「内部不正防止対策・体制整備等に関する中小企業等の状況調査」概要説明資料

2024年3月15日

作成：株式会社NTTデータ経営研究所
編集：情報処理推進機構

はじめに

【調査の背景】

企業が保有する秘密情報 の管理と保護は企業経営上の重要な課題であり、独立行政法人情報処理推進機構（以後、「IPA」という）では2021年度に「組織における内部不正防止ガイドライン」（以後、「内部不正防止ガイドライン」という）を第5版に改訂し、内部不正による情報漏えいの防止に資する情報提供を実施した。さらに、IPAでは、2022年度に「企業における内部不正防止体制に関する実態調査」（以下「2022年度調査」という）を実施したが、その調査結果から以下の問題点が浮き彫りになった。

- 内部不正防止対策に対する重要性の認識不足
- 中小企業等における取組の遅れ

さらには、今後の課題として次の3点が導出された

- 内部不正防止が「重要な経営課題」として認識されていない
- 営業秘密は各社の業務に依存するため定義が難しく、守るべき情報資産を特定できていない
- サイバーセキュリティ対策を講じているものの、内部不正対策は後手に回っている

これらの課題が特に中小企業等において顕著である。中小企業等の規模やリソースを考慮すると、情報セキュリティ対策と内部不正防止対策に別々に取り組むことは難しいことが想定される。

【調査の目的】

「組織における内部不正防止ガイドライン」の公開等によっても中小企業等の内部不正防止対策および体制整備が進展していないことから、本事業では、体制整備を進展させる改善策を整理した上で、実態調査を通じて、改善策の実施状況や関連する好事例を明らかにし、現状を改善するための今後の方向性を検討することを目的とした。そしてこの目的を実現するため、中小企業等における内部不正防止に対する経営者の意識向上、基本方針の策定、体制の整備、教育・リテラシー構築、実効性のある対策の実施が進展しない実態、及びこれらを進展させることができた企業の経営について調査を実施した。

目次

1. 調査方針
1-1. 調査のフレームワーク設定

本調査は、次の3項目で構成される調査フレームワークを適用して、実施した：

i. インタビュー調査及びアンケート調査の調査項目（調査票の質問項目）にしっかりとした一貫性を持たせるため、共通の調査軸を作業全体で適用

ii. 各調査軸に対し、インタビューとアンケートで共通して、改善策と現状の比較／好事例を抽出するための調査項目（設問）を設定
→昨年度は「現状・実態に対する仮説」であったところ、今年度は一歩進めて「企業の内部不正防止を改善する手段」の整理と実施状況を確認

iii. 各調査軸ごとに、インタビュー調査項目とアンケート調査項目を対比しながら同時に設計することで、両者で一貫した「改善策と現状の比較／好事例抽出、および改善策を補う示唆の導出」を実施

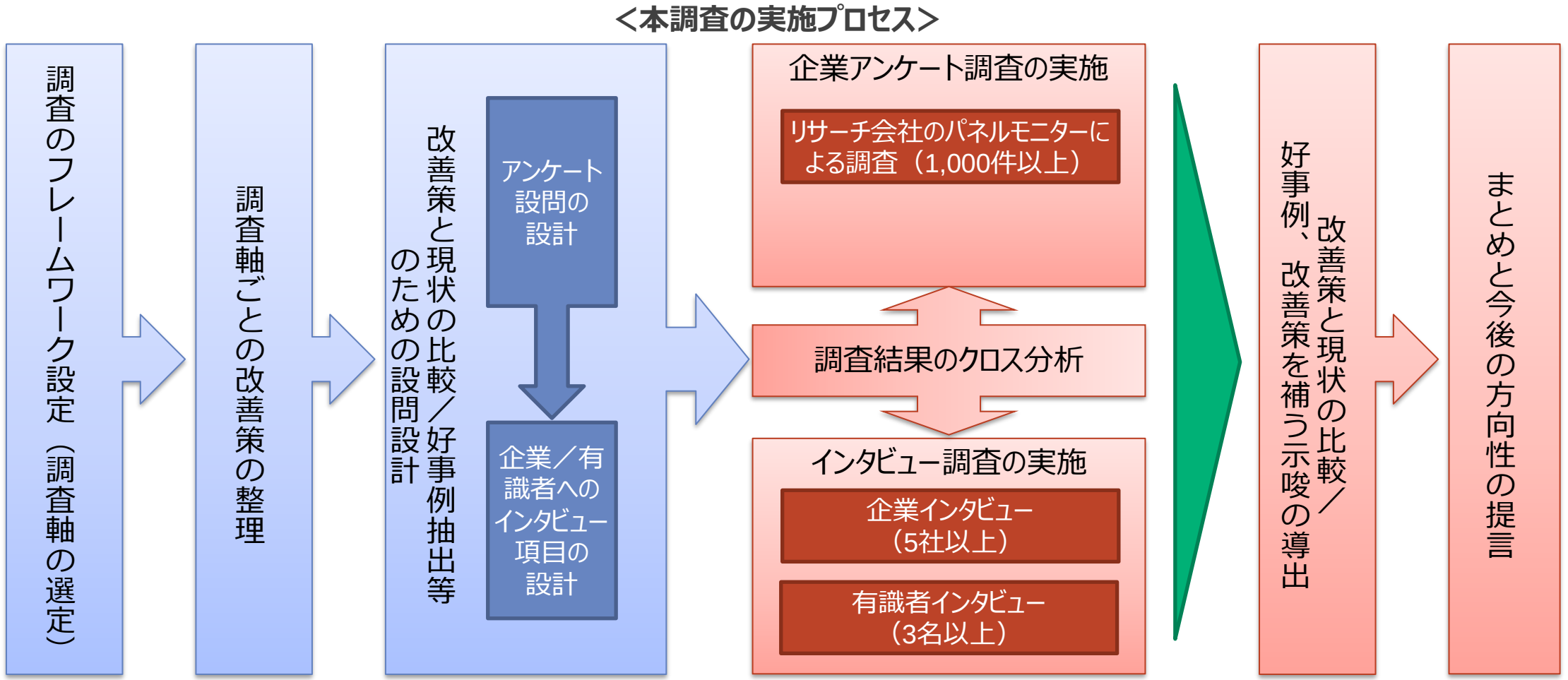
本調査では、次の７つの「共通の調査軸」を設定した。

① 経営課題の改善
② 重要な秘密の特定と取扱いの改善
③ 組織体制・連携に関する課題の改善
④ 社員教育とリテラシー構築に関する課題の改善
⑤ 対策実施に関する課題の改善
⑥ 中小企業の構造的課題の改善
⑦ ガイドラインの利用と実践に関する課題の改善

共通の調査軸を用いたインタビューおよびアンケートの実施プロセス（イメージ）について、次ページに示した。

1-2. 調査プロセス

本調査では、「調査軸ごとの改善策の整理」から「改善策と現状の比較等」「まとめ」に至る一連の作業の全てを、共通の調査軸に基づいて実施した。調査軸ごとに整理した改善策については、インタビュー調査、アンケート調査およびそれぞれの結果のクロス分析によって、調査軸ごとに現状との比較を行った。さらに現状の改善に役立てるため、好事例や、改善策を補う示唆の抽出も実施した。



1-2. 調査プロセス（続き）

本調査では、一連の作業の全てを、共通の調査軸ごとに実施した。

＜共通のフレームワークを適用した作業実施のイメージ＞

調査軸ごとの一貫した調査・分析

共通の調査軸	改善策の整理	インタビュー調査（企業・有識者）	アンケート調査（企業）	改善策と現状の比較／好事例、改善策を補う示唆の抽出	総括・提言
経営課題の改善	経営課題の改善策	経営課題改善に関するインタビュー結果	経営課題改善に関する設問の回答	調査結果の比較、分析による経営課題の改善策と現状の比較／好事例、改善策を補う示唆の導出	まとめと今後の方向性の提言
重要な秘密の特定と取扱いの改善	重要秘密特定／取扱いに関する改善策	重要秘密特定／取扱いの改善に関するインタビュー結果	重要秘密特定／取扱いの改善に関する設問の回答	調査結果の比較、分析による重要秘密特定／取扱いに関する改善策と現状の比較／好事例、改善策を補う示唆の導出	
組織体制・連携に関する課題の改善	組織体制・連携に関する改善策	組織体制・連携の改善に関するインタビュー結果	組織体制・連携の改善に関する設問の回答	調査結果の比較、分析による組織体制・連携に関する改善策と現状の比較／好事例、改善策を補う示唆の導出	
社員教育とリテラシー構築に関する課題の改善	教育・リテラシーに関する改善策	教育・リテラシー改善に関するインタビュー結果	教育・リテラシー改善に関する設問の回答	調査結果の比較、分析による教育・リテラシーに関する改善策と現状の比較／好事例、改善策を補う示唆の導出	
対策実施に関する課題の改善	対策実施に関する改善策	対策実施の改善に関するインタビュー結果	対策実施の改善に関する設問の回答	調査結果の比較、分析による対策実施に関する改善策と現状の比較／好事例、改善策を補う示唆の導出	
中小企業の構造的課題の改善	中小企業の課題に関する改善策	中小企業の課題改善に関するインタビュー結果	中小企業の課題改善に関する設問の回答	調査結果の比較、分析による中小企業の課題に関する改善策と現状の比較／好事例、改善策を補う示唆の導出	
ガイドラインの利用と実践に関する課題の改善	ガイドライン利用・実践に関する改善策	ガイドライン利用・実践の改善に関するインタビュー結果	ガイドライン利用・実践の改善に関する設問の回答	調査結果の比較、分析によるガイドライン利用・実践に関する改善策と現状の比較／好事例、改善策を補う示唆の導出	

2.調査軸ごとの改善策の整理(1/6)

各調査軸に対し、本調査によって実践状況の把握を試みる改善策を整理した（下表参照）。

具体的には、秘密情報の漏えいに関する内部不正防止の取組を改善する改善策を列挙した上で、それらの施策の実践状況を調査した。実践の割合が低い施策があれば、問題点・課題の背景要因であると推定されると同時に、その施策を推進することで状況の改善につながると考えられる。

調査軸	#	課題 ⇒ 改善策
経営課題の改善	1-1	経営層、内部不正防止に関する組織全体の責任者等が、重要な営業秘密等（個人情報以外）の漏えい／内部不正リスクを重要な経営課題として認識する必要がある。 ⇒法務・知財部門（社外の法律相談サービスを含む）の協力を得る等の取組を検討して、営業秘密等の漏えい事件（事例）から、事業リスクとしての重要性や当事者がしてはならないこと等を率先して学ぶ。
	1-2	経営層が内部不正防止対策に係るリーダーシップを十分に発揮し、内部不正防止の必要性を従業員に広く認識させる必要がある。 ⇒経営層によるセキュリティ確保のリーダーシップ発揮の機会／場を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。
	1-3	関連する取組を集約し、内部統制の効率化と強化を実現することが望ましい。 ⇒重要情報漏えいのリスクマネジメント体制の下で、サイバーセキュリティと内部不正防止の両方をカバーする。
重要な秘密の特定と取扱いの改善	2-1	自組織にとって重要性／機密性の高い情報資産のうち、個人情報以外の情報（営業秘密、重要なデータ等）の特定と、その旨の表示を強化する必要がある。 ⇒経営層も積極的に関与して、事業リスクが高い（漏えいした場合のインパクトが大きい）営業秘密等を特定するための基準作り、従業員の営業秘密に対する対策意識の醸成、営業秘密の定期的な見直し等に取り組む。

2.調査軸ごとの改善策の整理(2/6)

（続き）

調査軸	#	課題 ⇒ 改善策
組織体制・連携に関する課題の改善	3-1	組織全体としての、内部不正防止における責任・権限を明確にし、主管部門（責任部門）と実際の当事者となる関連部門との連携について全般に底上げする必要がある。 ⇒責任部門自体（リスク・コンプライアンス部門等）と関連部門（情報システム部門：対策実施部門、法務・知財部門、営業・事業部門）が協働する体制の整備を検討する。
	3-2	情報システム部門は、法務・知財担当者との連携を強化し、情報システム担当者の重要情報／内部不正に関する法知識を深める必要がある。 ⇒対策を実施する情報システム部門が責任部門となる体制を取る場合は、知財・法務部門等と協力してガバナンスを確保する。
	3-3	社内で内部不正の予兆を検知し、インシデントが発生した際に報告するための体制を整備することで、インシデントの発生を低減し、発生時の影響も効果的に軽減する必要がある。 ⇒重要な秘密が不自然に取り扱われているところを目にしたら、上に報告するというリテラシーと、上に報告できない事情がある場合は内部通報ができる体制を構築する。
	3-4	経営層による不正であっても検知したら黙認することのないよう、経営の透明性を高める必要がある。 ⇒役職の高い者を特別扱いしないマネジメントシステムを構築し、体制を整備する。
社員教育とリテラシー構築に関する課題の改善	4-1	営業秘密保護に係る制度について、情報システム担当者に法務・知財の知識を浸透させることが重要である。 ⇒法務・知財部門の協力を得た教育・研修等によって、対策を担当する情報システム部門の重要情報漏えい／内部不正に関する法知識（不正競争防止法等）の理解を深める。
	4-2	営業秘密、重要なデータ等の知識を組織全体に根付かせる必要がある。 ⇒入社／人事異動／退職等の重要なタイミングで、具体的に重要な秘密を示して、何をしてはいけないのか、どのような時に上への報告が必要か等を周知・徹底する。
	4-3	従業員の意識を底上げし、重要な秘密を漏れなく特定・管理する必要がある。 ⇒事業や経営における重要性や価値、当該情報が漏えい・毀損等した場合の影響・損害などを踏まえた、秘密の重要度の判別基準を明文化した上で、この基準に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。
	4-4	既存の機会をうまく活用する等の実施しやすい方法で効率的に周知し、組織全体の基礎知識の底上げ・理解促進と従業員への抑止力を強化することが望ましい。 ⇒企業のサイバーセキュリティ／コンプライアンス等に関する取組の一環として、重要情報漏えい／内部不正防止の社内規程及びその規則、モニタリングの目的や実施状況等に焦点を当てる回数を増やす。
	4-5	教育・研修の実効性を高めるため、形式的なe-learningに留まらず、実効性の高い教育方法を取り入れる必要がある。 ⇒インシデント事例、解説動画・イラスト等のリッチコンテンツ、グループディスカッション、定期的な規則遵守のセルフチェック等を積極的に活用して理解を深める取組を推進すると共に、従業員に対し、営業秘密や限定提供データについて、何をしてはいけないのかを教育する。

2.調査軸ごとの改善策の整理(3/6)

（続き）

調査軸	#	課題 ⇒改善策
対策実施に関する課題の改善	5-1	情報漏えい対策の技術面を担当する情報システム部門においても、営業秘密保護の要点を集約できるような社内連携を行うことが望ましい。 ⇒情報システム部門と法務・知財部門が連携し、重要情報（営業秘密や限定提供データ等の知財を含む）漏えいへの対策に役立つ官民の関連ガイドライン／ハンドブックの情報を収集し、活用を進めることで、必要な対策を見直す。
	5-2	内部不正防止対策を強化する上で、従業員の行動監視、ログの記録と分析等は有用だが、従業員のプライバシーを侵害していると受け取られる恐れがあり、両者のバランスを適切に取る必要がある。 ⇒個人情報保護法の解釈に基づいて適切にバランスを取るための知見を得た上で、対策や教育に取り組む。
	5-3	サイバーセキュリティ対策と内部不正防止対策に資金やリソースを重複投資しないよう配慮し、効率的に対策を実施することが望ましい。 ⇒重要情報漏えい防止体制の下で、サイバーセキュリティ対策と内部不正防止対策の両方に一貫して取り組む。
	5-4	秘密情報漏えい対策の選定にあたっては、内部不正の脅威（例：従業員の超過勤務、ハラスメントや処遇等の不満、業績の詐称、会社等への怨恨による不正、離職前のデータ の持ち出し、転職先での情報利用等）を考慮し、経営層を含む中途退職者／中途採用者の内部不正対策を強化すると共に、内部不正リスクへの効率的・効果的な対策を実現する必要がある。 ⇒内部不正のリスクシナリオも加味して重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。この際には、不正に対する人的・組織的対策と技術的対策のバランスの適正化を考慮する。また、経営層の不正防止と透明性確保、アクセスログの確認範囲拡大、他社の重要情報の不正な社内持ち込み防止、重要プロジェクト就任／離任時にも秘密保持義務の誓約書を取得、重要性の高い秘密に触れる場合の誓約書の詳細度の変更等を実施する。
	5-5	重要情報の範囲が個人情報から技術情報・ノウハウ等にまで広がっている一方で、個人情報以外の漏えいに対するリスク認識が十分ではなく、技術情報・ノウハウ等の情報漏えい、及び内部不正防止の対策を強化する必要がある。 ⇒個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。
	5-6	情報漏えい対策として、中途退職・異動・昇格等によって不要になったアクセス権限の削除、不要になった秘密情報の削除等を適時に行い、不用意な秘密情報の漏えいを防ぐ必要がある。 ⇒情報機密区分に応じたアクセス権限付与状況の点検、アクセス権限付与者についての定期的な棚卸しを実施する。

2.調査軸ごとの改善策の整理(4/6)

（続き）

調査軸	#	課題 ⇒改善策
中小企業の構造的課題の改善	6-1-1	中小企業においても、重要な営業秘密等（個人情報以外）の漏えい／内部不正リスクを重要な経営課題として経営者等が認識し、秘密情報漏えい・内部不正防止の取組を効率的に改善する必要がある。 ⇒経営層または内部不正防止に関する組織全体の責任者等が率先して、重要な秘密情報漏えい／内部不正リスクを重要な経営課題として認識する機会を増やし、サイバーセキュリティ確保と内部不正防止を一体的に認識した経営を行う。
	6-1-2	中小企業においても、経営者等が内部不正防止対策に係るリーダーシップを十分に発揮し、内部不正防止の必要性を従業員に広く認識させる必要がある。 ⇒中小企業では、全社集会などの経営層が従業員に周知徹底する機会を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。
	6-2-1	特に中小企業において、守るべき情報資産を特定できていないことが懸念される。中小企業の規模では、この問題の改善にあたり、経営者等が積極的に関与することが望ましい。 ⇒中小企業では、経営層が自ら判断する、あるいは判断基準を示すことで、自社の事業にとって重要性／機密性の高い秘密情報を的確に特定する。
	6-3-1	組織全体としての、内部不正防止における責任・権限を明確にし、主管部門（責任部門）と実際の当事者となる関連部門との連携について全般に底上げする必要がある。 ⇒中小企業では、責任者である経営層が中心となって、総務・人事・法務や情報システム等の関連部門との調整を行う。
	6-3-2	情報システム部門は、法務・知財担当者との連携を強化し、情報システム担当者の重要情報／内部不正に関する法知識の理解を深める必要がある。 ⇒中小企業では、通常は法務・知財に一定の知識と経験を持つ経営層が全社責任を負うため、情報システム部門は技術面から経営層を支えることに集中することで、内部不正防止の強化に貢献する。
	6-3-3	社内で内部不正の予兆を検知し、インシデントが発生した際に報告するための体制を整備することで、インシデントの発生を低減し、発生時の影響も効果的に軽減する必要がある。 ⇒重要な秘密が不自然に取り扱われている様を目撃した際に上に報告することの徹底と、上に報告できない事情がある場合は内部通報ができる体制を構築する。
	6-3-4	経営層による不正であっても検知したら黙認することのないよう、経営の透明性を高める必要がある。 ⇒経営層を特別扱いしない内部不正防止体制を整備する。
	6-4-1	営業秘密保護に係る制度について、情報システム担当者に法務・知財の知識を浸透させることが重要である。 ⇒中小企業では、経営層のリーダーシップと社外の専門家（ITコーディネータ、弁護士・弁理士等）の協力により、情報システム部門や他の従業員に法務・知財の知識を広める。

2.調査軸ごとの改善策の整理(5/6)

（続き）

調査軸	#	課題 ⇒改善策
中小企業の構造的課題の改善	6-4-2	営業秘密、重要データの知識を組織全体に根付かせる必要がある。 ⇒中小企業では、入社／人事異動／退職等の重要なタイミングで、経営層が重要な秘密を具体的に示し、その取扱い指示を徹底する。
	6-4-3	従業員の意識と秘密の取り扱いを底上げし、重要な秘密を漏れなく特定・管理する必要がある。 ⇒経営層または経営層が権限を移譲した責任者が各々の秘密の重要度を指定した上で、この指定に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。
	6-4-4	既存の機会をうまく活用する等の実施しやすい方法で効率的に周知し、組織全体の基礎知識の底上げ・理解促進と従業員への抑止力を強化することが望ましい。 ⇒企業のサイバーセキュリティ／コンプライアンス等に関する取組の一環として、重要情報漏えい／内部不正防止の社内規程及びその規則、モニタリングの目的や実施状況等に焦点を当てる回数を増やす。
	6-4-5	形式的なe-Learningに留まらず、実効性の高い教育方法を取り入れることで、教育・研修の実効性を高める必要がある。 ⇒【6-4-5a】中小企業では、経営層が自ら事業リスクに基づいて、営業秘密や限定提供データの取り扱いについて何をしてはいけないのかを指示・啓発する。 ⇒【6-4-5b】中小企業では、経営層が全社集会などで直接従業員に教育・意識づけする。
	6-5-1	情報漏えい対策の技術面を担当する情報システム部門においても、営業秘密保護の要点を集約できるような社内連携を行うことが望ましい。 ⇒中小企業では、経営層と担当者が協力して、重要情報（営業秘密や限定提供データ等の知財を含む）漏えい対策に役立つ官民の関連ガイドライン／ハンドブックの情報を収集し、活用を進めることで、必要な対策を見直す。
	6-5-2	内部不正防止対策を強化する上で、従業員の行動監視、ログの記録と分析等は有用だが、従業員のプライバシーを侵害していると受け取られる恐れがあり、両者のバランスを適切に取ることが必要である。 ⇒経営層が積極的に従業員とコミュニケーションを取ることで、従業員の行動監視やログの記録・分析等に対する従業員の理解を得る。
	6-5-3	サイバーセキュリティ対策と内部不正防止対策に資金やリソースを重複投資しないよう配慮し、限られたリソースを効率的に活用して対策を実施することが望ましい。⇒中小企業では、重要情報漏えいの防止体制の下で、サイバーセキュリティと内部不正防止の両方に共通する対策を積極的に１つにまとめる。

2.調査軸ごとの改善策の整理(6/6)

（続き）

調査軸	#	課題 ⇒改善策
中小企業の構造的課題の改善	6-5-4	秘密情報漏えい対策の選定にあたり、限られた資金／リソースの範囲内で、内部不正の脅威（例：従業員の超過勤務、ハラスメントや処遇等の不満、業績の詐称、会社等への怨恨による不正、離職前のデータ の持ち出し、転職先での情報利用等）に効率的に対処する必要がある。 ⇒内部不正のリスクシナリオを加味した重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。
	6-5-5	重要情報の範囲が個人情報から技術情報・ノウハウ等にまで広がっているものの、これらの漏えいに対するリスク認識が十分ではなく、技術情報・ノウハウ等の情報漏えい、及び内部不正防止の対策を強化する必要がある。 ⇒個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。
	6-5-6	情報漏えい対策として、中途退職・異動・昇格等によって不要になったアクセス権限の削除、不要になった秘密情報の削除等を適時に行うことが必要である。 ⇒情報機密区分に応じたアクセス権限付与状況の点検、アクセス権限付与者についての定期的な棚卸しを実施する。
ガイドラインの利用と実践に関する課題の改善	7-1	IPAが公開している「組織における内部不正防止ガイドライン」には一定の認知度がある。しかし、IPAとの接点が希薄な傾向にある企業の法務・知財部門では十分に認知されていない可能性がある。読み解くには法的知識等が必要なガイドラインであるため、法務・知財部門でもガイドラインを認知してもらう工夫が必要である。他方、IPAとの接点が多い傾向にあり、ガイドラインを既に認知しているIT／セキュリティ部門との連携を強化することで、ガイドラインの活用を促進できる可能性がある。同時に、内部不正防止対策だけに特化した本ガイドラインは、情報漏えいに関する内部不正防止対策をセキュリティ対策の一環として位置付けている企業にとって、その存在が認知されにくいことが懸念される。 ⇒認知度・活用度合の高い「サイバーセキュリティ経営ガイドライン」「秘密情報の保護ハンドブック」「営業秘密管理指針」「限定提供データに関する指針」「経済安全保障の確保に向けて2022～技術・データ・製品等の流出防止～」との相互参照を進める。また、支援ツール開発や外部専門家派遣による適用開始支援等を検討する。
	7-2	「内部不正防止ガイドライン」は認知されていても、必ずしも活用はされていない。企業ニーズを踏まえ、活用しやすい啓発資料・補足資料等を追加することが望ましい。 ⇒概要版の作成、活用しやすい情報量の調整・表現の工夫、社内規程整備のために活用しやすい内容の増補、従業員への周知・教育にそのまま使えるコンテンツの充実等を検討し、「組織における内部不正防止ガイドライン」適用の実効性を高める。

3. 事例調査

事例調査は、①「メディア等の事例一覧サイト」を用いた調査対象事件の抽出・名寄せ及びリスト化、②記事・解説レポートとの照合による内容確認、③信憑性の高い情報ソースを用いた裏取りと調査結果の深掘り、④調査結果の分類および実態・特徴・違い等の比較分析 という手順に沿って実施した。

	①抽出・名寄せ・リスト化	②内容確認	③レビュー・深掘り	④結果の分類と分析
実施プロセス	**メディア等の事例一覧サイトを用いた調査対象事件の抽出および名寄せによるリスト化** 事件についての**粗情報の整理**　※整理のための項目は後述	リスト化された事件のそれぞれに対し、**対応する記事・レポートを検索し、内容を照合** 事件についての**情報整理のアップデート**	リスト化された事件のそれぞれに対し、信憑性が高い情報ソースを確認し、レビューを実施 事件についての**情報整理の深掘り**	**整理した事例を分類**（以下、例） ① 中小企業等と大企業 ② 発生した事象の種別（情報漏えい、他） ③ 漏えいした情報の種別（個人情報と営業秘密等） ④ 原因（内部不正、他）等 分類結果に基づき、**内部不正に起因する事件の実態や特徴、その他の事件との違い等を分析**
情報ソース等	**メディア等の事例一覧サイト**（前々ページの表参照）	マスコミによる**記事**、セキュリティベンダーによる**解説レポート**　等	**当事者企業・団体のリリース**（続報含む）、**公的機関が発表した情報**、有識者・学識経験者による**詳細で質の高い解説**、**裁判例**　等	–
ポイントとなる事項	■ **基本方針**の適用（前述） ■ 組織や個別事案ごとに**名寄せして整理** ■ 最終的に200件を確保できるように**余裕を持ってリスト化***（**候補としては、2割増しの240件程度をリストアップ**）	■ 対応する記事・レポートが見つからない場合は、状況によっては、リストから削除 ■ この段階で**新たに見つかった事例**については、**基本方針に照らして適宜追記**	■ 裁判例については、2020年度以降に公開されたもの（事件発生はこれより前の場合がありうる） ■ この段階で**新たに見つかった事例**については、**基本方針に照らして適宜追記**	■ 現状把握によって確かめる想定を予め準備 ■ 事例調査結果による現状把握により、想定を現状と比較し、一致／乖離を確認 ■ 想定の確認にあたり、上記の４分類を適用

4. アンケート調査の対象

企業において次の要件のうちいずれか１つを満たす者を対象として、企業アンケート調査を実施した。

i. 情報システム関連部門の担当者
ii. 情報システム関連部門を所掌・所管する部門の責任者
iii. リスクマネジメント計画・実践に関わる部署の担当者
iv. リスクマネジメント計画・実践に関わる部署を所掌・所管する部門の責任者
v. 経営企画部門のIT/セキュリティ戦略担当者
vi. 経営企画部門のIT/セキュリティ戦略担当を所掌・所管する部門の責任者
vii. 経営層
viii. ｉ～ｖｉ以外の部門でも、リスクマネジメントに関する業務を実施していると認識している担当者

■ 主たる調査対象者は、市場調査会社の大規模調査パネルに登録しているモニター（以下、「パネルモニター」という）から選定し、アンケートへの回答をWeb回答システムで取得した。

※厳密には、回答は所属企業の現状に基づく個人の見解と想定

5. インタビュー調査の対象

国内の中小企業の経営者／経営幹部等

次の7つの要件のうち、1つ以上に合致している国内の中小企業8社の経営者／経営幹部等に対して、インタビュー調査を実施した。

i. 内部不正対策に積極的と目される企業
ii. 実効性のある内部不正リスク管理態勢を整備していると目される企業
iii. 内部不正リスクを重要な経営課題の一つとして取組、公表している企業
iv. 個人情報に留まらず企業の重要情報や営業秘密情報等を適切に分別、管理していると目される企業
v. セキュリティ対策に積極的と目される企業
vi. 営業秘密に係る内部統制が充実していると目される企業
vii. 限定提供データなどの新たな秘密情報の保護・活用に積極的と目される企業等

インタビュー先の中小企業は、主としてITベンチャー企業、サプライヤ企業等から選定した。

有識者

内部不正防止や営業秘密管理に関する有識者や法律の専門家に対してインタビュー調査を実施した。インタビュー対象とする有識者として、以下の３要件のうち１つ以上に合致する専門家を4名選定した。

i. 最新の法制度の動向に詳しい専門家
ii. 内部統制、リスクマネジメントの専門家
iii. データ利活用、知的財産関連の専門家
iv. 内部不正事案、営業秘密侵害事犯等に係る検挙、刑事や民事の訴訟対応や法律相談に詳しい弁護士

【インタビュー対象とした有識者（50音順、敬称略）】

#	氏名	専門性	所属、資格等
1	小原 荘平	iii	独立行政法人工業所有権情報・研修館(INPIT) 知財活用支援センター知財戦略部 営業秘密・知財戦略相談窓口知的財産戦略アドバイザー
2	松本 慶	i ～iv	橋口・松本法律事務所　弁護士
3	山口 利昭	i , ii , iv	山口利昭法律事務所　弁護士
4	山戸 昭三	ii	早稲田大学グローバルソフトウェアエンジニアリング研究所 招聘研究員

6. 調査結果

ここでは、事例調査結果、企業アンケート調査の単純集計結果、企業インタビュー調査結果、有識者インタビュー調査結果について取りまとめた。

【調査の実績】

i. 事例調査
   - ■ 2020年4月以降の秘密情報漏えい／内部不正、サイバー攻撃、システム障害事案の調査結果： 257件

ii. 企業アンケート調査
   - ■ ＜主たる回答＞パネルモニター： 1,248名から回収（所属企業1,000社以上）

iii. 企業インタビュー調査： 8社
   - ■ 秘密情報漏えい／内部不正の防止の取組が進んでいる中小企業： 8社

iv. 有識者インタビュー調査： 4名
   - ■ 内部統制、不正防止の有識者： 2名
   - ■ 知財保護の有識者： 2名

6-1. 事例調査結果

2020年4月以降に発生した内部不正（故意、不注意／ミス）、サイバー攻撃、システム障害による事案のうち、メディアで報道されたものから257件を抽出し、事案の概要、原因と被害の種別、情報漏えいの有無と漏えいした情報の種別・規模、取引先の関与の有無等について調査を実施した。

事例調査の対象とした事案の類型と配分

分類する項目	配分	
	種別	事案の件数
事象の種別（257件）	情報漏えいのみ	191件
	サービス／システムの障害	48件
	両方が同時に発生	13件
	それ以外	5件
漏えいした情報の種別（204件：情報漏えいを伴った事案のみ、重複あり）	個人情報、決済情報	178件
	営業秘密、限定提供データ	27件
	その他の情報	21件
発生原因	不正に漏えい／利用	69件
	サイバー攻撃	106件
	誤送信・設定ミス・紛失	62件
	システム障害（内部要因）	20件

調査結果

事案の特徴

- 報道ベースでは個人情報の漏えい事案が圧倒的に多い
- 潜在している可能性が高いが、サイバー攻撃で営業秘密が漏えいした事案の報道はほとんど見られない。サイバー攻撃で情報漏えいが生じている事案の報道の多くがクレジットカード情報等の決済情報を含む個人情報の漏えい事案である
- 報道ベースでは、営業秘密の漏えいは、ほとんどが故意の内部不正によるものである
- 電子メールの誤送信は相変わらず多く発生している
- ECサイト等のWebサイトやクラウドサービスのセキュリティ設定ミスが多く、目立っている
- ランサムウェアによるサイバー攻撃は引き続き頻繁に発生し、報道されている

得られた示唆

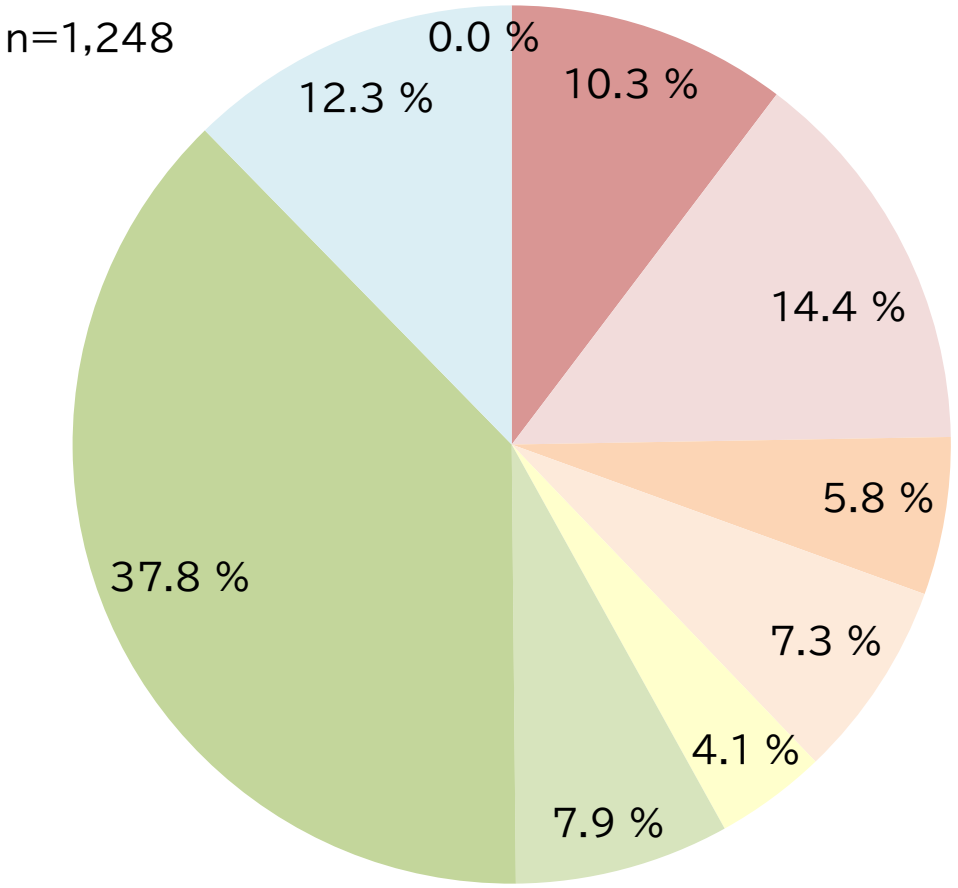
- 内部不正事案の多くは情報漏えいを伴う
- 営業秘密の漏えいは内部不正によるものが看過しえないほど多くを占める
- 企業規模に拠らず営業秘密漏えいは発生しており、内部不正も多数含まれる
- 取引先からの情報漏えいや取引先に起因するシステム／サービス停止は重大事案に発展するリスクが高まっており、今後は注意が必要である

（注）調査対象とした事例の数は、報道されているものの10分の1程度に過ぎない。このため、社会でどのような事案が多く発生しているかを指摘することは適切ではない。しかし、調査過程に照らし、上記のような特徴があるとして矛盾しない。

6-2. 企業アンケートの単純集計結果(1/16) ～回答者の属性～

パネルモニターの回答者が担当する業務については、経営層が37.8%で最も多く、このうち約73%は中小企業の経営層であった。次いで情報システム関連部門を所掌・所管する部門の責任者が14.4%となっている。

SQ1.勤務している企業・組織であなたが担当している業務について、最もよく当てはまるものを1つだけ選んでお答えください。兼務している場合もどれか1つだけお選びください。(単一選択)

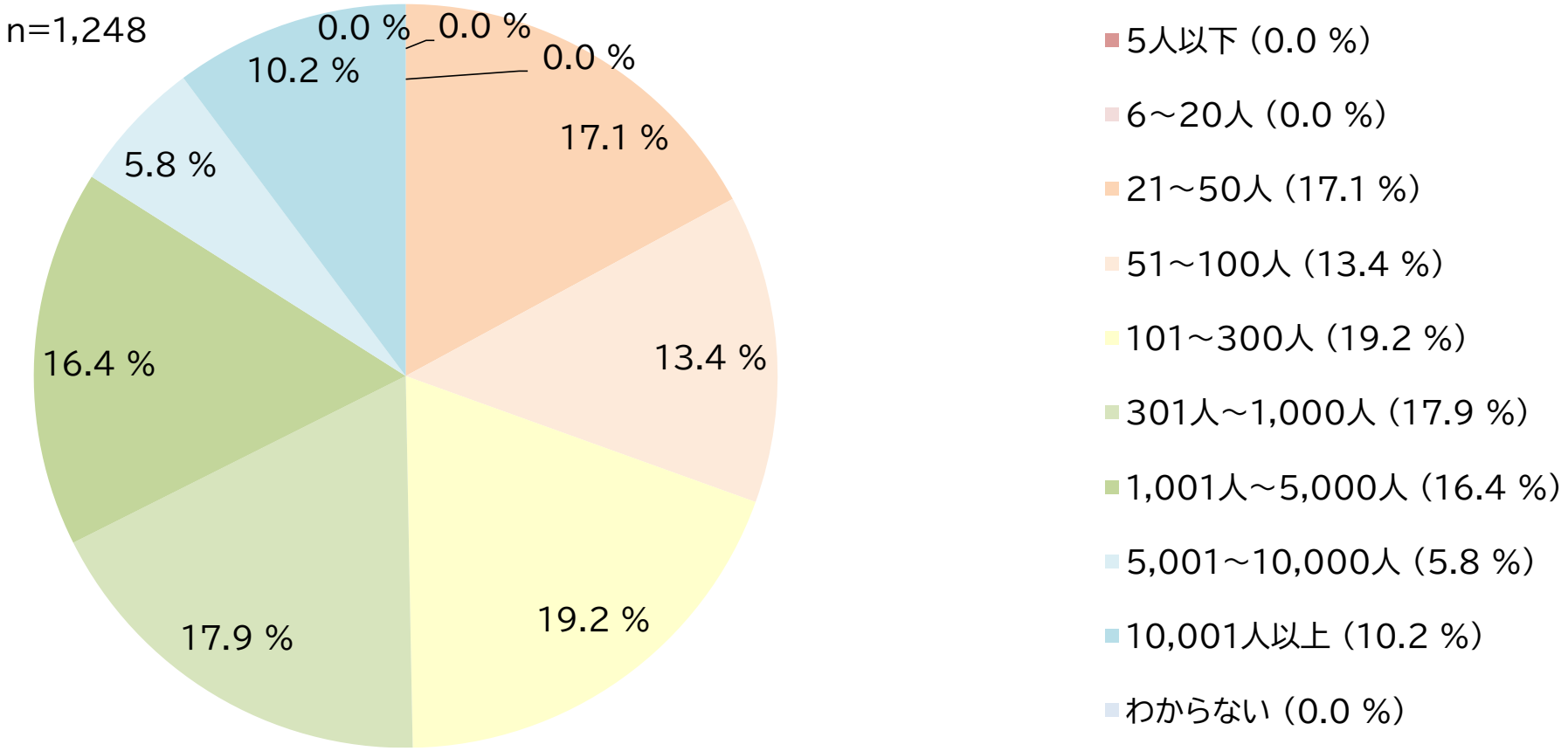


- a. 情報システム関連部門の担当者 (10.3 %)
- b. 情報システム関連部門を所掌・所管する部門の責任者 (14.4 %)
- c. リスクマネジメント計画・実践に関わる部署の担当者 (5.8 %)
- d. リスクマネジメント計画・実践に関わる部署を所掌・所管する部門の責任者 (7.3 %)
- e. 経営企画部門のIT／セキュリティ戦略担当者 (4.1 %)
- f. 経営企画部門のIT／セキュリティ戦略担当を所掌・所管する部門の責任者 (7.9 %)
- g. 経営層 (37.8 %)
- h. a～f以外の部門でも、リスクマネジメントに関する業務を実施していると認識している担当者 (12.3 %)
- i. どれにもあてはまらない (0.0 %)

6-2. 企業アンケートの単純集計結果(2/16) ～回答者の所属企業の常用雇用者数～

パネルモニターの回答者が所属する企業については、大企業と中小企業がほぼ半々となっている。

SQ2.貴社が常時使用する従業員(注1)の数についてお聞きします。
直近の会計年度の人数を1つお選びください。(単一選択)



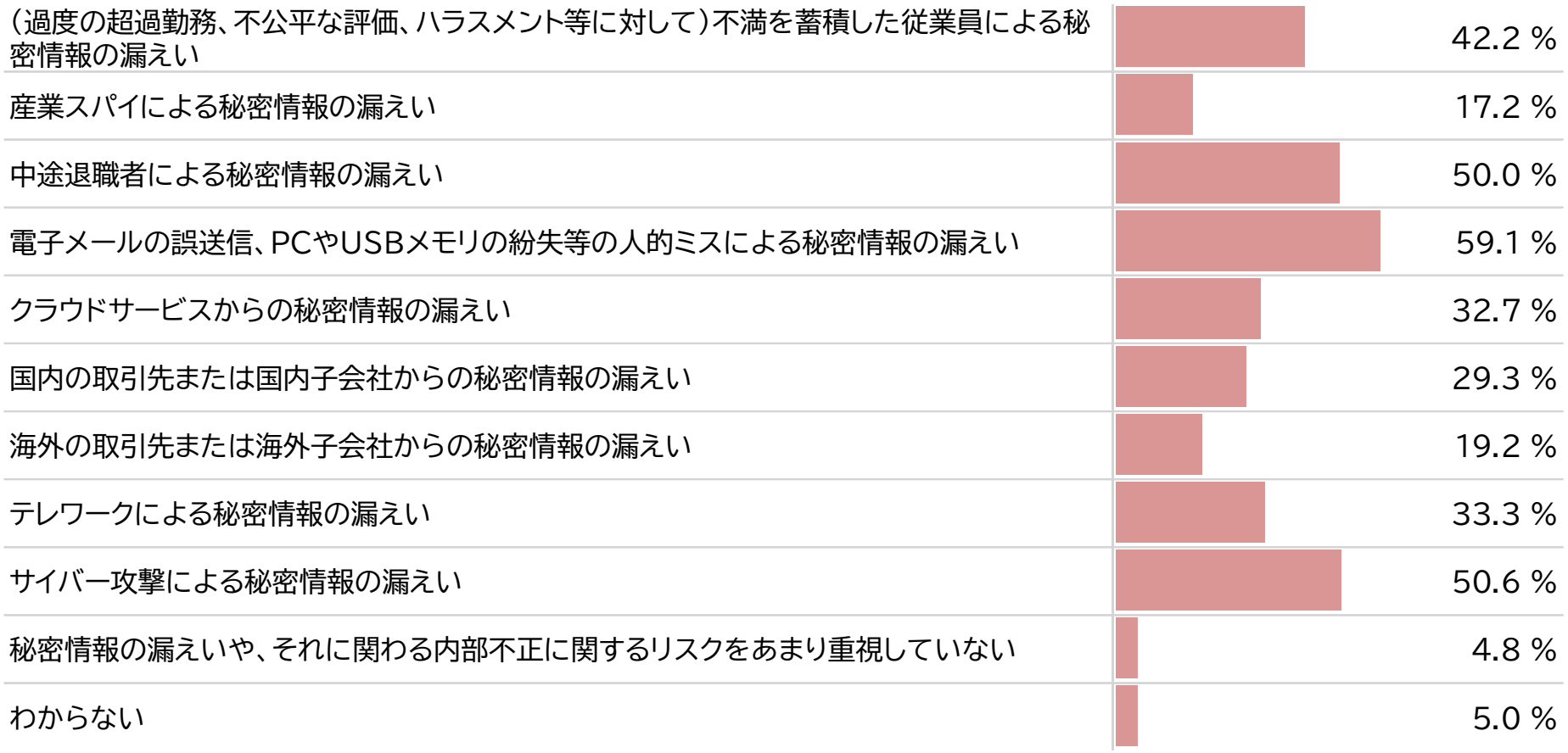
(注1) 常時使用する従業員とは、正社員、パート、アルバイトなどの名称にかかわらず、①期間の定めなく雇用している者、②過去1年以上の期間について引き続き雇用している者、または③雇い入れ時から1年以上引き続き雇用すると見込まれる者のことを指す。

6-2. 企業アンケートの単純集計結果(3/16) ～秘密情報漏えいに関するリスクの認識状況～

経営層や責任者は、秘密情報の漏えいについては、特に「中途退職者の悪意」、「誤送信／可搬媒体の紛失（不注意、ミス）」、「サイバー攻撃」によるリスクを強く認識しており、内部不正とサイバー攻撃の両方を危惧している。

Q2.経営層や、秘密情報保護を統括する組織等の責任者は、秘密情報の漏えいに関するどのようなリスクが高いと認識していると思いますか。あてはまるものをすべてお選びください。（複数選択）

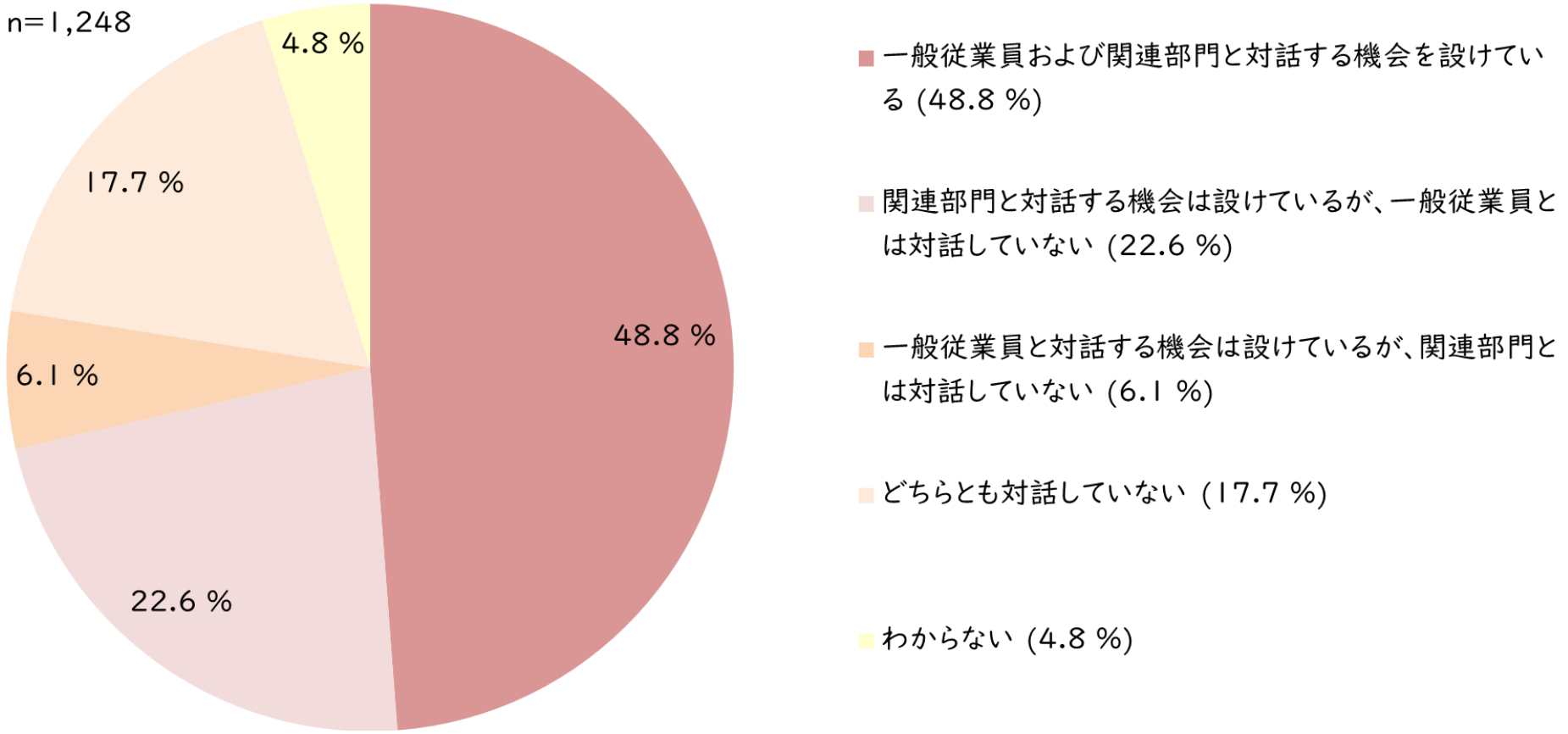
n=1,248



6-2. 企業アンケートの単純集計結果(4/16) ～経営課題の改善～

内部不正への対応方針等について、経営層が一般従業員と対話機会を設けている割合は54.7%に達しており、過半の経営層がリーダーシップを発揮して内部不正防止に関する社内への発信を行っている。

Q3. 経営層は、「秘密情報の漏えいに繋がる内部不正」（注5）への対応方針等について、一般従業員や関連部門と対話する機会を設けていますか。あてはまるものを１つお選びください。（単一選択）

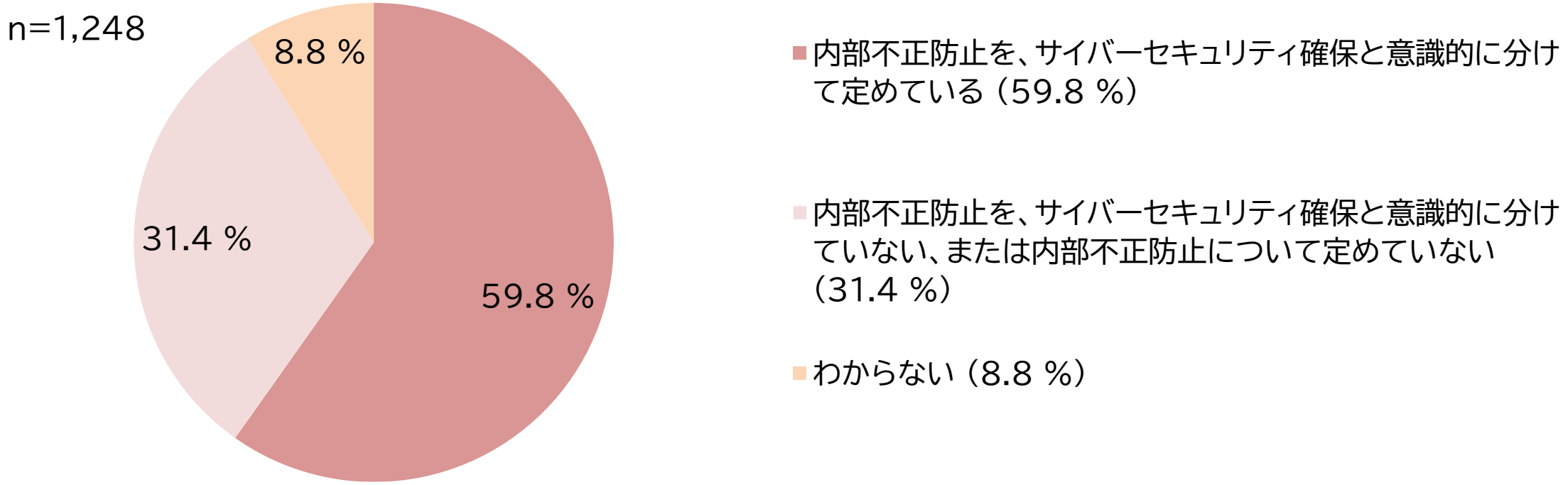


（注5）例えば、会社等への不満・鬱憤をきっかけとした秘密情報の開示・漏えい、離職前の秘密情報持ち出し・転職先での利用、不注意による秘密情報の社外送信／公開・記録媒体の紛失等がある。

6-2. 企業アンケートの単純集計結果(5/16) ～経営課題の改善～

基本方針において内部不正防止の取組をサイバーセキュリティ確保と意識的に分けて定めている企業の割合は59.8%に達しており、内部不正防止に特有の取組の必要性を認識している企業は過半を占める。

Q4.経営層は、秘密情報保護に関する基本方針等で、内部不正防止（注5）をサイバーセキュリティ確保と意識的に分けて定めていますか。あてはまるものを1つお選びください。（単一選択）



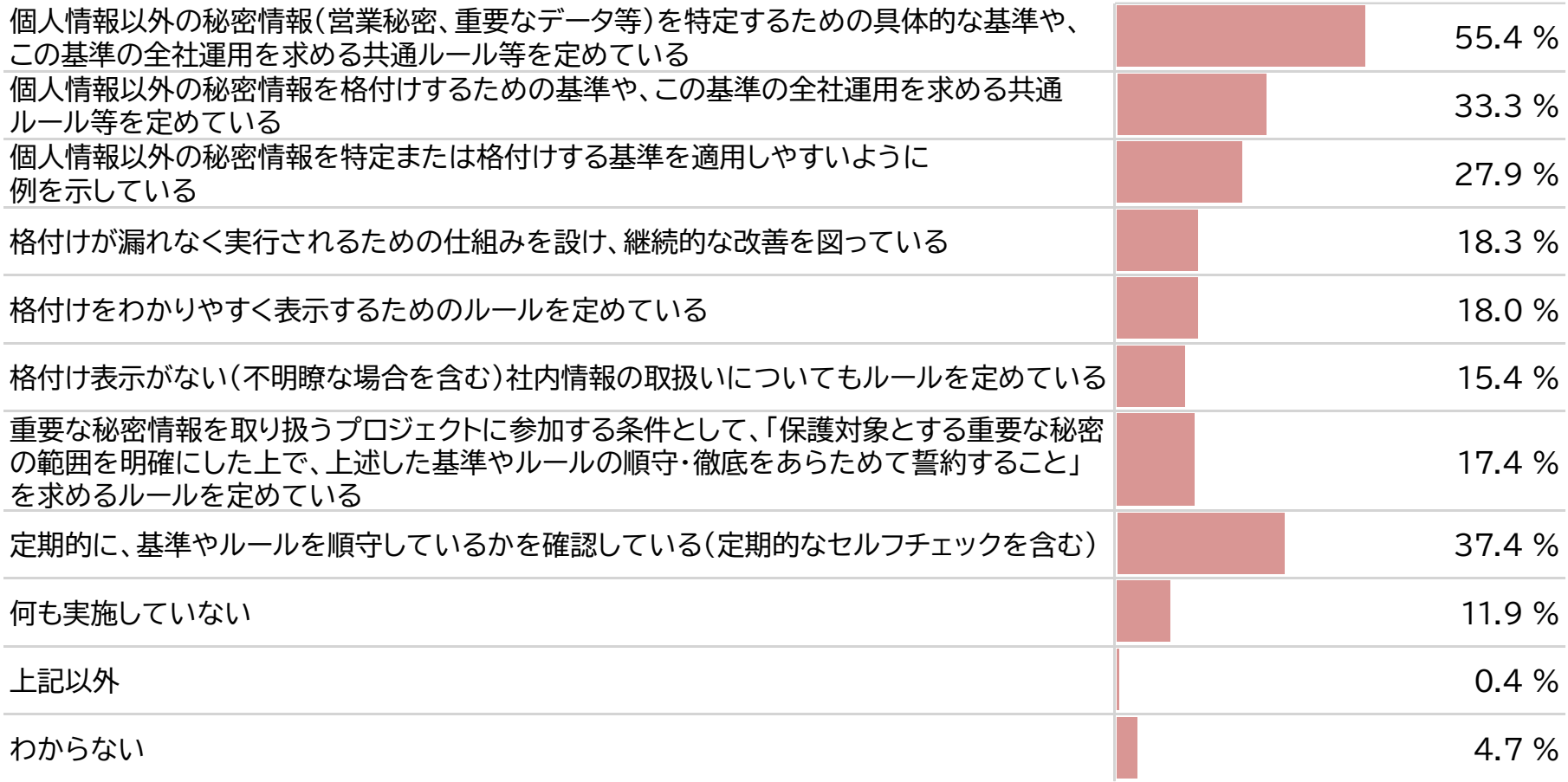
（注5）例えば、会社等への不満・鬱憤をきっかけとした秘密情報の開示・漏えい、離職前の秘密情報持ち出し・転職先での利用、不注意による秘密情報の社外送信／公開・記録媒体の紛失等がある。

6-2. 企業アンケートの単純集計結果(6/16) ～重要な秘密の特定と取扱いの改善～

個人情報以外の秘密情報を特定するための具体的な基準や、その基準の全社運用を求める共通ルール等を定めている企業が55.4%に達している一方で、秘密情報の格付けに関するルールを定めている企業は33.3%に留まり、格付けの表示に関するルールを定めている企業は18.0%と更に少ない。格付け表示にまで至っている企業は少数派である。

Q7.個人情報以外の秘密情報(営業秘密、重要なデータ等)の特定と格付けの実効性を高めるために、組織全体でどのような取組を実施していますか。あてはまるものをすべてお選びください。(複数選択)

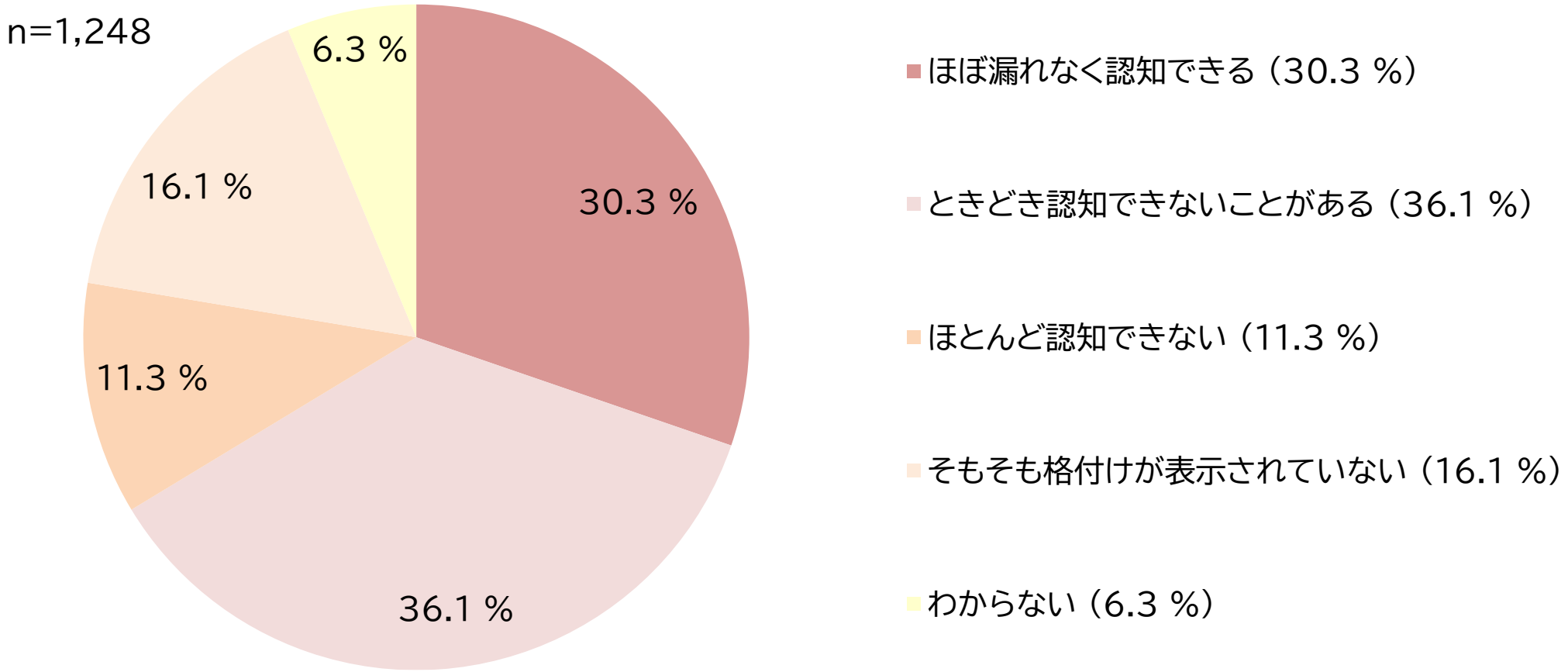
n=1,248



6-2. 企業アンケートの単純集計結果(7/16) ～重要な秘密の特定と取扱いの改善～

従業員が秘密情報を目にした際にそれが秘密情報であるとほぼ漏れなく認知できると回答した企業は30.3%しかなく、秘密情報が不正に取り扱われている時に周囲の従業員が気付いて通報できる職場環境にある企業は少数派である。

Q8.従業員は、自部署・他部署の情報に関わらず、個人情報以外の秘密情報に触れた際に、格付けの表示等によってほぼ漏れなく秘密情報であることを認知できますか。あてはまるものを1つお選びください。（単一選択）

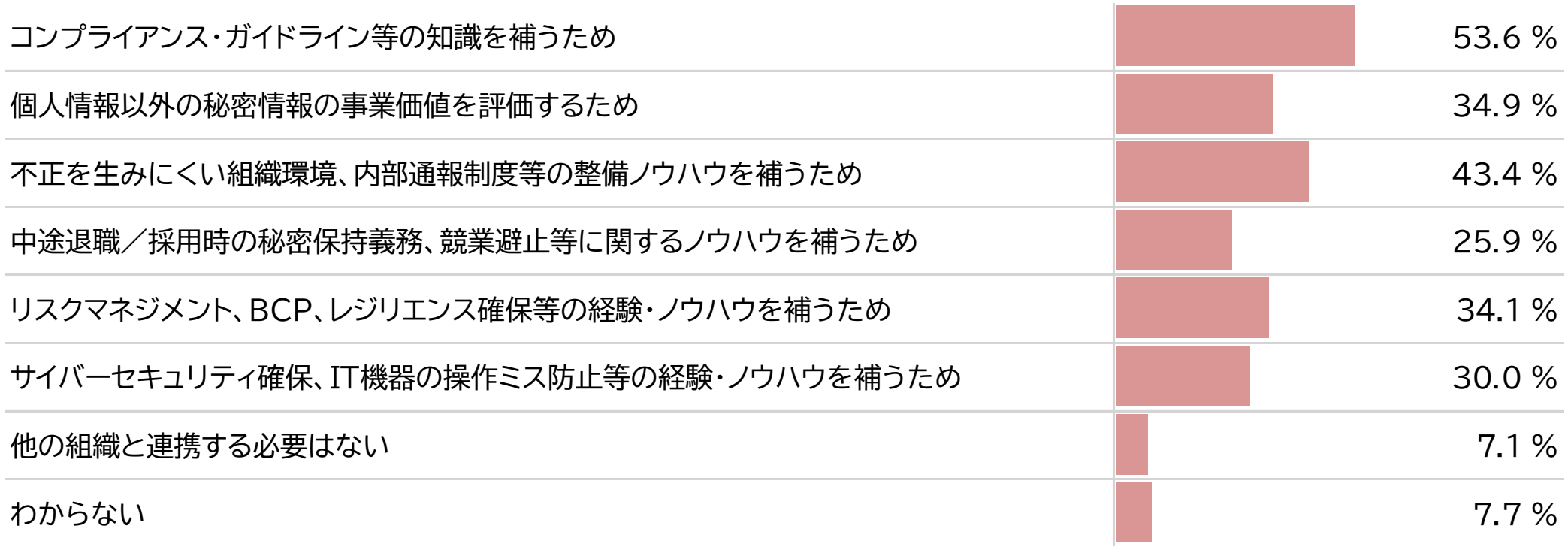


6-2. 企業アンケートの単純集計結果(8/16) ～組織体制・連携に関する課題の改善～

責任部門と他組織の連携においては、過半の企業で、連携先からコンプライアンス・ガイドライン等の知識を補うことを目的としている（53.6%）。その次に求められているのは、不正を生みにくい組織環境、内部通報制度等の整備ノウハウを補うことである（43.4%）。個人情報以外の秘密情報の事業価値を評価することを目的とする企業の割合は34.9%に留まる。

Q11.「秘密情報の漏えいに繋がる内部不正」に対応する経営層や組織は、平時に他の組織とどのような目的で連携していますか。あてはまるものをすべてお選びください。（複数選択）

n=1,248

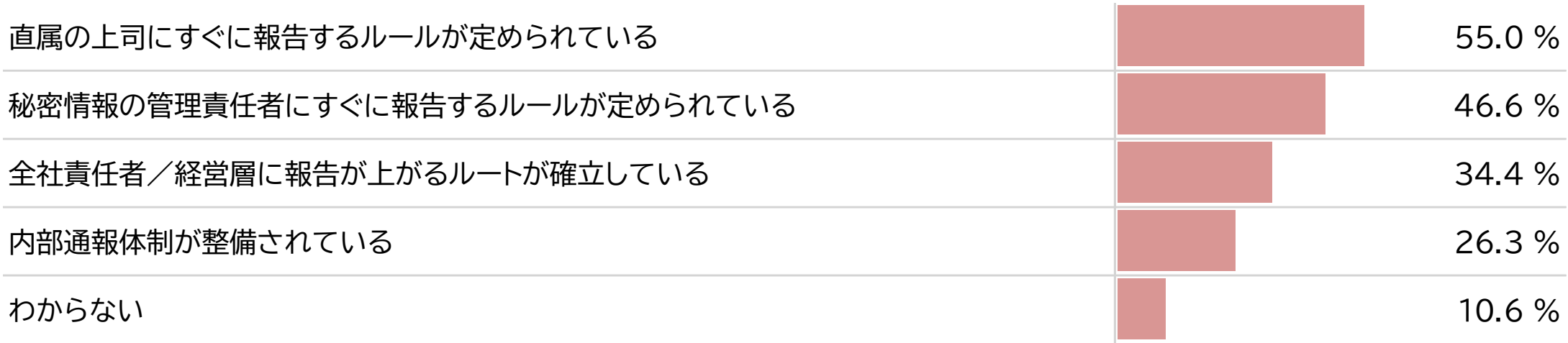


6-2. 企業アンケートの単純集計結果(9/16) ～組織体制・連携に関する課題の改善～

秘密情報の不自然な取扱いや社外への不正な漏えいを目撃した際に、直属の上司にすぐに報告するルールを定めている企業が55.0%を占め、秘密情報の管理責任者に報告することを定めている企業は46.6%となっている。全社責任者/経営層に報告が上がるルートが確立している企業は34.4%でより少なく、内部通報体制を整備している企業は26.3%と更に少ない。

Q12.秘密情報が不自然に取り扱われていることや、社外への不正な漏えいを目撃した際に、上司や全社責任者／経営層に報告を上げる体制やルールがありますか。あてはまるものをすべてお選びください。（複数選択）

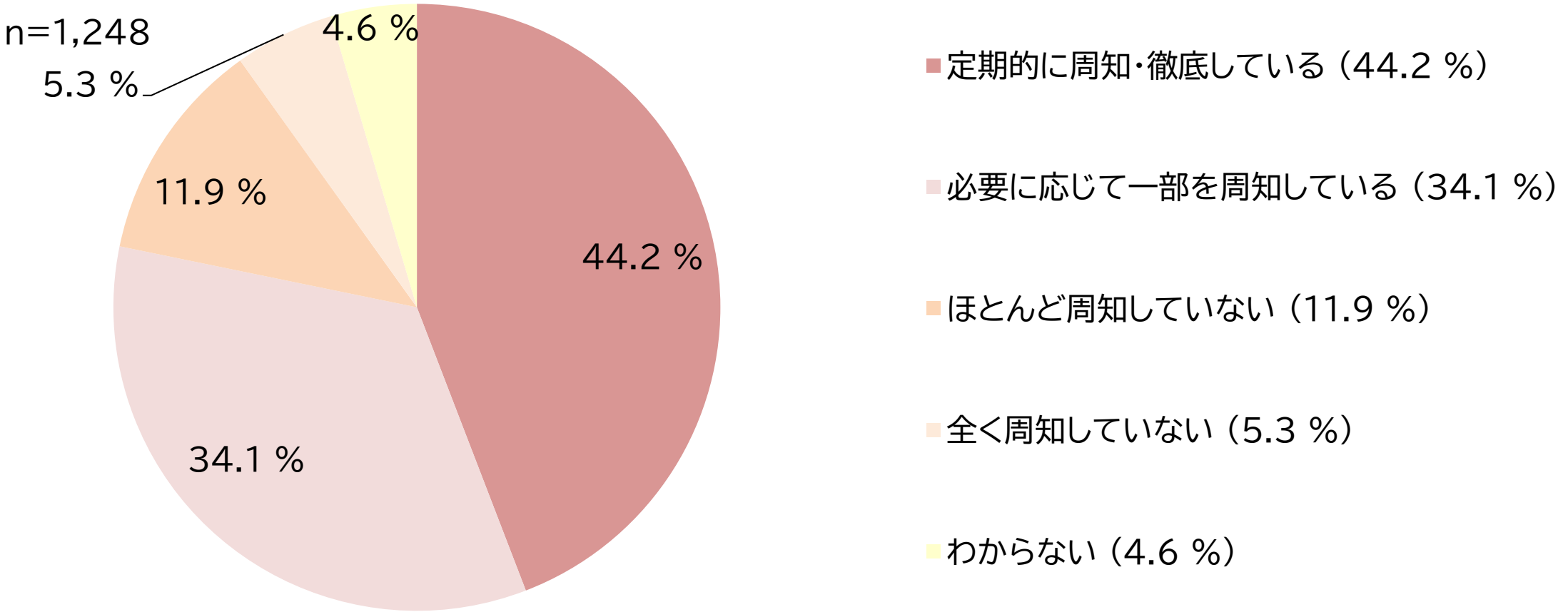
n=1,248



6-2. 企業アンケートの単純集計結果(10/16) ～社員教育とリテラシー構築に関する課題の改善～

秘密情報の不自然な扱いや社外への不正な漏えいを目撃した際の適切な行動を、定期的に周知・徹底している企業は44.2%と半分近くあり、必要に応じて一部を周知している企業も合わせれば、78.3%の企業がその周知に取り組んでいる。

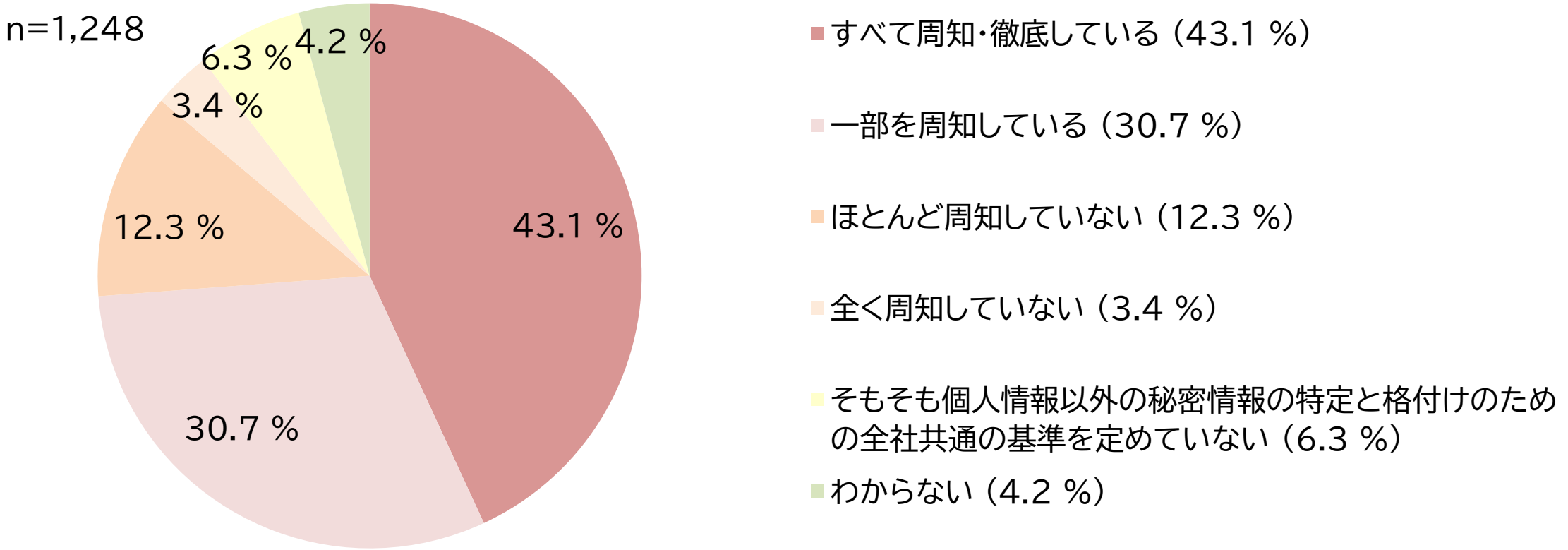
Q16.秘密情報が不自然に取り扱われていることや、社外への不正な漏えいを目撃した際の適切な行動について、社員教育等で組織全体に周知・徹底していますか。あてはまるものを1つお選びください。(単一選択)



6-2. 企業アンケートの単純集計結果(11/16) ～社員教育とリテラシー構築に関する課題の改善～

営業秘密等の特定と格付けのための全社共通の基準のすべてまたは一部を、社員教育等で全従業員に周知している企業は73.8%を占める。

Q15.個人情報以外の秘密情報(営業秘密、重要なデータ等)の特定と格付けのための全社共通の基準を、社員教育等で全ての従業員に周知・徹底していますか。あてはまるものを1つお選びください。(単一選択)

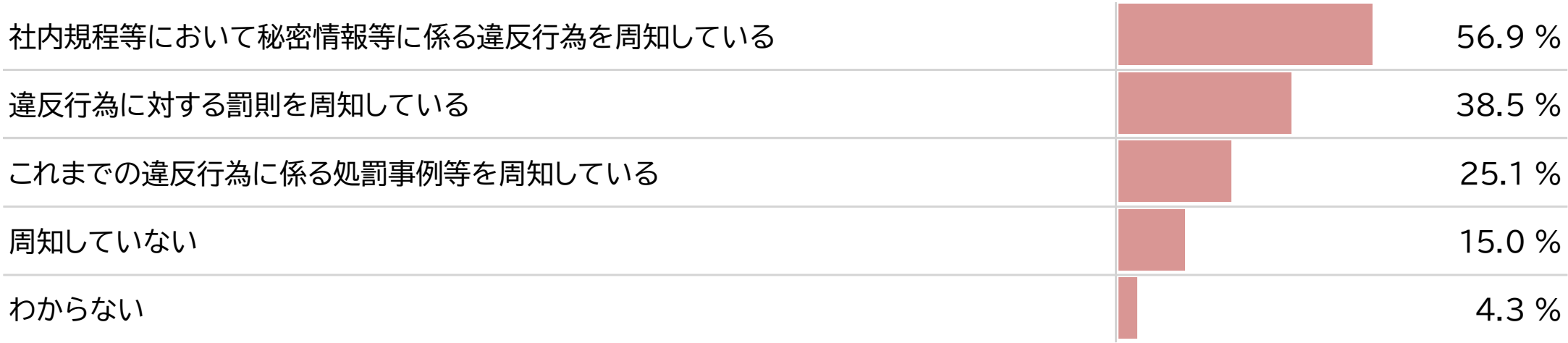


6-2. 企業アンケートの単純集計結果(12/16) ～社員教育とリテラシー構築に関する課題の改善～

営業秘密や重要なデータ等の漏えいや内部不正に関する違反行為を従業員に周知している企業は56.9%に上るが、罰則を周知している企業は38.5%に留まる。

Q17.個人情報以外の秘密情報(営業秘密、重要なデータ等)の漏えいや内部不正に関し、何をしてはいけないのか、何をするとどのように罰せられるのかを例示する等、従業員に対してわかりやすく周知していますか。あてはまるものをすべてお選びください。(複数選択)

n=1,248

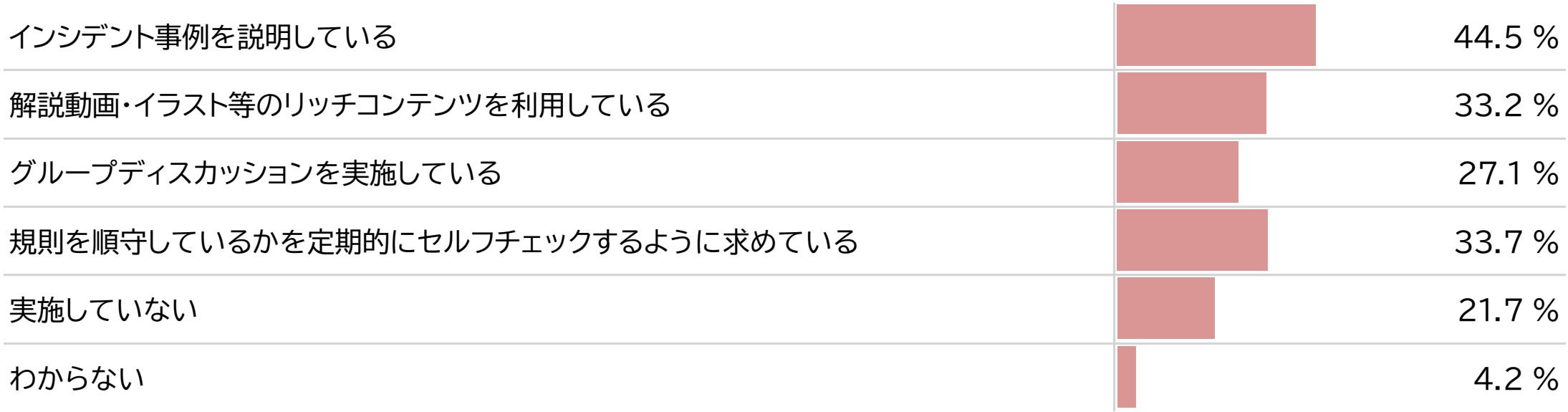


6-2. 企業アンケートの単純集計結果(13/16) ～社員教育とリテラシー構築に関する課題の改善～

e-Learning以外の具体的な方法としては、インシデント事例の説明を44.5%の企業が行っている他、定期的なセルフチェックは33.7%、リッチコンテンツの利用は33.2%、グループディスカッションは27.1%となっている。

Q18.秘密情報漏えいや内部不正防止の従業員教育にあたり、e-Learning以外の方法を実施していますか。あてはまるものをすべてお選びください。（複数選択）

n=1,248

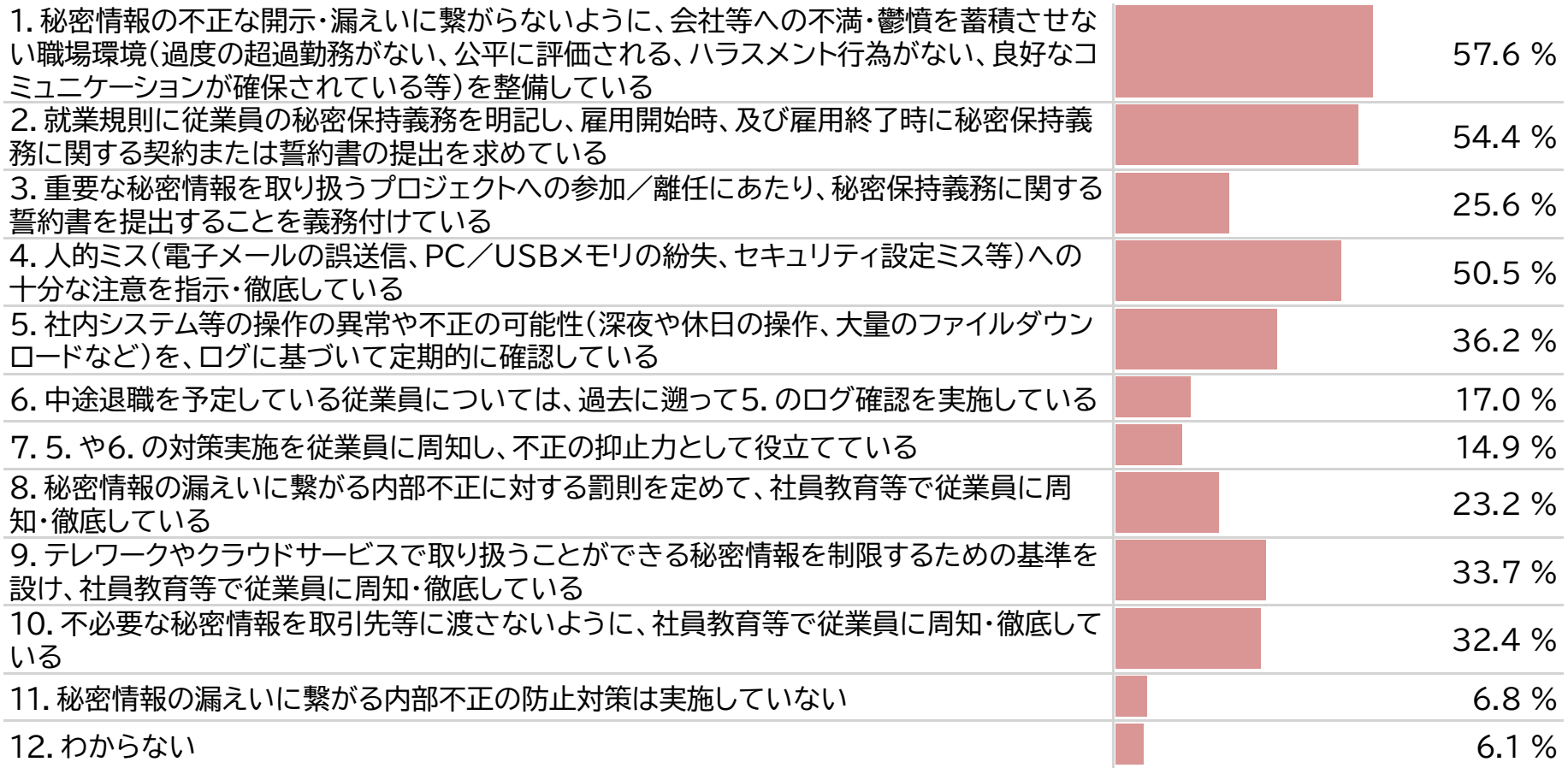


6-2. 企業アンケートの単純集計結果(14/16) ～対策実施に関する課題の改善～

過半の組織で実施されている内部不正防止に特有の対策は、不満・鬱憤を蓄積させない職場環境の整備（57.6%）、雇用開始・終了時の秘密保持義務契約／誓約書提出（54.4%）、人的ミスへの十分な注意の指示・徹底（50.5%）である。他の対策で実施割合が4割を超えるものはない。

Q22.以下に列挙した「秘密情報の漏えいに繋がる内部不正の防止」に特有の対策のうち、貴社で実際に実施しているものはどれですか。あてはまるものをすべてお選びください。（複数選択）

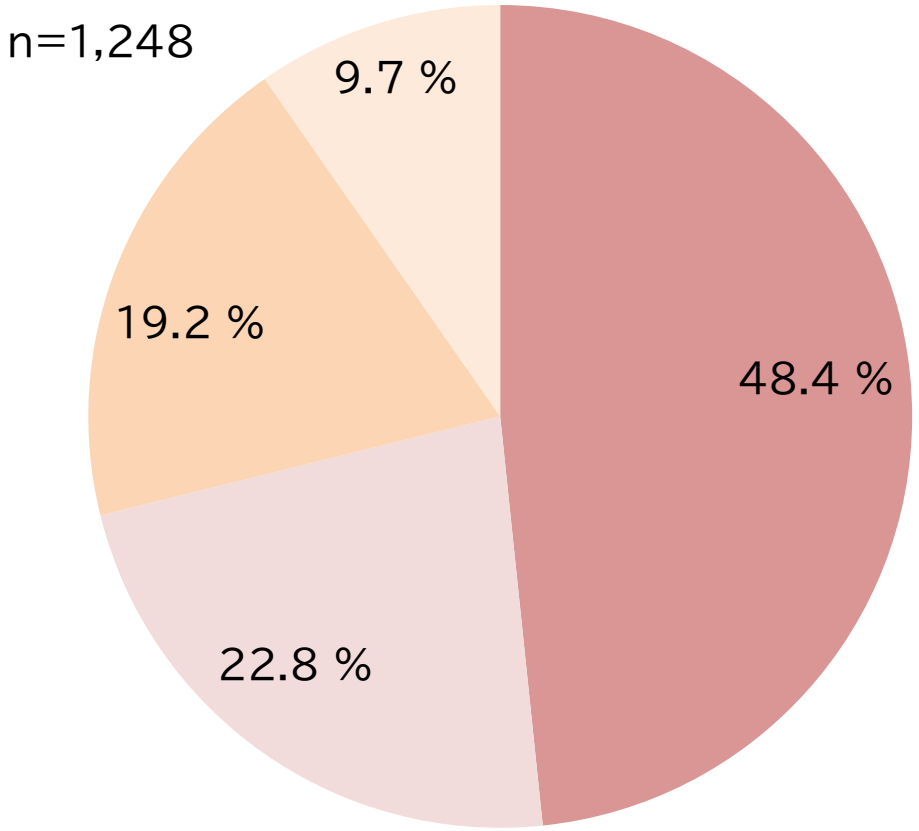
n=1,248



6-2. 企業アンケートの単純集計結果(15/16) ～対策実施に関する課題の改善～

サイバー攻撃対策や会計不正等への対策と内部不正防止対策とを、経営層が示した基本方針に基づいて意識的に使い分け、更に定期的に経営層にその有効性を報告している企業は48.4%に上る。経営層の把握していない現場組織の裁量の範囲でこの使い分けを行っている企業も約22.8%存在する。

Q23.「秘密情報の漏えいに繋がる内部不正の防止対策」を「サイバー攻撃対策」や「会計不正・ハラスメント等の対策」と意識的に使い分けていますか。あてはまるものを1つお選びください。(単一選択)

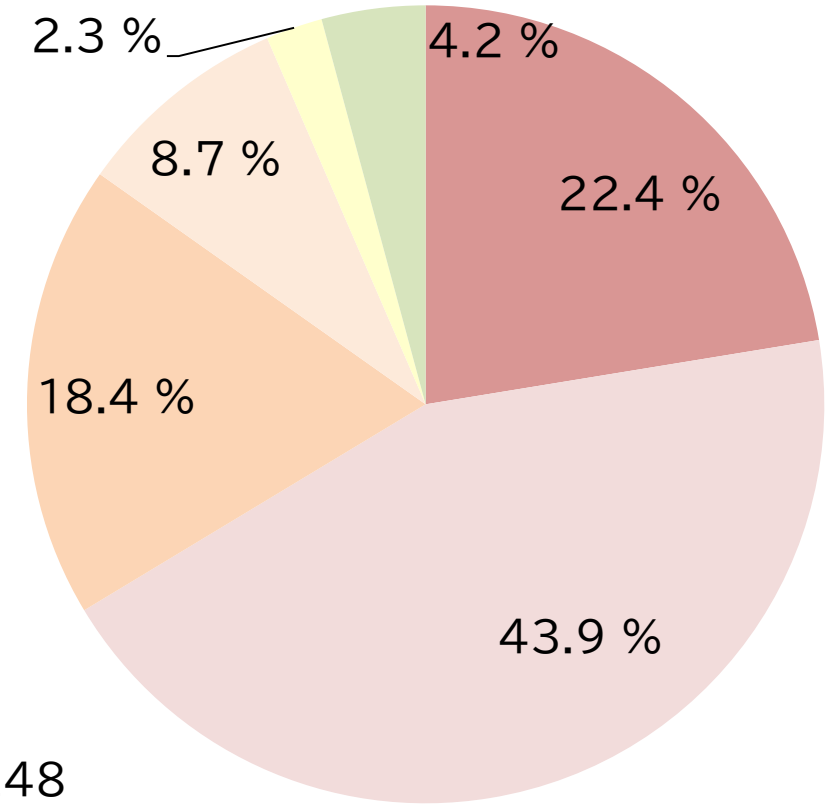


- 経営層が指示した基本方針に基づいて対策を意識的に使い分けており、定期的に経営層にその有効性を報告している（48.4 %）
- 「サイバー攻撃対策」または「会計不正・ハラスメント等の対策」を実施する現場部門の裁量で対策を使い分けているが、経営層はその使い分けを把握していない（22.8 %）
- 対策の意識的な使い分けは行っていない、または「秘密情報の漏えいに繋がる内部不正の防止対策」は実施していない（19.2 %）
- わからない（9.7 %）

6-2. 企業アンケートの単純集計結果(16/16) ～対策実施に関する課題の改善～

営業秘密等を個人情報と同等あるいはそれ以上に重視している企業の割合は66.3%に達している。

Q20.個人情報保護だけでなく、それ以外の秘密情報（営業秘密、重要なデータ等）を保護する対策も重視していますか。あてはまるものを1つお選びください。（単一選択）



n=1,248

- 個人情報を保護する対策以上に重視している（22.4 %）
- 個人情報を保護する対策と同じくらい重視している（43.9 %）
- 個人情報を保護する対策ほどではないが、ある程度重視している（18.4 %）
- あまり重視していない（8.7 %）
- 全く重視していない（2.3 %）
- わからない（4.2 %）

6-3. 企業と有識者のインタビュー結果の整理・比較　～中小企業について～（1/3）

中小企業の経営者が自ら主導して技術情報管理・ISMS等の認証を取得することが、秘密情報漏えい／内部不正リスクを重要な経営課題として認識するための良い契機となりうることが分かった。認証の取得によって、情報資産台帳を用いた秘密情報管理の導入も期待できる。有識者によると、中小企業に営業秘密管理を根付かせることが良い入口になりうるとのことだった。経営者が自ら戦略を語り、基本方針を周知徹底し、コミットメントへの自身の想いを伝えることで、従業員に対するリーダーシップを発揮している好事例があった。経営者が率先して、事業リスクの判断や秘密情報の特定・格付けを行っている企業も見られた。中小企業であっても、経営者と関連部門幹部が連携・情報共有できる場として委員会を設けることが有効であることが分かった。ヒヤリハット、インシデント等の社内報告体制整備については、人間関係が良く性善説を基に経営する中小企業が多いことから、従業員の不信感が高まらないように注意しながら取り組むことが必要であると分かった。

調査軸（中小企業関係）	中小企業の経営者または秘密情報漏えい等の主担当者の調査結果（重要事項の抜粋）	有識者の調査結果（重要事項の抜粋）
調査軸６の１ 中小企業における経営課題の改善	■ 業界の流れを意識し、技術情報管理の認証取得に取り組んだことが、秘密情報漏えい／内部不正リスクを重要な経営課題として認識した契機となった ■ ISMS、プライバシーポリシー、技術情報管理等の認証取得が、中小企業の経営者が基本方針を定める契機となって取組が進んだ ■ 経営層が従業員に秘密情報漏えい／内部不正防止を周知徹底している好事例： ・経営者が自ら基本方針を全社に周知徹底 ・定期的にも日常的にも経営者が社員に語ることで意識付け・啓発に効果を発揮 ・漏えいが自社の信頼失墜に直結することを強く認識して全社に周知・啓発等	■ 中小企業では経営層が高い意識を持って率先して牽引すれば会社全体の取組状況をがらりと変えられる可能性がある ■ 中小企業では、営業秘密を社内できちんと保護する体制を構築することで、秘密情報漏えい／内部不正防止にも好ましい効果が生じる ■ 経営者も従業員もお互いに直接顔が見えるため、性善説を前提とした管理になりがちなのが問題点だが、従業員と直接コミュニケーションを取って趣旨をしっかりと伝えることで、ある程度はリスクに対応できる ■ 中小企業の取組強化に向けては、経営者が戦略を語り、コミットメントや指示に自身の想いやこだわりを込め、日々語ることが重要である
調査軸６の２ 中小企業における重要な秘密の特定と取扱の改善	■ 経営者が自ら事業リスクの判断や秘密情報の特定・格付けを行っている企業があった ■ 経営者が決断し情報セキュリティや技術情報管理の認証取得を取り組んだことを契機とし、営業秘密等の特定・格付け・表示に関する体制整備が進んだ企業があった。また、認証が要求する管理基準に従い、秘密情報を管理できる情報資産台帳を作成・運用している例があった	■ 経営者が過負荷にならないように、部下を育成して権限移譲することも必要である ■ 紙に書かれた秘密情報の物理的管理がしっかりできていたとしても、電子化された秘密情報の管理はほとんどできていない中小企業が多い
調査軸６の３ 中小企業における組織体制・連携に関する課題の改善	■ 経営者を責任者とする3~5名程度の幹部による委員会を設置している。その下にシステム、総務・人事、教育、内部監査等を担当する幹部が集まって委員会を構成する。具体的には、情報管理委員会を設けている例と、情報セキュリティ委員会を設けている例が見られた。 ■ 秘密情報漏えい／内部不正の防止の取組が進んでいる中小企業の中には、秘密情報が漏えいした時や従業員がヒヤリハット・不信感を認識した時に、直属の上司を通じて経営者にすぐに報告が上がってくる仕組みを設けている企業があった	■ 法務部門がない、または知財・法務に精通する経営層や幹部がいない中小企業では、法制度への対応や規程の制定／社内への浸透等が社長室や総務部門の雑多な業務の１つとして片手間で扱うことになりがちなので、社内に委員会を設けるなどして複数部門が連携して取り組むことができる体制を検討することが望ましい ■ 中小企業は人間関係が良く性善説を基にしていることが多いので、内部通報ができる仕組みを構築すると逆に従業員の不信感が高まる恐れがあり、注意が必要である

6-3. 企業と有識者のインタビュー結果の整理・比較　～中小企業について～（2/3）

秘密情報漏えい／内部不正防止を従業員に教育するにあたり、何を教育するかと、どうやって理解しやすく教育するかの２つが論点になる。

何を教育するかについては、リスクとその重要性、実際に発生した損害・影響の大きさ、営業秘密の取扱方法等の中核となる内容に加えて、社内で発生したヒヤリハットの経緯や内容、禁止事項・内規の懲罰規定・法の遵守等の好事例が見られた。また有識者からは、秘密情報漏えい防止等の対策として従業員のアクセスログを取得していることを周知することへの前向きな意見が得られた。

一方、どうやって理解しやすく教育するかについては、経営層が自ら経営方針やそこに込めた想いを教育、秘密情報を持ち出した事例等を用いた教育、禁止事項・懲罰規定等を積極的に伝える教育、ITコーディネータ等の外部講師による研修などの進んだ手法を取り入れている中小企業が見られた。教育で用いる類似事例情報の収集については、経営者が自ら収集する、セキュリティ支援会社への委託や外部講師から提供を受ける等の好事例があった。

調査軸（中小企業関係）	中小企業の経営者または秘密情報漏えい等の主担当者の調査結果（重要事項の抜粋）	有識者の調査結果（重要事項の抜粋）
調査軸６の４ 中小企業における社員教育とリテラシー構築に関する課題の改善	■ 経営者が自ら基本方針を全社に周知・徹底している。定期的にも日常的にも経営者が社員に語ることで意識付け・啓発に効果を上げている。 ※調査軸６の１から転載 ■ 営業秘密・重要データの知識に関する社員教育に取り組んでいる ■ 営業秘密や限定提供データに関する従業員教育で、これらの取扱方法に加えて、禁止事項・内規の懲罰規定・法の遵守等についても教育している ■ 従業員に、秘密情報漏えい／内部不正リスクとその重要性、過去に発生した事例における重要なリスクと実際に発生した損害、社内で発生したヒヤリハットの経緯や内容等を教育している企業があった ■ 従業員に、退職時に秘密情報を持ち出すリスク、実際に持ち出した事例等に重点を置いて教育している企業があった ■ 他社事例情報を収集するため、経営層が率先して集める、外部委託先から情報提供を受ける等の手法で、他社で発生した事案の情報を取りまとめ、社会的な影響なども含めて教育している企業があった ■ 営業秘密等に関する従業員教育で、営業秘密等の取扱方法に加えて、禁止事項・内規の懲罰規定・法の遵守等についても教育している企業があった ■ 経営層が従業員に直接周知徹底することに加えて、ITコーディネータ等の外部講師に研修の講師を依頼している企業があった	■ 中小企業は、営業秘密の秘密管理性の確保が自己防衛及びビジネス拡大に不可欠であることを、大企業以上に認識することが望ましい ■ 秘密情報漏えい防止等の対策として従業員のアクセスログを取得すること等に対して抵抗感を持つ中小企業が多く見られるが、有識者の適切な助言等に基づいてこれを導入し組織に根付かせることで、むしろ会社への帰属意識や仕事に対するプライドといったものが上がってきて緊張感が醸成され、会社の雰囲気が良くなってきたと言われることも多い

6-3. 企業と有識者のインタビュー結果の整理・比較　～中小企業について～（3/3）

対策を講じる上では、その前提としてどのリスクに焦点を当てるかが問われる。秘密情報持ち出しリスク、不注意やミスによる情報漏えいリスク、中途退職者の秘密情報持ち出しリスクを重視している企業が見られた。秘密情報漏えいリスクの管理に取り組んだ理由として、技術情報管理等の認証を取得するために必要だったことに加えて、自社事業との関わりで秘密情報漏えい事件を起こした際の事業リスクが甚大だからという理由を挙げた企業があった。

ISMSや技術情報管理の認証のスコープが両方をカバーしているため、秘密情報漏えい防止に向けた内部不正防止対策とサイバーセキュリティ対策を、同一の取組の一環として実施している企業が見られた。

秘密情報漏えい／内部不正防止のために実施している対策として、採用・退職・プロジェクト異動等の際の秘密保持義務契約、秘密情報の定期的な棚卸し、不注意／ミスの自主的な報告を奨励するインセンティブ、ITシステムのアクセス等のログを取得して定期的に確認することの従業員への周知等を挙げた企業があった。有識者からは、退職時の秘密保持義務契約において対象とする秘密情報の範囲を具体的に示すことが重要であるという意見が得らえた。

調査軸（中小企業関係）	中小企業の経営者または秘密情報漏えい等の主担当者の調査結果（重要事項の抜粋）	有識者の調査結果（重要事項の抜粋）
調査軸６の５ 中小企業における対策実施に関する課題の改善	■ 秘密情報持ち出しリスク、不注意やミスによる情報漏えいリスク、中途退職者の持ち出しリスクを重視している企業があった。秘密情報漏えいリスクの管理に取り組んだ理由としては、認証を取得するために必要だったことに加えて、自社事業との関わりで秘密情報漏えい事件を起こした際の事業リスクが甚大だからとした企業があった ■ ISMSや技術情報管理の認証のスコープが両方をカバーしているため、秘密情報漏えい防止に向けた内部不正防止対策とサイバーセキュリティ対策を、同一の取組の一環として実施している企業が見られた ■ 経営者のリーダーシップの下で、採用・退職・プロジェクト異動等の際に、都度必要な秘密保持義務契約を締結している企業があった ■ 入社時に提出を求める誓約書で「退職する時にも誓約書を提出すること」を誓約させる好事例があった ■ 技術情報管理認証を取得した企業では、秘密情報の定期的な棚卸しや不要なものの消去、アクセス権限の見直しに重点を置いて実施していた ■ ミスが発生した際の報告については、これを隠ぺいする組織風土にならないように、自発的な報告を考課で高く評価している好事例があった ■ 不正が発覚した際の社内告知については、特に1人1人の顔が見えるぐらいの組織規模の場合に、慎重に伝え方を選ぶ必要があるという意見があった ■ ITシステムのアクセス等のログを取得して定期的に確認することについて、十分なコミュニケーションを取ってインシデント対応のために必要であることをていねいに説明することで、従業員の理解と信頼が得られている好事例があった	■ 中小企業では他社の事例等に基づいて意識の高い経営層がリスクを判断できれば、秘密情報漏えいや内部不正のリスク評価をある程度代替できる ■ 退職時の秘密保持義務契約において対象とする秘密情報の範囲を具体的に示すことが重要である

7. 調査結果の分析

7-1. 企業アンケート調査のクロス集計による分析(1/14) ～中小企業の現状分析～

パネルモニターからのアンケート回答を対象としてクロス集計を実施し、その結果を分析した。概要説明資料では、中小企業に関する分析結果を示す。

中小企業では、経営層の秘密情報漏えいに関するリスク認識が全体平均と比べて全般に低い。しかし、組織が小さい分、経営層のリスク認識さえ上がれば、全社の状況を一変させやすい環境にはあるので、中小企業では経営層の意識を高めることが非常に重要になる。

Q2.経営層や、秘密情報保護を統括する組織等の責任者は、秘密情報の漏えいに関するどのようなリスクが高いと認識していると思いますか。あてはまるものをすべてお選びください。（複数選択）

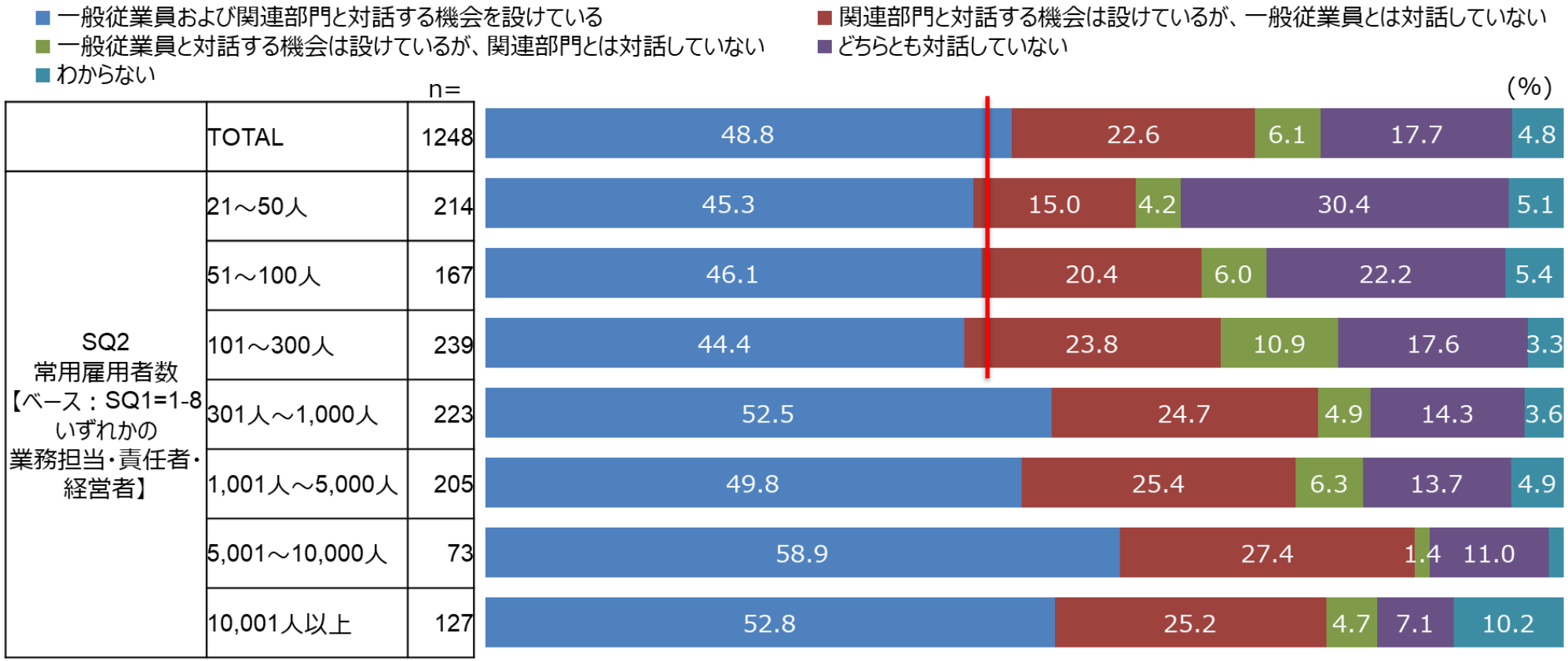
(%)

		n=	（過度の超過勤務、不公平な評価、ハラスメント等に対して）不満を蓄積した従業員による秘密情報の漏えい	産業スパイによる秘密情報の漏えい	中途退職者による秘密情報の漏えい	電子メールの誤送信、PCやUSBメモリの紛失等の人的ミスによる秘密情報の漏えい	クラウドサービスからの秘密情報の漏えい	国内の取引先または国内子会社からの秘密情報の漏えい	海外の取引先または海外子会社からの秘密情報の漏えい	テレワークによる秘密情報の漏えい	サイバー攻撃による秘密情報の漏えい	秘密情報の漏えいや、それに関わる内部不正に関するリスクをあまり重視していない	わからない
	TOTAL	1248	42.2	17.2	50.0	59.1	32.7	29.3	19.2	33.3	50.6	4.8	5.0
SQ2 常用雇用者数【ベース：SQ1=1-8いずれかの業務担当・責任者・経営者】	21～50人	214	35.0	9.3	54.7	49.5	21.0	17.8	7.5	24.3	39.7	8.4	5.1
	51～100人	167	42.5	11.4	46.1	61.1	27.5	23.4	7.8	29.3	49.7	4.8	7.2
	101～300人	239	40.2	9.6	44.4	56.1	25.9	20.5	8.8	25.1	46.0	5.9	5.0
	301人～1,000人	223	39.9	20.6	52.0	61.9	38.1	31.8	19.7	39.0	52.9	4.0	3.1
	1,001人～5,000人	205	50.2	17.6	48.8	62.0	38.5	34.6	26.3	39.0	55.1	2.9	4.9
	5,001～10,000人	73	49.3	38.4	57.5	72.6	39.7	52.1	39.7	43.8	67.1	0.0	0.0
	10,001人以上	127	44.9	33.9	52.0	61.4	48.8	47.2	48.8	43.3	57.5	3.9	7.9

7-1. 企業アンケート調査のクロス集計による分析(2/13)　～中小企業の現状分析～

企業規模が小さくなるほど、秘密情報の漏えいにつながる内部不正に関して、経営層と一般従業員・関連部門の対話を設けているとする回答割合が下がる。従業員数が100人以下の中小企業は従業員数が少ない分、経営者と従業員はお互いに顔が見える関係であり、さらに経営者自らが講師を務める集合教育を実施しやすい。現状を踏まえると、この利点をより積極的に活かすことが望ましい。

Q3. 経営層は、「秘密情報の漏えいに繋がる内部不正」（注5）への対応方針等について、一般従業員や関連部門と対話する機会を設けていますか。あてはまるものを１つお選びください。（単一選択）

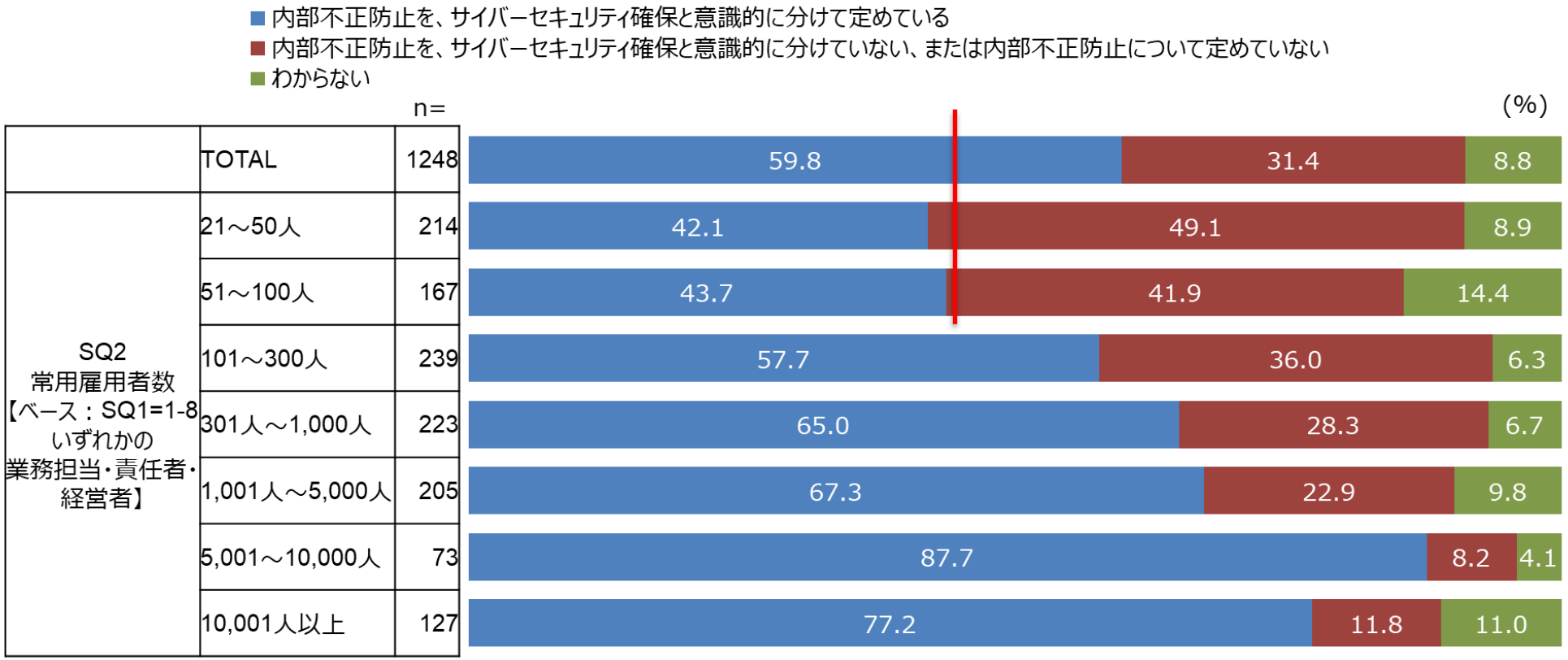


（注5：再掲）例えば、会社等への不満・鬱憤をきっかけとした秘密情報の開示・漏えい、離職前の秘密情報持ち出し・転職先での利用、不注意による秘密情報の社外送信／公開・記録媒体の紛失等がある。

7-1. 企業アンケート調査のクロス集計による分析(3/13)　～中小企業の現状分析～

従業員数が100人以下の企業では、内部不正防止の基本方針を別建てで定めているところは、全体平均と比べて格段に少ない。回答割合は42-44%に留まっており、半分に満たない。原因の１つが要員数やリソースの不足にあるとすれば、無理して内部不正防止とサイバーセキュリティの取組を別建てにしようとするよりは、経営層の強いリーダーシップの下で両者に一体的に取り組む体制を構築し、内部不正防止に特有の取組を後から補強する方が合理的であると考える。

Q4.経営層は、秘密情報保護に関する基本方針等で、内部不正防止（注5）をサイバーセキュリティ確保と意識的に分けて定めていますか。あてはまるものを１つお選びください。（単一選択）



（注5：再掲）例えば、会社等への不満・鬱憤をきっかけとした秘密情報の開示・漏えい、離職前の秘密情報持ち出し・転職先での利用、不注意による秘密情報の社外送信／公開・記録媒体の紛失等がある。

7-1. 企業アンケート調査のクロス集計による分析(4/13)　～中小企業の現状分析～

若干の例外はあるが、従業員数が小さくなるほど、個人情報以外の秘密情報の特定・格付け・表示に関する取組の実施率が低下する。従業員数が50人以下になると、回答割合は約32%に留まり、ほぼ少数派である。このため、秘密情報を特定するためのルール作りを強化するための取組が求められる。これらの改善を進めるためには、経営層のリーダーシップが企業を大きく変える中小企業の特性を活かすことが効果的であり、事業リスクの理解度が高い経営層が自社の事業にとって重要な秘密情報の特定を主導するのが合理的だと考えられる。

Q7.個人情報以外の秘密情報（営業秘密、重要なデータ等）の特定と格付けの実効性を高めるために、組織全体でどのような取組を実施していますか。あてはまるものをすべてお選びください。（複数選択）

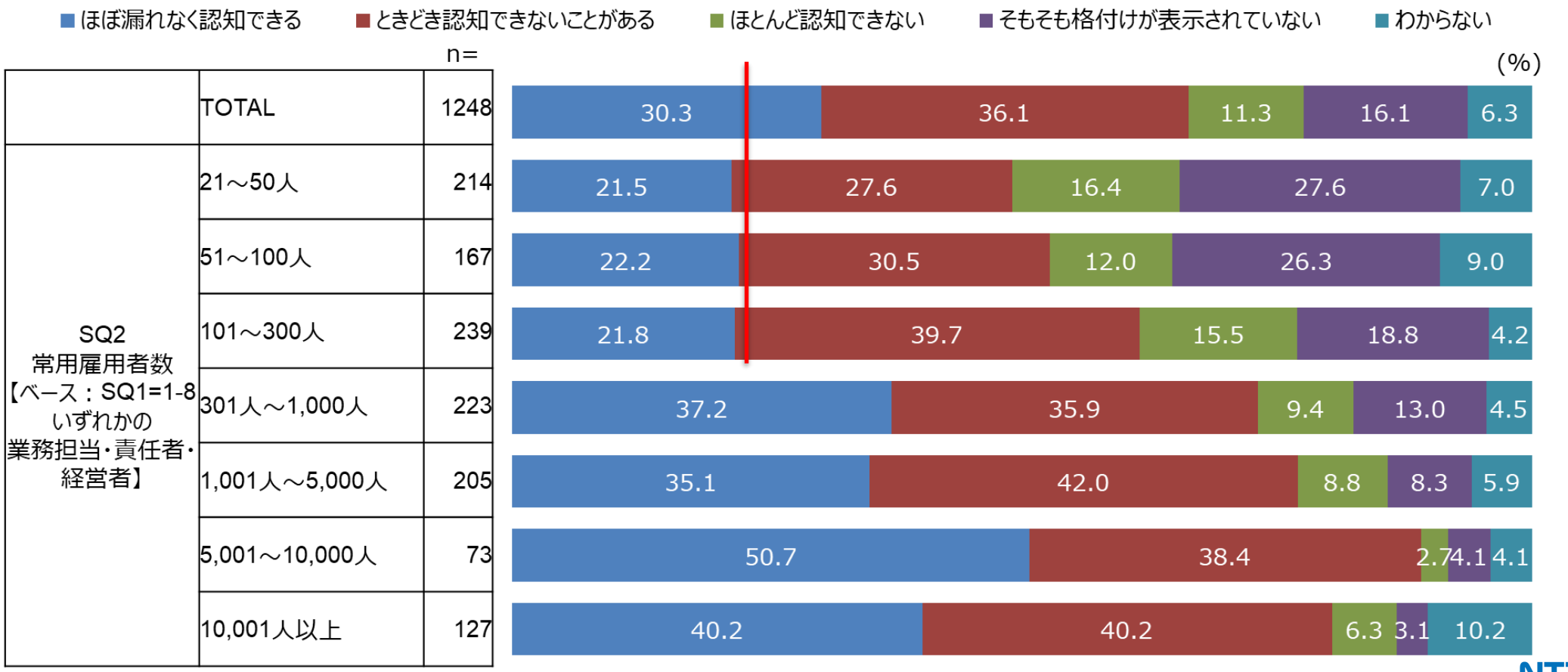
(%)

		n=	個人情報以外の秘密情報（営業秘密、重要なデータ等）を特定するための具体的な基準や、この基準の全社運用を求める共通ルール等を定めている	個人情報以外の秘密情報を格付けするための基準やこの基準の全社運用を求める共通ルール等を定めている	個人情報以外の秘密情報を特定または格付けする基準を適用しやすいように例を示している	格付けが漏れなく実行されるための仕組みを設け、継続的な改善を図っている	格付けをわかりやすく表示するためのルールを定めている	格付け表示がない（不明瞭な場合を含む）社内情報の取扱いについてもルールを定めている	重要な秘密情報を取り扱うプロジェクトに参加する条件として、「保護対象とする重要な秘密の範囲を明確にした上で、上述した基準やルールの順守・徹底をあらためて誓約すること」を求めるルールを定めている	定期的に、基準やルールを順守しているかを確認している（定期的なセルフチェックを含む）	何も実施していない	上記以外	わからない
	TOTAL	1248	55.4	33.3	27.9	18.3	18.0	15.4	17.4	37.4	11.9	0.4	4.7
SQ2 常用雇用者数【ベース：SQ1=1-8いずれかの業務担当・責任者・経営者】	21～50人	214	32.2	15.4	16.4	7.5	7.9	8.9	7.0	24.8	29.4	0.0	5.6
	51～100人	167	44.9	22.8	19.2	11.4	10.8	13.8	12.6	28.1	19.2	1.2	7.8
	101～300人	239	50.6	34.3	24.7	13.4	12.1	12.1	14.2	30.1	11.7	0.4	3.3
	301人～1,000人	223	64.6	29.6	29.1	17.9	22.4	15.7	17.5	47.5	7.2	0.0	4.0
	1,001人～5,000人	205	63.9	39.0	35.1	23.9	17.6	15.1	19.0	40.5	3.9	0.0	4.9
	5,001～10,000人	73	75.3	56.2	38.4	35.6	37.0	21.9	35.6	54.8	0.0	2.7	1.4
	10,001人以上	127	75.6	59.8	44.9	36.2	37.8	30.7	33.9	52.0	1.6	0.0	4.7

7-1. 企業アンケート調査のクロス集計による分析(5/13)　～中小企業の現状分析～

中小企業では秘密情報の格付け表示が実効性を持って実施されている割合が全体平均と比べて低く、従業員が内容を見なくても秘密情報であると認識できる状況とは言い難い。回答割合は22%前後に留まっており少数派である。個人情報以外の秘密情報の特定と格付けの全社基準に基づくシステム上の分離保管（フォルダで仕分けし、アクセス権限を格付けに合わせて設定）の導入等が現実的な対応であると考えられる。

Q8.従業員は、自部署・他部署の情報に関わらず、個人情報以外の秘密情報に触れた際に、格付けの表示等によってほぼ漏れなく秘密情報であることを認知できますか。あてはまるものを１つお選びください。（単一選択）



7-1. 企業アンケート調査のクロス集計による分析(6/13)　～中小企業の現状分析～

従業員数と、秘密情報の不自然な扱いや不正な漏えいを報告するルール等を定めているとの回答割合は連動しており、前者が増えるほど後者も高まる。中小企業では従業員と経営層の距離は大企業に比べて近いはずだが、経営層へと報告が上がるルートの確立度合いは大企業が勝る。一方で中小企業は、経営層のリーダーシップ次第でこの状況を一変できる可能性を持っていると考える。

Q12.秘密情報が不自然に取り扱われていることや、社外への不正な漏えいを目撃した際に、上司や全社責任者／経営層に報告を上げる体制やルールがありますか。あてはまるものをすべてお選びください。（複数選択）

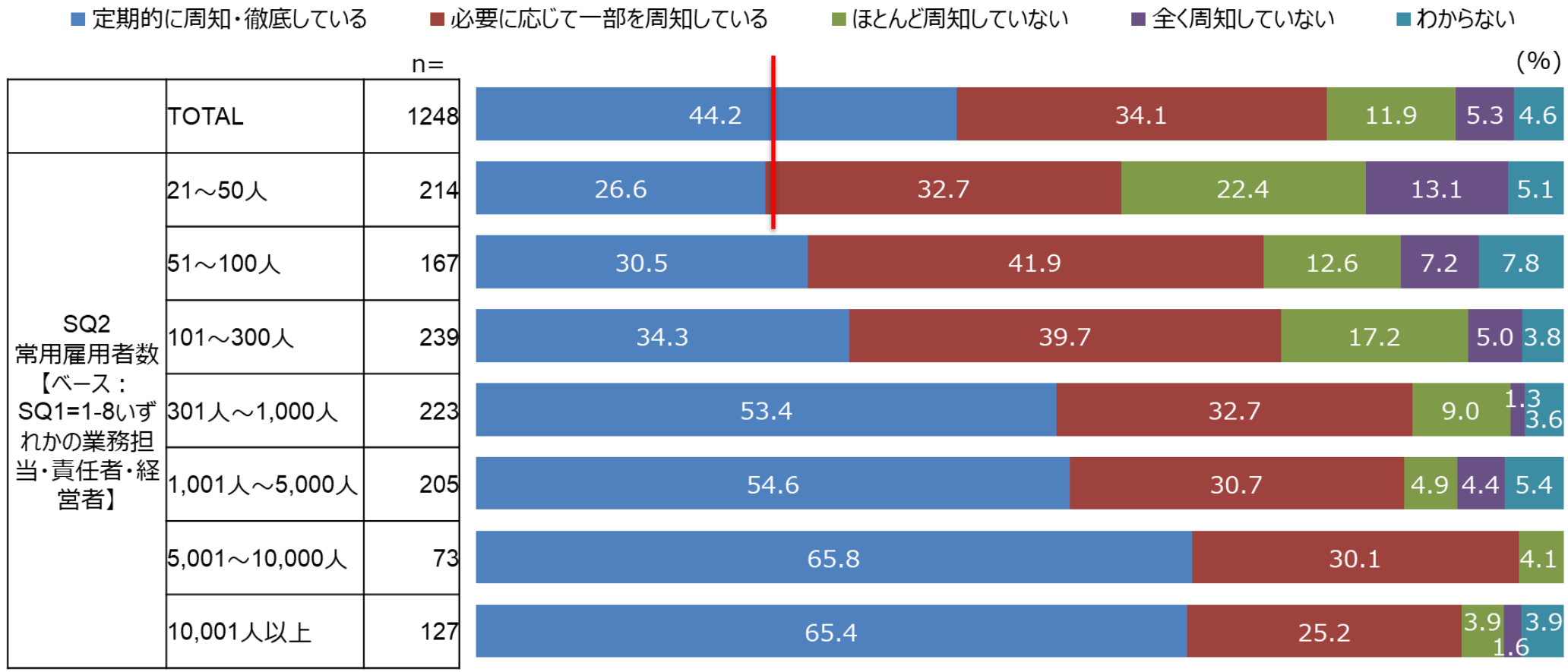
(%)

		n=	直属の上司にすぐに報告するルールが定められている	秘密情報の管理責任者にすぐに報告するルールが定められている	全社責任者／経営層に報告が上がるルートが確立している	内部通報体制が整備されている	わからない
	TOTAL	1248	55.0	46.6	34.4	26.3	10.6
SQ2 常用雇用者数【ベース：SQ1=1-8いずれかの業務担当・責任者・経営者】	21～50人	214	37.9	23.4	29.4	14.5	22.0
	51～100人	167	49.1	35.9	29.3	20.4	16.8
	101～300人	239	49.0	46.9	33.9	20.5	11.3
	301人～1,000人	223	64.1	50.7	35.0	30.9	7.6
	1,001人～5,000人	205	62.4	60.0	36.1	29.3	3.4
	5,001～10,000人	73	72.6	65.8	46.6	35.6	1.4
	10,001人以上	127	65.4	59.1	39.4	46.5	3.9

7-1. 企業アンケート調査のクロス集計による分析(7/13)　～中小企業の現状分析～

秘密情報の不自然な扱いや不正な漏えいを目撃した際の望ましい行動を定期的に周知・徹底している割合は、従業員数が増すほど高まる。従業員数が100名以下の企業においては該当するのはほぼ少数派である。お互いに顔が見える関係であるため、性善説に拠っていることが多く、内部不正等の報告等に必ずしも積極的ではないものと推察される。

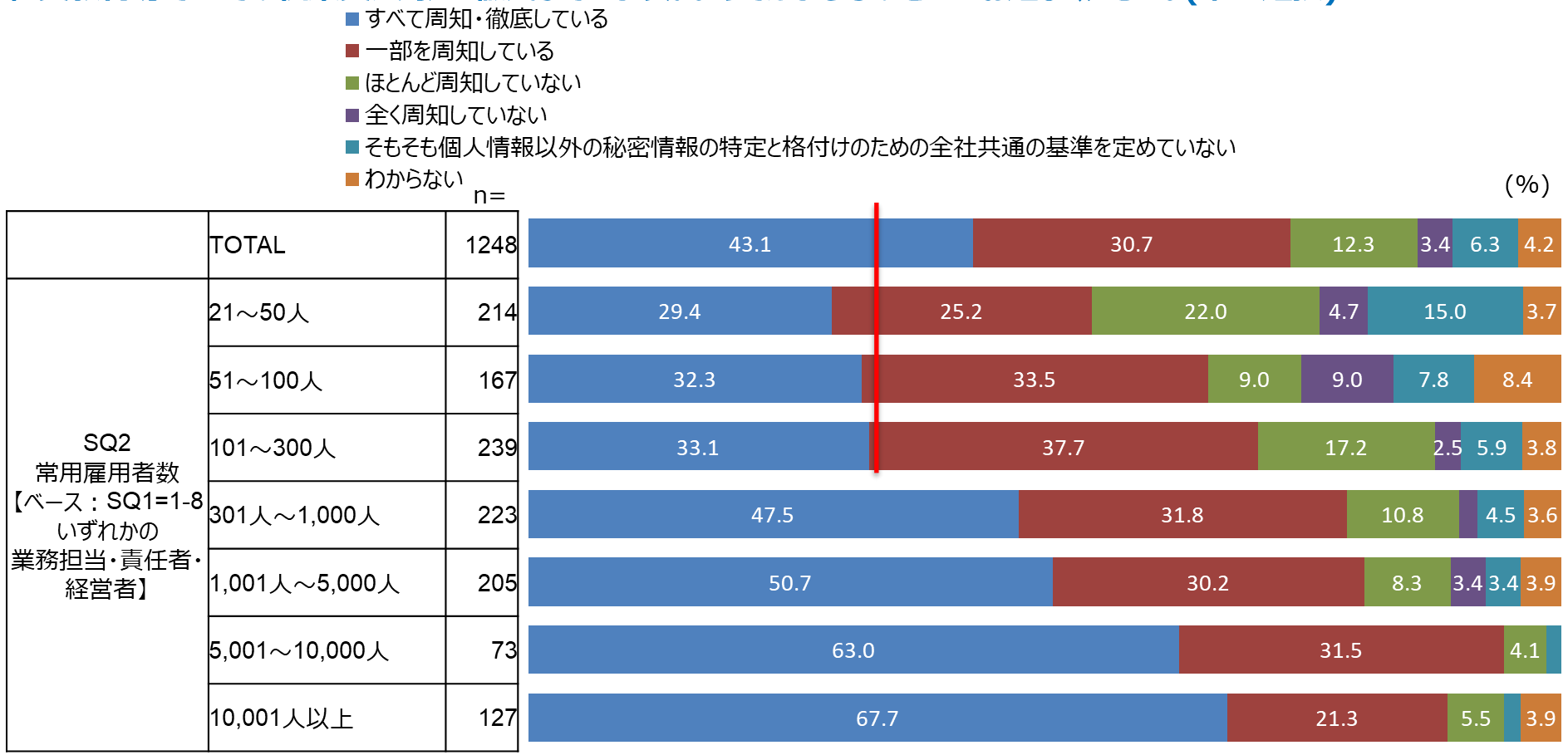
Q16.秘密情報が不自然に取り扱われていることや、社外への不正な漏えいを目撃した際の適切な行動について、社員教育等で組織全体に周知・徹底していますか。あてはまるものを１つお選びください。(単一選択)



7-1. 企業アンケート調査のクロス集計による分析(8/13)　～中小企業の現状分析～

個人情報以外の秘密情報の特定と格付けの全社基準を周知・教育については、大企業ではほぼ過半が実施しているのに対し、該当する中小企業はほぼ少数派である。この現状を改善するためには、例えば、こうした基準に基づくシステム上の分離保管（フォルダで仕分けし、アクセス権限を格付けに合わせて設定）等の簡易な仕組みを構築し、当該基準の周知・徹底を推進するのが現実的であると考えられる。

Q15.個人情報以外の秘密情報（営業秘密、重要なデータ等）の特定と格付けのための全社共通の基準を、社員教育等で全ての従業員に周知・徹底していますか。あてはまるものを１つお選びください。(単一選択)



7-1. 企業アンケート調査のクロス集計による分析(9/13)　～中小企業の現状分析～

内部不正にあたる違反行為や罰則の定めを周知している割合は従業員数が減るほど下がる。中小企業での回答割合は、違反行為の周知が35-50%、罰則の定めの周知が28-35%に留まっており、改善が求められる。経営層が経営方針として営業秘密等の保護に関する禁止事項や罰則を重視しているのであれば、経営層自らが従業員を集めて周知徹底することの効果が高い。

Q17.個人情報以外の秘密情報（営業秘密、重要なデータ等）の漏えいや内部不正に関し、何をしてはいけないのか、何をするとどのように罰せられるのかを例示する等、従業員に対してわかりやすく周知していますか。あてはまるものをすべてお選びください。(複数選択)

(%)

		n=	社内規程等において秘密情報等に係る違反行為を周知している	違反行為に対する罰則を周知している	これまでの違反行為に係る処罰事例等を周知している	周知していない	わからない
	TOTAL	1248	56.9	38.5	25.1	15.0	4.3
SQ2　常用雇用者数【ベース：SQ1=1-8いずれかの業務担当・責任者・経営者】	21～50人	214	35.0	28.0	21.0	31.3	4.2
	51～100人	167	47.3	26.9	24.6	19.2	6.6
	101～300人	239	49.4	34.3	21.8	18.4	3.8
	301人～1,000人	223	67.7	43.9	26.5	9.0	3.6
	1,001人～5,000人	205	63.4	46.8	24.9	7.8	4.9
	5,001～10,000人	73	82.2	49.3	39.7	2.7	1.4
	10,001人以上	127	76.4	50.4	28.3	4.7	4.7

7-1. 企業アンケート調査のクロス集計による分析(10/13)　～中小企業の現状分析～

e-Learning以外の方法を取り入れている割合は従業員数が減るほど下がる。特に、従業員数が50人以下の中小企業では全般的に回答割合が30%を下回っている現状にある。中小企業に対し、インシデント事例や解説動画などの積極的な活用を推奨していくことが望ましい。

Q18.秘密情報漏えいや内部不正防止の従業員教育にあたり、e-Learning以外の方法を実施していますか。あてはまるものをすべてお選びください。(複数選択)

(%)

		n=	インシデント事例を説明している	解説動画・イラスト等のリッチコンテンツを利用している	グループディスカッションを実施している	規則を順守しているかを定期的にセルフチェックするように求めている	実施していない	わからない
	TOTAL	1248	44.5	33.2	27.1	33.7	21.7	4.2
SQ2 常用雇用者数【ベース：SQ1=1-8いずれかの業務担当・責任者・経営者】	21～50人	214	24.8	15.4	17.8	21.5	40.2	3.3
	51～100人	167	32.9	13.8	23.4	29.9	31.1	8.4
	101～300人	239	38.1	25.9	21.3	29.3	25.1	4.2
	301人～1,000人	223	52.0	39.5	27.4	37.2	18.4	2.7
	1,001人～5,000人	205	53.7	46.8	32.2	39.0	9.8	4.4
	5,001～10,000人	73	63.0	61.6	46.6	41.1	6.8	1.4
	10,001人以上	127	66.1	52.8	38.6	48.0	5.5	4.7

7-1. 企業アンケート調査のクロス集計による分析(11/13)　～中小企業の現状分析～

秘密保持義務契約／誓約を求めている企業の割合は従業員数が小さくなるほど下がる。会社全体で取扱う秘密情報の数と種類が多くない中小企業では、現実的な負荷の範囲で「秘密保持義務を課す秘密情報の範囲をリスト化する」ことができると見込まれることから、まずは雇用終了時の契約／誓約を強化するとともに、上述したリストによって秘密保持義務の適用範囲の明確化に取り組むのが良いと考えられる。

Q22.以下に列挙した「秘密情報の漏えいに繋がる内部不正の防止」に特有の対策のうち、貴社で実際に実施しているものはどれですか。あてはまるものをすべてお選びください。（複数選択）

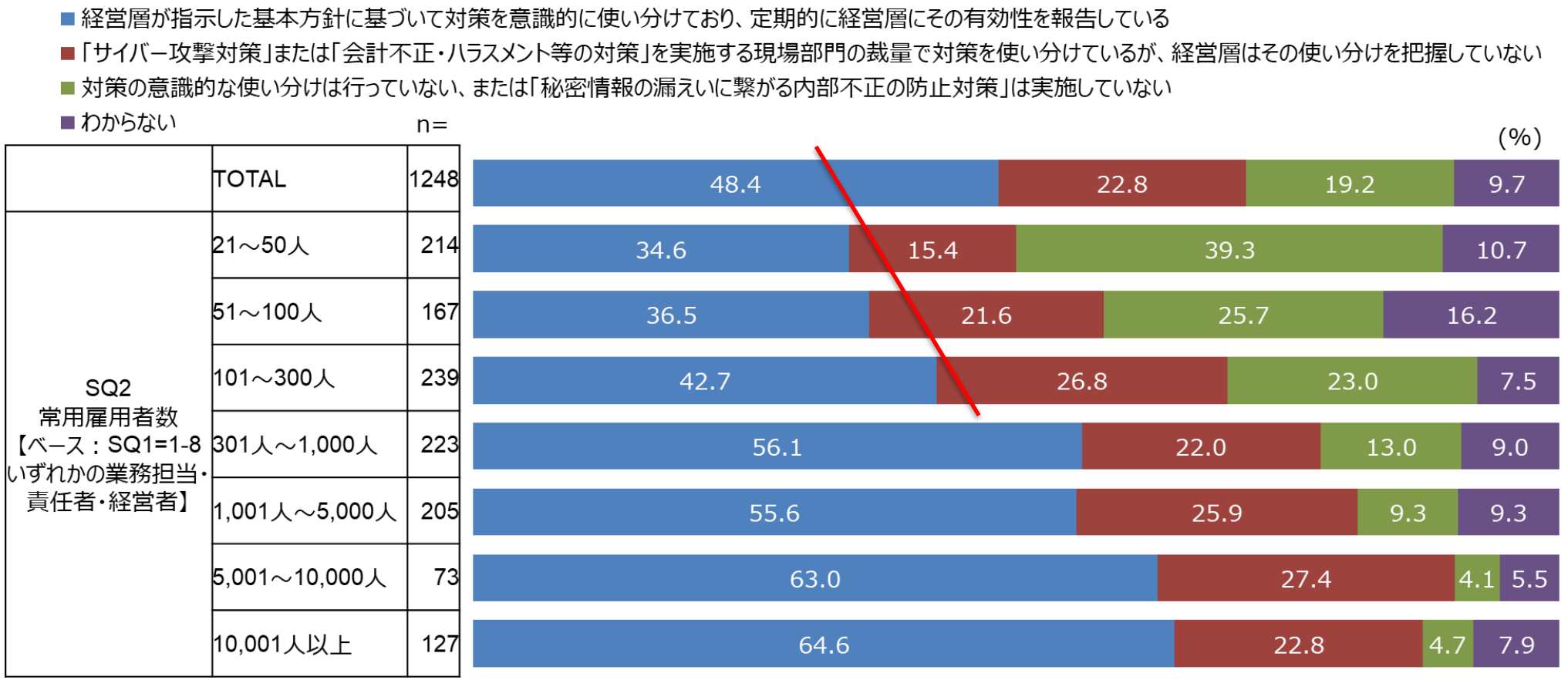
(%)

		n=	1．秘密情報の不正な開示・漏えいに繋がらないように、会社等への不満・鬱憤を蓄積させない職場環境（過度の超過勤務がない、公平に評価される、ハラスメント行為がない、良好なコミュニケーションが確保されている等）を整備している	2．就業規則に従業員の秘密保持義務を明記し、雇用開始時、及び雇用終了時に秘密保持義務に関する契約または誓約書の提出を求めている	3．重要な秘密情報を取り扱うプロジェクトへの参加／離任にあたり、秘密保持義務に関する誓約書を提出することを義務付けている	4．人的ミス（電子メールの誤送信、PC／USBメモリの紛失、セキュリティ設定ミス等）への十分な注意を指示・徹底している	5．社内システム等の操作の異常や不正の可能性（深夜や休日の操作、大量のファイルダウンロードなど）を、ログに基づいて定期的に確認している	6．中途退職を予定している従業員については、過去に遡って5．のログ確認を実施している	7．5．や6．の対策実施を従業員に周知し、不正の抑止力として役立てている	8．秘密情報の漏えいに繋がる内部不正に対する罰則を定めて、社員教育等で従業員に周知・徹底している	9．テレワークやクラウドサービスで取り扱うことができる秘密情報を制限するための基準を設け社員教育等で従業員に周知・徹底している	10．不必要な秘密情報を取引先等に渡さないように、社員教育等で従業員に周知・徹底している	11．秘密情報の漏えいに繋がる内部不正の防止対策は実施していない	12．わからない
	TOTAL	1248	57.6	54.4	25.6	50.5	36.2	17.0	14.9	23.2	33.7	32.4	6.8	6.1
SQ2 常用雇用者数【ベース：SQ1=1-8いずれかの業務担当・責任者・経営者】	21～50人	214	38.3	41.6	15.9	36.9	15.0	10.7	7.0	13.1	15.4	20.1	16.8	8.9
	51～100人	167	46.1	47.9	19.8	45.5	22.2	11.4	10.2	24.0	22.8	34.7	8.4	10.8
	101～300人	239	51.5	54.4	16.7	49.0	34.3	11.7	10.5	15.9	27.2	27.6	7.5	5.4
	301人～1,000人	223	64.1	57.4	29.6	55.6	41.7	17.9	14.3	21.5	39.9	34.5	3.6	4.9
	1,001人～5,000人	205	67.8	57.1	27.8	55.1	48.8	18.5	19.0	29.8	43.4	38.0	2.9	5.4
	5,001～10,000人	73	76.7	69.9	42.5	61.6	50.7	34.2	31.5	42.5	52.1	38.4	0.0	0.0
	10,001人以上	127	78.0	66.1	46.5	59.8	55.9	30.7	27.6	33.9	53.5	42.5	2.4	3.1

7-1. 企業アンケート調査のクロス集計による分析(12/13)　～中小企業の現状分析～

従業員数が増えるほど、内部不正防止対策と、サイバー攻撃や会計不正・ハラスメント等の対策とを意識的に使い分ける傾向がある。中小企業での使い分けの割合は34-43%に留まっている。原因の１つが要員数やリソースの不足にあるとすれば、無理して内部不正防止対策とサイバーセキュリティ対策を別建てにしようとするよりは、両者を一体的に強化できる対策は積極的に共有し、内部不正防止に特有の対策を後から補強する方が合理的であると考える。

Q23.上述した「秘密情報の漏えいに繋がる内部不正の防止対策」を「サイバー攻撃対策」や「会計不正・ハラスメント等の対策」と意識的に使い分けていますか。あてはまるものを１つお選びください。(単一選択)

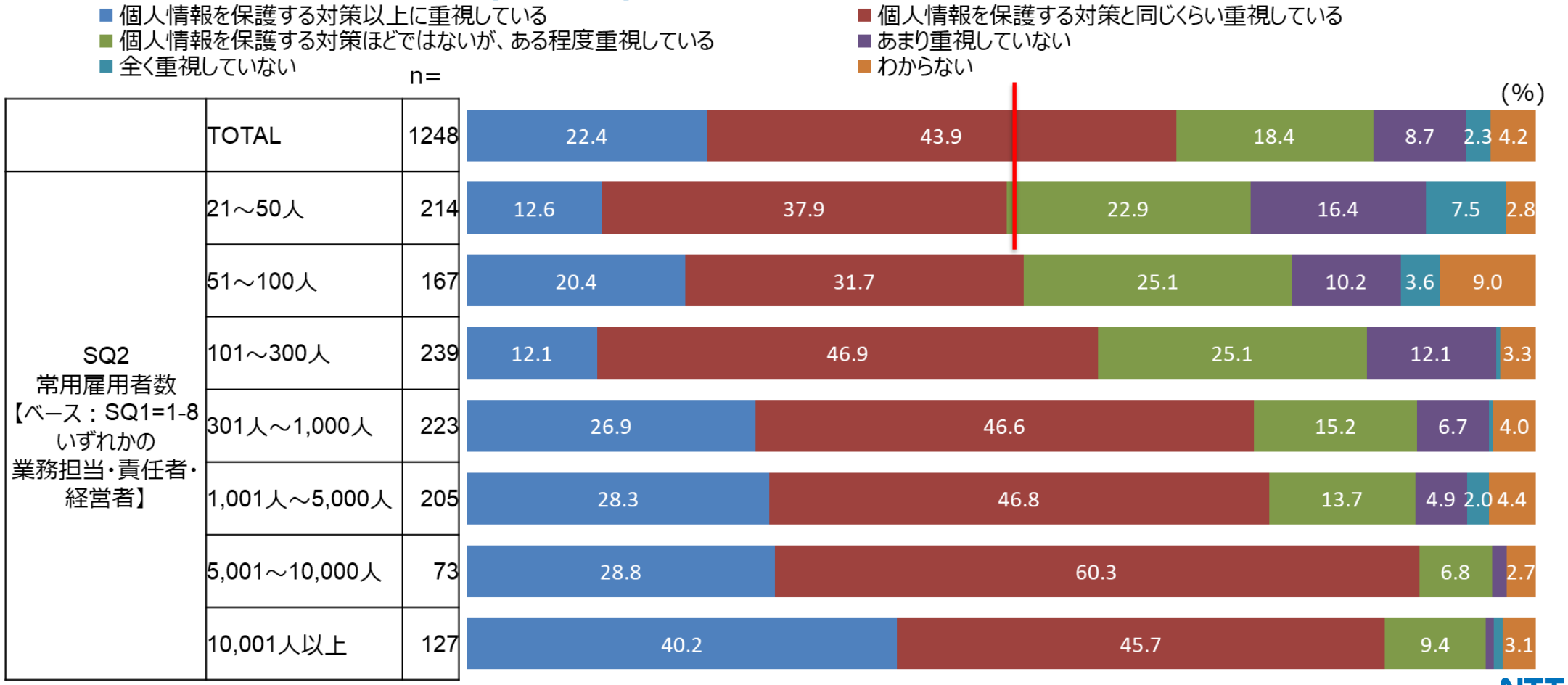


		n=	経営層が指示した基本方針に基づいて対策を意識的に使い分けており、定期的に経営層にその有効性を報告している	「サイバー攻撃対策」または「会計不正・ハラスメント等の対策」を実施する現場部門の裁量で対策を使い分けているが、経営層はその使い分けを把握していない	対策の意識的な使い分けは行っていない、または「秘密情報の漏えいに繋がる内部不正の防止対策」は実施していない	わからない
	TOTAL	1248	48.4	22.8	19.2	9.7
SQ2 常用雇用者数【ベース：SQ1=1-8いずれかの業務担当・責任者・経営者】	21～50人	214	34.6	15.4	39.3	10.7
	51～100人	167	36.5	21.6	25.7	16.2
	101～300人	239	42.7	26.8	23.0	7.5
	301人～1,000人	223	56.1	22.0	13.0	9.0
	1,001人～5,000人	205	55.6	25.9	9.3	9.3
	5,001～10,000人	73	63.0	27.4	4.1	5.5
	10,001人以上	127	64.6	22.8	4.7	7.9

7-1. 企業アンケート調査のクロス集計による分析(13/13)　～中小企業の現状分析～

個人情報保護との比較において営業秘密等を保護する対策を同等以上に重視している割合は従業員数が小さくなるほど下がる。特に、従業員数が50人以下の中小企業では格段に少なく、回答割合は50.5%である。製造業のサプライヤ等のように、中小企業であっても技術情報等の営業秘密の重要性が高い企業も多くあるため、さらに底上げしていくことが望ましい。

Q20.個人情報保護だけでなく、それ以外の秘密情報（営業秘密、重要なデータ等）を保護する対策も重視していますか。あてはまるものを１つお選びください。(単一選択)



7-2. 改善策と現状を比較した結果　～中小企業について～

＜中小企業における調査軸１：経営課題の改善＞

中小企業に焦点を絞って、「経営課題の改善」という調査軸に対して整理された改善策と現状を比較するとともに、改善策に関わる好事例や改善策を補う示唆を抽出し、取りまとめた。（以後同様）

改善策	改善策と現状の比較	改善策に関わる好事例	改善策を補う示唆
【6-1-1】経営層または内部不正防止に関する組織全体の責任者等が率先して、重要な秘密情報漏えい／内部不正リスクを重要な経営課題として認識する機会を増やし、サイバーセキュリティ確保と内部不正防止を一体的に認識した経営を行う。	中小企業における経営層のリスク認識は相対的に低く、その一方で、社会環境の変化に伴う秘密情報の漏えいや内部不正防止といった課題の重要度は高まっているとの認識が広がっている。リスク認識の担い手となる意識の高い人材の不足が指摘されており、人材確保・育成と共に、すべての起点となる経営者自身の意識を高めることが特に重要であると考えられる。	・業界の流れを意識し、技術情報管理の認証取得に取り組んだことが良い契機となった。 ・秘密情報との関りが深い事業を展開しているため自社でもしっかり取り組むことが必須だった。 ・悪意の有無に関わらず、人為的な秘密情報漏えいのリスクが高いと考えて経営している。	・中小企業では経営層が高い意識を持って率先し牽引すれば会社全体の取組状況をがらりと変えられる可能性を持っている。 ・経営層が秘密情報の漏えいや内部不正防止について全社にしっかりと自分の経営方針を話していくことが望ましい。 ・中小企業では、営業秘密を社内できちんと保護する体制を構築することで、秘密情報漏えい／内部不正防止にも好ましい効果が生じる。
【6-1-2】中小企業では、全社集会などの経営層が従業員に周知徹底する機会を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。	全体としても過半の企業において経営層による一般従業員・関連部門との対話の場が設けられている中で、中小企業ではそれが奏功した場合の効果が大きく期待できることに強みがあると言える。実際、意識の高い経営者による積極的な取組と、それが実際の効果につながっている事例が確認された。他方で、企業規模が小さくなるほど取組度合いも弱くなる傾向があり、大企業を含む全体平均に比べると相対的に不十分である。経営層が部下に任せきりになりがち、潤沢にリソースを投入することが難しい等の、中小企業における一般的課題が関わっているものと考えられる。 また、従業員100名以下の企業では、内部不正防止をサイバーセキュリティ確保と意識的に分けるかどうかが概ね拮抗しているため、サイバー攻撃防止とは異なる内部不正防止の特徴等を発信できていない企業が相対的に多くなる。	・経営者が自ら基本方針を全社に周知・徹底している。 ・定期的にも日常的にも経営者が社員に語ることで意識付け・啓発に効果を上げている。 ・漏えいが自社の信頼失墜に直結することを強く認識して全社に周知・啓発している。 ・秘密情報漏えい／内部不正防止の取組が特に進んでいる中小企業では、情報漏えい／内部不正防止に関する基本方針を情報セキュリティポリシーとは完全に別建てで定めている。 ・ISMS、プライバシーポリシー、技術情報管理等の認証取得が、中小企業の経営者が基本方針を定める契機となって取組が進んだ。	・従業員と直接コミュニケーションを取って趣旨をしっかりと伝えることで、ある程度リスクに対応できる。 ・中小企業の取組強化に向けては、経営者が戦略を語り、コミットメントや指示に自身の想いやこだわりを込め、日々語ることが重要である。 ・経営層が何をどの程度重視しているかを率直に伝えることで、従業員がこれを評価して行動することを期待できる。 ・埋めるべきギャップは大企業より中小企業の方が小さいので、ひとたび良い方向に動き始めると、目標レベルに素早く到達できる。 ・中小企業の規模やリソースを考慮すると、秘密情報漏えい／内部不正防止とサイバーセキュリティを敢えて分けて取り組む必要はない。

7-2. 改善策と現状を比較した結果　～中小企業について～

＜中小企業における調査軸２：重要な秘密の特定と取扱いの改善＞

改善策	改善策と現状の比較	改善策に関わる好事例	改善策を補う示唆
【6-2-1】中小企業では、経営層が自ら判断する、あるいは判断基準を示すことで、自社の事業にとって重要性／機密性の高い秘密情報を的確に特定する。	全体としても秘密情報の格付け・表示に課題がある中で、中小企業における取組は更に劣後している。秘密情報の特定も十分ではない。紙媒体のような物理的実体のある秘密の保護に比べ、電子化された秘密情報の管理は進んでいない。一方、内部不正防止にもつながる認証の取得を経て具体的な取組に至る事例もあり、経営者の意識付けも兼ねて、何らかの認証の取得を考慮することが実践的な方策の一つになると考えられる。	・経営者が自ら事業リスクの判断や秘密情報の特定・格付けを行っている。 ・経営者が情報セキュリティや技術情報管理の認証取得を決断し、これに取り組んだことが契機となって、営業秘密等の特定、格付け、表示に関する体制整備が進んだ。 ・認証制度が要求する管理基準に従い、秘密情報を管理できる情報資産台帳を作成している。 ・認証制度に沿って特定した情報資産については、情報の保存場所や保存期間、データ消去の方法やリスクの大きさ、格付けを台帳管理している。 ・情報資産を保存する共有フォルダ等の場所を格付けに沿って切り分け、かつ、適切なアクセス制御・記録を合わせることで、格付け・表示・アクセス管理を一体に実施している。	・経営者の負担を避けるため、部下を育成し、権限移譲を考えることも必要である。

7-2. 改善策と現状を比較した結果　～中小企業について～

＜中小企業における調査軸３：組織体制・連携に関する課題の改善＞

改善策	改善策と現状の比較	改善策に関わる好事例	改善策を補う示唆
【6-3-1】 中小企業では、責任者である経営層が中心となって、総務・人事・法務や情報システム等の関連部門との調整を行う。	規模によれども中小企業では人事・法務といった専門部署が必ずしも細かく分かれていないという現実がある中で、調査結果からは内部不正防止についても経営層が直接の責任者となりやすい様子がうかがえる。改善策が求めるような、経営層が中心となっての総務・人事・法務や情報システム等の担当との調整は、リソース制約の大きい中小企業では現実的な選択肢と言える一方で、それが片手間の取組となって効果を損なうことのないように注意する必要がある。	・秘密情報漏えい／内部不正防止とサイバーセキュリティの担当役員を分け、監督も別々に実施し、経営者がこれを統括している。 ・経営者を責任者とする3~5名程度の幹部による委員会を設置している。その下にシステム、総務・人事、教育、内部監査等を担当する幹部が集まって委員会を構成する。 ・経営者が責任を担い、品質管理責任者が横串を通す形で、関連部門を連携させている。各種のマネジメントシステムを構築・運用する際に品質管理責任者が必ずこれに協力し、品質管理責任者を中心とした社内ネットワークを形成している。 ・秘密情報保護に関する重要な主題（秘密保持義務の誓約、懲罰、情報セキュリティ対応等）ごとに担当チームを組成し、各チームが基本方針を定めて取組を実施している。経営者はチーム全体の統括責任者となり、必要に応じて各チームと関連組織の協議を主導する。	・社内に委員会を設けるなどして、複数部門が連携して取り組むことができる体制を検討することが望ましい。
【6-3-3】 重要な秘密が不自然に取り扱われている様を目撃した際に上に報告することの徹底と、上に報告できない事情がある場合は内部通報ができる体制を構築する。	中小企業では従業員と経営層の距離が近いと目されるところ、経営層へと報告が上がるルートの確立度合いは大企業が勝っている。この背後には、ルールに基づくマネジメントの浸透度合いと企業規模が連動するという傾向に加え、距離が近いからこそ性善説を頼ってしまいがちであるという文化も関わる。体制の整備に先立ち、経営層による現場への具体的な意識付けを行うことが有効であると考えられる。	・秘密情報が漏えいした時や従業員がヒヤリハット・不信感を認識した時に、直属の上司を通じて経営者にすぐに報告が上がってくる仕組みを設けている。	・中小企業は人間関係が良く性善説を基にしていることが多いので、内部通報ができる仕組みを構築すると逆に従業員の不信感が高まる恐れがあり、注意が必要である。

7-2. 改善策と現状を比較した結果　～中小企業について～

＜中小企業における調査軸４：社員教育とリテラシー構築に関する課題の改善＞　(1/2)

改善策	改善策と現状の比較	改善策に関わる好事例	改善策を補う示唆
【6-4-1】中小企業では、経営層のリーダーシップと社外の専門家（ITコーディネータ、弁護士・弁理士等）の協力により、情報システム部門や他の従業員に法務・知財の知識を広める。	社外の専門家の助力を得て法務・知材の知識を情報システム部門等に広める取組の実態を調査するには至らなかった。	―	・事業拡大に悪影響を及ぼしうることを考慮し、知財専門人材が社内にいない場合は業界団体等を通じて外部の専門職（弁護士・弁理士等）と連携することが望ましい。
【6-4-2】中小企業では、入社／人事異動／退職等の重要なタイミングで、経営層が重要な秘密を具体的に示し、その取扱い指示を徹底する。	改善策に言うような退職時における秘密取り扱いの説明・教育を行っている事例は見出されたが、中小企業における取組は全体としては劣後しており、例えば経営幹部のそれも含め、内部不正の発生を全社に告知している企業は4割に達しない。他社で発生した参考事例の情報を収集することも中小企業では難しく、全般に取組の底上げを図る必要があると言える。	・営業秘密・重要データの知識に関する社員教育にも取り組み、入社時のオリエンテーション、年1度のe-Learningや年2回の集合教育、全社集会の機会を活用した教育を行っている。 ・リスクとその重要性、過去に発生した事例における重要なリスクと実際に発生した損害、社内で発生したヒヤリハットの経緯や内容等を伝えている。 ・退職時に秘密情報を持ち出すリスク、実際に持ち出した事例等に重点を置いて教育している。 ・中途退職時に禁止されている事項を教育している。 ・経営者が自ら参考事例等の情報を収集している。 ・セキュリティ会社に委託し、他社で発生した事件の情報、注意点、セキュリティ管理の考え方等の情報を提供してもらっている。	・中小企業には営業秘密の秘密管理性の確保が自己防衛及びビジネス拡大に不可欠であることを大企業以上に認識してもらうことが望ましい。
【6-4-3】経営層または経営層が権限を移譲した責任者が各々の秘密の重要度を指定した上で、この指定に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。	中小企業における営業秘密等の特定・格付けに関する周知・教育の実施割合は大企業に比べてはっきりと劣後している。しかしながら、そうした周知・教育の定期実施や、表裏一体になるはずの秘密情報の格付け・表示の徹底は大企業でも十分とは言えない状況であり、中小企業における実践と有効化は非常に難しい課題であると考えられる。	・経営者が自ら事業リスクの判断や秘密情報の特定・格付けを行っている。	―
【6-4-4】企業のサイバーセキュリティ／コンプライアンス等に関する取組の一環として、重要情報漏えい／内部不正防止の社内規程及びその規則、モニタリングの目的や実施状況等に焦点を当てる回数を増やす。	内部不正防止対策として従業員の行動を記録・監視することへの抵抗感が中小企業の間には見られる。有識者も指摘する通り、中小企業では経営層と従業員の距離が近く、このような心理的課題への対処に当たっては経営層自身の細やかな配慮が必要になると考えられる。	・抵抗感を示す事例以上に、有識者の適切な助言等に基づいてこれを導入し組織に根付かせることで、むしろ会社への帰属意識や仕事に対するプライドといったものが上がってきて緊張感が醸成され、会社の雰囲気が良くなってきたと言われることも多い。	―

7-2. 改善策と現状を比較した結果　～中小企業について～

＜中小企業における調査軸４：社員教育とリテラシー構築に関する課題の改善＞　(2/2)

改善策	改善策と現状の比較	改善策に関わる好事例	改善策を補う示唆
【6-4-5a】 中小企業では、経営層が自ら事業リスクに基づいて、営業秘密や限定提供データの取り扱いについて何をしてはいけないのかを指示・啓発する。	内部不正に当たる違反行為や罰則の定めを周知している割合は、大企業で過半を占めるのに対し、中小企業では半分に満たず、取組状況に隔たりが見られる。経営層による指示・啓発の全体像を調査するには至ってないが、実際に経営者が手ずから取り組んでいる事例は確認できており、改善策の方向性は妥当であり、かつ、今後の浸透が望まれる内容と言える。	・営業秘密や限定提供データに関する従業員教育で、これらの取扱方法に加えて、禁止事項・内規の懲罰規定・法の遵守等についても教育している。 ・個人情報保護法、不正競争防止法、外為法等を対象として解説動画や弁護士の説明を教材に取り入れて従業員に教育することで、民事的な賠償責任や刑事責任を負ったりする場合があること等を理解させている。 ・経営層が率先して集める、外部委託先から情報提供を受ける等の手法で、他社で発生した事案の情報を取りまとめ、社会的な影響なども含めて教育している。	―
【6-4-5b】 中小企業では、経営層が全社集会などで直接従業員に教育・意識づけする。	中小企業ではe-Learning以外の方法を取り入れている割合が下がる傾向がある。相対的によく実施されているのはインシデント事例の説明だが、実施率で見ると4割に満たず、経営層と従業員の距離の近さを生かし切れていない状況と言える。	・人数とリソースが少ない中小企業が選択しやすい教育方法として、外部講師（例えばITコーディネータ）を招いて研修を行っている。 ・日常業務において秘密情報の取り扱いに問題がないか、社員同士で相互確認する日々実践形式の教育を取り入れている。	―

7-2. 改善策と現状を比較した結果　～中小企業について～

＜中小企業における調査軸５：対策実施に関する課題の改善＞　(1/2)

改善策	改善策と現状の比較	改善策に関わる好事例	改善策を補う示唆
【6-5-1】中小企業では、経営層と担当者が協力して、重要情報（営業秘密や限定提供データ等の知財を含む）漏えい対策に役立つ官民の関連ガイドライン／ハンドブックの情報を収集し、活用を進めることで、必要な対策を見直す。	中小企業における各種ガイドラインの活用状況を具体的に調査するには至らなかった。	―	―
【6-5-2】経営層が積極的に従業員とコミュニケーションを取ることで、従業員の行動監視やログの記録・分析等に対する従業員の理解を得る。	内部不正防止の一環として従業員の行動を記録・監視することに中小企業の間では抵抗感がある一方で、十分なコミュニケーションをとり、なぜ記録・監視が必要であるかをていねいに説明することで理解を得ている事例のあることを確認できた。改善策の示す方向の妥当性を裏打ちするものと言える。	・ITシステムのアクセス等のログを取得して定期的に確認することについて、十分なコミュニケーションを取ってインシデント対応のために必要であることをていねいに説明することで、従業員の理解と信頼が得られている。	―
【6-5-3】中小企業では、重要情報漏えいの防止体制の下で、サイバーセキュリティと内部不正防止の両方に共通する対策を積極的に１つにまとめる。	中小企業においては内部不正防止対策とサイバーセキュリティ対策を同一の取組の一環として実施する傾向がある。この背景には、リソース制約に加えて、ISMSや技術情報管理のような認証制度のスコープ中に内部不正防止が含まれていることが関わっていると考えられる。ただし、これは内部不正防止に固有の対策の実施が弱体化するという懸念もはらむものであり、実際、従業員数が増えるほど内部不正防止対策を他の対策と使い分ける傾向も見出された。経営資源に合わせた適切なバランス配分・判断が必要であると言える。	・秘密情報の漏えい防止に向けた内部不正防止対策とサイバーセキュリティ対策を同一の取組の一環として実施している。この一因として、ISMSや技術情報管理の認証のスコープが両者をカバーしていることが挙げられる。 ・ミスが発生した際の報告について、これを隠ぺいする組織風土にならないように、自発的な報告を考課で高く評価している。 ・経営者が自ら事業運営と内部不正防止／情報セキュリティの両方にコミットしている。	・不正が発覚した際の社内告知については、特に1人1人の顔が見えるぐらいの組織規模の場合に、慎重に伝え方を選ぶ必要がある。 ・経営者の負担が大きくなりすぎないように気を付ける必要がある。

7-2. 改善策と現状を比較した結果　～中小企業について～

＜中小企業における調査軸５：対策実施に関する課題の改善＞　(2/2)

改善策	改善策と現状の比較	改善策に関わる好事例	改善策を補う示唆
【6-5-4】内部不正のリスクシナリオを加味した重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。	内部不正防止はサイバーセキュリティに比べれば浸透していない考え方である。そこで、内部不正防止対策をサイバーセキュリティ対策に対して追加的に組み合わせる道筋の一つとして、まず内部不正リスクそのものを評価する取組に本調査では着目した。しかし、内部不正リスクを他のリスクと切り分けて評価する中小企業は半分に満たない。事例からは、リスクアセスメントの実施が、関連する認証制度の規定に強く影響されている様子が垣間見える。それぞれの企業の事情に応じたリスクアセスメントに基づく内部不正防止のアプローチは、まだハードルの高いものであると推察される。	・秘密情報漏えいの事業リスクとその重要度を事業継続性の中でどのように位置付けるかについて、経営層の間で認識を共有している。 ・従業員の秘密保持義務に関し、入社時の誓約書で「退職する時にも誓約書を提出すること」を誓約してもらっている。 ・対処の難しさを理解した上で次のような色々なリスクに注意を払っている：秘密情報の意図的な持ち出し、電子メールの誤送信、その他不注意やミスによる情報漏えい、個人所有のBYOD利用、中途退職者の持ち出し。	・中小企業では他社の事例等に基づいて意識の高い経営層がリスクを判断できれば、秘密情報漏えいや内部不正のリスク評価をある程度代替できる。
【6-5-5】個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。	内部不正防止は営業秘密漏えいの防止と密接に結びつくが、そもそも営業秘密等の保護を重視する企業の割合は企業規模が小さいほど下がる。営業秘密等の保護をあまり重視しないとする中小企業は一定数存在し、経営層を筆頭にその重要性を浸透させていくことが重要な状況と言える。	・経営者のリーダーシップの下で、採用・退職・プロジェクト異動等の際に、都度必要な秘密保持義務契約を締結している。 ・社長の意識づけに従い、プロジェクトごとに情報資産を定義しており、これに基づいて秘密情報を識別できるようにしている。これを活用し、秘密保持義務契約の対象となる秘密情報を具体的に示している。	・営業秘密を管理するための体制、何が秘密なのかをきちんと資産管理すること等から着手し、これを社内に浸透させていく過程で、自然にこれが内部不正防止・営業秘密保護・サイバーセキュリティの全ての質が向上する。 ・退職時の秘密保持義務契約において、対象とする秘密情報の範囲を具体的に示すことが重要である。 ・入社時の契約書／誓約書で、「退職時にも契約する／誓約書を出す」という条項を書いておくことが有効である。
【6-5-6】情報機密区分に応じたアクセス権限付与状況の点検、アクセス権限付与者についての定期的な棚卸しを実施する。	企業規模が小さくなるほど、情報管理の定期的な見直しや情報資産の棚卸しを定期的に実施している割合が下がる。ここでも見られるのは、技術情報管理などの認証制度を取得した場合に、その規程に沿った取組として実施が確立するという傾向である。実際上の取組を促すと同時に理解を深めるきっかけとして、これらの認証制度が果たす役割は大きいと言える。	・技術情報管理認証を取得した企業では、秘密情報の定期的な棚卸しや不要なものの消去、アクセス権限の見直しに重点を置いてこれを実施している。	―

7-3. 中小企業にとっての問題点・課題と今後のあり方

中小企業にとっての問題点・課題と、その克服に向けて得られた示唆（総括）

各調査軸に対する本調査の結論、課題及び今後の方向性について総括した。

(1) 経営課題の改善

本調査では、まだ秘密情報漏えい／内部不正防止の取組に着手できていない中小企業が、どのように取組を始めるのが良いかについて検討してきた。例えば、業界全体で技術情報管理認証の取得を推進している等の進んだ環境がある場合は、大企業と同じように、意識の高い経営者が内部不正防止とサイバーセキュリティを別の経営課題と捉えて取組を推進することもできる。しかし、こうした環境にない中小企業では、まずは経営者が秘密情報漏えい／内部不正防止を経営課題として捉え、その重要さをしっかりと理解する必要がある。これを推進するにあたり、技術情報管理等の認証取得、営業秘密管理の導入、外部専門家の支援を仰ぐ等が契機となる。ひとたび学びを得た後は、経営者は従業員に向かって、秘密情報漏えい／内部不正防止に係る自らの事業リスク認識、重視している取組、基本方針と経営戦略等をしっかりと伝えることが望ましい。

問題点・課題	克服に向けて得られた示唆
■ 経営者次第で秘密情報漏えい／内部不正の防止の取組が大きく変わってくるにも関わらず、当該主題にほとんど関心がない経営者が多い点が一番の問題点。この状況を少しでも変えていくことが大きな課題と言える。	■ 経営者が「秘密情報漏えい／内部不正の防止」の重要さを学ぶために、例えば以下のような機会を積極的に活かしていくことが望ましい。 ＜経営者が「秘密情報漏えい／内部不正の防止」の重要さを学ぶ機会（例）＞ • 業界団体による業界全体での意識付け • 認証の取得（技術情報管理認証、ISMSなど） • キーマンとなる、「秘密情報漏えい／内部不正の防止」の実務に詳しい幹部の採用 • ITコーディネータ等の外部専門家による支援 • 痛い目に遭って経験する／他社の事例から学ぶ • 営業秘密管理を社内に導入することに着手する　等 ＜経営者の学びに関する将来を見据えた有識者からの示唆＞ • 社外顧問、社外取締役等が提起した議論からの学びの活用 • グループ全体でのITガバナンス向上要請からの学びの活用 • 個人情報保護法の両罰規定（当事者企業が罰を受ける規定）を端緒とした危機感の醸成 • 委託元からの助言型監査を活用した委託元実務家との対話からの学びの活用
■ 企業規模が小さくなるほど、経営層による一般従業員・関連部門との対話への取組度合いが弱くなる。これが奏功した場合の効果が大きく期待できる中小企業の強みを活かせていない。	■ 経営者が自ら従業員に伝えるべき秘密情報漏えい／内部不正防止に係る事業リスク認識、重視している取組、基本方針と経営戦略等を持つことが課題克服の第一歩となる。このためには、まずは経営層が「秘密情報漏えい／内部不正の防止」についてしっかり学ぶ必要がある。

7-3. 中小企業にとっての問題点・課題と今後のあり方

中小企業にとっての問題点・課題と、その克服に向けて得られた示唆（総括）

(2) 重要な秘密の特定と取扱いの改善

本調査では、中小企業が重要な秘密の管理を改善するにあたり、秘密情報の特定・格付け・表示およびライフサイクル管理をどのように社内に根付かせるかに着目して検討してきた。秘密情報漏えい／内部不正防止の取組が進んでいる中小企業の事例などを基に考えると、経営者が自ら積極的に重要な秘密の特定・格付け・表示にコミットし、情報管理台帳の作成を牽引して、秘密情報のライフサイクル管理の構築を進めることが望ましい。このためには、中小企業の経営者は「秘密情報漏えい／内部不正の防止」の重要さを学ぶ機会を積極的に活かしていくことが望ましい。

問題点・課題	克服に向けて得られた示唆
■ 中小企業だからこそ、経営者が事業リスクに関する深い理解を積極的に活かして、重要な秘密情報の特定と判定基準作りに直接関与することができるが、経営者に取り組む動機を与えないとこれが動き始めない。従って、まずは経営者にどうやって動機付けするかが課題になる。	■ 経営者が「秘密情報漏えい／内部不正の防止」の重要さを学ぶために、例えば以下のような機会を積極的に活かしていくことが望ましい。（再掲） ＜経営者が「秘密情報漏えい／内部不正の防止」の重要さを学ぶ機会（例）＞ • 業界団体による業界全体での意識付け • 認証の取得（技術情報管理認証、ISMSなど） • キーマンとなる、「秘密情報漏えい／内部不正の防止」の実務に詳しい幹部の採用 • ITコーディネータ等の外部専門家による支援 • 痛い目に遭って経験する／他社の事例から学ぶ • 営業秘密管理を社内に導入することに着手する　等
■ 秘密情報をライフサイクル全体で管理する体制を構築することが課題である。この体制がないと、秘密情報を精度高く特定し格付けできたとしても、しっかり保護することは難しくなる。	■ 情報管理台帳を用いて秘密情報を管理することで、秘密情報のライフサイクル管理の進展を期待できる。 ■ こうした管理体制の構築は、ISMS、技術情報管理等の認証を取ることがきっかけになることが多い。従って、業界全体で認証の取得に取り組んでいる好事例等から学ぶのも一案である。

7-3. 中小企業にとっての問題点・課題と今後のあり方

中小企業にとっての問題点・課題と、その克服に向けて得られた示唆（総括）

(3) 組織体制・連携に関する課題の改善

本調査では、まだ秘密情報漏えい／内部不正防止の取組に着手できていない中小企業が、これらに取り組むための組織体制・連携をどのように構築するのが良いかを検討してきた。基本的には、現状のサイバーセキュリティ体制を活かし、秘密情報漏えい／内部不正防止に特有の取組を、総務・人事部門などと協力して補うことが望ましい。経営層は現場に任せきりにせず、自ら取組をコミットし、組織連携を指示する必要がある。また、総務・人事部門を含む関連部署との社内連携に関しては、経営者と数名の幹部から構成する委員会を活用すると良い。内部通報ができる体制の構築は経営者の判断に委ねるものの、中小企業においても、秘密情報漏えい／内部不正の疑い事象／ヒヤリハットを経営者までエスカレーションできる体制を積極的に整備することが望ましい。

問題点・課題等	克服に向けて得られた示唆
■ 経営層が中心となっての総務・人事・法務や情報システム等の担当との調整は、リソース制約の大きい中小企業では現実的な選択肢だが、片手間の取組となって効果を損なうことが多い。	■ 「秘密情報漏えい／内部不正の防止」の取組を社長室や総務部門に任せきりにして、経営者からはブラックボックスというような事態は避ける。経営者が自ら「秘密情報漏えい／内部不正の防止」の取組にコミットすることが求められる。 ■ 秘密情報漏えい／内部不正防止には組織横断の対策が必要である。中小企業の場合は、担当者のようなより小さな単位で経営機能が分割されていることが多いので、委員会設置などにより社内を横断しての連携が機能するよう取り計らう必要がある。
■ 中小企業では従業員と経営層の距離が近いと目されるところ、経営層へと報告が上がるルートの確立が遅れている。ルールに基づくマネジメントの浸透が進んでいないことに加え、距離が近いからこそ性善説に頼ってしまいがちであるという文化も関係している。	■ 性善説に頼りがちな中小企業の良好な人間関係を壊してしまって従業員の不信感がかえって高まるようなことがないように、経営者が従業員と十分なコミュニケーションを繰り返しながら、経営者にまで報告が上がる体制、内部通報ができる体制等の構築を進めることが望ましい。

7-3. 中小企業にとっての問題点・課題と今後のあり方

中小企業にとっての問題点・課題と、その克服に向けて得られた示唆（総括）

(4) 社員教育とリテラシー構築に関する課題の改善

本調査では、中小企業が秘密情報漏えい／内部不正防止に関する従業員教育とリテラシー構築にどのように取り組むのが良いかを検討してきた。秘密情報漏えい／内部不正防止において経営者が果たす役割の重要さを考えると、経営者は積極的に機会を設けて、自ら「秘密情報漏えい／内部不正の防止」の重要さを学ぶことが望ましい。その上で、従業員に効果的に行動を促すため、リテラシー教育において危機感に訴える方法（経営層が自らの考えで危機感やリスク認識を率直に伝える、事例を紹介して重要な秘密の内容と事件による影響の大きさ・受けた懲罰・刑罰の重さ等に気付かせる等）も併用していくことが望ましい。

問題点・課題	克服に向けて得られた示唆
■ 経営者は従業員に、「秘密情報漏えい／内部不正防止」の重要性について学ぶ機会を十分に与えていないことが多い。 ＜リテラシー構築のために学ぶべき知見の例＞ ➢ 秘密情報漏えい／内部不正リスクとその重要性 ➢ 営業秘密等の重要性 ➢ 営業秘密等の特定・格付け・周知に関する全社基準 ➢ 内部不正に当たる違反行為や罰則の定め ➢ 退職時における秘密取扱と禁止事項 ➢ 秘密情報の不自然な扱いや不正な漏えいを目撃した際の望ましい行動	■ まず、経営者が「秘密情報漏えい／内部不正の防止」の重要さを学ぶために、例えば以下のような機会を積極的に活かしていくことが望ましい。（再掲） <u>＜経営者が「秘密情報漏えい／内部不正の防止」の重要さを学ぶ機会（例）＞</u> • 業界団体による業界全体での意識付け • 認証の取得（技術情報管理認証、ISMSなど） • キーマンとなる、「秘密情報漏えい／内部不正の防止」の実務に詳しい幹部の採用 • ITコーディネータ等の外部専門家による支援 • 痛い目に遭って経験する／他社の事例から学ぶ • 営業秘密管理を社内に導入することに着手する　等 ■ 例えば以下のように従業員の危機感に訴える方法で教育することが、従業員の行動に繋がりやすい。 ➢ 経営者が自ら、自分が持つ強い危機感や、リスクが事業に及ぼす影響の大きさを、従業員に語って聞かせる。 ➢ 秘密情報の不自然な扱いや不正な漏えいを、自社や同業他社で発生した事例に照らして学ばせる。 ➢ 過去に発生した事例を紹介して、重要なリスクやこれが発現した時の影響の大きさを気付かせる。また、漏えいリスクが大きくなる重要な秘密に気付かせる。 ➢ 過去に発生した事例を紹介して、受けた懲罰や刑罰の重さに気付かせる。従業員が原因となって会社が刑罰を受ける可能性があることに気付かせる。 ■ 事例の収集は経営者が率先して行うか、あるいは経営者の考えに従って委託先（セキュリティ会社等）や専門家（ITコーディネータ等）に集めてもらう。

7-3. 中小企業にとっての問題点・課題と今後のあり方

中小企業にとっての問題点・課題と、その克服に向けて得られた示唆（総括）

(5) 対策に関する課題の改善

本調査では、まだ秘密情報漏えい／内部不正防止の取組に着手できていない中小企業が、これらに関する対策実施をどのように進めるのが良いかを検討してきた。原則としては内部不正防止対策をサイバーセキュリティ対策等と使い分けることが望ましいが、取組に着手したばかりの中小企業にこれを求めることは現実的ではないことが多い。リソース制約の厳しい中小企業においては、むしろ内部不正防止とサイバーセキュリティで共通性の高い対策を積極的に一本化しつつ、適切なバランスを考慮して個別の対策を追加的に組み合わせるのが合理的である。

また、秘密情報管理と内部不正対策の両方を同時に進展させる効果を期待できるため、秘密情報漏えい／内部不正防止の取組にこれから着手する中小企業では、まずは営業秘密管理の導入から始めて、その後の内部不正防止へのステップアップに繋げる手法を採ることが効果的である。

問題点・課題	克服に向けて得られた示唆
■ 内部不正防止対策とサイバーセキュリティ対策を同一の取組の一環として実施する傾向があり、内部不正防止に固有の対策の実施が弱体化する懸念がある。 ■ 内部不正リスクを他のリスクと切り分けて評価できていない企業が多い。それぞれの企業の事情に応じたリスクアセスメントに基づく内部不正防止のアプローチは、まだハードルが高い。 ■ 営業秘密を重視しない企業がまだ多く、内部不正防止に固有の対策に関する意識の低さが懸念される。	■ 内部不正防止対策とサイバーセキュリティ対策等は**原則として**使い分ける方がよい。経営リソースの制約がある中で効果を最大化するためには、各々別々にリスクアセスメントを行い、その結果に基づいて適材適所で講ずべき対策を選択することが必要である。 ■ しかし、経営資源が限られた中小企業、特にこれから新たに内部不正防止に取り組もうとする中小企業では、対策の細分化と実施コストの上昇を伴うこの原則に従うことが難しいことが想定される。 ⇒リソース制約の厳しい中小企業においては、むしろ内部不正防止とサイバーセキュリティで共通性の高い対策を積極的に一本化しつつ、適切なバランスを考慮して個別の対策を追加的に組み合わせるのが合理的である。 ■ 営業秘密管理の導入は、秘密情報管理と内部不正対策の両方を同時に進展させるので、積極的に取り組むのが良い。

7-3. 中小企業にとっての問題点・課題と今後のあり方

中小企業と大企業の結論の比較（総括）

本調査の結果として、秘密情報漏えい／内部不正防止への望ましい取組は、大企業と中小企業でかなり異なることが示唆されることとなった。
これらの示唆を踏まえ、今後は大企業と中小企業のそれぞれで、あるべき姿に向けた取組を推進されることが望まれる。

調査軸	中小企業について得られた結論（総括）	大企業について得られた結論（総括）
経営課題の改善	■ 内部不正防止とサイバーセキュリティを切り分けるべきか否かといった経営課題としての適正な認識は経営規模によって変化する。状況に照らして経営者の判断が肝要。 ■ 適切な判断の基礎を得るためにも、経営者が自ら率先して学ぶことが望ましい。ISMS、技術情報管理等の認証取得、業界全体での取組への対応等は取組の向上と学びのきっかけとして有意義。 ■ 経営者の判断と行動が自社の変革において極めて力強い役割を担うことを、経営者は強く自覚することが望まれる。	■ 内部不正防止とサイバーセキュリティは別の経営課題として捉えることが望まれる。 ■ 大企業であっても経営層のリスク認識を高めることの重要性は変わらない。リスクの洗い出しが可能なリスクマップ等の可視化ツールを活用することで経営層におけるリスク認識の適正化を図ることもできる。
重要な秘密の特定と取扱いの改善	■ 秘密情報の特定・格付け・表示の徹底は不十分である。 ■ 経営者が自ら重要な秘密を特定し、格付けすることが可能である。但し、経営層が過負荷にならないように留意することが望まれる。	■ 秘密情報の特定・格付け・表示の徹底は不十分である。 ■ 秘密の特定・格付けルール策定や表示の徹底、情報資産管理の実施と定期的な見直しの仕組みを作り、策定したルールや管理策が有効に機能するよう努めることが望まれる。
組織体制・連携に関する課題の改善	■ 経営層の主導の下、組織横断の対策が適切に実施されるよう、必要に応じて部署・担当者間の連携を具体化することが望まれる。	■ 内部不正防止やサイバーセキュリティなどの分野別に、それぞれが主体的に動くべき関連部署・部門間の適切な連携体制を構築することが望まれる。
社員教育とリテラシー構築に関する課題の改善	■ 全社集会等を活用して、経営者自身の言葉を用いて経営方針や知見を伝えることが有効。	■ 従業員にとって分かりやすい内容と方法で教育することが望まれる。
対策に関する課題の改善	■ 認証制度等の既存の枠組みも参考にしつつ、内部不正防止に特有の対策を選定し、サイバーセキュリティ対策へ追加する形で実施することが望まれる。	■ 内部不正リスクを切り出して評価し、適切な対策を選定・実施することが望まれる。