Vol.2021-EIP-92 No.6
2021/6/7

事業リスクとしてのセキュリティリスク分析に関する要因の検討*

半貫貴久[1]　小川隆一[1]　竹村敏彦[2]

概要：企業がITを積極的に活用する「攻めの経営」と，情報セキュリティレベルを高めることによって情報資産を守る「守りの経営」を高いレベルで両立させるためには，経営層の示す経営方針に基づくセキュリティ対策の実践が重要である．2020年3月に独立行政法人情報処理推進機構が発表した「企業のCISO等やセキュリティ対策推進に関する実態調査」の調査報告書では，セキュリティに関する事業リスク評価の重要性が指摘されているものの，CISO等を任命している企業でさえもリスク評価を行っている割合は約50%に留まるという結果が示されている．なお，この報告書ではCISO等が任命されていない企業のリスク評価については明らかにされていない．この状況を鑑みて，この調査データを用いた多重コレスポンデンス分析を行った結果，とりわけ，事業リスクとしてのセキュリティリスク分析と評価を実施している企業は経営層の積極的な情報セキュリティへの関与が強いことなどを明らかにした．

キーワード：セキュリティリスク分析，セキュリティリスク評価，最高情報セキュリティ責任者（CISO），組織体制，多重コレスポンデンス分析

To Investigate Relations among Organizational Factors and Implementing Analysis of Security Risk as Business Risk

TAKAHISA HANNUKI[†1]　RYUICHI OGAWA[†1]　TOSHIHIKO TAKEMURA[†2]

Abstract: For balancing proactive management using IT and management protecting information assets, it is important to implement information security measures based on company's management policies. Generally speaking, it is important to implement security risk analysis and security risk assessment. IPA (Information-technology Promotion Agency, Japan) reported a real situation on implementation of organizational security measures in Japan, March 2020. According to this report, the ratio of firms implementing assessment of the security risk would be around 50% even if CISO is appointed in the firm. However, in the report it is not clarified whether firms without CISOs implement the risk assessment. In this article, by running multiple correspondence analysis with micro data collected from the above survey, we investigate relations among organizational factors and implementing analysis/assessment of security risk. As a result, for instance, it is found that in the firms where the management proactively participate in information security measures, it is implementing security risk analysis/assessment as part of business.

Keywords: Security Risk Analysis，Security Risk Assessment，Chief Information Security Officer (CISO)，Organizational Structure，Multiple correspondence analysis

1. はじめに

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て，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[1]．また，経営層による主体的取組みの推進には，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た上で，企業内の総合調整や実務者層をリードできる人材の必要性も併せて指摘されている．加えて，「サイバーセキュリティ経営ガイドライン Ver.2.0」[2]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（CISO; Chief Information Security Officer）等[a]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も重要とされている．しかしながら，これらのことが指摘されているにも関わらず，国内では，CISO等の役割は技術そのものに関するものであり，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ことが指摘されている[b]．

独立行政法人情報処理推進機構（IPA）が2017年に公開した報告書[4]では，CISOに期待されている役割やスキルはセキュリティ偏重であること，セキュリティ部門と経営層を

* 本研究の意見は，著者たち個人に帰属し，所属機関の公式見解を示すものではないことをことわっておく．

1 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan
2 城西大学
Josai University

a 本研究において，CISO または同等の責任者を「CISO 等」と称することとする．

b 海外においては，CISO 等を任命している企業の割合は北米やシンガポールの企業はともに 8 割を超えており，セキュリティ対策の実施状況においても北米やシンガポールの企業はともに 8 割の企業が定期的に実施していることが報告されている[3].

つなぐ橋渡しとしての役割は，まだ企業では認知されていないこと等を明らかにしている．また，2018年公開された報告書[1]では，改めて経営・事業に関する役割を十分果たしているCISO 等は少ないこと等が指摘され，調査からCISO等の経営・事業的役割を実現させるための手引きや事例が求められていることを確認している．さらに，2020年に公開された報告書[5]では，2019年に実施した調査結果を踏まえて，CISO等を任命している企業では，セキュリティ上のリスクを経営・事業上のリスク分析の対象として分析・評価を実施している傾向が強いことなどを明らかにするとともに，経営層のセキュリティ認識やCISO等に求められる役割等について整理している．2020年6月には「サイバーセキュリティ経営ガイドライン Ver 2.0実践のためのプラクティス集 第2版」[6]が公開されて，経営ガイドラインをCISO 等が実践するための手引きや事例となるプラクティス集等の作成も進んでいる．しかしながら，依然として，企業はサイバーセキュリティ対策のための体制整備を含むリソース（人材・予算）の確保，経営層の意識改善，CISO等の経営・事業的役割等，さらにITサプライチェーンに対する具体的なセキュリティ対策についての検討等の課題が山積している状況にあるといえる．

文献[1,4]は国内企業を対象とした調査に基づくものであるが，文献[5]はCISO等を任命している企業を対象とした報告書であるため，CISO等を任命していない企業等についての状況を明らかにするに至っていない．しかしながら，この報告書の中で実施された「企業のCISO等やセキュリティ対策推進に関する実態調査」（2019年10月）にはCISO等を任命していない企業も対象に含まれている．そのため，改めて CISO等を任命していない企業も分析対象として含めることも可能である．

本研究では，文献[5]の分析を深掘りし，企業において必要とされる事業リスクとしてのセキュリティ分析やその評価の実施状況と企業規模や企業のセキュリティに関する組織体制などの関係について明らかにしていく．具体的には，専任の CISO 等を任命している企業と兼任の CISO 等を任命している企業とではセキュリティ分析やその評価の実施状況に違いがあるのか，経営層がセキュリティについて議論している企業とそうでない企業ではセキュリティ分析やその評価の実施状況に違いがあるのか等について見ていく．これに加えて，単一の視点だけでなく，複数の視点でもってセキュリティ分析やその評価の実施状況についての分析も試みる．例えば，企業規模とセキュリティに関する組織体制の 2 つの視点を考えた場合，企業規模が十分に大きかったとしても，組織体制が整備されていなければ，セキュリティ分析やその評価ができていないか等についての考察を行っていく．

2. 関連研究

企業において組織的な情報セキュリティ・サイバーセキュリティ対策を実施し，さらに PDCA サイクルとして回していくためには，文献[2]などでも指摘されているように，経営層のセキュリティへの関与ならびに CISO 等の存在やチームとして情報セキュリティ対策をサポートしていく組織体制が必要である．これらのことについて第 1 節でもいくつか紹介したように，既にいくつもの調査報告が行われている．また，これらについて経営組織論等の視点でもって分析を試みている研究も少なからず存在する[7,8,9].

文献[7]は CSIRT(Computer Security Incident Response Team）という組織体制が組織のレジリエンスを高めるために重要な存在であることを指摘している．他方で，CSIRT は業種を問わず様々な組織において構築されるため，必ずしも情報セキュリティに対応できる人員・人材がそろっているわけではないという理由から，レジリエントなパフォーマンスを持とうとすればするほど，レジリエントなパフォーマンスの発揮と維持が困難になっていく「レジリエンスの罠」という現象が発生することもあわせて指摘している．

文献[8]は，CISO をはじ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，あるべき体制についての考察を行っている．そして，情報システム部門が CISO を兼任するのなら，リスクの見える化と自らの事業とは峻別した経営視点での説明，経営者による評価が重要であることを指摘している．

文献[9]では，サイバー保険に着目した企業のサイバーリスクに対する体制整備や各種セキュリティ対策の実施がサイバー保険の加入に与える影響について分析を行っている．そして，サイバーリスクに対して，組織の事業戦略に沿ったリスク分析を実施し，適切にリスクをコントロールすることが重要であることを指摘している．

文献[8,9]は調査データに基づく定量的な分析を行っているが，この種の研究の多くは文献[7]のように，理論に基づく概念的な議論にとどまっていることが多い．本研究では，上述した 2019 年 10 月に IPA が実施した調査データを用いて，事業リスクとしてのセキュリティ分析やその評価の実施状況と企業規模や企業のセキュリティに関する組織体制などの関係について明らかにしていく．この試みは，情報セキュリティに関する各種ガイドラインやハンドブックで重要とされている点の検証にも当たると考えられる．その意味において，学術的にも実務的にも意義があると思われる．

3. アンケート調査

3.1 調査概要

本研究の分析では，IPA が国内企業の CISO の事業的役割等に関する動向や企業のセキュリティ対策の取り組み状況を把握することを目的として，2019 年 10 月に実施した「企業の CISO 等やセキュリティ対策推進に関する実態調査」（以下，

「CISO 調査」と称す）で収集した個票データを用いる．「CISO 調査」は，郵送調査形式ならびにウェブ調査形式を併用して実施され，調査対象者は従業員数が 301 人以上の国内企業のセキュリティや情報システム関連部門に属する従業員（1,097 人）である[c]．

3.2 質問項目と概況

ここでは，本研究の分析で用いる質問項目と回答結果の概況を紹介する．

(1) セキュリティリスク分析と評価の実施状況

「CISO 調査」では，情報漏えい，サイバー攻撃による社内システムの停止，サイバー攻撃による顧客サービスシステムの停止といったセキュリティリスクに対する分析ならびに経営層の事業リスク評価の実施について質問を行っている．この質問に対する選択肢として「リスクを分析し，結果を経営層の事業リスク評価に役立てている」「リスクを分析してはいるが，結果を経営層の事業リスク評価に役立てていない」「リスク分析を行っていない」「わからない」を提示し，これらのうち該当するものを 1 つだけを回答者に選択してもらっている．このうち，本研究で対象とする「情報漏えい」に関する結果は図 1 の通りである．図 1 を見てわかるように，セキュリティリスク分析を行っている企業の回答者は全体の約 7 割程度であるものの，事業リスク評価に役立てている企業の回答者となるとその割合は全体の 3 割程度に留まっていることがわかる[d]．

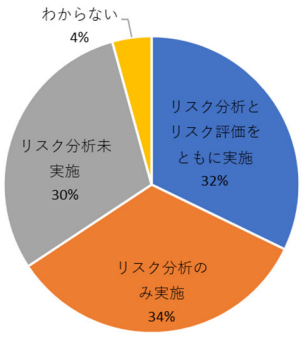

図 1： セキュリティリスク分析と評価の実施状況

(2) 情報セキュリティに関する組織体制

情報セキュリティに関する組織体制として様々なものが考えられるが，本研究では「CISO 調査」で質問している CISO 等の任命状況ならびに組織的な情報セキュリティ対策状況，経営層のセキュリティへの関与状況を取り上げることにする．

「CISO 調査」では，組織全体の情報セキュリティ対策を統括する CISO または同等の責任者（以下，「CISO 等」と称す）を任命しているかどうかについて質問を行っている．この回答の分布は図 2 の通りである．

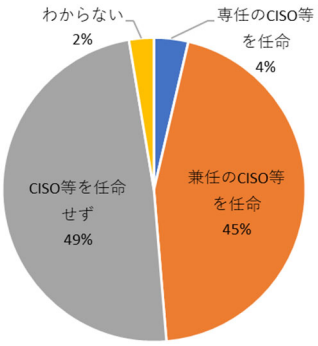

図 2：CISO 等の任命状況

組織全体の情報セキュリティ対策を統括する CISO 等を任命している企業の回答者の割合とそうでない回答者の割合はほぼ同程度となっている．また，CISO 等の任命に関して，専任と兼任別で見てみると，ほとんどの企業で兼任として CISO 等を任命していることが図 2 からわかる．

次に，図 3 は組織全体の情報セキュリティ対策を統括する CISO 等をサポートする組織的体制があるかどうかについての結果をまとめたものである．図 3 を見てわかるように，回答者の約 58%が組織内に CISO 等をサポートする体制があると回答している．一方で，サポート体制がない回答者の割合が 27%，また「わからない」と回答した割合が 15%となり，組織としての情報セキュリティ対策が十分に行われているとは必ずしも言えないことがわかる．

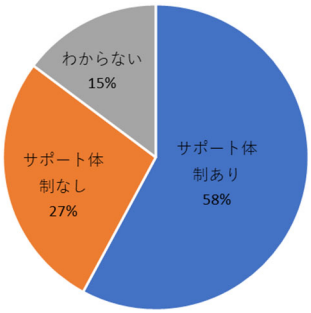

図 3：CISO 等をサポートする組織的体制状況

続いて，文献[2]などでも重要性が指摘されている経営層

c なお，文献[5]では CISO 等を任命している企業の回答者（534 人）を対象とした調査結果が報告されている．しかしながら，本研究では CISO 等を特に任命していない企業の回答者も含んだ個票データでもって分析を行っていく．CISO 等を任命している企業のみを対象とした「CISO 調査」の単純集計などについては文献[5]を参照されたい．

d なお， CISO 等を任命している企業の回答者に限定すると，リスクを分析し，結果を経営層の事業リスク評価に役立てている」と回答した割合は約 50%，「リスクを分析してはいるが，結果を経営層の事業リスク評価に役立てていない」と回答した割合は約 32%となり，CISO 等の任命の有無によりこの状況が異なることがわかる．

の情報セキュリティ対策への関与について考える．「CISO 調査」には，セキュリティリスクの評価，インシデントへの対応方針，投資計画等のサイバーセキュリティの全社的な戦略・方針について，最もよく議論されている（経営層が参加する）会議等についての質問がある．この質問に対する回答をまとめたものが図 4 である（この質問では最も議論される会議を 1 つだけ回答者に選択してもらう形をとっている）．

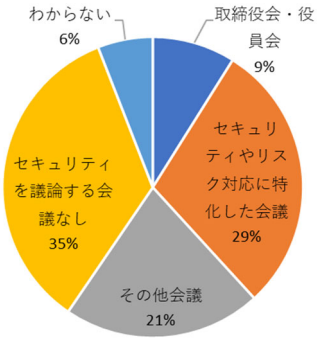

図 4：経営層のセキュリティへの関与状況

図 4 を見てわかるように，取締役会や役員会で情報セキュリティに取り上げている回答者の割合は 9%程度に留まっているが，経営層が参加する会議等で情報セキュリティに関する事案が取り上げられる割合は約 60%となっている．しかしながら，セキュリティを議論する会議がないと回答した割合は 35%もあり，経営層の情報セキュリティ対策への関与は途半ばであると言えるかもしれない．

(3) 企業規模（従業員数）・業種

「CISO 調査」の回答者の所属する企業規模（従業員数）ならびに業種についてまとめたものが図 5 と図 6 である．

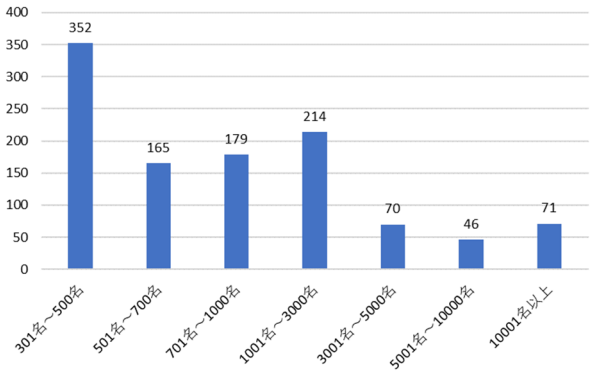

図 5：企業規模（従業員数）

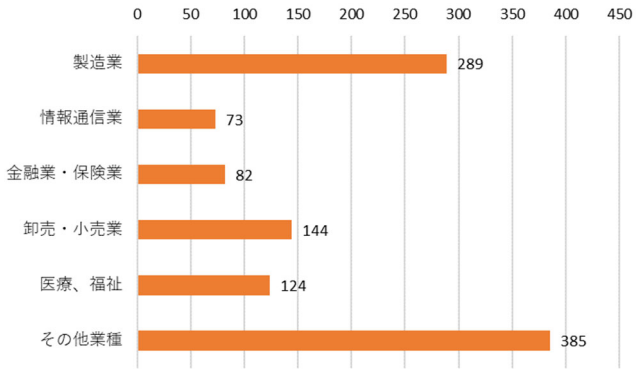

図 6：業種

本研究の分析に従業員数を用いた理由として，企業規模が大きいほど，その企業が所有する情報資産が多いと考えている．そのため，本研究では，従業員数が所有する情報資産の規模を表わす代理変数としている[e]．図 5 を見てわかるように，301 名～500 名未満の従業員数である企業の回答者の割合が全体の 32%で最も割合が高く，従業員数が 3001 名以上の企業の回答者の割合は全体の 17%になっている．

「CISO 調査」では日本標準産業分類に基づいて業種を 17 カテゴリに分類しているが，本研究では，①製造業，②情報通信業，③金融業・保険業，④卸売・小売業，⑤医療・福祉，⑥その他業種の 6 カテゴリに分類している．その結果が図 6 である．「CISO 調査」の回答者の約 3 割が製造業の企業に属していることがわかる．

4. 分析

本研究では，多重コレスポンデンス分析を行い，セキュリティリスク分析と評価の実施状況と情報セキュリティに関する組織体制，企業規模などの関係性・類似性について検討を試みる．

4.1 多重コレスポンデンス分析

2 つのカテゴリ（質的）変数間の関係について調べる方法はコレスポンデンス（対応）分析と呼ばれる．2 つのカテゴリ変数は行項目と列項目に分けられ，その関連性についてはクロス集計表を用いて表の形で示すことができるが，行と列の項目数が多くなれば，表の解釈が難しくなるといった難点がある．コレスポンデンス分析は，それぞれの項目を散布図で視覚化するだけではなく，2 つの項目を組み合わせた散布図で項目間の関係を視覚的に捉えることができるといった特徴を持つ．コレスポンデンス分析を拡張し，3 つ以上のカテゴリ変数間の関連性・類似性を，平面的な（もしくは，立体的な）図で示す分析方法が多重コレスポンデンス分析（multiple correspondence analysis）である[10]．

多重コレスポンデンス分析は，コレスポンデンス分析と同様に，多重クロス集計表の関連性を分析することになる．

e この仮定については今後，更なる検証を行う必要がある．

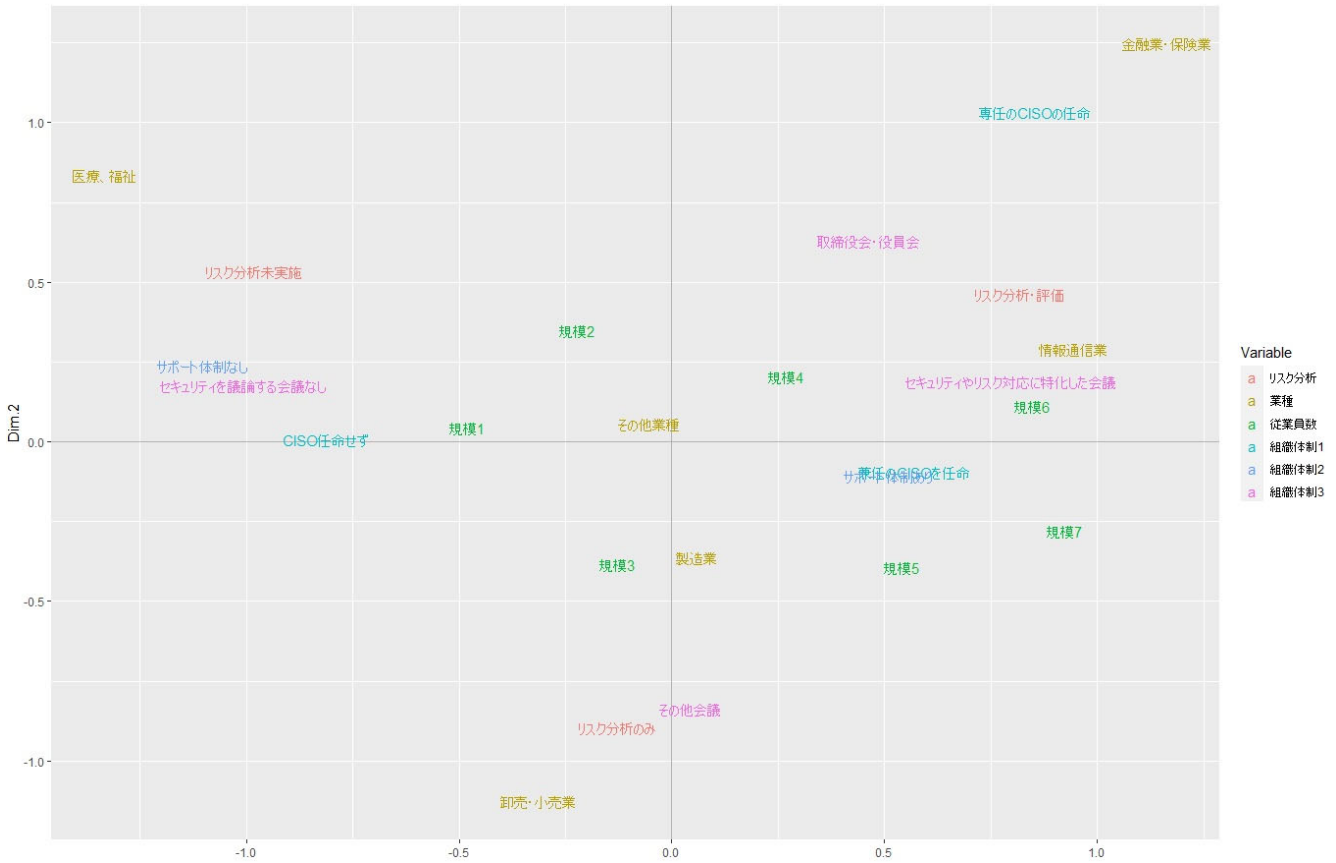

図 8：分析結果

また，多重コレスポンデンス分析では，質問項目だけでなく，大量の回答データから特徴的な傾向やパターンを抽出するデータマイニングにも適している．

4.2 質問項目の加工

多重コレスポンデンス分析を行うためには，アンケート調査によって収集された回答データを加工する必要がある．

第 3.2 節で示した「セキュリティリスク分析と評価の実施状況」「CISO 等の任命状況」「経営層のセキュリティへの関与状況」「従業員数」「業種」に対してこれらの変換作業を行う[f]．また，いずれの質問にも「わからない」という選択肢が与えられており，これらを含めて分析することも可能であるが，本研究ではいずれか一つでも「わからない」を選択した回答者は分析から除外することとした．そのため，実際の分析では回答者数（1,097 人）と一致しないことを断っておく．

「セキュリティリスク分析と評価の実施状況」は 3 カテゴリ，「CISO 等の任命状況」は 3 カテゴリ，「経営層のセキュリティへの関与状況」は 4 カテゴリ，「従業員数」は 7 カテゴリ，「業種」は 6 カテゴリである．

4.3 分析結果

本研究では，R version 4.0.3 を用いて，「セキュリティリスク分析と評価の実施状況」「CISO 等の任命状況」（組織体制 1）「CISO 等をサポートする組織的体制状況」（組織体制 2）「経営層のセキュリティへの関与状況」（組織体制 3）「従業員数」「業種」の多重コレスポンデンス分析を行った[11]．その分析結果を図示したものが図 7 である．

この分析に用いられているサンプルサイズは 866 人，カテゴリ総数は 20 であり，多重コレスポンデンス分析における最大次元数は 19 である．紙面の都合上，省略するが，多重コレスポンデンス分析を実行して得られる固有値に関する結果に関して，累積寄与率が第 2 軸までで 20.82%であり，一定の水準に達しているといえる．第 3 軸までを見ると 27.14 %となり，必ずしも大きな改善は見られない．また，多次元空間でプロットを解釈することは非常に困難であるため，本研究では平面の結果を採択することにする．

多重コレスポンデンス分析では，第 1 軸と第 2 軸の解釈を与える必要がある．これらは因子分析や主成分関などと同様に，分析に投入したカテゴリデータから抽出された概念的なものである．図 8 を見てみると，第 1 軸は従業員数（企業規模）や経営層の関与の程度といった要因でもって構成されるもの，また第 2 軸は経営層の関与の程度や重要インフラといった要因でもって構成されるものであると解釈できる．

f 「CISO 等をサポートする組織的体制状況」についてはもともと「サポート体制あり」「サポート体制なし」の 2 値を持つものなので特に変換作業の必要はない．

4.4 考察

第 4.3 節の多重コレスポンデンス分析によって,「セキュリティリスク分析と評価の実施状況」「CISO 等の任命状況」「経営層のセキュリティへの関与状況」「従業員数」「業種」の関係が平面に可視化された．まず，図 7 の見方について簡単に説明する．例えば，組織体制 3（経営者のセキュリティへの関与）の一つである「セキュリティやリスクに特化した会議」の近くに位置しているものとして「情報通信業」「規模 6（従業員数 5,001 名～10,000 名）」「リスク分析・評価（リスク分析と評価をともに実施）」「サポート体制あり」「兼任の CISO を任命」などがある．これらの要因は，セキュリティやリスクに特化した会議においてセキュリティに関して経営者と情報共有等を行っている企業の特徴であると言える．一方で，例えば「規模 1（従業員数 301 名～500 名）」とは離れているため，この要因との関係性は弱いと言える．このように，注目する要因 A があった場合、その近くにある他の要因でもってその特徴付けが可能となる．これを踏まえて，以下，これの分析結果に対する考察を行っていく．

続いて,「セキュリティリスク分析と評価の実施状況」に着目すると,「リスク分析・評価（リスク分析と評価をともに実施）」「リスク分析のみ」「リスク分析未実施」はいずれも離れた場所に位置している．そこで見えてくる特徴として，以下のことが挙げられる．

1) リスク分析を実施していない企業は，CISO 等をサポートする組織的体制がないだけでなく，経営層の関与も弱い（セキュリティを議論する会議がない）ことなどが見てとれる．また，企業規模も従業員数が 700 名以下であること（「規模 1」「規模 2」）がわかる．この結果は中小企業の情報セキュリティ対策ならびにそのための組織体制の整備の遅れを表しているかもしれない．

2) リスク分析のみを実施している企業の特徴は，取締役会・役員会やセキュリティやリスク対応に必ずしも特化していない会議（「その他会議」）でもってセキュリティなどに関する情報共有を行っており，業種としては卸売・小売業に多く見られること，また，企業規模も従業員数が 700～1000 名程度（「規模 3」）であることがわかる．さらにサポート体制については「サポート体制あり」とも「サポートなし」ともある程度の距離があるために，明確なことはわからない．これから組織体制などを整えていく可能性を秘めていると言える．

3) リスク分析と評価をともに実施している企業の特徴は，1)や 2)と比べると，顕著な特徴があることがわかる．経営層のセキュリティへの関与が比較的強く（「取締役会・役員会」「セキュリティやリスク対応に特化した会議」），企業規模としては従業員数が 5,001 名～10,000 名と比較的多く，専任もしくは兼任の CISO 等を任命しているとともに，彼らをサポートする組織体制も整備されていることが見てとれる．しかしながら，企業規模に関して従業員数が 1,001 名～3,000 名（「規模 4」）である企業にも同様の傾向があることが示唆される．一方で，「規模 5」「規模 7」とは距離があるため，従業員数が多いからといって必ずしもリスク分析と評価をともに実施されるとは限らないことがわかる．また，業種としては，情報通信業に多く見られる傾向があることがうかがえる．

これに加えて，図 7 より金融業・保険業に属する企業は専任の CISO の任命を行う傾向が強い一方で，情報通信業に比べるとリスク分析と評価をともに実施している企業数は必ずしも多くはないことが読み取れる．

5. おわりに

本研究では, IPA が 2019 年 10 月に実施した「企業の CISO 等やセキュリティ対策推進に関する実態調査」で収集した個票データを用いて，事業リスクとしてのセキュリティ分析やその評価の実施状況と企業規模や企業のセキュリティに関する組織体制などの関係について多重コレスポンデンス分析を試みて，セキュリティ分析やその評価の実施状況に応じた企業の特徴を明らかにした．その結果，リスク分析を実施していない企業の特徴として，CISO 等をサポートする組織的体制がないだけでなく，経営層の関与も弱い傾向があること，またリスク分析のみを実施している企業の特徴は，取締役会・役員会やセキュリティやリスク対応に必ずしも特化していない会議で経営者とのセキュリティに関する情報共有を行っている傾向があることを明らかにした．これに加えて，リスク分析と評価をともに実施している企業の特徴は経営層のセキュリティへの関与が比較的強く，専任もしくは兼任の CISO 等を任命しているとともに，彼らをサポートする組織体制も整備されていることなどが明らかになった．

これらのことから，リスク分析と評価をともに実施していくにあたって，リスク分析のみを行っている企業は今後 CISO 等の任命ならびに CSIRT などの企業のセキュリティ対策をサポートする組織体制の構築が望まれるとともに，経営層のセキュリティへの関与が高められることが期待される．

最後に，本研究の今後の展望を述べる．本研究では明らかにできていない，また昔から注目されている経営層と情報システム部門や CISO 等とのサイバーセキュリティに対する意識ギャップの存在などについての検証を行いたい．

参考文献

[1] 情報処理推進機構, 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 https://www.ipa.go.jp/files/000065213.pdf（参照 2021-5-5）
[2] 経済産業省・情報処理推進機構, サイバーセキュリティ経営ガイドライン Ver2.0, 2017, http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf（参照 2021-5-5）
[3] NRI セキュアテクノロジーズ, NRI Secure Insight 2019, 2019 年

https://www.secure-sketch.com/news/news_20190718（参照 2021-5-5）
[4] 情報処理推進機構, 企業の CISO や CSIRT に関する実態調査 2017」報告書,2017 年, https://www.ipa.go.jp/security/fy29/reports/ciso-csirt/index.html（参照 2021-5-5）
[5] 情報処理推進機構, 企業の CISO 等やセキュリティ対策推進に関する実態調査, 2020 年 https://www.ipa.go.jp/security/fy2019/reports/2019DL_index.html（参照 2021-5-5）
[6] 情報処理推進機構, サイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集 第 2 版, 2020 年 https://www.ipa.go.jp/security/fy30/reports/ciso/index.html（参照 2021-5-5）
[7] 近藤光・寺本直城・杉原大輔・中西晶, CSIRT におけるレジリエンスの罠, 日本情報経営学会誌, 37(3), 27-48, 2018 年
[8] 金子啓子･原田要之助, 情報セキュリティガバナンスについて, IPSJ SIG Technical Report, 2018－EIP-79(7), 1-10, 2018 年
[9] 和泉あゆみ・加藤慎也・小松文子・竹村敏彦, サイバーリスクに関する実証分析, Proceeding of Computer Security Symposium 2015, 631-638, 2015 年
[10] Le Roux, B., Rouanet, H.: Multiple Correspondence Analysis, SAGE Publications, 2010
[11] 川端一光・岩間徳兼・鈴木雅之, R による多変量解析入門: データ分析の実践と理論, オーム社, 2018 年