第12回情報セキュリティマネージャー ISACAカンファレンス in Tokyo
Session 3：パネルディスカッション

DX時代の内部不正対策

– 組織を守り、強くする対策とは何か -

ISACA
Tokyo Chapter

パネリスト

ノートルダム清心女子大学
特別招聘教授 **小松 文子 氏**

NECにてネットワーク管理、セキュリティ製品・サービスの研究開発に従事後、IPA情報セキュリティ分析ラボラトリーラボラトリー長、長崎県立大学教授・副学長をを経て現職. 公的機関では、経済産業省産業構造審議会　知的財産分科会不正競争防止小委員会、NISC 重要インフラ専門調査会、研究開発戦略専門調査会などで委員を務める。
博士(情報学)

独立行政法人 情報処理推進機構(IPA)
セキュリティセンター
セキュリティ対策推進部　セキュリティ分析グループ
主任研究員 **佐川 陽一 氏**

住友電気工業株式会社研究開発本部サイバーセキュリティ研究開発室に所属する傍ら、情報処理推進機構の研究員として2015年から現在まで一貫して営業秘密管理や内部不正防止に関する実態や対策の調査、情報発信の業務に従事。

参考資料:
組織における内部不正防止ガイドライン（IPA 独立行政法人 情報処理推進機構）

ISACA Tokyo Chapter

組織における内部不正対策

IPA　組織における内部不正対策改訂検討会　座長
小松文子（ノートルダム清心女子大学）

自己紹介（小松文子）

- NECにてネットワーク管理製品の開発，標準化、セキュリティ製品・サービスの研究開発に従事
- IPA情報セキュリティ分析ラボラトリー初代ラボラトリー長
- 長崎県立大学　情報セキュリティ学科学科長・教授・副学長を経て
- 2023年4月よりノートルダム清心女子大学　特別招聘教授（現職）
- 経済産業省産業構造審議会　知的財産分科会不正競争防止小委員会、NISC 重要インフラ専門調査会、研究開発戦略専門調査会などで委員を務める。
- 主な研究領域は，「情報セキュリティと社会・組織・人間行動」「情報セキュリティリスクマネジメント」
- 博士（情報学）横浜国立大学大学院，第10回情報セキュリティ文化賞（2014年）

組織における内部不正防止のための活動@IPA

- IPAセキュリティセンター情報セキュリティ分析ラボラトリー
  - 情報セキュリティに対する社会科学的な観点からの調査・分析をミッションとした組織（2009年～）
- 情報セキュリティに関する行動原理を調査研究する必要性
  - セキュリティ対策の意思決定，対策実施行動
  - **内部者の不正**
- 内部者の不正
  - 顕在化しにくい（組織の評判・信頼への懸念による）
  - 技術的対策のみで防ぐことは困難（権限を保持する内部者による）
  - （国外の状況を調査後）組織における内部不正防止ガイドライン委員会発足(2012年)
    - **社会心理学，**法律家の専門家とともに検討を開始
  - 組織における内部不正防止ガイドライン　初版発行（2013年3月），第5版（2022年4月）

内部不正を誘発する要因

- **環境犯罪学**の観点から
  - 内部不正の3要素（機会，動機，正当化）
  - 状況的犯罪予防5原則
    - 犯行を難しくする（やりにくくする）
    - 捕まるリスクを高める（やると見つかる）
    - 犯行の見返りを減らす（割に合わない）
    - 犯行の誘因を減らす（その気にさせない）
    - 犯罪の弁明をさせない（言い訳させない）
- **組織心理学**の観点から
  - 組織帰属意識（忠誠心，満足度，組織コミットメント）
  - 日本的経営（年功序列，終身雇用，属人風土）
  - 不適切な組織ルール

DXやリモートワークなどの
職場環境の変化により
これら要因に影響を与えない
かに留意が必要である.

最新版（第5版）での更新・追加内容

- 経営者へのメッセージの強化
  - 経営者の責任，ガバナンスの必要性

- 社会環境や企業の事業環境の変化に対応
  - テレワーク導入・雇用の流動化に伴う対策の追加
  - モニタリングプログラムと人権侵害のバランス

- 第4版以降の関連法案（個人情報保護法，不正競争防止法，産業競争力強化法）改訂等への対応
  - 個人データ漏えい時の報告義務
  - 「限定提供データ」の取り扱い　など

CISMパネルディスカッション
内部不正対策に関するIPA動向ご紹介

2024年2月17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　セキュリティ分析グループ
佐川　陽一

IPA Better Life with IT

自己紹介（佐川 陽一）

■ 所属

（１）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　セキュリティ分析グループ
（２）住友電気工業株式会社
　　研究開発本部　サイバーセキュリティ研究開発室

■ 業務遍歴

- ネットワークシステム開発
- ネットワークのシステムエンジニア
- IT資産管理・セキュリティ管理システムエンジニア
- 営業秘密管理・保護関連事業（IPA）2015年～
- データ利活用関連事業（IPA）2017～2019年
- サイバーセキュリティ全般の調査・分析（住友電工）

IPA　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
2013	**組織における内部不正防止ガイドライン** 初版			
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 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**

※経済産業省　秘密情報の保護ハンドブック：
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

「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月に**改訂第5版**発行。

【組織における内部不正防止ガイドライン】

1．背景
2．概要
3．用語の定義と関連する法律
4．内部不正を防ぐための管理のあり方
- 4-1　基本方針
- 4-2　資産管理
- 4-3　物理的管理
- 4-4　技術・運用管理
- 4-5　原因究明と証拠確保
- 4-6　人的管理
- 4-7　コンプライアンス
- 4-8　職場管理
- 4-9　事後対策
- 4-10　組織の管理

付録Ⅰ～Ⅷ（内部不正事例、チェックリスト等）

状況的犯罪予防の5原則
1．やりにくくする
2．やれば捕まる
3．わりにあわない
4．動機を減らす
5．いいわけさせない
をベースに整理

「企業の内部不正防止体制に関する実態調査」から

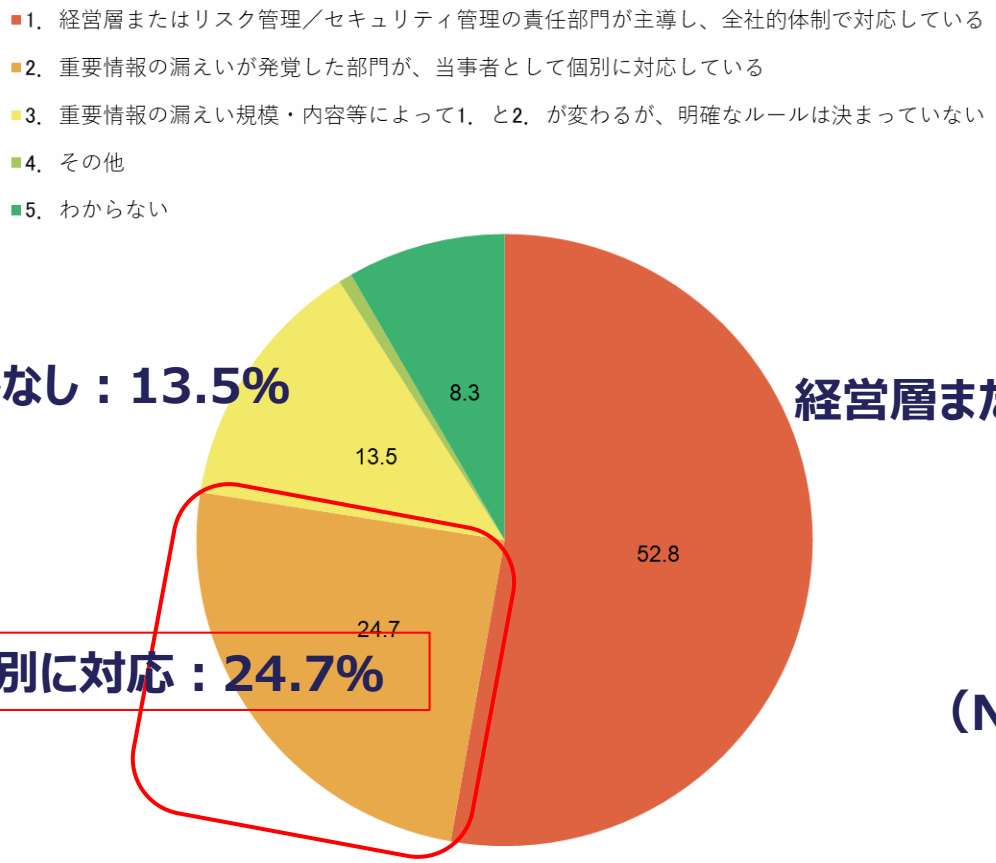
https://www.ipa.go.jp/security/reports/economics/ts-kanri/20230406.html

IPA

IPA　2022年度実施

- **内部不正対策に取り組む組織的体制**
  →重要情報漏えい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状況

Q10.重要情報が漏えいした時の組織的対応



明確なルールなし：13.5%

経営層または統括責任部門が主導：52.8%

当事者部門が個別に対応：24.7%

（N=1,179）

「企業の内部不正防止体制に関する実態調査」から

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

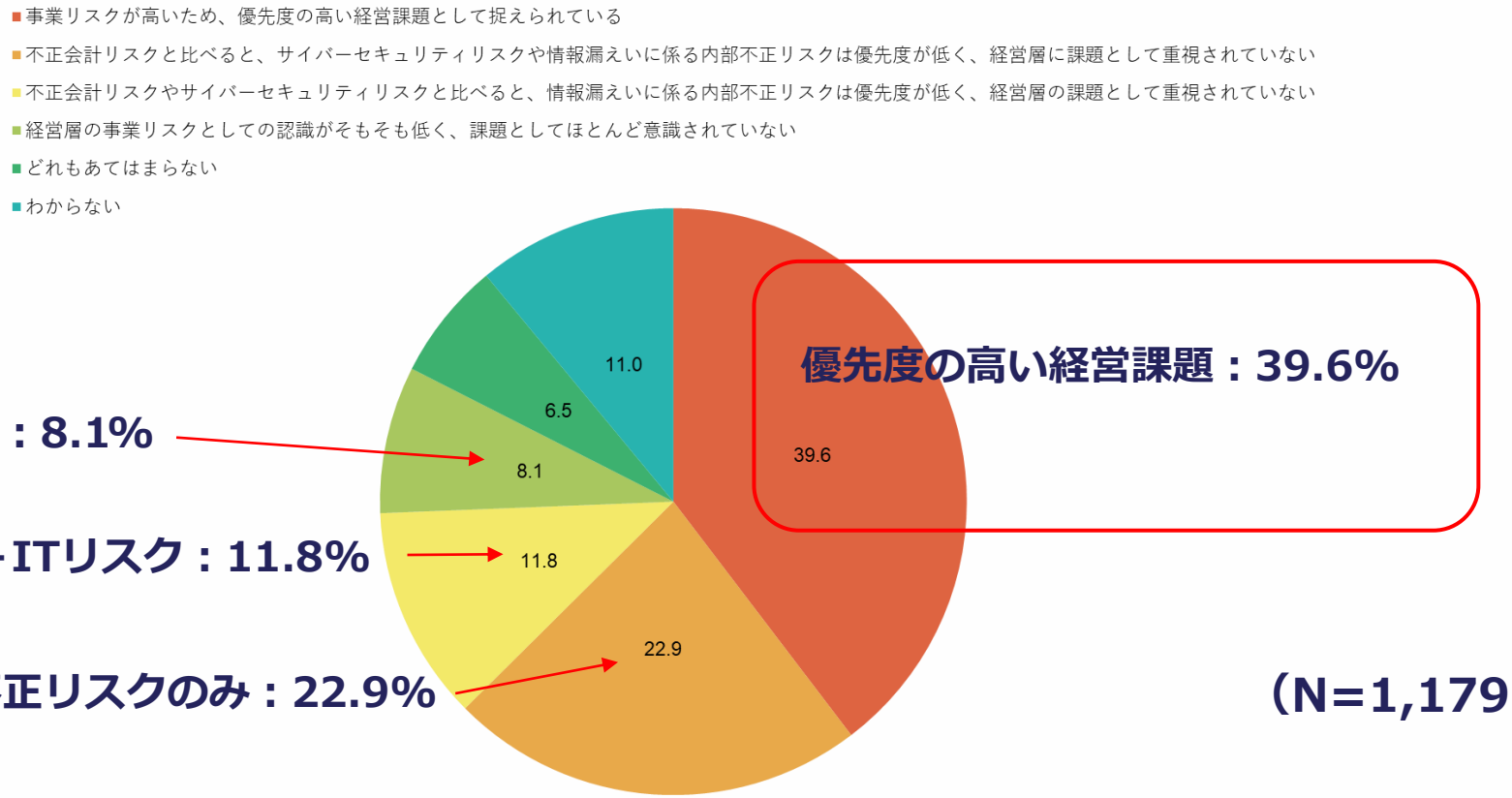
IPA

IPA　2022年度実施

- **内部不正対策に取り組む経営層の姿勢**

  →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。



優先度の高い経営課題：39.6%

課題として認識せず：8.1%

一般的な不正リスク+ITリスク：11.8%

一般的な不正リスクのみ：22.9%

（N=1,179）

「企業の内部不正防止体制に関する実態調査」から

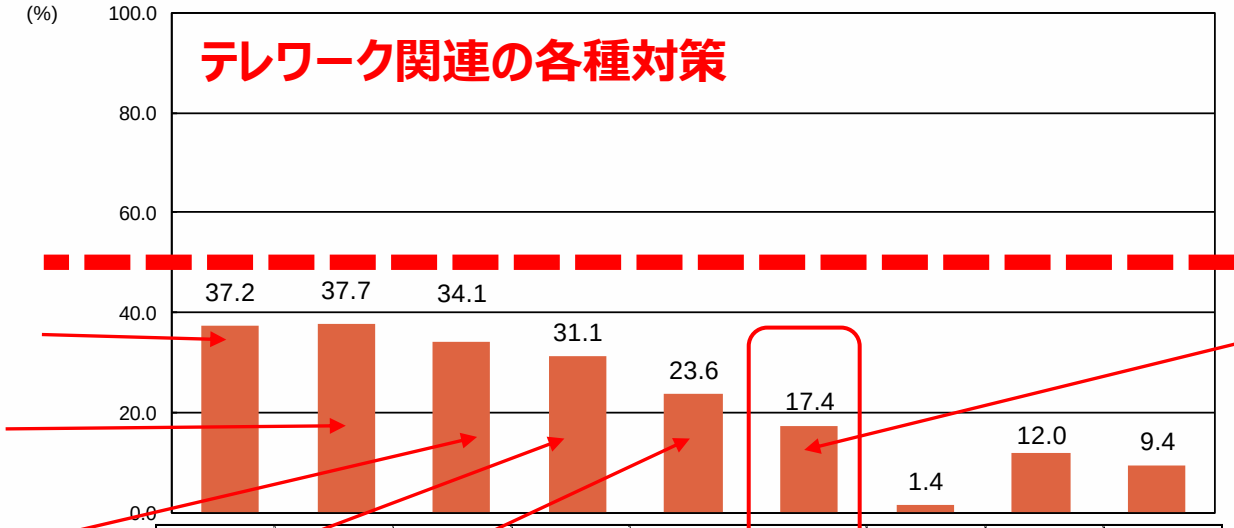
https://www.ipa.go.jp/security/reports/economics/ts-kanri/20230406.html

IPA

IPA　2022年度実施

- **テレワーク勤務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、時代変化をキャッチアップしているとはいいがたい状況

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



規則教育・徹底：37.2%

重要情報を制限：37.7%

ログ分析の強化：34.1%

ID・認証の強化：31.1%

公平な処遇：23.6%

コミュニケーションを確保する策を講じている：17.4%

	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

実施率が低い各内部不正対策（同実態調査）

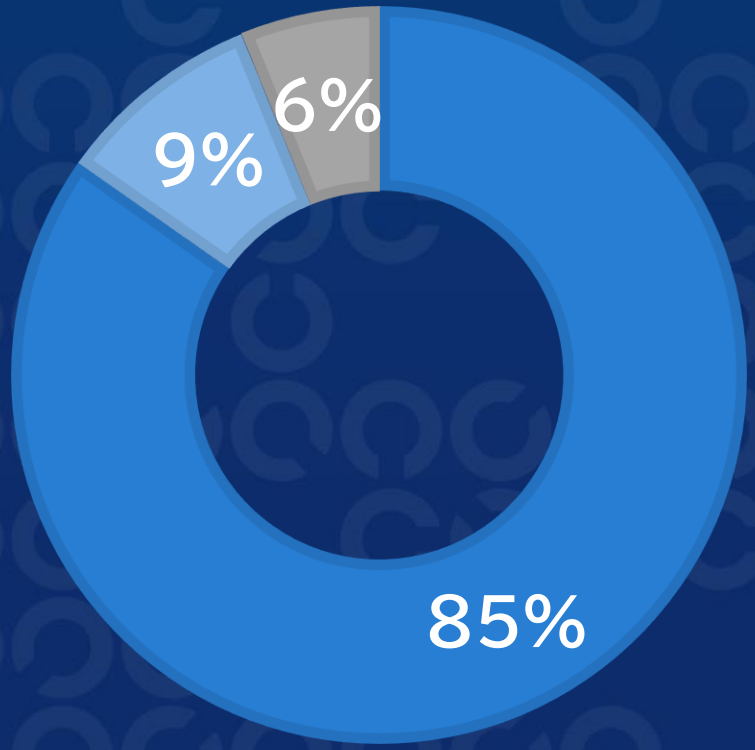
実施率（%）	対策（選択肢の要約）　IPA　2022年度実施
27.7	異動時・昇進時・新プロジェクトへの参加・終了時などに秘密保持契約締結または誓約書提出を求める
22.9	営業や技術の重要人物の退職が決まった段階で、重要情報へのアクセス監視及びアクセスログ確認等を強化する
21.4	重要情報を含む電子文書は容易に判別できるようにする
21.3	重要情報は定期的に棚卸しを行い、不要なものを消去する
21.1	BYODは許可しない
19.8	ガイドライン等に従い会社支給PCのテレワーク対策を強化する
19.8	テレワークで扱える重要情報の範囲をルール化する
19.7	使用できるクラウドやクラウドで扱う重要情報をルール化する
18.4	委託先等との重要情報の受渡しを厳格に管理、暗号化する
17.6	委託先等の情報漏えい対策を契約時・契約中に確認する
15.9	組織内外で内部不正事故が起こった場合、組織内で共有する

参加者アンケート結果

ISACA Tokyo Chapter

参加者アンケート

第12回情報セキュリティマネージャーISACAカンファレンス in Tokyoへの参加をお申込みいただいた方々の内訳



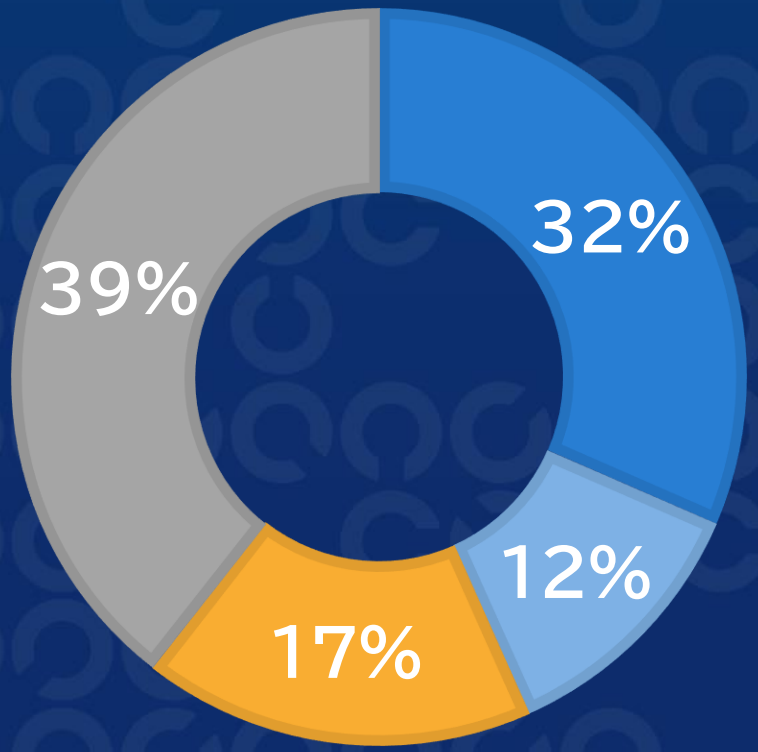
- ISACA東京支部会員
- 後援団体･他ISACA支部会員
- 一般

ISACA東京支部会員	374
後援団体･他ISACA支部会員	40
一般	27

ISACA Tokyo Chapter

お立場

内部不正対策に対するあなたのお立場をお聞かせください。

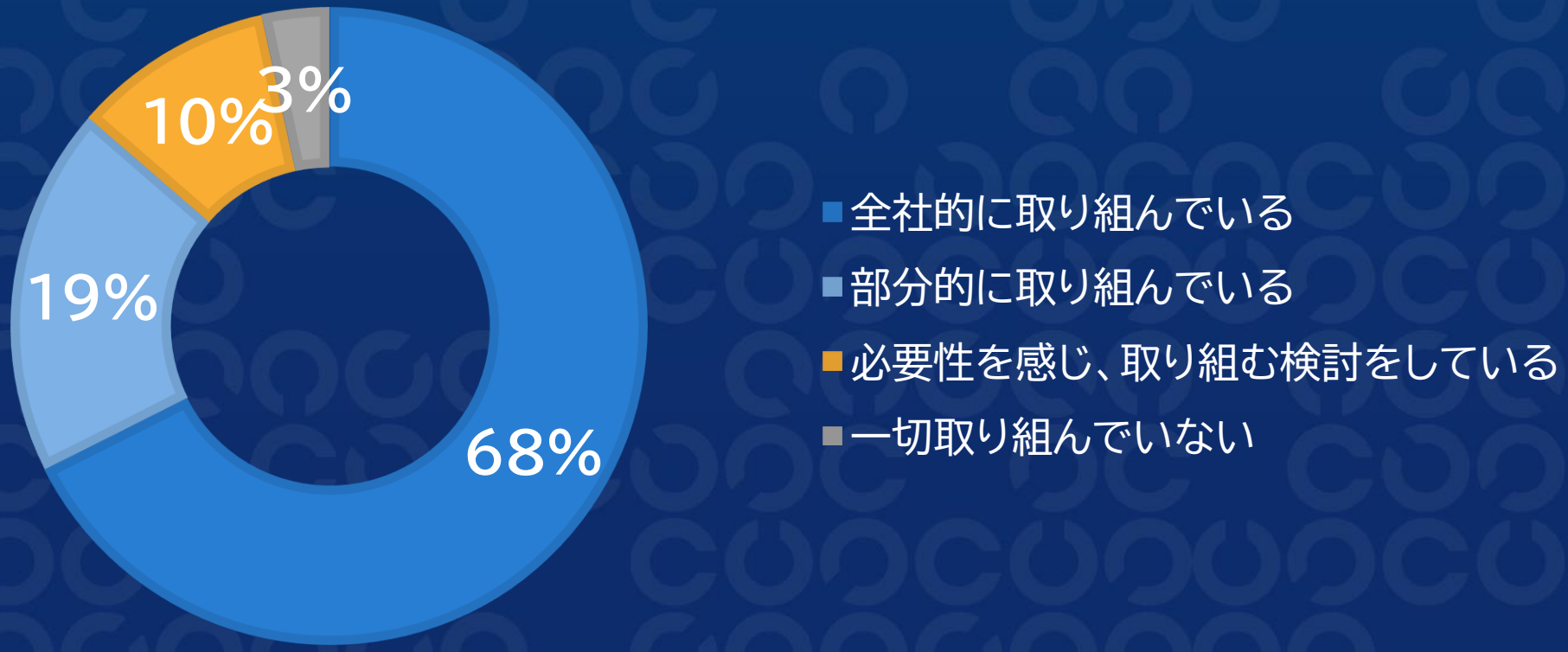


- 組織全体の内部不正対策を検討・実行する立場
- 組織の一部門の内部不正対策を検討・実行する立場
- 他社に内部不正対策を提案する立場
- 内部不正対策の検討には直接かかわる立場ではない

ISACA Tokyo Chapter

営業秘密の三要件

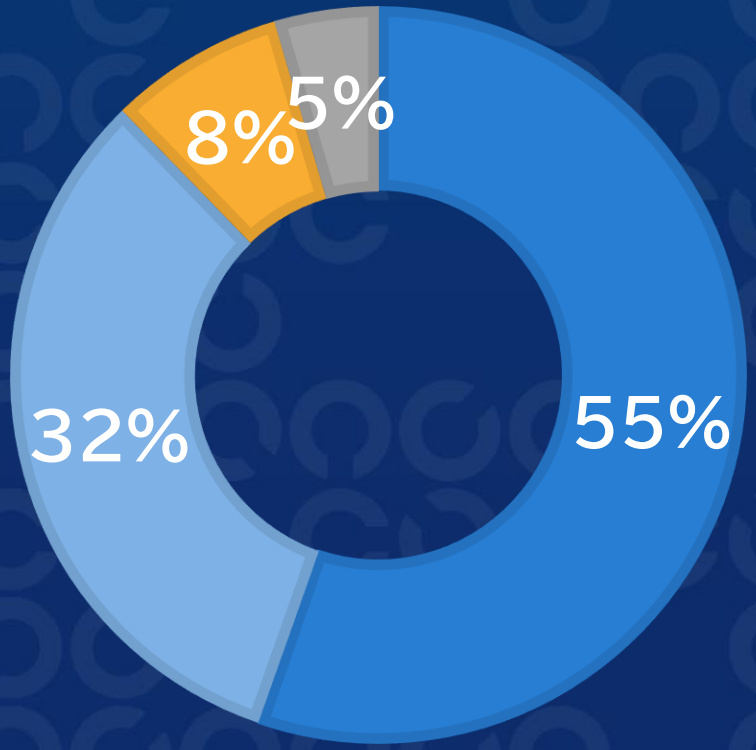
あなたの組織では営業秘密の三要件を満たす保護対策に取り組んでいますか？



ISACA Tokyo Chapter

ビジネス環境の変化

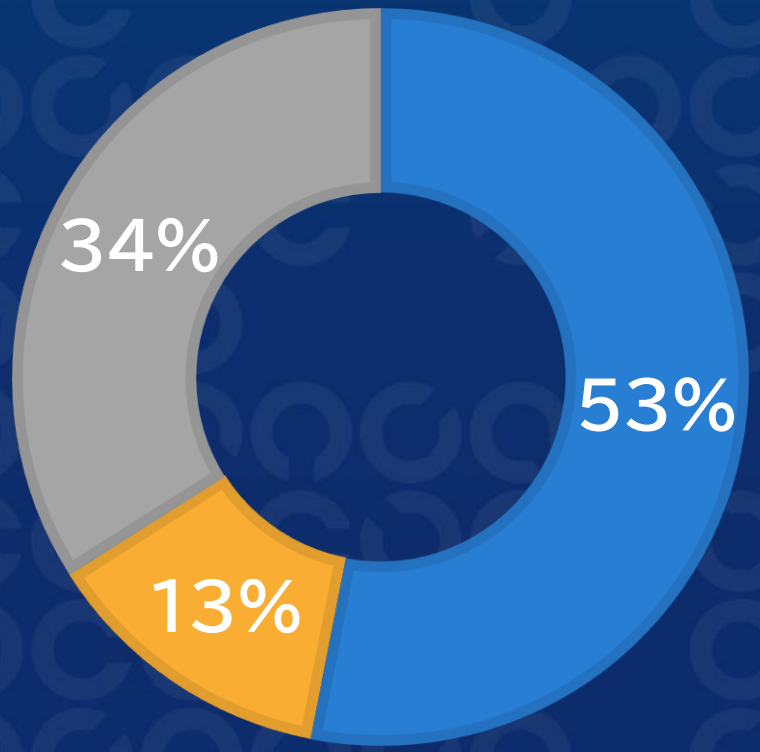
あなたの組織の内部不正対策は、ビジネス環境の変化に合わせて見直しが行われていますか？



ISACA Tokyo Chapter

ビジネスを優先したリスクの高い行動の増加

ビジネス目標の達成のためにセキュリティリスクの高い行動をしてしまうケースが増えていると感じますか？



ISACA Tokyo Chapter

いただいたご意見やご質問①

- 不正競争防止法の社会への浸透に伴い、内部不正対策が以前よりは各企業に浸透しつつあるように思います。かたや、法が意図している内容が今一つ、正しく理解されていないのではないかと思う場面に出くわすこともあるため、組織内における正しい理解と啓蒙活動への更なる努力の必要性についてのメッセージを積極的に伝えていただけると、バランスの取れた社会への浸透が促されるのではないかと現場で働く者としては感じています。
- 予算や人員がギリギリで組織が以前よりギシギシした感じになり、また利益優先になっていることから、不正が起こりやすくなっている。
- ビジネスとしての利益やスピード、結果をマネジメント層が重視する余り、リスク評価時の指摘事項についても、結果、セキュリテイ面を軽視するケースを目にする事が多く、非常に悩ましく感じている。(しかも、セキュリテイ・インシデント発生時には、その責を問われる事が免責される訳でもない)企業規模としてはグローバルを含めると3万人以上在籍するタイプである為、1担当者として、そうしたマネジメント層の動きを止めることもできない。改善事例などがあれば、ご教示頂けると幸いです。どうぞ宜しくお願い致します。

ISACA Tokyo Chapter

いただいたご意見やご質問②

- 内部不正は過去から変わらず、認証、認可、監視、アラートなどの抑止をどこまで周知できているかに大きく依存するものと考える。セキュリティ対策を細かく伝えることで穴を見つけられるリスクもあるのでどうするかが気になるところではあります。
- 中小企業において情報セキュリティ担当者は兼任であることが一般的であると思います。自部門の業務に集中してしまう中で内部不正やその対策が十分にできているかを考えることは難しく、対策の前に経営者が方針を示してほしいと思う。以前うちの会社で起きた内部不正は内々で済ませてしまっていたようで再発防止ができているとは思えない。
- 今後は、国際的にも日本企業に求められてくる重要な要件の一つとなると思います。
- 昨今の報道を賑わせているニュースにフェイクニュースがかなり多いそうですが、正しい情報を見抜く方法があればご教授ください。
- 社員の行動の振る舞い検知の導入を検討しています。事業部や職種によっても行動パターンはことなりなのですが、組織ごとに振る舞い検知をしてアラートをあげるパターンを変えるなどするのは運用がまわらないのですが、やはりそうしていくしかないでしょうか。アドバイスいただけないでしょうか。

ISACA Tokyo Chapter

いただいたご意見やご質問③

- 退職時のデータの持ち出しなどに注意が必要と考えている。
- 内部性を助長させる環境・要因などがございましたら、ご紹介いただけませんでしょうか。
- 内部不正の完全防御は困難でリスク許容度の設定が不可欠と感じている。また社員教育は重要なリスク低減要素であるとも考えている。
- 低コストで始められる内部不正の技術的対策
- 本人に貿易コンプライアンスを含めて内部不正の意識がなく情報漏洩その他の不正行為をしてしまう事例が増えていると感じている。
- 内部不正対策は、人に対する対策が重要だと思います。
- 営業秘密情報の不正持出し、漏えい対策以前に、身近にある営業秘密に対する理解が不足しているので、教育が重要であると考えています。
- 内部不正に関する事例紹介を期待します。

ISACA Tokyo Chapter

いただいたご意見やご質問④

- 内部監査で不正リスクを指摘した場合、フローの改善などに確実に活かすことが重要かと思います
- 内部不正やその対策の初学者にとってどのように学習、経験していけばよいか指針をお教えいただけないでしょうか。(情報処理安全確保支援士、CISAなど資格を取得して知識を徐々に習得していますが、内部不正に関する知識や経験が伴っていないためご指導いただきたい)
- 社外とのビジネス連携の機会が増えており、業務上で知得した機密情報の取り扱い、インサイダー取引の監視に定期的に取り組んでいる。
- 企業文化や、人材の質などで、内部不正の種類も変わってくると思います。こういう企業、こういう人員構成だと、こういった不正が発生しやすい。など、実績の分析も知りたいです。
- ガバナンス対策が最重要だと考える
- ガバナンスを効かせるために、内外組織の支援を上手く活用することが最も重要だと感じています。

ISACA Tokyo Chapter

いただいたご意見やご質問⑤

- 昨今のインシデント傾向からふさわしいテーマの選定をありがとうございます。
- 他社事例がなかなか公表されない領域であり対策案の策定が難しい。
- インシデントが起きた場合の対応の留意点についても知りたい。
- 不正機会を削減するだけでく、不正の正当化・動機を生まないような役職員の意識改革・ガバナンスの徹底も必要。不正手段の知識は、不正兆候の発見・防止に役立つ。

ISACA Tokyo Chapter

さいごに

■ ガイドラインは網羅的なToBe。あなたの企業・組織にとって優先課題は？

是非、トップダウンで体制・対策の整備を。手薄な課題、優先すべき対策を見極め順次実施しましょう。

情報漏えいに関する内部不正対策でも、個人情報保護と営業秘密保護では意識に差が生じがち。

対策できたつもりでも、「重要情報の特定・格付け管理」は永く継続する課題となってしまうことも。

■ 内部不正対策は「北風と太陽」の両立作戦の側面あり

アクセスログ管理の徹底ひとつでも、二つの側面を持ちます。

北風　悪いことをすると必ずばれる、という抑止力期待

太陽　善意の従業員の皆さんを守るために対策する、というPOSITIVEな（対策実施の）動機づけ

■ 経営層の対策も分け隔てなく…

近年、経営層の中途退職による内部不正事例も目立ちますので抜かりなく。