2024年度実施
企業における営業秘密管理に関する実態調査　報告書について

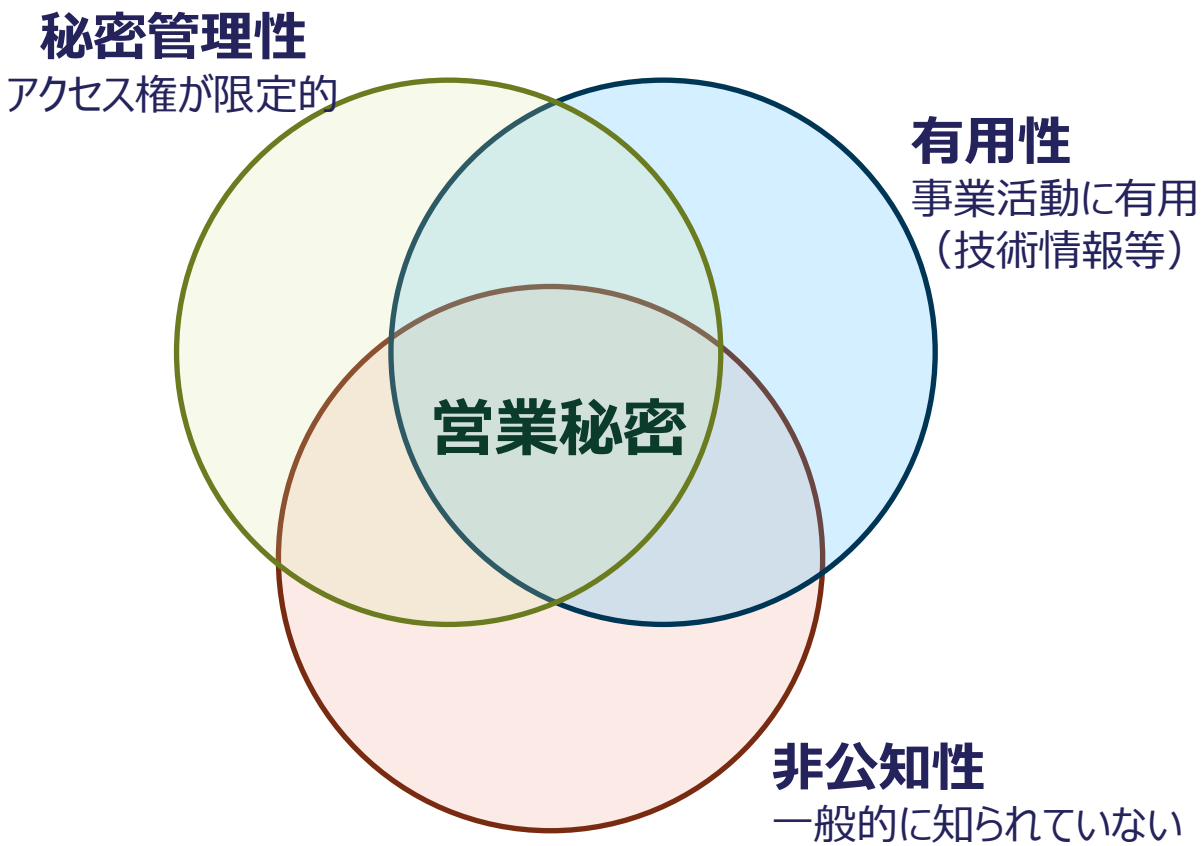
2026/3/11

独立行政法人情報処理推進機構
入来 星衣

IPA Better Life with IT

背景①（企業における営業秘密管理とIPAの関係）

- 営業秘密：不正競争防止法で保護される



- 営業秘密は各企業の競争力の源泉

各企業において
適切に**管理・活用**を行う必要がある

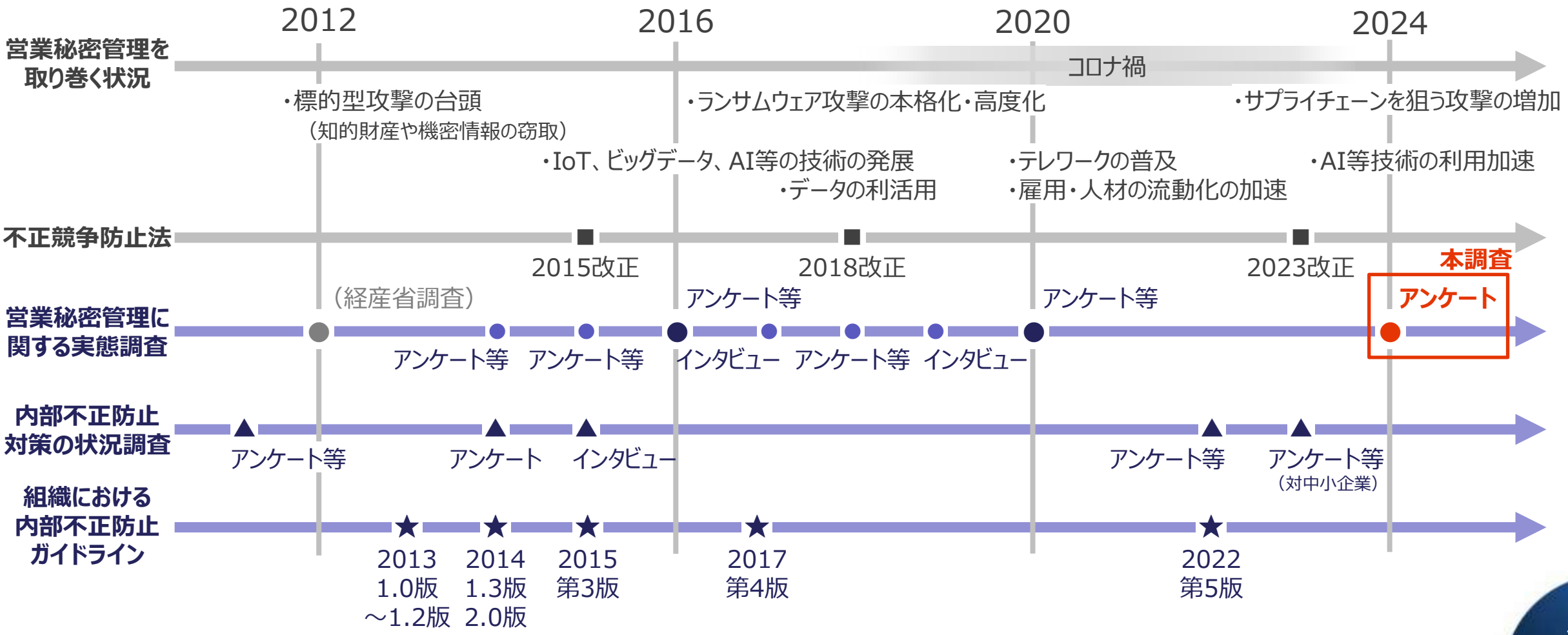
参考になる情報例
- 漏えいの実態（内部不正の発生状況等）
- 情報セキュリティ上の脅威動向
- 関連する法令の改正
- 他の企業の対策の取組状況
- 判例

IPAは各企業での営業秘密管理の参考になる情報を提供
- 調査結果の公表
- ガイドラインの提示　等

←組織における内部不正防止ガイドライン

背景②（今回調査の立ち位置）

- 情報を提供するために、状況の変化を、調査で確かめて、ガイドライン等に反映する



2024年度調査　概要

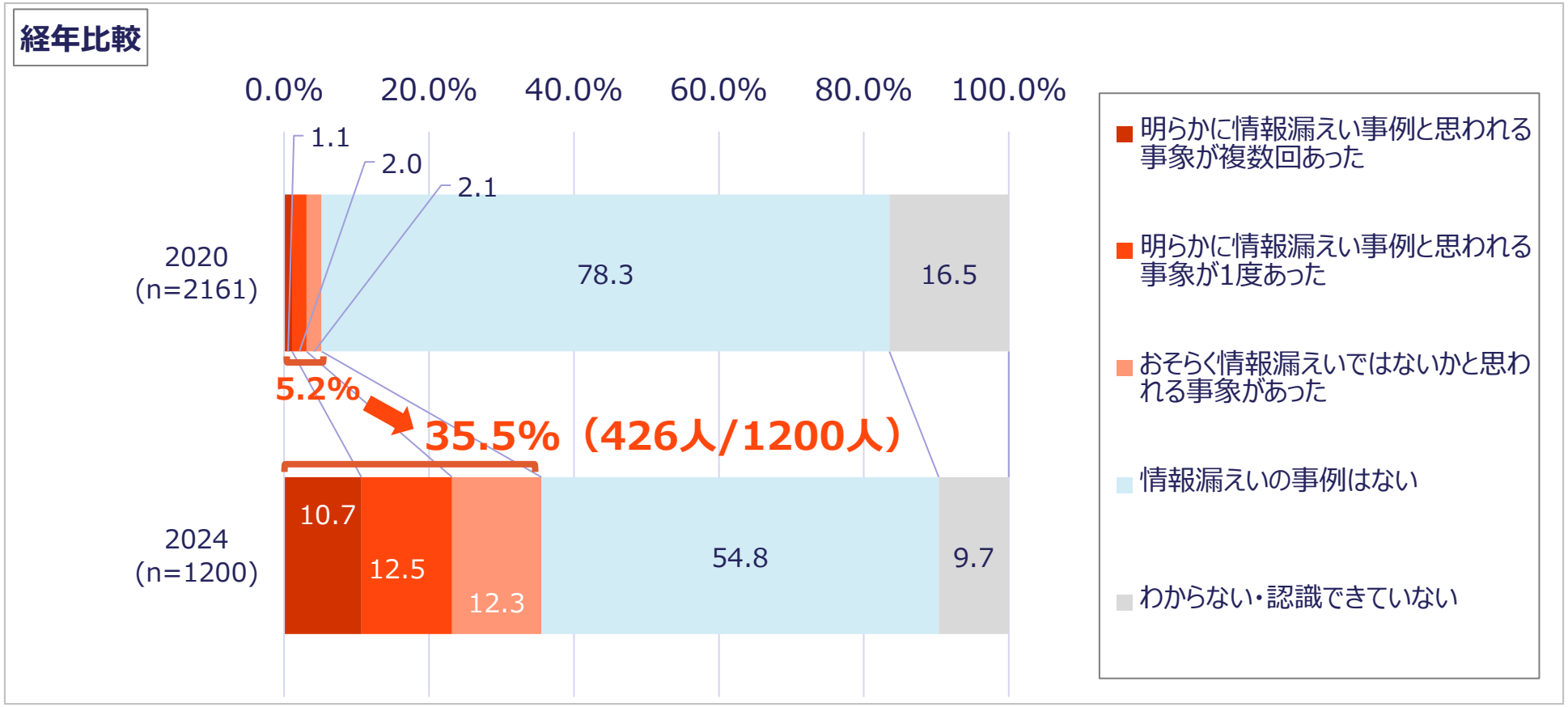
- 企業における営業秘密の漏えいの発生状況、漏えい対策等の実態を明らかにし、営業秘密漏えいを防ぐために有用な情報を提供することを目的とし、企業・組織のセキュリティ実務担当者や経営層を対象としたアンケートによる意識調査を実施。

調査期間	2025年1月23日～31日
調査方法	ウェブアンケート
調査数	1,200人
調査対象	企業の「情報システム関連部門」、「リスクマネジメント関連部門」、「サイバーセキュリティ関連部門」、「経営企画部門」、「経営層」、「その他セキュリティやリスクマネジメントに関する業務を実施している部門」に属する方
調査内容	• 営業秘密の漏えいの実態（漏えい有無、漏えい先等） • 営業秘密管理の実態（脅威と対策必要性認識、情報管理、限定提供データの保有状況等） • 営業秘密管理において実施している対策（技術的対策、環境的対策、秘密保持契約等） • 最近の動向を踏まえた対策（サプライチェーン管理、クラウドサービス・生成AI利用時等） • 政府機関等の営業秘密管理に関する活動（各種ガイドライン、相談窓口事業等）

※本調査は、2020年度に実施した「企業における営業秘密管理に関する実態調査2020」（以下、2020年度調査）の継続調査である。
　当該調査は郵送アンケートで行われていたため、調査方法の違いが、経年比較で見られる選択比率の増減に影響している可能性がある。
※本資料における（SA）は単一回答、（MA）は複数回答を表す。

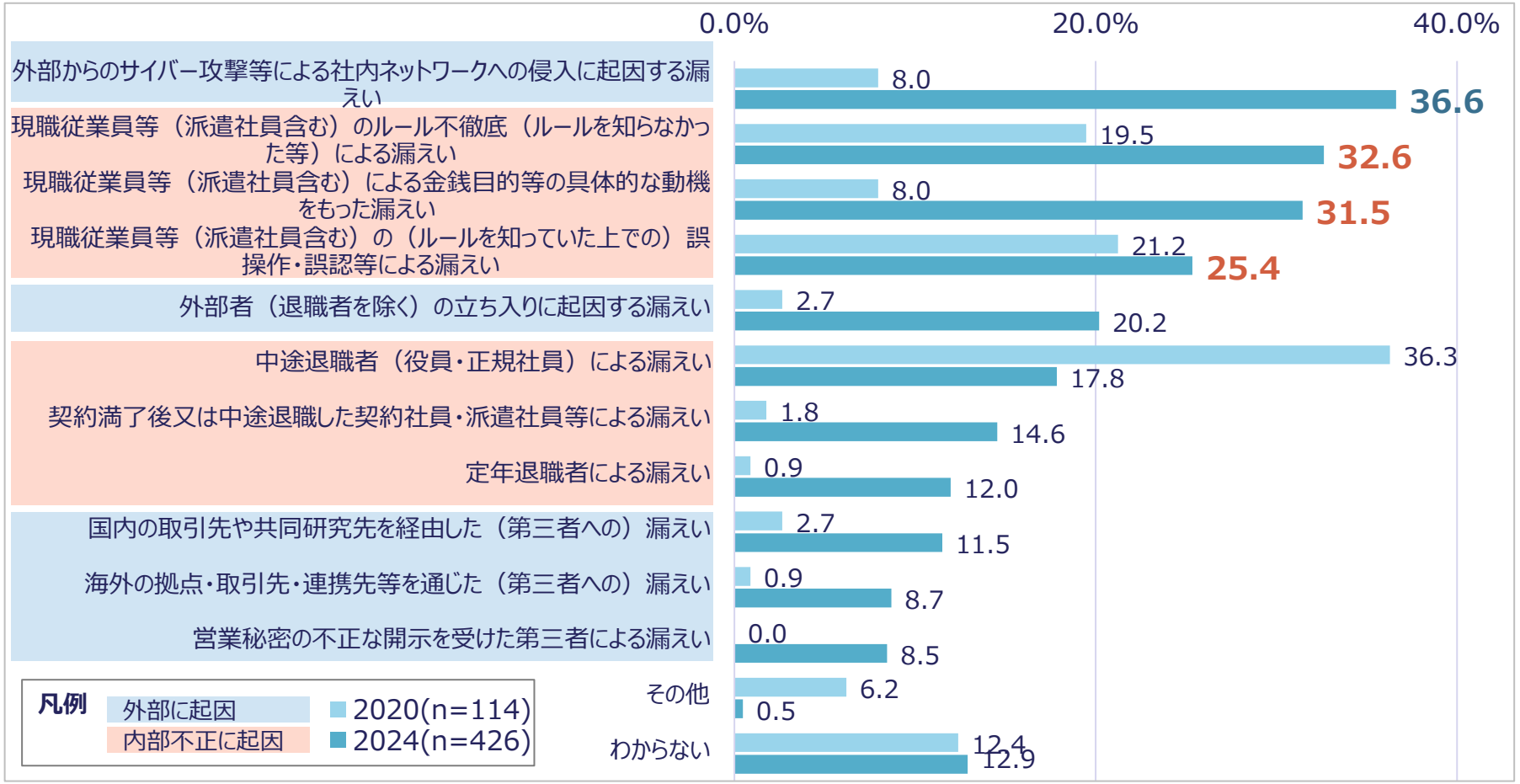
2024年度調査　結果紹介①　漏えい有無

- 過去５年以内の営業秘密の漏えい事例（SA）について、漏えい事例・事象を認識している割合は35.5%であり、2020年度調査と比較して認識割合が大幅に増加している。



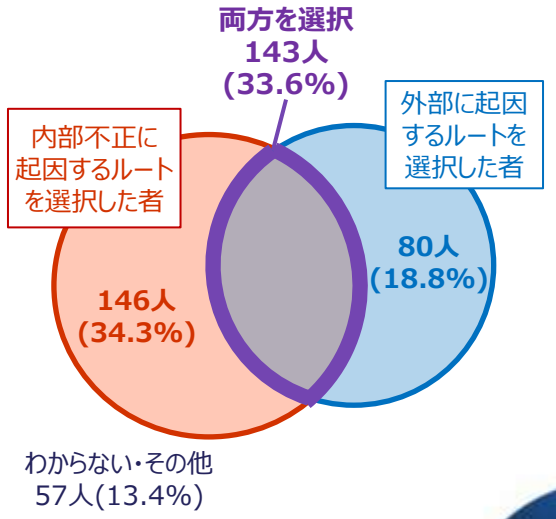
2024年度調査　結果紹介②　漏えいルート

- 営業秘密の漏えいのルート（MA）について、外部からのサイバー攻撃等に起因する漏えい（36.6%）が大幅に増加している。次いで、現職従業員等のルール不徹底（32.6%）、金銭目的（31.5%）、誤操作・誤認等（25.4%）の内部不正相当の割合が上位を占めている。



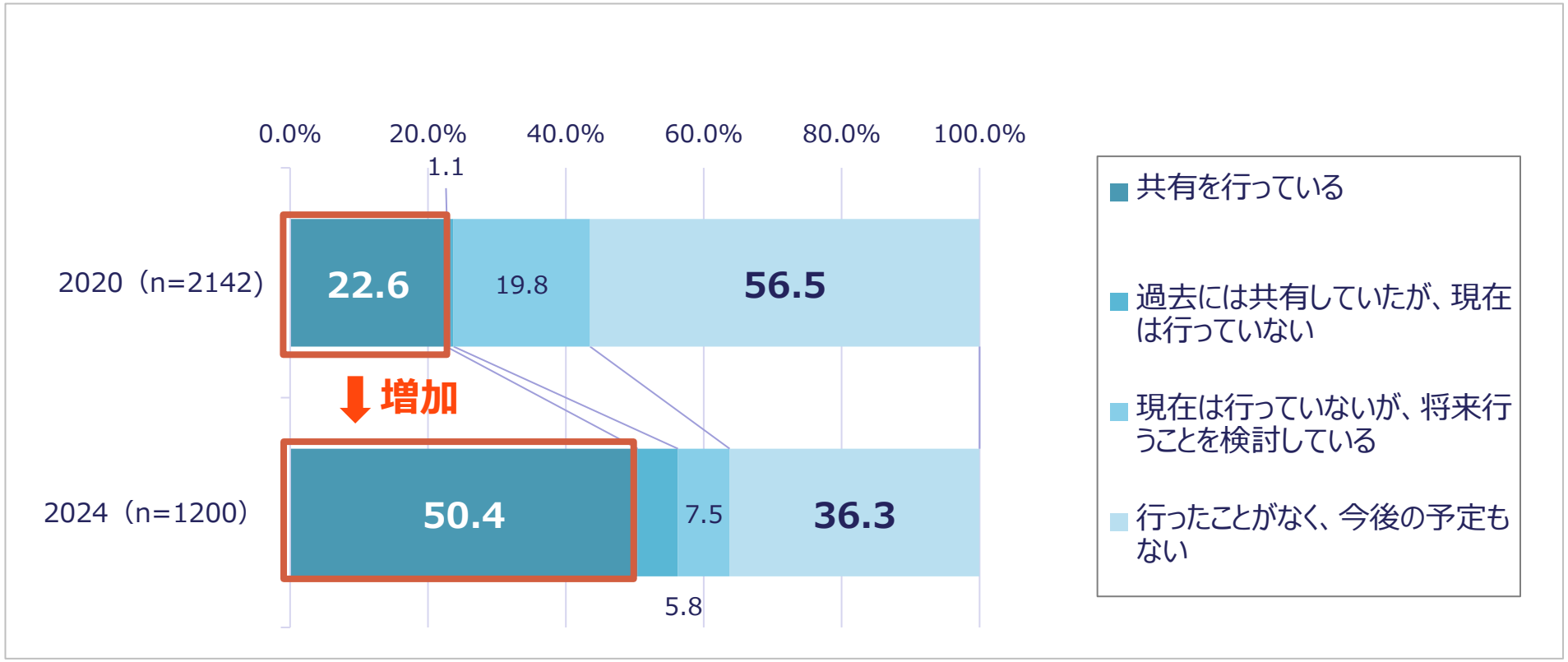
（9/10公開の白書に掲載）

➢ 漏えい事例を認識していた426人が、
・内部不正に起因するルートと、
・外部に起因するルート
どちらを選んだか



2024年度調査　結果紹介③　クラウドを利用した秘密情報の共有

- クラウドを利用した秘密情報の共有を実施している割合（SA）は50.4%、2020年度調査と比較して大幅に増加している。



2024年度調査　結果紹介④　内部不正を誘発する環境や状況

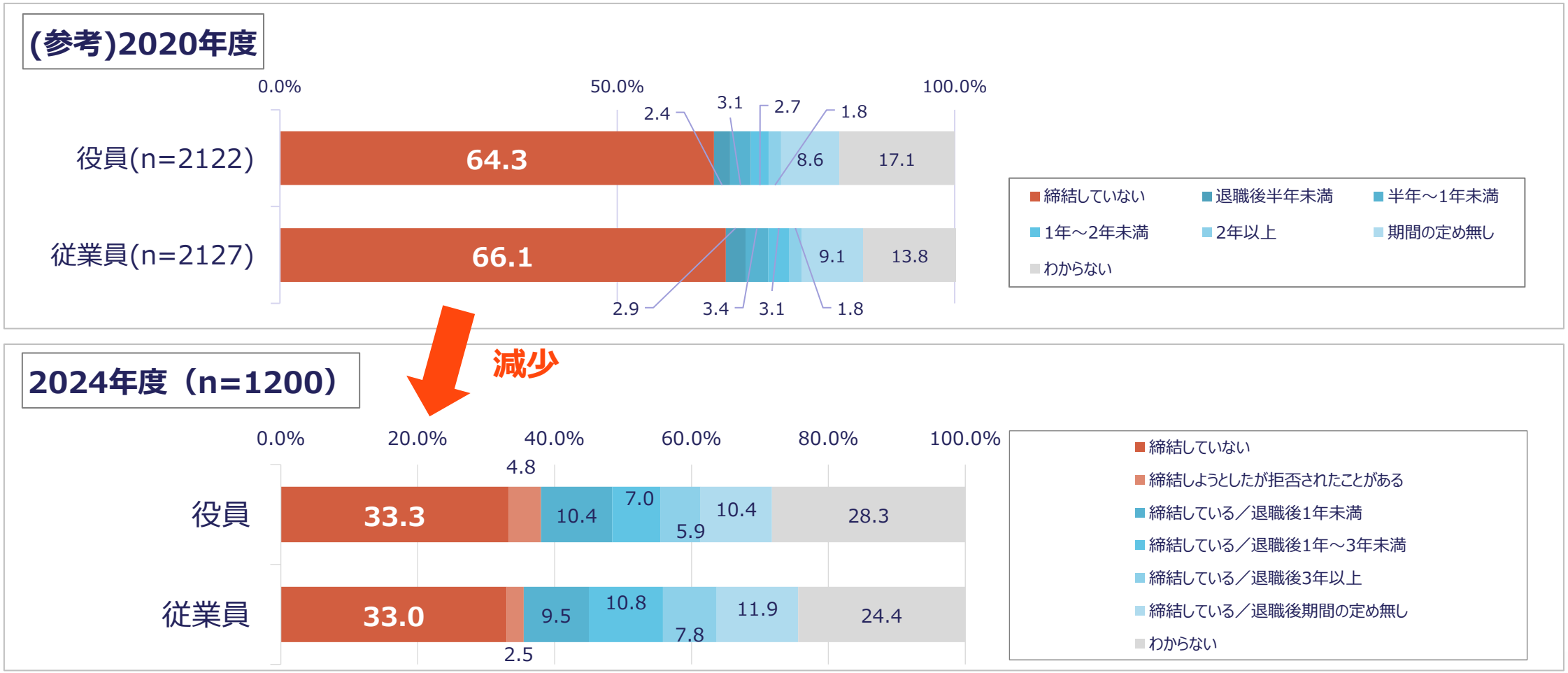
内部不正を誘発する環境や状況（MA）について

- 経営層では「当てはまる物はない」が最も高いが、「同じ業務を同じ人が長期継続」、「少ない人数で業務を回している」を内部不正誘発の要因と強く認識。
- 一方、サイバーセキュリティ部門やリスクマネジメント部門ではこれら以外にも、「人間関係等への恨みが大きい」「借金のある人が営業秘密を扱う」「弱みを握られて脅迫されている」も内部不正誘発の要因と認識。

部門別(%)		同じ業務を同じ人が長期継続	少ない人数で業務を回している	人間関係等への恨みが大きい	借金のある人が営業秘密を扱う	弱みを握られて脅迫されている	当てはまる物はない	回答したくない
全体　n=1200		36.8	39.5	21.2	10.3	6.8	26.1	6.2
部門別	企業における情報システム関連部門	46.2	38.9	21.0	11.9	7.6	22.2	7.9
部門別	**企業のリスクマネジメント計画・実践に関わる部門**	32.3	43.0	**37.3**	**18.4**	**10.1**	12.7	3.2
部門別	**企業のサイバーセキュリティに関わる部門**	40.5	48.1	**43.0**	**30.4**	**16.5**	7.6	2.5
部門別	経営企画部門	31.9	33.3	22.5	6.6	6.6	26.3	8.9
部門別	**経営層**	**32.0**	**38.7**	5.4	1.7	1.0	**45.1**	4.7
部門別	その他セキュリティやリスクマネジメントに関する業務を実施している部門	34.7	43.5	22.6	10.5	8.9	19.4	6.5

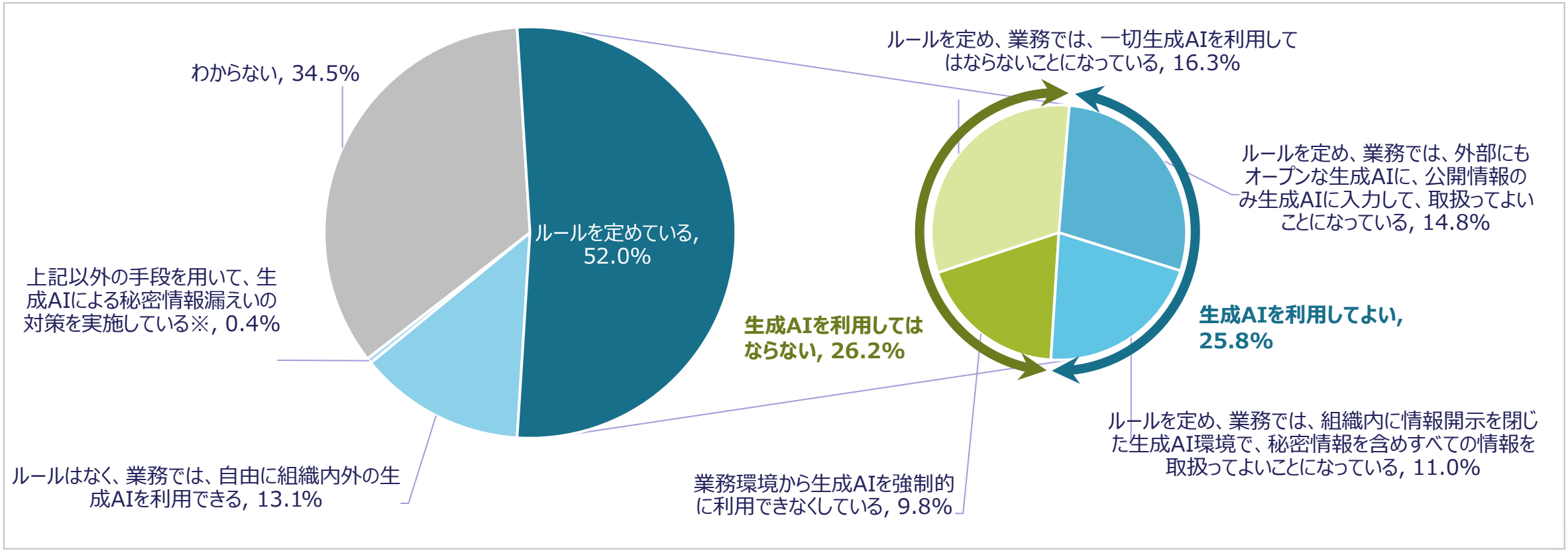
2024年度調査　結果紹介⑤　競業避止義務契約の締結状況

- 競業避止義務契約の締結状況（SA）について、締結していない割合は、役員、従業員ともに2020年度調査と比較して減少している。



2024年度調査　結果紹介⑥　生成AIの業務利用

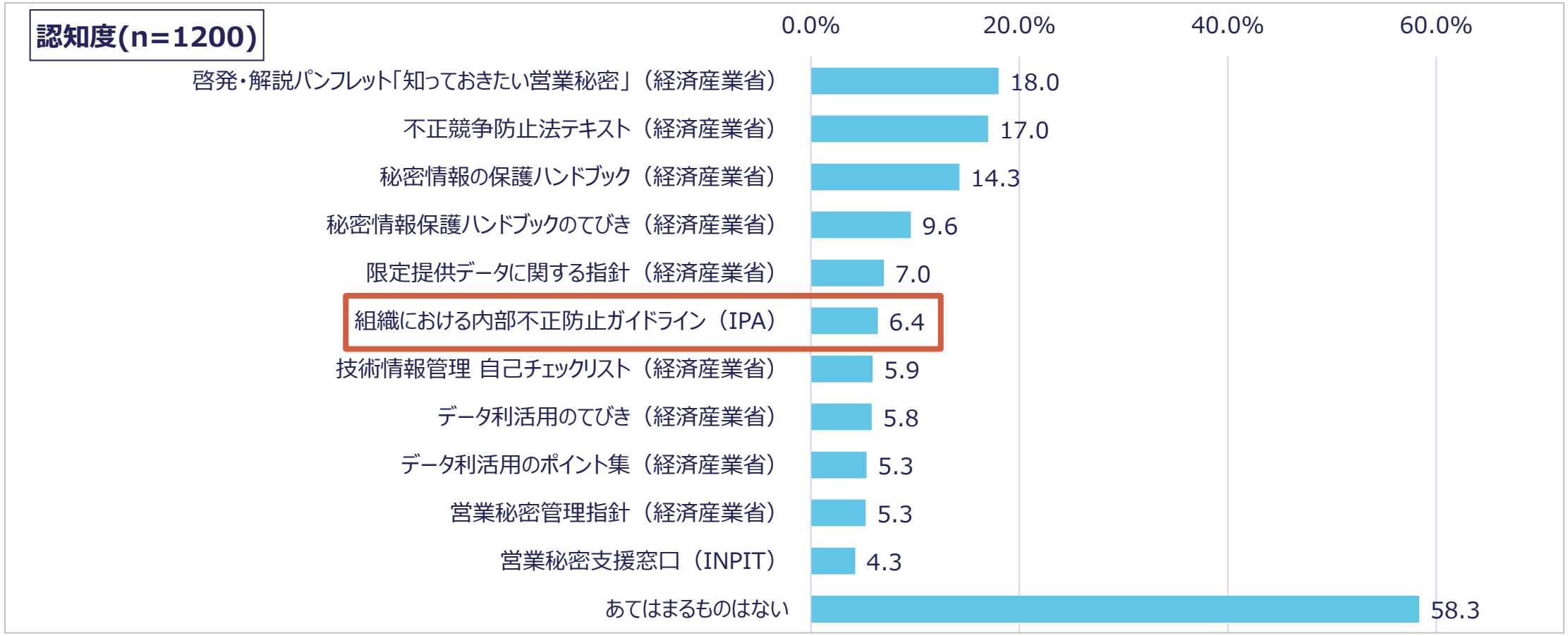
- 生成AIの業務利用可否（SA）について、何らかのルールを定めているのは52.0%。
- そのうち、生成AIを利用してよいこととしている割合は25.8%、利用してはならない割合は26.2%となっている。



※印を選択した場合は自由記述欄に追記。「利用が無い」旨や、「業務情報の種別から生成AIで扱う対象ではない」等の記述があった。

2024年度調査　結果紹介⑦　行政サービス等の認知度

- 行政サービス、ガイドライン等の認知度（MA）について、「知っておきたい営業秘密」が最も高く18.0%、次いで「不正競争防止法テキスト」が17.0%、「秘密情報の保護ハンドブック」が14.3%であった。



2024年度調査　まとめ

結果①、②
- 過去5年以内の**営業秘密の漏えい事例・事象を認識している割合は35.5%**に増加、営業秘密の漏えいルートでは**サイバー攻撃**だけでなく**内部不正相当**のルートも上位を占める。**サイバー対策と内部不正防止の両面**で対策に取り組む必要がある。

結果③、④
- **クラウドを利用した秘密情報の共有割合は50.6%**に増加するなど、**組織における情報の活用が進んでいる**傾向が見られる。一方、内部不正を誘発する環境や状況について**経営者と部門担当者のリスク認識に相違がある**。組織単位での対策に後れを取り、漏えい等につながるおそれがある。内部統制やリスク共有の仕組みを整備し、**経営トップから現場まで一貫したリスク認識**を持つ必要がある。

結果⑤
- **競業避止義務契約の締結は増加**しているものの、全般的に対策状況は大きく変わっておらず、違反を見つけられないリスクが依然残ると考えられる。**契約内容の管理と遵守の徹底、違反時の厳正な対応を組織的に進める**必要がある。

結果⑥
- 業務における生成AIの利用について、**何らかのルールを定めている割合は52.0%**。その内訳は、生成AIを利用してよい割合が25.8%、利用してはならない割合が26.2%となっている。各企業が**適切なルールを整備したうえで**生成AIを**適切かつ安全に利用していくことを一層促していく**必要がある。

結果⑦
- 行政サービス、ガイドライン等で知っているものについて、20%を超えるものはない。企業での対策実施を促すため、**官民連携よる継続的な普及啓発を推進する**必要がある。

今後の展望

- 組織における情報や新技術の活用が進んでいる
- 企業における営業秘密管理が十分とはいえない

- 企業での対策実施を促すために、本調査結果も活用し、官民連携による継続的な普及啓発を推進していく必要がある
  - 企業の営業秘密管理に資する有益な情報提供
    - 本調査の継続調査
    - 営業秘密の漏えいや管理の実態に関する深堀調査による取組み事例の作成
    - 監査や内部通報の仕組みとその有効性分析等の異なる視点での調査
  - 営業秘密を取り巻く情勢を踏まえた継続的な改善を促していく
    - 本調査結果をもとに、営業秘密管理の観点で、具体的かつ優先順位付けされた対策を検討
    - 「組織における内部不正防止ガイドライン」を改訂

参考情報

今回紹介した2024年度報告書のダウンロード等

- 報告書のダウンロード

  「企業における営業秘密管理に関する実態調査2024」報告書

  https://www.ipa.go.jp/security/reports/economics/ts-kanri/tradesecret2024.html

- 関連するガイドライン

  組織における内部不正防止ガイドライン

  https://www.ipa.go.jp/security/guide/insider.html

情報セキュリティ10大脅威
https://www.ipa.go.jp/security/10threats/10threats2026.html

- IPAが情報セキュリティ対策の普及を目的に2006年から毎年発行している資料
- 前年に発生したセキュリティ事故や攻撃の状況等から**IPAが脅威候補を選出**、セキュリティ専門家や企業のシステム担当等から構成される**「10大脅威選考会」が投票**、**TOP10入りした脅威を「10大脅威」**として脅威の概要、被害事例、対策方法等を解説

＜2026組織編　2026/1/29公表＞

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサム攻撃による被害	2016	11年連続11回目
2	サプライチェーンや委託先を狙った攻撃	2019	8年連続8回目
3	AIの利用をめぐるサイバーリスク	2026	初選出
4	システムの脆弱性を悪用した攻撃	2016	6年連続9回目
5	機密情報を狙った標的型攻撃	2016	11年連続11回目
6	地政学的リスクに起因するサイバー攻撃（情報戦を含む）	2025	2年連続2回目
7	内部不正による情報漏えい等	2016	11年連続11回目
8	リモートワーク等の環境や仕組みを狙った攻撃	2021	6年連続6回目
9	DDoS攻撃（分散型サービス妨害攻撃）	2016	2年連続7回目
10	ビジネスメール詐欺	2018	9年連続9回目

脅威に対して様々な立場の方が存在

立場ごとに注意すべき脅威も異なるはず

- 家庭等でパソコンやスマホを利用する人 **「個人」**

- 企業や政府機関などの組織
- 組織のシステム管理者や社員・職員 **「組織」**

「個人」と「組織」の２つの立場で脅威を解説

中小企業の情報セキュリティ対策ガイドライン
https://www.ipa.go.jp/security/guide/sme/about.html

- 中小企業の経営者や実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したガイドライン
- 本編2部と付録より構成
  - 経営者が認識すべき「3原則」、経営者がやらなければならない「重要7項目の取組」を記載（第1部）
  - 情報セキュリティ対策の具体的な進め方を分かりやすく説明（第２部）
  - すぐに使える「情報セキュリティ基本方針」や「情報セキュリティ関連規程」等のひな形を付録

映像で知る情報セキュリティ
https://www.ipa.go.jp/security/videos/list.html

2023年度制作映像

今、そこにある脅威
～内部不正による情報流出のリスク～

今、そこにある脅威
～組織を狙うランサムウェア攻撃～

華麗なる情報セキュリティ対策
（8話構成）

現在、計34本をYouTube内のIPA Channelで公開中。
主要な映像は動画ファイルでも配布。

[企業・組織向け] 内部不正対策、標的型攻撃、ビジネスメール詐欺、ランサムウェア対策、中小企業向け対策、新人研修など
[一般向け] ワンクリック請求、スマホセキュリティ、SNS利用の心得、パスワード、小学生、中高生向けなど

活用実績 (2025/3/31時点)

◆動画ファイルの2024年度申込数 ：

申込み**1,371件** 研修での受講予定者数： **約64万名**

◆インターネット動画再生回数： IPA Channelで全作品の累計 **約703万回**　2024年度は約81万回

参考　営業秘密の区分及び格付実施の有無（経年比較）

- 「営業秘密とそれ以外の情報とを区分しており、営業秘密に関してはさらに秘密性のレベルに応じて区分している」と「営業秘密とそれ以外の情報とを区分しているが、秘密性のレベルに応じた区分はしていない」を合わせた、営業秘密情報を区分して管理している割合は53.3%から61.5%に増加
- 「わからない」は7.4%から16.2%に増加

図　32 Q12 営業秘密の区分及び格付け実施の有無（経年比較）

※報告書から抜粋

参考：社内規程として定められた管理ルールの運用状況（経年比較）

- 「全体において厳密な運用が徹底されている割合」が2020年度調査の17.0%から20.6%に微増
- 一方で、「ある程度厳密に運用されている（部署やチーム等によって事情が異なる場合も含む）」、「厳密な運用を目指して改善の途中にある」及び「管理ルールを制定したのみ」の3項目は、2020年度調査から減少
- 「厳密な運用とはいえない」は14.9%から19.3%に微増し、「わからない」は2.1%から13.9%と大幅に増加

図 34 Q13 社内規程として定められた管理ルールの運用状況（経年比較）

※報告書から抜粋

参考：営業秘密対策実施上の課題

- 「対策のための人的リソースを割くことが難しいこと」、「技術的対策に要するコストが高額なこと」、「対策の費用対効果を明示しにくいこと」は、業種、従業員数、売上高、所属部門に関わらず、比較的共通の認識

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

(%)

		対策投資に関する経営層の承認を得ることに苦労すること	対策のための人的リソースを割くことが難しいこと	技術的対策に要するコストが高額なこと	対策の費用対効果を明示しにくいこと	電子メールで授受される営業秘密の管理が徹底されていないこと	テレワーク(在宅勤務等)やビデオ会議、クラウドサービスの利用、コラボレーションツールの利用等、新たな業務環境における適切な対策の見極めができていないこと	従業員に秘密情報管理のルール遵守を徹底させることが難しいこと	従業員の私物端末における対策の徹底が難しいこと	海外の拠点等で秘密情報管理のルール遵守を徹底させることが難しいこと	顧客・取引先から提供された営業秘密情報の管理にあたり、顧客等から過剰に厳しい対策を要求されること	自社の営業秘密情報を委託先や協業先に提供する場合に、秘密保持契約を締結しても効果が不明なこと	自社で利用する情報システムやサービスの特権管理者による内部不正を完全に防ぐのが難しいこと	自社の役員による内部不正を完全に防ぐのが難しいこと	退職者の追跡が難しいこと	その他	わからない	問題は特にない
合計		8.	16.6	13.9	15.	13.9	16.8	16.8	16.2	9.2	10.6	12.4	12.3	10.9	13.7	−	6.4	21.3
業種	製造業	9.	19.3	15.5	15.	16.5	19.8	20.7	16.8	12.2	12.2	14.5	15.7	12.3	15.8	−	5.8	15.2
	非製造業	6.	13.8	12.3	14.	11.3	13.8	12.8	15.5	6.2	9.0	10.3	9.0	9.5	11.5	−	7.0	27.3
従業員数	301 人以上	10.	18.8	14.2	15.	16.8	22.0	18.5	18.2	12.5	12.8	16.7	17.2	13.8	16.2	−	8.3	12.8
	300 人以下	5.	14.3	13.7	14.	11.0	11.7	15.0	14.2	5.8	8.3	8.2	7.5	8.0	11.2	−	4.5	29.7
従業員数・業種	従業員数 301 人以上かつ製造業	14.	22.3	17.3	16.	20.0	25.7	23.0	19.0	16.7	14.7	20.7	23.0	14.7	18.0	−	7.0	8.3
	従業員数 300 人以下かつ製造業	4.	16.3	13.7	15.	13.0	14.0	18.3	14.7	7.7	9.7	8.3	8.3	10.0	13.7	−	4.7	22.0
	従業員数 301 人以上かつ非製造業	7.	15.3	11.0	14.	13.7	18.3	14.0	17.3	8.3	11.0	12.7	11.3	13.0	14.3	−	9.7	17.3
	従業員数 300 人以下かつ非製造業	6.	12.3	13.7	14.	9.0	9.3	11.7	13.7	4.0	7.0	8.0	6.7	6.0	8.7	−	4.3	37.3
売上高	10 億円以下	4.	13.1	13.1	12.	7.7	9.5	12.9	12.9	2.8	7.2	7.2	5.4	6.4	8.2	−	5.1	39.6
	10 億円超～100 億円以下	6.	17.7	11.9	14.	16.5	14.2	18.8	19.2	8.8	8.8	11.9	11.2	10.0	17.7	−	6.5	12.3
	100 億円超～1,000 億円以下	11.	18.3	15.0	16.	17.2	21.6	17.6	18.3	12.5	15.0	13.2	17.2	13.2	12.8	−	6.2	12.8
	1,000 億円超～5,000 億円以下	10.	17.9	13.2	15.	18.9	22.6	18.9	10.4	11.3	11.3	20.8	17.9	11.3	18.9	−	7.5	10.4
	5,000 億円超	13.	19.2	17.4	19.	15.7	26.2	19.8	19.2	17.4	13.4	18.6	18.6	18.6	18.0	−	8.7	13.4
所属部門	企業における情報システム関連部門	10.	19.5	14.3	17.	13.1	20.4	20.1	16.4	11.9	11.9	12.8	15.2	12.5	12.8	−	11.2	16.7
	企業のリスクマネジメント計画・実践に関わる部門	15.	22.8	16.5	16.	17.7	22.8	22.8	25.9	20.3	17.1	20.3	20.9	21.5	18.4	−	0.6	6.3
	企業のサイバーセキュリティに関わる部門	13.	20.3	19.0	19.	29.1	32.9	17.7	15.2	12.7	19.0	21.5	20.3	16.5	22.8	−	3.8	5.1
	経営企画部門	5.	11.7	12.2	12.	14.6	16.4	18.8	13.1	4.2	8.5	9.9	10.8	8.9	14.6	−	7.0	17.8
	経営層	2.	12.5	12.1	13.	7.4	7.7	10.1	11.8	4.0	5.4	8.4	5.1	3.4	8.4	−	4.0	45.5
	その他セキュリティやリスクマネジメントに関する業務を実施している部門	6.	16.9	13.7	12.	16.1	12.1	12.1	19.4	6.5	9.7	9.7	8.9	11.3	15.3	−	7.3	10.5

※報告書から抜粋

参考：営業秘密の漏えいに気付くための技術的対策

- 2020年度調査と比較すると、営業秘密の漏えいに気付くための技術的対策を実施しているとする「実施しており、従業員等にも周知されている」及び「実施しているが、従業員等には周知していない」の割合が減少
- 「実施することを検討中」、「実施しておらず、今後の予定もない」、「わからない」は増加

- 実施しているあるいは実施することを検討している技術的対策で、最も実施率が高かったのは「ウイルス対策ソフトの導入」

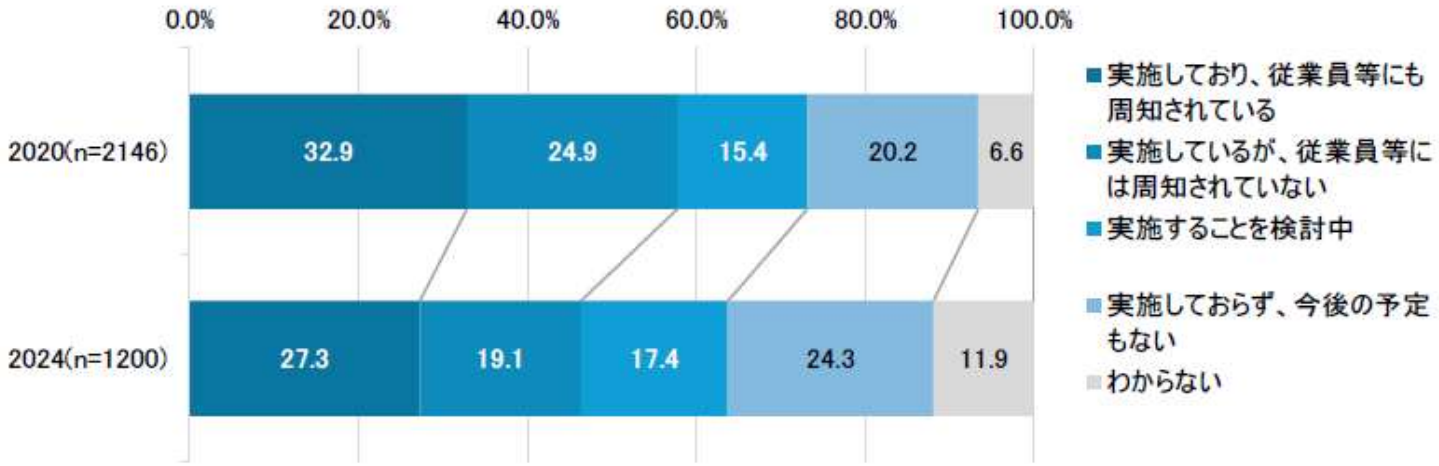


図 45 Q16 営業秘密の漏えいに気付くための技術的対策の実施（経年比較）

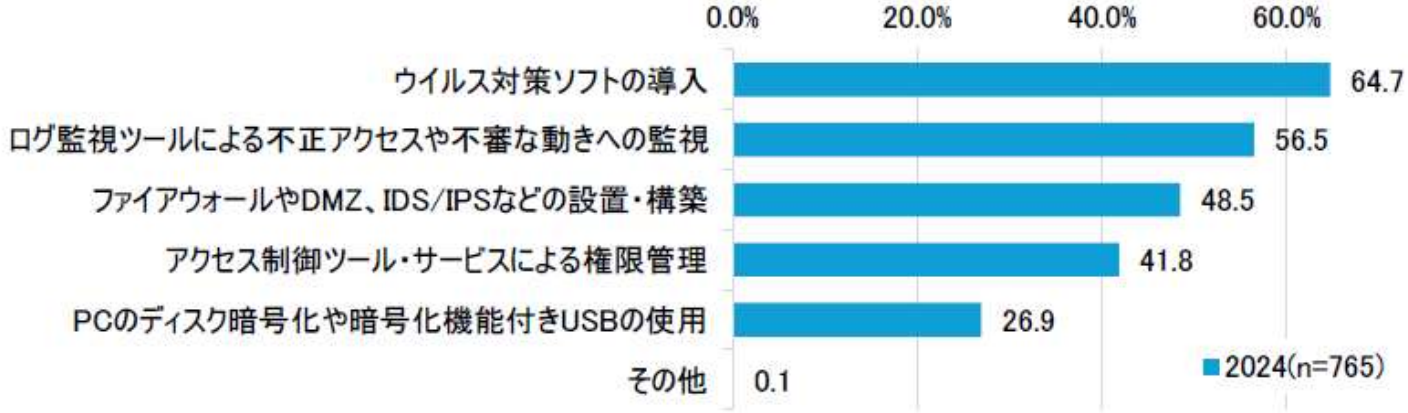


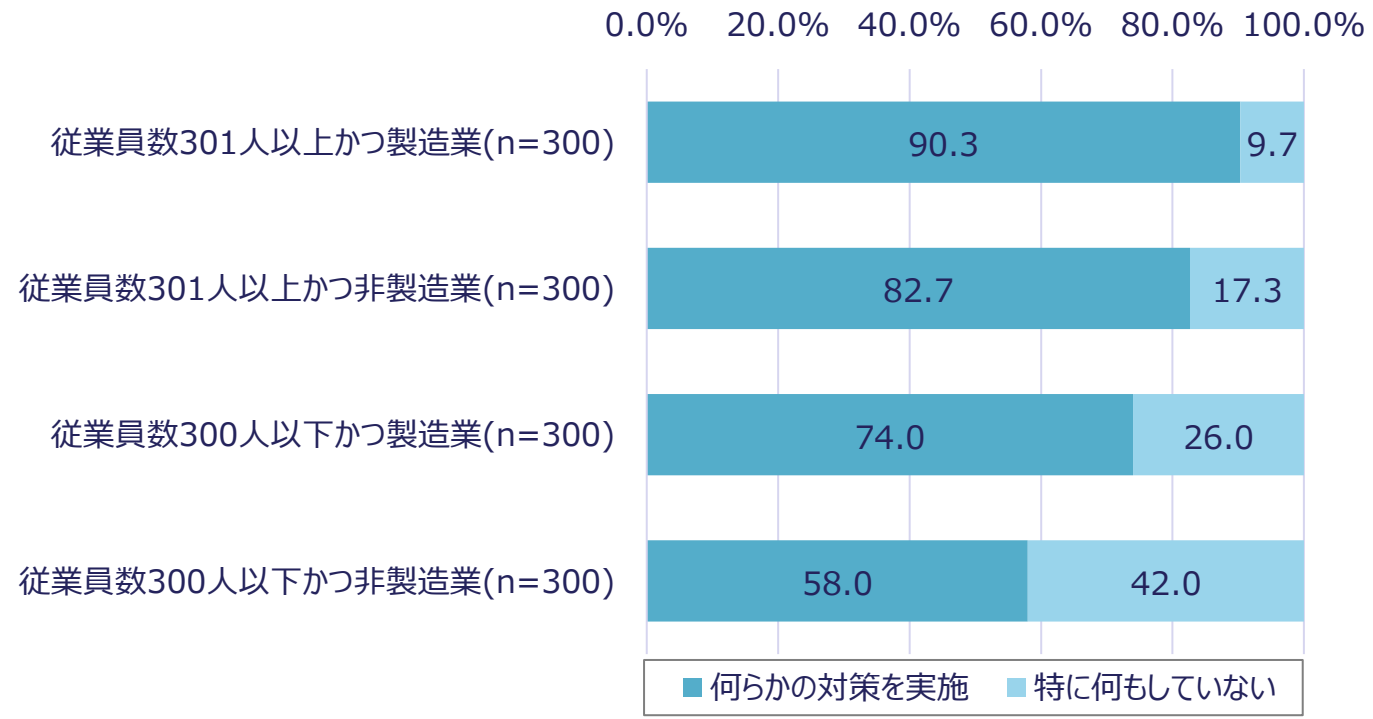
図 46 Q17 実施しているあるいは実施することを検討している技術的対策 (MA、n=765)

※報告書概要から抜粋

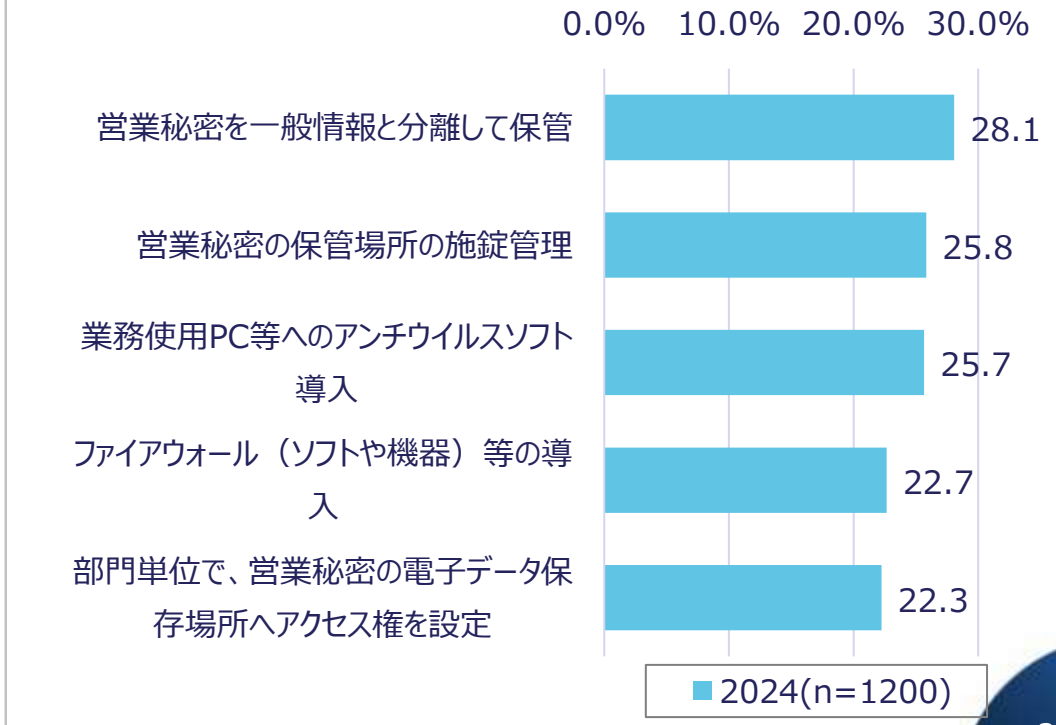
参考　営業秘密情報への不正アクセス防止策として実施している対策

- 不正アクセス防止の実施状況について、従業員数301人以上の製造業は何らかの対策を実施している割合が90.3%であり、従業員数が多い製造業ほど対策を実施している。
- 実施している対策は「営業秘密を一般情報と分離して保管」が最も高くなっている（28.1%）。

従業員数・業種別

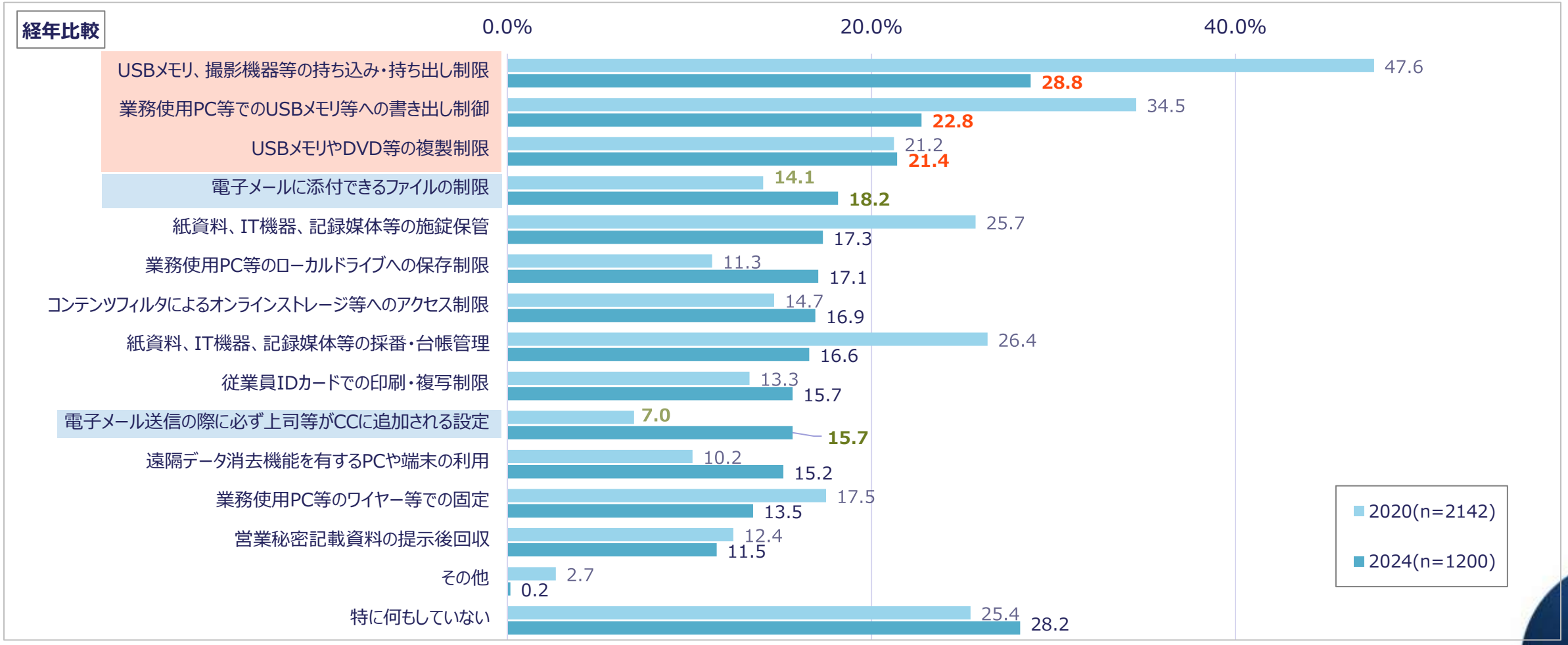


実施されている対策　上位5つ



参考：社外への不正持出防止策として実施している対策

- 社外への不正持出防止策の実施状況について、USBメモリ等の利用に関する対策が比較的多く実施されている。電子メールに関する対策実施の割合は2020年度調査と比較して微増。



※報告書から抜粋

参考：営業秘密の漏えいを生じさせにくい環境を作るための実施策

- いずれも実施率が高くても20~30%程度
- 2020年度調査と比較すると、「職場の整理整頓、不要文書廃棄」、「情報システムのログの記録・保管と周知」、「防犯カメラ設置と周知」、「従業員への社員証や名札等の着用義務付け」が減少
- 2020年度調査と比較すると、「従業員による不正検知が容易な座席レイアウトの工夫」、「特に何もしていない」は増加

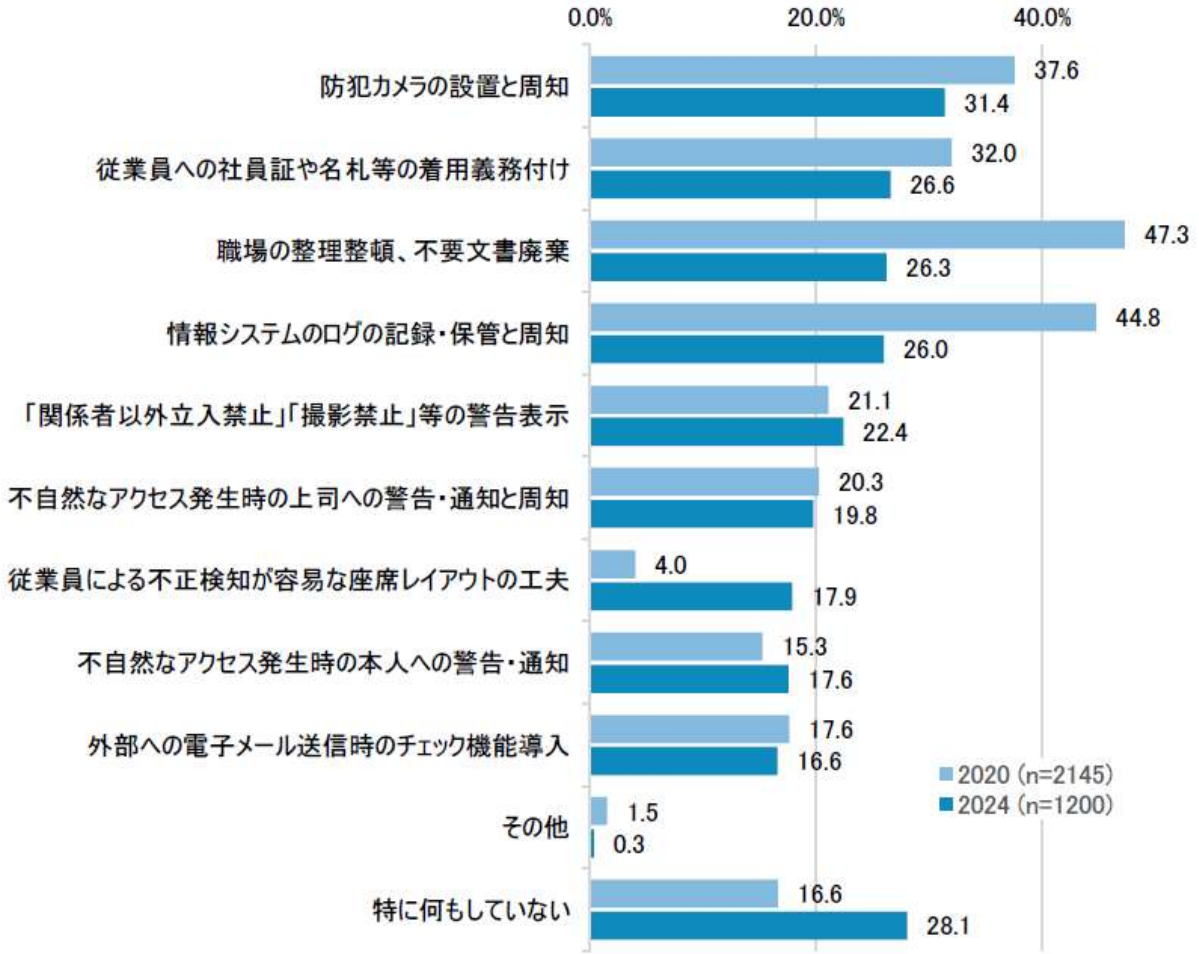


図 52 Q20 営業秘密の漏えいを生じさせにくい環境をつくるために実施している対策（経年比較）