企業における
内部不正防止体制に関する実態調査

調査報告書

令和５年１月

請負者：株式会社エヌ・ティ・ティ・データ経営研究所

(This page is intentionally left blank.)

目次

別紙

(This page is intentionally left blank.)

1. 概要

(1) 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。今後は、近年の環境変化を踏まえて改訂された内部不正防止ガイドラインが、企業において実効性を持って活用されるべく、必要な施策を検討していくことが必要となっている。

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などが挙げられる。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ている。

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機密情報等も、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。

(2) 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。

(3) 調査の全体構成

本調査では、企業における電子化された重要情報[1]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。

- 企業・組織全体として知っておくべき基礎知識の実態
- 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
- 組織全体への周知・教育の実態

---

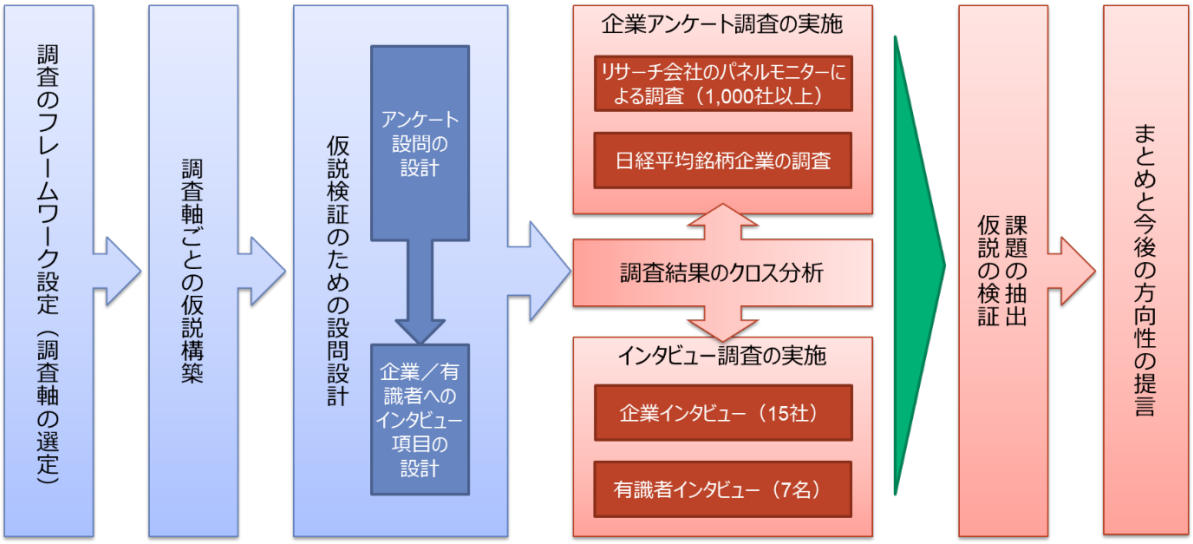
[1] 本調査報告書では、「重要情報」という用語を、IPA「組織における内部不正防止ガイドライン」第 5 版と同じ意味で使用している。企業や組織が保有・管理し、活用する情報のうち、その情報の不正利用により事業に影響を及ぼす可能性があるもの。

■　内部不正防止の課題と対策の実態
■　内部不正防止ガイドライン利用の実態

さらに、これらの調査軸の設定を踏まえ、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ものと見込まれる。

５つの共通の調査軸を適用した本調査全体の進め方を図表１に示した。

図表 1 本調査の全体構造



2. 動向調査の実施方法

ここでは、図表１で示した本調査の全体構造に基づき、各ステップの作業の実施方法について述べる。

(1) 調査のフレームワーク

既に述べたとおり本調査では、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共通の調査軸に基づいて実施している。その概要を図表２に示した。

図表 2 本調査のフレームワーク

このように、すべての作業を共通した調査軸ごとに実施することで、それぞれの軸において仮説、アンケート設問、インタビュー調査項目の関係性（紐付け）が明確になり、仮説の検証に則した設問・調査項目の設計が可能になるほか、アンケートとインタビューの調査結果の比較・分析（クロス分析）が容易になる。その結果、仮説検証の質的向上を期待することができる。

(2) 仮説の構築

各調査軸に対し、本調査の実態把握によって検証を試みる仮説を設定した。基本的には、仮説は重要情報の漏えいに関する内部不正対策・体制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ている。

①企業・組織全体として知っておくべき基礎知識の実態について

企業においては、重要情報の情報漏えいに対する内部不正対策は、セキュリティ対策や会計不正対策等と比較して優先順位が低いのではないかという懸念が元々存在している。さらには、

社会のデジタル変革の急速な進展に伴って、重要情報の電子化（いわゆる「ボーンデジタル」を含む）の進展、テレワークの常態化、クラウド利用の急拡大、サプライチェーン問題の顕在化、関連法規やガイドラインの活発な改訂、これらに伴う社内方針・規程の様々な改訂等の広範かつ速度の速い変化が生じている状況である。この現状を踏まえ、一度基本に返って、そもそも従業員に必要な基礎知識が最新の状態にアップデートされて、企業内で広く浸透しているかを確認する必要があると考えている。

そこで、この調査軸においては、「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」という仮説を設け、社内規程／法制度についての知識／関連するガイドライン等の知識、情報漏えい／セキュリティリスクの各切り口からこの仮説の検証を試みることとした。

②内部不正防止に取り組む組織的体制の実態について

内部不正防止ガイドラインの第 5 版改訂の際に、企業・組織全体で内部不正防止に取り組むにあたっての組織体制の在り方については、いろいろと議論があったものの、十分なコンセンサスを得ることができなかった。この経緯を踏まえると、企業・組織全体における内部不正防止のための組織体制については、まだ確立された拠るべき指針が存在しておらず、実態調査を通じてさらにこれを検討していく必要があるものと考えられる。そこで、本調査では「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、内部不正防止に対する組織全体としての体制整備ができていない」という仮説を設け、実態調査を通じてこの仮説の検証を試みることとした。ここで、経営層のコミットと重要情報管理の成熟度については、ニューノーマルに対応していく現状も踏まえて、次の 6 点に焦点を当てている。

- 経営層による明確で十分な情報発信
- 内部不正防止に関する組織全体としての責任・権限の明確化
- 経営層のリーダーシップによる、社内ポリシー／規定整備の充実
- 経営層による、内部不正防止に必要なリソースの適切な配分
- 内部不正対策に関するマネジメントシステムの充実
- テレワーク等の働き方変革に対する従業員支援体制の整備・充実

③組織全体への周知・教育の実態について

近年、e-Learning の広範な普及と相俟って、セキュリティ対策やコンプライアンスについての企業・組織全体へのリテラシー教育は広く浸透してきたと見込まれる。一方で、重要情報の漏えいに対する内部不正対策については、どのような形式や方法で企業・組織全体に周知・教育されているかの実態は必ずしも把握できていない。そこで本調査では、内部不正対策に関するリテラシー教育がセキュリティ対策や企業リスク管理／コンプライアンスの教育の一部として実施されていることを想定し、「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」という仮説を設けて、実態調査を通じてこの仮説の検証を試みることとした。

さらに、リテラシー教育が組織全体での対策実践に繋がり、実効性を発揮しているかを実態把握するため、「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」という仮説を設け、その検証を試みた。

④内部不正防止の課題と対策の実態について

「組織全体への周知・教育」においても述べた通り、重要情報の漏えいに対する内部不正対策はセキュリティ対策または企業リスク管理／コンプライアンス確保の一部として実施されていることが想定され、高い優先順位で重点を置いて実施されているとは考えにくい面がある。他方で、個人情報、重要技術情報・ノウハウの漏えいリスクに対する企業・組織の認識は高まってきており、今後、内部不正対策に対する関心が高まることも想定される。このような現況を踏まえ、本調査では「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」という仮説を設け、実態調査を通じてこの仮説の検証を試みた。ここで、内部不正対策の進捗状況については、次の 7 点に焦点を当てている。

- 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

⑤内部不正防止ガイドライン利用の実態について

内部不正防止ガイドラインが我が国の企業・組織においてどの程度活用されているかの実態は、まだ必ずしも明らかになっていない。今後の当該ガイドラインの普及啓発方針を検討する上でも、現在の活用実態を把握しておくことが必要である。そこで本調査では、「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」という仮説の下で、実態調査によってこれを検証することを試み

た。ここで、「効果的に活用されているか」については、次の２つの観点を考慮した。

- あまり知られていない
- 存在は知っていても、あまり読まれていない

⑥まとめ

ここまでの検討に基づいて設けた仮説を一覧できるように、表形式で取りまとめて図表３に示した。

図表３ 本調査で検証を試みる仮説

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
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) アンケートとインタビューを組み合わせた仮説検証の方法

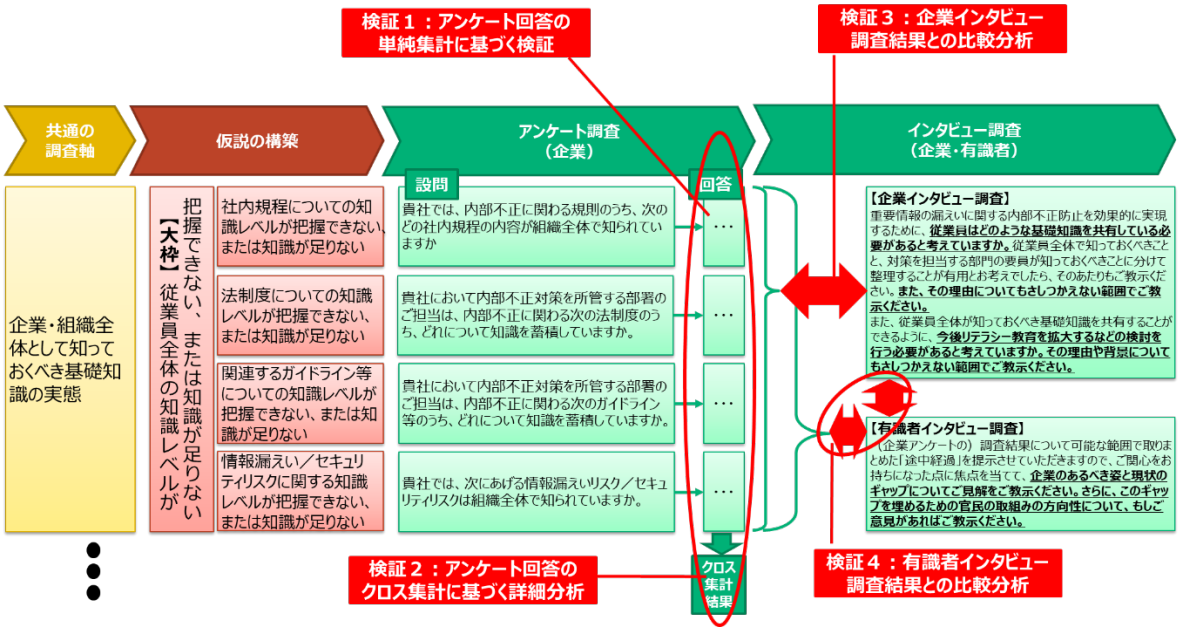
既に述べた通り、本調査では実態調査で検証を試みる仮説の構築、企業アンケートの設問や企業／有識者へのインタビュー項目の設計、調査結果の集計・分析、仮説の検証と課題の抽出という一連の作業の全てを共通の調査軸の上で横串を通して実施した。この共通の調査軸と本調査のフレームワークについては図表２に示した通りである。仮説の検証は、共通の調査軸に基づいて設計された企業アンケート調査、企業インタビュー調査、有識者インタビュー調査の結果を、共通の調査軸の上で比較分析することによって実施した。

仮説の検証においては、具体的には次の４つのステップによって単独での分析／比較分析を

実施した。この検証方法について図表４に取りまとめたので参照されたい。

i. 企業アンケートの回答の単純集計結果に基づく分析（単独での分析）
ii. 企業アンケートの回答のクロス集計に基づく詳細分析（単独での分析、業種／企業規模等による傾向の違いを深掘り）
iii. 企業アンケート調査結果と企業インタビュー調査結果の比較分析
iv. 企業アンケート調査結果と有識者インタビュー調査結果の比較分析（企業の実態を踏まえた有識者の提言等）、企業インタビュー調査結果と有識者インタビュー調査結果の比較分析

図表 4 仮説検証の方法



今回、企業アンケート調査で経営層から一定数の回答（約 14%）を得ることができたこと、企業インタビュー調査においても大企業／中堅企業／IT ベンチャー企業の経営層や監査担当役員から数件の回答を得ることができたことを踏まえ、経営層の認識や担当者との意識の違いについても比較分析を実施することとした。

(4) 企業アンケート調査の実施方法

ここでは、企業アンケート調査の実施方法について述べる。

①調査対象者

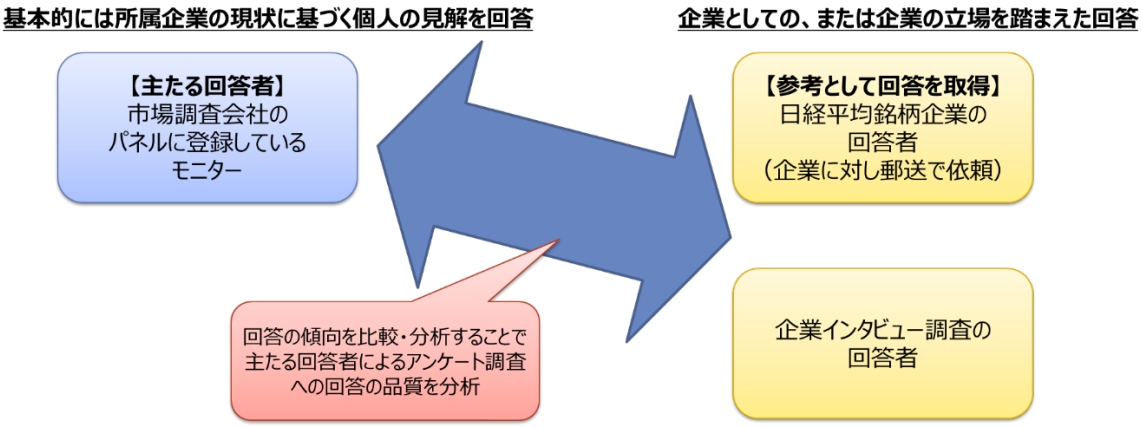
企業アンケート調査では、企業において次の要件のうちいずれか１つを満たす者を対象とした。

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

また、主たる調査対象者は調査仕様に基づき、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）から選定した。しかし、パネルモニターの回答は基本的には所属企業の現状に基づく個人の見解であると想定されることから、念のため回答の質的検証を試みることが望ましいと考えられた。そこで本調査では、日経平均銘柄企業（225 社）に対して書面（郵送）でアンケート調査への回答を依頼し、少数ではあるが企業としての正式回答を収集した。こうして集約された立場の違う 2 つの調査対象者群の回答傾向を比較・分析することで、主たる調査対象者の回答の品質を考察した。さらには、後述する企業インタビュー調査の回答も「企業の立場を踏まえた正式回答」とみなせることから、当該回答も比較分析の対象として追加し、主たる調査対象者のアンケート回答の品質確認に役立てた。（図表 5 参照）

図表 5 調査対象者の立場の違い



②アンケート調査の実施プロセス

パネルモニターと日経平均銘柄企業のそれぞれに対するアンケート調査の実施プロセスを図表 6 に取りまとめた。基本的には回答者を決めて回答を依頼し、Web システムを用いてアンケートに回答していただき、オンラインで回答を回収して品質を確認し、回答の単純集計とクロス集計を実施するという流れであり、この実施プロセスは両者で共通している。しかし、各ステップでの実施方法には調査対象毎に多少の違いが存在する。

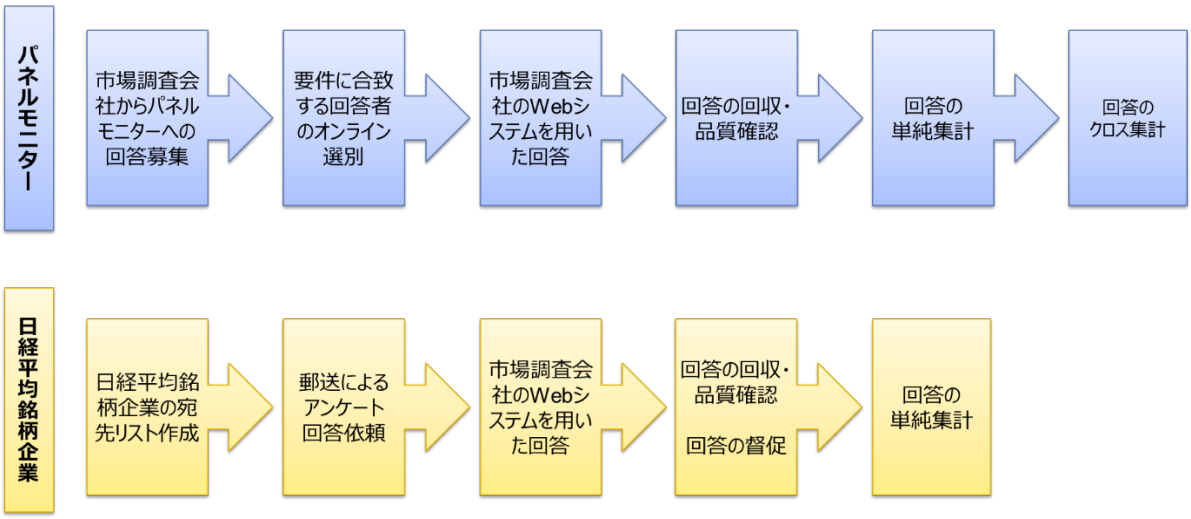
回答者を決めて回答を依頼するまでのステップでは、パネルモニターの場合は市場調査会社がオンラインでパネル登録者の回答を募集し、回答者が満たすべき要件（担当している業務等）について質問して要件に合致する回答者を選別した。これに対し、日経平均銘柄企業の場合は

公知情報から宛先企業リストを作成し、アンケート依頼状を郵送で公式窓口に送付することで回答を依頼した。

アンケート調査への回答については、どちらの場合も市場調査会社の Web システムを用いてオンラインでご回答を得た。パネルモニターについては督促を行う必要はなかったが、日経平均銘柄企業に対しては葉書による回答督促を一度実施した。

調査回答の集計については、まずそれぞれの調査対象について単純集計を実施した。さらに、パネルモニターからの回答についてはクロス集計を実施した。日経平均銘柄企業については、元々の想定回答数が少ないためクロス集計は実施しない方針とした。

図表 6 アンケート調査の実施プロセス



③回答の回収数に対する要件

パネルモニターからの回答は仕様上、回収数についてのみ要件が設定されており、これを満足するべく調査を実施した。回収要件は次の 2 点である。

i. 国内の企業 1,000 社以上に所属する回答者から回答を得ること
ii. 従業員数が 301 名以上の企業に所属する回答者から 300 件以上の回答を得ること。

市場調査会社のノウハウを活用し、上記の回答要件を満足できる規模のパネルモニターを選別してアンケート回答を回収した。なお、同一企業に所属するパネルモニターの回答は特に排除してはいないが、国内の企業 1,000 社以上から回答を回収することが求められているため、「回答者が同一企業に所属していないことを推定するロジック」を適用することで回答企業数を推定し、十分に 1,000 社を超えるように回答を回収した。このロジックを適用するため、アンケート設問として「企業の設立年」「企業の本社所在地」を追加し、これらの設問に対する回答も考慮して「推定ロジック」を適用した。

他方で、日経平均銘柄企業からの回答回収数については特段の要件が設定されていないため、概ね 20～25 社程度の回答を回収するべく依頼と督促を実施した。

④回答効率の向上策

今回、調査対象者は Web システムを用いて回答したため、回答に関する画面制御を工夫するなどの回答者の負荷低減策を用いて効率的な回答数確保を行った。具体的には次のような工夫を実施した。

i. 前の回答内容に応じた自動画面遷移
ii. 回答不備（必須項目で回答なし、回答数の制限を超過、回答内容に矛盾等）を自動で検出し、エラーを表示
iii. 排他防止機能の適用（複数選択の設問で矛盾した選択肢を同時に選択できないように自動制御する機能等）
iv. 回答の中断、回答の送信前に確認・修正を可能とすること 等

これに加えて、自動回答ツールを使用する等の不正な方法による回答、回答時間が質問数に対して極端に短い回答等を検知して排除した。

⑤アンケート設問の設計

a. 要件に合致する調査対象者の選別（スクリーニング）

回答者の業務が調査対象者の要件に合致しているかを確認するため、次の設問を設けた。この設問はクロス集計の軸として、「経営者」と「それ以外」の回答傾向の違いを分析することにも用いた。

■ 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。

b. 同一企業に所属していないことを推定するロジックで用いる設問

既に述べた通り、同一企業に所属していないことを推定するロジックで用いるため、所属企業の設立年と本社所在地について尋ねる設問を設けた。

c. クロス集計の軸として用いる設問

クロス集計の軸として用いる属性として、業種と常用雇用者数を尋ねる設問を設けた。

d. 構築した仮説を検証するために設けた設問

図表 3 で示した各調査軸の各仮説に対し、これを検証するためのアンケート設問を以下のよう

に設計した。

【調査軸１：企業・組織全体として知っておくべき基礎知識の実態】

図表３で示した「企業・組織全体として知っておくべき基礎知識の実態」という調査軸に紐づく各仮説に対し、これを検証するためのアンケート設問を作成した。その結果を図表７に示した。

図表７ 調査軸１に紐づく各仮説を検証するためのアンケート設問等の設計結果

仮説の大枠	検証を試みる仮説	仮説検証のためのアンケート設問	対応する企業インタビュー調査項目	有識者インタビュー調査項目
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	・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。	**【内部不正防止に関し、組織全体が知っておくべき基礎的な知識について】** ・重要情報の漏えいに関する内部不正防止を効果的に実現するために、従業員はどのような基礎知識を共有している必要があると考えていますか。 ・従業員全体で知っておくべきことと、対策を担当する部門の要員が知っておくべきことに分けて整理することが有用とお考えでしたら、そのあたりもご教示ください。 ・また、その理由についてもさしつかえない範囲でご教示ください	・企業のあるべき姿と現状のギャップについてご見解をご教示ください。 ・さらに、このギャップを埋めるための官民の取組みの方向性について、もしご意見があればご教示ください。
	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	・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。		
	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	・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。		
	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	・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。 - 機器・システムの脆弱性 - サイバー攻撃、だましの手口 - 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 - サプライチェーンにおける不必要な重要情報の授受 - クラウドセキュリティのあいまいな責任分担		

		- テレワークの不十分なセキュリティガバナンス - プライバシーを侵害する従業員監視 - 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 - 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		

【調査軸２：内部不正防止に取り組む組織的体制の実態】

図表３で示した「内部不正防止に取り組む組織的体制の実態」という調査軸に紐づく各仮説に対し、これを検証するためのアンケート設問を作成した。その結果を図表８に示した。

図表８ 調査軸２に紐づく各仮説を検証するためのアンケート設問等の設計結果

仮説の大枠	検証を試みる仮説	仮説検証のためのアンケート設問	対応する企業インタビュー調査項目	有識者インタビュー調査項目
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	・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。 ・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。	・貴社では、セキュリティ対策／内部統制等の一環として、内部不正防止についても経営層がリーダーシップを発揮しておられますか。また、どのようなリーダーシップを発揮しておられるかについてご教示ください。	・企業のあるべき姿と現状のギャップについてご見解をご教示ください。 ・さらに、このギャップを埋めるための官民の取組みの方向性について、もしご意見があればご教示ください。
	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	・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。 ・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。	・内部不正対策を整備し、実践する責任は、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のどちらが担っていますか。その理由	

		・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。	や利点についてもお考えをご教示ください。 ・また、重要情報漏えいに関する貴社全体の内部不正対策の責任者は、サイバーセキュリティ対策の責任者と同じでしょうか、それとも内部統制の責任者と同じでしょうか。あるいは、これらの責任者はいずれも同じでしょうか。	
	社内ポリシー／規定の整備が不十分な企業が多い	・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。	－	
	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	・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。	－	
	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	・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。 ・貴社では内部防止不正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。	－	
	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	・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。	－	

【調査軸３：組織全体への周知・教育の実態】

図表３で示した「組織全体への周知・教育の実態」という調査軸に紐づく各仮説に対し、これを検証するためのアンケート設問を作成した。その結果を図表９に示した。

図表 9 調査軸 3 に紐づく各仮説を検証するためのアンケート設問等の設計結果

仮説の大枠	検証を試みる仮説	仮説検証のためのアンケート設問	対応する企業インタビュー調査項目	有識者インタビュー調査項目
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	・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。 ・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。 ・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。 ・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。	**【内部不正防止について組織全体で実施している周知・教育の現状】** ・貴社では、重要情報の漏えいに関する内部不正防止について、現在組織全体でどのようなリテラシー教育を実施していますか。また、実施している理由についてご教示ください。 ・また、今後は何についてのリテラシー教育を強化する必要があると考えていますか。	・企業のあるべき姿と現状のギャップについてご見解をご教示ください。 ・さらに、このギャップを埋めるための官民の取組みの方向性について、もしご意見があればご教示ください。
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	・あなたは、内部不正防止のために周知・教育した内容が、組織全体での実践に寄与していると感じていますか。 ・周知・教育が組織全体の実践に寄与できていない理由は何だと考えていますか。	・内部不正防止のために周知・教育した内容の実効性をどのようにモニタリングしていますか。また、その理由や効果についてもさしつかえない範囲でご教示ください。	

【調査軸 4 ：内部不正防止の課題と対策の実態】

図表 3 で示した「内部不正防止の課題と対策の実態」という調査軸に紐づく各仮説に対し、これを検証するためのアンケート設問を作成した。その結果を図表 10 に示した。

図表 10 調査軸４に紐づく各仮説を検証するためのアンケート設問等の設計結果

仮説の大枠	検証を試みる仮説	仮説検証のためのアンケート設問	対応する企業インタビュー調査項目	有識者インタビュー調査項目
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	－	**【全体共通】** ・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。	**【組織として現在重視している内部不正防止対策、及び重視している理由】** ・組織として、現在どのような内部不正防止対策を重視していますか。また、今後重視したいと考えている内部不正対策についてもご教示ください。また、これらを重視している理由についてご教示ください。 ・テレワーク中やクラウドサービス利用中の内部不正対策については、どのように取り組んでおられますか。	・企業のあるべき姿と現状のギャップについてご見解をご教示ください。 ・さらに、このギャップを埋めるための官民の取組みの方向性について、もしご意見があればご教示ください。
	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	・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。		
	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	・貴社では重要情報の管理ルールを厳格に適用していますか。 ・貴社では、内部不正防止対策を具体的に選択する上での課題は何ですか。		
	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	・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。 ・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。		
	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	・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。 ・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。 ・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。 ・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。		

	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	・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。 ・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。		
	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	・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。		
	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	・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。		

【調査軸５：内部不正防止ガイドライン利用の実態】

図表３で示した「内部不正防止ガイドライン利用の実態」という調査軸に紐づく各仮説に対し、これを検証するためのアンケート設問を作成した。その結果を図表 11 に示した。

図表 11 調査軸５に紐づく各仮説を検証するためのアンケート設問等の設計結果

仮説の大枠	検証を試みる仮説	仮説検証のためのアンケート設問	対応する企業インタビュー調査項目	有識者インタビュー調査項目
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	・あなたは（独）情報処理推進機構（以降、「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」をご存じでしたか。 ・あなたは IPA「組織における内部不正防止ガイドライン」が、電子化された重要情報を漏えいさせる等の内部不正に焦点を当てて書かれていることをご存じでしたか。 ・貴社では、内部不正防止対策を検討するにあた	・内部不正防止対策を選択するにあたり、内部不正との関わりが深い情報セキュリティ／内部統制関係のガイドライン等を活用することが考えられます。こうしたガイドライン等＊は活用していますか。 ・また、情報セキュリティ関係のガイドラインと内部統制関係のガイドラインでは、どちらをよく参考にしますか。	・企業のあるべき姿と現状のギャップについてご見解をご教示ください。 ・さらに、このギャップを埋めるための官民の取組みの方向性について、もしご意見があればご教示ください。

		り、どのようなガイドラインを参考にしていますか。	*ご参考：IPA では「組織における内部不正防止ガイドライン」を公開しています。	
	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	・貴社では、「組織における内部不正防止ガイドライン」のどの項目を参考にしていますか。	・「組織における内部不正防止ガイドライン」の内容及び普及啓発についてご意見があればお聞かせください。	

e. アンケート調査票としてのとりまとめ

a.～d.の検討結果に基づき、アンケート調査票としての取りまとめを実施した。企業アンケート調査で実際に使用した調査項目について別紙１に示した。

(5) 企業インタビューの実施方法

①調査対象者（国内の企業）

国内の企業 15 社以上に対し、企業インタビュー調査を実施した。調査対象としては次の４つの要件のうち 1 つ以上に合致していると考えられる企業を選定し、インタビュー調査へのご協力を依頼した。

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

インタビュー先の企業は、大企業、中堅企業、ベンチャー企業を網羅しており、業種も情報通信／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した。各社におけるインタビュイーの属性は、経営層、監査担当役員、情報システム／セキュリティ担当者、知財保護担当者、リスク管理／コンプライアンス／内部監査担当者等多岐に亘っている。

②インタビューの実施方法

インタビューは原則としてオンライン（Teams または Webex を使用）で実施した。但し、対面での実施を希望した複数のインタビュー先については、指定の場所を訪問してインタビューを行った。

③企業インタビューの調査項目設計

本調査全体で一貫して共用している５つの調査軸のそれぞれに紐づく仮説を検証するために、企業アンケートの回答から取得できる知見／情報のさらなる深掘りや補完を目的として、企業インタビューの調査項目を設計した。各調査軸における、仮説検証のための知見／情報の深掘り及び補完の方針について図表 12 に取りまとめた。

図表 12 インタビュー調査項目設計における仮説検証のための知見／情報の深掘り／補完方針

共通の調査軸	調査項目設計の方針	
	仮説検証のための知見／情報の深掘り	仮説検証のための知見／情報の補完
企業・組織全体として知っておくべき基礎知識の実態	・知っておくべき基礎知識に対する優先度とその理由	・従業員全体で知っておくべきことと担当部門の要員が知っておくべきことの区分け
内部不正防止に取り組む組織的体制の実態	・経営層のリーダーシップ ・具体的な組織体制や責任体制 ・リスク管理／コンプライアンスを担う組織とセキュリティ管理を担う組織の間の具体的な関係	－
組織全体への周知・教育の実態	・リテラシー教育の実態に加えて、それを実施している理由 ・リテラシー教育の実効性を高める取組み	・今後強化すべきリテラシー教育の優先度
内部不正防止の課題と対策の実態	・内部不正防止対策の優先度とその理由 ・テレワークやクラウド利用に関する内部不正対策	－
内部不正防止ガイドライン利用の実態	・良く参考にしているガイドラインの実状 ・内部不正防止ガイドラインの認知／活用状況	・内部不正防止ガイドラインの内容及び普及啓発に対するご意見等

図表 12 で示した方針に従って企業インタビュー調査項目を設計した結果を図表７～図表 11 に示した。また調査票の形に取りまとめたもの（企業インタビュー調査票）を別紙２に示した。

(6) 有識者インタビューの実施方法

①調査対象者

内部不正防止や秘密情報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は、以下の３要件のうち１つ以上に合致する専門家を７名選定した。

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

＜インタビュー対象とした有識者（50 音順、敬称略）＞

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
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
蔦大輔（i に該当）	森・濱田松本法律事務所　弁護士
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
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
和貝享介（ii に該当）	公認会計士
渡邉遼太郎（i ,iii に該当）	東京八丁堀法律事務所　弁護士

なお、金子氏には、企業アンケート調査票の設計においても、有識者としてのご意見をいただいたことを付記しておく。

②インタビューの実施方法

インタビューはオンライン（Teams）で実施した。

③有識者インタビューの調査項目設計

インタビューを実施した有識者においては、５つの共通の調査軸のそれぞれについて、これに紐づく仮説を検証するための企業アンケート回答結果の速報（単純集計の速報）を踏まえて、次の２つの観点から専門家としての見解を聴取した。

i. 有識者としての、企業のあるべき姿と現状のギャップに関するご意見
ii. 企業をあるべき姿に導くために、IPA の政策（内部不正防止ガイドラインの改訂、同ガイドラインの普及啓発等）や民間の自主的取組みはどうあるべきかについてのご提言

この調査項目について調査票の形に取りまとめたもの（有識者インタビュー調査票）を別紙３に示した。

(7) クロス分析の実施方法

①企業アンケート回答のクロス集計による分析

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。クロス集計のための分析軸としては、アンケート設問に基づいて次の６軸を設定した。

i. 回答者の担当業務の違い（経営層とそれ以外）
ii. 製造業とそれ以外
iii. 大企業と中小企業
iv. 責任部門の違い（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）
v. 内部不正を重要な経営課題と認識する企業とそれ以外
vi. 内部不正事案／疑われる事態が発生した企業とそれ以外

次に、各調査軸に紐づく仮説を検証するためのアンケート調査結果を補強するため、上記の６つの分析軸を用いてクロス集計を実施するアンケート設問の観点を抽出してみた。その結果を一覧として図表 13 に示す。

図表 13 クロス集計を実施する対象の一覧

※クロス集計のための分析軸の記載については、上記のⅰ～ⅵの分析軸番号を参照

共通の調査軸等	検証する仮説	クロス集計の対象	
		対象とするアンケート設問の観点	分析軸
回答者の属性	回答している経営層は中小企業の経営層が多い	回答者の業務	iii
	リスクマネジメント担当者の回答は大企業が多い	回答者の業務	iii
企業・組織全体として知っておくべき基礎知識の実態	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	組織全体のリスク認識の現状についての感じ方	i
		組織全体のリスク認識の現状	iv，v
内部不正防止に取り組む組織的体制の実態	経営層の情報発信が明確ではない、又は不十分な企業が多い	経営層が方針を周知・指示しているかの現状についての感じ方	i
		経営層が方針を周知・指示しているかの現状	v
	社内ポリシー／規定の整備が不十分な企業が多い	策定されている指針や規則の現状	iv，v
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・教育は不足している	内部不正事件／疑われる事態の発生状況についての感じ方	i
		内部不正事件／疑われる事態の発生状況	ii，iii
		実施しているリテラシー教育の内容	iv，v

内部不正防止の課題と対策の実態	全仮説に共通	実施している対策の現状	ii，iii，iv，v
	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	内部不正リスクを重要な経営課題と捉えているかの現状についての感じ方	i
		内部不正リスクを重要な経営課題と捉えているかの現状	iii，iv，vi
	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	重要情報を特定する仕組みの充実の現状	ii
		個人情報以外の重要情報にも対応できているかの現状についての感じ方	i
		個人情報以外の重要情報にも対応できているかの現状	ii，iii
	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	中途退職者対策の現状	ii，iii

なお、クロス集計結果については、興味深い分析結果が出たものを中心に抜粋して仮説の検証に役立てるとともに、その結果の図表を報告書に記載した。

②企業アンケート回答、企業インタビュー結果、有識者インタビュー結果のクロス分析

図表４に示した通り、各調査軸に紐づく仮説を検証するにあたって、企業アンケート回答、企業インタビュー結果、有識者インタビュー結果の間で次の２つのクロス分析を実施した。

i. 企業アンケート調査結果と企業インタビュー調査結果の比較分析
ii. 企業アンケート調査結果と有識者インタビュー調査結果の比較分析（企業の実態を踏まえた有識者の提言等）、企業インタビュー調査結果と有識者インタビュー調査結果の比較分析

3. 調査結果

ここでは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基づき、仮説の基本検証を実施した結果を取りまとめた。また、企業アンケート調査の主たる回答はパネルモニターが所属企業の現状に基づいて個人として回答したものであるため、参考までに、企業として回答した結果（参考回答：日経平均銘柄企業に郵送でアンケート回答を依頼した結果）との間に傾向の違い等が見られるかも分析してみた。

次に、各調査の回答回収実績を示した。

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
	●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
iii.	有識者インタビュー調査：	7 名

(1) 企業アンケート調査の単純集計結果

以下では、企業アンケート調査の単純集計結果に基づき、仮説の基本検証を実施した結果を取りまとめた。

①回答者及び所属企業の属性

パネルモニターの回答者（主たる回答）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（情報システム関連部門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）が 46.2%で最も多く、次いでリスクマネジメント関係業務（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、上記以外のリスクマネジメントに関する業務の担当者）が 39.7%となっている。今回、経営層から 14.2%（167 名）の回答を得ているが、これはパネルモニターから回答者を選抜したことによる効果と考えられる。このうち約 70%は中小企業の経営層であり、残りの半分程度は従業員数が 1,000 名を超える大企業の経営層となっている。また、大企業と中小企業の間で回答者の割合が大きく異なっているのは経営層のみであり、その他の業務の担当者の配分はあまり差はない。（図表 14 参照）

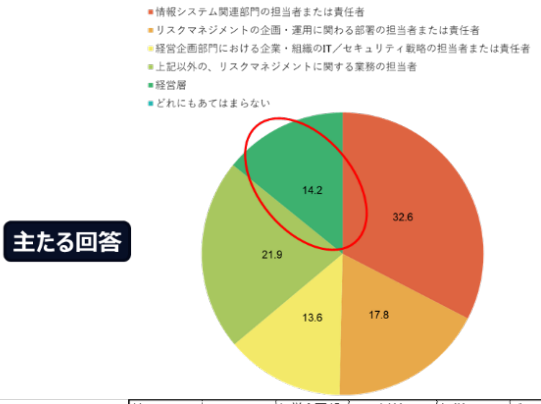
参考までに、ほとんどが大企業である日経平均銘柄企業からの回答を見てみると、情報システム／セキュリティ関係業務を担当する方からの回答が 84%に達している。もし仮に大企業に対して郵送アンケート調査を実施し、「企業名での正式回答」を集約したとすると、日経平均銘柄企業からの回答と同じように情報システム／セキュリティ関係業務の担当者からの回答の割合が、現在（パネルモニターからの回答）よりも増える可能性がある。

図表 14 回答者の担当業務

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。

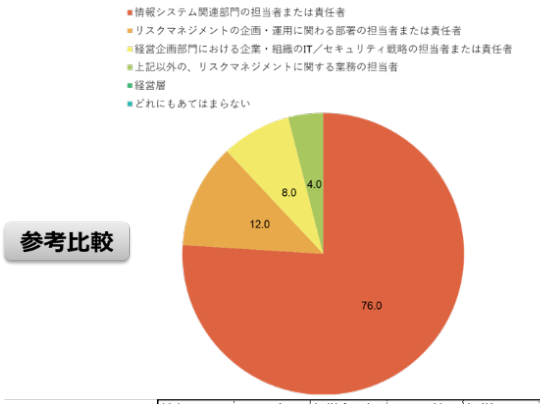
＜パネルモニターのみの集計＞

（ご参考：日経平均銘柄企業25社の集計）



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

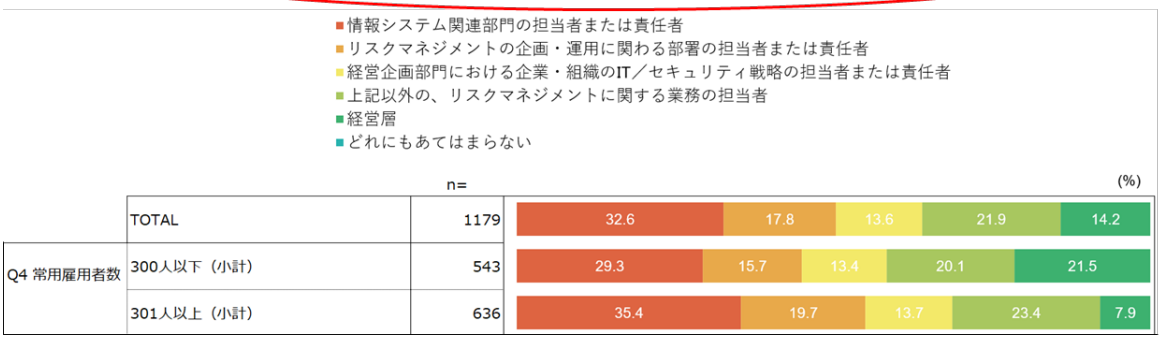


参考比較

	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

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

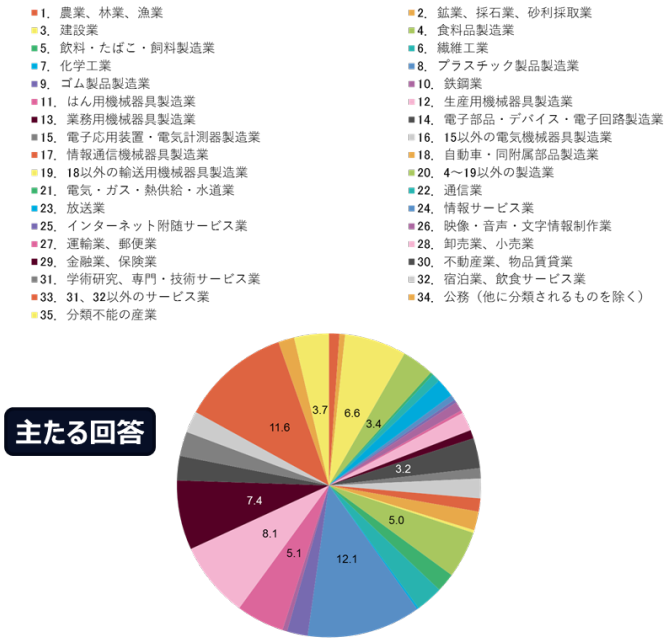


パネルモニターの回答者が所属する企業の業種は幅広く分布しているが、製造業、情報サービス業、卸売業・小売業、金融業・保険業、その他のサービス業等が多くなっている。（図表 15 参照）

図表 15 所属企業の業種

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＞



（ご参考：日経平均銘柄企業25社の集計）

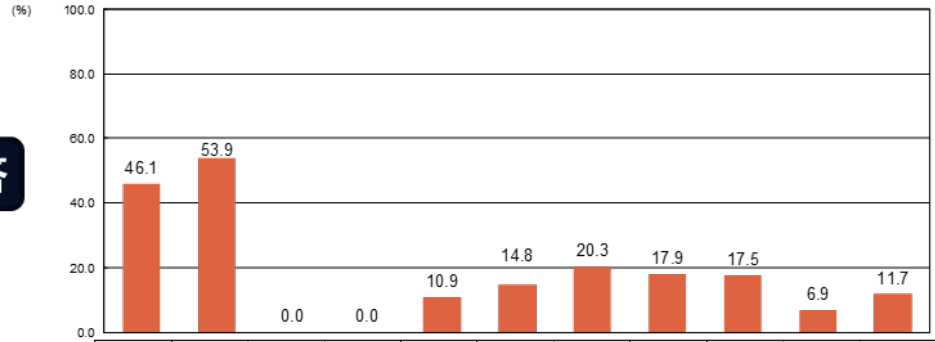
パネルモニターの回答者が所属する企業については、大企業と中小企業がほぼ半々となっている。他方で、参考として回答を集約した日経平均銘柄企業については、ほとんどすべてが大企業であった。（図表 16 参照）

図表 16 所属企業の常用雇用者数

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＞

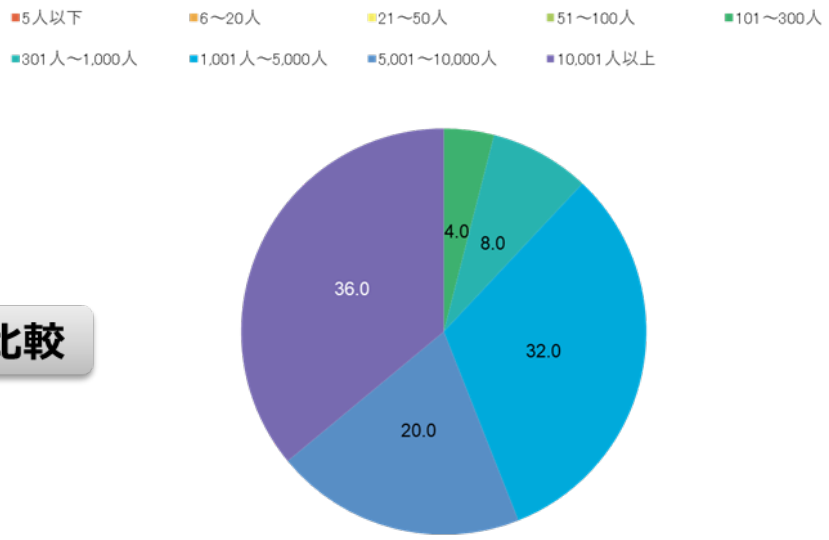
主たる回答



	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

②企業・組織全体として知っておくべき基礎知識の実態

ここでは、社内規程／法制度／関連するガイドライン／関連するリスクのそれぞれに対して設定した仮説について、企業アンケート調査結果を用いて検証を試みた。

【検証したい仮説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

内部不正防止に関わる主要な社内規程が、企業・組織においてどの程度広く認知されているかについて、その実態を調査した。パネルモニターのアンケート回答の単純集計結果を図表 17 に示した。

ここに示したような主要な社内規程は、どの企業でも組織全体で認知されていることが望ましい。この観点で調査結果を見ると、60～70%以上の企業が組織全体で認知していると回答している規程は就業規則しかなく、全体に亘ってもう少し底上げが必要な状況と考えられる。例えば、大企業が中心の日経平均銘柄企業の回答では60%を超えている規程が８つあり、今後めざすべき到達点を示唆しているものと考えられる。以上の結果を考慮すると、仮説が示唆している通り、内部不正防止に関わる社内規程についての組織全体としての知識がまだ十分ではない、または知識レベルがしっかりと把握できていない企業がまだ多い実状が伺われる。

他方で、秘密保持・情報管理規則、営業秘密管理の規則、限定提供データ管理の規則については、日経平均銘柄企業においても組織全体での認知が低いままである。これらについては企業全体に共通する課題であると考えられる。

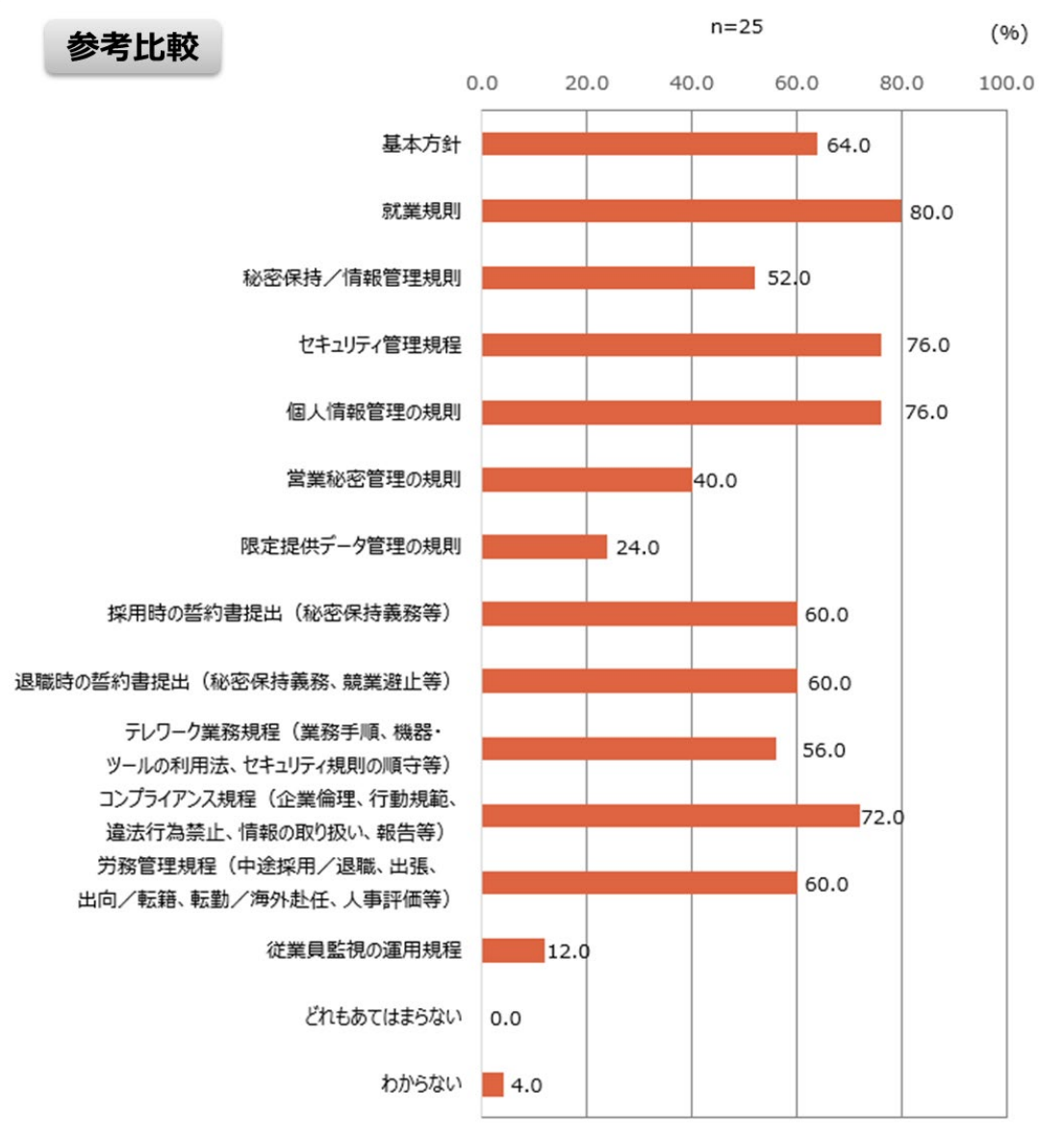
図表 17 内部不正に関わる社内規程の組織全体への浸透状況

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＞

（図表 17 の続き）

（ご参考：日経平均銘柄企業25社の集計）



【検証したい仮説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

内部不正防止に関わる法制度の知識が、企業の内部不正対策を担当する部署にどの程度蓄積されているかについて、その実態を調査した。パネルモニターのアンケート回答の単純集計結果を図表 18 に示した。

内部不正対策を所管する担当部署としては、個人情報保護法、不正競争防止法、不正アクセス防止法等の関連知識を十分に蓄積しておくことが望ましいと言える。しかし実際には、一番

蓄積が進んでいるはずの個人情報保護法に関する知識でも、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。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。

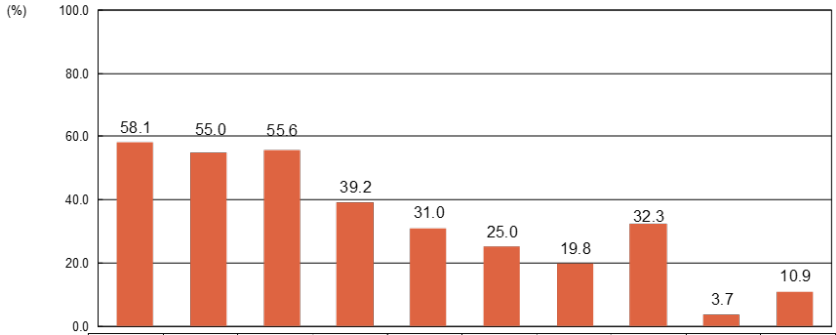
参考までに、ほとんどが大企業である日経平均銘柄企業の回答と比較してみると、法制度全般に亘って回答が底上げされており、企業が目指すべき理想的な水準の目安を示唆していると考えることができる。しかし、それでも担当部署が不正競争防止法の知識を蓄積していると回答した企業の割合が 60%程度に留まっており、この率がもう少し上がることが望ましい。

図表 18 内部不正対策を所管する部署に蓄積されている法制度の知識

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＞

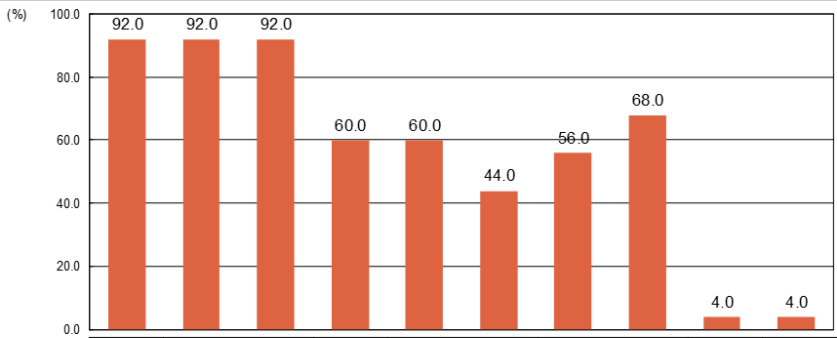
主たる回答



	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

（ご参考：日経平均銘柄企業25社の集計）

参考比較



	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	25	92.0	92.0	92.0	60.0	60.0	44.0	56.0	68.0	4.0	4.0

【検証したい仮説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

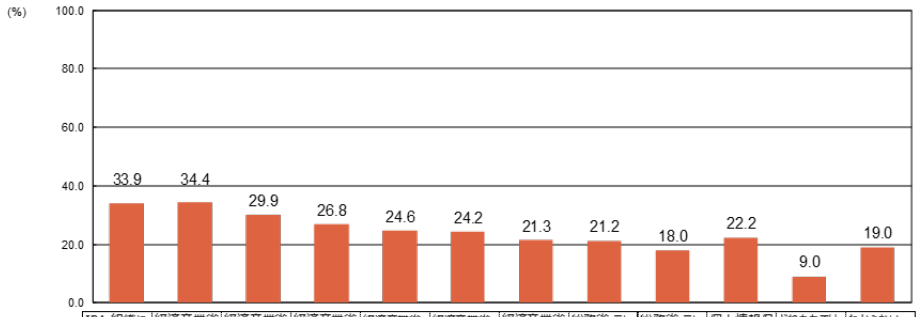
内部不正防止に関連するガイドライン等の知識が、企業の内部不正対策を担当する部署にどの程度蓄積されているかについて、その実態を調査した。パネルモニターのアンケート回答の単純集計結果を図表 19 に示した。関連するガイドライン全般に亘り、内部不正対策の担当部署における必要知識の蓄積状況は 40%未満に留まっており、まだ改善の余地がある。従って、仮説が示す通り、関連するガイドライン等についての知識はまだ不足しているものと考えられる。

図表 19 内部不正対策を所管する部署に蓄積されている関係ガイドライン等の知識

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＞

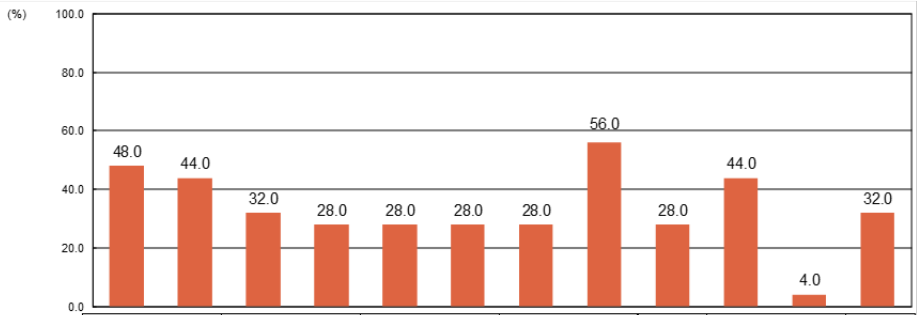
主たる回答



	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 ―データ利活用の共創が生み出す新しい価値―	経済産業省 データ利活用のてびき ― 正しいデータ利活用で新たな価値を生み出そう！―	経済産業省 データ利活用の事例集 ―データ利活用のポイント集 別冊―	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

（ご参考：日経平均銘柄企業25社の集計）

参考比較



	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 ―データ利活用の共創が生み出す新しい価値―	経済産業省 データ利活用のてびき ― 正しいデータ利活用で新たな価値を生み出そう！―	経済産業省 データ利活用の事例集 ―データ利活用のポイント集 別冊―	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	25	48.0	44.0	32.0	28.0	28.0	28.0	28.0	56.0	28.0	44.0	4.0	32.0

他方で、内部不正防止ガイドラインや経済産業省秘密情報の保護ハンドブックについての知識が担当部署に蓄積されているという回答の割合が 30%を超えている点、その他のガイドライン等についても回答割合が 20%を超えているものがほとんどである点については、想定よりも高い結果になっているため、参考までに日経平均銘柄企業からの回答と比較してみた。この対比では一部のガイドライン等を除いて回答割合が同程度のものが多く見られた。パネルからの募集に応えた回答者は情報漏えいや内部不正に関心がある方が多いと考えられることに加えて、所属部署や業務内容で回答者を絞り込んだこともあり、内部不正防止に対する経験・知見が豊富な回答者の割合が高くなっている可能性があり、これが回答割合を押し上げたものと推察される。

【検証したい仮説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

情報漏えい／セキュリティリスクに関する知識が、企業・組織においてどの程度広く認知されているかについて、その実態を調査した。パネルモニターのアンケート回答の単純集計結果を図表 20 に示した。

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仮説が示唆している通りまだ十分とは言えない状況である。参考までに日経平均銘柄企業からの回答を見てみると、「組織全体で知られている」という回答の割合は概ね底上げされており、企業が目指すべき理想的な水準の目安を示唆していると考えることができる。但し、「サイバー攻撃、だましの手口」については、日経平均銘柄企業はパネルモニターよりも、リスクに関する知識を組織全体で知っておくべきと考えている割合がかなり高くなっている。また、「クラウドセキュリティのあいまいな責任分担」については、日経平均銘柄企業はパネルモニターとは異なり、リスクに関する知識の蓄積を「対策の担当者」に委ねる傾向が強く出ていて興味深い。

図表 20 情報漏えい／セキュリティリスクに関する知識の組織全体への浸透状況

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＞

主たる回答 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%

（ご参考：日経平均銘柄企業25社の集計）

参考比較 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	25	44.0%	56.0%	0.0%	0.0%
サイバー攻撃、だましの手口	25	88.0%	12.0%	0.0%	0.0%
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	25	52.0%	48.0%	0.0%	0.0%
サプライチェーンにおける不必要な重要情報の授受	25	52.0%	44.0%	0.0%	4.0%
クラウドセキュリティのあいまいな責任分担	25	24.0%	60.0%	4.0%	12.0%
テレワークの不十分なセキュリティガバナンス	25	64.0%	36.0%	0.0%	0.0%
プライバシーを侵害する従業員監視	25	28.0%	28.0%	28.0%	16.0%
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	25	8.0%	60.0%	16.0%	16.0%
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	25	36.0%	48.0%	4.0%	12.0%

③内部不正防止に取り組む組織的体制の実態

重要情報漏えいに関する内部不正防止への対応は、サイバーセキュリティ／情報漏えいや内

部統制（IT 統制等）への対応の一部分として位置づけられ、必ずしも企業・組織の優先順位が高くないことが懸念されている。ここでは、この懸念が内部不正防止に取り組む組織的体制の整備の遅れや経営層の意識の低さに繋がっていないかを明らかにするため、次の 5 つの観点から仮説を構築してその検証を試みた。

i. 経営層の情報発信
ii. 組織全体としての責任・権限
iii. 社内ポリシー／規定の整備
iv. 内部不正防止に必要なリソース配分
v. 内部不正対策に関するマネジメントシステム

【検証したい仮説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

経営層が、「従業員が内部不正防止についての情報発信であると認識できる形」で内部不正防止の取組方針等について周知・指示しているかについて、実態を調査した。パネルモニターのアンケート回答の単純集計結果を図表 21 及び図表 22 に示した。

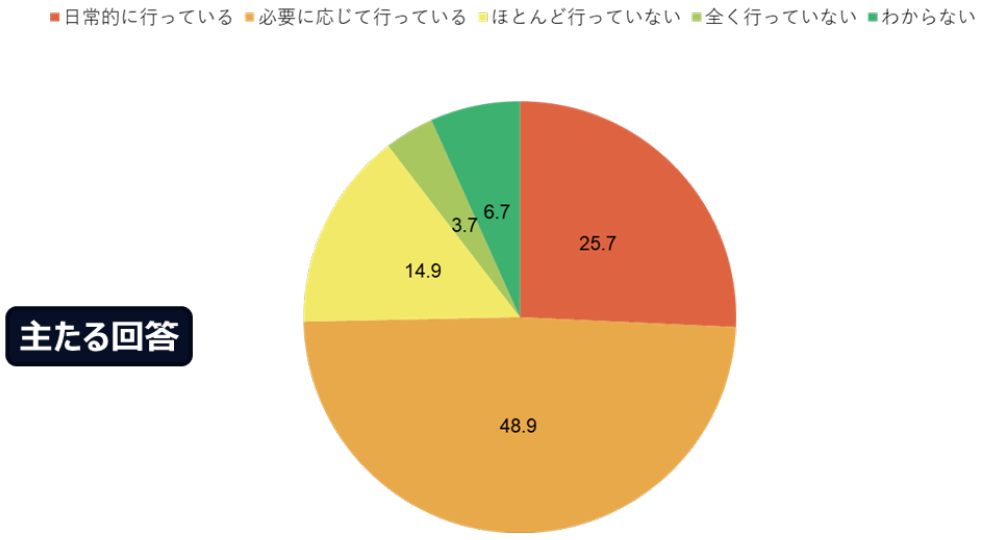
図表 21 によると、経営層が行う情報発信において従業員が「内部不正防止の取組方針等の周知・指示」を特定し、認識している割合は約 75%に及んでおり、「経営層の情報発信が明確ではない、または不十分な企業が多い」という仮説は必ずしも実態とは合っていないことが分かる。参考までに日経平均銘柄企業からの回答を見てみると、従業員が日常的に経営層の発信を認識している割合がさらに増えており、パネルモニターからの回答と対比して違和感はない。

一方、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、内部不正防止に特化した情報発信でないため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する結果となっている。

図表 21 経営層による内部不正防止の取組方針等についての周知・指示の状況

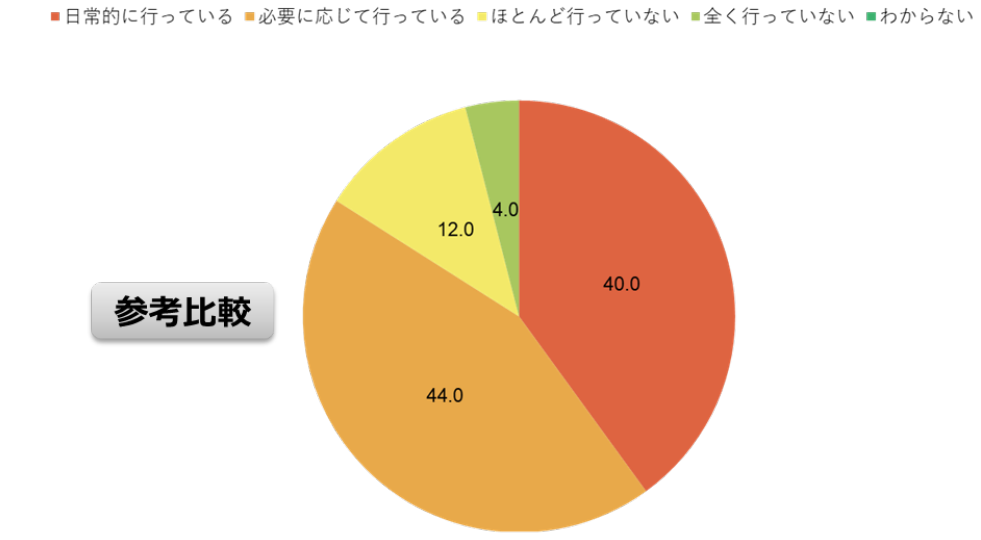
Q18.経営層は、組織全体での内部不正防止の取組み方針等について、
全従業員に周知、指示していますか。

＜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

（ご参考：日経平均銘柄企業25社の集計）



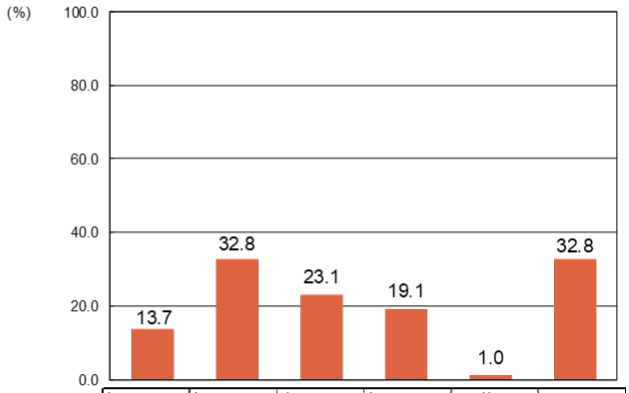
	n=	日常的に行っている	必要に応じて行っている	ほとんど行っていない	全く行っていない	わからない
TOTAL	25	40.0	44.0	12.0	4.0	0.0

図表 22 経営層が内部不正防止の取組方針等についてほとんど周知・指示していない等と感じる理由

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＞

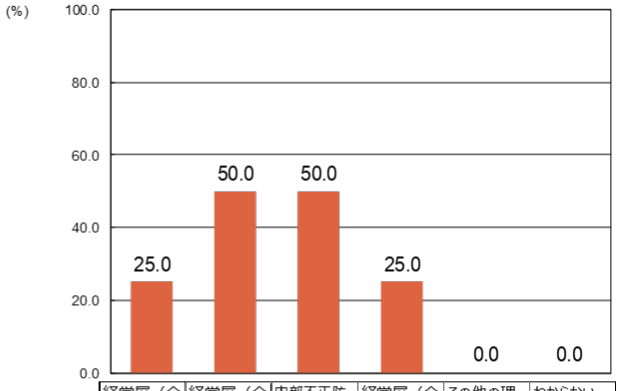
主たる回答



	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

（ご参考：日経平均銘柄企業25社の集計）

参考比較



	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	4	25.0	50.0	50.0	25.0	0.0	0.0

【検証したい仮説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

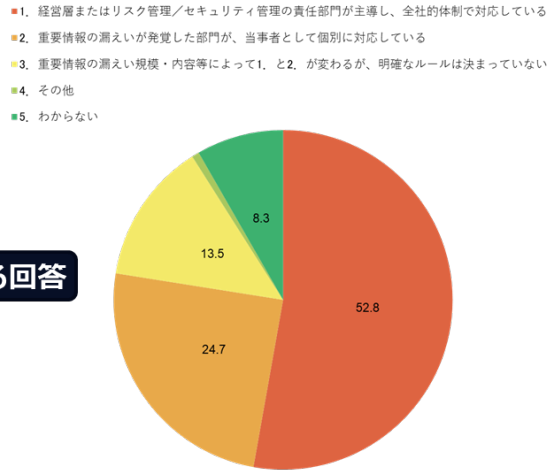
この仮説について検証するために、まず企業・組織が組織全体として重要情報の漏えいに取り組む体制になっているかについて実態を調査した。パネルモニターのアンケート回答の単純集計結果を図表 23 に示した。調査結果からは、重要情報漏えいへの対応を全社的組織体制で掌握できている企業の割合は半数に過ぎず、現場組織の個別対応がかなり残っていることが分かる。この結果は重要情報の漏えいに関する内部不正においても現場が個別に対応するケースがある程度見込まれることを示唆しており、組織全体としての責任・権限が明確になっていないことが懸念される。参考までに、ほとんどが大企業である日経平均銘柄企業の回答を見てみると、重要情報漏えいへの対応のほとんどが責任部門の主導による全社的体制によって実施されており、これが目指すべき姿を示しているものと考えられる。

図表 23 重要情報が漏えいした時の組織的対応の体制

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＞

主たる回答



	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

（ご参考：日経平均銘柄企業25社の集計）

参考比較

	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	25	96.0	0.0	4.0	0.0	0.0

次に、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を調査したところ、回答は概ね「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であると懸念されるその他の回答の割合は少ない。（図表 24 参照）

この結果を分析するにあたっては、内部不正対策に関する責任・権限を次の２つに仕分けすることが有効であると考えられる。

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

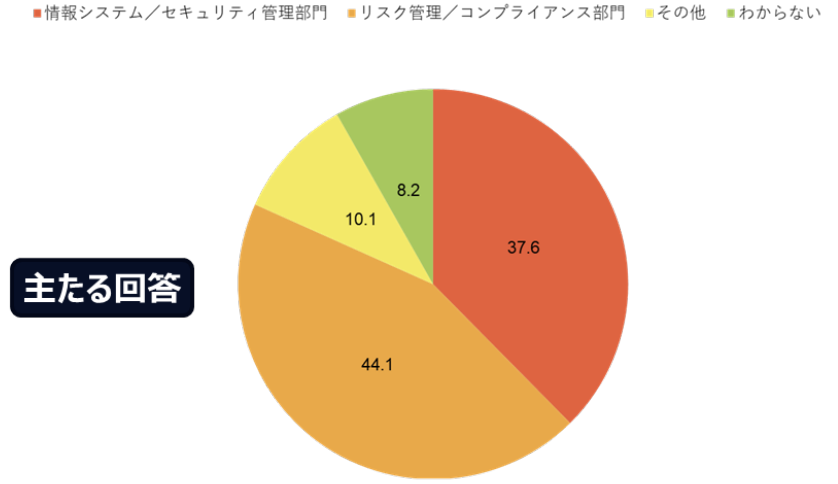
情報システム／セキュリティ管理部門が組織全体に対する責任・権限を持つ場合は、上記の２つの責任・権限を両方とも集約しているものと考えられる。一方、リスク管理／コンプライアンス部門が責任・権限を持つ場合は、当該部門は組織全体に対して ii を有しており、i を有する情報システム／セキュリティ管理部門を牽制できる体制になっていると言える。リスク・コンプライアンスのリソースが比較的厚い大企業においてはどちらかというとリスク管理／コンプライアンス部門が内部不正防止を主管する方が全社的な統制が効きやすく、企業規模が小さくなると情報システム／セキュリティ管理部門が主管する方が簡潔で実務運用がしやすくなることが考えられる。参考までに、ほとんどが大企業である日経平均銘柄企業の回答を見てみると、「リスク管理／コンプライアンス部門が組織全体に対する責任を負っている」という回答が 80%に達している。

以上の検討を考慮すると、「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」という仮説は必ずしも実態を反映しておらず、むしろ仮に２つの部門が上記２つの責任・権限を分担する形になっていなくても、１つの部門が２つの責任・権限の両方を備えて全社的に対応できることの方が重要であると考えられる。

図表 24 内部不正対策の主管部門

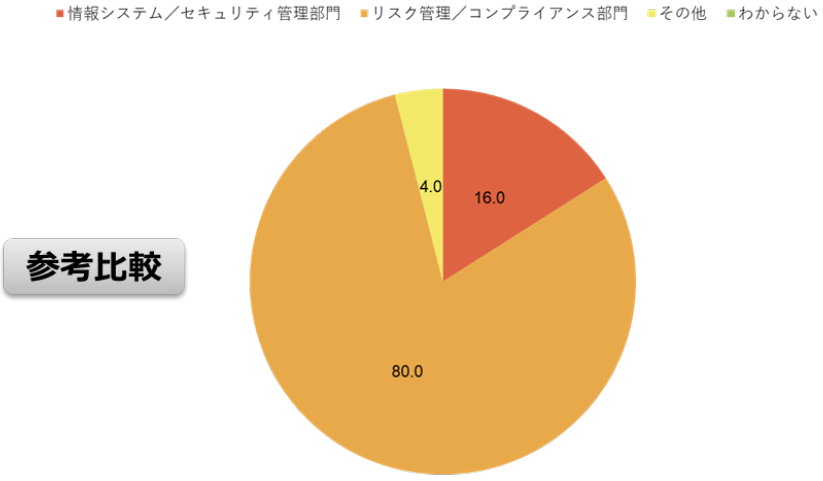
Q20. 貴社において内部不正防止対策を主管し、組織全体に対する責任を負っている部門はどこですか。

＜パネルモニターが所属する企業のみの集計＞



	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）



	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

次に、内部不正対策の主管部門と関連部門の連携について実態を調査した。パネルモニターのアンケート回答の単純集計結果を図表 25 に示した（母数から Q20 で「わからない」の 97 件を除外）。

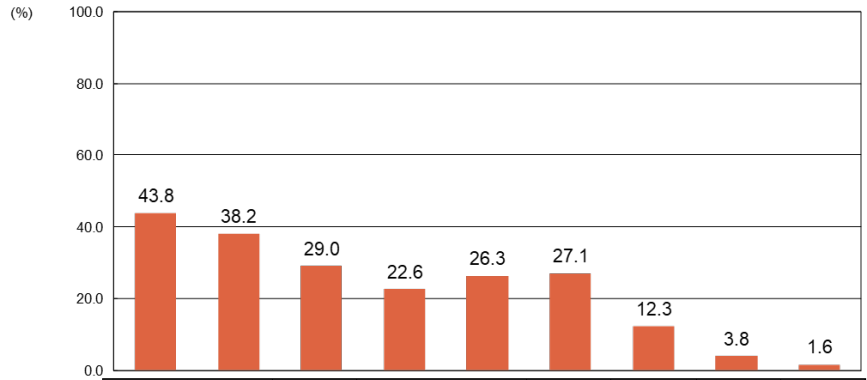
結果を見ると主管部門との連携については全般に底上げが必要であるものの、雇用・労務管理・リテラシー教育等で重要な役割を果たす人事・教育部門、個人情報・営業秘密の管理やサプライチェーン対応等で重要な役割を果たす法務・知財部門との連携は少し進展していると言える。他方で、重要情報を実際に取扱うことが多い事業部門／営業部門との連携は必ずしも進んでおらず、リテラシー教育にも力を入れつつ、主管部門との連携をさらに強化する必要がある。

図表 25 内部不正対策の主管部門と連携して対策や事後対応にあたる関連部門

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＞

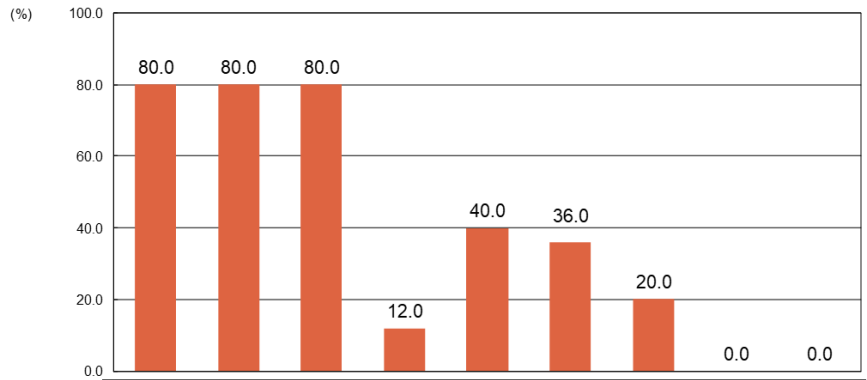
主たる回答



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

（ご参考：日経平均銘柄企業25社の集計）

参考比較



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 25	80.0	80.0	80.0	12.0	40.0	36.0	20.0	0.0	0.0

【検証したい仮説③－３】
社内ポリシー／規定の整備が不十分な企業が多い

この仮説について検証するために、企業・組織が内部不正防止についてどのような指針・規則を定めているかの実態を調査した。パネルモニターのアンケート回答の単純集計結果を図表 26 に示した。

日経平均銘柄企業の回答を参考にすると、60%以上の企業・組織が基本方針、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の主要な規則を定めている状態が当面の到達目標と想定できるが、パネルモニターの回答ではどの方針・規則もその水準に到達していない。従って仮説が示す通り、内部不正に関する社内ポリシー／規定の整備はまだ不十分な企業が多いのが実状であり、全般に底上げが必要な状況であると言える。

個別に見ていくと、まずパネルモニターの回答では「内部不正防止だけで独立した基本方針」を定めているとした割合が 30%を超えているが、これは内部不正だけで独立した基本方針を定めている企業はほとんどないという元々の想定と合わない。日経平均銘柄企業の方ではこの回答割合は 8%しかなく、こちらの方が実態に近いものと考えられる。

次にパネルモニターの回答では、「重要情報の取り扱いに関する規則類」を定めていると答えた割合が 30%にも達しておらず、かなり低くなっている。重要情報を的確に特定してラベル付けすることは情報漏えい防止の基本であり、企業・組織においてしっかりとした取り組みが求められているが、現状はかなり不十分な実態となっている。参考までに日経平均銘柄企業の回答を確認すると、これらの規則類を定めていると答えた割合は約 50-70%に達している。

個人情報管理と営業秘密管理に関する規則の策定状況を比較してみるとそれぞれの割合が 37%と 24%であり、個人情報管理の方が規則の策定率がかなり高くなっている。この回答傾向は日経平均銘柄企業でも共通しており、企業規模等に拠らず広く当てはまるものと考えられる。また、「営業秘密管理のための規則」を定めている企業の割合は日経平均銘柄企業の回答であっても 45%に達しておらず、パネルモニターの回答との差は小さい。このことから、営業秘密管理の規則策定の現状は大企業も含めてまだ不十分な実態であると推定される。

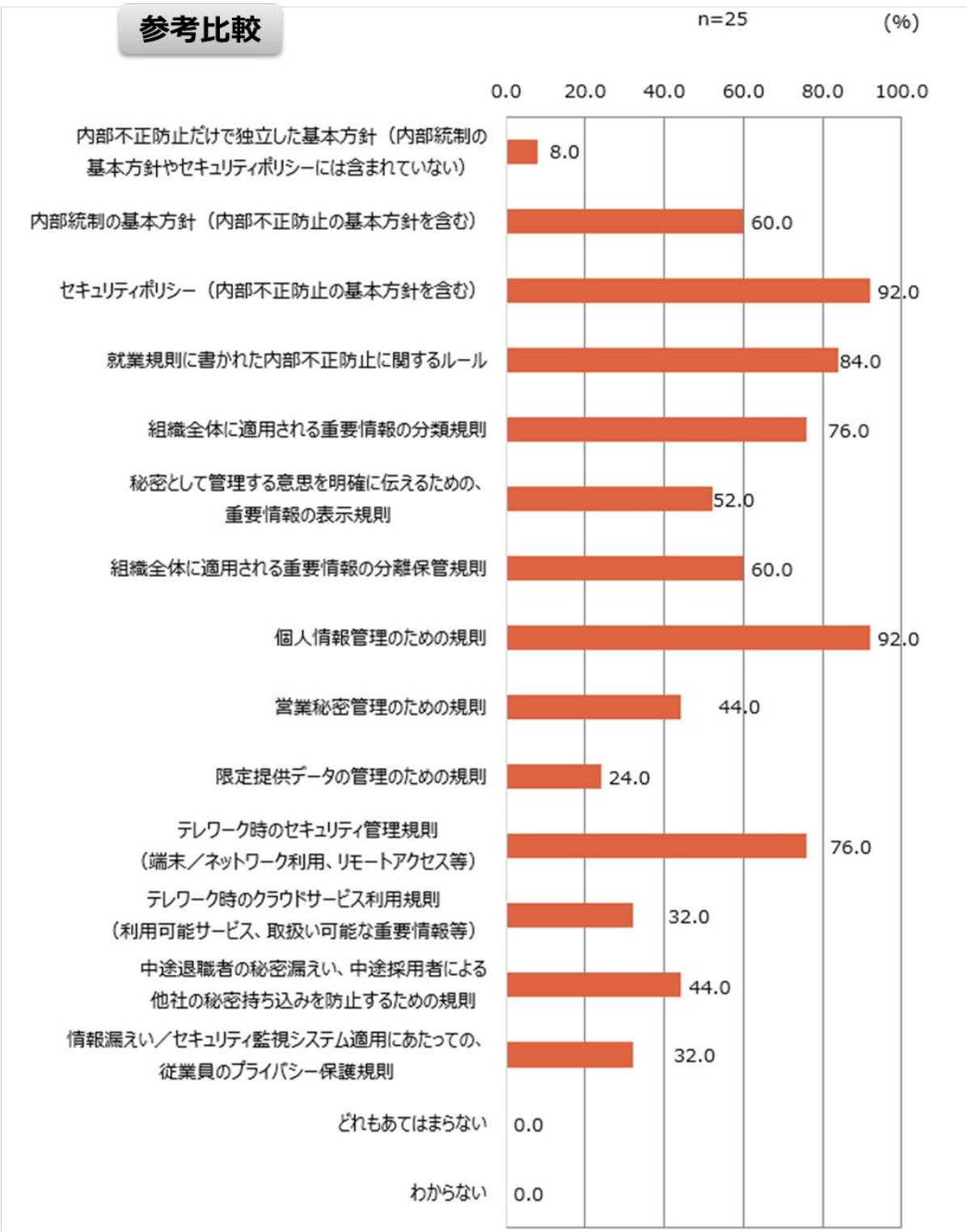
これと同様に、「テレワーク時のクラウドサービス利用規則」を定めている企業の割合がパネルモニターと日経平均銘柄企業の両方の回答で共通して低くなっており、業務で利用可能なクラウドサービスを制限している企業が多い実態を反映していない。これについては、「テレワーク時」に限定して質問したことが影響しているものと推定され、単に「クラウドサービス利用規則」について尋ねておけば、定めているという回答がかなり増加したものと考えられる。

図表 26 内部不正防止について定めた指針・規則

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＞

（図表 26 の続き）

（ご参考：日経平均銘柄企業25社の集計）



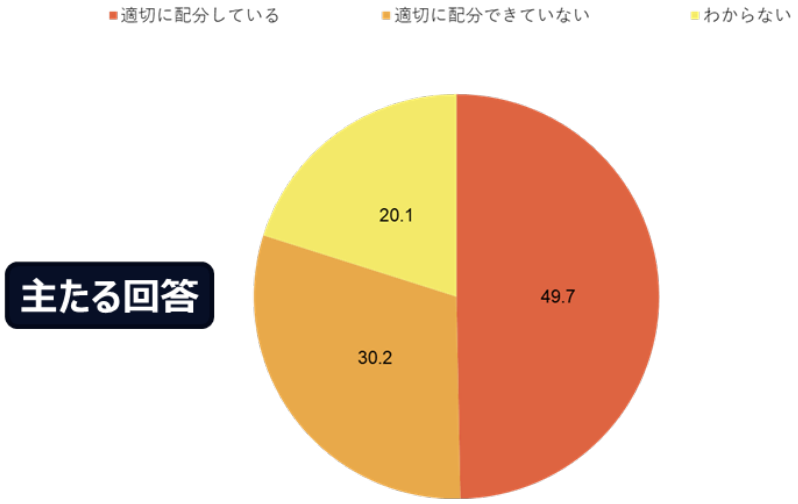
【検証したい仮説③－４】
経営層がリソースを適切に配分できていない企業が多い

この仮説を検証するために、経営層が内部不正防止に必要なリソースを適切に配分しているかの実態を調査した。パネルモニターのアンケート回答の単純集計結果を図表 27 に示した。「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ことが分かった。

図表 27 経営層による内部不正防止に必要なリソースの配分状況

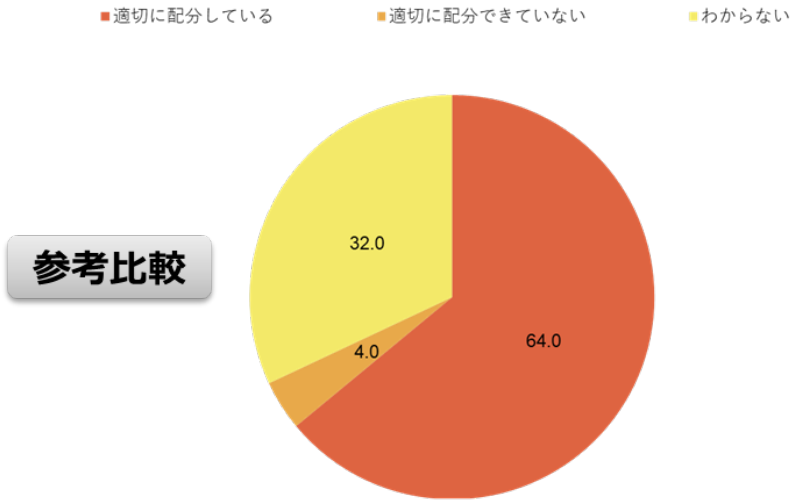
Q22. 経営層は、内部不正防止に必要なリソース（予算、人材、施設・設備等）を適切に配分していますか。

＜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

（ご参考：日経平均銘柄企業25社の集計）



	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	25	64.0	4.0	32.0

【検証したい仮説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

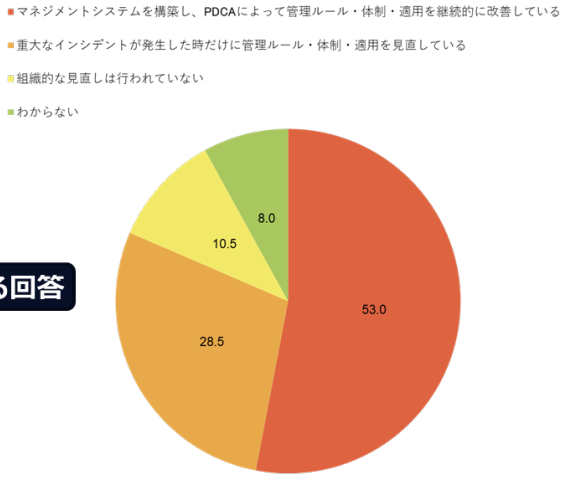
この仮説を検証するために、企業・組織が PDCA を回すことで重要情報の管理ルール・体制・適用を実効的・継続的に改善しているかの実態を調査した。パネルモニターのアンケート回答の単純集計結果を図表 28 に示した。「マネジメントシステムを構築し、PDCA によって管理ルール・体制・適用を継続的に改善している」を選択した回答者が 50%を超えており、実態として内部不正を含む重要情報漏えい対策のマネジメントシステムが機能している企業の割合は比較的高い水準に達していることが分かった。

図表 28 重要情報の管理ルール・体制・適用の見直し方法

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。

＜パネルモニターが所属する企業のみの集計＞

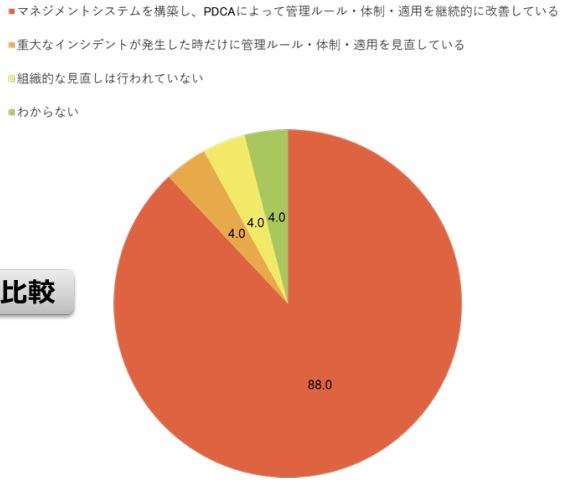
主たる回答



	n=	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

（ご参考：日経平均銘柄企業25社の集計）

参考比較



	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	25	88.0	4.0	4.0	4.0

また、企業・組織が内部不正防止対策のマネジメントシステムを構築、運用しているかについても実態を調査した。パネルモニターのアンケート回答の単純集計結果を図表 29 に示した。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。日経平均銘柄企業の回答を参考にすると、この回答率が少しでも 70%に近付くことが望ましいと言える。他の選択肢についても概ね底上げが必要な状況である。

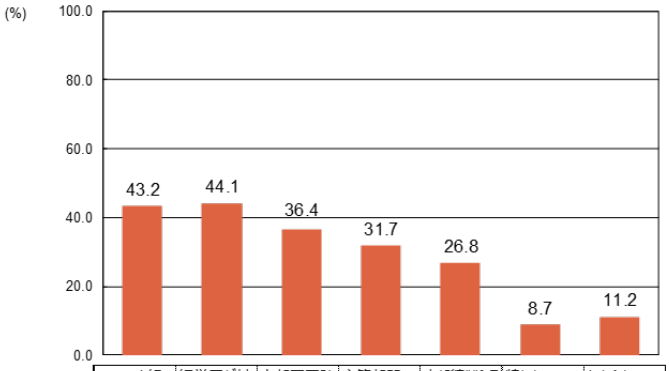
これらの結果から、仮説が示す通り、内部不正対策に関するマネジメントシステムが十分に機能していない企業がまだ多いと考えられるものの、重要情報の漏えい対策まで視野を広げるとマネジメントシステムが機能している企業の方が多いという実状であることが分かった。

図表 29 内部不正防止対策のマネジメントシステムの現状

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＞

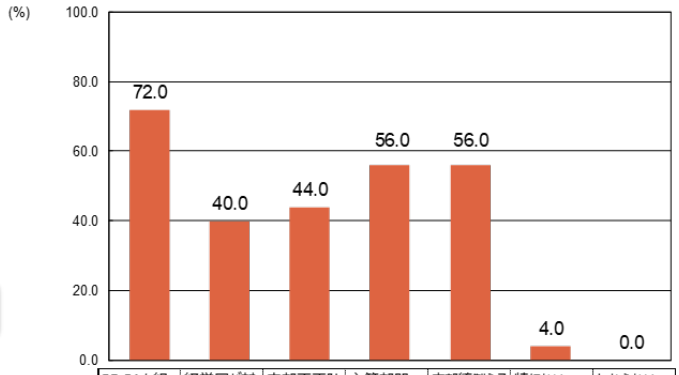
主たる回答



	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

（ご参考：日経平均銘柄企業25社の集計）

参考比較



	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	25	72.0	40.0	44.0	56.0	56.0	4.0	0.0

【検証したい仮説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

この仮説を検証するために、企業・組織がテレワークを行う従業員を支援し、内部不正を行う

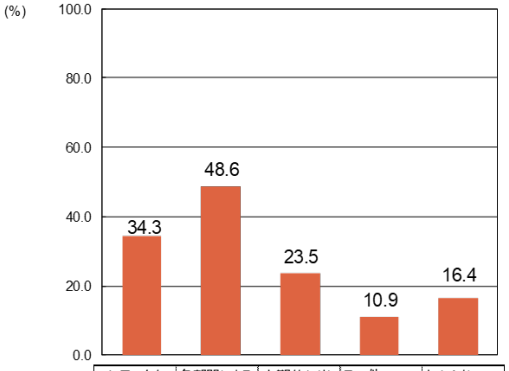
気にさせないための対策を講じているかの実態を調査した。パネルモニターのアンケート回答の単純集計結果を図表 30 に示した。

図表 30 テレワークを行う従業員に内部不正の動機を与えないための環境整備の現状

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＞

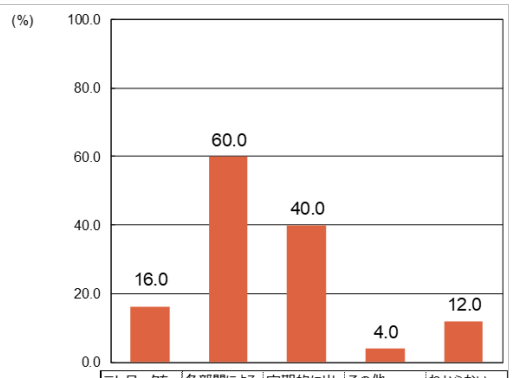
主たる回答



	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

（ご参考：日経平均銘柄企業25社の集計）

参考比較



	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	25	16.0	60.0	40.0	4.0	12.0

その結果に基づくと、企業・組織が最も重点を置いて実施している対策は「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」であることが分かった。この対策を実施しているとした回答の割合はほぼ 50%に達している。参考までに、日経平均銘柄企業の回答を見てみると、回答率は 60%であり、概ね望ましい水準に近付いているとは言えるが、それでもまだ少しの乖離が残っているものと考えられる。以上のことから、「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」という仮説は必ずしも実態と合っていないことが分かった。

④組織全体への周知・教育の実態

ここでは、企業・組織の内部不正防止の対応に関する優先順位が必ずしも高くないことが、内部不正防止の教育の遅れに繋がっていないかを検証した。また、教育した内容が組織全体での実践に繋がっていくために必要な環境が整備されているかについても調査した。

【検証したい仮説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

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企業は、周知・教育を含めて内部不正防止に積極的に取り組んでいるのではないかと想定されるため、まずこうした経験をした企業がどの程度あるのかの実態を調査した。パネルモニターのアンケート回答の単純集計結果を図表 31 に示した。

その結果に基づくと、個人情報の漏えい事案／インシデントが最も多い（約 36%）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。他方で、日経平均銘柄企業の回答では、個人情報の漏えいが突出し、営業秘密や限定提供データの漏えいはかなり少ない。この理由としては例えば次のような可能性を想定できるが、具体的にどれが実態と合うのかについてはクロス集計の分析において後ほど説明する。

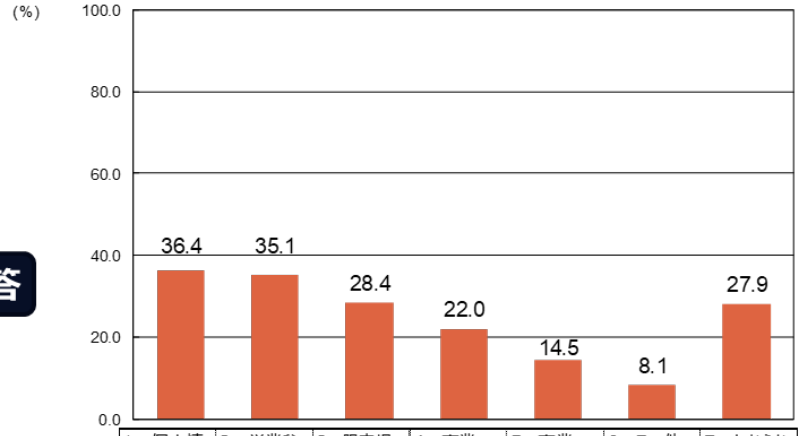
- 大企業の方が営業秘密／限定提供データの漏えい防止対策が成熟していること、
- 大企業の方が営業秘密／限定提供データの漏えい事案／インシデントの組織全体への周知に消極的であること
- パネルからの募集に応えた回答者は情報漏えいや内部不正に関心がある方が多いと考えられることに加えて、所属部署や業務内容で回答者を絞り込んだこともあり、内部不正防止に対する経験・知見が豊富な回答者の割合が高くなっている可能性があること

図表 31 内部不正事件等の経験状況

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＞

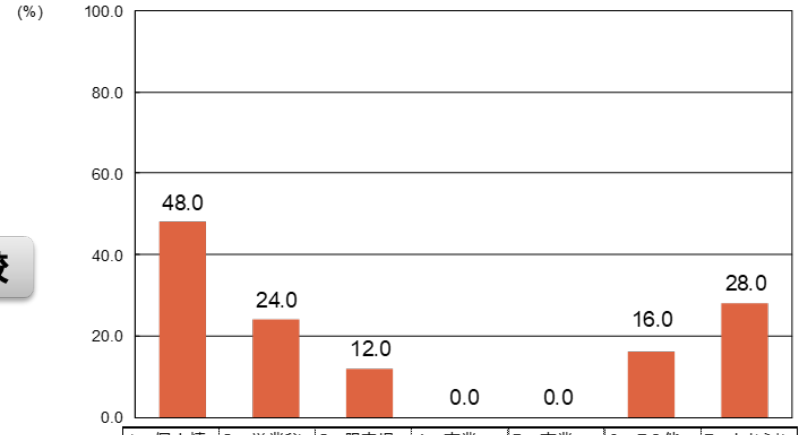
主たる回答



	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

（ご参考：日経平均銘柄企業25社の集計）

参考比較



	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	25	48.0	24.0	12.0	0.0	0.0	16.0	28.0

次に仮説を検証するため、重要情報の管理ルールの周知・徹底状況と内部不正防止についてのリテラシー教育の実施状況について実態を調査した。パネルモニターのアンケート回答の単純集計結果を、それぞれ図表 32 と図表 33 に示した。

重要情報の管理ルールの周知・徹底については、雇用開始時の教育、年次等の定期的な教育の実施割合は 50%を超えており、まずまずの状況ではあるが、日経平均銘柄企業の回答割合と比較すると、さらなる底上げが必要と考えられる。他方で、雇用終了時の重要情報等の返却・削除ルールの周知、重要プロジェクト開始／終了時の重要情報管理ルールの教育等については、仮説が示唆する通り、まだ不足している状態と言える。特に、重要プロジェクトの開始／終了時のルール教育については、日経平均銘柄企業の回答割合もかなり低くなっていることから、今後の課題として、好事例を周知する等のさらなる啓発を検討する必要がある。

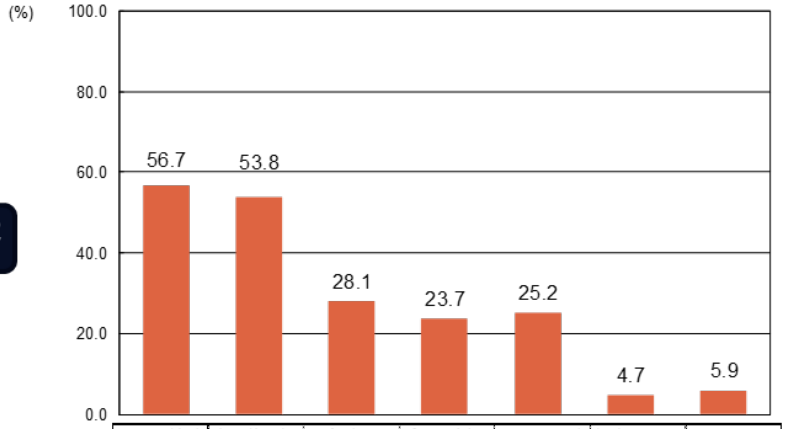
一方、内部不正防止に関するリテラシー教育については、組織全体で定期的に実施していると回答した割合は40%に満たず、まだ十分とは言えない実態を示している。また、組織全体で必要に応じて実施していると回答した割合が 30%を超えており、このことを考慮すると 70%近くが内部不正についてのリテラシー教育を実施していると回答している。参考までに日経平均銘柄企業の回答割合を見てみると、定期的に実施している企業は 75%に達しており、この回答割合が目指すべき水準を示唆していると考えることができる。

図表 32 重要情報の管理ルールの周知・徹底状況

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＞

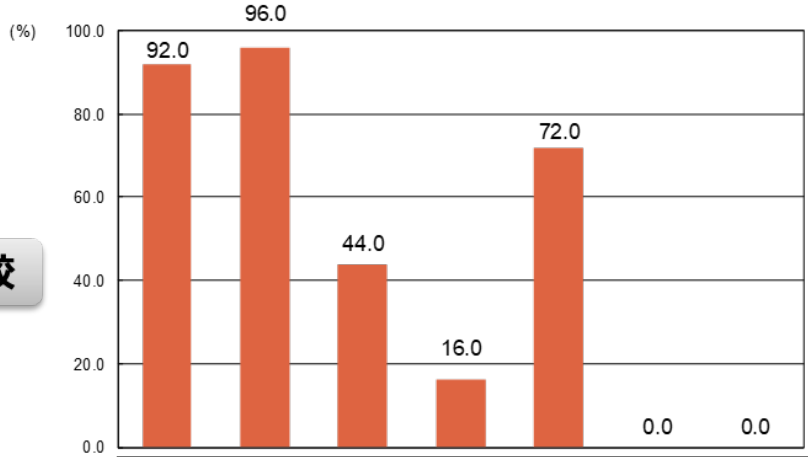
主たる回答



	n=	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

（ご参考：日経平均銘柄企業25社の集計）

参考比較

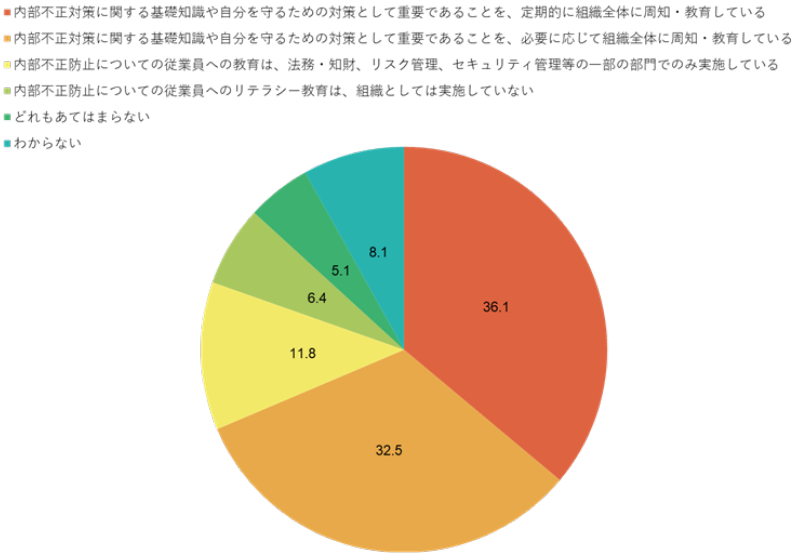


	n=	雇用開始時に、就業規則や誓約書等を通じて教育している	定期的な教育（例：毎年1度のeラーニング受講等）によって全社に周知・徹底している	異動時・昇進時等にルールを教育し直している	プロジェクトの開始、参加、終了時等にルールを教育し直している	雇用終了時の重要情報等の返却・削除ルールについて、教育で全社に周知・徹底している	教育による周知は実施していない	わからない
TOTAL	25	92.0	96.0	44.0	16.0	72.0	0.0	0.0

図表 33 内部不正防止についてのリテラシー教育の実施状況

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。

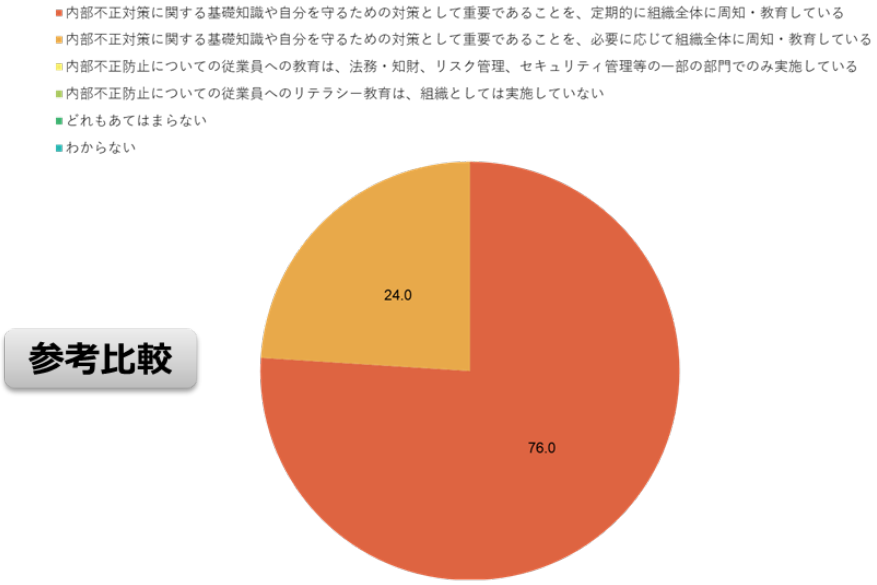
＜パネルモニターが所属する企業のみの集計＞



	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

（図表 33 の続き）

（ご参考：日経平均銘柄企業25社の集計）



	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	25	76.0	24.0	0.0	0.0	0.0	0.0

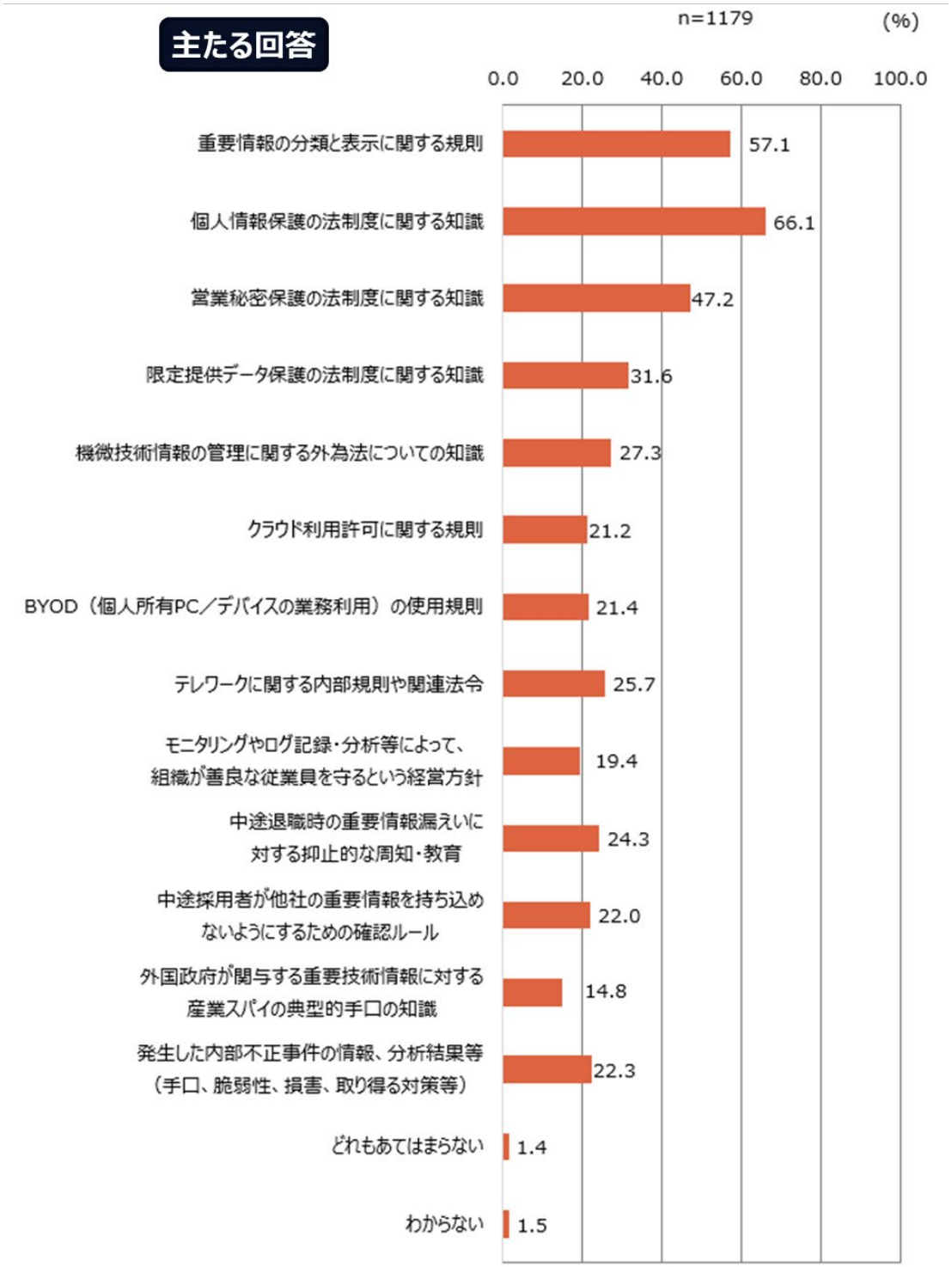
さらに、主題別に組織全体でのリテラシー教育の実施状況を調査した結果が図表 34 である。この結果を見ると、重要情報の分類と表示に関する規則、個人情報保護法の知識については、リテラシー教育を実施しているという回答の割合が 50%を超えており、「内部不正対策に関する周知・教育は不足している」という仮説は必ずしも実態を示していない。日経平均銘柄企業の回答と比較すると、これらの主題については回答割合 70%以上が目指すべき水準であると考えられる。他方で、日経平均銘柄企業の回答との対比から、クラウド利用許可に関する規則、テレワークに関する内部規則や関連法令についてのリテラシー教育は、回答割合が 60%を超える水準まで底上げすることが望ましい。

以上を総合すると、「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」という仮説は、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、概ね実態を表していると言うことができる。

図表 34 内部不正防止についてのリテラシー教育の実施内容

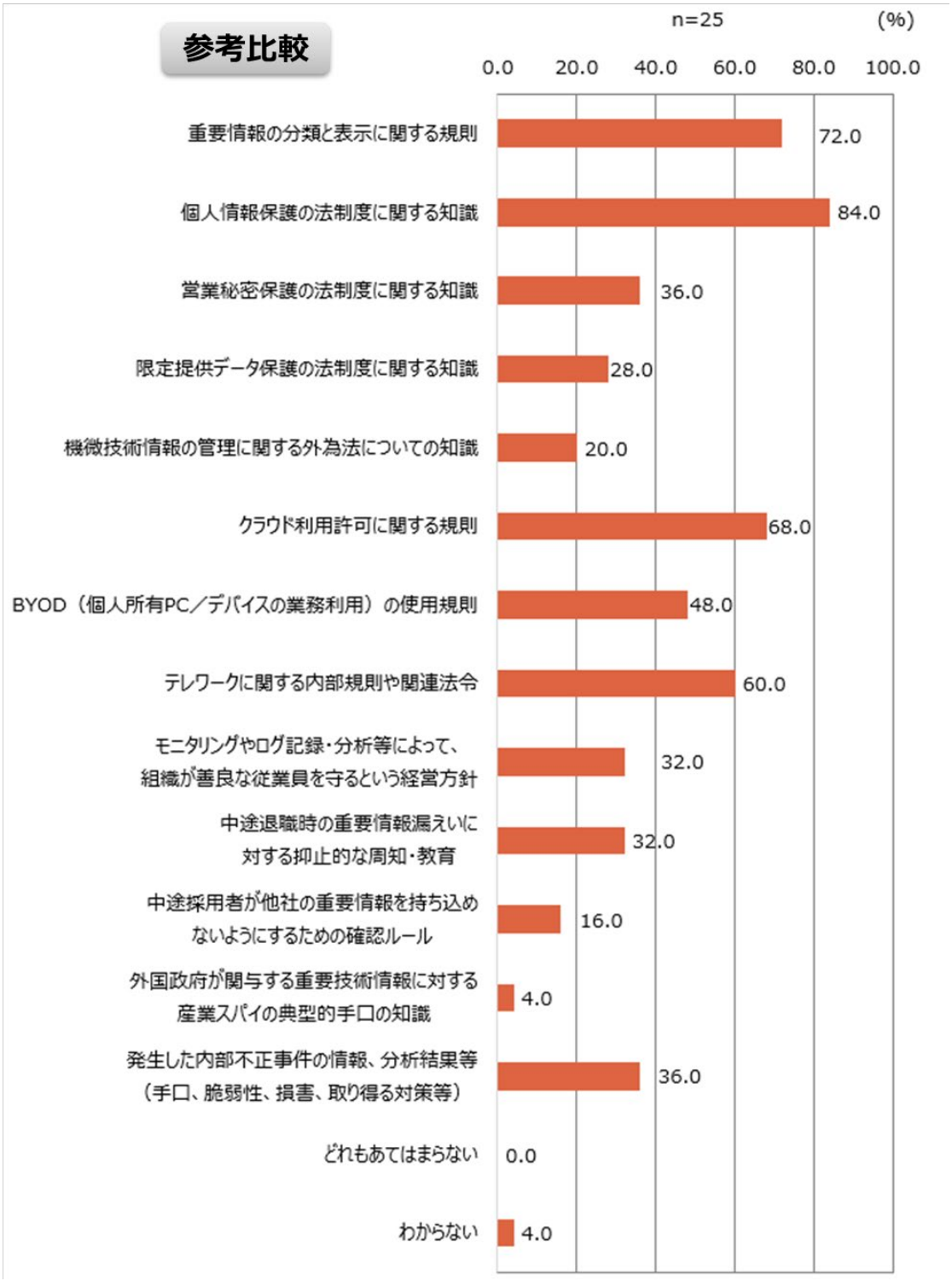
Q27. 貴社では内部不正防止についての従業員へのリテラシー教育において、具体的にどのような内容を周知・教育していますか。

＜パネルモニターが所属する企業のみの集計＞



（図表 34 の続き）

（ご参考：日経平均銘柄企業25社の集計）



【検証したい仮説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

この仮説を検証するために、内部不正防止のリテラシー教育の実効性と、教育が実践に繋がっていない理由について実態調査を行った。パネルモニターのアンケート回答の単純集計結果を図表 35 と図表 36 に示した。内部不正防止についてのリテラシー教育が組織全体での実践に寄与していると答えた回答者の割合は 70%に迫っており、十分に高い水準である。他方で、内部不正防止についてのリテラシー教育が組織全体での実践に寄与していない理由としては、組織的な対策やマネジメントが徹底していないという回答が多く見られた（図表 36 の母数は、Q28 で「いいえ」の回答数）。

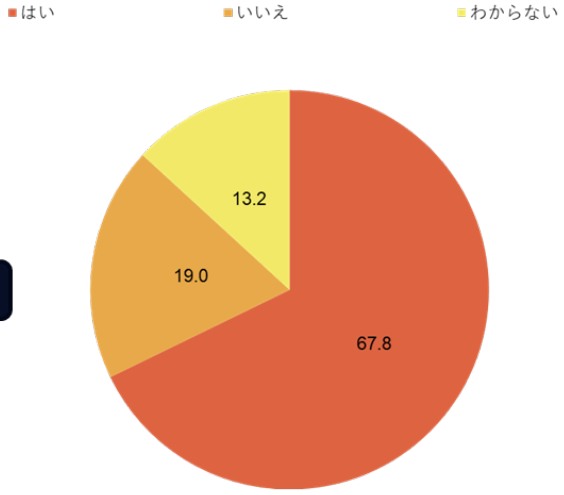
以上の結果を考慮すると、「内部不正対策を組織全体で実践できる環境が整っていない」という仮説は必ずしも実態と合っていない。また、内部不正対策やマネジメントの強化に組織全体で取り組むことで、リテラシー教育の実効性を高める環境を改善できると言える。

図表 35 内部不正防止についてのリテラシー教育の実効性

Q28. あなたは、内部不正防止のために周知・教育した内容が、組織全体での実践に寄与していると感じていますか。

＜パネルモニターが所属する企業のみの集計＞

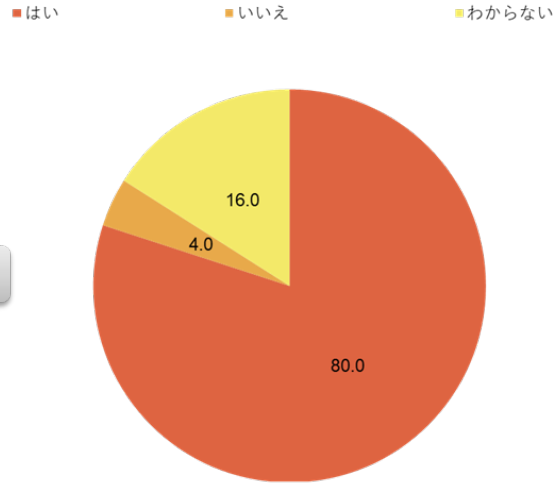
主たる回答



	n=	はい	いいえ	わからない
TOTAL	948	67.8	19.0	13.2

（ご参考：日経平均銘柄企業25社の集計）

参考比較



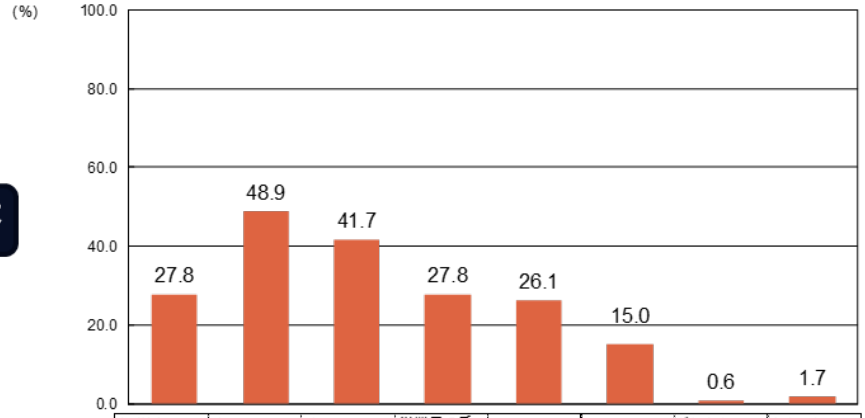
	n=	はい	いいえ	わからない
TOTAL	25	80.0	4.0	16.0

図表 36 内部不正防止についてのリテラシー教育が実践に寄与できていない理由

Q29. 周知・教育が組織全体の実践に寄与できていない理由は何だと考えていますか。

＜パネルモニターが所属する企業のみの集計＞

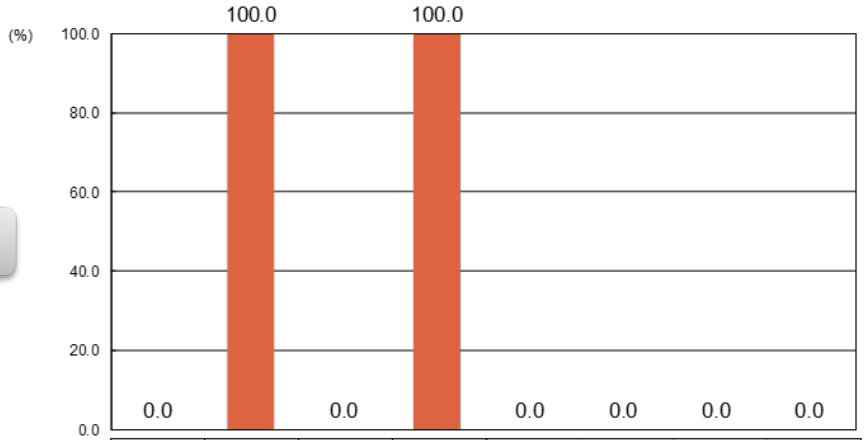
主たる回答



	n=	経営者のリーダーシップや従業員を守る姿勢が不足しているため	内部不正防止に関する組織的対策が徹底していないため	内部不正防止に関する組織マネジメントが徹底していないため	従業員の重要情報に対する認識が低く、情報漏えい対策の必要性を感じていないため	従業員の不満が蓄積しやすい職場環境であるため	従業員の、内部不正防止への対応スキルが十分ではないため	どれもあてはまらない	わからない
TOTAL	180	27.8	48.9	41.7	27.8	26.1	15.0	0.6	1.7

(ご参考：日経平均銘柄企業25社の集計)

参考比較



	n=	経営者のリーダーシップや従業員を守る姿勢が不足しているため	内部不正防止に関する組織的対策が徹底していないため	内部不正防止に関する組織マネジメントが徹底していないため	従業員の重要情報に対する認識が低く、情報漏えい対策の必要性を感じていないため	従業員の不満が蓄積しやすい職場環境であるため	従業員の、内部不正防止への対応スキルが十分ではないため	どれもあてはまらない	わからない
TOTAL	1	0.0	100.0	0.0	100.0	0.0	0.0	0.0	0.0

⑤内部不正防止の課題と対策の実態

今まで一貫して、重要情報漏えいに関する内部不正防止への対応が、サイバーセキュリティ／情報漏えいや内部統制（IT 統制等）への対応の一部分として位置づけられ、必ずしも企業・組織の優先順位が高くないのではないかという懸念を指摘してきた。ここでは、この懸念が内部不正対策へのリソース割り当てや対策実施の遅れに繋がっていないかを明らかにするため、次の観点から仮説を構築して検証を試みた。

i. 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
ii. 内部不正に対する具体的な対策や事後対策の選択の困難さ
iii. 重要技術情報・ノウハウ等の漏えいに対するリスク認識の不足
iv. ニューノーマル等の環境変化への対応の遅れ
v. 中途退職者／中途採用者の内部不正に対する対策整備の遅れ、未対応
vi. 内部不正を誘発しない職場環境の整備
vii. 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

【対策実施の現状（全体像の俯瞰）】

まず、企業・組織における内部不正対策実施の全体像を把握するため、内部不正防止ガイドラインを参考にして対策項目を幅広に列挙し、これに対する実施状況について調査を実施した。パネルモニターのアンケート回答の単純集計結果を図表 37 に示した。

全体を俯瞰してまず注目されるのは、回答割合が 50%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と言える。ここで、対象としている対策はリテラシー教育を受けた一般従業員が実践する対策というよりは、組織的・技術的に実施される内部不正対策が中心であるため、リテラシー教育やこれを実践できる環境の整備とは必ずしも連動していない。また、日経平均銘柄企業の回答と比較することで、次に示す対策は目指すべき水準として回答割合 60%～70%以上を目指すことが望ましいと言える。

- 経営層による内部不正対策の基本方針の策定、周知
- 経営層が従業員のプライバシー保護を明言
- 経営層が自ら必要なリソース確保を決定・指示
- 経営層が重要情報の範囲や条件を明確に定めて周知
- 組織全体における責任部門・責任者の明示
- 定期的／事故発生時のリテラシー教育実施
- テレワーク実施者に対する関連社内規程等の教育
- 退職後の速やかな ID／アクセス権限の削除
- 従業員の労務管理、人事管理、コミュニケーション管理

- ID 管理と本人認証の強化
- 重要情報に必要最小限の従業員しかアクセスできない管理
- 重要情報の棚卸しと不要な情報の削除
- 入退室管理、PC・デバイスの社外持出管理等
- 重要情報のアクセス監視・ログ記録と、抑止力としての組織全体への周知
- 会社支給 PC のテレワーク対策強化
- 業務で使用できるクラウドサービスの制限、クラウド上で扱うことができる重要情報の制限
- サプライヤーや委託業者と受け渡す情報の暗号化等
- サプライヤーとの契約に組み込む要件、モニタリング要件
- 内部不正事故等の情報の共有による心理的抑止力　等

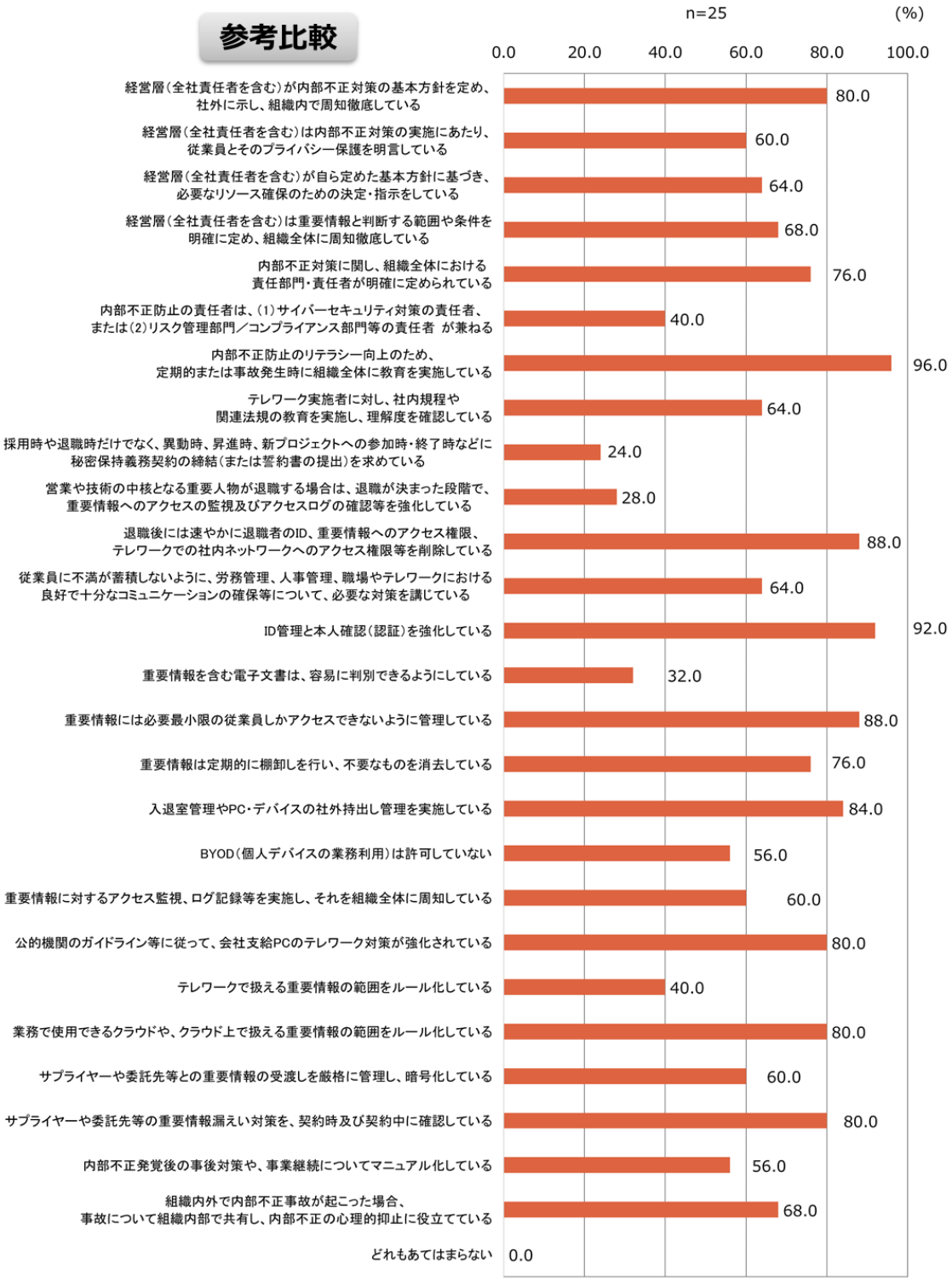
図表 37 内部不正防止対策の実施状況

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＞

（図表 37 の続き）

（ご参考：日経平均銘柄企業25社の集計）



【検証したい仮説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

この仮説を検証するために、経営層が内部不正リスクを重要な経営課題として捉えているかについて調査した。パネルモニターのアンケート回答の単純集計結果を図表 38 に示した。

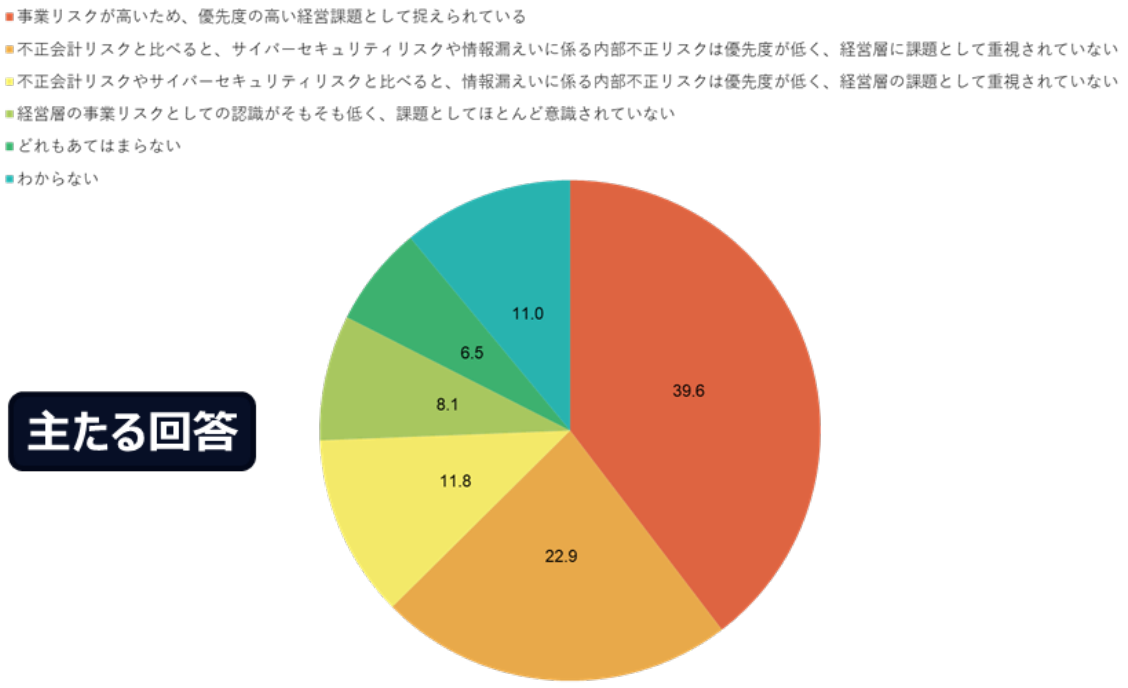
経営層が内部不正の事業リスクについて十分に認識し、優先度の高い経営課題として捉えていると答えた回答者の割合はほぼ 40%に留まっており、十分に高い水準に達しているとは言えない。これらの結果を考慮すると、「内部不正リスクは、経営リスクや事業リスクとしての優先度が高くない」という仮説は実態に合っていると言え、対策実施が後回しとなる恐れが十分にあるものと推察される。

なお、参考までに日経平均銘柄企業の回答を見てみると、回答割合は 60%を超えており、これが企業・組織が目指すべき水準を示唆しているものと考えられる。

図表 38 内部不正の事業リスクについての経営層の認識

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。

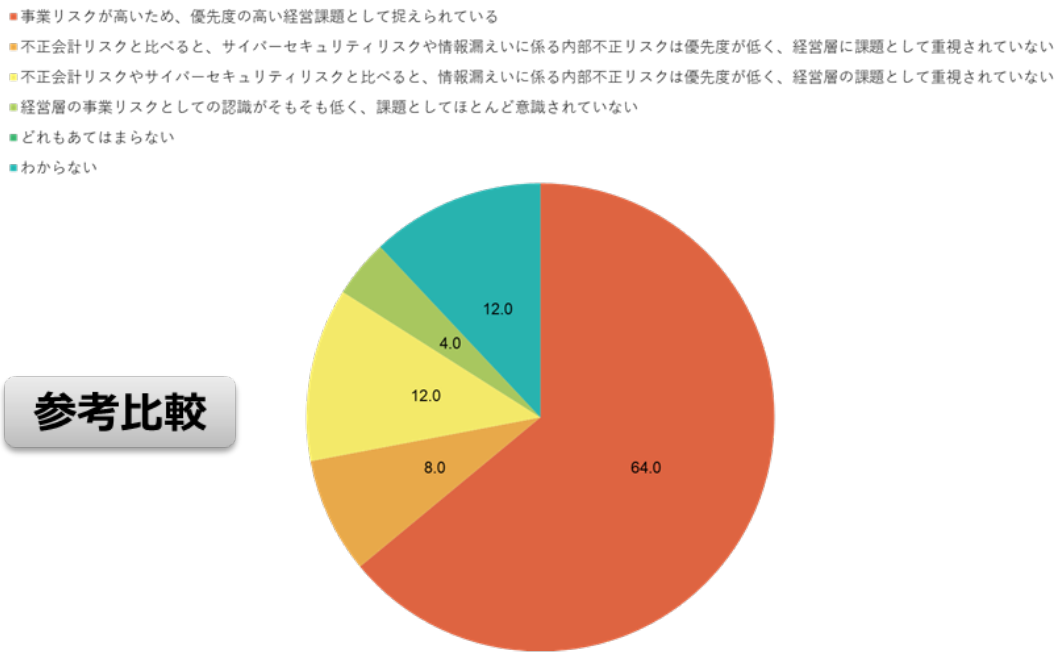
＜パネルモニターが所属する企業のみの集計＞



	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

（図表 38 の続き）

（ご参考：日経平均銘柄企業25社の集計）



	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

【検証したい仮説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

この仮説を検証するために、企業・組織が重要情報の管理ルールを具体的に適用し、運用できているかと、内部不正対策を具体的に選択する上での課題は何かについて、調査を実施した。パネルモニターのアンケート回答の単純集計結果を図表 39 と図表 40 に示した。

重要情報の管理ルールを詳しく定めて適用できていると答えた回答者の割合は 46%程度、詳しく定めるためにルールを改訂中と答えた回答者の割合は 24%程度となっており、両者を合算すると約 70%の企業・組織が重要情報の漏えいに関する内部不正に対して具体的な対策を選

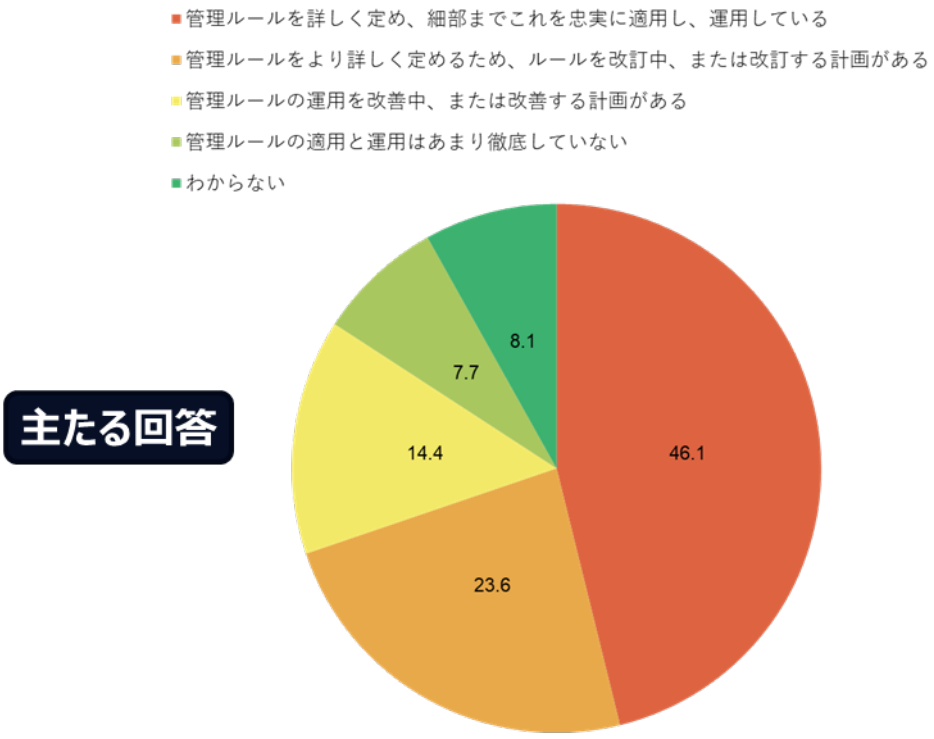
択できているものと考えられる。また、内部不正対策を具体的に選択する上での課題としては、組織内での関連知識や経験値の不足を指摘した回答者が最も多かったものの、回答割合は40%弱に留まっている。参考として日経平均銘柄企業の回答を見てみると、回答割合は 20%程度である。

以上の結果を考慮すると、「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」という仮説は必ずしも実態と合っていないと言える。

図表 39 重要情報の管理ルールの適用状況

Q8. 貴社では重要情報の管理ルールを厳格に適用していますか。

＜パネルモニターが所属する企業のみの集計＞

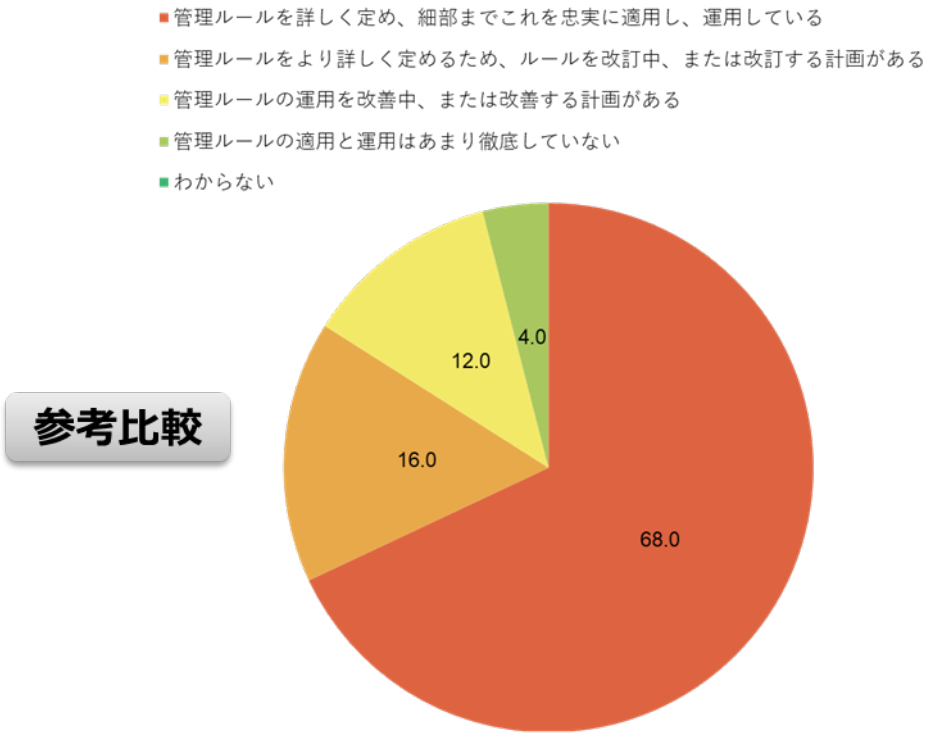


主たる回答

	n=	管理ルールを詳しく定め、細部までこれを忠実に適用し、運用している	管理ルールをより詳しく定めるため、ルールを改訂中、または改訂する計画がある	管理ルールの運用を改善中、または改善する計画がある	管理ルールの適用と運用はあまり徹底していない	わからない
TOTAL	1179	46.1	23.6	14.4	7.7	8.1

（図表 39 の続き）

（ご参考：日経平均銘柄企業25社の集計）



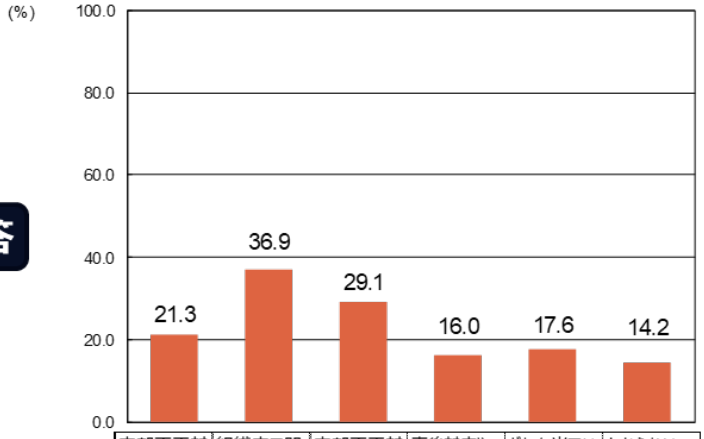
	n＝	管理ルールを詳しく定め、細部までこれを忠実に適用し、運用している	管理ルールをより詳しく定めるため、ルールを改訂中、または改訂する計画がある	管理ルールの運用を改善中、または改善する計画がある	管理ルールの適用と運用はあまり徹底していない	わからない
TOTAL	25	68.0	16.0	12.0	4.0	0.0

図表 40 内部不正防止対策を選択する上での課題の現状

Q31. 貴社では、内部不正防止対策を具体的に選択する上での課題は何ですか。

＜パネルモニターが所属する企業のみの集計＞

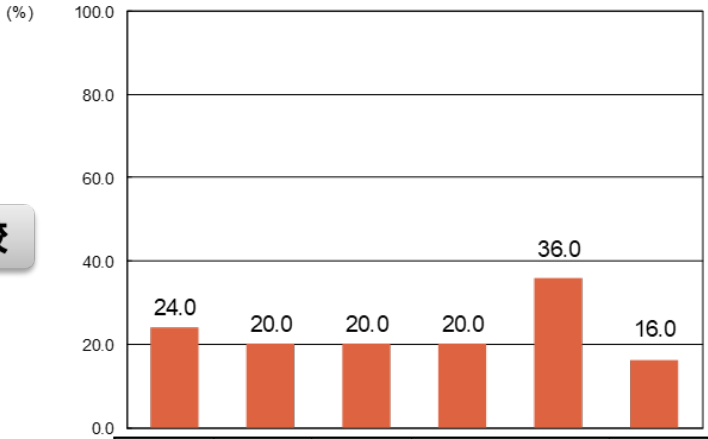
主たる回答



	n=	内部不正対策を対象としたベンダーソリューションが少なく、うまく選択できていない	組織内で関連知識や経験値が不足しており、対策を具体的に選定できていない	内部不正対策に対するマネジメントシステムがなく、課題の改善策をうまく選定できていない	事後対応や事業継続についての計画やマニュアルがなく、適切な対応策や法的措置を選択できない	どれも当てはまらない	わからない
TOTAL	1179	21.3	36.9	29.1	16.0	17.6	14.2

（ご参考：日経平均銘柄企業25社の集計）

参考比較



	n=	内部不正対策を対象としたベンダーソリューションが少なく、うまく選択できていない	組織内で関連知識や経験値が不足しており、対策を具体的に選定できていない	内部不正対策に対するマネジメントシステムがなく、課題の改善策をうまく選定できていない	事後対応や事業継続についての計画やマニュアルがなく、適切な対応策や法的措置を選択できない	どれも当てはまらない	わからない
TOTAL	25	24.0	20.0	20.0	20.0	36.0	16.0

【検証したい仮説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

この仮説を検証するために、個人情報以外に対しても重要情報として特定できる仕組みを有しているかと、個人情報以外の重要情報の漏えいに関する内部不正対策を実施できているかの実態について調査した。パネルモニターのアンケート回答の単純集計結果を図表 41 と図表 42 に示した。

まず、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を特定する仕組みを持っていると答えた回答者の割合は 45%前後である。他方で利活用する価値が高い重要データや他社から「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については、重要情報と特定できる仕組みを作っていると答えた回答者の割合は約 30%に過ぎない。これらを考慮すると、個人情報以外の重要情報を特定する仕組みを持つ企業は必ずしもまだ多くなく、全般に底上げが必要な状況と言える。参考までに日経平均銘柄企業の回答を見てみると、いずれも 60%を超えており、これが目指すべき到達点を示唆しているものと考えられる。

一方、個人情報以外の重要情報の漏えいに関する内部不正対策を実施できているかについては、重要技術情報・ノウハウや重要データにも対応できていると答えた回答者の割合は30%にも届いていない。従って、個人情報以外の重要情報の漏えいに関する内部不正対策の実施についても、全般に底上げが必要な状況である。ちなみに、日経平均銘柄企業の回答割合は50%を超えており、少なくともこの程度の水準は目指すべきであると言える。

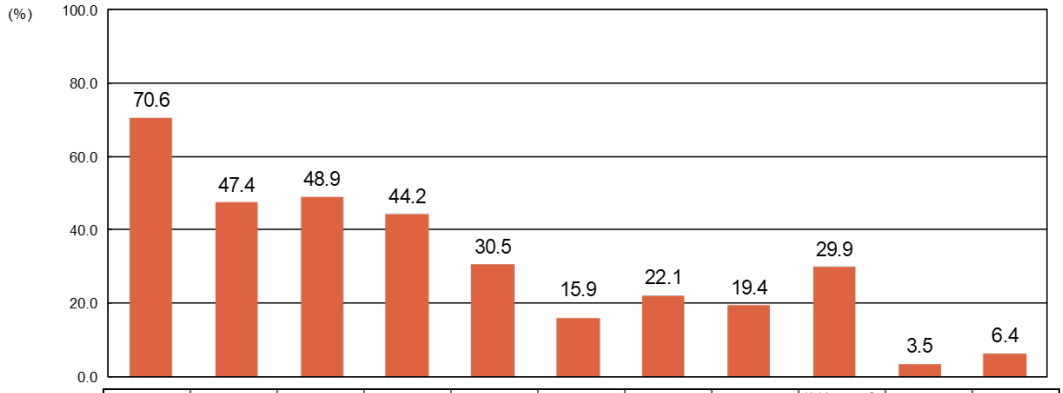
以上の結果を考慮すると、「重要情報の範囲が技術情報・ノウハウ等にまで広がっているものの、これらの漏えいに対する内部不正対策の拡張が進んでいない」という仮説は実態を捉えていると言える。

図表 41 特定する仕組みを持っている重要情報の種別

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＞

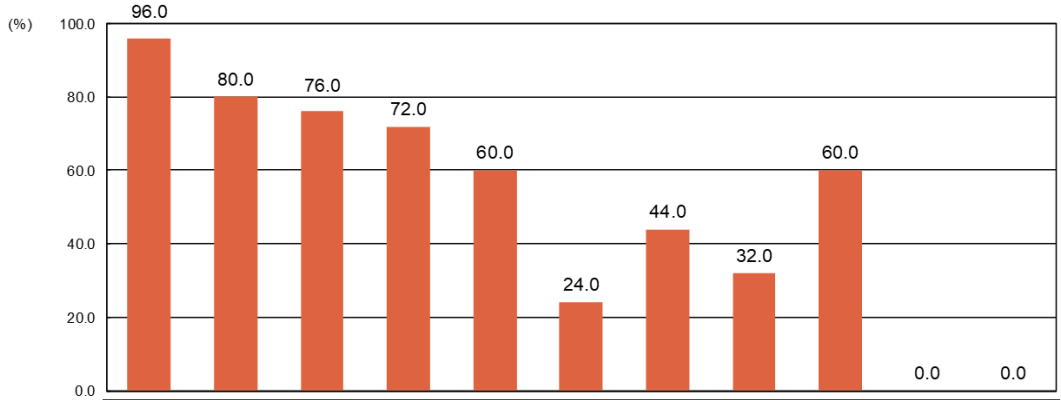
主たる回答



	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

（ご参考：日経平均銘柄企業25社の集計）

参考比較



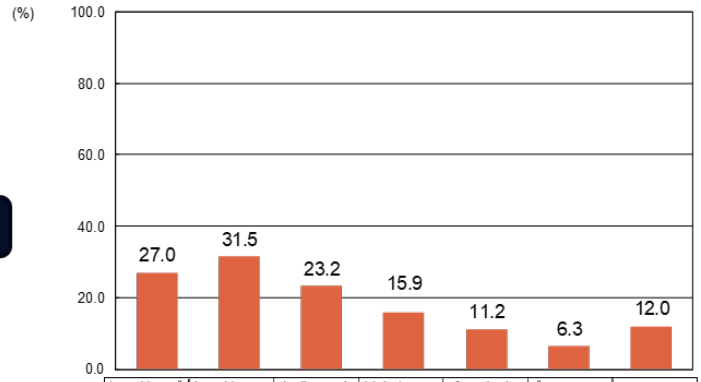
	n=	個人情報	重要な技術情報・ノウハウ	重要な営業情報	営業秘密として管理している情報	利活用する価値が高い重要データ	AI学習用のデータセット	限定提供データとして管理しているデータ	安全保障貿易管理（輸出管理）に係る機微技術情報	他社から「重要であるため秘密にして欲しい」と言われて受け取っている情報	どれもあてはまらない	わからない
TOTAL	25	96.0	80.0	76.0	72.0	60.0	24.0	44.0	32.0	60.0	0.0	0.0

図表 42 個人情報以外の重要情報の漏えいに関する内部不正対策への取組み状況

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＞

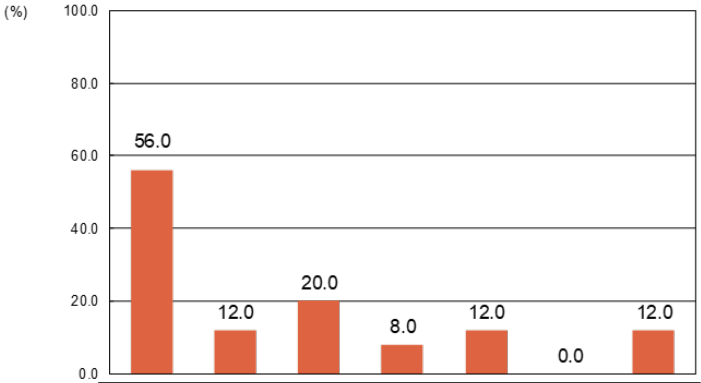
主たる回答



	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

（ご参考：日経平均銘柄企業25社の集計）

参考比較



	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	25	56.0	12.0	20.0	8.0	12.0	0.0	12.0

【検証したい仮説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

この仮説を検証するため、以下に示す内容について調査を実施した。パネルモニターのアンケート回答の単純集計結果を図表 43～図表 46 に示した。

i. 重要情報の管理策のサプライチェーンでの合意状況
ii. 非正規雇用者の内部不正対策
iii. テレワーク時の内部不正対策
iv. クラウドサービス利用時の内部不正対策

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い難い実状である。参考までに日経平均銘柄企業の回答割合を見てみると、次のような項目については強化したい点であると言える。（図表 43 参照）

- 重要情報の管理水準、暗号化、返却・廃棄の方法等についての契約での合意
- 受渡しができる重要情報の範囲についての明文化と合意
- 取扱いを委託した個人情報の漏えい時の調査協力についての契約での合意
- 重要情報漏えい時の事後対応や事業継続に関する連携体制についての合意

なお、自社の重要情報と他社の重要情報を分離した管理や、重要なデータのサプライチェーンでの取扱いについては、日経平均銘柄企業であっても回答割合が不十分な水準に留まっており、今後の底上げが強く求められる状況と言える。

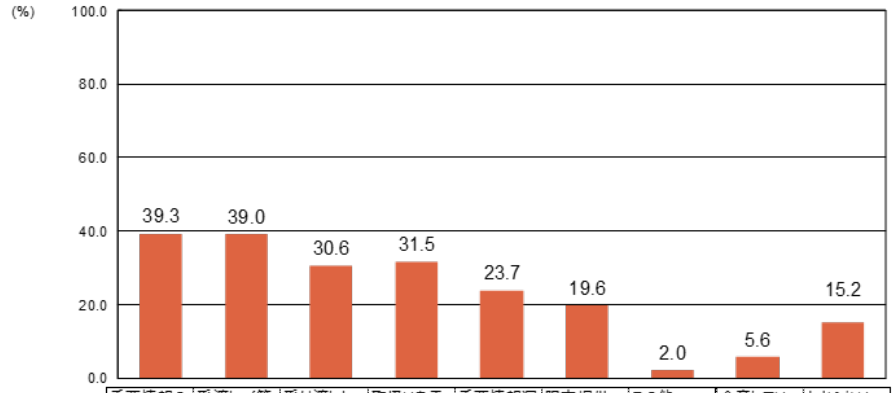
非正規雇用者の内部不正対策については、重要情報へのアクセスを許可しない、または契約形態に則した対策を実施していると回答した割合が 70%を超えており、十分に高い水準に達していると考えられる。（図表 44 参照）

図表 43 重要情報の管理策についての委託先等との合意状況

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＞

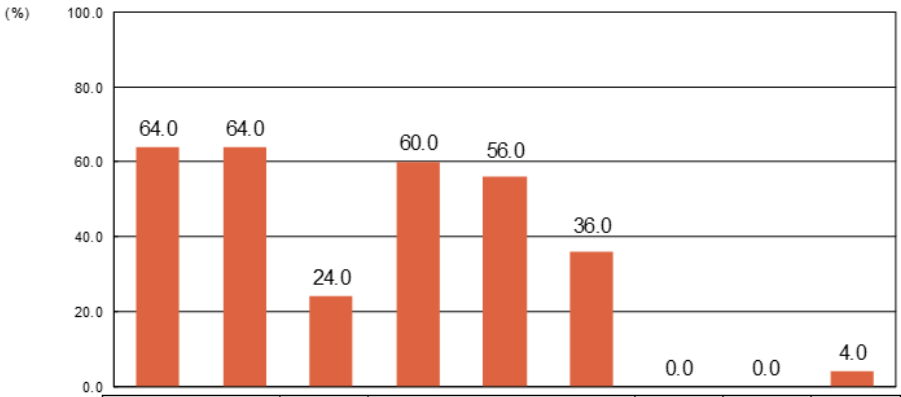
主たる回答



	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

（ご参考：日経平均銘柄企業25社の集計）

参考比較

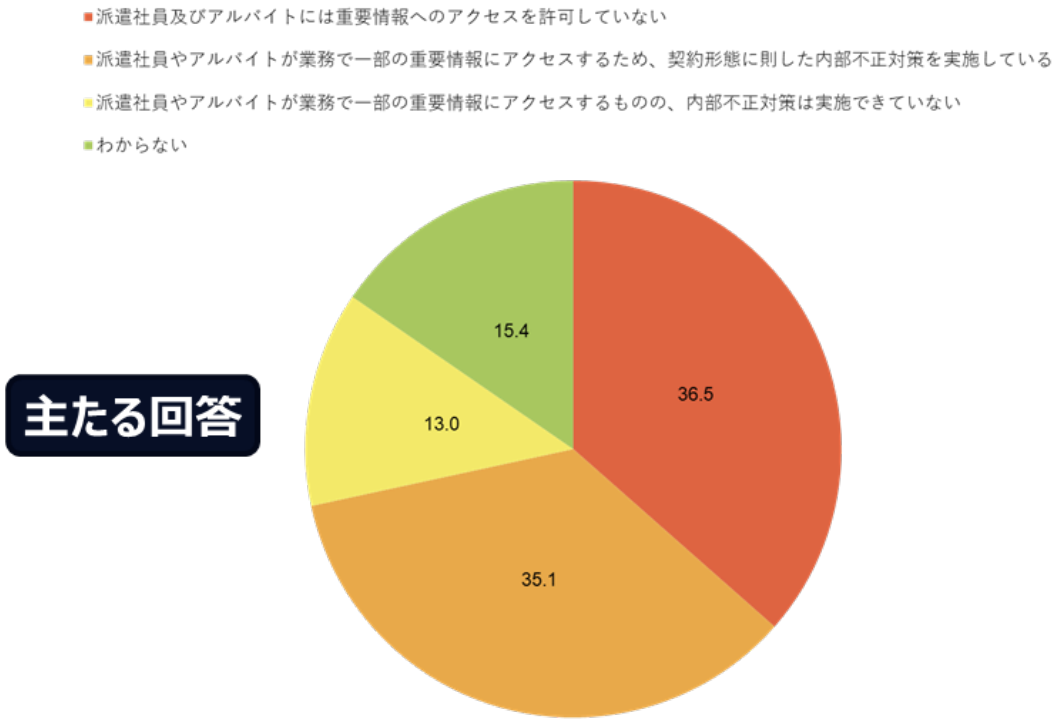


	n=	重要情報の管理水準、暗号化、返却・廃棄の方法等について、契約等を通じて合意している	受渡し（第三者提供を含む）ができる重要情報の範囲について明文化し、合意している	受け渡した重要情報は、自社情報と他社情報に分けて管理することで合意している	取扱いを委託した個人情報が漏えいした場合に、サプライヤーや委託先が、貴社が行う調査に協力することを、契約を通じて合意している	重要情報漏えい時の事後対応や事業継続について、サプライヤーや委託先と協力できるように連携体制について合意している	限定提供データとして保護される、またはライセンス供与される重要データの共有と利活用に関するルールについて、契約等を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	25	64.0	64.0	24.0	60.0	56.0	36.0	0.0	0.0	4.0

図表 44 非正規雇用者の内部不正対策の現状

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。

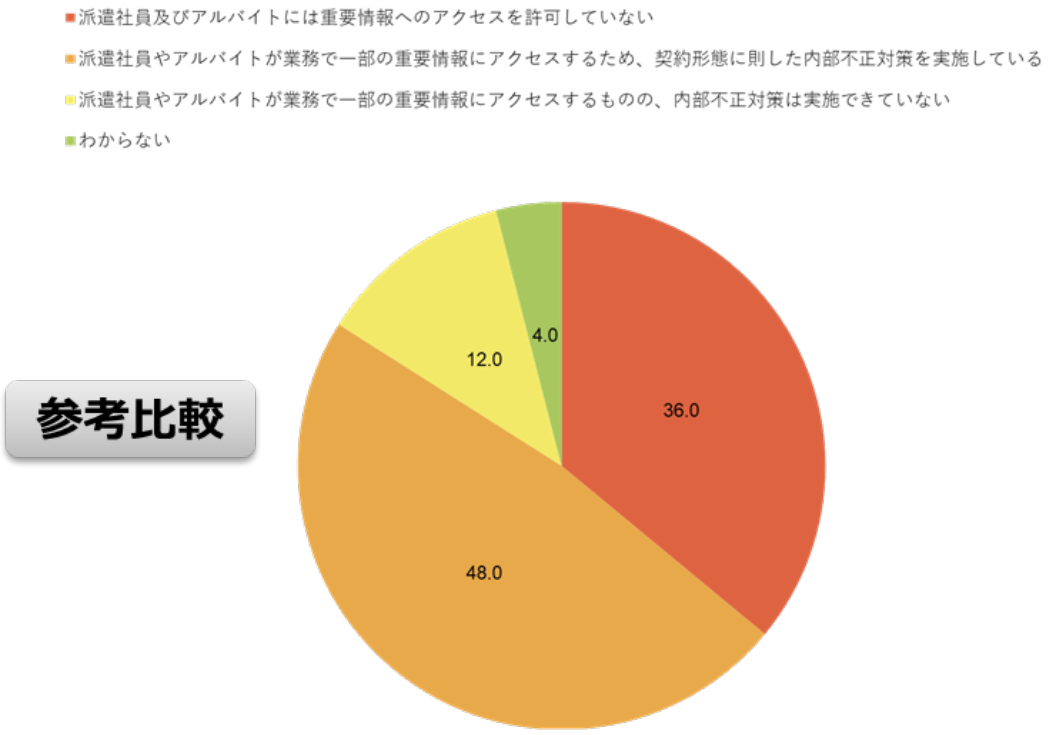
＜パネルモニターが所属する企業のみの集計＞



	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

（図表 44 の続き）

（ご参考：日経平均銘柄企業25社の集計）



	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	25	36.0	48.0	12.0	4.0

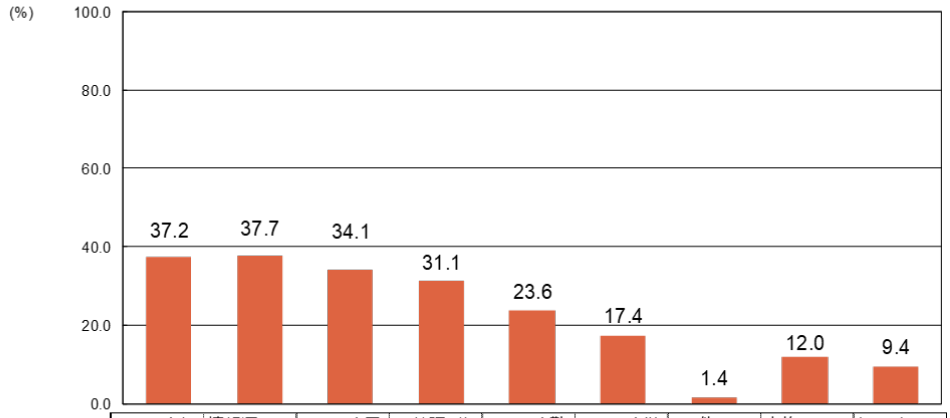
テレワーク時の内部不正対策については、いずれの対策も回答割合が 40%に満たず、十分な水準に達しているとは言い難い実状である。参考までに日経平均銘柄企業の回答割合を見てみると、各対策項目につき強化が必要な状況であると言える。（図表 45 参照）

図表 45 テレワーク時の内部不正対策の実施状況

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＞

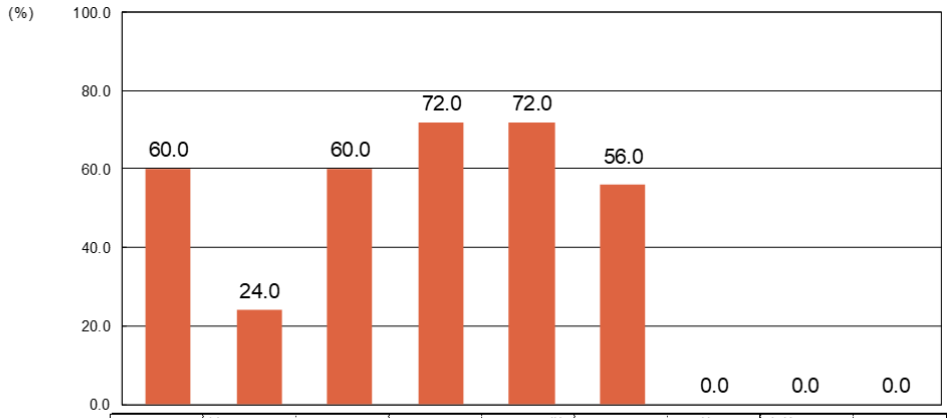
主たる回答



	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

（ご参考：日経平均銘柄企業25社の集計）

参考比較



	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	25	60.0	24.0	60.0	72.0	72.0	56.0	0.0	0.0	0.0

但し、テレワークで取り扱うことができる重要情報については、技術・運用対策で担保できるならば、必ずしも積極的に制限しなくても良いという考え方が広がっている可能性がある。

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い難い実状である。参考までに日経平均銘柄企業の回答割合を見てみると、クラウドサービス利用ルールの周知・教育、許可していないクラウドサービスの利用禁止、クラウドサービスとの責任分担の明確化等については、強化したい点であると言える。他方で、クラウドサービス上で取り扱うことができる重要情報の制限やクラウドプロキシの適用については、日経平均銘柄企業であっても必ずしも積極的とは言えず、今後の課題と考えられる。（図表 46 参照）

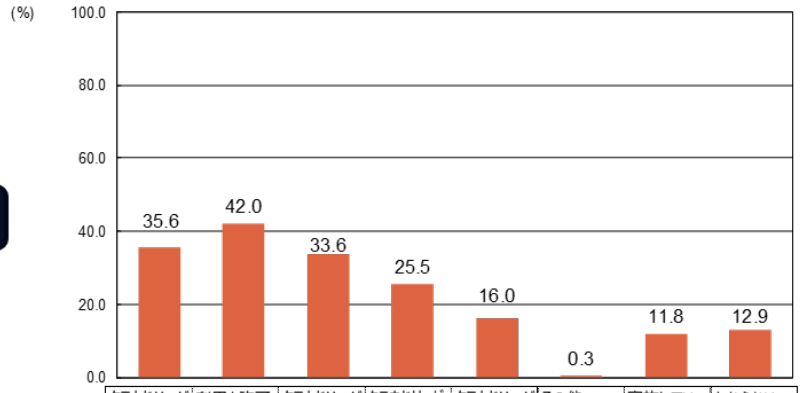
以上の結果を踏まえると、「ニューノーマル等の環境変化への対応が遅れており、リスクが高まる内部不正に関する規則が未整備、または対策を実施できていない」という仮説は、非正規雇用者の内部不正対策を除いて、概ね実態に合っていると言える。

図表 46 クラウドサービス利用時の内部不正対策の実施状況

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＞

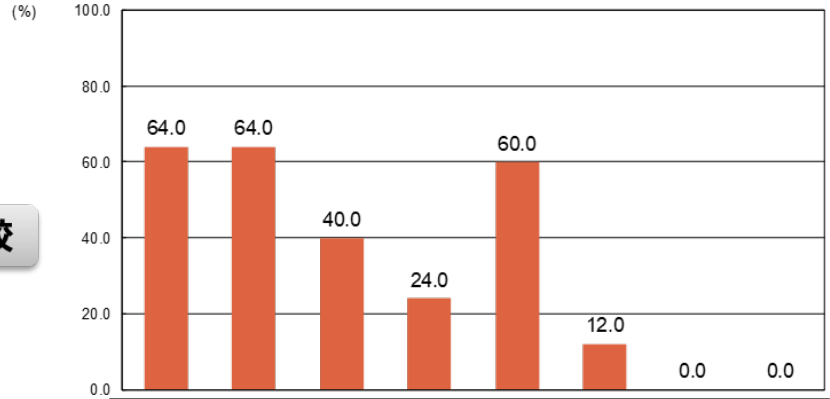
主たる回答



	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

（ご参考：日経平均銘柄企業25社の集計）

参考比較



	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	25	64.0	64.0	40.0	24.0	60.0	12.0	0.0	0.0

【検証したい仮説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

この仮説を検証するために、中途退職時の内部不正対策の実施と中途退職／中途採用時の内部不正防止規則の策定の実態について調査した。パネルモニターのアンケート回答の単純集計結果を図表 47 と図表 48 に示した。

この結果に基づくと、中途退職者に課す秘密保持義務の実効性を高めるためには、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、就業規則に退職後の定めを規定すること等が対策の中心となっている。その回答割合は 50%に達しておらず、十分な水準に達しているとは言い難い実状である。日経平均銘柄企業の回答と比較すると、これらの項目については強化が必要な状況であると考えられる。また既に記載した通り、重要プロジェクト単位での秘密保持義務契約の締結／誓約書の提出はあまり行われていない。

一方、中途採用時／中途退職時の内部不正防止に関する規則の策定については、パネルモニターの回答割合が日経平均銘柄企業の回答割合を上回っている選択肢が多く存在している。しかし、いずれも回答割合が 50%に達していない。従って、大企業／中小企業を問わず、当該規則の策定水準を大きく引き上げることが課題であると言える。

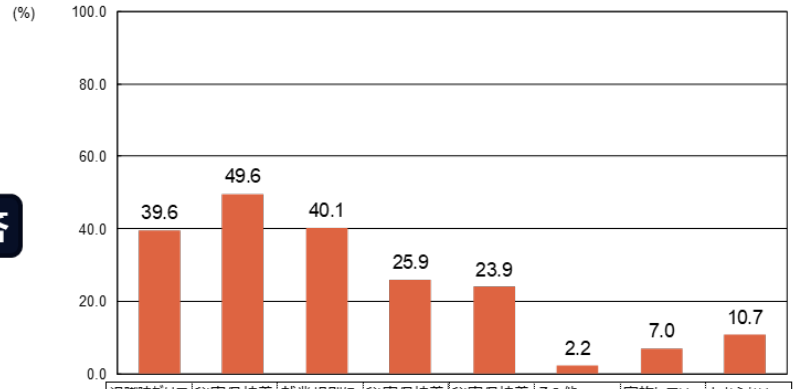
以上の結果を踏まえると、「急増する中途退職者／中途採用者の内部不正に対する対策整備が遅れている、または対策が実施できていない」という仮説は実態に合っていると言える。

図表 47 中途退職者に課す秘密保持義務の実効性を高める対策の実施状況

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＞

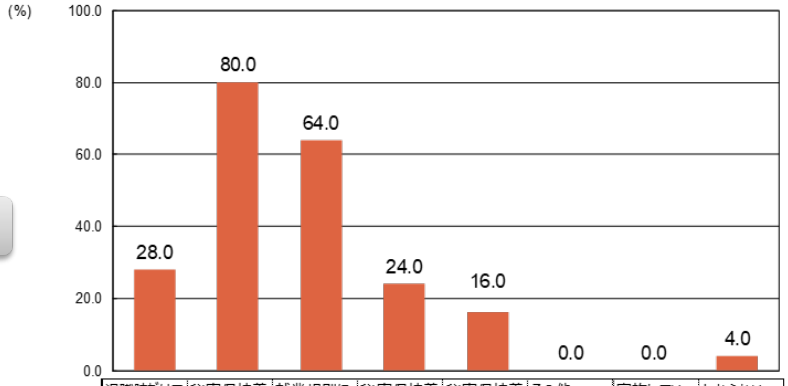
主たる回答



	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

（ご参考：日経平均銘柄企業25社の集計）

参考比較



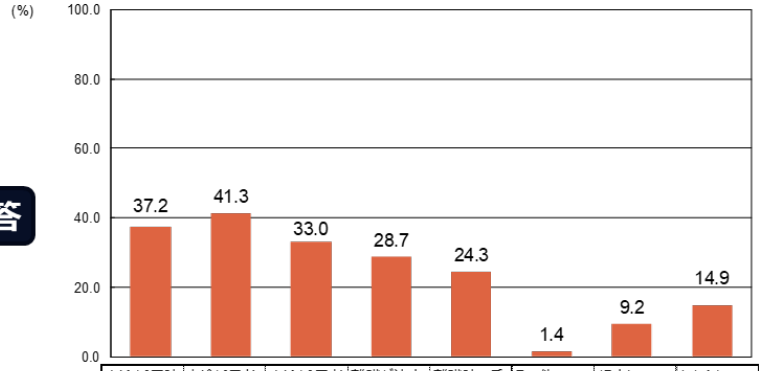
	n=	退職時だけでなく、就職時、異動時、昇格時、新プロジェクトへの配属時・終了時等に、秘密保持義務契約の締結（または誓約書の提出）を求めている	秘密保持義務契約の締結（または誓約書の提出）についての内部規則を定め、就業規則でその順守を求めている	就業規則に退職後の定めを規定している	秘密保持義務の有効期間を十分長く設定している	秘密保持義務の対象となる重要情報の範囲・内容を明確に定めている	その他	実施していない	わからない
TOTAL	25	28.0	80.0	64.0	24.0	16.0	0.0	0.0	4.0

図表 48 採用時と離職時の内部不正防止に関する規則の策定状況

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＞

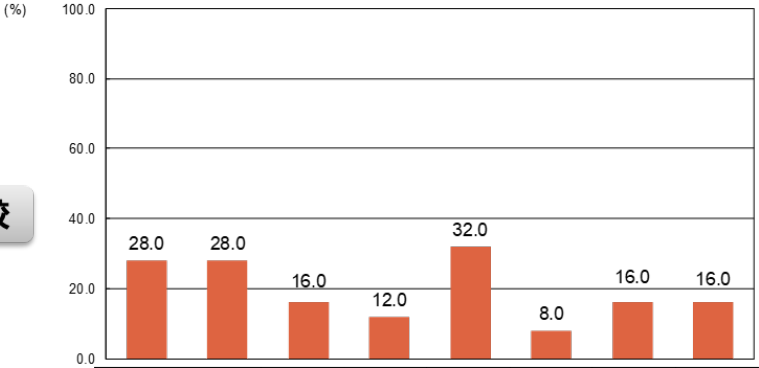
主たる回答



	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

（ご参考：日経平均銘柄企業25社の集計）

参考比較



	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	25	28.0	28.0	16.0	12.0	32.0	8.0	16.0	16.0

【検証したい仮説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

この仮説を検証するために、従業員の不満を蓄積しない職場環境構築のための対策の実施状況について調査を行った。パネルモニターのアンケート回答の単純集計結果を図表 49 に示した。

いずれの選択肢も回答割合が 50%に達しておらず、十分な水準とは言いがたいものの、すべてが 35%を超えているので、全くできていないわけではない。但し、日経平均銘柄企業の回答を見ると、全ての回答割合が 70%程度あるいはそれを超えており、さらなる強化が必要な状況であると考えることができる。

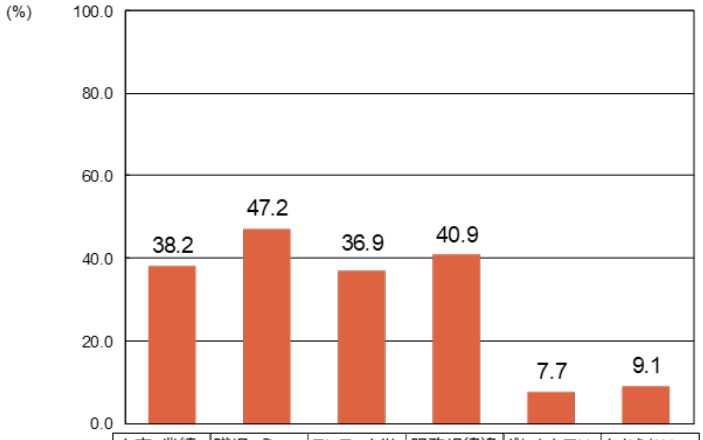
以上の結果を踏まえると、「不満を蓄積せず、内部不正を誘発しない職場環境の整備が十分ではない」という仮説は実態に合っていると言える。

図表 49 不満を蓄積しない職場環境を構築するための対策の実施状況

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＞

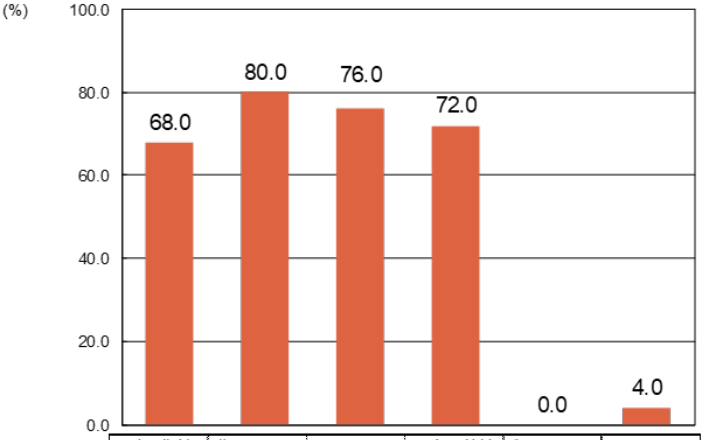
主たる回答



	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

（ご参考：日経平均銘柄企業25社の集計）

参考比較



	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	25	68.0	80.0	76.0	72.0	0.0	4.0

【検証したい仮説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

この仮説を検証するために、退職者の内部不正を発見したときの対応準備をどこまで進めているかについて調査を行った。パネルモニターのアンケート回答の単純集計結果を図表 50 に示した。

この結果を踏まえると、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。この設問については、日経平均銘柄企業の方がずっと消極的な回答をしていることが注目される。パネルからの募集に応えた回答者は情報漏えいや内部不正に関心がある方が多いと考えられることに加えて、所属部署や業務内容で回答者を絞り込んだこともあり、内部不正防止に対する経験・知見が豊富な回答者の割合が高くなっているかも知れず、これが日経平均銘柄企業よりも積極的な回答割合を導出した可能性がある。

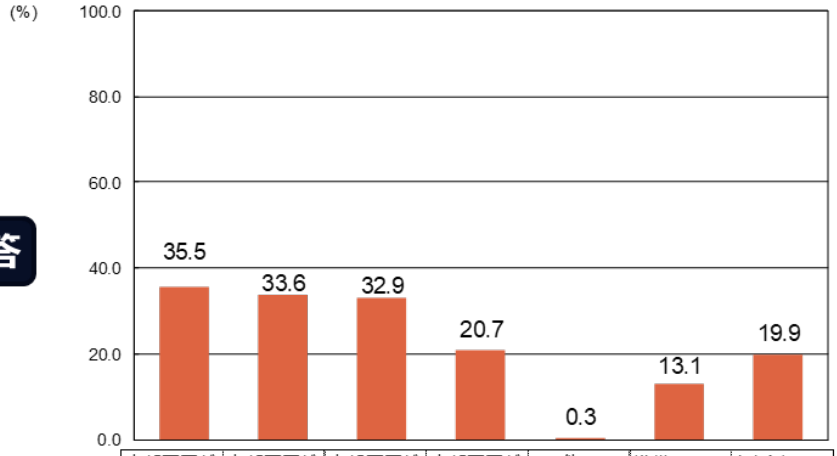
以上の結果を踏まえると、「内部不正による重要情報の漏えい発覚時に、侵害先にどこまで対応するかの方針がない」という仮説は実態に合っていると言える。

図表 50 退職者による内部不正を発見した時の対応についての準備状況

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＞

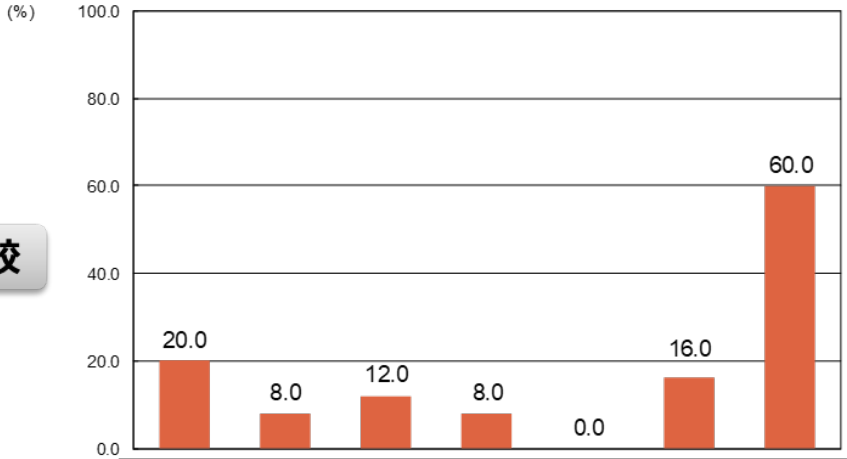
主たる回答



	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

（ご参考：日経平均銘柄企業25社の集計）

参考比較



	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	25	20.0	8.0	12.0	8.0	0.0	16.0	60.0

⑥内部不正防止ガイドライン利用の実態

ここでは内部不正防止ガイドラインが効果的に活用されているかの実態を把握するため、次の観点から仮説を設けてその検証を試みた。

i. 内部不正防止ガイドラインの認知状況

ii. 内部不正防止ガイドラインの利用状況

【検証したい仮説⑥－１】
内部不正防止ガイドラインはあまり知られていない

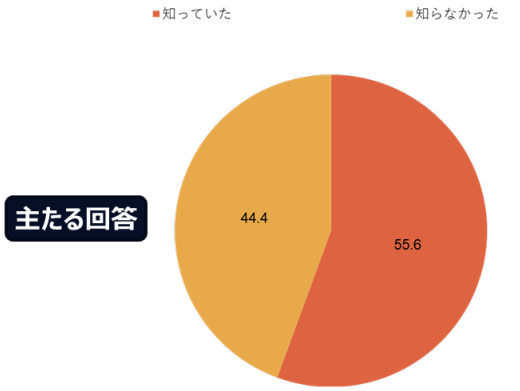
この仮説を検証するために、内部不正防止ガイドラインとそのカバー範囲の認知状況について実態を調査した。パネルモニターのアンケート回答の単純集計結果を図表 51 と図表 52 に示した。

これらの回答結果に基づくと、内部不正防止ガイドラインは 55%程度の企業・組織に認知されていた。この状況は日経平均銘柄企業においてもほぼ同じである。また、内部不正防止ガイドラインを認知している企業・組織のほとんどが、当該ガイドラインが電子化された重要情報を漏えいさせる等の内部不正に焦点を当てていることを認知していた。従って、「内部不正防止ガイドラインはあまり知られていない」という仮説は必ずしも実態に合っていないことが分かった。

図表 51「組織における内部不正防止ガイドライン」の認知状況

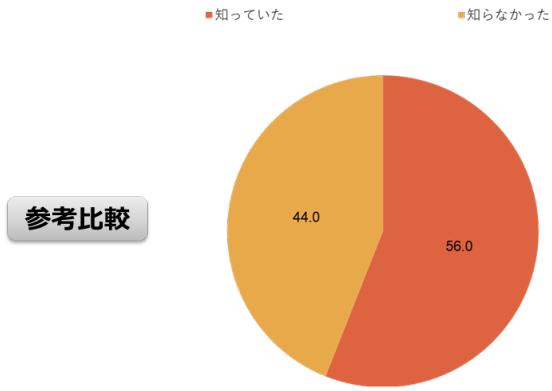
Q1. あなたはIPAが公開している「組織における内部不正防止ガイドライン」をご存じでしたか。

＜パネルモニターが所属する企業のみの集計＞



	n=	知っていた	知らなかった
TOTAL	1179	55.6	44.4

（ご参考：日経平均銘柄企業25社の集計）



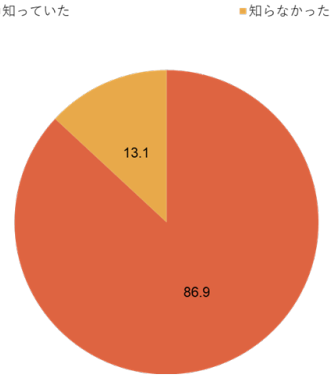
	n=	知っていた	知らなかった
TOTAL	25	56.0	44.0

図表 52「組織における内部不正防止ガイドライン」のスコープについての認知状況

Q2. あなたはIPA「組織における内部不正防止ガイドライン」が、電子化された重要情報を漏えいさせる等の内部不正に焦点を当てて書かれていることをご存じでしたか。

＜パネルモニターが所属する企業のみの集計＞

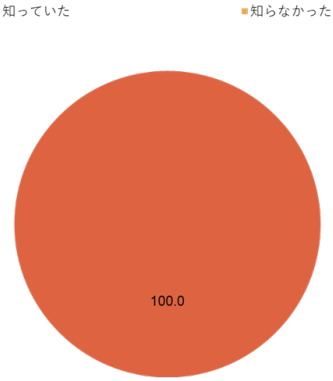
主たる回答



n=	知っていた	知らなかった
TOTAL 656	86.9	13.1

（ご参考：日経平均銘柄企業25社の集計）

参考比較



n=	知っていた	知らなかった
TOTAL 14	100.0	0.0

【検証したい仮説⑥－２】
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

この仮説を検証するために、内部不正対策の検討にあたって参考にしているガイドラインと、内部不正防止ガイドラインで参考にしている対策項目について、その実態を調査した。パネルモニターのアンケート回答の単純集計結果を図表 53 と図表 54 に示した。

これらの結果に基づくと、内部不正対策の検討にあたって内部不正防止ガイドラインを活用しているという回答割合は 25%程度に留まっており、十分に活用されているとは言い難い状況である。しかし、内部不正防止ガイドラインを活用している企業・組織では当該ガイドラインの対策項目を網羅的に参照していることが分かった。

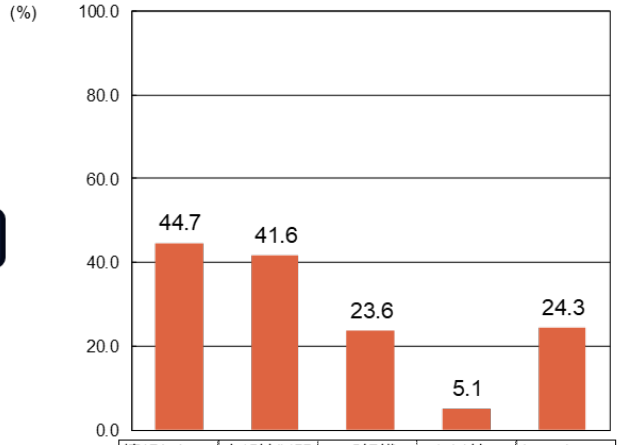
以上の結果を踏まえると、「内部不正防止ガイドラインの存在は知っていても、あまり読まれていない」という仮説は実態に合っている。しかし、活用されている場合は、企業・組織が記載内容全般を参考にしている実態があるため、今後は当該ガイドラインの認知度をさらに高めるとともに、活用推進を支援するための施策を検討していくことが必要である。

図表 53 内部不正対策を検討するにあたって参考にしているガイドライン

Q41. 貴社では、内部不正防止対策を検討するにあたり、どのようなガイドラインを参考にしていますか。

＜パネルモニターが所属する企業のみの集計＞

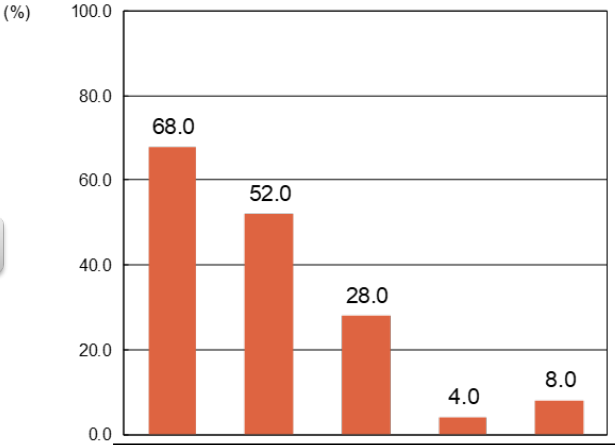
主たる回答



	n=	情報セキュリティ関係のガイドラインの内部不正と関わりが深い箇所を参考にしている	内部統制関係のガイドラインの内部不正に関わる箇所を参考にしている	IPA「組織における内部不正防止ガイドライン」を参考にしている	それ以外	わからない
TOTAL	1179	44.7	41.6	23.6	5.1	24.3

（ご参考：日経平均銘柄企業25社の集計）

参考比較



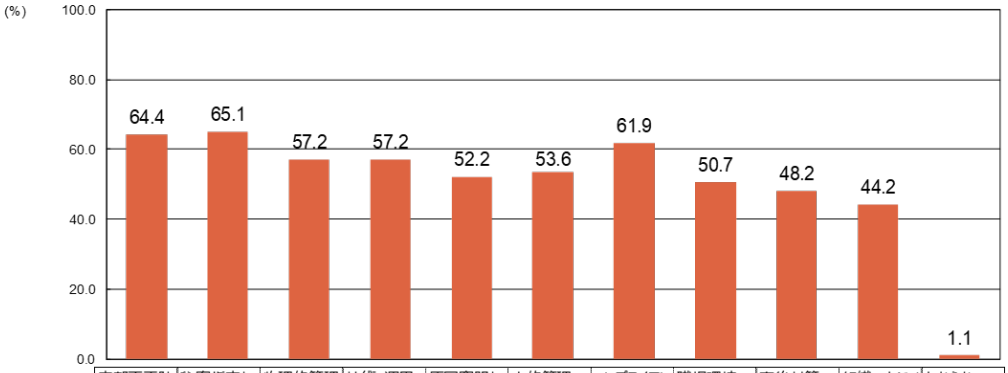
	n=	情報セキュリティ関係のガイドラインの内部不正と関わりが深い箇所を参考にしている	内部統制関係のガイドラインの内部不正に関わる箇所を参考にしている	IPA「組織における内部不正防止ガイドライン」を参考にしている	それ以外	わからない
TOTAL	25	68.0	52.0	28.0	4.0	8.0

図表 54 内部不正対策を検討するにあたって参考にしている「組織における内部不正防止ガイドライン」の項目

Q42. 貴社では、「組織における内部不正防止ガイドライン」のどの項目を参考にしていますか。

＜パネルモニターが所属する企業のみの集計＞

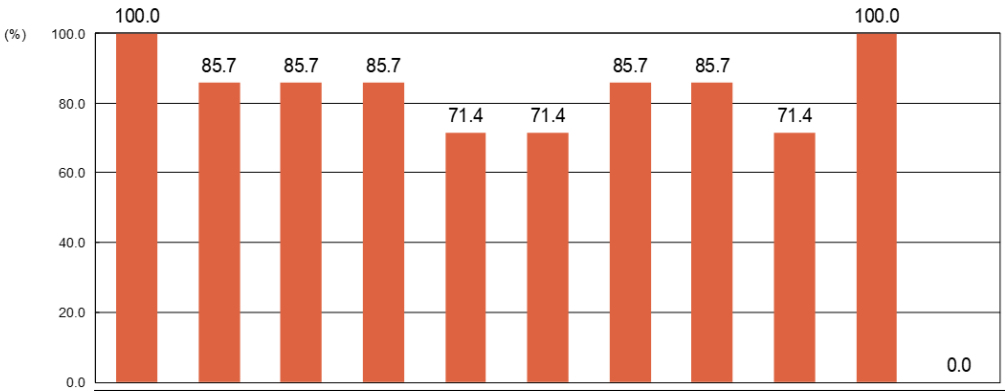
主たる回答



	n=	内部不正防止に関する基本方針	秘密指定とアクセス権指定	物理的管理	技術・運用管理	原因究明と証拠確保	人的管理	コンプライアンスの確保	職場環境の改善	事後対策	組織マネジメント（通報制度、対策のレビュー／監査等）	わからない
TOTAL	278	64.4	65.1	57.2	57.2	52.2	53.6	61.9	50.7	48.2	44.2	1.1

（ご参考：日経平均銘柄企業25社の集計）

参考比較



	n=	内部不正防止に関する基本方針	秘密指定とアクセス権指定	物理的管理	技術・運用管理	原因究明と証拠確保	人的管理	コンプライアンスの確保	職場環境の改善	事後対策	組織マネジメント（通報制度、対策のレビュー／監査等）	わからない
TOTAL	7	100.0	85.7	85.7	85.7	71.4	71.4	85.7	85.7	71.4	100.0	0.0

(2) 企業インタビュー調査からの示唆

①概要

ここでは企業インタビューで得られた調査結果について取りまとめた。企業インタビューは 15 社に対して実施した。その内訳は下記の通りである。

- 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 2 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

予め設定しておいた仮説の検証に役立てるため、インタビュー調査を通じて企業の実態を把握した。得られた調査結果を各仮説に対応付けて仕分けし、これに基づいて各仮説の検証に役立つ示唆の抽出を行った。

②企業・組織として知っておくべき基礎知識の実態

【検証したい仮説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

a. 企業インタビューから得られた知見

【重要情報についての知識】

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である。この知識については、組織全体にこまめに周知徹底して従業員の基礎知識を高めている企業と、敢えて細かい管理を求めず、業務で生み出された情報をすべて重要情報として取扱う企業とに分かれた。

【最新の知識へのアップデート】

基本方針、対策規程、マニュアル等は環境変化（働き方変革、関連法規制の改訂等）に基づいて都度見直されていくため、周知・教育等により、従業員の基礎知識をこまめにアップデートできるようにしている好事例が見られた。

【紙で保管する伝統的企業文化からの転換】

重要情報を紙で保管して物理的に保護するという意識がまだ強く、電子化された重要情報の保護に関する基礎知識は現在熟成中であるという企業があった。

b. 仮説に対して得られた示唆

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。この環境変化には、重要情報の紙保管から電子的な保管への移行も含まれる。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ことになる。

【検証したい仮説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

a. 企業インタビューから得られた知見

【個人情報の取り扱い】

個人情報保護を充実させていると回答した企業が多かった。その中には、事業上個人情報保護法の遵守は不可欠、製造業であっても技術情報は少なく個人情報保護が中心等のコメントもあった。

【重要技術情報の取り扱い】

製造業では、営業秘密管理を非常に厳格に実施している企業があった。また、不正競争防止法や営業秘密の取扱いについても、関連規定を周知・教育していると回答した企業が複数あった。

【限定提供データの取り扱い】

限定提供データの保護に対処できている企業はなかった。

【法制度の知識を教育する範囲】

個人情報、営業秘密の保護に関する法的知識は担当部署が理解していれば良いと指摘したベンチャー企業があった。

b. 仮説に対して得られた示唆

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。

【検証したい仮説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

a. 企業インタビューから得られた知見

【ガイドラインに対する一般的な周知の姿勢】

ガイドラインへの適合は義務ではないので、法令と比較するとガイドライン周知の程度は弱い可能性があると指摘した企業があった。

b. 仮説に対して得られた示唆

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。

【検証したい仮説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

a. 企業インタビューから得られた知見

【情報漏えい／セキュリティリスクの知識】

以下に示すように、従業員が情報漏えい／セキュリティリスクに関する知識を持つことが重要であり、日頃からの周知が求められるという指摘があった。

- 従業員全体に対してセキュリティリスクの知識を底上げすることが必要
- 情報漏えいがどのような背景・理由で発生するのかをしっかりと認識することが必要
- 事例（内部不正、サイバー攻撃）についての知識を蓄積することが必要

また、同業他社で発生した事件等を半期に一度取り上げて、自社に当てはめた検討をしている好事例も見られた。

【サプライチェーンセキュリティのリスク】

再委託先に関するインシデントを経験し、再委託先のセキュリティリスクを懸念していると指摘した企業があった。

b. 仮説に対して得られた示唆

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、重要情報の漏えい等の背景・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。

③内部不正防止に取り組む組織的体制の実態

【検証したい仮説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

a. 企業インタビューから得られた知見

【経営層の取り組み姿勢】

インタビューを実施した企業の中には、経営層がしっかりとした姿勢でコンプライアンスや内部不正対策に係るリーダーシップを発揮している企業が複数あった。

（例）

- 経営層がコンプライアンス（内部不正）を指揮することが規則で定められており、技術と教育／啓発の両面からリーダーシップを発揮して対策強化を指示している（IT サービス企業）
- グローバル企業の現地法人社長が責任を持って、内部不正対策、営業秘密管理等に関する全般的な内容の周知を指示している（製造業）
- 社長が自ら作成したセキュリティポリシーの宣言や規程の冒頭に、自社の事業モデルでは顧客の重要情報を受領して仕事をするので、重要情報を決して漏えいしてはならないことを記載し、企業全体に周知・徹底している（IT ベンチャー企業）

他方で、取引先に対する印象として、グループ企業ではない中堅企業において、重要情報の漏えいや内部不正対策に対する経営層の認識があまり高くない傾向が見られるとの指摘もあった。

【内部不正に関する情報発信の文脈】

経営層が、主として情報セキュリティに関する文脈の一部として、内部不正防止のメッセージを発信している企業があった。

b. 仮説に対して得られた示唆

仮説どおりの企業が多かったものの、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。

【検証したい仮説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

a. 企業インタビューから得られた知見

【重要情報の特定・管理責任の明確化】

最高デジタル責任者（以下、「CDO」という）の任命、情報資産管理の専門組織の設置、知的資産保護の専門組織の設置等を通じて、重要情報の特定、資産管理、棚卸し等に対する責任を明確化した興味深い好事例が見られた。重要情報の多様化に対応しやすい手法として注目される。

【内部不正防止、インシデント対応の全社責任者】

内部不正防止、インシデント対応の全社責任者を誰が務めるかは企業によって異なっている。今回の調査では、次のような事例が見られた。

- リスク管理担当の役員とコンプライアンス担当の役員で分担。コンプライアンス担当役員は退職時の情報漏えい等を所管
- 最高情報セキュリティ責任者（以下、「CISO」という）、システムリスクマネジメントの責任者等
- リスク管理担当役員が CISO を兼務、CISO としてサイバーセキュリティとコンプライアンスの責任者を兼務、一人の役員が情報セキュリティと内部監査の両方の責任者を兼務等
- グローバルな事業部単位で設けられた知的資産保護の専門組織長が総括責任者を務める
- 責任者である CISO が CDO や最高情報責任者（以下、「CIO」という）と必要に応じて密に連携

基本的にはリスク・コンプライアンス管理責任者が全社責任者となるケース、情報セキュリティ責任者が全社責任者となるケース、その折衷形式の３つに分類することができる。また、これには当てはまらないケースとして、知的資産保護の専門組織長が責任者となる好事例があり、営業秘密を含む知的財産の保護に専念する組織の長が内部不正防止の組織責任も担うというシンプルで分かりやすい構造が優れていると考えられる。

【内部不正防止、インシデント対応の組織体制】

内部不正、インシデント対応の全社責任者をどのように定めるかに従って、その配下の組織構成にも違いが見られた。今回の調査では、次のような事例が見られた。

- 内部不正防止等を分担するリスク管理、コンプライアンス、IT／セキュリティはそれぞれ別の組織体系
- 内部不正防止等を分担するリスク・コンプライアンスと IT／セキュリティはそれぞれ別の組織体系
- 内部不正防止等を担当するリスク管理組織の下に情報システム部門を配置
- リスク管理組織の中に情報資産管理、システムリスク管理を担当し、IT／セキュリティ組織を牽制する組織を設置
- リスク管理、コンプライアンス、情報セキュリティ等で全社委員会を設置し、主管組織と他組織の横連携を強化
- リスク管理、コンプライアンス、情報セキュリティ等の全社委員会が情報漏えいを重複してカバーし、抜け漏れを防止
- 内部不正防止等をセキュリティ組織やシステムリスクマネジメント組織が担当
- 内部不正防止等を情報セキュリティ統括組織が担当し、事業部統括組織と連携

・　知的資産保護の専門組織が担当、購買・製造・技術・営業部門と連携
・　どの部門が対応するかは明確に決まっていない

b. 仮説に対して得られた示唆

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件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。

【検証したい仮説③－３】
社内ポリシー／規定の整備が不十分な企業が多い

a. 企業インタビューから得られた知見

リスク管理を担う委員会の場で議論して社内規則を作成し、全社に周知している企業があった。

b. 仮説に対して得られた示唆

内部不正防止に関する規則の整備についても、既存の社内委員会をうまく活用することが考えられる。また、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である。このように、社内委員会の活用は、仮説が示す「社内ポリシー／規定の整備が不十分」という状況の改善に有効である。

【検証したい仮説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

a. 企業インタビューから得られた知見

経営層が内部不正防止に高い関心を持っている大企業では、リソースの配分にあたってコストに捉われない、十分なリソースが配分されている等の好事例が見られた。

b. 仮説に対して得られた示唆

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。

【検証したい仮説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

a. 企業インタビューから得られた知見

マネジメントシステムを活用して内部不正対策を継続的に改善しているとした企業が複数あった。この中には、CDO の任命や知的資産保護の専門組織を設置することで、重要情報保護にしっかりと取り組んでいる企業が含まれていた。

また、PDCA を回すにあたり、内部監査で重要情報保護に関する課題を抽出し、当該課題の翌年度の改善達成率を KPI として規定して管理している好事例が見られた。

b. 仮説に対して得られた示唆

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えれば、仮説は実態と合わなくなる。

【検証したい仮説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

a. 企業インタビューから得られた知見

特になし。

b. 仮説に対して得られた示唆

特になし。

④組織全体への周知・教育の実態

【検証したい仮説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

a. 企業インタビューから得られた知見

企業インタビューでは、内部不正対策に関わるリテラシー教育について、多数の好事例を集約できたのでここで取りまとめた。また、法律で規定された義務や対応を遵守する個人情報保護とは異なり、営業秘密保護では秘密文書の実務上の扱いが重要であるとの指摘があった。

【重要情報の特定と保護に関するリテラシー教育例】

＜一般＞

- 年 3 回の e-Learning で情報資産保護に関する研修を受講し、経営機密情報の取り扱い等を周知・教育
- 業務上扱う情報種別の理解、各種別に適用される法令の概要等を目的別に周知・教育
- 秘密区分（機密レベル）の概要を周知・教育
- 秘密区分の考え方（情報の内容に応じた区分）を定期的に周知・教育

＜個人情報保護＞
- 役員が年に 2 回全拠点を回り、個人情報保護を含むコンプライアンス勉強会を開催
- 日々多くの顧客及び個人情報に接する営業職員に対し、朝礼で週 1 回、個人情報保護を含むコンプライアンス教育（うっかりミス防止を含む）を実施
- 個人情報保護法が改正されたタイミングで、全社に周知・教育を実施
- 毎年 1 度、全正社員に対して、法務部門が個人情報保護法等の訓練を実施

＜営業秘密保護＞
- 不正競争防止法や外為法の関連規定について周知・教育
- 営業秘密等の取り扱いについて周知・教育
- 営業秘密の保護制度に関する知識を教育し直すことを準備中
- 基礎的な教育の中で、「営業秘密とは何か」を頻繁に教育
- 限定提供データを含めて営業秘密の取扱いに注意し、きちんと保護するための知識を実務面から教育・周知

【内部不正を対象としたリテラシー教育例】
- コンプライアンス教育の一環として、2 か月に 1 回の頻度で内部不正に関する研修を実施
- インシデントが発生した際に、原因究明のためにログを確認することを周知・教育（ポップアップで画面に警告を表示する等を含む）
- 毎年のリフレッシュ研修で、誤った行動を取ると、どのようなリスクが生じるかを簡潔に周知・教育

【インシデント事例を活用したリテラシー教育例】
- 社内で発生したセキュリティインシデントの事例を、最近のリスク内容とともに周知・教育（周知先としてグループ企業を含む）
  （例）中途退職者／中途採用者の重要情報漏えい／持ち込みについてのインシデントが増えているため、事例として周知・教育
- 他社で事故が発生した際に、これを取り上げて周知・教育

・　インシデント発生時に、メールマガジンやチャットツールを用いた注意喚起、周知等を実施

【テレワーク時の内部不正に関するリテラシー教育例】

・　内部規則を策定し、テレワーク開始前にこれを周知・教育

【サプライチェーンでの重要情報保護に関するリテラシー教育例】

・　外部委託を実施する部門に対して、契約管理や監査の指示に加えて、リテラシー教育を実施

b. 仮説に対して得られた示唆

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。

これに関して、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ため、積極的に取り組むことで仮説を否定し、内部不正対策に関する周知・教育の充実に貢献できる（【検証した仮説④－２】を参照）。

【検証したい仮説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

a. 企業インタビューから得られた知見

【インシデント事例の活用】

自社で発生した事件／インシデント／ヒヤリハットを取り上げて教育すること、他社で発生した事件を自社に当てはめて教育することは、従業員の具体的な理解を進める上で効果が高く、実践に繋がりやすいという指摘があった。

【ルールや対策の背景にある理由の理解を進める教育】

ルール上の禁止事項や対応方法等を周知するだけでなく、なぜそれをしてはいけないのか、なぜその方法が良いのか等を理解してもらわないと、従業員個人の実践に繋がりにくいという指摘があった。

【実践に繋がる効果が高い教育方法】

自社で起きた事件／インシデント／ヒヤリハットや自社独自のルールについて、グループで時間を掛けて集中して考える機会を与える、ディスカッション形式の教育の場を設ける企業があった。従業員同士で直接コミュニケーションを取りながら、互いの理解を確認できる場を設けることで、ルールや対策の背景にある理由の理解が深まるため、実際の行動に結びつきやすい。

内部不正による情報の持ち出しについて、その時に何が起きたかを振り返って再発防止を図ることができるようなコンテンツを自社制作し、全従業員に閲覧させている企業もあった。特に動画の視聴であれば、背景にある理由の解説を分かりやすく伝えられるため、従業員の理解が深まるものと期待される。また、発生した重大事件の教育用再現動画を制作し、その動画の中で「アクセスログ等を全部見ているため必ず見つかる」ということをかなり厳しい表現で伝えている好事例が見られた。

同様に、事例とセットで「これをすると、こうなるから、してはならない」という禁止メッセージを伝えることで、悪意を持つ者への抑止効果が高まるという指摘があった。

この他に、テレワークルールの遵守に関するセルフチェックを全従業員に毎月求めることで、テレワークルールの周知・教育にも役立てているという事例があった。

b. 仮説に対して得られた示唆

リテラシー教育を従業員の実践に繋げていくためには、社内外の事件／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、規定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）、定期的なルール遵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である。このような従業員の実践に繋がるような教育方法のノウハウを積極的に組織全体に適用することで、仮説に合致しない組織環境を実現することができる。

⑤内部不正防止の課題と対策の実態

【検証したい仮説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

a. 企業インタビューから得られた知見

企業インタビューにおいても、内部不正に対する課題認識は後回しにされている企業があった。

他方で、日々顧客に接する営業職員を多数抱える企業等では、顧客の個人情報を格納したノート PC 紛失等のうっかりミスや、出来心での小さな情報漏えいに対しても極めて厳しいリスク認識を持っており、年間ベースでゼロを目指すという高優先度での取り組みを実践していた。

b. 仮説に対して得られた示唆

以上を考慮すると、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一方で、仮説が当てはまってしまっている企業の例も散見された。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。

【検証したい仮説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

a. 企業インタビューから得られた知見

対策を網羅的に措置するよりも、費用対効果を考えながら、従業員教育に軸足を置く方が良いという指摘があった。この背景には、従業員監視に対する企業側の迷いが深い現状があるものと推察される。

b. 仮説に対して得られた示唆

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遵守などの人的・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と考えられる。このような方針を採ることで、仮説は必ずしも当てはまらなくなる。

【検証したい仮説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

a. 企業インタビューから得られた知見

【重要情報の特定】

内部不正対策を適用する際の前提条件として、個人情報以外で保護対象となる重要情報を正しく特定・分類できているかが問われる。今回のインタビューでも、現在重要情報の定義に重点を置き、個人情報以外の重要情報とは何かを検討しているところであると回答した企業があった。

また、重要プロジェクトが生み出す重要情報に対して、社内規程で管理・共有ルールを策定して周知している好事例も見られた。

【高度なソリューションの適用】

重要情報のアクセス権限設定、暗号化、編集／コピー／印刷／転送の制限、使用期限の

設定等を可能にする高度な情報保護基盤ツールを最近導入し、営業秘密を厳格に分類・保護し始めた先進的な企業もあった。

b. 仮説に対して得られた示唆

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ため、仮説は必ずしも当てはまらなくなる。

【検証したい仮説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

a. 企業インタビューから得られた知見

【テレワーク時の情報漏えいや内部不正への対応】

テレワークを意識して、エンドポイントの端末機能を制限する対策は多くの企業が採用していた。

さらに、ゼロトラストの概念を積極的に導入している企業が複数あった。また、情報漏えい対策として IRM（Information Rights Management）や DLP（Data Loss Prevention）を検討している企業もあった。

インタビューした企業の中では BYOD を許可している企業はなかった。

【クラウドサービス利用時の情報漏えいや内部不正への対応】

どのインタビュー先企業も、無許可や業務で使用できるクラウドサービスを制限することに重点を置いていたが、これと比較すると、クラウドサービス上で扱うことができる重要情報の制限に言及した企業は少なかった。

委託先が再委託先と情報をやり取りするためにクラウドサービスの利用を要請してくるという課題を指摘した企業があった。

【サプライチェーンからの情報漏えいや内部不正を重視する環境変化への対応】

グローバルサプライチェーンのサプライヤーをセキュリティ対策のレベルで何段階かに分類し、各段階に応じてアクセス可能な重要情報のレベルや、印刷可否、ダウンロード可否等を定めて、サプライヤーの権限管理に適用している企業があった。

取引先との間で重要情報をやり取りするにあたり、契約で取り扱う情報の重要度に応じて暗号化が必要なレベル、暗号化を推奨するレベル等の情報保護方針を定めた上で、お互いの責任範囲と紛争解決方法を定めている企業もあった。

サプライヤーが多数あるので、サプライヤーに専用の検査ツールを渡し、重要情報保持状況の

自動検査結果を返送してもらい、確認している企業もあった。

b. 仮説に対して得られた示唆

重要情報漏えい防止に関するニューノーマル等の環境変化への対応については、まず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。

また、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。

総括すると、インタビュー先の大企業においては、仮説が言うように、重要情報漏えい防止に関してニューノーマルへの対応が遅れているとは必ずしも言い切れない。

【検証したい仮説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

a. 企業インタビューから得られた知見

【入社・退職時の対策強化の必要性】

内部不正については役員や従業員の入社／退職時のリスクが高いので、ここに集中して監視する必要があるとの指摘があった。退職者は従業員満足度が低く、退職後に忠誠心や愛社精神（ロイヤルティ）が下がることがあるので、退職時が一番危険なタイミングと認識して十分に配慮しているとした企業もあった。

【実施している周知・教育】

役員及び従業員に対し、重要情報の持ち出しだけでなく、持ち込みについても法令違反や刑事罰の対象となりうることを教育している企業があった。

【秘密保持義務契約や誓約書の運用】

最近、秘密保持契約書を改訂し、書式の運用の見直しを実施した企業があった。期限の無い秘密保持義務契約を入社時に結び、退職時には入社時に同意した契約が退職後も有効であると伝えている企業もあった。

他方で、重要プロジェクト単位で秘密保持の誓約書を取得している企業はほとんど見られなかった。但し、機微情報を扱う重要プロジェクトでは、契約時等に顧客から、従事者全員の秘密保持誓約書の提示を求められることはあるとの指摘があった。

【中途退職者／採用者のチェックとそのためのルール策定】

中途退職者に対する監視やチェックはしっかりと行っており、退職が決まった時点で厳格にチェックしている企業があった。他方で、中途採用者が他社の重要情報を持ち込まないようにするための確認規則は手当てしていないと回答した企業があった。

b. 仮説に対して得られた示唆

「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。しかし、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である。

一方で、先に述べた通り、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。また、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。

【検証したい仮説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

a. 企業インタビューから得られた知見

内部不正対策として、従業員に不満が蓄積しないように、労務管理、人事管理、コミュニケーション管理で必要な対策を講じることを最も重視していると回答した企業があった。従業員の忠誠心や愛社精神をモニタリングしつつ、これらを上げるための対策を講じている企業もあった。愛社精神等を上げる対策としては、従業員の心理的安全性を保ちつつコミュニケーション環境に優れた職場を作ること、やりがいのある仕事に取り組む機会が得られるような組織運営を行うことなどの好事例が見られた。

また、テレワークに関する環境整備については、毎週出勤日を設け、テレワークを行う従業員がコミュニケーション不足に陥らない対策を行っている企業があった。

b. 仮説に対して得られた示唆

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り、必ずしも仮説に合わない実態が見られる。

【検証したい仮説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

a. 企業インタビューから得られた知見

特になし。

b. 仮説に対して得られた示唆

特になし。

⑥内部不正防止ガイドライン利用の実態

【検証したい仮説⑥－１】
内部不正防止ガイドラインはあまり知られていない

a. 企業インタビューから得られた知見

【内部不正防止ガイドラインの認知状況】

インタビュー調査を実施した企業の中でも、内部不正防止ガイドラインを知らなかった企業と元々知っていた企業に分かれた。一般的に、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。逆に言えば、日頃から産業スパイ等の脅威に晒されているハイテク製造業等においては、内部不正に限定した用途で良く認知されている可能性がある。

他方で、内部不正防止ガイドラインを元々認知していた企業においては、担当部署の一部従業員だけに認知されている、社内連携を取る他部署では必ずしも認知されていない等の指摘があった。

【内部不正防止のために参照しているガイドライン】

内部不正対策の実施においても、サイバーセキュリティに関するガイドライン（経済産業省、総務省）を参照している企業が多くあった。また、情報の取り扱いに関して、個人情報の保護に関する法律についてのガイドラインを確認する機会が多いとの指摘もあった。

【内部不正防止ガイドラインの認知度を向上させる工夫】

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（経済産業省「サイバーセキュリティ経営ガイドライン」等）との間で相互参照、相関の解説等を行うのが良いとの指摘があった。また、個人情報漏えい事案・インシデントが発生した際に、内部不正防止ガイドラインと個人情報の保護に関する法律についてのガイドラインをどのように使い分けるのが良いかを明示すると良いとの指摘もあった。

b. 仮説に対して得られた示唆

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、仮説が成立しない状況に近付けることができる。

【検証したい仮説⑥－２】
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

a. 企業インタビューから得られた知見

【活用しやすい内容の充実】

内部不正防止ガイドラインの活用を促進する方法の１つとして、企業ニーズの高い主題に関する記載を充実させることがある。例えば、中途入社時／中途退職時に必要となる内部不正対策、中途退職者による内部不正事例等についての記載を増補・周知することが考えられる。この他にも、紙で保管する重要情報の内部不正対策を統合すること、グローバル視点でのリスク／対策の記載を充実させること等を希望する指摘があった。

【社内規程整備への活用促進】

公的なガイドラインは、社内規程の整備に活用しやすいという指摘があった。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すことで、社内規程に内部不正対策を加筆する際に活用しやすくなる。

【概要版の作成】

内部不正対策を経営層に説明する際に活用しやすいように、簡潔に要旨をまとめた概要版を作成・公開してほしいという要望があった。

【従業員への周知・教育にそのまま使えるコンテンツの整備】

内部不正対策を従業員に周知・教育する際に積極的に役立てるため、ガイドラインの改訂と相俟って、次に示すようなそのまま活用できるコンテンツの整備を期待する指摘があった。

- e-Learning 用の設問、解説等の公開
- 内部不正対策の要点をまとめた動画コンテンツの公開
- その他、従業員教育にそのまま活用できる素材の充実

【周知啓発活動への希望】

内部不正防止ガイドラインの周知啓発のため、IPA 主催で座談会やオンラインによる講演を継続的に実施してほしいという要望があった。

b. 仮説に対して得られた示唆

現状の内部不正防止ガイドラインは、仮説が示すように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

(3) 有識者インタビュー調査からの示唆

①概要

ここでは、有識者インタビューで得られた調査結果について取りまとめた。有識者インタビューは、重要情報漏えいや内部不正の防止に関する最新の法制度の動向、企業リスクマネジメント、データ利活用と保護等に詳しい有識者 7 名に対して実施した。その内訳は下記の通りである。

- 弁護士 4 名
- 民間企業・組織経験者 3 名（うち 1 名は公認会計士）

インタビューにあたっては、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・見解等の提示を受けた。その上で、予め設定しておいた仮説の検証に役立てるため、得られた調査結果を各仮説に対応付けて仕分けし、仮説に対して得られた示唆の抽出を行った。

②企業・組織として知っておくべき基礎知識についての示唆

【検証したい仮説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

a. 有識者の分析・意見の要旨

特に議論なし。

b. 仮説に対して得られた示唆

特になし。

【検証したい仮説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

a. 有識者の分析・意見の要旨

【法制度についての知識のあり方】

- 従業員一般への基礎知識の周知・教育については、一般的な法知識よりも、してはいけないことを警告のような形で伝えるのが良い。うっかり事故の防止については、やってはいけないことや対策を広く教育すべき。悪意の不正に対しては、それが犯罪であること、刑事

罰等があること、巨額の損害賠償もありうることなどを、実例とともに示すべき。

- 主管部署についてはもっと高い割合で知識を持っていただくことが理想だが、難しいのであれば個人情報保護法のようにやるべきことを明確化した上で、法務部や外部専門家との連携を促していくべき。内部不正防止の主管が法務部ではない場合やむをえない側面もあるが、担当部門の不正競争防止法（営業秘密）の知識は本来、個人情報保護法と同程度の水準であるべき。
- 限定提供データの認知度は営業秘密よりもさらに低いのが現状。限定提供データは営業秘密との関係が非常に強い制度であるため、営業秘密と限定提供データの法知識の周知に同時に取り組むべき。例えば、次のような方法が良い。
  - 会社にとって重要なデータという括りで大まかに整理してリテラシー教育を実施。
  - 限定提供データとしても営業秘密としても連続して保護。
- 限定提供データそのものは無個性の場合が多く、不正利用侵害の発見が難しい場合が多いこと、刑事罰がないため警察の強制捜査ができないことなどは周知しておくと良い。
- 外為法はマネーローンダリング防止の観点からも重要な法規制であり、企業活動の根幹を左右する重要な規制であるという認識を高めるべき。

【法律適用のあり方】

- 対象となる重要情報を特定した上で、組織的に管理をしているという客観的な状態を作ることが重要。
- 営業秘密、限定提供データ、その他のデータと 3 つの分類があり、それによって効果がどう違うかという話をするよりも、これらのデータは全部重要で勝手に漏えいさせたり持ち出したりしてはいけないという教育をしたほうが、理解が容易。
  - 基本的にはその会社で扱っているデータは全部重要であり、漏洩させていいデータはないというような形でリテラシー教育をしていくべき。
  - 退職時にも、基本的に会社のデータは全て持ち出せないという形にして、例外的に持ち出せるものを個別に列挙すべき。

【データの取扱いについて必要な知識】

- これまでデータを意識しなかった企業の意識向上が必要。自社データの重要性を認識させるべき。
- 契約に基づいて取得したデータを誰から受け取ったものなのか、契約条件がどうなっているのかを明確に確認せずに扱っているケースはかなり多い。データが提供先からさらに別の提供先に流通していくと、ますますよくわからない状態になる。今後、こうした状況で契約違反が問題になる事例が増えてきてもおかしくない。

b. 仮説に対して得られた示唆

仮説の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。限定提供データの法知識の周知については、営業秘密の法知識の周知とセットで取り組むことで、従業員への周知が期待できる。

【検証したい仮説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

a. 有識者の分析・意見の要旨

・ 金融庁が金融機関に「サイバーセキュリティ・セルフアセスメントツール」を配布している。その中で、ログ管理は重要なセルフチェック項目となっている。当該ツールは金融機関向けの規制要件を示すものだが、一般企業に同様のアセスメントツールを提供することは有効。

b. 仮説に対して得られた示唆

業界単位でのトップダウンの周知は、仮説の状況の改善に効果がある。

【検証したい仮説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

a. 有識者の分析・意見の要旨

特に議論なし。

b. 仮説に対して得られた示唆

特になし。

③内部不正防止に取り組む組織的体制についての示唆

【検証したい仮説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

a. 有識者の分析・意見の要旨

特に議論なし。

b. 仮説に対して得られた示唆

特になし。

【検証したい仮説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

a. 有識者の分析・意見の要旨

- 情報漏えいに関する内部不正が対象なので、組織全体の責任・権限が IT／セキュリティ部門とリスク管理／コンプライアンス部門で二分されている状況は不思議ではない。
- 内部不正防止は、リスク管理部門が所管し、実行部隊として IT システム部門が対策・モニタリングシステムの運用を行うのが望ましい。重要情報にアクセスできる IT システム部門に対しては、リスク管理部門による牽制機能が必要。

b. 仮説に対して得られた示唆

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。この形態は金融等の企業ガバナンスが厳格に求められる業種・業態で実践されているものだが、仮説の状況を改善できる１つの選択肢として参考にすることができる。

【検証したい仮説③－３】
社内ポリシー／規定の整備が不十分な企業が多い

a. 有識者の分析・意見の要旨

- 就業規則の中で重要情報を漏えいしてはならないと記述することは普通に行われているが、さらに詳細化した営業秘密保護規程まで作成している企業は少ない。

b. 仮説に対して得られた示唆

特になし。

【検証したい仮説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

a. 有識者の分析・意見の要旨

特に議論なし。

b. 仮説に対して得られた示唆

特になし。

【検証したい仮説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

a. 有識者の分析・意見の要旨

- 内部不正防止対策は、現場の担当者からすると、積極的に取り組む動機を持ちにくい傾向があり、経営層のリーダーシップが重要。他方で、経営層の交替によってリーダーシップが崩れてしまう点に問題意識を持っている。
- 大きな事件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、計画的に事前防止に取り組むことが重要。大きな事件が発生していない企業では経営層の意識が高くない恐れがある。
- 主管部門がモニタリング結果を取締役会に報告して議論することは、PDCA を回す上での基本的な態勢であり、KPI 設定のためにも重要。これが必ずしもできていない企業が多いことは懸念材料である。
- 経営層など高い役職の人物が内部不正を行った場合、組織内の内部レビューや内部監査が機能せず、内部不正が組織内で蔓延してしまうリスクがある。例えば、役職の高い人物が持ち込んだ他社情報を部下に分析、共有するように指示すると、法人についても営業秘密侵害が成立することが懸念される。

b. 仮説に対して得られた示唆

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、仮説の状況の改善を期待できる。なお、大きな事件が発生する前にこの取り組みを開始することが必要である。

役職の高い人物が内部不正を行った場合、マネジメントシステムの内部レビューや内部監査が機能しない懸念がある。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である。

【検証したい仮説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

a. 有識者の分析・意見の要旨

特に議論なし。

b. 仮説に対して得られた示唆

特になし。

④組織全体への周知・教育についての示唆

【検証したい仮説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

a. 有識者の分析・意見の要旨 [2]

【内部不正対策の教育の形態】

- セキュリティ対策の一環として情報漏えい対策を教育し、情報漏えい対策の一環として内部不正（重要情報の故意による持ち出し、不注意による漏えい）に気を付けるように周知する形態が一般的。

【望ましいリテラシー教育の方法】

- 法制度については、最低限の知識を身に付けることを前提として、ポイントを絞って必要なことを教育すべき。
- 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ることが一番肝要。個人情報については対応可能でも、営業秘密／限定提供データについて「何をしてはいけないのか」等まで教育できる企業は少ないと見込まれる。
- 自分の実務と具体的にどう繋がっているのかを示しながら教育すべき。

【営業秘密／限定提供データの保護についての教育のあり方】

- 不正競争防止法は、どの企業においても、個人情報保護法と同程度の重要性がある。
- 企業の担当者に対してセミナー等を通じて、法律上の保護を受けられるよう、具備すべき具体的な要件等を共有することが有用。
- 営業秘密保護に係る制度について、法務・知財担当者に留まらず、情報システム担当者にいかにして知識を浸透させるかが重要。

【適切なタイミングでのリテラシー教育の重要性】

- 入社、人事異動、退職等のポイントで営業秘密に関する確認をすることは重要。
- 人事異動の際に、プロジェクトで重要情報に触れることになる従業員に対して、重要情報を具体的に提示し、禁止事項に関して教育することが重要。
- 退職時に具体的に重要情報を提示し、「この情報についてはこういう使い方はしないでください、使うと営業秘密侵害となります」と説明することが有効。

[2] 組織全体への周知・教育と基礎知識は対策と結果の関係にあり、関わりが深いため、ここで述べた要旨は、②の企業・組織として知っておくべき基礎知識に対する仮説の要旨と一部重複している。

【内部不正対策における「内部」の範囲の望ましい捉え方】

・ 企業・組織における内部不正防止体制を考えるに当たり、内部不正の「内部」には従業員だけでなく、経営層（主に役員）、取引先、サプライチェーンも含めるべき。どこまでが企業の内部で、どこからが外部なのかという意識付けをすることが重要。

b. 仮説に対して得られた示唆

仮説の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る。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。

また、一般の職員ではないが、法務・知財担当者を通じて、情報システム担当者に重要情報や内部不正についての必要な法知識を浸透させることも有効である。

【検証したい仮説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

a. 有識者の分析・意見の要旨

【対策実施の必要性が理解できる教育の実践】

・ 社内規程でルールを定めているものの、これに従ってやっていないという印象を受ける。
・ 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）を包み隠さず周知・説明することが重要。とかく大企業ほど、内部不正事案を社員に開示せず、一部関係者のみでそっと処理する実態が見られる。
・ 教育・研修の際に他社事例を入れると抑止効果がある。

【国の政策としての事例周知】

・ 可能であれば企業名も出した上で、内部不正防止ガイドラインに基づいて新たに始めた取り組みや、見直しをした取り組み等の具体的な事例を公表できれば良い。

b. 仮説に対して得られた示唆

仮説の状況を改善する上で、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必要がある。

⑤内部不正防止の課題と対策についての示唆

【検証したい仮説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

a. 有識者の分析・意見の要旨

- 我が国企業における内部不正の認識が総じて低いことがうかがえ、この認識不足が経営層にもそのまま浸透してしまっていると考えられる。意識改革を現場からボトムアップで成立させることは困難であり、国や業界団体から徹底的にトップダウンで実践させる必要がある。
- 個人情報と比較して営業秘密の漏えいへの認識が低い企業も見られ、これが内部不正に対する視野を狭めている。
- 内部不正事案は経営に与える影響が甚大になる恐れがあり、BCP の想定事象の１つとして位置づけるべき。
- 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が明確に定義されていれば、この課題解消の糸口となる。

b. 仮説に対して得られた示唆

仮説の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である。

また、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ることが有効である。

【検証したい仮説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

a. 有識者の分析・意見の要旨

- 従業員監視の強化について社内調整や有効性で悩む企業が多いが、規程類を正しく整備することでその懸念は解消できるはずである。

b. 仮説に対して得られた示唆

特になし。

【検証したい仮説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

a. 有識者の分析・意見の要旨

【重要情報の定義、業務における認識の高さ】

- リスクコントロールマトリックスと、重要な情報の特定をうまく繋げられると良い。

- 重要情報という概念が、企業にとっては依然として顧客情報や個人情報にとどまっているようで、引き続き営業情報や営業秘密といったものの認識が低位にとどまっている。経営層からの指示がなければリスクと重要な情報の紐付けがうまくいかず、経営者の感度が高くない場合にはそのまま放置されてしまう可能性が高い。
- 重要情報の取り扱いについて金融業界が先行しているのは、当局の指導によるところが大きい。製造業については外為法による貿易管理があるほか、経済安全保障によって対応の高度化が自然に促されるはずである。それ以外の業種業態が取り残される恐れがあり、これに対する効果的な施策を打ち出す必要が生じる可能性がある。

【重要情報の特定、分類】

- 企業アンケート調査結果で、営業秘密や重要な技術情報を特定できている企業が５割に達していないのは、衝撃的な結果である。重要情報を特定できていなければ、取り扱いや対応もできない。
- 重要情報を特定する方法を把握できていない企業が多い。自社にとって競争力の源泉となる情報は何かを正確に把握し、事業リスクを踏まえて深掘りができる人材が必要。こうした人材がいない場合、外部のサポートがなければ重要情報の特定は難しいと考える。継続的な支援ができる相談窓口、企業の内部に入り込んで助言する等のサポートが望ましい。
- 重要情報をランク分けすることの重要性は、今後ますます高まっていく。

【個人情報に対する認識が高い理由】

- 個人情報かどうかは、従業員が判断しやすい。
- 経験上、この十年ほどで個人情報法保護法のプレゼンスは相当上がっている気がする。社会情勢、GDPR 等を踏まえ、従業員の個人情報に対する意識が敏感になったと考えられる。
- 個人情報の扱いに対する世間の関心が高いため、個人情報が漏えいすると世間から批判されやすい。このため、レピュテーションリスクによる企業ダメージを避けるべく、きちんと対応していると考えられる。
- 日本の個人情報保護法は違反に対する制裁が大きいわけではなく、基本的に勧告などが法律上の制裁だが、それにしては世間の関心が高いという印象がある。
- 個人情報の特徴は、①対象となる情報がイメージしやすいこと、②法律上、利用目的の公表、利用範囲の限定、第三者提供の制限、漏洩等発生時の個人情報保護委員会への報告、開示、訂正、利用停止などの本人からの請求への対応等、義務が多数存在することであり、企業としては普段から対応を求められることが多い。

【個人情報以外の重要情報に対する認識】

- 営業秘密については、これは営業秘密である、ということをきちんと示しておかないと、別に秘密にしなくてもよいという感覚が生まれやすい。営業秘密をきちんと守らなければいけない、漏えいすると罰則がある、ということをきちんと教えて、当事者意識を持ってもらう必要がある。
- 営業秘密、重要な技術情報等の重要情報は、企業にとっては重要であるが、世間から見ればあまり関心のない情報である。従って、これらの重要情報が漏えいしても世間で大きく取り上げられることは少ない。しかし、自社のリスク認識の低さにより漏えいさせてしまった場合、競合他社に資することになり、事業活動そのものがうまくいかなくなる恐れがあるため、事業リスクとしてはかなり大きい。
- 営業機密、限定提供データについては想定よりは意識されているようだが、個人情報保護への対応と比べると意識は低い印象。個人情報保護法のように、企業として求められる対応を具体的に提示することで、改善される可能性がある。
- 企業の競争力の観点では、営業秘密や限定提供データを守ることによって企業の付加価値向上に資する可能性が高い。しかし、企業は規制対応として個人情報保護への対応を優先させているのが現状。今後は、企業が企業価値の保護に資する営業秘密や限定提供データの保護にさらに取り組むことを期待する。
- 他社から開示を受けた重要情報も含めて営業秘密を特定できている企業の割合が、最低でも個人情報と同程度の水準であることが望ましい。

【他社から受領した重要情報】

- 他社から「重要であるため秘密にしてほしい」と言われて受け取っている情報は、個人情報同様に、流出した際の制裁リスクがあるという点で意識が上がっていると考えられる。体感的には、まだかなり低い水準でしか守られていない印象がある。
- 秘密保持義務契約違反が認められれば損害賠償請求等に問われる可能性が高いが、それにも関わらず現在のような低い水準に留まっているのは問題と言える。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が求められる。

【従業員の教育】

- 全従業員に対してやるべき教育と特定の従業員に対してやるべき教育が、頻度、タイミング、内容において異なるはずであり、使いわける必要がある。

b. 仮説に対して得られた示唆

仮説の状況は、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ができる人材

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。

【検証したい仮説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

a. 有識者の分析・意見の要旨

- 企業・組織における内部不正防止体制を考えるに当たり、内部不正の「内部」には従業員だけでなく、経営層（主に役員）、取引先、サプライチェーンも含めるべき。どこまでが企業の内部で、どこからが外部なのかという意識付けをすることが重要。
- サプライチェーンも含めて一つの組織であるという考え方を浸透させ、リスク管理のための対策を進めるべき。それぞれが独立しているというよりは、運命共同体であるという方向を目指していかなければ、不正を防ぐことはできない時代である。

b. 仮説に対して得られた示唆

仮説の状況のうち、特にサプライチェーンへの対応の遅れについては、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。

【検証したい仮説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

a. 有識者の分析・意見の要旨

【経営層による退職者の情報持ち出しへの感度】

- 従業員の退職・転職が多い企業では情報の持ち出しがよく問題になるため、経営層も感度が高い傾向がある。
- 退職者が多い企業にはその原因があり、これに感度高く対応するとさらに転職率が上がる傾向があり、対策が難しい。

【退職者による重要情報漏えいへの対策強化】

- 退職者による重要情報漏えいへの対策は、社内プロセスをきちんと整備すれば対応できると考えている。
- 退職者が辞める際に、辞意を表明してから実際に退職するまでの間、退職者の重要情報操作を監視していて不正が発覚することが多い。最近は人材の流動化が進んでいるた

め、このような対策の重要性が増している。

- 経営層が退職する際にも、従業員同様に重要情報が持ち出されるケースが多い。しかし、経営層の場合、情報の持ち出しを咎められにくい実態がある。従業員に対する対策が、経営層に対しても同じように適用され、例外は認められないというメッセージを提示することは重要である。
- 退職者による重要情報持ち出しを防止するうえで抑止力にもなるのが、システムへのアクセスログの管理である。意図的に外部に重要情報を持ち出そうとする人間は、退職意志を会社に示した以後に情報を持ち出すだけでなく、相当程度の時間をかけて情報を小分けにして持ち出しているものと想像される。このため、退職者については、少なくとも半年程度（理想的には 1 年間）前までの情報システムへのアクセスログを確認する必要があるだろう。しかし、確認した範囲内ではこうした企業はまだ少ないのが実態である。

【転入者による他社の重要情報の不正持ち込みへの対策】

- 転職で入社した従業員が社内で他社の重要情報をばらまき、警察に組織的な営業秘密の不正利用として捜査されて報道された場合、企業としては大きなダメージを被り、後手の対応になりがちである。経営層としても認識しておくことが必要。

【秘密保持義務の誓約書を求めるタイミング】

- 入社時／退社時に秘密保持義務の誓約書を取っている企業は多いが、重要プロジェクトについては誓約書を取っている企業は非常に少ない。
- 誓約書には何が重要情報かという記載はなく、単に「機密情報」といった一般的な文言しか記載されていないことが多いため、社内ルールとしては機能しているかもしれないが、従業員に対する意識付けまではできていないと考える。秘密情報のランク分けをしておき、ランクが中程度の秘密情報までしか触れていないのであればテンプレートどおりの誓約書でも良いが、重要性の高い秘密に触れている人についてはより強い制約を課すという意味で、誓約書も詳細化する必要がある。特に重要プロジェクトとなると、その必要性が高い。

【従業員のプライバシー保護とモニタリングのバランス】

- プライバシー侵害と社員のモニタリングのどちらを優先するかは従業員の了解も必要だが、日本国内に留まらず、海外においても解決すべき問題である。

b. 仮説に対して得られた示唆

仮説の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ることが有効。

- 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、必要な契約等を行う。
- 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。

【検証したい仮説⑤－６】
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が十分ではない

a. 有識者の分析・意見の要旨

特に議論なし。

b. 仮説に対して得られた示唆

特になし。

【検証したい仮説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

a. 有識者の分析・意見の要旨

特に議論なし。

b. 仮説に対して得られた示唆

特になし。

⑥内部不正防止ガイドライン利用についての示唆

【検証したい仮説⑥－１】
内部不正防止ガイドラインはあまり知られていない

a. 有識者の分析・意見の要旨

【内部不正防止ガイドラインの認知状況】

- 内部不正防止ガイドラインを企業に紹介することはよくあるが、知っている人はあまりいない。

【内部不正防止ガイドラインの認知向上のための方策】

- 経済産業省の「営業秘密管理指針」からの引用、あるいは「秘密情報の保護ハンドブック」に記載する等が考えられる。不正競争防止法の逐条解説に近いような公的文書への引用もよいと考える。

・ セキュリティ関連のガイドラインと内部不正防止ガイドラインが相互に引用する記載を増やすことで、企業が内部不正防止ガイドラインを参照する機会が増えるはずである。
・ 公安調査庁から機微性の高いデータの流出防止に関するパンフレットが出ている。内部不正にかなり関係すると考えられるので、外部参照として相互リンクがあると良い。

【内部不正防止ガイドラインのタイトルと認知の関わり】

・ 「内部不正」という用語に違和感がある。「不正」等の表現の方が妥当である。
・ 「内部不正」という用語にあまり馴染みがない可能性がある。
・ 「内部不正」という用語は意味合いが広いので、知らない人がタイトルを見た時に何の内部不正が対象なのかがもう少し伝わるようにする方が良い。

b. 仮説に対して得られた示唆

仮説の状況は、他の知名度の高い公的文書と内部不正ガイドラインの間で相互引用することで、改善される。また、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。

【検証したい仮説⑥－２】
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

a. 有識者の分析・意見の要旨

【活用促進に資するための内容改訂】

・ ガイドラインを見ると、内部不正に関して「資産の授受」という項目が見当たらない。提供先において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と考える。
・ 内部不正防止ガイドラインは、規定に基づいた対策を説明する準則アプローチの方法を取っている。リスクアプローチの方法で記載することもありうる。

【活用して取り組みを始めるまでのサポートができる体制の整備】

・ 企業が内部不正防止ガイドラインの内容を読み解いた上で、自主的に内部不正防止に取り組むには少し内容が難しい。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。
・ 弁護士等の外部の専門家はサービスを提供するために内部不正防止ガイドラインを参照し、有用な資料として活用している。

【活用するためのツール整備】

- 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。
- 内部不正防止について先進的な取り組みを行っている企業の好事例を公開して周知することで、企業全体の底上げを目指すべき。現状は適用しうる管理手法を説明することに留まっているが、企業が取り組むべきことを明示して、どれを実践しなければならないのかを明確にすると良い。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。

b. 仮説に対して得られた示唆

仮説の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。

4. 調査結果の分析

ここでは、アンケート調査のクロス集計及びアンケート調査結果とインタビュー調査結果の比較を行うことで、第 3 章で報告した調査結果のクロス分析を実施した。クロス分析は各仮説に対して行っている。分析結果を以下に示した。

(1) 企業アンケート調査のクロス集計による分析

パネルモニターによる企業アンケート調査の回答（1179 名）を用いて、クロス集計による分析を実施した。回答者の中には経営層が 167 名含まれており、その約 70%は中小企業の経営層、約 15%は常時雇用者数が 1,000 人を超える大企業の経営者である。

【検証したい仮説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

仮説②－４に関する単純集計結果からは、情報漏えい／セキュリティリスクに関する組織全体での知識レベルはまだ十分とは言えないことが分かっている。それでは経営層は、これらについての組織全体での知識レベルをどのように見ているのだろうか。これについて分析するため、「回答者の担当業務の違いによる、「組織全体のリスク認識の現状」についての感じ方の違い」についてクロス集計を行い、その結果を分析したところ、各リスクで概ね同じような傾向が見られた。ここでは経営層との関わりが深い次の２つのリスクについてクロス集計結果を図表 55 に示した。

- サプライチェーンにおける不必要な重要情報の授受
- 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

経営層においては、これらのリスクが「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、経営層は組織が情報漏えい／セキュリティリスクに関する知識を持っていることに懐疑的な傾向を持っており、課題を感じているものと考えられる。

次に、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、情報漏えい／セキュリティリスクに関する知識の習得も進んでいるのかについて分析するため、「内部不正リスクが重要な経営課題として捉えられているかの違いによる組織全体のリスク認識の現状の違い」についてクロス集計を行い、その結果を分析した。クロス集計結果は図表 56 に示した。その結果、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ことが分かった。

図表 55 回答者の担当業務の違いによる組織全体のリスク認識の現状についての感じ方の違い

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。
～サプライチェーンにおける不必要な重要情報の授受

■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

		n=	(%)			
	TOTAL	1179	27.7	41.8	17.2	13.3
SQ1H 担当業務	情報システム関連部門の担当者または責任者	384	28.9	42.4	13.8	14.8
	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	33.3	45.2	15.7	5.7
	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	160	28.1	40.6	21.9	9.4
	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	23.6	43.4	16.7	16.3
	経営層	167	23.4	34.7	23.4	18.6

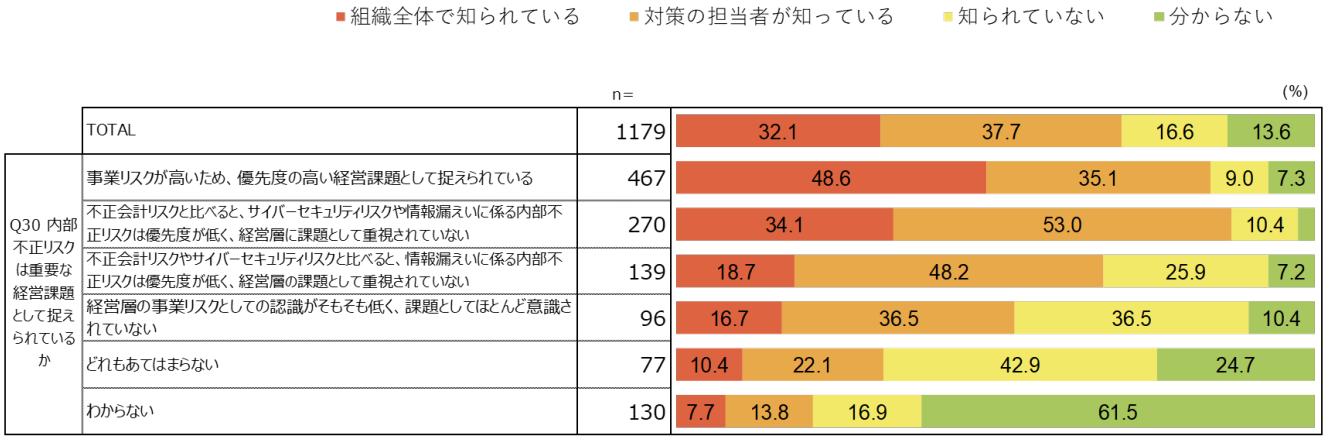
～外国政府が関与した重要技術情報への合法的／非合法的アプローチ

■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

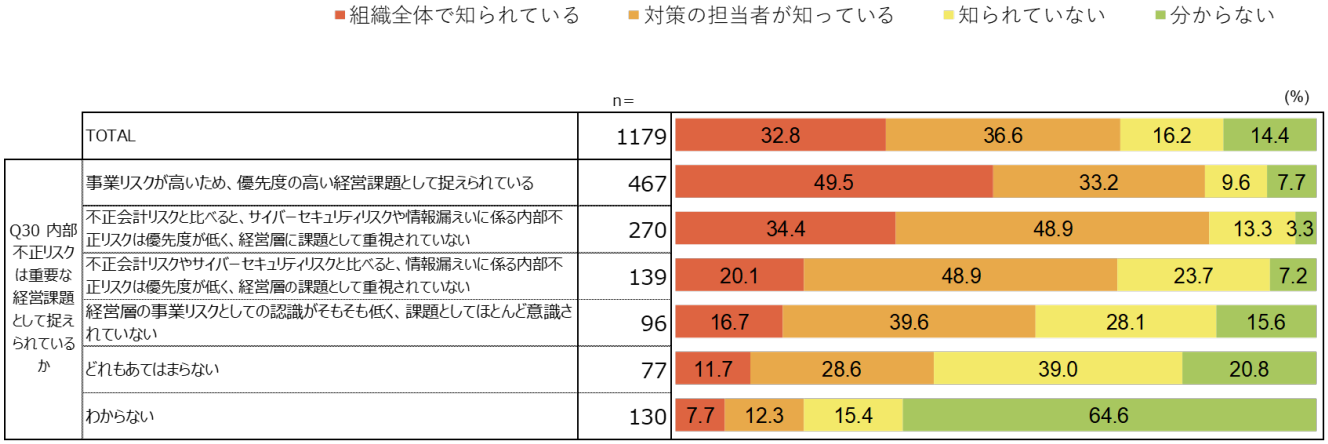
		n=	(%)			
	TOTAL	1179	24.5	33.8	22.0	19.8
SQ1H 担当業務	情報システム関連部門の担当者または責任者	384	28.1	32.8	19.5	19.5
	リスクマネジメントの企画・運用に関わる部署の担当者または責任者	210	26.2	44.3	19.5	10.0
	経営企画部門における企業・組織のIT／セキュリティ戦略の担当者または責任者	160	25.0	39.4	21.3	14.4
	上記以外の、リスクマネジメントに関する業務の担当者	258	22.1	29.1	21.7	27.1
	経営層	167	17.4	24.6	31.7	26.3

図表 56 内部不正リスクが重要な経営課題として捉えられているかの違いによる組織全体のリスク認識の現状の違い

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。
～テレワークの不十分なセキュリティガバナンス



～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



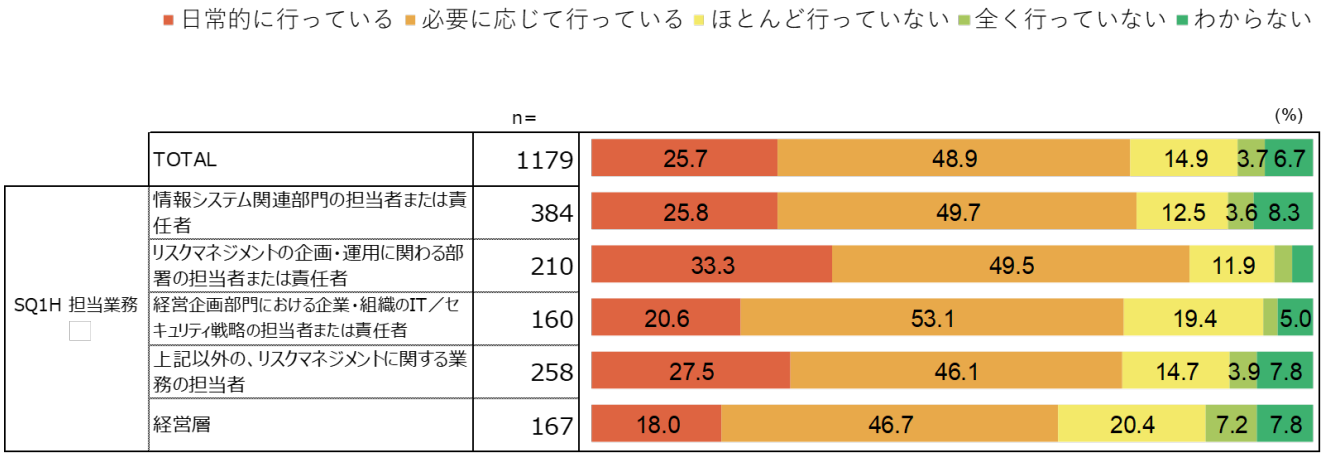
【検証したい仮説③－１】
経営層の情報発信が明確ではない、又は不十分な企業が多い

仮説③－１に関する単純集計結果からは、経営層の情報発信が高い割合で従業員に認知されていることが分かっている。それでは経営層自身は、内部不正防止の取組み方針等に関する自らの情報発信の度合いについてどのように見ているのだろうか。これについて分析するため、「回答者の担当業務の違いによる経営層が方針を周知・指示しているかの現状についての感じ方の違い」についてクロス集計を行い、その結果を分析した。クロス集計結果は図表 57 に示した。その結果、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。今年度の調査結果から、経営層と従業員の間でどうしてこのような認識のギャップが生じるのかの理由を分析することは難しいが、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。

図表 57 回答者の担当業務の違いによる
経営層が方針を周知・指示しているかの現状についての感じ方の違い

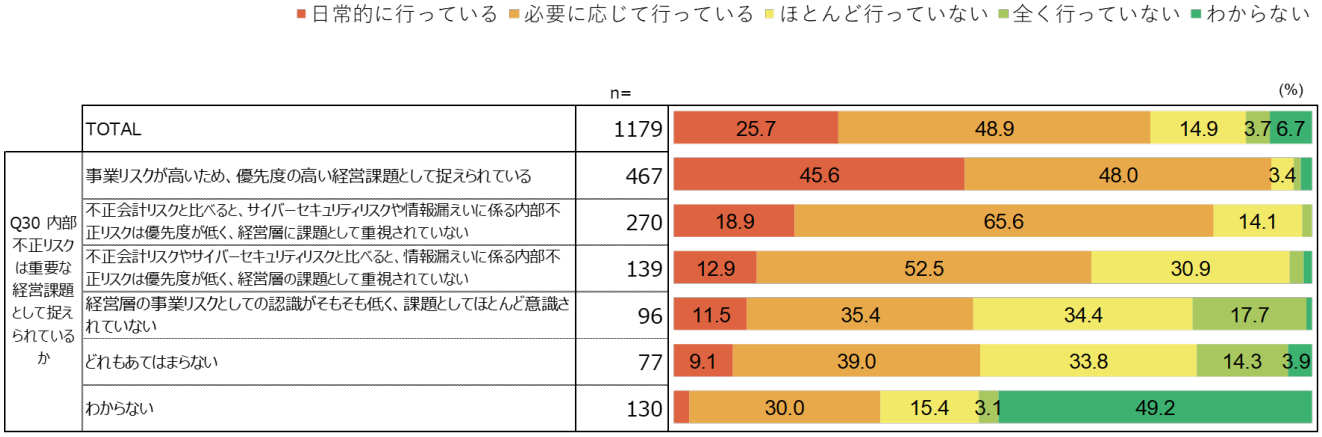
Q18 経営層は、組織全体での内部不正防止の取組み方針等について、全従業員に周知、指示していますか。



次に、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、経営層は積極的に内部不正防止の取組み方針等を全従業員に周知、指示しているのかについて分析するため、「内部不正リスクが重要な経営課題として捉えられているかの違いによる、経営層が方針を周知・指示しているかの現状の違い」についてクロス集計を行い、その結果を分析した。クロス集計結果は図表 58 に示した。その結果、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ことが分かった。

図表 58 内部不正リスクが重要な経営課題として捉えられているかの違いによる経営層が方針を周知・指示しているかの現状の違い

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。



【検証したい仮説③－３】
社内ポリシー／規定の整備が不十分な企業が多い

仮説③－３に関する単純集計結果からは、内部不正防止に関する社内ポリシー／規定の整備が不十分な企業が多いことが分かっている。それでは、内部不正リスクを重要な経営課題として捉えている企業ではどうであろうか。これについて分析するため、「内部不正リスクが重要な経営課題として捉えられているかの違いによる策定されている指針や規則の現状の違い」についてクロス集計を行い、その結果を分析した。クロス集計結果は図表 59 に示した。その結果、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ことが分かった（表中の赤い色付け部分）。

図表 59 内部不正リスクが重要な経営課題として捉えられているかの違いによる策定されている指針や規則の現状の違い

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。

		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					
	TOTAL	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
n=	1179	467	270	139	96	77	130
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）	33.3	48.2	33.3	26.6	20.8	10.4	10.0
内部統制の基本方針（内部不正防止の基本方針を含む）	45.7	60.6	45.6	46.0	26.0	29.9	16.2
セキュリティポリシー（内部不正防止の基本方針を含む）	47.2	59.7	49.3	43.9	31.3	31.2	22.3
就業規則に書かれた内部不正防止に関するルール	42.2	55.7	33.7	38.1	40.6	37.7	20.0
組織全体に適用される重要情報の分類規則	26.0	39.2	20.0	23.0	15.6	13.0	10.0
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	20.5	32.8	15.6	16.5	11.5	10.4	3.8
組織全体に適用される重要情報の分離保管規則	17.3	28.9	11.1	15.1	8.3	7.8	3.1
個人情報管理のための規則	36.9	52.0	23.7	27.3	35.4	32.5	23.8
営業秘密管理のための規則	23.8	39.4	13.0	15.1	20.8	13.0	8.5
限定提供データの管理のための規則	16.8	26.1	12.6	13.7	12.5	7.8	3.8
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）	25.9	37.9	19.3	24.5	12.5	22.1	10.0
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）	19.0	28.1	17.0	15.8	11.5	9.1	5.4
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	23.0	34.5	17.8	13.7	20.8	13.0	10.0
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	23.3	37.9	14.1	18.7	12.5	10.4	10.8
どれもあてはまらない	3.1	0.6	0.0	0.0	11.5	20.8	4.6
わからない	7.2	1.1	1.1	1.4	4.2	3.9	52.3

【検証したい仮説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

仮説④－１に関する単純集計結果からは、「１．個人情報の漏えい事件／インシデントが発生」を選択した割合が最も大きいものの「２．営業秘密の漏えい事件・インシデントが発生」や「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」を選択した割合との差は小さい。他方で、その他の「転職に関する事態（選択肢４．、５．に該当）」を選択した割合は、上記の情報漏えいと比べて小さいことが分かっている。それでは、業種・業態や企業規模によってはどのような傾向の違いが見られるだろうか。これについて分析するため、「業種による内部不正事件／疑われる事態の発生状況の違い」と「常用雇用者数の違いによる内部不正事件／疑われる事態の発生状況の違い」についてクロス集計を行い、その結果を分析した。クロス集計結果は図表 60 と図表 61 にそれぞれ示した。

個人情報の漏えい事件／インシデントについては、金融業・保険業が最も高い割合で経験している。これは金銭や健康等に係る機微な個人情報を取扱うサービスを提供していることが理由であると考えられる。この他、回答数が 30 以上ある業種では、通信業、学術研究・専門／技術サービス業が 50%を超えている。次に営業秘密の漏えい事件／インシデントについては、製造業が全般に高い割合になっており、回答数が 10 以上ある製造業の業態では情報通信機械器具製造業が 70.6%で最も高く、次に電子応用装置・電気計測機器製造業が 61.5%であり、鉄鋼業、業務用機械器具製造業が 50%を超えている。製造業で事件／インシデントが多いのは、重要技術情報・ノウハウを取扱うからであると考えられる。なお製造業については、限定提供データの漏えい事件／インシデントや他の転職に関する事態についても経験した割合が高い傾向が見られる。

他方で、企業規模との関係を見てみると、個人情報、営業秘密、限定提供データの全てにおいて、企業規模が大きくなるほど内部不正事件／疑われる事態を経験した割合が大きくなっている。転職に関する事態もほぼ同じ傾向である。但し、この調査結果だけから、中小企業では内部不正／疑われる事態が少ないと結論付けるのは早計であると考えられる。大企業のサプライチェーン上で製造技術等の重要情報を管理している中小企業が、内部不正／疑われる事態を見逃している可能性を否定できない。

図表 60 業種による内部不正事件／疑われる事態の発生状況の違い

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。

		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
Q3 企業・組織の業種	1. 農業、林業、漁業	13	15.4	30.8	38.5	0.0	0.0	7.7	15.4
	2. 鉱業、採石業、砂利採取業	7	14.3	57.1	14.3	14.3	14.3	0.0	0.0
	3. 建設業	78	29.5	35.9	23.1	19.2	11.5	6.4	29.5
	4. 食料品製造業	40	30.0	40.0	37.5	17.5	20.0	5.0	25.0
	5. 飲料・たばこ・飼料製造業	3	0.0	66.7	33.3	33.3	33.3	0.0	0.0
	6. 繊維工業	11	27.3	54.5	9.1	27.3	9.1	0.0	9.1
	7. 化学工業	23	34.8	39.1	43.5	26.1	13.0	4.3	21.7
	8. プラスチック製品製造業	7	0.0	14.3	28.6	14.3	14.3	0.0	42.9
	9. ゴム製品製造業	3	33.3	33.3	33.3	33.3	33.3	0.0	33.3
	10. 鉄鋼業	12	25.0	50.0	41.7	8.3	16.7	0.0	25.0
	11. はん用機械器具製造業	3	33.3	33.3	0.0	33.3	0.0	66.7	0.0
	12. 生産用機械器具製造業	24	41.7	37.5	50.0	29.2	29.2	4.2	12.5
	13. 業務用機械器具製造業	11	63.6	54.5	45.5	54.5	27.3	0.0	9.1
	14. 電子部品・デバイス・電子回路製造業	38	44.7	36.8	23.7	39.5	26.3	13.2	23.7
	15. 電子応用装置・電気計測器製造業	13	38.5	61.5	53.8	30.8	15.4	7.7	7.7
	16. 15以外の電気機械器具製造業	25	44.0	36.0	28.0	24.0	16.0	12.0	24.0
	17. 情報通信機械器具製造業	17	41.2	70.6	47.1	41.2	29.4	5.9	5.9
	18. 自動車・同附属部品製造業	23	39.1	26.1	21.7	30.4	21.7	17.4	26.1
	19. 18以外の輸送用機械器具製造業	3	33.3	66.7	33.3	0.0	0.0	0.0	33.3
	20. 4～19以外の製造業	59	25.4	40.7	27.1	27.1	13.6	6.8	33.9
	21. 電気・ガス・熱供給・水道業	23	43.5	30.4	30.4	17.4	0.0	4.3	17.4
	22. 通信業	34	52.9	35.3	32.4	26.5	14.7	2.9	23.5
	23. 放送業	2	0.0	0.0	0.0	0.0	0.0	0.0	100.0
	24. 情報サービス業	143	30.1	27.3	19.6	14.7	9.1	7.7	46.2
	25. インターネット附随サービス業	26	26.9	26.9	23.1	23.1	11.5	7.7	38.5
	26. 映像・音声・文字情報制作業	6	0.0	0.0	0.0	0.0	0.0	16.7	83.3
	27. 運輸業、郵便業	60	31.7	40.0	28.3	31.7	13.3	15.0	25.0
	28. 卸売業、小売業	95	31.6	31.6	26.3	14.7	11.6	12.6	28.4
	29. 金融業、保険業	87	67.8	42.5	34.5	21.8	14.9	5.7	19.5
	30. 不動産業、物品賃貸業	31	38.7	25.8	29.0	29.0	16.1	9.7	16.1
	31. 学術研究、専門・技術サービス業	31	54.8	29.0	29.0	35.5	12.9	3.2	25.8
	32. 宿泊業、飲食サービス業	27	33.3	29.6	18.5	7.4	11.1	3.7	44.4
	33. 31、32以外のサービス業	137	33.6	32.1	27.0	19.0	16.8	10.2	27.0
	34. 公務（他に分類されるものを除く）	20	45.0	45.0	35.0	20.0	20.0	10.0	10.0
	35. 分類不能の産業	44	31.8	27.3	34.1	22.7	18.2	6.8	34.1

図表 61 常用雇用者数の違いによる内部不正事件／疑われる事態の発生状況の違い

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。

		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

次に、内部不正防止の責任部門が情報システム／セキュリティ管理部門である場合、及びリスク管理／コンプライアンス部門である場合について、従業員へのリテラシー教育の内容に違いが見られるかを分析してみた。この分析のため、「責任部門の違いによる実施しているリテラシー教育の内容の違い」についてクロス集計を行った。クロス集計結果は図表 62 に示した。責任部門が情報システム／セキュリティ管理部門である場合、重要情報の分類と表示に関する規則の教育に力を入れている傾向が見られた。他方で、責任部門がリスク管理／コンプライアンス部門である場合は、単純集計結果と比べて特に目立った差異は見られなかった。

さらに、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がどの内容の教育に注力しているかを分析するため「内部不正リスクが重要な経営課題として捉えられているかの違いによる策定されている指針や規則の現状の違い」についてクロス集計を行った。クロス集計結果は図表 63 に示した。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（表の赤で色付けした部分左端の 2 枠）。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（赤で色付けした部分の左から 3 番目の枠）、一層の底上げが期待される。この結果は、内部不正リスクを重要な経営課題と捉えている企業であっても、営業秘密保護に対する認識がまだ十分とは言えない可能性を示唆している。

図表 62 責任部門の違いによる実施しているリテラシー教育の内容の違い

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。

		Q20 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			
	TOTAL	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
n=	948	383	472	77	16
重要情報の分類と表示に関する規則	57.1	67.9	53.0	33.8	31.3
個人情報保護の法制度に関する知識	66.1	66.8	68.2	55.8	37.5
営業秘密保護の法制度に関する知識	47.2	47.3	48.1	41.6	43.8
限定提供データ保護の法制度に関する知識	31.6	36.3	29.7	20.8	31.3
機微技術情報の管理に関する外為法についての知識	27.3	31.6	25.4	15.6	37.5
クラウド利用許可に関する規則	21.2	25.1	20.6	9.1	6.3
BYOD（個人所有PC／デバイスの業務利用）の使用規則	21.4	24.8	19.7	15.6	18.8
テレワークに関する内部規則や関連法令	25.7	30.5	24.2	14.3	12.5
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	19.4	21.9	19.9	6.5	6.3
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	24.3	26.6	23.9	16.9	12.5
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	22.0	23.5	22.7	14.3	6.3
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	14.8	17.2	14.0	7.8	12.5
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	22.3	23.5	22.9	11.7	25.0
どれもあてはまらない	1.4	1.6	0.4	6.5	0.0
わからない	1.5	2.1	0.8	1.3	6.3

図表 63 内部不正リスクが重要な経営課題として捉えられているかの違いによる実施しているリテラシー教育の内容の違い

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。

		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					
	TOTAL	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
n=	948	453	253	121	55	34	32
重要情報の分類と表示に関する規則	57.1	72.4	45.1	38.0	45.5	38.2	46.9
個人情報保護の法制度に関する知識	66.1	76.6	56.1	53.7	58.2	58.8	65.6
営業秘密保護の法制度に関する知識	47.2	54.1	42.3	40.5	38.2	47.1	28.1
限定提供データ保護の法制度に関する知識	31.6	37.3	30.0	26.4	21.8	26.5	6.3
機微技術情報の管理に関する外為法についての知識	27.3	34.7	21.3	25.6	16.4	17.6	6.3
クラウド利用許可に関する規則	21.2	26.0	17.0	17.4	14.5	20.6	12.5
BYOD（個人所有PC／デバイスの業務利用）の使用規則	21.4	32.2	11.1	9.9	9.1	23.5	12.5
テレワークに関する内部規則や関連法令	25.7	34.7	16.6	15.7	20.0	29.4	15.6
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	19.4	28.0	12.6	9.1	12.7	14.7	6.3
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	24.3	33.6	13.8	12.4	21.8	38.2	9.4
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	22.0	28.3	17.0	14.0	18.2	29.4	3.1
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	14.8	17.9	13.0	10.7	10.9	14.7	6.3
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）	22.3	32.2	12.6	8.3	14.5	32.4	12.5
どれもあてはまらない	1.4	0.7	0.4	0.0	9.1	8.8	3.1
わからない	1.5	1.3	0.4	0.0	0.0	5.9	15.6

【対策実施の現状（全体像の俯瞰）】

「常用雇用者数の違いによる実施している対策の現状の違い」と「内部不正リスクが重要な経営課題として捉えられているかの違いによる実施している対策の現状の違い」についてクロス集計を行い、その結果を分析した。クロス集計結果は図表 64 と図表 65 に示した。

図表 64 によると、企業規模が 5,000 人を超えると、内部不正防止対策を実施している企業の割合が、対策全般に亘って明らかに高まっており（表の赤で色付けした部分）、50%を超える企業が実施している対策もいくつか見られるようになる。

図表 65 を見ると、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、あきらかに内部不正防止対策を実施している割合が高まっており（表の赤で色付けした部分）、しかもそれはほぼ全部の対策に亘っている。対策を実施している企業の割合が単純集計結果からの差分で 10%を超えて大きく増加している内部不正対策も多く、経営層による周知徹底／基本方針策定、重要情報特定方法の周知、内部不正防止に関する責任者の配置、定期的等のリテラシー教育、秘密保持義務契約の締結、退職後の ID／アクセス権限等の削除、不満が蓄積しない職場環境の整備、多数の技術的対策等がこれに当たる。

図表 64 常用雇用者数の違いによる実施している対策の現状の違い

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。

		Q4 常用雇用者数								
	TOTAL	300人以下（小計）	301人以上（小計）	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
n=	1179	543	636	129	175	239	211	206	81	138
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	49.0	38.9	57.7	31.8	36.0	44.8	51.2	58.3	64.2	63.0
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	34.7	28.9	39.6	24.8	23.4	35.1	40.3	35.4	42.0	43.5
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	33.2	27.8	37.9	20.2	25.7	33.5	36.5	33.5	48.1	40.6
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	29.7	26.5	32.4	23.3	26.9	28.0	30.3	27.7	39.5	38.4
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	42.1	33.9	49.1	27.1	33.7	37.7	43.1	49.5	61.7	50.0
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	27.7	23.9	31.0	11.6	27.4	28.0	28.4	30.1	28.4	37.7
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	41.8	34.6	48.0	20.2	35.4	41.8	40.8	50.5	53.1	52.2
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	21.3	16.6	25.3	16.3	16.0	17.2	18.0	24.3	33.3	33.3
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	28.4	21.7	34.1	18.6	19.4	25.1	33.2	33.0	39.5	34.1
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	19.8	13.6	25.2	8.5	11.4	18.0	23.2	24.3	27.2	28.3
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	32.7	28.5	36.3	23.3	28.6	31.4	35.5	34.5	45.7	34.8
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	32.5	26.3	37.7	22.5	26.9	28.0	32.2	40.8	42.0	39.1
ID管理と本人確認（認証）を強化している	35.5	26.7	43.1	17.1	26.9	31.8	38.9	44.2	50.6	43.5
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	18.4	12.7	23.3	6.2	14.9	14.6	22.3	17.0	33.3	28.3
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	30.4	24.7	35.2	16.3	25.7	28.5	32.7	33.5	43.2	37.0
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	19.8	14.0	24.8	10.1	15.4	15.1	20.4	19.4	34.6	34.1
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	35.0	26.5	42.3	14.7	25.1	33.9	40.3	42.7	51.9	39.1
BYOD（個人デバイスの業務利用）は許可していない	21.1	15.5	25.9	14.7	10.9	19.2	19.9	26.2	37.0	28.3
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	31.4	22.3	39.2	11.6	21.1	28.9	35.5	37.4	46.9	42.8
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	21.4	13.4	28.1	10.1	9.1	18.4	25.6	23.3	38.3	33.3
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	19.7	12.5	25.8	11.6	10.3	14.6	22.3	22.3	30.9	33.3
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	22.9	16.6	28.3	13.2	17.7	17.6	25.1	26.2	37.0	31.2
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	15.9	8.8	21.9	4.7	6.9	12.6	17.5	20.4	22.2	30.4
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	17.6	12.5	22.0	11.6	9.7	15.1	16.1	21.4	29.6	27.5
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	35.3	27.4	42.0	17.8	26.3	33.5	36.5	41.3	54.3	44.2
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	29.0	23.9	33.3	15.5	25.1	27.6	29.9	30.1	42.0	38.4
どれもあてはまらない	9.6	12.3	7.2	17.8	13.7	8.4	8.1	8.7	3.7	5.8

図表 65 内部不正リスクが重要な経営課題として捉えられているかの違いによる実施している対策の現状の違い

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。

		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					
	TOTAL	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
n=	1179	467	270	139	96	77	130
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	49.0	73.4	45.2	34.5	22.9	23.4	19.2
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	34.7	44.5	34.1	38.1	21.9	24.7	12.3
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	33.2	44.8	33.7	29.5	20.8	20.8	11.5
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	29.7	41.1	23.7	27.3	16.7	22.1	17.7
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	42.1	63.4	32.2	29.5	26.0	29.9	18.5
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	27.7	35.8	21.1	33.1	22.9	18.2	16.2
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	41.8	62.7	30.0	33.8	33.3	20.8	18.5
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	21.3	28.5	16.7	18.7	15.6	18.2	13.8
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	28.4	39.4	26.3	25.2	21.9	16.9	8.5
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	19.8	27.8	20.4	15.1	12.5	9.1	6.9
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	32.7	47.5	20.0	26.6	30.2	26.0	18.5
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	32.5	52.0	23.3	20.1	20.8	15.6	13.1
ID管理と本人確認（認証）を強化している	35.5	55.0	24.8	26.6	19.8	19.5	18.5
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	18.4	30.0	11.9	17.3	9.4	6.5	5.4
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	30.4	46.0	17.0	18.7	31.3	19.5	20.0
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	19.8	33.0	11.9	7.9	9.4	13.0	13.8
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	35.0	53.7	24.4	20.9	19.8	20.8	24.6
BYOD（個人デバイスの業務利用）は許可していない	21.1	34.3	10.0	12.9	13.5	14.3	15.4
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	31.4	49.3	21.1	20.1	25.0	14.3	15.4
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	21.4	33.4	15.6	17.3	10.4	9.1	10.0
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	19.7	30.4	14.1	14.4	10.4	11.7	10.0
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	22.9	35.3	12.6	23.7	9.4	18.2	11.5
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	15.9	28.7	9.6	7.9	5.2	9.1	3.1
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	17.6	28.1	12.2	13.7	9.4	11.7	5.4
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	35.3	52.5	28.1	25.2	31.3	10.4	16.9
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	29.0	39.0	23.7	23.7	26.0	20.8	16.9
どれもあてはまらない	9.6	1.1	1.5	1.4	17.7	29.9	47.7

【検証したい仮説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⑤－１に関する単純集計結果からは、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十分に高い水準に達しているとは言えないという示唆が得られている。しかし、クロス集計による他の分析（図表 56、図表 58、図表 59、図表 63、図表 65 参照）を見ると、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、それ以外の企業と比べると、内部不正防止に関する取り組みや対策の実施状況が明らかに進展している。以上を考慮すると、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、企業の内部不正防止対策や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。

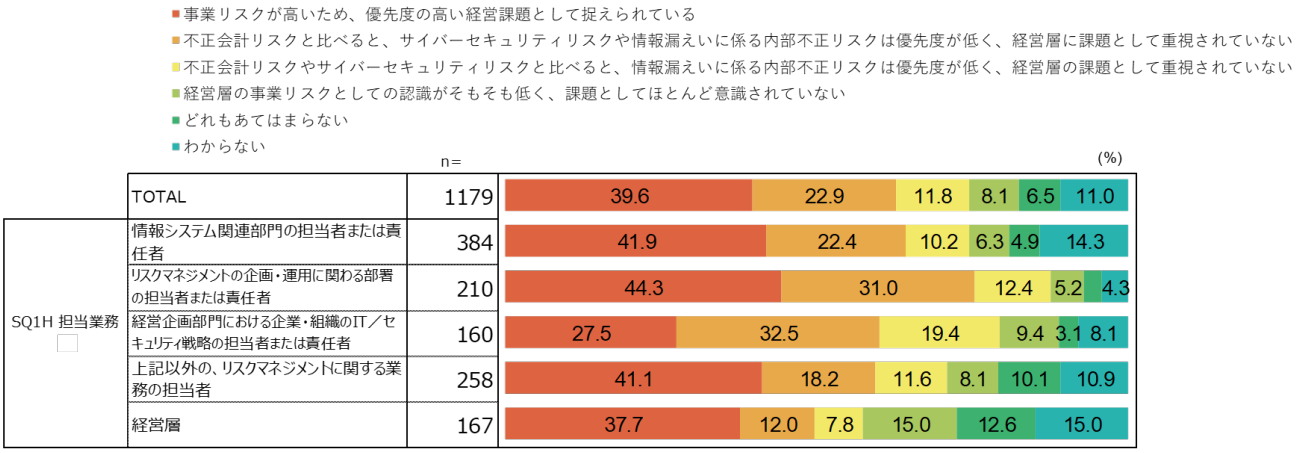
ここでは以上を勘案し、経営層が内部不正リスクを重要な経営課題として認識しているかについて現状を深掘りした。このため、「担当業務の違いによる内部不正リスクを重要な経営課題と捉えているかの現状についての感じ方の違い」についてクロス集計を行い、その結果を分析した。クロス集計結果は図表 66 に示した。この結果を見ると、単純集計結果と比較して経営層には次の特徴があることが分かる。

- 「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」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っている（34.7%→19.8%）。
- 「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（19.1%→30%）。

従って「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（割合は単純集計結果とほぼ同じ）」と「経営課題としてほとんど意識していない経営層（単純集計よりも割合が増えている）」にはっきりと分かれる傾向が見られ、特に「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」や「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」との違いが顕著である。この実態を踏まえると、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と言える。

図表 66 担当業務の違いによる
内部不正リスクを重要な経営課題と捉えているかの現状についての感じ方の違い

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。



		n=	(%)						
	TOTAL	1179	39.6	22.9	11.8	8.1	6.5	11.0
SQ1H 担当業務	情報システム関連部門の担当者または責任者	384	41.9	22.4	10.2	6.3	4.9	14.3
	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	44.3	31.0	12.4	5.2	4.3	
	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責任者	160	27.5	32.5	19.4	9.4	3.1	8.1
	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	41.1	18.2	11.6	8.1	10.1	10.9
	経営層	167	37.7	12.0	7.8	15.0	12.6	15.0

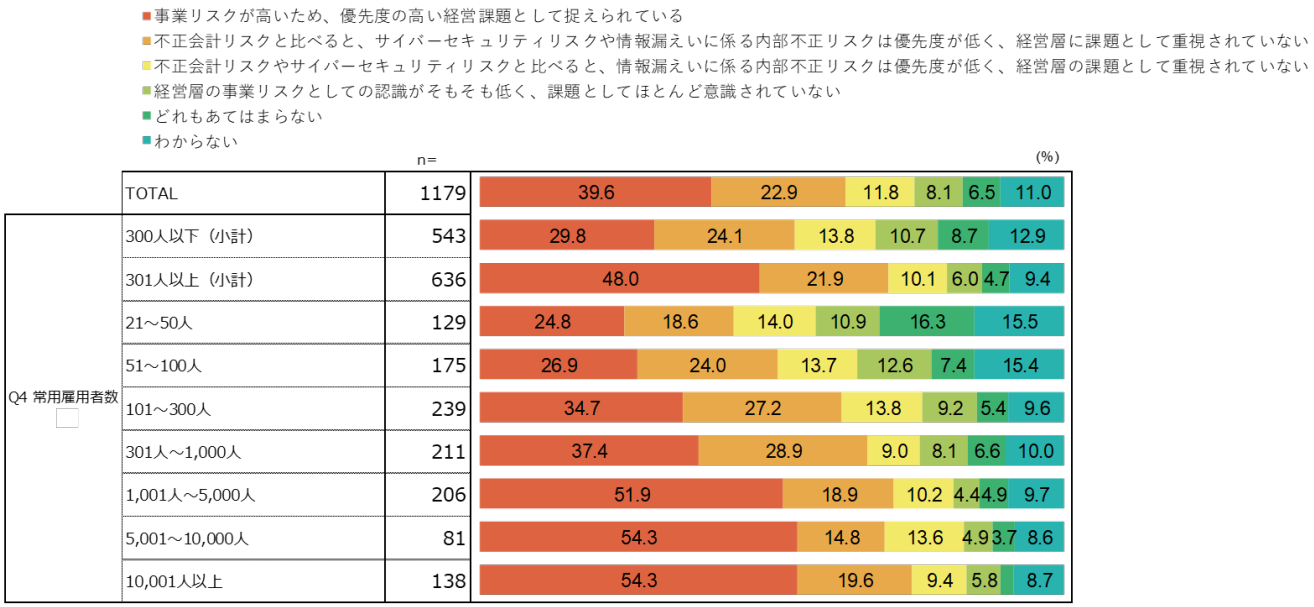
さらに次の 3 つの要素が、企業が内部不正リスクを重要な経営課題として認識することにどのように関係しているかを分析することとした。

- 企業規模（常用雇用者数）
- 責任部門の違い
- 内部不正事件等の経験の違い

まず、企業規模による違いを分析するため、「常用雇用者数の違いによる内部不正リスクを重要な経営課題と捉えているかの現状の違い」についてクロス集計を行い、その結果を分析した。クロス集計結果は図表 67 に示した。この結果を見ると、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、企業規模が大きくなるについて着実に伸びており、特に常時雇用者数が 1,000 人を超える企業ではこの割合が 50%を超えている。この状況を踏まえると、中小企業の経営層に対する内部不正リスクの周知啓発が重要であることが分かる。

図表 67 常用雇用者数の違いによる
内部不正リスクを重要な経営課題と捉えているかの現状の違い

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。

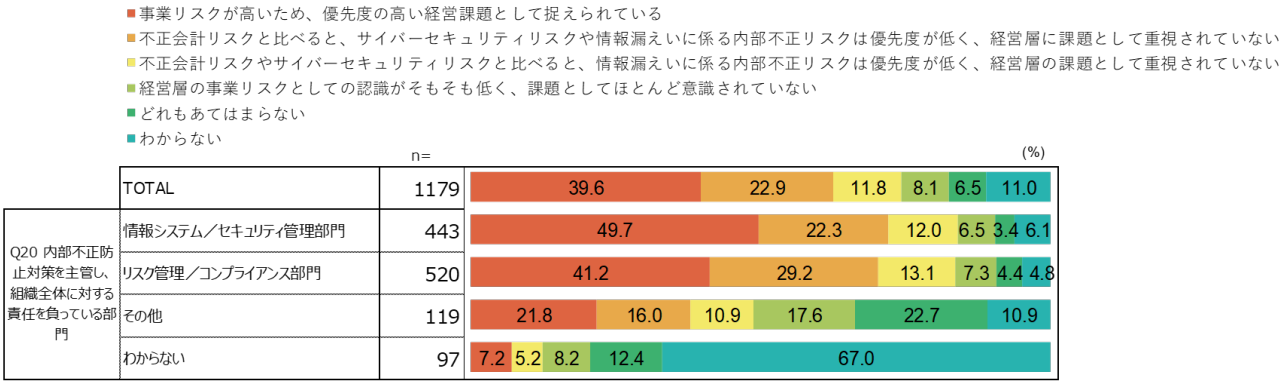


		n=	(%)						
	TOTAL	1179	39.6	22.9	11.8	8.1	6.5	11.0	
Q4 常用雇用者数	300人以下（小計）	543	29.8	24.1	13.8	10.7	8.7	12.9	
	301人以上（小計）	636	48.0	21.9	10.1	6.0	4.7	9.4	
	21～50人	129	24.8	18.6	14.0	10.9	16.3	15.5	
	51～100人	175	26.9	24.0	13.7	12.6	7.4	15.4	
	101～300人	239	34.7	27.2	13.8	9.2	5.4	9.6	
	301人～1,000人	211	37.4	28.9	9.0	8.1	6.6	10.0	
	1,001人～5,000人	206	51.9	18.9	10.2	4.4	4.9	9.7	
	5,001～10,000人	81	54.3	14.8	13.6	4.9	3.7	8.6	
	10,001人以上	138	54.3	19.6	9.4	5.8		8.7	

次に、責任部門による違いを分析するため、「責任部門の違いによる内部不正リスクを重要な経営課題と捉えているかの現状の違い」についてクロス集計を行い、その結果を分析した。クロス集計結果は図表 68 に示した。この結果を見ると、内部不正防止を情報システム／セキュリティ管理部門が主管する場合の方が、リスク管理／コンプライアンス部門が主管する場合よりも、内部不正を優先度の高い経営課題として捉えている割合が高くなっている。この結果は、事業リスク管理に直接関わるリスク管理部門が内部不正リスクに対する感度が低いことを示唆しており、想定外の結果となっている。このような結果が出た理由をこの調査の結果から推定することは難しいため、今後さらなる調査分析が必要である。

図表 68 責任部門の違いによる
内部不正リスクを重要な経営課題と捉えているかの現状の違い

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。

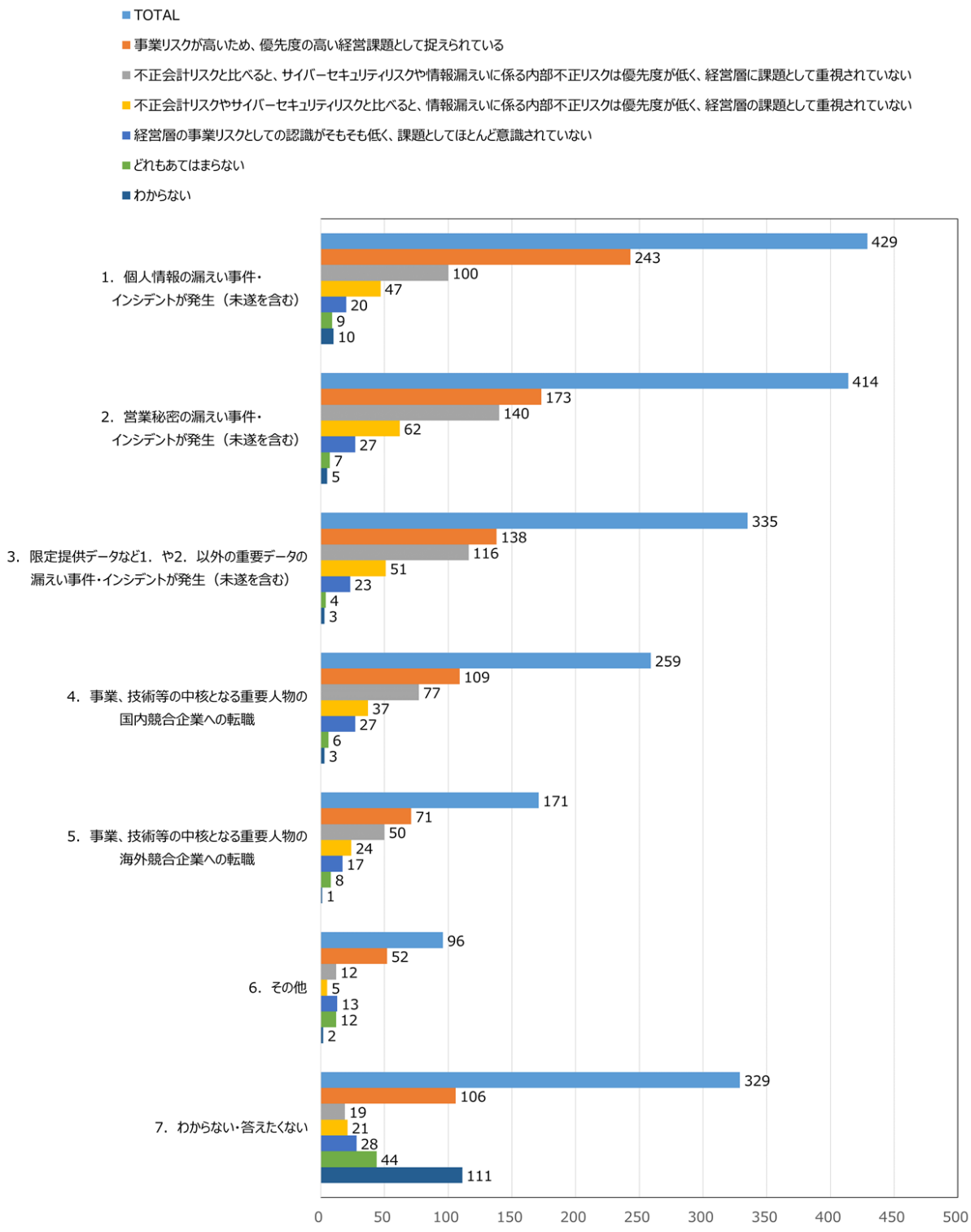


最後に、内部不正事件等の経験が、企業が内部不正リスクを重要な経営課題として認識することにどのような影響を及ぼすかについて分析した。この分析のために、「内部不正事件等の経験の違いによる内部不正リスクを重要な経営課題と捉えているかの現状の違い」についてクロス集計を行った。クロス集計結果は図表 69 に示した。この結果を見ると、個人情報の漏えい事件／インシデントを経験した企業では、内部不正リスクを重要な経営課題として捉えている割合が顕著に大きくなっている。これに対して、営業秘密の漏えい事件／インシデントや事業／技術の中核人材の国内競合企業への転職を経験した企業では、内部不正リスクを重要な経営課題として捉えている割合がそれほどでもないという結果となっている。この調査結果は、企業が依然として、内部不正リスクや事業リスクとして社会への周知に繋がりやすい個人情報漏えいリスクの方を重く見ており、営業秘密漏えいリスクの重大さをまだ十分に認識できていない企業が多いことを示唆しているものと考えられる。従って、営業秘密保護の重要性をさらに企業に強く周知していくことや、法務・知財部門と内部不正防止の担当部門の連携強化（社外の法律相談サービス[3]の積極活用を含む）の必要性を啓発することが求められている。

[3] 弁護士による法律相談、顧問弁護士への相談等

図表 69 内部不正事件等の経験の違いによる
内部不正リスクを重要な経営課題と捉えているかの現状の違い

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。



【検証したい仮説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

仮説⑤－３に関する単純集計結果からは、個人情報以外の重要情報を特定する仕組みを持つ企業は必ずしも多くなく、個人情報以外の重要情報の漏えいに関する内部不正対策の実施についても全般に底上げが必要な状況であることが分かっている。そこで、まず重要情報を特定する枠組みの浸透と業種がどのように関係しているかを分析してみた。このため、「業種による重要情報を特定する仕組みの充実度の違い」についてクロス集計を行った。クロス集計結果は図表70に示した。この結果を見ると、個人情報以外の重要情報を特定する仕組みを持っている業種は概ね製造業、通信業、卸売業・小売業、金融業・保険業等であることが分かった。

図表 70 業種による重要情報を特定する仕組みの充実度の違い

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。

		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
Q3 企業・組織の業種	1. 農業、林業、漁業	13	46.2	53.8	30.8	23.1	23.1	0.0	7.7	23.1	0.0	0.0	0.0
	2. 鉱業、採石業、砂利採取業	7	14.3	14.3	28.6	28.6	0.0	14.3	14.3	14.3	14.3	0.0	0.0
	3. 建設業	78	57.7	44.9	56.4	32.1	30.8	10.3	11.5	11.5	26.9	5.1	5.1
	4. 食料品製造業	40	65.0	52.5	57.5	42.5	25.0	10.0	17.5	12.5	25.0	0.0	5.0
	5. 飲料・たばこ・飼料製造業	3	66.7	66.7	33.3	0.0	33.3	33.3	0.0	0.0	0.0	0.0	0.0
	6. 繊維工業	11	45.5	63.6	27.3	36.4	18.2	27.3	27.3	27.3	9.1	0.0	0.0
	7. 化学工業	23	69.6	65.2	39.1	39.1	26.1	13.0	30.4	8.7	21.7	0.0	4.3
	8. プラスチック製品製造業	7	57.1	71.4	42.9	57.1	57.1	28.6	28.6	14.3	42.9	14.3	0.0
	9. ゴム製品製造業	3	33.3	33.3	33.3	33.3	0.0	0.0	0.0	0.0	33.3	0.0	33.3
	10. 鉄鋼業	12	66.7	50.0	50.0	33.3	33.3	0.0	25.0	8.3	25.0	0.0	0.0
	11. はん用機械器具製造業	3	100.0	100.0	33.3	100.0	0.0	0.0	0.0	0.0	33.3	0.0	0.0
	12. 生産用機械器具製造業	24	66.7	50.0	50.0	45.8	41.7	25.0	29.2	37.5	37.5	4.2	0.0
	13. 業務用機械器具製造業	11	81.8	72.7	54.5	63.6	27.3	45.5	36.4	36.4	36.4	0.0	0.0
	14. 電子部品・デバイス・電子回路製造業	38	97.4	68.4	50.0	52.6	42.1	26.3	39.5	44.7	39.5	0.0	0.0
	15. 電子応用装置・電気計測器製造業	13	61.5	69.2	53.8	53.8	46.2	23.1	30.8	30.8	30.8	0.0	7.7
	16. 15以外の電気機械器具製造業	25	68.0	72.0	60.0	56.0	44.0	28.0	32.0	44.0	48.0	0.0	4.0
	17. 情報通信機械器具製造業	17	70.6	64.7	58.8	58.8	35.3	35.3	29.4	29.4	41.2	0.0	0.0
	18. 自動車・同附属部品製造業	23	43.5	56.5	43.5	30.4	26.1	17.4	21.7	39.1	43.5	13.0	4.3
	19. 18以外の輸送用機械器具製造業	3	66.7	33.3	66.7	100.0	0.0	0.0	0.0	66.7	0.0	0.0	0.0
	20. 4～19以外の製造業	59	74.6	62.7	52.5	45.8	33.9	23.7	27.1	28.8	44.1	0.0	5.1
	21. 電気・ガス・熱供給・水道業	23	65.2	47.8	47.8	34.8	34.8	21.7	26.1	4.3	26.1	4.3	4.3
	22. 通信業	34	76.5	64.7	55.9	58.8	38.2	17.6	44.1	44.1	41.2	0.0	11.8
	23. 放送業	2	50.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	50.0
	24. 情報サービス業	143	67.1	52.4	44.8	46.9	29.4	16.1	20.3	21.0	34.3	4.2	14.0
	25. インターネット附随サービス業	26	61.5	50.0	53.8	38.5	23.1	19.2	19.2	34.6	26.9	0.0	15.4
	26. 映像・音声・文字情報制作業	6	83.3	33.3	66.7	50.0	33.3	16.7	33.3	0.0	16.7	0.0	16.7
	27. 運輸業、郵便業	60	80.0	41.7	53.3	50.0	28.3	18.3	31.7	21.7	33.3	3.3	5.0
	28. 卸売業、小売業	95	73.7	32.6	56.8	55.8	29.5	5.3	20.0	8.4	33.7	5.3	4.2
	29. 金融業、保険業	87	92.0	50.6	64.4	57.5	40.2	16.1	23.0	12.6	32.2	0.0	3.4
	30. 不動産業、物品賃貸業	31	80.6	35.5	54.8	41.9	19.4	6.5	12.9	16.1	22.6	6.5	3.2
	31. 学術研究、専門・技術サービス業	31	87.1	41.9	41.9	41.9	41.9	12.9	19.4	9.7	29.0	0.0	0.0
	32. 宿泊業、飲食サービス業	27	66.7	29.6	51.9	48.1	33.3	11.1	11.1	14.8	33.3	7.4	11.1
	33. 31、32以外のサービス業	137	73.7	33.6	40.9	33.6	25.5	13.1	18.2	13.1	22.6	5.8	6.6
	34. 公務（他に分類されるものを除く）	20	60.0	45.0	20.0	30.0	20.0	15.0	15.0	5.0	10.0	15.0	0.0
	35. 分類不能の産業	44	45.5	25.0	22.7	25.0	22.7	25.0	15.9	18.2	11.4	6.8	15.9

次に、個人情報以外の重要情報の漏えいに関する内部不正対策の実施について、経営層はどのように捉えているかを分析してみた。このため、「担当業務の違いによる個人情報以外の重

要情報にも対応できているかの現状についての感じ方の違い」についてクロス集計を行った。クロス集計結果は図表 71 に示した。この結果を見ると、経営層と従業員の間で大きな違いは見られなかった。

図表 71 担当業務の違いによる
個人情報以外の重要情報にも対応できているかの現状についての感じ方の違い

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
SQ1H 担当業務	情報システム関連部門の担当者または責任者	384	27.9	29.9	22.4	13.3	10.9	6.8	16.1
	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	31.9	35.7	32.9	16.7	10.5	2.9	4.8
	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	160	18.8	42.5	27.5	23.1	13.1	3.8	7.5
	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	28.3	26.0	17.4	15.1	9.3	8.5	13.6
	経営層	167	24.6	27.5	17.4	15.0	13.8	8.4	13.8

さらに、個人情報以外の重要情報の漏えいに関する内部不正対策の実施状況が、企業規模によってどのように変わるかを分析してみた。このため、「常用雇用者数の違いによる個人情報以外の重要情報にも対応できているかの現状の違い」についてクロス集計を行った。クロス集計結果は図表 72 に示した。この結果によると、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ことが分かる。しかし、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%にも満たず、底上げが強く求められる状況である。なお、個人情報以外の重要情報にうまく対応できていない理由については、2 ～ 5 番目の選択肢の全てで平均を上回っており、理由は多岐に亘っていることがうかがえる結果となっている。

図表 72 常用雇用者数の違いによる
個人情報以外の重要情報にも対応できているかの現状の違い

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

【検証したい仮説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

仮説⑤－５に関する単純集計結果からは、中途退職者に課す秘密保持義務の実効性を高める対策、中途採用時／中途退職時の内部不正防止に関する規則の策定ともに、十分な水準に達していないことが分かっている。ここでは、業種や企業規模によってこれらの対策実施や規則策定の状況がどのように違っているかについて分析してみた。

まず、業種や企業規模によっ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の実施状況がどのように違っているかを分析した結果について述べる。このため、「業種による中途退職者対策の現状の違い」と「常用雇用者数による中途退職者対策の現状の違い」についてクロス集計を行った。クロス集計結果は図表 73 と図表 74 に示した。この結果によると、中途退職者対策に積極的に取り組んでいる業種は製造業全般（11.～20.等）、金融業・保険業（29.）、通信業（22.）等であることが分かる。また、常用雇用者数が 1,000 人を超える企

業の対策実施が進んでおり、秘密保持義務契約の締結に関する対策が 50%を超えている。他方で、ここでも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な状況であると考えられる。

図表 73 業種による中途退職者対策の現状の違い

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
Q3 企業・組織の業種	1．農業、林業、漁業	13	15.4	46.2	30.8	15.4	15.4	0.0	0.0	7.7
	2．鉱業、採石業、砂利採取業	7	42.9	42.9	0.0	28.6	0.0	0.0	0.0	0.0
	3．建設業	78	34.6	50.0	29.5	17.9	16.7	0.0	16.7	9.0
	4．食料品製造業	40	22.5	50.0	40.0	15.0	15.0	0.0	10.0	12.5
	5．飲料・たばこ・飼料製造業	3	33.3	33.3	0.0	33.3	0.0	0.0	33.3	0.0
	6．繊維工業	11	45.5	18.2	45.5	27.3	18.2	0.0	0.0	0.0
	7．化学工業	23	34.8	56.5	47.8	34.8	30.4	0.0	0.0	8.7
	8．プラスチック製品製造業	7	14.3	14.3	14.3	28.6	0.0	0.0	28.6	14.3
	9．ゴム製品製造業	3	33.3	33.3	66.7	33.3	66.7	0.0	0.0	0.0
	10．鉄鋼業	12	41.7	75.0	41.7	25.0	8.3	8.3	0.0	0.0
	11．はん用機械器具製造業	3	0.0	66.7	33.3	33.3	33.3	0.0	33.3	0.0
	12．生産用機械器具製造業	24	45.8	50.0	33.3	20.8	41.7	0.0	8.3	0.0
	13．業務用機械器具製造業	11	45.5	90.9	54.5	36.4	36.4	9.1	0.0	0.0
	14．電子部品・デバイス・電子回路製造業	38	57.9	50.0	52.6	31.6	31.6	7.9	7.9	5.3
	15．電子応用装置・電気計測器製造業	13	53.8	53.8	15.4	30.8	15.4	0.0	0.0	7.7
	16．15以外の電気機械器具製造業	25	48.0	52.0	52.0	48.0	52.0	4.0	8.0	4.0
	17．情報通信機械器具製造業	17	58.8	58.8	64.7	47.1	41.2	0.0	0.0	5.9
	18．自動車・同附属部品製造業	23	60.9	47.8	34.8	17.4	8.7	0.0	17.4	8.7
	19．18以外の輸送用機械器具製造業	3	33.3	66.7	0.0	0.0	0.0	0.0	0.0	33.3
	20．4～19以外の製造業	59	35.6	55.9	42.4	27.1	22.0	3.4	3.4	10.2
	21．電気・ガス・熱供給・水道業	23	26.1	65.2	26.1	30.4	21.7	0.0	0.0	4.3
	22．通信業	34	41.2	47.1	55.9	47.1	41.2	2.9	2.9	11.8
	23．放送業	2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0
	24．情報サービス業	143	39.9	48.3	38.5	24.5	22.4	2.1	3.5	21.7
	25．インターネット附随サービス業	26	38.5	34.6	38.5	38.5	19.2	0.0	3.8	23.1
	26．映像・音声・文字情報制作業	6	33.3	16.7	0.0	0.0	16.7	0.0	33.3	16.7
	27．運輸業、郵便業	60	46.7	48.3	38.3	28.3	33.3	3.3	10.0	10.0
	28．卸売業、小売業	95	35.8	44.2	42.1	21.1	10.5	2.1	7.4	12.6
	29．金融業、保険業	87	50.6	63.2	48.3	33.3	31.0	1.1	4.6	6.9
	30．不動産業、物品賃貸業	31	35.5	41.9	45.2	12.9	22.6	3.2	6.5	3.2
	31．学術研究、専門・技術サービス業	31	32.3	64.5	45.2	12.9	35.5	3.2	3.2	0.0
	32．宿泊業、飲食サービス業	27	51.9	44.4	48.1	22.2	22.2	3.7	0.0	14.8
	33．31、32以外のサービス業	137	35.0	46.0	39.4	25.5	25.5	2.2	9.5	11.7
	34．公務（他に分類されるものを除く）	20	35.0	40.0	35.0	30.0	10.0	0.0	5.0	5.0
	35．分類不能の産業	44	38.6	43.2	34.1	18.2	22.7	6.8	11.4	11.4

図表 74 常用雇用者数による中途退職者対策の現状の違い

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

次に、企業規模によって中途採用時／中途退職時の内部不正防止に関する規則の策定状況がどのように違っているかを分析してみた。このため、「常用雇用者数による中途退職者／中途採用者の不正防止ルール策定の現状の違い」についてクロス集計を行った。クロス集計結果を図表 75 に示す。

この結果によると、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、常用雇用者数が 1,000 人を超える企業で対応が進んでおり、企業規模が大きくなるほど対応が進んでいる傾向が見て取れる。但し、常用雇用者数が多い企業であっても、周知・教育を通じて中途採用者に注意喚起することをルール化することについてはそれほど積極的ではないことが分かった。一方、中途退職時については、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%を超えていることは注目に値する。

他方で、ここでも中小企業によるルール策定への取り組みは遅れており、さらなる啓発が必要な状況であると考えられる。

図表 75 常用雇用者数による中途退職者／中途採用者の不正防止ルール策定の現状の違い

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

(2) アンケート調査結果とインタビュー調査結果のクロス分析

ここでは、企業アンケート調査結果（単純集計、クロス集計）とインタビュー調査結果（企業、有識者）を、共通の調査軸の同じ仮説ごとに比較分析した結果について取りまとめた。

【検証したい仮説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

近年、重要情報の漏えいとこれに関わる内部不正に影響を及ぼす環境変化や法改正などが急速に進んでおり、これに伴って社内規程の改訂も急務となっている。この現状を踏まえると、社内規程の内容を組織全体に周知・教育することへの注力に留まらず、社内規程を適時に改訂して最新化し、改訂箇所についても周知・教育を強化することが求められている。

【検証したい仮説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

法制度については、内部不正対策を所管する部署に蓄積されている知識について実態を調査したが、有識者からは一般の従業員が持つべき基礎知識と担当部署が蓄積すべき知識を別々に考えるべきであるとのご指摘をいただいた。具体的には一般の従業員は、「してはいけないこと」と「してしまったらどうなるか」を、事例を交えて学ぶことが望ましく、担当部署は法制度の知識を高いレベルで蓄積することが求められる。但し、担当部署だけで対応することが難しい場合は、法務部や外部専門家との連携を図れば良いとのことであった。

【検証したい仮説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

企業インタビューからは、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が効果的であるという示唆が得られている。

一方、企業アンケートのクロス集計からは、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という結果が出ている。

以上を考慮すると、経営層が他社の事例から率先して学び、重要情報漏えい等の背景・理由を理解することで、内部不正リスクを重要な経営課題として捉えることができるようになるため、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進展することが期待される。

【検証したい仮説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

企業インタビューからは、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であれば、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という示唆が得られている。

一方、企業アンケートの単純集計では、経営層は内部不正防止の取組み方針を日常的又は必要に応じて情報発信しているという結果が出ている。

他方で、企業アンケートのクロス集計からは、内部不正防止の取組み方針等についての情報発信を日常的に行っていると考えている経営層がまだ少ないという結果が得られている。また、内部不正リスクを重要な経営課題として捉えている場合は、経営層が日常的に全従業員に対して周知・指示することが増えているという結果もある。

まず注目されるのは、従業員と経営層の間で情報発信について認識の違いが見られることである。従業員が経営層の情報発信についてより積極的な回答をしている理由は明確ではないが、パネルからの募集に応えたアンケート回答者は情報漏えいや内部不正に関心がある方が多いと考えられることに加えて、所属部署や業務内容で回答者を絞り込んだこともあり、内部不正防止に対する経験・知見が豊富な回答者の割合が高くなっている可能性がある。

また、企業インタビュー結果と企業アンケートのクロス集計を比較すると、経営層が情報漏えいや内部不正の事業リスクを重要な経営課題として捉え、コンプライアンスを重視することが、経営層の方針の日常的な情報発信を促進するものと期待される。

【検証したい仮説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

企業アンケートの単純集計では、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、企業インタビュー調査では、さらに細かい責任・権限体制の実態を把握することができた。

（確認できた事例）

- 責任は「リスク管理／コンプライアンス部門」が持つ
- 責任は「情報システム／セキュリティ部門」が持つ
- 「リスク管理／コンプライアンス部門」と「情報システム／セキュリティ部門」が責任を分担
- 「リスク管理／コンプライアンス部門」の下位に「情報システム／セキュリティ部門」を配置して責任を分担
- 全社委員会を設置して責任を分担
- 責任は「知的資産保護部門」が持つ　等

このように、責任が「情報システム／セキュリティ部門」と「リスク管理／コンプライアンス部門」に分かれているとはいっても、実際には様々なバリエーションがあり、単純で画一的な責任体制のあり方を導出することは難しかった。一方で、企業アンケートの単純集計の取りまとめが示唆しているように、組織全体の中に「内部不正対策を具体的に計画、実施する責任・権限」と「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」という２つの責任・権限を配置することは不可欠であり、各企業の実態に則した様々な組織構造の中でその配置を明確に定義し、組織全体に示すことが求められている。

なお有識者からは、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との指摘があった。

【検証したい仮説③－３】
社内ポリシー／規定の整備が不十分な企業が多い

企業アンケートでは、内部不正に関する社内ポリシー／規定の整備がまだ不十分な企業が多いが、内部不正リスクを重要な経営課題として捉えることで、その整備状況を底上げできるという結果が出ている。

他方で企業インタビューでは、既存の社内委員会をうまく活用して内部不正防止に関する規則を整備することの有効性を示している。

以上を考慮すると、経営層が主催する既存の社内委員会をうまく活用して、経営層のリスク認識を高めることと内部不正防止に関する規則を検討することを同時に進める手法を検討することが考えられる。

【検証したい仮説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

企業アンケートや企業インタビューでは、全般に経営層の内部不正までは考慮していなかった。しかし有識者から、経営層が内部不正を行った場合、組織の内部レビューや内部監査が機能せず、内部不正が組織内で蔓延してしまうリスクがあることを指摘された。対策の適用においてもマネジメントレビューにおいても経営層を例外とせず、従業員と同等に取り扱うことが求められる。また今後の調査では、経営層の内部不正もスコープに入れることが望ましい。

【検証したい仮説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

企業アンケートの単純集計結果からは、内部不正対策に関する組織全体でのリテラシー教育

は、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等の一部の例外を除けば、組織全体で不足していることが分かっている。企業インタビュー調査結果もこの結果と概ね矛盾していないが、企業インタビュー調査では、営業秘密保護についてのリテラシー教育は必ずしも少なくないとしていて、若干の食い違いがある。一方、企業アンケートのクロス集計結果では、内部不正リスクを重要な経営課題として捉えている企業であっても営業秘密保護に関する知識をリテラシー教育している割合は 54%に留まっていて一層の底上げが求められている。営業秘密保護のリテラシー教育の調査結果にこの食い違いが生じた理由としては、営業秘密保護に対する意識が高い企業を中心にインタビューした可能性がある。

企業アンケートの単純集計結果において、大企業の方が営業秘密等の漏えい事件の組織全体への周知に消極的なのではないかという懸念が示されているが、図表 64 のクロス集計結果で「組織内外で内部不正事件が起こった場合、事故について組織内部で共有する」という対策の実施状況を見ると大企業の実施割合が高くなっており、この懸念は実態に合っていないことが分かる。また図表 64 から、大企業の方が営業秘密／限定提供データの漏えい防止が成熟していることも分かる。

一方、企業及び有識者のインタビュー調査結果から、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示唆されているが、企業アンケートのクロス集計を確認すると、企業規模が大きくなるほど内部不正事件／疑われる事態を経験した割合が高くなっており、営業秘密漏えいに焦点を絞れば製造業全般が内部不正事件／疑われる事態を経験した割合が高く、教育の素材となる事例を多く蓄積しているものと推察される。なお有識者からは、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べきとの指摘があった。

【検証したい仮説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

企業アンケートの単純集計によると、非正規雇用者の内部不正対策を除き、重要情報漏えい防止に関してニューノーマル等の環境変化への対応は遅れているという結果が出ている。他方で、企業インタビュー調査結果では、インタビュー先の大企業においてニューノーマルへの対応が遅れているとは必ずしも言い切れないと結論付けている。この結果は一見矛盾しているように見えるが、実際には図表 64 に見られるように大企業と中小企業の間で対応状況にかなり差が出ており、恐らく取り組みが進んでいる企業と進んでいない企業の間でも大きな差があることが見込まれるため、たまたま取り組みが進んでいる企業に多くインタビューを実施したことが理由であると推察される。

今回の調査を通じて、基本知識、リテラシー教育、対策の実施等の全般に亘り、中小企業の取り組みが遅れていることが明確になったため、今後中小企業に対する啓発にどのように取り組む

かが重要な課題であると思料される。

一方、近年の大きな環境変化の１つであるサプライチェーン保護の必要性の高まりについては、有識者からは、内部不正の「内部」には従業員だけでなく、経営層（主に役員）、取引先、サプライチェーンも含めて考えるべきであり、サプライチェーンも含めて一つの組織であるという考え方を浸透させた上で、リスク管理のための対策を進めるべきであるとの指摘をいただいた。

【検証したい仮説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

仮説⑤－４と同等の状況が見られるものの、その理由も⑤－４と同様であると考えられる。

ここでも有識者から、経営層の内部不正に対する対策も考慮すべきとの指摘をいただいた。経営層が退職する際に重要情報を持ち出した場合、これを咎められにくい実態があるため、従業員に対する対策が経営層にもそのまま適用され、例外は認められないというメッセージを発出することが重要である。

【検証したい仮説⑤－６】
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が十分ではない

仮説⑤－４と同等の状況が見られるものの、その理由も⑤－４と同様であると考えられる。

(3) 仮説の検証結果

本調査で設定した仮説を、企業アンケート、インタビュー（企業、有識者）、企業アンケートのクロス集計、企業アンケート結果とインタビュー結果の比較分析によって検証した結果について、図表 76 に取りまとめた。仮説の検証結果は、検証できたもの（〇）、否定されたもの（×）、どちらともいえないもの又は部分的に否定されたもの（△）に分かれた。

図表 76 設定した仮説の検証結果（全体）

調査軸	#	検証を試みる仮説	検証結果	根拠、分析
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	〇	■ 60～70%以上の企業が組織全体で認知していると回答している規程は就業規則しかなく、全体に亘って底上げが必要。 ■ 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。
	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	〇	■ 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い。 ■ 個人情報保護法に関する知識でさえ、担当部署に蓄積されていると答えなかった回答者が 40%を超えている。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。 ■ 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察される。 ■ 一般の従業員が持つべき基礎知識と担当部署が蓄積すべき知識は、別々に考えるべき。具体的には一般の従業員は、「してはいけないこと」と「してしまったらどうなるか」を、事例を交えて学ぶことが望ましく、担当部署は法制度の知識を高いレベルで蓄積することが求められる。
	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	〇	■ 関連するガイドライン全般に亘り、内部不正対策の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、改善の余地が多い。 ■ それでも、想定したよりは多く必要知識が蓄積されていた。 ■ 内部不正防止に対する経験・知見が豊富な回答者の割合が高くなっている可能性があり、これが回答割合を押し上げたものと推察される。

調査軸	#	検証を試みる仮説	検証結果	根拠、分析
	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	○	■ 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%前後に留まっている。 ■ 経営層は組織が情報漏えい／セキュリティリスクに関する知識を持っていることに懐疑的な傾向を持っており、課題を感じている。 ■ 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。
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	×	■ 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%に達している。 ■ 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単純集計結果よりも大きくなっている。 ■ 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、単純集計結果と比べて明らかに増えている。
	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	△	■ 重要情報漏えいへの対応を全社的な組織体制で掌握できている企業の割合は半数に過ぎず、現場組織の個別対応がかなり残っている。 ■ 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」に二分されていて、明確である。 ■ 主管部門（責任部門）と関連部門との連携については全般に底上げが必要。重要情報を実際に取扱うことが多い事業部門／営業部門との連携は必ずしも進んでいない。

調査軸	#	検証を試みる仮説	検証結果	根拠、分析
	③－3	社内ポリシー／規定の整備が不十分な企業が多い	○	■ 60%以上の企業・組織が基本方針、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の主要な規則を定めている状態が当面の到達目標と想定できるが、どの方針・規則もその水準に到達していない。 ■ 「重要情報の取り扱いに関する規則類」を定めていると答えた回答者の割合は 30%にも達しておらず、かなり低い。 ■ 個人情報管理と営業秘密管理に関する規則の策定状況を比較してみるとそれぞれの割合が 37%と24%であり、個人情報管理の方が規則の策定率が高くなっている。営業秘密管理の規則策定は個人情報管理よりも遅れている実態がある。 ■ 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。
	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	×	■ 「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%に達している。
	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が十分に機能していない企業がまだ多いが、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くなる。 ■ 実態として（内部不正を含む）重要情報漏えい対策のマネジメントシステムが機能している企業の割合は比較的高い水準に達している。「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」を選択した回答者は 50%を超えている。 ■ 他方で、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、まだ十分な水準に到達していない。
	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	×	■ 「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」を実施していると回答した割合はほぼ50%に達している。

調査軸	#	検証を試みる仮説	検証結果	根拠、分析
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	△	■ 重要情報の管理ルールの周知・徹底については、雇用開始時の教育、年次等の定期的な教育の実施割合が 50%を超えている。 ■ 雇用終了時の重要情報等の返却・削除ルールの周知、重要プロジェクト開始／終了時の重要情報管理ルールの教育等は不足している。 ■ 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・教育は不足している。 ■ 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、または必要に応じて実施していると回答した割合が 70%程度。 ■ リテラシー教育が最も充実しているのは個人情報保護。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のリテラシー教育は少なくはない。しかし、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、経験も必要であることから、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。 ■ 責任部門が情報システム／セキュリティ管理部門である場合、重要情報の分類と表示に関する規則の教育に力を入れている傾向が見られた。他方で、責任部門がリスク管理／コンプライアンス部門である場合は、単純集計結果との差異はなかった。 ■ 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。 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。
	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	×	■ 内部不正防止についてのリテラシー教育が組織全体での実践に寄与していると答えた回答者の割合は 70%に迫っており、十分に高い水準である。

調査軸	#	検証を試みる仮説	検証結果	根拠、分析
内部不正防止の課題と対策の実態	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	△	■ 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%に留まっている。 ■ 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、一般にこの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同様である。 ■ 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、それ以外の企業と比べると、内部不正防止に関する取り組みや対策の実施状況が明らかに進展している。 ■ 個人情報の漏えい事件／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大きくなっている。 他方で、営業秘密の漏えい事件／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必ずしも大きくない。 この調査結果は、企業が依然として、内部不正リスクや事業リスクとして個人情報漏えいリスクの方を重く見ており、営業秘密漏えいリスクの重大さをまだ十分に認識できていない企業が多いことを示唆している。
	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	×	■ 重要情報の管理ルールを詳しく定めて適用できていると答えた回答者の割合は 46%程度、詳しく定めるためにルールを改訂中と答えた回答者の割合は 24%程度となっており、両者を合算すると約 70%の企業・組織が重要情報の漏えいに関する内部不正に対して具体的な対策を選択できているものと推察される。

調査軸	#	検証を試みる仮説	検証結果	根拠、分析
	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	○	■ 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を特定する仕組みを持っていると答えた回答者の割合は45%前後である。利活用する価値が高い重要データや他社から「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については、重要情報と特定できる仕組みを作っていると答えた回答者の割合は約30%に過ぎない。 ■ 個人情報以外の重要情報を特定する仕組みを持っている業種は製造業、通信業、卸売業・小売業、金融業・保険業等である。 ■ 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くなっている。しかし、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%にも満たない。 ■ 個人情報以外の重要情報の漏えいに関する内部不正対策を実施できているかについては、重要技術情報・ノウハウや重要データにも対応できていると答えた回答者の割合は 30%に届いていない。
	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	○ 但し、非正規雇用者の内部不正対策のみ× 	■ 左記の仮説は実態と合っている（非正規雇用者の内部不正対策を除く）。 ■ 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、いずれの対策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い難い。 ■ 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%を超えている。 ■ テレワーク時の内部不正対策については、いずれの対策項目も実施している割合が 40%に満たない。 ■ エンドポイントの端末機能を制限する対策、クラウドサービスの利用制限等は幅広く実施されている。 ■ クラウドサービス利用時の内部不正対策については、いずれの対策項目も回答割合が 40%に満たない。

調査軸	#	検証を試みる仮説	検証結果	根拠、分析
	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	○	■ 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、就業規則に退職後の定めを規定すること等の回答割合は50%に達していない。 ■ 重要プロジェクト単位での秘密保持義務契約の締結／誓約書の提出はあまり行われていない。 ■ 中途退職者対策に積極的に取り組んでいる業種は製造業全般、金融業・保険業、通信業等である。 ■ 常用雇用者数が 1,000 人を超える企業の対策実施が進んでおり、秘密保持義務契約の締結に関する対策が50%を超えている。他方で、中小企業による対策への取り組みは遅れている。 ■ 中途採用時／中途退職時の内部不正防止に関する規則の策定については、いずれも回答割合が50%に達していない。 ■ 中途採用者に他社の重要情報を持ち込ませないための規則策定については、常用雇用者数が1,000 人を超える企業で対応が進んでおり、企業規模が大きくなるほど対応が進んでいる。 ■ 中途退職時については、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規則を定めている企業の割合は、常用雇用者数が 5,000 人を超えるあたりから増加しており、10,000 人を超える企業では 40%を超えている。
	⑤－6	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が十分ではない	○	■ いずれの対策項目も実施している割合が 50%に達しておらず、十分な水準とは言いがたい。 ■ 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。
	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	○	■ 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。

(4) 現状の課題と取り得る対策

企業アンケート、インタビュー（企業、有識者）、企業アンケートのクロス集計、企業アンケート結果とインタビュー結果の比較分析によって仮説を検証した際に、同時に抽出された課題と取りうる対策について、図表 77 に取りまとめた。ここで抽出された内容は、今後の内部不正防止ガイドライン改訂、啓発用の好事例紹介等の検討にあたり、参考とすることができる。

図表 77 仮説の検証から抽出された課題と取り得る対策（全体）

調査軸	#	検証を試みる仮説	検証結果	課題と取りうる対策
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	○	■ 社内規程の内容を組織全体に周知・教育することへの注力に留まらず、社内規程を適時に改訂して最新化し、改訂箇所についても周知・教育を強化することが必要。
	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	○	■ 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べき。 ■ 限定提供データの法知識の組織全体への周知を促進するためには、従業員に対して営業秘密の法知識と同時に周知することが望ましい。
	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	○	■ 仮説が示唆する必要知識の不足を克服するためには、ガイドラインに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適切に選択することが必要。 ■ 業界単位でのトップダウンの周知が有効。
	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	○	■ 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、知識不足の状態を改善できる。 ■ 経営層が他社の事例から率先して学び、重要情報漏えい等の背景・理由を理解することで、内部不正リスクを重要な経営課題として捉えられるようになる。これによって、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を促進できる。

調査軸	#	検証を試みる仮説	検証結果	課題と取りうる対策
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	×	■ 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。 ■ 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経営層の方針の日常的な情報発信を引き出すため、経営層に重要情報漏えいの事業リスクをしっかりと認識してもらい、コンプライアンスを重視していくことが望ましい。
	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	△	■ 最終的に次の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一番重要。 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 ガバナンス上は２つの部門が各々の責任・権限を分担する形が望ましいが、１つの部門が両方の責任・権限を実効的に担保する選択肢もありうる。 ■ 組織全体の中に「内部不正対策を具体的に計画、実施する責任・権限」と「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」という２つの責任・権限を配置することは不可欠であり、各企業の実態に則した様々な組織構造の中でその配置を明確に定義し、組織全体に示すことが必要。 ■ 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件発生時の法的対応を支援し、重要情報にアクセスできる 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言える。この形態は金融等の企業ガバナンスが厳格に求められる業種・業態で実践されている。 ■ 他方で、IT／セキュリティ部門が責任部門となっていることも多い。 法務・知財部門や事業部の統括組織等と連携することで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、CDO を任命等の工夫によって、重要情報の特定／分類についての指導力を強化し、組織全体の統制を適正に運用している事例も参考にできる。

調査軸	#	検証を試みる仮説	検証結果	課題と取りうる対策
	③－3	社内ポリシー／規定の整備が不十分な企業が多い	○	■ 経営層が主催する既存の社内委員会をうまく活用して、経営層のリスク認識を高めることと内部不正防止に関する規則を検討することを同時に進めるという方法があり、効率的かつ効果的である。
	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	△	■ 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れば、これ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可能。これに繋げるため、重要情報保護に対する意識を高め、その責任・組織体制の充実を図るべき。 ■ 役職の高い人物が内部不正を行った場合、マネジメントシステムの内部レビューや内部監査が機能しない懸念がある。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。
	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	×	－
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	△	■ 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く、内部不正対策に関する周知・教育の充実に貢献できる。 ■ 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る。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重要情報や内部不正についての必要な法知識を浸透させることが有効である。
	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	×	■ リテラシー教育を従業員の実践に繋げるためには、社内外の事件／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べき。 ■ 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）、定期的な規則遵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。 ■ 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。

調査軸	#	検証を試みる仮説	検証結果	課題と取りうる対策
内部不正防止の課題と対策の実態	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	△	■ 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ることが有効。 ■ 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、企業の内部不正防止対策やその他の取り組みの促進に大きな効果を期待できる。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必要。 ■ 経営層の内部不正に対する意識改革は、現場からのボトムアップでは難しく、国や業界団体からのトップダウンアプローチが有効。 ■ 営業秘密保護の重要性をさらに企業に強く周知することや、法務・知財部門と内部不正防止の担当部門の連携強化（社外の法律相談サービスの積極活用を含む）の重要性を啓発することが必要。 ■ 中小企業の経営層に対する内部不正リスクの周知啓発が重要。
	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	×	■ 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遵守などの人的・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べき。
	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	○	■ 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くべき。このためには、次のような対応が有効： ・ 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ができる人材の育成。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。

調査軸	#	検証を試みる仮説	検証結果	課題と取りうる対策
	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	○ 但し、非正規雇用者の内部不正対策のみ×	■ サプライチェーンへの対応の遅れは、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。 ■ 基本知識、リテラシー教育、対策の実施等の全般に亘り、中小企業の取り組みが遅れていることが明確になったため、今後中小企業に対する啓発にどのように取り組むかが重要な課題。 ■ ゼロトラスト、IRM、DLP 等の高度な概念やツールの検討・導入は、有効性が高い。 ■ サプライチェーンの内部不正対策では、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が有効。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好事例もあった。
	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	○	■ 仮説の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ることが有効： ・ 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に加えて、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。 ・ 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、必要な対策を実施。 ・ 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得。 ・ 重要性の高い秘密に触れている役職員については、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。
	⑤－６	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が十分ではない	○	■ 職場環境の整備は技術的対策の絞り込みと重点化に繋がり、対策コスト削減にも効果があることを周知して、取り組みを促すべき。
	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	○	■ 実際の対応はケースバイケースとなるため、仮処分命令・差止請求・損害賠償・刑事罰等についての法的理解を深め、予め方針を定めておくことで、対応力を高めることが可能。

5. まとめと今後の方向性

(1) 調査結果の総括と得られた示唆

①企業・組織全体として知っておくべき基礎知識

【調査結果の総括】

内部不正防止のリテラシー向上において必要性が高く、早期に企業・組織全体に根付かせるべき基礎知識として、本調査では社内規程、法制度、ガイドライン、情報漏えい／セキュリティリスクに関する知識に焦点を当て、国内企業における知識習得の実態を調査した。基本的には組織全体としての実態を調査したが、法制度／ガイドラインに限ってはその専門性を考慮し、担当部署を調査対象とした。

調査結果として、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。

【調査結果と得られた示唆】

社内規程は経営層や従業員が遵守すべき規則を定めたものであり、その内容は原則として全員が知っておくべき基礎知識である。しかし実際には、内部不正防止に関わる種々の規程において、関連規則が十分に認知されていない（または規則自体が定められていない）企業が多いという実態が浮き彫りになった。企業のサイバーセキュリティ、コンプライアンスに関するリテラシー教育において、重要情報の漏えい／内部不正の防止に焦点を当てる回数を増やす等により、内部不正防止に関する規程及びその規則に対する従業員の基礎知識と理解を深める取り組みが急務である。またインタビュー調査では、内部不正防止に影響を及ぼす近年の大きな環境変化を捉え、最新の基礎知識を取り急ぎ社内規程に反映して従業員に周知・教育することの必要性が指摘された。

法制度については、全般に関連する基礎知識が不足する中で、個人情報保護法だけが知識の蓄積が少し進んでおり、他の関連法との間に顕著な違いが見られた。特に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、担当部署に蓄積された営業秘密の法知識は明らかに不十分であった。限定提供データに関する法知識の蓄積はさらに遅れていた。不正競争防止法に関するこの問題点を改善するためには、営業秘密に関して「してはいけないこと」を警告として事例を交えて伝えることに加えて、これと同じ機会に限定提供データの法知識を併せて周知することが望ましい。

また法制度については、組織全体に周知すべきかそれとも担当部署が知っておけば良いのかという議論があったが、有識者からは、一般の従業員が持つべき基礎知識と担当部署が蓄積すべき知識を別々に考えるべきであるとのご指摘をいただいた。一般の従業員については、「してはいけないこと」と「してしまったらどうなるか」を、事例を交えて教えることで、内部不正防止の効果を高めることができる。他方で、担当部署は法制度の知識を高いレベルで蓄積することにより、組織全体として、法の趣旨に則った重要情報の保護と内部不正防止体制／対策を確立すべきである。

ガイドラインについても、担当部署に蓄積された知識は不十分だったが、当初想定したほど状況は悪くなかった。この状況を改善するためには、ガイドラインに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適切に選択することが必要となる。

情報漏えい／セキュリティリスクに関する基礎知識についても、組織全体に浸透している企業の割合は低かった。リスクを理解することは対策の必要性を感じ取る上で不可欠な前提となるため、この問題点の改善は優先度の高い喫緊の課題と言える。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、現状を改善することができる。

なお、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たことから、これらの基礎知識を組織全体で定着させるためには、内部不正リスクを経営層に経営課題として認識してもらうことが有効であることが示唆された。経営層においても、他社の事例から率先して学び、重要情報漏えい等の背景・理由を理解することで、内部不正リスクを重要な経営課題として捉えられるようになるものと期待される。

②内部不正防止に取り組む組織的体制

【調査結果の総括】

内部不正防止に取り組む組織的体制の整備・運用にあたり、特に重要と考えられる事項として、本調査では内部不正防止に係る経営層のリーダーシップ、組織全体としての責任・権限の明確化、社内ポリシー／規定の整備、経営リソースの配分、マネジメントシステムの実効性確保に焦点を当て、国内企業における実態を調査した。また、近年の働き方変革の進展を踏まえ、その代表格と言えるテレワークに注目し、国内企業がテレワーク環境の改善に組織全体で取り組んでいるかの実態についても併せて調査した。

調査結果として、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。また、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。

【調査結果と得られた示唆】

経営層の情報発信は、必ずしも不十分ではないという調査結果が得られた。また、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、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ことが分かった。従って、経営層に重要情報漏えいや内部不正の事業リスクをしっかりと認識してもらい、コンプライアンスを重視することが求められる。

組織全体としての責任・権限の明確化については、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であり、責任部門と重要情報を実際に取扱うことが多い現場の事業部門／営業部門との連携は必ずしも進んでいなかった。重要情報漏えいへの対応についても、現場任せが残っている企業が少なくなかった。このような現状を踏まえ、今後企業が目指すべき姿を想定すると、最終的には次の２つの責任・権限が実効的に確立され、全社で実際に行使できる組織体制とすることが最も重要であると考えらえる。ガバナンス上は２つの部門が各々の責任・権限を分担する形が望ましいが、１つの部門が両方の責任・権限を実効的に担保する選択肢もありうる。

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

社内ポリシー／規定の整備については、まだ不十分な企業が多かった。個人情報管理と営業秘密管理に関する規則の策定状況を比較してみると、個人情報管理の取り組みの方が進んでおり、営業秘密管理の規則策定の現状は、大企業も含めてまだ不十分である実態が浮き彫りとなった。このような状況の中で、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他の群の数値より 10%以上底上げされていることが分かった。今後の望ましい対応としては、経営層が主催する既存の社内委員会をうまく活用し、経営層のリスク認識を高めることと内部不正防止に関する規則を検討することを同時に進める方法がある。

組織全体として内部不正防止のための体制を整備し、必要な対策を実施し、これを継続的に改善できるマネジメントシステムを構築するためのリソースを経営層が適切に配分できていない企業は、実態として必ずしも多くはなかった。

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。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企業の割合は半数にも達しておらず、まだ十分な水準まで到達していなかった。ところで有識者から、役職の高い者が内部不正を行うと、マネジメントシステムの内部レビューや内部監査が機能しなくなる懸念があるという指摘があった。役職の高い者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であると言える。この問題についてはさらなる検討が必要と考えられるため、今後は経営層の内部不正について掘り下げることが望まれる。

テレワークを行う従業員を支援する体制については、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等が進んでいる企業が多かった。

③組織全体への周知・教育

【調査結果の総括】

内部不正防止について組織全体に周知・教育を行う上で、周知・教育の内容を充実させて受講機会を増やすことと、従業員が内容を理解して実践に繋げることが重要であることから、本調査ではそれぞれに焦点を当て、国内企業における実態を調査した。

調査結果として、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。他方で、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。

【調査結果と得られた示唆】

一般の職員に対して、内部不正対策に関するリテラシー教育を組織全体で定期的、または必要に応じて実施している企業の割合は高く、70%弱に達していた。そこで、どのような内容について周知・教育しているのかを調査したところ、一般の従業員に対する、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しており、55%を超える企業が実施していた。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。

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、着目した項目に対して網羅的にリテラシー教育を提供している割合が高くなっており、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の教育が進展していた。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決して高くなく、一層の底上げが期待される。

内部不正防止に関する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取り組みについては、インタビュー調査で実態の深掘りを実施した。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く、内部不正対策に関する周知・教育の充実に貢献できる。社内外の事件／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ことが望ましい。さらには、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も必要となる。

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ることが求められる。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重要情報や内部不正についての必要な法知識を浸透させることも有効である。

この他、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）、定期的な規則遵守のセルフチェックなど、e-Learning に留まらない教育の実践が有効である。

④内部不正防止の課題と対策

【調査結果の総括】

内部不正対策の充実に向けて具備すべき重要な要件のうち、本調査では特に「内部不正を経営課題として優先しているか」、「内部不正対策の選定に苦心していないか」、「個人情報以外の重要情報にも対応できているか」、「対策がニューノーマルの急な環境変化*に追いついているか」、「中途退職者／中途採用者の急増に対応できているか」、「内部不正を誘発しない職場環境づくりができているか」、「重要情報の侵害先に毅然として対応できるか」に焦点を当て、国内企業における実態を調査した。

*ここでは、サプライチェーン対策、非正規雇用者の増加、テレワークとクラウド利用の拡大を取り上げた。

調査結果として、次の実態が明らかになった：

- 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、必ずしも苦心してはいなかった。
- 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、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。

【調査結果と得られた示唆】

「内部不正を経営課題として優先しているか」について：

当初想定していた「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」という懸念については、総じて実態を示しているものの、「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」という調査結果が得られたため、一部実態とは合っていないことが分かった。また、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は、それ以外の企業と比べると、内部不正防止に関する取り組みや対策の実施状況が明らかに進展していた。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。例えば、国や業界団体からトップダウンで働きかける手法がこの一例である。

個人情報の漏えい事件／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大きくなっている。他方で、営業秘密の漏えい事件／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個人情報漏えいの場合と比較して相対的に低い。この調査結果は、企業が依然として、内部不正リスクや事業リスクとして個人情報漏えいリスクの方を重く見ており、営業秘密漏えいリスクの重大さをまだ十分に認識できていない企業が多いことを示唆している。この状況を改善するためには、法務・知財部門（社外の法律相談サービスを含む）を内部不正防止の担当部門と強く連携させ、この連携を通じて担当部門に営業秘密保護の重要性を徹底させる手法が有効であると考えられる。

この他、中小企業の経営層は、内部不正リスクを重要な経営課題として捉えていない傾向が強いため、これを改善する周知啓発を行うことが望ましい。

「内部不正対策の選定に苦心していないか」について：

約 70%の企業が重要情報の漏えいに対する具体的な対策を選択できていると見込まれる等、企業は必ずしも内部不正対策の選択に苦心していない実態が分かった。他方で、内部不正対策では職場環境の整備や秘密保持義務の遵守などの人的・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ことが望ましいという指摘もあった。

「個人情報以外の重要情報にも対応できているか」について：

総じて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という状況が確認されたと言える。しかし、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以外の重要情報に対応できている企業が他の群よりも顕著に増加していた。

まずは、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くべきであると考えられる。このためには、経営層のリーダーシップの下で、営業秘密に対して求められる対応を個人情報の場合と同じように具体的に提示し、これを実践できる人材を育成し、他社から受領した営業秘密にも十分に気を配ることが求められる。

「対策がニューノーマルの急な環境変化に追いついているか」について：

ニューノーマル等の環境変化に対する内部不正対策の対応については、非正規雇用者の内部不正対策を除いて概ね不十分な水準に留まっていた。

サプライチェーンへの対応の遅れは、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。

テレワークとクラウド利用の拡大については、エンドポイントの端末機能を制限する対策、クラウドサービスの利用制限等が幅広く実施されていた。

「中途退職者／中途採用者の急増に対応できているか」について：

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については、まだ対策が十分に進んでいない実状であると分かった。常用雇用者数が 1,000 人を超える企業の対策実施が進んでいる一方で、中小企業による対策への取り組みは遅れていた。中途退職時については、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 人を超えるあたりから増加していた。

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、経営層にも従業員と同じ規則を適用して透明性を高めること、退職者の情報システムへのアクセスログの確認範囲を広げること、他社の重要情報を勝手に社内に持ち込ませない対策を講じること、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すること、重要性の高い秘密に触れている役職員については誓約書を詳細化すること等を検討することが望ましい。

「内部不正を誘発しない職場環境づくりができているか」について：

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はまだ改善の余地が大きい状況であった。職場環境の整備は技術的対策の絞り込みと重点化に繋がり、対策コスト削減にも効果があることを周知し、取り組みを促すことが望ましい。

「重要情報の侵害先に毅然として対応できるか」について：

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かった。実際の対応はケースバイケースとなるため、仮処分命令・差止請求・損害賠償・刑事罰等についての法的理解を深め、予め方針を定めておくことで、対応力を高めることが可能となる。

(2) 課題に対する今後の方向性

前節の取りまとめに基づき、課題に対する今後の方向性を抽出・整理した。その結果を図表 78 に示した。

図表 78 課題に対する今後の方向性（総括）

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） ■ 個人情報に留まらない重要情報の漏えい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のための要件検討
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

このうち特に重要なのは、「共通事項」として述べた「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。本調査の結果から、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という示唆を得ることができた。そこから、内部不正リスクを課題として十分に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有効であり、求められていると言える。

さて、この意識変革を促すための方法としては、何が有効なのであろうか。ここで鍵となるのが「事例から学ぶ」ということである。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大きくなっているため、この経験を前向きに活用することが重要であると考えられる。

一方で、営業秘密等の個人情報以外の重要情報の漏えい事案／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個人情報の場合と比較してそれほど高くはない。この実態は、経営層や内部不正防止の全社責任者の営業秘密等に対する経験値や理解レベルが十分ではない企業が多いことに起因している可能性がある。従って、営業秘密保護に関し、経営層・全社責任者・責任部門等を対象として、意識変革に繋がる啓発を引き続き実施してこうした傾向を改善していくことで、営業秘密の漏えい事案／インシデントを経験した企業においてはもちろん、いまだそうした経験のない企業においても、事例からの学びにより改善され、内部不正リスクを重要な経営課題として捉えることができるようになるものと期待する。このような意識変革に繋がる啓発手段の例としては、次のようなものが有効であると考えられる。

（例）

- 経営層に対してサイバーセキュリティ／重要情報漏えい／内部不正防止の講義を行う機会が多い有識者、コンサルタント、弁護士、社内担当者等が活用しやすい事例集／プラクティス集を作成・公開
- 事例を分かりやすく解説するのに大いに役立つ動画、イラスト等のコンテンツを作成・公開
- 上述したコンテンツを活用できる人材を育成するためのワークショップ、セミナー、講習会等を実施
- 法務・知財部門（社外の法律相談サービスを含む）を内部不正防止の責任部門と強く連携させ、この連携を通じて責任部門に営業秘密保護の重要性を徹底させる　等

(3) ガイドラインとその普及啓発に関する今後の方向性

①内部不正防止ガイドラインの認知度の向上に向けて

今回の調査を通じて、内部不正防止ガイドラインは元々想定していたよりは認知されていることが分かってきた。特に、日頃から産業スパイ等の脅威に晒されているハイテク製造業等においては、内部不正に限定した用途で良く認知されている可能性がある。一方で、次のような指摘をいただいた。

- IPA から公開されたガイドラインであるため、（IPA との接点が希薄な傾向にある）企業の法務・知財部門では良く認知されていない恐れがある。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良く認知してもらい、もともと IPA との接点が多い傾向がある、ガイドラインを既に知っている 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認知、活用が期待できる可能性がある。
- 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その必要性が認知されにくいことが懸念される。

内部不正防止ガイドラインの認知度を高めるために今後取り組むべき施策としては、認知度・活用度合の高い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を検討すべきである。例えば、次のような文書と相互参照するのが良いとの指摘があった。

- 経済産業省 「サイバーセキュリティ経営ガイドライン」
- 経済産業省 「営業秘密管理指針」、「限定提供データに関する指針」
- 公安調査庁の経済安全保障啓発パンフレット 「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～」 等

②内部不正防止ガイドラインの活用促進に向けて

企業アンケート調査では、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という調査結果が得られた。この実態を変えていく必要がある。このための施策としては、想定する読者を意識した情報量の調整、表現の工夫と周知啓発活動を強化していくことの２つの側面が考えられる。

【利用しやすくするための改善施策】

企業インタビュー／有識者インタビューの調査結果を踏まえると、内部不正防止ガイドラインを利用しやすくするための改善施策は次の４つに集約される。

i. 概要版の作成
ii. 活用しやすい情報量の調整、表現の工夫
iii. 社内規程整備のために活用しやすい内容の増補

iv. 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

概要版については、担当部署や一般の従業員にとって読みやすくするという側面ももちろんあるが、より重視すべきなのは、内部不正対策を経営層に説明する際に活用しやすくすることである。

活用しやすい内容の充実に関しては、例えば中途退職者／入社者の内部不正対策の強化などの企業ニーズが高い主題に焦点を絞って記載を充実させることが望ましい。但し、記載の充実といっても単に内容を丁寧に説明すれば良いということではなく、例えば内部不正事例について解説する等、経営層への説明に役立てるという視点での活用しやすさに重点を置く必要がある。

社内規程整備のために活用しやすい内容の増補については、既存の社内規程が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を参考に書かれていることを前提として、これらのガイドラインと内部不正防止ガイドラインとの関係を明確に示すことが考えられる。こうすることで、サイバーセキュリティのガイドラインを参考に既に記載されている内部規程の条文を、内部不正防止ガイドラインを参考にして内部不正防止の観点でも充実させることが可能になる。

最後に、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については、例えば次のような施策を検討することが望ましい。

- e-Learning 用の設問、解説等の公開
- 内部不正対策の要点をまとめた動画コンテンツの公開
- その他、従業員教育にそのまま活用できる素材の充実

【ガイドラインの周知啓発活動の強化】

内部不正防止ガイドラインの周知啓発については、まず周知啓発に活用できるツールや好事例を整備することが挙げられる。ここでツールとは、例えば経済産業省「サイバーセキュリティ経営ガイドライン」の支援ツール（プラクティス集、可視化ツール、手引き等）のようなものを想起できる。

また有識者から、内部不正防止ガイドラインは、自主的に内部不正対策に取り組むには少し内容が難しいという指摘を受けた。一方で、一度企業が取り組みを始めてしまえば、その後は内部不正防止ガイドラインを継続的に活用してもらえるものと期待できる。そこで、一度取り組みを始めるまでのサポートを実施するために、外部の専門家を派遣してオンサイトで指導する際に、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構築する等の施策を検討することが望ましい。

この他、企業インタビューでは、内部不正防止ガイドラインの継続的なオンライン講演等を望む声もあった。こうした周知啓発の取り組みも今後検討していくことが望ましい。

③内部不正防止ガイドラインに対するその他の指摘

複数の有識者から、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べきであるとのご意見をいただいた。これについ

ては今後検討することが望ましい。

　また、企業インタビューからは、紙で保管する重要情報の内部不正対策を統合すること、グローバル視点でのリスク／対策の記載を充実させること等の要望があった。これらについては、今後どのように取り組むべきかの検討を始めるところから着手することが考えられる。

(This page is intentionally left blank.)

別紙

1．企業アンケート調査票（骨子）

本アンケートは、**（独）情報処理推進機構（IPA）セキュリティセンターセキュリティ対策推進部セキュリティ分析グループより委託を受けて、「令和 4 年度企業における内部不正防止体制に関する実態調査」の一環として、当該事業を受託した株式会社 NTT データ経営研究所が実施する**ものです。お手数をお掛け致しますが、何卒宜しくご協力のほどお願い申し上げます。

なお、アンケート調査のご回答につきましては、集計処理を実施し、個別企業が特定されない形にした上で、当該事業の報告書等において公開する予定です。

【ご回答にあたって】

- **所要時間：** 30 分程度
- **ご回答方法：** Web 回答システムを用いてご回答ください。

（注：重要）
本アンケートでは、電子化された重要情報の漏えい等に関する内部不正を対象としています。ここで重要情報としては、個人情報に加え、不正競争防止法における営業秘密（製法・ノウハウ等の技術情報、顧客情報・接客マニュアル等の営業情報）、限定提供データ（提供／利用先を限定している重要なビッグデータや AI 学習用データセット等）、外為法における機微技術情報、法令の保護対象ではないものの機密性が高い秘密情報等も対象となります。

Ⅰ．はじめに

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。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）

1．　情報システム関連部門の担当者または責任者
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
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責任者
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
5．　経営層
6．　どれにもあてはまらない

Q1．あなたは（独）情報処理推進機構（以降、「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」をご存じでしたか。あてはまるものを１つお選びください。（単一選択）

1．　知っていた	2．　知らなかった　⇒**Q3 へ**

Q1 の選択肢で１．を選択した方にお伺いします。

Q2．あなたは IPA「組織における内部不正防止ガイドライン」が、電子化された重要情報を漏えいさせる等の内部不正に焦点を当てて書かれていることをご存じでしたか。あてはまるものを１つお選びください。（単一選択）

1．　知っていた	2．　知らなかった

Ⅱ．あなたが勤務している企業・組織（以降、「貴社」）の概要について伺います

Q3．貴社の企業・組織の業種（注１）についてあてはまるもの（注２）を１つお選びください。（単一選択）

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

（注１）総務省「日本標準産業分類」に基づく

（注２）取り扱う製品、部素材、サービス等が複数ある場合は、直近の決算で最も売上高の多いものなど、主たる事業

に関する業種を選んでください。

Q4. 貴社の常用雇用者数（注３）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)

1. 5 人以下	2. 6～20 人	3. 21～50 人
4. 51～100 人	5. 101～300 人	6. 301 人～1,000 人
7. 1,001 人～5,000 人	8. 5,001～10,000 人	9. 10,001 人以上

（注３）常用雇用者数とは、正社員、パート、アルバイトなどの名称にかかわらず、以下(1)～(3)のことを指します。

(1) 期間の定めなく雇用されている者

(2) 過去 1 年以上の期間について引き続き雇用されている者

(3) 雇い入れ時から 1 年以上引き続き雇用されると見込まれる者のことを指します。

Q5. 貴社の設立年についてあてはまるものを１つお選びください。(単一選択)

1. 2020 年以降	2. 2010 年～2019 年	3. 2000 年～2009 年
4. 1980 年～1999 年	5. 1960 年～1979 年	6. 1930 年～1959 年
7. 1900 年～1929 年	8. それ以前	

Q6. 貴社の本社所在地についてお答えください。 （1.もしくは 3.は必ず記入ください）

1. 都道府県（ ）
2. 区・市・郡・町・村（ ）※番地までは不要
3. 本社が日本国外の場合 国・地域名（ ）

Ⅲ. 貴社の重要情報（個人情報、営業秘密、重要データ等）管理の概要について伺います

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。あてはまるものをすべてお選びください。（複数選択）

1. 個人情報	2. 重要な技術情報・ノウハウ
3. 重要な営業情報	4. 営業秘密として管理している情報
5. 利活用する価値が高い重要データ	6. AI 学習用のデータセット
7. 限定提供データとして管理しているデータ	
8. 安全保障貿易管理（輸出管理）に係る機微技術情報	
9. 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	
10. どれもあてはまらない	11. わからない

Q8. 貴社では重要情報の管理ルールを厳格に適用していますか。あてはまるものを１つお選びください。（単一選択）

1. 管理ルールを詳しく定め、細部までこれを忠実に適用し、運用している
2. 管理ルールをより詳しく定めるため、ルールを改訂中、または改訂する計画がある
3. 管理ルールの運用を改善中、または改善する計画がある
4. 管理ルールの適用と運用はあまり徹底していない
5. わからない

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。あてはまるものをすべてお選びください。（複数選択）

1. 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
2. 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
3. 異動時・昇進時等にルールを教育し直している
4. 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
5. 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
6. 教育による周知は実施していない
7. わからない

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。あてはまるものを１つお選びください。（単一選択）

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

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。あてはまるものを１つお選びください。（単一選択）

1. 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
2. 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
3. 組織的な見直しは行われていない
4. わからない

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。あてはまるものをすべてお選びください。（複数選択）

（経営層のコミットメントについて）
1. 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。
2. 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
3. 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
4. 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
（内部不正防止の組織体制について）
5. 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
6. 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
（組織全体での教育について）
7. 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
8. 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
（中途退職者等に関する対策について）
9. 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
10. 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
11. 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
（内部不正のモチベーションを生まない職場環境について）
12. 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
（資産管理、ID 管理について）
13. ID 管理と本人確認（認証）を強化している
14. 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
15. 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
16. 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
（物理的管理について）
17. 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
18. BYOD（個人デバイスの業務利用）は許可していない
（技術・運用対策について）
19. 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

20. 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
21. 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
22. 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
23. 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
24. 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
（内部不正の事後対応について）
25. 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
26. 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
（その他）
27. どれもあてはまらない

Ⅳ. 貴社における、内部不正対策の基礎知識の普及状況について伺います

※以下では内部不正とは、重要情報の漏えいに関する内部不正のことを指しています。

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。あてはまるものをすべてお選びください。(複数選択)

1. 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）
2. 内部統制の基本方針（内部不正防止の基本方針を含む）
3. セキュリティポリシー（内部不正防止の基本方針を含む）
4. 就業規則に書かれた内部不正防止に関するルール
5. 組織全体に適用される重要情報の分類規則
6. 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
7. 組織全体に適用される重要情報の分離保管規則
8. 個人情報管理のための規則
9. 営業秘密管理のための規則
10. 限定提供データの管理のための規則
11. 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）
12. 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）
13. 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
14. 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
15. どれもあてはまらない
16. わからない

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。あてはまるものをすべてお選びください。(複数選択)

1. 基本方針	2. 就業規則	3. 秘密保持／情報管理規則
4. セキュリティ管理規程	5. 個人情報管理の規則	6. 営業秘密管理の規則
7. 限定提供データ管理の規則	8. 採用時の誓約書提出（秘密保持義務等）	
9. 退職時の誓約書提出（秘密保持義務、競業避止等）		
10.テレワーク業務規程（業務手順、機器・ツールの利用法、セキュリティ規則の順守等）		
11.コンプライアンス規程（企業倫理、行動規範、違法行為禁止、情報の取り扱い、報告等）		
12.労務管理規程（中途採用／退職、出張、出向／転籍、転勤／海外赴任、人事評価等）		
13.従業員監視の運用規程	14.どれもあてはまらない	15.わからない

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。各項目につき、あてはまるものを１つお選びください。(単一選択)

機器・システムの脆弱性		1. 組織全体で知られている	2. 対策の担当者が知っている	3. 知られていない	4. わからない
サイバー攻撃、だましの手口		1. 組織全体で知られている	2. 対策の担当者が知っている	3. 知られていない	4. わからない
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		1. 組織全体で知られている	2. 対策の担当者が知っている	3. 知られていない	4. わからない
サプライチェーンにおける不必要な重要情報の授受		1. 組織全体で知られている	2. 対策の担当者が知っている	3. 知られていない	4. わからない
クラウドセキュリティのあいまいな責任分担		1. 組織全体で知られている	2. 対策の担当者が知っている	3. 知られていない	4. わからない
テレワークの不十分なセキュリティガバナンス		1. 組織全体で知られている	2. 対策の担当者が知っている	3. 知られていない	4. わからない
プライバシーを侵害する従業員監視		1. 組織全体で知られている	2. 対策の担当者が知っている	3. 知られていない	4. わからない
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		1. 組織全体で知られている	2. 対策の担当者が知っている	3. 知られていない	4. わからない
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		1. 組織全体で知られている	2. 対策の担当者が知っている	3. 知られていない	4. わからない

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。あてはまるものをすべてお選びください。(複数選択)

1. 個人情報保護法（利用目的の順守）	2. 個人情報保護法（第三者提供の要件）
3. 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）	

4. 不正競争防止法（営業秘密の要件）	
5. 不正競争防止法（限定提供データの要件）	
6. 外国為替及び外国貿易法（外為法）	7. 経済安全保障推進法
8. 不正アクセス禁止法	
9. どれもあてはまらない	10.わからない

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。あてはまるものをすべてお選びください。(複数選択)

1. IPA 組織における内部不正防止ガイドライン
2. 経済産業省 秘密情報の保護ハンドブック
3. 経済産業省 営業秘密管理指針
4. 経済産業省 限定提供データに関する指針
5. 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
6. 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
7. 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
8. 総務省 テレワークセキュリティガイドライン
9. 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）
10.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
11.どれもあてはまらない
12.わからない

Ⅴ．貴社における内部不正対策の組織体制について伺います

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。あてはまるものを１つお選びください。(単一選択)

1. 日常的に行っている ⇒**Q20 へ**	2. 必要に応じて行っている ⇒**Q20 へ**
3. ほとんど行っていない	4. 全く行っていない
5. わからない	

Q18 の選択肢 3．～5．の中でいずれかを選択した方にお伺いします。

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。(複数選択)

1. 経営層（全社責任者を含む）が必要性を感じていないから
2. 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

3. 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
4. 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
5. その他の理由： 具体的に（ ）
6. わからない

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。あてはまるものを１つお選びください。(単一選択)

1. 情報システム／セキュリティ管理部門	2. リスク管理／コンプライアンス部門
3. その他	4. わからない ⇒**Q22 へ**

Q20 の選択肢 1.～3. の中でいずれかを選択した方にお伺いします。

Q21. 貴社の内部不正防止体制において、Q20 の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。あてはまるものをすべてお選びください。(複数選択)

1. 人事・教育部門	2. 法務・知財部門
3. 情報システム／セキュリティ管理部門	4. リスク管理／コンプライアンス部門
5. 経理・財務部門	6. 事業部門、営業部門
7. その他の部門	8. 特にない
9. 分からない	

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。あてはまるものを１つお選びください。(単一選択)

1. 適切に配分している	2. 適切に配分できていない	3. わからない

Q23. 貴社では内部防止不正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。あてはまるものをすべてお選びください。(複数選択)

1. 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
2. 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
3. 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
4. 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
5. 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
6. 特にない
7. わからない

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。あてはまるものをすべてお選びください。(複数選択)

1. 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
2. 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
3. 定期的に出勤日を設けている
4. その他
5. わからない

Ⅵ. 貴社における、内部不正防止に関する組織全体への周知・教育について伺います

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。あてはまるものをすべてお選びください。(複数選択)

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

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。あてはまるものを１つお選びください。(単一選択)

1. 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
2. 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
3. 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
4. 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 **⇒Q30へ**
5. どれもあてはまらない **⇒Q30へ**
6. わからない **⇒Q30へ**

Q26 の選択肢 1．～3．の中でいずれかを選択した方にお伺いします。

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。あてはまるものをすべてお選びください。(複数選択)

1. 重要情報の分類と表示に関する規則
2. 個人情報保護の法制度に関する知識
3. 営業秘密保護の法制度に関する知識
4. 限定提供データ保護の法制度に関する知識
5. 機微技術情報の管理に関する外為法についての知識
6. クラウド利用許可に関する規則
7. BYOD（個人所有 PC／デバイスの業務利用）の使用規則
8. テレワークに関する内部規則や関連法令
9. 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
10. 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
11. 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
12. 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
13. 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）
14. どれもあてはまらない
15. わからない

Q28. あなたは、内部不正防止のために周知・教育した内容が、組織全体での実践に寄与していると感じていますか。あてはまるものを 1 つお選びください。(単一選択)

1. はい ⇒**Q30 へ**	2. いいえ	3. わからない ⇒**Q30 へ**

Q28 の選択肢 2. を選択した方にお伺いします。

Q29. 周知・教育が組織全体の実践に寄与できていない理由は何だと考えていますか。あてはまるものをすべてお選びください。(複数選択)

1. 経営者のリーダーシップや従業員を守る姿勢が不足しているため
2. 内部不正防止に関する組織的対策が徹底していないため
3. 内部不正防止に関する組織マネジメントが徹底していないため
4. 従業員の重要情報に対する認識が低く、情報漏えい対策の必要性を感じていないため
5. 従業員の不満が蓄積しやすい職場環境であるため
6. 従業員の、内部不正防止への対応スキルが十分ではないため
7. どれもあてはまらない
8. わからない

Ⅶ. 貴社における、内部不正防止対策に関する課題と対策の現状について伺います

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。あてはまるものを 1 つお

選びください。(単一選択)

1. 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
2. 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
3. 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
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
5. どれもあてはまらない
6. わからない

Q31. 貴社では、内部不正防止対策を具体的に選択する上での課題は何ですか。あてはまるものをすべてお選びください。(複数選択)

1. 内部不正対策を対象としたベンダーソリューションが少なく、うまく選択できていない
2. 組織内で関連知識や経験値が不足しており、対策を具体的に選定できていない
3. 内部不正対策に対するマネジメントシステムがなく、課題の改善策をうまく選定できていない
4. 事後対応や事業継続についての計画やマニュアルがなく、適切な対応策や法的措置を選択できない
5. どれもあてはまらない
6. わからない

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。あてはまるものをすべてお選びください。(複数選択)

1. 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
2. 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
3. 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
4. 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
5. 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
6. どれもあてはまらない
7. わからない

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。あてはまるものをすべてお選びください。(複数選択)

1. 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
2. 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
3. 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

4. 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
5. 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
6. 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
7. その他
8. 合意していない
9. わからない

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。あてはまるものを１つお選びください。(単一選択)

1. 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
2. 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
3. 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
4. わからない

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。あてはまるものをすべてお選びください。(複数選択)

1. 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
2. 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
3. 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
4. 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
5. テレワーク勤務と社内勤務を公平に処遇している
6. 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
7. その他　具体的に：（　　）
8. 実施していない
9. わからない

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。あてはまるものをすべてお選びください。(複数選択)

1. 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

2. 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
3. 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
4. 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
5. 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
6. その他　具体的に：（　　）
7. 実施していない
8. わからない

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。あてはまるものをすべてお選びください。(複数選択)

1. 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
2. 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
3. 就業規則に退職後の定めを規定している
4. 秘密保持義務の有効期間を十分長く設定している
5. 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
6. その他
7. 実施していない
8. わからない

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。あてはまるものをすべてお選びください。(複数選択)

1. 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
2. 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
3. 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
4. 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
5. 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
6. その他
7. 規定していない

8. わからない

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。あてはまるものをすべてお選びください。(複数選択)

1. 人事・業績評価の公平性を高めている
2. 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
3. テレワーク従事者と社内勤務者を公平に処遇している
4. 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
5. どれもあてはまらない
6. わからない

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。あてはまるものをすべてお選びください。(複数選択)

1. 内部不正が疑われる退職者本人への警告
2. 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）
3. 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）
4. 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
5. その他
6. 準備していない
7. わからない

Ⅷ. IPA「組織における内部不正防止ガイドライン」について伺います

Q41. 貴社では、内部不正防止対策を検討するにあたり、どのようなガイドラインを参考にしていますか。あてはまるものをすべてお選びください。(複数選択)

1. 情報セキュリティ関係のガイドラインの内部不正と関わりが深い箇所を参考にしている
2. 内部統制関係のガイドラインの内部不正に関わる箇所を参考にしている
3. IPA「組織における内部不正防止ガイドライン」を参考にしている　**⇒Q42 へ**
4. それ以外
5. わからない

Q41 の選択肢 3. を選択した方にお伺いします。3. を選択しなかった方は、設問はこれで終わりです。

Q42. 貴社では、「組織における内部不正防止ガイドライン」のどの項目を参考にしていますか。あてはま

るものをすべてお選びください。(複数選択)

1. 内部不正防止に関する基本方針
2. 秘密指定とアクセス権指定
3. 物理的管理
4. 技術・運用管理
5. 原因究明と証拠確保
6. 人的管理
7. コンプライアンスの確保
8. 職場環境の改善
9. 事後対策
10. 組織マネジメント（通報制度、対策のレビュー／監査等）
11. わからない

調査は以上で終了です。本アンケート調査にご協力いただき、心より感謝申し上げます。

2. 企業インタビュー調査票（骨子）

【インタビュー調査項目について】

本インタビュー調査では、次の主題についてお伺いしたく存じます。何卒宜しくご協力のほどお願い申し上げます。

（１）	内部不正に関わりがある情報セキュリティ／内部統制関係のガイドライン等の活用状況
（２）	内部不正防止に関し、組織全体が知っておくべき基礎的な知識についてのお考え
（３）	内部不正対策を実施するための組織体制と、経営層によるリーダーシップの現状
（４）	内部不正防止について組織全体で実施している周知・教育の現状
（５）	組織として現在重視している内部不正防止対策、及び重視している理由
（６）	その他（IPA の政策へのご要望等）

【注記】

1. **本調査では、電子化された重要情報を漏えいさせる／破壊する等の内部不正を対象としています。対象とする内部不正の範囲が限定されていますので、ご注意ください。**
2. **重要情報とは、個人情報に加え、不正競争防止法における営業秘密（重要技術情報を含む）、限定提供データ（ビッグデータや AI 学習用データセット等）等も対象となります。**
3. **本日のインタビューでは、上記（・）（・）（・）についてお伺いしたく存じます。その他の項目については、ご回答が可能なものだけをご選択ください。**

（注）上記の（・）の部分は、インタビュー対象者ごとに書き分けを行った。

【内部不正に関わりがある情報セキュリティ／内部統制関係のガイドライン等の活用状況】

内部不正防止対策を選択するにあたり、内部不正との関わりが深い情報セキュリティ／内部統制関係のガイドライン等を活用することが考えられます。こうしたガイドライン等*は活用していますか。

また、情報セキュリティ関係のガイドラインと内部統制関係のガイドラインでは、どちらをよく参考にしますか。

*ご参考：IPA では「組織における内部不正防止ガイドライン」を公開しています。

【内部不正防止に関し、組織全体が知っておくべき基礎的な知識についてのお考え】

重要情報の漏えいに関する内部不正防止を効果的に実現するために、従業員はどのような基礎知識を共有している必要があると考えていますか。従業員全体で知っておくべきことと、対策を担当する部門の要員が知っておくべきことに分けて整理することが有用とお考えでしたら、そのあたりもご教示ください。

また、その理由についてもさしつかえない範囲でご教示ください。

（ご参考：基礎知識の例）

<u>従業員全体：</u>

関係する社内規則、情報漏えいリスク／セキュリティリスクに関する知識、社会で注目された事件の情報など

<u>対策を担当する部門の要員：</u>

上記（従業員全体）に加えて、関係する法制度・ガイドライン、情報漏えい対策技術とその運用、サプライヤーや委託先との契約における注意点等

また、従業員全体が知っておくべき基礎知識を共有することができるように、今後リテラシー教育を拡大するなどの検討を行う必要があると考えていますか。その理由や背景についてもさしつかえない範囲でご教示ください。

【内部不正対策を実施するための組織体制と、経営層によるリーダーシップの現状】

貴社では、セキュリティ対策／内部統制等の一環として、内部不正防止についても経営層がリーダーシップを発揮しておられますか。また、どのようなリーダーシップを発揮しておられるかについてご教示ください。

（ご参考：経営層のリーダーシップの例）

基本方針の策定と周知徹底、マネジメントシステムの構築と全社での継続的改善、必要なリソースの配分、社外に向けて積極的に情報発信、社内に向けて主体的に周知／指示等

内部不正対策を整備し、実践する責任は、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のどちらが担っていますか。その理由や利点についてもお考えをご教示ください。

また、重要情報漏えいに関する貴社全体の内部不正対策の責任者は、サイバーセキュリティ対策の責任者と同じでしょうか、それとも内部統制の責任者と同じでしょうか。あるいは、これらの責任者はいずれ

も同じでしょうか。

【内部不正防止について組織全体で実施している周知・教育の現状】

貴社では、重要情報の漏えいに関する内部不正防止について、現在組織全体でどのようなリテラシー教育を実施していますか。また、実施している理由についてご教示ください。

（ご参考：従業員全体に行うべきリテラシー教育の主題例）

16. 重要情報の分類と表示に関する規則
17. 営業秘密の保護制度に関する知識
18. 限定提供データの保護制度に関する知識
19. クラウド利用許可に関する規則
20. BYOD（個人所有 PC／デバイスの業務利用）の使用規則
21. テレワークに関する内部規則や関連法令
22. 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の明確化
23. 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
24. 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
25. 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

また、今後は何についてのリテラシー教育を強化する必要があると考えていますか。上記の主題例以外にも重点を置くべき観点はありますか。

内部不正防止のために周知・教育した内容の実効性をどのようにモニタリングしていますか。また、その理由や効果についてもさしつかえない範囲でご教示ください。

【組織として現在重視している内部不正防止対策、及び重視している理由】

組織として、現在どのような内部不正防止対策を重視していますか。また、今後重視したいと考えている内部不正対策についてもご教示ください。また、これらを重視している理由についてご教示ください。

テレワーク中やクラウドサービス利用中の内部不正対策については、どのように取り組んでおられますか。

（内部不正防止対策の例）

（資産管理、ID 管理）
28. テレワークが増えてから、ID 管理と本人確認（認証）を強化している
29. 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ある
30. 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、厳しく管理されている
31. 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

（物理的管理）
32. 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
33. BYOD（個人デバイスの業務利用）は許可していない
（技術・運用対策）
34. 重要情報に対するアクセス監視、ログ記録及び定期的なログ分析が実施され、それが組織全体に周知されている
35. 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
36. 業務で使用できるクラウドや、クラウド上で扱うことができる重要情報の範囲をルール化している
37. 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
38. サプライヤーや委託先等の重要情報漏えい対策を、契約前及び契約中に確認している
（中途退職者に関する対策）
39. 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などに秘密保持義務契約を結んでいる
40. 退職後には速やかに利用者 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
（内部不正のモチベーションを生まない職場環境）
41. 従業員に不満が蓄積しないように、労務管理、人事管理、コミュニケーション管理で必要な対策を講じている
（内部不正の事後対応について）
42. 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
43. 内部不正の事例を組織内部に告知し、内部不正の心理的抑止に役立てている

【その他】

最後に、電子化された重要情報の漏えい等についての内部不正防止に係る IPA の政策にご要望等がございましたら、お聞かせください。

また、IPA「組織における内部不正防止ガイドライン」をもしお読みになっておられましたら、ご意見をお聞かせいただければ幸甚です。

インタビュー項目は以上です。調査にご協力いただき、どうもありがとうございました。

3. 有識者インタビュー調査票（骨子）

【インタビュー調査項目について】

本インタビュー調査では、次の主題のうち４～５項目についてお伺いしたく存じます。何卒宜しくご協力のほどお願い申し上げます。

（１）	企業・組織における重要情報の特定と分類の現状（アンケート／インタビュー調査経過）とあるべき姿の対比
（２）	企業・組織における内部不正防止体制の現状（アンケート／インタビュー調査経過）とあるべき姿との対比 ・経営層のリーダーシップ ・内部統制（リスク管理／コンプライアンス管理）あるいはサイバーセキュリティの体制との関係 ・内部不正に対する内部レビュー／内部監査を行う体制のあり方等
（３）	企業・組織全体のリテラシー教育で教えている内容の現状（アンケート／インタビュー調査経過）とあるべき姿との対比
（４）	企業・組織全体で実施するリテラシー教育で、法制度についてどこまで踏み込んで教育すべきか
（５）	限定して提供される価値の高いビッグデータを内部不正から保護するにあたり、法的観点も含めて課題として認識されていること、またこれらの課題を克服するための望ましいアプローチ
（６）	企業・組織における内部不正防止対策の実施状況（アンケート／インタビュー調査経過）とあるべき姿との対比
（７）	組織における内部不正防止ガイドラインの改善点、周知啓発のための望ましい施策

【注記】

4. 本調査では、電子化された重要情報を漏えいさせる／破壊する等の内部不正を対象としています。対象とする内部不正の範囲が限定されていますので、ご注意ください。

5. 重要情報とは、個人情報に加え、不正競争防止法における営業秘密（重要技術情報を含む）、限定提供データ（ビッグデータや AI 学習用データセット等）等も対象となります。

6. 本日のインタビューでは、上記（・）、（・）、（・）、（７）についてお伺いしたく存じます。

（注）上記の（・）の部分は、インタビュー対象者ごとに書き分けを行った。

【企業・組織における重要情報の特定と分類の現状（アンケート／インタビュー調査経過）とあるべき姿の対比】

企業アンケートでは例えば次のような設問により、各社の実態等を伺っています。また、企業インタビューで深掘りした関連情報もございます。

（関連するアンケート設問例）

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。

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。 **等**

これらの調査結果について可能な範囲で取りまとめた「途中経過」を提示させていただきますので、ご関心をお持ちになった点に焦点を当てて、企業のあるべき姿と現状のギャップについてご見解をご教示ください。さらに、このギャップを埋めるための官民の取組みの方向性について、もしご意見があればご教示ください。

【企業・組織における内部不正防止体制の現状（アンケート／インタビュー調査経過）とあるべき姿との対比】

企業アンケートでは例えば次のような設問により、各社の実態等を伺っています。また、企業インタビューで深掘りした関連情報もございます。

（関連するアンケート設問例）

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。

Q23．貴社では内部防止不正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。

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。 **等**

これらの調査結果について可能な範囲で取りまとめた「途中経過」を提示させていただきますので、ご関心をお持ちになった点に焦点を当てて、次の４つの観点等から、企業のあるべき姿と現状のギャップについてのご見解をご教示ください。さらに、このギャップを埋めるための官民の取組みの方向性について、もしご意見があればご教示ください。

- **経営層のリーダーシップ**
- **内部統制（リスク管理／コンプライアンス管理）あるいはサイバーセキュリティの体制との関係**
- **組織全体でのマネジメントシステム（PDCA）の運用**
- **内部不正に対する内部レビュー／内部監査を行う体制のあり方　等**

【企業・組織全体のリテラシー教育で教えている内容の現状（アンケート／インタビュー調査経過）とあるべき姿との対比】

企業アンケートでは例えば次のような設問により、各社の実態等を伺っています。また、企業インタビューで深掘りした関連情報もございます。

（関連するアンケート設問例）

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。
Q28．あなたは、内部不正防止のために周知・教育した内容が、組織全体での実践に寄与していると感じていますか。 **等**

これらの調査結果について可能な範囲で取りまとめた「途中経過」を提示させていただきますので、ご関心をお持ちになった点に焦点を当てて、企業のあるべき姿と現状のギャップについてご見解をご教示ください。さらに、このギャップを埋めるための官民の取組みの方向性について、もしご意見があればご教示ください。

【企業・組織全体で実施するリテラシー教育で、法制度についてどこまで踏み込んで教育すべきか】

企業アンケートでは例えば次のような設問により、各社の実態等を伺っています。また、企業インタビューで深掘りした関連情報もございます。

（関連するアンケート設問例）
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。
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。 **等**

これらの調査結果について可能な範囲で取りまとめた「途中経過」を提示させていただきますので、ご関心をお持ちになった点に焦点を当てて、企業のあるべき姿と現状のギャップについてご見解をご教示ください。さらに、このギャップを埋めるための官民の取組みの方向性について、もしご意見があればご教示ください。また、情報漏えいに関する内部不正防止に関わる法制度（例：個人情報保護法、不正競争防止法等）において、全従業員への周知・教育を強く推奨すべきとお考えになる基礎知識等がございましたら、ご教示ください。

【限定して提供される価値の高いビッグデータを内部不正から保護するにあたり、法的観点も含めて課題として認識されていること、またこれらの課題を克服するための望ましいアプローチ】

限定して提供される価値の高いビッグデータを内部不正から保護するにあたり、法的観点も含めて課題として認識されていること、またこれらの課題を克服するための望ましいアプローチについて、ご意見やお考えがあればご教示ください。

【企業・組織における内部不正防止対策の実施状況（アンケート／インタビュー調査経過）とあるべき姿との対比】

企業アンケートでは例えば次のような設問により、各社の実態等を伺っています。また、企業インタビューで深掘りした関連情報もございます。

（関連するアンケート設問例）
Q12．重要情報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。
Q31．貴社では、内部不正防止対策を具体的に選択する上での課題は何ですか。
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。 **等**

これらの調査結果について可能な範囲で取りまとめた「途中経過」を提示させていただきますので、ご関心をお持ちになった点に焦点を当てて、企業のあるべき姿と現状のギャップについてご見解をご教示ください。さらに、このギャップを埋めるための官民の取組みの方向性について、もしご意見があればご教示ください。

【組織における内部不正防止ガイドラインの改善点、周知啓発のための望ましい施策】

企業アンケートでは次のような設問により、各社の実態等を伺っています。また、企業インタビューで深掘りした関連情報もございます。

Q41．貴社では、内部不正防止対策を検討するにあたり、どのようなガイドラインを参考にしていますか。 Q42．貴社では、「組織における内部不正防止ガイドライン」のどの項目を参考にしていますか。

これらの調査結果について可能な範囲で取りまとめた「途中経過」を提示させていただきますので、その内容も踏まえ、IPA「組織における内部不正防止ガイドライン」の改善点や望ましい周知啓発方法について、忌憚ないご意見を賜りたく、宜しくお願いします。

インタビュー項目は以上です。調査にご協力いただき、どうもありがとうございました。