「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」の概要

2024年7月29日

独立行政法人情報処理推進機構
セキュリティセンター リスクマネジメント部
佐川　陽一

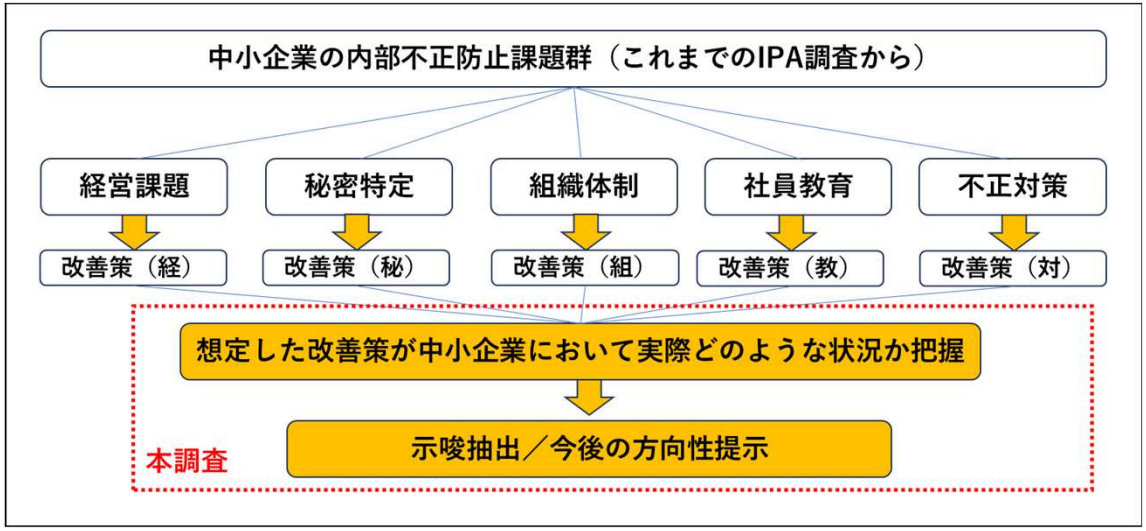
IPA Better Life with IT

本調査の背景・目的

以前の内部不正対策調査で判明した課題

内部不正防止対策および体制整備が進展していない
（特に中小企業等において顕著）

経営課題としての内部不正防止の認識、重要情報資産特定、
内部不正防止対策が後手に回っている状況など



本調査の目的

中小企業に焦点を当てつつ―

1. 内部不正防止体制整備を進展させる
   改善策を整理する
2. 実態調査を通じて、
   改善策の実施状況や関連する
   好事例を明らかにする
3. 現状を改善するための
   今後の方向性を検討する

調査の方法

調査メニュー

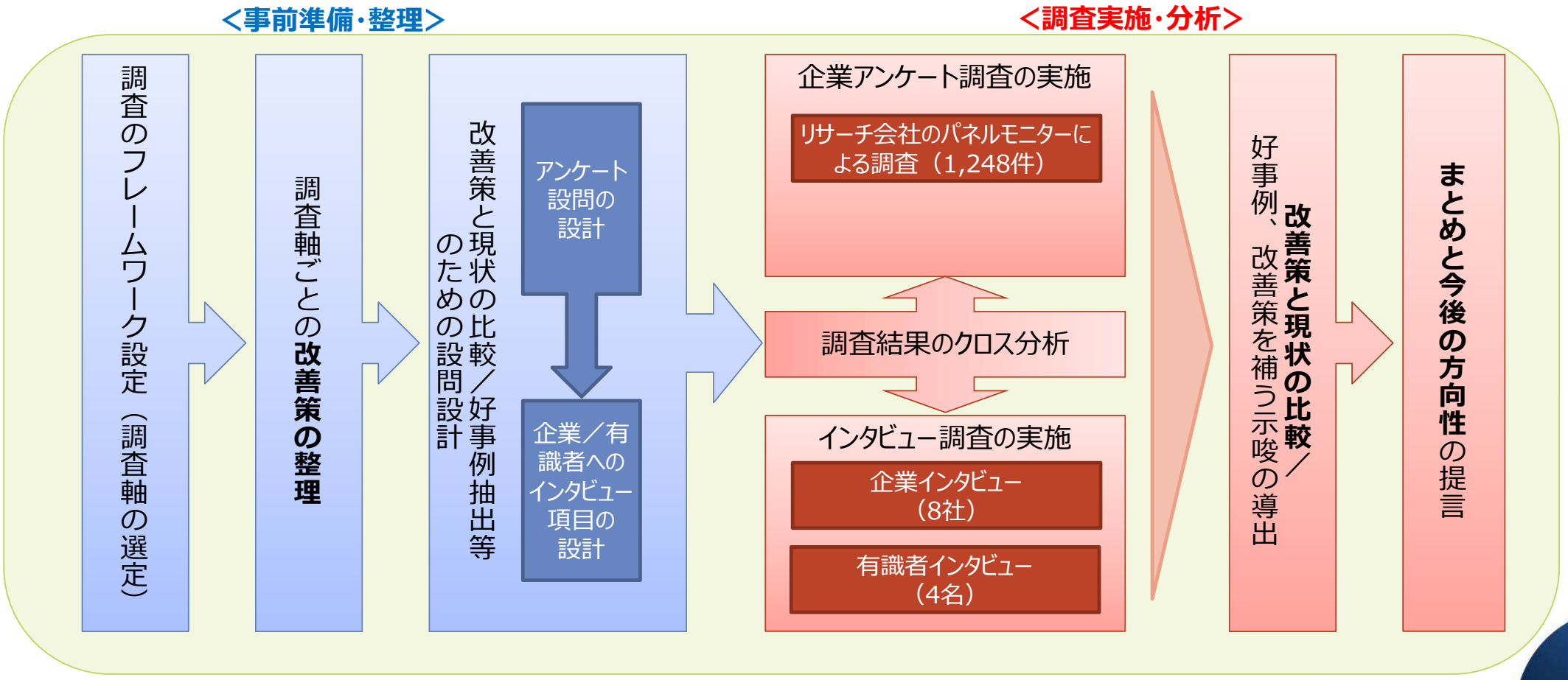
- **アンケート調査**
  - オンラインWebアンケート
  - 回答結果をクロス分析
- **インタビュー調査**
  - 有識者と先進的中小企業にインタビュー
  - 好事例等の有用な示唆を収集

７つの調査軸

- **下記７つの視点を調査軸として設定**
  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
- **この７軸に沿い、一連の改善策を整理**
- **アンケート/インタビューで**
  これらの改善策に関する実態を調査

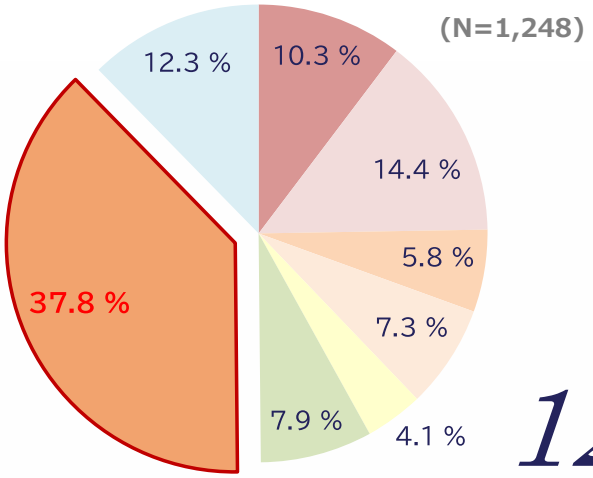
調査プロセス

「改善策の整理」→「改善策と現状の比較」→「まとめ」作業を共通の調査軸に基づき実施



調査の対象

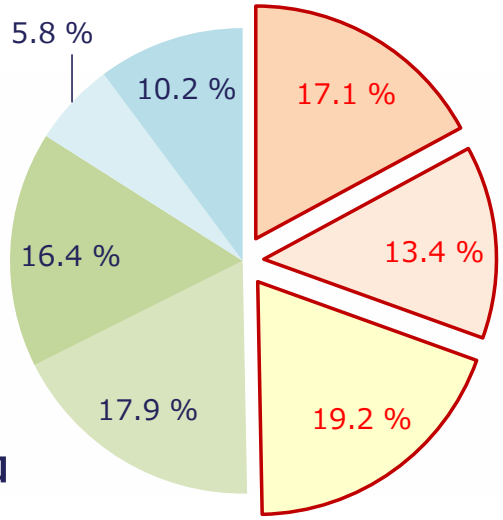
アンケート調査対象者の役職
1/3以上が経営層



1248名

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

アンケート調査対象者の所属企業規模
半分が中小企業



- **21～50人（17.1 %）**
- **51～100人（13.4 %）**
- **101～300人（19.2 %）**
- 301人～1,000人（17.9 %）
- 1,001人～5,000人（16.4 %）
- 5,001～10,000人（5.8 %）
- 10,001人以上（10.2 %）

インタビュー調査

- 秘密情報漏えい／内部不正の防止の取組が進んでいる中小企業

8社

- 内部統制、不正防止の有識者

2名

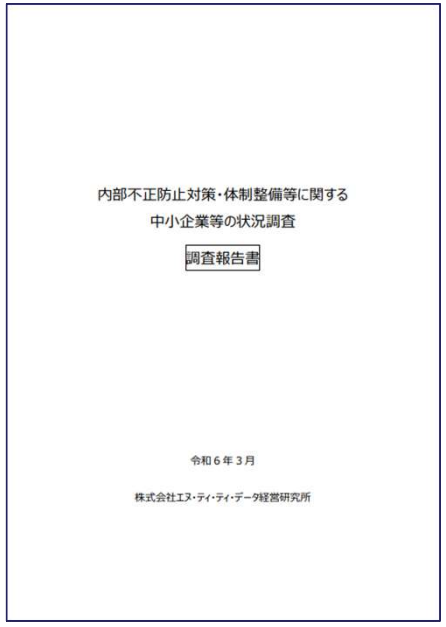
- 知財保護の有識者

2名

調査報告資料

- 2023年度「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」報告書

  https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html



調査報告書

概要説明資料

調査結果：主な改善策への取組実態

【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、一般従業員および関連部門と**対話する機会**を設けているとする回答の割合

52.4% 大企業 vs 45.2% 中小企業

【Q4】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**とする回答の割合

70.9% 大企業 vs 48.5% 中小企業

【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**できるとの回答の割合

38.7% 大企業 vs 21.8% 中小企業

【Q20】個人情報以外の秘密情報（**営業秘密**、重要なデータ等）を保護する対策を、**個人情報を保護する対策以上に重視**しているとする回答の割合

30.3% 大企業 vs 14.5% 中小企業

※ アンケートのクロス集計結果を基に比率算定。本調査では常時使用する従業員が300名以下を中小企業、それ以外を大企業に分類

調査結果：その他実態～経営層のリスク認識

中小企業では、**経営層の秘密情報漏えいに関するリスク認識が全体平均と比べて全般に低い**。
ただし経営層のリスク認識さえ上がれば、状況を一変させやすい環境にはあり、まずは経営層の意識を高めることが重要。

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

低調

調査結果：その他実態～秘密情報特定・格付の取組

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**。

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

低調

調査結果：中小企業の内部不正対策推進のヒント

◆中小規模ならではのリーダーシップ発揮

- ✓ 中小企業における経営層の意識やリーダーシップが持つ意味は大変大。そうした意識のもと、リーダーシップを発揮し、リスクや対策優先度の判断を行い内部不正対策強化の推進力とする。
  中小企業では経営者と従業員の距離が近く、経営層のメッセージが響くため
  社員が集まる機会等で全従業員に、内部不正対策の経営方針や判断、蓄積した知見を直接伝える。

◆リソース節約型の部門連携

- ✓ 内部不正防止に特化したリスク管理体制がない場合でも、情報システム／セキュリティ部門が内部不正防止で必要とされるIT技術面をカバーし、総務・人事部門が内部不正防止体制をカバーするように指向し、少ないリソースで専門管理部門設置と同等の効果を期待する。

◆最小限の内部不正対策付加

- ✓ サイバーセキュリティ対策でカバーできない内部不正特有の対策等は、ある程度実施されている既存のサイバーセキュリティ対策に上乗せすること（共通の対策を適用しつつ、守るべきものとリスクの違いに応じて足りないところを補うのみとする）が、効率的かつ効果的。

調査結果：インタビュー調査からの示唆･好事例

◆取りかかるきっかけを生かす

- ✓ 経営者が自ら主導して*技術情報管理*や*ISMS*等の可視化しやすい認証を取得すること等が秘密情報漏えい／内部不正リスクを重要な経営課題として認識するための契機に。
- ✓ （未導入であれば）*情報資産台帳*を用いた秘密情報管理の導入も同時に期待。

◆小回りの利く機動力を生かす

- ✓ 経営者が自ら戦略を語り、基本方針を周知徹底
  自身の想いを伝えることで従業員に対するリーダーシップを発揮。
- ✓ 中小企業ならではの機動性を生かし、事業リスクの判断や秘密情報の特定・格付けをスピードアップ。

◆風通しの良さを生かす

- ✓ 社員が少数という中小規模ならではの風通しの良さ、顔の見える人間関係を生かしつつ、
  内部不正防止のための監視・報告体制整備に際し、その意義をじっくり説明しながら構築。
- ✓ 唐突な体制整備による不信感を抑止。


IPA