

PwC「グローバル経済犯罪実態調査2022」

防御を固め備えよ：


外部犯行者による

不正の増加



pwc

www.pwc.com/jp



環境、地政学、財政および社会的な要因により、リスクを取り巻く環境がこれまで以上に不安定になっており、不正やその他の経済犯罪を未然に防止することがより難しくなっている。企業は、情勢の変化に迅速に対応している一方、変化に乗り、企業の防御の隙を狙って不正を企む者が存在する。

次々と新しいデジタル技術が導入され続ける現代のビジネス環境において、十分な統制はなされているだろうか。ハイブリッドな勤務環境に伴うリスクは適切に管理されているだろうか。アフターコロナの不透明な経済を乗り切るために必要なルールやインセンティブは導入されているだろうか。そもそも、企業が今日直面している不正リスクとは何なのか。

社内規程、研修、内部統制、モニタリングを通じた長年にわたる企業の不正対策は、内部犯行者による不正を防止するには効果があった。一方、2022年度のグローバル経済犯罪実態調査では、外部犯行者による攻撃については企業の防御が脆く、新たに深刻な脅威となっている状況が浮き彫りとなった。

1

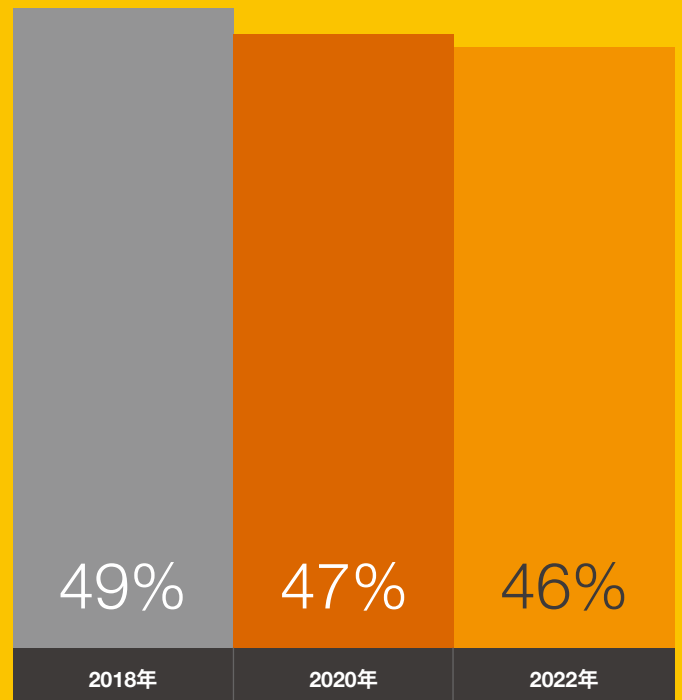


不正対策の取り組みには一定の効果あり

全体的に見ると、不正、汚職、その他経済犯罪の発生率は、2018年以降ほぼ横ばいが続いている。今回の調査では、「過去2年以内に何らかの不正や経済犯罪を経験したことがある」と回答した企業は、全体の半数弱（46%）であった。サプライチェーンの混乱、不安定な環境および国際情勢、不透明な経済、人材不足、その他さまざまなリスクが混在している昨今において、不正および経済犯罪の被害発生率が大きく上昇していないという結果は、ある意味朗報である。

一方、IT業界においてはその限りでない。IT業界が成熟するにつれ、不正検知数の増加が2020年以降顕著である。今回の調査に協力いただいたIT、メディア、通信業界の企業のうち、「何らかの不正を経験したことがある」と回答したのは約3分の2に上り、業界全体の中で最も高い割合であった。

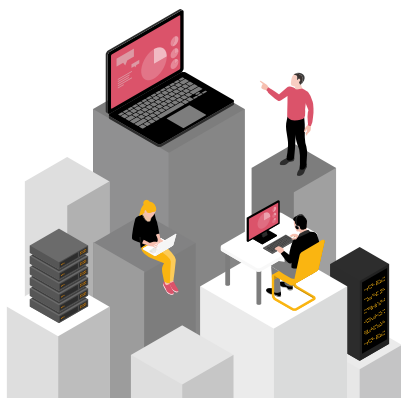
不正、汚職、その他経済犯罪を経験したことがある企業の割合





不正および経済・金融犯罪の発生率は、年々さほど変化していないものの、不正や犯罪行為が企業に与える経済的インパクトは企業規模を問わず深刻である。世界レベルでの年間売上高が100億米ドル（約1兆4,000億円¹）以上の大企業においては、52%が「過去2年以内に不正を経験したことがある」と回答し、うち約5社に1社が、「最も重大なケースが自社に与えた経済的インパクトは、一事案あたり5,000万米ドル（約70億円）以上」と回答した。また、年間売上高が1億米ドル（約140億円）未満の中小企業においては、38%が不正を経験し、うち約4社に1社が「自社に与えた経済的インパクトの累計は100万米ドル（約1億4,000万円）以上」と回答した。

発生リスクが最も高い不正は、どのようなものであろうか。企業規模を問わず、今回の調査で最も多かった不正はサイバー犯罪で、次いで顧客による不正や資産横領だった（2020年の前回調査も同様の結果）。



46%

過去2年以内に何らかの不正や経済犯罪を経験したと回答した企業の割合

¹ 1米ドル=140円で換算（以下同様）

大企業と中小企業における不正の発生割合と経済的インパクト

年間売上高が100億米ドル以上の大企業

52%

過去2年以内に不正を経験したことがある企業の割合

18%

うち、最も重大なケースが自社に与えた経済的インパクトは、一事案あたり5,000万米ドル以上と回答した企業の割合

年間売上高が1億米ドル未満の中小企業

38%

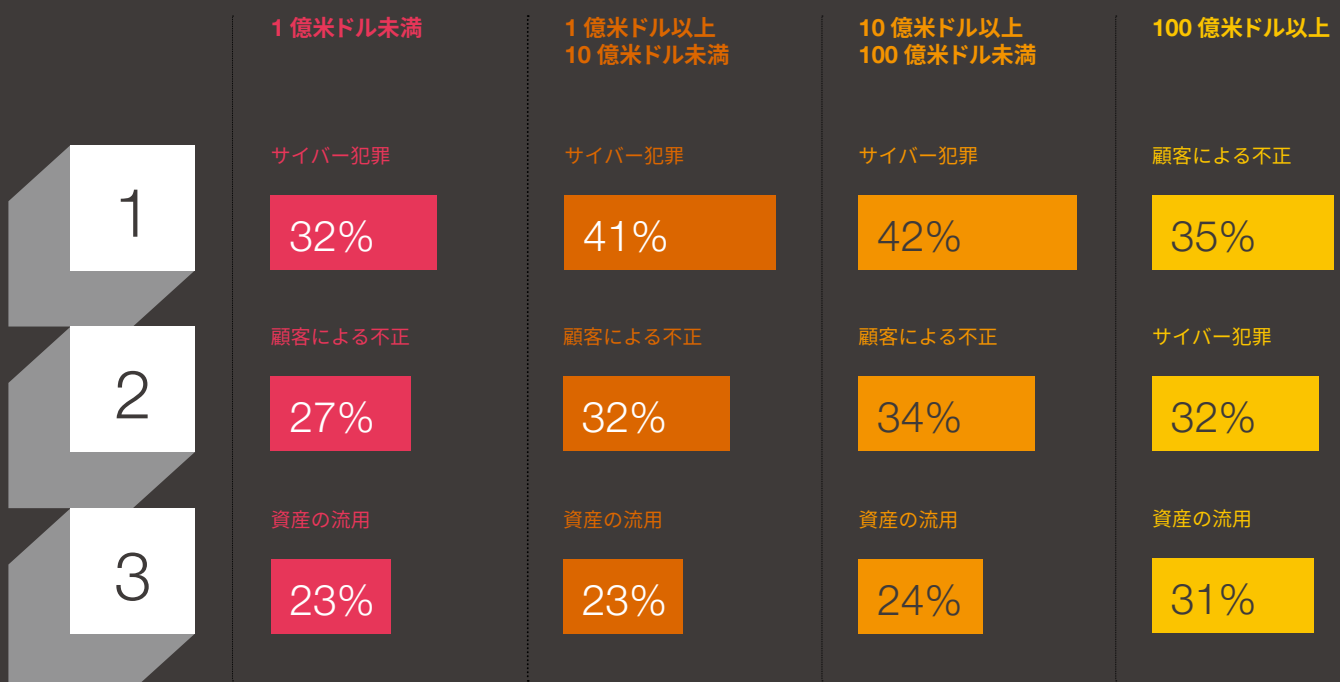
過去2年以内に不正を経験したことがある企業の割合

22%

うち、自社に与えた経済的インパクトの累計は100万米ドル以上と回答した企業の割合

企業はテクノロジーを駆使し
つつ、より強固な内部統制を
構築している

企業規模別に見た発生率の高い不正（グローバルレベルでの売上高）

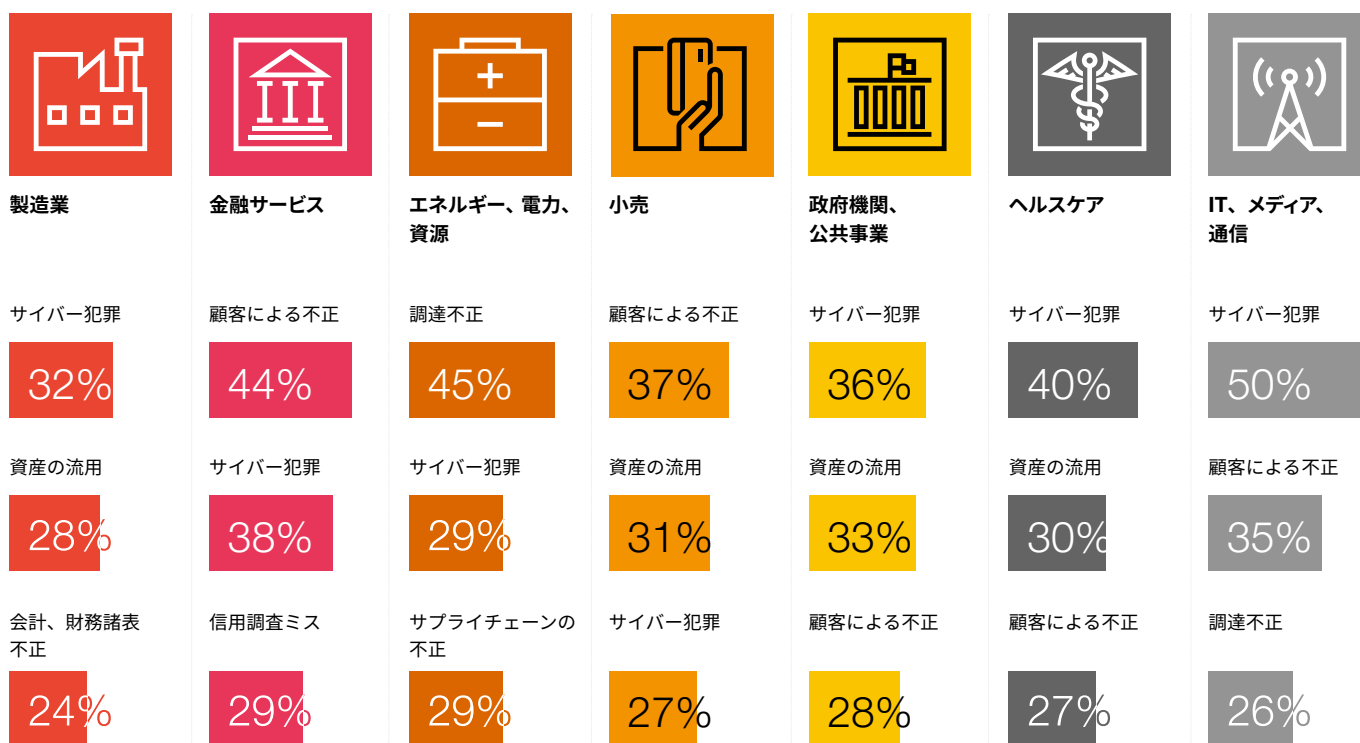




業界全体では、サイバー犯罪の被害割合が最も高かったのに対し、エネルギー、電力、資源業界においては、購買不正の被害割合が最も高かった。具体的には、エネルギー、電力、資源業界では、不正を経験したことがあると回答した企業は31%で、うち半数近くが購買不正を占めた。他の業界と比べると、デジタル・フットプリント（インターネットを使用した際に残る記録）が残る取引が少なく、また顧客との接点が少ないため、不正被害の内容が他の業界と異なるのももっともである。しかしながら、近年の動きを見ると、近い将来、サイバー攻撃はインフラ業界に対し、新たな脅威をもたらす可能性が高い。

正しい行いをしようとする従業員を後押しするため、方針や規程の策定、研修の実施などに力を入れ、組織的な変革をすることは、不正やその他の経済的犯罪に対する企業のディフェンス力を強化するのに有効である。一方、今回の調査では、不正や経済犯罪を経験した企業のうち、「最も重大なケースは、自社の内部統制システムを通じて発見された」と回答した企業が3分の2に上った（前回2020年調査時から7ポイント上昇）。このことから、近年、多くの企業が、高度なテクノロジーを導入し、より強固な内部統制や検知メカニズムの構築に力を入れていることが分かる。

業界別に見た発生率の高い不正



フォーカス

景気後退時における不正

新型コロナウイルス感染症（COVID-19）がもたらしたパンデミックは、企業のデジタルトランスフォーメーション（DX）を加速させた一方、新たな脆弱性を生み出した。「資産の流用」は、いまだに発生割合の高い不正の一つではあるが、リモートワークにより会社資産へのアクセスが制限されたことが影響したせいか、2年前の前回調査と比べると全体に占める割合は減っている。他方、リモートワークにより高まったリスクは、情報セキュリティ関連だけではない。例えば、企業機密データを狙って、在宅勤務の従業員にブラックメールを送ったり、身体的危害を加えたりするなど、従業員の安全に対するリスクが高まったという回答が見受けられた。「過去2年以内にディスインフォメーション（いわゆるフェイクニュース）などの情報操作型サイバー攻撃を経験したことがある」と回答した企業の割合は全体の15%を占め、企業はこの種の新たなリスクを周知していく必要があるだろう（[ディスインフォメーションへの対策強化については、PwCのポッドキャストをご視聴ください](#)）。

2007年から2009年に起きたリーマンショックのような過去の景気後退時には、不況を乗り越えるための貴重な教訓が生まれてきたが、パンデミックからの脱却を目指す昨今においても同様のことがいえる。不正の傾向というのは、過去の例を見ても、社会的な混乱が生じてすぐに現れるものではなく、1年半から2年ぐらいたった後に見えてくることが多い。経済規模が縮小していた時期から拡大していく転換期というのは、内部不正を検知する際において重要なタイミングといえる。

経済の移行時には、往々にして、企業が掲げる新しい目標に従業員が着いて行けず、多くの内部不正が目に見えるようになる。例えば、景気後退時におよそ達成不可能な売上目標を掲げた場合、従業員はそれを達成するために不正行為に及ぶ可能性がある。また外部犯行者も、経済の転換期における市場の混乱を利用し、特に消費者になりすましたスキームを用いてチャンスを狙う。さらに不況下においては、組織的な犯罪グループが、リストラなどで急に職を失った人々を中心に、より容易にメンバーを集めることができる。これらを踏まえると、景気が後退している局面では、企業はこれまであまり注目していなかった不正リスクに特に注意する必要があるといえる。

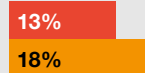
コロナ禍での混乱がもたらした経済犯罪

コロナ禍の影響で、新しいタイプの不正の発生や、リスクの増加を経験した企業の割合

不適切行為のリスク



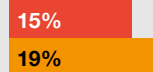
法的リスク



サイバー犯罪



インサイダー取引



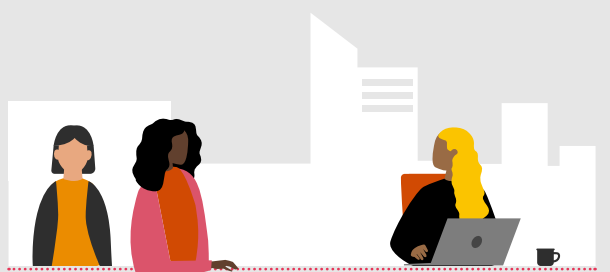
プラットフォームリスク



■ 新しいタイプの不正が発生した分野

■ リスクが高まった分野

出所：PwC「グローバル経済犯罪実態調査2022」



70%

不正を経験した企業のうち、コロナ禍の影響で新しいタイプの不正を経験した企業の割合

2



企業の防衛線が外部攻撃によって脅かされている

今回の調査では、これまで見られなかった新たな脅威の存在が見えてきた。すなわち、自社のコントロールや管理が行き届かない外部の人間による不正や経済犯罪が急増しており、手口も巧妙化してきている。

不正を経験した企業の70%近くが、最も重大なケースは、外部犯行者、または内部犯行者と外部犯行者との共謀によるものであったと回答している。外部からの攻撃の場合、社内規程の整備、研修、チェック体制の実施といった従来の内部不正向けの防止対策では太刀打ちできない。

外部攻撃の中で最も多いハッカーや組織的犯罪グループによる不正のインパクトは、この2年間で大幅に増加した。今回の調査では、外部犯行者による不正を経験した企業のうち、ハッカーによるものが約3分の1、組織的犯罪グループによるものが約28%を占め、いずれも2020年の前回調査より増加している。

企業が経験した最も重大なケースの犯行者



外部犯行者

43%

(2020年41%)



外部犯行者による不正を経験したことがある企業は、欧州企業の割合(56%)がそれ以外の地域の企業と比べて著しく高い。



内部犯行者

31%

(2020年38%)



不適切行為の重大ケースは、内部犯行者によるもの(35%)がサイバー攻撃(16%)に比べて著しく高い。



内部犯行者と外部犯行者の共謀

26%

(2020年21%)



内部犯行者と外部犯行者との共謀による不正を経験したことがある企業は、中国および香港企業の割合(50%)が、それ以外の地域の企業と比べて著しく高い。



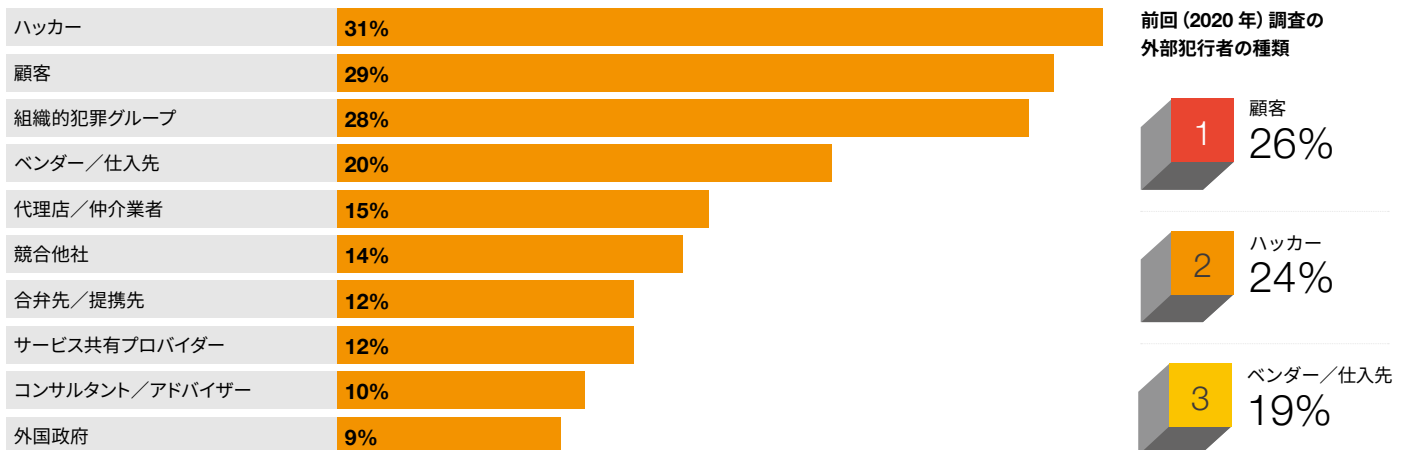
組織的犯罪グループは、明確な目標、動機、報酬構造を備え、より専門化かつ洗練されてきている。組織的犯罪グループは、企業の脆弱性に目を付け、攻撃のチャンスを常に狙っている。こうした外部からの不正は、企業側のコントロールや管理が及ばないため、内部不正に対する防止策とは異なる。

いくつかの要因が外部犯行者による不正の増加に寄与していると考えられる。近年増加しているデータ侵害の増加傾向は、今後間違いなく続き、顧客の個人情報を守る責務を負う企業にとっては、より一層強化した保護が求められ、負担が増えていくであろう。また、かかる傾向は、これまでに企業が外部攻撃に備えノウハウとして蓄積してきた認証戦略にも影響が出てくるであろう。

不正の実行者側も、他の実行者と手を組むことで、攻撃頻度を増やし、また不正手段の洗練化を図っている。チャットルーム、ダークウェブや仮想通貨の普及により、ハッキング、虚偽IDの作成、侵入手口の考案など、サイバー犯罪に関するあらゆる分野のスペシャリストが繋がり、協力し、やりとりができるようになっている（[ランサムウェアによる攻撃の増加については、PwCのポッドキャストをご視聴ください](#)）。

また、近年では、犯罪とは縁のなかった一般の市民が不正実行者のグループに加わる例が増えてきている。こうした傾向は、社会および経済的に貧しい国において特に顕著であり、経済的機会に恵まれない人が、不正行為への関与を正当化する理由となっている。

外部犯行者の種類



3



新しい攻撃先となる デジタル・プラットフォーム

過去2年以内に不正を経験した企業のうち、「顧客信用調査、ディスインフォメーション、マネーロンダリング、テロ資金供与、輸出禁止措置に関する不正など何らかのかたちで、自社が利用するデジタル・プラットフォームに関連する不正を経験したことがある」と回答した企業が40%に上った。ソーシャルメディア、オンラインショッピング、eコマース（例えばライドシェアや宿泊予約）などのデジタル・プラットフォームの普及に伴い、多くの企業がまだ認識していない無数の不正や経済犯罪リスクに直面しつつある。

デジタル・プラットフォームを発端とする不正のリスクは、ドミノ倒しのようなもので、1カ所に被害が及ぶと組織全体に影響が広がりがちである。したがって、デジタル・プラットフォームを狙った不正を防止するためには、社内の各部署が連携して、課題解決のマインドセットおよび風土を作り上げ、組織全体で横断的に取り組んでいく必要がある。

フォーカス

新たに台頭しつつある脅威

新たに台頭しつつある不正リスクは、今後数年間でより深刻なインパクトを引き起こす可能性がある。今回の調査でそれらの発生割合が低かったらといって安心はできず、近い将来、被害の範囲が急拡大する可能性がある。例えば、今回の調査で、「過去2年以内に輸出規制取引に関連する不正を経験したことがある」と回答した企業はわずか6%であったが、グローバルレベルでの制裁が近年例を見ないほど厳しくなっていることに伴い、今後2年間に変化が起こる可能性は高い。

顕在化しつつある不正リスクに対処する上で陥りがちな問題は、見えている部分のみに注意を払い、見えていない部分に意識が及ばないことである。潜在的に最も懸念される不正リスクは何であろうか。少なくとも以下の2点について留意する必要があるだろう。

ESG開示情報の虚偽記載

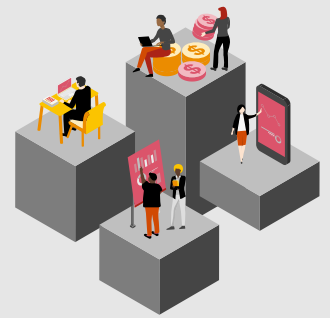
信頼度は、企業価値を判断する上で非常に重要な要素となってきた。PwCが実施した第25回世界CEO意識調査では、企業の信頼度の高さと変革力の相関性について取り上げた。ただ、信頼とは脆いものである。透明性が欠如すると（実際に欠如している場合はもちろん、そうでなくても欠如していると思われる場合も）、企業のレピュテーションおよびその根底にある信頼をも大いに傷つけてしまう可能性がある。昨今、ステークホルダーにとって、企業のESG（環境、社会、ガバナンス）に対する責任の重要性が増しており、正確な情報をESG報告書に開示することは必須義務である。過去2年以内に不正を経験した企業のうち、「ESG開示情報に関する不正を経験したことがある」と回答したのはわずか8%に過ぎなかったが、今後、偽りのESG情報を記載しようとする動機が増え、それと同時に、被害も大きくなっていくであろう。

サプライチェーン不正

今回の調査に参加した企業のうち、8社に1社が、「コロナ禍の混乱が要因で、サプライチェーンにおける不正を新たに経験した」と回答した。また、5社に1社が、「サプライチェーンにおける不正リスクが増加したと感じている」と回答した。自社のサプライチェーンにおける不正行為やリスクを認識している企業は少ないように見受けられ、多くの企業は気付いていないところでリスクに晒されている可能性がある。

6%

過去2年以内に
輸出禁輸措置に
関する不正を経験
した企業の割合



8%

過去2年以内に不正を
経験した企業のうち、
ESG開示情報の不正
を経験した企業の割合



8社に1社

コロナ禍の混乱が要因の
サプライチェーン不正を経験した
企業の割合



防衛線を強化する際のポイント

今回の調査回答を見れば、企業は、不正を防止し、早期発見するため、内部統制、テクノロジー、報告体制を強化しているといえる。しかし、外部犯行者による攻撃に対しては、これまでとは異なる対策が必要である。社外攻撃による不正が増える中、企業が自社の防衛線を強化するためには、以下の3つポイントを抑えることが重要である。

1

顧客と接点のある取引の一連の流れを把握すること。取引全体を見渡し、不正の実行者が入り込んで、自社に金銭的、法的、風評ダメージが及ぶ隙を分析、特定する必要がある。想定される不正が、どこでどのように起こりそうか、それを防ぐにはどうすべきか、実際に起こった場合にどう対応すべきかを検討しておくことが有用である。

2

ユーザーエクスペリエンスとリスク管理の適切なバランスを見つけること。顧客との接点およびコミュニケーションを守るためには、顧客満足度と、不正を検知、排除することとの間の微妙なバランスを保つ必要がある。不正検知のためのテクノロジー、戦略、手続をうまく組み合わせることで、正常な取引を不正と誤検知する確率を下げ、本当の不正を検知する確率を上げていくことができる。

3

データを集約すること。不正のシグナルは、分断された異なるシステムから発せられることが多く、不定期に実施されるマニュアル監査で見つかることが多い。不正の兆候となる情報を一つのプラットフォームに集約させ、ユーザー（顧客、犯行者であることを問わず）との一連の取引の中で必要なアラートが上がる仕組みを構築しておくことが極めて重要である。

結論

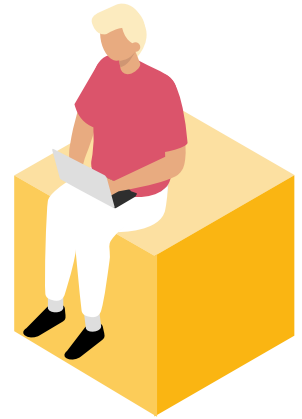
不正やその他の経済犯罪を防ぐのは、複雑な課題であり、社内規程の整備、研修の実施、実効的な内部統制の構築に加え、より高度なテクノロジーを導入し、取り組みを継続していく必要がある。犯行者たちの手口は年々巧妙化してきており、企業としては、今後さらに自社の防御を固めていくための対策を講じる必要がある。

調査について

今年度の「グローバル経済犯罪実態調査」では、企業を取り巻く不正および経済犯罪に対する意識および取り組みについて質問し、53の国および地域における1,296人からの回答を得た。本調査は、2022年度の第一弾であり、不正の傾向とリスクに焦点を当てたものである。

PwCの「グローバル経済犯罪実態調査」は20年以上にわたり、以下を含む数々の犯罪を調査してきた。

- 会計・財務諸表不正
- 独占禁止法違反
- 資産の流用
- 贈収賄と汚職
- 顧客の不正行為
- サイバー犯罪
- 詐欺的取引慣行
- 人事に関する不正
- インサイダー／未承認取引
- 知的財産 (IP) 窃盗
- マネーロンダリングおよび経済制裁
- 調達不正
- 税金不正



61%

回答者に占める経営層の割合

39%

回答した企業のうち、年間売上高が10億米ドルを超える企業の割合
(1億米ドルを超える企業は65%)





PwCグローバルネットワーク

Kristin Rivera

Global Forensics Leader, Partner, PwC US
kristin.d.rivera@pwc.com

Ryan Murphy

US Forensics & Investigations Leader, Partner, PwC US
ryan.d.murphy@pwc.com

Claire Reid

UK Forensics Services Leader, Partner, PwC UK
claire.reid@pwc.com

Claudia Nestler

Germany Forensics Services Leader, Partner, PwC Germany
claudia.nestler@pwc.com

Mark Rigby

Australia Forensics Services Leader, Partner, PwC Australia
mark.rigby@pwc.com

Sirshar Qureshi

EMEA Forensics Co-Leader, Partner, PwC Czech Republic
sirshar.queshi@pwc.com

Stefan Heißner

EMEA Forensics Co-Leader, Partner, PwC Germany
stefan.heissner@pwc.com



日本のお問い合わせ先

PwC Japanグループ

www.pwc.com/jp/ja/contact.html



PwCアドバイザリー合同会社

丸山 琢永
パートナー

平尾 明子
ディレクター

志村 亜希
マネージャー



www.pwc.com/jp

PwC Japan グループは、日本における PwC グローバルネットワークのメンバーファームおよびそれらの関連会社（PwC あらた有限責任監査法人、PwC 京都監査法人、PwC コンサルティング合同会社、PwC アドバイザリー合同会社、PwC 税理士法人、PwC 弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。

複雑化・多様化する企業の経営課題に対し、PwC Japan グループでは、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約 10,200 人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。

PwC は、社会における信頼を構築し、重要な課題を解決することを Purpose（存在意義）としています。私たちは、世界 152 カ国に及ぶグローバルネットワークに約 328,000 人のスタッフを擁し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細は www.pwc.com をご覧ください。

本報告書は、PwC メンバーファームが 2022 年 4 月に発行した『PwC's Global Economic Crime and Fraud Survey 2022』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。

オリジナル（英語版）はこちらからダウンロードできます。 <https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html>

日本語版発刊年月：2023 年 1 月 管理番号：I202212-04

©2023 PwC. All rights reserved.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.