「企業における内部不正防止体制に関する実態調査」実施背景とポイント

2023年5月26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　セキュリティ対策推進部
佐川 陽一

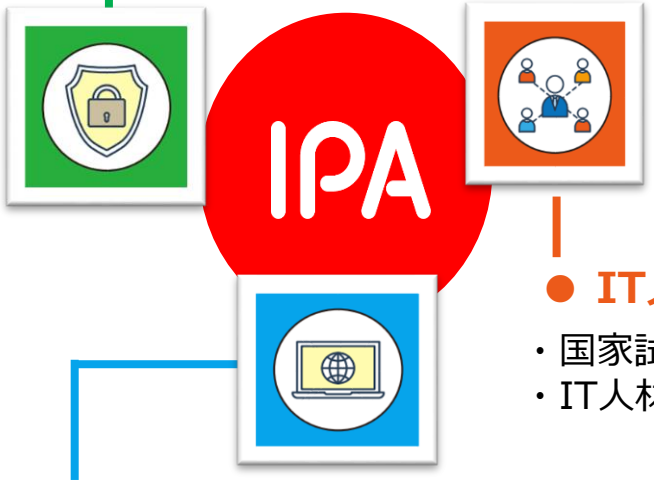
概要

1. IPAの内部不正防止に関する活動
2. 近年の内部不正事案
3. 2022年度内部不正防止体制調査の概要

1．IPA(情報処理推進機構)の活動

Information-technology Promotion Agency, Japan

- 日本のIT国家戦略を技術面、人材面から支える経済産業省所管の独立行政法人
- 誰もが安心してITのメリットを実感できる「 **頼れるIT社会** 」を目指しています



● 情報セキュリティ

・ウイルス、不正アクセス等の届出機関
・情報セキュリティの調査研究、普及啓発活動
・標的型サイバー攻撃への情報共有・初動対応の実施

● IT人材育成

・国家試験「情報処理技術者試験」の実施機関
・IT人材の育成・発掘・スキル明確のとりくみ。若手人材育成

● IT社会の動向調査・分析・基盤構築

・新たなIT社会の動向調査、新しい技術の安全性・信頼性の確保に向けた指針策定など

情報セキュリティ10大脅威 2023 脅威ランキング

https://www.ipa.go.jp/security/vuln/10threats2023.html

・2022年に発生した情報セキュリティ事案を専門家投票によりランクづけ

前年順位	個人	順位	組織	前年順位
1位	フィッシングによる個人情報等の詐欺	1位	ランサムウェアによる被害	1位
2位	ネット上の誹謗・中傷・デマ	2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	メールやSMS等を使った脅迫・詐欺の手口による金銭被害	3位	標的型攻撃による機密情報の窃取	2位
4位	クレジットカード情報の不正利用	4位	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	5位	テレワーク等のニューノーマルな働き方を狙った攻撃	4位
7位	不正アプリによるスマートフォン利用者への被害	6位	修正プログラムの公開前を狙う攻撃（ゼロディ攻撃）	7位
6位	偽警告によるインターネット詐欺	7位	ビジネスメール詐欺による金銭被害	8位
8位	インターネット上のサービスからの個人情報の窃取	8位	脆弱性対策の公開に伴う悪用増加	6位
10位	インターネット上のサービスへの不正ログイン	9位	不注意による情報漏えい等の被害	10位
圏外	ワンクリック請求等の不正請求による金銭被害	10位	犯罪のビジネス化（アンダーグラウンドサービス）	圏外

IPAが脅威候補を選出し、専門家約200名からなる「10大脅威選考会」が投票

IPAの営業秘密保護・内部不正防止関連活動

年度	内部不正防止	営業秘密保護	データ利活用	関連事象・成果移転先
2014	組織における内部不正防止ガイドライン 改訂第2版	営業秘密保護システムPP作成		ベネッセ事件 営業秘密保護システムPP
2015	改訂第3版	企業のログ管理状況調査		営業秘密管理指針改正
2016		企業の営業秘密管理実態調査		不正競争防止法改正 秘密情報の保護ハンドブック
2017	改訂第4版	秘密情報の管理と利活用に関するリスク・対策調査	データ利活用における重要情報共有状況調査（米国）	クラウド・モバイル・AI等のIT環境変化
2018			安全なデータ利活用に向けた準備・ 課題認識調査	不正競争防止法改正（限定提供データによる利活用推進）
2019			企業におけるデータ利活用・保護の戦略立案調査	企業におけるデータ利活用・保護戦略立案の手引き書（2020）
2020		企業の営業秘密管理実態調査2020		テレワーク（コロナ） 個人情報保護法改正
2021～	改訂第5版公開	企業の内部不正防止体制実態調査2022		秘密情報の保護ハンドブック改訂

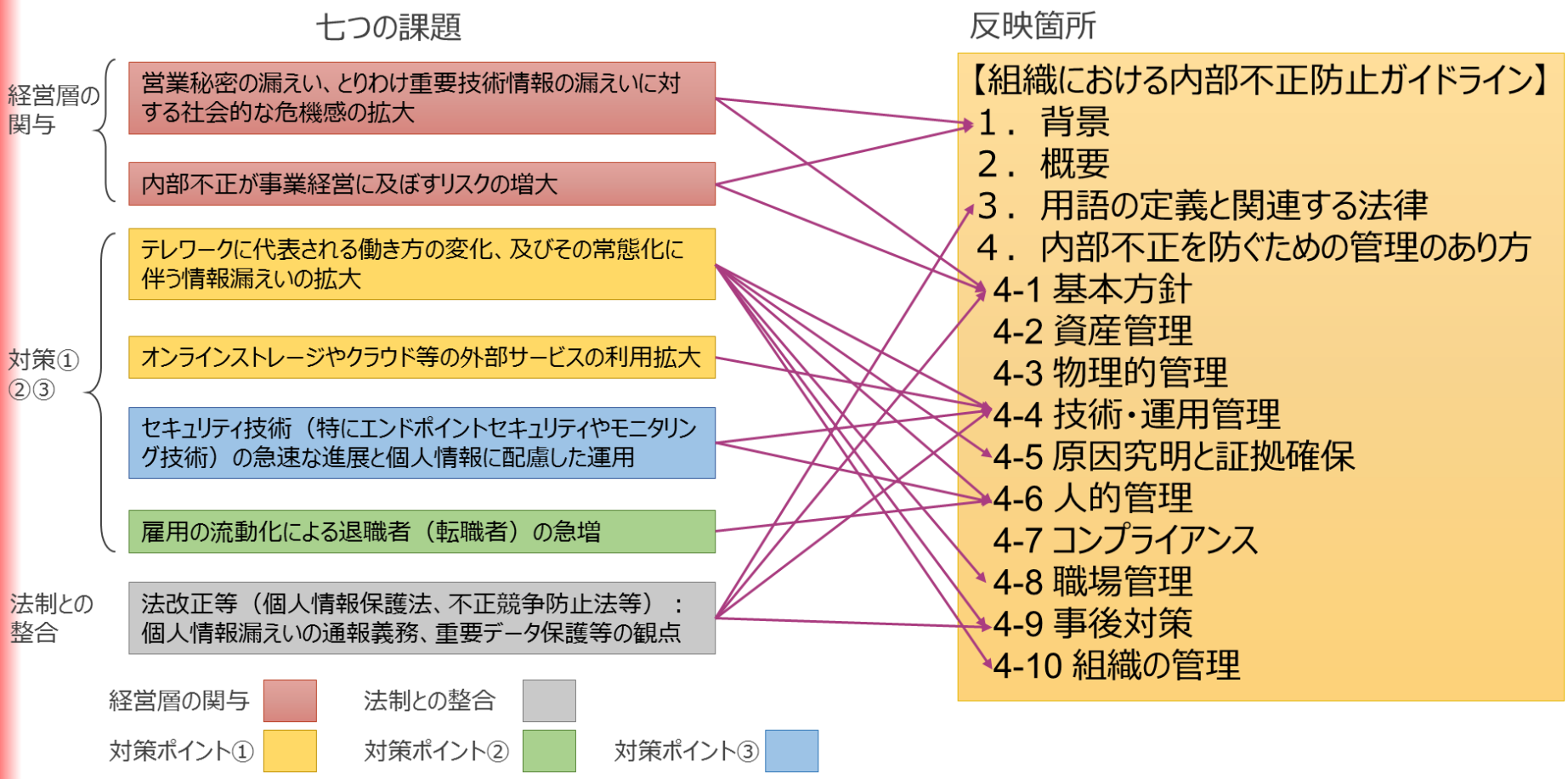
組織における内部不正防止ガイドライン

https://www.ipa.go.jp/security/guide/insider.html

・組織の情報漏えいに関する内部不正対策に特化したガイドライン。
　2022年4月　改訂第5版発行（PDF）。

内部不正防止ガイドライン第5版の改訂

・2022年4月の第5版改訂ポイント



2. 近年の内部不正事案

事案の類型（ガイドライン付録記載）

類型	不正の内容
技術情報の国外への漏えい	企業の防衛・宇宙部門の職員：技術情報を国外に漏えい。 職員の出身国であった外国政府がアプローチ。
営業秘密情報漏えい	企業の職員：退職後に機密情報に不正アクセスし情報を窃取。 解雇に不満。退職後に共有アカウントのパスワードが変更されず。
顧客情報・個人情報の不正な持ち出し	委託を受けた海外現地法人職員：業務用PCへデータを許可なくダウンロード、海外のクラウドストレージへアップロード。 海外現地法人の教育、内部不正対策の周知徹底が不十分。
個人情報の暴露	自治体職員：貸与PCから個人情報を含むファイルを入手し、新聞社にメール。貸与PCに個人情報が残存。 職員に待遇の不満。管理不備をマスコミに告発する欲求から。
システム／プログラム破壊	企業の職員：退職前に開発中のソースコードを社内で共有せず削除。 処遇に不満。プログラム管理システムへのソースコード登録の手続き不備も被害拡大の一因。
システム／プログラム改ざん	企業の職員：貸与 PCにハッキングツールをインストール、他職員の認証情報を窃取、外部者に提供。 外部者は認証情報を用いて不正アクセス、Webサイト改ざん。 支給コンピュータにハッキングツールをインストール可能だった。

事案1　教育/介護/保育事業者

- 委託先の保守管理担当者による顧客情報大量流出

流出した個人情報は
約　**3,504万件**

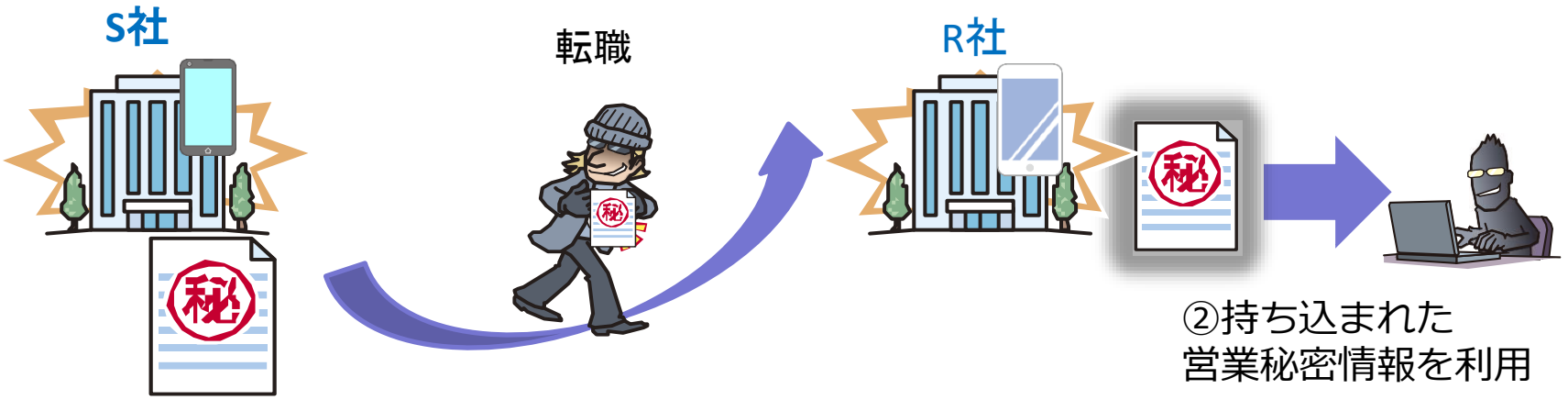
業務被害
- **2014年度第1四半期特別損失　260億円**
  2014年度当期純損失　107億円
- **役員2名辞任**

事案2　携帯電話事業者

- 転職者による営業秘密情報漏えい

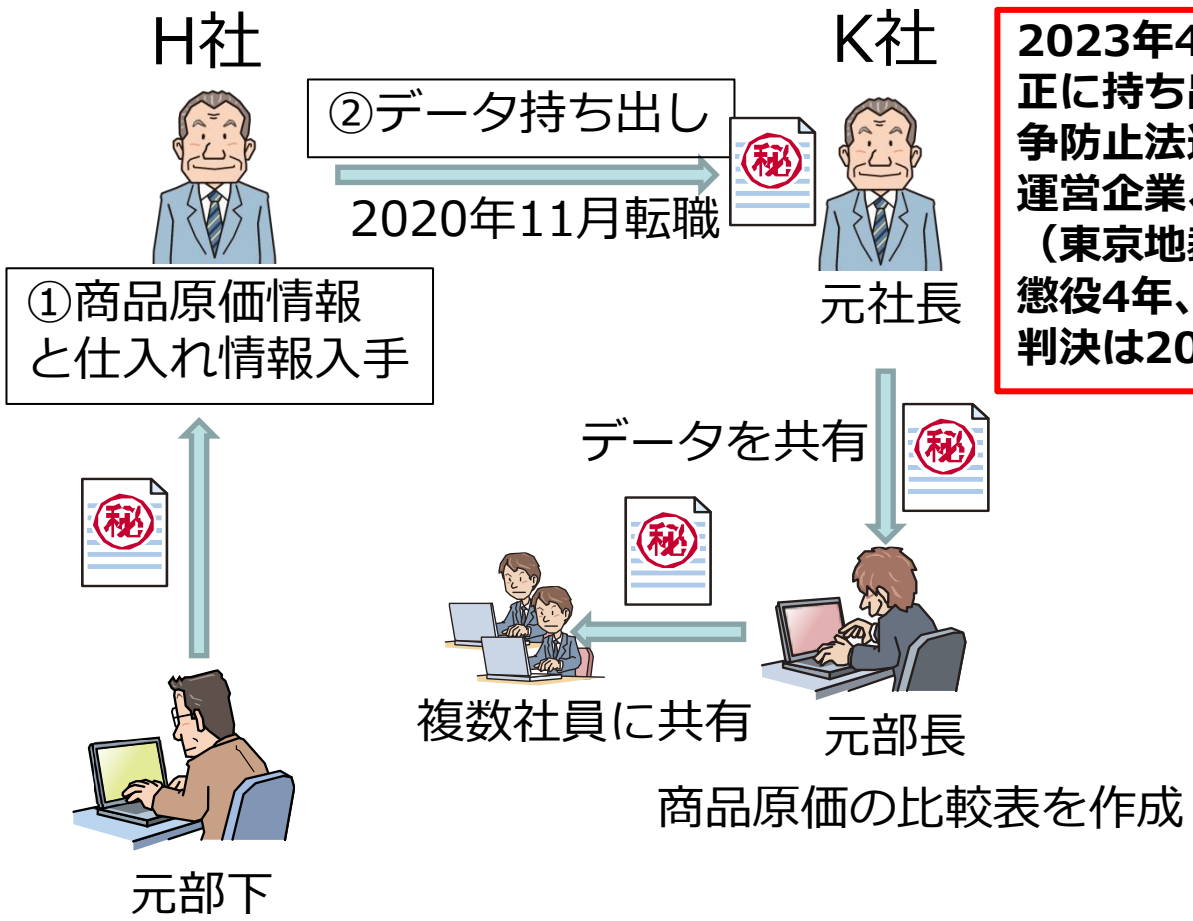
不正競争防止法に基づく損害賠償請求

2020年1月　元従業員転職（S社→R社）
2021年1月　元従業員逮捕
2022年12月 元従業員に懲役2年、執行猶予4年
罰金100万円刑有罪判決
なおR社に10億円損害賠償の係争中



事案3　飲食事業者

- 幹部による営業秘密情報漏えい



2023年4月 競合企業の営業秘密を不正に持ち出し使用したとして、不正競争防止法違反罪に問われた「K寿司」運営企業、K社元社長の論告求刑公判（東京地裁）。
懲役4年、罰金200万円を求刑、結審。
判決は2023/5/31。

事案4　証券会社

- 保守委託者による顧客情報の不正利用事例

➢ 2021年3月　証券会社M社のシステムの保守を委託されていた企業S社の元従業員が証券会社の顧客情報を不正に取得、使用したとして逮捕された

➢ 2022年１月　懲役4年6月の実刑判決

➢ 顧客12名の ID、パスワード、暗証番号等を利用
有価証券の売却や現金の不正出金
被害総額は約2億円弱に上った

➢ 事案後
M社は保守管理業務についての監視強化
S社は情報セキュリティーに関する研修の強化などの再発防止策を実施

事案5　米国国防総省

- アクセス権を付与されていた州兵による機密文書漏えい
  - 2023年4月　マサチューセッツ州空軍州兵がクリアランスの結果アクセスを許可されていた軍事機密を流出させたとしてFBIにより逮捕
  - ゲームコミュニティで自慢するために曝露したと供述、スパイ・政治的意図はなかったとされる
  - ウクライナの軍事機密をはじめ、同盟国の諜報に関する内容も含まれていた

3. 2022年度実施 内部不正防止体制調査の概要

2023年4月　調査報告書を公開

企業の内部不正防止体制に関する実態調査

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

調査概要

■ 企業アンケート調査

＜主たる回答＞パネルモニター：　**1,179名**（所属企業1,000社以上）
＜参考回答＞日経平均銘柄企業：　25社

■ 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

■ 有識者インタビュー調査：7名

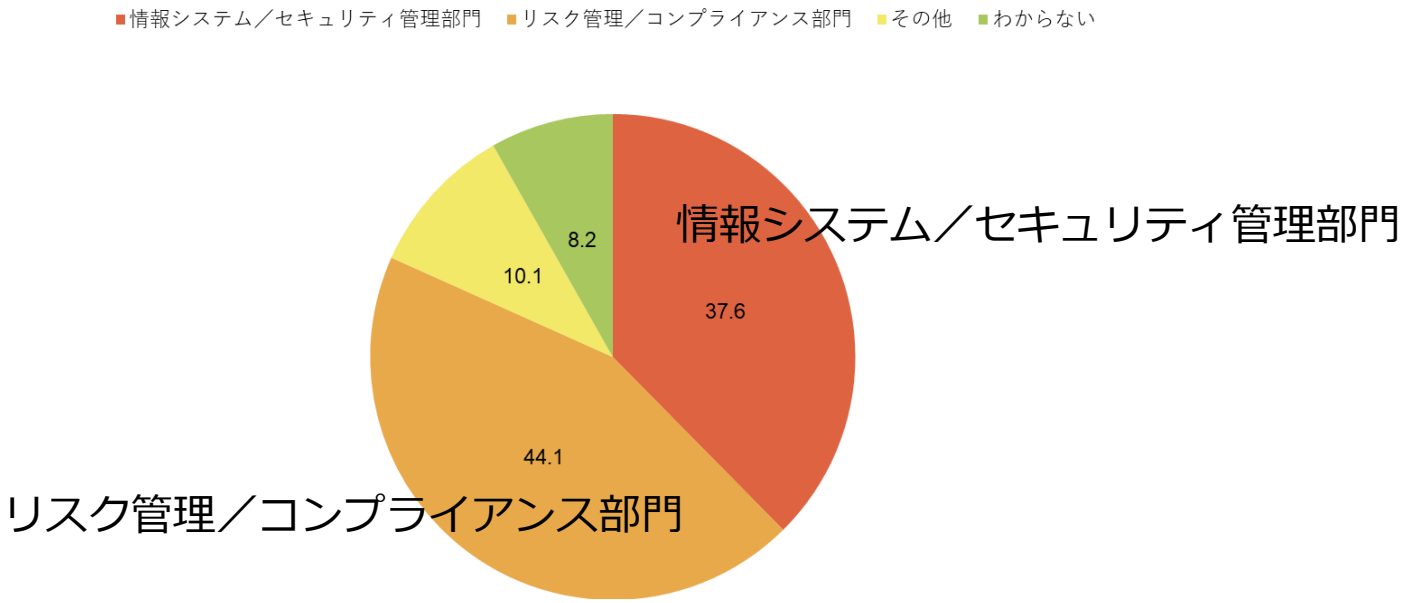
弁護士：　4名
民間企業経験者：　3名（うち1名は公認会計士）

内部不正対策に取り組む組織的体制

組織の状況

- 内部不正対策の責任部門
  概ね「情報システム／セキュリティ管理部門」と
  「リスク管理／コンプライアンス部門」に**二分**

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



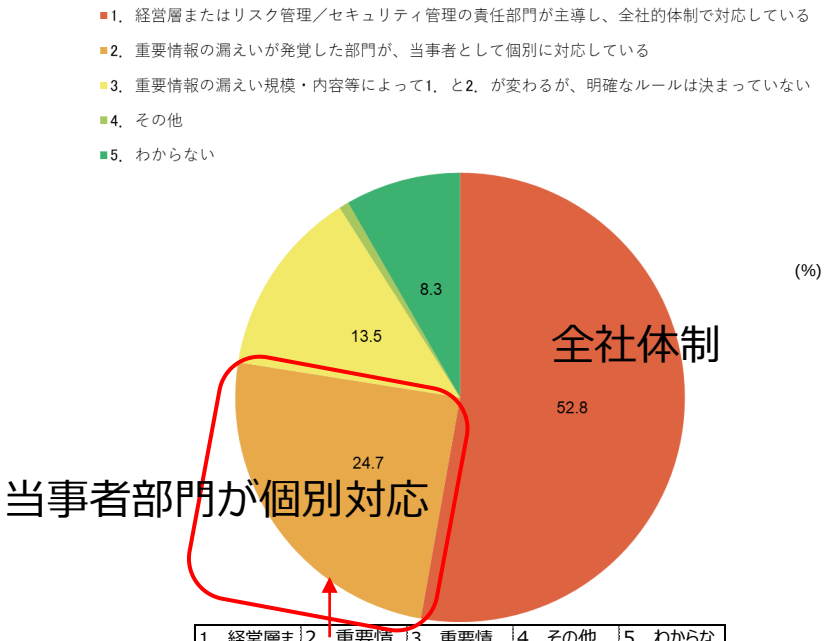
	n=	情報システム／セキュリティ管理部門	リスク管理／コンプライアンス部門	その他	わからない
TOTAL	1179	37.6	44.1	10.1	8.2

内部不正対策に取り組む組織的体制

組織の状況

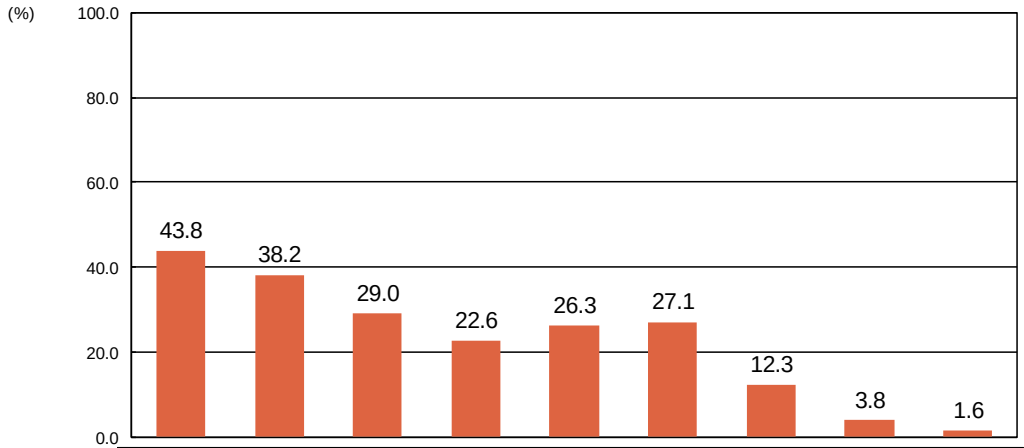
- 重要情報漏えいへの対応を**全社体制で行える割合は半数**
  現場組織の個別対応がかなり残っている

Q10. 重要情報が漏えいした時の組織的対応



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

Q21. 主管部門の統括の下で、連携して対策や事後対応にあたる関連部門



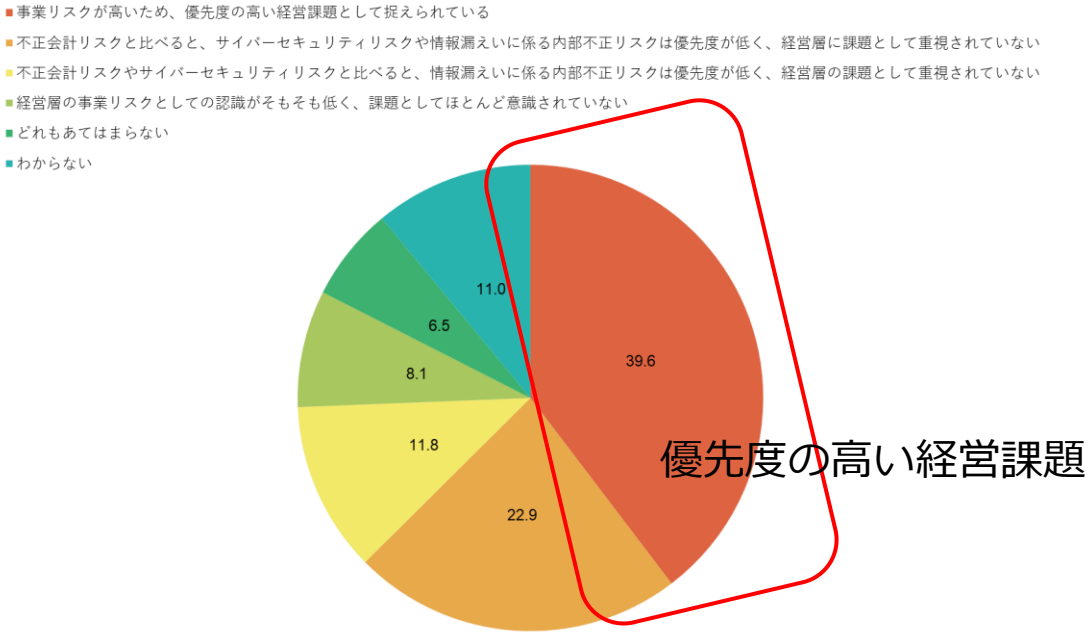
	n=	人事・教育部門	法務・知財部門	情報システム／セキュリティ管理部門	リスク管理／コンプライアンス部門	経理・財務部門	事業部門・営業部門	その他部門	特にない	わからない
	1082	43.8	38.2	29.0	22.6	26.3	27.1	12.3	3.8	1.6

内部不正対策に取り組む経営層の姿勢

組織の状況

- 経営層が内部不正リスクを優先度の高い**経営課題とした率は約40%**

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



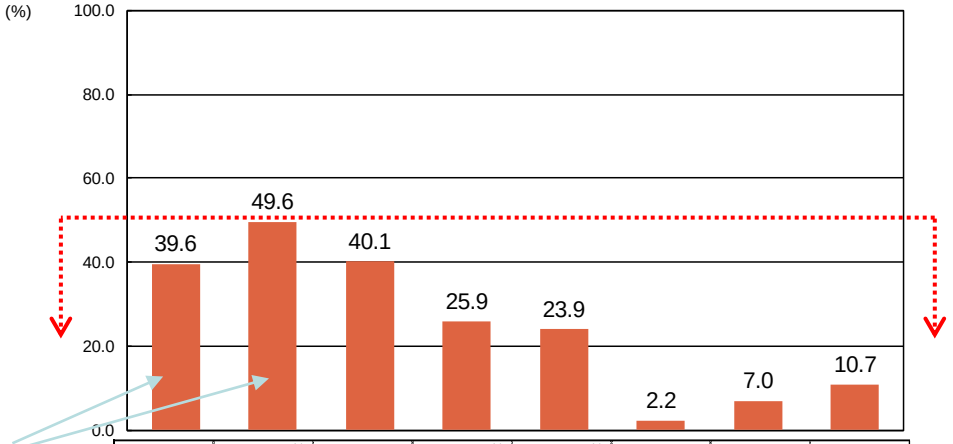
	n=	事業リスクが高いため、優先度の高い経営課題として捉えられている	不正会計リスクと比べると、サイバーセキュリティリスクや情報漏えいに係る内部不正リスクは優先度が低く、経営層に課題として重視されていない	不正会計リスクやサイバーセキュリティリスクと比べると、情報漏えいに係る内部不正リスクは優先度が低く、経営層の課題として重視されていない	経営層の事業リスクとしての認識がそもそも低く、課題としてほとんど意識されていない	どれもあてはまらない	わからない
TOTAL	1179	39.6	22.9	11.8	8.1	6.5	11.0

中途退職者への対応

対策の状況

- 中途退職者に課す秘密保持義務の実効性を高める対策
  内部規則に基づき秘密保持契約締結／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だが、実施は**50%に達していない**

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。



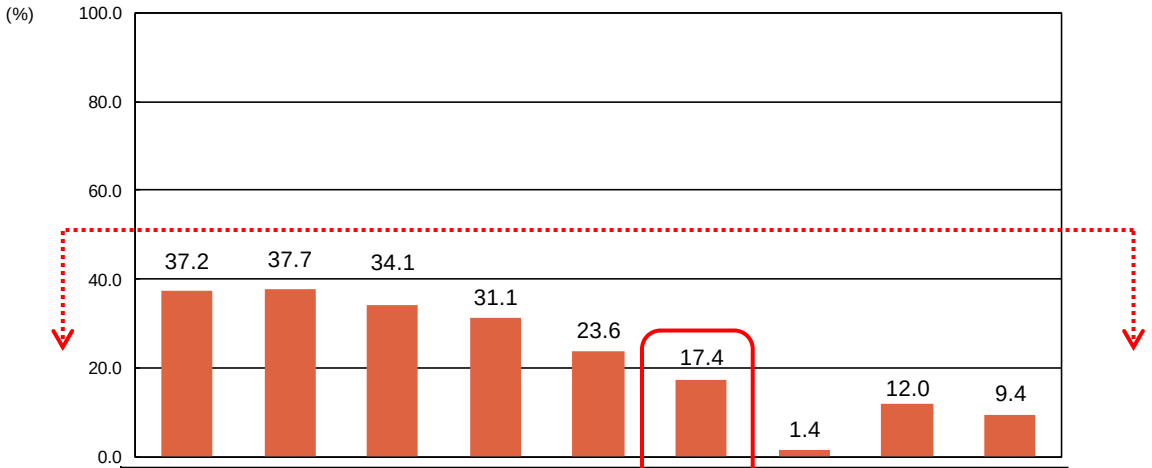
n=	退職時だけでなく、就職時、異動時、昇格時、新プロジェクトへの配属時・終了時等に、秘密保持義務契約の締結（または誓約書の提出）を求めている	秘密保持義務契約の締結（または誓約書の提出）についての内部規則を定め、就業規則でその順守を求めている	就業規則に退職後の定めを規定している	秘密保持義務の有効期間を十分長く設定している	秘密保持義務の対象となる重要情報の範囲・内容を明確に定めている	その他	実施していない	わからない
TOTAL 1179	39.6	49.6	40.1	25.9	23.9	2.2	7.0	10.7

テレワーク勤務の内部不正対策

対策の状況

- テレワーク時の内部不正対策について
  いずれの対策も実施の**回答が40%に満たず**、十分とはいいがたい

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



	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

概括

- 不正防止の**社内規程等の学習機会**、繰り返し周知が大切
- 組織の**権限の実効的確保、全社的対応できる体制**が必要
- 情報漏えいによる内部不正防止対策は「情報セキュリティ対策の一部」に留まり明示されないことが多い
- 個人情報保護と営業秘密保護ではまだ意識に差がある
- **重要情報の特定・棚卸**は、重要かつ残り続ける課題
- 低コストの従業員教育に軸足を置きつつ、悪意の不正対策は技術的対策でカバーし、効果の最大化を図るべき
- **経営層の対策**も「分けへだてなく」実施することが重要（不正に対する対策と透明性の確保）
- 中途退職者等の内部不正に対応できる**アクセスログ**の活用も重要


IPA
Better Life
with IT