企業における営業秘密管理に関する実態調査

－ 調査報告書 －

平成 29 年 3 月 17 日

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目次

1. はじめに

1.1. 背景および目的

経済のグローバル化やITの発展に伴う情報化等が著しく進展する現代において、我が国の企業が競争力を維持・強化していくためには、技術情報や営業情報に代表されるような、各企業の競争力の源泉となるような情報を適切に管理・活用していくことが重要となっている。

一方で、企業の経営に影響をおよぼしかねない営業秘密漏えい事案が後を絶たず、報道等で明らかになっているものだけでも様々な業種・規模の企業が被害を受けており、その漏えいのルート・手段も多様であることから企業側も対策に苦慮しており、深刻な状況となっている。

このような背景を受け、企業に対して営業秘密の保護強化に向けた情報セキュリティ対策等の実施を促す必要がある。営業秘密の漏えいを防ぐための対策については、経済産業省が平成28年2月に公表した「秘密情報の保護ハンドブック～企業価値向上に向けて～[1]」の中で、情報の分類の考え方や、漏えいルート等に応じた対策の例、他社の営業秘密の侵害を防ぐための対策例、漏えい事案への対応例等が紹介されており、営業秘密管理の手段や重要性を周知してきたところである。

しかしながら、依然として営業秘密の漏えい事案が継続的に発生していることからも、企業において必ずしも有用な対策が施されているとは言えず、引き続き営業秘密管理の重要性や侵害があった際の対応方法、管理手法等についての普及啓発が必要な状況である。

企業におけるこうした営業秘密の管理実態については、2012年度に経済産業省が「人材を通じた技術流出に関する調査研究[2]」（以下、「過年度調査」と記載）の中で調査しており、本調査では過年度調査の結果や、その後の法改正や社会動向の変化等を踏まえて、企業における営業秘密の漏えいや管理に係る対策状況について、アンケート調査やインタビュー調査、判例等の調査を通じて実態の把握を行った。

---

1 経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～」（平成28年2月）
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

2 経済産業省（委託先：三菱UFJリサーチ＆コンサルティング株式会社）「人材を通じた技術流出に関する調査研究」
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/H2503chousa.pdf

1.2. 実施概要

本調査では、企業における営業秘密の漏えいや管理の実態を把握し、有効な対策を検討することを目的として以下に示す調査を行い、その結果を本報告書に取りまとめた。

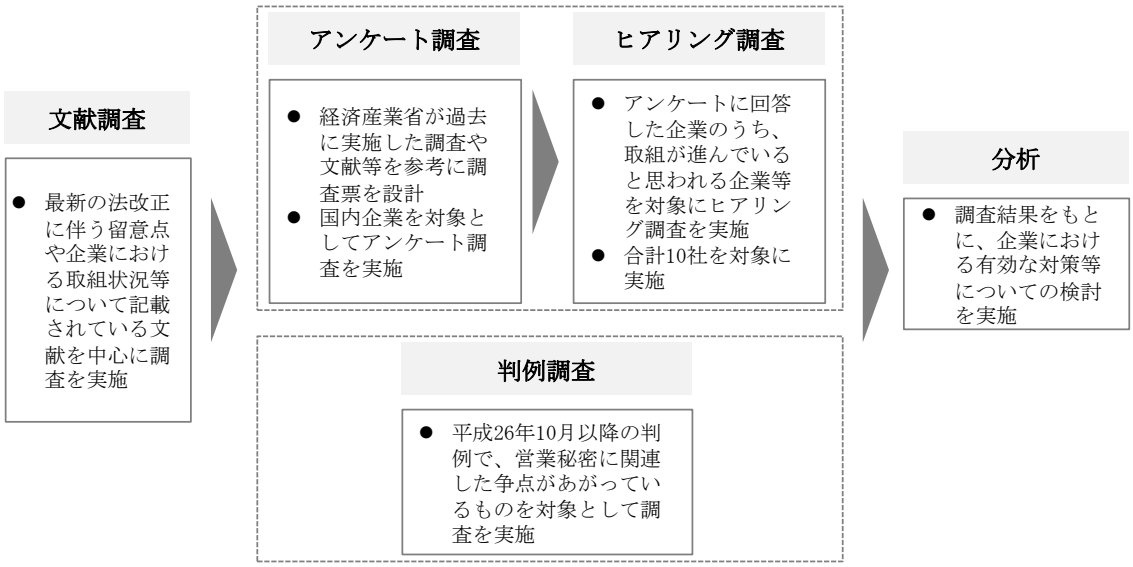

図 1.2-1　調査実施概要

2. 営業秘密管理の実態

2.1. 近年の営業秘密漏えい実態

近年、報道等によっても明らかとなっている通り、大企業における営業秘密の漏えいが社会的にも注目されている。

今回実施した調査結果より、営業秘密の漏えいに関する状況として、以下の実態が明らかになった。

- アンケート調査の回答者全体の中で8.6%の企業が過去５年間に営業秘密の漏えいを経験したと回答しており、明確に漏えいを認識した企業の割合は過年度調査時の 13.5%と比較して減っている。
- ただし「漏えいがあったかわからない」と回答している企業の割合は 16.2%→18.1%と若干ではあるが増えており、明るみになっていない営業秘密漏えいも一定数発生しているものと思われる。
- 営業秘密の漏えいルートについては、営業秘密の漏えいを経験した企業のうち、43.8%の企業が「現職従業員等のミスによる漏えい」と回答しており、「中途退職者（正規社員）を通じた漏えい」については 24.8%の企業が回答している。
- 営業秘密の漏えい先は、「国内の競合他社」が最も多く、32.4%であった。一方で、22.9%の企業については「わからない」と回答している。
- 漏えいを認識したきっかけについては、41.3%の企業が「第三者から指摘を受けた」と回答し、38.5%の企業が「役員・従業員等からの報告があった」と回答している。
- 営業秘密の漏えいによる損害の規模については、54.3%の企業が「わからない」と回答しており、損害の規模を把握できていない。損害の規模を把握している企業においては、「1,000 万円未満」と回答している企業の割合が 31.4%と高い。また、少数ではあるが、製造業の大規模企業においては、「1,000 億円以上」と回答している企業があった。
- 営業秘密の漏えいによる損害額の内容については、31.1%の企業が「原因調査や再発防止策の費用」と回答しており、また 27.9%の企業が「自社が得ることができたと想定される利益の額」と回答している。
- 過去５年間に営業秘密の漏えいを経験した企業のうち、侵害者へ行った対応として「事実関係の調査」を実施した割合は 46.6%であり、懲戒処分を実施している企業は 18.4%に留まる。

2.1.1. 過去５年間における営業秘密の漏えい状況

本調査研究において実施した「営業秘密の管理実態に関するアンケート調査」（以下、本アンケート調査と記載する。調査結果は報告書別冊参照。）によれば、8.6%の企業（全体から「漏えい事例はないと回答した企業（73.3%）」「わからないと回答した企業（18.1%）」を除いた企業）が過去５年間で営業秘密の漏えい（漏えいした可能性があると認識しているケースを含む）があったと回答している（図 2.1-1）。なお、このうち、「明らかな」情報漏えい事例があったと回答した企業は 5.0%（回答した全企業に対する割合）であった。

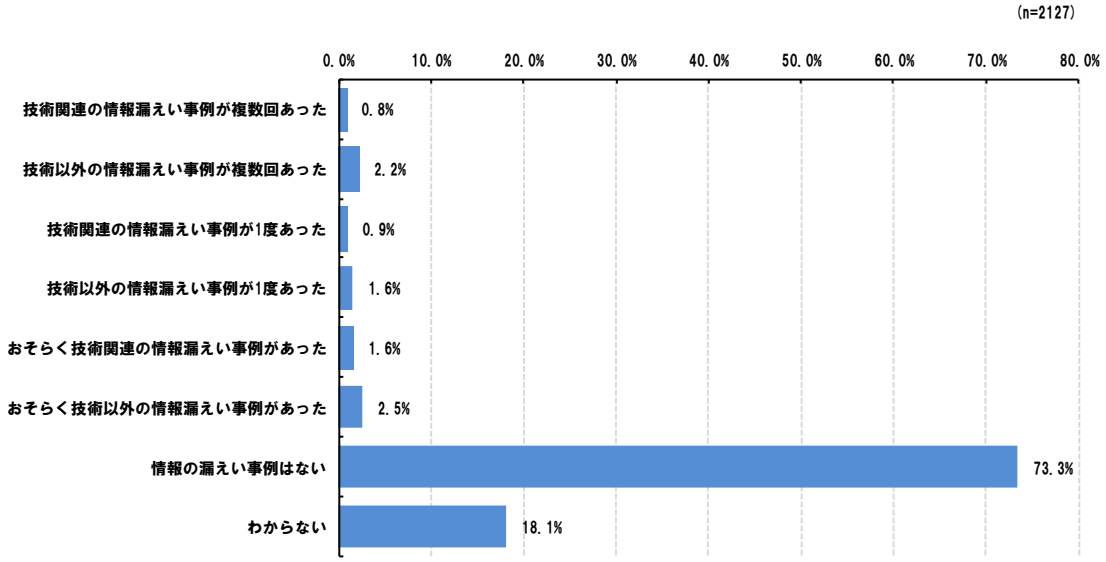

図 2.1-1　過去５年間における営業秘密漏えいの実態（全業種・全規模）（問８）

2012 年度に経済産業省が実施した「営業秘密の管理実態に関するアンケート調査[3]」（以下、過年度アンケート調査と記載）によれば（別冊 P50）、当時は 13.5%程度の企業が過去５年の間に営業秘密の漏えいを経験しており、漏えいを認識している企業の数は相対的に減っている[4]。ただ、過年度アンケート調査と比較すると、「わからない」と回答している企

[3] 経済産業省（委託先：三菱 UFJ リサーチ＆コンサルティング株式会社）「人材を通じた技術流出に関する調査研究報告書（別冊）「営業秘密の管理実態に関するアンケート」調査結果」（平成 25 年 3 月）
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/H2503chousa.pdf

[4] 過年度アンケート調査では、回答を「人を通じた漏えい（役員、従業員、転退職者、取引先、派遣社員等を通じた漏えい）」に限定しているが、本調査ではそうした限定を行わず広い範囲での回答を求めている。したがって、調査結果の単純な比較はできないが、本調査の方が広い範囲での回答となっているという前提を踏まえれば、やはり漏えいを認識した企業が過年度アンケート調査と比較して減っていると解釈することはできる。

業が増えていることから（16.2%→18.1%）、営業秘密が漏えいしたことを認識できていない企業が過年度アンケート調査時点よりも多く存在している。

企業の業種（製造業／非製造業）および規模（301 人以上（以降、大規模と記載）／300 人以下（以降、中小規模と記載））で見ると、「大規模の製造業」が最も多く、14.6%の企業が過去５年間に何らかの営業秘密の漏えいを経験している。また、次いで多いのが「大規模の非製造業」であり、10.3%の企業が漏えいを経験している（図 2.1-2）。

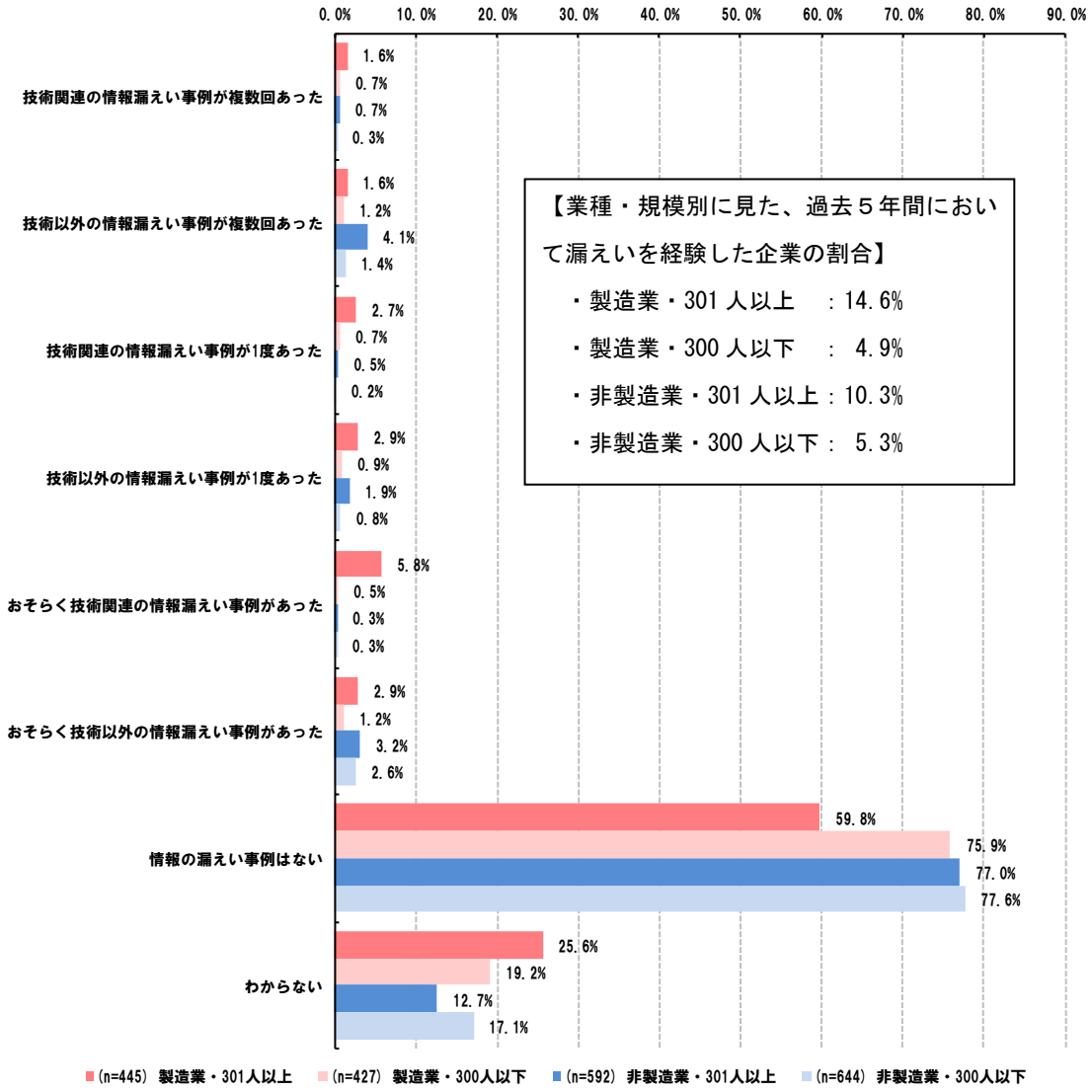

図 2.1-2　過去５年間における営業秘密漏えいの実態（業種・規模別）（問８）

従業員規模別に細かく見てみると、特に従業員数が 3,001 人以上の規模の企業においては、22.7%の企業が過去５年間に営業秘密の漏えいを経験していることがわかる（図 2.1-3）。

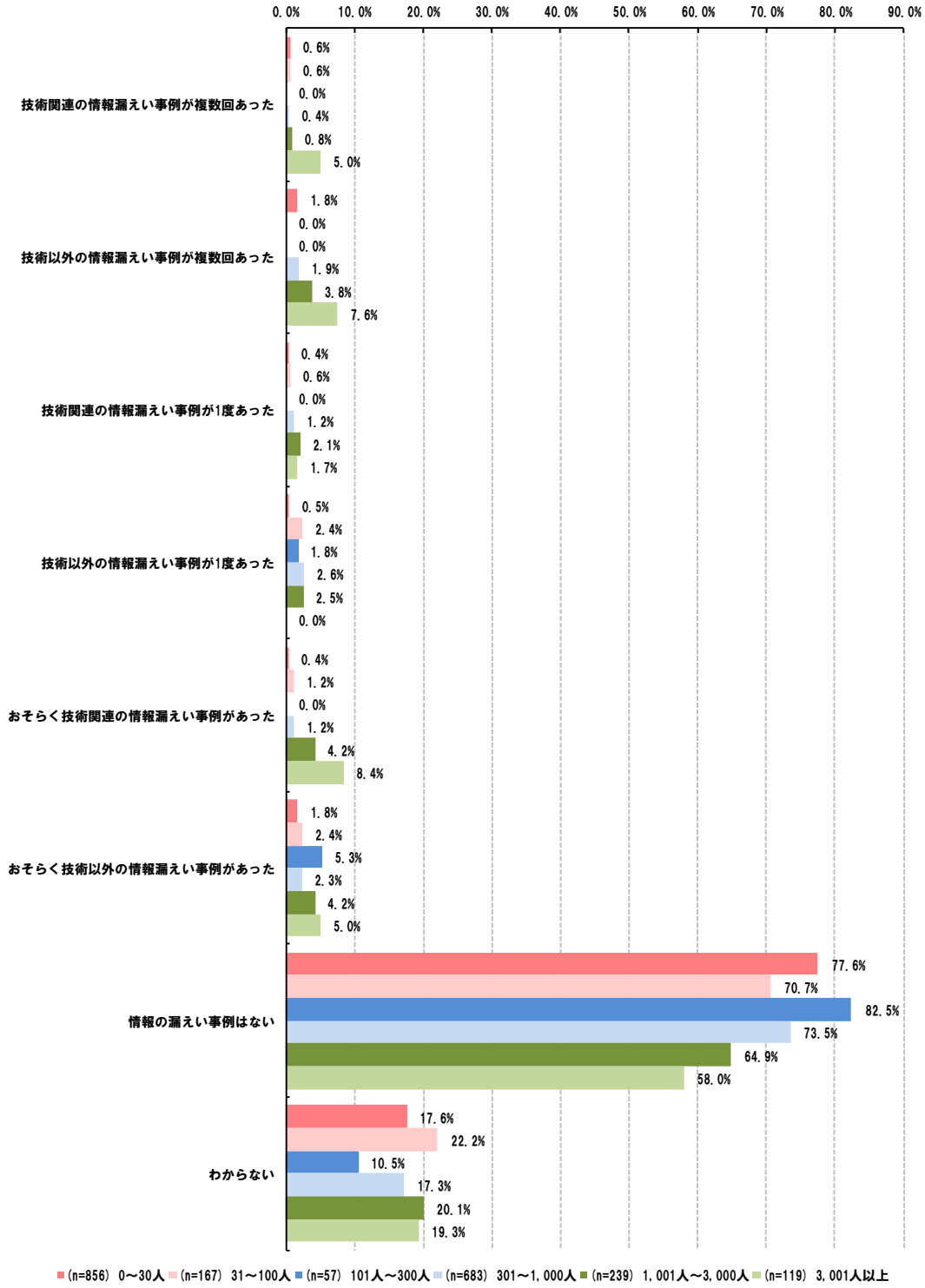

図 2.1-3　過去５年間における営業秘密漏えいの実態（従業員規模別）（問８）

次に、漏えいを経験した企業について、細かく実態を調べる。

2.1.2. 営業秘密の漏えいルート

営業秘密の漏えいが発生した企業に漏えいのルートを聞くと、「現職従業員等によるミス」もしくは「中途退職した正規社員による漏えい」が主なルートとして目立つ傾向が見られる。また、それらと比べて割合は低いが、「取引先や共同研究先を経由した漏えい」や、「現職従業員等による具体的な動機をもった漏えい」も一定数発生していることが窺える。

なお、過年度アンケート調査と比較すると、現職従業員等によるミスが過年度アンケート調査時には 26.9%であったのに対し、今回の調査では 43.8%と大きく増加している。一方、中途退職した正規社員が漏えいしたケースについては、過年度アンケート調査では最も割合が高く 50.3%であったが、今回の調査では 24.8%となっており、減少している。(図 2.1-4)

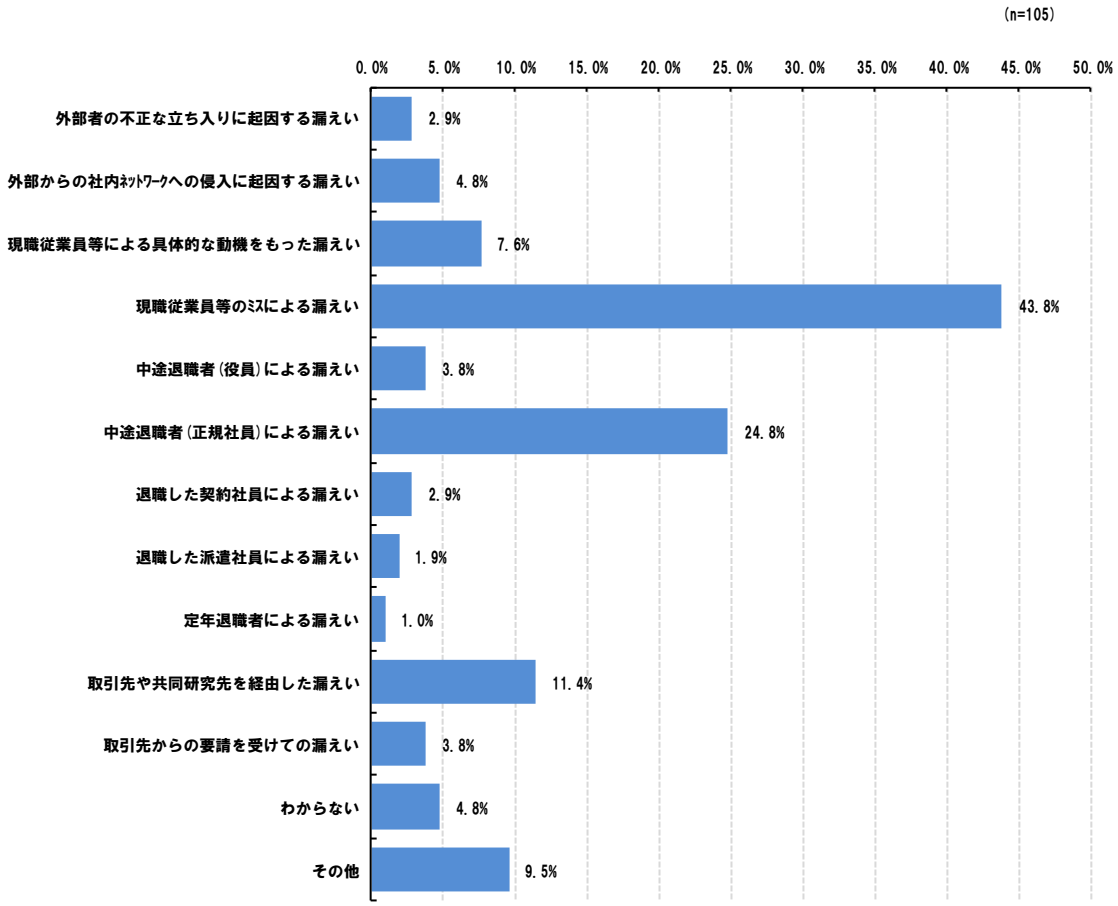

図 2.1-4　営業秘密の漏えいルート（全業種・全規模）（問 13）

業種・規模別に見ると、大規模企業では現職従業員等のミスにより漏えいが発生した割合が高くなっており、特に非製造業の大規模企業では 63.4%となっている。一方で、中小

規模企業においては、中途退職者（正規社員）による漏えいの割合が相対的に高く、製造業で 28.6%、非製造業では 46.7%となっている（図 2.1-5）。現職従業員等のミスによる漏えい発生の割合については大規模企業と中小規模企業の差が大きくなっているが、これは大規模企業において事務的なミスを検知する仕組みや報告のルール等が整備されているために、漏えいの発生を認知できる機会が相対的に多かったということに起因していると捉えることもできる[5]。

[5] 例えば、図 2.2-12 で示されているように、大規模企業は中小規模企業と比較して「情報システムのログを記録・保管している」「外部送信のメールのチェック体制が整っている」等、検知や事後調査が可能となる対策に取り組んでいる割合が高い。

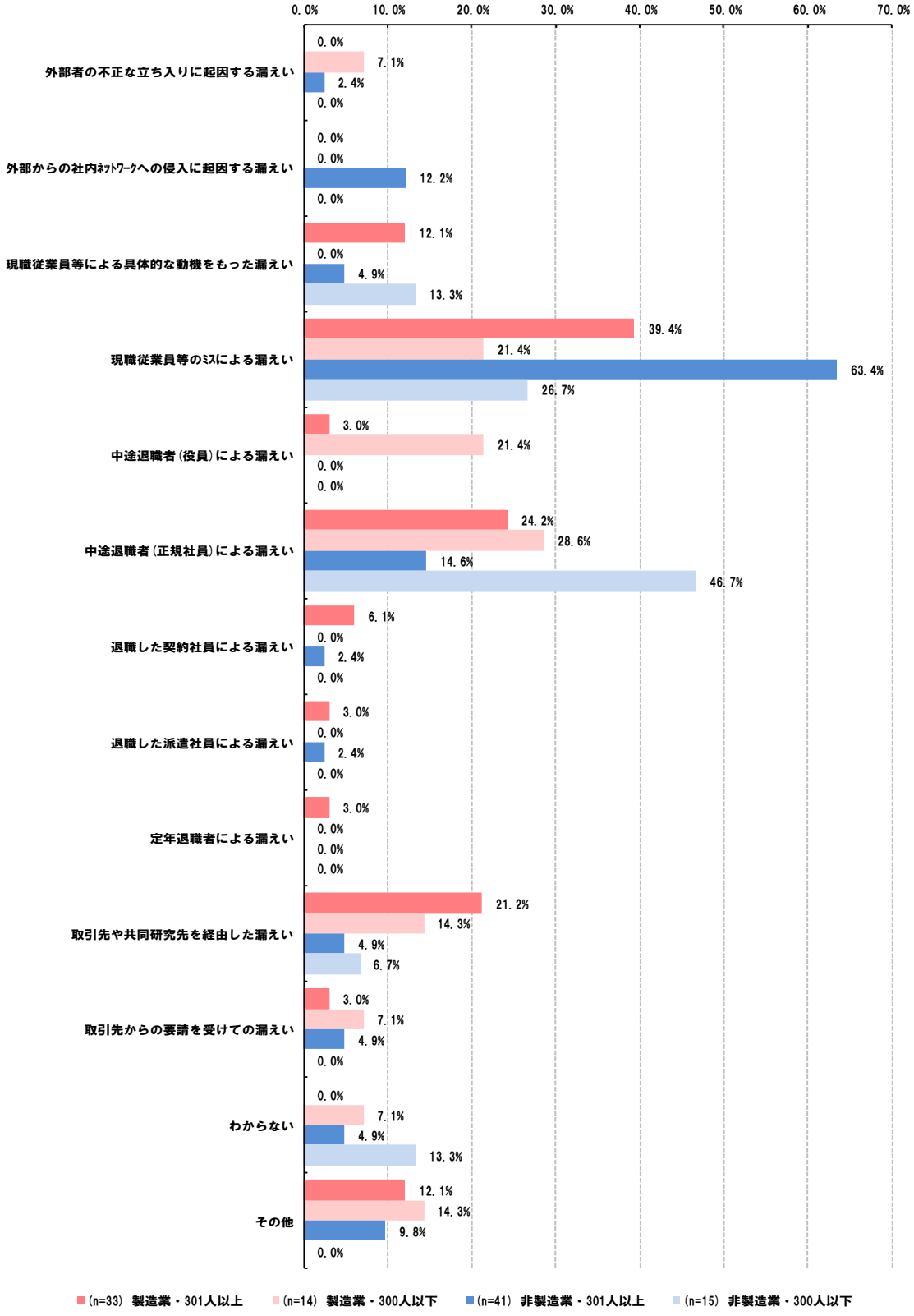

図 2.1-5　営業秘密の漏えいルート（業種・規模別）（問 13）

インタビュー調査においては、現職従業員等のミスによる漏えい事例は聞かれなかったが、中途退職者による漏えいや、他社への安易な技術指導の実施によって漏えいが発生した事例があった。

【営業秘密の漏えいルート（インタビュー調査結果）】
- 技術情報保有者の競合企業への転職に伴う漏えいが発生した。（製造業）
- 親切心から技術指導をしたことがきっかけとなり、営業秘密が外部に漏えいした。類似する製品が上市されたことによって発覚したものである。（製造業）

2.1.3. 営業秘密の漏えい先

営業秘密の漏えい先については、全体的には国内の競合他社というケースが最も多く、32.4%を占めている。また、漏えいしたこと自体は把握できているものの、その漏えい先までは把握できていないケース（わからないと回答したケース）が 22.9%存在している（図 2.1-6）。

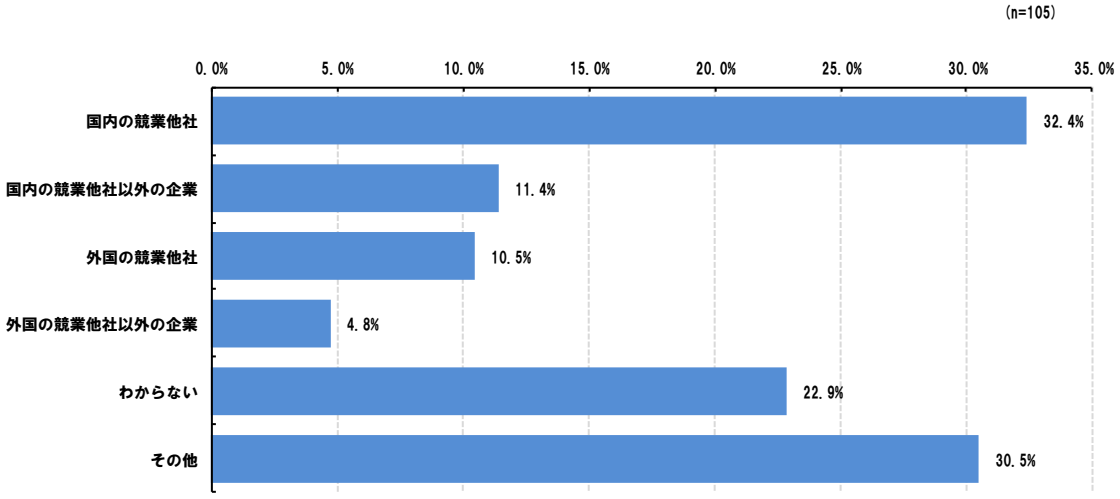

図 2.1-6　営業秘密の漏えい先（全業種・全規模）（問 14）

業種・規模別に見ると中小規模企業では主に国内企業への漏えいが発生している一方で、大規模の製造業では外国企業への漏えいも一定数発生していることが窺える。また、漏えい先を把握できていないケースは企業の規模を問わず一定数存在している（図 2.1-7）。

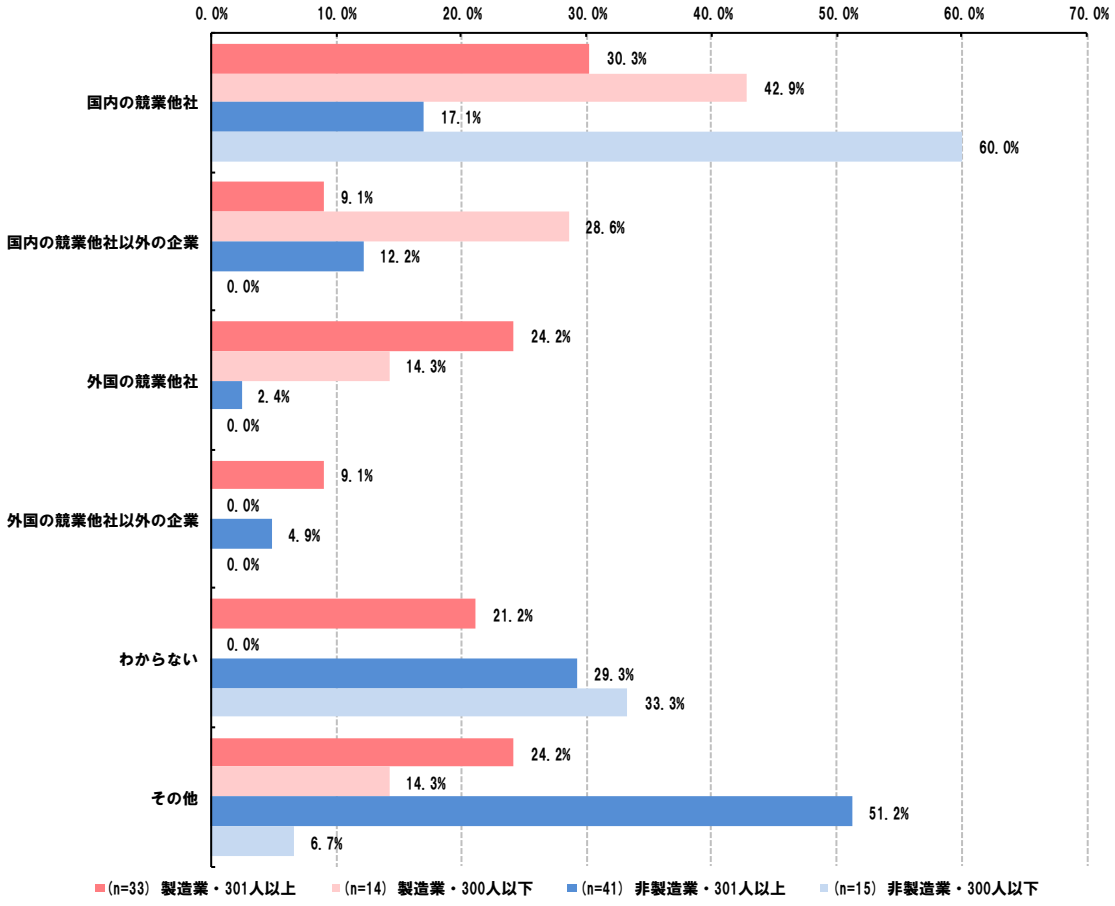

図 2.1-7　営業秘密の漏えい先（業種・規模別）（問 14）

大規模の非製造業については、その他の回答の割合が高く、本アンケート調査結果によれば、顧客に営業秘密が漏えいした例やインターネット上に掲載されてしまった例、社内で関係のない従業員等に開示されてしまった例等が見られた。

【営業秘密の漏えい先：「その他」の回答例（アンケート調査結果）】
- 当社の顧客に情報が渡ってしまった。（非製造業）
- 顧客情報・個人情報がインターネット上に掲載されてしまった。（非製造業）
- 外部ではなく、本来はその情報に触れられない社内の従業員に情報が開示されてしまった。（非製造業）

2.1.4. 営業秘密の漏えいを認識したきっかけ

漏えいを経験した企業においては、全体的には第三者からの指摘もしくは役員・従業員等からの報告によって漏えいを認識する企業の割合が高く、自発的な活動によって漏えいを認識した企業の割合が相対的には低くなっている（図 2.1-8）。

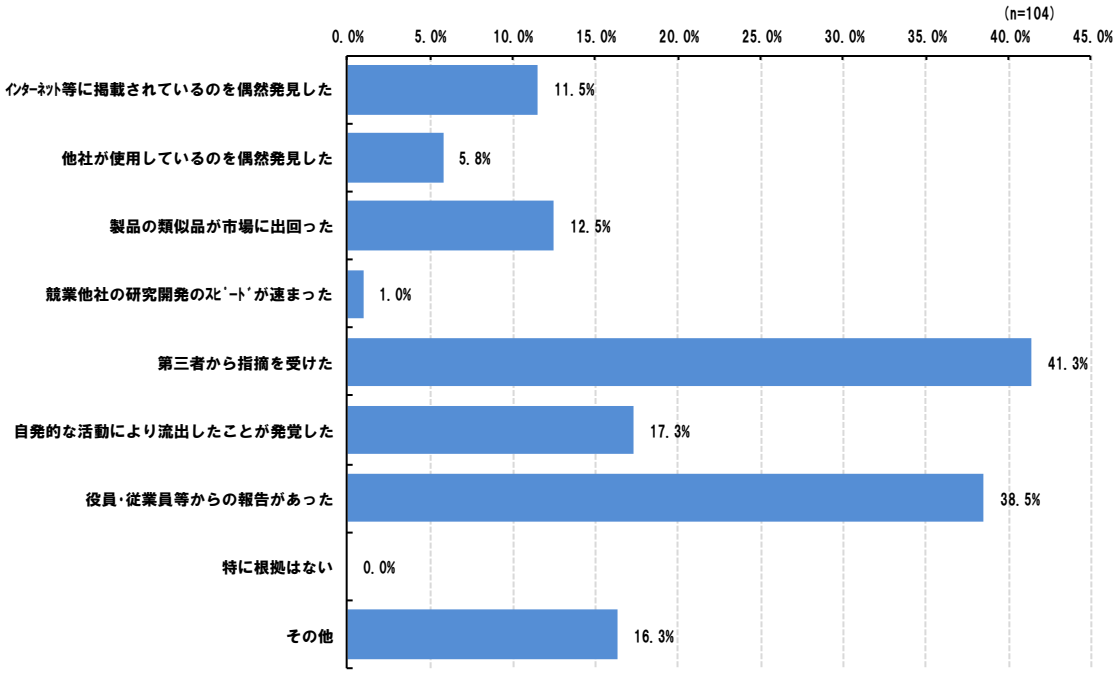

図 2.1-8　営業秘密の漏えいを認識したきっかけ（全業種・全規模）（問 12）

業種・規模別に見ても、全体的な傾向は大きく変わらないが、例えば大規模の製造業では「インターネット等に掲載されているのを偶然発見した」ことで漏えいの発生を認識したケースが相対的に多くなっている。また、中小規模の製造業では類似品が市場に出回ったことや、第三者からの指摘によって漏えいの発生を認識したケースが多いこと等の特徴も見られ、模倣品等の発生が増えている可能性がある（図 2.1-9）。過年度アンケート調査結果と比較すると、特に「第三者から指摘を受けた」と回答している企業の割合が製造業を中心に増加している。特に中小規模の製造業については今回の調査結果では 57.1%であり、過年度調査結果の 23.8%と比べて 30%以上増加している。

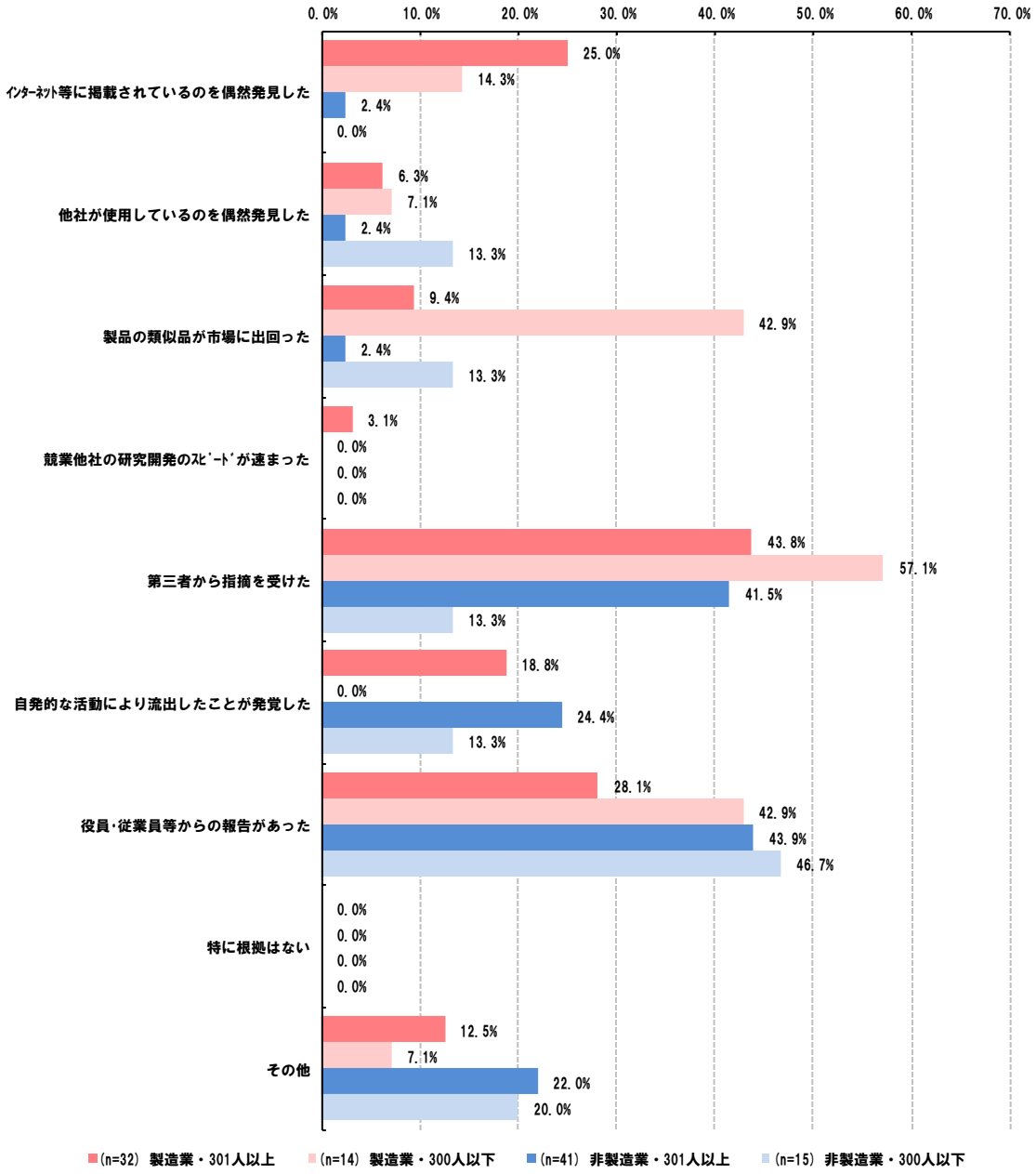

図 2.1-9　営業秘密の漏えいを認識したきっかけ（業種・規模別）（問 12）

2.1.5. 営業秘密の漏えいによる損害の規模

漏えいを経験した企業が認識している損害の規模については、54.3%の企業が「わからない」と回答しており、当該営業秘密の漏えいが自社に対してどの程度の影響があったかを

具体的に把握できていないことが窺える。また、具体的な損害規模を把握できている場合には、1,000 万円未満の規模と回答している割合が最も高く、31.4%となっている（図 2.1-10）。

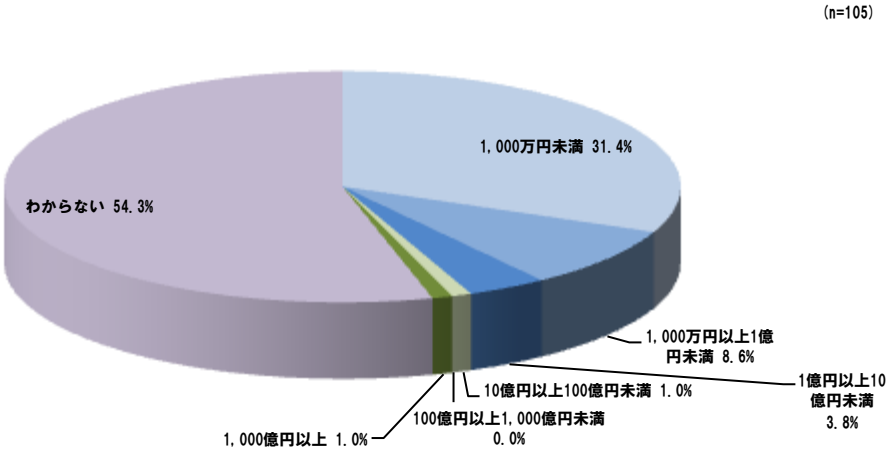

図 2.1-10　営業秘密の漏えいによる損害規模（全業種・全規模）（問 15）

業種・規模別に見ても、大きな傾向は全体と変わらないが、相対的には大規模企業の方が損害規模を把握できていない割合が高く、中小規模の企業では損害額を「1,000 万円未満」と回答している割合が高くなっている。また、大規模の非製造業では相対的に「1,000 万円以上 1 億円未満」と回答している割合の企業が高く、加えて、大規模の製造業では、非常に少数ではあるが、「1,000 億円以上」という非常に高額な損害を認識している企業もあり、営業秘密の漏えいによって、多額の損害が発生している事例もある[6]（図 2.1-11）。

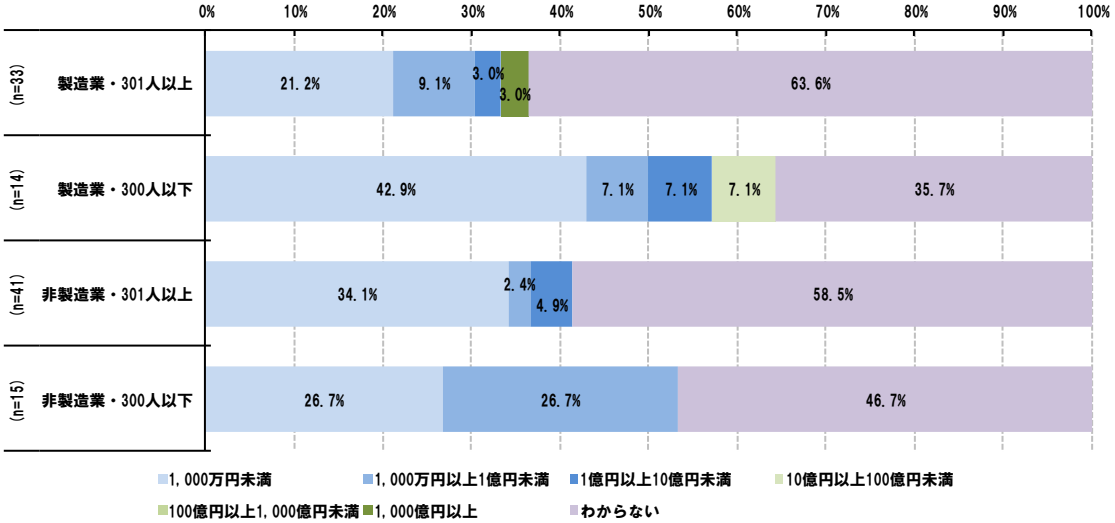

図 2.1-11　営業秘密の漏えいによる損害規模（業種・規模別）（問 15）

[6] 例えば、過去に報じられた事例では、ベネッセホールディングスが個人情報の流出に伴い、原因調査および再発防止策の一環として、200 億円程度を用意して顧客に対する金銭的補償を行うことを発表している。
http://www.benesse-hd.co.jp/ja/about/release_20140717_2.pdf

2.1.6. 営業秘密の漏えいによって被った損害額の内容

図 2.1-10 で、具体的な損害額を認識していた回答者に対して、認識している損害額の内容を尋ねた結果を図 2.1-12 に示す。漏えいによる損害額を認識している企業は、全体としてはその損害額を「自社が得ることができたと想定される利益の額」もしくは「原因調査や再発防止策の費用」と捉えている傾向がある。

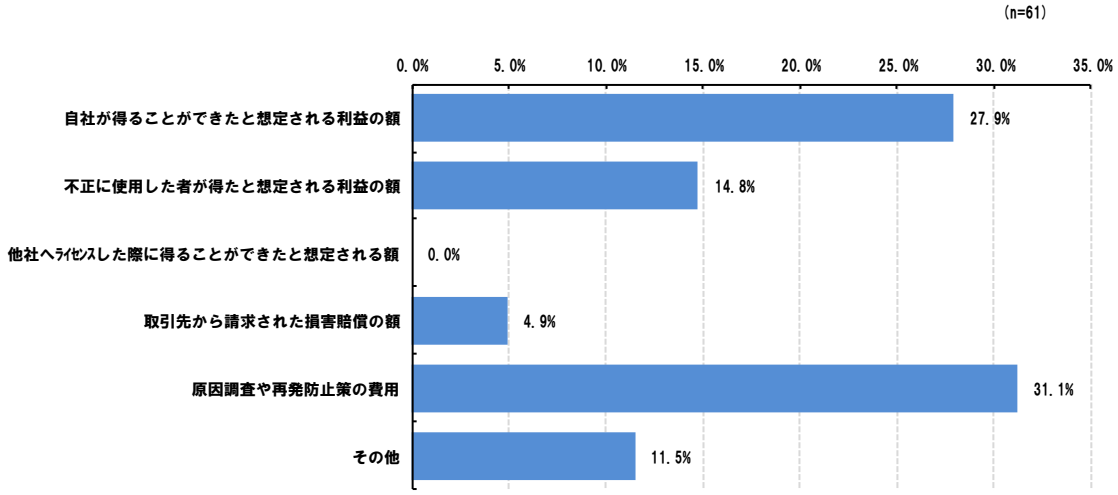

図 2.1-12 営業秘密の漏えいによる損害額の内容（全業種・全規模）（問 16）

業種・規模別に見ると、主に企業の規模によって損害額の算出・推定の方法に差があることが窺える。具体的には、中小規模企業は「自社が得ることができたと想定される利益の額」もしくは「不正に使用した者が得たと想定される利益の額」と回答する割合が高いのに対し、大規模企業では「原因調査や再発防止策の費用」と回答する割合が高く、漏えいを認識するだけではなく、原因調査の徹底や今後の対策等にまで取り組んでいることが窺える（図 2.1-13）。中小規模企業においては、「原因調査や再発防止策の費用」と回答した企業の割合が、大規模企業と比べて相対的に低いが、漏えいした情報の影響の大きさによっては、こうした費用が発生することも認識しておく必要がある。

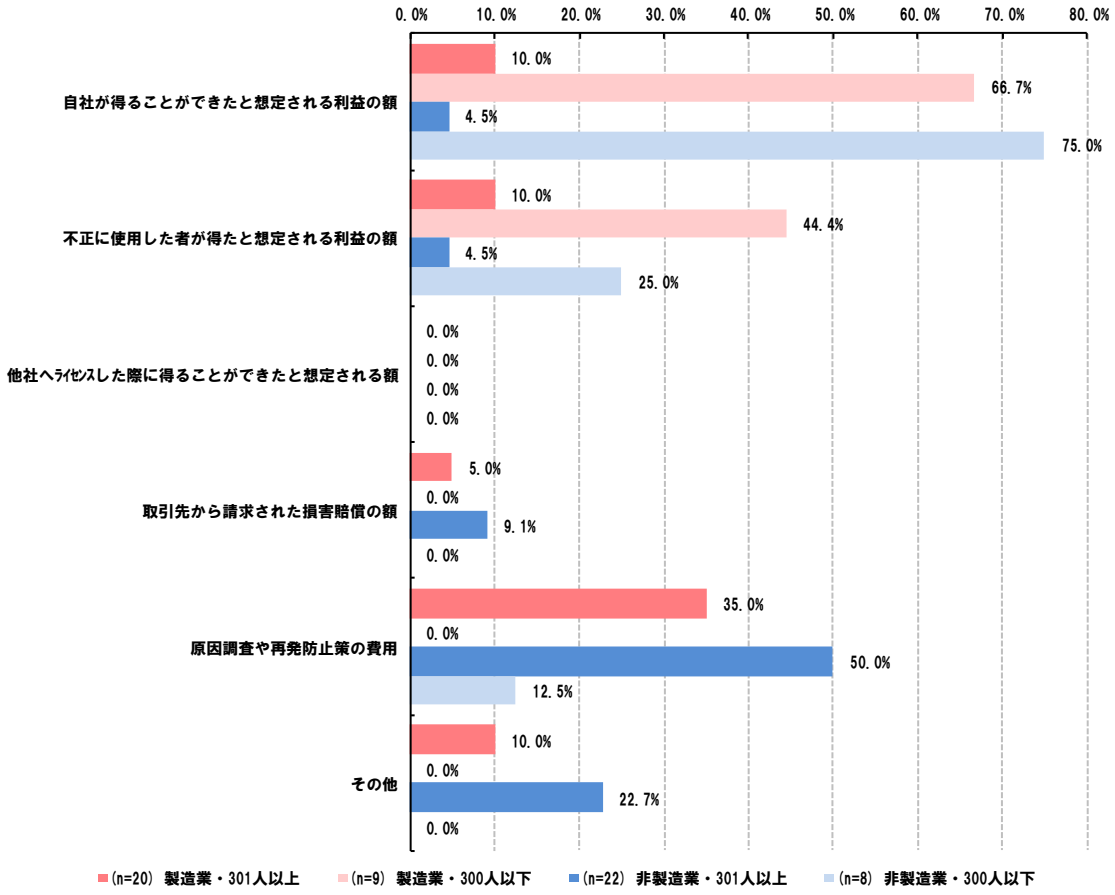

図 2.1-13　営業秘密の漏えいによる損害額の内容（業種・規模別）（問 16）

2.1.7. 営業秘密漏えいの事後対応

本アンケート調査結果によれば、過去５年間に営業秘密の漏えいを経験した企業において、46.6%の企業でしか事実関係の調査が行われていない。また、懲戒処分といった社内処分による対応は 18.4%の企業で実施されているものの、民事的措置や刑事的措置のような司法の場で争ったケースは数%に留まり、ほとんどの営業秘密漏えい事案でこのような対応までは実施されていないことがわかる（図 2.1-14）。

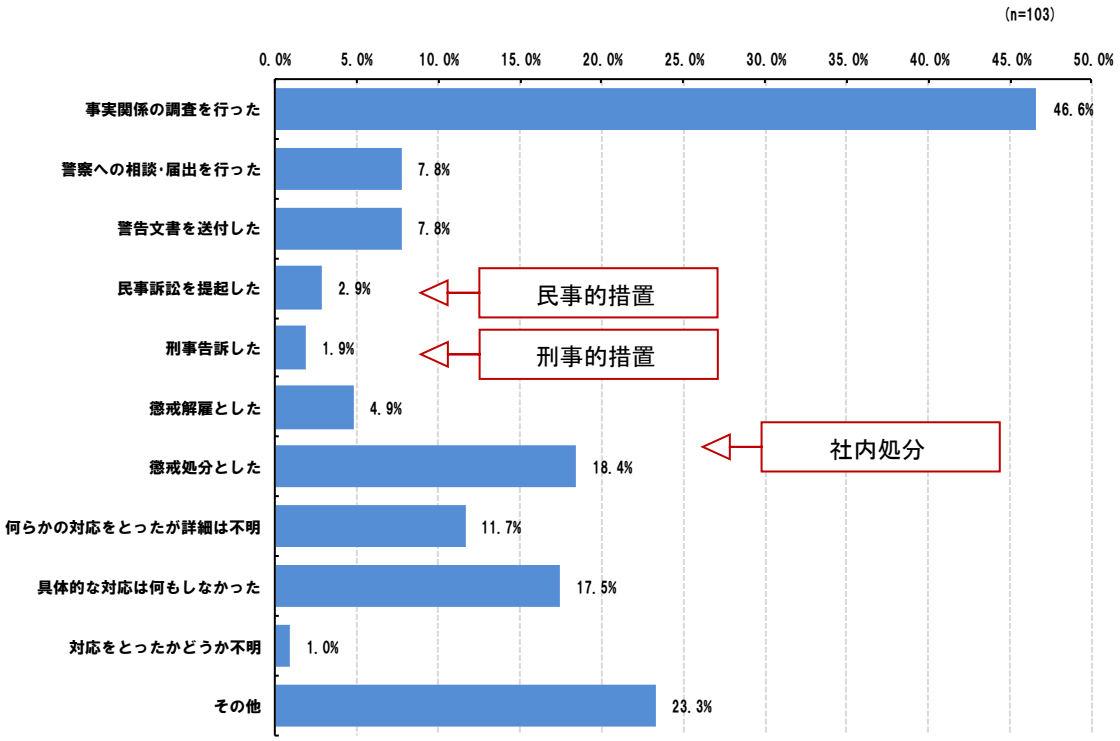

図 2.1-14　営業秘密侵害を行った者への対応（全業種・全規模）（問 17）

特に中小規模企業においては、基本的な事後対応の一つである「事実関係の調査を行った」についても２割程度の企業でしか実施されておらず、相対的に漏えい後の対応が手薄になっている傾向があることが窺える（図 2.1-15）。

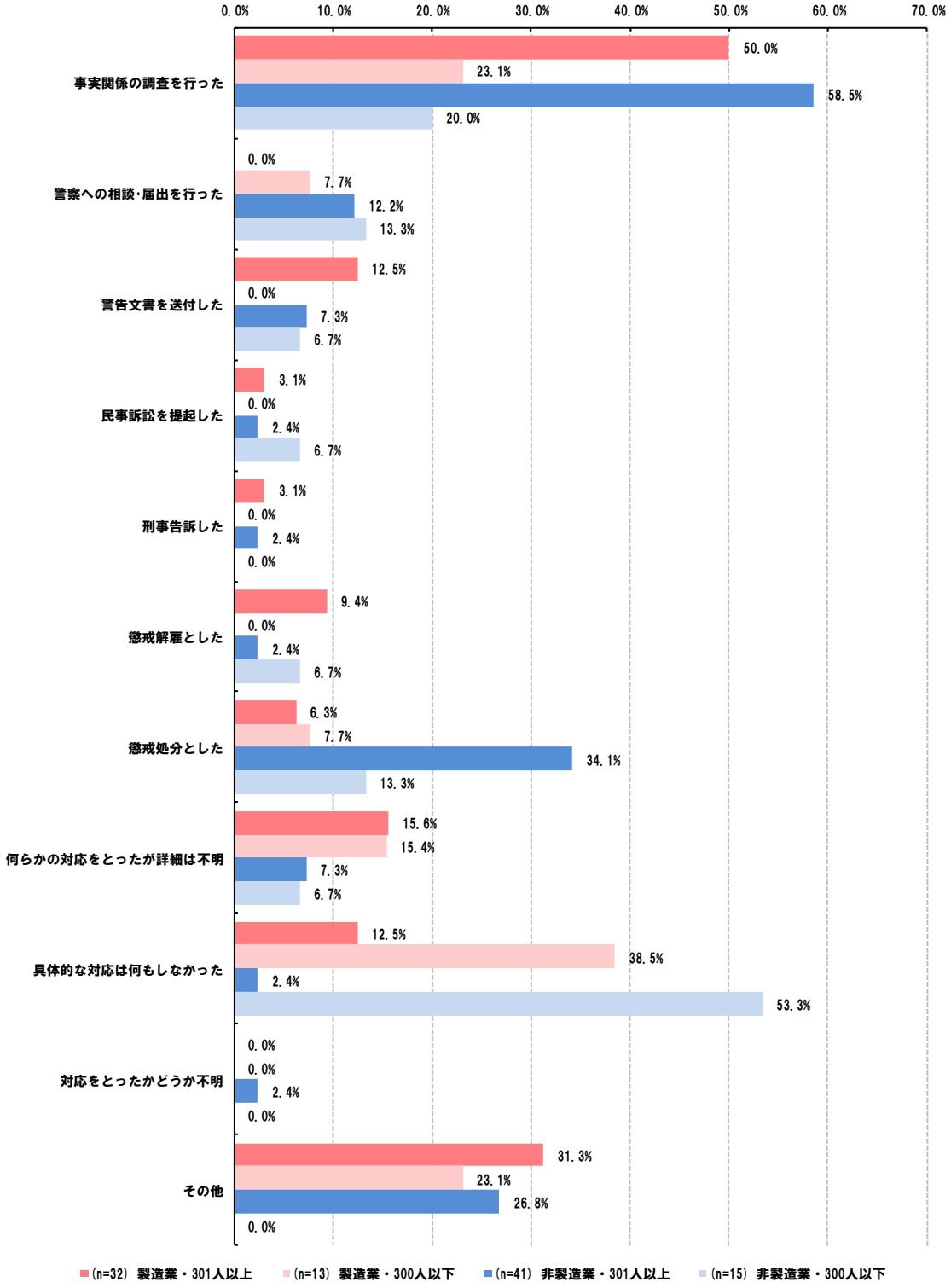

図 2.1-15　営業秘密侵害を行った者への対応（業種・規模別）（問 18）

仮に民事訴訟の提起等の手段による対応を実施したとしても、必ずしも原告の訴えが認められるわけではない。例えば、営業秘密が争点となった訴訟では営業秘密として認められず、訴えが棄却されるケースも多い。これは、原告側が十分に立証できていないことが一つの原因であると考えられ、そのような観点に立つと日頃からエンフォース（法執行）を意識し、証拠となる情報を集めておくことが重要となる。証拠保全に資する取組として、システムログの収集等に代表される検知活動の実施があげられるが、検知活動は証拠保全に資する活動であるだけでなく、未然防止・抑止の効果もあり、漏えいの兆候の事前把握に資する活動でもある。

本アンケート調査結果によれば、50.2%の企業で検知活動が実施されており、うち39.8%の企業では、検知活動を実施していることを従業員等にも周知している（図 2.1-16）。

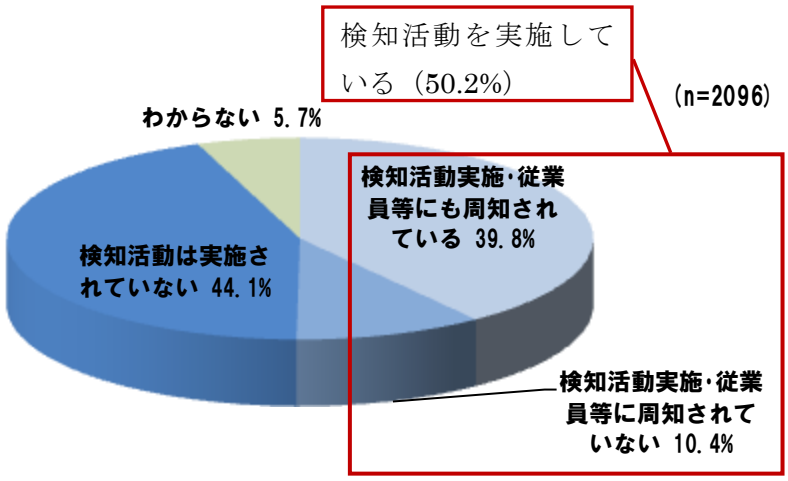

図 2.1-16　検知活動の実施状況（全業種・全規模）（問９）

2.2. 漏えい対策の取組状況

営業秘密の保護に資する対策は物理的な手段やシステム的な手段、人的な手段等、様々なものがこれまで紹介されてきている。平成 28 年 2 月に公表された「秘密情報の保護ハンドブック」によれば、①秘密情報に近寄りにくくするための対策（接近の制御）、②秘密情報の持出しを困難にするための対策（持出し困難化）、③漏えいが見つかりやすい環境づくりのための対策（視認性の確保）、④秘密情報と思わなかったという事態を招かないための対策（秘密情報に対する認識向上）、⑤社員のやる気を高めるための対策（信頼関係の維持・向上等）という５つの手段を組み合わせて実施することが有効であるとされている。従い、これら５つの手段ごとに調査を実施している。

今回実施調査結果によれば、営業秘密の漏えい対策への取組について、以下の実態が明らかになっている。

- 接近制御に資する物理的な対策については、42.3%の企業が「営業秘密を破棄する際には復元が不可能な方法で実施している」と回答している一方で、「営業秘密が保管されている場所に対する入室制限を設けている」という取組については 24.3%の企業でしか実施されていない。
- 接近の制御に資するシステム的な対策については、60.9%の企業が「PC 等の情報端末にはアンチウイルスソフトを導入している」と回答しており、53.7%の企業が「ファイアーウォール等を導入している」と回答している。一方で、「営業秘密を含むファイル等にはパスワードを設定している」については 36.7%の企業でしか実施できていない。
- 持出し困難化に資する物理的な対策については、37.4%の企業で「USB メモリや DVD 等の持ち込み・持ち出しを禁止している」という取組が実施されているが、その他の対策についてはいずれも 15%程度に留まっている。
- 持出し困難化に資するシステム的な対策については、24.2%の企業で「Web メールサイトやアップロードサイト等への接続の制限」が実施されているが、「ノート PC のローカルドライブに業務用資料のコピーを制御」については、4.7%の企業でしか実施されていない。
- 視認性の確保に資する物理的な対策として、39.9%の企業が「不要な書類等の廃棄等、職場全体が整理整頓されている」と回答し、また 37.6%の企業が「社員に社員証等の着用を義務付けている」と回答している。一方で、「座席配置等、職場のレイアウトを工夫している」については、実施している企業の割合が 20.6%に留まっている。
- 視認性の確保に資するシステム的な対策として、42.8%の企業が「情報システムのログを記録・保管している」と回答している。一方で、「不自然なアクセスは、本人に警告される」等、それ以外の対策について取り組んでいる企業の割合は、いずれも１割程

度に留まっている。

- 秘密情報に対する認識向上に資する対策として、36.4%の企業が役員との間で秘密保持契約を締結しており、46.1%の企業が従業員との間で秘密保持契約を締結している。また、35.4%の企業が「社内における営業秘密の取扱ルール等を研修等で周知する」という取組を実施している。
- 信頼性の維持・向上等に資する対策として、21.5%の企業が「自社への帰属意識を高められるようにしている」と回答しており、また 18.3%の企業が「人事評価や表彰制度等でモチベーションを向上させる」と回答している。

2.2.1. 接近制御に資する対策

2.2.1.1. 接近制御に資する物理的な対策

本アンケート調査結果によると、接近制御に資する物理的な対策として、42.3%の企業で「営業秘密を破棄する際には復元が不可能な方法で実施している」という取組が実施されている。一方で、「営業秘密が保管されている場所に対する入室制限を設けている」という取組については、相対的に遅れており、24.3%の企業でしか実施されていない。また、34.0%の企業が「特に何もしていない」と回答している（図 2.2-1）。

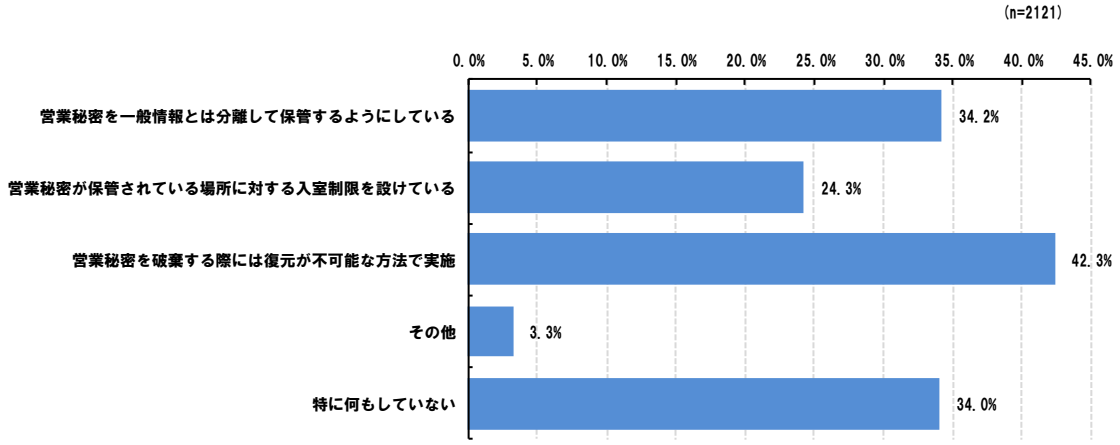

図 2.2-1 営業秘密への接近制御に資する物理的な対策への取組状況（全業種・全規模）（問31）

入室制限に関する取組について、インタビュー調査においては、エリアに対して区分を設けた上で、その区分に応じた入室制限を設けている事例があった。

【入室制限に関する取組例（インタビュー調査結果）】
- 機密エリア、執務エリア、商談エリアを区分けしており、立ち入り制限のみならず、各エリアで利用・保管できる情報も制限されている。（非製造業）
- 入室制限に関するアクセス区分として、制限が厳格なものからアクセス制限エリア、オフィスエリア、ゲストエリア、一般エリアとして、４つの区分を設けている。（製造業）

2.2.1.2. 接近制御に資するシステム的な対策

接近制御に資するシステム的な対策については、60.9%の企業で「PC 等の情報端末にはアンチウイルスソフトを導入している」、53.7%の企業で「ファイアーウォール等を導入している」という取組が実施されている。一方で、「営業秘密を含むファイル等にはパスワードを設定している」という取組については 36.7%の企業でしか実施できていない。また、20.1%企業が「特に何もしていない」と回答している（図 2.2-2）。

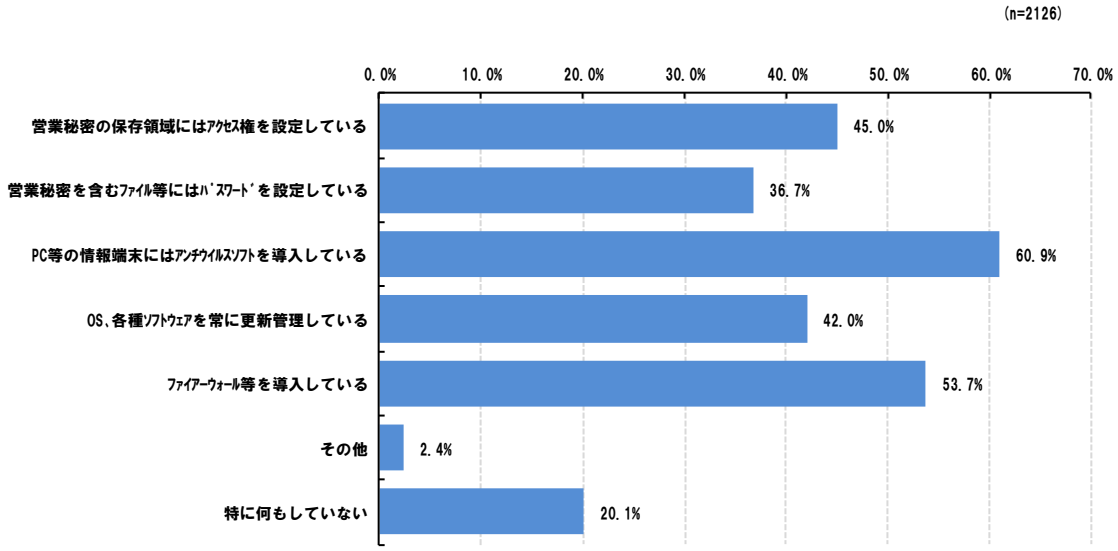

図 2.2-2 営業秘密への接近制御に資するシステム的な対策への取組状況（全業種・全規模）（問 32）

業種・規模別に見ると、いずれの対策についても大規模企業と中小規模企業との間で取組状況に大きな差があることがわかる。アンチウイルスソフトやファイアーウォールの導入といった基本的な対策でさえ、中小規模企業においては３～４割程度しか実施されていない。また、営業秘密の保存領域へのアクセス権の設定についても、中小規模企業では１～２割程度という実施状況となっている。一方、営業秘密を含むファイル等へのパスワードの設定については、大規模企業においても５割前後の実施状況となっており、必ずしも徹底した対策が実施されていないことが窺える（図 2.2-3）。

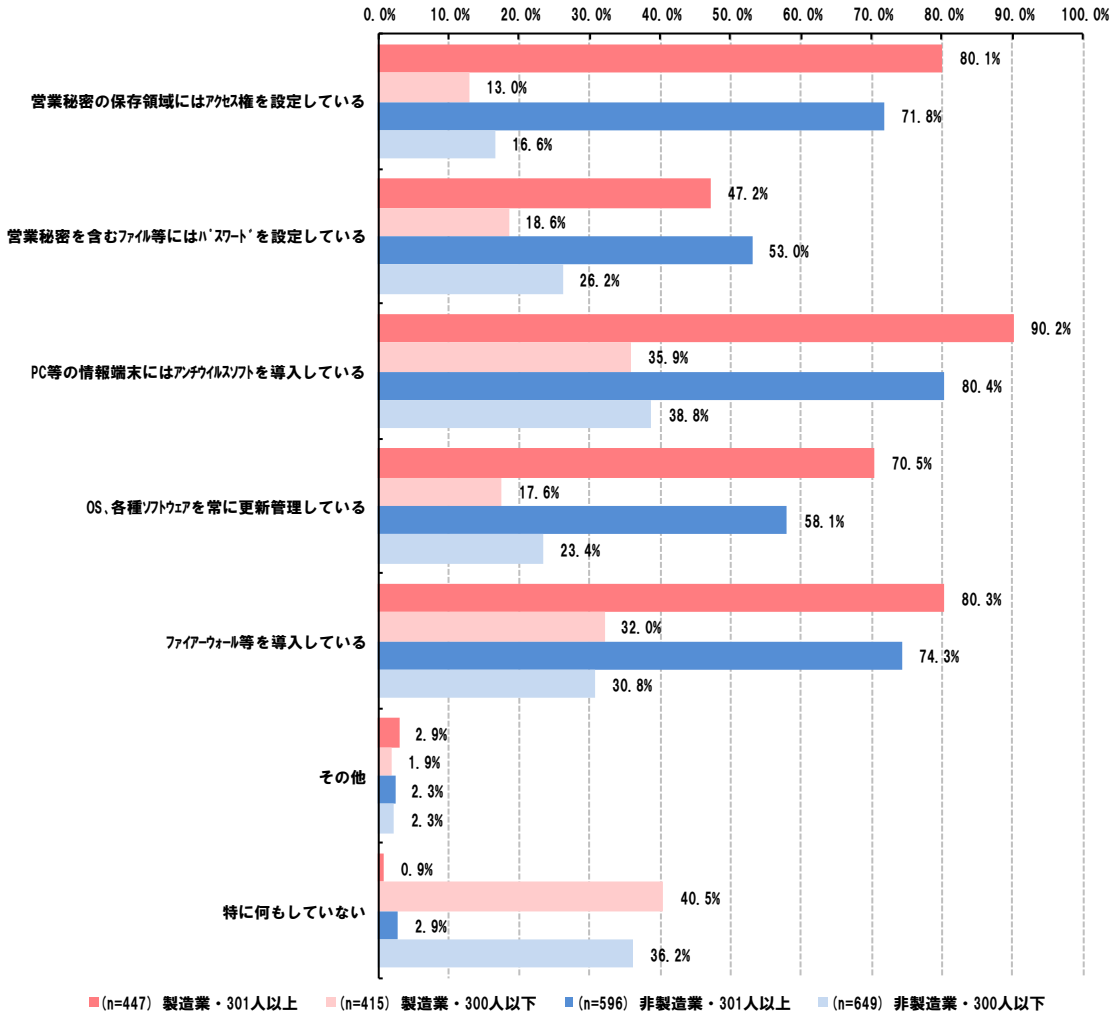

図 2.2-3　営業秘密への接近制御に資するシステム的な対策への取組状況（業種・規模別）（問 32）

なお、営業秘密への接近制御に資するシステム的な対策への取組状況を従業員規模別に細かく見てみると、101 人以上の規模の企業であれば、「OS、各種ソフトウェアを常に更新管理している」を除いて、5 割以上の企業で実施できているが、100 人以下の企業については「PC 等の情報端末にはアンチウイルスソフトを導入している」という基本的な対策を除いて、どの対策についても実施できている企業の割合は 4 割に満たない（図 2.2-4）。この点について、法律専門家へのインタビュー調査によれば、「小規模の企業については、一人の担当者が複数の業務を担当していることが多いため、個々の業務に対しては十分なリソースを割けない状況にあり、どうしても実施できる取組が限定的になってしまう。」との指摘があった。今回の調査結果と照らし合わせても、特に 100 人以下の企業においては、例えば「営業秘密の保存領域にはアクセス権を設定している」等のシステム的な対策にまで

十分にリソースを割けていない状況にあることが窺える。

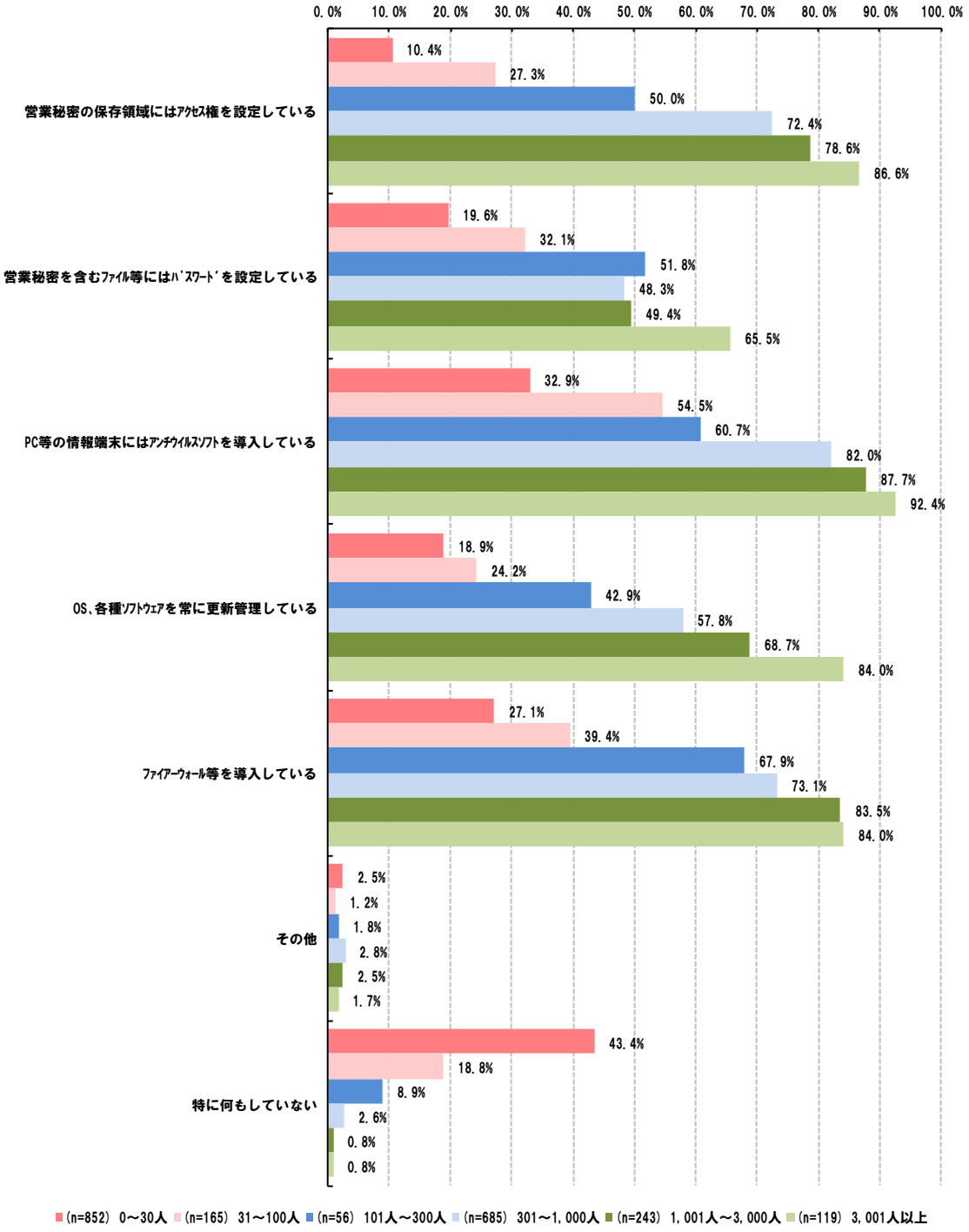

図 2.2-4　営業秘密への接近制御に資するシステム的な対策への取組状況（従業員規模別）（問 32）

インタビュー調査においては、特にアクセス権限の設定については基本的には情報区分に応じてアクセスできる者が定められており、また情報の種類によっては関与している事業部門やプロジェクトチーム、あるいは個別に定めた社員のみがアクセスできるように設定する等、ある程度厳格に運用されている事例があった。

【営業秘密へのアクセスをシステム的に制御する取組例（インタビュー調査結果）】
- 営業秘密を含むファイルを格納するフォルダ単位で管理がなされており、それぞれに対してアクセスできる者を制限している。（非製造業）
- フォルダへのアクセスとデータファイルは ID とパスワードによって管理を行っている。個々人の PC ごとに ID・パスワードを付与し、その ID とパスワードを通じて認証される仕組みである。（製造業）

2.2.2. 持出し困難化に資する対策

2.2.2.1. 持出し困難化に資する物理的な対策

本アンケート調査結果によると、持出し困難化に資する物理的な対策については、37.4%の企業で「USB メモリや DVD 等の持ち込み・持ち出しを禁止している」という取組が実施されている。一方で、それ以外の対策についてはいずれも 15%程度に留まっている。また、43.0%の企業が「特に何もしていない」と回答している（図 2.2-5）。

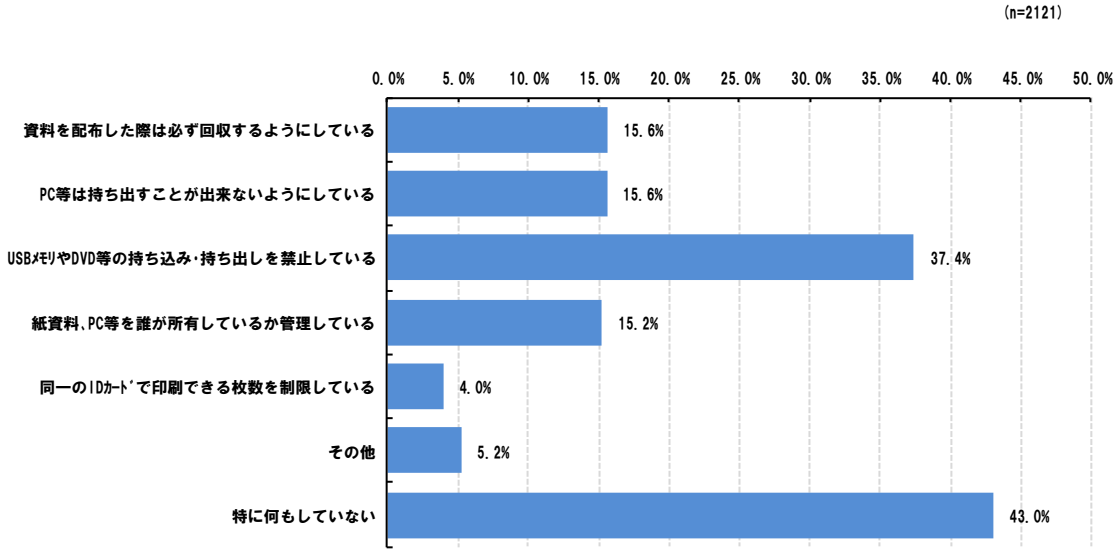

図 2.2-5 営業秘密の持出し困難化を目的とした物理的な対策への取組状況（全業種・全規模）（問 33）

インタビュー調査においては、先のグラフに列挙されている対策には含まれていないが、そもそも印刷自体を原則禁止としている例があった。

【営業秘密の持出しを困難化する対策例（インタビュー調査結果）】
- プリントアウトは原則不可としている。一部の上席社員はプリントアウト可能だが、印刷物に対して、印刷者を特定できる文字等が一緒に印字される仕組みになっており、またプリントアウトログもとっているため、持出しが発生した際には故意によるものとしか考えられない仕組みになっている。（製造業）

2.2.2.2. 持出し困難化に資するシステム的な対策

持出し困難化に資するシステム的な対策については、他の対策と比べて相対的に遅れていることが見受けられ、「Web メールサイトやアップロードサイト等への接続の制限」が最も多くの企業で実施されているものの 24.2%に留まる。また、「社内 PC に USB メモリ等を接続することを制御」「メールに添付できない設定や送信容量の制限などの制御」については、それぞれ 23.9%、22.7%となっている。一方で、「ノート PC のローカルドライブへのファイルコピー制御」については、4.7%の企業でしか実施されておらず、取組が進んでいないことが窺える。また、51.5%の企業で「特に何もしていない」という回答がなされている（図 2.2-6）。

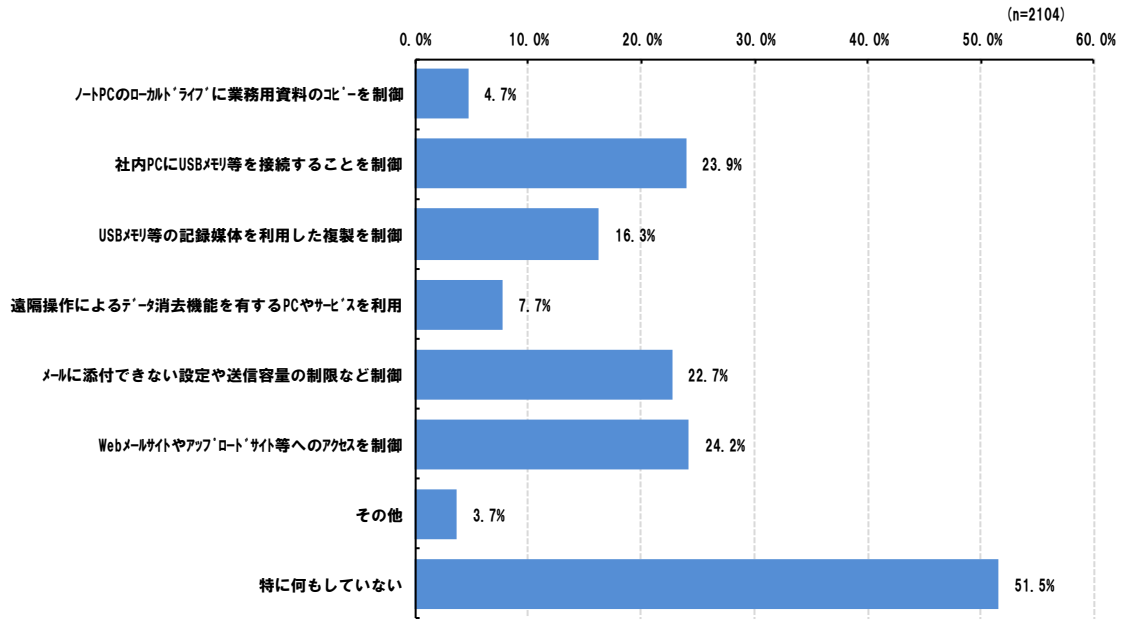

図 2.2-6　営業秘密の持出し困難化を目的としたシステム的な対策への取組状況（全業種・全規模）（問 34）

業種・規模別に見ると、やはり大規模企業と中小規模企業との間で取組状況に大きな差が見られ、特に「社内 PC に USB メモリ等を接続することを制御」「メールに添付できない設定や送信容量の制限などの制御」「Web メールサイトやアップロードサイト等への接続の制限」については 30%以上の差が見られる。一方で、「ノート PC のローカルドライブに業務用資料のコピーを制御」については大規模企業においても実施している企業が 1 割にも満たず、必ずしも十分にシステム的な対策が実施されている状況ではないことが窺える（図 2.2-7）。

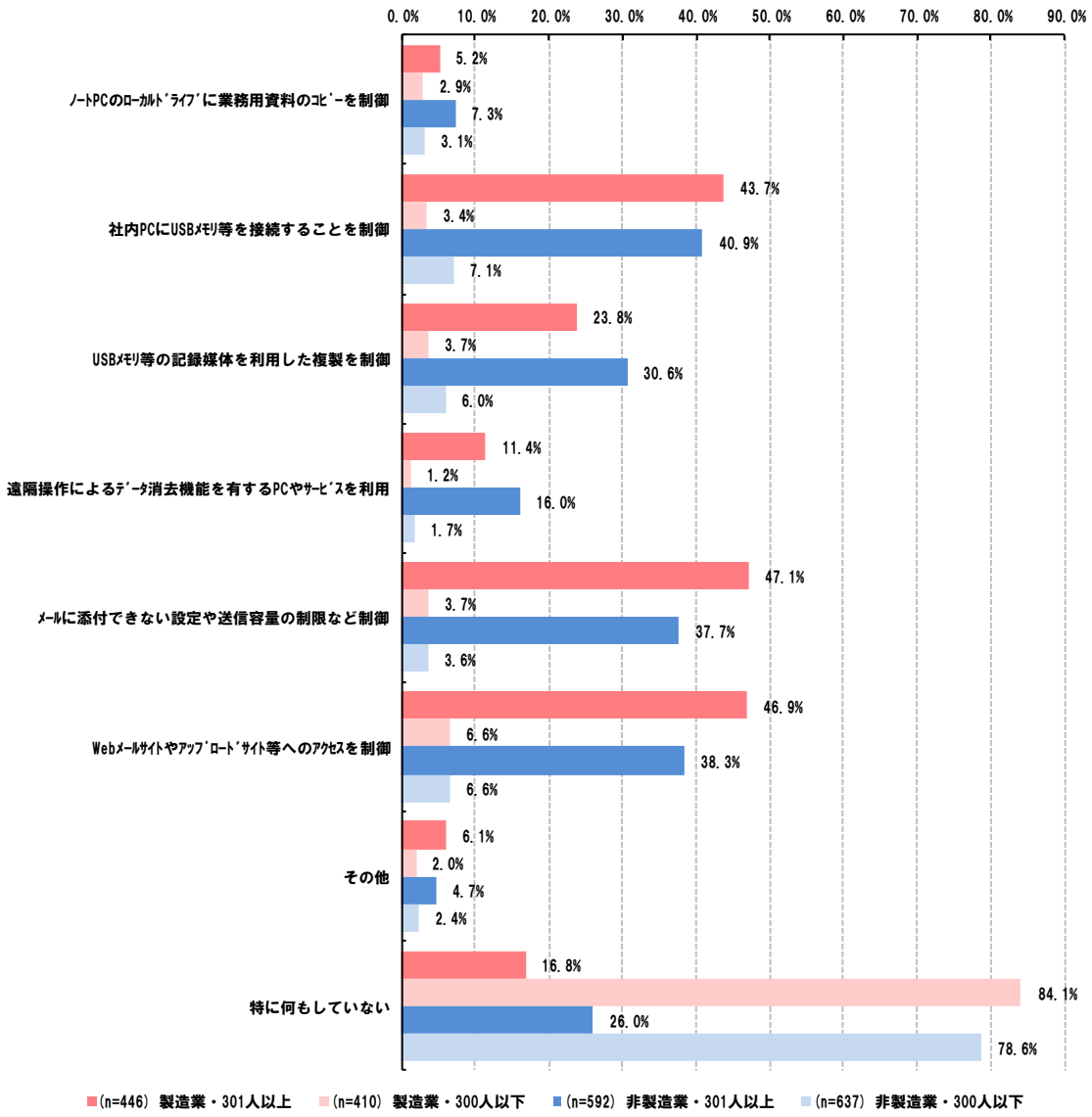

図 2.2-7　営業秘密の持出困難化を目的としたシステム的な対策への取組状況（業種・規模別）（問 34）

営業秘密の持出困難化を目的としたシステム的な対策への取組状況について、従業員規模別に細かく見てみると、やはり 100 人以下の企業については 101 人以上の規模の企業と比べて、相対的に対策に取り組めていないことが見受けられる。例えば、「社内 PC に USB メモリ等を接続することを制御」「USB メモリ等の記録媒体を利用した複製を制御」「メールに添付できない設定や送信容量の制限などの制御」といった対策については、100 人以下の企業と 101 人以上の企業の取組状況に大きな差が見られる（図 2.2-8）。

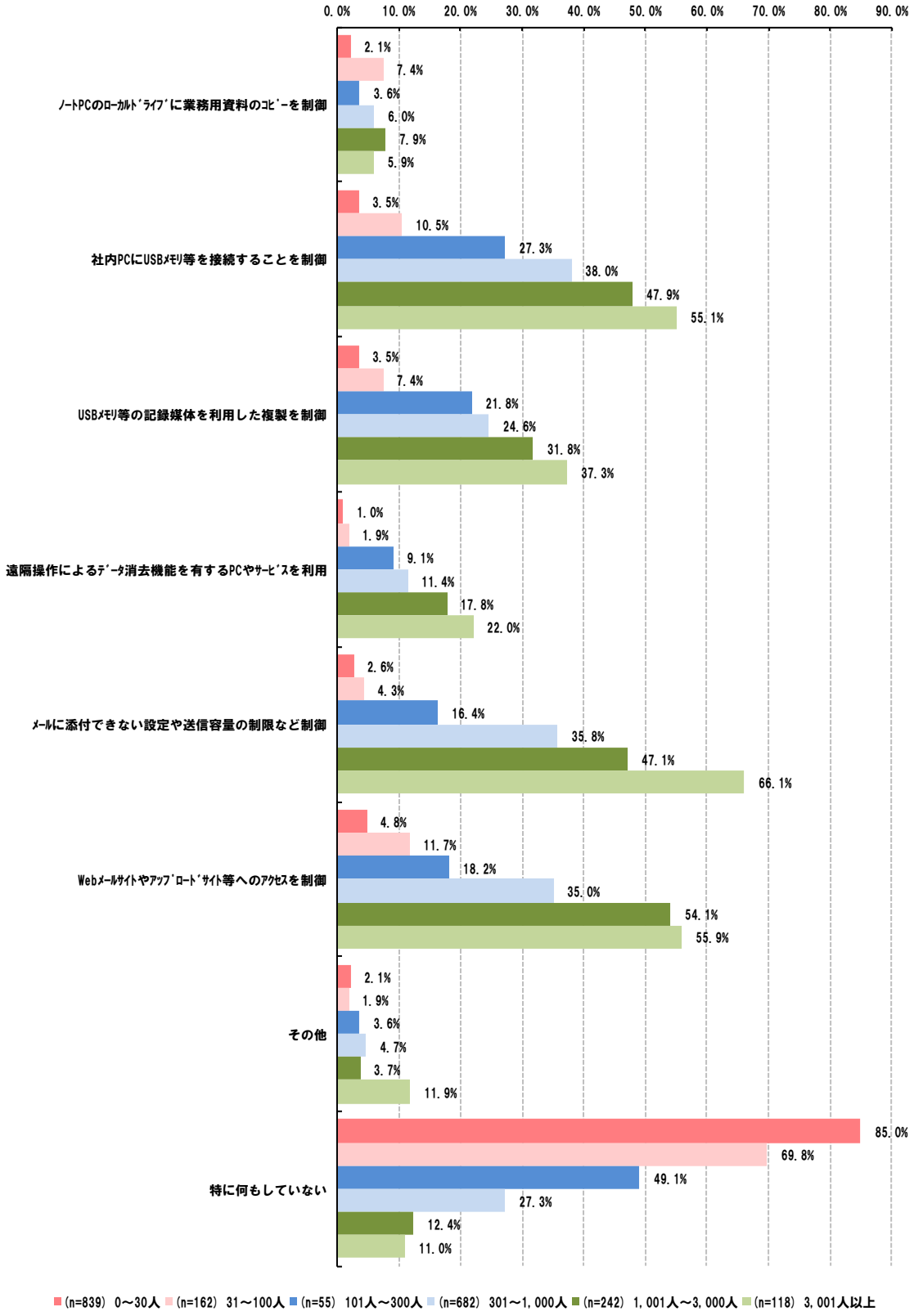

図 2.2-8　営業秘密の持出困難化を目的としたシステム的な対策への取組状況（従業員規模別）（問 34）

「ノート PC のローカルドライブに業務用資料のコピーを制御」については、インタビュー調査において、具体的な手法として、PC のシャットダウン時に自動的にデータを削除するソフトウェアを導入している例があった。

【ノート PC のローカルドライブへの資料コピーをシステム的に制御する対策例（インタビュー調査結果）】

- 外部に持ち出す PC については、シャットダウン時に自動的にローカルドライブ上のデータを削除するソフトを導入し、万一の紛失等に伴う情報の流出を防止している。（製造業）
- ローカルドライブへの電子データの保存はシステム上できなくしている。（非製造業）

また、ノート PC のローカルドライブへの資料コピーをシステム的には制御できていないが、コピーする際には必ずパスワードをかけることをルール上規定している例も見られた。

【ノート PC のローカルドライブへの資料コピーをルールで制限している例（インタビュー調査結果）】

- データを PC のローカルドライブに保存することは可能となっており、ルール上はデータファイルにパスワードをかけることになっているが、自動的にパスワードがかかる仕組みではないため、実質的にはパスワードをかけていないファイルをローカルドライブに保存することは可能となってしまっている。（非製造業）

USB メモリの使用については、システム的な使用を制御している例が見られた一方で、ルール上は USB メモリの利用を禁止しているものの業務上やむを得ない場合もあるため一律禁止とすることが困難であると感じている例も見られた。

【USB メモリの使用に関する例（インタビュー調査結果）】

（USB メモリの使用をシステム的に制御）

- USB メモリ接続をした場合にアラートが発生し、書き込みを制御する仕組みになっているため、PC に USB メモリを接続してデータを持ち出すことは、システム的にできないようになっている。（非製造業）

（ルール上管理）

- 自動暗号化機能の USB メモリを貸与し、その他の私有 USB メモリ等を、PC 等ネットワークに繋がる端末に接続することは、ルール上は禁止している。し

かしながら、会社が貸与した USB メモリ以外の媒体を業務上やむを得ない理由で使用するケースがあり、会社が貸与した USB メモリ以外の使用を一律に禁止することはできないため、USB メモリとのデータ授受のログを監視することで対処している。（製造業）

また、Web メールサイト等の特定の外部サイトに対するアクセスを制限している例も見られた。

【特定の Web サイトへのアクセス制限について（インタビュー調査結果）】
- クラウドファイル共有サービスやウェブメール等、特定の外部サイトに対して、フィルタリングを導入してアクセスを制限している。（製造業）

一部の企業では、遠隔操作によって情報機器に保存されたデータを消去する機能を導入している例が見られた。

【遠隔消去機能の導入について（インタビュー調査結果）】
- スマホやタブレット端末に保存されたファイルの遠隔消去ソフトを導入している。ルール上、ローカルドライブにファイルを保存することは禁止しているが、メール添付ファイルを閲覧する際に一時的にファイルが保存されるケース等があるため、二重の対策として営業で使用するスマートフォンやタブレット端末に遠隔消去ソフトを導入している。（製造業）

2.2.3. 視認性の確保に資する対策

2.2.3.1. 視認性の確保に資する物理的な対策

本アンケート調査結果によると、視認性の確保に資する物理的な対策として、39.9%の企業が「不要な書類等の廃棄等、職場全体が整理整頓されている」と回答し、37.6%の企業が「社員に社員証等の着用を義務付けている」と回答している。一方で、「座席配置等、職場のレイアウトを工夫している」については、実施している企業が 20.6%に留まっている。また、32.9%の企業が「特に何もしていない」と回答している（図 2.2-9）。

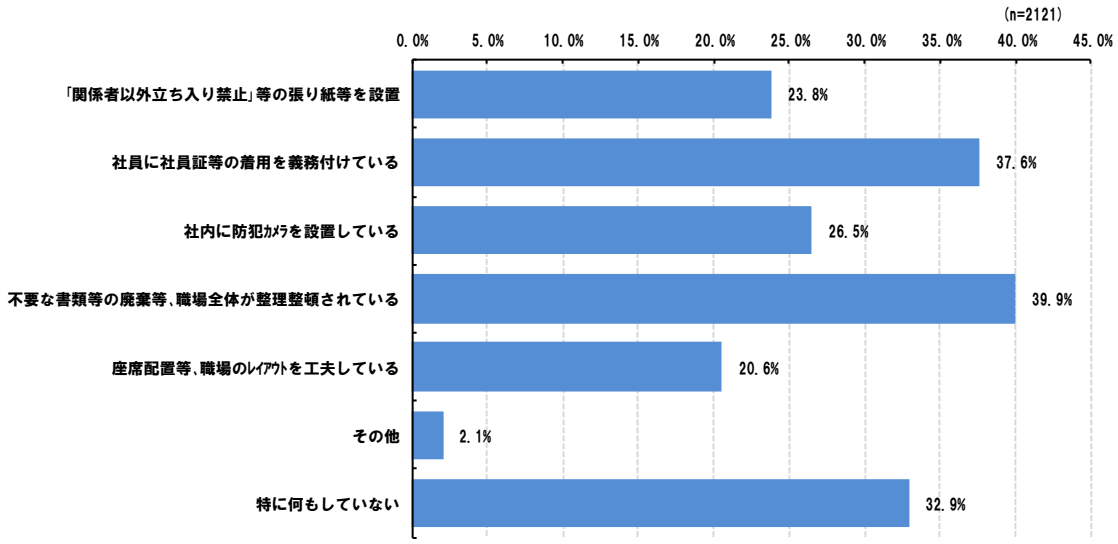

図 2.2-9 視認性の確保に資する物理的な対策への取組状況（全業種・全規模）（問 35）

このうち、防犯カメラの設置については、インタビュー調査においては、研究拠点や工場等の製造拠点等に設置している例が見られた。また、カメラについては、情報管理というよりは製造工程における品質管理等を目的としていたというケースもあった。

【防犯カメラの設置について（インタビュー調査結果）】
- 研究開発拠点では、入室制限の実施に加えて監視カメラの設置も行っている。（製造業）
- 監視カメラについては、もともとは情報管理というよりも、異物混入の確認等、生産管理を目的とした映像記録のために設置したものである。（製造業）
- オフィスの入口やメインエリアに監視カメラを設置している他、外部者の侵入対策として製造工程の一部にもカメラを設置しているが、情報管理というよりは品質管理の徹底を図る目的で実施している。（製造業）

業種・規模別に見ると、やはり大規模企業と中小規模企業との間で取組状況に大きな差が見られ、中小規模企業においては「社員証等の着用の義務付け」についても 1 割以下の企業でしか実施されていない。また、「「関係者以外立ち入り禁止」等の張り紙等の設置」については、大規模企業の中でも業種によって取組状況に差が見られ、製造業では 57.9%の企業で実施されているのに対し、非製造業では 24.1%となっている（図 2.2-10）。製造業では特に研究所や工場等の中で機微な情報を扱うケースがあることに起因していることが

推察されるが、規模の大きな企業であっても、個別の対策については業種によって取組状況に差があることが窺える。

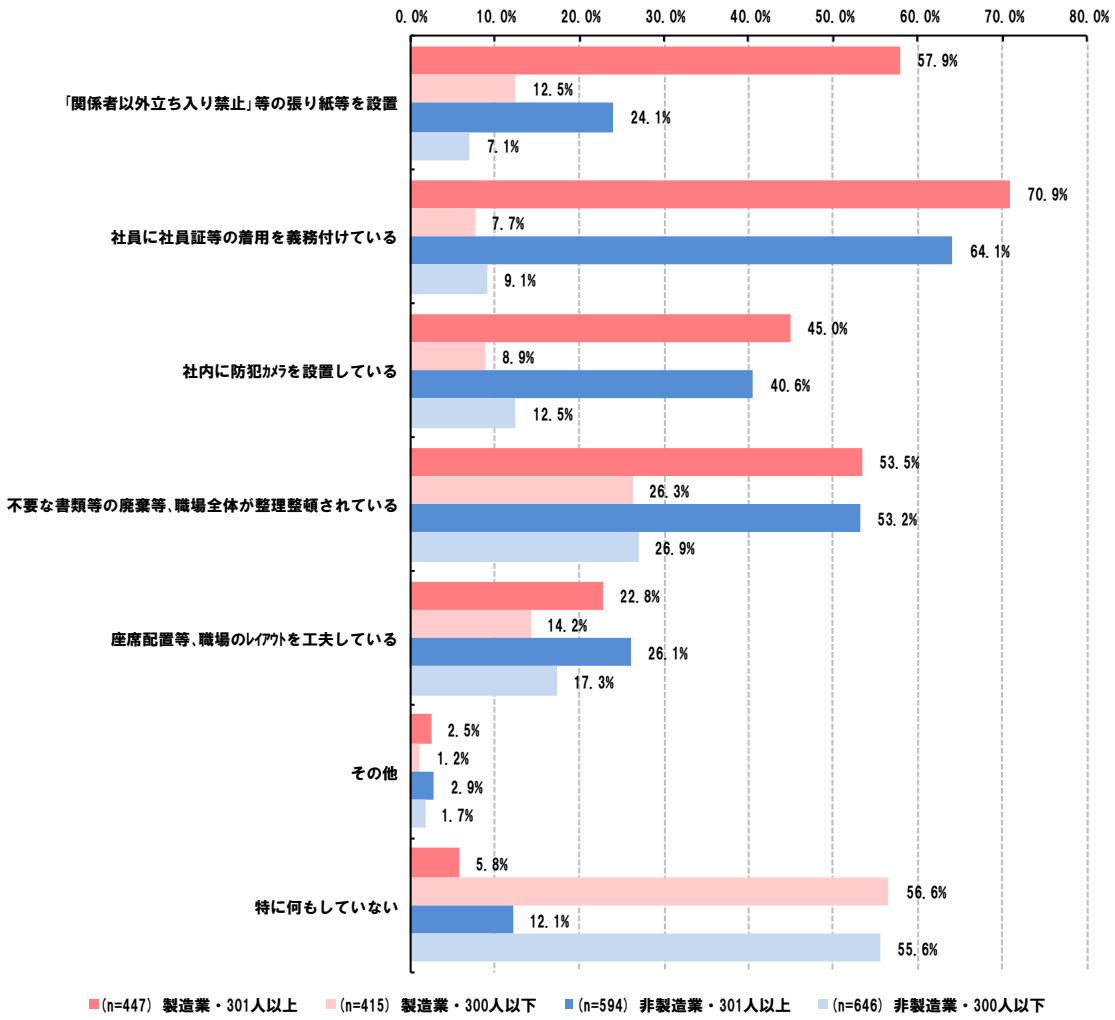

図 2.2-10 視認性の確保に資する物理的な対策への取組状況（業種・規模別）（問 35）

2.2.3.2. 視認性の確保に資するシステム的な対策

視認性の確保に資するシステム的な対策として、42.8%の企業が「情報システムのログを記録・保管している」と回答している。一方で、その他の対策について取り組んでいる企業の割合は、いずれも 1 割程度に留まっている。また、49.0%の企業が「特に何もしていない」と回答している（図 2.2-11）。

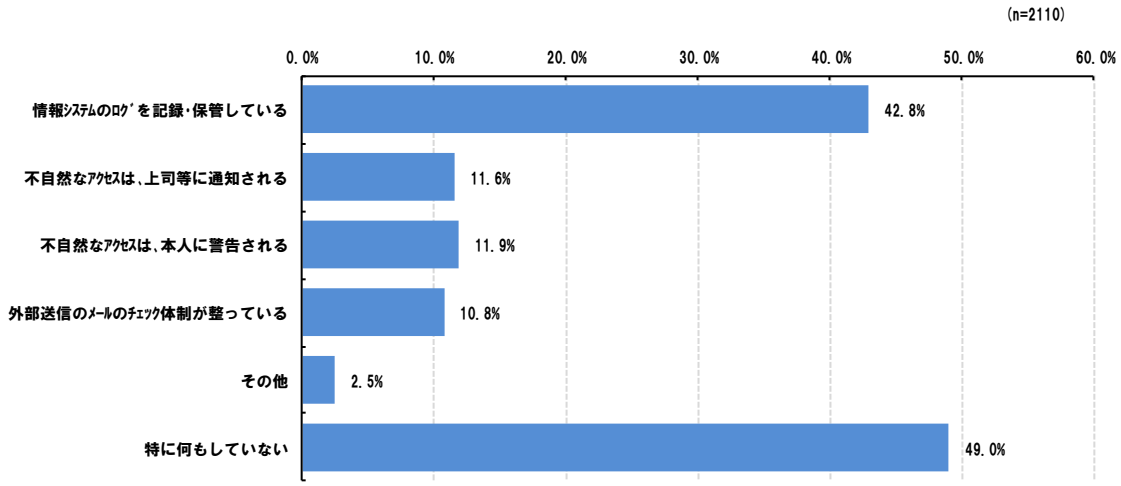

図 2.2-11 視認性の確保に資するシステム的な対策への取組状況（全業種・全規模）（問 36）

業種・規模別に見ると、「情報システムのログの記録・保管」については、大規模企業と中小規模企業との間で大きな差が見られ、大規模企業では７割以上の企業で実施されているのに対し、中小規模企業では１割前後となっている。その他の対策を見ても、中小規模企業ではすべて１割に満たない状況となっており、こうしたシステム的な手段が必要となる対策については資金面・人員面での投資も求められるため、必ずしもそうした資源が十分ではない中小規模企業では取組が後手に回ってしまうものと考えられる（図 2.2-12）。

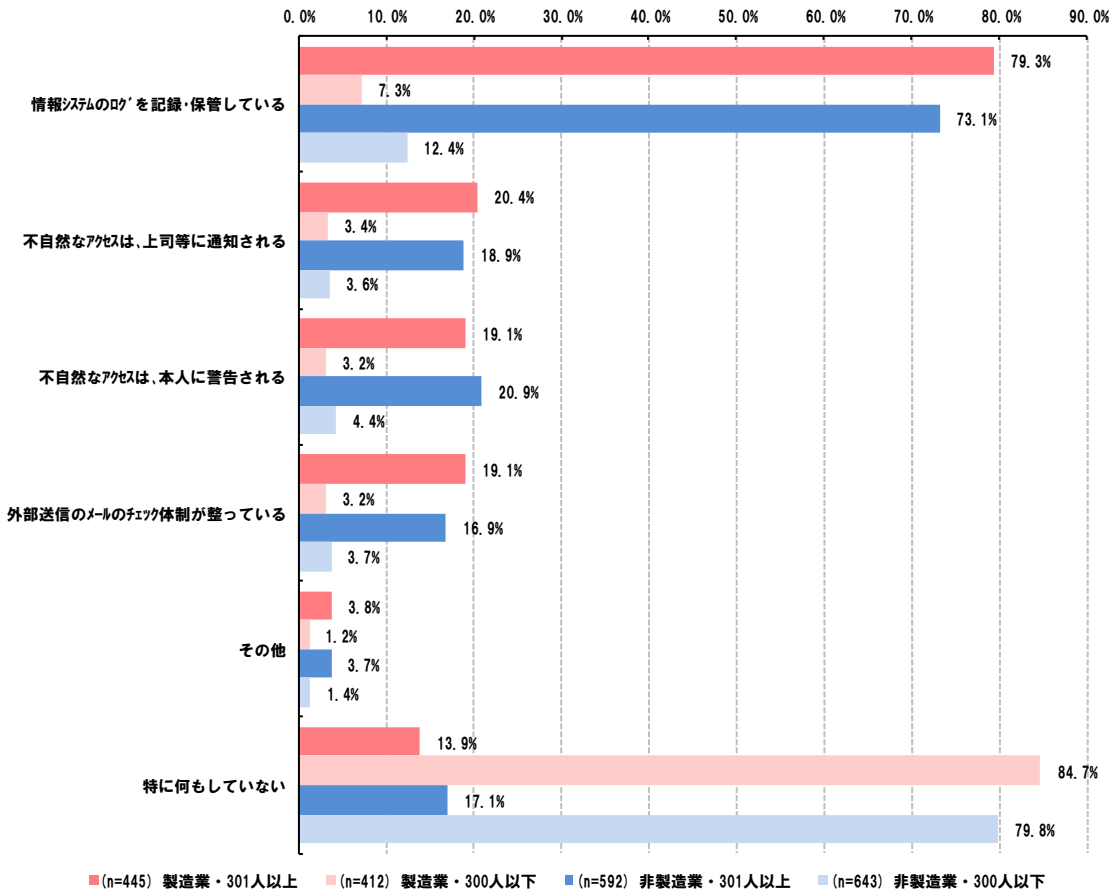

図 2.2-12 視認性の確保に資するシステム的な対策への取組状況（業種・規模別）（問 36）

インタビュー調査において、記録されたログの中で不自然なものについては管理担当部署に通知されるようになっている例やログを取得していることを従業員にも周知している例があった。

【ログの記録について（インタビュー調査結果）】
（不自然なログの通知）
- 社員の全メール情報やフォルダへのアクセス記録については、毎日ログを記録している。その中から不自然と思われるものが担当部署に通知されるようになっている。（製造業）

（従業員への周知）
- 社員にはログをモニタリングしているという事実を周知していることに加え、ルールにも明記している。（製造業）
- 例えば業務に関係ないホームページの閲覧時間等のログのモニタリングを実施

しているという事実は社員にも周知しており、心理的な牽制効果を期待している。（非製造業）

（その他）

- フォルダアクセスや電子メールのログは取得しているが、リアルタイムでのモニタリングは行っておらず、年一回の内部監査時に確認している。（製造業）
- メールへの電子データ添付による外部送信は可能であるが、全てログを記録している。（製造業）
- 営業秘密が格納される領域では、特定のフォルダのアクセスログを記録している。（製造業）
- 不自然なログが収集された場合、人事部と相談の上、ファイルの中身を含むログの詳細を調査するが、この段階まで調査するのは年 1 名程度である。この段階まで踏み込んだ調査が行われた事実を知っているのは、人事部と情報システム部のみである。（製造業）
- PC 使用状況について、不審な点は定期的に確認している。具体的には、決められたキーワードで不審な行動を検知しており、例えば会社への不満がある者や退職意向者は、転職サイト等を閲覧しているケースがあるため、それに関連したキーワード等によってある程度検知できる。（製造業）

2.2.4. 秘密情報に対する認識向上に資する対策

2.2.4.1. 秘密情報に対する認識向上に資する対策

【秘密保持契約】

本アンケート調査結果によると、36.4%の企業が役員との間で秘密保持契約を締結していると回答している。締結している期間に着目すると、「期間の定め無し」としている企業が最も多い一方で、5.1%ではあるが「在職中のみ」と回答している企業が一定数存在しており、退職後まで秘密保持を義務付けられていないことがわかる。また、55.1%の企業では、役員との間で秘密保持契約が締結されていない（図 2.2-13）。

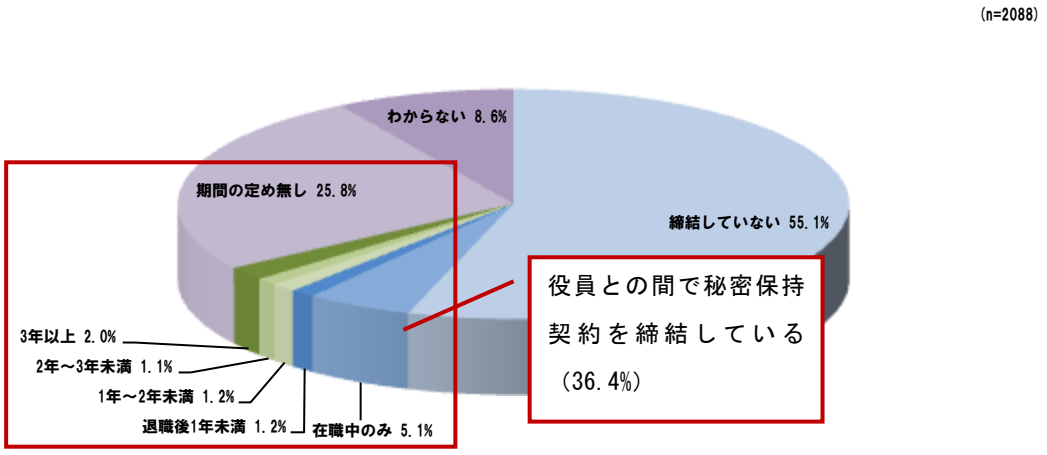

図 2.2-13 役員との秘密保持契約の締結状況と期間（全業種・全規模）（問 37）

また、従業員との間の秘密保持契約の締結については、46.1%の企業が実施していると回答しており、役員との間で秘密保持義務を締結している割合よりも高くなっている。締結している期間については、役員との締結期間と同様に「期間の定め無し」と回答した企業が 31.4%であり、最も多くなっている。在職中のみ契約を締結している企業が 7.3%存在しており、退職後にまで秘密保持を義務付けられていない。また、49.2%の企業では、従業員との間で秘密保持契約を締結していない（図 2.2-14）。

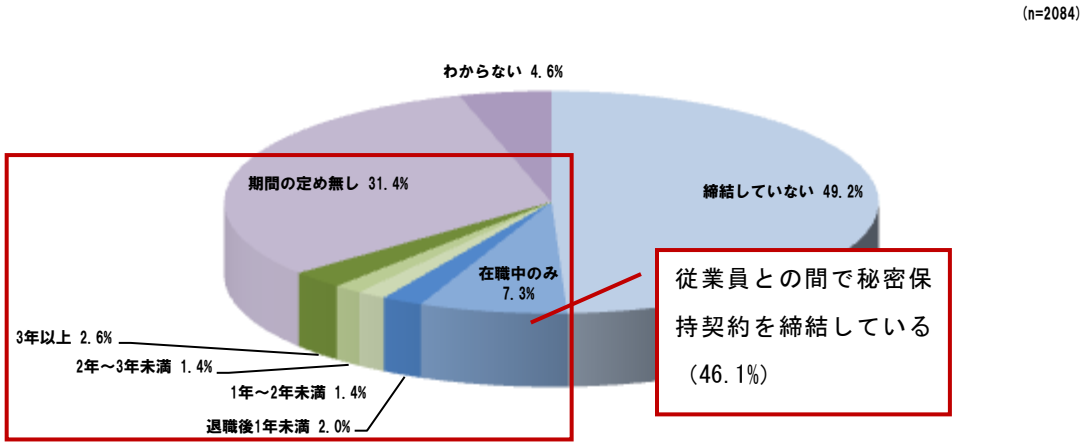

図 2.2-14 従業員との秘密保持契約の締結状況と期間（全業種・全規模）（問 37）

役員・従業員との間で秘密保持契約を締結していない理由については、「特に理由はない」という回答が 51.9%と最も多い結果になっている（図 2.2-15）。秘密保持契約を締結しておくことは、従業員等自身が契約の当事者になるため、営業秘密に対する認識を持たせる効

果があるとされており、こうした企業においては対策を検討することが望ましい。

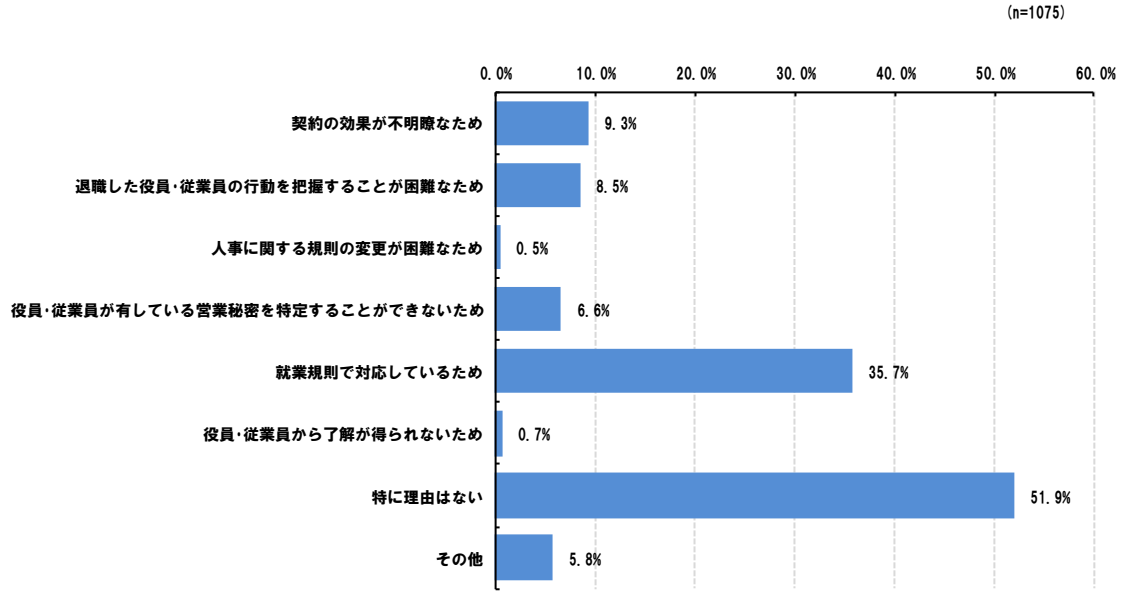

図 2.2-15 秘密保持契約を締結していない理由（全業種・全規模）（問 39）

【競業避止義務契約】

競業避止義務契約については、それ自体が直接的に秘密情報に対する認識向上につながるものではないが、秘密保持義務の有効性を高めるという意味では効果を期待できるものである。

本アンケート調査結果によると、13.2%の企業が役員との間で競業避止義務契約締結していると回答している。締結している期間については、6.2%ではあるが「期間の定め無し」と回答している企業が一定数存在している。一方で、75.7%の企業では、役員との間で競業避止義務契約が締結されていない（問 2.2-16）。

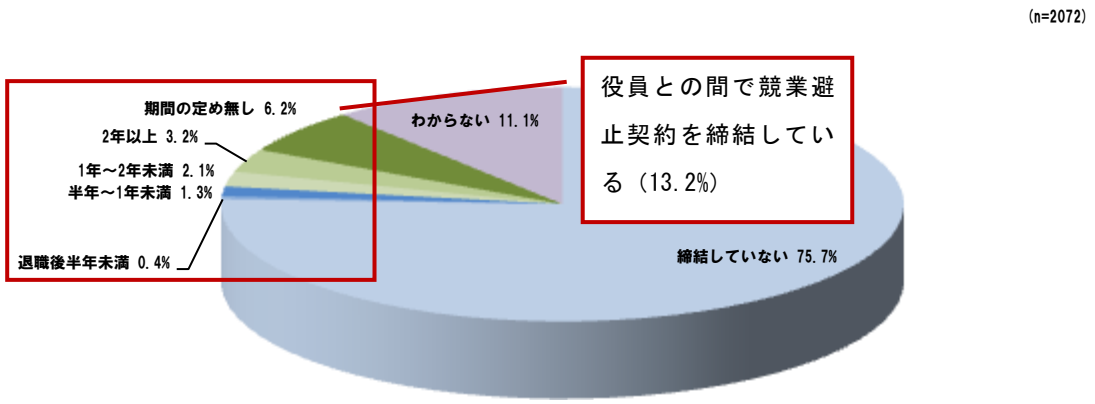

図 2.2-16 役員との競業避止義務契約の締結状況と期間（全業種・全規模）（問 40）

また、従業員との間では、14.9%の企業が競業避止義務契約を締結していると回答しており、5.9%が「期間の定め無し」と回答している。一方で、77.3%の企業では、従業員との間で競業避止義務契約が締結されていない（図 2.2-17）。

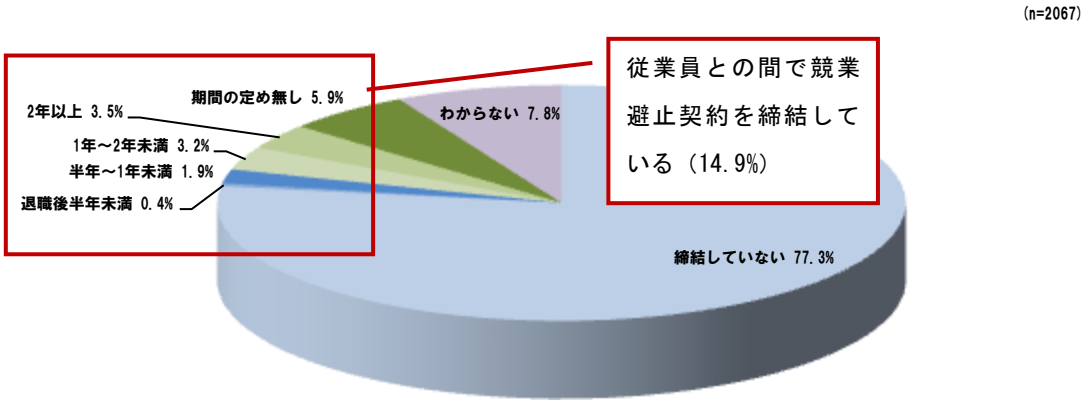

図 2.2-17 従業員との競業避止義務契約の締結状況と期間（全業種・全規模）（問 40）

秘密保持契約等の締結以外に、秘密情報に対する認識向上を目的とした対策として、社内における営業秘密の取り扱いルールを研修等で周知する取組が挙げられる。本アンケート調査結果によれば、35.4%の企業がこうした取組を実施している（図 2.2-18）。

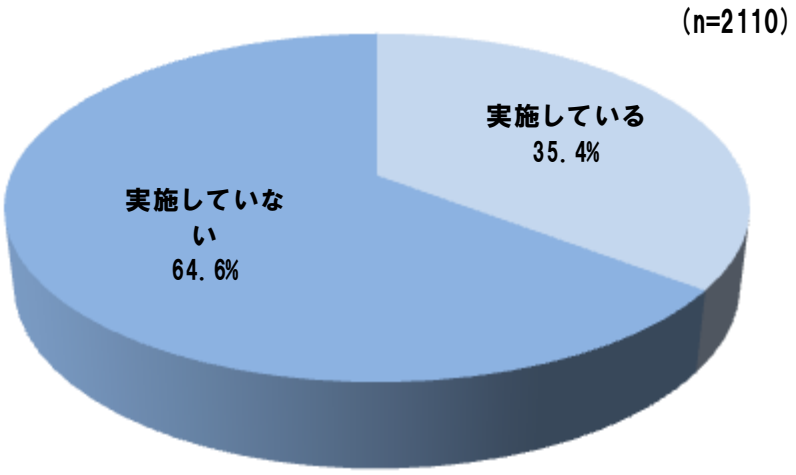

図 2.2-18　研修実施等による営業秘密の取扱ルールの周知状況（全業種・全規模）（問 42）

インタビュー調査において、研修等の実施形態としてイントラネットを通じた情報提供という例が見られたほか、実施内容については仮想の標的型攻撃による訓練や実際の漏えい事例を想定したケーススタディ等の例があった。また、一部の企業では研修の受講を資

格要件としている例もあった。

【研修等の実施例（インタビュー調査結果）】
- 月 1 回の頻度で、社内イントラネットに情報セキュリティに関する時事ネタを掲載し、注意喚起を促している。（製造業）
- 実際の情報漏えいを想定したケーススタディ形式を含めた研修内容とすることで、情報管理に対する意識を高めて、情報漏えいに対する心理的な抑止力に繋げることを想定している。（製造業）
- 年一回、情報の取扱に関する基本的な内容に関する研修を実施し、注意喚起している。（製造業）
- セキュリティ研修等の受講が昇格要件として定められている。（非製造業）
- 標的型攻撃に関する訓練（仮想の攻撃メールへの対応）を実施している。（製造業）

2.2.5. 信頼関係の維持・向上等に資する対策

2.2.5.1. 信頼関係の維持・向上等に資する対策

働きやすい環境を整備し、従業員の企業に対する帰属意識を高めたり、透明性の高い評価制度等を構築することで従業員のモチベーションを高めたりすることによって、信頼関係の維持・向上等を図る取組も有効な対策の一つである。

本アンケート調査結果によれば、21.5%の企業が「自社への帰属意識を高められるようにしている」と回答し、18.3%の企業が「人事評価や表彰制度等でモチベーションを向上させる」と回答している（図 2.2-19）。

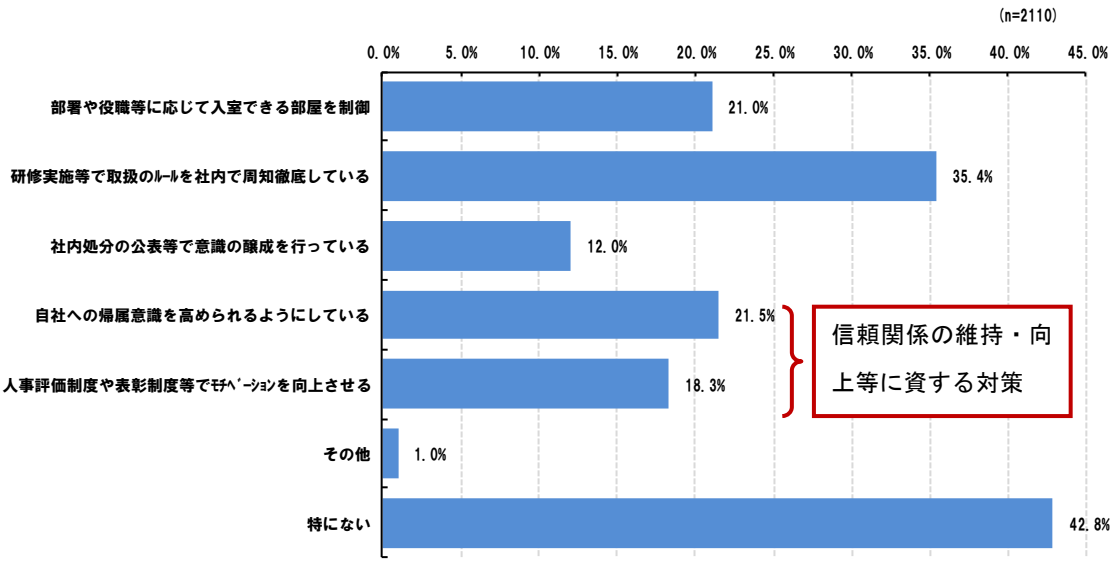

図 2.2-19　信頼関係の維持・向上等に資する対策（全業種・全規模）（問 42）

インタビュー調査においては、モチベーション向上のための施策として、特定の従業員に対して賞与面でのインセンティブを持たせている例があった。

【従業員のモチベーション向上策の実施例（インタビュー調査結果）】
- コアな技術情報に接している人材は賞与の観点でインセンティブを持たせるようにしている。（製造業）

2.3. 対象者の種別に応じた対策の取組状況

2.1.2 営業秘密の漏えいルートの調査データでも示される通り、営業秘密の漏えいは、現職の従業員等の内部者だけでなく、退職者、委託先などの外部者も含めて、様々な経路から起こりうる。営業秘密の漏えいが発生するルートとしては、①現職の従業員等、②退職者等、③取引先、④外部者の４つが代表的なものとしてあげられ、各ルートに対して、その特徴を意識した対策を実施する必要がある。

今回実施したアンケート調査およびインタビュー調査からは、対象者の種別に応じた対策への取組状況として、以下の実態が明らかになっている。

- 従業員等向けの対策については、35.4%の企業が「研修実施等で取扱のルールを社内で周知徹底している」と回答しているが、従業員等向けの他の対策については１～２割程度の割合の企業でしか実施されていない。
- 退職者向けの対策については、25.8%の企業で「速やかに会社貸与の記録媒体等を返却させる」という対策が実施されているが、退職者向けの他の対策については１割未満の企業でしか実施されていない。インタビュー調査においても、複数の企業において「退職予定者のアクセスログ等をモニタリングする等、退職予定者向けの対策を実施することの必要性を感じてはいるが、現実的にはそこまで実施できていない」というコメントがあった。
- 取引先向けの対策については、45.7%の企業で「営業秘密授受が発生する取引先には秘密保持契約を締結」が実施されており、また 38.1%の企業で「契約書に情報漏えいに関する損害賠償等の条項を入れる」が実施されている。一方、他の対策については１割前後の企業でしか実施されていない。
- 外部者向けの対策については、31.4%の企業が「来訪者には必ず入館前に記名してもらう」と回答している。

2.3.1. 従業員等向けの対策

自社での業務に従事する者には、役員や自社雇用の従業員だけでなく、派遣労働者や委託先従業員、また実習生等があげられる。こうした対象者については、直接的に自社の営業秘密に触れる場面が多く、そうした情報を不正に持ち出すような意識を発生させないような環境の整備も含めた多重的な対策を実施することが重要となる。

本アンケート調査結果によると、35.4%の企業が「研修実施等で取扱のルールを社内で周知徹底している」と回答している。一方でその他の対策については１～２割程度の割合の企業でしか実施されていない。また、42.8%の企業が「特にない」と回答している（図 2.3-1）。

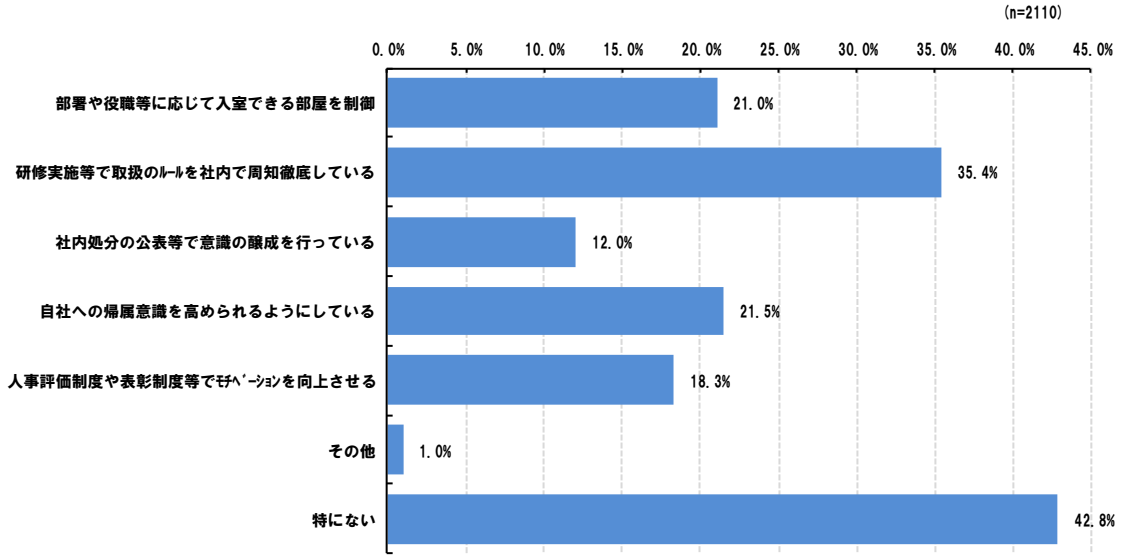

図 2.3-1 従業員等向けの特有の対策（全業種・全規模）（問 42）

業種・規模別に見ると、大規模企業では「研修実施等で取扱のルールを社内で周知徹底している」と回答した割合が６割前後であるのに対し、中小規模企業では１割前後でしか実施されておらず、大きな差が見られる。また、中小規模企業については、７割程度の企業が「特にない」と回答している（図 2.3-2）。

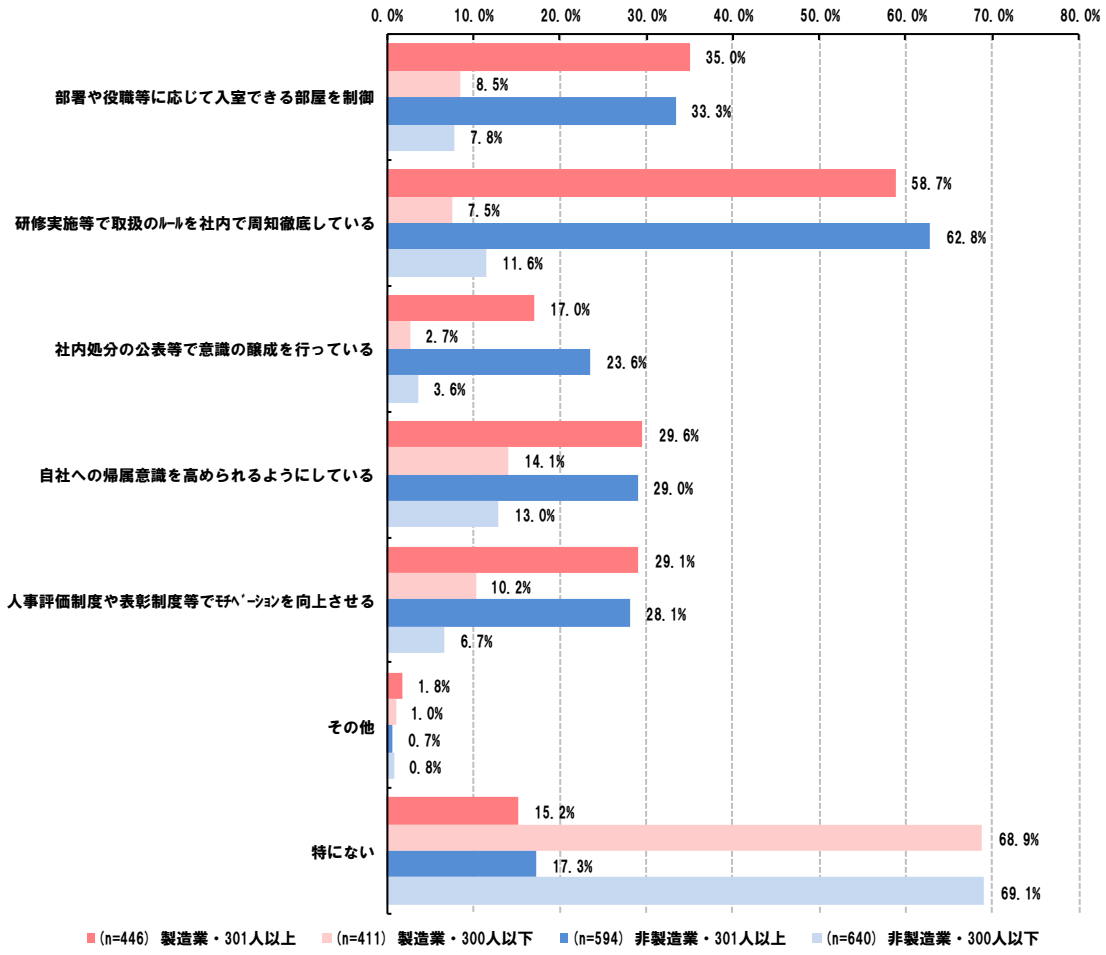

図 2.3-2　従業員等向けの特有の対策（業種・規模別）（問 42）

2.3.2. 退職者等向けの対策

本アンケート調査結果によると、「速やかに会社貸与の記録媒体等を返却させる」といった一般的な取組を実施している企業は 25.8%であったが、「退職者の動向を把握する」「既存の対策をより厳格化する」といった具体的な取組まで実施している企業は数%に留まっている。また、69.9%の企業においては、退職者等を特に意識した対策に取り組めていない（図 2.3-3）。

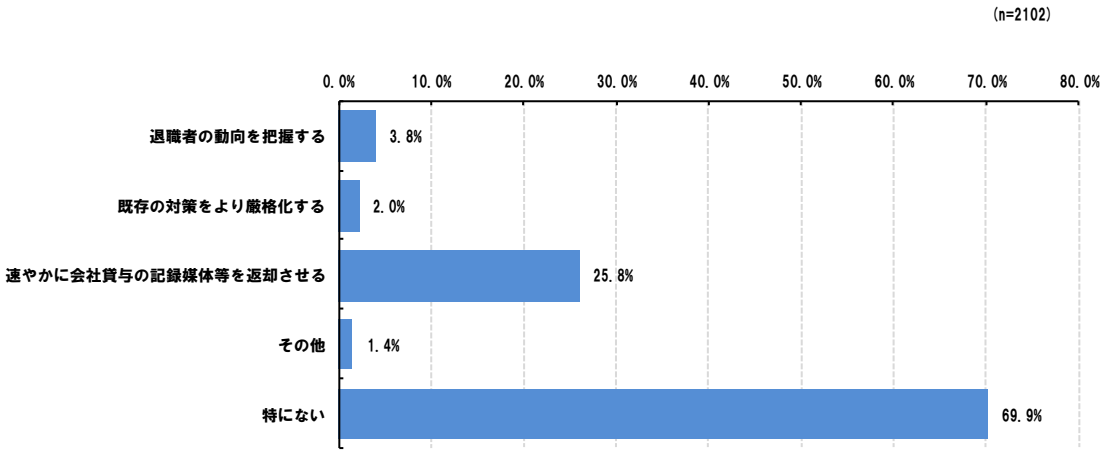

図 2.3-3 退職者等向けの特有の対策（全業種・全規模）（問 43）

業種・規模別に見ると、４割前後の大規模企業が「速やかに会社貸与の記録媒体等を返却させる」と回答している。一方、退職予定者に対して「既存の対策をより厳格化する」と回答した企業は、大規模企業であっても１割未満であり、十分に対策を実施できていない現状が窺える（図 2.3-4）。

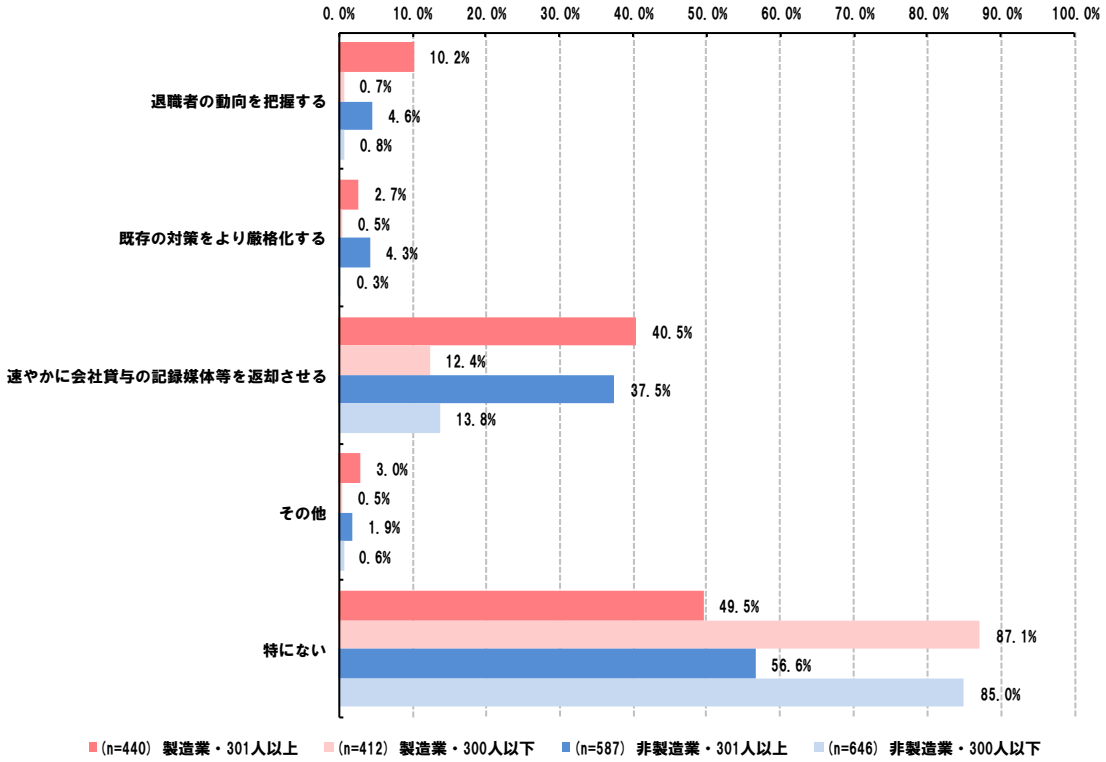

図 2.3-4　退職者等向けの特有の対策（業種・規模別）（問 43）

なお、インタビュー調査においては、退職時に誓約書へのサインをさせて秘密保持の認識を持たせている例や誓約書に競業避止条項まで含めている例、退職予定者のログのモニタリングを強化している例等があった。

【退職者向けの対策例（インタビュー調査結果）】

（誓約書への署名）

- 退職時に誓約書で秘密保持に関する念書をとっている。（退職時に誓約書にサインすることは就業規則で定めている）（製造業）
- 退職者に対しては、誓約書へ署名させ、その上で極秘情報・機密情報・社外秘情報を漏えいしないよう求めている。（非製造業）
- 競合他社に転職する場合には秘密保持契約を締結している。（製造業）

（競業避止条項）

- 退職時に誓約を交わしており、競業避止条項を含めるようにしている。競業避止条項を含めることで、情報漏えい行為に対する牽制になると認識している。（製造業）

（退職予定者へのモニタリング強化）

- 人事部から依頼を受けて、退職希望者が退職するまでの数カ月間のログをモニタリングしている。（製造業）
- 退職時に誓約書の提出を求めていたが、形骸化しつつあったため、過去３か月分のログを人事部に提供する運用に変更した。その内容を確認した上で、人事部は退職者本人と面談を行い、営業秘密を漏えいしないよう伝えている。（製造業）

2.3.3. 取引先向けの対策

取引先向けの対策については、45.7%の企業において「営業秘密授受等が発生する取引先には秘密保持契約を締結」という取組が実施されている。また「契約書に情報漏えいに関する損害賠償等の条項を入れる」と回答した企業も 38.1%となっており、その他の対策と比べると相対的に取組が進んでいると思われる。一方で、「取引先の情報管理体制や実施状況等を確認する」「取引先の情報管理状況の監査ができる」等の取組については１割程度の企業でしか実施されていないことから、大半の企業が取引先と秘密保持契約を締結しているものの、その履行状況を確認し、必要に応じて履行を求めていくことまでは実施できて

いない、という実態があることが推察される（図 2.3-5）。

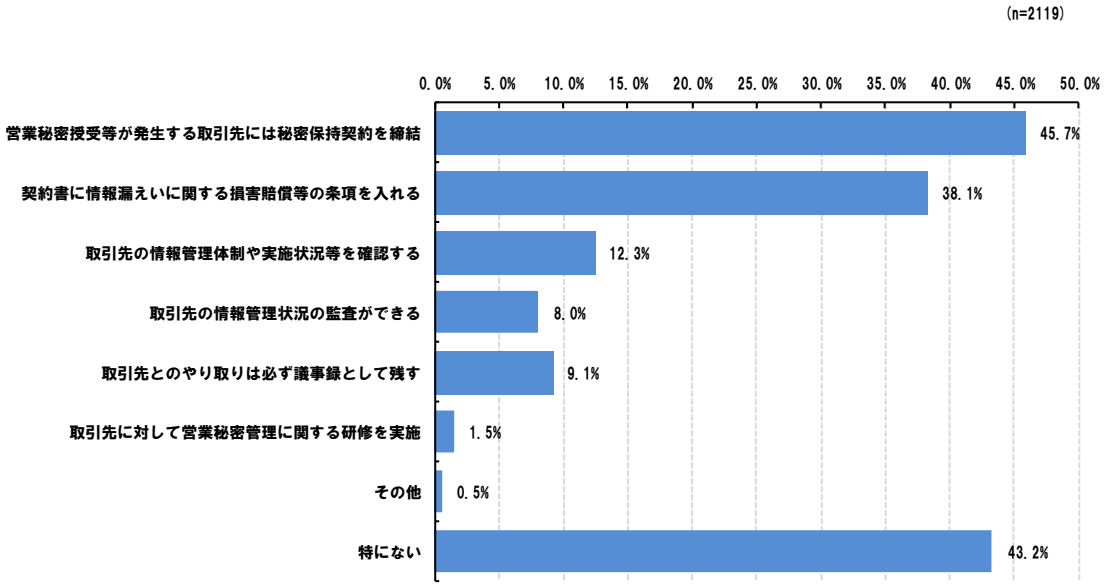

図 2.3-5 取引先向け特有の対策（全業種・全規模）（問 44）

業種・規模別に見ると、やはり大規模企業と中小規模企業との間で取組状況には大きな差があり、中小規模企業では取引先との間で秘密保持契約を締結している割合が２割未満となっている。また、取引先の情報管理体制の確認や管理状況の監査まで実施できている中小規模企業は数%であることに加えて、大規模企業でも１～２割程度であることから、こうした取組がほとんど実施されていない状況であることが窺える[7]（図 2.3-6）。法律専門家に対するインタビュー調査によれば、「中小規模企業は情報管理を徹底できていないことが多いので、特に大規模企業は下請け企業等に渡す営業秘密の管理を厳重に行う必要がある」という指摘がなされている。また、これに加えて「昨今業務を外部委託する機会が増えてきているので、秘密保持契約の重要性が高まっている。その際に、可能な限り秘密保持の対象となる情報を特定した方が、漏えい等が発生した際に立証しやすくなる。」との指摘もあった。

---

7 経済産業省（委託事業者：三菱 UFJ リサーチ＆コンサルティング株式会社）「営業秘密管理の実態に関する調査研究」（平成 27 年 3 月）によれば、中小企業では取引先との間で締結する契約書に秘密保持条項を盛り込むことまでは実施されているケースがあるが、長年にわたって取引を実施してきた委託先等が多く、信頼関係を重視しているため、取引先における情報管理体制や状況等を具体的に調査・確認するようなことまではしない、という声があることが報告されている。同報告書は、営業秘密管理に係るグッドプラクティスおよびベストプラクティスを調査したものであるが、大企業においても取引先に対して契約前に情報管理体制等を調査する一方で、契約後の監査までは実施できていないという例があったことが報告されている。
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/h26jittai.pdf

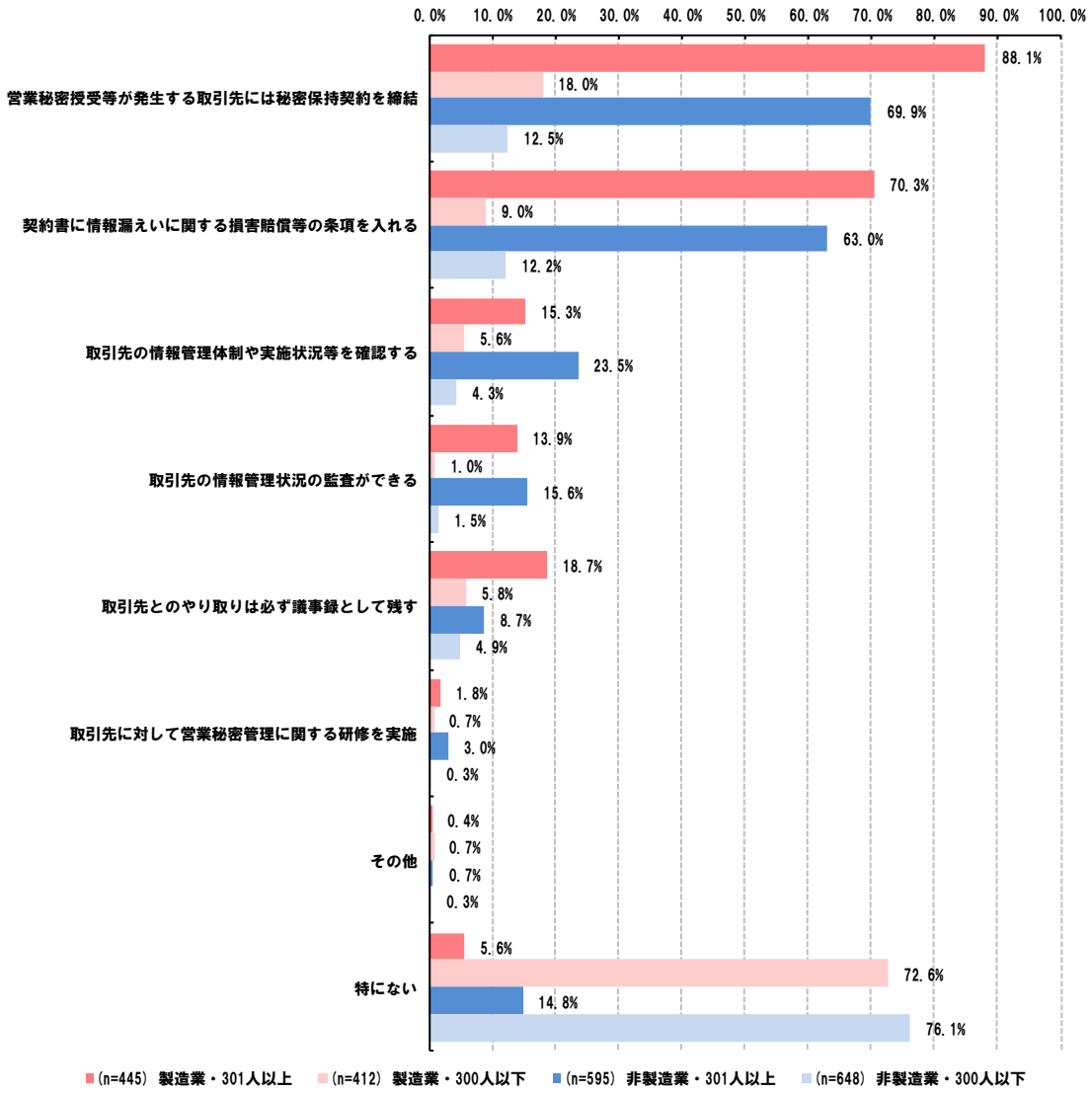

図 2.3-6 取引先向け特有の対策（業種・規模別）（問 44）

インタビュー調査においては、具体的に取引先の情報管理体制等を事前にチェックしている例や、情報の授受・処分等に関する記録を取得している例があった。

【取引先向けの対策例（インタビュー調査結果）】
（取引先のチェック）
- 過去の情報漏えい事故の有無やプライバシーマーク取得状況を確認している。こうした確認は、新規契約時および既存パートナー企業に対しても年 1 回の頻度で実施している。（非製造業）

・ 外部委託先のチェック項目としては、物理的なセキュリティ対策の実施状況や、従業員への守秘義務の指導・誓約状況等の項目を設定している。（製造業）

（情報の授受・処分等の記録）

・ 機密保持契約を締結する他、情報授受記録、情報処分（廃棄）記録を管理している。（製造業）

2.3.4. 外部者向けの対策

外部者向けの対策については、31.4%の企業が「来訪者には必ず入館前に記名してもらう」と回答している。一方で、「記録媒体や撮影機器等の持ち込み禁止」と回答している企業は14.4%であり、外部者の機器持ち込みに関する対策を徹底できていない状況であることが窺える。また、53.0%の企業が「特にない」と回答している（図 2.3-7）。

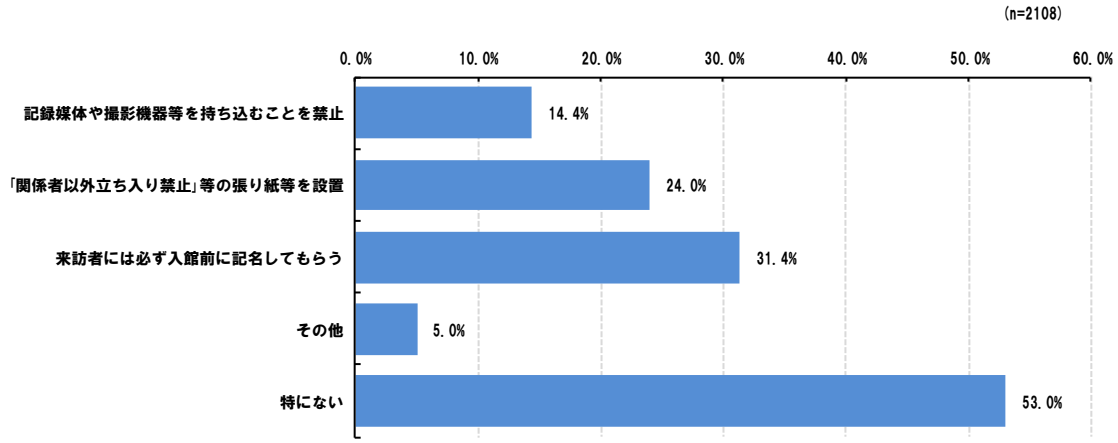

図 2.3-7 外部者向け特有の対策（全業種・全規模）（問 45）

外部者向けの対策については、業種や規模によって差が見られており、傾向として中小規模企業は大規模企業と比較して全体的に対策を実施できていない。特に全体では 31.4%の企業で実施されていた「入館前の記名」についても、実施できている企業は 1 割未満である。また、特に大規模企業においては製造業と非製造業との間での実施状況にも差が見られ、製造業の方が、相対的に取組が進んでいると言える（図 2.3-8）。

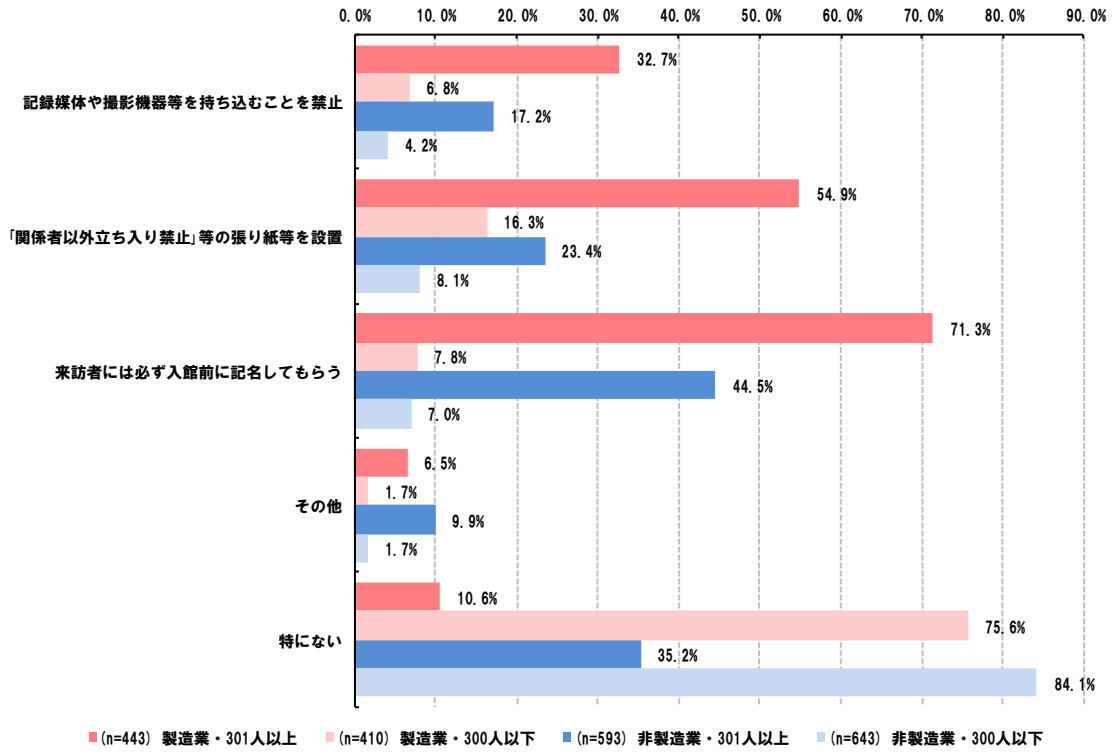

図 2.3-8 外部者向け特有の対策（業種・規模別）（問 45）

2.4. 営業秘密管理に対する考え方と組織体制

営業秘密漏えいに関する近年の報道事例等からも明らかなように、企業の競争力の源泉となるような情報の漏えいや、大量の顧客情報等の流出は、企業の経営に大きな影響を与えるだけでなく、社会問題にまで発展する場合がある。したがって、営業秘密管理は、企業にとって些末な問題ではなく経営に直結する問題の一つと捉えて検討されるべきものであり、また全社的に体制を整備した上で取り組むべき問題である。

今回実施したアンケート調査およびインタビュー調査の結果、営業秘密管理に対する考え方や組織体制として、以下の実態が明らかになっている。

- 営業秘密管理の考え方については、57.1%の企業が「コンプライアンス上の問題」と回答しており、また 55.2%が「情報セキュリティ対策の問題」、53.3%が「経営に直結する問題」と回答している。
- 営業秘密として管理する情報とそれ以外の情報との区分については、47.1%の企業で区分がなされている。うち、23.1%の企業では情報の管理区分として、さらに秘密性のレベルに応じた格付けを行っている。
- 営業秘密の漏えいが発生した際の体制については、「経営層主導で対策を検討する」という体制になっている企業が 38.1%である一方で、「特にない」と回答している企業も 34.7%存在している。

2.4.1. 営業秘密管理に対する意識

本アンケート調査結果によれば、57.1%の企業が営業秘密管理を「コンプライアンス上の問題」と捉えており、また 55.2%の企業が「情報セキュリティ対策の問題」、53.3%の企業が「経営に直結する問題」と捉えている。一方で、14.0%の企業が「わからない」と回答していることからも、営業秘密管理の重要性が、必ずしも全体にまんべんなく浸透しているわけではない現状が窺える（図 2.4-1）。

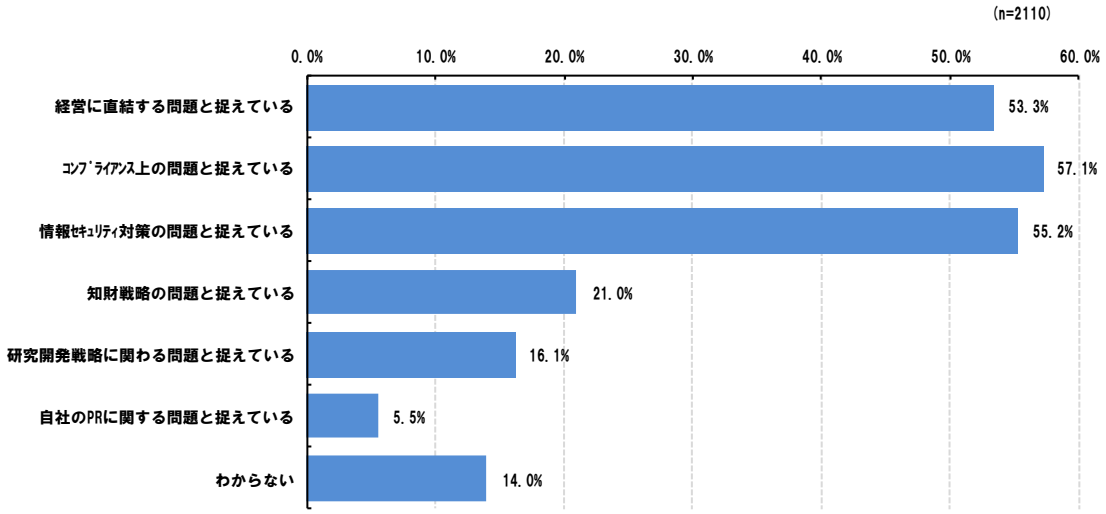

図 2.4-1 営業秘密管理の捉え方（全業種・全規模）（問 26）

業種・規模別に見ると、大規模の製造業においては「経営に直結する問題」「コンプライアンス上の問題」「情報セキュリティ対策の問題」と捉えられていると同時に、多くの技術情報を扱っていることもあり「知財戦略の問題」「研究開発戦略に関わる問題」としても捉えられる傾向がある。一方で２～３割程度の中小規模企業が「わからない」と回答しており、営業秘密管理の重要性を認識し、企業活動の一環として捉えきれていない傾向が窺える。また、営業秘密管理に取り組んでいることを、「自社の PR に関する問題」と捉えている企業については、業種・規模を問わず、いずれも１割未満となっており、営業秘密管理への取組状況が必ずしも企業の PR 等の材料として活用しきれていない状況が窺える（図 2.4-2）。

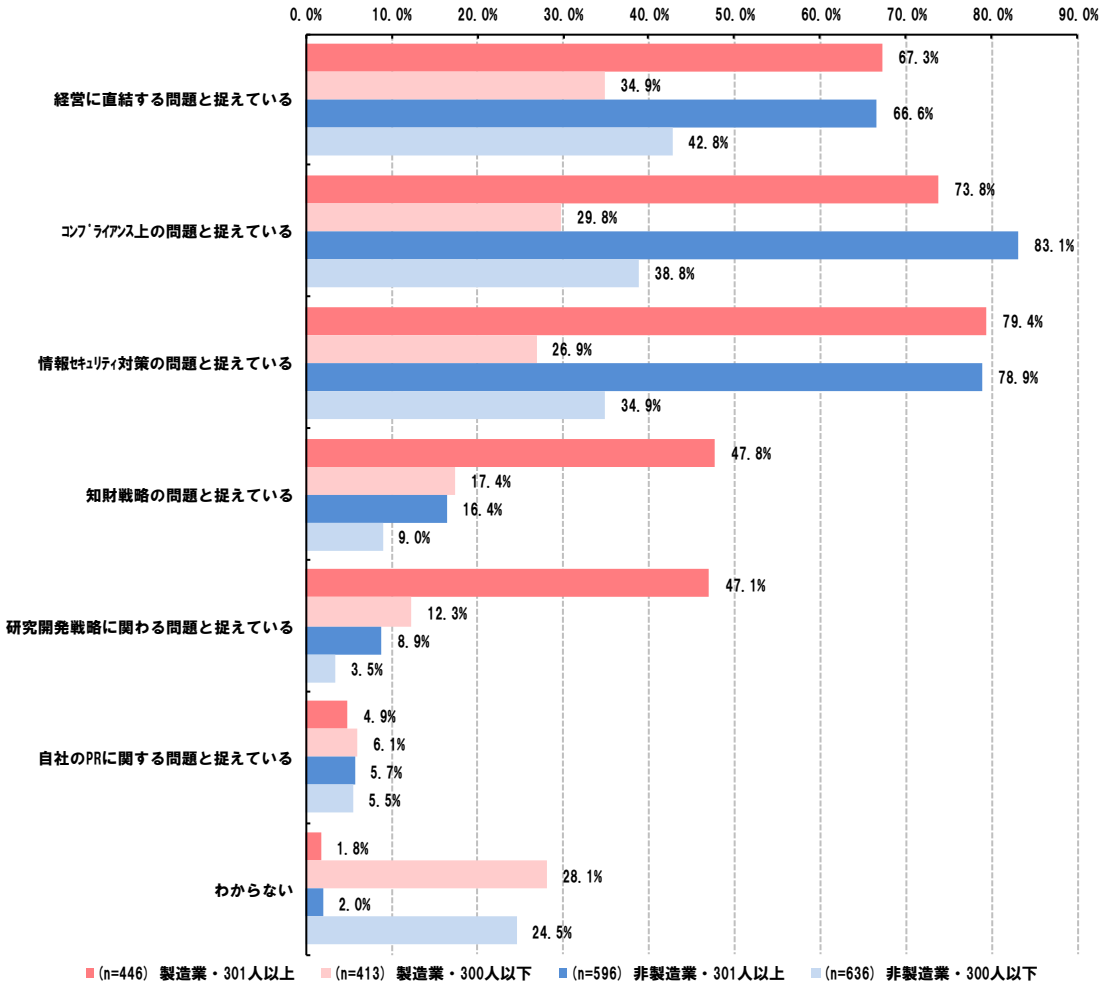

図 2.4-2 営業秘密の捉え方（業種・規模別）（問 26）

2.4.2. 営業秘密として管理する情報の区分

本アンケート調査結果によれば、営業秘密とそれ以外の情報を区分している企業の割合は、回答者全体で 47.1%であった。また、営業秘密とそれ以外の情報を区分するだけでなく、情報の管理区分としてさらに秘密性のレベルに応じた格付けを行っている企業の割合は 23.1%であった（図 2.4-3）。

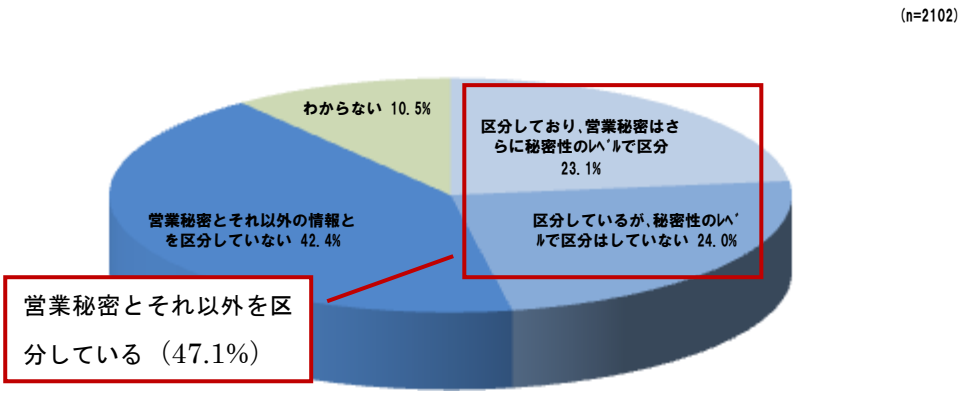

図 2.4-3　営業秘密とそれ以外の情報の区分状況（全業種・全規模）（問 21）

業種・規模別に見ると、大規模企業では６～７割程度が営業秘密とそれ以外の情報とを区分しており、特に大規模の製造業においては 45.7%の企業で、情報の管理区分としてさらに秘密性のレベルに応じた格付けまで実施されている。一方で、中小規模企業においては３割前後の企業しか営業秘密とそれ以外の情報とを区分できていない状況であり、情報の管理区分としてさらに秘密性のレベルに応じた格付けを行っている企業の割合は１割未満であった（図 2.4-4）。

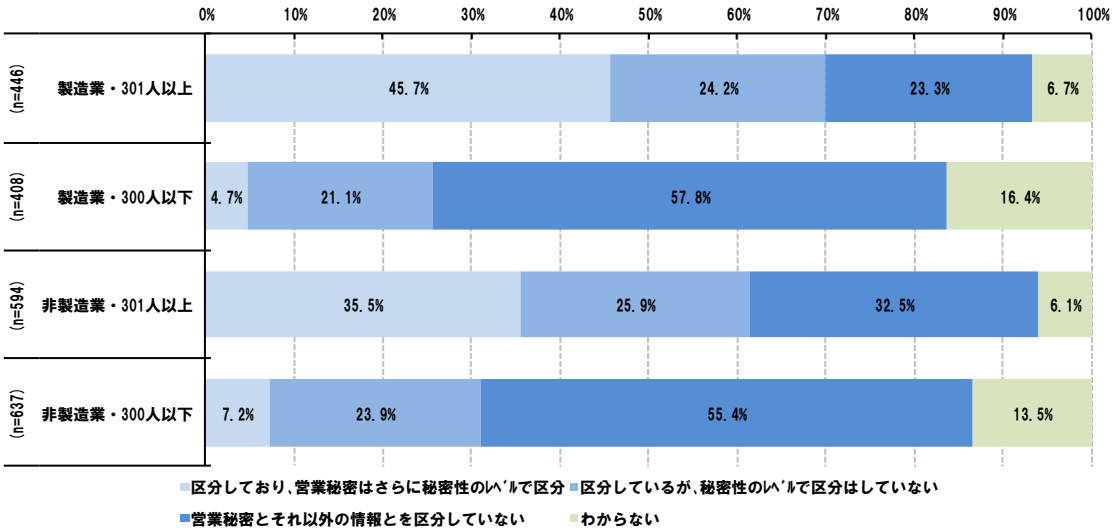

図 2.4-4　営業秘密とそれ以外の情報の区分状況（業種・規模別）（問 21）

なお、従業員規模別に細かく見てみると、人数規模が大きくなるにつれて、営業秘密とそれ以外の情報を区分する取組を積極的に実施するようになる傾向があることが窺える。また、営業秘密として区分した情報をさらに秘密性のレベルに応じて格付けする取組につ

いては、101 人以上の規模になると、一定程度取り組む企業が増えてくることもわかる。(図 2.4-5)

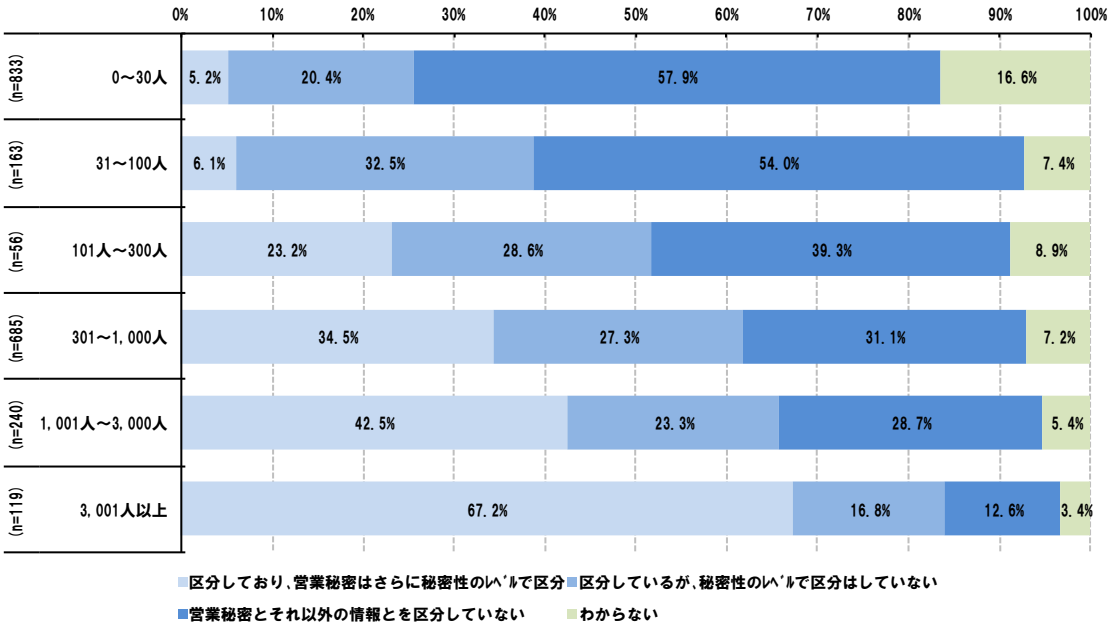

図 2.4-5　営業秘密とそれ以外の情報の区分状況（従業員規模別）（問 21）

また、本来は営業秘密として管理するべき情報の中で、実際に営業秘密として管理できている情報の割合については、68.5%の企業が半分以上の情報については営業秘密として管理できていると回答しており、中でも 39.7%の企業については「ほぼすべての情報」を営業秘密として管理できているとのことであった。一方で、21.0%の企業については「３分の１程度の情報」もしくは「ごくわずかの情報」と回答しており、本来は営業秘密として管理するべき情報を十分に管理できていない状況であることが窺える（図 2.4-6）。

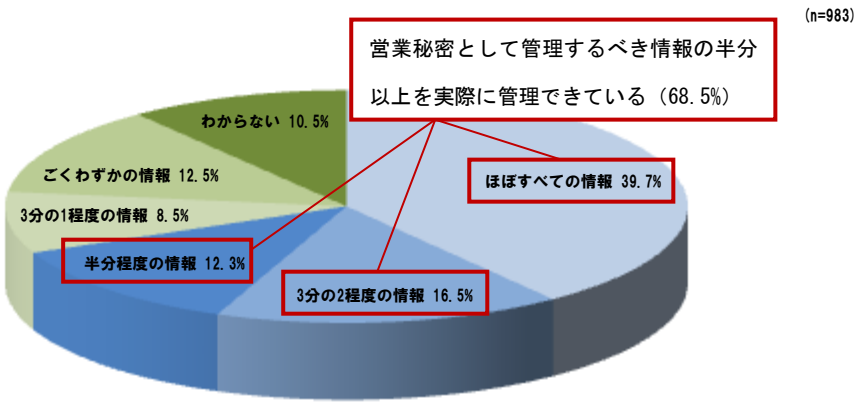

図 2.4-6　営業秘密として管理するべき情報を実際に管理できている割合（全業種・全規模）（問 25）

業種・規模別に見ると、大規模企業においては、７～８割程度の企業が半分以上の情報を営業秘密として管理できており、特に大規模の非製造業については 54.4%が「ほぼすべての情報」を営業秘密として管理できている。一方、中小規模企業においては、半分以上の情報を営業秘密として管理できている企業の割合は５割程度に留まっており、社内における重要な情報の棚卸等を行った上で管理することが十分にできていないことが窺える（図 2.4-7）。

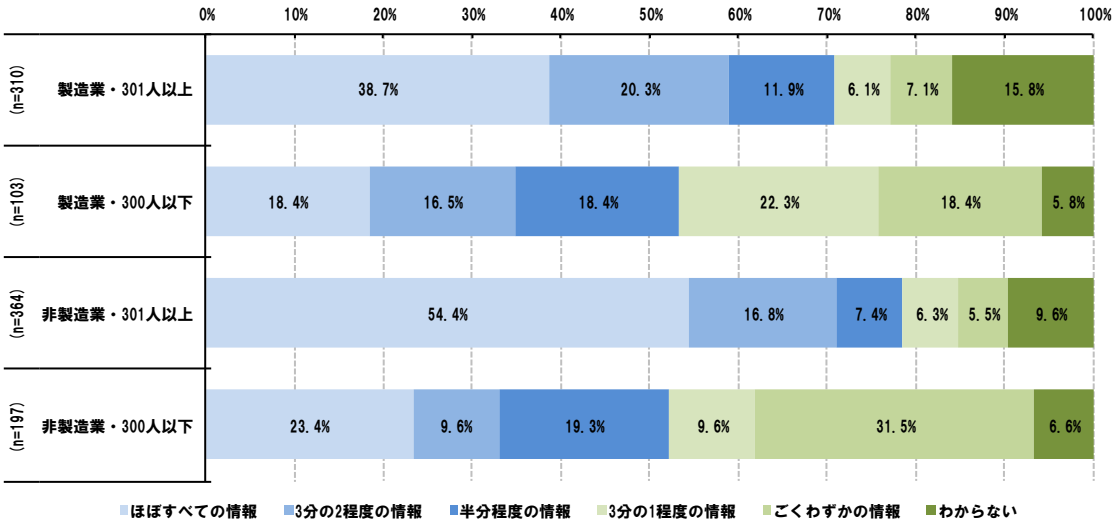

図 2.4-7　営業秘密として管理するべき情報を実際に管理できている割合（業種・規模別）（問 25）

2.4.3. 営業秘密管理に関する組織体制

本アンケート調査結果によれば、営業秘密管理を所管している部署は全体で見ると「特になし」という回答が 27.5%となっており、最も多かった。所管が決められているケースでは、「経営者・経営者直轄チーム」「総務部門・業務管理担当者」がそれぞれ 22.0%、20.9%と比較的割合としては高く、次いで「情報システム部門・情報システム担当者」が 11.3%であった（図 2.4-8）。

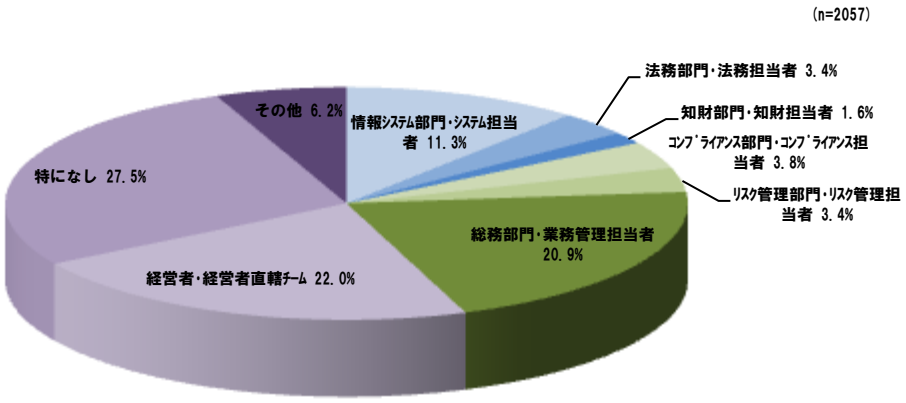

図 2.4-8 営業秘密管理を所管している部署（全業種・全規模）（問 56）

業種・規模別に見ると、中小規模企業では「特になし」「経営者・経営者直轄チーム」という回答が合計で８割程度を占めている。中小規模企業の場合、営業秘密管理に取り組めていない企業が大規模企業と比較して多いことから、そもそもこうした管理を所管する部署・担当者を設置していないケースが一定数存在するということは十分に推定できる。また、中小規模企業の場合、人的資源・投下可能予算が十分でないことから、営業秘密管理を所管する部署や担当者を設置できず、経営者が直轄で所管するというケースが一定数存在することも十分に類推できる。一方で、大規模企業の場合は営業秘密管理を所管する部署等が明確に定められているケースが多く、そのほとんどが「情報システム部門・システム担当者」もしくは「総務部門・業務管理担当者」である。大規模の製造業においては、11.0%ではあるが、「法務部門・法務担当者」という回答もある（図 2.4-9）。

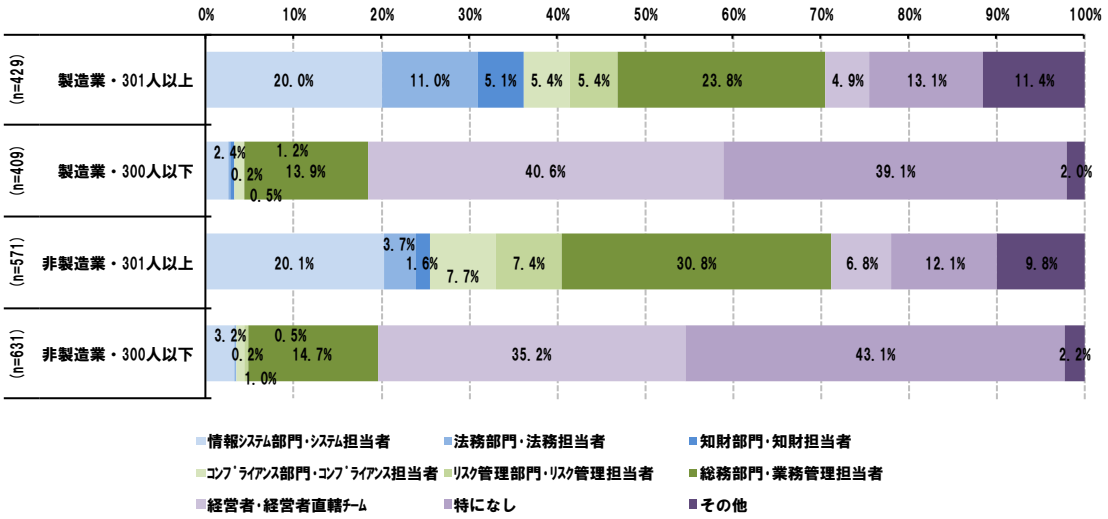

図 2.4-9 営業秘密管理を所管している部署（業種・規模別）（問 56）

営業秘密管理を所管する部署については、企業の規模による差が見られるのと同時に、業種によっても特徴的な差が見られるものもある。例えば、情報通信業や金融業・保険業においては、「リスク管理部門・リスク管理担当者」が所管している割合が高い（図 2.4-10）。

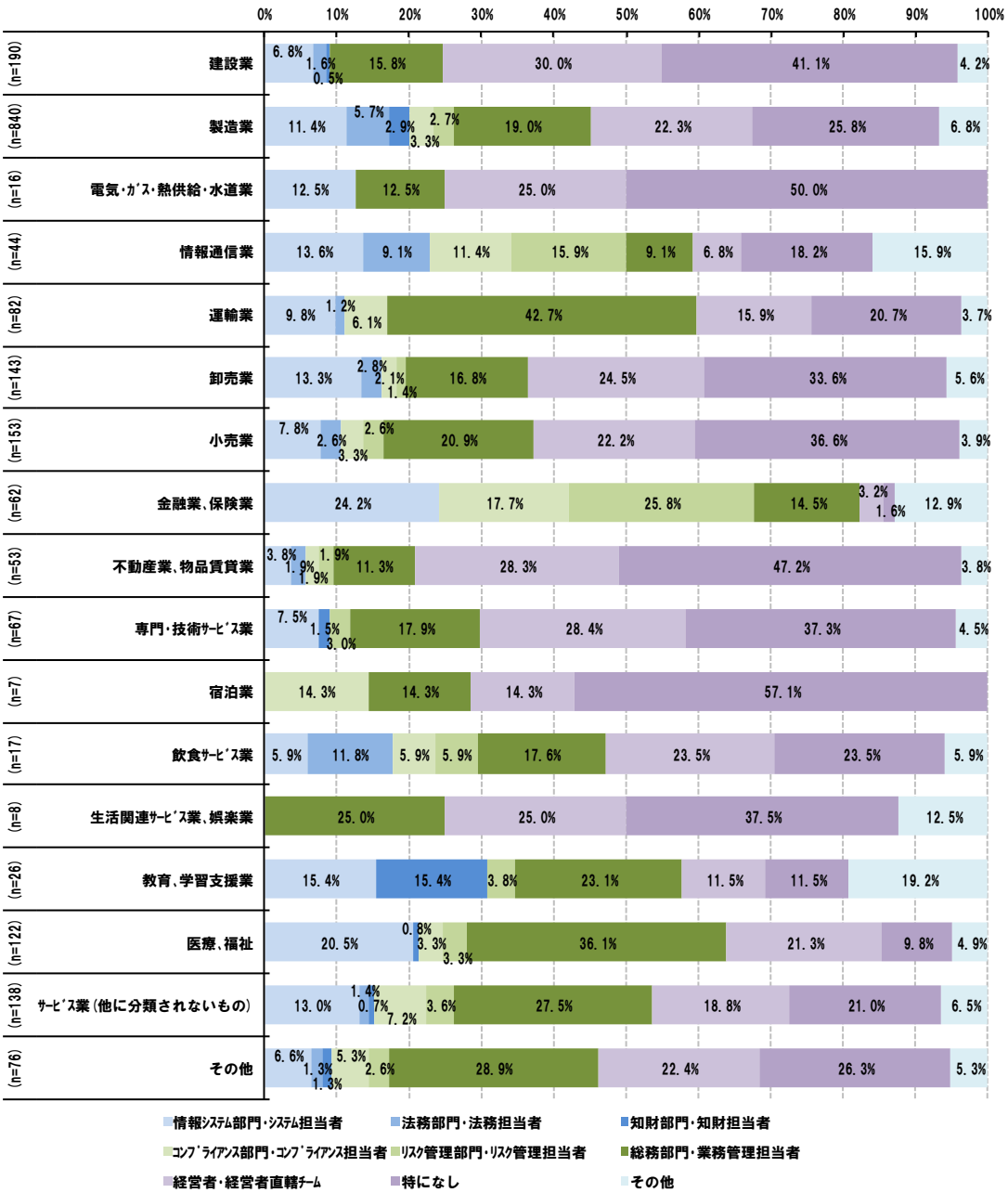

図 2.4-10 営業秘密管理を所管している部署（業種別）（問 56）

漏えい発生時等、有事における営業秘密の組織体制については、全体的には「経営層主導」での対策が実施される割合が 38.1%であり最も高くなっている。一方で、「特にない」という回答も 34.7%あり、有事の際の対策が十分に整備されていない企業が一定数存在することが窺える（図 2.4-11）。

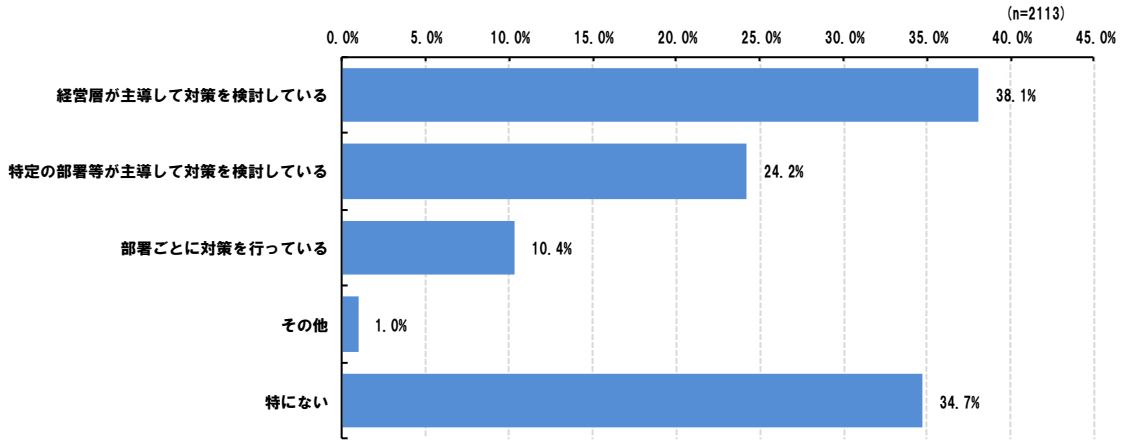

図 2.4-11　有事の際の営業秘密管理に関する組織体制（全業種・全規模）（問 54）

業種・規模別に見ると、中小規模企業では「特にない」という回答が 6 割程度であることから、有事の際の対策・手順等が十分に整備されていない企業がほとんどであることが窺える。大規模企業については、「経営層主導」のケースと同程度「特定の部署等が主導」というケースがある（図 2.4-12）。

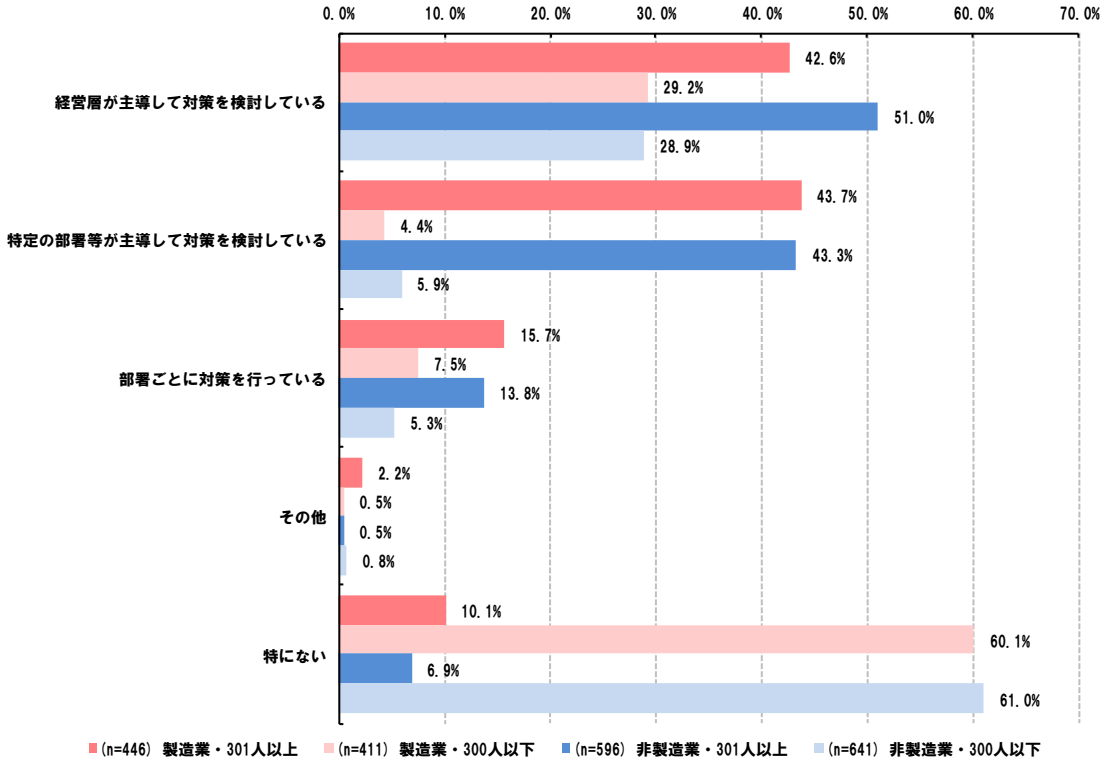

図 2.4-12　有事の際の営業秘密管理に関する組織体制（業種・規模別）（問 54）

2.5. 他社の営業秘密の侵害を防ぐための取組状況

企業間同士の取引や協業、転退職による人材の流動化に伴い、意図せずして他社の営業秘密に接してしまうケースが発生する可能性がある。例えば他社と共同研究をする際に、他社から開示されたノウハウ等を活用して協業を進めるケース等が考えられるが、こうしたケースが発生することを事前に想定して、意図せずに他社の営業秘密を侵害しないようにするための対策を実施しておくことが重要である。

秘密情報の保護ハンドブックによると、「転職者の受入れ」「共同・受託研究開発」「取引の中での秘密情報の授受」「技術情報・営業情報の売込み」等の場面で、他社の営業秘密の意図しない侵害が発生する可能性があるとされており、こうした場面に応じた対策を実施することが求められる[8]。

今回実施したアンケート調査およびインタビュー調査の結果によると、他社の営業秘密侵害を防ぐための対策への取組状況として、以下の実態が明らかになっている。

- 転職者受入時の対策については、いずれの取組も１割未満の企業でしか実施されておらず、84.3%の企業が「特にない」と回答している。
- 共同・受託研究開発実施時の対策については、25.8%の企業が「情報授受の際に秘密保持契約を締結」といった取組を実施しているが、その他の対策についてはいずれも１割未満の企業でしか実施されていない
- 取引先向けの対策については、23.4%の企業で「取引先から開示された営業秘密を取り扱う自社社員の限定」が実施されている一方で、その他の対策は１割前後の企業でしか実施されていない。
- 外部者による売込発生時については、20.8%の企業が「そもそも売込みに応じない」と回答している。一方で、その他の対策については１割未満の企業でしか実施されていない。

[8] 例えば、野中武「営業秘密の保護強化に関する不正競争防止法の改正　自社が不正を行っていないことを積極的に証明できるようにすべき」(労働基準広報、2016.6.11)においては、他社の営業秘密侵害を防ぐための対策として、①自社情報については自社のものとして証明できるようにしておくこと、②他社の情報と自社の情報を分離して管理しておくこと、③受け取ったものが営業秘密侵害品でないことを確認すること、④情報へのアクセスや持出し等のログを保管しておくこと等を日頃より実施しておくことが重要であると指摘されている。

2.5.1. 転職者受入れ時の対策

本アンケート調査結果によれば、転職者の受入れ時における対策（「前職で締結している契約関係を確認している」「前職の営業秘密を持ち込まない誓約書を提出させる」「業務内容を定期的に確認している」）についてはいずれも１割未満の企業でしか実施されておらず、取組が遅れている。また、84.3%の企業が「特にない」と回答している（図 2.5-1）。

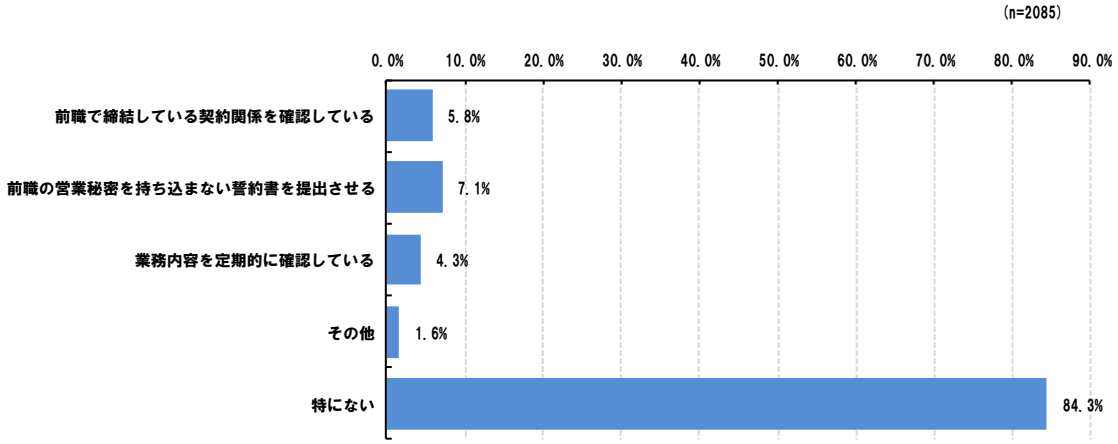

図 2.5-1 転職者受入れ時の対策（全業種・全規模）（問 47）

業種・規模別に見ると、大規模の製造業では 18.6%の企業で「前職の営業秘密を持ち込まない旨を記した誓約書の提出」を実施しており、また 16.1%の企業で「前職の企業との間で締結している契約関係の確認」を実施していることが特徴的ではあるが、その他の業種・規模の企業ではほとんどの対策が実施されていない状況である（図 2.5-2）。

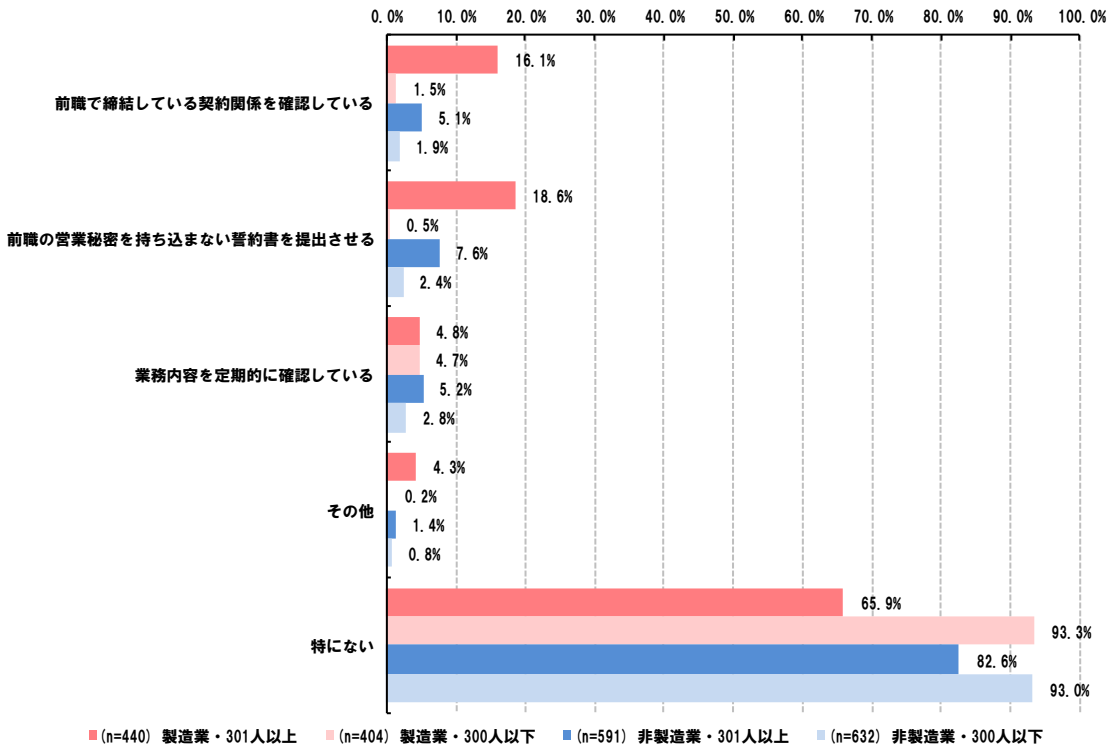

図 2.5-2 転職者受入時に実施している対策（業種別・規模別）（問 47）

インタビュー調査においては、受け入れた転職者を一定期間、前職での業務とは関係のない業務に従事させるようにした例があったが、前職での営業秘密を使用しない旨を記載した誓約書等は特に提出させていないという例も複数あった。

【転職者受入れ時の対策例（インタビュー調査結果）】

（一定期間の業務内容制限）

- 競合から転職してきた社員を受け入れるケースはあったが、あらかじめ事業部長に伝えた上で 1 年間、全く関係のない業務に従事してもらった。（製造業）

（書面による誓約等の取り交わしなし）

- 他社からの採用者に対して、入社後の守秘義務契約はしているが、前職で得た情報を使用しないような書面での誓約は交わしていない。（製造業）
- 他社からの転職者の受け入れについては、人事担当者が経歴を確認している。加えて入社時の情報セキュリティ研修で情報の取扱いの注意喚起を行っているが、前職の情報を持ち込まないという誓約は交わしていない。（非製造業）

2.5.2. 共同・受託研究開発実施時の対策

本アンケート調査結果によると、25.8%の企業が「情報授受の際に秘密保持契約を締結」といった取組を実施していることがわかる。一方で、その他の対策についてはいずれも 1 割未満の企業でしか実施されていない。また、65.9%の企業が「特にない」と回答している（図 2.5-3）。

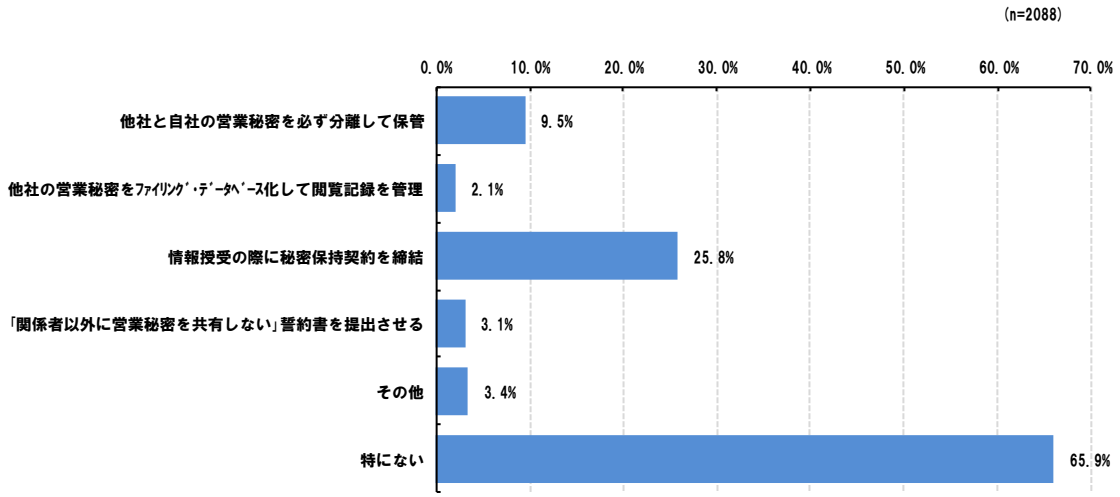

図 2.5-3 共同・受託研究実施時の対策（全業種・全規模）（問 48）

業種・規模別に見ると、製造業の大規模企業では 66.0%の企業が「情報授受の際に秘密保持契約を締結」と回答しており、その他の業種・規模の企業と比較して取組が進んでいる。一方で中小規模企業ではこうした対策がほとんど実施されておらず、また大規模企業であっても非製造業については、製造業の大規模企業と比較すると取組が遅れていることが窺える（図 2.5-4）。

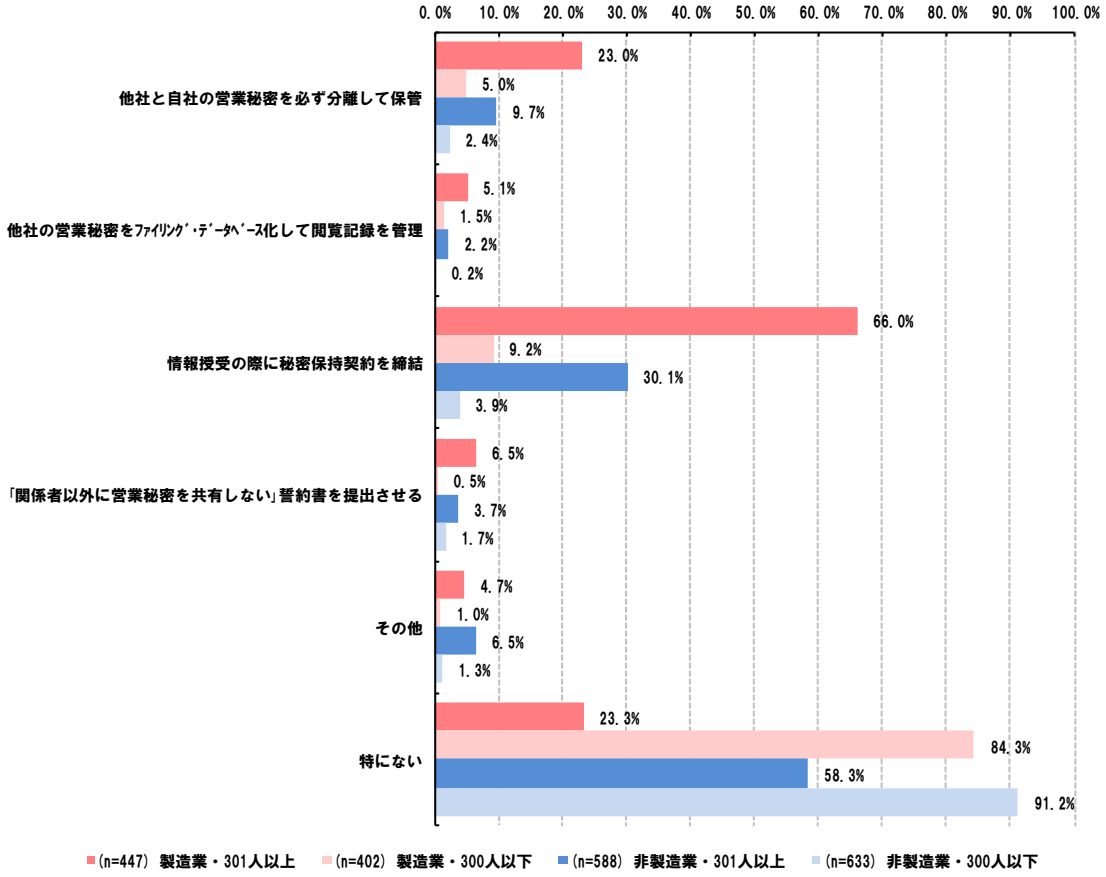

図 2.5-4 共同・受託研究実施時の対策（業種別・規模別）（問 48）

2.5.3. 取引時の対策

本アンケート調査結果によれば、23.4%の企業で「取引先から開示された営業秘密を取り扱う自社社員の限定」が実施されている一方で、その他の対策は 1 割前後の企業でしか実施されておらず、現状では十分な取組がなされていないことが窺える（図 2.5-5）。

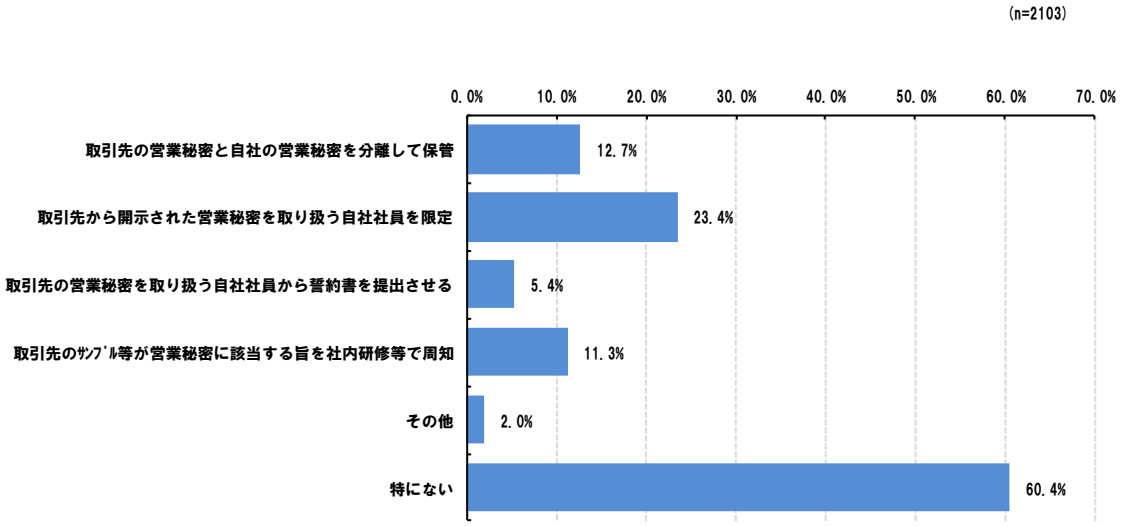

図 2.5-5　取引先向けの対策（全業種・全規模）（問 49）

業種・規模別に見ると、大規模の製造業では、41.9%の企業「取引先から開示された営業秘密を取り扱う自社社員の限定」を実施しており、また「取引先のサンプル等が営業秘密に該当する旨を社内研修等で周知」「取引先の営業秘密と自社の営業秘密を分離して保管」につては、それぞれ 24.7%、24.4%で実施されている（図 2.5-6）。

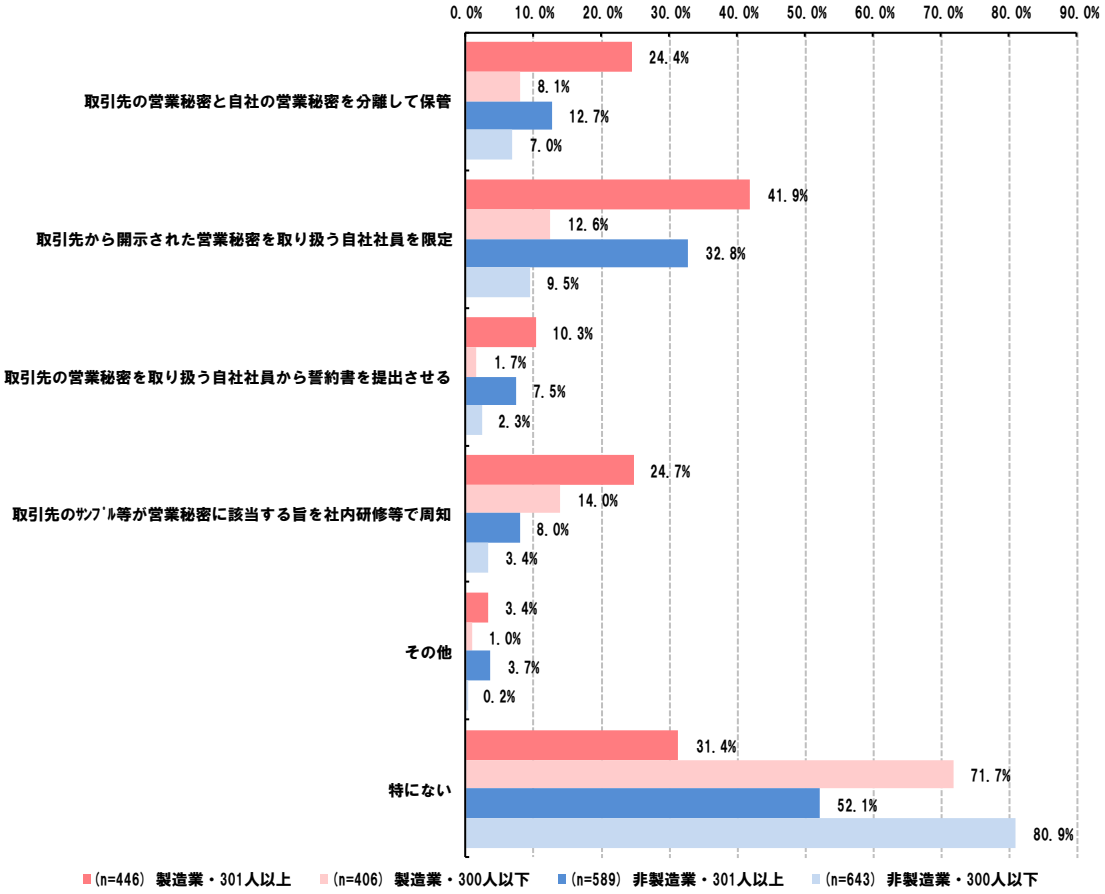

図 2.5-6　取引先向けの対策（全業種・全規模）（問 49）

2.5.4. 技術情報・営業情報の売込み時の対策

本アンケート調査結果によれば、20.8%の企業が「そもそも売込みに応じない」と回答している。一方で、その他の対策については１割未満の企業でしか実施されていない。また、65.1%の企業が「特に実施していない」と回答している（図 2.5-7）。

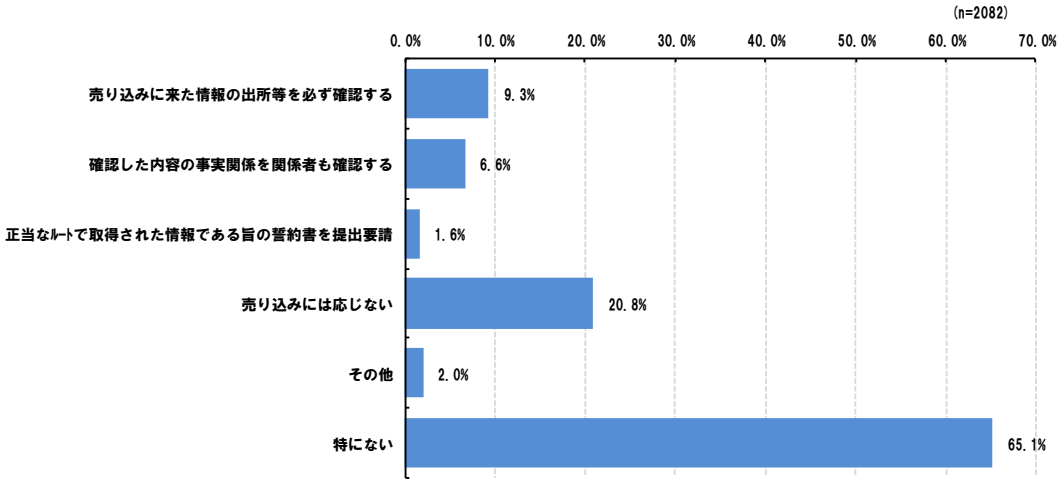

図 2.5-7　外部者による売込みへの対策（全業種・全規模）（問 50）

業種・規模別に見ると、「そもそも売込みに応じない」という回答が全業種・規模で一定程度見られた。一方で、「売り込みに来た情報の出所等を必ず確認する」については、製造業の大規模企業では 17.1%で実施されているが、中小規模企業では５%前後に留まっている（図 2.5-8）。

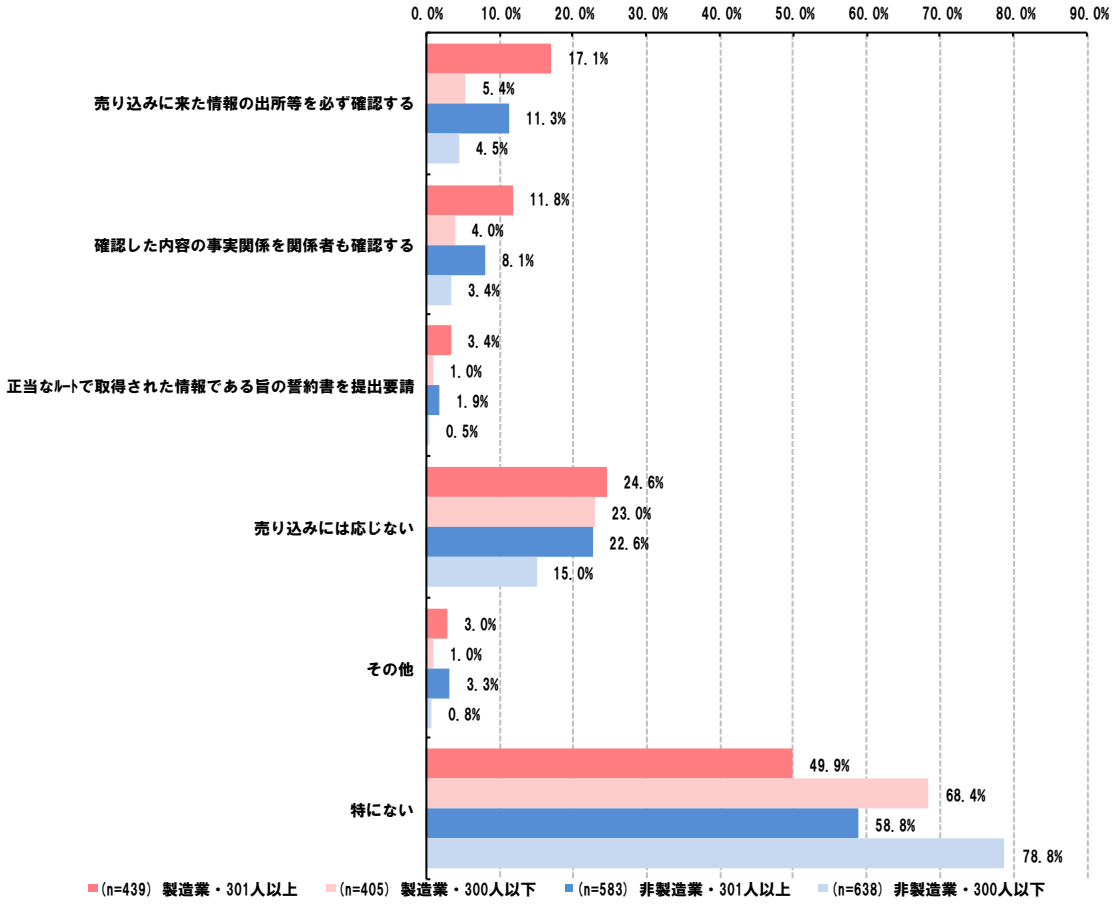

図 2.5-8　外部者による売込みへの対策（業種・規模別）（問 50）

3. 営業秘密管理を取り巻く環境

情報端末の性能の向上等に伴い、情報端末を通じて扱われる情報は質・量共に変化し、その重要性を増している。また、そうした電子化された情報を対象とした標的型攻撃が増加しており、営業秘密管理に取り組んでいく際にも見過ごすことができない脅威となっている。

今回実施した調査結果から、営業秘密を取り巻く環境への認識について、以下の実態が明らかになっている。

- 営業秘密の漏えいリスクの高まりを感じる社会動向の変化について、51.9%の企業が「標的型攻撃の増加」、51.4%の企業が「スマートフォン・タブレット機器等の急速な普及」と回答している。一方、11.6%の企業が「高まっていると感じていない」と回答している。
- 53.4%の企業において、データを重要な経営資源と捉えて営業秘密として取り扱う意思があり、実際に 23.8%の企業においては既に営業秘密として管理していると回答している。
- オープンイノベーションに関する取組については、59.7%の企業が「全く検討していない」と回答しており、「具体的な取組をしており、成果が出ている」と回答した企業は7.7%に留まっている。
- オープン＆クローズ戦略に関するノウハウの管理・活用に関する取組については、21.3%の企業が「権利化するものとノウハウとして秘匿するものを社内で都度検討」と回答している。一方で、65.8%の企業においては特に取組が実施されていない。
- 平成 26 年 10 月 1 日～平成 28 年 8 月 23 日までの判例の中で、営業秘密が争点となったものは 35 件あり、うち営業秘密として認定されたものは 12 件であった。

3.1. 社会動向の変化と営業秘密への関心

スマートフォンやタブレット機器等の普及により、営業秘密を含めた様々な情報がネットワークに接続された情報端末を通じて扱われる機会が増加しており、これまで以上に標的型攻撃等に伴う情報漏えいのリスクに対する認識を高めておく必要がある[9]。また、業種や職種にもよるが、転退職等に伴う人材の流動化や、他社との連携機会の増加という点も、やはり情報漏えいリスクを伴う社会動向の変化と捉える事ができると考えられる。

本アンケート調査結果によれば、社会動向の変化のうち「標的型攻撃の増加」については51.9%の企業が、「スマートフォン・タブレット機器等の急速な普及」については51.4%の企業が情報漏えいリスクを感じている。また、41.8%の企業が「データの活用機会の増加」について漏えいリスクの高まりを感じており、総じて情報機器の発展・普及に関連したリスクを多くの企業が感じていると捉えられる。また。33.7%の企業については、「人材の流動化」について、情報漏えいのリスクを感じており、情報システム面での対策だけでなく、人的な対策についても日頃から注意すべき状況であることが窺える（図 3.1-1）。

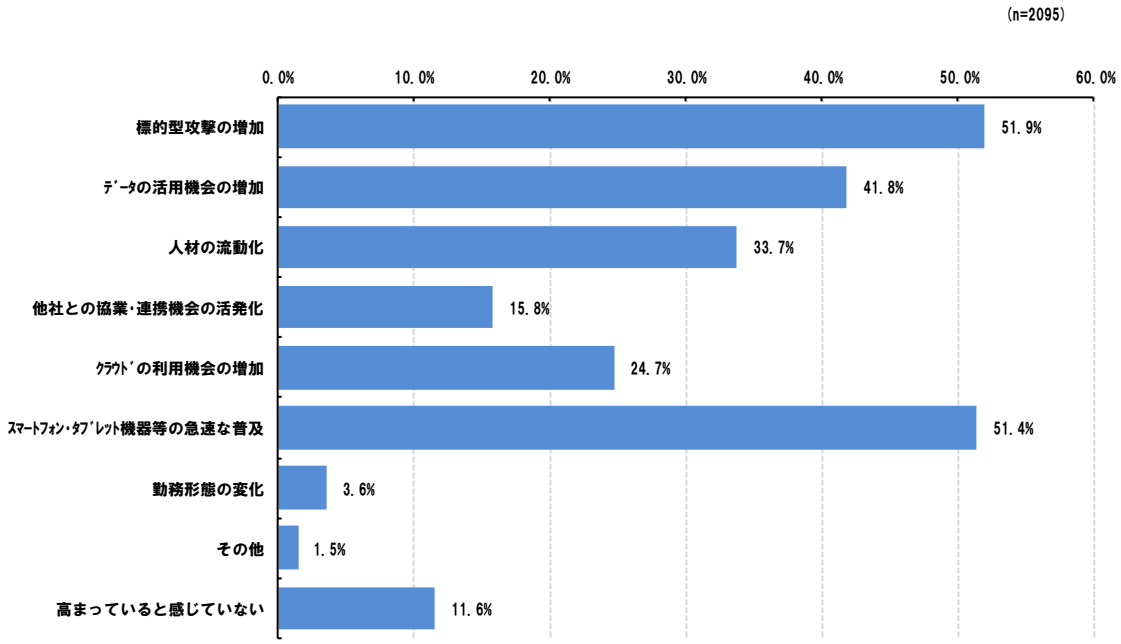

図 3.1-1 情報漏えいのリスクを感じる社会的動向の変化（全業種・全規模）（問 19）

業種・規模別に見ると、大規模企業についてはほぼ全ての企業が何かしらの社会動向の

9 平成 28 年 3 月 17 日に警察庁より公表された広報資料「平成 27 年におけるサイバー空間をめぐる脅威の情勢について」によれば、平成 27 年における標的型メール攻撃の件数が平成 26 年の 1,723 件から大きく増加して 3,828 件であったことが報告されている。
https://www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf

変化に対して、情報漏えいのリスクを感じており、特に「標的型攻撃の増加」「スマートフォン・タブレット機器等の急速な普及」については６割以上の企業がリスクを感じている。また、特に大規模の製造業ではこれらに加えて「人材の流動化」や「他社との協業・連携機会の活発化」についても多くの企業でリスクと捉えられている（図 3.1-2）。

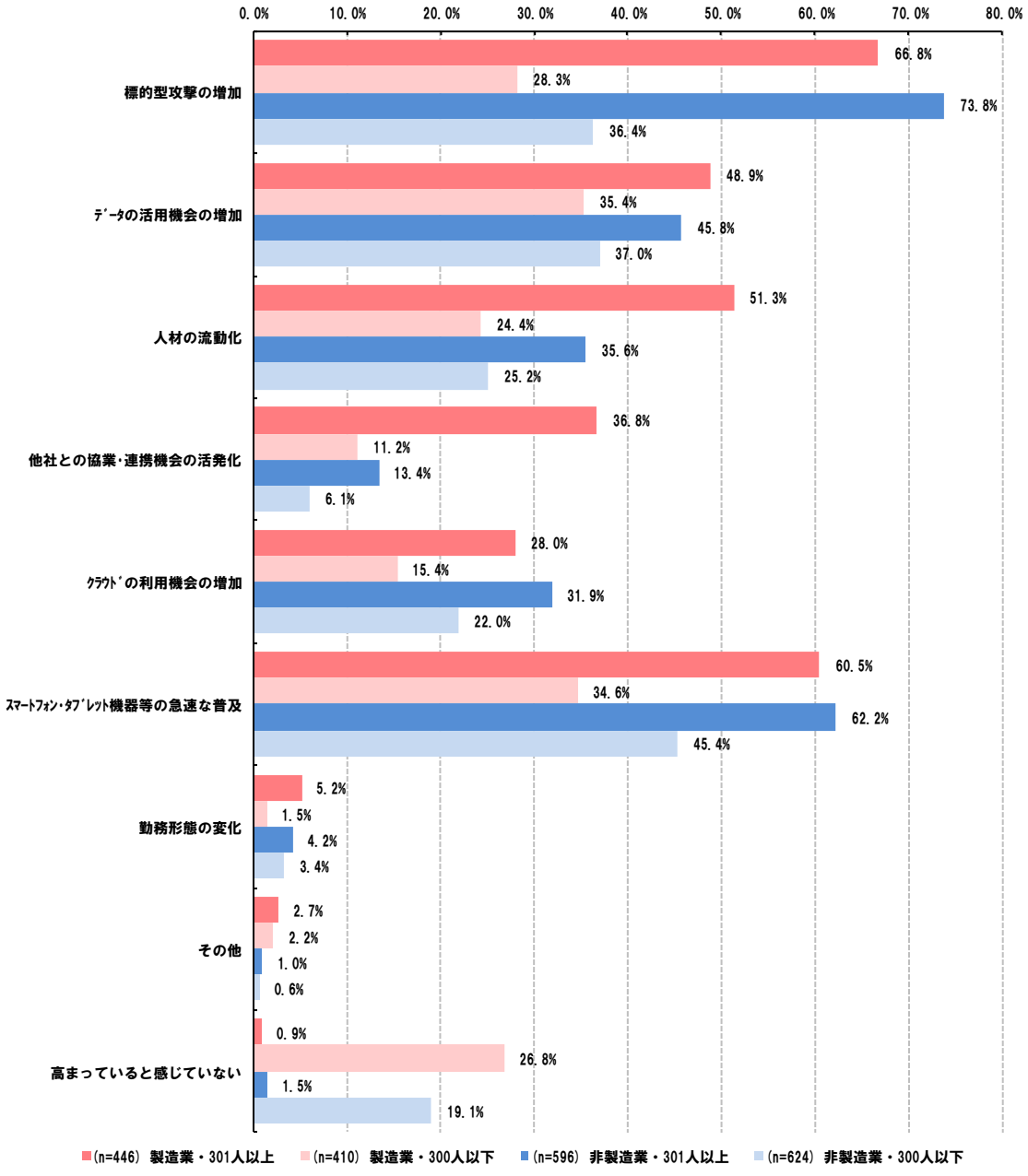

図 3.1-2 情報漏えいのリスクを感じる社会的動向の変化（業種・規模別）（問 19）

標的型攻撃等、情報システム面でのリスクへの関心が高まっているが、本アンケート調

査結果によれば、49.2%の企業が半分程度もしくはそれ以上の量の営業秘密を電子化して管理していると回答している（図 3.1-3）。管理手法は企業の考え方によって異なるものであるため、営業秘密を電子化すること自体が問題というわけではないが、標的型攻撃やばらまき型の攻撃が増加している状況等も踏まえて、電子化された情報に対してはシステム的な対策を十分に行う必要がある。

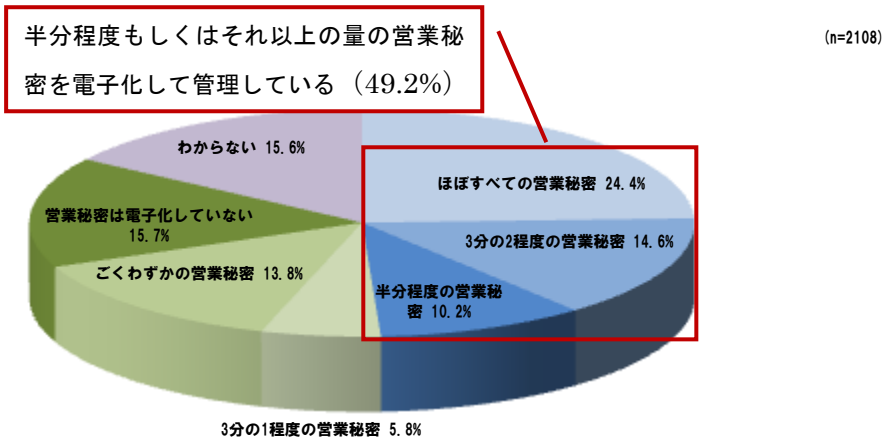

図 3.1-3　電子化した状態で管理されている営業秘密（全業種・全規模）（問 20）

また、クラウド活用の進展に伴うビッグデータの集積や AI（人工知能）技術の進展によって、これまで価値が無いと見なされていたデータを収集・分析・活用することで、既存ビジネスの効率化や新たなビジネス・サービスを創出することへの関心が社会的に高まってきている[10]。こうした社会的動向の中、本アンケート調査結果によれば、53.4%の企業がデータを営業秘密と捉えて管理する意思があるという状況が明らかとなった（図 3.1-4）。

10 「日本再興戦略 2015 改訂」（2015 年 6 月）において、アベノミクスの更なる発展のために新産業構造ビジョンとして「① IoT・ビッグデータ・人工知能がもたらす変革の姿や時期（産業構造、就業構造、経済社会システムの変革）、②ビジネスチャンスの可能性、③官民が行うべき対応（規制制度改革、研究開発・設備・人材投資等）、について時間軸を明確にしながら検討」を提示している。このような動きを踏まえ、経済産業省では 2015 年 9 月より新産業構造部会を設置し、IoT・ビッグデータ・人工知能をはじめとした新たな技術による産業構造の変革を「第 4 次産業革命」と捉え、データの収集・蓄積とその利用手法・戦略が付加価値の新たな源泉として重要となる可能性について言及している。新産業構造部会は、2015 年 9 月の設置以降、2016 年 12 月までに計 12 回実施されている。

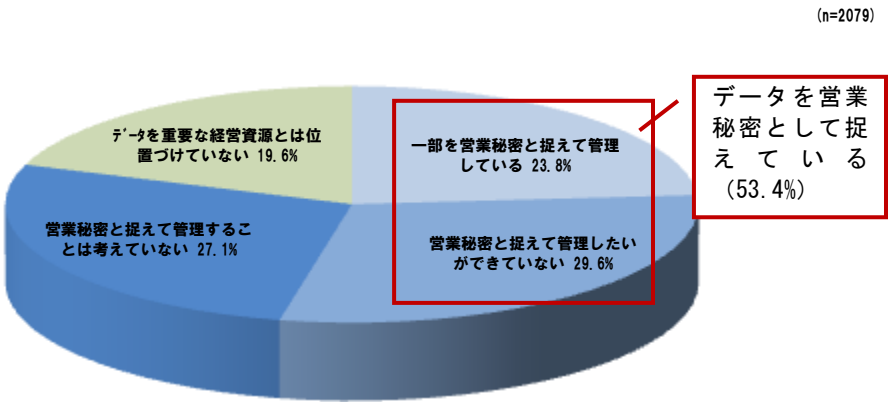

図 3.1-4　データに対する考え方（全業種・全規模）（問 30）

こうした意識は、大規模企業の方が高い傾向にあり、７割前後の企業でデータを営業秘密として捉えて管理していく意思がある傾向が見られた。一方で、中小規模企業においては、データを営業秘密として捉えていない企業の割合が６～７割存在しているだけでなく、そもそもデータを営業秘密どころか重要な経営資源としても捉えていない企業も３割程度存在しており、企業の規模によってデータに対する考え方に差があることが窺える（図 3.1-5）。

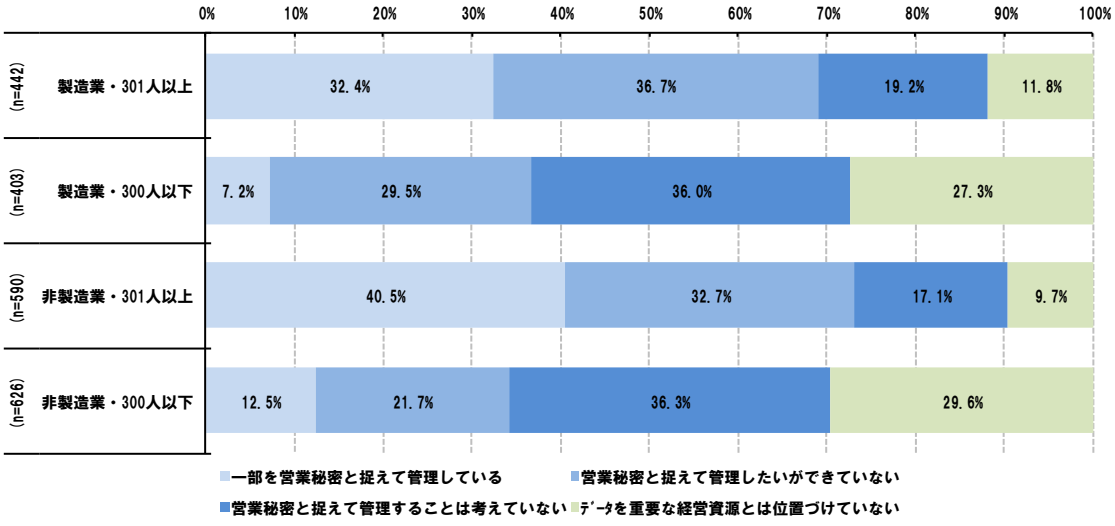

図 3.1-5　データに対する考え方（業種・規模別）（問 30）

なお、インタビュー調査においては、データを営業秘密として守りたいが、どのようにすればよいかわからないという趣旨のコメントがあった。

【データ利活用に関するコメント（インタビュー調査結果）】

・ データの利活用に取り組んでいく中で、営業秘密として守りたいものはあるが、どのようにすれば守れるかを思案中である。（製造業）

昨今、技術やアイデア等を他社と交流させることでイノベーションの促進を図る活動（オープンイノベーション[11] [12]）に対する注目が集まっているが、こうした活動への取組については 59.7%の企業が「全く検討していない」という状況であった。一方で、7.7%という少数の企業ではあるが、具体的な取組を推進し成果が出ていると回答している（図 3.1-6）。

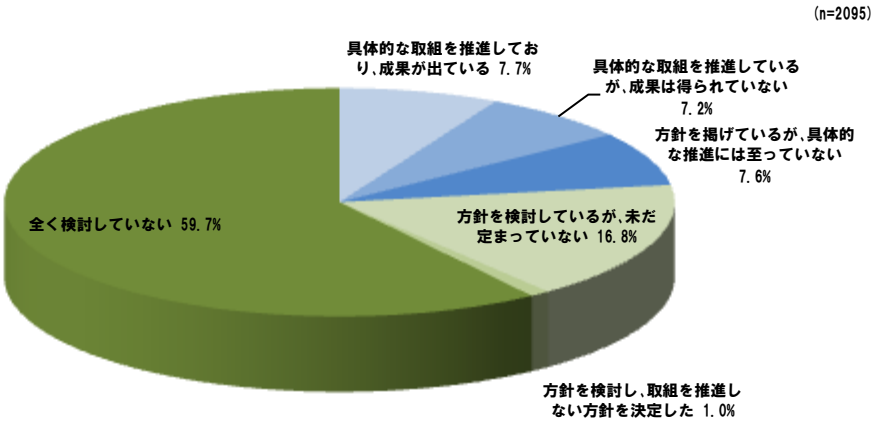

図 3.1-6　オープンイノベーションに関する取組（全業種・全規模）（問 29）

こうした取組を通じて外部との連携を実施していくにあたっては、日頃から自社のノウハウをしっかりと管理することが重要[13]であるが、本アンケート調査結果によれば、65.8%

[11] Henry W. Chesbrough は著書「Open Innovation」（2003 年）の中で、オープンイノベーションを「組織内部のイノベーションを促進するために、意図的かつ積極的に内部と外部の技術やアイデアなどの資源の流出入を活用し、その結果組織内で創出したイノベーションを組織外に展開する市場機会を増やすことである」と定義している。

[12] オープンイノベーション協議会（JOIC。事務局：NEDO）は、「日本企業を取り巻く競争環境が厳しさを増す中、自社のリソースのみで、新たな顧客の価値を生み出すイノベーションを起こすことはもはや不可能であり、世界中に広がるリソースを活用するオープンイノベーションは、企業にとって必須の戦略である」と捉え、わが国のオープンイノベーションの推進に向けた取組として、2015 年度にセミナー3 回、連携イベント 2 回、ワークショップ 2 回、マッチングイベント 6 回を実施したほか、2016 年 7 月にはオープンイノベーションに関する調査として「オープンイノベーション白書」を報告している。

[13] 近畿経済産業局「中小・ベンチャー企業のためのオープン・イノベーション ハンドブック」（平成 28 年 2 月）では、特に中小企業やベンチャー企業が他社とのオープンな連携を進めて行く上での留意点等が整理されている。その中で、連携前に社内で実施するべきこととして、営業秘密として扱う情報の仕分けが重要である点や、自社のノウハウを守るための対策（契約）について触れられている。

の企業がノウハウの管理・活用に関する取組について「特に実施していない」と回答している。「権利化するものとノウハウとして秘匿するものを社内で都度検討」については 21.3%の企業で実施されているが、「ノウハウを契約で他社にライセンス」といった活用に関する取組や「ノウハウを形式知化して管理」といった取組については 5%以下の企業でしか実施されていない（図 3.1-7）。

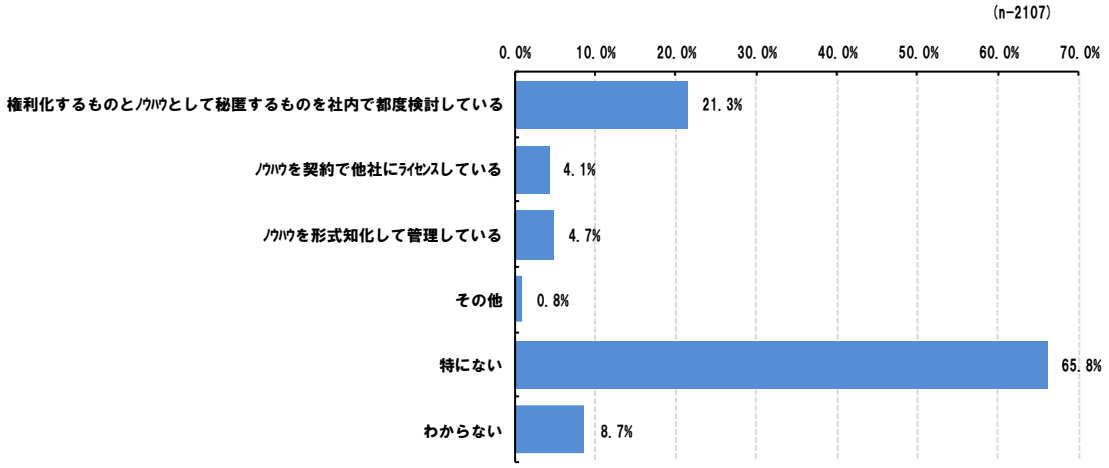

図 3.1-7　ノウハウの管理・活用に関する取組（全業種・全規模）（問 27）

業種・規模別に見ると、大規模の製造業では 58.1%の企業で「権利化するものとノウハウとして秘匿するものを社内で都度検討」が実施されており、また「ノウハウを契約で他社にライセンス」については 11.7%、「ノウハウを形式知化して管理」についても 11.9%の企業で実施されている。一方で、その他の業種・規模の企業では、大規模の製造業と比べると、ほとんどの取組がなされていない状況であった（図 3.1-8）。

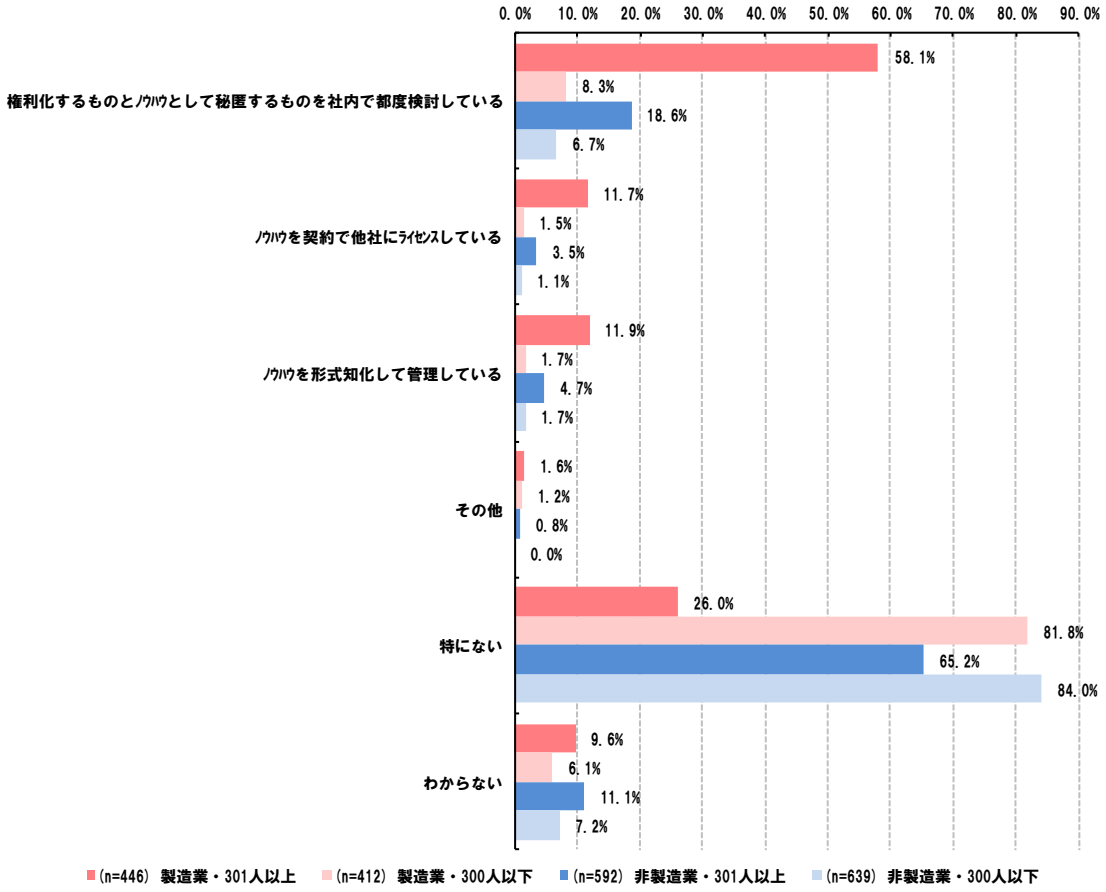

図 3.1-8　ノウハウの管理・活用に関する取組（業種別・規模別）（問 27）

「ノウハウを契約で他社にライセンス」を実施している企業が他社にライセンスしているノウハウ件数の過去５年間における推移は、68.0%の企業で「横ばい」もしくは「増加傾向」であった（図 3.1-9）。

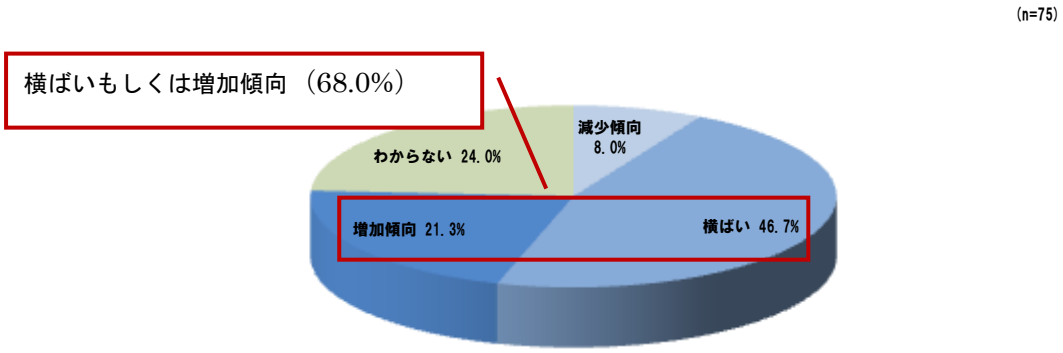

図 3.1-9　他社にライセンスしているノウハウ件数の推移（全業種・全規模）（問 28）

「ノウハウを形式知化して管理」を実施している企業が管理しているノウハウの件数の過

去５年間における推移は、72.7%の企業で「横ばい」もしくは「増加傾向」であった（図3.1-10）。

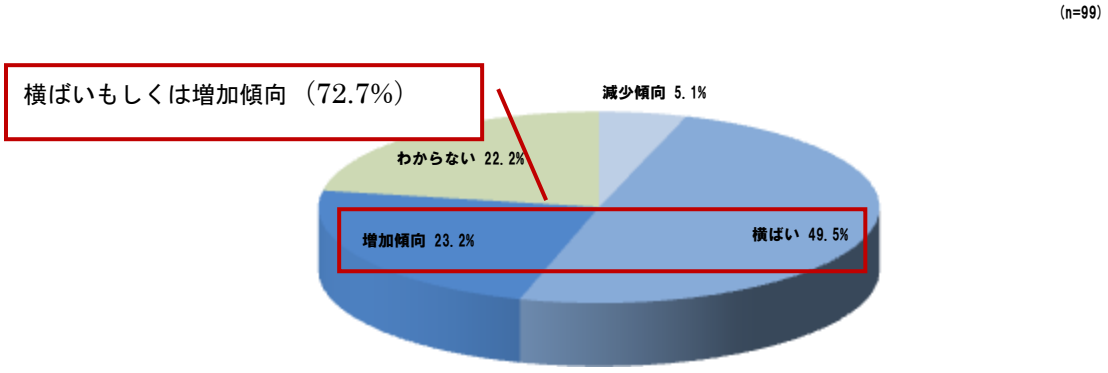

図 3.1-10　形式知化して管理しているノウハウの推移（全業種・全規模）（問 28）

3.2. 政策への関心・要望

2016 年２月に、経済産業省が秘密情報の漏えい対策として有効な情報を紹介する資料として、「秘密情報の保護ハンドブック」を公表したところではあるが、本アンケート調査結果によれば 34.4%の企業がこの存在自体は認知していると回答している。ただし、社内で活用していると回答した企業は 3.0%であり、存在の認知だけでなく、更なる活用も望まれるところである（図 3.2-1）。

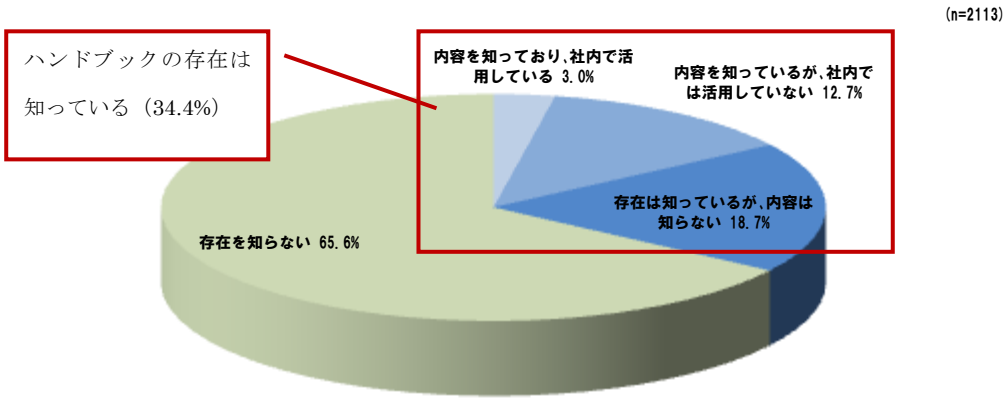

図 3.2-1　秘密情報の保護ハンドブックの認知状況（全業種・全規模）（問 58）

業種・規模別に見ると、大規模の製造業において相対的に活用されており、8.5%の企業が「内容を知っており、社内で活用している」と回答している。一方で、中小規模企業においては８割程度の企業が「存在を知らない」と回答しており、さらなる周知の取組が必要であると思われる（図 3.2-2）。

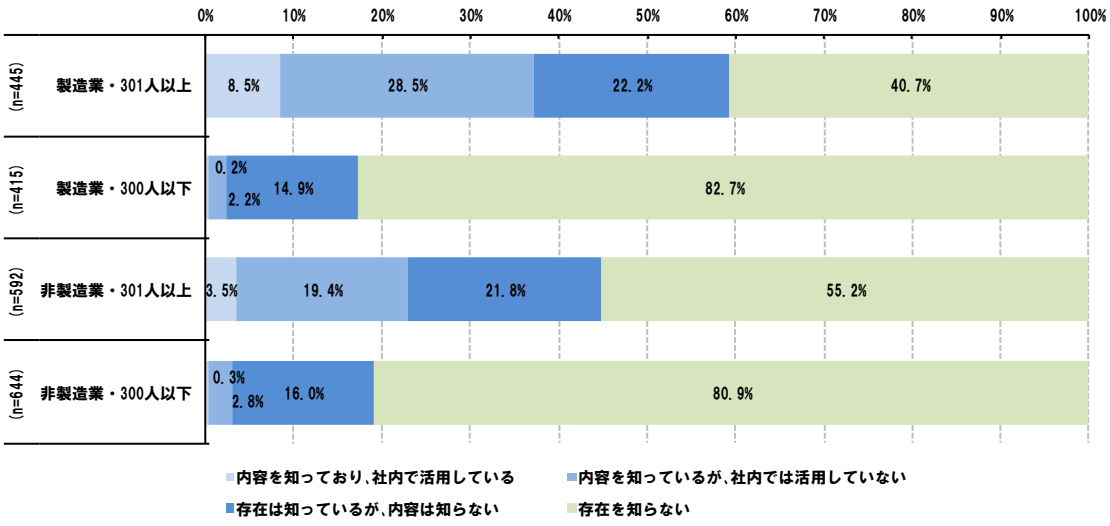

図 3.2-2　秘密情報の保護ハンドブックの認知状況（業種・規模別）（問 58）

「内容を知っており、社内で活用している」と回答した企業における具体的な活用方法としては、以下のような事例が回答として得られている。

【「秘密情報の保護ハンドブック」の活用方法（アンケート調査結果）】
- 社内の営業秘密管理規程および業務の見直しに活用した。（製造業）
- 社内研修資料作成時の参考とした。（製造業）
- 社内体制見直しの検討材料として活用した。（製造業）
- 海外関係会社への情報管理説明会で活用した。（製造業）

なお、営業秘密や情報管理になじみのない企業等においても、秘密情報の保護ハンドブックの有効活用をサポートする情報として、経済産業省が平成 28 年 12 月 5 日に「秘密情報の保護ハンドブックのてびき[14]」を公開した。

企業が今後提供を望む営業秘密管理に関する情報として、本アンケート調査結果によれば 49.5%の企業が「営業秘密管理に関する失敗事例」と回答しており、営業秘密管理にしっかりと取り組まないことによって、企業にどのような影響があるのかを知りたいというニーズを読み取れる。この点について、法律専門家へのインタビュー調査において、「営業秘密が争点になった過去の判例の中で、営業秘密該当性が否定されたケースを失敗事例として紹介することが有用ではないか」とのコメントがあった。「営業秘密管理に関する優良事例」を望む回答も 40.4%あり、具体的に何を実施すればよいのかを知りたいという企業も一定数いることが窺える。また、「企業の規模や業種等に応じた営業秘密管理の取組状況に関する相場観」を望む企業も 39.3%存在しており、自社と似たような企業が、実際にどの程度の水準の対策を実施しているのかを知りたいという企業のニーズであると捉えられる（図 3.2-3）。

14 経済産業省「秘密情報の保護ハンドブックのてびき」
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/hbtebiki.pdf

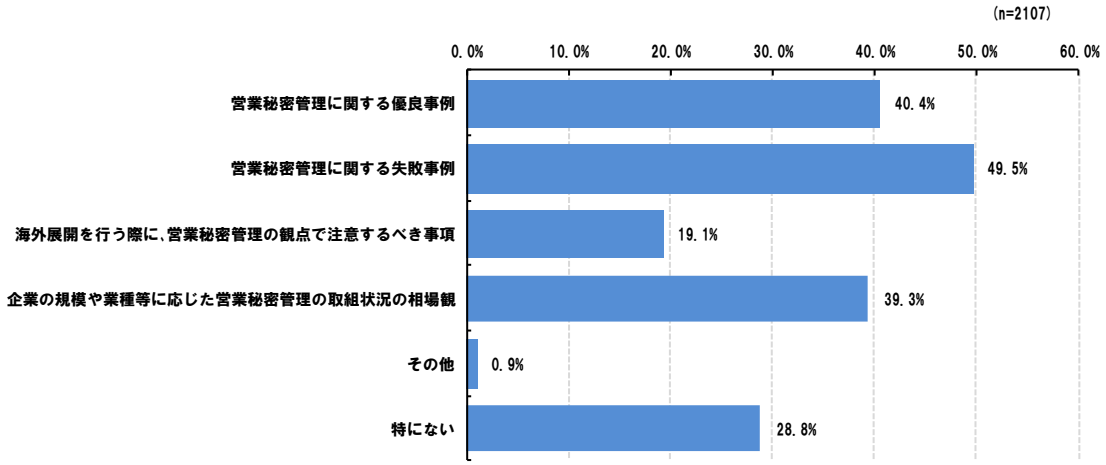

図 3.2-3　営業秘密管理について提供を希望する情報（全業種・全規模）（問 59）

業種・規模別に見ると、中小規模企業では「特にない」という回答が 4 割以上あり、営業秘密管理に対する関心が大規模企業と比較して低い傾向にあることが窺える。一方、大規模企業については、全ての項目に対して比較的関心が高く、また大規模の製造業については「海外展開を行う際に営業秘密管理の観点で注意するべき事項」を望む企業が 52.9%存在しており、この背景として今後海外展開を進めて行こうとしている企業が増えていることや、現に海外に拠点を有している中でどのように営業秘密管理を実施すればよいか悩んでいる等の事情があるものと類推され、大規模の製造業に特徴的なニーズとして捉える事ができると思われる（図 3.2-4）。

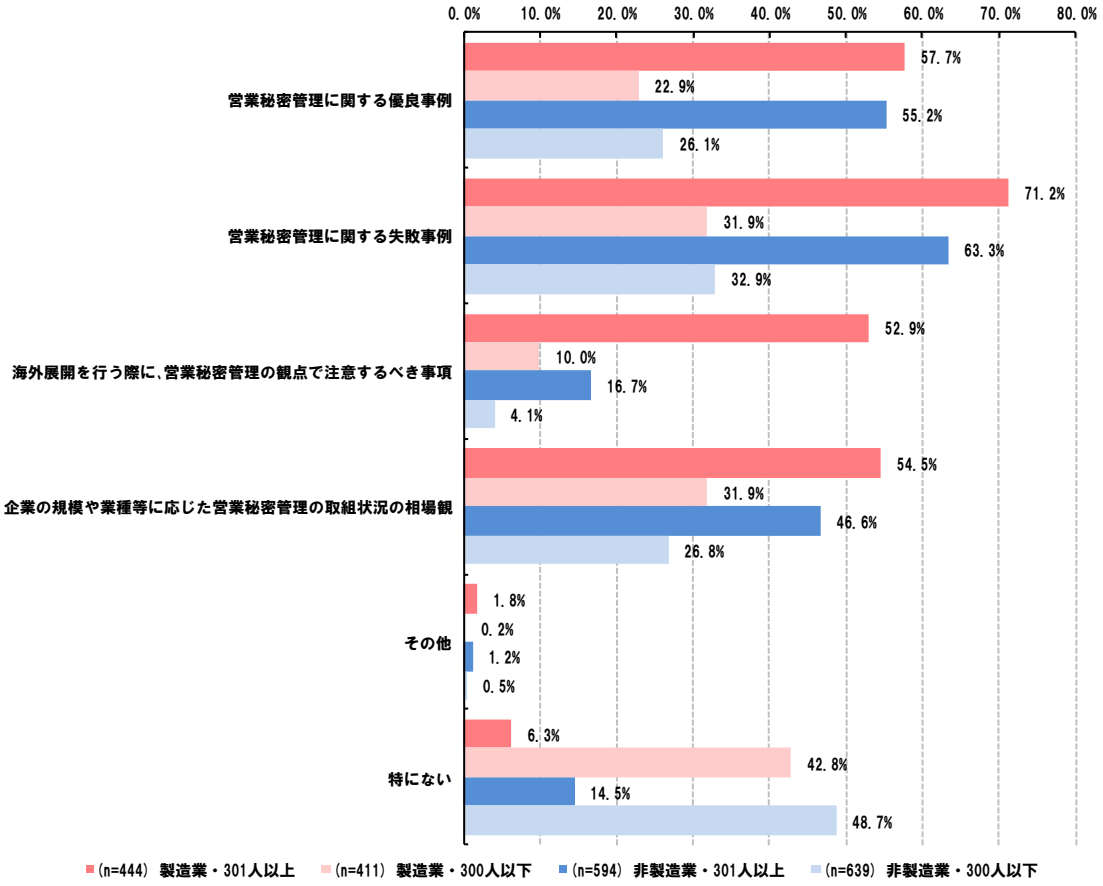

図 3.2-4　営業秘密管理について提供を希望する情報（業種・規模別）（問 59）

3.3. 営業秘密の漏えいに関する判例の動向

3.3.1. 調査概要

3.3.1.1. 判例の抽出方法

判例データベース（LEX/DB）を用いて、「営業秘密」というキーワードで抽出された判例について、営業秘密が争点になっているものと争点になっていないものの仕分けを実施した。営業秘密が争点になっているものを今回の調査対象とし、さらに営業秘密としての認定の有無という観点で仕分けを行った。

営業秘密として認定された判例と、認定されていない判例の比較を行うことにより、営業秘密として認定する上での裁判所の判断のポイント等についての分析を行った(図 3.3-1)。

なお、調査の対象は平成 26 年 10 月 1 日～平成 28 年 8 月 23 日までの判例としている。

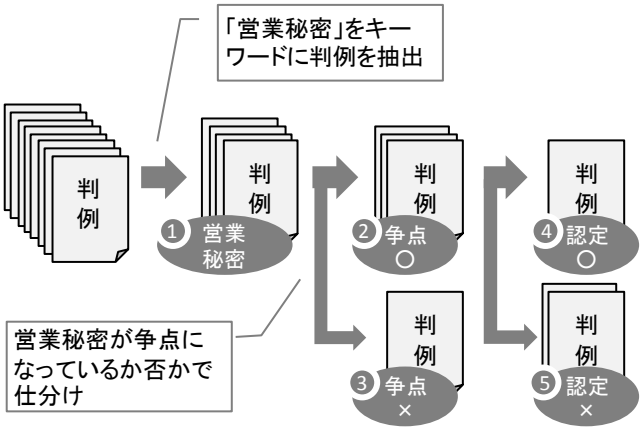

図 3.3-1 判例抽出フロー

3.3.1.2. 抽出結果

3.3.1.1.で記した方法で抽出した結果、次の件数の判例が抽出された（図 3.3-2)。

① 「営業秘密」というキーワードで抽出された判例【72 件】
② ①のうち、営業秘密が争点になった判例【35 件】
③ ①のうち、営業秘密は争点になっていない判例【37 件】
④ ②のうち、営業秘密として認定された判例【12 件】
⑤ ②のうち、営業秘密として認定されなかった判例【23 件】

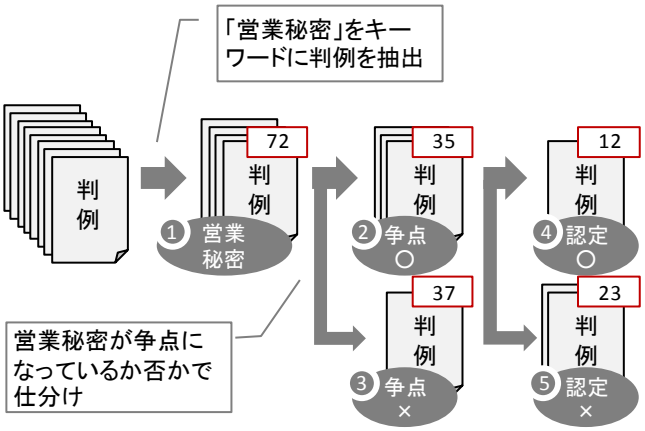

図 3.3-2 抽出された判例の件数

3.3.1.3. 裁判所における判断

営業秘密関連の判例の中で裁判所が行う判断の傾向を調査するにあたり、①営業秘密 3 要件（秘密管理性・有用性・非公知性）の判断に際して、裁判所はどのような営業秘密管理に係る取組を肯定的に評価しているのかという点と、②営業秘密に係る不正行為[15]の有無についてどのような判断がなされているのかという点に特に着目した。

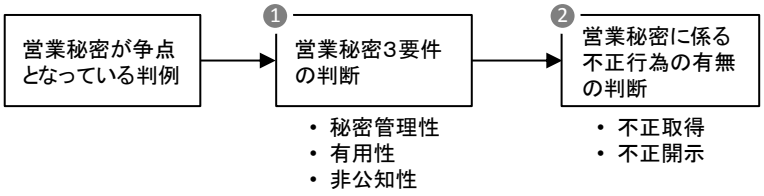

図 3.3-3 裁判所の判断フローと認定のポイント

3.3.2. 営業秘密に係る 3 要件の判断について

抽出された 35 件の判例において、3 要件すべてについて肯定・否定を明確に認定してい

[15] 営業秘密に係る不正行為は、「営業秘密の不正取得行為（不正競争防止法 2 条 1 項 4 号・5 号・6 号）」と「営業秘密の不正開示行為（同 7 号・8 号・9 号）」に分類される。平成 27 年不正競争防止法改正によって、これらの 2 つの類型の中で、技術上の秘密に関する不正使用行為によって生じた物の、譲渡、引渡又は引渡のための展示、輸出、輸入、電気通信回線を通じて提供する行為を新たに追加した。

るものは 9 件であり、うち 5 件が 3 要件すべてを肯定、4 件が 3 要件すべてを否定している。判例は事案毎に個別性が高く、当事者の主張内容によってもその判断が大きく異なり、必ずしも 3 要件が全て精緻に検討されている訳ではない。

また抽出された 35 件の判例の中で問題となっている情報等が、営業秘密に該当すると認定されたものは 12 件であるが、うち秘密管理性が明確に肯定されているのが 7 件[16]、有用性が明確に肯定されているのが 8 件、非公知性が明確に肯定されているのが 5 件である。秘密管理性の判断については、どのような事項が肯定的に捉えられたのか、また逆に否定的に捉えられたのかについて把握することで、企業が現在行っている営業秘密管理に係る取組について検証を行ったり、今後取り組もうとしている事項について優先順位や程度感を検討する際の参考とすることが出来る。また秘密管理性についてはもちろん、有用性や非公知性が否定された判例の中には、それぞれの要件について十分な証拠を上げることが出来なかったものがあり[17]、実際に司法救済を求める場合、どの程度の証拠を準備しておく必要があるか（その前提としてどのような管理が必要となるか）についても参考となる。

表 3.3-1 対象とした判例一覧

判例	民事／刑事	情報の性質	秘密管理性の判断に関連して争点となった事項							秘密管理性	有用性	非公知性	営業秘密該当性
			情報区分・表示	秘密保持義務	社内規程等	研修等	アクセス制御	施錠管理	その他				
大阪地判 H26.10.23	民	技	－	－	○	－	－	○	－	否定	否定	－	否定
		営	－	－	－	－	－	－	－	－	否定	－	否定
東京地判 H26.11.20	民	技	－	●	－	－	－	－	－	－	否定	－	★ ※1

16 経済産業省（委託先：NTT データ経営研究所）「平成 26 年度産業経済研究委託事業（営業秘密保護制度に関する調査研究）」では、平成 22 年～平成 26 年までに営業秘密の「秘密管理性について判断を行った判例 28 件」を対象とした調査を行っている。28 件の判例のうち、秘密管理性を肯定した判例が 12 件、否定したものが 16 件であったと報告している。
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/26chousa-hontai.pdf

17 例えば秘密管理性について、「抽象化された「発想」が，どのように秘密として管理されていたかについて，被告は何ら具体的に主張しておらず，これ以上検討するまでもなく，この点についての被告の主張は失当（大阪地判 H26.10.23 [LEX/DB: 25446744]）」、「各業者間において技術情報が秘密管理されるべきこと，互いに尊重すべきことについて暗黙の了解がされていると主張するにとどまり，本件において，原告が被告に開示した技術情報について，これに接する者が営業秘密であることが認識できるような措置を講じていたとか，これに接する者を限定していたなど，具体的に秘密として管理されている実体があることについて，主張も立証もしていない（東京地判 H26.12.19 [LEX/DB: 25540842]）」といった指摘がなされている判例がある。

判例	民事／刑事	情報の性質	秘密管理性の判断に関連して争点となった事項							秘密管理性	有用性	非公知性	営業秘密該当性
			情報区分・表示	秘密保持義務	社内規程等	研修等	アクセス制御	施錠管理	その他				
東京地判 H26.12.19	民	技	－	●	－	－	－	－	－	否定	－	－	否定
名古屋地判 H27.1.20	刑	営	－	－	－	－	－	－	－	－	－	－	肯定 ※2
知財高判 H27.2.19	民	営	－	○ ※3	○ ※3	－	○ ※3	○ ※3	－	肯定	肯定	肯定	肯定
東京地判 H27.2.27	民	著	－	－	－	－	－	－	－	－	－	否定	否定
東京地判 H27.3.9	刑	技	－	○	○	－	○	－	－	－	－	－	肯定 ※4
大阪地判 H27.3.12	民	営	－	－	－	－	－	－	－	－	－	－	★
東京地判 H27.3.27	民	経	－	－	－	－	○	－	－	肯定	肯定	肯定	肯定
知財高判 H27.5.27	民	技	－	● ※5	－	－	－	－	－	否定	－	－	否定
名古屋高判 H.27.7.29	刑	技	－	－	－	－	－	－	－	－	肯定	－	肯定 ※6
東京地判 H27.8.27	民	技	－	●	－	－	－	－	－	否定	－	否定	否定
		営	－	－	－	－	●	●	－	否定	否定	否定	
東京地判 H27.9.3	民	技	－	－	－	－	－	－	－	－	－	－	★
東京高判 H27.9.4	刑	技	－	－	－	－	－	－	－	－	肯定 ※7	－	肯定
東京地判 H27.9.11	民	営	－	－	－	－	－	－	－	否定	－	－	★
東京地判 H27.9.17	民	技	－	－	－	－	－	－	－	－	－	－	★ ※8
東京地判 H27.10.22	民	営	●	－	●	－	－	●	－	否定	否定	否定	否定 ※9

判例	民事／刑事	情報の性質	秘密管理性の判断に関連して争点となった事項							秘密管理性	有用性	非公知性	営業秘密該当性
			情報区分・表示	秘密保持義務	社内規程等	研修等	アクセス制御	施錠管理	その他				
東京地判 H27.10.29	民	営	－	－	－	－	－	－	－	－	－	－	★
大阪地判 H27.11.13	刑	営	－	－	－	－	○	－	－	肯定	肯定	－	肯定
大阪地判 H27.11.26	民	営	－	－	－	－	－	－	－	－	－	否定 ※10	否定 ※10
大阪地判 H27.12.17	民	営	●	○	●	－	●	●	● ※11	否定	－	－	否定
知財高判 H27.12.24	民	著	－	－	－	－	－	－	－	－	－	否定	否定
横浜地判 H28.1.29	刑	技	－	－	－	－	－	－	－	－	肯定 ※12	－	肯定 ※12
東京地判 H28.2.15	民	営	●	●	●	－	●	●	－	否定	－	－	否定
知財高判 H28.3.8	民	営	●	●	－	－	●	－	－	否定	－	－	否定 ※13
東京地判 H28.3.29	刑	営	○	○	○	○	○	－	○ ※14	肯定	－ ※15	－ ※15	肯定
東京地判 H28.4.27	民	技	－	－	－		○			肯定	肯定	肯定	肯定
東京地判 H28.4.27	民	営	●	●	－	－	● ※16	－	－	否定	－	－	否定
知財高判 H28.4.27	民	技	－	○	－	－	○	－	－	肯定	肯定	肯定	肯定
		技	●	－	－	－	●	－	－	否定	否定	否定	否定
東京地判 H28.5.31	民	営	－	－	－	－	－	－	－	否定	－	－	否定 ※17
知財高判 H28.6.13	民	営	－	－	－	－	－	－	－	－	否定	－	否定 ※18
富山地判 H28.6.15	民	営	●	●	－	－	－	－	－	否定	－	－	否定

判例	民事／刑事	情報の性質	秘密管理性の判断に関連して争点となった事項							秘密管理性	有用性	非公知性	営業秘密該当性
			情報区分・表示	秘密保持義務	社内規程等	研修等	アクセス制御	施錠管理	その他				
大阪地判 H28.6.23	民	営	－	－	○	○	○	－		肯定	肯定	肯定	肯定
東京地判 H28.6.30	民	技	－	－	－	－	－	－	－	－	否定	否定	否定
大阪地判 H28.7.21	民	技	－	－	－	－	－	－	－	否定	否定	否定	否定

【凡例】
民：民事事件　刑：刑事事件
技：技術情報　営：営業情報（顧客情報、取引先情報等）　著：著作物（記事原稿）　経：経営情報
○：肯定的要素として認定　●：否定的要素として認定　－認定した事実なし
★：営業秘密該当性の判断を明示的に行わず

【注記】
※1：不正競争を構成する行為がなかったとして、当該設計図が営業秘密に該当するか判断せず。
※2：なりすまし電話により、虚偽の苦情を述べる等の方法で、営業秘密、個人情報として管理されていた契約者名や住所等の情報を不正に取得し、これを使用・開示したことで有罪となった事案（被告は、他社から報酬を得て、第三者の個人情報等を入手することを業として、常習的に行っていた）で、漏えいの対象となった契約者名や住所等について 3 要件の認定については特段なされていない。
※3：営業秘密該当性の判断は原審の判断を支持しており、付記のあった箇所のみ記載。
※4：東芝の技術流出事案に係る刑事事件で、有罪となった事案である。アクセス制御（パスワードやアクセス権限）や複製禁止・退職後の秘密保持等の事実が肯定的に示されている。
※5：営業秘密該当性の判断は原審の判断を支持しており、付記のあった箇所のみ記載（東京地判 H26.12.19 [LEX/DB: 25540842]の控訴審）。
※6：原審が秘密管理性を認めているが、この点について控訴審では争われておらず、控訴審では、控訴人が有用性について争ったため、この点について判断がなされた。
※7：東京地判 H27.3.9 [LEX/DB: 25506161]の控訴審で、原審の量刑が過大であるという趣旨で控訴されたものであり、有用性について丁寧な認定がなされている。
※8:不正取得の事実を認定する証拠がないとして、当該ソースコードが営業秘密に該当するか判断せず。
※9：営業秘密該当性について争点となった対象が、名刺帳に保管されていた名刺という特殊性がある。
※10：顧客名簿が営業秘密に該当するかどうかよりも、これを取得し、外部に持ち出したかどうかという不正競争行為の存否が争点となっており、持ち出しにはシステム的に専用の USB メモリを使用する設定がなされ、外部送信メールには上司を CC に入れなければ送信出来ない設定がなされる等の措置があり、当該名簿の取得、持ち出しの事実を認定出来ないとして、不正競争行為の存在を否定した事案。顧客情報が公知情報の集積物であることから、非公知性を欠く可能性を指摘しながらも、結論としては、仮に営業秘密に該当するとしても不正取得の事実無しという判断をしている。
※11：退職時に問題となった情報について破棄させていない。
※12：営業秘密侵害罪の成立について争いがなく、量刑について争いがある事案であり、営業秘密該当性について具体的な当てはめ、判断はなされていない。
※13：営業秘密該当性の判断について、これに該当するものと認めることには疑問が残るとした上で、不正競争行為を認定するに足りる証拠がないとしている。
※14：PC の持ち出し制限（鍵付きチェーンロックで固定、入退館・入退室管理、防犯カメラの設置等）。
※15：有用性、非公知性については争われていない。
※16：ファクシミリが広く共用され、誰でも受信した指示書などを見ることができた点を認定。

※17：営業秘密の内容が特定されておらず、差止・破棄・引き渡し請求の対象が特定されていないことから、当該請求を不適法として却下。
※18：東京地判 H27.10.29 [25447591]の控訴審で、有用性を否定。仮に営業秘密に該当するとしても、使用についても具体的な主張立証がなく、その使用の事実を認める余地がないとして、不正競争に基づく請求は理由がないと判断。

3.3.3. 秘密管理性について

秘密管理性の要件について、当初から「当該営業秘密について、従業員、外部者から、認識可能な程度に客観的に秘密の管理状態を維持している」ことを要するとされており、具体的には、①当該情報にアクセスした者に当該情報が営業秘密であることを認識できるようにされていること、②当該情報にアクセス出来る者が制限されていることが考えられると指摘されていた[18]。

判例の理解も、主要な判例や先行研究を見る限り、同様に解されているが、具体的な当てはめと判断については、時期によって多少の変化があったことが知られている[19]。この点、2015 年 1 月には営業秘密管理指針が全部改訂され、秘密管理性の要件について、「秘密管理性要件の趣旨は、企業が秘密として管理しようとする対象（情報の範囲）が従業員等に対して明確化されることによって、従業員等の予見可能性、ひいては、経済活動の安定性を確保することにある」[20]と明記した。また必要な秘密管理措置の程度については、「秘密管理性要件が満たされるためには、営業秘密保有企業の秘密管理意思が秘密管理措置によって従業員等に対して明確に示され、当該秘密管理意思に対する従業員等の認識可能性が確保される必要がある」[21]として、認識可能性に力点を置いた表現となっている。この点、同管理指針は、上記①と②について、「両者は秘密管理性の有無を判断する重要なファクターであるが、それぞれ別個独立した要件ではなく、『アクセス制限』は、『認識可能性』を担保する一つの手段であると考えられる。したがって、情報にアクセスした者が秘密であると認識できる（『認識可能性』を満たす）場合に、十分なアクセス制限がないことを根拠に秘密管理性が否定されることはない」[22]としている。これに対して、本調査の対象とした判例においては、同管理指針の公表後においても、基本的にはこれまでの考え方を踏襲するものが散見される[23]。

---

18 通商産業省知的財産政策室監修『営業秘密－逐条解説改正不正競争防止法』（有斐閣、1990 年）55－56 頁。
19 例えば田村善之「営業秘密の不正利用行為の規律に関する課題と展望」知的財産法政策学研究 47 号（2015 年）は、①緩和期－2000 年代初頭までー、②裁判例の転換－2000 年代初頭～2000 年代中盤における厳格期（客観説）の到来ー、③裁判例の揺戻し－2000 年代終盤～現在における主観説（認識可能性説）の台頭ー、という 3 つの時期に分解して整理を行っている。
20 経済産業省「営業秘密管理指針（全部改訂：平成 27 年 1 月 28 日）」3 頁。
21 前掲注 20、5 頁。
22 前掲注 20、5 頁。
23 これまでの考え方を概ね踏襲していると考えられる判例では、「不競法上の営業秘密に該当す

上記①②の判断に際しては、情報区分・表示の有無、秘密保持義務の有無、社内規程等の有無、研修等実施の有無、アクセス制御の有無、施錠管理の有無といった事項が裁判所の判断に影響していることが確認出来た。なお、これらの項目の１つを満たせば秘密管理性が認められるということではなく、当事者が主張した事実を裁判所が総合考慮して秘密管理性を判断している点には留意を要する[24]。

3.3.3.1. 情報区分・表示

社内規程によって業務で取り扱う情報をマル秘，機密，社外秘に区分し、問題となっている情報が認識可能な状態で機密情報として管理されていた事案では、この点を肯定的要素として捉えている。一方、情報区分・表示についてはこれが十分になされていないことが否定的要素として捉えられている判例の方が目立ち、「マル秘」表示等、営業秘密であることを客観的に認識させるための表示を講じていなかったことが否定的に捉えられている[25]。

●肯定的要素として捉えている判例

・ 情報管理規程細則において，業務で取り扱う情報をマル秘，機密，社外秘に区分し，機密については，取扱者を社内の業務遂行上の関係者に限定するなどの管理方法を規定するとともに，同細則の別紙として情報資産管理基準及び同細則に基づく情報資産一覧表

るためには，不競法 2 条 6 項にいう『秘密として管理されている』ことが必要であり，このようにいえるためには，当該情報にアクセスした者に当該情報が営業秘密であることが認識できるようにしていることや，当該情報にアクセスできる者が限定されていることなど，当該情報に接した者が，これが秘密として管理されていることを認識し得る程度に秘密として管理している実体があったといえることが必要というべきである（東京地判 H28.4.27 [LEX/DB: 25447972]）」、「ある情報が秘密として管理されているといえるためには，当該情報に接し得る者が制限され，当該情報に接した者に当該情報が秘密であると認識し得るようにしていることが必要であると解される（富山地判 H28.6.15 [LEX/DB: 25543186]）」といった指摘がなされている。

[24] 小野昌延＝松村信夫『新・不正競争防止法概説〔第 2 版〕』（青林書院、2015 年）335 頁はこの点について判例検討を踏まえ、「秘密管理性を肯定された事例と否定された事例を比較しても、何が両者の分水嶺であったかは一概にはいえないが、前述した秘密情報への物理的アクセス制限の強弱だけでなく、アクセス可能者に対して秘密保持義務を課していたか否かという法的管理体制、秘密を管理する責任者が存在したか否かや、従業員に対する秘密管理情報の徹底などの組織的管理体制、さらには従業員に業務上使用する目的で交付した営業秘密を記載した書類（複製物）の回収を怠っていたか否かという業務上の管理体制などの有無を総合的に評価して、秘密管理性の有無が決定されていると思われる」と指摘している。

[25] この点については以前から同様の裁判例が散見されている。例えば「各キャビネットには『未承認品目・新製品』といったように収納されている書類の分類を記載したラベルが貼られていたが、一部の書類に『マル秘』など秘密として管理されていることを示す表示を付するような取扱いはされていなかった（東京地判 H12.9.28 [LEX/DB: 28052116]）」、「上記キャビネット自体は施錠されておらず、各図面には、特に秘密として扱われるべきことが明らかとなるような印等は付されていなかった（大阪高判 H17.2.17 [LEX/DB: 28100466]）」等がある。

を策定し，本件データベース等に集積されるａの顧客情報を機密情報として位置付ける旨規定していた。また，ａは，文書・電磁的記録管理規程を策定して業務で取り扱う情報の区分を規定するとともに，同規程を踏まえた機密情報管理マニュアルにおいて，顧客リストを機密として位置付けていた。（東京地判 H28.3.29 [LEX/DB: 25543202]）

●否定的要素として捉えている判例

- 「秘」の文字その他秘密情報であることを示す表示は付されていなかった（東京地判 H27.10.22 [LEX/DB: 25447549]）
- 顧客カルテは，その表紙などに営業秘密である旨の表示はなく，本件店舗の従業員であれば誰でも見られる状態で保管（東京地判 H28.2.15 [LEX/DB: 25447813]）
- 本件指示書等には「部外秘」「秘密」などの秘密情報が記載されていることを示す印字や押印がされていなかった（東京地判 H28.4.27 [LEX/DB: 25447972]）
- 本件懸場帳及び得意先カードに「マル秘」，「社外秘」等，これに係る情報を営業秘密として扱う旨の表示をせず，また，社内には本件顧客情報につき営業担当従業員に秘密保持を義務付ける就業規則の規定や同旨の誓約書は存在しなかったこと，被告がフォーユー・メディカル元気を退職する際，Ｆから本件顧客情報につき秘密を保持する旨の誓約書の作成を求められることはなく，これが求められたのは被告が退職し，本件懸場帳等が原告中部薬品に譲渡された後の平成２６年１月末ころであったことが認められる。これによれば，フォーユー・メディカル元気は，本件顧客情報を秘密として取り扱うことを被告を含む営業担当従業員に対し的確に示していなかったということができる。（富山地判 H28.6.15 [LEX/DB: 25543186]）

3.3.3.2. 秘密保持義務

秘密保持義務については、就業規則によってその旨が明記され周知されていたことや、退職後の秘密保持義務についても別途誓約書等を差し入れさせることによって、当該義務を負わせていたこと等が、肯定的要素として取り上げられている[26]。なお問題となっている患者情報が医師等専門職の守秘義務の対象であると認識していたとしても、営業秘密の管理体制が不十分であった事案においては、営業秘密として管理されているものと認識することは出来ないと判断した事案もある（大阪地判 H27.12.17）。

[26] 前掲注 16、6－7 頁によれば、技術情報の秘密管理性について判断を行った判例のうち、従業員による不正使用が問題となった裁判例 3 件においてはいずれも従業員は雇用契約又は就業規則により秘密保持義務を負っていたと指摘している。また同報告書の 9 頁によれば、営業情報の秘密管理性について判断を行った判例の中で、秘密管理性が肯定された 6 件の判例の全てにおいて従業員に秘密保持義務が課されていたことが報告されている。

否定的要素として捉えられた例をみると、そもそも秘密保持義務を口頭ベースでしか負わせていなかったことから、証拠としてこれを示せなかった事例や、就業規則等によって一般的に秘密保持義務を定めていたものの、問題となっている情報がその対象となっていたかどうかについて明らかではない等の理由が示されている。

●肯定的要素として捉えている判例

- 就業規則等で本件顧客情報の守秘義務を従業員に課すとともに，その周知に努めていたものと認められる（知財高判 H27.2.19 [LEX/DB: 25447086]）
- 在職中においては個人所有の電磁的記録媒体等への前記営業秘密の複製禁止等の内部規則を遵守することはもとより，退職後もｑ５工場で知った営業秘密を保持すべき任務を負っていた（東京地判 H27.3.9 [LEX/DB: 25506161]）
- 原告の職員らが，本件患者情報は，医師等専門職の職業上の守秘義務の対象であると認識していたとしても，原告の営業秘密として管理されているものと認識することはできなかったというほかないから，上記のような管理体制のもとでは本件患者情報が秘密として管理されていたということはできない（大阪地判 H27.12.17 [LEX/DB: 25447745]）
- 就業規則において，社員の服務心得（７条（６））として，「業務上の機密事項および会社の不利益となる事項を他に漏らさないこと」を，退職後の責任（３８条）として，「社員は退職後も，在職中に知り得た会社の機密を他に漏らしてはならない。」ことを，懲戒解雇事由として（４７条（６））として，「職務上知り得た業務上の重要機密を外部に漏らし，または漏らそうとしたとき」を，それぞれ規定している。また，被控訴人は，退職する従業員に対しては，おおむね以下の事項の遵守を誓約する旨の「秘密保持に関する誓約書」の提出を求めており（知財高判 H28.4.27 [LEX/DB: 25448025]）

●否定的要素として捉えている判例

- 被告取締役その他関係者の発言等があったとしても，これらによっては上記合意が成立したと認めるに足りず，他に上記合意が成立したことを認めるに足りる証拠はない（東京地判 H26.11.20 [LEX/DB: 25446791] ）
- お互いにそれぞれの有する技術ノウハウを尊重しており，契約の成約時に秘密保持契約を締結していること，成約までの過程で技術資料の交換を行うことはあるが，その際，いちいち秘密保持契約を締結するわけにはいかないため，成約時に契約すること，その間は当事者同士が互いに秘密を守ってきていることが記載されているにとどまっている（知財高判 H27.5.27 [LEX/DB: 25447272]）
- その従業員に対し，就業規則において秘密保持義務を課していたことが認められるものの，その対象は，「会社の機密事項または会社の不利益となる事項」（１３条（２)），「業務上知悉した関係会社の機密事項」（同（３））とされているにとどまり，本件登録情報が上記の各事項に含まれるのかはその文言上必ずしも一義的に明らかではない。また，

従業員の資格を失った時には，業務に関連して得た会社及び顧客に関する資料，データその他の情報を直ちに返納し，又は破棄することとはされているものの（５５条２項），本件登録情報に係る情報そのものについてどのように扱われるかはその文言からは必ずしも明確ではない。　前記ａ（ｃ）の「秘密保持に関する誓約書」の記載をみても，「秘密情報等」の対象とされているのは，控訴人に関係する情報であり（２項），顧客に関係する本件登録情報がこれに含まれるのかは一義的に明確ではない（知財高判 H28.3.8 [LEX/DB: 25447837]）

- 秘密保持契約を締結していたものの，同契約における秘密保持の対象は技術的な情報に限られており，顧客情報は秘密保持の対象とされていなかった（東京地判 H28.4.27 [LEX/DB: 25447972]）
- 本件顧客情報につき営業担当従業員に対し秘密保持を義務付ける就業規則の規定を持たず，同従業員に秘密保持を義務付ける内容の誓約書を差し入れさせることもなかった（富山地判 H28.6.15 [LEX/DB: 25543186]）

3.3.3.3. 社内規程等

社内規程等において営業秘密として管理すべき情報やその管理方法等が定められていれば、当該企業における秘密情報の管理実態が証拠としても示せることに加え、これが従業員等に周知されていることによって、認識可能性があったことを強く推認させることができる。この点、社内規程等において、具体的に営業秘密として管理の対象となる情報や、その取扱い手順等が示され、これを従業員に認識させていたこと等を肯定的要素として捉えている判例がある一方、社内規程等が存在していないことを重要な否定的要素として捉え、従業員の認識可能性を否定している判例も見られる。

●肯定的要素として捉えている判例

- 企業秘密管理規程が定められ，企業秘密に関する申告があった場合には，速やかにこれを審査し，企業秘密を指定し，秘密を保持する期間，開示できるものの範囲などについて決定し，役員は入社及び退職にあたって，別に定める秘密保持誓約書を会社に提出しなければならない（大阪地判 H26.10.23 [LEX/DB: 25446744]）
- 顧客別の売上情報及び顧客別の平均販売価率情報は，従業員しか閲覧することのできない社内ネットで管理されており，閲覧できる範囲についても従業員の所属部署，地位に応じて定められていて，従業員においてもそのような情報保護の規程があることを認識することができた状況にあった（大阪地判 H28.6.23 [LEX/DB: 25446744]）
- 営業部員については，特に営業情報保護手順書が定められており，業務上知り得た医療機関の情報等について漏えいしてはならないなどとされていたことからすれば，従業員

において，本件情報が秘密であることを十分認識できたものといえる（大阪地判 H28.6.23 [LEX/DB: 25446744]）

●否定的要素として捉えている判例

- 被告が原告に在職していた当時，原告において，従業員に秘密保持義務を課す情報管理規定も存在していなかったというのであるから，本件店舗の顧客情報が，情報の利用者である従業員において秘密であると認識し得る程度に管理されていたと認めることは困難というほかない（東京地判 H28.2.15 [LEX/DB: 25447813]）

3.3.3.4. 研修等

秘密保持義務の存在や内容、社内規則等の存在や内容を周知・徹底する上で、研修等が実施されていることは、認識可能性を強く推認することから、肯定的要素として捉えている判例もある。全体として研修等が実施されていたことを認定している事例は少ないが、裁判官の心証形成も含め、認識可能性について有効な証拠の１つとなり得る要素であると言える。

●肯定的要素として捉えている判例

- 内部情報保護規程による定めが従業員には周知されている状況にあり，管理職が秘密情報の管理についての研修も行い，本件情報が，営業活動上，重要な情報であることを十分に認識できたものと認められる（大阪地判 H28.6.23 [LEX/DB: 25446744]）
- 毎年，従業者全員を対象とした情報セキュリティ研修を実施した上，個人情報や機密情報の漏えい等をしてはならない旨記載された受講報告書のほか，個人情報及び機密情報の保秘を誓約する内容の同意書の提出を求めており，被告人も，ｂでの業務開始時に加え，その後も毎年，前記研修を受講し，前記受講報告書及び前記同意書を作成して提出していた（東京地判 H28.3.29 [LEX/DB: 25543202]）

3.3.3.5. アクセス制限の有無

今回調査対象とした判例の中でも、秘密管理性の判断にあたってアクセス制限の有無が問題となっているケースが多く見られた。アクセス制限の設定範囲については、情報の種別に応じて ID とパスワードや USB メモリ等の記録媒体の接続制限といった手段で、アク

セスできる従業員を制限するという水準で管理をしていれば秘密管理性を判断する上で肯定的要素として捉えている例が散見される。

一方、従業員であれば誰でもIDとパスワードを知っておりアクセス可能であった等、実質的にアクセスできる者とそうでない者を区別したり、アクセスできる情報を特定していないような場合には、これが否定的要素として捉えられている[27]。

●肯定的要素として捉えている判例

- 本件顧客情報を管理部に設置された顧客管理パソコンに集約した上で，（中略）顧客管理パソコンについてのパスワードの設定，本件顧客情報へのアクセス権者の限定（知財高判 H27.2.19 [LEX/DB: 25447086]）
- 営業秘密が記録され，ｑ３が管理する営業秘密記録媒体たるコンピュータ・ネットワーク内のデータベースにアクセスするための識別符号及び同データベース内に電磁的記録として蔵置された３社の営業秘密を閲覧・編集する権限を付与される（東京地判 H27.3.9 [LEX/DB: 25506161]）
- 原告らは，部外者がアクセスできないように構築されたイントラネット内に本件データを含む各種データを保管し，従業員には，事務所内に設置されたパソコンから保管されたデータにアクセスさせながら執務させている。この原告ら事務所内に設置されているパソコンを従業員が起動するには，従業員各自が与えられているパソコン用のＩＤとパスワードを入力する必要がある。このＩＤとパスワードは，原告らのイントラネット内のフォルダに保存されている各種データのうち，当該従業員がアクセスを許されているものとそうではないものとを識別する役割を果たしている。その識別は，イントラネット内にアクセスする際に改めてＩＤやパスワードを入力させるのではなく，どのＩＤとパスワードでパソコンを起動させたかによって自動的にされる。そして，本件データを含む集計シートのデータのように機密性の高いものについては，アクセス可能なのは正社員及び役員のみであり，パート・アルバイトや派遣スタッフはアクセスすることができない（東京地判 H27.3.27 [LEX/DB: 25540197]）
- 本件データベースサーバには，ＩＤ及びパスワードでログインを要する業務用パーソナルコンピュータからのみアクセスが可能な設定となっており，同コンピュータは，各人

[27] この点については以前から同様の裁判例が散見されている。例えば「原告の顧客データへのアクセスについてはパスワード等による保護はされておらず，事務所にいる者なら誰でもこのデータを見ることができる状態にあった（東京地判 H14.4.23 [LEX/DB: 28070858)」といった例や、「同システムでは，コンピュータを立ち上げるにはパスワードが必要であったが，パスワードは上記のようなシステムの導入当初ということもあって，付箋に記載されてコンピュータに貼ってあったため，従業員は，上記事務担当者以外の，商品発送に関わる者も含め，全員がパスワードを知っていた。また，コンピュータが立ち上がった後は，事務所に居合わせた者は，誰でもその画面で会員情報を見ることができた（東京地判 H15.5.15 [LEX/DB: 28090821])」といったパスワードの管理が不十分であった事案でこれを否定的要素として捉えている例がある。

の執務室机上に錠付きチェーンロックで固定され，業務上の必要がある場合を除き，持ち出しが禁止されていたこと，入退館出入口や個人情報を取り扱う業務の執務スペース等の出入口にはＩＣカード認証による入退管理が実施されていた上，ｂ　ｄ事業所の入退館出入口には防犯カメラが設置されていたこと等の管理状況からすれば，業務用パーソナルコンピュータの不正使用や部外者による執務室内への入室は制限されていたといえる。さらに，社内のネットワークに関しては，拠点単位でファイアウォールが設定されるなど，内部的なアクセス制御もしていたこと，外部からのインターネットを介した不正アクセスに対しては，対策ソフトを設定したり，セキュリティ会社が２４時間監視する体制をとっていたことからすれば，社内外を問わず，本件システムは業務上無関係なネットワークから遮断されており，部外者からのアクセスに対する防止措置がとられていた（東京地判 H28.3.29 [LEX/DB: 25543202]）

・ セキュリティソフトにより，業務用パーソナルコンピュータからＵＳＢメモリ等の外部記録媒体への書き出しが制御されていたのであり，多くのスマートフォン機種については書き出し制御の対象外となっていたなど不完全な点はあるものの，顧客情報の複製等について一定の制限が加えられていた（東京地判 H28.3.29 [LEX/DB: 25543202]）

・ 図面や部品表のデジタルデータは，社内サーバに保存された上，社内文書管理システムであるアークスイートを用いて管理されており，原告の従業員がデータを検索，閲覧，印刷するには所定の利用登録を受ける必要があるほか，サーバに蓄積されているデータを個別又は一括してダウンロードし，記録媒体に保存する権限を与えられているのは，技術部門の一部の従業員に限られていた（東京地判 H28.4.27 [LEX/DB: 25447938]）

・ 開発を担当するプログラマの使用するパソコンにはパスワードの設定がされ，また，被控訴人は，完成したプログラムのソースコードを研究開発部のネットワーク共有フォルダ「ＲａｎｄＤ＿ＨＤＤ」サーバの「ＳＯＦＴ＿Ｓｏｕｒｃｅ」フォルダに保管し，当該フォルダをパスワード管理した上で，アクセス権者を限定するとともに，従業員に対し，上記管理体制を周知し，不正利用した場合にはフォルダへのアクセスの履歴（ログ）が残るので，どのパソコンからアクセスしたかを特定可能である旨注意喚起するなどしていたことに照らすと，原告ソースコードは，被控訴人において，秘密として管理されていたものというべき（知財高判 H28.4.27 [LEX/DB: 25448025]）

●否定的要素として捉えている判例

・ 鍵のかかるキャビネット内に保管された台帳及びログインが必要なシステム上で管理され，台帳については鍵を借りる許可を得た従業員のみが，システムについては，原告からアカウントを発行され，パスワードを設定した従業員のみが，それぞれアクセスできる旨主張するが，本件名簿情報１及び２にアクセスできる従業員の範囲等について具体的な主張立証はない。（東京地判 H27.8.27 [LEX/DB: 25447488]）

- 電子カルテにアクセスするためには，ＩＤ及びパスワードが必要であるが，ＩＤ及びパスワードは医師及び看護師だけでなく，原告の事務職員は誰でも知っており，誰でもアクセス可能であった。また，本件患者情報の持出しは禁止されておらず，原告診療所において訪問診療を行う際には，電子カルテのみならず，電子カルテを打ち出したものを携行して利用していた。また，そのように打ち出したものやコピーしたものを事後に回収したり復元不可能な措置を講じて廃棄したりすることはなく，そのための指針もなかった（大阪地判 H27.12.17 [LEX/DB: 25447745]）
- 顧客管理システムは，本件店舗の従業員であればパスワード等を用いることなく誰でも顧客情報を閲覧することができた（東京地判 H28.2.15 [LEX/DB: 25447813]）
- 本件登録情報は，元来，各コンサルタントが顧客から取得する情報であるし，前記ａ（ａ）のとおり，管理部門等コンサルタント業務以外の会社情報のように，アクセスできる従業員が限定されている情報が存在する一方で，本件登録情報については，同情報の登録された販売管理システムにログインするためにユーザー名及びパスワードの入力が必要とされていたものの，控訴人の従業員であれば誰でもログイン可能であり，アクセスできる従業員が限定されていないものである（知財高判 H28.3.8 [LEX/DB: 25447837]）

3.3.3.6. 施錠管理の有無

施錠管理等の有無についても、情報に対する物理的なアクセス制御の側面があるが、施錠や警備装置等によって物理的にアクセスを制限している点を肯定的要素として捉えている判例がある。一方で、施錠等が十分に行われておらず、だれでも当該情報にアクセスできると判断されるような場合にはこれを否定的要素として捉えているケースも散見される。施錠管理等には、外部からの侵入を防ぐという意図がある場合も少なくないが、「オフィス部分の入口には生体認証システムが設けられ，入室が制限されていた」場合であっても、従業員であれば内部のどこにでも入室できる状態にある中、個別の引き出しが施錠管理されていなかった点を否定的に捉えている例もある（東京地判 H27.10.22）[28]。

●肯定的要素として捉えている判例

- 施錠や警備装置の設置によって，管理部内への部外者の立入りを制限（知財高判 H27.2.19 [LEX/DB: 25447086]）
- 鍵のかかるキャビネット内に保管された台帳及びログインが必要なシステム上で管理

[28] 同趣旨の判例として「同棚は一般顧客からは見えない位置にあり，その棚には扉も鍵もあるが，常時施錠されているわけではなく，扉さえ閉めていないことが多かった。また，本件情報カードは，被告ら在籍当時，一部の限られた従業員しか見ることができないような厳格な管理下におかれているものではなかった。（東京地判 H16.9.30 [LEX/DB: 28092603]）」

され，台帳については鍵を借りる許可を得た従業員のみが，システムについては，原告からアカウントを発行され，パスワードを設定した従業員のみが，それぞれアクセスできる旨主張するが，本件名簿情報１及び２にアクセスできる従業員の範囲等について具体的な主張立証はない。（東京地判 H27.8.27 [LEX/DB: 25447488]）

・ 文書管理についても，機密文書は鍵のある箇所に保管するなどとされていた（大阪地判 H26.10.23 [LEX/DB: 25446744]）

●否定的要素として捉えている判例

・ 本件顧客名簿が秘密として管理されていたこと（秘密管理性）に関するとされる客観的証拠は甲８のみしかなく，その内容を見ても秘密管理性を裏付けるものか判然としない上，原告の本社事務所には，顧客の名称，住所・電話番号等の連絡先，購入商品等が記載された納品書や注文書をまとめたファイルが，施錠等をされることもなく，誰でも自由に閲覧可能な状態で置かれていた（東京地判 H28.5.31 [LEX/DB: 25447995]）

・ 原告のオフィスのあるビルへの入館にはカードキーが必要であり，さらに，オフィス部分の入口には生体認証システムが設けられ，入室が制限されていたものの，オフィス内に従業員が立ち入れない箇所は特段定められていなかった。本件名刺帳は被告Ａの秘書業務を担当する従業員の袖机の引き出しに保管されていたが，この引き出しは施錠されていなかった（東京地判 H27.10.22 [LEX/DB: 25447549]）

・ 本件指示書等をファクシミリで被告に送信していたが，被告が本件指示書等の受信に用いたファクシミリは，原告との取引に関与する産業機械の部署のみならず，流体機械部門やバルブを担当する部署も共通して使用しており，原告から本件指示書等を受領する担当者以外の被告従業員も，本件指示書等を容易に見ることができたこと及び原告は上記ファクシミリの設置状況を認識していたことが認められる。これらを総合すると，本件指示書等に記載された顧客情報に接した者が，これが秘密として管理されていることを認識し得る程度に秘密として管理している実体があったとは認められず（東京地判 H28.4.27 [LEX/DB: 25447938]）

3.3.4. 有用性について

有用性の要件については、不正競争防止法２条６項によれば「生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報」と記載されており、これは「技術に関する情報又は営業活動において使用・利用される情報であって、企業が財・サービスの生産・販売・研究開発等の事業活動を行っていく上で有用性のあるもの」[29]であると言われている。

[29] 前掲注 18、57－58 頁。東京地判 H14.2.14[LEX/DB: 28070351]はこれと同趣旨の基準を示しており、「不正競争防止法は，このように秘密として管理されている情報のうちで，財やサー

更に「有用性」については、「当該情報自身が事業活動に使用・利用されたり、又は、このように使用・利用されることによって費用の節約、経営効率の改善等に役立つもの」であり、「保有者の主観によって決められるものではなく、客観的に判断されるもの」と言われている[30]。

本調査結果では、例えば業務の効率化につながる等、事業活動に対して有効な効果をもたらす情報については有用性が認定される傾向が見られた。また、その効果の度合いについては、質的に高い優位性・独自性まで求められるものではなく、作業効率の向上等の業務改善に資する程度のものであっても有用性が認められている。一方で、単に企業名と住所を羅列しただけの情報や、効果を示すための証拠に乏しいような情報に対しては、有用性が認められないケースが見受けられた[31]。

なお刑事事件においては、有用性の判断が量刑に影響すること等から、この点が争われている事案がある（名古屋高判 H27.7.29 [LEX/DB: 25541038]、横浜地判 H28.1.29 [LEX/DB: 25542109]）。そもそも刑事事件の場合、営業秘密として管理されていたことに加え、営業秘密侵害行為があったことを証拠として上げて主張する必要があることから、この点についての争いよりも、侵害行為の有無や有用性等の判断について争点となっているものと考えられる。

●有用性を肯定した例

・ 有用性とは，正当な事業活動を行ううえで客観的な経済価値を有することをいい，製品の設計図や製法などのような技術的情報のみならず，顧客名簿，営業マニュアル等の営業情報も含むと解されるところ，前提となる事実（３）アのとおり，本件データには顧客の名称，一部の顧客に関する報酬の時間単価が記載されていることから，その有用性を否定することはできない（東京地判 H27.3.27 [LEX/DB: 25540197]）

・ 本件ファイルは，本件工作機械の製造に利用される図面情報であり，本件工作機械を製造，販売する同社の事業活動に有用な技術上の情報であって，有用性が認められる。（名

ビスの生産，販売，研究開発に役立つなど事業活動にとって有用なものに限り保護の対象としているが，この趣旨は，事業者の有する秘密であればどのようなものでも保護されるというのではなく，保護されることに一定の社会的意義と必要性のあるものに保護の対象を限定するということである。」としている。

30 前掲注 18、58 頁。

31 情報の技術的な価値について有用性を判断する中で考慮した判例もある。例えば、東京地判 H14.10.1 [LEX/DB: 28072954]は、クレープの調理方法につき、「当然に考えられる配合の割合である」、「クレープの品質にとって，どのように，どの程度有用であるのかは，証拠上一切明らかでない」等と判断して、有用性を否定している。また大阪地判 H20.11.4 [LEX/DB: 25421292]は、融雪板構造や生産方法について争われた事例で、「特段の優れた作用効果を奏すると認めるに足りる証拠はない」、「業者であれば通常の創意工夫の範囲内において適宜に選択する設計的事項にすぎない」としている。なお大阪地判 H20.11.4 の判断については、「このような情報まで有用性がないとして営業秘密として保護を否定してよいかは問題である」（前掲注 24、343 頁）といった疑問も呈されている。

古屋高判 H27.7.29 [LEX/DB: 25541038]）

・ 本件各犯行において使用された各設計図は，被害会社の技術面での優位性や高いオリジナリティーのある営業秘密であるとまでいうことはできないが，効率的な設計・製造を可能とするという点で有用性の認められるものである。（横浜地判 H28.1.29 [LEX/DB: 25542109]）

・ 原告は，過去に製作した図面等をそのまま用いたり，あるいはＣＡＤソフトで修正を施したりして，設計，開発に要する期間を短縮するなどしているのであるから，基本的な光学理論と従業員の能力，経験をもって一から製品の設計，開発，製造ができるとしても，なお本件データが事業活動に有用な技術上の情報であるとの認定は左右されないというべきである（東京地判 H28.4.27 [LEX/DB: 25447938]）

・ 原告プログラムは，理化学機器の開発，製造及び販売等を業とする被控訴人にとって，その売上げの大きな部分を占める接触角計に用いる専用のソフトウエアであるから，そのソースコードは，被控訴人の事業活動に有用な技術上の情報であり，また，公然と知られてないものである（知財高判 H28.4.27 [LEX/DB: 25448025]）

・

●有用性を否定した例

・ 本件名簿情報１は，その対象顧客数がわずか１３にすぎない上，その多くが金融機関や大手警備会社などであり，しかも，その内容は顧客名及び所在地のみである。そうすると，本件名簿情報１は，原告の名簿によらずとも第三者が容易に入手可能な情報というべきであって，経済的有用性を有する情報に当たるとは認め難い。（東京地判 H27.8.27 [LEX/DB: 25447488]）

・ 錫の切削性が失われず，加工，鋳造が容易になるという効果の証拠を提出していないため、認められない。（大阪地判 H28.7.21 [LEX/DB: 25448128]）

3.3.5. 非公知性について

非公知性の要件については、不正競争防止法２条６項によれば「公然と知られていないもの」であることが求められている。「公然と知られていない」とは、「当該情報が刊行物に記載されていない等、保有者の管理下以外では一般的に入手できない状態にあること」[32]ないし「当該営業秘密が一般的に知られた状態になっていない状態、又は容易に知ること

[32] 前掲注 18、60 頁。

ができない状態」[33]を言うとされている。もっともこのような状態にあったことの主張・立証責任を厳格に原告に課すとすればあまりに酷であることから、原告としては、「当該情報が一般的に入手できないことを合理的な範囲で立証すれば」[34]、事実上、公然と知られていないことが推定され、逆に反証しなければならないと解されている。

本調査結果では、情報の保有者の管理下以外では一般的に入手できない状態になっているものや、一般的に公になっていない情報であることが明らかであるような場合には、非公知性の判断にあたり肯定的に捉えられている例が見られた。一方で、守秘義務が課されていない状況で第三者に開示された情報やリバースエンジニアリングで容易に第三者が知ることができる情報については、非公知性の判断にあたって否定的に捉えられる例が見られた。

この点、訴訟手続において、原告が営業秘密であると主張する情報について、民事訴訟法に基づく閲覧等制限の申し立てを行わず、結果として当該情報が誰にでも自由に閲覧できる状態に置かれていたことを等から非公知性を否定した事例（大阪地判 H28.7.21）や、リバースエンジニアリングによって情報を容易に知ることができる場合には、非公知性が否定されるとした事例（大阪地判 H28.7.21）等も注目に値する。

リバースエンジニアリングについては、古い判例においても「技術的秘密を有するとしても、市販されている債権者製品の分析により極めて容易に製造しうるものであるとすれば、それは債権者にとって主観的にはともかく、客観的には保護に値する秘密とは言い難い」（奈良地判 S45.10.23 [LEX/DB: 27441334]）という判断を示したものもある[35]。そのため、立法当初から「誰でもごく簡単に製品を解析することによって営業秘密を取得できるような場合には、当該製品を市販したことによって営業秘密自体を公開したに等しい」、一方で「特殊な技術をもって相当な期間が必要であり、誰でも容易に当該情報を知ることが出来ない場合には、製品を市販したことをもって営業秘密が公知化することにはならない」と言われている[36]。その後の判例をみてもリバースエンジニアリングに多額の費用と時間を掛けて専門家が分析する必要があるとの理由で非公知性を認めた判例（大阪地判 15.2.27）や、市場で流通する製品から容易に取得できる情報であることを理由に非公知性を否定した判例（知財高判 H23.7.21）等があり、概ね同様の考え方は維持されているものと考えられる[37]。

---

[33] 前掲注 20、16 頁。
[34] 前掲注 18、60 頁。
[35] リーディングケースとしてしばしば参照されるいわゆる「フォセコ・ジャパン事件」である。なお本件で問題となった技術情報自体については、「市販されている債権者製品を分析することにより直ちに製造しうるものではないと推認して差しつかえないと解する。従って債権者は客観的に保護されるべき技術上の秘密を有しているといえる。」と判断している。
[36] 前掲注 18、155 頁。
[37] リバースエンジニアリングについては、「昨今、リバースエンジニアリングの技術が進歩しており、分野によっては分析すれば大概のことは容易にわかるようになっているため、非公知性が認められにくいのではないか」という懸念を指摘する声もある（本調査で実施した製造業に対す

●非公知性を肯定した例

- 本件データは，原告らの従業員の労働時間数に留まらず，原告らの顧客の名称，原告らが受任した業務に関する報酬を内容としている点で，原告会社内部における情報を記載したものであって，当該情報を保有者の管理下以外では一般的に入手できない状態にあるという本件データの管理体制に照らすと，本件データの非公知性を認めることができる。（東京地判 H27.3.27 [LEX/DB: 25540197]）
- 社内において秘密管理されており，営業部員においても第三者に閲覧させるなどすることは許されていないことからすれば，非公知の情報であったといえる。（大阪地判 H28.6.23 [LEX/DB: 25446744]）
- 顧客である各医療機関は，当然のことながら自らに対する売上げ等についての情報を有しており，これらの情報について原告に対して守秘義務を負っているものではないが，検査対象患者のプライバシー情報等を含む臨床検査に関する情報を公にしているものでないことは一般的に明らかであるから，本件情報は非公知であるといえる。（大阪地判 H28.6.23 [LEX/DB: 25446744]）

●非公知性を否定した例

- 原告は，長嶋氏関連原稿は，いずれも原告の営業秘密に該当するものとして記事編集機に保存されたものであるとするところ，前記１（２），（３）で認定したとおり，記事編集機に保存された内容には既に公知となったものも多数含まれていることからすると，記事編集機に保存された内容の全てが非公知であるとは認められないこととなる（東京地判 H27.2.27 [LEX/DB: 25447165]）
- 原告が，平成２６年７月３０日に本件訴訟を提起した後，口頭弁論の終結日（平成２７年５月２８日）に至るまで，本件鍵情報と同一内容が記載された訴状別紙「営業秘密目録」記載１につき，民事訴訟法９２条１項２号に基づく閲覧等制限の申立てさえせず，その結果，約１０か月間にわたって，本件鍵情報が何人も自由に閲覧できる状態に置かれていた（東京地判 H27.8.27 [LEX/DB: 25447488]）
- 原告は，本件名刺帳に収納された名刺に記載された情報が原告の営業秘密に当たる旨主張するが，名刺は他人に対して氏名，会社名，所属部署，連絡先等を知らせることを目的として交付されるものであるから，その性質上，これに記載された情報が非公知であると認めることはできない。なお、守秘義務を負うべき状況下で特定の者に対して名刺を手交するような場合には，その記載内容が非公知性を有することもあり得ようが,本件においてそのような事情は見当たらない。（東京地判H27.10.22 [LEX/DB: 25447549]）

るインタビュー調査より）。

・ 市場で流通している原告製品から容易に本件合金の成分及び配合比率を分析（ＩＣＰ発光分光分析）できるのであれば，本件合金は「公然と知られていないもの」とはいえない（リバースエンジニアリング）。本件合金は，原告製品の分析により，第三者が容易に知ることができるものであり，非公知性を欠くというべきである。（大阪地判 H28.7.21 [LEX/DB: 25448128]）

3.3.6. 不正の手段による営業秘密の取得

不正取得行為の判断にあたっては、業務上の目的外で取得した事案において不正取得行為として認定されたケースがあった。一方で、不正取得行為を立証する証拠に乏しく、不正行為が認められないケースもあった。

いずれも間接事実から不正取得行為の存在を判断しており、東京地判 H28.4.27 の場合、計画をもって競合する新会社を設立したことや、退職前に大量のデータをダウンロードしていること、技術的に同種の製品の製造販売を行っていること等から、不正取得行為を推認している[38]。今回の調査対象となった判例は、技術情報[39]及び記事という著作物が問題となった事例であったが、顧客名簿等の営業情報が問題となった過去の典型的な事例で言えば、顧客が酷似しているという間接事実から不正行為を推認している事例がある（東京地判 11.7.23）[40]。

---

[38] 田村・前掲注 19、53 頁は、不正行為の存在が直接証明されることはほとんどないと指摘しており、例外的に直接の証明に成功した判例として、顧客名簿の複写及び持ち出しについて目撃証言があったことを認定事実の 1 つとしてあげる東京地判 H12.11.13 が紹介されている。

[39] 技術情報について判断した判例として、例えば「被告のフラップジョイント及び試作機は、パイプ鍔部成形機における最も重要な部分であるコーンの構造､回転容量等の面で原告のフレアマシンとは顕著な差異を有する」として、製作図の使用を利用する必要性は少なかったと判断したもの（東京地判 H8.1.31 [LEX/DB: 28031046]）や、「原告製品と被告製品の各精製方法が同一のものであると認められるためには,それぞれに使用される有機溶媒の種類が同一であるということのみならず,それらが使用される手順や使用に当たっての条件などをも含んだ一連の精製工程全体の同一性が確認される必要がある」と指摘した上で、「確認し得るのは，せいぜい使用された有機溶媒の種類の同一性にとどまるのであって,それらが使用された手順や使用に当たっての条件などの同一性についてまで確認することはできない」として、同一性を否定した事案等がある（東京地判 H22.4.28 [LEX/DB: 25442161]）。

[40] 同判例は、「原告は、その顧客から、住所・電話番号は原告にしか教えていないのにもかかわらず、被告会社から電話でのセールスがあった、という苦情を受けるようになった。右事実によれば、被告会社が本件顧客情報を利用して営業活動をしたことを推認できる。」として、不正行為を認定した。逆に 579 名中、10 名に対して被告から会社案内が送付されたという証拠しか示されていない事案では、偶然の可能性を排除出来ないとして、名簿使用の事実を否定した判例もある（大阪地判 H11.9.14）。

●不正取得行為が認められた例

- 前記認定事実によれば，〔1〕被告は，同年７月３１日，Ｂから新会社の設立計画をスタートする旨の電子メールを受領し，これに対して必要となる設備を挙げる内容の返信をしていること，〔2〕Ｂは，同日，原告の取引先にも新会社の設立を示唆する内容の電子メールを送っていることからすれば，同日時点で，被告やＢらによる新会社設立の計画は相当程度具体化していたと推察されること，〔3〕被告は，原告が希望退職者を募集し，Ｂ，Ｄ，Ｃ及びＥが退職届を提出した同年９月上旬に，特に集中して，アークスイートから過去に比して極めて多量のデジタルデータをダウンロードしており，作業日報上，ここまで多量なデジタルデータを取り扱った旨も記載されていないこと，〔4〕本件データのうち別紙２「電子データ一覧表Ａ」記載の電子データは，原告が設計，開発した２ラインセンサ方式のオートフォーカス顕微鏡に関する組立図，部品図又は部品表のデータであること，〔5〕被告は，原告を退職して間もなくＢらと設立したフェイスにおいて設計業務を担当し，フェイスは，原告の主力製品のひとつである２ラインセンサ方式のオートフォーカス顕微鏡と同一の特徴を持つ「装置組込用オートフォーカスシステム」，「高感度２ラインセンサー方式による顕微鏡オートフォーカスを実現するための製品」を製造販売していることなどの事実が認められるところ，これらの事実を総合すれば，被告は，既に設立の計画が相当程度具体化していた新会社（後に設立されたフェイス）において，「高感度２ラインセンサー方式による顕微鏡オートフォーカスを実現するための製品」等の設計に用いる目的を持って，アークスイートにアクセスの上，本件データを含む原告の製品の設計データをまとめてダウンロードし，これを外部媒体等に保存して持ち去ったものと合理的に推認できる。被告は，原告を退職後に設立する予定であった新会社（後に設立されたフェイス）での設計業務に用いるため，原告の営業秘密に属する本件データを持ち去ったものと認められる。（東京地判 H28.4.27 [LEX/DB: 25447938]）

●不正取得行為が認められなかった例

- 第１のメールないし第３のメール自体には，記事編集機に存した原稿であることを窺わせる記載は全くないばかりか，かえってＤ自身が作成したメモであるかのような体裁となっていることが認められる。そして，Ｄ自身も，被告に宛てた第１のメールに「Ｄの原稿等を添付しました。」と記載しており，被告が明示的にＤに記事編集機にある本件各原稿を含む長嶋氏関連原稿等を送付するよう指示した事実についても，これを認めるに足りる証拠は存しない。加えて，被告は，平成２２年１２月当時，原告の関連会社である巨人軍の取締役球団代表の地位にあり，Ｄの再起を図るとの目的があったか否かについては措くとしても，職務に関連して読売ジャイアンツの元選手である長嶋氏や川上氏についての情報を入手すること自体は不自然なこととはいえず，その相当性はともかくとして直ちにＢに対し電子メールを転送したことも，Ｂに対する

電子メールの記載内容に照らし被告による違法ないし不正な取得を裏付けるものとはいい難い。以上によれば，被告がDから第１のメールないし第３のメールの送付を受けた動機については明らかとはいえないものの，被告においてDからのメールに添付されていた本件各送信原稿が記事編集機から取得されたものであるとの認識を持ち得るものと認めることはできないから，原告の主張する本件営業秘密につき，被告において，刑罰法規違反に該当する行為やそれと同等の違法性を有する公序良俗違反の行為を通じて営業秘密を取得したものとは認められないというべきである。（東京地判 H27.2.27 [LEX/DB: 25447165]）

3.3.7. 不正に取得した営業秘密の使用・開示

不正使用・開示の判断にあたっては、不正に利益を得、あるいは相手方を害する目的で営業秘密を取得し、使用・開示したことを合理的に推認できる場合に不正使用・開示が認められたケースがあった。

●不正使用・開示が認められた例

- 被告会社転職後にその余の転職者らとともに本件情報を被告会社に開示し，使用したと推認する方が自然であり，また合理的である。また，そのような原告との競業のための被告会社に対する開示・使用である以上，これが不正の利益を得，あるいは保有者である原告を害する目的でなされたことも容易に認定できるところである。後記検討するとおり，原告在職時の担当者として築いた人的関係が被告会社転職後にも活用できたであろうことを全面的に否定できないとしても，原告から被告会社に臨床検査の委託先を変更した顧客の中には，被告Ｐ１ら転職者が担当していなかったところもあるというのであるから，人的関係が貢献する場面があったとしても，それだけでは被告Ｐ１ら転職者が保有する本件情報が使用されたとの上記認定を全面的に覆すには足りないというべきである。（大阪地判 H28.6.23 [LEX/DB: 25446744]）

なお、平成 27 年の不正競争防止法改正により、不正使用行為の推定規定（第５条の２）が新たに導入されたが、今回調査した判例の中ではこれを活用したものはなかった。

3.3.8. その他

その他、営業秘密侵害は認定されなかったが、不法行為によって原告の請求が一部認容されたケースも見られた。

●営業秘密として認定されなかったが請求が一部認容された例（東京地判H28.5.31 [LEX/DB: 25447995]）

営業秘密としての認定について

- 原告は，本件顧客名簿が原告の営業秘密に当たると主張する一方，上記１のとおり，本件顧客名簿の具体的内容について何ら主張していないのであるから，本件顧客名簿が営業秘密に当たるとは認められない。

  仮にこの点を措くとしても，本件顧客名簿が秘密として管理されていたこと（秘密管理性）に関するとされる客観的証拠は甲８のみしかなく，その内容を見ても秘密管理性を裏付けるものか判然としない上，原告の本社事務所には，顧客の名称，住所・電話番号等の連絡先，購入商品等が記載された納品書や注文書をまとめたファイルが，施錠等をされることもなく，誰でも自由に閲覧可能な状態で置かれていたこと（乙３３）も併せ考慮すれば，本件顧客名簿が秘密として管理されていたこと（秘密管理性）も認めるに足りない。

不法行為の認定について

- 被告Ａは，上記（１）のとおり，Ｅ，Ｆ，Ｇ及びＨに対し，同ワイン生産者らの日本におけるワインの市場開拓を行ったのが被告Ａであり，原告には被告Ａの後継者がいないなどと告げるとともに，自らが原告のために購入予約をしていたワインを被告Ａが立ち上げた被告会社として購入したいなどと申し込むメールを送信し，同ワイン生産者らの了解を得て，これらのワインを被告会社として購入したことが認められる。加えて，被告Ａが，原告在職中に，同ワイン生産者らの出荷時期等に関して，事実と異なる内容を記載した社内メールを送信したり，虚偽の内容の引継書を作成したりして，原告が購入予約に係るワインを購入することを妨げる行為に及んだことも勘案すれば，被告Ａは，本来は原告において購入するはずであったワインを不当に奪取して被告会社に購入させたものと評価できる。そして，原告は，被告Ａの上記行為により，これらのワインを購入することができなくなったのであるから，被告Ａの上記行為は原告に対する不法行為に当たるというべきである。
- 原告の主張する本件横奪行為のうち，被告Ａが，原告において購入予約をしていたＥ，Ｆ，Ｇ及びＨの各ワインを，被告会社として購入した行為及

び同購入に向けられた一連の行為（前記２（２）ア（ア））については，原告に対する不法行為が成立すると認められるところ，同不法行為によって原告に生じた損害額は以下のとおりと認められる。

- 被告Ａの不法行為により，原告に上記（１）の合計額である２９５万８７９８円の損害が生じたと認められる。

4. 営業秘密管理に取り組むにあたっての示唆

今回実施したアンケート調査やインタビュー調査、判例調査等から、企業における営業秘密管理について、企業規模によって取組状況が異なることや、大規模企業であっても取組が遅れている対策があること等、営業秘密の保護対策を検討するための材料として、様々な実態が明らかとなっている。

こうした結果を踏まえて、企業にとって有効な営業秘密保護対策を検討していくにあたり、組織的な取組が進んでいると想定される企業や、営業秘密管理に対する意識が高いと思われる企業等における考え方や実施されている対策等に着目することで有益な示唆を得られる可能性がある。

今回、このような観点として

「漏えいを経験した企業が現在取り組んでいる対策」
「漏えい対策を行う前提として、営業秘密管理の対象とする情報をしっかりと区分けできている企業が実施している対策」
「営業秘密管理を経営の問題と捉えて、組織的に取り組んでいる企業が実施している対策」
「営業秘密漏えいに関する検知活動を行っている企業が実施している対策」

等に着目して得られた調査結果の分析を実施したところ、以下のような示唆が得られた。

- 過去５年間に営業秘密の漏えいを経験した企業では、「人材の流動化」等の社会動向の変化に対して営業秘密漏えいのリスクを感じる割合が相対的に高い。漏えいを経験していない企業においてもこれらを社会環境変化に基づくリスク要因として認識し、関連する対策に着手することがプロアクティブな施策として有用であることが示唆されている。
- 営業秘密とそうではない情報を区分している企業においては、区分できていない企業と比べて全体的に営業秘密管理のための取組が進んでいる。情報を区分し営業秘密としての管理対象を特定し明確化することは、「営業秘密管理指針」や「秘密情報の保護ハンドブック」でも重要事項とされており、個別具体的な対策を行う前提として改めてその重要性が示唆されている。
- 営業秘密管理に関する取組状況として、大規模企業と比較して、中小規模企業では全体的に取組が遅れている。特にシステム的な投資が必要となる対策については実施されていない企業の割合が多い。また、大規模企業においても、「情報システムのログの記録・保管」自体は多くの企業で実施されているものの、「不自然なアクセスがあった際の上司や本人への通知」等、ログを適切に管理して具体的なアクションにまでつなげられている割合は相対的に低い。

- 営業秘密管理を経営の問題として捉えている企業と、経営の問題として捉えていない企業とでは、各種対策への取組状況について全体的に大きな差が見られる。営業秘密管理に取り組むにあたっては経営層が積極的に関与して組織横断的に対策を検討していくことが重要であることが示唆されている。
- 情報漏えい検知活動を実施している企業では、検知活動を実施していない企業と比べて全体的に営業秘密漏えい対策への取組が進んでいる。検知活動ができていると営業秘密の侵害者に対して訴訟や社内処分等の具体的な対応まで実施できている割合も相対的に高くなっている。個別具体的な対策を実施するだけでなく、検知活動にもあわせて取り組むことが有効であり、漏えいの未然防止や具体的な事後対応にもつながる可能性が高いことが示唆されている。

4.1. 営業秘密の漏えい経験がある企業からの示唆

本アンケート調査結果によれば、全体で１割弱の企業が過去５年間の間に営業秘密の漏えい（おそらく漏えいがあった、という回答も含む）を経験しており、特に従業員数規模が 3,001 人以上の企業においては、「2.1.1. 過去５年間における営業秘密の漏えい状況」で触れたように２割程度の企業が過去５年間に営業秘密の漏えいがあったと回答している。一方で、300 人以下の企業では過去５年間に営業秘密の漏えいを経験した企業は数%程度と相対的に少ない割合になっているが、301 人以上の規模の企業も含めて漏えいの有無が「わからない」と回答している企業が２割程度存在していることから、企業が認識できていない営業秘密の漏えいも含めると、実際にはより多くの営業秘密の漏えいが発生しているものと思われる。

近年も様々な企業で営業秘密の漏えいが発生しており、報道等でその被害内容や規模等が明らかになっている（表 4.1-1）。こうした営業秘密の漏えいを経験した企業は、一般的にその後営業秘密の漏えいを防ぐための個別の対策や管理体制を強化することに積極的に取り組む場合が多い[41]。そのため、過去に営業秘密の漏えいを経験した企業が現在取り組んでいる対策等については、営業秘密の漏えいを経験していない企業にとっても学ぶべき示唆があるものと思われる。

表 4.1-1　営業秘密の漏えい発生後に対策を強化した例

時期	営業秘密が漏えいした企業	漏えい先	事案概要	漏えい後に取り組んだ強化対策
2014 年 3 月	東芝	SK ハイニックス	東芝の提携先であるサンディスクの元技術者が、東芝の研究データを不正に複製し、韓国 SK ハイニックスに転職した際に当該データを漏えいさせていたとされる事案。	・情報漏えい防止体制の構築[42]
2014 年 7 月	ベネッセコーポレーション	－	ベネッセコーポレーションのシステム運用を行っているグループ会社の業務委託先の元社員が、大量の顧客情報を不正に持ち出し、利益を得る目的で名簿業者に売却したと	・アクセスの監視強化と外部への持ち出しの制限の強化[43] ・社長を最高責任者と

[41] 例えば、顧客情報の漏えいが発生した株式会社ベネッセコーポレーションでは、経済産業省に対して提出した改善報告書の中で、顧客情報の管理体制の見直し案等について検討した内容を報告している。
http://www.benesse.co.jp/customer/bcinfo/02_1.html

[42] 株式会社東芝プレスリリース（2014 年 3 月 13 日）より
http://www.toshiba.co.jp/about/press/2014_03/pr_j1302.htm

[43] 株式会社ベネッセホールディングスプレスリリース（2014 年 7 月 9 日）より
http://www.benesse-hd.co.jp/ja/about/release_20140709.pdf

			されている事案。	する特別チーム組成 ・情報セキュリティ監視委員会の設置[44]

そこで、今回のアンケート調査結果について、過去に漏えいを経験した企業と漏えいを経験していない企業とに分けた上で、営業秘密管理に対する意識や各種対策への取組状況の比較分析を試みた。

全体としては、営業秘密管理に対する意識や、各種対策への取組状況の割合について、過去に営業秘密の漏えいを経験した企業の方が相対的に高い傾向がある。

漏えいを経験した企業がリスクとして捉えている社会動向の変化と、漏えいを経験していない企業がリスクとして捉えている社会動向の変化を比較すると、「標的型攻撃の増加」や「データの活用機会の増加」「クラウドの利用機会の増加」「スマートフォン・タブレット機器等の急速な普及」等、情報端末の普及やネットワークを通じたデータ活用機会の増加等については差が見られず、両者ともに一定のリスクを感じている傾向にある。一方、「人材の流動化」については、漏えいを経験した企業においては 59.3%の企業がリスクを感じている一方で、漏えいを経験していない企業においては 28.6%に留まっている。人を通じた漏えい対策の重要性については、過年度の調査でも指摘されていた点であり、引き続き留意が必要であると思われる。また、「他社との協業・連携機会の活発化」についても、漏えいを経験した企業においては 29.1%がリスクを感じているのに対し、漏えいを経験していない企業では 13.0%に留まっており意識の差が見受けられる（図 4.1-1）。これらの２点については、漏えいを経験した企業と経験していない企業との間で、感じ方に差が見られた項目であり、特に漏えいを経験していない企業においては、こうした観点についても日頃から留意するべきポイントとして捉えておく必要があると思われる。

44 株式会社ベネッセホールディングスプレスリリース（2014 年 10 月 16 日）より
http://blog.benesse.ne.jp/bh/ja/news/m/2014/10/16/docs/20141016release.pdf

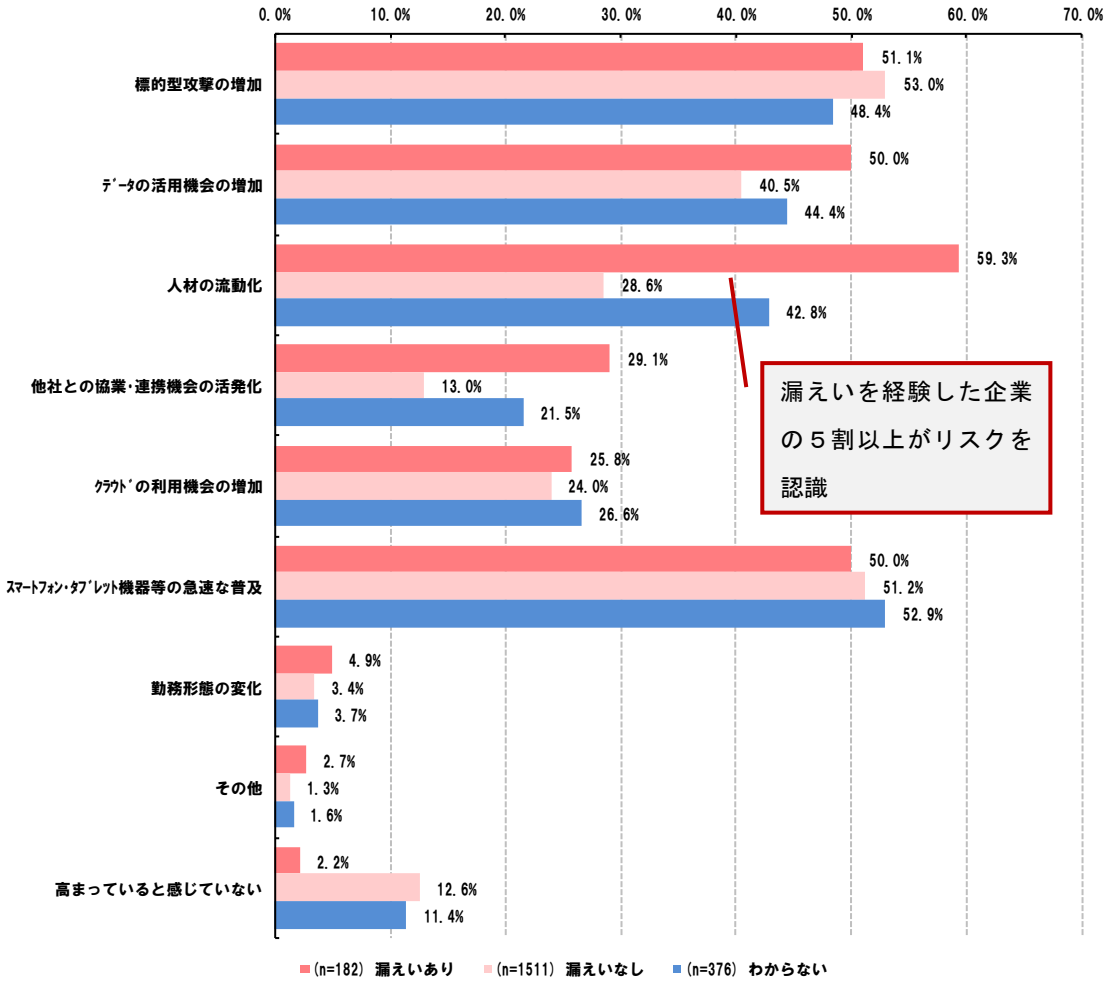

図 4.1-1　漏えい経験の有無によるリスク認識の比較（問 19×問 8）

具体的な対策への取組状況については全体的に漏えいを経験した企業の方が、漏えいを経験していない企業と比較して、相対的に取組が進んでいる傾向がある。例えば営業秘密へのアクセスをシステム的に制御することを目的とした対策の中で「PC 等の情報端末にはアンチウイルスソフトを導入している」「ファイアーウォール等を導入している」という基本的な取組について、漏えいを経験した企業においてはそれぞれ 78.0%、68.1%が実施しているのに対し、漏えいを経験していない企業においてはそれぞれ 59.8%、52.5%という状況である。また、「営業秘密の保存領域にはアクセス権を設定している」については漏えいを経験した企業の 63.2%が実施している一方で、漏えいを経験していない企業では 44.2%での実施に留まっており、漏えいを経験した企業が営業秘密へのアクセスをシステム的に制御するための基本的な対策を実施しているだけでなく、営業秘密の保存領域へのアクセス権の設定等も含めた多重的な取組を実施している傾向があることが窺える（図 4.1-2）。

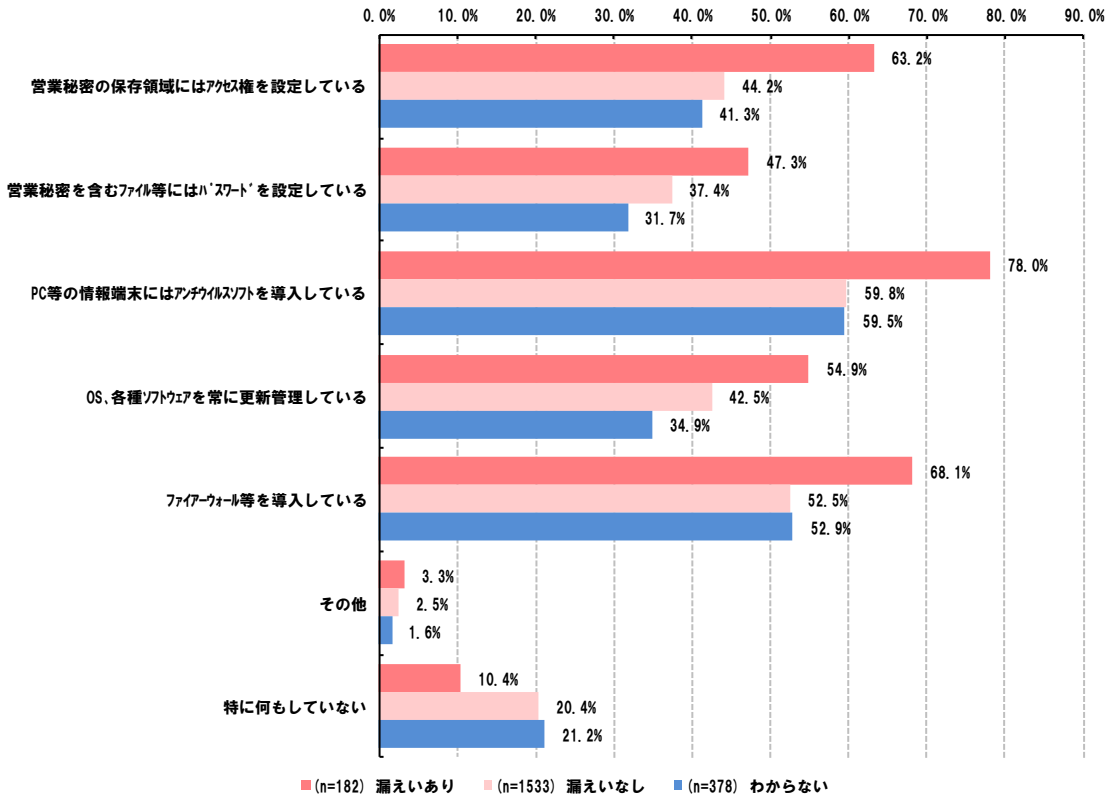

図 4.1-2　営業秘密へのアクセスをシステム的に制御する取組の比較（問 32×問 8）

営業秘密の持出しを困難化することを目的とした対策についても両者の取組状況に差が見られ、例えば「社内 PC に USB メモリ等を接続することを制御」について、漏えいを経験した企業では 41.8%が実施しているが、漏えいを経験していない企業では 24.0%に留まっている。また、「Web メールサイトやアップロードサイト等へのアクセスを制御」についても同様に、漏えいを経験した企業では 39.6%が実施しているが、漏えいを経験していない企業では 23.4%の実施に留まっている（図 4.1-3）。

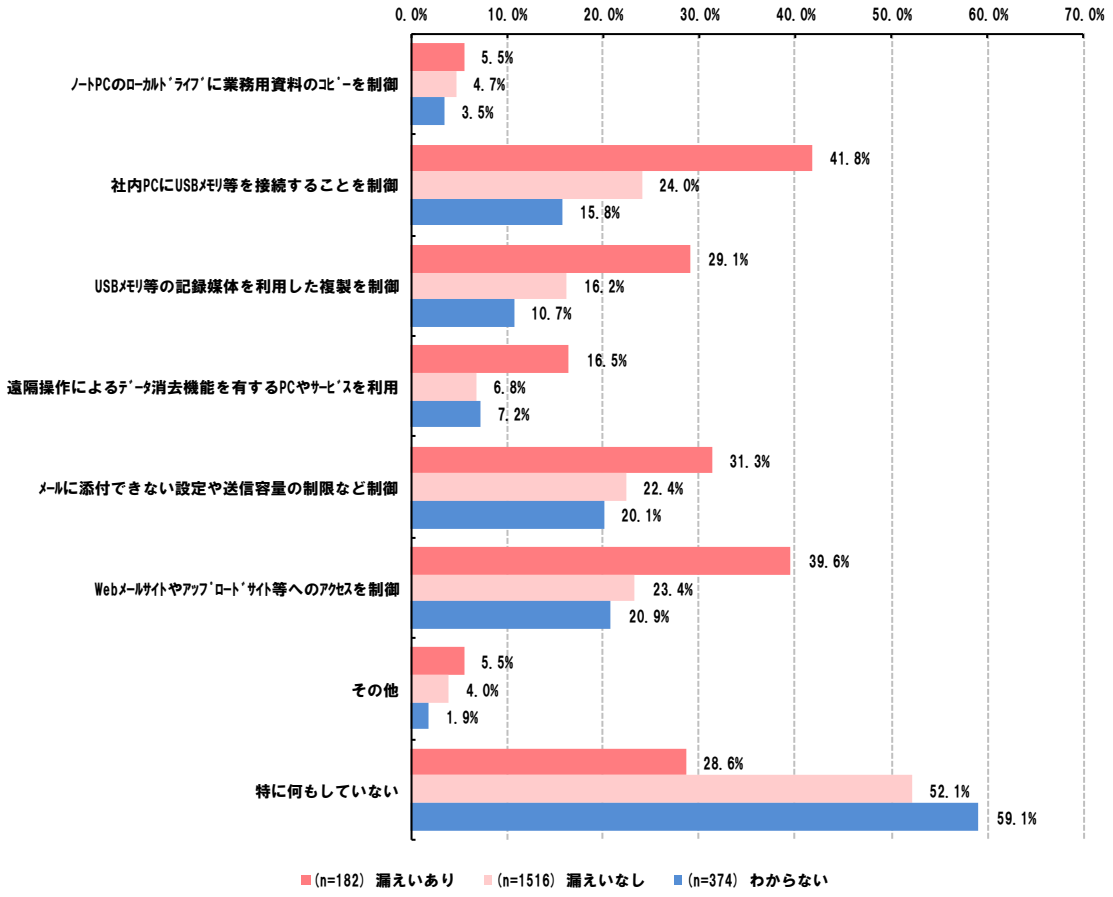

図 4.1-3　営業秘密の持出しをシステム的に困難化するための取組の比較（問 34×問 8）

漏えいしにくい環境をつくるためのシステム的な対策についても両者の取組状況に差が見られ、特に「情報システムのログを記録・保管している」については、漏えいを経験した企業においては 62.0%で実施されているが、漏えいを経験していない企業においては 42.4%に留まっている状況である。一方で、「不自然なアクセスは上司等に通知される」については、漏えいを経験した企業は、経験していない企業と比べてやや高い割合になっているものの、それでも 17.9%に留まっている。加えて、「不自然なアクセスは本人に警告される」については営業秘密の漏えいを経験した企業、経験していない企業の両方が 13%程度となっており、差は見られない（図 4.1-4）。したがって、営業秘密の漏えいを経験した企業は、まずは情報システムのログを記録・保管するという取組を強化していていることが窺えるが、その結果を分析等して通知するというような具体的なアクションにまではつなげられていないことが窺える。

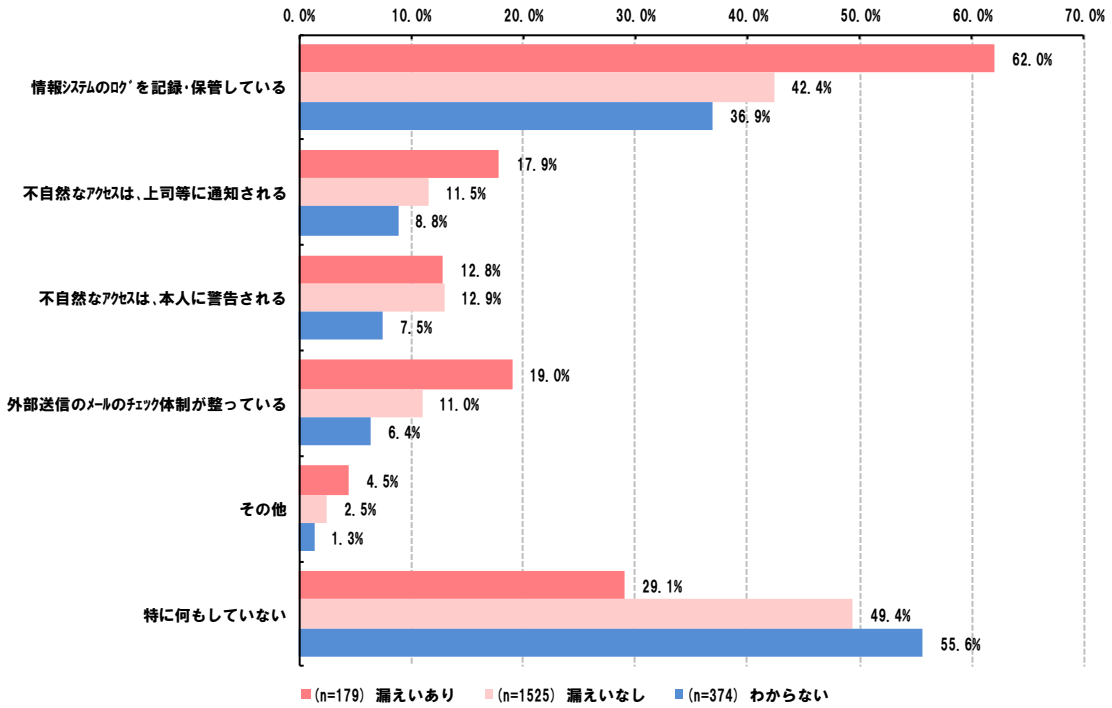

図 4.1-4　営業秘密が漏えいしにくい環境をつくるためのシステム的な対策の比較（問 36×問 8）

従業員等向けの特有の対策として、「研修実施等で取扱のルールを社内で周知徹底している」については、漏えいを経験した企業においては 55.6%で実施されているのに対し、漏えいを経験していな企業では 36.1%でしか実施されておらず、大きな差が見られる（図 4.1-5）。

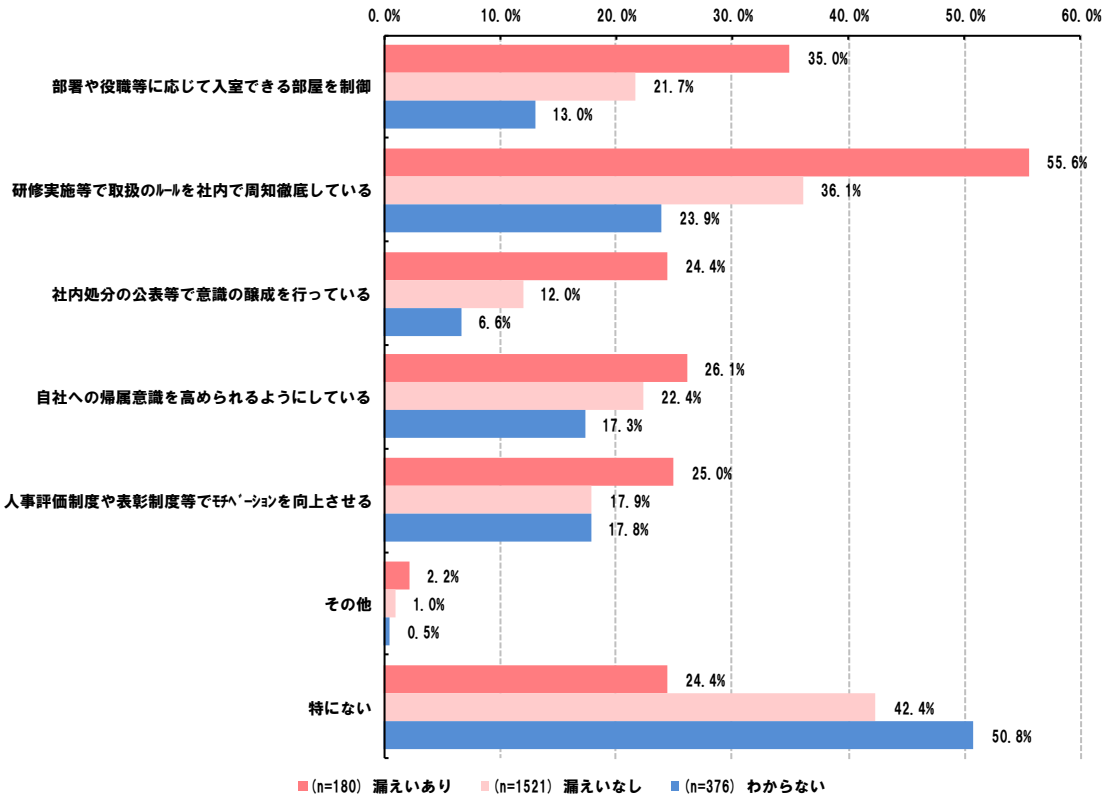

図 4.1-5　従業員等向け対策の比較（問 42×問 8）

取引先向けの特有の対策についても両者の取組状況に差が見られ、「営業秘密授受等が発生する取引先には秘密保持契約を締結」については営業秘密の漏えいを経験した企業のうち 64.1%で実施されているのに対し、漏えいを経験していない企業では 44.1%となっている。また、「契約書に情報漏えいに関する損害賠償等の条項を入れる」についても、営業秘密の漏えいを経験した企業のうち 58.0%で実施されている一方で、漏えいを経験していない企業では 37.2%となっている。加えて、「取引先の情報管理状況の監査ができる」について、営業秘密の漏えいを経験した企業の 20.4%が実施できているのに対し、漏えいを経験していない企業では 7.8%でしか実施できておらず、営業秘密の漏えいを経験した企業では、一定程度ではあるが、秘密保持契約を締結するだけでなく、その履行状況についても実際に確認を行うことまで実施する意識があるという傾向が窺える（図 4.1-6）。

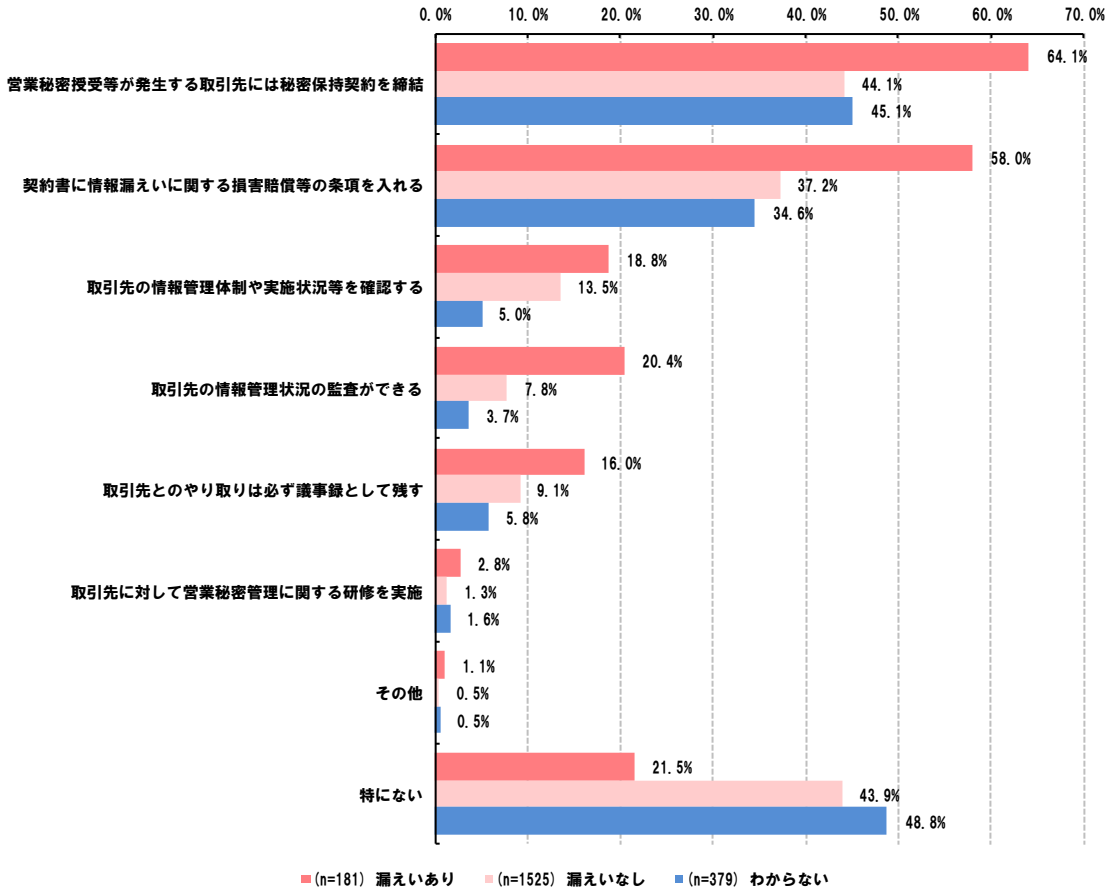

図 4.1-6　取引先向け対策の比較（問 44×問 8）

また、こうした個別具体的な対策に加えて、営業秘密の漏えいに気付けるような活動についても、営業秘密の漏えいを経験した企業の方が積極的に取り組んでいる傾向が見られる。営業秘密の漏えいを経験した企業のうち、74.2%でこうした活動が実施されているが、漏えいを経験していない企業では 51.2%に留まっている。さらに、営業秘密の漏えいを経験した企業のうち、55.5%でこうした活動を実施していることを従業員等に周知しており、検知活動の有効性を高める取組を積極的に実施していることが窺える（図 4.1-7）。

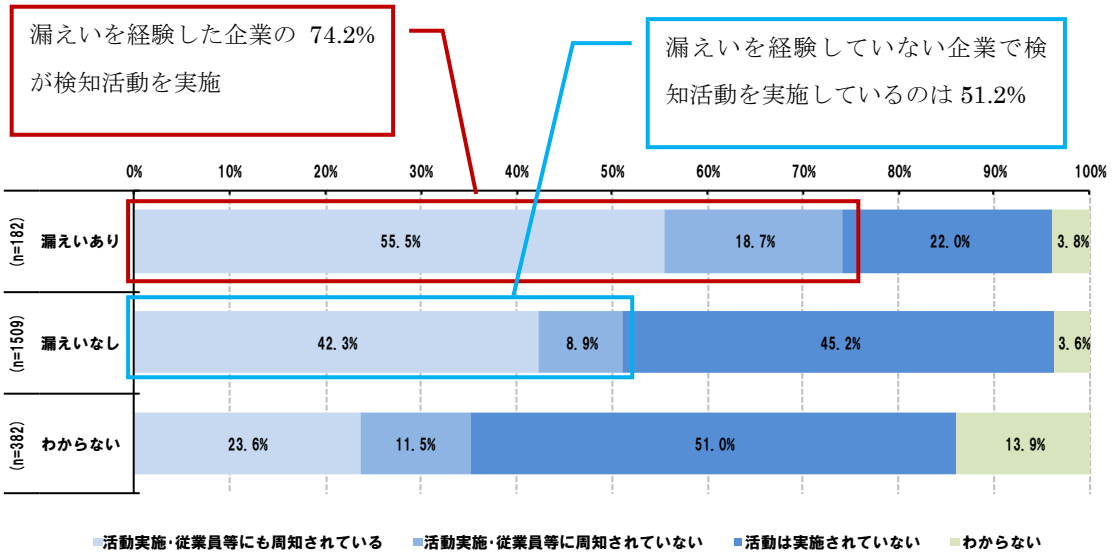

図 4.1-7　漏えいに気付けるような活動の実施状況の比較（問 9×問 8）

過去５年間で営業秘密の漏えいを経験していない企業は、漏えいが発生していない要因として、相対的に高い割合の企業が「データ等の暗号化・アクセス制限を行ったこと（24.3%）」「データ等の持ち出し制限を行ったこと（33.1%）」「秘密保持契約を締結していること（25.0%）」「情報管理方針等を整備していること（30.4%）」をあげている（図 4.1-8）。これらの対策は、図 4.1-2 や図 4.1-3 で示した通り、過去５年間で営業秘密の漏えいを経験した企業の多くが現在積極的に取り組んでいることが窺える内容であり、効果的な取組の一つであると考えられる。

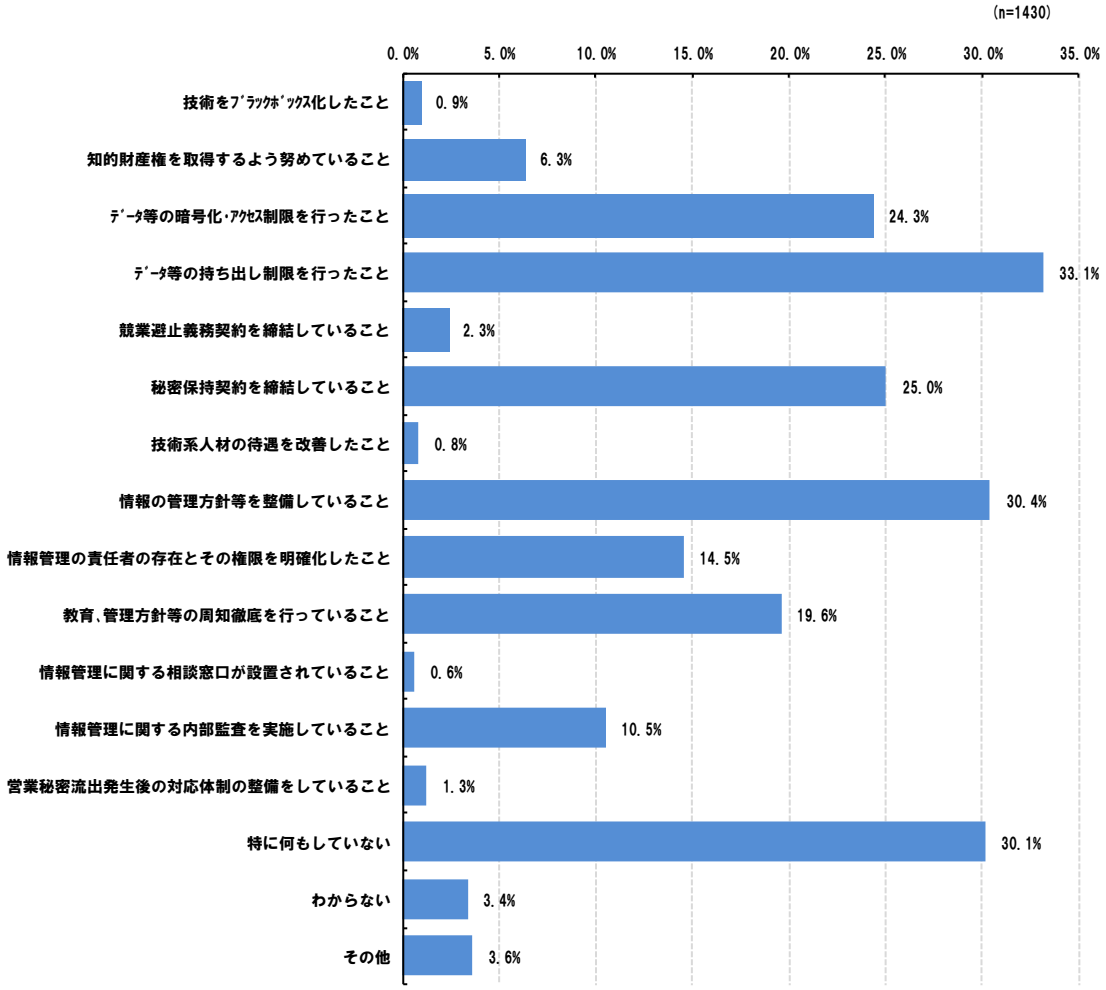

図 4.1-8　営業秘密の漏えいが発生していない要因（全業種・全規模）（問 18）

4.2. 営業秘密管理の対象の明確化

秘密情報の保護ハンドブックにも記載されているように、個別具体的な対策に取り組む前提として、社内にある情報のうち、営業秘密として管理するものと管理しないものを区分することから始めるのが重要である。営業秘密として管理する対象と、そのような管理を行わない対象を区分することの意義は、営業秘密としての管理対象を特定することで、その対象の重要性等を考慮した適切な管理を検討できる点にある。また、情報の管理区分として、さらに重要度等に応じて適宜格付け（「極秘」「秘」「社外秘」等）を行うことも有用である。ただし、インタビュー調査においては、社内の全ての情報に対してこうした区分を行い管理することは現実的ではないため、ある程度メリハリをつけた上で取り組んでいく必要があることが指摘されている。その際に、例えば漏えいした際の法的なエンフォースメントの必要性等の観点で営業秘密管理の対象として区分するべきかどうかを検討していくことも有用である。こうした区分を行うことは、社内で営業秘密として扱うものを明確化したり、また管理の水準等を検討したりする上で必要となるため、営業秘密管理に関する基本的な取組となる。営業秘密が争点となった過去の判例からも、営業秘密として管理する対象が明らかになっていないようなケースでは、そのことを否定的要素として捉えているものもあり[45]、営業秘密として管理する対象を明確化することの重要性を示唆している。そのため、営業秘密として管理する対象と、管理を行わない対象を明確に区分している企業においては、個別具体的な漏えい対策への取組も進んでいると思われ、その実施内容等は参考になると考えられる。

そこで、営業秘密として管理する対象と、そうではない対象を区分できている企業とできていない企業とに分けた上で、各種対策等への取組状況の比較分析を試みた。

全体的な傾向としては、営業秘密とそれ以外の情報を区分できている企業の方が、そうではない企業と比べて取組が進んでいることが窺える。例えば営業秘密へのアクセスを物理的に制御する取組である「営業秘密を一般情報とは分離して保管するようにしている」「営業秘密を破棄する際には復元が不可能な方法で実施」については、営業秘密とそれ以外の情報を区分し、営業秘密の中でも区分を行っている企業においては、それぞれ 69.8%、67.9%の企業が実施しているが、営業秘密とそれ以外の情報を区分していない企業では前者が 14.9%、後者が 30.9%という状況であり、両者の間に大きな差が見られる（図 4.2-1）。

[45] 営業秘密として管理する対象を明らかにしなかったことで、秘密管理性の否定的要素に働いたケースでは、例えば「秘密とする旨の表示もなかったというのであるから，秘密管理性を認めることは困難である（東京地判 H27.10.22 [LEX/DB: 25447549]）」という指摘がなされている。

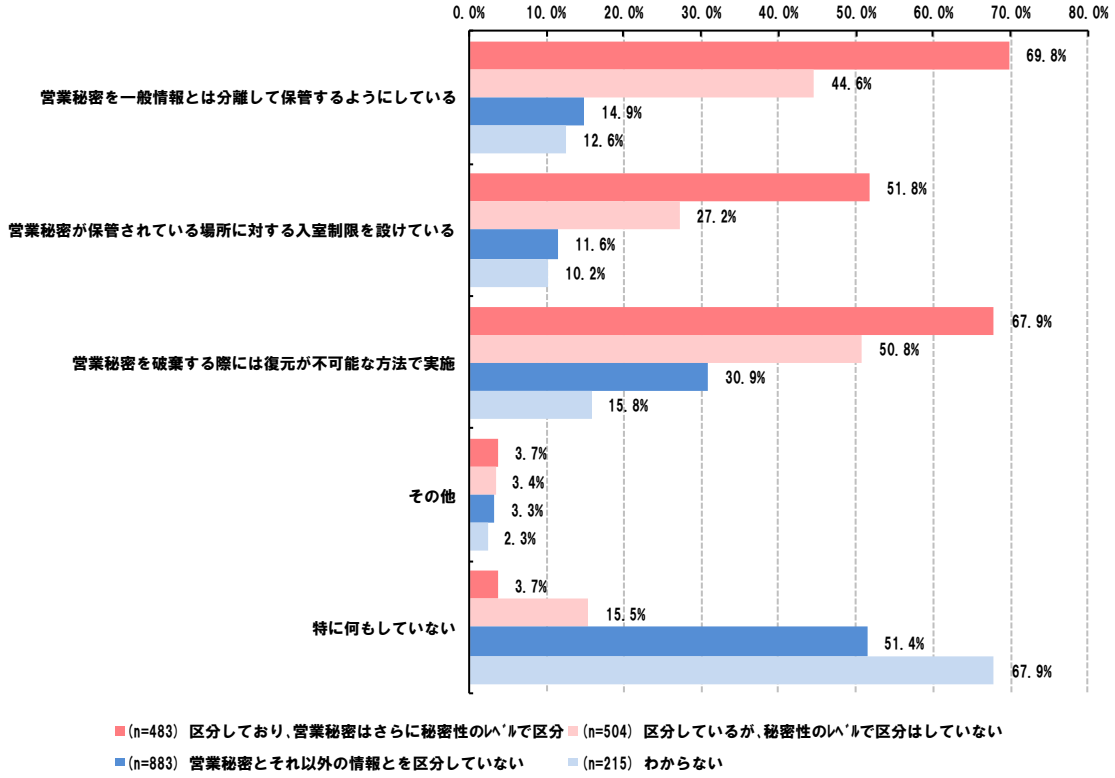

図 4.2-1　営業秘密へのアクセスを物理的に制御する対策への取組状況の比較
（問 31×問 21）

営業秘密へのアクセスをシステム的に制御する取組についても同様に、営業秘密とそれ以外の情報を区分し、営業秘密の中でも区分を行っている企業においては「営業秘密の保存領域にはアクセス権を設定している」「PC 等の情報端末にはアンチウイルスソフトを導入している」「ファイアーウォール等を導入している」についてそれぞれ 84.7%、86.5%、81.0%の企業が実施できているが、営業秘密とそれ以外の情報を区分していない企業では、それぞれ 25.8%、50.0%、43.8%に留まる状況であり、基本的な対策も含めた対応に取り組む必要があると思われる（図 4.2-2）。

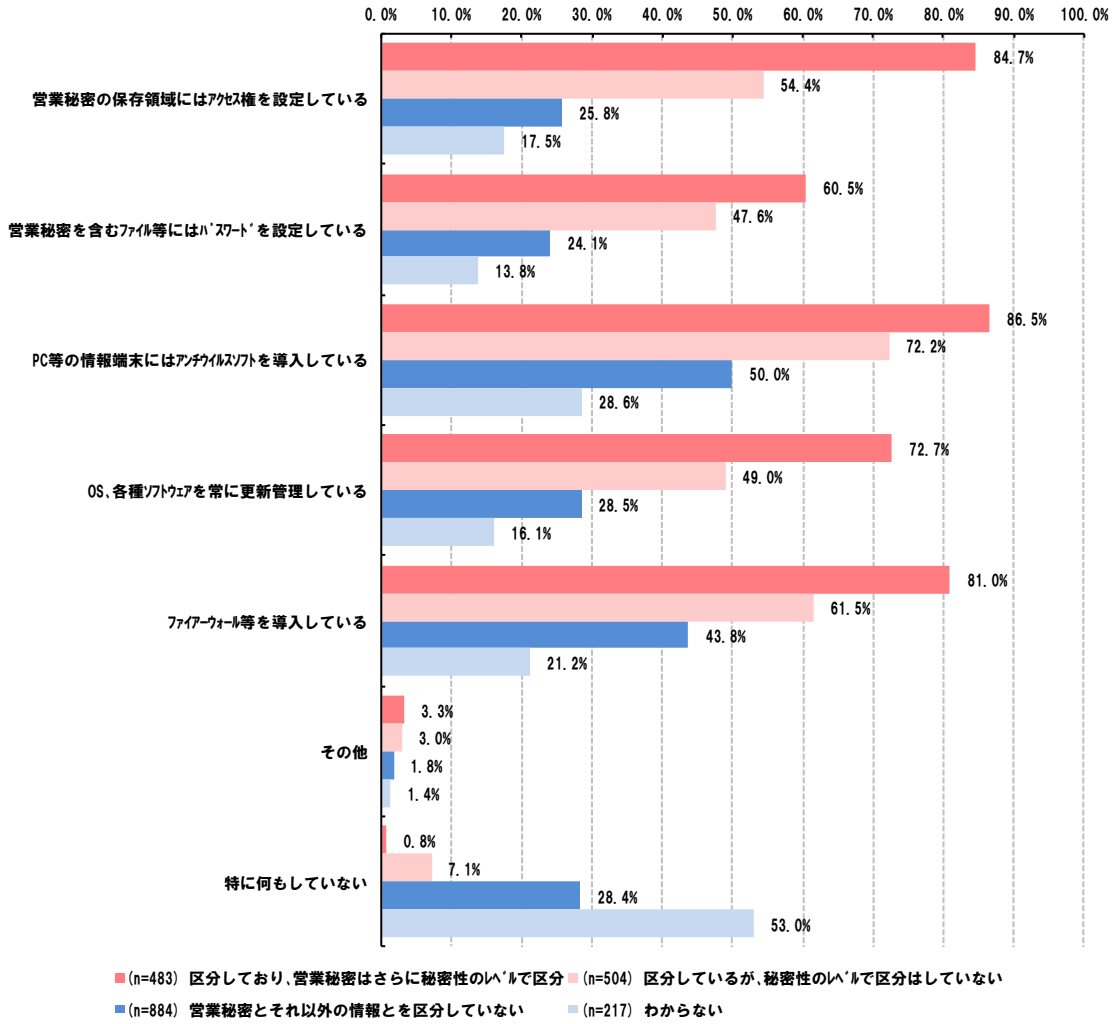

図 4.2-2　営業秘密へのアクセスをシステム的に制御する対策への取組状況の比較
（問 32×問 21）

営業秘密を保護する上で有用な対策として、上述したような営業秘密への接近制御に資する対策のほかに、営業秘密の持出し困難化に資する対策もある。営業秘密とそれ以外の情報を区分し、営業秘密の中でも区分を行っている企業では、例えば「USB メモリや DVD 等の持ち込み・持ち出しを禁止している」という対策については、65.4%が取り組んでいるのに対し、営業秘密とそれ以外の情報を区分していない企業では 23.3%しか取り組めていない。また、「PC 等は持ち出すことが出来ないようにしている」については、営業秘密とそれ以外の情報を区分し、営業秘密の中でも区分を行っている企業では 37.1%が取り組めているが、営業秘密とそれ以外の情報を区分していない企業では 8.0%しか取り組めておらず、営業秘密へのアクセスだけでなく、持出しという観点でも両者の取組状況に大きな差があることが窺える（図 4.2-3）。

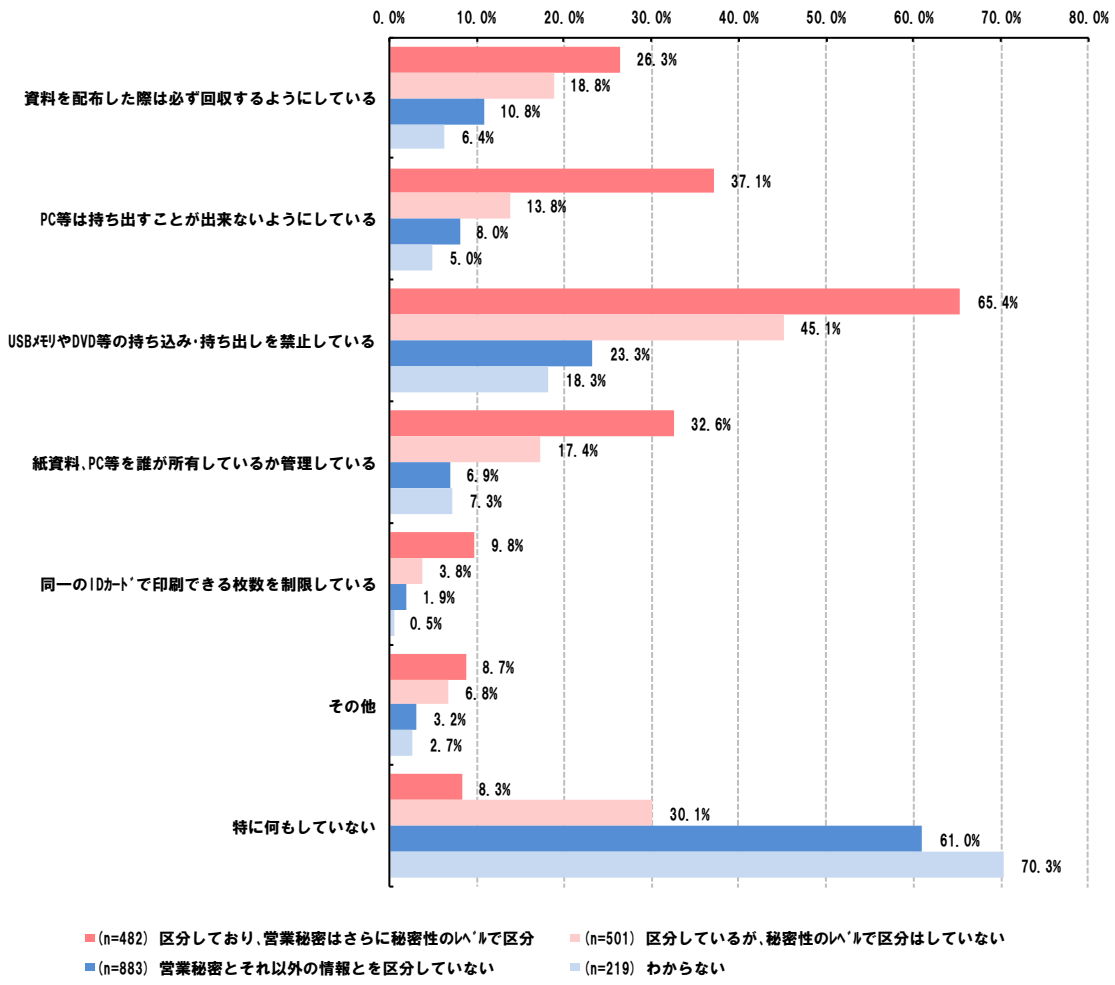

図 4.2-3　営業秘密の持出しを物理的に困難にする対策への取組状況の比較(問 33×問 21)

また、視認性の確保を目的とした物理的な対策については、営業秘密とそれ以外の情報を区分し、営業秘密の中でも区分を行っている企業では、例えば「社員に社員証等の着用を義務付けている」については、73.6%が取り組んでいるのに対し、営業秘密とそれ以外の情報を区分していない企業ではこうした容易に取り組める基本的な対策でも 21.8%という状況である。加えて、「不要な書類等の廃棄等、職場全体が整理整頓されている」というような基本的な取組についても、営業秘密とそれ以外の情報を区分し、営業秘密の中でも区分を行っている企業では 62.8%が取り組んでいるのに対し、営業秘密とそれ以外の情報を区分していない企業では 28.2%という状況である（図 4.2-4)。

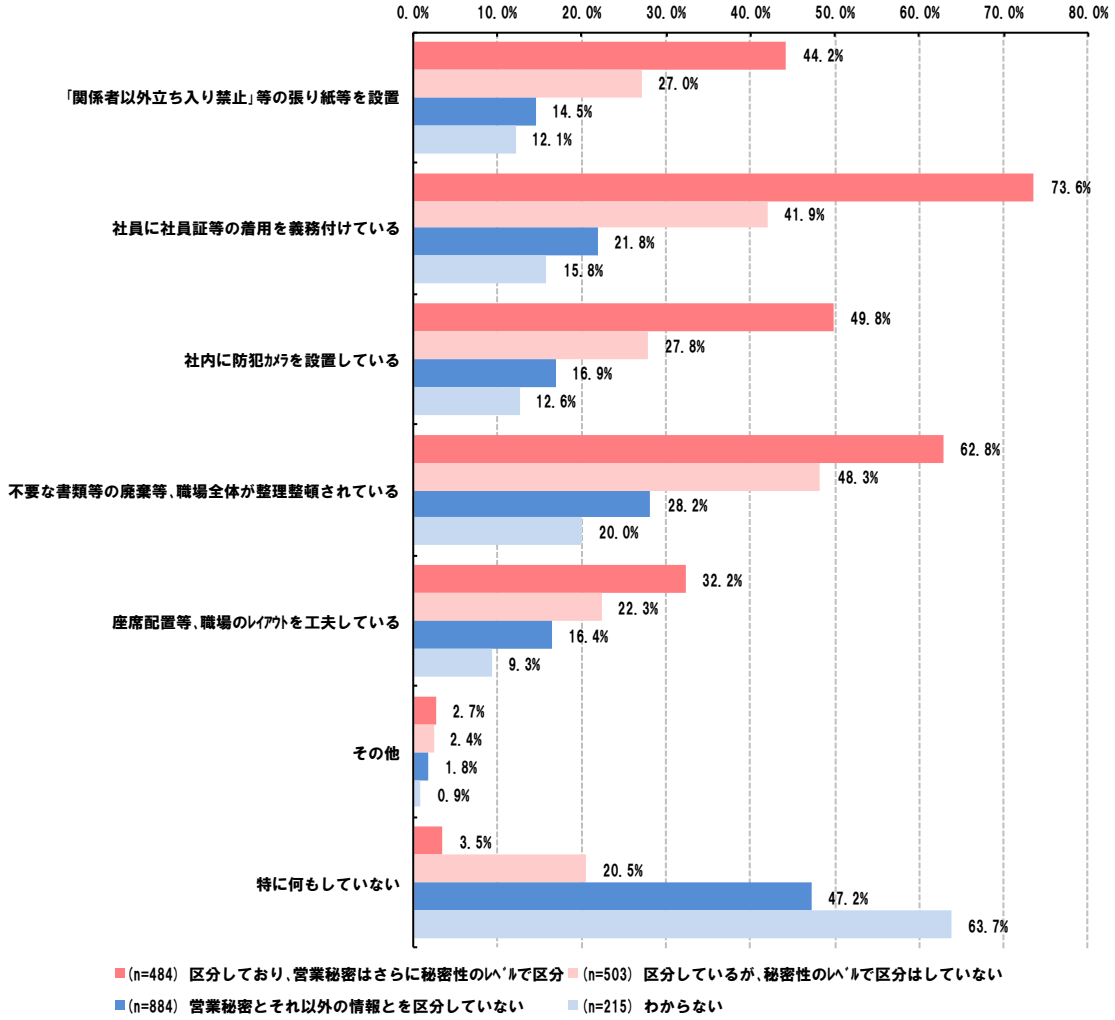

図 4.2-4　営業秘密が漏えいしにくい環境をつくるための物理的な対策への取組状況の比較（問 35×問 21）

視認性の確保を目的としたシステム的な対策への取組状況についても両者の間に大きな差があることが見受けられ、営業秘密とそれ以外の情報を区分し、営業秘密の中でも区分を行っている企業では、例えば「情報システムのログを記録・保管している」については、81.5%が取り組んでいるのに対し、営業秘密とそれ以外の情報を区分していない企業では25.0%しか取り組めていないという状況である。また、営業秘密とそれ以外の情報を区分し、営業秘密の中でも区分を行っている企業では 28.0%が「不自然なアクセスは、上司等に通知される」等、ログの収集だけでなく、その内容から具体的なアクションにまでつなげられているが、営業秘密とそれ以外の情報を区分していない企業での取組の割合は 5.2%に留まっている（図 4.2-5）。

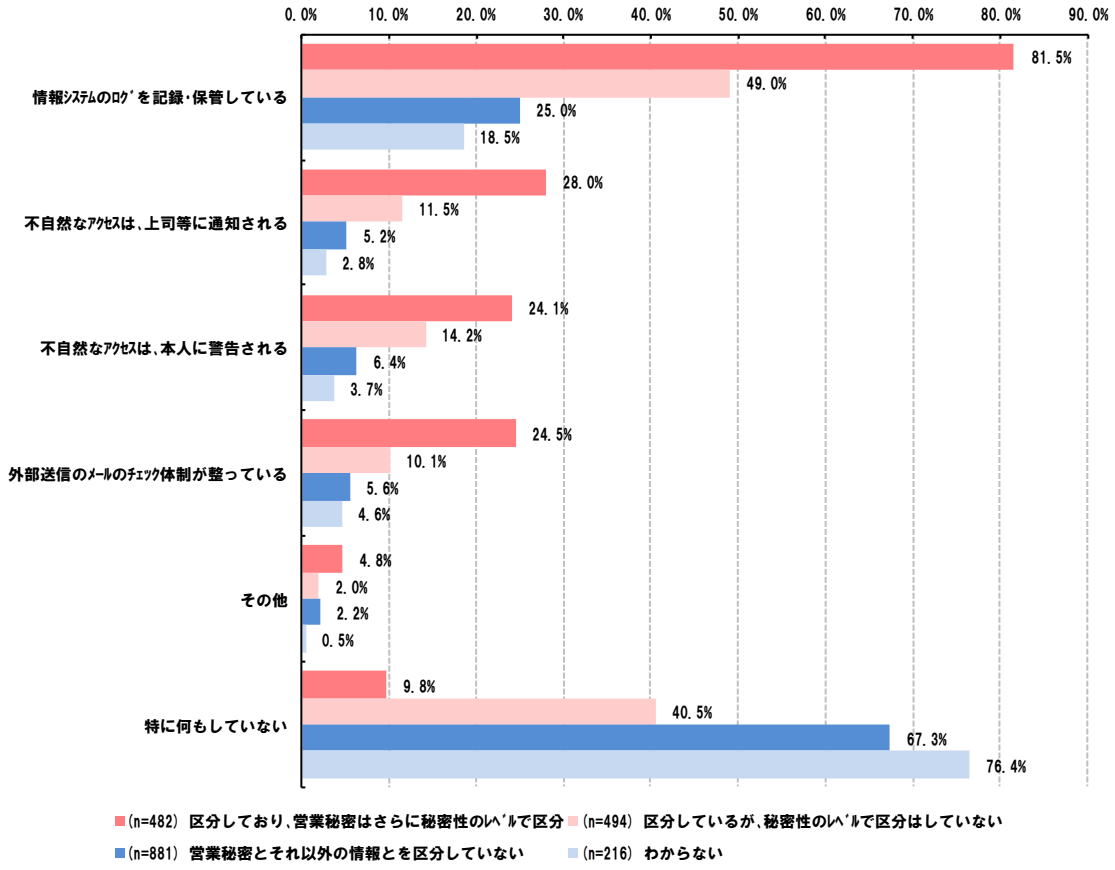

図 4.2-5　営業秘密が漏えいしにくい環境をつくるためのシステム的な対策への取組状況の比較（問 36×問 21）

こうした取組を企業として実施することが重要であるのと同時に、営業秘密管理の重要性を従業員等に対して示して認識してもらう等、従業員向けに特化した対策を実施することも重要である。

営業秘密とそれ以外の情報を区分し、営業秘密の中でも区分を行っている企業では、例えば「研修実施等で取扱のルールを社内で周知徹底している」については、74.2%が実施して普及啓発に取り組んでいるのに対し、営業秘密とそれ以外の情報を区分していない企業では 18.0%という状況である。また、「部署や役職等に応じて入室できる部屋を制御」についても、営業秘密とそれ以外の情報を区分し、営業秘密の中でも区分を行っている企業では 46.0%が取り組んでいるのに対し、営業秘密とそれ以外の情報を区分していない企業では 11.9%しか取り組めておらず、従業員向けの十分な対策を実施できていない（図 4.2-6）。

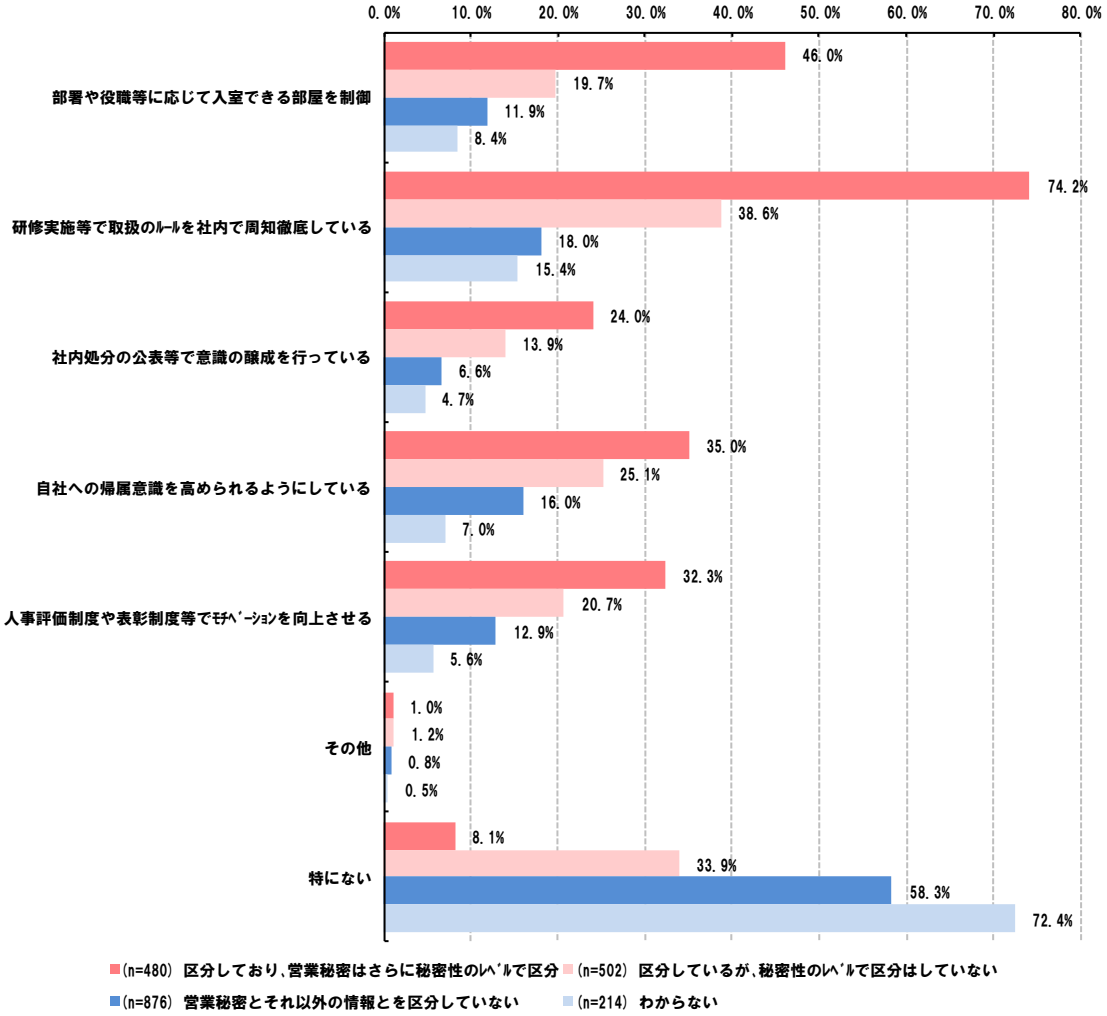

図 4.2-6　従業員等向けの特有の対策への取組状況の比較（問 42×問 21）

4.3. 企業の特性等に応じた営業秘密保護対策の考え方

営業秘密の漏えい対策については、実施するために一定のコストを要するものや、金銭的なコストはほとんど費やさずに実施できるもの等、様々なものが提唱されているが、これらの対策の全てを実施しなければならないというものではなく、企業の規模等に応じて、適切な対策を講じることが重要である。こうした指摘は、かねてよりなされてきたところであり、また昨今経済産業省が公開した秘密情報の保護ハンドブック内でも言及されている。

秘密情報の保護ハンドブックによれば、①接近の制御、②持出し困難化、③視認性の確保、④秘密情報に対する認識向上、⑤信頼関係の維持・向上といった５つの目的に応じた営業秘密漏えい対策を、企業の規模や業種、対策にかけることのできる費用等を鑑みた上で、バランス良く選択して実施していくことが重要であるとされている。企業において、営業秘密の保護対策を検討・実施する際には、闇雲に対策を実施してしまうと、対策に偏りが生じてしまったり、必要以上に業務上の制限やコスト等が発生してしまったりする可能性があるため、こうした５つの目的を意識しながら実施することが望ましい。これは、場所・状況・環境に潜む「機会」が犯罪を誘発するという犯罪学の考え方などを参考としている。

こうして分類した各種対策の中でも、物理的な手法で実施する対策やシステム的に実施する対策、人的な観点で実施する対策等があり、大規模企業であっても全て網羅的に導入することは難しい場合もある。したがって、そのような多種多様な対策の中で、例えば大規模企業であっても取組が遅れている対策や、特に中小規模企業において取組の遅れが目立つ対策等に着目することは、今後企業がどのような対策に取り組んでいくことが有用であるかを検討する上での示唆になるものと思われる。

全体的な取組状況を見ると、大規模企業で実施されている割合と、中小規模企業で実施されている割合に差がある対策が多いのが事実であるが、例えばシステム的な投資を要する対策等については特に中小規模企業では取り組まれていないケースが多い。ただ、中小規模企業の中でも、101 人～300 人程度の規模の場合には、システム的な対策も含めてある程度取り組まれている場合も多い。したがって、大規模と中小規模で二分するよりも細かく分けて取組状況を捉えることが有用であると思われるため、企業の規模を６つに分けて比較分析を試みた。

4.3.1. 接近制御：入室制限に関する対策

この中で、例えば①接近の制御に関する対策である「入室制限」については、中小規模企業では１割未満、大規模企業であっても４割前後の企業でしか実施できておらず、他の

対策と比較して大規模企業も含めて相対的に取組が進んでいない（図 4.3-1）。

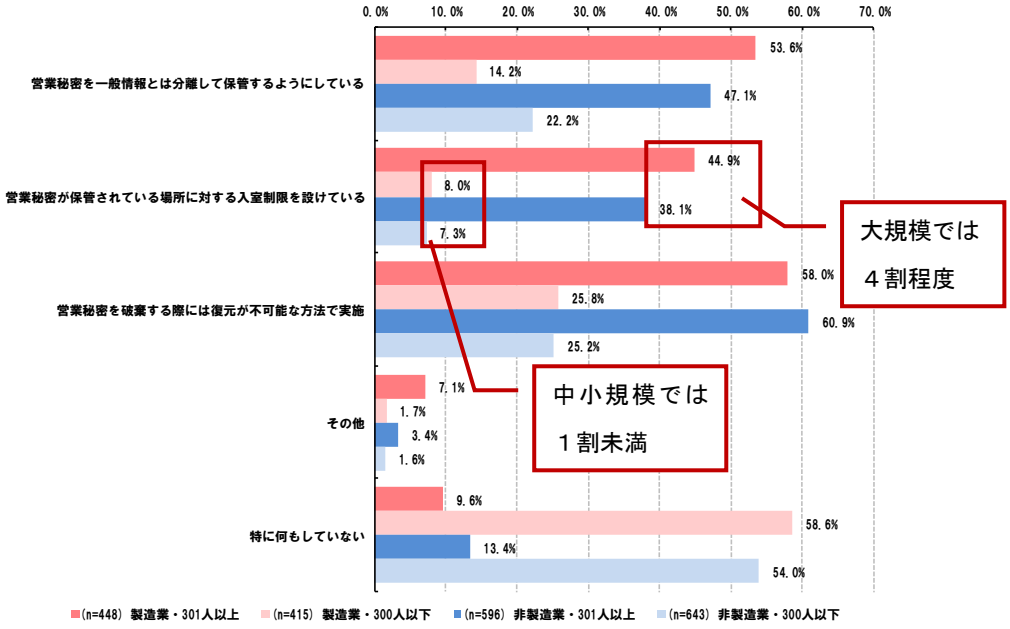

図 4.3-1　入室制限に関する対策への取組状況（問 31）

従業員規模別に細かく見ると、特に従業員規模が 100 人以下の企業で取組が遅れていることが見受けられる。また、101 人～3,000 人規模の企業でも３～５割程度の実施状況であり、ある程度の規模の企業でも取組が進んでいない（図 4.3-2）。この点について、入室制限の実施にあたっては従業員の ID 等に紐づいた権限が設定されたセキュリティカードと、そのセキュリティカードによって開錠の可否を認識できる機器の導入等が必要であり、他の対策よりも一定の投資が必要となることにも起因すると考えられる。

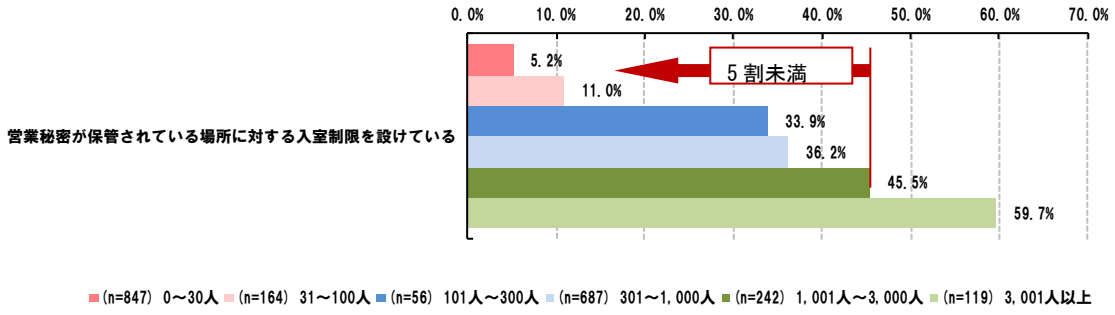

図 4.3-2　入室制限に関する対策への取組状況（従業員規模別）（問 31×問 4）

4.3.2. 接近制御：営業秘密が保存された領域へのアクセス権の設定に関する対策

また、「営業秘密が保存された領域へのアクセス権の設定」については、大規模企業で実

施されている割合と、中小規模企業で実施されている割合の差が目立って大きくなっている。この点については、中小規模企業の中でも特に 100 人以下の企業での取組が目立って遅れている状況である（図 4.3-3）。営業秘密等が格納されたフォルダ等へのアクセス権の設定については、一般的な手法であれば、大きなコストを要するものではなく、また営業秘密が争点となった判例からもアクセス権の設定の有無が裁判所の判断に影響をあたえる可能性があることが示唆されている。加えて、過去に営業秘密の漏えいを経験していない企業と比較した際に、過去に営業秘密の漏えいを経験した企業が現在実施している割合が相対的に高い対策でもある。こうしたことからも、中小規模企業に対して、アクセス権の設定の重要性を周知していく必要があると思われる。

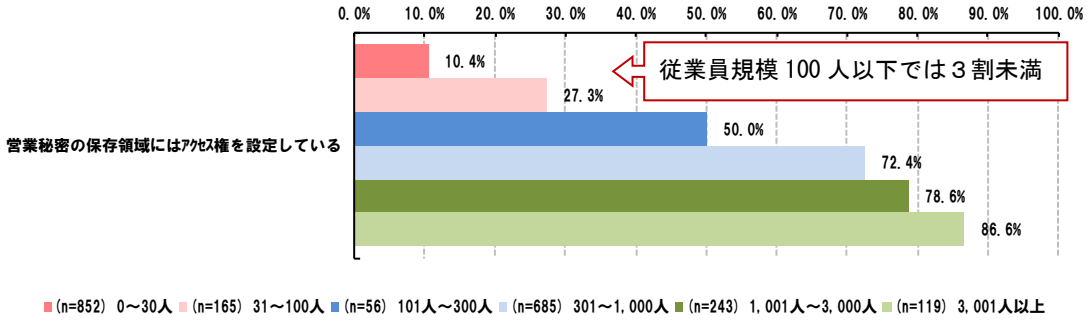

図 4.3-3　営業秘密の保存領域へのアクセス権設定（従業員規模別）（問 32×問 4）

4.3.3. 持出し困難化：PC の持出し制御に関する対策

②持出し困難化に資する対策については、①接近の制御に資する対策等と比較すると相対的に対策への取組が遅れている傾向がある。例えば、「PC の持ち出し禁止」については 3,001 人以上の規模の企業であっても 35.9%であり、100 人以下の企業においては１割以下の割合の企業でしか取り組めていない（図 4.3-4）。

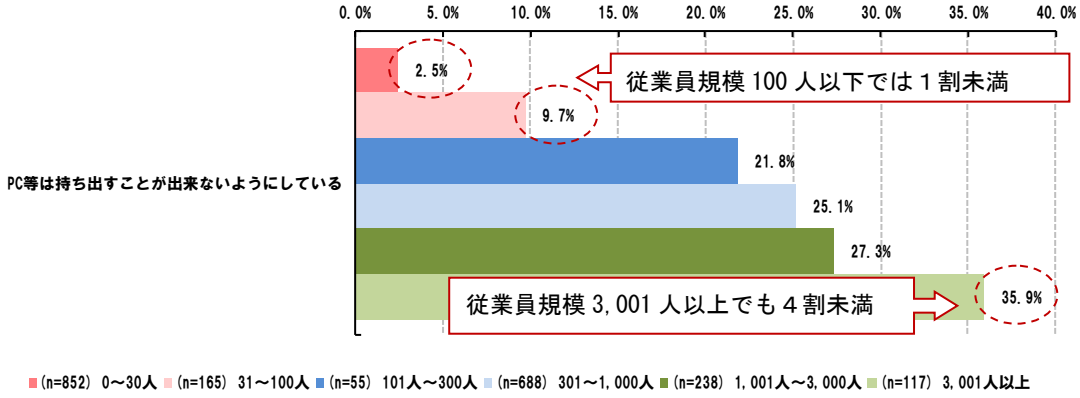

図 4.3-4　PC 等の持出し制御に関する取組状況（従業員規模別）（問 33×問 4）

インタビュー調査の対象とした一部の企業では、シャットダウン時にローカルドライブに保存されたファイルを全て消去する機能が備わっているという前提で PC の持出しを許可しているという例があったが、アンケート調査結果では「ノート PC のローカルドライブに業務用資料のコピーを制御」については大規模企業、中小規模企業ともに 1 割未満でしか実施されていないため、そのような対策をあわせて実施している企業はごく一部であると推察される（図 4.3-5）。この点については、コスト的な問題というよりも、情報端末を利用して業務を行うことが一般的となっているためノート PC 等を日常的に持出して業務を行う企業も少なくなく、運用面での問題であると考えられる。そのような事情を鑑みて、PC の持出しが企業によっては日常的に発生せざるをえないものであるという前提に立てば、PC の紛失等に伴う営業秘密漏えいを防止するために、ノート PC にログインする際に複数回パスワードの入力を行うことや、ノート PC のローカルドライブへのコピーの禁止か、シャットダウン時のローカルファイル一括削除等、システム的に何かしらの対策を講じておくことが望ましい。

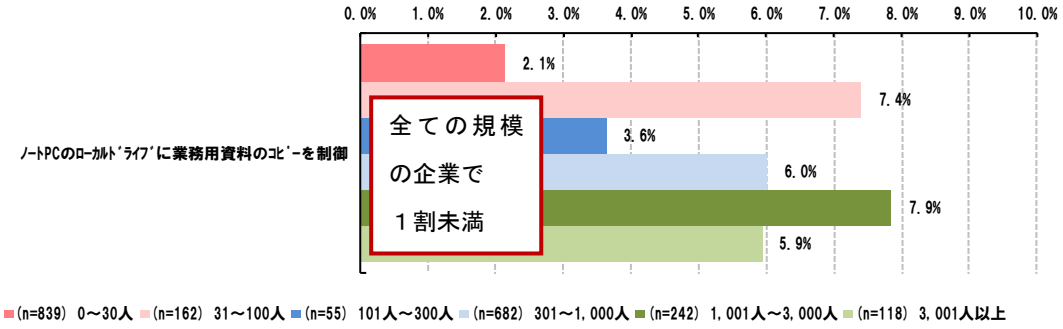

図 4.3-5　PC のローカルドライブへのファイルコピー制御に関する取組状況（問 34×問 4）

4.3.4. 持出し困難化：USB メモリの制御に関する対策

「USB メモリや DVD 等の持ち込み・持ち出しの禁止」「PC への USB メモリ等の接続制御」「USB メモリ等への複製制御」については、大規模企業と中小規模企業との間で取組状況に大きな差が見られ、特に 100 人以下の企業で取組が遅れている傾向が目立っている（図 4.3-6）。

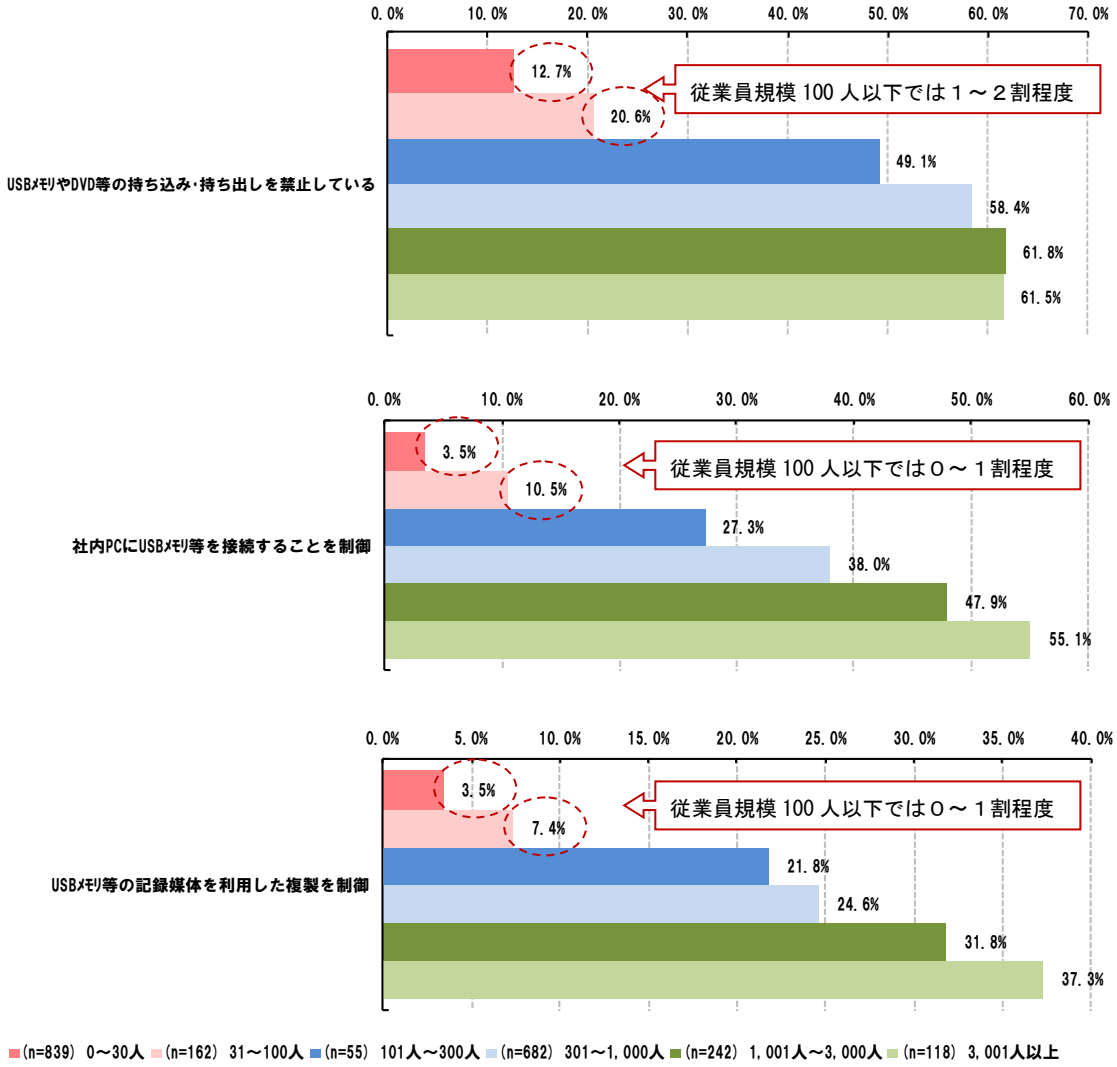

図 4.3-6　USB メモリの利用制御等に関する取組状況（従業員規模別）（問 33・34×問 4）

USB メモリ等の接続制御等を導入するにあたっては、一定の投資が必要となる可能性があるが、図 4.1-3 でも示されている通り、過去に漏えいを経験した企業が現在相対的に積極的に取り組んでいる対策であることや、実際に人を通じて発生した漏えい事案が記録媒体を利用したものであったケースも複数あるため、中小規模企業においても可能な範囲での対策に取り組むことが重要であると思われる。

4.3.5. 視認性の確保：ログの記録・保管等に関する対策

③視認性の確保に資する対策は、秘密情報の保護ハンドブックによれば、漏えい行為を

行ったとしても見つかってしまう可能性が高いということを認識する状況を作り出すことを目的とした対策である。例えば、「情報システムログの保管」については、情報漏えいが発生した際の証拠の確保手段としての意義もあるとされている。ログの保管そのものについては、大規模企業においては７割以上の企業が実施できているが、中小規模企業においては５割未満の企業しか実施できておらず、特に 100 人以下の従業員規模になると２割未満の企業でしか実施されていない（図 4.3-7）。この点については、ログの記録・保管ができるツール等の導入や、それを運用する人員の確保等、リソースが不足している中小規模企業にとっては対策を行う上での障壁が存在する可能性がある。一方、大規模企業においては、ログの保管そのものについては多くの企業が実施できているが、「不自然なアクセスは上司等に通知される」「不自然なアクセスは本人に警告される」等、実際のアクションにまでつなげられている企業は３割未満に留まっている。インタビュー調査においても、ログは取得しているが、日頃からモニタリングしているわけではなく、漏えい等が発生した際の事後調査のための情報としてしか捉えられていない事例が複数あった。不自然な挙動のログを検知するには、決められた条件に合致するログが発生した際に担当部署・担当者等に自動で通知されるようなツールを導入する方法や、担当者を設置して定期的にログに対して特定のキーワード等で検索する方法等が考えられ、実施を検討することが必要であると思われる。また、ログの記録等、従業員等の挙動を確認できるようになっている（検知活動を実施している）ことについては、漏えい行為の抑止効果の意味合いも兼ねて、従業員等に周知することが有用であると思われる。

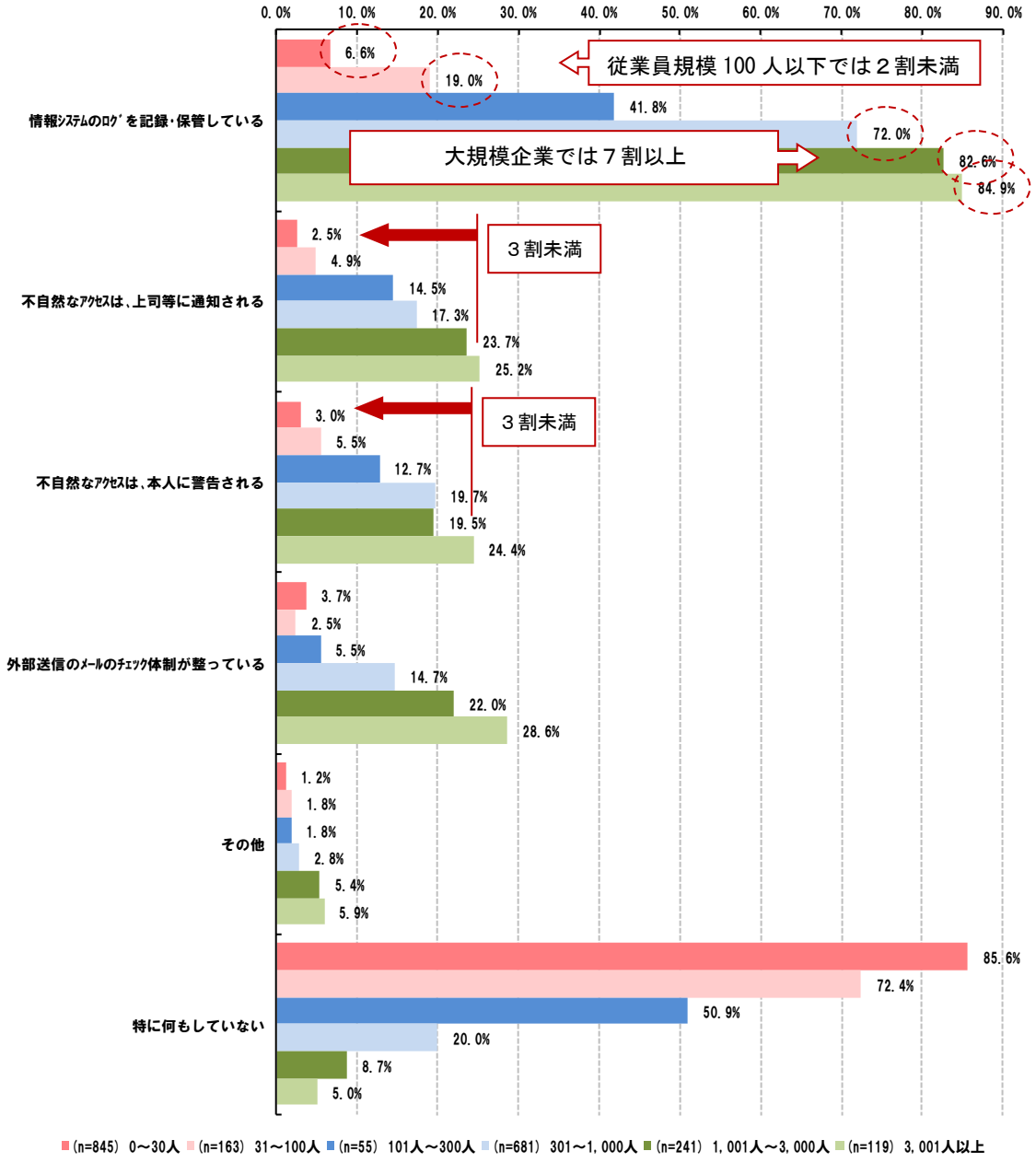

図 4.3-7　ログの取得と活用の状況（従業員規模別）（問 36×問 4）

4.3.6. 企業が有効性を実感している対策

アンケート調査結果によると、企業が取り組んでいる対策の中で、特に「PC 等の情報端末にはアンチウイルスソフトを導入している（21.7%）」「営業秘密の保存領域にはアクセス権を設定している（21.0%）」「ファイアーウォール等を導入している（17.8%）」については、相対的に回答する企業の割合が高く、その他の回答も含めてシステム的な対策に有効

性を感じている企業が多い。回答の割合が高い対策の中には、基本的なものもあり、この対策だけ実施すればよいというわけではないが、取組が遅れている企業が今後着手していく対策を検討する際には参考になると思われる（図 4.3-8）。

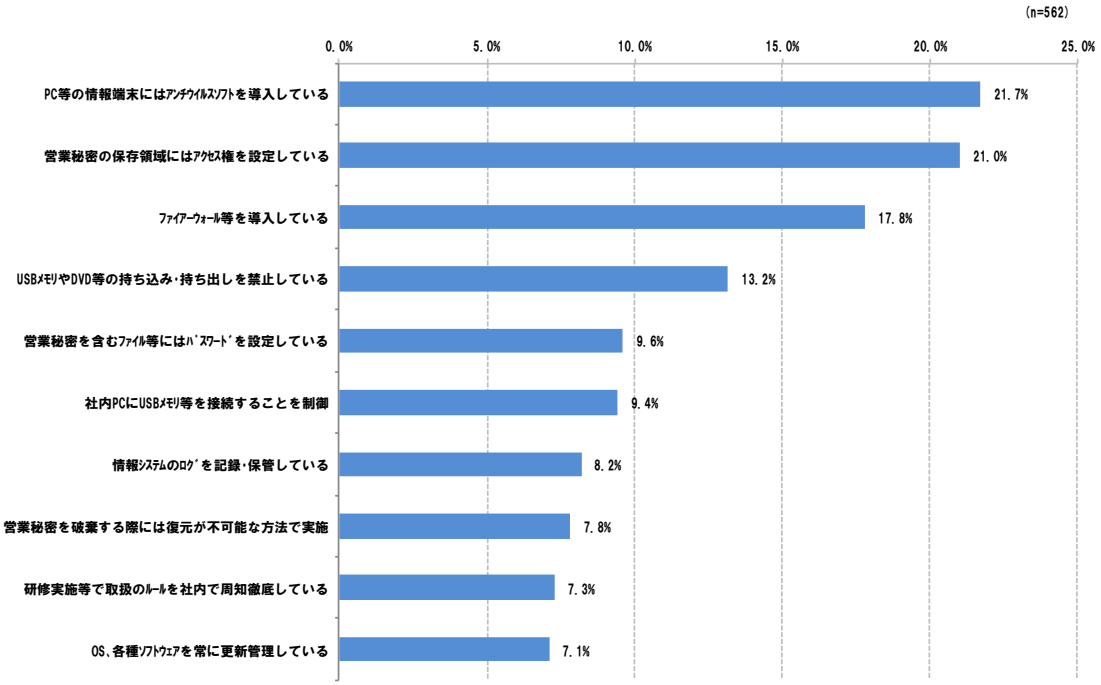

図 4.3-8　有効性が高いと感じた対策（上位 10 項目）（全業種・全規模）（問 51）

4.4. 組織横断的な取組の重要性

営業秘密は様々な部門等に存在しているものであるため、営業秘密管理に取り組むにあたっては、個々の担当者や部門等が独自に実施するのではなく全社的に検討した上で取り組んでいくことが望ましい。報道事例等からも明らかであるように、営業秘密の漏えいが企業の経営に大きな影響を与えるケースがあることは否定できず、したがって企業においては営業秘密を管理することを、経営に直結する問題の一つとして捉えて、経営層が積極的に関与した体制で管理方針や具体的手法等を検討していく事が重要である。

本アンケート調査結果によれば、53.3%の企業が営業秘密管理を経営に直結する問題と捉えている一方で、残りの企業は経営に直結する問題とは捉えていない（図 2.4-1 参照）。

社内における営業秘密とそれ以外の情報の区分の実態について、両者を比較してみると、営業秘密管理を経営に直結する問題として捉えている企業のうち 62.1%が営業秘密とその他の情報を区分しているのに対し、営業秘密管理を経営に直結する問題として捉えていない企業では 30.2%しか区分できていない（図 4.4-1）。

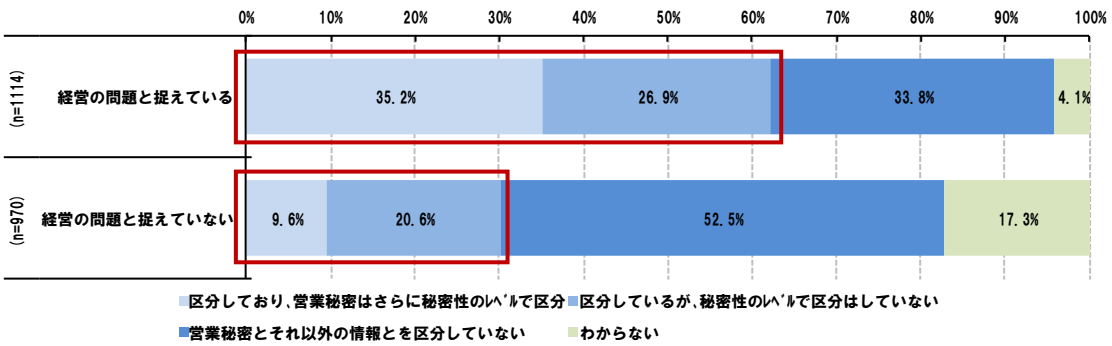

図 4.4-1　営業秘密とそれ以外の情報の区分状況の比較（問 21×問 26）

また、本来営業秘密として管理するべき情報を実際に営業秘密として管理できている割合についても、両者の間で差が見られる。営業秘密管理を経営に直結する問題として捉えている企業は、77.2%の企業において半分以上は営業秘密として管理できているが、営業秘密管理を経営に直結する問題として捉えていない企業においては、営業秘密として管理できている情報の比率が半分以上に達している企業は 47.5%だけである（図 4.4-2）。

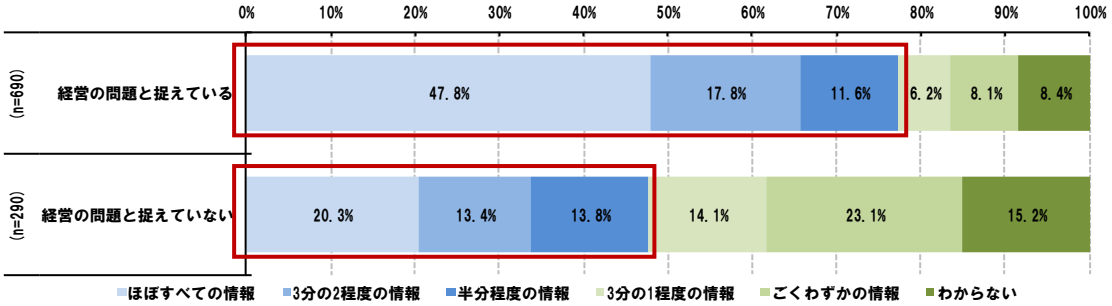

図 4.4-2　営業秘密として管理するべき情報を実際に管理できている割合の比較
（問 25×問 26）

営業秘密管理に取り組む前提としての情報の区分け等について、営業秘密管理を経営に直結する問題として捉えている企業と、捉えていない企業との間で実施状況に差が見られたが、具体的な対策の実施状況についても両者の間に差が見られる。

例えば、営業秘密へのアクセスを物理的に制御する対策の実施状況については、営業秘密管理を経営に直結する問題と捉えている企業のうち 47.9%が「営業秘密を一般情報とは分離して保管するようにしている」と回答しており、また 52.7%が「営業秘密を破棄する際には復元が不可能な方法で実施」と回答している。一方で営業秘密管理を経営に直結する問題として捉えていない企業では、それぞれ 19.1%、30.9%しか実施できていない。また、「営業秘密が保管されている場所に対する入室制限を設けている」という対策についても、両者の間に差が見られる（図 4.4-3）。

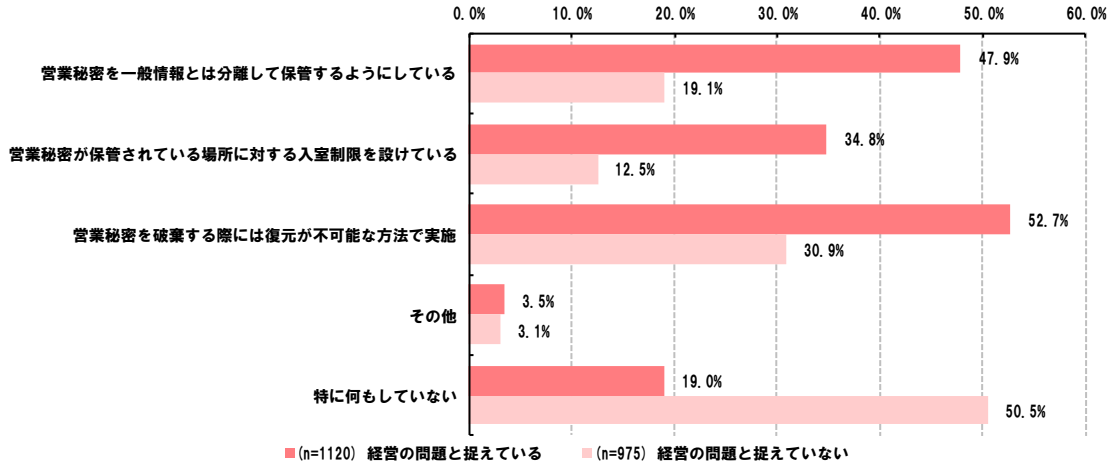

図 4.4-3　営業秘密へのアクセスを物理的に制御する対策の実施状況の比較（問 31×問 26）

また、営業秘密へのアクセスをシステム的に制御する対策の実施状況についても両者の間に差が見られる。例えば、「PC 等の情報端末にはアンチウイルスソフト導入している」「ファイアーウォール等を導入している」といった基本的な取組については、営業秘密管理を経営の問題として捉えている企業のうち、それぞれ 75.3%、67.6%が実施できているが、営業秘密管理を経営の問題として捉えていない企業では 45.6%、38.6%という低い実施率となっている。加えて、営業秘密管理を経営に直結する問題として捉えている企業では、前述の基本的な取組だけでなく「営業秘密の保存領域にはアクセス権を設定している」といった対策についても 60.9%の企業が実施できているが、営業秘密管理を経営に直結する問題として捉えていない企業では、27.4%の企業でしか実施できておらず、営業秘密管理の捉え方の違いによって、具体的な取組の実施状況にも差が見られる傾向となった（図 4.4-4）。

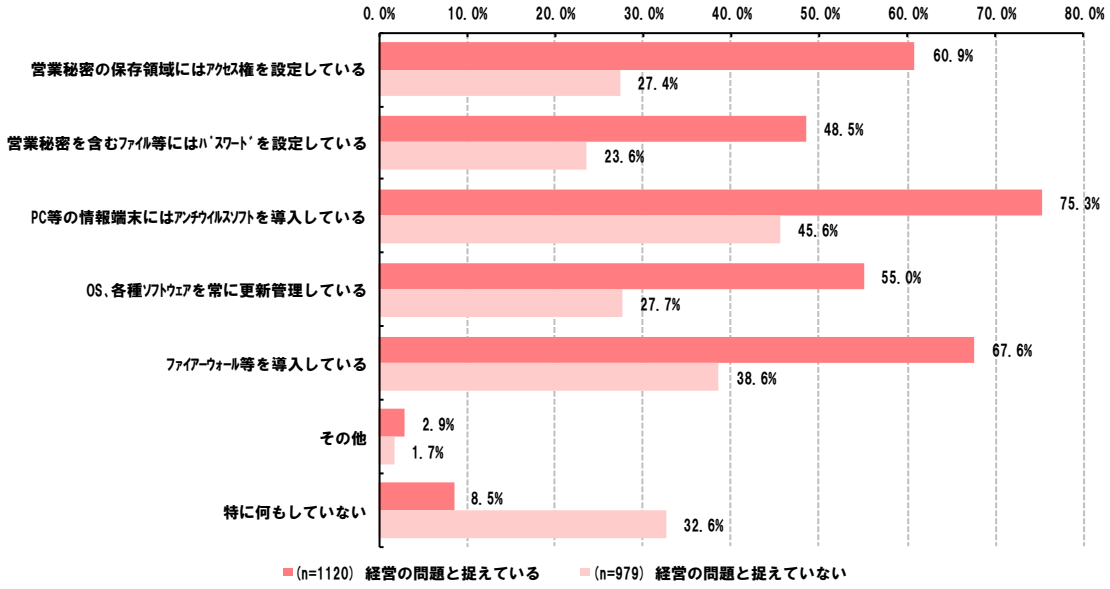

図 4.4-4　営業秘密へのアクセスをシステム的に制御する対策の実施状況の比較
（問 32×問 26）

営業秘密に対する従業員の認識を向上させるための対策として、秘密保持契約の締結が有効な手段の一つとなっているが、営業秘密管理を経営に直結する問題として捉えている企業においては、59.9%が従業員との間で秘密保持契約を締結しているが、営業秘密管理を経営に直結する問題として捉えていない企業では 30.9%でしか契約が締結されていない（図 4.4-5）。

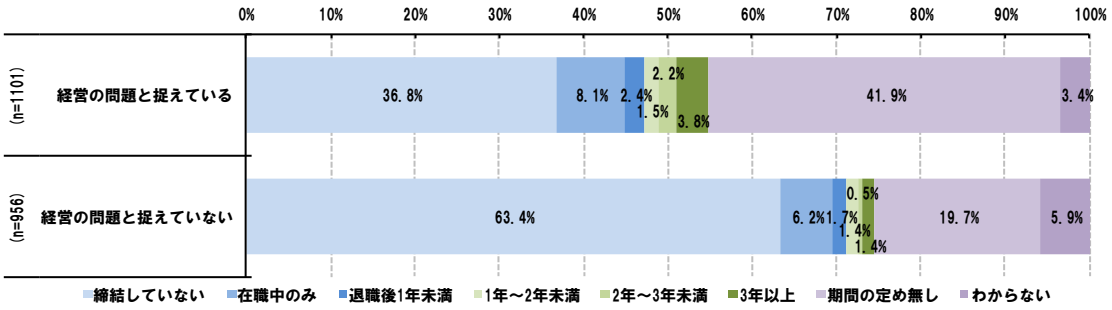

図 4.4-5　従業員との間での秘密保持契約締結状況の比較（問 37×問 26）

対象者別の対策についても両者の間で取組状況に差が見られるところであるが、例えば退職者向けの対策については、営業秘密管理を経営に直結する問題として捉えている企業では「速やかに会社貸与の記録媒体等を返却させる」という取組については、34.8%が実施できているのに対し、営業秘密管理を経営に直結する問題として捉えていない企業では、実施している割合が 15.9%に留まっている。また、割合としては低いものの「退職者の動向を把握する」「既存の対策をより厳格化する」という対策について、営業秘密管理を経営に直結する問題として捉えている企業の一部は取り組んでいる一方で、営業秘密管理を経営に直結する問題として捉えていない企業ではほとんどが取り組んでいない（図 4.4-6）。

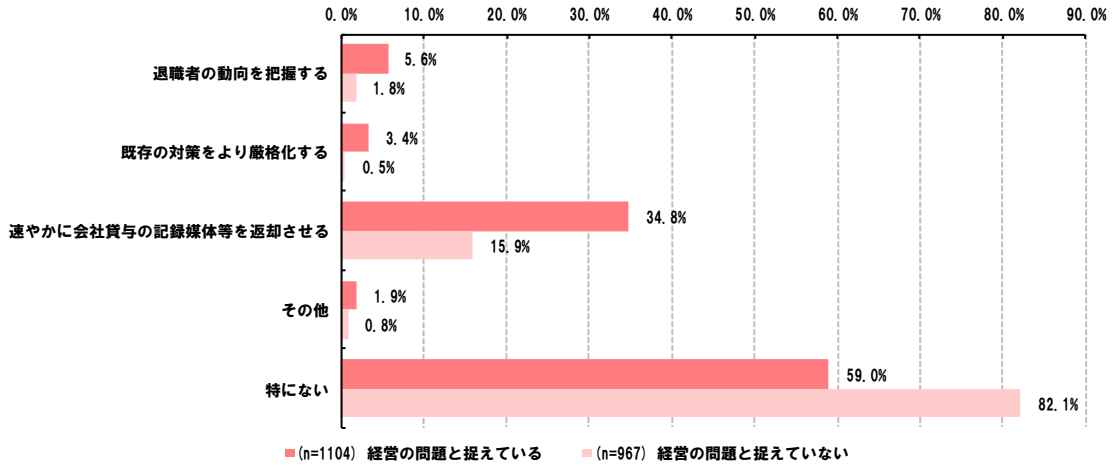

図 4.4-6　退職者向けの対策の実施状況の比較（問 43×問 26）

上述の通り、具体的な対策の実施状況については、営業秘密管理を経営に直結する問題として捉えている企業と、捉えていない企業との間で総じて差が見られる傾向となった。

営業秘密管理に取り組むにあたっては、具体的な漏えい防止対策を実施することが重要であると同時に、漏えいの予兆等を検知する取組も重要である。こうした営業秘密の漏えいに気づけるような活動の実施状況についても、両者の間で差が見られる。営業秘密管理を経営に直結する問題として捉えている企業においては、67.2%の企業でそうした活動が実施されている（うち、54.9%の企業では、そうした活動を実施していることを従業員に周知している）が、一方で営業秘密管理を経営に直結する問題として捉えていない企業では 31.9%の企業でしか実施されていない（図 4.4-7）。

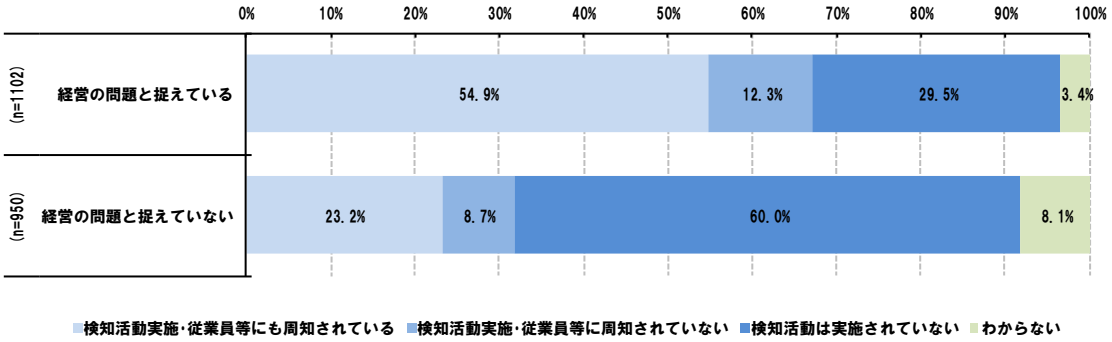

図 4.4-7　漏えいに気づけるような活動の実施状況の比較（問 9×問 26）

漏えいに気づけるような活動の実施と同様に、日頃から情報セキュリティリスクへの対策を万全にしておくことが望ましいと思われるが、営業秘密管理を経営に直結する問題として捉えている企業では、こうしたリスクへの取組として 41.0%が「対応・報告の手順を取り決めている」と回答しており、有事の際に備えた対策を検討できている一方で、営業秘密管理を経営に直結する問題として捉えていない企業においては、こうした対策を実施できている企業は 15.8%に留まっている（図 4.4-8）。

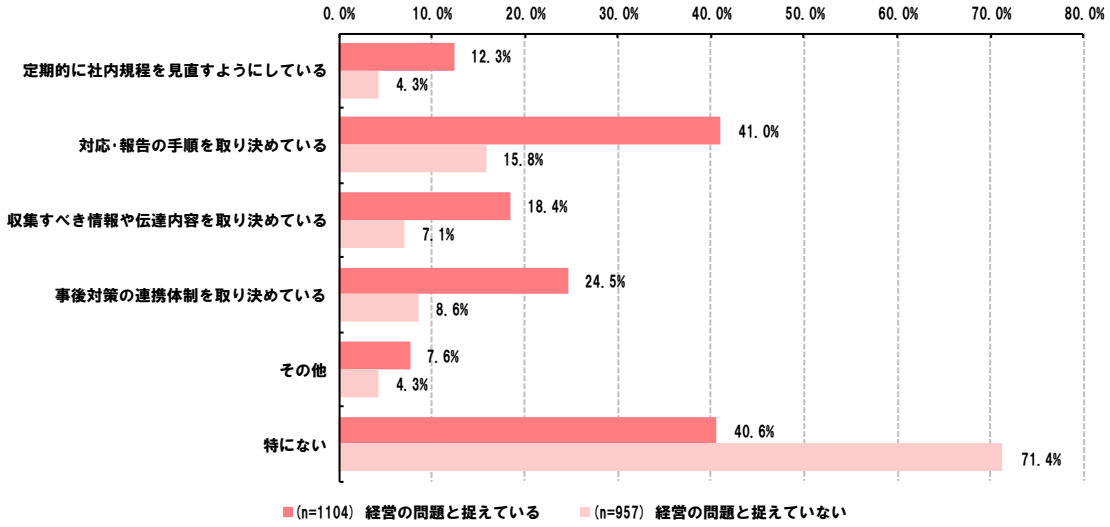

図 4.4-8　情報セキュリティリスクに関する対策の実施状況の比較（問 57×問 26）

4.5. 検知活動の重要性

昨今、情報漏えいの手口が多様化・高度化しており、どれだけ入念に漏えい対策を実施していても、漏えいを防げないケースが発生してしまう可能性がある。漏えいを未然に防ぐための検知活動を十分に実施することは、抑止力の観点からも重要であることはもちろんのことであるが、同時に漏えいが発生した際の対応を迅速に実施できるようにしておくと言う意味でも有効であり、重要なことである[46]。

秘密情報の保護ハンドブックによれば、「漏えいの兆候を事前に把握できるようにしておくこと」「漏えいが起こった際の初動対応を迅速に実施できるようにしておくこと」「被害回復のための責任追及を徹底的に実施すること」「漏えいの事実を裏付ける証拠を積み上げること（証拠の保全・収集）」が漏えい事案への対応として重要なポイントであるとされている。

検知活動を実施している企業と、実施していない企業で、営業秘密漏えい対策の実施状況を比較すると、全体的に検知活動を実施している企業の方が、体制の整備や個別の対策への取組が進んでいる傾向があることが見受けられる。例えば、検知活動を実施している企業では、検知活動を実施していない企業と比べて情報セキュリティリスクへの対策を事前に検討する体制が整備されていることが窺える。具体的な対策としては、例えば「対応・報告の手順を取り決めている」については、検知活動を実施（従業員等への周知も実施）している企業のうち 53.9%で実施されているのに対し、検知活動を実施していない企業においては、8.9%の企業でしか実施されていないという状況になっている。また、「事後対策の連携体制を取り決めている」についても、検知活動を実施（従業員等への周知も実施）している企業では 32.1%が実施しており、営業秘密管理に関する活動を行う上で、有事の際を想定した体制も整備し、組織的に取り組んでいる企業が一定程度いることが窺える（図 4.5-1）。

[46] 2015 年の不正競争防止法の改正に伴い、新法では営業秘密侵害について「未遂」に対する処罰が新たに規定されることになった。例えば、齋藤憲道、岡村久道「営業秘密を守るには」（NBL、No.1069）の中でも、未遂行為の処罰の導入によって、これまで営業秘密に対して不正にアクセスしたことを確認できても、その持出し等を立証できずに起訴できなかったような事案に対して、今後有罪にすることができる可能性があると指摘されている。こうした観点からも、営業秘密に対するアクセスのログを取得しておくこと等の検知活動を行うことは重要であると考えられる。

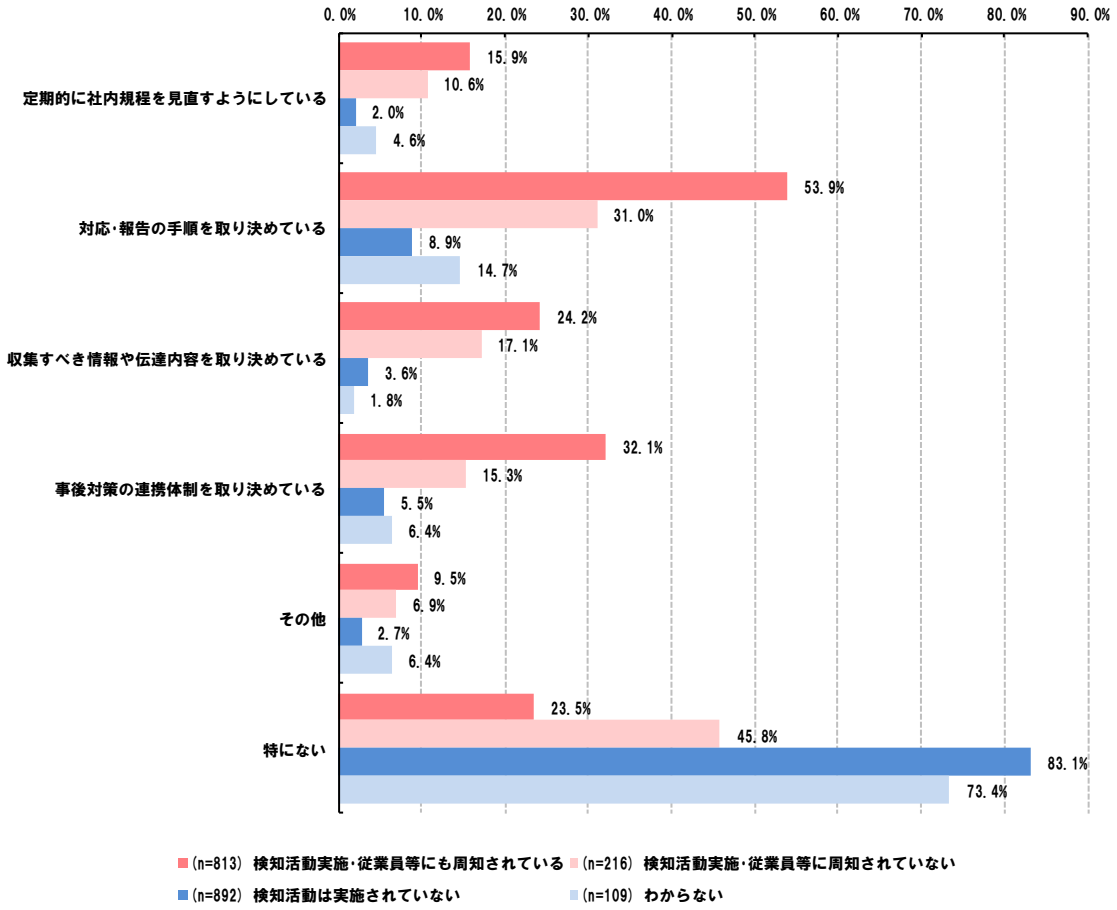

図 4.5-1　情報セキュリティリスクへの対策状況の比較（問 57×問 9）

また、検知活動を実施（従業員等への周知も実施）している企業では、38.9%が営業秘密管理ルールを全社で徹底して運用している一方で、その他の企業では運用できている割合が 15%にも満たない（図 4.5-2）。こうした点からも、検知活動を実施（従業員等への周知も実施）している企業は営業秘密管理の体制を整備し、組織的に取り組んでいることが窺える。

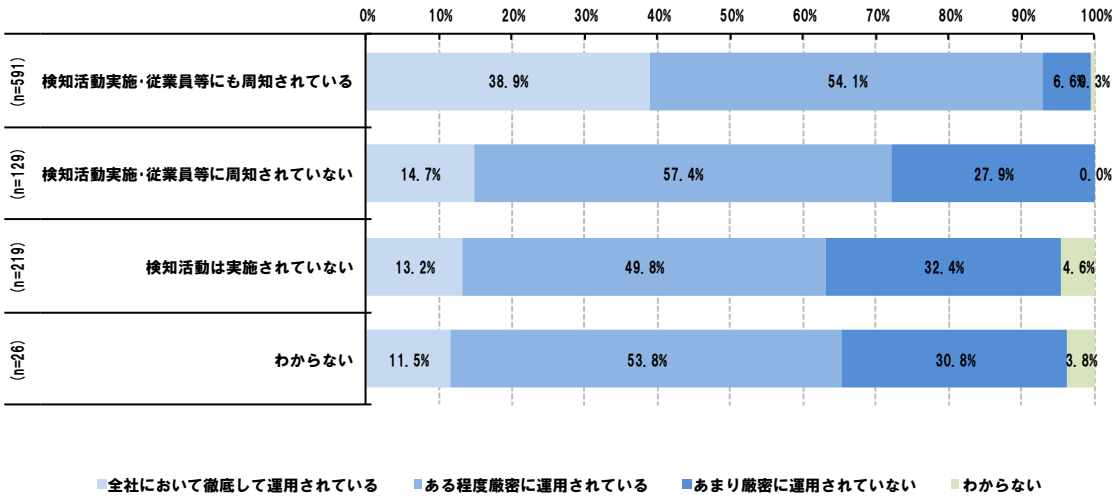

図 4.5-2　営業秘密管理ルールの運用状況の比較（問 23×問 9）

個別具体的な対策の実施状況についても、やはり検知活動を実施（従業員等への周知も実施）している企業がその他の企業と比べて積極的に取り組んでいる傾向がある。例えば営業秘密の持出しを物理的に制御することを目的とした取組については、検知活動を実施（従業員等への周知も実施）している企業のうち、63.1%が「USB メモリや DVD 等の持ち込み・持ち出しを禁止している」を実施できているのに対し、検知活動を実施していない企業では 16.8%しか実施できていない（図 4.5-3）。

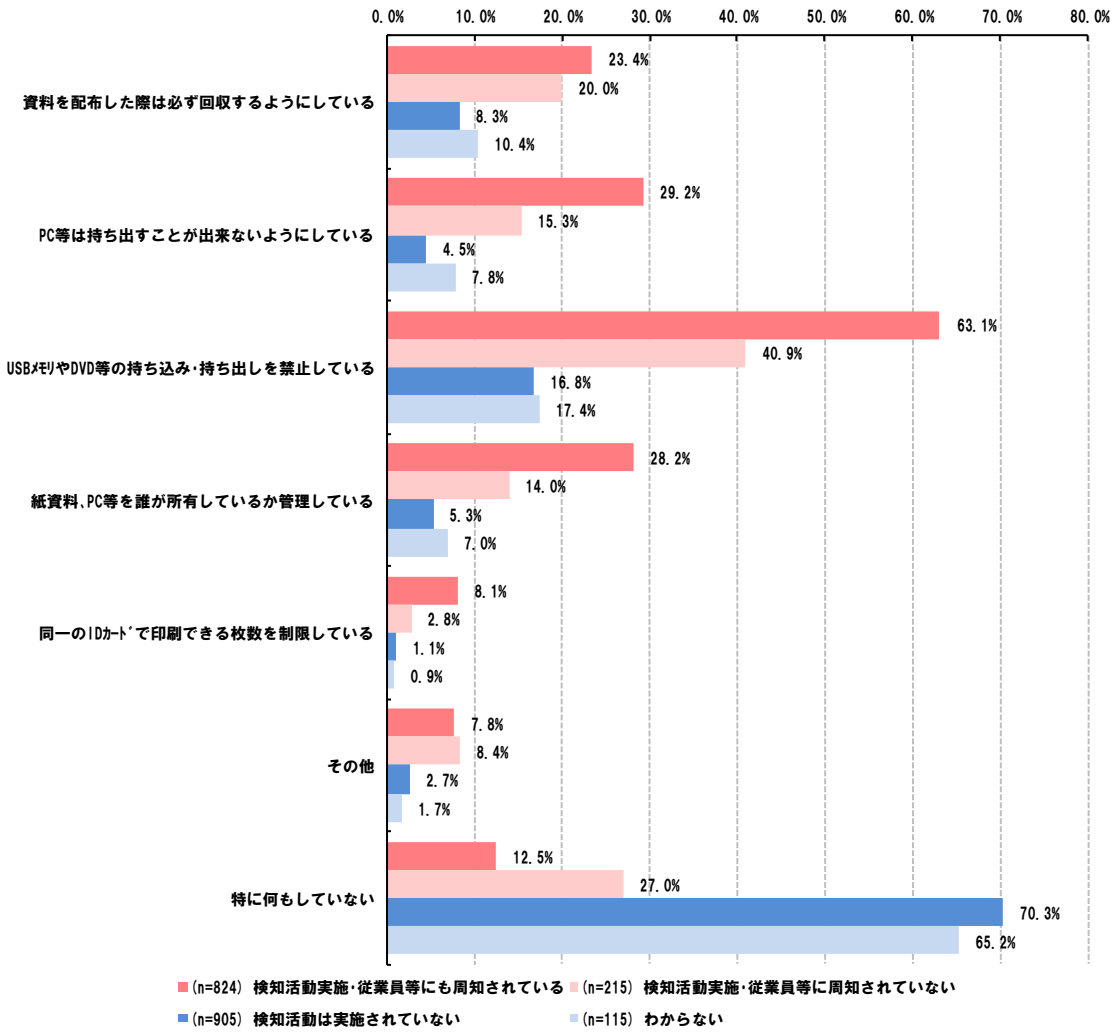

図 4.5-3　営業秘密の持出しを物理的制御するための対策の比較（問 33×問 9）

また、営業秘密が漏えいしにくい環境をつくるためのシステム的な対策についても、検知活動を実施（従業員等への周知も実施）している企業においては、例えば「情報システムのログを記録・保管している」について、74.4%で実施できているのに対し、検知活動を実施していない企業では 14.2%でしか実施できていない。加えて、「不自然なアクセスは上司等に通知される」「不自然なアクセスは本人に警告される」「外部送信のメールのチェック体制が整っている」について、検知活動を実施（従業員等への周知も実施）している企業ではいずれの対策も 2 割程度で実施されているが、検知活動を実施していない企業ではいずれも 2～3%であり、ほとんど実施されていない（図 4.5-4）。こうした対策は、検知活動を実施することによって有効に機能する対策であるため、検知活動の実施有無によって取組状況に大きな差があることが見受けられる。

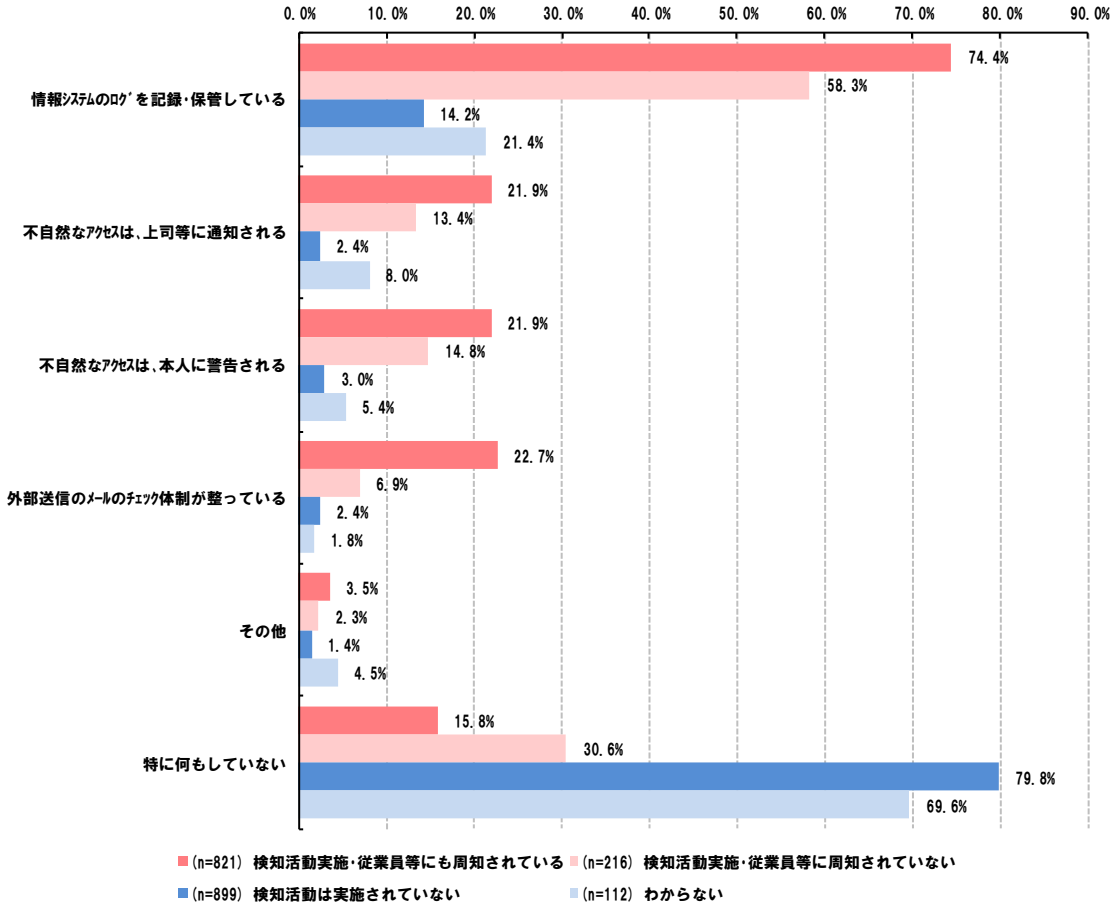

図 4.5-4　営業秘密が漏えいしにくい環境をつくるためのシステム的な対策の比較（問 36×問 9）

対象者別の対策として、例えば従業員向けの特有の対策についても、検知活動を実施（従業員等への周知も実施）している企業では「研修実施等で取扱のルールを社内で周知徹底している」について、65.1%で実施されているのに対し、検知活動を実施していない企業では 11.1%という状況であり、取組状況に大きな差があることが見受けられる。また、「部署や役職等に応じて入室できる部屋を制御」についても、検知活動を実施（従業員等への周知も実施）している企業では 35.6%で実施できているのに対し、検知活動を実施していない企業では 8.0%である（図 4.5-5）。

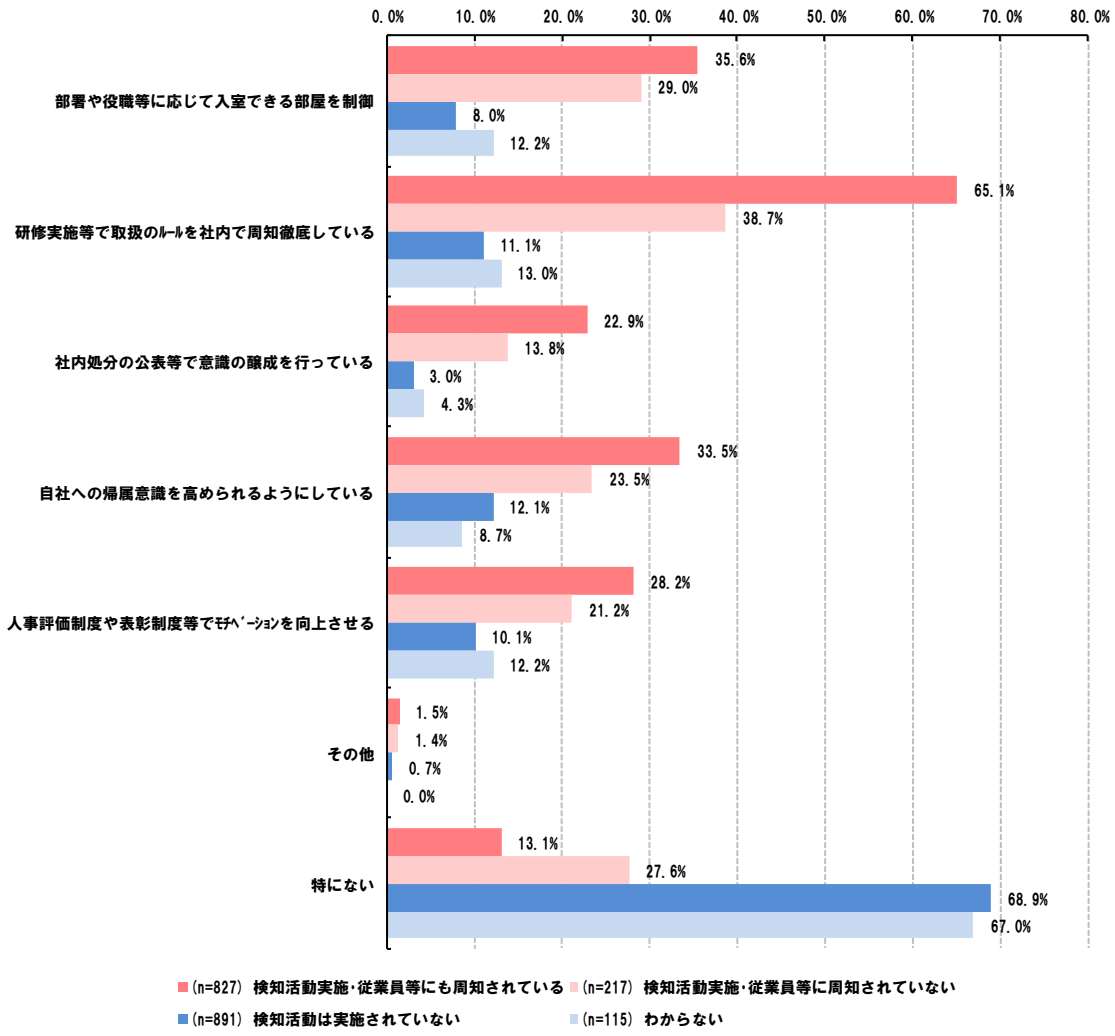

図 4.5-5　従業員等に対する特有の対策の比較（問 42×問 9）

検知活動を実施（従業員等への周知も実施）しており、かつ過去５年間で営業秘密の漏えいが発生していない企業では、漏えいが発生していない要因について相対的に高い割合の企業が「データ等の暗号化・アクセス制限を行ったこと（42.2%）」「データ等の持ち出し制限を行ったこと（53.0%）」「秘密保持契約を締結していること（36.0%）」「情報の管理方針等を整備していること（48.8%）」「教育・管理方針等の周知徹底を行っていること（34.0%）」を挙げている。このうち、特に「データ等の暗号化・アクセス制限を行ったこと」「データ等の持ち出し制限を行ったこと」「情報の管理方針を整備していること」については検知活動を実施していない企業と３割以上の差があり、意識に差が出やすい対策であると思われる（図 4.5-6）。

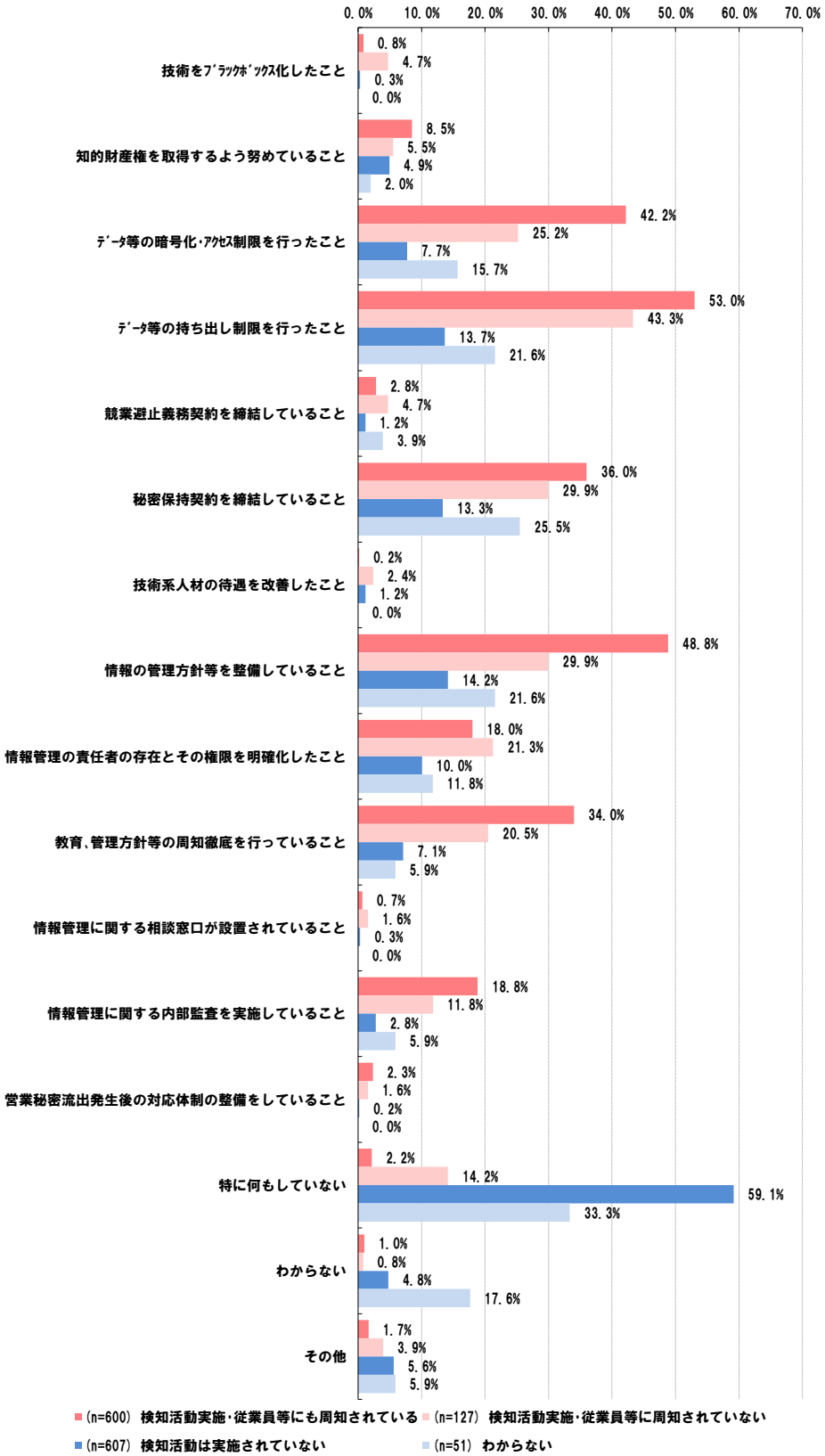

図 4.5-6　営業秘密の漏えいが発生していない要因の比較（問 18×問 9）

検知活動を実施（従業員等への周知も実施）しており、かつ過去５年間で営業秘密の漏えいが発生した企業においては、侵害を行った者への対応として、60.3%が「事実関係の調査を行った」と回答しているのに対し、検知活動を実施していない企業では 15.0%でしか実施されていない。検知活動を実施していない企業では、こうした調査を行えるだけの情報も不足しているため、実施が難しいことに起因しているとも考えられる。また、「懲戒処分とした」については、検知活動を実施（従業員等への周知も実施）している企業のうち 25.4%が実施している。加えて、割合こそ高くないものの、「警察への相談・届出を行った」「警告文書を送付した」「民事訴訟を提起した」「刑事告訴した」「懲戒解雇とした」といった対応についても、検知活動を実施していない企業と比較すると、検知活動を実施（従業員等への周知も実施）している企業の方が対応できている割合が高く、こうしたことからも、日頃の検知活動を行うことで営業秘密の漏えいが発生した際に、漏えいによる被害回復のための徹底的な責任追及に資する具体的なアクションにまでつなげられる可能性が高まることを示唆している（図 4.5-7）。

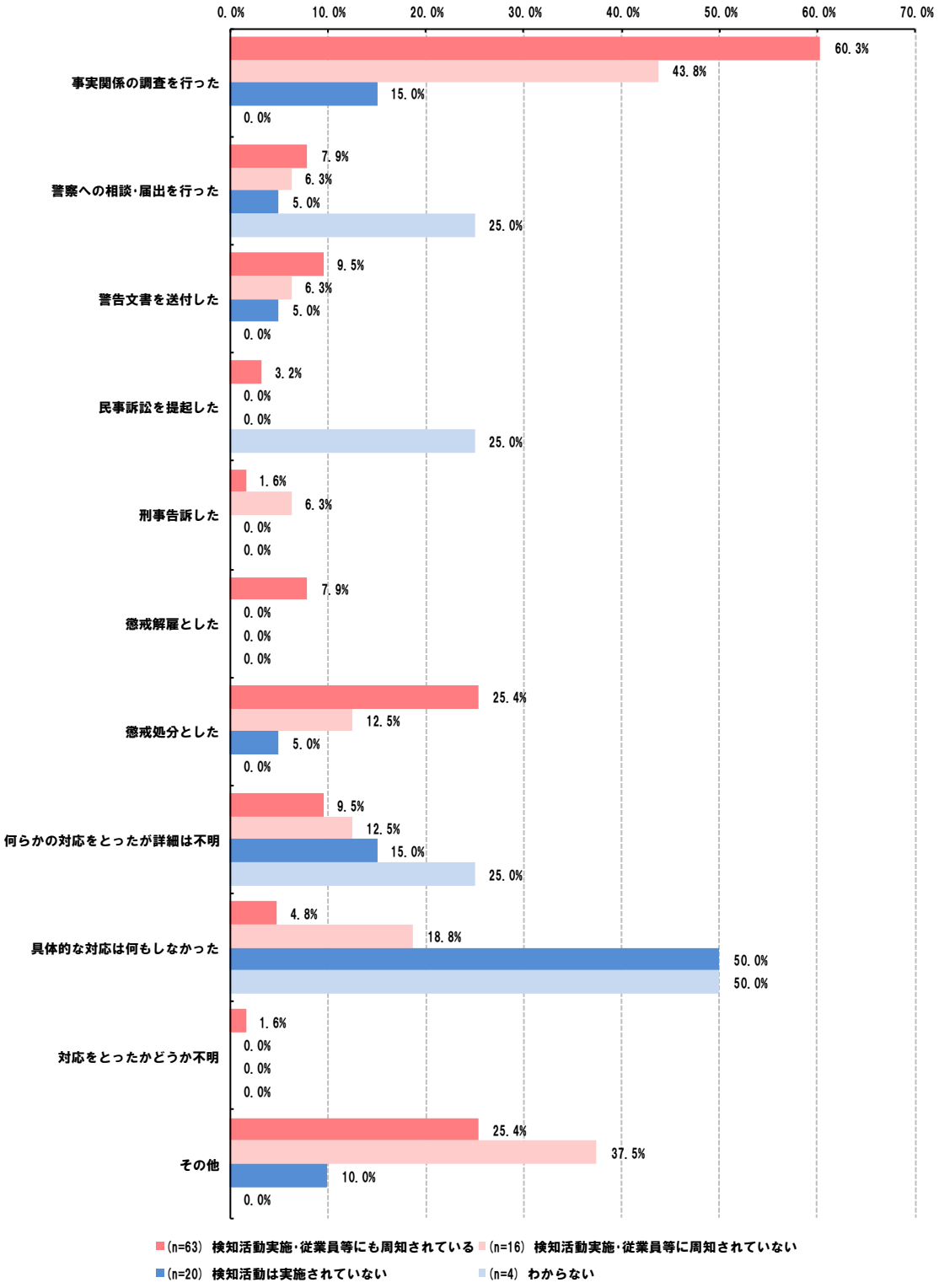

図 4.5-7　営業秘密の侵害者への対応の比較（問 17×問 9）