KPMG

不正行為者に関するグローバル調査

社内の脅威 ― 企業における不正行為者の人物像

KPMG. Make the Difference.

目次

はじめに

企業不正は「ホワイトカラー犯罪」とも呼ばれ、損害を被る企業は後を絶たず、世界中のメディアの誌面を賑わせています。我々は、KPMGフォレンジックサービス部門での業務を通じ、企業不正が企業や従業員、そして社会全体に及ぼす深刻な影響を目の当たりにしてきました。不正対策で肝要なことは、いかに不正に対する守りを固め、不正を防止し、また早期に発見するかに尽きます。

こうした不正対策の重要課題を掘り下げるため、KPMGは広範なグローバル調査を実施し、不正行為者の主な人物像と手口、そして不正行為者が付け込む企業の弱点を明らかにしました。

企業不正にはさまざまな要因が複雑に絡み合っているため、守りを固めるには、強固な内部統制の導入、倫理的な文化の醸成、検知メカニズムやテクノロジーの強化、協力体制と透明性の強化、テクノロジーの変化への対応など、積極的な対策が必要です。KPMGは、クライアントがこれらの対策に取り組み、企業不正に効果的に対抗するための支援を提供しています。

この調査結果が、安全かつ信頼性の高い企業環境の構築に少しでも貢献できれば幸いです。

Alexander Geschonneck
Global Forensic Leader
KPMG in Germany

Hiroyuki Nishijima
ASPAC Forensic Leader
KPMG in Japan

不正行為者の人物像と、その手口は？
企業が不正に対する守りを固めるには？

KPMGグローバル不正調査：結果の要点

不正行為者は主に男性、**36～55歳、評価が高く**勤務年数が長い

最もよく見られたのは資産の不正流用、特に**横領**と**調達不正**

不正は事業部門、財務部門、CEO室、調達部門など**さまざまな部門で発生**

不正の最大の原因は**統制の不備と見られる**

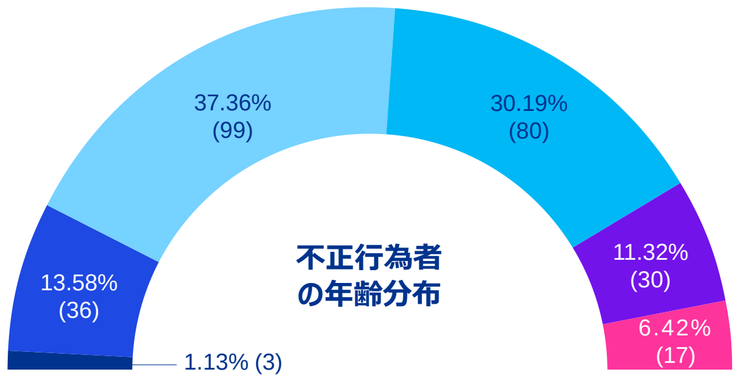
検知のきっかけとして最も多いのは**内部通報や非公式な情報源**からの情報提供

不正の**55%**は共謀によるもので、**2～5人が絡む**ことが多い

不正行為者の人物像

「不正行為者は、周囲から敬意を持たれており、勤続年数が長く、誠実そうに見え、周囲の人物が疑いもしないような人物であることが多いです。そのため監視と強固な内部統制が重要になります。」

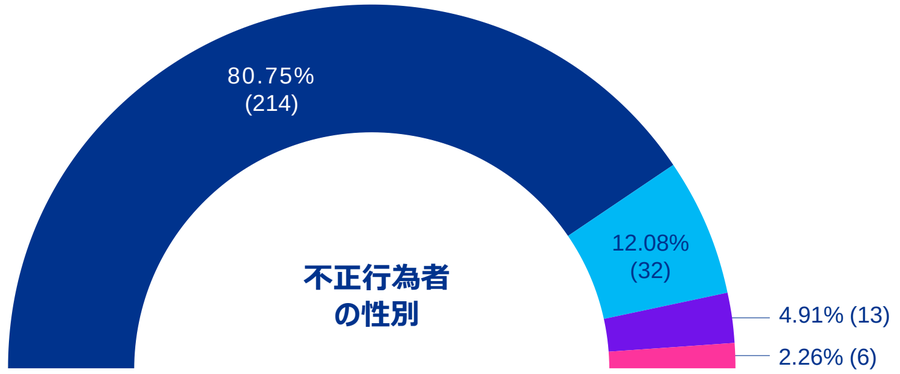
不正行為者は当然それぞれが異なる個性を持つものの、本調査では共通する特徴がいくつか見られました。本調査で導き出された典型的な不正行為者像は、36～55歳の男性で、被害企業で比較的長く（6年以上）勤務している人物です。社内での地位は、役員が31%、管理職が30%、一般従業員が24%と、ほぼ均等に分布しており、半数をやや上回る51%が多国籍・グローバル企業に勤務しています。
明らかに不審な特徴はこれといって見られません。彼らは概して「周囲の尊敬を受け」、「社交的」、「親切」とされ、「中程度～高い評価」を受けていますが、自己優越感を持っていることが特徴です。雇用主に対して明らかに不満を持っている様子がないのは興味深い点です。



出典：不正行為者に関するグローバル調査（2025年）

18～25歳
26～35歳
36～45歳
46～55歳
56歳以上
不明

不正行為者の年齢層の内訳。年齢と不正行為の関係可能性を整理。

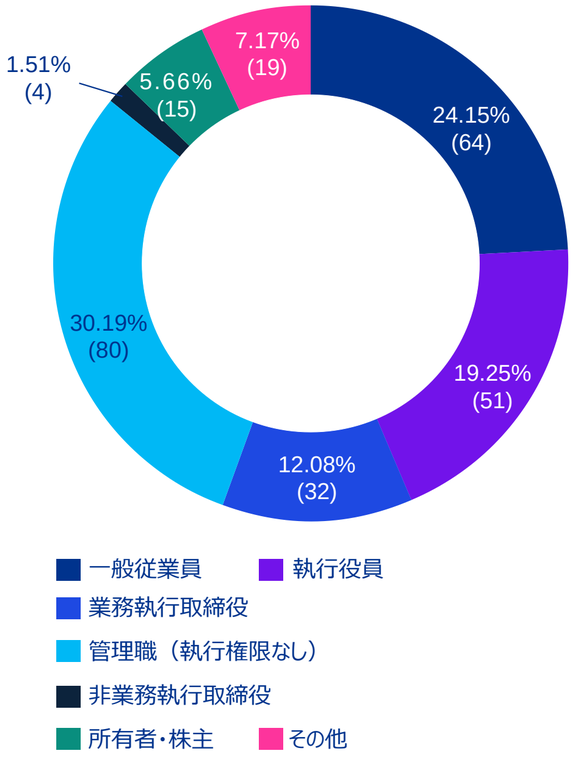


出典：不正行為者に関するグローバル調査（2025年）

男性
女性
その他
不明

不正行為者が男女どちらに多い傾向があるか把握のために、不正行為者の性別分布を分析。

不正行為者が私生活や仕事で困難を抱えている様子は見られませんでした。中には、損失を隠蔽する、または業務目標を達成することで社内評価を維持・向上するため、あるいは私生活の経済的な苦境を脱するために不正を働いた例もありますが、少数です。不正の背景にある最大の動機は、単純な金銭的利益、貪欲さ、次いで出来心でした。

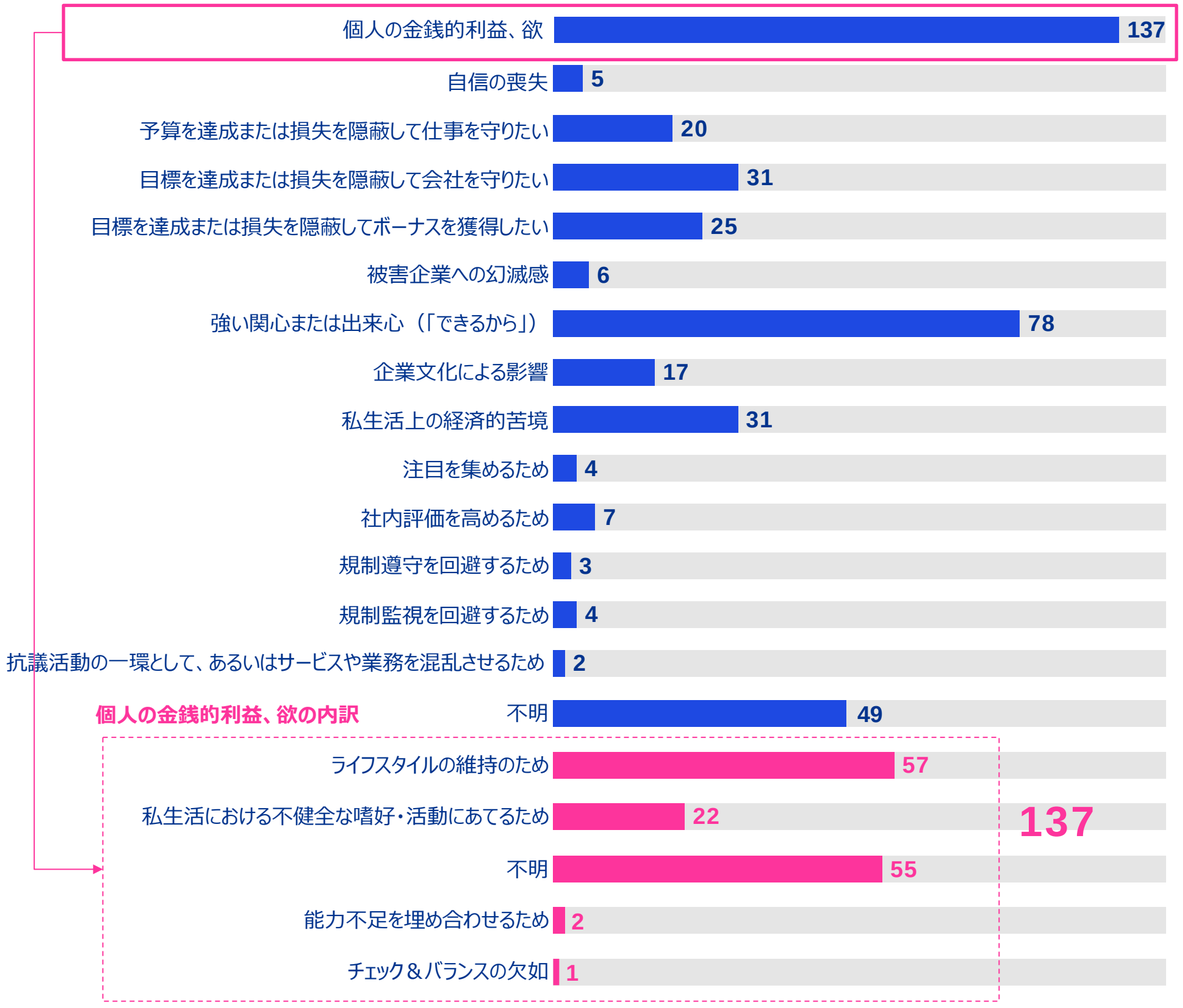


出典：不正行為者に関するグローバル調査（2025年）

被害企業における不正行為者の役職・地位の内訳。不正が下位・中位職者によるものか、上位職者（幹部）によるものかを示した。

不正行為者の動機

不正行為者の最大の動機は何でしたか？



出典：不正行為者に関するグローバル調査（2025年）

不正行為の根底にある動機の内訳（個人的な金銭的利益、業績目標達成のプレッシャー、その他の個人的または業務上の理由）

勤続年数

3.40%(9)

18.49% (49)

13.21% (35)

64.91% (172)

- 1年未満
- 1～4年
- 4～6年
- 6年～

出典：不正行為者に関するグローバル調査（2025年）

不正行為者が被害企業に在籍していた期間の内訳。在籍期間の傾向と、不正行為への潜在的影響を把握するために整理。

不正の特徴と発生場所

「資産の不正流用は今でも最も多い不正であり、厳格な資産管理や調達管理が必要であることは明らかです。」

調査対象となった不正事例の取引毎の金額の約7割は、20万米ドル（約28百万円）未満でした。その他20万～100万米ドル（約28百万～140百万円）及び100万～500万米ドル（約140百万～700百万円）が それぞれ約1割、残りが500万米ドル（約7億円）超です。

国境を超える不正はわずか13%ですが、被害額が高額となる傾向があり、およそ半数の事例で500万米ドルを超えています。
本調査の対象となった事例としては資産の不正流用が最も多く、全事例の52%を占め、次いで書類の偽造（29%）が続きました。書類の偽造は不正流用の手段でもあります。他には資産の窃盗（24%）などがありました。

資産の不正流用の半数（50%）は横領（信頼される立場にある者が、自らの管理下にある資産を個人的利益のために不正利用する）でした。38%は調達不正で、ベンダーと共謀して水増し価格を設定させ、その結果ベンダーが余分に得た収益の一部を着服するなどの手口があります。

国境を超える不正はわずか**13%** だが、

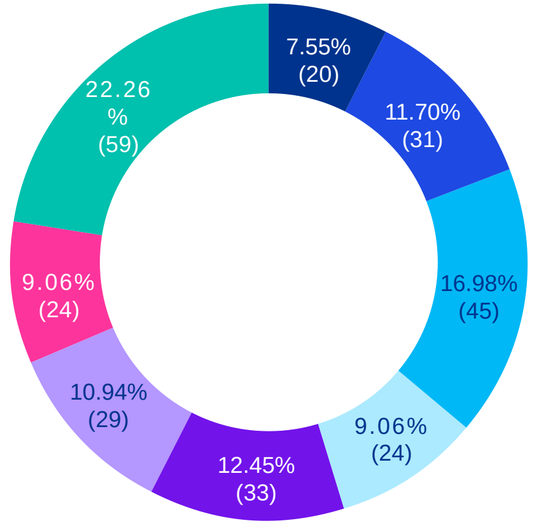
被害額が高額となる傾向があり、およそ半数の事例で

500万米ドル（約7億円）

を超えた。

ドルからの円換算を1ドル＝140円で行っている。

不正による被害者の財務損失額

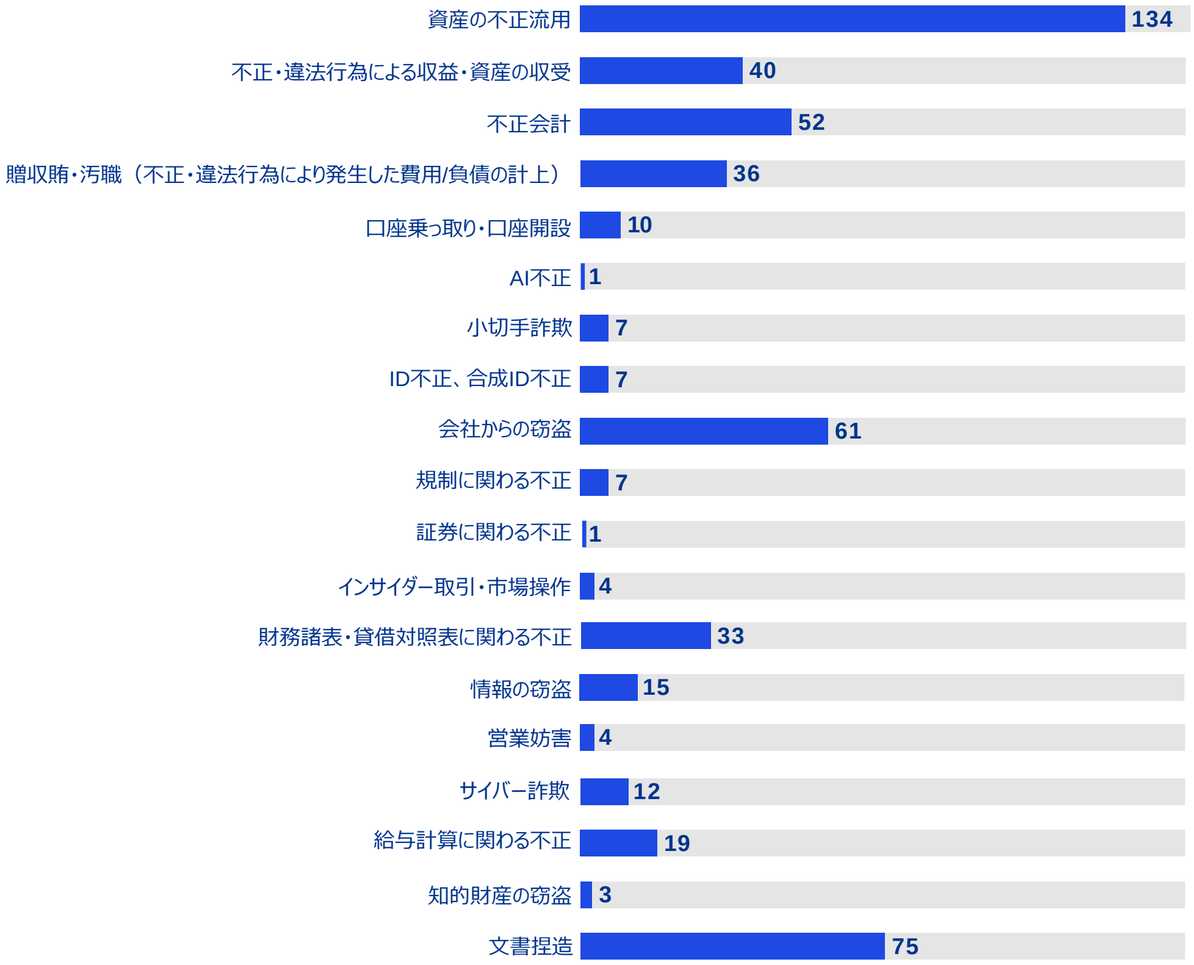


- ～1,000ドル
- 1,001ドル～50,000ドル
- 50,001ドル～200,000ドル
- 200,001ドル～500,000ドル
- 5000,001ドル～1,000,000ドル
- 1,000,001ドル～2,000,000ドル
- 2,000,001ドル～5,000,000ドル
- 5,000,001ドル～

出典：不正行為者に関するグローバル調査（2025年）

被害企業が被った経済的損失を定量化して詳細を明らかにし、不正の財務影響の重大さを評価。

不正の内容は？

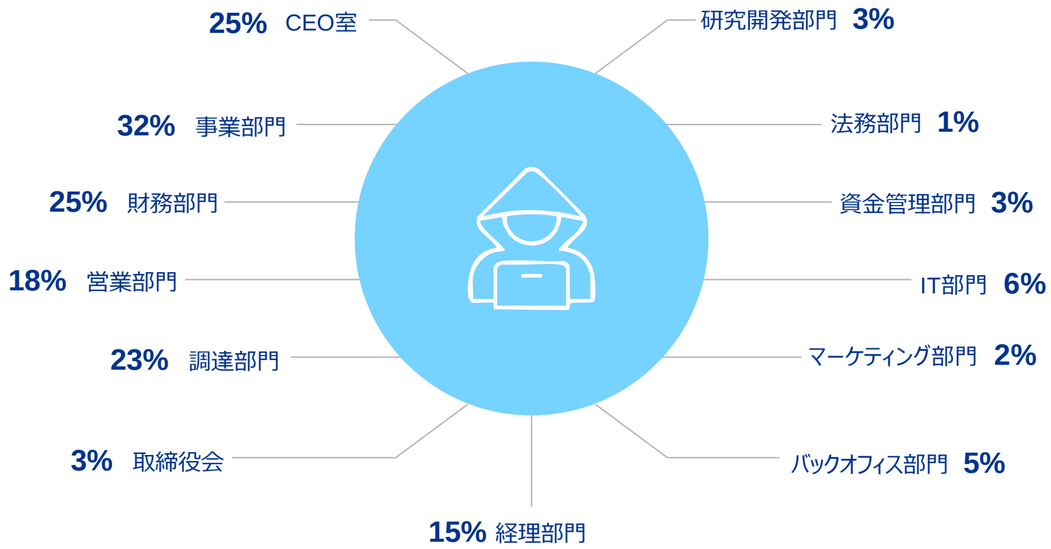


出典：不正行為者に関するグローバル調査（2025年）

不正行為の具体的な性質を理解するため、不正行為の内容を資産の流用、贈収賄、サイバー攻撃などに詳細に分類した。

不正事例の5件に1件（20%）は不正会計でした。そのうち過半数（56%）が不適切な収益認識で、財務諸表上の利益を多く見せるため、収益の架空計上や前倒し計上が行われていました。

不正はさまざまな部門で発生し、特に事業部門（32%）、財務部門（25%）、CEO室（25%）、調達部門（23%）に目立ちます。資産の不正流用の34%はCEO室で発生していますが、必ずしもCEOや経営層が不正行為を行ったわけではありません。
CEO室は、組織自体の権限が強いため、不正の機会が多くある恐れがあります。

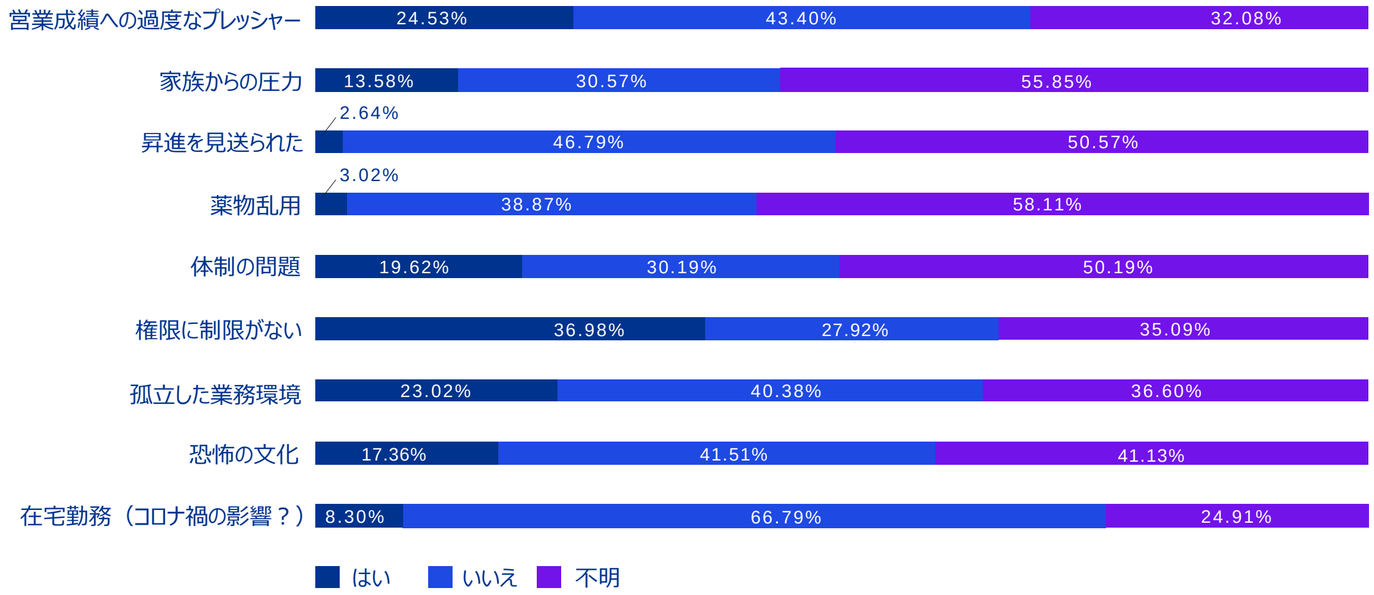


出典：不正行為者に関するグローバル調査（2025年）

企業内で不正が発生した部署の概要。不正が発生しやすい部署を具体的に示した。

組織の脆弱性を検出する

「内部統制が不十分な場合、不正行為が発生しやすくなります。リスクを軽減するには、まずは内部統制システムを強化すべきです。」



出典：不正行為者に関するグローバル調査（2025年）

過度なプレッシャーをよしとする職場環境、家族からの圧力、薬物乱用、恐怖の文化など、不正行為者が不正を行う動機となった可能性のあるさまざまな環境要因を調査した。

内部統制は、不正の防止・検知の重要な鍵を握ります。調査対象の事例のうち、内部統制の不備が主な原因とされたのは4件中3件（76%）に上ります。前回の不正行為者に関する調査において内部統制の不備が原因とされたのは61%であったため、著しい増加です。
実際に被害企業の51%では、不正発生時点で不正防止に関する内部統制が整備されていませんでした。内部統制が整備されている企業では、行動規範（81%）、内部監査（64%）、内部通報制度（60%）が防止策としてよく利用されています。

効果的な防御策が不足していることを考えれば、情報提供（正式な内部通報ホットラインまたは匿名の非公式な情報源）が不正検知のきっかけの1位（45%）となったのも当然といえます。この結果が示すのは、「声を上げる」ことのできる倫理的な企業文化を奨励し、情報提供に対し迅速かつ的確に対応するのが重要だということです。とはいえ、あまりに多くの不正が予防対策をすり抜けており、早期発見・被害最小化のためには内部監視体制の強化が必要です。

「権限に制限がない」は不正行為の環境要因の１位でした。これに該当する事例の半数（49%）では、被害金額が100万米ドルを上回りました。被害金額が500万米ドル超の全事例のうち、不正行為者の権限に制限がなかった割合は29%であったのに対し、100万～200万米ドルの事例では9%、200万～500万米ドルの事例では11%でした。被害金額が多いほど、不正行為者の権限に制限がなかった可能性が高いことを示唆しています。

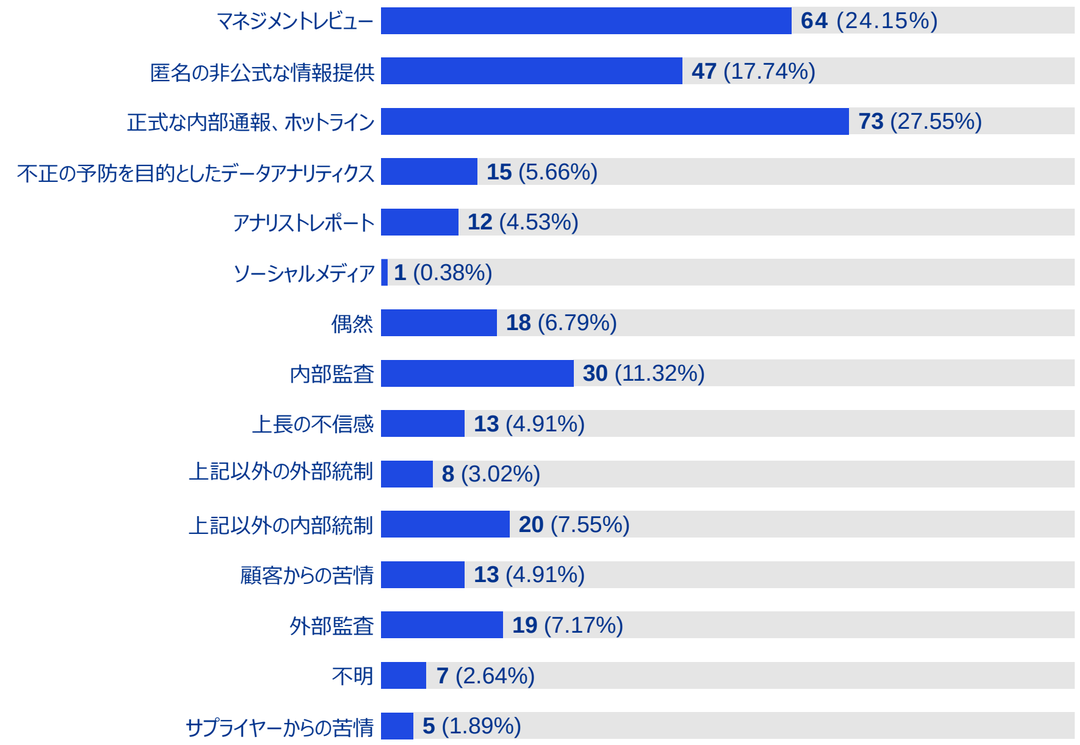
一方、権限が制限されていた不正行為者のうち、100万米ドルを超える被害をもたらしたのは少数（12%）でした。
上記の調査結果は、内部統制システムにおけるチェック＆バランスの不十分さと、監視の強化・権限範囲の明確化の必要性を示しています。いかなる上級職者や高い影響力を持つ人物に対しても、権限の範囲と管理体制を正式に定め、常に適用すべきです。

リモートワークへの移行による影響はわずか

「ハイブリッドワーク、リモートワークは新たな課題をもたらしましたが、不正の大きな増加の要因とはなっていません。とはいえ、テクノロジーを悪用した不正行為が急激に進化していることから、新たな働き方に合わせた管理体制を整備すべきです。」

不正やその調査は数年にわたり継続する可能性があることから、本調査ではコロナ禍で一気に拡大したリモートワークについても評価しました。調査対象の事例のうち、リモートワークが「発生に寄与した」のはわずか5%であり、リモートワークにより管理体制や監視が「多少なりとも損なわれた」のも9%のみでした。一方で、不正が起きてしまった企業において偽造された電子文書を十分に精査しなかった、リモートで稼働を装う架空の業務委託先が存在した、などの事実が明らかになっており、こうした教訓から学べる点もあります。

不正の検知につながったのは？



出典：不正行為者に関するグローバル調査（2025年）

匿名の通報、内部監査、外部監査など、不正検知の手段や経路の概要を示した。

権限に制限がない

36.98%(98)

27.92%(74)

35.09%(93)

■ はい
■ いいえ
■ 不明

企業内で不正行為者の権限に制限がなかったことが不正行為の実行可能性に寄与したかどうかを調査した。権限を牽制しないことのリスクを示唆している。

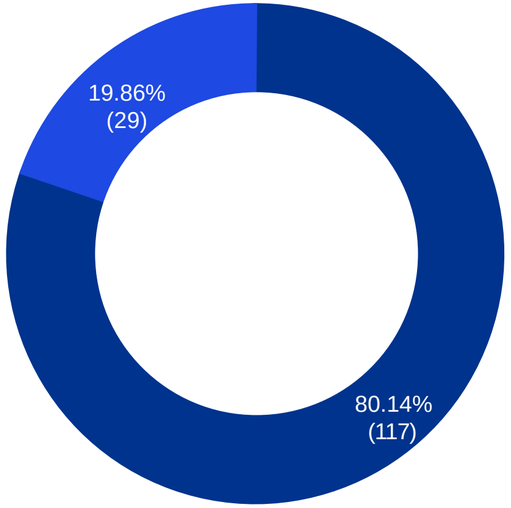
協力者を理解する

「不正行為は共謀して行われることが多いため、企業は透明性の向上を図り、特にハイリスクのサードパーティを中心にやりとりを綿密に監視すべきです。」

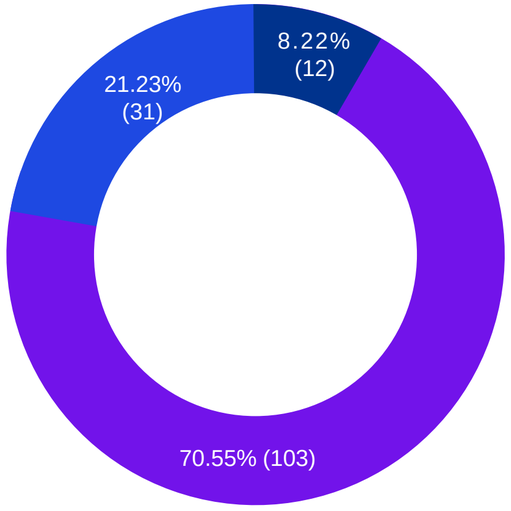
共謀による不正行為は55%と、前回の調査から7%低下しています。その理由としては、テクノロジーの進化により一人でも不正行為を働きやすくなったためである可能性があります。共謀による不正は多国籍企業に多く見られました。組織の規模が大きいため、同じ企みを持つ人物を比較的見つけやすいためと考えられます。共謀事例において、首謀者は外部の人物ではなく従業員でした。

共謀事例の多く（71%）は、2～5人の協力者と共に行われました。ほとんどの場合、協力者の一部または全員が社内の従業員であり、39%は社内の人間のみによる行為でした。首謀者のほとんどは男性ですが、共謀による不正事例の約半数（52%）には女性が関与していました。

協力者を特定する上で有効な手段は、メールの調査、不正行為者への聞き取り調査における証言、財務記録の分析でした。

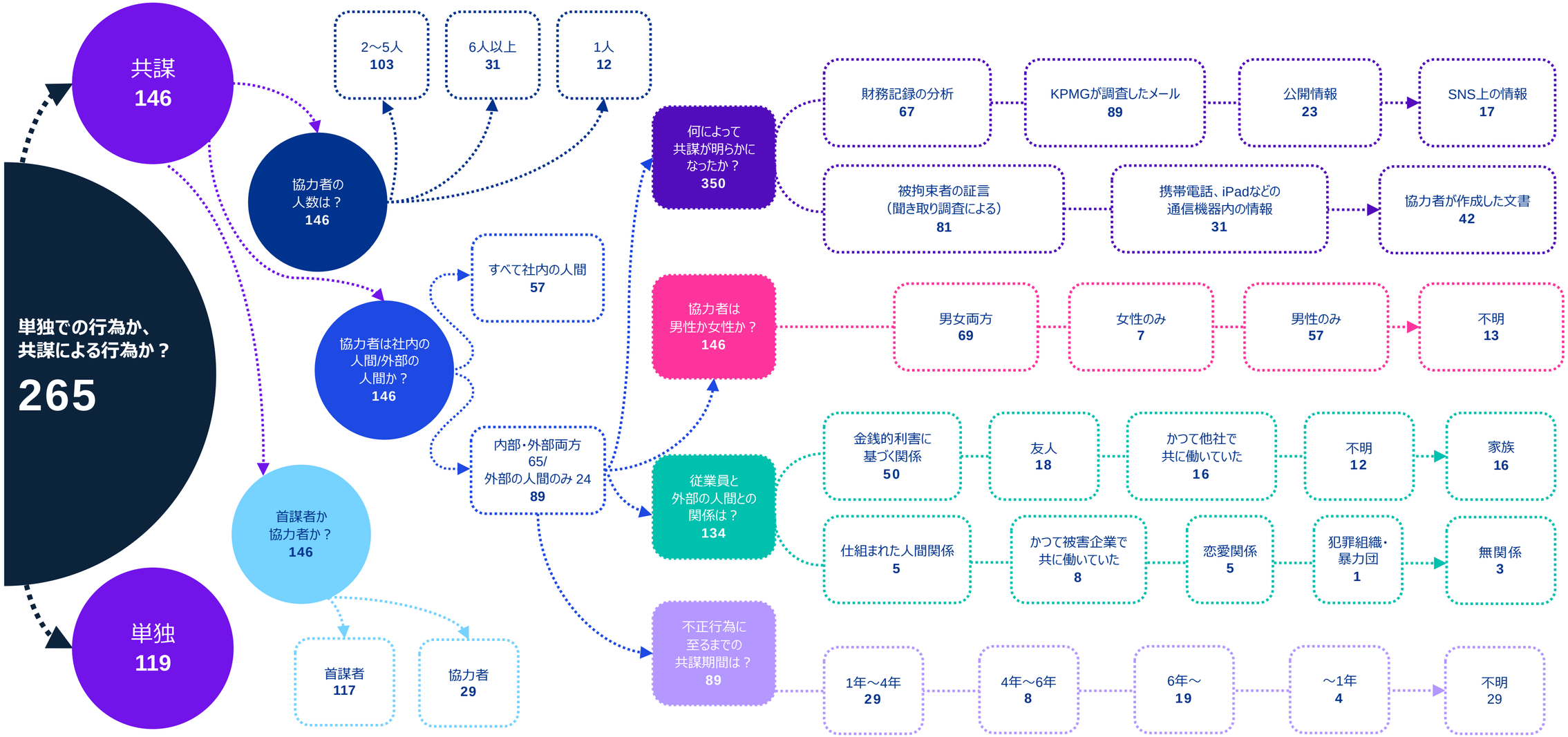


共謀して不正を行った者が、首謀者（主な不正行為者）であったか、または協力者（補佐役または仲介役）であったかを調査し、共謀の特徴を明らかにした。



協力者が1人から6人以上に及ぶ事例まで、不正に関与した人数を幅広く検証し、不正の規模に関する示唆とした。

出典：不正行為者に関するグローバル調査（2025年）



出典：不正行為者に関するグローバル調査（2025年）

不正行為者が他者とどのように共謀したか、各々の役割（首謀者か協力者か）、協力者の人数、関係性（社内か社外か）を詳細に分析した。

サイバー攻撃

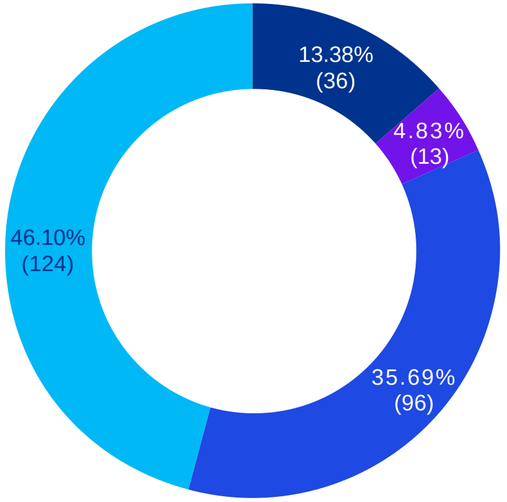
「不正においてAIと暗号通貨の存在感が強まっており、脅威の進化が浮き彫りになっています。こうしたリスクと戦うには、継続的な対応と監視が重要です。」

本調査の対象となった不正事例の一部（5%）には、「サイバー攻撃」と呼ばれるフィッシング、CEOを騙った不正、ビジネスメール詐欺、ハッキング、マルウェア、ランサムウェアなども含まれました。
これらのサイバー攻撃は、個人情報の取得、サービスの混乱、恐喝、個人情報の窃盗などを目的として行われたものでした。 不正行為者グループの主なメンバーがハッカーであったのは想像に難くありません。人工知能（AI）は、今後サイバー攻撃において存在感を増すとされ、特に取引承認権限を持つ人物になりすます「ディープフェイク」の悪用が拡大すると予想されます。
AIは新しい技術のため、本調査の対象となった事例でAIが利用されたのはごく一部で、暗号通貨についても同様の状況です。しかしKPMGは、今後この状況は変化すると見ています。サイバー攻撃は、ほかの不正と比較して、サイバー攻撃に特化したデータアナリティクスやマネジメントレビュー、その他の内部統制手段によって検知されることが多い傾向がありました。これは、サイバーリスクに対する内部統制手段が一定の効果を発揮している可能性があること、また企業の従業員がサイバー攻撃の脅威を認識して積極的に低減に努めていることを示唆しています。それと同時に、管理体制が不十分なために多くのサイバー攻撃が見逃されている可能性もあります。

テクノロジーはまだ不正の主要な手段ではない

「テクノロジーが進展する一方、多くの不正行為はいまだに従来の手段を用いて行われています。これは、テクノロジーは不正の検知には役立つものの、基本的な管理体制がこれからも欠かせないことを示しています。」

私たちの身の回りにはスマートフォン、ノートパソコン、アプリがあふれているにも関わらず、本調査の対象となった不正事例においては、テクノロジーは重要な役割を果たしてはいないようです。ほぼ半数（46%）の事例ではテクノロジーが一切利用されていません。35%の事例では「ある程度」利用されたものの、テクノロジーを利用せずとも実行できた可能性があります。テクノロジーを利用した不正の件数は、KPMGの前回の不正行為者に関する調査から増加していません。その理由は定かではありませんが、テクノロジーを利用した手段は、人の手による従来の手段よりも追跡しやすいことに加え、企業が防御策を強化しやすいためかもしれません。



- テクノロジーは不正の実行に不可欠だった
- テクノロジーは不正の実行に大きく寄与した
- 不正はテクノロジーを利用せずとも実行できた可能性がある
- 不正はテクノロジーを一切利用せずに実行された

出典： 不正行為者に関するグローバル調査（2025年）

デジタルプラットフォームやAIの利用、サイバーセキュリティの欠陥を突いた攻撃など、テクノロジーが不正の実行にどの程度寄与したかを調査した。

重要なポイント

本調査の結果から、以下のような行動を検討することで、ホワイトカラー犯罪に対する脆弱性の改善につながることが明らかになりました。

1

内部統制の強化

- 定期的な監査や監視システムなど、強固な内部統制を導入・実現する
- 個人の地位や評判に捉われず、権限に明確な制限を設けて常に監視する

2

倫理的な文化の促進

- 「声を上げる」文化を奨励し、従業員が正式な内部通報窓口を通じて不審な行動を安心して報告できるようにする
- 倫理的行動や不正に関する意識を高めるため、全従業員に対し定期研修を実施する

3

検知機能の強化

- 高度なデータアナリティクスおよび不正検知テクノロジーを活用して、不審な行動を事前に発見し調査する
- 新たな脅威と脆弱性に対応するため、不正検知・防止策を定期的に見直し更新する

4

部門間協力と透明性の促進

- 部門間の協力と透明性を促進し、共謀を起こしにくくする
- リスクの高いポジションにある従業員に対し綿密な身辺調査を実施し、継続的に監視する

5

取引先の把握

- 取引先を理解するため、サードパーティに対しデューデリジェンスを実施する
- ハイリスク、支払額が高い、あるいは支払額の一時的な急増が見られたサードパーティを定期的に調査し、実在性の確認に加え、業務上の根拠や支払額の正当性の評価を行う

6

テクノロジーの進化への対応

- 最新の技術革新と不正への潜在的影響について継続的に情報収集する
- サイバー攻撃の脅威を認識し対応するために、サイバーセキュリティ対策への投資および従業員教育を行う

KPMGの支援内容

昨今、企業はますます不正の被害を受けやすい状況にあり、企業のコンプライアンスへの取り組みに対する規制当局・利害関係者の期待も高まっています。業務への支障と損害を最小限に抑え、利益を守るためには、不正・不祥事の予防、検知、対処を迅速かつ決断力を持って行うことが不可欠です。不正のリスク、内部統制上の脆弱性に加え、不正対策方針（監視、特定、報告、上申、対応）を明確にしなくてはなりません。また不正行為による被害を受けた際は、徹底的に調査し、不正行為者を的確に特定・追及することが極めて重要です。

KPMGの専門家は、グローバルなネットワーク、テクノロジー、業界や各地域に関する知見、さらに株主、取締役会、監査人、規制当局の懸念事項への対応などの豊富な経験を活かし、世界最大規模のあらゆる企業にサービスを提供しています。規制当局の期待や、最新の動向に関する理解のもと、有益な調査結果を導き出す支援をします。

KPMGは以下のようなサービスを提供しています。

- **従業員の不正行為全般にわたる内部調査**
- **不正会計・収益操作、横領、資産の不正流用の調査**
- **規制、贈収賄、汚職に関する懸念に関する支援**
- **フォレンジックテクノロジーサービス（証拠収集、Eディスカバリ、フォレンジックデータアナリティクスなど）**
- **リスク・脆弱性評価**
- **金融犯罪対策、制裁、マネー・ロンダリング防止に関するコンプライアンス関連支援**
- **倫理およびコンプライアンスに関する助言**
- **サードパーティリスク管理**

本調査について

本調査では、世界のKPMGメンバーファームのフォレンジック専門家に対してアンケート調査を行い、不正行為者の詳細を尋ねました。アンケートに協力したのは不正の被害を受けた企業の依頼に基づいて不正を調査した専門家で、各不正行為者について詳細な回答が提供されました。これらの不正調査では、不正行為者に対する聞き取り調査が多く実施されたため、不正行為者および不正行為の内容の詳細が明らかとなっています。
本報告書は、過去5年間にKPMGメンバーファームが調査した256件の不正事例の分析結果をまとめたものです。2人以上の不正行為者が関与した事例があるため、回答内容に基づけば、669人以上の不正行為者が対象となっています。

お問合わせ先

Alexander Geschonneck
Partner, Global Forensic Leader KPMG in Germany
M +49 174 320 1475
ageschonneck@kpmg.com

Hiroyuki Nishijima
Partner, ASPAC Forensic Leader
KPMG in Japan
M +81 8081710946
Hiroyuki.Nishijima@jp.kpmg.com

Mariko Yamada
Director,
KPMG in Japan
M +81 8087602289
Mariko.yamada@jp.kpmg.com

Asaki Kaminaga
Senior Associate
KPMG in Japan
M +81 8078575020
Asaki.kaminaga@jp.kpmg.com

本書で紹介するサービスは、公認会計士法、独立性規則および利益相反等の観点から、提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。株式会社KPMG Forensic & Risk Advisory詳しくは株式会社KPMG Forensic & Risk Advisoryまでお問い合わせください。