と「有識者調査」の結果を踏まえ、日本企業の CISO 等の経営・事業に関する役割の実態等を把握するため、アンケート調査を行う。
4. まとめ・今後の取組み：「文献調査」「有識者調査」「アンケート調査」の結果から CISO 等の経営・事業に関する役割について知見をまとめ、今後の取組みの方向性について述べる。

2. CISO 等セキュリティ推進者の経営・事業に関する役割についての文献調査

2.1 調査概要

文献調査においては、以下の観点を取り上げた国内外の公開レポート等から CISO 等の経営・事業に関する役割について、情報を収集・調査した。また、そうした役割については CISO 等を養成する教育プログラムにおいても検討が行われていることから、併せて調査した。既存の役割事例や役割に関する検討結果を整理した上で、重視されている点、課題等を明らかにした。

今回調査対象とした文献等[2]を下表に示す。各文献等の概要は「2.3　CISO 等の経営・事業に関する役割についての国内外文献調査」、「2.4　CISO 等の教育プログラムに関する調査」に示す。

表 2.1-1　調査文献一覧

観点	調査文献	文献番号
CISO 等の経営・事業に関する役割	産業横断サイバーセキュリティ人材育成検討会「第一期最終報告書 第 1.0 版」及び「第一期最終報告書第 1.0 版付 A3 産業横断 人材定義リファレンス　～機能と業務に基づくセキュリティ人材定義～」2016.9.14、「第二期中間報告 第 1.0 版」2017.11.21	文献 1
	内閣サイバーセキュリティセンター（以下、NISC と記載）「サイバーセキュリティ人材育成プログラム」2017.4.18	文献 2
	経済産業省／IPA「サイバーセキュリティ経営ガイドライン（Ver. 2.0）」2017.11.16	文献 3
	Deloitte, ”The new CISO - Leading the strategic security organization” 2016	文献 4
	Info-communications Development Authority of Singapore, “National Infocomm Competency Framework NICF, NICF Overview Map, Horizontals, Infocomm Security, Security Management, Chief Information Security Officer, Job Role & Competencies” 2009, 2011	文献 5
	NIST SP800-181, “National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework” 2017.8	文献 6
	Bill Bonney 他, “ CISO Desk Reference Guide: A Practical Guide for CISOs” 2016	文献 7
	IT Capability Maturity Framework(IT-CMF) 2015	文献 8

[2] なお、記載の文献以外にも、上記観点を取り上げたものがある。企業のセキュリティ中核を担う推進者として CISO 等に求められる役割は注目を集めており、今後も各所において役割に関する検討が進むと考えられる。CISO 等の経営・事業に関する役割について、より詳細な具体化を図る際、こうした検討成果を踏まえることが必要である。

観点	調査文献	文献番号
	SANS, “Mixing Technology and Business: The Roles and Responsibilities of the Chief Information Security Officer” 2003	文献 9
CISO 等の教育プログラム	EC-Council CISO Program, “Certified CISO Body of Knowledge”	文献 10
	カーネギーメロン大学 Heinz 校　CISO 認定プログラム	文献 11

2.2 文献調査から得られた考察

(1) CISO 等に求められる経営・事業に関する役割の重要性

CISO 等に求められる役割について、技術的役割に加え経営・事業に関する役割の重要性がより高まるとの見解が、国内外の文献調査の結果から得られた。

CISO 等の経営・事業に関する役割の重要性について言及した国内文献としては、文献１がある。同文献では、経営的な知見とサイバー攻撃やネットワークインフラなどの専門的な知見を有して、経営を支援しながら関係部署をリードする役割が求められるとしている。また文献２は、CISO 等には、IT を利活用した新しい価値の創出など経営・事業戦略的な視点を持ちつつ、最新のサイバーセキュリティに関する知識・能力の向上が必要としている。IPA の昨年度調査[3]でも、今後 CISO 等には「ガバナンス」や「事業貢献」等の経営・事業に関する役割が、より重視されるとの結果が出ており、技術的役割に加え経営・事業に関する役割が CISO 等に求められると考えられる。

海外文献では、文献４において CISO に求められる役割を「技術者」・「監視者」・「アドバイザー」・「戦略家」の 4 つの側面で分類し、各役割について現在の業務比率と今後望ましいと考えられている業務比率を調査している。現在は、サイバー脅威の監視、撃退、及び対応といった技術的役割を担う「技術者」と「監視者」の業務比率が高いが、今後は、事業戦略や情報セキュリティ戦略、リスクマネジメントといった経営・事業に関する役割を担う「アドバイザー」と「戦略家」の業務比率が高まるとしている。

また、シンガポールの IDA（Info-communications Development Authority of Singapore ）[4]が公表している文献５では、CISO の責任範囲として、情報セキュリティ戦略・リスクマネジメント戦略と事業戦略との整合が求められている。また、要求スキル・経験としては IT だけではなくビジネスプロセスに対する理解も求めている。文献８は、リスクマネジメントの分野では、IT リスクが事業目標や組織の意思決定に与える影響を明確にすること、自社事業に与えるマイナスの影響を低減することの重要性等、経営・事業に関する役割について言及している。

国内外の文献調査の結果から、CISO 等は自社の経営、事業の内容やプロセスを理解した上で役割を果たすことが求められており、技術的役割に加え経営・事業に関する役割が重要になると考えられる。

---

[3] IPA「企業の CISO や CSIRT に関する実態調査 2017」

[4] IDA は 2016 年 10 月 1 日に、MDA（Media Development Authority）と組織再編され、現在は IMDA（Infocomm Media Development Authority）となっている。

(2) CISO 等に求められる経営・事業に関する役割の要素とその分類、記述の観点

調査対象の文献から、CISO 等の経営・事業に関する役割に該当する要素を抽出し、分類を試みた。これは、今後こうした役割について様々な検討を加える際に、役割に関する表現の細かな違いにとらわれず、ある程度共通な、あるいは主要だと思われる表現に整理したうえで検討を加えることが、現実的であると考えられるからである。本調査では、後述するアンケート調査において、どのような経営・事業に関する役割がより多くの企業の CISO 等によって担われているか実態を調べるために、分類の項目を用いた。

分類項目としては、IPA の昨年度調査（前述）で導入した分類項目の表現を若干見直したものを用い、4 つの項目（事業貢献、コーポレートガバナンス、リスク管理、セキュリティ対策）を設定した。

表 2.2-1 は、調査対象の文献毎、抽出した役割の要素の数を示したものである。なお文献 11 のみ、役割の数ではなく教育プログラムのカリキュラムの数を示している。各カリキュラムにおいて CISO 等の経営・事業に関する役割が扱われていることから、カリキュラムの名称を役割の要素の代わりとして分類対象に加えた。

表 2.2-1　分類の対象とした CISO 等に求められる役割

文献番号	表番号/タイトル	役割の数
文献 1	表 2.3-1　CISO/CRO/CIO 等の役割定義 の「サイバーセキュリティ対策機能を実現する業務」	12
文献 3	表 2.3-3　CISO 等に指示すべき重要 10 項目	10
文献 5	表 2.3-6　CISO に求められる役割一覧	18
文献 6	表 2.3-8、表 2.3-9　専門分野の定義と役割 の「専門分野」	7
文献 8	表 2.3-12　情報セキュリティマネジメントの目標・目的・価値・役割	7
文献 9	表 2.3-13　CISO の 7 つの責任	7
文献 10	表 2.4-1　CISO に求められる知識と経験	5
文献 11	表 2.4-6　CISO 認定プログラムのカリキュラム	14

上記の文献で示されている役割を 4 つの項目で分類し、共通の要素・主な要素と思われるものを抽出した結果が表 2.2-2 である。また共通要素・主な要素を抽出するにあたり、文献別に CISO 等に求められる役割を分類毎に整理したものが、表 2.2-3 及び表 2.2-4 である。

この表で示したように、文献から抽出した役割の要素は、結果として、概ね上記の 4 分類に整理できた。

表 2.2-2　文献調査で示された CISO 等に求められる役割の共通要素・主な要素

分類	文献で示された共通要素・主な要素
事業貢献	・事業戦略との整合性 ・事業戦略に即するセキュリティ投資 ・利用者の利便性 ・事業継続計画
コーポレートガバナンス	・ガバナンス体制の構築及び運営 ・セキュリティ目標の策定 ・予算策定 ・ステークホルダーとの連携・情報共有 ・セキュリティに関する意識向上
リスク管理	・リスクの管理、監督 ・リスクの分析 ・リスクの優先順位決定・対応 ・コンプライアンス ・外部対応（官公庁、顧客、パートナー等）
セキュリティ対策	・セキュリティルールの策定及び評価 ・ソリューションの実装 ・緊急時体制（CSIRT 等）、監視組織（SOC 等）の構築・運営 ・インシデント対応

CISO 等の経営・事業に関する役割の記述の観点については、文献５が参考になった。この文献は、セキュリティ推進者に必要な能力を、その能力を発揮することで遂行できる役割の説明や、能力を支える知識、能力を適用する業務の広がり等の多岐にわたる観点から多面的に記述している。能力を記述する際に、単に、その能力を要素に分解して列挙するという手法だけによるのではなく、様々な角度から説明することによって、読者の理解を助けることが容易になっている。

今後、CISO 等に求められる経営・事業に関する役割について議論を展開する際には、こうした多面的な観点で記述する方法が参考になる。

表 2.2-3　CISO 等に求められる役割と分類（文献別）

分類軸	文献1	文献3	文献5	文献6
事業貢献	・ICT環境における事業継続計画の策定サイバーセキュリティ保険の導入検討 ・災害対策（DR）に関するICT環境改善計画の策定 ・災害対策及び災害発生時に関する稼働計画の策定 ・ユーザビリティの観点に基づく機能改善・実装計画の企画立案、エンドポイント及びUIに関するセキュリティ機能改善計画の策定 ・各事業に対するIT導入・構築運用改善計画の企画立案、ガイドライン・マニュアルの策定		・戦略策定への貢献 ・戦略および行動計画策定 ・企業の事業戦略におけるITニーズとの整合 ・ビジネスイノベーションの特定と実行 ・IT投資のビジネス価値の最大化 ・情報セキュリティプログラム投資をサポートするビジネスケースの策定	・戦略的計画と政策（SPP）
コーポレートガバナンス	・サイバーセキュリティ対策に関する全社的統括 ・コンプライアンス、ガバナンス及びリスクマネジメントの観点に基づくセキュリティ対策（事業戦略または中期計画）	・PDCAサイクルの実施と対策の開示 ・予算の確保、人材配置・育成 ・系列企業・ビジネパートナー ・情報収集・共有 ・被害発覚後の開示体制整備	・情報セキュリティ目標の確立 ・プロジェクト成功のためのステークホルダーマネジメント ・予算策定	・訓練、教育、啓発（TEA）
リスク管理	・情報資産保護活動におけるICT環境改善計画の策定、情報資産の保護基準・保護方法の改善、情報漏洩保険の導入検討 ・情報資産保護活動におけるICT運用改善活動の策定、情報資産の棚卸	・リスク管理体制の構築 ・リスクの把握、対応計画策定 ・ITシステム管理・外部委託先	・情報セキュリティ全体のリスクマネジメント ・ビジネスソリューションプロバイダーに対するリスク評価と計画 ・コンプライアンスへの理解と適用	・リスク管理（RSK） ・エグゼクティブ・サイバー・リーダーシップ（EXL） ・法的助言と政策提言（LGA）
セキュリティ対策	・セキュリティ対策に係る実施計画の企画立案、規程・ルールの策定 ・システムセキュリティの観点に基づく機能改善・実装計画の企画立案システム構成に関するセキュリティ機能改善計画の策定	・サイバーセキュリティ対応方針の策定 ・緊急時対応体制（CSIRT等）整備、定期的な演習の実施	・事業に関する技術モデルの選択 ・適切なIT戦略およびソリューションの決定 ・変更管理プロセスの実装	・サイバーセキュリティ・マネジメント（MGT） ・プログラム/プロジェクト・マネジメントおよびアクイジション（PMA）
その他	・ライセンス管理を踏まえた、リプレース計画の企画立案、固定資産管理・ソフトウェア会計管理		・プロジェクトコスト管理 ・プロジェクトリスク管理 ・プロジェクト監督	

表 2.2-4　CISO 等に求められる役割と分類（文献別）

分類軸	文献8	文献9	文献10	文献11
事業貢献		・組織の戦略的ビジネス計画とセキュリティニーズのバランスを調整し、リスク要因を特定し、ソリューションを選定する。		・Security Strategy & Innovation（セキュリティ戦略とイノベーション） ・Digital Transformation: Security Implications（デジタルトランスフォーメーション：セキュリティへの影響）
コーポレートガバナンス	・役割や責任、説明責任を含む情報セキュリティガバナンスモデルの構築 ・セキュリティ関連のコミュニケーションの管理と従業員教育	・顧客、パートナー、または一般の人々との議論を含め、セキュリティ侵害への対応を計画し、テストする。	・ガバナンス ・戦略策定及び予算、ベンダマネジメント	・Enterprise Security Governance & Planning（企業セキュリティガバナンスと計画） ・Security Financial Management（セキュリティ予算管理） ・Effective Communication Strategies（効果的なコミュニケーション戦略）
リスク管理	・情報セキュリティリスク及びインシデントの評価・優先順位付け・対応・監視 ・情報セキュリティ活動及びコンプライアンスレベルの報告	・組織のセキュリティ担当者を監督する。（ファイアウォールデバイスを管理するネットワーク技術者からセキュリティ委託会社まで） ・セキュリティ戦略に関する組織の代表者として、顧客、パートナー等に対応する。 ・組織の代表として行動し、社員によるネットワーク攻撃や情報盗難の原因を追求しながら、法執行機関と対処する。	・セキュリティリスクマネジメント及びコントロール、監査	・Cyber Risk Management （サイバーリスクマネジメント） ・External Dependency Management（外部ステークホルダー管理） ・Cyber Law & Compliance（サイバー分野に関連する法とコンプライアンス）
セキュリティ対策	・既存のセキュリティアプローチやポリシー、管理策の効率性評価 ・認証されていないアクセスや利用、情報開示、破壊、変更、デジタル化された情報資産の破壊からの保護 ・物理的なITコンポーネントとエリアの保護	・コアビジネス要件に沿う適切なビジネスアプリケーション保護を提供するセキュリティポリシーおよび手順を開発する ・アウトソーシングにおけるセキュリティハードウェアおよびソフトウェア製品の選定テスト、展開、保守を監督する。	・セキュリティプログラムマネジメント及び運用 ・情報セキュリティに関するコアコンセプト	・Security Metrics & Operational Resilience（セキュリティ評価指標と運用レジリエンス） ・Security Structure & Operations（セキュリティ構造と運用） ・Threat & Incident Response（脅威とインシデントレスポンス） ・Managing Operational Threat（運用上の脅威管理） ・Building an Insider Threat Program（内部不正プログラム設計） ・A Realistic View of Security Technology（セキュリティ技術に対する現実的評価）
その他				

(3) CISO 等の経営・事業に関する役割の課題

CISO 等の経営・事業に関する役割の課題として、①事業を理解した上で経営層に対して進言すると共に実務者を指揮できるような橋渡しを行う人材の育成・確保と、②経営層や現場、ステークホルダー間のコミュニケーションがあげられている。

このような要素についても、「経営・事業に関する役割」として示していくことが必要と考えられる。

1) 橋渡し人材の必要性、重要性と課題

文献２では、経営層と実務者層の橋渡しを行う人材である「橋渡し人材」の必要性を指摘している。一方、橋渡し人材が必要だと認識している企業のうち、7 割の企業は不足しているとしており、橋渡し人材の確保が課題とされている。この結果に対し、NISC「次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方」（決定）の「資料 1-2 次期サイバーセキュリティ戦略の検討に関する検討事項等について」[5]においては、「セキュリティマインドを持った企業経営の推進」の課題として、以下の役割を担う「橋渡し人材層」の育成があげられており、橋渡し人材の育成と確保の重要性を指摘している。

- 経営層の示す経営方針を理解する
- サイバーセキュリティに係るビジョンを提示する
- 実務者層との間のコミュニケーションの支援を行う

また、IPA の昨年度調査（前述）では、CISO 等の役割のうち「経営層との橋渡し」について、米国・欧州では今後重要性が高まると認識されている一方、日本では今後も重要性が高まると認識されていないことが分かった。

CISO 等には事業を理解した上で、経営層と現場をつなぐ「橋渡し人材」としての役割が求められると考えられる。しかし、現状ではこの役割を担う人材が不足しており、日本ではまだ重要性が認識されていないことから、橋渡し人材の育成・確保や、橋渡し人材の重要性に対する理解の向上が課題になると考えられる。

2) 社内外コミュニケーションの必要性・重要性と課題

文献３の指示 10 において、情報共有活動への参加があげられており、CISO 等の役割として社内外とのコミュニケーションが求められている。また、IPA の昨年度調査（前述）では、CISO 等には社内外との「コミュニケーションスキル（経営層や現場、ステークホルダー等）」が求められるとの結果があった。

海外文献においてもコミュニケーション・社内調整の必要性、重要性が指摘されている。文献７では、経営・事業に関する役割までを担う CISO の役割として、社内外のステークホルダーとのコミュニケーション・調整が示されている。また文献４では、CISO の経営・事業に関する役割を遂行するための問題点として、社内においてコミュニケーションと協力が

[5] https://www.nisc.go.jp/conference/cs/dai16/pdf/16shiryou01.pdf （P12 参照）

取れていないことが指摘されている。

CISO 等が経営・事業に関する役割を遂行するためには、社内外との調整が必要な要素と考えられる。そのため、CISO 等が円滑に社内外とのコミュニケーションができるよう、CISO 等の個人のスキル・能力の育成だけではなく、社内外とのコミュニケーションが適切にできるような組織的な環境整備も必要になると考えられる。組織的な環境整備としては、外部のステークホルダーに対する情報提供の仕組み等が考えられる。

3) CISO 等が役割を十分遂行するための要件

CISO 等が役割を十分に遂行するための要件として、各文献では経営層からの権限委譲及び CISO 等の権限と責任の明確化が指摘されている。

文献１では、CISO は役員である必要はなく、CISO がその任務を果たすことができる権限が経営トップから委譲されていればよいとしている。また文献２においても、CISO 等にあたる「橋渡し人材層」がその役割を十分に遂行できるよう、「権限」と「責任」を明示する必要があることが指摘されている。さらに文献３では、「経営者は、CISO 等に対して、以下の 10 項目を指示し、着実に実施させるとともに、 実施内容について CISO 等から定期的に報告を受けることが必要である」と言及しており、CISO 等がその役割を十分に果たすためには経営層からの権威付けや支援が必要になると考えられる。

また CISO 等がその役割を十分果たせない理由として、文献４では、サイバーリスクは技術的な問題だと考えられていること、マネジメントに関する訓練が不足していること、事業を理解した上でサイバーリスクを捉えられないこと等を指摘している。また文献９は、CISO 等が役割を十分に果たせない理由として、セキュリティに投資する際に、リスク要素を特定し、経営戦略や事業の方向性に照らして対応の優先順位をつけることができていない点を指摘している。

CISO 等が経営・事業に関する役割を遂行するためには、経営者から任命され、必要な権限と責任が明確にされていること、CISO 等が経営戦略や事業戦略・内容を理解した上で、セキュリティリスクを特定し、投資まで結びつける役割を果たすことが必要と考えられる。

2.3 CISO 等の経営・事業に関する役割の国内外文献調査

2.3.1 産業横断サイバーセキュリティ人材育成検討会「第一期最終報告書 第 1.0 版」[6]、「第一期最終報告書 第1.0版付A3 産業横断 人材定義リファレンス ～機能と業務に基づくセキュリティ人材定義～」[7]2016.9.14（文献 1-1）、「第二期中間報告書 第 1.0 版」[8]2017.11.21（文献 1-2）

産業横断サイバーセキュリティ人材育成検討会「第一期最終報告書 第 1.0 版」は、「産業横断サイバーセキュリティ人材育成検討会」の 2015 年 6 月から 2016 年 6 月までの活動内容をまとめた報告書で、人材育成の観点から CISO 等のサイバーセキュリティ人材に関す

[6] http://cyber-risk.or.jp/sansanren/xs_20160914_01_Report_1.0.pdf (2018.2.15 参照)

[7] http://cyber-risk.or.jp/sansanren/xs_20160914_A1_Report_JinzaiTeigiReference_1.0.pdf (2018.2.15 参照)

[8] http://cyber-risk.or.jp/cric-csf/report/CRIC-CSF-2nd-Interim-Report.pdf(2018.3.27 参照)

る取組内容及びその成果が報告されている。また、「第一期最終報告書 第 1.0 版 付 A3 産業横断 人材定義リファレンス ～機能と業務に基づくセキュリティ人材定義～」は、「産業横断サイバーセキュリティ人材育成検討会」の成果物としてとりまとめられたもので、日本のユーザ企業における情報システム部門をスコープに、必要となるサイバーセキュリティ機能を洗い出し、それらの機能を実現する業務とそれを担う各種役割（担当）の要求知識と業務区分について整理したものである。

「第一期最終報告書 第 1.0 版 付 A3 産業横断 人材定義リファレンス ～機能と業務に基づくセキュリティ人材定義～」では、「サイバーセキュリティ対策統括」機能に責任を負う役割として CISO/CRO/CIO 等を位置づけ、その役割を「機能」と「機能を実現する業務」で定義している。CISO/CRO/CIO 等に求められる主な機能としては、サイバーセキュリティ統括の機能に対して業務責任を負う他、 IT 戦略やシステム企画、事業継続、セキュリティ対策に関して、業務責任者を支援・補佐することと定義している。

表 2.3-1 CISO/CRO/CIO 等のサイバーセキュリティに関する機能定義

主な機能概要	セキュリティ機能定義	サイバーセキュリティ対策機能を実現する業務(例)	業務区分
全体統括管理	サイバーセキュリティ統括	サイバーセキュリティ対策に関する全社的統括	5（業務責任を負う）
IT 戦略	事業戦略 中期計画	コンプライアンス、ガバナンス及びリスクマネジメントの観点に基づくセキュリティ対策	4（業務責任者を支援・補佐する）
	年次計画	セキュリティ対策に係る実施計画の企画立案 規程・ルールの策定	4
	ICT 企画 （個別 IT 企画）	各事業に対する IT 導入・構築運用改善計画の企画立案 ガイドライン・マニュアルの策定	4
		ライセンス管理を踏まえた、リプレース計画の企画立案 固定資産管理・ソフトウェア会計管理	4
システム企画	セキュリティ実装計画	ユーザビリティの観点に基づく機能改善・実装計画の企画立案 エンドポイント及び UI に関するセキュリティ機能改善計画の策定	4
		システムセキュリティの観点に基づく機能改善・実装計画の企画立案 システム構成に関するセキュリティ機能改善計画の策定	4
事業継続	IT-BCP	ICT 環境における事業継続計画の策定 サイバーセキュリティ保険の導入検討	4
セキュリティ対策	ディザスタリカバリ	災害対策（DR）に関する ICT 環境改善計画の策定	4
		災害対策及び災害発生時に関する稼働計画の策定	4
	情報セキュリティマネジメント	情報資産保護活動における ICT 環境改善計画の策定 情報資産の保護基準・保護方法の改善、情報漏洩保険の導入検討	4
		情報資産保護活動における ICT 運用改善活動の策定 情報資産の棚卸	4

出所）産業横断サイバーセキュリティ人材育成検討会「第一期最終報告書第 1.0 版 付 A3 産業横断 人材定義リファレンス ～機能と業務に基づくセキュリティ人材定義～」 より一部抜粋

産業横断サイバーセキュリティ人材育成検討会「第一期最終報告書 第 1.0 版」では、CISO の位置づけについて検討会で行われた議論の観点の一つとして、「CISO はその企業の情報セキュリティ対策を実施する上での責任者であればよいので役員である必要はない。」「CISO がその任務を果たすことができる権限が経営トップから委譲されていればよい。」ということが取り上げられている（文献 1 -1 P.34 参照）。また CISO 等には、インシデント発生時に SOC 等の技術的部門からの技術的情報を、経営層が経営判断するために理解でき

るよう翻訳する役割が求められるとしている（文献 1-1 P.36 参照）。さらに同文献で、営業秘密等の重要情報をサイバー攻撃から守る体制を整えることにより、将来的には日本の産業競争力が高められるとし、そのためには CISO 等のセキュリティの全体統括を担う CISO を支える専門部署（同文献では、「サイバーセキュリティ統括（室等）」）の設置が必要としている（文献 1-1 P.49 参照）。

CISO 等はサイバーセキュリティ統括の責任者として、技術的役割に加え経営・事業的役割を担う必要があると考えられる。そして、その業務を遂行するためには、経営者から任命され、必要な権限と責任が明確にされていることが必要な要素になると考えられる。

「第二期中間報告書 第 1.0 版」（文献 1-2）は、2016 年 7 月から 2017 年 9 月までの活動内容に関する中間報告書である。このなかで主要な検討ポイントの一つとして、セキュリティ統括人材像の明確化と育成に向けた研修プログラムの整備を挙げている。

経営的な知見とサイバー攻撃やネットワークインフラ等の専門的な知見を有して、経営を支援しながら関係部署をリードする「セキュリティ統括人材」の育成が急務であり（文献 1-2 P6）、経営に基づいたセキュリティに関する意思決定およびその実行を支援することのできる“セキュリティ統括人材”の重要性はますます増している（文献 1-2 P10）、としている。

2.3.2 NISC「サイバーセキュリティ人材育成プログラム」2017.4.18（文献 2）[9]

企業をはじめとする社会で活躍できるサイバーセキュリティに関連する人材育成の方向性を示すことにより、安全な経済社会の活動基盤としてのサイバー空間の形成に向けた環境整備を図ることを目的にまとめられた報告書である。具体的には、産学官の連携により、サイバーセキュリティ人材の「需要」と「供給」の好循環を形成するため、サイバーセキュリティ人材を取り巻く課題を明らかにし、それに対する産学官の人材育成戦略の方向性を示している。

この文献では、経営層と実務者層の橋渡しを行う人材を「橋渡し人材」として定義し、その位置づけ、役割、必要とされるスキルを以下のように整理し、その必要性を指摘している。橋渡し人材には自社の経営戦略や事業を理解した上での、セキュリティ対策の推進が求められている。（文献 2　P.12,P.17）

表 2.3-2　橋渡し人材の位置づけ・役割・スキル

位置づけ	経営層の補佐的な役割を担う人材であり、経営層に対しセキュリティに関する課題と対応を進言するとともに、実務者層を指揮することができる人材
役割	自社の経営戦略や事業そのものについての深い理解と、サイバーセキュリティの素養を持つことを前提に、新しい IT を利活用したビジネス戦略と一体となったサイバーセキュリティ対策について企画・立案
スキル	IT を利活用した新しい価値の創出など経営・事業戦略的な視点、及び最新のサイバーセキュリティに関する知識・能力

[9] https://www.nisc.go.jp/active/kihon/pdf/jinzai2017.pdf　(2018.2.15 参照)

	最新のサイバーセキュリティの知識について、組織を超えた連携等による手段で高めておくことが期待される

また、橋渡し人材の確保について、NISC のアンケート調査によると、橋渡し人材が必要だと認識している企業のうち、7 割の企業は不足しているとの認識を持っており、人材の確保を課題としてあげている。また、橋渡し人材がその役割を十分に遂行できるよう「権限」と「責任」を明示する必要があるとしている。（文献 2　p.12）

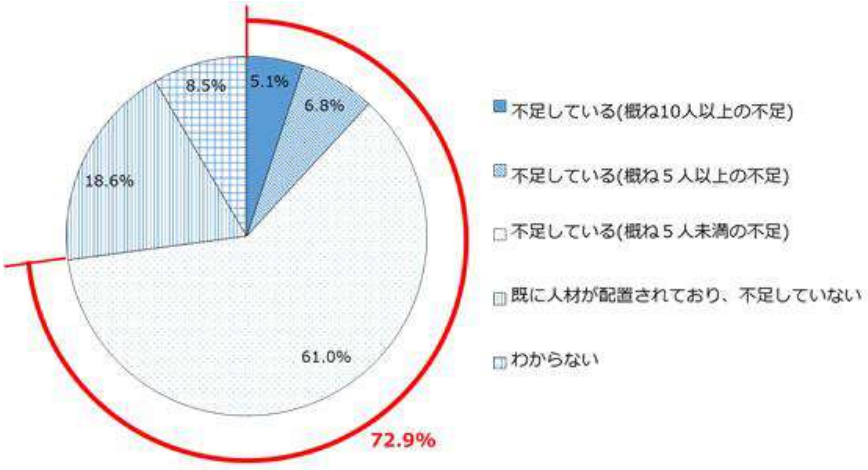

図 2.3-1　橋渡し人材層の必要性

出所）内閣サイバーセキュリティセンター「サイバーセキュリティ人材育成プログラム」

CISO 等には自社の事業を理解した上でセキュリティの取組を推進すること、経営層と現場をつなぐ「橋渡し人材」としての役割が今後求められると考えられる。現状ではこの役割を担う人材は不足しているため、橋渡し人材の育成・確保が課題になると考えられる。

2.3.3 経済産業省／IPA「サイバーセキュリティ経営ガイドライン Ver.2.0」2017.11.16（文献 3）[10]

IT に関するシステムやサービス等を供給する企業及び経営戦略上 IT の利活用が不可欠である大企業及び中小企業の経営者を対象として、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある「3 つの原則」と経営者が CISO 等に指示すべき「重要 10 項目」をまとめた、サイバーセキュリティ対策推進のためのガイドラインである。2015 年 12 月に第 1 版が公開され、2017 年 12 月に第 2 版が公開された。

同ガイドラインで示された CISO 等に指示すべき「重要 10 項目」の多くが経営・事業的役割に関連すると考えられるため、CISO 等の経営・事業的役割を検討する上で参考となる。また、同ガイドラインでは、セキュリティポリシーの策定や体制の整備に加え、セキュリティインシデントの発生を想定した事業継続計画の策定や外部ステークホルダーとのコミュニケーションの必要性について言及している。

[10] http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf　(2018.2.15 参照)

表 2.3-3　CISO 等に指示すべき重要 10 項目

指示	実施内容
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リスクを経営リスクの一つとして認識し、組織全体での対応方針（セキュリティポリシー）を策定させる。
指示 2　サイバーセキュリティリスク管理体制の構築	サイバーセキュリティ対策を行うため、サイバーセキュリティリスクの管理体制（各関係者の責任の明確化も含む）を構築させる。その際、組織内のその他のリスク管理体制とも整合を取らせる。
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	サイバーセキュリティリスクへの対策を実施するための予算確保とサイバーセキュリティ人材の育成を実施させる。
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	経営戦略の観点から守るべき情報を特定させた上で、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、リスクに対応するための計画を策定させる。その際、サイバー保険の活用や守るべき情報について専門ベンダへの委託を含めたリスク移転策も検討した上で、残留リスクを識別させる。
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リスクに対応するための保護対策（防御・検知・分析に関する対策）を実施する体制を構築させる。
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	計画を確実に実施し、改善していくため、サイバーセキュリティ対策を PDCA サイクルとして実施させる。その中で、定期的に経営者に対策状況を報告させた上で、問題が生じている場合は改善させる。また、ステークホルダーからの信頼性を高めるため、対策状況を開示させる。
指示 7　インシデント発生時の緊急対応体制の整備	影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を速やかに実施するための組織内の対応体制（CSIRT 等）を整備させる。被害発覚後の通知先や開示が必要な情報を把握させるとともに、情報開示の際に経営者が組織の内外へ説明ができる体制を整備させる。また、インシデント発生時の対応について、適宜実践的な演習を実施させる。
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	インシデントにより業務停止等に至った場合、企業経営への影響を考慮していつまでに復旧すべきかを特定し、復旧に向けた手順書策定や、復旧対応体制の整備をさせる。 BCP との連携等、組織全体として整合の取れた復旧目標計画を定めさせる。また、業務停止等からの復旧対応について、適宜実践的な演習を実施させる。
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	監査の実施や対策状況の把握を含むサイバーセキュリティ対策の PDCA について、系列企業、サプライチェーンのビジネスパートナーやシステム管理の運用委託先等を含めた運用をさせる。システム管理等の委託について、自組織で対応する部分と外部に委託する部分で適切な切り分けをさせる。
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	社会全体において最新のサイバー攻撃に対応した対策が可能となるよう、サイバー攻撃に関する情報共有活動へ参加し、積極的な情報提供及び情報入手を行わせる。また、入手した情報を有効活用するための環境整備をさせる。

出所）経済産業省/IPA「サイバーセキュリティ経営ガイドライン Ver.2.0」　に基づき MRI 作成

2.3.4 Deloitte, ”The new CISO - Leading the strategic security organization” 2016（文献 4）[11]

CISO に求められる 4 つの顔を「技術者」・「監視者」・「アドバイザー」・「戦略家」の 4 つに分類し、それぞれに求められる役割と、現在の業務比率と今後望ましいと考えられる業務比率を整理した報告書である。

この文献では、CISO の顔として、現在はコンプライアンス要件を満たしながら、サイバー脅威の監視、撃退、及び対応する「技術者」と「監視者」が重要視されているが、今後は事業内容の方向性に応じ情報セキュリティ戦略を確立するための、「アドバイザー」と「戦略家」の顔が求められるとし、経営・事業的役割が重視されるとしている。

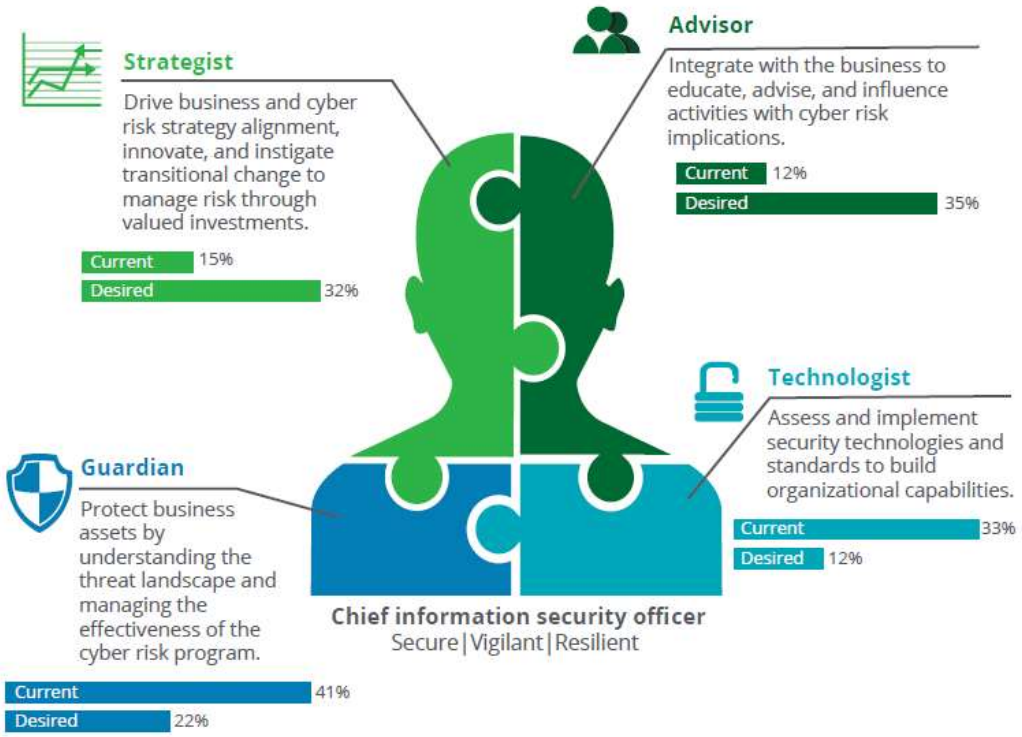

図 2.3-2　CISO の 4 つの顔

出所）Deloitte, ”The new CISO - Leading the strategic security organization”

また、同文献では、CISO に係る現状の問題点について、CISO を含むセキュリティ組織と事業部門に分けて 5 つに整理し、それぞれに対する解決策を提示している。

CISO は各事業のサイバーリスクを理解した上で事業決断を支援する役割を担うが、現状この役割を遂行するために問題を抱えているとしている。CISO が事業決断を支援する役割を遂行するためには、社内外との調整が不可欠であり、そのためには CISO 等が円滑に社内外とのコミュニケーションができるよう、スキル・環境作りが必要になると考えられる。

[11] https://www2.deloitte.com/content/dam/insights/us/articles/ciso-next-generation-strategic-security-organization/DR19_TheNewCISO.pdf (2018.2.15 参照)

表 2.3-4　CISO に係る現状の問題点と解決策

	問題点	理由	解決策
セキュリティ組織側	視野の狭隘	マネジメントに関する訓練を受けたことがない	• 軸をセキュリティからリスクに置き、事業全体に関する議論を促進する • リスクを新しいビジネスチャンスとして捉える
	コミュニケーションと協力	サイバーリスクはただの技術問題と捉えられている	• 多機能型のチームを構築する • 行動や考えを伝えるコミュニケーション環境を作る • 複数のコミュニケーションチャネルを確保する
	能力の欠落	チームメンバーの人数と経験が足りない	• チームスキルを高める • リスクの高いシナリオにおける訓練を実施する • リーダーシップポテンシャルを育てる
事業部側	セキュリティに対する誤解	セキュリティ＝コンプライアンスという誤解が多い	• 現在のリスクレベルを可視化する • コンプライアンスとサイバーリスク管理の違いを教育する
	競合する課題	成長戦略とサイバーリスクとはつながりにくい	• 事業を詳しく理解し、戦略家とアドバイザーになる • 事業の優先度に応じるリスク計測基準を提供する • 共有責任を促進するために感情のつながりを作る

出所）Deloitte, ”The new CISO - Leading the strategic security organization”に基づき MRI で作成

2.3.5 Info-communications Development Authority of Singapore , “National Infocomm Competency Framework NICF, NICF Overview Map, Horizontals, Infocomm Security, Security Management, Chief Information Security Officer, Job Role & Competencies”[12] 2009, 2011（文献 5）

シンガポールの IDA が策定した、CISO 等に求められる役割と知識等についてまとめた報告書である。

同文献では、CISO 等の責任範囲と要求スキル・経験が整理されており、CISO 等の責任範囲の中には、情報セキュリティ戦略・リスクマネジメント戦略と事業戦略との整合を求めている。また、要求スキル・知識としては IT だけではなくビジネスプロセスに対する理解も求めており、技術的役割だけではなく経営・事業的役割も求めている。

[12] https://www.imda.gov.sg/nicf/framework/job-roles/chiefinformationsecurityofficer　(2018.2.15 参照)

表 2.3-5　CISO 等の責任範囲と要求スキル・経験

責任範囲	要求スキル・経験
• 企業の情報セキュリティ分野におけるリーダーシップの提供 • 情報セキュリティポリシー・標準・手順の策定 • 予算及び資本、運用支出の管理 • 情報セキュリティ及び情報リスクマネジメント戦略をレビューし、承認を取得し、事業戦略と整合するよう調整する • 情報セキュリティに関して経営陣のサポートを獲得し、全体的な情報セキュリティリスクについて責任を担う	• 情報セキュリティに関連した分野での少なくとも 10 年のマネジメント経験 • セキュリティポリシー及び手順に関する知識 • IT とビジネスプロセスに関する理解と、それらの関係性に関する理解 • 複数の組織や多面的なチームと連携して、セキュリティポリシーと手順を策定、実施、監視する能力 • コンピュータサイエンス、情報システム、工学に関する学位または同等の知識

出所）Info-communications Development Authority of Singapore , “National Infocomm Competency Framework NICF, NICF Overview Map, Horizontals, Infocomm Security, Security Management, Chief Information Security Officer, Job Role & Competencies”　に基づき MRI 作成

同文献で示されている 18 の役割は下表の通りで、その役割を遂行する上での具体的な取組内容や、求められるスキル・知識等が整理されている。CISO 等が役割を遂行する上で参考になると考えられる。

表 2.3-6　CISO 等に求められる役割一覧

役割	
IT-CIO-401S-1	戦略策定への貢献（Contribute to the development of a strategy plan）
IT-CIO-405S-1	事業に関する技術モデルの選択（Select new technology models for business）
IT-CIO-502S-1	予算策定（Develop a budget）
IT-CIO-503S-1	戦略及び行動計画策定（Develop strategic and action plans）
IT-CIO-506S-1	企業の事業戦略における IT ニーズとの整合（Align the IT needs with the strategic direction of the enterprise）
IT-CIO-508S-1	ビジネスイノベーションの特定と実行（Identify and implement business innovation）
IT-CIO-515S-1	IT 投資のビジネス価値の最大化（Maximise business value of IT investments）
IT-CIO-517S-1	ビジネスソリューションプロバイダーに対するリスク評価と計画（Review and plan for risk to business solution providers）
IT-CIO-518S-1	変更管理プロセスの実装（Implement change management process）
IT-CIO-601S-1	適切な IT 戦略及びソリューションの決定（Determine appropriate IT strategies and solutions）
IT-PM-405S-1	プロジェクトコスト管理（Manage project costs）
IT-PM-406S-1	プロジェクトリスク管理（Manage project risk）
IT-PM-503S-1	プロジェクト監督（Direct projects）
IT-PM-507S-1	プロジェクト成功のためのステークホルダーマネジメント（Manage stakeholders for project success）
IT-SM-407S-1	コンプライアンスへの理解と適用（Understand and apply compliance standards）
IT-SM-502S-1	情報セキュリティプログラム投資をサポートするビジネスケースの策定（Develop business case that support information security program investments）
IT-SM-601S-1	情報セキュリティ目標の確立（Formulate information security goals and objectives）
IT-SM-602S-1	情報セキュリティ全体のリスクマネジメント（Manage overall information security risk）

出所）Info-communications Development Authority of Singapore , “National Infocomm Competency Framework NICF, NICF Overview Map, Horizontals, Infocomm Security, Security Management, Chief Information Security Officer, Job Role & Competencies”　に基づき MRI 作成

上記の役割のうち、経営・事業的役割に関連するものの一例として、

・　企業の事業戦略における IT ニーズとの整合

・　IT 投資のビジネス価値の最大化

の 2 つの役割について、同文献で示されている具体例、スキル・知識を以下に示す。

表 2.3-7　役割に関する具体例/スキル･知識

役割	役割に関する具体例	スキル・知識
企業の事業戦略における IT ニーズとの整合	1. 業界環境及び現行の組織目標に関連して組織戦略計画を分析する。 2. 可能な IT ギャップと改善の機会を判断するために現在の運用実務と戦略計画に関連する情報を比較する。 3. 現在及び提案されている IT システムを見直し、変更の影響を評価する。 4. 組織的ガイドラインに従い、実施できる行動計画を策定する。	＜必要とするスキル・知識＞ 1. ベンダと技術動向を評価･予想するために必要となる技術と製品の方向性に関する知識を有する。 2. 組織の戦略方向性を理解する。 ＜土台となる知識＞ 1. 戦略計画スキル 2. 現在のシステム機能 3. IT 戦略計画要素の俯瞰図 4. ビジネスケースの準備 5. 戦略的環境の分析
IT 投資のビジネス価値の最大化	1. 特定の財務要件に基づき IT 資産のビジネスケースを確立する。 2. エンタープライズ･アーキテクチャを参照し IT 投資を調整する。 3. 構造化された方法論をシステム開発に適用する。 4. サービスレベルが確実に達成されるように正式な運用管理方法を開発する。	＜必要とするスキル・知識＞ 1. ベンダと技術動向を評価･予見するための技術及び製品の方向性に関する知識を有する。 2. 技術的問題や管理要件に対する分析と計画のアプローチを理解する。 3. 内部及び外部の経営環境を評価するための知識を有する。 4. 現在の業務慣行と将来の要件、及び IT 改革に関連する幅広い戦略計画スキルを有する。 ＜土台となる知識＞ 1. 費用便益分析 2. 現行の技術動向 3. システム開発の方法論 4. 運営管理

出所）Info-communications Development Authority of Singapore , “National Infocomm Competency Framework NICF, NICF Overview Map, Horizontals, Infocomm Security, Security Management, Chief Information Security Officer, Job Role & Competencies”　に基づき MRI 作成

2.3.6 NIST SP800-181 , “National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework” 2017.8（文献 6）[13]

サイバーセキュリティ分野に関連する人材に求められるスキルやタスク､知識等について、役割別にまとめたもの。CISO 等については明確に言及してはいないが、サイバーセキュリティに関する専門分野毎にその定義と役割が整理されており、CISO 等のタスク、スキルを検討する際の参考となる。

同文献で示されている役割のうち、CISO 等の役割として、「リスク管理」、「サイバーセキュリティ・マネジメント」、「プログラム/プロジェクト・マネジメント及びアクイジション」の他、法律面での支援や人材育成の専門分野が該当すると考えられる。

表 2.3-8 専門分野の定義と役割（ Securely Provision （SP） ）

専門分野	定義	役割
リスク管理（RSK）	• 既存及び新規の情報技術（IT）システムが組織のサイバーセキュリティ及びリスク要件を満たしていることを保証するために必要な、文書化、検証、評価、承認プロセスを監督、評価し、支援する。 • 内外の視点から、リスク、コンプライアンス、アシュアランスの適切な取り扱いを確保する。	• 組織の運営（ミッション、機能、イメージ、評判など）、組織の資産、各人材、その他の組織、国家について許容可能なレベルのリスクで情報システムを運用する責任を正式に請け負う。 • 情報技術（IT）システムで採用または継承された、マネジメント、運用、技術上のセキュリティ管理と管理強化について、独立した包括的評価を実施し（NIST SP 800-37 で定義されている）管理の全体的な有効性を判断する。

出所） NIST SP800-181 ,“National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework” に基づき MRI 作成

表 2.3-9 専門分野の定義と役割（ Oversee and Govern （OV））

専門分野	定義	役割
法的助言と政策提言（LGA）	• 関係する対象分野の様々な重要トピックについて、リーダーやスタッフに法的に確かな助言や推奨を行う。 • 法規や政策の変更を提言し、法的見解や訴訟手続きなど、書面や口頭によりクライアントに代わって論証を行う。	• サイバー法に関する重要トピックについて、法的な助言と推奨を行う。 • プライバシー・コンプライアンス・プログラムとプライバシー・プログラム・スタッフ（ガバナンス/ポリシー、コンプライアンス、インシデント対応/違反など）を展開、監督し、プライバシーやセキュリティ担当の役員及びそのチームのプライバシー・コンプライアンスに関するニーズをサポートする。
訓練、教育、啓発（TEA）	• 関係する対象分野で人材のトレーニングを行う。 • トレーニング・コース、手法、技術を適切に開発、計画、調整、提供し、評価を行う。	• 教育ニーズに基づいて、サイバー・トレーニング/教育コース、手法、テクニックを開発し、その計画、取りまとめ、評価を行う。 • サイバー分野の人材のトレーニングや教育を開発、実施する。

[13] https://www.hsdl.org/?view&did=802949 (2018.2.15 参照)

専門分野	定義	役割
サイバーセキュリティ・マネジメント（MGT）	• 情報システムやネットワークのサイバーセキュリティ・プログラムを監督する。 • 組織内の情報セキュリティの影響、特定のプログラム、その他の担当分野（戦略、人材、インフラ、要件、政策施行、エマージェンシー計画、セキュリティ啓発、その他のリソースなど）のマネジメントを含む。	• プログラム、組織、システムのサイバーセキュリティを担当する。 • 組織の通信セキュリティ（COMSEC）リソースを管理する。
戦略的計画と政策（SPP）	• 政策を展開し、組織のサイバースペース・イニシアチブや必要な変更/強化をサポートするための政策変更の計画、啓蒙を行う。	• サイバースペースの労働力計画、戦略、ガイダンスを展開し、サイバースペースの労働力、人材、トレーニングや教育要件のサポート、サイバースペースの政策、原則、構成要素、マンパワー構成、教育・訓練要件の変化に対処する。 • 組織のサイバースペース・ミッションとイニシアチブのサポートや、それと整合するためのサイバースペース計画、戦略、政策を展開する。
エグゼクティブ・サイバー・リーダーシップ（EXL）	• サイバー関連やサイバー・オペレーションの作業を行う作業員や作業の監督、管理及び指導を行う。	• 意思決定の権限を執行し、組織のサイバー及びサイバー関連のリソースやオペレーションのビジョンと方向性を確立する。
プログラム/プロジェクト・マネジメント及びアクイジション（PMA）	• データ、情報、プロセス、組織のやり取り、スキル、分析の専門知識、及びシステム、ネットワーク、情報交換機能に関する知識を活用し、アクイジション・プログラムを管理する。 • ハードウェア、ソフトウェア、情報システム・アクイジション・プログラム、その他のプログラム・マネジメント方針を管理する。 • IT 関連の法律や政策を適用し、情報技術（IT）（国家安全システムを含む）を用いるアクイジションを直接サポートし、アクイジション・ライフサイクル全体を通じて IT 関連のガイダンスを提供する。	• プログラムを主導し、調整し、コミュニケーションを取り、統合し、そのプログラムの全体的な成功に責任を負い、重要な機関や企業の優先事項との整合性を確保する。 • 情報技術プロジェクトを直接管理する。 • システムとコンポーネントをいつでも運用できるよう維持するために必要なサポート機能のパッケージを管理する。 • ミッションと企業の優先事項の全体的なニーズに合わせて IT 投資のポートフォリオを管理する。 • IT プログラムやその個々のコンポーネントの評価を実施し、公表されている規格の遵守を判断する。

出所）NIST SP800-181, “National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework” に基づき MRI 作成

2.3.7 Bill Bonney 他, “ CISO Desk Reference Guide: A Practical Guide for CISOs” 2016（文献 7）

CISO 及び CxO 等の CISO を任命・管理する立場の人を対象にした、CISO の役割やその役割を遂行する上で必要となる要素等を解説した文献。同文献では、CISO 等に技術的役割を重視する立場、経営・事業的役割を重視する立場等、著者の間でも CISO の立場について考えがやや異なる。

CISO の種類と求められる役割・特徴について、著者の一人である Hayslip 氏の整理によると、権限を有する CISO（The Empowered CISO）、すなわち経営･事業的役割までを担う CISO の役割として、以下の 6 点があげられている。CISO 等には、経営層や関係部署との調整等の社内のコミュニケーションに加え､社外とのコミュニケーションも求められるとしている。また、組織目標とセキュリティ目標を一致させ、セキュリティが事業推進を損なわないようにすることが求められている。

CISO 等には、経営戦略と整合させる形でのセキュリティの取組を推進させる経営・事業的役割が求められており、その役割を遂行する上では、社内外のコミュニケーションが重要になると考えられる。

表 2.3-10　経営･事業的役割までを担う CISO の役割

	CISO の役割
1	経営層がサイバーをリスクとして捉えるためには、サイバーセキュリティに関するリスク要因をドキュメント化・評価し経営層に共有する必要があり、そのためには CISO から CEO や CFO にレポートすることが重要（可能であれば定例の経営会議に CISO も参加）
2	CISO は IT 関連部署だけではなく、社内の関連する他部署（法務や契約等）や外部のステークホルダーに対する報告も必要
3	幅広い技術に関する深い知識や組織に関係するリスクマネジメント・プライバシー・法律・規制等に関する理解
4	組織の経営戦略・組織が扱う情報やデータ・事業ラインとステークホルダー・組織全体のリスク許容度に対する理解、社内調整スキルが求められる
5	非 IT メンバーとの頻繁なコミュニケーションを取り、組織目標やステークホルダーの目標、シャドーIT、鍵となるベンダ関係等の把握が必要
6	Empowered　CISO は組織目標とサイバーセキュリティ目標を一致させるように取組み、組織の事業の遅延や機敏性を損なわないようにすることが求められる

出所）Bill Bonney 他, “ CISO Desk Reference Guide: A Practical Guide for CISOs” に基づき MRI 作成

2.3.8 IT Capability Maturity Framework(IT-CMF) 2015（文献 8）

IT 管理における課題について、36 分野別に各分野の目的や目標、成熟度別に解説したもの。ここでは、36 の分野の中から CISO 等の役割に関わる「リスクマネジメント」と「情報セキュリティマネジメント」の概要に触れる。

リスクマネジメントは下表の通りで、事業目標や組織の意思決定に与える影響を明確にすることを目的としてあげており、自社事業に与えるマイナスの影響を低減することを重要視している。このことから CISO 等には、セキュリティリスクを低減する上で、自社の事業との関係を考慮することが求められると考えられる。

表 2.3-11　リスクマネジメントの目標・目的・価値・役割

項目	内容
目標	• IT リスクから組織を保護すること
目的	• IT 関連リスクの特定と評価（ビジネスにおける現在の脆弱性、適切なリスクハンドリング戦略の決定、それら効率性の評価） • IT 関連リスク（IT セキュリティ、IT サポタージュ、データ保護、プライバシー、製品やプロジェクトのライフサイクル、IT 投資）の管理とインシデント発生時に受ける影響からの組織の保護 • 外部規制や技術利用や展開に関連する倫理ポリシーに対応するよう、コンプライアンスの強化 • IT 関連リスクが事業目標や意思決定に与える影響を明確にする • 信頼されたサプライチェーンビジネスパートナーとして組織のレピュテーション改善に貢献する
価値	• リスクマネジメントを実施することにより、組織の事業運営に負の影響を与える IT リスクに関して、発生頻度と影響の深刻度を軽減
役割	• IT リスクマネジメントプログラム及びポリシーの策定 • リスクマネジメントに関する役割と責任の決定 • リスクマネジメントに関連するものとのコミュニケーションとトレーニング • 組織の IT リスク許容度の理解 • リスクプロファイルの特定 • 異なるタイプのリスクに対する評価と優先順位付け • 特定された IT リスクに対して、リスク対処方針（受容・回避・軽減・移転）を特定 • IT リスクのモニタリング • IT リスクマネジメントとエンタープライズマネジメント（BCP やディザスタリカバリ、情報セキュリティ、監査、保証）の統合

出所）IT Capability Maturity Framework(IT-CMF)に基づき MRI 作成

また、情報セキュリティマネジメントで求められる役割等は以下の通り整理されている。

表 2.3-12　情報セキュリティマネジメントの目標・目的・価値・役割

項目	内容
目標	• 組織の情報に対する損害からの保護や有害な利用の防止、正当な運用及びビジネス利用のために情報セキュリティマネジメントを実施
目的	• 組織の情報資産を保護するために、平時及び有事に備えた情報セキュリティアプローチやポリシー、管理策を策定する（CIA 及びユーザビリティ・利用可能性の観点から） • インシデント等を適切に調査し取り扱うために、全ての情報セキュリティインシデントやセキュリティ上の弱点が疑われるケースに関して、適切なチャネルで報告される体制を確立する • 情報セキュリティインシデントの発生頻度と影響の深刻度を最小化するために、従業員が適切なセキュリティ意識やスキルを維持できるよう支援する • 特定されたセキュリティリスクに関して、技術的分析や軽減策を実施し、残留リスクに関して鍵となるステークホルダーの承認を受ける
価値	• 情報セキュリティインシデントの発生頻度の低減と情報漏えい発生時の影響を制限する
役割	• 認証されていないアクセスや利用、情報開示、破壊、変更、デジタル化された情報資産の破壊からの保護 • 役割や責任、説明責任を含む情報セキュリティガバナンスモデルの構築 • 既存のセキュリティアプローチやポリシー、管理策の効率性評価 • セキュリティ関連のコミュニケーションの管理と従業員教育 • 情報セキュリティリスク及びインシデントの評価・優先順位付け・対応・監視 • 物理的な IT コンポーネントとエリアの保護 • 情報セキュリティ活動及びコンプライアンスレベルの報告

出所）IT Capability Maturity Framework(IT-CMF)　に基づき MRI 作成

2.3.9 SANS，”Mixing Technology and Business: The Roles and Responsibilities of the Chief Information Security Officer[14] 2003（文献 9）

CISO は IT セキュリティマネジャーとして、ビジネス面と技術面の役割を果たすために遂行すべき責任を 7 つあげている。

表 2.3-13　CISO の 7 つの責任

	CISO の責任
1	セキュリティ戦略に関する組織の代表者として、顧客、パートナー等に対応する。
2	組織の代表として行動し、社員によるネットワーク攻撃や情報盗難の原因を追求しながら、法執行機関と対処する。
3	組織の戦略的ビジネス計画とセキュリティニーズのバランスを調整し、リスク要因を特定し、ソリューションを選定する。
4	コアビジネス要件に沿う適切なビジネスアプリケーション保護を提供するセキュリティポリシー及び手順を開発する。
5	顧客、パートナー、または一般の人々との議論を含め、セキュリティ侵害への対応を計画し、テストする。
6	アウトソーシングにおけるセキュリティハードウェア及びソフトウェア製品の選定テスト、展開、保守を監督する。
7	組織のセキュリティ担当者を監督する。（ファイアウォールデバイスを管理するネットワーク技術者からセキュリティ委託会社まで）

また、CISO が責任をうまく果たせない理由として、セキュリティマネジメントにおいてリスク要素を特定し、優先順位を付け、セキュリティ投資を強化することができていない点を指摘しており、これを改善するためには、以下の要素を考える必要があるとしている。

要素 1：セキュリティ対策コスト

- ビジネスの規模、類型、特性を考慮する。
- コストは環境における脅威の大きさによるものなので、IT サービス業や大企業の方がコスト単価は高い。

要素 2：セキュリティ予算配分

- 有効性を考慮し、予算を配分する。
- 組織の IT 予算の 10.3%（2002 年は 9.5%）はセキュリティに使うという報告がある。

さらには、高い Return On Investment (ROI)（回収期間、正味現在価値（NPV）、内部利益率（IRR））を示し、経営層と交渉する必要があると指摘している。

[14] https://www.sans.org/reading-room/whitepapers/assurance/mixing-technology-business-roles-responsibilities-chief-information-security-officer-1044 (2018.2.15 参照)

2.4 CISO 等の教育プログラムに関する文献調査

2.4.1 EC-Council CISO Program, “Certified CISO Body of Knowledge”[15]（文献 10）

EC-Council が提供するトップレベルの情報セキュリティプロフェッショナルの認定を目的とした CISO 認定プログラムである。EC-Council は 2003 年に設立された機関で、セキュリティのプロフェッショナル人材について認定プログラムを提供していることで有名である。認定プログラムには、ホワイトハッカー（Ethical Hacker）やネットワーク技術者（Network Defender）、フォレンジック調査員（Forensic Anvestigator）等、様々な人材があり、CISO はそのうちの 1 つである。EC-Council はその他、関連するカンファレンスやコンサルティングサービス等も実施している。

同プログラムでは CISO に求められる知識と経験として下表の 5 分野をあげており、分野毎に具体的役割及び知識・スキルを定義している。（尚、「4.情報セキュリティに関するコアコンセプト」は技術的対策に関する内容が中心であるため、本報告書では割愛する）。

表 2.4-1　CISO に求められる知識と経験

	CISO に求められる知識と経験
1	ガバナンス
2	セキュリティリスクマネジメント及びコントロール、監査
3	セキュリティプログラムマネジメント及び運用
4	情報セキュリティに関するコアコンセプト
5	戦略策定及び予算、ベンダマネジメント

CISO の役割としては、組織の事業目標とセキュリティ関連施策の整合、外部のステークホルダー・経営層との調整、費用対効果の検証、リスクの許容等の判断をあげている。

表 2.4-2　「ガバナンス」に関する役割・スキル・知識

ドメイン	具体的役割	スキル・知識
ガバナンス	• リーダーシップ及び組織構造、プロセスを含む情報セキュリティガバナンスプログラムの策定・実装・管理・維持 • 情報セキュリティガバナンスフレームワークと組織の目標・ガバナンス（リーダーシップ、企業哲学、価値、標準、ポリシー等）との整合 • 情報セキュリティマネジメント組織の設立 • 情報セキュリティガバナンスのモニタリングフレームワークの構築（管理策導入による費用対効果や ROI を考慮） • コンプライアンスチームの管理 • 組織に適用可能な、全ての法規制や標準、ベストプラクティスの分析	• 情報セキュリティプログラムに影響を与える、標準や法規制等に関する理解 • 企業の情報セキュリティコンプライアンスプログラムに対する理解 • ISO27000 シリーズや、FIPS、FISMA、SOX 法等に対する知識 • 情報セキュリティの変化やトレンド、ベストプラクティスに対する理解 • 情報セキュリティ組織や適切な産業グループ、フォーラム、ステークホルダーの重要性理解 • 情報セキュリティコンプライアンスプロセスと手順に関する理解 • コンプライアンス監査及び認定プログラムに関する理解

[15] https://ciso.eccouncil.org/　(2018.2.15 参照)

ドメイン	具体的役割	スキル・知識
	• コンプライアンスに関する主要なエンタープライズリスク要因の評価 • 規制リスクを低減するための、情報セキュリティ戦略・計画・ポリシー・手順の調整 • 組織のコンプライアンスプログラム管理策の管理 • コンプライアンスプログラムの編集・分析･報告	• 組織倫理に従うこと

出所）EC-Council CISO Program, “Certified CISO Body of Knowledge”に基づき MRI 作成

表 2.4-3 「セキュリティリスクマネジメント及びコントロール、監査」に関する役割・スキル・知識

カテゴリー	具体的役割	スキル・知識
情報セキュリティ管理策	• 組織の運用プロセスと事業目標にあったリスク許容レベルの特定 • 組織の運用ニーズや目標に沿った情報システム管理策のデザイン及び管理策を実装前の、効率性・有効性の確認を目的としたテストの実施 • 情報システム管理策の効果的な実装と維持のために必要なリソース（人材、情報、インフラ、アーキテクチャ等）の特定と選択 • 予算と範囲に従い、情報システム管理プロセスを適切なタイミングで実装することを監視し、進捗状況をステークホルダーに報告 • リスクを軽減するよう情報システム管理策を設計し実装 • 情報システム管理策の運用状況について、KPI を設定して評価し文書化 • 効率性や不足事項、組織のポリシーや標準、手順との整合性を確保するために、情報セキュリティ管理策を設計しテストを実施 • 不足事項を適切に修正し、課題管理（適切なタイミングで課題を解決できるように課題を記録し分析）状況を把握できるようなプロセスの設計と実装 • 情報システム管理策を自動化できる技術やツールの評価と実装 • 情報システムの運用やメンテナンス、組織の戦略や目標との整合状況等に関するレポートを作成し、経営層の意思決定をサポートし関連するステークホルダーへ共有	
監査管理	• 情報システム技術の評価とテストを実施するにあたり、情報システム監査の原理やスキル、技術の応用及び、リスクベースの IT 監査戦略に基づいた設計と実装 • 確立された標準に基づいた監査プロセスを実施し、情報システムが組織の目標を支援する上で保護・管理され効率的であることを保障するために、定義された基準に基づき結果を解釈する • 監査結果を効果的に評価し、累積された監査証拠との関連性、正確性を評価する • 管理策が不十分または不足している箇所について、これらを改善するための、費用対効果を考慮した対策を検討 • IT 監査の文書化プロセスを構築し、意思決定の基本となる	• IT 監査のプロセス･IT 監査標準に対する理解

カテゴリー	具体的役割	スキル・知識
	関連するステークホルダーに共有する • 監査結果を基に必要な対策を適切なタイミングで実装	

出所）EC-Council CISO Program, “Certified CISO Body of Knowledge”に基づき MRI 作成

表 2.4-4　「セキュリティプログラムマネジメント及び運用」に関する役割・スキル・知識

ドメイン	具体的役割	スキル・知識
セキュリティプログラムマネジメントと運用	• 各情報システムプロジェクトに関しては、組織の目的と整合するようスコープを明確にする • 情報システムプログラムを成功させるために必要な活動や活動期間の推計、スケジュールや人員計画の策定 • 情報システムプログラム予算の起案及び管理、各プロジェクトの管理コストの推定 • 情報システムプログラムを効果的に設計実装するために必要となるリソースの特定、交渉、獲得、管理 • 情報セキュリティプロジェクトチームの設立と管理 • 情報セキュリティ担当者の役割の明確な付与、効果的な運用と説明責任を保障するための、継続的な訓練の提供 • 情報セキュリティ担当者への指示及びコミュニケーションの確立、情報システムチームと他のセキュリティ関連担当者の連携 • 時間やコスト、能力等の担当者やチームに関する課題の解決 • ベンダとの合意及びコミュニケーションの特定、交渉、管理 • 推奨されるソリューションの評価検証（提案されたソリューションの課題や不適合性等を検討）に関してベンダ及びステークホルダーともに参加 • 組織のリスク管理の実施中に、コスト効果の高い方法でビジネス上の要求を達成できているか、プロジェクトマネジメントプラクティス及びコントロールを評価する • 最適なシステムパフォーマンスを確保するための効果的な情報システムプロジェクトを遂行するために、継続的な対策計画を検討 • ステークホルダーの特定、ステークホルダーの期待管理、ステークホルダーに対する進捗・運用状況の効果的な報告 • 必要に応じて情報システムプロセスの必要な変化と改善を実施する	• 特に明示的な記載はなし

出所）EC-Council CISO Program, “Certified CISO Body of Knowledge”に基づき MRI 作成

表 2.4-5 「戦略策定及び予算、ベンダマネジメント」に関する役割・スキル・知識

カテゴリー	具体的役割・スキル	スキル・知識
戦略策定	• ビジネスプロセスや ITSW/HW、LAN/WAN、人、運用、プロジェクトを全社のセキュリティ戦略に基づくよう、企業の情報セキュリティアーキテクチャ（EISA）を設計・構築・維持する • 組織の外部環境（顧客・競合・市場・産業環境等）及び内部環境（リスクマネジメント・組織としての能力・経営指標等）を分析し、情報セキュリティプログラムを組織の目標と整合させる • 組織の目標を理解するために、キーステークホルダーを特定し協議する • 組織の運用ニーズをサポートするような明確な目標を有する情報セキュリティプログラムについて、将来性のある革新的な戦略計画を策定する • KPI を設定し継続的に効果を評価する • IT 投資が組織の戦略目標をサポートできているかを検証し、調整する • 説明責任と進捗状況を把握するために、活動を監視し更新する	
財務	• IT 部門の運営予算について、分析・予想し、計画を立てる • 情報セキュリティ計画を実装・管理するために必要なリソースを獲得し管理する • 情報セキュリティプログラムに係る、プロジェクト、プロセス、ユニットに対して予算を配分する • 戦略計画との整合を確保するために、情報セキュリティプロジェクトのコスト管理、IT インフラストラクチャ及びセキュリティに関連する重要な購入品の ROI を確認する • 財務指標を確認し、ステークホルダーに報告する • EISA に基づく IT セキュリティ投資のポートフォリオと組織のセキュリティ優先事項とのバランスを取る • 取得物のライフサイクルを理解し、ビジネスインパクト分析を実施して調達の重要性を判断する • IT セキュリティ製品やサービスの調達に関連する多様なステークホルダー（内部顧客、法律家、IT セキュリティプロフェッショナル、プライバシープロフェッショナル、セキュリティエンジニア、サプライヤー等）と協力する • 買収計画や費用推計、契約、SLA、調達関連文書の評価要素に、リスクベースの IT セキュリティ要求事項を含めるようにする • ベンダ選定プロセス及び管理ポリシーの設計 • 契約に基づき納品された IT セキュリティ製品・サービスの評価及び受け入れ基準を定めた、契約管理ポリシーを作成する • SOW やその他適切な調達に関する文書を含む IA セキュリティ要求事項を理解する	• 異なる調達戦略を把握し、情報システムの調達時における費用便益分析の重要性を理解する • SOO(Statement of objectives)や SOW(Statement of Work)、TOC(Total cost of ownership）といった、基本的な調達コンセプトを理解する

出所）EC-Council CISO Program, “Certified CISO Body of Knowledge”に基づき MRI 作成

2.4.2 カーネギーメロン大学 Heinz 校　CISO 認定プログラム[16]（文献 11）

カーネギーメロン大学では、サイバーリーダーに求められるスキルを育成する CISO 認定プログラムを、同大学のソフトウェアエンジニアリング研究所（SEI）の CERT プログラムと協力し、2012 年 9 月に立ち上げている。SEI は、米国国防総省の後援を受け、連邦政府の研究開発センターとして同大学が運営しており、CERT プログラムは SEI におけるセキュリティの研究、分析、トレーニングの中核を担っている。カリキュラムは最新の情報セキュリティアプローチや成功するサイバーセキュリティプロジェクトの設計と実装を想定した実習で構成されている。また、同プログラムでは、大学の専門教員による指導や最新事例の紹介、プログラム参加者との意見交換等を実施している。

プログラムを構成する 14 のカリキュラムは下表の通りで、前述の EC-Council と共に具体的な指針になると考えられる。

表 2.4-6　CISO 認定プログラムのカリキュラム

カリキュラム名	概要
Cyber Risk Management	サイバーセキュリティに関するガバナンスと戦略計画の現状、リスクマネジメントフレームワーク、規制、セキュリティ評価基準を利用し、事業に対する影響の議論を行う講義。
Enterprise Security Governance & Planning	運用リスクとサイバーセキュリティリスクのマネジメント（実際の戦略目標を使い、特定のビジネスゴール、可能な問題、指標、実行可能な評価基準を展開）、経営層との有効なコミュニケーション手段に関する講義。
Security Metrics & Operational Resilience	リスクマネジメント（情報セキュリティ、システム開発、事業継続性、IT オペレーション等）に関する講義。
External Dependency Management	レジリエンスの概念（運用・管理・関連事項や課題等）の理解や、組織のセキュリティやレジリエンスを確保するための手法について学ぶ。
Security Structure & Operations	組織のセキュリティプログラムに関して、①セキュリティチームとのコミュニケーション②組織目標との整合③セキュリティ対策のメリット④セキュリティ対策コスト⑤目標への進捗状況の観点から学ぶ。
Security Financial Management	予算を策定し、支援を得る方法に関する講義。
Effective Communication Strategies	情報漏えい等、組織の運営に大きく影響を与えるインシデントが発生した際の社内外とのコミュニケーション戦略に関する講義。
Security Strategy & Innovation	フレームワーク、アプローチ、及び方法論等の戦略開発の基礎的な視点を学び、企業の生存を脅かす「パワーシフト」を議論し、デジタル化等組織の戦略策定に影響を与えるものについて学ぶ。
Threat & Incident Response	CSIRT の構築、維持、運用における共通の課題を理解し、インシデント対応プロセスやフレームワーク等のツールを利用し、マネジメントする方法を学ぶ。

[16] https://www.heinz.cmu.edu/programs/executive-education/chief-information-security-officer-certificate (2018.2.15 参照)

カリキュラム名	概要
Managing Operational Threat	運用上の脅威に対処する際の CISO の役割と責任を理解し、管理及び技術的対策方法を学ぶ。
Building an Insider Threat Program	組織が内部脅威の可能性を効果的に緩和するプログラムを構築するため、内部犯行に対する技術的、行動的、組織的問題に対応するポリシー、手順、技術を学ぶ。（従業員の意識向上を含む。）
Cyber Law & Compliance	セキュリティインシデントに関連する法規制についてケーススタディ等を基に学ぶ。
A Realistic View of Security Technology	現在のセキュリティ保護技術や組織の能力と欠点を理解し、攻撃者の動機やパターンを分析する。
Digital Transformation: Security Implications	デジタル化によって激変した 4 領域における企業のケーススタディを通じ、セキュリティに関する影響を評価し、フレームワークを構築する。

3. CISO 等セキュリティ推進者の経営・事業に関する役割についての有識者調査

3.1 調査概要

CISO 等が担うべき重要な役割、日本の CISO 等の役割上の課題等について、国内外の有識者を対象としたインタビュー調査を実施した。

インタビュー調査の概要は下表に示す通りである。

表 3.1-1　有識者調査の概要

調査対象・件数	・　国内有識者（セキュリティ関連の企業団体リーダー、セキュリティコンサルティング会社幹部、計 3 名） ・　海外の有力セキュリティ関連団体　1 団体、計 2 名 ・　CISO 認定プログラムを有する海外大学のプログラム責任者 1 名
主な質問項目	＜国内有識者＞ ・　CISO 等に求められる経営・事業的役割 ・　日本企業における CISO 等の課題 ・　CISO 等が経営・事業的役割を遂行する上での課題・ポイント ・　CISO 等に経営・事業的役割を重要視している企業の特徴 ・　CISO 等が経営･事業的役割を果たすのに必要なスキルと習得方法、キャリアパス ・　経営者に CISO 等における経営･事業的役割の重要性を理解してもらうための方法 ＜海外の有力セキュリティ関連団体＞ ・　欧米企業の CISO 等に求められる経営・事業的役割 ・　CISO 等に経営・事業的役割を重要視している企業の特徴 ・　CISO 等が経営･事業的役割を果たすのに必要なスキルと習得方法、キャリアパス ・　経営者に CISO 等における経営･事業的役割の重要性を理解してもらうための方法 ・　欧米企業における CISO 等の課題 ＜海外大学の CISO 認定プログラム責任者＞ ・　CISO 育成プログラムが想定している CISO のロールモデル ・　CISO 育成プログラムの概要 ・　CISO 育成プログラムの設計思想・背景 ・　CISO 等人材を育成する上での課題

本章は、まず最初の節で有識者調査全体から得た知見・考察等をまとめ、以降の節で、国内の有識者、欧米の有識者、海外大学の有識者を対象とした調査のそれぞれで得た知見を整理する。

3.2 有識者調査からの考察

(1) CISO 等に求められる経営・事業的役割の重要性

国内有識者調査の結果から、今後事業基盤の IT 化（IoT、デジタルトランスフォーメーション等）の進展により、多くの企業で事業推進上 IT がこれまで以上に必要不可欠な要素となり、それに伴いセキュリティも重要になる、という意見があった。

ひとたびセキュリティインシデントなどが発生すると、事業を支える IT システムやサービスの機能が低下したり、一時停止せざるを得なくなったり、場合によってはその企業全体の事業に対する社会的評価の悪化にも繋がりかねず、事業収益や企業全体のブランド価値を毀損する惧れすらある。こうしたセキュリティリスクをいかに回避・低減等するかという役割は、もはや技術に関する役割には限定できず、経営・事業に関する役割にまで広がらざる得ない。こうした事情により CISO 等の経営・事業に関する役割の重要性が高まると考えられる。

一方、海外有識者のインタビュー調査では、CISO 等はセキュリティ技術の専門家としての役割が求められており、CIO 等をはじめとした経営層の経営・事業に関する意思決定について、セキュリティの面から CISO 等が助言することの重要性が指摘された。このことから、CISO 等には経営・事業的役割が求められる点では国内外ともに一致していると考えられる。

これまで CISO 等には、主にセキュリティの責任者として技術的な役割が求められると考えられていたが、今後事業と IT が不可分の関係になるつれ、事業に貢献する経営・事業的役割の重要性が高まると考えられる。IT を活用した事業を安心して進めるためには、セキュリティ対策が必要不可欠であり、CISO 等が経営・事業に関して大きな役割を担うようになると考えられる。

(2) CISO 等が経営・事業に関する役割を十分果たせていない理由

有識者調査の結果より、CISO 等が経営・事業的役割を十分に果たせていない理由として、組織面と人材面の課題があげられた。

組織面について、日本企業では CISO 等に対して十分な責任と権限、リソースが与えられていないため、CISO 等が経営・事業的役割を果たせていないとの意見があった。経営層のサポートを十分得られていない点に関して、海外の有識者の意見では、CISO 等が経営層とコミュニケーションを取る等の努力が必要であることが指摘された。

CISO 等を担う人材に関しては、CISO に限らず日本では CxO を担うマネジメントや戦略人材が不足していることがあげられた。さらに、CISO 等にはセキュリティ技術に加え CxO に共通して必要なマネジメント能力が求められるが、IT 出身者は財務や法律、事業に詳しくないことが多いため、経営・事業的役割を十分果たせていないとの意見があった。海外有識者のインタビューでも、CISO 等には技術だけではなくマネジメントに関する能力が求められるとの意見もあり、CISO 等が経営・事業的役割を果たすためにはマネジメント能力の強化が重要となる。

(3) CISO 等に求められる経営・事業に関する役割として注目すべき項目

文献調査では言及されていなかった CISO 等に求められる経営・事業的役割として、「事

業現場の利便性を考慮したルールの策定」が挙がった。また、文献調査でも言及されていた「社内外とのコミュニケーション」は、有識者調査でも重要性が指摘された。

「事業現場の利便性を考慮したルールの策定」に関しては、現場に負担をかけず、現場が意識せずともセキュリティが確保されているような、セキュリティの構築が重要になるという意見があった。セキュリティルールの強化により、セキュリティ対策が場合によっては事業部門の負荷や事業推進の阻害要因になる可能性がある。CISO 等が事業に貢献するという観点で考えた場合、事業部門の負荷を最小化しながら一定のセキュリティレベルを担保するためのルールや対策の検討が求められる。

「社内外とのコミュニケーション」に関して、社内とのコミュニケーションでは経営層と現場をつなぐ「橋渡し人材」の役割が求められるとの意見があった。海外有識者のインタビューでは、CISO 等は技術の専門家として経営層や事業責任者に対してセキュリティに関してアドバイスし、間接的にではあるが経営層の意思決定を支えることで経営に貢献しているとの意見もあった。社外とのコミュニケーションに関しては、自社のセキュリティ対策の取組についてステークホルダーに説明すること、日常的に社外の情報共有の取組（ISAC 等）に参加し、社外の CISO 等との横のつながりを維持することが必要との意見があった。

(4) チームとしての機能の有効性

CISO 等の役割は、違う専門性を備えた複数の要員のチームとして構成することが有効との見解があった。たとえば、経営を理解している人材と技術を理解している人材にチームを組ませることにより、CISO 等に求められる多岐にわたる役割を充足するということである。経営・事業的役割を果たす上では、自社の事業を広く、よく理解していることが必要であり、それに適した業務経験をつんでいることが必要である。一方、セキュリティ技術に関する理解では、日進月歩の技術の進展や日々変化する脅威に関する知見・業務経験が必要になるものである。この両者を、ひとりの人材に期待するのは困難を伴う。この困難を解決する方策として、経営・事業とセキュリティとをそれぞれ理解している人材を組ませる考え方は、有効に機能する可能性がある。

文献調査や有識者調査で示した通り、CISO 等に求められる役割は幅広く、求められる能力やスキルも幅広い。そのため、CISO 単独でこの役割を担うことは困難であると考えられる。CISO 単独ではなく、チームとして CISO 等の役割を果たすことが解決策の 1 つと考えられる。

3.3 調査結果

3.3.1 国内有識者に対する調査結果

(1) CISO 等に求められる経営・事業的役割について

今後多くの企業が事業基盤の IT 化に直面することから、CISO 等が事業で ICT を活用していく上でのセキュリティ面を支える役割を担うとの意見があった。

CISO 等に求められる経営・事業的役割については、CISO 等には社内外とのコミュニケーションが求められるとの意見があった。特に社内では経営層と現場をつなぐ橋渡し人材と

しての役割が求められるとの意見があった。また、今後は事業を理解している人とセキュリティを理解している人をうまくつなげ役割分担していくことが CISO 等に求められるとの意見もあった。社外向けのコミュニケーションに関しては、外部から入手した情報を適切に利用・共有するために、社外とのつながりが重要であるとの指摘があった。

また、インシデント発生時の危機管理、ガバナンス、ルール策定も CISO 等の経営・事業的役割としてあげられた。特にルール策定に関しては、ビジネスを安心して進められる環境を整備することが CISO 等の役割としてあげられた。

有識者の主な意見は以下の通り。

- CISO の役割は責任を持つということ。ルールを決めてビジネスを安心して進めるために、インシデントが発生した時の危機管理をすることが重要である。それが CISO 等に経営・事業的役割が必要な理由である。
- セキュリティルールを効率的に運用できるよう実装するのが CISO の役割である。自社では、ルール策定はセキュリティ担当が実施して、CIO が実装に落とし込んでいる。
- CISO がうまく機能するためには事業リスク管理チームとの連携が重要だと考える。CISO のメインとなる役割は、①ルールの決定、②トラブル等万が一の際に技術的支援をすること、③事業部門と連携することである。現場に安心できる事業開発・運営環境を提供することが、CISO の役割である。
- ガバナンスの役割も重要である。自社を例にすると、これまで CIO は外向けのサービスには関与せず、社内の情報環境を整えることに専念していた。しかし、インシデントをきっかけに経営層の考え方が変わった。今はセキュリティに関する権限を CIO に集中し、CISO が CIO を補佐している。
- CISO 等には経営層と現場をつなぐ役割が求められる。
- オペレーションを中心に、ストラテジーからタクティクスまでリーチできるのが理想的な CISO である。
- CISO の役割として、対外的な役割もポイントとなる。また情報共有の視点から外部から情報を持ってくることや横とのつながり等も重要である。
- CISO 室のように組織の中心としてセキュリティ対策を推進するメンバーが必要である。また、産業横断サイバーセキュリティ人材育成検討会では、OT 系において統括人材は事業部門側にも必要になるのではないかと議論した。
- どの企業もデジタルトランスフォーメーションには無関心ではいられない。事業で ICT を活用していくための旗振りが必要である。積極的にデジタルを活用し、事業を変えていくためのポジティブなメッセージを出してはどうか。セキュリティと事業推進のバランスだけではなく、デジタルエイジに向けて事業を変えていくというイメージを示すとよいのではないか。CISO はその役割を担いつつある。
- IT と OT も見る必要があること、自社の事業を理解していることが CISO に必要なことを伝える必要があるのではないか。
- 自社の事業を理解している人は生え抜きでたくさんいるが、セキュリティのこと

を理解している人は少ない。事業を理解している人とセキュリティを理解している人をどうつなげ、どのように役割を分担させるかが重要である。

(2) 日本企業における CISO 等の課題について

日本企業における CISO 等の課題として、まず CISO 等に必要な権限とリソースが与えられていないことがあげられた。また、CISO や CxO を担える人材（各事業部門を統合する戦略マネジメント機能を果たすオペレーション人材）が十分にいないことが指摘された。

これらの背景として、経営層が CISO 等に対して経営・事業的役割を期待しているにも関わらず、企業組織全体としてはそうした役割の必要性が広く認識されていないために CISO 等が経営・事業的役割を発揮する際に協力する雰囲気が醸成されていないこと、さらにはそれに起因して、組織が CISO や CxO 人材を適切に評価できていないこと、等の理由が指摘された。

有識者の主な意見は以下の通り。

- 経営層が、経営・事業的役割に必要となる権限を CISO に与えていないことが原因で、役割を果たせない。権限を与えた後は、能力と責任を果たすためのリソースが重要になる。日本はこの点が欧米と比べて遅れている。
- 日本企業において CISO という職は名ばかりという現状がある。
- オペレーションの機能（経営層が示した戦略と現場の個別の取組を調整する機能）が重要であるが、CISO や CxO を担えるような人材が日本には十分いない。
- 人材が不足している理由は、①企業組織がこうした役割の必要性を広く認識できていない、②候補となる人材が受けてきた教育が、経営層としてのリテラシーを育成してこなかった、③CISO や CxO 人材を適切に評価できない等の要因が考えられる。複合要因であり、経営者だけの責任ではない。

(3) CISO 等が経営・事業的役割をうまく遂行する上でのポイントについて

CISO 等が経営・事業的役割を果たすためには、事業を理解し、セキュリティリスクを把握するために、事業リスク管理チームとの連携が必要であるとの意見があった。

また、事業を進めるにあたっては、リスクを過剰に捉えたり、リスクに見合わない過剰なセキュリティ対策を実施することにより、事業の推進を阻害することがあってはならないとの意見があった。そのため、事業における利便性を考慮しながらセキュリティルールを策定することや、IT 活用を推進する CIO との連携を行いながら、事業部門が安心して事業を行えるような環境作りが必要であるとの意見があった。

CISO 等は、技術がわかり、経営にコミットできる人の任命が望ましいが、CISO 等の人材が不足している場合は、経営がわかる人と技術がわかる人で一時的にチームを組ませる等の方法も有効であるとの意見があった。

有識者の主な意見は以下の通り。

- CISO がうまく機能するためには、経営・事業リスクを管理する部門との連携が重要だと考える。

- 事業現場の利便性を考慮しながらルールを作ることが重要である。いかに現場に負担をかけず、自然の流れで保護されるセキュリティの仕組みを構築するかがポイントである。例えば、外部のサービスを利用する際に、最初は個人情報を扱うことはないとしても、業務を運営しているうちに個人情報を扱う可能性がないかを確認するルールが必要である。単に導入時の検討や申請手続きのルールだけではなく、運営上のリスクがなくかつ効率性のよいルールが必要である。
- CIO との連携も重要である。ルール作りは CISO が担当し、実装に関するオペレーションは CIO が実施する、等。
- 経営リスクを減らしながら、具体的に IT を活用する方法を考えることである。例えば、アプリケーションの開発を事業とする際に、セキュリティに関するテストプロセスを作ることが考えられる。また、このような工夫は事故の防止だけでなく、顧客に安心できる商品を提供していることを示す証拠として使えるはずである。差別化の要因にもなる。
- 経営にコミットできない人を CIO や CISO に任命しても意味がない。経営にコミットできる人と技術がわかる人を組ませて、一時的にチーム制で運用する方法もあるのではないか。
- CISO の役割を一人で実現するのは困難なため、セキュリティ統括室（CISO 室）が重要となる。CISO 室の体制にすれば、CISO は統括人材として責任を果たせると考える。

(4) CISO 等に経営・事業的役割を重要視している企業の特徴について

CISO 等に経営・事業的役割を重視している企業は、ビジネスにおいてデジタル化が重要な企業であり、企業リスクとしてセキュリティを捉えていることから、責任者として CISO 等を設置し、権限を与えているとの意見があった。

有識者の主な意見は以下の通り。

- ビジネスにおいてデジタル化が重要と考える経営者であれば、リスクとしてセキュリティまで考えているのではないか。
- これからの事業展開にデジタルが関連しない企業は少ないことから、企業は自然に、経営・事業に貢献させることを主眼に、セキュリティに取組まざるを得なくなるのではないか。
- トップが権限を与えている企業は CIO や CISO が経営・事業的役割をうまく果たしているのではないか。
- CISO 等が機能している企業としては IT 系企業が候補になるのではないか。

(5) CISO 等が経営・事業的役割を果たすのに必要なスキルと習得方法、キャリアパスについて

CISO 等が経営・事業的役割を果たすためには、経営に詳しいことや意思決定ができるこ

と、セキュリティを理解していることが求められるとの意見があった。

有識者の主な意見は以下の通り。

- 自社の事業を理解させるよりも、セキュリティを理解させる方が時間がかかる。企業文化や事業内容は 2 年程度で理解できるが、セキュリティを短期間で理解するのは難しい。
- IT 出身者は経営に詳しくない。財務諸表、法律に関する知識もない。詳細は専門家に聞けばよいが、何がセキュリティリスクにつながるか、大まかな仕組みを知らないと管理はできないのではないか。
- CISO には CxO 共通の能力とセキュリティ技術に関する知識が必要である。CxO は経営を理解し、優先順位を付ける意思決定が重要である。意思決定は失敗することもあるが、そこから教訓を学ぶことができなければならない。
- 早い段階でリスクマネジメントに関する教育・訓練を受けることが必要である。リスクマネジメント等の知識をベースに、サイバーセキュリティ等の特定テーマも学んでもらう必要がある。

(6) 経営者に CISO 等における経営・事業的役割の重要性を理解してもらう方法について

多くの企業では、経営者が CISO 等の経営・事業的役割を重視していないと考えられるが、その重要性を理解してもらうために、取引先からの要求や、法律による義務化や罰則規定など、経営上の強制力が働くことで意識し始める可能性が高いとの意見があった。将来的には、リスクが定量化できるようになることで、経営者の理解が促進されると考えられる。さらには、例えば有価証券報告書にセキュリティに関する取組を記載し、市場が評価する形など、セキュリティ対策が投資家の評価につながる社会になれば重要性の理解が高まるとの意見があった。

有識者の主な意見は以下の通り。

- セキュリティ対策を推進してもらうために、法律による義務化や罰則を策定するのは考えられる。例えば、予算のある大企業でありながら、セキュリティ課題を放置し、何かの社会問題を起こしたということがあれば、その企業に対し罰則を与える等は考えられる。
- Society5.0 の進展により、セキュリティに関するリスクを数値で出すことができるようになれば、経営層の理解はより簡単に得られるはずである。現状としては、データの量がまだ足りない。
- 取引先への要求により、リスクマネジメントに対する意識が他業種に伝播していくことは期待できる。
- セキュリティ対策をきちんと取っていることを IR に載せ、投資家がこのことを評価するような社会になることが期待される。

3.3.2 欧米有識者に対する調査

(1) 欧米企業の CISO 等に求められる経営・事業的役割

欧米企業では、国や組織、業界により CISO 等に求められる役割は異なっており、銀行や製薬等のセキュリティが重要となる業界では、CISO 等の役割が確立されているとの意見があった。ただし、これらの業界でも CISO 等の役割が確立できているのは、上場企業やグローバルに事業を展開している企業がほとんどであるとの指摘があった。また、CISO 等には情報セキュリティ関連だけではなく、コンプライアンスやデータプライバシー、事業継続等の役割が求められており、その役割の範囲は拡大しているとの意見があった。

有識者の主な意見は以下の通り。

- 欧米と言っても、地域的に広範囲なので一般化して説明することは難しい。CISO 等の役割は、比較的最近登場したものである。この役職の責務は、組織によって多様で、業界により異なる。
- CISO 等は、IT 運用業務遂行に必要となるセキュリティ要件から生み出された役割である。セキュリティポリシー、リスク管理やコンプライアンス等の幅広い要素が、組織に必要な状況になってきたため、“スーパー”レベルのセキュリティ人材を配置する必要性が出てきた。CISO 等の”C”が付けられたのは、その重要性が認識されたこと、他の C レベルと呼ばれているレベルと同等に引き上げることを意図している。
- 国、組織や業界により変わる。英国や北欧においては、CISO 等は役職として確立されているが、他の欧州地域ではそうではない。中東やアフリカでは、最近になり組織内に CISO 等を置く動きが出始めている。中東では、国外からの人材が CISO 等に就くことにより役割が確立されるようになってきた。
- 業界別では、銀行、製薬、宇宙などは、CISO 等がいることが多く、役割も確立されている傾向がある。一方で、小売業は正反対の状況である。ただし、各業界において役割が確立されているのは、上場企業やグローバル企業に限られている。大多数の従業員 250 名以下の中小企業は、CISO 等は置いておらず、IT チームまたは IT ディレクターがその職務の一部として担っている。
- 多くの CISO 等は、情報セキュリティ関連の責務だけでなく、コンプライアンス、データプライバシー、事業継続、インシデント対応、レコード管理などの業務にまで責務が拡大している。これは、CISO 等が唯一、これらの業務のことを考えている、あるいは組織や事業が CISO 等を「テクノロジやセキュリティを知っている」と考えているためである。主に英国においては、CISO 等自身が、情報保護において、技術的側面だけではなく、前述のような幅広い責務を積極的に担おうとしてきていることも事実である。とくに、IoT/ICS/SCADA の保護を経営陣と共に遂行しているような CISO 等が、このケースに該当している。

(2) CISO 等に求められるスキルとキャリアパス

CISO 等にはセキュリティに関する複合的・体系的知識、ビジネス知識、コミュニケーションスキルが必要であり、OJT の中でマネジメント手法等を学ぶ必要があるとの意見があった。

有識者の主な意見は以下の通り。

- 大切なのは、トレーニング、教育、スキルである。CISO 等になりたいと考えている人に必要なのは、複合的、体系的な知識である。大学などでの体系的な教育を基礎とした幅広い教育が必要である。技術面のスキルはトレーニングとハンズオンでの経験で得ることができる。CISSP を始めとする資格は、セキュリティ業務従事者が、当該分野における幅広い知識を体系的に保有していることの証拠となり、サイバーセキュリティ分野において貢献できるリーダーになるために必要なトレーニングや経験を積むにあたってのフレームワークとして使える。
- 鍵となるスキルは以下の通りである。
  ①経営陣との関係構築・維持：シニアマネージャーとの関係構築・維持と彼らが必要としている情報の提供と保証の確保
  ②ファイナンス：予算立案、予算執行確認、収益の考え方・見方
  ③デリバリー：各種プロジェクト、プログラム等の遂行
  ④コミュニケーション：上層部、部下、社内関連部署、その他社内、社外等と、文書・口頭またはそれ以外の全てのコミュニケーション
  ⑤ビジネス思考：情報セキュリティを広範囲なビジネス文脈に置き、ビジネスの成功にどう影響（プラス・マイナス）を及ぼすのかを理解すること
- キャリアパスとしては以下のようなものが考えられる。
  ①事業側の立場と、セキュリティのプロジェクト・プログラムの立場を兼任する。
  ②複数組織をまたいで構成されるチームをリードし、コーポレートコミュニケーションやマーケティングなどからのインプットを得つつ、意識向上プログラムなどにおいて結果を出す。
  ③コーチングや関係性を構築しながら、経営層等シニアマネージャー陣の仕事のやり方を学ぶ。
  ④適当なメンターを選び、必要な知識やスキルを学ぶ手法についてのディスカッションをしたり、学びや実践での成功事例などをディスカッションしたりする。
- MBA 取得などを含め、ビジネスに関する教育を受けることも重要な要素である。これにより、CISO 等になった際に必要とされる、ビジネス全般で必要とされる知識やスキルに触れる機会を得られる。

(3) 経営層に CISO 等の経営・事業に関する役割の重要性を理解してもらう方法

経営層に CISO 等における経営・事業的役割の重要性を理解してもらうための方法としては、リスク分析等を基に、経営層と効果的なコミュニケーションをすること、CISO 等の役

割が事業に利益をもたらすことを証明することが有効であるとの意見があった。

有識者の主な意見は以下の通り。

- サイバーセキュリティを引っ張っているリーダークラスの CISO 達は、常に業界に還元することを考えている。各人は、経営トップから必要な支援を受けられるよう努力しないといけない。そのために、経験豊富な CISO 等は、効果的なマトリックスやリスク分析を使って、経営層ほかシニアリーダー達との効果的なコミュニケーションを確実にするための努力をしている。
- CISO 等は、情報セキュリティが、ビジネスプロセス、調達、デザインなどを含め、事業の中で日常的なものとして組み込まれていくことに注力すべきである。CISO 等が経営・事業に関わる責務を得て、経営陣の一部として認知されるための最適解は、事業自体に焦点をあてる立場に自らの立ち位置をシフトでき、事業に利益をもたらすことが証明できることである。

3.3.3 欧米教育機関に対する調査

(1) 提供するプログラムと想定する CISO のロールモデル

今回のインタビュー対象者が責任者を勤める CISO の養成プログラムでは、セキュリティ業務に従事している専門家について、とくに経営・事業に関するマネジメントのスキル向上にも比重を置いているとのことであった。

CISO には、インシデントの現状把握、将来的な脅威の特定、計画策定、予算執行の正当性証明、導入・リスク・成功指標の理解、C スイートレベルの経営陣やボードとのコミュニケーションスキル、デジタルトランスフォーメーション、セキュリティに関する法律知識などが必要であるとされている。

また、ケーススタディは実際の事例を基に作成しており、受講者がさらに調査することで深堀できる内容となっている。

有識者の主な意見は以下の通り。

- 全てのモジュールが CISO の経営に関する役割に関したものになっているが、経営により特化したものとしては、「Strategy, Security Measures, Digital Transformation」と「Building an Insider Threat Program and Communications」がある。
- セキュリティ業務に従事しているセキュリティ専門家のマネジメント関連のスキル向上を目的としている。多くの受講者が CISO になるキャリアパスを進んでいるが、受講者の所属部門は、事業部門、法務、リスク、プライバシーなど広範囲に渡っている。受講者は、リスクプロフィール、セキュリティ対処プロセスや文化などを構築するにあたって、組織が直面する課題や現状などについてのクリティカルシンキングが求められる。
- 演習には、CISO のキャリアにおいて、絶対必要となる要素を含めている。インシデントの現状把握、将来的な脅威ベクターの特定、計画策定、予算執行の正当性

証明、導入・リスク・成功メトリックスの理解などが含まれる。講義の多くは、基本的な技術要素を中心に学習するが、C スイートレベルの経営陣やボードとのコミュニケーションスキル、デジタルトランスフォーメーション、コミュニケーション、セキュリティに関する法律等を含んだ内容で、グローバルチームのマネジメントを可能にするスキルを取得できる内容も提供している。

・ ケースやストーリーは実際に起きた漏えい事例をベースにリサーチャーが作成する。ケースが常に受講者にとって関連性のあるものにし、また受講者自身がさらにリサーチし、深堀できるように作成している。

(2) CISO 等人材を育成する上での課題

CISO 等は、関連するステークホルダーとのコミュニケーションを図り、セキュリティの価値に関する理解を得ることが重要であるとの指摘があった。また、自社のセキュリティレベルが企業全体､業界内のレベルに合致しているか理解することも重要であるとの意見もあった。

有識者の主な意見は以下の通り。

・ 多くのセキュリティ専門家にとっての課題は、セキュリティにおけるプロセスや手順に関連した価値を全てのステークホルダーに理解させること、様々な立ち位置の相手（直接の関係者以外も）への効果的なコミュニケーションをすること、必要なリソースと予算割当ての正当性を主張し社内でのポジショニングを向上することである。

・ さらに、自社のセキュリティが各部署、企業全体、業界内のレベルにどう合致しているのかを理解し、それぞれの関係各位からの納得・了解を得ることは大変重要な業務になっている。本プログラムでは、実際に自組織でこれらのチャレンジに成功したセキュリティ専門家からの実例やストーリーで、どのようにこういったチャレンジに向かっていけばよいかを学ぶ。

4. アンケート調査

4.1 調査概要[17]

第 2 章文献調査の結果と第 3 章有識者調査の結果を踏まえ、日本企業の CISO 等の経営・事業的役割の実態等を把握するため、従業員数 301 人以上かつ CISO 等を任命している日本企業を対象に、アンケート調査を実施した。

調査の概要を表 4.1-1 に示す。回答企業の属性及び全アンケート回答の詳細に関しては第 6 章を参照のこと。

表 4.1-1　本アンケート調査の概要

調査目的	第 2 章文献調査の結果と第 3 章有識者調査の結果を踏まえ、日本企業の CISO 等の経営・事業的役割の実態等を把握する。
調査対象	従業員数 301 人以上かつ CISO 等を任命している日本企業
調査期間	2017 年 10 月下旬から 11 月中旬
調査方法	ウェブアンケート調査
回収結果	有効回答 263 件
調査項目	・　回答企業の基本情報 ・　セキュリティリスクに関する経営層の認識とリスク分析実施状況 ・　CISO 等の基礎情報と設置状況 ・　経営者が CISO 等に期待している経営・事業的役割 ・　CISO 等が現在担っている役割 ・　経営・事業的役割を重視している理由　等
データ精査	回答データに関して下記の方針で精査し、該当したものは回答内容に矛盾があるという意味で信頼性に問題があると判断し、除外した。 ・　回答時間が 120 秒未満の回答 ・　異常値入力等の不正回答 ・　問 1「IT 依存度」で選択肢 1 または 2 を選択し、問 11（3）「経営層が経営・事業的役割を重視しない理由」で選択肢 2 を選択した回答 ・　問 1「IT 依存度」で選択肢 3 または 4 を選択し、問 11（2）「経営層が経営・事業的役割を重視する理由」で選択肢 1 を選択した回答 ・　問 13（4）「経営・事業的役割を遂行できていない理由」で選択肢 1 または 3 を選択し、問 14（1）で選択肢 1 または 2 を選択した回答 ・　同一企業による重複回答

[17] 本調査における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 とはならない箇所がある。

4.1.1 分析軸

今回の調査では、企業がセキュリティを経営・事業的リスクと捉えるかどうかは、事業でどれだけ IT を活用しているかが影響すると想定し、主に「IT 依存度」[18]という軸を利用して分析を行った。

IT 依存度に関しては、問 1「事業の IT システム・IT サービスの依存度」の回答を基に以下の通り分類した。

- カテゴリー1：事業の基盤における IT 活用の度合い[19]が高い企業
- カテゴリー2：事業の基盤における IT 活用の度合いが低い企業

分類	問 1「IT 依存度」の選択肢
カテゴリー1	・ 選択肢 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、通信、ネット通販等）」を選択した回答
カテゴリー2	・ 選択肢 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）」を選択した回答 ・ 選択肢 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、一次的な停止であれば事業への影響は小さい」を選択した回答

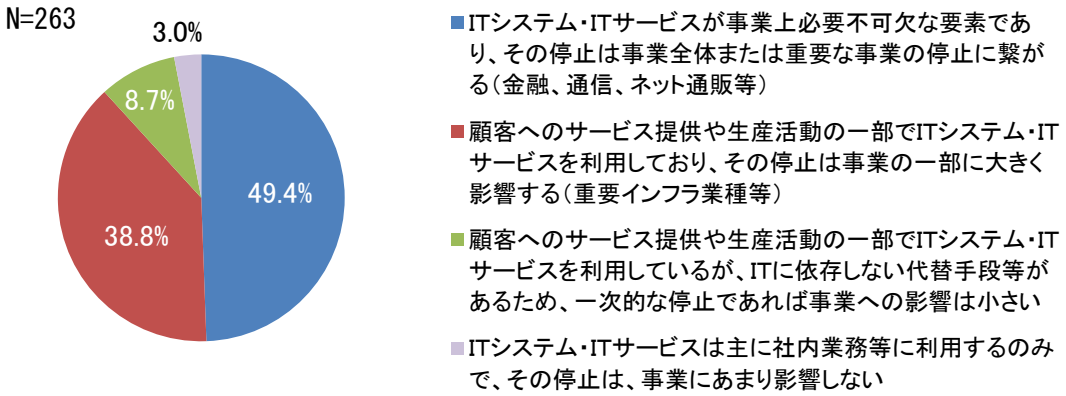

図 4.1-1 IT 依存度

[18] 本調査における IT 依存度に関する分析は、問 1 の選択肢「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」(N=8)を選んだ回答を除いて比較したため、母数は 263 とならない。

[19] 本調査における IT 活用の度合いとは、事業全体における IT 利用の比率ではなく、事業において根幹となる部分における IT 利用の比率と定義する。

4.2 アンケート調査結果からの考察

(1) CISO 等が経営・事業的役割を担っているケースは半数以下

アンケート調査結果より、経営層は CISO 等に求める役割として経営・事業的役割を重視しているにも関わらず、CISO 等の半数以上は経営・事業的役割を有していないことが示された。

経営層が重要視する CISO 等の役割について、経営層が CISO 等に対して経営・事業的役割を重視（「経営・事業的役割」「技術的役割と経営・事業的役割の両方」の合計）している割合は、75.3%となっている（図 4.2-1 参照）。

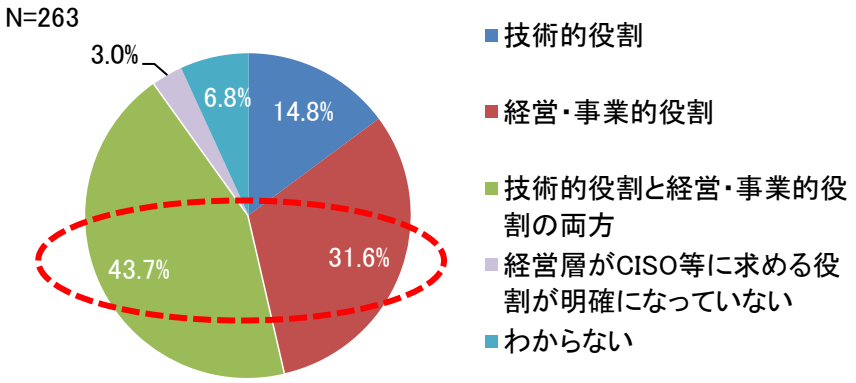

図 4.2-1 経営層が重要視する CISO 等の役割

CISO 等の具体的な役割を把握するために、本調査では「事業貢献」「コーポレートガバナンス」「リスク管理」「セキュリティ対策」の 4 分類を以下のように定義した。

役割	定義
事業貢献	・ セキュリティ投資の事業価値最大化や、セキュリティ対策の事業運営に対する負荷の最小化等、事業を推進するためのセキュリティを検討・実装する役割
コーポレートガバナンス	・ セキュリティガバナンス体制（「企業が自身の被害の局限化や法令遵守の観点に加え、社会的責任の観点も踏まえた」[20]体制）の構築・運営、セキュリティ計画・予算の策定・評価、社内のセキュリティ意識の醸成、セキュリティ要員の確保・育成等、社内全般のセキュリティに関する統制や計画・体制に関する役割
リスク管理	・ リスク分析の実施や、リスクに関する法令遵守や監査等の対応を行う役割
セキュリティ対策	・ セキュリティ対策の策定・実装や運用・評価、セキュリティ監視やインシデント対応を行う SOC や CSIRT 等の平時の構築・運営等、主に技術的なセキュリティ対策を検討・実施・運用する役割

[20] 経済産業省『企業における情報セキュリティガバナンスのあり方に関する研究会報告書』、p9。

上記のうち、本調査では、CISO 等の経営・事業的役割は「事業貢献」及び「コーポレートガバナンス」とした。

この 4 分類で、CISO 等が実際に有する役割を見ると、経営・事業的役割である「事業貢献」や「コーポレートガバナンス」を有している CISO 等は 50%を下回り、CISO 等の半数以上は経営・事業的役割を有していないことがわかる（図 4.2-2 参照）。

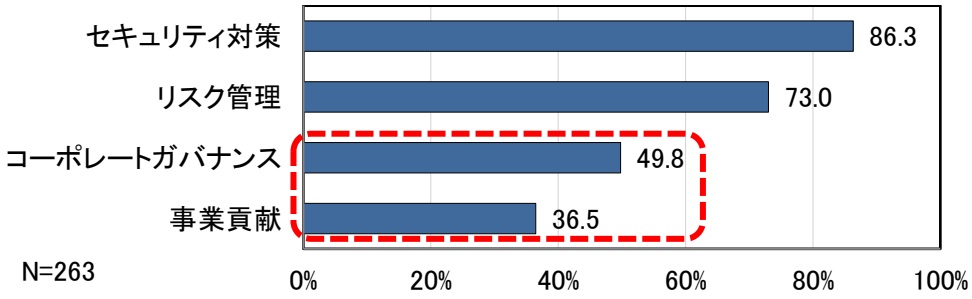

図 4.2-2 CISO 等が実際に有する役割

(2) CISO 等の所掌範囲からも事業を推進するためのセキュリティへの関与は低いと伺える

アンケート調査結果から、商品である自社製品や自社サービスのセキュリティの確保については、CISO 等は責任を有する主体でないことが把握できた。

CISO 等が、セキュリティの確保について責任を有する主体である割合は、自社製品に対する場合で 25.5%、自社サービスに対する場合で 26.6%であり高くない。6 割以上の場合で、セキュリティ確保はその事業の担当部門任せになっている（図 4.2-3 参照）。

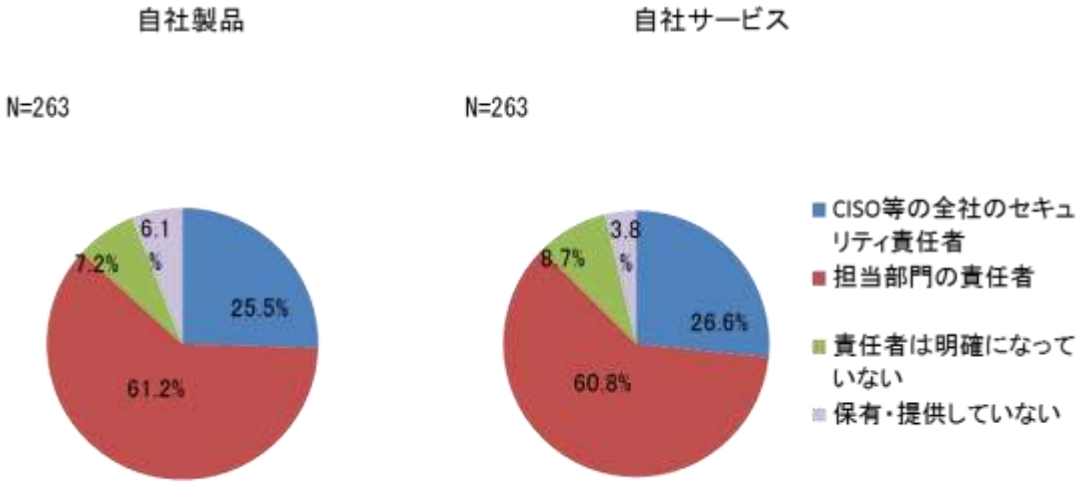

図 4.2-3 商品に対するセキュリティ確保の責任の主体

(3) CISO 等には多様な専門性を持つサポートメンバーが必要である

アンケート調査結果より、多くの企業で CISO 等をサポートするメンバーを設置していることが示された。

CISO 等に対するサポートメンバーの設置状況を見ると、ほとんどの企業がサポートメンバーを設置している（図 4.2-4 参照）。

サポートメンバーの設置理由を見ると、「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」、「CISO 等がセキュリティの専門家であり、それ以外の専門知識をもったメンバーがサポートする必要があるため」、「CISO 等の業務所掌範囲が広く、ひとりで対応するのが困難であるため」と言った理由が多かった（図 4.2-5 参照）。

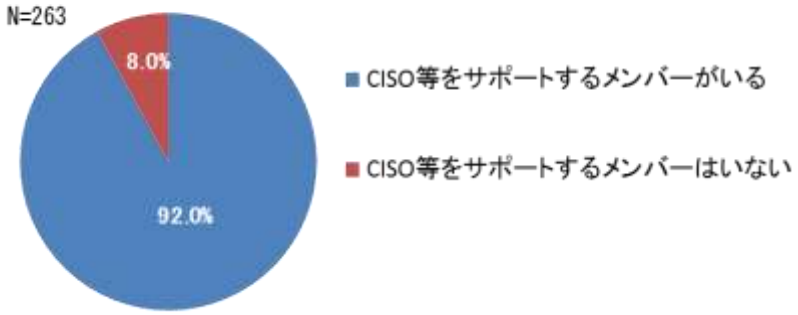

図 4.2-4 CISO 等をサポートするメンバーの有無

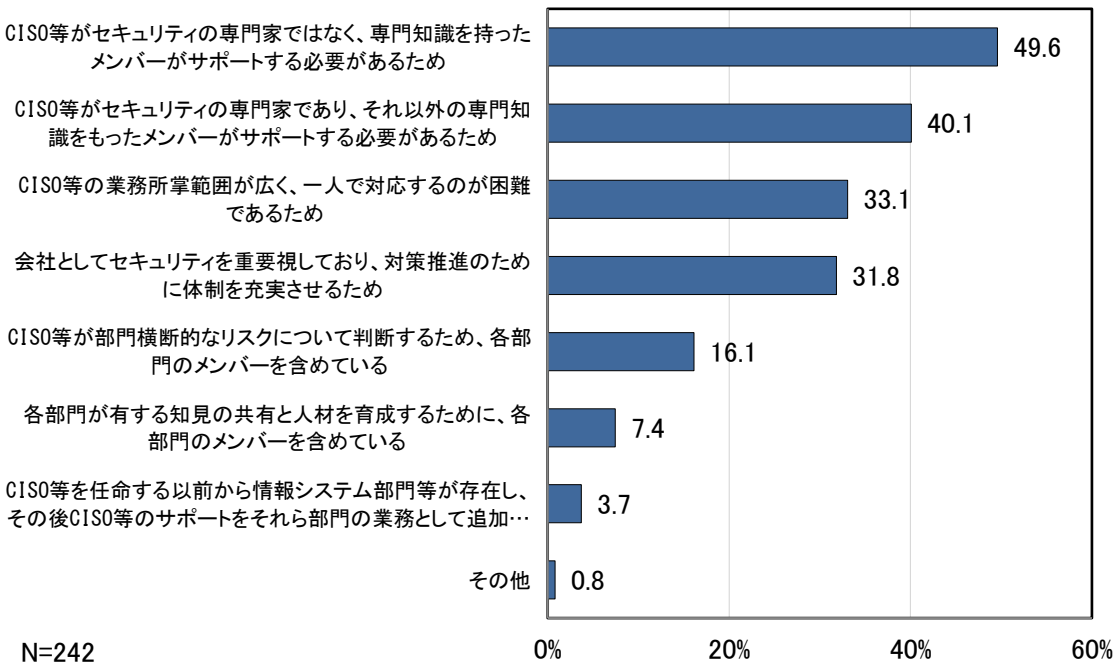

図 4.2-5 サポートメンバーの設置理由

CISO 等をサポートするメンバーの出身・所属部署を調べたところ、情報システム部門、情報セキュリティ部門が多いものの、リスク管理部門、総務部門、法務部門等、様々な部門のメンバーが支援している実態が把握できた（図 4.2-6 参照）。

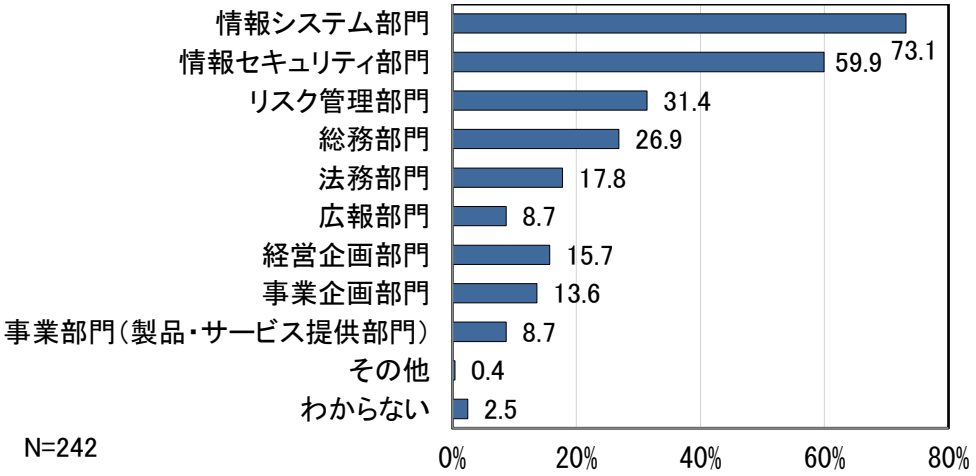

図 4.2-6 サポートメンバーの出身・所属部門

多くの企業で、CISO 等の多岐にわたる役割を支えるために、様々な専門性を備えたメンバーでチームを構成して、全体として CISO 等の役割を担う体制にしていることが読み取れる。

4.3 調査結果

以下の特徴的なアンケート調査結果を示す。全アンケート回答の詳細に関しては第 6 章を参照のこと。

- 経営層のセキュリティに関する認識
- CISO 等の設置状況
- CISO 等の所掌範囲

4.3.1 経営層のセキュリティに関する認識

(1) 経営層におけるセキュリティに関する議論の有無

セキュリティが経営における議題として取り上げられているかどうかを確認するために、経営層が主体となるセキュリティに関して審議する会議等の有無について調査した。アンケート結果では、「会議等があり、セキュリティに関する意思決定の場として機能している」が 70.3%と最も高い（図 4.3-1 参照）。

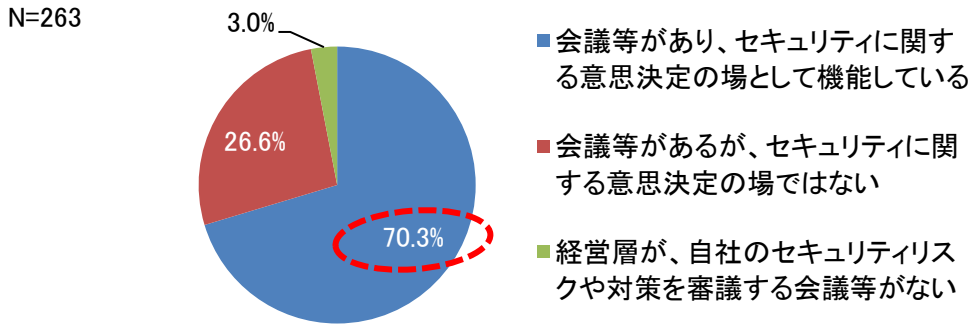

図 4.3-1 経営層が主体となるセキュリティに関して審議する会議等の有無

IT 依存度別に見ると、カテゴリー1 では「会議等があり、セキュリティに関する意思決定の場として機能している」が 83.1%であり、カテゴリー2 より 23.1 ポイント高い（図 4.3-2 参照）。

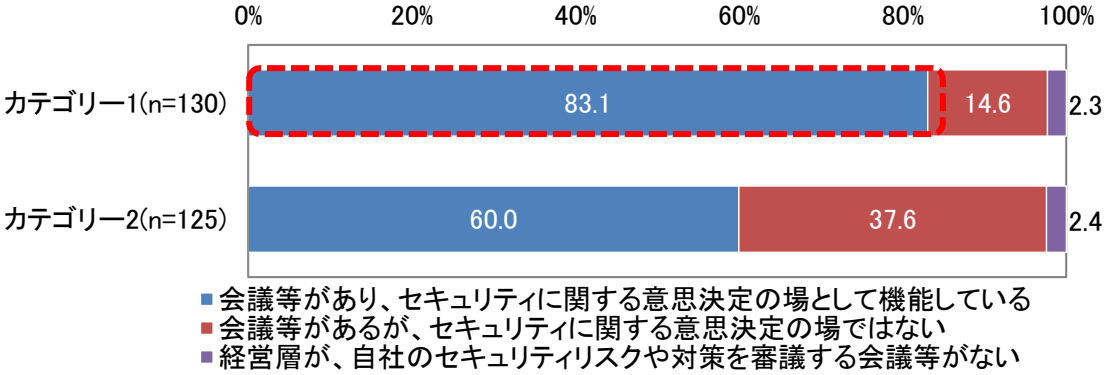

図 4.3-2 経営層が主体となるセキュリティに関して審議する会議等の有無（IT 依存度別）

(2) セキュリティを対象とした経営・事業的リスク分析の実施

「セキュリティを経営・事業的リスクとしたリスク分析の有無」については、「セキュリティを対象に入れたリスク分析を実施している」のは 78.7%となっており、セキュリティを経営・事業的リスクとして捉えリスク分析している割合が高い（図 4.3-3 参照）。

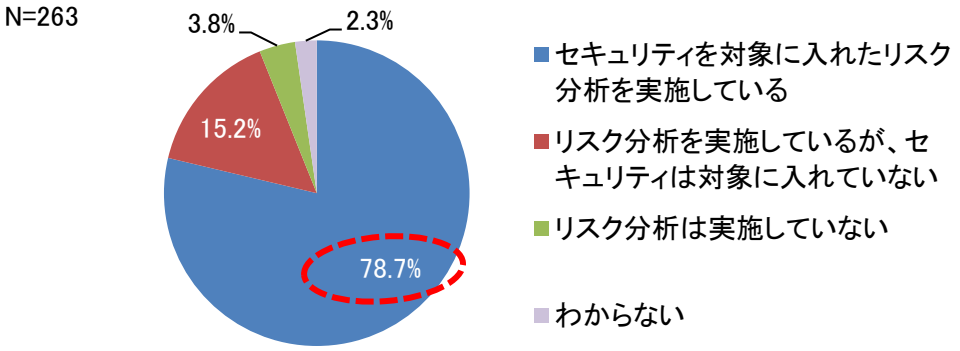

図 4.3-3 セキュリティを経営・事業的リスクとしたリスク分析の有無

IT 依存度別に見ると、とくにカテゴリー1 の方がリスク分析の実施割合は 11.8 ポイント高い（図 4.3-4 参照）。

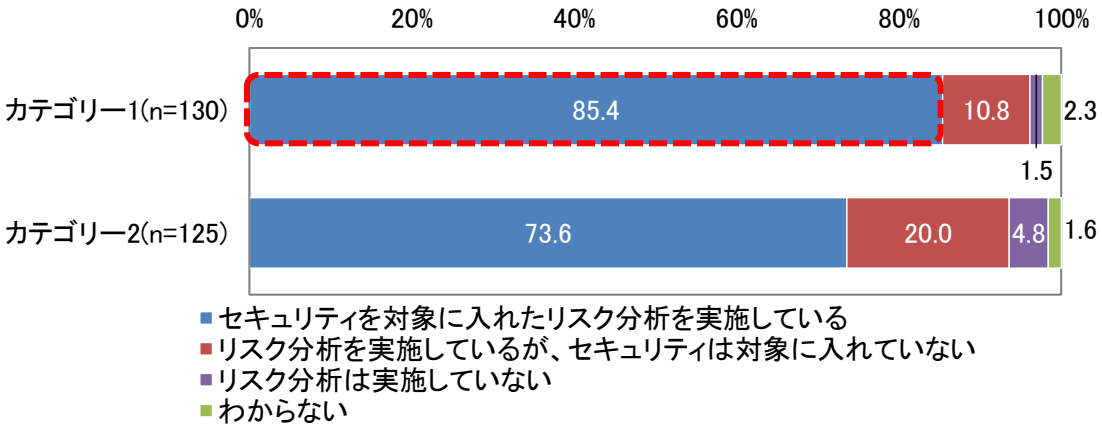

図 4.3-4 セキュリティを経営・事業的リスクとしたリスク分析の有無（IT 依存度別）

8 割近い企業がセキュリティを経営・事業的リスクとしたリスク分析を行っており、特にカテゴリー1 ではリスク分析の実施率が高いことから、多くの企業、特に IT 依存度が高い企業においては、セキュリティを経営・事業的リスクとして捉えていると考えられる。

4.3.2 CISO 等の設置状況

(1) CISO 等の組織における位置づけ

CISO 等の組織における位置づけを見ると、CISO 等を経営層（「取締役」または「執行役」）として設置している割合は 36.9%である（図 4.3-5 参照）。

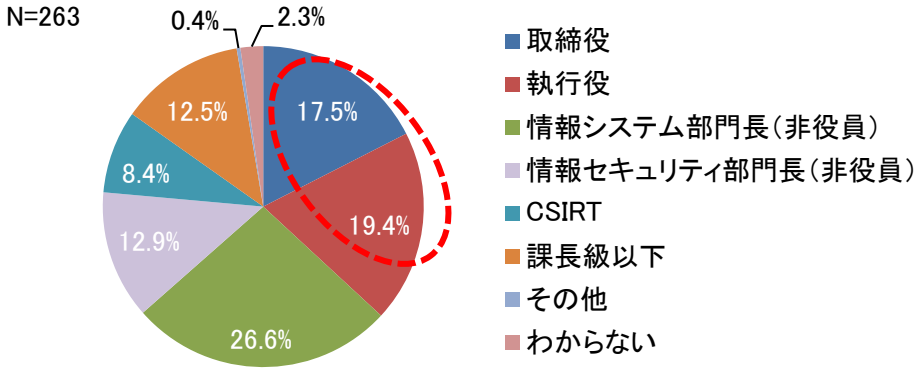

図 4.3-5 CISO 等の組織における位置づけ

IT 依存度別に見ると、カテゴリー1 では 43.0%、カテゴリー2 では 32.0%が経営層に CISO を設置している（図 4.3-6 参照）。

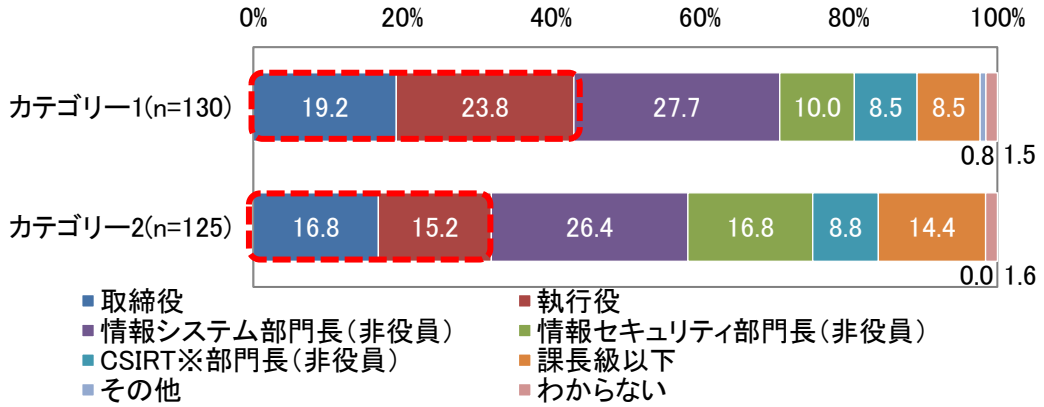

図 4.3-6 CISO 等の組織における位置づけ(IT 依存度別)[21]

4 割弱が経営層に CISO 等を設置しており、とくに IT 依存度の高い企業では、CISO 等を経営層として設置している割合が高い。

(2) CISO 等に関する体制

CISO 等の設置状況を専任／兼任別に見ると、専任の CISO 等を設置しているのは 47.9%とほぼ半数である（図 4.3-7 参照）

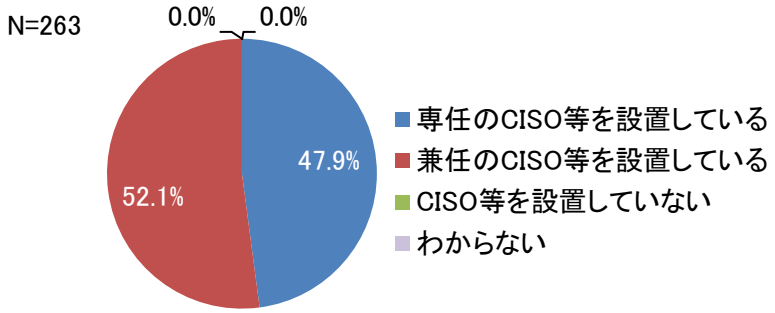

図 4.3-7 CISO 等の設置状況

IT 依存度別に見ると、カテゴリー1 は専任の CISO 等を設置している割合が 56.2%であるが、カテゴリー2 は 39.2%で、カテゴリー1 の方が専任の CISO 等を設置している割合が高い（図 4.3-8 参照）。

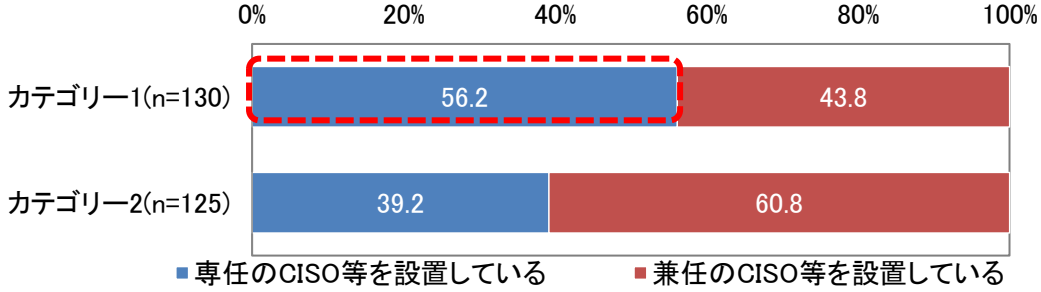

図 4.3-8 CISO 等の設置状況(IT 依存度別)

[21] ※ Computer Security Incident Response Team

4.3.3 CISO 等の所掌範囲

セキュリティ確保に責任を有する主体について調査した。

社内情報システムについては「CISO 等の全社のセキュリティ責任者」（58.9%）が最も高く、次に「担当部門の責任者」（37.6%）が高い（図 4.3-9 参照）。

事業部門が保有する情報システムでは「CISO 等の全社のセキュリティ責任者」（48.3%）と「担当部門の責任者」（44.5%）と同程度の割合となっている（図 4.3-10 参照）。しかし、事業部門が保有する制御システムでは、「担当部門の責任者」が責任を有している割合が 49.8%と高い。（図 4.3-11 参照）

自社製品、自社サービスの責任を有する主体は、両者とも「担当部門の責任者」との回答割合が約 60%で最も高い。（図 4.3-12 及び図 4.3-13 参照）

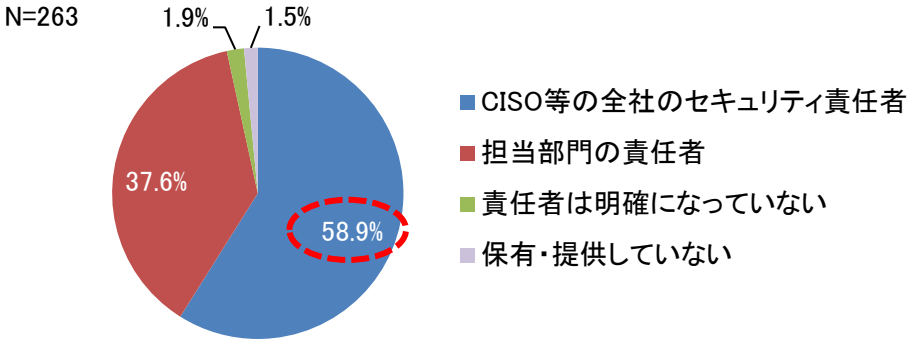

図 4.3-9 セキュリティ確保に関する責任者（社内情報システム）

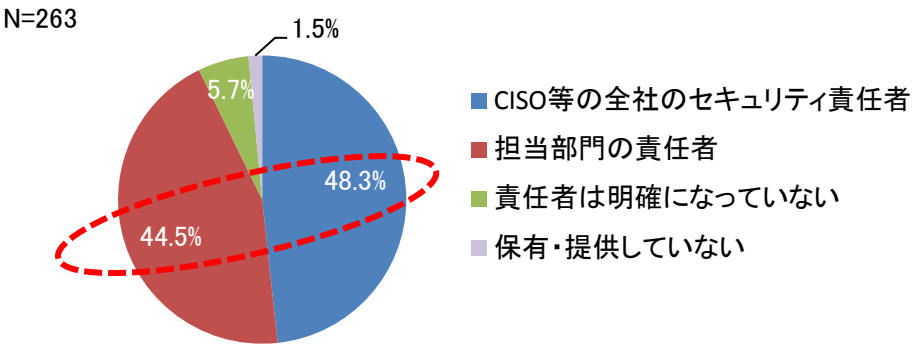

図 4.3-10 セキュリティ確保に関する責任者（事業部門が保有する情報システム）

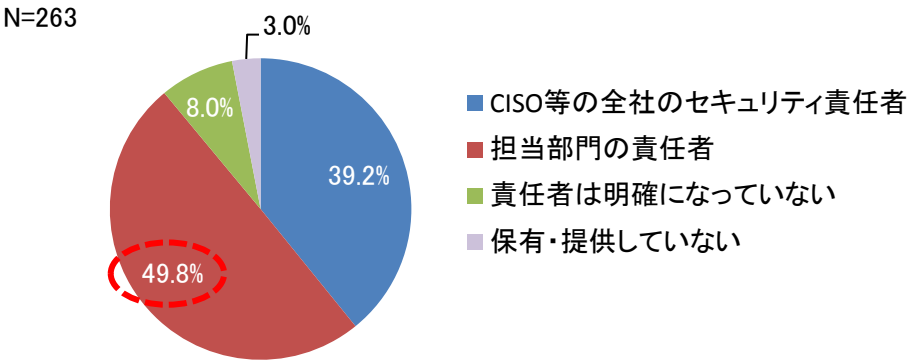

図 4.3-11 セキュリティ確保に関する責任者（事業部門が保有する制御システム）

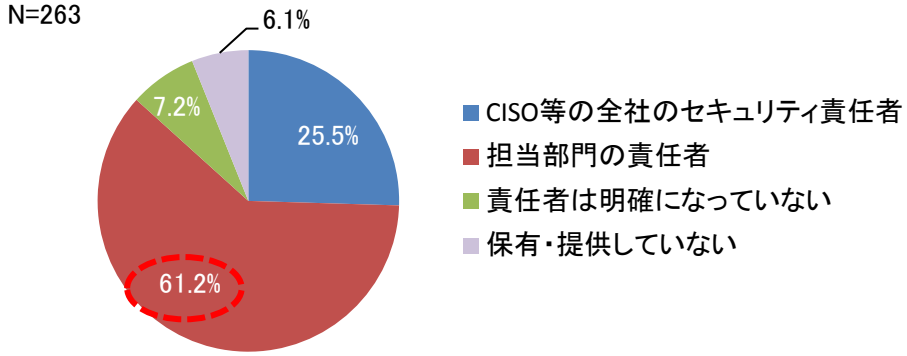

図 4.3-12 セキュリティ確保に関する責任者（自社製品）

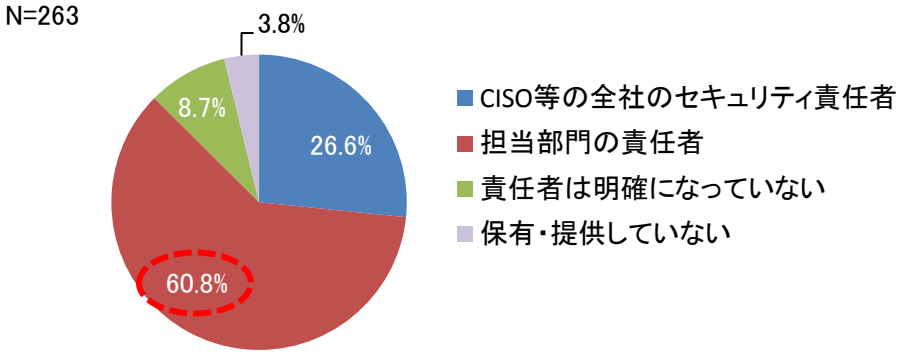

図 4.3-13 セキュリティ確保に関する責任者（自社サービス）

IT 依存度別に見ると、いずれのシステム、製品・サービスについても、CISO 等が責任者である割合はカテゴリー1 がカテゴリー2 より高い。特に、「事業部門が保有する情報システム」（27.9 ポイント差）と「事業部門が保有する制御システム」（25.1 ポイント差）については両者の差が大きい。

一方、「自社製品」と「自社サービス」については、カテゴリー1 もカテゴリー2 も担当部門の責任者が担う割合が一番高く、CISO 等が担う割合は 35%以下となっている。（図 4.3-14 参照）

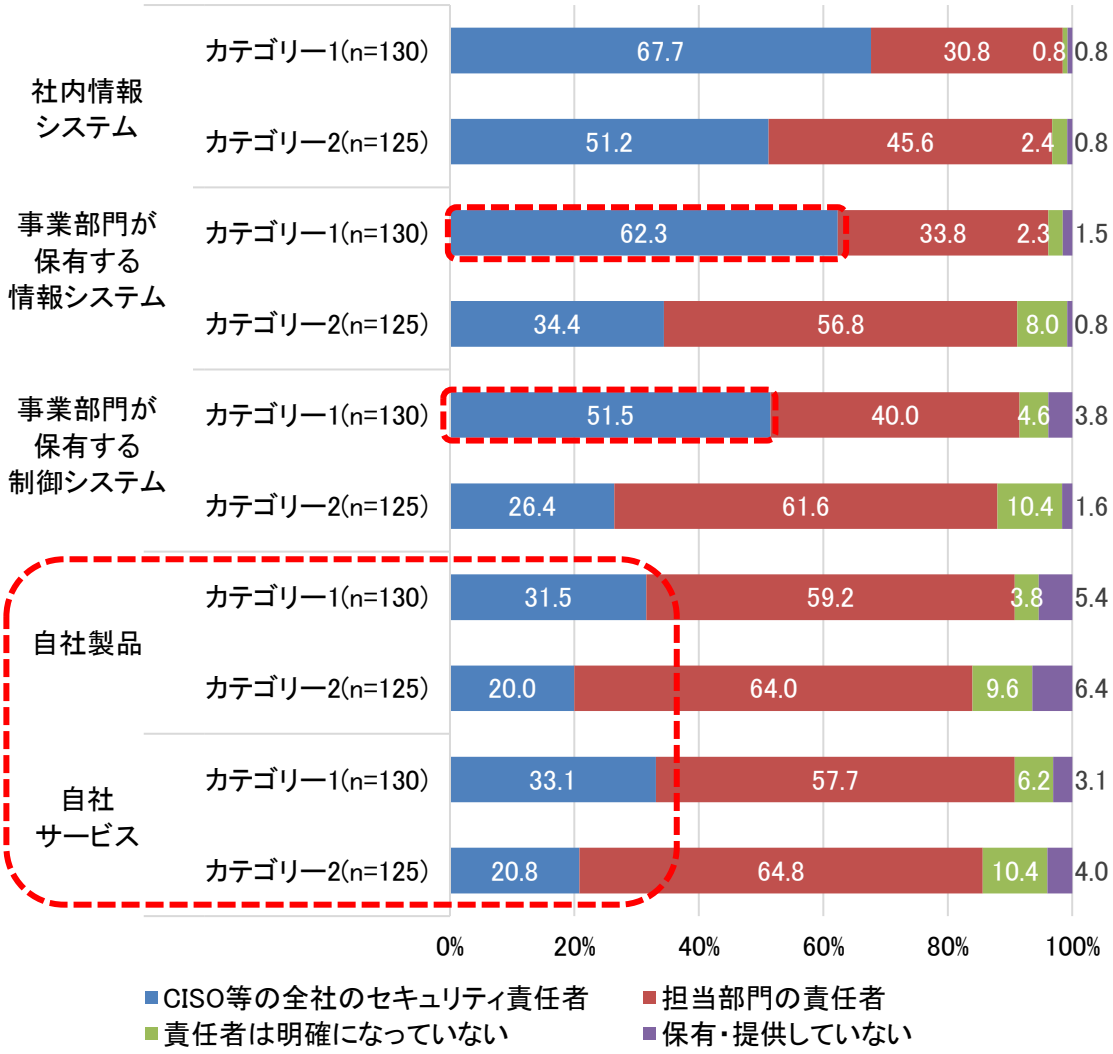

図 4.3-14　保有システムと自社製品・サービスの責任主体（IT 依存度別）

CISO 等の所掌範囲は、事業部門の情報システムにも責任を持つ企業が半数弱存在するが、基本的には社内情報システムが中心であると言える。事業部門の制御システムや、自社製品・サービスに関して責任を持つ主体はそれぞれの担当部門である。IT 依存度が高い企業においては、CISO 等のセキュリティ責任者が責任を有する主体となっている割合が高いが、自社製品・サービスについては担当部門の責任者が責任を有する傾向にある。

5. まとめ・今後の取り組み

5.1 調査結果のまとめ

調査結果を改めて整理し、考察を行う。

(1) 企業のセキュリティへの取組みが、経営と事業に貢献するようマネジメントする役割の重要性が指摘されている

文献調査において、CISO 等に対して、セキュリティ戦略やリスクマネジメント戦略と経営戦略・事業戦略との整合を求めることや、事業内容や方向性に応じセキュリティ戦略を確立するための助言・戦略立案の役割が求められるとの記載が見られた。IPA の昨年度調査でも、日米の CISO 等においては、今後「事業目標との整合」の重要性が高まるとの調査結果が得られている。また、アンケート調査でも、CISO 等に対して経営・事業に関する役割を求める企業が多いことが示された。
これらの調査結果により、CISO 等に対しては、技術的役割に加えて経営・事業に関する役割が求められていると言える。

(2) 経営・事業上のセキュリティリスクの最小化に貢献するセキュリティ対策・投資の策定や実施を担う役割が重要である

文献調査の結果、CISO 等がその役割をうまく果たせない理由として、CISO 等が事業を理解していないために裏に隠れているセキュリティリスクを捉えられない点や、セキュリティマネジメントにおいてリスク要素を特定しながら優先順位を付け投資ができていない点等がみえてきた。
CISO 等には、セキュリティ対策やセキュリティ投資が経営や事業上のセキュリティリスクの最小化にしっかり貢献するように、事業計画や事業の実情を把握した上で、リスク分析を行うことが求められる。

(3) 事業運営への負荷を最小化するセキュリティ対策の策定・実施を担う役割が求められる

有識者調査の結果から、事業部門の利便性を考慮したセキュリティ対策の策定・実施の重要性が見えてきた。これまで、CISO 等の役割として明確に指摘されてこなかった役割である。
セキュリティルールの強化により業務負荷が上がると、事業推進のスピードが落ちる等事業の阻害要因になる恐れや、ルールが守られにくく対策が形骸化する恐れがある。事業部門が安心して事業を進めるためには、業務遂行において自然とセキュリティが確保されるような対策策定や実施をマネジメントする役割が求められる。

(2)や(3)の役割は CISO 等が担うべき、基本的な経営・事業に関する役割であるが、CISO

等に求められる役割はこれだけに限らず、これらの役割に付随して発生する役割が考えられる。たとえば、セキュリティインシデント発生時の危機管理や、企業内のセキュリティガバナンス体制の構築・運営等の役割がそうした例である。CISO 等の経営・事業に関する役割に関する議論を深める中で、多くの企業に共通な役割の全体像を描く取組みが必要となるであろう。

(4) 経営・事業に関する役割を十分果たしている CISO 等は少ない

CISO 等は経営・事業に関する役割を求められていながら、実態として経営・事業に関する役割を十分に果たせていない。

アンケート調査によって、日本の CISO 等の役割として、経営・事業に関する役割である「コーポレートガバナンス」と「事業貢献」を有しているのは半分以下であり、CISO 等が経営・事業に関する役割を有している企業は半数にも満たないことが明らかになった。さらに、CISO 等が経営・事業に関する役割を「十分遂行している」のは 2 割以下の企業にとどまった。

この理由について、CISO 等が経営・事業に関する役割を果たすためには権限、責任が必要であることが文献調査で示されているが、日本の CISO 等には権限と責任が与えられていないと考えられるとの意見が有識者調査であった。

また、文献調査では、CISO 等が経営・事業に関する役割を十分果たせていない理由として、マネジメントに関する訓練が不足していること、事業戦略とセキュリティリスクの紐付けができていないことも指摘されている。さらに、有識者調査では、マネジメント人材や経営と現場をつなぐ人材が不足している点を指摘する意見もあった。

(5) 経営・事業に関する役割を果たす上で、社内外連携・橋渡しがポイントとなる

文献調査及び有識者調査からは、社内におけるコミュニケーションとして経営層と現場をつなぐ「橋渡し人材」の役割が求められることが示された。

経営・事業に関する役割を果たすためには、経営層が定める経営戦略を理解し、それに基づき、経営・事業リスクを踏まえた上で、事業における利便性を考慮しながらセキュリティルールを定め、それを実装することが必要になる。そのため、経営層（例えば CIO 等）、リスク管理部門、事業部門等、社内の関係部署と連携し、実効的な対策方針を立案し、取組を進めることが必要である。

また、文献調査からは、セキュリティに関する取組を外部に開示することで、説明責任を果たしたり、セキュリティに関する取組を企業価値向上に結びつけたりすることが求められていると分かった。その他、セキュリティに関する情報を他の組織等と共有し、最新の情報や効果的な対策に関する情報を入手することで、適切な対応を検討することが可能となる。

これらの結果から、CISO 等が経営・事業に関する役割を果たすために社内外の連携や、円滑なコミュニケーションにより調整を行う橋渡しが重要であると言える。

(6) CISO 等の役割は、様々な専門性を備える複数の要員が分担して担うことが有効である

有識者の調査から、経営を理解している人材と技術を理解している人材をチームとして組ませ、共同で経営・事業に関する役割を担うようにすることが有効との知見を得た。有識者調査ではさらに、日本では、特有の事業環境や組織構造を背景として CxO を担える人材や戦略マネジメント機能を果たす人材が十分にいないため、CISO 等の役割を果たす人材が不足していると考えられる、との見解が示された。

アンケート調査からも、CISO ひとりでは担うことが難しい多岐にわたる機能を、様々な専門性を備えた多様な要員が共同して提供する体制を採っている企業が多いということが分かった。

企業の規模や業種・業態などによっては、経営・事業に関する役割を果たす上で必要となる専門性のすべてを、社内要員でまかなうのは困難なケースが想定される。そうした場合、アウトソースを積極的に活用して必要な専門性を調達することは、現実的な方策である。

5.2 今後の取り組み

セキュリティマインドをもった経営への理解の促進については、従来から、政府・民間において施策が展開されてきた。しかし、これにより経営層のセキュリティへの認識が今後より強まるとしても、求められる役割を果たせる人材が十分いなければ、有効な対策策定・実施には結びつかない。

経営・事業に関する役割を担える CISO 等の候補者が十分にいる状況を作るには、様々な施策がありえる。実際、下記のような方策が、既に着手あるいは検討されているところである。

A) 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
B) CISO 等が担うべき経営・事業に関する役割について参考情報を提供すること
C) CISO 等に適した人材の養成・演習等の教育プログラムを整備すること
D) セキュリティに係る人材が、経営・事業に関する役割を担う CISO 等を目指すモチベーションを持てるようなキャリアパス等を整備すること

(A)については、サイバーセキュリティ経営ガイドラインの普及活動の一部等で、すでに実施されている。(C)や(D)については官民のいくつかの場で検討が行われており、一部ではすでに実施されているものがある。一方、本調査で検討してきた経営・事業に関する役割について主要な課題として取組んでいるものは少ない。

(B)は、(C)や(D)の前段階の方策として位置付けることができ、(C)、(D)の充実にも繋がる可能性がある。CISO 等が経営・事業に関する役割を果たす上では、それぞれの企業の特性に合せて自らの役割を検討するための手引きや事例があると助けになるであろう。たとえば、CISO 等の経営・事業に関する役割の経験談の紹介、プラクティス集、ケーススタディなどがそうした手引き・事例になると考えられる。

本調査に続く取組みとして、CISO 等が担うべき経営・事業に関する役割に関する参考情

報の提供の取組みを検討している。そうした参考情報には、前節で示した調査結果を反映することが重要であると考えている。

6. データ集

「4.アンケート調査」の設問及び単純集計結果を以下に示す。

6.1 回答企業の属性情報

S1　貴社の総従業員数（有給役員,正社員・正職員,準社員・準職員,アルバイト等を含む）について、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。

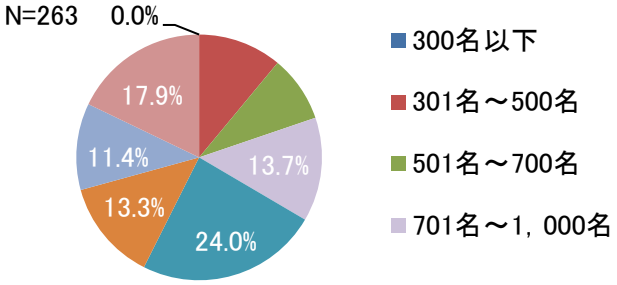

図 6.1-1　従業員数

S2　貴社の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。

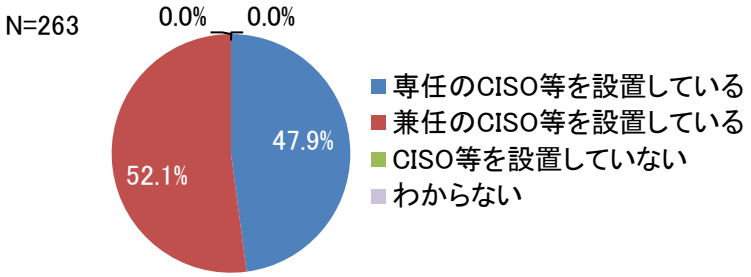

図 6.1-2　CISO 等設置状況

S3　貴社におけるあなたの立場として最も近いものを 1 つお選びください。

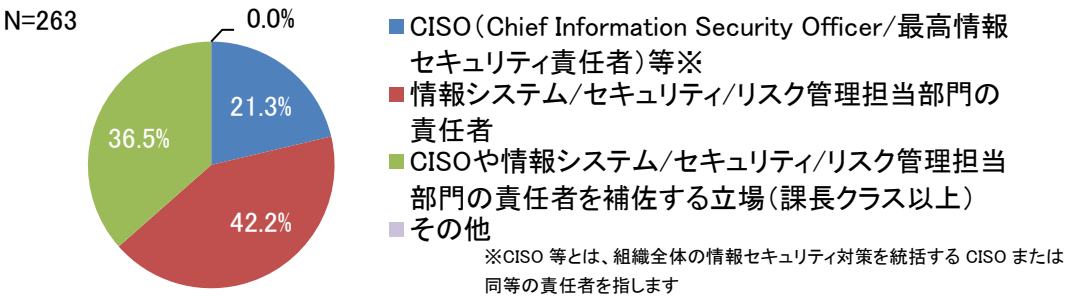

図 6.1-3　回答者の役職

S4　貴社の主な業種（日本標準産業分類に基づく）について、当てはまるものを 1 つお選びください。

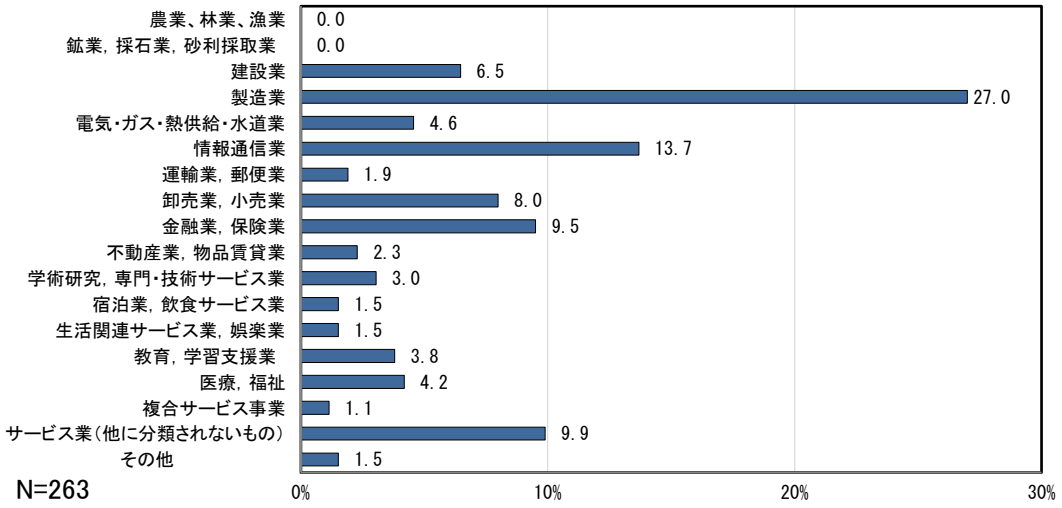

図 6.1-4　業種

S5　貴社の総売上高について、直近の会計年度の金額として、当てはまるものを 1 つお選びください。

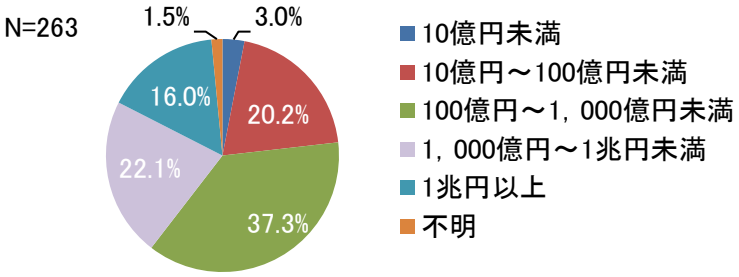

図 6.1-5　総売上高

6.2 IT 依存度

問 1　貴社事業の IT システム・IT サービスの依存度について、最も近いものを 1 つお選びください。

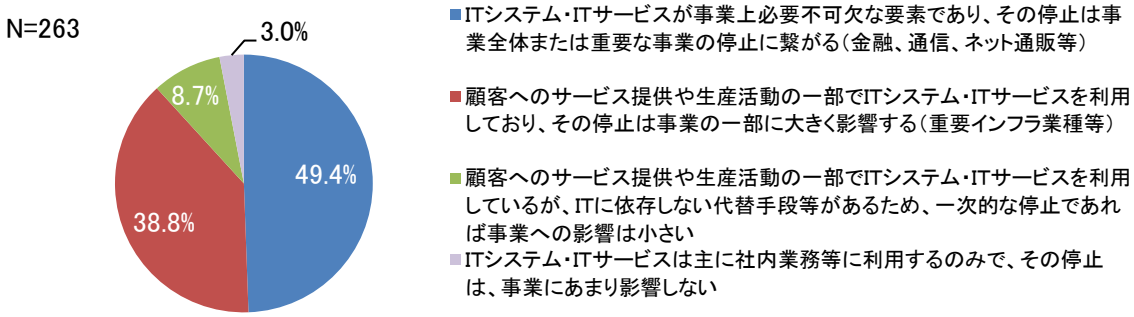

図 6.2-1　IT 依存度（現在）

問 2　貴社事業の IT システム・IT サービスへの依存度は、今後どのようになる見込みですか。当てはまるものを 1 つお選びください。

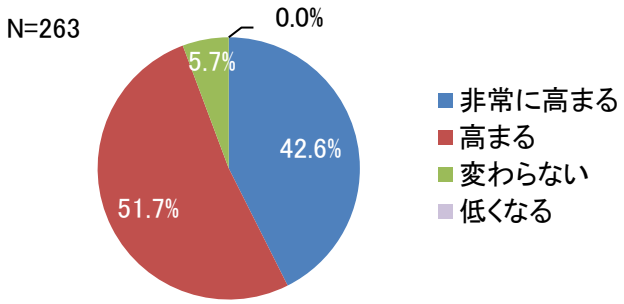

図 6.2-2　IT 依存度（今後）

6.3 経営層の認識・リスク分析実施状況

問 3　貴社の経営層のセキュリティに対する関与について、お伺いします。経営層が主体的に、自社のセキュリティリスクや対策、投資計画を審議する会議等について、当てはまるものを 1 つお選びください。

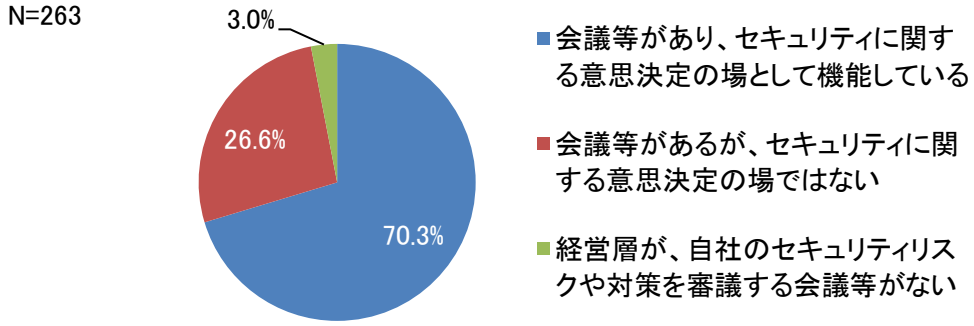

図 6.3-1　経営層の認識

問 4　貴社では、セキュリティ上のリスク（情報漏えい、サイバー攻撃等によるシステム停止等）を経営・事業上のリスク分析の対象とし、分析・評価を実施していますか。当てはまるものを 1 つお選びください。

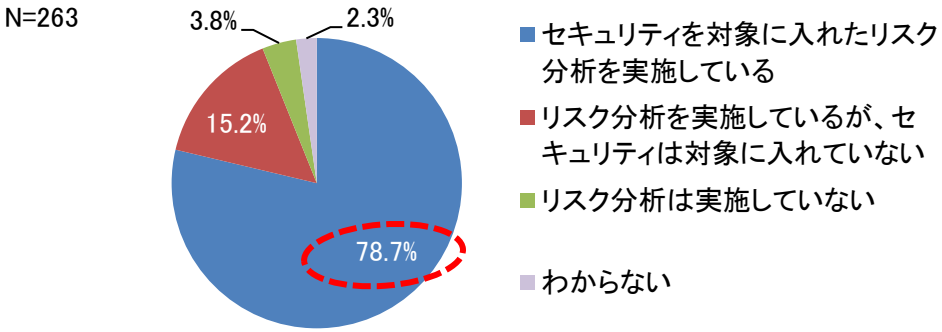

図 6.3-2　リスク分析実施状況

6.4 CISO 等に関する基本情報

問 5　貴社の CISO 等の位置づけとして最も近いものを 1 つお選びください。

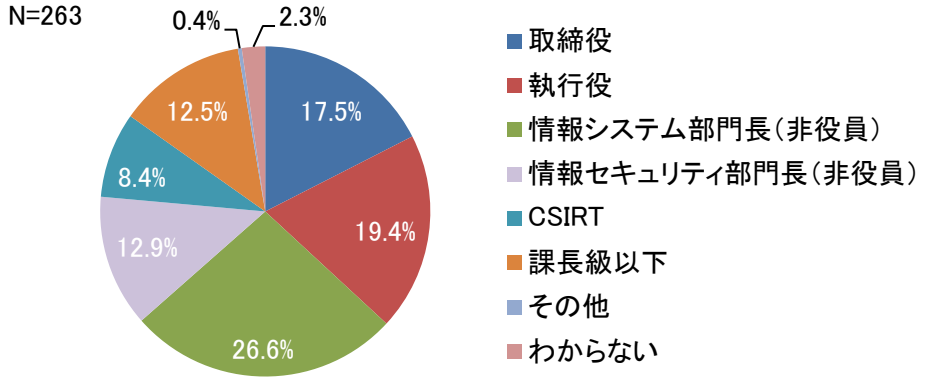

図 6.4-1　CISO 等の組織での位置づけ

問 6　貴社の現在の 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。

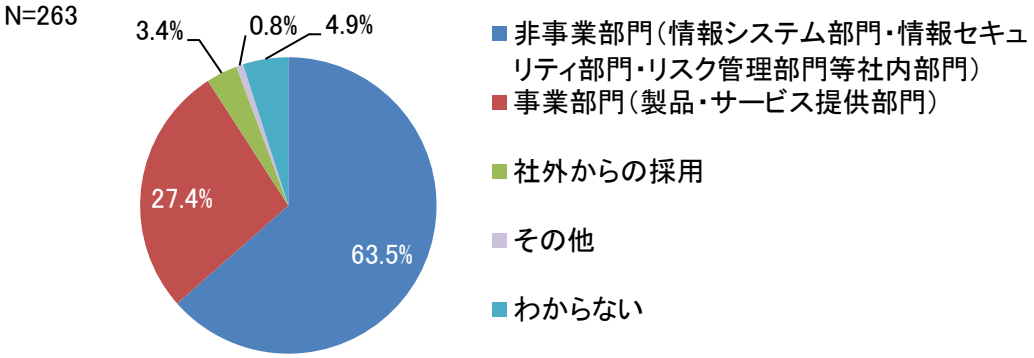

図 6.4-2　CISO 等の前の所属組織

問 7　貴社の CISO 等が有する権限として、当てはまるものを全てお選びください。

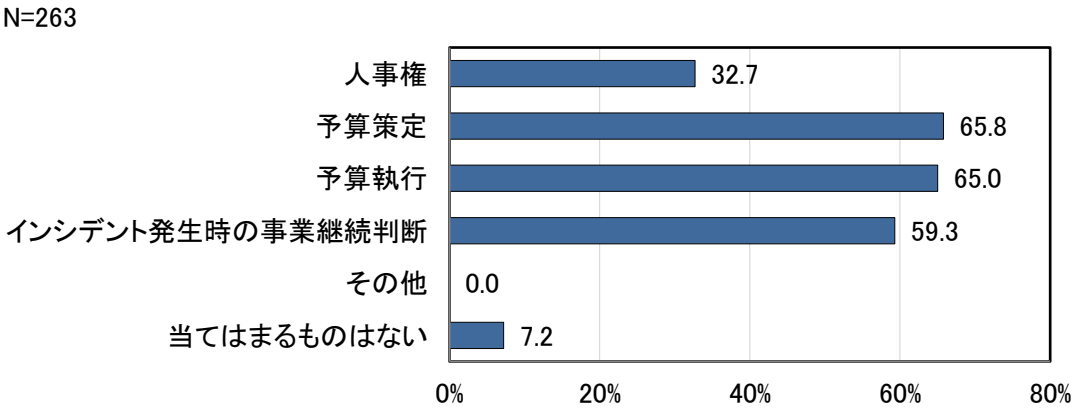

図 6.4-3　CISO 等が有する権限

問 8　貴社が保有するシステム及び提供する製品・サービスのセキュリティの確保に関して、責任を有する主体として当てはまるものを、それぞれ 1 つお選びください。

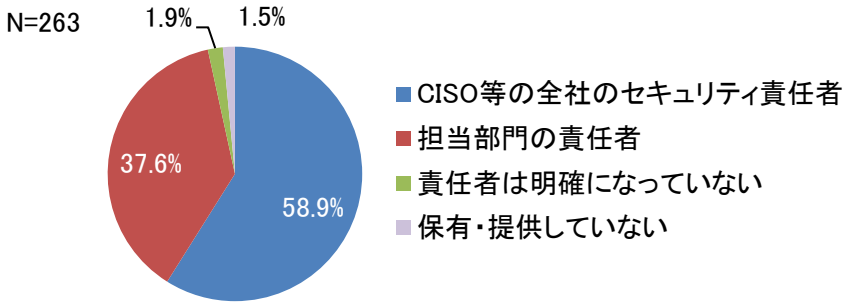

図 6.4-4　セキュリティ確保に関する責任者（社内情報システム）

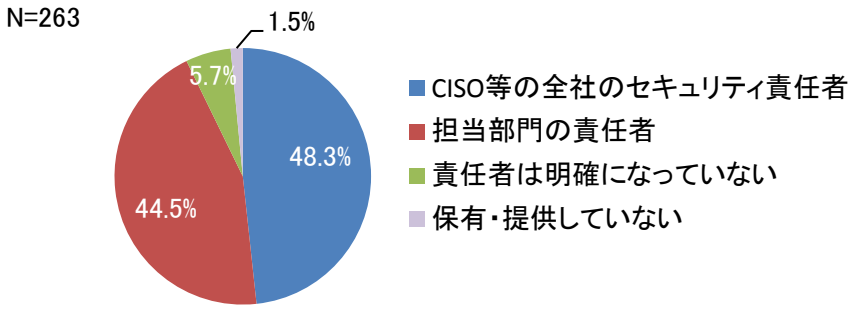

図 6.4-5　セキュリティ確保に関する責任者（事業部門が保有する情報システム）

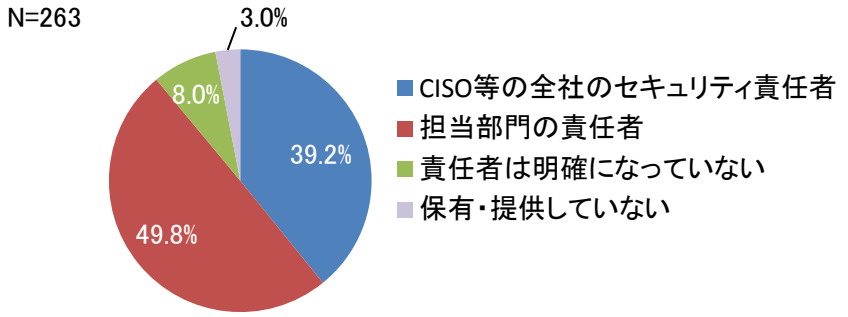

図 6.4-6　セキュリティ確保に関する責任者（事業部門が保有する制御システム）

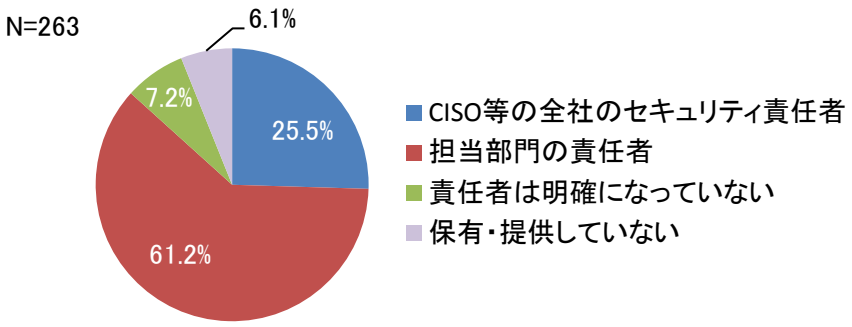

図 6.4-7　セキュリティ確保に関する責任者（自社製品）

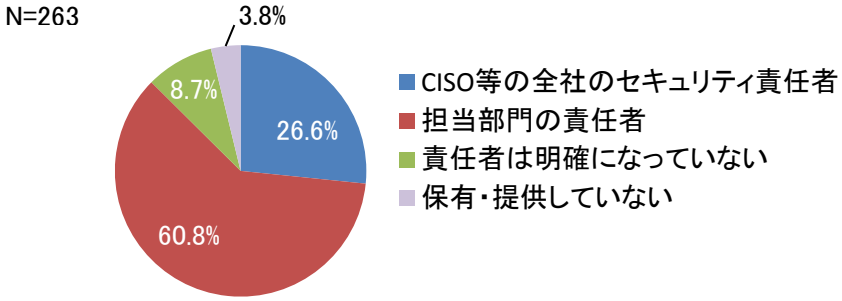

図 6.4-8　セキュリティ確保に関する責任者（自社サービス）

問 9　貴社の CISO 等が報告義務を負う上位職として当てはまるものを、全てお選びください。

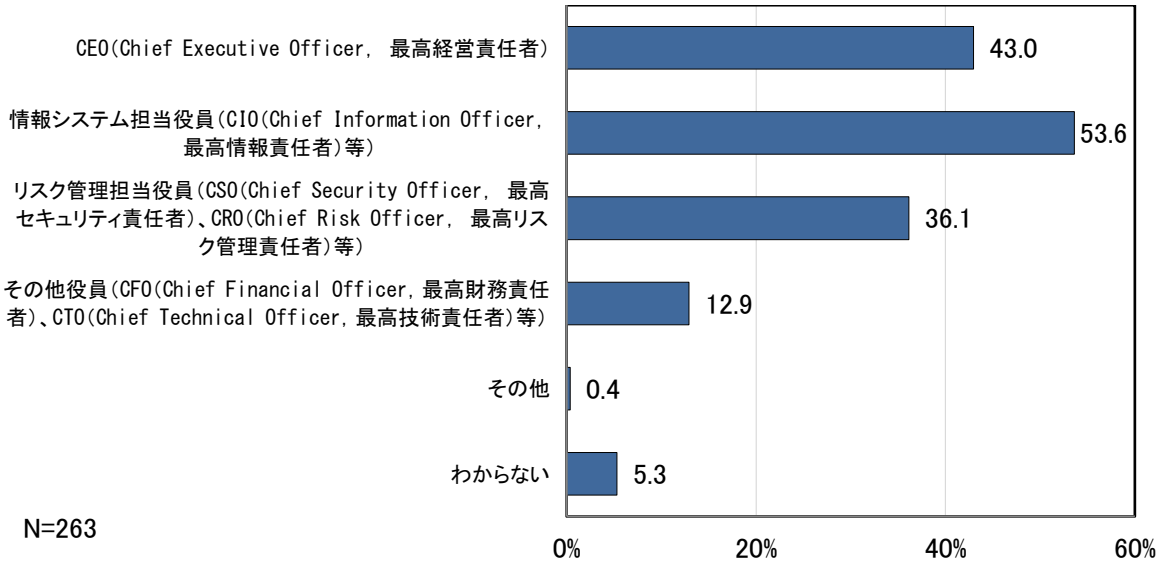

図 6.4-9　CISO 等が報告義務を負う上位職

6.5 CISO 等のサポートメンバー設置状況

問 10（1）　貴社では、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。

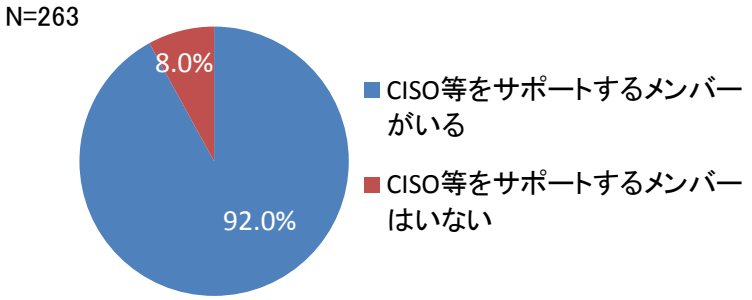

図 6.5-1　CISO 等をサポートするメンバーの有無

問 10（2）　CISO 等をサポートするメンバーの出身・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。

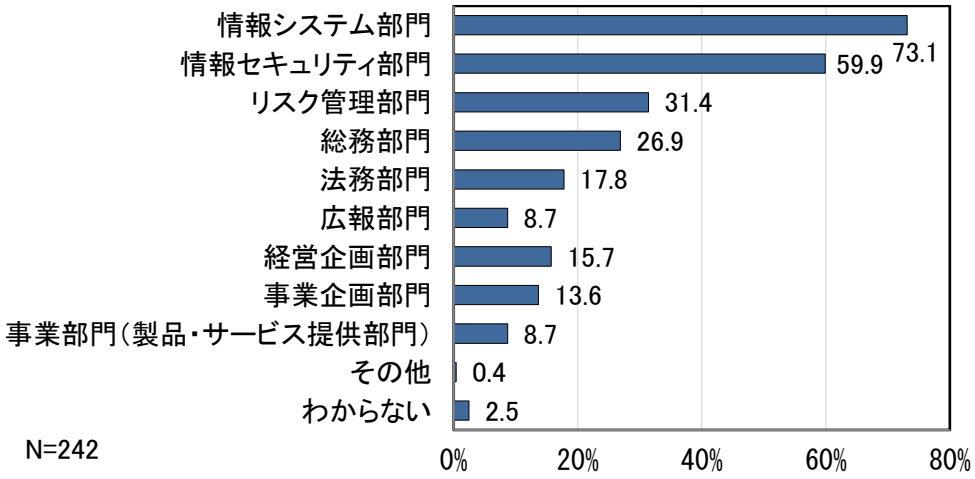

図 6.5-2　CISO 等のサポートメンバーの構成

問 10（3）　貴社で CISO 等をサポートするメンバーがいる理由として、当てはまるものを 3 つまでお選びください。

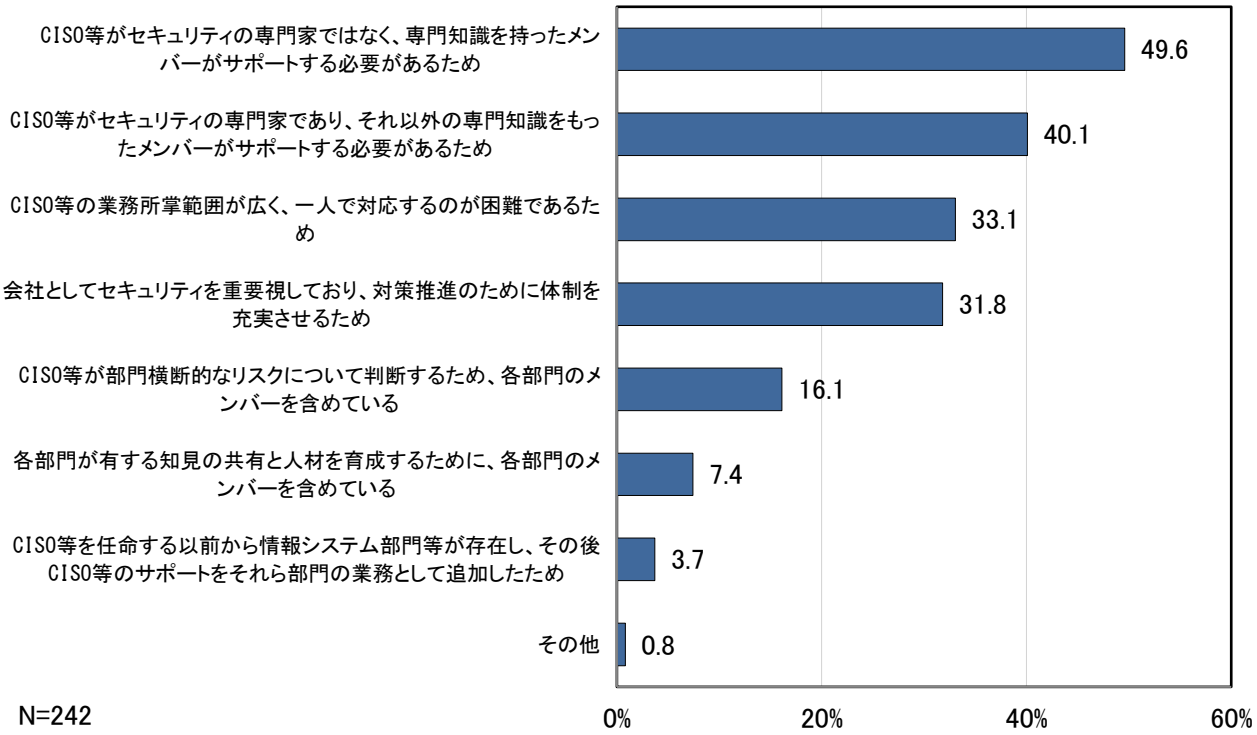

図 6.5-3　CISO 等サポートメンバーの設置理由

6.6 経営層が CISO 等に求める役割

問 11（1）　貴社の経営層が現在 CISO 等に求める役割として重要視しているのは、「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。

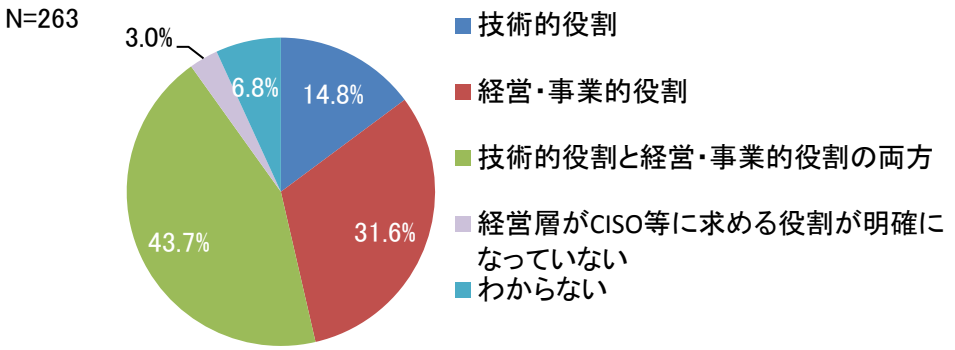

図 6.6-1　経営層が CISO 等に求める役割

問 11（2）　貴社の経営層が「経営・事業的役割」を重要視する理由として、当てはまるものを 3 つまでお選びください。

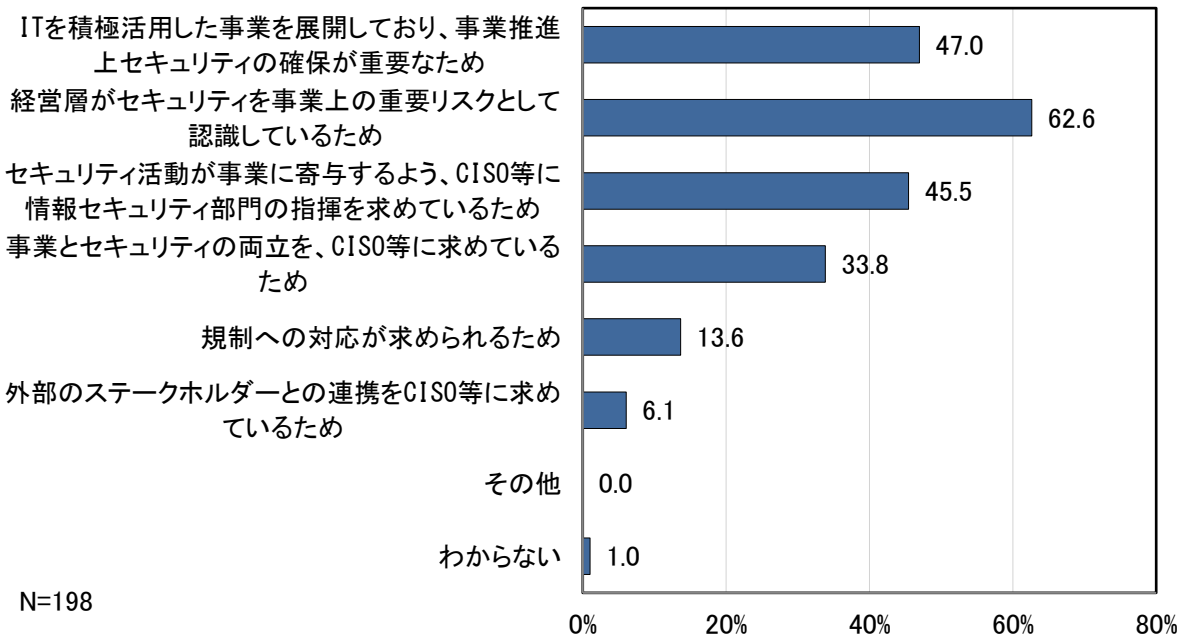

図 6.6-2　経営層が経営・事業的役割を重要視する理由

問 11（3）　貴社の経営層が「経営・事業的役割」を重要視しない理由として、当てはまるものを 3 つまでお選びください。

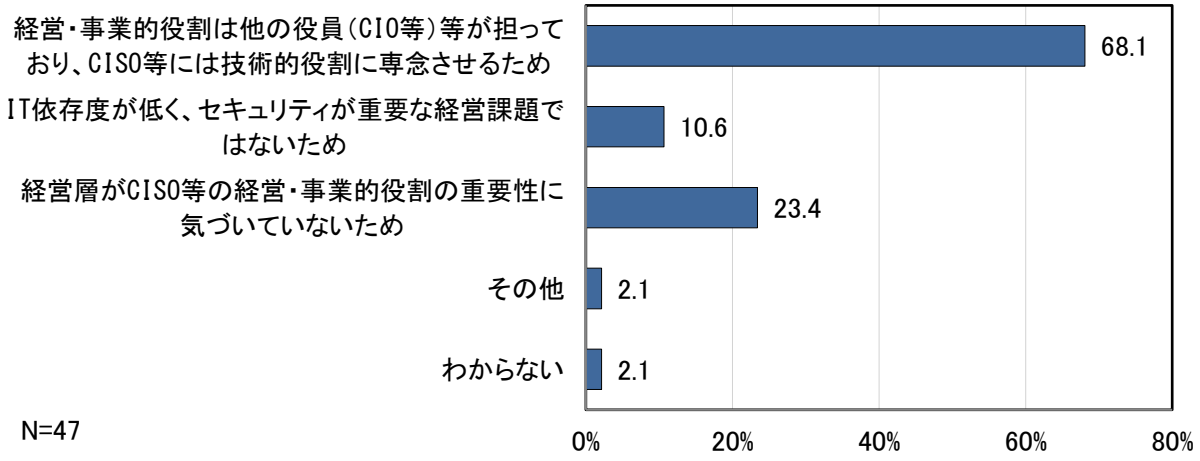

図 6.6-3　経営層が経営・事業的役割を重要視しない理由

6.7 CISO 等に求められる役割

問 12（1）　貴社の CISO 等が有する役割として当てはまるものを全てお選びください。

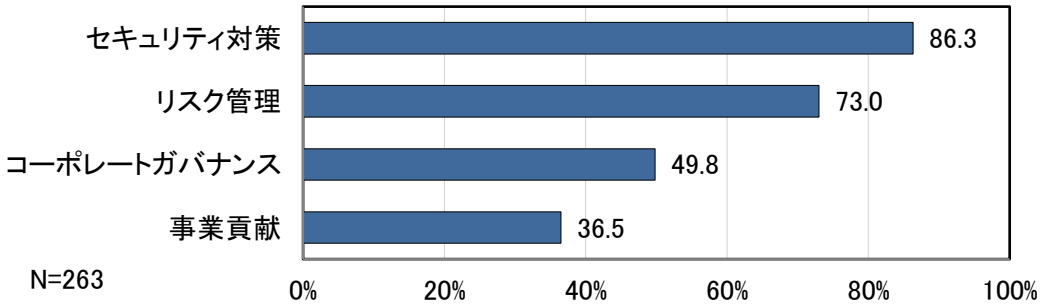

図 6.7-1　CISO 等が有する役割

問 12（2）　貴社の CISO 等の各役割のおおよその従事割合（%）をお答えください。各役割の従事割合は 0～100 の値を入力いただき、合計が 100 となるように入力してください。

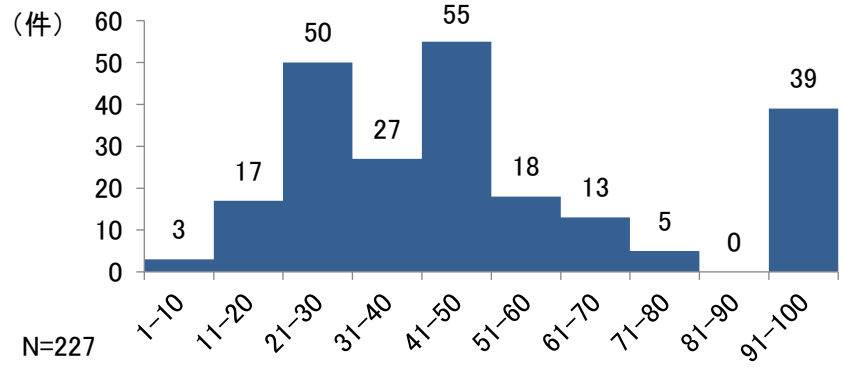

図 6.7-2　CISO 等が有する役割の従事割合（セキュリティ対策）

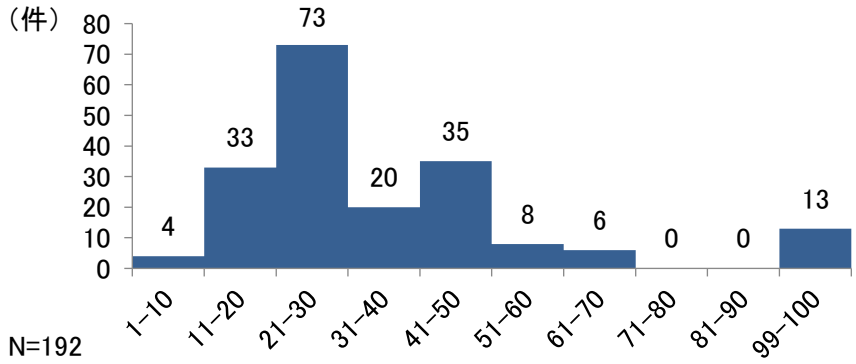

図 6.7-3　CISO 等が有する役割の従事割合（リスク管理）

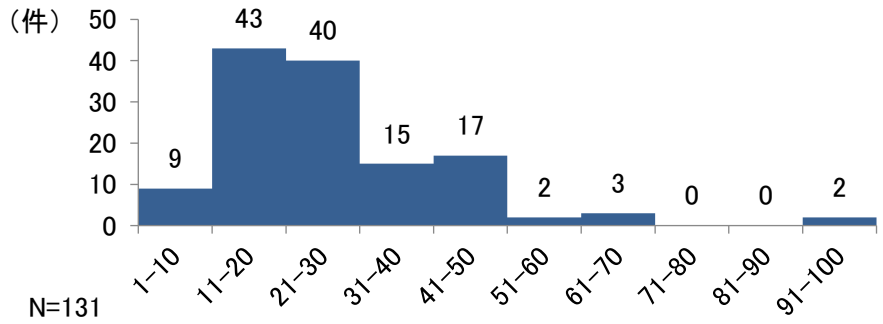

図 6.7-4　CISO 等が有する役割の従事割合（コーポレートガバナンス）

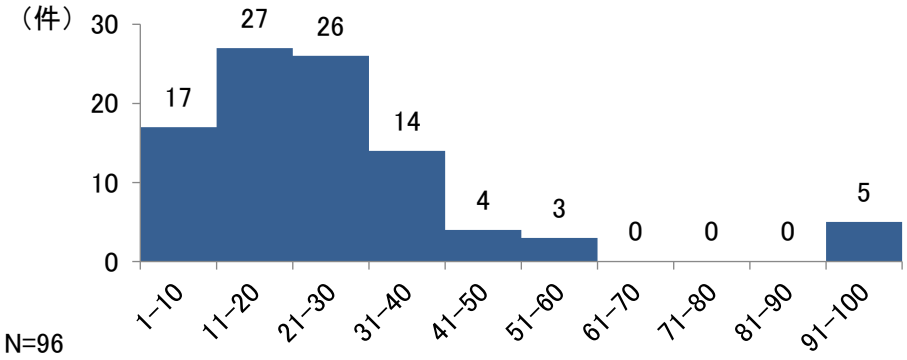

図 6.7-5　CISO 等が有する役割の従事割合（事業貢献）

6.8 CISO 等が担う経営・事業的役割

問 13（1）　貴社の CISO 等が有する経営・事業的役割として当てはまるものを全てお選びください。

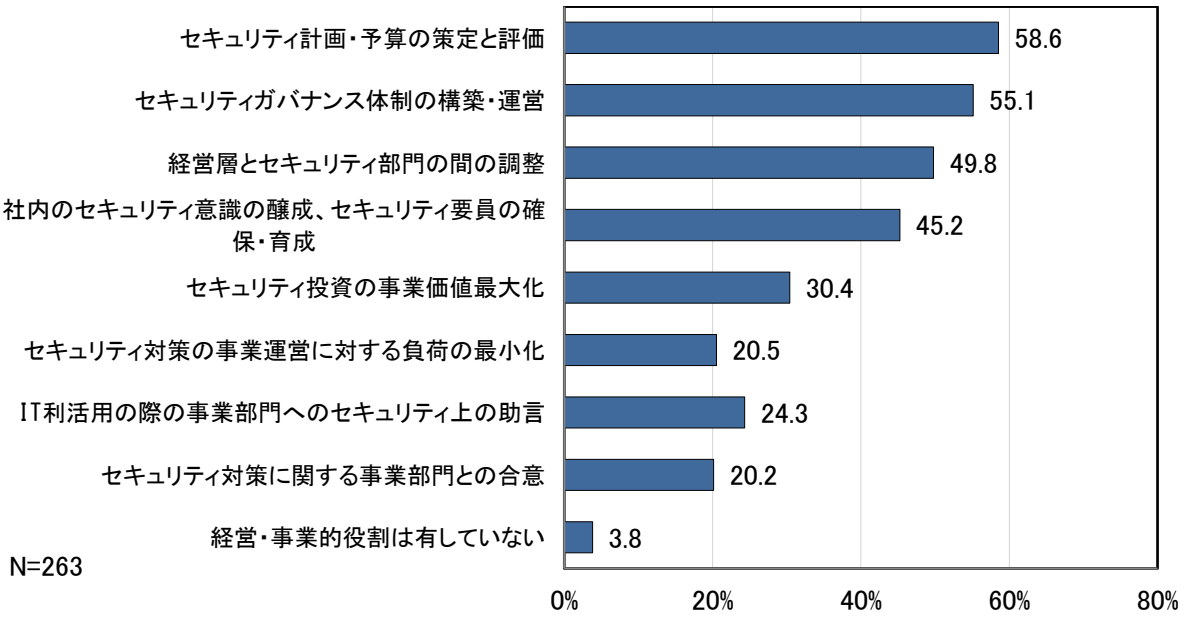

図 6.8-1　CISO 等が担う経営・事業的役割

問 13（2）　貴社の CISO 等は経営・事業的役割を十分に遂行していますか。当てはまるものを 1 つお選びください。

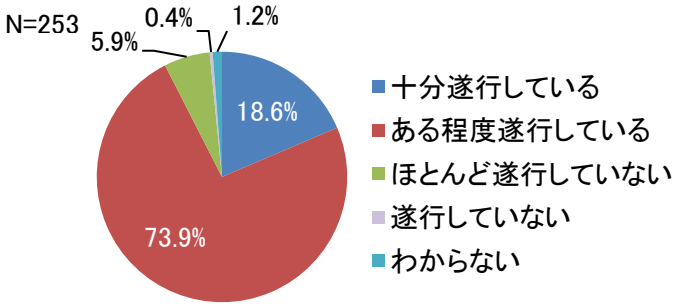

図 6.8-2　CISO 等の経営・事業的役割の遂行状況

問 13（3）　貴社の CISO 等が経営・事業的役割を遂行している理由として、当てはまるものを 3 つまでお選びください。

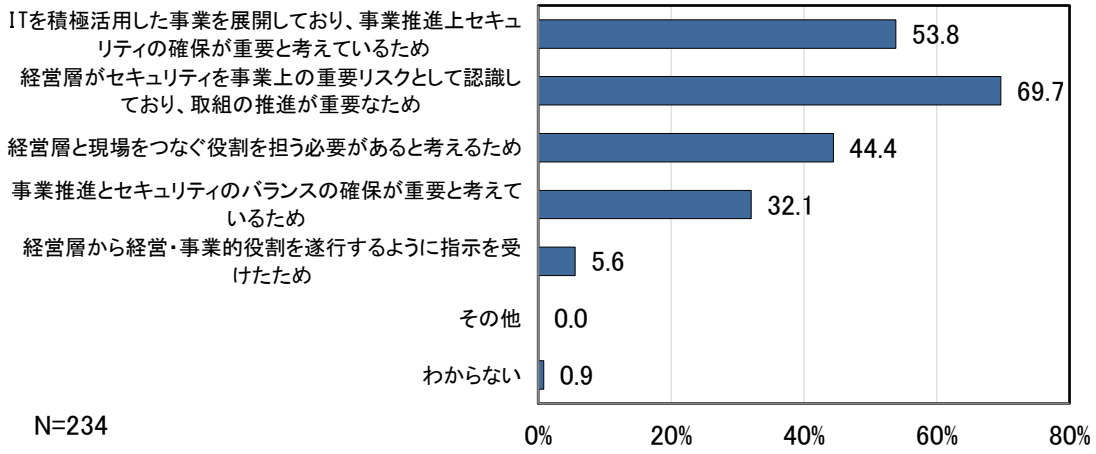

図 6.8-3　経営・事業的役割を遂行している理由

問 13（4）　貴社の CISO 等が経営・事業的役割を遂行していない理由として、当てはまるものを 3 つまでお選びください。

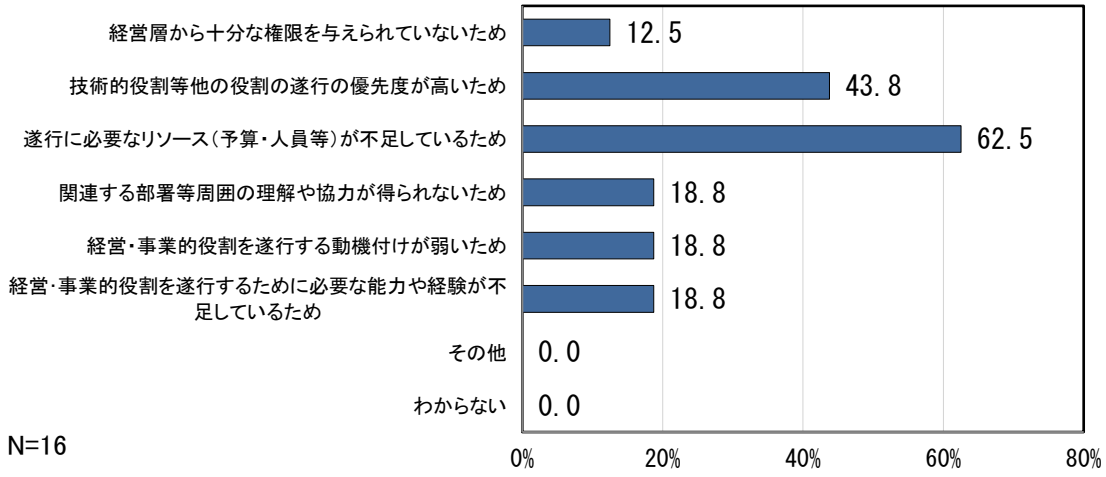

図 6.8-4　経営・事業的役割を遂行していない理由

6.9 CISO 等が役割を遂行する上で必要となる権限の付与状況

問 14（1）　貴社の CISO 等が役割を遂行する上で、十分な権限（予算策定やリソース確保、セキュリティ対策の推進等）を経営層から与えられていますか。

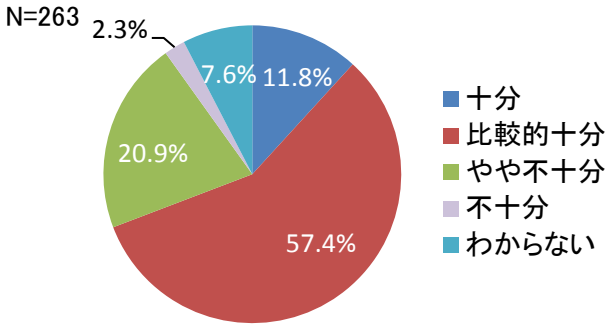

図 6.9-1　CISO 等が役割を遂行する上で必要な権限の付与状況

問 14（2）　十分な権限が経営層から付与されない理由として、当てはまるものを 3 つまでお選びください。

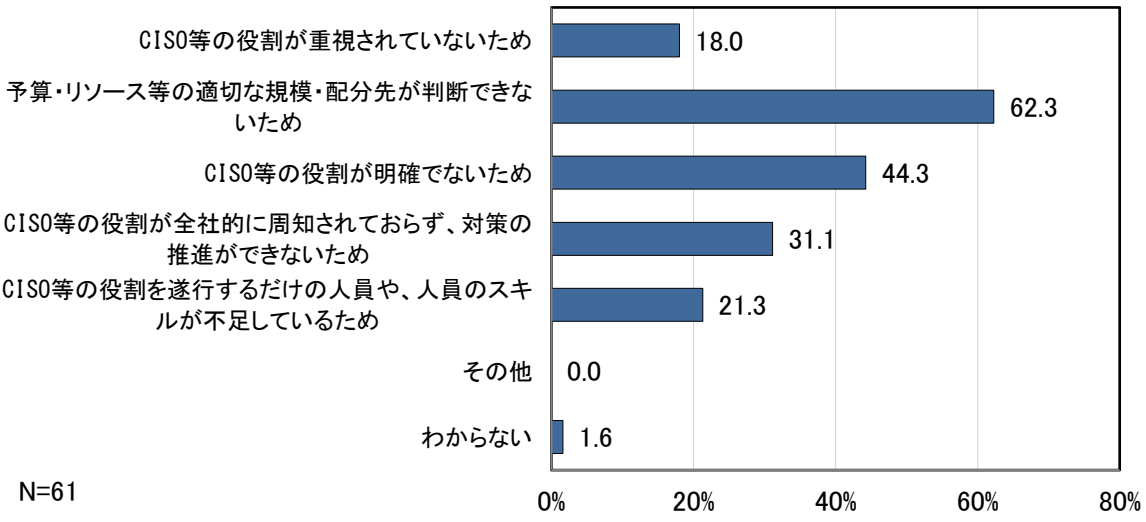

図 6.9-2　CISO 等が役割を遂行する上で必要な権限の付与が不十分な理由

6.10 CISO 等に求められるスキル・経験

問 15　貴社では 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られていますか。重視する能力を 3 つまでお選びください。

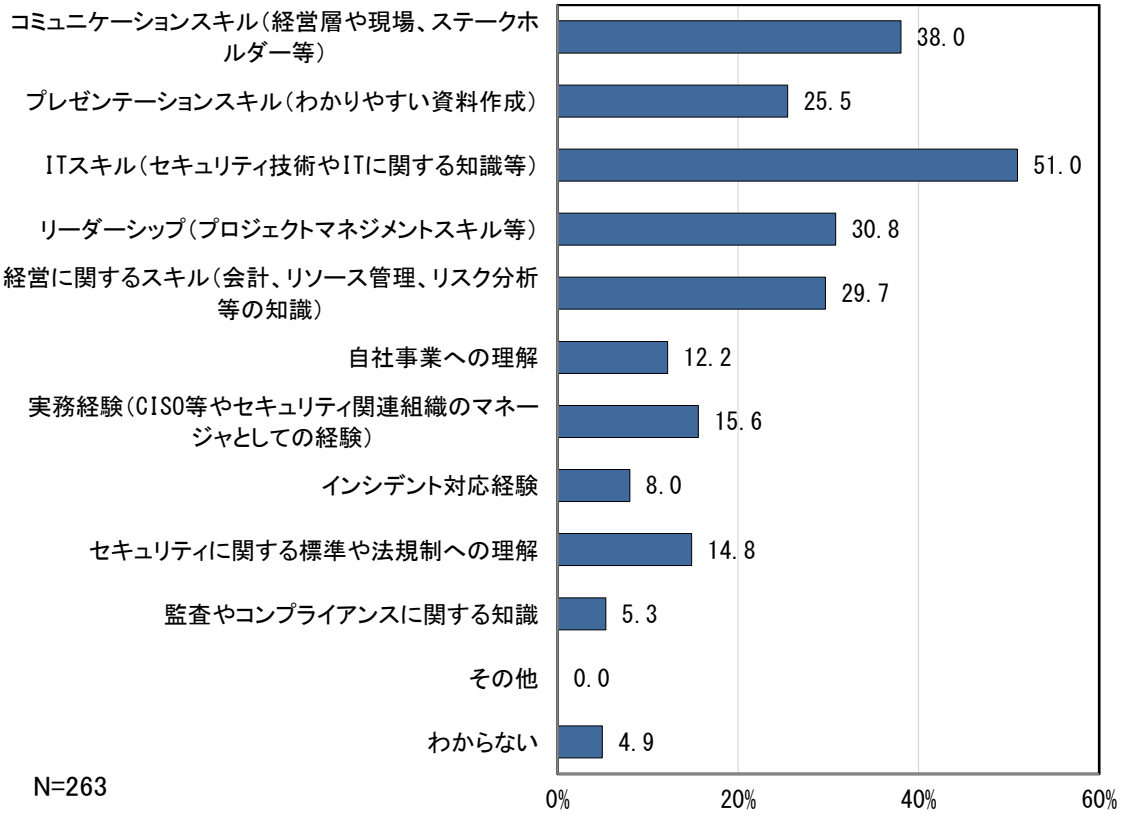

図 6.10-1　CISO 等において重要なスキル・経験

6.11 セキュリティ対策を進める上での課題

問 16　貴社のセキュリティ対策を推進する上での課題点について、特に課題と感じるものを 3 つまでお選びください。

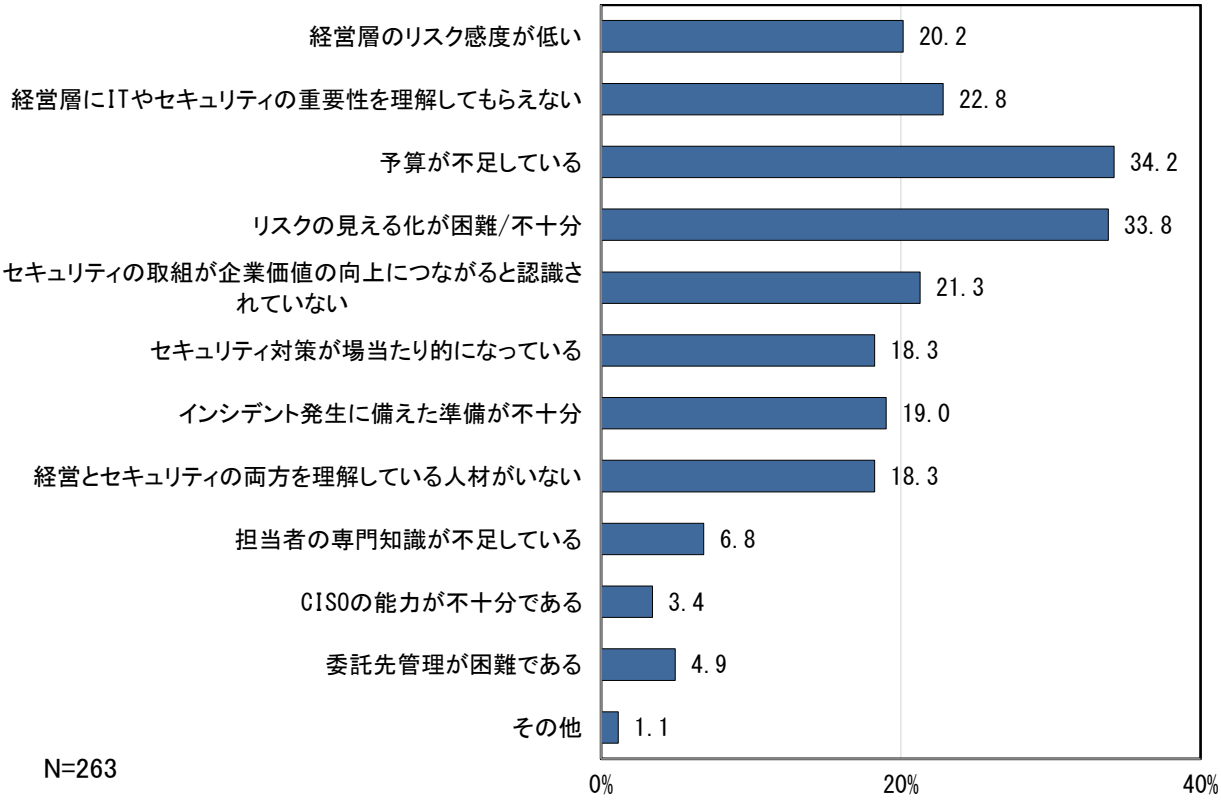

図 6.11-1　セキュリティ対策を推進する上での課題点