資料４-２

平成 28 年度内閣サイバーセキュリティセンター委託調査

平成 28 年度
企業のサイバーセキュリティ対策
に関する調査報告書

平成 29 年３月

ニュートン・コンサルティング株式会社

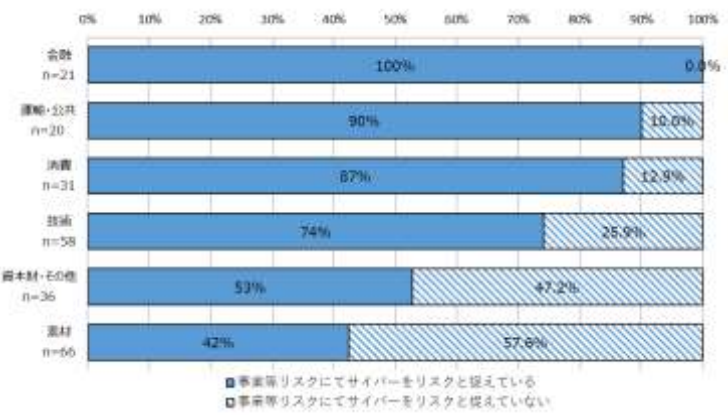
【目　次】

エグゼクティブサマリ

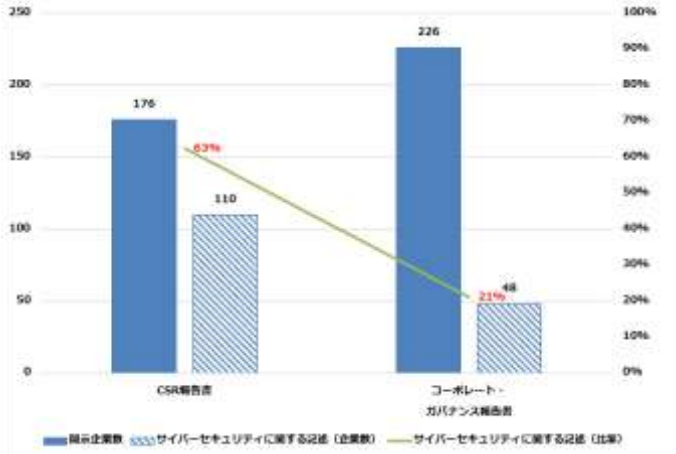
これまで、我が国の IT の利活用は業務効率化を主な目的にしていたが、近年では、IoT や AI、ビッグデータなど新しい価値を創造するようなビジネス・イノベーションが求められている。その際、情報システム部門にとどまらず、企業内の幅広い組織においてサイバーセキュリティに取り組むことが重要である。サイバーセキュリティの取組に向けた経営者の意識改革を進め、サイバーセキュリティ人材の活躍できる場（雇用）の確保、つまり需要面における対応が必要である。その上で、サイバーセキュリティ人材の需要に応じた、教育・訓練、評価等の人材の供給面の整備も必要であり、サイバーセキュリティの企画・立案や経営層への説明、実務者層全体を指揮する橋渡し人材層の育成・確保や企業内の幅広い組織におけるそれぞれの役割に応じたサイバーセキュリティの知識・能力の向上が重要となっている。サイバーセキュリティの人材育成においては、これらの「人材の需要」と「人材の供給」を相応させ、好循環の形成を促進することが必要である。

今回の調査は、こうしたサイバーセキュリティ人材育成における「人材の需要」と「人材の供給」の状況を把握し、企業における経営層の意識改革・橋渡し人材層の配置状況や人材の量的拡大と質的向上の取組状況を明らかにするため、調査・分析を実施した。調査は、平成 28 年 9 月から 10 月にかけて上場企業 225 社等を対象として実施し、公開している文書のサイバーセキュリティに関する記載状況を調査するとともに、アンケート調査を実施した。

有価証券報告書の「事業等のリスク」へサイバーセキュリティについて記載する企業は年々増加している。その記載率を業種別にみると、上位から金融、運輸・公共、消費、技術、資本財・その他、素材となっており、金融は全ての企業がサイバーセキュリティについて記載している。有価証券報告書以外では、コーポレート・ガバナンス報告書と CSR 報告書の開示数及びサイバーセキュリティの記載率に着目すると、開示数はコーポレート・ガバナンス報告書が多いが、サイバーセキュリティの記載率は CSR 報告書が高い。サイバーセキュリティの取組に関する情報発信は、企業統治という観点ではなく、社会的責任として行われている可能性がある。



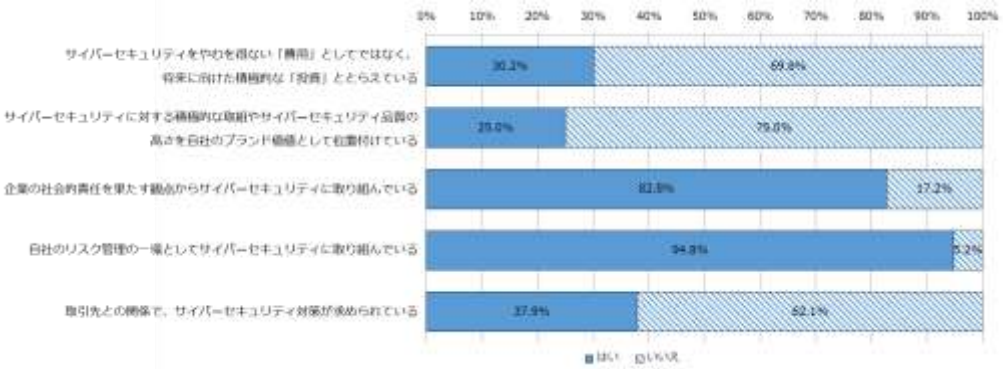
【図表 1】分野別サイバーセキュリティに関する記載状況



【図表 2】その他資料を公開している企業

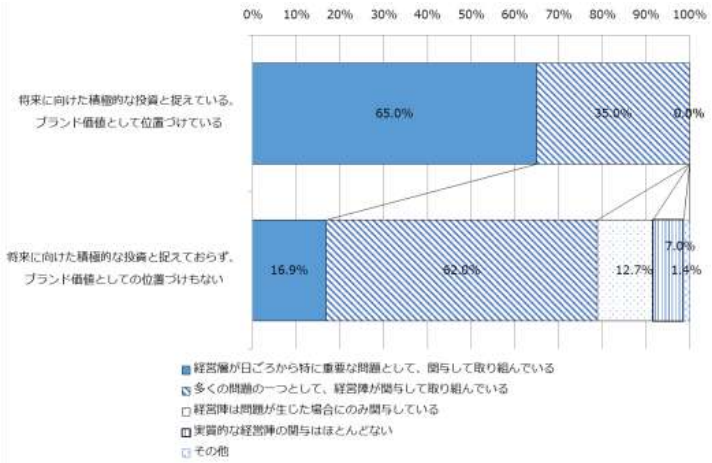
アンケート結果では経営層がサイバーセキュリティをやむを得ない費用ではなく投資と捉え、高いレベルのセキュリティ品質の実現が自社のブランド価値の

向上につながると考えている企業は、社会的責任やリスク管理として取り組んでいる企業と比較して約 3 割と少ない。



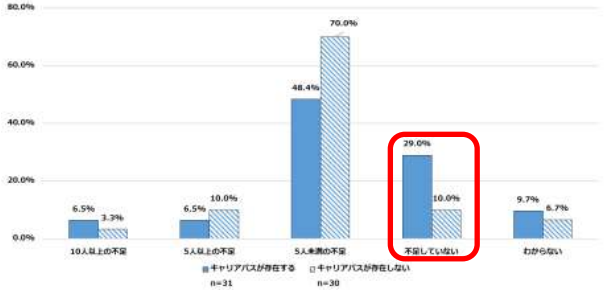
【図表 3】企業がサイバーセキュリティに取り組む姿勢

しかし、サイバーセキュリティへの取組を投資やブランド価値として位置づけている企業は、他の企業と比較して経営層が日ごろから特に重要な問題としてサイバーセキュリティに取り組んでおり、人材の明確化や人材育成の対応が進み、キャリアパスの確立など体制の整備が進んでいる傾向がある。また経営層が日ごろから特に重要な問題としてサイバーセキュリティに取り組んでいる企業では、有価証券報告書等の公開資料を用いた情報発信も積極的に行っており、経営層の意識の高まりが、体制整備や積極的な情報発信等につながり、人材の需要を生み出していると考えられる。さらに、キャリアパスを構築していない企業の方が、構築している企業に比べ、橋渡し人材や事業部門におけるサイバーセキュリティ人材が不足している傾向がみられる。



【図表 4】サイバーセキュリティの取組と経営層の関与

今後、新たな価値の創造という「挑戦」に付随する「責任」としてサイバーセキュリティに取り組むという、経営層への意識改革を促すことにより、サイバーセキュリティにおける需要（雇用・キャリアパス）が高まると同時に、それに併せた供給（教育・訓練等）の好循環を生み出すことが期待される。



【図表 5】橋渡し人材層の過不足とキャリアパスの設定

1章. 本調査の背景、目的及び調査概要

1.1. 背景

これまで、我が国の IT の利活用は業務効率化を目的にしたものが中心であり、情報システム部門に代表される IT の専門部署が中核となり、セキュリティ対策も含めて取り組むケースが多かった。近年では、こうした IT 利活用に加え、IoT や AI、ビッグデータなど、IT の利活用により新しい価値を創造するようなビジネス・イノベーションが求められている。こうしたビジネスにおける「挑戦」においては、事業そのものと深く関わる IT の専門部署にとどまらず、事業部門はもちろんのこと、経営企画部門、製造部門、法務部門など、企業内の幅広い組織においてサイバーセキュリティへ取り組むことが重要となっている。

こうした状況の変化に伴い、経営層は、サイバーセキュリティを経営問題として捉えるだけでなく、ビジネス・イノベーションを通じた新しい価値の創造という「挑戦」に付随する「責任」として、サイバーセキュリティに取り組むことが重要となっている。また、サイバーセキュリティへの取組に係る姿勢や方針等の自社のレベルの高さを「セキュリティ品質」として主体的に情報発信していくことで、関係者の理解が深まり、社会的評価を高めることにつながる可能性がある。このような経営者の意識改革を進め、サイバーセキュリティ人材の活躍できる場（雇用・キャリアパス）を確保していくこと、すなわち需要面における対応が、サイバーセキュリティ人材の検討においては大前提となる。

また、こうしたサイバーセキュリティ人材の需要に対応した、教育・訓練、評価等の供給面の整備も重要である。例えば、実務者層では、サイバーセキュリティに関わる役割の範囲が広がった結果、情報セキュリティ技術に関する知識・能力の向上だけでなく、各部門のそれぞれの役割を担う人材がチームとなってサイバーセキュリティを推進する体制が重要となっている。また、このような体制の下で、サイバーセキュリティ以外を中核とする業務に従事する人材についても、共通の基礎知識と分野特有のサイバーセキュリティの基礎知識を身に着けることが必要となる。さらに、経営層が実務者層と直接コミュニケーションをとることは難しいため、サイバーセキュリティの企画・立案を行い、経営層への説明や承認を得るとともに、幅広い役割を持ったセキュリティに関わる実務者層全体を指揮する橋渡し人材層の育成・確保が重要となっている。

サイバーセキュリティ人材育成においては、これらの「人材の需要」と「人材の供給」を相応させ、好循環の形成を促進することが必要であり、ビジネスにおける「挑戦」とそれに付随する「責任」としてのサイバーセキュリティを実現する観点を含め、企業におけるサイバーセキュリティ人材に係る課題を検討していくことが重要である。

1.2. 目的

サイバーセキュリティ人材育成において、需要（雇用・キャリアパス等）と供給（教育・訓練等）の状況を把握するため、企業における経営層の意識改革・橋渡し人材層の配置状況や人材の量的拡大と質的向上の状況を明らかにし、需要と供給の好循環がどの程度進んでいるのか把握することを目的とする。

1.3. 調査概要

1.3.1. サイバーセキュリティ対策に係る情報発信内容の調査

(1). 有価証券報告書におけるサイバーセキュリティの情報開示状況調査

日経 225 等の企業を対象に、直近 7 期年の開示状況を調査し、「事業等のリスク」としてサイバーセキュリティを捉えている企業の時系列的な変化や業種ごとの特徴、その記載内容からサイバーセキュリティに対する取組姿勢や抱える課題の傾向について調査・分析した。

(2). 「その他開示資料」における記載されたサイバーセキュリティの情報開示状況調査

日経 225 等の企業を対象に、情報セキュリティ報告書、情報セキュリティ基本方針、CSR 報告書、サステナビリティレポート及びコーポレート・ガバナンス報告書を「その他開示資料」と位置づけ、サイバーセキュリティに関する記載状況から、サイバーセキュリティに対する取組姿勢や抱える課題の傾向について調査・分析した。

1.3.2. アンケートによるサイバーセキュリティへの取組状況調査

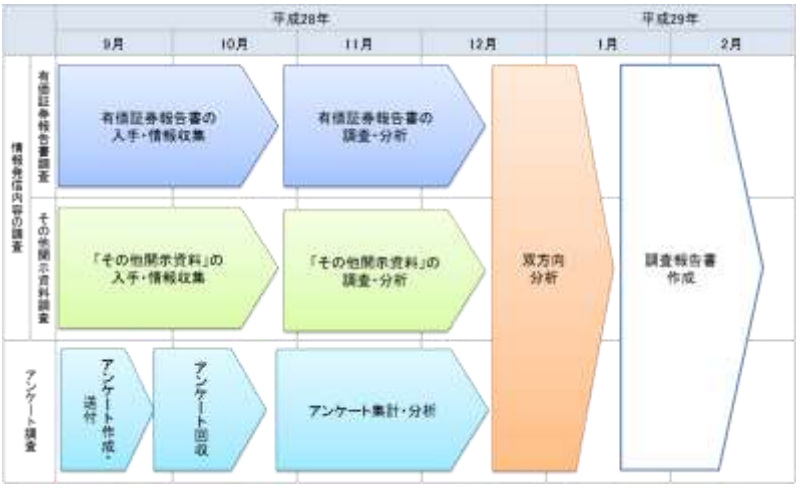
日経 225 等の企業を対象に、各企業のサイバーセキュリティを担当する部門に対して、自社のサイバーセキュリティに関する経営層の関わり方、橋渡し人材層や実務者層の配置状況や育成に関する課題等の実態を明らかにするためアンケート調査を行い、その傾向を分析した。

1.3.3. 情報発信状況とサイバーセキュリティ取組状況の調査結果を用いた双方向分析

日経 225 等の企業を対象に、有価証券報告書及びその他開示資料におけるサイバーセキュリティリスクの記載状況と担当部門へのアンケートを利用したサイバーセキュリティへの取組状況を用いて、需要と供給の循環についてその傾向を双方向分析した。

1.4. 実施スケジュール

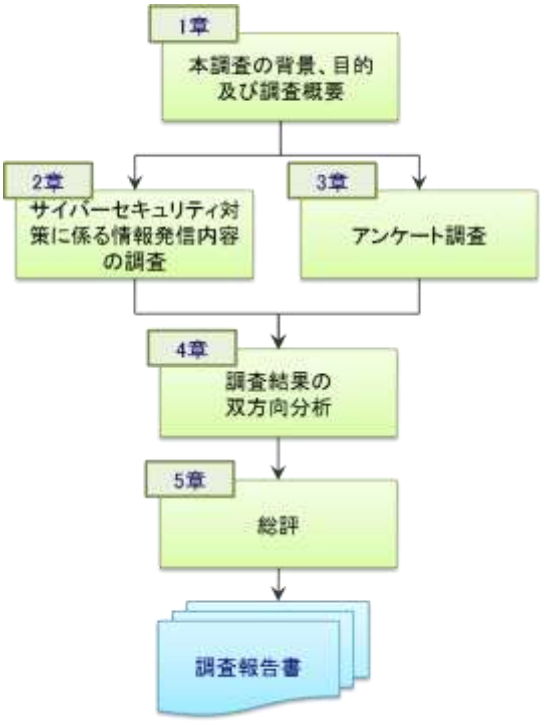
本調査は、平成 28 年 9 月から開始し、有価証券報告書及びその他開示資料の調査・分析を進めるとともに、9 月 30 日から 10 月 17 日にかけてアンケートを実施し、その結果も踏まえて総合的に分析した。



【図表 1-1】実施スケジュール

1.5. 本報告書の構成

本報告書の構成は、1 章において本調査の背景や目的を示すとともに、2 章及び 3 章において調査・分析を行い、4 章にて更なる詳細分析を実施、5 章にて総評として取りまとめている。



【図表 1-2】本報告書の構成

2章. サイバーセキュリティ対策に係る情報発信内容の調査

2.1. 目的

サイバー攻撃の脅威は深刻化しており、その影響は地域や社会全体にも支障を来す可能性がある。企業のサイバーセキュリティへの取組の情報発信は、地域や社会における関係者の理解を深め、ひいては自社の社会的評価を高めることにつながる可能性がある。

本調査では、有価証券報告書、及びその他開示資料を対象として、サイバーセキュリティに関して想定する被害や脅威及び対策等の記載状況を調査し、以下の観点から情報発信の状況を明らかにすることを目的とする。

【有価証券報告書における調査・分析の観点】

① 時系列的な変化(開示状況の増減)

② 業種別及び事業形態別の開示状況

③ サイバーセキュリティリスクに関する記載内容（脅威と感じているサイバー攻撃の種類や想定する被害状況、具体的な対策等)

【その他開示資料における調査・分析の観点】

① 各資料におけるサイバーセキュリティに関する記載状況

2.2. 調査対象と調査方法

2.2.1. 対象企業

上場企業　225 社（平成 26 年 11 月 1 日現在の日経平均株価指数銘柄）等

2.2.2. 対象資料と選定理由

企業は情報発信の方法として、一般的に認知されている文書を活用する可能性があるため、幾つかの資料から以下の 6 つの文書を調査対象として選定した。

(1). 有価証券報告書

有価証券報告書の「事業等のリスク」において、サイバーセキュリティに関して記載している可能性があり選定した。

(2). その他開示資料

- 情報セキュリティ報告書

企業の社会的責任の一つとして機密保持を確保するための方針や情報セキュリティ管理体制、人材育成の考え方等が記載されており、サイバーセキュリティの取組が記載されている可能性があるため選定した。

- 情報セキュリティ基本方針

企業が活動の一つとして、情報資産を取り扱う際のセキュリティに対する基本的な考え方を開示するためのものであり、開示企業のセキュリティに対する姿勢が把握できる可能性があり選定した。

- CSR 報告書

企業の社会的責任としての活動を記載する文書であり、企業が社会的責任の一貫としてサイバーセキュリティの確保が必要と捉えて開示している可能性があり選定した。

- サステナビリティレポート

CSR 報告書と同様に、社会的責任の一つとして企業がサイバーセキュリティに取り組み、その内容を開示している可能性があり選定した。

- コーポレート・ガバナンス報告書

コーポレート・ガバナンスコードの原則において、「法令に基づく開示以外の情報提供にも主体的に取り組むべきである」とされ、サイバーセキュリティへの取組を情報提供している可能性があり選定した。

2.2.3. 対象期間

(1). 有価証券報告書

平成 21 年度～平成 27 年度発行分

※ 7 期年を対象とした理由としては、平成 26 年度において同様の調査を実施しており、その際に平成 21 年度を起点として調査を実施している。今回の調査においては、前回調査との差異(時系列的な変化)についても着目すべきであるとの視点から 7 期年を対象とした。

(2). その他開示資料

平成 27 年度発行分

※ その他開示資料については、前回の調査においては対象としておらず、今回初調査という位置づけであり、直近年のみとした。

2.2.4. 調査方法

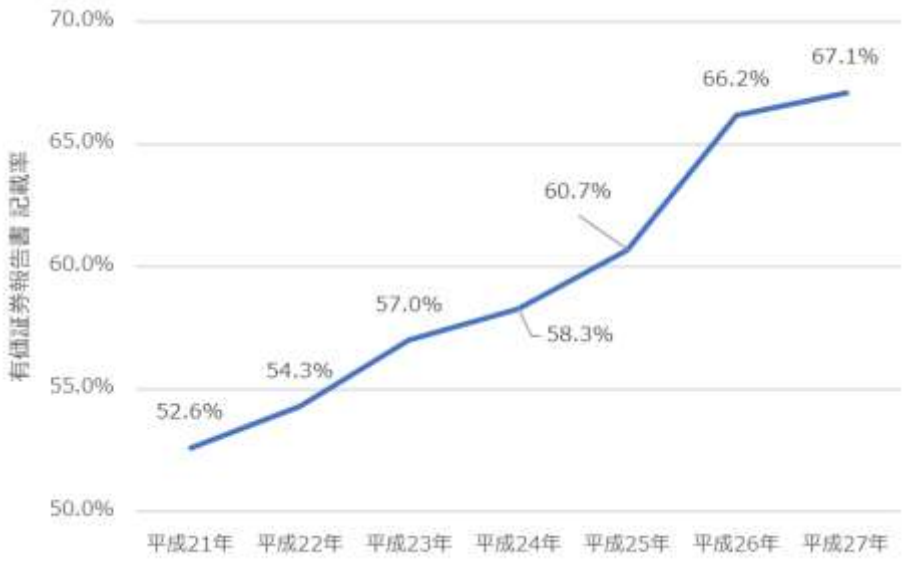
対象となる有価証券報告書及びその他開示資料を収集し、各資料におけるサイバーセキュリティに関する記載内容を確認する形で調査を行った。

2.3. 調査結果

2.3.1. 有価証券報告書に関する調査

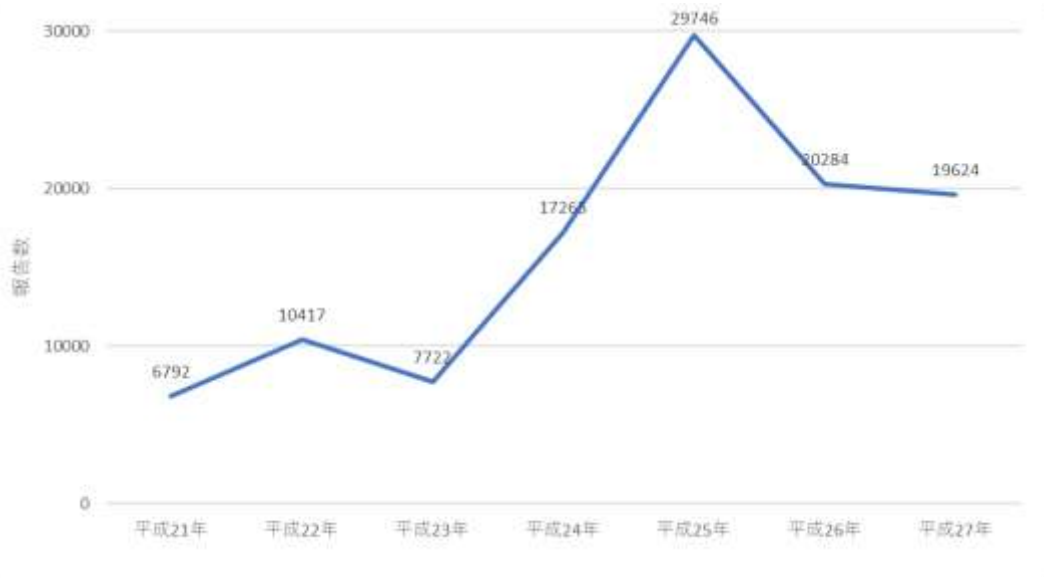
(1). 時系列的な変化(開示状況の増減)

平成 16 年 3 月期から有価証券報告書への記載が義務付けられている「事業等のリスク」項目において、サイバーセキュリティリスクを開示する企業の割合は、平成 21 年には 52.6%であったが、平成 27 年には 67.1%と年々増加しており、また、単年でみると平成 25 年から平成 26 年にかけて 5.5%と一番高い上昇率を示している。



【図表 2-1】サイバーセキュリティに関する記載状況の変化

セキュリティインシデントの報告数は、平成 23 年にいったん減少するが年々増加し、平成 25 年に 29,746 件に達し、20,000 件前後で推移している。



【図表 2-2】（参考）JPCERT/CC によるセキュリティインシデント報告数

※　グラフは、JPCERT/CC が公開しているデータを基に新たに作成
https://www.jpcert.or.jp/ir/report.html

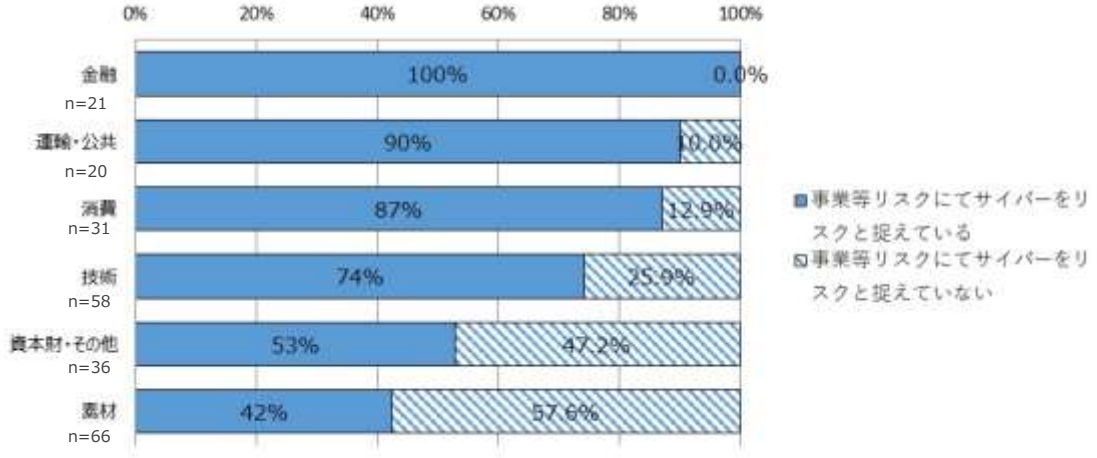
【考 察】

JPCERT/CC の公開データによると、改ざんされた Web サイトの閲覧によって PC がマルウエアに感染するセキュリティインシデント等が急増し、平成 25 年に報告数が約 30,000 件に達した後、翌年には約 20,000 件に減少している。また、有価証券報告書へのサイバーセキュリティ記載率は平成 26 年に上昇したが、平成 27 年には伸びが鈍っている。

インシデントの発生が前年（平成 25 年）の約 30,000 件か 3 割程度減少した結果、有価証券報告書の記載率の上昇が鈍った可能性がある。

(2). 業種別及び事業形態別の開示状況

直近年の開示状況を業種別にみると、平成 27 年度におけるサイバーセキュリティに関する記載率は、上位から金融、運輸・公共、消費、技術、資本財・その他、素材となっており、金融では記載率が 100%、続いて運輸・公共が 90%、消費が 87%と続いている。



【図表 2-3】分野別サイバーセキュリティに関する記載状況

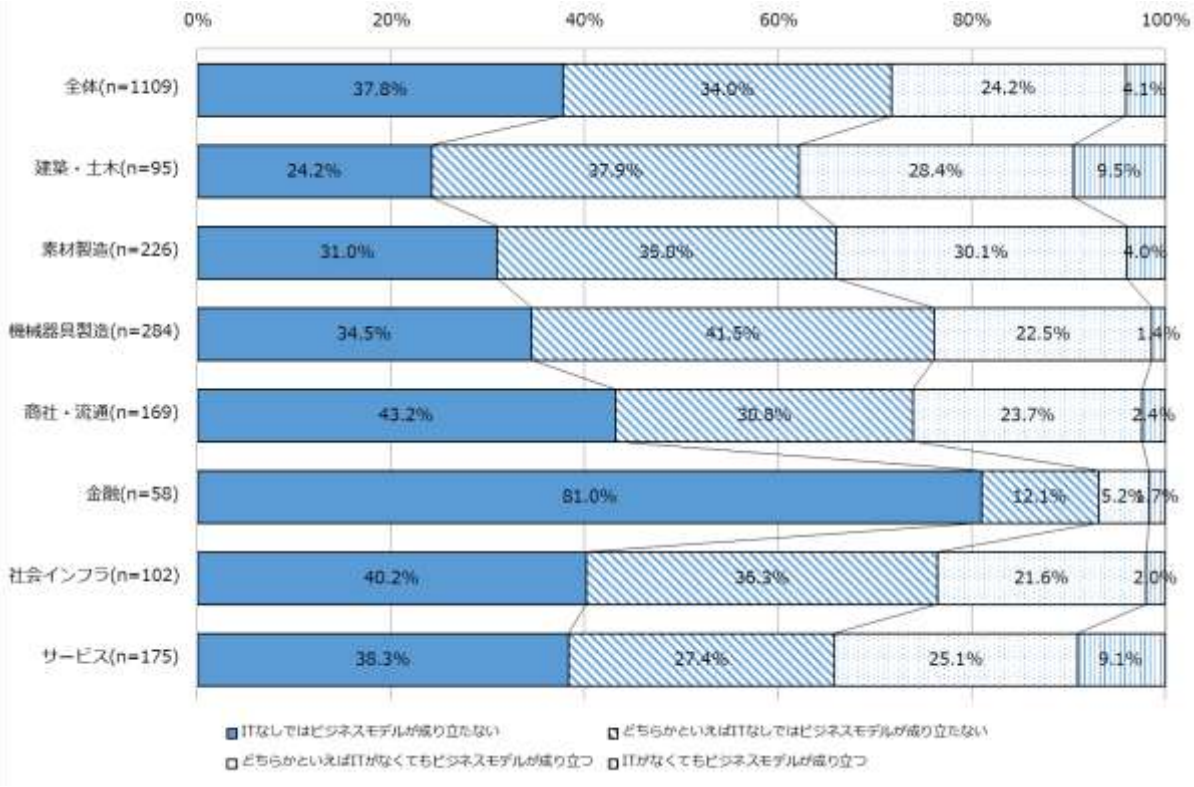
平成 21 年度からのサイバーセキュリティに関する記載が増加した企業について業種別に分類した結果、記載が増加した業種は、技術、素材が多く、消費、金融、運輸・公共が少ない結果となった。また、年度別では、技術において平成 23 年年度に 4 企業、平成 25、26 年度に計 7 企業、素材においては、平成 25、26 年度に計 10 企業と増加している。

分野	平成 22 年度	平成 23 年度	平成 24 年度	平成 25 年度	平成 26 年度	平成 27 年度	合計
技術	0	4	0	2	5	2	13
素材	1	1	1	3	7	0	13
資本財・その他	1	1	1	1	0	0	4
消費	0	0	1	0	1	0	2
金融	1	0	0	0	0	0	1
運輸・公共	0	0	0	0	1	0	1
合計	3	6	3	6	14	2	34

【図表 2-4】サイバーセキュリティを新たに記載した企業数の変化

※　分野を細分化したデータについては、「6.3 有価証券報告書における業種別サイバーセキュリティ情報開示状況」を参照

一般社団法人　日本情報システム・ユーザー協会（Japan Users Association of Information Systems:以下、JUAS）の公開しているデータによると、IT なしではビジネスモデルが成り立たない業種は、金融が81%と最も多く、続いて商社・流通が 43.2%、社会インフラが 40.2%及びサービスが 38.3%となっている。



【図表 2-5】（参考）JUAS による主たるビジネスモデルと IT との関係

※　グラフは、JUAS が公開しているデータを基に新たに作成
http://www.juas.or.jp/servey/it16/it16_ppt.pdf

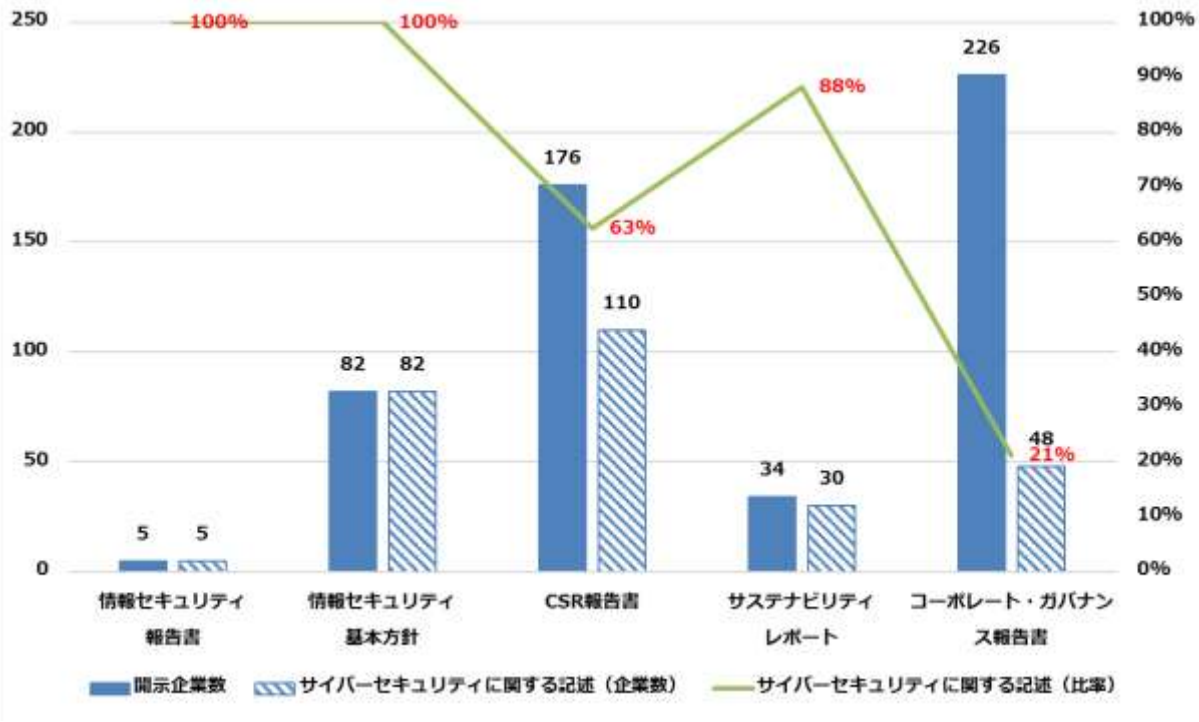
【考 察】

全ての企業が有価証券報告書へサイバーセキュリティに関して記載している「金融」において、JUAS のデータでは「IT なしではビジネスモデルが成り立たない」と回答した企業の割合が突出して高い。また、有価証券報告書の「資本財・その他」は約 5 割の記載率及び「素材」は約 4 割の記載率であるが、JUAS のデータにおいて「資本財・その他」の企業が含まれる「建築・土木」は 2 割強、「素材」が含まれる「素材製造」は約 3 割と「IT なしではビジネスモデルが成り立たない」と回答した企業の割合がその他の業種と比較して低い傾向がある。すなわち、IT とビジネスモデルの関係性が深いほど、情報開示を行う傾向にある。

2.3.2.「その他開示資料」に関する調査

(1). その他開示資料の公開及びサイバーセキュリティインシデントの記載状況

コーポレート・ガバナンス報告書は上場企業に対して公開が義務付けられているため、調査対象の全 226 社が資料を公開しており、CSR 報告書、情報セキュリティ基本方針、サステナビリティレポートと続いている。サイバーセキュリティに関する記述は、情報セキュリティ報告書及び情報セキュリティ基本方針を除くと、サステナビリティレポート、CSR 報告書と続いている。



【図表 2-6】その他資料を公開している企業

【考 察】

CSR 報告書とコーポレート・ガバナンス報告書の公開企業数に着目すると、CSR 報告書の開示企業数は 176 社であるが、サイバーセキュリティに関する記述率は、コーポレート・ガバナンス報告書の約 2 割と比較して、CSR 報告書が約 6 割と高い。サイバーセキュリティの取組は、企業統治の観点ではなく社会的責任として行われている可能性がある。

3章. アンケート調査

3.1. 目的

企業には従来の業務効率化を目的としたITの利活用だけではなく、新しい価値を創造するビジネスにおけるイノベーションの実現が求められており、サイバーセキュリティの対象が企業内の幅広い組織に拡大しており、経営層、幅広い組織の実務者層、そして橋渡し人材層それぞれが、経営戦略の下に連携し、サイバーセキュリティに取り組むことが求められている。

本調査では、以下の観点から経営層の意識改革の状態、実務者層のサイバーセキュリティ人材の確保・育成及び橋渡し人材層の配置状況と確保・育成について明らかにすることを目的とする。

【アンケートにおける調査・分析の観点】

① ITの位置づけと経営層の取組姿勢

② 橋渡し人材層の配置状況と課題

③ 企業内の様々な部門のサイバーセキュリティ人材（組織面について）

④ サイバーセキュリティに関する情報発信の考え方

3.2. 調査対象と実施方法

(1). 対象企業

上場企業　225社(平成26年11月1日現在の日経平均株価指数銘柄)等

※ 可能な限り連結子会社の対策を含めた回答を想定

(2). アンケート実施期間

平成28年9月30日～10月末日

3.2.1. 回答者

サイバーセキュリティ対策に関する担当者

3.2.2. 調査方法

(1). アンケート送付方法

以下を郵便で送付し、アンケートを記入後、同封した返信用封筒で回収した。希望する企業には、別途、電子データを電子メールで送付し、回収した。

【送付物】

- アンケート調査の協力依頼について
- アンケート票
- 返信用封筒

※詳細は 6 章 資料編を参照のこと

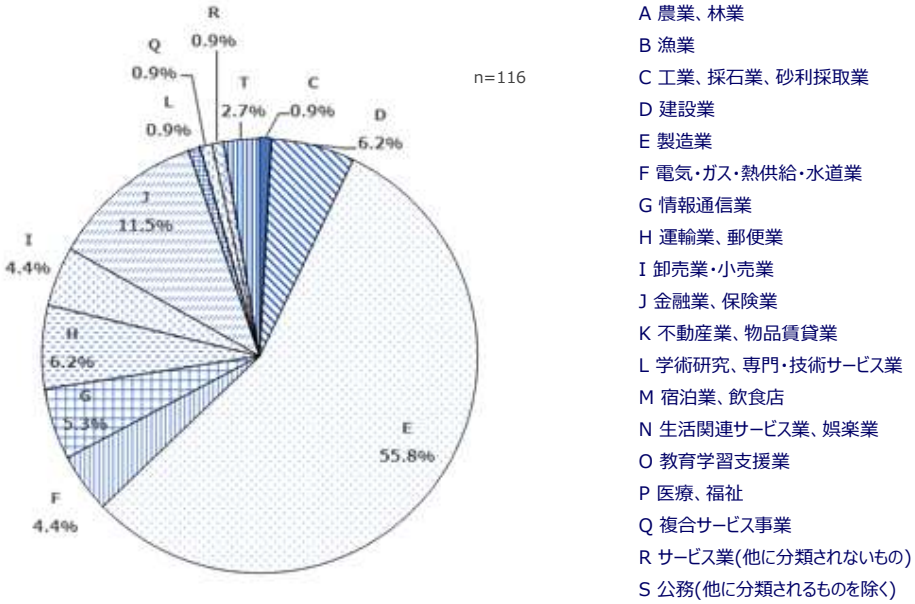
3.3. 調査結果

(1). 回答企業データ

有効回答数：116 社（回答率 約 51%）

(2). 業種

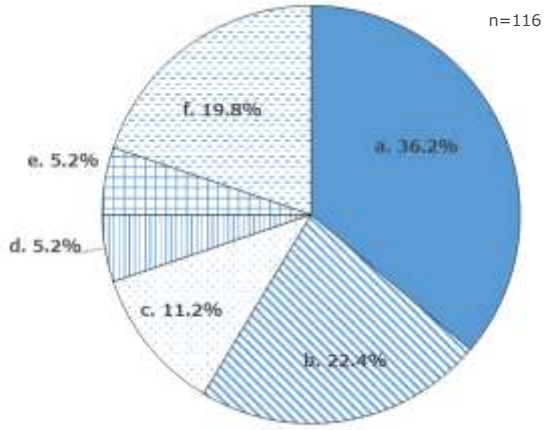
回答した企業の中でも、「製造業」が 55.8%と突出して多く、「金融業、保険業」が 11.5%であり、その他の業種は全て 10%未満であった。



【図表 3-1】回答企業データの業種

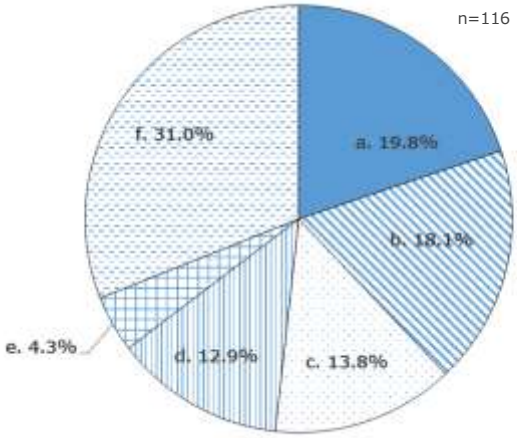
(3). 年間売上高及び従業員数

年間売上高及び従業員数は、連結決算の対象であるグループ全体について集計した。



A ¥0-¥999,999
B ¥1,000,000-¥1,999,999
C ¥2,000,000-¥2,999,999
D ¥3,000,000-¥3,999,999
E ¥4,000,000-¥5,000,000
F ¥>5,000,000

【図表 3-2】売上高（百万円）

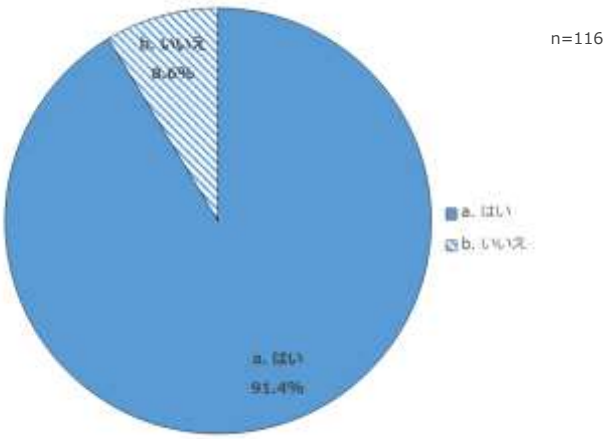


A 0-9,999
B 10,000-19,999
C 20,000-29,999
D 30,000-39,999
E 40,000-50,000
F >50,000

【図表 3-3】従業員数

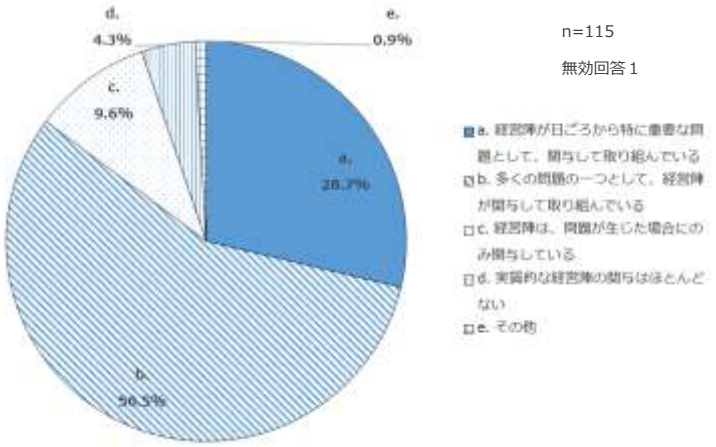
3.3.1. IT の位置づけと経営層の取組姿勢

IT を単なる自社内の業務効率化ではなく、事業戦略に位置づけている企業は、91.4%とほぼ全ての企業が事業において IT を利活用している状況である。



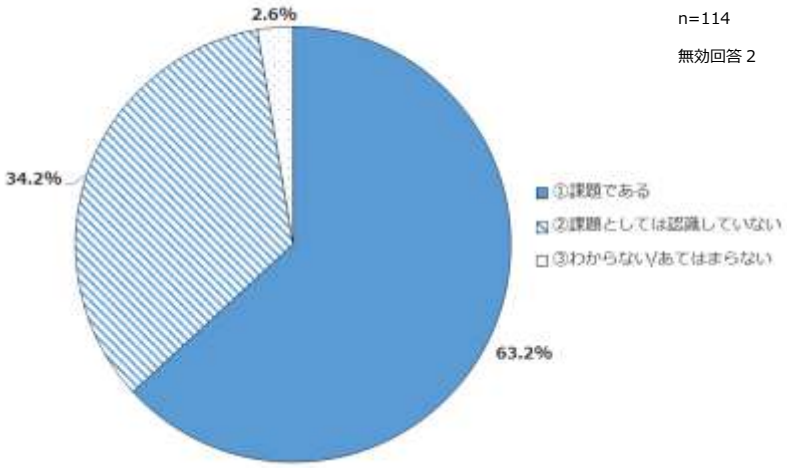
【図表 3-4】IT の利活用を事業戦略に位置づけている企業

また、経営層のサイバーセキュリティに関する関与度合いをみると、日ごろから特に重要な問題として又は多くの問題の一つとして取り組んでいる企業が 85.2%である。



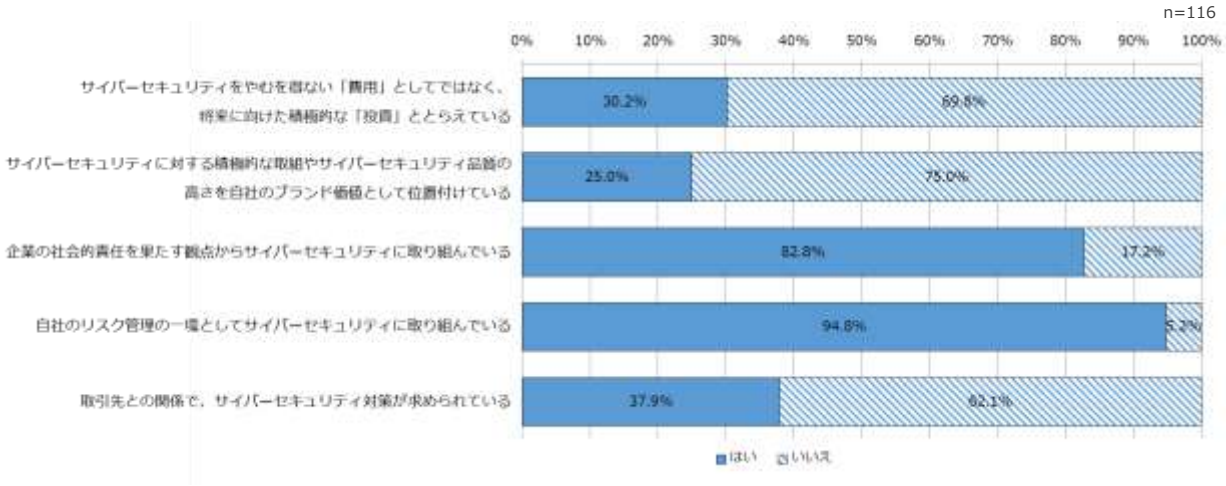
【図表 3-5】サイバーセキュリティに対する経営層の関与

しかし、サイバーセキュリティの取組において経営層の理解と対策の推進を課題として認識している企業は、63.2%である。



【図表 3-6】経営層のサイバーセキュリティに対する理解と対策の推進

また、サイバーセキュリティに取り組む姿勢については、将来に向けた積極的な投資や自社のブランド価値として認識している企業はそれぞれ 30.2%、25.0%である。

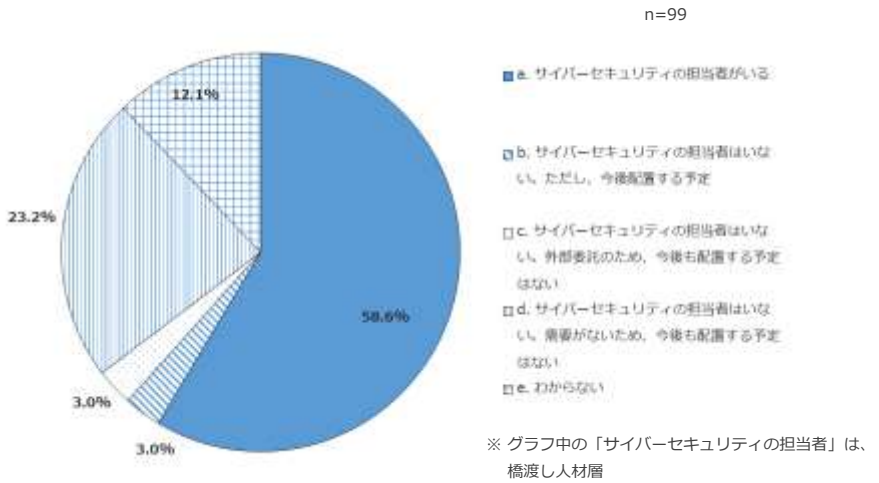


【図表 3-7】 企業がサイバーセキュリティに取り組む姿勢

【考 察】
IT の積極的な利活用や、サイバーセキュリティに対する経営層の関心は高いものの、約 6 割の企業において経営層がサイバーセキュリティを理解し、推進することを課題としている。また約 8 割の企業がサイバーセキュリティを社会的責任、9 割強の企業がリスク管理の一つとして捉えているのに対し、サイバーセキュリティを費用ではなく投資、自社のブランド価値として位置づけている企業はそれぞれ約 3 割である。

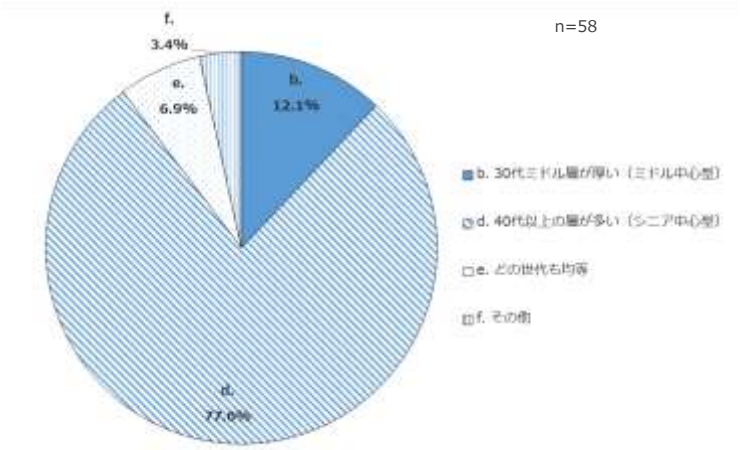
3.3.2. 橋渡し人材層の配置状況と課題

サイバーセキュリティへの対応のため、58.6%の企業は経営層と実務者層をつなぐ「橋渡し人材層」を配置している。



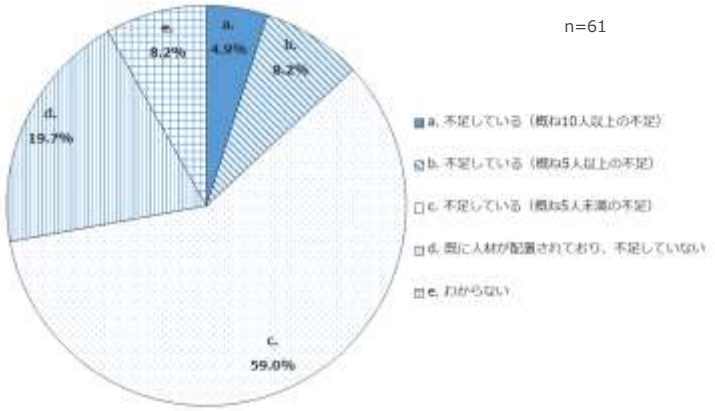
【図表 3-8】 橋渡し人材層（経営・企画・セキュリティ統括部門）の配置

橋渡し人材層は、サイバーセキュリティの知識だけではなく、企業が進める事業等の知識も必要としており、40 代以上の年齢層が多い企業が 77.6%である。



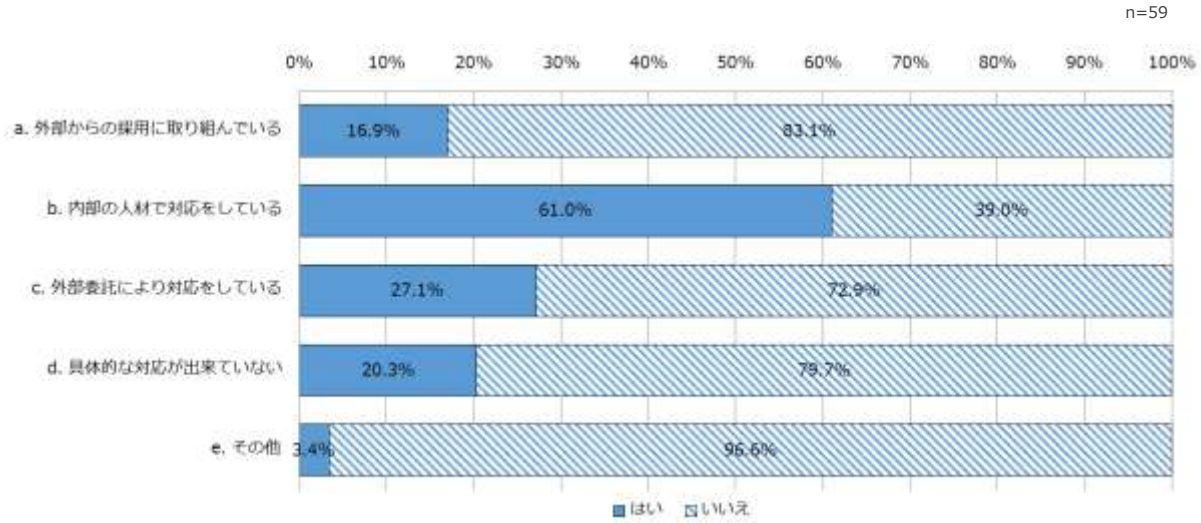
【図表 3-9】 橋渡し人材層（経営・企画・セキュリティ統括部門）の年齢層

しかし、72.1%の企業は橋渡し人材層が不足していると回答しており、59.0%の企業が 5 人未満の不足である。



【図表 3-10】 橋渡し人材層（経営・企画・セキュリティ統括部門）の不足

人材不足への対応は、61%の企業が内部の人材への教育や部門の異動等を活用している。



【図表 3-11】 橋渡し人材層（経営・企画・セキュリティ統括部門）不足への対応

【考 察】

約 6 割の企業で橋渡し人材層を配置しているが、その内、約 7 割の企業で橋渡し人材が不足しており、8 割弱の企業が 40 代以上の層（シニア中心型）で構成されている。業務経験が豊富な人材を橋渡し人材層として位置づけている可能性がある。

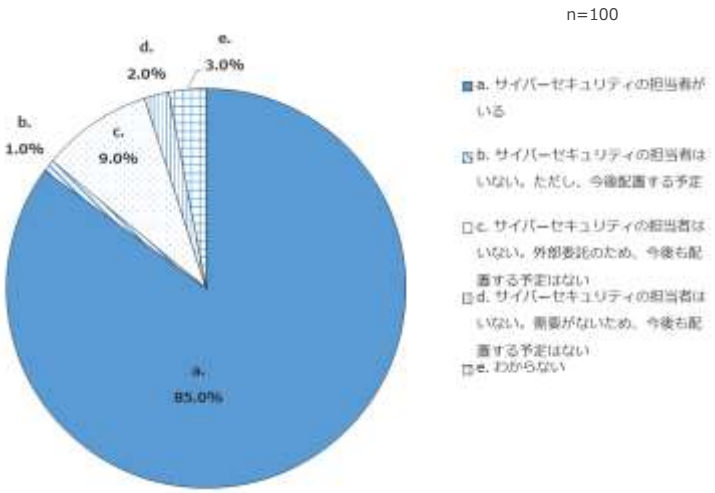
3.3.3. 企業内の様々な部門のサイバーセキュリティ人材（組織面について）

(1). 情報システム部門

事業で攻めるためのサイバーセキュリティは、78.1%の企業において情報システム部門が担っている。

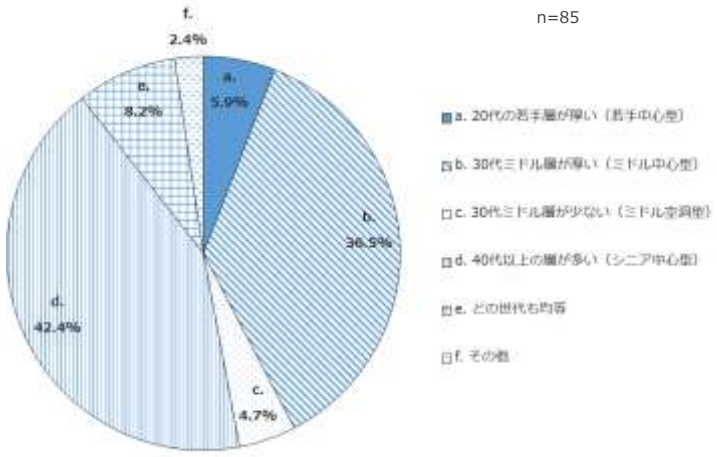
【図表 3-12】 事業で攻めるためのサイバーセキュリティを担う組織

また、85.0%の企業が情報システム部門にサイバーセキュリティの担当者がいると回答している。



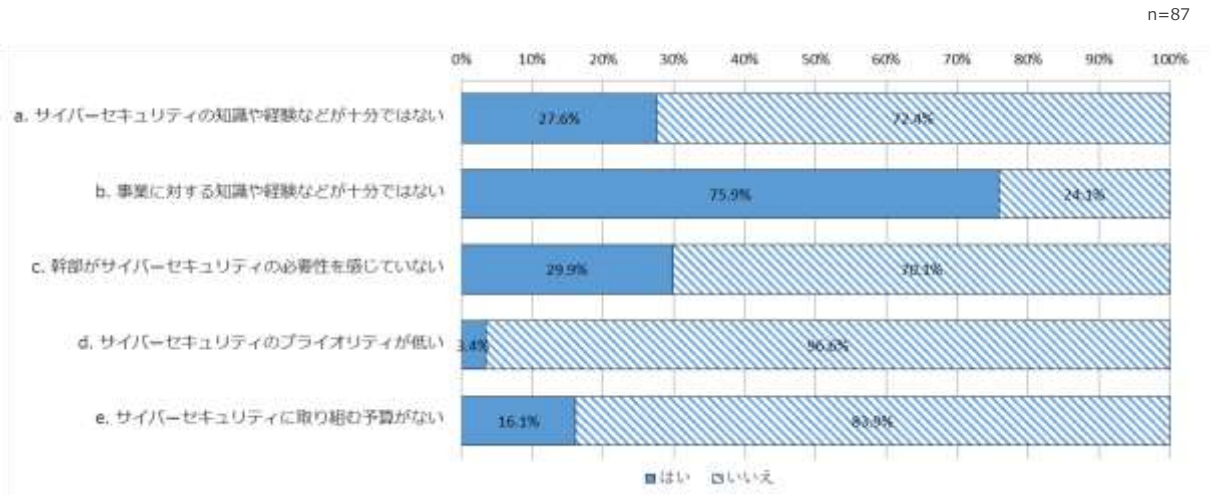
【図表 3-13】 情報システム部門（実務者層）におけるサイバーセキュリティ人材の配置状況

また、情報システム部門では、20 代、30 代ミドル層で構成される企業が 42.4%、40 代以上の年齢で構成されている企業が 42.4%と年齢の分布が分かれている。



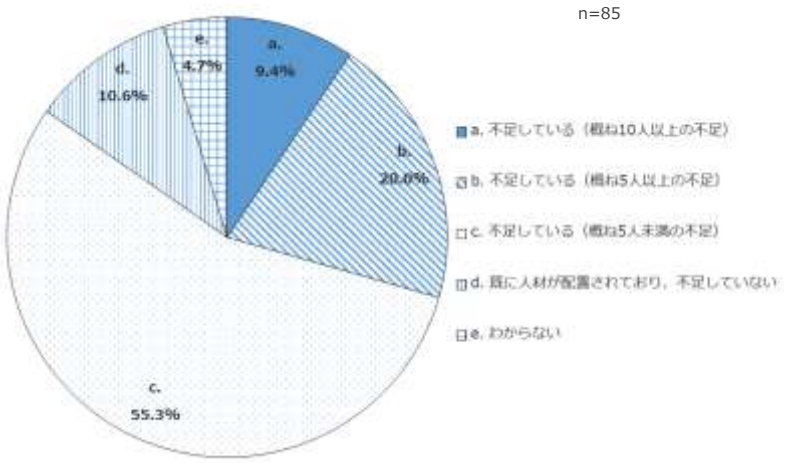
【図表 3-14】 情報システム部門（実務者層）におけるサイバーセキュリティ人材の年齢構成

このような状況において、事業戦略として IT を利活用するためには事業に対する知識や経験が十分ではない企業が 75.9%である。



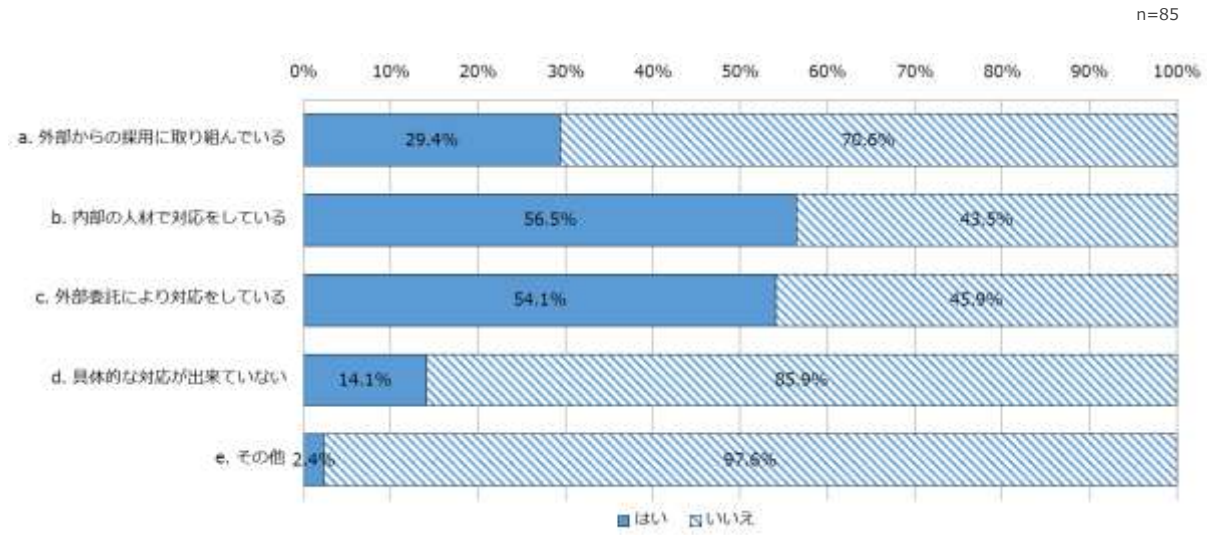
【図表 3-15】情報システム部門における事業戦略として IT を利活用する際の課題

また、情報システム部門のサイバーセキュリティ人材についても 84.7%の企業が不足と回答しており、55.3%の企業が 5 人未満の不足である。



【図表 3-16】情報システム部門におけるサイバーセキュリティ人材の不足

情報システム部門の人材不足に対する対応状況をみると、56.5%の企業が内部の人材で対応しており、54.1%の企業では外部委託も活用して補っている。



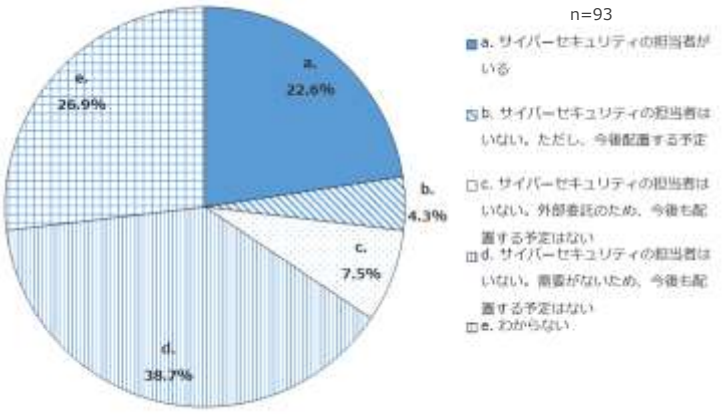
【図表 3-17】情報システム部門における人材不足への対応

【考 察】

サイバーセキュリティの取組は、約 8 割の企業において情報システム部門が担っているが、IT を利活用して新たなビジネスを創造する際に、同部門が抱える課題として、事業に対する知識や経験の不足を挙げる企業が多く、情報システム部門が企業内の幅広い組織におけるサイバーセキュリティに対応できていない可能性がある。

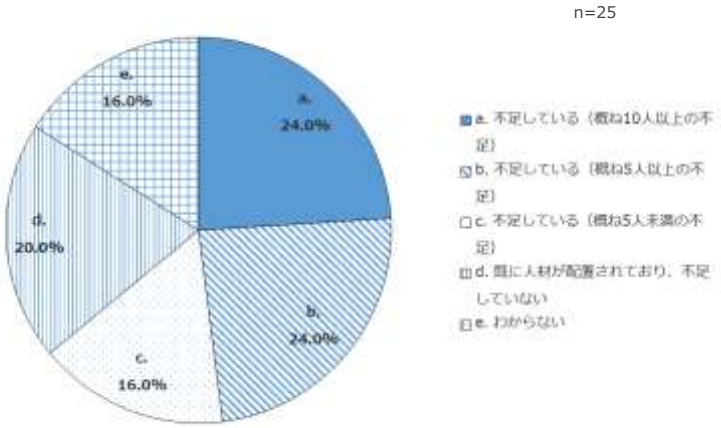
(2). 事業部門

IT を利活用して新しい価値を創造するような新規事業を立ち上げる場合は、事業部門にサイバーセキュリティの知識を持った人材が必要となるが、担当者がいる、あるいは今後配置する予定と回答した企業は全体の 26.9%である。



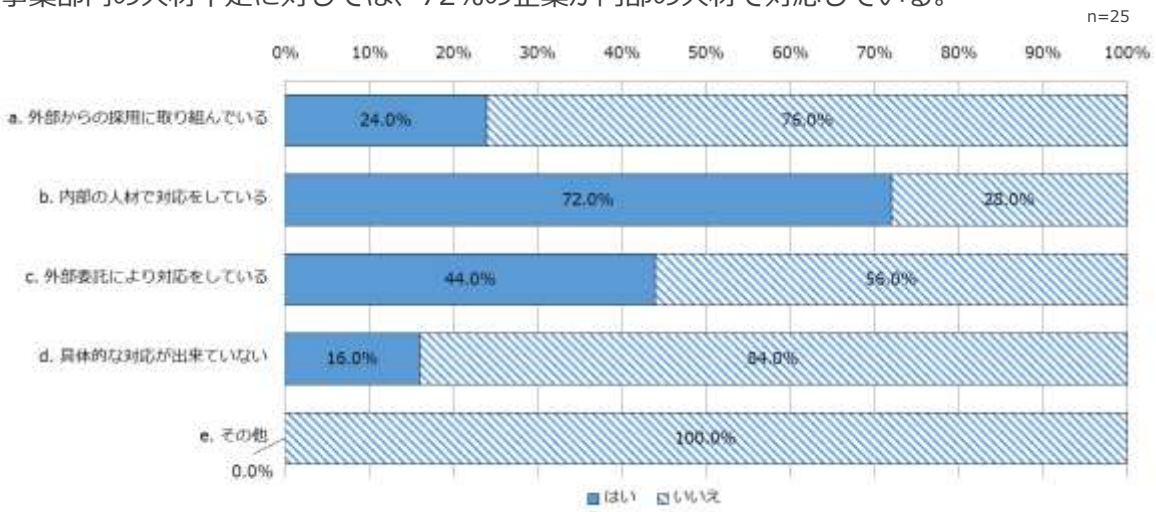
【図表 3-18】事業部門におけるサイバーセキュリティ人材

また、事業部門におけるサイバーセキュリティ人材の不足人数は、概ね 10 人以上の不足、概ね 5 人以上の不足がそれぞれ 24%である。



【図表 3-19】事業部門におけるサイバーセキュリティ人材の不足

事業部門の人材不足に対しては、72%の企業が内部の人材で対応している。



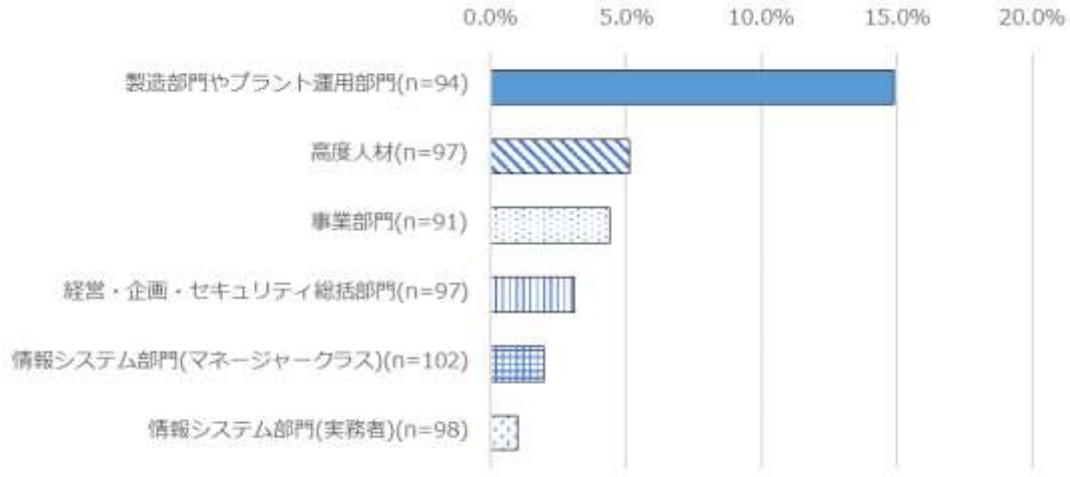
【図表 3-20】事業部門における人材不足の対応

【考 察】

事業部門におけるサイバーセキュリティ人材については、既に配置あるいは今後配置予定とする企業は約 3 割である。しかし、事業部門におけるサイバーセキュリティ人材の不足人数は、情報システム部門と比較して多い。また、不足への対応には内部の人材で対応する傾向があり、事業部門の人材がサイバーセキュリティの知識や経験の素養を身に付けることが課題となっている可能性がある。

(3). その他部門

現在は配置していないが、今後サイバーセキュリティ人材を配置する予定があると回答した部門の内、最も割合が多いのが、製造部門やプラント運用部門であり、約 15%である。



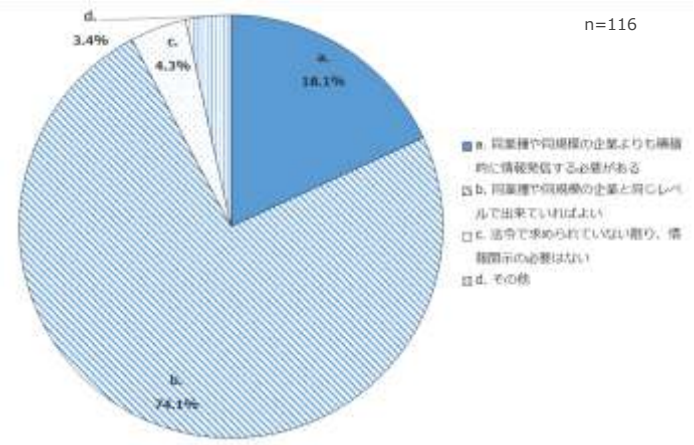
【図表 3-21】現在は配置していないが今後サイバーセキュリティ人材を配置する予定の部門

【考 察】

製造やプラント運用以外の部門では、今後、サイバーセキュリティ人材の配置を予定する企業が 1 割弱だが、製造部門やプラント運用部門では 2 割弱あり、制御システムへのセキュリティ対応ニーズが高まっている可能性がある。

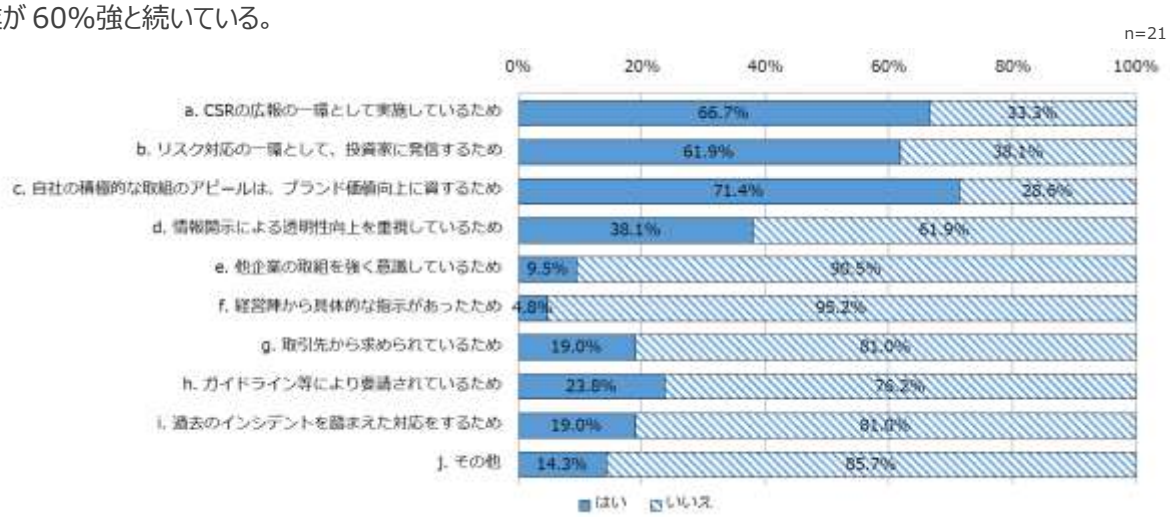
3.3.4. サイバーセキュリティに関する情報発信の考え方

サイバーセキュリティに関する情報発信については、他の企業と同じレベルでできていればよいと考える企業が 74.1%であり、他企業よりも積極的に情報発信をする必要があると考えている企業は 18.1%である。



【図表 3-22】サイバーセキュリティに関する情報発信の姿勢

積極的な情報発信をする必要があると考えている 18.1%の企業の内、積極的な情報発信はブランド価値向上に資すると回答した企業が 71.4%と高く、次に CSR 広報の一つやリスク対応の一つとして実施していると回答した企業が 60%強と続いている。



【図表 3-23】積極的に情報発信を行う理由

【考 察】

情報発信は同業種や同規模の企業と同レベルでできていればよいと考える企業が約 8 割であり、約 2 割の積極的な情報発信に関心のある企業は、サイバーセキュリティへの取組を発信することでブランド価値向上に資すると考えている。

4章. 調査結果の双方向分析

4.1. 目的

サイバーセキュリティの確保には、経営層の意識改革による対策の推進やサイバーセキュリティ技術を担う人材の育成が必要であり、「需要」と「供給」を相応させて、好循環を形成することが求められている。

本調査では、「第 2 章 サイバーセキュリティ対策に係る情報発信内容の調査」及び「第 3 章 アンケート調査」の調査結果をクロス集計し、以下の観点から需要と供給の関係を分析するとともに、現在の進捗について明らかにすることを目的としている。

有価証券報告書については、アンケート調査結果と以下の観点からサイバーセキュリティに対する取組姿勢や姿勢がもたらす効果、抱える課題等について明らかにする。

【有価証券報告書とアンケート調査結果の分析】

① 経営層の関与とサイバーセキュリティへの取組意識(投資・ブランド価値としての位置づけ)
② サイバーセキュリティに取り組む人材層の明確化・育成と経営層の関与
③ サイバーセキュリティに取り組む人材層の明確化・育成とキャリアパスの設定
④ 情報開示している企業の取組意識
⑤ 経営層の関与と企業の情報開示状況
⑥ サイバーセキュリティに取り組む上での法規制の必要性

「その他開示資料」については、第 2 章の結果を基に以下の観点から、サイバーセキュリティに関する情報発信をしている企業の特徴を明らかにする。

【その他開示資料とアンケート調査結果の分析】

① サステナビリティレポートと CSR 報告書に記載している企業の特徴
② コーポレート・ガバナンス報告書にてサイバーセキュリティについて記載している企業の特徴

4.2. 分析対象と分析方法

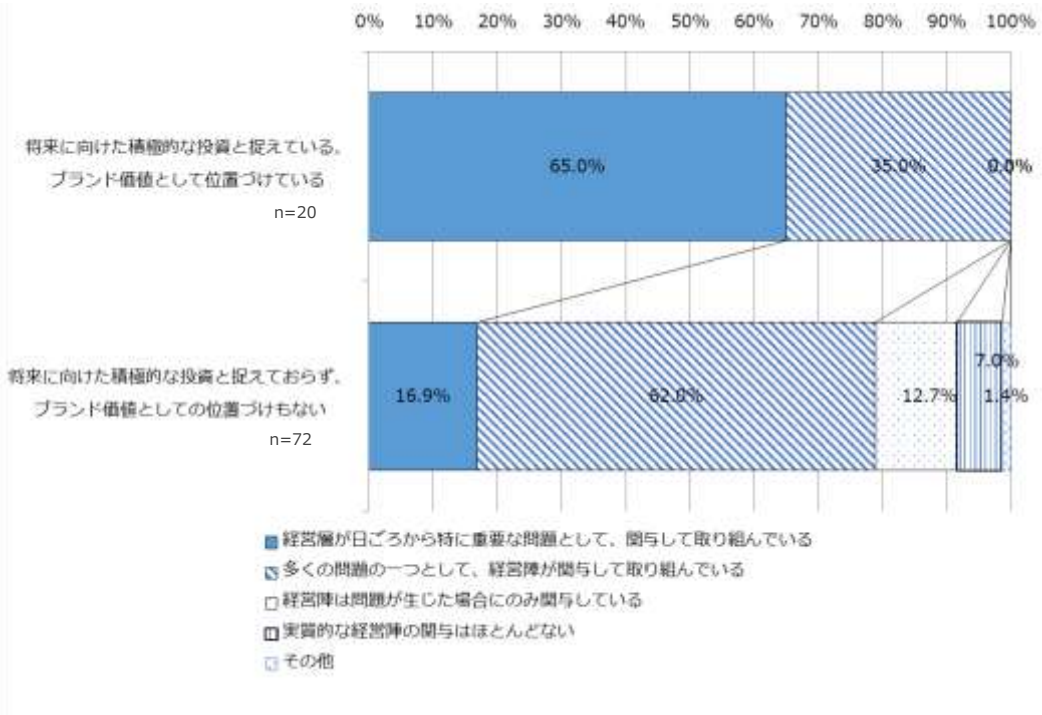
第 2 章「サイバーセキュリティ対策に係る情報発信内容の調査」及び第 3 章「アンケート調査」の調査結果に対してクロス集計を行った。

4.3. 分析結果

4.3.1. 需要面

(1). 経営層の関与とサイバーセキュリティへの取組意識(投資・ブランド価値としての位置づけ)

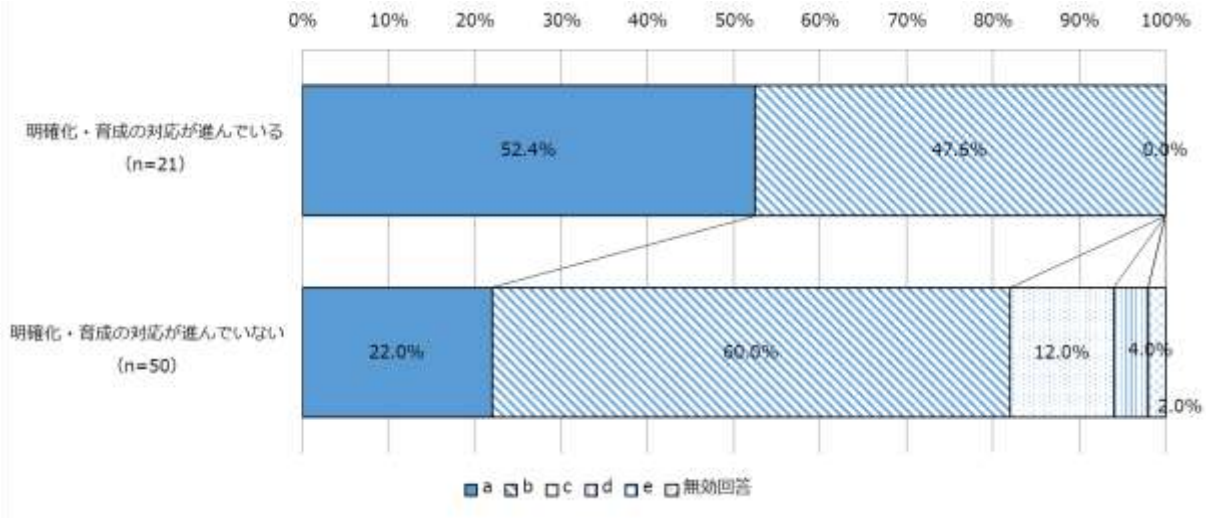
サイバーセキュリティを将来に向けた積極的な投資やブランド価値として捉えている企業では、65.0%の経営層が日ごろから重要な問題として取り組んでおり、35.0%の企業が多くの問題の一つとして取り組んでいる。



【図表 4-1】サイバーセキュリティの取組と経営層の関与

(2). サイバーセキュリティに取り組む人材像の明確化・育成と経営層の関与

サイバーセキュリティに取り組む人材像の明確化・育成が進んでいる企業においては、52.4%の企業において経営層が日ごろから特に重要な問題として取り組んでいる。

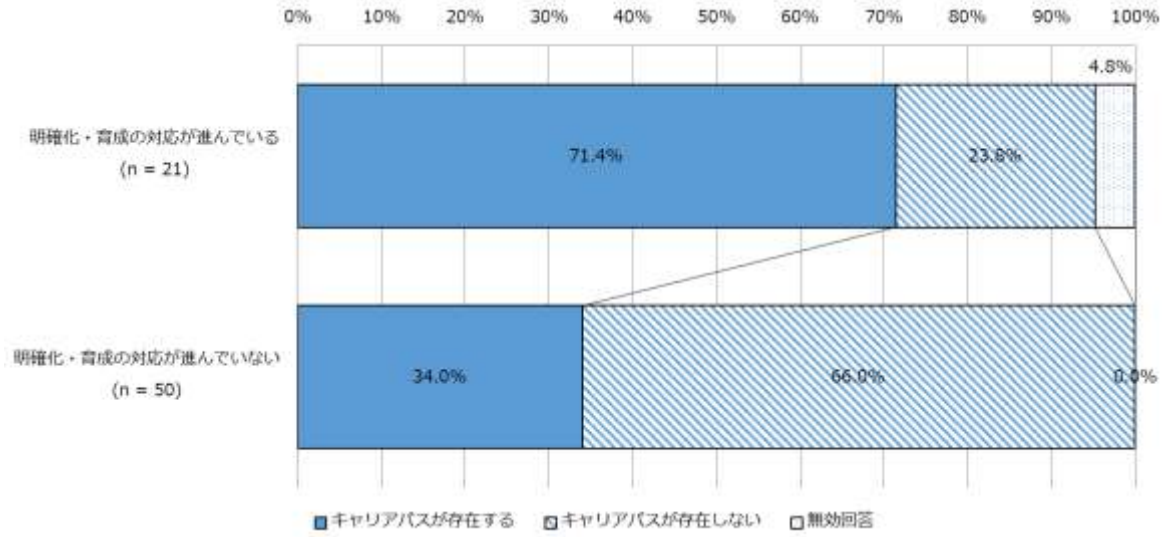


a. 経営層が日ごろから特に重要な問題として、関与して取り組んでいる
b. 多くの問題の一つとして、経営層が関与して取り組んでいる
c. 経営層は、問題が生じた場合にのみ関与している
d. 実質的な経営層の関与はほとんどない
e. その他

【図表 4-2】サイバーセキュリティに取り組む人材像の明確化・育成と経営層の関与

(3). サイバーセキュリティに取り組む人材像の明確化・育成とキャリアパスの設定

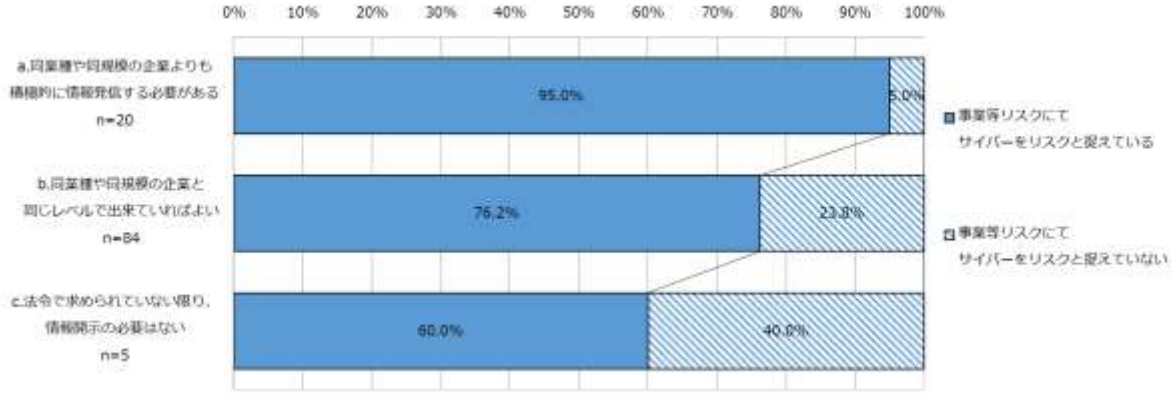
サイバーセキュリティに取り組む人材像の明確化・育成が進んでいる企業は、キャリアパスが存在する企業が71.4%、人材像の明確化・育成が進んでいない企業では、キャリアパスが存在する企業が 34.0%である。



【図表 4-3】サイバーセキュリティに取り組む人材像の明確化・育成とキャリアパスの設定

(4). 情報開示している企業の取組意識

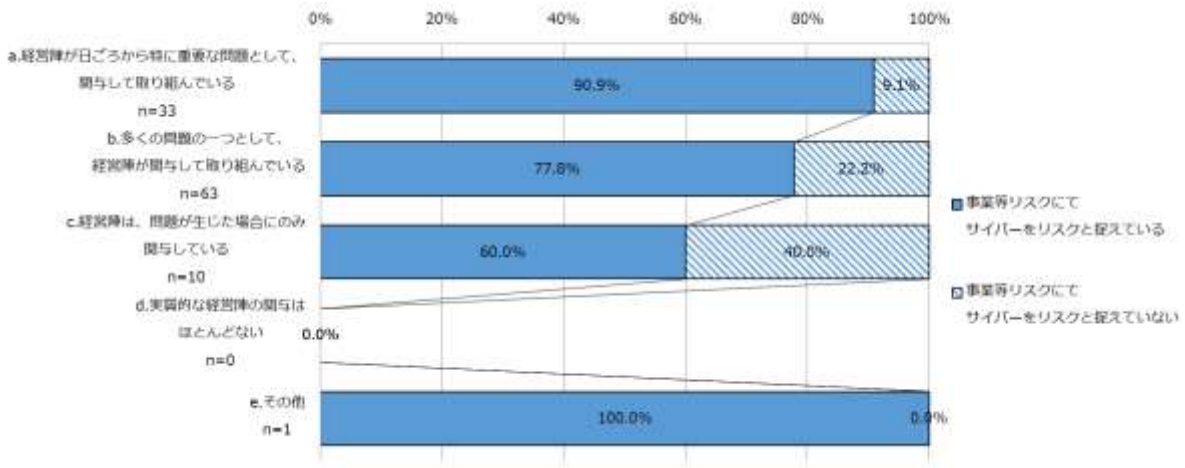
同業種や同規模の企業よりも積極的に情報発信する必要があるとしている企業では有価証券報告書での事業等のリスクにおいてサイバーセキュリティをリスクと捉えている企業が多く 95.0%、同業種や同規模と同じレベルでできていればよい企業では 76.2%、法令で求められていない限り、情報開示の必要はない企業では 60.0%である。



【図表 4-4】情報発信に係る方向性と有価証券報告書の記載状況

(5). 経営層の関与と企業の情報開示状況

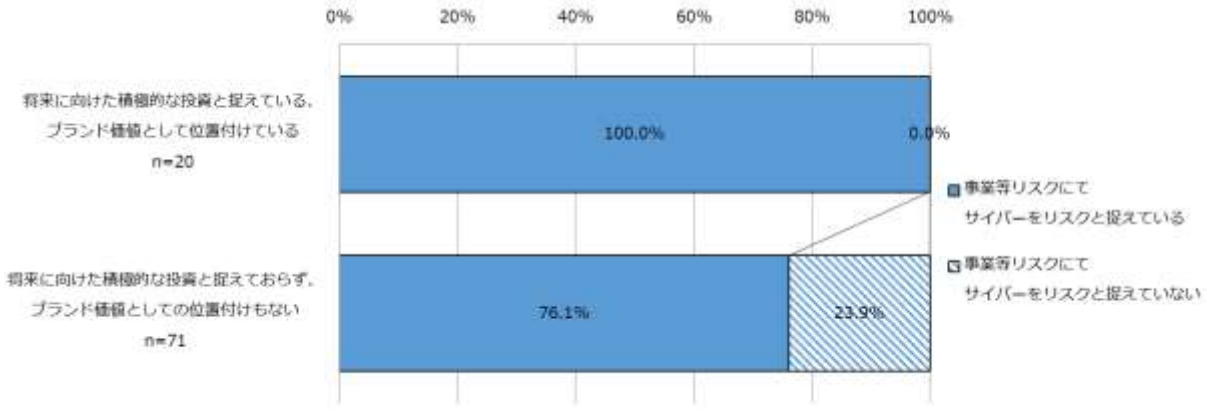
経営層が日ごろから特に重要な問題として、関与して取り組んでいる企業では、有価証券報告書での事業等のリスクにおいてサイバーセキュリティをリスクと捉えている企業が 90.9%、多くの問題の一つとして経営層が関与して取り組んでいる企業では 77.8%、経営層は問題が生じた場合にのみ関与している企業では 60.0%、実質的な経営層の関与はほとんどない企業では 0%である。



【図表 4-5】経営層の関与と有価証券報告書の記載状況

(6). サイバーセキュリティを投資・ブランド価値と捉えている企業の情報開示状況

サイバーセキュリティを将来に向けた積極的な投資として捉えている、ブランド価値として位置づけている企業では、有価証券報告書での事業等のリスクにおいてサイバーをリスクと捉えている企業が 100%、投資やブランド価値として位置づけていない企業では 76.1%である。



【図表 4-6】取組の捉えかた・位置づけと有価証券報告書の記載状況

(7). サイバーセキュリティに取り組む上での法規制の必要性

サイバーセキュリティへの取組を投資と捉えている企業では、国による法規制を不要と捉えている企業が 33%、サイバーセキュリティへの取組を自社のブランドとして捉えている企業では、国による法規制を不要と捉えている企業が 28%である。一方、サイバーセキュリティへの取組を投資と捉えている企業及びサイバーセキュリティへの取組を自社のブランドとして捉えている企業では、国による法規制を不要と捉えている企業が 0%である。

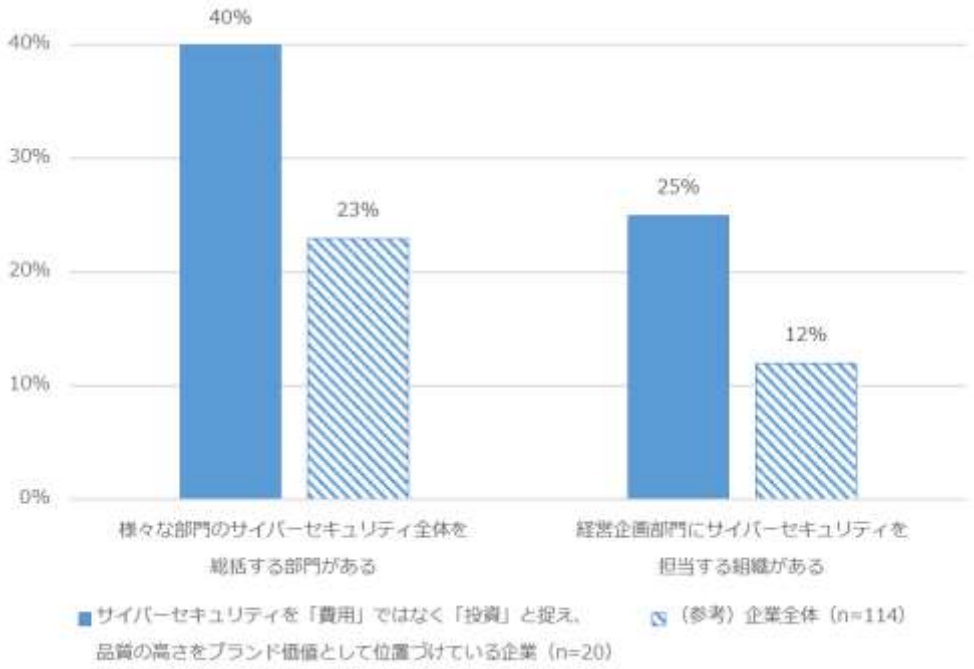
【考 察】

サイバーセキュリティの取組を将来に向けた積極的な投資と捉え、自社のブランド価値として位置づけている企業及びサイバーセキュリティ人材の明確化・育成の対応が進んでいる企業では、サイバーセキュリティを日ごろから特に重要な問題と位置づけ、経営層の関与が進んでいる傾向がある。また、サイバーセキュリティ人材の明確化・育成の対応が進んでいる企業ではキャリアパスが存在しており、人材の需要面の対応が進んでいる傾向にある。さらに、サイバーセキュリティに対する経営層の関与、取組を投資や自社のブランドと捉える意識及び情報発信の必要性を高く認識している企業であるほど、有価証券報告書の「事業等のリスク」においてサイバーセキュリティを記載する傾向がある。

4.3.2. 供給面

(1). サイバーセキュリティへの取組を投資・ブランド価値として捉えている企業の人材配置状況

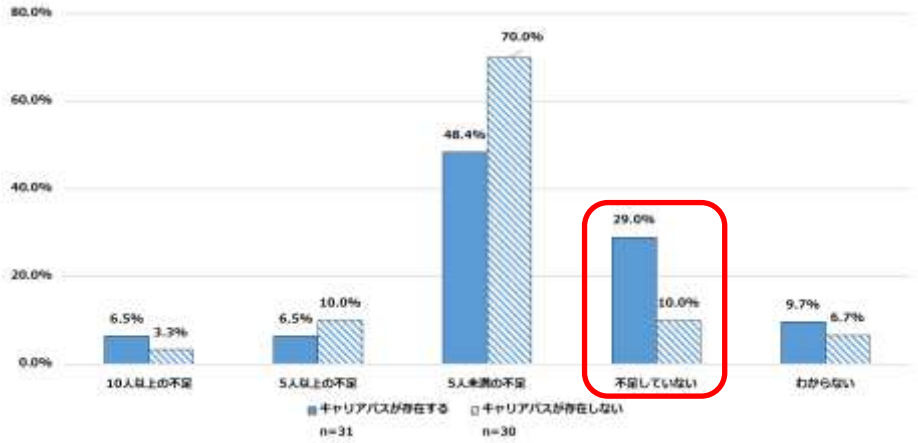
サイバーセキュリティへの取組を、将来に向けた投資あるいはブランド価値として位置づけている企業では、40%の企業において様々な部門のサイバーセキュリティ全体を統括する部門を配置しており、25%の企業において経営企画部門にサイバーセキュリティを担当する組織を配置している。



【図表 4-7】サイバーセキュリティを投資、ブランドと位置づけている企業の統括する部門の配置

(2). キャリアパスを設定している企業の人材の過不足(橋渡し人材層)

橋渡し人材が不足していない企業では、キャリアパスが存在する企業が 29.0%、キャリアパスの存在しない企業が 10.0%である



【図表 4-8】橋渡し人材層の過不足とキャリアパスの設定

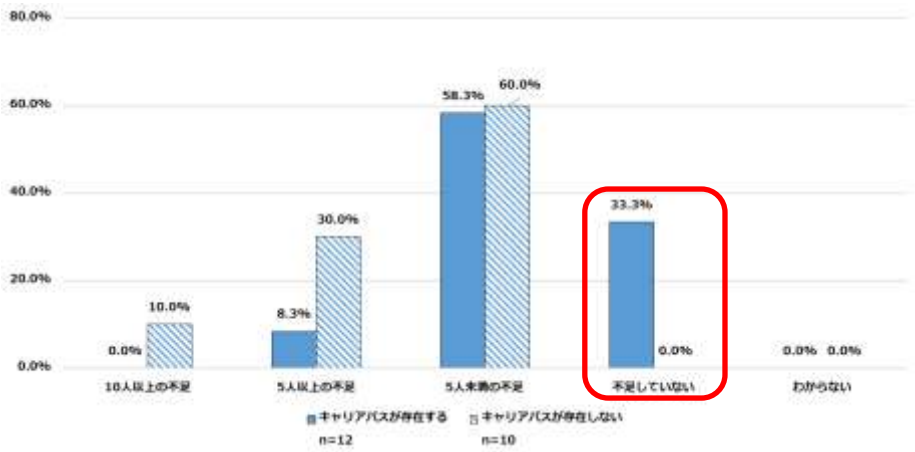
(3). キャリアパスを設定している企業の人材の過不足(事業部門)

事業部門におけるサイバーセキュリティ人材が不足していない企業では、キャリアパスが存在する企業が 28.6%、キャリアパスの存在しない企業が 9.1%である。

【図表 4-9】事業部門における人材の過不足とキャリアパスの設定

(4). キャリアパスを設定している企業の人材の過不足(高度なセキュリティ人材)

高度なセキュリティ人材が不足していない企業では、キャリアパスの存在する企業が 33.3%、キャリアパスが存在しない企業が 0.0%である。



【図表 4-10】高度なセキュリティ人材の過不足とキャリアパスの設定

【考 察】

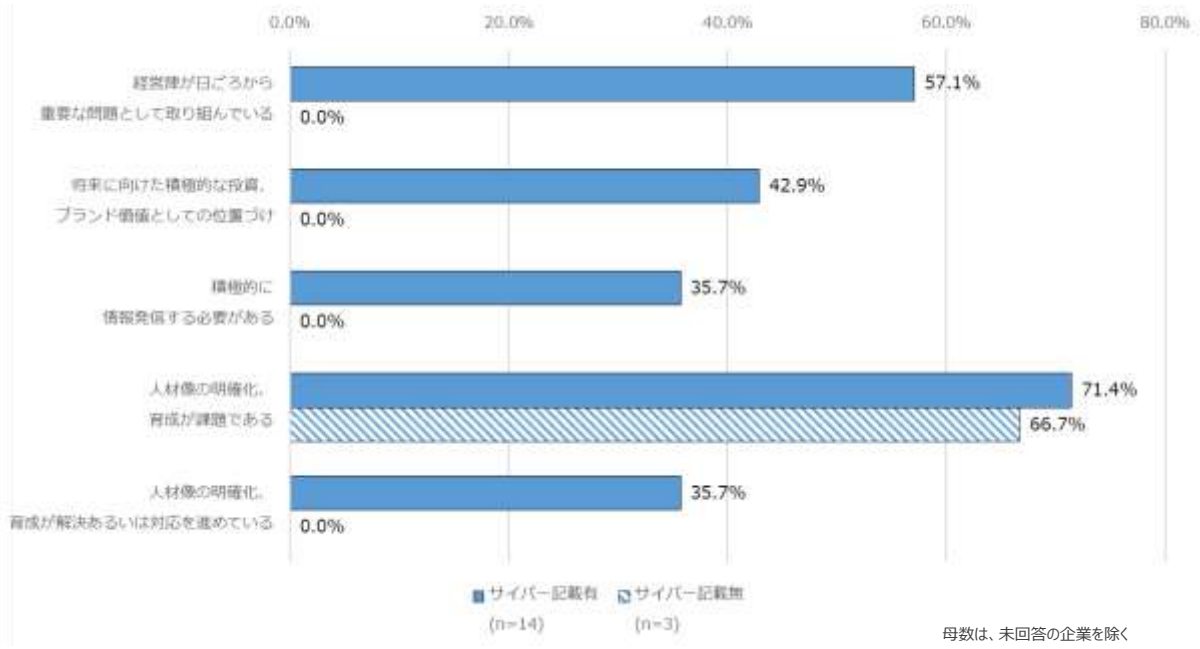
サイバーセキュリティへの取組を費用ではなく投資と捉え、サイバーセキュリティ品質の高さを自社のブランド価値の向上に資すると考えている企業では、企業全体と比較して、様々な部門のサイバーセキュリティ全体を統括する部門及び経営企画部門にサイバーセキュリティを担当する組織を配置する傾向がある。また、サイバーセキュリティ人材のキャリアパスを設定していない企業では、橋渡し人材層、事業部門におけるセキュリティ人材、高度なセキュリティ人材において人材が不足している傾向がある。

4.3.3. その他開示資料とアンケート結果による双方向の分析

(1). サステナビリティレポートへサイバーセキュリティについて記載している企業の特徴

サステナビリティレポートへサイバーセキュリティに関する内容を記載している企業では、経営層が日ごろから重要な課題として取り組んでおり、積極的な投資やブランド価値としての位置づけ、積極的に情報発信する必要があると回答している。また、資料への記載状況に関わらず人材の明確化・育成を課題と感じているが、資料へ記載している企業では、人材像の明確化・育成について解決あるいは対応が進んでいる。

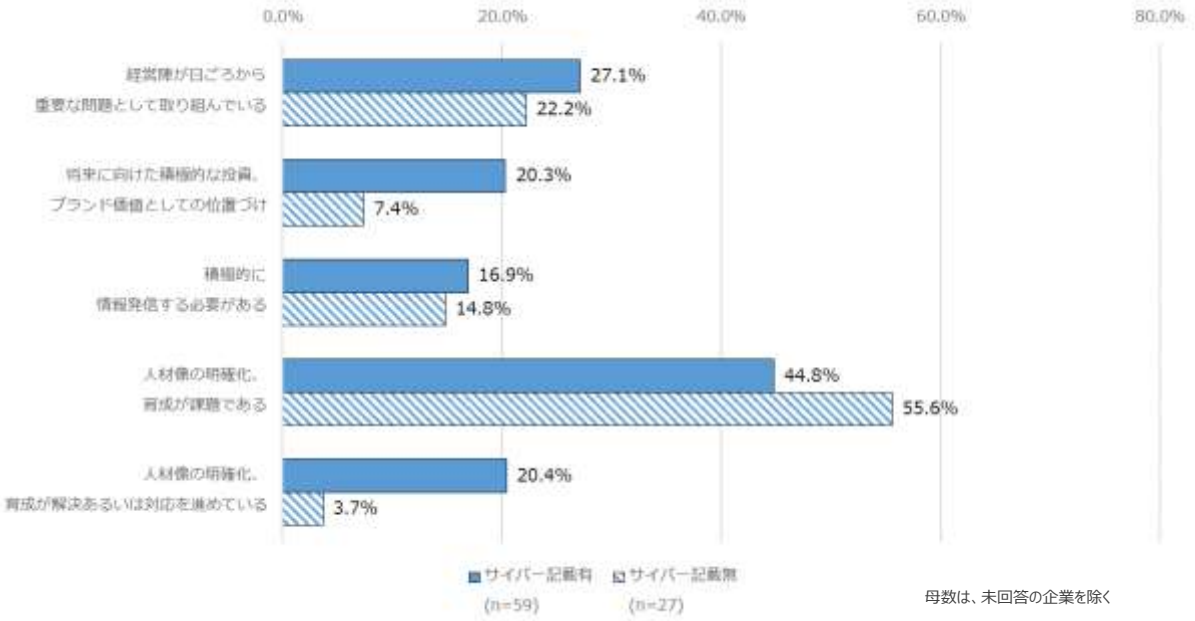
※　グラフは「サイバー記載有」の母数が 14、「サイバー記載無」の母数が 3 と少ないため注意が必要



【図表 4-11】サステナビリティレポートに記載している企業の特徴

(2). CSR 報告書へサイバーセキュリティについて記載している企業の特徴

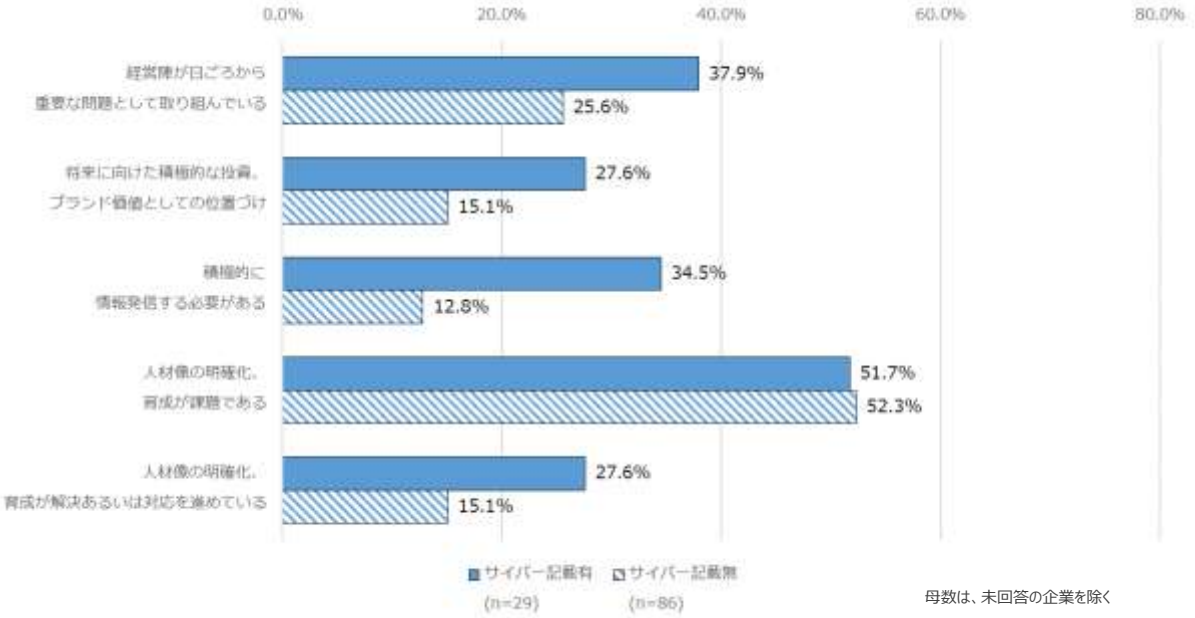
CSR 報告書にサイバーセキュリティに関する内容を記載している企業では、経営層が日ごろから重要な課題として取り組んでおり、積極的な投資やブランド価値としての位置づけ、積極的に情報発信する必要があると回答する傾向がみられる。また、CSR 報告書への記載状況に関わらず人材の明確化・育成を課題と感じているが、CSR 報告書に記載している企業では、人材像の明確化・育成が解決あるいは対応が進んでいる傾向がある。



【図表 4-12】CSR 報告書に記載している企業の特徴

(3). コーポレート・ガバナンス報告書へサイバーセキュリティについて記載している企業の特徴

コーポレート・ガバナンス報告書にサイバーセキュリティに関する内容を記載している企業では、経営層が日ごろから重要な課題として取り組んでおり、積極的な投資やブランド価値としての位置づけ、積極的に情報発信する必要があると回答している。また、報告書への記載状況に関わらず人材の明確化・育成を課題と感じているが、報告書へ記載している企業では、人材像の明確化・育成が解決あるいは対応が進んでいる。



【図表 4-13】コーポレート・ガバナンス報告書に記載している企業の特徴

【考 察】

CSR 報告書及びコーポレート・ガバナンス報告書においてサイバーセキュリティに関する自社の取組を情報発信している企業では、情報発信していない企業と比較して経営層が日ごろからサイバーセキュリティを重要な課題として位置づけ、その課題解決に取り組んでおり、積極的な投資やブランド価値としてサイバーセキュリティを位置づけている可能性がある。

5章. 総評

サイバーセキュリティの人材育成において、需要（雇用・キャリアパス等）と供給（教育・訓練等）の好循環の状況を把握するため、企業のサイバーセキュリティに係る課題や取組状況について調査・分析を行った。結果として、サイバーセキュリティにおける人材育成の需要と供給の好循環は進み始めたものの、いまだ課題が多いと考えられる。

人材の需要では、経営層がサイバーセキュリティをやむを得ない費用ではなく投資と捉え、高いレベルのセキュリティ品質の実現が自社のブランド価値の向上につながると考えている企業は、約 3 割にすぎない。しかし、その約 3 割の企業では、そうでない企業と比較して橋渡し人材等の人材像の明確化が進み、人材育成に向けたキャリアパスが確立され、サイバーセキュリティ全体を統括する部門が設置されるなど、体制整備が進んでいる傾向がある。さらに、経営層が日ごろから特に重要な課題としてサイバーセキュリティへ関与している企業では、有価証券報告書等の公開資料を用いた情報発信も積極的に行っている。実務者層だけの問題ではなく、サイバーセキュリティを経営課題として捉える経営層のサイバーセキュリティ意識の高まりが、体制整備や積極的な情報発信等につながり、需要を生み出していると考えられる。

一方、人材の供給に目を向けると、橋渡し人材や情報システム部門・事業部門のサイバーセキュリティ人材を設置している企業の内、橋渡し人材は約 7 割、情報システム部門では 8 割強、事業部門では 6 割強の企業において人材が不足している。そして、サイバーセキュリティ人材には、サイバーセキュリティの素養に加え、事業に必要な知識や経験が求められる。したがって、不足している人材に対して、外部からの採用や外部委託による対応ではなく、事業に必要な知識や経験を持つ社内の人材育成で対応する傾向があり、人材の育成を課題と認識する一因であると考えられる。しかしながら、サイバーセキュリティ人材のキャリアパスを確立している企業（全体の約 3 割）は、そうでない企業と比べ、橋渡し人材、高度なセキュリティ人材及び事業部門におけるサイバーセキュリティ人材を充足している傾向がみられる。

このようにサイバーセキュリティにおける人材育成の「需要」と「供給」の好循環は一部において進展がみられるものの、事業のすそ野の広がりに対して人材の供給が追い付いていないなど、いまだ課題が多い。

今回の調査では、人材の需要を決める上で、経営層のサイバーセキュリティ意識の高まりが非常に重要であり、そのことが自社内のキャリアパスの確立や、サイバーセキュリティ人材の育成、充足につながっていくと考えられることが確認されたといえる。今後、新たな価値の創造という「挑戦」に付随する「責任」としてサイバーセキュリティに取り組むとの認識に立ち、経営層は自ら意識改革に努めて様々な課題に取り組み、サイバーセキュリティにおける需要（雇用・キャリアパス等）と供給（教育・訓練等）の好循環を生み出すことが期待される。

以 上

6章. 資料編

6.1. 日経 225 業種の大分類及び中分類

平成 29 年度 2 月 1 日現在

大分類	中分類	企業数
技術 (58)	医薬品	8
	電気機器	29
	自動車	10
	精密機器	5
	通信	6
金融 (21)	銀行	11
	その他金融	1
	証券	3
	保険	6
消費 (30)	水産	2
	食品	11
	小売業	8
	サービス	9
素材 (61)	鉱業	1
	繊維	4
	パルプ・紙	3
	化学	17
	石油	2
	ゴム	2
	窯業	8
	鉄鋼	5
	非鉄・金属	12
	商社	7
資本財・その他 (35)	建設	9
	機械	16
	造船	2
	輸送用機器	0
	その他製造	3
	不動産	5
運輸・公共 (20)	鉄道・バス	8
	陸運	2
	海運	3
	空運	1
	倉庫	1
	電力	3
	ガス	2

【図表 6-1】日経 225 業種の大分類及び中分類

6.2. 有価証券報告書における業種別サイバーセキュリティ情報開示状況

日経業種分類				開示企業数	開示企業%	
大分野	大分野社数	中分野	中分野社数		中分野	大分野
A 技術	58	01 医薬品	8	5	62.5%	74.1%
		02 電気機器	29	22	75.9%	
		03 自動車	10	7	70.0%	
		04 精密機器	5	3	60.0%	
		05 通信	6	6	100.0%	
B 金融	21	06 銀行	11	11	100.0%	100.0%
		07 その他金融	1	1	100.0%	
		08 証券	3	3	100.0%	
		09 保険	6	6	100.0%	
C 消費	31	10 水産	3	1	33.3%	87.1%
		11 食品	11	10	90.9%	
		12 小売業	8	8	100.0%	
		13 サービス	9	8	88.9%	
D 素材	66	14 鉱業	1	0	0.0%	42.4%
		15 繊維	5	1	20.0%	
		16 パルプ・紙	5	0	0.0%	
		17 化学	18	7	38.9%	
		18 石油	2	2	100.0%	
		19 ゴム	2	1	50.0%	
		20 窯業	9	3	33.3%	
		21 鉄鋼	5	1	20.0%	
		22 非鉄・金属	12	7	58.3%	
		23 商社	7	6	85.7%	
E 資本財・その他	36	24 建設	9	5	55.6%	52.8%
		25 機械	16	8	50.0%	
		26 造船	2	2	100.0%	
		27 その他製造	3	3	100.0%	
		28 不動産	6	1	16.7%	
F 運輸・公共	20	29 鉄道・バス	8	8	100.0%	90.0%
		30 陸運	2	2	100.0%	
		31 海運	3	1	33.3%	
		32 空運	1	1	100.0%	
		33 倉庫	1	1	100.0%	
		34 電力	3	3	100.0%	
		35 ガス	2	2	100.0%	
合計	232		232	156		

【図表 6-2】業種別サイバーセキュリティ情報開示状況

6.3. 有価証券報告書における業種別サイバーセキュリティ情報開示状況

※ A:H26 or H27 に新たに開示、B:H26 or H27 に記載内容の変化あり、C:H21～H25 で記載内容の変化あり（H26 or H27 は変化なし）、D:H22 年以降に途中開示後変化なし、E:7 年同一、F:開示なし、-:H27 有価証券報告書なし

業種				開示状況別社数							開示状況別 %							情報開示企業総数（A＋B＋C+D+E）	中分野別開示率（A＋B＋C+D+E）	大分野別開示率（A＋B＋C+D+E）
大分野	社数	中分野	社数	A	B	C	D	E	F	-	A	B	C	D	E	F	-			
A 技術	58	01 医薬品	8	3	0	0	0	2	3	0	38%	0%	0%	0%	25%	38%	0%	5	63%	74.1%
		02 電気機器	29	2	10	2	2	6	7	0	7%	34%	7%	7%	21%	24%	0%	22	76%	
		03 自動車	10	2	2	1	2	0	3	0	20%	20%	10%	20%	0%	30%	0%	7	70%	
		04 精密機器	5	0	1	0	1	1	2	0	0%	20%	0%	20%	20%	40%	0%	3	60%	
		05 通信	6	0	5	1	0	0	0	0	0%	**83%**	17%	0%	0%	0%	0%	6	**100%**	
B 金融	21	06 銀行	11	0	7	1	0	3	0	1	0%	64%	9%	0%	27%	0%	9%	11	**100%**	**100.0%**
		07 その他金融	1	0	0	0	0	1	0	0	0%	0%	0%	0%	**100%**	0%	0%	1	**100%**	
		08 証券	3	0	1	1	0	1	0	0	0%	33%	33%	0%	33%	0%	0%	3	**100%**	
		09 保険	6	0	6	0	0	0	0	0	0%	**100%**	0%	0%	0%	0%	0%	6	**100%**	
C 消費	31	10 水産	3	0	0	0	0	1	2	0	0%	0%	0%	0%	33%	67%	0%	1	33%	**87.1%**
		11 食品	11	0	2	1	1	6	1	0	0%	18%	9%	9%	55%	9%	0%	10	**91%**	
		12 小売業	8	0	1	4	0	3	0	1	0%	13%	50%	0%	38%	0%	13%	8	**100%**	
		13 サービス	9	1	3	3	0	1	1	0	11%	33%	33%	0%	11%	11%	0%	8	**89%**	
D 素材	66	14 鉱業	1	0	0	0	0	0	1	0	0%	0%	0%	0%	0%	**100%**	0%	0	0%	42.4%
		15 繊維	5	1	0	0	0	0	4	0	20%	0%	0%	0%	0%	**80%**	0%	1	20%	
		16 パルプ･紙	5	0	0	0	0	0	5	0	0%	0%	0%	0%	0%	**100%**	0%	0	0%	
		17 化学	18	2	2	1	2	0	11	0	11%	11%	6%	11%	0%	61%	0%	7	39%	
		18 石油	2	0	0	0	0	2	0	0	0%	0%	0%	0%	**100%**	0%	0%	2	**100%**	
		19 ゴム	2	0	1	0	0	0	1	0	0%	50%	0%	0%	0%	50%	0%	1	50%	
		20 窯業	9	0	1	2	0	0	6	0	0%	11%	22%	0%	0%	67%	0%	3	33%	
		21 鉄鋼	5	1	0	0	0	0	4	0	20%	0%	0%	0%	0%	**80%**	0%	1	20%	
		22 非鉄･金属	12	2	1	0	0	4	5	0	17%	8%	0%	0%	33%	42%	0%	7	58%	
		23 商社	7	1	2	1	0	2	1	0	14%	29%	14%	0%	29%	14%	0%	6	**86%**	
E 資本財･その他	36	24 建設	9	0	2	0	0	3	4	0	0%	22%	0%	0%	33%	44%	0%	5	56%	52.8%
		25 機械	16	0	3	0	0	5	8	0	0%	19%	0%	0%	31%	50%	0%	8	50%	
		26 造船	2	0	1	0	1	0	0	0	0%	50%	0%	50%	0%	0%	0%	2	**100%**	
		27 その他製造	3	0	1	1	0	1	0	0	0%	33%	33%	0%	33%	0%	0%	3	**100%**	
		28 不動産	6	0	0	1	0	0	5	1	0%	0%	17%	0%	0%	**83%**	17%	1	17%	
F 運輸･公共	20	29 鉄道･バス	8	1	1	3	0	3	0	0	13%	13%	38%	0%	38%	0%	0%	8	**100%**	**90.0%**
		30 陸運	2	0	2	0	0	0	0	0	0%	**100%**	0%	0%	0%	0%	0%	2	**100%**	
		31 海運	3	0	1	0	0	0	2	0	0%	33%	0%	0%	0%	67%	0%	1	33%	
		32 空運	1	0	1	0	0	0	0	0	0%	**100%**	0%	0%	0%	0%	0%	1	**100%**	
		33 倉庫	1	0	1	0	0	0	0	0	0%	**100%**	0%	0%	0%	0%	0%	1	**100%**	
		34 電力	3	0	2	0	0	1	0	0	0%	67%	0%	0%	33%	0%	0%	3	**100%**	
		35 ガス	2	0	2	0	0	0	0	0	0%	**100%**	0%	0%	0%	0%	0%	2	**100%**	
総計(大分類)	232	総計(中分類)	232	16	62	23	9	46	76	3	7%	27%	10%	4%	20%	33%	1%	156	67%	
			構成比	6.9%	26.7%	9.9%	3.9%	19.8%	32.8%	1.3%										

【図表 6-3】平成 27 年度 業種別開示状況

6.4. 有価証券報告書における中分類ごとの情報・サイバーセキュリティ記載状況順位

#	A		#	B		#	C		#	D		#	E		#	F	
	中分類	開示率		中分類	開示率		中分類	開示率		中分類	開示率		中分類	開示率		中分類	開示率
1	01 医薬品	37.5%	1	09 保険	100.0%	1	12 小売業	50.0%	1	26 造船	50.0%	1	07 その他金	100.0%	1	14 鉱業	100.0%
2	03 自動車	20.0%	1	30 陸運	100.0%	2	29 鉄道・バ	37.5%	2	03 自動車	20.0%	1	18 石油	100.0%	1	16 パルプ・	100.0%
2	15 繊維	20.0%	1	32 空運	100.0%	3	08 証券	33.3%	2	04 精密機器	20.0%	2	11 食品	54.5%	2	28 不動産	83.3%
2	21 鉄鋼	20.0%	1	33 倉庫	100.0%	3	13 サービス	33.3%	3	17 化学	11.1%	3	12 小売業	37.5%	3	15 繊維	80.0%
3	22 非鉄・金	16.7%	1	35 ガス	100.0%	3	27 その他製	33.3%	4	11 食品	9.1%	3	29 鉄道・バ	37.5%	3	21 鉄鋼	80.0%
4	23 商社	14.3%	2	05 通信	83.3%	4	20 窯業	22.2%	5	02 電気機器	6.9%	4	08 証券	33.3%	4	10 水産	66.7%
5	29 鉄道・バ	12.5%	3	34 電力	66.7%	5	05 通信	16.7%	6	01 医薬品	0.0%	4	10 水産	33.3%	4	20 窯業	66.7%
6	13 サービス	11.1%	4	06 銀行	63.6%	5	28 不動産	16.7%	6	05 通信	0.0%	4	22 非鉄・金	33.3%	4	31 海運	66.7%
6	17 化学	11.1%	5	19 ゴム	50.0%	6	23 商社	14.3%	6	06 銀行	0.0%	4	24 建設	33.3%	5	17 化学	61.1%
7	02 電気機器	6.9%	5	26 造船	50.0%	7	03 自動車	10.0%	6	07 その他金	0.0%	4	27 その他製	33.3%	6	19 ゴム	50.0%
8	04 精密機器	0.0%	6	02 電気機器	34.5%	8	06 銀行	9.1%	6	08 証券	0.0%	4	34 電力	33.3%	6	25 機械	50.0%
8	05 通信	0.0%	7	08 証券	33.3%	8	11 食品	9.1%	6	09 保険	0.0%	5	25 機械	31.3%	7	24 建設	44.4%
8	06 銀行	0.0%	7	13 サービス	33.3%	9	02 電気機器	6.9%	6	10 水産	0.0%	6	23 商社	28.6%	8	22 非鉄・金	41.7%
8	07 その他金	0.0%	7	27 その他製	33.3%	10	17 化学	5.6%	6	12 小売業	0.0%	7	06 銀行	27.3%	9	04 精密機器	40.0%
8	08 証券	0.0%	7	31 海運	33.3%	11	01 医薬品	0.0%	6	13 サービス	0.0%	8	01 医薬品	25.0%	10	01 医薬品	37.5%
8	09 保険	0.0%	8	23 商社	28.6%	11	04 精密機器	0.0%	6	14 鉱業	0.0%	9	02 電気機器	20.7%	11	03 自動車	30.0%
8	10 水産	0.0%	9	24 建設	22.2%	11	07 その他金	0.0%	6	15 繊維	0.0%	10	04 精密機器	20.0%	12	02 電気機器	24.1%
8	11 食品	0.0%	10	03 自動車	20.0%	11	09 保険	0.0%	6	16 パルプ・	0.0%	11	13 サービス	11.1%	13	23 商社	14.3%
8	12 小売業	0.0%	10	04 精密機器	20.0%	11	10 水産	0.0%	6	18 石油	0.0%	12	03 自動車	0.0%	14	13 サービス	11.1%
8	14 鉱業	0.0%	11	25 機械	18.8%	11	14 鉱業	0.0%	6	19 ゴム	0.0%	12	05 通信	0.0%	15	11 食品	9.1%
8	16 パルプ・	0.0%	12	11 食品	18.2%	11	15 繊維	0.0%	6	20 窯業	0.0%	12	09 保険	0.0%	16	05 通信	0.0%
8	18 石油	0.0%	13	12 小売業	12.5%	11	16 パルプ・	0.0%	6	21 鉄鋼	0.0%	12	14 鉱業	0.0%	16	06 銀行	0.0%
8	19 ゴム	0.0%	13	29 鉄道・バ	12.5%	11	18 石油	0.0%	6	22 非鉄・金	0.0%	12	15 繊維	0.0%	16	07 その他金	0.0%
8	20 窯業	0.0%	14	17 化学	11.1%	11	19 ゴム	0.0%	6	23 商社	0.0%	12	16 パルプ・	0.0%	16	08 証券	0.0%
8	24 建設	0.0%	14	20 窯業	11.1%	11	21 鉄鋼	0.0%	6	24 建設	0.0%	12	17 化学	0.0%	16	09 保険	0.0%
8	25 機械	0.0%	15	22 非鉄・金	8.3%	11	22 非鉄・金	0.0%	6	25 機械	0.0%	12	19 ゴム	0.0%	16	12 小売業	0.0%
8	26 造船	0.0%	16	01 医薬品	0.0%	11	24 建設	0.0%	6	27 その他製	0.0%	12	20 窯業	0.0%	16	18 石油	0.0%
8	27 その他製	0.0%	16	07 その他金	0.0%	11	25 機械	0.0%	6	28 不動産	0.0%	12	21 鉄鋼	0.0%	16	26 造船	0.0%
8	28 不動産	0.0%	16	10 水産	0.0%	11	26 造船	0.0%	6	29 鉄道・バ	0.0%	12	26 造船	0.0%	16	27 その他製	0.0%
8	30 陸運	0.0%	16	14 鉱業	0.0%	11	30 陸運	0.0%	6	30 陸運	0.0%	12	28 不動産	0.0%	16	29 鉄道・バ	0.0%
8	31 海運	0.0%	16	15 繊維	0.0%	11	31 海運	0.0%	6	31 海運	0.0%	12	30 陸運	0.0%	16	30 陸運	0.0%
8	32 空運	0.0%	16	16 パルプ・	0.0%	11	32 空運	0.0%	6	32 空運	0.0%	12	31 海運	0.0%	16	32 空運	0.0%
8	33 倉庫	0.0%	16	18 石油	0.0%	11	33 倉庫	0.0%	6	33 倉庫	0.0%	12	32 空運	0.0%	16	33 倉庫	0.0%
8	34 電力	0.0%	16	21 鉄鋼	0.0%	11	34 電力	0.0%	6	34 電力	0.0%	12	33 倉庫	0.0%	16	34 電力	0.0%
8	35 ガス	0.0%	16	28 不動産	0.0%	11	35 ガス	0.0%	6	35 ガス	0.0%	12	35 ガス	0.0%	16	35 ガス	0.0%

A)H26 or H27 に新たに公開　B)H26 or H27 に記載内容の変化あり　C)H21～H25 で記載内容の変化あり（H26 or H27 は変化なし）、D)H22 年以降に途中公開後変化なし　E)7 年同一　F)公開なし

【図表 6-4】有価証券報告書における中分類ごとの情報・サイバーセキュリティ記載状況順位

6.5. その他開示資料における中分類ごとの情報・サイバーセキュリティ記載状況順位

情報セキュリティ報告書

#	中分類	記載比率%
1	02 電気機器	100%
1	05 通信	100%
2	01 医薬品	0%
2	03 自動車	0%
2	04 精密機器	0%
2	06 銀行	0%
2	07 その他金	0%
2	08 証券	0%
2	09 保険	0%
2	10 水産	0%
2	11 食品	0%
2	12 小売業	0%
2	13 サービス	0%
2	14 鉱業	0%
2	15 繊維	0%
2	16 パルプ・	0%
2	17 化学	0%
2	18 石油	0%
2	19 ゴム	0%
2	20 窯業	0%
2	21 鉄鋼	0%
2	22 非鉄・金	0%
2	23 商社	0%
2	24 建設	0%
2	25 機械	0%
2	26 造船	0%
2	27 その他製	0%
2	28 不動産	0%
2	29 鉄道・バ	0%
2	30 陸運	0%
2	31 海運	0%
2	32 空運	0%
2	33 倉庫	0%
2	34 電力	0%
2	35 ガス	0%

情報セキュリティ方針

#	中分類	記載比率%
1	01 医薬品	100%
1	02 電気機器	100%
1	03 自動車	100%
1	04 精密機器	100%
1	05 通信	100%
1	08 証券	100%
1	09 保険	100%
1	10 水産	100%
1	11 食品	100%
1	12 小売業	100%
1	13 サービス	100%
1	14 鉱業	100%
1	15 繊維	100%
1	17 化学	100%
1	18 石油	100%
1	19 ゴム	100%
1	20 窯業	100%
1	21 鉄鋼	100%
1	22 非鉄・金	100%
1	23 商社	100%
1	24 建設	100%
1	25 機械	100%
1	26 造船	100%
1	27 その他製	100%
1	28 不動産	100%
1	29 鉄道・バ	100%
1	30 陸運	100%
1	31 海運	100%
1	32 空運	100%
1	33 倉庫	100%
1	35 ガス	100%
2	06 銀行	0%
2	07 その他金	0%
2	16 パルプ・	0%
2	34 電力	0%

CSR報告書

#	中分類	記載比率%
1	05 通信	100%
1	07 その他金	100%
1	08 証券	100%
1	15 繊維	100%
1	27 その他製	100%
1	31 海運	100%
1	33 倉庫	100%
1	34 電力	100%
1	35 ガス	100%
2	02 電気機器	90%
3	01 医薬品	83%
4	28 不動産	80%
5	17 化学	73%
6	06 銀行	67%
6	13 サービス	67%
6	24 建設	67%
7	04 精密機器	60%
7	09 保険	60%
8	29 鉄道・バ	57%
9	18 石油	50%
9	25 機械	50%
9	26 造船	50%
9	30 陸運	50%
10	22 非鉄・金	45%
11	03 自動車	40%
11	20 窯業	40%
11	21 鉄鋼	40%
12	16 パルプ・	33%
12	23 商社	33%
13	12 小売業	29%
14	11 食品	25%
15	10 水産	0%
15	14 鉱業	0%
15	19 ゴム	0%
15	32 空運	0%

サステナビリティレポート

#	中分類	記載比率%
1	02 電気機器	100%
1	03 自動車	100%
1	05 通信	100%
1	09 保険	100%
1	11 食品	100%
1	13 サービス	100%
1	14 鉱業	100%
1	17 化学	100%
1	18 石油	100%
1	19 ゴム	100%
1	22 非鉄・金	100%
1	23 商社	100%
1	24 建設	100%
2	04 精密機器	50%
2	25 機械	50%
3	01 医薬品	0%
3	06 銀行	0%
3	07 その他金	0%
3	08 証券	0%
3	10 水産	0%
3	12 小売業	0%
3	15 繊維	0%
3	16 パルプ・	0%
3	20 窯業	0%
3	21 鉄鋼	0%
3	26 造船	0%
3	27 その他製	0%
3	28 不動産	0%
3	29 鉄道・バ	0%
3	30 陸運	0%
3	31 海運	0%
3	32 空運	0%
3	33 倉庫	0%
3	34 電力	0%
3	35 ガス	0%

コーポレートガバナンス報告

#	中分類	記載比率%
1	14 鉱業	100%
1	35 ガス	100%
2	05 通信	83%
3	27 その他製	67%
4	13 サービス	56%
5	09 保険	50%
5	18 石油	50%
6	23 商社	43%
7	34 電力	33%
8	25 機械	25%
8	29 鉄道・バ	25%
9	24 建設	22%
10	03 自動車	20%
10	04 精密機器	20%
10	15 繊維	20%
11	06 銀行	18%
11	11 食品	18%
12	02 電気機器	18%
13	17 化学	17%
14	22 非鉄・金	8%
15	01 医薬品	0%
15	07 その他金	0%
15	08 証券	0%
15	10 水産	0%
15	12 小売業	0%
15	16 パルプ・	0%
15	19 ゴム	0%
15	20 窯業	0%
15	21 鉄鋼	0%
15	26 造船	0%
15	28 不動産	0%
15	30 陸運	0%
15	31 海運	0%
15	32 空運	0%
15	33 倉庫	0%

※　平成 27 年度データ

【図表 6-5】その他開示資料における中分類ごとの情報・サイバーセキュリティ記載状況順位

6.6. 有価証券報告書における記載状況

有価証券報告書に記載されている「想定脅威」、「一次被害」、「二次被害」について平成 26 年度調査時のデータと今回調査時のデータを比較した。「情報セキュリティ対策」は、今回新たに調査した内容を記載した。

6.6.1. 想定脅威

サイバー攻撃に関する想定脅威	平成 28 年度(156 社)		平成 25 年度(136 社)	
	記載企業数	割合	記載企業数	割合
コンピュータウイルス	76	49%	69	51%
不正アクセス	49	31%	45	33%
サイバー攻撃・ハッキング	41	26%	35	26%
「予期せぬ」「不測」等の一般的な記載	109	70%	86	63%

【図表 6-6】想定脅威

6.6.2. 一次被害

記載されている一次被害	平成 28 年度(156 社)		平成 25 年度(136 社)	
	記載企業数	割合	記載企業数	割合
個人情報漏えい/流出	124	79%	113	83%
機密情報漏えい/流出	111	71%	105	77%
システム障害	90	58%	85	63%

【図表 6-7】一次被害

6.6.3. 二次被害

記載されている二次被害	平成 28 年度(156 社)		平成 25 年度(136 社)	
	記載企業数	割合	記載企業数	割合
業績への影響	125	80%	113	83%
社会的信用の低下	81	52%	80	59%
財務/財政状況への影響	76	49%	73	54%
訴訟提起/損害賠償責任	65	42%	60	44%

【図表 6-8】二次被害

6.6.4. 情報セキュリティ対策

記載されている情報セキュリティ対策	平成 28 年度(156 社)	
	記載企業数	割合
システム対策などのハード面	83	53%
一般社員（従業員）に対する教育	39	25%
演習・訓練の実施	5	3%
経営層に対する教育	4	3%
専門人材の育成	3	2%
CISO の設置	1	1%
CSIRT の設置	1	1%
その他対策（規程・委員会・内部監査など）	128	82%

【図表 6-9】情報セキュリティ対策

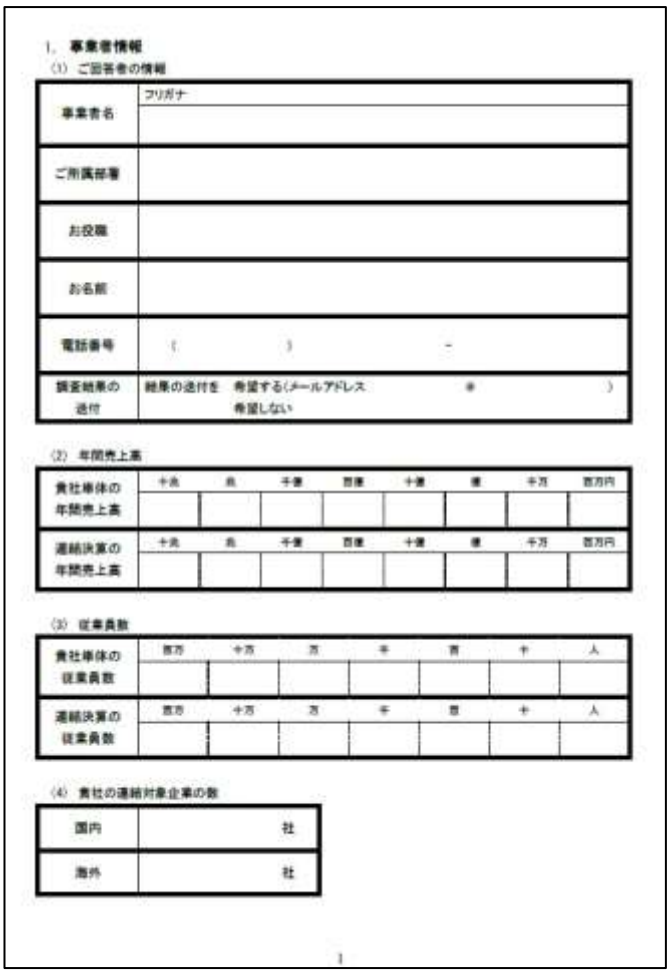
6.7. 送り状及び調査アンケート本文

※詳細は別添資料参照

【送付状】

アンケート調査の協力依頼について

【調査アンケート】



1. 事業者情報

(1) ご回答者の情報

事業者名	フリガナ
ご所属部署	
お役職	
お名前	
電話番号	( ) -
調査結果の送付	結果の送付を 希望する(メールアドレス ※) 希望しない

(2) 年間売上高

	十兆	兆	千億	百億	十億	億	千万	百万円
貴社単体の年間売上高								
連結決算の年間売上高								

(3) 従業員数

	百万	十万	万	千	百	十	人
貴社単体の従業員数							
連結決算の従業員数							

(4) 貴社の連結対象企業の数

国内	社
海外	社

【図表 6-10】送り状及びアンケート本文（抜粋）

6.8. JUAS による業種グループ分類

業種グループ	件数	割合	属する業種
建築・土木	95	8.5	15.建設業
素材製造	227	20.4	1．食料品、飲料・たばこ・飼料製造業、2．繊維工業 、3．パルプ・紙・紙加工品製造業、 4．化学工業、5．石油・石炭・プラスチック製品製造、6．窯業・土石製品製造業 7．鉄鋼業、8．非鉄金属・金属製品製造業
機械器具製造	288	25.8	9．電気機械器具製造業、10．情報通信機械器具製造業 11．輸送用機械器具製造業、 s 12．その他機械器具製造業 13．その他の製造業
商社・流通	169	15.2	22．卸売業、23．小売業
金融	58	5.2	24．金融業・保険業
社会インフラ	102	9.1	16．電気・ガス・熱供給・水道業、17．映像・音声情報制作・放送・通信業、 18．新聞・出版業、20．運輸業・郵便業
サービス	176	15.8	14．農林漁業・同協同組合、鉱業、19．情報サービス業、 20．宿泊、飲食、旅行サービス業 25．医療業、26．教育、学習支援、27．その他の非製造業
全体	1115	100.0	

【図表 6-11】JUAS による業種グループ分類

※　表は、JUAS が公開しているデータを基に新たに作成
http://www.juas.or.jp/servey/it16/it16_ppt.pdf

【問合せ窓口】

ニュートン・コンサルティング株式会社

〒102-0083　東京都千代田区麹町 1-7 相互半蔵門ビルディング 9F

Tel: 03-3239-9209

Fax: 03-5913-9950

Mail: info@newton-consulting.co.jp

Web: http://www.newton-consulting.co.jp/