Vol.2018-EIP-79 No.7
2018/2/16

情報セキュリティガバナンス体制について

金子啓子† 原田要之助†

概要：情報システム部門は、情報セキュリティだけではなく、現実の運用やコストダウンの要求への対応、新たなシステムの企画・開発・導入など、様々な要請を解決する立場にあり、必ずしも情報セキュリティが優先されるわけではない。権限分離を考えると、情報セキュリティの社内ガバナンスは情報システム部門とは異なる別の部門が担当するべきかもしれないが、情報システム部門との緊張関係も生じ、リソースやスキル上の重複という課題もある。
この論文では、情報セキュリティ大学院大学原田研究室のアンケート結果の分析等により、CISO を始めとした情報セキュリティガバナンス体制の現状と課題を分析し、あるべき体制を考察する。

キーワード：情報セキュリティガバナンス　CISO

On Organization for Information Security Governance

KEIKO KANEKO†1　YONOSUKE HARADA†1

Abstract: The information systems department is in a position to solve various requests such as not only information security but also actual operation and cost reduction, and planning, development and introduction of new systems. Thus information security is not always prioritized. From the view point of the segregation of authority, internal governance of information security should be handled by another department than the information system department, but there are a tense relationship with the information systems department, and resources and skill issues.
This paper analyzes the present situation and issues of information security governance organization such as CISO by analyzing questionnaire result of Harada Laboratory of Institute of Information Security and considers how it should be.

Keywords: information security governance, CISO

1. はじめに

「係長セキュリティから社長セキュリティに」aと言われて久しい。情報セキュリティは IT の一部の対策ではなく、経営リスクの一つで、そのような視点で判断し推進しなければならない、というメッセージであった。また、2009 年に公表された経済産業省の「情報セキュリティガバナンス導入ガイダンス」においても、情報セキュリティガバナンスはコーポレートガバナンスの一環として確立され、IT のみならず、組織が価値を認めるあらゆる情報資産を対象とするとし、情報セキュリティと IT ガバナンスは一部重複するが明確に異なる関係としている。

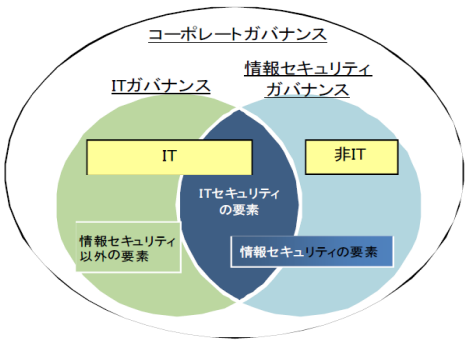

図 1　コーポレートガバナンスと情報セキュリティガバナンスの関係b

筆者が 2004 年に米国の進んだ IT 企業を訪問した際、初めに示されたのが、下記のような図であった。

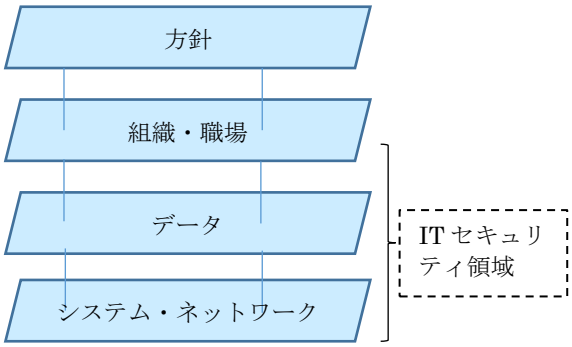

図 2 情報セキュリティ全体像と IT セキュリティの関係

これは、IT セキュリティが独自にあるのではなく、経営リスクの観点から何をどの程度守るか、どの範囲で情報を共有するか、などの方針ありきで、決めていくものである、という考え方であった。

筆者も、経営上、やみくもに、情報セキュリティに費用を掛けられない中、経営者に必要性を説明するにあたっても、経営リスクの観点から説明する必要があった。個人情報保護

†1 情報セキュリティ大学院大学
Institute of Information Security
a 林 紘一郎「係長セキュリティから社長セキュリティへ：日本的経営と情報セキュリティ」情報セキュリティ総合科学 2 巻, 1 頁, 2010
b 経済産業省　「情報セキュリティガバナンス導入ガイダンス」2009、2 頁

法上の安全管理義務や、企業が営業秘密を守るための現実の秘密管理性の要請、競合の状況などからそれが狙われる可能性も評価しつつ説明し、法や経営上、リスクマネジメントの観点から、必要性を理解してもらい、予算を獲得して情報セキュリティを推進してきた。

このように、経営上のリスクマネジメントの観点からの判断は、情報システムの責任者の職責より、むしろ、内部統制や法務、リスクマネジメントなどを担当する部門の職責により近い。ISO/IEC27002 の 6.1.1「情報セキュリティの役割及び責任」のためにはすべての組織へのガバナンスが必要であり、7「人的資源のセキュリティ」のためには人事やすべての組織責任者を説得し、11「物理的及び環境セキュリティ」のために、総務を説得しなければならない。やがて、内部統制系の部門として情報セキュリティ専門部署も登場する。特に、日本の場合、個人情報保護法の安全管理義務もさることながら、1998 年から始まったプライバシーマークや、個人情報保護法の立法機運のきっかけとなった 1999 年の宇治市の個人情報漏えい事件など、個人情報保護から情報セキュリティが拡がったこともあり、情報システム主導の情報セキュリティというより、法務や内部統制が主管となりつつ委員会などで関係職能がリードするパターンが広がった。実際、情報システム部門は自らの傘下の IT 機器やネットワークの管理はできても、各部署が勝手に IT 機器を導入したり ASP サービスを導入したり Web サイトを立てることに対する社内行政は必ずしも得意ではないため、これらの内部統制系の部署が主管すること自体は効果的でもあった。

しかし、最近では、政府も「情報セキュリティ」ではなく、より重点を明確にした「サイバーセキュリティ」にフォーカスしており、「サイバーセキュリティ経営ガイドライン Ver 2.0」においても、IT の利活用とそれに伴うリスク、という観点にフォーカスしている。そこでは、経営者の役割を強調するとともに、「経営戦略の観点から守るべき情報を特定」することが、「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」の対策例として挙げられるcなど、その名残を残している。

一方、このように、情報システム主導ではない体制の場合、ややもすれば、情報システム部門との軋轢が生じる。運用の現実をかかえ、利用部門や経営者から IT のコストダウンを要請されている情報システム部門に対し、定期的なパッチマネジメントの実施や、内部者牽制のための書き出し制御ツールの導入を要請することは軋轢を生んだ。しかし、逆に言えば、別の組織だからこそ要求できる、という、一種の権限分離のような側面もある。

しかし、情報セキュリティのなかでも、IT セキュリティ、とりわけサイバーセキュリティの重要性がより高まり、様々な事故が報道され、経営者もその必要性を認識する昨今、この状況は変わりつつあるのかもしれない。CISO は CIO とはどのような関係であるべきか、CPO とはどのような関係であるべきか。CISO はどのような職能が担うべきであろうか。

2. 分析方法

情報セキュリティ大学院大学原田研究室では「情報セキュリティ調査」を 2012 年より実施している。2017 年情報セキュリティ調査においては 2017 年 8 月に、日本国内のプライバシーマーク取得企業、ISMS 認証取得企業、官公庁、教育機関などから、ランダムに選んだ 4,500 組織に対し、「情報セキュリティ調査」を実施。429 組織から回答を得たd。本稿では、回答の未記入及び択一問題における重複回答等の無効回答は「無回答」として処理している。

分析１　全体と業態・規模による比較

全体及び、種類・規模により、対象を下記に分類した分析。
① 中堅・大企業　（②以外の企業）
② 中小企業
- 卸売業であり資本金 1 億円以下または従業員 100 人以下
- 小売業であり、資本金 5 千万円以下または従業員 50 人以下
- 情報処理業以外のサービス業であり、資本金 5 千万円以下または従業員 100 人以下
- 上記以外（ソフトウェア業・情報処理サービス業を含む）で、資本金 3 億円以下または従業員 300 人以下

③ 自治体
④ 大学
⑤ その他

種類・規模が無回答の 3 件は割愛。N=426

分析２　主務による比較

Q24 の回答から、情報セキュリティの主務が、下記のものに分類して、関係質問を分析。
① 情報セキュリティ専任（主務）
② 情報システムと兼務で、情報システムが主務
③ 広義の内部統制（総務、法務、内部統制、RM、人事）と兼務で、広義の内部統制が主務

Q24 が、その他と無回答は割愛。　N=308

分析３　クロス分析による主務による情報セキュリティレベルの比較（業態別）

いずれを主務とする体制が、情報セキュリティが進むか？情報セキュリティの進化・充実を示すと思われるいくつかの質問の結果を、分析３の主務の分類で比較。N=308

c 経済産業省「サイバーセキュリティ経営ガイドライン Ver 2.0」10 頁
http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf

d アンケート内容等は、http://lab.iisec.ac.jp/~harada_lab/survey.html

これによる N 数をまとめると以下の通り。

表 1　分析対象と N 数

業態・規模		大企業・中堅	企業中小	自治体	大学	その他	無回答	合計
Q6		Q6-8	Q6-1,2,3,4	Q6-5,6,7,9	Q6-10	Q6-11		
全体		30	231	79	69	17	3	429

						左記合計
情報セキュリティ	Q24-1	2	39	12	9	62
情報システム	Q24-2	8	49	6	18	81
広義の内部統制（内部統制、リスクマネジメント、法務、人事、総務）	Q24-3,4,5,6,7	8	93	43	21	165
上記 3 主務合計		18	181	61	48	308
その他	Q8	9	44	13	14	80
無回答		3	6	5	7	21
合計		30	231	79	69	409

分析 1
分析 2
分析 3

3. 分析結果

3.1 分析 1　全体分析　業態・規模による分析

[Q22]. 情報セキュリティ責任者の職位

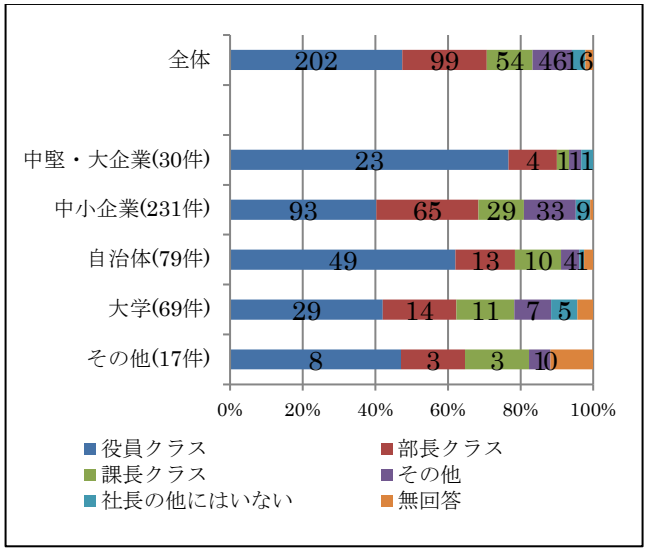

図 3　情報セキュリティ責任者の職位（業態・規模別）

全体でも、半数近くが役員クラス、部長職以上では 7 割あり、経営者セキュリティに近づいている。
業態・規模別では、中堅・大企業と自治体で、役員クラスが過半を占める。一方、「その他」の記述に「一般社員」の記載のある組織が、中小企業で 9 件、中堅・大企業と大学で各 1 件あった。

[Q23]. 情報セキュリティ責任者に最も期待する役割

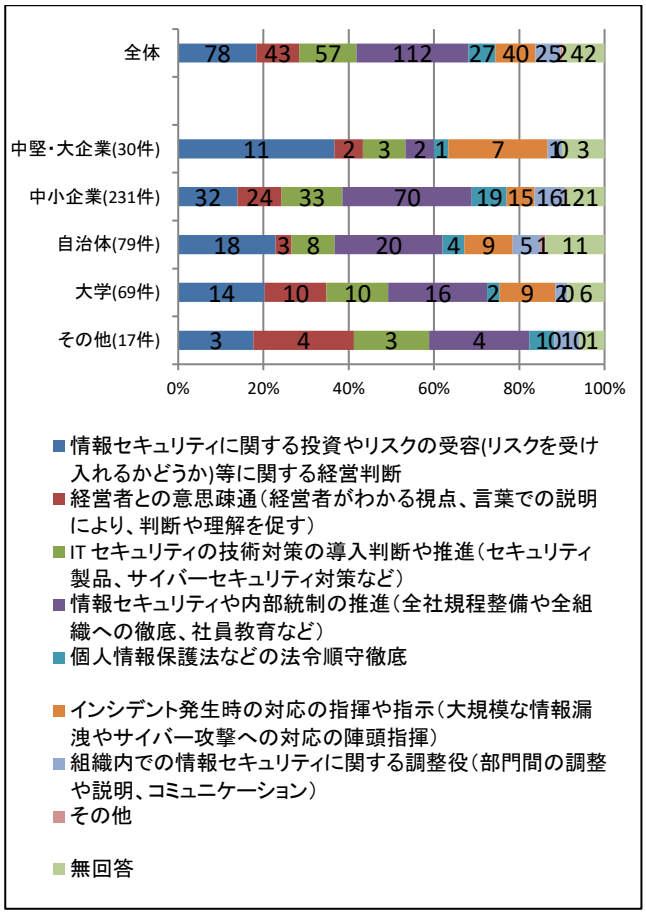

図 4 情報セキュリティ責任者に最も期待する役割（業態・規模別）

全体では情報セキュリティや全社規程整備や全組織への徹底、社員教育など内部統制の推進が最も多く、次いで投資やリスクの受容の経営判断となっており、冒頭にのべた、経営リスクとしての情報セキュリティの推進が期待されている。3 位が IT セキュリティの技術対策の導入判断や推進となっている。

業態・規模別にみると、中堅・大企業では経営判断やインシデント発生時の指揮が期待されるが、中小企業、自治体、大学では内部統制の推進が期待されており、内部への徹底の難しさを伺わせる。大企業の方が大きいため内部徹底が難しいと思われるが、それを期待するのが少数なのは、他にも内部統制を担う部門があって、情報セキュリティ責任者にはもっと経営的な判断を求めているものと推測される。

[Q24]. 情報セキュリティ責任者の主務

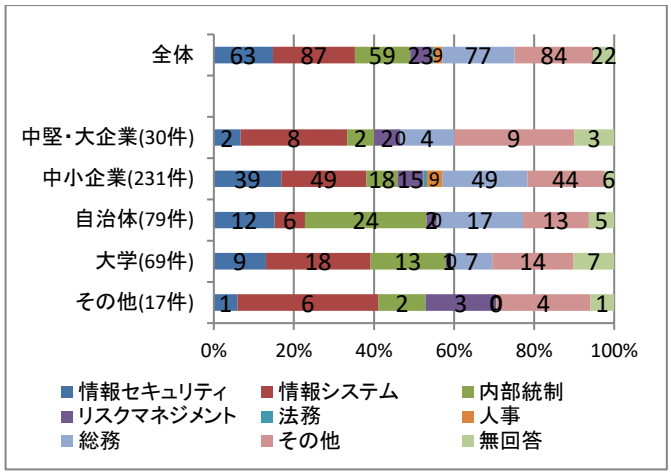

図 5 情報セキュリティ責任者の主務（業態・規模別）

全体では、情報セキュリティを主務とするのは、第 3 位で 15%。1 位は情報システム、2 位は総務。法務は 2 件で 0.5%に届かず、意外であった。その他の自由記述は 57 件あり、大別して下記の通りとなっている。

経営系　　20 件
営業系　　12 件
IT 系　　7 件
管理系　　6 件
教員・開発　6 件

情報セキュリティ主務が少数であることは残念だが、情報システム以外の職能が情報セキュリティ責任者となっている組織が約 6 割という見方もできる。
情報セキュリティという新たな職能に人員を割けないからか、と考えたが、業態・規模別にみると、意外なことに、情報セキュリティを主務とする割合が、中堅・大企業よりも中小企業の方が高い。中堅・大企業で情報セキュリティ責任者が情報セキュリティを主務とするものが 2 社しかなかったのは意外であり残念だった。
自治体では情報セキュリティ主務と内部統制が多い。総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン」等で CISO の設置が要請されているからと思われるが、副首長クラスとされており、必ずしも情報セキュリティを主務としなければならない訳ではない。「それを補佐する情報セキュリティに関する外部の専門家を最高情報セキュリティアドバイザーとして置くことが望ましい」とされているところから、専任組織もあるのかもしれない。逆に情報システムが主務の自治体の割合は低い。
大学は情報システムが多いが、内部統制よりも NW やシステム的対応でなければ学生を規律できないからと推測される。

[Q25]. 情報セキュリティ上の要請と、情報システム上の要請が対立するときの対応
Q25-1 優先順位の判断をする主な部門
Q25-2 リスクを判断する部門が IT セキュリティを実行する部門を説得するために必要と考えること（複数選択可）

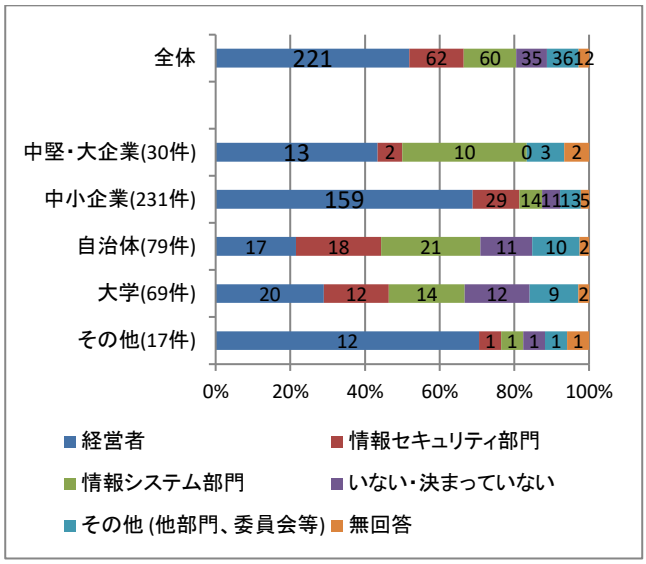

図 6　優先順位の判断をする主な部門　（業態・規模別）

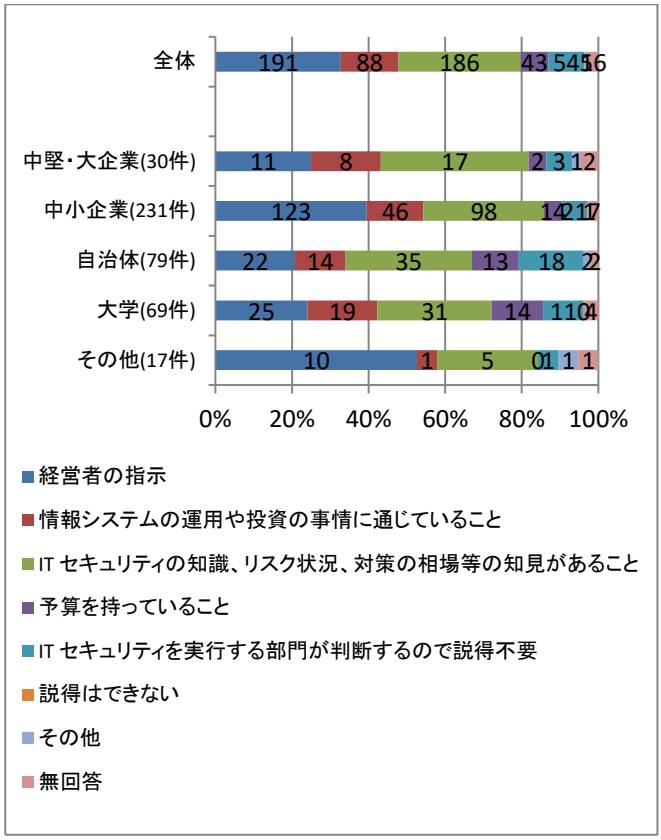

図 7　IT セキュリティを実行する部門を説得するために必要と考えること（業態・規模別）

運用上の困難、IT コストの上昇、効率性の低下など、情報セキュリティ上の要請と、情報システム上の要請が対立するときの判断は経営者が行うという組織が過半数。次いで情報セキュリティを担当する部門となっており、ポリシーが IT の事情を上回るというガバナンスが機能していそうな組織が 67%。しかし、情報システム部門が判断するという組織も 14%あり。業態・規模別では、情報システム部門が判断する割合が最も高いのは中堅・大企業である。情報セキュリティ主務が少ないこととも平仄が合う。中小企業に比べて情報システムが情報セキュリティも含めた見識を持っているからかもしれないが、二律背反の要請に、経営視点で自らを

追い込む判断ができるか、心配な面がある。
IT セキュリティを実行する部門を説得するために必要なことの 1 位は経営者の指示となっているが、経営者が判断するとしても、誰か専門性のある者がそのリスクや影響と IT の事情を合わせて説明する必要があると思われる。次いで、IT セキュリティの知識・知見があることとなっており、統制部門が情報セキュリティ責任を負っているのであれば、IT セキュリティの専門家を擁する必要がありそうである。意外なことに予算を持っていることは高くない。

[Q26]. 情報セキュリティ部門と情報システム部門の関係
情報セキュリティ部門と情報システム部門の関係はどうあるべきかを尋ねた。
Q26-1 情報セキュリティ部門と情報システム部門とは独立してあるべきか
Q26-2 1 の回答の理由 （複数選択可）

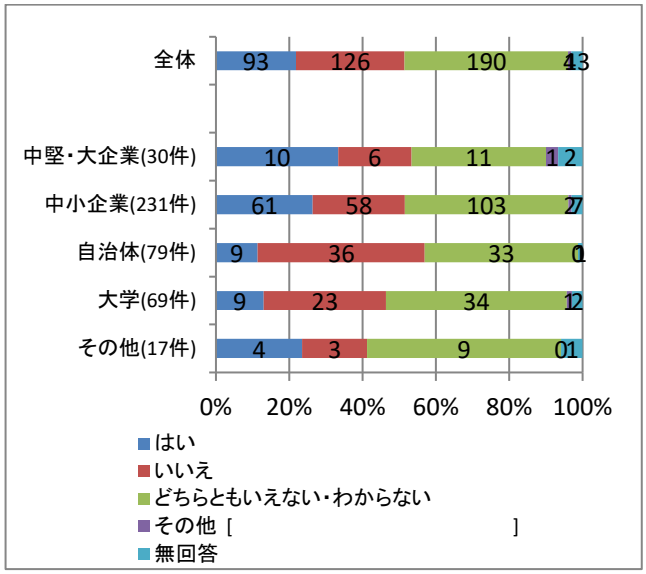

図 8 情報セキュリティ部門と情報システム部門とは独立してあるべきか（業態・規模別）

「分からない」が約半分に上り、次いで「いいえ（情報システムと同一部門であるべき）」となった。
業態・規模別では、情報システム部門が情報セキュリティ責任を担っている中堅・大企業で比較的独立すべし、との意見が多いのは興味深く、逆に、情報セキュリティ・内部統制が担っている自治体で情報システムと同一部門であるべき、との意見が多いのも興味深い。
それぞれ、現状を是としていなさそうである。

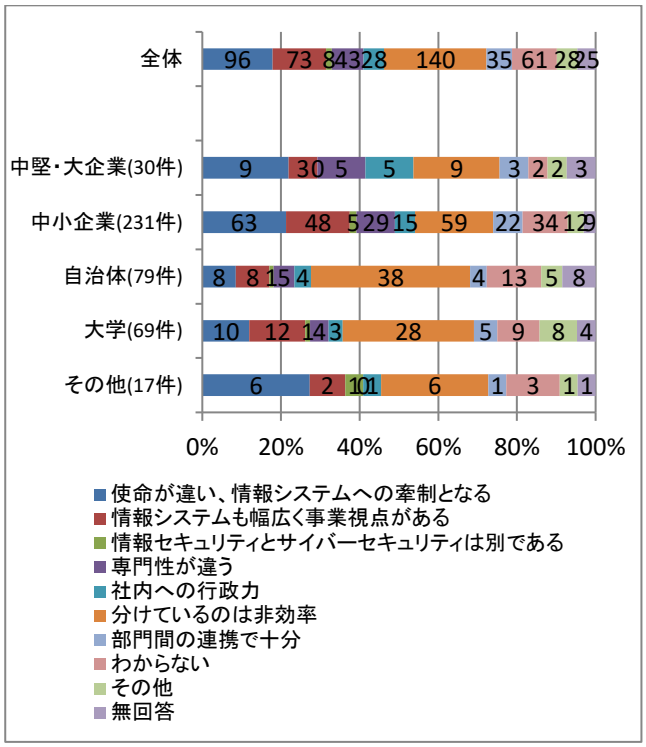

図 9 1 の回答の理由 （業態・規模別）

Q25-1 の回答の理由は、「分けているのは非効率」が最も多く、次いで、「使命が違い情報システムへの牽制となる」が多かった。
Q26-2 の回答を Q26-1 の回答別に分類した結果を図 10 に示す。

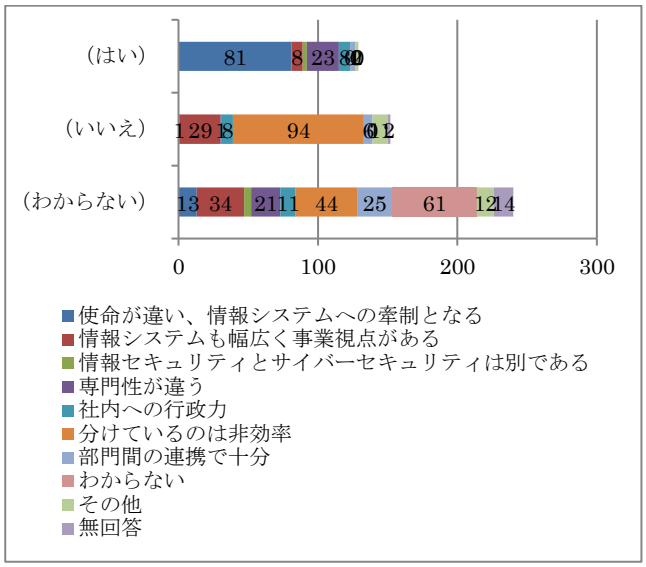

図 10 情報セキュリティ部門と情報システム部門とは独立してあるべきか、とその理由

「独立してあるべき」、との立場では、「使命が違い、情報システムへの牽制となる」、という理由が過半を占め、次いで「専門性が違う」との意見が多かった。
「独立すべきではない」、との立場では、「分けているのは非効率」、が過半を占め、次いで、「情報システムも事業視点がある」ため、経営視点での判断も可能、という意見が多かった。
最も多数派の、「独立すべきかどうかはわからない」、との

意見では、理由も「わからない」が最多、次いで「分けているのは非効率」「情報システムも事業視点がある」が続き、どちらかというと、分けない意見と思われる。

業態・規模別にみて、図 8 図 9 を突き合わせると、当然ながら、業態による差というより、Q26-1 の意見による差と思われる。

3.2 分析２　情報セキュリティ責任者の主務による分析

Q25（情報セキュリティ上の要請と情報システム上の要請が対立するときの対応）と Q26（情報セキュリティ部門と情報システム部門の関係）について、情報セキュリティ責任者の主務により分析する。
主務については、Q24 の回答から下記の 3 分類とする。

①　情報セキュリティの専任または情報セキュリティを主務にしている組織
②　情報システムと兼務し情報システムを主務にしている組織
③　広義の内部統制（総務・法務・内部統制・RM・人事などの広義の内部統制を担当する部門が兼務し主務とする組織）

なお、中堅・大企業で、情報セキュリティを主務にする組織は 2 件しかなく、主務別の業種・規模別分析は特筆すべきものがない限り行わない。

[Q25].　情報セキュリティ上の要請と、情報システム上の要請が対立するときの対応

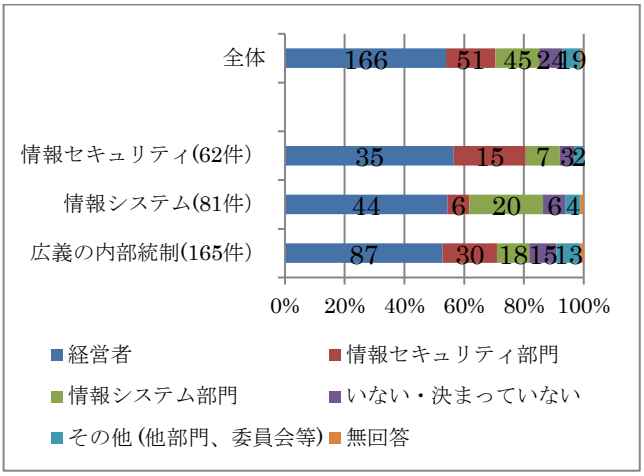

図 11 優先順位の判断をする主な部門　（主務別）

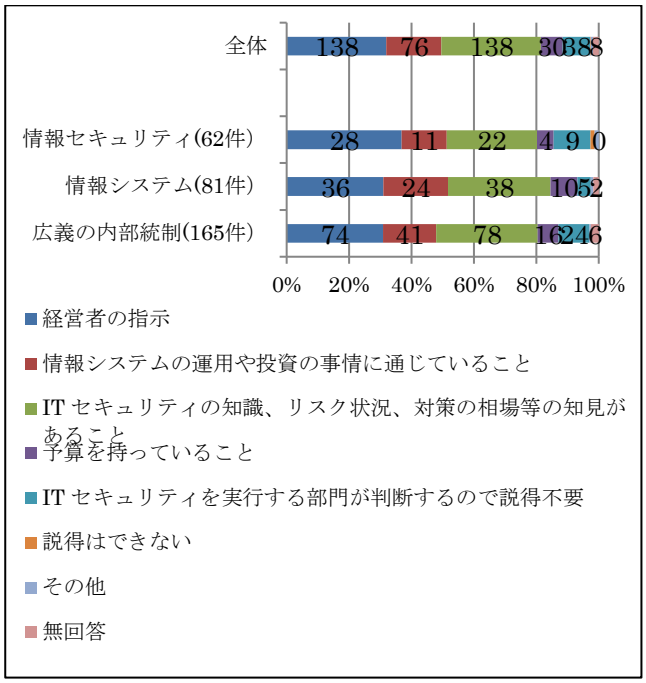

図 12 Q25-2 リスクを判断する部門が IT セキュリティを実行する部門を説得するために必要と考えること（主務別）

責任者の主務にかかわらず、経営者の指示が多く、次いで、ほぼ同数が「IT セキュリティの知識、リスク状況、対策の相場等の知見があること」と回答。経営者が判断するにせよ、専門家の見解が必要であることを考えると、この点が鍵と思われる。情報システム側の事情に通じていることは情報システム以外が主務では多くはなく、牽制という意味では忖度して遠慮することなく、要請することが期待できる。
情報システムが主務の場合、自らが決めることになるが、情報セキュリティや広義の内部統制が主務であっても情報システムが判断する組織も一定数あり、権限が弱いか、IT セキュリティの見識に自信がないと推測される。
特に自治体ではいずれが主務でも情報システムが判断する比率が大きい。

[Q26].　情報セキュリティ部門と情報システム部門の関係

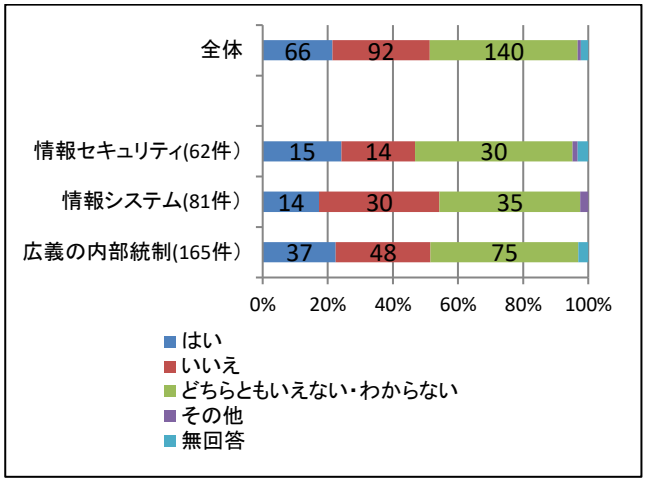

図 13　情報セキュリティ部門と情報システム部門とは独立してあるべきか　（主務別）

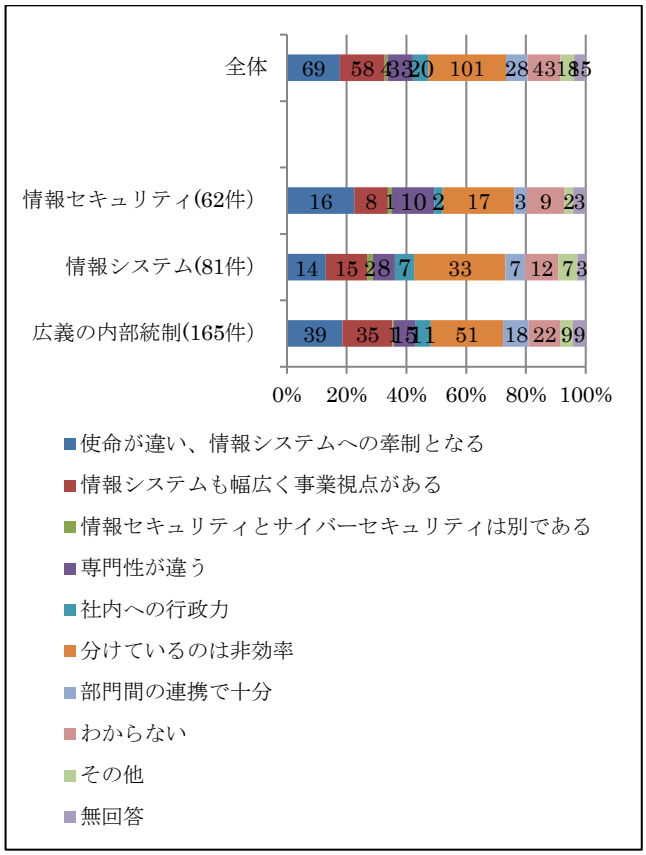

図 14　Q26-1 の回答の理由　（複数選択可）（主務別）

情報セキュリティが主務の組織でも「いいえ」が約 2 割、情報システムが主務の組織でも「はい」が約 2 割と、いずれの分類でも、現状と異なる選択が 1/4 弱あり、それに対応すると思われる理由も同様に選択されている。特に、広義の内部統制が担当する組織では、分けているのは非効率との回答の割合が比較的高い。情報システム部門が担当する組織で現状肯定的意見が多い。

3.3 分析３　情報セキュリティ責任者の主務による情報セキュリティの取組の進化の分析

では、情報セキュリティ責任者の主務によって、情報セキュリティへの取組に差が出るだろうか。情報システムに対するけん制が独立させる目的とすると、情報システムが主務でない方がより高い情報セキュリティ対策ができている又はより成熟した経営リスク的視点からの情報セキュリティができていることになるが、果たしてそうだろうか。

情報セキュリティの進化・充実を示すと思われる下記（１）～（４）の項目を、分析の前提となる（０）も考慮しつつ、分析。

（０）情報セキュリティ責任者に最も期待する役割
[Q23]. 情報セキュリティ責任者に最も期待する役割をお答えください。（〇印はひとつだけ）

（１）マネジメントシステム、組織としての取組
[Q7]. 貴社ではプライバシーマーク（P マーク）、ISMS、BCMS を認証取得していますか。（複数選択可）

（２）リスク分析（と状況に応じた対応）
[Q9]. 情報セキュリティに関するリスク分析・評価を最後に実施したのはいつですか。　（〇印はひとつだけ）　※リスク分析評・価とは、保護すべき情報資産を明らかにし、それらに対するリスクを分析・評価すること。

（３）情報セキュリティ投資　（IT セキュリティ）
[Q17]. 情報セキュリティに関する支出※についてお伺いします。売上（政府・自治体・大学の場合は予算）に対する割合
※支出：セキュリティ関連システム開発、運用、ライセンス等外部への支出総計

（４）現場教育
[Q40]. 各状況を想定した教育・研修を実施したことはありますか？　（各項目の 1～4 で〇印はひとつだけ）
Q40-1　自社 Web サイトの改ざん
Q40-2　ランサムウェアへの感染
Q40-3　ソーシャルエンジニアリング

（０）情報セキュリティ責任者に最も期待する役割
[Q23]. 情報セキュリティ責任者に最も期待する役割をお答えください。（〇印はひとつだけ）

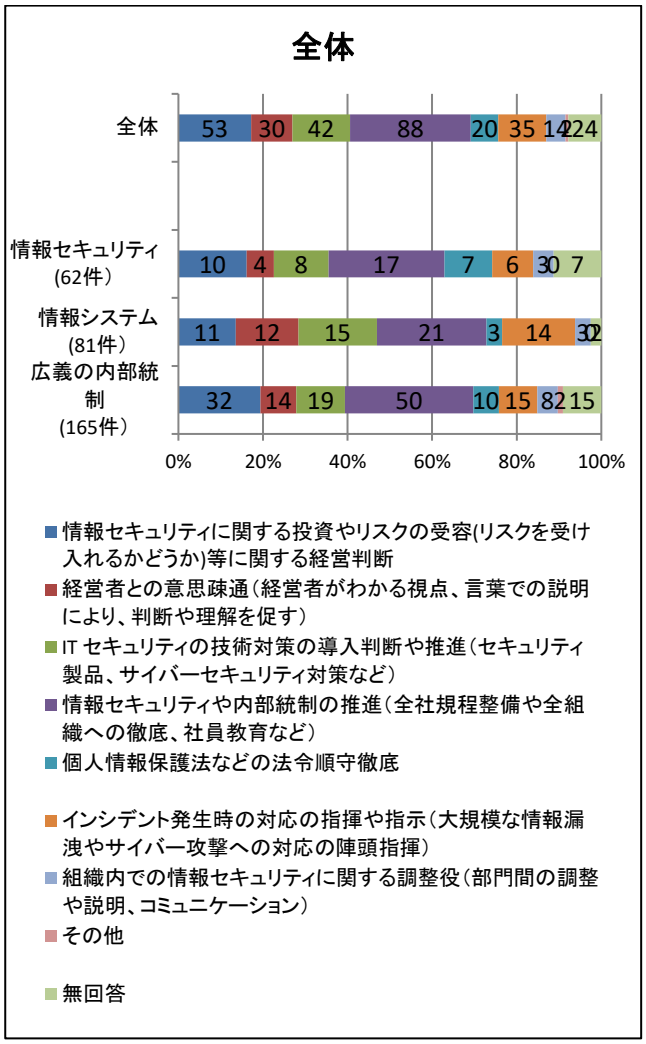

図 15　情報セキュリティ責任者への期待　主務別（全業態）

いずれを主務にする場合も、全社規定整備や全組織への教区などの情報セキュリティ内部統制を期待する比率が最も高い。情報システムを主務とする組織では、インシデント発生時の対応や指揮、IT セキュリティの導入判断や推進も比較的多い。

（1）マネジメントシステム、組織としての取組

[Q7]. 貴社ではプライバシーマーク（P マーク）、ISMS、BCMS を認証取得していますか。（複数選択可）

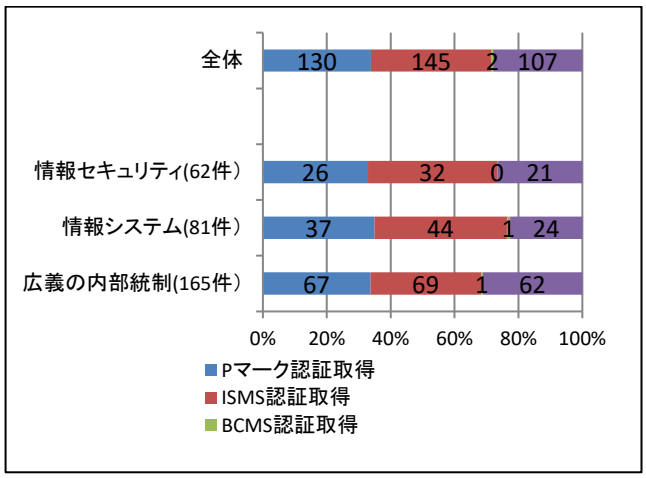

図 16 マネジメントシステムの認証取得 （複数選択可）主務別 （全業態）

マネジメントシステムについては、いずれを主務とする場合でも違いは見られない。
むしろ、民間企業ではいずれかを認証しているが、自治体、大学ではほとんど認証取得していない、と、業態により大きな差がある。

（2）リスク分析（と状況に応じた対応）

[Q9]. 情報セキュリティに関するリスク分析・評価を最後に実施した時期。

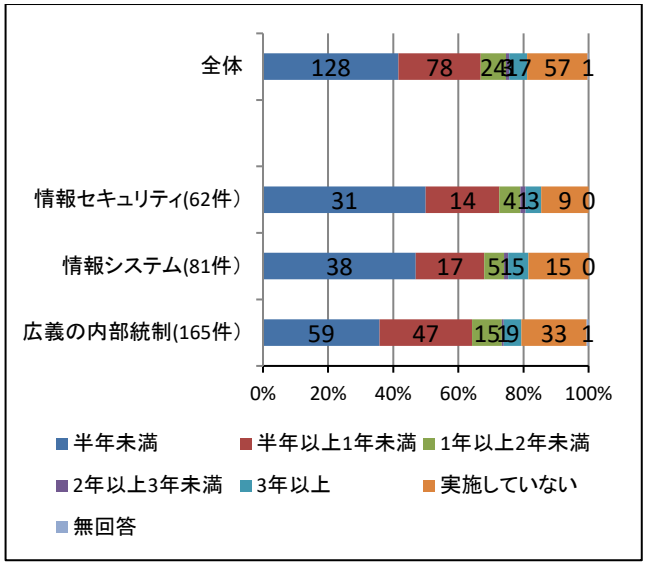

図 17 情報セキュリティに関するリスク分析・評価を最後に実施した時期 主務別 （全業態）

リスク分析の実施は、分析の結果、必要と判断された対策の導入も進んでいる、と推定すると、情報セキュリティレベルも高い、と考えられる。

主務で顕著な差はないが、1 年以内にリスク分析を行った組織の比率は主務が情報セキュリティ、情報システム、広義の内部統制の順。リスク分析を実施していない組織の割合もその逆で、広義の内部統制では情報セキュリティへの取り組みが比較的弱い。
自治体、大学では、情報システムが担当する組織でも、リスク分析を実施していない組織の比率が高い。

（3）情報セキュリティ投資 （IT セキュリティ）

[Q17]. 情報セキュリティに関する支出の売上（政府・自治体・大学の場合は予算）に対する割合

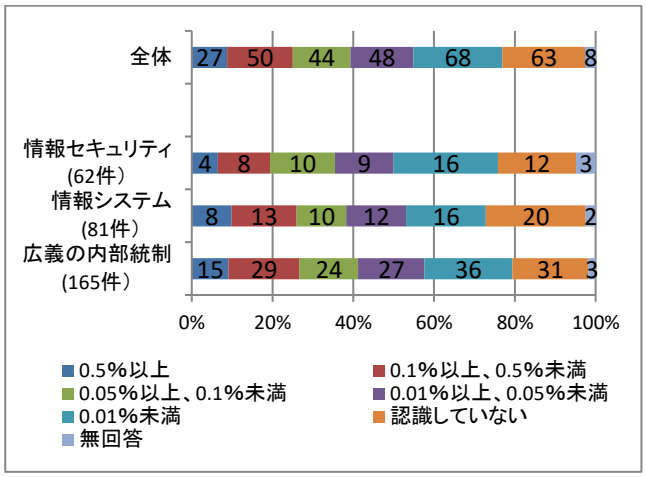

図 18 情報セキュリティに関する支出の売上（政府・自治体・大学の場合は予算）に対する割合 主務別 （全業態）

支出を、「セキュリティ関連システム開発、運用、ライセンス等外部への支出総計」と、IT セキュリティへの投資と定義しているため、投資が多いほど、IT セキュリティのレベルが高い、と推定した。

主務による顕著な差はないが、広義の内部統制、情報システムが主務の方が、情報セキュリティが主務の組織より情報セキュリティ支出の売上比が高い。
情報セキュリティ部門の力がないのか、情報セキュリティが主務の場合、ツール先行型になりにくいのか、理由は不明。
情報システムが主務の場合、情報セキュリティ投資額を認識していない割合が高い。

（4）現場教育

[Q40]. 各状況を想定した教育・研修を実施したことはありますか？ （各項目の 1～4 で○印はひとつだけ）

Q40-1 自社 Web サイトの改ざん
Q40-2 ランサムウェアへの感染
Q40-3 ソーシャルエンジニアリング

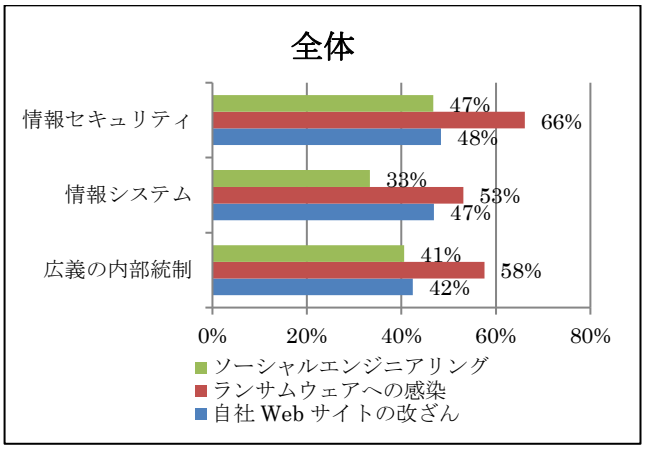

図 19　各状況を想定した教育・研修の実施割合
主務別　（全業態）
(実施したことがある、類似事例なら実施したことがあるの合計)

いずれが主務の組織も、比較的高い実績だが、自社 Web サイトの改ざん以外では、情報セキュリティや広義の内部統制が担当する場合の実施比率が高い。自社 Web サイトの改ざんは、訓練しなくても情報システム部門に通報することが多いと考えられる。

4. 考察

4.1 調査の分析からわかること

分析からわかったことは以下の通り。

- 情報セキュリティ責任者は、約半分の組織では役員クラスが、7 割以上は、部長以上が担当しており、「経営者セキュリティ」は浸透しつつある。
- 情報セキュリティ責任者が情報セキュリティを専任・主務とする組織は 15%ほどで、多くはない。情報システムが兼務する割合は 20%で最大。特に、民間企業、とりわけ中堅大企業においては、情報セキュリティ専任は少なく、情報システムの兼務が多い。
- しかし、内部統制・リスクマネジメント・総務・人事・法務などの広義の内部統制を担う部門やその他を合わせると、情報システム以外の職能が情報セキュリティ責任者となる組織は 7 割以上で、それなりに情報システムへの牽制は期待できる。
- 情報セキュリティ責任者に期待することは、全社規定整備や全組織への教区などの情報セキュリティ内部統制が最も高く、次いで情報セキュリティに関する投資やリスクの受容等に関する経営判断となっている。情報システム部門が情報セキュリティを担当する組織では IT セキュリティの導入判断や経営者との意思疎通も期待されている。
- 情報システムと情報セキュリティの要請が対立するときの判断は経営者に委ねられている。情報セキュリティ責任者が情報セキュリティ主務の場合は、他に比べて情報セキュリティ部門が判断する比率は高いが、それでも 1/4 程度。情報セキュリティ責任者が情報システムを主務とする場合は、経営者に次いで、情報システム部門が判断する割合が高く牽制にはならない。経営者の判断には専門部署のインプットが必要と思われるが、もしそれが不十分な場合は、専門部署として逃げている、との見方もできる。
- 情報システム部門を説得するために必要なことは、経営者の指示の他、IT セキュリティの知識、リスク状況、対策の相場等の知見があることが多数。
- 情報セキュリティは情報システムとは独立してあるべきかについては、「わからない」が 44%、「いいえ」が 30%、「はい」が 22%。理由については、「いいえ」では「分けているのは非効率」が多く、「はい」では「使命が違い、情報システムへの牽制となる」が多い。情報システムへの牽制という視点を持っている組織が一定数あることは評価できる。
- 現状、情報セキュリティ専任とする組織でも「いいえ」が 2 割強、情報システムが兼務する組織でも「はい」が 2 割弱、と一定数、見直しが必要と考えている組織がある。
- 情報セキュリティ責任者の主務により、情報セキュリティのレベルに顕著な大きな差はないが一定の傾向はある。リスク分析の実施については情報セキュリティ主務の方が進み、IT セキュリティへの投資は広義の内部統制が主務の場合が進み情報セキュリティが主務の組織では比較的低めである。現場への教育・訓練については、情報セキュリティが主務の組織で最も高い。
- 以上から、最も期待されて入いる情報セキュリティ内部統制の役割は、リスク分析も含め、情報セキュリティや広義の内部統制を主務とする場合の方が進んでいるが、IT セキュリティについては、かならずしも牽制がある方が進むかどうかはわからない、ということが言えよう。
- いずれにせよ、鍵を握るのは経営者であり、経営者にどのように情報セキュリティの現状やリスクを理解してもらうか、が重要と思われる。

4.2 IPA 調査との比較

独立行政法人情報処理推進機構（以下 IPA という）では、2016 年から「企業の CISO や CSIRT に関する実態調査」を実施している。「企業の CISO や CSIRT に関する実態調査 2017e」(以下 IPA 調査という)では、本調査と関係のある項目がいくつかあるので、突き合わせて考察する。

（1）情報セキュリティ専任の CISO の割合

IPA 調査によれば、「専任の CISO 等を設置している」との回答割合は、日本は 27.9%、米国では 78.7%、欧州では 67.1%となっているf。また、日本における情報セキュリティの専門部署（担当者）がある」の回答は、日本 45.2%で、CISO が兼任でも専任の部署がある組織が 36.6%に上っている。しかし、セキュリティ人材は「やや不足している」が 44.9%を占めているg。一方、本調査では、Q24 について、図 5 のように、CISO が情報セキュリティ専任である組織は 15%であり、IPA 調査より少ない結果になっている。本調査では過半数が売上高 50 億円未満であり、一方、IPA 調査では、この規模の組織は 14%に過ぎない、という差はあるが、本調査では図 5 のとおり、中堅・大企業の方が中小企業よりも情報セキュリティ専任が少なく、規模の差が原因とも考えにくい。

（2）CISO と経営者の距離

本調査 Q25 で、情報セキュリティ上の要請と情報システム上の要請が対立するときの判断は、過半の組織で経営者が判断という結果であった。IPA 調査では、セキュリティ投資

e 独立行政法人情報処理推進機構「企業の CISO や CSIRT に関する実態調査 2017」（2017 年 4 月 13 日）https://www.ipa.go.jp/security/fy29/reports/ciso-csirt/index.html#L1

f IPA　前掲注 e、22 頁
g IPA　前掲注 e　43 頁

に対する経営層と情報セキュリティ担当部門又は情報システム担当部門の認識の差について調査し、「一致している」は日本が 59.3%で最も高かった。また「一致してない」が米国で 45%、欧州で 37%あるが日本では 22%ほどとなっているh。日本では投資額については比較的経営者が関与しているのではないか。

（３）CISO に期待される役割

本調査 Q23 では、図 4 のとおり、最も期待する役割は「情報セキュリティの内部統制」28.6%、「投資やリスク受容の経営判断」17.2%、「IT セキュリティの技術対策の導入判断や推進」13.6%の順であった。IPA 調査では、「CISO の現在重要視されている役割」について、日本については「(技術)セキュリティ技術分析・評価」52.0%、「(ガバナンス) セキュリティ目標・計画・予算の策定・評価」40.8%、「(リスク管理) リスク分析・評価」35.5%の順になっておりi、IT 系の役割が上位となってはいるものの、上位 3 つについては、類似している。米国についても「(技術)セキュリティ技術分析・評価」59.2%が断トツに高いが、「(リスク管理) リスク分析・評価」34.9%、「(ガバナンス) セキュリティ目標・計画・予算の策定・評価」32.3%と上位３つは日本と変わらない。IPA 調査の方が、本調査よりも、IT 技術への期待が大きいj。

（４）情報セキュリティの取組

IPA 調査では、CISO の専任が多い米国では、ほとんどの回答者が情報セキュリティ投資の評価を実施しているが日本では 26.9%が評価を実施していないk。また、日本でも CISO 設置会社の方が評価を実施している。本調査では、前述のとおり、情報セキュリティ主務の組織で IT セキュリティ投資が比較的少なかったが、評価の結果、ツール先行の投資が少ない、ということも言えるのではないか。

また、IPA 調査では、リスク分析も CISO が専任の回答者の方が実施しており、本調査の結果とも符合している。

IPA 調査では、発見しにくい攻撃の発見力にも日米の差がわかる。サイバー攻撃と内部不正についてl、「発生していない（監視していないが、被害の報告は受けていない）」「わからない」の合計を「管理できていない」とするとその割合は、日本は 26.2%、米国は 18.4%であった。また、SOC の導入（日本 8.2%、米国 26.2%）、SIEM の導入（日本 22.9%、米国 24.9%）、外部専門家によるセキュリティ監視サービスの活用（日本 18.8%、米国 33.2%）などのこれらの発見力につながるシステム・サービスも米国の方が高い。CISO の専任による差のデータは開示されていないが、相関関係はあると推測される。

4.3 CISO の兼務と今後の課題

以上のように、IPA 調査の日米比較を見ると、日本の場合は兼務が多く経営者の見方に近くトータルな判断を重視している。一方、米国の場合は、専任の CISO で経営者との違いも認識しつつ、恐らく CIO への牽制も視野に専任が多いものと思われる。

終身雇用ではなく、専門性を武器に転職するのが当然の米国企業では、新たに出てきた重要な分野については、スキルのある専門家を外から雇用して社内を統制し牽制することは当然の動きである。また、性悪説に基づいた権限分離の考え方も実行されている。一方、日本では、本調査での回答のように、「情報セキュリティと情報システムを分けているのは非効率」という見方も多いが、これは、終身雇用で雇用契約の解除が難しい中で、新たに出てきた重要な分野は社内の人材を教育して再配置する、という動きになるからであろう。従って類似スキルをもった人材を別々の組織で擁することは非効率に映る。J-SOX 導入時に、開発・保守と運用の権限分離について、米国のような権限分離を求めず、第三者の立会があれば、開発・保守の人間が本番データの入ったシステムにアクセスできる、としたことmと、同根であろう。

日本でも、CISO と CIO の関係は取り上げられることもあるn。IPA 調査では、CISO が専任であるか兼任であるかは本質ではなく、経営的な立場へのセキュリティの取組が十分に機能するかどうかが重要、と結論づけるoが、日本ではやむを得ないのかもしれない。しかし、情報システム部門が CISO を兼務するのなら、リスクの見える化と自らの事情とは峻別した経営視点での経営者への説明、経営者による評価が重要であろう。最終的にインシデントによって顧客や社会に謝罪するのは経営者なのだから。

謝辞

本調査を実施するにあたり、アンケートの回答にご協力を頂きました企業や団体、組織の皆様に感謝いたします。
また、アンケートの封入、データ入力に多大なご協力を頂いた各位に感謝いたします。更に、ご指導いただいた本学原田研究室の客員研究員、在学生各位、並びに本学事務局の皆様に感謝いたします。

h IPA　前掲注 e　25 頁
i IPA　前掲注 e　35 頁
j 本調査の Q23 は 1 つ選択で全回答中の比率、IPA 調査では 3 つ選択で全回答者中の比率であり、%での単純な比較はできない。
k IPA　前掲注 e　38 頁
l IPA　前掲注 e　57,58 頁
mシステム管理基準　追補版（財務報告に係る IT 統制ガイダンス）
http://www.meti.go.jp/policy/netsecurity/downloadfiles/guidance.pdf
3-(1)-③-イ、他。
なお、ISO/IEC27002：2013 は、「6.1.2 職務の分離」において、最後に「小さな組織では、職務の分離を実現するのは難しい場合がある。しかし、この原則は可能な限り適用することが難しい。分離が困難である場合には、他の管理策（例えば、活動の監視、監査証跡、管理層による監督）を考慮することが望ましい」とする。
n 「CISO と CIO、どっちが偉い？」ITPRO2016 年 11 月 28 日
http://itpro.nikkeibp.co.jp/atcl/watcher/16/110700001/112600010/?rt=nocnt
o IPA　前掲注 e　64 頁