NISC

National center of Incident readiness and Strategy for Cybersecurity

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（概要）

平成31年3月29日

内閣サイバーセキュリティセンター

株式会社エヌ・ティ・ティ・データ経営研究所

１．調査内容

目的

企業のサイバーセキュリティの取組に関する情報発信状況と、サイバーセキュリティに対する意識や人材育成等の実態について把握し、課題等の分析を行う。

１．概要

- 日経２２５の企業等に対し、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アンケート調査を実施し分析を行う。

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

- 日経２２５の企業等を対象として次の２点の文書を収集。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・分析を実施。
  - 有価証券報告書
    (調査期間：平成28年-29年発行分)
  - コーポレート・ガバナンス報告書
    (調査期間：平成28年-29年発行分)

３．アンケート調査

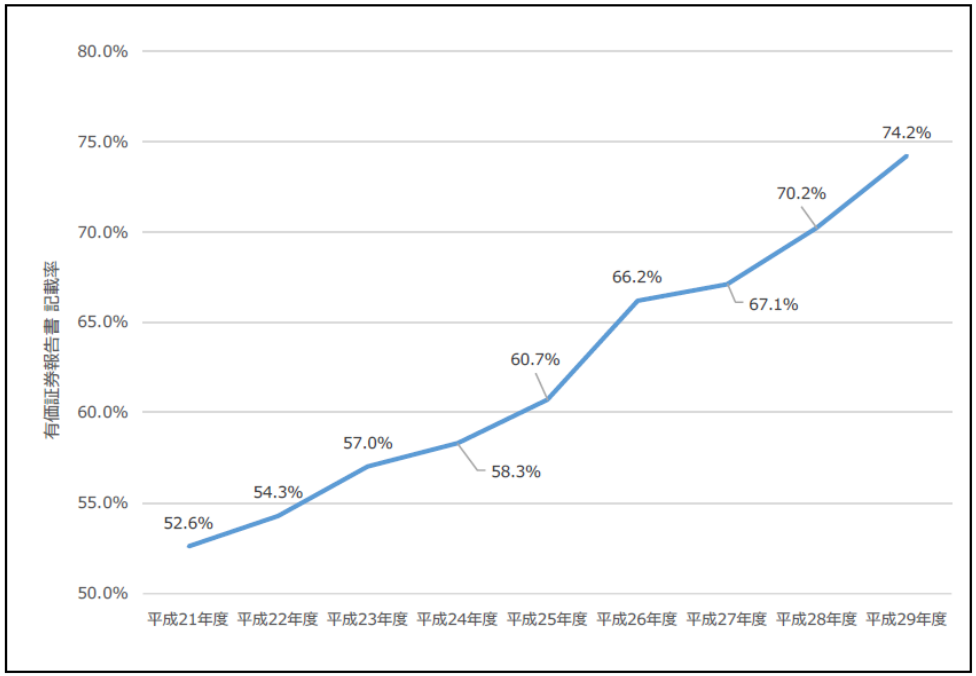
- 日経２２５等の企業に対し、平成３１年１月～２月にサイバーセキュリティに関するアンケート調査を実施。
- 経営層のサイバーセキュリティに対する意識や、戦略マネジメント層の人材の確保・育成状況等についてアンケート調査を行い、分析を実施。

４．調査結果の総合分析

- 「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「アンケート調査」の結果を用いて相関分析を実施。
- 英国政府による「FTSE 350 Cyber Governance Health Check Report」の調査結果と「アンケート調査」の結果の比較分析を実施。

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（主な結果）

- 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する記載を行っている企業は着実に増加している。ただし、業界による記載率の差は大きく、「金融」は全ての企業が記載しているのに対し、「素材」は、４５％にとどまっている。
- 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に関する記載率は平成２８～２９年度に急増している。金融は必ずしも記載率が高くなく、技術や素材の方が高い。



図：有価証券報告書にサイバーセキュリティに関する記載を行っている企業の割合の推移*

*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

【有価証券報告書】

業種分類	平成28年度		平成29年度	
	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%
金融	21	100.0%	21	100.0%
消費	27	90.0%	29	90.6%
素材	27	45.0%	32	54.2%
資本財・その他	22	59.5%	21	58.3%
運輸・公共	17	85.0%	17	85.0%
計	158	70.2%	167	74.2%

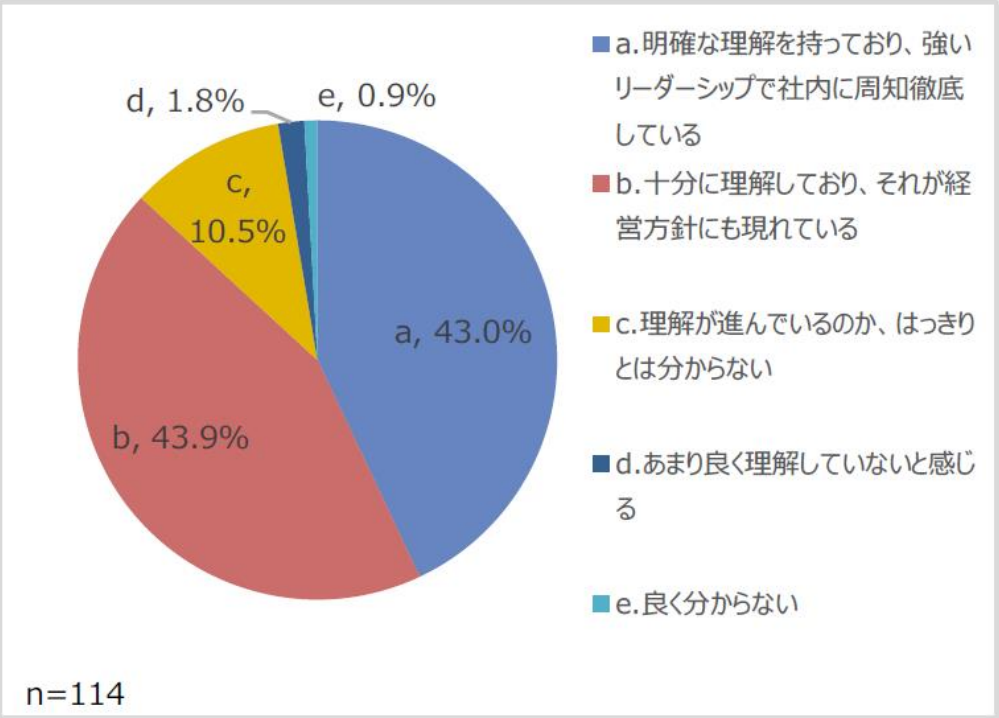
【コーポレートガバナンス報告書】

業種分類	平成28年度		平成29年度	
	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%
金融	3	14.3%	6	28.6%
消費	7	23.3%	14	43.8%
素材	14	23.3%	20	33.9%
資本財・その他	10	27.0%	16	44.4%
運輸・公共	2	10.0%	5	25.0%
計	50	22.2%	86	38.2%

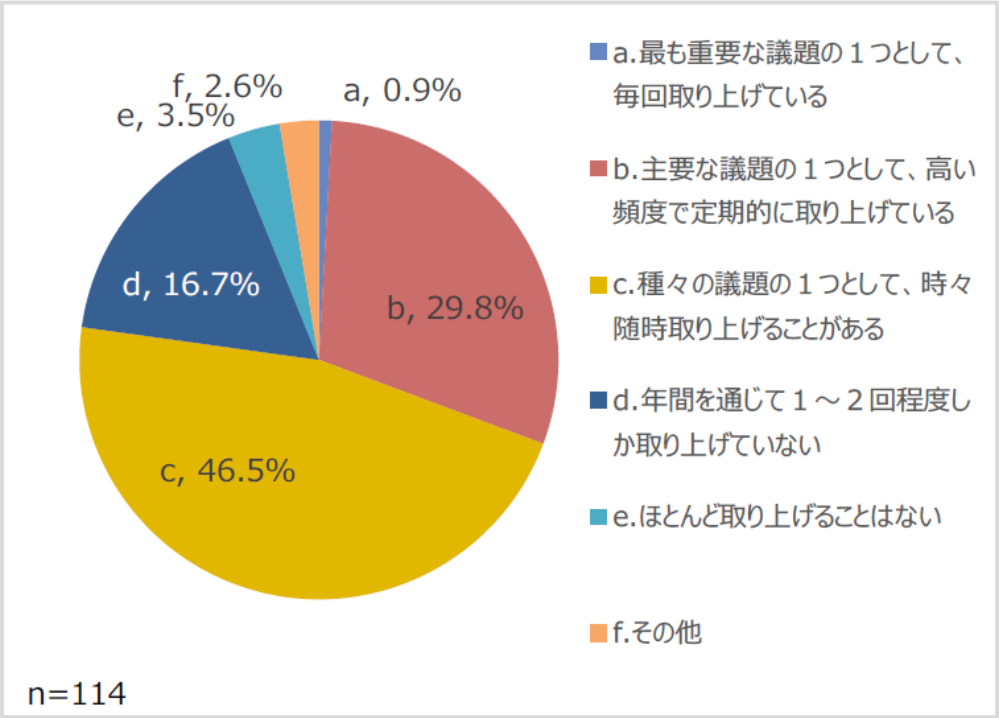
表：分野別サイバーセキュリティに関する記載状況

3．アンケート調査（1）（主な結果）

・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、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
・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



図：サイバーセキュリティに関するリスクへの経営層の理解

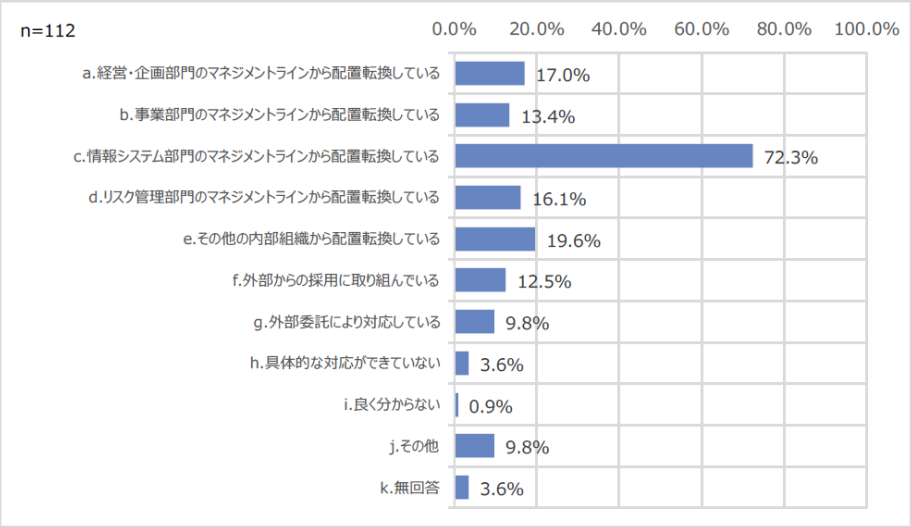


図：経営会議・取締役会でのサイバーセキュリティに関する報告・議論の頻度

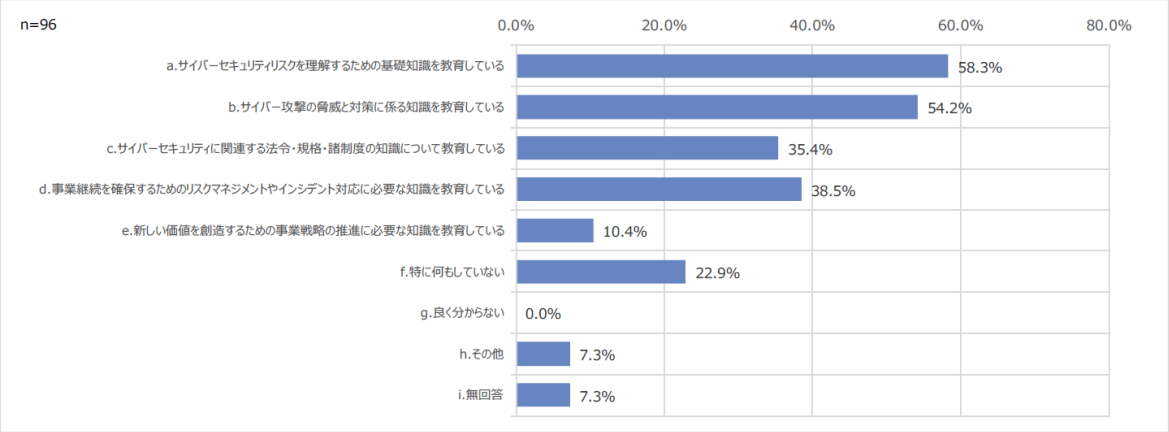
3．アンケート調査（2）
（主な結果）

・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。

図：「戦略マネジメント層」の配置・確保方法

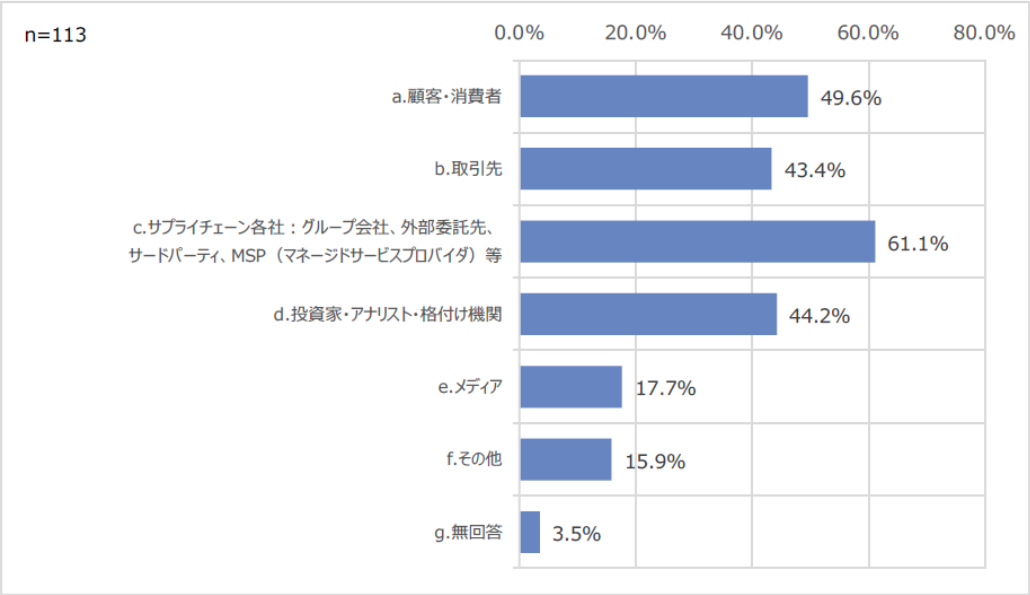


図：「戦略マネジメント層」の育成方法

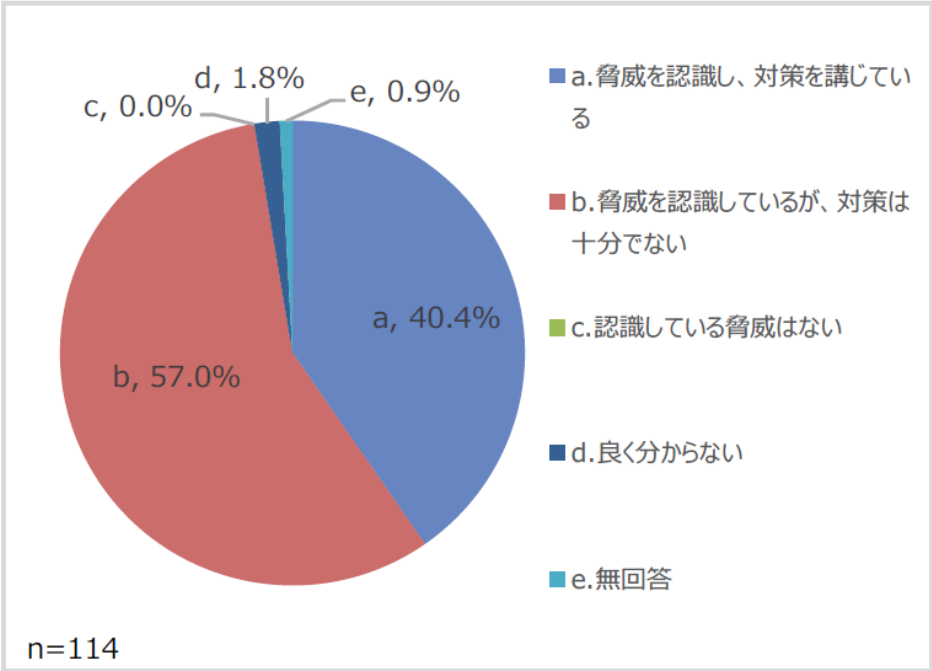


3．アンケート調査（3）
（主な結果）

・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。



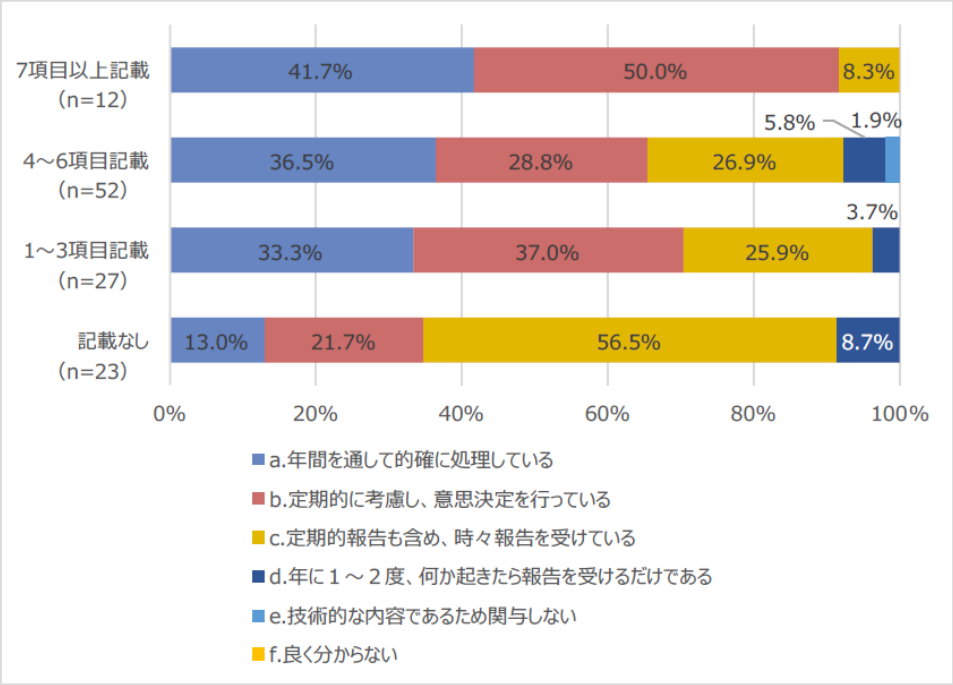
図：企業の主たる情報発信先



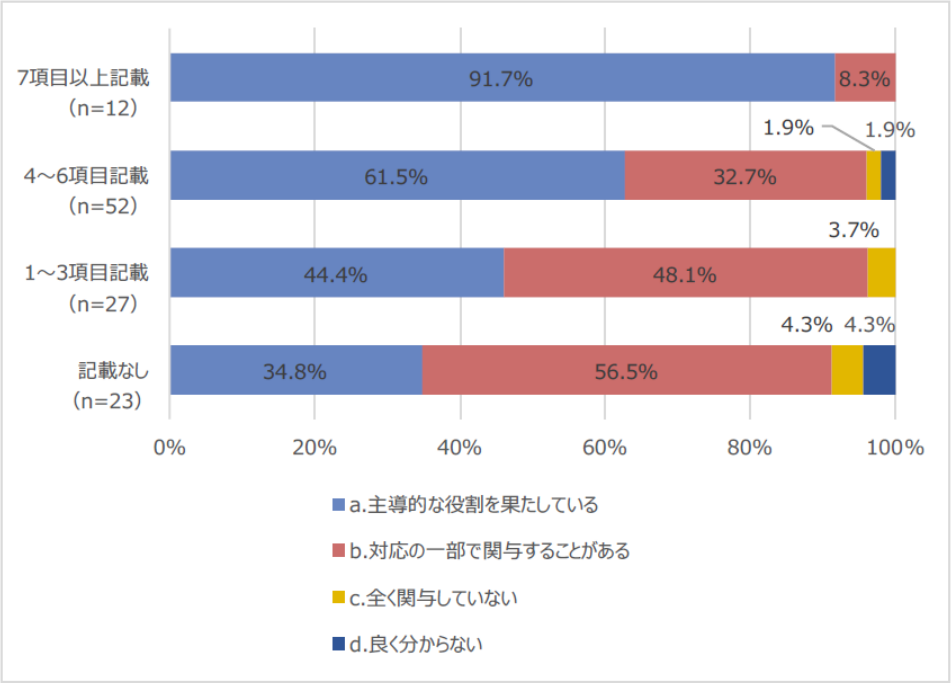
図：サプライチェーンを想定した対応の度合い

4．調査結果の総合分析（主な結果）

・ 有価証券報告書における記載の深度が深ければ深いほど、経営層がサイバーセキュリティやサイバーインシデント対応指揮に関与する度合いが強い。この両者の間には明確で強い相関があるものと理解できる。



図：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



図：有価証券報告書における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