NTT DATA
Trusted Global Innovator

企業における内部不正防止体制に関する実態調査
概要説明資料

2023年1月31日

作成：株式会社エヌ・ティ・ティ・データ経営研究所

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。こうした近年の環境変化を踏まえた内部不正防止ガイドラインの活用等、企業において実効性を持った施策が検討される重要性が高まっている。

情報漏えいに関する内部不正に影響を及ぼす近年の環境変化としては、テレワークやクラウド利用が増えたニューノーマル環境や雇用流動化等の社会情勢の変化、AIの応用等の新たな技術環境への移行等が急激に顕在化してきた。
しかし、これらの急激な変化・移行に対し、現状では企業における内部不正を防止する対策や体制の変革は必ずしも進んではいないことが、新たな課題として懸念される。

さらには、個人情報や営業秘密といった従来から認識されてきた情報に加えて、企業が保有する限定提供データ等の重要データや技術関連の重要情報等も、内部不正による情報漏えいから保護することが新たに必要になってきている。

他方で、企業における、上記のような課題認識、対策状況、マネジメント体制等の変革の実態は必ずしも明らかにはなっていない。

【調査の目的】

本調査では、企業の内部不正防止対策・体制に関する現在の問題点を把握して課題の解決に資するべく、企業における内部不正防止対策・体制に関する実態を調査し、各企業における有効な施策立案を支援することを目的とする。

目次

1．調査方針
1-1. 調査のフレームワーク設定

本調査では、企業における電子化された重要情報の漏えい防止並びにこれに関わる内部不正防止の実態調査を行うにあたり、内部不正防止ガイドライン第4版における対策のポイント、第5版改訂において重点を置いた働き方・環境・法制度等の変化、及びこれに対応できる新たな対策等を考慮し、次の５つの調査軸を設定した。

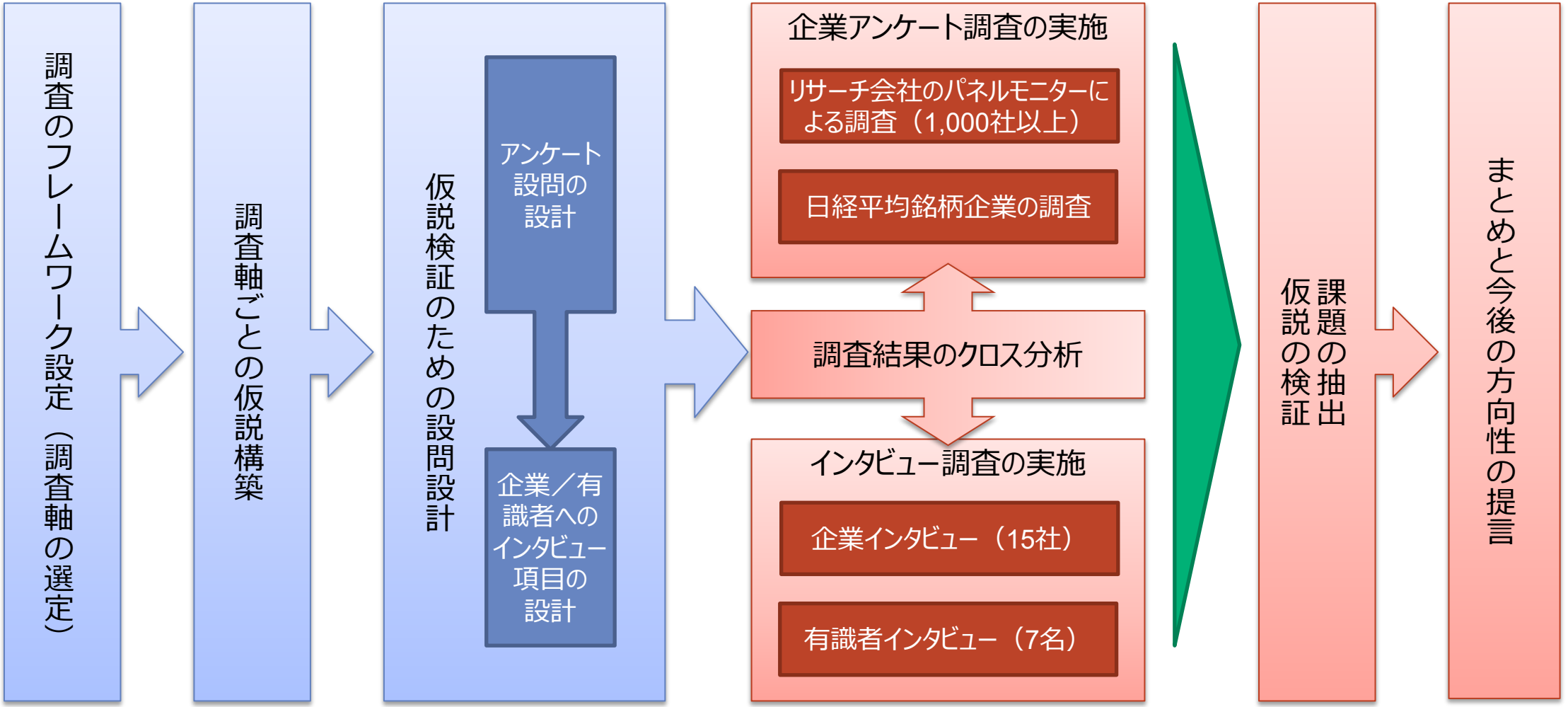
① 企業・組織全体として知っておくべき基礎知識の実態
② 内部不正防止に取り組む組織的体制（組織全体の体制）の実態
③ 組織全体への周知・教育の実態
④ 内部不正防止の課題と対策の実態
⑤ 内部不正防止ガイドライン利用の実態

さらに、本調査において一貫した調査フレームワークとして、実態調査で検証を試みる仮説の構築、企業アンケートの設問や企業／有識者へのインタビュー項目の設計、調査結果の集計・分析、仮説の検証と課題の抽出という一連の作業の全てを上記5軸による共通の分類に基づいて実施することとした。こうすることで、調査結果のクロス分析が容易かつ的確になり、分析結果の質的向上が実現できる。

1-2. 調査プロセス

本調査では、調査軸ごとに設定した仮説を、アンケート調査、インタビュー調査及びそれぞれの結果のクロス分析によって検証した。また、仮説の検証を通じて抽出された課題を整理し、その克服に向けた今後の方向性を取りまとめた。

【本調査の実施プロセス】



1-2. 調査プロセス

本調査では、仮説の構築から検証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。

【本調査のフレームワーク】

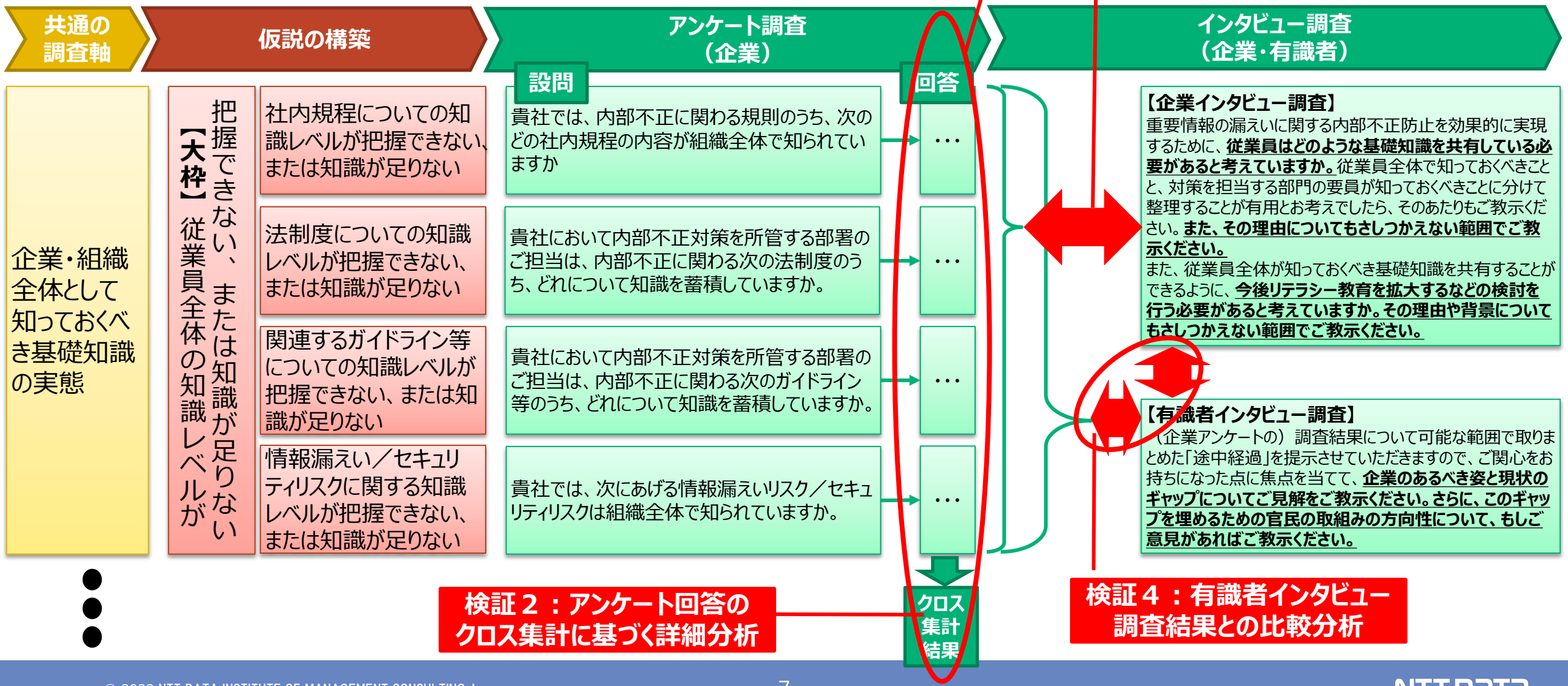
調査軸ごとの一貫した調査・分析・仮説検証

共通の調査軸	仮説の構築	アンケート調査（企業）	インタビュー調査（企業・有識者）	仮説検証・課題抽出	総括・提言
企業・組織全体として知っておくべき基礎知識の実態	基礎知識の仮説	基礎知識に関する設問の回答	基礎知識に関するインタビュー結果	調査結果の比較、分析による基礎調査の仮説検証・課題抽出	まとめと今後の方向性の提言
内部不正防止に取り組む組織的体制の実態	組織的体制の仮説	組織的体制に関する設問の回答	組織的体制に関するインタビュー結果	調査結果の比較、分析による組織的体制の仮説検証・課題抽出	
組織全体への周知・教育の実態	組織全体への周知・教育の仮説	組織全体への周知・教育に関する設問の回答	組織全体への周知・教育に関するインタビュー結果	調査結果の比較、分析による組織全体への周知・教育の仮説検証・課題抽出	
内部不正防止の課題と対策の実態	課題と対策の仮説	課題と対策に関する設問の回答	課題と対策に関するインタビュー結果	調査結果の比較、分析による課題と対策の仮説検証・課題抽出	
内部不正防止ガイドライン利用の実態	内部不正防止ガイドライン利用及び啓発の仮説	内部不正防止ガイドライン利用及び啓発に関する設問の回答	内部不正防止ガイドライン利用及び啓発に関するインタビュー結果	調査結果の比較、分析による内部不正防止ガイドライン利用及び啓発の仮説検証・課題抽出	

1-3. 仮説検証の方法

本調査では、アンケートとインタビューを組み合わせて、仮説を検証した。

【仮説検証の方法】



2．調査軸ごとの仮説構築（1/2）

アンケート／インタビューの調査結果に基づいて検証を試みる仮説を、各調査軸に対して設定した。仮説は、重要情報の漏えいに関する内部不正防止の組織的体制・対策及びリテラシー教育の問題点を改善する際の重要な着眼点を与えるものとして構築した。

調査軸	仮説の大枠	検証を試みる仮説
企業・組織全体として知っておくべき基礎知識の実態	従業員全体の知識レベルが把握できない、または知識が足りない	社内規程についての知識レベルが把握できない、または知識が足りない
		法制度についての知識レベルが把握できない、または知識が足りない
		関連するガイドライン等についての知識レベルが把握できない、または知識が足りない
		情報漏えい／セキュリティリスクに関する知識レベルが把握できない、または知識が足りない
内部不正防止に取り組む組織的体制の実態	経営層のコミットが弱い、または重要情報管理の成熟度が低い企業は、組織全体としての体制ができていない	経営層の情報発信が明確ではない、又は不十分な企業が多い
		組織全体としての責任・権限が明確に定められていない企業が多い
		社内ポリシー／規定の整備が不十分な企業が多い
		経営層がリソースを適切に配分できていない企業が多い
		内部不正対策に関するマネジメントシステムが十分に機能していない企業が多い
		テレワークを行う従業員を支援する体制が整備できていない企業が多い
組織全体への周知・教育の実態	セキュリティ対策の教育が優先されているものの、内部不正対策の教育は必ずしも充実していない	一般の職員に対する、内部不正対策に関する周知・教育は不足している
	内部不正対策を教育していても、それが組織全体での実践に繋がっていない	内部不正対策を組織全体で実践できる環境が整っていない

2．調査軸ごとの仮説構築（2/2）

（続き）

調査軸	仮説の大枠	検証を試みる仮説
内部不正防止の課題と対策の実態	今まで低い優先順位で扱われてきたことから、今後内部不正対策への関心が高まると想定されるにも関わらず、その重要性に見合う十分な対策やリソースが確保できていない	内部不正リスクは、経営リスクや事業リスクとしての優先度が高くなく、対策実施が後回しとなっている
		セキュリティ対策等と比較すると、内部不正に対する具体的な対策や事後対策の選択が難しい
		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、内部不正対策の拡張が進んでいない
		セキュリティ対策等と比較すると、ニューノーマル等の環境変化への対応が遅れており、リスクが高まる内部不正に関する規則が未整備、または対策を実施できていない
		急増する中途退職者／中途採用者の内部不正に対する対策整備が遅れている、または対策が実施できていない
		不満を蓄積せず、内部不正を誘発しない職場環境の整備が十分ではない
		内部不正による重要情報の漏えい発覚時に、侵害先にどこまで対応するかの方針がない
内部不正防止ガイドライン利用の実態	内部不正防止ガイドラインは効果的に活用されていない	内部不正防止ガイドラインはあまり知られていない
		内部不正防止ガイドラインの存在は知っていても、あまり読まれていない

3 .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または責任者
ii. リスクマネジメントの企画・運用に関わる部署の担当者または責任者
iii. 経営企画部門における企業・組織のIT／セキュリティ戦略の担当者または責任者
iv. 上記以外の、リスクマネジメントに関する業務の担当者
v. 経営層

- 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。

  ※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

- 参考として比較するため、大企業を中心とした企業にアンケートへの回答を依頼し、Web回答システムで回答を取得。具体的には、日経平均銘柄企業（225社）に書面（郵送）で回答を依頼。

４．インタビュー調査の対象
4-1. 国内の企業

次の４つの要件のうち、1つ以上に合致している国内の企業15社に対して、企業インタビュー調査を実施した。

i. セキュリティ対策に積極的と目される企業
ii. 内部不正対策に積極的と目される企業
iii. 内部統制（リスク管理、コンプライアンス、内部監査等）が充実していると目される企業
iv. データの利活用と保護（例：限定提供データ等）に積極的と目される企業

- インタビュー先企業は、大企業、中堅企業、ベンチャー企業を網羅。
- 業種は、情報通信／ITサービス、製造業、建設業、警備業、金融・保険などを幅広くカバー。
- インタビューへの回答者は、経営層、監査担当役員、情報システム／セキュリティ担当者、法務・知財担当者、リスク管理担当者、内部監査担当者等、多岐に亘っている。

4-2. 有識者

以下の３要件のうち１つ以上に合致する、内部不正防止・秘密情報管理に関する有識者／法律の専門家７名に対してインタビュー調査を実施した。

i. 内部不正防止に関わる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

【インタビューを実施した有識者（50音順、敬称略）】

#	氏名	専門性	所属、資格等
1	大野 博堂	ii に該当	株式会社NTTデータ経営研究所　パートナー 金融政策コンサルティングユニット長
2	金子 啓子	i , ii に該当	内部不正防止ガイドライン第5版改訂時の検討会委員
3	蔦 大輔	i に該当	森・濱田松本法律事務所　弁護士
4	殿村 桂司	i , iii に該当	長島・大野・常松法律事務所　パートナー　弁護士
5	西川 喜裕	i , iii に該当	三浦法律事務所　パートナー　弁護士 内部不正防止ガイドライン第5版改訂時の検討会委員
6	和貝 享介	ii に該当	公認会計士
7	渡邉 遼太郎	i , iii に該当	東京八丁堀法律事務所　弁護士

5．調査結果

各種調査の実施件数は以下の通り。

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を示す。

【調査の実施および回収件数】

i. 企業アンケート調査
- ■ ＜主たる回答＞パネルモニター：　1,179名から回収（所属企業1,000社以上）
- ■ ＜参考回答＞日経平均銘柄企業：　25社から回収

ii. 企業インタビュー調査：　15社
- ■ 大手企業：　10社
  - ➢ 製造業3社、通信・ITサービス等3社、ゼネコン1社、警備1社、金融・保険1社
- ■ 中堅・ベンチャー企業：　5社
  - ➢ ITサービス・コンサルティング5社

iii. 有識者インタビュー調査：　7名
- ■ 弁護士：　4名
- ■ 民間企業経験者：　3名

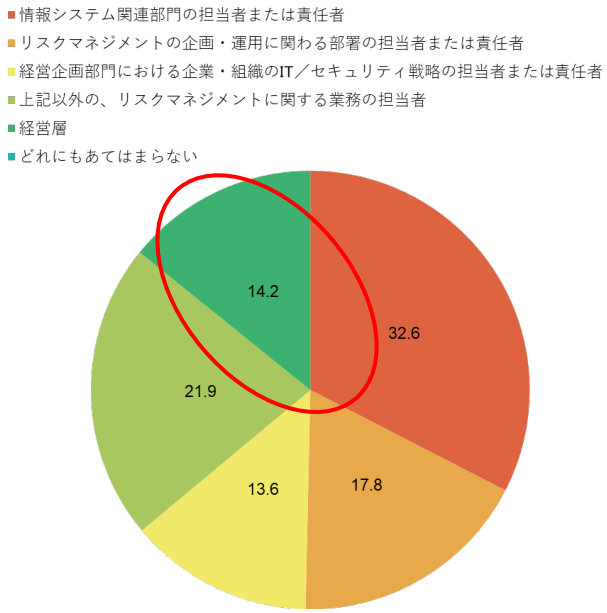
5-1. 企業アンケート調査の単純集計結果（1/26）　～回答者の属性～

パネルモニターの回答者が担当する業務については、情報システム／セキュリティ関係業務が46.2%で最も多く、次いでリスクマネジメント関係業務が39.7%である。今回、経営層から14.2%（167名）の回答を得た。

SQ1H. 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。

＜パネルモニターのみの集計＞

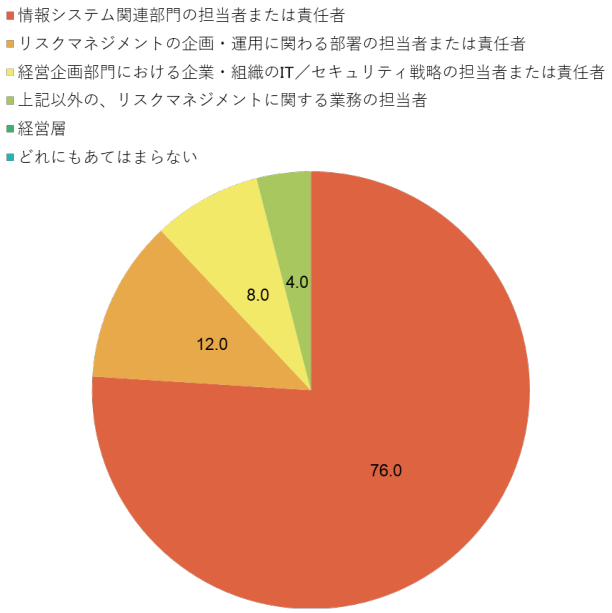
主たる回答



	n=	情報システム関連部門の担当者または責任者	リスクマネジメントの企画・運用に関わる部署の担当者または責任者	経営企画部門における企業・組織のIT／セキュリティ戦略の担当者または責任者	上記以外の、リスクマネジメントに関する業務の担当者	経営層	どれにもあてはまらない
TOTAL	1179	32.6	17.8	13.6	21.9	14.2	0.0

（ご参考：日経平均銘柄企業25社の集計）

参考比較



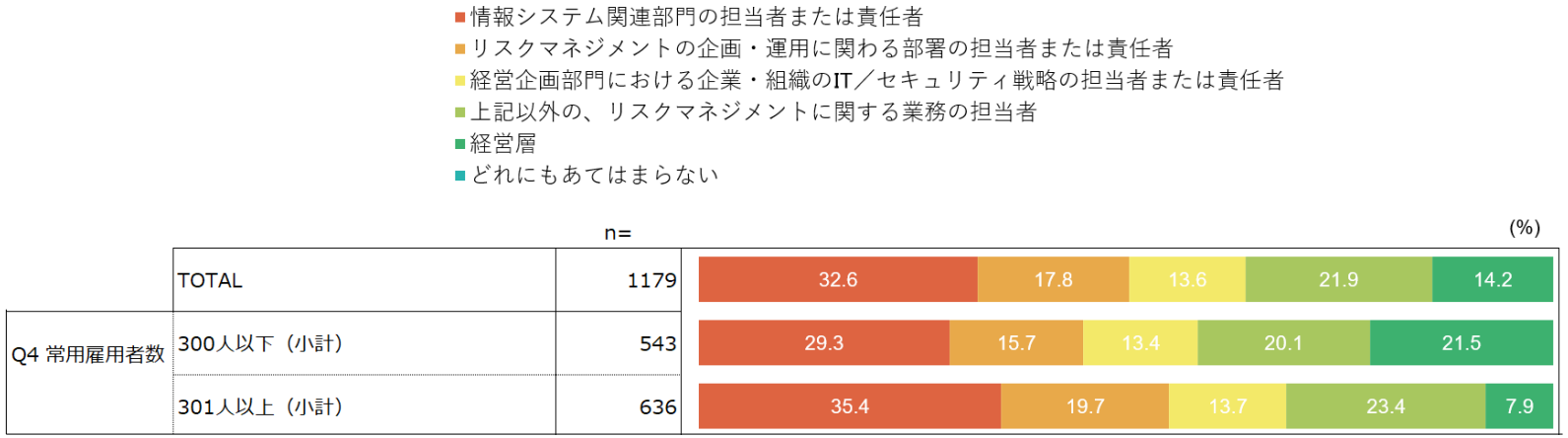
	n=	情報システム関連部門の担当者または責任者	リスクマネジメントの企画・運用に関わる部署の担当者または責任者	経営企画部門における企業・組織のIT／セキュリティ戦略の担当者または責任者	上記以外の、リスクマネジメントに関する業務の担当者	経営層	どれにもあてはまらない
TOTAL	25	76.0	12.0	8.0	4.0	0.0	0.0

5-1. 企業アンケート調査の単純集計結果（2/26）　～回答者の属性～

経営層の回答のうち、約70%は中小企業の経営層。他方で約15%が、従業員数が1,000名を超える大企業の経営層の回答。

1段目　横%		0 TOTAL	1 300人以下（小計）	2 301人以上（小計）
0	TOTAL	1179	46.1	53.9
1	情報システム関連部門の担当者または責任者	384	41.4	58.6
2	リスクマネジメントの企画・運用に関わる部署の担当者または責任者	210	40.5	59.5
3	経営企画部門における企業・組織のIT／セキュリティ戦略の担当者または	160	45.6	54.4
4	上記以外の、リスクマネジメントに関する業務の担当者	258	42.2	57.8
5	経営層	167	70.1	29.9

※1,000人以下と
それ以上で概ね半分ずつ



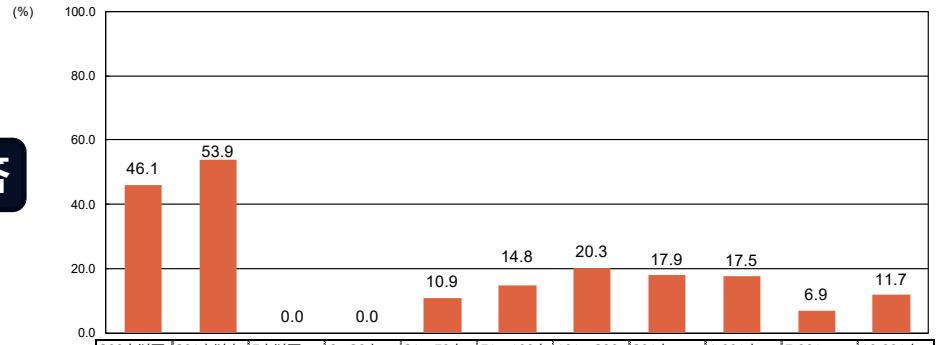
5-1. 企業アンケート調査の単純集計結果（3/26）　～回答者の属性～

パネルモニターの回答者が所属する企業は、大企業と中小企業がほぼ半々。他方で、回答した日経平均銘柄企業は、ほとんどすべてが大企業。

Q4. 貴社の常用雇用者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。

＜パネルモニターが所属する企業のみの集計＞

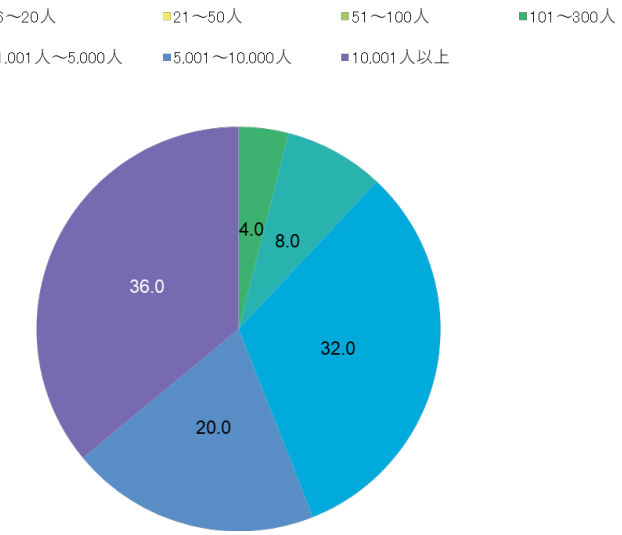
主たる回答



	n=	300人以下（小計）	301人以上（小計）	5人以下	6～20人	21～50人	51～100人	101～300人	301人～1,000人	1,001人～5,000人	5,001～10,000人	10,001人以上
TOTAL	1179	46.1	53.9	0.0	0.0	10.9	14.8	20.3	17.9	17.5	6.9	11.7

（ご参考：日経平均銘柄企業25社の集計）

参考比較



	n=	5人以下	6～20人	21～50人	51～100人	101～300人	301人～1,000人	1,001人～5,000人	5,001～10,000人	10,001人以上
TOTAL	25	0.0	0.0	0.0	0.0	4.0	8.0	32.0	20.0	36.0

5-1. 企業アンケート調査の単純集計結果（4/26）　～回答者の業種～

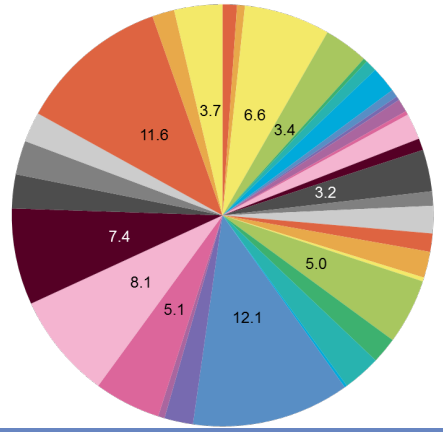
回答者が所属する企業の業種は幅広く分布しているが、製造業、情報サービス業、卸売業・小売業、金融業・保険業、その他のサービス業等が多い。

Q3. 貴社の企業・組織の業種についてあてはまるものを１つお選びください。

＜パネルモニターが所属する企業のみの集計＞

- 1. 農業、林業、漁業
- 2. 鉱業、採石業、砂利採取業
- 3. 建設業
- 4. 食料品製造業
- 5. 飲料・たばこ・飼料製造業
- 6. 繊維工業
- 7. 化学工業
- 8. プラスチック製品製造業
- 9. ゴム製品製造業
- 10. 鉄鋼業
- 11. はん用機械器具製造業
- 12. 生産用機械器具製造業
- 13. 業務用機械器具製造業
- 14. 電子部品・デバイス・電子回路製造業
- 15. 電子応用装置・電気計測器製造業
- 16. 15以外の電気機械器具製造業
- 17. 情報通信機械器具製造業
- 18. 自動車・同附属部品製造業
- 19. 18以外の輸送用機械器具製造業
- 20. 4～19以外の製造業
- 21. 電気・ガス・熱供給・水道業
- 22. 通信業
- 23. 放送業
- 24. 情報サービス業
- 25. インターネット附随サービス業
- 26. 映像・音声・文字情報制作業
- 27. 運輸業、郵便業
- 28. 卸売業、小売業
- 29. 金融業、保険業
- 30. 不動産業、物品賃貸業
- 31. 学術研究、専門・技術サービス業
- 32. 宿泊業、飲食サービス業
- 33. 31、32以外のサービス業
- 34. 公務（他に分類されるものを除く）
- 35. 分類不能の産業

主たる回答



	n=	1. 農業、林業、漁業	2. 鉱業、採石業、砂利採取業	3. 建設業	4. 食料品製造業	5. 飲料・たばこ・飼料製造業	6. 繊維工業	7. 化学工業	8. プラスチック製品製造業	9. ゴム製品製造業	10. 鉄鋼業	11. はん用機械器具製造業	12. 生産用機械器具製造業	13. 業務用機械器具製造業
TOTAL	1179	1.1	0.6	6.6	3.4	0.3	0.9	2.0	0.6	0.3	1.0	0.3	2.0	0.9

14. 電子部品・デバイス・電子回路製造業	15. 電子応用装置・電気計測器製造業	16. 15以外の電気機械器具製造業	17. 情報通信機械器具製造業	18. 自動車・同附属部品製造業	19. 18以外の輸送用機械器具製造業	20. 4～19以外の製造業	21. 電気・ガス・熱供給・水道業	22. 通信業	23. 放送業	24. 情報サービス業	25. インターネット附随サービス業
3.2	1.1	2.1	1.4	2.0	0.3	5.0	2.0	2.9	0.2	12.1	2.2

26. 映像・音声・文字情報制作業	27. 運輸業、郵便業	28. 卸売業、小売業	29. 金融業、保険業	30. 不動産業、物品賃貸業	31. 学術研究、専門・技術サービス業	32. 宿泊業、飲食サービス業	33. 31、32以外のサービス業	34. 公務（他に分類されるものを除く）	35. 分類不能の産業
0.5	5.1	8.1	7.4	2.6	2.6	2.3	11.6	1.7	3.7

5-1. 企業アンケート調査の単純集計結果（5/26）　～組織全体で知っておくべき基礎知識～

情報漏えい／セキュリティリスクは組織全体で認知されていることが望ましいが、ほとんどのリスクで「組織全体で知られている」という回答の割合が30%前後に留まっており、組織全体での知識レベルは十分とは言えない状況。

Q15. 貴社では、次にあげる情報漏えいリスク／セキュリティリスクは組織全体で知られていますか。

＜パネルモニターが所属する企業のみの集計＞

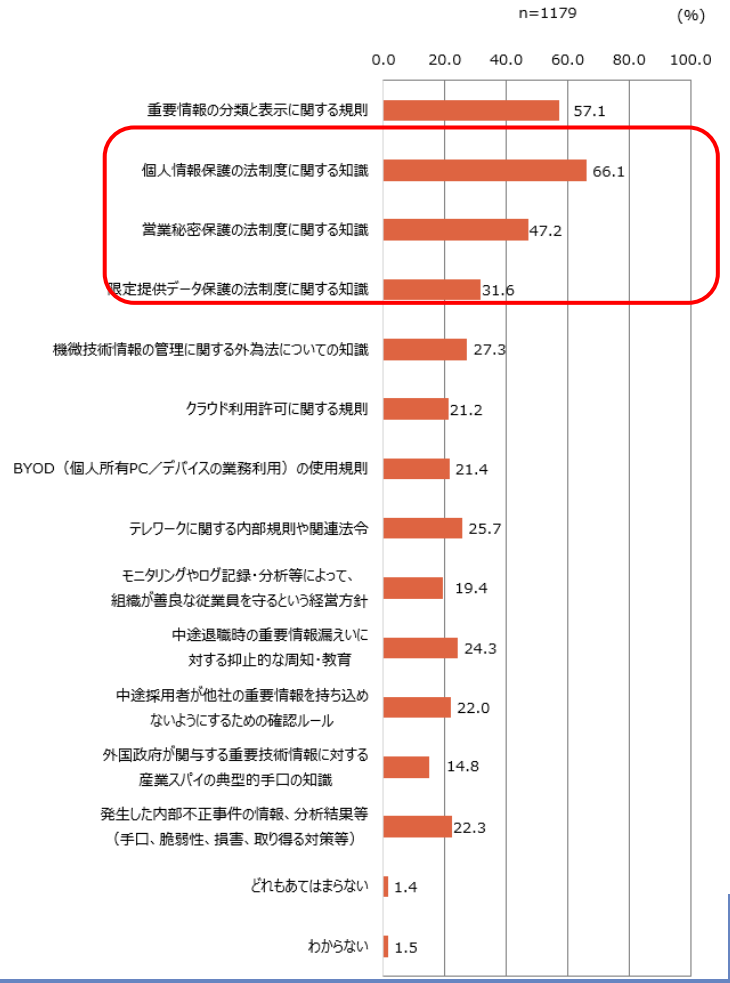
情報漏えい／セキュリティリスク	n=	組織全体で知られている	対策の担当者が知っている	知られていない	分からない
機器・システムの脆弱性	1179	37.9%	43.2%	10.1%	8.8%
サイバー攻撃、だましの手口	1179	40.7%	38.8%	11.9%	8.7%
サプライチェーンにおけるセキュリティ上の脆弱点の存在	1179	28.9%	42.4%	16.3%	12.4%
サプライチェーンにおける不必要な重要情報の授受	1179	27.7%	41.8%	17.2%	13.3%
クラウドセキュリティのあいまいな責任分担	1179	25.9%	41.8%	17.9%	14.4%
テレワークの不十分なセキュリティガバナンス	1179	32.1%	37.7%	16.6%	13.6%
プライバシーを侵害する従業員監視	1179	32.4%	36.2%	17.4%	14.0%
外国政府が関与した重要技術情報への合法的／非合法的アプローチ	1179	24.5%	33.8%	22.0%	19.8%
退職者を通じた自社の重要情報の漏えい／中途採用者を通じた他社の重要情報の混入	1179	32.8%	36.6%	16.2%	14.4%

5-1. 企業アンケート調査の単純集計結果（6/26）　～組織全体で知っておくべき基礎知識～

営業秘密／限定提供データの管理規則は、個人情報の管理規則ほど知られていない。この傾向は、法制度に関する知識のリテラシー教育の実態と一致しており、営業秘密／限定提供データについては教育も不十分である。

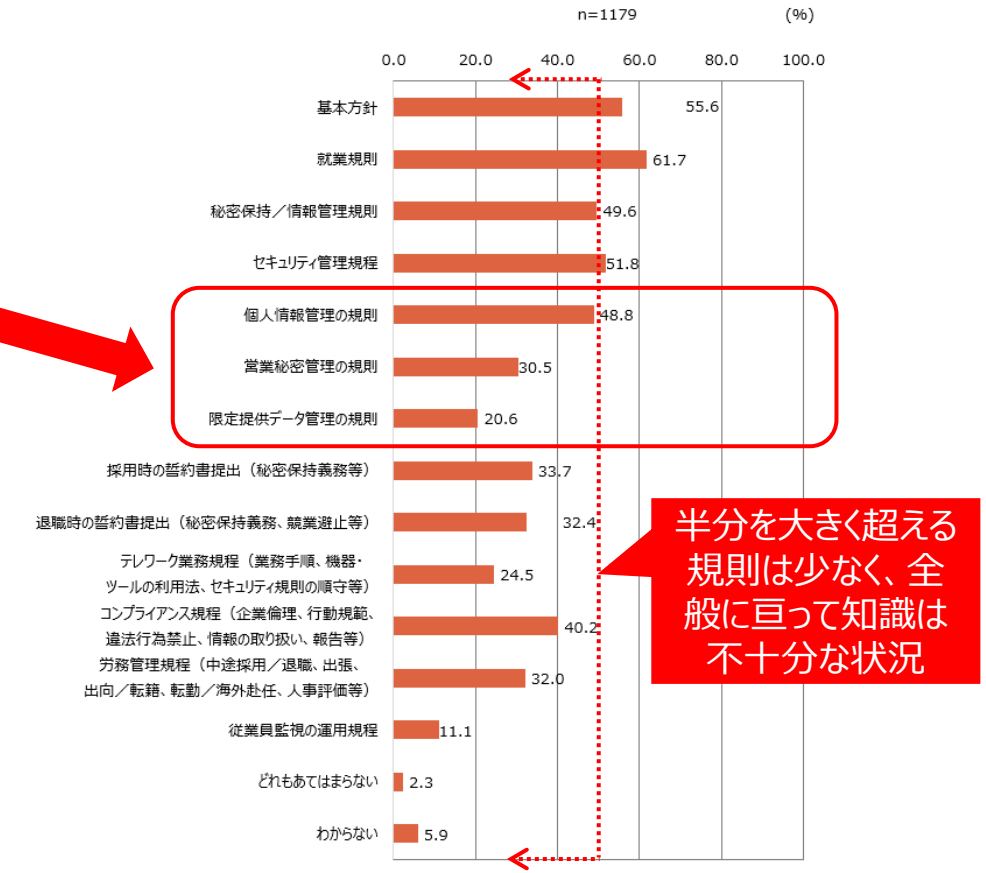
Q27. 貴社では内部不正防止についての従業員へのリテラシー教育において、具体的にどのような内容を周知・教育していますか。

＜パネルモニターが所属する企業のみの集計＞



Q14. 貴社では、内部不正に関わる規則のうち、次のどの社内規程の内容が組織全体で知られていますか。

＜パネルモニターが所属する企業のみの集計＞

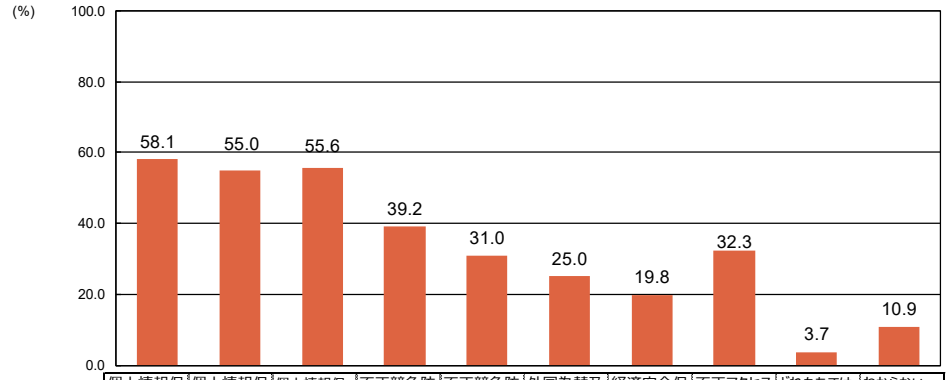


5-1. 企業アンケート調査の単純集計結果（7/26）　～内部不正対策を所管する部署に蓄積されている知識～

法制度に関する知識については、一番蓄積が進んでいるはずの個人情報保護法でさえ、40%以上の回答者が担当部署に蓄積されていないと回答している。不正競争防止法については、企業にとっての営業秘密の重要性と比べると知識の蓄積がさらに不十分な実態である。内部不正防止に関連するガイドライン等の知識についても、担当部署における必要知識の蓄積状況は40%未満に留まっており、まだ改善の余地がある。担当部署において知識の蓄積が不十分であるならば、組織全体としてもまだ必要な知識が足りていないと推定できる。

Q16. 貴社において内部不正対策を所管する部署のご担当は、内部不正に関わる次の法制度のうち、どれについて知識を蓄積していますか。

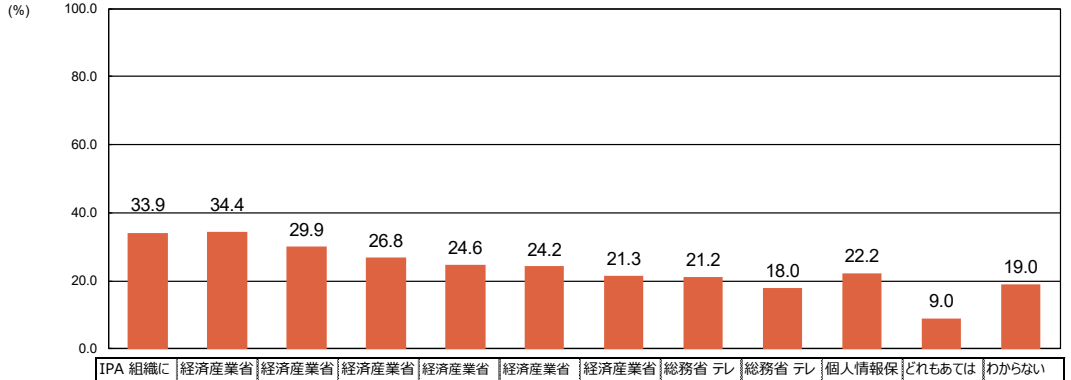
＜パネルモニターが所属する企業のみの集計＞



	n=	個人情報保護法（利用目的の順守）	個人情報保護法（第三者提供の要件）	個人情報保護法（内部不正による個人データ漏えい時の報告義務）	不正競争防止法（営業秘密の要件）	不正競争防止法（限定提供データの要件）	外国為替及び外国貿易法（外為法）	経済安全保障推進法	不正アクセス禁止法	どれもあてはまらない	わからない
TOTAL	1179	58.1	55.0	55.6	39.2	31.0	25.0	19.8	32.3	3.7	10.9

Q17. 貴社において内部不正対策を所管する部署のご担当は、内部不正に関わる次のガイドライン等のうち、どれについて知識を蓄積していますか。

＜パネルモニターが所属する企業のみの集計＞



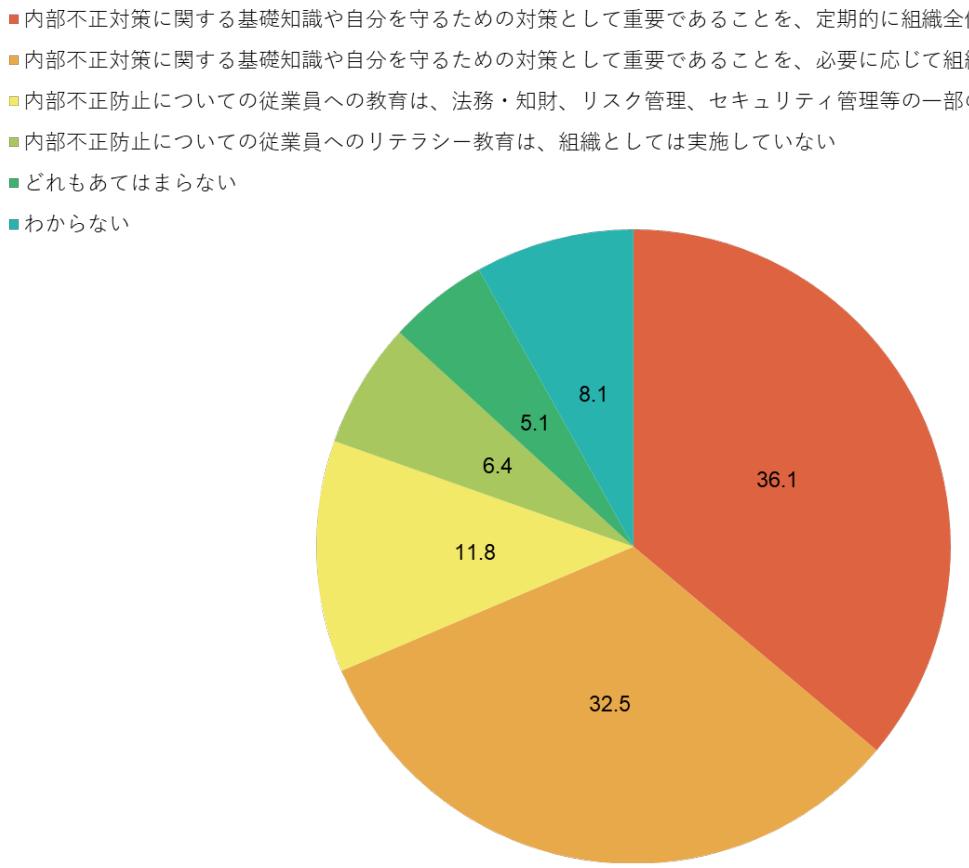
	n=	IPA 組織における内部不正防止ガイドライン	経済産業省秘密情報の保護ハンドブック	経済産業省営業秘密管理指針	経済産業省限定提供データに関する指針	経済産業省データ利活用のポイント集ーデータ利活用の共創が生み出す新しい価値ー	経済産業省データ利活用のてびき ー正しいデータ利活用で新たな価値を生み出そう！ー	経済産業省データ利活用の事例集ーデータ利活用のポイント集 別冊ー	総務省 テレワークセキュリティガイドライン	総務省 テレワーク時における秘密情報管理のポイント（Q&A解説）	個人情報保護委員会 テレワークに伴う個人情報漏えい事案に関する注意事項	どれもあてはまらない	わからない
TOTAL	1179	33.9	34.4	29.9	26.8	24.6	24.2	21.3	21.2	18.0	22.2	9.0	19.0

5-1. 企業アンケート調査の単純集計結果（8/26）　～組織全体への周知・教育～

内部不正防止に関するリテラシー教育については、組織全体で定期的に実施していると回答した割合は40%に満たず、まだ十分とは言えない。また、組織全体で必要に応じて実施していると回答した割合が30%を超えており、ここまで含めると70%近くが内部不正についてのリテラシー教育を実施していると回答している。

Q26. 貴社では内部不正防止についての従業員へのリテラシー教育を実施していますか。

＜パネルモニターが所属する企業のみの集計＞



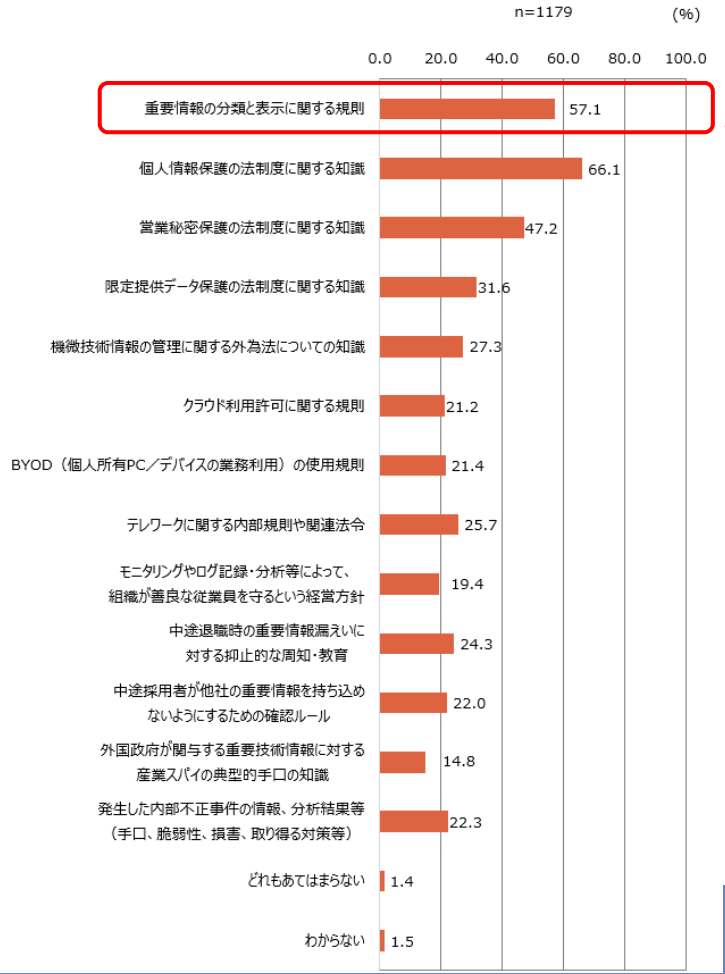
	n=	内部不正対策に関する基礎知識や自分を守るための対策として重要であることを、定期的に組織全体に周知・教育している	内部不正対策に関する基礎知識や自分を守るための対策として重要であることを、必要に応じて組織全体に周知・教育している	内部不正防止についての従業員への教育は、法務・知財、リスク管理、セキュリティ管理等の一部の部門でのみ実施している	内部不正防止についての従業員へのリテラシー教育は、組織としては実施していない	どれもあてはまらない	わからない
TOTAL	1179	36.1	32.5	11.8	6.4	5.1	8.1

5-1. 企業アンケート調査の単純集計結果（9/26）　～組織全体への周知・教育～

従業員に対して重要情報の分類と表示に関する規則の周知・教育を実施している企業は半数を超えていた。また、重要情報管理ルールを定期的に教育する企業も半数を超えた。これらはまずまずの状況ではあるものの、さらなる底上げが期待される。他方で、重要プロジェクトの開始／終了時のルールの教育し直し（より詳しい教育等）は十分ではなかった。

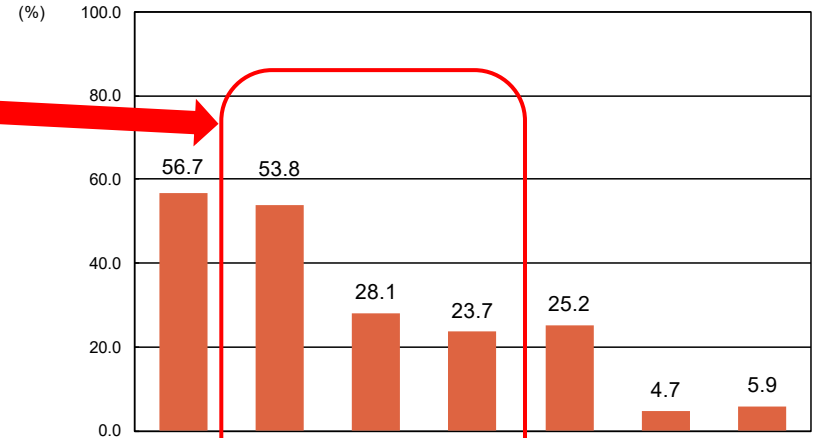
Q27. 貴社では内部不正防止についての従業員へのリテラシー教育において、具体的にどのような内容を周知・教育していますか。

＜パネルモニターが所属する企業のみの集計＞



Q9. 貴社では重要情報の管理ルールを従業員に周知・徹底していますか。

＜パネルモニターが所属する企業のみの集計＞



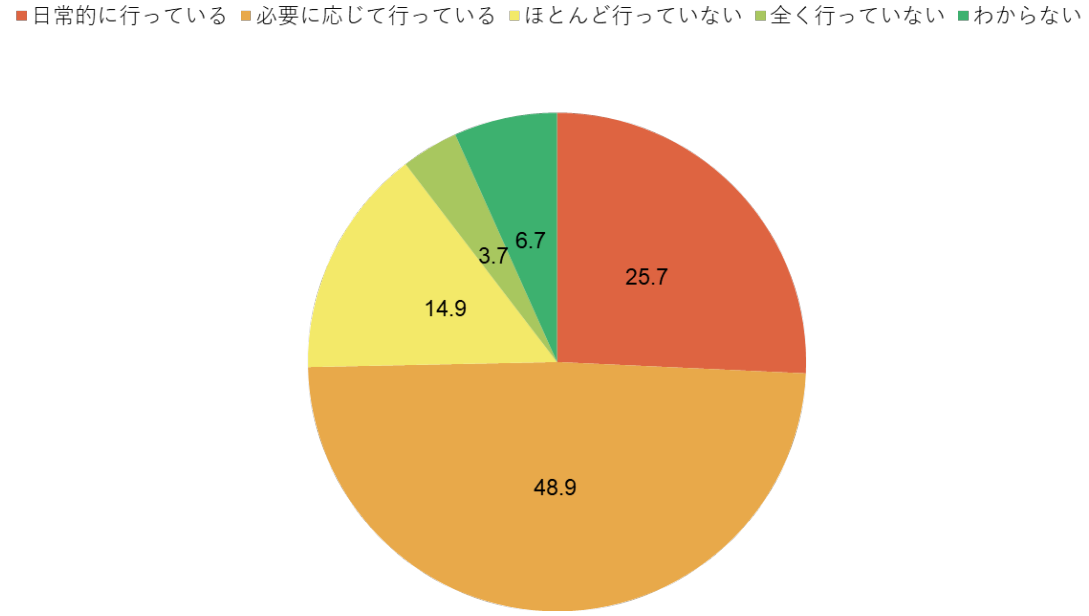
n=	1179	雇用開始時に、就業規則や誓約書等を通じて教育している	定期的な教育（例：毎年1度のeラーニング受講等）によって全社に周知・徹底している	異動時・昇進時等にルールを教育し直している	プロジェクトの開始、参加、終了時等にルールを教育し直している	雇用終了時の重要情報等の返却・削除ルールについて、教育で全社に周知・徹底している	教育による周知は実施していない	わからない
TOTAL	1179	56.7	53.8	28.1	23.7	25.2	4.7	5.9

5-1. 企業アンケート調査の単純集計結果（10/26）　～内部不正対策に取り組む組織的体制～

経営層が行う情報発信において従業員が「内部不正防止の取組方針等の周知・指示」を特定し、認識している割合は約75%に達しており、「経営層の情報発信が明確ではない、または不十分な企業が多い」という仮説は必ずしも実態とは合っていない。一方で、経営層が行う「内部不正防止の取組方針等の周知・指示」を特定・認識できていない従業員にその理由を聞いてみると、内部不正防止についての情報発信であることが明確に伝わらないという理由を選択した回答者が多く、経営層にとって工夫の余地があることを示唆している。

Q18.経営層は、組織全体での内部不正防止の取組み方針等について、全従業員に周知、指示していますか。

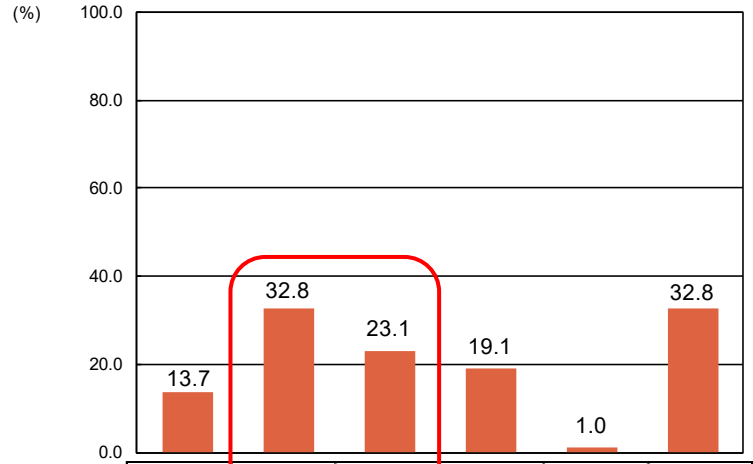
＜パネルモニターが所属する企業のみの集計＞



	n=	日常的に行っている	必要に応じて行っている	ほとんど行っていない	全く行っていない	わからない
TOTAL	1179	25.7	48.9	14.9	3.7	6.7

Q19.経営層が内部不正防止の取組み方針等について、全従業員にほとんど周知・指示していない、またはわからないと感じている理由について、あなたがあてはまると思うものをすべてお選びください。

＜パネルモニターが所属する企業のみの集計＞



	n=	経営層（全社責任者を含む）が必要性を感じていないから	経営層（全社責任者を含む）が内部不正対策だけに焦点を絞って周知・指示することはほとんどないから	内部不正防止の方針は、情報漏えい対策やコンプライアンス順守の方針とまとめて周知・指示されることが多く、区別することが難しいから	経営層（全社責任者を含む）は全従業員への周知・指示を、全社の責任部門の対応に任せているから	その他の理由　具体的に：	わからない
TOTAL	299	13.7	32.8	23.1	19.1	1.0	32.8

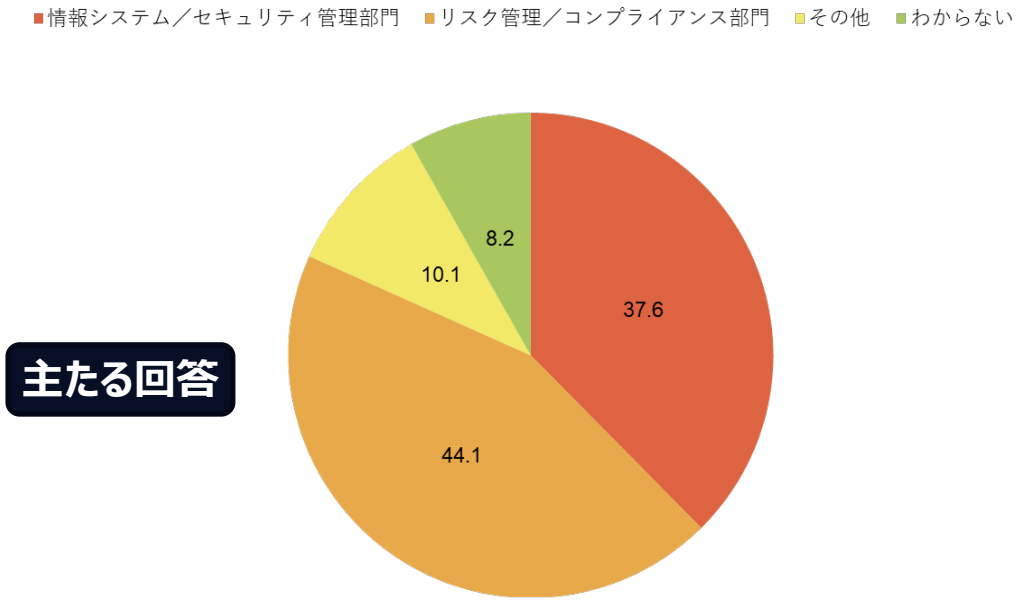
5-1. 企業アンケート調査の単純集計結果（11/26）　～内部不正対策に取り組む組織的体制～

内部不正対策を主管して組織全体に対する責任を負う部門は、概ね「情報システム／セキュリティ管理部門」と「リスク管理／コンプライアンス部門」に二分されており、責任の所在があいまいと懸念されるその他の回答は少なかった。

Q20. 貴社において内部不正防止対策を主管し、組織全体に対する責任を負っている部門はどこですか。

＜パネルモニターが所属する企業のみの集計＞

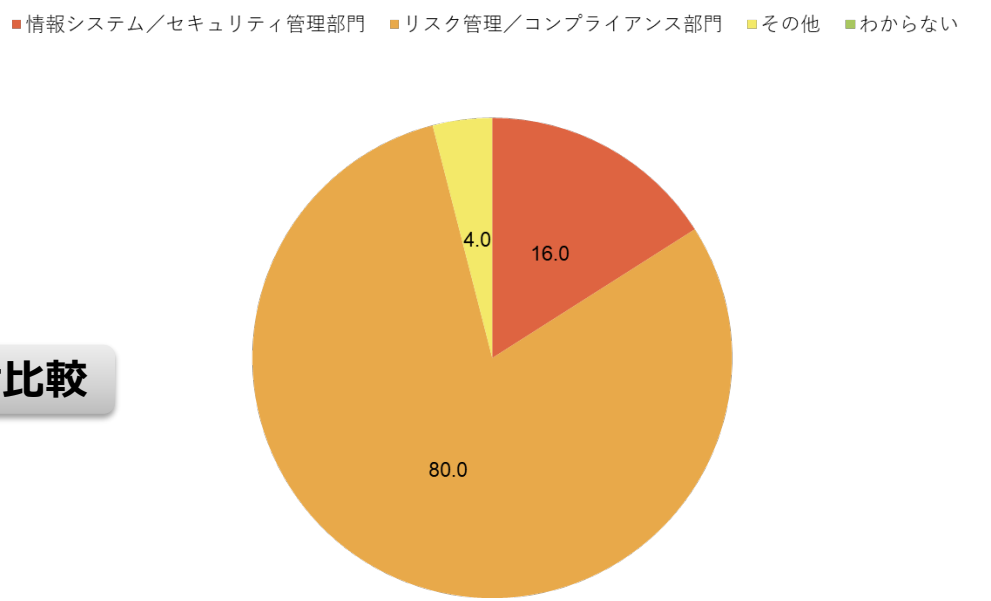
主たる回答



	n=	情報システム／セキュリティ管理部門	リスク管理／コンプライアンス部門	その他	わからない
TOTAL	1179	37.6	44.1	10.1	8.2

（ご参考：日経平均銘柄企業25社の集計）

参考比較

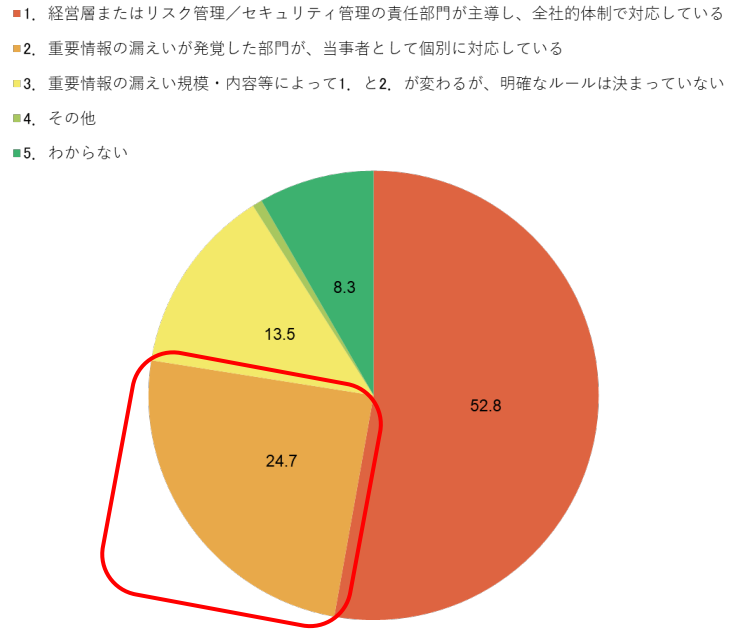


	n=	情報システム／セキュリティ管理部門	リスク管理／コンプライアンス部門	その他	わからない
TOTAL	25	16.0	80.0	4.0	0.0

5-1. 企業アンケート調査の単純集計結果（12/26）　～内部不正対策に取り組む組織的体制～

重要情報漏えいへの対応を全社的組織体制で掌握できている企業の割合は半数に過ぎない。現場組織の個別対応がかなり残っており、組織全体としての責任・権限が明確になっていないことが懸念される。また、重要情報を実際に取扱うことが多い現場組織（事業部門／営業部門）は、主管部門との連携も進んでいるとは言えない。

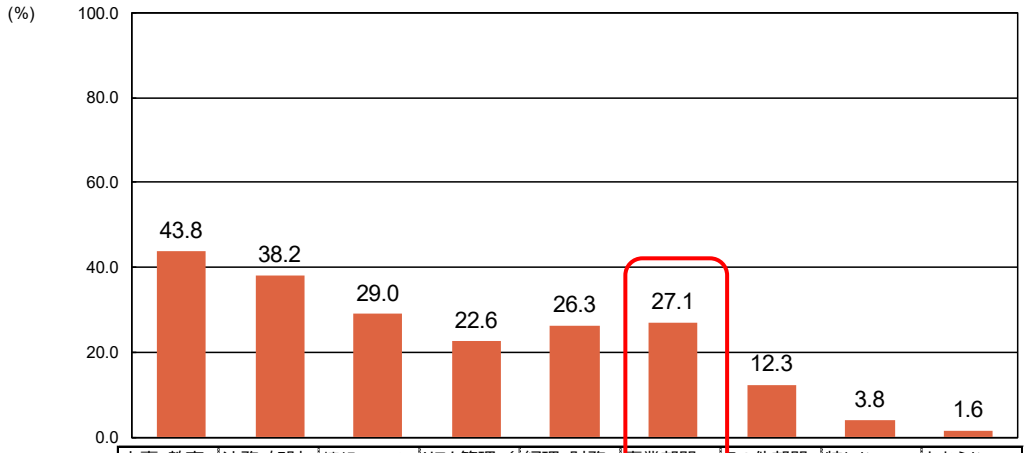
Q10. 重要情報が漏えいした時の組織的対応の体制について伺います。
＜パネルモニターが所属する企業のみの集計＞



	n=	1. 経営層またはリスク管理／セキュリティ管理の責任部門が主導し、全社的体制で対応している	2. 重要情報の漏えいが発覚した部門が、当事者として個別に対応している	3. 重要情報の漏えい規模・内容等によって1. と2. が変わるが、明確なルールは決まっていない	4. その他	5. わからない
TOTAL	1179	52.8	24.7	13.5	0.7	8.3

Q21. 貴社の内部不正防止体制において、主管部門の統括の下で、連携して対策や事後対応にあたっている関連部門はどれですか。

＜パネルモニターが所属する企業のみの集計＞



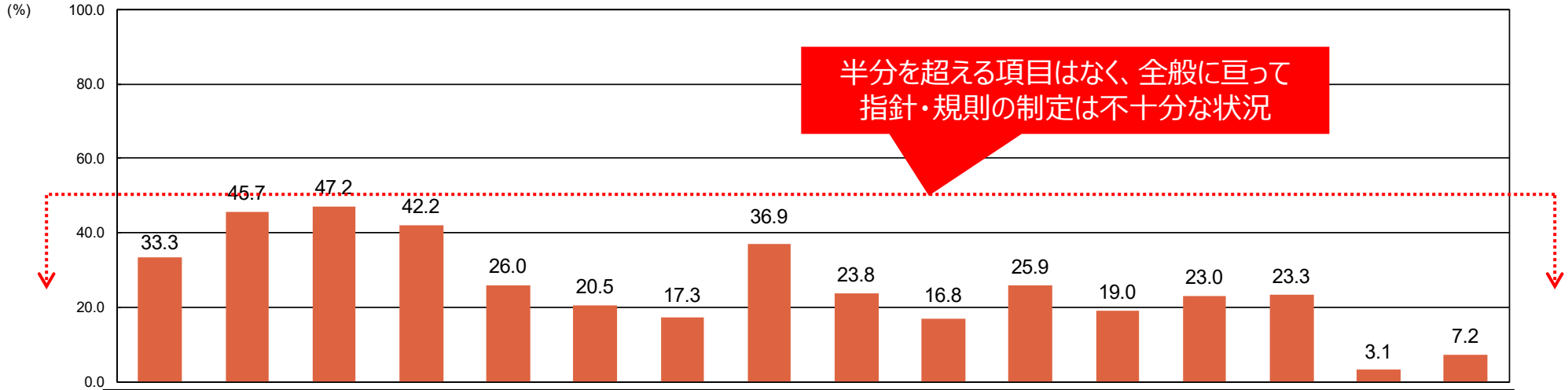
	n=	人事・教育部門	法務・知財部門	情報システム／セキュリティ管理部門	リスク管理／コンプライアンス部門	経理・財務部門	事業部門・営業部門	その他部門	特にない	わからない
TOTAL	1082	43.8	38.2	29.0	22.6	26.3	27.1	12.3	3.8	1.6

5-1. 企業アンケート調査の単純集計結果（13/26）　～内部不正対策に取り組む組織的体制～

内部不正防止について定めた指針・規則について、企業が基本方針、就業規則、重要情報の取り扱いに関する規則類、個人情報管理のための規則、営業秘密管理のための規則、テレワーク時のセキュリティ管理規則、クラウド利用規則等を定めている割合は十分ではない。

Q13. 貴社では内部不正防止について、どのような指針や規則が定められていますか。

＜パネルモニターが所属する企業のみの集計＞



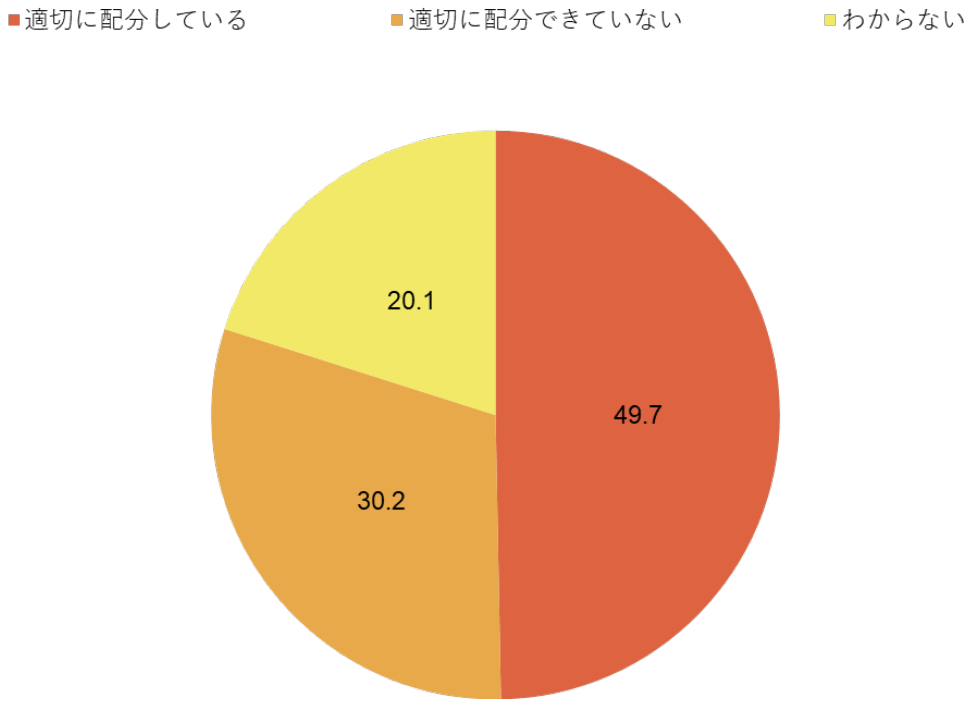
	n=	内部不正防止だけで独立した基本方針（内部統制の基本方針やセキュリティポリシーには含まれていない）	内部統制の基本方針（内部不正防止の基本方針を含む）	セキュリティポリシー（内部不正防止の基本方針を含む）	就業規則に書かれた内部不正防止に関するルール	組織全体に適用される重要情報の分類規則	秘密として管理する意思を明確に伝えるための、重要情報の表示規則	組織全体に適用される重要情報の分離保管規則	個人情報管理のための規則	営業秘密管理のための規則	限定提供データの管理のための規則	テレワーク時のセキュリティ管理規則（端末／ネットワーク利用、リモートアクセス等）	テレワーク時のクラウドサービス利用規則（利用可能サービス、取扱い可能な重要情報等）	中途退職者の秘密漏えい、中途採用者による他社の秘密持ち込みを防止するための規則	情報漏えい／セキュリティ監視システム適用にあたっての、従業員のプライバシー保護規則	どれもあてはまらない	わからない
TOTAL	1179	33.3	45.7	47.2	42.2	26.0	20.5	17.3	36.9	23.8	16.8	25.9	19.0	23.0	23.3	3.1	7.2

5-1. 企業アンケート調査の単純集計結果（14/26）　～内部不正対策に取り組む組織的体制～

「経営層がリソースを適切に配分している」という回答の割合がほぼ50%に達しており、「経営層がリソースを適切に配分できていない企業が多い」という仮説は必ずしも実態と合っていない。

Q22. 経営層は、内部不正防止に必要なリソース（予算、人材、施設・設備等）を適切に配分していますか。

＜パネルモニターが所属する企業のみの集計＞



	n=	適切に配分している	適切に配分できていない	わからない
TOTAL	1179	49.7	30.2	20.1

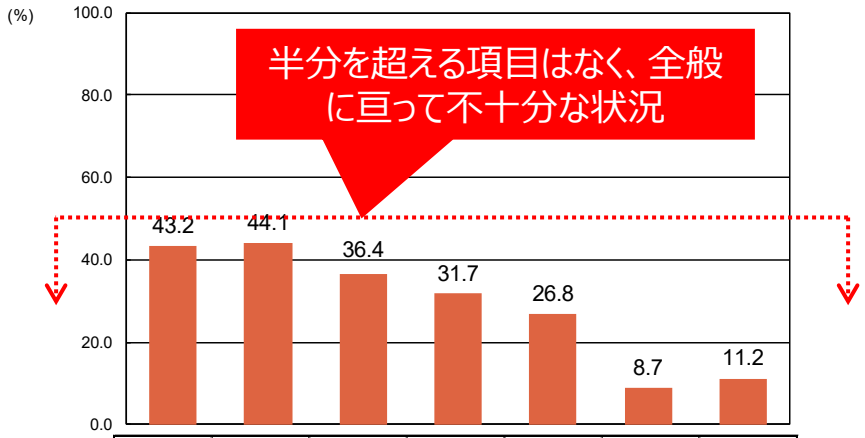
5-1. 企業アンケート調査の単純集計結果（15/26）　～内部不正対策に取り組む組織的体制～

内部不正対策に特化してみると、PDCAによって対策を継続的に改善していると回答した割合は43%に留まっており、まだ十分な水準まで到達していない。しかし、重要情報漏えい対策にまで視野を広げると、PDCA によって管理ルール・体制・適用を継続的に改善していると回答した割合が半数を超えている。

Q23. 貴社では内部不正防止対策のマネジメントシステムを構築し、運用していますか。

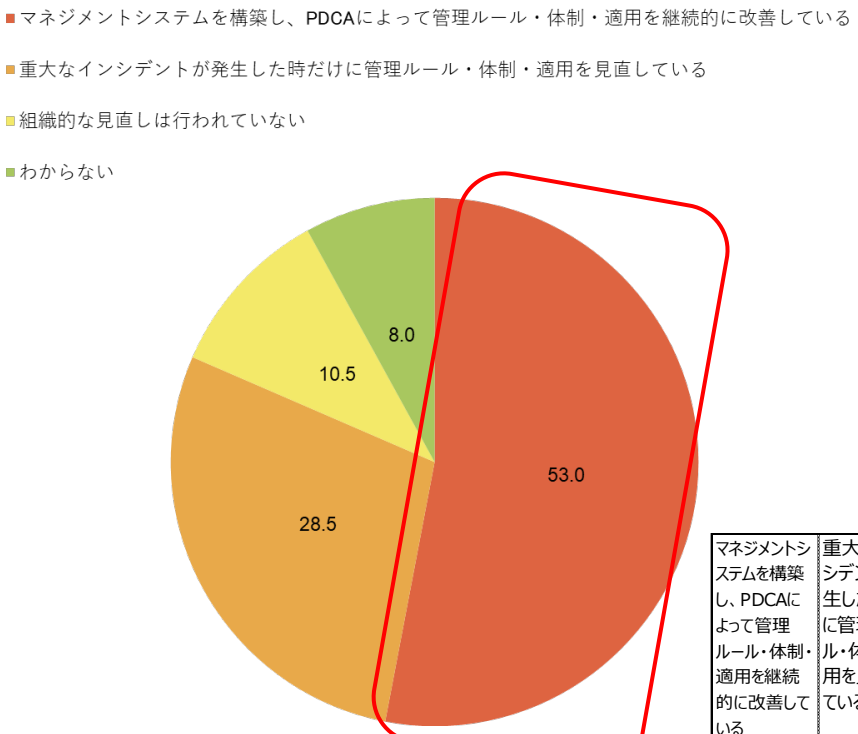
＜パネルモニターが所属する企業のみの集計＞

主たる回答



	n=	PDCAを組織として定期的に回し、内部不正防止対策を継続的に改善している	経営層が対策の改善に向けた方針を提示し、リーダーシップを発揮している	内部不正防止対策の効果をレビューまたは内部監査する体制が確立している	主管部門が、事故対応、対策のレビュー／内部監査結果等を取締役会等で報告している	内部統制システムやセキュリティマネジメントシステムの運用の一環として、内部不正防止対策の改善にも取り組んでいる	特にない	わからない
TOTAL	1179	43.2	44.1	36.4	31.7	26.8	8.7	11.2

Q11. 重要情報の管理ルール・体制・適用はどのように見直されていますか。



	n=	マネジメントシステムを構築し、PDCAによって管理ルール・体制・適用を継続的に改善している	重大なインシデントが発生した時だけに管理ルール・体制・適用を見直している	組織的な見直しは行われていない	わからない
TOTAL	1179	53.0	28.5	10.5	8.0

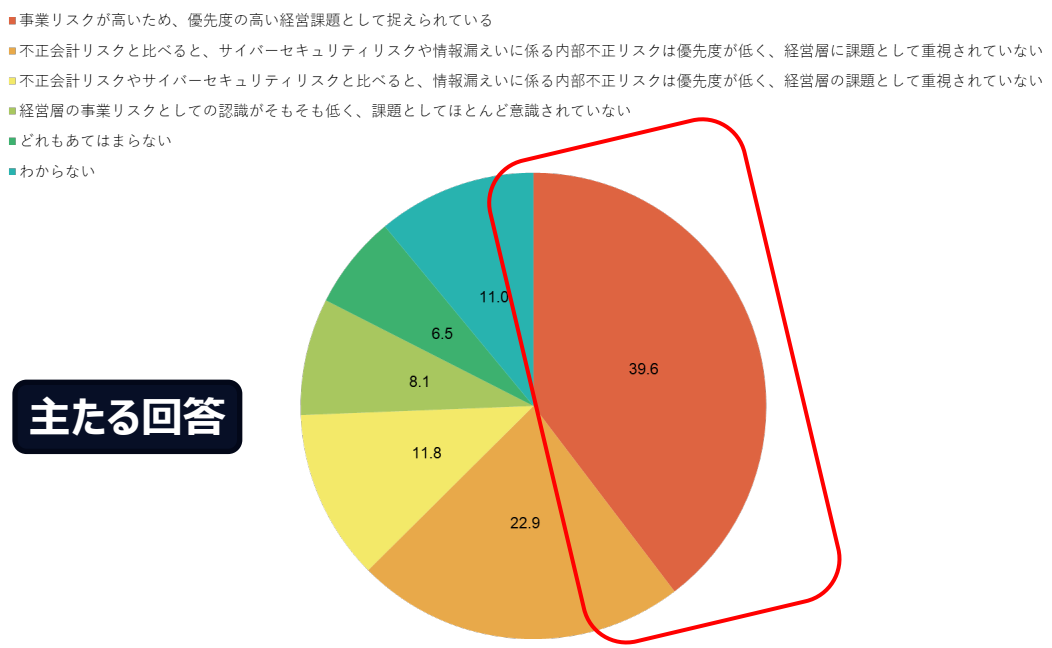
5-1. 企業アンケート調査の単純集計結果（16/26）　～内部不正防止の課題と対策～

経営層が内部不正の事業リスクについて十分に認識し、優先度の高い経営課題として捉えていると答えた回答者の割合はほぼ40%に留まっており、十分に高い水準に達しているとは言えない。内部不正防止に関する企業の取り組みが劣後される恐れがある。

Q30. 貴社では、内部不正リスクは重要な経営課題として捉えられていますか。

＜パネルモニターが所属する企業のみの集計＞

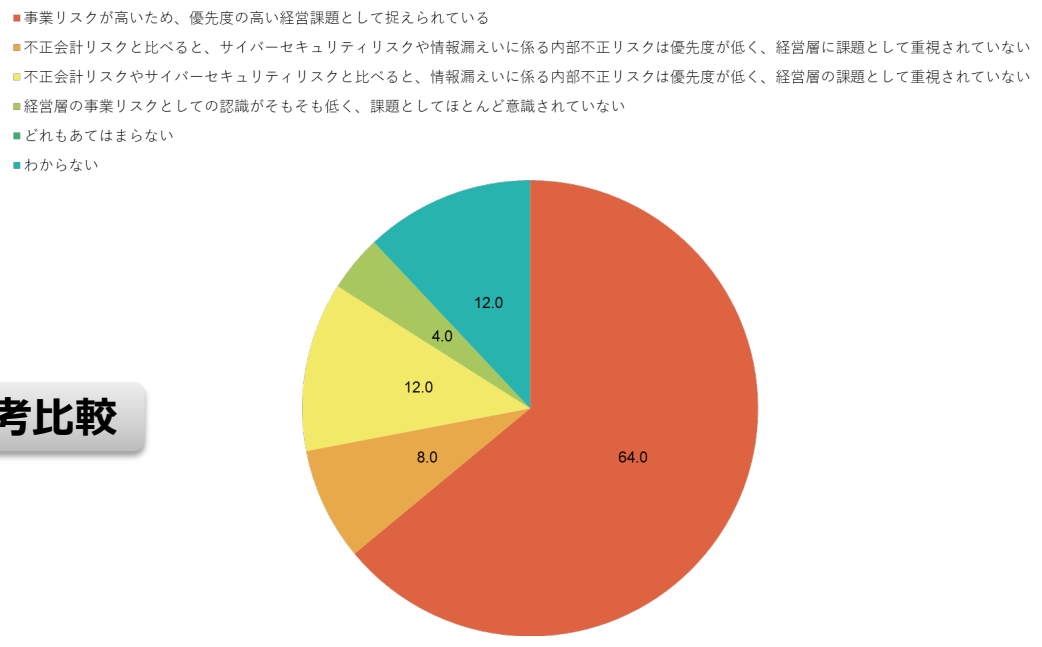
主たる回答



	n=	事業リスクが高いため、優先度の高い経営課題として捉えられている	不正会計リスクと比べると、サイバーセキュリティリスクや情報漏えいに係る内部不正リスクは優先度が低く、経営層に課題として重視されていない	不正会計リスクやサイバーセキュリティリスクと比べると、情報漏えいに係る内部不正リスクは優先度が低く、経営層の課題として重視されていない	経営層の事業リスクとしての認識がそもそも低く、課題としてほとんど意識されていない	どれもあてはまらない	わからない
TOTAL	1179	39.6	22.9	11.8	8.1	6.5	11.0

（ご参考：日経平均銘柄企業25社の集計）

参考比較



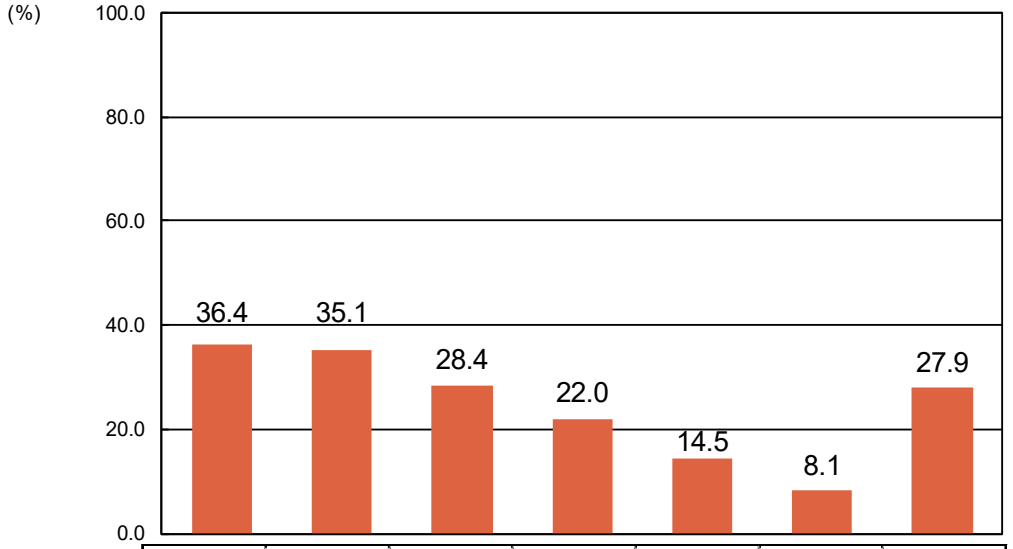
	n=	事業リスクが高いため、優先度の高い経営課題として捉えられている	不正会計リスクと比べると、サイバーセキュリティリスクや情報漏えいに係る内部不正リスクは優先度が低く、経営層に課題として重視されていない	不正会計リスクやサイバーセキュリティリスクと比べると、情報漏えいに係る内部不正リスクは優先度が低く、経営層の課題として重視されていない	経営層の事業リスクとしての認識がそもそも低く、課題としてほとんど意識されていない	どれもあてはまらない	わからない
TOTAL	25	64.0	8.0	12.0	4.0	0.0	12.0

5-1. 企業アンケート調査の単純集計結果（17/26）　～内部不正防止の課題と対策～

個人情報の漏えい事案／インシデントが最も多いものの、営業秘密や限定提供データの漏えい事案／インシデントとの間で大きな差は見られない。

Q25. 貴社では、内部不正事件の発生、またはそれが強く疑われる事態を経験したことがありますか。

＜パネルモニターが所属する企業のみの集計＞



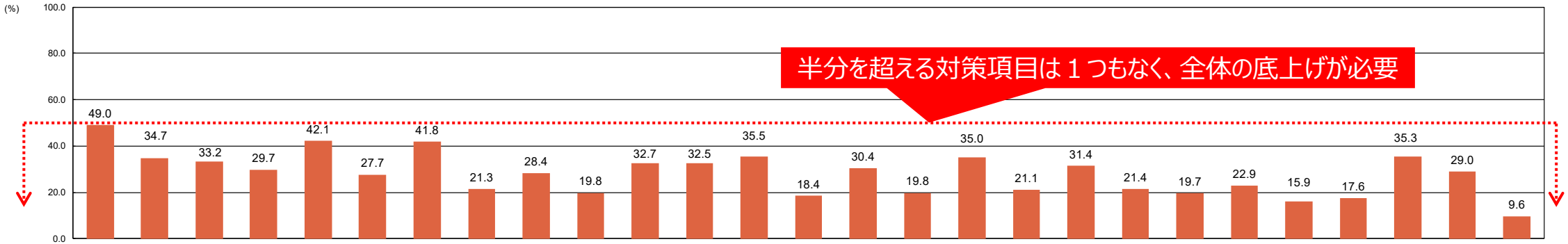
	n=	1．個人情報の漏えい事件・インシデントが発生（未遂を含む）	2．営業秘密の漏えい事件・インシデントが発生（未遂を含む）	3．限定提供データなど1．や2．以外の重要データの漏えい事件・インシデントが発生（未遂を含む）	4．事業、技術等の中核となる重要人物の国内競合企業への転職	5．事業、技術等の中核となる重要人物の海外競合企業への転職	6．その他	7．わからない・答えたくない
TOTAL	1179	36.4	35.1	28.4	22.0	14.5	8.1	27.9

5-1. 企業アンケート調査の単純集計結果（18/26）　～内部不正防止の課題と対策～

内部不正防止対策の実施状況について全体を俯瞰して注目されるのは、回答が半数を超える対策項目が１つもないことである。これは総じて対策が進んでいないことを示しており、まず全体を底上げする必要がある。

Q12. 重要情報の漏えいに関する内部不正を防止するために、貴社では次のどの対策を実施していますか。

＜パネルモニターが所属する企業のみの集計＞



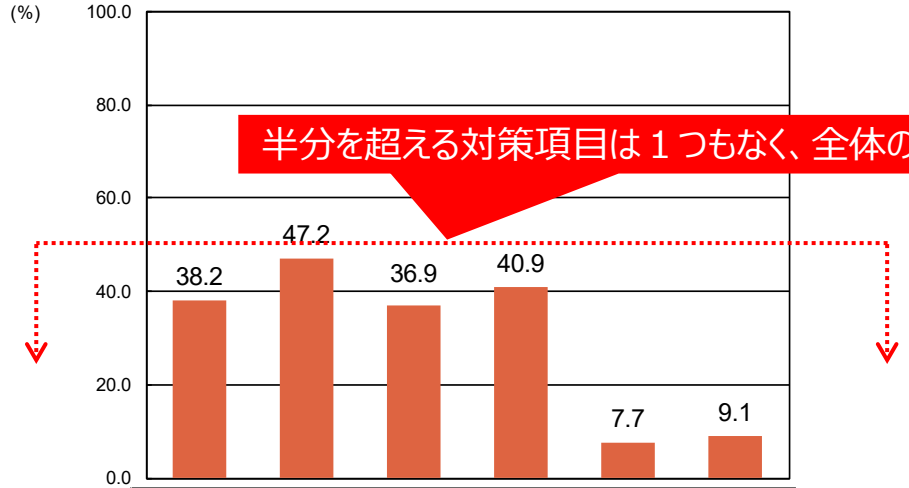
	n=	経営層（全社責任者を含む）が内部不正対策の基本方針を定め、社外に示し、組織内で周知徹底している	経営層（全社責任者を含む）は内部不正対策の実施にあたり、従業員とそのプライバシー保護を明言している	経営層（全社責任者を含む）が自ら定めた基本方針に基づき、必要なリソース確保のための決定・指示をしている	経営層（全社責任者を含む）は重要情報と判断する範囲や条件を明確に定め、組織全体に周知徹底している	内部不正対策に関し、組織全体における責任部門・責任者が明確に定められている	内部不正防止の責任者は、（1）サイバーセキュリティ対策の責任者、または（2）リスク管理部門／コンプライアンス部門等の責任者が兼ねる	内部不正防止のリテラシー向上のため、定期的または事故発生時に組織全体に教育を実施している	テレワーク実施者に対し、社内規程や関連法規の教育を実施し、理解度を確認している	採用時や退職時だけでなく、異動時、昇進時、新プロジェクトへの参加時・終了時などに秘密保持義務契約の締結（または誓約書の提出）を求めている	営業や技術の中核となる重要人物が退職する場合は、退職が決まった段階で、重要情報へのアクセスの監視及びアクセスログの確認等を強化している	退職後には速やかに退職者のID、重要情報へのアクセス権限、テレワークでの社内ネットワークへのアクセス権限等を削除している	従業員に不満が蓄積しないように、労務管理、人事管理、職場やテレワークにおける良好で十分なコミュニケーションの確保等について、必要な対策を講じている	ID管理と本人確認（認証）を強化している	重要情報を含む電子文書は、容易に判別できるようにしている	重要情報には必要最小限の従業員しかアクセスできないように管理している	重要情報は定期的に棚卸しを行い、不要なものを消去している	入退室管理やPC・デバイスの社外持出し管理を実施している	BYOD（個人デバイスの業務利用）は許可していない	重要情報に対するアクセス監視、ログ記録等を実施し、それを組織全体に周知している	公的機関のガイドライン等に従って、会社支給PCのテレワーク対策が強化されている	テレワークで扱える重要情報の範囲をルール化している	業務で使用できるクラウドや、クラウド上で扱える重要情報の範囲をルール化している	サプライヤーや委託先等との重要情報の受渡しを厳格に管理し、暗号化している	サプライヤーや委託先等の重要情報漏えい対策を、契約時及び契約中に確認している	内部不正発覚後の事後対策や、事業継続についてマニュアル化している	組織内外で内部不正事故が起こった場合、事故について組織内部で共有し、内部不正の心理的抑止に役立てている	どれもあてはまらない
TOTAL	1179	49.0	34.7	33.2	29.7	42.1	27.7	41.8	21.3	28.4	19.8	32.7	32.5	35.5	18.4	30.4	19.8	35.0	21.1	31.4	21.4	19.7	22.9	15.9	17.6	35.3	29.0	9.6

5-1. 企業アンケート調査の単純集計結果（19/26）　～内部不正防止の課題と対策～

従業員の不満を蓄積させない職場環境構築のための対策は、いずれも回答割合が50%に達しておらず、十分な実施水準とは言えない。
また、テレワークを行う従業員を支援し、内部不正を行う気にさせないための対策については、「各部門による自主的なコミュニケーション強化の取組みの奨励」に最も重点が置かれており、この対策を実施している割合はほぼ50%に達している。

Q39. 貴社では、従業員が不満を蓄積しない職場環境を構築するための対策をとっていますか。

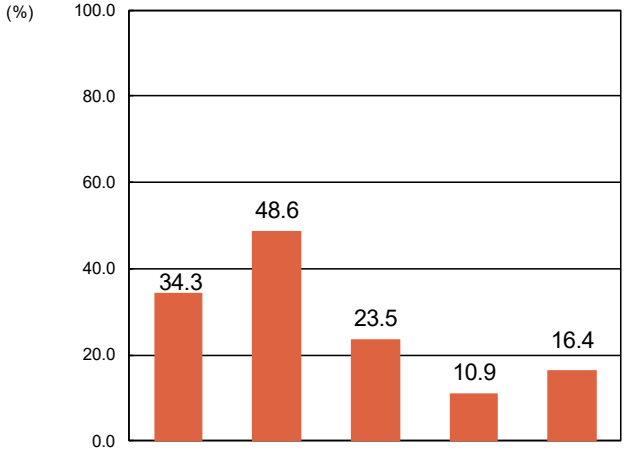
＜パネルモニターが所属する企業のみの集計＞



	n=	人事・業績評価の公平性を高めている	職場コミュニケーションの充実に持続的に取り組んでいる	テレワーク従事者と社内勤務者を公平に処遇している	服務規律違反、法令違反、ハラスメント、その他の不正行為についての内部通報制度を設けている	どれもあてはまらない	わからない
TOTAL	1179	38.2	47.2	36.9	40.9	7.7	9.1

Q24. 貴社では、テレワークを行う従業員に対する支援を行い、内部不正を行う気にさせないための対策を講じていますか。

＜パネルモニターが所属する企業のみの集計＞



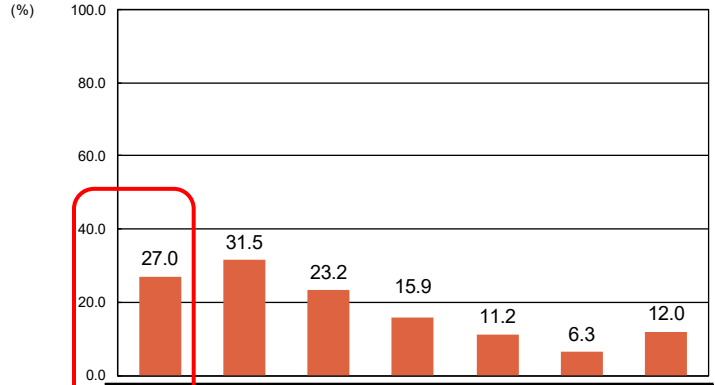
	n=	テレワークを行う従業員のための全社的な連絡窓口を設置して、積極的に相談にのっている	各部門による自主的なコミュニケーション強化の取組みを推奨し、テレワークを行う従業員の孤立・不安・ストレス・不満の発見・緩和に努めている	定期的に出勤日を設けている	その他	わからない
TOTAL	1179	34.3	48.6	23.5	10.9	16.4

5-1. 企業アンケート調査の単純集計結果（20/26）　～内部不正防止の課題と対策～

内部不正防止にあたり、個人情報以外の重要情報にも対応できていると回答した割合は30%に届いておらず、その漏えいに関する内部不正対策はかなり不十分な状況である。そもそも、個人情報以外の重要情報を特定する仕組みを持つ企業でさえ半数に満たないのが現状。特定できていない重要情報を内部不正から守ることはできないので、まずは個人情報以外の重要情報を特定する能力から底上げすることが必要である。

Q32. 貴社では、内部不正防止への取組みにあたり、重要情報が多様化していることに対応できていますか。

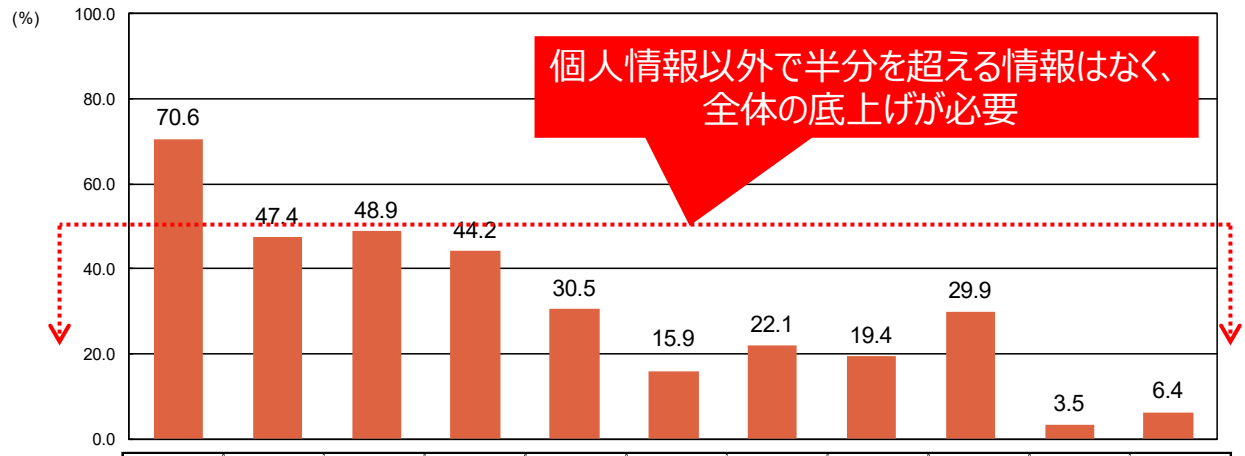
＜パネルモニターが所属する企業のみの集計＞



	n=	個人情報だけでなく、重要技術情報・ノウハウ、重要データにも対応できている	個人情報以外の重要情報（重要技術情報・ノウハウ、重要データ）を十分に特定・分類できていないため、うまく対応できていない	脅威やリスクが異なるため、重要技術情報・ノウハウや重要データにはうまく対応できていない	対応する法制度が異なるため、重要技術情報・ノウハウや重要データにはうまく対応できていない	重要データについては共有・利活用の知識や経験値が不足しており、うまく対応できていない	どれもあてはまらない	わからない
TOTAL	1179	27.0	31.5	23.2	15.9	11.2	6.3	12.0

Q7. 貴社ではどのような種類の重要情報を特定する仕組みを作っていますか。

＜パネルモニターが所属する企業のみの集計＞



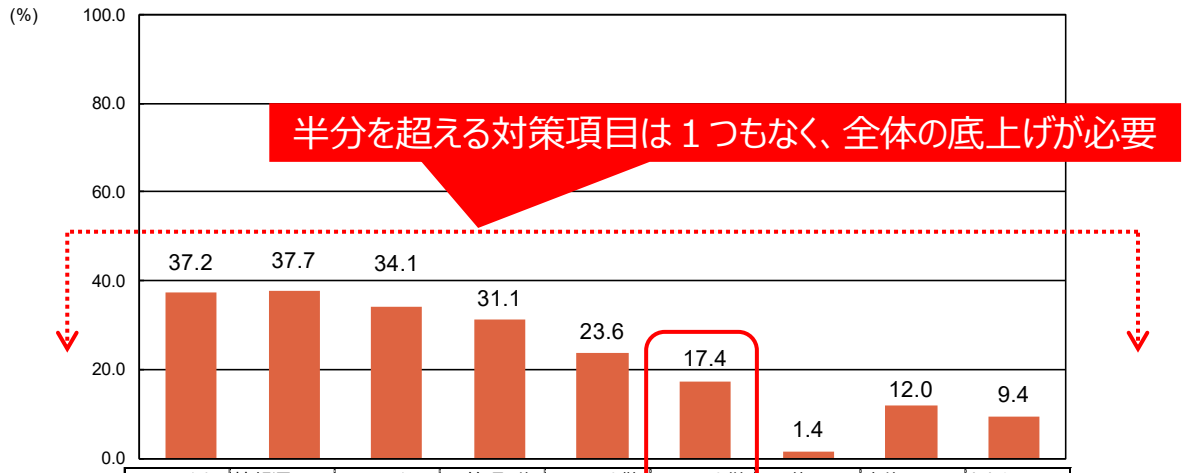
	n=	個人情報	重要な技術情報・ノウハウ	重要な営業情報	営業秘密として管理している情報	利活用する価値が高い重要データ	AI学習用のデータセット	限定提供データとして管理しているデータ	安全保障貿易管理（輸出管理）に係る機微技術情報	他社から「重要であるため秘密にして欲しい」と言われて受け取っている情報	どれもあてはまらない	わからない
TOTAL	1179	70.6	47.4	48.9	44.2	30.5	15.9	22.1	19.4	29.9	3.5	6.4

5-1. 企業アンケート調査の単純集計結果（21/26）　～内部不正防止の課題と対策～

テレワーク時の内部不正対策については、いずれの対策も回答割合が40%に満たず、十分な水準に達しているとは言えない。
テレワーク従事者のコミュニケーションを確保し、孤立・不安・ストレス・不満の発見と緩和を促進する対策については、各部門による自主的な取り組みが組織全体での措置を大きく上回っている。

Q35. 貴社では、テレワークを行う従業員の内部不正防止対策を実施していますか。

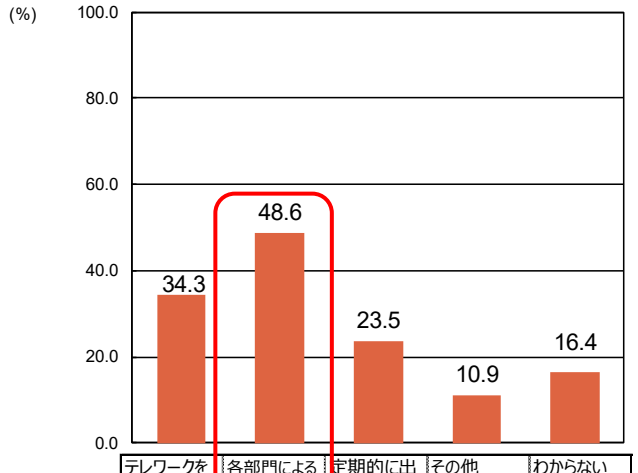
＜パネルモニターが所属する企業のみの集計＞



	n=	テレワークを行う従業員に対し、テレワークに関わる社内規則／法制度を教育・徹底している	情報漏えいに備えて、テレワークで取り扱うことができる重要情報を制限している	テレワーク用の会社支給PC等の操作ログの取得・分析等で、内部不正の早期発見や事後対応の機能を強化している	ID管理、権限管理、当人認証等を強化することで、テレワークによって分散した重要情報のアクセス管理を強化している	テレワーク勤務と社内勤務を公平に処遇している	テレワーク従事者との十分なコミュニケーションを確保できる対策を講じている	その他	実施していない	わからない
TOTAL	1179	37.2	37.7	34.1	31.1	23.6	17.4	1.4	12.0	9.4

Q24. 貴社では、テレワークを行う従業員に対する支援を行い、内部不正を行う気にさせないための対策を講じていますか。（再掲）

＜パネルモニターが所属する企業のみの集計＞



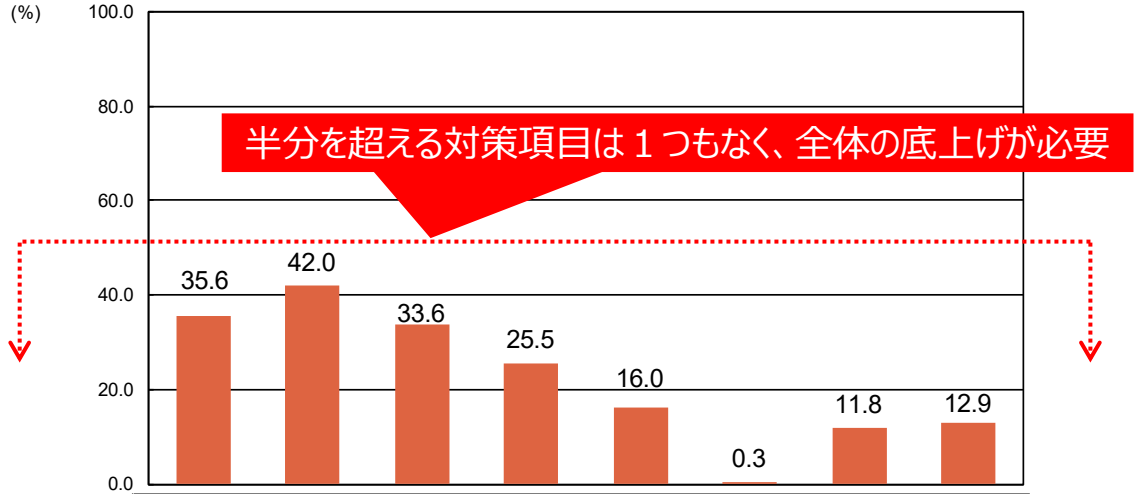
	n=	テレワークを行う従業員のための全社的な連絡窓口を設置して、積極的に相談にのっている	各部門による自主的なコミュニケーション強化の取組みを推奨し、テレワークを行う従業員の孤立・不安・ストレス・不満の発見・緩和に努めている	定期的に出勤日を設けている	その他	わからない
TOTAL	1179	34.3	48.6	23.5	10.9	16.4

5-1. 企業アンケート調査の単純集計結果（22/26）　～内部不正防止の課題と対策～

クラウドサービス利用時の内部不正対策についても、いずれの対策も回答割合が40%に満たず、十分な水準に達しているとは言えない。

Q36. 貴社では、クラウドサービスを利用する従業員の内部不正防止対策を実施していますか。

＜パネルモニターが所属する企業のみの集計＞



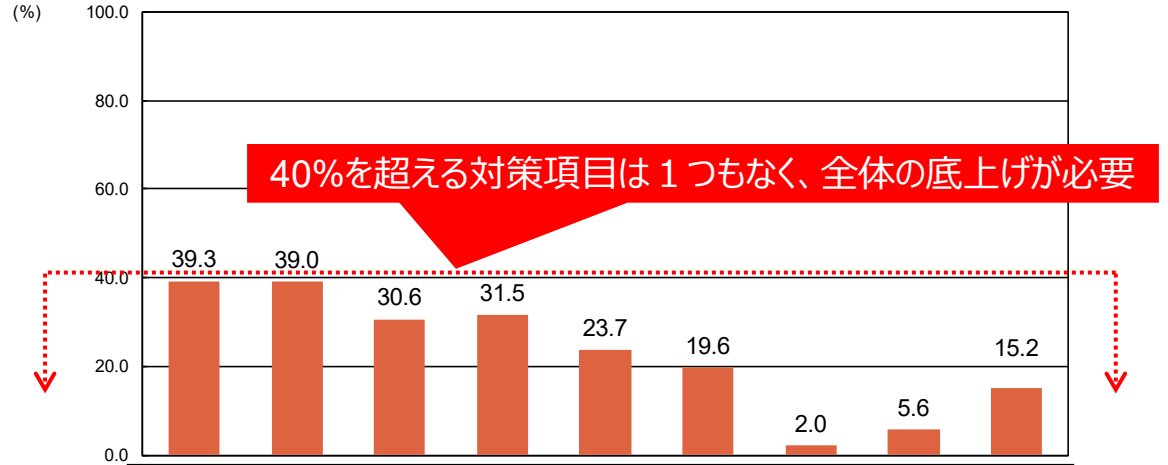
	n=	クラウドサービスの利用ルールに関する組織全体への周知・教育を実施している	利用を許可するクラウドサービスの一覧を定めて管理しており、それ以外の利用を禁止している	クラウドサービス上で取り扱うことができる重要情報を制限している	クラウドサービス上で取り扱う重要情報に対するアクセス権管理やデータ管理を実施するとともに、利用状況をモニタリングしている	クラウドサービス利用に関する管理責任及びインシデント対応責任の分担を明確に定めている	その他	実施していない	わからない
TOTAL	1179	35.6	42.0	33.6	25.5	16.0	0.3	11.8	12.9

5-1. 企業アンケート調査の単純集計結果（23/26）　～内部不正防止の課題と対策～

企業・組織がサプライヤーや委託先と重要情報の管理策について合意しているかについては、いずれの項目も合意していると答えた回答者の割合が40%に届いておらず、十分な水準に達しているとは言えない。

Q33. 貴社において、サプライヤーや委託先と重要情報の管理策について合意していますか。

＜パネルモニターが所属する企業のみの集計＞



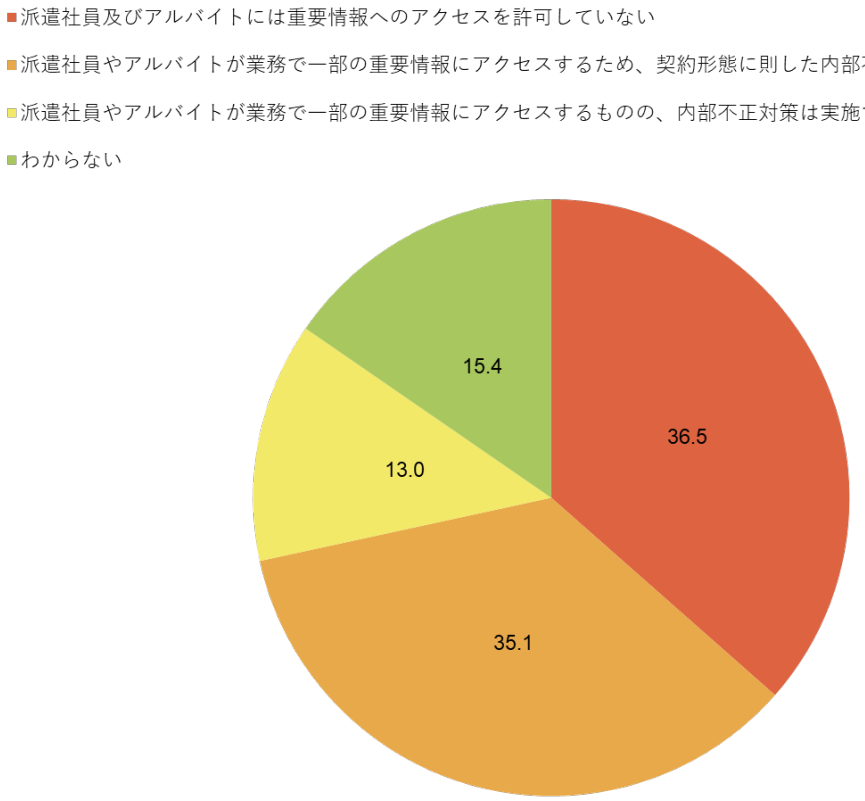
	n=	重要情報の管理水準、暗号化、返却・廃棄の方法等について、契約等を通じて合意している	受渡し（第三者提供を含む）ができる重要情報の範囲について明文化し、合意している	受け渡した重要情報は、自社情報と他社情報に分けて管理することで合意している	取扱いを委託した個人情報が漏えいした場合に、サプライヤーや委託先が、貴社が行う調査に協力することを、契約を通じて合意している	重要情報漏えい時の事後対応や事業継続について、サプライヤーや委託先と協力できるように連携体制について合意している	限定提供データとして保護される、またはライセンス供与される重要データの共有と利活用に関するルールについて、契約等を通じて合意している	その他	合意していない	わからない
TOTAL	1179	39.3	39.0	30.6	31.5	23.7	19.6	2.0	5.6	15.2

5-1. 企業アンケート調査の単純集計結果（24/26）　～内部不正防止の課題と対策～

非正規雇用者の内部不正対策については、重要情報へのアクセスを許可しない、または契約形態に則した対策を実施していると回答した割合が70%を超えており、十分に高い水準に達している。

Q34. 貴社では、近年増加している非正規雇用者の内部不正対策を実施していますか。

＜パネルモニターが所属する企業のみの集計＞



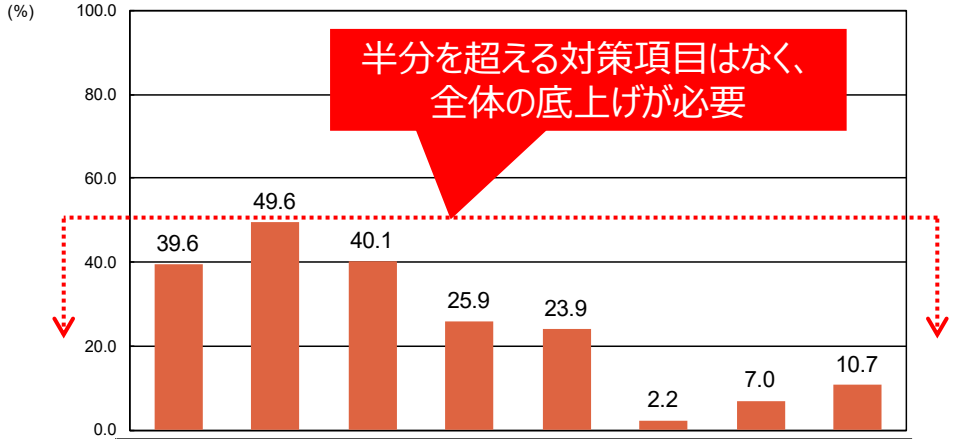
	n=	派遣社員及びアルバイトには重要情報へのアクセスを許可していない	派遣社員やアルバイトが業務で一部の重要情報にアクセスするため、契約形態に則した内部不正対策を実施している	派遣社員やアルバイトが業務で一部の重要情報にアクセスするものの、内部不正対策は実施できていない	わからない
TOTAL	1179	36.5	35.1	13.0	15.4

5-1. 企業アンケート調査の単純集計結果（25/26）　～内部不正防止の課題と対策～

中途退職者に課す秘密保持義務の実効性を高めるための対策としては、秘密保持義務契約の締結についての内部規則を定めて就業規則でその遵守を求めること、この規則に従って契約締結／誓約書提出を行うこと、就業規則に退職後の定めを規定すること等が中心となっている。しかし、中心となる対策でさえ回答は半数に達しておらず、十分な水準であるとは言えない。また、中途採用時／中途退職時の内部不正防止に関する規則を策定している割合も、いずれも50%に達しておらず、こちらも十分な水準とは言えない状況である。

Q37. 貴社では、雇用の流動化を踏まえて、中途退職者に課す秘密保持義務の実効性を高める対策を実施していますか。

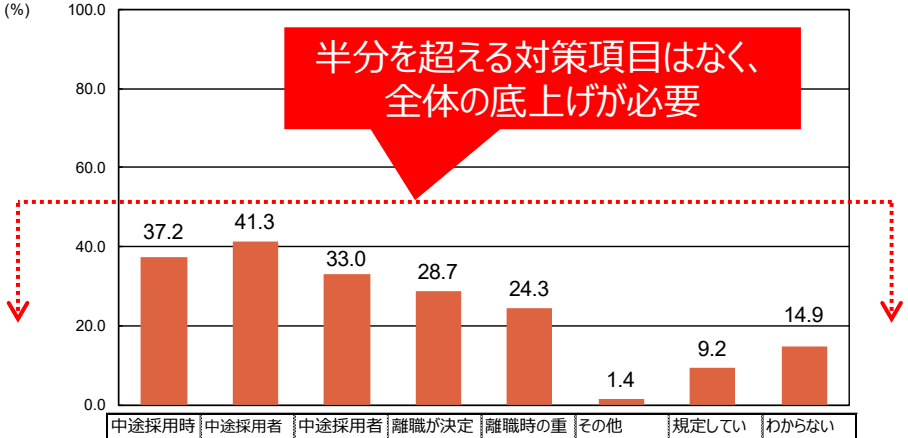
＜パネルモニターが所属する企業のみの集計＞



	n=	退職時だけでなく、就職時、異動時、昇格時、新プロジェクトへの配属時・終了時等に、秘密保持義務契約の締結（または誓約書の提出）を求めている	秘密保持義務契約の締結（または誓約書の提出）についての内部規則を定め、就業規則でその順守を求めている	就業規則に退職後の定めを規定している	秘密保持義務の有効期間を十分長く設定している	秘密保持義務の対象となる重要情報の範囲・内容を明確に定めている	その他	実施していない	わからない
TOTAL	1179	39.6	49.6	40.1	25.9	23.9	2.2	7.0	10.7

Q38. 貴社では、社内規程において採用時と離職時の不正防止に関する規則を規定していますか。

＜パネルモニターが所属する企業のみの集計＞



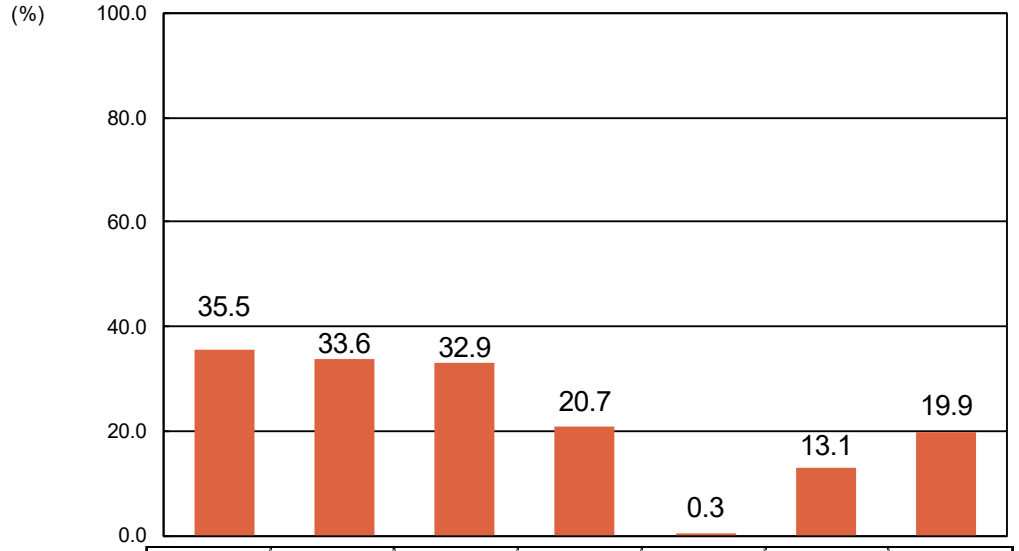
	n=	中途採用時に他社の個人情報、営業秘密、限定提供データ等の重要情報を持ち込まないように、誓約書の提出を規定している	中途採用者による他社の重要情報の持ち込みが発生しないように、私物の記録媒体や許可されていないオンラインストレージの使用を禁止あるいは監視するよう規定している	中途採用者による重要情報の持ち込みを抑止するため、周知・教育を通じて中途採用者に注意喚起することを規定している	離職が決定した後離職するまでの間に重要情報の不正な持ち出しが発生しないように、重要情報へのアクセス等の監視強化を規定している	離職時の重要情報持ち出しを抑止するため、周知・教育を通じて中途退職者に注意喚起することを規定している	その他	規定していない	わからない
TOTAL	1179	37.2	41.3	33.0	28.7	24.3	1.4	9.2	14.9

5-1. 企業アンケート調査の単純集計結果（26/26）　～内部不正防止の課題と対策～

退職者の内部不正を発見したときの対応については、企業側はまだ取り組みが成熟していない状況であると推察される。

Q40. 貴社では、退職者による内部不正を発見した時の対応について準備していますか。

＜パネルモニターが所属する企業のみの集計＞



	n=	内部不正が疑われる退職者本人への警告	内部不正が疑われる退職者の転職先への警告（内容証明等を含む）	内部不正が疑われる退職者や転職先への差止／損害賠償請求（民事訴訟等）	内部不正が疑われる退職者や転職先の刑事告訴に向けた警察への相談	その他	準備していない	わからない
TOTAL	1179	35.5	33.6	32.9	20.7	0.3	13.1	19.9

5-2. 企業のインタビュー調査からの示唆　～企業・組織全体として知っておくべき基礎知識

企業・組織で知っておくべき基礎知識について、企業インタビューで実態を確認するとともに、課題克服に向けた示唆を抽出した。

- ■ 社内規程が求める「重要情報の識別と秘密区分」の基準は特に重要な基礎知識だが、組織全体に周知する企業と、敢えて従業員に知識を求めずすべてを重要情報として扱う企業に分かれた。
- ■ 法制度／ガイドラインの知識については、個人情報保護を重視する企業が多く、不正競争防止法との間に違いが見られた。ガイドラインについては、これに適合しない場合に企業がどのようなリスクを受容することになるかを認識した上で、組織全体への周知のあり方を調整する必要があるという示唆を得た。
- ■ 情報漏えい／セキュリティリスクの基礎知識については、事例から学び、その背景や理由をしっかりと認識することが必要だと分かった。

共通の調査軸	知識の種別	対象	得られた示唆
企業・組織全体として知っておくべき基礎知識の実態	社内規程についての知識	組織全体	■ 重要情報の識別と秘密区分の理解は、従業員が知っておくべき基礎知識の中でも特に重要な項目だが、組織全体に周知徹底する企業に加えて、業務で生み出された情報を敢えてすべて重要情報として取扱う企業もあった。 ■ 内部不正防止に関する近年の環境変化は急であり、必要とされる基礎知識の最新化に繋がる企業の社内規程見直しの取り組みが問われている。最新の基礎知識を反映するための社内規程の改訂が遅れると、その周知・教育を通じて組織全体に浸透するはずの最新の基礎知識が従業員に伝わらず、結果として仮説が示唆するような知識不足の状態に陥る。
	法制度についての知識	内部不正防止の担当部署	■ インタビュー対象企業においても、不正競争防止法よりも個人情報保護法の知識に重点を置いている企業が多かった。不正競争防止法についての知識が足りないという仮説を否定するほどの根拠は見出せなかった。
	関連するガイドライン等についての知識	内部不正防止の担当部署	■ ガイドラインへの適合の重要性はその内容と企業特有のリスクの状況の対比によって変化するので、適合しない場合に自社が受容することになるリスクを十分に認識した上で、組織全体に周知するガイドラインの範囲や程度を調整することで、仮説が示唆する必要知識の不足を克服できる。
	情報漏えい／セキュリティリスクに関する知識	組織全体	■ 他社の事例を自社に当てはめてみる等によって事例から学び、重要情報漏えい等の背景・理由をしっかりと認識し、従業員全体で情報漏えいリスクの知識を高めていくことで、仮説が示す知識不足の状態を改善できる。

5-2. 企業のインタビュー調査からの示唆　～内部不正防止に取り組む組織的体制

内部不正防止に取り組む組織的体制についての企業インタビュー結果：

- ■ 経営層の情報発信、経営層によるリソース配分については、重要情報漏えいや内部不正防止に対する経営層の認識・関心の高さがポイントとなる。
- ■ 内部不正防止等のための組織体制としては、リスク管理を統括する役員が全社責任者となり、リスク管理部門が責任部門となり、コンプライアンス部門が人的管理や事案発生時の法的対応を支援し、IT／セキュリティ部門が技術・運用面を支援する構造がモデルケース。しかし、関連部門との連携等をうまく活かすことで、IT／セキュリティ部門が責任部門としてうまく機能している事例もあり、全ての企業をモデルケースに当てはめる必要はないと考えられる。
- ■ 社内ポリシー／規定の整備については、社内委員会をうまく活用することが考えられる。
- ■ 重要情報保護に対する意識が高く、その責任・組織体制が充実している企業では、重要情報保護対策についてのマネジメントシステムが充実している。

共通の調査軸	仮説に基づく調査項目	得られた示唆
内部不正防止に取り組む組織的体制の実態	経営層の情報発信	■ 経営層が重要情報漏えいの事業リスクをしっかりと認識し、コンプライアンスを重視している企業については、内部不正防止についての経営層の高いリーダーシップや率先した情報発信を期待できる。
	組織全体としての責任・権限の明確化	■ 内部不正防止等のための組織体制としては、リスク管理を統括する役員が全社責任者となり、リスク管理部門が責任部門となり、コンプライアンス部門が人的管理や事案発生時の法的対応を支援し、IT／セキュリティ部門が技術・運用面を支援する構造がモデルケースと考えられる。しかし、企業の考え方によって実際の体制は多様であり、全てをモデルケースに収めることは難しい。 ■ IT／セキュリティ部門が責任部門となっていることも多く、法務・知財部門や事業部の統括組織等と連携して内部不正に関する事業リスクやコンプライアンス上の判断を円滑に処理すること、CDOを任命する等によって重要情報の特定／分類についての指導力を強化すること等の工夫によって、組織全体の体制をうまく回している企業も複数あった。
	社内ポリシー／規定の整備	■ 内部不正防止に関する規則の整備について、既存の社内委員会をうまく活用することが考えられる。 ■ テレワークの推進、クラウド利用の拡大、関連する法規制等の動向を踏まえて、社内規程を随時更新していく上でも、社内委員会を活用して意見集約を行う手法は有益。
	経営層によるリソースの適切な配分	■ 経営層が内部不正防止に高い関心を持っている大企業は、必ずしも仮説に合致しない。
	内部不正対策に関するマネジメントシステム	■ 重要情報保護に対する意識が高く、その責任・組織体制が充実している企業では、重要情報保護対策についてのマネジメントシステムが充実しており、このマネジメントシステムを活用して内部不正対策の改善にも効果を上げることができる。このような企業が増やすことが必要。
	テレワークの従業員支援体制	■ 特に言及なし。

5-2. 企業のインタビュー調査からの示唆　～組織全体への周知・教育

組織全体への周知・教育についての企業インタビュー結果：

- 内部不正対策は、コンプライアンス研修の一環として周知・教育されることが中心。
- 個人情報に対する不正の知識は良く周知・教育されている。営業秘密保護についてリテラシー教育を実施している企業も少なくはないが、秘密文書の実務上の扱いが重要であり、経験も必要とされることから、教育効果をどこまで期待できるかが難しい。
- 誤った行動、意図した不正によるインシデント事例を活用したリテラシー教育は、実践に繋がる効果が高い。事例を解説して腹落ちさせるのが良い。
- 規程や対策のリテラシー教育においても、その背景にある理由の理解を進めることで、従業員の実践に繋がることを期待できる。グループディスカッション、再発防止教育用の動画等の制作＆視聴、定期的なルール順守のセルフチェック等の教育方法が有効。

共通の調査軸	仮説に基づく調査項目	得られた示唆
組織全体への周知・教育の実態	一般の職員に対する、内部不正対策に関する周知・教育	■ 内部不正対策は、コンプライアンス研修の一環として周知・教育されることが中心であると考えられる。リフレッシュ教育で、ミス（誤った行動）をするとどのようなリスクが生じるのかを簡潔に教育している好事例が見られた。 ■ 全体を俯瞰してリテラシー教育が最も充実しているのは個人情報保護である。個人情報に対する不正の知識は良く周知・教育されており、仮説には合致しない。 ■ 営業秘密保護についてのリテラシー教育も決して少なくはなく、仮説が当てはまるかは微妙である。但し、営業秘密保護では秘密文書の実務上の扱いが重要であり、経験も必要とされることから、リテラシー教育の効果をどこまで期待できるかが難しい面がある。 ■ インシデント事例を活用したリテラシー教育は実践に繋がる効果が高いことが知見として得られた。これに積極的に取り組むことで、内部不正対策に関する周知・教育の充実に貢献できる。
	内部不正対策を組織全体で実践できる環境	■ リテラシー教育を従業員の実践に繋げていくためには、社内外の事案／インシデント／ヒヤリハットを事例として取り上げ、解説して腹落ちさせる手法が有効と考えられる。 ■ 同様に、規程や対策のリテラシー教育においても、その背景にある理由の理解を進めることで従業員の実践に繋げることができるため、グループディスカッション、再発防止教育用のコンテンツ（動画等）の制作＆閲覧（視聴）、定期的なルール順守のセルフチェックなど、e-Learningに留まらない教育方法の適用が有効。

5-2. 企業のインタビュー調査からの示唆　～内部不正防止の課題と対策

内部不正防止の課題と対策についての企業インタビュー結果：

- 経営リスクや事業リスクとしての内部不正リスクの優先度は必ずしも高くなく、対策が進んでいない企業が散見された。しかし事業の特性上、個人情報の漏洩リスクが強く意識されている企業では、内部不正防止に重点が置かれていた。
- 内部不正対策においては、従業員教育にまず重点を置き、これでカバーできないところに順次技術的対策を適用していくのが効率的・効果的であるという示唆が得られた。
- 個人情報以外の重要情報の漏洩や内部不正に対処するためには、まず当該情報を正しく特定・分類するところから始める必要があるとの指摘があった。
- ニューノーマル等の環境変化に伴う内部不正リスクの高まりについては、EDRやクラウドサービスの利用制限等の対策が広く実施されていた。また、大企業において、先進的な対策技術や調達マネジメント手法を適用している事例が見られた。
- 中途退職者／中途採用者の内部不正対策は必ずしも遅れてはいないが、重要情報の源泉となる重要プロジェクトの秘密保持や他社の重要情報の持ち込みについてはまだ対策が十分でない企業が多かった。
- 内部不正を誘発しない職場環境の整備に重点を置いて取り組んでいる企業が複数あったが、必ずしも大企業ばかりではなく、ベンチャー系中小企業の中にもこうした意識の高い企業が見られた。

共通の調査軸	仮説に基づく調査項目	得られた示唆
内部不正防止の課題と対策の実態	経営リスクや事業リスクとしての内部不正リスクの優先度	■ 優先度が低く、対策が進んでいない企業の例が散見された。 ■ 顧客の個人情報の漏えいリスクが大きく、これを強く意識している企業では一般に仮説が当てはまらない。大手ハイテク製造業のように営業秘密の窃取リスクを強く意識している企業もある。これらを踏まえると、仮説が実際に当てはまるかは相半ばの状況であると考えられる。
	内部不正に対する具体的な対策や事後対策の選択の難しさ	■ 内部不正対策においては、職場環境の整備や秘密保持義務の順守などの人的・組織的側面が重要であるため、まずは従業員教育に軸足を置き、これでカバーできないところから技術的対策を順次適用していくという優先順位を置くことが有効。
	個人情報以外の重要情報（技術情報・ノウハウ等）の漏えいに対するリスク認識と内部不正対策	■ まず、個人情報以外の重要情報（技術情報・ノウハウ等）を正しく特定・分類できる基準の策定に重点を置き、この課題を克服できれば、後は最新の情報保護基盤ツール、不正警告機能等を適用することで、早期に情報漏えい／内部不正対策を強化できる。
	ニューノーマル等の環境変化によってリスクが高まる内部不正に関する規則・対策	■ エンドポイントの端末機能を制限する対策やクラウドサービスの利用制限等は幅広く実践されていた。 ■ 大企業の取り組みの中に好事例が多い印象を受けた。 テレワークに関しては、大企業で予算が潤沢だからこそゼロトラスト、IRM、DLP等の高度な概念やツールの検討や導入が可能になる。一方、サプライチェーンの内部不正対策では、サプライヤーが世界にまたがるほど広範だからこそ、サプライヤーのレベル分けとレベルに応じた重要情報取り扱い制限の必要性が高まる。またサプライヤーが非常に多いからこそ、サプライヤーに検査ツールを渡し、重要情報の保持状況を自動検査してその結果を確認する必要性が生じる。
	急増する中途退職者／中途採用者の内部不正に対する対策整備	■ 「中途退職者／中途採用者の内部不正に対する対策整備が遅れている」という仮説は必ずしも実態に合っていない。 ■ 中途退職者の急増を受けて秘密保持誓約書を改訂し、運用を見直した企業も見られるように、対策のさらなる強化が求められている状況。 ■ 重要プロジェクト単位で秘密保持義務の誓約書の提出を求める対策はあまり浸透していない。 ■ 中途採用者が他社の重要情報を持ち込むことへの対策については、企業によって少し温度差があった。
	不満を蓄積させず、内部不正を誘発しない職場環境の整備	■ 内部不正を誘発しない職場環境の整備に重点を置いている企業が複数あった。
	内部不正による重要情報の漏えい発覚時に、侵害先にどこまで対応するか	■ 特に言及なし。

5-2. 企業のインタビュー調査からの示唆　～内部不正防止ガイドラインの利用

内部不正防止ガイドラインの利用についての企業インタビュー結果：

- ■ 良く読まれているサイバーセキュリティのガイドラインとの間で相互参照、相関の解説等を行うことで、内部不正防止ガイドラインの認知度が高まるという指摘があった。
- ■ 現状の内部不正防止ガイドラインは必ずしも活用しやすい形態となっておらず、「社内規程に内部不正対策を加筆しやすくすること」、「経営者への説明に活用できるようにすること」、「リテラシー教育にそのまま活かせるコンテンツを追加すること」などが求められていることが分かった。また、継続的な啓発活動（オンライン講演等）が必要だという指摘もあった。

共通の調査軸	仮説に基づく調査項目	得られた示唆
内部不正防止ガイドライン利用の実態	内部不正防止ガイドラインの認知度	■ 情報漏えいに関する内部不正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では、内部不正対策だけに特化したガイドラインは認知されにくいことが懸念される。 ■ 良く読まれているサイバーセキュリティのガイドラインとの間で相互参照、相関の解説等を行うことで、内部不正防止ガイドラインの認知度が高まり、仮説と異なり、活用度合いが高まる。
	内部不正防止ガイドラインの活用	■ 現状の内部不正防止ガイドラインは必ずしも活用しやすい形態となっていないが、次に示すような施策に取り組むことで、この状況を効果的に改善することができる。 • 良く読まれているサイバーセキュリティのガイドラインとの相関を明確に示して社内規程に内部不正対策を加筆しやすくすること • 経営者への説明を意識した概要版を作成すること • リテラシー教育にそのまま活かせるコンテンツを公表すること • 継続的なオンライン講演等の実施等に取り組むこと

5-3. 有識者インタビュー調査からの示唆　～企業・組織で知っておくべき基礎知識

有識者に企業アンケート調査結果を見ていただきながら、現状とあるべき姿の乖離やこれを解消するための対策等について、専門的な知見・見解等をご提示いただいた。その上で得られた調査結果を各調査軸に対応付けて仕分けし、得られた示唆の整理を行った。

企業・組織で知っておくべき基礎知識についての有識者インタビュー結果：

- ■ 法制度の知識を根付かせるためには、従業員一般と主管／担当部署では異なるアプローチを取ることが効果的である。
- ■ 不正競争防止法の営業秘密の制度を従業員一般に周知・教育するためには、してはいけないことを事例で伝えるべき。代替案として、組織で扱う自社情報は全て重要と伝える方法もある。限定提供データ保護制度の知識は、営業秘密保護制度の知識と同時に教育するのが良い。
- ■ 重要情報の漏えいや内部不正の防止に関するガイドラインの効果的な周知方法として、業界単位でのトップダウンアプローチがある。

共通の調査軸	知識の種別	得られた示唆
企業・組織全体として知っておくべき基礎知識の実態	社内規程についての知識	■ 特に言及なし。
	法制度についての知識	■「法制度についての知識が足りない」という状況を改善するためには、従業員一般と主管／担当部署では異なるアプローチを取ることが効果的。 ■ 不正競争防止法の営業秘密の制度を従業員一般に周知・教育するためには、してはいけないことを警告のような形で、事例を交えて伝えるのが良い。また、組織で扱う自社情報は全部重要で勝手に持ち出してはいけないという伝え方をする方が理解されやすい。 ■ 限定提供データについては、営業秘密の保護と同時に取り組むことで、従業員への周知を期待できる。
	関連するガイドライン等についての知識	■ 業界単位でのトップダウンの周知は、「関連するガイドライン等についての知識が足りない」という状況の改善に効果がある。
	情報漏えい／セキュリティリスクに関する知識	■ 特に言及なし。

5-3. 有識者インタビュー調査からの示唆　～内部不正防止に取り組む組織的体制

内部不正防止に取り組む組織的体制についての有識者インタビュー結果：

- ■ 内部不正防止に対する組織全体としての責任・権限の典型的なモデルは、重要情報にアクセスできるITシステム部門が技術・運用等を担当し、リスク管理部門がこれを監督して責任部門となる形態である。
- ■ 経営層が組織全体での内部不正防止への取り組みを牽引することで、マネジメントシステムも十分に機能する。大きな事案を起こす前に、計画的に事前防止やマネジメント確立に取り組むべき。
- ■ 役職の高い人物を特別扱いしない対策に基づくマネジメントシステムが重要。

共通の調査軸	仮説に基づく調査項目	得られた示唆
内部不正防止に取り組む組織的体制の実態	経営層の情報発信	■ 特に言及なし。
	組織全体としての責任・権限の明確化	■ 内部不正防止に対する責任・権限の典型的なモデルは、重要情報にアクセスできるITシステム部門が技術・運用等を担当し、リスク管理部門がこれを監督して責任部門となる形態である。この形態が社会に浸透すれば、「組織全体としての責任・権限が明確に定められていない企業が多い」という状況は改善される。
	社内ポリシー／規定の整備	■ 特に言及なし。
	経営層によるリソースの適切な配分	■ 特に言及なし。
	内部不正対策に関するマネジメントシステム	■ 経営層が組織全体での内部不正防止への取り組みを牽引することで、「内部不正対策に関するマネジメントシステムが十分に機能していない」という状況の改善を期待できる。 ■ 大きな事案が起こってしまった後に内部不正対策に取り組むことが多いが、計画的に事前防止やマネジメントに取り組むことが重要。 ■ 役職の高い人物を特別扱いしない対策に基づくマネジメントシステムが重要。
	テレワークを行う従業員を支援する体制	■ 特になし。

5-3. 有識者インタビュー調査からの示唆　～組織全体への周知・教育

組織全体への周知・教育についての有識者インタビュー結果：

- ■ 一般の職員に対しては、営業秘密の漏えいと不正についての教育を浸透させることがポイント。入社、人事異動、退職等の重要なタイミングで、具体的に重要情報を示し、何をしてはいけないのかを周知徹底すべき。
- ■ 情報システム担当者に対しては、法務・知財担当者が協力して、必要な知識を浸透させることが有効。
- ■ 内部不正対策を組織全体で実践できるようにするためには、社内で発生したインシデント情報を包み隠さず社員に開示する風土を構築することが必要。

共通の調査軸	仮説に基づく調査項目	得られた示唆
組織全体への周知・教育の実態	一般の職員に対する、内部不正対策に関する周知・教育	■「一般の職員に対する、内部不正対策に関する周知・教育は不足している」という状況を改善する上で、営業秘密の漏えいと不正についての教育を浸透させることがポイントとなる。営業秘密については、何をしてはいけないのかを周知徹底すべき。特に、入社、人事異動、退職等の重要なタイミングで、具体的に重要情報を示して教育する必要がある。 ■ 法務・知財担当者を通じて、情報システム担当者に必要な知識を浸透させることも有効。
	内部不正対策を組織全体で実践できる環境	■「内部不正対策を組織全体で実践できる環境」を改善する上で、社内で発生したインシデント情報（原因、重要情報奪取の方法等）を包み隠さず社員に開示する風土を構築することが必要。

5-3. 有識者インタビュー調査からの示唆　～内部不正防止の課題と対策

内部不正防止の課題と対策についての有識者インタビュー結果：

- 経営層の内部不正に対する認識を高めることで、経営リスクや事業リスクとしての内部不正リスクの優先度を上げられる。
- 経営層からの率先した指示に従ってリスクと重要な情報の紐付けを強化し、自社にとって競争力の源泉となる情報を正確に把握して事業リスクを深掘りできる人材を育成し、営業秘密に対して求められる対応を具体的に提示し、他社から受領した営業秘密の侵害を警告することで、個人情報だけでなく営業秘密の漏えいに対する内部不正対策を強化できる。
- サプライチェーンまで含めて企業の内部と捉え直した上でリスク管理対策を進めることで、サプライチェーン全体の内部不正対策を強化できる。
- 急増する中途退職者／中途採用者の内部不正に対する対策を強化するためには、この問題に対する経営層の感度を高めるとともに、経営層に対しても従業員と同様の対策を適用すること、退職者については半年から１年前まで遡って情報システムへのアクセスログを確認すること、他社の重要情報を社内でばらまかないように対策すること、入社時・退社時に加えて重要プロジェクト就任／離任時に秘密保持義務の誓約書を取ること、重要性の高い秘密に触れている人には通常より詳細化した誓約書の文面を用いること等が有効である。

共通の調査軸	仮説に基づく調査項目	得られた示唆
内部不正防止の課題と対策の実態	経営リスクや事業リスクとしての内部不正リスクの優先度	■「経営リスクや事業リスクとしての優先度が高くない」状況を改善するためには、経営層の内部不正に対する認識を高める必要がある。 ■ 現場からのボトムアップでは意識改革は難しく、国や業界団体からのトップダウンアプローチが効果的。
	内部不正に対する具体的な対策や事後対策の選択の難しさ	■「セキュリティ対策等と比較すると、内部不正に対する具体的な対策や事後対策の選択が難しい」という状況を改善するためには、内部不正対策の実施を指示する主管部署とこれを組み込んで運用する情報システム部門の役割分担を促すような組織構造を持たせれば良い。
	個人情報以外の重要情報（技術情報・ノウハウ等）の漏えいに対するリスク認識と内部不正対策	■「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い」という状況は、次のような対応によって改善される。 • 経営層からの率先した指示に従って、リスクと重要な情報の紐付けを強化 • 自社にとって競争力の源泉となる情報を正確に把握し、事業リスクを深掘りできる人材の育成。または外部サポートの積極的な活用 • 個人情報保護法と同じように、営業秘密に対して求められる対応を具体的に提示 • 他社から受領した営業秘密の保護に焦点を当てた啓発活動の推進
	ニューノーマル等の環境変化によってリスクが高まる内部不正に関する規則・対策	■「環境変化（サプライチェーン）への対応が遅れており、リスクが高まる内部不正に関する対策ができていない」と言う状況は、サプライチェーンまで含めて企業の内部と捉え直した上でリスク管理対策を進めることで改善される。
	急増する中途退職者／中途採用者の内部不正に対する対策整備	■「急増する中途退職者／中途採用者の内部不正に対する対策整備が遅れている」という状況を改善するためには、この問題に対する経営層の感度を高めるとともに、次に示す対策を適宜選択して適用すれば良い。 • 経営層に対しても従業員と同じように対策し、例外は認めない。 • 退職者については、辞意を表明してから実際に退職するまでの間だけでなく、半年から1年前まで遡って情報システムへのアクセスログを確認する。 • 転入した従業員が他社の重要情報を社内でばらまかないように、必要な対策を行う。 • 入社時、退社時、重要プロジェクト就任／離任時に秘密保持義務の誓約書を取る。 • 重要性の高い秘密に触れている人については、テンプレートどおりの誓約書をそのまま用いず、誓約書を詳細化する。
	不満を蓄積させず、内部不正を誘発しない職場環境の整備	■ 特に言及なし。
	内部不正による重要情報の漏えい発覚時に、侵害先にどこまで対応するか	■ 特に言及なし。

5-3. 有識者インタビュー調査からの示唆　～内部不正防止ガイドラインの利用

内部不正防止ガイドラインの利用についての有識者インタビュー結果：

- ■ 他の知名度の高い公的文書と内部不正防止ガイドラインの間で相互引用することで、内部不正防止ガイドラインの認知度は改善される。ガイドラインの対象が「重要情報の漏えいに関する内部不正」であることが自明であるようにタイトルを変更することも考えられる。
- ■ 認知に留まらず、内部不正防止ガイドラインの利用を促進するためには、内容の改訂、活用するためのツールや好事例の整備、活用して取り組みを始めるまでのサポート体制の整備等について検討することが望ましい。

共通の調査軸	仮説に基づく調査項目	得られた示唆
内部不正防止ガイドライン利用の実態	内部不正防止ガイドラインの認知度	■「内部不正防止ガイドラインはあまり知られていない」という状況は、他の知名度の高い公的文書と内部不正防止ガイドラインの間で相互引用することで、改善される。 ■ 内部不正防止ガイドラインの対象が「重要情報の漏えいに関する内部不正」であることが自明であるようにタイトルを変更することも考えられる。
	内部不正防止ガイドラインの活用	■ 仮説が示す「内部不正ガイドラインが認知されていても活用されていない」という状況を改善するため、内容の改訂、活用するためのツールや好事例の整備、活用して取り組みを始めるまでのサポート体制の整備等について検討していく必要がある。 • 提供先において重要な情報・データの利用目的や期間の管理を行うことが重要になるので、資産の授受における契約関係を記載しても良い。 • サイバーセキュリティ経営ガイドラインの付録にあるようなツールを整備することも考えられる。 • 先進的な取り組みをしている企業を選定し、その取り組みを分析した上で、良い取り組みを他社に広げていくのが良い。 • 専門家を派遣して現場で指導し、その際に内部不正防止ガイドラインを活用して企業の取り組みをレベルアップさせる仕組みを作る等の対応も考えられる。一度取り組みを始めるまでのサポートができる体制があれば、より多くの企業に参考にしてもらえるはずである。

6．調査結果の分析
6-1. 企業アンケート調査のクロス集計による分析（1/14）

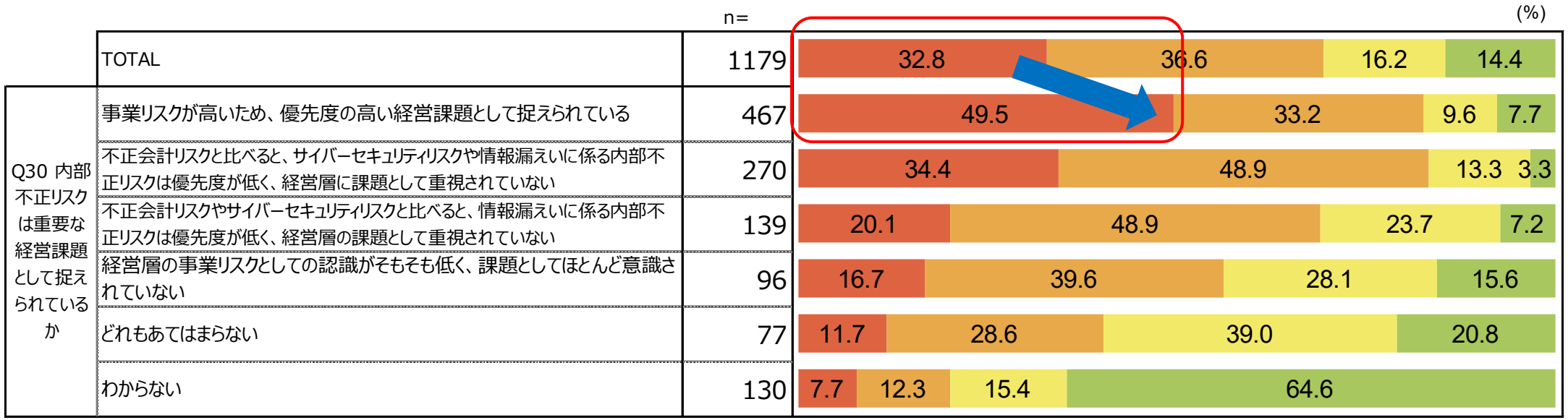
「内部不正リスクを重要な経営課題として捉えているか」「常用雇用者数」「回答者の担当業務（経営層を含む）」等を軸としてクロス集計を行い、その結果を分析した。

内部不正リスクを重要な経営課題として捉えている企業では、組織全体及び担当部署での情報漏えい／セキュリティリスクに関する知識の習得が明らかに進んでいる。

Q15 貴社では、次にあげる情報漏えいリスク／セキュリティリスクは組織全体で知られていますか。

（例）

＜退職者を通じた自社の重要情報の漏えい／中途採用者を通じた他社の重要情報の混入＞



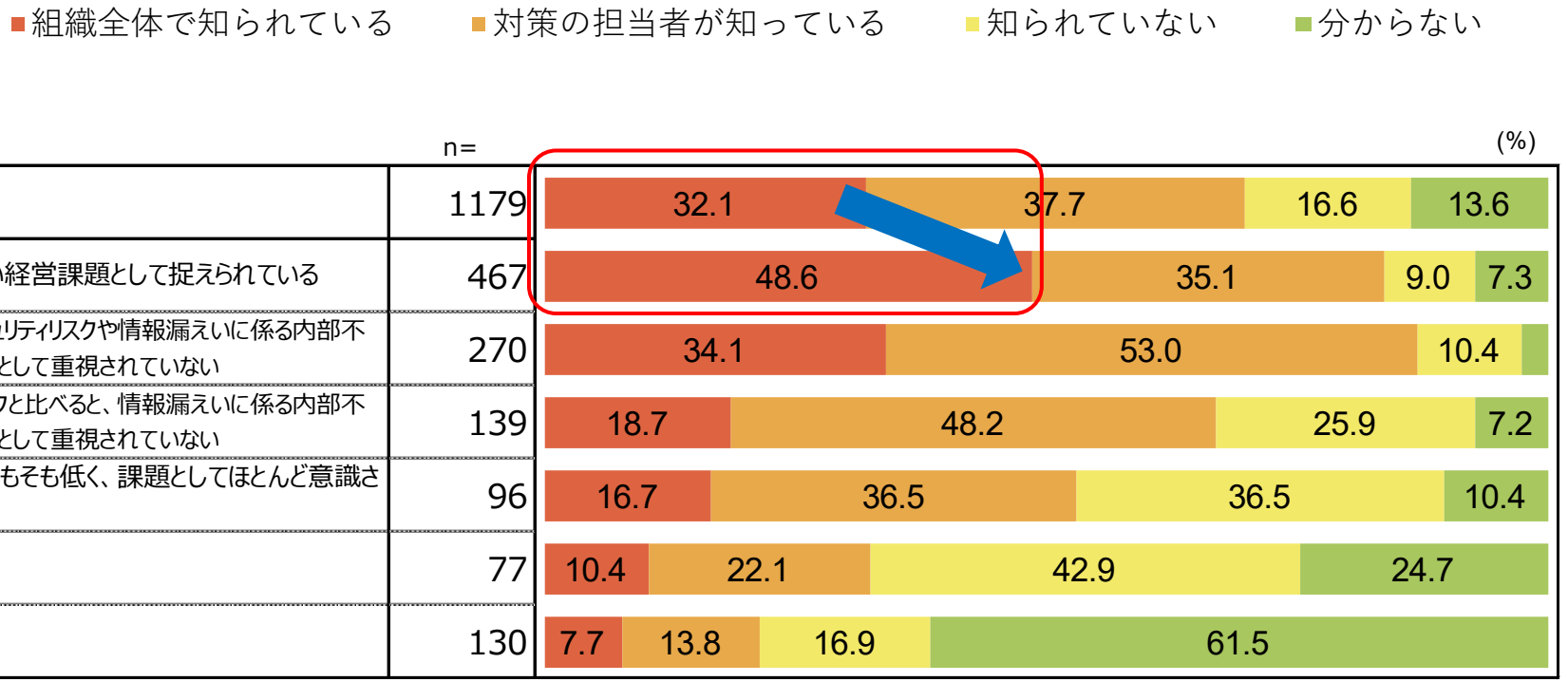
6．調査結果の分析
6-1. 企業アンケート調査のクロス集計による分析（2/14）

内部不正リスクを重要な経営課題として捉えている企業では、テレワーク中のセキュリティ対策が徹底されないことで生じるリスクに関する知識が明らかに浸透している。

Q15 貴社では、次にあげる情報漏えいリスク／セキュリティリスクは組織全体で知られていますか。

（例）

<テレワークの不十分なセキュリティガバナンス>



6-1. 企業アンケート調査のクロス集計による分析（3/14）

内部不正リスクを重要な経営課題として捉えている企業は、ほぼすべての内容に対してリテラシー教育を提供している割合が高くなっているが、特に重要情報の分類と表示に関する規則と個人情報保護法の法制度に関する知識について教育している割合が70%を超えている点は注目される。他方で、営業秘密保護の法制度に関する知識を教育する割合は54%に留まっており、一層の底上げが期待される。

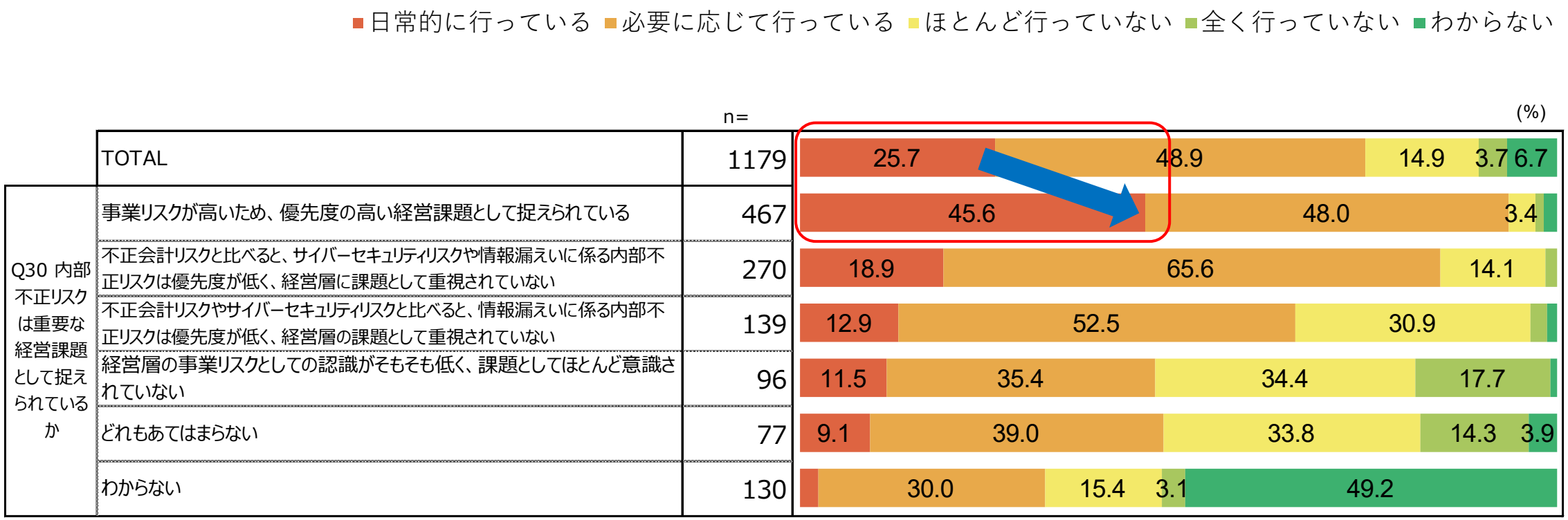
Q27 貴社では内部不正防止についての従業員へのリテラシー教育において、具体的にどのような内容を周知・教育していますか。

		n=	重要情報の分類と表示に関する規則	個人情報保護の法制度に関する知識	営業秘密保護の法制度に関する知識	限定提供データ保護の法制度に関する知識	機微技術情報の管理に関する外為法についての知識	クラウド利用許可に関する規則	BYOD（個人所有PC／デバイスの業務利用）の使用規則	テレワークに関する内部規則や関連法令	モニタリングやログ記録・分析等によって、組織が善良な従業員を守るという経営方針	中途退職時の重要情報漏えいに対する抑止的な周知・教育	中途採用者が他社の重要情報を持ち込めないようにするための確認ルール	外国政府が関与する重要技術情報に対する産業スパイの典型的手口の知識	発生した内部不正事件の情報、分析結果等（手口、脆弱性、損害、取り得る対策等）	どれもあてはまらない	わからない
	TOTAL	948	57.1	66.1	47.2	31.6	27.3	21.2	21.4	25.7	19.4	24.3	22.0	14.8	22.3	1.4	1.5
Q30 内部不正リスクは重要な経営課題として捉えられているか	事業リスクが高いため、優先度の高い経営課題として捉えられている	453	72.4	76.6	54.1	37.3	34.7	26.0	32.2	34.7	28.0	33.6	28.3	17.9	32.2	0.7	1.3
	不正会計リスクと比べると、サイバーセキュリティリスクや情報漏えいに係る内部不正リスクは優先度が低く、経営層に課題として重視されていない	253	45.1	56.1	42.3	30.0	21.3	17.0	11.1	16.6	12.6	13.8	17.0	13.0	12.6	0.4	0.4
	不正会計リスクやサイバーセキュリティリスクと比べると、情報漏えいに係る内部不正リスクは優先度が低く、経営層の課題として重視されていない	121	38.0	53.7	40.5	26.4	25.6	17.4	9.9	15.7	9.1	12.4	14.0	10.7	8.3	0.0	0.0
	経営層の事業リスクとしての認識がそもそも低く、課題としてほとんど意識されていない	55	45.5	58.2	38.2	21.8	16.4	14.5	9.1	20.0	12.7	21.8	18.2	10.9	14.5	9.1	0.0
	どれもあてはまらない	34	38.2	58.8	47.1	26.5	17.6	20.6	23.5	29.4	14.7	38.2	29.4	14.7	32.4	8.8	5.9
	わからない	32	46.9	65.6	28.1	6.3	6.3	12.5	12.5	15.6	6.3	9.4	3.1	6.3	12.5	3.1	15.6

6-1. 企業アンケート調査のクロス集計による分析（4/14）

内部不正リスクを重要な経営課題として捉えている企業では、経営層が日常的に内部不正防止の取組み方針等を全従業員に周知、指示しているという回答が明らかに増えている。

Q18 経営層は、組織全体での内部不正防止の取組み方針等について、全従業員に周知、指示していますか。



6-1. 企業アンケート調査のクロス集計による分析（5/14）

内部不正リスクを重要な経営課題として捉えている企業では、指針や規定を定めている割合がほぼ全般に亘って10%以上底上げされている。

Q13 貴社では内部不正防止について、どのような指針や規則が定められていますか。

		n=	内部不正防止だけで独立した基本方針（内部統制の基本方針やセキュリティポリシーには含まれていない）	内部統制の基本方針（内部不正防止の基本方針を含む）	セキュリティポリシー（内部不正防止の基本方針を含む）	就業規則に書かれた内部不正防止に関するルール	組織全体に適用される重要情報の分類規則	秘密として管理する意思を明確に伝えるための、重要情報の表示規則	組織全体に適用される重要情報の分離保管規則	個人情報管理のための規則	営業秘密管理のための規則	限定提供データの管理のための規則	テレワーク時のセキュリティ管理規則（端末／ネットワーク利用、リモートアクセス等）	テレワーク時のクラウドサービス利用規則（利用可能サービス、取扱い可能な重要情報等）	中途退職者の秘密漏えい、中途採用者による他社の秘密持ち込みを防止するための規則	情報漏えい／セキュリティ監視システム適用にあたっての、従業員のプライバシー保護規則	どれもあてはまらない	わからない
	TOTAL	1179	33.3	45.7	47.2	42.2	26.0	20.5	17.3	36.9	23.8	16.8	25.9	19.0	23.0	23.3	3.1	7.2
Q30 内部不正リスクは重要な経営課題として捉えられているか	事業リスクが高いため、優先度の高い経営課題として捉えられている	467	48.2	60.6	59.7	55.7	39.2	32.8	28.9	52.0	39.4	26.1	37.9	28.1	34.5	37.9	0.6	1.1
	不正会計リスクと比べると、サイバーセキュリティリスクや情報漏えいに係る内部不正リスクは優先度が低く、経営層に課題として重視されていない	270	33.3	45.6	49.3	33.7	20.0	15.6	11.1	23.7	13.0	12.6	19.3	17.0	17.8	14.1	0.0	1.1
	不正会計リスクやサイバーセキュリティリスクと比べると、情報漏えいに係る内部不正リスクは優先度が低く、経営層の課題として重視されていない	139	26.6	46.0	43.9	38.1	23.0	16.5	15.1	27.3	15.1	13.7	24.5	15.8	13.7	18.7	0.0	1.4
	経営層の事業リスクとしての認識がそもそも低く、課題としてほとんど意識されていない	96	20.8	26.0	31.3	40.6	15.6	11.5	8.3	35.4	20.8	12.5	12.5	11.5	20.8	12.5	11.5	4.2
	どれもあてはまらない	77	10.4	29.9	31.2	37.7	13.0	10.4	7.8	32.5	13.0	7.8	22.1	9.1	13.0	10.4	20.8	3.9
	わからない	130	10.0	16.2	22.3	20.0	10.0	3.8	3.1	23.8	8.5	3.8	10.0	5.4	10.0	10.8	4.6	52.3

6-1. 企業アンケート調査のクロス集計による分析（6/14）

内部不正リスクを重要な経営課題として捉えている企業においては、ほぼ全部の対策に亘って、あきらかに内部不正対策を実施している割合が高まっている。

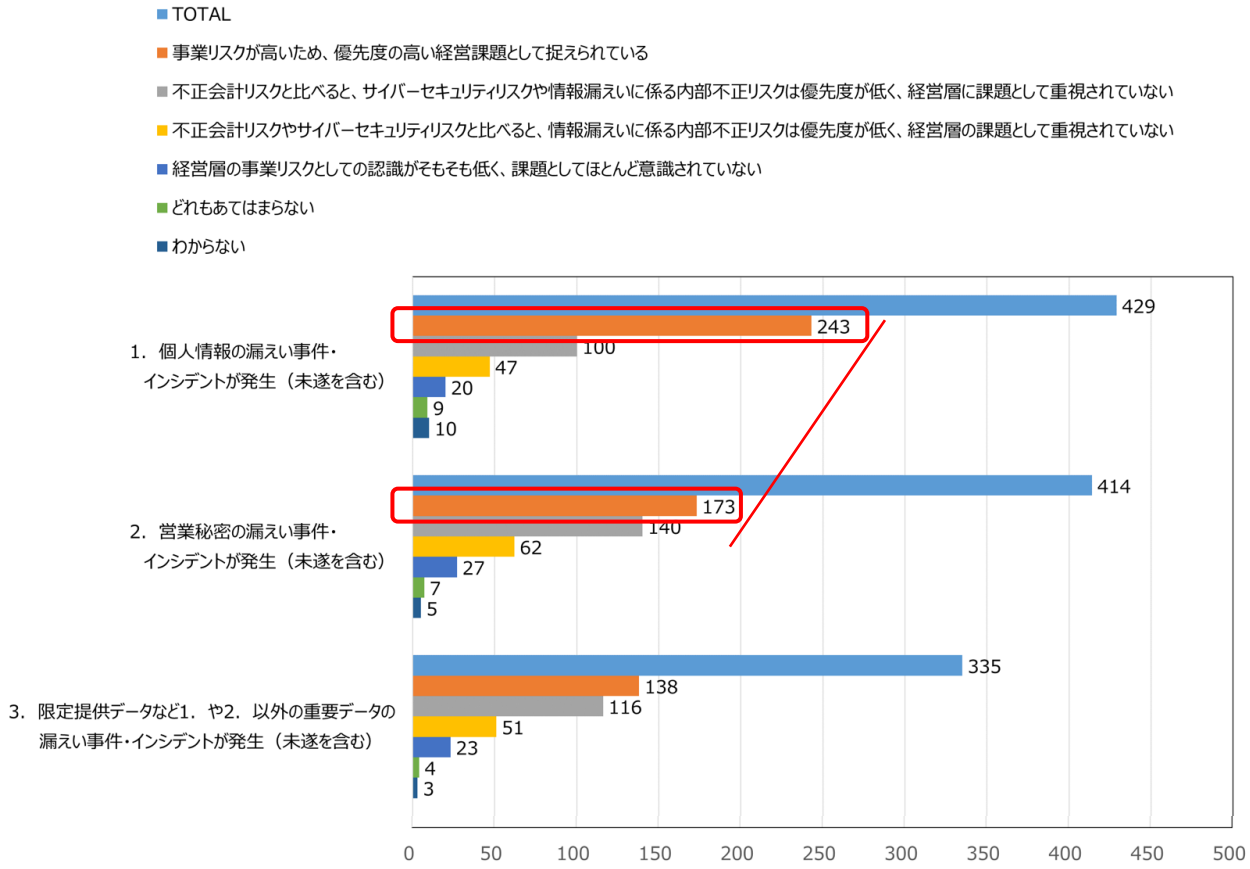
Q12 重要情報の漏えいに関する内部不正を防止するために、貴社では次のどの対策を実施していますか。

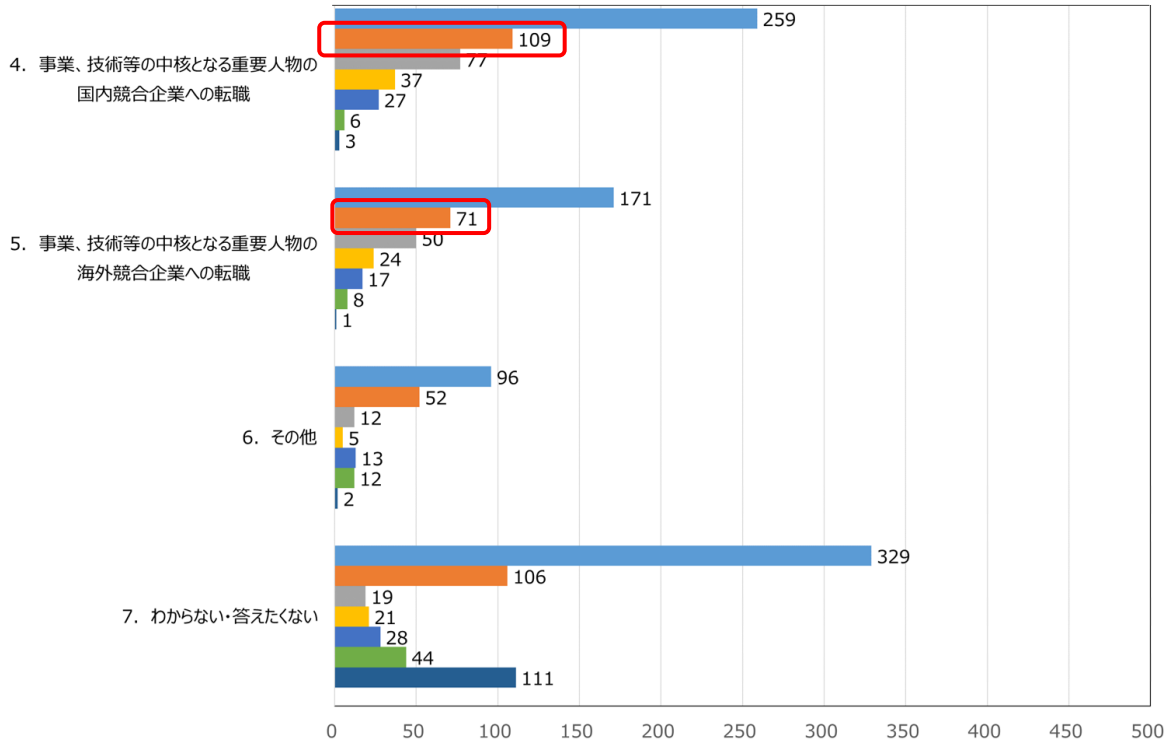
		n=	経営層（全社責任者を含む）が内部不正対策の基本方針を定め、社外に示し、組織内で周知徹底している	経営層（全社責任者を含む）は内部不正対策の実施にあたり、従業員とそのプライバシー保護を明言している	経営層（全社責任者を含む）が自ら定めた基本方針に基づき、必要なリソース確保のための決定・指示をしている	経営層（全社責任者を含む）は重要情報と判断する範囲や条件を明確に定め、組織全体に周知徹底している	内部不正対策に関し、組織全体における責任部門・責任者が明確に定められている	内部不正防止の責任者は、（1）サイバーセキュリティ対策の責任者、または（2）リスク管理部門／コンプライアンス部門等の責任者が兼ねる	内部不正防止のリテラシー向上のため、定期的または事故発生時に組織全体に教育を実施している	テレワーク実施者に対し、社内規程や関連法規の教育を実施し、理解度を確認している	採用時や退職時だけでなく、異動時、昇進時、新プロジェクトへの参加時・終了時などに秘密保持義務契約の締結（または誓約書の提出）を求めている	営業や技術の中核となる重要人物が退職する場合は、退職が決まった段階で、重要情報へのアクセスの監視及びアクセスログの確認等を強化している	退職後には速やかに退職者のID、重要情報へのアクセス権限、テレワークでの社内ネットワークへのアクセス権限等を削除している	従業員に不満が蓄積しないように、労務管理、人事管理、職場やテレワークにおける良好で十分なコミュニケーションの確保等について、必要な対策を講じている	ID管理と本人確認（認証）を強化している	重要情報を含む電子文書は、容易に判別できるようにしている	重要情報には必要最小限の従業員しかアクセスできないように管理している	重要情報は定期的に棚卸しを行い、不要なものを消去している	入退室管理やPC・デバイスの社外持出し管理を実施している	BYOD（個人デバイスの業務利用）は許可していない	重要情報に対するアクセス監視、ログ記録等を実施し、それを組織全体に周知している	公的機関のガイドライン等に従って、会社支給PCのテレワーク対策が強化されている	テレワークで扱える重要情報の範囲をルール化している	業務で使用できるクラウドや、クラウド上で扱える重要情報の範囲をルール化している	サプライヤーや委託先等との重要情報の受渡しを厳格に管理し、暗号化している	サプライヤーや委託先等の重要情報漏えい対策を、契約時及び契約中に確認している	内部不正発覚後の事後対策や、事業継続についてマニュアル化している	組織内外で内部不正事故が起こった場合、事故について組織内部で共有し、内部不正の心理的抑止に役立てている	どれもあてはまらない
	TOTAL	1179	49.0	34.7	33.2	29.7	42.1	27.7	41.8	21.3	28.4	19.8	32.7	32.5	35.5	18.4	30.4	19.8	35.0	21.1	31.4	21.4	19.7	22.9	15.9	17.6	35.3	29.0	9.6
Q30 内部不正リスクは重要な経営課題として捉えられているか	事業リスクが高いため、優先度の高い経営課題として捉えられている	467	73.4	44.5	44.8	41.1	63.4	35.8	62.7	28.5	39.4	27.8	47.5	52.0	55.0	30.0	46.0	33.0	53.7	34.3	49.3	33.4	30.4	35.3	28.7	28.1	52.5	39.0	1.1
	不正会計リスクと比べると、サイバーセキュリティリスクや情報漏えいに係る内部不正リスクは優先度が低く、経営層に課題として重視されていない	270	45.2	34.1	33.7	23.7	32.2	21.1	30.0	16.7	26.3	20.4	20.0	23.3	24.8	11.9	17.0	11.9	24.4	10.0	21.1	15.6	14.1	12.6	9.6	12.2	28.1	23.7	1.5
	不正会計リスクやサイバーセキュリティリスクと比べると、情報漏えいに係る内部不正リスクは優先度が低く、経営層の課題として重視されていない	139	34.5	38.1	29.5	27.3	29.5	33.1	33.8	18.7	25.2	15.1	26.6	20.1	26.6	17.3	18.7	7.9	20.9	12.9	20.1	17.3	14.4	23.7	7.9	13.7	25.2	23.7	1.4
	経営層の事業リスクとしての認識がそもそも低く、課題としてほとんど意識されていない	96	22.9	21.9	20.8	16.7	26.0	22.9	33.3	15.6	21.9	12.5	30.2	20.8	19.8	9.4	31.3	9.4	19.8	13.5	25.0	10.4	10.4	9.4	5.2	9.4	31.3	26.0	17.7
	どれもあてはまらない	77	23.4	24.7	20.8	22.1	29.9	18.2	20.8	18.2	16.9	9.1	26.0	15.6	19.5	6.5	19.5	13.0	20.8	14.3	14.3	9.1	11.7	18.2	9.1	11.7	10.4	20.8	29.9
	わからない	130	19.2	12.3	11.5	17.7	18.5	16.2	18.5	13.8	8.5	6.9	18.5	13.1	18.5	5.4	20.0	13.8	24.6	15.4	15.4	10.0	10.0	11.5	3.1	5.4	16.9	16.9	47.7

6-1. 企業アンケート調査のクロス集計による分析（7/14）

個人情報の漏えい事案／インシデントを経験した企業では、内部不正リスクを重要な経営課題として捉えている割合が顕著に増えている。他方で、営業秘密の漏えい事案／インシデントや事業／技術の中核人材の国内競合企業への転職を経験した企業では、内部不正リスクを重要な経営課題として捉えている割合がそれほど増えていない。

Q30 貴社では、内部不正リスクは重要な経営課題として捉えられていますか。





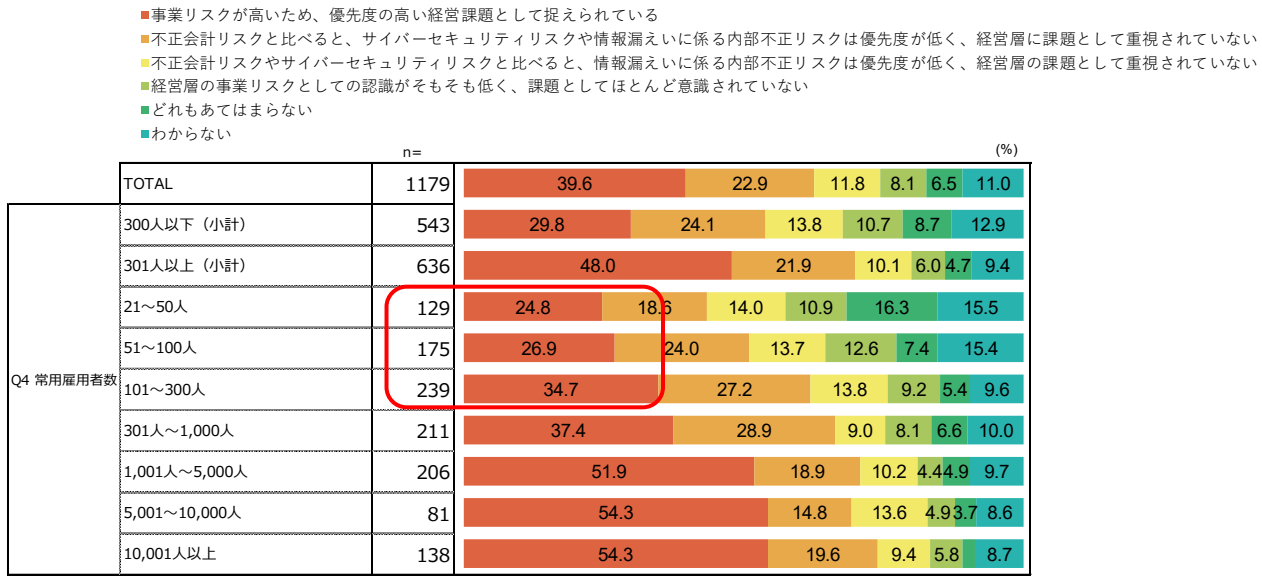
6-1. 企業アンケート調査のクロス集計による分析（8/14）

内部不正リスクを優先度の高い経営課題として捉えている割合は、企業規模が小さくなるにつれて減少していく。中小企業は内部不正事案／それが強く疑われる事態をあまり認識できておらず、これが意識の差として表れている可能性がある。

Q25 貴社では、内部不正事件の発生、またはそれが強く疑われる事態を経験したことがありますか。

		n=	1. 個人情報の漏えい事件・インシデントが発生（未遂を含む）	2. 営業秘密の漏えい事件・インシデントが発生（未遂を含む）	3. 限定提供データなど1. や2. 以外の重要データの漏えい事件・インシデントが発生（未遂を含む）	4. 事業、技術等の中核となる重要人物の国内競合企業への転職	5. 事業、技術等の中核となる重要人物の海外競合企業への転職	6. その他	7. わからない・答えたくない
	TOTAL	1179	36.4	35.1	28.4	22.0	14.5	8.1	27.9
Q4 常用雇用者数	300人以下（小計）	543	26.2	30.0	24.1	18.4	11.4	9.9	31.1
	301人以上（小計）	636	45.1	39.5	32.1	25.0	17.1	6.6	25.2
	21～50人	129	20.9	24.8	13.2	12.4	6.2	11.6	38.0
	51～100人	175	27.4	28.6	25.1	19.4	14.3	8.6	29.1
	101～300人	239	28.0	33.9	29.3	20.9	12.1	10.0	28.9
	301人～1,000人	211	38.4	35.5	32.7	24.6	15.6	6.6	26.1
	1,001人～5,000人	206	44.2	36.4	25.2	19.4	14.1	6.3	33.5
	5,001～10,000人	81	49.4	39.5	33.3	29.6	18.5	4.9	17.3
	10,001人以上	138	54.3	50.0	40.6	31.2	23.2	8.0	15.9

Q30 貴社では、内部不正リスクは重要な経営課題として捉えられていますか。



6-1. 企業アンケート調査のクロス集計による分析（9/14）

常用雇用者数が1,000人を超える大企業においては「個人情報だけでなく重要技術情報・ノウハウ、重要データにも対応できている」を選択した企業の割合が30%を超えており、個人情報以外の重要情報に対応できている企業が多い。一方、中小企業では個人情報以外の重要情報に対応できている企業は20%に満たず、底上げが強く求められる状況である。

Q32 貴社では、内部不正防止への取組みにあたり、重要情報が多様化していることに対応できていますか。

		n=	個人情報だけでなく、重要技術情報・ノウハウ、重要データにも対応できている	個人情報以外の重要情報（重要技術情報・ノウハウ、重要データ）を十分に特定・分類できていないため、うまく対応できていない	脅威やリスクが異なるため、重要技術情報・ノウハウや重要データにはうまく対応できていない	対応する法制度が異なるため、重要技術情報・ノウハウや重要データにはうまく対応できていない	重要データについては共有・利活用の知識や経験値が不足しており、うまく対応できていない	どれもあてはまらない	わからない
	TOTAL	1179	27.0	31.5	23.2	15.9	11.2	6.3	12.0
Q4 常用雇用者数	300人以下（小計）	543	18.4	33.5	25.2	18.0	14.0	6.3	12.9
	301人以上（小計）	636	34.3	29.7	21.4	14.0	8.8	6.3	11.3
	21～50人	129	17.1	26.4	14.0	15.5	16.3	12.4	15.5
	51～100人	175	17.7	35.4	28.0	18.3	14.3	5.7	12.6
	101～300人	239	19.7	36.0	29.3	19.2	12.6	3.3	11.7
	301人～1,000人	211	28.4	33.2	24.2	15.6	11.8	8.1	11.8
	1,001人～5,000人	206	38.3	25.7	18.9	8.3	6.8	7.3	10.7
	5,001～10,000人	81	33.3	32.1	27.2	18.5	11.1	4.9	9.9
	10,001人以上	138	37.7	29.0	17.4	17.4	5.8	2.9	12.3

6-1. 企業アンケート調査のクロス集計による分析（10/14）

中小企業は大企業と比べると、全般に亘って内部不正防止対策を実施している割合が低くなっており、一層の啓発が必要である。またこの現状は、内部不正リスクを優先度の高い経営課題として捉えている中小企業の割合が低いことと相関があるものと考えられる。

Q12 重要情報の漏えいに関する内部不正を防止するために、貴社では次のどの対策を実施していますか。

		n=	経営層（全社責任者を含む）が内部不正対策の基本方針を定め、社外に示し、組織内で周知徹底している	経営層（全社責任者を含む）は内部不正対策の実施にあたり、従業員とそのプライバシー保護を明言している	経営層（全社責任者を含む）が自ら定めた基本方針に基づき、必要なリソース確保のための決定・指示をしている	経営層（全社責任者を含む）は重要情報と判断する範囲や条件を明確に定め、組織全体に周知徹底している	内部不正対策に関し、組織全体における責任部門・責任者が明確に定められている	内部不正防止の責任者は、（1）サイバーセキュリティ対策の責任者、または（2）リスク管理部門／コンプライアンス部門等の責任者が兼ねる	内部不正防止のリテラシー向上のため、定期的または事故発生時に組織全体に教育を実施している	テレワーク実施者に対し、社内規程や関連法規の教育を実施し、理解度を確認している	採用時や退職時だけでなく、異動時、昇進時、新プロジェクトへの参加時・終了時などに秘密保持義務契約の締結（または誓約書の提出）を求めている	営業や技術の中核となる重要人物が退職する場合は、退職が決まった段階で、重要情報へのアクセスの監視及びアクセスログの確認等を強化している	退職後には速やかに退職者のID、重要情報へのアクセス権限、テレワークでの社内ネットワークへのアクセス権限等を削除している	従業員に不満が蓄積しないように、労務管理、人事管理、職場やテレワークにおける良好で十分なコミュニケーションの確保等について、必要な対策を講じている	ID管理と本人確認（認証）を強化している	重要情報を含む電子文書は、容易に判別できるようにしている	重要情報には必要最小限の従業員しかアクセスできないように管理している	重要情報は定期的に棚卸しを行い、不要なものを消去している	入退室管理やPC・デバイスの社外持出し管理を実施している	BYOD（個人デバイスの業務利用）は許可していない	重要情報に対するアクセス監視、ログ記録等を実施し、それを組織全体に周知している	公的機関のガイドライン等に従って、会社支給PCのテレワーク対策が強化されている	テレワークで扱える重要情報の範囲をルール化している	業務で使用できるクラウドや、クラウド上で扱える重要情報の範囲をルール化している	サプライヤーや委託先等との重要情報の受渡しを厳格に管理し、暗号化している	サプライヤーや委託先等の重要情報漏えい対策を、契約時及び契約中に確認している	内部不正発覚後の事後対策や、事業継続についてマニュアル化している	組織内外で内部不正事故が起こった場合、事故について組織内部で共有し、内部不正の心理的抑止に役立てている	どれもあてはまらない
	TOTAL	1179	49.0	34.7	33.2	29.7	42.1	27.7	41.8	21.3	28.4	19.8	32.7	32.5	35.5	18.4	30.4	19.8	35.0	21.1	31.4	21.4	19.7	22.9	15.9	17.6	35.3	29.0	9.6
Q4 常用雇用者数	300人以下（小計）	543	38.9	28.9	27.8	26.5	33.9	23.9	34.6	16.6	21.7	13.6	28.5	26.3	26.7	12.7	24.7	14.0	26.5	15.5	22.3	13.4	12.5	16.6	8.8	12.5	27.4	23.9	12.3
	301人以上（小計）	636	57.7	39.6	37.9	32.4	49.1	31.0	48.0	25.3	34.1	25.2	36.3	37.7	43.1	23.3	35.2	24.8	42.3	25.9	39.2	28.1	25.8	28.3	21.9	22.0	42.0	33.3	7.2
	21～50人	129	31.8	24.8	20.2	23.3	27.1	11.6	20.2	16.3	18.6	8.5	23.3	22.5	17.1	6.2	16.3	10.1	14.7	14.7	11.6	10.1	11.6	13.2	4.7	11.6	17.8	15.5	17.8
	51～100人	175	36.0	23.4	25.7	26.9	33.7	27.4	35.4	16.0	19.4	11.4	28.6	26.9	26.9	14.9	25.7	15.4	25.1	10.9	21.1	9.1	10.3	17.7	6.9	9.7	26.3	25.1	13.7
	101～300人	239	44.8	35.1	33.5	28.0	37.7	28.0	41.8	17.2	25.1	18.0	31.4	28.0	31.8	14.6	28.5	15.1	33.9	19.2	28.9	18.4	14.6	17.6	12.6	15.1	33.5	27.6	8.4
	301人～1,000人	211	51.2	40.3	36.5	30.3	43.1	28.4	40.8	18.0	33.2	23.2	35.5	32.2	38.9	22.3	32.7	20.4	40.3	19.9	35.5	25.6	22.3	25.1	17.5	16.1	36.5	29.9	8.1
	1,001人～5,000人	206	58.3	35.4	33.5	27.7	49.5	30.1	50.5	24.3	33.0	24.3	34.5	40.8	44.2	17.0	33.5	19.4	42.7	26.2	37.4	23.3	22.3	26.2	20.4	21.4	41.3	30.1	8.7
	5,001～10,000人	81	64.2	42.0	48.1	39.5	61.7	28.4	53.1	33.3	39.5	27.2	45.7	42.0	50.6	33.3	43.2	34.6	51.9	37.0	46.9	38.3	30.9	37.0	22.2	29.6	54.3	42.0	3.7
	10,001人以上	138	63.0	43.5	40.6	38.4	50.0	37.7	52.2	33.3	34.1	28.3	34.8	39.1	43.5	28.3	37.0	34.1	39.1	28.3	42.8	33.3	33.3	31.2	30.4	27.5	44.2	38.4	5.8

6-1. 企業アンケート調査のクロス集計による分析（11/14）

常用雇用者数が1,000人を超える企業では、秘密保持義務契約の締結に関する対策が50%を超えており、対策実施が進んでいる 。他方で、中小企業による対策への取り組みは遅れており、さらなる啓発が必要である。中途採用者に他社の重要情報を持ち込ませないためのルール作りについても同様の傾向である。離職が決定した後離職するまでの間重要情報へのアクセス監視等を強化するルールを定めている企業の割合は、常用雇用者数が5,000人を超える企業から増加しており、10,000人を超える企業では40%を超えているが、中小企業による取り組みは遅れている。

Q37 貴社では、雇用の流動化を踏まえて、中途退職者に課す秘密保持義務の実効性を高める対策を実施していますか。

		n=	退職時だけでなく、就職時、異動時、昇格時、新プロジェクトへの配属時・終了時等に、秘密保持義務契約の締結（または誓約書の提出）を求めている	秘密保持義務契約の締結（または誓約書の提出）についての内部規則を定め、就業規則でその順守を求めている	就業規則に退職後の定めを規定している	秘密保持義務の有効期間を十分長く設定している	秘密保持義務の対象となる重要情報の範囲・内容を明確に定めている	その他	実施していない	わからない
	TOTAL	1179	39.6	49.6	40.1	25.9	23.9	2.2	7.0	10.7
Q4 常用雇用者数	300人以下（小計）	543	30.2	45.5	36.8	21.2	18.8	1.7	9.0	11.4
	301人以上（小計）	636	47.6	53.1	42.9	29.9	28.3	2.7	5.2	10.1
	21～50人	129	22.5	39.5	28.7	14.7	11.6	2.3	15.5	14.0
	51～100人	175	31.4	47.4	37.7	21.1	17.7	1.7	6.9	13.1
	101～300人	239	33.5	47.3	40.6	24.7	23.4	1.3	7.1	8.8
	301人～1,000人	211	42.7	51.7	40.8	28.4	28.4	1.9	5.7	10.4
	1,001人～5,000人	206	48.1	50.5	43.2	30.1	25.2	1.5	7.8	9.7
	5,001～10,000人	81	51.9	55.6	48.1	28.4	29.6	1.2	3.7	11.1
	10,001人以上	138	52.2	58.0	42.8	32.6	31.9	6.5	1.4	9.4

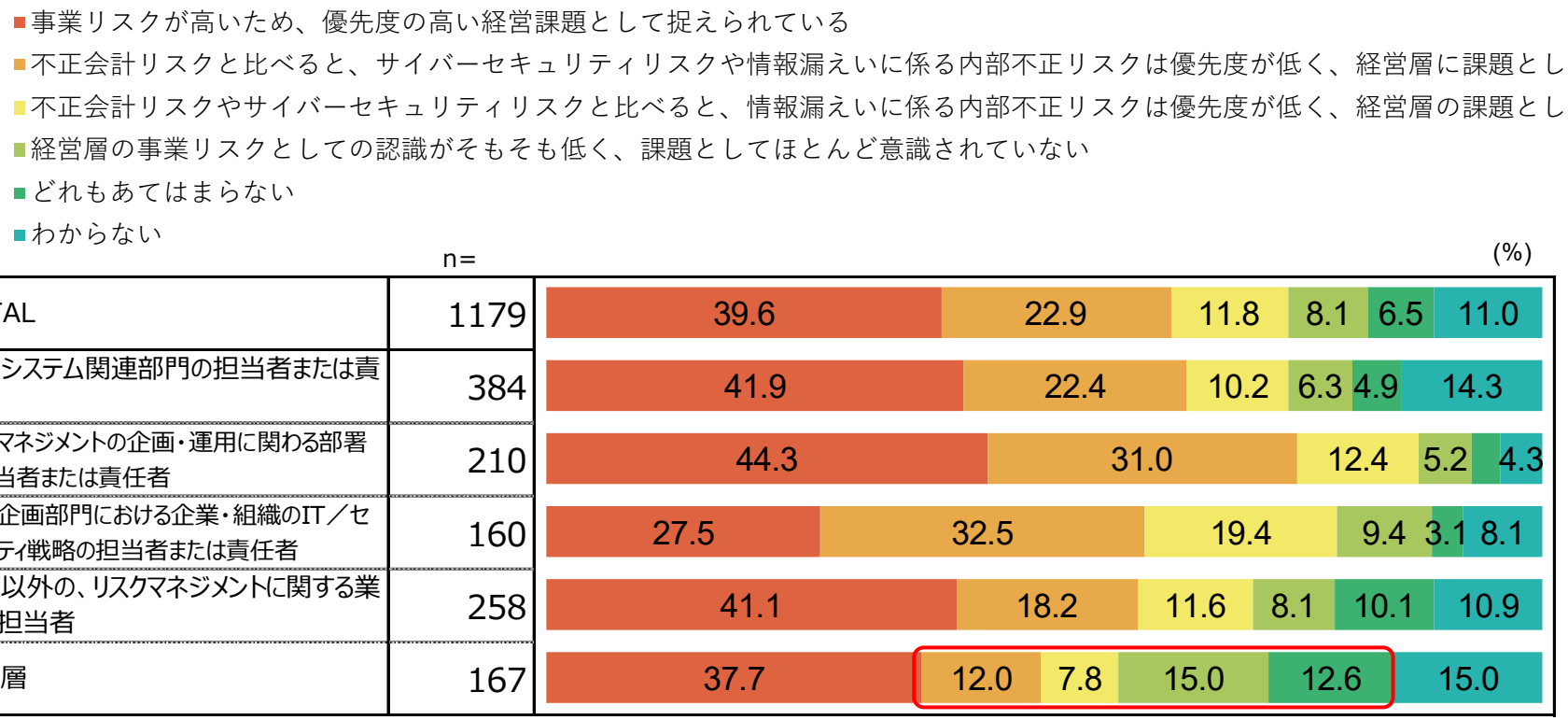
Q38 貴社では、社内規程において採用時と離職時の不正防止に関する規則を規定していますか。

		n=	中途採用時に他社の個人情報、営業秘密、限定提供データ等の重要情報を持ち込まないように、誓約書の提出を規定している	中途採用者による他社の重要情報の持ち込みが発生しないように、私物の記録媒体や許可されていないオンラインストレージの使用を禁止あるいは監視するよう規定している	中途採用者による重要情報の持ち込みを抑止するため、周知・教育を通じて中途採用者に注意喚起することを規定している	離職が決定した後離職するまでの間に重要情報の不正な持ち出しが発生しないように、重要情報へのアクセス等の監視強化を規定している	離職時の重要情報持ち出しを抑止するため、周知・教育を通じて中途退職者に注意喚起することを規定している	その他	規定していない	わからない
	TOTAL	1179	37.2	41.3	33.0	28.7	24.3	1.4	9.2	14.9
Q4 常用雇用者数	300人以下（小計）	543	29.3	35.5	27.4	23.4	19.9	1.3	12.2	15.8
	301人以上（小計）	636	44.0	46.2	37.7	33.2	28.1	1.6	6.6	14.2
	21～50人	129	21.7	31.0	19.4	17.1	17.1	2.3	20.2	16.3
	51～100人	175	32.6	37.1	22.9	25.1	26.9	0.0	7.4	17.7
	101～300人	239	31.0	36.8	35.1	25.5	16.3	1.7	11.3	14.2
	301人～1,000人	211	39.3	42.7	38.9	30.8	24.2	1.4	10.4	13.3
	1,001人～5,000人	206	47.6	42.2	35.9	28.2	24.8	1.9	7.3	15.5
	5,001～10,000人	81	48.1	46.9	39.5	34.6	32.1	1.2	3.7	17.3
	10,001人以上	138	43.5	57.2	37.7	43.5	37.0	1.4	1.4	11.6

6-1. 企業アンケート調査のクロス集計による分析（12/14）

経営層に焦点を当てると、「不正会計リスクと比べ、サイバーセキュリティリスクや情報漏えいに係る内部不正リスクは優先度が低く、経営層に課題として重視されていない」や「不正会計リスクやサイバーセキュリティリスクと比べると、情報漏えいに係る内部不正リスクは優先度が低く、経営層の課題として重視されていない」を選択した割合がかなり減り、「経営層の事業リスクとしての認識がそもそも低く、課題としてほとんど認識されていない」や「分からない」を選択した割合がある程度増えている。この調査結果は、「内部不正リスクを優先度の高い経営課題と捉えている経営層」と「経営課題としてほとんど意識していない経営層」にはっきりと分かれる傾向があることを示唆している。内部不正リスクを課題としてほとんど認識していない経営層に、はっきりと優先度の高い経営課題であると捉えてもらうための意識変革を促す施策が求められている。

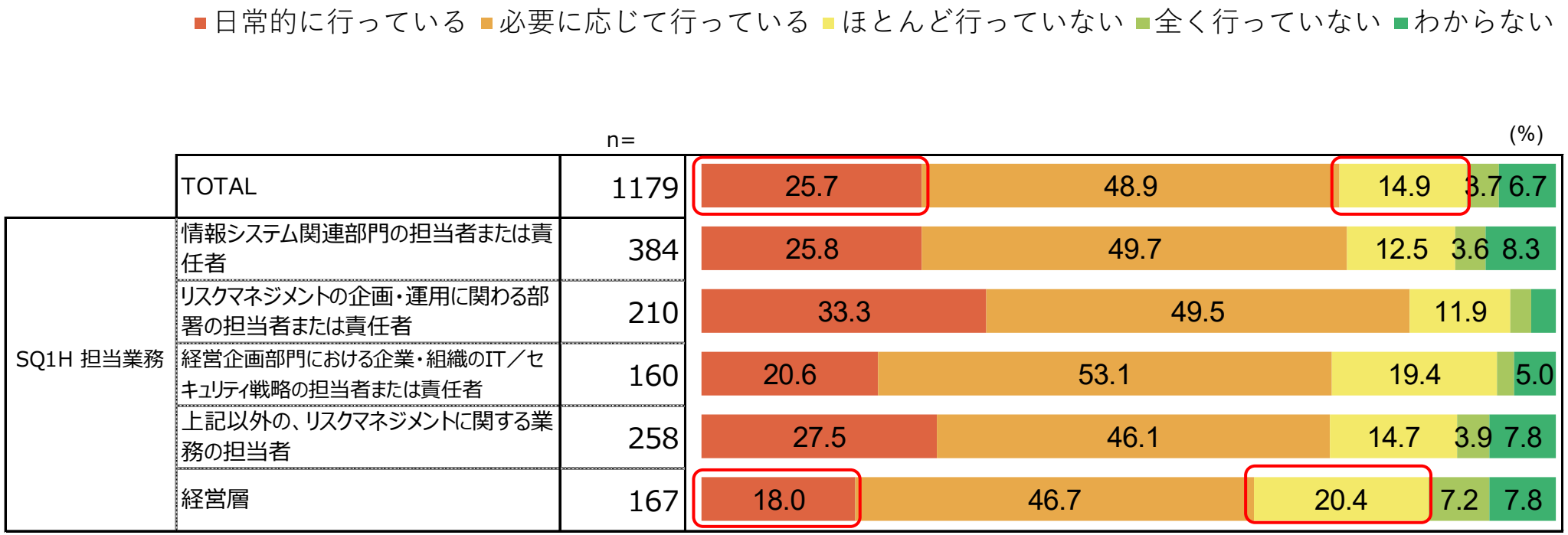
Q30 貴社では、内部不正リスクは重要な経営課題として捉えられていますか。



6-1. 企業アンケート調査のクロス集計による分析（13/14）

経営層自身は情報発信を「日常的に行っている」と考えている割合が小さく、むしろ「ほとんど行っていない」と考えている割合が増加している。従業員が「経営層」の範囲をより広く捉えているのに対して、経営者はこれをより狭く厳密に捉えていることが影響している可能性がある。

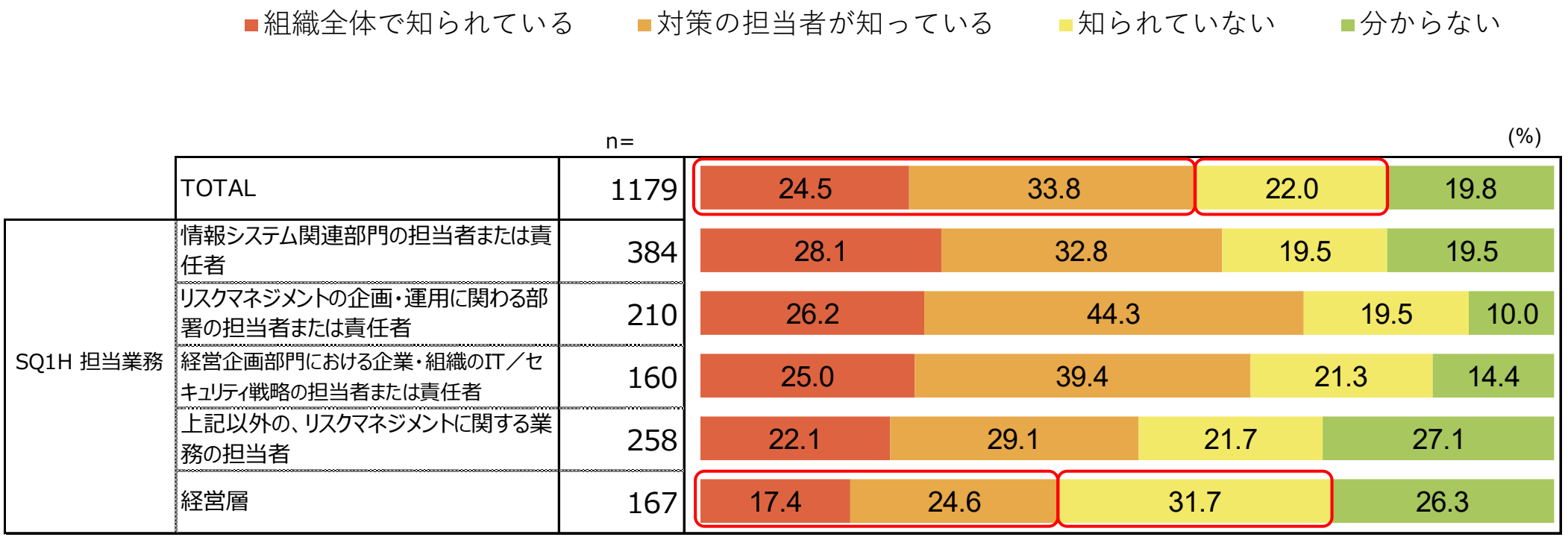
Q18 経営層は、組織全体での内部不正防止の取組み方針等について、全従業員に周知、指示していますか。



6-1. 企業アンケート調査のクロス集計による分析（14/14）

経営層においては、外国政府が関与した重要技術情報への合法的／非合法的アプローチに起因するリスクが「組織全体で知られている」または「対策の担当者が知っている」と回答している割合が明らかに低く、逆に「知られていない」と回答した割合が高くなっている。このことから、経営層は組織が当該リスクに関する認識が低いと捉えており、課題を感じているものと考えられる。

Q15 貴社では、次にあげる情報漏えいリスク／セキュリティリスクは組織全体で知られていますか。
～外国政府が関与した重要技術情報への合法的／非合法的アプローチ



6-2. 仮説の検証結果　～企業・組織全体として知っておくべき基礎知識～

アンケート調査（クロス集計を含む）、インタビュー調査の分析結果に基づき、仮説の検証を実施した。

社内規程、法制度、ガイドライン、情報漏えい／セキュリティリスクの全般に亘り、基礎知識の習得が不十分である実態が明らかになった。

調査軸	検証を試みる仮説	仮説の検証結果	備考
企業・組織全体として知っておくべき基礎知識の実態	②－1 社内規程についての知識レベルが把握できない、または知識が足りない	○	
	②－2 法制度についての知識レベルが把握できない、または知識が足りない	○	
	②－3 関連するガイドライン等についての知識レベルが把握できない、または知識が足りない	○	
	②－4 情報漏えい／セキュリティリスクに関する知識レベルが把握できない、または知識が足りない	○	

6-2. 仮説の検証結果　～内部不正防止に取り組む組織的体制～

- 経営層は従業員への情報発信を通じてリーダーシップを発揮していること、経営リソースを適切に配分していること、テレワーク環境の改善に組織全体で取り組んでいることが分かった。
- 一方で、内部不正防止に関する社内ポリシー／規定の整備はまだ不十分であった。
- 組織全体としての責任・権限は明確であったが、重要情報漏えいへの現場の個別対応、責任部門と関連部門の不十分な連携等の問題点が残っていることが分かった。
- マネジメントシステムの実効性は、重要情報漏えい対策に対しては確保されているものの、内部不正対策についてはまだ十分に確保されていない実態が明らかになった。

調査軸	検証を試みる仮説	仮説の検証結果	備考
内部不正防止に取り組む組織的体制の実態	③－1 経営層の情報発信が明確ではない、又は不十分な企業が多い	×	
	③－2 組織全体としての責任・権限が明確に定められていない企業が多い	△	■ 内部不正対策を主管して組織全体に対する責任を負う部門は概ね「情報システム／セキュリティ管理部門」と「リスク管理／コンプライアンス部門」に二分されていた。 ■ 他方で、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は全般に底上げが必要。 ■ 重要情報漏えいへの対応について、現場任せが残っている企業が少なくなかった。
	③－3 社内ポリシー／規定の整備が不十分な企業が多い	○	
	③－4 経営層がリソースを適切に配分できていない企業が多い	×	
	③－5 内部不正対策に関するマネジメントシステムが十分に機能していない企業が多い	△	■ 内部不正対策に関するマネジメントシステムについては、まだ十分に機能していない企業が多いと考えられるものの、重要情報の漏えい対策まで視野を広げるとマネジメントシステムが機能している企業の方が多かった。
	③－6 テレワークを行う従業員を支援する体制が整備できていない企業が多い	×	

6-2. 仮説の検証結果　～組織全体への周知・教育～

- 重要情報の分類と表示に関する規則／個人情報保護法の知識についてのリテラシー教育等の一部の例外を除けば、内部不正対策に関する周知・教育を受ける機会は不足している実態が明らかになった。
- 受けたリテラシー教育の内容の理解を深め、組織全体での実践に繋げることに取り組む企業は多い。好事例が複数見られたことに加えて、リテラシー教育が組織全体での実践に寄与していると回答した企業の割合が十分に高い水準に達していた。

調査軸	検証を試みる仮説	仮説の検証結果	備考
組織全体への周知・教育の実態	④－1 一般の職員に対する、内部不正対策に関する周知・教育は不足している	△	■ 重要情報の分類と表示に関する規則、個人情報保護法の知識についてのリテラシー教育は進展 ■ 営業秘密保護についてのリテラシー教育を実施している企業も決して少なくはなかったが、営業秘密保護では秘密文書の実務上の扱いが重要であり、経験も必要とされることから、リテラシー教育の効果が現時点でどこまで有効になっているか判ずるのは難しい面がある。 ■ それ以外の知識・規則・情報等に対するリテラシー教育は不足していた。
	④－2 内部不正対策を組織全体で実践できる環境が整っていない	×	

6-2. 仮説の検証結果　～内部不正防止の課題と対策～

- 経営層は一部の例外を除けば、重要情報漏えいに関する内部不正を必ずしも優先度の高い経営課題として捉えていなかった。特に、個人情報以外の重要情報の漏えいについてはその傾向が強かった。
- 内部不正対策の選択については、情報セキュリティ対策と比べて、苦心しているとは限らなかった。
- 個人情報以外の重要情報の漏えいに対する内部不正対策は、十分ではなかった。
- 内部不正対策は、必ずしもニューノーマルの急な環境変化（非正規雇用者の増加を除く）に対応できていなかった。
- 中途退職者／中途採用者の急増への対応は十分ではなかった。
- 内部不正を誘発しない職場環境の整備は十分ではなかった。
- 重要情報の侵害先に毅然として対応できるかについては、方針が定まっておらず、準備も十分とは言えなかった。

調査軸	検証を試みる仮説	仮説の検証結果	備考
内部不正防止の課題と対策	⑤－1 内部不正リスクは、経営リスクや事業リスクとしての優先度が高くなく、対策実施が後回しとなっている	△	■ 仮説は総じて実態を示している。 ■ しかし、顧客の個人情報の漏えいリスクが大きく、これを強く意識している企業等は内部不正防止に重点を置いて取り組んでいる。
	⑤－2 セキュリティ対策等と比較すると、内部不正に対する具体的な対策や事後対策の選択が難しい	×	
	⑤－3 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、内部不正対策の拡張が進んでいない	○	
	⑤－4 セキュリティ対策等と比較すると、ニューノーマル等の環境変化への対応が遅れており、リスクが高まる内部不正に関する規則が未整備、または対策を実施できていない	△	■ 非正規雇用者の内部不正対策だけは、対応が十分に進んでいた。
	⑤－5 急増する中途退職者／中途採用者の内部不正に対する対策整備が遅れている、または対策が実施できていない	○	
	⑤－6 不満を蓄積せず、内部不正を誘発しない職場環境の整備が十分ではない	○	
	⑤－7 内部不正による重要情報の漏えい発覚時に、侵害先にどこまで対応するかの方針がない	○	

6-3. 課題と今後の方向性

仮説の検証結果と得られた示唆を取りまとめるにあたり、課題とこれに対する今後の方向性を抽出・整理した。

このうち特に重要なのは、「経営層が重要情報漏えい／内部不正リスクを重要な経営課題として認識する意識変革の推進」である。経営層に内部不正リスクを重要な経営課題として認識させることで、企業の内部不正対策や、リテラシー教育等のその他の取り組みの促進に大きな効果を期待することができる。この変革のきっかけとなるのは重要情報の漏えい事案のリアルな事例に触れることであり、経営層がこれらから学ぶ感性を養うことが重要である。

主題	課題	今後の方向性
共通事項	■ 内部不正リスクが重要な経営課題であるという認識を企業に浸透させることが必要。 ■ 経営層、組織全体の責任者等が営業秘密漏えい等の事案／インシデントから学び、事業リスクを強く認識することが必要。	■ **重要情報漏えい／内部不正リスクを重要な経営課題として認識する意識変革の推進（To: 経営層、内部不正防止に関する組織全体の責任者等）** ■ **個人情報に留まらず、他の重要情報の漏えい事案などリアルな事例に触れることで、事業リスクとしての重要性を学ぶことができる感性とリテラシーを育成（To: 経営層、内部不正防止に関する組織全体の責任者等）**
内部不正防止に関する組織全体としての基礎知識の取得と周知・教育のあり方	■ 重要情報漏えい／内部不正防止の社内規程及びその規則を学ぶ機会をさらに増やすことが必要。 ■ 営業秘密の知識を根付かせるために、従業員に法知識よりも何をしてはいけないのかを教育することが必要。 ■ 情報システム部門が内部不正防止の全社責任を負うためには、当該部門の持つ法知識を強化することが必要。 ■ 必要な知識を組織に根付かせるには、教育するだけでなく、教育した内容を理解させることが必要。	■ 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り組みの一環として、重要情報漏えい／内部不正防止の社内規程及びその規則に焦点を当てる回数を増やし、組織全体の基礎知識と理解を促進（To: 従業員） ■ 営業秘密の知識を組織全体に根付かせるため、入社／人事異動／退職等の重要なタイミングで、具体的に重要情報を示して、何をしてはいけないのかを周知徹底（To: 従業員） ■ 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促進 ■ e-Learningに限定せず、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り組みを推進（To: 経営層、従業員）
内部不正防止のための組織的体制整備のあり方	■ 次の２つの責任・権限が実効的に確保され、全社的に対応できることが必要。 i. 内部不正対策を具体的に計画し、実施する責任・権限 ii. 経営層が定める基本方針に基づき、組織全体の立場から内部不正対策の計画を承認し、実施を統制する責任・権限 ■ 経営層の不正に対しても内部不正対策のマネジメントシステムが実効的に機能することが必要。	■ 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、法務・知財部門、営業・事業部門）との協働、または対策実施・統制部門（情報システム部門等）と関連部門との協働等による組織全体のガバナンス構築 ■ 経営層の不正への対策と透明性の確保について調査検討
重要情報漏えい／内部不正対策強化のあり方	■ 個人情報以外の重要情報の漏えい／内部不正対策の強化が必要。 ■ 悪意の不正に対し、効果とコストを両立できる対策の整備が必要。 ■ 中途退職者／中途採用者の急増に対応できる内部不正対策を確保することが必要。	■ 個人情報以外の重要情報の特定と対策の推進（To: 従業員） ■ 悪意の不正に対する人的・組織的対策と技術的対策のバランスの適正化（まずは従業員教育に軸足を置き、これでカバーできないところから技術的対策を順次適用していく等） ■ 企業の中途退職者／中途採用者の内部不正に対する対策強化の推進 ・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かによる誓約書の詳細度の変更　等