内部不正防止対策・体制整備等に関する
中小企業等の状況調査

調査報告書

令和６年３月

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

内部不正防止対策・体制整備等に関する 中小企業等の状況調査 1

調査報告書 1

1. 概要 4

(1) 背景 4

(2) 調査の目的 4

(3) 調査の全体構成 5

2. 動向調査の実施方法 7

(1) 調査のフレームワーク 7

(2) 改善策の整理 7

① 経営課題の改善（調査軸１） 8
② 重要な秘密の特定と取扱いの改善（調査軸２） 8
③ 組織体制・連携に関する課題の改善（調査軸３） 9
④ 社員教育とリテラシー構築に関する課題の改善（調査軸４） 9
⑤ 対策実施に関する課題の改善（調査軸５） 11
⑥ 中小企業の構造的課題の改善（調査軸６の１～５） 12
⑦ ガイドラインの利用と実践に関する課題の改善（調査軸７） 16
⑧ まとめ 17

(3) 事例調査の実施方法 19

(4) アンケートとインタビューを組み合わせた改善策と現状の比較分析・示唆抽出方法 21

(5) 企業アンケート調査の実施方法 22

① 調査対象者 22
② アンケート調査の実施プロセス 23
③ 回答の回収数に対する要件 23
④ 回答率の向上策 24

⑤　アンケート設問の設計 24

(6)　企業インタビューの実施方法 32

①　調査対象者 32
②　インタビューの実施方法 33
③　企業インタビューの調査項目設計 33

(7)　有識者インタビューの実施方法 41

①　調査対象者 41
②　インタビューの実施方法 41
③　有識者インタビューの調査項目設計 42

3.　調査結果 50

(1)　事例調査結果 50

(2)　企業アンケート調査の単純集計結果 51

①　回答者及び所属企業の属性 51
②　経営課題の改善（調査軸１） 54
③　重要な秘密の特定と取扱いの改善（調査軸２） 56
④　組織体制・連携に関する課題の改善（調査軸３） 58
⑤　社員教育とリテラシー構築に関する課題の改善（調査軸４） 60
⑥　対策実施に関する課題の改善（調査軸５） 64
⑦　中小企業の構造的課題の改善（調査軸６の１～５） 67
⑧　ガイドラインの利用と実践に関する課題の改善（調査軸７） 67

(3)　企業と有識者のインタビュー調査結果の整理・比較 69

①　全体的な課題の改善（調査軸１～５） 70
②　中小企業の構造的課題の改善（調査軸６の１～５） 75
③　ガイドラインの利用と実践に関する課題の改善（調査軸７） 84
④　有識者インタビューで得られたその他の有益な示唆 85

4.　調査結果の分析 89

(1)　事例調査結果の分析からの示唆 89

①　企業規模による事案発生傾向の違い 89
②　情報漏えいとサービス／システム停止の事案発生傾向の違い 90

③　個人情報漏えいと営業秘密漏えいの事案発生傾向の違い 90
④　内部不正とサイバー攻撃の事案発生傾向の違い..... 91
⑤　まとめ..... 92

(2)　クロス分析の実施方法..... 92

①　企業アンケート回答のクロス集計による分析..... 92
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 96

(3)　企業アンケート調査のクロス集計による分析..... 96

①　全体的な課題の改善（調査軸１～５） 96
②　中小企業の構造的課題の改善（調査軸６の１～５） 114
③　ガイドラインの利用と実践に関する課題の改善（調査軸７） 129

(4)　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..... 132

①　全体的な課題の改善（調査軸１～５） 132
②　中小企業の構造的課題の改善（調査軸６の１～５） 142
③　ガイドラインの利用と実践に関する課題の改善（調査軸７） 154

(5)　結論と今後の方向性 155

①　全体的な課題の改善（調査軸１～５） 156
②　中小企業の構造的課題の改善（調査軸６の１～５） 160
③　ガイドラインの利用と実践に関する課題の改善（調査軸７） 167

5.　まとめと今後の方向性..... 168

(1)　調査結果のまとめ 168

(2)　調査の課題と今後の方向性 171

謝辞..... 172

1. 概要

(1) 背景

企業が保有する秘密情報[1]の管理と保護は企業経営上の重要な課題であり、独立行政法人情報処理推進機構（以後、「IPA」という）では 2021 年度に「組織における内部不正防止ガイドライン」（以後、「内部不正防止ガイドライン」という）を第 5 版に改訂し、内部不正による情報漏えいの防止に資する情報提供を実施した。さらに、IPA では、2022 年度に「企業における内部不正防止体制に関する実態調査」（以下「2022 年度調査」という）を実施したが、その調査結果から以下の問題点が浮き彫りになった。

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

さらには、今後の課題として次の 3 点が導出された。

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

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

(2) 調査の目的

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

[1] 本調査にいう秘密情報は、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している。

ができた企業の経営について調査を実施する。本事業の調査結果は、今後のより実効性の高い施策への改善、対策実施の支援等に活用していく。なお、本調査では常用雇用者数 300 人以下を中小企業と定義する。

(3) 調査の全体構成

本調査では、内部不正防止対策・体制整備等に関する中小企業等の状況を調査するにあたり、2022 年度調査において着実な成果を挙げた調査フレームワークを引き続き適用する。具体的には次の 3 項目を実施する：

i. インタビュー調査及びアンケート調査の調査項目（調査票の質問項目）にしっかりとした一貫性を持たせるため、共通の調査軸を作業全体で適用
ii. 各調査軸に対し、インタビューとアンケートで共通して、改善策と現状の比較／好事例を抽出するための調査項目（設問）を設定
→昨年度は「現状・実態に対する仮説」であったところ、今年度は一歩進めて「企業の内部不正防止を改善する手段」の整理と実施状況を確認
iii. 各調査軸で、インタビュー調査項目とアンケート調査項目を対比しながら同時に設計することで、両者で一貫した改善策と現状の比較／好事例、改善策を補う示唆を導出

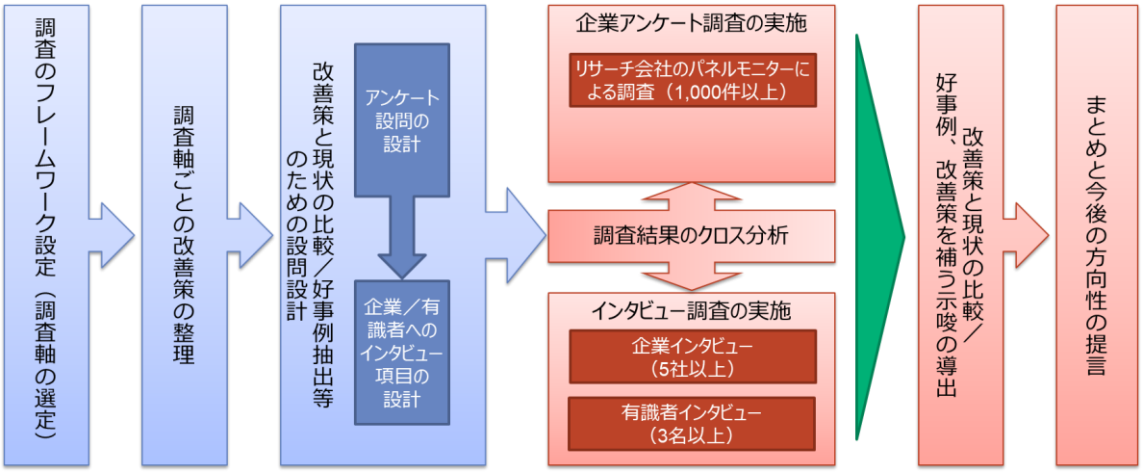
ここで、共通の調査軸としては以下の 7 項目を設定した。

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

そして、これらの調査軸の設定を踏まえ、上述の一貫した調査フレームワークを適用して、必要な取組進展のための改善策の整理、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、改善策と現状の比較／好事例、改善策を補う示唆の導出という一連の作業の全てを上記 7 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。

7 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



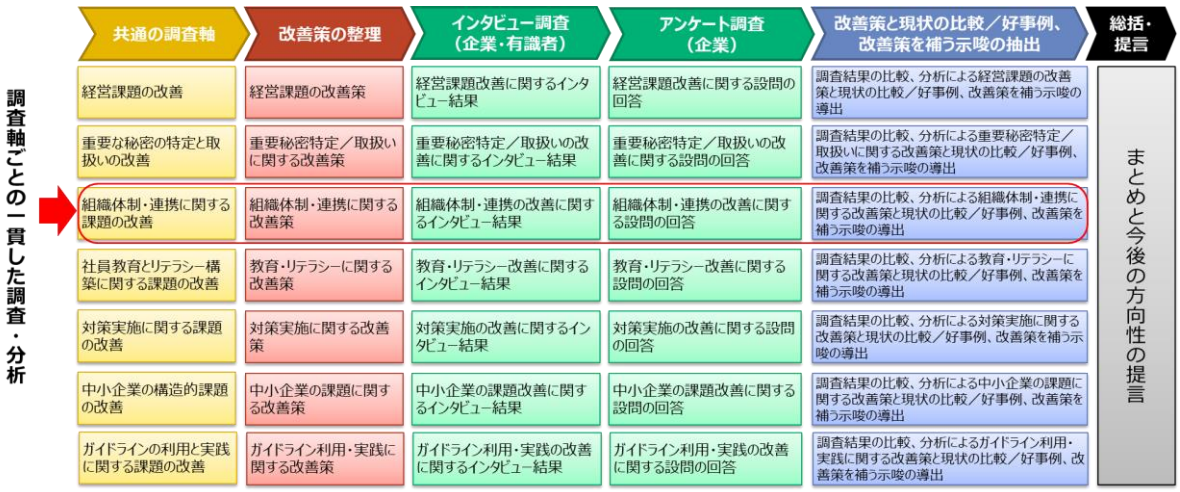
2. 動向調査の実施方法

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、必要な取組進展のための改善策の整理、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、改善策と現状の比較／好事例、改善策を補う示唆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改善策、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、改善策の実践状況把握に則した設問・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、改善策と現状の比較／好事例、改善策を補う示唆の抽出の質的向上を期待することができる。

(2) 改善策の整理

各調査軸に対し、本調査によって実践状況の把握を試みる改善策を整理した。基本的には、2022 年度の実態調査で特定された、「(1)背景」で示した 2 つの問題点と 3 つの課題に焦点を当て、今年度は、これらの問題点と課題につながる因子の特定を試みる。具体的には、問題点と課題の解消に有効な、秘密情報の漏えいに関する内部不正防止の対策・体制を改善する

施策を列挙した上で、それらの施策の実践状況を調査する。実践の割合の低い施策があれば、問題点・課題の背景要因であると推定されると同時に、その施策を推進することで状況の改善につながると考えられる。

以下では昨年度の調査で導出した望ましい方向性を囲み枠中に示した後に、それに続く形で、上記で言うその方向性を実現するための、良い（あるいは効果が期待できる、有識者が望ましいと考える）改善策を列記する。

①経営課題の改善（調査軸１）

1-1：企業においては、秘密情報漏えいに関する内部不正等のリスクが、重要な経営課題として認識されていないのではないかという懸念がある。経営層、内部不正防止に関する組織全体の責任者等が、重要な営業秘密等（個人情報以外）の漏えい／内部不正リスクを重要な経営課題として認識する必要がある。

- 【1-1】法務・知財部門（社外の法律相談サービスを含む）の協力を得る等の取組を検討して、営業秘密等の漏えい事件（事例）から、事業リスクとしての重要性や当事者がしてはならないこと等を率先して学ぶ。

1-2：経営層が内部不正防止対策に係るリーダーシップを十分に発揮し、内部不正防止の必要性を従業員に広く認識させる必要がある。

- 【1-2】経営層によるセキュリティ確保のリーダーシップ発揮の機会／場を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。

1-3：関連する取組を集約し、内部統制の効率化と強化を実現することが望ましい。

- 【1-3】重要情報漏えいのリスクマネジメント体制の下で、サイバーセキュリティと内部不正防止の両方をカバーする。

②重要な秘密の特定と取扱いの改善（調査軸２）

2-1：営業情報、技術情報、その他の情報など個人情報以外の情報資産のうち、自組織にとって重要な守るべき対象を把握できていないことが懸念されている。自組織にとって重要性／機密性の高い情報資産のうち、個人情報以外の情報（営業秘密、重要なデータ等）の特定と、その旨の表示を強化する必要がある。

・ 【2-1】経営層も積極的に関与して、事業リスクが高い（漏えいした場合のインパクトが大きい）営業秘密等を特定するための基準作り、従業員の営業秘密に対する対策意識の醸成、営業秘密の定期的な見直し等に取り組む。

③組織体制・連携に関する課題の改善（調査軸３）

3-1：組織全体としての、内部不正防止における責任・権限を明確にし、主管部門（責任部門）と実際の当事者となる関連部門との連携について全般に底上げする必要がある。

・ 【3-1】責任部門自体（リスク・コンプライアンス部門等）と関連部門（情報システム部門：対策実施部門、法務・知財部門、営業・事業部門）が協働する体制の整備を検討する。

3-2：情報システム部門は、法務・知財担当者との連携を強化し、情報システム担当者の重要情報／内部不正に関する法知識を深める必要がある。

・ 【3-2】対策を実施する情報システム部門が責任部門となる体制を取る場合は、知財・法務部門等と協力してガバナンスを確保する。

3-3：社内で内部不正の予兆を検知し、インシデントが発生した際に報告するための体制を整備することで、インシデントの発生を低減し、発生時の影響も効果的に軽減する必要がある。

・ 【3-3】重要な秘密が不自然に取り扱われているところを目にしたら、上に報告するというリテラシーと、上に報告できない事情がある場合は内部通報ができる体制を構築する。

3-4：経営層による不正であっても検知したら黙認することのないよう、経営の透明性を高める必要がある。

・ 【3-4】役職の高い者を特別扱いしないマネジメントシステムを構築し、体制を整備する。

④社員教育とリテラシー構築に関する課題の改善（調査軸４）

4-1：個人情報については、その取り扱い、情報セキュリティ対策、コンプライアンス等の教育・研修が広く実施されていると見込まれる。一方で、相対的に言及の少ない営業秘密は、個人情報に比べて優先度が必ずしも高くないと認識される懸念がある。営業秘密保護に係る制度について、情報システム担当者に法務・知財の知識を浸透させることが重要である。

・ 【4-1】 法務・知財部門の協力を得た教育・研修等によって、対策を担当する情報システム部門の重要情報漏えい／内部不正に関する法知識（不正競争防止法等）の理解を深める。

4-2：漏えいしても個人情報のような報告義務はないといった理由から、営業秘密漏えいに関する切迫感が持てていないという懸念がある。このため、営業秘密、重要なデータ等の知識を組織全体に根付かせる必要がある。

・ 【4-2】 入社／人事異動／退職等の重要なタイミングで、具体的に重要な秘密を示して、何をしてはいけないのか、どのような時に上への報告が必要か等を周知・徹底する。

4-3：各種情報資産について、事業や経営における重要性や価値、当該情報が漏えいや毀損等した場合の影響、損害などが、従業員に認識されていないことが懸念される。従業員の意識を底上げし、重要な秘密を漏れなく特定・管理する必要がある。

・ 【4-3】 事業や経営における重要性や価値、当該情報が漏えい・毀損等した場合の影響・損害などを踏まえた、秘密の重要度の判別基準を明文化した上で、この基準に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。

4-4：重要情報漏えい／内部不正防止に関する管理規程、不正に係る懲罰、モニタリングの目的や実施状況等が周知されていないと、抑止力が効かないことが懸念されるため、既存の機会をうまく活用する等の実施しやすい方法で効率的に周知し、組織全体の基礎知識の底上げ・理解促進と従業員への抑止力を強化することが望ましい。

・ 【4-4】 企業のサイバーセキュリティ／コンプライアンス等に関する取組の一環として、重要情報漏えい／内部不正防止の社内規程及びその規則、モニタリングの目的や実施状況等に焦点を当てる回数を増やす。

4-5：教育・研修は行っているが実効性が十分でなく、営業秘密等を実際に社外へ持ち出したり、転職先へ持ち込んだりするとどうなるかが従業員に浸透していないことが懸念される。教育・研修の実効性を高めるため、形式的な e-Learning に留まらず、実効性の高い教育方法を取り入れる必要がある。

・ 【4-5】 インシデント事例、解説動画・イラスト等のリッチコンテンツ、グループディスカッション、定期的な規則遵守のセルフチェック等を積極的に活用して理解を深める取組を推進すると共に、従業員に対し、営業秘密や限定提供データについて、何をしてはいけないのかを

教育する。

⑤対策実施に関する課題の改善（調査軸５）

5-1：営業秘密は個人情報に比べて優先度が必ずしも高くないと認識されてしまうと、情報漏えい対策において営業秘密保護の重要な観点が見落とされる懸念がある。このため、情報漏えい対策の技術面を担当する情報システム部門においても、営業秘密保護の要点を集約できるような社内連携を行うことが望ましい。

- 【5-1】情報システム部門と法務・知財部門が連携し、重要情報（営業秘密や限定提供データ等の知財を含む）漏えいへの対策に役立つ官民の関連ガイドライン／ハンドブックの情報を収集し、活用を進めることで、必要な対策を見直す。

5-2：内部不正防止対策を強化する上で、従業員の行動監視、ログの記録と分析等は有用だが、従業員のプライバシーを侵害していると受け取られる恐れがあり、両者のバランスを適切に取る必要がある。

- 【5-2】個人情報保護法の解釈に基づいて適切にバランスを取るための知見を得た上で、対策や教育に取り組む。

5-3：重要情報漏えいの防止にあたり、サイバーセキュリティと内部不正防止は技術的対策を中心に多くの対策を共有している。サイバーセキュリティ対策と内部不正防止対策に資金やリソースを重複投資しないよう配慮し、効率的に対策を実施することが望ましい。

- 【5-3】重要情報漏えい防止体制の下で、サイバーセキュリティ対策と内部不正防止対策の両方に一貫して取り組む。

5-4：秘密情報漏えい対策の選定にあたっては、内部不正の脅威（例：従業員の超過勤務、ハラスメントや処遇等の不満、業績の詐称、会社等への怨恨による不正、離職前のデータの持ち出し、転職先での情報利用等）を考慮し、経営層を含む中途退職者／中途採用者の内部不正対策を強化すると共に、内部不正リスクへの効率的・効果的な対策を実現する必要がある。

- 【5-4】 内部不正のリスクシナリオも加味して重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。この際には、不正に対する人的・組織的対策と技術的対策のバランスの適正化を考慮する。また、経営層の不正防止と透明性確保、アクセスログの確認範囲拡大、他社の重要情報

の不正な社内持ち込み防止、重要プロジェクト就任／離任時にも秘密保持義務の誓約書を取得、重要性の高い秘密に触れる場合の誓約書の詳細度の変更等を実施する。

*内部不正のリスクシナリオ：従業員の超過勤務／業績の詐称 ／ハラスメントや処遇等の不満／会社等への怨恨を契機とした不正、離職前のデータの持ち出し、転職先での情報利用等が挙げられる。

**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。

5-5：重要情報の範囲が個人情報から技術情報・ノウハウ等にまで広がっている一方で、個人情報以外の漏えいに対するリスク認識が十分ではなく、技術情報・ノウハウ等の情報漏えい、及び内部不正防止の対策を強化する必要がある。

- 【5-5】個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。

5-6：情報漏えい対策として、中途退職・異動・昇格等によって不要になったアクセス権限の削除、不要になった秘密情報の削除等を適時に行い、不用意な秘密情報の漏えいを防ぐ必要がある。

- 【5-6】情報機密区分に応じたアクセス権限付与状況の点検、アクセス権限付与者についての定期的な棚卸しを実施する。

⑥中小企業の構造的課題の改善（調査軸６の１～５）

中小企業は、大企業と比較するとリソースが限られており、2022 年度調査では内部不正防止に関する体制整備、対策実施、周知・教育等において、取組の遅れが浮き彫りになった。上述の調査軸「経営課題の改善」、「重要な秘密の特定と取扱いの改善」、「組織体制・連携に関する課題の改善」、「社員教育とリテラシー構築に関する課題の改善」、「対策実施に関する課題の改善」で提示した秘密情報漏えい／内部不正防止の問題点に対し、中小企業における改善策を整理した。

6-1-1：中小企業においても、重要な営業秘密等（個人情報以外）の漏えい／内部不正リスクを重要な経営課題として経営者等が認識し、秘密情報漏えい・内部不正防止の取組を効率的に改善する必要がある。

・ 【6-1-1】 経営層または内部不正防止に関する組織全体の責任者等が率先して、重要な秘密情報漏えい／内部不正リスクを重要な経営課題として認識する機会を増やし、サイバーセキュリティ確保と内部不正防止を一体的に認識した経営を行う。

6-1-2：中小企業においても、経営者等が内部不正防止対策に係るリーダーシップを十分に発揮し、内部不正防止の必要性を従業員に広く認識させる必要がある。

・ 【6-1-2】 中小企業では、全社集会などの経営層が従業員に周知徹底する機会を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。

6-2-1：特に中小企業において、守るべき情報資産を特定できていないことが懸念される。中小企業の規模では、この問題の改善にあたり、経営者等が積極的に関与することが望ましい。

・ 【6-2-1】 中小企業では、経営層が自ら判断する、あるいは判断基準を示すことで、自社の事業にとって重要性／機密性の高い秘密情報を的確に特定する。

6-3-1：組織全体としての、内部不正防止における責任・権限を明確にし、主管部門（責任部門）と実際の当事者となる関連部門との連携について全般に底上げする必要がある。

・ 【6-3-1】 中小企業では、責任者である経営層が中心となって、総務・人事・法務や情報システム等の関連部門との調整を行う。

6-3-2：情報システム部門は、法務・知財担当者との連携を強化し、情報システム担当者の重要情報／内部不正に関する法知識の理解を深める必要がある。

・ 【6-3-2】 中小企業では、通常は法務・知財に一定の知識と経験を持つ経営層が全社責任を負うため、情報システム部門は技術面から経営層を支えることに集中することで、内部不正防止の強化に貢献する。

6-3-3：社内で内部不正の予兆を検知し、インシデントが発生した際に報告するための体制を整備することで、インシデントの発生を低減し、発生時の影響も効果的に軽減する必要がある。

・ 【6-3-3】 重要な秘密が不自然に取り扱われている様を目撃した際に上に報告することの徹底と、上に報告できない事情がある場合は内部通報ができる体制を構築する。

6-3-4：経営層による不正であっても検知したら黙認することのないよう、経営の透明性を高める必要がある。

・ 【6-3-4】経営層を特別扱いしない内部不正防止体制を整備する。

6-4-1：個人情報については、その取り扱い、情報セキュリティ対策、コンプライアンス等の教育・研修が広く実施されていると見込まれる。一方で、相対的に言及の少ない営業秘密は、個人情報に比べて優先度が必ずしも高くないと認識される懸念がある。営業秘密保護に係る制度について、情報システム担当者に法務・知財の知識を浸透させることが重要である。

・ 【6-4-1】中小企業では、経営層のリーダーシップと社外の専門家（IT コーディネータ、弁護士・弁理士等）の協力により、情報システム部門や他の従業員に法務・知財の知識を広める。

6-4-2：営業秘密、重要データの知識を組織全体に根付かせる必要がある。

・ 【6-4-2】中小企業では、入社／人事異動／退職等の重要なタイミングで、経営層が重要な秘密を具体的に示し、その取扱い指示を徹底する。

6-4-3：従業員の意識と秘密の取り扱いを底上げし、重要な秘密を漏れなく特定・管理する必要がある。

・ 【6-4-3】経営層または経営層が権限を移譲した責任者が各々の秘密の重要度を指定した上で、この指定に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。

6-4-4：重要情報漏えい／内部不正防止に関する管理規程、不正に係る懲罰、モニタリングの目的や実施状況等が周知されていないと、抑止力が効かないことが懸念される。このため、既存の機会をうまく活用する等の実施しやすい方法で効率的に周知し、組織全体の基礎知識の底上げ・理解促進と従業員への抑止力を強化することが望ましい。

・ 【6-4-4】企業のサイバーセキュリティ／コンプライアンス等に関する取組の一環として、重要情報漏えい／内部不正防止の社内規程及びその規則、モニタリングの目的や実施状況等に焦点を当てる回数を増やす。

6-4-5：教育・研修は行っているが実効性が十分でなく、営業秘密等を実際に社外へ持ち出したり、不正入手した営業秘密等を転職先へ持ち込んだりするとどうなるかが従業員に浸透していないことが懸念される。形式的な e-Learning に留まらず、実効性の高い教育方法を取り入れることで、教育・研修の実効性を高める必要がある。

- 【6-4-5a】中小企業では、経営層が自ら事業リスクに基づいて、営業秘密や限定提供データの取り扱いについて何をしてはいけないのかを指示・啓発する。
- 【6-4-5b】中小企業では、経営層が全社集会などで直接従業員に教育・意識づけする。

6-5-1：個人情報に比べて営業秘密は優先度が必ずしも高くないと認識されてしまうと、情報漏えい対策において営業秘密保護の重要な観点が見落とされる懸念がある。このため、情報漏えい対策の技術面を担当する情報システム部門においても、営業秘密保護の要点を集約できるような社内連携を行うことが望ましい。

- 【6-5-1】中小企業では、経営層と担当者が協力して、重要情報（営業秘密や限定提供データ等の知財を含む）漏えい対策に役立つ官民の関連ガイドライン／ハンドブックの情報を収集し、活用を進めることで、必要な対策を見直す。

6-5-2：内部不正防止対策を強化する上で、従業員の行動監視、ログの記録と分析等は有用だが、従業員のプライバシーを侵害していると受け取られる恐れがあり、両者のバランスを適切に取ることが必要である。

- 【6-5-2】経営層が積極的に従業員とコミュニケーションを取ることで、従業員の行動監視やログの記録・分析等に対する従業員の理解を得る。

6-5-3：重要情報漏えいの防止にあたり、サイバーセキュリティと内部不正防止は技術的対策を中心に多くの対策を共有している。サイバーセキュリティ対策と内部不正防止対策に資金やリソースを重複投資しないよう配慮し、限られたリソースを効率的に活用して対策を実施することが望ましい。

- 【6-5-3】中小企業では、重要情報漏えいの防止体制の下で、サイバーセキュリティと内部不正防止の両方に共通する対策を積極的に１つにまとめる。

6-5-4：秘密情報漏えい対策の選定にあたり、限られた資金／リソースの範囲内で、内部不正の脅威（例：従業員の超過勤務、ハラスメントや処遇等の不満、業績の詐称、会社等への怨恨による不正、離職前のデータ の持ち出し、転職先での情報利用等）に効率的に対処する必要がある。

- 【6-5-4】内部不正のリスクシナリオを加味した重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。

6-5-5：重要情報の範囲が個人情報から技術情報・ノウハウ等にまで広がっているものの、これらの漏えいに対するリスク認識が十分ではなく、技術情報・ノウハウ等の情報漏えい、及び内部不正防止の対策を強化する必要がある。

- 【6-5-5】個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。

6-5-6：情報漏えい対策として、中途退職・異動・昇格等によって不要になったアクセス権限の削除、不要になった秘密情報の削除等を適時に行うことが必要である。

- 【6-5-6】情報機密区分に応じたアクセス権限付与状況の点検、アクセス権限付与者についての定期的な棚卸しを実施する。

⑦ガイドラインの利用と実践に関する課題の改善（調査軸７）

7-1：IPA が公開している「組織における内部不正防止ガイドライン」には一定の認知度がある。しかし、IPA との接点が希薄な傾向にある企業の法務・知財部門では十分に認知されていない可能性がある。読み解くには法的知識等が必要なガイドラインであるため、法務・知財部門でもガイドラインを認知してもらう工夫が必要である。他方、IPA との接点が多い傾向にあり、ガイドラインを既に認知している IT／セキュリティ部門との連携を強化することで、ガイドラインの活用を促進できる可能性がある。同時に、内部不正防止対策だけに特化した本ガイドラインは、情報漏えいに関する内部不正防止対策をセキュリティ対策の一環として位置付けている企業にとって、その存在が認知されにくいことが懸念される。

- 【7-1】認知度・活用度合の高い「サイバーセキュリティ経営ガイドライン」「秘密情報の保護ハンドブック」「営業秘密管理指針」「限定提供データに関する指針」「経済安全保障の確保に向けて 2022～技術・データ・製品等の流出防止～」との相互参照を進める。また、支援ツール開発や外部専門家派遣による適用開始支援等を検討する。

7-2：「内部不正防止ガイドライン」は認知されていても、必ずしも活用はされていない。企業ニーズを踏まえ、活用しやすい啓発資料・補足資料等を追加することが望ましい。

- 【7-2】概要版の作成、活用しやすい情報量の調整・表現の工夫、社内規程整備のために活用しやすい内容の増補、従業員への周知・教育にそのまま使えるコンテンツの充実等を検討し、「組織における内部不正防止ガイドライン」適用の実効性を高める。

⑧まとめ

ここまでの検討に基づいて整理した改善策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 本調査で整理した改善策

調査軸	改善策
経営課題の改善（調査軸１）	
	【1-1】法務・知財部門（社外の法律相談サービスを含む）の協力を得る等の取組を検討して、営業秘密等の漏えい事件（事例）から、事業リスクとしての重要性や当事者がしてはならないこと等を率先して学ぶ。
	【1-2】経営層によるセキュリティ確保のリーダーシップ発揮の機会／場を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。
	【1-3】重要情報漏えいのリスクマネジメント体制の下で、サイバーセキュリティと内部不正防止の両方をカバーする。
重要な秘密の特定と取扱いの改善（調査軸２）	
	【2-1】経営層も積極的に関与して、事業リスクが高い（漏えいした場合のインパクトが大きい）営業秘密等を特定するための基準作り、従業員の営業秘密に対する対策意識の醸成、営業秘密の定期的な見直し等に取り組む。
組織体制・連携に関する課題の改善（調査軸３）	
	【3-1】責任部門自体（リスク・コンプライアンス部門等）と関連部門（情報システム部門：対策実施部門、法務・知財部門、営業・事業部門）が協働する体制の整備を検討する。
	【3-2】対策を実施する情報システム部門が責任部門となる体制を取る場合は、知財・法務部門等と協力してガバナンスを確保する。
	【3-3】重要な秘密が不自然に取り扱われているところを目にしたら、上に報告するというリテラシーと、上に報告できない事情がある場合は内部通報ができる体制を構築する。
	【3-4】役職の高い者を特別扱いしないマネジメントシステムを構築し、体制を整備する。
社員教育とリテラシー構築に関する課題の改善（調査軸４）	
	【4-1】法務・知財部門の協力を得た教育・研修等によって、対策を担当する情報システム部門の重要情報漏えい／内部不正に関する法知識（不正競争防止法等）の理解を深める。
	【4-2】入社／人事異動／退職等の重要なタイミングで、具体的に重要な秘密を示して、何をしてはいけないのか、どのような時に上への報告が必要か等を周知・徹底する。
	【4-3】事業や経営における重要性や価値、当該情報が漏えい・毀損等した場合の影響・損害などを踏まえた、秘密の重要度の判別基準を明文化した上で、この基準に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。
	【4-4】企業のサイバーセキュリティ／コンプライアンス等に関する取組の一環として、重要情報漏えい／内部不正防止の社内規程及びその規則、モニタリングの目的や実施状況等に焦点を当てる回数を増やす。
	【4-5】インシデント事例、解説動画・イラスト等のリッチコンテンツ、グループディスカッション、定期的な規則遵守のセルフチェック等を積極的に活用して理解を深める取組を推進すると共に、従

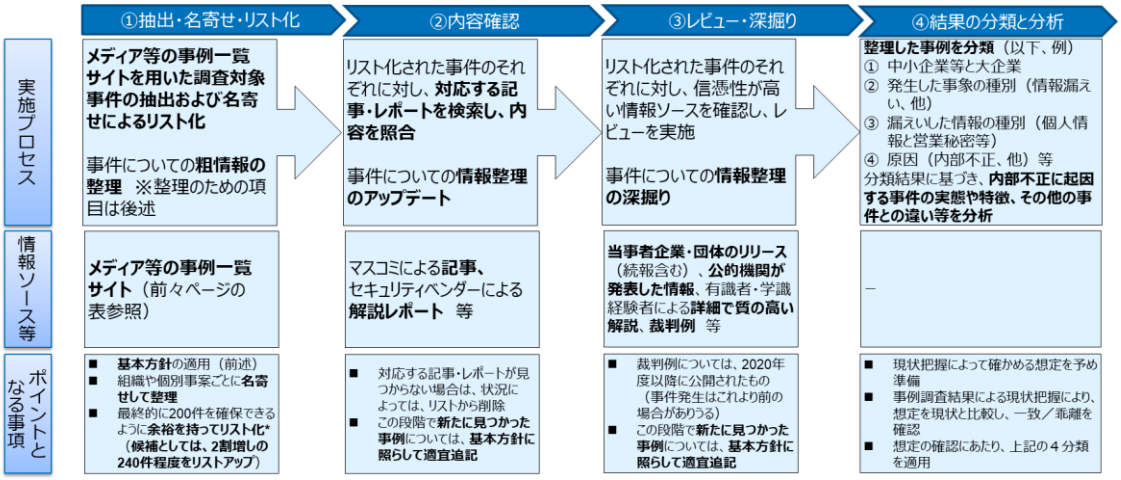
調査軸	改善策
	業員に対し、営業秘密や限定提供データについて、何をしてはいけないのかを教育する。
対策実施に関する課題の改善（調査軸５）	
	【5-1】情報システム部門と法務・知財部門が連携し、重要情報（営業秘密や限定提供データ等の知財を含む）漏えいへの対策に役立つ官民の関連ガイドライン／ハンドブックの情報を収集し、活用を進めることで、必要な対策を見直す。
	【5-2】個人情報保護法の解釈に基づいて適切にバランスを取るための知見を得た上で、対策や教育に取り組む。
	【5-3】重要情報漏えい防止体制の下で、サイバーセキュリティ対策と内部不正防止対策の両方に一貫して取り組む。
	【5-4】 内部不正のリスクシナリオも加味して重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。この際には、不正に対する人的・組織的対策と技術的対策のバランスの適正化を考慮する。また、経営層の不正防止と透明性確保、アクセスログの確認範囲拡大、他社の重要情報の不正な社内持ち込み防止、重要プロジェクト就任／離任時にも秘密保持義務の誓約書を取得、重要性の高い秘密に触れる場合の誓約書の詳細度の変更等を実施する。
	【5-5】個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。
	【5-6】情報機密区分に応じたアクセス権限付与状況の点検、アクセス権限付与者についての定期的な棚卸しを実施する。
中小企業の構造的課題の改善（調査軸６）	
	【6-1-1】経営層または内部不正防止に関する組織全体の責任者等が率先して、重要な秘密情報漏えい／内部不正リスクを重要な経営課題として認識する機会を増やし、サイバーセキュリティ確保と内部不正防止を一体的に認識した経営を行う。
	【6-1-2】中小企業では、全社集会などの経営層が従業員に周知徹底する機会を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。
	【6-2-1】中小企業では、経営層が自ら判断する、あるいは判断基準を示すことで、自社の事業にとって重要性／機密性の高い秘密情報を的確に特定する。
	【6-3-1】中小企業では、責任者である経営層が中心となって、総務・人事・法務や情報システム等の関連部門との調整を行う。
	【6-3-2】中小企業では、通常は法務・知財に一定の知識と経験を持つ経営層が全社責任を負うため、情報システム部門は技術面から経営層を支えることに集中することで、内部不正防止の強化に貢献する。
	【6-3-3】重要な秘密が不自然に取り扱われている様を目撃した際に上に報告することの徹底と、上に報告できない事情がある場合は内部通報ができる体制を構築する。
	【6-3-4】経営層を特別扱いしない内部不正防止体制を整備する。
	【6-4-1】中小企業では、経営層のリーダーシップと社外の専門家（IT コーディネータ、弁護士・弁理士等）の協力により、情報システム部門や他の従業員に法務・知財の知識を広める。
	【6-4-2】中小企業では、入社／人事異動／退職等の重要なタイミングで、経営層が重要な秘密を具体的に示し、その取扱い指示を徹底する。
	【6-4-3】経営層または経営層が権限を移譲した責任者が各々の秘密の重要度を指定した上で、この指定に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。

調査軸	改善策
	【6-4-4】企業のサイバーセキュリティ／コンプライアンス等に関する取組の一環として、重要情報漏えい／内部不正防止の社内規程及びその規則、モニタリングの目的や実施状況等に焦点を当てる回数を増やす。
	【6-4-5a】中小企業では、経営層が自ら事業リスクに基づいて、営業秘密や限定提供データの取り扱いについて何をしてはいけないのかを指示・啓発する。
	【6-4-5b】中小企業では、経営層が全社集会などで直接従業員に教育・意識づけする。
	【6-5-1】中小企業では、経営層と担当者が協力して、重要情報（営業秘密や限定提供データ等の知財を含む）漏えい対策に役立つ官民の関連ガイドライン／ハンドブックの情報を収集し、活用を進めることで、必要な対策を見直す。
	【6-5-2】経営層が積極的に従業員とコミュニケーションを取ることで、従業員の行動監視やログの記録・分析等に対する従業員の理解を得る。
	【6-5-3】中小企業では、重要情報漏えいの防止体制の下で、サイバーセキュリティと内部不正防止の両方に共通する対策を積極的に１つにまとめる。
	【6-5-4】内部不正のリスクシナリオを加味した重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。
	【6-5-5】個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。
	【6-5-6】情報機密区分に応じたアクセス権限付与状況の点検、アクセス権限付与者についての定期的な棚卸しを実施する。
ガイドラインの利用と実践に関する課題の改善（調査軸７）	
	【7-1】認知度・活用度合の高い「サイバーセキュリティ経営ガイドライン」「秘密情報の保護ハンドブック」「営業秘密管理指針」「限定提供データに関する指針」「経済安全保障の確保に向けて 2022～技術・データ・製品等の流出防止～」との相互参照を進める。また、支援ツール開発や外部専門家派遣による適用開始支援等を検討する。
	【7-2】概要版の作成、活用しやすい情報量の調整・表現の工夫、社内規程整備のために活用しやすい内容の増補、従業員への周知・教育にそのまま使えるコンテンツの充実等を検討し、「組織における内部不正防止ガイドライン」適用の実効性を高める。

(3) 事例調査の実施方法

ここでは、国内のインシデント発生状況、そのうち内部不正等に係る実態について調査した。図表４に示した通り、①「メディア等の事例一覧サイト」を用いた調査対象事件の抽出・名寄せ及びリスト化、②記事・解説レポートとの照合による内容確認、③信憑性の高い情報ソースを用いたレビューと調査結果の深掘り、④調査結果の分類及び実態・特徴・違い等の分析 という手順に沿って調査を実施した。

図表４　事例調査の実施手順



各段階における調査の実施内容は次の通りである。図表５に予め準備した現在の実態や動向に関する想定を示す。

①　抽出・名寄せ・リスト化

事例一覧サイトから 2020 年４月以降に公表された事例を抽出してリスト化した。

②　内容確認

①でリスト化した事例について、対応する記事・レポートを検索し、内容を確認した。

③　レビュー・深掘り

②で確認した事例について、プレスリリース、調査報告書、裁判例等の信憑性が高い情報ソースを確認して、各事例の内容のレビューと追記（深掘り）を実施した。

④　結果の分類と分析

分析の ４ つの切り口毎に、現在の実態や動向に関する想定を予め準備しておき、事例調査結果からの現状把握によって想定と現状を比較し、その一致と乖離を確認した。

図表５　予め準備した現在の実態や動向に関する想定

分析の切り口	現在の実態や動向に関する想定（現状との比較を試みるもの）
①企業規模による事案発生傾向の違い	
	■ 営業秘密は大企業だけでなく、規模が小さい企業等からも漏えいしている ■ 内部不正は大企業だけでなく、規模が小さい企業等でも発生している ■ 規模が小さい企業等であっても、情報漏えいによる被害のインパクトは大きい

分析の切り口	現在の実態や動向に関する想定（現状との比較を試みるもの）
②情報漏えいとサービス／システム停止の事案発生傾向の違い	
	■ 内部不正の場合は情報漏えいがほとんどであり、サービス／システムの停止を伴うことはほとんどない ■ 取引先からの情報漏えい、取引先に起因するサービス／システム停止の両方が目立ってきている ■ サイバー攻撃による情報漏えいの目的が、産業スパイ（他国政府、民間企業）であることはまだ少ない
③個人情報漏えいと営業秘密漏えいの事案発生傾向の違い	
	■ 規模が小さい営業秘密の漏えいは表に出ていない ■ 営業秘密漏えいによる被害規模は、個人情報漏えいの場合と比べてみても、十分に大きい ■ ミスによる情報漏えいは個人情報の漏えいが多いが、営業秘密の漏えいも目立ってきている ■ 取引先からの情報漏えいは、個人情報でも営業秘密でも発生している ■ 外国政府の関与が疑われるのは、営業秘密が漏えいした場合である
④内部不正とサイバー攻撃の事案発生傾向の違い	
	■ 営業秘密の漏えいは内部不正によるものが中心である ■ 個人情報の漏えいは、サイバー攻撃でも内部不正でも多く発生している ■ 取引先でも、内部不正とサイバー攻撃の両方が多く発生している ■ 外国政府の関与が疑われるサイバー攻撃が目立ってきている

(4) アンケートとインタビューを組み合わせた改善策と現状の比較分析・示唆抽出方法

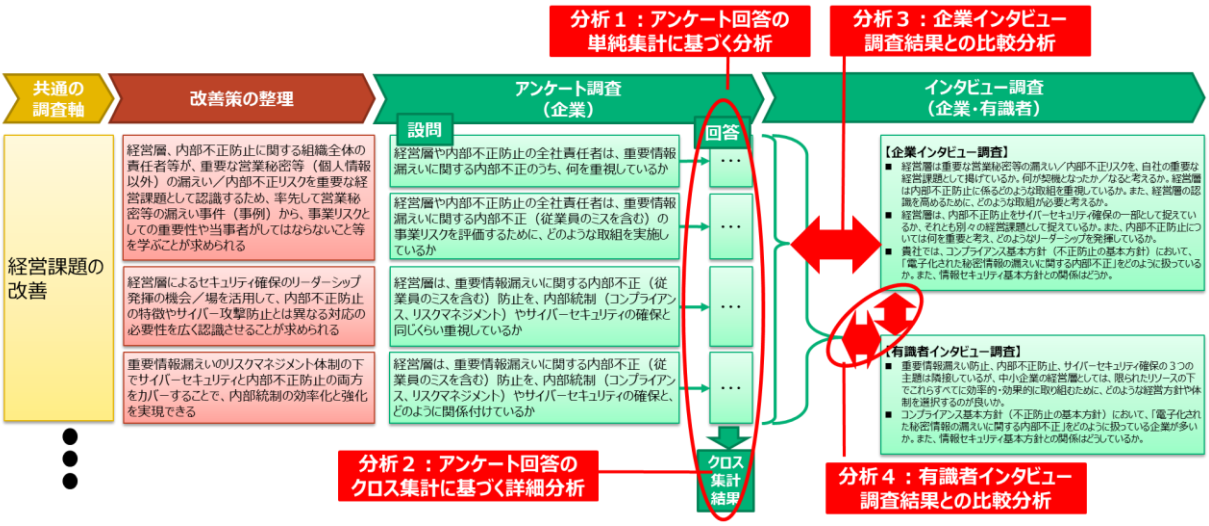
既に述べた通り、本調査では実態調査で実践状況の把握を試みる改善策の整理、企業アンケートの設問や企業／有識者へのインタビュー項目の設計、調査結果の集計・分析、改善策と現状の比較／好事例、改善策を補う示唆の抽出という一連の作業の全てを共通の調査軸の上で横串を通して実施した。この共通の調査軸と本調査のフレームワークについては図表２に示した通りである。調査結果（全体）の分析は、共通の調査軸に基づいて設計された企業アンケート調査、企業インタビュー調査、有識者インタビュー調査の結果を、共通の調査軸の上で比較することによって実施した。

調査結果の分析においては、具体的には次の４つのステップで単独での分析及び比較分析を実施した。この分析方法について図表６に取りまとめたので参照されたい。

- **分析１：**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）
- **分析２：**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、企業規模による傾向の違いを深掘り）

- **分析３：**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
- **分析４：**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６　調査結果の分析方法



今回、企業アンケート調査で経営層から一定数の回答（約 38%、そのうち７割以上が中小企業の経営層）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中小企業の経営者／経営幹部から複数社にわたって共通性のある回答を得ることができたことを踏まえ、中小企業の経営層の認識やリーダーシップの現状についても掘り下げて分析することとした。

(5) 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
ii.　情報システム関連部門を所掌・所管する部門の責任者
iii.　リスクマネジメント計画・実践に関わる部署の担当者
iv.　リスクマネジメント計画・実践に関わる部署を所掌・所管する部門の責任者
v.　経営企画部門の IT/セキュリティ戦略担当者

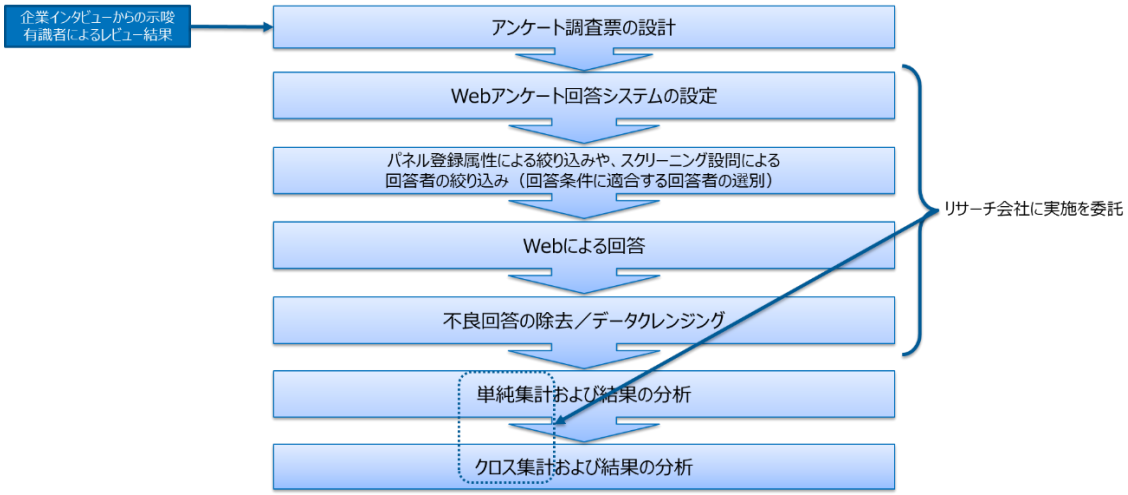
vi. 経営企画部門の IT/セキュリティ戦略担当を所掌・所管する部門の責任者
vii. 経営層
viii. ⅰ ～ vi 以外の部門でも、リスクマネジメントに関する業務を実施していると認識している担当者

主たる調査対象者は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。加えて、アンケート冒頭で、回答者に担当している業務を問うスクリーニング設問に回答してもらい、アンケート回答要件に合致する回答者のみが本設問の回答に進むことができるように、回答システムを設定する手段を適用した。

②アンケート調査の実施プロセス

パネルモニターに対するアンケート調査の実施プロセスを図表 7 に取りまとめた。基本的にはオンラインで回答者を選んで回答を依頼し、Web システムを用いてアンケートに回答してもらい、集めた回答の品質を確認し、回答の単純集計とクロス集計を実施するというプロセスである。

図表 7．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、これに沿い調査を実施した。回収要件は次の 5 点である。なお、本調査では Web を用いて回答を回収することとし、郵送による手段は用いなかった。

i. 国内企業に所属する回答者から、有効回答を 1,000 件（または 1,000 社)以上収集すること
ii. 回答企業（回答者の所属する企業）の従業員数、業種（製造業／非製造業）を把握し、調査結果のクロス分析を可能とすること
iii. 製造業の回答を 300 件以上、非製造業の回答を 400 件以上集めること
iv. 回答企業（回答者の所属する企業）の従業員数が 301 名以上の回答を 300 件以上集めること
v. 部門の責任者及び経営層の回答を 200 件以上集めること

市場調査会社のパネルモニターとノウハウを活用し、上記の回収要件を満足できる規模のアンケート回答を回収した。

④回答率の向上策

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担低減策を適用した。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

調査軸と改善策に沿ったアンケート設問の設計について以下で述べる。なお、アンケート調査票の設問一式を別冊 1 に添付している。

(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。

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

また、回答者の勤務先が常時使用する従業員の数を確認するため、常時使用する従業員数を尋ねる設問を設けた。その回答に基づき、常時使用する従業員数が 5 人以下、6 ～20 人の企業に属する回答者は調査対象外として、回答を依頼しなかった。クロス集計では従業員の数が 301 人以上と、300 人以下を区分して分析を行った。

(b) 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、回答者が所属する企業の業種を尋ねる設問を設けた。

(c) 改善策の実践状況を把握するために設けた設問

図表 3 で示した各調査軸の各改善策に対し、その実践状況を把握するためのアンケート設問を設計した。

以下、調査軸ごとに、改善策とアンケート設問の対応表を掲示する。

経営課題の改善（調査軸１）

図表８．調査軸１に紐づく各改善策と現状の比較／好事例抽出のためのアンケート設問の設計結果

改善策	改善策と現状の比較／好事例抽出のためのアンケート設問
【1-1】法務・知財部門（社外の法律相談サービスを含む）の協力を得る等の取組を検討して、営業秘密等の漏えい事件（事例）から、事業リスクとしての重要性や当事者がしてはならないこと等を率先して学ぶ。 【1-2】経営層によるセキュリティ確保のリーダーシップ発揮の機会／場を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。 【1-3】重要情報漏えいのリスクマネジメント体制の下で、サイバーセキュリティと内部不正防止の両方をカバーする。	Q2．経営層や、秘密情報保護を統括する組織等の責任者は、秘密情報の漏えいに関するどのようなリスクが高いと認識していると思うか。 Q3．経営層は、「秘密情報の漏えいに繋がる内部不正」への対応方針等について、一般従業員や関連部門と対話する機会を設けているか。 Q4．経営層は、秘密情報保護に関する基本方針等で、内部不正防止をサイバーセキュリティ確保と意識的に分けて定めているか。 Q5．経営層は、内部不正防止について定めた基本方針等を公表しているか。(Q4.で「1．内部不正防止を、サイバーセキュリティ確保と意識的に分けて定めている」と回答した場合のみ) Q6．基本方針等の公表に至った理由は何だと思うか(Q5.で「1.公表している」と回答した場合のみ)

重要な秘密の特定と取扱いの改善（調査軸２）

図表９．調査軸２に紐づく各改善策と現状の比較／好事例抽出のためのアンケート設問の設計結果

改善策	改善策と現状の比較／好事例抽出のためのアンケート設問
【2-1】経営層も積極的に関与して、事業リスクが高い（漏えいした場合のインパクトが大きい）営業秘密等を特定するための基準作り、従業員の営業秘密に対する対策意識の醸成、営業秘密の定期的な見直し等に取り組む。	Q7．個人情報以外の秘密情報（営業秘密、重要なデータ等）の特定と格付けの実効性を高めるために、組織全体でどのような取組を実施しているか。 Q8．従業員は、自部署・他部署の情報に関わらず、個人情報以外の秘密情報に触れた際に、格付けの表示等によってほぼ漏れなく秘密情報であることを認知できるか。

組織体制・連携に関する課題の改善（調査軸３）

図表 10. 調査軸３に紐づく各改善策と現状の比較／好事例抽出のためのアンケート設問の設計結果

改善策	改善策と現状の比較／好事例抽出のためのアンケート設問
【3-1】責任部門自体（リスク・コンプライアンス部門等）と関連部門（情報システム部門：対策実施部門、法務・知財部門、営業・事業部門）が協働する体制の整備を検討する。 【3-2】対策を実施する情報システム部門が責任部門となる体制を取る場合は、知財・法務部門等と協力してガバナンスを確保する。 【3-3】重要な秘密が不自然に取り扱われているところを目にしたら、上に報告するというリテラシーと、上に報告できない事情がある場合は内部通報ができる体制を構築する。 【3-4】役職の高い者を特別扱いしないマネジメントシステムを構築し、体制を整備する。	Q9.「秘密情報の漏えいに繋がる内部不正」が発生した際に、誰が主体的に対応するかが、社内規程等で定められているか。 Q10. 経営層または関連組織による「秘密情報の漏えいに繋がる内部不正」への当面の対応は、不十分であると感じているか。(Q9 で「主体的に対応する部署は定められていない」または「わからない」と回答した場合のみ) Q11.「秘密情報の漏えいに繋がる内部不正」に対応する経営層や組織は、平時に他の組織とどのような目的で連携しているか。 Q12. 秘密情報が不自然に取り扱われていることや、社外への不正な漏えいを目撃した際に、上司や全社責任者／経営層に報告を上げる体制やルールがあるか。

社員教育とリテラシー構築に関する課題の改善（調査軸４）

図表１１．調査軸４に紐づく各改善策と現状の比較／好事例抽出のためのアンケート設問の設計結果

改善策	改善策と現状の比較／好事例抽出のためのアンケート設問
【4-1】法務・知財部門の協力を得た教育・研修等によって、対策を担当する情報システム部門の重要情報漏えい／内部不正に関する法知識（不正競争防止法等）の理解を深める。 【4-2】入社／人事異動／退職等の重要なタイミングで、具体的に重要な秘密を示して、何をしてはいけないのか、どのような時に上への報告が必要か等を周知・徹底する。 【4-3】事業や経営における重要性や価値、当該情報が漏えい・毀損等した場合の影響・損害などを踏まえた、秘密の重要度の判別基準を明文化した上で、この基準に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。 【4-4】企業のサイバーセキュリティ／コンプライアンス等に関する取組の一環として、重要情報漏えい／内部不正防止の社内規程及びその規則、モニタリングの目的や実施状況等に焦点を当てる回数を増やす。 【4-5】インシデント事例、解説動画・イラスト等のリッチコンテンツ、グループディスカッション、定期的な規則遵守のセルフチェック等を積極的に活用して理解を深める取組を推進すると共に、従業員に対し、営業秘密や限定提供データについて、何をしてはいけないのかを教育する。	Q13．経営幹部の不正も含めて、社内で発生した秘密情報漏えいや、その要因となった内部不正の事実を社内に告知しているか。 Q14．貴社では、個人情報以外の秘密情報（営業秘密、重要なデータ等）の保護が、個人情報保護と同じように重要であることを周知・教育しているか。 Q15．個人情報以外の秘密情報（営業秘密、重要なデータ等）の特定と格付けのための全社共通の基準を、社員教育等で全ての従業員に周知・徹底しているか。 Q16．秘密情報が不自然に取り扱われていることや、社外への不正な漏えいを目撃した際の適切な行動について、社員教育等で組織全体に周知・徹底しているか。 Q17．個人情報以外の秘密情報（営業秘密、重要なデータ等）の漏えいや内部不正に関し、何をしてはいけないのか、何をするとどのように罰せられるのかを例示する等、従業員に対してわかりやすく周知しているか。 Q18．秘密情報漏えいや内部不正防止の従業員教育にあたり、e-Learning 以外の方法を実施しているか。

対策実施に関する課題の改善（調査軸５）

図表１２．調査軸５に紐づく各改善策と現状の比較／好事例抽出のためのアンケート設問の設計結果

改善策	改善策と現状の比較／好事例抽出のためのアンケート設問
【5-1】情報システム部門と法務・知財部門が連携し、重要情報（営業秘密や限定提供データ等の知財を含む）漏えいへの対策に役立つ官民の関連ガイドライン／ハンドブックの情報を収集し、活用を進めることで、必要な対策を見直す。 【5-2】個人情報保護法の解釈に基づいて適切にバランスを取るための知見を得た上で、対策や教育に取り組む。 【5-3】重要情報漏えい防止体制の下で、サイバーセキュリティ対策と内部不正防止対策の両方に一貫して取り組む。 【5-4】 内部不正のリスクシナリオも加味して重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。この際には、不正に対する人的・組織的対策と技術的対策のバランスの適正化を考慮する。また、経営層の不正防止と透明性確保、アクセスログの確認範囲拡大、他社の重要情報の不正な社内持ち込み防止、重要プロジェクト就任／離任時にも秘密保持義務の誓約書を取得、重要性の高い秘密に触れる場合の誓約書の詳細度の変更等を実施する。 【5-5】個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。 【5-6】情報機密区分に応じたアクセス権限付与状況の点検、アクセス権限付与者についての定期的な棚卸しを実施する。	Q19．機密性の高い重要な秘密情報へのアクセス権の定期的な見直しや棚卸しを実施しているか。 Q20．個人情報保護だけでなく、それ以外の秘密情報（営業秘密、重要なデータ等）を保護する対策も重視しているか。 Q21．「秘密情報の漏えいに繋がる内部不正リスク」を、「サイバー攻撃リスク」や「会計不正・ハラスメント等のリスク」と意識的に分けて評価しているか。 Q22．（以下に列挙した）「秘密情報の漏えいに繋がる内部不正防止」に特有の対策のうち、貴社で実際に実施しているものはどれか。 Q23．（上述した）「秘密情報の漏えいに繋がる内部不正防止対策」を「サイバー攻撃対策」や「会計不正・ハラスメント等の対策」と意識的に使い分けているか。

中小企業の構造的課題の改善（調査軸６の１～５）

図表１３．調査軸６に紐づく各改善策と現状の比較／好事例抽出のためのアンケート設問の設計結果

改善策	改善策と現状の比較／好事例抽出のためのアンケート設問
【6-1-1】経営層または内部不正防止に関する組織全体の責任者等が率先して、重要な秘密情報漏えい／内部不正リスクを重要な経営課題として認識する機会を増やし、サイバーセキュリティ確保と内部不正防止を一体的に認	調査軸６では、回答者の勤務先が常時使用する従業員数を問う設問と、調査軸１～５に紐づく設問のクロス集計結果を用いて分析を行う。

識した経営を行う。 【6-1-2】中小企業では、全社集会などの経営層が従業員に周知徹底する機会を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。	（クロス集計の実施イメージ） **●常時使用従業員数（300 人以下が対象）× 調査軸１～５に紐づく設問** （各調査軸でクロス集計の対象とする設問の一覧） ●調査軸１：経営課題の改善 Q2，Q3，Q4
【6-2-1】中小企業では、経営層が自ら判断する、あるいは判断基準を示すことで、自社の事業にとって重要性／機密性の高い秘密情報を的確に特定する。	●調査軸２：重要な秘密の特定と取扱いの改善 Q7，Q8
【6-3-1】中小企業では、責任者である経営層が中心となって、総務・人事・法務や情報システム等の関連部門との調整を行う。 【6-3-2】中小企業では、通常は法務・知財に一定の知識と経験を持つ経営層が全社責任を負うため、情報システム部門は技術面から経営層を支えることに集中することで、内部不正防止の強化に貢献する。 【6-3-3】重要な秘密が不自然に取り扱われている様を目撃した際に上に報告することの徹底と、上に報告できない事情がある場合は内部通報ができる体制を構築する。 【6-3-4】経営層を特別扱いしない内部不正防止体制を整備する。	●調査軸３：組織体制・連携に関する課題の改善 Q9，Q12
【6-4-1】中小企業では、経営層のリーダーシップと社外の専門家（ITコーディネータ、弁護士・弁理士等）の協力により、情報システム部門や他の従業員に法務・知財の知識を広める。 【6-4-2】中小企業では、入社／人事異動／退職等の重要なタイミングで、経営層が重要な秘密を具体的に示し、その取扱い指示を徹底する。 【6-4-3】経営層または経営層が権限を移譲した責任者が各々の秘密の重要度を指定した上で、この指定に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。 【6-4-4】企業のサイバーセキュリティ／コンプライアンス等に関する取組の一環として、重要情報漏えい／内部不正防止の社内規程及びその規則、モニタリングの目的や実施状	●調査軸４：社員教育とリテラシー構築に関する課題の改善 Q13，Q16，Q14，Q15，Q17，Q18

況等に焦点を当てる回数を増やす。 【6-4-5a】中小企業では、経営層が自ら事業リスクに基づいて、営業秘密や限定提供データの取り扱いについて何をしてはいけないのかを指示・啓発する。 【6-4-5b】中小企業では、経営層が全社集会などで直接従業員に教育・意識づけする。	
【6-5-1】中小企業では、経営層と担当者が協力して、重要情報（営業秘密や限定提供データ等の知財を含む）漏えい対策に役立つ官民の関連ガイドライン／ハンドブックの情報を収集し、活用を進めることで、必要な対策を見直す。 【6-5-2】経営層が積極的に従業員とコミュニケーションを取ることで、従業員の行動監視やログの記録・分析等に対する従業員の理解を得る。 【6-5-3】中小企業では、重要情報漏えいの防止体制の下で、サイバーセキュリティと内部不正防止の両方に共通する対策を積極的に 1 つにまとめる。 【6-5-4】内部不正のリスクシナリオを加味した重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。 【6-5-5】個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。 【6-5-6】情報機密区分に応じたアクセス権限付与状況の点検、アクセス権限付与者についての定期的な棚卸しを実施する。	●調査軸 5 ：対策実施に関する課題の改善 Q22，Q23，Q21，Q20，Q19

ガイドラインの利用と実践に関する課題の改善（調査軸７）

図表１４．調査軸７に紐づく各改善策と現状の比較／好事例抽出のためのアンケート設問の設計結果

改善策	改善策と現状の比較／好事例抽出のためのアンケート設問
【7-1】 認知度・活用度合の高い「サイバーセキュリティ経営ガイドライン」「秘密情報の保護ハンドブック」「営業秘密管理指針」「限定提供データに関する指針」「経済安全保障の確保に向けて 2022～技術・データ・製品等の流出防止～」との相互参照を進める。また、支援ツール開発や外部専門家派遣による適用開始支援等を検討する。 【7-2】 概要版の作成、活用しやすい情報量の調整・表現の工夫、社内規程整備のために活用しやすい内容の増補、従業員への周知・教育にそのまま使えるコンテンツの充実等を検討し、「組織における内部不正防止ガイドライン」適用の実効性を高める。	Q24．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」をどのように活用しているか。 Q25．「組織における内部不正防止ガイドライン」以外に参考としている資料はあるか。

(6) 企業インタビューの実施方法

①調査対象者

国内の中小企業等 5 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 7 つの要件のうち基本的に 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協力を依頼した。

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

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

②インタビューの実施方法

インタビュー調査はオンライン会議（Microsoft Teams）で実施した。

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 7 つの調査軸のそれぞれに紐づく改善策の実践状況を把握し、企業アンケートの回答から得られる結果と比較分析を行うため、企業インタビューの調査項目を設計した。調査項目の設計にあたり、通常用いる調査項目（「通常版」と表記）に加えて、より簡潔な調査票を希望するインタビュー先に配慮した調査項目（「簡潔版」と表記）を併せて設計した。

各調査軸に対する改善策とインタビュー調査項目の対応を図表１５～２１に取りまとめた。また、企業インタビュー調査票の体裁に取りまとめた書面を別冊２に示した。

経営課題の改善（調査軸１）

図表１５．調査軸１に紐づく各改善策と現状の比較／好事例抽出のための企業インタビュー調査項目の設計結果

改善策	対応する企業インタビュー調査項目	
	通常版	簡潔版
【1-1】法務・知財部門（社外の法律相談サービスを含む）の協力を得る等の取組を検討して、営業秘密等の漏えい事件（事例）から、事業リスクとしての重要性や当事者がしてはならないこと等を率先して学ぶ。 【1-2】経営層によるセキュリティ確保のリーダーシップ発揮の機会／場を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。 【1-3】重要情報漏えいのリスクマネジメント体制の下で、サイバーセキュリティと内部不正防止の両方をカバーする。	1.「秘密情報漏えい及びその主因である内部不正」の経営課題としての位置づけ、及び経営層が重視する取組とリーダーシップの現状 (1) 経営課題としての位置付け、基本方針による意識付け ● 経営層は、秘密情報の漏えいやこれに関わる内部不正防止を貴社の重要な経営課題として掲げていますか。何が経営課題として掲げる契機となったか／なると考えるか。 ● また、情報漏えいや内部不正防止に向けた取組の基本方針を定めて公表しているか。公表している場合、公表に至った理由は何か。	1．情報セキュリティ基本方針について ● 貴社では、情報セキュリティの基本方針を定めているか。また、定めた基本方針を公開しているか。 ● 上記の情報セキュリティ基本方針において、秘密情報の保護に関する方針を定めているか。 2．情報セキュリティにおける経営層のリーダーシップについて ● 経営層は、率先して情報セキュリティの確保に取り組んでいるか。

改善策	対応する企業インタビュー調査項目	
	通常版	簡潔版
	● この基本方針は、企業リスクマネジメントやサイバーセキュリティの基本方針とは「別建て」で定めているか。 (2) 経営層が重視する取組とリーダーシップ ● 経営層は、秘密情報の漏えいを防止するため、内部不正防止に係るどのような取組を重視してリーダーシップを発揮していますか。また、経営層の認識を高めるためには、どのような取組が必要と考えるか。 (3) 内部不正（従業員のストレス・会社等への不満の蓄積を契機とした不正、離職前のデータ持ち出しと転職先での利用、不注意によるミス等）防止に特有の取組への対応 ● 秘密情報の漏えいを防止するための内部不正防止の取組は、企業リスクマネジメント（内部統制）またはサイバーセキュリティへの対応の一環ですか。それとも、別の経営課題として、企業リスクマネジメントやサイバーセキュリティとは「別建て」で取り組んでいるか。 ● 企業リスクマネジメントやサイバーセキュリティへの対応の一環として内部不正防止に取り組んでいる場合は、どうしてこの方法を選択したのか、その理由を教えてほしい。 ● 企業リスクマネジメントやサイバーセキュリティとは「別建て」で内部不正防止に取り組んでいる場合は、経営課題として何が顕著に違っていると考えているか。	● 情報セキュリティに関して、経営層は何に特に危機感を感じているか。 個人情報の漏えいについてはどうか。 社内で扱う秘密情報を中途退職者が社外に持ち出すことについてはどうか。

重要な秘密の特定と取扱いの改善（調査軸２）

図表１６．調査軸２に紐づく各改善策と現状の比較／好事例抽出のための企業インタビュー調査項目の設計結果

改善策	対応する企業インタビュー調査項目	
	通常版	簡潔版
【2-1】 経営層も積極的に関与して、事業リスクが高い（漏えいした場合のインパクトが大きい）営業秘密等を特定するための基準作り、従業員の営業秘密に対する対策意識の醸成、営業秘密の定期的な見直し等に取り組む。	1.「秘密情報漏えい及びその主因である内部不正」の経営課題としての位置づけ、及び経営層が重視する取組とリーダーシップの現状 (4) 個人情報以外の秘密情報の特定、格付け、保護管理、表示 ● 個人情報以外の秘密情報の特定・格付け・保護管理、および格付け等の表示について、どのような取組を重視しているか。その取組に対して、経営層はどのように関与しているか。	3. 情報資産（特に秘匿する情報）の管理について ● 情報セキュリティ管理において、情報資産管理はどのように実施しているか。 ● 情報資産の１つとして、個人情報や社内で扱う秘密情報は漏れなく管理できていますか。また、個人情報や秘密情報を従業員が識別できるようにしているか。 ● 一般の従業員の方々は、個人情報や秘密情報を十分に注意して取り扱っているか。万一漏らしてしまったらどのように上に報告するかが規則で定められているか。

組織体制・連携に関する課題の改善（調査軸３）

図表１７．調査軸３に紐づく各改善策と現状の比較／好事例抽出のためのインタビュー調査項目の設計結果

改善策	対応する企業インタビュー調査項目	
	通常版	簡潔版
【3-1】 責任部門自体（リスク・コンプライアンス部門等）と関連部門（情報システム部門：対策実施部門、法務・知財部門、営業・事業部門）が協働する体制の整備を検討する。 【3-2】 対策を実施する情報システム部門が責任部門となる体制を取る場合は、知財・法務部門等と協力してガバナンスを確保する。 【3-3】 重要な秘密が不自然に取り	2.「秘密情報漏えい及びその主因である内部不正」の防止に向けた体制と責任分担 (1) 体制と責任分担の構造 ● 組織として、秘密情報の漏えい防止に取り組む体制と責任分担についてご教示ください。 ● 秘密情報の漏えいを防止するために内部不正防止に取り組む責任は、経営層が担っていますか。また	４．情報セキュリティに関する体制 ● 経営層は、情報セキュリティの責任者を決めているか。 ● 情報セキュリティを主に担当する組織を設けているか（または人を定めているか）。情報資産の管理はこの組織（または人）が担当しているか。 ● 就業規則における秘密保持義務を所管する総務部、法律（個人

改善策	対応する企業インタビュー調査項目	
	通常版	簡潔版
扱われているところを目にしたら、上に報告するというリテラシーと、上に報告できない事情がある場合は内部通報ができる体制を構築する。 【3-4】役職の高い者を特別扱いしないマネジメントシステムを構築し、体制を整備する。	は、専門組織を設けて責任を持たせているか。 ● 責任を持つ経営層または専門組織の配下の内部不正防止体制はどのような構造になっていますか。 ● 専門組織を設けている場合、秘密情報の漏えい防止のために、経営層と専門組織はそれぞれどのような役割を担っているか。 ● 内部不正防止の取組の責任者は、サイバーセキュリティ対策の責任者と同じでしょうか、それとも企業リスクマネジメント（内部統制）の責任者と同じでしょうか。あるいはどちらとも別に任命しているか。 (2) リスク管理体制とその実効性 ● 秘密情報漏えいをもたらす内部不正リスクは、会計不正、その他のコンプライアンス違反、ハラスメント等のリスクマネジメントと同等の体制で管理されているか。限られた経営リソースの中で、実効性のある管理体制を構築し運用するためには、何が重要だと考えますか。また、克服しがたい課題があれば伺いたい。	情報保護法、不正競争防止法を含む情報セキュリティ関連法）を担当する経営層または法務部、秘密情報を生み出す現業部門等は、情報セキュリティの取組にどのように協力しているか。

社員教育とリテラシー構築に関する課題の改善（調査軸４）

図表１８．調査軸４に紐づく各改善策と現状の比較／好事例抽出のための企業インタビュー調査項目の設計結果

改善策	対応する企業インタビュー調査項目	
	通常版	簡潔版
【4-1】法務・知財部門の協力を得た教育・研修等によって、対策を担当する情報システム部門の重要情報漏えい／内部不正に関する法知識（不正競争防止法等）の理解	3.「秘密情報漏えい及びその主因である内部不正」の防止に向けて組織全体で実施している周知・教育の現状、リテラシー構築に関する課題を	5. 情報セキュリティに関する教育とリテラシーについて ● 貴社では、情報セキュリティに関する従業員教育や注意喚起を定期

改善策	対応する企業インタビュー調査項目	
	通常版	簡潔版
を深める。 【4-2】入社／人事異動／退職等の重要なタイミングで、具体的に重要な秘密を示して、何をしてはいけないのか、どのような時に上への報告が必要か等を周知・徹底する。 【4-3】事業や経営における重要性や価値、当該情報が漏えい・毀損等した場合の影響・損害などを踏まえた、秘密の重要度の判別基準を明文化した上で、この基準に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。 【4-4】企業のサイバーセキュリティ／コンプライアンス等に関する取組の一環として、重要情報漏えい／内部不正防止の社内規程及びその規則、モニタリングの目的や実施状況等に焦点を当てる回数を増やす。 【4-5】インシデント事例、解説動画・イラスト等のリッチコンテンツ、グループディスカッション、定期的な規則遵守のセルフチェック等を積極的に活用して理解を深める取組を推進すると共に、従業員に対し、営業秘密や限定提供データについて、何をしてはいけないのかを教育する。	改善するための取組 (1) 社員教育 ● 貴社では、秘密情報の保護や内部不正防止について、どのような社員教育を実施しているか。また、実施している理由について伺いたい。 (2) 従業員の認識を高めるための工夫 ● 秘密情報の漏えいリスクに対する従業員の認識を高めるために実施していることがあれば教えてほしい。 ● 従業員に対して、何をしてはいけないのか、どのような時に上への報告が必要か等を教育しているか。その理由や効果についてもさしつかえない範囲で訊きたい。 (3) 教育方法 ● 内部不正防止のための教育として、e-Learning 以外の手法も取り入れているか。	的に実施しているか。e-Learning 以外の方法も取り入れているか。 ● 秘密情報の漏えい防止の必要性や、禁じられた取扱いについても、従業員に教育や注意喚起をしているか。 個人情報についてはどうか。 また、社内で扱う秘密情報についてはどうか。

対策実施に関する課題の改善（調査軸５）

図表１９．調査軸５に紐づく各改善策と現状の比較／好事例抽出のための企業インタビュー調査項目の設計結果

改善策	対応する企業インタビュー調査項目	
	通常版	簡潔版
【5-1】情報システム部門と法務・知財部門が連携し、重要情報（営業秘密や限定提供データ等の知財を	4．組織として現在重視している「秘密情報漏えい及びその主因である内部不正」の防止対策、及び課題を	６．組織・人・情報の管理に関する情報セキュリティ対策について

改善策	対応する企業インタビュー調査項目	
	通常版	簡潔版
含む）漏えいへの対策に役立つ官民の関連ガイドライン／ハンドブックの情報を収集し、活用を進めることで、必要な対策を見直す。 【5-2】 個人情報保護法の解釈に基づいて適切にバランスを取るための知見を得た上で、対策や教育に取り組む。 【5-3】 重要情報漏えい防止体制の下で、サイバーセキュリティ対策と内部不正防止対策の両方に一貫して取り組む。 【5-4】 内部不正のリスクシナリオも加味して重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。この際には、不正に対する人的・組織的対策と技術的対策のバランスの適正化を考慮する。また、経営層の不正防止と透明性確保、アクセスログの確認範囲拡大、他社の重要情報の不正な社内持ち込み防止、重要プロジェクト就任／離任時にも秘密保持義務の誓約書を取得、重要性の高い秘密に触れる場合の誓約書の詳細度の変更等を実施する。 【5-5】 個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。 【5-6】 情報機密区分に応じたアクセス権限付与状況の点検、アクセス権限付与者についての定期的な棚卸しを実施する。	改善するための取組 (1) 課題と改善のための対応 ● 秘密情報の保護や漏えい防止に向けた内部不正防止対策について何を課題と感じており、どのような対応策を講じているか。 (2) 内部不正に特有の対策への対応 ● 秘密情報の漏えい防止に向けた内部不正防止対策に効率的に取り組むために、既存のサイバーセキュリティ対策や内部統制の取組をどのように活用しているか。 ● また、既存のサイバーセキュリティ対策や内部統制の取組の活用ではどうしてもカバーできない内部不正対策にはどのようなものがあるか。	● IPA「中小企業の情報セキュリティ対策ガイドライン 」の「【表 5 】自社診断のための 25 項目」が示す組織・人・情報の管理に関する対策のうち、以下を実施しているか。 ・（情報の管理）秘密情報に対する適切なアクセス制限を行っている ・（情報の管理）電子メールや FAX の送信ミスを防ぐ取組を実施している ・（情報の管理）秘密情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしている。 ・（人）従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルール（懲罰の定めを含む）を守らせている（中途退職後の守秘義務を含む） ・（組織）個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしている ・（組織）秘密情報の授受を伴う取引先との契約書には、秘密保持条項を規定している ・（組織）クラウドサービスやウェブサイトの運用などで利用する外部サービスは、安全・信頼性を把握して選定している（選定されたサービス以外の使用を禁ずることを含む） ● 上記以外にも、次の対策を実施しているか。 ・（情報の管理）個人情報や秘密

改善策	対応する企業インタビュー調査項目	
	通常版	簡潔版
		情報を定期的に棚卸ししている ・（人）従業員が不満や鬱憤を蓄積しないように、十分なコミュニケーション、労務管理、人事管理に注意している ・（組織）発生した情報セキュリティインシデントについて、社内に告知している

中小企業の構造的課題の改善（調査軸６の１～５）

企業インタビュー調査は対象が中小企業のみなので、中小企業に対し、調査軸１～５及び調査軸７に紐づく調査項目を尋ねる構造になっている。このため、調査軸６に紐づく独立した調査項目はない。この構造のイメージを図表２０に示した。

なお、後述するクロス分析においては、企業インタビュー調査結果は全て調査軸６の調査結果（中小企業に特化）として取扱うことになる。換言すれば、調査軸１～５については、クロス分析で比較対象とする企業インタビュー調査結果はない。

図表２０．調査軸６に関する調査項目の構造

改善策	対応する企業インタビュー調査項目	
	通常版	簡潔版
図表 3 における調査軸：「中小企業の構造的課題の改善」に紐づく改善策	●調査軸１の企業インタビュー調査項目（図表 15 で既出）	●調査軸１の企業インタビュー調査項目（図表 15 で既出）
・調査軸１の改善策：中小企業版	●調査軸２の企業インタビュー調査項目（図表１６で既出）	●調査軸２の企業インタビュー調査項目（図表１６で既出）
・調査軸２の改善策：中小企業版	●調査軸３の企業インタビュー調査項目（図表１７で既出）	●調査軸３の企業インタビュー調査項目（図表１７で既出）
・調査軸３の改善策：中小企業版	●調査軸４の企業インタビュー調査項目（図表１８で既出）	●調査軸４の企業インタビュー調査項目（図表１８で既出）
・調査軸４の改善策：中小企業版	●調査軸５の企業インタビュー調査項目（図表１９で既出）	●調査軸５の企業インタビュー調査項目（図表１９で既出）
・調査軸５の改善策：中小企業版		

ガイドラインの利用と実践に関する課題の改善（調査軸７）

図表２１．調査軸７に紐づく各改善策と現状の比較／好事例抽出のための企業インタビュー調査項目の設計結果

改善策	対応する企業インタビュー調査項目	
	通常版	簡潔版
【7-1】 認知度・活用度合の高い「サイバーセキュリティ経営ガイドライン」「秘密情報の保護ハンドブック」「営業秘密管理指針」「限定提供データに関する指針」「経済安全保障の確保に向けて 2022～技術・データ・製品等の流出防止～」との相互参照を進める。また、支援ツール開発や外部専門家派遣による適用開始支援等を検討する。 【7-2】 概要版の作成、活用しやすい情報量の調整・表現の工夫、社内規程整備のために活用しやすい内容の増補、従業員への周知・教育にそのまま使えるコンテンツの充実等を検討し、「組織における内部不正防止ガイドライン」適用の実効性を高める。	5．ガイドラインの利用と実践に関する課題の改善 (1) ガイドラインの活用方法 ● IPA「組織における内部不正防止ガイドライン」を知っているか。何を見て／どうやって知ったか。また、「組織における内部不正防止ガイドライン」を活用しているか。活用している場合、どのように活用しているか。 (2) ガイドラインの改善要望 ● 「組織における内部不正防止ガイドライン」を活用している場合、IPA に対して改善要望等はあるか。 (3) 活用しているその他のガイドライン ● IPA「組織における内部不正防止ガイドライン」の他に内部不正防止のために活用しているガイドラインはありますか。活用しているガイドラインがある場合、どのように活用しているか。 6．その他（IPA の事業へのご要望等） 最後に、電子化された秘密情報の漏えい防止や内部不正防止に係る IPA の事業に要望等はあるか。	7．その他（IPA の事業へのご要望等） 最後に、電子化された秘密情報の漏えい防止に係る IPA の事業に要望等はあるか。

(7) 有識者インタビューの実施方法

①調査対象者

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

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

＜インタビュー対象とした有識者（50 音順、敬称略）＞

独立行政法人工業所有権情報・研修館(INPIT)
営業秘密・知財戦略相談窓口知的財産戦略アドバイザー
小原 荘平（iiiに該当）

橋口・松本法律事務所　弁護士
松本 慶（ｉ～ivに該当）

山口利昭法律事務所　弁護士
山口 利昭（ｉ,ii,ivに該当）

早稲田大学グローバルソフトウェアエンジニアリング研究所招聘研究員
山戸 昭三（ｉiに該当）

②インタビューの実施方法

インタビューはオンライン会議（Microsoft 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から、7 つの共通の調査軸に紐づく改善策について、次の 2 つの観点で専門家としての見解を聴取し、これを企業アンケート調査結果や企業インタビュー調査結果と比較分析するため、有識者インタビューの調査項目を設計した。

i. 企業のあるべき姿と現状のギャップに関する有識者としての意見
ii. 企業をあるべき姿に導くために、企業や業界団体等の自主的取組はどうあるべきかについての提言

有識者インタビューは、企業インタビューと異なり、対象を中小企業だけに限定せずに行っている。このため、有識者から大企業と中小企業の両方に対する見解を聞き取ることができるように、「・・・は企業規模の大小によってどのように変わるか」という質問を調査項目に入れ込んである。こうして得られたインタビュー調査結果は、大企業に関する内容は調査軸 1 ～ 5 の調査結果として、中小企業に関する内容は調査軸 6 の調査結果として、それぞれを整理し、各軸のクロス分析で活用している。

さらに、調査項目の設計にあたり、内部統制／不正防止に主眼を置いた調査項目と知財保護に主眼を置いた調査項目を、それぞれ別々に設計した。各調査軸に対するインタビュー項目を図表 22～28 に取りまとめた。また、有識者インタビュー調査票の体裁に取りまとめた書面を別冊 3 に示した。

改善策と有識者インタビュー項目の対応表を以下に列記する。

経営課題の改善（調査軸１）

図表２２．調査軸１に紐づく各改善策に対する有識者インタビュー調査項目の設計結果

改善策	有識者インタビュー調査項目
【1-1】法務・知財部門（社外の法律相談サービスを含む）の協力を得る等の取組を検討して、営業秘密等の漏えい事件（事例）から、事業リスクとしての重要性や当事者がしてはならないこと等を率先して学ぶ。 【1-2】経営層によるセキュリティ確保のリーダーシップ発揮の機会／場を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。 【1-3】重要情報漏えいのリスクマネジメント体制の下で、サイバーセキュリティと内部不正防止の両方をカバーする。	【内部統制、不正防止の有識者】 ● 企業における「①秘密情報漏えいに繋がる内部不正防止」と「②会計不正、品質不正等の不正行為やハラスメントの防止」の取組方針・体制を比較した場合に、主な共通点と相違点は何か。また、重要で無視できない相違点だと考えるものがあれば訊きたい。 ● 上記の「主な共通点・相違点」、「重要で無視できない相違点」等は、**企業規模の大小によってどのように変わるか。** ● 「①秘密情報漏えいに繋がる内部不正防止」と「②会計不正、品質不正等の不正行為やハラスメントの防止」の取組方針・体制は、意識的に分けて取扱うべきだと考えるか。 ● 「①秘密情報漏えいに繋がる内部不正防止」において、経営層による不正を防止するためには、どのような方法を採るべきだと考えるか。また、まず取り組むべき改善策は何か。 【知財保護の有識者】 ● 「秘密情報の漏えい防止に関する取組方針・体制」における「①内部不正防止」と「②サイバーセキュリティ」の取扱いを比較した場合に、主な共通点と相違点は何か。また、重要で無視できない相違点だと考えるものがあれば訊きたい。 ● 上記の「主な共通点・相違点」、「重要で無視できない相違点」等は、**企業規模の大小によってどのように変わるか。** ● 「秘密情報の漏えい防止に関する取組方針・体制」において、「①内部不正防止」と「②サイバーセキュリティ」は意識的に分けて取扱うべきだと考えるか。

重要な秘密の特定と取扱いの改善（調査軸２）

図表２３．調査軸２に紐づく各改善策に対する有識者インタビュー調査項目の設計結果

改善策	有識者インタビュー調査項目
【2-1】 経営層も積極的に関与して、事業リスクが高い（漏えいした場合のインパクトが大きい）営業秘密等を特定するための基準作り、従業員の営業秘密に対する対策意識の醸成、営業秘密の定期的な見直し等に取り組む。	【内部統制、不正防止の有識者】 ― 【知財保護の有識者】 ● 企業において、経営層に「個人情報以外の秘密情報（営業秘密、重要なデータ等）を保護すること」の重要性に気付いてもらうためには、どのような方法を採るべきだと考えるか。また、まず取り組むべき改善策は何か。 ● 企業において、従業員に「個人情報以外の情報（営業秘密、重要なデータ等）を保護すること」の重要性を認識してもらうためには、どのような方法を採るべきだと考えるか。また、まず取り組むべき改善策は何か。

組織体制・連携に関する課題の改善（調査軸３）

図表２４．調査軸３に紐づく各改善策に対する有識者インタビュー調査項目の設計結果

改善策	有識者インタビュー調査項目
【3-1】 責任部門自体（リスク・コンプライアンス部門等）と関連部門（情報システム部門：対策実施部門、法務・知財部門、営業・事業部門）が協働する体制の整備を検討する。 【3-2】 対策を実施する情報システム部門が責任部門となる体制を取る場合は、知財・法務部門等と協力してガバナンスを確保する。 【3-3】 重要な秘密が不自然に取り扱われているところを目にしたら、上に報告するというリテラシーと、上に報告できない事情がある場合は内部通報ができる体制を構築する。 【3-4】 役職の高い者を特別扱いしないマネジメントシステムを構築し、体制を整備する。	【内部統制、不正防止の有識者】 ● 企業において、「①秘密情報漏えいに繋がる内部不正防止」の取組を統括する組織／人や、「②会計不正、品質不正等の不正行為やハラスメントの防止」の取組を統括する組織／人は、関連組織とどのように連携すべきと考えるか。 ● ヒヤリハットや不正等の疑いが経営層に円滑にエスカレーションされるようにするためには、内部通報制度を含め、どのような体制を構築するのが効果的だと考えるか。 ● 上記の「関連組織との連携のあり方」や「経営層に円滑にエスカレーションできる体制づくり」は、**企業規模の大小によってどのように変わると考えるか**。

改善策	有識者インタビュー調査項目
	【知財保護の有識者】 ● 知財・法務部門が、「秘密情報の漏えい」における「①内部不正防止」と「②サイバーセキュリティ」に対しどのような役割を果たすべきかについて、お考えを伺いたい。 ● 知財・法務部門の立場から見て、情報システム／セキュリティ部門には、「①内部不正防止」と「②サイバーセキュリティ」に関するどのような課題があると考えるか。 ● 上記の課題は、**企業規模の大小によってどのように変わると考えるか。**

社員教育とリテラシー構築に関する課題の改善（調査軸４）

図表２５．調査軸４に紐づく各改善策に対する有識者インタビュー調査項目の設計結果

改善策	有識者インタビュー調査項目
【4-1】法務・知財部門の協力を得た教育・研修等によって、対策を担当する情報システム部門の重要情報漏えい／内部不正に関する法知識（不正競争防止法等）の理解を深める。 【4-2】入社／人事異動／退職等の重要なタイミングで、具体的に重要な秘密を示して、何をしてはいけないのか、どのような時に上への報告が必要か等を周知・徹底する。 【4-3】事業や経営における重要性や価値、当該情報が漏えい・毀損等した場合の影響・損害などを踏まえた、秘密の重要度の判別基準を明文化した上で、この基準に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。 【4-4】企業のサイバーセキュリティ／コンプライアンス等に関する取組の一環として、重要情報漏えい／内部不正防止の社内規程及びその規則、モニタリングの目的や実施状況等に焦点を当てる回数を増やす。 【4-5】インシデント事例、解説動画・イラスト等のリッチコンテンツ、グループディスカッション、定期的な規則遵守のセルフチェック等を積極的に活用して理解を深める取組を推進すると共に、従業員に対し、営業秘密や限定提供	【内部統制、不正防止の有識者】 ● 「秘密情報漏えいに繋がる内部不正」の防止に資するように、従業員に効果的に抑止力を与えるための適切な方法について訊きたい。また、「会計不正、品質不正等の不正行為やハラスメント」を抑止する場合との重要な相違点があれば訊きたい。 【知財保護の有識者】 ● 企業が、秘密情報の重要度を判別する基準（事業や経営における重要性や価値、当該情報が漏えいや毀損等した場合の影響、損害など）を明文化して従業員に教育している好事例があれば、訊きたい。

改善策	有識者インタビュー調査項目
データについて、何をしてはいけないのかを教育する。	

対策実施に関する課題の改善（調査軸５）

図表２６．調査軸５に紐づく各改善策に対する有識者インタビュー調査項目の設計結果

改善策	有識者インタビュー調査項目
【5-1】情報システム部門と法務・知財部門が連携し、重要情報（営業秘密や限定提供データ等の知財を含む）漏えいへの対策に役立つ官民の関連ガイドライン／ハンドブックの情報を収集し、活用を進めることで、必要な対策を見直す。 【5-2】個人情報保護法の解釈に基づいて適切にバランスを取るための知見を得た上で、対策や教育に取り組む。 【5-3】重要情報漏えい防止体制の下で、サイバーセキュリティ対策と内部不正防止対策の両方に一貫して取り組む。 【5-4】 内部不正のリスクシナリオも加味して重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。この際には、不正に対する人的・組織的対策と技術的対策のバランスの適正化を考慮する。また、経営層の不正防止と透明性確保、アクセスログの確認範囲拡大、他社の重要情報の不正な社内持ち込み防止、重要プロジェクト就任／離任時にも秘密保持義務の誓約書を取得、重要性の高い秘密に触れる場合の誓約書の詳細度の変更等を実施する。 【5-5】個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。 【5-6】情報機密区分に応じたアクセス権限付与状況の点検、アクセス権限付与者についての定期的な棚卸しを実施する。	【内部統制、不正防止の有識者】 ● 企業における「①秘密情報漏えいに繋がる内部不正」と「②会計不正、品質不正等の不正行為やハラスメント」のリスク及びそれぞれの対策を比較した場合に、主な共通点と相違点は何か。また、重要で無視できない相違点だと考えるものがあれば訊きたい。 ● 「①秘密情報漏えいに繋がる内部不正」に特有のリスクや対策の重点ポイントを教えてほしい。 ● 上記の「主な共通点と相違点」、「重要で無視できない相違点」、「①に特有のリスク・対策の重点ポイント」等は、**企業規模の大小によってどのように変わるか。** 【知財保護の有識者】 ● 「秘密情報の漏えい」における「①内部不正」と「②サイバーセキュリティ」のリスク及びそれぞれの対策を比較した場合に、主な共通点と相違点は何か。また、重要で無視できない相違点だと考えるものがあれば訊きたい。 ● 上記の「主な共通点・相違点」、「重要で無視できない相違点」等は、**企業規模の大小によってどのように変わるか。** ● 「秘密情報の漏えい」における「①内部不正」と「②サイバーセキュリティ」のリスク及びそれぞれの対策は、意識的に分けて取扱うべきだと考えるか。 ● 中小企業における「個人情報以外の秘密情報（営業秘密、重要なデータ等）の漏えい防止対策」について、何が重要な課題だと考えるか。また、この課題を改善するためには何から始めるのが良いと考えるか。

中小企業の構造的課題の改善（調査軸６の１～５）

図表３で示した「中小企業の構造的課題の改善」という調査軸に紐づく各改善策に対し、上記ⅰ、ⅱの観点から有識者インタビュー調査項目を作成した。その結果を図表２７に示した。

なお、既に述べたとおり、実際のインタビューでは調査軸１～５について聞き取りを行い、得られた結果のうち中小企業に特化した内容を調査軸６の調査結果として整理している。

図表２７．調査軸６に紐づく各改善策に対する有識者インタビュー調査項目の設計結果

改善策	有識者インタビュー調査項目
【6-1-1】経営層または内部不正防止に関する組織全体の責任者等が率先して、重要な秘密情報漏えい／内部不正リスクを重要な経営課題として認識する機会を増やし、サイバーセキュリティ確保と内部不正防止を一体的に認識した経営を行う。 【6-1-2】中小企業では、全社集会などの経営層が従業員に周知徹底する機会を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。 【6-2-1】中小企業では、経営層が自ら判断する、あるいは判断基準を示すことで、自社の事業にとって重要性／機密性の高い秘密情報を的確に特定する。 【6-3-1】中小企業では、責任者である経営層が中心となって、総務・人事・法務や情報システム等の関連部門との調整を行う。 【6-3-2】中小企業では、通常は法務・知財に一定の知識と経験を持つ経営層が全社責任を負うため、情報システム部門は技術面から経営層を支えることに集中することで、内部不正防止の強化に貢献する。 【6-3-3】重要な秘密が不自然に取り扱われている様を目撃した際に上に報告することの徹底と、上に報告できない事情がある場合は内部通報ができる体制を構築する。 【6-3-4】経営層を特別扱いしない内部不正防止体制を整備する。 【6-4-1】中小企業では、経営層のリーダーシップと社外	【内部統制、不正防止の有識者】 ● 企業における「①秘密情報漏えいに繋がる内部不正防止」と「②会計不正、品質不正等の不正行為やハラスメントの防止」の取組方針・体制を比較した場合に、主な共通点と相違点は何か。また、重要で無視できない相違点だと考えるものがあれば訊きたい。（再掲） ● 上記の「主な共通点・相違点」、「重要で無視できない相違点」等は、**企業規模の大小によってどのように変わるか。**（再掲） ● 企業において、「①秘密情報漏えいに繋がる内部不正防止」の取組を統括する組織／人や、「②会計不正、品質不正等の不正行為やハラスメントの防止」の取組を統括する組織／人は、関連組織とどのように連携すべきと考えるか。（再掲） ● ヒヤリハットや不正等の疑いが経営層に円滑にエスカレーションされるようにするためには、内部通報制度を含め、どのような体制を構築するのが効果的だと考えるか。（再掲） ● 上記の「関連組織との連携のあり方」や「経営層に円滑にエスカレーションできる体制づくり」は、**企業規模の大小によってどのように変わると考えるか。**（再掲） ● 企業における「①秘密情報漏えいに繋がる内部不正」と「②会計不正、品質不正等の不正行為やハラスメント」のリスク及びそれぞれの対策を比較した場合に、主な共通点と相違点は何か。また、重要で無視できない相違

改善策	有識者インタビュー調査項目
の専門家（IT コーディネータ、弁護士・弁理士等）の協力により、情報システム部門や他の従業員に法務・知財の知識を広める。 【6-4-2】中小企業では、入社／人事異動／退職等の重要なタイミングで、経営層が重要な秘密を具体的に示し、その取扱い指示を徹底する。 【6-4-3】経営層または経営層が権限を移譲した責任者が各々の秘密の重要度を指定した上で、この指定に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。 【6-4-4】企業のサイバーセキュリティ／コンプライアンス等に関する取組の一環として、重要情報漏えい／内部不正防止の社内規程及びその規則、モニタリングの目的や実施状況等に焦点を当てる回数を増やす。 【6-4-5a】中小企業では、経営層が自ら事業リスクに基づいて、営業秘密や限定提供データの取り扱いについて何をしてはいけないのかを指示・啓発する。 【6-4-5b】中小企業では、経営層が全社集会などで直接従業員に教育・意識づけする。 【6-5-1】中小企業では、経営層と担当者が協力して、重要情報（営業秘密や限定提供データ等の知財を含む）漏えい対策に役立つ官民の関連ガイドライン／ハンドブックの情報を収集し、活用を進めることで、必要な対策を見直す。 【6-5-2】経営層が積極的に従業員とコミュニケーションを取ることで、従業員の行動監視やログの記録・分析等に対する従業員の理解を得る。 【6-5-3】中小企業では、重要情報漏えいの防止体制の下で、サイバーセキュリティと内部不正防止の両方に共通する対策を積極的に１つにまとめる。 【6-5-4】内部不正のリスクシナリオを加味した重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行	点だと考えるものがあれば訊きたい。（再掲） ● 「①秘密情報漏えいに繋がる内部不正」に特有のリスクや対策の重点ポイントを教えてほしい。（再掲） ● 上記の「主な共通点と相違点」、「重要で無視できない相違点」、「①に特有のリスク・対策の重点ポイント」等は、**企業規模の大小によってどのように変わるか。**（再掲） 【知財保護の有識者】 ● 知財・法務部門が、「秘密情報の漏えい」における「①内部不正防止」と「②サイバーセキュリティ」に対しどのような役割を果たすべきかについて、考えを訊きたい。（再掲） ● 知財・法務部門の立場から見て、情報システム／セキュリティ部門には、「①内部不正防止」と「②サイバーセキュリティ」に関するどのような課題があると考えるか。（再掲） ● 上記の課題は、**企業規模の大小によってどのように変わると考えるか。**（再掲） ● 中小企業における「個人情報以外の秘密情報（営業秘密、重要なデータ等）の漏えい防止対策」について、何が重要な課題だと考えるか。また、この課題を改善するためには何から始めるのが良いと考えるか。（再掲）

改善策	有識者インタビュー調査項目
う。 【6-5-5】 個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。 【6-5-6】 情報機密区分に応じたアクセス権限付与状況の点検、アクセス権限付与者についての定期的な棚卸しを実施する。	

ガイドラインの利用と実践に関する課題の改善（調査軸７）

図表３で示した「ガイドラインの利用と実践に関する課題の改善」という調査軸に紐づく各改善策については、有識者インタビューでは見解を聴取する対象としていない。

図表２８． 調査軸７に紐づく各改善策に対する有識者インタビュー調査項目の設計結果

改善策	有識者インタビュー調査項目
【7-1】 認知度・活用度合の高い「サイバーセキュリティ経営ガイドライン」「秘密情報の保護ハンドブック」「営業秘密管理指針」「限定提供データに関する指針」「経済安全保障の確保に向けて 2022～技術・データ・製品等の流出防止～」との相互参照を進める。また、支援ツール開発や外部専門家派遣による適用開始支援等を検討する。 【7-2】 概要版の作成、活用しやすい情報量の調整・表現の工夫、社内規程整備のために活用しやすい内容の増補、従業員への周知・教育にそのまま使えるコンテンツの充実等を検討し、「組織における内部不正防止ガイドライン」適用の実効性を高める。	―

3. 調査結果

本調査で実施した事例調査、企業アンケート調査、中小企業及び有識者のインタビュー調査の結果をまとめる。

(1) 事例調査結果

2020 年 4 月以降に発生した内部不正（故意、不注意／ミス）、サイバー攻撃、システム障害による事案のうち、メディアで報道されたものから 257 件を抽出し、事案の概要、原因と被害の種別、情報漏えいの有無と漏えいした情報の種別・規模、取引先の関与の有無等について調査を実施した。実際には 2020 年 4 月以降に報道された事案は 2,500 件を超えると見込まれるが、このうちの多くが、個人情報が漏えいしたものである。この傾向を念頭に置きつつ、他の類型の事案も広くバランスよく調査できるように、かつ、大きく報道された事案が漏れないように、調査対象事案を選定した。調査対象として抽出した事案種別の状況は図表 29 のとおりである。

図表２９． 事例調査の対象とした事案の類型と配分

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

事例調査の実施手順は図表４の通りである。最初の段階での事案の抽出は、過去に発生した事案の一覧・検索を提供しているニュースサイトを活用して実施した。次に、各社のニュース報道等を基に事案の情報を収集・確認し、さらに、事案の当事者によるプレスリリースや調査報告書、サイバーセキュリティ専門家が解説するブログ、裁判例等と照合して、取りまとめの正確性を高めた。

図表２９の件数は実際に発生している事案の分布を反映したものではない。調査対象とした

事例の数は、報道されているものの 10 分の 1 程度に過ぎない。このため、表中の数字を基に、どのような事案が多く発生しているかを指摘することは適切ではない。しかし、報道された事案を抽出に際して幅広く俯瞰し、次のような特徴があるとしても矛盾はない。

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

事例調査結果のさらに詳しい分析については、「4.(1)事例調査結果の分析からの示唆」で取りまとめているので、詳細はこちらを参照されたい。

(2) 企業アンケート調査の単純集計結果

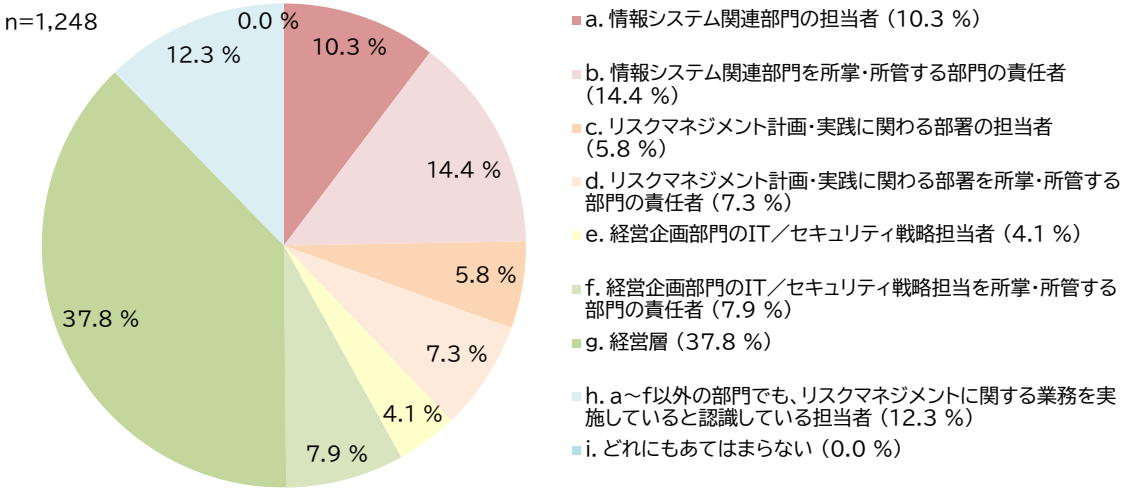
以下では、企業アンケート調査の単純集計結果に基づき、改善策と現状の比較を実施した結果を取りまとめた。

①回答者及び所属企業の属性

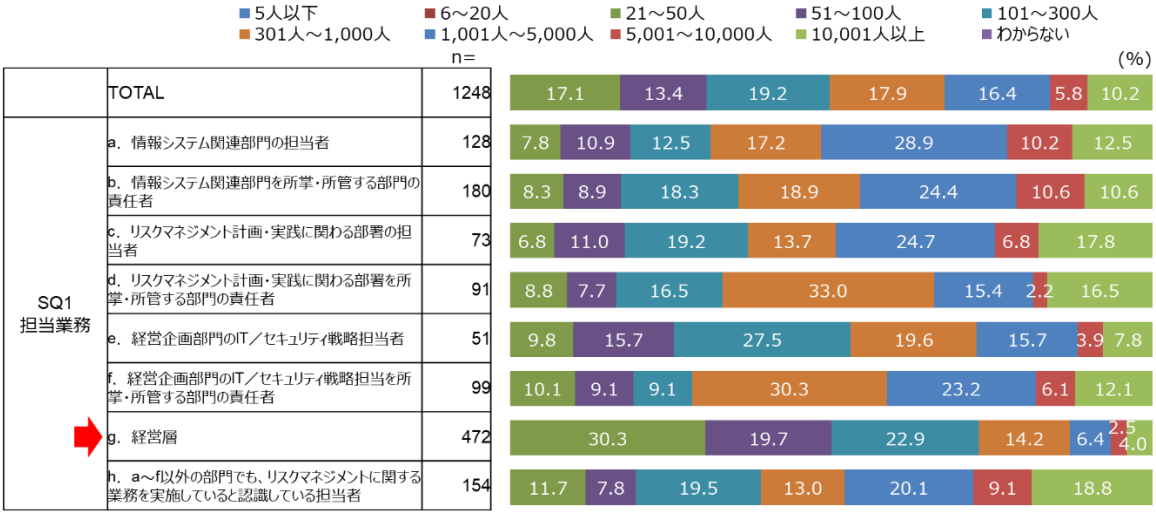
パネルモニターの回答者（主たる回答）が担当する業務については、経営層が 37.8%で最も多く、パネルモニターから回答者を選抜したことによる効果と考えられる。このうち約 73%は中小企業の経営層である。次いで情報システム関連部門を所掌・所管する部門の責任者が 14.4%となっている。（図表３０参照）

図表３０．回答者の担当業務

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



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



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。その中で、情報サービス業、その他サービス業、卸売業・小売業等が 10%を超える、または 10%に近い割合となっている。（図表３１参照）

図表３１．所属企業の業種

Q1.貴社の業種の業種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）　（%）

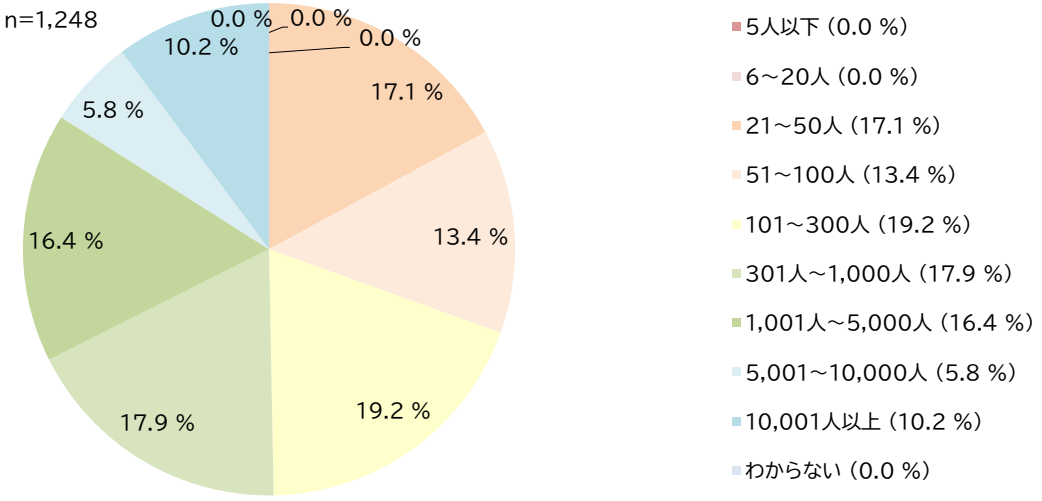
	n=	1. 農業、 林業、漁業	2. 鉱業、 採石業、 砂利採取業	3. 建設業	4. 食料品 製造業	5. 飲料・ たばこ・ 飼料製造業	6. 繊維工業	7. 化学工業	8. プラスチック 製品製造業	9. ゴム製品 製造業	10. 鉄鋼業	11. はん用 機械器具 製造業	12. 生産用 機械器具 製造業
		0.2	0.2	5.4	3.6	0.9	1.1	2.5	0.6	0.6	1.4	0.5	2.0
TOTAL	1248	13. 業務用 機械器具 製造業	14. 電子部品・ デバイス・ 電子回路 製造業	15. 電子応用 装置・ 電気計測器 製造業	16. 15以外の 電気機械 器具 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
		1.6	4.2	1.0	2.4	0.6	2.8	1.0	7.1	1.9	1.8	0.0	12.5
			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
			1.8	0.3	4.1	9.3	5.4	3.6	2.9	2.1	12.3	0.2	2.1

（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。

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。（図表３２参照）

図表３２．所属企業の常用雇用者数

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



以後、各改善策についてのアンケート調査結果を基に、改善策に対する取組の現状がどうなっているかを確認し、抽出する。なお、次頁以降で参照する抽出結果の内、現状を説明するものについては該当箇所を二重鉤括弧『』で括って示している。また、比率の読み取りに際しては、

70%以上を「大半」、30%未満を「少数派」と表現するものと定める。

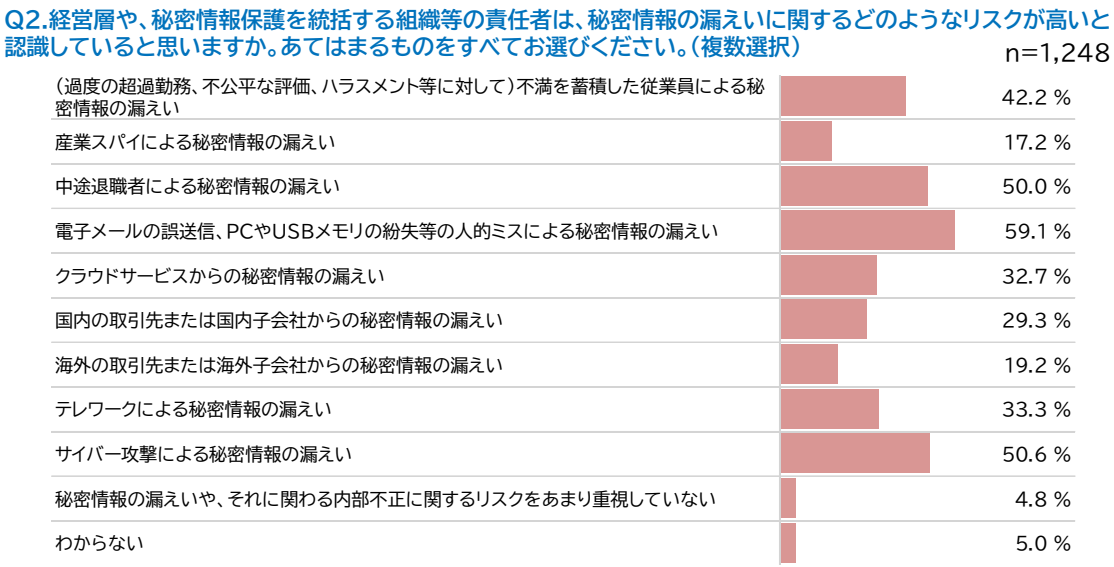
②経営課題の改善（調査軸１）

改善策 1-1 に関する現状

【1-1】法務・知財部門（社外の法律相談サービスを含む）の協力を得る等の取組を検討して、営業秘密等の漏えい事件（事例）から、事業リスクとしての重要性や当事者がしてはならないこと等を率先して学ぶ。

秘密情報の漏えいについて懸念されるリスクの上位３つは、「誤送信／可搬媒体の紛失（不注意、ミス）」（59.1%）、「サイバー攻撃」（50.6%）、「中途退職者の悪意」（50.0%）となっており、『過半の経営層や責任者は内部不正とサイバー攻撃の両方を危惧している』様子を見て取ることができる。（図表３３参照）

図表３３．秘密情報漏えいに関するリスクの認識状況



改善策 1-2 に関する現状

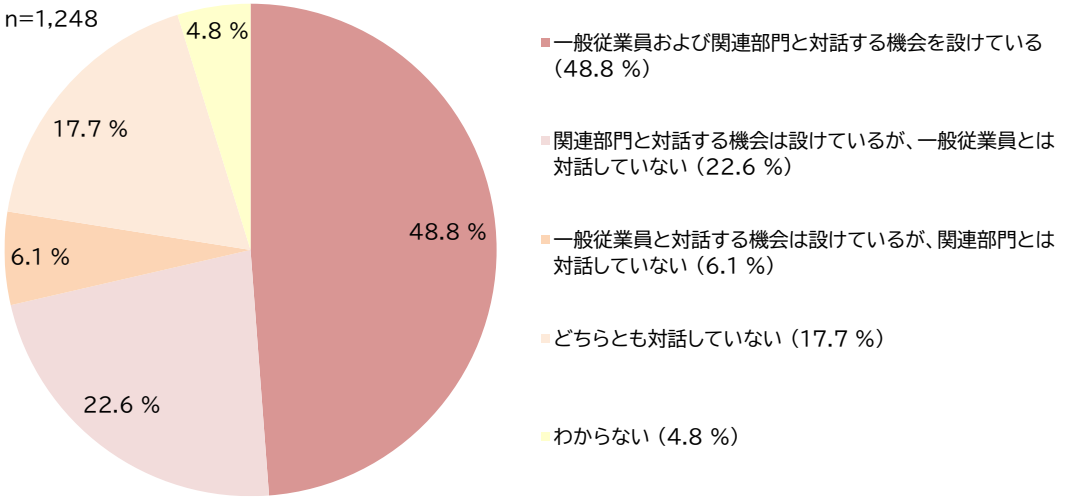
【1-2】経営層によるセキュリティ確保のリーダーシップ発揮の機会／場を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。

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

の発信を行っている』と考えられる。（図表３４参照）

図表３４．経営層がリーダーシップを発揮する機会／場の活用状況

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

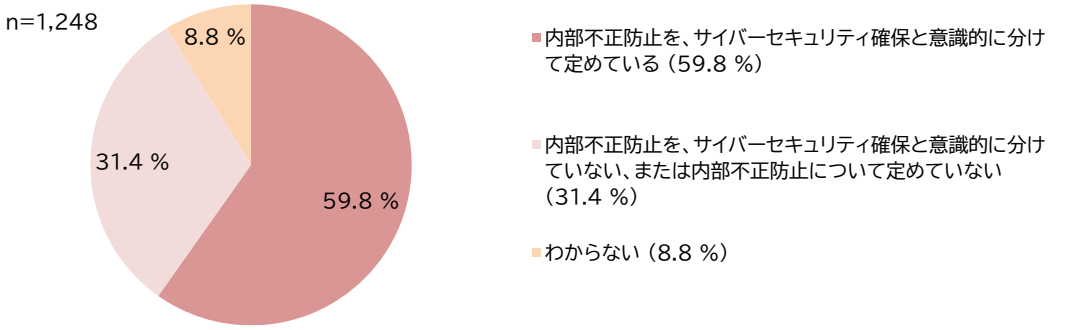


（注5）例えば、会社等への不満・鬱憤をきっかけとした秘密情報の開示・漏えい、離職前の秘密情報持ち出し・転職先での利用、不注意による秘密情報の社外送信／公開・記録媒体の紛失等がある。

内部不正防止の取組とサイバーセキュリティ確保を基本方針において意識的に分けて定めている企業の割合は 59.8%に達しており、『内部不正防止に特有の取組の必要性を認識している企業は過半を占める』と言える。（図表３５参照）

図表３５．基本方針における内部不正防止とサイバーセキュリティ確保の取扱状況

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

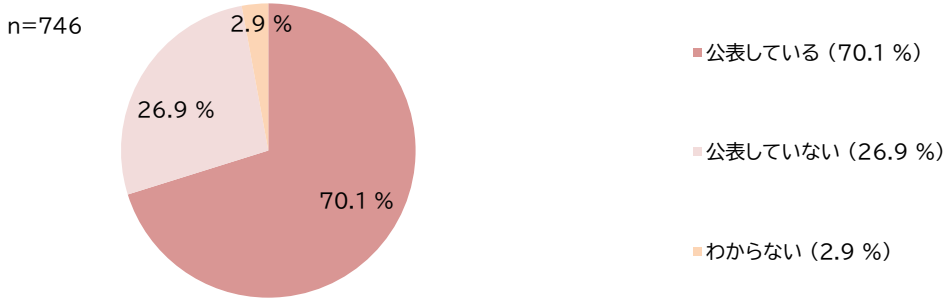


内部不正防止の取組とサイバーセキュリティ確保を基本方針において意識的に分けて定めている企業の 70.1%がこの基本方針を公表している。また、当該基本方針を公表している企業の

74.4%がその理由を経営の透明性確保するためであると回答している。『内部不正防止に意識的に取り組む企業の過半は経営の透明性確保にも関心を持っている』と言える。（図表３６、３７参照）

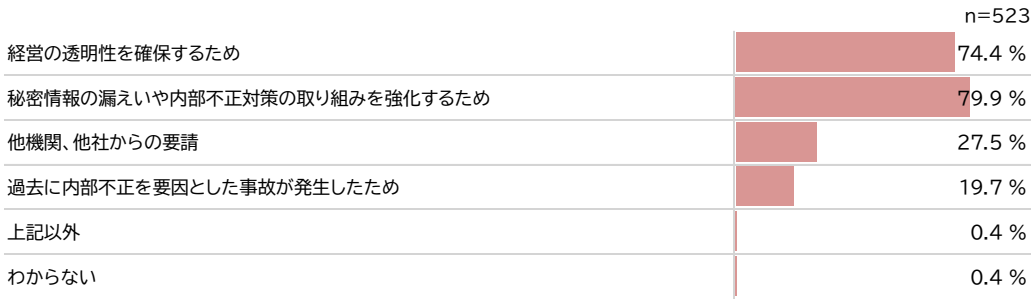
図表３６．内部不正防止について定めた基本方針等の公表状況

（Q4.で「1. 内部不正防止を、サイバーセキュリティ確保と意識的に分けて定めている」と回答した方に伺います。）
Q5.経営層は、内部不正防止について定めた基本方針等を公表していますか。
あてはまるものを1つお選びください。（単一選択）



図表３７．基本方針等を公表した理由

（Q5.で「1.公表している」と回答した方に伺います。）
Q6. 基本方針等の公表に至った理由は何だと思いますか。あてはまるものをすべてお選びください。（複数選択）



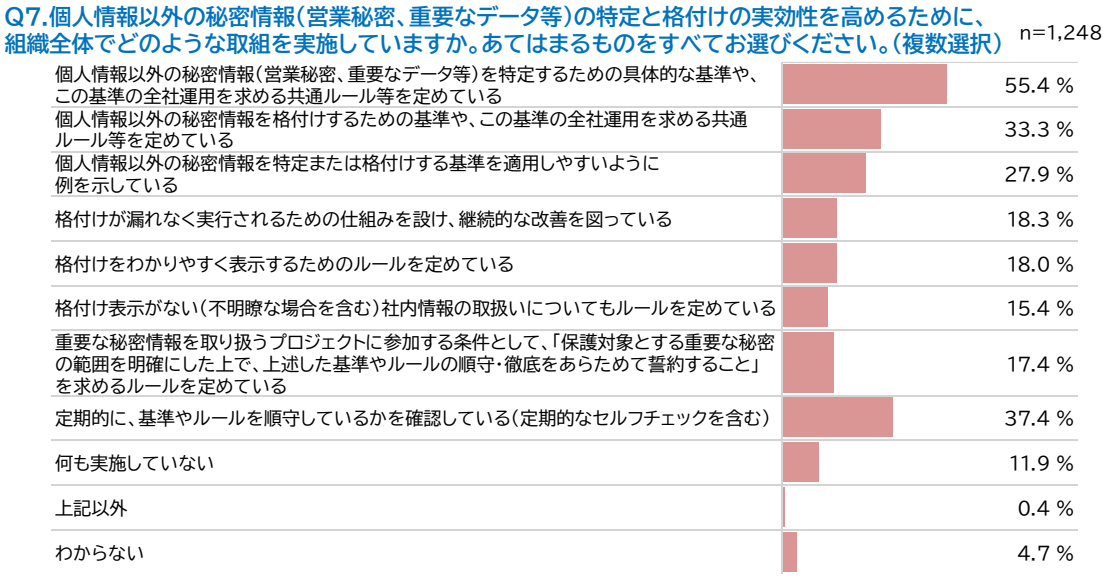
③重要な秘密の特定と取扱いの改善（調査軸２）

改善策 2-1 に関する現状

【2-1】経営層も積極的に関与して、事業リスクが高い（漏えいした場合のインパクトが大きい）営業秘密等を特定するための基準作り、従業員の営業秘密に対する対策意識の醸成、営業秘密の定期的な見直し等に取り組む。

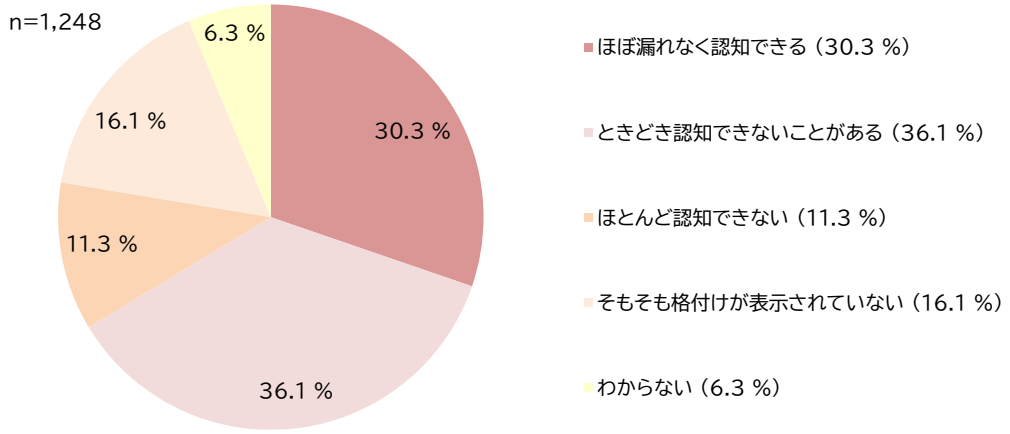
個人情報以外の秘密情報を特定するための具体的な基準や、その基準の全社運用を求める共通ルール等を定めている企業が 55.4%に達している一方で、秘密情報の格付けに関するルールを定めている企業は 33.3%に留まり、格付けの表示に関するルールを定めている企業は18.0%と更に少ない。『過半の企業でルール作りが行われている一方で、格付け表示にまで至っている企業は少数派である』と言える。従業員が秘密情報を目にした際にそれが秘密情報であるとほぼ漏れなく認知できると回答した企業は 30.3%しかなく、『秘密情報が不正に取り扱われている時に周囲の従業員が気付いて通報できる職場環境にある企業は少数派である』と言える。（図表３８、３９参照）

図表３８．秘密情報の特定と格付けの実効性を高めるための取組の実施状況



図表３９．秘密情報の格付け表示の実効性の状況

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



④組織体制・連携に関する課題の改善（調査軸３）

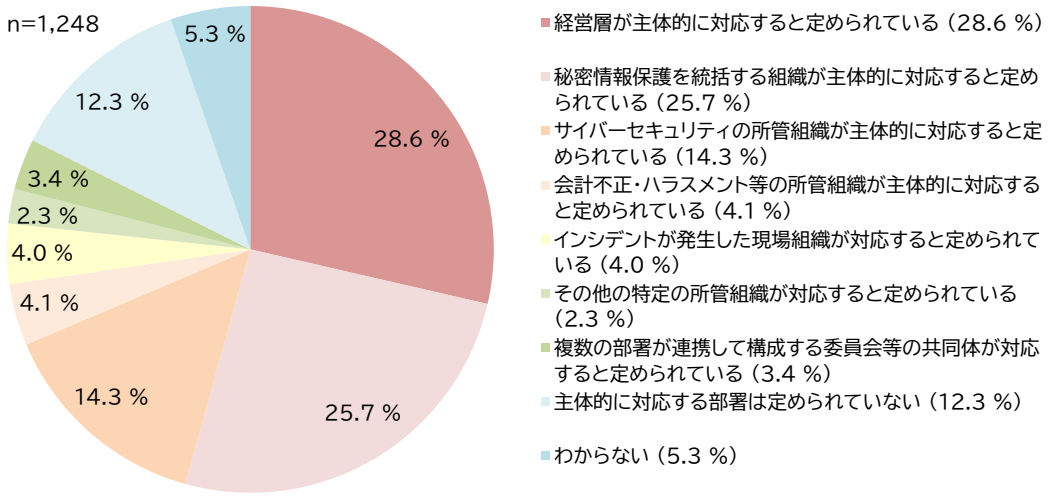
改善策 3-1 に関する現状

【3-1】責任部門自体（リスク・コンプライアンス部門等）と関連部門（情報システム部門：対策実施部門、法務・知財部門、営業・事業部門）が協働する体制の整備を検討する。

内部不正への対応についての責任の所在が定められている企業は 82.4%を占め、『大半の企業で内部不正防止の責任の所在が定められている』と言える。中でも、経営層が主体的に対応する企業と最大の割合（28.6%）を占め、次いで、秘密情報保護を統括する組織が主体的に対応する企業の割合（25.7%）が大きかった。（図表４０参照）

図表４０．内部不正防止における責任・権限の取り決め状況

Q9.「秘密情報の漏えいに繋がる内部不正」(注5)が発生した際に、
誰が主体的に対応するかが、社内規程等で定められていますか。あてはまるものを1つお選びください。(単一選択)



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

『責任部門と他組織の連携においては、過半の企業で、連携先からコンプライアンス・ガイドライン等の知識を補うことを目的としている』（53.6%）。その次に求められているのは、不正を生みにくい組織環境、内部通報制度等の整備ノウハウを補うことである（43.4%）。個人情報以外の秘密情報の事業価値を評価することを目的とする企業の割合は 34.9%に留まる。（図表４１参照）

図表４１．内部不正に対応する組織の連携状況

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

n=1,248

コンプライアンス・ガイドライン等の知識を補うため	53.6 %
個人情報以外の秘密情報の事業価値を評価するため	34.9 %
不正を生みにくい組織環境、内部通報制度等の整備ノウハウを補うため	43.4 %
中途退職／採用時の秘密保持義務、競業避止等に関するノウハウを補うため	25.9 %
リスクマネジメント、BCP、レジリエンス確保等の経験・ノウハウを補うため	34.1 %
サイバーセキュリティ確保、IT機器の操作ミス防止等の経験・ノウハウを補うため	30.0 %
他の組織と連携する必要はない	7.1 %
わからない	7.7 %

改善策 3-3 に関する現状

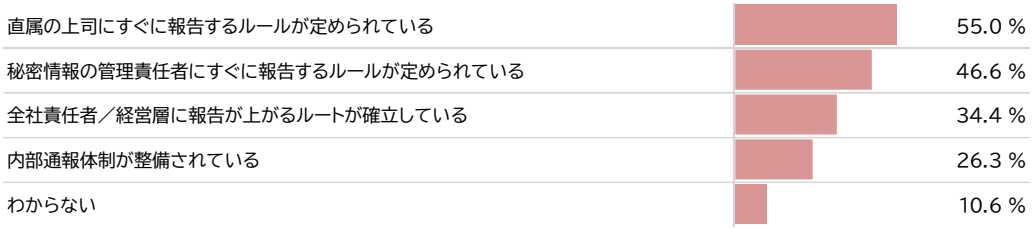
【3-3】重要な秘密が不自然に取り扱われているところを目にしたら、上に報告するというリテラシーと、上に報告できない事情がある場合は内部通報ができる体制を構築する。

秘密情報の不自然な取扱いや社外への不正な漏えいを目撃した際に、直属の上司にすぐに報告するルールを定めている企業が 55.0%を占め、秘密情報の管理責任者に報告することを定めている企業は 46.6%となっている。全社責任者／経営層に報告が上がるルートが確立している企業は 34.4%と相対的に少なく、内部通報体制を整備している企業は 26.3%と更に少ない。『不正の通報先としては上司が直属の上司が第一で、経営層までのエスカレーションルートがある企業は半分に満たず、内部通報体制がある企業は少数派である』と言える。（図表４２参照）

図表４２．内部不正を目撃した際の内部通報体制の構築状況

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

n=1,248



⑤社員教育とリテラシー構築に関する課題の改善（調査軸４）

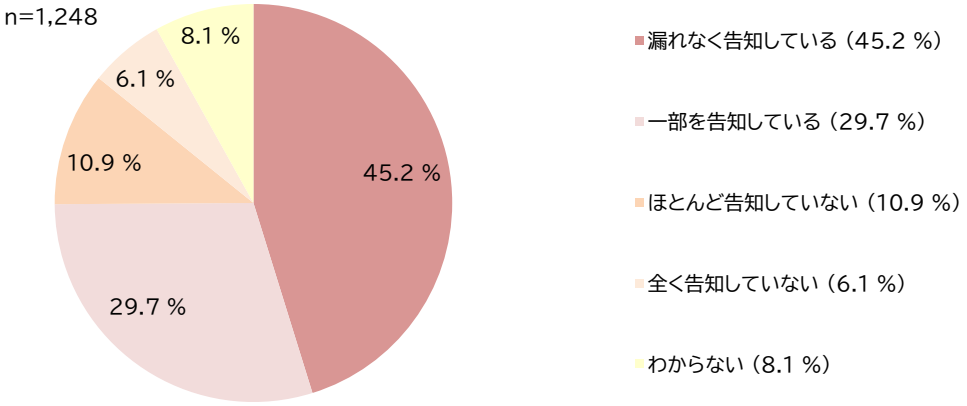
改善策 4-2 に関する現状

【4-2】入社／人事異動／退職等の重要なタイミングで、具体的に重要な秘密を示して、何をしてはいけないのか、どのような時に上への報告が必要か等を周知・徹底する。

社内で発生した秘密情報漏えい／内部不正の事実を社内に告知している企業は 74.9%に上る。問題事案であればこそ社内に告知しているのだから、『社内での事件発生時には、その告知内容を通じて、何をしてはいけないのか・何が問題となるのかということを、大半の企業が社内に周知している』と言える。（図表４３参照）

図表４３．秘密情報の漏えい、その要因となった内部不正の社内告知状況

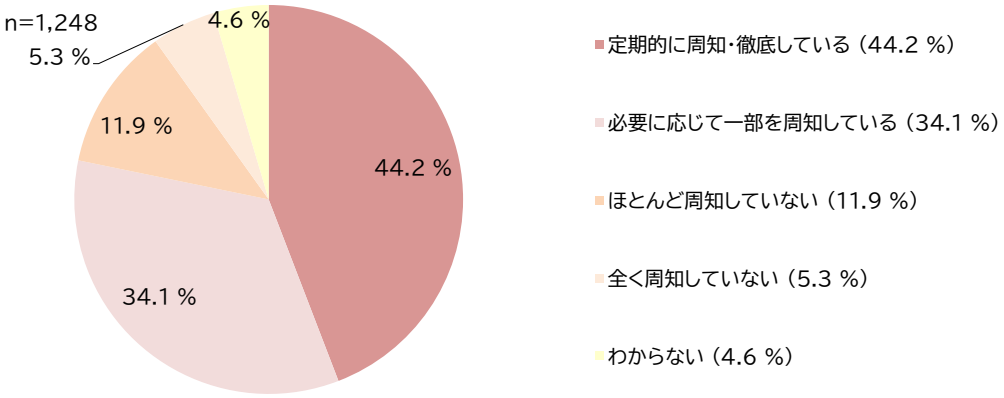
Q13.経営幹部の不正も含めて、社内で発生した秘密情報漏えいや、
その要因となった内部不正の事実を社内に告知していますか。あてはまるものを1つお選びください。（単一選択）



秘密情報の不自然な扱いや社外への不正な漏えいを目撃した際の適切な行動を、定期的に周知・徹底している企業は 44.2%と半分近くあり、必要に応じて一部を周知している企業も合わせれば、78.3%の企業がその周知に取り組んでいる。『大半の企業において、秘密情報の不自然な扱いや社外への不正な漏えいを目撃した際の適切な行動が周知されている』と言える。（図表４４参照）

図表４４．秘密情報の不自然な取扱い等を目撃した際の適切な行動の周知状況

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



改善策 4-3 に関する現状

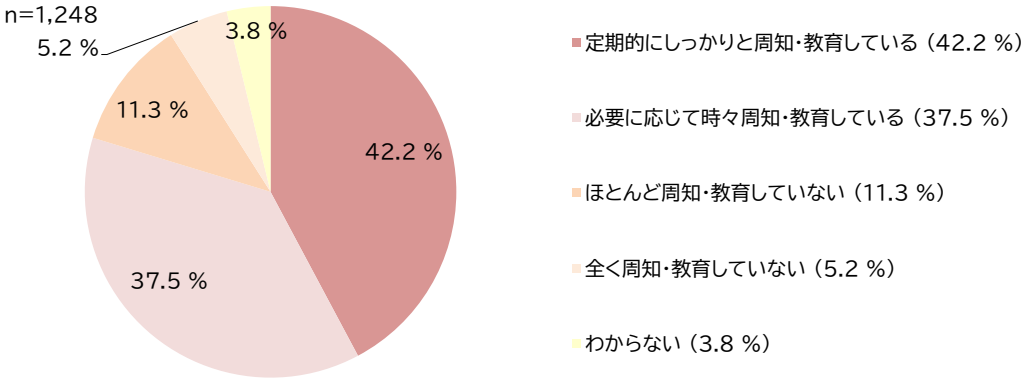
【4-3】事業や経営における重要性や価値、当該情報が漏えい・毀損等した場合の影響・損害などを踏まえた、秘密の重要度の判別基準を明文化した上で、この基準に基づくラベリング等を

行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。

営業秘密等の保護が個人情報保護と同じように重要であることを定期的にしっかりと周知・教育している企業は 42.2%を占め、必要に応じて時々そうしている企業は 37.5%となっている。両者を合わせると 79.7%となり、『大半の企業において、営業秘密等の保護が個人情報保護と同じように重要であることを周知・教育している』と言える。（図表４５参照）

図表４５．個人情報以外の秘密情報の重要性の周知状況

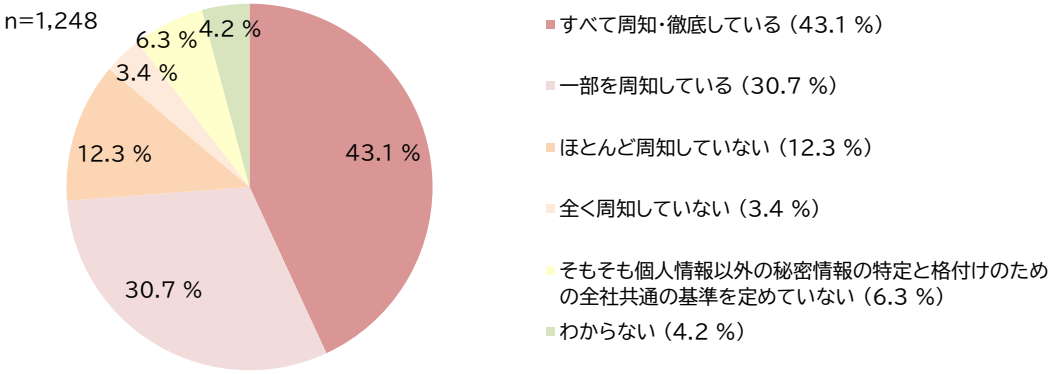
Q14.貴社では、個人情報以外の秘密情報（営業秘密、重要なデータ等）の保護が、個人情報保護と同じように重要であることを周知・教育していますか。あてはまるものを1つお選びください。（単一選択）



営業秘密等の特定と格付けのための全社共通の基準のすべてまたは一部を、社員教育等で全従業員に周知している企業は 73.8%を占める。『大半の企業において、営業秘密等の特定と格付けのための基準を周知・教育しているが、定期的に取り組めている企業は半分に満たない』と言える。（図表４６参照）

図表４６．秘密情報の特定と格付けのための全社共通の基準に関する周知状況

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



改善策 4-5 に関する現状

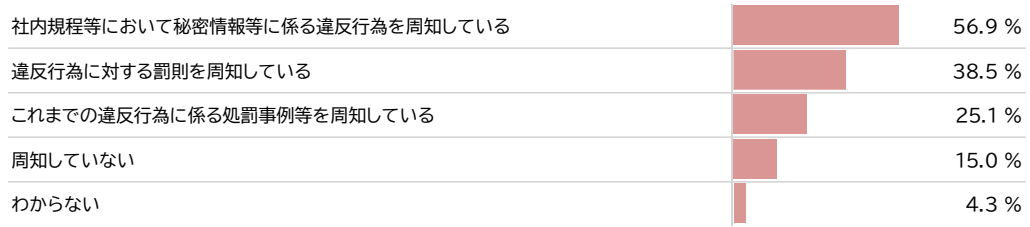
【4-5】インシデント事例、解説動画・イラスト等のリッチコンテンツ、グループディスカッション、定期的な規則遵守のセルフチェック等を積極的に活用して理解を深める取組を推進すると共に、従業員に対し、営業秘密や限定提供データについて、何をしてはいけないのかを教育する。

営業秘密や重要なデータ等の漏えいや内部不正に関する違反行為を従業員に周知している企業は 56.9%に上るが、罰則を周知している企業は 38.5%に留まる。『営業秘密等の漏えいや内部不正に関し、過半の企業において違反行為が示されているが、罰則までも明確である企業は相対的に少ない』と言える。（図表４７参照）

図表４７．秘密情報の漏えい、内部不正に関する禁止事項、罰則等の周知状況

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

n=1,248

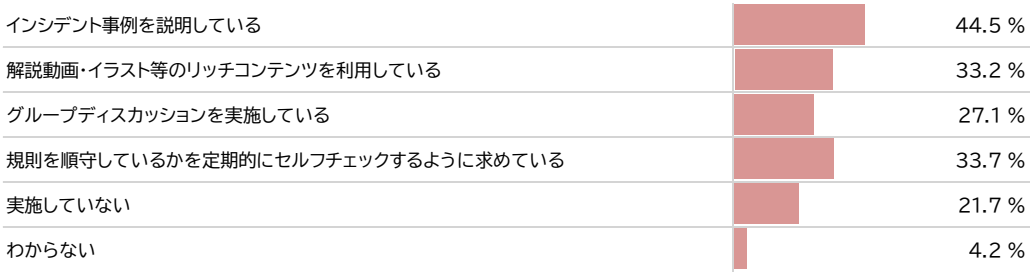


e-Learning 以外の方法を実施している企業は 74.1%に上る。具体的な方法としては、インシデント事例の説明を 44.5%の企業が行っている他、定期的なセルフチェックは 33.7%、リッチコンテンツの利用は 33.2%、グループディスカッションは 27.1%となっている。選択肢の構成上、他の実施内容は判然としないが、『大半の企業において e-Learning 以外の方法を実践に取り入れている』と見られる。（図表４８参照）

図表４８．e-Learning 以外の方法による内部不正防止等の従業員教育の実施状況

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

n=1,248



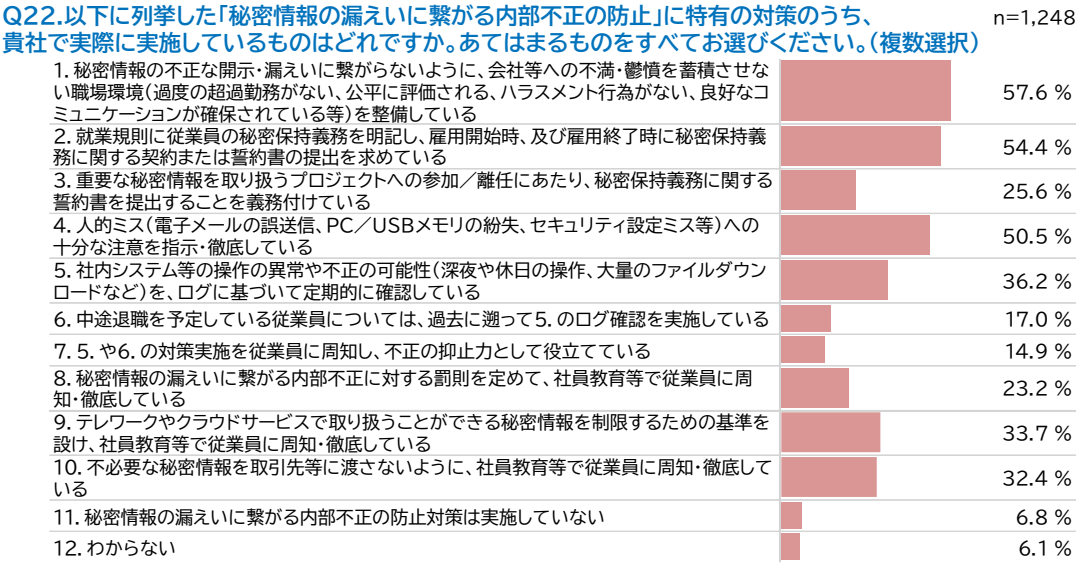
⑥対策実施に関する課題の改善（調査軸５）

改善策 5-3 に関する現状

【5-3】重要情報漏えい防止体制の下で、サイバーセキュリティ対策と内部不正防止対策の両方に一貫して取り組む。

過半の組織で実施されている内部不正防止に特有の対策は、不満・鬱憤を蓄積させない職場環境の整備（57.6%）、雇用開始・終了時の秘密保持義務契約／誓約書提出（54.4%）、人的ミスへの十分な注意の指示・徹底（50.5%）である。他の対策で実施割合が４割を超えるものはなく、『快適な職場環境の整備、秘密保持義務の明文化、徹底した注意喚起という３つの取組が、内部不正防止に特有の対策として一般的である』と見られる。（図表４９参照）

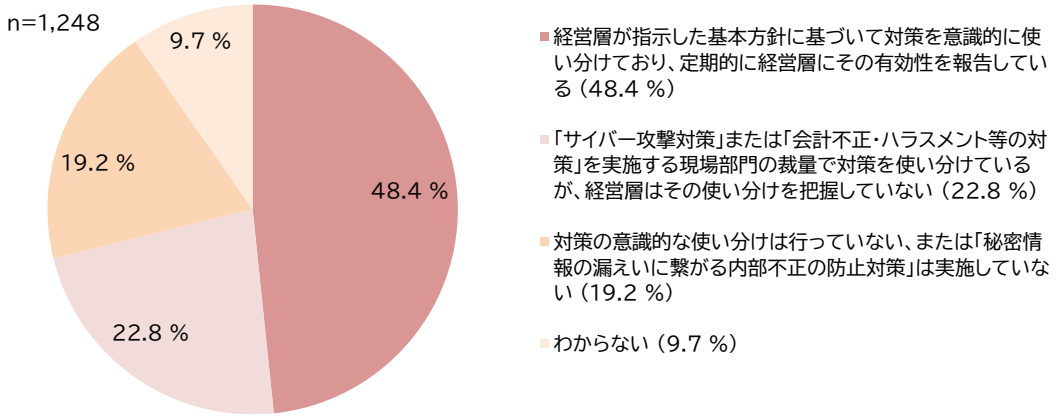
図表４９．内部不正防止に特有の対策の取組み状況



サイバー攻撃対策や会計不正等への対策と内部不正防止対策とを、経営層が示した基本方針に基づいて意識的に使い分け、更に定期的に経営層にその有効性を報告している企業は48.4%に上る。経営層の把握していない現場組織の裁量の範囲でこの使い分けを行っている企業も約 22.8%存在する。全体として、『大半の企業において内部不正防止対策とサイバー攻撃対策や会計不正等の対策とを使い分けている』と言える。（図表５０参照）

図表５０．内部不正防止対策とサイバー攻撃対策等の使い分けの状況

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



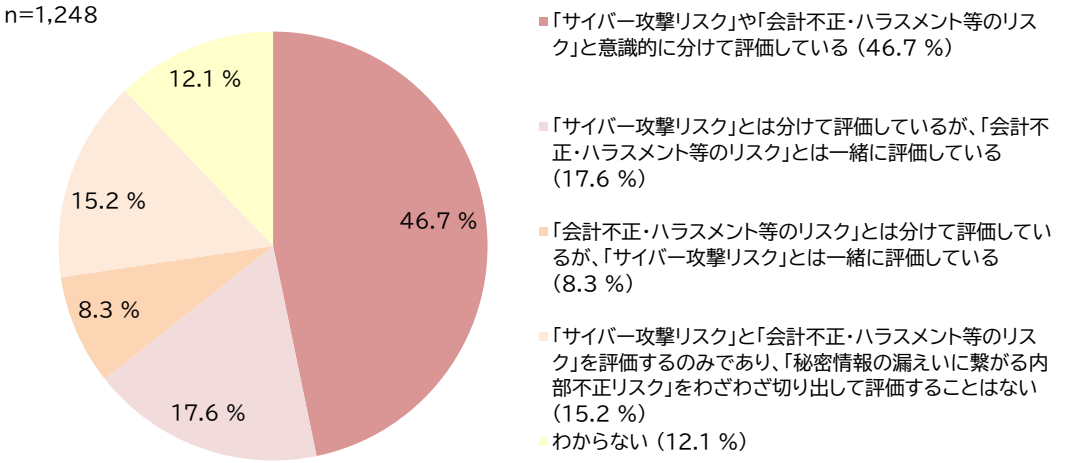
改善策 5-4 に関する現状

【5-4】 内部不正のリスクシナリオも加味して重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。この際には、不正に対する人的・組織的対策と技術的対策のバランスの適正化を考慮する。また、経営層の不正防止と透明性確保、アクセスログの確認範囲拡大、他社の重要情報の不正な社内持ち込み防止、重要プロジェクト就任／離任時にも秘密保持義務の誓約書を取得、重要性の高い秘密に触れる場合の誓約書の詳細度の変更等を実施する。

内部不正リスクをサイバー攻撃リスクとも会計不正等のリスクとも別に評価している企業の割合は 46.7%である。サイバー攻撃リスクや会計不正等のリスクと一体に扱いはするものの、内部不正リスクを意識して評価する企業は 25.9%あり、『大半の企業で内部不正リスクをそれと意識して評価している』と見られる。（図表５１参照）

図表５１．内部不正防止リスクの評価の実施状況

Q21.「秘密情報の漏えいに繋がる内部不正(注5)リスク」を、「サイバー攻撃リスク」や「会計不正・ハラスメント等のリスク」と意識的に分けて評価していますか。あてはまるものを1つお選びください。(単一選択)



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

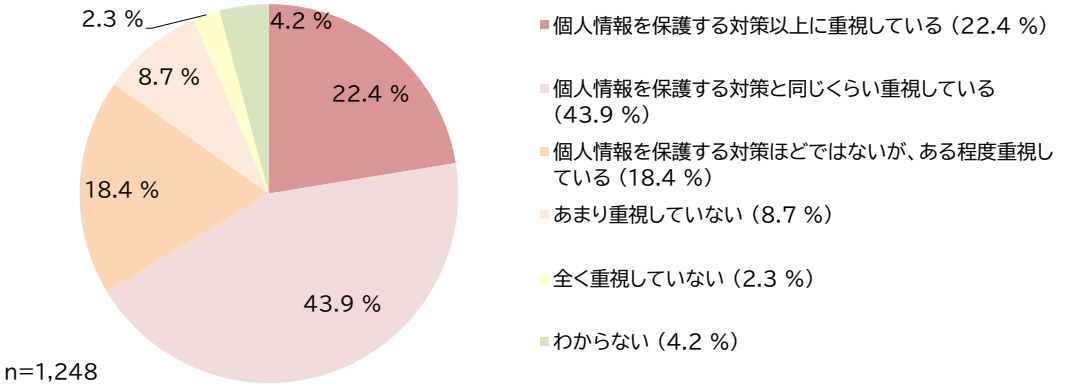
改善策 5-5 に関する現状

【5-5】個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。

営業秘密等を個人情報と同等あるいはそれ以上に重視している企業の割合は 66.3%に達している。『過半の企業において営業秘密等を個人情報と同等以上に重視している』と言える。（図表５２参照）

図表５２．個人情報以外の秘密情報を保護する対策の重視状況

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



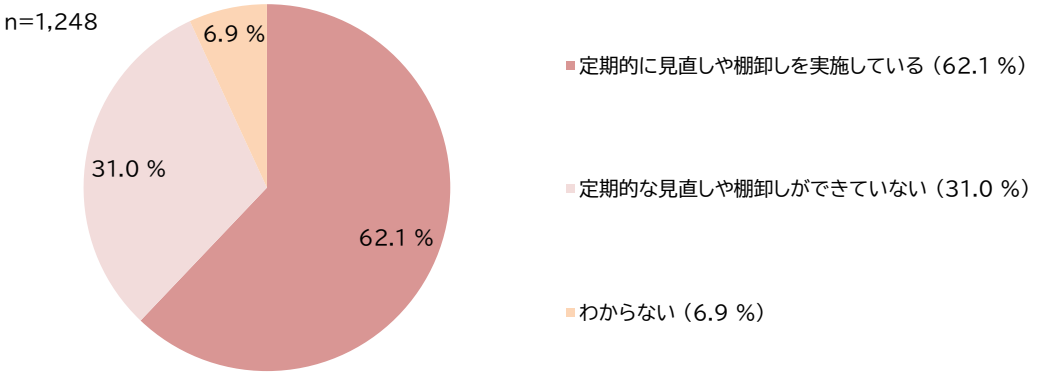
改善策 5-6 に関する現状

【5-6】情報機密区分に応じたアクセス権限付与状況の点検、アクセス権限付与者についての定期的な棚卸しを実施する。

機密性の高い重要な秘密情報へのアクセス権の定期的な見直し・棚卸しを実施している企業は 62.1%を占める。『機密性の高い秘密情報については過半の企業が管理の定期的な見直し・棚卸しに取り組んでいる』と言える。（図表５３参照）

図表５３．秘密情報管理の棚卸しの実施状況

Q19.機密性の高い重要な秘密情報へのアクセス権の定期的な見直しや棚卸し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）



⑦中小企業の構造的課題の改善（調査軸６の１～５）

アンケート調査の単純集計では、中小企業に特化した分析は実施していない。

⑧ガイドラインの利用と実践に関する課題の改善（調査軸７）

ここでは、企業アンケート調査結果を用いて、調査軸 7：ガイドラインの利用と実践に関する課題の改善において整理した改善策と現状の比較を試みた。

改善策 7-1 に関する現状

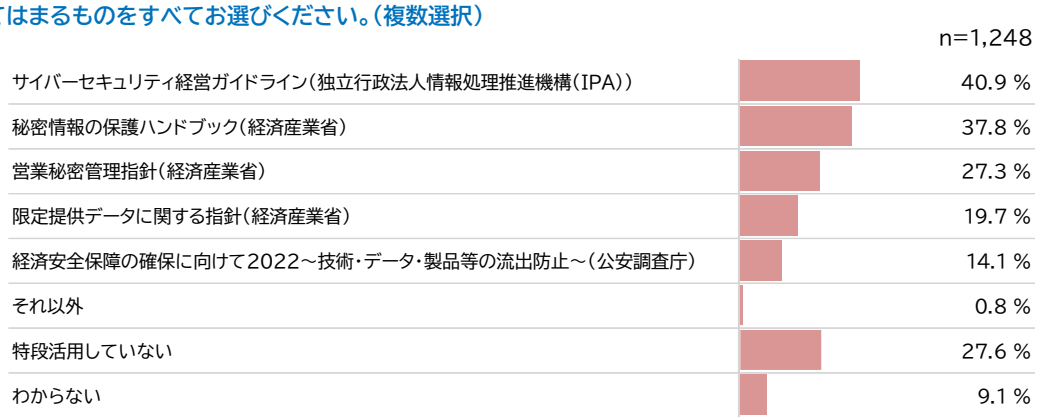
【7-1】認知度・活用度合の高い「サイバーセキュリティ経営ガイドライン」「秘密情報の保護ハンドブック」「営業秘密管理指針」「限定提供データに関する指針」「経済安全保障の確保に向けて 2022～技術・データ・製品等の流出防止～」との相互参照を進める。また、支援ツール開発

や外部専門家派遣による適用開始支援等を検討する。

経済産業省のガイドライン（サイバーセキュリティ経営ガイドライン、秘密情報の保護ハンドブック）も参考にするという回答が 40%前後あることを考慮し、これらとの相乗効果を狙って、相互参照を進めることも一案である。（図表５４参照）

図表５４．「組織における内部不正防止ガイドライン」以外に参考としている資料

Q25.「組織における内部不正防止ガイドライン」以外に参考としている資料はありますか。あてはまるものをすべてお選びください。（複数選択）



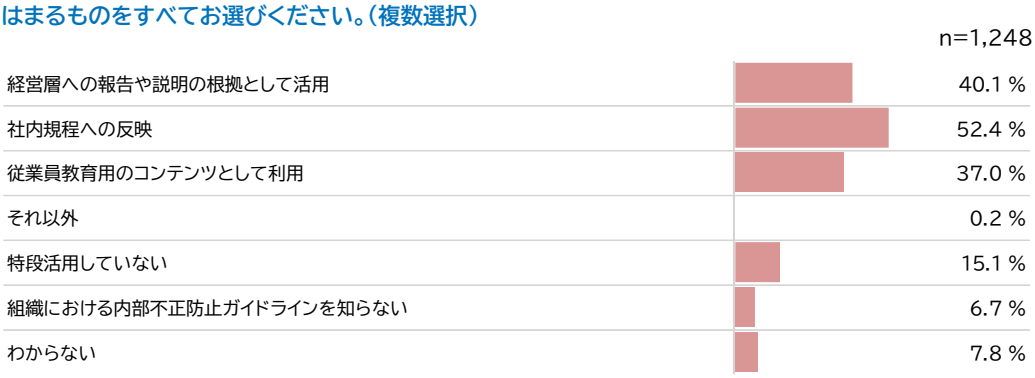
改善策 7-2 に関する現状

【7-2】概要版の作成、活用しやすい情報量の調整・表現の工夫、社内規程整備のために活用しやすい内容の増補、従業員への周知・教育にそのまま使えるコンテンツの充実等を検討し、「組織における内部不正防止ガイドライン」適用の実効性を高める。

ガイドラインは、社内規程への反映に最も多く活用されており（約 52%）、経営層への説明の根拠（40%）、従業員教育用のコンテンツ（37%）としての利用はまだあまり多くない。今後、従業員教育の教材として利用しやすい別添のコンテンツ（概要版、講義に活用できるスライド形式の説明資料、動画等）を追加することも一案と考える。（図表５５参照）

図表５５．「組織における内部不正防止ガイドライン」の活用状況

Q24.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」をどのように活用していますか。あてはまるものをすべてお選びください。（複数選択）



(3) 企業と有識者のインタビュー調査結果の整理・比較

ここでは、中小企業（8 社）及び有識者（4 名）に対するインタビュー調査の結果をそれぞれの調査軸ごとに取りまとめた。調査軸 1 ～ 5 および 7 では企業規模によらない改善策を整理して分析しているため、インタビュー調査結果としては有識者が企業規模によらず回答した内容だけを対象としてまとめている。一方、調査軸 6 は中小企業を対象とした改善策を整理して分析しているため、中小企業の経営者／経営幹部を対象としたインタビュー調査結果と、有識者が中小企業について回答した内容の両方を対象としてまとめている。各調査軸とインタビュー調査結果の関係を図表５６に示す。

図表５６．調査軸とインタビュー調査の関係

見出し	調査軸	中小企業調査結果	有識者インタビュー結果	
			企業規模によらない回答	中小企業についての回答
①　全体的な課題の改善	1	—	○	—
	2	—	○	—
	3	—	○	—
	4	—	○	—
	5	—	○	—
②中小企業の構造的課題の改善	6	○	—	○
③ガイドラインの利用と実践に関する課題の改善	7	—	○	—

以下、各調査軸に属する改善策について、インタビューから見出された現状、好事例、示唆を列記する。なお、インタビュー対象となった中小企業は内部不正防止や情報漏えい対策に積極的な組織ばかりであり、以下に含まれる好事例は、こうした企業で実践されている模範的取組に

相当している。

①全体的な課題の改善（調査軸１～５）

経営課題の改善（調査軸１）

改善策 1-1 に関する調査結果

【1-1】法務・知財部門（社外の法律相談サービスを含む）の協力を得る等の取組を検討して、営業秘密等の漏えい事件（事例）から、事業リスクとしての重要性や当事者がしてはならないこと等を率先して学ぶ。

有識者の現状認識

- 無関心な経営層にいかに関心を持ってもらうかが課題である。

有識者が示した好事例

- 社外取締役弁護士等からの提起で、取締役会で秘密情報漏えい／内部不正防止について議論する機会を多く設ける。
- 有事の際の損害の大きさを示すリスクマップを活用し、秘密情報漏えいや内部不正が重大なリスクであるという経営層の認識を高める。リスクマップは大企業で作成が進んでいる。

改善策 1-2 に関する調査結果

【1-2】経営層によるセキュリティ確保のリーダーシップ発揮の機会／場を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。

有識者の現状認識

- 内部不正のリスクの大きさを見積もることが難しいため、予算やリソースが配分されにくい。
- 経営層に被害者意識が働くため取組が進みにくい。
- 経営層は内部不正リスクを軽視しがちであり、IT 担当役員が責任者になって社長が進捗報告を受けるような平常時に類する体制が選ばれ、取組も甘くなる傾向がある。

有識者による示唆

- 経営層等が自分の考えを全社に何度も伝え、その熱意が全社に浸透していれば、従業

員のあるべき行動に繋がっていく。
- 経営層の認識を「加害者でもありうる」というものに変革する必要がある。
- 秘密情報漏えい／内部不正防止とサイバーセキュリティは本来であれば目的が異なる取組なので、しっかりと対応するためには分けて進めるべきである。

重要な秘密の特定と取扱いの改善（調査軸２）

改善策 2-1 に関する調査結果

【2-1】 経営層も積極的に関与して、事業リスクが高い（漏えいした場合のインパクトが大きい）営業秘密等を特定するための基準作り、従業員の営業秘密に対する対策意識の醸成、営業秘密の定期的な見直し等に取り組む。

有識者が示した好事例

- 技術・事業・営業・取引等のノウハウについても、特定すべき重要な営業秘密として、価値を決めることが必要で、大企業ではこの問題意識を持つ担当者が育ってきている。

有識者による示唆

- 知らないうちに競合他社に持ち出されるくらいならば営業秘密をきちんと明確化しておこうという動機付けをするのがよい。
- 会社にとって有用な営業秘密をリストアップし、自分たちがやっている仕事がその保護に貢献していることが可視化されると、会社の重要な仕事に貢献しているという認識と満足感が浸透することを期待できる。

組織体制・連携に関する課題の改善（調査軸３）

改善策 3-1 に関する調査結果

【3-1】 責任部門自体（リスク・コンプライアンス部門等）と関連部門（情報システム部門：対策実施部門、法務・知財部門、営業・事業部門）が協働する体制の整備を検討する。

有識者の現状認識

- 大企業では、知財部門は「秘密情報の価値を決められるのは現場の事業部門である」と考えていることが多い。しかし、現場の事業部門に秘密情報の価値決めを任せてしまうと視野が狭くなり、部門間のばらつきが出るというリスクを抱えることになる。

有識者による示唆

- 大企業においては知財部門が全社のハブとなり、事業部門などの他の部門と確認を取り合いながら、秘密情報の価値を決めるとよい。

改善策 3-2 に関する調査結果

【3-2】対策を実施する情報システム部門が責任部門となる体制を取る場合は、知財・法務部門等と協力してガバナンスを確保する。

有識者の現状認識

- 情報システム部門の意見やリスク認識が経営層に適切に伝わらないという問題が企業規模に関わらず生じており、情報システム部門が秘密情報の漏えい／内部不正防止の全社責任を負う上での重要な障害になっている。
- 情報システム部門は法律・知財に関する知識が十分でないため、技術的な取組が中心となってしまい、人的・組織的取組に漏れが生じる恐れがある。

改善策 3-4 に関する調査結果

【3-4】役職の高い者を特別扱いしないマネジメントシステムを構築し、体制を整備する。

有識者による示唆

- 経営者がまず原則を示し率先してこれを指示した上で、経営層に対する監督強化、内部統制システムの構築、意思決定の透明性確保、倫理意識の醸成、内部通報制度の整備、定期的なリスク評価と対策改善に取り組む必要がある。
- 役職の高い者を特別扱いしないマネジメントの確立には、経験とノウハウの蓄積も必要である。

社員教育とリテラシー構築に関する課題の改善（調査軸４）

改善策 4-1 に関する調査結果

【4-1】法務・知財部門の協力を得た教育・研修等によって、対策を担当する情報システム部門の重要情報漏えい／内部不正に関する法知識（不正競争防止法等）の理解を深める。

有識者による示唆

- 営業秘密保護に係る制度（不正競争防止法）については、営業秘密侵害は刑事罰が非常に厳しいこと、両罰規定で会社も罰せられるリスクがあることという 2 点が重要なので、経営層をはじめとして、情報システム担当者やその他の従業員にこの事実を教育・警告すべきである。

参考情報：転職時の営業秘密侵害事案で両罰規定が適用されるのは、転職者のみならず転職先企業の他の役員・従業員の関与が認められた場合である。実際に両罰規定が適用された事例は多くないが、最近これが認められた事案があった。（両罰規定で会社が罰せられた最近の事件としては、カッパ・クリエイト社の前社長がはま寿司の営業秘密を不正に入手・利用したとして不正競争防止法違反の罪に問われた事件がある。この事件では、法人のカッパ・クリエイト社も不正競争防止法の両罰規定で起訴されており、2024 年 2 月 26 日に東京地裁は同社に求刑通り罰金 3,000 万円の有罪判決を言い渡している。転職時の営業秘密侵害事案で両罰規定が適用されるのは、転職者のみならず転職先企業の他の役員・従業員の関与が認められた場合であり、本件ではカッパ・クリエイト社の商品企画部長（当時）が関与したと認められたことによる（元商品企画部長も不正競争防止法違反で有罪判決）。その後、カッパ・クリエイト社と元商品企画部長は判決に不服があるとして共に控訴した。）

改善策 4-2 に関する調査結果

【4-2】 入社／人事異動／退職等の重要なタイミングで、具体的に重要な秘密を示して、何をしてはいけないのか、どのような時に上への報告が必要か等を周知・徹底する。

有識者の現状認識

- 従業員に少しでもリスクに気付いて貰えていれば被害を防ぐことができた事例が多い。

有識者による示唆

- 従業員には、営業秘密や重要なデータ等の漏えいがどの程度の損害を生じるのかを教育し、広く認識してもらうことが重要である。
- 従業員のリテラシー欠如、法令やガイドラインに対する無知は内部不正に含まれるという認識を、事例と共に従業員に周知教育すべきである。同時に、基本的な取組の重要性や、法令・ガイドラインを周知できていない経営層にも責任がある。
- ログをきちんと取得して確認していることを社内に通知する、起こった事例を包み隠さず企業内に周知する、罰則を設けてこれを周知する等が有効である。

改善策 4-3 に関する調査結果

【4-3】 事業や経営における重要性や価値、当該情報が漏えい・毀損等した場合の影響・損害などを踏まえた、秘密の重要度の判別基準を明文化した上で、この基準に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。

有識者の現状認識

- 大企業であっても、重要度を判別する基準を決めて教育するところまでは至っていない企業が多い可能性がある。

対策実施に関する課題の改善（調査軸５）

改善策 5-3 に関する調査結果

【5-3】 重要情報漏えい防止体制の下で、サイバーセキュリティ対策と内部不正防止対策の両方に一貫して取り組む。

有識者による示唆

- 広い視野で見ればサイバーセキュリティ対策と内部不正防止対策の観点は同じであり、サイバーセキュリティと内部不正防止で共通の対策は適用しつつ、守るべきものとリスクの違いに合わせて足りないところを補っていけばよい。

改善策 5-4 に関する調査結果

【5-4】 内部不正のリスクシナリオも加味して重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。この際には、不正に対する人的・組織的対策と技術的対策のバランスの適正化を考慮する。また、経営層の不正防止と透明性確保、アクセスログの確認範囲拡大、他社の重要情報の不正な社内持ち込み防止、重要プロジェクト就任／離任時にも秘密保持義務の誓約書を取得、重要性の高い秘密に触れる場合の誓約書の詳細度の変更等を実施する。

有識者の現状認識

- 不満を持つ従業員が秘密情報を漏えいさせるケースでは、欲しい秘密に的を絞って狙ってくるので、対応が難しいことがある。
- 継続中の事業に係る漏えいリスクは、楽観論から「不正をする担当者はいない」と思いた

い心理が働きやすい。

有識者による示唆

- 秘密情報漏えいの事業リスクアセスメントは、本来プロジェクトごとに実施すべきである。
- 秘密情報が漏えいすると企業の存続すら危うくしうるという危機感を持ち、対策にリソースを投入すべきである。

改善策 5-5 に関する調査結果

【5-5】個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。

有識者の現状認識

- どちらが良いというものではないが、大企業は、資金や人員が潤沢であるため、秘密情報漏えいが起きない体制作りに注力する企業と、（資金や人員には限界があり漏えいが発生することは避けられないとの考えから）秘密情報漏えいの早期発見に注力する企業とに、二分できる。

②中小企業の構造的課題の改善（調査軸６の１～５）

中小企業の課題改善については、有識者に加えて、中小企業の経営者または秘密情報管理／情報セキュリティの主担当者にインタビューを行い、その実態、認識、意見等を聴取した。

経営課題の改善（調査軸６の１）

改善策 6-1-1 に関する調査結果

【6-1-1】経営層または内部不正防止に関する組織全体の責任者等が率先して、重要な秘密情報漏えい／内部不正リスクを重要な経営課題として認識する機会を増やし、サイバーセキュリティ確保と内部不正防止を一体的に認識した経営を行う。

中小企業の現状認識

- コロナ禍、働き方改革、人手不足などにより、経営課題として秘密情報の漏えい／内部不正防止の重要度がますます高まっている。

中小企業の好事例

- 業界の流れを意識し、技術情報管理の認証取得に取り組んだことが良い契機となった。
- 秘密情報との関りが深い事業を展開しているため自社でもしっかり取り組むことが必須だった。
- 悪意の有無に関わらず、人為的な秘密情報漏えいのリスクが高いと考えて経営している。

有識者の現状認識

- 中小企業では秘密情報漏えい／内部不正防止に関する意識の高い幹部がキーマンとなりうるが、こうした意識の高い幹部が少ない。

有識者による示唆

- 中小企業では経営層が高い意識を持って率先し牽引すれば会社全体の取組状況をがらりと変えられる可能性を持っている。
- 経営層が秘密情報の漏えいや内部不正防止について全社にしっかりと自分の経営方針を話していくことが望ましい。
- 中小企業では、営業秘密を社内できちんと保護する体制を構築することで、秘密情報漏えい／内部不正防止にも好ましい効果が生じる。

改善策 6-1-2 に関する調査結果

【6-1-2】中小企業では、全社集会などの経営層が従業員に周知徹底する機会を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。

中小企業の好事例

- 経営者が自ら基本方針を全社に周知・徹底している。
- 定期的にも日常的にも経営者が社員に語ることで意識付け・啓発に効果を上げている。
- 漏えいが自社の信頼失墜に直結することを強く認識して全社に周知・啓発している。
- 秘密情報漏えい／内部不正防止の取組が特に進んでいる中小企業では、情報漏えい／内部不正防止に関する基本方針を情報セキュリティポリシーとは完全に別建てで定めている。
- ISMS、プライバシーポリシー、技術情報管理等の認証取得が、中小企業の経営者が基本方針を定める契機となって取組が進んだ。
- 情報漏えい／内部不正防止に関する経営者の考えを全社に何度も繰り返し伝えることが重要であると認識し、経営者自ら実践している。

有識者の現状認識

- IT 関連のリスクに対する中小企業の対応状況はまだ十分でない。
- 自社で事件が発生するまで内部不正防止の体制整備に注力できない。
- 基本方針で秘密情報管理の重要性を明記している企業はあまり見られず、管理がなされていても部下に任せきりで経営層にとってリスクの所在がブラックボックスになっている。
- 経営者も従業員もお互いに直接顔が見えるため中小企業では性善説を前提とした管理になりがちである。

有識者による示唆

- 従業員と直接コミュニケーションを取って趣旨をしっかりと伝えることで、ある程度リスクに対応できる。
- 中小企業の取組強化に向けては、経営者が戦略を語り、コミットメントや指示に自身の想いやこだわりを込め、日々語ることが重要である。
- 経営層が何をどの程度重視しているかを率直に伝えることで、従業員がこれを評価して行動することを期待できる。
- 埋めるべきギャップは大企業より中小企業の方が小さいので、ひとたび良い方向に動き始めると、目標レベルに素早く到達できる。
- 中小企業の規模やリソースを考慮すると、秘密情報漏えい／内部不正防止とサイバーセキュリティを敢えて分けて取り組む必要はない。

重要な秘密の特定と取扱いの改善（調査軸６の２）

改善策 6-2-1 に関する調査結果

【6-2-1】 中小企業では、経営層が自ら判断する、あるいは判断基準を示すことで、自社の事業にとって重要性／機密性の高い秘密情報を的確に特定する。

中小企業の好事例

- 経営者が自ら事業リスクの判断や秘密情報の特定・格付けを行っている。
- 経営者が情報セキュリティや技術情報管理の認証取得を決断し、これに取り組んだことが契機となって、営業秘密等の特定、格付け、表示に関する体制整備が進んだ。
- 認証制度が要求する管理基準に従い、秘密情報を管理できる情報資産台帳を作成している。
- 認証制度に沿って特定した情報資産については、情報の保存場所や保存期間、データ消去の方法やリスクの大きさ、格付けを台帳管理している。

- 情報資産を保存する共有フォルダ等の場所を格付けに沿って切り分け、かつ、適切なアクセス制御・記録を合わせることで、格付け・表示・アクセス管理を一体に実施している。

中小企業による示唆

- 経営者の負担を避けるため、部下を育成し、権限移譲を考えることも必要である。

有識者の現状認識

- 紙に書かれた秘密情報の物理的管理がしっかりできていたとしても、電子化された秘密情報の管理はほとんどできていない中小企業が多い。

組織体制・連携に関する課題の改善（調査軸６の３）

改善策 6-3-1 に関する調査結果

【6-3-1】 中小企業では、責任者である経営層が中心となって、総務・人事・法務や情報システム等の関連部門との調整を行う。

中小企業の好事例

- 秘密情報漏えい／内部不正防止とサイバーセキュリティの担当役員を分け、監督も別々に実施し、経営者がこれを統括している。
- 経営者を責任者とする 3~5 名程度の幹部による委員会を設置している。その下にシステム、総務・人事、教育、内部監査等を担当する幹部が集まって委員会を構成する。具体的には、情報管理委員会を設けている例と、情報セキュリティ委員会を設けている例が見られた。
- 経営者が責任を担い、品質管理責任者が横串を通す形で、関連部門を連携させている。各種のマネジメントシステムを構築・運用する際に品質管理責任者が必ずこれに協力し、品質管理責任者を中心とした社内ネットワークを形成している。この属人的な社内ネットワークを活用し、情報管理、情報セキュリティ、内部統制、教育管理などの担当組織の間に、マネジメントシステムの運用を軸にして横串を通している。
- 秘密情報保護に関する重要な主題（秘密保持義務の誓約、懲罰、情報セキュリティ対応等）ごとに担当チームを組成し、各チームが基本方針を定めて取組を実施している。経営者はチーム全体の統括責任者となり、必要に応じて各チームと関連組織の協議を主導する。

有識者の現状認識

- 法務部門がない、または知財・法務に精通する経営層や幹部がいない中小企業では、法制度への対応や規程の制定／社内への浸透等が社長室や総務部門の雑多な業務の１つとして片手間で扱うことになりがちである。

有識者による示唆

- 社内に委員会を設けるなどして、複数部門が連携して取り組むことができる体制を検討することが望ましい。

改善策 6-3-3 に関する調査結果

【6-3-3】重要な秘密が不自然に取り扱われている様を目撃した際に上に報告することの徹底と、上に報告できない事情がある場合は内部通報ができる体制を構築する。

中小企業の好事例

- 秘密情報が漏えいした時や従業員がヒヤリハット・不信感を認識した時に、直属の上司を通じて経営者にすぐに報告が上がってくる仕組みを設けている。

有識者による示唆

- 中小企業は人間関係が良く性善説を基にしていることが多いので、内部通報ができる仕組みを構築すると逆に従業員の不信感が高まる恐れがあり、注意が必要である。

社員教育とリテラシー構築に関する課題の改善（調査軸６の４）

改善策 6-4-1 に関する調査結果

【6-4-1】中小企業では、経営層のリーダーシップと社外の専門家（ITコーディネータ、弁護士・弁理士等）の協力により、情報システム部門や他の従業員に法務・知財の知識を広める。

有識者による示唆

- 事業拡大に悪影響を及ぼしうることを考慮し、知財専門人材が社内にいない場合は業界団体等を通じて外部の専門職（弁護士・弁理士等）と連携することが望ましい。

改善策 6-4-2 に関する調査結果

【6-4-2】中小企業では、入社／人事異動／退職等の重要なタイミングで、経営層が重要な秘密を具体的に示し、その取扱い指示を徹底する。

中小企業の現状認識

- 中小企業では、他社で発生した事件の情報を収集することは難しい。経営者による情報収集は過大な負担ともなりうる。

中小企業の好事例

- 営業秘密・重要データの知識に関する社員教育にも取り組み、入社時のオリエンテーション、年 1 度の e-Learning や年 2 回の集合教育、全社集会の機会を活用した教育を行っている。
- リスクとその重要性、過去に発生した事例における重要なリスクと実際に発生した損害、社内で発生したヒヤリハットの経緯や内容等を伝えている。
- 退職時に秘密情報を持ち出すリスク、実際に持ち出した事例等に重点を置いて教育している。
- 中途退職時に禁止されている事項を教育している。
- 経営者が自ら参考事例等の情報を収集している。
- セキュリティ会社に委託し、他社で発生した事件の情報、注意点、セキュリティ管理の考え方等の情報を提供してもらっている。

有識者による示唆

- 中小企業には営業秘密の秘密管理性の確保が自己防衛及びビジネス拡大に不可欠であることを大企業以上に認識してもらうことが望ましい。

改善策 6-4-3 に関する調査結果

【6-4-3】経営層または経営層が権限を移譲した責任者が各々の秘密の重要度を指定した上で、この指定に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。

中小企業の好事例（再掲）

- 経営者が自ら事業リスクの判断や秘密情報の特定・格付けを行っている。

改善策 6-4-4 に関する調査結果

【6-4-4】企業のサイバーセキュリティ／コンプライアンス等に関する取組の一環として、重要情報漏えい／内部不正防止の社内規程及びその規則、モニタリングの目的や実施状況等に焦点を当てる回数を増やす。

有識者の現状認識

- 秘密情報漏えい防止等の対策として従業員のアクセスログを取得すること等に対して抵抗感を持つ中小企業が多く見られる。

有識者の示す好事例

- 抵抗感を示す事例以上に、有識者の適切な助言等に基づいてこれを導入し組織に根付かせることで、むしろ会社への帰属意識や仕事に対するプライドといったものが上がってきて緊張感が醸成され、会社の雰囲気が良くなってきたと言われることも多い。

改善策 6-4-5a に関する調査結果

【6-4-5a】中小企業では、経営層が自ら事業リスクに基づいて、営業秘密や限定提供データの取り扱いについて何をしてはいけないのかを指示・啓発する。

中小企業の好事例

- 営業秘密や限定提供データに関する従業員教育で、これらの取扱方法に加えて、禁止事項・内規の懲罰規定・法の遵守等についても教育している。
- 個人情報保護法、不正競争防止法、外為法等を対象として解説動画や弁護士の説明を教材に取り入れて従業員に教育することで、民事的な賠償責任や刑事責任を負ったりする場合があること等を理解させている。
- 経営層が率先して集める、外部委託先から情報提供を受ける等の手法で、他社で発生した事案の情報を取りまとめ、社会的な影響なども含めて教育している。

改善策 6-4-5b に関する調査結果

【6-4-5b】中小企業では、経営層が全社集会などで直接従業員に教育・意識づけする。

中小企業の好事例

- 人数とリソースが少ない中小企業が選択しやすい教育方法として、外部講師（例えばIT コーディネータ）を招いて研修を行っている。
- 日常業務において秘密情報の取り扱いに問題がないか、社員同士で相互確認する日々実践形式の教育を取り入れている。

対策実施に関する課題の改善（調査軸６の５）

改善策 6-5-2 に関する調査結果

【6-5-2】経営層が積極的に従業員とコミュニケーションを取ることで、従業員の行動監視やログの記録・分析等に対する従業員の理解を得る。

中小企業の好事例

- IT システムのアクセス等のログを取得して定期的に確認することについて、十分なコミュニケーションを取ってインシデント対応のために必要であることをていねいに説明することで、従業員の理解と信頼が得られている。

改善策 6-5-3 に関する調査結果

【6-5-3】中小企業では、重要情報漏えいの防止体制の下で、サイバーセキュリティと内部不正防止の両方に共通する対策を積極的に１つにまとめる。

中小企業の好事例

- 秘密情報の漏えい防止に向けた内部不正防止対策とサイバーセキュリティ対策を同一の取組の一環として実施している。この一因として、ISMS や技術情報管理の認証のスコープが両者をカバーしていることが挙げられる。
- ミスが発生した際の報告について、これを隠ぺいする組織風土にならないように、自発的な報告を考課で高く評価している。
- 経営者が自ら事業運営と内部不正防止／情報セキュリティの両方にコミットしている。

中小企業による示唆

- 不正が発覚した際の社内告知については、特に 1 人 1 人の顔が見えるぐらいの組織規模の場合に、慎重に伝え方を選ぶ必要がある。

- 経営者の負担が大きくなりすぎないように気を付ける必要がある。

改善策 6-5-4 に関する調査結果

【6-5-4】内部不正のリスクシナリオを加味した重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。

中小企業の現状認識

- ISMS 取得に必要な範囲で情報リスク評価を実施している。
- 技術情報管理認証が退職後に秘密情報を持ち出すリスクを重視している。
- 他社の秘密保護を支援する事業を提供しており、自社で秘密情報漏えい事件を起こしてしまうとレピュテーションリスクが甚大であると認識している。

中小企業の好事例

- 秘密情報漏えいの事業リスクとその重要度を事業継続性の中でどのように位置付けるかについて、経営層の間で認識を共有している。
- 従業員の秘密保持義務に関し、入社時の誓約書で「退職する時にも誓約書を提出すること」を誓約してもらっている。
- 対処の難しさを理解した上で次のような色々なリスクに注意を払っている：秘密情報の意図的な持ち出し、電子メールの誤送信、その他不注意やミスによる情報漏えい、個人所有の BYOD 利用、中途退職者の持ち出し。

有識者による示唆

- 中小企業では他社の事例等に基づいて意識の高い経営層がリスクを判断できれば、秘密情報漏えいや内部不正のリスク評価をある程度代替できる。

改善策 6-5-5 に関する調査結果

【6-5-5】個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。

中小企業の好事例

- 経営者のリーダーシップの下で、採用・退職・プロジェクト異動等の際に、都度必要な秘密保持義務契約を締結している。

- 社長の意識づけに従い、プロジェクトごとに情報資産を定義しており、これに基づいて秘密情報を識別できるようにしている。これを活用し、秘密保持義務契約の対象となる秘密情報を具体的に示している。

有識者による示唆

- 営業秘密を管理するための体制、何が秘密なのかをきちんと資産管理すること等から着手し、これを社内に浸透させていく過程で、自然に内部不正防止・営業秘密保護・サイバーセキュリティの全ての質が向上する。
- 退職時の秘密保持義務契約において、対象とする秘密情報の範囲を具体的に示すことが重要である。
- 入社時の契約書／誓約書で、「退職時にも契約する／誓約書を出す」という条項を書いておくことが有効である。

改善策 6-5-6 に関する調査結果

【6-5-6】情報機密区分に応じたアクセス権限付与状況の点検、アクセス権限付与者についての定期的な棚卸しを実施する。

中小企業の好事例

- 技術情報管理認証を取得した企業では、秘密情報の定期的な棚卸しや不要なものの消去、アクセス権限の見直しに重点を置いてこれを実施している。

③ガイドラインの利用と実践に関する課題の改善（調査軸７）

改善策 7-1 に関する調査結果

【7-1】認知度・活用度合の高い「サイバーセキュリティ経営ガイドライン」「秘密情報の保護ハンドブック」「営業秘密管理指針」「限定提供データに関する指針」「経済安全保障の確保に向けて 2022～技術・データ・製品等の流出防止～」との相互参照を進める。また、支援ツール開発や外部専門家派遣による適用開始支援等を検討する。

中小企業の好事例

- 中小企業の担当者にも理解しやすく、有用な学習用資料として、東京都が公開した「中小企業向けサイバーセキュリティ対策の極意」を利用している。

中小企業による示唆

- 中小企業の情報漏えい／内部不正防止対策を強化する上で、「組織における内部不正防止ガイドライン」や「中小企業の情報セキュリティ対策ガイドライン」との相互参照を検討できる可能性がある。

改善策 7-2 に関する調査結果

【7-2】概要版の作成、活用しやすい情報量の調整・表現の工夫、社内規程整備のために活用しやすい内容の増補、従業員への周知・教育にそのまま使えるコンテンツの充実等を検討し、「組織における内部不正防止ガイドライン」適用の実効性を高める。

中小企業の現状

- 「組織における内部不正防止ガイドライン」を基本方針や社内規程の検討に役立てている。
- 「組織における内部不正防止ガイドライン」を社員教育用資料のコンテンツとして活用している。
- 「組織における内部不正防止ガイドライン」を対策投資の説明根拠として活用している。

中小企業による示唆

- 概要版や中小企業向けのハンドブックのような冊子が欲しい。
- 中小企業において求められるコスト・時間と、社員に与えるミッションや情報利用の利便性の間のバランスをどのように取るべきか、またこれについてどのような好事例があるのかについて情報提供して欲しい。

④有識者インタビューで得られたその他の有益な示唆

中小企業における秘密情報漏えい／内部不正防止の取組の進展において、経営者の高い意識と強いリーダーシップは決定的な意味を持っている。従って、秘密情報漏えい／内部不正防止に関心がない多くの中小企業経営者の意識をどうやって変えるかが大きなポイントとなる。これについて有識者から、将来を見据えた有効な示唆が得られたので、ここで取りまとめておく。

まず、有識者から得られた４つの観点を以下に示す。

a. 社外顧問、社外取締役等が提起した議論からの学び
b. グループ全体での IT ガバナンス向上要請からの学び

c. 個人情報保護法の両罰規定（当事者企業が罰を受ける規定）を端緒とした意識付け
d. 助言型監査を活用した委託元との対話からの学び

次に、各観点に関する有識者の示唆を取りまとめる。

a. 社外顧問、社外取締役等が提起した議論からの学び

コーポレート・ガバナンス構築は、現在は上場企業などの大企業を対象に議論されることが多いが、最近は中小企業においてもその重要性が指摘されている。例えば、中小企業庁は 2023 年 6 月に「中小エクイティ・ファイナンス活用に向けたガバナンス・ガイダンス[2]」を公開し、エクイティ・ファイナンス活用における中小企業のコーポレート・ガバナンスの重要性を解説している。このような文脈で重要な役割を果たすのが社外取締役や社外顧問であり、弁護士や中小企業診断士等がその任に就くことが多い。

有識者の示唆は、こうした社外取締役／社外顧問が取締役会等での議事を提起し、例えば新商品の開発／ビジネスの資金調達の議論においてバランスシート等を提示した上で、秘密情報保護の重要性を確認する等を行えば、経営者を含むその場に参加した役員等に、秘密情報保護が重要であることを意識付けられるというものである。

取締役会で秘密情報保護／内部不正防止について議論する機会を増やす必要があるという指摘は良くあるが、誰がきっかけを作るべきかという観点で有効な示唆であると考える。

b. 個人情報保護法の両罰規定（当事者企業が罰を受ける規定）を端緒とした意識付け

個人情報保護法の両罰規定は企業の信用に非常に大きな影響を及ぼすため、中小企業の経営者も個人情報漏えいには敏感である。有識者の示唆は、これを入口として、①営業秘密の内容が個人情報の場合は、個人情報保護法で立件することが多く、同法の両罰規定が企業に適用されるリスクがあること、②営業秘密保護

[2] 中小企業庁「中小エクイティ・ファイナンス活用に向けたガバナンス・ガイダンス（概要版）」（2023 年 6 月公開）
https://www.chusho.meti.go.jp/koukai/kenkyukai/equityfinance/guidance/guidance_01.pdf
（2024 年 3 月 14 日現在）

（不正競争防止法）にも両罰規定があり、これが企業に適用されるリスクがあることを説き、その上で、秘密情報漏えい／内部不正リスクの大きさを中小企業の経営者にも強く認識してもらうのが良いというものである。最近、不正競争防止法の両罰規定を適用して、企業に罰金刑を課した判決があったが、この動きが活性化すれば、中小企業の経営者に与えるリスク認識も高まるものと推察する。

c. グループ全体での IT ガバナンス向上要請からの学び

サプライチェーン保護への社会の要請が益々強まるにつれて、企業グループ全体で IT ガバナンスを向上させる機運が高まっている。より高い見地を持つ親会社からの要請で中小企業が IT ガバナンスの強化に取り組む際に、経営者が率先してこれを主導し、秘密情報漏えい／内部不正防止をその射程に置くことができれば、当該企業の経営者の秘密情報漏えい／内部不正防止に対する意識は高まるものと期待できる。

d. 助言型監査を活用した委託元との対話からの学び

委託元企業の中には、サプライヤ企業に定期的に助言型監査を行う企業も見られる。この助言型監査では、委託元企業の意識の高い担当責任者とサプライヤ企業の経営層が直接リスクコミュニケーションを行う機会を設けることが多く、サプライヤ企業の経営層が委託元企業の高い意識や進んだ取組を学ぶ良い機会になる。これを契機として、サプライヤ企業の経営者に、秘密情報漏えい／内部不正防止に対する意識を高めてもらう方法も有効であると考えられる。

これらの示唆をすぐに実現することは一般には難しいが、中長期的な視野で見れば将来のあるべき姿を示していると考えられるので、今後こうした取組を推進できる社会環境が着実に整備されることに期待したい。

コラム：SaaS 事業者の情報漏えい／内部不正防止対策の現状とは

SaaS 事業者はスタートアップの中小企業が多い業態である。今回、SaaS のセキュリティ評価プラットフォームを提供する株式会社アシュアードへのインタビューを実施し、SaaS 事業者の情報漏えい／内部不正防止対策の現状についての知見を得た。

【SaaS 事業者の情報漏えい対策充実の分岐点とは】

スタートアップの SaaS 事業者にとって、情報管理や情報セキュリティの重要性を強く認識するようになるのは、事業規模が拡大して従業員数が 100 人を超え、大企業や個人情報を大量に扱う業界（例：金融、人材等）の顧客との取引が増えてくる時点であることが多い。元々は重要な情報の保護よりもサービス提供やサービス機能の拡充を優先する傾向が強いところ、大企業が設定するセキュリティ要件によって失注が増え、顧客の求めが厳しくなるため、情報管理や情報セキュリティの強化が待ったなしの状況になるためである。従って、従業員数が 100 人を超える規模の SaaS 事業者は、「重要な秘密の保護」に対して十分な認識を具備していることが多いと考えて良い。

【内部不正防止対策は大丈夫か】

内部不正防止については、技術的な対策もさることながら、従業員教育が重要になる。情報セキュリティについては、利用者企業から教育の実施を求められることもあり、SaaS 事業者は通常、個人情報保護法、セキュリティインシデントの事例、IPA が提供するコンテンツなどの教育をしっかりと実施している。内部不正防止の教育は情報セキュリティ教育の一部として実施されることが多いが、セキュリティ設定ミスに関する教育が良く実施されている一方で、不正行為対策は教育に組み込みづらい様子が見られる。SaaS 事業者の内部不正防止対策については、必要に応じて念のため、注意深く確認することを検討すると良い。

【セキュリティ設定ミス対策としてのセキュアバイデフォルトは、国内ではまだこれから】

SaaS のセキュリティ設定ミスによる情報漏えいに対する SaaS 事業者の危機感は相当高まっている。しかし、セキュリティ設定のデフォルトを安全側にする等のセキュアバイデフォルトの設計思想が、国内の SaaS 事業者には必ずしも浸透していないと感じている。また、セキュリティ設定ミス対策やその他のセキュリティ対策がサービスの利便性を損なうと考える SaaS 事業者がまだ多い。

【AI が SaaS の情報漏えい対策の認識を変える？】

SaaS 事業者は、基本的には預託情報の内容を閲覧しないが、近年は AI サービスのアップデートや研究開発のために、預託情報の内容を閲覧する機会が増えており、情報管理の複雑さが増して、情報漏えいリスクが高まっていると感じている。

4. 調査結果の分析

以下では、事例調査結果の分析、アンケート調査結果のクロス集計、アンケートとインタビューの調査結果のクロス分析を実施し、その結果を踏まえて現状の課題と取り得る対策を取りまとめた。

(1) 事例調査結果の分析からの示唆

ここでは、事例調査結果のデータを用いて、「図表 5　予め準備した現在の実態や動向に関する想定」でまとめた想定と現在の社会状況の比較分析を実施し、4 つの切り口に沿って得られる示唆を取りまとめた。これらの示唆は、企業アンケート調査のクロス集計結果を分析する際などに、秘密情報漏えいやサイバー攻撃において頻度やリスクの高い類型等に関する前提知識として活かすことができる。

①企業規模による事案発生傾向の違い

【現在の実態や動向と比較する予め準備した想定】

- 営業秘密は大企業だけでなく、規模が小さい企業（従業員 300 名以下）等からも漏えいしている。
- 内部不正は大企業だけでなく、規模が小さい企業（従業員 300 名以下）等でも発生している。
- 規模が小さい企業（従業員 300 名以下）等であっても、情報漏えいによる被害のインパクトは大きい。

整理した 2020 年 4 月以降の事案を分析すると、営業秘密の漏えい事案は規模が小さい企業でも 5 件以上発生している。本事例調査で世の中の事案を網羅できている訳ではないが、大企業でも 20 件弱の事例が観測されている傍らでの件数であり、規模が小さい企業の事案がほとんど観測されないということはなかった。むしろ、営業秘密漏えい事案は無視できない頻度で発生していると考える方が妥当である。一方、内部不正による情報漏えいについても、規模の小さな企業での故意の漏えいが 10 件を超えており、電子メールの誤送信、Web サイトやクラウドサービスの設定ミス、PC や可搬メディアの紛失はさらに多発している。従って、規模の小さな企業でも内部不正は多く発生していると言える。

規模の小さい企業では、EC サイトを中心に多くの個人情報漏えい事案が発生しているが、その漏えい件数は大企業と比較しても決して少ないとは言えない。中には 200 万件弱の個人情報が漏えいし、インパクトが大きい被害を受けてしまう事案も見られた。

②情報漏えいとサービス／システム停止の事案発生傾向の違い

【現在の実態や動向と比較する予め準備した想定】

- 内部不正の場合は情報漏えいがほとんどであり、サービス／システムの停止を伴うことはほとんどない。
- 取引先からの情報漏えい、取引先に起因するサービス／システム停止の両方が目立ってきている。
- サイバー攻撃による情報漏えいの目的が、産業スパイ（他国政府、民間企業）であることはまだ少ない。

2020 年 4 月以降の事例で、内部不正でサービス／システムが停止した事案は見つからなかった。基本的には、内部不正事案の多くは情報漏えいを伴うと考えて良い。

取引先で発生する事案では情報漏えいは多く発生しており、この中にはコールセンタを運用する委託先で大規模な個人情報漏えいが発生した重大事案が含まれている。取引先が原因となって自社のサービス／システムが停止した事案についても、少なくとも 1 件大規模病院でランサムウェアによる重大事案が発生しており、グループ企業が共用するシステムがランサムウェア被害を受けたことでグループ全体のシステムが機能停止した重大事案もあった。このように、取引先からの情報漏えいや取引先に起因するシステム／サービス停止は重大事案に発展するリスクが高くなってきており、今後は注意が必要である。

産業スパイがサイバー攻撃で秘密情報を盗み出そうとした事案については、明確なものを特定することはできなかった。

③個人情報漏えいと営業秘密漏えいの事案発生傾向の違い

【現在の実態や動向と比較する予め準備した想定】

- 規模が小さい営業秘密の漏えいは表に出ていない。
- 営業秘密漏えいによる被害規模は、個人情報漏えいの場合と比べてみても、十分に大きい。
- ミスによる情報漏えいは個人情報の漏えいが多いが、営業秘密の漏えいも目立ってきている。
- 取引先からの情報漏えいは、個人情報でも営業秘密でも発生している。
- 外国政府の関与が疑われるのは、営業秘密が漏えいした場合である。

2020 年 4 月以降の事案から、規模が小さい営業秘密の漏えいが表に出ていないことを確かめることはできなかった。一方で、報道されている営業秘密漏えい事案は、基本的に刑事事件として立件または提訴されたものが中心[3]なので、これに当たらないような小さな事案は潜在している可能性を否定できない。

漏えいした際の被害の大きさは、発生した時点で見ると、基本的には個人情報漏えいの方が報告や報道等によるインパクトが大きい傾向にある。営業秘密漏えいの場合は、民事で提訴しても国内で認定される損害額は必ずしも大きくなく、また中長期的視点で見ないとその損害の大きさを見積もれないという特性もあって、本当の事業損失がどのくらいの規模なのかを公知情報や裁判例から読み取ることが難しかった。

不注意やミスによる情報漏えいや取引先に起因する情報漏えいは、多くが個人情報の漏えいであり、営業秘密の漏えいはほとんど見つからなかった。前述したように、営業秘密の漏えいが報道されるのは刑事事件として立件または提訴されたものが中心なので、ミスで漏えいした事案は報道されていなくても不思議ではない。

2020 年 4 月以降の事案で、外国政府の関与が濃厚と言える事案は見当たらなかったが、少しは可能性があると考えられるものが数件あった。これらはいずれも営業秘密が漏えいした事案であった。

④内部不正とサイバー攻撃の事案発生傾向の違い

【現在の実態や動向と比較する予め準備した想定】

- 営業秘密の漏えいは内部不正によるものが中心である。
- 個人情報漏えいは、サイバー攻撃でも内部不正でも多く発生している。
- 取引先でも、内部不正とサイバー攻撃の両方が多く発生している。
- 外国政府の関与が疑われるサイバー攻撃が目立ってきている。

2020 年 4 月以降の事案で、サイバー攻撃によって営業秘密が漏えいした事案は見つからなかった。従って、公知情報に基づく分析結果としては、営業秘密の漏えいは内部不正によるものが中心であると言って良いものと考える。但し、サイバー攻撃の場合には、被疑者を特定し、営業秘密侵害で立件や提訴することが難しいので、発生してもほとんど報道されていない可能性を否

[3] 将来的には、経済安全保障推進法違反を問われる事案が増える可能性がある。

定できない。

個人情報の漏えいについては、サイバー攻撃によるものも、内部不正によるものも、調査した範囲で数十件程度発生しており、どちらも多く発生していると言える。

本調査が対象とした事案の範囲では、取引先で発生した事案はサイバー攻撃よりも内部不正の方が多く発生しているが、これだけで実態を分析するのは難しいと考える。外国政府の関与が疑われるサイバー攻撃については、事案が見つからず、分析ができなかった。

⑤まとめ

事例調査結果の分析でここまでに得られた結果を俯瞰すると、重要な示唆は以下の４つであると考えられる。これらの示唆を、この後の企業アンケート調査のクロス集計の分析や、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で活かしていくことにする。

【得られた重要な示唆】

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

(2) 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（301 人以上）と中小企業（300 人以下）
iv. 経営層による対話機会を設けている企業とそれ以外
v. 内部不正防止とセキュリティ確保を意図的に分けている企業とそれ以外
vi. 個人情報以外の秘密情報保護対策を重視している企業とそれ以外

次に、各調査軸に紐づく改善策を現状と比較する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た。結果を一覧として図表５７に示す。（※クロス集計の分析軸は、上記のｉ～viの分析軸番号を参照）

図表５７．クロス集計を実施する対象の一覧

調査軸	実践状況を分析する改善策	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
経営課題の改善（調査軸１）			
	【1-1】法務・知財部門（社外の法律相談サービスを含む）の協力を得る等の取組を検討して、営業秘密等の漏えい事件（事例）から、事業リスクとしての重要性や当事者がしてはならないこと等を率先して学ぶ。	経営層の秘密情報漏えいに関するリスク認識	ｉ,vi
	【1-2】経営層によるセキュリティ確保のリーダーシップ発揮の機会／場を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。	経営層のリーダーシップ発揮の違い	v
		内部不正防止とセキュリティ確保を別建てにしているか	iv、vi
重要な秘密の特定と取扱いの改善（調査軸２）			
	【2-1】経営層も積極的に関与して、事業リスクが高い（漏えいした場合のインパクトが大きい）営業秘密等を特定するための基準作り、従業員の営業秘密に対する対策意識の醸成、営業秘密の定期的な見直し等に取り組む。	秘密情報の特定と格付けの実効性を高めるための取組	i, v、vi
		秘密情報の取り扱い方	v、vi
組織体制・連携に関する課題の改善（調査軸３）			
	【3-1】責任部門自体（リスク・コンプライアンス部門等）と関連部門（情報システム部門：対策実施部門、法務・知財部門、営業・事業部門）が協働する体制の整備を検討する。	内部不正に対応する経営層／組織の連携の目的	vi.
	【3-3】重要な秘密が不自然に取り扱われているところを目にしたら、上に報告するというリテラシーと、上に報告できない事情がある場合は内部通報ができる体制を構築する。	内部不正を目撃した際の内部通報体制／ルール整備の状況	vi.
社員教育とリテラシー構築に関する課題の改善（調査軸４）			
	【4-2】入社／人事異動／退職等の重要なタイミングで、具体的に重要な秘密を示して、何をしてはいけないのか、どのような時に上への報告が必要か等を周知・徹底する。	秘密情報漏えい／内部不正の事実の告知状況	vi
		秘密情報の不自然な扱いや不正な漏えいを目撃した際の望ましい行動の周知状況	vi
	【4-3】事業や経営における重要性や価値、当該情報が漏えい・毀損等した場合の影響・損害などを踏まえた、秘密の重要度の判別基準を明文化した上で、この基準に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。	秘密情報保護の周知・教育の状況	v

調査軸	実践状況を分析する改善策	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
	【4-5】インシデント事例、解説動画・イラスト等のリッチコンテンツ、グループディスカッション、定期的な規則遵守のセルフチェック等を積極的に活用して理解を深める取組を推進すると共に、従業員に対し、営業秘密や限定提供データについて、何をしてはいけないのかを教育する。	秘密情報漏えいや内部不正に関する禁止行為や罰則の周知状況	v、vi
対策実施に関する課題の改善（調査軸５）			
	【5-3】重要情報漏えい防止体制の下で、サイバーセキュリティ対策と内部不正防止対策の両方に一貫して取り組む。	内部不正防止対策の取組状況	v
		内部不正防止とセキュリティ確保を別建てにしているか	vi
	【5-4】 内部不正のリスクシナリオも加味して重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。この際には、不正に対する人的・組織的対策と技術的対策のバランスの適正化を考慮する。また、経営層の不正防止と透明性確保、アクセスログの確認範囲拡大、他社の重要情報の不正な社内持ち込み防止、重要プロジェクト就任／離任時にも秘密保持義務の誓約書を取得、重要性の高い秘密に触れる場合の誓約書の詳細度の変更等を実施する。	内部不正リスクをサイバー攻撃リスク等と意識的に分けて評価しているか	vi
	【5-5】 個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。	秘密情報保護対策の重視度	vi.
中小企業の構造的課題の改善（調査軸６）			
	【6-1-1】経営層または内部不正防止に関する組織全体の責任者等が率先して、重要な秘密情報漏えい／内部不正リスクを重要な経営課題として認識する機会を増やし、サイバーセキュリティ確保と内部不正防止を一体的に認識した経営を行う。	秘密情報漏えいのリスク認識	iii.
	【6-1-2】 中小企業では、全社集会などの経営層が従業員に周知徹底する機会を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。	経営層のリーダーシップ発揮	
		内部不正防止とセキュリティ確保を別建てにしているか	
	【6-2-1】中小企業では、経営層が自ら判断する、あるいは判断基準を示すことで、自社の事業にとって重要性／機密性の高い秘密情報を的確に特定する。【	秘密情報の特定と格付けの実効性を高めるための取組	
		秘密情報の取り扱い方	
	【6-3-1】 中小企業では、責任者である経営層が中心となって、総務・人事・法務や情報システム等の関連部門との調整を行う。	内部不正発生時の対応者	
	【6-3-3】 重要な秘密が不自然に取り扱われている様を目撃した際に上に報告することの徹底と、上に報告で	内部通報体制／ルール整備の状況	

調査軸	実践状況を分析する改善策	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
	きない事情がある場合は内部通報ができる体制を構築する。		
	【6-4-2】中小企業では、入社／人事異動／退職等の重要なタイミングで、経営層が重要な秘密を具体的に示し、その取扱い指示を徹底する。	秘密情報漏えい／内部不正の事実の告知状況の違い	
		秘密情報の不自然な扱いや不正な漏えいを目撃した際の望ましい行動の周知状況	
	【6-4-3】経営層または経営層が権限を移譲した責任者が各々の秘密の重要度を指定した上で、この指定に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。	秘密情報保護の周知・教育の状況	
		秘密情報の特定と格付けのための全社共通基準の周知状況	
	【6-4-5a】中小企業では、経営層が自ら事業リスクに基づいて、営業秘密や限定提供データの取り扱いについて何をしてはいけないのかを指示・啓発する。 【6-4-5b】中小企業では、経営層が全社集会などで直接従業員に教育・意識づけする。	秘密情報漏えいや内部不正防止の従業員教育の状況	
	【6-5-3】中小企業では、重要情報漏えいの防止体制の下で、サイバーセキュリティと内部不正防止の両方に共通する対策を積極的に１つにまとめる。	内部不正防止対策の取組状況	
		内部不正防止とセキュリティ確保を別建てにしているか	
	【6-5-4】内部不正のリスクシナリオを加味した重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。	内部不正リスクをサイバー攻撃リスク等と意識的に分けて評価しているか	
	【6-5-5】個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。	秘密情報保護の対策の重視度	
	【6-5-6】情報機密区分に応じたアクセス権限付与状況の点検、アクセス権限付与者についての定期的な棚卸しを実施する。	秘密情報へのアクセス権の見直し／棚卸しの取組み状況	
ガイドラインの利用と実践に関する課題の改善（調査軸７）			
	【7-2】概要版の作成、活用しやすい情報量の調整・表現の工夫、社内規程整備のために活用しやすい内容の増補、従業員への周知・教育にそのまま使えるコンテンツの充実等を検討し、「組織における内部不正防止ガイドライン」適用の実効性を高める。	ガイドラインの活用状況の違い	ii、iii、vi

なお、クロス集計結果については、図表を報告書に記載すると共に、興味深い分析結果が出たものを中心に抜粋して改善策の実践状況の分析に役立てた。

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５７に示した通り、各調査軸に紐づく改善策の実践状況を分析するにあたって、企業アンケート結果（単純集計・クロス集計）及び企業／有識者インタビューの結果を比較分析し、改善策と現状の比較を行うと共に、好事例の抽出、改善策を補う示唆の抽出を実施した。

なお、業種・業態を軸にしたクロス集計結果の分析にあたり、回答数が 10 に満たない業種・業態は対象としていない。また、以降のクロス集計図表からの読み取りにおいて、回答割合が全体平均よりも 15%以上高くなっている、あるいは低くなっている場合に、「格段に」という評価を附記している。

(3) 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（1,248 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 472 名含まれており、このうち約 73%は中小企業の経営層である。

①全体的な課題の改善（調査軸１～５）

経営課題の改善（調査軸１）

<u>改善策 1-1 に関する現状</u>

【1-1】法務・知財部門（社外の法律相談サービスを含む）の協力を得る等の取組を検討して、営業秘密等の漏えい事件（事例）から、事業リスクとしての重要性や当事者がしてはならないこと等を率先して学ぶ。

個人情報保護との比較においてそれ以外の秘密情報保護を重視する度合いの強い組織ほど、内部不正に係る情報漏えいのリスクが高いと認識している。（図表５８参照）

図表５８．秘密情報保護対策の重視度の違いによる秘密情報漏えいのリスク認識の違い

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

（%）

		n=	（過度の超過勤務、不公平な評価、ハラスメント等に対して）不満を蓄積した従業員による秘密情報の漏えい	産業スパイによる秘密情報の漏えい	中途退職者による秘密情報の漏えい	電子メールの誤送信、PCやUSBメモリの紛失等の人的ミスによる秘密情報の漏えい	クラウドサービスからの秘密情報の漏えい	国内の取引先または国内子会社からの秘密情報の漏えい	海外の取引先または海外子会社からの秘密情報の漏えい	テレワークによる秘密情報の漏えい	サイバー攻撃による秘密情報の漏えい	秘密情報の漏えいや、それに関わる内部不正に関するリスクをあまり重視していない	わからない
	TOTAL	1248	42.2	17.2	50.0	59.1	32.7	29.3	19.2	33.3	50.6	4.8	5.0
Q20 個人情報以外の秘密情報を保護する対策も重視しているか	個人情報を保護する対策以上に重視している	280	51.8	31.1	53.9	62.5	47.1	37.9	34.6	44.6	55.7	2.1	5.0
	個人情報を保護する対策と同じくらい重視している	548	47.3	17.7	54.7	68.2	36.9	34.9	19.5	38.7	59.3	1.5	1.1
	個人情報を保護する対策ほどではないが、ある程度重視している	230	30.9	10.9	45.2	53.9	23.0	20.4	10.0	25.7	41.7	6.1	2.6
	あまり重視していない	108	32.4	1.9	44.4	42.6	13.0	16.7	8.3	13.0	34.3	17.6	4.6
	全く重視していない	29	24.1	6.9	34.5	17.2	6.9	0.0	0.0	3.4	17.2	27.6	13.8
	わからない	53	18.9	3.8	20.8	26.4	9.4	7.5	5.7	7.5	22.6	9.4	50.9

経営層は、産業スパイ・クラウドサービス・国内外の取引先／子会社、テレワークに起因するリスクを高いと認識する割合が全体平均よりも低い。（図表５９参照）

図表５９．回答者の担当業務の違いによる秘密情報漏えいのリスク認識の違い

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

（%）

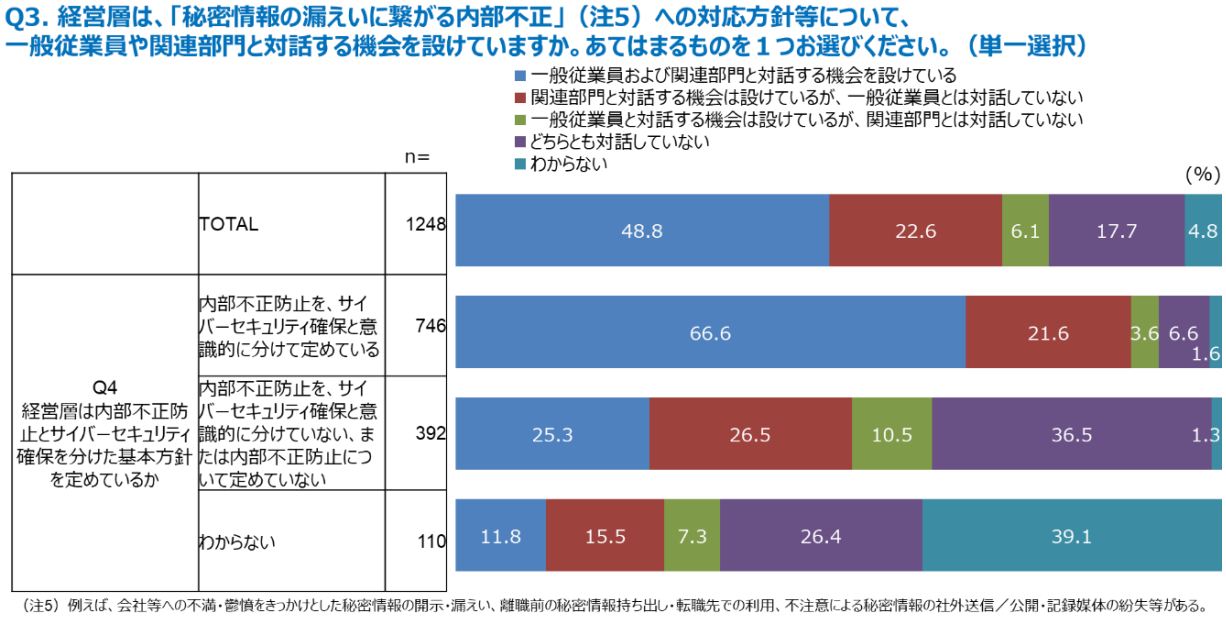
		n=	（過度の超過勤務不公平な評価、ハラスメント等に対して）不満を蓄積した従業員による秘密情報の漏えい	産業スパイによる秘密情報の漏えい	中途退職者による秘密情報の漏えい	電子メールの誤送信、PCやUSBメモリの紛失等の人的ミスによる秘密情報の漏えい	クラウドサービスからの秘密情報の漏えい	国内の取引先または国内子会社からの秘密情報の漏えい	海外の取引先または海外子会社からの秘密情報の漏えい	テレワークによる秘密情報の漏えい	サイバー攻撃による秘密情報の漏えい	秘密情報の漏えいや、それに関わる内部不正に関するリスクをあまり重視していない	わからない
	TOTAL	1248	42.2	17.2	50.0	59.1	32.7	29.3	19.2	33.3	50.6	4.8	5.0
SQ1 担当業務	a．情報システム関連部門の担当者	128	41.4	28.1	40.6	46.1	32.0	27.3	22.7	28.9	39.8	7.0	5.5
	b．情報システム関連部門を所掌・所管する部門の責任者	180	43.3	23.3	55.6	65.6	47.2	36.1	28.9	34.4	54.4	1.1	1.7
	c．リスクマネジメント計画・実践に関わる部署の担当者	73	38.4	23.3	39.7	54.8	30.1	38.4	17.8	35.6	41.1	2.7	4.1
	d．リスクマネジメント計画・実践に関わる部署を所掌・所管する部門の責任者	91	48.4	13.2	53.8	65.9	34.1	39.6	20.9	37.4	51.6	0.0	2.2
	e．経営企画部門のIT／セキュリティ戦略担当者	51	33.3	19.6	41.2	54.9	35.3	31.4	19.6	49.0	51.0	5.9	2.0
	f．経営企画部門のIT／セキュリティ戦略担当を所掌・所管する部門の責任者	99	52.5	27.3	61.6	65.7	49.5	45.5	26.3	54.5	61.6	4.0	3.0
	g．経営層	472	39.6	9.5	48.7	55.5	23.7	19.5	10.6	26.3	49.4	7.6	6.1
	h．a～f以外の部門でも、リスクマネジメントに関する業務を実施していると認識している担当者	154	44.2	16.9	53.2	68.8	32.5	31.8	26.0	34.4	55.2	2.6	9.1

改善策 1-2 に関する現状

【1-2】経営層によるセキュリティ確保のリーダーシップ発揮の機会／場を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。

基本方針で内部不正をサイバーセキュリティと別建てにしている企業では、経営層と一般従業員や関連部門と対話する機会を設けている割合は 91.8%に達し、そうでない企業における 56.2%という割合の 1.6 倍を超える。（図表６０参照）

図表６０．内部不正防止とセキュリティ確保を別建てにしているかの違いによる経営層のリーダーシップ発揮の違い

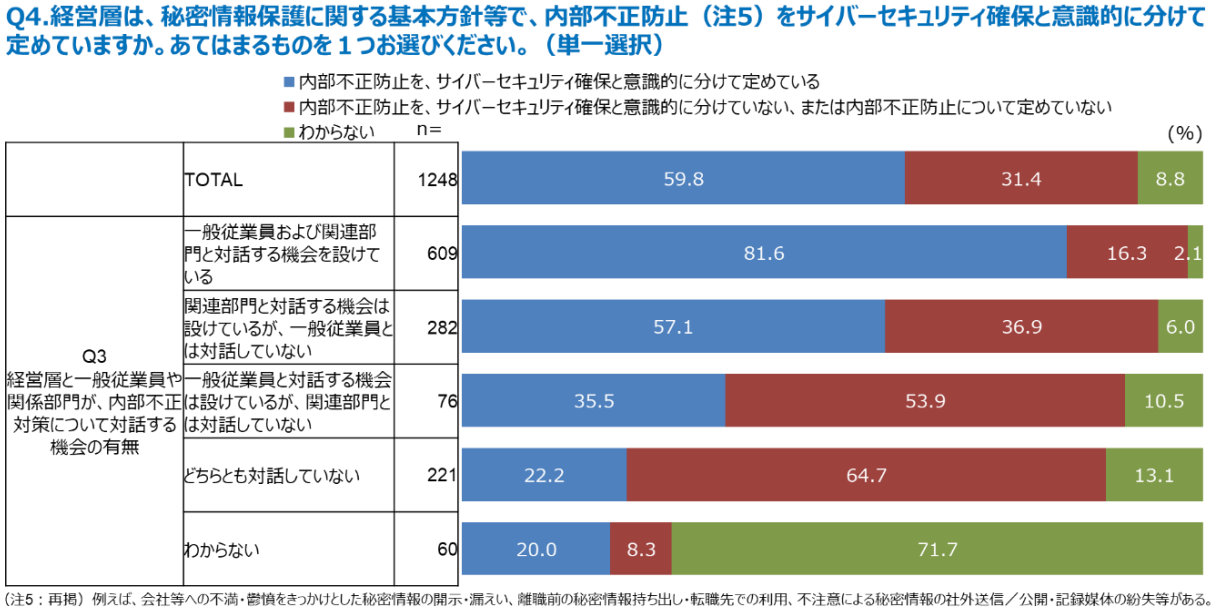


（注5）例えば、会社等への不満・鬱憤をきっかけとした秘密情報の開示・漏えい、離職前の秘密情報持ち出し・転職先での利用、不注意による秘密情報の社外送信／公開・記録媒体の紛失等がある。

逆に、経営層が一般従業員や関連部門と対話する機会を設けている企業では、基本方針で内部不正をサイバーセキュリティと別建てにしている割合が 8 割を超えている。「経営層が現場との対話の機会を設けること」と「基本方針で内部不正をサイバーセキュリティと別建てとすること」の間には強い結びつきがあると言える。

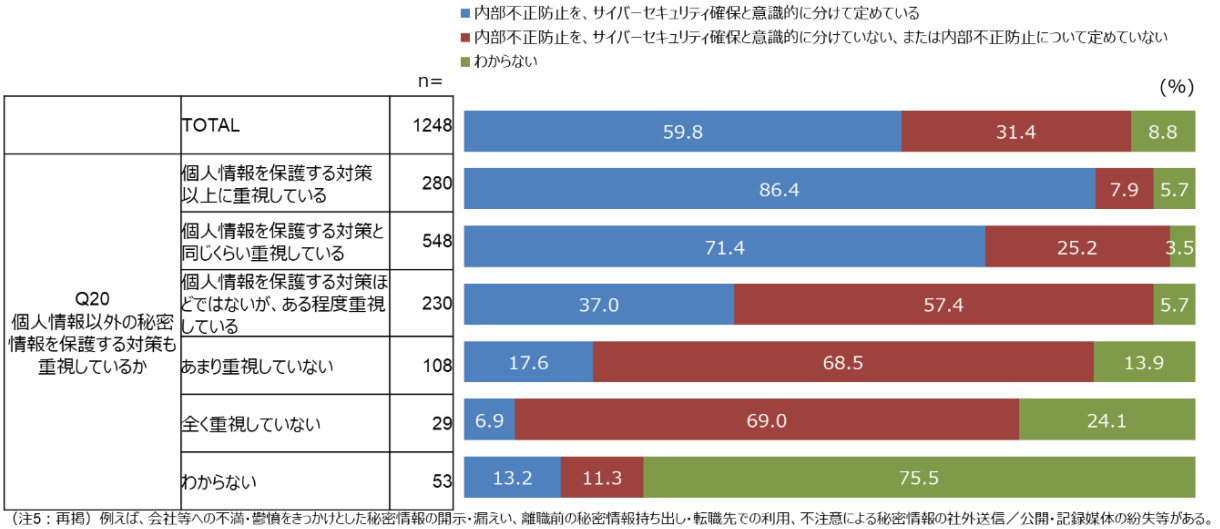
事例調査で得られた「営業秘密の漏えいは内部不正によるものが看過しえないほど多くを占める」というインシデント傾向を踏まえると、営業秘密保護の意識が高い経営層は、内部不正防止を重視すると共に、現場との対話に力を入れていると解釈できる。（図表６１参照）

図表６１．経営層のリーダーシップ発揮の違いによる内部不正防止とセキュリティ確保を別建てにしているかの違い



個人情報以外の秘密情報の保護を重視している経営層の大半は、内部不正とサイバーセキュリティを方針等で別建てにしている。営業秘密保護の意識が高い経営層は、内部不正防止は情報漏えい防止における重点課題だと理解していることの表れと解釈できる。（図表６２参照）

図表６２．秘密情報保護対策の重視度の違いによる内部不正防止とセキュリティ確保を別建てにしているかの違い



重要な秘密の特定と取扱いの改善（調査軸２）

改善策 2-1 に関する現状

【2-1】経営層も積極的に関与して、事業リスクが高い（漏えいした場合のインパクトが大きい）営業秘密等を特定するための基準作り、従業員の営業秘密に対する対策意識の醸成、営業秘密の定期的な見直し等に取り組む。

個人情報以外の秘密情報の保護の取組（特定、格付け、表示等）の割合が全体平均よりも高くなっている業種は、電子部品・デバイス・電子回路製造業、電子応用装置・電気計測器製造業、それ以外の電気機械器具製造業、電気・ガス・熱供給・水道業、通信業、金融業・保険業等である。但し、エレクトロニクス関係の製造業と基幹インフラ（電気、ガス、通信、金融・保険等）の取組が平均以上である理由を、今回の調査結果で結論付けることは難しい。（図表６３参照）

図表６３．回答者の業種・業態の違いによる秘密情報の特定と格付けの実効性を高めるための取組の違い

	n=	個人情報以外の秘密情報（営業秘密、重要なデータ等）を特定するための具体的な基準や、この基準の全社運用を求める共通ルール等を定めている	個人情報以外の秘密情報を格付けするための基準や、この基準の全社運用を求める共通ルール等を定めている	個人情報以外の秘密情報を特定または格付けする基準を適用しやすいように例を示している	格付けが漏れなく実行されるための仕組みを設け、継続的な改善を図っている	格付けをわかりやすく表示するためのルールを定めている	格付け表示がない（不明瞭な場合を含む）社内情報の取扱いについてもルールを定めている	重要な秘密情報を取り扱うプロジェクトに参加する条件として、「保護対象とする重要な秘密の範囲を明確にした上で、上述した基準やルールの順守・徹底をあらためて誓約すること」を求めるルールを定めている	定期的に、基準やルールを順守しているかを確認している（定期的なセルフチェックを含む）	何も実施していない	上記以外	わからない
TOTAL	1248	55.4	33.3	27.9	18.3	18	15.4	17.4	37.4	11.9	0.4	4.7
1．農業、林業、漁業	3	66.7	100	66.7	66.7	33.3	33.3	66.7	66.7	0	0	0
2．鉱業、採石業、砂利採取業	3	66.7	33.3	0	0	0	0	0	0	33.3	0	0
3．建設業	68	52.9	35.3	27.9	13.2	16.2	16.2	14.7	38.2	17.6	0	5.9
4．食料品製造業	45	60	20	22.2	15.6	13.3	11.1	11.1	28.9	17.8	0	2.2
5．飲料・たばこ・飼料製造業	11	54.5	36.4	9.1	9.1	9.1	0	9.1	27.3	9.1	0	9.1
6．繊維工業	14	57.1	50	50	28.6	28.6	21.4	35.7	42.9	0	0	7.1
7．化学工業	31	38.7	29	12.9	6.5	9.7	9.7	9.7	32.3	9.7	0	6.5
8．プラスチック製品製造業	8	50	0	12.5	12.5	12.5	0	12.5	12.5	12.5	0	12.5
9．ゴム製品製造業	7	42.9	42.9	42.9	0	28.6	28.6	0	42.9	0	0	14.3
10．鉄鋼業	17	29.4	23.5	23.5	17.6	5.9	5.9	5.9	35.3	17.6	0	11.8
11．はん用機械器具製造業	6	50	66.7	33.3	16.7	16.7	16.7	0	66.7	0	0	0
12．生産用機械器具製造業	25	60	56	56	40	36	32	24	44	4	0	0
13．業務用機械器具製造業	20	60	25	35	25	40	10	15	20	15	0	0
14．電子部品・デバイス・電子回路製造業	52	73.1	44.2	34.6	26.9	28.8	21.2	30.8	34.6	1.9	0	1.9
15．電子応用装置・電気計測器製造業	12	75	58.3	33.3	16.7	16.7	33.3	25	41.7	0	0	0
16．15以外の電気機械器具製造業	30	73.3	43.3	43.3	26.7	30	36.7	36.7	50	6.7	0	0
17．情報通信機械器具製造業	7	57.1	28.6	14.3	14.3	28.6	28.6	28.6	28.6	0	0	14.3
18．自動車・同附属部品製造業	35	62.9	42.9	42.9	31.4	25.7	17.1	17.1	40	11.4	0	5.7
19．18以外の輸送用機械器具製造業	12	50	50	41.7	25	33.3	8.3	25	50	0	0	0
20．4～19以外の製造業	89	51.7	25.8	20.2	7.9	12.4	11.2	14.6	33.7	15.7	0	5.6
21．電気・ガス・熱供給・水道業	24	66.7	54.2	45.8	45.8	41.7	29.2	16.7	50	4.2	0	0
22．通信業	22	86.4	63.6	45.5	31.8	31.8	18.2	18.2	59.1	4.5	0	9.1
24．情報サービス業	156	62.2	42.9	33.3	21.2	21.2	16.7	23.7	45.5	6.4	0.6	4.5
25．インターネット附随サービス業	23	60.9	34.8	43.5	21.7	21.7	21.7	43.5	43.5	4.3	0	4.3
26．映像・音声・文字情報制作業	4	75	0	0	0	0	25	25	50	25	0	0
27．運輸業、郵便業	51	37.3	25.5	13.7	19.6	13.7	23.5	7.8	33.3	15.7	2	3.9
28．卸売業、小売業	116	45.7	24.1	17.2	10.3	10.3	11.2	11.2	31.9	18.1	2.6	7.8
29．金融業、保険業	68	77.9	33.8	23.5	22.1	13.2	11.8	19.1	51.5	4.4	0	0
30．不動産業、物品賃貸業	45	44.4	33.3	26.7	13.3	11.1	8.9	8.9	37.8	11.1	0	6.7
31．学術研究、専門・技術サービス業	36	47.2	27.8	27.8	8.3	13.9	5.6	19.4	19.4	19.4	0	5.6
32．宿泊業、飲食サービス業	26	50	26.9	19.2	15.4	23.1	19.2	7.7	34.6	7.7	0	7.7
33．31、32以外のサービス業	153	46.4	22.2	23.5	17	14.4	11.1	11.8	32	20.3	0	5.2
34．公務（他に分類されるものを除く）	3	66.7	100	33.3	0	33.3	33.3	66.7	33.3	0	0	0
35．分類不能の産業	26	46.2	19.2	38.5	19.2	11.5	19.2	26.9	30.8	15.4	0	3.8

経営層が基本方針で内部不正防止をサイバーセキュリティ確保と意識的に分けて定めている企業では、取組に関する全ての選択肢で、全体平均と比べて回答割合が高くなっている。但し、

大半の組織で実践されている取組は「秘密情報を特定するルールの制定」のみであり、他の取組を実践している組織はいずれも半数に満たない。内部不正防止を重視する経営層は営業秘密等の情報資産管理の実践に力を入れているが、そのような組織であっても実践にまで及んでいない取組が多数ある状況が一般的であると解釈できる。（図表６４参照）

図表６４．内部不正防止とセキュリティ確保を意図的に分けているかの違いによる秘密情報の特定と格付けの実効性を高めるための取組の違い

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

（%）

		n=	個人情報以外の秘密情報（営業秘密、重要なデータ等）を特定するための具体的な基準や、この基準の全社運用を求める共通ルール等を定めている	個人情報以外の秘密情報を格付けするための基準や、この基準の全社運用を求める共通ルール等を定めている	個人情報以外の秘密情報を特定または格付けする基準を適用しやすいように例を示している	格付けが漏れなく実行されるための仕組みを設け、継続的な改善を図っている	格付けをわかりやすく表示するためのルールを定めている	格付け表示がない（不明瞭な場合を含む）社内情報の取扱いについてもルールを定めている	重要な秘密情報を取り扱うプロジェクトに参加する条件として「保護対象とする重要な秘密の範囲を明確にした上で、上述した基準やルールの順守・徹底をあらためて誓約すること」を求めるルールを定めている	定期的に基準やルールを順守しているかを確認している（定期的なセルフチェックを含む）	何も実施していない	上記以外	わからない
	TOTAL	1248	55.4	33.3	27.9	18.3	18.0	15.4	17.4	37.4	11.9	0.4	4.7
Q4 経営層は内部不正防止とサイバーセキュリティ確保を分けた基本方針を定めているか	内部不正防止を、サイバーセキュリティ確保と意識的に分けて定めている	746	72.3	42.9	37.4	26.8	23.6	19.4	23.3	47.7	2.9	0.3	0.9
	内部不正防止を、サイバーセキュリティ確保と意識的に分けていない、または内部不正防止について定めていない	392	31.4	21.7	13.8	5.9	11.5	10.7	9.7	22.2	27.8	0.8	2.0
	わからない	110	26.4	10.0	13.6	4.5	3.6	4.5	4.5	21.8	16.4	0.0	40.0

個人情報保護との比較において営業秘密保護を重視する度合いが高い組織ほど、関連する取組の実施割合が高まる傾向がある。但し、過半の組織で実践されている取組は「秘密情報を特定するルールの制定」（82.1%）のみである。（図表６５参照）

図表６５．秘密情報保護対策の重視度の違いによる

秘密情報の特定と格付けの実効性を高めるための取組の違い

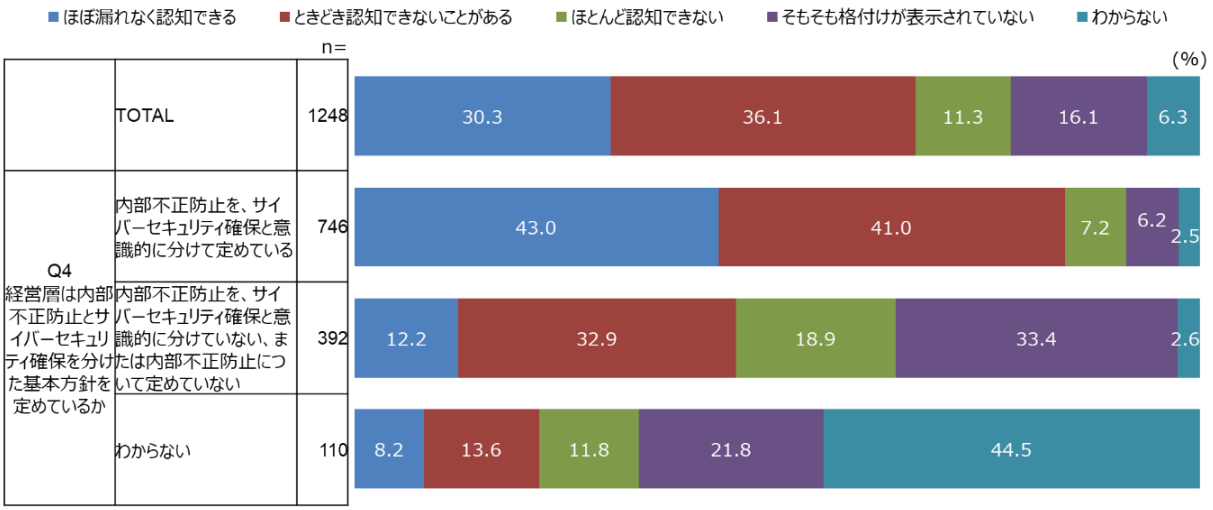
Q7.個人情報以外の秘密情報（営業秘密、重要なデータ等）の特定と格付けの実効性を高めるために、組織全体でどのような取組を実施していますか。あてはまるものをすべてお選びください。（複数選択）

(%)

		n=	個人情報以外の秘密情報（営業秘密、重要なデータ等）を特定するための具体的な基準や、この基準の全社運用を求める共通ルール等を定めている	個人情報以外の秘密情報を格付けするための基準や、この基準の全社運用を求める共通ルール等を定めている	個人情報以外の秘密情報を特定または格付けする基準を適用しやすいように例を示している	格付けが漏れなく実行されるための仕組みを設け、継続的な改善を図っている	格付けをわかりやすく表示するためのルールを定めている	格付け表示がない（不明瞭な場合を含む）社内情報の取扱いについてもルールを定めている	重要な秘密情報を取り扱うプロジェクトに参加する条件として、「保護対象とする重要な秘密の範囲を明確にした上で、上述した基準やルールの順守・徹底をあらためて誓約すること」を求めるルールを定めている	定期的に基準やルールを順守しているかを確認している（定期的なセルフチェックを含む）	何も実施していない	上記以外	わからない
	TOTAL	1248	55.4	33.3	27.9	18.3	18.0	15.4	17.4	37.4	11.9	0.4	4.7
Q20 個人情報以外の秘密情報を保護する対策も重視しているか	個人情報を保護する対策以上に重視している	280	82.1	46.4	42.1	28.2	30.4	23.9	30.4	46.4	1.1	0.4	2.1
	個人情報を保護する対策と同じくらい重視している	548	66.4	39.1	31.0	21.9	19.5	14.4	19.0	45.3	6.6	0.2	1.1
	個人情報を保護する対策ほどではないが、ある程度重視している	230	33.0	25.7	21.3	11.3	13.9	12.6	10.0	28.7	14.3	0.9	2.6
	あまり重視していない	108	11.1	9.3	4.6	1.9	0.9	13.9	4.6	13.9	48.1	0.0	4.6
	全く重視していない	29	10.3	6.9	3.4	0.0	0.0	3.4	0.0	10.3	69.0	3.4	0.0
	わからない	53	11.3	1.9	9.4	1.9	0.0	1.9	0.0	9.4	9.4	0.0	67.9

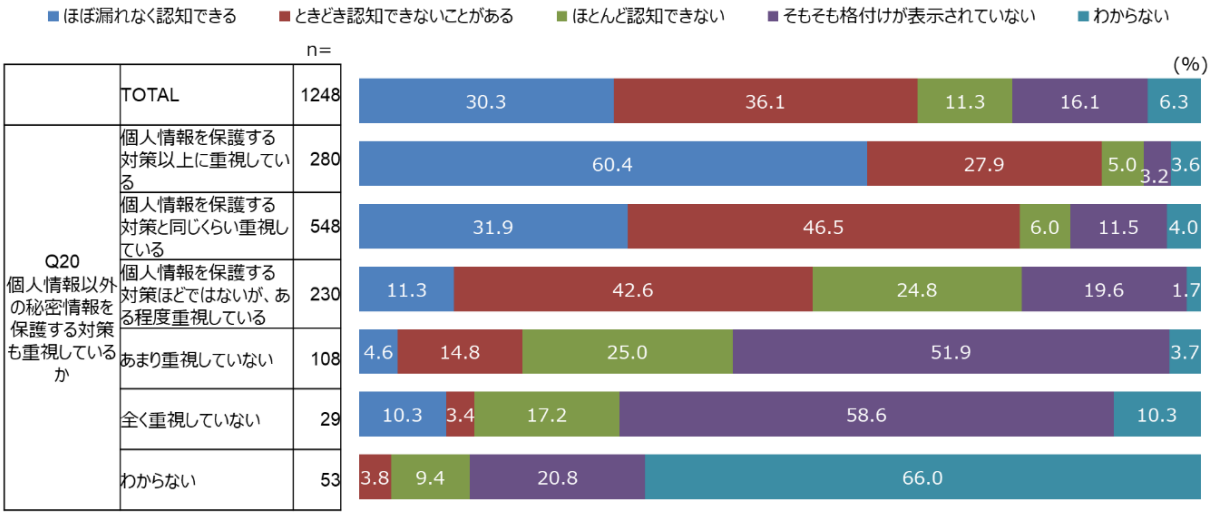
経営層が内部不正防止の基本方針をサイバーセキュリティと別建てで定めており営業秘密保護の意識が高いと見られる企業では、営業秘密等への格付け表示に実効性があるという回答割合が全体平均よりも高くなっており、格付け表示が相対的にしっかりと実践されている。但し、回答割合は 43.0%に留まっており、意識が高い組織の過半で、秘密情報をそれと認知できないことがある。（図表６６参照）

図表６６．内部不正防止とセキュリティ確保を別建てにしているかの違いによる秘密情報の認知可能状況の違い



営業秘密の保護を個人情報の保護以上に重視する組織の60.4%で、秘密情報をそれと認知できる表示等が確立している。しかし、そのような組織は 22.4%に過ぎない。情報の格付けと表示が行き届いた組織であれば従業員が営業秘密等を認識し、自身及び周囲での取扱に注意することを期待できるが、それを実践できている組織は少数派である。（図表６７参照）

図表６７．秘密情報保護対策の重視度の違いによる秘密情報の認知可能状況の違い



組織体制・連携に関する課題の改善（調査軸３）

改善策 3-1 に関する現状

【3-1】責任部門自体（リスク・コンプライアンス部門等）と関連部門（情報システム部門：対策実施部門、法務・知財部門、営業・事業部門）が協働する体制の整備を検討する。

営業秘密等の保護を個人情報保護よりも重視している企業では、すべての連携目的で全体平均よりも高い回答割合を示している。内部不正に対応する経営層や組織は、コンプライアンス・ガイドライン等の知識を補うことができる組織との連携に軸足を置くと同時に、多種多様な組織間の連携に積極的であると考えられる。（図表６８参照）

図表６８．秘密情報保護対策の重視度の違いによる経営層等の他組織との連携目的の違い

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

（%）

		n=	コンプライアンス・ガイドライン等の知識を補うため	個人情報以外の秘密情報の事業価値を評価するため	不正を生みにくい組織環境、内部通報制度等の整備ノウハウを補うため	中途退職／採用時の秘密保持義務、競業避止等に関するノウハウを補うため	リスクマネジメント、BCP、レジリエンス確保等の経験・ノウハウを補うため	サイバーセキュリティ確保、IT機器の操作ミス防止等の経験・ノウハウを補うため	他の組織と連携する必要はない	わからない
	TOTAL	1248	53.6	34.9	43.4	25.9	34.1	30.0	7.1	7.7
Q20 個人情報以外の秘密情報を保護する対策も重視しているか	個人情報を保護する対策以上に重視している	280	76.8	54.3	58.2	38.6	44.6	39.3	0.7	1.8
	個人情報を保護する対策と同じくらい重視している	548	63.3	38.7	51.1	26.1	40.5	34.9	2.9	2.4
	個人情報を保護する対策ほどではないが、ある程度重視している	230	33.0	26.1	34.8	22.6	26.1	23.5	10.9	4.3
	あまり重視していない	108	23.1	7.4	13.9	13.9	15.7	14.8	25.0	18.5
	全く重視していない	29	10.3	10.3	3.4	6.9	3.4	6.9	62.1	10.3
	わからない	53	5.7	1.9	5.7	5.7	1.9	3.8	1.9	84.9

改善策 3-3 に関する現状

【3-3】重要な秘密が不自然に取り扱われているところを目にしたら、上に報告するというリテラシーと、上に報告できない事情がある場合は内部通報ができる体制を構築する。

個人情報保護との比較において営業秘密保護を重視する度合いが高い組織ほど、秘密情報の不自然な扱いや不正な漏えいを報告する体制の整備に関する取組の回答割合が高くなる傾向がある。但し、営業秘密保護を個人情報保護以上に重視している場合でも、「経営層等に報告が上がるルートの確立」ができている組織は半分に満たない。（図表６９参照）

図表６９．秘密情報保護対策の重視度の違いによる内部通報体制／ルール整備の状況の違い

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

(%)

		n=	直属の上司にすぐに報告するルールが定められている	秘密情報の管理責任者にすぐに報告するルールが定められている	全社責任者／経営層に報告が上がるルートが確立している	内部通報体制が整備されている	わからない
	TOTAL	1248	55.0	46.6	34.4	26.3	10.6
Q20 個人情報以外の秘密情報を保護する対策も重視しているか	個人情報を保護する対策以上に重視している	280	76.1	53.9	44.6	30.0	1.1
	個人情報を保護する対策と同じくらい重視している	548	63.5	57.1	39.6	32.1	2.7
	個人情報を保護する対策ほどではないが、ある程度重視している	230	37.4	42.6	27.8	18.3	9.1
	あまり重視していない	108	28.7	13.0	16.7	17.6	30.6
	全く重視していない	29	17.2	3.4	6.9	17.2	58.6
	わからない	53	7.5	7.5	5.7	3.8	81.1

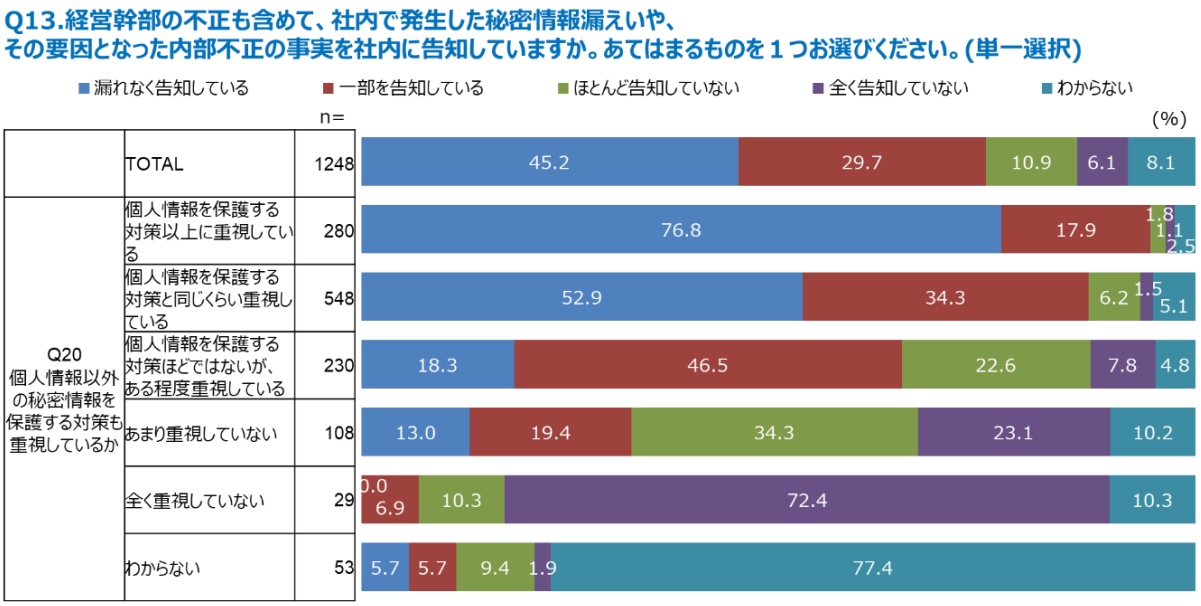
社員教育とリテラシー構築に関する課題の改善（調査軸４）

改善策 4-2 に関する現状

【4-2】入社／人事異動／退職等の重要なタイミングで、具体的に重要な秘密を示して、何をしてはいけないのか、どのような時に上への報告が必要か等を周知・徹底する。

個人情報保護との比較において営業秘密保護を重視する度合いが高い組織ほど、経営幹部のそれも含めて内部不正を全社に告知する割合が高まる。営業秘密の保護と経営層のコンプライアンスに対する厳格な姿勢は軌を一にするものになっていると解釈できる。（図表７０参照）

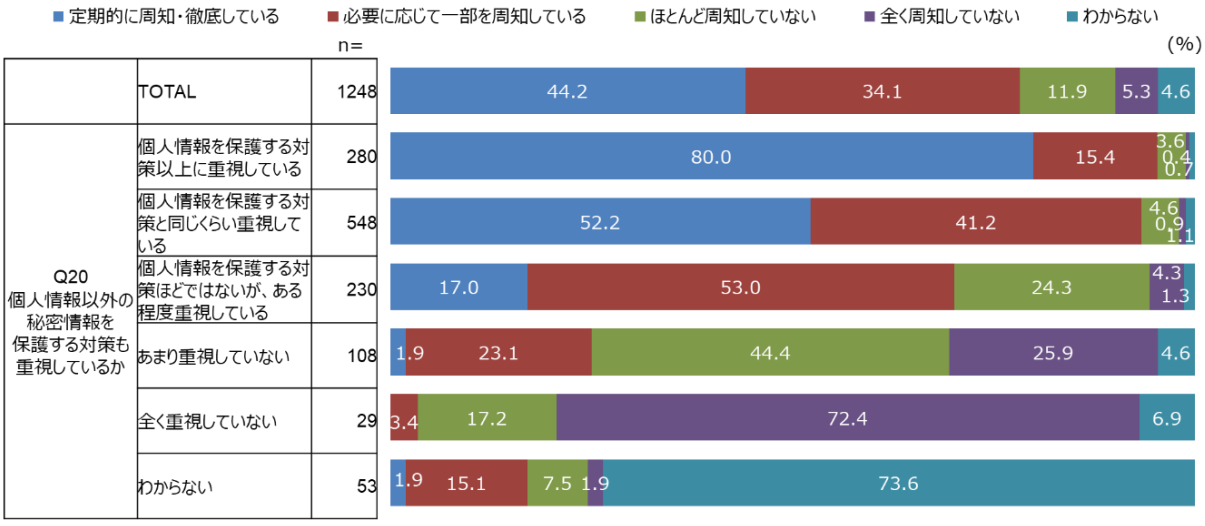
図表７０．秘密情報保護対策の重視度の違いによる秘密情報漏えい／内部不正の事実の告知状況の違い



個人情報保護との比較において営業秘密保護を重視する度合いが高い組織ほど、秘密情報の不自然な扱いや不正な漏えいを目撃した際の望ましい行動の、周知・徹底に関する回答割合が高まる。特に、営業秘密等の保護を個人情報保護以上に重視している企業の大半がその種の周知・徹底に定期的に取り組んでいる。（図表７１参照）

図表７１．秘密情報保護対策の重視度の違いによる

秘密情報の不自然な扱いや不正な漏えいを目撃した際の望ましい行動の周知状況の違い

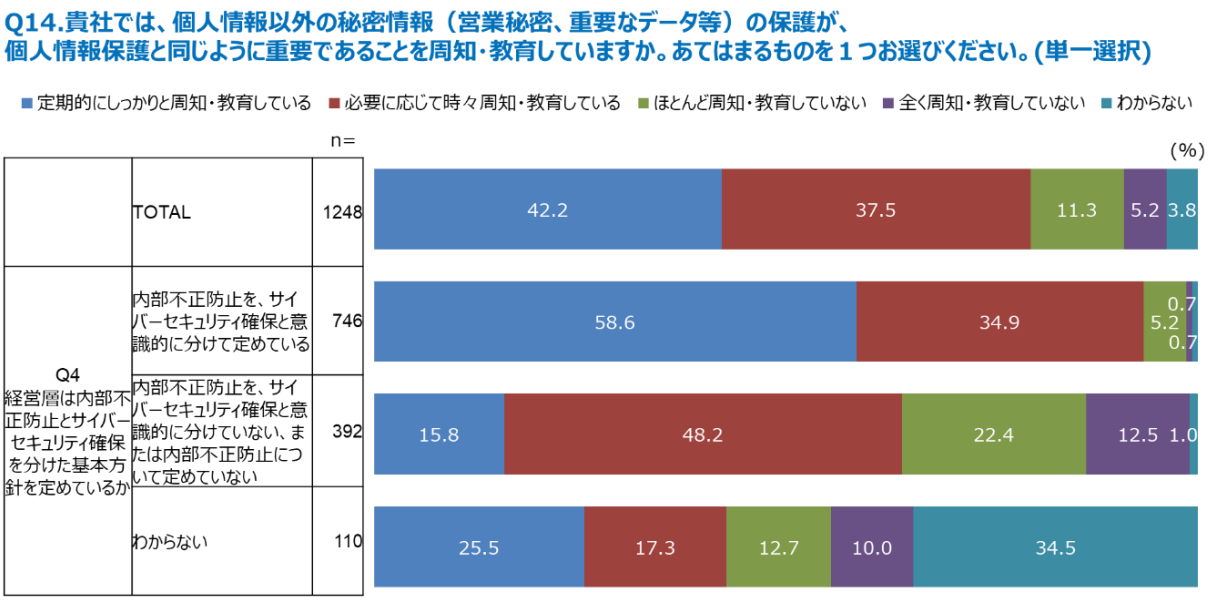


改善策 4-3 に関する現状

【4-3】事業や経営における重要性や価値、当該情報が漏えい・毀損等した場合の影響・損害などを踏まえた、秘密の重要度の判別基準を明文化した上で、この基準に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。

基本方針で内部不正防止をサイバーセキュリティと別建てにしている企業の、営業秘密等の重要性を定期的に周知・教育している割合は58.6%に達し、両者を別建てとしていない企業における 17.9%という割合の 3 倍を超え、過半を占める。事例調査が示すように「内部不正事案の多くは情報漏えいを伴う」ところ、実際の情報漏えいの対策においても、営業秘密等の漏えいが重視されていることの表れと解釈できる。（図表７２参照）

図表７２．内部不正防止とセキュリティ確保を別建てにしているかの違いによる秘密情報保護の周知・教育の状況の違い



改善策 4-5 に関する現状

【4-5】インシデント事例、解説動画・イラスト等のリッチコンテンツ、グループディスカッション、定期的な規則遵守のセルフチェック等を積極的に活用して理解を深める取組を推進すると共に、従業員に対し、営業秘密や限定提供データについて、何をしてはいけないのかを教育する。

基本方針で内部不正防止をサイバーセキュリティと別建てにしている企業の大半（75.1%）で、秘密情報等に係る違反行為を周知している。その割合は両者を別建てとしていない企業

（29.9%）の 2 倍を超える。（図表７３参照）

図表７３．内部不正防止とセキュリティ確保を別建てにしているかの違いによる禁止行為や罰則の周知状況の違い

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

（%）

		n=	社内規程等において秘密情報等に係る違反行為を周知している	違反行為に対する罰則を周知している	これまでの違反行為に係る処罰事例等を周知している	周知していない	わからない
	TOTAL	1248	56.9	38.5	25.1	15.0	4.3
Q4 経営層は内部不正防止とサイバーセキュリティ確保を分けた基本方針を定めているか	内部不正防止を、サイバーセキュリティ確保と意識的に分けて定めている	746	75.1	48.0	29.5	3.6	1.2
	内部不正防止を、サイバーセキュリティ確保と意識的に分けていない、または内部不正防止について定めていない	392	31.1	27.0	20.9	34.2	1.8
	わからない	110	25.5	15.5	10.0	23.6	34.5

個人情報保護との比較において営業秘密保護を重視する度合いが高い組織ほど、秘密情報の漏えいや内部不正に関する違反行為や罰則等を従業員に周知している割合が高い。こうすることで、教わった内容が腑に落ち、具体的な行動に繋がりやすくなる。営業秘密等の保護を個人情報保護以上に重視している企業の 88.9%が、違反行為の周知を行っている。（図表７４参照）

図表７４．秘密情報保護対策の重視度の違いによる禁止行為や罰則の周知状況の違い

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

（%）

		n=	社内規程等において秘密情報等に係る違反行為を周知している	違反行為に対する罰則を周知している	これまでの違反行為に係る処罰事例等を周知している	周知していない	わからない
	TOTAL	1248	56.9	38.5	25.1	15.0	4.3
Q20 個人情報以外の秘密情報を保護する対策も重視しているか	個人情報を保護する対策以上に重視している	280	88.9	42.1	32.9	2.1	0.4
	個人情報を保護する対策と同じくらい重視している	548	69.3	48.0	24.3	5.7	1.1
	個人情報を保護する対策ほどではないが、ある程度重視している	230	28.7	34.3	28.7	23.5	2.2
	あまり重視していない	108	11.1	16.7	18.5	56.5	1.9
	全く重視していない	29	0.0	3.4	0.0	93.1	3.4
	わからない	53	5.7	3.8	3.8	15.1	73.6

対策実施に関する課題の改善（調査軸５）

改善策 5-3 に関する現状

【5-3】重要情報漏えい防止体制の下で、サイバーセキュリティ対策と内部不正防止対策の両方に一貫して取り組む。

基本方針で内部不正防止をサイバーセキュリティと別建てにしている企業では、内部不正防止に特有の対策の実施割合が、両者を別建てとしない組織に比べて 1.5 倍から４倍になる。但し、内部不正防止に積極的な組織においても、実施割合が過半を占めるのは「不満を蓄積させない職場環境の整備」（72.5%）、「雇用開始／終了時の秘密保持義務契約／誓約書提出」（65.4%）、「人的ミスへの十分な注意指示等」（61.3%）に限られ、内部不正防止のために実施すべき対策の浸透状況は、意識の高い組織においても十分とは言い難い。（図表７５参照）

図表７５．内部不正防止とセキュリティ確保を別建てにしているかの違いによる

内部不正防止対策の取組状況の違い

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

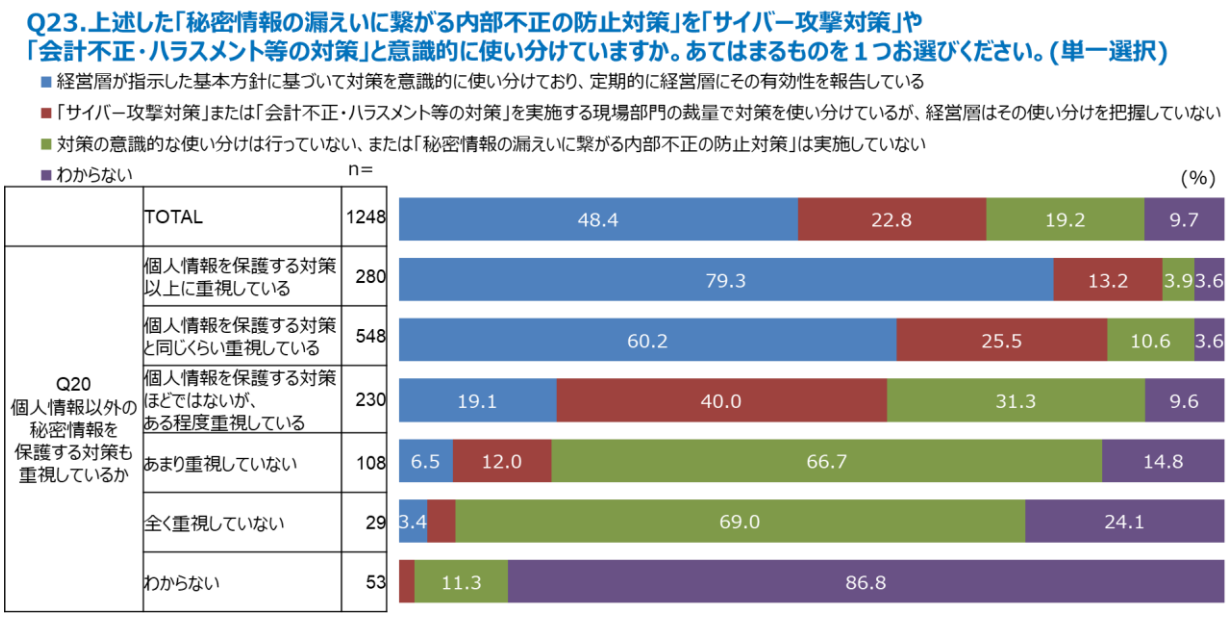
（%）

		n=	1．秘密情報の不正な開示・漏えいに繋がらないように、会社等への不満・鬱憤を蓄積させない職場環境（過度の超過勤務がない、公平に評価されるハラスメント行為がない、良好なコミュニケーションが確保されている等）を整備している	2．就業規則に従業員の秘密保持義務を明記し、雇用開始時、及び雇用終了時に秘密保持義務に関する契約または誓約書の提出を求めている	3．重要な秘密情報を取り扱うプロジェクトへの参加／離任にあたり、秘密保持義務に関する誓約書を提出することを義務付けている	4．人的ミス（電子メールの誤送信、PC／USBメモリの紛失セキュリティ設定ミス等）への十分な注意を指示・徹底している	5．社内システム等の操作の異常や不正の可能性（深夜や休日の操作大量のファイルダウンロードなど）を、ログに基づいて定期的に確認している	6．中途退職を予定している従業員については、過去に遡って5．のログ確認を実施している	7．5．や6．の対策実施を従業員に周知し、不正の抑止力として役立てている	8．秘密情報の漏えいに繋がる内部不正に対する罰則を定めて、社員教育等で従業員に周知・徹底している	9．テレワークやクラウドサービスで取り扱うことができる秘密情報を制限するための基準を設け、社員教育等で従業員に周知・徹底している	10．不必要な秘密情報を取引先等に渡さないように、社員教育等で従業員に周知・徹底している	11．秘密情報の漏えいに繋がる内部不正の防止対策は実施していない	12．わからない
	TOTAL	1248	57.6	54.4	25.6	50.5	36.2	17.0	14.9	23.2	33.7	32.4	6.8	6.1
Q4 経営層は内部不正防止とサイバーセキュリティ確保を分けた基本方針を定めているか	内部不正防止を、サイバーセキュリティ確保と意識的に分けて定めている	746	72.5	65.4	32.6	61.3	47.7	24.7	21.3	30.6	47.5	39.7	1.1	1.3
	内部不正防止を、サイバーセキュリティ確保と意識的に分けていない、または内部不正防止について定めていない	392	38.3	43.1	16.3	39.0	21.4	6.1	6.4	13.5	15.1	24.2	16.8	4.1
	わからない	110	25.5	20.0	11.8	18.2	10.9	3.6	1.8	7.3	6.4	11.8	10.0	45.5

個人情報保護との比較において営業秘密保護を重視する度合いが高い組織ほど、内部不正防止対策をサイバー攻撃対策や会計不正・ハラスメント等の対策と意識的に使い分けていると回答する割合が高まる。営業秘密等の保護を個人情報保護以上に重視している企業の大半がこれらを使い分け、更に、定期的に経営層にその有効性を報告している。（図表７６参照）

図表７６．秘密情報保護対策の重視度の違いによる

内部不正防止対策をサイバー攻撃対策等と意識的に使い分けているかの違い



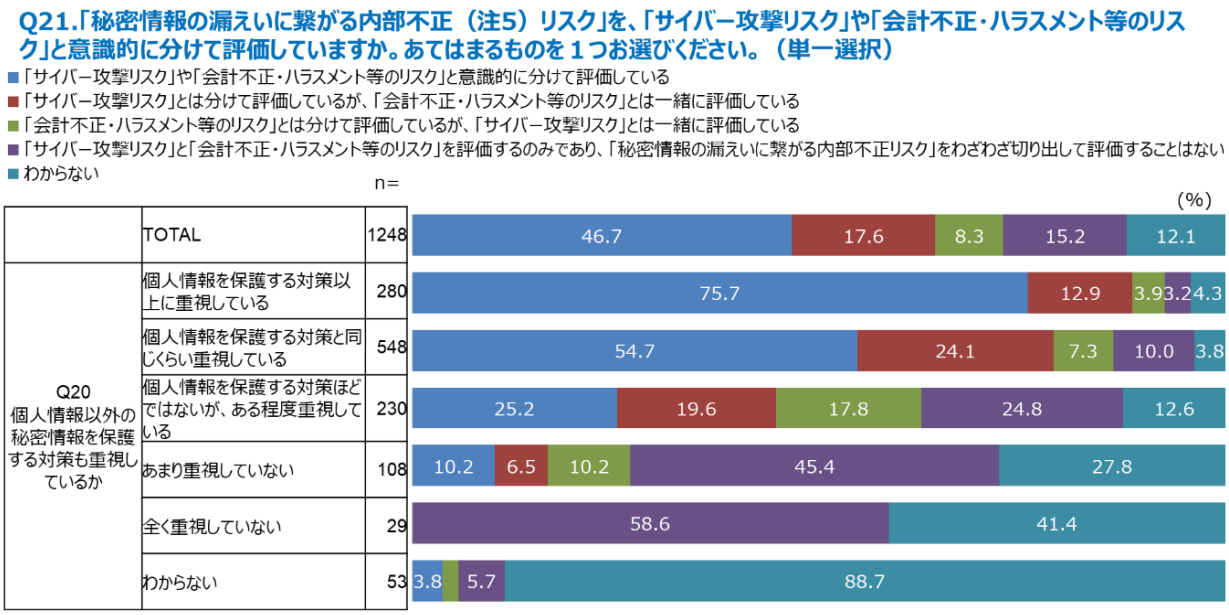
改善策 5-4 に関する現状

【5-4】 内部不正のリスクシナリオも加味して重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。この際には、不正に対する人的・組織的対策と技術的対策のバランスの適正化を考慮する。また、経営層の不正防止と透明性確保、アクセスログの確認範囲拡大、他社の重要情報の不正な社内持ち込み防止、重要プロジェクト就任／離任時にも秘密保持義務の誓約書を取得、重要性の高い秘密に触れる場合の誓約書の詳細度の変更等を実施する。

個人情報保護との比較において営業秘密保護を重視する度合いが高い組織ほど、内部不正のリスクをサイバー攻撃や会計不正・ハラスメント等のリスクと分けて評価する割合が高まる。営業秘密等の保護を個人情報保護以上に重視している企業の大半がこれらを分けている。（図表７７参照）

図表７７．秘密情報保護対策の重視度の違いによる

内部不正リスクをサイバー攻撃リスク等と意識的に分けて評価しているかの違い

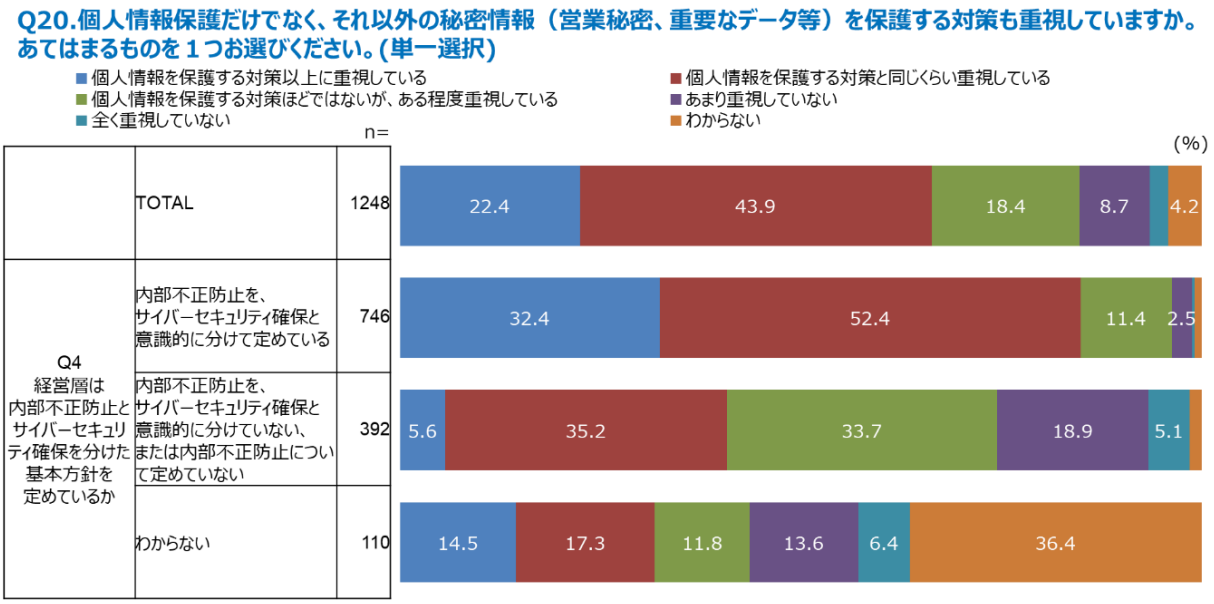


改善策 5-5 に関する現状

【5-5】個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。

基本方針で内部不正防止をサイバーセキュリティと別建てにしている企業では、営業秘密等を保護する対策を個人情報保護と同等以上に重視している割合（84.8%）が、両者を別建てにしていない企業（38.8%）の 2 倍を超え、大半を占める。これに対し、内部不正防止とサイバーセキュリティとを必ずしも分けていない企業においては、個人情報保護を重視する回答割合とそれ以外の秘密情報保護を重視する回答割合とが概ね拮抗しており、営業秘密等の保護を重視することが内部不正防止を別建てにすることと強く結びついていると解釈できる。（図表７８参照）

図表７８．内部不正防止とセキュリティ確保を別建てにしているかの違いによる秘密情報保護対策の重視度の違い



②中小企業の構造的課題の改善（調査軸６の１～５）

経営課題の改善（調査軸６の１）

改善策 6-1-1 に関する現状

【6-1-1】経営層または内部不正防止に関する組織全体の責任者等が率先して、重要な秘密情報漏えい／内部不正リスクを重要な経営課題として認識する機会を増やし、サイバーセキュリティ確保と内部不正防止を一体的に認識した経営を行う。

中小企業では、秘密情報漏えいに関する経営層のリスク認識が大企業も含めた全体平均と比べて全般に低い。（図表７９参照）

図表７９．常用雇用者数の違いによる秘密情報漏えいのリスク認識の違い

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

（%）

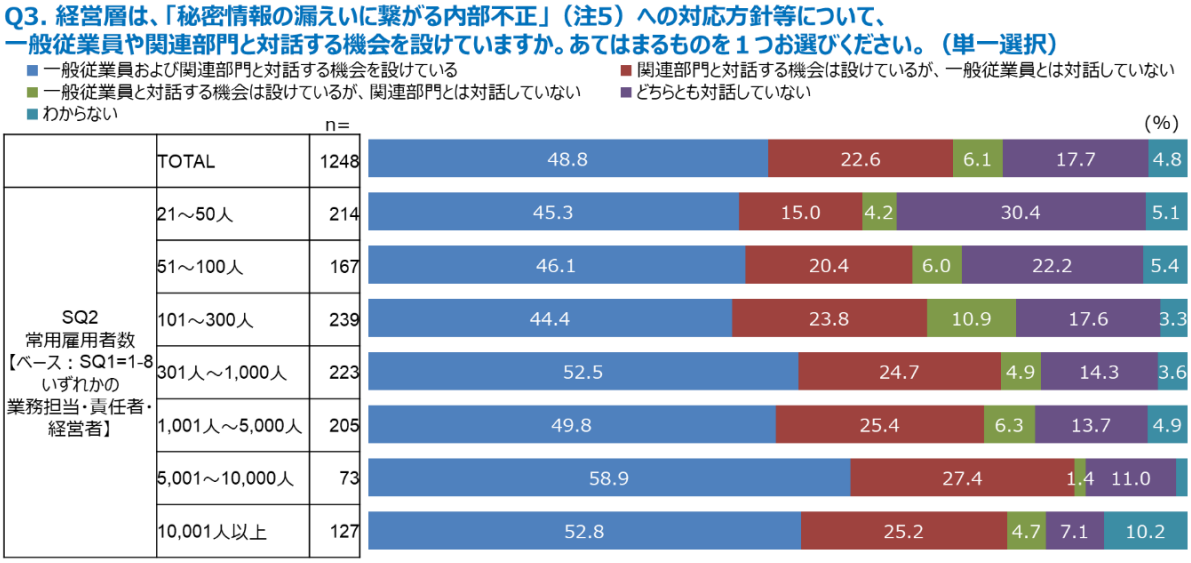
		n=	（過度の超過勤務、不公平な評価、ハラスメント等に対して）不満を蓄積した従業員による秘密情報の漏えい	産業スパイによる秘密情報の漏えい	中途退職者による秘密情報の漏えい	電子メールの誤送信、PCやUSBメモリの紛失等の人的ミスによる秘密情報の漏えい	クラウドサービスからの秘密情報の漏えい	国内の取引先または国内子会社からの秘密情報の漏えい	海外の取引先または海外子会社からの秘密情報の漏えい	テレワークによる秘密情報の漏えい	サイバー攻撃による秘密情報の漏えい	秘密情報の漏えいや、それに関わる内部不正に関するリスクをあまり重視していない	わからない
	TOTAL	1248	42.2	17.2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

改善策 6-1-2 に関する現状

【6-1-2】中小企業では、全社集会などの経営層が従業員に周知徹底する機会を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。

企業規模が小さくなるほど、秘密情報の漏えいにつながる内部不正に関して、経営層と一般従業員・関連部門の対話を設けているとする回答割合が下がる。（図表８０参照）

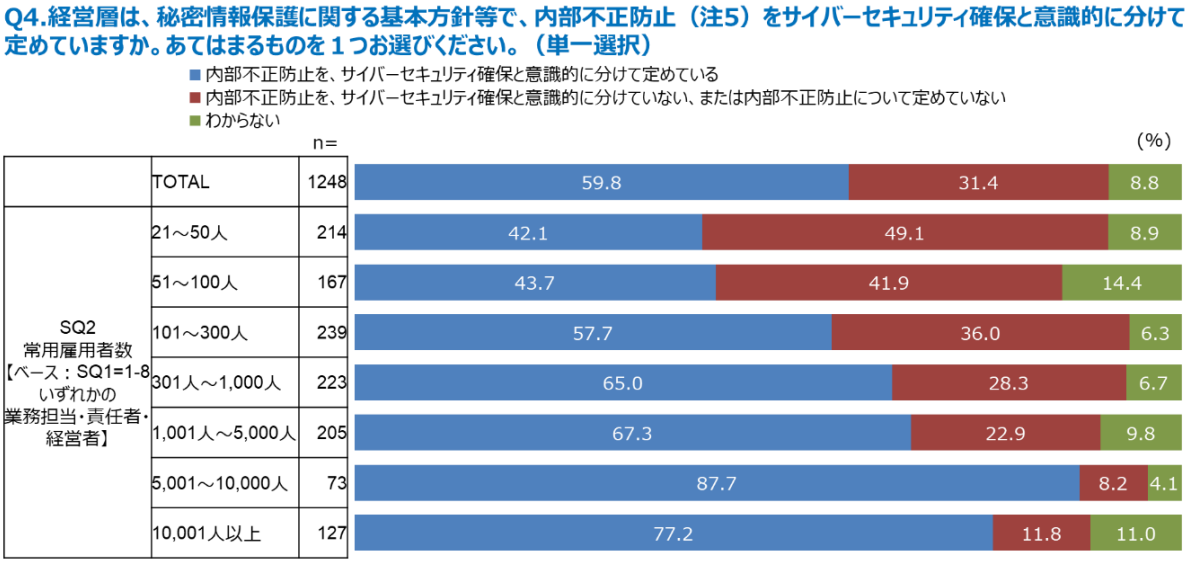
図表８０．常用雇用者数の違いによる経営層のリーダーシップ発揮の違い



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

内部不正防止をサイバーセキュリティ確保とは意識的に分けて扱う企業の割合は従業員数が増えるほど高まる。大企業では両者を分けるという組織が過半あるいは大半を占めるのに対し、従業員 100 名以下の企業では両者を分けるかどうかが概ね拮抗している。（図表８１参照）

図表８１．常用雇用者数の違いによる内部不正防止とセキュリティ確保を別建てにしているかの違い



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

重要な秘密の特定と取扱いの改善（調査軸６の２）

改善策 6-2-1 に関する現状

【6-2-1】中小企業では、経営層が自ら判断する、あるいは判断基準を示すことで、自社の事業にとって重要性／機密性の高い秘密情報を的確に特定する。

若干の例外はあるが、従業員数が小さくなるほど、個人情報以外の秘密情報の特定・格付け・表示に関する取組の実施率が低下する。（図表８２参照）

図表８２．常用雇用者数の違いによる秘密情報の特定と格付けの実効性を高めるための取組の違い

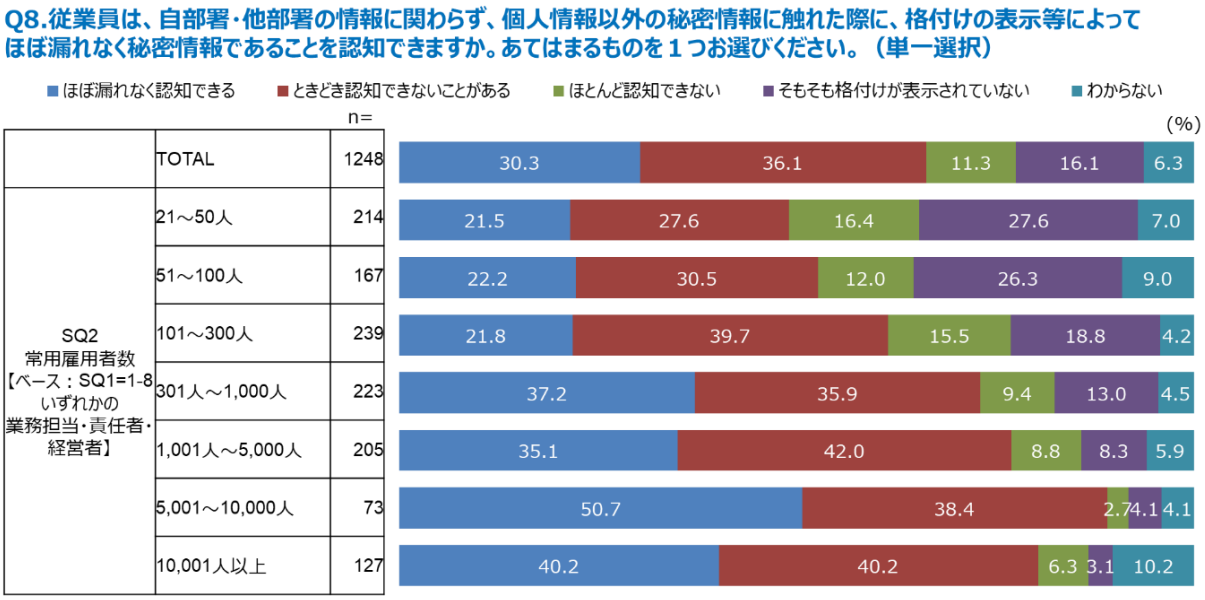
Q7.個人情報以外の秘密情報（営業秘密、重要なデータ等）の特定と格付けの実効性を高めるために、組織全体でどのような取組を実施していますか。あてはまるものをすべてお選びください。（複数選択）

（%）

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

中小企業において秘密情報をそれと認知できるような格付け・表示等がなされている割合は20%前後であり、少数派である。大企業ではこの割合が最低でも 35%には達しており、取組の度合いに明白な違いがある。（図表８３参照）

図表８３．常用雇用者数の違いによる秘密情報の認知可能状況の違い



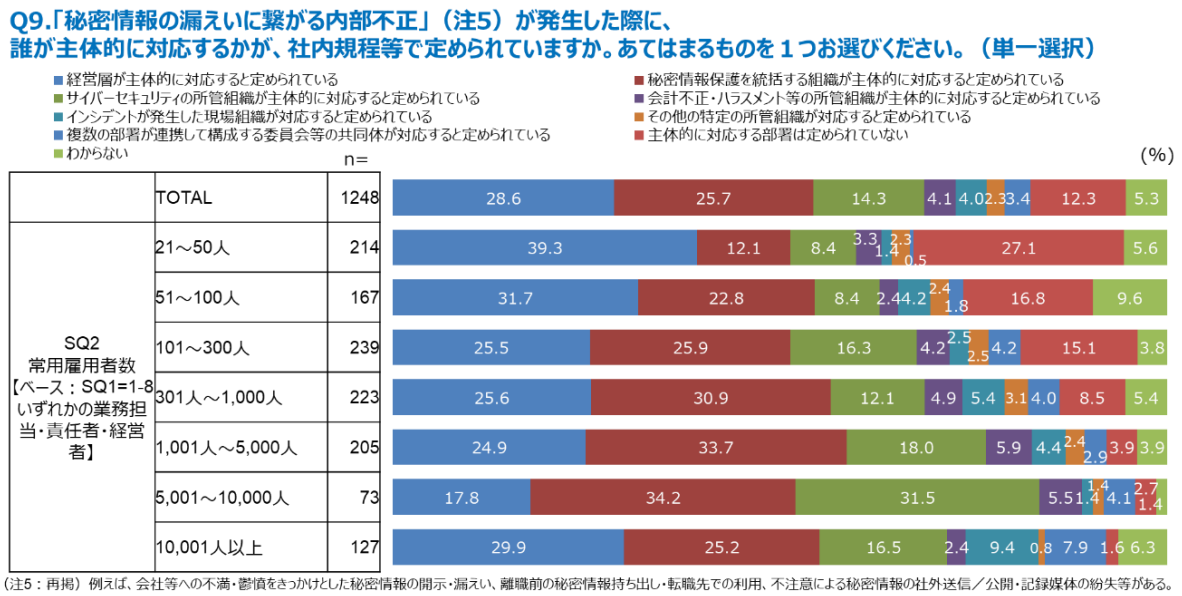
組織体制・連携に関する課題の改善（調査軸６の３）

改善策 6-3-1 に関する現状

【6-3-1】中小企業では、責任者である経営層が中心となって、総務・人事・法務や情報システム等の関連部門との調整を行う。

秘密情報の漏えいに繋がる内部不正に経営層が主体的に対応するとの回答割合は、従業員数が増すほど低下するが、従業員数 10,001 人以上のとりわけ大きな企業においては逆に割合が増す。この傾向と軌を一にして、従業員数が増すほど、所定の統括組織が主体的に対応するとの回答割合が高まる。（図表８４参照）

図表８４．常用雇用者数の違いによる内部不正発生時の対応者の違い



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

改善策 6-3-3 に関する現状

【6-3-3】重要な秘密が不自然に取り扱われている様を目撃した際に上に報告することの徹底と、上に報告できない事情がある場合は内部通報ができる体制を構築する。

従業員数と、秘密情報の不自然な扱いや不正な漏えいを報告するルール等を定めているとの回答割合は連動しており、前者が増えるほど後者も高まる。中小企業では従業員と経営層の距離は大企業に比べて近いはずだが、経営層へと報告が上がるルートの確立度合いは大企業が勝る。（図表８５参照）

図表８５．常用雇用者数の違いによる内部通報体制／ルール整備の状況の違い

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

(%)

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

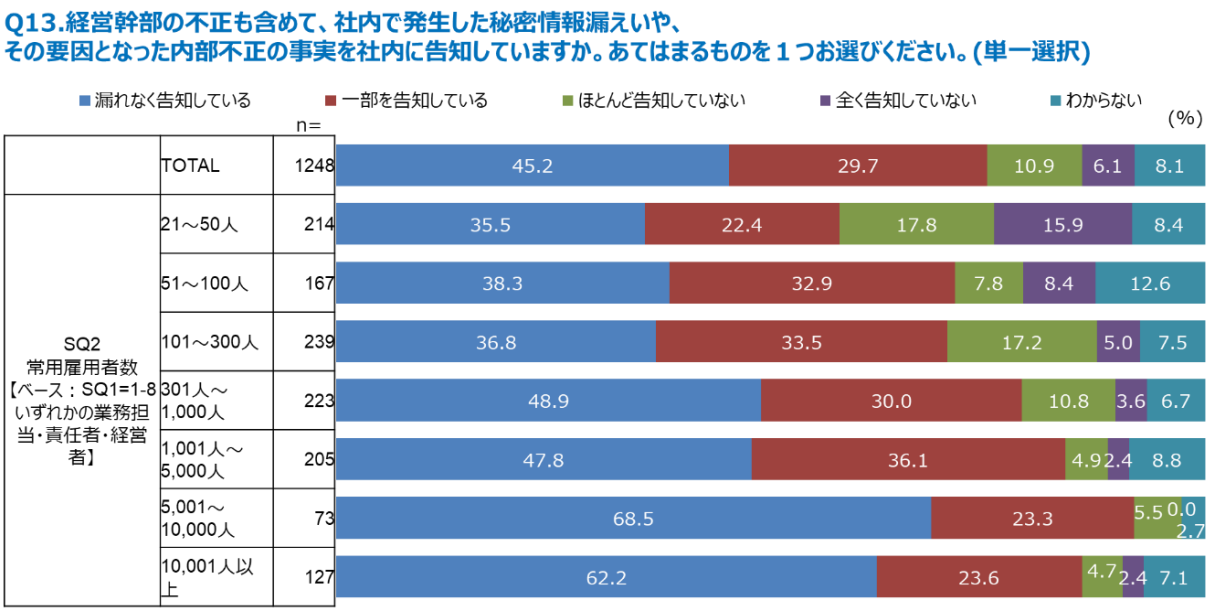
社員教育とリテラシー構築に関する課題の改善（調査軸６の４）

改善策 6-4-2 に関する現状

【6-4-2】中小企業では、入社／人事異動／退職等の重要なタイミングで、経営層が重要な秘密を具体的に示し、その取扱い指示を徹底する。

経営幹部のそれも含め、発生した内部不正を全社に告知しているとする回答割合は従業員数に連動しており、中小企業では告知される割合が 40%に満たない。（図表８６参照）

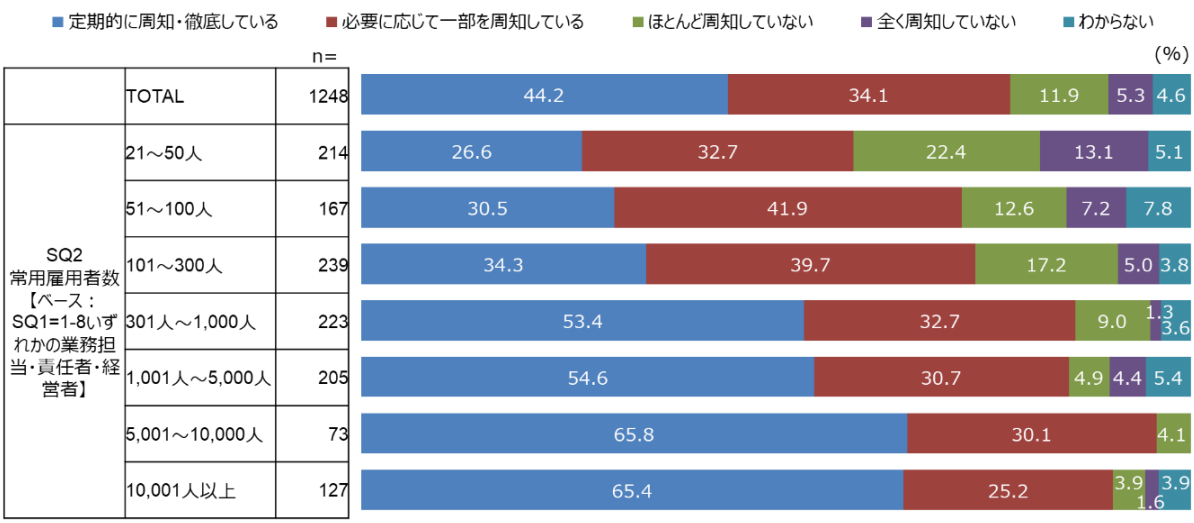
図表８６．常用雇用者数の違いによる秘密情報漏えい／内部不正の事実の告知状況の違い



秘密情報の不自然な扱いや不正な漏えいを目撃した際の望ましい行動を定期的に周知・徹底している割合は、従業員数が増すほど高まる。従業員数が 100 名以下の企業においては該当するのはほぼ少数派と言ってよい。（図表８７参照）

図表８７．常用雇用者数の違いによる

秘密情報の不自然な扱いや不正な漏えいを目撃した際の望ましい行動の周知状況の違い

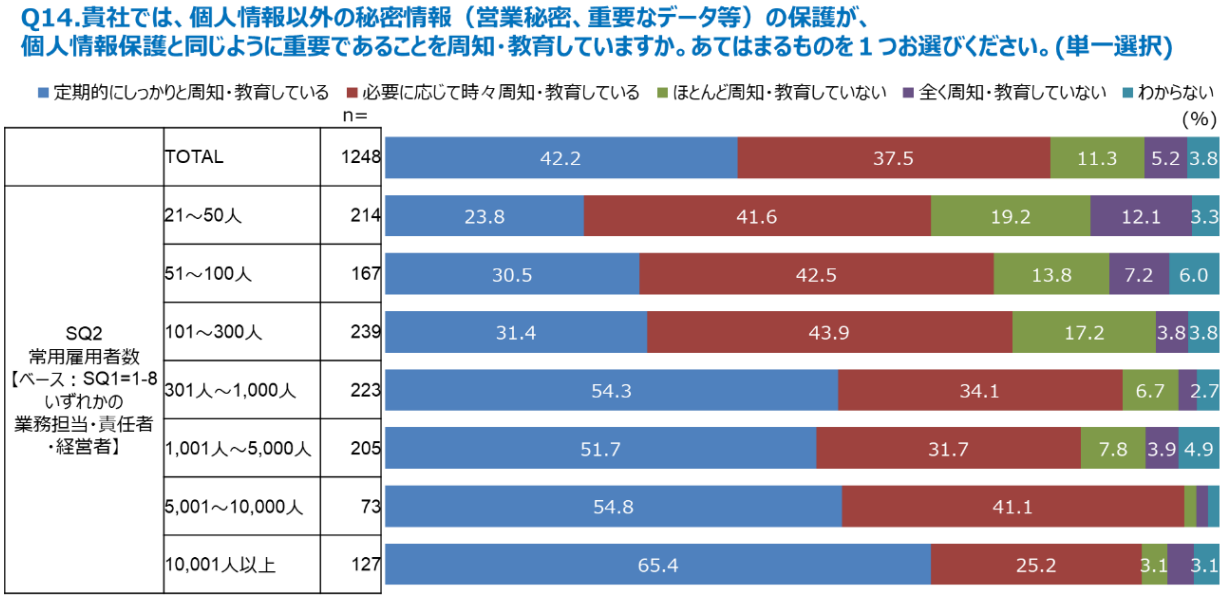


改善策 6-4-3 に関する現状

【6-4-3】経営層または経営層が権限を移譲した責任者が各々の秘密の重要度を指定した上で、この指定に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。

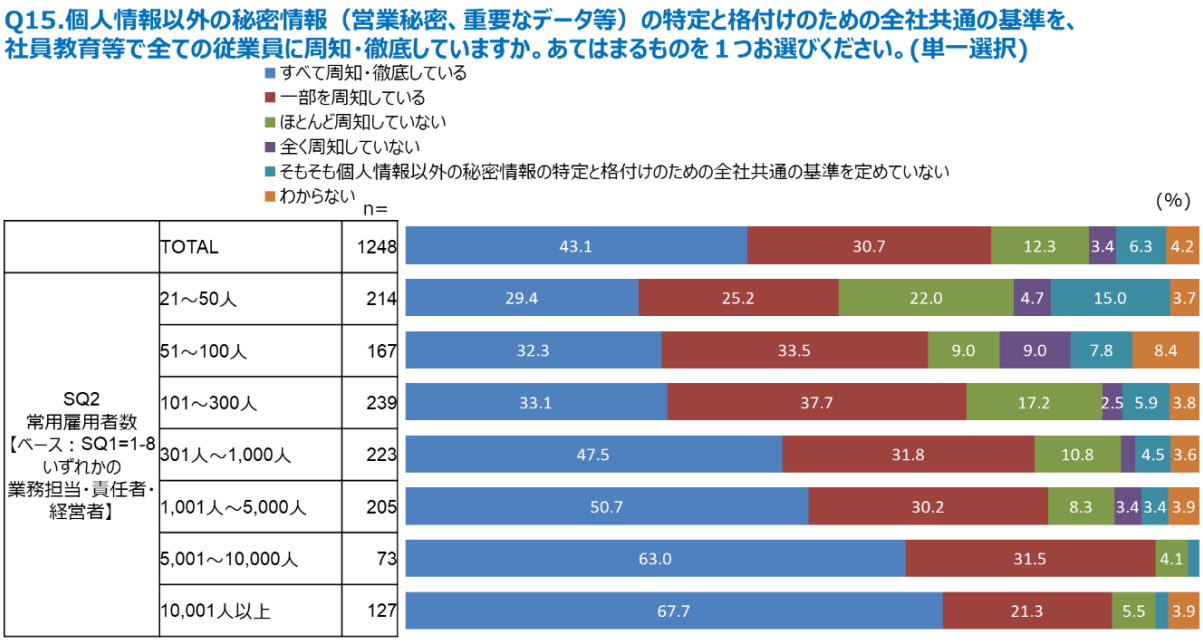
営業秘密等の重要性を定期的に周知・教育している割合は従業員数に連動しており、若干のぶれはあるものの、従業員数が増すほど取組の実施率も高まる。大企業では過半で定期的な取組があるのに対し、該当する中小企業はほぼ少数派である。（図表８８参照）

図表８８．常用雇用者数の違いによる秘密情報保護の周知・教育の状況の違い



個人情報以外の秘密情報の特定と格付けの全社基準を周知・教育している割合は従業員数が増すほど高まる。大企業ではほぼ過半がすべてを周知・徹底しているとするのに対し、該当する中小企業はほぼ少数派である。（図表８９参照）

図表８９．常用雇用者数の違いによる秘密情報の特定と格付けのための全社共通基準の周知状況の違い



改善策 6-4-5a に関する現状

【6-4-5a】中小企業では、経営層が自ら事業リスクに基づいて、営業秘密や限定提供データの取り扱いについて何をしてはいけないのかを指示・啓発する。

内部不正にあたる違反行為や罰則の定めを周知している割合は従業員数が減るほど下がる。中小企業において秘密情報等に係る違反行為を周知している企業は半数に満たず、より大きな規模の企業では逆に過半が周知していることと対照的である。（図表９０参照）

図表９０．常用雇用者数の違いによる禁止行為や罰則の周知状況の違い

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

(%)

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

改善策 6-4-5b に関する現状

【6-4-5b】中小企業では、経営層が全社集会などで直接従業員に教育・意識づけする。

e-Learning 以外の方法を取り入れている割合は従業員数が減るほど下がる。インシデント事例の説明が最もよくある取組で、これに規則順守のセルフチェックが続く。いずれも中小企業における実施率は４割に満たず、大企業とは対照的である。（図表９１参照）

図表９１．常用雇用者数の違いによる秘密情報漏えいや内部不正防止の従業員教育の状況の違い

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

(%)

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

対策実施に関する課題の改善（調査軸６の５）

改善策 6-5-3 に関する現状

【6-5-3】中小企業では、重要情報漏えいの防止体制の下で、サイバーセキュリティと内部不正防止の両方に共通する対策を積極的に１つにまとめる。

秘密保持義務契約／誓約を求めている企業の割合は従業員数が小さくなるほど下がる。ただし、本調査で一番小さな企業規模に対応する従業員数 21～50 名の場合でも 41.6%の実施率となっており、過半における実施を達成するまでの差異はログ確認のような他の対策に比べて小さい。（図表９２参照）

図表９２．常用雇用者数の違いによる内部不正防止対策の取組状況の違い

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

（%）

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

従業員数が増えるほど、内部不正防止対策と、サイバー攻撃や会計不正・ハラスメント等の対策とを意識的に使い分ける傾向がある。大企業では過半が使い分けを行うのに対し、該当する中小企業は半数に満たない。（図表９３参照）

図表９３．常用雇用者数の違いによる

内部不正防止対策をサイバー攻撃対策等と意識的に使い分けているかの違い

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

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

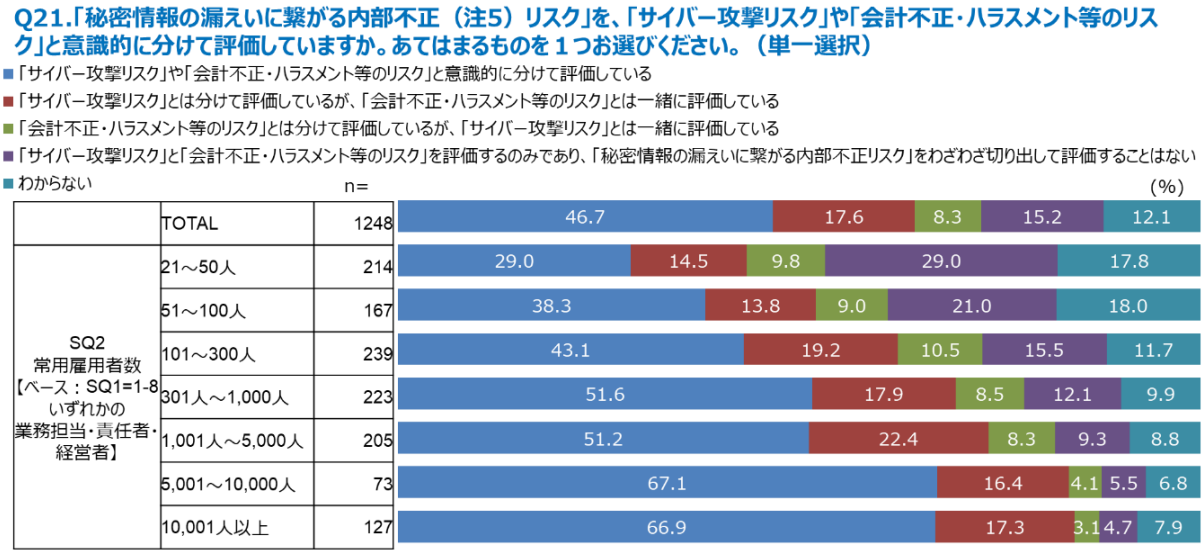
		n=	経営層が指示した基本方針に基づいて対策を意識的に使い分けており、定期的に経営層にその有効性を報告している	「サイバー攻撃対策」または「会計不正・ハラスメント等の対策」を実施する現場部門の裁量で対策を使い分けているが、経営層はその使い分けを把握していない	対策の意識的な使い分けは行っていない、または「秘密情報の漏えいに繋がる内部不正の防止対策」は実施していない	わからない
	TOTAL	1248	48.4	22.8	19.2	9.7
SQ2 常用雇用者数【ベース：SQ1=1-8いずれかの業務担当・責任者・経営者】	21～50人	214	34.6	15.4	39.3	10.7
	51～100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

改善策 6-5-4 に関する現状

【6-5-4】内部不正のリスクシナリオを加味した重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。

内部不正リスクをサイバー攻撃リスク等と意識的に分けて評価している割合は、従業員数が小さくなるほど下がる。大企業では過半が両者を分けるのに対し、該当する中小企業は半数に満たない。（図表９４参照）

図表９４．常用雇用者数の違いによる
内部不正リスクをサイバー攻撃リスク等と意識的に分けて評価しているかの違い



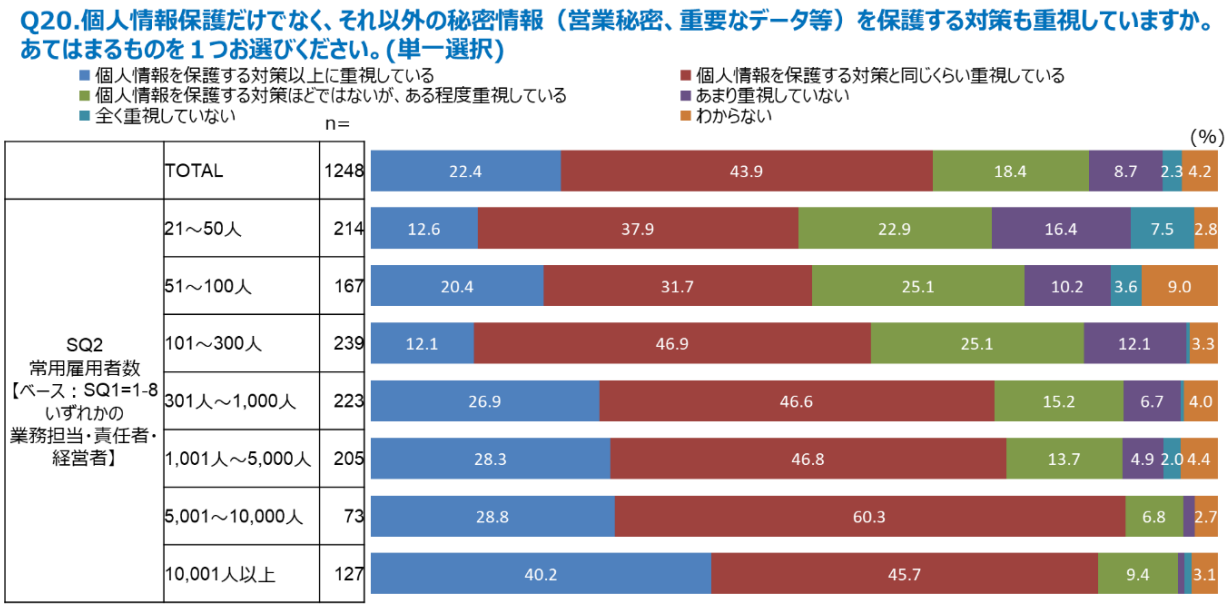
（注5：再掲）例えば、会社等への不満・鬱憤をきっかけとした秘密情報の開示・漏えい、離職前の秘密情報持ち出し・転職先での利用、不注意による秘密情報の社外送信／公開・記録媒体の紛失等がある。

改善策 6-5-5 に関する現状

【6-5-5】個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。

個人情報保護との比較において営業秘密等を保護する対策を同等以上に重視している割合は従業員数が小さくなるほど下がる。中小企業においては、これらの秘密情報の保護をあまり重視していないとする回答も 1 割を超えており、逆に 1 割を超えることのない大企業の傾向と対照的である。（図表９５参照）

図表９５．常用雇用者数の違いによる秘密情報保護の対策の重視度の違い

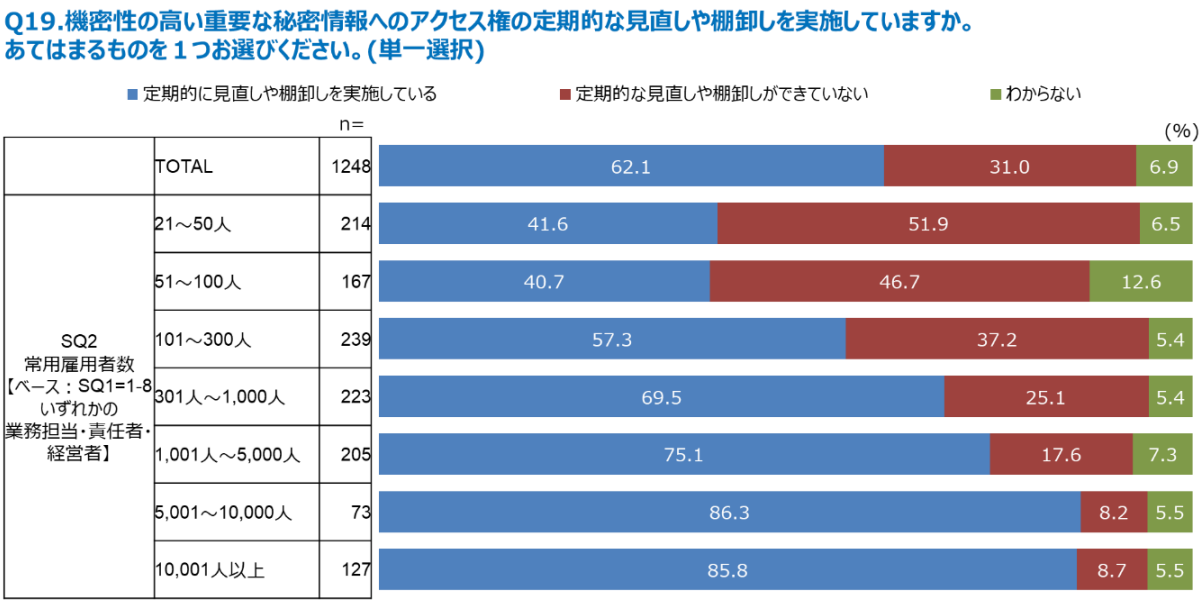


改善策 6-5-6 に関する現状

【6-5-6】情報機密区分に応じたアクセス権限付与状況の点検、アクセス権限付与者についての定期的な棚卸しを実施する。

資産管理している秘密情報を定期的に見直す、あるいは棚卸しを行っている割合は従業員数が小さくなるほど下がる。特に、従業員数が 100 人以下の企業では定期的な対応ができていないとする回答の方が多い。（図表９６参照）

図表９６．常用雇用者数の違いによる秘密情報へのアクセス権の見直し／棚卸しの取組み状況の違い



③ガイドラインの利用と実践に関する課題の改善（調査軸７）

改善策 7-2 に関する現状

【7-2】概要版の作成、活用しやすい情報量の調整・表現の工夫、社内規程整備のために活用しやすい内容の増補、従業員への周知・教育にそのまま使えるコンテンツの充実等を検討し、「組織における内部不正防止ガイドライン」適用の実効性を高める。

「組織における内部不正防止ガイドライン」の活用については、エレクトロニクス関係の製造業、基幹インフラ、ネットサービス業、繊維工業等で、活用している割合が全体平均と比べて高くなっている。一方で、他の製造業、卸売・小売業、サービス業等では、活用している割合が全体平均と比べて低い。この違いの原因がどこにあるのかを本調査で分析することは難しい。（図表９７参照）

図表９７．回答者の業種の違いによるガイドラインの活用状況の違い

	n=	経営層への報告や説明の根拠として活用	社内規程への反映	従業員教育用のコンテンツとして利用	それ以外	特段活用していない	組織における内部不正防止ガイドラインを知らない	わからない
TOTAL	1248	40.1	52.4	37	0.2	15.1	6.7	7.8
1．農業、林業、漁業	3	33.3	66.7	33.3	0	33.3	0	0
2．鉱業、採石業、砂利採取業	3	0	66.7	33.3	0	33.3	0	0
3．建設業	68	39.7	58.8	36.8	0	13.2	7.4	5.9
4．食料品製造業	45	26.7	55.6	26.7	0	17.8	8.9	8.9
5．飲料・たばこ・飼料製造業	11	18.2	54.5	36.4	0	9.1	9.1	0
6．繊維工業	14	42.9	71.4	28.6	0	14.3	7.1	7.1
7．化学工業	31	29	61.3	32.3	0	25.8	0	0
8．プラスチック製品製造業	8	12.5	62.5	37.5	0	12.5	12.5	12.5
9．ゴム製品製造業	7	28.6	42.9	71.4	0	0	28.6	0
10．鉄鋼業	17	52.9	47.1	35.3	0	17.6	5.9	11.8
11．はん用機械器具製造業	6	33.3	83.3	16.7	0	0	16.7	0
12．生産用機械器具製造業	25	44	44	60	0	20	4	0
13．業務用機械器具製造業	20	35	60	40	0	5	5	20
14．電子部品・デバイス・電子回路製造業	52	53.8	61.5	53.8	0	1.9	0	9.6
15．電子応用装置・電気計測器製造業	12	66.7	66.7	41.7	0	8.3	0	0
16．15以外の電気機械器具製造業	30	30	73.3	43.3	0	13.3	3.3	0
17．情報通信機械器具製造業	7	42.9	42.9	28.6	0	0	0	28.6
18．自動車・同附属部品製造業	35	45.7	45.7	48.6	0	17.1	5.7	11.4
19．18以外の輸送用機械器具製造業	12	41.7	75	41.7	0	0	0	8.3
20．4～19以外の製造業	89	25.8	44.9	28.1	1.1	21.3	7.9	13.5
21．電気・ガス・熱供給・水道業	24	41.7	70.8	41.7	0	12.5	4.2	4.2
22．通信業	22	59.1	63.6	36.4	0	9.1	0	4.5
24．情報サービス業	156	48.7	57.1	42.3	0.6	12.8	5.1	6.4
25．インターネット附随サービス業	23	56.5	65.2	47.8	0	4.3	4.3	0
26．映像・音声・文字情報制作業	4	25	25	0	0	25	25	25
27．運輸業、郵便業	51	39.2	27.5	37.3	0	23.5	11.8	7.8
28．卸売業、小売業	116	38.8	49.1	37.9	0.9	17.2	9.5	6
29．金融業、保険業	68	48.5	58.8	41.2	0	8.8	8.8	7.4
30．不動産業、物品賃貸業	45	44.4	46.7	40	0	20	4.4	8.9
31．学術研究、専門・技術サービス業	36	38.9	52.8	30.6	0	16.7	2.8	8.3
32．宿泊業、飲食サービス業	26	53.8	50	42.3	0	11.5	3.8	7.7
33．31、32以外のサービス業	153	31.4	41.2	25.5	0	19	11.1	9.8
34．公務（他に分類されるものを除く）	3	33.3	66.7	33.3	0	0	0	33.3
35．分類不能の産業	26	46.2	42.3	23.1	0	19.2	3.8	11.5

営業秘密保護を個人情報保護以上に重視している企業では、ガイドラインを活用している割合が全体平均と比べて高い。特に、「経営層への報告や説明の根拠」「社内規程への反映」「従業員教育用のコンテンツ」としての活用では、いずれも過半を占める。回答割合はそれぞれ71.8%、68.9%、52.5%に達している。ガイドラインの重点は元々個人情報保護にあったが、第５版改訂時に営業秘密保護も重視することに転換した。この方針転換は妥当であったと判断できる傍証の１つと言える。（図表９８参照）

図表９８．秘密情報保護対策の重視度の違いによるガイドラインの活用状況の違い

Q24.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」をどのように活用していますか。あてはまるものをすべてお選びください。(複数選択)

(%)

		n=	経営層への報告や説明の根拠として活用	社内規程への反映	従業員教育用のコンテンツとして利用	それ以外	特段活用していない	組織における内部不正防止ガイドラインを知らない	わからない
	TOTAL	1248	40.1	52.4	37.0	0.2	15.1	6.7	7.8
Q20 個人情報以外の秘密情報を保護する対策も重視しているか	個人情報を保護する対策以上に重視している	280	71.8	68.9	52.5	0.0	2.9	1.1	1.8
	個人情報を保護する対策と同じくらい重視している	548	44.0	62.2	43.1	0.4	13.5	3.1	4.4
	個人情報を保護する対策ほどではないが、ある程度重視している	230	20.0	42.6	27.8	0.4	22.2	9.6	6.5
	あまり重視していない	108	8.3	19.4	13.0	0.0	36.1	24.1	7.4
	全く重視していない	29	3.4	0.0	0.0	0.0	37.9	37.9	20.7
	わからない	53	5.7	1.9	1.9	0.0	9.4	9.4	73.6

中小企業であっても、「組織における内部不正防止ガイドライン」を知らない企業は少ない。しかし、中小企業ではガイドラインを活用している割合が全体平均と比べて低い。特に、従業員数が 50 人以下の中小企業では、格段に低くなっている。この結果を踏まえると、中小企業がガイドラインを活用しやすい環境整備のあり方をさらに検討する必要があると考える。（図表９９参照）

図表９９．常用雇用者数の違いによるガイドラインの活用状況の違い

Q24.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」をどのように活用していますか。あてはまるものをすべてお選びください。(複数選択)

(%)

		n=	経営層への報告や説明の根拠として活用	社内規程への反映	従業員教育用のコンテンツとして利用	それ以外	特段活用していない	組織における内部不正防止ガイドラインを知らない	わからない
	TOTAL	1248	40.1	52.4	37.0	0.2	15.1	6.7	7.8
SQ2 常用雇用者数【ベース：SQ1=1-8 いずれかの業務担当・責任者・経営者】	21～50人	214	32.7	36.4	19.2	0.0	24.3	13.1	8.4
	51～100人	167	28.7	41.3	33.5	0.0	18.0	12.6	10.2
	101～300人	239	32.6	51.5	31.4	0.0	18.0	5.0	6.7
	301人～1,000人	223	45.3	54.3	40.8	0.4	16.6	4.5	5.4
	1,001人～5,000人	205	47.8	62.0	43.9	0.5	7.3	4.4	10.2
	5,001～10,000人	73	53.4	74.0	60.3	1.4	6.8	1.4	4.1
	10,001人以上	127	52.8	64.6	51.2	0.0	4.7	2.4	7.9

(4) 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、共通の調査軸ごとに設定された各改善策について、アンケート調査結果（単純集計、クロス集計）、インタビュー調査結果（中小企業の経営者・幹部等、有識者）を比較している。まず分析結果を「改善策と現状の比較」として示した上で、分析の材料を「改善策」「現状」「改善策を補う示唆」「好事例」の４つの観点で整理して表にまとめた。

①全体的な課題の改善（調査軸１～５）

経営課題の改善（調査軸１）

図表１００．経営課題の改善についてのクロス分析結果

改善策 1-1 と現状の比較	
過半の経営層や責任者は内部不正とサイバー攻撃の両方を危惧しており、そこに事業リスクがありうるという認識自体は珍しいものではなくなっていると言える。しかし、経営層に関心を持ってもらうことが課題であると有識者は指摘しており、実際の内部不正対策につながるほどの理解の深さや確かさは必ずしも確立していないのが現状であると考えられる。言い換えれば、改善策が指摘する、経営層自身の率先による学びは引き続き重要な課題となっている。	
改善策	**現状**
【1-1】法務・知財部門（社外の法律相談サービスを含む）の協力を得る等の取組を検討して、営業秘密等の漏えい事件（事例）から、事業リスクとしての重要性や当事者がしてはならないこと等を率先して学ぶ。	・過半の経営層や責任者は内部不正とサイバー攻撃の両方を危惧している。 ・個人情報保護との比較においてそれ以外の秘密情報保護を重視する度合いの強い組織ほど、内部不正に係る情報漏えいのリスクが高いと認識している。 ・経営層は、産業スパイ・クラウドサービス・国内外の取引先／子会社、テレワークに起因するリスクを高いと認識する割合が全体平均よりも低い。 ・無関心な経営層にいかに関心を持ってもらうかが課題である。
改善策を補う示唆	**好事例**
—	・社外取締役弁護士等からの提起で、取締役会で秘密情報漏えい／内部不正防止について議論する機会を多く設ける。 ・有事の際の損害の大きさを示すリスクマップを活用し、秘密情報漏えいや内部不正が重大なリスクであ

	るという経営層の認識を高める。リスクマップは大企業で作成が進んでいる。
改善策 1-2 と現状の比較	
内部不正防止に関して、経営層による一般従業員・関連部門との対話の場は過半の企業において設けられており、リーダーシップを発揮し内部不正防止に関する発信が一定程度行われていると言える。従って改善策が示すような、元々あるセキュリティ確保の機会／場を用いて内部不正防止も発信するというような効率化は必ずしも必要とされていない可能性がある。他方で、経営層による内部不正リスクの軽視傾向があるという指摘があることも考慮すると、対話を行うという正しい方向性に沿った取組が進んでいる一方で、その実効性を高めていく必要があると言える。	
改善策	**現状**
【1-2】 経営層によるセキュリティ確保のリーダーシップ発揮の機会／場を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。	・過半の経営層がリーダーシップを発揮して内部不正防止に関する社内への発信を行っている。 ・内部不正防止に特有の取組の必要性を認識している企業は過半を占める。 ・内部不正防止に意識的に取り組む企業の過半は経営の透明性確保にも関心を持っている。 ・「経営層が現場との対話の機会を設けること」と「基本方針で内部不正をサイバーセキュリティと別建てとすること」の間には強い結びつきがある ・営業秘密保護の意識が高い経営層は、内部不正防止を重視すると共に、現場との対話に力を入れている。 ・営業秘密保護の意識が高い経営層は、内部不正防止は情報漏えい防止における重点課題だと理解している。 ・内部不正のリスクの大きさを見積もることが難しいため、予算やリソースが配分されにくい。 ・経営層に被害者意識が働くため取組が進みにくい。 ・経営層は内部不正リスクを軽視しがちであり、IT担当役員が責任者になって社長が進捗報告を受けるような平常時に類する体制が選ばれ、取組も甘くなる傾向がある。
改善策を補う示唆	**好事例**
・経営層等が自分の考えを全社に何度も伝え、その熱意が全社に浸透していれば、従業員のあるべき行	―

動に繋がっていく。 ・経営層の認識を「加害者でもありうる」というものに変革する必要がある。 ・秘密情報漏えい／内部不正防止とサイバーセキュリティは本来であれば目的が異なる取組なので、しっかりと対応するためには分けて進めるべきである。	

重要な秘密の特定と取扱いの改善（調査軸２）

図表１０１．重要な秘密の特定と取扱いの改善についてのクロス分析結果

改善策 2-1 と現状の比較	
内部不正防止を進める上で基盤となるのが、何が守るべき秘密であるかということを明確にし、従業員自身がそれを認知し、適切に行動できる環境を作ることである。しかし、その具体化となる、秘密の特定および格付けルール策定や表示の徹底、情報資産管理の実施と定期的な見直しといった個別の取組が浸透しているとは言えない。営業秘密保護への意識が高いと関連する取組の実施割合が高まることから、動機付け・意識付けによって改善できる余地はあると見られ、どのようにそれを進めるかが課題であると言える。	
改善策	**現状**
【2-1】経営層も積極的に関与して、事業リスクが高い（漏えいした場合のインパクトが大きい）営業秘密等を特定するための基準作り、従業員の営業秘密に対する対策意識の醸成、営業秘密の定期的な見直し等に取り組む。	・過半の企業でルール作りが行われている一方で、格付け表示にまで至っている企業は少数派である。 ・秘密情報が不正に取り扱われている時に周囲の従業員が気付いて通報できる職場環境にある企業は少数派である。 ・内部不正防止を重視する経営層は営業秘密等の情報資産管理の実践に力を入れているが、そのような組織であっても実践にまで及んでいない取組が多数ある状況が一般的である。 ・個人情報保護との比較において営業秘密保護を重視する度合いが高い組織ほど、関連する取組の実施割合が高まる傾向がある。 ・営業秘密保護の意識が高いと見られる企業では、営業秘密等への格付け表示に実効性があるという回答割合が全体平均よりも高くなっており、格付け表示が相対的にしっかりと実践されている。但し、回答割合は 43.0%に留まっており、意識が高い組織の過半で、秘密情報をそれと認知できないことがある。

	・情報の格付けと表示が行き届いた組織であれば従業員が営業秘密等を認識し、自身及び周囲での取扱に注意することを期待できるが、それを実践できている組織は少数派である。
改善策を補う示唆	**好事例**
・知らないうちに競合他社に持ち出されるくらいならば営業秘密をきちんと明確化しておこうという動機付けをするのがよい。 ・会社にとって有用な営業秘密をリストアップし、自分たちがやっている仕事がその保護に貢献していることが可視化されると、会社の重要な仕事に貢献しているという認識と満足感が浸透することを期待できる。	・技術・事業・営業・取引等のノウハウについても、特定すべき重要な営業秘密として、価値を決めることが必要で、大企業ではこの問題意識を持つ担当者が育ってきている。

組織体制・連携に関する課題の改善（調査軸３）

図表１０２．組織体制・連携に関する課題の改善についてのクロス分析結果

改善策 3-1 と現状の比較	
大半の企業で内部不正防止の責任の所在が定められており、更にその責任部門は関連部門と連携し、自部門だけでは賄いきれない専門知識や助力を得ている。組織体制の基本は浸透していると言える一方で、部門間連携の方法には配慮が必要であり、単に連携体制を整備するだけでなく、その連携が生み出す効果にも目を向けることが望ましい。	
改善策	**現状**
【3-1】責任部門自体（リスク・コンプライアンス部門等）と関連部門（情報システム部門：対策実施部門、法務・知財部門、営業・事業部門）が協働する体制の整備を検討する。	・大半の企業で内部不正防止の責任の所在が定められている。 ・責任部門と他組織の連携においては、過半の企業で、連携先からコンプライアンス・ガイドライン等の知識を補うことを目的としている。 ・内部不正に対応する経営層や組織は、コンプライアンス・ガイドライン等の知識を補うことができる組織との連携に軸足を置くと同時に、多種多様な組織間の連携に積極的である。 ・大企業では、知財部門は「秘密情報の価値を決められるのは現場の事業部門である」と考えていることが多い。しかし、現場の事業部門に秘密情報の価値決めを任せてしまうと視野が狭くなり、部門間のばらつきが出るというリスクを抱えることになる。
改善策を補う示唆	**好事例**
・大企業においては知財部門が全社のハブとなり、	―

事業部門などの他の部門と確認を取り合いながら、秘密情報の価値を決めるとよい。	

改善策 3-2 と現状の比較

情報システム部門が内部不正防止の責任部門となる場合には、知財・法務部門等の異なる専門部署との連携が必要になる。しかし、組織の在り方の課題としては、それら専門部署間の連携以前に、経営層に対して情報システム部門の意見やリスク認識が伝わらないことが大きいとの指摘があった。これは経営層の積極姿勢が重要であるという指摘の裏返しで、経営層が現場任せにして自らコミットすることを怠ると、責任部門が孤立しうる恐れを示唆する結果と言える。

改善策	現状
【3-2】 対策を実施する情報システム部門が責任部門となる体制を取る場合は、知財・法務部門等と協力してガバナンスを確保する。	・情報システム部門の意見やリスク認識が経営層に適切に伝わらないという問題が企業規模に関わらず生じており、情報システム部門が秘密情報の漏えい／内部不正防止の全社責任を負う上での重要な障害になっている。 ・情報システム部門は法律・知財に関する知識が十分でないため、技術的な取組が中心となってしまい、人的・組織的取組に漏れが生じる恐れがある。
改善策を補う示唆	**好事例**
—	—

改善策 3-3 と現状の比較

重要な秘密の不自然な扱いを適切に報告・通報できる仕組みの整備は行き届いていない。経営層までのエスカレーションルートがある企業は半分に満たず、内部通報体制の整った企業は更に少ない。個人情報以上に営業秘密保護を重視する組織では取組度合いが深まるが、それでもこの傾向は変わらない。大きな課題があると言える。

改善策	現状
【3-3】 重要な秘密が不自然に取り扱われているところを目にしたら、上に報告するというリテラシーと、上に報告できない事情がある場合は内部通報ができる体制を構築する。	・不正の通報先としては上司が直属の上司が第一で、経営層までのエスカレーションルートがある企業は半分に満たず、内部通報体制がある企業は少数派である。 ・個人情報保護との比較において営業秘密保護を重視する度合いが高い組織ほど、秘密情報の不自然な扱いや不正な漏えいを報告する体制の整備に関する取組の回答割合が高くなる傾向がある。但し、営業秘密保護を個人情報保護以上に重視している場合でも、「経営層等に報告が上がるルートの確立」ができている組織は半分に満たない。
改善策を補う示唆	**好事例**
—	—

改善策 3-4 と現状の比較

役職の高い者を特別扱いしないマネジメントシステムの構築・整備状況については実態を調べるに至らなかった。

改善策	現状
【3-4】役職の高い者を特別扱いしないマネジメントシステムを構築し、体制を整備する。	―
改善策を補う示唆	**好事例**
・経営者がまず原則を示し率先してこれを指示した上で、経営層に対する監督強化、内部統制システムの構築、意思決定の透明性確保、倫理意識の醸成、内部通報制度の整備、定期的なリスク評価と対策改善に取り組む必要がある。 ・役職の高い者を特別扱いしないマネジメントの確立には、経験とノウハウの蓄積も必要である。	―

社員教育とリテラシー構築に関する課題の改善（調査軸４）

図表１０３．社員教育とリテラシー構築に関する課題の改善についてのクロス分析結果

改善策 4-1 と現状の比較	
内部不正防止に特有の概念や対策についての法的理解が、法務・知財等の部門から情報システム部門へとどのように連携されているかという実態を調査するには至らなかった。	
改善策	**現状**
【4-1】法務・知財部門の協力を得た教育・研修等によって、対策を担当する情報システム部門の重要情報漏えい／内部不正に関する法知識（不正競争防止法等）の理解を深める。	―
改善策を補う示唆	**好事例**
・営業秘密保護に係る制度（不正競争防止法）については、営業秘密侵害は刑事罰が非常に厳しいこと、両罰規定で会社も罰せられるリスクがあることという 2 点が重要なので、経営層をはじめとして、情報システム担当者やその他の従業員にこの事実を教育・警告すべきである。	―
改善策 4-2 と現状の比較	
内部不正に関する理解を従業員へと浸透させる施策という点では、社内での事件発生時にこれを周辺情報と共に告知したり、秘密情報の不自然な扱いや社外への不正な漏えいを目撃した場合の適切な行動を周知したりするなど、一通りの取組がなされている。個人情報保護以上に営業秘密保護を重視する組織では取組の度合いが深まる傾向があり、問題意識の深さと取組が不可分であることの表れと言える。	
改善策	**現状**
【4-2】入社／人事異動／退職等の重要なタイミングで、具体的に重要な秘密を示して、何をしてはいけないのか、どのような時に上への報告が必要か等を周知・徹底する。	・社内での事件発生時には、その告知内容を通じて、何をしてはいけないのか・何が問題となるのかということを、大半の企業が社内に周知している。 ・大半の企業において、秘密情報の不自然な扱い

	や社外への不正な漏えいを目撃した際の適切な行動が周知されている。 ・従業員に少しでもリスクに気付いて貰えていれば被害を防ぐことができた事例が多い。 ・個人情報保護との比較において営業秘密保護を重視する度合いが高い組織ほど、経営幹部のそれも含めて内部不正を全社に告知する割合が高まる。営業秘密の保護と経営層のコンプライアンスに対する厳格な姿勢は軌を一にするものになっている。 ・個人情報保護との比較において営業秘密保護を重視する度合いが高い組織ほど、秘密情報の不自然な扱いや不正な漏えいを目撃した際の望ましい行動の、周知・徹底に関する回答割合が高まる。特に、営業秘密等の保護を個人情報保護以上に重視している企業の大半がその種の周知・徹底に定期的に取り組んでいる。
改善策を補う示唆	**好事例**
・従業員には、営業秘密や重要なデータ等の漏えいがどの程度の損害を生じるのかを教育し、広く認識してもらうことが重要である。 ・従業員のリテラシー欠如、法令やガイドラインに対する無知は内部不正に含まれるという認識を、事例と共に従業員に周知教育すべきである。同時に、基本的な取組の重要性や、法令・ガイドラインを周知できていない経営層にも責任がある。 ・ログをきちんと取得して確認していることを社内に通知する、起こった事例を包み隠さず企業内に周知する、罰則を設けてこれを周知する等が有効である。	―
改善策 4-3 と現状の比較	
従業員に対する営業秘密等の特定・格付けに関する周知・教育自体は大半の企業で行われている。しかし、その実効性を高めるために有効であると思われる定期的な反復や、各自で自己判断できるような深度ある教育となると、大企業でもまだ十分には取り組めていない。	
改善策	**現状**
【4-3】 事業や経営における重要性や価値、当該情報が漏えい・毀損等した場合の影響・損害などを踏まえた、秘密の重要度の判別基準を明文化した上で、この基準に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。	・大半の企業において、営業秘密等の保護が個人情報保護と同じように重要であることを周知・教育している。 ・大半の企業において、営業秘密等の特定と格付けのための基準を周知・教育しているが、定期的に取

	り組めている企業は半分に満たない。 ・「内部不正事案の多くは情報漏えいを伴う」ところ、実際の情報漏えいの対策においても、営業秘密等の漏えいが重視されている。 ・大企業であっても、重要度を判別する基準を決めて教育するところまでは至っていない企業が多い可能性がある。
改善策を補う示唆	**好事例**
—	—
改善策 4-5 と現状の比較	
内部不正防止に限らず、専門的な内容の教育手段としては e-Learning が重用されるところ、実効性を高めるにはそれ以外の教育方法も取り入れていることが望ましい。しかし、取りうる方法別で見ると、そのような企業は半数に満たない。手段ではなく伝えるべき内容に目を向けてみても、営業秘密等の漏えいや内部不正に関し、してはいけないことを周知している企業は過半を占めるが、どのように罰せられるかを周知している企業はより少ない。総じて、内部不正防止に関する教育には底上げの余地があると言える。	
改善策	**現状**
【4-5】インシデント事例、解説動画・イラスト等のリッチコンテンツ、グループディスカッション、定期的な規則遵守のセルフチェック等を積極的に活用して理解を深める取組を推進すると共に、従業員に対し、営業秘密や限定提供データについて、何をしてはいけないのかを教育する。	・営業秘密等の漏えいや内部不正に関し、過半の企業において違反行為が示されているが、罰則までも明確である企業は相対的に少ない。 ・大半の企業において e-Learning 以外の方法を実践に取り入れている。 ・基本方針で内部不正防止をサイバーセキュリティと別建てにしている企業の大半（75.1%）で、秘密情報等に係る違反行為を周知している。その割合は両者を別建てとしていない企業（29.9%）の 2 倍を超える。 ・個人情報保護との比較において営業秘密保護を重視する度合いが高い組織ほど、秘密情報の漏えいや内部不正に関する違反行為や罰則等を従業員に周知している割合が高い。
改善策を補う示唆	**好事例**
—	—

対策実施に関する課題の改善（調査軸５）

図表１０４．対策実施に関する課題の改善についてのクロス分析結果

改善策 5-3 と現状の比較
大半の企業が内部不正防止対策とサイバーセキュリティ等のそれ以外の対策とを使い分けており、特に、内

部不正防止を基本方針の段階でサイバーセキュリティ等と分けて別建てとしている組織では、内部不正防止に特有の対策を別建てとしない組織よりも積極的に実施している。しかし、そのような意識の高い組織においても、実施すべき対策の浸透状況は十分とは言い難い。個人情報保護以上に営業秘密保護を重視する企業の大半は、対策の使い分けに加えて経営層に定期的にそれらの有効性を報告しており、経営層の積極姿勢につながれば更なる改善も期待できると考えられる。

改善策	現状
【5-3】 重要情報漏えい防止体制の下で、サイバーセキュリティ対策と内部不正防止対策の両方に一貫して取り組む。	・快適な職場環境の整備、秘密保持義務の明文化、徹底した注意喚起という 3 つの取組が、内部不正防止に特有の対策として一般的である ・大半の企業において内部不正防止対策とサイバー攻撃対策や会計不正等の対策とを使い分けている。 ・基本方針で内部不正防止をサイバーセキュリティと別建てにしている企業では、内部不正防止に特有の対策の実施割合が、両者を別建てとしない組織に比べて 1.5 倍から 4 倍になる。 ・内部不正防止のために実施すべき対策の浸透状況は、意識の高い組織においても十分とは言い難い。 ・個人情報保護との比較において営業秘密保護を重視する度合いが高い組織ほど、内部不正防止対策をサイバー攻撃対策や会計不正・ハラスメント等の対策と意識的に使い分けていると回答する割合が高まる。営業秘密等の保護を個人情報保護以上に重視している企業の大半がこれらを使い分け、更に、定期的に経営層にその有効性を報告している。
改善策を補う示唆	**好事例**
・広い視野で見ればサイバーセキュリティ対策と内部不正防止対策の観点は同じであり、サイバーセキュリティと内部不正防止で共通の対策は適用しつつ、守るべきものとリスクの違いに合わせて足りないところを補っていけばよい。	―

改善策 5-4 と現状の比較

大半の企業において内部不正リスクをそれと意識し評価している。営業秘密保護を重視する度合いの高さと内部不正リスクを分けて評価する傾向は軌を一にしている。他方で、継続中の事業に係る漏えいリスクは楽観論の影響を受けて軽視される傾向がある。内部不正に目を向けたリスク評価の結果が具体的にどのような対策に反映されているかという実態は今回の調査では把握するに至らなかった。

改善策	現状
【5-4】 内部不正のリスクシナリオも加味して重要情報漏えいに対するリスクアセスメントを実施し、セキュ	・大半の企業で内部不正リスクをそれと意識して評

リティ対策に加えて、内部不正防止対策の割り当てと選別を行う。この際には、不正に対する人的・組織的対策と技術的対策のバランスの適正化を考慮する。また、経営層の不正防止と透明性確保、アクセスログの確認範囲拡大、他社の重要情報の不正な社内持ち込み防止、重要プロジェクト就任／離任時にも秘密保持義務の誓約書を取得、重要性の高い秘密に触れる場合の誓約書の詳細度の変更等を実施する。	価している。 ・個人情報保護との比較において営業秘密保護を重視する度合いが高い組織ほど、内部不正のリスクをサイバー攻撃や会計不正・ハラスメント等のリスクと分けて評価する割合が高まる。営業秘密等の保護を個人情報保護以上に重視している企業の大半がこれらを分けている。 ・不満を持つ従業員が秘密情報を漏えいさせるケースでは、欲しい秘密に的を絞って狙ってくるので、対応が難しいことがある。 ・継続中の事業に係る漏えいリスクは、楽観論から「不正をする担当者はいない」と思いたい心理が働きやすい。
改善策を補う示唆	**好事例**
・秘密情報漏えいの事業リスクアセスメントは、本来プロジェクトごとに実施すべきである。 ・秘密情報が漏えいすると企業の存続すら危うくしうるという危機感を持ち、対策にリソースを投入すべきである。	―
改善策 5-5 と現状の比較	
過半の企業において営業秘密等を個人情報と同等以上に重視しており、しかも、営業秘密等の保護対策を重視する傾向は内部不正防止を別建てにすることと強く結びついている。問題意識と対策の方向性が一致しており、基本的には望ましい状況であると考えられる。	
改善策	**現状**

【5-5】個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。	・過半の企業において営業秘密等を個人情報と同等以上に重視している。 ・基本方針で内部不正防止をサイバーセキュリティと別建てにしている企業では、営業秘密等を保護する対策を個人情報保護と同等以上に重視している割合（84.8%）が、両者を別建てにしていない企業（38.8%）の 2 倍を超え、大半を占める。 ・営業秘密等の保護を重視することが内部不正防止を別建てにすることと強く結びついている ・どちらが良いというものではないが、大企業は、資金や人員が潤沢であるため、秘密情報漏えいが起きない体制作りに注力する企業と、（資金や人員には限界があり漏えいが発生することは避けられないとの考えから）秘密情報漏えいの早期発見に注力する企業とに、二分できる。
改善策を補う示唆	**好事例**
—	—
改善策 5-6 と現状の比較	
機密性の高い秘密情報については過半の企業が管理の定期的な見直し・棚卸しに取り組んでおり、望ましい状況を概ね達成していると考えられる。	
改善策	**現状**
【5-6】情報機密区分に応じたアクセス権限付与状況の点検、アクセス権限付与者についての定期的な棚卸しを実施する。	・機密性の高い秘密情報については過半の企業が管理の定期的な見直し・棚卸しに取り組んでいる。
改善策を補う示唆	**好事例**
—	—

②中小企業の構造的課題の改善（調査軸６の１～５）

経営課題の改善（調査軸６の１）

図表１０５．中小企業の経営課題の改善についてのクロス分析結果

改善策 6-1-1 と現状の比較	
中小企業における経営層のリスク認識は相対的に低く、その一方で、社会環境の変化に伴う秘密情報の漏えいや内部不正防止といった課題の重要度は高まっているとの認識が広がっている。リスク認識の担い手となる意識の高い人材の不足が指摘されており、人材確保・育成と共に、すべての起点となる経営者自身の意識を高めることが特に重要であると考えられる。	
改善策	**現状**

【6-1-1】経営層または内部不正防止に関する組織全体の責任者等が率先して、重要な秘密情報漏えい／内部不正リスクを重要な経営課題として認識する機会を増やし、サイバーセキュリティ確保と内部不正防止を一体的に認識した経営を行う。	・中小企業では、秘密情報漏えいに関する経営層のリスク認識が大企業も含めた全体平均と比べて全般に低い。 ・コロナ禍、働き方改革、人手不足などにより、経営課題として秘密情報の漏えい／内部不正防止の重要度がますます高まっている。 ・中小企業では秘密情報漏えい／内部不正防止に関する意識の高い幹部がキーマンとなりうるが、こうした意識の高い幹部が少ない。
改善策を補う示唆	**好事例**
・中小企業では経営層が高い意識を持って率先し牽引すれば会社全体の取組状況をがらりと変えられる可能性を持っている。 ・経営層が秘密情報の漏えいや内部不正防止について全社にしっかりと自分の経営方針を話していくことが望ましい。 ・中小企業では、営業秘密を社内できちんと保護する体制を構築することで、秘密情報漏えい／内部不正防止にも好ましい効果が生じる。	・業界の流れを意識し、技術情報管理の認証取得に取り組んだことが良い契機となった。 ・秘密情報との関りが深い事業を展開しているため自社でもしっかり取り組むことが必須だった。 ・悪意の有無に関わらず、人為的な秘密情報漏えいのリスクが高いと考えて経営している。
改善策 6-1-2 と現状の比較	
全体としても過半の企業において経営層による一般従業員・関連部門との対話の場が設けられている中で、中小企業ではそれが奏功した場合の効果が大きく期待できることに強みがあると言える。実際、意識の高い経営者による積極的な取組と、それが実際の効果につながっている事例が確認された。他方で、企業規模が小さくなるほど取組度合いも弱くなる傾向があり、大企業を含む全体平均に比べると相対的に不十分である。経営層が部下に任せきりになりがち、潤沢にリソースを投入することが難しい等の、中小企業における一般的課題が関わっているものと考えられる。 また、従業員 100 名以下の企業では、内部不正防止をサイバーセキュリティ確保と意識的に分けるかどうかが概ね拮抗しているため、サイバー攻撃防止とは異なる内部不正防止の特徴等を発信できていない企業が相対的に多くなる。	
改善策	**現状**
【6-1-2】中小企業では、全社集会などの経営層が従業員に周知徹底する機会を活用して、内部不正防止の特徴やサイバー攻撃防止とは異なる対応の必要性を発信する。	・企業規模が小さくなるほど、秘密情報の漏えいにつながる内部不正に関して、経営層と一般従業員・関連部門の対話を設けているとする回答割合が下がる。 ・内部不正防止をサイバーセキュリティ確保とは意識的に分けて扱う企業の割合は従業員数が増えるほど高まる。大企業では両者を分けるという組織が過半あるいは大半を占めるのに対し、従業員 100 名

	以下の企業では両者を分けるかどうかが概ね拮抗している。 ・IT 関連のリスクに対する中小企業の対応状況はまだ十分でない。 ・自社で事件が発生するまで内部不正防止の体制整備に注力できない。 ・基本方針で秘密情報管理の重要性を明記している企業はあまり見られず、管理がなされていても部下に任せきりで経営層にとってリスクの所在がブラックボックスになっている。 ・経営者も従業員もお互いに直接顔が見えるため中小企業では性善説を前提とした管理になりがちである。
改善策を補う示唆	**好事例**
・従業員と直接コミュニケーションを取って趣旨をしっかりと伝えることで、ある程度リスクに対応できる。 ・中小企業の取組強化に向けては、経営者が戦略を語り、コミットメントや指示に自身の想いやこだわりを込め、日々語ることが重要である。 ・経営層が何をどの程度重視しているかを率直に伝えることで、従業員がこれを評価して行動することを期待できる。 ・埋めるべきギャップは大企業より中小企業の方が小さいので、ひとたび良い方向に動き始めると、目標レベルに素早く到達できる。 ・中小企業の規模やリソースを考慮すると、秘密情報漏えい／内部不正防止とサイバーセキュリティを敢えて分けて取り組む必要はない。	・経営者が自ら基本方針を全社に周知・徹底している。 ・定期的にも日常的にも経営者が社員に語ることで意識付け・啓発に効果を上げている。 ・漏えいが自社の信頼失墜に直結することを強く認識して全社に周知・啓発している。 ・秘密情報漏えい／内部不正防止の取組が特に進んでいる中小企業では、情報漏えい／内部不正防止に関する基本方針を情報セキュリティポリシーとは完全に別建てで定めている。 ・ISMS、プライバシーポリシー、技術情報管理等の認証取得が、中小企業の経営者が基本方針を定める契機となって取組が進んだ。 ・情報漏えい／内部不正防止に関する経営者の考えを全社に何度も繰り返し伝えることが重要であると認識し、経営者自ら実践している。

重要な秘密の特定と取扱いの改善（調査軸６の２）

図表１０６．中小企業の重要な秘密の特定と取扱いの改善についてのクロス分析結果

改善策 6-2-1 と現状の比較	
全体としても秘密情報の格付け・表示に課題がある中で、中小企業における取組は更に劣後している。秘密情報の特定も十分ではない。紙媒体のような物理的実体のある秘密の保護に比べ、電子化された秘密情報の管理は進んでいない。一方、内部不正防止にもつながる認証の取得を経て具体的な取組に至る事例もあり、経営者の意識付けも兼ねて、何らかの認証の取得を考慮することが実践的な方策の一つになると考えられる。	
改善策	**現状**
【6-2-1】中小企業では、経営層が自ら判断する、あるいは判断基準を示すことで、自社の事業にとって重要性／機密性の高い秘密情報を的確に特定する。	・若干の例外はあるが、従業員数が小さくなるほど、個人情報以外の秘密情報の特定・格付け・表示に関する取組の実施率が低下する。 ・中小企業において秘密情報をそれと認知できるような格付け・表示等がなされている割合は 20%前後であり、少数派である。大企業ではこの割合が最低でも 35%には達しており、取組の度合いに明白な違いがある。 ・紙に書かれた秘密情報の物理的管理がしっかりできていたとしても、電子化された秘密情報の管理はほとんどできていない中小企業が多い。
改善策を補う示唆	**好事例**
・経営者の負担を避けるため、部下を育成し、権限移譲を考えることも必要である。	・経営者が自ら事業リスクの判断や秘密情報の特定・格付けを行っている。 ・経営者が情報セキュリティや技術情報管理の認証取得を決断し、これに取り組んだことが契機となって、営業秘密等の特定、格付け、表示に関する体制整備が進んだ。 ・認証制度が要求する管理基準に従い、秘密情報を管理できる情報資産台帳を作成している。 ・認証制度に沿って特定した情報資産については、情報の保存場所や保存期間、データ消去の方法やリスクの大きさ、格付けを台帳管理している。 ・情報資産を保存する共有フォルダ等の場所を格付けに沿って切り分け、かつ、適切なアクセス制御・記録を合わせることで、格付け・表示・アクセス管理を一体に実施している。

組織体制・連携に関する課題の改善（調査軸６の３）

図表１０７．中小企業の組織体制・連携に関する課題の改善についてのクロス分析結果

改善策 6-3-1 と現状の比較	
規模によれども中小企業では人事・法務といった専門部署が必ずしも細かく分かれていないという現実がある中で、調査結果からは内部不正防止についても経営層が直接の責任者となりやすい様子がうかがえる。改善策が求めるような、経営層が中心となっての総務・人事・法務や情報システム等の担当との調整は、リソース制約の大きい中小企業では現実的な選択肢と言える一方で、それが片手間の取組となって効果を損なうことのないように注意する必要がある。	
改善策	**現状**
【6-3-1】 中小企業では、責任者である経営層が中心となって、総務・人事・法務や情報システム等の関連部門との調整を行う。	・秘密情報の漏えいに繋がる内部不正に経営層が主体的に対応するとの回答割合は、従業員数が増すほど低下するが、従業員数 10,001 人以上のとりわけ大きな企業においては逆に割合が増す。この傾向と軌を一にして、従業員数が増すほど、所定の統括組織が主体的に対応するとの回答割合が高まる。 ・法務部門がない、または知財・法務に精通する経営層や幹部がいない中小企業では、法制度への対応や規程の制定／社内への浸透等が社長室や総務部門の雑多な業務の１つとして片手間で扱うことになりがちである。
改善策を補う示唆	**好事例**
・社内に委員会を設けるなどして、複数部門が連携して取り組むことができる体制を検討することが望ましい。	・秘密情報漏えい／内部不正防止とサイバーセキュリティの担当役員を分け、監督も別々に実施し、経営者がこれを統括している。 ・経営者を責任者とする 3~5 名程度の幹部による委員会を設置している。その下にシステム、総務・人事、教育、内部監査等を担当する幹部が集まって委員会を構成する。 ・経営者が責任を担い、品質管理責任者が横串を通す形で、関連部門を連携させている。各種のマネジメントシステムを構築・運用する際に品質管理責任者が必ずこれに協力し、品質管理責任者を中心とした社内ネットワークを形成している。 ・秘密情報保護に関する重要な主題（秘密保持義務の誓約、懲罰、情報セキュリティ対応等）ごとに担当チームを組成し、各チームが基本方針を定め

	て取組を実施している。経営者はチーム全体の統括責任者となり、必要に応じて各チームと関連組織の協議を主導する。
改善策 6-3-3 と現状の比較	
中小企業では従業員と経営層の距離が近いと目されるところ、経営層へと報告が上がるルートの確立度合いは大企業が勝っている。この背後には、ルールに基づくマネジメントの浸透度合いと企業規模が連動するという傾向に加え、距離が近いからこそ性善説を頼ってしまいがちであるという文化も関わる。体制の整備に先立ち、経営層による現場への具体的な意識付けを行うことが有効であると考えられる。	
改善策	**現状**
【6-3-3】重要な秘密が不自然に取り扱われている様を目撃した際に上に報告することの徹底と、上に報告できない事情がある場合は内部通報ができる体制を構築する。	・従業員数と、秘密情報の不自然な扱いや不正な漏えいを報告するルール等を定めているとの回答割合は連動しており、前者が増えるほど後者も高まる。 ・中小企業では従業員と経営層の距離は大企業に比べて近いはずだが、経営層へと報告が上がるルートの確立度合いは大企業が勝る。
改善策を補う示唆	**好事例**
・中小企業は人間関係が良く性善説を基にしていることが多いので、内部通報ができる仕組みを構築すると逆に従業員の不信感が高まる恐れがあり、注意が必要である。	・秘密情報が漏えいした時や従業員がヒヤリハット・不信感を認識した時に、直属の上司を通じて経営者にすぐに報告が上がってくる仕組みを設けている。

社員教育とリテラシー構築に関する課題の改善（調査軸６の４）

図表１０８．中小企業の社員教育とリテラシー構築に関する課題の改善についてのクロス分析結果

改善策 6-4-1 と現状の比較	
社外の専門家の助力を得て法務・知材の知識を情報システム部門等に広める取組の実態を調査するには至らなかった。	
改善策	**現状**
【6-4-1】中小企業では、経営層のリーダーシップと社外の専門家（IT コーディネータ、弁護士・弁理士等）の協力により、情報システム部門や他の従業員に法務・知財の知識を広める。	―
改善策を補う示唆	**好事例**
・事業拡大に悪影響を及ぼしうることを考慮し、知財専門人材が社内にいない場合は業界団体等を通じて外部の専門職（弁護士・弁理士等）と連携することが望ましい。	―
改善策 6-4-2 と現状の比較	
改善策に言うような退職時における秘密取り扱いの説明・教育を行っている事例は見出されたが、中小企業における取組は全体としては劣後しており、例えば経営幹部のそれも含め、内部不正の発生を全社に告知している企業は ４ 割に達しない。他社で発生した参考事例の情報を収集することも中小企業では難しく、全	

般に取組の底上げを図る必要があると言える。	
改善策	**現状**
【6-4-2】 中小企業では、入社／人事異動／退職等の重要なタイミングで、経営層が重要な秘密を具体的に示し、その取扱い指示を徹底する。	・経営幹部のそれも含め、発生した内部不正を全社に告知しているとする回答割合は従業員数に連動しており、中小企業では告知される割合が 40%に満たない。 ・秘密情報の不自然な扱いや不正な漏えいを目撃した際の望ましい行動を定期的に周知・徹底している割合は、従業員数が増すほど高まる。従業員数が 100 名以下の企業においては該当するのはほぼ少数派と言ってよい。 ・中小企業では、他社で発生した事件の情報を収集することは難しい。経営者による情報収集は過大な負担ともなりうる。
改善策を補う示唆	**好事例**
・中小企業には営業秘密の秘密管理性の確保が自己防衛及びビジネス拡大に不可欠であることを大企業以上に認識してもらうことが望ましい。	・営業秘密・重要データの知識に関する社員教育にも取り組み、入社時のオリエンテーション、年 1 度の e-Learning や年 2 回の集合教育、全社集会の機会を活用した教育を行っている。 ・リスクとその重要性、過去に発生した事例における重要なリスクと実際に発生した損害、社内で発生したヒヤリハットの経緯や内容等を伝えている。 ・退職時に秘密情報を持ち出すリスク、実際に持ち出した事例等に重点を置いて教育している。 ・中途退職時に禁止されている事項を教育している。 ・経営者が自ら参考事例等の情報を収集している。 ・セキュリティ会社に委託し、他社で発生した事件の情報、注意点、セキュリティ管理の考え方等の情報を提供してもらっている。
改善策 6-4-3 と現状の比較	
中小企業における営業秘密等の特定・格付けに関する周知・教育の実施割合は大企業に比べてはっきりと劣後している。しかしながら、そうした周知・教育の定期実施や、表裏一体になるはずの秘密情報の格付け・表示の徹底は大企業でも十分とは言えない状況であり、中小企業における実践と有効化は非常に難しい課題であると考えられる。	
改善策	**現状**
【6-4-3】 経営層または経営層が権限を移譲した	・営業秘密等の重要性を定期的に周知・教育して

責任者が各々の秘密の重要度を指定した上で、この指定に基づくラベリング等を行い、リテラシー教育等によって、適切な取り扱いを従業員に周知・徹底する。	いる割合は従業員数に連動しており、若干のぶれはあるものの、従業員数が増すほど取組の実施率も高まる。大企業では過半で定期的な取組があるのに対し、該当する中小企業はほぼ少数派である。 ・個人情報以外の秘密情報の特定と格付けの全社基準を周知・教育している割合は従業員数が増すほど高まる。大企業ではほぼ過半がすべてを周知・徹底しているとするのに対し、該当する中小企業はほぼ少数派である。
改善策を補う示唆	**好事例**
—	・経営者が自ら事業リスクの判断や秘密情報の特定・格付けを行っている。
改善策 6-4-4 と現状の比較	
内部不正防止対策として従業員の行動を記録・監視することへの抵抗感が中小企業の間には見られる。有識者も指摘する通り、中小企業では経営層と従業員の距離が近く、このような心理的課題への対処に当たっては経営層自身の細やかな配慮が必要になると考えられる。	
改善策	**現状**
【6-4-4】 企業のサイバーセキュリティ／コンプライアンス等に関する取組の一環として、重要情報漏えい／内部不正防止の社内規程及びその規則、モニタリングの目的や実施状況等に焦点を当てる回数を増やす。	・秘密情報漏えい防止等の対策として従業員のアクセスログを取得すること等に対して抵抗感を持つ中小企業が多く見られる。
改善策を補う示唆	**好事例**
—	・抵抗感を示す事例以上に、有識者の適切な助言等に基づいてこれを導入し組織に根付かせることで、むしろ会社への帰属意識や仕事に対するプライドといったものが上がってきて緊張感が醸成され、会社の雰囲気が良くなってきたと言われることも多い。
改善策 6-4-5a と現状の比較	
内部不正に当たる違反行為や罰則の定めを周知している割合は、大企業で過半を占めるのに対し、中小企業では半分に満たず、取組状況に隔たりが見られる。経営層による指示・啓発の全体像を調査するには至ってないが、実際に経営者が手ずから取り組んでいる事例は確認できており、改善策の方向性は妥当であり、かつ、今後の浸透が望まれる内容と言える。	
改善策	**現状**
【6-4-5a】 中小企業では、経営層が自ら事業リスクに基づいて、営業秘密や限定提供データの取り扱いについて何をしてはいけないのかを指示・啓発する。	・内部不正にあたる違反行為や罰則の定めを周知している割合は従業員数が減るほど下がる。中小企業において秘密情報等に係る違反行為を周知している企業は半数に満たず、より大きな規模の企業では逆に過半が周知していることと対照的である。
改善策を補う示唆	**好事例**

—	・営業秘密や限定提供データに関する従業員教育で、これらの取扱方法に加えて、禁止事項・内規の懲罰規定・法の遵守等についても教育している。 ・個人情報保護法、不正競争防止法、外為法等を対象として解説動画や弁護士の説明を教材に取り入れて従業員に教育することで、民事的な賠償責任や刑事責任を負ったりする場合があること等を理解させている。 ・経営層が率先して集める、外部委託先から情報提供を受ける等の手法で、他社で発生した事案の情報を取りまとめ、社会的な影響なども含めて教育している。

改善策 6-4-5b と現状の比較
中小企業では e-Learning 以外の方法を取り入れている割合が下がる傾向がある。相対的によく実施されているのはインシデント事例の説明だが、実施率で見ると 4 割に満たず、経営層と従業員の距離の近さを生かし切れていない状況と言える。

改善策	現状
【6-4-5b】中小企業では、経営層が全社集会などで直接従業員に教育・意識づけする。	・e-Learning 以外の方法を取り入れている割合は従業員数が減るほど下がる。インシデント事例の説明が最もよくある取組で、これに規則順守のセルフチェックが続く。いずれも中小企業における実施率は 4 割に満たず、大企業とは対照的である。
改善策を補う示唆	**好事例**
—	・人数とリソースが少ない中小企業が選択しやすい教育方法として、外部講師（例えば IT コーディネータ）を招いて研修を行っている。 ・日常業務において秘密情報の取り扱いに問題がないか、社員同士で相互確認する日々実践形式の教育を取り入れている。

対策実施に関する課題の改善（調査軸６の５）

図表１０９．中小企業の対策実施に関する課題の改善についてのクロス分析結果

改善策 6-5-1 と現状の比較	
中小企業における各種ガイドラインの活用状況を具体的に調査するには至らなかった。	
改善策	**現状**
【6-5-1】中小企業では、経営層と担当者が協力して、重要情報（営業秘密や限定提供データ等の知財を含む）漏えい対策に役立つ官民の関連ガイ	—

ドライン／ハンドブックの情報を収集し、活用を進めることで、必要な対策を見直す。	
改善策を補う示唆	**好事例**
—	—
改善策 6-5-2 と現状の比較	
内部不正防止の一環として従業員の行動を記録・監視することに中小企業の間では抵抗感がある一方で、十分なコミュニケーションをとり、なぜ記録・監視が必要であるかをていねいに説明することで理解を得ている事例のあることを確認できた。改善策の示す方向の妥当性を裏打ちするものと言える。	
改善策	**現状**
【6-5-2】 経営層が積極的に従業員とコミュニケーションを取ることで、従業員の行動監視やログの記録・分析等に対する従業員の理解を得る。	—
改善策を補う示唆	**好事例**
—	・IT システムのアクセス等のログを取得して定期的に確認することについて、十分なコミュニケーションを取ってインシデント対応のために必要であることをていねいに説明することで、従業員の理解と信頼が得られている。
改善策 6-5-3 と現状の比較	
中小企業においては内部不正防止対策とサイバーセキュリティ対策を同一の取組の一環として実施する傾向がある。この背景には、リソース制約に加えて、ISMS や技術情報管理のような認証制度のスコープ中に内部不正防止が含まれていることが関わっていると考えられる。ただし、これは内部不正防止に固有の対策の実施が弱体化するという懸念もはらむものであり、実際、従業員数が増えるほど内部不正防止対策を他の対策と使い分ける傾向も見出された。経営資源に合わせた適切なバランス配分・判断が必要であると言える。	
改善策	**現状**
【6-5-3】 中小企業では、重要情報漏えいの防止体制の下で、サイバーセキュリティと内部不正防止の両方に共通する対策を積極的に 1 つにまとめる。	・秘密保持義務契約／誓約を求めている企業の割合は従業員数が小さくなるほど下がる。ただし、本調査で一番小さな企業規模に対応する従業員数 21～50 名の場合でも 41.6%の実施率となっており、過半における実施を達成するまでの差異はログ確認のような他の対策に比べて小さい。 ・従業員数が増えるほど、内部不正防止対策と、サイバー攻撃や会計不正・ハラスメント等の対策とを意識的に使い分ける傾向がある。大企業では過半が使い分けを行うのに対し、該当する中小企業は半数に満たない。
改善策を補う示唆	**好事例**

・不正が発覚した際の社内告知については、特に 1 人 1 人の顔が見えるぐらいの組織規模の場合に、慎重に伝え方を選ぶ必要がある。 ・経営者の負担が大きくなりすぎないように気を付ける必要がある。	・秘密情報の漏えい防止に向けた内部不正防止対策とサイバーセキュリティ対策を同一の取組の一環として実施している。この一因として、ISMS や技術情報管理の認証のスコープが両者をカバーしていることが挙げられる。 ・ミスが発生した際の報告について、これを隠ぺいする組織風土にならないように、自発的な報告を考課で高く評価している。 ・経営者が自ら事業運営と内部不正防止／情報セキュリティの両方にコミットしている。

改善策 6-5-4 と現状の比較

内部不正防止はサイバーセキュリティに比べれば浸透していない考え方である。そこで、内部不正防止対策をサイバーセキュリティ対策に対して追加的に組み合わせる道筋の一つとして、まず内部不正リスクそのものを評価する取組に本調査では着目した。しかし、内部不正リスクを他のリスクと切り分けて評価する中小企業は半分に満たない。事例からは、リスクアセスメントの実施が、関連する認証制度の規定に強く影響されている様子が垣間見える。それぞれの企業の事情に応じたリスクアセスメントに基づく内部不正防止のアプローチは、まだハードルの高いものであると推察される。

改善策	現状
【6-5-4】内部不正のリスクシナリオを加味した重要情報漏えいに対するリスクアセスメントを実施し、セキュリティ対策に加えて、内部不正防止対策の割り当てと選別を行う。	・内部不正リスクをサイバー攻撃リスク等と意識的に分けて評価している割合は、従業員数が小さくなるほど下がる。大企業では過半が両者を分けるのに対し、該当する中小企業は半数に満たない。 ・ISMS 取得に必要な範囲で情報リスク評価を実施している。 ・技術情報管理認証が退職後に秘密情報を持ち出すリスクを重視している。 ・他社の秘密保護を支援する事業を提供しており、自社で秘密情報漏えい事件を起こしてしまうとレピュテーションリスクが甚大であると認識している。
改善策を補う示唆	**好事例**
・中小企業では他社の事例等に基づいて意識の高い経営層がリスクを判断できれば、秘密情報漏えいや内部不正のリスク評価をある程度代替できる。	・秘密情報漏えいの事業リスクとその重要度を事業継続性の中でどのように位置付けるかについて、経営層の間で認識を共有している。 ・従業員の秘密保持義務に関し、入社時の誓約書で「退職する時にも誓約書を提出すること」を誓約してもらっている。 ・対処の難しさを理解した上で次のような色々なリスクに注意を払っている：秘密情報の意図的な持ち出し、電子メールの誤送信、その他不注意やミスによる情報漏えい、個人所有の BYOD 利用、中途退職者の持ち出し。
改善策 6-5-5 と現状の比較	
内部不正防止は営業秘密漏えいの防止と密接に結びつくが、そもそも営業秘密等の保護を重視する企業の割合は企業規模が小さいほど下がる。営業秘密等の保護をあまり重視しないとする中小企業は一定数存在し、経営層を筆頭にその重要性を浸透させていくことが重要な状況と言える。	
改善策	**現状**
【6-5-5】個人情報以外（営業秘密、重要なデータ等）を念頭に置いた重要情報漏えいの対策を強化する。	・個人情報保護との比較において営業秘密等を保護する対策を同等以上に重視している割合は従業員数が小さくなるほど下がる。中小企業においては、これらの秘密情報の保護をあまり重視していないとする回答も 1 割を超えており、逆に 1 割を超えることのない大企業の傾向と対照的である。

改善策を補う示唆	好事例
・営業秘密を管理するための体制、何が秘密なのかをきちんと資産管理すること等から着手し、これを社内に浸透させていく過程で、自然に内部不正防止・営業秘密保護・サイバーセキュリティの全ての質が向上する。 ・退職時の秘密保持義務契約において、対象とする秘密情報の範囲を具体的に示すことが重要である。 ・入社時の契約書／誓約書で、「退職時にも契約する／誓約書を出す」という条項を書いておくことが有効である。	・経営者のリーダーシップの下で、採用・退職・プロジェクト異動等の際に、都度必要な秘密保持義務契約を締結している。 ・社長の意識づけに従い、プロジェクトごとに情報資産を定義しており、これに基づいて秘密情報を識別できるようにしている。これを活用し、秘密保持義務契約の対象となる秘密情報を具体的に示している。

改善策 6-5-6 と現状の比較	
企業規模が小さくなるほど、情報管理の定期的な見直しや情報資産の棚卸しを定期的に実施している割合が下がる。ここでも見られるのは、技術情報管理などの認証制度を取得した場合に、その規程に沿った取組として実施が確立するという傾向である。実際上の取組を促すと同時に理解を深めるきっかけとして、これらの認証制度が果たす役割は大きいと言える。	
改善策	**現状**
【6-5-6】 情報機密区分に応じたアクセス権限付与状況の点検、アクセス権限付与者についての定期的な棚卸しを実施する。	・資産管理している秘密情報を定期的に見直す、あるいは棚卸しを行っている割合は従業員数が小さくなるほど下がる。特に、従業員数が 100 人以下の企業では定期的な対応ができていないとする回答の方が多い。
改善策を補う示唆	**好事例**
―	・技術情報管理認証を取得した企業では、秘密情報の定期的な棚卸しや不要なものの消去、アクセス権限の見直しに重点を置いてこれを実施している。

③ガイドラインの利用と実践に関する課題の改善（調査軸７）

図表１１０．ガイドラインの利用と実践に関する課題の改善についてのクロス分析結果

改善策 7-1 と現状の比較	
改善策についての現状は確認できていない。	
改善策	**現状**
【7-1】 認知度・活用度合の高い「サイバーセキュリティ経営ガイドライン」「秘密情報の保護ハンドブック」「営業秘密管理指針」「限定提供データに関する指針」「経済安全保障の確保に向けて 2022～技術・データ・製品等の流出防止～」との相互参照を進める。また、支援ツール開発や外部専門家派遣による適用開始支援等を検討する。	―

改善策を補う示唆	好事例
・経済産業省のガイドライン（サイバーセキュリティ経営ガイドライン、秘密情報の保護ハンドブック）との相乗効果を狙って、相互参照を進めることも一案である。 ・東京都の「中小企業向けサイバーセキュリティ対策の極意」は中小企業の担当者にも理解しやすく、有用な学習用資料であり、当該資料との相互参照を実現できると良い。	—

改善策 7-2 と現状の比較	
改善策で示しているニーズが実際にあることを確認できた。営業秘密保護を個人情報保護以上に重視している企業では、ガイドラインを活用している割合が全体平均と比べて高く、特に「経営層への報告や説明の根拠」「社内規程への反映」「従業員教育用のコンテンツ」としての活用は過半を占める。	
改善策	**現状**
【7-2】 概要版の作成、活用しやすい情報量の調整・表現の工夫、社内規程整備のために活用しやすい内容の増補、従業員への周知・教育にそのまま使えるコンテンツの充実等を検討し、「組織における内部不正防止ガイドライン」適用の実効性を高める。	・「組織における内部不正防止ガイドライン」を基本方針や社内規程の検討に役立てている。 ・「組織における内部不正防止ガイドライン」を社員教育用資料のコンテンツとして活用している。 ・「組織における内部不正防止ガイドライン」を対策投資の説明根拠として活用している。 ・営業秘密保護を個人情報保護以上に重視している企業では、ガイドラインを活用している割合が全体平均と比べて高い。特に、「経営層への報告や説明の根拠」「社内規程への反映」「従業員教育用のコンテンツ」としての活用では、いずれも過半を占める。
改善策を補う示唆	**好事例**
・概要版や中小企業向けのハンドブックのような冊子が欲しい。 ・中小企業において求められるコスト・時間と、社員に与えるミッションや情報利用の利便性の間のバランスをどのように取るべきか、またこれについてどのような好事例があるのかについて情報提供して欲しい。	—

(5) 結論と今後の方向性

ここでは、改善策に基づき、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を行った結果に基づき、秘密情報漏えい／内部不正防止の推進における現状の課題と今後の取り得る対策を整理した。

①全体的な課題の改善（調査軸１～５）

経営課題の改善（調査軸１）

過半の経営層や責任者は内部不正とサイバー攻撃の両方を危惧しており、そこに事業リスクがありうるという認識自体は珍しいものではなくなっていると言える。しかし、経営層に関心を持ってもらうことが課題であると有識者は指摘しており、実際の内部不正対策につながるほどの理解の深さや確かさは必ずしも確立していないのが現状であると考えられる。言い換えれば、改善策が指摘する、経営層自身の率先による学びは引き続き重要な課題となっている。

調査を通じて見出された好事例には次のようなものがあった。

- 社外取締役弁護士等からの提起で、取締役会で秘密情報漏えい／内部不正防止について議論する機会を多く設ける。
- 有事の際の損害の大きさを示すリスクマップを活用し、秘密情報漏えいや内部不正が重大なリスクであるという経営層の認識を高める。リスクマップは大企業で作成が進んでいる。

経営層による学びの実態を今回の調査において直接に調べることはできなかった。

内部不正防止に関して、経営層による一般従業員・関連部門との対話の場は過半の企業において設けられており、リーダーシップを発揮し内部不正防止に関する発信が一定程度行われていると言える。従って改善策が示すような、元々あるセキュリティ確保の機会／場を用いて内部不正防止も発信するというような効率化は必ずしも必要とされていない可能性がある。他方で、経営層による内部不正リスクの軽視傾向があるという指摘があることも考慮すると、対話を行うという正しい方向性に沿った取組が進んでいる一方で、その実効性を高めていく必要があると言える。

調査を通じて見出された好事例や示唆には次のようなものがあった。

- 経営層等が自分の考えを全社に何度も伝え、その熱意が全社に浸透していれば、従業員のあるべき行動に繋がっていく。
- 経営層の認識を「加害者でもありうる」というものに変革する必要がある。
- 秘密情報漏えい／内部不正防止とサイバーセキュリティは本来であれば目的が異なる取組なので、しっかりと対応するためには分けて進めるべきである。

経営者が積極的に自身の考えを社内に伝えることの重要性は、有識者の指摘に加え、中小企業における実例としても確認することができた。

重要な秘密の特定と取扱いの改善（調査軸２）

内部不正防止を進める上で基盤となるのが、何が守るべき秘密であるかということを明確にし、従業員自身がそれを認知し、適切に行動できる環境を作ることである。しかし、その具体化となる、秘密の特定および格付けルール策定や表示の徹底、情報資産管理の実施と定期的な見直しといった個別の取組が浸透しているとは言えない。営業秘密保護への意識が高いと関連する取組の実施割合が高まることから、動機付け・意識付けによって改善できる余地はあると見られ、どのようにそれを進めるかが課題であると言える。

調査を通じて見出された好事例や示唆には次のようなものがあった。

- 知らないうちに競合他社に持ち出されるくらいならば営業秘密をきちんと明確化しておこうという動機付けをするのがよい。
- 会社にとって有用な営業秘密をリストアップし、自分たちがやっている仕事がその保護に貢献していることが可視化されると、会社の重要な仕事に貢献しているという認識と満足感が浸透することを期待できる。
- 技術・事業・営業・取引等のノウハウについても、特定すべき重要な営業秘密として、価値を決めることが必要で、大企業ではこの問題意識を持つ担当者が育ってきている。

組織体制・連携に関する課題の改善（調査軸３）

大半の企業で内部不正防止の責任の所在が定められており、更にその責任部門は関連部門と連携し、自部門だけでは賄いきれない専門知識や助力を得ている。組織体制の基本は浸透していると言える一方で、部門間連携の方法には配慮が必要であり、単に連携体制を整備するだけでなく、その連携が生み出す効果にも目を向けることが望ましい。

調査を通じて見出された示唆には次のものがあった。

- 大企業においては知財部門が全社のハブとなり、事業部門などの他の部門と確認を取り合いながら、秘密情報の価値を決めるとよい。

情報システム部門が内部不正防止の責任部門となる場合には、知財・法務部門等の異なる専門部署との連携が必要になる。しかし、組織の在り方の課題としては、それら専門部署間の連携以前に、経営層に対して情報システム部門の意見やリスク認識が伝わらないことが大きいとの指摘があった。これは経営層の積極姿勢が重要であるという指摘の裏返しで、経営層が現場任せにして自らコミットすることを怠ると、責任部門が孤立しうる恐れを示唆する結果と言える。

重要な秘密の不自然な扱いを適切に報告・通報できる仕組みの整備は行き届いていない。

経営層までのエスカレーションルートがある企業は半分に満たず、内部通報体制の整った企業は更に少ない。個人情報以上に営業秘密保護を重視する組織では取組度合いが深まるが、それでもこの傾向は変わらない。大きな課題があると言える。

役職の高い者を特別扱いしないマネジメントシステムの構築・整備状況については実態を調べるに至らなかった。有識者からは次のような示唆が得られた。

- 経営者がまず原則を示し率先してこれを指示した上で、経営層に対する監督強化、内部統制システムの構築、意思決定の透明性確保、倫理意識の醸成、内部通報制度の整備、定期的なリスク評価と対策改善に取り組む必要がある。
- 役職の高い者を特別扱いしないマネジメントの確立には、経験とノウハウの蓄積も必要である。

社員教育とリテラシー構築に関する課題の改善（調査軸４）

内部不正防止に特有の概念や対策についての法的理解が、法務・知財等の部門から情報システム部門へとどのように連携されているかという実態を調査するには至らなかった。有識者からは次の示唆が得られた。

- 営業秘密保護に係る制度（不正競争防止法）については、営業秘密侵害は刑事罰が非常に厳しいこと、両罰規定で会社も罰せられるリスクがあることという 2 点が重要なので、経営層をはじめとして、情報システム担当者やその他の従業員にこの事実を教育・警告すべきである。

内部不正に関する理解を従業員へと浸透させる施策という点では、社内での事件発生時にこれを周辺情報と共に告知したり、秘密情報の不自然な扱いや社外への不正な漏えいを目撃した場合の適切な行動を周知したりするなど、一通りの取組がなされている。個人情報保護以上に営業秘密保護を重視する組織では取組の度合いが深まる傾向があり、問題意識の深さと取組が不可分であることの表れと言える。

有識者からは次のような示唆が得られた。

- 従業員には、営業秘密や重要なデータ等の漏えいがどの程度の損害を生じるのかを教育し、広く認識してもらうことが重要である。
- 従業員のリテラシー欠如、法令やガイドラインに対する無知は内部不正に含まれるという認識を、事例と共に従業員に周知教育すべきである。同時に、基本的な取組の重要性や、法令・ガイドラインを周知できていない経営層にも責任がある。
- ログをきちんと取得して確認していることを社内に通知する、起こった事例を包み隠さず企

業内に周知する、罰則を設けてこれを周知する等が有効である。

従業員に対する営業秘密等の特定・格付けに関する周知・教育自体は大半の企業で行われている。しかし、その実効性を高めるために有効であると思われる定期的な反復や、各自で自己判断できるような深度ある教育となると、大企業でもまだ十分には取り組めていない。

内部不正防止に限らず、専門的な内容の教育手段としては e-Learning が重用されるところ、実効性を高めるにはそれ以外の教育方法も取り入れていることが望ましい。しかし、取りうる方法別で見ると、そのような企業は半数に満たない。手段ではなく伝えるべき内容に目を向けてみても、営業秘密等の漏えいや内部不正に関し、してはいけないことを周知している企業は過半を占めるが、どのように罰せられるかを周知している企業はより少ない。総じて、内部不正防止に関する教育には底上げの余地があると言える。

対策実施に関する課題の改善（調査軸５）

大半の企業が内部不正防止対策とサイバーセキュリティ等のそれ以外の対策とを使い分けており、特に、内部不正防止を基本方針の段階でサイバーセキュリティ等と分けて別建てとしている組織では、内部不正防止に特有の対策を別建てとしない組織よりも積極的に実施している。しかし、そのような意識の高い組織においても、実施すべき対策の浸透状況は十分とは言い難い。個人情報保護以上に営業秘密保護を重視する企業の大半は、対策の使い分けに加えて経営層に定期的にそれらの有効性を報告しており、経営層の積極姿勢につながれば更なる改善も期待できると考えられる。

有識者からは次の示唆が得られた。

- 広い視野で見ればサイバーセキュリティ対策と内部不正防止対策の観点は同じであり、サイバーセキュリティと内部不正防止で共通の対策は適用しつつ、守るべきものとリスクの違いに合わせて足りないところを補っていけばよい。

一見すると、サイバーセキュリティ対策と内部不正防止対策を本来であれば目的の違う取組とする見解とは衝突する示唆と言えるが、実際の対策には共通するものが少なくないのが実情であり、両者を安易に同一視すべきでないことと無駄な重複は省くべきであるということが同時に指摘されていると解釈すれば、矛盾するものではない。

大半の企業において内部不正リスクをそれと意識し評価している。営業秘密保護を重視する度合いの高さと内部不正リスクを分けて評価する傾向は軌を一にしている。他方で、継続中の事業に係る漏えいリスクは楽観論の影響を受けて軽視される傾向がある。内部不正に目を向けたリスク評価の結果が具体的にどのような対策に反映されているかという実態は今回の調査では把

握するに至らなかった。

有識者からは次のような示唆が得られた。

- 秘密情報漏えいの事業リスクアセスメントは、本来プロジェクトごとに実施すべきである。
- 秘密情報が漏えいすると企業の存続すら危うくしうるという危機感を持ち、対策にリソースを投入すべきである。

過半の企業において営業秘密等を個人情報と同等以上に重視しており、しかも、営業秘密等の保護対策を重視する傾向は内部不正防止を別建てにすることと強く結びついている。問題意識と対策の方向性が一致しており、基本的には望ましい状況であると考えられる。機密性の高い秘密情報については過半の企業が管理の定期的な見直し・棚卸しに取り組んでおり、望ましい状況を概ね達成していると考えられる。

②中小企業の構造的課題の改善（調査軸６の１～５）

経営課題の改善（調査軸６の１）

中小企業における経営層のリスク認識は相対的に低く、その一方で、社会環境の変化に伴う秘密情報の漏えいや内部不正防止といった課題の重要度は高まっているとの認識が広がっている。リスク認識の担い手となる意識の高い人材の不足が指摘されており、人材確保・育成と共に、すべての起点となる経営者自身の意識を高めることが特に重要であると考えられる。

調査を通じて見出された好事例や示唆には次のようなものがあった。

- 業界の流れを意識し、技術情報管理の認証取得に取り組んだことが良い契機となった。
- 秘密情報との関りが深い事業を展開しているため自社でもしっかり取り組むことが必須だった。
- 悪意の有無に関わらず、人為的な秘密情報漏えいのリスクが高いと考えて経営している。
- 中小企業では経営層が高い意識を持って率先し牽引すれば会社全体の取組状況をがらりと変えられる可能性を持っている。
- 経営層が秘密情報の漏えいや内部不正防止について全社にしっかりと自分の経営方針を話していくことが望ましい。
- 中小企業では、営業秘密を社内できちんと保護する体制を構築することで、秘密情報漏えい／内部不正防止にも好ましい効果が生じる。

何らかの認証取得のような、外部との関りの中で取組を深める機会は、意識付けのきっかけと

しても有効であると考えられる。

全体としても過半の企業において経営層による一般従業員・関連部門との対話の場が設けられている中で、中小企業ではそれが奏功した場合の効果が大きく期待できることに強みがあると言える。実際、意識の高い経営者による積極的な取組と、それが実際の効果につながっている事例が確認された。他方で、企業規模が小さくなるほど取組度合いも弱くなる傾向があり、大企業を含む全体平均に比べると相対的に不十分である。経営層が部下に任せきりになりがち、潤沢にリソースを投入することが難しい等の、中小企業における一般的課題が関わっているものと考えられる。

また、従業員 100 名以下の企業では、内部不正防止をサイバーセキュリティ確保と意識的に分けるかどうかが概ね拮抗しているため、サイバー攻撃防止とは異なる内部不正防止の特徴等を発信できていない企業が相対的に多くなる。

調査を通じて見出された好事例や示唆には次のようなものがあった。

- 経営者が自ら基本方針を全社に周知・徹底している。
- 定期的にも日常的にも経営者が社員に語ることで意識付け・啓発に効果を上げている。
- 漏えいが自社の信頼失墜に直結することを強く認識して全社に周知・啓発している。
- 秘密情報漏えい／内部不正防止の取組が特に進んでいる中小企業では、情報漏えい／内部不正防止に関する基本方針を情報セキュリティポリシーとは完全に別建てで定めている。
- ISMS、プライバシーポリシー、技術情報管理等の認証取得が、中小企業の経営者が基本方針を定める契機となって取組が進んだ。
- 情報漏えい／内部不正防止に関する経営者の考えを全社に何度も繰り返し伝えることが重要であると認識し、経営者自ら実践している。
- 従業員と直接コミュニケーションを取って趣旨をしっかりと伝えることで、ある程度リスクに対応できる。
- 中小企業の取組強化に向けては、経営者が戦略を語り、コミットメントや指示に自身の想いやこだわりを込め、日々語ることが重要である。
- 経営層が何をどの程度重視しているかを率直に伝えることで、従業員がこれを評価して行動することを期待できる。
- 埋めるべきギャップは大企業より中小企業の方が小さいので、ひとたび良い方向に動き始めると、目標レベルに素早く到達できる。
- 中小企業の規模やリソースを考慮すると、秘密情報漏えい／内部不正防止とサイバーセキュリティを敢えて分けて取り組む必要はない。

重要な秘密の特定と取扱いの改善（調査軸６の２）

全体としても秘密情報の格付け・表示に課題がある中で、中小企業における取組は更に劣後している。秘密情報の特定も十分ではない。紙媒体のような物理的実体のある秘密の保護に比べ、電子化された秘密情報の管理は進んでいない。一方、内部不正防止にもつながる認証の取得を経て具体的な取組に至る事例もあり、経営者の意識付けも兼ねて、何らかの認証の取得を考慮することが実践的な方策の一つになると考えられる。

調査を通じて見出された好事例や示唆には次のようなものがあった。

- 経営者が自ら事業リスクの判断や秘密情報の特定・格付けを行っている。
- 経営者が情報セキュリティや技術情報管理の認証取得を決断し、これに取り組んだことが契機となって、営業秘密等の特定、格付け、表示に関する体制整備が進んだ。
- 認証制度が要求する管理基準に従い、秘密情報を管理できる情報資産台帳を作成している。
- 認証制度に沿って特定した情報資産については、情報の保存場所や保存期間、データ消去の方法やリスクの大きさ、格付けを台帳管理している。
- 情報資産を保存する共有フォルダ等の場所を格付けに沿って切り分け、かつ、適切なアクセス制御・記録を合わせることで、格付け・表示・アクセス管理を一体に実施している。
- 経営者の負担を避けるため、部下を育成し、権限移譲を考えることも必要である。

組織体制・連携に関する課題の改善（調査軸６の３）

規模によれども中小企業では人事・法務といった専門部署が必ずしも細かく分かれていないという現実がある中で、調査結果からは内部不正防止についても経営層が直接の責任者となりやすい様子がうかがえる。改善策が求めるような、経営層が中心となっての総務・人事・法務や情報システム等の担当との調整は、リソース制約の大きい中小企業では現実的な選択肢と言える一方で、それが片手間の取組となって効果を損なうことのないように注意する必要がある。

調査を通じて見出された好事例や示唆には次のようなものがあった。

- 秘密情報漏えい／内部不正防止とサイバーセキュリティの担当役員を分け、監督も別々に実施し、経営者がこれを統括している。
- 経営者を責任者とする 3~5 名程度の幹部による委員会を設置している。その下にシステム、総務・人事、教育、内部監査等を担当する幹部が集まって委員会を構成する。
- 経営者が責任を担い、品質管理責任者が横串を通す形で、関連部門を連携させている。各種のマネジメントシステムを構築・運用する際に品質管理責任者が必ずこれに協力し、品質管理責任者を中心とした社内ネットワークを形成している。

- 秘密情報保護に関する重要な主題（秘密保持義務の誓約、懲罰、情報セキュリティ対応等）ごとに担当チームを組成し、各チームが基本方針を定めて取組を実施している。経営者はチーム全体の統括責任者となり、必要に応じて各チームと関連組織の協議を主導する。
- 社内に委員会を設けるなどして、複数部門が連携して取り組むことができる体制を検討することが望ましい。

中小企業では従業員と経営層の距離が近いと目されるところ、経営層へと報告が上がるルートの確立度合いは大企業が勝っている。この背後には、ルールに基づくマネジメントの浸透度合いと企業規模が連動するという傾向に加え、距離が近いからこそ性善説を頼ってしまいがちであるという文化も関わる。体制の整備に先立ち、経営層による現場への具体的な意識付けを行うことが有効であると考えられる。

調査を通じて見出された好事例や示唆には次のようなものがあった。

- 秘密情報が漏えいした時や従業員がヒヤリハット・不信感を認識した時に、直属の上司を通じて経営者にすぐに報告が上がってくる仕組みを設けている。
- 中小企業は人間関係が良く性善説を基にしていることが多いので、内部通報ができる仕組みを構築すると逆に従業員の不信感が高まる恐れがあり、注意が必要である。

社員教育とリテラシー構築に関する課題の改善（調査軸６の４）

社外の専門家の助力を得て法務・知材の知識を情報システム部門等に広める取組の実態を調査するには至らなかった。改善策に言うような退職時における秘密取り扱いの説明・教育を行っている事例は見出されたが、中小企業における取組は全体としては劣後しており、例えば経営幹部のそれも含め、内部不正の発生を全社に告知している企業は 4 割に達しない。他社で発生した参考事例の情報を収集することも中小企業では難しく、全般に取組の底上げを図る必要があると言える。

調査を通じて見出された好事例や示唆には次のようなものがあった。

- 営業秘密・重要データの知識に関する社員教育にも取り組み、入社時のオリエンテーション、年 1 度の e-Learning や年 2 回の集合教育、全社集会の機会を活用した教育を行っている。
- リスクとその重要性、過去に発生した事例における重要なリスクと実際に発生した損害、社内で発生したヒヤリハットの経緯や内容等を伝えている。
- 退職時に秘密情報を持ち出すリスク、実際に持ち出した事例等に重点を置いて教育している。

- 中途退職時に禁止されている事項を教育している。
- 経営者が自ら参考事例等の情報を収集している。
- セキュリティ会社に委託し、他社で発生した事件の情報、注意点、セキュリティ管理の考え方等の情報を提供してもらっている。
- 中小企業には営業秘密の秘密管理性の確保が自己防衛及びビジネス拡大に不可欠であることを大企業以上に認識してもらうことが望ましい。
- 事業拡大に悪影響を及ぼしうることを考慮し、知財専門人材が社内にいない場合は業界団体等を通じて外部の専門職（弁護士・弁理士等）と連携することが望ましい。

中小企業における営業秘密等の特定・格付けに関する周知・教育の実施割合は大企業に比べてはっきりと劣後している。しかしながら、そうした周知・教育の定期実施や、表裏一体になるはずの秘密情報の格付け・表示の徹底は大企業でも十分とは言えない状況であり、中小企業における実践と有効化は非常に難しい課題であると考えられる。調査では次の好事例が見出されたが、経営者の負担という点で課題なしとはできない。

- 経営者が自ら事業リスクの判断や秘密情報の特定・格付けを行っている。

内部不正防止対策として従業員の行動を記録・監視することへの抵抗感が中小企業の間には見られる。有識者も指摘する通り、中小企業では経営層と従業員の距離が近く、このような心理的課題への対処に当たっては経営層自身の細やかな配慮が必要になると考えられる。有識者からは次の好事例が示された。

- 抵抗感を示す事例以上に、有識者の適切な助言等に基づいてこれを導入し組織に根付かせることで、むしろ会社への帰属意識や仕事に対するプライドといったものが上がってきて緊張感が醸成され、会社の雰囲気が良くなってきたと言われることも多い。

内部不正に当たる違反行為や罰則の定めを周知している割合は、大企業で過半を占めるのに対し、中小企業では半分に満たず、取組状況に隔たりが見られる。経営層による指示・啓発の全体像を調査するには至ってないが、実際に経営者が手ずから取り組んでいる事例は確認できており、改善策の方向性は妥当であり、かつ、今後の浸透が望まれる内容と言える。

調査を通じて見出された好事例には次のようなものがあった。

- 営業秘密や限定提供データに関する従業員教育で、これらの取扱方法に加えて、禁止事項・内規の懲罰規定・法の遵守等についても教育している。
- 個人情報保護法、不正競争防止法、外為法等を対象として解説動画や弁護士の説明を教材に取り入れて従業員に教育することで、民事的な賠償責任や刑事責任を負ったりする場合があること等を理解させている。

- 経営層が率先して集める、外部委託先から情報提供を受ける等の手法で、他社で発生した事案の情報を取りまとめ、社会的な影響なども含めて教育している。

中小企業では e-Learning 以外の方法を取り入れている割合が下がる傾向がある。相対的によく実施されているのはインシデント事例の説明だが、実施率で見ると 4 割に満たず、経営層と従業員の距離の近さを生かし切れていない状況と言える。

調査を通じて見出された好事例には次のようなものがあった。

- 人数とリソースが少ない中小企業が選択しやすい教育方法として、外部講師（例えば IT コーディネータ）を招いて研修を行っている。
- 日常業務において秘密情報の取り扱いに問題がないか、社員同士で相互確認する日々実践形式の教育を取り入れている。

対策実施に関する課題の改善（調査軸６の５）

内部不正防止の一環として従業員の行動を記録・監視することに中小企業の間では抵抗感がある一方で、十分なコミュニケーションをとり、なぜ記録・監視が必要であるかをていねいに説明することで理解を得ている事例のあることを確認できた。改善策の示す方向の妥当性を裏打ちするものと言える。

中小企業においては内部不正防止対策とサイバーセキュリティ対策を同一の取組の一環として実施する傾向がある。この背景には、リソース制約に加えて、ISMS や技術情報管理のような認証制度のスコープ中に内部不正防止が含まれていることが関わっていると考えられる。ただし、これは内部不正防止に固有の対策の実施が弱体化するという懸念もはらむものであり、実際、従業員数が増えるほど内部不正防止対策を他の対策と使い分ける傾向も見出された。経営資源に合わせた適切なバランス配分・判断が必要であると言える。

調査を通じて見出された好事例や示唆には次のようなものがあった。

- 秘密情報の漏えい防止に向けた内部不正防止対策とサイバーセキュリティ対策を同一の取組の一環として実施している。この一因として、ISMS や技術情報管理の認証のスコープが両者をカバーしていることが挙げられる。
- ミスが発生した際の報告について、これを隠ぺいする組織風土にならないように、自発的な報告を考課で高く評価している。
- 経営者が自ら事業運営と内部不正防止／情報セキュリティの両方にコミットしている。
- 不正が発覚した際の社内告知については、特に 1 人 1 人の顔が見えるぐらいの組織規模の場合に、慎重に伝え方を選ぶ必要がある。

■ 経営者の負担が大きくなりすぎないように気を付ける必要がある。

内部不正防止はサイバーセキュリティに比べれば浸透していない考え方である。そこで、内部不正防止対策をサイバーセキュリティ対策に対して追加的に組み合わせる道筋の一つとして、まず内部不正リスクそのものを評価する取組に本調査では着目した。しかし、内部不正リスクを他のリスクと切り分けて評価する中小企業は半分に満たない。事例からは、リスクアセスメントの実施が、関連する認証制度の規定に強く影響されている様子が垣間見える。それぞれの企業の事情に応じたリスクアセスメントに基づく内部不正防止のアプローチは、まだハードルの高いものであると推察される。

調査を通じて見出された好事例や示唆には次のようなものがあった。

■ 秘密情報漏えいの事業リスクとその重要度を事業継続性の中でどのように位置付けるかについて、経営層の間で認識を共有している。
■ 従業員の秘密保持義務に関し、入社時の誓約書で「退職する時にも誓約書を提出すること」を誓約してもらっている。
■ 対処の難しさを理解した上で次のような色々なリスクに注意を払っている：秘密情報の意図的な持ち出し、電子メールの誤送信、その他不注意やミスによる情報漏えい、個人所有の BYOD 利用、中途退職者の持ち出し。
■ 中小企業では他社の事例等に基づいて意識の高い経営層がリスクを判断できれば、秘密情報漏えいや内部不正のリスク評価をある程度代替できる。

内部不正防止は営業秘密漏えいの防止と密接に結びつくが、そもそも営業秘密等の保護を重視する企業の割合は企業規模が小さいほど下がる。営業秘密等の保護をあまり重視しないとする中小企業は一定数存在し、経営層を筆頭にその重要性を浸透させていくことが重要な状況と言える。

調査を通じて見出された好事例や示唆には次のようなものがあった。

■ 経営者のリーダーシップの下で、採用・退職・プロジェクト異動等の際に、都度必要な秘密保持義務契約を締結している。
■ 社長の意識づけに従い、プロジェクトごとに情報資産を定義しており、これに基づいて秘密情報を識別できるようにしている。これを活用し、秘密保持義務契約の対象となる秘密情報を具体的に示している。
■ 営業秘密を管理するための体制、何が秘密なのかをきちんと資産管理すること等から着手し、これを社内に浸透させていく過程で、自然に内部不正防止・営業秘密保護・サイバーセキュリティの全ての質が向上する。

- 退職時の秘密保持義務契約において、対象とする秘密情報の範囲を具体的に示すことが重要である。
- 入社時の契約書／誓約書で、「退職時にも契約する／誓約書を出す」という条項を書いておくことが有効である。

企業規模が小さくなるほど、情報管理の定期的な見直しや情報資産の棚卸しを定期的に実施している割合が下がる。ここでも見られるのは、技術情報管理などの認証制度を取得した場合に、その規程に沿った取組として実施が確立するという傾向である。実際上の取組を促すと同時に理解を深めるきっかけとして、これらの認証制度が果たす役割は大きいと言える。

③ガイドラインの利用と実践に関する課題の改善（調査軸７）

組織における内部不正防止ガイドラインを活用しやすくするために、読み手にどのようなニーズがあるかをあらためて調査した結果、従来からある概要版の作成、活用しやすい情報量の調整・表現の工夫、社内規程整備のために活用しやすい内容の増補、従業員への周知・教育にそのまま使えるコンテンツの充実等へのニーズがあることを確認できた。また新たに、従業員教育の教材として利用しやすい別添のコンテンツ（講義に活用できるスライド形式の説明資料、動画等）の提供希望があることが分かった。

- 組織における内部不正防止ガイドラインを実務で活用しやすくするためには、引き続き、概要版の作成、活用しやすい情報量の調整・表現の工夫、社内規程整備のために活用しやすい内容の増補、従業員への周知・教育にそのまま使えるコンテンツの充実等が求められている。
- 新たな要望としては、従業員教育の教材として利用しやすい別添のコンテンツ（講義に活用できるスライド形式の説明資料、動画等）への希望があった。

5. まとめと今後の方向性

(1) 調査結果のまとめ

本調査の調査結果と今後の方向性については、一旦４．(5)でまとめた。ここでは、この取りまとめ結果を踏まえて、得られた示唆における中小企業と大企業の間の違いについて述べる。

【経営課題の改善】

第一の論点として、秘密情報漏えい／内部不正防止とサイバーセキュリティを別々の経営課題として捉えるべきかどうかという判断がある。両者を別建てにして扱う組織では内部不正防止対策の実施度合いも深まる傾向のあることが調査結果に表れており、可能であれば分けて考えることが望ましいと言える。他方で、中小企業では経営課題として両者を意識的に分ける傾向が弱く、むしろ共通する対策を一本化しつつ、固有の対策を適宜組み合わせるといった、シンプルな対策を主軸に据えた様子が垣間見えた。企業規模の拡大と共に後者から前者へと進展する様子もあり、単純に別建てを目指すというよりも、状況や目的に即した内部不正防止対策の先鋭化を判断することが重要であると考えられる。

第二の論点は、意識の低い経営層にどうやって秘密情報漏えい／内部不正防止の重要性を認識してもらうかということである。大企業であればリスクマップのようなツールを活用してリスクとその特性を可視化することが手段となりうる。ただ、この種のツールの導入・運用は一般に容易ではなく、企業規模によらず一律に推奨できる方法と直ちに言うことはできない。むしろ中小企業では、ISMS や技術情報管理等の認証取得、業界全体での取組等をきっかけとして、対策の実施と合わせて理解や意識が深まる様子がある。加えて、少数の経営層の権限が強い中小企業においては、経営層の理解・判断が企業全体の在り方に及ぼす影響が、大企業よりも速やかに浸透する。そのことを踏まえ、外部の IT コーディネータ等の力も借りながら、中小企業では経営者が自身の努力で学びを深め、それを具体的な経営判断に反映してゆくことが必要である。

【重要な秘密の特定と取扱いの改善】

秘密情報の特定・格付け・表示に関する取組は企業規模によらず不十分である。この背後には、扱わなければならない情報の量と、秘密情報の特定・格付け・表示に投入できる経営リソースの量の兼ね合いがあるところ、リソースに対し情報量が一般に過大となっている状況があると解釈しうる。同時に、中小企業において大企業よりも有利なポイントは、事業内容によるとはいえ、中小企業の規模であれば経営者が自ら重要な秘密を特定し、特定や格付けに取り組む機動力を発揮しうるところである。重要な秘密の事業価値と漏えいリスクについて、経営者が自らの理解と判断を示すことで、特定・格付け・表示の実効性を高められると期待できる。但し、経営者が

これを行うことで、自らが過負荷にならないように留意する必要がある。

【組織体制・連携に関する課題の改善】

調査結果からは、内部不正防止やサイバーセキュリティの分野ごとに対策方針を明確化するのに伴い、個別の対策の実施が深まる様子が明らかになっている。この傾向は企業規模の増大とも軌を一にする。大企業においては人事・総務・法務・知材・情報システムといった専門部署がそれぞれに独立した組織として社内に設置されるのが普通だが、中小企業では必ずしもそうではなく、特定の担当はいても部署はない、あるいは、多くの機能を経営者や部門責任者等が兼担することが珍しくない。内部不正防止は組織横断の対策が必要な分野であるところから、各種の機能が部門等の組織に分かれている場合には社内での組織間連携が必要であり、担当者のようなより小さな単位で経営機能が分割されている場合には委員会設置などにより社内を横断しての連携が機能するよう取り計らう必要がある。いずれにせよ、経営者は全体の方針決定や調整に重要な役割を担うことになる。

【社員教育とリテラシー構築に関する課題の改善】

今回の調査では内部不正防止に関する専門知識が社内連携を通じてどのように支えられているかを把握するには至らなかった。

社員教育とリテラシー構築に関しては、内部不正防止に限らず e-Learning が有力な手段と考えられる一方で、教育効果の向上や定着を進めるために、e-Learning 以外の方法を取り入れたり、周知・教育の実施を定期化したりすることが望ましい。この点では大企業の取組も道半ばと言える。この点での中小企業の強みは、経営者と従業員の対話の場を設けやすく、そうした場で経営者が全従業員に、自分の経営方針や蓄積した知見を直接伝えることができるというところである。経営者の言葉で語られる内容は、それだけ強い力を持って浸透するものと期待できる。他方で大企業においては、従業員に分かりやすい内容と方法で教育する仕組みが必要となる。

【対策に関する課題の改善】

リスクマネジメントの一般論として、経営リソースの制約がある中で効果を最大化するには、リスクアセスメントに基づき適材適所で講ずべき対策を選択することが望ましい。内部不正リスクとそれ以外のリスクを分けて評価する傾向が内部不正防止対策の実施度合いの高まりと連動していることはこの表れと言える。これと一体に、内部不正防止対策とサイバーセキュリティ対策等は原則として使い分ける方がよい。しかしながら、対策の細分化は実施コストの上昇も伴うため、リソース制約の厳しい中小企業においては、むしろ共通性の高い対策を積極的に一本化しつつ、適切なバランスを考慮して個別の対策を追加的に組み合わせるのが合理的であると考えられる。ISMS や技術情報管理などの認証制度の中にはリスクアセスメントも個別的対策も一式が含ま

れ体系化されていることから、中小企業においては自社に適切と思われる認証の取得を検討し、それを起点に取組を深めてゆくことがよい礎になると考えられる。

このように、秘密情報漏えい／内部不正防止への望ましい取組は、大企業と中小企業でかなり異なることが分かってきた。これを踏まえ、今後あるべき姿のさらなる具体化に取り組むことが望ましい。図表１１１はここまでで述べた内容のまとめである。

図表１１１．得られた結論　～中小企業と大企業の比較～

調査軸	中小企業	大企業
経営課題の改善（調査軸１）		
	■内部不正防止とサイバーセキュリティを切り分けるべきか否かといった経営課題としての適正な認識は経営規模によって変化する。状況に照らして経営者の判断が肝要となる。 ■適切な判断の基礎を得るためにも、経営者が自ら率先して学ぶことが望ましい。ISMS、技術情報管理等の認証取得、業界全体での取組への対応等は取組の向上と学びのきっかけとして有意義である。 ■経営者の判断と行動が自社の変革において極めて力強い役割を担うことを、経営者は強く自覚すべきである。	■内部不正防止とサイバーセキュリティは別の経営課題として捉えるべきである。 ■大企業であっても経営層のリスク認識を高めることの重要性は変わらない。リスクマップ等の可視化ツールを活用することで経営層におけるリスク認識の適正化を図りうる。
重要な秘密の特定と取扱いの改善（調査軸２）		
	■秘密情報の特定・格付け・表示の徹底は不十分である。 ■経営者が自ら重要な秘密を特定し、格付けすることが可能である。但し、経営層が過負荷にならないように留意しなければならない。	■秘密情報の特定・格付け・表示の徹底は不十分である。 ■秘密の特定・格付けルール策定や表示の徹底、情報資産管理の実施と定期的な見直しの仕組みを作り、策定したルールや管理策が有効に機能するよう努めるべきである。
組織体制・連携に関する課題の改善（調査軸３）		
	■経営層の主導の下、組織横断の対策が適切に実施されるよう、必要に応じて部署・担当者間の連携を具体化するべきである。	■内部不正防止やサイバーセキュリティなどの分野別に、それぞれが主体的に動くべき関連部署・部門間の適切な連携体制を構築するべきである。
社員教育とリテラシー構築に関する課題の改善（調査軸４）		
	■全社集会等を活用して、経営者自身の言葉を用いて経営方針や知見を伝えることが有効である。	■従業員にとって分かりやすい内容と方法で教育することが必要である。
対策に関する課題の改善（調査軸５）		
	■認証制度等の既存体系を参考にしつつ、内	■内部不正リスクを切り出して評価し、適切な

調査軸	中小企業	大企業
	部不正防止に特有の対策等を選定し、サイバーセキュリティ対策等へ追加する形で実施すべきである。	対策を選定・実施すべきである。

(2) 調査の課題と今後の方向性

本調査では、昨年度の調査結果を念頭に置き、中小企業の実態把握に重点を移して調査を実施した。その一環として、秘密情報管理に対する意識が高い複数の中小企業の経営者や経営幹部を対象にインタビューを実施し、有意義な調査結果も得られている。これらの中小企業は、秘密情報漏えい／内部不正防止の取組が非常に進んだ企業に相当し、中小企業が目指すべき好事例を多数確認することができた。また、内部不正防止に関わる領域の複数の有識者から多角的な意見を集め、実態調査と有識者による示唆とを組み合わせた総合的な結果を得ることができた。これは本件調査のフレームワークの有効性を示す成果とも言える。

他方で、今回の調査では改善策の整理を通じて得られた多種多様な視点が十分には体系化されておらず、アンケート調査の質問項目等にすべての論点を反映することはできなかった。この結果として、調査に関わる論点として意識していたにも関わらず、直接に対応する調査結果を得られなかった項目もある。議論の精緻化や、調査結果の説得力向上を果たすためには、こうした欠落を減らす必要がある。加えて、調査期間が短期集中でもあり、膨大な量の収集情報を前に、考察を深める余地が多く残った印象もある。

今後の調査では、上記の成果と課題を意識しつつ、有益な知見を更に得ることを目指したい。特に、本調査により特定された個別の課題と改善策の取組状況について、中小企業による実践を強化・促進する具体的な知見を得られればと願う次第である。

謝辞

最後に、本調査におけるアンケートやインタビューにご協力いただいた皆様に、感謝を申し上げる。また、本報告書の事例調査の遂行にご協力いただいた弁護士法人 NEX の渡邉遼太郎弁護士に感謝の意を表し、本報告書を締めくくる。