「企業における営業秘密管理に関する実態調査 2024」

調査実施報告書

2025 年 8 月

独立行政法人情報処理推進機構

IPA
Information-technology
Promotion
Agency, Japan

修正履歴

年月日	箇所	内容
2026 年 3 月 27 日	p.19 図 19	図中の系列名を修正 （修正前）2020(n=11**4**) （修正後）2020(n=11**1**)
	p.21 図 21	図中の系列名を修正 （修正前）2020(n=11**4**) （修正後）2020(n=11**3**)
	p.24 図 24	図中の系列名を修正 （修正前）2020(n=11**4**) （修正後）2020(n=11**1**)

目次

1　はじめに

1.1　背景及び目的

企業の技術情報や顧客情報等、営業上重要な情報である営業秘密の漏えい事案が近年も後を絶たない。営業秘密の漏えいは事業に深刻な影響を及ぼすことから、その保護は喫緊の課題である。

独立行政法人情報処理推進機構（以下、「IPA」という）では、企業における営業秘密の漏えいの発生状況、漏えい対策等の実態を明らかにし、営業秘密漏えいを防ぐために有用な情報を提供することを目的として、「企業における営業秘密管理に関する実態調査 2024」を実施した。

なお、営業秘密管理に関する調査として、2020 年度に IPA が「企業における営業秘密管理に関する実態調査 2020」（以下、「2020 年度調査」という）を実施している。本調査は、2020 年度調査も参考にしながら近年の最新動向を反映した情報の提供を目指したものである。

1.2　実施内容

本調査は、国内企業に属する個人に対してウェブアンケートの方式で実施した。調査委託元である株式会社ネオマーケティングの保有するパネルに対し、2025 年 1 月 23 日から 2025 年 1 月 24 日にかけて配信し、2025 年 1 月 28 日に回収、2025 年 1 月 31 日までの期間に、データクレンジング、集計等を行った。本調査における属性（業種、従業員数）毎の最終回収数は以下の通りであった。

表 1 本調査で実施したアンケート調査における業種・従業員数別の最終回収数

	製造業	非製造業
従業員 301 名以上	300 人	300 人
従業員 300 名以下	300 人	300 人

1.2.1　アンケートの構成

本調査では、営業秘密管理に関する本質問とは別に、回答者の属性を確認する目的で予備質問を設定した。また、予備質問とは別に、営業秘密管理に関する問いを本質問として、全部で 37 問設定した。調査フローは図 1 に示す通りで、回答者が予備質問及び本質問に回答し、表 1 の最終回収数に達したところで、本調査は終了した。

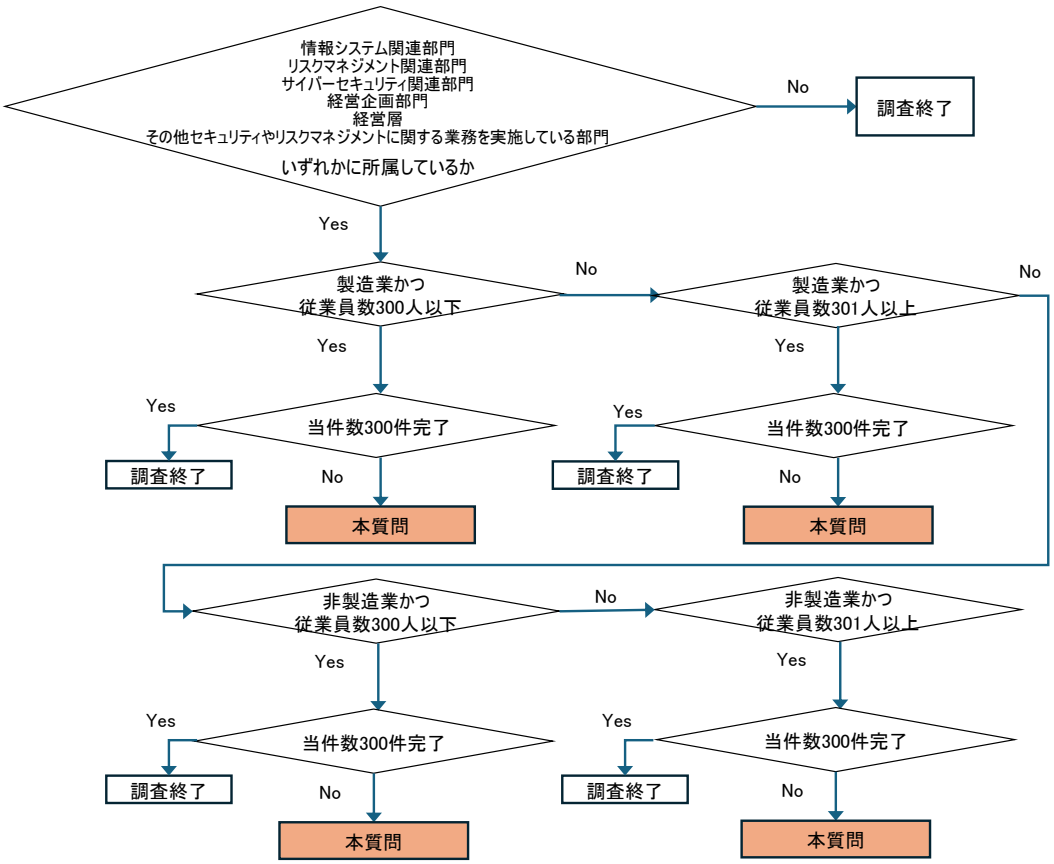


図 1 調査フロー

予備質問

予備質問の項目は以下の通りである。

- 回答者の性別
- 回答者の年代
- 回答者の居住地域
- 所属組織の概況
  - 業種及び所属組織が製造業の場合の中分類
  - 従業員数
  - 資本金
  - 売上高（2023 年度）

・ 所属組織における回答者の所属部門
  - 「情報システム関連部門」、「リスクマネジメント関連部門」、「サイバーセキュリティ関連部門」、「経営企画部門」、「経営層」、「その他セキュリティやリスクマネジメントに関する業務を実施している部門」のいずれかに所属しているか

本質問概要

本質問の内容を大別すると以下の 5 項目である。

・ 営業秘密の漏えいの実態
  - 過去 5 年以内の営業秘密の漏えい事例の有無
  - 漏えいした情報の種類
  - 漏えいした情報の重要度
  - 漏えい事例を認識したきっかけ
  - 漏えいによる推定損害額
・ 営業秘密管理の実態
  - 営業秘密の漏えいに関して必要な対策
  - 内部不正を誘発する環境・状況
  - 営業秘密の区分及び格付け実施の有無
  - 営業秘密の管理ルールの運用状況
  - 営業秘密管理を実践する上での問題
・ 営業秘密管理において実施している対策
  - 営業秘密の漏えいに気付くための技術的対策の実施
  - 実施しているあるいは実施することを検討している技術的対策
  - 営業秘密情報への不正アクセス防止策として実施している対策
  - 営業秘密情報の社外への不正持出防止策として実施している対策
  - 営業秘密の漏えいを生じさせにくい環境をつくるために実施している対策
・ 最近の動向を踏まえた対策
  - サプライチェーンにおける営業秘密の管理状況の把握
  - クラウドサービスを使用した営業秘密の共有や参照
  - クラウドサービスにて営業秘密の不正使用リスクを想定し実施している対策
  - 「シャドークラウド」が生ずることを防止する対策を講じているか
  - 生成 AI の業務利用についてルールを定めている割合
・ 政府機関等の営業秘密管理に関する活動
  - 「秘密情報の保護ハンドブック」の今後の改定で実施してほしい内容
  - 行政サービス、ガイドライン等で知っているもの

本質問の内容の詳細及び集計結果の詳細は、「2 調査結果」に記述する。

1.2.2　本調査回答者の属性情報

本調査回答者の予備質問の結果からわかる属性情報は、以下に示す図 2 から図 8 及び表 2 の通りであった。

① 回答者の年代

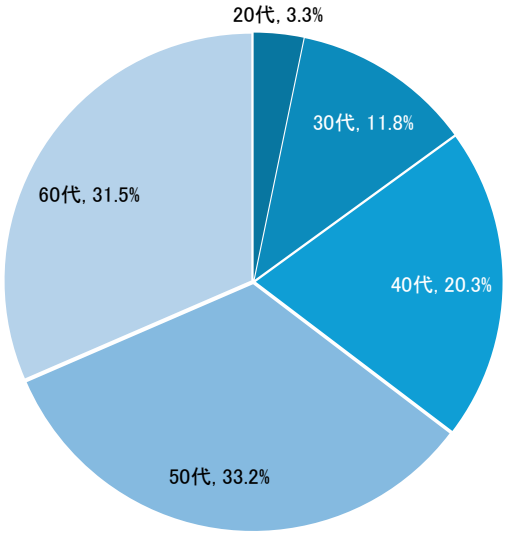


図 2 回答者の年代(n=1200)

② 回答者の居住地域

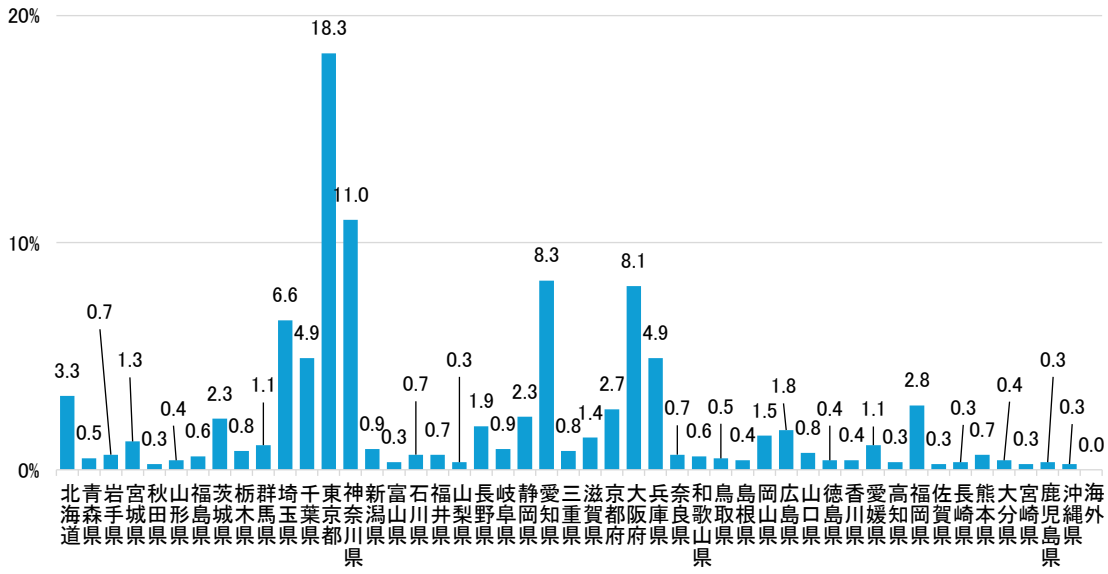


図 3 回答者の居住地域(n=1200)

③ 回答者の所属組織の業種

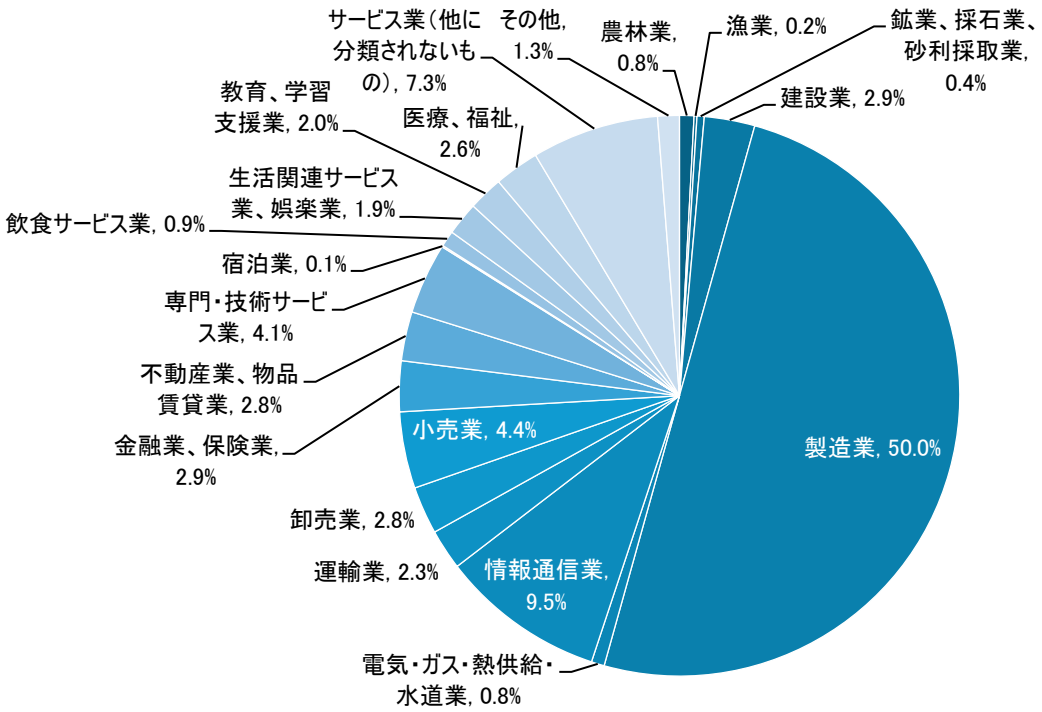


図 4 回答者の所属組織の業種（n=1200）

④ 回答者の所属組織の業種(中分類)

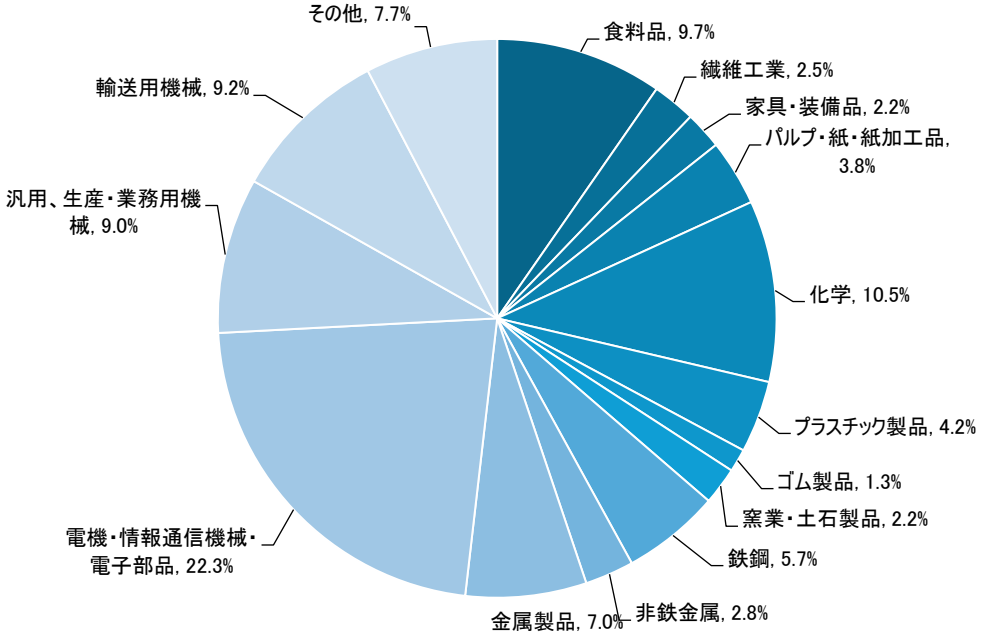


図 5 回答者の所属組織の業種(中分類)(n=600)

⑤ 回答者の所属組織の従業員数

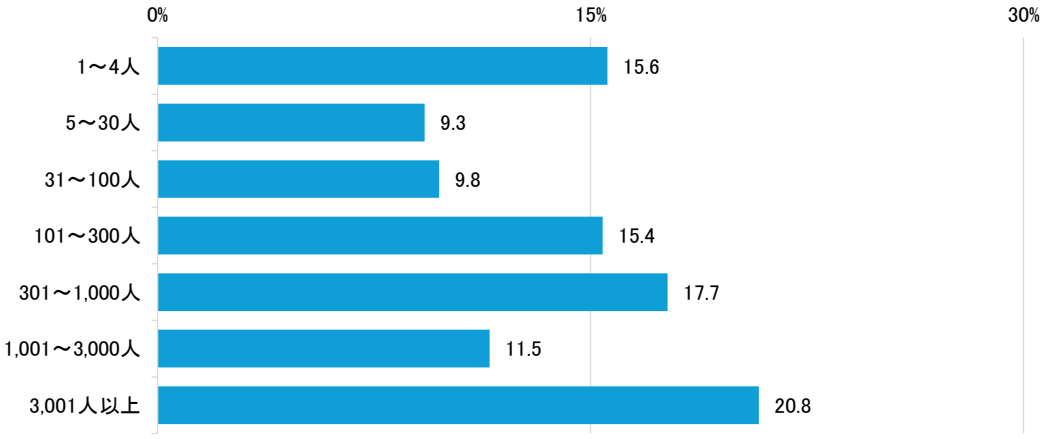


図 6 回答者の所属組織の従業員数(n=1200)

⑥ 回答者の所属組織の売上高（2023 年度）

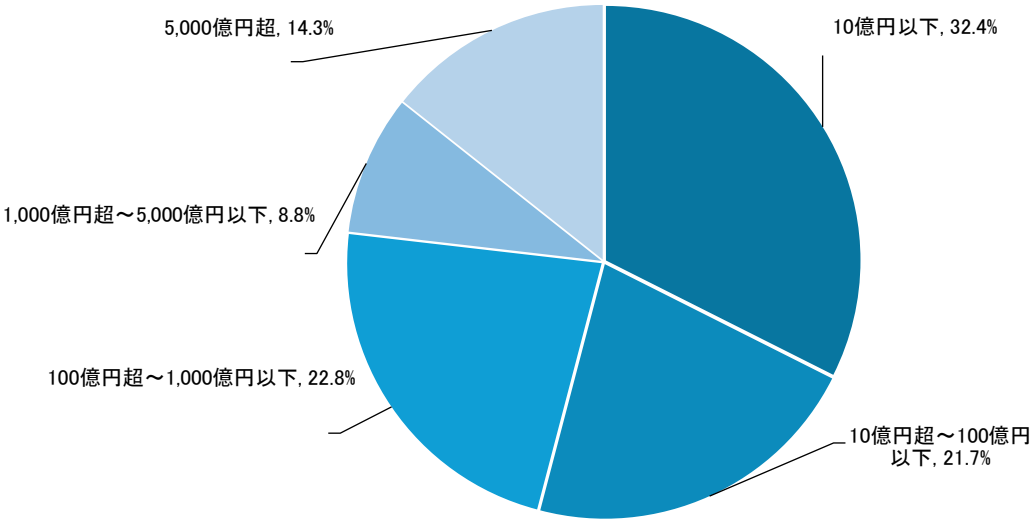


図 7 回答者の所属組織の売上高（2023 年度）(n=1200)

⑦ 回答者の所属部門

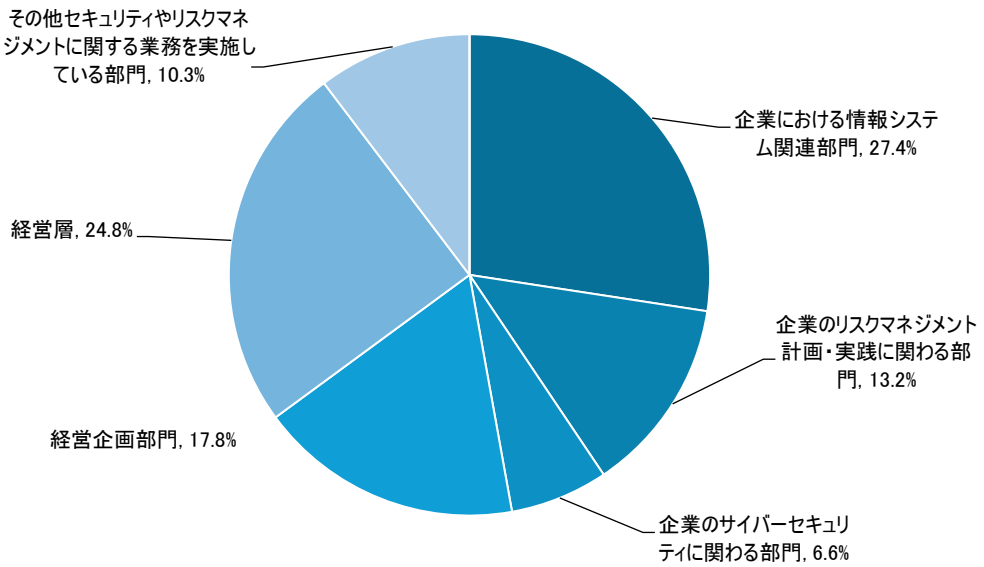


図 8 回答者の所属部門(n=1200)

⑧ 業種、従業員数、売上高毎で見る、所属部門が占める割合

表 2 業種、従業員数、売上高毎で見る、所属部門が占める割合

(%)

		企業における情報システム関連部門	企業のリスクマネジメント計画・実践に関わる部門	企業のサイバーセキュリティに関わる部門	経営企画部門	経営層	その他セキュリティやリスクマネジメントに関する業務を実施している部門
合計		27.4	13.2	6.6	17.8	24.8	10.3
業種	製造業	27.0	17.8	7.3	19.0	17.2	11.7
	非製造業	27.8	8.5	5.8	16.5	32.3	9.0
従業員数	301 人以上	38.7	15.8	8.7	19.2	5.7	12.0
	300 人以下	16.2	10.5	4.5	16.3	43.8	8.7
従業員数・業種	従業員数 301 人以上かつ製造業	36.0	19.7	7.7	20.7	4.0	12.0
	従業員数 300 人以下かつ製造業	18.0	16.0	7.0	17.3	30.3	11.3
	従業員数 301 人以上かつ非製造業	41.3	12.0	9.7	17.7	7.3	12.0
	従業員数 300 人以下かつ非製造業	14.3	5.0	2.0	15.3	57.3	6.0
売上高	10 億円以下	14.7	4.4	1.8	14.1	57.6	7.5
	10 億円超～100 億円以下	29.2	16.5	8.1	18.5	14.6	13.1
	100 億円超～1,000 億円以下	35.5	18.3	9.2	19.4	7.7	9.9
	1,000 億円超～5,000 億円以下	36.8	17.9	14.2	14.2	4.7	12.3
	5,000 億円超	34.9	16.9	6.4	24.4	5.2	12.2

1.3　留意事項

質問によっては、2020 年度調査の結果と比較（以下、経年比較という）しているが、2020 年度調査と本調査は調査方法が異なるため、回答の選択割合の差は参考に留めるべきである。

また、クロス集計表は、表内のどの数値とどの数値を比較するかという観点で、着色のパターンが異なる。3 パターンあるため、ご注意いただきたい。それぞれのパターンの説明は、以下の通りである。

・ **回答者全体での割合と、各系列での割合との比較**

(%)

（例）	選択肢 A	選択肢 B	選択肢 C	選択肢 D
合計	25.3	30.3	20.4	20.3
系列 1	21.5	36.7	29.7	27.8
系列 2	21.5	49.4	24.1	39.2
系列 3	20.7	28.6	19.2	17.8
系列 4	16.2	20.9	10.8	9.8

全員合計した際の割合に比べ、＋10 ポイント以上の場合、蜜柑色に着色している。

全員合計した際の割合に比べ、+5 ポイントの場合、黄色に着色している。

全員合計した際の割合に比べ、-5 ポイントの場合、水色に着色している。

全員合計した際の割合に比べ、-10 ポイントの場合、青色に着色している。

・ **選択肢ごと、系列間での割合の比較**

数値の大小に応じて赤から青のグラデーションに着色している。

(%)

（例）	選択肢 A	選択肢 B	選択肢 C
系列 1	67.6	20.6	47.1
系列 2	64.7	41.2	23.5
系列 4	58.6	24.1	34.5
系列 5	56.4	27.3	29.1
系列 6	56.0	12.0	44.0
系列 7	52.2	17.4	34.8
系列 8	46.2	7.7	38.5
系列 9	35.7	14.3	21.4

縦方向の比較

・ **系列ごと、選択肢間での割合の比較**

数値の大小に応じて橙から白のグラデーションに着色している。

(%)

（例）	選択肢 A	選択肢 B	選択肢 C
系列 1	19.5	17.2	13.0
系列 2	11.4	21.9	12.3
系列 3	13.6	11.4	15.9
系列 4	15.1	9.4	0.0

横方向の比較

2　調査結果

アンケート調査の本調査項目全 37 問について、質問ごとの集計結果を示す。なお、(SA)は単一回答、(MA)は複数回答を表す。

2.1　各設問の集計結果

2.1.1　営業秘密の漏えいの実態

Q1 あなたが所属する組織において、過去 5 年以内で営業秘密の漏えい事例はありましたか。(SA)

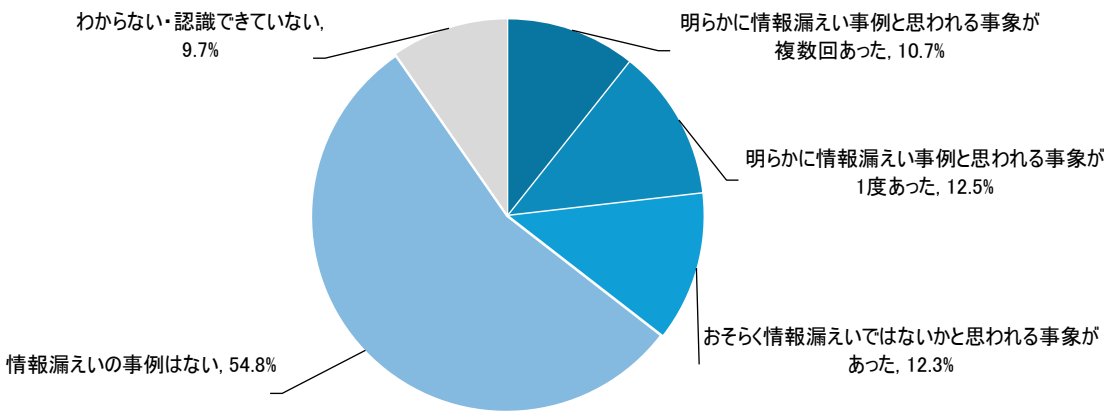


図 9 Q1 過去 5 年以内の営業秘密の漏えい事例の有無(n=1200)

過去 5 年以内の営業秘密の漏えい事例の経験の有無について、「明らかに情報漏えい事例と思われる事象が複数回あった」、「明らかに情報漏えい事例と思われる事象が 1 度あった」、及び「おそらく情報漏えいではないかと思われる事象があった」の 3 項目を合わせた割合は 35.5%となった。

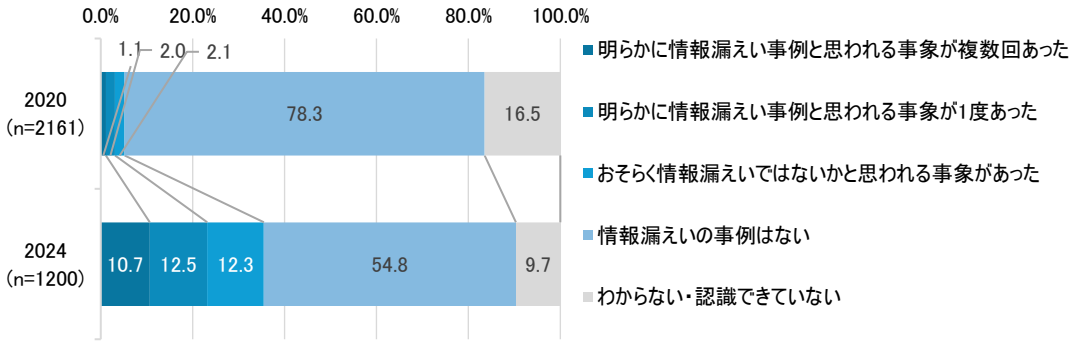


図 10 Q1 過去 5 年以内の営業秘密の漏えい事例の有無(経年比較)

2020 年度調査と比較すると、「明らかに情報漏えい事例と思われる事象が複数回あった」、「明らかに情報漏えい事例と思われる事象が 1 度あった」、及び「おそらく情報漏えいではないかと思われる事象があった」の 3 項目を合わせた割合は、5.2%から 35.5%となり、2020 年度調査と比較して顕著に増加していた。また、「わからない・認識できていない」の割合は 16.5%から 9.7%と減少した。

表 3 Q1 過去 5 年以内の営業秘密の漏えい事例の有無
(業種、従業員数、売上高、所属部門別)

(%)

		明らかに情報漏えい事例と思われる事象が複数回あった	明らかに情報漏えい事例と思われる事象が 1 度あった	おそらく情報漏えいではないかと思われる事象があった	情報漏えいの事例はない	わからない・認識できていない
合計		10.7	12.5	12.3	54.8	9.7
業種	製造業	12.2	13.5	14.5	51.2	8.7
	非製造業	9.2	11.5	10.2	58.5	10.7
従業員数	301 人以上	15.8	15.0	15.0	44.0	10.2
	300 人以下	5.5	10.0	9.7	65.7	9.2
従業員数・業種	従業員数 301 人以上かつ製造業	18.0	15.3	14.0	44.7	8.0
	従業員数 300 人以下かつ製造業	6.3	11.7	15.0	57.7	9.3
	従業員数 301 人以上かつ非製造業	13.7	14.7	16.0	43.3	12.3
	従業員数 300 人以下かつ非製造業	4.7	8.3	4.3	73.7	9.0
売上高	10 億円以下	2.8	5.1	5.4	76.9	9.8
	10 億円超～100 億円以下	8.5	15.8	16.2	49.2	10.4
	100 億円超～1,000 億円以下	13.9	19.4	16.8	42.5	7.3
	1,000 億円超～5,000 億円以下	20.8	14.2	17.9	37.7	9.4
	5,000 億円超	20.3	12.2	11.6	43.6	12.2
所属部門	企業における情報システム関連部門	15.2	13.7	11.6	47.7	11.9
	企業のリスクマネジメント計画・実践に関わる部門	14.6	29.1	25.3	27.2	3.8
	企業のサイバーセキュリティに関わる部門	26.6	34.2	13.9	22.8	2.5
	経営企画部門	9.4	9.4	9.9	59.2	12.2
	経営層	2.7	1.3	3.0	85.5	7.4
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	4.8	6.5	23.4	48.4	16.9

業種、従業員数、売上高、所属部門別に集計したところ、従業員数・業種別の区分で各項目の選択率に差が見られたので、従業員数・業種別の区分でグラフを作成した。

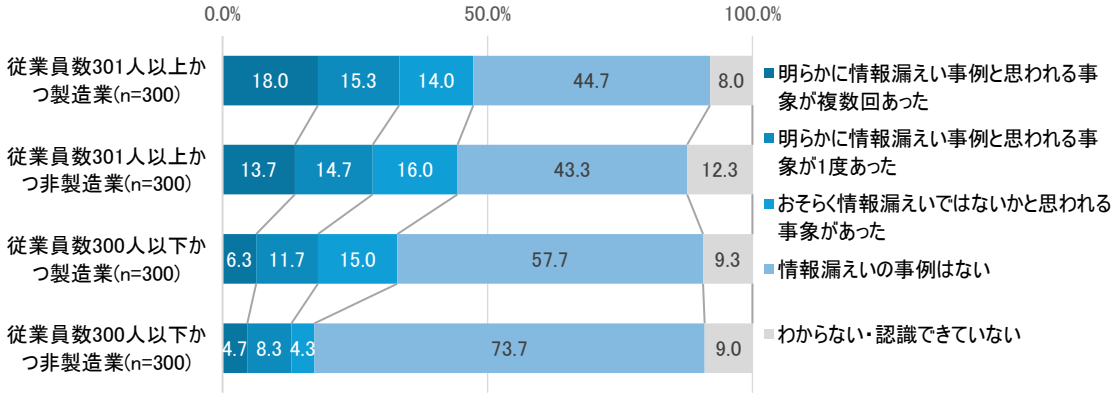


図 11 Q1 過去 5 年以内の営業秘密の漏えい事例の有無(従業員数・業種別)

従業員数・業種別では、「明らかに情報漏えい事例と思われる事象が複数回あった」、「明らかに情報漏えい事例と思われる事象が 1 度あった」、及び「おそらく情報漏えいではないかと思われる事象があった」の 3 項目を合わせた割合は、非製造業よりも製造業において高い傾向が見られ、また従業員数 301 人以上の企業の方が従業員数 300 人以下の企業よりも高い傾向が示された。

Q2 漏えいした営業秘密は、具体的にどのようなものでしたか。また、流出したそれぞれの営業秘密はあなたが所属する組織の事業においてどの程度重要な情報でしたか。複数流出している場合は、最も重要な情報について記載してください。（お答えはそれぞれ 1 つずつ）

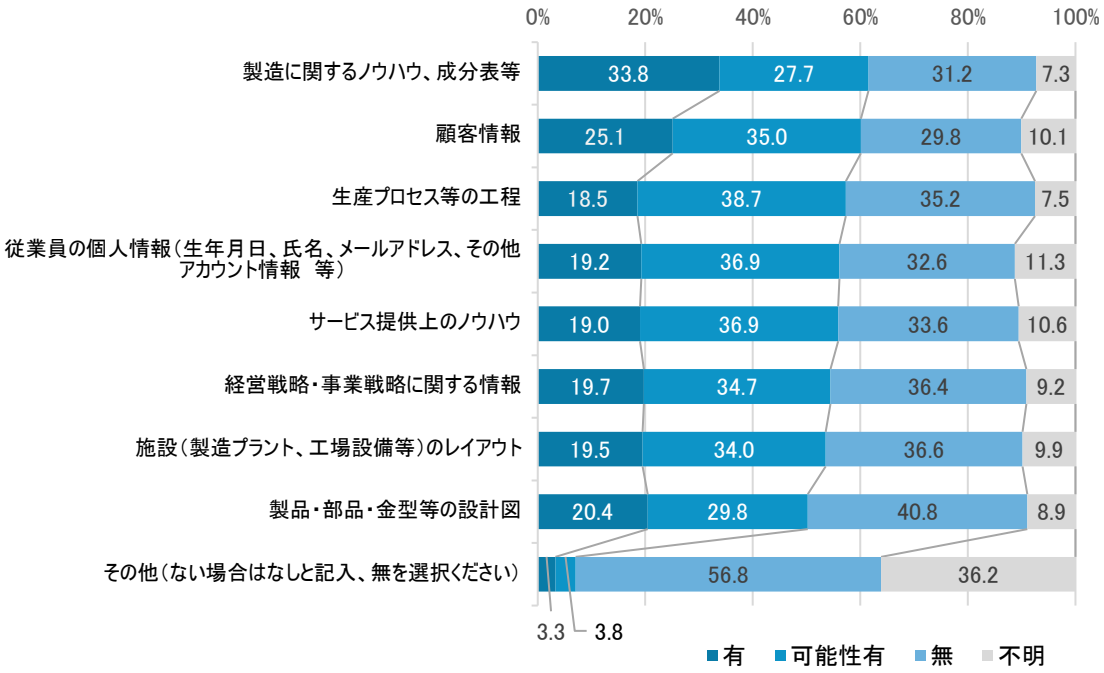


図 12 Q2 漏えいした情報の種類(n=426)

漏えいした情報の種類について、流出があった「有」及び流出の可能性があった「可能性有」の 2 項目を合計した割合は、「製造に関するノウハウ、成分表等」が最も高く 61.5%であった。次いで「顧客情報」が 60.1%、「生産プロセス等の工程」が 57.2%であった。

Q3 漏えいした営業秘密は、具体的にどのようなものでしたか。また、流出したそれぞれの営業秘密はあなたが所属する組織の事業においてどの程度重要な情報でしたか。複数流出している場合は、最も重要な情報について記載してください。（お答えはそれぞれ 1 つずつ）

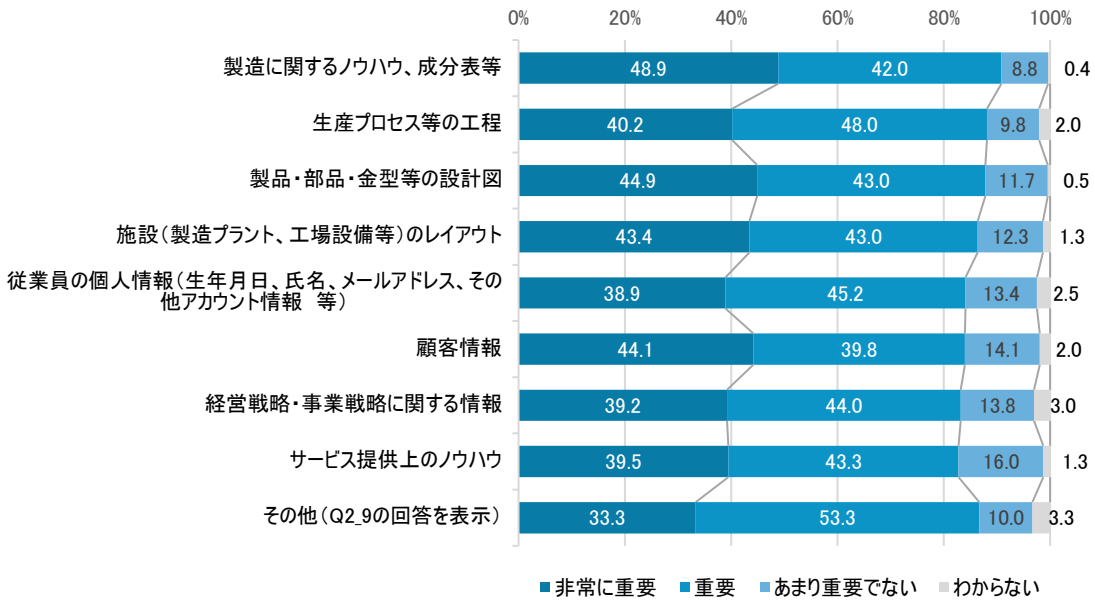


図 13 Q3 漏えいした情報の重要度(n=426)

漏えいした情報の重要度について、「製造に関するノウハウ、成分表等」では、「非常に重要」は 48.9%、「重要」は 42.0%で、合計すると 90.9%であり、当該情報を重要と捉えている割合は他の種類の情報に比べて最も高かった。その他の情報についても「非常に重要」と「重要」の割合を足すと 80%以上であった。

Q4 どのようなことから漏えい事例を認識しましたか。(MA)

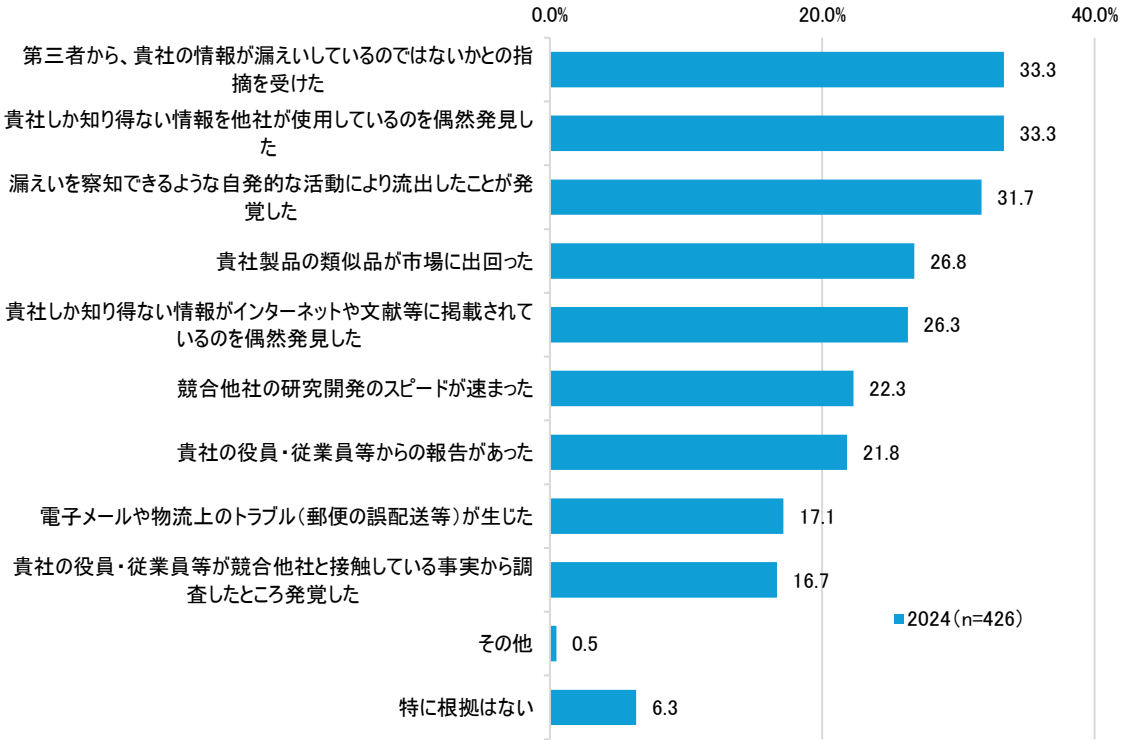


図 14 Q4 漏えい事例を認識したきっかけ(MA、n=426)

漏えい事例を認識したきっかけについて、最も割合が高かったのは「第三者から、貴社の情報が漏えいしているのではないかとの指摘を受けた」と「貴社しか知り得ない情報を他社が使用しているのを偶然発見した」の 2 項目で、33.3%であった。次いで、「漏えいを察知できるような自発的な活動により流出したことが発覚した」が 31.7%、「貴社製品の類似品が市場に出回った」が 26.8%であった。

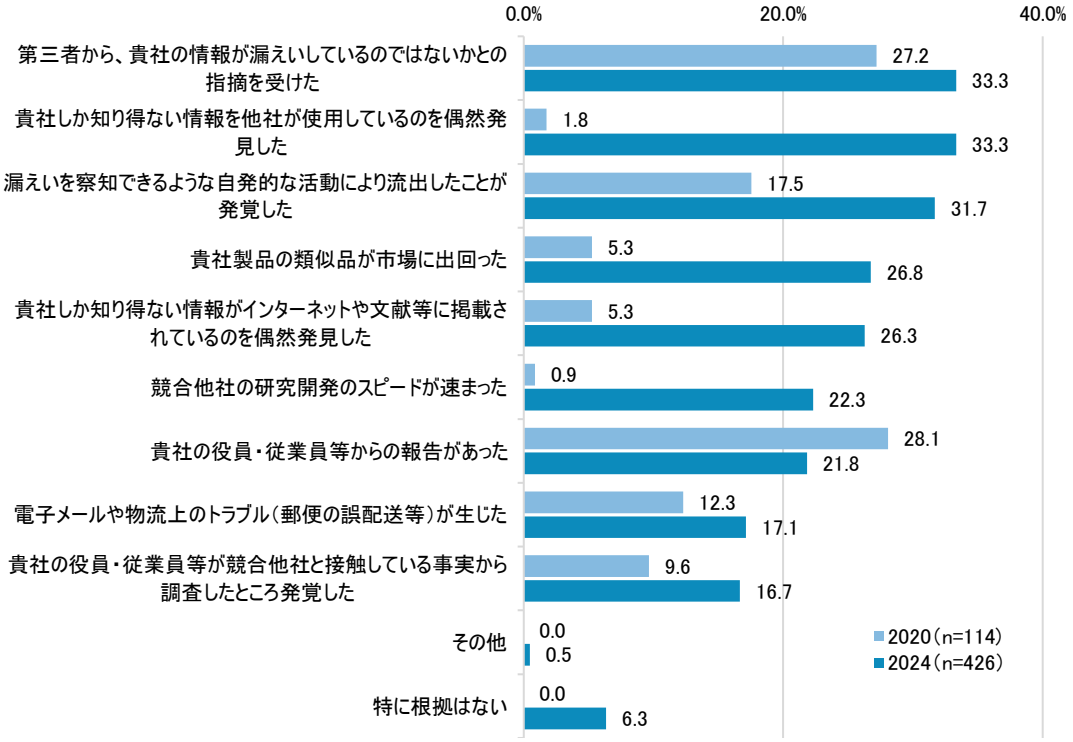


図 15 Q4 漏えい事例を認識したきっかけ（MA、経年比較）

2020 年度調査と比較すると、「第三者から、貴社の情報が漏えいしているのではないかとの指摘を受けた」の割合は、27.2%から 33.3%に微増していた。

また、2020 年度調査から割合が顕著に増加した項目があり、「貴社しか知り得ない情報を他社が使用しているのを偶然発見した」は 1.8%から 33.3%、に、「漏えいを察知できるような自発的な活動により流出したことが発覚した」は 17.5%から 31.7%に、「貴社製品の類似品が市場に出回った」は 5.3%から 26.8%に、「貴社しか知り得ない情報がインターネットや文献に掲載されているのを偶然発見した」は 5.3%から 26.3%に、「競合他社の研究開発のスピードが速まった」は 0.9%から 22.3%に増加した。

Q5 営業秘密の漏えいによって、どの程度の損害（2 回以上流出している場合はその合計）が生じていると考えていますか（大まかな推定で構いません）。（SA）

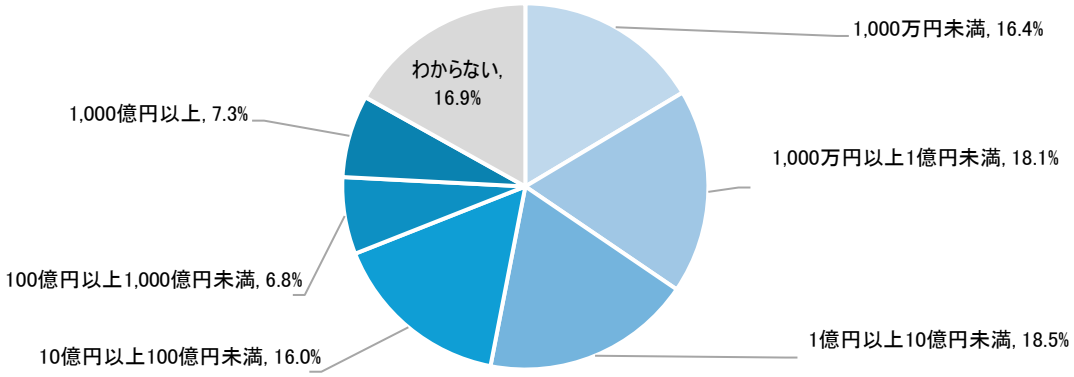


図 16 Q5 漏えいによる推定損害額（n=426）

漏えいによる推定損害額について、「1,000 万円未満」は全体の 16.4%を占めていた。「1,000 万円以上 1 億円未満」は 18.1%、「1 億円以上 10 億円未満」は 18.5%、「10 億円以上 1,000 億円未満」は 16.0%、「100 億円以上 1,000 億円未満」は 6.8%、「1,000 億円以上」は 7.3%であった。「わからない」は 16.9%であった。

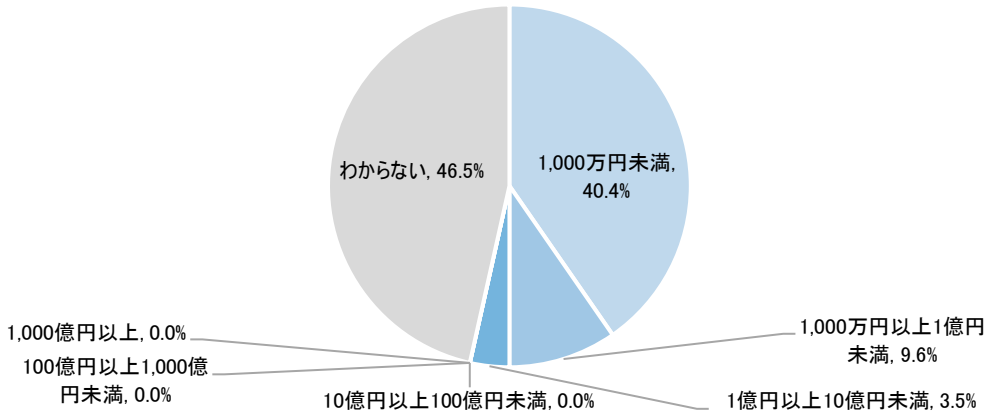


図 17 Q5 (参考) 漏えいによる推定損害額（2020 年度調査、n=114）

2020 年度調査と比較すると、10 億円以上の損害額の割合は 0%であったが、本調査では 30.0%と大幅に増加した。また、「1,000 万円以上 1 億円未満」の割合は 9.6%から 18.1%に、「1 億円以上 10 億円未満」の割合は 3.5%から 18.5%に増加した。「1,000 万円未満」の割合は、2020 年度調査では 40.4%であったところ 16.4%に減少した。

Q6 営業秘密はどこに漏えいしましたか（したと思いますか）。（MA）

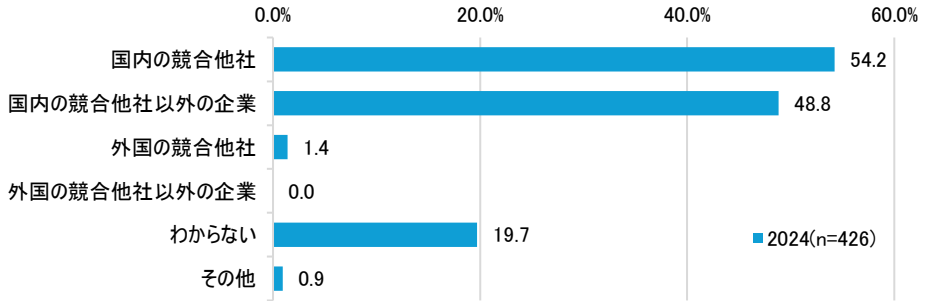


図 18 Q6 漏えい先(MA、n=426)

漏えい先について、最も割合の大きかったのは「国内の競合他社」で 54.2%、次いで「国内の競合他社以外の企業」が高く 48.8%であった。対して「外国の競合他社」は 1.4%、「外国の競合他社以外の企業」は 0%と、外国の競合他社への漏えいの割合は国内への漏えいと比較すると僅少であった。

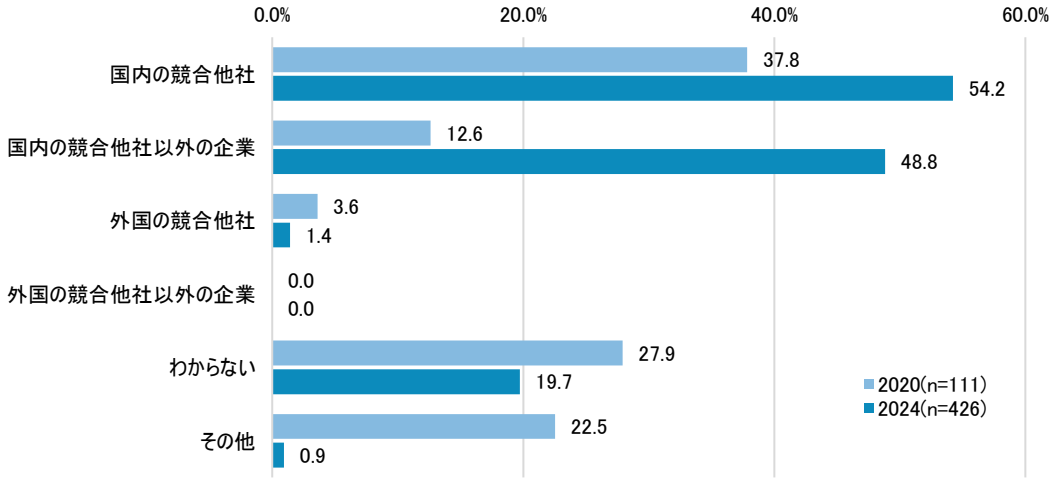


図 19 Q6 営業秘密の漏えい先（MA、経年比較)

2020 年度調査と比較したところ、「国内の競合他社」は 37.8%から 54.2%へ、「国内の競合他社以外の企業」は 12.6%から 48.8%へ、大きく増加していた。一方で、外国の競合他社への営業秘密漏えい割合は 3.6%から 1.4%へ微減した。

本調査では、「外国の競合他社」を選択した場合に自由記述にて漏えい先の国名を問うように設定したが、その回答の内訳は、中国が 3 件、アフリカが 2 件であった。

Q7 どのようなルートで、営業秘密の漏えい事例が発生しましたか。(MA)

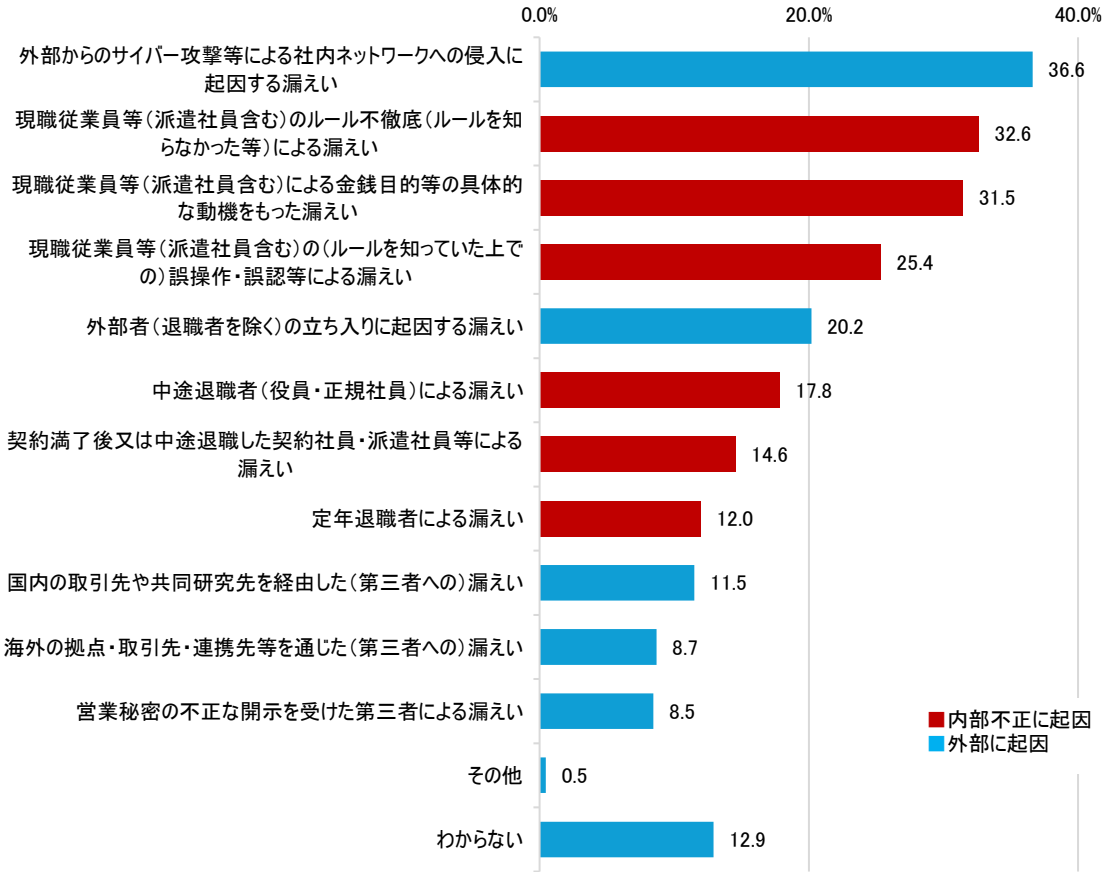


図 20 Q7 漏えいルート(MA、n=426)

営業秘密の漏えいルートについて、本調査で最も割合が大きかったのは、「外部からのサイバー攻撃等による社内ネットワークへの侵入に起因する漏えい」で 36.6%であった。次いで、「現職従業員等(派遣社員含む)のルール不徹底(ルールを知らなかった等)による漏えい」が 32.6%、「現職従業員等(派遣社員含む)による金銭目的等の具体的な動機を持った漏えい」が 31.5%、さらに、「現職従業員等(派遣社員含む)の(ルールを知っていた上での)誤操作・誤認等による漏えい」25.4%と、内部不正に起因する漏えいルートの選択割合が上位 2～4 位を占めた。また、外部に起因する漏えいルートの「外部者(退職者を除く)の立ち入りに起因する漏えい」の 20.2%をはさんで、再び内部不正に起因する漏えいルートに相当する項目が続き、「中途退職者(役員・正規社員)による漏えい」が 17.8%、「契約満了後又は中途退職した契約社員・派遣社員等による漏えい」が 14.6%、「定年退職者による漏えい」が 12.0%であった。

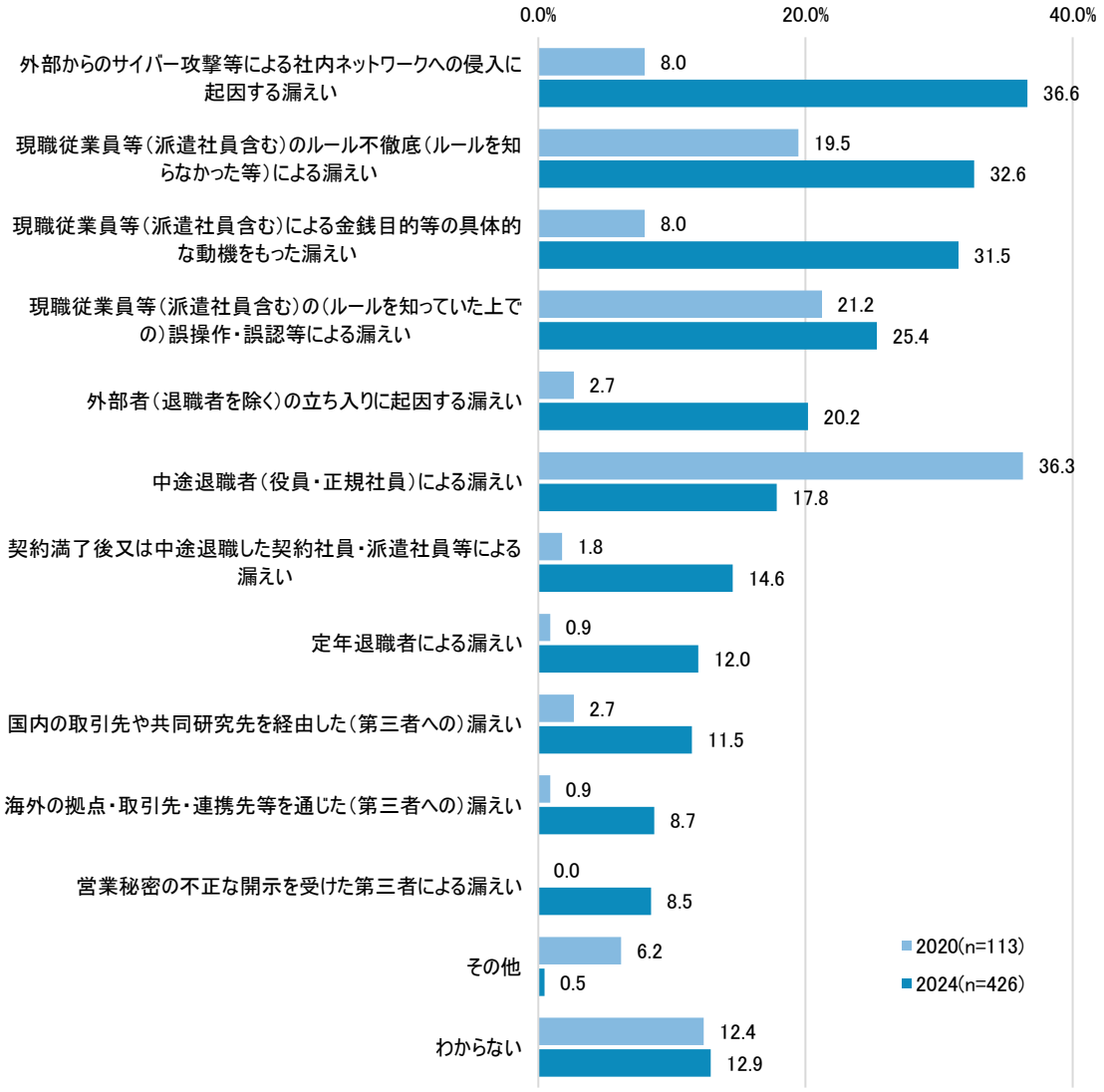
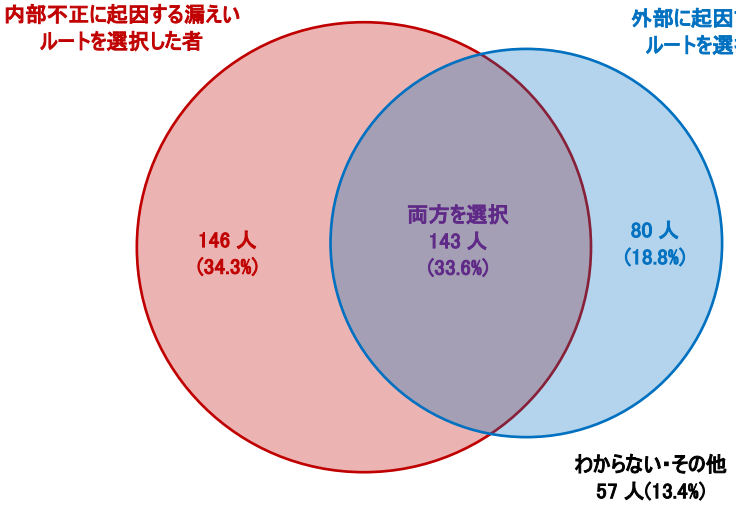


図 21 Q7 漏えいルート（MA、経年比較）

2020 年度調査と比較すると、「中途退職者（役職員・正規社員）による漏えい」は 36.3%から 17.8%に減少した一方で、その他の漏えいルートの割合は、いずれも増加した。特に、本調査で最も割合が大きかった「外部からのサイバー攻撃等による社内ネットワークへの侵入に起因する漏えい」は 8.0%から大幅に増加し 36.6%であった。また、「現職従業員等（派遣社員含む）のルール不徹底（ルールを知らなかった等）による漏えい」は 19.5%から 32.6%に増加、「現職従業員等（派遣社員含む）による金銭目的等の具体的な動機を持った漏えい」は 8.0%から 31.5%と大幅に増加、「現職従業員等（派遣社員含む）の（ルールを知っていた上での）誤操作・誤認等による漏えい」は 21.2%から 25.4%に増加した。



人数構成	300人以下	301人以上
全体n=426	137	232
内部不正 n=146	63	83
内外両方 n=143	45	98
外部に起因 n=80	29	51

図 22 Q7 営業秘密漏えい事例回答者のルートによる分類(n=426 人)

Q7 で回答者が内部不正に起因する漏えいルートと外部に起因する漏えいルートどちらを選択したかを分析したところ、内部不正に起因する漏えいルートのみを選択した回答者が 146 人(34.3%)、外部に起因する漏えいルートのみを選択した回答者は 80 人(18.8%)、内部不正に起因する漏えいルートと外部に起因する漏えいルート両方を選択した回答者は 143 人(33.6%)であった。

Q8 営業秘密の侵害行為を行った行為者・企業に対してどのような対応をとりましたか。(MA)

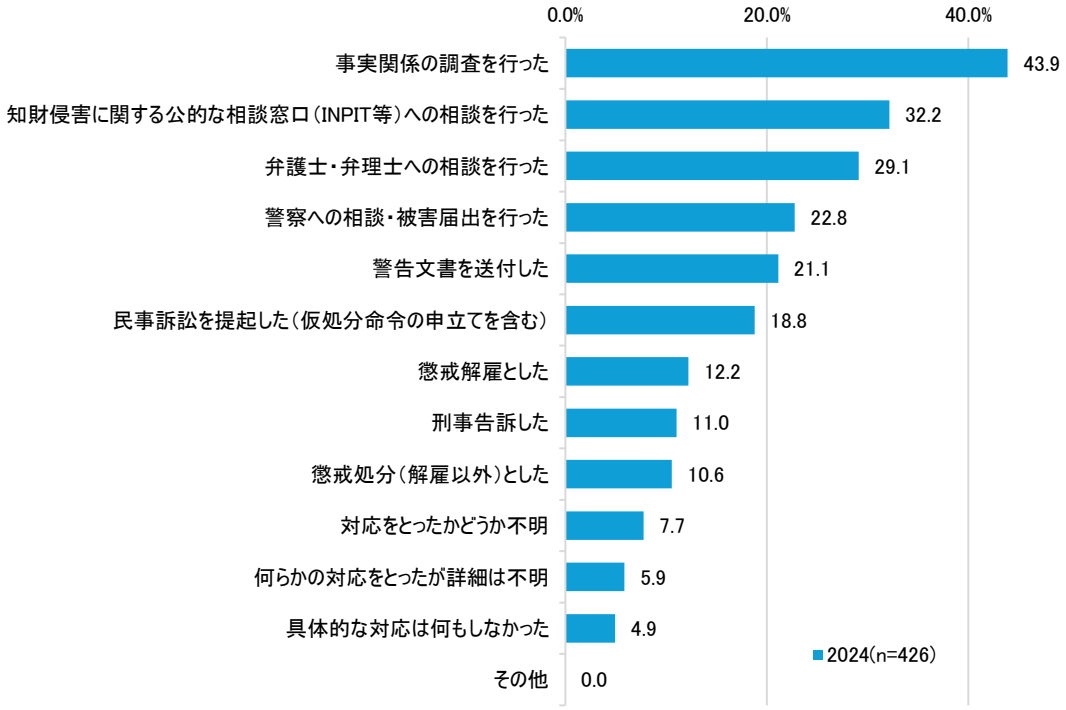


図 23 Q8 営業秘密の侵害行為への対応(MA、n=426)

営業秘密の侵害行為への対応について、「事実関係の調査を行った」が最も高く 43.9%であった。次いで、「知財侵害に関する公的な相談窓口(INPIT 等)への相談を行った」が 32.3%、「弁護士・弁理士への相談を行った」が 29.1%であった。

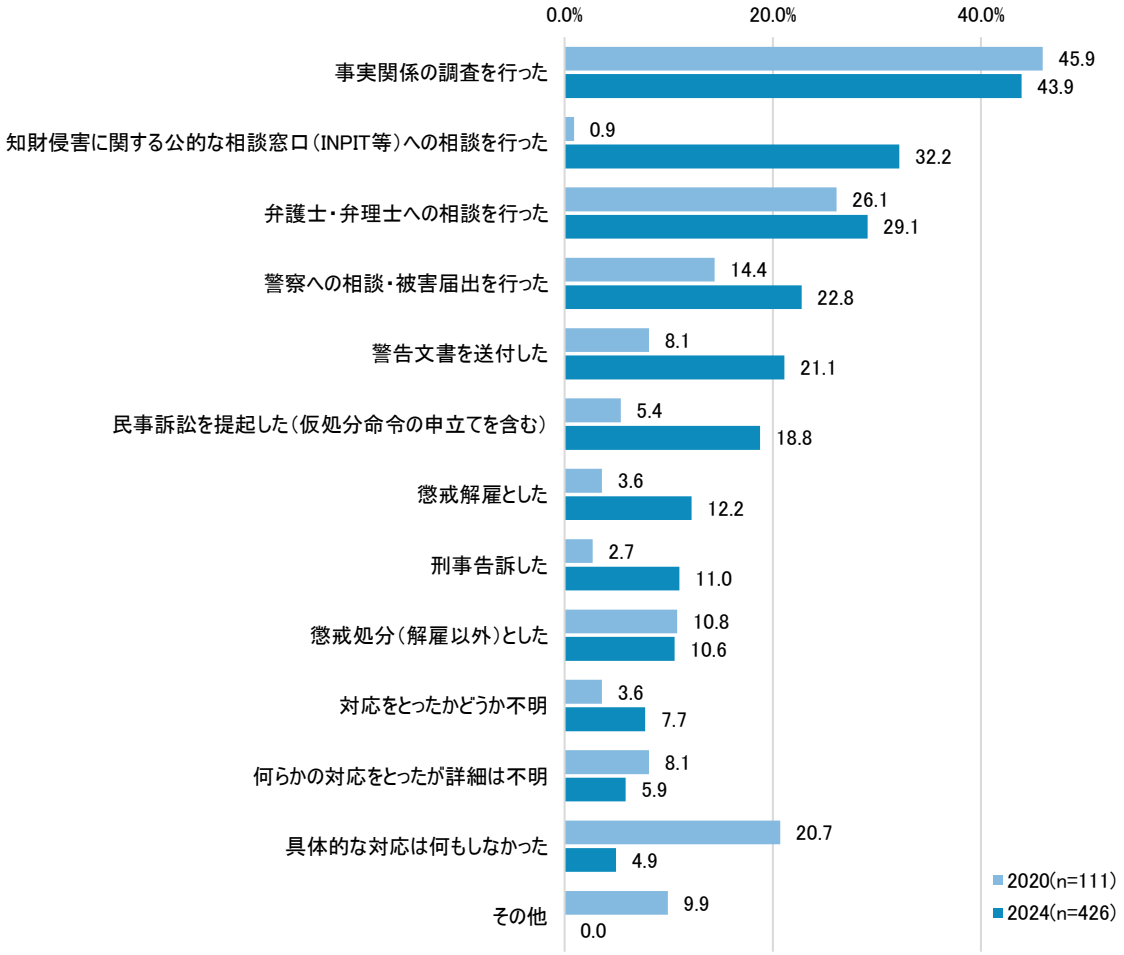


図 24 Q8 営業秘密の侵害行為への対応（MA、経年比較）

2020 年度調査と比較すると、「事実関係の調査を行った」は 2020 年度から最多であることは変わらないものの、45.9%から 43.9%にやや減少した。一方で、「知財侵害に関する公的な相談窓口（INPIT 等）への相談を行った」は 0.9%から 32.3%に大幅に増加し、「弁護士・弁理士への相談を行った」も 26.1%から 29.1%に増加、「警察への相談・被害届出」も 14.4%から 22.8%に増加した。さらに、「警告文書を送付した」は 8.1%から 21.1%に、「民事訴訟を提起した（仮処分命令の申立てを含む）」は 5.4%から 18.8%に、「懲戒解雇とした」は 3.6%から 12.2%に、「刑事告訴とした」は 2.7%から 11.0%に増加した。また、「具体的な対応は何もしなかった」の割合は 20.7%から 4.9%に大きく減少した。

Q9 営業秘密の漏えい後、以下の不審な現象は観察されましたか。(MA)

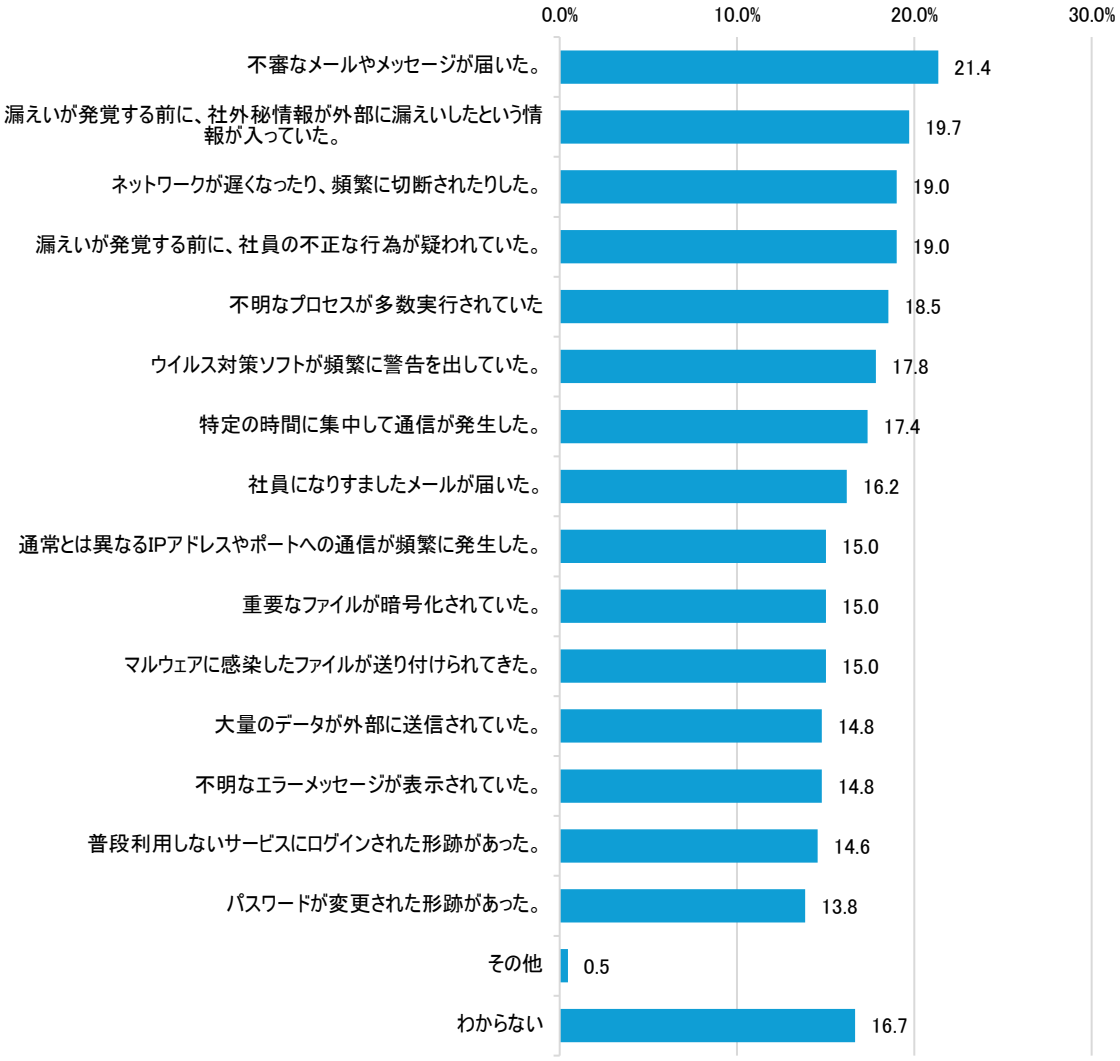


図 25 Q9 営業秘密の漏えい後に観察された不審な事象(MA、n=426)

営業秘密の漏えい後に観察された不審な事象について、いずれの不審な状況についても 15%～20%程度で、特段の傾向はみられなかったので、従業員数・業種別に集計を行った。

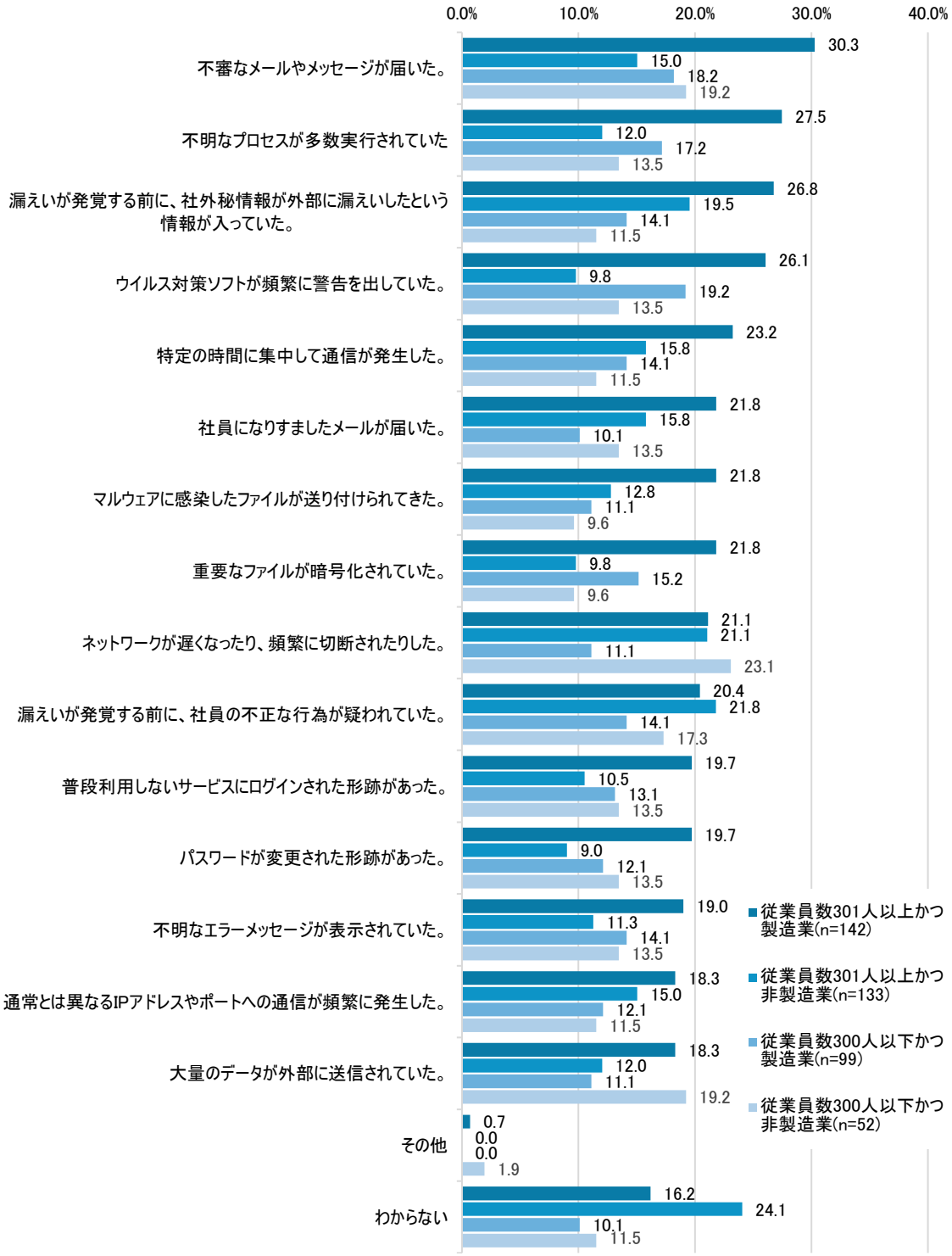


図 26 Q9 営業秘密の漏えい後に観察された不審な現象（従業員数・業種別集計、MA）

従業員数・業種別では、従業員数 301 人以上の製造業では、全体的に不審な現象を観測している割合が 20%～30%程度と、他の従業員数・業種区分に比べて高かった。

2.1.2　営業秘密管理の実態

Q10 自社の営業秘密の漏えいに関して、現在脅威と感じ、対策が必要と考えているものを、最大3つまで選択してください。（お答えは3つまで）

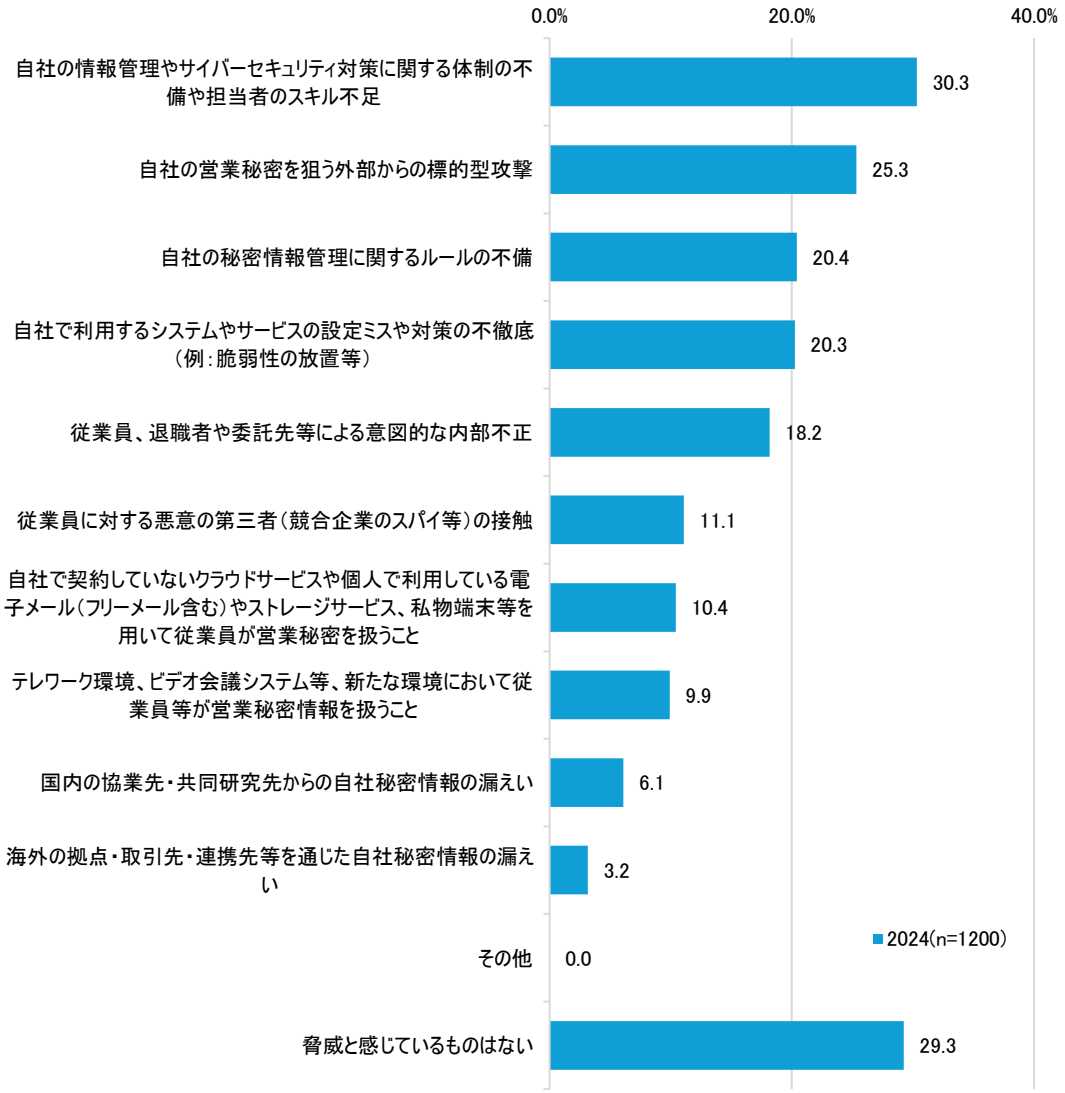


図 27 Q10 営業秘密の漏えいに関して必要な対策（最大3つ、n=1200）

営業秘密の漏えいに関して必要な対策としては、「自社の情報管理やサイバーセキュリティ対策に関する体制の不備や担当者のスキル不足」が最も高く 30.3%であった。次いで、「自社の営業秘密を狙う外部からの標的型攻撃」が 25.3%、「自社の秘密情報管理に関するルール不備」が 20.4%であった。

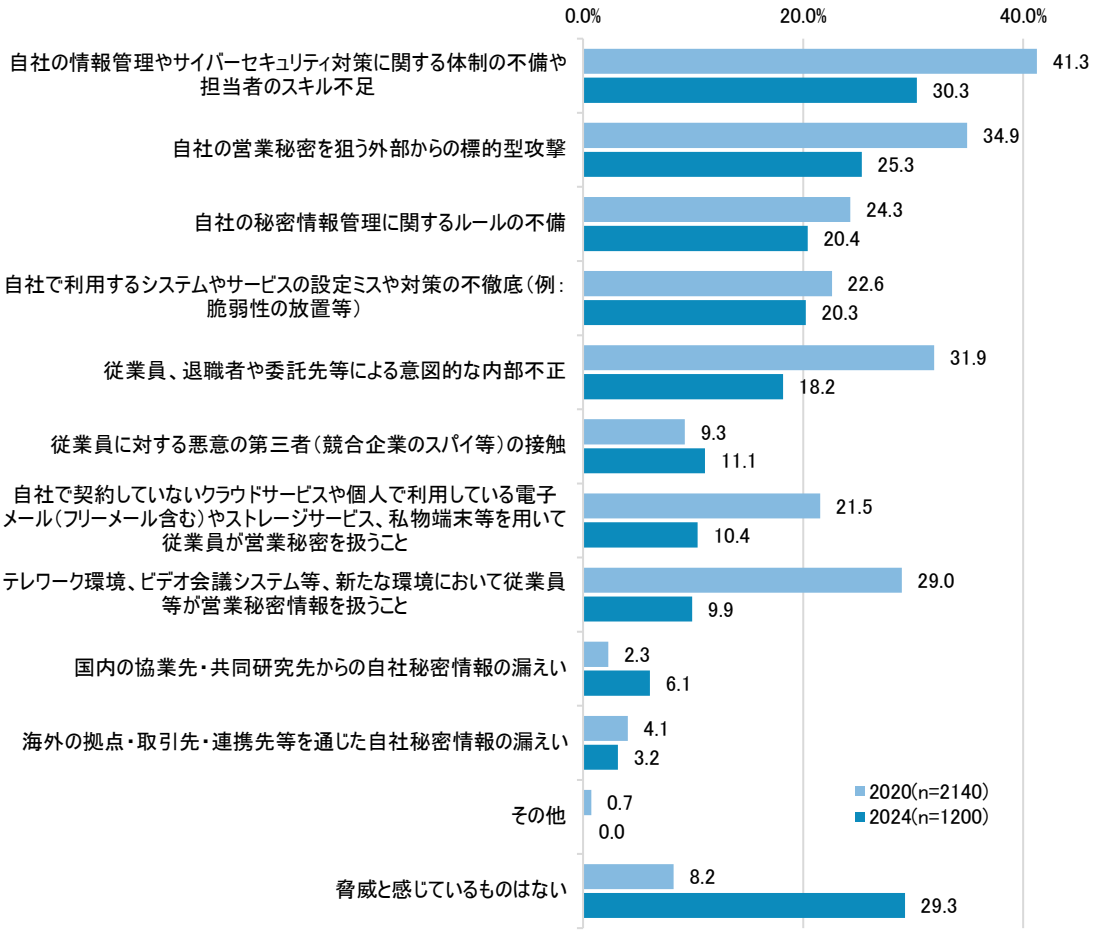


図 28 Q10 営業秘密の漏えいに関して必要な対策（経年比較）

2020 年度調査と比較すると、「自社の情報管理やサイバーセキュリティ対策に関する体制の不備や担当者のスキル不足」は 41.3%から 30.3%に減少した。また、「自社の営業秘密を狙う外部からの標的型攻撃」は 34.9%から 25.3%に、「従業員、退職者や委託先等による意図的な内部不正」は 31.9%から 18.2%に、「自社で契約していないクラウドサービスや個人で利用している電子メール（フリーメール含む）やストレージサービス、私物端末等を用いて従業員が営業秘密を扱うこと」は 21.5%から 10.4%に、「テレワーク環境、ビデオ会議システム等、新たな環境において従業員等が営業秘密情報を扱うこと」は 29.0%から 9.9%に減少した。

一方で、2020 年度調査から本調査で増加したものについて、「国内の協業先・共同研究先からの自社秘密情報の漏えい」は 2.3%から 6.1%に微増、「脅威と感じているものはない」は 8.2%から 29.3%に増加した。

表 4 Q10 営業秘密の漏えいに関して必要な対策
（業種、従業員数、売上高、所属部門別）

（%）

		自社の営業秘密を狙う外部からの標的型攻撃	自社の情報管理やサイバーセキュリティ対策に関する体制の不備や担当者のスキル不足	自社の秘密情報管理に関するルールの不備	自社で利用するシステムやサービスの設定ミスや対策の不徹底（例：脆弱性の放置等）	従業員、退職者や委託先等による意図的な内部不正	従業員に対する悪意の第三者（競合企業のスパイ等）の接触	自社で契約していないクラウドサービスや個人で利用している電子メール（フリーメール含む）やストレージサービス、私物端末等を用いて従業員が営業秘密を扱うこと	テレワーク環境、ビデオ会議システム等、新たな環境において従業員等が営業秘密情報を扱うこと	国内の協業先・共同研究先からの自社秘密情報の漏えい	海外の拠点・取引先・連携先等を通じた自社秘密情報の漏えい	その他	脅威と感じているものはない
合計		25.3	30.3	20.4	20.3	18.2	11.1	10.4	9.9	6.1	3.2	−	29.3
業種	製造業	27.7	33.8	22.7	24.0	19.8	12.0	11.2	11.7	7.0	4.2	−	21.5
	非製造業	23.0	26.8	18.2	16.5	16.5	10.2	9.7	8.2	5.2	2.2	−	37.0
従業員数	301 人以上	33.3	34.0	23.7	24.3	20.5	13.3	12.0	10.5	6.7	4.2	−	19.5
	300 人以下	17.3	26.7	17.2	16.2	15.8	8.8	8.8	9.3	5.5	2.2	−	39.0
従業員数・業種	従業員数 301 人以上かつ製造業	36.7	35.7	27.3	28.7	20.3	14.0	12.7	14.0	7.7	5.7	−	13.0
	従業員数 300 人以下かつ製造業	18.7	32.0	18.0	19.3	19.3	10.0	9.7	9.3	6.3	2.7	−	30.0
	従業員数 301 人以上かつ非製造業	30.0	32.3	20.0	20.0	20.7	12.7	11.3	7.0	5.7	2.7	−	26.0
	従業員数 300 人以下かつ非製造業	16.0	21.3	16.3	13.0	12.3	7.7	8.0	9.3	4.7	1.7	−	48.0
売上高	10 億円以下	15.4	23.1	12.1	13.4	12.1	7.2	6.9	7.2	4.6	2.1	−	50.4
	10 億円超～100 億円以下	21.9	31.9	26.5	20.0	22.3	10.4	11.5	11.9	6.9	2.3	−	23.5
	100 億円超～1,000 億円以下	27.1	34.8	20.9	23.8	21.2	14.7	14.3	9.2	6.2	4.8	−	19.0
	1,000 億円超～5,000 億円以下	34.9	35.8	28.3	25.5	28.3	11.3	9.4	12.3	9.4	4.7	−	12.3
	5,000 億円超	44.2	33.7	24.4	27.3	14.5	15.1	11.0	12.8	5.8	3.5	−	16.9
所属部門	企業における情報システム関連部門	39.2	32.8	23.7	22.5	18.5	10.9	9.7	10.3	4.3	3.0	−	23.4
	企業のリスクマネジメント計画・実践に関わる部門	21.5	36.7	29.7	27.8	29.1	15.2	13.3	12.0	7.0	3.8	−	11.4
	企業のサイバーセキュリティに関わる部門	21.5	49.4	24.1	39.2	25.3	17.7	13.9	10.1	8.9	2.5	−	7.6
	経営企画部門	20.7	28.6	19.2	17.8	18.3	12.2	9.9	9.9	7.0	4.7	−	28.2
	経営層	16.2	20.9	10.8	9.8	11.1	6.4	7.4	7.4	6.4	1.0	−	53.5
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	25.8	29.0	22.6	21.8	15.3	11.3	14.5	12.1	5.6	5.6	−	25.0

業種、従業員数、売上高、所属部門別に集計したところ、「自社の営業秘密を狙う外部からの標的型攻撃」については、従業員数 301 人以上の製造業、売上高 1,000 億円超、企業における情報システム関連部門のそれぞれの場合で、割合が全体＋5 ポイント以上であった。また、「自社の情報管理やサイバーセキュリティ対策に関する体制の不備や担当者のスキル不足」、「自社で利用するシステムやサービスの設定ミスや対策の不徹底（例：脆弱性の放置等）」の 2 項目は、従業員数 301 人以上の製造業、売上高 1,000 億円超、企業のリスクマネジメント計画・実践に関わる部門、企業のサイバーセキュリティに関わる部門の場合、回答者全体での割合に比べて、+5 ポイント以上であった。「自社の秘密情報管理に関するルールの不備」については、売上高 10 億円超～100 億円以下の企業でも割合が全体＋5 ポイント以上であった。

従業員数 300 人以下かつ非製造業、売上高 10 億円以下、経営層の区分では、「自社の営業秘密を狙う外部からの標的型攻撃」、「自社の情報管理やサイバーセキュリティ対策に関する体制の不備や担当者のスキル不足」、「自社の秘密情報管理に関するルールの不備」、「自社で利用するシステムやサービスの設定ミスや対策の不徹底（例：脆弱性の放置等）」、「従業員、退職者や委託先等による意図的な内部不正」の割合が、いずれも全体と比較して、－5 ポイント程度、低くなっていた。また、「脅威と感じているものはない」の割合が全体と比較して＋5 ポイント以上高かったのは、従業員数 300 人以下かつ非製造業、売上高 10 億円以下、経営層の区分であった。

Q11 内部不正を誘発する環境や状況として以下が例として挙げられます。あなたが所属する組織またはあなたの身の回りに当てはまるものはありますか。(MA)

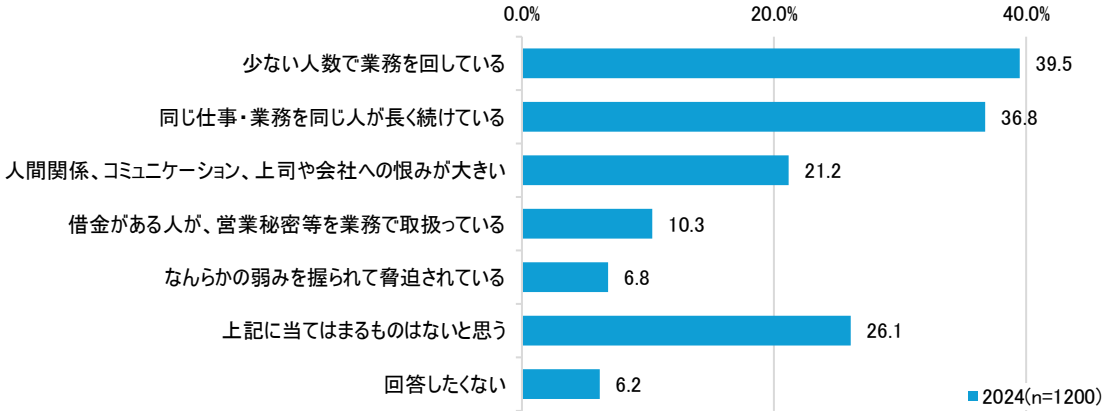


図 29 Q11 内部不正を誘発する環境や状況 (MA、n=1200)

内部不正を誘発する環境や状況について、「少ない人数で業務を回している」が最も高く 39.5%であった。次いで「同じ仕事・業務を同じ人が長く続きている」が 36.8%、「人間関係、コミュニケーション、上司や会社への恨みが大きい」が 21.2%であった。

表 5 Q11 内部不正を誘発する環境や状況
(業種、従業員数、所属部門別)

(%)

		同じ仕事・業務を同じ人が長く続けている	少ない人数で業務を回している	人間関係、コミュニケーション、上司や会社への恨みが大きい	借金がある人が、営業秘密等を業務で取扱っている	なんらかの弱みを握られて脅迫されている	上記に当てはまるものはないと思う	回答したくない
合計		36.8	39.5	21.2	10.3	6.8	26.1	6.2
業種	製造業	40.8	41.0	25.2	11.7	9.0	22.3	5.0
	非製造業	32.7	38.0	17.2	9.0	4.7	29.8	7.3
従業員数	301 人以上	40.3	35.8	26.2	14.2	9.5	20.5	9.0
	300 人以下	33.2	43.2	16.2	6.5	4.2	31.7	3.3
従業員数・業種	従業員数 301 人以上かつ製造業	47.0	38.0	29.7	15.3	13.3	18.0	6.3
	従業員数 300 人以下かつ製造業	34.7	44.0	20.7	8.0	4.7	26.7	3.7
	従業員数 301 人以上かつ非製造業	33.7	33.7	22.7	13.0	5.7	23.0	11.7
	従業員数 300 人以下かつ非製造業	31.7	42.3	11.7	5.0	3.7	36.7	3.0
所属部門	企業における情報システム関連部門	46.2	38.9	21.0	11.9	7.6	22.2	7.9
	企業のリスクマネジメント計画・実践に関わる部門	32.3	43.0	37.3	18.4	10.1	12.7	3.2
	企業のサイバーセキュリティに関わる部門	40.5	48.1	43.0	30.4	16.5	7.6	2.5
	経営企画部門	31.9	33.3	22.5	6.6	6.6	26.3	8.9
	経営層	32.0	38.7	5.4	1.7	1.0	45.1	4.7
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	34.7	43.5	22.6	10.5	8.9	19.4	6.5

業種、従業員数、所属部門別に集計したところ、「従業員数 301 人以上かつ製造業」の区分では、「同じ仕事・業務を同じ人が長く続けている」の割合が他の区分に比べて割合が大きく、合計の割合に比べて＋10 ポイント以上の 47.0%であった。また、「人間関係、コミュニケーション、上司や会社への恨みが大きい」についても比較的割合が大きく、合計の割合に比べて＋5 ポイント以上で 29.7%であった。「なんらかの弱みを握られて脅迫されている」についても比較的割合が大きく、合計の割合に比べて＋5 ポイント以上で、13.3%であった。「従業員数 300 人以下かつ非製造業」については、「上記に当てはまるものはないと思う」が高く、合計の割合に比べて 10 ポイント以上の 36.7%であった。

所属部門別では、部門ごとに各項目の選択率に違いが見られたので、棒グラフで部門間の選択率の差を見ることにした。

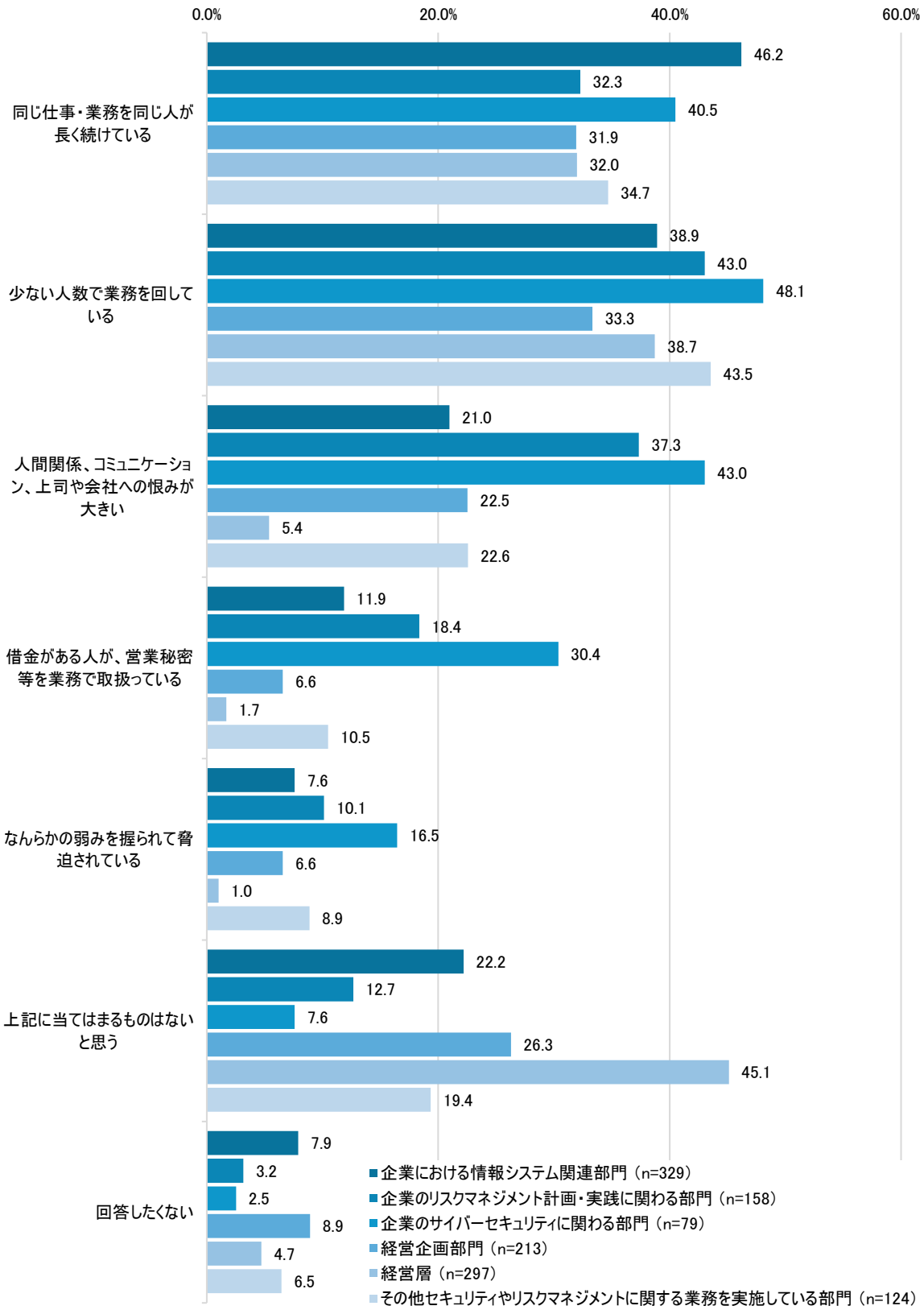


図 30 Q11 内部不正を誘発する環境や状況（MA、所属部門別）

所属部門別で見ると、「上記に当てはまるものはない」を選択した割合は経営層で最も大きく、45.1%であった。また、「同じ仕事・業務を同じ人が長く続けている」を選択した割合が高かったのは「企業における情報システム関連部門」で 46.2%、「少ない人数で業務を回している」を選択した割合が高かったのは「企業のリスクマネジメント計画・実践に関わる部門」で 43.0%、「人間関係、コミュニケーション、上司や会社への恨みが大きい」と「借金がある人が、営業秘密等を業務で取扱っている」、及び「何らかの弱みを握られて脅されている」といった人間関係による内部不正を誘発する環境や状況を選択した割合が高かったのは「企業のサイバーセキュリティに関わる部門」で、それぞれ 43.0%、30.4%、16.5%と、内部不正を誘発する環境や状況として認識しているものが異なる傾向が見られた。また、「経営層」では「上記に当てはまるものはないと思う」を選択した割合が高く 45.1%、「人間関係、コミュニケーション、上司や会社への恨みが大きい」等の人間関係による内部不正を誘発する環境や状況を選択している割合がいずれも 10%未満であった。

また、選択肢ごとに選択割合の差を見ると、人間関係による内部不正を誘発する環境や状況のうち「人間関係、コミュニケーション、上司や会社への恨みが大きい」において「企業におけるサイバーセキュリティに関わる部門」と「経営層」の間で差は最大となり 37.7%、それに比較して人手不足等の業務の遂行に直結する誘因については部門間での差が小さく、「同じ仕事・業務を同じ人が長く続きている」において「企業における情報システム部門」と「経営企画部門」との間で差は最大となり 14.3%であった。

Q12 あなたが所属する組織の保有する情報について、営業秘密とそれ以外の情報とを区分していますか。また、営業秘密をその秘密性のレベルに応じて格付け(「極秘」、「秘」など)していますか。(SA)

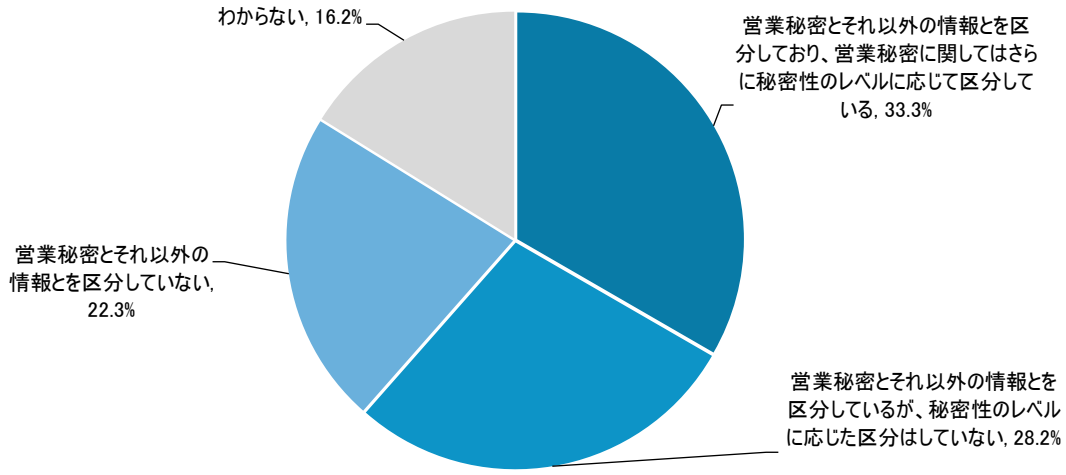


図 31 Q12 営業秘密の区分及び格付け実施の有無(n=1200)

営業秘密との区分及び格付け実施について、「営業秘密とそれ以外の情報とを区分しており、営業秘密に関してはさらに秘密性のレベルに応じて区分している」が最も高く 33.3%であった。次いで、「営業秘密とそれ以外の情報とを区分しているが、秘密性のレベルに応じた区分はしていない」が 28.2%、「営業秘密とそれ以外の情報とを区分していない」が 22.3%、「わからない」が 16.2%であった。

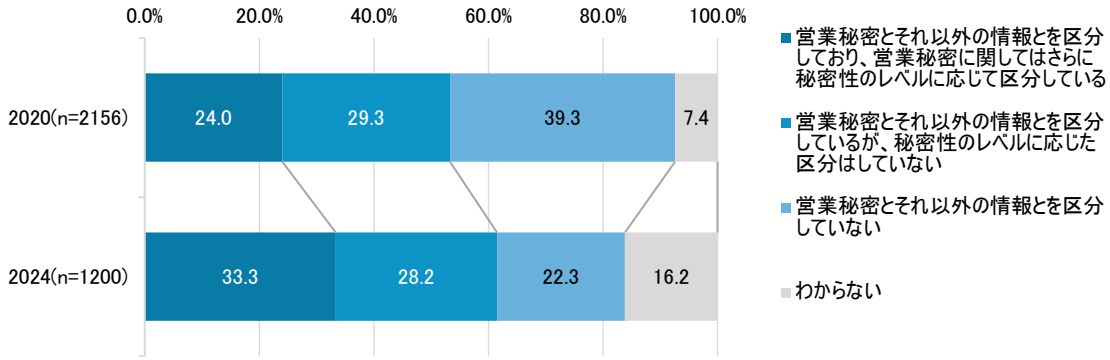


図 32 Q12 営業秘密の区分及び格付け実施の有無(経年比較)

2020 年度調査と比較すると、「営業秘密とそれ以外の情報とを区分しており、営業秘密に関してはさらに秘密性のレベルに応じて区分している」と「営業秘密とそれ利害の情報とを区分しているが、秘密性のレベルに応じた区分はしていない」を合わせた、営業秘密情報を区分して管理している割合は 53.3%から 61.5%に増加していた。

表 6 Q12 営業秘密の区分及び格付け実施の有無
（業種、従業員数、売上高、所属部門別）

(%)

		営業秘密とそれ以外の情報とを区分しており、営業秘密に関してはさらに秘密性のレベルに応じて区分している	営業秘密とそれ以外の情報とを区分しているが、秘密性のレベルに応じた区分はしていない	営業秘密とそれ以外の情報とを区分していない	わからない
合計		33.3	28.2	22.3	16.2
業種	製造業	37.8	28.8	19.2	14.2
	非製造業	28.8	27.5	25.5	18.2
従業員数	301 人以上	45.5	27.8	9.2	17.5
	300 人以下	21.2	28.5	35.5	14.8
従業員数・業種	従業員数 301 人以上かつ製造業	52.3	26.7	7.3	13.7
	従業員数 300 人以下かつ製造業	23.3	31.0	31.0	14.7
	従業員数 301 人以上かつ非製造業	38.7	29.0	11.0	21.3
	従業員数 300 人以下かつ非製造業	19.0	26.0	40.0	15.0
売上高	10 億円以下	17.7	23.4	41.9	17.0
	10 億円超～100 億円以下	31.5	33.5	19.6	15.4
	100 億円超～1,000 億円以下	35.9	35.5	13.6	15.0
	1,000 億円超～5,000 億円以下	50.0	32.1	3.8	14.2
	5,000 億円超	57.0	16.9	7.6	18.6
所属部門	企業における情報システム関連部門	44.4	20.4	14.3	21.0
	企業のリスクマネジメント計画・実践に関わる部門	41.8	38.0	9.5	10.8
	企業のサイバーセキュリティに関わる部門	45.6	41.8	3.8	8.9
	経営企画部門	27.2	31.0	25.8	16.0
	経営層	18.5	22.6	43.8	15.2
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	31.5	36.3	14.5	17.7

業種、従業員数、売上高、所属部門別に集計したところ、従業員数・業種別では、「従業員数 301 人以上の製造業」では 52.3%、「従業員数 301 人以上の非製造業」では 38.7%と割合が高い。所属部門別では、「企業における情報システム関連部門」、「企業のリスクマネジメント計画・実装に関わる部門」、「企業のサイバーセキュリティに関わる部門」において、営業秘密情報を区分して管理している割合が全体と比べて＋5 ポイント以上であり、「経営企画部門」及び「経営層」においては全体－5 ポイント以上であった。

「わからない」選択をした割合が顕著に低かったのは、「企業のリスクマネジメント計画・実装に関わる部門」の 10.8%と「企業のサイバーセキュリティに関わる部門」の 8.9%で、その他の部門ではあまり傾向に差は見られなかった。

Q13 あなたが所属する組織の保有する営業秘密について、社内規程として定められた管理ルールはどの程度厳密に運用されているとお考えですか（例：エビデンスを残す、定期的な内部監査・アセスメントの実施等）。（SA）

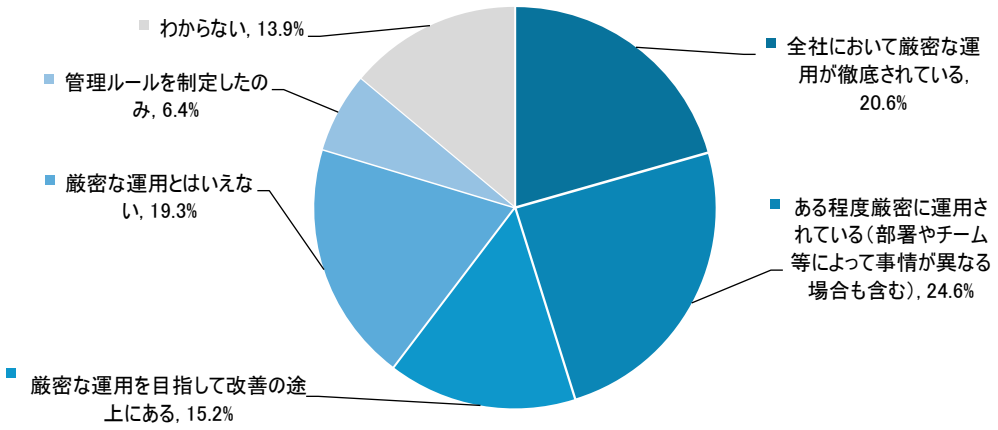


図 33 Q13 営業秘密の管理ルールの運用状況(n=1200)

営業秘密の管理ルールの運用状況について、「全体において厳密な運用が徹底されている」は20.6%、「ある程度厳密に運用されている（部署やチーム等によって事情が異なる場合も含む）」は24.5%、「厳密な運用を目指して改善の途上にある」は 15.2%、「厳密な運用とはいえない」は19.3%、「管理ルールを制定したのみ」は 6.4%、「わからない」は 13.9%であった。

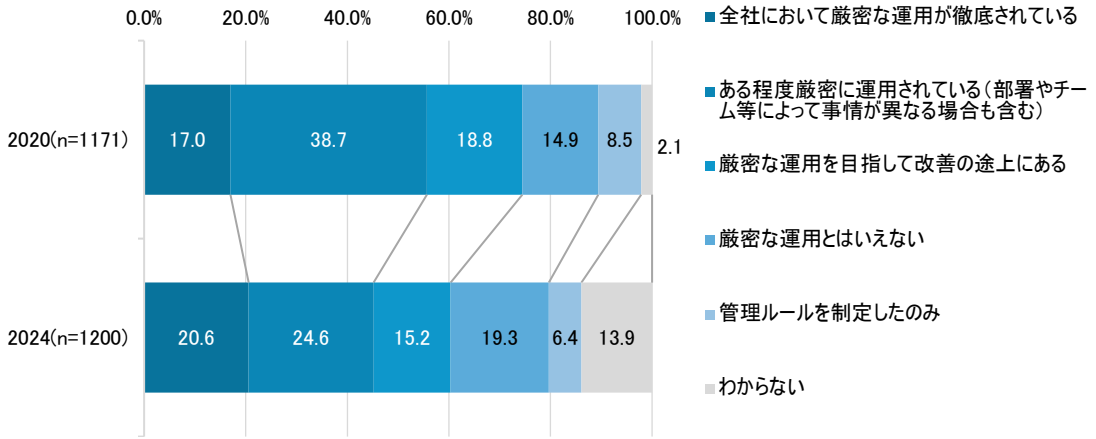


図 34 Q13 社内規程として定められた管理ルールの運用状況（経年比較）

2020 年度調査と比較すると、「全体において厳密な運用が徹底されている割合」が 2020 年度調査の 17.0%から 20.6%に微増している。

一方で、「ある程度厳密に運用されている（部署やチーム等によって事情が異なる場合も含む）」、「厳密な運用を目指して改善の途中にある」及び「管理ルールを制定したのみ」の 3 項目は、2020

年度調査から減少していた。「ある程度厳密に運用されている（部署やチーム等によって事情が異なる場合も含む）」は 38.7%から 24.6%に、「厳密な運用を目指して改善の途中にある」は 18.8%から 15.2%に、「管理ルールを制定したのみ」は 8.5%から 6.4%に減少した。さらに、「厳密な運用とはいえない」は 14.3%から 19.5%に微増し、「わからない」は 2.1%から 13.9%と大幅に増加した。

Q14 営業秘密情報の保護対策を実践する上で問題と感じる事項を選択してください。（MA）

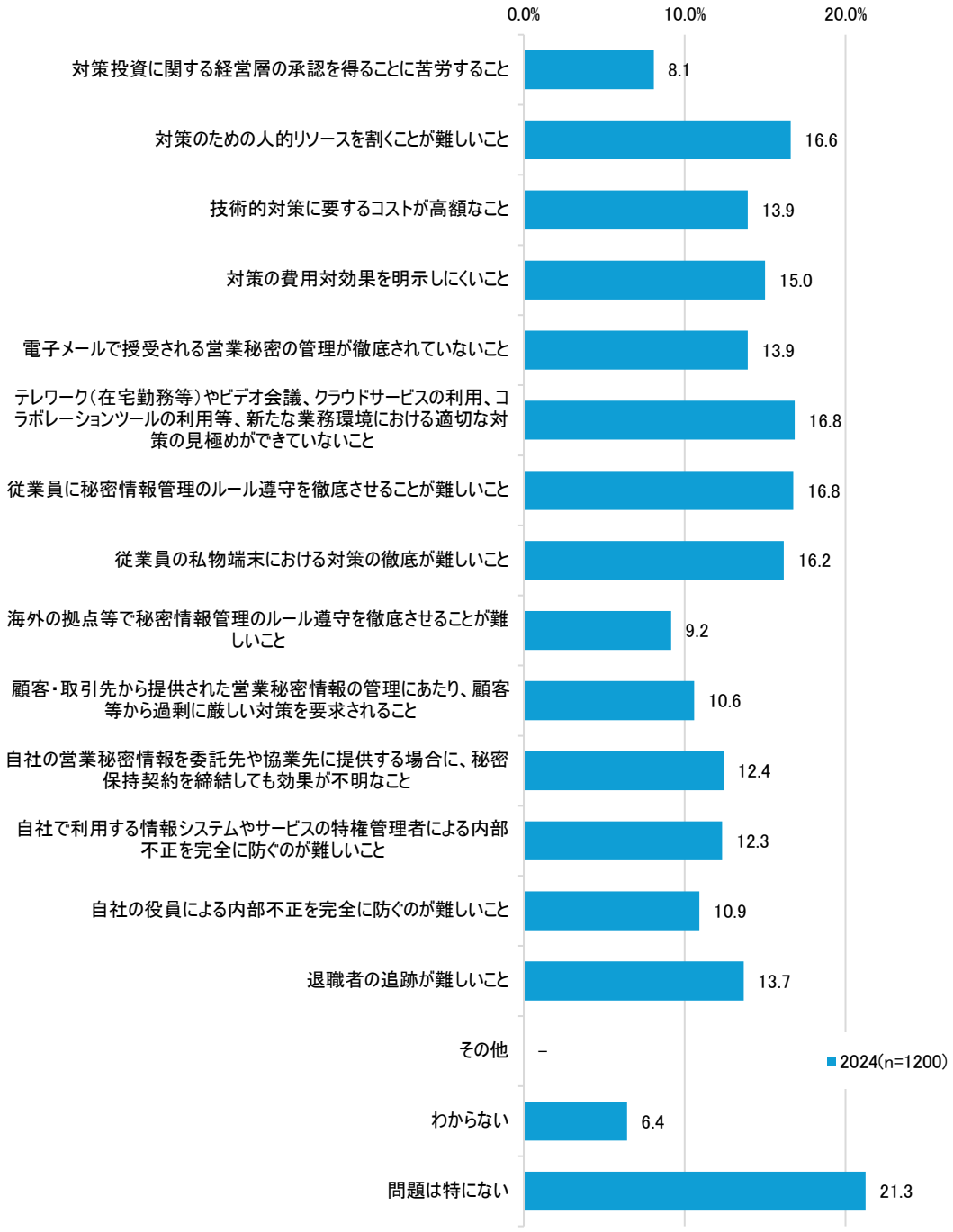


図 35 Q14 営業秘密管理を実践する上での問題（MA、n=1200）

営業秘密管理を実践する上での問題について、全体で見るといずれの項目についても 10%程度から 20%未満であり、特に意識されている項目はなかった。

表 7 Q14 営業秘密管理を実践する上での問題 (業種、従業員数、売上高、所属部門別)

(%)

		対策投資に関する経営層の承認を得ることに苦労すること	対策のための人的リソースを割くことが難しいこと	技術的対策に要するコストが高額なこと	対策の費用対効果を明示しにくいこと	電子メールで授受される営業秘密の管理が徹底されていないこと	テレワーク(在宅勤務等)やビデオ会議、クラウドサービスの利用、コラボレーションツールの利用等、新たな業務環境における適切な対策の見極めができていないこと	従業員に秘密情報管理のルール遵守を徹底させることが難しいこと	従業員の私物端末における対策の徹底が難しいこと	海外の拠点等で秘密情報管理のルール遵守を徹底させることが難しいこと	顧客・取引先から提供された営業秘密情報の管理にあたり、顧客等から過剰に厳しい対策を要求されること	自社の営業秘密情報を委託先や協業先に提供する場合に、秘密保持契約を締結しても効果が不明なこと	自社で利用する情報システムやサービスの特権管理者による内部不正を完全に防ぐのが難しいこと	自社の役員による内部不正を完全に防ぐのが難しいこと	退職者の追跡が難しいこと	その他	わからない	問題は特にない
合計		8.1	16.6	13.9	15.0	13.9	16.8	16.8	16.2	9.2	10.6	12.4	12.3	10.9	13.7	−	6.4	21.3
業種	製造業	9.3	19.3	15.5	15.7	16.5	19.8	20.7	16.8	12.2	12.2	14.5	15.7	12.3	15.8	−	5.8	15.2
	非製造業	6.8	13.8	12.3	14.3	11.3	13.8	12.8	15.5	6.2	9.0	10.3	9.0	9.5	11.5	−	7.0	27.3
従業員数	301 人以上	10.8	18.8	14.2	15.5	16.8	22.0	18.5	18.2	12.5	12.8	16.7	17.2	13.8	16.2	−	8.3	12.8
	300 人以下	5.3	14.3	13.7	14.5	11.0	11.7	15.0	14.2	5.8	8.3	8.2	7.5	8.0	11.2	−	4.5	29.7
従業員数・業種	従業員数 301 人以上かつ製造業	14.0	22.3	17.3	16.3	20.0	25.7	23.0	19.0	16.7	14.7	20.7	23.0	14.7	18.0	−	7.0	8.3
	従業員数 300 人以下かつ製造業	4.7	16.3	13.7	15.0	13.0	14.0	18.3	14.7	7.7	9.7	8.3	8.3	10.0	13.7	−	4.7	22.0
	従業員数 301 人以上かつ非製造業	7.7	15.3	11.0	14.7	13.7	18.3	14.0	17.3	8.3	11.0	12.7	11.3	13.0	14.3	−	9.7	17.3
	従業員数 300 人以下かつ非製造業	6.0	12.3	13.7	14.0	9.0	9.3	11.7	13.7	4.0	7.0	8.0	6.7	6.0	8.7	−	4.3	37.3
売上高	10 億円以下	4.1	13.1	13.1	12.3	7.7	9.5	12.9	12.9	2.8	7.2	7.2	5.4	6.4	8.2	−	5.1	39.6
	10 億円超～100 億円以下	6.2	17.7	11.9	14.6	16.5	14.2	18.8	19.2	8.8	8.8	11.9	11.2	10.0	17.7	−	6.5	12.3
	100 億円超～1,000 億円以下	11.4	18.3	15.0	16.5	17.2	21.6	17.6	18.3	12.5	15.0	13.2	17.2	13.2	12.8	−	6.2	12.8
	1,000 億円超～5,000 億円以下	10.4	17.9	13.2	15.1	18.9	22.6	18.9	10.4	11.3	11.3	20.8	17.9	11.3	18.9	−	7.5	10.4
	5,000 億円超	13.4	19.2	17.4	19.2	15.7	26.2	19.8	19.2	17.4	13.4	18.6	18.6	18.6	18.0	−	8.7	13.4
所属部門	企業における情報システム関連部門	10.6	19.5	14.3	17.3	13.1	20.4	20.1	16.4	11.9	11.9	12.8	15.2	12.5	12.8	−	11.2	16.7
	企業のリスクマネジメント計画・実践に関わる部門	15.8	22.8	16.5	16.5	17.7	22.8	22.8	25.9	20.3	17.1	20.3	20.9	21.5	18.4	−	0.6	6.3
	企業のサイバーセキュリティに関わる部門	13.9	20.3	19.0	19.0	29.1	32.9	17.7	15.2	12.7	19.0	21.5	20.3	16.5	22.8	−	3.8	5.1
	経営企画部門	5.2	11.7	12.2	12.2	14.6	16.4	18.8	13.1	4.2	8.5	9.9	10.8	8.9	14.6	−	7.0	17.8
	経営層	2.4	12.5	12.1	13.8	7.4	7.7	10.1	11.8	4.0	5.4	8.4	5.1	3.4	8.4	−	4.0	45.5
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	6.5	16.9	13.7	12.1	16.1	12.1	12.1	19.4	6.5	9.7	9.7	8.9	11.3	15.3	−	7.3	10.5

業種、従業員数、売上高、所属部門別に集計したところ、従業員数・業種別と、所属部門別の集計結果において、割合にばらつきが見られたので、それぞれグラフを作成した。

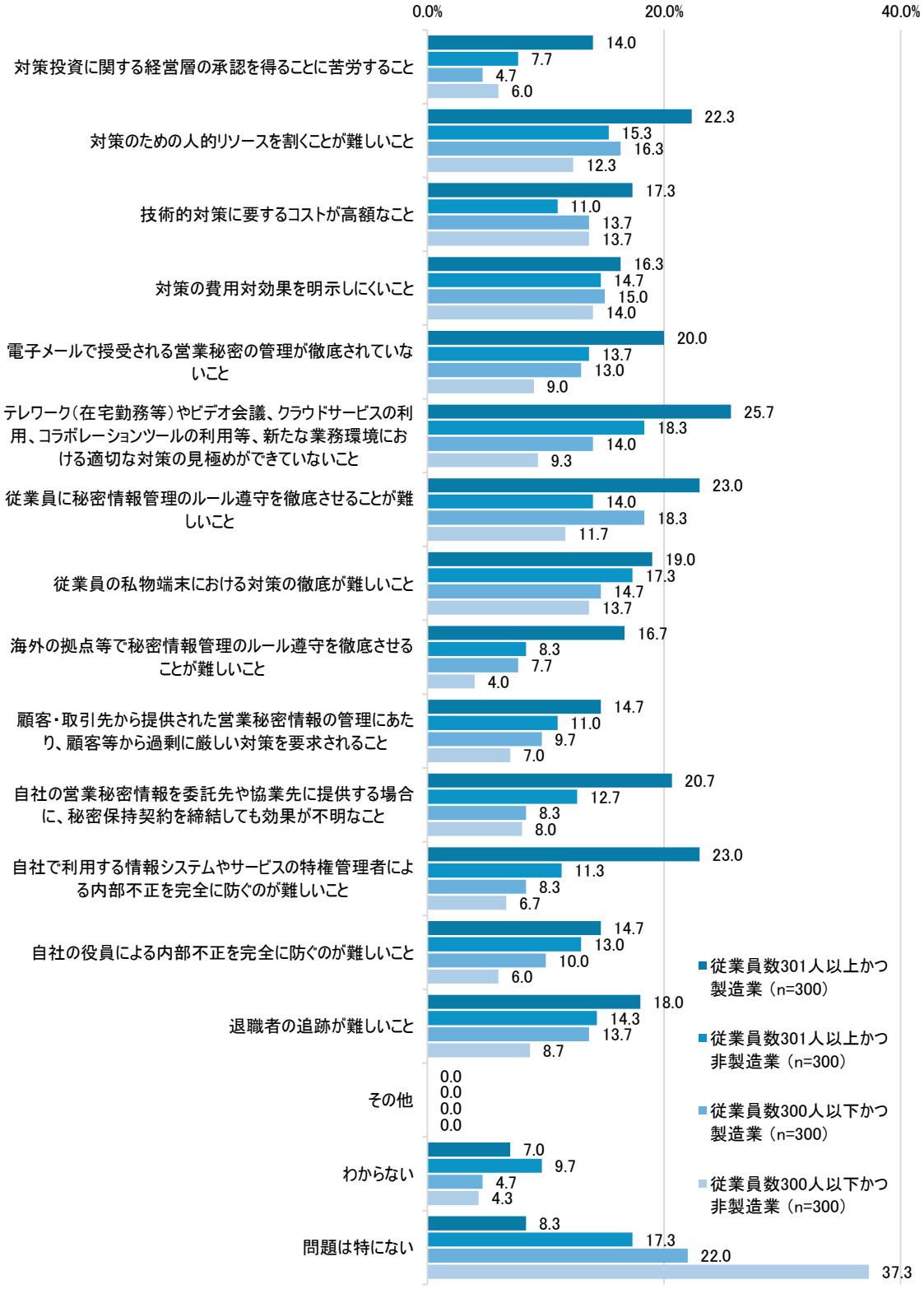


図 36 Q14 営業秘密管理を実践する上での問題（MA、従業員数・業種別）

従業員数・業種別に集計すると、従業員が 301 人以上かつ製造業の区分では、営業秘密管理を実践する上での問題の項目によっては割合が 20%を超えていたが、他の区分ではいずれの項目についても割合が 20%に満たなかった。

従業員が 301 人以上かつ製造業の区分で最も割合が大きかったのは、「テレワーク（在宅勤務等）やビデオ会議、クラウドサービスの利用、コラボレーションツールの利用等新たな業務環境における適切な対策の見極めができていないこと」で 25.7%であった。次いで、「従業員に秘密情報管理のルール遵守を徹底させることが難しいこと」と「自社で利用する情報システムやサービスの特権管理者による内部不正を完全に防ぐのが難しいこと」が高く、どちらも 23.0%であった。また、「対策のための人的リソースを割くことが難しいこと」は 22.3%、「自社の営業秘密情報を委託先や協業先に提供する場合に、秘密保持契約を締結しても効果が不明なこと」は 20.7%、「電子メールで授受される営業秘密の管理が徹底されていないこと」は 20.0%であった。

従業員数 300 人以下かつ非製造業別では、「問題は特にない」とする割合が 37.7%であった。営業秘密管理を実践する上での問題の項目については、他の従業員数・業種の区分に比べると、いずれも割合が小さかった。その中でも割合が大きかったのは、「対策の費用対効果を明示しにくいこと」で 14.0%、「技術的対策に要するコストが高額なこと」及び「従業員の私物端末における対策の徹底が難しいこと」で 13.7%、「対策のための人的リソースを割くことが難しいこと」で 12.3%、「従業員に秘密情報管理のルールの遵守を徹底させることが難しいこと」で 11.7%であった。

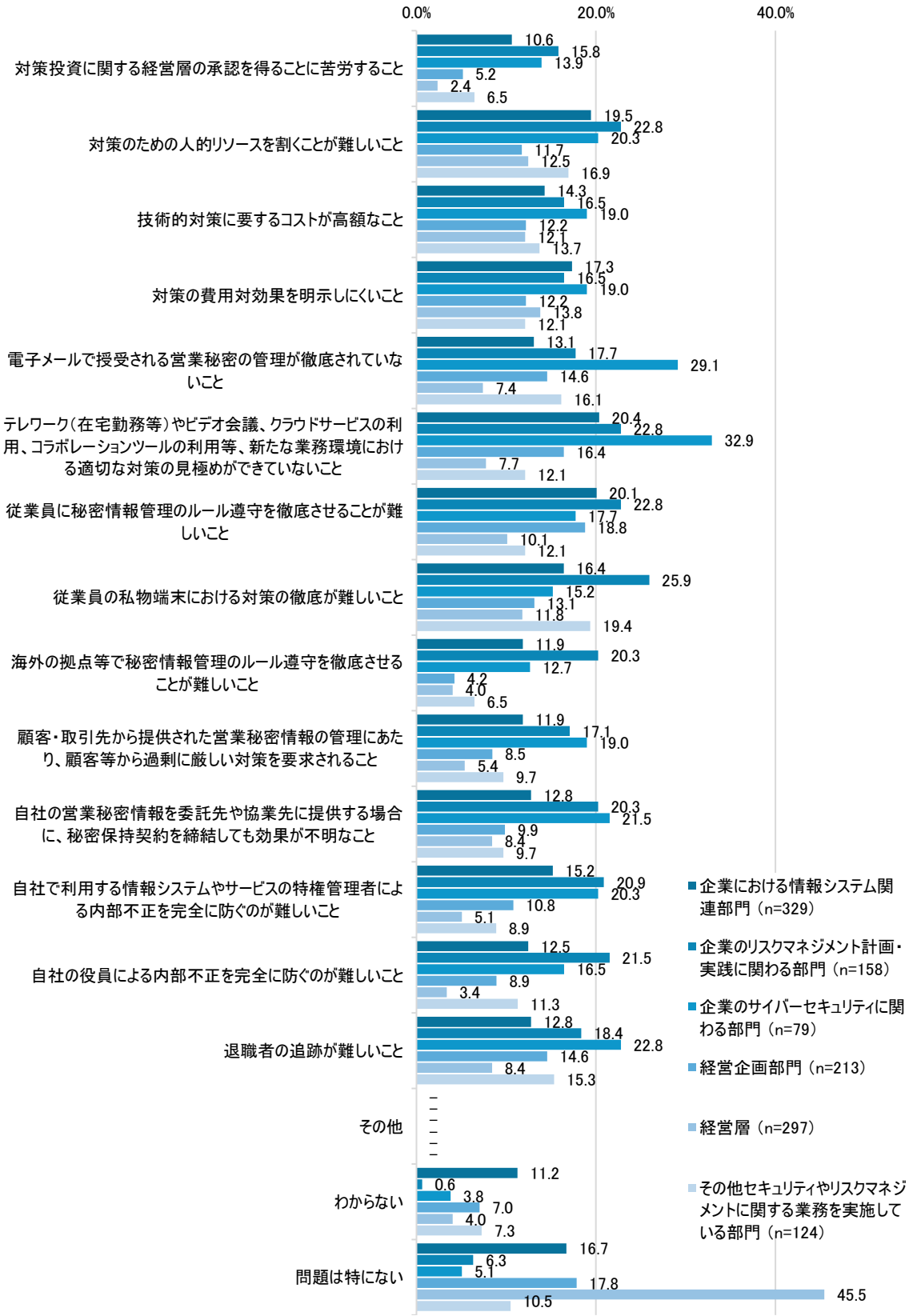


図 37 Q14 営業秘密管理を実践する上での問題（MA、所属部門別）

所属部門別に集計すると、企業におけるサイバーセキュリティに関わる部門では、「電子メールで授受される営業秘密の管理が徹底されていないこと」が 29.1%、「テレワーク（在宅勤務等）やビデオ会議、クラウドサービスの利用、コラボレーションツールの利用等新たな業務環境における適切な対策の見極めができていないこと」が 32.9%と、電子メールの送信に関する問題とテレワーク等の新たな業務環境での対策の問題が意識されている傾向が観測された。

また、経営層については、45.5%が「問題は特にない」を選択していた。営業秘密管理を実践する上での問題の項目について、割合が 10%を超えているもの別では、「対策の費用対効果を明示しにくいこと」で 13.8%、「技術的対策に要するコストが高額なこと」で 12.1%、「対策のための人的リソースを割くことが難しいこと」で 12.5%、「従業員の私物端末における対策の徹底が難しいこと」で 11.8%であり、対策の費用対効果を明示しにくいこと、人材、費用の両面のリソース不足も一因と考えられる私物端末の利用が問題視されている傾向が見られた。

Q15 あなたが所属する組織では、営業秘密のほか、限定提供データに相当する情報を保有しており、ビジネスで活用していますか。(SA)

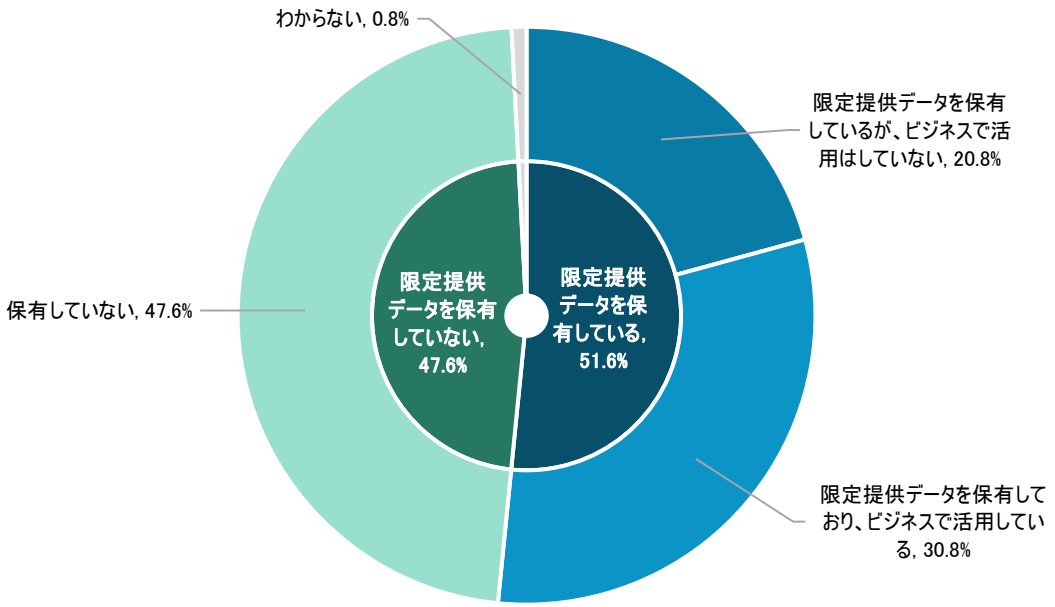


図 38 Q15 限定提供データの保有と活用(n=1200)

限定提供データの保有と活用について、「限定提供データを保有しているが、ビジネスで活用はしていない」は 20.8%、「限定提供データを保有しており、ビジネスで活用している」は 30.8%、「保有していない」は 47.6%であった。

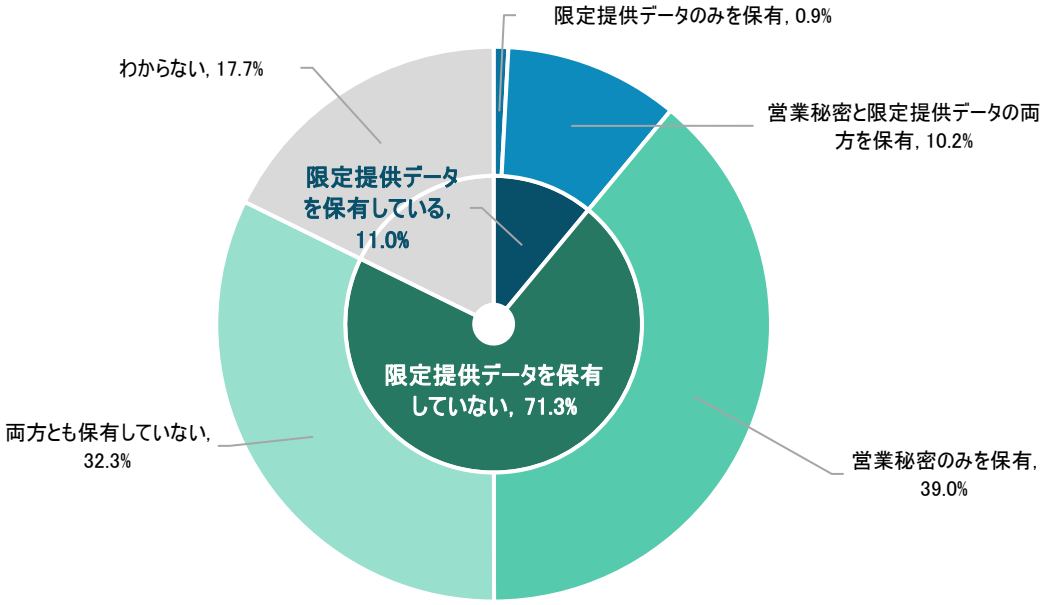


図 39 Q15 参考 限定提供データの保有(2020 年度調査、n=2115)

2020 年度調査と比較すると、限定提供データを保有している割合は 11.1%から 51.6%に、大幅に増加した。そのうち、「限定提供データを保有しており、ビジネスで活用している」とする割合は 30.8%であった。他方、限定提供データを保有していない割合は、71.3%から 47.6%に減少した。また、「わからない」とする割合は、17.7%から 0.8%まで減少した。

表 8 Q15 限定提供データの保有と活用(業種、従業員数、売上高、所属部門別)

(%)

		限定提供データを保有しているが、ビジネスで活用はしていない	限定提供データを保有しており、ビジネスで活用している	保有していない	わからない
合計		20.8	30.8	47.6	0.8
業種	製造業	21.7	34.3	42.7	1.3
	非製造業	19.8	27.3	52.5	0.3
従業員数	301 人以上	24.5	40.0	33.8	1.7
	300 人以下	17.0	21.7	61.3	−
従業員数・業種	従業員数 301 人以上かつ製造業	26.0	42.0	29.3	2.7
	従業員数 300 人以下かつ製造業	17.3	26.7	56.0	−
	従業員数 301 人以上かつ非製造業	23.0	38.0	38.3	0.7
	従業員数 300 人以下かつ非製造業	16.7	16.7	66.7	−
売上高	10 億円以下	14.4	14.7	70.7	0.3
	10 億円超～100 億円以下	21.9	31.2	46.5	0.4
	100 億円超～1,000 億円以下	22.3	42.1	35.5	−
	1,000 億円超～5,000 億円以下	27.4	45.3	26.4	0.9
	5,000 億円超	26.7	40.1	29.1	4.1
所属部門	企業における情報システム関連部門	24.9	28.9	45.3	0.9
	企業のリスクマネジメント計画・実践に関わる部門	25.9	47.5	25.9	0.6
	企業のサイバーセキュリティに関わる部門	30.4	55.7	13.9	−
	経営企画部門	22.1	32.9	43.2	1.9
	経営層	9.4	12.5	78.1	−
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	21.8	39.5	37.1	1.6

業種、従業員数、売上高、所属部門別に集計したところ、従業員数別では、301 人以上では、「限定提供データを保有しており、ビジネスで活用している」の割合が 40.0%、「限定提供データを保有しており、ビジネスで活用していない」の割合が 24.5%と、限定提供データを保有している割合は 60%以上となった。反対に、300 人以下では、「保有していない」の割合が 61.3%であった。

業種別では、従業員数別に比べると、顕著な差はなかった。

所属部門別では、「限定提供データを保有しており、ビジネスで活用している」割合は「企業のリスクマネジメント計画・実践に関わる部門」で 47.5%、「企業のサイバーセキュリティに関わる部門」で 55.7%であった。また、「限定提供データを保有しているが、ビジネスで活用していない」割合は、「企業のリスクマネジメント計画・実践に関わる部門」で 25.9%、「企業のサイバーセキュリティに関わる部門」で 30.4%であった。

表 9 Q15 限定提供データの保有と活用(業種別(大分類) 割合)

(%)

	限定提供データを保有している			保有していない	わからない
	合計	ビジネスでの活用なし	ビジネスでの活用あり		
製造業	56.0	21.7	34.3	42.7	1.3
情報通信業	49.1	26.3	22.8	50.9	0.0
サービス業(他に分類されないもの)	43.2	22.7	20.5	55.7	1.1
小売業	39.6	15.1	24.5	60.4	0.0
専門・技術サービス業	24.5	6.1	18.4	75.5	0.0
建設業	31.4	2.9	28.6	68.6	0.0
金融業、保険業	60.0	17.1	42.9	37.1	2.9
不動産業、物品賃貸業	38.2	11.8	26.5	61.8	0.0
卸売業	60.6	27.3	33.3	39.4	0.0
医療、福祉	54.8	25.8	29.0	45.2	0.0
運輸業	53.6	14.3	39.3	46.4	0.0
教育、学習支援業	58.3	25.0	33.3	41.7	0.0
生活関連サービス業、娯楽業	47.8	21.7	26.1	52.2	0.0
その他	66.7	33.3	33.3	33.3	0.0
飲食サービス業	45.5	18.2	27.3	54.5	0.0
農林業	50.0	30.0	20.0	50.0	0.0
電気・ガス・熱供給・水道業	88.9	22.2	66.7	11.1	0.0
鉱業、採石業、砂利採取業	60.0	20.0	40.0	40.0	0.0
漁業	100.0	100.0	0.0	0.0	0.0
宿泊業	100.0	0.0	100.0	0.0	0.0

業種別(大分類)別に集計したところ、製造業において、限定提供データを保有している割合は56.0%で、保有していない割合は 42.7%であった。また限定提供データを保有している場合、ビジネスでの活用ありの割合は 34.3%、ビジネスでの活用なしの割合は 21.7%であった。

表 10 Q15 限定提供データの保有と活用(製造業(中分類)別)

(%)

	限定提供データを保有している			保有していない	わからない
	合計	ビジネスでの活用なし	ビジネスでの活用あり		
鉄鋼	67.6	20.6	47.1	32.4	0.0
化学	66.7	27.0	39.7	31.7	1.6
非鉄金属	64.7	41.2	23.5	35.3	0.0
電機・情報通信機械・電子部品	60.4	21.6	38.8	35.1	4.5
繊維工業	60.0	13.3	46.7	40.0	0.0
食料品	58.6	24.1	34.5	39.7	1.7
輸送用機械	56.4	27.3	29.1	43.6	0.0
プラスチック製品	56.0	12.0	44.0	44.0	0.0
パルプ・紙・紙加工品	52.2	17.4	34.8	47.8	0.0
その他	50.0	10.9	39.1	50.0	0.0
汎用、生産・業務用機械	48.1	27.8	20.4	51.9	0.0
家具・装備品	46.2	7.7	38.5	53.8	0.0
窯業・土石製品	46.2	30.8	15.4	53.8	0.0
ゴム製品	37.5	12.5	25.0	62.5	0.0
金属製品	35.7	14.3	21.4	64.3	0.0

製造業(中分類)で集計したところ、限定提供データを保有している割合は、鉄鋼が最も高く67.6%、次いで化学が 66.7%、3 位が非鉄金属の 64.7%であった。その中でも、ビジネスで活用している割合が最も高かったのは鉄鋼で、47.1%であった。回答者数が 134 人と製造業の中では最も高かった電機・情報通信機械・電子部品では、限定データを保有しているという回答者が 60%程度を占め、そのうちビジネスでの活用があると回答した割合は 38.8%であった。

Q33 秘密情報の漏えい時におけるあなたが所属する組織の組織体制について、選択してください。(SA)

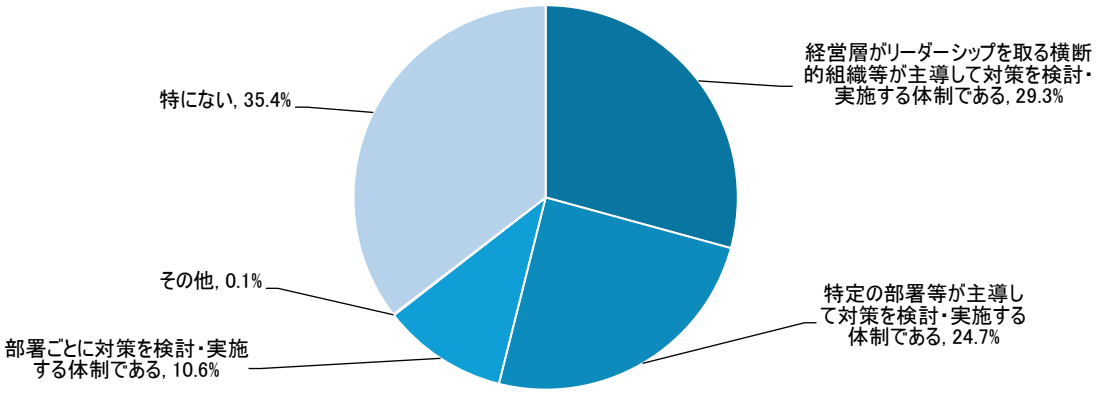


図 40 Q33 秘密情報の漏えい時の組織体制(n=1200)

秘密情報の漏えい時の組織体制について、「特にない」と回答したのは 35.4%で、最も高かった。次いで、「経営層がリーダーシップを取る横断的組織等が主導して対策を検討・実施する体制」が 29.3%、「特定の部署等が主導して対策を検討・実施する体制である」が 24.7%であり、漏えい時に対策の検討と実施を主導する部署を定めているのは 54.0%であった。

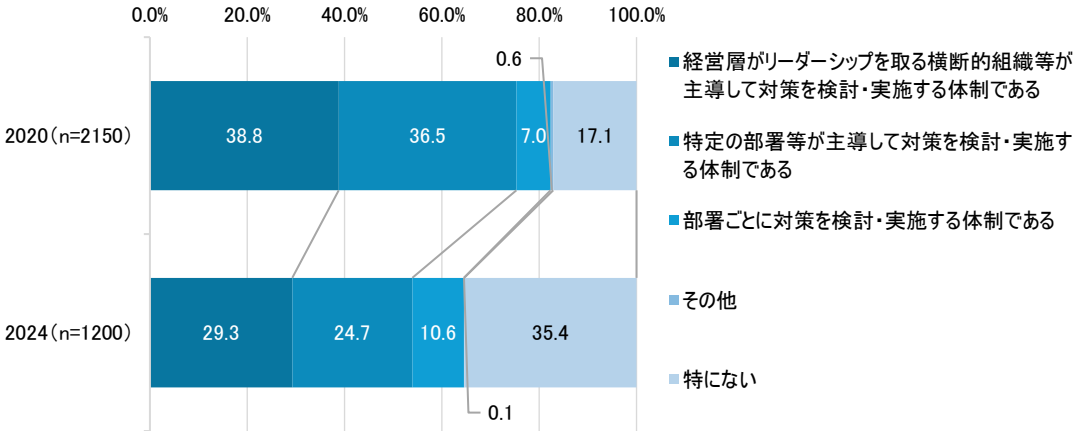


図 41 Q33 秘密情報の漏えい時の組織体制(経年比較)

2020 年度調査と比較すると、「経営層がリーダーシップを取る横断的組織等が主導して対策を検討・実施する体制」の割合が 38.8%から 29.3%に減少していた。また、「特定の部署等が主導して対策を検討・実施する体制である」の割合も、36.5%から 24.7%に減少していた。一方で、「部署ごとに対策を検討・実施する体制である」は 7.0%から 10.6%に微増していた。「特にない」の割合は、17.1%から 35.4%に大きく増加していた。

表 11 Q33 秘密情報の漏えい時の組織体制(業種、従業員数、売上高、所属部門別)

(%)

		経営層がリーダーシップを取る横断的組織等が主導して対策を検討・実施する体制である	特定の部署等が主導して対策を検討・実施する体制である	部署ごとに対策を検討・実施する体制である	その他	特にない
合計		29.3	24.7	10.6	0.1	35.4
業種	製造業	32.2	27.7	11.2	−	29.0
	非製造業	26.3	21.7	10.0	0.2	41.8
従業員数	301 人以上	32.3	32.8	10.8	−	24.0
	300 人以下	26.2	16.5	10.3	0.2	46.8
従業員数・業種	従業員数 301 人以上かつ製造業	37.3	33.0	9.7	−	20.0
	従業員数 300 人以下かつ製造業	27.0	22.3	12.7	−	38.0
	従業員数 301 人以上かつ非製造業	27.3	32.7	12.0	−	28.0
	従業員数 300 人以下かつ非製造業	25.3	10.7	8.0	0.3	55.7
売上高	10 億円以下	26.2	8.5	8.0	0.3	57.1
	10 億円超～100 億円以下	28.1	28.5	14.6	−	28.8
	100 億円超～1,000 億円以下	24.9	36.6	13.9	−	24.5
	1,000 億円超～5,000 億円以下	40.6	31.1	10.4	−	17.9
	5,000 億円超	37.8	32.6	5.2	−	24.4
所属部門	企業における情報システム関連部門	29.8	26.7	10.3	−	33.1
	企業のリスクマネジメント計画・実践に関わる部門	37.3	33.5	12.0	−	17.1
	企業のサイバーセキュリティに関わる部門	26.6	50.6	10.1	−	12.7
	経営企画部門	26.3	26.8	13.6	−	33.3
	経営層	30.0	6.7	5.4	0.3	57.6
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	22.6	30.6	16.9	−	29.8

業種、従業員数、売上高、所属部門別に集計したところ、秘密情報の漏えい時の組織体制が「特にない」とする割合は、所属部門別では経営層の場合に最も高く、57.6%であった。従業員数・業種別では、従業員数 300 人以下かつ非製造業の場合 55.7%であった。また、売上高別では、10 億円以下の場合に 57.1%であった。所属部門別では、経営層の場合 57.6%であった。

「経営層がリーダーシップをとる横断的組織等が主導して対策を検討・実施する体制である」とする割合は、売上高別では 1000 億円以上～5000 億円以下の場合 40.6%、5000 億円超の場合 37.8%と、他の区分に比べて高かった。また所属部門別では、企業のリスクマネジメント計画・実証に関わる部門で 37.3%、その他セキュリティやリスクマネジメントに関する業務を実施している部門では 22.6%であった。

「特定の部署等が主導して対策を検討・実施する体制である」とする割合は、所属部門別では、企業のサイバーセキュリティに関わる部門で最も高く 50.6%、経営層で最も低く 6.7%であった。また、売上高別では、100 億円以上の区分で 30%以上と比較的高く、10 億円以下の区分では 8.5%であった。従業員数・業種別では、従業員数 301 人以上の製造業及び非製造業の場合、30%以上で比較的高く、従業員数 300 人以下かつ非製造業の場合は 10.7%で最も低かった。

「部署ごとに対策を検討・実施する体制である」とする割合は、売上高別では 5000 億円超の場合 5.2%と低かった。

Q34 秘密情報の漏えい時に対応を主導する部署・担当はどこですか。(SA)

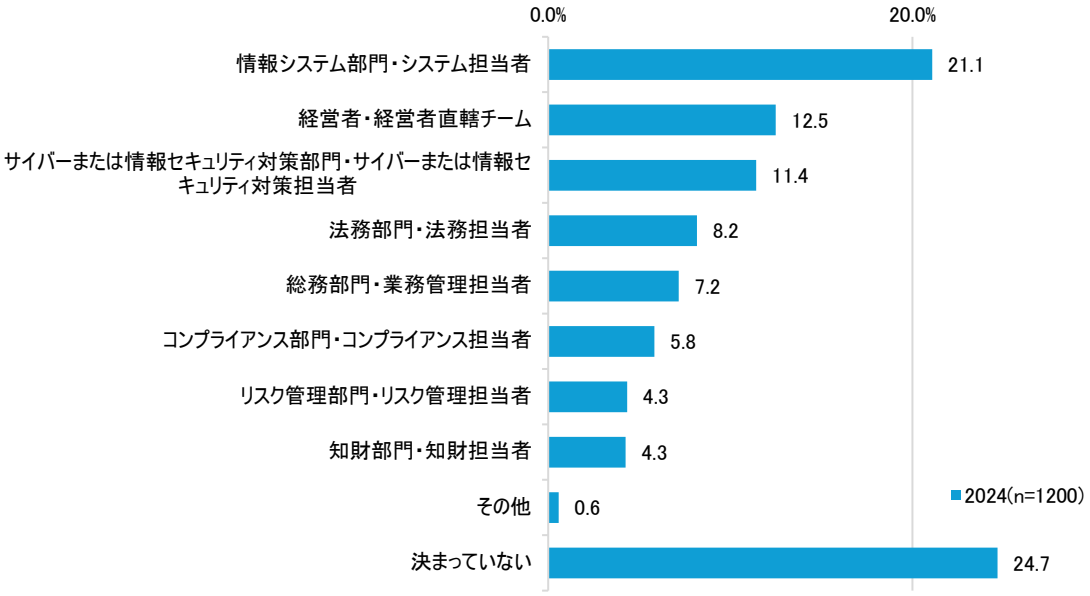


図 42 Q34 秘密情報の漏えい時に対応を主導する部署・担当(n=1200)

秘密情報の漏えい時に対応を主導する部署・担当について、最も割合の高かったのは「情報システム部門・システム担当者」で 21.1%であった。次いで、「経営者・経営者直轄チーム」が高く 12.5%であった。「決まっていない」を選択した割合も高く 24.7%であった。

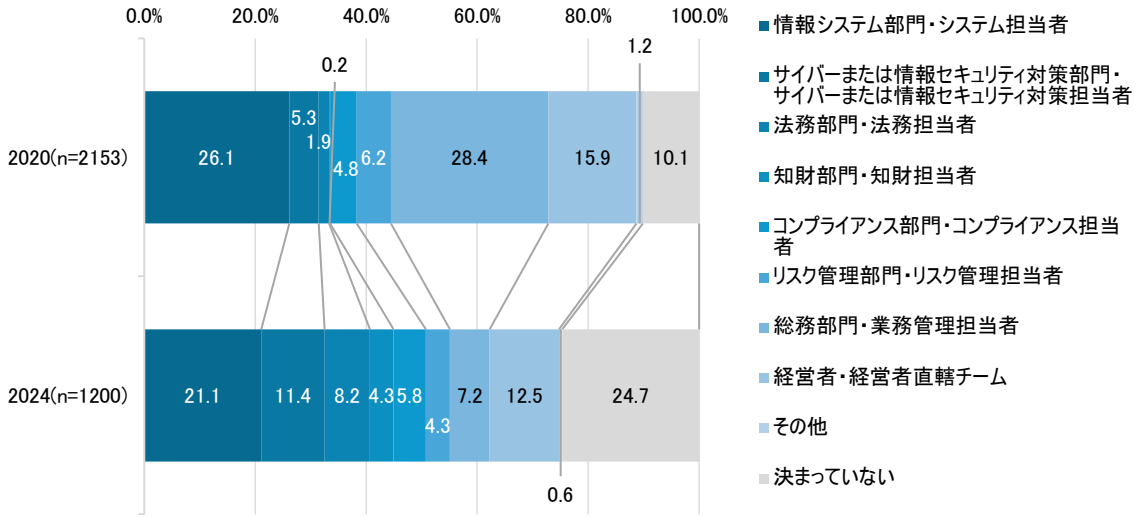


図 43 Q34 秘密情報の漏えい時に対応を主導する部署・担当(経年比較)

2020 年度調査と比較すると、「情報システム部門・システム担当者」26.1%から 21.1%に、「総務部門・業務管理担当者」は 28.4%から 7.2%に減少し、その他の部門の割合が増加している傾向にあった。また、「決まっていない」とする割合は 10.1%から 24.7%に増加した。

表 12 Q34 秘密情報の漏えい時に対応を主導する部署・担当
(業種、従業員数、売上高、所属部門別)

(%)

		情報システム部門・システム担当者	サイバーまたは情報セキュリティ対策部門・サイバーまたは情報セキュリティ対策担当者	法務部門・法務担当者	知財部門・知財担当者	コンプライアンス部門・コンプライアンス担当者	リスク管理部門・リスク管理担当者	総務部門・業務管理担当者	経営者・経営者直轄チーム	その他	決まっていない
合計		21.1	11.4	8.2	4.3	5.8	4.3	7.2	12.5	0.6	24.7
業種	製造業	25.5	12.0	8.2	5.7	6.8	4.8	7.8	9.5	0.3	19.3
	非製造業	16.7	10.8	8.2	2.8	4.8	3.8	6.5	15.5	0.8	30.0
従業員数	301 人以上	29.8	17.0	10.3	3.5	9.0	5.7	5.0	2.7	0.7	16.3
	300 人以下	12.3	5.8	6.0	5.0	2.7	3.0	9.3	22.3	0.5	33.0
従業員数・業種	従業員数 301 人以上かつ製造業	36.7	16.0	10.0	3.7	9.7	6.0	4.3	1.3	0.3	12.0
	従業員数 300 人以下かつ製造業	14.3	8.0	6.3	7.7	4.0	3.7	11.3	17.7	0.3	26.7
	従業員数 301 人以上かつ非製造業	23.0	18.0	10.7	3.3	8.3	5.3	5.7	4.0	1.0	20.7
	従業員数 300 人以下かつ非製造業	10.3	3.7	5.7	2.3	1.3	2.3	7.3	27.0	0.7	39.3
売上高	10 億円以下	9.8	2.1	4.1	2.3	2.1	1.5	5.4	30.1	1.0	41.6
	10 億円超～100 億円以下	20.4	13.5	8.5	5.4	5.8	5.4	13.5	6.5	−	21.2
	100 億円超～1,000 億円以下	26.4	15.8	11.7	7.0	8.8	6.6	7.0	3.7	0.4	12.8
	1,000 億円超～5,000 億円以下	34.0	17.9	11.3	3.8	8.5	10.4	0.9	2.8	0.9	9.4
	5,000 億円超	31.4	18.6	9.3	2.9	8.1	1.7	5.8	1.7	0.6	19.8
所属部門	企業における情報システム関連部門	37.1	16.1	6.4	0.9	5.5	4.0	3.3	2.1	0.3	24.3
	企業のリスクマネジメント計画・実践に関わる部門	15.8	21.5	16.5	9.5	6.3	7.0	10.1	1.9	−	11.4
	企業のサイバーセキュリティに関わる部門	20.3	20.3	8.9	15.2	13.9	7.6	2.5	5.1	−	6.3
	経営企画部門	20.7	7.0	12.7	4.2	7.0	6.6	12.2	9.4	0.5	19.7
	経営層	7.1	2.7	2.0	1.0	1.7	1.3	5.1	36.4	0.3	42.4
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	20.2	8.9	8.9	7.3	8.9	3.2	12.9	6.5	3.2	20.2

業種、従業員数、売上高、所属部門別に集計すると、従業員数・業種別では、従業員数 301 人以上かつ製造業の場合、「情報システム部門、システム担当者」の割合が全体に比較して 10 ポイント以上高く36.7%で、「経営者・経営者直轄チーム」は全体に比較して10ポイント以上少なく1.3%であった。それに対して、従業員数300 人以下の製造業及び非製造業では、「情報システム部門、システム担当者」の割合は全体に比較して 5 ポイント以上少なく、「経営者・経営者直轄チーム」の割合は全体に比較して 5 ポイント以上高かった。

所属部門別では、経営層の場合「決まっていない」とする割合が全体に比べて 10 ポイント以上高く 42.4%であった。企業における情報システム関連部門の場合は「情報システム部門・システム担当者」が全体に比べて 10 ポイント以上高く 37.1%であった。企業のリスクマネジメント計画・実践に関わる部門の場合は「サイバーまたは情報セキュリティ対策部門・サイバーまたは情報セキュリティ対策担当者」が全体に比べて 10 ポイント以上高く 21.5%、「法務部門・法務担当者」は全体に比

べて 5 ポイント以上高く 16.5%、「知財部門・知財担当者」は全体に比べて 5 ポイント以上高く 9.5%であった。企業のサイバーセキュリティに関わる部門では、「サイバーまたは情報セキュリティ対策部門・サイバーまたは情報セキュリティ対策担当者」が全体に比べて 5 ポイント以上高く 20.3%、「知財部門・知財担当者」が全体に比べて 10 ポイント以上高く 15.2%、「コンプライアンス部門・コンプライアンス担当者」が全体に比べて 5 ポイント以上高く 13.9%であった。経営企画部門の場合、「総務部門・業務管理担当者」が全体に比べて 5 ポイント以上高く 12.2%であった。その他セキュリティやリスクマネジメントに関する業務を実施している部門の場合、経営企画部門と同様、「総務部門・業務管理担当者」が全体に比べて 5 ポイント以上高く 12.9%であった。

2.1.3　営業秘密管理において実施している対策

Q16 あなたが所属する組織において、サーバーのアクセスログの確認やメールのモニタリング等、営業秘密の漏えいに気付くことができるような技術的対策は実施されていますか。(SA)

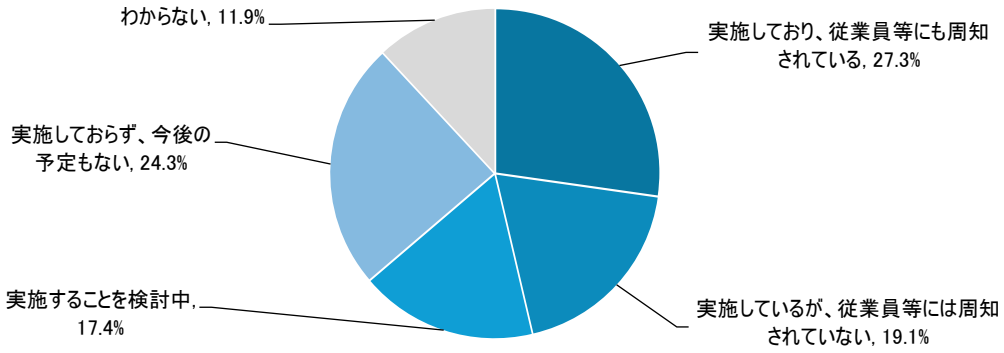


図 44 Q16 営業秘密の漏えいに気付くための技術的対策の実施 (n=1200)

営業秘密の漏えいに気付くための技術的対策の実施について、「実施しており、従業員等にも周知されている」が 27.3%、「実施しているが、従業員等には周知されていない」が 19.1%、「実施することを検討中」が 17.4%、「実施しておらず、今後の予定もない」が 24.3%、「わからない」が 11.%であった。

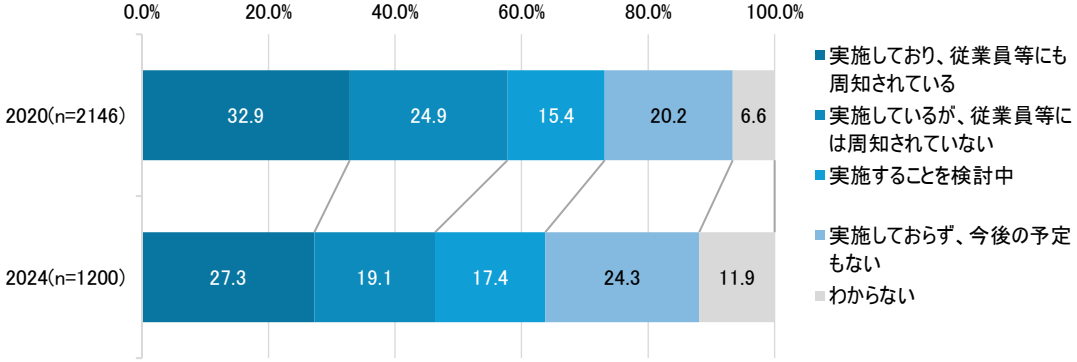


図 45 Q16 営業秘密の漏えいに気付くための技術的対策の実施(経年比較)

2020 年度調査と比較すると、営業秘密の漏えいに気付くための技術的対策を実施しているとする「実施しており、従業員等にも周知されている」及び「実施しているが、従業員等には周知していない」の割合について、前者は 32.9%から 27.3%に、後者は 24.9%から 19.1%に減少した。「実施することを検討中」とする割合は 15.4%から 17.4%に微増した。「実施しておらず、今後の予定もない」とする割合は 20.2%から 24.3%に増加し、「わからない」とする割合は 6.6%から 11.9%に増加した。

表 13 Q16 営業秘密の漏えいに気付くための技術的対策の実施
(業種、従業員数、売上高、所属部門別)

(%)

		実施しており、従業員等にも周知されている	実施しているが、従業員等には周知されていない	実施することを検討中	実施しておらず、今後の予定もない	わからない
合計		27.3	19.1	17.4	24.3	11.9
業種	製造業	29.3	22.7	19.2	19.3	9.5
	非製造業	25.2	15.5	15.7	29.3	14.3
従業員数	301 人以上	36.8	22.0	16.8	9.0	15.3
	300 人以下	17.7	16.2	18.0	39.7	8.5
従業員数・業種	従業員数 301 人以上かつ製造業	41.0	23.0	18.0	7.0	11.0
	従業員数 300 人以下かつ製造業	17.7	22.3	20.3	31.7	8.0
	従業員数 301 人以上かつ非製造業	32.7	21.0	15.7	11.0	19.7
	従業員数 300 人以下かつ非製造業	17.7	10.0	15.7	47.7	9.0
売上高	10 億円以下	12.9	8.5	16.7	52.7	9.3
	10 億円超～100 億円以下	27.3	26.9	17.7	16.5	11.5
	100 億円超～1,000 億円以下	34.1	24.2	20.1	9.5	12.1
	1,000 億円超～5,000 億円以下	38.7	23.6	22.6	4.7	10.4
	5,000 億円超	41.9	20.3	11.0	7.6	19.2
所属部門	企業における情報システム関連部門	38.0	16.4	12.5	14.9	18.2
	企業のリスクマネジメント計画・実践に関わる部門	31.0	36.7	17.1	10.8	4.4
	企業のサイバーセキュリティに関わる部門	29.1	41.8	15.2	6.3	7.6
	経営企画部門	26.3	16.0	23.9	21.1	12.7
	経営層	15.5	7.1	14.5	53.5	9.4
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	22.6	23.4	28.2	13.7	12.1

業種、従業員数、売上高、所属部門別に集計したところ、「実施しており、従業員等にも周知されている」の割合が合計の割合＋10 ポイント以上となったのは、従業員数 301 人以上かつ製造業の場合で 41.0%、売上高 1000 億円超～5000 億円以下の場合で 38.7%、5000 億円超の場合で 41.9%、所属部門別では企業における情報システム関連部門が 38.0%であった。また、合計の割合－10 ポイント以上となったのは、売上高 10 億円以下の場合で 12.9%、所属部門別では経営層の場合 15.5%であった。

「実施しているが、従業員等には周知されていない」の割合が合計の割合＋10 ポイント以上となったのは、所属部門別で企業のリスクマネジメント計画・実践に関わる部門の場合 36.7%、企業のサイバーセキュリティに関わる部門の場合 41.8%であった。また、合計の割合－10 ポイント以上となったのは、売上高 10 億円以下の場合で 8.5%、所属部門別では経営層の場合 7.1%であった。従業員数・業種別では目立つ傾向は無かった。

「実施することを検討中」の割合が合計の割合＋10 ポイント以上となったのは、所属部門別でその他セキュリティやリスクマネジメントに関する業務を実施している部門の場合で 28.2%であった。従業員数・業種別、売上高別では目立つ傾向は無かった。

「実施しておらず、今後の予定もない」の割合については、上述の「実施しており、従業員等にも周知されている」、「実施しているが、従業員等には周知されていない」、「実施することを検討中」とは逆の傾向を示しており、従業員数 301 人以下の場合 39.7%、従業員数 300 人以下かつ非製造業の場合 47.7%、売上高 10 億円以下の場合 52.7%、所属部門別では経営層の場合 53.5%と、合計の割合＋10 ポイント以上となった。

「わからない」については、目立つ傾向は無かった。

Q17 技術的対策を実施している、あるいは実施することを検討している場合、具体的な内容をご回答ください。(MA)

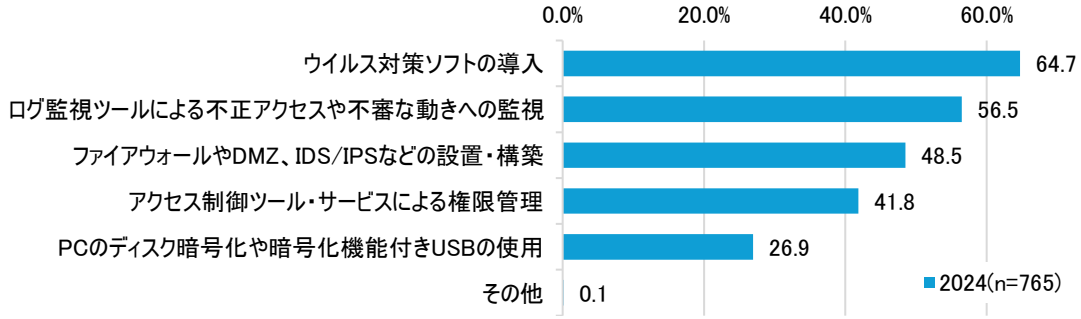


図 46 Q17 実施しているあるいは実施することを検討している技術的対策 (MA、n=765)

Q17 では、Q16 において「実施しており、従業員等にも周知されている」、「実施しているが、従業員等には周知されていない」、「実施することを検討中」を選んだ 765 人に対して、実施しているまたは実施することを検討している対策の内容を質問した。

最も多かったのは「ウイルス対策ソフトの導入」で 64.7%であった。次いで、「ログ監視ツールによる不正アクセスや不審な動きへの監視」が 56.5%、「ファイアウォールや DMZ、IDS/IPS などの設置・構築」が 48.5%であった。

表 14 Q17 実施しているあるいは実施することを検討している技術的対策 (業種、従業員数、売上高、所属部門別)

(%)

		ファイアウォールやDMZ、IDS/IPSなどの設置・構築	ウイルス対策ソフトの導入	ログ監視ツールによる不正アクセスや不審な動きへの監視	アクセス制御ツール・サービスによる権限管理	PC のディスク暗号化や暗号化機能付き USB の使用	その他
合計		48.5	64.7	56.5	41.8	26.9	0.1
業種	製造業	49.4	64.2	57.4	41.0	28.3	0.2
	非製造業	47.3	65.4	55.3	42.9	25.1	−
従業員数	301 人以上	54.2	62.3	64.5	47.8	32.6	−
	300 人以下	40.2	68.2	44.7	33.1	18.6	0.3
従業員数・業種	従業員数 301 人以上かつ製造業	56.1	63.0	64.6	48.8	36.2	−
	従業員数 300 人以下かつ製造業	40.3	65.7	47.5	30.4	17.7	0.6
	従業員数 301 人以上かつ非製造業	51.9	61.5	64.4	46.6	28.4	−
	従業員数 300 人以下かつ非製造業	40.0	71.5	40.8	36.9	20.0	−
売上高	10 億円以下	31.8	69.6	36.5	33.1	21.6	0.7
	10 億円超～100 億円以下	54.0	65.2	54.5	36.9	21.4	−
	100 億円超～1,000 億円以下	44.4	62.1	61.2	43.0	25.2	−
	1,000 億円超～5,000 億円以下	51.1	57.8	62.2	46.7	24.4	−
	5,000 億円超	65.1	67.5	70.6	54.0	46.0	−
所属部門	企業における情報システム関連部門	67.3	71.8	68.2	50.5	37.7	−
	企業のリスクマネジメント計画・実践に関わる部門	39.6	65.7	53.7	35.1	20.1	−
	企業のサイバーセキュリティに関わる部門	35.3	60.3	64.7	39.7	20.6	−
	経営企画部門	39.7	59.6	48.9	39.0	24.8	0.7
	経営層	45.5	69.1	40.0	41.8	25.5	−
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	43.5	52.2	57.6	37.0	20.7	−

業種、従業員数、売上高、所属部門別に集計したところ、「ファイアウォールや DMZ、IDS/IPS などの設置・構築」の割合が合計の割合＋10 ポイント以上となったのは、売上高 5000 億円超の場合で 65.1%、所属部門別では企業における情報システム関連部門が 67.3%であった。また、合計の割合－10 ポイント以上となったのは、売上高 10 億円以下の場合で 31.8%、所属部門別では企業のサイバーセキュリティに関わる部門の場合 35.3%であった。

「ウイルス対策ソフトの導入」の割合が合計の割合＋5 ポイント以上となったのは、所属部門別で企業における情報システム関連部門が 71.8%であった。また、合計の割合－10 ポイント以上となったのは、所属部門別ではその他セキュリティやリスクマネジメントに関する業務を実施している部門の場合で 35.3%であった。

「ログ監視ツールによる不正アクセスや不審な動きへの監視」の割合が合計の割合＋10 ポイント以上となったのは、売上高 5000 億円超の場合で 70.6%、所属部門別では企業における情報システム関連部門が 68.2%であった。また、合計の割合－10 ポイント以上となったのは、従業員数別では 300 人以下の場合で 44.7%、従業員数・業種別では従業員数 300 人以下かつ非製造業の場合で 40.8%、売上高 10 億円以下の場合で 36.5%、所属部門別では経営層の場合 40.0%であった。

「アクセス制御ツール・サービスによる権限管理」の割合が合計の割合＋10 ポイント以上となったのは、売上高 5000 億円超の場合で 54.0%であった。また、合計の割合－10 ポイント以上となったのは、従業員数・業種別では従業員数 300 人以下かつ製造業の場合 30.4%であった。

「PC のディスク暗号化や暗号化機能付き USB の使用」の割合が合計の割合＋10 ポイント以上となったのは、売上高 5000 億円超の場合で 46.0%、所属部門別では企業における情報システム関連部門が 37.7%であった。

Q18 営業秘密情報（紙と電子媒体の両方）への不正なアクセスを防ぐための対策として、実施しているものを選択してください。（MA）

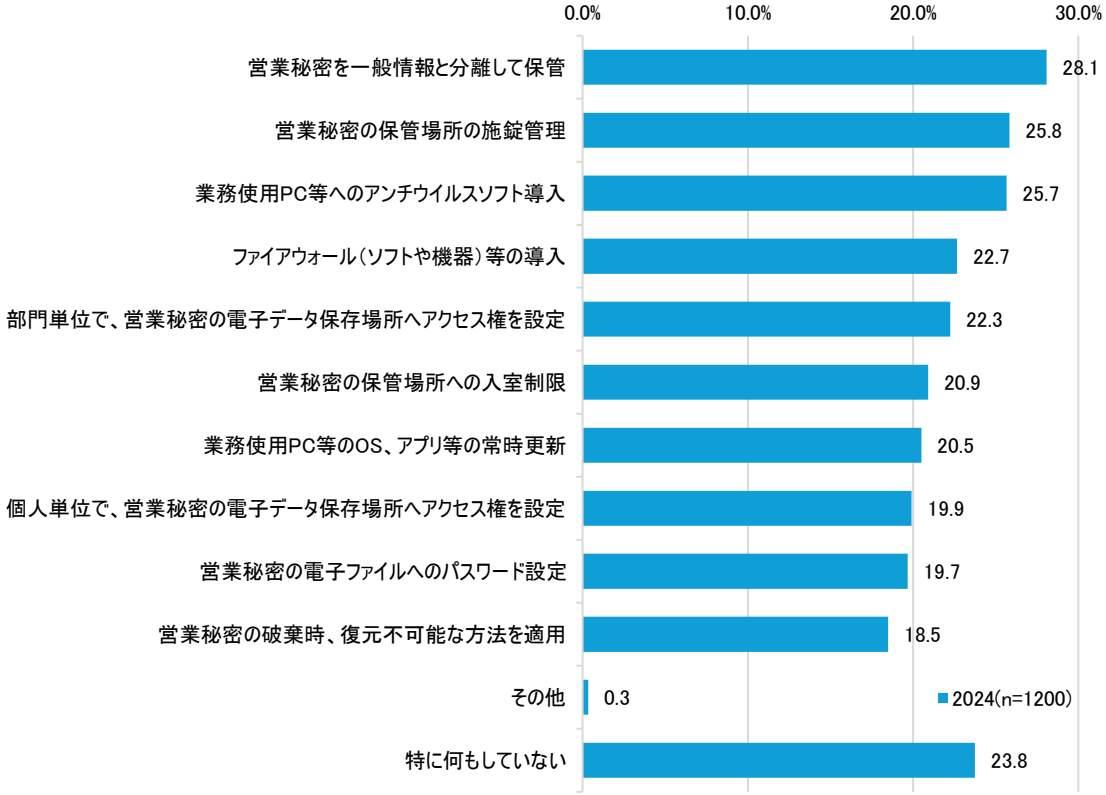


図 47 Q18 営業秘密情報への不正アクセス防止策として実施している対策(MA、n=1200)

営業秘密情報への不正アクセス防止策として実施している対策について、最も割合が高かったのは「営業秘密を一般情報と分離して保管」の 28.1%であった。次いで、「営業秘密の保管場所の施錠管理」が 25.8%、「業務使用 PC 等へのアンチウィルスソフト導入」が 25.7%であった。

全体的には、いずれの対策についても 30%以下であったため、業種等とのクロス集計を行った。

表 15 Q18 営業秘密情報への不正アクセスを防止する対策として実施している対策 (業種、従業員数、売上高、所属部門別)

(%)

		営業秘密を一般情報と分離して保管	営業秘密の保管場所への入室制限	営業秘密の保管場所の施錠管理	営業秘密の破棄時、復元不可能な方法を適用	部門単位で、営業秘密の電子データ保存場所へアクセス権を設定	個人単位で、営業秘密の電子データ保存場所へアクセス権を設定	営業秘密の電子ファイルへのパスワード設定	業務使用 PC 等へのアンチウィルスソフト導入	業務使用 PC 等の OS、アプリ等の常時更新	ファイアウォール（ソフトや機器）等の導入	その他	特に何もしていない
合計		28.1	20.9	25.8	18.5	22.3	19.9	19.7	25.7	20.5	22.7	0.3	23.8
業種	製造業	31.3	23.3	28.2	19.7	25.7	23.3	21.7	29.5	22.5	25.5	0.2	17.8
	非製造業	24.8	18.5	23.5	17.3	18.8	16.5	17.7	21.8	18.5	19.8	0.5	29.7
従業員数	301 人以上	35.7	28.8	36.3	26.3	31.3	26.3	27.0	28.3	24.2	26.3	0.3	13.5
	300 人以下	20.5	13.0	15.3	10.7	13.2	13.5	12.3	23.0	16.8	19.0	0.3	34.0
従業員数・業種	従業員数 301 人以上かつ製造業	40.0	30.3	38.3	28.0	33.7	30.7	32.3	35.0	29.0	31.7	0.3	9.7
	従業員数 300 人以下かつ製造業	22.7	16.3	18.0	11.3	17.7	16.0	11.0	24.0	16.0	19.3	−	26.0
	従業員数 301 人以上かつ非製造業	31.3	27.3	34.3	24.7	29.0	22.0	21.7	21.7	19.3	21.0	0.3	17.3
	従業員数 300 人以下かつ非製造業	18.3	9.7	12.7	10.0	8.7	11.0	13.7	22.0	17.7	18.7	0.7	42.0
売上高	10 億円以下	18.3	9.0	12.1	8.2	9.0	10.0	12.1	23.7	16.7	18.8	0.5	43.4
	10 億円超～100 億円以下	28.1	22.7	27.3	15.8	23.8	20.8	16.5	22.3	16.9	21.2	−	18.8
	100 億円超～1,000 億円以下	28.6	23.4	32.6	23.8	28.2	22.7	26.4	25.3	20.1	21.2	−	13.2
	1,000 億円超～5,000 億円以下	35.8	26.4	36.8	27.4	33.0	29.2	22.6	29.2	29.2	24.5	−	10.4
	5,000 億円超	44.8	37.8	37.2	32.0	33.7	30.8	29.1	33.7	29.7	34.9	1.2	11.6
所属部門	企業における情報システム関連部門	35.3	27.4	30.4	20.4	33.4	25.8	24.6	30.4	27.1	27.7	0.3	21.0
	企業のリスクマネジメント計画・実践に関わる部門	29.7	31.6	41.1	25.3	24.1	30.4	24.7	25.9	19.0	18.4	−	7.0
	企業のサイバーセキュリティに関わる部門	26.6	43.0	34.2	40.5	35.4	27.8	24.1	24.1	21.5	24.1	−	3.8
	経営企画部門	27.7	15.0	24.4	15.5	22.1	15.5	18.8	23.5	16.4	18.8	0.5	22.1
	経営層	18.5	6.7	11.1	7.4	6.1	10.4	9.8	23.6	17.2	21.5	0.7	45.1
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	31.5	20.2	26.6	22.6	21.0	16.1	22.6	22.6	19.4	23.4	−	16.9

業種、従業員数、売上高、所属部門別に集計したところ、従業員数別では、301 人以上の場合、「営業秘密を一般情報と分離して保管」、「営業秘密の保管場所への入室制限」、「営業秘密の保管場所の施錠管理」、「営業秘密の破棄時、復元不可能な方法を適用」、「部門単位で、営業秘密の電子データ保存場所へアクセス権を設定」、「個人単位で、営業秘密の電子データ保存場所へアクセス権を設定」、「営業秘密の電子ファイルへのパスワード設定」の割合が合計に比べて＋5 ポイント以上大きく、反対に、300 人以下の場合＋5 ポイント以上低かった。

従業員数・業種別では、従業員数 301 人以上かつ製造業の場合、いずれの対策についても合計に比べて＋5 ポイント以上実施割合が高かった。

また、売上高別では、100 億円超の場合、金額が大きいほど、合計に比べて＋5 ポイント以上の実施割合である対策の数が高く、実施割合も高かった。

所属部門別では、企業における情報システム関連部門、企業のリスクマネジメント計画・実践に関わる部門及び企業のサイバーセキュリティに関わる部門において、実施割合が合計に比べて＋5 ポイント以上である対策が 5 つあった。反対に、経営層に関しては「特に何もしていない」とする割合が合計に比べて＋10 ポイント以上高く、45.1%であった。

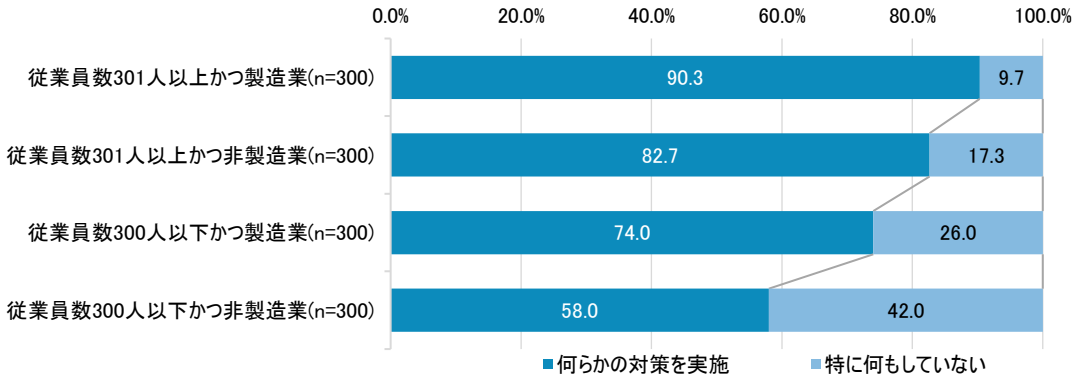


図 48 Q18 何らかの不正アクセス防止対策を実施している割合

回答者が「特に何もしていない」か、またはそれ以外の「営業秘密を一般情報と分離して保管」、「営業秘密の保管場所への入室制限」、「営業秘密の保管場所の施錠管理」、「営業秘密の破棄時、復元不可能な方法を適用」、「部門単位で、営業秘密の電子データ保存場所へアクセス権を設定」、「個人単位で、営業秘密の電子データ保存場所へアクセス権を設定」、「営業秘密の電子ファイルへのパスワード設定」、「業務使用 PC 等へのアンチウィルスソフト導入」、「業務使用 PC 等の OS、アプリ等の常時更新」、「ファイアウォール(ソフトや機器)等の導入」のいずれかを選んでおり何らかの対策を実施しているか、どちらに相当するかに着目し、従業員数と業種別で集計した。

「何らかの対策を実施」している割合について、従業員数 301 人以上かつ製造業の場合最も高く 90.3%、従業員数 301 人以上かつ非製造業の場合 82.7%、従業員数 300 人以下かつ製造業の場合 74.0%、最も割合が低かったのは、従業員数 300 人以下かつ非製造業で 58.0%であった。

Q19 営業秘密情報の社外への不正な持出を防ぐための対策として、実施しているものを選択してください。(MA)

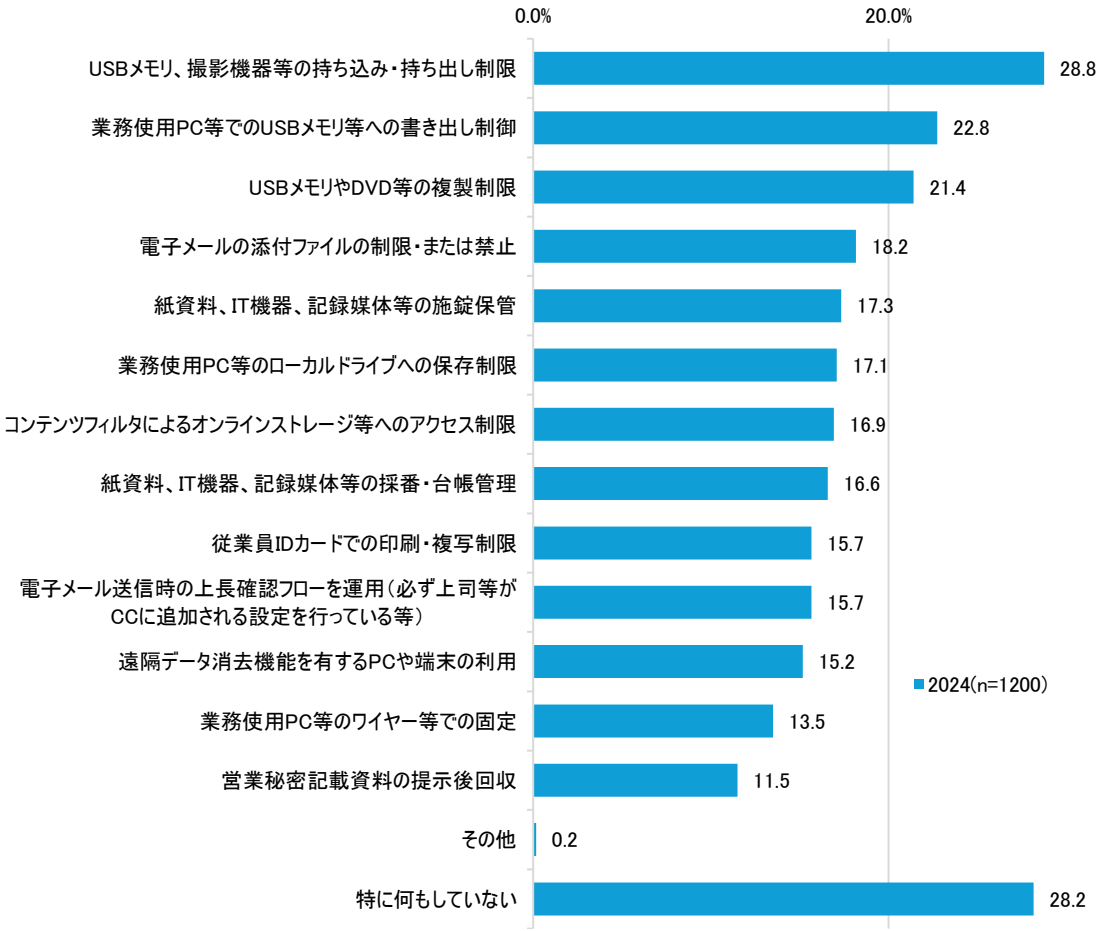


図 49 Q19 営業秘密情報の社外への不正持出防止策として実施している対策(MA、n=1200)

営業秘密情報の社外への不正持出防止策として実施している対策について、全体的に実施割合が 20%前後であったものの、最も実施している割合が高かったのは、「USB メモリ、撮影機器等の持込み・持ち出し制限」で 28.8%であった。次いで、「業務用 PC 等での USB メモリ等への書き出し制御」が 22.8%、「USB メモリや DVD 等の複製制限」が 21.4%と、USB メモリ等の利用に関する対策の実施割合が高かった。

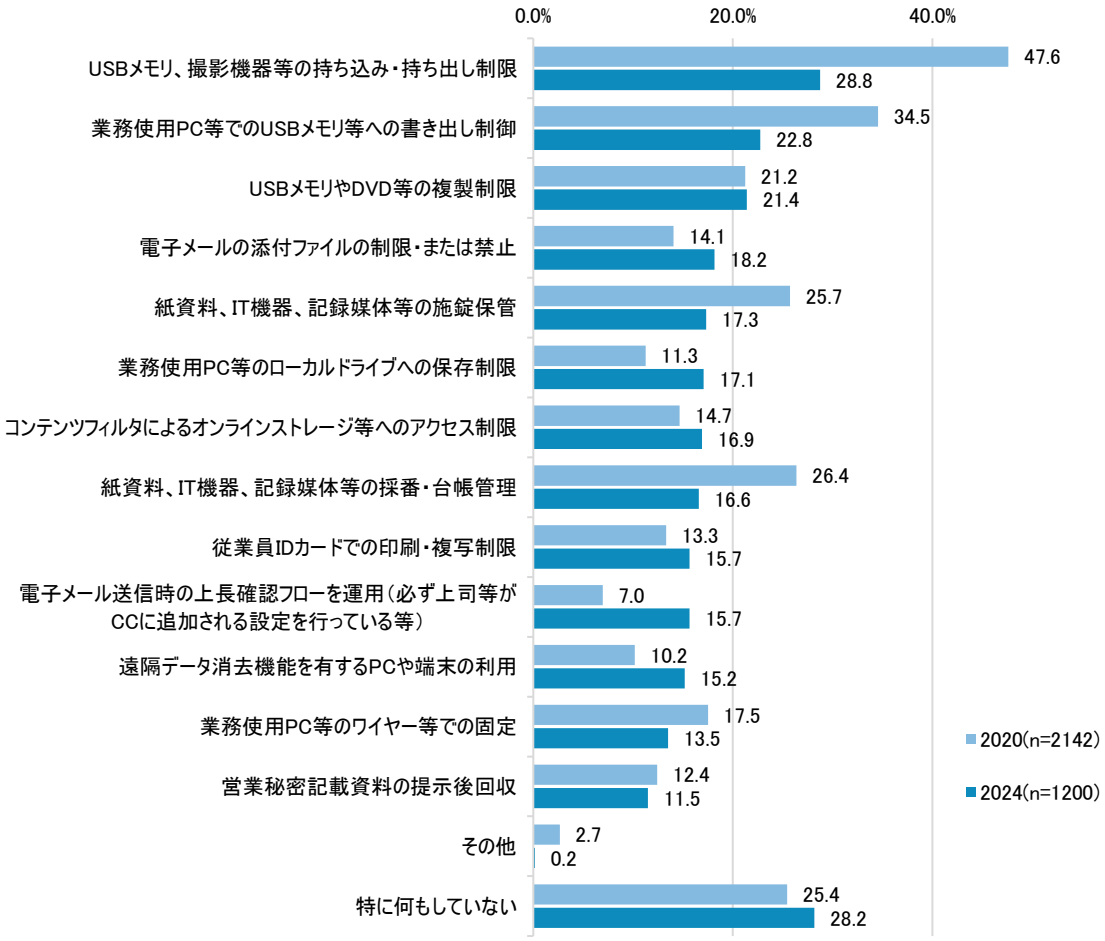


図 50 Q19 営業秘密情報の社外への不正持出防止策として実施している対策(経年比較)

2020 年度調査と比較すると、紙資料、IT 機器、記録媒体等の管理に関する 2 項目で割合が減少しており、「紙資料、IT 機器、記録媒体等の施錠保管」は 25.7%から 17.3%に、「紙資料、IT 機器、記録媒体等の裁判・台帳管理」は 26.4%から 16.6%に減少した。また、「USB メモリ、撮影機器等の持込み・持ち出し制限」及び「業務用 PC 等での USB メモリ等への書き出し制御」の割合も減少しており、前者は 47.6%から 28.8%に、後者は 34.5%から 22.8%に減少した。「業務使用 PC 等のワイヤー等での固定」の割合も 17.5%から 13.5%に減少した。

一方で、2020 年度調査と比較して割合が増加した項目もあった。電子メールの利用に関する 2 項目については、「電子メールに添付できるファイルの制限」は 14.1%から 18.2%に、「電子メール送信時の上長確認フローを運用（必ず上司等が CC に追加される設定を行っている等）」は 7.0%から 15.7%に増加した。また、PC 等でのデータの取扱いに関する 3 項目でも割合が増加しており、「業務使用 PC 等のローカルドライブへの保存制限」は 11.3%から 17.1%に、「コンテンツフィルタによるオンラインストレージ等へのアクセス制限」は 14.7%から 16.9%に、「遠隔データ表居機能を有する PC や端末の利用」は 10.2%から 15.2%に増加した。

表 16 Q19 営業秘密情報の社外への不正持出の防止策として実施している対策
(業種、従業員数、売上高、所属部門別)

(%)

		営業秘密記載資料の提示後回収	業務使用PC等のワイヤー等での固定	USBメモリ、撮影機器等の持ち込み・持ち出し制限	紙資料、IT機器、記録媒体等の採番・台帳管理	紙資料、IT機器、記録媒体等の施錠保管	従業員IDカードでの印刷・複写制限	業務使用PC等のローカルドライブへの保存制限	業務使用PC等でのUSBメモリ等への書き出し制御	USBメモリやDVD等の複製制限	遠隔データ消去機能を有するPCや端末の利用	電子メールの添付ファイルの制限・または禁止	電子メール送信時の上長確認フローを運用(必ず上司等がCCに追加される設定を行っている等)	コンテンツフィルタによるオンラインストレージ等へのアクセス制限	その他	特に何もしていない
合計		11.5	13.5	28.8	16.6	17.3	15.7	17.1	22.8	21.4	15.2	18.2	15.7	16.9	0.2	28.2
業種	製造業	12.2	14.8	31.7	18.8	19.8	19.0	18.3	23.8	24.0	15.7	21.3	16.7	20.2	−	23.2
	非製造業	10.8	12.2	25.8	14.3	14.8	12.3	15.8	21.7	18.8	14.7	15.0	14.7	13.7	0.3	33.2
従業員数	301人以上	15.0	20.7	38.2	22.5	23.7	22.5	24.3	32.7	30.7	21.8	24.5	21.0	23.2	−	13.8
	300人以下	8.0	6.3	19.3	10.7	11.0	8.8	9.8	12.8	12.2	8.5	11.8	10.3	10.7	0.3	42.5
従業員数・業種	従業員数301人以上かつ製造業	16.7	23.0	42.7	25.7	28.3	26.0	26.0	33.3	35.7	21.3	29.0	21.0	26.7	−	10.7
	従業員数300人以下かつ製造業	7.7	6.7	20.7	12.0	11.3	12.0	10.7	14.3	12.3	10.0	13.7	12.3	13.7	−	35.7
	従業員数301人以上かつ非製造業	13.3	18.3	33.7	19.3	19.0	19.0	22.7	32.0	25.7	22.3	20.0	21.0	19.7	−	17.0
	従業員数300人以下かつ非製造業	8.3	6.0	18.0	9.3	10.7	5.7	9.0	11.3	12.0	7.0	10.0	8.3	7.7	0.7	49.3
売上高	10億円以下	6.2	4.6	18.0	10.3	10.5	7.2	7.5	10.3	11.6	7.2	10.0	8.0	7.7	0.5	54.5
	10億円超～100億円以下	11.5	11.2	26.9	12.7	13.8	12.7	18.5	19.6	17.3	13.8	14.2	16.2	16.2	−	22.3
	100億円超～1,000億円以下	12.8	17.9	35.5	19.8	21.2	19.0	17.2	30.0	27.1	18.7	21.2	19.4	20.1	−	12.5
	1,000億円超～5,000億円以下	11.3	18.9	38.7	26.4	23.6	23.6	27.4	28.3	27.4	18.9	28.3	19.8	25.5	−	8.5
	5,000億円超	21.5	26.7	39.0	25.6	27.9	29.1	30.2	40.7	37.2	27.3	31.4	23.8	28.5	−	14.5
所属部門	企業における情報システム関連部門	12.5	20.1	35.9	21.6	21.6	21.3	20.4	30.1	28.6	21.3	22.5	19.1	22.8	−	22.2
	企業のリスクマネジメント計画・実践に関わる部門	17.7	16.5	30.4	20.9	20.3	19.6	21.5	26.6	20.9	19.6	27.2	27.2	25.3	−	6.3
	企業のサイバーセキュリティに関わる部門	13.9	19.0	35.4	24.1	29.1	21.5	27.8	32.9	30.4	21.5	22.8	27.8	16.5	−	5.1
	経営企画部門	11.3	10.8	25.4	14.6	14.6	15.5	15.5	21.1	22.5	11.7	17.8	10.8	15.0	−	26.3
	経営層	7.7	4.7	16.8	8.8	10.4	5.4	7.1	10.1	10.8	6.7	7.1	5.7	8.1	0.7	57.2
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	8.9	14.5	37.9	15.3	16.1	16.9	22.6	25.0	21.0	15.3	19.4	16.1	15.3	−	20.2

業種、従業員数、売上高、所属部門別に集計したところ、従業員数・業種別では、従業員数 301 人以上の製造業で、対策の実施割合が全般的に高かった。また、売上高が大きくなるほど、対策の実施割合が高くなる傾向が見られた。電磁的記録媒体の利用に関する対策(太字)は、従業員数、業種、売上高、所属部門に限らず、実施割合が比較的高い傾向が見られた。「特に何もしていない」を選択した割合が合計に比べて＋10 ポイント以上高かったのは、従業員数別では 300 人以下で 42.5%、従業員数・業種別では従業員数 300 人以下かつ非製造業の場合で 49.3%、売上高別では 10 億円以下の場合で 54.5%、所属部門別では経営層の場合で 57.2%であった。

Q20 営業秘密の漏えいを生じさせにくい環境をつくるための対策として、実施しているものを選択してください。(MA)

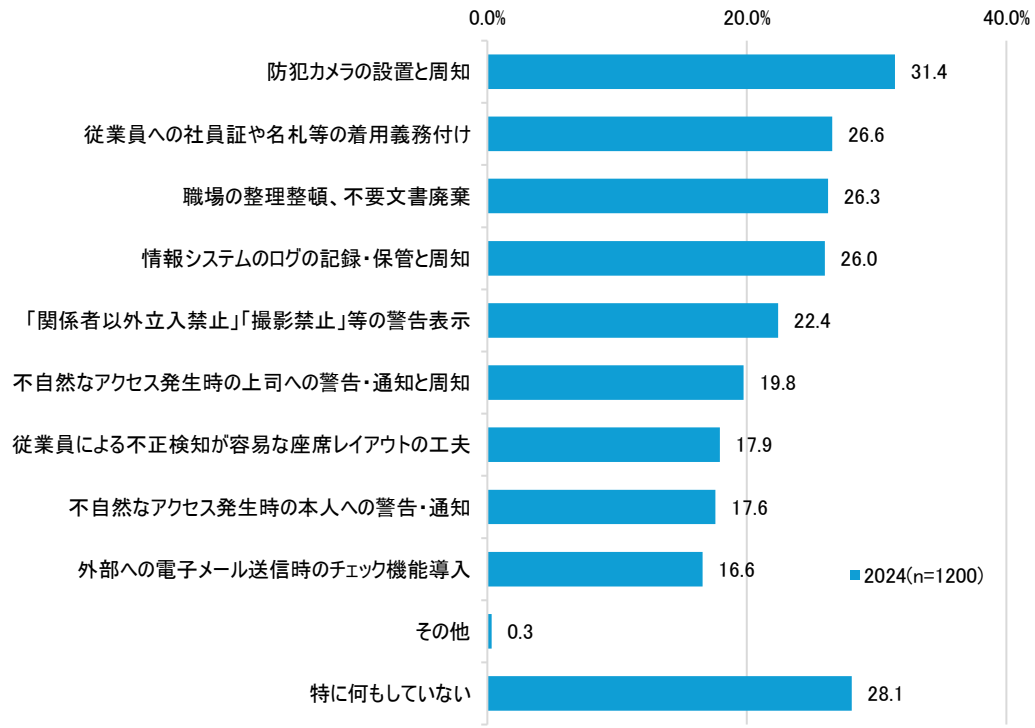


図 51 Q20 営業秘密の漏えいを生じさせにくい環境をつくるために実施している対策(MA、n=1200)

営業秘密の漏えいを生じさせにくい環境をつくるために実施している対策について、「防犯カメラの設置と周知」が最も高く 31.4%であった。次いで「従業員への社員証や名札などの着用義務付け」が 26.6%、「職場の整理整頓、不要文書廃棄」が 26.3%であった。

いずれも実施率が高くても 20~30%程度にとどまっていた。「特に何もしていない」とする割合は 28.1%であった。

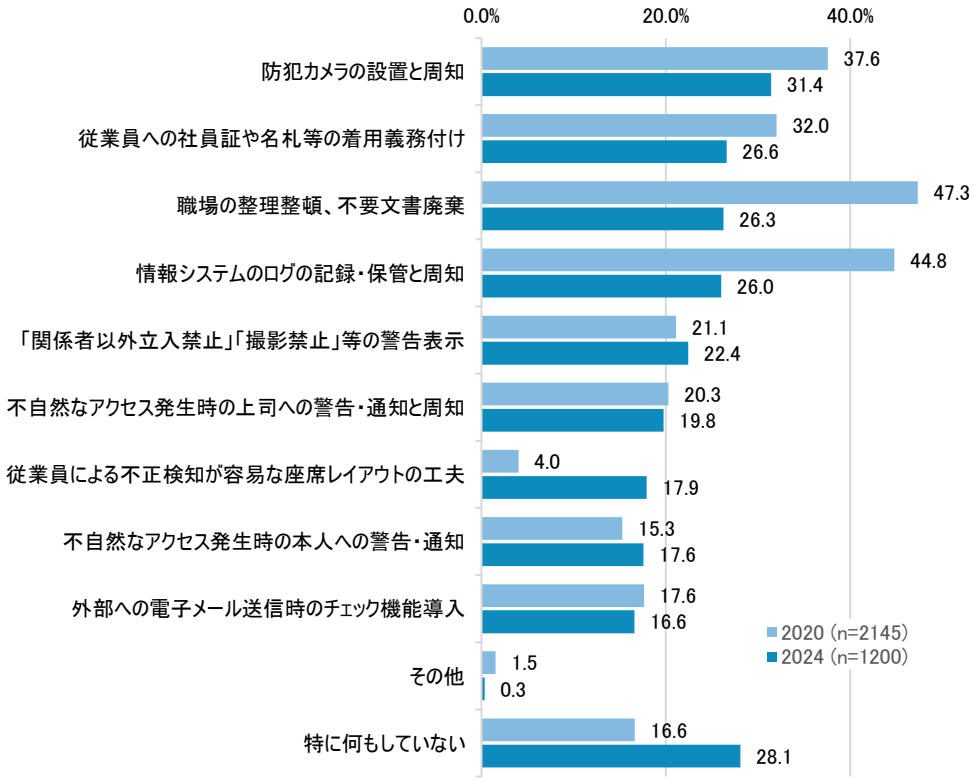


図 52 Q20 営業秘密の漏えいを生じさせにくい環境をつくるために実施している対策（経年比較）

2020 年度調査と比較すると、「職場の整理整頓、不要文書廃棄」は 47.3%から 26.3%に、「情報システムのログの記録・保管と周知」は 44.8%から 26.0%に大きく減少した。また「防犯カメラ設置と周知」も減少し 37.6%から 31.4%に、「従業員への社員証や名札等の着用義務付け」は 32.0%から 26.6%に減少した。一方、「従業員による不正検知が容易な座席レイアウトの工夫」の割合は 4.0%から 17.9%に大きく増加していた。また、「特に何もしていない」も増加しており、16.6%から 28.1%となった。

表 17 Q20 営業秘密の漏えいを生じさせにくい環境をつくるために実施している対策
(業種、従業員数、売上高、所属部門別)

(%)

		「関係者以外立入禁止」「撮影禁止」等の警告表示	従業員への社員証や名札等の着用義務付け	防犯カメラの設置と周知	職場の整理整頓、不要文書廃棄	従業員による不正検知が容易な座席レイアウトの工夫	情報システムのログの記録・保管と周知	不自然なアクセス発生時の上司への警告・通知と周知	不自然なアクセス発生時の本人への警告・通知	外部への電子メール送信時のチェック機能導入	その他	特に何もしていない
合計		22.4	26.6	31.4	26.3	17.9	26.0	19.8	17.6	16.6	0.3	28.1
業種	製造業	27.2	29.2	34.2	28.2	21.0	29.5	22.0	20.0	18.3	−	23.3
	非製造業	17.7	24.0	28.7	24.3	14.8	22.5	17.5	15.2	14.8	0.7	32.8
従業員数	301 人以上	31.7	38.2	42.3	33.2	23.7	35.7	25.8	23.3	23.0	0.2	14.7
	300 人以下	13.2	15.0	20.5	19.3	12.2	16.3	13.7	11.8	10.2	0.5	41.5
従業員数・業種	従業員数 301 人以上かつ製造業	36.7	40.3	44.3	35.7	28.0	40.3	29.0	25.3	26.0	−	12.0
	従業員数 300 人以下かつ製造業	17.7	18.0	24.0	20.7	14.0	18.7	15.0	14.7	10.7	−	34.7
	従業員数 301 人以上かつ非製造業	26.7	36.0	40.3	30.7	19.3	31.0	22.7	21.3	20.0	0.3	17.3
	従業員数 300 人以下かつ非製造業	8.7	12.0	17.0	18.0	10.3	14.0	12.3	9.0	9.7	1.0	48.3
売上高	10 億円以下	10.0	11.3	15.2	16.2	9.3	11.8	11.6	10.8	9.3	0.8	52.7
	10 億円超～100 億円以下	20.0	27.3	30.8	25.8	16.2	30.0	16.5	16.5	12.7	−	22.3
	100 億円超～1,000 億円以下	27.5	35.2	42.9	31.9	22.7	31.9	26.0	22.7	21.2	−	13.9
	1,000 億円超～5,000 億円以下	30.2	35.8	34.9	34.9	27.4	34.0	25.5	17.9	19.8	−	9.4
	5,000 億円超	41.3	40.7	48.8	35.5	26.7	37.8	29.7	26.2	29.7	0.6	15.1
所属部門	企業における情報システム関連部門	31.6	37.7	37.7	27.7	21.0	36.2	26.4	21.0	18.5	0.3	22.2
	企業のリスクマネジメント計画・実践に関わる部門	29.7	36.1	35.4	34.8	27.8	32.3	25.3	21.5	16.5	−	8.2
	企業のサイバーセキュリティに関わる部門	29.1	36.7	41.8	32.9	36.7	34.2	30.4	20.3	16.5	−	5.1
	経営企画部門	21.1	25.4	36.6	25.4	14.1	19.7	16.4	17.8	18.3	−	25.4
	経営層	9.1	7.1	16.5	16.2	5.7	12.1	11.1	9.1	11.4	1.0	56.9
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	18.5	27.4	29.8	33.1	21.0	29.8	14.5	21.8	21.0	−	19.4

業種、従業員数、売上高、所属部門別に集計したところ、業種別では、合計に比べて＋5 ポイント以上の差が生じている項目は無かった。

従業員数・業種別では、従業員数 301 人以上かつ製造業の場合、9 つのうち「防犯カメラの設置と周知」等 5 つの対策では合計に比べて＋10%ポイント以上、残る 4 つの対策においても合計に比べて＋5ポイント以上の割合となっていた。一方で、従業員数 300 人以下かつ非製造業の場合、9 つのうち「防犯カメラの設置と周知」等 4 つの対策では合計に比べて－10 ポイント以上、残る 5 つの対策についても合計に比べて－5 ポイント以上の割合の割合かつ「特に何もしていない」が 48.8%であった。

売上高別では、100 億円超になると実施割合が合計に比べて＋5 ポイント以上となる対策が高くなり、5000 億円以上の場合、いずれの対策においても合計に比べて＋5 ポイント以上の割合となっていた。一方で、10 億円以下の場合、いずれの対策においても実施割合が合計に比べて－5 ポ

イント以上の割合かつ「特に何もしていない」が 52.7%であった。

所属部門別では、企業における情報システム関連部門、企業のリスクマネジメント計画・実践に関わる部門及び企業のサイバーセキュリティに関わる部門の場合、実施割合が合計に比べて＋5 ポイント以上となる対策が高かった。一方で、経営層は、9 つの対策のうち 6 つでは合計に比べて－10 ポイント以上の割合、残る 3 つの対策についても合計に比べて－5 ポイント以上の割合、さらに「特に何もしていない」が 56.9%であった。

Q21 転職者・出向者の受け入れや、共同研究・研究受託等によって、自社の情報と他者の情報との混在（コンタミネーション）が生じることがあります。こうした情報のコンタミネーションにより、他者の秘密情報を意図せず使用してしまうリスクが考えられますが、こうしたリスクに対して、どのような対策を行っていますか。（MA）

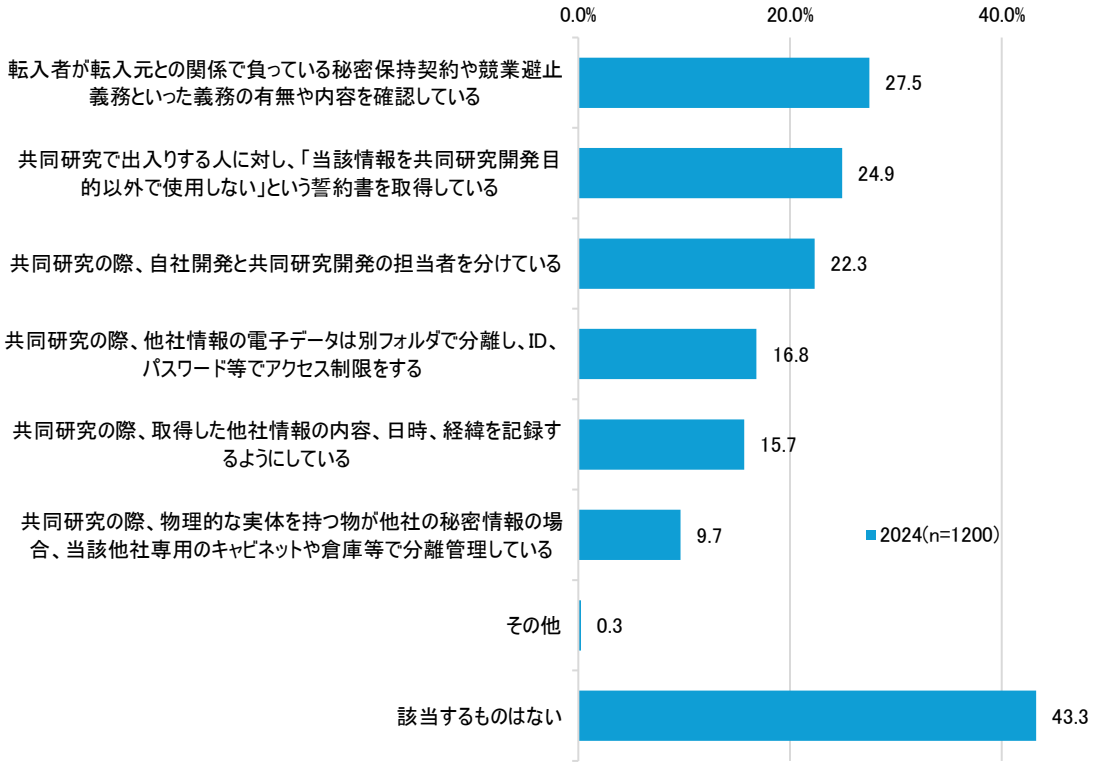


図 53 Q21 情報のコンタミネーション対策(MA、n=1200)

情報のコンタミネーション対策として、「該当するものはない」を除き、最も実施しているとされる割合が高かったのは「転入者が転入元との関係で負っている秘密保持契約や競業避止義務契約といった義務の有無や内容を確認している」で 27.5%であった。次いで「共同研究で出入りする人に対し、「当該情報を共同研究開発目的以外で使用しない」という誓約書を取得している」が 24.9%、「共同研究の際、自社開発と共同研究開発の担当者を分けている」が 22.3%であった。

全体としては、「該当するものはない」が最も高く 43.3%であった。

表 18 Q21 情報のコンタミネーション対策(業種、従業員数、売上高、所属部門別)

(%)

		転入者が転入元との関係で負っている秘密保持契約や競業避止義務といった義務の有無や内容を確認している	共同研究の際、自社開発と共同研究開発の担当者を分けている	共同研究で出入りする人に対し、「当該情報を共同研究開発目的以外で使用しない」という誓約書を取得している	共同研究の際、取得した他社情報の内容、日時、経緯を記録するようにしている	共同研究の際、他社情報の電子データは別フォルダで分離し、ID、パスワード等でアクセス制限をする	共同研究の際、物理的な実体を持つ物が他社の秘密情報の場合、当該他社専用のキャビネットや倉庫等で分離管理している	その他	該当するものはない
合計		27.5	22.3	24.9	15.7	16.8	9.7	0.3	43.3
業種	製造業	31.7	24.8	30.0	18.8	19.0	12.0	0.3	36.5
	非製造業	23.3	19.8	19.8	12.5	14.7	7.3	0.2	50.0
従業員数	301 人以上	35.0	30.0	33.7	20.2	25.8	14.0	0.3	28.7
	300 人以下	20.0	14.7	16.2	11.2	7.8	5.3	0.2	57.8
従業員数・業種	従業員数 301 人以上かつ製造業	39.7	31.0	39.7	24.7	29.3	17.3	0.7	24.3
	従業員数 300 人以下かつ製造業	23.7	18.7	20.3	13.0	8.7	6.7	−	48.7
	従業員数 301 人以上かつ非製造業	30.3	29.0	27.7	15.7	22.3	10.7	−	33.0
	従業員数 300 人以下かつ非製造業	16.3	10.7	12.0	9.3	7.0	4.0	0.3	67.0
売上高	10 億円以下	14.7	11.8	10.8	9.5	8.2	3.9	0.3	67.6
	10 億円超～100 億円以下	28.1	20.4	25.4	13.8	11.9	9.2	−	41.5
	100 億円超～1,000 億円以下	33.0	25.3	32.6	19.0	24.2	12.1	−	28.2
	1,000 億円超～5,000 億円以下	35.8	32.1	34.0	18.9	22.6	10.4	−	24.5
	5,000 億円超	41.9	38.4	38.4	25.0	28.5	19.2	1.2	26.2
所属部門	企業における情報システム関連部門	33.4	29.8	27.7	17.9	21.9	10.9	−	40.7
	企業のリスクマネジメント計画・実践に関わる部門	40.5	36.7	42.4	24.7	19.0	13.9	0.6	13.9
	企業のサイバーセキュリティに関わる部門	39.2	45.6	45.6	30.4	20.3	16.5	−	7.6
	経営企画部門	24.9	15.0	21.1	9.9	15.5	8.0	0.5	44.6
	経営層	12.8	5.4	9.1	7.1	8.1	4.4	0.3	74.4
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	27.4	22.6	26.6	19.4	21.8	12.1	−	33.1

業種、従業員数、売上高、所属部門別に集計したところ、従業員数・業種別では、従業員数 301 人以上かつ製造業の場合にいずれの対策についても合計に比べて＋5 ポイント以上で、例えば「転入者が転入元との関係で負っている秘密保持契約や競業避止義務といった義務の有無や内容を確認している」は 39.7%、「共同研究で出入りする人に対し、「当該情報を共同研究開発目的以外で使用しない」という誓約書を取得している」は 39.7%、「共同研究の際、他社情報の電子データは別フォルダで分離し、ID、パスワード等でアクセス制限をする」は 29.3%であった。

所属部門別では、「転入者が転入元との関係で負っている秘密保持契約や競業避止義務といった義務の有無や内容を確認している」、「共同研究の際、自社開発と共同研究開発の担当者を分けている」、「共同研究で出入りする人に対し、「当該情報を共同研究開発目的以外で使用しない」という誓約書を取得している」、「共同研究の際、取得した他社情報の内容、日時、経緯を記録するようにしている」の 4 つの対策について、企業のリスクマネジメント計画・実践に関わる部門及び企業のサイバーセキュリティに関わる部門の 2 部門で合計に比べて＋5 ポイント以上の割合となっていた。企業のリスクマネジメント計画・実践に関わる部門では、「転入者が転入元との関係で負っている秘密保持契約や競業避止義務といった義務の有無や内容を確認している」が 40.5%、「共同研究の際、自社開発と共同研究開発の担当者を分けている」が 36.7%、「共同研究で出入り

する人に対し、「当該情報を共同研究開発目的以外で使用しない」という誓約書を取得している」が 42.4%、「共同研究の際、取得した他社情報の内容、日時、経緯を記録するようにしている」が 24.7%であった。企業のサイバーセキュリティに関わる部門では、「転入者が転入元との関係で負っている秘密保持契約や競業避止義務といった義務の有無や内容を確認している」が 39.2%、「共同研究の際、自社開発と共同研究開発の担当者を分けている」が 45.6%、「共同研究で出入りする人に対し、「当該情報を共同研究開発目的以外で使用しない」という誓約書を取得している」が 45.6%、「共同研究の際、取得した他社情報の内容、日時、経緯を記録するようにしている」が 30.4%であった。

表 19 Q21 情報のコンタミネーション対策(対策項目ごとの実施割合)

(%)

		転入者が転入元との関係で負っている秘密保持契約や競業避止義務といった義務の有無や内容を確認している	共同研究の際、自社開発と共同研究開発の担当者を分けている	共同研究で出入りする人に対し、「当該情報を共同研究開発目的以外で使用しない」という誓約書を取得している	共同研究の際、取得した他社情報の内容、日時、経緯を記録するようにしている	共同研究の際、他社情報の電子データは別フォルダで分離し、ID、パスワード等でアクセス制限をする	共同研究の際、物理的な実体を持つ物が他社の秘密情報の場合、当該他社専用のキャビネットや倉庫等で分離管理している	その他	該当するものはない
合計		27.5	22.3	24.9	15.7	16.8	9.7	0.3	43.3
業種	製造業	31.7	24.8	30.0	18.8	19.0	12.0	0.3	36.5
	非製造業	23.3	19.8	19.8	12.5	14.7	7.3	0.2	50.0
従業員数	301 人以上	35.0	30.0	33.7	20.2	25.8	14.0	0.3	28.7
	300 人以下	20.0	14.7	16.2	11.2	7.8	5.3	0.2	57.8
従業員数・業種	従業員数 301 人以上かつ製造業	39.7	31.0	39.7	24.7	29.3	17.3	0.7	24.3
	従業員数 300 人以下かつ製造業	23.7	18.7	20.3	13.0	8.7	6.7	−	48.7
	従業員数 301 人以上かつ非製造業	30.3	29.0	27.7	15.7	22.3	10.7	−	33.0
	従業員数 300 人以下かつ非製造業	16.3	10.7	12.0	9.3	7.0	4.0	0.3	67.0
売上高	10 億円以下	14.7	11.8	10.8	9.5	8.2	3.9	0.3	67.6
	10 億円超～100 億円以下	28.1	20.4	25.4	13.8	11.9	9.2	−	41.5
	100 億円超～1,000 億円以下	33.0	25.3	32.6	19.0	24.2	12.1	−	28.2
	1,000 億円超～5,000 億円以下	35.8	32.1	34.0	18.9	22.6	10.4	−	24.5
	5,000 億円超	41.9	38.4	38.4	25.0	28.5	19.2	1.2	26.2
所属部門	企業における情報システム関連部門	33.4	29.8	27.7	17.9	21.9	10.9	−	40.7
	企業のリスクマネジメント計画・実践に関わる部門	40.5	36.7	42.4	24.7	19.0	13.9	0.6	13.9
	企業のサイバーセキュリティに関わる部門	39.2	45.6	45.6	30.4	20.3	16.5	−	7.6
	経営企画部門	24.9	15.0	21.1	9.9	15.5	8.0	0.5	44.6
	経営層	12.8	5.4	9.1	7.1	8.1	4.4	0.3	74.4
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	27.4	22.6	26.6	19.4	21.8	12.1	−	33.1

また、区分ごとに対策項目それぞれの実施割合を見ると、比較的高く実施されている傾向にあったのは「転入者が転入元との関係で負っている秘密保持契約や競業避止義務といった義務の有無や内容を確認している」、「共同研究で出入りする人に対し、「当該情報を共同研究開発目的以外で使用しない」という誓約書を取得している」の 2 つであった。「共同研究の際、自社開発と共同研究開発の担当者を分けている」は、売上高が 1000 億円超になると実施されている割合も比較的高く 30%以上で、所属部門別では、企業における情報システム関連部門、企業のリスクマネジメント計画・実践に関わる部門及び企業のサイバーセキュリティに関わる部門でも比較的高く、30%以上であった。

Q22 就業規則以外に役員・従業員と秘密保持契約（それに準じるような誓約書を含む）を締結していますか。締結している場合は、秘密保持の期間についてもお答えください。（SA）

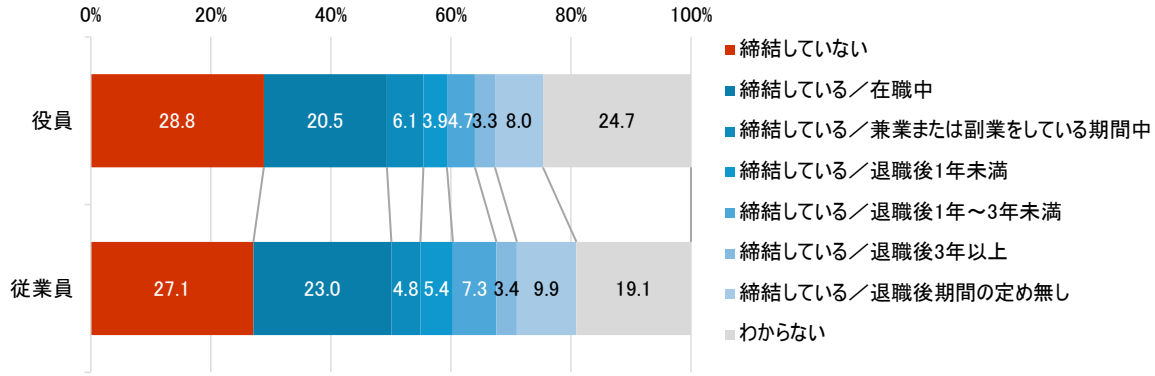


図 54 Q22 秘密保持契約の締結状況(n=1200)

秘密保持契約の締結状況について、「締結していない」の割合は、役員については 28.8%、従業員については 27.1%であった。締結している期間については、「在職中」が最も高く、役員は 20.5%、従業員は 23.0%であった。次いで、「退職後期間の定め無し」が高く、役員の場合 8.0%、従業員の場合 9.9%であった。

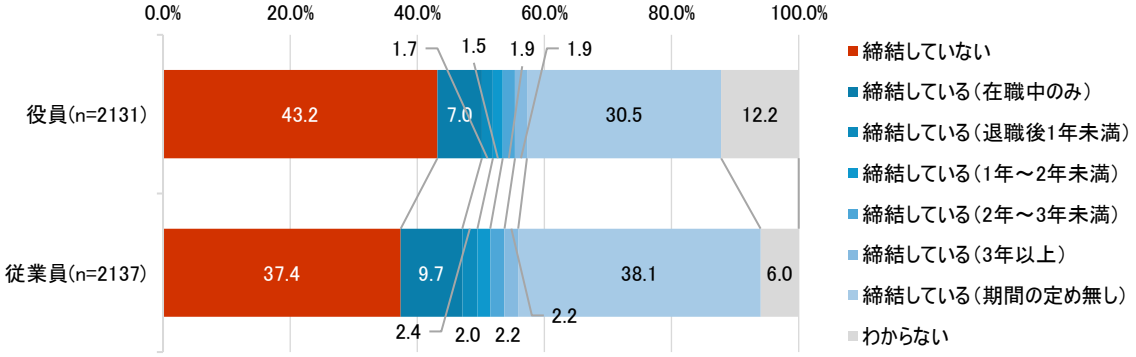


図 55 Q22 (参考)2020 年度調査 秘密保持契約の締結状況

2020 年度調査と比較すると、「締結していない」の割合は減少し、役員は 43.2%から 28.8%に、従業員は 37.4%から 27.1%となった。また、締結している期間については期間の定めがない割合が減少し、役員は 30.5%から 8.0%に、従業員は 38.1%から 9.9%となった。一方で締結している期間に期限がある割合は増加しており、例えば「在職中のみ」とする割合は役員では 7.0%から 20.5%に、従業員では 9.7%から 23.0%に増加した。また、「わからない」とする割合も増加していた。

表 20 Q22 役員の秘密保持契約の締結状況(業種、従業員数別)

(%)

		締結していない	締結している／在職中	締結している／兼業または副業をしている期間中	締結している／退職後 1 年未満	締結している／退職後 1 年～3 年未満	締結している／退職後 3 年以上	締結している／退職後期間の定め無し	わからない
合計		28.8	20.5	6.1	3.9	4.7	3.3	8.0	24.7
業種	製造業	26.2	22.0	6.5	4.2	6.3	4.5	7.5	22.8
	非製造業	31.5	19.0	5.7	3.7	3.0	2.2	8.5	26.5
従業員数	301 人以上	14.3	22.5	8.3	4.3	6.3	4.7	8.3	31.2
	300 人以下	43.3	18.5	3.8	3.5	3.0	2.0	7.7	18.2
従業員数・業種	従業員数 301 人以上かつ製造業	16.3	22.0	9.3	3.7	8.3	5.7	7.3	27.3
	従業員数 300 人以下かつ製造業	36.0	22.0	3.7	4.7	4.3	3.3	7.7	18.3
	従業員数 301 人以上かつ非製造業	12.3	23.0	7.3	5.0	4.3	3.7	9.3	35.0
	従業員数 300 人以下かつ非製造業	50.7	15.0	4.0	2.3	1.7	0.7	7.7	18.0

役員の秘密保持契約の締結状況を業種、従業員数別に集計したところ、従業員数・業種別では、「締結していない」の割合が合計に比べて＋10 ポイント以上であったのは従業員数 300 人以下かつ非製造業の場合で 50.7%、＋5 ポイント以上であったのは従業員数 300 人以下かつ製造業の場合で 36.0%であった。

表 21 Q22 従業員の秘密保持契約の締結状況(業種、従業員数別)

(%)

		締結していない	締結している／在職中	締結している／兼業または副業をしている期間中	締結している／退職後 1 年未満	締結している／退職後 1 年～3 年未満	締結している／退職後 3 年以上	締結している／退職後期間の定め無し	わからない
合計		27.1	23.0	4.8	5.4	7.3	3.4	9.9	19.1
業種	製造業	24.7	24.7	5.5	6.3	9.0	4.3	9.3	16.2
	非製造業	29.5	21.3	4.2	4.5	5.5	2.5	10.5	22.0
従業員数	301 人以上	11.3	26.3	5.2	6.3	10.5	5.0	12.5	22.8
	300 人以下	42.8	19.7	4.5	4.5	4.0	1.8	7.3	15.3
従業員数・業種	従業員数 301 人以上かつ製造業	13.3	26.7	6.0	6.3	12.7	6.0	12.0	17.0
	従業員数 300 人以下かつ製造業	36.0	22.7	5.0	6.3	5.3	2.7	6.7	15.3
	従業員数 301 人以上かつ非製造業	9.3	26.0	4.3	6.3	8.3	4.0	13.0	28.7
	従業員数 300 人以下かつ非製造業	49.7	16.7	4.0	2.7	2.7	1.0	8.0	15.3

従業員の秘密保持契約の締結状況を業種、従業員数別に集計したところ、役員と同様の傾向が見られた。従業員数・業種別では、「締結していない」の割合が合計に比べて＋10 ポイント以上であったのは従業員数 300 人以下かつ非製造業の場合で 49.7%、＋5 ポイント以上であったのは従業員数 300 人以下かつ製造業の場合で 36.0%であった。

Q23 役員・従業員との競業避止義務契約（それに準じるような誓約書を含む）を締結していますか。締結している場合は、競業避止の期間についてもお答えください。なお、就業規則のみで対応している場合は「締結していない」を選択ください。（お答えはそれぞれ 1 つずつ）

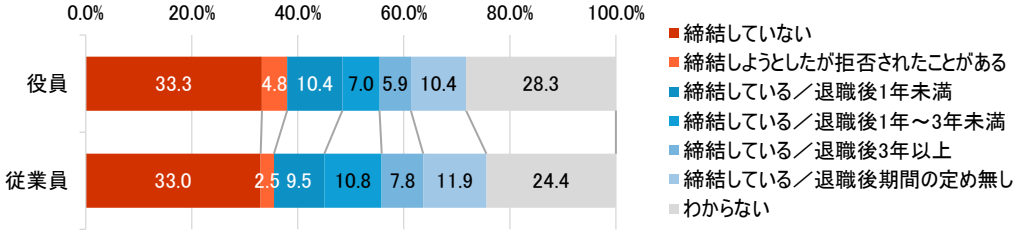


図 56 Q23 競業避止義務契約の締結状況（n=1200）

競業避止義務契約の締結状況について、役員と従業員のいずれも、「役員・従業員との競業避止義務契約（またはそれに準じる誓約書）」を締結していない割合が最も高く、役員は 33.3%、従業員は 33.0%であった。

競業避止義務契約（またはそれに準じる誓約書）を締結している期間については、退職後 1 年未満は役員では 10.4%、従業員では 9.5%、退職後 1 年～3 年未満は役員では 7.0%、従業員では 10.8%、退職後 3 年以上は役員では 5.9%、従業員では 7.8%、退職後期間の定めが無いのは役員で 10.4%、従業員で 11.9%であった。

また、競業避止義務契約を締結しているかについて「わからない」と回答したのは役員では 28.3%、従業員では 24.4%であった。

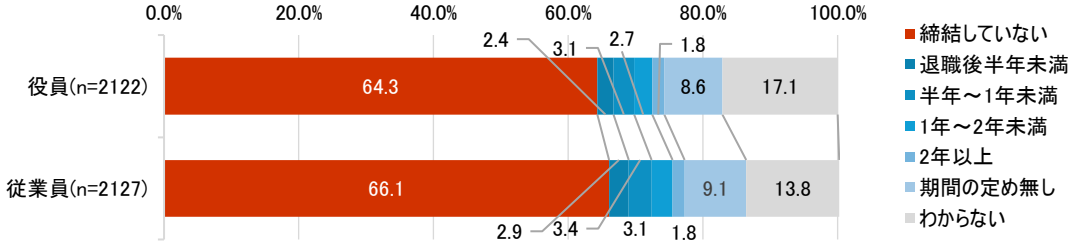


図 57 (参考)2020 年度調査 競業避止義務契約の締結状況

2020 年度調査と比較すると、役員、従業員とも、「締結していない」割合が大きく減少しており、65%程度から 33%程度まで減少した。

また、2020 年度調査時は「わからない」を除くと競業避止義務契約を締結している「退職後半年未満」、「半年～1 年未満」、「1 年～2 年未満」、「2 年以上」、「期間の定め無し」を合わせた割合は役員、従業員ともに半数に満たなかった。しかし、本調査では「わからない」を除くと競業避止義務契約を締結している「締結している／退職後 1 年未満」、「締結している／退職後 1 年～3 年未満」、「締結している／退職後 3 年以上」、「締結している／退職後期間の定め無し」を合わせた割合は、役員、従業員共に半数程度を占めていた。

Q24 役員・従業員との競業避止義務契約（それに準じるような誓約書を含む）の中では、競業避止の期間以外に、どのような内容を取り決めていますか。（MA）

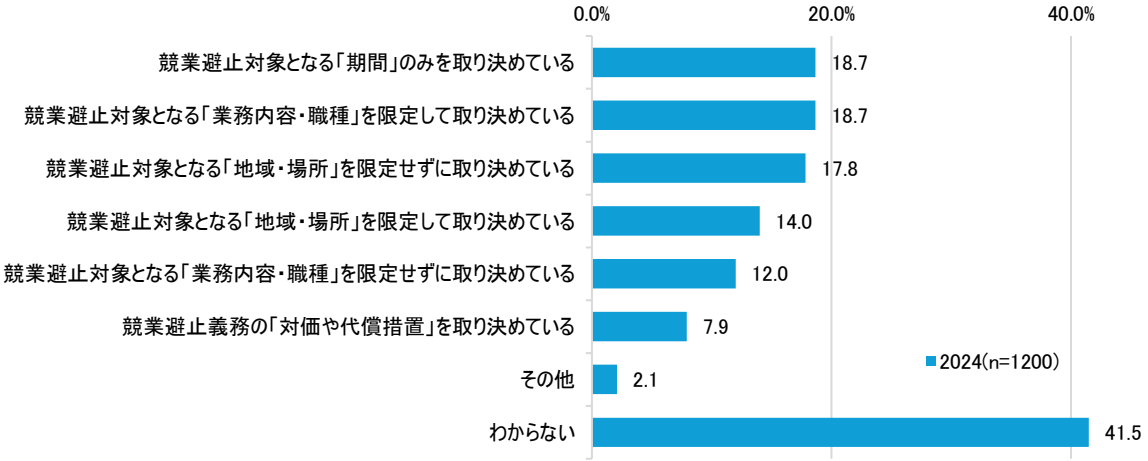


図 58 Q24 競業避止義務契約の対象とする内容の範囲(MA、n=1200)

競業避止義務契約の対象とする内容の範囲について、「業務内容・職種」を限定して取り決めている企業は 18.7%、「地域・場所」を限定して取り決めている企業は 17.8%であった。

競業避止義務契約の対象とする内容の範囲を限定せず、「期間のみを取り決めている」企業は 18.7%であった。また、「場所を限定せずに取り決めている」は 14.0%、「業務内容・職種を限定せずに取り決めている」は 7.9%であった。

また、「義務の対価や代償措置」を取り決めているのは 7.9%、「答えがわからない」が最も高く 41.5%であった。

Q25 競業避止義務に違反した役員・従業員に対してどのような対応をとりましたか。(MA)

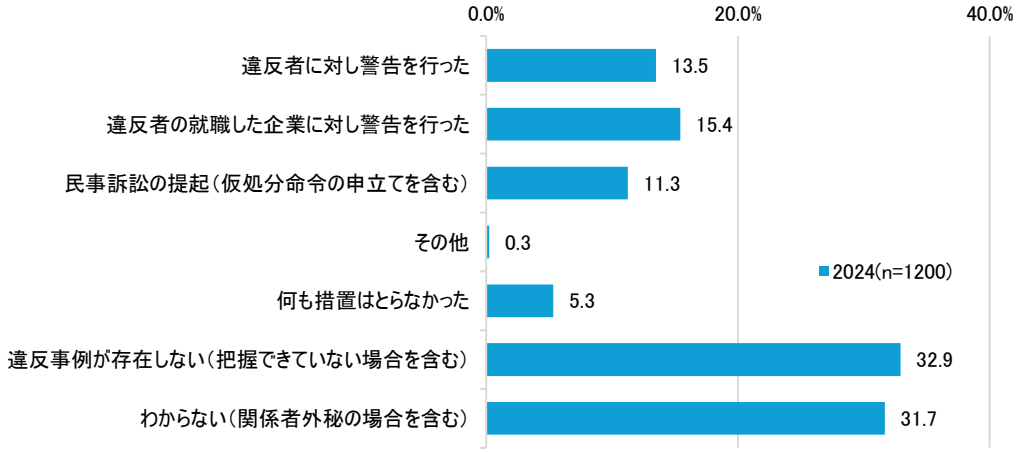


図 59 Q25 競業避止義務に違反した役員・従業員への対応(MA)

競業避止義務に違反した役員・従業員に対して実際に行った対応について、全体で最も高かったのは「違反事例が存在しない(把握できていない場合を含む)」で 32.9%、次いで「わからない(関係者外秘の場合を含む)」が 31.7%であった。

また、実際に行った対応としては、「違反者の就職した企業に対し警告を行った」が最も多く 15.4%であった。次いで「違反者に対し警告を行った」が 13.5%、「民事訴訟の提起(仮処分命令の申立て含む)」が 11.3%であった。「何も措置の取らなかった」は 5.3%であった。

2.1.4　最近の動向を踏まえた対策

Q26 子会社、関連会社、取引先、共同研究先など、あなたが所属する組織事業のサプライチェーンにおける営業秘密の管理状況について、どこまで把握していますか。最も近いものを選択してください。（SA）

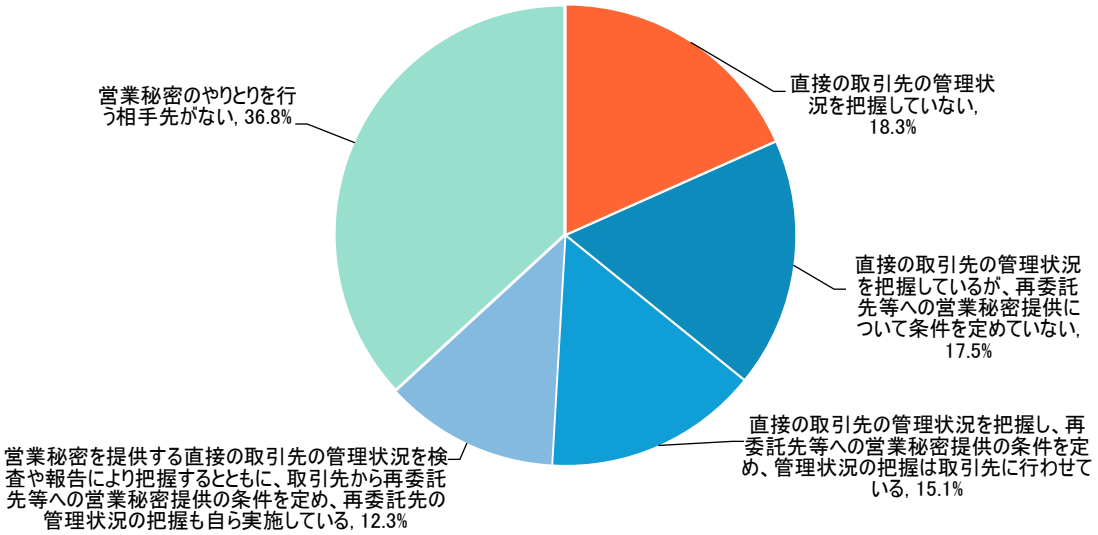


図　60 Q26 サプライチェーンにおける営業秘密の管理状況の把握（n=1200）

サプライチェーンにおける営業秘密の管理状況の把握について、直接の取引先の管理状況を把握している場合、「再委託先等への営業秘密提供について条件を定めていない」の割合が最も高く 17.5%、「再委託先等への営業秘密提供の条件を定め、管理状況の把握は取引先に行わせている」が 15.1%、「取引先から再委託先等への営業秘密提供の条件を定め、再委託先の管理状況の把握も自ら実施している」が 12.3%であった。これらを合わせた直接の取引先の管理状況を把握している割合は 44.8%となった。

一方で、「直接取引先の管理状況を把握していない」の割合は 18.3%であった。また、「営業秘密のやりとりを行う相手先がない」は 36.8%であった。

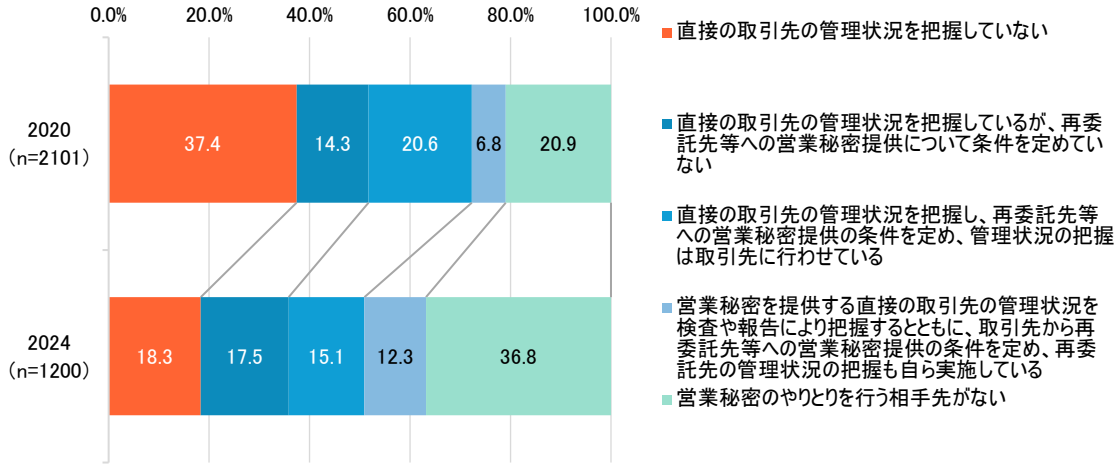


図 61 Q26 サプライチェーンにおける営業秘密の管理状況の把握（経年比較）

2020 年度調査と比較すると、直接の取引先の管理状況を把握している場合、「再委託先等への営業秘密提供について条件を定めていない」の割合が 14.3%から 17.5%に増加、「再委託先等への営業秘密提供の条件を定め、管理状況の把握は取引先に行わせている」が 20.6%から 15.1%に減少、「取引先から再委託先等への営業秘密提供の条件を定め、再委託先の管理状況の把握も自ら実施している」が 6.8%から 12.3%に増加した。また、「再委託先等への営業秘密提供について条件を定めていない」、「再委託先等への営業秘密提供の条件を定め、管理状況の把握は取引先に行わせている」、「取引先から再委託先等への営業秘密提供の条件を定め、再委託先の管理状況の把握も自ら実施している」の 3 項目を合わせた直接の取引先の管理状況を把握している割合は、2020 年度調査では 41.6%で、本調査では 44.9%であった。

「直接取引先の管理状況を把握していない」の割合は大きく減少し、37.4%から 18.3%になった。

一方で、「営業秘密のやりとりを行う相手先がない」は 20.9%から 36.8%に増加した。

「営業秘密のやり取りを行う相手先がない」を除くと、「直接の取引先の管理状況を把握していない」の割合は減少し、「再委託先等への営業秘密提供について条件を定めていない」、「再委託先等への営業秘密提供の条件を定め、管理状況の把握は取引先に行わせている」及び「取引先から再委託先等への営業秘密提供の条件を定め、再委託先の管理状況の把握も自ら実施している」の 3 項目を合わせた直接の取引先の管理状況を把握している割合は増加した。

表 22 Q26 所属組織事業のサプライチェーンにおける営業秘密の管理状況の把握について (業種別)

(%)

【業種別】	直接の取引先の管理状況を把握していない	直接の取引先の管理状況を把握している				営業秘密のやりとりを行う相手先がない
		合計	再委託先等への営業秘密提供について条件を定めていない	再委託先等への営業秘密提供の条件を定め、管理状況の把握は取引先に行わせている	営業秘密を提供する直接の取引先の管理状況を検査や報告により把握するとともに、取引先から再委託先等への営業秘密提供の条件を定め、再委託先の管理状況の把握も自ら実施している	
製造業	20.7	49.7	19.5	17.2	13.0	29.7
情報通信業	17.5	45.6	11.4	21.9	12.3	36.8
サービス業(他に分類されないもの)	13.6	40.9	13.6	11.4	15.9	45.5
小売業	13.2	24.5	15.1	9.4	0.0	62.3
専門・技術サービス業	22.4	24.5	8.2	6.1	10.2	53.1
金融業、保険業	22.9	37.1	14.3	11.4	11.4	40.0
建設業	11.4	45.7	22.9	5.7	17.1	42.9
不動産業、物品賃貸業	26.5	26.5	11.8	2.9	11.8	47.1
卸売業	15.2	48.5	21.2	18.2	9.1	36.4
医療、福祉	12.9	45.2	22.6	9.7	12.9	41.9
運輸業	17.9	39.3	25.0	14.3	0.0	42.9
教育、学習支援業	4.2	54.2	8.3	16.7	29.2	41.7
生活関連サービス業、娯楽業	8.7	43.5	21.7	17.4	4.3	47.8
その他	13.3	53.3	20.0	26.7	6.7	33.3
飲食サービス業	18.2	27.3	18.2	0.0	9.1	54.5
農林業	0.0	40.0	30.0	0.0	10.0	60.0
電気・ガス・熱供給・水道業	22.2	55.6	22.2	11.1	22.2	22.2
鉱業、採石業、砂利採取業	20.0	60.0	20.0	20.0	20.0	20.0
漁業	50.0	50.0	0.0	0.0	50.0	0.0
宿泊業	0.0	100.0	0.0	100.0	0.0	0.0

直接の取引先の管理状況を把握している場合において、「再委託先等への営業秘密提供について条件を定めていない」、「再委託先等への営業秘密提供の条件を定め、管理状況の把握は取引先に行わせている」及び「取引先から再委託先等への営業秘密提供の条件を定め、再委託先の管理状況の把握も自ら実施している」の割合を業種別に比較すると、全体的に、「再委託先等への営業秘密提供について条件を定めていない」の割合が高い傾向が見られた。

製造業においては、直接の取引先の管理状況を把握している合計の割合が 49.7%で、その中でも「再委託先等への営業秘密提供について条件を定めていない」が最も高く 19.5%であった。金融・保険業も製造業同様に、「再委託先等への営業秘密提供について条件を定めていない」が最も高く 14.3%であった。

表 23 Q26 サプライチェーンにおける営業秘密の管理状況の把握(製造業(中分類)別)

(%)

【製造業(中分類)】	直接の取引先の管理状況を把握していない	直接の取引先の管理状況を把握している				営業秘密のやりとりを行う相手先がない
		合計	再委託先等への営業秘密提供について条件を定めていない	再委託先等への営業秘密提供の条件を定め、管理状況の把握は取引先に行わせている	営業秘密を提供する直接の取引先の管理状況を検査や報告により把握するとともに、取引先から再委託先等への営業秘密提供の条件を定め、再委託先の管理状況の把握も自ら実施している	
非鉄金属	23.5	76.5	47.1	29.4	0.0	0.0
繊維工業	13.3	66.7	20.0	20.0	26.7	20.0
ゴム製品	12.5	62.5	25.0	25.0	12.5	25.0
化学	20.6	60.3	27.0	20.6	12.7	19.0
鉄鋼	17.6	58.8	29.4	14.7	14.7	23.5
プラスチック製品	4.0	56.0	8.0	16.0	32.0	40.0
輸送用機械	20.0	52.7	25.5	12.7	14.5	27.3
電機・情報通信機械・電子部品	22.4	50.7	17.2	20.9	12.7	26.9
食料品	22.4	48.3	10.3	17.2	20.7	29.3
金属製品	23.8	42.9	21.4	11.9	9.5	33.3
汎用、生産・業務用機械	27.8	40.7	14.8	16.7	9.3	31.5
パルプ・紙・紙加工品	21.7	39.1	30.4	4.3	4.3	39.1
その他	21.7	34.8	8.7	15.2	10.9	43.5
窯業・土石製品	23.1	30.8	15.4	15.4	0.0	46.2
家具・装備品	0.0	30.8	15.4	15.4	0.0	69.2

製造業(中分類)別では、直接の取引先の管理状況を把握している場合において、「再委託先等への営業秘密提供について条件を定めていない」、「再委託先等への営業秘密提供の条件を定め、管理状況の把握は取引先に行わせている」及び「取引先から再委託先等への営業秘密提供の条件を定め、再委託先の管理状況の把握も自ら実施している」の割合を業種別に比較すると、直接の取引先の管理状況を把握している割合が高い業種でも、「取引先から再委託先等への営業秘密提供の条件を定め、再委託先の管理状況の把握も自ら実施している」割合は比較的低い傾向が見られた。

Q27 あなたが所属する組織では、クラウドサービスを使って、社内・社外を問わず、営業秘密の共有や参照を行っていますか。(SA)

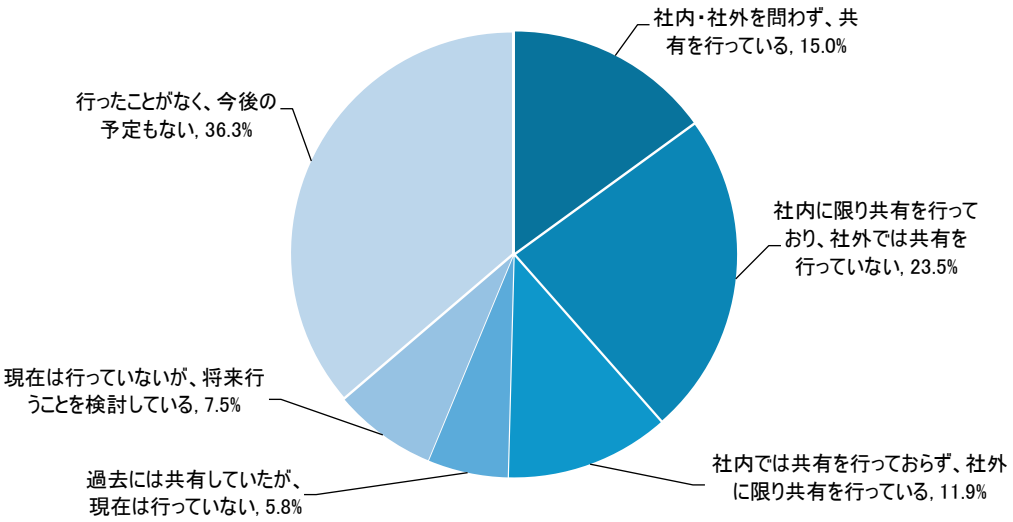


図 62 Q27 クラウドサービスを使用した営業秘密の共有や参照(n=1200)

クラウドサービスを使用した営業秘密の共有や参照について、「社内・社外を問わず、共有を行っている」の割合は 15.0%、「社内に限り共有を行っており、社外では共有を行っていない」が 23.5%、「社内では共有を行っておらず、社外に限り共有を行っている」が 11.9%で、これらを合わせた、クラウドを利用した秘密情報の共有を実施している割合は、全体の約半数(50.4%)を占めていた。

クラウドを利用して秘密情報の共有・参照をしていない場合について、「過去には共有していたが、現在は行っていない」が 5.8%、「現在は行っていないが、将来行うことを検討している」が 7.5%、「行ったことがなく、今後の予定もない」が 36.3%であった。

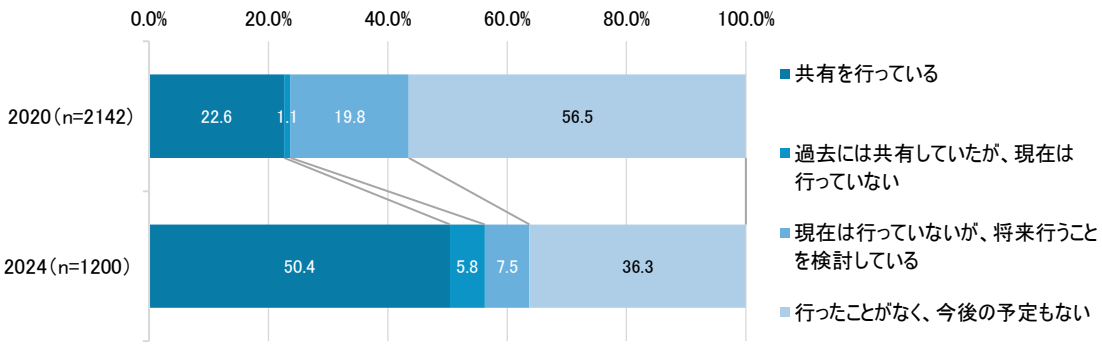


図 63 Q27 クラウドサービスを使用した営業秘密の共有や参照（経年比較）

2020 年度調査と比較するため、2024 年度調査の「社内・社外を問わず、共有を行っている」、「社内に限り共有を行っており、社外では共有を行っていない」及び「社内では共有を行っておらず、社外に限り共有を行っている」を合わせて「共有を行っている」として集計した。

2020 年度調査実施と比較すると、「共有を行っている」の割合は 22.8%から 50.4%に増加した。また、クラウドを利用して秘密情報の共有・参照をしていない場合について、「過去には共有していたが、現在は行っていない」が 1.1%から 5.8%に増加、「現在は行っていないが、将来行うことを検討している」が 19.8%から 7.5%に減少、「行ったことがなく、今後の予定もない」が 56.5%から 36.3%に減少した。

表 24 Q27 クラウドサービスを使用した営業秘密の共有や参照
(業種、従業員数、売上高、所属部門別)

(%)

		社内・社外を問わず、共有を行っている	社内に限り共有を行っており、社外では共有を行っていない	社内では共有を行っておらず、社外に限り共有を行っている	過去には共有していたが、現在は行っていない	現在は行っていないが、将来行うことを検討している	行ったことがなく、今後の予定もない
合計		15.0	23.5	11.9	5.8	7.5	36.3
業種	製造業	15.7	25.2	13.5	6.5	8.0	31.2
	非製造業	14.3	21.8	10.3	5.2	7.0	41.3
従業員数	301 人以上	20.2	26.3	16.0	7.3	5.7	24.5
	300 人以下	9.8	20.7	7.8	4.3	9.3	48.0
従業員数・業種	従業員数 301 人以上かつ製造業	22.7	27.0	14.7	7.3	6.0	22.3
	従業員数 300 人以下かつ製造業	8.7	23.3	12.3	5.7	10.0	40.0
	従業員数 301 人以上かつ非製造業	17.7	25.7	17.3	7.3	5.3	26.7
	従業員数 300 人以下かつ非製造業	11.0	18.0	3.3	3.0	8.7	56.0
売上高	10 億円以下	8.7	15.4	3.6	3.1	9.3	59.9
	10 億円超～100 億円以下	13.8	26.5	15.4	6.9	7.7	29.6
	100 億円超～1,000 億円以下	15.8	30.8	19.0	6.2	7.0	21.2
	1,000 億円超～5,000 億円以下	23.6	21.7	16.0	9.4	7.5	21.7
	5,000 億円超	24.4	26.7	11.6	7.6	4.1	25.6
所属部門	企業における情報システム関連部門	21.0	25.5	12.5	4.3	5.5	31.3
	企業のリスクマネジメント計画・実践に関わる部門	17.1	32.9	19.0	8.9	7.6	14.6
	企業のサイバーセキュリティに関わる部門	11.4	29.1	35.4	11.4	3.8	8.9
	経営企画部門	14.1	21.1	9.9	7.5	11.3	36.2
	経営層	8.8	16.5	1.7	2.7	6.7	63.6
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	15.3	23.4	14.5	7.3	10.5	29.0

業種、従業員数、売上高、所属部門別に集計したところ、従業員数別では、「社内・社外を問わず、共有を行っている」の割合は、301 人以上の場合、合計に比べて＋5 ポイント以上で 20.2%、300 人以下の場合、合計に比べて－5 ポイント以上で 9.8%であった。

また、売上高別では、「社内・社外を問わず、共有を行っている」の割合が合計に比べて＋5 ポイント以上であったのは、1,000 億円超～5,000 億円以下の場合の 23.6%と、5000 億円超の 24.4%であった。売上高が 100 億円超～1000 億円以下の場合になると、社内または社外のいずれかに限定して共有を行っている割合が合計に比べて＋5 ポイント以上となっており、「社内に限り共有を行っており、社外では共有を行っていない」は 30.8%、「社内では共有を行っておらず、社外に限り共有を行っている」は 19.0%であった。10 億円以下の場合、「行ったことがなく、今後の予定もない」が合計に比べて＋10 ポイント以上の 59.9%であった。

所属部門別では、「企業のサイバーセキュリティに関わる部門」では、社外または社内のどちらかに限り共有を行っている傾向が見られ、「社内に限り共有を行っており、社外では共有を行っていない」は合計に比べて＋5 ポイント以上の 29.1%、「社内では共有を行っておらず、社外に限り共有を行っている」は合計に比べて－10 ポイント以上の 35.4%であった。経営層は、共有を行っている割合が合計に比べて－5 ポイント以上となっており、「社内・社外を問わず、共有を行っている」は 8.8%、「社内に限り共有を行っており、社外では共有を行っていない」は 16.5%、「社内では共有を行っておらず、社外に限り共有を行っている」は 1.7%であった。

表 25 Q27 クラウドサービスを使用した営業秘密の共有や参照(業種別)

(%)

【業種別】	共有を行っている				過去には共有していたが、現在は行っていない	現在は行っていないが、将来行うことを検討している	行ったことがなく、今後の予定もない
	合計	社内・社外を問わず、共有を行っている	社内に限り共有を行っており、社外では共有を行っていない	社内では共有を行っておらず、社外に限り共有を行っている			
製造業	54.3	15.7	25.2	13.5	6.5	8.0	31.2
情報通信業	53.5	17.5	21.9	14.0	4.4	6.1	36.0
サービス業(他に分類されないもの)	46.6	17.0	19.3	10.2	1.1	15.9	36.4
小売業	37.7	9.4	15.1	13.2	0.0	5.7	56.6
専門・技術サービス業	38.8	12.2	22.4	4.1	4.1	2.0	55.1
建設業	51.4	17.1	22.9	11.4	2.9	11.4	34.3
金融業、保険業	40.0	5.7	22.9	11.4	11.4	2.9	45.7
不動産業、物品賃貸業	32.4	14.7	8.8	8.8	2.9	8.8	55.9
卸売業	51.5	12.1	36.4	3.0	12.1	9.1	27.3
医療、福祉	54.8	9.7	29.0	16.1	6.5	0.0	38.7
運輸業	50.0	17.9	21.4	10.7	3.6	0.0	46.4
教育、学習支援業	54.2	16.7	29.2	8.3	8.3	8.3	29.2
生活関連サービス業、娯楽業	43.5	4.3	30.4	8.7	13.0	0.0	43.5
その他	60.0	26.7	20.0	13.3	6.7	6.7	26.7
飲食サービス業	27.3	18.2	0.0	9.1	9.1	9.1	54.5
農林業	20.0	10.0	10.0	0.0	20.0	10.0	50.0
電気・ガス・熱供給・水道業	77.8	33.3	44.4	0.0	0.0	0.0	22.2
鉱業、採石業、砂利採取業	40.0	0.0	40.0	0.0	20.0	0.0	40.0
漁業	50.0	0.0	0.0	50.0	0.0	50.0	0.0
宿泊業	0.0	0.0	0.0	0.0	0.0	0.0	100.0

「社内・社外を問わず共有を行っている」、「社内に限り共有を行っており、社外では共有を行っていない」及び「社内では共有を行っておらず、社外に限り共有を行っている」のそれぞれの割合を業種別に比較すると、「社内に限り共有を行っており、社外では共有を行っていない」の割合が比較的高い傾向が見られ、例えば、製造業では 25.2%、情報通信業では 21.9%であった。

表 26 Q27 クラウドサービスを使用した営業秘密の共有や参照(製造業(中分類)別)

(%)

【製造業(中分類)】	共有を行っている				過去には共有していたが、現在は行っていない	現在は行っていないが、将来行うことを検討している	行ったことがなく、今後の予定もない
	合計	社内・社外を問わず、共有を行っている	社内に限り共有を行っており、社外では共有を行っていない	社内では共有を行っておらず、社外に限り共有を行っている			
非鉄金属	82.4	5.9	52.9	23.5	0.0	11.8	5.9
鉄鋼	70.6	11.8	29.4	29.4	2.9	2.9	23.5
化学	63.5	20.6	27.0	15.9	14.3	4.8	17.5
輸送用機械	60.0	20.0	20.0	20.0	9.1	9.1	21.8
電機・情報通信機械・電子部品	59.7	13.4	32.8	13.4	6.7	6.0	27.6
窯業・土石製品	53.8	23.1	7.7	23.1	0.0	7.7	38.5
食料品	51.7	20.7	19.0	12.1	3.4	1.7	43.1
汎用、生産・業務用機械	48.1	11.1	27.8	9.3	1.9	7.4	42.6
パルプ・紙・紙加工品	47.8	8.7	30.4	8.7	8.7	8.7	34.8
金属製品	47.6	11.9	28.6	7.1	4.8	26.2	21.4
プラスチック製品	44.0	28.0	8.0	8.0	8.0	8.0	40.0
繊維工業	40.0	20.0	20.0	0.0	20.0	13.3	26.7
ゴム製品	37.5	12.5	0.0	25.0	12.5	12.5	37.5
その他	37.0	17.4	17.4	2.2	4.3	8.7	50.0
家具・装備品	30.8	0.0	7.7	23.1	0.0	7.7	61.5

クラウドサービスを使用して営業秘密の共有を行っている場合について、「社内・社外を問わず共有を行っている」、「社内に限り共有を行っており、社外では共有を行っていない」及び「社内では共有を行っておらず、社外に限り共有を行っている」のそれぞれの割合を製造業(中分類)の業種ごとに比較すると、クラウドサービスを利用して営業秘密の共有を行っている割合が最も大きかったのは非鉄金属で、鉄鋼、化学がそれに次いでいた。また、「社内に限り共有を行っており、社外では共有を行っていない」の割合が比較的高い傾向が見られ、例えば非鉄金属では 52.9%、鉄鋼では 29.4%であった。

Q28 クラウドサービスにおける営業秘密に関する不正使用リスクを想定した対策として、実施しているものを選択してください。(MA)

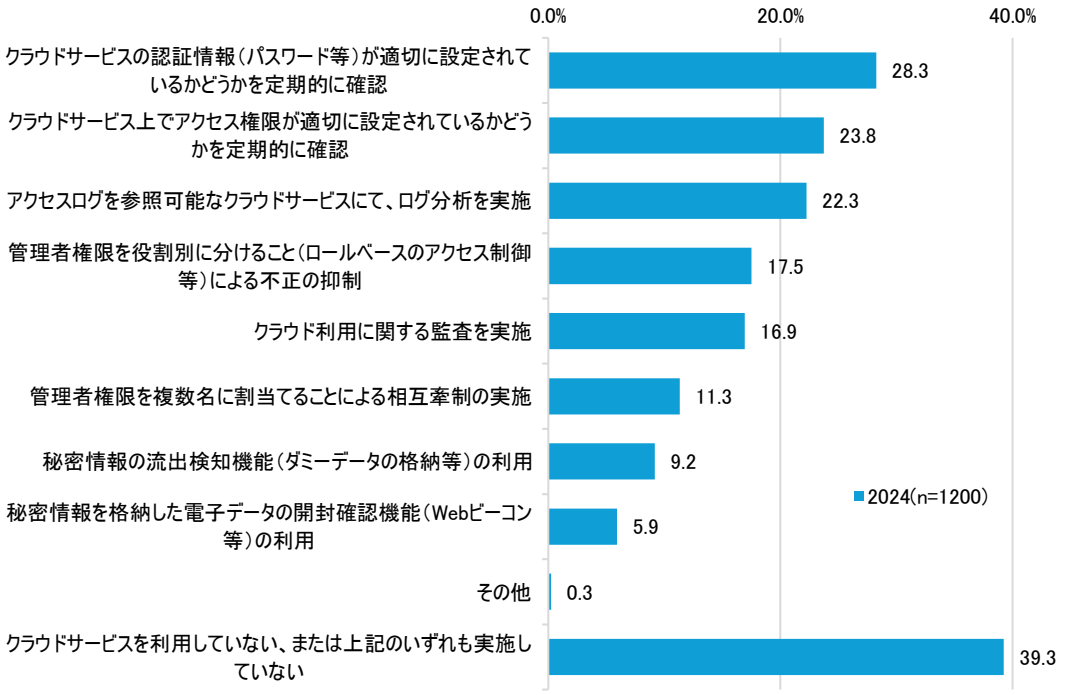


図 64 Q28 クラウドサービスにおける営業秘密の不正使用リスク対策(MA、n=1200)

クラウドサービスにおける営業秘密の不正使用リスク対策について、実施しているものとしては、「クラウドサービスの認証情報が適切に設定されているかどうかを定期的に確認」が最も高く 28.3%であった。次いで、「クラウドサービス上でアクセス権限が適切に設定されているかを定期的に確認」が 23.8%、「アクセスログを参照可能なクラウドサービスにて、ログ分析を実施」が 22.3%であった。

全体としては、「クラウドサービスを利用していない、または上記のいずれも実施していない」が最も高く 39.3%であった。

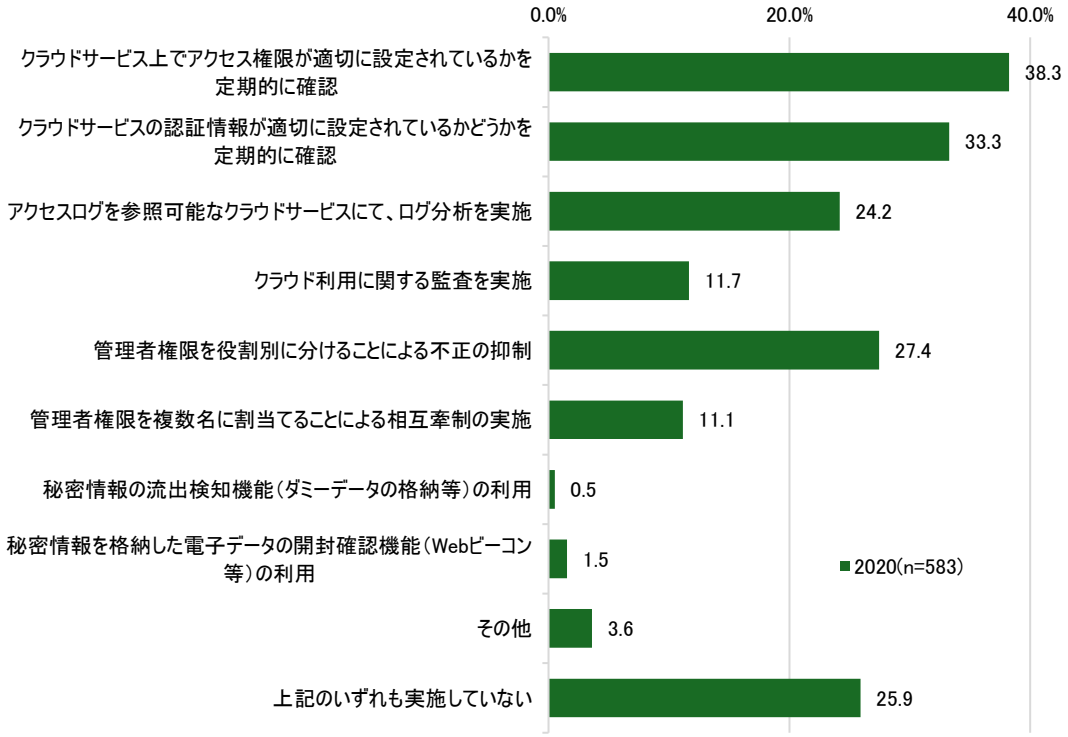


図 65 Q28（参考）クラウドサービスにおける営業秘密の不正使用リスク対策（2020 年度調査、MA、n=583）

2020 年度調査では、本調査とは異なり、回答者の中でクラウドサービスを利用している者を対象に質問しているため、単純比較はできないが、「クラウドサービスの認証情報が適切に設定されているかどうかを定期的に確認」及び「クラウドサービス上でアクセス権限が適切に設定されているかを定期的に確認」の 2 項目の割合が高い傾向は変わっていなかった。

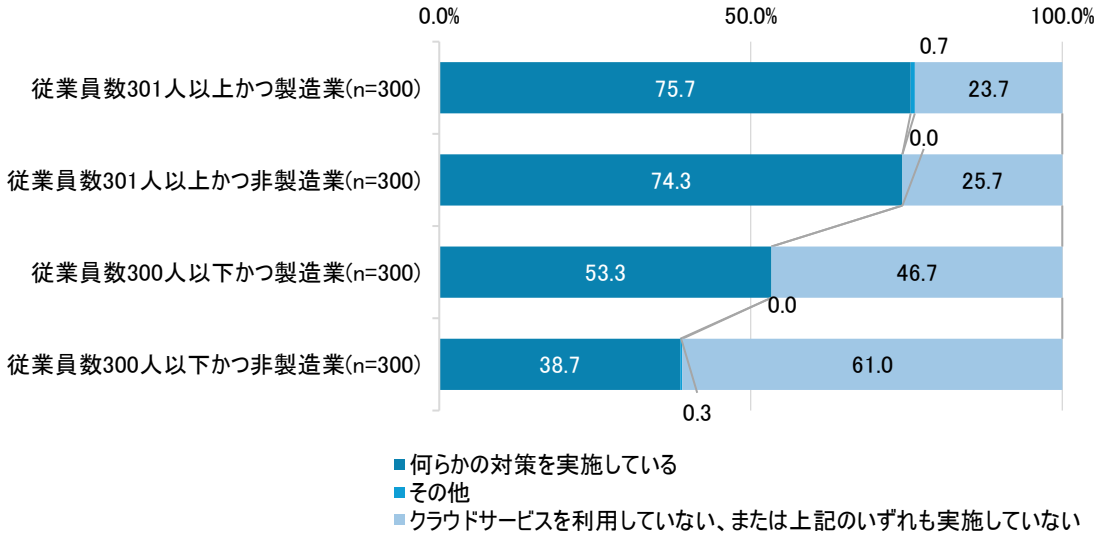


図 66 Q28 クラウドサービスにて何らかの対策を実施している割合

各対策が選択された割合に大きな差が見られず、いずれも 30%未満であったため、従業員数・業種別に、選択肢の中で「クラウドサービスの認証情報が適切に設定されているかどうかを定期的に確認」、「クラウドサービス上でアクセス権限が適切に設定されているかを定期的に確認」、「アクセスログを参照可能なクラウドサービスにて、ログ分析を実施」、「管理者権限を役割別に分けること(ロールベースのアクセス制御等)による不正の抑制」、「クラウド利用に関する監査を実施」、「管理者を複数名に割当てることによる相互牽制の実施」、「秘密情報の流出検知機能(ダミーデータの格納等)の利用」及び「秘密情報を格納した電子データの開封確認機能(Web ビーコン等)の利用」のいずれかを選択した人を「何らかの対策を実施している」人として、「何らかの対策を実施している」人、「その他」を選択した人、「クラウドサービスを利用していない、または上記のいずれも実施していない」を選択した人の数を集計した。

従業員数 301 人以上の場合、クラウドサービスの利用に関して、何らかの対策を実施している割合が 75%以上であった。一方で、従業員数 300 人以下の場合、クラウドサービスを利用しており、何らかの対策を実施している割合は製造業の方が高く 53.3%、非製造業の場合 38.7%であった。

Q29 あなたが所属する組織では、「シャドークラウド」（あなたが所属する組織のセキュリティ担当者が把握していない、個人や部署が勝手に利用しているようなクラウドサービス）が生ずることを防止する対策を講じていますか。（SA）

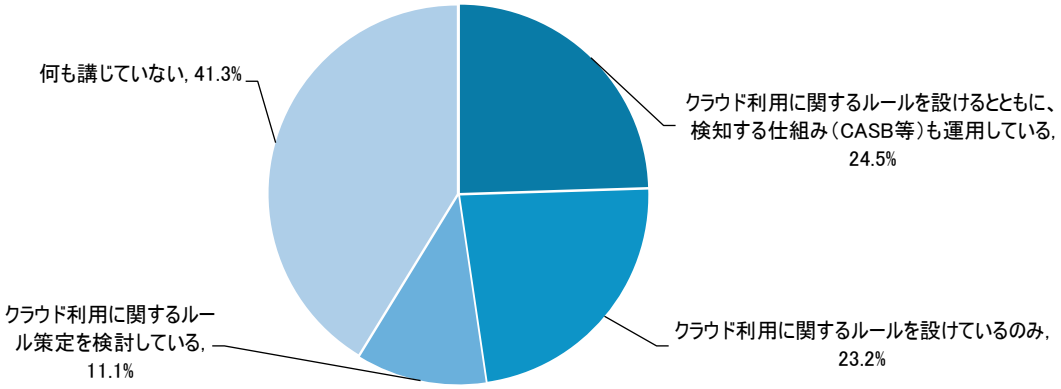


図 67 Q29 「シャドークラウド」が生ずることを防止する対策の実施状況（n=1200）

「シャドークラウド」が生ずることを防止する対策として、「クラウド利用に関するルールを設けるとともに、検知する仕組み（CASB 等）も運用している」が 24.5%であった。また、「クラウド利用に関するルールを設けるとともに、検知する仕組み（CASB 等）も運用している」と「クラウド利用に関するルールを設けているのみ」を合わせたクラウド利用に関するルールを設けている割合は 47.7%で、Q27 でクラウドを利用した秘密情報の共有を実施している割合（50.4%）と同程度となった。「クラウド利用に関するルール策定を検討している」は 11.1%であった。「何も講じていない」は 41.3%であった。

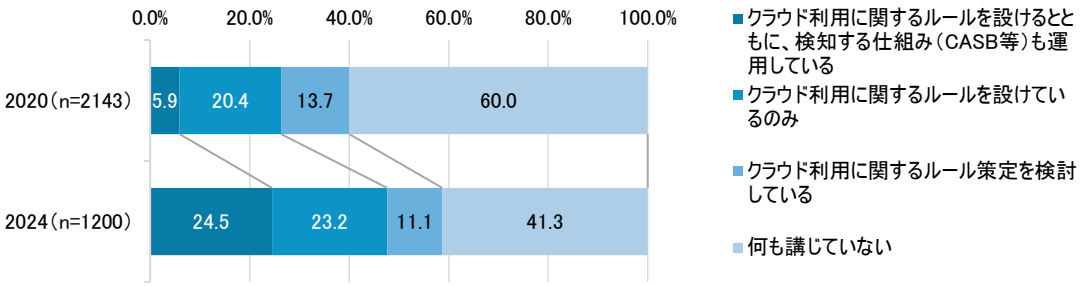


図 68 Q29 「シャドークラウド」が生ずることを防止する対策の実施状況(経年比較)

2020 年度調査と比較すると、「クラウド利用に関するルールを設けるとともに、検知する仕組み（CASB 等）も運用している」の割合は 5.9%から 24.5%に大きく増加した。「クラウド利用に関するルールを設けているのみ」の割合は 20.4%から 23.2%と微増し、「クラウド利用に関するルール策定を検討している」は 13.7%から 11.1%に微減した。「何も講じていない」は 60.0%から 41.3%に大きく減少した。

表 27 Q29 「シャドークラウド」が生ずることを防止する対策を講じているか
（業種、従業員数、売上高、所属部門別）

（%）

		クラウド利用に関するルールを設けるとともに、検知する仕組み（CASB 等）も運用している	クラウド利用に関するルールを設けているのみ	クラウド利用に関するルール策定を検討している	何も講じていない
合計		24.5	23.2	11.1	41.3
業種	製造業	29.0	24.0	11.8	35.2
	非製造業	20.0	22.3	10.3	47.3
従業員数	301 人以上	35.0	28.5	10.8	25.7
	300 人以下	14.0	17.8	11.3	56.8
従業員数・業種	従業員数 301 人以上かつ製造業	41.0	28.0	9.7	21.3
	従業員数 300 人以下かつ製造業	17.0	20.0	14.0	49.0
	従業員数 301 人以上かつ非製造業	29.0	29.0	12.0	30.0
	従業員数 300 人以下かつ非製造業	11.0	15.7	8.7	64.7
売上高	10 億円以下	7.5	15.4	9.8	67.4
	10 億円超～100 億円以下	27.7	20.8	13.8	37.7
	100 億円超～1,000 億円以下	27.5	33.0	13.9	25.6
	1,000 億円超～5,000 億円以下	36.8	32.1	7.5	23.6
	5,000 億円超	45.9	23.3	7.6	23.3
所属部門	企業における情報システム関連部門	33.1	24.3	9.7	32.8
	企業のリスクマネジメント計画・実践に関わる部門	39.2	30.4	9.5	20.9
	企業のサイバーセキュリティに関わる部門	36.7	43.0	11.4	8.9
	経営企画部門	21.6	21.6	16.0	40.8
	経営層	6.4	11.4	10.1	72.1
	その他セキュリティやリスクマネジメントに関する業務	23.4	29.0	10.5	37.1

業種、従業員数、売上高、所属部門別に集計したところ、従業員数・業種別では、「クラウド利用に関するルールを設けるとともに、検知する仕組み（CASB 等）も運用している」の割合が合計の割合＋10 ポイント以上であったのは従業員数 301 人以上かつ製造業の場合で 41.0%であった。また合計の割合－10 ポイント以上であったのは従業員数 300 人以下かつ非製造業の場合で 11.0%であった。また「クラウド利用に関するルールを設けているのみ」の割合が合計の割合＋5 ポイント以上であったのは従業員数 300 人以下かつ製造業の場合で 29.0%であった。「何も講じていない」の割合が大きく合計の割合＋10 ポイント以上であったのは従業員数 300 人以下かつ非製造業の場合で 64.7%であった。

売上高別では、「クラウド利用に関するルールを設けるとともに、検知する仕組み（CASB 等）も運用している」の割合が合計の割合＋10 ポイント以上であったのは 1000 億円超～5000 億円以下と 5000 億円超の 2 区分で前者は 36.8%、後者は 45.9%であった。また、「クラウド利用に関するルールを設けているのみ」の割合が合計の割合＋5 ポイント以上であったのは 100 億円超～1000 億円以下と 1000 億円超～5000 億円以下の 2 区分で、前者は 33.0%、後者は 32.1%であった。

所属部門別では、「クラウド利用に関するルールを設けるとともに、検知する仕組み（CASB 等）も運用している」の割合が合計の割合＋10 ポイント以上であったのは企業のリスクマネジメント計画・実践に関わる部門と企業のサイバーセキュリティに関わる部門の 2 部門で、前者は 39.2%、後者は 36.7%であった。「クラウド利用に関するルールを設けているのみ」の割合が合計の割合＋5 ポイント以上であったのは企業におけるサイバーセキュリティに関わる部門と企業のリスクマネジメント計画・実践に関わる部門で前者は 43.0%、後者は 30.4%であった。経営層は「何も講じていない」とする割合が高く、合計の割合＋10 ポイント以上で 72.1%であった。

Q30 近年、生成 AI の技術が急速に発展し、情報検索から画像編集に至るまで、さまざま分野で活用が進んでいます。生成 AI を業務に利用する際、秘密情報を誤って生成 AI に入力してしまう可能性が想定されます。あなたが所属する組織における生成 AI の業務利用について、秘密情報を保護する観点でどのような対策を行っていますか。(SA)

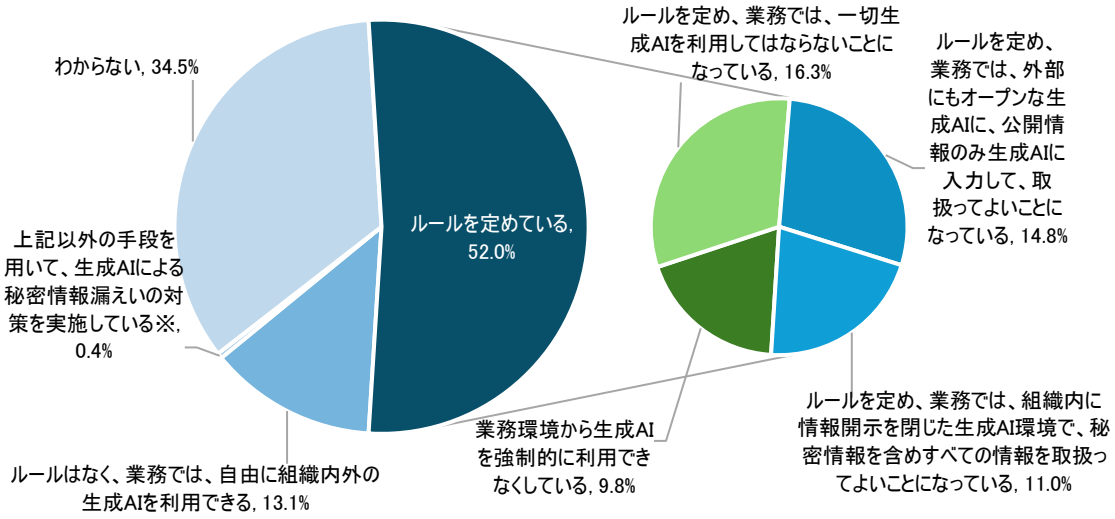


図 69 Q30 生成 AI の業務利用に関してルールを定めている割合(n=1200)

生成 AI の利用に関してルールを定めている割合は 52.0%であった。他方で、「ルールはなく、業務では、自由に組織内外の生成 AI を利用できる」の割合は 13.1%であった。ルールを定めている 52.0%のうち、「外部にもオープンな生成 AI に、公開情報のみ生成 AI に入力して、取扱ってよいことになっている」のは 14.8%、「組織内に情報開示を閉じた生成 AI 環境で、秘密情報を含めすべての情報を取扱ってよいことになっている」は 11.0%、「一切生成 AI を利用してはならないことになっている」は 16.3%、「業務環境から生成 AI を強制的に利用できなくしている」は 9.8%であった。

なお、「上記以外の手段を用いて、生成 AI による秘密情報の漏えいの対策を実施している」については、利用が無い旨の回答や、業務情報の種別から生成 AI で扱う対象ではない等の記述があった。

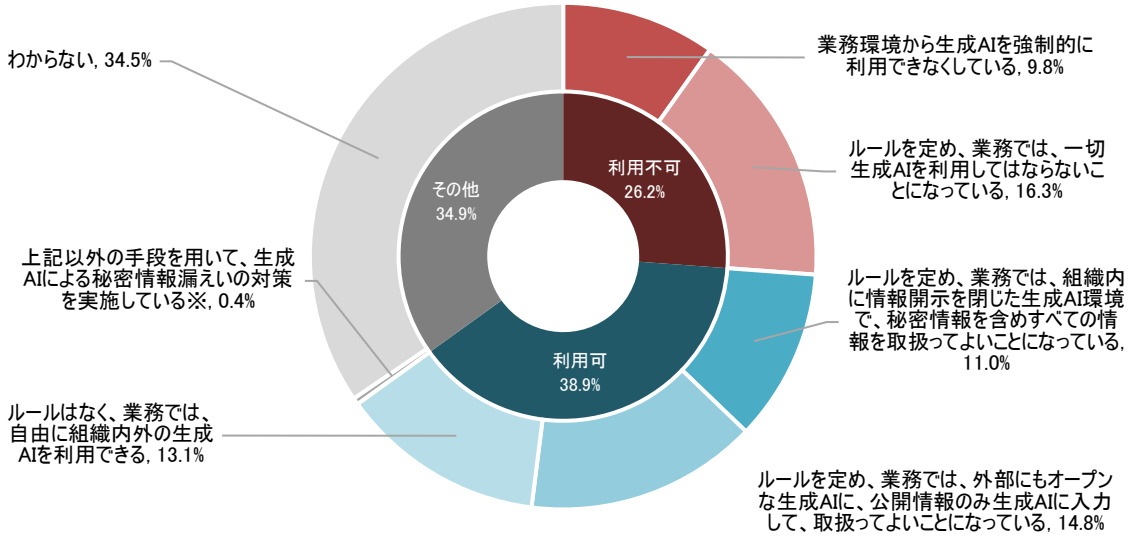


図 70 Q30 生成 AI の業務利用可否と取扱い可能な情報の種別（n=1200）

生成 AI を業務において利用できないという選択肢を選んだのは全体の 26.2%で、内訳としては「業務環境から生成 AI を強制的に利用できなくしている」は 9.8%、「ルールを定め、業務では、一切生成 AI を利用してはならないことになっている」は 16.3%であった。

また、生成 AI を業務において利用できるという選択肢を選んだのは全体の 38.9%で、そのうち「ルールを定め、業務では、組織内に情報開示を閉じた生成 AI 環境で、秘密情報を含めすべての情報を取扱ってよいことになっている」を選択したのは 11.0%であった。

表 28 Q30 生成 AI の業務利用について秘密情報保護の観点で実施している対策 (業種、従業員数、売上高、所属部門別)

(%)

		業務環境から生成 AI を強制的に利用できなくしている	ルールを定め、業務では、一切生成 AI を利用してはならないことになっている	ルールを定め、業務では、外部にもオープンな生成 AI に、公開情報のみ生成 AI に入力して、取扱ってよいことになっている	ルールを定め、業務では、組織内に情報開示を閉じた生成 AI 環境で、秘密情報を含めすべての情報を取扱ってよいことになっている	ルールはなく、業務では、自由に組織内外の生成 AI を利用できる	上記以外の手段を用いて、生成 AI による秘密情報漏えいの対策を実施している	わからない
合計		9.8	16.3	14.8	11.0	13.1	0.4	34.5
業種	製造業	10.5	16.7	16.5	13.7	11.5	0.3	30.8
	非製造業	9.2	16.0	13.2	8.3	14.7	0.5	38.2
従業員数	301 人以上	12.2	19.5	19.0	15.3	8.2	−	25.8
	300 人以下	7.5	13.2	10.7	6.7	18.0	0.8	43.2
従業員数・業種	従業員数 301 人以上かつ製造業	12.3	18.7	19.0	17.7	9.0	−	23.3
	従業員数 300 人以下かつ製造業	8.7	14.7	14.0	9.7	14.0	0.7	38.3
	従業員数 301 人以上かつ非製造業	12.0	20.3	19.0	13.0	7.3	−	28.3
	従業員数 300 人以下かつ非製造業	6.3	11.7	7.3	3.7	22.0	1.0	48.0
売上高	10 億円以下	5.1	10.8	6.7	5.4	20.8	1.0	50.1
	10 億円超～100 億円以下	12.7	17.7	17.7	10.0	10.8	0.4	30.8
	100 億円超～1,000 億円以下	9.5	21.2	19.4	16.1	9.5	−	24.2
	1,000 億円超～5,000 億円以下	10.4	22.6	22.6	11.3	9.4	−	23.6
	5,000 億円超	16.3	15.1	16.9	16.9	7.0	−	27.9
所属部門	企業における情報システム関連部門	11.6	16.4	15.5	15.8	9.1	−	31.6
	企業のリスクマネジメント計画・実践に関わる部門	13.9	29.1	20.9	14.6	4.4	0.6	16.5
	企業のサイバーセキュリティに関わる部門	16.5	31.6	19.0	15.2	7.6	−	10.1
	経営企画部門	9.4	13.6	12.7	9.9	14.6	−	39.9
	経営層	6.4	7.4	8.4	4.4	21.5	1.3	50.5
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	4.8	16.1	21.8	8.9	15.3	−	33.1

業種、従業員数、売上高、所属部門別に集計したところ、従業員数・業種別では、従業員数 301 人以上または製造業である方が「わからない」の割合が少なく、従業員数 301 人以上かつ製造業の場合は合計の割合－10 ポイント以上で 23.3%、従業員数 301 人以上かつ非製造業の場合は合計の割合－5 ポイント以上で 28.3%であった。従業員数 300 人以下かつ非製造業の場合は合計の割合＋10 ポイント以上の 48.0%であった。

また、「ルールはなく、業務では自由に組織内外の生成 AI を利用できる」の割合別では、合計の割合＋5 ポイント以上となったのは、従業員数・業種別では 300 人以下かつ非製造業である場合で 22.0%、売上高別では、10 億円以下の場合で 20.8%であった。

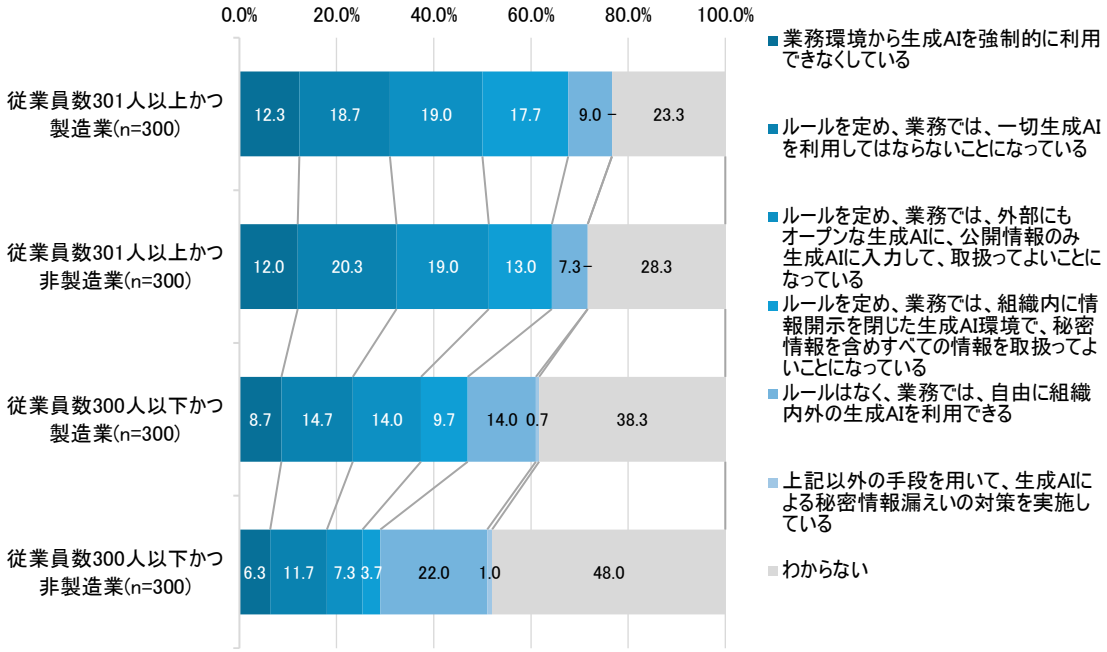


図 71 Q30 生成 AI の業務利用について秘密情報保護の観点で実施している対策 (従業員数・業種別)

従業員数・業種別では、「わからない」の割合は、従業員数 301 人以上かつ製造業の場合が最も少なく 23.3%、従業員数 301 人以上かつ非製造業の場合は 28.3%であった。従業員数 300 人以下かつ非製造業の場合は最も高く 48.0%であった。

「ルールはなく、業務では自由に組織内外の生成 AI を利用できる」の割合別では、従業員数 300 人以下かつ非製造業である場合で最も高く 22.0%であった。

「業務環境から生成 AI を強制的に利用できなくしている」の割合については、従業員数 301 人以上の場合、製造業は非製造業よりも割合が大きく 12.3%、非製造業の場合は 12.0%と、従業員数 301 人以上の場合、10.0%を上回った。一方で従業員数 300 人以下の場合は 10%を下回っており、製造業の場合 8.7%、非製造業の場合 6.3%であった。

「ルールを定め、業務では、一切生成 AI を利用してはならないことになっている」の割合は、従業員数 301 人以上の場合、製造業の方が非製造業よりも割合がやや小さく 18.7%、非製造業は 20.3%であった。従業員数 300 人以下の場合、製造業では 14.7%、非製造業では 11.7%であった。

「ルールを定め、業務では、外部にもオープンな生成 AI に、公開情報のみ生成 AI に入力して取扱ってよいことになっている」の割合は、従業員数 301 人以上の場合、製造業、非製造業ともに 19.0%、従業員数 300 人以下の場合、製造業では 14.0%、非製造業では 7.3%であった。

「ルールを定め、業務では、組織内に情報開示を閉じた生成 AI 環境で、秘密情報を含めすべての情報を取扱ってよいことになっている」については、従業員数 301 人以上の場合、製造業では 17.7%、非製造業では 13.0%、従業員数 300 人以下の場合、製造業では 8.7%、非製造業では 3.7%であった。

表 29 Q30 生成 AI の業務利用について秘密情報保護の観点で実施している対策(業種別)

(%)

【業種別】	生成 AI の利用に関して何らかが定められている					ルールはなく、業務では、自由に組織内外の生成 AI を利用できる	上記以外の手段を用いて、生成 AI による秘密情報漏えいの対策を実施している	わからない
	合計	業務環境から生成 AI を強制的に利用できなくしている	ルールを定め、業務では、一切生成 AI を利用してはならないことになっている	ルールを定め、業務では、外部にもオープンな生成 AI に、公開情報のみ生成 AI に入力して、取扱ってよいことになっている	ルールを定め、業務では、組織内に情報開示を閉じた生成 AI 環境で、秘密情報を含めすべての情報を取扱ってよいことになっている			
製造業	57.3	10.5	16.7	16.5	13.7	11.5	0.3	30.8
情報通信業	60.5	11.4	17.5	19.3	12.3	7.9	0.0	31.6
サービス業(他に分類されないもの)	44.3	8.0	14.8	14.8	6.8	13.6	1.1	40.9
小売業	32.1	5.7	17.0	3.8	5.7	15.1	0.0	52.8
専門・技術サービス業	28.6	4.1	6.1	10.2	8.2	22.4	2.0	46.9
建設業	40.0	2.9	14.3	8.6	14.3	2.9	2.9	54.3
金融業、保険業	48.6	14.3	14.3	8.6	11.4	17.1	0.0	34.3
不動産業、物品賃貸業	29.4	8.8	11.8	5.9	2.9	23.5	0.0	47.1
卸売業	45.5	12.1	15.2	15.2	3.0	27.3	0.0	27.3
医療、福祉	54.8	6.5	22.6	9.7	16.1	16.1	0.0	29.0
運輸業	50.0	10.7	21.4	10.7	7.1	14.3	0.0	35.7
教育、学習支援業	62.5	16.7	16.7	29.2	0.0	16.7	0.0	20.8
生活関連サービス業、娯楽業	43.5	8.7	17.4	17.4	0.0	13.0	0.0	43.5
その他	53.3	13.3	13.3	20.0	6.7	33.3	0.0	13.3
飲食サービス業	36.4	9.1	9.1	9.1	9.1	0.0	0.0	63.6
農林業	40.0	10.0	20.0	0.0	10.0	30.0	0.0	30.0
電気・ガス・熱供給・水道業	88.9	11.1	55.6	11.1	11.1	0.0	0.0	11.1
鉱業、採石業、砂利採取業	60.0	20.0	0.0	40.0	0.0	0.0	0.0	40.0
漁業	100.0	0.0	50.0	0.0	50.0	0.0	0.0	0.0
宿泊業	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0

業種別の集計では、特定の業種に顕著な傾向はみられなかった。

生成 AI の利用に関して何らかが定められている割合として、「業務環境から生成 AI を強制的に利用できなくしている」、「ルールを定め、業務では、一切生成 AI を利用してはならないことになっている」、「ルールを定め、業務では、外部にもオープンな生成 AI に公開情報のみ生成 AI に入力して、取扱ってよいことになっている」、「ルールを定め、業務では、組織内に情報開示を閉じた生成 AI 環境で、秘密情報を含めすべての情報を取扱ってよいことになっている」の 4 項目の割合を合計した値を出した。回答人数が 100 人以上の業種別では、この値は、製造業では 57.3%、情報通信業では 60.5%であった。

表 30 Q30 生成 AI の業務利用について秘密情報保護の観点で実施している対策 (製造業(中分類)別)

(%)

【製造業(中分類)】	生成 AI の利用に関して何らかが定められている					ルールはなく、業務では、自由に組織内外の生成 AI を利用できる	上記以外の手段を用いて、生成 AI による秘密情報漏えいの対策を実施している	わからない
	合計	業務環境から生成 AI を強制的に利用できなくしている	ルールを定め、業務では、一切生成 AI を利用してはならないことになっている	ルールを定め、業務では、外部にもオープンな生成 AI に、公開情報のみ生成 AI に入力して、取扱ってよいことになっている	ルールを定め、業務では、組織内に情報開示を閉じた生成 AI 環境で、秘密情報を含めすべての情報を取扱ってよいことになっている			
化学	74.6	7.9	27.0	22.2	17.5	1.6	0.0	23.8
鉄鋼	67.6	17.6	29.4	11.8	8.8	8.8	0.0	23.5
電機・情報通信機械・電子部品	64.2	9.7	21.6	15.7	17.2	3.7	0.0	32.1
繊維工業	60.0	20.0	6.7	13.3	20.0	13.3	0.0	26.7
非鉄金属	58.8	5.9	17.6	11.8	23.5	17.6	0.0	23.5
汎用、生産・業務用機械	57.4	13.0	16.7	16.7	11.1	16.7	0.0	25.9
パルプ・紙・紙加工品	56.5	17.4	4.3	4.3	30.4	13.0	4.3	26.1
輸送用機械	54.5	10.9	10.9	20.0	12.7	14.5	0.0	30.9
食料品	53.4	8.6	15.5	13.8	15.5	15.5	0.0	31.0
ゴム製品	50.0	25.0	0.0	25.0	0.0	0.0	0.0	50.0
金属製品	47.6	4.8	7.1	28.6	7.1	19.0	0.0	33.3
プラスチック製品	44.0	16.0	0.0	16.0	12.0	32.0	0.0	24.0
その他	41.3	4.3	13.0	19.6	4.3	21.7	2.2	34.8
窯業・土石製品	38.5	15.4	15.4	0.0	7.7	0.0	0.0	61.5
家具・装備品	38.5	7.7	30.8	0.0	0.0	0.0	0.0	61.5

製造業(中分類)別の集計では、特定の業種に顕著な傾向はみられなかった。

生成 AI の利用に関して何らかが定められている割合が最も高かったのは化学で 74.6%、鉄鋼では 67.6%、電機・情報通信機械・電子部品では 64.2%であった。

Q35 テレワーク（在宅勤務等）の環境で営業秘密を扱う場合のルールの具体的内容として、あてはまるものを選択してください。（MA）

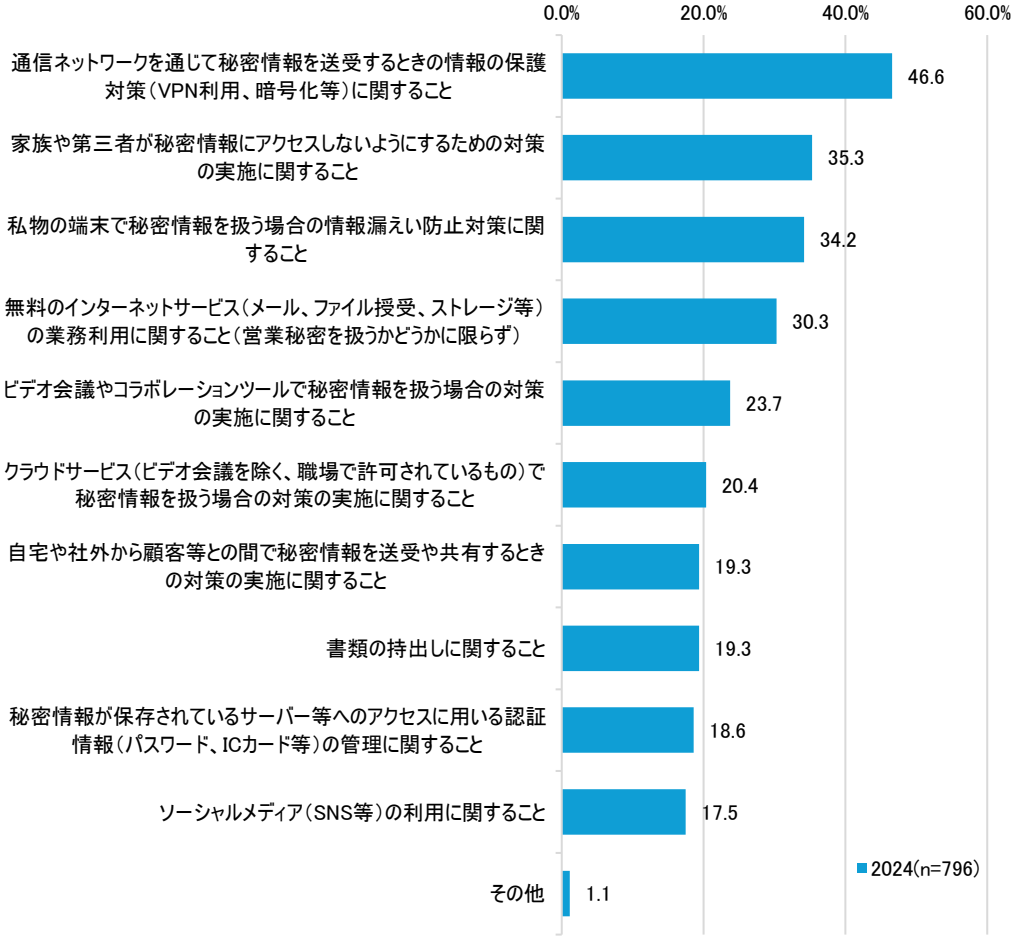


図 72 Q35 テレワーク環境で営業秘密を扱う場合のルール (MA、n=1200)

テレワーク環境で営業秘密を扱う場合のルールについて、「テレワークにおける情報管理のルールはない」が最も高く 33.7%であった。

テレワーク（在宅勤務等）の環境で営業秘密を扱う場合のルールの具体的内容として最も割合が高かったのは「通信ネットワークを通じて秘密情報を送受信する際の情報の保護対策（VPN、暗号化など）」で、30.9%であった。次いで、「家族や第三者が秘密情報にアクセスしないようにするための対策の実施に関すること」が 23.4%、「私物の端末で秘密情報を扱う場合の情報漏えい防止対策に関すること」が 22.7%であった。

「その他」は、テレワークを実施していない旨の回答か「わからない」というもののみであった。

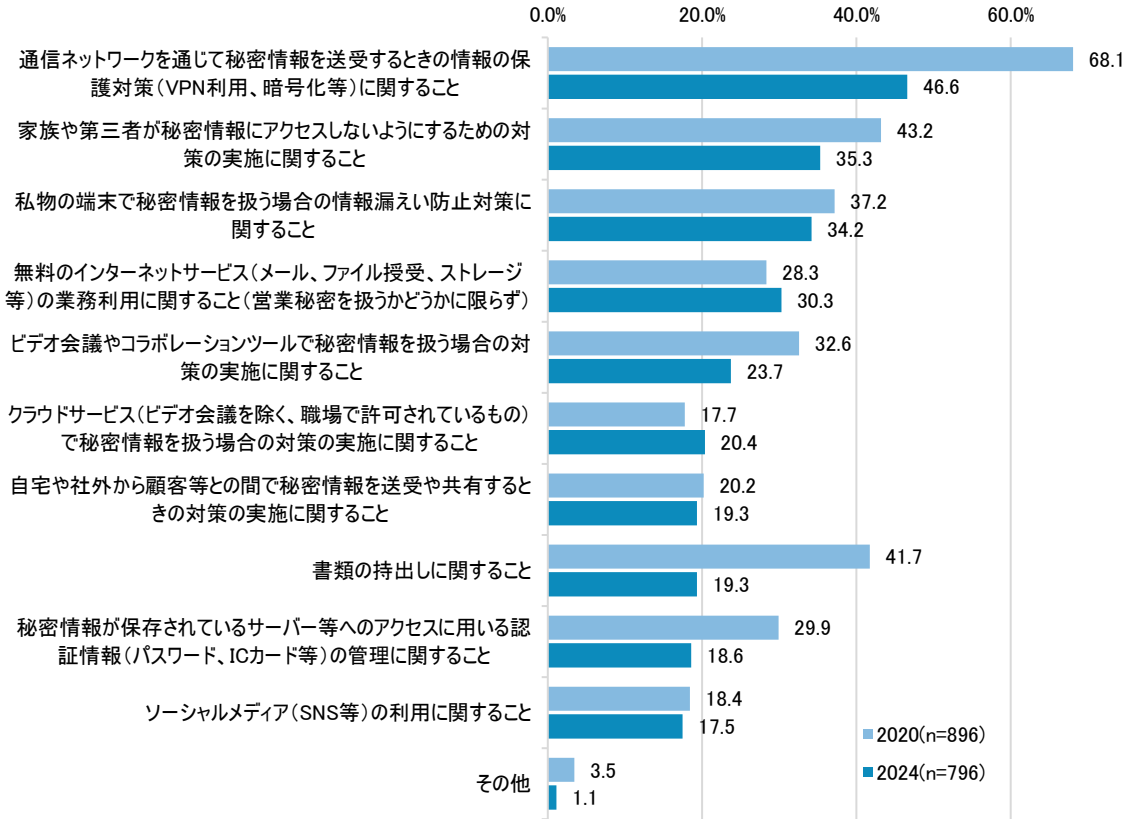


図 73 Q35 テレワーク環境で営業秘密を扱う場合のルール (MA、経年比較)

「テレワークにおける情報管理のルールはない」は 2024 年度調査独自の項目かつ排他のため、これを除いて、2020 年度調査と比較した。

「無料のインターネットサービス（メール、ファイル送受信、ストレージ等の業務利用に関すること）」は 28.3%から 20.1%、「クラウドサービスやビデオ会議、顧客に許可されているもので秘密情報を扱う場合の対策の実施に関すること」は 17.7%から 13.5%と、この 2 項目のみ微増した。

「通信ネットワークを通じて秘密情報を送受信する際の情報の保護対策（VPN、暗号化など）」は 2020 年度調査でも最も割合が大きかったが、比較すると減少しており、68.1%から 46.6%となった。「家族や第三者が秘密情報にアクセスしないようにするための対策の実施に関すること」は 43.2%から 35.3%に、「私物の端末で秘密情報を扱う場合の情報漏えい防止対策に関すること」は 37.2%から 34.2%に減少した。また、「ビデオ会議やコラボレーションツールで秘密情報を扱う場合の対策の実施に関すること」は 32.6%から 23.7%に、「自宅や外出先の電車や喫茶店等で秘密情報を送受信や共有するための対策の実施に関すること」は 20.2%から 19.3%に、「資料の持ち出しに関すること」については 41.7%から 19.3%に大きく減少した。「秘密情報が保存されているサーバー等へのアクセスに関し認証情報やパスワード等の管理に関すること」は 29.9%から 18.6%に、「ソーシャルメディア（SNS 等）の利用に関すること」は 18.4%から 17.5%に減少した。

Q31 営業秘密を含む技術情報や物品の海外への持ち出しに際しては、不正競争防止法に加え、外国為替及び外国貿易法（外為法）が定めるリスト規制やキャッチオール規制等にも対応する必要があります。外為法を遵守するための社内の輸出管理体制は整備されていますか。（SA）

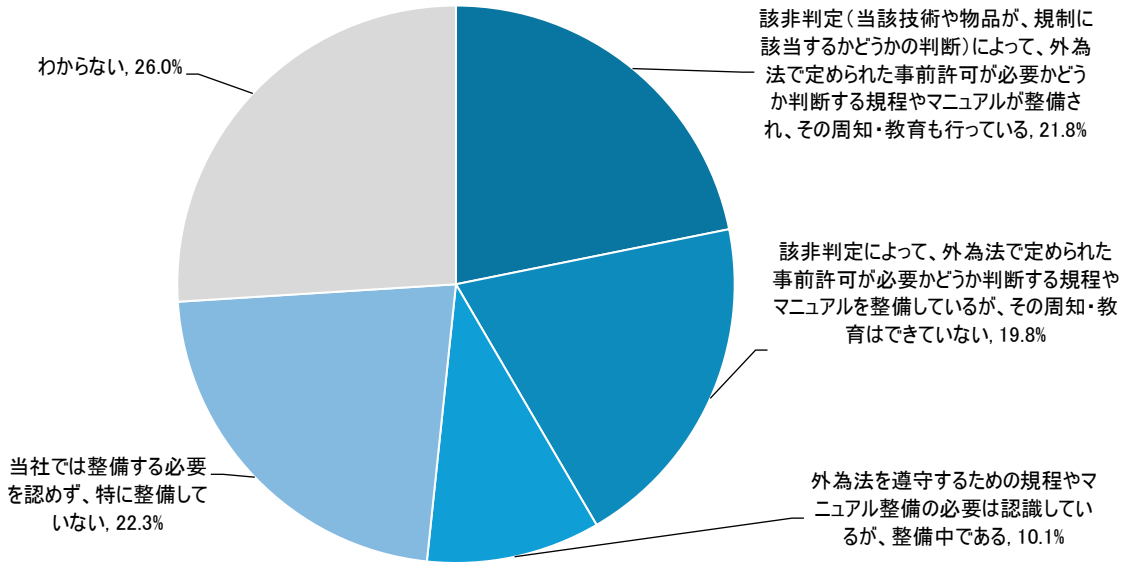


図 74 Q31 外為法を遵守するための社内の輸出管理体制の整備状況(n=1200)

外為法を遵守するための社内の輸出管理体制の整備状況について、最も割合が大きかったのは「わからない」で 26.0%であり、次いで外為法を遵守するための社内の輸出管理体制について「当社では整備する必要を認めず、特に整備していない」が大きく、22.3%であった。

また、「該非判定によって、外為法で定められた事前許可が必要かどうか判断する規程やマニュアルが整備され、その周知・教育も行っている」は 21.8%、「該非判定によって、外為法で定められた事前許可が必要かどうか判断する規程やマニュアルを整備しているが、その周知・教育は行っていない」が 19.8%であった。「外為法を遵守するための規程やマニュアルの整備の必要性は認識しているが、整備中である」は 10.1%であった。

表 31 Q31 外為法を遵守するための社内の輸出管理体制の整備状況
(業種、従業員数、売上高、所属部門別)

(%)

		該非判定(当該技術や物品が、規制に該当するかどうかの判断)によって、外為法で定められた事前許可が必要かどうか判断する規程やマニュアルが整備され、その周知・教育も行っている	該非判定によって、外為法で定められた事前許可が必要かどうか判断する規程やマニュアルを整備しているが、その周知・教育はできていない	外為法を遵守するための規程やマニュアル整備の必要は認識しているが、整備中である	当社では整備する必要を認めず、特に整備していない	わからない
合計		21.8	19.8	10.1	22.3	26.0
業種	製造業	25.7	23.0	11.2	18.7	21.5
	非製造業	18.0	16.5	9.0	26.0	30.5
従業員数	301 人以上	31.8	24.5	11.8	7.7	24.2
	300 人以下	11.8	15.0	8.3	37.0	27.8
従業員数・業種	従業員数 301 人以上かつ製造業	37.0	26.7	10.3	8.0	18.0
	従業員数 300 人以下かつ製造業	14.3	19.3	12.0	29.3	25.0
	従業員数 301 人以上かつ非製造業	26.7	22.3	13.3	7.3	30.3
	従業員数 300 人以下かつ非製造業	9.3	10.7	4.7	44.7	30.7
売上高	10 億円以下	8.7	9.8	8.0	42.9	30.6
	10 億円超～100 億円以下	19.6	21.9	10.4	21.5	26.5
	100 億円超～1,000 億円以下	24.5	28.6	12.8	12.1	22.0
	1,000 億円超～5,000 億円以下	34.0	30.2	11.3	4.7	19.8
	5,000 億円超	43.0	18.6	9.3	4.1	25.0
所属部門	企業における情報システム関連部門	28.9	20.7	7.6	11.9	31.0
	企業のリスクマネジメント計画・実践に関わる部門	34.8	35.4	11.4	6.3	12.0
	企業のサイバーセキュリティに関わる部門	32.9	39.2	13.9	1.3	12.7
	経営企画部門	18.8	15.0	15.0	22.5	28.6
	経営層	7.1	6.4	7.1	50.8	28.6
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	20.2	25.0	11.3	15.3	28.2

業種、従業員数、売上高、所属部門別に集計したところ、従業員数別では、300 人以下の企業の場合、「当社では整備する必要を認めず、特に整備していない」の割合が高く、合計に比べて＋10 ポイント以上で 37.0%であった。

従業員数・業種別では、「該非判定(当該技術や物品が、規制に該当するかどうかの判断)によって、外為法で定められた事前許可が必要かどうか判断する規程やマニュアルが整備され、その周知・教育も行っている」の割合は、従業員数 301 人以上かつ製造業の場合に、合計に比べて+10 ポイント以上で、37.0%、従業員数 300 人以下かつ非製造業の場合に合計に比べて－10 ポイント以上で、9.3%であった。

売上高別では、1000 億円超～5000 億円以下及び 5000 億円超の場合、該非判定によって、外為法で定められた事前許可が必要かどうか判断する規程やマニュアルを整備している割合が大きい傾向にあり、「該非判定(当該技術や物品が、規制に該当するかどうかの判断)によって、外為法で定められた事前許可が必要かどうか判断する規程やマニュアルが整備され、その周知・教育も行っている」は 1000 億円超～5000 億円以下では 34.0%、5000 億円超では 43.0%、「該非判定(当該技術や物品が、規制に該当するかどうかの判断)によって、外為法で定められた事前許可が必要かどうか判断する規程やマニュアルが整備しているが、その周知・教育はできていない」は 1000 億円超～5000 億円以下では 30.2%であった。

表 32 Q31 外為法を遵守するための社内の輸出管理体制の整備状況
(業種別、従業員数 300 人以下)

(%)

【業種別(大分類)300 人以下】	輸出管理体制の整備が必要だと認識			当社では整備する必要を認めず、特に整備していない	わからない
	該非判定(当該技術や物品が、規制に該当するかどうかの判断)によって、外為法で定められた事前許可が必要かどうか判断する規程やマニュアルが整備され、その周知・教育も行っている	該非判定によって、外為法で定められた事前許可が必要かどうか判断する規程やマニュアルを整備しているが、その周知・教育はできていない	外為法を遵守するための規程やマニュアル整備の必要は認識しているが、整備中である		
製造業	14.3	19.3	12.0	29.3	25.0
サービス業(他に分類されないもの)	5.9	19.6	2.0	45.1	27.5
情報通信業	18.4	10.5	5.3	34.2	31.6
小売業	0.0	3.3	6.7	66.7	23.3
専門・技術サービス業	3.4	3.4	0.0	62.1	31.0
不動産業、物品賃貸業	4.3	4.3	0.0	43.5	47.8
建設業	4.8	9.5	9.5	57.1	19.0
医療、福祉	16.7	11.1	16.7	22.2	33.3
卸売業	6.3	12.5	6.3	37.5	37.5
生活関連サービス業、娯楽業	6.7	6.7	0.0	40.0	46.7
金融業、保険業	18.2	0.0	0.0	54.5	27.3
教育、学習支援業	27.3	0.0	9.1	54.5	9.1
飲食サービス業	20.0	20.0	0.0	20.0	40.0
運輸業	22.2	11.1	0.0	22.2	44.4
農林業	0.0	25.0	12.5	25.0	37.5
電気・ガス・熱供給・水道業	50.0	50.0	0.0	0.0	0.0
鉱業、採石業、砂利採取業	0.0	0.0	0.0	100.0	0.0
漁業	–	–	–	–	–
宿泊業	–	–	–	–	–
その他	0.0	28.6	14.3	42.9	14.3

従業員数 300 人以下の場合について、業種別に各選択肢の選択割合を比較したところ、「当社では整備する必要を認めず、特に整備していない」の割合と、「わからない」と回答した割合が全体的に大きい傾向にあった。例えば、製造業では「当社では整備する必要を認めず、特に整備していない」の割合は 29.3%、「わからない」の割合は 25.0%であった。

表 33 Q31 外為法を遵守するための社内の輸出管理体制の整備状況
(製造業(中分類))別、従業員数 300 人以下)

(%)

【製造業(中分類)】	輸出管理体制の整備が必要だと認識			当社では整備する必要を認めず、特に整備していない	わからない
	該非判定(当該技術や物品が、規制に該当するかどうかの判断)によって、外為法で定められた事前許可が必要かどうか判断する規程やマニュアルが整備され、その周知・教育も行っている	該非判定によって、外為法で定められた事前許可が必要かどうか判断する規程やマニュアルを整備しているが、その周知・教育はできていない	外為法を遵守するための規程やマニュアル整備の必要は認識しているが、整備中である		
パルプ・紙・紙加工品	28.6	14.3	0.0	50.0	7.1
非鉄金属	11.1	44.4	0.0	44.4	0.0
輸送用機械	10.5	5.3	5.3	42.1	36.8
金属製品	3.1	12.5	21.9	34.4	28.1
汎用、生産・業務用機械	13.0	13.0	26.1	30.4	17.4
化学	8.7	17.4	4.3	26.1	43.5
ゴム製品	12.5	37.5	0.0	25.0	25.0
プラスチック製品	16.7	16.7	8.3	25.0	33.3
繊維工業	0.0	33.3	11.1	22.2	33.3
電機・情報通信機械・電子部品	25.9	18.5	14.8	20.4	20.4
食料品	25.0	28.1	6.3	18.8	21.9
鉄鋼	16.7	38.9	16.7	16.7	11.1
窯業・土石製品	12.5	12.5	25.0	12.5	37.5
家具・装備品	0.0	22.2	0.0	11.1	66.7
その他	3.3	10.0	13.3	53.3	20.0

従業員数 300 人以下の場合において、製造業(中分類)別で見ると、パルプ・紙・紙加工品、輸送用機械、金属製品、汎用、生産・業務用機械で「当社では整備する必要を認めず、特に整備していない」の割合が比較的大きく、30%以上であった。

また、「該非判定によって、外為法で定められた事前許可が必要かどうか判断する規程やマニュアルを整備しているが、その周知・教育はできていない」と回答した割合の大きい業種もあり、それは、非鉄金属、ゴム製品、繊維工業、食料品、鉄鋼の 5 業種であった。

電機・情報通信機械・電子部品については従業員数 300 人以下であっても、「該非判定によって、外為法で定められた事前許可が必要かどうか判断する規程やマニュアルが整備され、その周知・教育も行っている」の割合が比較的高く、25.9%であった。

Q32 メール等による情報のやり取りを含め、海外の拠点や取引先に対して秘密情報の提供等を行う際、他国の法令について配慮することはありますか。(MA)

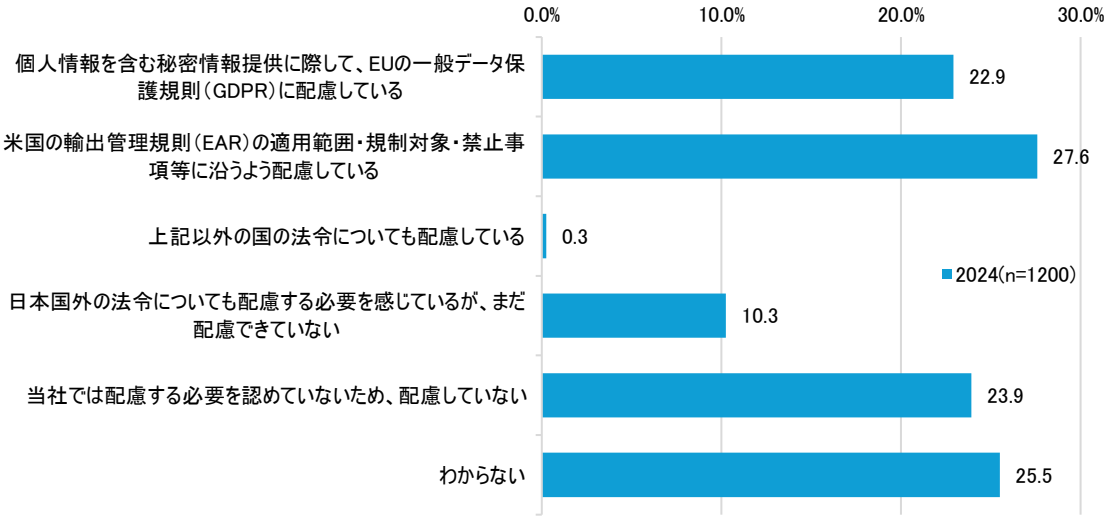


図 75 Q32 海外の拠点や取引先に対する秘密情報の提供等の際に配慮する他国の法令 (MA、n=1200)

海外の拠点や取引先に対する秘密情報の提供等の際に配慮する他国の法令について、一般データ保護規則(GDPR)より輸出管理制限(EAR)の方が、若干ではあるが配慮されている割合が高く、「米国の輸出管理制限(EAR)の適用内・規制対象・禁止事項に当たるおそれがある」は27.6%、「個人情報などを含む秘密情報等に関して、一般データ保護規則(GDPR)に配慮している」は22.9%であった。

また、「日本国外の法律について留意すべきことを感じているが、まったく配慮できていない」は10.3%であった。さらに、「当社は配慮すべきことを認識していないため、配慮していない」は 23.9%であった。「わからない」は25.5%であった。

また、「上記以外」で具体的な記載は「インドネシア」と「アジア」であった。

表 34 Q32 海外の拠点や取引先に対する秘密情報の提供等の際に配慮する他国の法令 (業種、従業員数、売上高、所属部門別)

(%)

		個人情報を含む秘密情報提供に際して、EU の一般データ保護規則（GDPR）に配慮している	米国の輸出管理規則（EAR）の適用範囲・規制対象・禁止事項等に沿うよう配慮している	上記以外の国の法令についても配慮している	日本国外の法令についても配慮する必要を感じているが、まだ配慮できていない	当社では配慮する必要を認めていないため、配慮していない	わからない
合計		22.9	27.6	0.3	10.3	23.9	25.5
業種	製造業	26.7	31.8	0.5	12.7	18.8	22.5
	非製造業	19.2	23.3	−	7.8	29.0	28.5
従業員数	301 人以上	34.0	40.2	0.2	8.2	9.5	25.0
	300 人以下	11.8	15.0	0.3	12.3	38.3	26.0
従業員数・業種	従業員数 301 人以上かつ製造業	41.0	44.0	0.3	8.3	8.3	20.3
	従業員数 300 人以下かつ製造業	12.3	19.7	0.7	17.0	29.3	24.7
	従業員数 301 人以上かつ非製造業	27.0	36.3	−	8.0	10.7	29.7
	従業員数 300 人以下かつ非製造業	11.3	10.3	−	7.7	47.3	27.3
売上高	10 億円以下	8.5	8.7	−	10.8	46.5	28.0
	10 億円超～100 億円以下	20.4	23.1	0.4	13.1	21.9	26.5
	100 億円超～1,000 億円以下	27.8	39.6	0.7	11.7	12.5	22.0
	1,000 億円超～5,000 億円以下	37.7	49.1	−	5.7	5.7	18.9
	5,000 億円超	42.4	44.8	−	5.2	5.2	27.9
所属部門	企業における情報システム関連部門	32.8	29.5	0.3	9.1	14.3	30.4
	企業のリスクマネジメント計画・実践に関わる部門	31.0	46.8	0.6	13.9	8.9	13.3
	企業のサイバーセキュリティに関わる部門	35.4	64.6	1.3	5.1	3.8	11.4
	経営企画部門	19.2	23.9	−	11.7	21.1	29.6
	経営層	7.7	8.1	−	8.8	54.2	25.3
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	21.0	27.4	−	12.9	13.7	30.6

業種、従業員数、売上高、所属部門別に集計したところ、従業員数別では、従業員数 301 人以上かつ製造業では他国の法令に配慮している傾向が強く、「個人情報を含む秘密情報提供に際して、EU の一般データ保護規則（GDPR）に配慮している」は合計に比べて＋10 ポイント以上で 41.0%、「米国の輸出管理規則（EAR）の適用範囲・規制対象・禁止事項等に沿うよう配慮している」も合計に比べて＋10 ポイント以上で 44.0%であった。一方で、従業員数 300 人以下の、特に非製造業の区分では、他国の法令への配慮の必要を認めていない割合が高く、「当社では配慮する必要を認めていないため、配慮していない」が合計に比べて＋10 ポイント以上で 47.3%であった。

売上高別では、100 億円超の区分から他国の法令に配慮している傾向が見られ、「個人情報を含む秘密情報提供に際して、EU の一般データ保護規則（GDPR）に配慮している」については 1000 億円超～5000 億円以下の場合 37.7%、5000 億円超の場合 42.4%であった。「米国の輸出管理規則（EAR）の適用範囲・規制対象・禁止事項等に沿うよう配慮している」については、100 億円超～1000 億円以下の場合 39.6%、1000 億円超～5000 億円以下の場合 49.1%、5000 億円超の場合 44.8%であった。

所属部門別では、企業における情報システム関連部門、企業のリスクマネジメント計画・実践に関わる部門、企業のサイバーセキュリティに関わる部門の 3 部門で 100 億円超の区分から他国の法令に配慮している傾向が見られた。「個人情報を含む秘密情報提供に際して、EU の一般データ保護規則（GDPR）に配慮している」については、企業における情報システム関連部門では

32.8%、企業のリスクマネジメント計画・実践に関わる部門では 31.0%、企業のサイバーセキュリティに関わる部門では 35.4%であった。「米国の輸出管理規則（EAR）の適用範囲・規制対象・禁止事項等に沿うよう配慮している」については、企業のリスクマネジメント計画・実践に関わる部門では46.8%、企業のサイバーセキュリティに関わる部門では 64.6%であった。

2.1.5　政府機関等の営業秘密管理に関する活動

Q36 経済産業省が 2016 年に公表した「秘密情報の保護ハンドブック」（以下、「ハンドブック」）を、あなたが所属する組織の対策における参考として活用している場合、今後の改定で実施してほしい内容を選んでください。（MA）

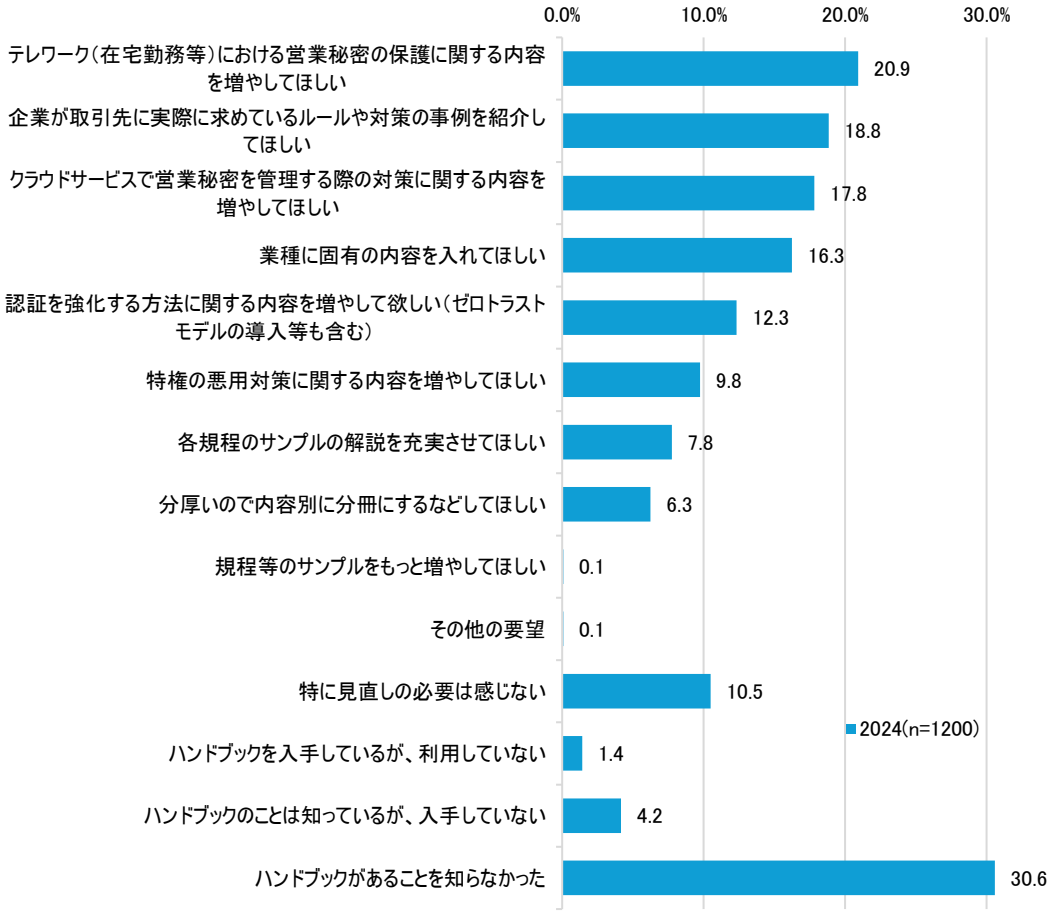


図　76 Q36「秘密情報の保護ハンドブック」の今後の改定で実施してほしい内容(MA、n=1200)

「秘密情報の保護ハンドブック」について、「ハンドブックがあることを知らなかった」の回答の割合は 30.6%（1200 人中 367 人）で最も高かった。

今後の改定で実施してほしい内容としては、「テレワーク（在宅勤務等）における営業秘密の保護に関する内容を増やしてほしい」が 20.9%、次いで「企業が取引先に実際に求めているルールや対策の事例を紹介してほしい」が 18.8%、「クラウドサービスで営業秘密を管理する際の対策に関する内容を増やしてほしい」が 17.8%であった。

表 35 Q36「秘密情報の保護ハンドブック」の今後の改定で実施してほしい内容（業種別）

	合計	ハンドブックがあることを知らなかった	
		人数	%
製造業	600	161	26.8
情報通信業	114	29	25.4
サービス業（他に分類されないもの）	88	31	35.2
小売業	53	20	37.7
専門・技術サービス業	49	25	51.0
建設業	35	18	51.4
金融業、保険業	35	8	22.9
不動産業、物品賃貸業	34	15	44.1
卸売業	33	13	39.4
医療、福祉	31	7	22.6
運輸業	28	8	28.6
教育、学習支援業	24	5	20.8
生活関連サービス業、娯楽業	23	12	52.2
その他	15	4	26.7
飲食サービス業	11	4	36.4
農林業	10	4	40.0
電気・ガス・熱供給・水道業	9	0	0.0
鉱業、採石業、砂利採取業	5	2	40.0
漁業	2	0	0.0
宿泊業	1	1	100.0

「ハンドブックがあることを知らなかった」と回答した割合について、業種別に集計した。回答者数が 100 人以上であった 2 区分別では、製造業では 26.8%、情報通信業では 25.4%であった。

Q37 営業秘密の保護にあたり、企業等が対策を講じる時、以下の行政サービス、ガイドライン等が利用できます。知っているものを全てお選びください。（MA）

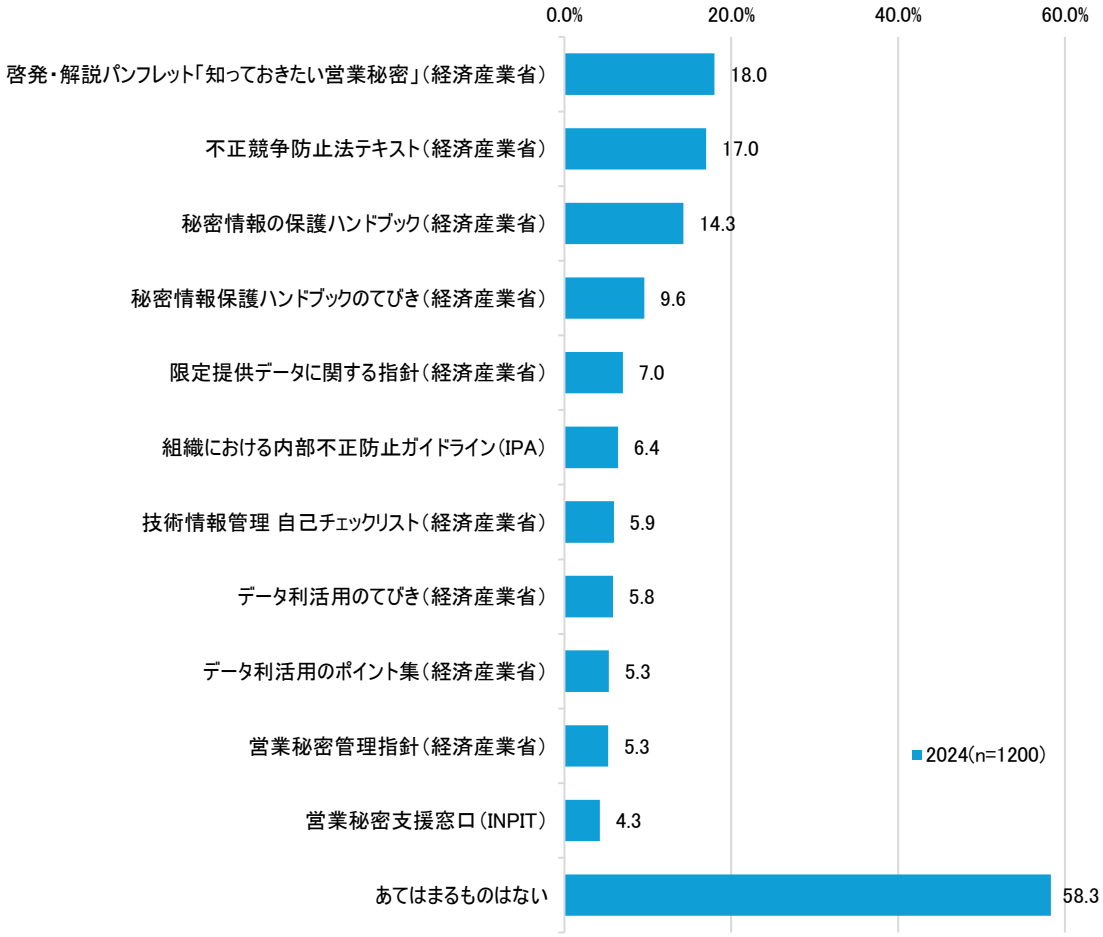


図 77 Q37 行政サービス、ガイドライン等で知っているもの（MA、n=1200）

行政サービス、ガイドライン等で知っているものについて、いずれも 20%に満たないが、その中でも「知っておきたい営業秘密」の認知度が最も高く、18.8%であった。経済産業省以外の INPIT のサービス及び IPA のガイドラインは、どちらも認知度は 10%に満たなかった。

表 36 Q37 行政サービス、ガイドライン等で知っているもの
(業種、従業員数、売上高、所属部門別)

(%)

		経済産業省									INPIT	IPA	
		不正競争防止法テキスト	啓発・解説パンフレット「知っておきたい営業秘密～予期せぬトラブルに巻き込まれないために～」	秘密情報の保護ハンドブック	情報管理も企業力 秘密情報保護ハンドブックのてびき	限定提供データに関する指針	データ利活用のポイント集	データ利活用のてびき	技術情報管理自己チェックリスト	営業秘密管理指針	営業秘密支援窓口	組織における内部不正防止ガイドライン	あてはまるものはない
合計		17.0	18.0	14.3	9.6	7.0	5.3	5.8	5.9	5.3	4.3	6.4	58.3
業種	製造業	18.5	20.3	16.3	11.3	8.7	6.7	6.5	6.5	7.3	5.2	6.8	53.3
	非製造業	15.5	15.7	12.2	7.8	5.3	4.0	5.2	5.3	3.2	3.3	6.0	63.3
従業員数	301 人以上	22.0	26.3	20.0	13.3	10.2	8.0	8.8	9.8	7.8	6.5	9.5	45.8
	300 人以下	12.0	9.7	8.5	5.8	3.8	2.7	2.8	2.0	2.7	2.0	3.3	70.8
従業員数・業種	従業員数 301 人以上かつ製造業	23.7	29.0	22.7	15.3	12.7	10.0	10.3	11.0	11.0	7.7	10.0	42.3
	従業員数 300 人以下かつ製造業	13.3	11.7	10.0	7.3	4.7	3.3	2.7	2.0	3.7	2.7	3.7	64.3
	従業員数 301 人以上かつ非製造業	20.3	23.7	17.3	11.3	7.7	6.0	7.3	8.7	4.7	5.3	9.0	49.3
	従業員数 300 人以下かつ非製造業	10.7	7.7	7.0	4.3	3.0	2.0	3.0	2.0	1.7	1.3	3.0	77.3
売上高	10 億円以下	9.0	6.7	6.9	3.6	2.6	2.1	2.6	1.5	2.6	1.0	2.8	80.2
	10 億円超～100 億円以下	17.3	15.8	14.6	6.5	6.5	4.6	3.8	3.8	4.6	3.1	4.6	56.2
	100 億円超～1,000 億円以下	20.9	29.3	16.5	15.0	10.6	8.1	8.8	9.2	7.0	7.7	7.7	40.3
	1,000 億円超～5,000 億円以下	21.7	17.9	19.8	15.1	9.4	7.5	11.3	9.4	6.6	3.8	12.3	45.3
	5,000 億円超	25.6	29.1	23.3	15.7	10.5	8.1	8.1	11.6	8.7	8.1	11.6	48.8
所属部門	企業における情報システム関連部門	21.6	19.8	20.4	13.4	9.4	7.3	6.4	7.9	5.8	5.2	10.0	54.4
	企業のリスクマネジメント計画・実践に関わる部門	20.9	33.5	19.6	14.6	12.7	7.6	11.4	7.6	9.5	7.0	8.2	34.8
	企業のサイバーセキュリティに関わる部門	19.0	38.0	16.5	17.7	16.5	10.1	11.4	12.7	8.9	6.3	7.6	29.1
	経営企画部門	16.0	15.0	12.2	7.0	3.8	3.8	5.2	6.1	2.3	2.8	3.8	60.6
	経営層	10.1	4.4	7.1	3.7	2.0	2.4	2.7	1.7	3.4	2.4	4.0	82.2
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	16.9	18.5	10.5	6.5	4.8	4.0	2.4	4.0	5.6	4.0	4.0	56.5

業種、従業員数、売上高、所属部門別に集計すると、従業員数・業種別では、従業員数 301 人以上かつ製造業の場合、経済産業省の「不正競争防止テキスト」や「啓発・解説パンフレット「知っておきたい営業秘密」～予期せぬトラブルに巻き込まれないために～」等の認知度が高く、7 項目で合計に比べて＋5 ポイント以上の割合であった。従業員数 300 人以下かつ非製造業では、特に認知度が高いものはなく、「あてはまるものはない」を選択した割合が 77.8%と、合計に比べて＋10 ポイント以上であった。

IPA の「組織における内部不正防止ガイドライン」については売上高に着目すると 1000 億円超～5000 億円及び 5000 億円超の区分で合計に比べて＋5 ポイント以上であったが、それ以外では特に認知度が高い区分はなかった。

表 37 Q37 行政サービス、ガイドライン等で知っているもの（業種別）

	経済産業省									INPIT	IPA	(%)
	不正競争防止法テキスト	啓発・解説パンフレット「知っておきたい営業秘密～予期せぬトラブルに巻き込まれないために～」	秘密情報の保護ハンドブック	情報管理も企業力 秘密情報保護ハンドブックのてびき	限定提供データに関する指針	データ利活用のポイント集	データ利活用のてびき	技術情報管理自己チェックリスト	営業秘密管理指針	営業秘密支援窓口	組織における内部不正防止ガイドライン	あてはまるものはない
合計	17.0	18.0	14.3	9.6	7.0	5.3	5.8	5.9	5.3	4.3	6.4	58.3
製造業	18.5	20.3	16.3	11.3	8.7	6.7	6.5	6.5	7.3	5.2	6.8	53.3
情報通信業	19.3	22.8	19.3	10.5	6.1	6.1	6.1	7.9	7.0	2.6	12.3	63.2
サービス業（他に分類されないもの）	11.4	15.9	6.8	6.8	5.7	4.5	8.0	3.4	1.1	5.7	4.5	63.6
小売業	15.1	11.3	11.3	1.9	5.7	0.0	3.8	0.0	0.0	1.9	1.9	71.7
専門・技術サービス業	14.3	8.2	10.2	6.1	0.0	2.0	2.0	2.0	2.0	0.0	4.1	75.5
建設業	17.1	11.4	2.9	8.6	0.0	2.9	2.9	8.6	0.0	0.0	2.9	68.6
金融業、保険業	20.0	17.1	14.3	11.4	2.9	2.9	5.7	5.7	0.0	2.9	0.0	60.0
不動産業、物品賃貸業	14.7	5.9	11.8	5.9	2.9	5.9	2.9	2.9	2.9	5.9	8.8	70.6
卸売業	9.1	9.1	12.1	3.0	6.1	0.0	0.0	12.1	3.0	3.0	3.0	60.6
医療、福祉	3.2	12.9	19.4	19.4	9.7	6.5	3.2	9.7	3.2	0.0	3.2	54.8
運輸業	21.4	21.4	14.3	7.1	10.7	10.7	7.1	7.1	3.6	10.7	3.6	60.7
教育、学習支援業	33.3	25.0	12.5	16.7	12.5	0.0	8.3	12.5	0.0	0.0	8.3	45.8
生活関連サービス業、娯楽業	13.0	17.4	8.7	4.3	0.0	0.0	0.0	0.0	13.0	4.3	4.3	65.2
その他	6.7	20.0	6.7	0.0	13.3	6.7	13.3	0.0	0.0	6.7	26.7	46.7
飲食サービス業	9.1	18.2	9.1	9.1	9.1	9.1	9.1	9.1	18.2	9.1	0.0	72.7
農林業	10.0	20.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	10.0	0.0	60.0
電気・ガス・熱供給・水道業	44.4	11.1	22.2	0.0	11.1	11.1	22.2	0.0	0.0	0.0	11.1	22.2
鉱業、採石業、砂利採取業	0.0	0.0	20.0	20.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	60.0
漁業	0.0	50.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	50.0
宿泊業	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0

業種別では、製造業では「あてはまるものはない」を選択した割合が合計に比べて－5 ポイント以上の 53.3%で、それ以外の行政サービス等の認知度は合計の割合と比較して大きな差はなかった。情報通信業では「秘密情報の保護ハンドブック」が 19.3%、「組織における内部不正防止ガイドライン」が 12.3%と合計に比べて＋5 ポイント以上であった。教育、学習支援業では、「不正競争防止テキスト」で 33.3%、「啓発・解説パンフレット「知っておきたい営業秘密～予期せぬトラブルに巻き込まれないために～」で 25.0%など、5 つの項目で合計に比べて＋5 ポイント以上であった。10 名以上の回答者がいる業種のうち、「あてはまるものはない」を選択した割合が大きかったのは 5 業種で、小売業では 71.7%、専門・技術サービス業では 75.5%、建設業では 68.6%、不動産業、物品賃貸業では 70.6%、飲食サービス業では 72.7%であった。

2.2　2 つの設問のクロス集計結果

営業秘密の漏えいに関して、特に注目すべき設問である、Q1、Q4、Q7、Q9 についてクロス集計を行った。

Q1（過去 5 年以内の営業秘密の漏えい事例の有無）と Q4（漏えい事例を認識したきっかけ）のクロス集計結果

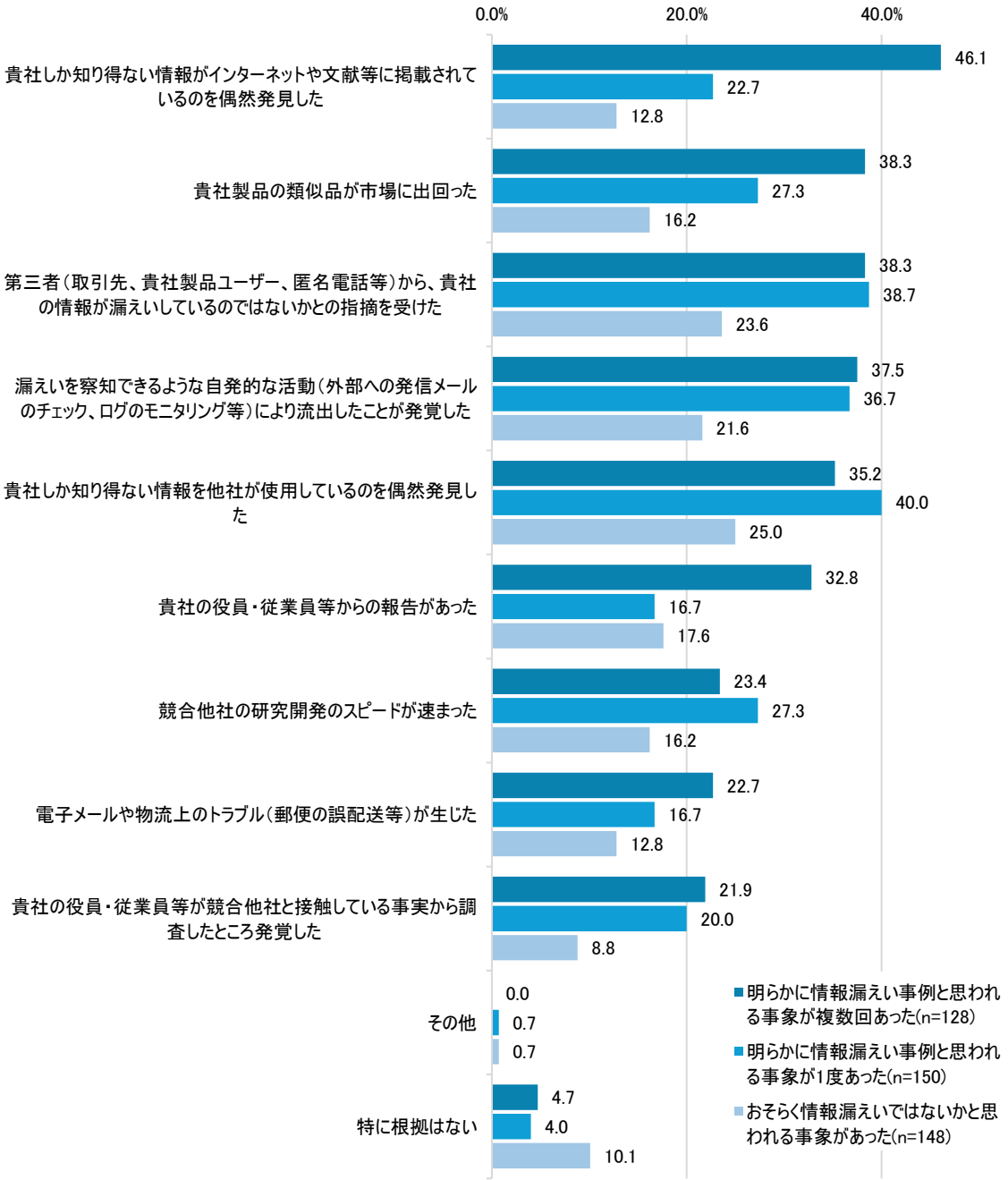


図 78 過去 5 年以内の営業秘密漏えい事例の有無と漏えい事例を認識したきっかけの関係

Q1 で明らかに漏えいと思われる事象があった場合の方が、おそらく情報漏えいではないかと思われる事象があった場合に比べて、Q4 で何らかの事象を選択している割合が高い傾向が見られた。

例えば、Q1 で「明らかに情報漏えい事例と思われる事象が複数回あった」」と回答した割合について、Q4 で「貴社しか知り得ない情報がインターネットや文献等に掲載されているのを偶然発見した」の割合が最も大きく 46.1%にもなったが、Q1 で「明らかに情報漏えい事例と思われる事象が 1 度あった」と回答した場合は 22.7%、Q1 で「おそらく情報漏えいではないかと思われる事例があった」と回答した場合は 12.8%であった。

また、「貴社製品の類似品が市場に出回った」については、Q1 で「明らかに情報漏えい事例と思われる事象が複数回あった」と回答した場合 38.3%、Q1 で「明らかに情報漏えい事例と思われる事象が 1 度あった」と回答した場合は 27.3%、Q1 で「おそらく情報漏えいではないかと思われる事例があった」と回答した場合は 16.2%であった。

「第三者（取引先、貴社製品ユーザー、匿名電話等）から、貴社の情報が漏えいしているのではないかとの指摘を受けた」については、Q1 で「明らかに情報漏えい事例と思われる事象が複数回あった」と回答した場合と「明らかに情報漏えい事例と思われる事象が 1 度あった」と回答した場合は同程度で、前者は 38.3%、後者は 38.7%、「おそらく情報漏えいではないかと思われる事例があった」と回答した場合は 23.6%であった。

「漏えいを察知できるような自発的な活動（外部への発信メールのチェック、ログのモニタリング等）により流出したことが発覚した」については、Q1 で「明らかに情報漏えい事例と思われる事象が複数回あった」と回答した場合と「明らかに情報漏えい事例と思われる事象が 1 度あった」と回答した場合は同程度で、前者は 37.5%、後者は 36.7%、「おそらく情報漏えいではないかと思われる事例があった」と回答した場合は 21.6%であった。

「貴社しか知り得ない情報を他社が使用しているのを偶然発見した」については、Q1 で「明らかに情報漏えい事例と思われる事象が複数回あった」と回答した場合と「明らかに情報漏えい事例と思われる事象が 1 度あった」と回答した場合は同程度で、前者は 35.2%、後者は 40.0%、「おそらく情報漏えいではないかと思われる事例があった」と回答した場合は 25.0%であった。

Q1（過去 5 年以内の営業秘密の漏えい事例の有無）と Q9（営業秘密の漏えい後に観察された不審な事象）のクロス集計結果

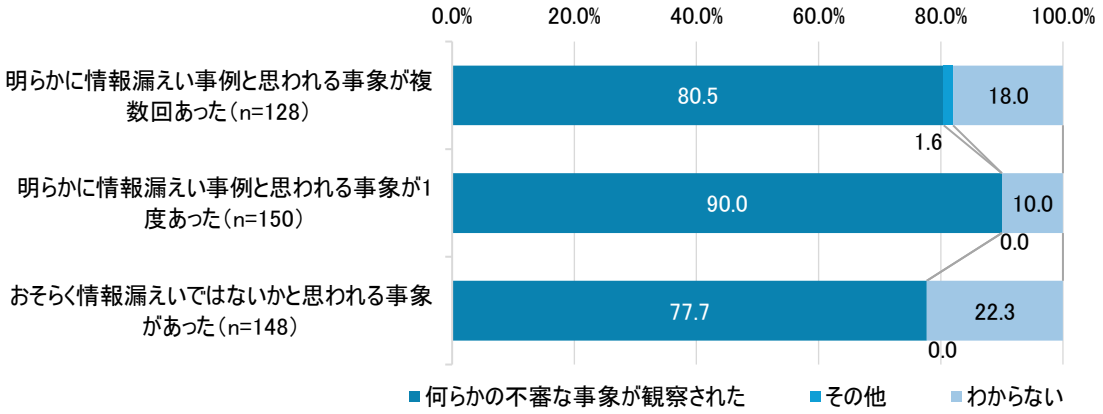


図 79 営業秘密漏えい後の不審な事象の経験有無

Q9 において、「その他」及び「わからない」以外の何らかの不審な事象が観察された割合と、「その他」を選択した割合、「わからない」を選択した割合を、Q1 で「明らかに情報漏えい事例と思われる事象が複数回あった」と回答した者、「明らかに情報漏えい事例と思われる事象が 1 度あった」と回答した者、「おそらく情報漏えいではないかと思われる事象があった」と回答した者、それぞれについて集計したところ、いずれの場合においても、「何らかの不審な事象が観察された」の割合が 75%以上であり、「明らかに情報漏えい事例と思われる事象が複数回あった」の場合 80.5%、「明らかに情報漏えい事例と思われる事象が 1 度あった」の場合 90.0%、「おそらく情報漏えいではないかと思われる事象があった」の場合 77.7%であった。

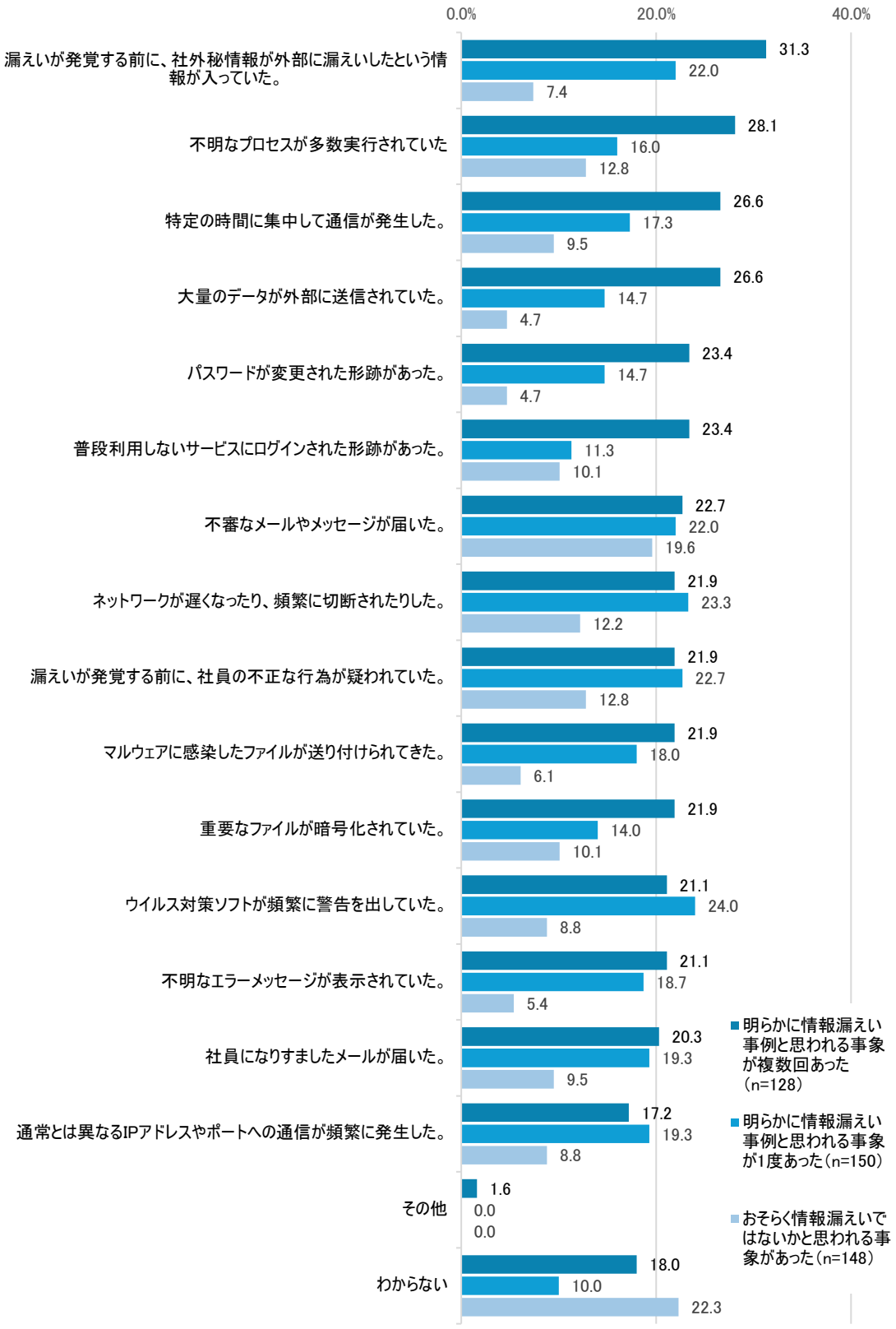


図 80 過去 5 年以内の営業秘密漏えい経験と漏えい後に観察された不審な現象の関係

Q9 において選択肢に提示した 15 個の不審な現象のうち「不審なメールやメッセージが届いた」を除く項目で、明らかに情報漏えい事例と思われる事象が複数回または 1 度あった場合の方が、おそらく情報漏えいではないかと思われる事象があった場合に比べて、選択された割合が高い傾向が見られた。

例えば、Q1 で「明らかに情報漏えい事例と思われる事象が複数回あった」と回答した割合について、Q9 で「漏えいが発覚する前に、社外秘情報が外部に漏えいしたという情報が入っていた」の割合が最も大きく 31.3%であったが、Q1 で「明らかに情報漏えい事例と思われる事象が 1 度あった」と回答した場合は 22.0%、Q1 で「おそらく情報漏えいではないかと思われる事例があった」と回答した場合は 7.4%であった。

また、「不明なプロセスが多数実行されていた」については、Q1 で「明らかに情報漏えい事例と思われる事象が複数回あった」と回答した場合 28.1%、Q1 で「明らかに情報漏えい事例と思われる事象が 1 度あった」と回答した場合は 16.0%、Q1 で「おそらく情報漏えいではないかと思われる事例があった」と回答した場合は 12.0%であった。

「特定の時間に集中して通信が発生した」については、Q1 で「明らかに情報漏えい事例と思われる事象が複数回あった」と回答した場合 26.6%、Q1 で「明らかに情報漏えい事例と思われる事象が 1 度あった」と回答した場合は 17.3%、Q1 で「おそらく情報漏えいではないかと思われる事例があった」と回答した場合は 9.5%であった。

「大量のデータが外部に送信されていた」については、Q1 で「明らかに情報漏えい事例と思われる事象が複数回あった」と回答した場合 26.6%、Q1 で「明らかに情報漏えい事例と思われる事象が 1 度あった」と回答した場合は 14.7%、Q1 で「おそらく情報漏えいではないかと思われる事例があった」と回答した場合は 4.7%であった。

「パスワードが変更された形跡があった」については、Q1 で「明らかに情報漏えい事例と思われる事象が複数回あった」と回答した場合 23.4%、Q1 で「明らかに情報漏えい事例と思われる事象が 1 度あった」と回答した場合は 14.7%、Q1 で「おそらく情報漏えいではないかと思われる事例があった」と回答した場合は 4.7%であった。

「普段利用しないサービスにログインされた形跡があった」については、Q1 で「明らかに情報漏えい事例と思われる事象が複数回あった」と回答した場合 23.4%、Q1 で「明らかに情報漏えい事例と思われる事象が 1 度あった」と回答した場合は 11.3%、Q1 で「おそらく情報漏えいではないかと思われる事例があった」と回答した場合は 10.1%であった。

一方で Q1 での回答によらず選択割合に差が無い項目が 1 つあり、それは「不審なメールやメッセージが届いた」であった。Q1 で「明らかに情報漏えい事例と思われる事象が複数回あった」と回答した場合 22.7%、Q1 で「明らかに情報漏えい事例と思われる事象が 1 度あった」と回答した場合は 22.0%、Q1 で「おそらく情報漏えいではないかと思われる事例があった」と回答した場合は 19.6%であった。

Q7（漏えいルート）と Q9（営業秘密の漏えい後に観察された不審な事象）のクロス集計結果

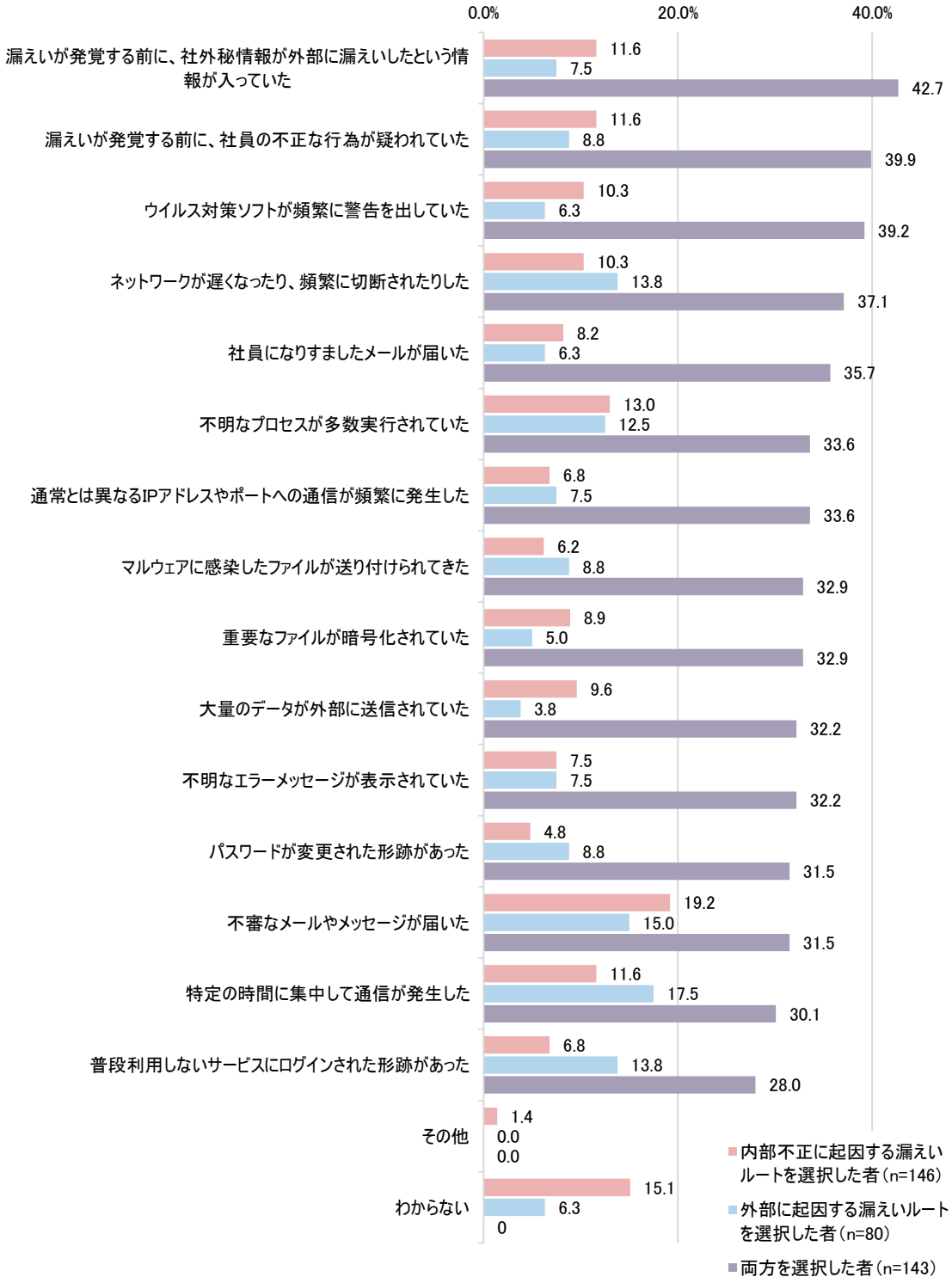


図 81 漏えいルートと営業秘密の漏えい後に観察された不審な事象の関係（MA、n=426）

Q7 の図 21 において、「内部不正に起因する漏えいルートを選択した者」、「外部に起因する漏

えいルートを選択した者」、「両方を選択した者」それぞれに分類された回答者が、Q9 においていずれの項目を選択したか集計した。

「その他」及び「わからない」を除くすべての不審な事象の項目について、「両方を選択した者」が選択した割合の方が、「内部不正に起因する漏えいルートを選択した者」及び「外部に起因する漏えいルートを選択した者」が選択した割合よりも 10%以上大きかった。「両方を選択した者」において、最も割合が大きかったのは、「漏えいが発覚する前に、社外秘情報が外部に漏えいしたという情報が入っていた」の 42.7%で、同項目は「内部不正に起因する漏えいルートを選択した者」では 11.6%、「外部に起因する漏えいルートを選択した者」では 7.5%であった。次いで割合が大きかったのは「漏えいが発覚する前に、社員の不正な行為が疑われていた」の 39.9%で、同項目は「内部不正に起因する漏えいルートを選択した者」では 11.6%、「外部に起因する漏えいルートを選択した者」では 8.8%であった。3 番目に割合が大きかったのは「ウイルス対策ソフトが頻繁に警告を出していた」の 39.2%で、同項目は「内部不正に起因する漏えいルートを選択した者」では 10.3%、「外部に起因する漏えいルートを選択した者」では 6.3%であった。

また、

「わからない」を選択した者の割合は、「内部不正に起因する漏えいルートを選択した者」で 15.1%、「外部に起因する漏えいルートを選択した者」で 6.3%、「両方を選択した者」では 0%であった。

3 考察

まず、本質問の内容を大別した 5 項目についてそれぞれ考察を行った後、それらを踏まえて、企業における営業秘密管理に関する課題等について述べる。

3.1 調査結果についての考察

3.1.1 営業秘密の漏えいの実態

過去 5 年間での営業秘密の漏えい事例の有無を問う Q1 の回答で、営業秘密の漏えいがあったと思われるという回答の割合が、2020 年度調査時から大幅に増加し 35.5%であったこと、「わからない・認識できていない」の割合が 2020 年度調査時から減少し 9.7%であったこと、及び漏えい事例を認識したきっかけを問う Q4 の回答で、ほぼ全ての回答の割合が 2020 年度調査時と比較して増加していたことから、単純に営業秘密の漏えい件数が増加傾向にある可能性の他、2020 年度よりも従業員から漏えいを報告する組織体制が整い、状況が把握できるシステム環境が進展した可能性が考えられる。

また、漏えいした情報の種類を問う Q2 の回答で、漏えいした場合に公表・報道されることの多い「顧客情報」よりも、「製造に関するノウハウ、成分表等」に関して「有」と「可能性有」を選択した割合の合計が大きいことから、広く公表・報道されていない営業秘密漏えいのインシデントが多いことが懸念される。さらに、営業秘密の漏えいによる推定損害額を問う Q5 の回答で、営業秘密の漏えいによる推定損害額が「わからない」とした割合が 2020 年度調査の 46.5%より減少して 16.9%に、10 億円以上とした割合が 2020 年度調査時の 0%より増加して 30%程度になっていることから、営業秘密の漏えいが事業に与える影響がより深刻になったと考えられる。

営業秘密の漏えい経路を問う Q7 の回答で最も割合が高かったのは、「外部からのサイバー攻撃等による社内ネットワークへの侵入に起因する漏えい」で 36.6%であり、2020 年度調査時に最も割合が高かった「中途退職者（役職員・正規社員）による漏えい」は、本調査では 17.8%であった。本調査の回答者が、企業の情報セキュリティやリスクマネジメントに関連する部門に所属する個人であることから、近年報告事例が増加しているランサム攻撃に伴う情報漏えい被害も「外部からのサイバー攻撃等による社内ネットワークへの侵入に起因する漏えい」に区分されている可能性がある。また、営業秘密の漏えい先を問う Q6 で、2020 年度調査時と比較して、「国内の競合他社以外の企業」の認識割合が特に増加し 48.8%となっていることを合わせると、外部からのサイバー攻撃等に起因する、漏えい先の特定が難しい事例が増加している可能性が考えられる。回答者が内部不正に起因する漏えいルートと外部に起因する漏えいルートのどちらを選択したか別では、内部不正に起因する漏えいルートのみを選択した割合と、内部不正に起因する漏えいルートと外部に起因する漏えいルートの両方を選択した割合がいずれも 30%程度で、外部に起因する漏えいルートのみを選択した割合が 20%程度であった。このことも踏まえると、個別の事象ではサイバー攻撃

等による漏えいの頻度が高いとしても、内部不正に起因する漏えい、外部に起因する漏えいを総合的に見れば、それぞれが発生した確率と両方が発生した確率は同程度であった可能性が考えられる。

営業秘密の漏えい後の対応を問うQ8の回答では、公的な相談窓口や弁護士・弁理士、警察への相談をしたとする割合が、いずれも 2020 年度調査時から増加していたことから、組織外への相談を行う傾向は高まっていることが示唆される。また、従業員数 301 人以上の製造業の区分では、他の従業員数・業種区分に比べて、営業秘密の漏えい事例の有無を問うQ1の回答では漏えいを経験した割合が高かったこと、及び営業秘密の漏えい後に観察された不審な事象を問う Q9 の回答では不審な事象を観測している割合が高かったことからは、従業員数 301 人以上の製造業では、漏えいの予兆や漏えいの結果生じるような不審な事象を検知する環境が整っている可能性が考えられる。従業員数 301 人以上の企業の方が、従業員数 300 人以下の企業に比べて、技術的対策を実施している割合が高い（Q17）ことからは、Q9 の回答ではそれぞれの不審な事象で従業員数 301 人以上の企業の方が、従業員数 300 人以下の企業に比べて選択した割合が高い傾向になることが推測されるが、実際には従業員数 301 人以上の企業と 300 人以下の企業で同程度に観察されている事象もあることから、漏えいした営業秘密の種類や漏えいのルート、組織で実施している対策の内容により観察される不審な事象が異なる可能性が考えられる。

3.1.2 営業秘密管理の実態

企業において営業秘密の管理をする上で、営業秘密の管理において脅威となる事象やそれに対する対策の必要性を認識することが重要である。特に、営業秘密の漏えいの原因となる内部不正は、業務における人手不足や、人間関係での恨みやコミュニケーション不足、営業秘密にアクセスできる従業員等の個人的な事情（転職や借金等）等に起因するので、内部不正を未然に防ぐにはこれらのような誘因が組織にあるかを把握し、対策することも重要である。また、企業の保有している情報の種別と、業務での活用状況を把握することも重要である。

自社の営業秘密の漏えいに関して、現在脅威と感じ、対策が必要と考えているものについて問うQ10では、業種、従業員数、売上高、所属部門別で分析した結果、表 3 に示されるように、従業員数 300 人以下かつ非製造業、売上高 10 億円以下、経営層の区分については、「特に感じているものはない」の割合が全体に比べて高い傾向にあった。実際に脅威が無い可能性だけでなく、自社の保有する営業秘密にとっての脅威を認識できていない可能性も考えられる。

また、営業秘密管理を実践する上での問題と感じていることを問うQ14において、従業員数 301 人以上かつ製造業の区分では、営業秘密管理を実践する上での問題の項目の一部で選択割合が 20%を超えており、他の区分ではいずれの問題の項目でも 20%を超えていなかった。このことから、従業員数 301 人以上かつ製造業の区分では、他の区分に比べて、営業秘密管理を実践する

上での問題を把握している可能性が考えられる。所属部門別に集計すると、企業におけるサイバーセキュリティに関わる部門では、電子メールの送信に関する問題とテレワーク等の新たな業務環境での対策の問題が意識されている傾向が観測され、経営層では、「問題は特にない」とする割合が 45%ではあったものの、対策の費用対効果を明示しにくいこと、人材、費用の両面のリソース不足及びリソース不足も一因と考えられる私物端末の利用が比較的問題視されている傾向が見られた。現場が、実際の業務に係る問題意識を経営層と共有できていないか、または問題意識が共有されていても、対策の費用対効果がわからないか、あるいはリソース不足であることにより、経営層が対策実施のための予算措置に踏み切れない状況にある可能性が考えられる。

内部不正を誘発する環境や状況について問う Q11 では、「同じ仕事・業務を同じ人が長く続きている」が 36.8%、「少ない人数で業務を回している」が 39.5%と全体で見ると回答割合が大きかったことから、組織体制として改善に着手可能な環境要因が、内部不正のリスク要因として残置されている状況が俯瞰できる。また、人手不足が問題と直結していると捉えられている傾向が大きいとも考えられる。所属部門別では、選択肢ごとに選択割合の差を見ると、「人間関係、コミュニケーション、上司や会社への恨みが大きい」等の人間関係による内部不正を誘発する環境や状況において経営に関わる「経営層」及び「経営企画部門」とその他の部門の間で差が大きく、それに比較して人手不足等の業務の遂行に直結する誘因については部門間での差が小さい傾向が見られた。このことから、現場で認識されている内部不正を誘発する環境や状況のうち、人手不足等の業務の遂行に直結するものに比べて、人間関係による内部不正を誘発する環境や状況は経営層まで共有されていない可能性が考えられる。

不正競争防止法で保護されており、データの利活用に関わる「限定提供データ」の保有とビジネスでの活用状況を問う Q15 について、限定提供データを保有している割合は 2020 年度調査から大きく増加し 51.6%であり、その半数以上がビジネスで活用していたことから、企業におけるデータの利活用が進んでいる可能性が考えられる。従業員数別では、301 人以上の企業では限定提供データを保有している割合が 60%以上である一方、300 人以下の企業では限定提供データを保有していない割合が 61.3%であったことから、従業員数が多い企業において、よりデータの利活用が進んでいる可能性が考えられる。

企業において営業秘密の管理を行うに当たっては、営業秘密とそれ以外の情報との区分及び秘密性のレベルに応じた格付けの実施は、重要情報を管理するための基本であり、企業の重要情報管理状況を把握する上で重要である。また、組織として営業秘密の管理ルールを定めた上で、従業員等に周知し、組織的に運用することにより、従業員等には営業秘密を持ち出す気を起こさせないことも重要である。

営業秘密とそれ以外の情報との区分及び格付けの実施有無を問う Q12 において、「営業秘密とそれ以外の情報とを区分していない」の割合は 22.3%であり、今後も改善の余地が大きいと考えられる。また、営業秘密情報を区分して管理している割合は 2020 年度調査から増加している点では、

対策が進展していると言える。さらに、従業員数・業種別では、製造業、非製造業とも、従業員数301 人以上の企業において対策が進んでいる。逆に、所属部門別ではリスクマネジメント関連部門とサイバーセキュリティ関連部門において情報区分管理の意識が高く、経営層において意識が希薄になっている傾向が示されている。

営業秘密を社内規程として定められた営業秘密の管理ルールの運用状況を問う Q13 において、「全体において厳密な運用が徹底されている割合」の割合が 2020 年度調査から微増している一方で、「ある程度厳密に運用されている（部署やチームなとによって事情が異なる場合も含む）」、「厳密な運用を目指して改善の途上にある」及び「管理ルールを制定したのみ」という、管理ルール等に沿った運用を心掛けていると推測される割合は、減少している。さらに、「厳密な運用とはいえない」と「わからない」という管理ルール等があったとしてもそれに則った運用をしていない或いは管理ルール等を認識していないと推測される割合は増加している。これらのことから、組織で統一した営業秘密の管理ルールを定めていないか定めていても組織内でのルールの周知が不十分で、営業秘密を持ち出す際の従業員等の心理的なハードルが低い状況にある企業が増加している可能性が考えられる。

企業において営業秘密の管理をする中では、秘密情報が漏えいした際に迅速に対応し、漏えいの影響を最小限に抑えるためにも、秘密情報の漏えい時の体制を整備し、漏えい時の対応を主導する部署を定めておくことが重要である。

秘密情報の漏えい時の組織体制を問う Q33 では、秘密情報の漏えい時の組織体制が「特にない」とする割合は全体では 35.4%で、2020 年度調査と比較すると増加していた。また、秘密情報の漏えい時に対応を主導する部署・担当を問うQ34 では、秘密情報の漏えい時に対応を主導する部署・担当が「決まっていない」とする割合が 2020 年度調査から増加し、24.7%であった。これらのことから、秘密情報の漏えい時の組織体制の整備がされていないか、あるいは回答者が自社で整備されている体制を認識できていない企業が一定数ある可能性が考えられる。

3.1.3 営業秘密管理において実施している対策

営業秘密管理においては、組織が保有する営業秘密の性質、従業員の規模、予算などに合わせて、技術的対策や環境的対策、秘密保持契約の締結等の法的な対策を行うことが重要である。

技術的対策のなかでもサーバーのアクセスログの管理やメールの監視などの対策は、不正行為の抑止と早期発見の観点、不正競争防止法における営業秘密の要件である秘密管理性の観点から、営業秘密管理における重点項目である。

営業秘密の漏えいに気付くことができるような技術的対策の実施状況を問う Q16 では、営業秘

密の漏えいに気付くことができるような技術的対策を実施しているか、実施することを検討中とする割合が 2020 年度調査から減少し、現在技術的対策を実施しておらず今後の予定もないとする割合、技術的対策の実施状況がわからないとする割合がそれぞれ微増した。このことから、自分の所属する企業において実施している技術的対策の実施状況を従業員が認識していない傾向が強まった可能性及び営業秘密管理において技術的対策を実施することの優先度が企業において低下している可能性が考えられる。

実施または実施を検討している技術的対策の具体的な内容を問う Q17 において、所属部門別では、情報システム部門で対策の選択割合が大きく、その他の部門では比較的割合が小さい傾向が見られた。このことから、企業において情報システムに対し技術的対策の導入を主導している当事者である部門では自組織で行われている技術的対策を認識している一方で、組織全体としては技術的対策を実施していることの周知が不十分である可能性が示唆された。サーバーのアクセスログの管理やメールの監視などの対策を周知することで、漏えいの機会を減らすだけでなく、内部の者が不正に情報を持ち出すと見つかるだろうという心理的な抑止力を高める効果も期待できるので、引き続き現在の対策を実施しつつ、実施している対策の内容を情報システム関連部門以外にも広く周知することで、現在の技術的対策が、外部からの攻撃だけでなく内部不正の対策としても効果を発揮できるようになると期待できる。また売上高別では、5,000 億円超の区分でそれぞれの対策の選択割合が大きい傾向にあったが、「ファイアウォールや DMZ、IDS/IPS などの設置・構築」の割合については 10 億円超～100 億円以下の区分でも選択割合が大きい傾向が見られた。具体的にどのような製品やサービスを利用しているのかを調査することで、比較的売上の規模が大きくない企業でも取り組みやすい対策を明らかにできると考えられる。

営業秘密情報の社外への不正持出防止策として実施しているものを問う Q19 では、USB メモリ等の電磁的記録媒体の利用に関する対策が比較的高く実施されている傾向が見られた。2020 年度調査と比較して、紙資料等の管理に関する対策の実施割合が低下していること、業務使用 PC 等への保存制限、オンラインストレージへのアクセス制限の実施割合が増加していることからは、業務上で、紙資料の取扱い減少、電磁的記録媒体の利用が減少してオンラインストレージ等の利用が促進されており、それに伴い実施される対策が変化していることが予想される。

環境的対策の実施状況を把握するために、Q20 では不正に持ち出せば見つかるような環境を整える対策として実施しているものを質問した。いずれの対策についても、実施割合は高くても 20~30%程度にとどまっていた。特に、営業秘密情報を外部に電子メールで送信する際に、環境面での情報漏えい対策として注意すべき、「外部への電子メール送信時のチェック機能導入」は 20%に達していなかった。Q19 での電子メールの利用時の対策（「電子メールの添付ファイルの制限または禁止」「電子メール送信時の上長確認フローを運用（必ず上司等が CC に追加される設定を行っている等）」でも割合が 2020 年度調査時から微増はしたものの 20％弱に留まったことも合わせると、全体的に、電子メールの利用の際の情報漏えい対策への意識が依然として低いと考えられる。

営業秘密管理においては、秘密保持契約の締結や、職業選択の自由を侵害するリスクもあるが競業避止義務契約の締結も法的な対策として有効である。

情報のコンタミネーションにより、他者の秘密情報を意図せず使用してしまうリスクに対して実施している対策を問う Q21 では、転入者が転入元との関係で負っている秘密保持契約や競業避止義務契約といった義務の有無や内容を確認している割合が最も大きかった。また、競業避止義務契約の具体的な内容を問う Q24 では、「答えがわからない」割合が最も高く 41.5%であった。さらに、秘密保持契約の締結状況を問う Q22 と競業避止義務契約の締結状況を問う Q23 では、「締結していない」とする割合は 2020 年度調査時と比較して減少し、締結しているとする割合が増加していた。これらのことから、秘密保持契約や競業避止義務契約の締結が営業秘密管理において有効だと考え、自組織の対策に取り入れている企業が一定数存在している一方で、従業員等の半数近くが競業避止義務契約の具体的な内容を把握していない、あるいは理解していない可能性が考えられる。また、競業避止義務契約違反後の対応を問う Q25 では、「違反事例が存在しない（把握できていない場合を含む）」は 32.9%、「わからない（関係者外秘の場合を含む）」は 31.7%と、2 項目の割合が高かったことから、高くの企業が違反の有無を把握できていない、あるいは対応しきれていない可能性が示唆され、高くの企業が違反の有無や内容の把握に課題を抱えていることや、違反が判明しても警告や訴訟などの法的措置をとるケースは一定割合にとどまっていると考えられる。

3.1.4 最近の動向を踏まえた対策

近年、取引先や委託先のセキュリティが手薄な企業を足掛かりに、最終的な標的である大企業への侵入を試みるケースが見られることから、サプライチェーンのセキュリティ管理が重要になってきている。営業秘密管理の観点からも、サプライチェーンにおいて自組織の営業秘密の取扱い状況を把握しておく必要がある。

サプライチェーンにおける営業秘密の管理状況に関する Q26 において、「営業秘密のやりとりを行う相手先がない」を除いた回答者に占める「直接の取引先の管理状況を把握していない」とする割合が 2020 年度調査と比べると減少していることから、取引先の管理が必要と認識している企業では取引先の管理が進んでいる可能性が示唆された。全体としては、「営業秘密のやりとりを行う相手先がない」とする割合が 2020 年度調査では 20.9%のところ本調査では 36.8%と 15%以上増加していること、直接の取引先の管理状況を把握している割合が 2020 年度調査時には 41.6%、本調査では 44.8%と大きくは増加していない。これらのことから、企業において対策の必要性は認識されているものの思うように進められていない可能性や、自社の営業秘密が何であるかを正しく認識できておらず、技術指導や取引先との情報共有を通じて知らないうちに取引先に営業秘密を提供してしまうリスクが強まっている可能性が考えられる。

また、企業のデジタル化の中でクラウドサービスや生成 AI の利用、テレワークの活用が進んでいる。クラウドサービスの利用においては、利用者側の設定ミスやパスワードの管理の不備などが原因で、情報漏えいにつながるリスクがある。生成 AI の利用においては、営業秘密等の機密情報を誤ってプロンプトに入力することで、その情報が学習データとして利用されるおそれがある。テレワークにおいては、業務用端末や紙資料の紛失、盗難、社外のネットワークを利用することで外部からの不正アクセスを受ける等のリスクがある。自組織の営業秘密を保護するためにも、クラウドサービスや生成 AI の利用、テレワークに関してルールを定め、従業員等が適切に情報を取扱えるようにする必要がある。

クラウドサービスを使用した営業秘密の共有や参照を問う Q27 では、2020 年度と比較すると、クラウドサービスを使用して営業秘密の共有を行っているとする割合が全体としては 22.8%から 50.4%と約 2 倍に増加しており、また、クラウドサービスの利用における対策の実施状況を問う Q28 では、従業員数 301 人以上の企業では 70%以上が何らかの対策を実施している一方で、従業員数 300 人以下の製造業では 50%、従業員数 300 人以下の非製造業では 40%弱にとどまっていた。さらに、「シャドークラウド」が生ずることを防止する対策の実施状況を問う Q29 では、2020 年度調査と比較すると、対策を「何も講じていない」とする割合は 60.0%から 41.3%に減少しているものの、クラウド利用に関するルールを定めているのは約半数、残りの約半数は現在「シャドークラウド」が生じることを防止する対策を実施できていない結果となった。これらのことを合わせると、全体として企業においてクラウドサービスの利用が進んでおり、営業秘密を取扱う場面も 2020 年に比べて増加している一方で、企業全体としてシャドークラウドを含むクラウド利用への対策が十分に進んでおらず、特に従業員数の少ない企業ほど、クラウドサービスの利用に関する対策が遅れている可能性が考えられる。

クラウドサービスを使用した営業秘密の共有や参照を問う Q27 で、社内または社外のいずれかに限定して共有を行っている割合は全体の約 1/3 程度、「行ったことが無く今後の予定もない」とする割合は 36.3%で約 1/3 程度であったこと、及び 2020 年度調査と比較して「現在は行っていないが、将来行うことを検討している」とする割合が減少していることからは、2020 年度調査からクラウドサービスの利用は進んでいるものの、全体の 2/3 の企業ではクラウドサービスによる営業秘密の共有や参照について慎重または非積極的な姿勢を示していると考えられる。

生成 AI の業務利用において秘密情報を保護する観点でどのような対策を行っているかを問う Q30 では、「わからない」とする割合が 34.9%であった。このことからは、生成 AI の利用に関して、そもそもルールが存在しない、ルールは存在するが従業員等に周知されていない、ルールは存在していても具体的に生成 AI の利用に関して何をしてよく、何をしてはいけないのかを理解できていない、回答者自身が生成 AI を利用しておらず組織が実施している対策を把握していない等の可能性が考えられる。また、「ルールはなく、業務では、自由に組織内外の生成 AI を利用できる」とする割合は全体としては 13.1%、従業員数・業種別では 300 人以下かつ非製造業である場合で 22.0%、売上高別では、10 億円以下の場合で 20.8%であったことを合わせると、特に売上高が大き

くない企業又は従業員数が少ない企業において、生成 AI の利用の際に営業秘密が安全に取扱われるようにするためには、生成 AI の利用に関してルールを従業員に理解させ、実践させることが課題になっていると考えられる。

テレワークの環境で営業秘密を扱う場合のルールの具体的な内容を問う Q35 では、全体として最も重視されているのは通信の暗号化やアクセス制御に関する対策であることがわかった。一方、ソーシャルメディアの利用やその他の項目については 20%以下と比較的低く、テレワークの環境での営業秘密の取扱いについて、さらなる注意喚起が必要と考えられる。

さらに、営業秘密を含む技術情報や物品の海外への持ち出しに際しては、意図しない技術流出を防止するという観点から、外為法も遵守する必要がある。海外拠点や海外の取引先と営業秘密をやり取りする際には、GDPR や EAR 等の他国の法令についても配慮が必要である。

外為法を遵守するための社内の輸出管理体制の整備状況を問う Q31 では、外為法を遵守するための規程やマニュアルの整備が必要としているのは全体の半数程度であった。また、海外拠点や取引先に対する秘密情報の提供等の際に配慮する他国の法令を問う Q32 では、GDPR に配慮している割合は 22.9%、EAR に配慮している割合は 27.6%であったことからは、多くの企業で輸出管理規制に注意を払っており、他国の法令についても一定の配慮をしていると考えられた。一方で、「わからない」とする割合は、Q31 で 26%、Q32 で 25.5%であったことから、海外との直接的な取引がない可能性、及び自組織に外為法を遵守するための輸出管理体制や他国の法令への配慮の必要性の認識が不十分である可能性が考えられる。

3.1.5 政府機関等の営業秘密管理に関する活動

政府機関等が行っている営業秘密に関する活動では、日常業務で営業秘密を取扱う可能性のある従業員等にまで情報が届き、適切に営業秘密を保護するための対策が実施されることを目指して、普及啓発に取り組む必要がある。

「秘密情報の保護ハンドブック」（経済産業省）の内容について取り込むべき内容を問う Q36 では、そもそもハンドブックがあることを知らなかったとする割合が 30.6%であったこと、及び経済産業省や独立行政法人の発行しているガイドラインやサービス、設置している相談窓口等で知っているものを問う Q37 では、「あてはまるものはない」とする割合が 58.3%であった。また、「2.1.3 営業秘密管理において実施している対策」において、複数の質問で「実施していない」とする回答の割合が 20%を超えている傾向があった。

これらのことから、各種ガイドライン、相談窓口事業等の認知度は全体的に低く、営業秘密を取扱う可能性のある従業員等に広く営業秘密の適切な管理を啓発しきれていないと考えられる。

各種ガイドライン、相談窓口事業等の認知度が低い理由としてはいくつか考えられ、特定の業界では独自の規格やガイドラインに基づいて情報管理が行われており、改めて政府機関等の取組に目を向ける機会が少ないという可能性、営業秘密管理は法や知的財産権の知識と密接に関わるやや専門的な分野であり、法務担当者のいない小規模の企業等では関心を持つ機会が少ないという可能性、国や独立行政法人の情報発信はマスメディアを通じた広告・広報活動が十分にできず多くの人の目に留まりにくいという側面がある可能性、営業秘密管理は企業において重要ではあるが緊急ではないとして、特に中小企業では日々の業務や営業活動が優先され、営業秘密管理に関する情報収集まで手が回っていない可能性、企業内で各種ガイドライン、相談窓口事業等の情報が展開されていない可能性等が考えられる。

また、漏えい経験者 426 人を対象に業秘密の侵害行為を行った行為者・企業に対して取った対応を問う Q8 で、「公的な相談窓口に相談を行った」の割合が 32.2%である一方で、回答者全員 1200 人を対象とする Q37 では、営業秘密支援窓口（INPIT）の認知度は 4.3%であった。このことから、平時は他の業務を優先していたところ実際に営業秘密の漏えいを経験したことをきっかけに公的機関への相談割合が高まったと考えられる。

3.2 企業における営業秘密管理に関する課題等

営業秘密管理はサイバー対策と内部不正防止の両面での対応が必要

2020 年度調査と比較すると、営業秘密の漏えい事例・事象を認識している割合が大幅に増加し、推定被害額は高額な方向に推移していることから、営業秘密の漏えいが事業に与える影響がより深刻になったと考えられる。また、サイバー攻撃による漏えい等の外部に起因する漏えいだけでなく、内部不正に起因する漏えいの両方の認識が増加していることから、サイバー対策と内部不正防止の両面で対策に取り組む必要がある。

経営トップから現場まで一貫したリスク認識が必要

2020 年度調査と比較すると、限定データの保有と活用が進み、クラウドを利用した秘密情報の共有割合が増加する等、組織における情報の活用が進んでいる傾向が見られる。一方で、内部不正を誘発する環境や状況について経営層と部門担当者のリスク認識に相違があることで、組織単位での対策に後れを取り、漏えい等につながるおそれがある。内部統制やリスク共有の仕組みを整備し、経営トップから現場まで一貫したリスク認識を持つ必要がある。

営業秘密管理に関する対策の実効性の向上

秘密保持契約や競業避止義務契約を締結する企業は一定数増加しているものの、多くの企業では、契約の締結だけにとどまり、契約内容の理解や従業員への周知が不十分な可能性や、違反後の対応も適切に行われていない可能性が示唆された。また、全体的に対策状況は 2020 年度調

査時と比較して大きく変わっていない。このため、違反を見つけられないリスクが依然残ると考えられる。契約内容の管理と遵守の徹底、違反時の厳正な対応を組織的に進める必要がある。

新技術を適切かつ安全に利用

生成 AI やクラウドサービス等の新技術の導入が進む一方で、営業秘密情報の取扱いに関するルールの整備及び利用者側の理解が追いついていない企業もあり、営業秘密情報を不適切に取扱うことによる漏えいのリスクが高まっていると考えられる。また、新技術の利用を必要以上に制限するルールを整備していることで、イノベーションの機会を逸している可能性がある。各企業においては、適切なルールを整備したうえで新技術を適切かつ安全に利用していく必要がある。

4　今後の展望

本調査では、組織における情報や新技術の活用が進んでいる傾向がみられるなか、企業における営業秘密管理が十分とはいえない現状が明らかとなった。企業での対策実施を促すために、本調査結果も活用し、官民連携による継続的な普及啓発を推進していく必要があると考える。

今後は、本調査の継続調査と合わせて、営業秘密の漏えいや管理の実態に関する深堀調査による取組み事例の作成や、監査や内部通報の仕組みとその有効性分析等の異なる視点での調査を行うことで、企業の営業秘密管理に資する有益な情報提供につなげたい。また、調査結果をもとに、営業秘密管理の観点で、具体的かつ優先順位付けされた対策を検討し、「組織における内部不正防止ガイドライン」を改訂することで、営業秘密を取り巻く情勢を踏まえた継続的な改善を促していきたい。

企業における営業秘密管理に関する実態調査 2024 調査実施報告書
https://www.ipa.go.jp/security/reports/economics/ts-kanri/tradesecret2024.html

2025 年 8 月
独立行政法人情報処理推進機構

https://www.ipa.go.jp/