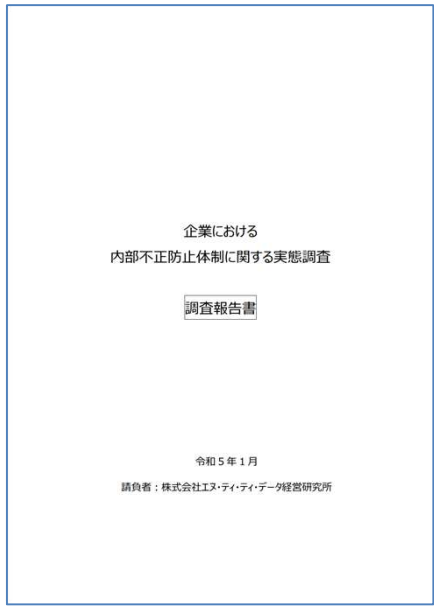
IPA「企業における内部不正防止体制に関する実態調査」のポイントを読み解く（調査結果の詳細解説）

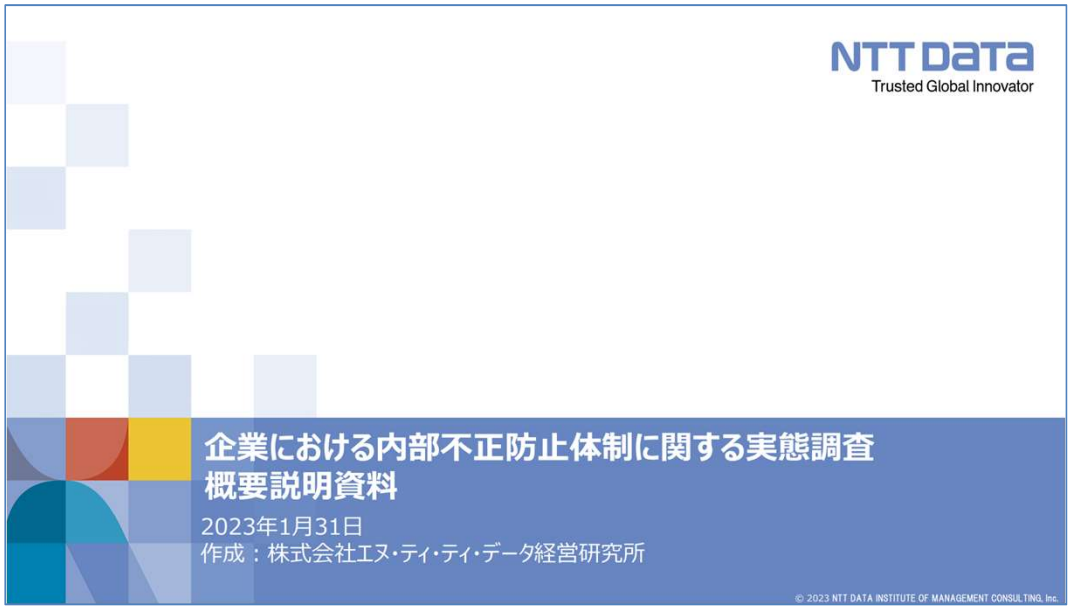
２０２３年　５月２６日

営業秘密保護推進研究会　事務局長
株式会社NTTデータ経営研究所　三笠　武則

はじめに

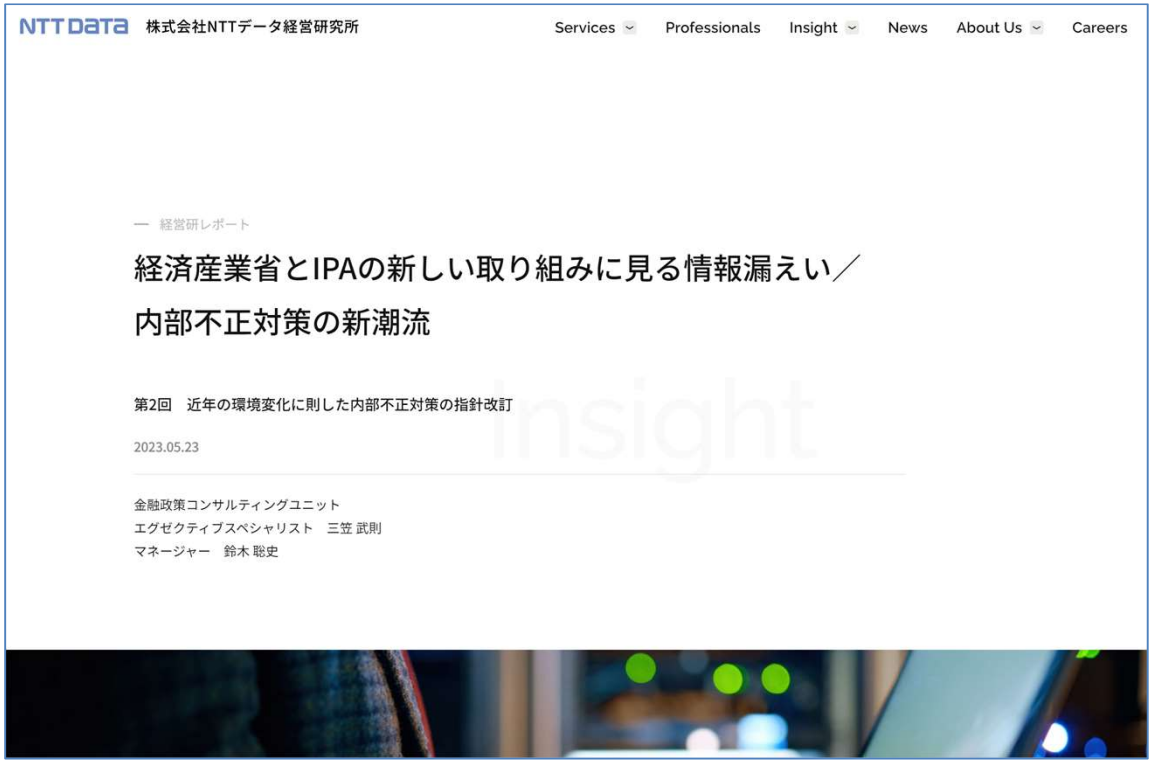
この資料における「内部不正」とは、デジタル化された重要情報の漏えいを生じる「内部不正」のことです。
この資料のベースとなった「企業における内部不正防止体制に関する実態調査」（以後、「IPA調査事業」）の成果物は下記で公開されています。
「企業の内部不正防止体制に関する実態調査」報告書（2023年4月6日公開）
https://www.ipa.go.jp/security/reports/economics/ts-kanri/20230406.html





（ご参考）IPA「組織における内部不正防止ガイドライン」第5版の解説

本資料と関わりが深いIPA「組織における内部不正防止ガイドライン」第5版については、最近公開した拙稿「経済産業省とIPAの新しい取り組みに見る情報漏えい／内部不正対策の新潮流　第2回　近年の環境変化に則した内部不正対策の指針改訂」をご参照ください。
https://www.nttdata-strategy.com/knowledge/reports/2023/230523_01/



IPA調査事業の背景と目的

（以下、引用）

IPA調査事業実施の背景：

企業が保有する営業秘密などの重要情報の保護は企業経営上の重要な課題であり、内部不正による情報漏えいの防止に資するため、IPAでは2022年4月に「組織における内部不正防止ガイドライン」を第5版に改訂し、近年の環境変化を踏まえた対策を加えた情報提供を実施しています。

一方で、内部不正による情報漏えいに係る企業の課題認識、対策状況、マネジメント体制等の実態は必ずしも明らかにはなっていません。

当該調査事業実施の目的：

このたびIPAでは、企業の対策・体制に関する実態を把握し、各企業における今後必要とされる有効な施策立案に資するための調査を行いましたのでその結果を公開します。

（出典）https://www.ipa.go.jp/security/reports/economics/ts-kanri/20230406.html

検証した仮説について

IPA調査事業が検証した仮説は4分野19項目に及ぶ。ここで4分野とは、「基礎知識の習得レベル」、「組織体制の整備」、「組織的な周知・教育の現状」、「対策整備の現状」である。

1. 企業・組織全体として知っておくべき基礎知識の実態（基礎知識の習得レベル）
   情報漏えい／セキュリティリスクに関する知識レベルが把握できない、または知識が足りない
   その他、社内規程、法制度／ガイドラインについての知識にも言及

2. 内部不正防止に取り組む組織的体制の実態（組織体制の整備）
   組織全体としての責任・権限が明確に定められていない
   社内ポリシー／規定の整備が不十分な企業が多い　等

3. 組織全体への周知・教育の実態（組織的な周知・教育の現状）
   一般の職員に対する、内部不正対策に関する周知・教育は不足している　等

4. 内部不正防止の課題と対策（対策整備の現状）
   重要情報の範囲が個人情報から技術情報・ノウハウ等にまで広がっているものの、これらの漏えいに対するリスク認識が十分ではなく、内部不正対策の拡張が進んでいない
   急増する中途退職者／中途採用者の内部不正に対する対策整備が遅れている、または対策が実施できていない　等

（出典）企業における内部不正防止体制に関する実態調査概要説明資料

今日の解説において特に重要なキーワードとは？

本日お話しする内容において、特に重要と考えている着眼点について提示しておきます。

1. 内部不正リスクは重要な経営課題として捉えられているか／どうすれば捉えてもらえるか？
2. 個人情報の漏えいに偏っていないか？重要技術情報・ノウハウ／その他の営業秘密や重要なデータ／限定提供データにも手が回っているか。
3. 組織全体での内部不正防止体制と責任分担は、どうあるべきなのか？
4. 事業リスクは腹落ちして重視されているか？対策は腹落ちして実践されているか？どうすれば腹落ちしてもらえるか？
5. 役職の高い人による内部不正にどう向き合うか？
6. サプライチェーンでの対策強化は、現場まで行き届いているか？
7. 中途退職時の秘密保持義務の有効性はどうすれば高められるか？
8. テレワークやクラウド利用時の内部不正防止に実効性はあるか？
9. どうすれば中小企業を底上げできるか？　　等

目次

1. IPA調査事業で実施した調査の概要
2. 概観　～アンケート単純集計より
3. アンケート調査結果の分析から得られた示唆
4. 企業／有識者の実感とあるべき姿への示唆
5. 総括

１．IPA調査事業で実施した調査の概要

実施した調査の種別

実施した調査は、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３つ。

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

企業アンケート調査

大規模調査パネル登録モニター

日経平均銘柄企業

※大企業の類型として参考比較調査を実施

結果を比較

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

企業インタビュー調査

結果インプット

有識者インタビュー調査

調査対象：「i.内部不正防止に関わる最新の法制度の動向に詳しい専門家」、「ii.内部統制、リスクマネジメントの専門家」、「iii.データ利活用、知的財産関連の専門家」

出典：企業における内部不正防止体制に関する実態調査概要説明資料

（ご参考）調査実績

各調査の実施件数は以下のとおり。

【調査の実施および回収件数】

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

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

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

出典：企業における内部不正防止体制に関する実態調査概要説明資料

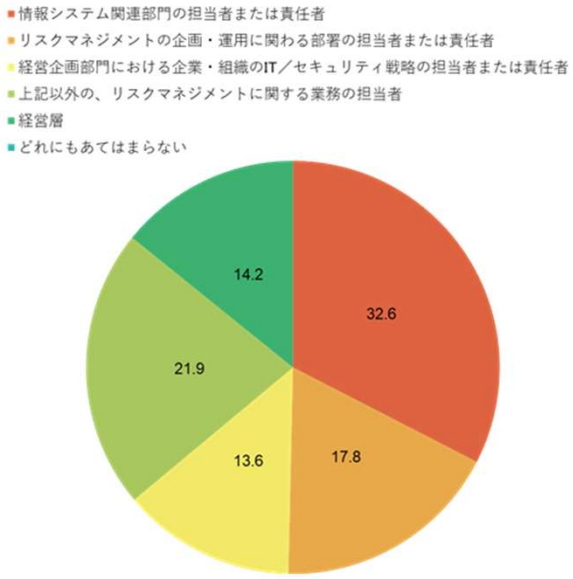
アンケート回答者の担当業務

情報システムやIT／セキュリティ担当者の回答が多く、次がリスクマネジメント担当者であった。

情報システム関連部門の担当者または責任者：　32.6%
経営企画部門における企業・組織のIT／セキュリティ戦略の担当者または責任者：　13.6%
小計：　46.2%

リスクマネジメントの企画・運用に関わる部署の担当者または責任者：　17.8%
その他のリスクマネジメントに関する業務の担当者：　21.9%
小計：　39.7%

経営層からの回答も14.2%ほどあった。
経営層自身がどのように回答しているかは興味深い！



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

出典：企業における内部不正防止体制に関する実態調査概要説明資料

ご回答いただいた経営層の内訳

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

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

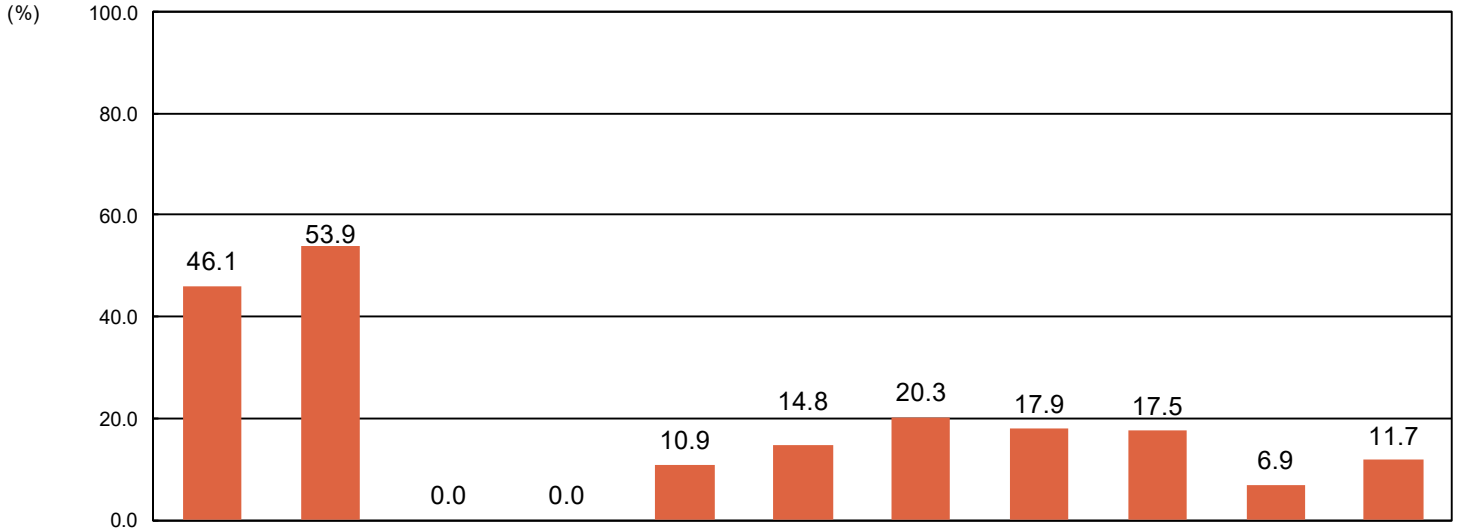
※1,000人以下と
それ以上で概ね半分ずつ

出典：企業における内部不正防止体制に関する実態調査概要説明資料

アンケート回答者の所属企業の企業規模

アンケート回答者は、大企業にも中小企業にも偏っておらず、大企業が若干多い程度である。

常用雇用者数が300人以下： 46.1%
常用雇用者数が301人以上： 53.9%



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

出典：企業における内部不正防止体制に関する実態調査概要説明資料

アンケート回答者の所属企業の業種

アンケート回答者が所属する企業の業種については、3.建設業（6.6%）、20.その他製造業（5.0%）、24.情報サービス業（12.1%）、27.運輸業・郵便業（5.1%）、28.卸売業・小売業（8.1%）、29.金融業・保険業（7.4%）、31.その他のサービス業などがやや数が多くなっている。なお、この割合は実際に存在する企業数の割合とは一致していない。

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

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

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

出典：企業における内部不正防止体制に関する実態調査概要説明資料

２．概観　～アンケート単純集計より

調査結果の注目点

調査結果を読み解く上で最も重要な注目点は、「企業が内部不正リスクを重要な経営課題として捉えているか」どうかである。**経営層や内部不正防止に関する全社責任者が事業リスクを十分に認識し、優先度の高い経営課題として捉えることこそが、まず目指すべき姿**である。

内部不正リスクを重要な経営課題として捉えている企業では、そうではない企業と比較して：

1. 経営層が日常的に内部不正防止の取組等を全従業員に周知、指示している
2. 情報漏えいリスク／セキュリティリスクの知識が、組織全体に、より一層浸透している
3. 内部不正防止のためのリテラシー教育の提供が、より一層進展している
4. 内部不正防止のための指針や規定を定めている割合が、より一層高い
5. 内部不正対策が全般に亘って、より進展している

などの特徴がはっきりと結果に表れている。
従って、「内部不正リスクを重要な経営課題として捉える」ことが、内部不正防止に関する取組を幅広く進める上での「起爆剤」になると考えてよい。

※詳細は「３．アンケート調査結果の分析から得られた示唆」で解説。

出典：企業における内部不正防止体制に関する実態調査概要説明資料

内部不正リスクを重要な経営課題として捉えている企業はどの程度あるのか

「貴社では、内部不正リスクは重要な経営課題として捉えられていますか」という問いに対して、「**経営層が内部不正の事業リスクについて十分に認識し、優先度の高い経営課題として捉えている**」と答えた回答者の割合はほぼ**40%**に留まっており、十分に高い水準に達しているとは言えない。この数字をさらに上げることが喫緊の課題。

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

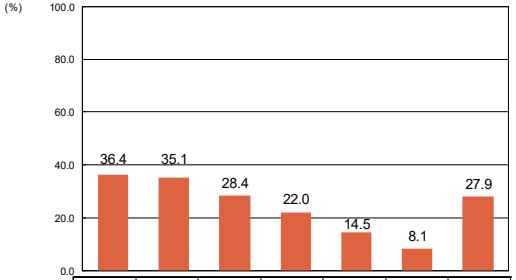
出典：企業における内部不正防止体制に関する実態調査概要説明資料

内部不正防止が個人情報に偏っていないか

もう１つの重要な注目点は、**情報漏えい及びこれに関わる内部不正防止が個人情報に偏っており、営業秘密や限定提供データでは対策が不十分なのではないか**という懸念である。

個人情報の漏えい事案／インシデントと、営業秘密や限定提供データの漏えい事案／インシデントとの間で
経験した割合に大きな違いはないが・・・

1. 個人情報の漏えい（未遂を含む）を経験：36.4%
2. 営業秘密の漏えい（未遂を含む）を経験：35.1%
3. 限定提供データなど１．や２．以外の重要データの漏えい（未遂を含む）を経験：28.4%



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

出典：企業における内部不正防止体制に関する実態調査概要説明資料

・・・しかしながら「個人情報保護」＞「営業秘密／限定提供データ保護」の現状が如実に顕在化している。

1. 個人情報保護法制と比べると、不正競争防止法（営業秘密、限定提供データ）に関する**リテラシー教育はかなり遅れている。**
2. その影響なのか、個人情報管理のための規則と比べると、営業秘密管理や限定提供データ管理のための**規則の制定はかなり遅れている**実態がある。
3. 従って、個人情報管理のための規則と比べると、営業秘密管理や限定提供データ管理のための**規則が組織全体で認知されている割合もかなり低い。**
4. さらには、個人情報の特定に比べると、営業秘密や重要データを**特定する仕組みの整備がかなり後手に回っている。**
5. **内部不正対策を所管する部署であっても**、個人情報保護法と比べて、不正競争防止法（営業秘密、限定提供データ）に関する**知識の蓄積がかなり遅れている。**
6. これらを考慮すると、「個人情報だけでなく、**重要技術情報・ノウハウ、重要データに対する内部不正にも対応できている」とした回答者の割合は27%に過ぎないことも納得できる。**

内部不正防止が個人情報に偏っていないか

前ページ右側の指摘に関する数的根拠を、このページで示した。

【リテラシー教育の遅れ】
リテラシー教育で周知・教育している割合：
1. 個人情報保護の法制度に関する知識　66.1%
2. 営業秘密保護の法制度に関する知識　47.2%
3. 限定提供データ保護の法制度に関する知識　31.6%

【規則制定の遅れ】
内部不正防止について規則が定められている割合：
1. 個人情報管理のための規則　36.9%
2. 営業秘密管理のための規則　23.8%
3. 限定提供データの管理のための規則　16.8%

【規則が組織全体で認知されている割合が低い】
規則が組織全体で認知されている割合：
1. 個人情報管理の規則　48.8%
2. 営業秘密管理の規則　30.5%
3. 限定提供データ管理の規則　20.6%

【重要情報を特定する仕組みの整備の遅れ】
重要情報を特定する仕組みを整備している割合：
1. 個人情報　70.6%
2. 重要な技術情報・ノウハウ　47.4%
3. 重要な営業情報　48.9%
4. 営業秘密として管理している情報　44.2%
5. 限定提供データとして管理しているデータ　22.1%

【内部不正対策を所管する部署における知識蓄積の遅れ】
内部不正に関わる法制度の知識を蓄積している割合：
1. 個人情報保護法（利用目的の遵守）　58.1%
2. 個人情報保護法（第三者提供の要件）　55.0%
3. 個人情報保護法（内部不正による個人データ漏えい時の報告義務）　55.6%
4. 不正競争防止法（営業秘密の要件）　39.2%
5. 不正競争防止法（限定提供データの要件）　31.0%

出典：企業における内部不正防止体制に関する実態調査概要説明資料

（参考）組織全体で知っておくべき基礎知識

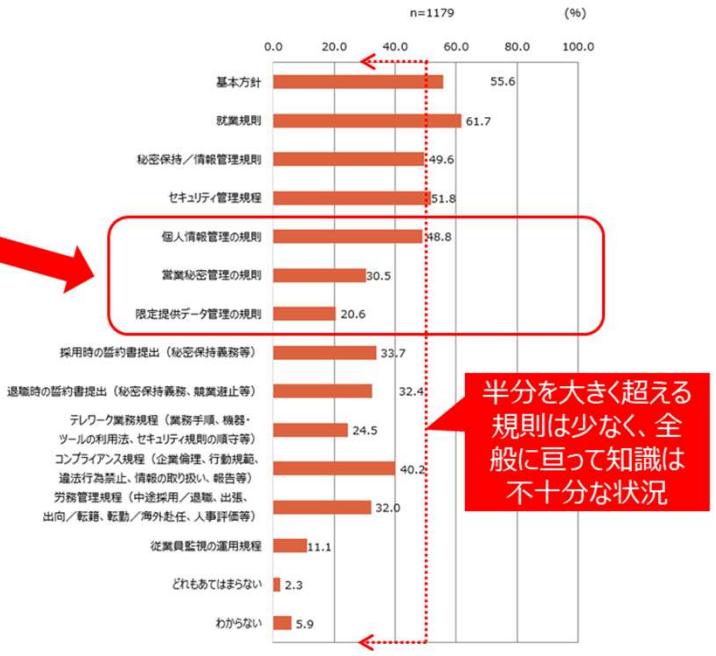
営業秘密／限定提供データの管理規則は、個人情報の管理規則ほど知られていない。この傾向は、法制度に関する知識のリテラシー教育の実態と一致しており、営業秘密／限定提供データについては教育も不十分である。

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

＜パネルモニターが所属する企業のみの集計＞

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

＜パネルモニターが所属する企業のみの集計＞



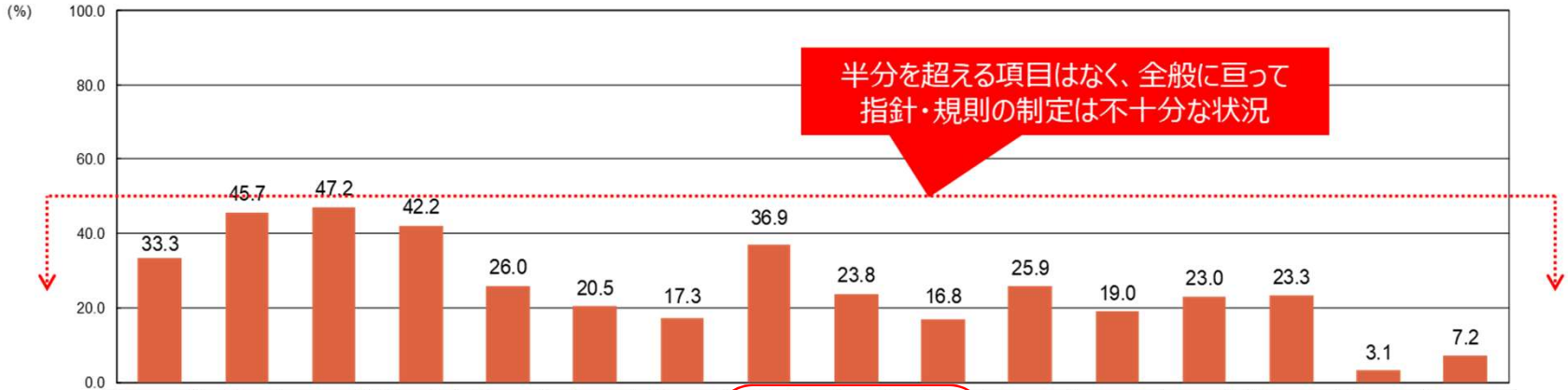
出典：企業における内部不正防止体制に関する実態調査概要説明資料

（参考）内部不正対策に取り組む規則の整備

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

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

＜パネルモニターが所属する企業のみの集計＞



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

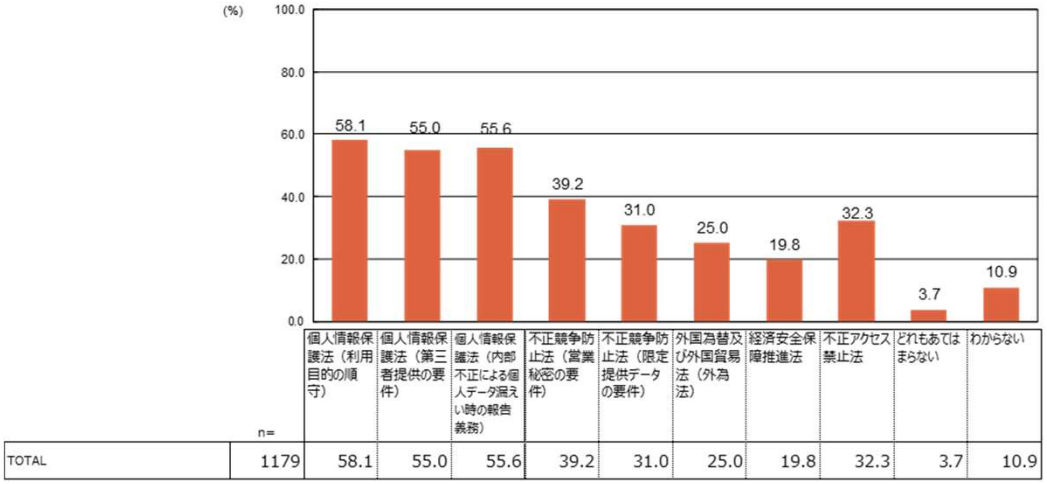
出典：企業における内部不正防止体制に関する実態調査概要説明資料

（参考）内部不正対策を所管する部署に蓄積されている知識

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

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

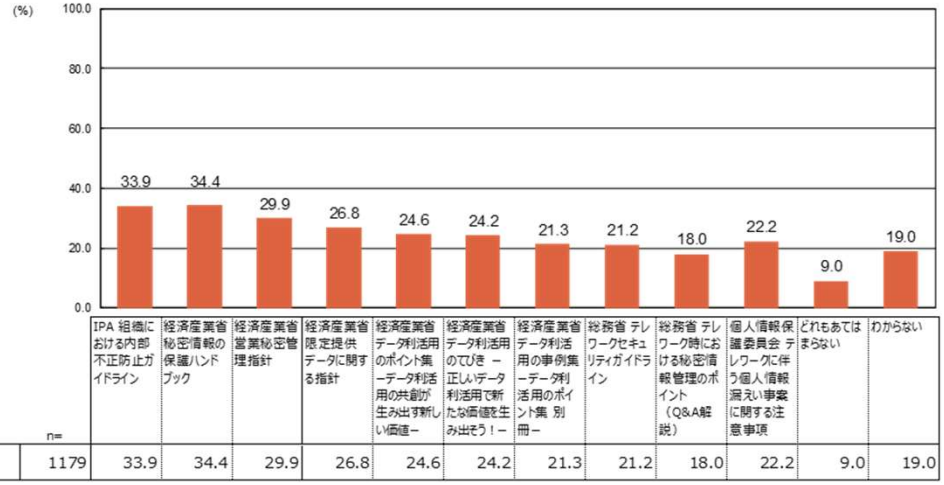
＜パネルモニターが所属する企業のみの集計＞



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

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

＜パネルモニターが所属する企業のみの集計＞



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

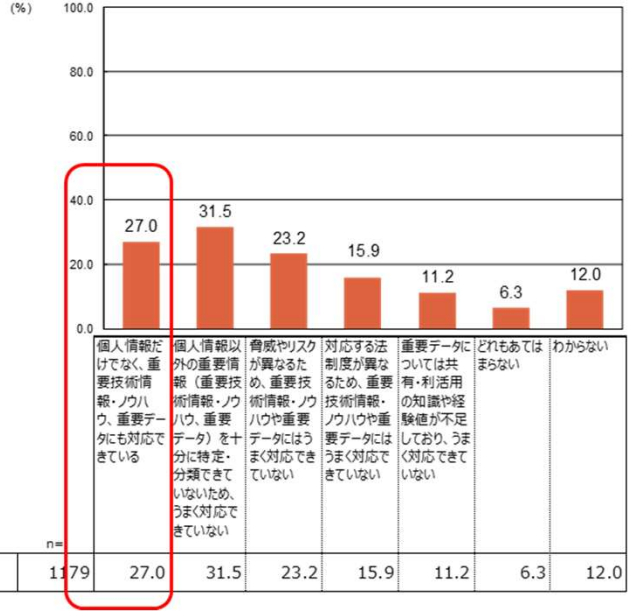
出典：企業における内部不正防止体制に関する実態調査概要説明資料

（参考）重要情報の特定と内部不正対策の現状

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

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

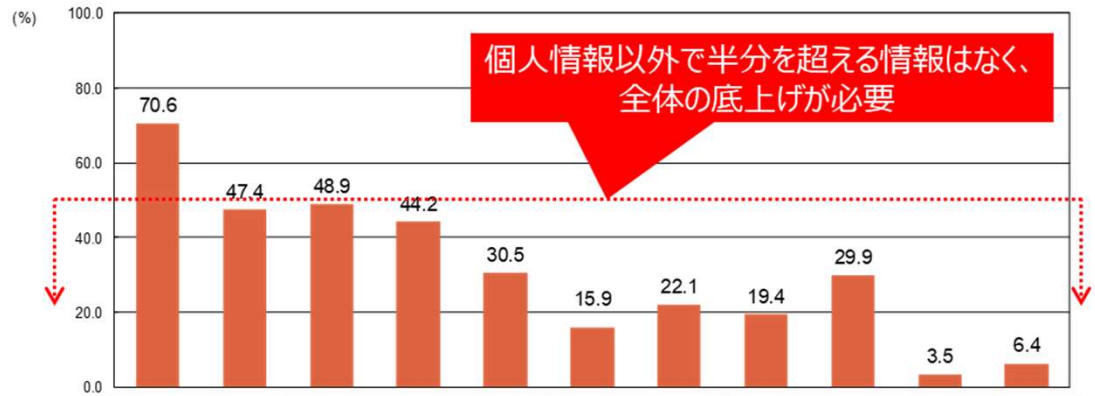
＜パネルモニターが所属する企業のみの集計＞



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

Q7. 貴社ではどのような種類の重要情報を特定する仕組みを作っていますか。

＜パネルモニターが所属する企業のみの集計＞



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

出典：企業における内部不正防止体制に関する実態調査概要説明資料

組織全体に対する内部不正防止の責任はどの組織が持っているか

内部不正防止を主管して組織全体に対する責任を負う部門は、「情報システム／セキュリティ管理部門」と「リスク管理／コンプライアンス部門」にほぼ二分されている。他方で、より一層ガバナンスを重視する日経平均銘柄企業では、「リスク管理／コンプライアンス部門」が責任を負うことが支配的である。（あるべき姿の論考については後述）

【内部不正防止対策を主管し、組織全体に対する責任を負っている部門】

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

（ご参考）日経平均銘柄企業25社の回答を集計

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

出典：企業における内部不正防止体制に関する実態調査概要説明資料

重要情報の漏えいに対し、組織的に対応できているか

内部不正が多い重要情報の漏えいに対し、責任部門が主導して全社的に対応できている企業・組織の割合は53%に過ぎない。当事者の現場組織が個別に対応している割合も1/4程度存在している。会計不正やハラスメントなどと比較すると、この現状はとても十分とは言えない。

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

出典：企業における内部不正防止体制に関する実態調査概要説明資料

内部不正による事業リスクは全社で認識されているか

内部不正による事業リスクは組織全体で認知されていることが望ましいが、ほとんどのリスクで「組織全体で知られている」という回答の割合が30%前後に留まっており、まだまだ十分とは言えない。内部不正対策は担当部署に任せておけば良いという訳にはいかない。

(%)

内部不正に関わるリスク	組織全体で知られている	対策の担当者が知っている	知られていない	分からない
サプライチェーンにおけるセキュリティ上の脆弱点の存在	28.9	42.4	16.3	12.4
サプライチェーンにおける不必要な重要情報の授受	27.7	41.8	17.2	13.3
クラウドセキュリティのあいまいな責任分担	25.9	41.8	17.9	14.4
テレワークの不十分なセキュリティガバナンス	32.1	37.7	16.6	13.6
退職者を通じた自社の重要情報の漏えい／中途採用者を通じた他社の重要情報の混入	32.8	36.6	16.2	14.4

出典：企業における内部不正防止体制に関する実態調査報告書

内部不正防止に関わる規則は組織全体で知られているか

営業秘密／重要データの取扱い、中途退職／中途採用、テレワーク等において、関係する内部不正防止規則が、組織全体で十分に浸透していない企業の割合が高い。

内部不正防止に関わる規則は組織全体で知られているか？

【50%程度またはそれ以上の企業で認知されている】

基本方針：	55.6%
就業規則：	61.7%
秘密保持／情報管理規則：	49.6%
セキュリティ管理規程：	51.8%
個人情報管理の規則：	48.8%

【認知されている企業の割合が低い】

営業秘密管理の規則：	30.5%
限定提供データ管理の規則：	20.6%
採用時の誓約書提出（秘密保持義務等）：	33.7%
退職時の誓約書提出（秘密保持義務、競業避止等）：	32.4%
テレワーク業務規程（業務手順、機器・ツールの利用法、セキュリティ規則の順守等）：	24.5%
コンプライアンス規程（企業倫理、行動規範、違法行為禁止、情報の取扱い、報告等）：	40.2%
労務管理規程（中途採用／退職、出張、出向／転籍、転勤／海外赴任、人事評価等）：	32.0%

出典：企業における内部不正防止体制に関する実態調査報告書

組織全体で重要情報を特定・識別できるリテラシーが構築されているか

重要なプロジェクトに関わるタイミングと重要プロジェクトから離れるタイミングで内部不正リスクが高まる。異動時や昇進時にも注意が必要である。これらの内部不正リスクが高まるタイミングで、関係者が重要情報取り扱いのリテラシーを学び直せば、リスク低減への効果を期待できるが、実際にはこれに取り組んでいる企業はまだ少ない。

重要情報の分類と表示に関する規則についてのリテラシー教育に取り組んでいると回答した企業は57.1%

■ 雇用開始時に教育	56.7%
■ 定期的な教育を実施（例：年１回等）	53.8%
■ 異動時・昇進時等にルールを教育し直す	28.1%
■ プロジェクトの開始・参加、終了時等にルールを教育し直す	23.7%

出典：企業における内部不正防止体制に関する実態調査報告書

（ご参考）重要情報の分類と表示に関する規則の組織全体への周知・教育

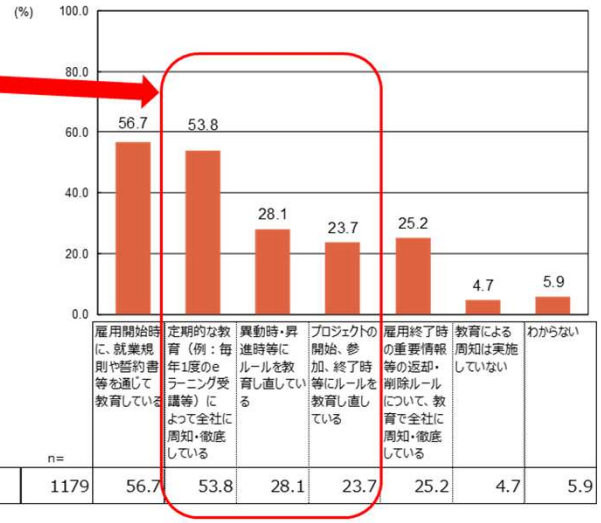
従業員に対して重要情報の分類と表示に関する規則の周知・教育を実施している企業は半数を超えていた。また、重要情報管理ルールを定期的に教育する企業も半数を超えた。これらはまずまずの状況ではあるものの、さらなる底上げが期待される。他方で、重要プロジェクトの開始／終了時のルールの教育し直し（より詳しい教育等）は十分ではなかった。

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

＜パネルモニターが所属する企業のみの集計＞

Q9. 貴社では重要情報の管理ルールを従業員に周知・徹底していますか。

＜パネルモニターが所属する企業のみの集計＞



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

出典：企業における内部不正防止体制に関する実態調査報告書

内部不正防止のための指針・規則の制定は十分か

アンケート調査の対象とした内部不正防止のための指針・規則は広範囲に亘っている。

基本方針等

- 内部不正防止だけで独立した基本方針
- 内部統制の基本方針（内部不正防止の基本方針を含む）
- セキュリティポリシー（内部不正防止の基本方針を含む）
- 就業規則に書かれた内部不正防止に関するルール

重要情報の特定・識別・取扱い等

- 組織全体に適用される重要情報の分類規則
- 秘密として管理する意思を明確に伝えるための、重要情報の表示規則
- 組織全体に適用される重要情報の分離保管規則

重要情報の種別に応じた管理規則

- 個人情報管理のための規則
- 営業秘密保護のための規則
- 限定提供データの管理のための規則

テレワーク関連の対策

- テレワーク時のセキュリティ管理規則
- テレワーク時のクラウドサービス利用規則

雇用流動化への対策

- 中途退職者の秘密漏えい、中途採用者による他社の秘密持ち込みを防止するための規則

等

出典：企業における内部不正防止体制に関する実態調査報告書

内部不正防止のための指針・規則の制定は十分か

50%を超える企業が定めている内部不正防止のための指針・規則はなく、全般に底上げが必要な状況と言える。

定めている企業の割合が比較的高い

基本方針等

- 内部不正防止だけで独立した基本方針：33.3%
- 内部統制の基本方針（内部不正防止の基本方針を含む）：45.7%
- セキュリティポリシー（内部不正防止の基本方針を含む）：47.2%
- 就業規則に書かれた内部不正防止に関するルール：42.2%

高い重要性が企業に認識されていない

重要情報の特定・識別・取扱い等

- 組織全体に適用される重要情報の分類規則：26.0%
- 秘密として管理する意思を明確に伝えるための、重要情報の表示規則：20.5%
- 組織全体に適用される重要情報の分離保管規則：17.3%

制定が個人情報管理に偏っている

重要情報の種別に応じた管理規則

- 個人情報管理のための規則：36.9%
- 営業秘密保護のための規則：23.8%
- 限定提供データの管理のための規則：16.8%

定めている企業の割合が3割にも満たない

テレワーク関連の対策

- テレワーク時のセキュリティ管理規則：25.9%
- テレワーク時のクラウドサービス利用規則：19.0%

定めている企業の割合が3割にも満たない

雇用流動化への対策

- 中途退職者の秘密漏えい、中途採用者による他社の秘密持ち込みを防止するための規則：23.0%

等

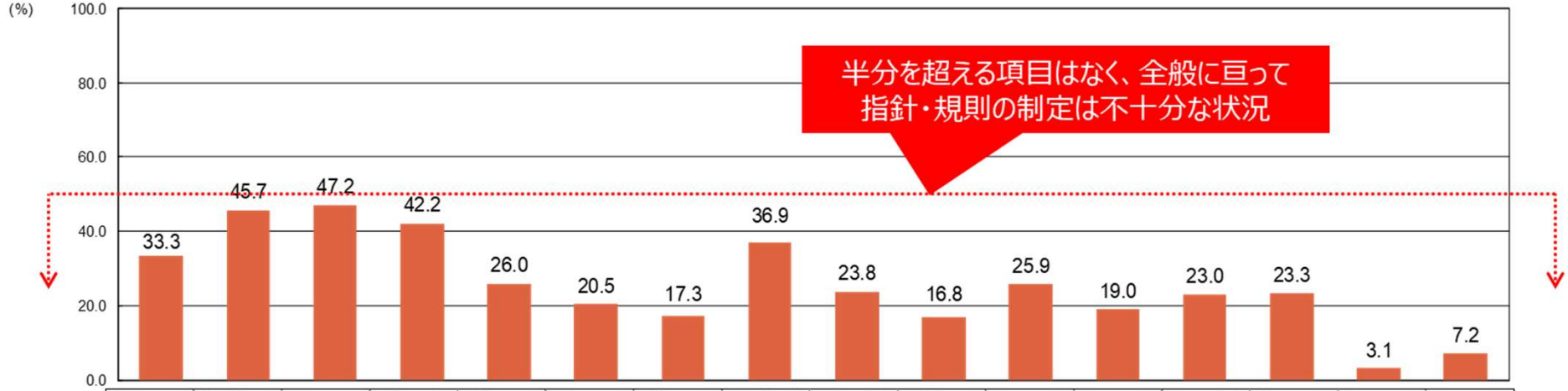
出典：企業における内部不正防止体制に関する実態調査報告書

（ご参考）内部不正防止のために定めている指針・規則

企業が内部不正防止のための指針・規則を定めている割合は、全般に亘って十分ではない。

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

＜パネルモニターが所属する企業のみの集計＞



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

出典：企業における内部不正防止体制に関する実態調査報告書

内部不正を防止するために実施している対策は十分か

アンケート調査の対象とした内部不正対策は**人の不正に対するもの**と**サイバーセキュリティと共通のもの**に分類できる。

【人の不正に対する主要な対策】

組織
- 内部不正に関し、組織全体における責任部門・責任者が明確に定められている

教育等
- 内部不正防止のリテラシー向上のため、定期的／事故発生時に組織全体で教育を実施
- テレワーク従事者に関連規程／法規の教育を実施

退職時の不正防止
- 採用時・退職時に加え、異動・昇格・新プロジェクトへの参加・離任時等に秘密保持義務契約を締結
- 営業／技術上の重要人物に対し、退職決定時以降、監視やログ確認を強化

職場環境の改善
- 不満が蓄積しないように、職場やテレワークにおける労務管理、人事管理、コミュニケーション確保等について、必要な対策を実施

再発防止等
- 組織内外で発生した内部不正事件について社内で周知することにより、内部不正を心理的に抑止

【それ以外のサイバーセキュリティと共通の主要な対策】

基本方針等
- 経営層が基本方針を定めて周知徹底
- 経営層が基本方針に基づき、必要なリソース確保の決定・指示を実施
- 経営層が重要情報と判断する範囲や条件を明確に定めて周知徹底

IT資産管理
- 退職後速やかに、退職者のIDやアクセス権限等を削除
- ID管理と本人確認（認証）を強化
- 重要情報にアクセスできる従業員の最少化
- 重要情報の定期的な棚卸し、不要情報の消去

物理的セキュリティ
- 入退室管理、PC・デバイスの社外持出管理の実施
- BYODの禁止

技術・運用管理
- 重要情報に対するアクセス監視／ログ記録等の実施と、社内全体への周知
- テレワーク端末のセキュリティ対策
- テレワークで扱える重要情報の範囲制限
- 利用できるクラウドサービスや、クラウドサービス上で扱える重要情報の範囲を制限
- サプライヤー等との重要情報の受渡しの厳格管理と暗号化
- サプライヤー等の重要情報漏えい対策を契約時／契約中に確認

事後対策・事業継続
- 事件／インシデント発覚後の事後対策や事業継続のマニュアル化

出典：企業における内部不正防止体制に関する実態調査報告書

内部不正を防止するために実施している対策は十分か

回答が半数を超える対策項目が１つもなく、総じて対策が進んでいない。社会全体の底上げが必要な現状と言える。

【人の不正に対する主要な対策】

組織

- **内部不正に関し、組織全体における責任部門・責任者が明確に定められている:42.1%**

教育等

- **内部不正防止のリテラシー向上のため、定期的／事故発生時に組織全体で教育を実施：41.8%**
- テレワーク従事者に関連規程／法規の教育を実施：21.3%

退職時の不正防止

- 採用時・退職時に加え、異動・昇格・新プロジェクトへの参加・離任時等に秘密保持義務契約を締結：28.4%
- 営業／技術上の重要人物に対し、退職決定時以降、監視やログ確認を強化：19.8%

職場環境の改善

- **不満が蓄積しないように、職場やテレワークにおける労務管理、人事管理、コミュニケーション確保等について、必要な対策を実施：32.5%**

再発防止等

- 組織内外で発生した内部不正事件について社内で周知することにより、内部不正を心理的に抑止：29.0%

【それ以外のサイバーセキュリティと共通の主要な対策】

基本方針等

- **経営層が基本方針を定めて周知徹底：49.0%**
- **経営層が基本方針に基づき、必要なリソース確保の決定・指示を実施：33.2%**
- 経営層が重要情報と判断する範囲や条件を明確に定めて周知徹底：29.7%

IT資産管理

- **退職後速やかに、退職者のIDやアクセス権限等を削除：32.7%**
- **ID管理と本人確認（認証）を強化：35.5%**
- **重要情報にアクセスできる従業員の最少化：30.4%**
- 重要情報の定期的な棚卸し、不要情報の消去：19.8%

物理的セキュリティ

- **入退室管理、PC・デバイスの社外持出管理の実施：35.0%**
- BYODの禁止：21.1%

技術・運用管理

- **重要情報に対するアクセス監視／ログ記録等の実施と、社内全体への周知：31.4%**
- テレワーク端末のセキュリティ対策：21.4%
- テレワークで扱える重要情報の範囲制限：19.7%
- 利用できるクラウドサービスや、クラウドサービス上で扱える重要情報の範囲を制限：22.9%
- サプライヤー等との重要情報の受渡しの厳格管理と暗号化：15.9%
- サプライヤー等の重要情報漏えい対策を契約時／契約中に確認：17.6%

事後対策・事業継続

- **事件／インシデント発覚後の事後対策や事業継続のマニュアル化：35.3%**

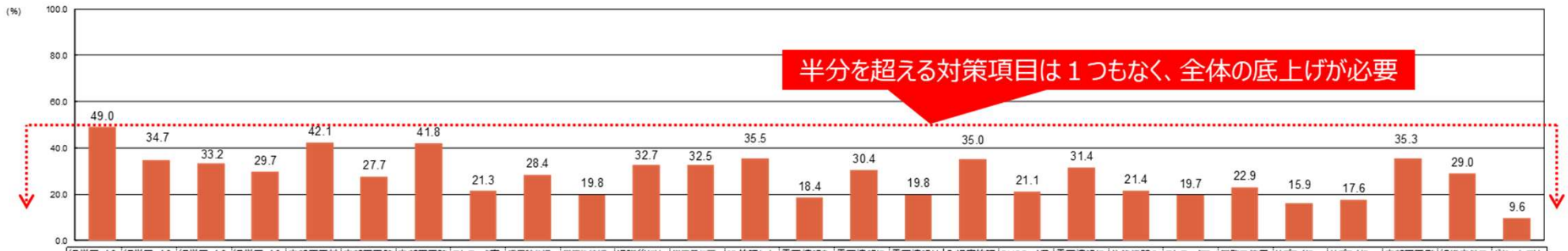
出典：企業における内部不正防止体制に関する実態調査報告書

（ご参考）重要情報の漏えいに関する内部不正を防止するために実施している対策

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

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

＜パネルモニターが所属する企業のみの集計＞



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

出典：企業における内部不正防止体制に関する実態調査報告書

テレワーク中の内部不正を防止する対策は十分か

テレワーク中の内部不正を防止するための**技術・運用面での対策の実施割合はいずれも30%台であり、まだ十分ではなかった。**一方、**人的管理面については**、各部門（現場）の裁量に委ねた自主的なコミュニケーション強化に最も重点が置かれており、この対策を実施している企業の割合は概ね半数に達している。しかし、**組織全体に適用されるトップダウンの対策（処遇、連絡窓口、出勤日、十分なコミュニケーション確保等）はまだ十分とは言えない。**

【テレワーク中の内部不正を防止する対策】

- （人的管理）テレワークを行う従業員に対し、関係する社内規則／法制度を教育・徹底：37.2%
- （技術・運用）情報漏えいに備えて、テレワークで取り扱うことができる重要情報を制限：37.7%
- （技術・運用）テレワーク用会社支給PC等の操作ログの取得・分析等で、内部不正の早期発見や事後対応の機能を強化している（EDRの導入等）：34.1%
- （技術・運用）テレワーク中のID管理、権限管理、当人認証等を強化：31.1%
- （人的管理）テレワーク勤務と社内勤務を公平に処遇している：23.6%
- **（人的管理）テレワーク中の従業員との十分なコミュニケーションを確保できる対策を講じている：17.4%**

現場任せが鮮明

【テレワーク中に内部不正を行う気にさせないための従業員支援（人的管理）】

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

出典：企業における内部不正防止体制に関する実態調査報告書

（ご参考）テレワーク中の内部不正防止のための組織的・人的対策

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

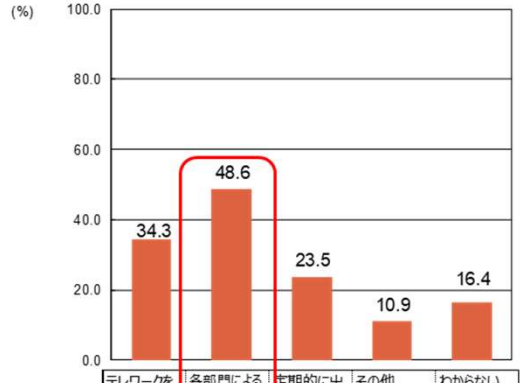
Q35. 貴社では、テレワークを行う従業員の内部不正防止対策を実施していますか。

＜パネルモニターが所属する企業のみの集計＞

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

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

＜パネルモニターが所属する企業のみの集計＞



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

出典：企業における内部不正防止体制に関する実態調査報告書

クラウドサービス利用中の内部不正を防止する対策は十分か

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

【技術・運用面での対策状況】

- 利用を許可するクラウドサービス以外の利用を禁止：42.0%
- クラウドサービス上で取り扱うことができる重要情報を制限：33.6%
- クラウドサービス上で取り扱う重要情報に対するアクセス権管理／データ管理および利用状況のモニタリング：25.5%

【外部サービスの契約・モニタリング面での対策状況】

- クラウドサービス利用に関する管理責任及びインシデント対応責任の分担を明確に定めている：16.0%

【人的管理面での対策状況】

- クラウドサービスの利用ルールに関する組織全体への周知・教育を実施：35.6%

出典：企業における内部不正防止体制に関する実態調査報告書

サプライヤーや委託先との間での、重要情報の管理策の合意は十分か

サプライヤーや委託先との間で重要情報の管理策について合意しているかについては、いずれの項目も回答者の割合が40%に届いておらず、十分な水準に達しているとは言えない。しかし、ここには「他社の営業秘密の混入防止」「法の順守」「事業継続の確保」などにおいて重要な対策が多く、取り組みの早期推進が急務と言える。

【重要情報の管理・取扱いに関する合意】

- 重要情報の管理水準、暗号化、ライフサイクル管理の方法等について契約で合意：39.3%
- 受渡しができる重要情報の範囲を明文化して合意：39.0%
- **受け渡した重要情報を、自社情報と他社情報に分けて管理することで合意：30.6%**

【改正個人保護法の報告義務への対応】

- 取扱いを委託した個人情報が漏えいした場合に、サプライヤーや委託先が、委託元が行う調査に協力することを契約で合意：31.5%

【事後対応、事業継続への対応】

- 重要情報漏えい時の事後対応や事業継続について、サプライヤーや委託先と協力できるように、連携体制について合意：23.7%

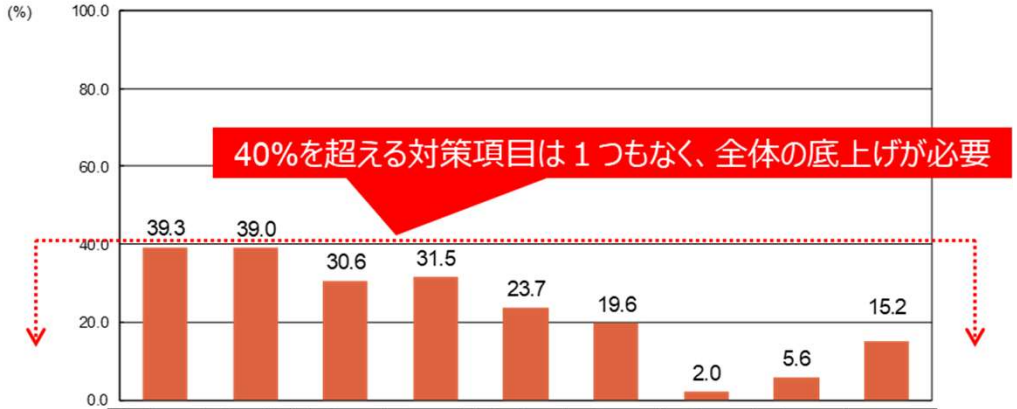
出典：企業における内部不正防止体制に関する実態調査報告書

（ご参考）サプライヤーや委託先との間での、重要情報の管理策の合意

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

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

<パネルモニターが所属する企業のみの集計>



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

出典：企業における内部不正防止体制に関する実態調査報告書

中途退職者に課す秘密保持義務の実効性を高める対策は十分か

中途退職者に課す秘密保持義務の実効性を高めるためには、**「基本となる対策」と「退職後も秘密保持義務の有効性が認められる可能性を高める対策」を組み合わせる**のが良い。「基本となる対策」で気になるのは、**秘密保持義務の対象となる重要情報の範囲・内容を明確に定めている企業の割合が少ない**ことである。他方で、「退職後も秘密保持義務の有効性が認められる可能性を高める対策」については、**社会全体での認知度を高めて底上げしていくことが必要**であると考えられる。

取るべき戦略とアンケート調査結果

49.6%

【基本】
（秘密保持義務契約）
1. 秘密保持義務契約の締結についての内部規則を定め、就業規則でその順守を要求
2. 就職時と退職時に秘密保持義務契約を締結

（言い逃れの防止）
3. 秘密保持義務の対象となる重要情報の範囲・内容を明確に定める

23.9%

＋

39.6%

【退職後も秘密保持義務の有効性が認められる可能性を高める対策】

1. 異動、昇格、新プロジェクトへの配属／離任時等、秘密保持義務契約を結ぶ機会を増やすことで、いつ中途退職しても契約期間が残る可能性を高める。
2. 就業規則に退職後の定めを規定しておく　40.1%
3. 秘密保持義務の有効期間を十分に長く設定しておく　25.9%

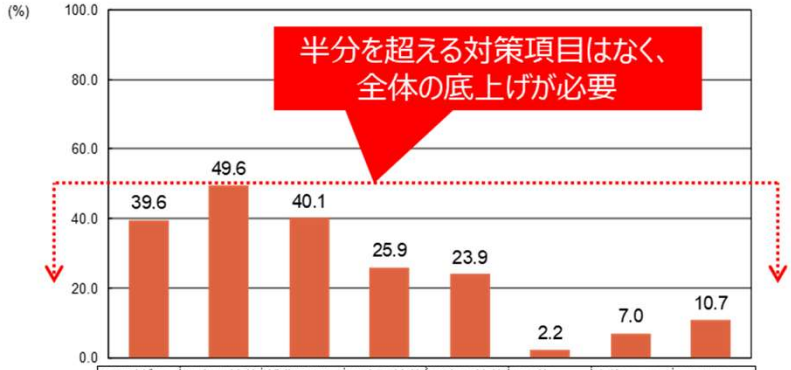
出典：企業における内部不正防止体制に関する実態調査報告書

（ご参考）中途退職者に課す秘密保持義務の実効性を高める対策

中途退職者に課す秘密保持義務の実効性を高めるための対策としては、秘密保持義務契約の締結についての内部規則を定めて就業規則でその遵守を求めること、この規則に従って契約締結／誓約書提出を行うこと、就業規則に退職後の定めを規定すること等が中心となっている。しかし、中心となる対策でさえ回答は半数に達しておらず、十分な水準であるとは言えない。

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

＜パネルモニターが所属する企業のみの集計＞



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

出典：企業における内部不正防止体制に関する実態調査報告書

３．アンケート調査結果の分析から得られた示唆

調査結果の注目点（再掲）

調査結果を読み解く上で最も重要な注目点は、「企業が内部不正リスクを重要な経営課題として捉えているか」どうかである。**経営層や内部不正防止に関する全社責任者が事業リスクを十分に認識し、優先度の高い経営課題として捉えることこそが、まず目指すべき姿**である。

内部不正リスクを重要な経営課題として捉えている企業では、そうではない企業と比較して：

1. 経営層が日常的に内部不正防止の取組等を全従業員に周知、指示している
2. 情報漏えいリスク／セキュリティリスクの知識が、組織全体に、より一層浸透している
3. 内部不正防止のためのリテラシー教育の提供が、より一層進展している
4. 内部不正防止のための指針や規定を定めている割合が、より一層高い
5. 内部不正対策が全般に亘って、より進展している

などの特徴がはっきりと結果に表れている。
従って、「内部不正リスクを重要な経営課題として捉える」ことが、内部不正防止に関する取組を幅広く進める上での「起爆剤」になると考えてよい。

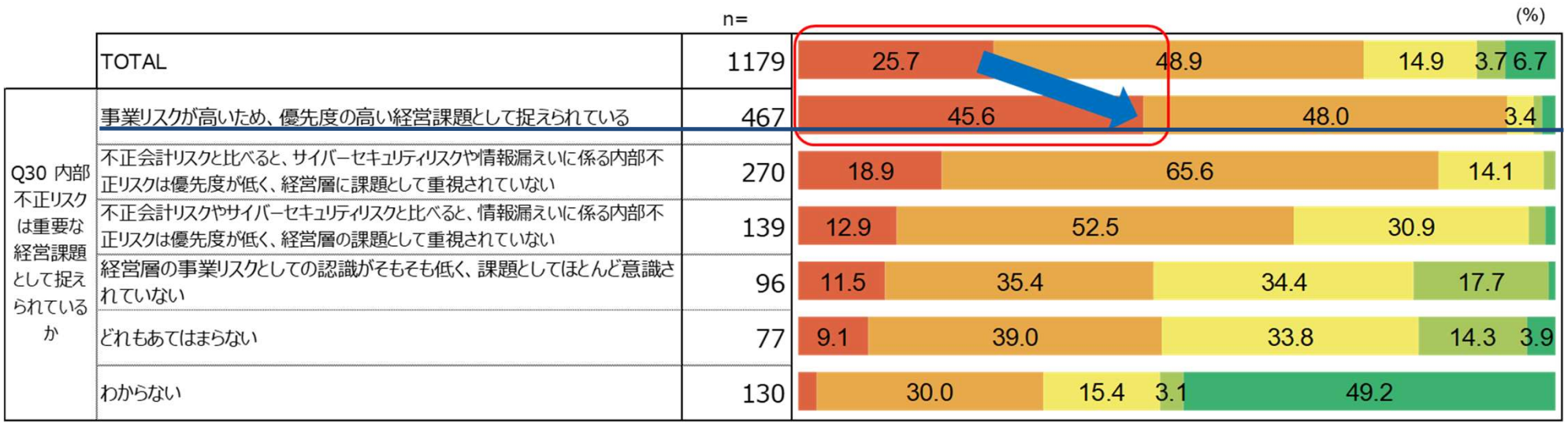
※詳細は「３．アンケート調査結果の分析から得られた示唆」で解説。

出典：企業における内部不正防止体制に関する実態調査概要説明資料

内部不正リスクを重要な経営課題として捉えている企業
～経営層による、内部不正防止の取組等の、全従業員への周知、指示

経営層が全従業員への周知、指示を行っていると回答した企業の割合は、**単純集計では25.7%に過ぎないが、内部不正リスクを重要な経営課題として捉えている企業では45.6%に達しており、約20%増えている。**
⇒**内部不正リスクを重要な経営課題として捉えている企業では**、そうではない企業と比較して、**経営層が日常的に内部不正防止の取組等を全従業員に周知、指示している**と言える。

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



出典：企業における内部不正防止体制に関する実態調査概要説明資料

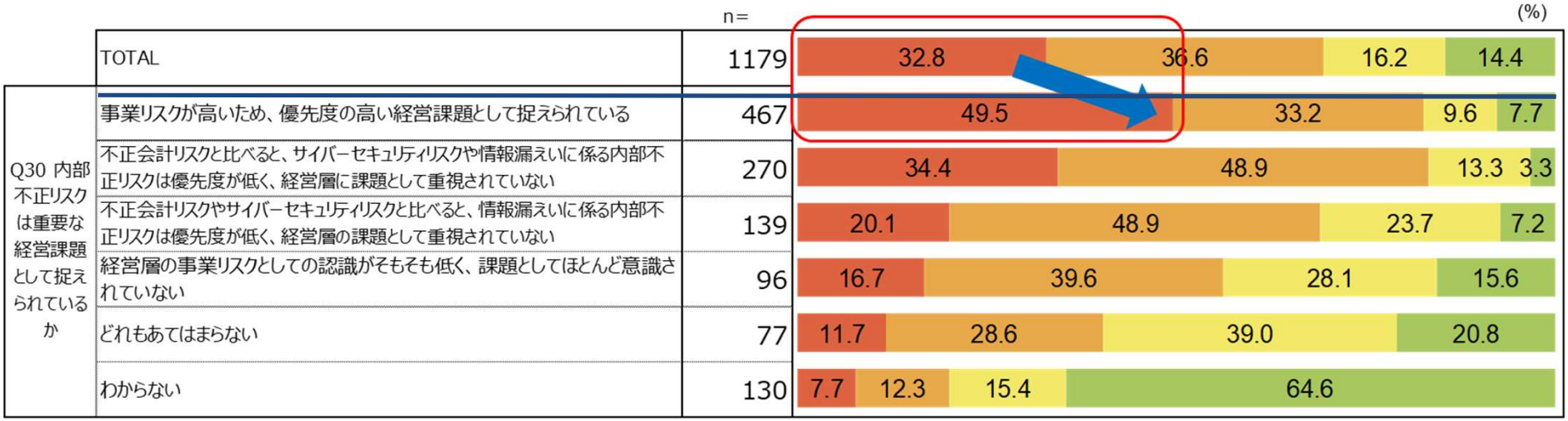
内部不正リスクを重要な経営課題として捉えている企業
～組織全体への「情報漏えいリスク／セキュリティリスクの知識」の浸透度（1/2）

退職者を通じた重要情報漏えい／中途採用者を通じた他社の重要情報の混入リスクが組織全体で知られていると回答した企業の割合が、**単純集計では32.8%に過ぎないが、内部不正リスクを重要な経営課題として捉えている企業では49.5%に達しており、約17%増えている。** ⇒退職者を通じた重要情報漏えい／中途採用者を通じた他社の重要情報の混入リスクの知識が、**組織全体に、より一層浸透していると言える。**

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

（例）

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



出典：企業における内部不正防止体制に関する実態調査概要説明資料

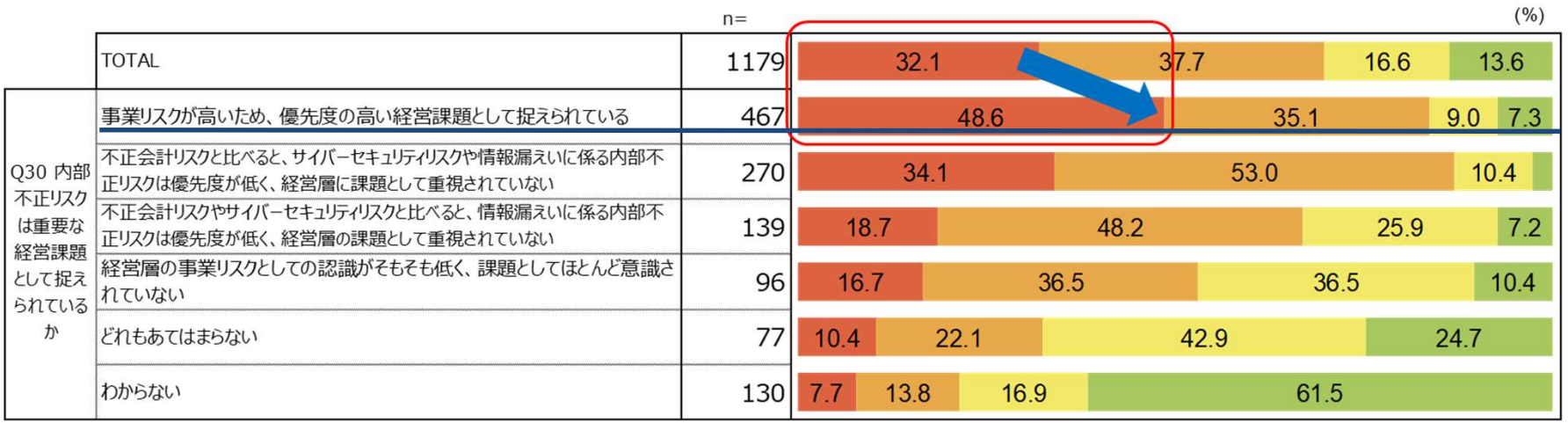
内部不正リスクを重要な経営課題として捉えている企業
～組織全体への「情報漏えいリスク／セキュリティリスクの知識」の浸透度（2/2）

テレワーク中のセキュリティ対策が徹底されないことで生じるリスクが組織全体で知られていると回答した企業の割合が、**単純集計では32.1%に過ぎないが、内部不正リスクを重要な経営課題として捉えている企業では48.6%に達しており、16.5%増えている。**
⇒テレワーク中のセキュリティ対策が徹底されないことで生じるリスクの知識が、**組織全体に、より一層浸透していると言える。**

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

（例）

<テレワークの不十分なセキュリティガバナンス>

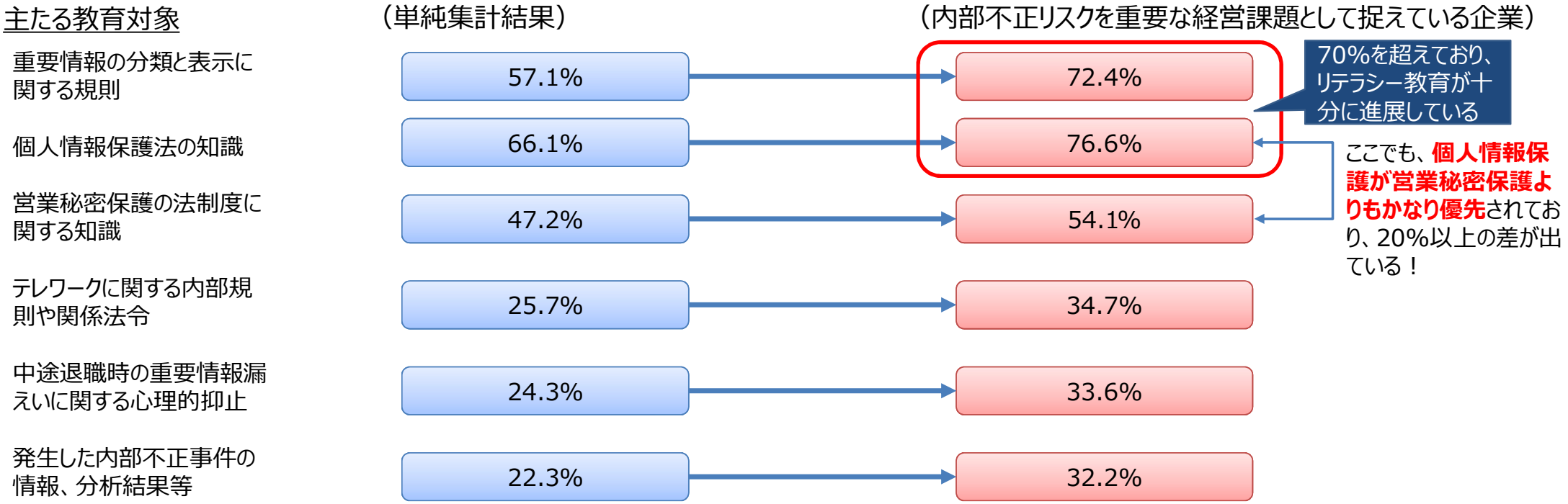


出典：企業における内部不正防止体制に関する実態調査概要説明資料

内部不正リスクを重要な経営課題として捉えている企業
～リテラシー教育の幅広い提供

「重要情報の分類と表示に関する規則」「個人情報保護法の知識」「営業秘密保護の法制度に関する知識」「テレワークに関する内部規則や関係法令」「中途退職時の重要情報漏えいに関する心理的抑止」「発生した内部不正事件の情報、分析結果等」の全てにおいて、内部不正リスクを重要な経営課題として捉えている企業の方が、リテラシー教育を提供している割合がかなり高くなっている。

【リテラシー教育の提供状況の比較】



出典：企業における内部不正防止体制に関する実態調査概要説明資料

（ご参考）リテラシー教育の提供状況の比較

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

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

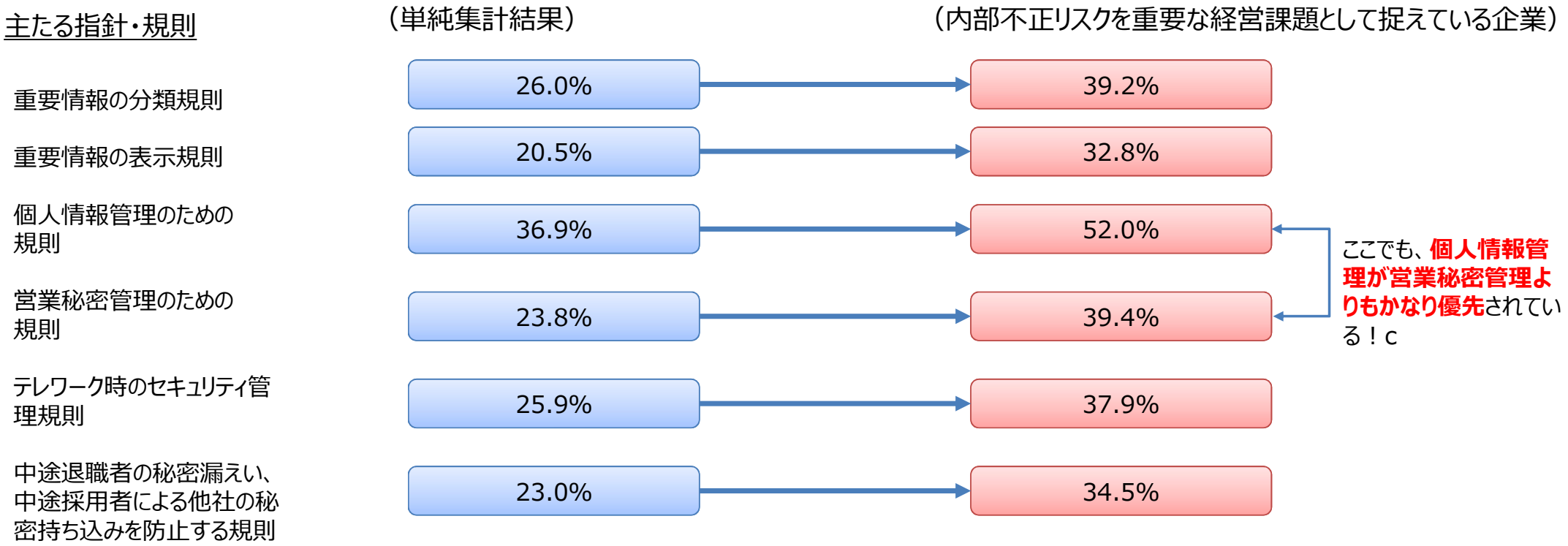
		n=	重要情報の分類と表示に関する規則	個人情報保護の法制度に関する知識	営業秘密保護の法制度に関する知識	限定提供データ保護の法制度に関する知識	機微技術情報の管理に関する外為法についての知識	クラウド利用許可に関する規則	BYOD（個人所有PC／デバイスの業務利用）の使用規則	テレワークに関する内部規則や関連法令	モニタリングやログ記録・分析等によって、組織が善良な従業員を守るという経営方針	中途退職時の重要情報漏えいに対する抑止的な周知・教育	中途採用者が他社の重要情報を持ち込めないようにするための確認ルール	外国政府が関与する重要技術情報に対する産業スパイの典型的手口の知識	発生した内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

出典：企業における内部不正防止体制に関する実態調査報告書

内部不正リスクを重要な経営課題として捉えている企業
～指針や規定の制定の進展

「重要情報の分類規則」「重要情報の表示規則」「個人情報管理のための規則」「営業秘密管理のための規則」「テレワーク時のセキュリティ管理規則」「中途退職者の秘密漏えい、中途採用者による他社の秘密持ち込みを防止する規則」の全てにおいて、内部不正リスクを重要な経営課題として捉えている企業の方が、指針・規程を制定している割合がかなり高くなっている。

【指針・規則の制定状況の比較】



出典：企業における内部不正防止体制に関する実態調査概要説明資料

（ご参考）指針や規定を定めている割合の比較

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

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

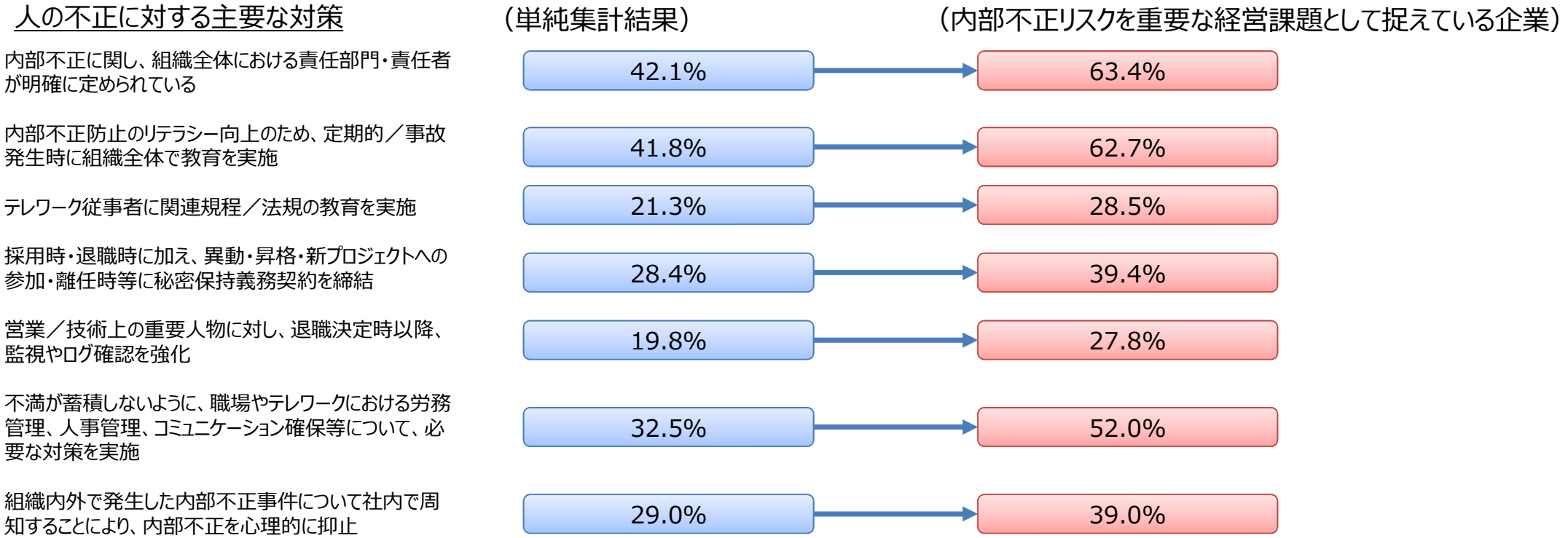
		n=	内部不正防止だけで独立した基本方針（内部統制の基本方針やセキュリティポリシーには含まれていない）	内部統制の基本方針（内部不正防止の基本方針を含む）	セキュリティポリシー（内部不正防止の基本方針を含む）	就業規則に書かれた内部不正防止に関するルール	組織全体に適用される重要情報の分類規則	秘密として管理する意思を明確に伝えるための、重要情報の表示規則	組織全体に適用される重要情報の分離保管規則	個人情報管理のための規則	営業秘密管理のための規則	限定提供データの管理のための規則	テレワーク時のセキュリティ管理規則（端末／ネットワーク利用、リモートアクセス等）	テレワーク時のクラウドサービ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

出典：企業における内部不正防止体制に関する実態調査報告書

内部不正リスクを重要な経営課題として捉えている企業 ～内部不正対策の実施の拡大（1/2）

人の不正に対する主要な対策の全てにおいて、内部不正リスクを重要な経営課題として捉えている企業の方が、対策を実施している割合がかなり高くなっている。

【内部不正対策の実施状況の比較】

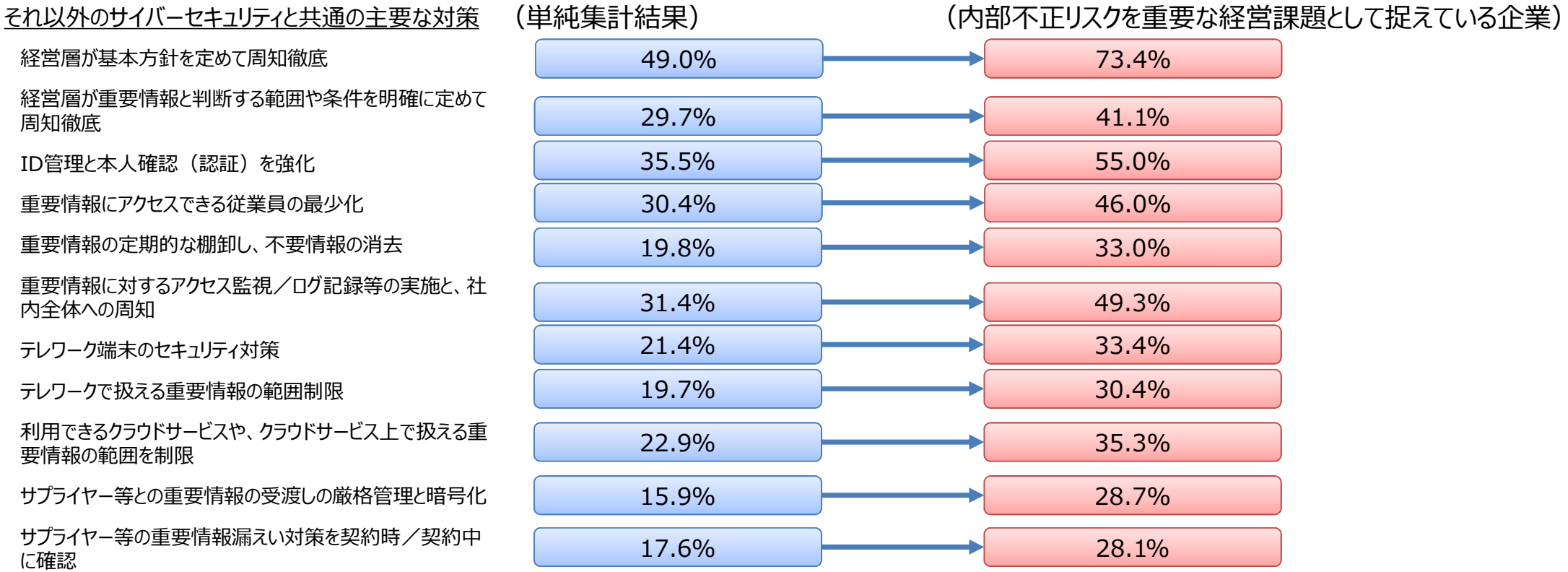


出典：企業における内部不正防止体制に関する実態調査概要説明資料

内部不正リスクを重要な経営課題として捉えている企業 ～内部不正対策の実施の拡大（2/2）

以下で示したサイバーセキュリティと共通の主要な対策の全てにおいて、内部不正リスクを重要な経営課題として捉えている企業の方が、対策を実施している割合がかなり高くなっている。

【内部不正対策の実施状況の比較】



出典：企業における内部不正防止体制に関する実態調査概要説明資料

（ご参考）内部不正対策を実施している割合の比較

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

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

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

出典：企業における内部不正防止体制に関する実態調査報告書

どうすれば、内部不正リスクを重要な経営課題として捉えることができるのか

ここまでのアンケート調査結果の分析に基づくと、**企業（経営層、全社の責任者等）が内部不正リスクを重要な経営課題として捉えることで**、リスクの理解や必要知識の全社への浸透、全社リテラシー教育、規則・指針の制定、内部不正対策の進展の**全てを期待できる。**
次に考えるべきことは、**それではどうすれば、企業に内部不正リスクを重要な経営課題として捉えてもらえるのか**ということである。

重要なキーワードは：

内部不正事件／インシデントの経験 × **腹落ち**

しかしそれぞれに問題点が・・・

中小企業は経験がかなり足りない！

次ページへ

常用雇用者数	個人情報の漏えい事件のインシデント発生（未遂を含む）	営業秘密の漏えい事件のインシデント発生（未遂を含む）	内部不正リスクを重要な経営課題として捉えている割合
300人以下	26.2%	30.0%	29.8%
301人以上	**45.1%**	39.5%	48.0%

10,001人以上だと50%を超える　　1,001人以上だと50%を超える

出典：企業における内部不正防止体制に関する実態調査概要説明資料

どうすれば、内部不正リスクを重要な経営課題として捉えることができるのか

企業（経営層、全社の責任者等）が**内部不正リスクを重要な経営課題として捉えるためには、重要情報の漏えい事件・インシデント（未遂を含む）を経験することが効果的**である。**特に、個人情報の漏えい事件・インシデント**を経験することで、この捉え方が目立って進展している。
他方で、実際の経験には足りないとしても、経営層／全社責任者が他社事例から学ぶことには一定の効果があるものと推定する。但し、学んだことについて腹落ちし、自分の考えにしっかりと取り込むことが必要と思われる。

事件等の種別	内部不正リスクを重要な経営課題として捉えている企業の割合
個人情報の漏えい事件・インシデント（未遂を含む）を経験した企業	56.6%
営業秘密の漏えい事件・インシデント（未遂を含む）を経験した企業	41.7%
事業・技術等の中核人材の国内競合企業への転職を経験した企業	42.0%
事業・技術等の中核人材の海外競合企業への転職を経験した企業	41.5%

**この差はなぜ生まれるのか？
「腹落ち」と関係！
インタビュー結果に基づく分析により後述**

**個人情報漏えいに限って言えば経験することが一番！経験することですぐに腹落ちできるため。
営業秘密漏えいはそう単純ではない。**

出典：企業における内部不正防止体制に関する実態調査概要説明資料

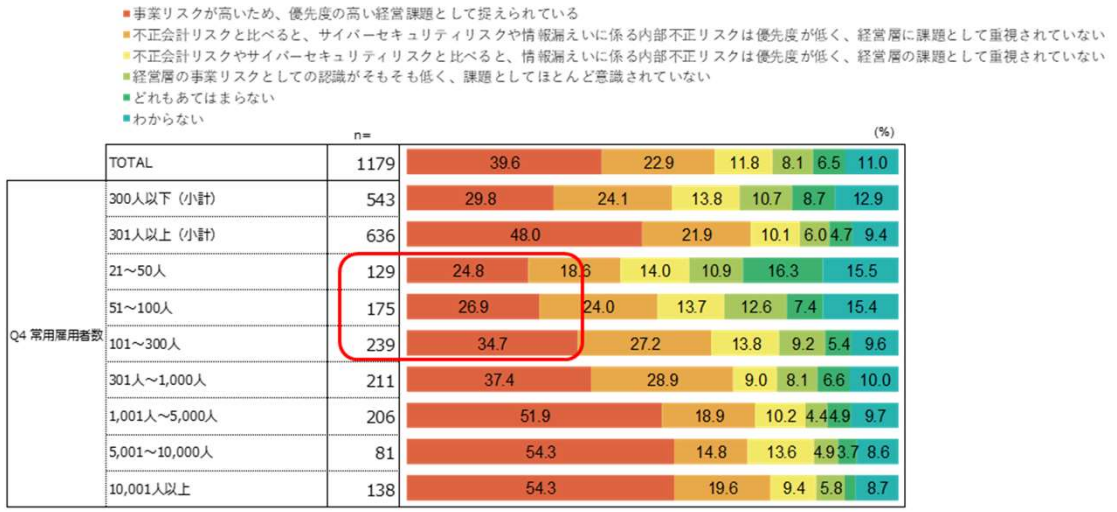
（ご参考）内部不正リスクを重要な経営リスクとして捉えられているか

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

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

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

Q30 貴社では、内部不正リスクは重要な経営課題として捉えられていますか。

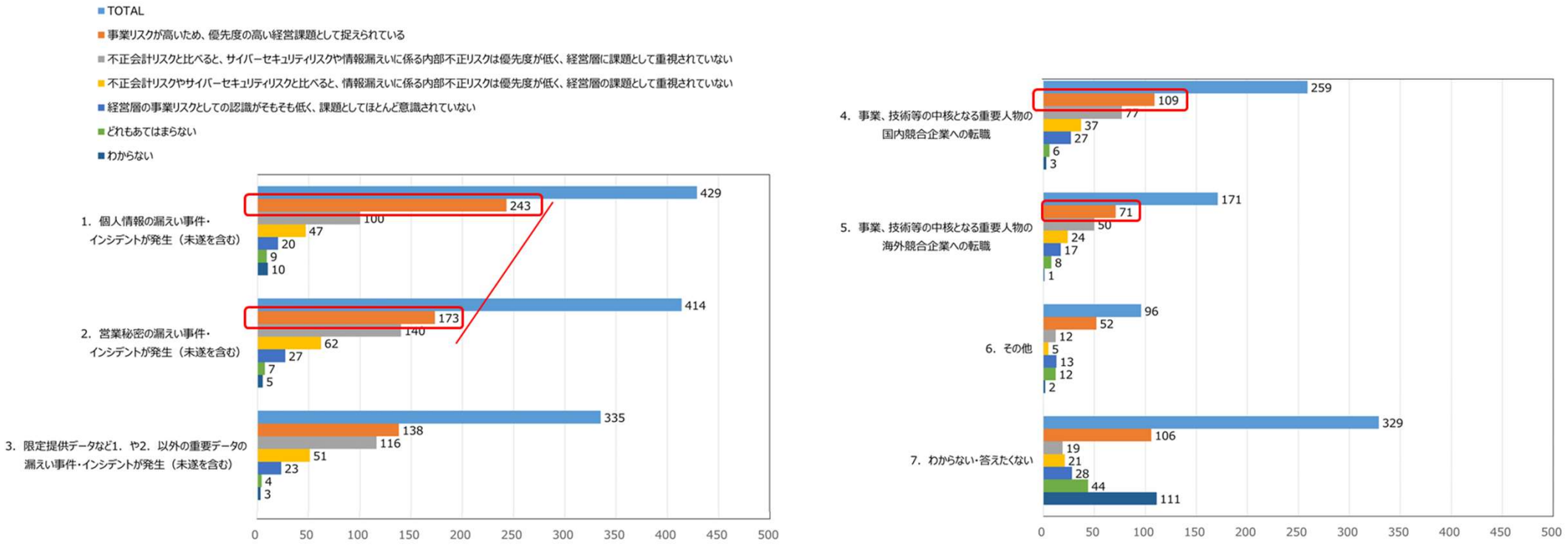


出典：企業における内部不正防止体制に関する実態調査報告書

（ご参考）内部不正リスクを重要な経営課題として捉えるきっかけ

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

Q30 貴社では、内部不正リスクは重要な経営課題として捉えられていますか。



出典：企業における内部不正防止体制に関する実態調査報告書

中小企業には問題が山積み

アンケート調査結果の分析から、中小企業では、「個人情報以外の重要情報への対応力」「内部不正対策の拡大」「雇用流動化対策の実施」において課題が見られた。今後、中小企業がキャッチアップできるような支援策や環境整備が必要になるものと考えられる。

1. 個人情報だけでなく**重要技術情報・ノウハウ、重要データの保護にも対応**できていると回答した常時雇用者数300人以下の企業は18.4%に過ぎず、301人以上の企業の34.3%と比較する**とかなり遅れている**状況が見られる。

2. 常時雇用者数300人以下の企業は、**「人の不正に対する主要な対策」と「それ以外のサイバーセキュリティと共通の主要な対策」の全てにおいて**、301人以上の企業よりも**取り組みが遅れている。**特に、「内部不正対策の基本方針策定」「内部不正対策に関する組織全体の責任部門／責任者の選定」「ID管理と本人確認（認証）の強化」「入退室管理やPC・デバイスの社外持出し管理の実施」「重要情報に対するアクセス監視、ログ記録等の実施と組織全体への周知」「内部不正発覚後の事後対応や事業継続のマニュアル化」については回答の割合に15%以上の差がある。一部、中小企業の特性上やむを得ないものもあるが、その他については差を埋めていくことが必要と考えられる。

3. **秘密保持義務契約の締結に関しては**、常用雇用者数が1,000人を超える企業で取り組みが進んでおり、40%を超える企業が対策を実施していると回答している。他方で、**常時雇用者数が300人以下の企業では割合が30%弱に留まっており、さらなる啓発が必要**と考えられる。

出典：企業における内部不正防止体制に関する実態調査概要説明資料

（ご参考）中小企業における個人情報以外の重要情報への対応力

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

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

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

出典：企業における内部不正防止体制に関する実態調査報告書

（ご参考）中小企業における内部不正対策の実施状況

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

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

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

出典：企業における内部不正防止体制に関する実態調査報告書

（ご参考）中小企業における雇用の流動化への対策状況

常用雇用者数が1,000人を超える企業では、秘密保持義務契約の締結に関する対策が50%を超えており、対策実施が進んでいる 。他方で、中小企業による対策への取り組みは遅れており、さらなる啓発が必要である。離職が決定した後離職するまでの間重要情報へのアクセス監視等を強化するルールを定めている企業の割合は、常用雇用者数が5,000人を超える企業から増加しており、10,000人を超える企業では40%を超えているが、中小企業による取り組みは遅れている。

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

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

出典：企業における内部不正防止体制に関する実態調査報告書

４．企業／有識者の実感とあるべき姿への示唆

経営層に対する有識者からのメッセージ（一部、講演者の考えを付記）

APPTraS 営業秘密保護推進研究会

- 経営層は内部不正に対する認識を高めるべき。
  そうすることで、経営リスクや事業リスクとしての内部不正リスクの優先度を上げられるはず。

- 経営層は率先して、**重大な事業リスクと重要情報の紐づけの強化**を全社に指示すべき。

- 役職の高い人物を特別扱いしない対策に基づくマネジメントシステムを構築すべき。
  経営層に対する対策の適用には透明性が必要。また、**経営層の不正に対しても、内部不正対策のマネジメントシステムが実効的に機能**することが必要。

- 経営層は率先して、**社内で発生したインシデント情報**（原因、重要情報奪取の方法等）**を包み隠さず社員に開示する風土**を構築すべき。

- サプライチェーン対策については、サイバーセキュリティ経営ガイドライン第3版でも強調されているとおり、経営層のリーダーシップが重要。経営層が率先して、**サプライチェーンまで含めて企業の内部と捉え直した上でリスク管理対策を進める**ことで、サプライチェーン全体の内部不正対策を強化できるはず。

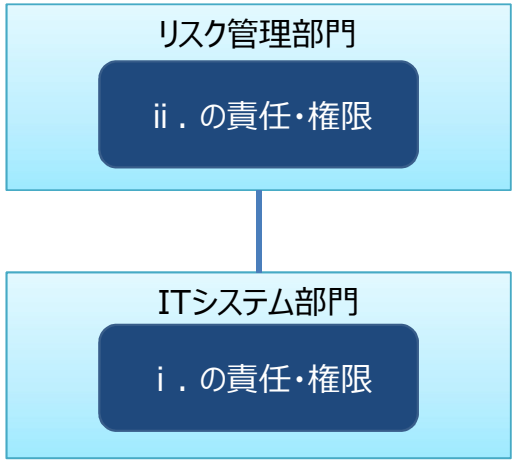
出典：企業における内部不正防止体制に関する実態調査概要説明資料

内部不正防止のための組織体制のあり方

内部不正防止に対する責任・権限の**典型的なモデルは、重要情報にアクセスできるITシステム部門が技術・運用等を担当し、リスク管理部門がこれを監督して責任部門となる形態**。こうすることで、ITシステム部門の不正にも対応できる。
他方で、**ITシステム部門が責任部門となっている企業**も多いが、この場合は、**法務・知財担当者を通じて、情報システム担当者に法制度等に関わる必要な知識を浸透させる**ことが有効。

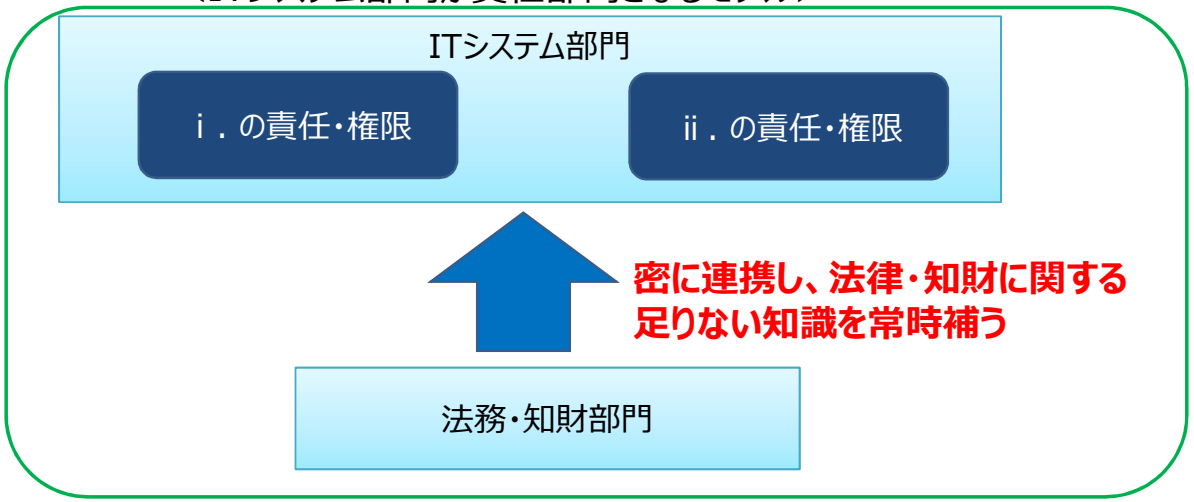
次の２つの責任・権限が実効的に確保され、全社的に対応できることが必要：
i. 内部不正対策を具体的に計画し、実施する責任・権限
ii. 経営層が定める基本方針に基づき、組織全体の立場から内部不正対策の計画を承認し、実施を統制する責任・権限

＜リスク管理部門が責任部門となるモデル＞



※内部不正防止のガバナンスが全社で行き届く形態
※ガバナンス要求が強い金融機関等ではこちらのモデルが支配的

＜ITシステム部門が責任部門となるモデル＞



※責任部門と関連部門の連携・協働によって、全社ガバナンスを形成する形態
※社内委員会をうまく活用することも有効と思量される

出典：企業における内部不正防止体制に関する実態調査概要説明資料

重要技術情報・ノウハウ（営業秘密）や重要データの保護を個人情報保護並みに高めていくための望ましい方策とは（1/2）

重要技術情報・ノウハウ（営業秘密）や重要データの保護を個人情報保護並みに高めていくためには：
1. リテラシー教育のグッドプラクティスの考え方を適用して、営業秘密や重要データの保護に関する**リテラシーを強化**
2. 営業秘密や重要データの保護に特化した対策を実施
という手順で取り組むことが効果的である。

【リテラシー教育のグッドプラクティスの考え方】

- 内部不正対策においては、**リテラシー教育にまず重点を置き、これでカバーできないところに、順次技術的対策を適用**していくのが効率的・効果的。従って、まずリテラシー教育から始めるべき。

- 重要情報漏えい／内部不正リスクの知識を組織全体に浸透させるためには、他社の事例を自社に当てはめてみる等によって**事例から学び、漏えい等の背景・理由をしっかりと認識し、腹落ちすることが重要**。腹落ちすればきっと実践に繋がる。例えば：
  - ✓ 誤った行動（してはいけないこと）や、ミスをするとどうなるのかを簡潔に解説
  - ✓ 背景にある対策が有効な理由の理解を深める
  - ✓ e-Learningだけに頼らず、グループディスカッション、再発防止教育用のコンテンツ（動画等）の制作＆閲覧（視聴）、定期的なルール順守のセルフチェックなどの手段も積極的に取り入れるべき

出典：企業における内部不正防止体制に関する実態調査概要説明資料

重要技術情報・ノウハウ（営業秘密）や重要データの保護を個人情報保護並みに高めていくための望ましい方策とは（2/2）

従業員による営業秘密／限定提供データ保護の理解を個人情報保護並みに進展させるためには、法制度を教育しようとはせず、**事例に基づいた動画解説、グループディスカッション、定期的なセルフチェック等によって、何をしてはいけないのかを腹落ちさせることに焦点を当てる**べき。

リテラシー教育の量において、「個人情報保護 ＞ 営業秘密保護」は必ずしも当てはまらない。それにも関わらず、営業秘密保護の知識や取組みの方が明らかに遅れている。その理由は何か？？

⇒**個人情報保護は法律の解説によっても理解しやすい！他方で、営業秘密や限定提供データは、同じだけ法律を解説しても、結局腹落ちしない人が多い・・・**

- 従業員一般への教育は、**何をしてはいけないのかを、事例に基づいて分かりやすく伝える**べき。特に、入社、**人事異動**、退職等の重要なタイミングで、**具体的に重要情報を示して教育**することが重要。
  （代替案として、「会社で扱う自社情報は全て重要」として周知徹底するプラクティスも存在）
- グループディスカッション、再発防止教育用のコンテンツ（動画等）の制作＆閲覧（視聴）、定期的なルール順守のセルフチェックなどの手段も積極的に取り入れるべき（前ページの再掲）
- なお、限定提供データの保護は、営業秘密の保護とあまり区別せず、同時に教えるのが良い。

出典：企業における内部不正防止体制に関する実態調査概要説明資料

中途退職者／中途採用者の内部不正対策の推進方法

急増する中途退職者／中途採用者の内部不正に対する対策を強化するためには、この問題に対する経営層の感度を高めるとともに、経営層に対しても従業員と同様の対策を適用すること、退職者については半年から１年前まで遡って情報システムへのアクセスログを確認すること、重要性の高い秘密に触れている人には通常より詳細化した誓約書の文面を用いること等が有効である。

（経営層）

中途退職者／中途採用者の
内部不正対策の重要性に対する
経営層の感度を高めるべき

＋

（有識者が推奨する対策）

1. **経営層に対しても従業員と同じように対策**し、例外は認めない。
2. 退職者については、**辞意を表明してから実際に退職するまでの間だけでなく、半年から1年前まで遡って情報システムへのアクセスログを確認**する。
3. 転入した従業員が他社の重要情報を社内でばらまかないように、必要な対策を行う。
4. 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る。
5. **重要性の高い秘密に触れている人については**、テンプレートどおりの誓約書をそのまま用いず、**誓約書を詳細化**する。

出典：企業における内部不正防止体制に関する実態調査概要説明資料

5．総括

主要な仮説の検証結果

IPA調査事業における主要な仮説については、結果として正しいと検証されたものが多く、重要情報漏えいに関わる内部不正体制の実態はまだ不十分な状況であることが浮き彫りになった。

分類軸	仮説	検証結果
企業・組織全体として知っておくべき基礎知識の実態（基礎知識の習得レベル）	情報漏えい／セキュリティリスクに関する知識レベルが把握できない、または知識が足りない　等	○
内部不正防止に取り組む組織的体制の実態（組織体制の整備）	組織全体としての責任・権限が明確に定められていない	△
	社内ポリシー／規定の整備が不十分な企業が多い	○
組織全体への周知・教育の実態（組織的な周知・教育の現状）	一般の職員に対する、内部不正対策に関する周知・教育は不足している	△
内部不正防止の課題と対策（対策整備の現状）	重要情報の範囲が個人情報から技術情報・ノウハウ等にまで広がっているものの、これらの漏えいに対するリスク認識が十分ではなく、内部不正対策の拡張が進んでいない	○
	急増する中途退職者／中途採用者の内部不正に対する対策整備が遅れている、または対策が実施できていない	○

出典：企業における内部不正防止体制に関する実態調査概要説明資料

得られた課題と今後の方向性（1/2）

仮説の検証結果と得られた示唆を取りまとめるにあたり、**課題とこれに対する今後の方向性を抽出・整理**した。
このうち**特に重要なのは、「経営層が重要情報漏えい／内部不正リスクを重要な経営課題として認識する意識変革の推進」**である。経営層に内部不正リスクを重要な経営課題として認識させることで、企業の内部不正対策や、リテラシー教育等のその他の取り組みの促進に大きな効果を期待することができる。この変革のきっかけとなるのは重要情報の漏えい事案のリアルな事例に触れることであり、**経営層はこれらから学ぶ感性を養うことが重要**である。

主題	課題	今後の方向性
共通事項	■ **内部不正リスクが重要な経営課題であるという認識を企業に浸透させることが必要。** ■ **経営層、組織全体の責任者等が営業秘密漏えい等の事案／インシデントから学び、事業リスクを強く認識することが必要。**	■ **重要情報漏えい／内部不正リスクを重要な経営課題として認識する意識変革の推進（To: 経営層、内部不正防止に関する組織全体の責任者等）** ■ **個人情報に留まらず、他の重要情報の漏えい事案などリアルな事例に触れることで、事業リスクとしての重要性を学ぶことができる感性とリテラシーを育成（To: 経営層、内部不正防止に関する組織全体の責任者等）**
内部不正防止に関する組織全体としての基礎知識の取得と周知・教育のあり方	■ 重要情報漏えい／内部不正防止の社内規程及びその規則を学ぶ機会をさらに増やすことが必要。 ■ **営業秘密の知識を根付かせるために、従業員に法知識よりも何をしてはいけないのかを教育することが必要。** ■ 情報システム部門が内部不正防止の全社責任を負うためには、当該部門の持つ法知識を強化することが必要。 ■ 必要な知識を組織に根付かせるには、教育するだけでなく、教育した内容を理解させることが必要。	■ 企業のサイバーセキュリティ／コンプライアンス等に関する取り組みの一環として、重要情報漏えい／内部不正防止の社内規程及びその規則に焦点を当てる回数を増やし、組織全体の基礎知識と理解を促進（To: 従業員） ■ **営業秘密の知識を組織全体に根付かせるため、入社／人事異動／退職等の重要なタイミングで、具体的に重要情報を示して、何をしてはいけないのかを周知徹底（To: 従業員）** ■ 法務・知財担当者との連携を強化し、情報システム担当者の重要情報／内部不正に関する法知識の理解を促進 ■ e-Learningに限定せず、インシデント事例、解説動画・イラスト等のリッチコンテンツ、グループディスカッション、定期的な規則遵守のセルフチェック等を積極的に活用して理解を深める取り組みを推進（To: 経営層、従業員）

出典：企業における内部不正防止体制に関する実態調査概要説明資料

得られた課題と今後の方向性（2/2）

（続き）

主題	課題	今後の方向性
内部不正防止のための組織的体制整備のあり方	■ 次の２つの責任・権限が実効的に確保され、全社的に対応できることが必要。 i. 内部不正対策を具体的に計画し、実施する責任・権限 ii. 経営層が定める基本方針に基づき、組織全体の立場から内部不正対策の計画を承認し、実施を統制する責任・権限 **■ 経営層の不正に対しても内部不正対策のマネジメントシステムが実効的に機能することが必要。**	■ 責任部門自体（リスク・コンプライアンス部門等）と関連部門（情報システム部門、法務・知財部門、営業・事業部門）との協働、または対策実施・統制部門（情報システム部門等）と関連部門との協働等による組織全体のガバナンス構築 **■ 経営層の不正への対策と透明性の確保について調査検討**
重要情報漏えい／内部不正対策強化のあり方	■ 個人情報以外の重要情報の漏えい／内部不正対策の強化が必要。 **■ 悪意の不正に対し、効果とコストを両立できる対策の整備が必要。** ■ 中途退職者／中途採用者の急増に対応できる内部不正対策を確保することが必要。	■ 個人情報以外の重要情報の特定と対策の推進（To：従業員） **■ 悪意の不正に対する人的・組織的対策と技術的対策のバランスの適正化（まずは従業員教育に軸足を置き、これでカバーできないところから技術的対策を順次適用していく等）** ■ 企業の中途退職者／中途採用者の内部不正に対する対策強化の推進 ・経営層の不正防止と透明性確保 ・アクセスログの確認範囲拡大 ・他社の重要情報の不正な社内持ち込み防止 ・重要プロジェクト就任／離任時にも秘密保持義務の誓約書を取得 ・重要性の高い秘密に触れるかによる誓約書の詳細度の変更　等

出典：企業における内部不正防止体制に関する実態調査概要説明資料

本資料に関するお問い合わせ先

【お問合せ先】

株式会社NTTデータ経営研究所　エグゼクティブスペシャリスト　三笠武則（みかさたけのり）
（営業秘密保護推進研究会　事務局長）

E-mail: mikasat@nttdata-strategy.com　　TEL: 090-1459-0597