IPA Better Life with IT

サイバーセキュリティ経営における推進体制の現実
～調査から見るCISO等に求められる役割～

2018年5月11日
独立行政法人　情報処理推進機構
技術本部　セキュリティセンター　情報セキュリティ分析ラボラトリー

本日のプレゼンテーション

1. 概要・調査の背景
2. サイバーセキュリティ経営における
   推進体制の要
3. 有識者の「CISO等」に対する役割イメージ
4. 企業「CISO等」の現実
5. まとめ

1. 概要・調査の背景～その1～

- 概要
  - 今年3月末に公開した調査報告「CISO*等セキュリティ推進者の経営・事業に関する役割調査」をご紹介
- 調査の背景
  - 「サイバーセキュリティは経営問題」（METI/IPA「サイバーセキュリティ経営ガイドライン」）
    - 経営者のリーダーシップで、サイバーセキュリティ対策を進めよ
    - 経営者は、セキュリティリスクを経営リスクの一つとし、責任者となる担当幹部を任命すべし
  - CISO等セキュリティ推進者に求められる役割とその現実を調査

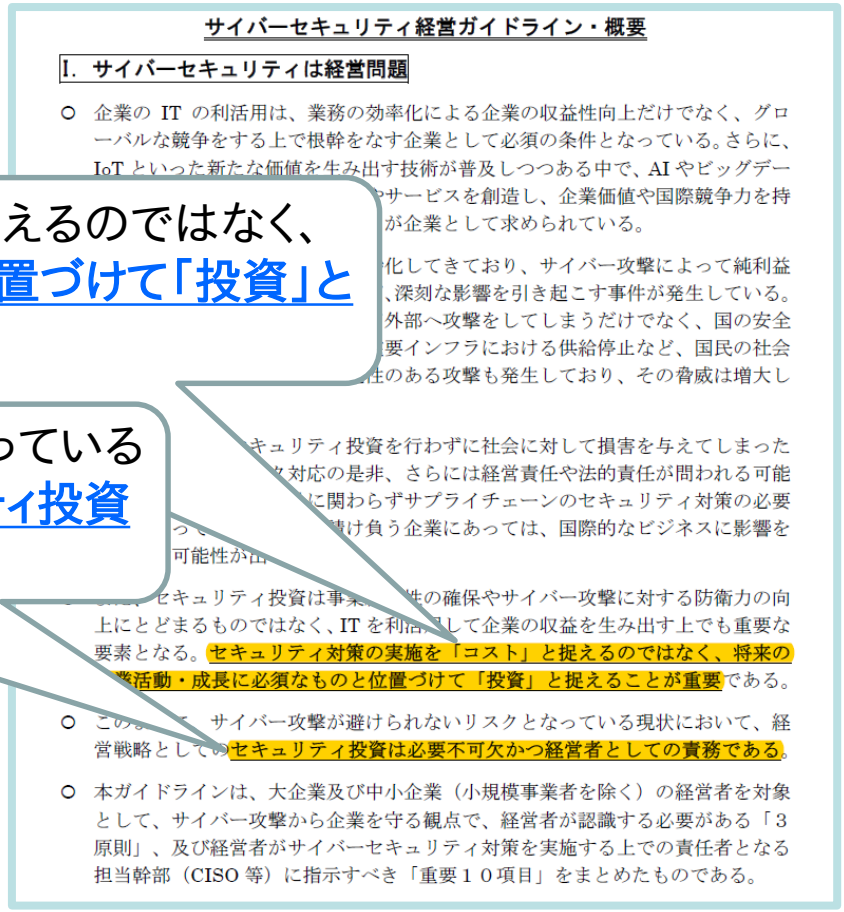
*CISO：Chief Information Security Officer；最高情報セキュリティ責任者

1. 概要・調査の背景～その2～

- 「サイバーセキュリティ経営ガイドライン」とは
  - 経営者のリーダーシップによって サイバーセキュリティ対策を推進 するため、経済産業省とIPAが 策定*

セキュリティ対策の実施を「コスト」と捉えるのではなく、**将来の事業活動・成長に必須なものと位置づけて「投資」と捉える**ことが重要

サイバー攻撃が避けられないリスクとなっている現状において、**経営戦略としてセキュリティ投資は必要不可欠**かつ**経営者の責務**



サイバーセキュリティ経営ガイドライン・概要

I. サイバーセキュリティは経営問題

○ 企業の IT の利活用は、業務の効率化による企業の収益性向上だけでなく、グローバルな競争をする上で根幹をなす企業として必須の条件となっている。さらに、IoT といった新たな価値を生み出す技術が普及しつつある中で、AI やビッグデー
サービスを創造し、企業価値や国際競争力を持
が企業として求められている。

化してきており、サイバー攻撃によって純利益
、深刻な影響を引き起こす事件が発生している。
外部へ攻撃をしてしまうだけでなく、国の安全
要インフラにおける供給停止など、国民の社会
性のある攻撃も発生しており、その脅威は増大し

キュリティ投資を行わずに社会に対して損害を与えてしまった
対応の是非、さらには経営責任や法的責任が問われる可能
に関わらずサプライチェーンのセキュリティ対策の必要
請け負う企業にあっては、国際的なビジネスに影響を
可能性が出

セキュリティ投資は事業
性の確保やサイバー攻撃に対する防衛力の向
上にとどまるものではなく、IT を利活用して企業の収益を生み出す上でも重要な
要素となる。セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の
業活動・成長に必須なものと位置づけて「投資」と捉えることが重要である。

○ この
サイバー攻撃が避けられないリスクとなっている現状において、経
営戦略としてセキュリティ投資は必要不可欠かつ経営者としての責務である。

○ 本ガイドラインは、大企業及び中小企業（小規模事業者を除く）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原則」、及び経営者が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（CISO 等）に指示すべき「重要１０項目」をまとめたものである。

- 本プレゼンでは「サイバーセキュリティ経営ガイドライン」で掲げられた上記考えに基づく企業経営を「**サイバーセキュリティ経営**」と呼ぶ

*:2015年初版策定、最新版はVer.2.0（2017年11月改訂）;http://www.meti.go.jp/policy/netsecurity/mng_guide.html

2. サイバーセキュリティ経営における推進体制の要～その1～

- 経営者自らが手を動かし、セキュリティ対策方針策定や実務者指揮等の実務を担うことは困難

➢ 経営者が示す経営方針に基づき、関係部署をまとめ実務者層を指揮する「橋渡し人材層」が必要*

  - 本プレゼンでは、こうした人材を「CISO等セキュリティ推進者」と総称し、「CISO等」と略記
    - ✓「CISO等」≠ CISO（相当の責任者）

- 「CISO等」は、サイバーセキュリティ経営の推進体制の要

*：サイバーセキュリティ戦略本部「サイバーセキュリティ人材育成プログラム」より
https://www.nisc.go.jp/active/kihon/pdf/jinzai2017.pdf

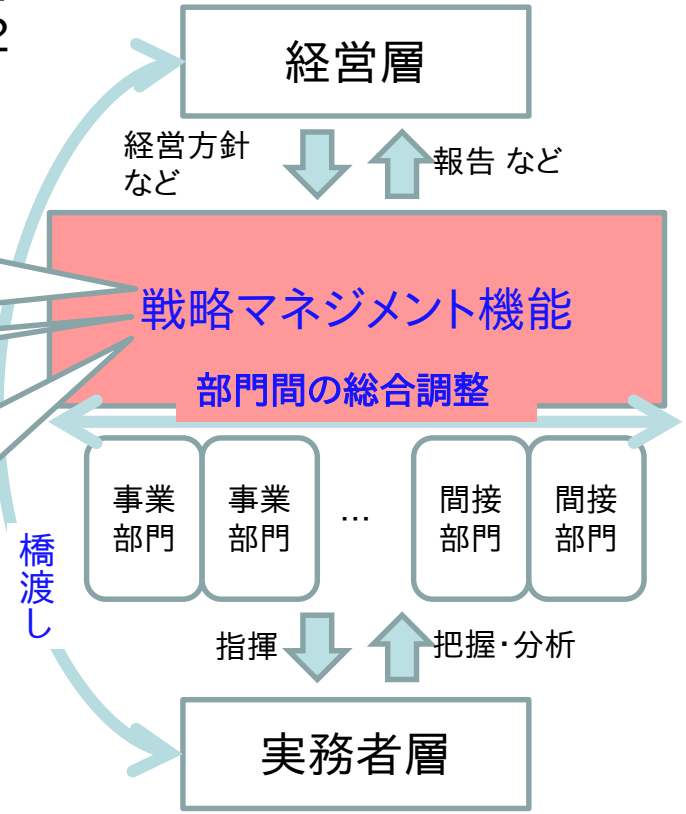
2. サイバーセキュリティ経営における推進体制の要～その2～

- 「CISO等」の役割の検討(1)
  - NISC[*1]資料「サイバーセキュリティ人材育成の検討の方向性（案）」[*2]

戦略マネジメント機能の遂行に必要となる**セキュリティ知識・スキル**などを習得

事業に関するセキュリティリスクが**事業利益・企業価値に与える影響**を把握・分析し経営層に説明

セキュリティ問題について他の部門と**チームとして連携**



*1：内閣官房　内閣サイバーセキュリティセンター
*2：http://www.nisc.go.jp/conference/cs/jinzai/wg2/dai02/pdf/02shiryou0102.pdf

2. サイバーセキュリティ経営における推進体制の要～その3～

- 「CISO等」の役割の検討(2)
  - CISOに求められる4つの顔（海外での議論の例）
  - 従来重視されてきたのは
    - 守護者
      - 情報資産の保護
    - 技術者
      - セキュリティ技術の調査・実装
  - 今後重要になるのは
    - **戦略家**
      - 事業とセキュリティ戦略を整合
      - 有効なセキュリティ投資でリスクマネジメント
    - （事業部門への）**アドバイザ**
      - セキュリティ活動や助言を事業と整合

（出典）Deloitte, “The new CISO – Leading the strategic security organization”, 2016 に基づきIPA作成

2. サイバーセキュリティ経営における推進体制の要～まとめ～

- このように、セキュリティ技術に関する役割に加え、企業の**セキュリティへの取組みが、経営と事業にしっかり貢献するようにマネジメントする役割**の必要性・重要性を指摘する文献、検討が増えている
  - 本プレゼンでは、こうした役割を「**経営・事業的役割**」と呼ぶ

3. 有識者の「CISO等」に対する役割イメージ～その1～

- 企業のセキュリティマネジメントに関する専門家・有識者へインタビュー

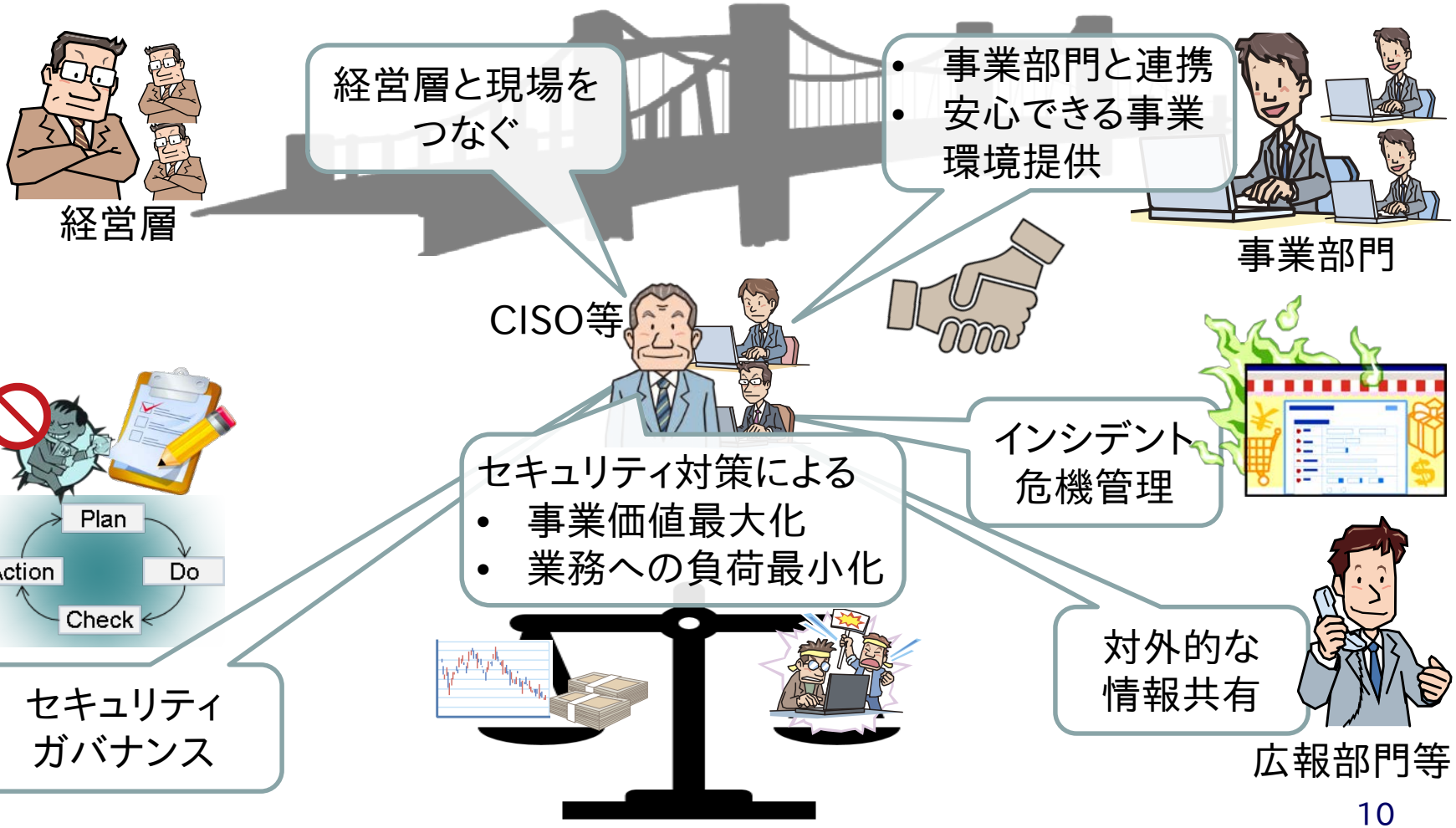
- インタビュー対象者
  - セキュリティに関する企業団体のリーダ
  - セキュリティコンサルティング会社幹部
  - 海外の有力セキュリティ関連団体役員
  - CISO養成プログラムを有する海外大学のプログラム責任者

- インタビュー項目
  - 「CISO等」の課題
  - 「CISO等」に求められる経営・事業的役割
  - そうした役割を担う上での課題・ポイント
  - 「CISO等」に対し、経営・事業的役割を重視している企業の特徴

など

3. 有識者の「CISO等」に対する役割イメージ～その2～

有識者が「CISO等」に求める「経営・事業的役割」



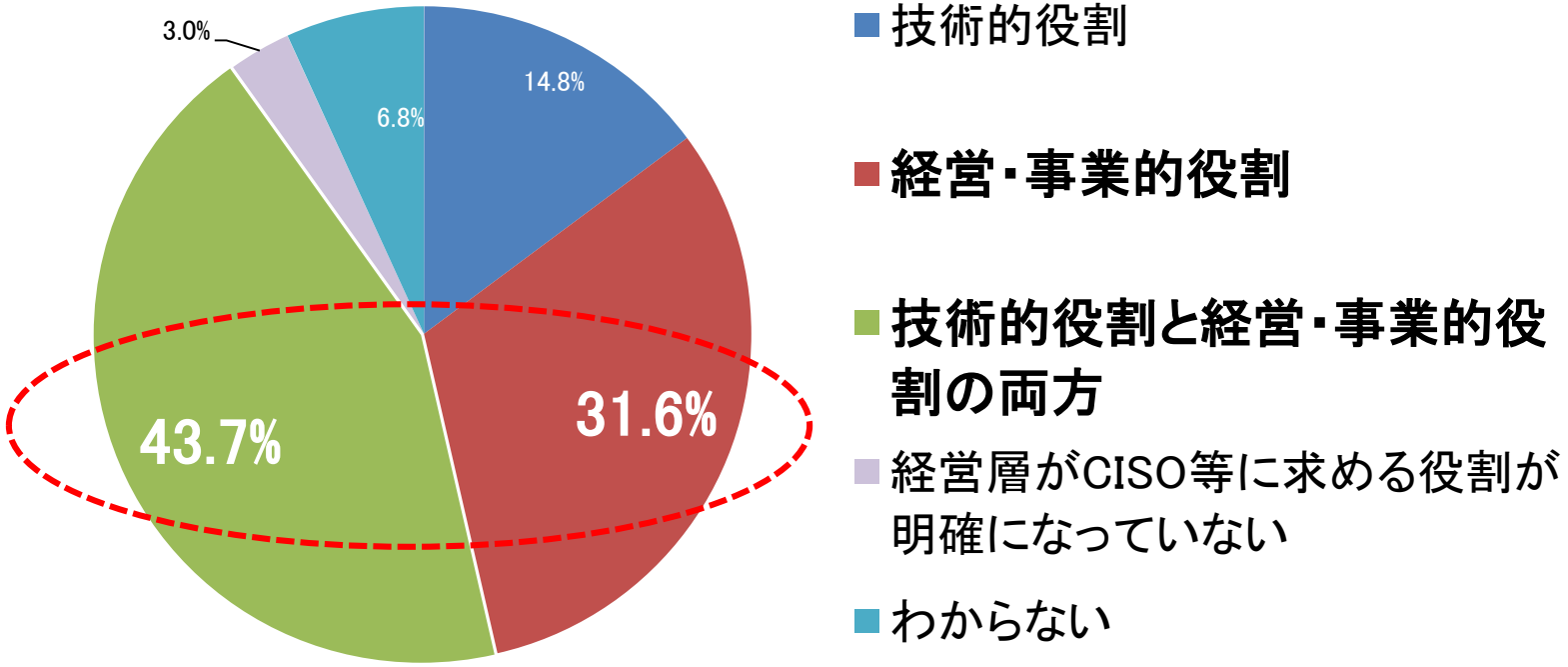
4. 企業「CISO等」の現実

- 企業の「CISO等」の実態に関して、関係者・当事者へアンケート調査

  - 回答者
    - 「CISO等」を任命している日本企業（従業員数301名以上）
    - 情報セキュリティに責任を持つ部門長以上、およびその補佐役
    - 有効回答数 263件
  - 調査期間・手法
    - 2017年10月下旬～11月中旬
    - Webアンケート調査
  - 調査項目
    - 「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　など

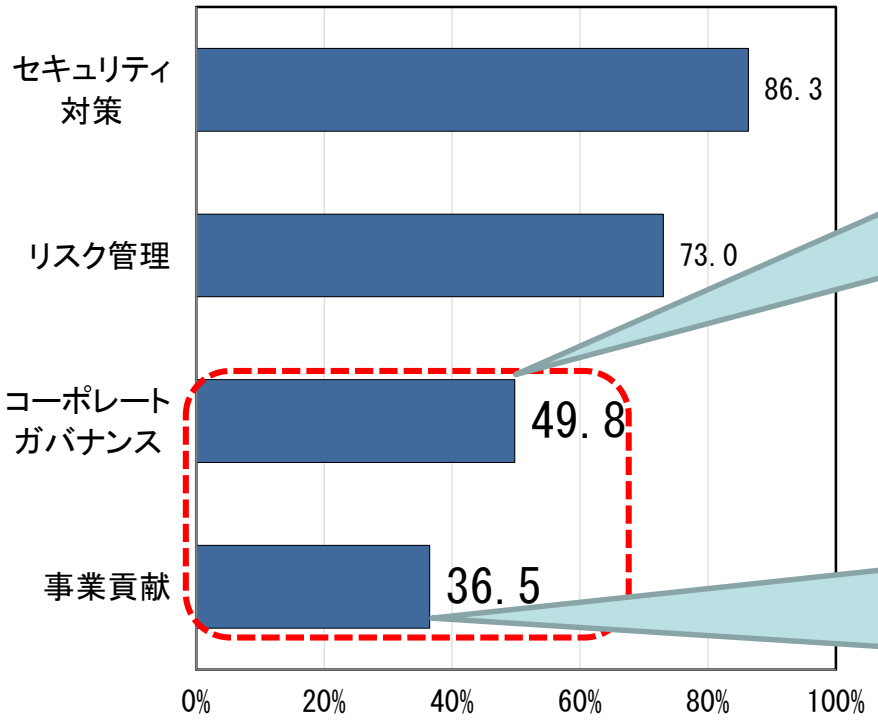
4. 企業「CISO等」の現実 ～役割についての調査結果その1～

① 多く（75%超）の企業経営者は、経営的役割や事業的役割を、「CISO等」に求める役割として重視している



4. 企業「CISO等」の現実 ～役割についての調査結果その2～

② しかし、コーポレートガバナンスや事業貢献を担っている「CISO等」は、半数以下に留まる



経営に関連する役割

- セキュリティ計画・予算の策定と評価
- セキュリティガバナンス体制の構築・運営
- 経営層とセキュリティ部門の間の調整
- 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

など

事業に関連する役割

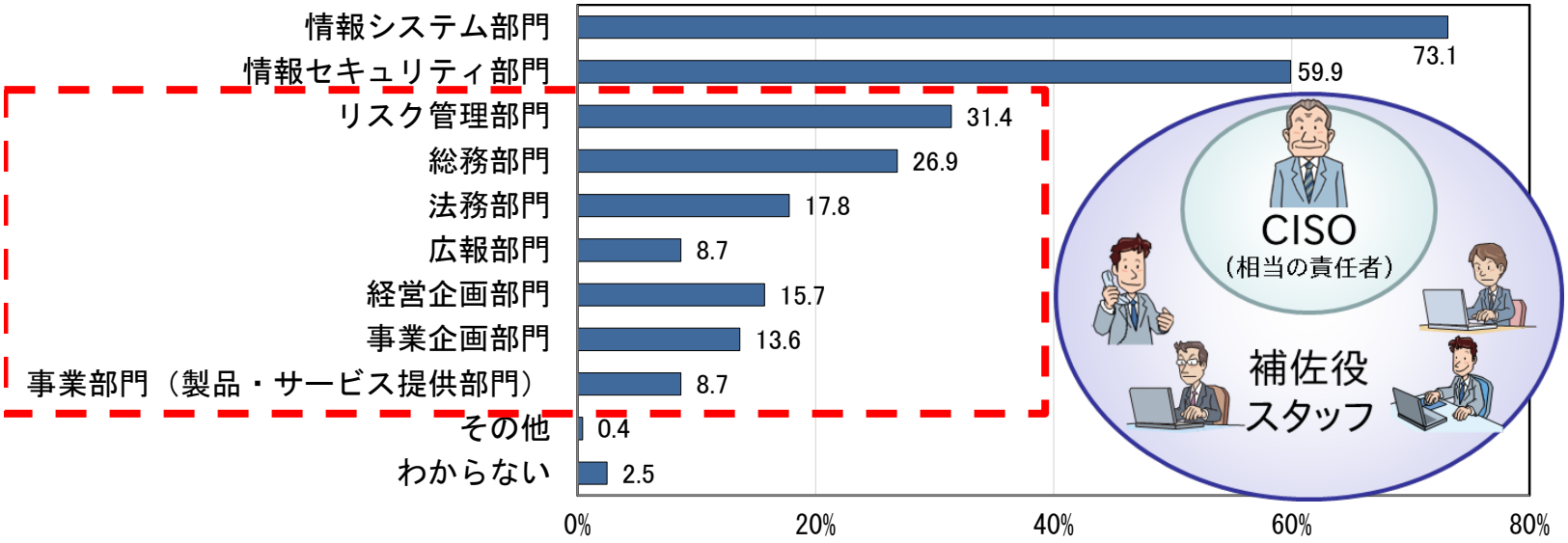
- セキュリティ投資の事業価値最大化
- セキュリティ対策の事業運営に対する負荷の最小化
- IT利活用の際の事業部門へのセキュリティ上の助言
- セキュリティ対策に関する事業部門との合意

など

4. 企業「CISO等」の現実
～支援メンバについての調査結果その1～

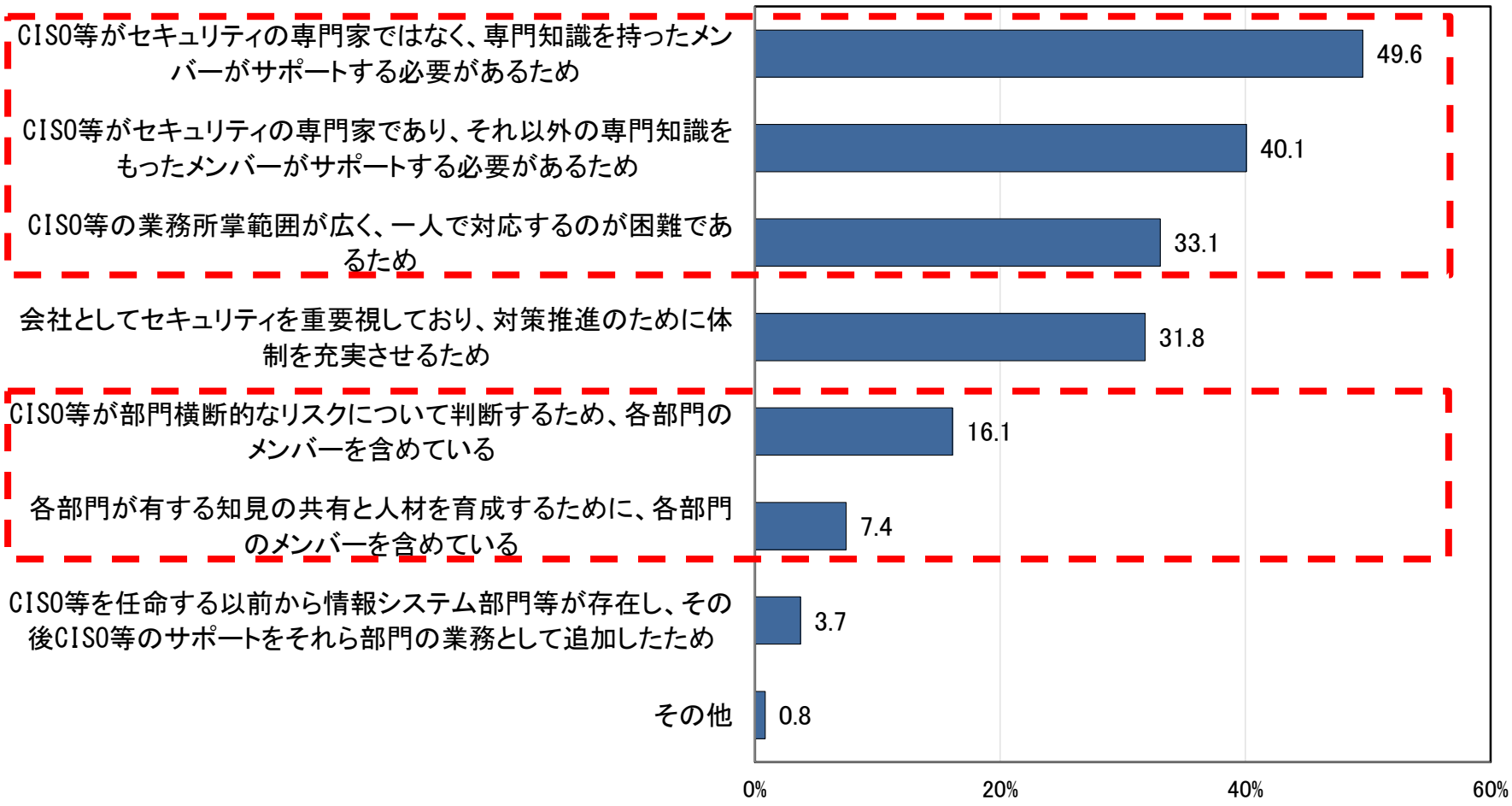
① ほとんどの企業（92%）が「CISO等」をサポートするメンバを設置

② サポートメンバの出身・所属は、情シス、セキュリティ部門以外に、**リスク管理、総務、法務、広報**など様々



4. 企業「CISO等」の現実
～支援メンバについての調査結果その2～

③ 主な理由は、広範な専門性をカバーするため



5. まとめ

- CISO等セキュリティ推進者は、サイバーセキュリティ経営における推進体制の要である
- 「CISO等」には、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主導**する役割が求められる
  - 「橋渡し人材」、「戦略マネジメント機能担当」…
- 現状、**経営・事業的役割を担っている「CISO等」は半数以下**に留まっている
- 「CISO等」に必要となる多様な専門性は、様々な出身・所属部門のメンバーが共同して提供している

本プレゼンの詳細については、IPAホームページで公開中の調査報告書をご覧ください。
「CISO等セキュリティ推進者の経営・事業に関する役割調査報告書」
https://www.ipa.go.jp/security/fy29/reports/ciso/index.html