

企業における営業秘密管理に関する実態調査
概要説明資料

平成29年3月17日

独立行政法人 情報処理推進機構

技術本部 セキュリティセンター

情報セキュリティ分析ラボラトリー

目次

1. 背景および目的
2. 調査概要
3. アンケート調査・判例調査方法
4. 営業秘密を取り巻く環境の変化の調査
5. 営業秘密の漏えい実態
6. 営業秘密の漏えいを検知する活動
7. 営業秘密の漏えい対策の取組状況
8. 漏えいを経験した企業の認識
9. 営業秘密管理を経営の問題と捉えている企業の取組
10. 判例調査
11. 調査結果まとめ

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、営業秘密漏えい事案は後を絶たず、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。

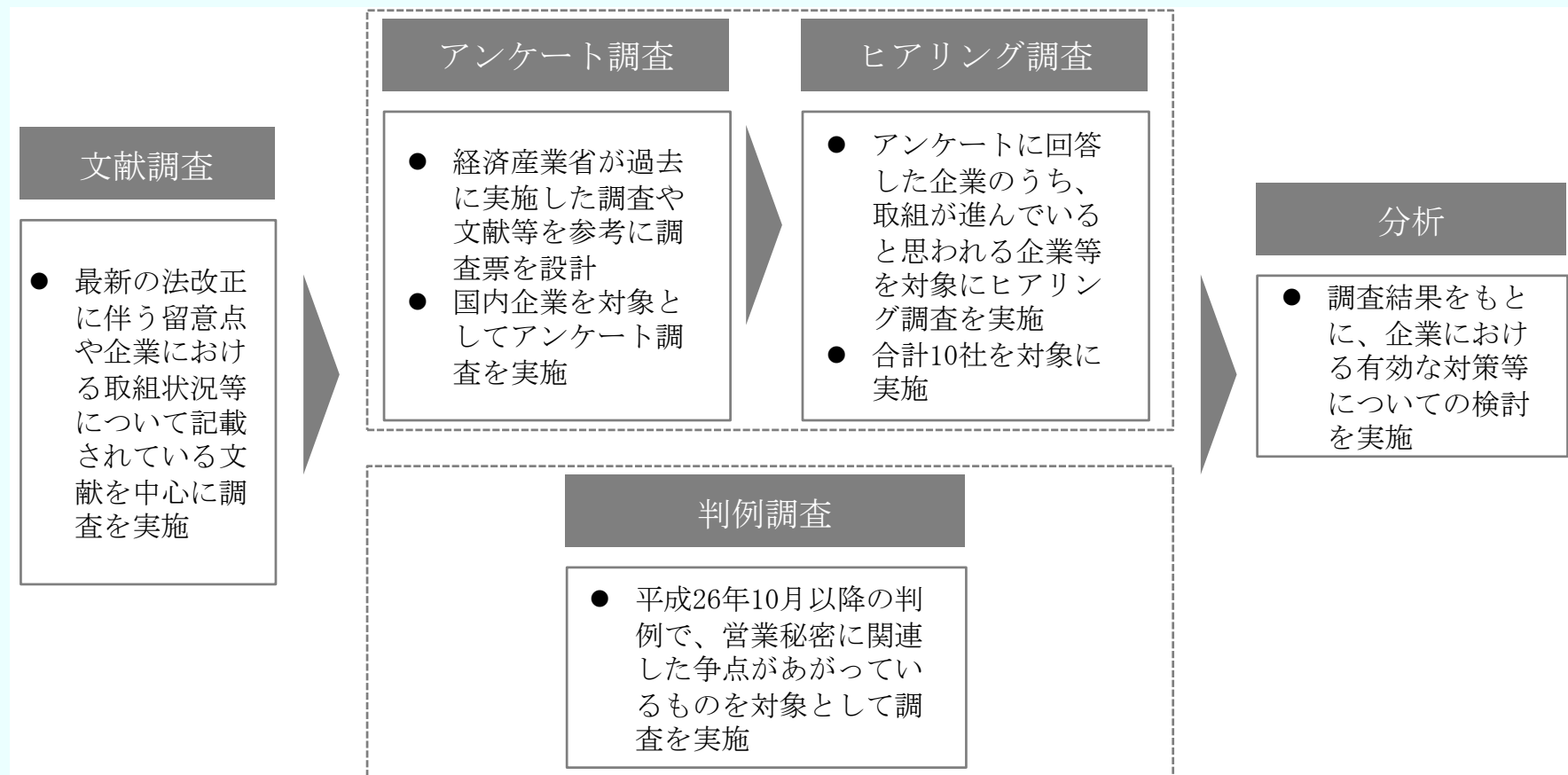
このような背景を受け、企業に対して**営業秘密の保護強化に向けた情報セキュリティ対策等の実施**を促す必要がある。営業秘密の漏えいを防ぐための対策については、経済産業省が平成28年2月に公表した「秘密情報の保護ハンドブック～企業価値向上に向けて～」の中で、情報の分類の考え方や、漏えいルート等に応じた対策の例、他社の営業秘密の侵害を防ぐための対策例、漏えい事案への対応例等が紹介されており、営業秘密管理の手段や重要性を周知してきたところである。

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、企業において必ずしも有用な対策が施されているとはいいがたく、引き続き営業秘密管理の重要性や漏えい対策、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、経済産業省が2012年度に「人材を通じた技術流出に関する調査研究」（以下、「過年度調査」と記載）で調査している。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、インタビュー調査、及び判例調査を通じて実態の把握を行った。**

2. 調査概要

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、その結果を報告書として取りまとめた。



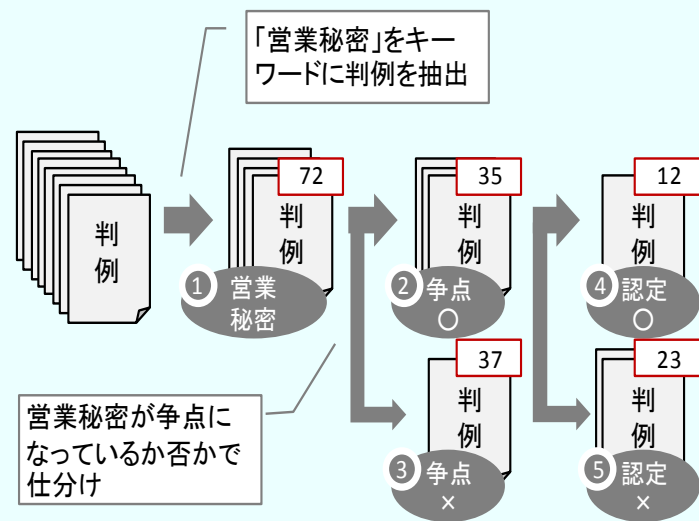
3. アンケート調査・判例調査方法

アンケート調査		判例調査	
調査対象	信用調査会社のデータベースから抽出した12,000社	抽出・分析方法	<ul style="list-style-type: none"> 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（平成26年10月1日～平成28年8月23日までの判例が対象） 抽出された判例を、営業秘密が争点になっているものといないもので選別 選別後、営業秘密としての認定有無等について比較分析
回答企業	2,175社		

回答企業の内訳

	製造業	非製造業
従業員301名以上	449社	599社
従業員300名以下	433社	670社

※業種または従業員数が無回答の24社については表に含まれていない。
 ※従業員301名以上の企業については、以降「大規模企業」と記載する。
 ※従業員300名以下の企業については、以降「中小規模企業」と記載する。
 ※集計にあたっては、「無回答」を母数から除いている。
 ※業種または従業員数について無回答の場合、全業種・全規模の集計結果には含まれるが、業種・規模別の集計結果には含まれない。



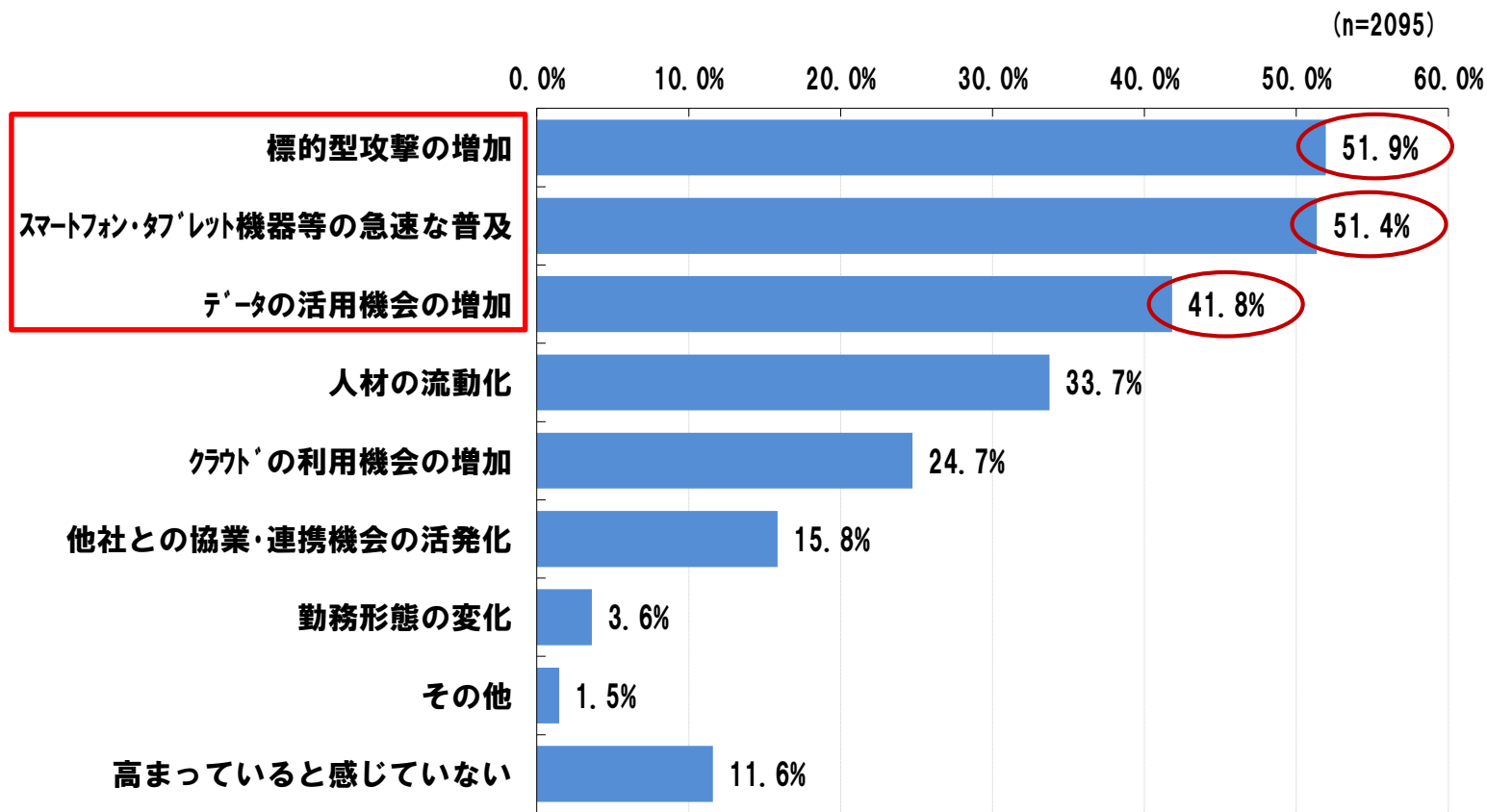
72 : 該当する判例の件数

4. 営業秘密を取り巻く環境の変化の調査

-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（全業種・全規模）

- 直近 5 年間程度におけ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
 全体的には「**標的型攻撃の増加（51.9%）**」の割合が最も高い。
 次いで「**スマートフォン・タブレット機器等の急速な普及（51.4%）**」、「**データの活用機会の増加（41.8%）**」。

<問19>「漏えいリスクの高まりを感じる社会動向の変化」【全業種・全規模】

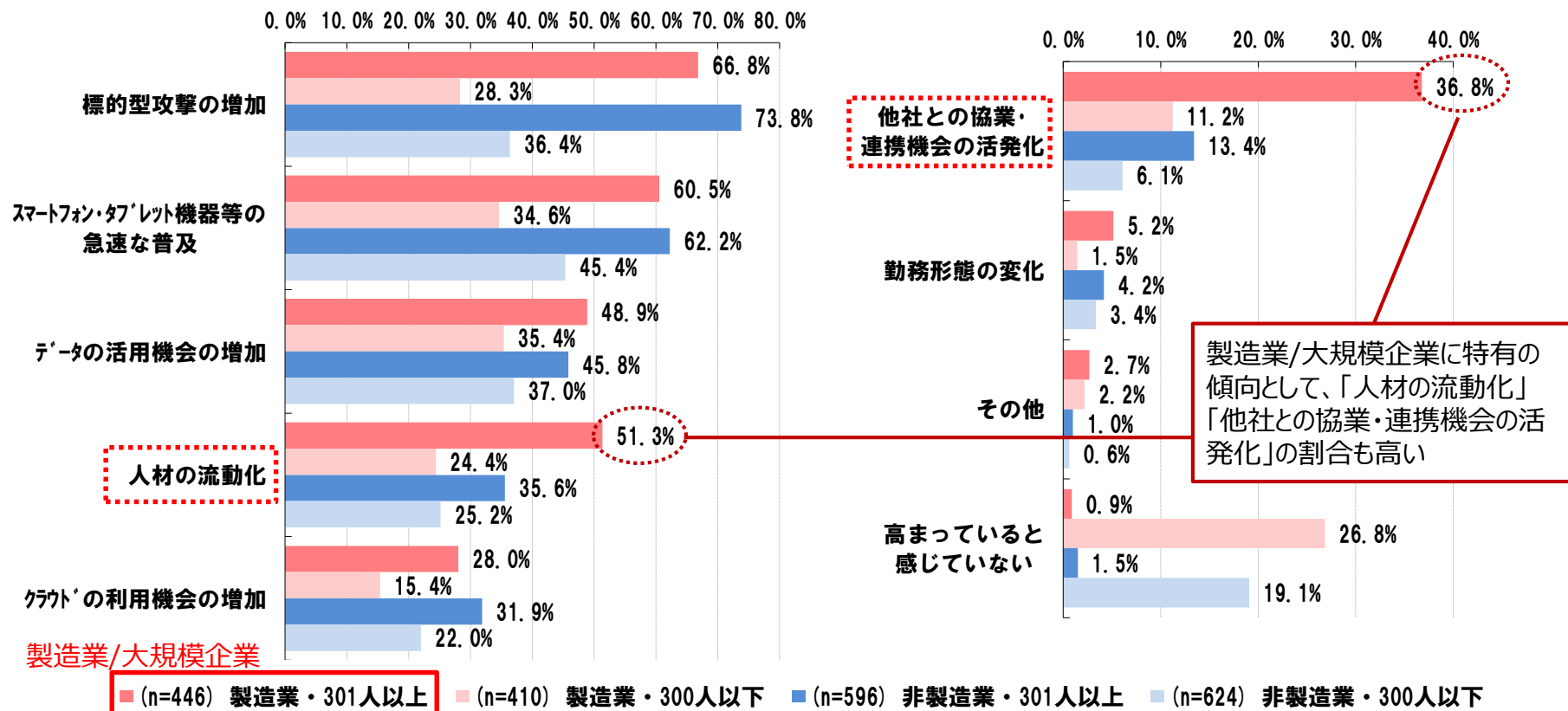


4. 営業秘密を取り巻く環境の変化の調査

-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（業種・規模別）

- 直近5年間程度におけ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
製造業/大規模企業においては、「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」、「データの活用機会の増加」（全業種・全規模でのTOP3）だけでなく、
「人材の流動化」「他社との協業・連携機会の活発化」と回答した企業の割合も高い。

<問19>「営業秘密の漏えいリスクの高まりを感じる社会的動向の変化」【業種・規模別】

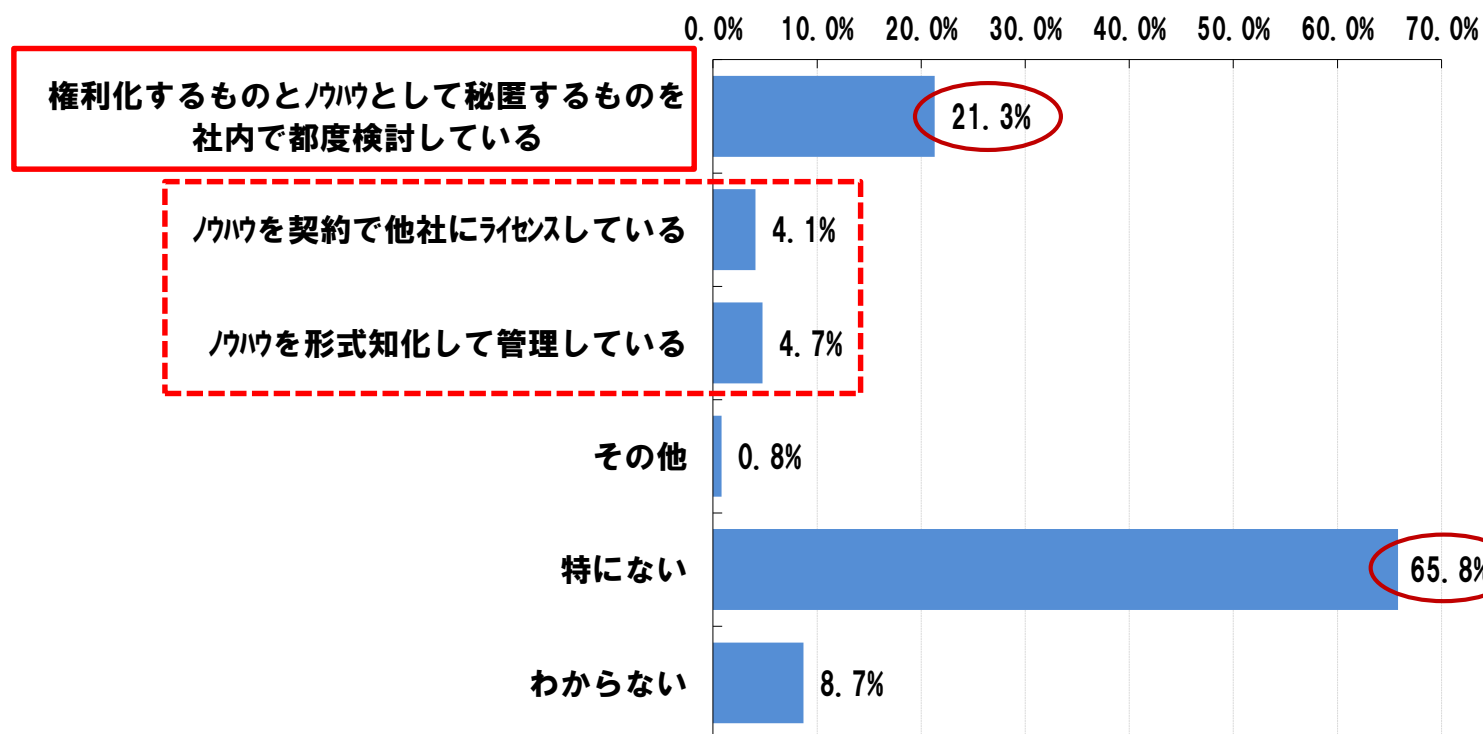


4. 営業秘密を取り巻く環境の変化の調査 -自組織のノウハウに対する考え方（全業種・全規模）

- 「オープン&クローズ戦略」や「オープンイノベーション」に係る環境変化
- ノウハウの管理や活用に関して実施している取組
全体では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している」と回答。
- 4.1%の企業が「ノウハウを契約で他社にライセンスしている」、4.7%の企業が「ノウハウを形式知化して管理している」と回答。
- 65.8%の企業が「特にない」と回答。

<問27>「ノウハウの管理・活用に関する取組」【全業種・全規模】

(n=2107)

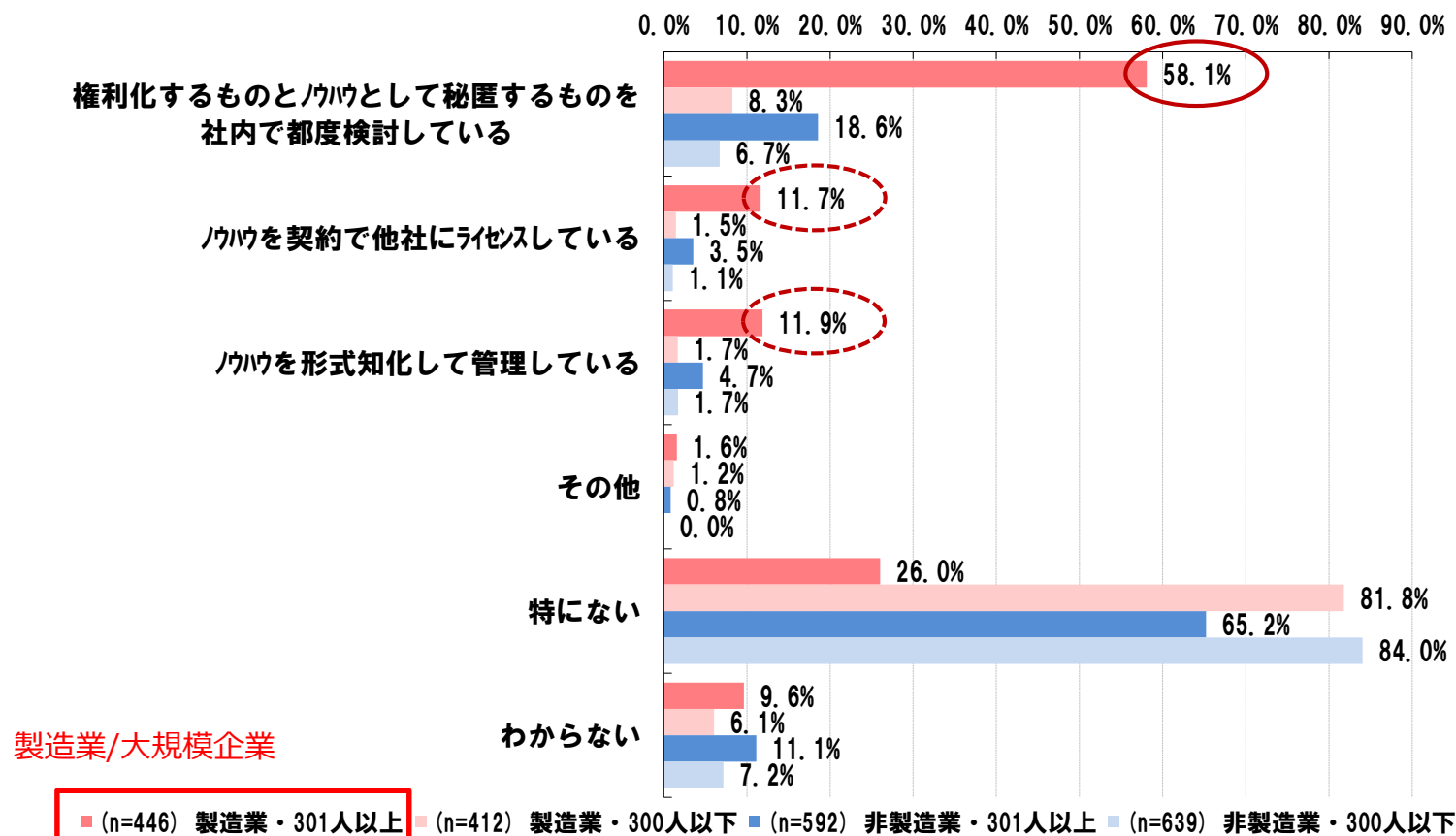


4. 営業秘密を取り巻く環境の変化の調査

-自組織のノウハウに対する考え方（業種・規模別）

- **製造業/大規模企業**：58.1%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している」と回答。
- 製造業/大規模企業のうち、1割程度の企業で「ノウハウを契約で他社にライセンスしている」「ノウハウを形式知化して管理している」といった取組を実施（オープンイノベーションの動き）。

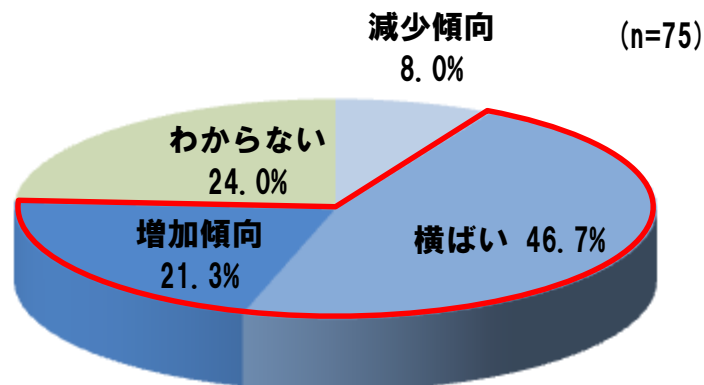
<問27>「ノウハウの管理・活用に関する取組【業種・規模別】



4. 営業秘密を取り巻く環境の変化の調査 -「オープンイノベーション」に係る取組

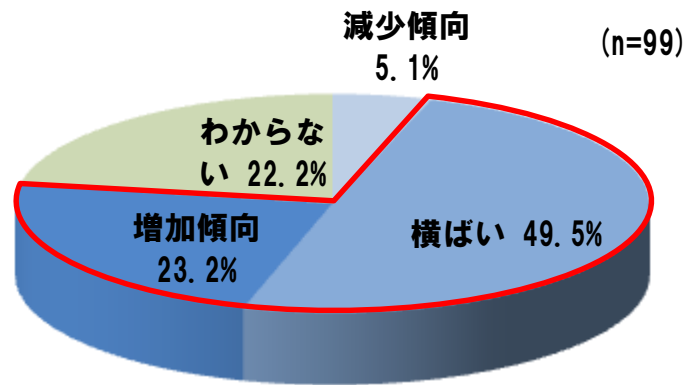
- オープンイノベーション/重要情報の他社との共有傾向の推移
- ノウハウを契約で他社にライセンスしていると回答した企業：
68.0%の企業において、過去5年間におけるライセンスしているノウハウ件数の推移が横ばい・増加傾向。
- ノウハウを形式知化して管理していると回答した企業：
72.7%の企業において、過去5年間における形式知化して管理しているノウハウ件数の推移が横ばい・増加傾向。

<問28>「他社にライセンスしているノウハウ件数の推移
(過去5年間)」【全業種・全規模】



横ばい+増加傾向 = 68.0%

<問28>「形式知化して管理しているノウハウ件数の推移
(過去5年間)」【全業種・全規模】



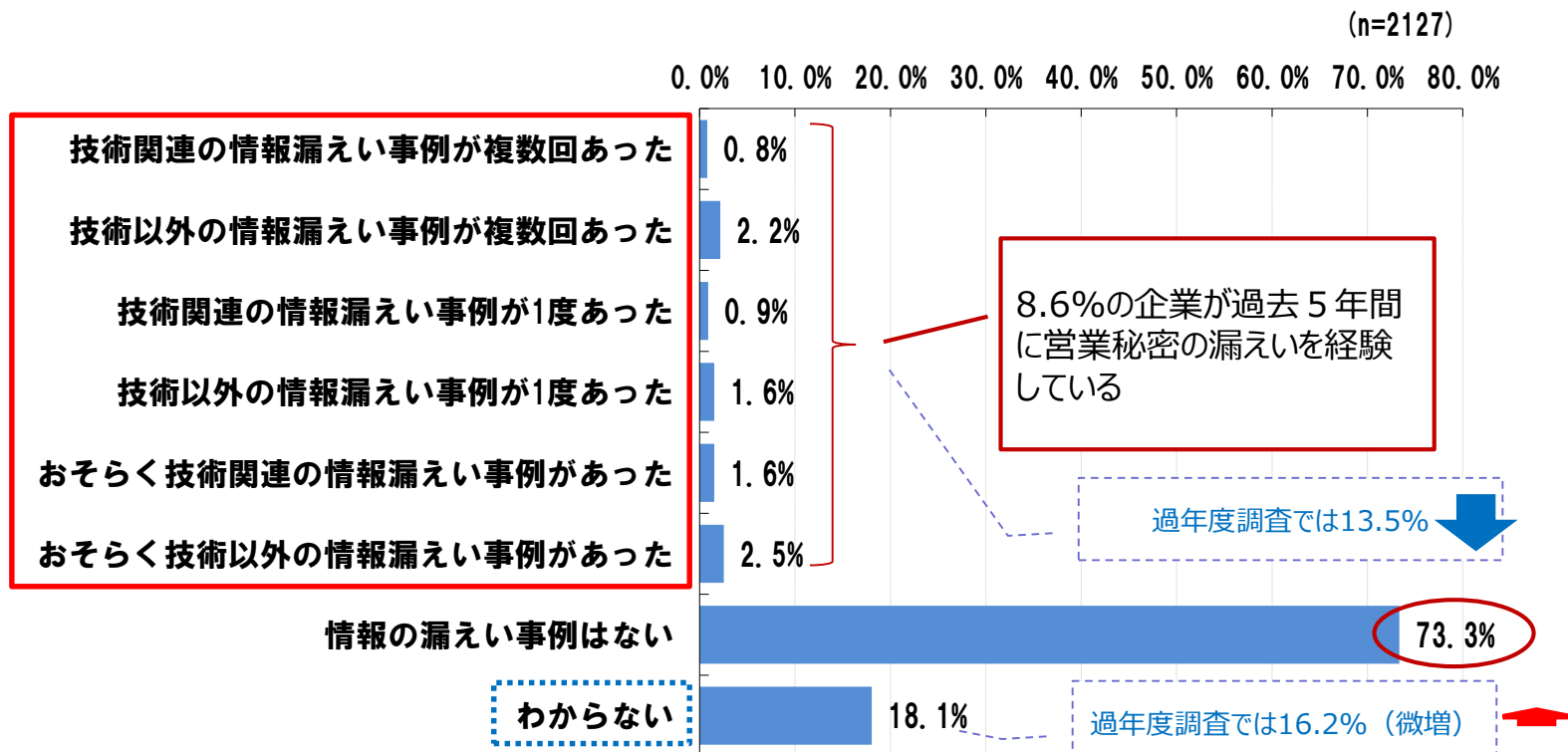
横ばい+増加傾向 = 72.7%

5. 営業秘密の漏えい実態

-過去5年間における営業秘密の漏えい状況（全業種・全規模）

- 過去5年間における営業秘密の漏えい状況について、**73.3%**の企業が「情報の漏えい事例はない」と回答。
- **8.6%**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（**10社に1社近く**）。
うち、5.0%の企業については、「明らかな」情報漏えい事例があったと回答。
- **18.1%**の企業は「**わからない**」と回答しており、漏えいに気付けるような活動等に取り組むことが必要。

<問8>「過去5年間における営業秘密漏えい状況」【全業種・全規模】



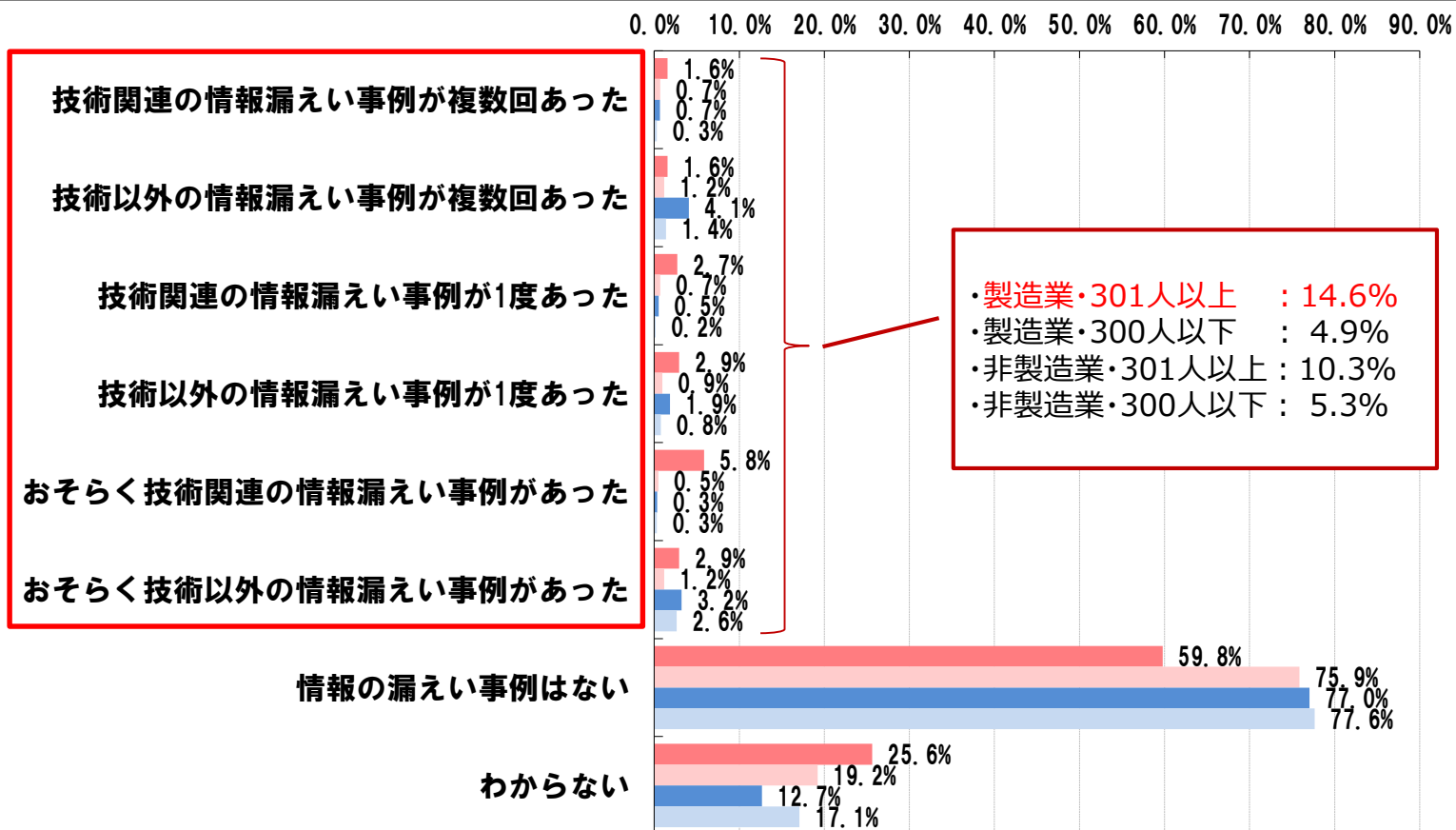
※漏えいを経験している企業の割合 = 全体から、「情報の漏えい事例はない（73.3%）」と「わからない（18.1%）」を除いた割合

5. 営業秘密の漏えい実態

-過去5年間における営業秘密の漏えい状況（業種・規模別）

- **製造業/大規模企業**：14.6%の企業が過去5年間で営業秘密の漏えいを経験している（全体と比較し、比率が高い）。

<問8>「過去5年間における営業秘密漏えい状況」【業種・規模別】



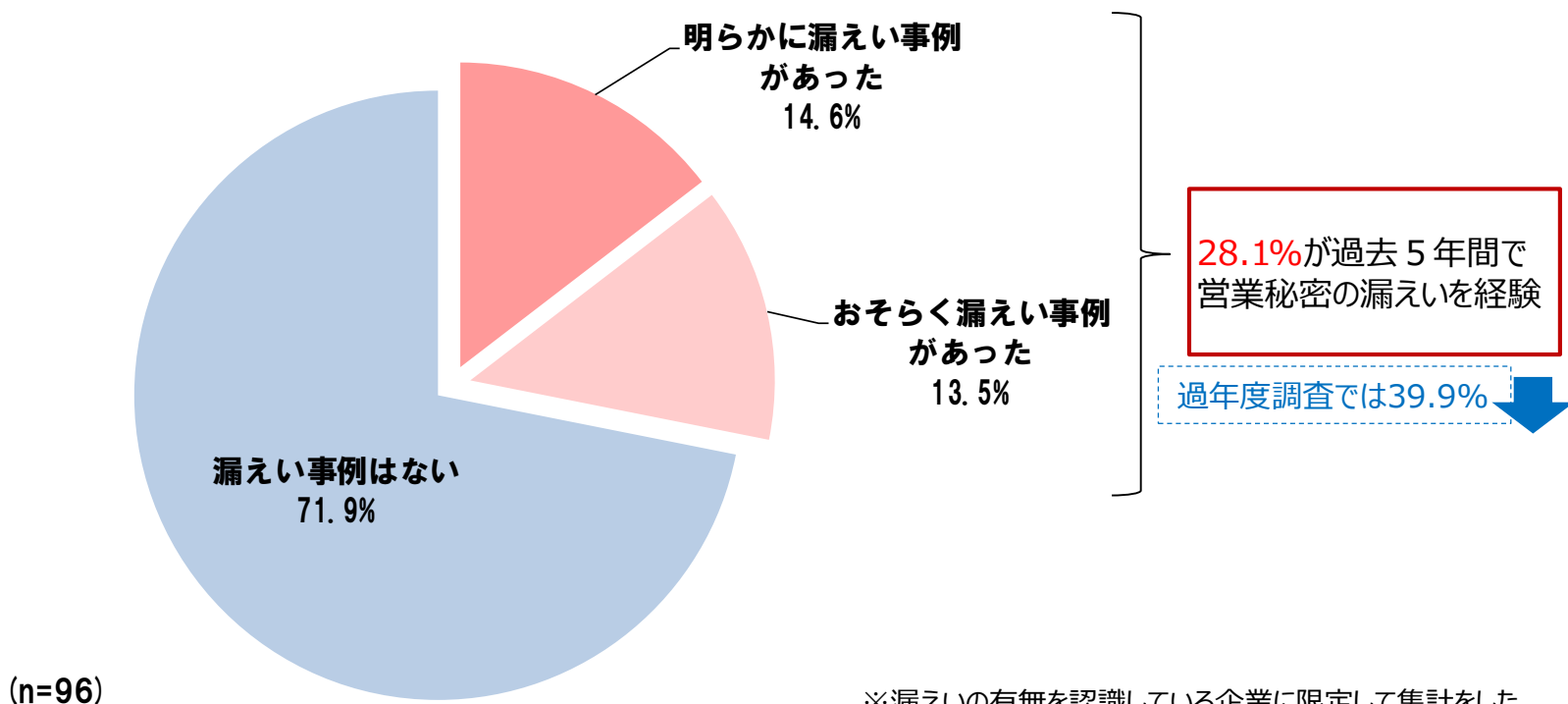
■ (n=445) 製造業・301人以上 ■ (n=427) 製造業・300人以下 ■ (n=592) 非製造業・301人以上 ■ (n=644) 非製造業・300人以下

5. 営業秘密の漏えい実態

-過去5年間における営業秘密の漏えい状況（従業員規模3,001人以上の企業）

- 特に大規模企業での漏えい状況
- 従業員規模3,001人以上の企業：28.1%が過去5年間で営業秘密の漏えいを経験。（過年度調査では39.9%）
- 14.6%の企業において、「明らかに漏えい事例があった」。
- 13.5%の企業について、「おそらく漏えい事例があった」。

<問8>「過去5年間における営業秘密漏えい状況」【従業員規模：3,001人以上】



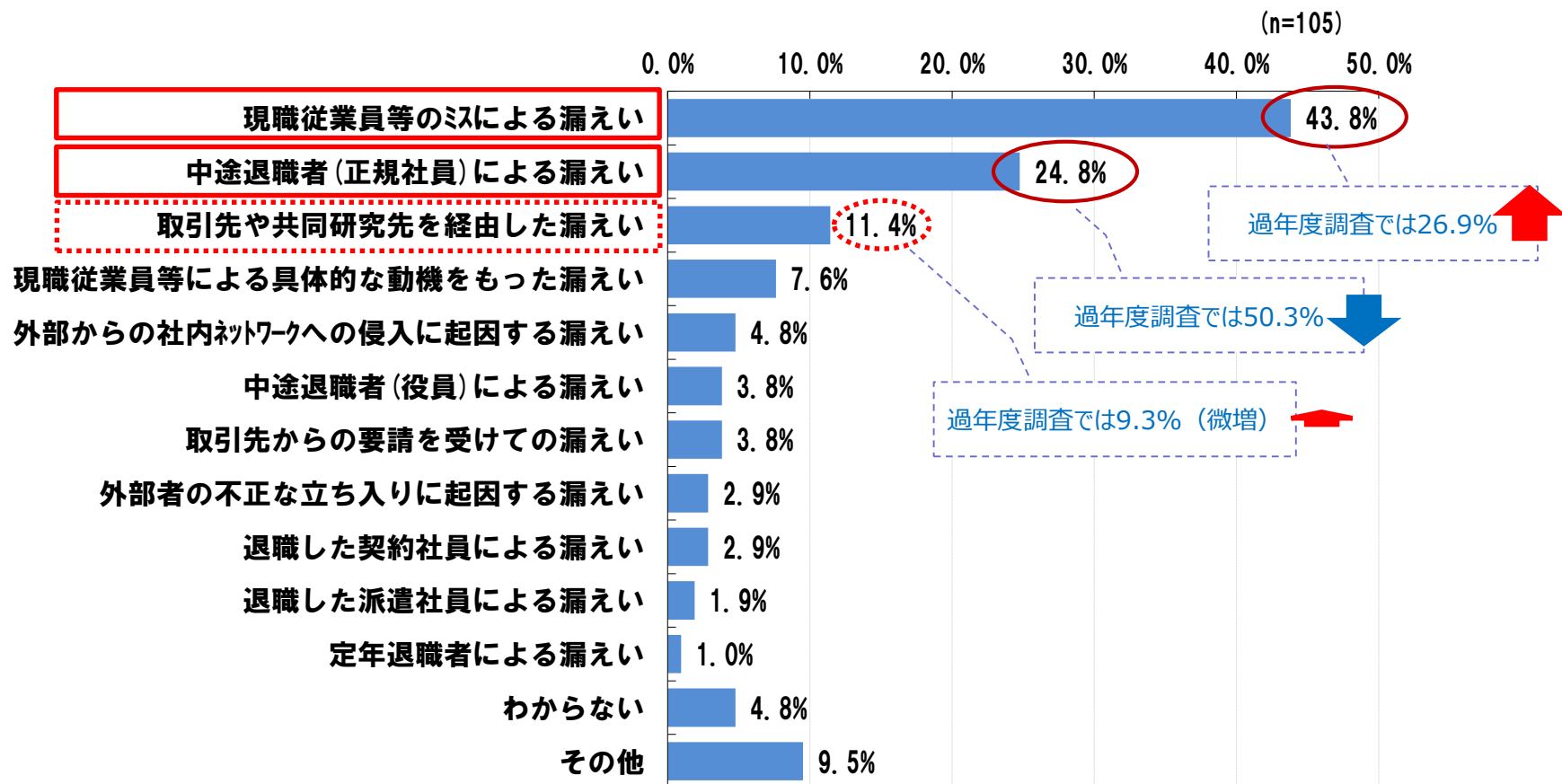
※漏えいの有無を認識している企業に限定して集計をしたため、「わからない」と回答した企業は母数から除外。

5. 営業秘密の漏えい実態

-営業秘密の漏えい発生ルート（漏えいあり企業）

- 営業秘密漏えいの発生ルートについては、「**現職従業員等のミスによる漏えい**」が最も割合が高く、**43.8%**。
- **中途退職者（正規社員）による漏えい**が次に割合が高く**24.8%**。
（過年度調査結果（50.3%）と比べると比率減少。中途退職者向け対策が進んだ企業もあることが推定される。）

<問13>「漏えいのルート」【全業種・全規模】

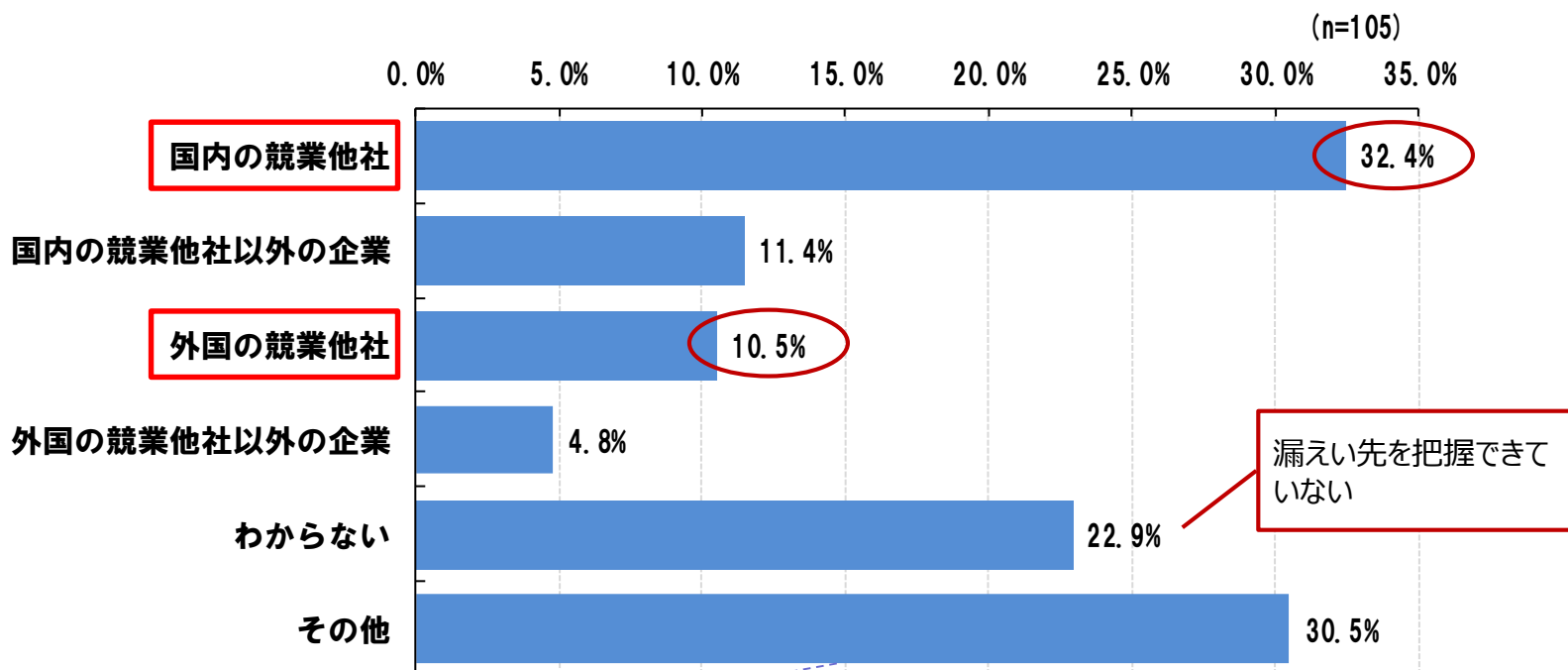


5. 営業秘密の漏えい実態

-営業秘密の漏えい先（漏えいあり企業）

- 明らかに漏えいが発生している企業のうち、**32.4%**の企業で「**国内の競業他社**」に営業秘密が漏えい。**10.5%**が「**外国の競業他社**」。
- 22.9%の企業が「わからない」と回答。（営業秘密の漏えい先を把握できていない。）

<問14>「営業秘密の漏えい先」【全業種・全規模】



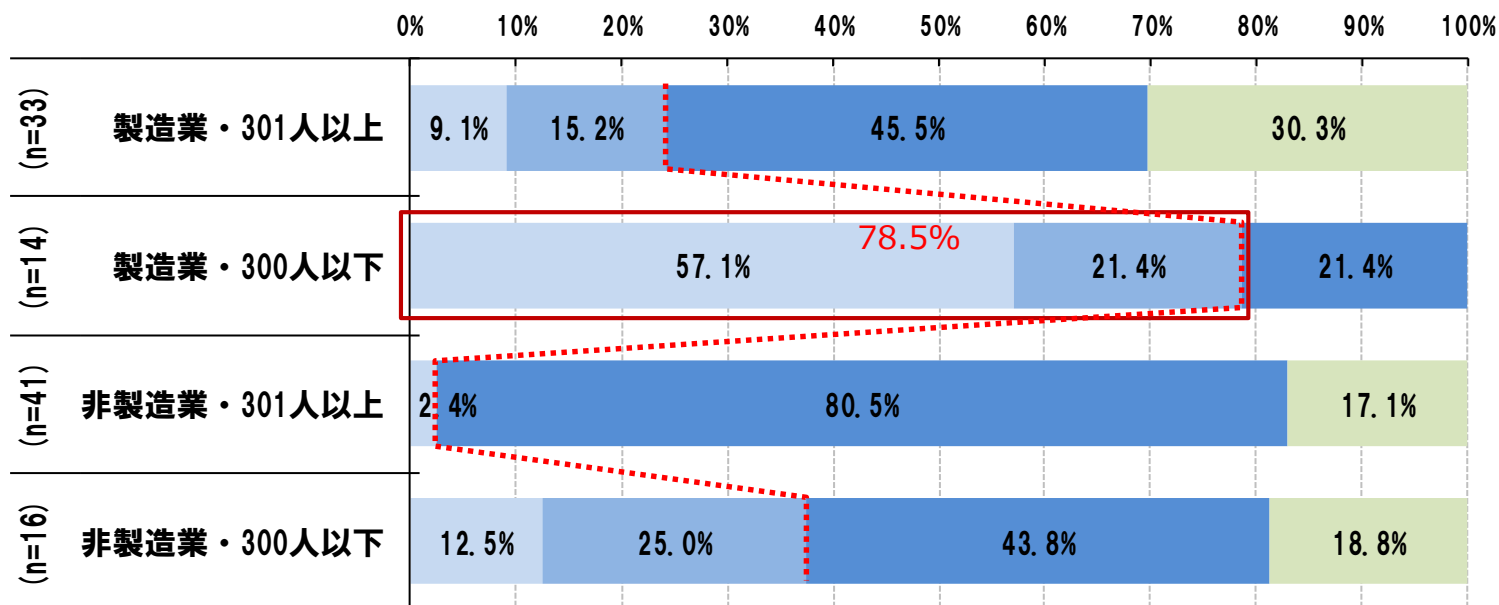
インターネット上に掲載されてしまった、
社内の他部署の従業員等に開示されてしまった
等

5. 営業秘密の漏えい実態

-漏えいした営業秘密が使用され生産された物品の流通（漏えいあり企業）

- 漏えいした営業秘密が使用され生産された物品が市場に流通した事例は、**製造業/中小規模企業**が最も高い割合で経験。「明確にあった」「おそらくあった」合計、**78.5%**。

＜問10＞「漏えいした営業秘密が使用され生産された物品が市場に流通した事例の有無」【業種・規模別】



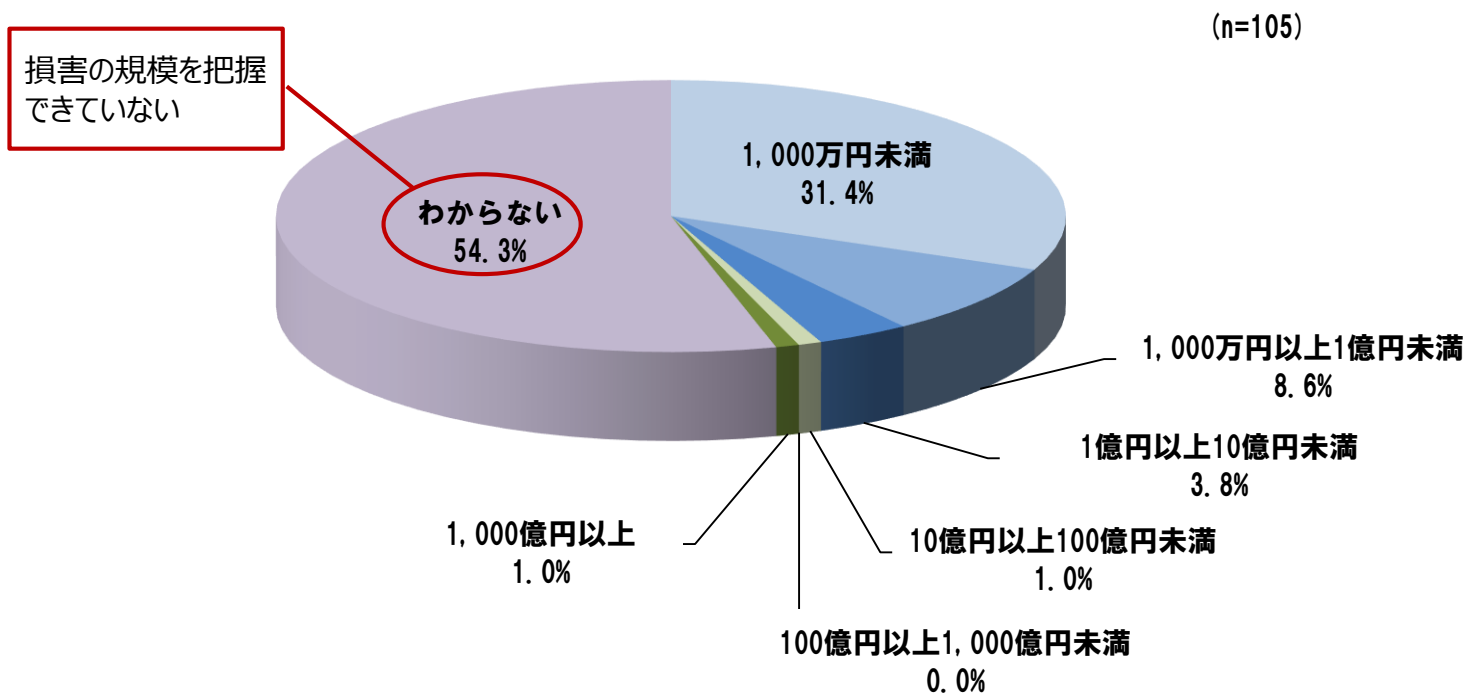
■ 流通した事例が明確にあった ■ 流通した事例がおそらくあった ■ 流通した事例はない ■ わからない

5. 営業秘密の漏えい実態

-営業秘密の漏えいにより被った損害の額（漏えいあり企業）

- 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。
（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。）
- 31.4%の企業が「1,000万円未満」と認識。

<問15>「漏えいによる損害規模」【全業種・全規模】

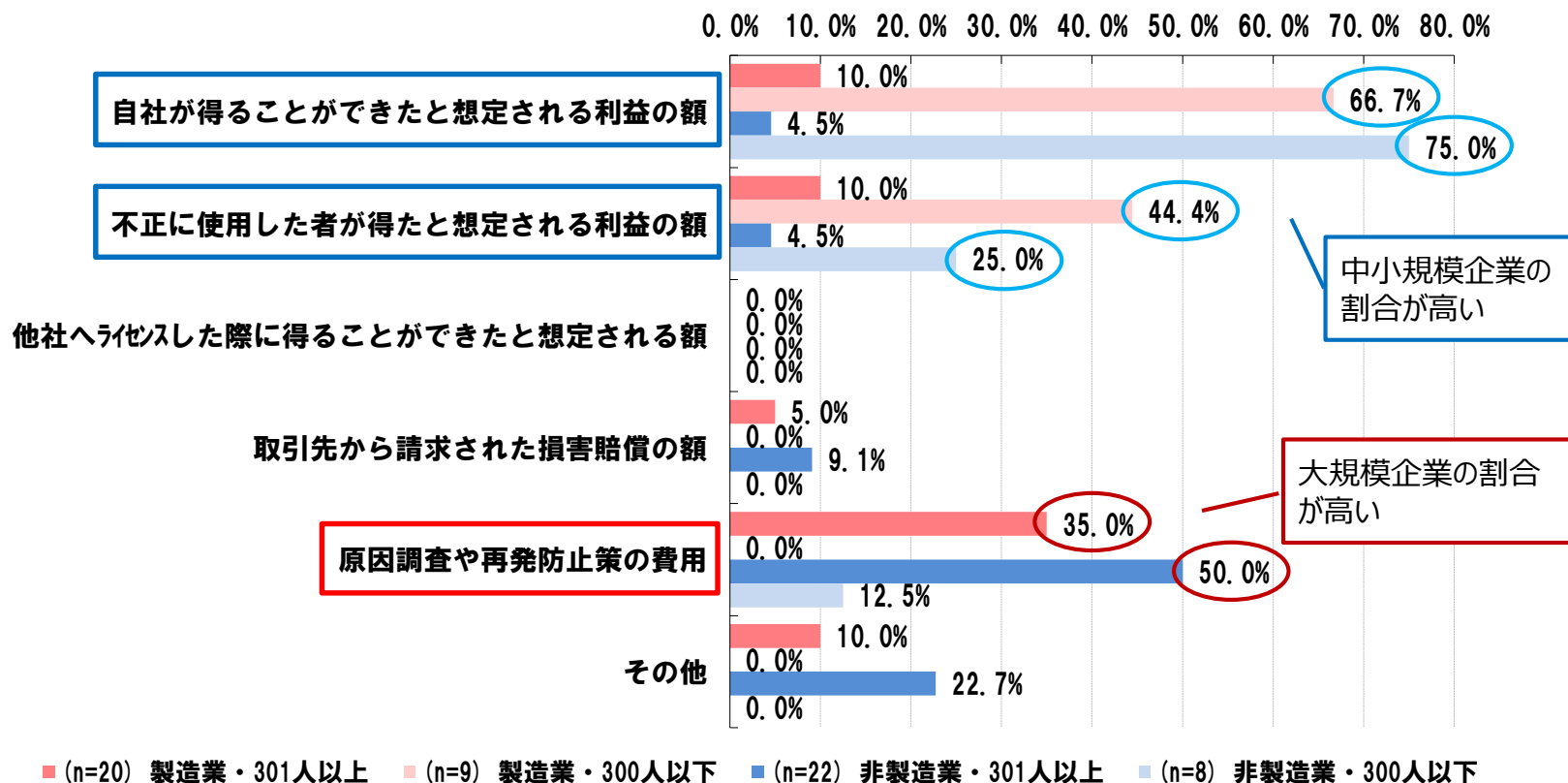


5. 営業秘密の漏えい実態

-営業秘密の漏えいにより被った損害の内容（漏えいあり/業種・規模別）

- **大規模企業**においては、営業秘密の漏えいによって被った損害額の内容を「**原因調査や再発防止策の費用**」と捉えている割合が高い。
- **中小規模企業**においては、「**自社が得ることができたと思定される利益の額**」「**不正に使用した者が得たと想定される利益の額**」と捉えている割合が高い。

<問16>「漏えいによる損害の内容」【業種・規模別】

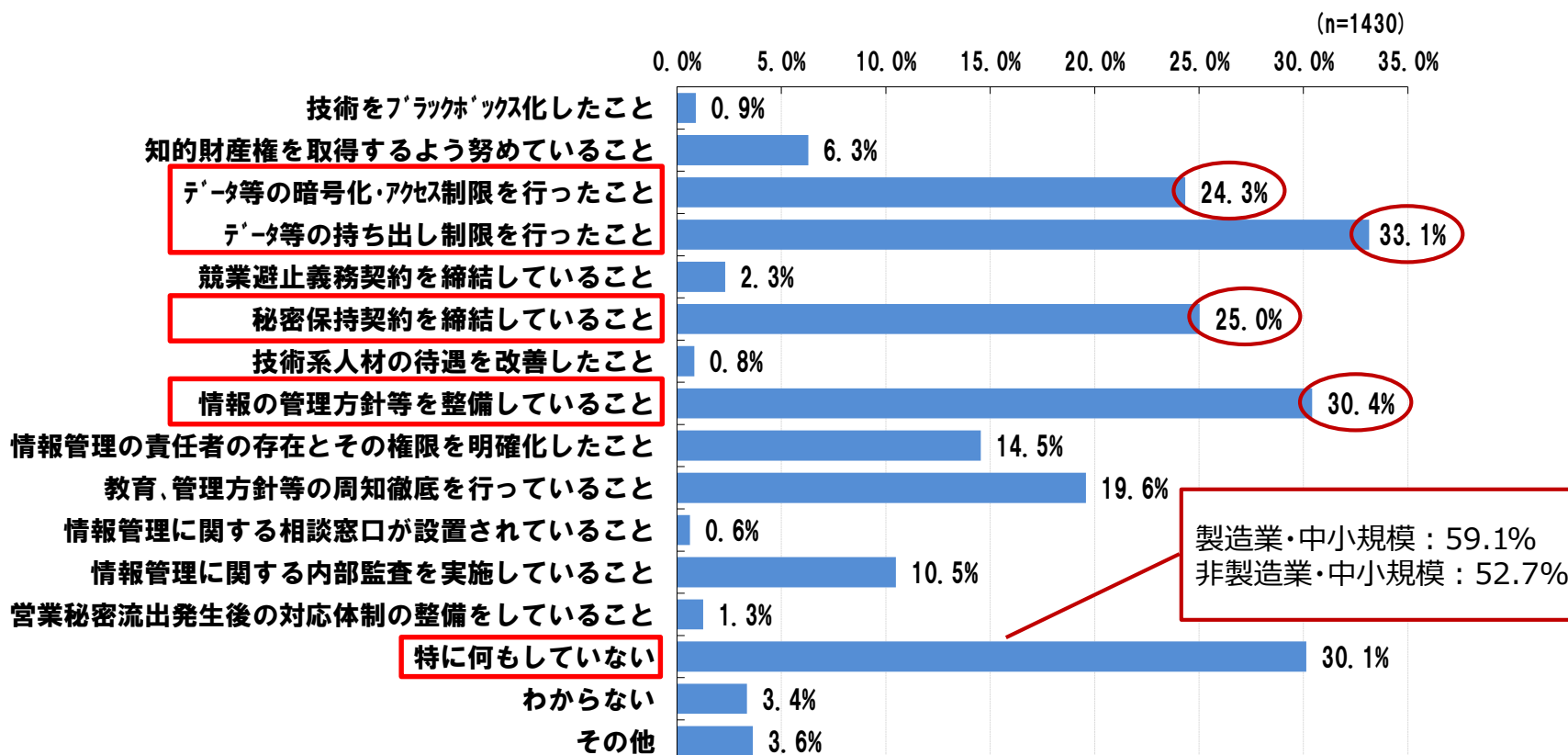


5. 営業秘密の漏えい実態

-営業秘密の漏えいが発生していない要因（漏えいなし回答企業）

- 漏えい事例は**ない**と回答した企業・要因：「**データ等の持ち出し制限を行ったこと**（33.1%）」「**情報の管理方針等を整備していること**（30.4%）」「**秘密保持契約を締結していること**（25.0%）」「**データ等の暗号化・アクセス制限を行ったこと**（24.3%）」。
- 「**特に何もしていない**」と回答した企業も30.1%存在。認識できていない漏えいが一定数存在している可能性がある。（特に中小規模企業では、「特に何もしていない」と回答している割合が高い。）

<問18>「漏えいが起こっていない要因」【全業種・全規模】

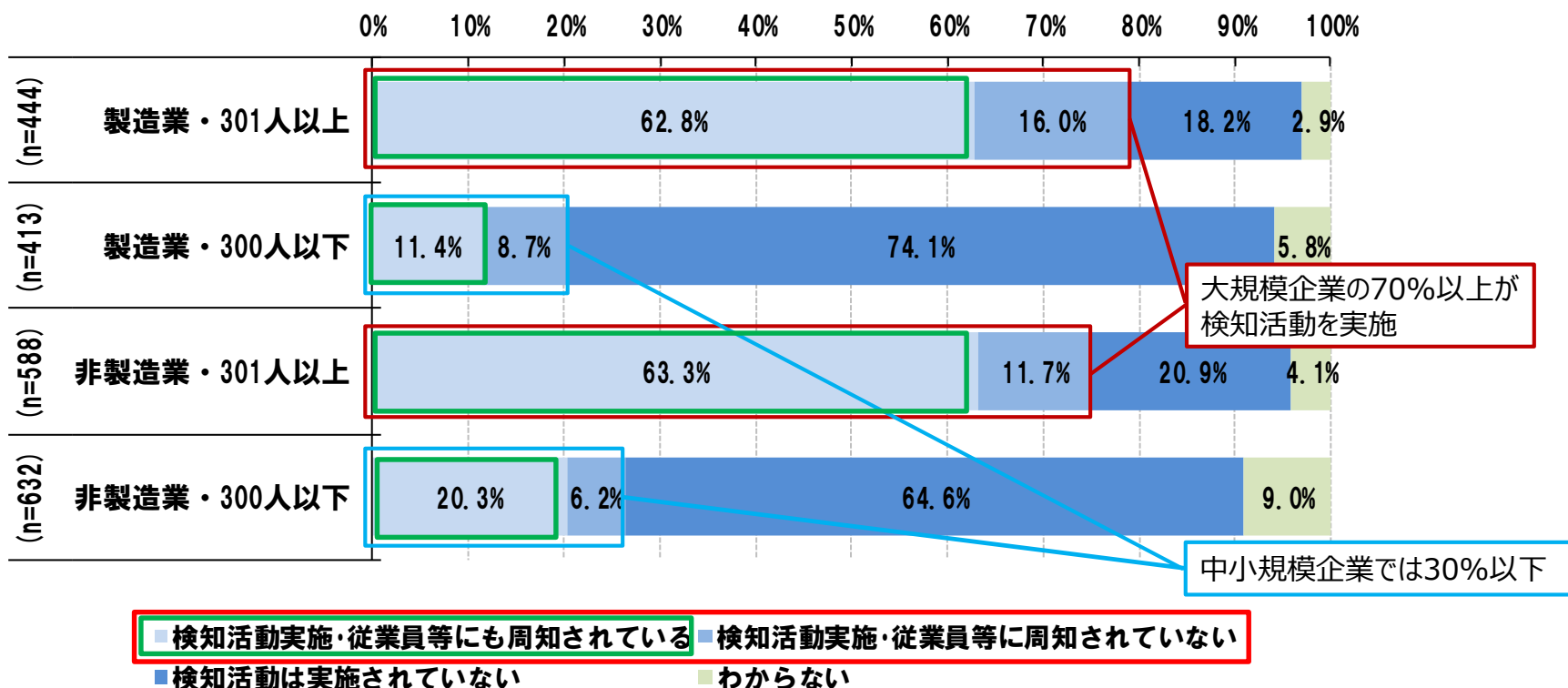


6. 営業秘密の漏えいを検知する活動

-営業秘密の漏えいを検知する活動に関する取組（業種・規模別）

- 営業秘密の漏えいを検知する活動：大規模企業のうち70%以上が実施できている。
- 中小規模企業では30%以下の企業でしか漏えい検知活動を実施できていない。
- 検知活動を実施していることを従業員等に周知することは、営業秘密の漏えいを未然に防ぐ効果があるとされており、大規模企業では60%以上が検知&周知の取組を実施、中小規模企業では10~20%程度でしか実施できていない。

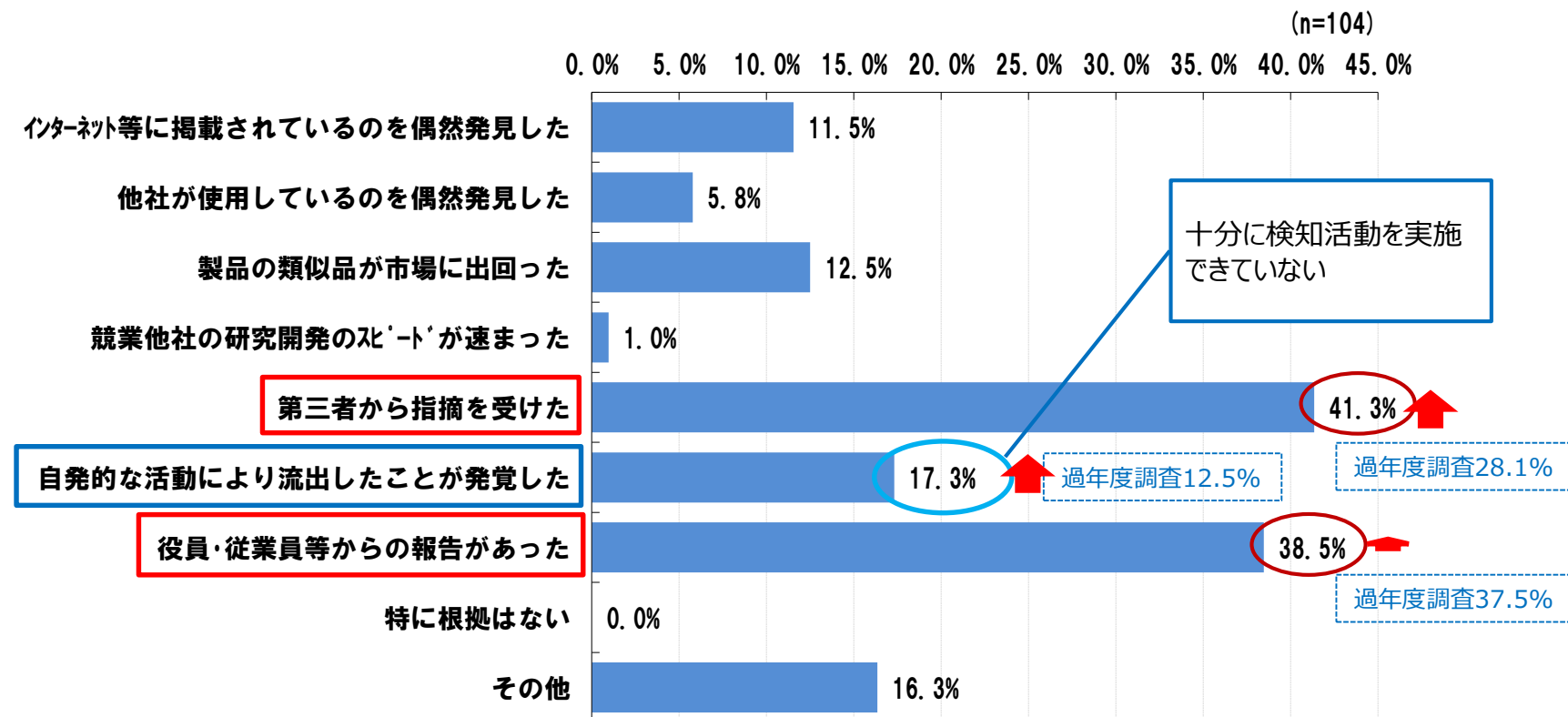
<問9>「漏えいに気付ける活動の実施状況」【業種・規模別】



6. 営業秘密の漏えいを検知する活動 -営業秘密の漏えい認識のきっかけ（漏えいあり企業）

- 過去5年間に営業秘密の漏えいを経験した企業が漏えいを認識したきっかけ「**第三者から指摘を受けた（41.3%）**」「**役員・従業員等からの報告があった（38.5%）**」の割合が高い。
- 「**自発的な活動により流出したことが発覚した**」と回答した企業の割合は**17.3%**に留まる。日頃から十分に検知活動を実施できていない企業が多いことが窺える。

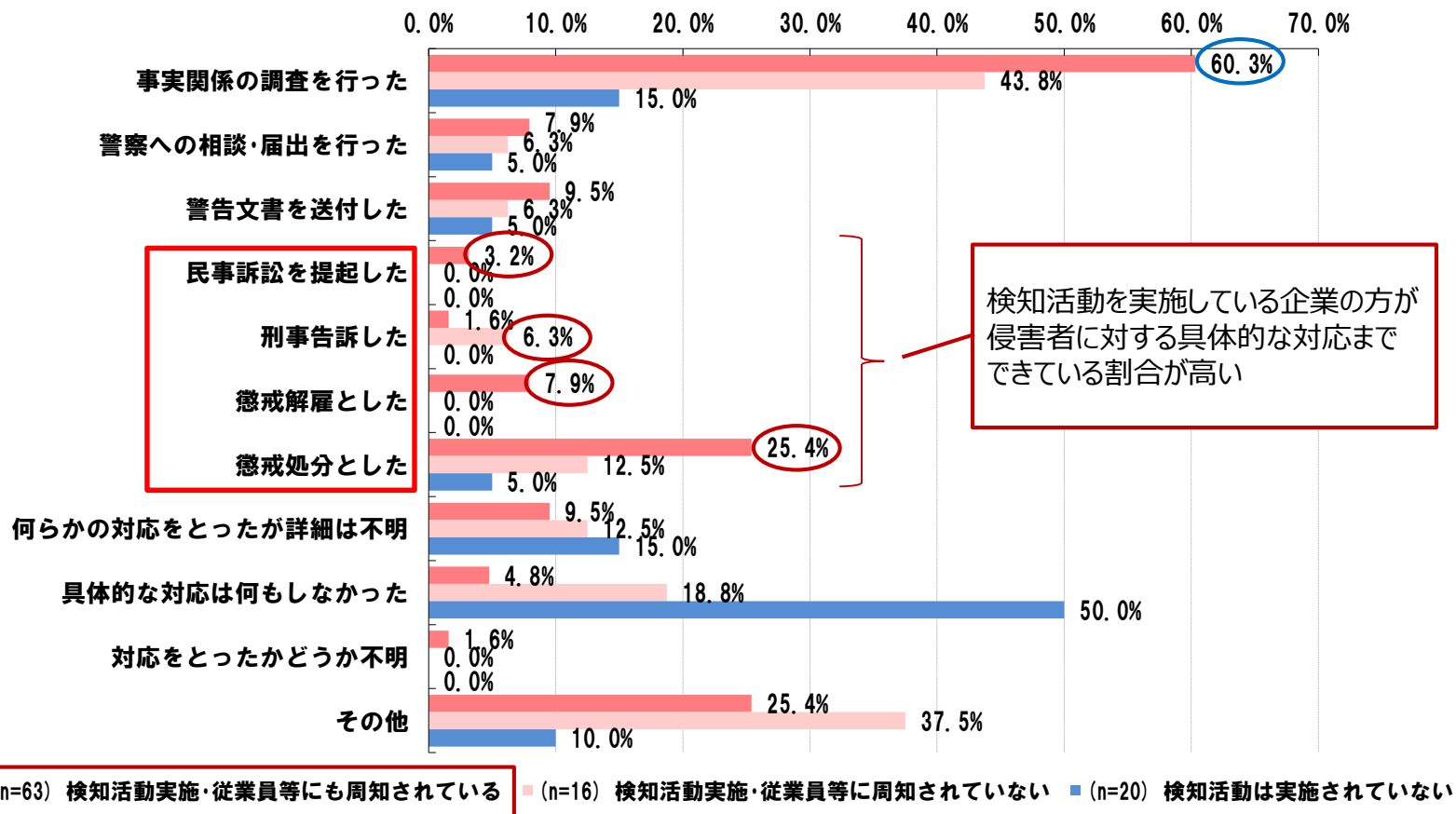
<問12>「漏えいを認識したきっかけ」【全業種・全規模】



6. 営業秘密の漏えいを検知する活動 -検知活動の有効性（侵害者への対応との関係）

- 検知活動を実施している企業は実施していない企業と比較して、侵害者に対して具体的な対応ができています割合が高い。
- 検知活動を実施している企業においては、事実関係の調査を実施するだけでなく、懲戒処分等の社内処分対応や、民事訴訟や刑事告訴といった法的手段による対応ができています企業もある。

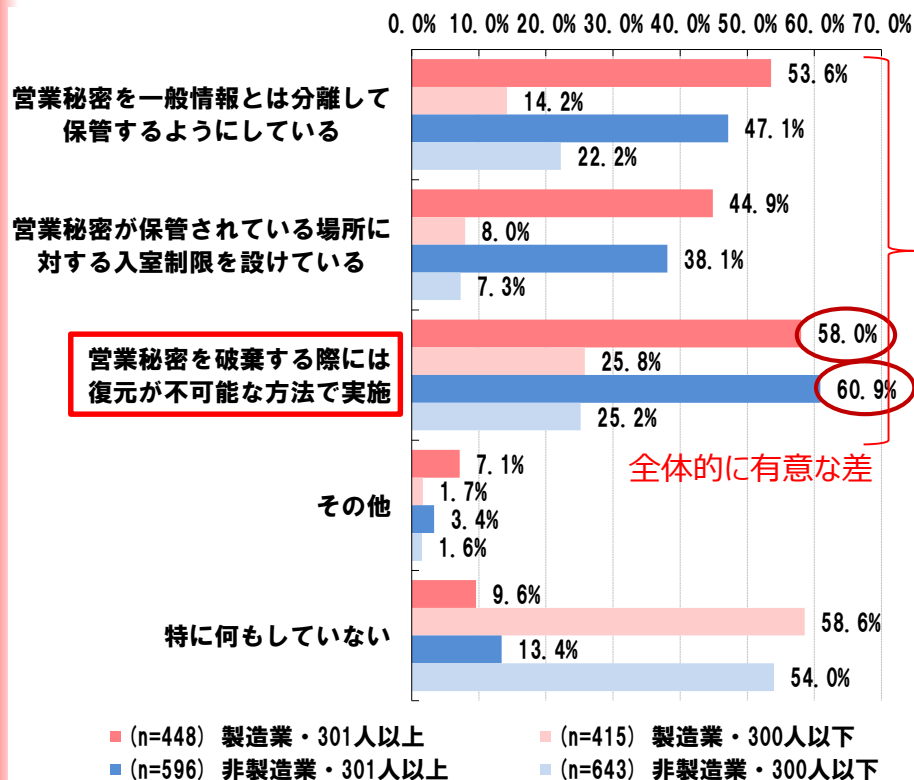
<問17×問9>「侵害行為を行った行為者・企業への対応」【検知活動・周知の有無別】



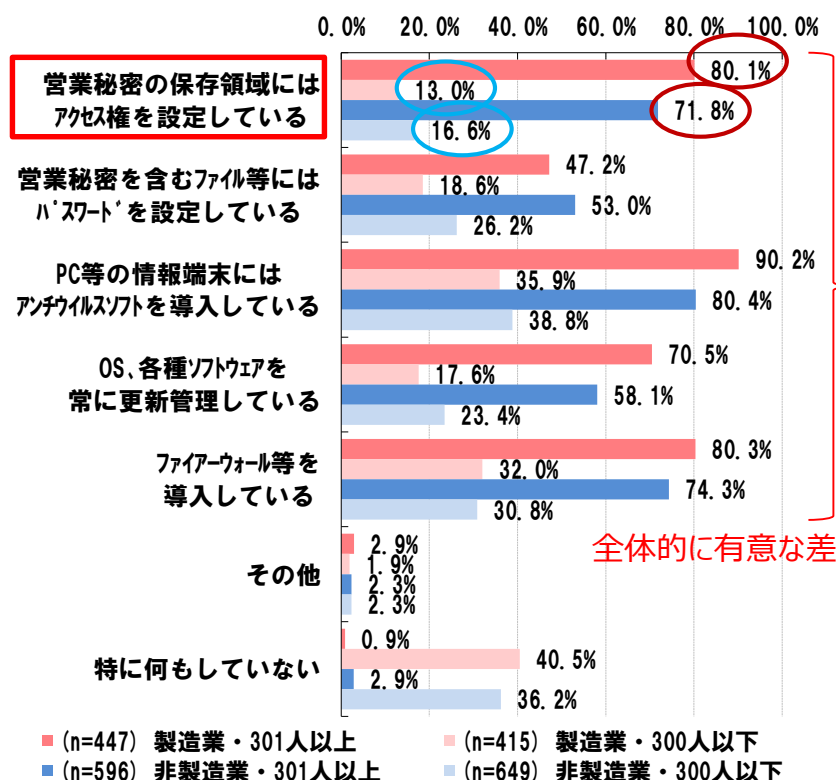
7. 営業秘密の漏えい対策の取組状況 -接近の制御に資する対策（業種・規模別）

- 営業秘密へのアクセスを物理的に制御する対策：全体的に有意な差あり。
60%前後の大規模企業が「営業秘密を破棄する際には復元が不可能な方法で実施」に取り組んでいる。中小規模企業では25%強。
- 営業秘密へのアクセスをシステムの的に制御する対策：全体的に有意な差あり。
70~80%程度の大規模企業が、「営業秘密の保存領域にはアクセス権を設定している」対策を実施。中小規模企業では10%強。

<問31>「営業秘密へのアクセスを物理的に制御するための対策」
【業種・規模別】



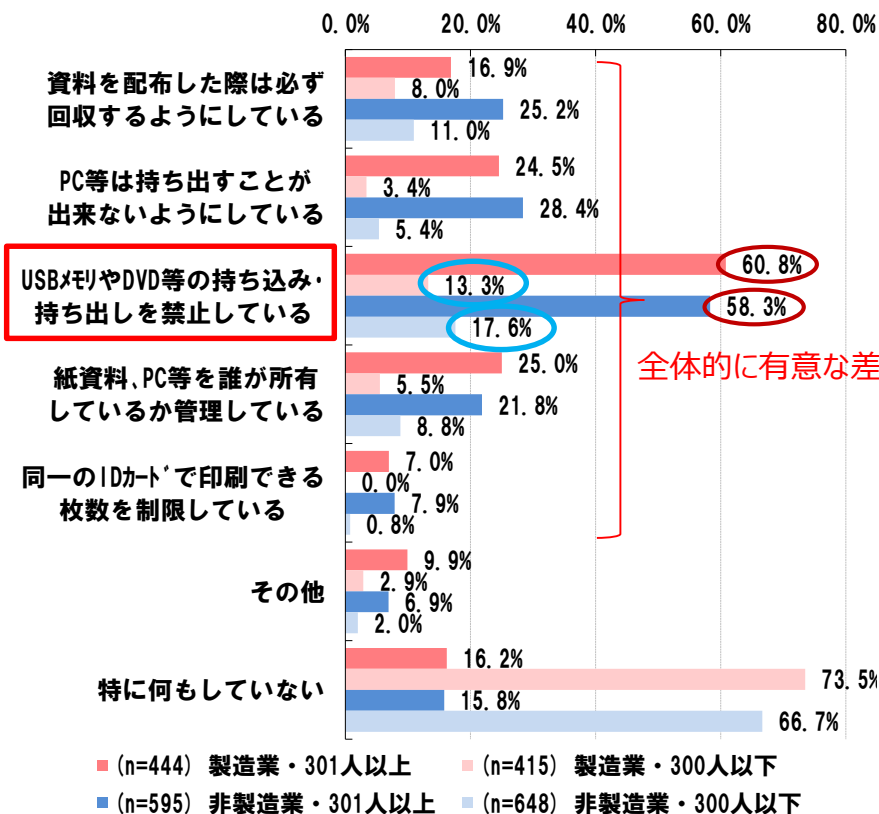
<問32>「営業秘密へのアクセスをシステムの的に制御するための対策」
【業種・規模別】



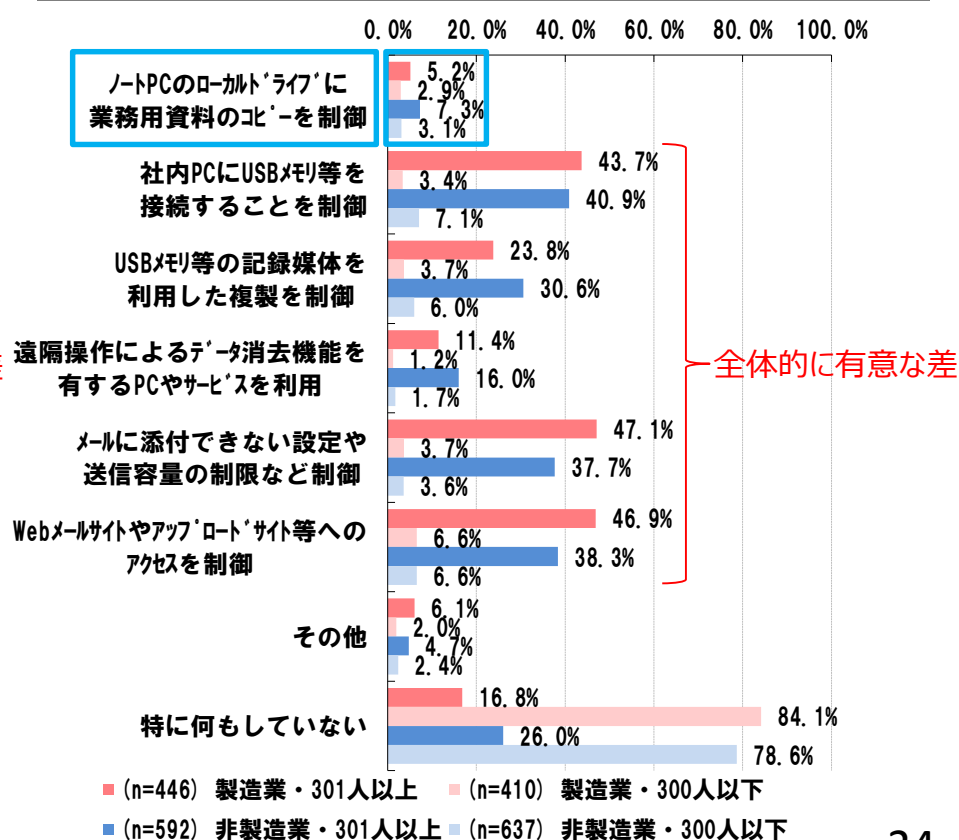
7. 営業秘密の漏えい対策の取組状況 -持出し困難化に資する対策（業種・規模別）

- 営業秘密の外部への持出を物理的に制御するための対策：全体的に有意な差あり。
「USBメモリやDVD等の持ち込み・持出を禁止」対策は大規模企業の60%前後で実施。中小企業では10～20%。
- 営業秘密の外部への持出をシステム的に制御するための対策：全体的に有意な差あり。遅れている対策：
「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、大規模企業であっても10%未満でしか実施できていない。

<問33>「営業秘密の持出を物理的に制御するための対策」
【業種・規模別】



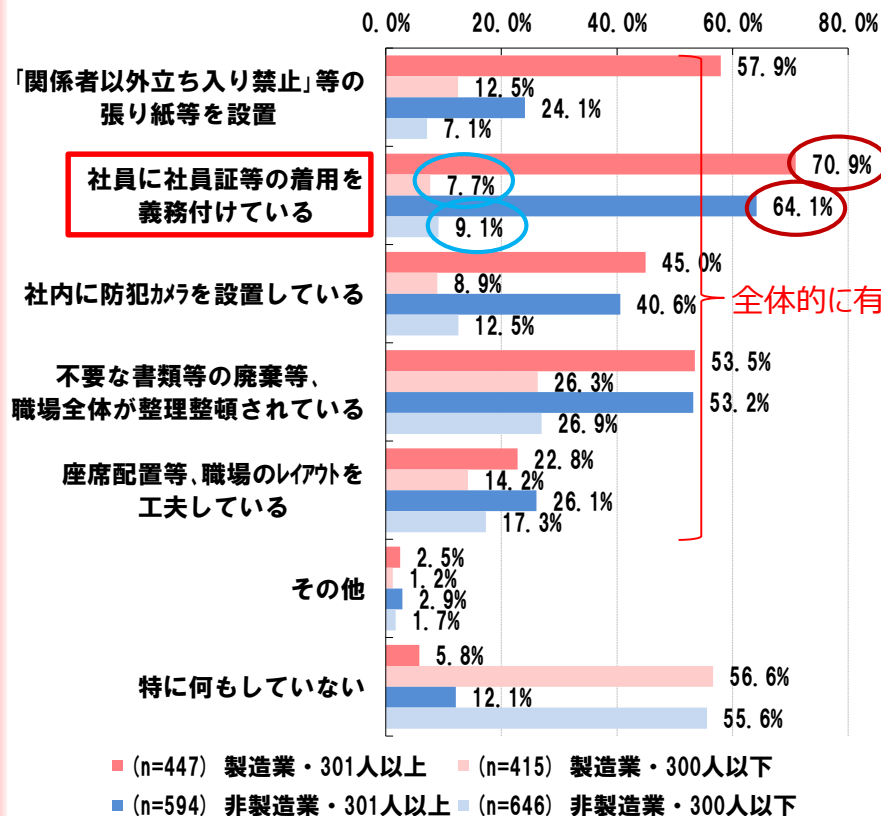
<問34>「営業秘密の持出をシステム的に制御するための対策」
【業種・規模別】



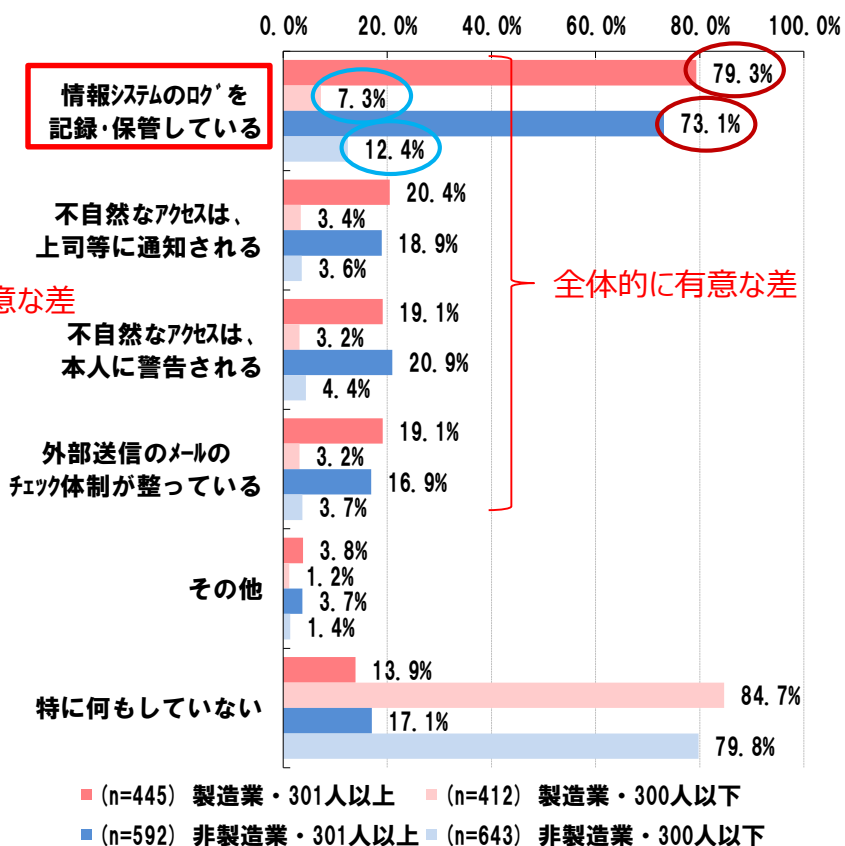
7. 営業秘密の漏えい対策の取組状況 -視認性の確保に資する対策（業種・規模別）

- 営業秘密の漏えいをしにくい環境をつくるための物理的な対策：全体的に有意な差あり。
大規模企業で60～70%程度が「社員に社員証等の着用を義務付けている」対策を実施。中小規模企業では10%未満。
- 営業秘密の漏えいをしにくい環境をつくるためのシステムの対策：全体的に有意な差あり。
大規模企業で70～80%程度が「情報システムログを記録・保管している」。中小規模企業では10%前後。

＜問35＞「営業秘密を漏えいしにくい環境をつくるための物理的な対策」【業種・規模別】



＜問36＞「営業秘密を漏えいしにくい環境をつくるためのシステムの対策」【業種・規模別】

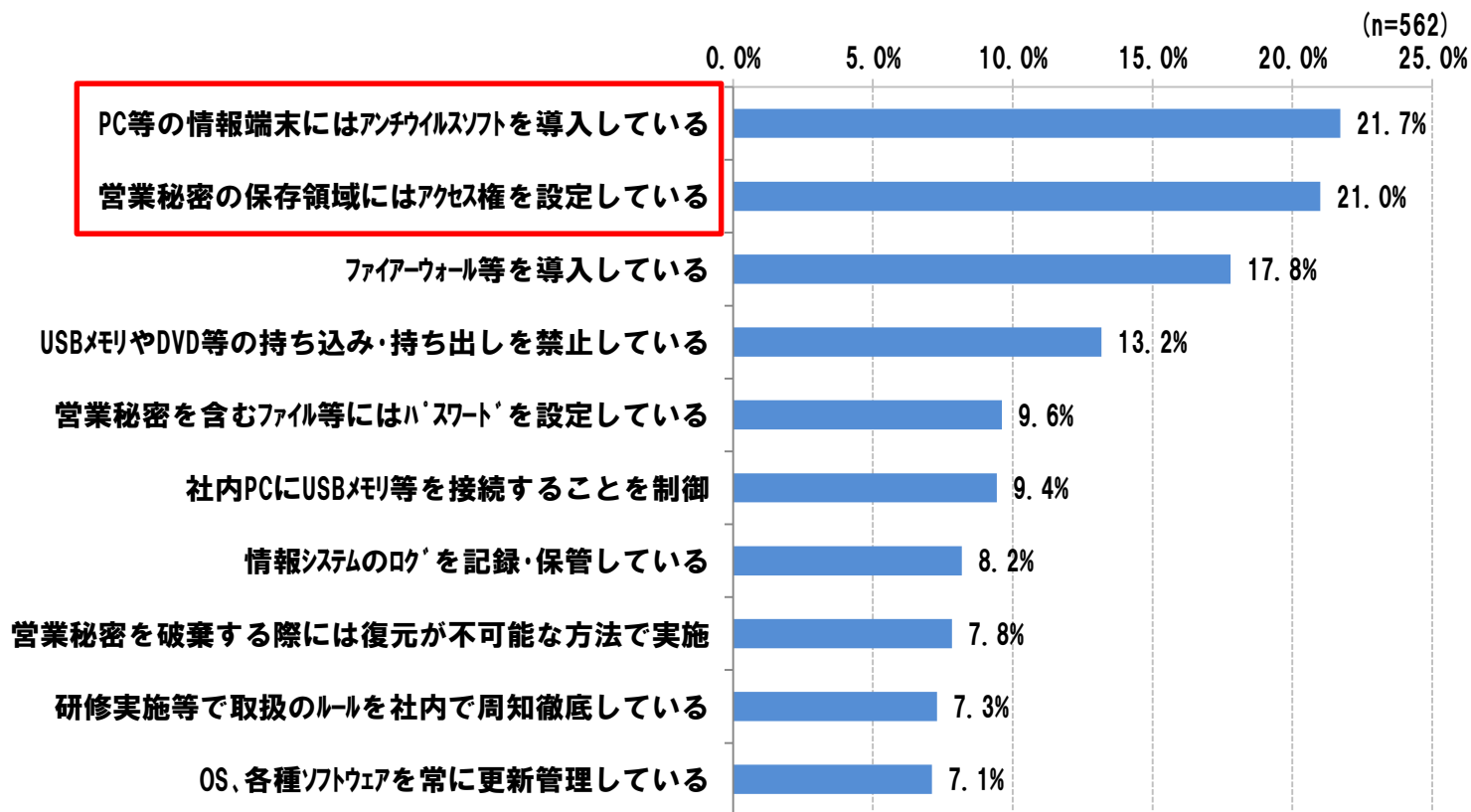


7. 営業秘密の漏えい対策の取組状況

-企業が有効性を感じている対策（企業の主観的意識・参考情報）

- 「PC等の情報端末にはアンチウイルスソフトを導入」「営業秘密の保存領域にはアクセス権を設定」対策
20%以上の企業が有効性を実感していると回答。
- 上位10項目に挙げられている対策には基本的なものも多く、この上位の対策だけ実施すればよいというわけでもない。
ただし取組が遅れている企業が今後着手していくべき対策・優先順位等を検討する際には参考にできる。

<問51>「有効性を実感できた対策（上位10項目）」【全業種・全規模】

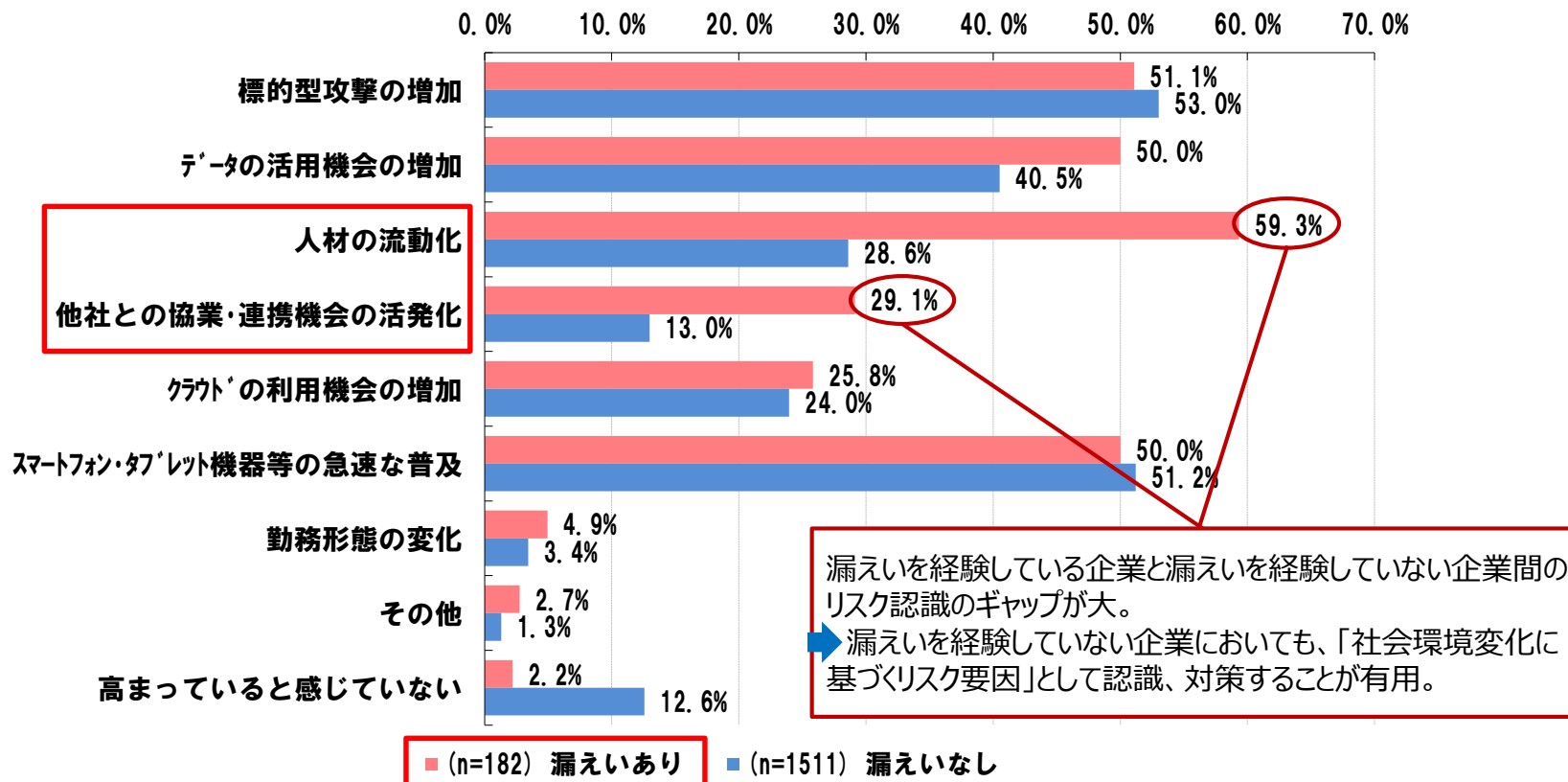


8. 漏えいを経験した企業の認識

-過去5年間に営業秘密の漏えいを経験した企業の社会動向意識

- 営業秘密の漏えいを経験した企業は、その後漏えい防止のための対策強化等に取り組むことが多い。漏えいを経験した企業の意識や取組等は、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。
- 過去5年間に漏えいを経験した企業と、経験していない企業について、漏えいリスクの高まりを感じる社会動向の変化を比較 → 「人材の流動化」「他社との協業・連携機会の活発化」について、大きな差を観測（大規模/製造業と同様の高い比率）。

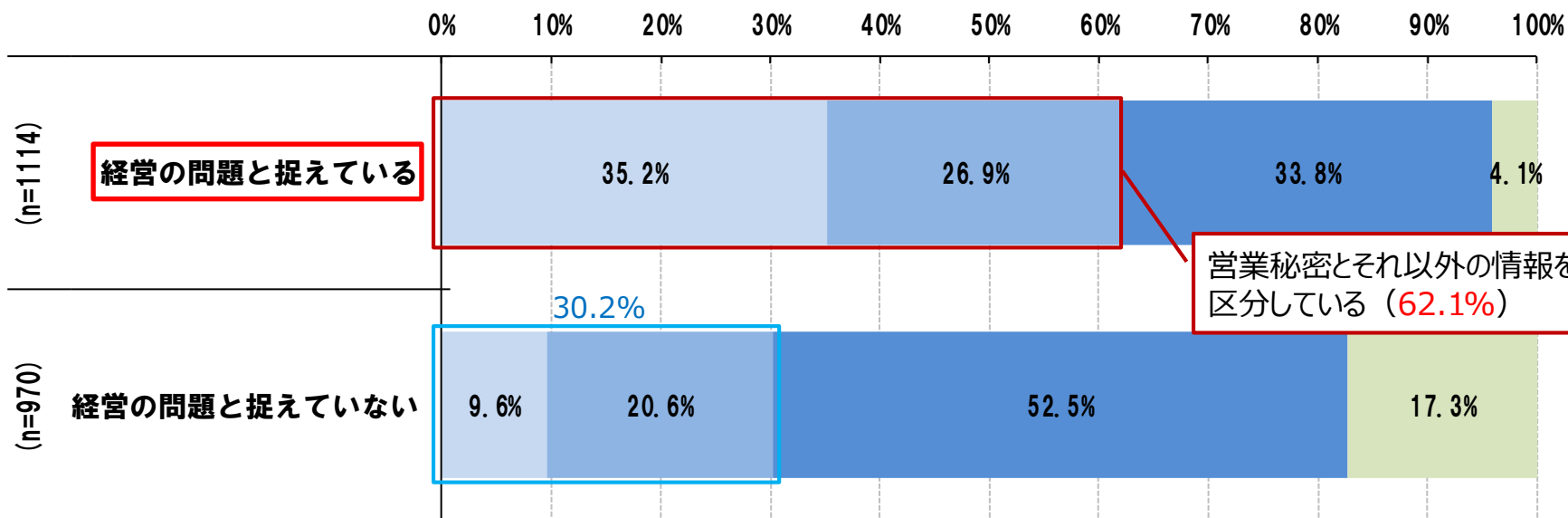
<問19×問8>「営業秘密の漏えいリスクの高まりを感じる社会的動向の変化」【過去5年間での漏えい経験の有無での比較】



9. 営業秘密管理を経営の問題と捉えている企業の取組 -情報の区分状況（経営課題意識の有無）

- 営業秘密管理を、経営課題の一つとして捉え、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する事が重要。
- 営業秘密管理を経営の問題として捉えている企業
→経営の問題と捉えていない企業と比較して、営業秘密とそれ以外の情報をしっかりと区分できている割合が高い（62.1%）。
- 情報の区分を実施することは、個別具体的な営業秘密保護対策を実施する上での前提となる基本的な取組
→営業秘密管理を経営の問題として捉えている企業は、経営の問題と捉えていない企業と比較して、個別具体的な営業秘密保護対策に取り組んでいる。（詳細は報告書本編参照）。

<問21×問26>「営業秘密とそれ以外の情報の区分状況」【営業秘密管理に関する捉え方の差異による比較分析】

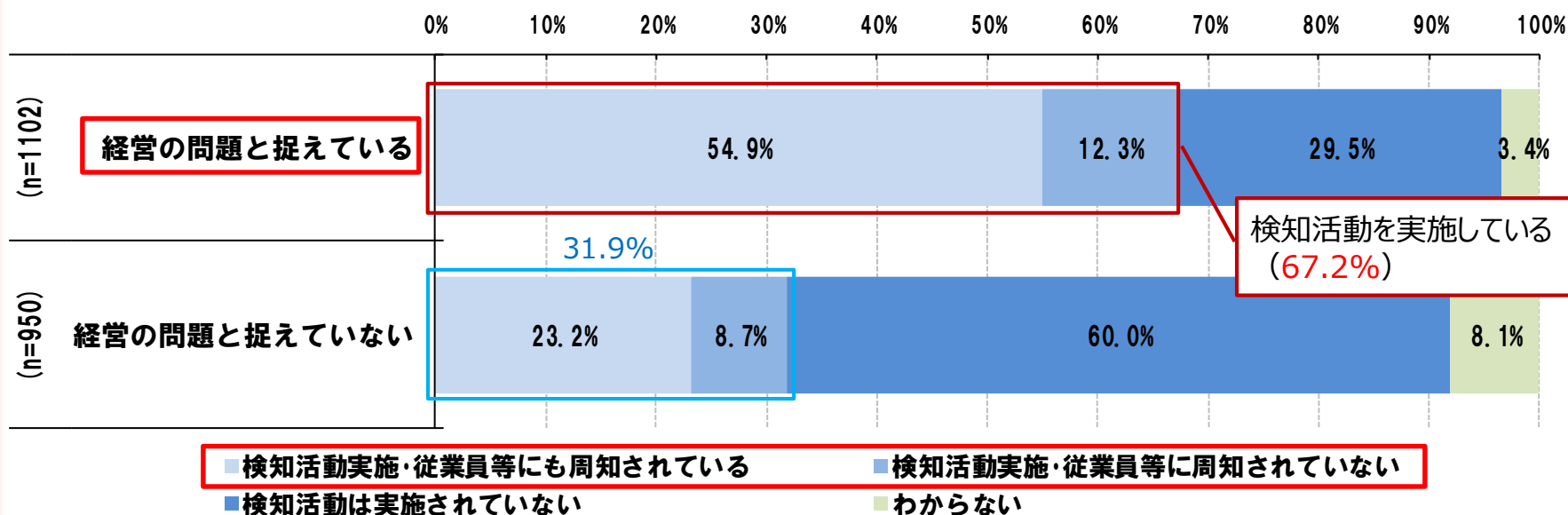


■ 区分しており、営業秘密はさらに秘密性のレベルで区分
■ 区分しているが、秘密性のレベルで区分はしていない
■ 営業秘密とそれ以外の情報とを区分していない
■ わからない

9. 営業秘密管理を経営の問題と捉えている企業の取組 -漏えい検知活動の実施状況（経営課題意識の有無）

- **営業秘密管理を経営の問題として捉えている企業**
→営業秘密とそれ以外の情報の分けや、個別具体的な営業秘密保護対策だけでなく、**漏えい検知活動**も積極的に取り組んでいる。
- 営業秘密管理を経営の問題として捉えていない企業においては、31.9%の企業でしか検知活動を実施できていない。

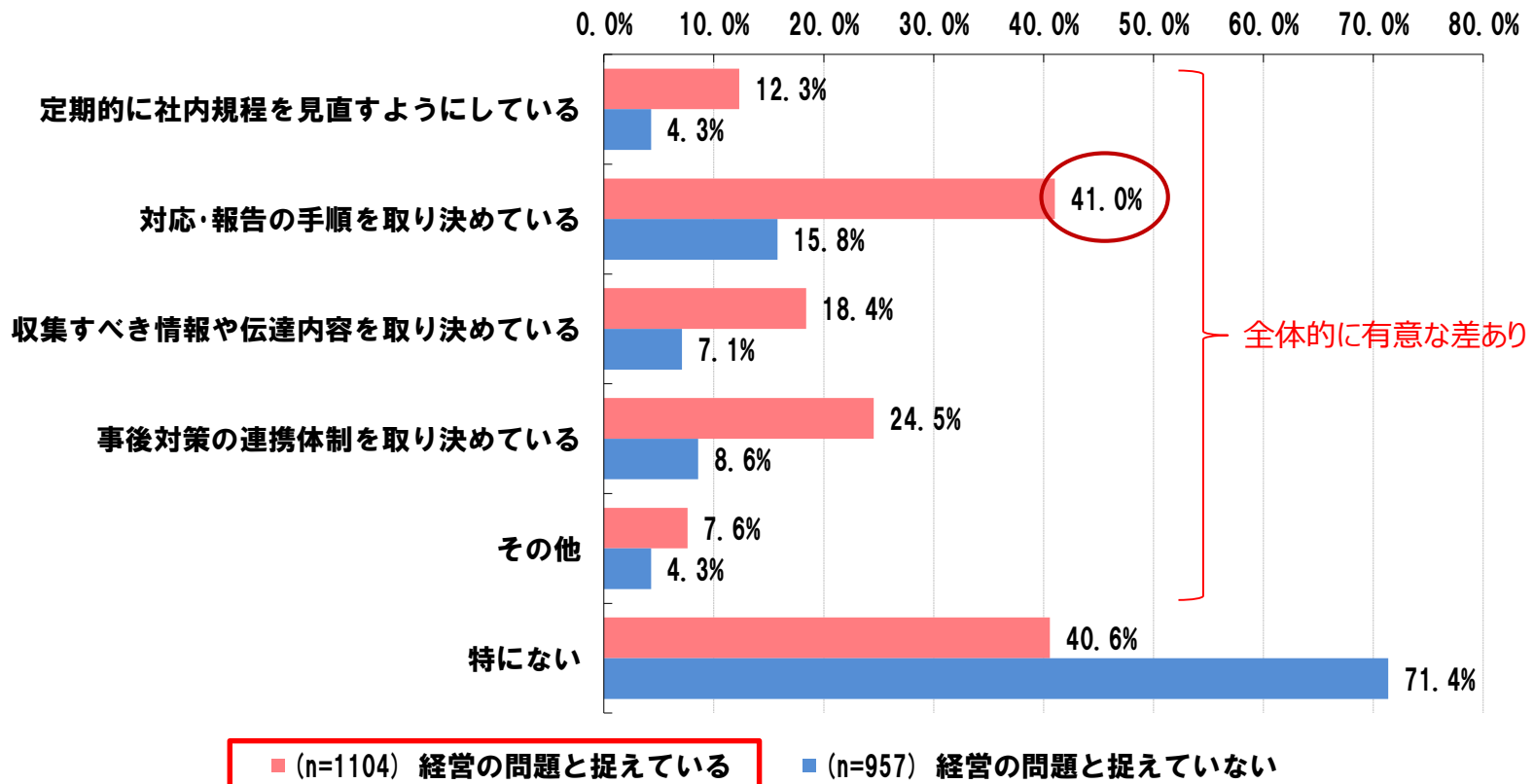
<問9×問26>「検知活動の実施状況」【営業秘密管理に関する捉え方の差異による比較分析】



9. 営業秘密管理を経営の問題と捉えている企業の取組 -情報セキュリティリスクへの対策（経営課題意識の有無）

- 情報漏えい対策や検知活動だけでなく、日頃から予防が困難な情報セキュリティリスクに対する準備しておくことが望ましい。
- **営業秘密管理を経営の問題と捉えている企業**のうち、**41.0%**が**有事の際の対応・報告の手順**を取り決めており、組織的な取組ができていることが窺える。

＜問57×問26＞「予防が困難な情報セキュリティリスクへの取組」【営業秘密管理に関する捉え方の差異による比較分析】

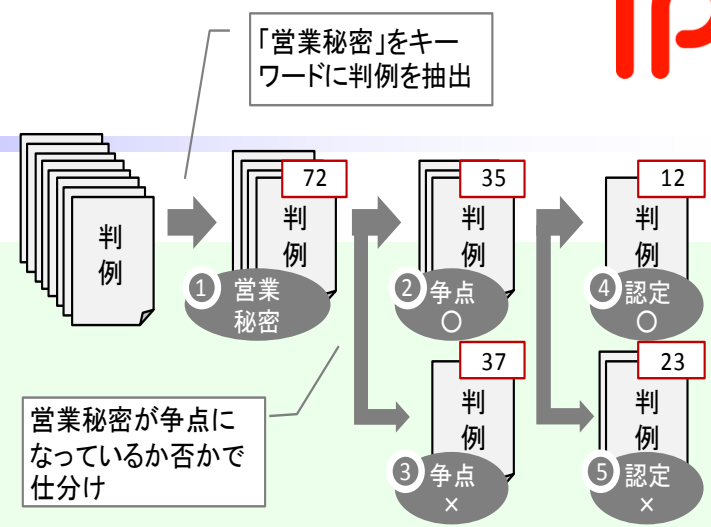


10. 判例調査

-裁判における営業秘密の認定傾向

- 2014年10月1日～2016年8月23日の営業秘密関連の判例調査
- 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を比較
- **営業秘密3要件**（秘密管理性・有用性・非公知性）の判断の調査

今回調査対象の判例において、裁判所の判断に影響したポイント



秘密管理性の認定

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秘密管理性認定に影響。
 これらの項目を1つでも満たせば自動的に秘密管理性が認められるものでもなく、当事者の主張事実を裁判所が総合考慮して判断。

有用性の認定

- 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。
 その効果の度合いについては、必ずしも質的に高い優位性・独自性まで求められるものではなく、例えば**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**、**効果の証拠に乏しい情報**は、有用性が認められない判例あり。

非公知性の認定

- 情報保有者の管理下以外では**一般的に入手できない状態**と認められたものや、**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場合に、非公知性が肯定的に捉えられた判例あり。
- 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、非公知性が否定的に捉えられた判例あり。

1.1. 調査結果まとめ

漏えい実態・営業秘密管理を取り巻く環境の変化

- 8.6%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（10社に1社近く。前回調査では13.5%）。
- **漏えいリスクを感じる社会動向変化** 上位3項目：
「標的型攻撃の増加（52%）」、「スマートフォン・タブレット機器等の急速な普及（51%）」、「データの活用機会の増加（42%）」
- **漏えいを経験した企業が漏えいリスクとして捉える社会動向変化＝「人材の流動化」「他社との協業・連携機会の活発化」**
▶ 漏えいがないとされる企業においても「社会環境変化に基づくリスク要因」として認識し、転職や他社協業に備えた施策が有用。

営業秘密漏えい対策への取組

- **予防的な漏えい対策の遅れ**
大規模企業と比較して、中小規模企業は全体的に漏えい対策への取組が遅れている。
中小規模企業では**システムの対策**、特に「**USBメモリの使用制御**」や「**システムログの記録・保管**」等、十分に取り組めていない。
大規模企業では「システムログの記録・保管」には取り組んでいる企業が多いが、**予防的な対策等**にはまだ十分に取り組めていない状況。
- **管理対象の明確化の重要性**
情報区分は大規模企業で70%弱、中小規模企業で30%程度で実施されている。
調査結果から、**情報の区分をしっかりとできている企業ほど、具体的な漏えい対策に関する取組も進んでいる**ことが示された。
▶ 情報区分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とされた対策の前提であり、改めてその重要性が示唆された。
- **漏えいを検知する活動**（漏えい未然防止、漏えい後の対策）
多様化・高度化した手口に備えて、ログ分析等による漏えい検知が重要であり、調査でも大規模企業の70%以上、中小規模企業の30%弱で実施。
調査結果から、**漏えい検知活動を実施している企業の方が、様々な対策への取組・侵害者に対する踏み込んだ対応ができている**。
▶ 先進的な企業では個別対策と不可分の措置として検知活動に取り組まれていること、およびその重要性が示唆された。

組織的な取組

- **経営層の関与と組織横断的な検討**
調査結果から、**営業秘密管理を経営の問題として捉えている企業の方が、総じて様々な取組が進んでいる**ことが示された。
▶ 経営層が積極的に関与し、経営に直結する問題として捉えて組織横断的に対策の検討等を推進していくことの重要性が示唆された。