平成 30 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 31 年 3 月

株式会社エヌ・ティ・ティ・データ経営研究所

目次

エグゼクティブサマリー

相次ぐ攻撃や各種報道によりサイバーセキュリティリスクへの関心が高まっている。的確な対応を行うには、経営層からの発信・社内への周知徹底だけでなく、管理方針の策定や運営態勢の整備、更には人材育成等、多様な取組を行う必要がある。本調査では、日経 225 等の企業を対象として、有価証券報告書及びコーポレートガバナンス報告書の分析を行うことでサイバーセキュリティリスクに関する情報発信内容を調査するとともに、アンケートにより各社のサイバーセキュリティへの取組状況を調査し、両者の相関について総合的な分析を実施した。

日経 225 等企業の情報発信状況については、まず有価証券報告書でのサイバーセキュリティリスク開示率が平成 27 年度以前と同等のペースで増加していることを確認した。また記載の深度も増している。サイバーセキュリティリスクに対する関心・問題意識の高まりとともに、企業がステークホルダーに対し、施策を含め丁寧に情報発信しようとする姿勢が醸成されてきていると考えられる。業種別で見ると、金融、消費、運輸・公共等で記載率が高く、素材、資本財・その他で記載率が低い。

一方、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リスクについて開示を行う企業はまだ少ないものの、平成 28 年度から 29 年度にかけて開示率が大きく高まっていることが判明した。また、記載の深度も増している。これは、リスク情報・非財務情報の開示意欲が、企業において急速に高まっている可能性を示唆している。但し、有価証券報告書において開示率の高い業種が必ずしもコーポレートガバナンス報告書での開示率が高い訳ではない。コーポレートガバナンス報告書は、資本市場をより強く意識したものであり、有価証券報告書と比べると、企業によっては、発信する情報の網羅性よりも投資家にとっての重要性・代表性を重んじている可能性がある。

アンケート調査からは、①サイバーセキュリティリスクに対する経営層の理解は十分あるものの、②経営会議・取締役会等での報告・議論の頻度の観点では不十分なところが見受けられること、③サイバーセキュリティインシデントに対する経営層の関与度合いには改善の余地があること、④「戦略マネジメント層」の確保・育成は途上にあり必ずしも適性が理解されていないこと、⑤社外への情報発信は強化されているがサプライチェーンを想定した対応は今後の課題であること等が確認された。

経営層のサイバーセキュリティに対する理解は高いものの、実際に報告をうけ、経営層が積極的にリーダーシップを発揮する形で意思決定を行うプロセスには至っていない企業がまだ 35%程度ある。会議体での報告・議論等、実際の運営・意思決定においても、まだ課題が残っている。インシデント発生時の経営層の関与については、まだかなり改善の余地が大きい。経営層は経費や機材・ツール導入等には既に投資しているが、人材の配置や育成についてはまだ十分に投資できていない。

戦略マネジメント層については、情報システム部門のマネジメントラインから配置転換していると回答した企業が 70%を超えており、適性を有すると考えられる事業部門や経営・企画部門のマネジメントラインからの配置転換はまだ少ない割合に留まっている。戦略マネジメント層の人材育成については、サイバーセキュリティの基礎知識の教育を超え、実務対応もできる人材育成が急務と考えられる。

企業の情報発信においては、近年のサプライチェーンセキュリティリスクの急速な拡大を踏まえて当該リスクへの対応が重視されているが、まだ当該リスクへの対応は十分でないと認識されている。

政府のサイバーセキュリティに係る税制優遇やサイバーセキュリティ保険についてはほとんどの日経 225 企業が認知してはいるものの、活用はまだ限定的（保険がせいぜい 2 割程度）に留まっている。

有価証券報告書等の分析結果とアンケート調査結果を組み合わせて分析することで、さらに、有価証券報告書等での記載情報が多い企業ほど、経営層の理解、経営層の関与、態勢整備、社外への発信等の取組が先行、ないしは積極的であることが判明した。

今回、アンケート調査を実施するにあたり、英国政府による「FTSE 350 Cyber Governance Health Check Report」と共通の項目を質問し、我が国における結果を得た上で、英国の調査結果との比較分析を試みた。その結果、両国の共通点としては、サーバーセキュリティリスクに対する経営層の理解が高まっていること、相違点としては、リスクガバナンスや、CISO の設置等態勢面で、英国は日本に大きく先行していることが分かった。

1 本調査の背景、目的および調査概要

(1) 背景と目的

相次ぐ攻撃や各種報道によりサイバーセキュリティリスクへの関心が高まっている。サイバーセキュリティリスクへの対応は、かつては、専ら情報システム等 1 つの部門で実施されているとされてきた。しかし、顕在化した際のインパクトの大きさや、顧客や取引先等の幅広いステークホルダーに影響を及ぼす可能性があること等から、外部への情報発信も含め、サイバーセキュリティリスクにどのように取り組むかは、企業経営層にとっての主要検討課題の 1 つとなってきている。

サイバーセキュリティリスクについて的確な対応を行うには、経営層からの発信・社内への周知徹底だけでなく、管理方針の策定や運営態勢の整備、更には人材育成等、多様な取り組みを行う必要がある。人材面では、専門性のほか、例えば、幅広い部門を巻き込むだけの行動力や、経営層に提言できるだけの戦略策定能力を兼ね備えた一定のプール(戦略マネジメント層)を整える必要がある。

本調査は、①サイバーセキュリティに関する主要企業のリスク認識や情報発信姿勢を有価証券報告書等の開示資料から分析するとともに、②企業に対し行ったアンケートへの回答を整理することで、サイバーセキュリティリスクに対する企業の取組の実態や動向を明らかにすることを目的とする。

(2) 調査概要

(ア) サイバーセキュリティリスク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リスクに関する情報発信状況調査

日経 225 等の企業を対象に、平成 28 年度(2017 年 3 月期)、平成 29 年度(2018 年 3 月期)の 2 ヶ年度につき、有価証券報告書におけるサイバーセキュリティリスクに関する情報発信状況を調査した。具体的には、「事業等リスク」の項目において記載された情報につき、リスク認識の有無や情報発信の詳細度等について分析を行った。

② コーポレートガバナンス報告書におけるサイバーセキュリティリスクに関する情報開示状況調査

上記①と同様、平成 28 年度(2017 年 3 月期)、平成 29 年度(2018 年 3 月期)の 2 ヶ年度につき、コーポレートガバナンス報告書におけるサイバーセキュリティリスクに関する情報発信状況を調査した。具体的には、記載された情報につき、リスク認識の有無や情報発信の詳細度等について分析を行った。

(イ) アンケートによるサイバーセキュリティリスクへの取組状況調査

日経 225 等の企業を対象に、サイバーセキュリティリスクに対する経営層の理解や関与、人材整備の状況や社内外への情報発信姿勢等についてアンケート調査を実施し、この結果を分析して企業の現状や傾向につ

いて取りまとめた。

(ウ)複合的な分析

上記(ア)(イ)の両方の結果に基づいて、以下の観点から複合的な分析を行った。

① 情報開示度合いとアンケート調査結果の関係性分析

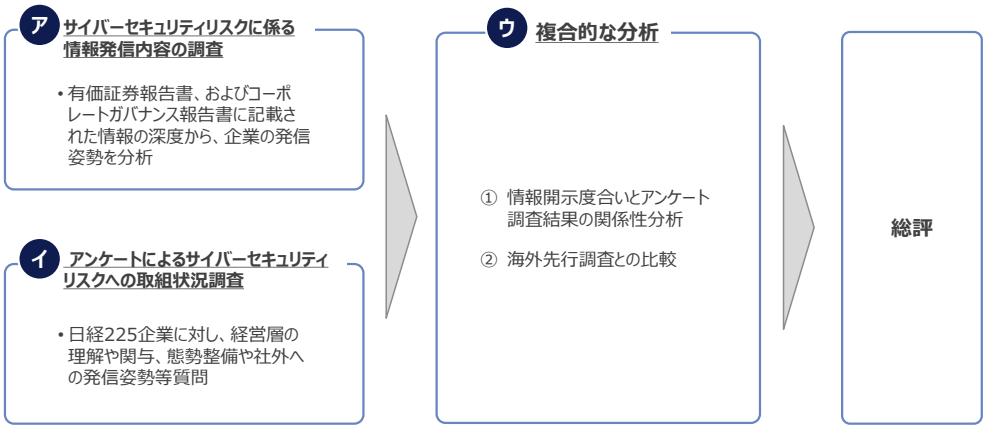
上記(ア)での分析を通して観測される、サイバーセキュリティに関する情報開示度合いが高い企業群について、アンケートでの回答を紐付け、経営層の理解や関与、態勢整備や外部への発信姿勢等、実際の取組について関係性分析を行った。

具体的には、サイバーセキュリティリスクに対し、経営層の問題意識の高い企業においては、態勢整備が先行し、自社だけでなく、ステークホルダーからの理解を一層得るため、外部への情報発信が強化されている等の仮説を構築し、その検証を行うべく分析を行った。

② 海外先行調査との比較

今回の調査と同等の観点から分析・考察を行った先行事例としては、例えば、英国政府による「FTSE 350 Cyber Governance Health Check Report」が挙げられる[1]。このレポートが示す英国の動向を整理するとともに、回答内容や傾向について比較を行った。

図 1-1. 調査フレームワーク



[1] https://www.gov.uk/government/publications/cyber-governance-health-check-2018

(3) 実施スケジュール

本調査は、平成 30 年 12 月に開始し、有価証券報告書等の調査・分析を進めるとともに、並行してアンケート調査を実施し、得られた結果に基づいて総合的な分析を実施した。また、これらの調査結果を、平成 31 年 3 月末までに報告書としてとりまとめた。

2 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) 目的

サイバー攻撃の脅威は深刻化しており、その影響は、顧客や取引先のほか、更には株主等、幅広いステークホルダーに波及する可能性がある。サイバーセキュリティへの取組に関する企業の積極的な情報発信は、これら関係者の理解を促しつつ、当該企業の社会的評価の向上につながる可能性がある。

本章では、有価証券報告書、及びコーポレートガバナンス報告書を対象として、サイバーセキュリティに関するリスク認識の有無や、リスク低減策も含めた記載の深度等につき、対象企業群の発信姿勢を明らかにする。

(2) 調査対象と調査方法

(ア) 対象企業

上場企業 225 社

※平成 28 年度・平成 29 年度それぞれ 10 月 1 日時点の日経平均株価指数採用銘柄

(イ) 対象資料と選定理由

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ることから選定した(前回調査[2]を踏襲)。

② 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ることから選定した(前回調査[2]を踏襲)。

(ウ) 対象期間

① 有価証券報告書

平成 28 年度～平成 29 年度発行分について分析を行った。

---

[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」https://www.nisc.go.jp/inquiry/pdf/kigyoutaisaku_honbun.pdf

② コーポレートガバナンス報告書

平成 28 年度～平成 29 年度発行分について分析を行った。

但し、コーポレートガバナンス報告書は適時開示となるため、該当年度での最新分を参照した。

(エ) 調査方法

対象となる有価証券報告書及びコーポレートガバナンス報告書をインターネットから収集し、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・分析することで調査を行った。

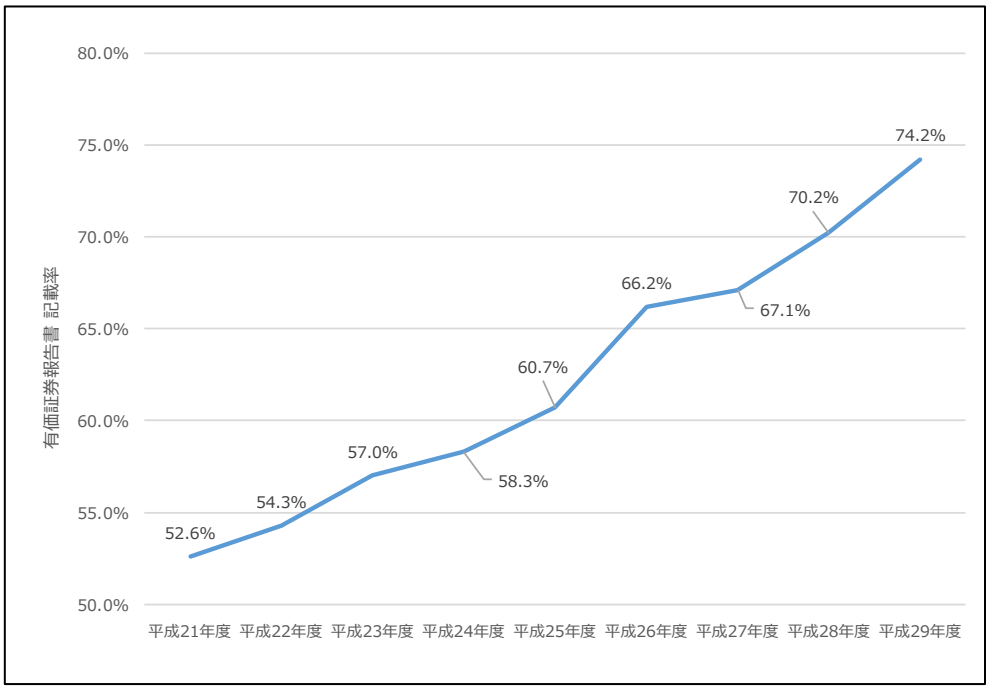
(3) 調査結果

(ア) 有価証券報告書に関する調査

① 時系列的な変化（開示率の増減）

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 年度には 52.6%であったが、平成 27 年度には 67.1%と年々増加した。今回調査の対象である平成 28 年度・29 年度については、それぞれ 70.2%、74.2%と、それまでと同等のペースで開示率が高まっていることを確認した。

図 2-1. サイバーセキュリティリスクに関する開示率の推移



（注）厳密には、平成 27 年度以前とそれ以降では開示に対する判断基準が異なるため、開示率の比較において留意が必要

② 業種別の開示状況

サイバーセキュリティリスクに関する開示状況を業種別にみると、金融、消費、運輸・公共等で記載率が高い（図 2-2）。特に金融や運輸・公共は、経済のインフラとも言える業種であり、サイバーセキュリティを含めリスク全般に対する認識が高いことが背景と考えられる。また、変化に着目すると、技術は、77.2%から 82.5%へ上昇している。

逆に、素材や、資本財・その他では記載率に課題が残る。業種特性や、経営からみた優先順位等、理由は区々想定されるが、企業を取り巻くステークホルダーの広がりや、サプライチェーンを踏まえた事業展開の必要性の高まり等、社会の動向を踏まえると、企業においては、サイバーセキュリティリスクについて発信の視座を高める必要がある。

図 2-2. 業種別にみた開示状況

業種分類	平成28年度		平成29年度		差分	
	該当企業数	開示企業%	該当企業数	開示企業%	該当企業数	開示企業%
技術	44	77.2%	47	82.5%	3	5.3%
金融	21	100.0%	21	100.0%	0	0.0%
消費	27	90.0%	29	90.6%	2	0.6%
素材	27	45.0%	32	54.2%	5	9.2%
資本財・その他	22	59.5%	21	58.3%	-1	-1.1%
運輸・公共	17	85.0%	17	85.0%	0	0.0%
計	158	70.2%	167	74.2%	9	4.0%

※資本財・その他における差分（-1）は、日経 225 における銘柄入れ替えに伴うもの

（イ）コーポレートガバナンス報告書に関する調査

同様の分析を、コーポレートガバナンス報告書についても実施した（図 2-3）。その結果、以下の 2 点を指摘することができる。

① 有価証券報告書と比べた場合、コーポレートガバナンス報告書においては、サイバーセキュリティリスクについて開示を行う企業は少ないものの、開示率は大きく高まっている

② 有価証券報告書において開示率の高い業種が必ずしもコーポレートガバナンス報告書での開示率が高い訳ではない

①の背景としては、非財務情報発信に対する意識の高まりが考えられる。コーポレートガバナンス報告書の紙幅は有価証券報告書と比べた場合、大きくない。他方、企業のガバナンスや発信姿勢等、財務諸表にはない情報（非財務情報）に対する投資家の関心は高まっている。適時開示という報告書の特性も相俟って、コーポレートガバナンス報告書を通じたリスク情報・非財務情報の開示意欲が、企業において急速に高まっている可能性がある。

②については、例えば、有価証券報告書での開示率が 100%であった金融が、コーポレートガバナンス報告書では 30%弱と大きく低下していることを指摘できる。コーポレートガバナンス報告書は、資本市場をより強く意識したものであり、有価証券報告書と比べると、企業によっては、発信する情報の網羅性よりも重要性・代表性を重んじている可能性がある。しかし、こうした報告書間の相違は、サイバーセキュリティリスクへの意識の高まりとともに徐々に解消されていくものと考える。

図 2-3. コーポレートガバナンス報告書における記載状況

業種分類	平成28年度		平成29年度		差分	
	該当企業数	開示企業%	該当企業数	開示企業%	該当企業数	開示企業%
技術	14	24.6%	25	43.9%	11	19.3%
金融	3	14.3%	6	28.6%	3	14.3%
消費	7	23.3%	14	43.8%	7	20.4%
素材	14	23.3%	20	33.9%	6	10.6%
資本財・その他	10	27.0%	16	44.4%	6	17.4%
運輸・公共	2	10.0%	5	25.0%	3	15.0%
計	50	22.2%	86	38.2%	36	16.0%

(ウ) 記載の深度

上記より、リスク認識の高まり等から、サイバーセキュリティリスクについて開示を行う企業が増していることが分かった。それで、記載の深度についてさらに分析を行った。

図 2-4 は、一般的なリスク評価アプローチを示したものである。固有リスクは関連する内部統制が存在していないと仮定した場合に生じうるリスクを、低減策は当該固有リスクを低減するための対策を、残存リスクは低減策を講じた後にも残りうるリスクをそれぞれ指す。サイバーセキュリティリスクに対する低減策としては、例えば、ポリシー・規程の策定、社内への周知徹底、牽制体制の構築などがある。今回調査では、「事業等リスク」に記載された情報から、図表 2-5 に示した 15 項目を基準として、記載の有無を確認した。

図 2-4. 一般的なリスク評価アプローチ

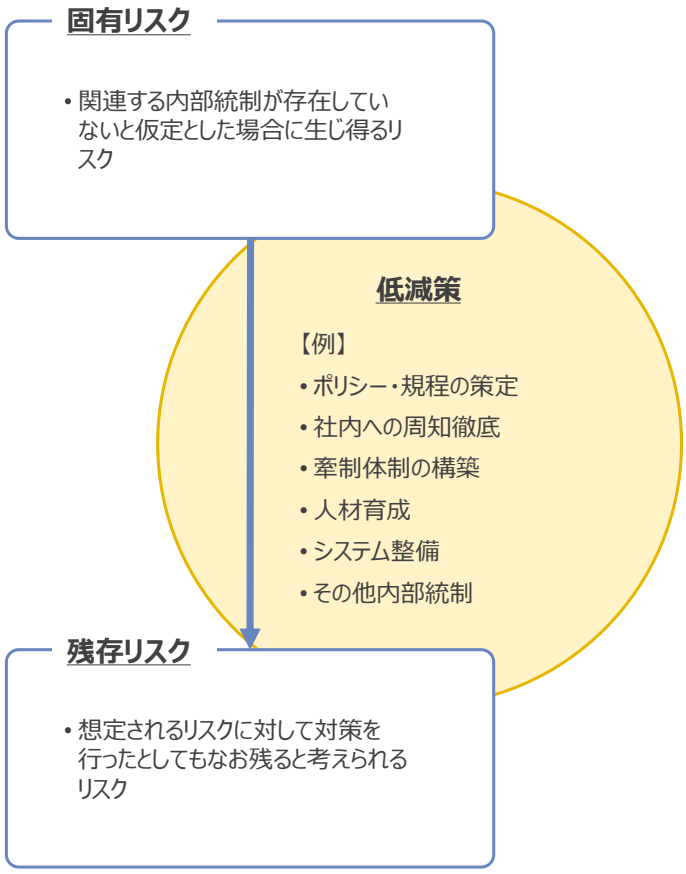
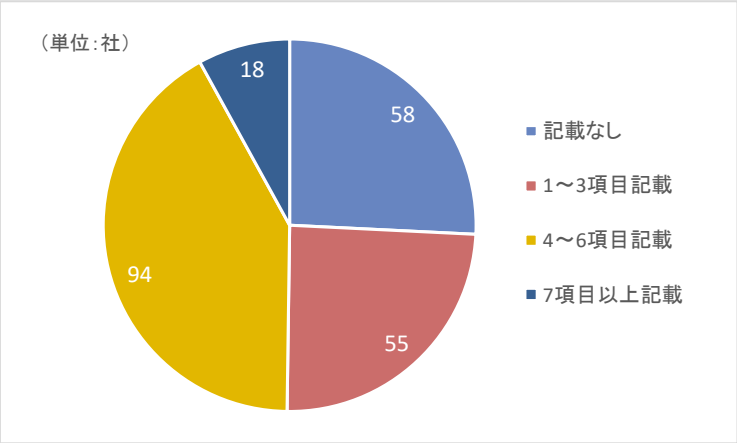


図 2-5.サイバーセキュリティリスクに関する記載についての評価項目（有価証券報告書）

項目		評価基準	例
1．リスク認識（固有リスク）			
	①サイバーを含めたセキュリティに関するリスクを認識している	リスク項目として、開示・明記があれば、「有り」とする	・有価証券報告書の事業等のリスクの欄に、「情報セキュリティ」「サイバーセキュリティ」「情報漏洩」に関する記載がある
2 低減策	1）基本施策		
	②セキュリティに関する基本方針やポリシーを開示している	明記の場合、「有り」とする	・具体的なセキュリティーポリシー、ガイドブックに関する記載がある ・「情報セキュリティ方針」をシステム捜査権限の設定の基準としている ・「情報セキュリティ委員会が、情報セキュリティ対策の方針制定」 ・「情報セキュリティの方針を定め」
	③セキュリティマネジメント体制について開示している	明記の場合、「有り」とする	・「体制の強化」 ・「管理体制の構築」 ・「管理体制の継続的な改善」 ・「情報管理に関する管理体制」 ・「コンプライアンスやリスク管理体制及び情報セキュリティ管理体制の再整備」 ・「機密情報の漏えいを防止する体制」
	2）更なる低減策		
	経営層		
	④経営者の積極的な取組姿勢について開示している	具体的な記載があれば、「有り」とする	・「機密情報の漏洩対策を最重要の経営課題として認識している」
	⑤経営者がサイバーセキュリティリスクをどう考えているかを開示している	具体的に定義している場合、「有り」とする	・「情報セキュリティ及び個人情報を含む重要情報の保護を経営の最重要課題のひとつとして捉えている」
	人材		
	⑥社員に対する教育・人材育成・啓蒙活動について開示している	明記の場合、「有り」とする	・「情報管理に関する管理体制と教育」 ・「社内教育」 ・「社内規程やマニュアルを整備し、社員に周知徹底」
	⑦ 社員に対する普及啓発のためのツール（マーク、スローガン）について開示している	明記の場合、「有り」とする	・「個人情報保護宣言(プライバシーポリシー)の制定」 ・「○○グループCSR憲章を制定」
	態勢		
	⑧ C-SIRTの設置について開示している	明記の場合、「有り」とする	・「情報漏洩等のインシデント発生時には、C-SIRTの設置を設置する体制を整えている」
	⑨社外との情報共有体制について開示している（ISAC、日本シーサート協議会への加盟等）	明記の場合、「有り」とする	・「日本シーサート協議会に加盟している」 ・「金融ISACに加入している」
	⑩ 第三者評価・認証の取得状況を開示している	明記の場合、「有り」とする	・「ISMS認証」
	⑪サイバー演習・訓練の実施方針等について開示している	明記の場合、「有り」とする	・「コンピュータ機器・回線の二重化や危機管理に対する訓練を実施」 ・「侵入リスクを低減する施策として、標的型攻撃等に対する訓練を定期的に実施」
	⑫ グループ企業全体についてのセキュリティ対策を開示している	明記の場合、「有り」とする	・「当社グループは、個人情報や機密情報の保護のための情報セキュリティの取組みを実施している」
	⑬サプライチェーン企業全体についてのセキュリティ対策を開示している	明記の場合、「有り」とする	・「当連結グループは事業活動において、顧客情報・個人情報等に接することがあり、また営業上・技術上の機密情報を保有しています。これら各種情報の取り扱い、機密保持には細心の注意を払っており、不正なアクセス、改ざん、破壊、漏洩、紛失等から守るため、管理体制及び取扱規則を定め、合理的な技術的対策を実施するなど、適切な安全措置を講じています。」
3．リスク認識（残存リスク）			
	⑭財務面の影響について開示している	明記の場合、「有り」とする	・「情報漏洩等の重大な障害が発生した場合、当社グループの業績や財務状況に影響を及ぼす可能性があります」
	⑮サイバーインシデント、重大なITシステム障害、情報漏えい等によって受けた被害やその影響範囲等ITからの影響について具体的に開示している	明記の場合、「有り」とする	・「顧客個人に支払う損害賠償による費用の発生」 ・「当社グループの社会的信用の失墜」 ・「お客様へ提供するサービスの遅延または停止が発生」 ・「監督官庁からの処分等を受ける」 ・「信用回復するまでの間、事業が停滞する」

前頁の基準に即し、「記載なし」、「1～3 項目記載」、「4～6 項目記載」、「7 項目以上記載」に分類した上で、対象企業の分布をみた（図 2-6）。そもそも記載のなかった 58 社を除く、167 社の中においても、7 項目以上記載していた企業は 18 社に留まる。すなわち、15 項目の中でも半分を超える項目について記載のあった企業が非常に限られていたことが分かる。

図 2-6. 記載の深度に関する企業の分布（平成 29 年度）



しかし、最近において状況は変化している。図 2-7 は、記載の深度を平成 28 年度のものと比較したものである。

図 2-7. 記載の深度の推移（平成 28～29 年度）

（単位：社）

	平成28年度	平成29年度	差分
記載なし	67	58	-9
1～3項目記載	65	55	-10
4～6項目記載	86	94	8
7項目以上記載	7	18	11

これをみると、①7 項目以上記載していた企業は、平成 28 年度には 7 社にとどまっていたのが平成 29 年度には 11 社増加したこと、②サイバーセキュリティリスクに関する記載がなかった企業が、平成 28 年度から平成 29 年度にかけ 9 社減少したこと、③1～3 項目記載の企業が 10 社減り、4～6 項目記載の企業が 8 社増加したこと、等が分かる。

すなわち、2 つの年度を比較するだけでも、有価証券報告書においてサイバーセキュリティリスクに関する記載内容が拡充されていることとなる。サイバーセキュリティリスクに対する関心・問題意識の高まりとともに、

企業がステークホルダーに対し、施策を含め丁寧に情報発信しようとする姿勢が醸成されてきていると考えられる。

同様の分析をコーポレートガバナンス報告書について行ったのが、図 2-8 である。有価証券報告書と比べた場合の記載量の違いから、図表 2-9 に示すように評価項目の数を 15 から 5 に絞り込んでいるが、平成 28 年度から平成 29 年度にかけて記載なしの企業が 175 社から 140 社へと 35 社減少した一方で、2～3 項目の記載であった企業が 41 社から 75 社と 34 社増加している。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リスクについて記載・開示を行う企業が限られていることは先に述べた通りであるが、有価証券報告書と同様、記載の深度は増している。

図 2-8. 記載の深度の推移（平成 28～29 年度）

（単位：社）

	平成28年度	平成29年度	差分
記載なし	175	140	-35
1項目記載	5	5	0
2～3項目記載	41	75	34
4項目以上記載	4	5	1

図 2-9. コーポレートガバナンス報告書における評価項目

項目			評価基準	例
1. リスク認識（固有リスク）				
		①サイバーを含めたセキュリティに関するリスクを認識している	リスク項目として、開示・明記があれば、「有り」とする	
2 低減策	1）基本施策			
		②セキュリティに関する基本方針やポリシーを開示している	明記の場合、「有り」とする	・具体的なセキュリティーポリシー、ガイドブックに関する記載がある ・「情報セキュリティ方針」をシステム捜査権限の設定の基準としている ・「情報セキュリティ委員会が、情報セキュリティ対策の方針制定」 ・「情報セキュリティの方針を定め」
		③セキュリティマネジメント体制について開示している	明記の場合、「有り」とする	・「情報セキュリティ委員会を設置」 ・「情報セキュリティ体制を整備」 ・「サイバーセキュリティに関する態勢整備」
		④社員に対する教育・人材育成・啓蒙活動について開示している	明記の場合、「有り」とする	・「情報管理に関する管理体制と教育」 ・「社内教育」 ・「社内規程やマニュアルを整備し、社員に周知徹底」
	2）更なる低減策			
		⑤上記以外の取り組みについて具体的に明記されている	明記の場合、「有り」とする	・「情報セキュリティマネジメントシステム(ISMS)の第三者による審査」

（エ）詳細分析

これまで、有価証券報告書、コーポレートガバナンス報告書それぞれにつき、開示率の変化や業種別の状況、時系列の変化を記した。本節では、相対的に記載情報の多かった有価証券報告書につき、図 2-5 で示した 15 の項目にかかる傾向を、①項目別、②業種別に考察する。

① 項目別

図 2-10 は、有価証券報告書にてサイバーセキュリティリスクに関し、記載のあった 167 社の記載状況を項目別にみたものである。これをみると、以下を指摘できる。

- 「基本的な取り組み」とした 2 項目（項目②～③）についてはそれぞれ 57 社、64 社と記載状況はほぼ同じ
- 「さらなる低減策」のうち、積極的な取組姿勢等の「経営層」に関する記載は限定的である一方（項目④～⑤）、「社員に対する教育・人材育成・啓蒙活動」に関する記載は比較的多い（項目⑥）
- 「態勢」のうち、C-SIRT の設置や社外情報共有体制等、項目⑧～⑪に関する記載は極めて限定的
- グループ企業全体についてのセキュリティ対策を開示している企業は相応にあるものの（項目⑫）、サプライチェーン企業全体についてのセキュリティ対策を開示している企業は極めて限られる（項目⑬）
- 「残存リスク」について記載のある企業は相応に存在（項目⑭～⑮）

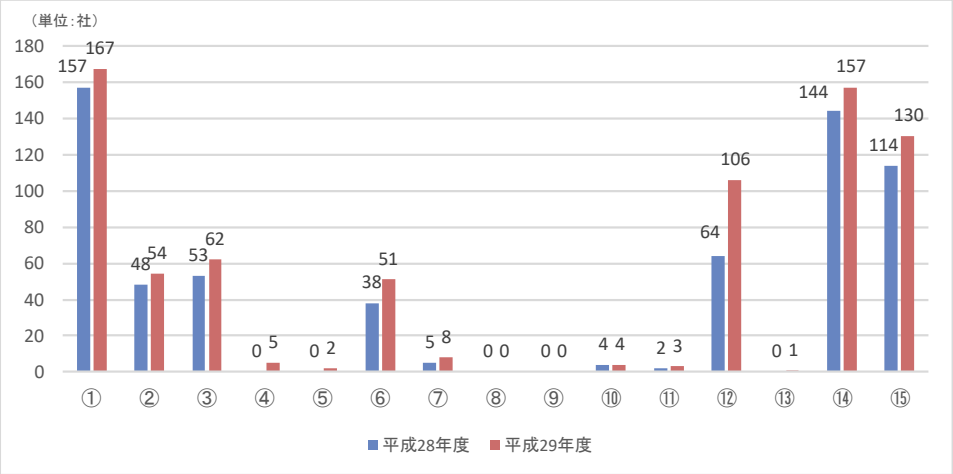
図 2-10. 項目別にみた記載の分布（平成 29 年度）

項目			社数
1．リスク認識（固有リスク）			
		①サイバーを含めたセキュリティに関するリスクを認識している	167
2 低減策	1）基本的施策		
		②セキュリティに関する基本方針やポリシーを開示している	54
		③セキュリティマネジメント体制について開示している	62
	2）更なる低減策		
	経営層		
		④経営者の積極的な取組姿勢について開示している	5
		⑤経営者がサイバーセキュリティリスクをどう考えているかを開示している	2
	人材		
		⑥社員に対する教育・人材育成・啓蒙活動について開示している	51
		⑦ 社員に対する普及啓発のためのツール（マーク、スローガン）について開示している	8

項目			社数
2 低減策	態勢		
		⑧ C-SIRTの設置について開示している	0
		⑨社外との情報共有体制について開示している（ISAC、日本シーサート協議会への加盟等）	0
		⑩ 第三者評価・認証の取得状況を開示している	4
		⑪サイバー演習・訓練の実施方針等について開示している	3
		⑫ グループ企業全体についてのセキュリティ対策を開示している	106
		⑬サプライチェーン企業全体についてのセキュリティ対策を開示している	1
3．リスク認識（残存リスク）			
		⑭財務面の影響について開示している	157
		⑮サイバーインシデント、重大なITシステム障害、情報漏えい等によって受けた被害やその影響範囲等ITからの影響について具体的に開示している	130

平成 28 年度と比較したものが、図 2-11 である。サイバーセキュリティリスクについて記載のあった企業が増加したことは先述の通りであるが、項目⑫「グループ企業全体についてのセキュリティ対策」を記載した企業が、平成 28 年度の 64 社から平成 29 年度には 106 社と大きく増加したことは注目に値する。これは、自社、場合によってはステークホルダーに広く影響を与えうるサイバーセキュリティリスクについては、企業単体ではなく、連結企業全体で対応すべきとの考えが強く反映されたものではないかと推察する。

図 2-11. 項目別にみた記載の分布（平成 28～29 年度）



② 業種別

図 2-12 は、業種別に記載状況の分布を記したものである。なお、各項目の定義は以下の通りである。

- 「記載なし」

  サイバーセキュリティリスクについて、有価証券報告書で記載なし

- 「記載あり」

  サイバーセキュリティリスクについて、有価証券報告書で記載あり

- 「基本施策を実施」

  図 2-5 で示した 15 の項目のうち、項目②～③（基本方針やポリシーの開示、セキュリティマネジメント体制）に関し記載して開示

- 「更なる低減策を実施」

図 2-5 で示した 15 の項目のうち、項目②～③に関する記載はないが、項目④～⑬(「更なる低減策」)について記載

- 「基本施策に加え、いずれかの更なる低減策を実施」

  図 2-5 で示した 15 の項目のうち、項目②～③に加え、項目④～⑬(「更なる低減策」)について記載

図 2-12. 業種別にみた記載の分布(平成 29 年度)

		技術		金融		消費	
		社数	割合	社数	割合	社数	割合
記載なし		10	17.5%	0	0.0%	3	9.4%
記載あり		47	82.5%	21	100.0%	29	90.6%
	リスク認識あり	17	29.8%	7	33.3%	7	21.9%
	基本施策を実施	4	7.0%	0	0.0%	2	6.3%
	更なる低減策のみ実施	7	12.3%	2	9.5%	3	9.4%
	基本施策に加え 更なる低減策いずれか実施	19	33.3%	12	57.1%	17	53.1%
計		57	100.0%	21	100.0%	32	100.0%

		素材		資本財・その他		運輸・公共	
		社数	割合	社数	割合	社数	割合
記載なし		27	45.8%	15	41.7%	3	15.0%
記載あり		32	54.2%	21	58.3%	17	85.0%
	リスク認識あり	3	5.1%	4	11.1%	1	5.0%
	基本施策を実施	1	1.7%	2	5.6%	0	0.0%
	更なる低減策のみ実施	19	32.2%	5	13.9%	6	30.0%
	基本施策に加え 更なる低減策いずれか実施	9	15.3%	10	27.8%	10	50.0%
計		59	100.0%	36	100.0%	20	100.0%

傾向としては、以下を指摘することができる。

- ポリシーや体制等、「基本施策」のみ記載した企業(凡例は「基本施策を実施」)は、いずれの業種も限定的
- リスク認識のある企業では、「基本的な取組み」に加え、「更なる低減策」について記載している場合が多い

- 「基本的な取組みに加え、更なる低減策を実施」している企業は、技術・金融・消費で多い
- 「素材」は、サイバーセキュリティについて、リスク認識がない企業が多い上、リスク認識があっても、「基本的な取組み」や「更なる低減策」に関して記載した企業は少ない
- 「資本財・その他」に属する企業では、リスク認識のない企業が多い

なお、業種中分類での傾向については、「6.資料編」にて掲載した。

(4) まとめ

以上、本節では、サイバーセキュリティリスクについて、開示率の推移に始まり、記載の深度、業種別や時系列等でみた傾向分析を行った。分析の結果、サイバーセキュリティリスクについては、①開示率は高まっているものの、②記載の有無に業種の差異があること、③低減策については、項目でみると、記載の深度に偏りがあること、④更に、その深度にも業種間で差異があること等が観測された。

③～④については、企業の情報発信姿勢に依存している可能性があるが、自社だけでなく、社会に影響を与えるサイバーセキュリティリスクについて、幅広いステークホルダーの理解を得つつ、企業の社会的価値を高めるためには、まずは情報発信の詳細度を高める必要がある。特に③低減策については、詳細な記載・発信が求められる。

3 アンケート調査

(1) 目的

企業にとって IT とは、コストの削減や迅速化といった業務の効率化だけでなく、新たな事業・サービスの創造等、イノベーションの源泉となるものである。他方、サイバーセキュリティリスクは、システム部門に閉じた課題ではなく、技術の進展とそのリスクが及ぼす影響の大きさから、リスク管理や経営企画、広報部門等、幅広い部門に影響を及ぼすものとなっている。これに伴い、サイバーセキュリティへの対応や、その管理も、現場社員のみで完結するものではなく、経営層、更には経営と現場を繋ぐ「戦略マネジメント層（橋渡し人材層）」[3]の関与や外部委託先との協力が不可欠である。

本調査では、サイバーセキュリティに対する経営層の理解や取り組み姿勢、態勢整備や社内外への発信姿勢、更には必要人材の確保や育成等、様々な視点で、企業におけるサイバーセキュリティに関する運営実態を明らかにすることを目的とした。さらには、税制面での優遇処置やサイバーセキュリティ保険への認識の有無等、直近の話題に関する質問も設けたことが、今回調査の大きな特徴である。

【アンケートにおける調査・分析の観点】

① サイバーセキュリティに対する経営層の理解と関与

② 態勢整備にむけた姿勢と浸透度合い

③「戦略マネジメント層」の確保と育成

④ 社外への発信

⑤ 税制優遇やサイバーセキュリティ保険に対する認識

(2) 調査対象と実施方法

(ア) 対象企業

上場企業 225 社(平成 30 年 11 月 1 日現在の日経平均株価指数銘柄)等を対象として調査した。

※可能な限り連結子会社の対策を含めた回答を想定

[3] 戦略マネジメント層とは、「経営層が示す経営戦略や事業戦略を実現するため、サイバーセキュリティに係るリスクを、管理すべきリスクの 1 つと捉え、運営の中心となる人材層」と定義する。具体的な業務としては、経営層が示した方針を踏まえた、サイバーセキュリティリスクへの対策立案、実務者層・技術者層の指揮、経営層への報告等がある。

（イ）実施期間

平成 31 年 2 月 4 日～3 月 1 日に調査を実施した。

（ウ）回答者

サイバーセキュリティ対策に関する担当者（リスク管理部門・経営企画部門・情報システム部門等）

（エ）調査方法

以下を郵便で送付し、アンケート票を記入後、同封した返信用封筒を用いて回収した。また、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、回収を行った。

【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

(3) 調査結果

（ア）回答企業データ

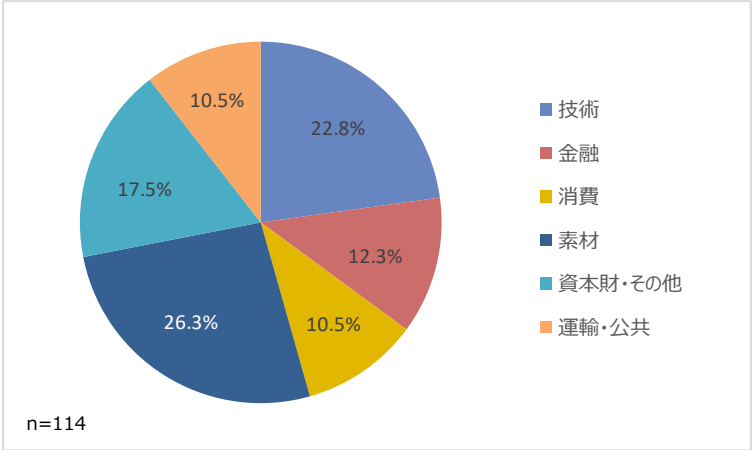
① 有効回答数

114 社（回答率：50.7％）

② 業種

日経業種分類（大分類）に即して、回答企業の分布を記すと、図 3-1 の通りとなる。

図 3-1. 回答企業の業種



③ 年間売上高及び従業員数

年間売上高、および従業員数は、連結決算の対象であるグループ企業全体について集計した。分布は、図 3-2、3-3 の通りである。

図 3-2. 回答企業の売上高(連結)の分布

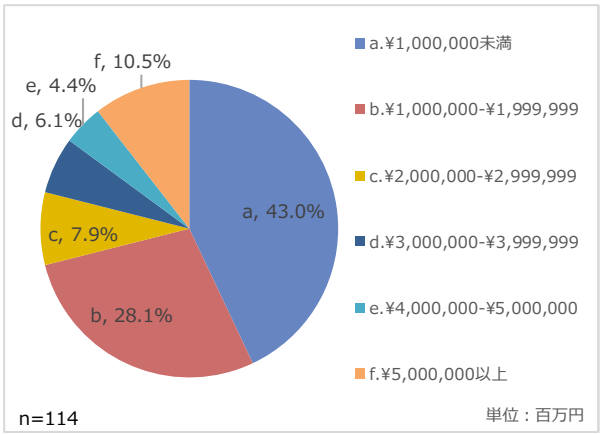
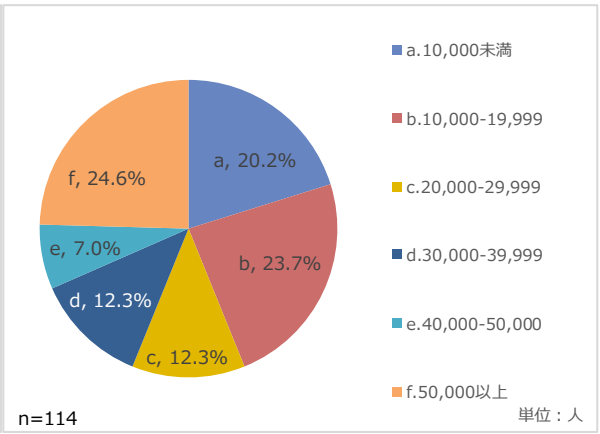


図 3-3. 回答企業の従業員数(連結)の分布



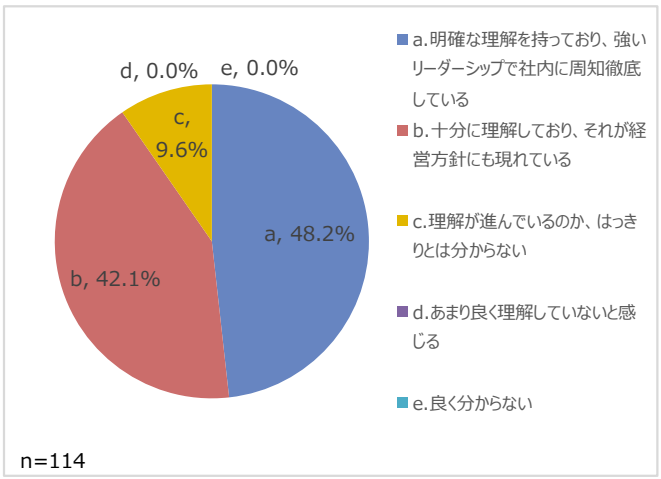
(イ) サイバーセキュリティに対する経営層の理解と関与

① 経営層の理解

まず始めに、経営層の理解について示す。図 3-4 は、「経営層は、事業の鍵を握る重要な情報やデータの損失・漏えいが、事業にどれほど大きな影響を及ぼすかについて良く理解していますか」との質問に対する回答である。

これをみると、「a.明確な理解を持っており、強いリーダーシップで社内に周知徹底している」、「b.十分に理解しており、それが経営方針にも現れている」とした企業が 90%超を占め、サイバーセキュリティリスクが企業経営層にとっての主要な経営課題の 1 つとなっていることが分かった。

図 3-4. 自社への影響に対する経営層の理解



同様の質問を、より踏み込んだ形で行った結果が、図 3-5 である。図 3-5 は、「経営層は、事業の鍵を握る重要な情報やデータは何か、またこれらの情報やデータが貴社・競業他社・犯罪者にとってどれほどの価値があるかについて良く理解していますか」との質問に対する回答である。自社への影響だけでなく、競合他社や犯罪者等、自社にとって脅威となる対象まで視野が及んでいるか明らかにするためのものであった。

この結果をみると、先の質問と比べると、若干割合は低下するものの、「a.明確な理解を持っており、強いリーダーシップで社内に周知徹底している」、「b.十分に理解しており、それが経営方針にも現れている」とした企業が 85%超を占め、サイバーセキュリティリスクをかなりの程度、経営層が理解していることが判明した。

図 3-5. サイバーセキュリティに関するリスクへ経営層の理解

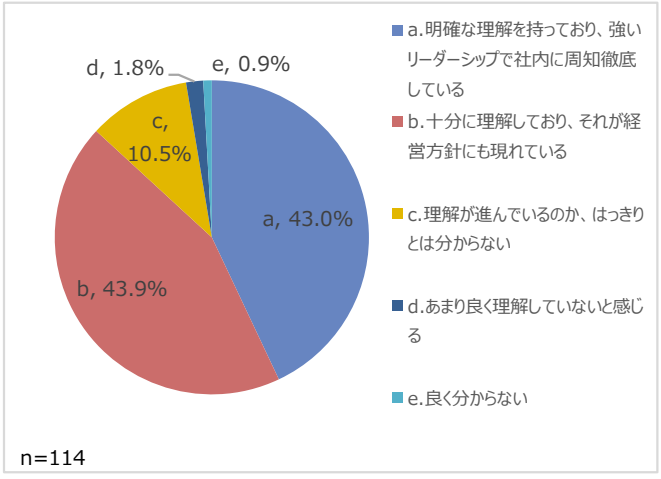
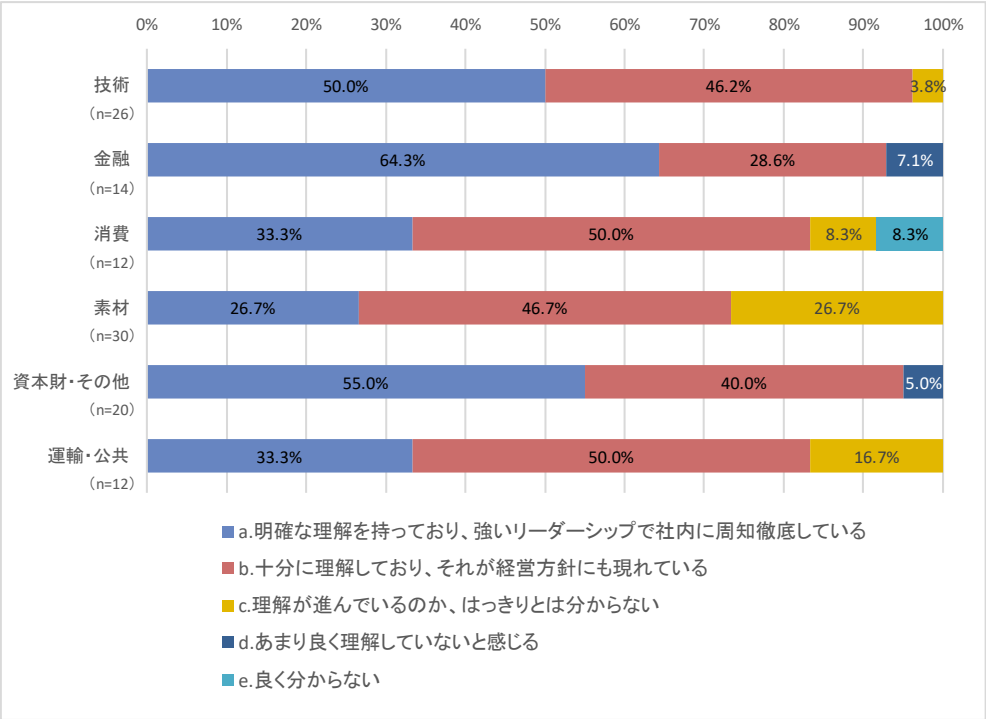


図 3-6. 業種別にみた経営層の理解



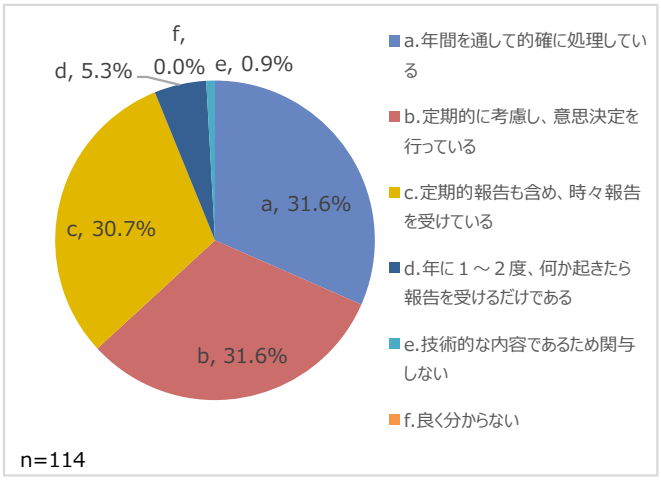
また、図 3-6.は、これを業種(大分類)別にみたものである。これをみると、「a.明確な理解を持っており、強いリーダーシップで社内に周知徹底している」と回答した企業は、金融(64.3%)、資本財・その他(55.0%)、技術(50.0%)の順で多い一方で、素材や運輸・交通では、「c.理解が進んでいるのか、はっきりとは分からない」と回答している企業の割合が 15-25%に及んでいることが分かる。

また、一部業種では、「d.あまり良く理解していないと感じる」、「e.良く分からない」との回答も見られる。業種の特性はあるものの、サイバーセキュリティリスク顕在化時の企業インパクトは決して軽視できるものではなくなっており、経営層の理解向上・促進が待たれる。

② 経営意思決定

次に、経営層の意思決定への関与度合いについて記す。図 3-7 は、「サイバーセキュリティに対する経営層の関与の度合いについて、最も良く当てはまる記述はどれですか」との質問に対する回答である。

図 3-7. 意思決定へ経営層の関与度合い

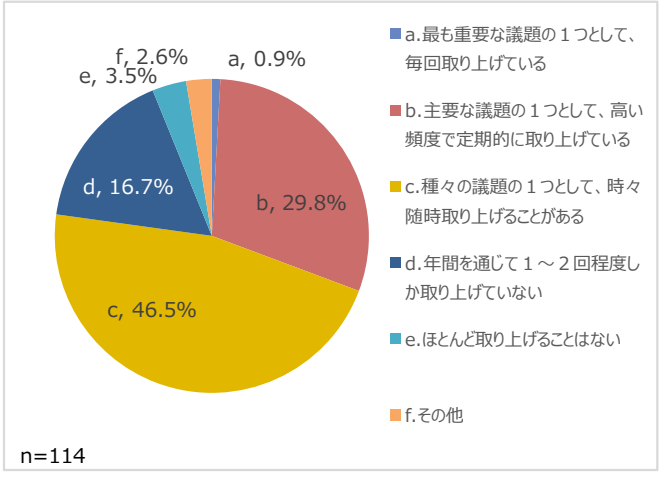


これをみると、「a.年間を通して的確に処理している」、「b.定期的に考慮し、意思決定を行っている」と答えた企業が 60%超を占める一方で、「c.定期的報告も含め、時々報告を受けている」、「d.年に 1～2 度、何か起きたら報告を受けるだけである」といった、経営層がまだまだ受け身の態勢であることを窺わせる回答が 35%程度あることが分かる。

「①経営層の理解」で述べた 2 つの質問に対する回答との関係を考慮すると、経営層のサイバーセキュリティに対する理解は高いものの、実際に報告をうけ、経営層が積極的にリーダーシップを発揮する形で意思決定を行うプロセスには至っていない企業が一定程度あることが分かる。

現場からの報告が経営層の意思決定につながっているかといった観点では、定量化しやすいものとして、経営層が参加する会議体で報告される頻度・議論される頻度が挙げられる。図 3-8 は、サイバーセキュリティに関する事項が、経営会議・取締役会等、経営層を含めた会議体でどの程度報告・議論されているか示したものである。

図 3-8. 経営会議・取締役会での報告・議論の頻度



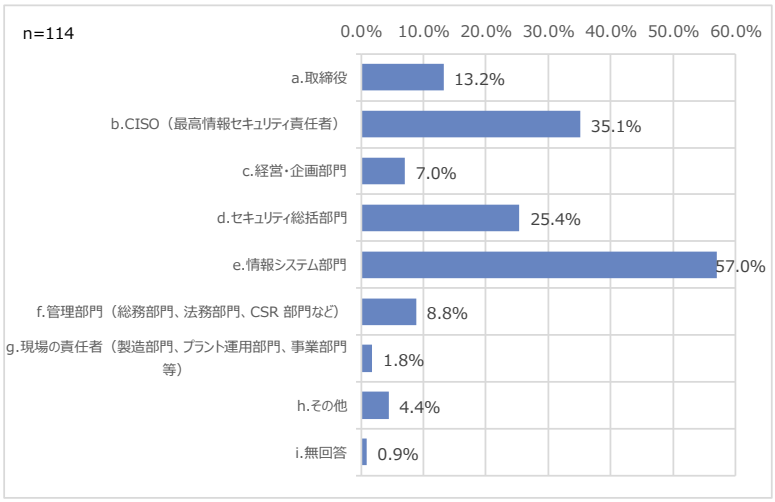
これをみると、「a.最も重要な議題の 1 つとして、毎回取り上げている」、「b.主要な議題の 1 つとして、高い頻度で定期的に取り上げている」とした企業群は 30%程度にとどまることが分かる。「①経営層の理解」で示された内容と合わせると、サイバーセキュリティに対する経営層の理解は高いものの、会議体での報告・議論等、実際の運営・意思決定においては、一定の課題が残る。

上記課題の背景としては、経営層に対する報告者に起因する部分がある。図 3-9 は、経営会議・取締役会での報告者の属性・所属部署についての回答である。

CISO（最高情報セキュリティ責任者）が報告とした企業が 35%程度あるものの、「d.セキュリティ統括部門」、「e.情報システム部門」が報告とした企業が 80%程度ある。複数選択の回答であるため、職責の重複は存在するものの、サイバーセキュリティリスクの責任者による報告を定期的に実施する態勢がとられていない可能性がある。

また、「c.経営・企画部門」による報告が 7.0%とかなり限定されている。周知の通り、サイバーセキュリティリスクは、情報システム部門に閉じたものではなく、経営・企画部門も含めた幅広い部門が組織横断的に対応すべき事項となっている。報告を行うフローは企業や業種、規模等で相違が想定されるが、活発な議論を行うには、経営層により近い経営・企画部門からの報告・発信が一層頻繁になされても然るべきである。

図 3-9. 経営会議・取締役会での報告者

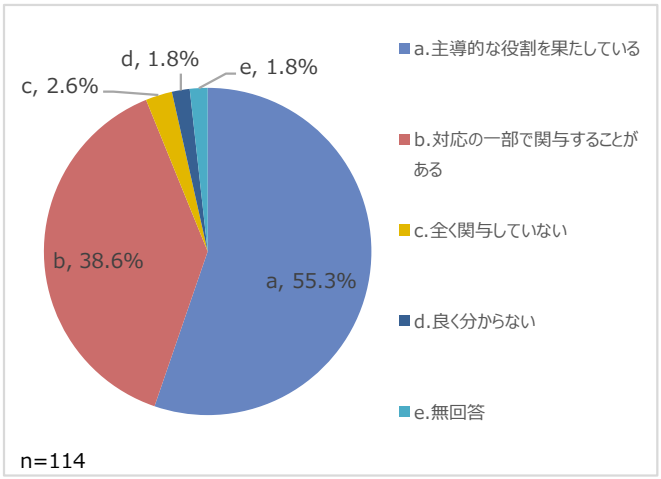


③ 関与の度合い

本節最後の論点として、経営層の関与度合いについて記したい。図 3-10 は、サイバーセキュリティインシデントが発生した際の経営層の関与度合いを示したものである。これをみると、「a.経営層が主導的な役割を果たしている」とした企業は、55%程度に留まっていることが分かる。インシデントが顕在化

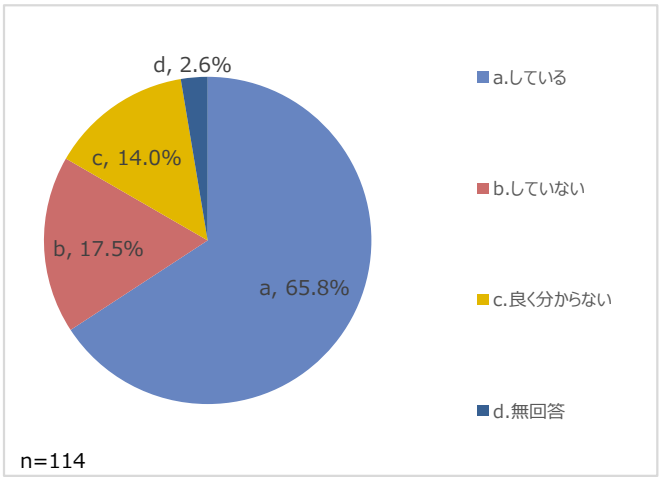
した際の社会的影響の大きさを鑑みると、インシデント発生時の経営層の関与については、まだかなり改善の余地が大きいと考えられる。

図 3-10. サイバーセキュリティインシデントに対する経営層の関与度合い



また、リスク顕在化を未然に防ぐ措置の例示として、今回調査では、「経営層は、顧客データのセキュリティに関する報告のレビューに積極的に関与しているか」との問いを設けた。回答結果は、図 3-11 の通りである。

図 3-11. 顧客データのセキュリティに関する報告のレビューへの経営層の関与度合い



これをみると、約 3 分の 2 の企業が、経営層の関与があるとしたものの、「b.していない」と回答した企業が 15%超存在することが分かる。サイバーセキュリティに関するリスクが顕在化した際のインパクトは、事前に測りづらいところがある一方、多様なステークホルダーに影響を及ぼす可能性があること、場合によっては、顧客離れや業務停止等により自社の業績や株価に多大な影響を与える可能性等想定すると、リスクを未然に防ぐ措置については、経営層の関与が一層強く求められる。

(ウ) 態勢整備にむけた姿勢と浸透度合い

① 態勢整備にむけた姿勢

前節では、サイバーセキュリティへの経営層の理解・問題意識は高いものの、会議体での報告・議論等、運営面に課題が残ることを示したが、経営層においては、サイバーセキュリティに対する取組み姿勢を社内に徹底させたいという意向は極めて強い。

図 3-12 は、「経営層は、現在の事業及びこれからのデジタル変革への対応において、サイバーセキュリティリスク対策への取組姿勢をどれほど明確に示していますか」との問いに対する回答である。これをみると、「a.取組み姿勢を全社に明確に示しており、対策の徹底を求めている」と回答した企業の割合が約 75%となった。また、業種別にみたものが、図 3-13 である。

図 3-12. 経営層のサイバーセキュリティ対策への取組姿勢の明確度合い

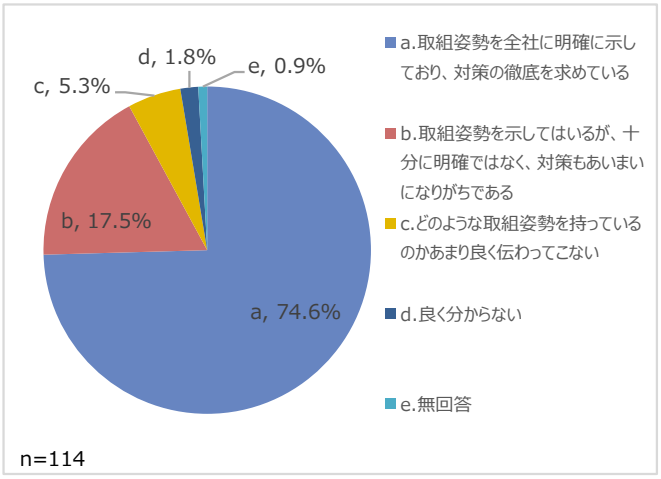
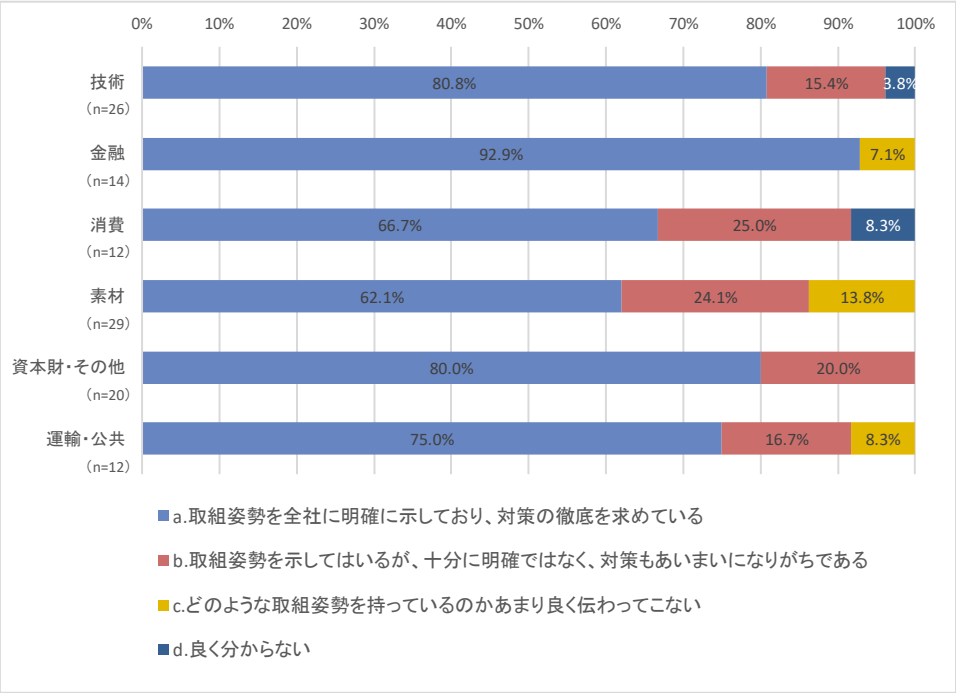


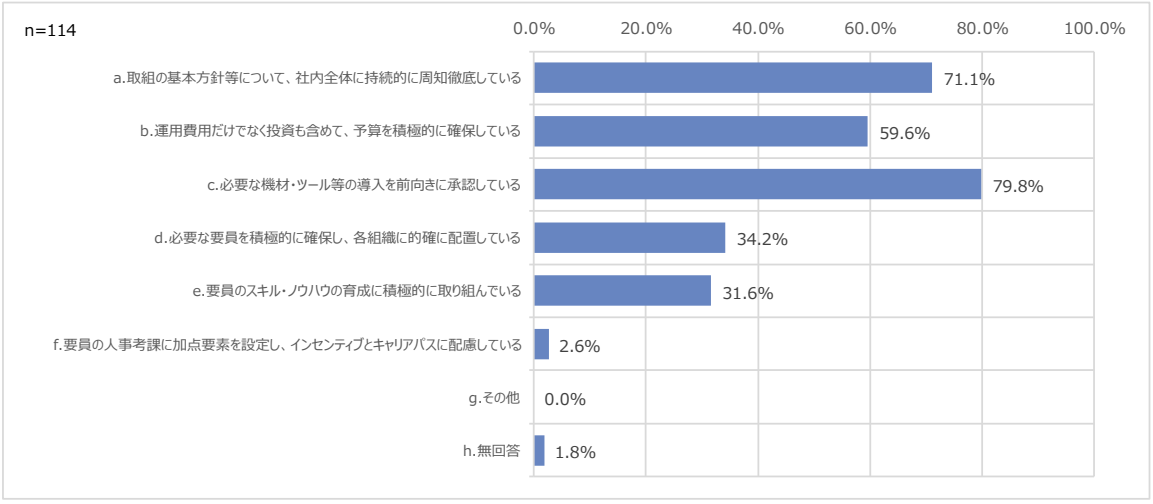
図 3-13. 業種別にみた取組姿勢の明確度合い



これをみると、「a.取組姿勢を全社に明確に示しており、対策の徹底を求めている」とした企業は、金融で特に多いことが分かる。いわゆるフィンテックや、デジタリゼーションの流れを汲み、オペレーションの変革途上にある業種とされるが、外部環境の変化と相俟って、サイバーセキュリティリスクへの感度が他業態と比べてもかなり高いことが確認された。

次に、図 3-14 は、「経営層は積極的にサイバーセキュリティ対策を確保する態勢整備に取り組んでいますか」との問いに対する回答である。

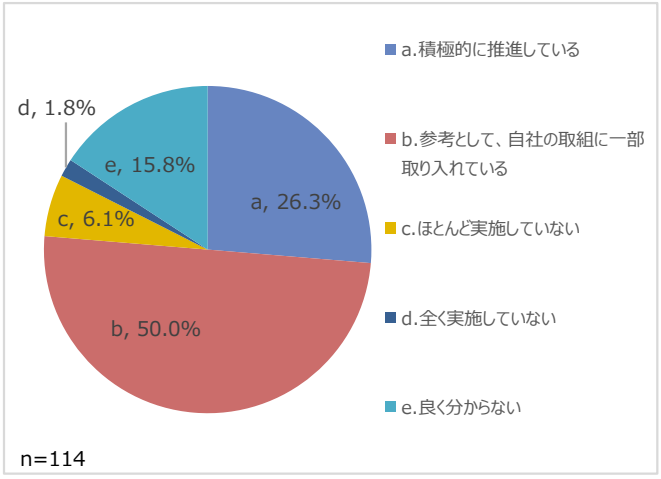
図 3-14. 経営層の支援の内容



複数選択の回答であることに留意の必要はあるが、「b.運用費用だけでなく投資も含めて、予算を積極的に確保している」、「c.必要な機材・ツール等の導入を前向きに承認している」とした企業群が、それぞれ 59.6%、79.8%とかなり高いことが分かる。未知のサイバー攻撃に対応するためには、IT 予算とは別の枠組みで、サイバー攻撃対策として、一定の予算を確保し、段階的に態勢強化を実施して行くことが必須である。

図 3-15 は、「経団連サイバーセキュリティ経営宣言」をうけての経営層の取組みについて尋ねた結果である。当該宣言に基づく取り組みを始めている割合は 75%以上に達していることが分かる。

図 3-15.「経団連サイバーセキュリティ経営宣言[4]」をうけての経営層の取組み

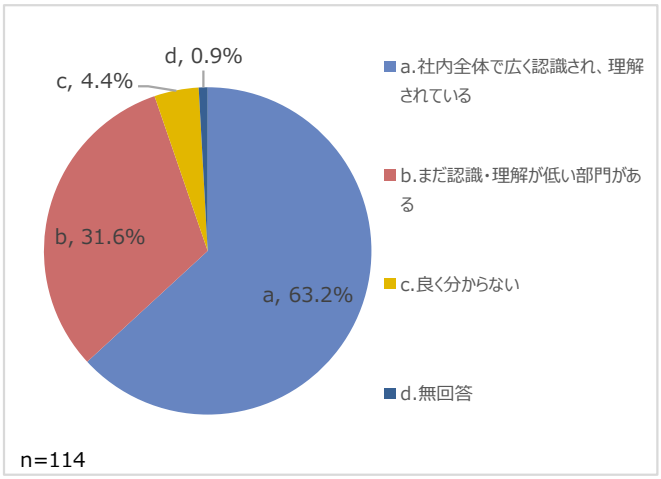


② 浸透度合い

次に、こうした経営層の意向が現場に伝わっているかを分析する。図 3-16 は、「サイバーセキュリティに対する取組の基本方針(サイバーセキュリティポリシー等)は社内全体で十分に認識・理解されていますか。」との問いに対する回答である。「a.社内全体で広く認識され、理解されている」とした企業が 60%超ある一方で、約 30%の企業が、「b.まだ認識・理解が低い部門がある」としている。

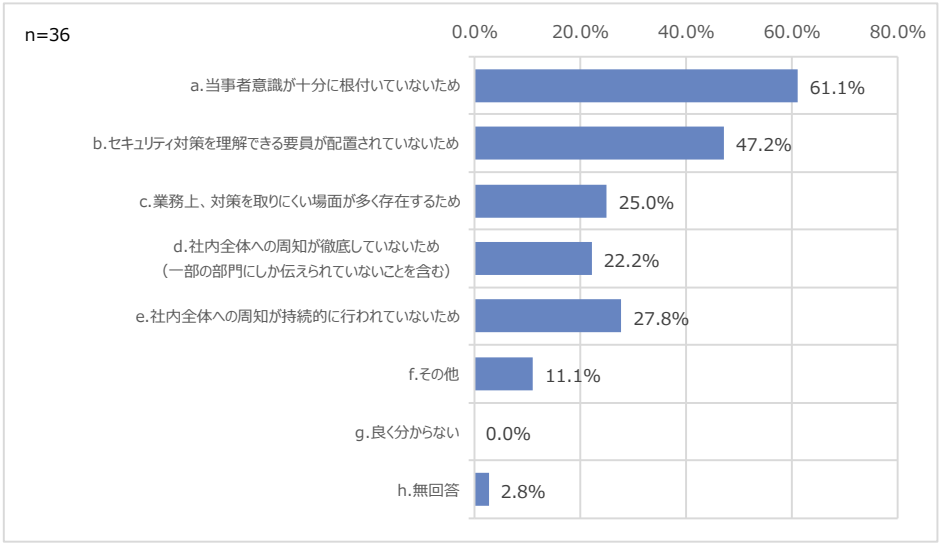
[4] 2017 年 12 月に公表された、一般社団法人日本経済団体連合会(経団連)による提言「Society 5.0 実現に向けたサイバーセキュリティの強化を求める」において、経団連が取り組むアクションプランとして掲げたもの。2018 年 3 月公表。http://www.keidanren.or.jp/policy/2018/018.pdf

図 3-16. 基本方針の社内への浸透度合い



「認識・理解が低い」背景を掘り下げたものが、図 3-17 である。認識や理解が低く留まっている理由を問うたもので、回答をみると、「a.当事者意識が十分に根付いていないため」とした企業が、最も多いことが分かる。サイバーセキュリティへの注目が大きく高まったのは近年であるが、自社、ないしは同業他社でサイバー攻撃の被害が起こらない限り、平常時に危機感を惹起しづらい可能性がある。

図 3-17. 認識や理解が低く留まる理由



次に多いのが、「b.セキュリティ対策を理解できる要員が配置されていないため」との回答である。詳細は、「③『戦略マネジメント層』の確保と育成」の項でも述べるが、予算の整備やツールの導入といったハード面だけでなく、人材配置や育成といったソフト面の整備も検討事項となる。

このほか、「d.社内全体への周知が徹底していないため」、「社内全体への周知が持続的に行われていないため」とした企業が一定割合存在することも注目される。サイバーセキュリティリスクに限定されるものではないが、継続して経営層が積極的に情報発信を行うことの大切さを窺わせる結果となった。

（エ）「戦略マネジメント層」の確保と育成

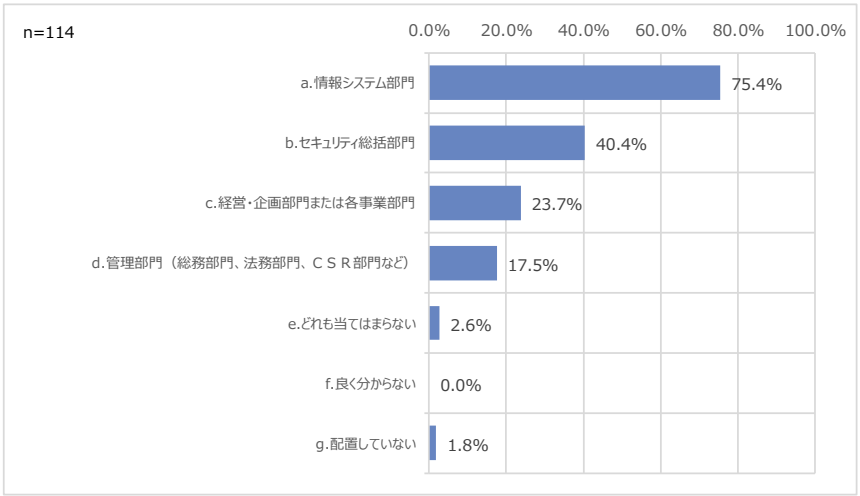
前節の図 3-17「認識や理解が低く留まる理由」の通り、「b.セキュリティ対策を理解できる要員が配置されていない」ことが、サイバーセキュリティに関する態勢整備において、相応のボトルネックとなっている。以下では、人材配置・育成の観点から、企業における現状と課題について深掘りを行いたい。

①「戦略マネジメント層」の担い手

図 3-18 は、サイバーセキュリティリスクへの対応につき、社内において重要となる「戦略マネジメント層」の担い手を示したものである。ここで、戦略マネジメント層とは、「経営層が示す経営戦略や事業戦略を実現するため、サイバーセキュリティに係るリスクを、管理すべきリスクの 1 つと捉え、運営の中心となる人材層」と定義する。具体的な業務としては、経営層が示した方針を踏まえた、サイバーセキュリティリスクへの対策立案、実務者層・技術者層の指揮、経営層への報告等がある。

図 3-18 をみると、担い手としては、「a.情報システム部門」が最も多く、次いで「セキュリティ総括部門」となっている。これまでの分析で、経営層と現場の距離が浮き彫りとなったが、担い手として期待される、事業部門や経営・企画部門は 23%程度とやや低い結果となっている。

図 3-18.「戦略マネジメント層」の担い手



これは、1 つの可能性を示唆している。すなわち、サイバーセキュリティリスクの所管部門が情報システムやセキュリティ統括部門と位置付けられており、同部門完結ないしは主導で、サイバーセキュリティリスクへの対応がなされるよう組織設計されている可能性である。これは、サイバーセキュリティリスクが最新かつ専門性を要する領域ゆえ、顕在化時に機動的な対応を行うため、相対的に親和性の高い部

門に必要人員を配置するという思想が背後にある可能性がある。

しかし、「戦略マネジメント層」の配置状況は変化しつつある。図 3-18 は、現場と経営の橋渡しを担うこととなる「戦略マネジメント層」の配置・確保方法を示したものである。「c.情報システム部門のマネジメントラインから配置転換している」と回答した企業が 70%超あることが確認できる。

サイバーセキュリティリスクは、最近認識されつつあるリスクカテゴリーである。習得には専門性を要する一方、全社的な影響を与えうることを鑑みれば、経営層に的確な情報を迅速に伝える人材を、経営層に近いところに配置する必要がある。こうした問題意識が「戦略マネジメント層」をめぐる人事施策に反映された可能性がある。

図 3-19.「戦略マネジメント層」の配置・確保方法

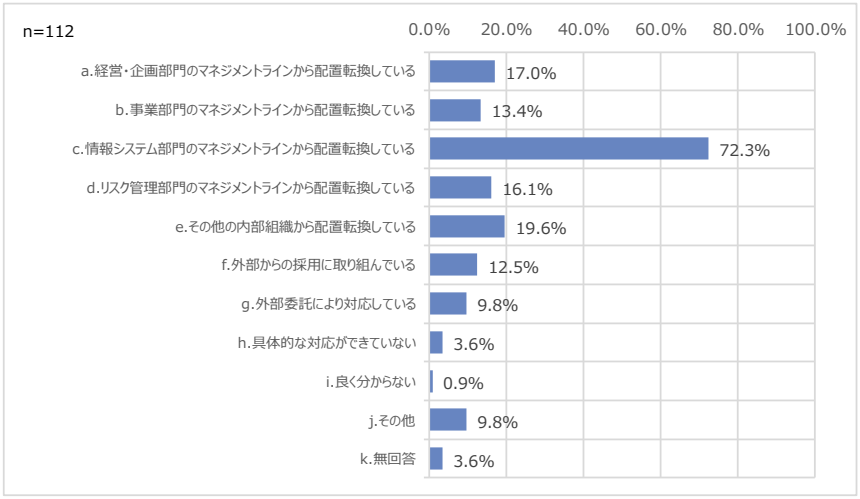
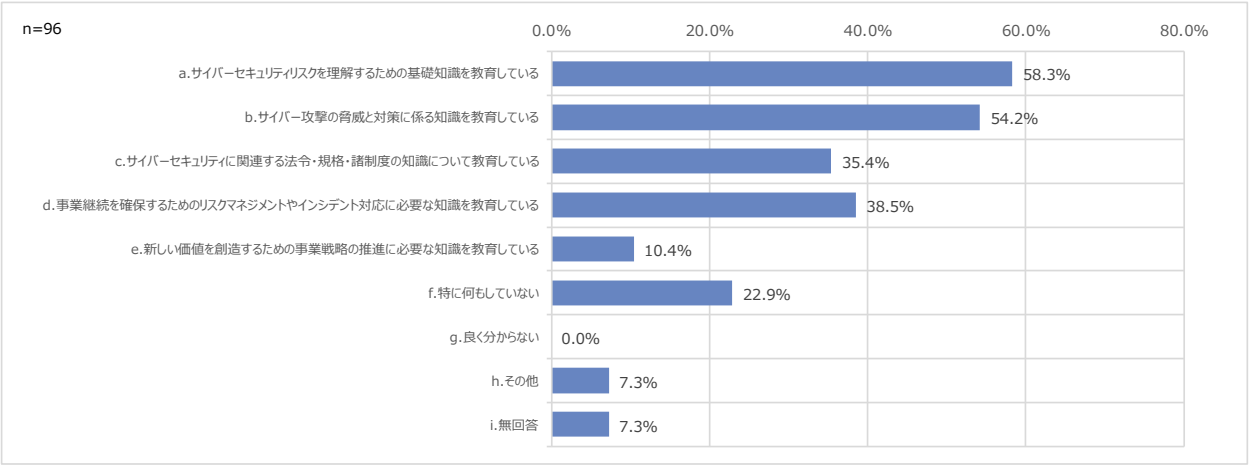


図 3-20 は、「戦略マネジメント層として着任する前に、どのような人材育成を実施していますか」との問いに対する回答を示したものである。

図 3-20.「戦略マネジメント層」の育成法



図をみると、「a.サイバーセキュリティリスクを理解するための基礎知識を教育している」、「b.サイバー攻撃の脅威と対策に係る知識を教育している」と回答した企業が 50%を超え、上位 1・2 位を占めていることが分かる。

但し、「d.事業継続を確保するためのリスクマネジメントやインシデント対応に必要な知識を教育している」との回答が、これに劣後していることには留意する必要がある。サイバーセキュリティリスクは、顕在化時の影響が大きいうえ、的確かつ迅速な対応が求められる。昨今の顕在化事象等鑑みると、基礎知識の教育を超え、実務対応もできる人材育成が急務である。

「戦略マネジメント層」は、専門性・リーダー・経営の 3 つを兼ね備えた人材が適任である。事業を統括し経営にも関与する事業部長の場合、現場でのリーダーとしての経験が活きる。

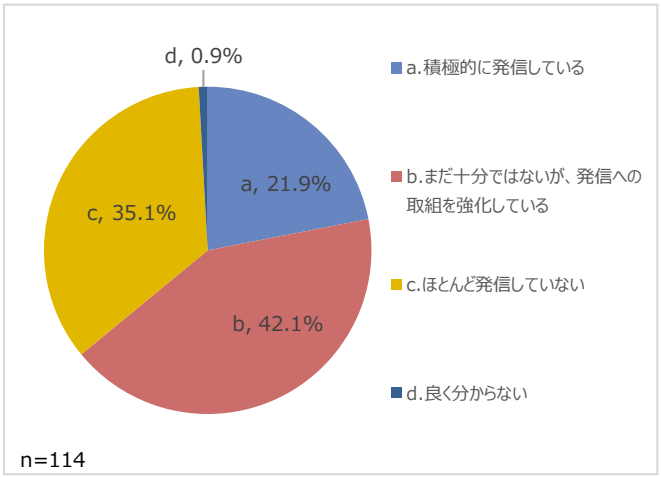
(オ) 社外への発信

これまでの節では、経営層の理解や関与、態勢整備にむけた姿勢や人材確保・育成等、「社内」に着目した整理を行った。本節では「社外」にむけた姿勢を整理する。

① 社外への発信

図 3-21 は、サイバーセキュリティに関する、社外への発信姿勢を示したものである。「a.積極的に発信している」、「b.まだ十分ではないが、発信への取組を強化している」とした企業が合わせて 65%程度観測されるものの、「c.ほとんど発信していない」と回答した企業が 35%程度ある等、二極化が窺える結果となった。

図 3-21. 社外への発信姿勢

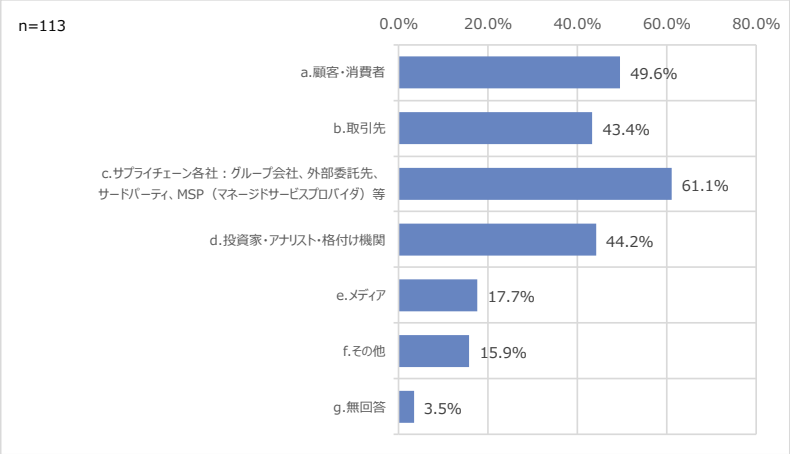


2 章「サイバーセキュリティ対策に係る情報発信内容の調査」でみた通り、開示の度合い・積極性は業種によって大きな相違がある。「c.ほとんど発信していない」とした企業群については、業界団体等の

積極的な関与等を検討していく必要がある。

次に、発信先について整理を行う。図表 3-22 は、「a. 積極的に発信している」、「b. まだ十分ではないが、発信への取組を強化している」、または「c. ほとんど発信していない」とした回答企業における発信先を示したものである。

図 3-22. 回答企業における発信先の分布



これをみると、多い順に、「c.サプライチェーン各社:グループ会社、外部委託先、サードパーティ、MSP(マネージドサービスプロバイダ)等」が 61.1%と最も多く、次いで、「a.顧客・消費者」(49.6%)、「d.投資家・アナリスト・格付け機関」(44.2%)、「b.取引先」(43.4%)となっていることが分かる。最近の潮流として、サイバーセキュリティリスクについては、サプライチェーンを想定した対応が重要となりつつあるが、当該結果はそれを裏付けるものとなっている。

但し、その対策はまだ十分ではない。図 3-23 は、「昨今、サプライチェーンを通じたサイバー攻撃が急激に深刻さを増しています。国内外の取引先を通じたサイバー攻撃(サーバ運用を委託する業者を踏み台とした攻撃等)等の脅威を認識して、仕様書にサイバーセキュリティ対策に関する項目を盛り込む等の対策を行っていますか」との問いに対する回答を示したものである。

これをみると、「a.脅威を認識し、対策を講じている」とした企業は 40%程度あるものの、60%弱の企業では、「c.脅威を認識しているが、対策は十分でない」としている。国や企業、業種・業態を跨いだ取引が増える中、ネットワークシステムの脆弱性を襲う高度なサイバー攻撃を想定した対応については、いまだ不十分と認識する企業は多い。

図 3-23. サプライチェーンを想定した対応の度合い

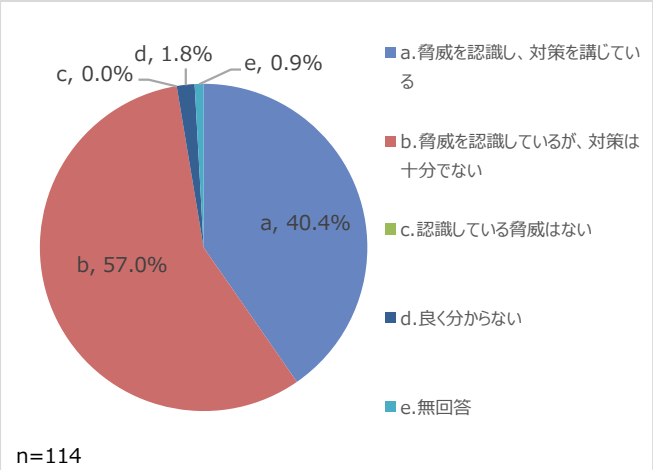
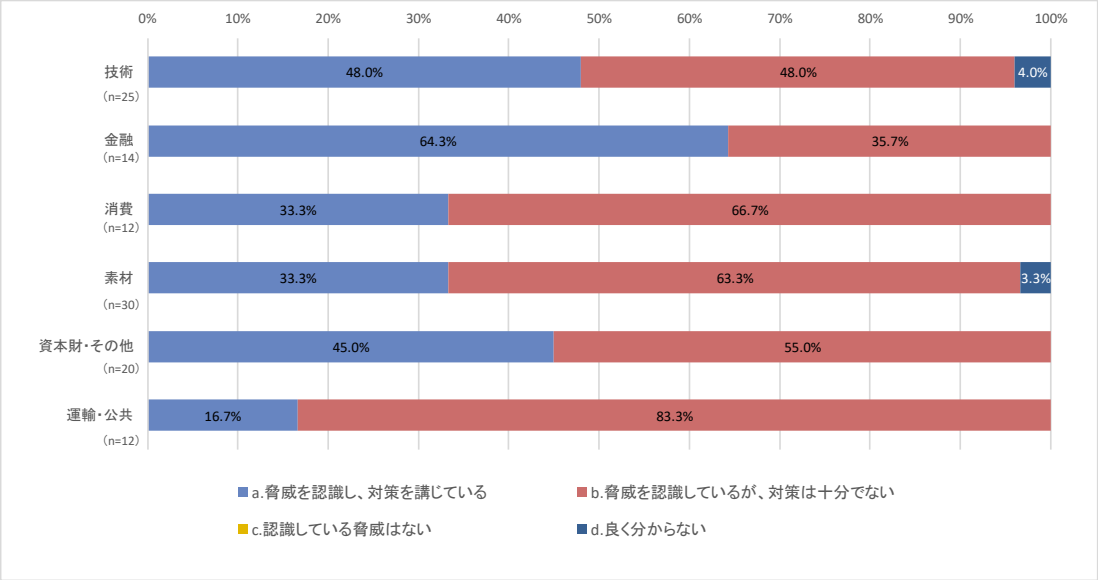


図 3-24. 業種別にみた対応の度合い

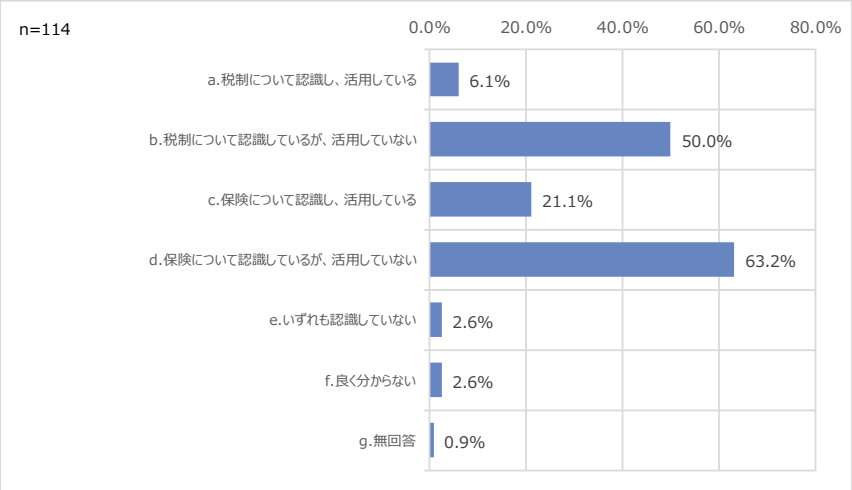


(カ) 税制優遇やサイバーセキュリティ保険に対する認識

今回調査では、サイバーセキュリティリスクへの対応にかかる行政支援や金融インフラについても質問を行った。取り上げたのは情報連携投資等促進税制、およびサイバーセキュリティ保険の 2 つである。

情報連携投資等促進税制とは、サイバーセキュリティ対策を取ることで税制優遇が受けられるもの、また、サイバーセキュリティ保険とは、損害補填(損害賠償、訴訟、復旧、調査等の費用を補填するもの)やインシデント対応支援を提供してくれる保険を指す。これらについての認識や活用の有無について質問を行った。回答は、図 3-24 の通りである。結果として、「b.税制について認識しているが、活用していない」、「d.保険について認識しているが、活用していない」がいずれも 50%を上回っていることが分かった。

図 3-25. 情報連携投資等促進税制・サイバーセキュリティ保険の認知・活用の有無



(4) まとめ

アンケートでは、サイバーセキュリティに対する経営層の理解・関与に始まり、「戦略マネジメント層」の確保や育成、社外への発信等、幅広い分野につき、主要企業へ調査を行った。

アンケートからは、①サイバーセキュリティリスクに対する経営層の理解は十分あるものの、②経営会議・取締役会等での報告・議論の頻度の観点では、不十分なところが見受けられること、③サイバーセキュリティインシデントに対する経営層の関与度合いには改善の余地があること、④「戦略マネジメント層」の確保・育成は途上にあり、必ずしも適性が理解されていないこと、⑤社外への発信は強化されているが、サプライチェーンを想定した対応は今後の課題であること等が確認された。

次章第 1 節では、第 2 章で取り上げた開示状況とアンケート結果について、関係性の有無・程度につき、考察を行う。

4　複合的な分析

(1) 記載の深度とアンケートでの回答の関係性

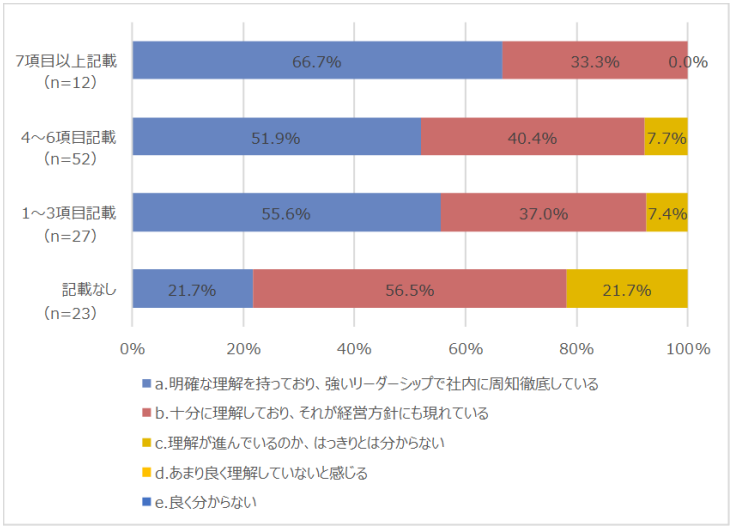
本節では、サイバーセキュリティリスクに関する企業の発信と取組姿勢の関係性について分析する。具体的には、第 2 章で取り上げた有価証券報告書での記載の深度別に、アンケートでの回答を比較・考察する。

(ア) 経営層の理解

図 4-1 は、第 2 章 図 2-5 で取り上げた、「経営層は、事業の鍵を握る重要な情報やデータは何か、またこれらの情報が貴社・競合他社・犯罪者にとってどれほどの価値があるかについてよく理解していますか」との問いに対する回答である。

図の通り、有価証券報告書にて 7 項目以上記載のあった企業は、サイバーセキュリティリスクにつき記載のなかった企業よりも、「a.明確な理解を持っており、強いリーダーシップで社内に周知徹底している」と回答した企業が多い(それぞれ 21.7%、66.7%)。

図 4-1. 有価証券報告書における記載の深度別にみた経営層の理解

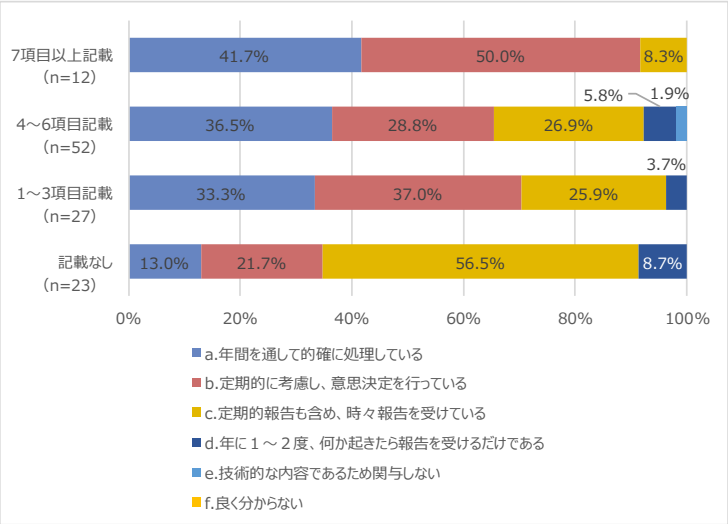


(イ) 経営層の関与

図 4-2 は、第 2 章 図 2-7 で取り上げた、「サイバーセキュリティに対する経営層の関与の度合いについて、最も良く当てはまる記述はどれですか」との問いに対する回答である。

図の通り、「a.最も重要な議題として、毎回取り上げている」と回答した企業は、有価証券報告書にてサイバーセキュリティリスクにつき言及のあった企業ほど、割合が高い。具体的には、「a.年間を通して的確に処理している」「b.定期的に考慮し、意思決定を行っている」と回答した企業の割合は、「7 項目以上記載」は、「記載なし」の 3 倍弱になった。

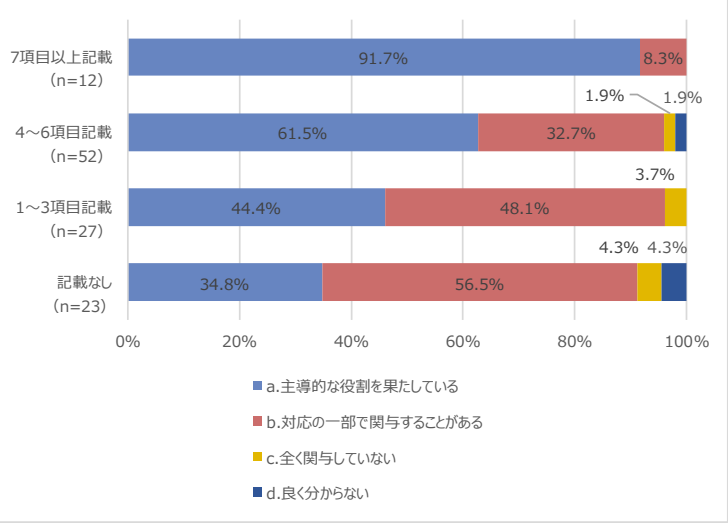
図 4-2. 有価証券報告書における記載の深度別にみた経営層の関与



同様の傾向は、図 3-10「経営層は、率先してサイバーセキュリティインシデントへの対応に関与していますか」との問いに対する回答についても確認できる(図 4-3)。

図の通り、「a.最も重要な議題として、毎回取り上げている」と回答した企業は、有価証券報告書にてサイバーセキュリティリスクにつき言及のあった企業ほど、割合が高い。「a.主導的な役割を果たしている」「b.対応の一部で関与することがある」を合計した割合についてみると、「7 項目以上記載」のあった企業の割合は、「記載なし」の企業の 3 倍近くとなった。

図 4-3. 記載の深度別にみたサイバーセキュリティインシデントに対する経営層の関与



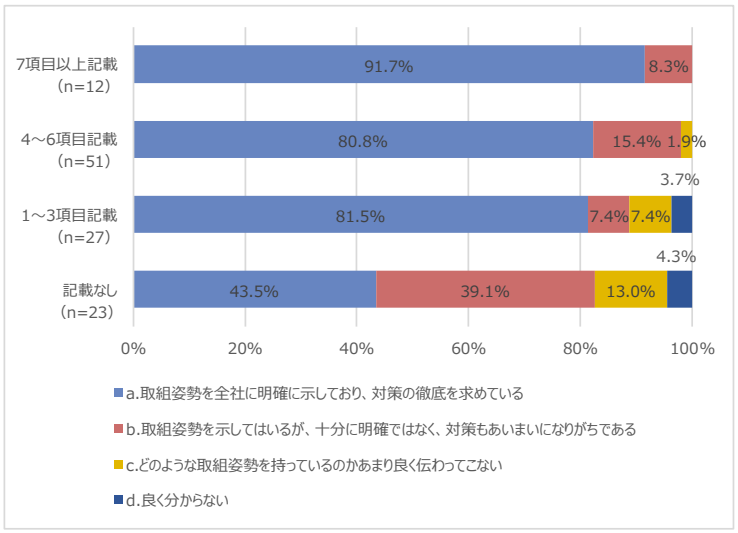
(ウ) 態勢整備にむけた姿勢

図 4-4 は、図 3-12 で取り上げた、「経営層は、現在の事業及びこれからのデジタル変革への対応において、サイバーセキュリティリスク対策への取組姿勢をどれほど明確に示していますか」との問いに対する回答

を同じく、記載の深度別にみたものである。

これまでの結果と同様に、記載の深度が高い企業ほど、「a.」、ないし「b.」と回答している。

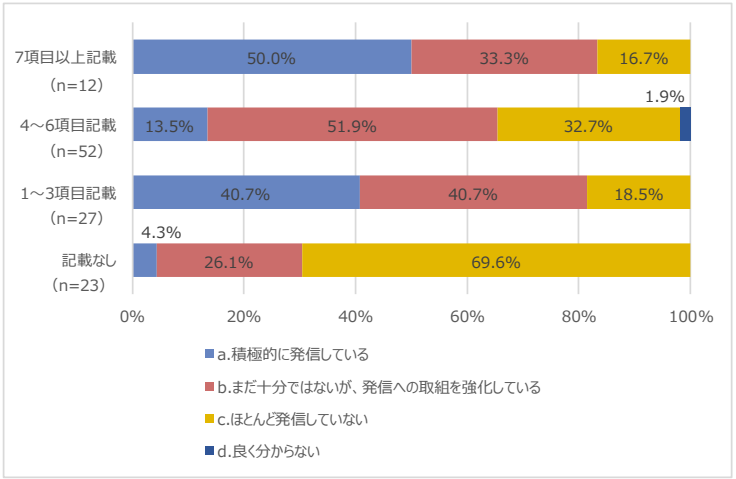
図 4-4. 記載の深度別にみた経営層の取組姿勢の明確度合い



(エ) 社外への発信

図 4-5 は、図 3-21 で取り上げた、「サイバーセキュリティに関する情報を、社外に積極的に発信していますか」との問いに対する回答を同じく、記載の深度別にみたものである。「a.」・「b.」については、項目の多寡で相関の度合いは若干低下したが、「c.ほとんど発信していない」との回答について、「7 項目以上記載」のあった企業は、「記載なし」の企業よりも遥かに少ない。

図 4-5. 記載の深度別にみた社外への発信姿勢



(オ) まとめ

本分析では、経営層の理解、経営層の関与、態勢整備、社外への発信、いずれについても、有価証券報告書等での記載情報が多い企業ほど、取組が先行、ないしは積極的であることが観測された。

因果関係としては、サイバーセキュリティリスクへの問題意識が高い企業ほど、取組が先行しており、高い問題意識から、ステークホルダーへの発信が充実しているという関係が想定される。

リスク管理において、サイバーセキュリティリスクへの関心は、急速に高まりつつある。ERM(全社的リスク管理)の観点だけでなく、並行してステークホルダーへの発信を強化させることが、当該企業の社会的評価を高め、ひいては社会全体のコスト低減につながるものと考える。

(2) 海外先行調査との比較

複合的な分析の 2 つ目の視点として、本節では、海外先行調査との比較を試みる。具体的には、英国の株価指数である、FTSE350 種総合株価指数に採用された企業におけるサイバーセキュリティリスクへの取組姿勢につき、年次で公表される「FTSE 350 Cyber Governance Health Check」を取り上げる。

(ア)「FTSE 350 Cyber Governance Health Check」とは

「FTSE 350 Cyber Governance Health Check」とは、FTSE350 種総合株価指数に採用された企業におけるサイバーセキュリティリスクへの取組姿勢を、同指数に採用された企業経営陣に対し行ったアンケートから整理したものである。実施主体は、英国 NCSC(National Cyber Security Centrum)であり、2013 年以降、これまで 5 回実施された。今回取り上げる第 5 回目の調査は、2018 年に実施された。

(イ) 2018 年度調査の主な結果

今回調査での主な結果は、以下の 11 項目である[5]。

① サイバーの脅威にかかるリスクについて、高い、ないしは非常に高いと回答した経営層の割合はかつてなく多い

② 速度は十分でないものの、事業上の重要な情報やデータ資産、システムに対する経営層の理解は向上が続く

③ 包括的に理解する経営層は少ないものの、サイバーの脅威に伴う損失や破壊(disruption)の影響に対する理解は継続して改善

④ サイバーの脅威や想定される影響につき、より包括的に理解する経営層は、密度のあるサイバーガ

[5] 「FTSE 350 Cyber Governance Health Check 2018」よりエヌ・ティ・ティ・データ経営研究所抄訳

バナンス(cyber governance)を実践

⑤ 経営層が得る情報が包括的なものと考える企業はやや少ないものの、多くは、得る情報を最新かつ広範と考えている

⑥ 最高情報セキュリティ責任者(CISO)が経営層に直接報告する企業においては、得た情報につき、経営層が包括的と回答する度合いが高い

⑦ サイバーセキュリティは、企業にとって戦略的な検討事項(strategic issue)とますます見られている

⑧ GDPR(General Data Protection Regulation; EU 一般データ保護規則)は、サイバーセキュリティに関連する事項について、経営層の取組(engagement)を高い水準で促進

⑨ 政府によるアドバイスは、FTSE350 に属する企業の経営陣にとって最も共通した情報源となっている

⑩ 多くは外部の監査は受けていないものの、サイバー・インシデントに対する計画を殆どの企業が保有

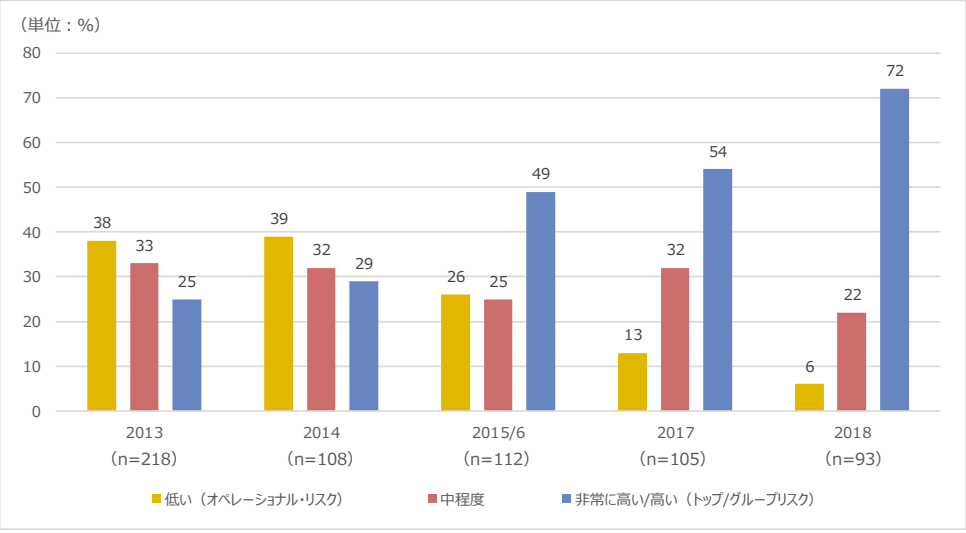
⑪ サプライチェーンは、サイバー攻撃の標的にますますなっているが、サプライチェーンにおけるサイバー・リスクについての認識は、事業において多くの割合で、甚大なギャップ(significant gap)があるように見受けられる

本節では、上記のうち、①経営層の理解、④サイバーガバナンス、⑥CISO、⑩サイバー・インシデント・プランの 4 つを取り上げる。

① 経営層の理解

図 4-6 は、サイバーセキュリティリスクに対する経営層の理解の度合いについて、2013 年からの暦年調査の結果を記したものである。

図 4-6. サイバーセキュリティリスクに対する経営層の理解(2013～2018)

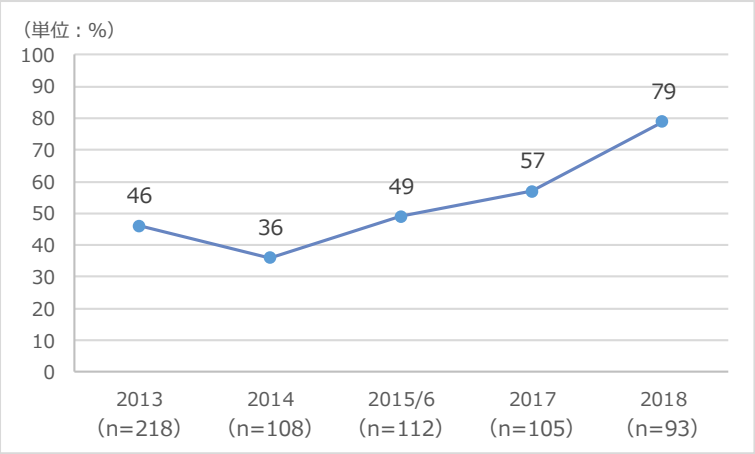


(出所)「FTSE 350 Cyber Governance Health Check 2018」

図をみると、①トップリスク、ないしはグループのリスクとして、「非常に高い」、もしくは「高い」と回答した企業が、2013 年には 25%であったが、2018 年には 72%まで増加、②並行して、「低い(オペレーショナルリスク)」としていた企業が、2013 年の 38%から 2018 年には 6%まで低下したことが確認できる。

また、サイバーセキュリティリスクが、顧客や評判、短期的な株価に影響を与えると理解する経営層の割合の推移が図表 4-7 である。

図 4-7. 顧客や評判、短期的な株価へ影響を与えることの理解(2013～2018)



(出所)「FTSE 350 Cyber Governance Health Check 2018」

英国においても、日本と同様にサイバーセキュリティリスクに対する経営層の理解が深まっていることが確認できる。

④ サイバーガバナンス

図 4-8 は、サイバー戦略(Cyber Strategy)の整備度合いについての回答の分布である。図の通り、「事業目的に即したリスク・ベースのサイバー戦略を策定」している企業が 6 割弱になるほか(凡例 青、赤)全体の約 4 割が、個別の予算を有している(凡例 青)。

図 4-8. サイバー戦略の策定状況（2018）

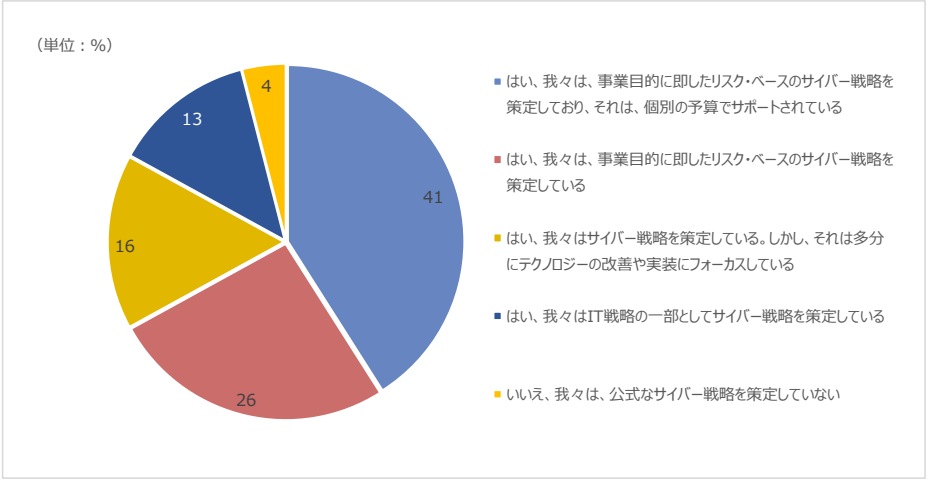
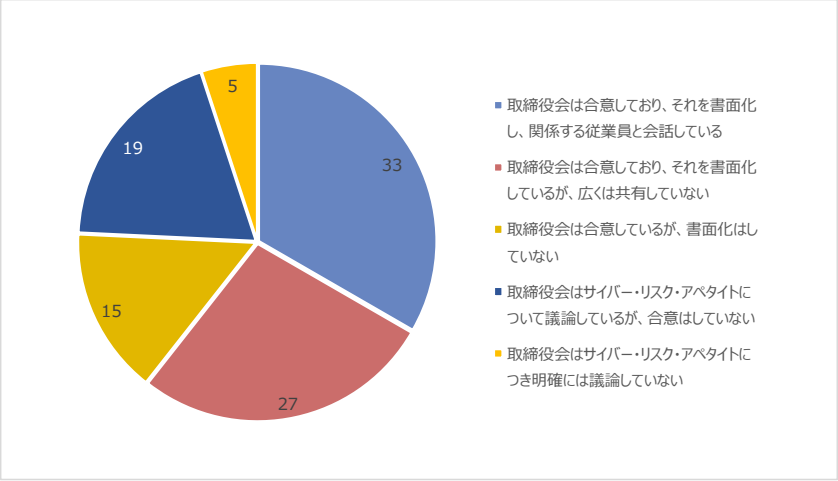


図 4-9 は、サイバーセキュリティリスクについてのリスク・アペタイト設定状況である。リスク・アペタイトとは、「戦略目的や事業計画達成のために、自社のリスク許容度の範囲で進んで受け入れるべきリスクの種類と総量」等と称され[6]、それを取り入れた経営管理の枠組みは、リスク・アペタイト・フレームワーク（RAF）として、金融危機をうけ浸透しつつある。

これをみると、サイバーセキュリティリスクについて、既に書面化し、従業員と会話している企業が 3 割強あることが分かる。日本において RAF は金融機関の大手等ごく一部で浸透しているのみであるため、既に導入している企業が英国では相応にあることは注目に値する。

図 4-9. リスク・アペタイトの設定状況（2018）



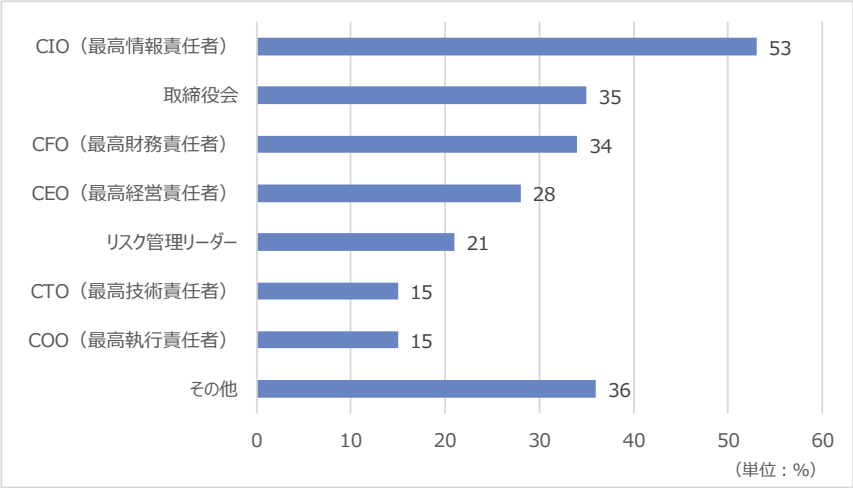
[6] FSB（金融安定理事会）等の定義を参照。

⑥ CISO

英国 NCSC（National Cyber Security Centrum）は、CISO（最高情報セキュリティ責任者）を、企業において最も重要な人材の 1 つと考えており、可能であれば、CISO が直接、CEO ないしは取締役会にて直接報告することを推奨している。

図 4-10 は、CISO の定期的な報告先を示したものである。複数回答ではあるが、主な報告先は、CIO（最高情報責任者）となっており、CEO や取締役会と回答した企業は、これに続く形に留まっていることが分かる。

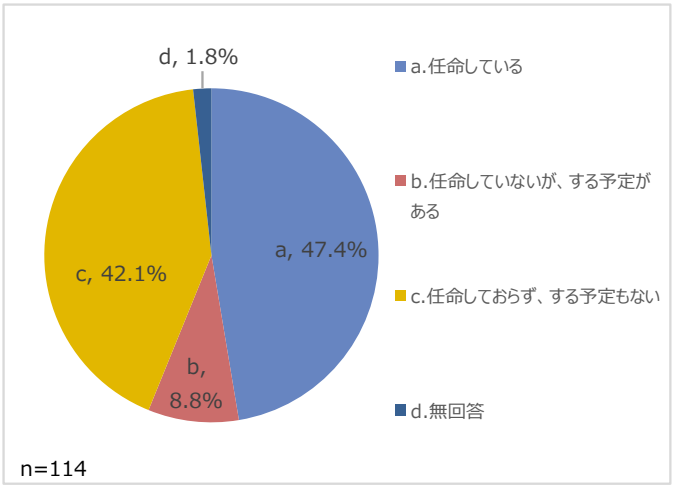
図 4-10. CISO の定期的な報告先（2018）



（出所）「FTSE 350 Cyber Governance Health Check 2018」

転じて日本では、CISO を設置していない、日経 225 等の企業が、アンケートの回答からは 40%強存在する（図 4-11）。英国 NSNC は FTSE350 企業の取組に改善の余地があるとしているが、わが国では、その段階に到達していない。

図 4-11. アンケートからみた日本における CISO 設置状況(2018)

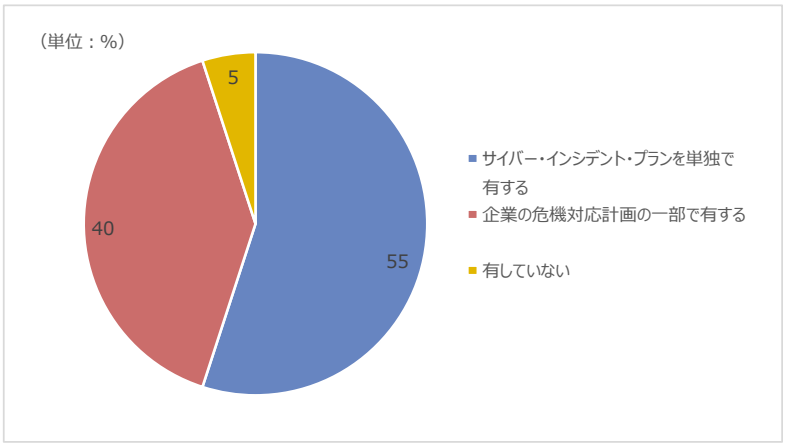


(出所)「FTSE 350 Cyber Governance Health Check 2018」

⑩ サイバー・インシデント・プラン

図 4-12 はサイバー・インシデントについて対応計画を有しているかどうかについての回答である。

図 4-12. サイバー・インシデント・プランの設置状況(2018)



(出所)「FTSE 350 Cyber Governance Health Check 2018」

これをみると、55%の企業がサイバー・インシデントにつき、単独(standalone)の対応計画を有しているとし、危機対応計画の 1 つとした企業(40%)を上回っていることが分かる。

日本においては、図 3-10 にて回答企業のうち、過半が、サイバー・インシデントにつき、「経営層が主導的な役割を果たしている」としていたが、今後は、単独のサイバー・インシデント・プランを策定の上、経営層が主導して、サイバーセキュリティリスクへの対応に関与する必要があると考える。

(ウ) まとめ

本節では、先行する英国調査より、サイバーセキュリティリスクに関する現地の対応状況について概観した。共通点としては、サーバーセキュリティリスクに対する経営層の理解が高まっていること、相違点としては、リスクガバナンスや、CISO の設置等態勢面で、英国は、日本を大きく先行していること等がある。

但し、調査を実施した英国 NCSC は、一層の改善が必要としている[7]。我が国においては、有価証券報告書等で記載の深度が高い金融や消費、運輸・公共等が先導する形で、サイバーセキュリティリスクに対する態勢を整備しつつ、例えば行政との対話を促すことで全体の底上げを図ることが実現可能性のある展開戦略と考える。

[7] 「UK Boards of biggest firms must do more to be cyber aware」(2019/3/5)
(https://www.gov.uk/government/news/uk-boards-of-biggest-firms-must-do-more-to-be-cyber-aware)

5　総評

本調査では、有価証券報告書、およびコーポレートガバナンス報告書における発信内容を、記載の有無からその詳細度、項目別・業種別にみた分析に始まり、実態を探るためのアンケート調査の整理、最後に複合的な分析として、開示度合いとアンケートの回答結果との関係性の分析、海外先行調査との傾向比較を実施した。

結果としては、以下を指摘することができる。

① サイバーセキュリティリスクに関する開示比率は高まっているものの、業種によりばらつきがある

② 有価証券報告書と比べると、コーポレートガバナンス報告書での開示は遅れがあるが、急速に記載企業が増えている

③ 開示内容では、固有リスク、残存リスクに関する記載はあるものの、具体的な低減策を記した企業は限られる

④ サイバーセキュリティリスクへの経営層の理解・関与は高いが、経営会議体での議論・運営等、組織的な意思決定には課題が残る

⑤ 態勢整備にかかる経営層の意向は強いものの、現場での意識づけ・態勢整備は強化の余地がある

⑥ 人材面では、引き続き「戦略マネジメント層」の育成が求められる

⑦ サプライチェーンを想定した対応は、拡充の余地がある

⑧ 有価証券報告書での記載の深度が高い企業ほど、サイバーセキュリティリスクへの取組が充実している

⑨ 英国では、リスク管理も含めたサイバーガバナンスが強化されている

本節では、このうち⑧と⑨について補記したい。

第 4 章 1 節では、サイバーセキュリティリスクに対する取組と発信姿勢に一定の相関があることが確認された。因果関係としては、同節最終部で触れた通り、サイバーセキュリティリスクへの問題意識が高い企業ほど、態勢整備が強化され、結果として、ステークホルダーへの発信の詳細度も高まるという相関が見られる。

サイバーセキュリティリスクに関する発信の高まりの背景としては、経営者の問題意識の高まりのほか、数値で現れない「非財務情報」への投資家の関心は高まりが想定される。リスク管理の分野でも、サイバーセキュリティリスクを含む「非財務リスク」の管理は急務となっている。リスク認識を含めた発信は、投資家をはじめとするステークホルダーへの配慮が背後にあると想定される。この観点では、第 4 章 2 節で取り上げた英国では、事業会社も含め、サイバーセキュリティに対するリスク・アペタイトの設定、フレームワーク（RAF）による管理が、進んでいることに注目する必要がある。

本文で指摘した通り、わが国での RAF 構築は、一部大手の金融機関に留まっているが、顕在化した際のインパクトが極めて大きいサイバーセキュリティリスクについては、損失を最小限に抑えるだけの態勢整備が金融機関

に限らず、急務である。経営層と現場の意思疎通を円滑にし、的確な意思決定・戦略策定のためにも、第 3 章で取り上げた「戦略マネジメント層」の育成は不可欠である。我が国においては、例えば、金融や消費、運輸・公共といった、開示先行業種の取組を参考にしつつ、行政・業界団体との対話を通し、サイバーセキュリティリスクに対し、企業全体の態勢整備、対応レベルの底上げを図っていくことが今後の施策として想定される。

6　資料編

(1)　業種別にみた日経225企業の記載状況（有価証券報告書）

日経業種分類		平成28年10月時点の日経225企業：平成28年度(2017年3月期)報告書													
大分類	中分類委	大分類社数	中分類社数	該当企業数		開示企業%		記載レベル							
								記載なし		1～3項目記載		4～6項目記載		7項目以上記載	
				中分類	大分類	中分類	大分類	中分類	大分類	中分類	大分類	中分類	大分類	中分類	大分類
A.技術	01.医薬品		9	7		77.8%		2		6		1		0	
	02.電気機器		27	20		74.1%		7		9		10		1	
	03.自動車	57	10	8	44	80.0%	77.2%	2	13	4	21	4	20	0	3
	04.精密機器		5	3		60.0%		2		0		3		0	
	05.通信		6	6		100.0%		0		2		2		2	
B.金融	06.銀行		11	11		100.0%		0		4		5		2	
	07.その他金融	21	1	1	21	100.0%	100.0%	0	0	0	9	1	9	0	3
	08.証券		3	3		100.0%		0		2		1		0	
	09.保険		6	6		100.0%		0		3		2		1	
C.消費	10.水産		2	1		50.0%		1		0		1		0	
	11.食品	30	11	10	27	90.9%	90.0%	1	3	3	9	7	17	0	1
	12.小売業		8	8		100.0%		0		3		5		0	
	13.サービス		9	8		88.9%		1		3		4		1	
D.素材	14.鉱業		1	0		0.0%		1		0		0		0	
	15.繊維		4	1		25.0%		3		1		0		0	
	16.パイプ・紙		3	0		0.0%		3		0		0		0	
	17.化学		18	6		33.3%		12		2		4		0	
	18.石油	60	2	2	27	100.0%	45.0%	0	33	1	13	1	14	0	0
	19.ゴム		2	1		50.0%		1		0		1		0	
	20.窯業		8	4		50.0%		4		2		2		0	
	21.鉄鋼		4	1		25.0%		3		1		0		0	
	22.非鉄金属製品		11	7		63.6%		4		4		3		0	
	23.商社		7	5		71.4%		2		2		3		0	
E.資本財・その他	24.建設		9	6		66.7%		3		3		3		0	
	25.機械		18	10		55.6%		8		4		6		0	
	26.造船	37	2	2	22	100.0%	59.5%	0	15	1	8	1	14	0	0
	27.その他製造		3	3		100.0%		0		0		3		0	
	28.不動産		5	1		20.0%		4		0		1		0	
F.運輸・公共	29.鉄道・バス		8	7		87.5%		1		0		7		0	
	30.陸運		2	2		100.0%		0		1		1		0	
	31.海運		3	1		33.3%		2		1		0		0	
	32.空運	20	1	1	17	100.0%	85.0%	0	3	0	5	1	12	0	0
	33.倉庫		1	1		100.0%		0		1		0		0	
	34.電力		3	3		100.0%		0		1		2		0	
	35.ガス		2	2		100.0%		0		1		1		0	

日経業種分類		平成29年10月時点の日経225企業：平成29年度(2018年3月期)報告書													
大分類	中分類	大分類社数	中分類社数	該当企業数		開示企業%		記載レベル							
								記載なし		1～3項目記載		4～6項目記載		7項目以上記載	
				中分類	大分類	中分類	大分類	中分類	大分類	中分類	大分類	中分類	大分類	中分類	大分類
A.技術	01.医薬品	57	9	8	47	88.9%	82.5%	1	10	7	20	1	24	0	3
	02.電気機器		27	21		77.8%		6		10		11		0	
	03.自動車		10	9		90.0%		1		1		7		1	
	04.精密機器		5	3		60.0%		2		0		3		0	
	05.通信		6	6		100.0%		0		2		2		2	
B.金融	06.銀行	21	11	11	21	100.0%	100.0%	0	0	3	7	1	6	7	8
	07.その他金融		1	1		100.0%		0		1		0		0	
	08.証券		3	3		100.0%		0		1		2		0	
	09.保険		6	6		100.0%		0		2		3		1	
C.消費	10.水産	32	2	1	29	50.0%	90.6%	1	3	0	9	1	17	0	3
	11.食品		11	10		90.9%		1		1		9		0	
	12.小売業		8	8		100.0%		0		2		6		0	
	13.サービス		11	10		90.9%		1		6		1		3	
D.素材	14.鉱業	59	1	0	32	0.0%	54.2%	1	27	0	9	0	22	0	1
	15.繊維		4	3		75.0%		1		1		2		0	
	16.パイプ・紙		2	0		0.0%		2		0		0		0	
	17.化学		18	7		38.9%		11		2		5		0	
	18.石油		2	2		100.0%		0		1		1		0	
	19.ゴム		2	1		50.0%		1		0		1		0	
	20.窯業		8	5		62.5%		3		1		4		0	
	21.鉄鋼		4	2		50.0%		2		1		0		1	
	22.非鉄金属製品		11	7		63.6%		4		2		5		0	
	23.商社		7	5		71.4%		2		1		4		0	
E.資本財・その他	24.建設	36	9	5	21	55.6%	58.3%	4	15	2	7	3	14	0	0
	25.機械		17	9		52.9%		8		3		6		0	
	26.造船		2	2		100.0%		0		1		1		0	
	27.その他製造		3	3		100.0%		0		0		3		0	
	28.不動産		5	2		40.0%		3		1		1		0	
F.運輸・公共	29.鉄道・バス	20	8	7	17	87.5%	85.0%	1	3	0	3	5	11	2	3
	30.陸運		2	2		100.0%		0		0		2		0	
	31.海運		3	1		33.3%		2		1		0		0	
	32.空運		1	1		100.0%		0		0		1		0	
	33.倉庫		1	1		100.0%		0		1		0		0	
	34.電力		3	3		100.0%		0		0		2		1	
	35.ガス		2	2		100.0%		0		1		1		0	

(2) 業種別にみた日経225企業の記載状況(コーポレートガバナンス報告書)

日経業種分類		平成28年10月時点の日経225採用銘柄 :平成28年度(2016/4～2017/3に発行分のうち最新)報告書													
大分類	中分類	大分類社数	中分類社数	該当企業数		開示企業%		記載レベル							
								記載なし		1項目記載		2～3項目記載		4項目以上記載	
				中分類	大分類	中分類	大分類	中分類	大分類	中分類	大分類	中分類	大分類	中分類	大分類
A.技術	01.医薬品	57	9	5	14	55.6%	24.6%	4	43	0	0	5	13	0	1
	02.電気機器		27	5		18.5%		22		0		5		0	
	03.自動車		10	2		20.0%		8		0		2		0	
	04.精密機器		5	2		40.0%		3		0		1		1	
	05.通信		6	0		0.0%		6		0		0		0	
B.金融	06.銀行	21	11	1	3	9.1%	14.3%	10	18	0	0	1	3	0	0
	07.その他金融		1	0		0.0%		1		0		0		0	
	08.証券		3	0		0.0%		3		0		0		0	
	09.保険		6	2		33.3%		4		0		2		0	
C.消費	10.水産	30	2	0	7	0.0%	23.3%	2	23	0	1	0	4	0	2
	11.食品		11	2		18.2%		9		0		2		0	
	12.小売業		8	0		0.0%		8		0		0		0	
	13.サービス		9	5		55.6%		4		1		2		2	
D.素材	14.鉱業	60	1	1	14	100.0%	23.3%	0	46	0	3	0	10	1	1
	15.繊維		4	1		25.0%		3		0		1		0	
	16.パイプ・紙		3	0		0.0%		3		0		0		0	
	17.化学		18	5		27.8%		13		1		4		0	
	18.石油		2	1		50.0%		1		0		1		0	
	19.ゴム		2	0		0.0%		2		0		0		0	
	20.窯業		8	1		12.5%		7		0		1		0	
	21.鉄鋼		4	2		50.0%		2		1		1		0	
	22.非鉄金属製品		11	1		9.1%		10		0		1		0	
	23.商社		7	2		28.6%		5		1		1		0	
E.資本財・その他	24.建設	37	9	4	10	44.4%	27.0%	5	27	0	1	4	9	0	0
	25.機械		18	5		27.8%		13		1		4		0	
	26.造船		2	0		0.0%		2		0		0		0	
	27.その他製造		3	1		33.3%		2		0		1		0	
	28.不動産		5	0		0.0%		5		0		0		0	
F.運輸・公共	29.鉄道・バス	20	8	1	2	12.5%	10.0%	7	18	0	0	1	2	0	0
	30.陸運		2	0		0.0%		2		0		0		0	
	31.海運		3	0		0.0%		3		0		0		0	
	32.空運		1	0		0.0%		1		0		0		0	
	33.倉庫		1	0		0.0%		1		0		0		0	
	34.電力		3	0		0.0%		3		0		0		0	
	35.ガス		2	1		50.0%		1		0		1		0	

日経業種分類		平成29年10月時点の日経225採用銘柄 :平成29年度(2017/4～2018/3に発行分のうち最新)報告書													
大分類	中分類	大分類社数	中分類社数	該当企業数		開示企業%		記載レベル							
								記載なし		1項目記載		2～3項目記載		4項目以上記載	
				中分類	大分類	中分類	大分類	中分類	大分類	中分類	大分類	中分類	大分類	中分類	大分類
A.技術	01.医薬品	57	9	6	25	66.7%	43.9%	3	32	0	0	6	23	0	2
	02.電気機器		27	9		33.3%		18		0		9		0	
	03.自動車		10	2		20.0%		8		0		2		0	
	04.精密機器		5	3		60.0%		2		0		2		1	
	05.通信		6	5		83.3%		1		0		4		1	
B.金融	06.銀行	21	11	3	6	27.3%	28.6%	8	15	0	0	3	6	0	0
	07.その他金融		1	0		0.0%		1		0		0		0	
	08.証券		3	0		0.0%		3		0		0		0	
	09.保険		6	3		50.0%		3		0		3		0	
C.消費	10.水産	32	2	1	14	50.0%	43.8%	1	18	0	1	1	11	0	2
	11.食品		11	5		45.5%		6		0		5		0	
	12.小売業		8	2		25.0%		6		1		1		0	
	13.サービス		11	6		54.5%		5		0		4		2	
D.素材	14.鉱業	59	1	1	20	100.0%	33.9%	0	39	0	2	0	17	1	1
	15.繊維		4	1		25.0%		3		0		1		0	
	16.パイプ・紙		2	0		0.0%		2		0		0		0	
	17.化学		18	6		33.3%		12		2		4		0	
	18.石油		2	1		50.0%		1		0		1		0	
	19.ゴム		2	1		50.0%		1		0		1		0	
	20.窯業		8	1		12.5%		7		0		1		0	
	21.鉄鋼		4	1		25.0%		3		0		1		0	
	22.非鉄金属製品		11	5		45.5%		6		0		5		0	
	23.商社		7	3		42.9%		4		0		3		0	
E.資本財・その他	24.建設	36	9	4	16	44.4%	44.4%	5	20	0	1	4	15	0	0
	25.機械		17	8		47.1%		9		1		7		0	
	26.造船		2	0		0.0%		2		0		0		0	
	27.その他製造		3	2		66.7%		1		0		2		0	
	28.不動産		5	2		40.0%		3		0		2		0	
F.運輸・公共	29.鉄道・バス	20	8	2	5	25.0%	25.0%	7	16	0	1	1	3	0	0
	30.陸運		2	0		0.0%		2		0		0		0	
	31.海運		3	1		33.3%		2		0		1		0	
	32.空運		1	0		0.0%		1		0		0		0	
	33.倉庫		1	0		0.0%		1		0		0		0	
	34.電力		3	1		33.3%		2		1		0		0	
	35.ガス		2	1		50.0%		1		0		1		0	

(3) 業種別にみた開示状況(平成 28 年度 有価証券報告書)

日経業種分類		平成28年10月時点の日経225採用銘柄：平成28年度(2017年3月期)報告書																						
				記載内容の調査																				分類と取組みのステージを関連付ける分析
					低減策												その他開示姿勢(残存リスク)		<参考>社外との情報共有体制 ※集計対象外項目		有報記載有無と日本シーサート協議会の加盟の関連性				考察
					基本的な取組み		更なる低減策																		
							経営層関連		人材関連		態勢関連										有報〇	有報〇	有報×	有報×	
大分野	中分野	中分野社数	該当企業数	リスク認識																	協議会〇	協議会×	協議会〇	協議会×	
				①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰					
A.技術	01.医薬品	9	7	6	1	0	0	0	1	0	0	0	0	0	0	0	7	5	1	2	1	5	0	3	医薬品業界では、7割弱の企業サイバーセキュリティに対するリスクを認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 しかし、具体的な取組みは実施できていない。 情報セキュリティポリシーの作成、情報セキュリティマネジメント体制の構築から取り組むことが求められる。 一方、日本シーサート協議会の加盟は9社中1社に留まる。
	02.電気機器	27	20	20	6	6	0	0	6	1	0	0	0	0	3	0	18	15	8	9	8	12	0	7	電機機器業界では、7割強の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 2割弱の企業が、情報セキュリティポリシーの作成、情報セキュリティマネジメント体制の構築など基本的な取組みを進めている。 一方、有価証券報告書のサイバーセキュリティに関する記載がなく、かつ日本シーサート協議会に加盟していない企業が一割強ある。
	03.自動車	10	8	8	2	2	0	0	1	0	0	0	0	0	2	0	8	6	3	3	3	5	0	2	自動車業界では、8割の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 2割の企業が、情報セキュリティポリシーの作成、情報セキュリティマネジメント体制の構築など基本的な取組みを進めている。 一方、日本シーサート協議会に加盟は3割である。
	04.精密機器	5	3	3	2	1	0	0	3	0	0	0	0	0	0	0	3	3	3	3	2	0	3	0	精密機器業界では、6割の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 約3割の企業が、情報セキュリティポリシーの作成、情報セキュリティマネジメント体制の構築など基本的な取組みを進めている。 一方、日本シーサート協議会に加盟しているにもかかわらず、有価証券報告書にサイバーセキュリティに関する記載が見られない企業が6割に上る。
	05.通信	6	6	6	2	1	0	0	2	1	0	0	0	0	4	0	6	6	6	6	6	0	0	0	通信業界では、すべての企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。また、日本シーサート協議会に加盟している。 しかし、情報セキュリティポリシーの作成、情報セキュリティマネジメント体制の構築など基本的な取組みを進めている企業は約2.5割に留まる。
B.金融	06.銀行	11	11	11	7	6	0	0	6	0	0	0	0	1	3	0	11	10	5	5	5	6	0	0	銀行業界では、すべて企業がサイバーセキュリティをリスクとして認識しており、9.5割の企業が情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 また、約6割の企業が、情報セキュリティポリシーの作成、情報セキュリティマネジメント体制の構築など基本的な取組みを進めている。 一方、日本シーサート協議会へ加盟している企業は、4.5割に留まっている。
	07.その他金融	1	1	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	1	0	0	その他金融業界の1社は、サイバーセキュリティに対するリスクを認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 しかし、具体的な取組みは実施できていない。 情報セキュリティポリシーの作成、情報セキュリティマネジメント体制の構築から取り組むことが求められる。 また、日本シーサート協議会には加盟していない。

平成28年10月時点の日経225採用銘柄：平成28年度(2017年3月期)報告書

日経業種分類		中分野社数	該当企業数	記載内容の調査																				分類と取組みのステージを関連付ける分析
				リスク認識	低減策												その他開示姿勢（残存リスク）		<参考>社外との情報共有体制 ※集計対象外項目		有報記載有無と日本シーサート協議会の加盟の関連性				考察
					基本的な取組み		更なる低減策														有報〇	有報〇	有報×	有報×	
							経営層関連		人材関連		態勢関連														
大分野	中分野			①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰	協議会〇	協議会×	協議会〇	協議会×	
D.素材	14.鉱業	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	鉱業界の1社は、有価証券報告書にサイバーセキュリティに関する事項を記載しておらず、また日本シーサート協議会に加盟していない。
	15.繊維	4	1	1	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	1	0	1	1	2	繊維業界では、4社中1社がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 また、情報セキュリティポリシーの作成や、情報セキュリティマネジメント体制の構築等の基本的な取組みを実施していない。 一方、日本シーサート協議会へ加盟している企業は、4社中1社である。
	16.パイプ・紙	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	パイプ・紙業界の3社は、有価証券報告書にサイバーセキュリティに関する事項を記載しておらず、また日本シーサート協議会に加盟していない。
	17.化学	18	6	6	2	1	0	0	0	0	0	0	0	0	5	0	6	3	5	6	4	2	1	11	化学業界では、サイバーセキュリティをリスクとして認識している企業は、3割強に留まる。 また、情報セキュリティポリシーの作成や、情報セキュリティマネジメント体制の構築等の基本的な取組みを実施している企業は一割に満たない。 一方、日本シーサート協議会へ加盟している企業は、11社中5社である。
	18.石油	2	2	2	0	1	0	0	0	0	0	0	0	0	0	0	2	2	1	1	1	1	0	0	石油業界では、2社ともサイバーセキュリティをリスクとして認識している。 しかし、基本的な取組みは、1社が情報セキュリティマネジメント体制を構築しているに留まり、今後の対策が望まれる。 一方、日本シーサート協議会へ加盟している企業は、2社中1社である。
	19.ゴム	2	1	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	1	1	0	0	1	ゴム業界では、2社中1社がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。。 情報セキュリティポリシーの作成や、情報セキュリティマネジメント体制の構築等の基本的な取組みを実施している企業はない。 一方、日本シーサート協議会へ加盟している企業は、2社中1社である。
	20.窯業	8	4	4	0	2	0	0	0	0	0	0	0	0	4	0	4	2	0	0	0	4	0	4	窯業界では、6割強の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 しかし、情報セキュリティマネジメント体制の構築を実施している企業は2割に留まり、情報セキュリティポリシーの作成について記載されている企業は見られない。今後の対策が望まれる。 一方、日本シーサート協議会へ加盟している企業はない。
	21.鉄鋼	4	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1	1	0	0	3	窯業界では、半数の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 基本的な取組みを実施している企業は見られないが、「機密情報の漏洩対策については最重要の経営課題としている」という記載が見られた。 一方の半数は、有価証券報告書にサイバーセキュリティに関する記載が見られず、また日本シーサート協議会へ加盟していない。
	22.非鉄金属製品	11	7	7	0	0	0	0	1	0	0	0	0	0	3	0	6	5	1	2	1	6	0	4	非鉄金属製品業界では、6割強の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 しかし、基本的な取組みを実施している企業は見られず、一部教育や、グループ全体の取組みを実施しているという記載が見られた。 一方、日本シーサート協議会は11社中1社に留まる。

平成28年10月時点の日経225採用銘柄：平成28年度(2017年3月期)報告書

日経業種分類		中分野社数	該当企業数	記載内容の調査																				分類と取組みのステージを関連付ける分析
				リスク認識	低減策												その他開示姿勢（残存リスク）		<参考>社外との情報共有体制 ※集計対象外項目		有報記載有無と日本シーサート協議会の加盟の関連性				考察
					基本的な取組み		更なる低減策																		
							経営層関連		人材関連		態勢関連														
大分野	中分野																				有報○	有報○	有報×	有報×	
				①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰	協議会○	協議会×	協議会○	協議会×	
	23.商社	7	5	5	4	2	0	0	0	0	0	0	0	1	2	0	4	2	1	1	1	4	0	2	商社業界では、7割強の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 また、その半分の3.5割が基本的な取組みを実施しているが更なる低減策を実施ていている企業は1割に満たない。 一方、日本シーサート協議会は7社中1社に留まる。
E.資本財・	24.建設	9	6	6	2	1	0	0	1	0	0	0	1	0	2	0	6	6	2	3	1	5	1	2	建設業界では、5割強の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 しかし、基本的な取組みを実施している企業は、1.6割に留まり、更なる低減策を実施ていている企業は1割に満たない。 一方、日本シーサート協議会は9社中2社に留まる。
	25.機械	18	10	10	4	4	0	0	0	0	0	0	1	0	5	0	7	5	2	1	2	8	0	8	機械業界では、5割強の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 しかし、基本的な取組みを実施している企業は、2.3割に留まり、更なる低減策を実施ていている企業は1割に満たない。 一方、日本シーサート協議会は17社中2社に留まる。
	26.造船	2	2	2	0	1	0	0	1	0	0	0	0	0	1	0	1	0	1	1	1	1	0	0	造船業界では、すべて企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 基本的な取組みとして、一社が情報管理の体制の構築を、また教育について記載している。 一方、日本シーサート協議会は2社中1社が加盟している。
	27.その他製造	3	3	3	1	3	0	0	1	0	0	0	0	0	2	0	2	3	2	2	2	1	0	0	その他製造業界では、すべて企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 また、基本的な取組みについて、すべての企業がセキュリティマネジメント体制について記述しているのに対し、情報セキュリティポリシーについては一社のみであった。 一方、日本シーサート協議会は3社中1社が加盟している。
	28.不動産	5	1	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	1	0	4	機械業界では、5割強の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 しかし、基本的な取組みを実施している企業は、2.3割に留まり、更なる低減策を実施ていている企業は1割に満たない。 一方、日本シーサート協議会は17社中2社に留まる。
F.運輸・公	29.鉄道・バス	8	7	7	5	4	0	0	2	0	0	0	0	0	3	0	7	5	2	3	2	5	0	1	鉄道・バスの業界では、9割弱の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 また、基本的な取組みを実施している企業は6割強と高く、更なる低減策では教育に関する記載が2.5割の企業に見られた。 一方、日本シーサート協議会は8社中3社が加盟している。
	30.陸運	2	2	2	1	0	0	0	1	0	0	0	0	0	0	0	2	2	1	1	1	1	0	0	鉄道・バスの業界では、9割弱の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 また、基本的な取組みを実施している企業は6割強と高く、更なる低減策では教育に関する記載が2.5割の企業に見られた。 一方、日本シーサート協議会は8社中3社が加盟している。

日経業種分類		平成28年10月時点の日経225採用銘柄：平成28年度(2017年3月期)報告書																							
		中分野社数	該当企業数	記載内容の調査																					分類と取組みのステージを関連付ける分析
				リスク認識	低減策												その他開示姿勢（残存リスク）		<参考>社外との情報共有体制 ※集計対象外項目		有報記載有無と日本シーサート協議会の加盟の関連性				考察
					基本的な取組み		更なる低減策														有報〇	有報〇	有報×	有報×	
							経営層関連		人材関連		態勢関連														
大分野	中分野			①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰	協議会〇	協議会×	協議会〇	協議会×	
	31.海運	3	1	1	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	1	0	1	1	1	海運の業界では、3社中1社のみが有価証券報告書にサイバーセキュリティをリスクとして認識している旨を記載し、日本シーサート協議会に加盟している。 有価証券報告書に記載がなく、日本シーサート協議会に加盟している企業が一社、どちらも該当しない企業が一社である。
	32.空運	1	1	1	1	0	0	0	0	1	0	0	0	0	1	0	1	1	0	0	0	1	0	0	空運の業界一社について、サイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 情報漏洩が起きた際の影響について重点的に記載されている。しかし、基本的な取組みについては記載されていない。 一方、日本シーサート協議会には加盟していない。
	33.倉庫	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	倉庫の業界一社について、サイバーセキュリティをリスクとして認識しており、標的型攻撃等に対する訓練を定期的に実施について記載されている。しかし、基本的な取組みについては記載されていない。 一方、日本シーサート協議会には加盟していない。
	34.電力	3	3	3	1	1	0	0	3	0	0	0	0	0	0	0	2	2	2	2	2	1	0	0	電力の業界について、3社すべてがサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 6割の企業が基本的な取組み、教育に関して記載している。 一方、日本シーサート協議会には3社中2社が加盟している。
	35.ガス	2	2	2	0	1	0	0	1	0	0	0	0	0	1	0	1	1	0	1	0	2	0	0	ガスの業界について、2社ともがサイバーセキュリティをリスクとして認識している。 その内一社が情報セキュリティ推進体制、教育について記載している。 一方、日本シーサート協議会には1社中1社が加盟している。

(4) 業種別にみた開示状況(平成 29 年度 有価証券報告書)

平成29年10月時点の日経225採用銘柄：平成29年度(2018年3月期)報告書																									
日経業種分類		中分野社数	該当企業数	記載内容の調査																					分類と取組みのステージを関連付ける分析
				リスク認識	低減策												その他開示姿勢(残存リスク)		<参考>社外との情報共有体制 ※集計対象外項目		有報記載有無と日本シーサート協議会の加盟の関連性				考察
					基本的な取組み		更なる低減策																			
							経営層関連		人材関連		態勢関連															
大分野	中分野																				有報○	有報○	有報×	有報×	
				①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰	協議会○	協議会×	協議会○	協議会×	
A.技術	01.医薬品	9	8	8	1	0	0	0	1	0	0	0	0	0	2	0	7	6	3	3	2	6	1	0	医薬品業界では、9割弱の企業サイバーセキュリティに対するリスクを認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 しかし、具体的な取組みは実施できていない。 情報セキュリティポリシーの作成、情報セキュリティマネジメント体制の構築から取り組むことが求められる。 一方、日本シーサート協議会の加盟は9社中2社に留まる。
	02.電気機器	27	21	21	8	7	0	0	7	1	0	0	0	0	6	0	20	16	10	10	10	11	0	6	電機機器業界では、8割弱の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 3割弱の企業が、情報セキュリティポリシーの作成、情報セキュリティマネジメント体制の構築など基本的な取組みを進めている。 一方、有価証券報告書のサイバーセキュリティに関する記載がなく、かつ日本シーサート協議会に加盟していない企業は二割強に上る。
	03.自動車	10	9	9	4	2	0	0	2	0	0	0	0	0	7	0	9	9	4	3	4	5	0	1	自動車業界では、9割の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 3割弱の企業が、情報セキュリティポリシーの作成、情報セキュリティマネジメント体制の構築など基本的な取組みを進めている。 一方、日本シーサート協議会に加盟は4割である。
	04.精密機器	5	3	3	3	2	1	0	0	3	0	0	0	0	0	3	0	3	3	3	2	0	3	0	精密機器業界では、6割の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 約3割の企業が、情報セキュリティポリシーの作成、情報セキュリティマネジメント体制の構築など基本的な取組みを進めている。 一方、日本シーサート協議会に加盟しているにもかかわらず、有価証券報告書にサイバーセキュリティに関する記載が見られない企業が6割に上る。
	05.通信	6	6	6	2	2	0	0	2	1	0	0	0	0	4	0	6	6	6	6	6	0	0	0	通信業界では、すべての企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。また、日本シーサート協議会に加盟している。 しかし、情報セキュリティポリシーの作成、情報セキュリティマネジメント体制の構築など基本的な取組みを進めている企業は約3割強に留まる。
B.金融	06.銀行	11	11	11	7	7	2	0	6	2	0	0	0	1	8	0	11	10	5	5	5	6	0	0	銀行業界では、すべて企業がサイバーセキュリティをリスクとして認識しており、9.5割の企業が情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 また、約6割の企業が、情報セキュリティポリシーの作成、情報セキュリティマネジメント体制の構築など基本的な取組みを進めている。 一方、日本シーサート協議会へ加盟している企業は、4.5割に留まっている。
	07.その他金融	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	0	その他金融業界の1社は、サイバーセキュリティに対するリスクを認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 しかし、具体的な取組みは実施できていない。 情報セキュリティポリシーの作成、情報セキュリティマネジメント体制の構築から取り組むことが求められる。 また、日本シーサート協議会には加盟していない。

平成29年10月時点の日経225採用銘柄：平成29年度(2018年3月期)報告書

日経業種分類		中分野社数	該当企業数	記載内容の調査																				分類と取組みのステージを関連付ける分析
大分野	中分野			リスク認識	低減策												その他開示姿勢（残存リスク）		<参考>社外との情報共有体制 ※集計対象外項目		有報記載有無と日本シーサート協議会の加盟の関連性				考察
					基本的な取組み		更なる低減策														有報〇	有報〇	有報×	有報×	
							経営層関連		人材関連		態勢関連														
				①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰	協議会〇	協議会×	協議会〇	協議会×	
	08.証券	3	3	3	1	1	0	0	0	0	0	0	0	0	2	0	3	3	1	1	1	2	0	0	証券業界では、3社すべてのサイバーセキュリティに対するリスクを認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 情報セキュリティポリシーの作成、情報セキュリティマネジメント体制の構築等基本的な取組みを実施している企業は1社に留まる。 日本シーサート協議会の加盟も前述と同様の1社である。
	09.保険	6	6	6	1	4	0	0	1	1	0	0	0	0	4	0	6	6	4	4	4	2	0	0	保険業界では、すべて企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 しかし、情報セキュリティポリシーの作成、情報セキュリティマネジメント体制の構築など基本的な取組みを進めている企業は4割に留まり、更なる低減策を実施している企業は、1割程度である。 一方、日本シーサート協議会へ加盟している企業は、6.7割である。
C.消費	10.水産	2	1	1	1	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0	0	1	0	1	水産業界では、2社中1社の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。また、情報セキュリティポリシーの作成、情報セキュリティマネジメント体制の構築など基本的な取組みを進めている。 一方、日本シーサート協議会へ加盟はしていない。
	11.食品	11	10	10	3	7	0	0	5	0	0	0	0	0	8	0	10	5	3	3	2	8	1	0	食品業界では、9割の企業がサイバーセキュリティをリスクとして認識しており、8割弱の企業が情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 また、基本的な取組みとしては、情報セキュリティマネジメント体制の構築（7社）の取組みが、情報セキュリティポリシーの作成（3社）を上回る。 一方、日本シーサート協議会へ加盟している企業は、4.5割に留まっている。
	12.小売業	8	8	8	0	5	0	0	1	0	0	0	1	0	4	0	8	7	1	2	1	7	0	0	小売業界では、すべて企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 情報セキュリティマネジメント体制の構築は6割の企業で進んでいるが、情報セキュリティポリシーの作成に関する記載は見られない。また、更なる低減策を実施している企業は1割に満たない。 一方、日本シーサート協議会へ加盟している企業は、8社中1社に留まる。
	13.サービス	11	10	10	3	4	1	0	1	2	0	0	1	0	4	0	9	9	6	6	6	4	0	1	サービス業界では、9割の企業がサイバーセキュリティをリスクとして認識しており、8割の情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 しかし、情報セキュリティポリシーの作成や、情報セキュリティマネジメント体制の構築等の基本的な取組みを実施している企業は3割程度である。また、更なる低減策を実施している企業は1割に満たない。 一方、日本シーサート協議会へ加盟している企業は、4.5割程度である。

平成29年10月時点の日経225採用銘柄：平成29年度(2018年3月期)報告書

日経業種分類		中分野社数	該当企業数	記載内容の調査																				分類と取組みのステージを関連付ける分析
				リスク認識	低減策												その他開示姿勢（残存リスク）		<参考>社外との情報共有体制 ※集計対象外項目		有報記載有無と日本シーサート協議会の加盟の関連性				考察
					基本的な取組み		更なる低減策														有報〇	有報〇	有報×	有報×	
							経営層関連		人材関連		態勢関連														
大分野	中分野			①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰	協議会〇	協議会×	協議会〇	協議会×	
D.素材	14.鉱業	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	鉱業界の1社は、有価証券報告書にサイバーセキュリティに関する事項を記載しておらず、また日本シーサート協議会に加盟していない。
	15.繊維	4	3	3	0	0	0	0	1	0	0	0	0	0	3	0	3	2	1	1	1	2	0	1	繊維業界では、4社中3社がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 しかし、情報セキュリティポリシーの作成や、情報セキュリティマネジメント体制の構築等の基本的な取組みを実施している企業はなく、今後の対策が望まれる。 一方、日本シーサート協議会へ加盟している企業は、4社中1社である。
	16.パイプ・紙	2	0	7	2	1	0	0	3	0	0	0	0	0	7	0	6	4	5	6	0	0	0	2	パイプ・紙業界の2社は、有価証券報告書にサイバーセキュリティに関する事項を記載しておらず、また日本シーサート協議会に加盟していない。
	17.化学	18	7	7	2	1	0	0	3	0	0	0	0	0	7	0	6	4	5	6	3	4	2	9	化学業界では、サイバーセキュリティをリスクとして認識している企業は、4割弱に留まる。 また、情報セキュリティポリシーの作成や、情報セキュリティマネジメント体制の構築等の基本的な取組みを実施している企業は一割に満たない。 一方、日本シーサート協議会へ加盟している企業は、11社中5社である。
	18.石油	2	2	2	0	1	0	0	0	0	0	0	0	0	1	0	1	2	1	1	1	1	0	0	石油業界では、2社ともサイバーセキュリティをリスクとして認識している。 しかし、基本的な取組みは、1社が情報セキュリティマネジメント体制を構築しているに留まり、今後の対策が望まれる。 一方、日本シーサート協議会へ加盟している企業は、2社中1社である。
	19.ゴム	2	1	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	1	1	0	0	1	ゴム業界では、2社中1社がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。。 情報セキュリティポリシーの作成や、情報セキュリティマネジメント体制の構築等の基本的な取組みを実施している企業はない。 一方、日本シーサート協議会へ加盟している企業は、2社中1社である。
	20.窯業	8	5	5	0	2	0	0	0	0	0	0	0	0	5	0	5	4	0	0	0	5	0	3	窯業界では、6割強の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 しかし、情報セキュリティマネジメント体制の構築を実施している企業は2割に留まり、情報セキュリティポリシーの作成について記載されている企業は見られない。今後の対策が望まれる。 一方、日本シーサート協議会へ加盟している企業はない。
	21.鉄鋼	4	2	2	0	0	1	1	1	0	0	0	0	0	2	0	2	1	1	1	1	1	0	2	鉄鋼業界では、半数の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 基本的な取組みを実施している企業は見られないが、「機密情報の漏洩対策については最重要の経営課題としている」という記載が見られた。 一方の半数は、有価証券報告書にサイバーセキュリティに関する記載が見られず、また日本シーサート協議会へ加盟していない。
	22.非鉄金属製品	11	7	7	0	0	0	0	1	0	0	0	0	0	5	0	7	7	1	2	1	6	0	4	非鉄金属製品業界では、6割強の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 しかし、基本的な取組みを実施している企業は見られず、一部教育や、グループ全体の取組みを実施しているという記載が見られた。 一方、日本シーサート協議会は11社中1社に留まる。

平成29年10月時点の日経225採用銘柄：平成29年度(2018年3月期)報告書

日経業種分類		中分野社数	該当企業数	記載内容の調査																	分類と取組みのステージを関連付ける分析				
				リスク認識	低減策												その他開示姿勢（残存リスク）		<参考>社外との情報共有体制 ※集計対象外項目		有報記載有無と日本シーサート協議会の加盟の関連性				考察
					基本的な取組み		更なる低減策														有報〇	有報〇	有報×	有報×	
							経営層関連		人材関連			態勢関連													
大分野	中分野			①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰	協議会〇	協議会×	協議会〇	協議会×	
	23.商社	7	5	5	4	1	0	0	1	0	0	0	0	0	4	0	4	2	1	1	1	4	0	2	商社業界では、7割強の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 また、その半分の3.5割が基本的な取組みを実施しているが更なる低減策を実施ていている企業は1割に満たない。 一方、日本シーサート協議会は7社中1社に留まる。
E.資本財・	24.建設	9	5	5	2	1	0	0	1	0	0	0	1	0	3	0	5	4	2	3	1	4	1	3	建設業界では、5割強の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 しかし、基本的な取組みを実施している企業は、1.6割に留まり、更なる低減策を実施ていている企業は1割に満たない。 一方、日本シーサート協議会は9社中2社に留まる。
	25.機械	17	9	9	3	5	0	0	2	0	0	0	1	0	4	1	7	5	2	2	2	7	0	8	機械業界では、5割強の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 しかし、基本的な取組みを実施している企業は、2.3割に留まり、更なる低減策を実施ていている企業は1割に満たない。 一方、日本シーサート協議会は17社中2社に留まる。
	26.造船	2	2	2	0	1	0	0	1	0	0	0	0	0	2	0	2	1	1	1	1	1	0	0	造船業界では、すべて企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 基本的な取組みとして、一社が情報管理の体制の構築を、また教育について記載している。 一方、日本シーサート協議会は2社中1社が加盟している。
	27.その他製造	3	3	3	1	3	1	1	1	0	0	0	0	0	1	0	3	1	2	2	2	1	0	0	その他製造業界では、すべて企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 また、基本的な取組みについて、すべての企業がセキュリティマネジメント体制について記述しているのに対し、情報セキュリティポリシーについては一社のみであった。 一方、日本シーサート協議会は3社中1社が加盟している。
	28.不動産	5	2	2	0	0	0	0	0	0	0	0	0	0	2	0	2	1	0	0	0	2	0	3	不動産業界では、5割強の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 しかし、基本的な取組みを実施している企業は、2.3割に留まり、更なる低減策を実施ていている企業は1割に満たない。 一方、日本シーサート協議会は17社中2社に留まる。
F.運輸・公	29.鉄道・バス	8	7	7	5	5	0	0	4	0	0	0	0	1	6	0	7	7	3	4	3	4	0	1	鉄道・バスの業界では、9割弱の企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 また、基本的な取組みを実施している企業は6割強と高く、更なる低減策では教育に関する記載が2.5割の企業に見られた。 一方、日本シーサート協議会は8社中3社が加盟している。
	30.陸運	2	2	2	1	0	0	0	1	0	0	0	0	0	2	0	2	2	1	1	1	1	0	0	陸運の業界では、すべての企業がサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 しかし、情報セキュリティポリシーの作成と教育を１社が実施しているに留まる。 一方、日本シーサート協議会は2社中1社が加盟している。

平成29年10月時点の日経225採用銘柄：平成29年度(2018年3月期)報告書																										
日経業種分類		中分野社数	該当企業数	記載内容の調査																						分類と取組みのステージを関連付ける分析
大分野	中分野			リスク認識	低減策													その他開示姿勢（残存リスク）		<参考>社外との情報共有体制 ※集計対象外項目		有報記載有無と日本シーサート協議会の加盟の関連性				考察
					基本的な取組み		更なる低減策																有報〇	有報〇	有報×	有報×	
							経営層関連		人材関連		態勢関連																
				①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰	協議会〇	協議会×	協議会〇	協議会×	
	31.海運	3	1	1	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	1	0	1	1	1	海運の業界では、3社中1社のみが有価証券報告書にサイバーセキュリティをリスクとして認識している旨を記載し、日本シーサート協議会に加盟している。 有価証券報告書に記載がなく、日本シーサート協議会に加盟している企業が一社、どちらも該当しない企業が一社である。
	32.空運	1	1	1	0	0	0	0	0	1	0	0	0	0	1	0	1	1	0	0	0	1	0	0	空運の業界1社について、サイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 情報漏洩が起きた際の影響について重点的に記載されている。しかし、基本的な取組みについては記載されていない。 一方、日本シーサート協議会には加盟していない。
	33.倉庫	1	1	3	3	1	0	0	3	0	0	0	0	0	2	0	3	2	2	2	0	1	0	0	倉庫の業界1社について、サイバーセキュリティをリスクとして認識しており、標的型攻撃等に対する訓練を定期的に実施について記載されている。しかし、基本的な取組みについては記載されていない。 一方、日本シーサート協議会には加盟していない。
	34.電力	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	0	0	電力の業界について、3社すべてがサイバーセキュリティをリスクとして認識しており、情報漏洩等の事故が生じた場合に業績や財務状況に影響があることを認識している。 6割の企業が基本的な取組み、教育に関して記載している。 一方、日本シーサート協議会には3社中2社が加盟している。
	35.ガス	2	2	2	0	1	0	0	1	0	0	0	0	0	1	0	1	2	1	2	1	1	0	0	ガスの業界について、2社ともがサイバーセキュリティをリスクとして認識している。 その内一社が情報セキュリティ推進体制、教育について記載している。 一方、日本シーサート協議会には1社中1社が加盟している。

(5) アンケートでの質問

【サイバーセキュリティに対する経営層の理解】

Q1. 経営層は、事業の鍵を握る重要な情報やデータは何か、またこれらの情報やデータが貴社・競業他社・犯罪者にとってどれほどの価値があるかについて良く理解していますか。（単一選択）

a. 明確な理解を持っており、強いリーダーシップで社内に周知徹底している
b. 十分に理解しており、それが経営方針にも現れている
c. 理解が進んでいるのか、はっきりとは分からない
d. あまり良く理解していないと感じる
e. 良く分からない

Q2. 経営層は、事業の鍵を握る重要な情報やデータの損失・漏えいが、事業にどれほど大きな影響を及ぼすかについて良く理解していますか。（単一選択）

a. 明確な理解を持っており、強いリーダーシップで社内に周知徹底している
b. 十分に理解しており、それが経営方針にも現れている
c. 理解が進んでいるのか、はっきりとは分からない
d. あまり良く理解していないと感じる
e. 良く分からない

【サイバーセキュリティに対する経営層の関与】

Q3. サイバーセキュリティに対する経営層の関与の度合いについて、最も良く当てはまる記述はどれですか。（単一選択）

a. 年間を通して的確に処理している
b. 定期的に考慮し、意思決定を行っている
c. 定期的報告も含め、時々報告を受けている
d. 年に１～２度、何か起きたら報告を受けるだけである
e. 技術的な内容であるため関与しない
f. 良く分からない

Q4. サイバーセキュリティを、経営会議・取締役会の議題としてどの程度取り上げていますか。（単一選択）

a. 最も重要な議題の１つとして、毎回取り上げている
b. 主要な議題の１つとして、高い頻度で定期的に取り上げている
c. 種々の議題の１つとして、時々随時取り上げることがある
d. 年間を通じて１～２回程度しか取り上げていない
e. ほとんど取り上げることはない
f. その他　（具体的に　　）

Q5. 経営会議・取締役会において、サイバーセキュリティについて報告するのはどなたですか。（複数選択可）

a. 取締役
b. CISO（最高情報セキュリティ責任者）
c. 経営・企画部門
d. セキュリティ総括部門
e. 情報システム部門
f. 管理部門（総務部門、法務部門、CSR 部門など）
g. 現場の責任者（製造部門、プラント運用部門、事業部門等）
h. その他（具体的に　　）

Q6. 経営層は顧客データのセキュリティに関する報告のレビューに積極的に関与していますか。（単一選択）

a. している
b. していない
c. 良く分からない

Q7. 経営層は、率先してサイバーセキュリティインシデントへの対応に関与していますか。（単一選択）

a. 主導的な役割を果たしている
b. 対応の一部で関与することがある
c. 全く関与していない
d. 良く分からない

【サイバーセキュリティに対する経営層の取組姿勢・態勢整備】

Q8. 経営層は、現在の事業及びこれからのデジタル変革への対応において、サイバーセキュリティリスク対策への取組姿勢をどれほど明確に示していますか。（単一選択）

a. 取組姿勢を全社に明確に示しており、対策の徹底を求めている
b. 取組姿勢を示してはいるが、十分に明確ではなく、対策もあいまいになりがちである
c. どのような取組姿勢を持っているのかあまり良く伝わってこない
d. 良く分からない

Q9. 経営層は積極的にサイバーセキュリティ対策を確保する態勢整備に取り組んでいますか。当てはまるものをすべてお答えください。（複数選択可）

a. 取組の基本方針等について、社内全体に持続的に周知徹底している
b. 運用費用だけでなく投資も含めて、予算を積極的に確保している
c. 必要な機材・ツール等の導入を前向きに承認している
d. 必要な要員を積極的に確保し、各組織に的確に配置している
e. 要員のスキル・ノウハウの育成に積極的に取り組んでいる
f. 要員の人事考課に加点要素を設定し、インセンティブとキャリアパスに配慮している
g. その他（具体的に　　）

Q10. 経営層は「経団連サイバーセキュリティ経営宣言」*を理解し、これに基づく取組を実施していますか。（単一選択）

a. 積極的に推進している
b. 参考として、自社の取組に一部取り入れている
c. ほとんど実施していない
d. 全く実施していない
e. 良く分からない

＊「経団連サイバーセキュリティ経営宣言」 http://www.keidanren.or.jp/policy/2018/018.pdf

【サイバーセキュリティに対する取組の基本方針等に係る社内全体の理解・認識】

Q11.サイバーセキュリティに対する取組の基本方針（サイバーセキュリティポリシー等）は社内全体で十分に認識・理解されていますか。（単一選択）

a. 社内全体で広く認識され、理解されている
b. まだ認識・理解が低い部門がある （例： ）
c. 良く分からない

Q12. **Q11.で「b. まだ認識・理解が低い部門がある」**と回答した方に伺います。認識や理解が低く留まっている理由は何であると考えていますか。（複数選択可）

a. 当事者意識が十分に根付いていないため
b. セキュリティ対策を理解できる要員が配置されていないため
c. 業務上、対策を取りにくい場面が多く存在するため
d. 社内全体への周知が徹底していないため（一部の部門にしか伝えられていないことを含む）
e. 社内全体への周知が持続的に行われていないため
f. その他（具体的に ）
g. 良く分からない

【サイバーセキュリティに関する社外への積極的な情報発信】

Q13. サイバーセキュリティに関する情報を、社外に積極的に発信していますか。（単一選択）

a. 積極的に発信している
b. まだ十分ではないが、発信への取組を強化している
c. ほとんど発信していない
d. 良く分からない

Q14. **Q13.で「a. 積極的に発信している」「b. まだ十分ではないが、発信への取組を強化している」**または**「c. ほとんど発信していない」**と回答した方に伺います。社外への情報発信は、主としてどの相手に対して行っていますか。（複数選択可）

a. 顧客・消費者
b. 取引先
c. サプライチェーン各社：グループ会社、外部委託先、サードパーティ、MSP（マネージドサービスプロバイダ）等
d. 投資家・アナリスト・格付け機関
e. メディア
f. その他（具体的に ）

＜以下を御確認の上、設問に御回答ください＞

■「戦略マネジメント層」の定義

経営層が示す経営戦略や事業戦略の下、業務やサービス等を実現するためのリスクの一つとして、サイバーセキュリティに係るリスクを認識し、そのマネジメントを中心となって支える立場。経営層が示した方針を踏まえた対策の立案、実務者層・技術者層の指揮、経営層への報告等の役割を担う。

【戦略マネジメント層の確保と人材育成】

Q15.戦略マネジメント層の機能はどの部門が担っていますか。（複数選択可）

a. 情報システム部門
b. セキュリティ総括部門
c. 経営・企画部門または各事業部門
d. 管理部門（総務部門、法務部門、ＣＳＲ部門など）
e. どれも当てはまらない（他部門：　　）
f. 良く分からない
g. 配置していない

Q16. **Q15.で「a. 情報システム部門」 ～ 「e. どれも当てはまらない」のいずれか**を回答した方に伺います。戦略マネジメント層をどのように確保していますか。（複数選択可）

a. 経営・企画部門のマネジメントラインから配置転換している
b. 事業部門のマネジメントラインから配置転換している
c. 情報システム部門のマネジメントラインから配置転換している
d. リスク管理部門のマネジメントラインから配置転換している
e. その他の内部組織から配置転換している（例：総務部門、法務部門、広報部門等）
f. 外部からの採用に取り組んでいる
g. 外部委託により対応している
h. 具体的な対応ができていない
i. 良く分からない
j. その他（具体的に　　）

Q17. **Q16.で「a. 経営・企画部門のマネジメントラインから配置転換している」 ～ 「g. 外部委託により対応している」のいずれか**を回答された方にお伺いします。戦略マネジメント層として着任する前に、どのような人材育成を実施していますか。 （複数選択可）

a. サイバーセキュリティリスクを理解するための基礎知識を教育している
b. サイバー攻撃の脅威と対策に係る知識を教育している
c. サイバーセキュリティに関連する法令・規格・諸制度の知識について教育している
d. 事業継続を確保するためのリスクマネジメントやインシデント対応に必要な知識を教育している
e. 新しい価値を創造するための事業戦略の推進に必要な知識を教育している
f. 特に何もしていない
g. 良く分からない
h. その他（具体的に　　）

【税制優遇やサイバーセキュリティ保険に対する企業の認識】

Q18. 現在、情報連携投資等促進税制（サイバーセキュリティ対策を取ることで税制優遇を受けられるもの）やサイバーセキュリティ保険（損害補填（損害賠償、訴訟、復旧、調査等の費用を補填するもの）やインシデント対応支援を提供してくれる保険）のような取組が実施されています。このような動向を認知や活用していますか。（複数選択可）

a. 税制について認識し、活用している
b. 税制について認識しているが、活用していない
c. 保険について認識し、活用している
d. 保険について認識しているが、活用していない
e. いずれも認識していない
f. 良く分からない

Q19.サイバーセキュリティ保険を活用していますか。（単一選択）

a. 既に加入して活用している
b. 保険の内容は調べており、今後活用を検討したい
c. 活用の予定はない
d. 良く分からない

Q20.昨今、サプライチェーンを通じたサイバー攻撃が急激に深刻さを増しています。国内外の取引先を通じたサイバー攻撃（サーバ運用を委託する業者を踏み台とした攻撃等）等の脅威を認識して、仕様書にサイバーセキュリティ対策に関する項目を盛り込む等の対策を行っていますか。（単一選択）

a. 脅威を認識し、対策を講じている
b. 脅威を認識しているが、対策は十分でない
c. 認識している脅威はない
d. 良く分からない

【属性項目】

Q21. 貴社の最も新しい年間売上高についてご教示ください。

貴社単体	百万円
連結決算	百万円

Q22. 貴社の従業員数についてご教示ください。

貴社単体	人 （うち正社員 人）
連結決算	人 （うち正社員 人）

Q23. 貴社の連結対象企業数についてご教示ください。

国内	社
海外	社

Q24. 貴社では CISO（最高情報セキュリティ責任者）を任命していますか。（単一選択）

a. 任命している
b. 任命していないが、する予定がある
c. 任命しておらず、する予定もない

Q25. 貴社の事業は、その特性上、サイバーセキュリティリスクの影響を強く受けやすいと考えますか。（単一選択）

a. はい （その理由： ）
b. いいえ
c. 良く分からない

Q26. 貴社の主要事業が属する業種について１つだけ選んでご教示ください。（単一選択）

a. 農業、林業
b. 漁業
c. 工業、採石業、砂利採取業
d. 建設業
e. 製造業
f. 電気・ガス・熱供給・水道業
g. 情報通信業
h. 運輸業、郵便業
i. 卸売業・小売業
j. 金融業、保険業
k. 不動産業、物品賃貸業
l. 学術研究、専門・技術サービス業
m. 宿泊業、飲食店
n. 生活関連サービス業、娯楽業
o. 教育学習支援業
p. 医療、福祉
q. 複合サービス事業
r. サービス業(他に分類されないもの)
s. 公務(他に分類されるものを除く)
t. その他（具体的に　　）