経済犯罪実態調査2020

日本分析版

pwc

www.pwc.com/jp

目次

はじめに

新型コロナウイルス危機下における不正シナリオとは

本レポート「経済犯罪実態調査2020」を編集している最中、世界は新型コロナウイルス感染症（以下COVID-19とする）拡大という「危機」に見舞われることになった。日本においても、2020年4月7日に政府により緊急事態宣言が発出され、これを受け、対象地域の都道府県知事により①住民に対して外出自粛への全面的な協力要請、②事業者に対して営業の自粛要請が出されるなど、日常生活に加えビジネスにも多大な影響を与えた。そして緊急事態宣言が解除された後も、COVID-19の危機が去ったわけではなく、従業員、顧客、取引先を含む多くのステークホルダーが、感染拡大の第2波襲来に不安を感じつつ、新しい生活様式への適応、業績の急速な悪化への対応などの苦難を強いられている状況にある。COVID-19対応は、これまで誰も経験したことがない異常事態といえる。このような状況下で、組織のリーダーは、「緊急対応」と「事業継続」という二つの重い課題に取り組まなければならない。「通常のビジネスボリュームは減った上、従業員を守り事業継続することに精一杯で、不正行為などする余裕もない」といった声も聞こえてくるが、果たしてそうであろうか。想定されるリスクシナリオから、トップがすべきことを考えてみたい。

想定リスクシナリオ

COVID-19の拡大により、リモートワークが半ば強制的に求められるなど、短期間で主要な業務プロセスの変更やインフラの整備を行わなければならない「プレッシャー」が生まれた。このプレッシャーの中、イレギュラーな事態への対処や判断を迫られる、業務を中断せざるを得ない、また、リソースやインフラキャパシティが不足するなどといったケースが生じ、結果的に、従来のコントロールの範疇にないリスクが高まっている（なお、以下の想定リスクシナリオは全て架空であり、特定の組織・事例を示すものではない点に留意されたい）。

①資産の不正流用

多くの企業が、「リモートワークを前提とした内部統制」が構築されていなまま、リモートワークを導入せざるを得なかったのではないか。規定通りの証憑が入手できない、または、入手できたとしても「現物」を確認できる状況にないなど、当初の保証水準での統制業務の実施が不可能な状況が生じやすくなった。解決するための方法として、今回限りの「特別ルール」や「特別な承認」を設けた企業も多く存在するだろう。

- A社では、社内経費承認の際には、証憑「原本」の提出が必要であるとし、経理部において複数人で確認する体制を敷いている。しかしながら、緊急事態宣言下の移動規制を理由に、経費申請の際に必要な「原本」が提出できないケースが生じた。そのため、特例として、「証憑の原本が提出できない場合、原本を確認しなくても特段不合理でない限り、システム上の申請のみで承認可能」というルールを策定した。この統制上の特別ルールを悪用し、ある従業員が領収書を提出することなく私用目的の支出を経費として申請した。特段疑いを持たなかった経理スタッフは申請を承認し、不正に会社資産が流用された。

- B社では、社内決裁は紙面上に「ハンコ」を押す方式で決裁が行われている。緊急事態宣言下で全社的にリモートワークに移行したため、「ハンコ」承認の代わりに、eメールでの承認を特例として認め、eメールを印刷したものを承認結果として提出可能というルールを設けた。ある従業員が、私用でのタクシー代について経費申請をし、その際、上長が承認したように見えるよう作成したメールの印刷結果を添付し、経理担当者はこれが偽造であることに気が付かなかった。また、本来であれば経理部内で上長によるダブルチェックが必要なところ、リモートワーク下のイレギュラーな対応に追われたこともあり、うっかり上長承認ルートをとばして経費処理をしてしまった。結果的に、不正に会社資産が流用された。

リモートワークによって従来存在したコミュニケーションも希薄化し、平常時の牽制機能が効かなくなりつつある。加えて、緊急事態を理由とした業務遂行上の制限が生じ、必要なところにリソースが不足するなどいつもとは違う状況下で、平時よりも業務にミスが生じる、または、コンプライアンスに反する事案に疑いを持たないといった問題が起こりやすくなる。結果、不正を看過してしまう上記のようなケースもあるだろう。

②不正会計

COVID-19による業績への影響は不透明であるが、多くの企業において業績の悪化は避けられないと思われ、財務的なプレッシャーが高まることによって直接的または間接的な不正の「動機」が生まれる可能性がある。また、財務状況の悪化から人員削減を行った結果、内部統制が従来通りに機能しなくなり不正の「機会」が生まれてしまうケースや、外部監査が例年と同様の方法で実施できないケースもあるかもしれない。

- C社は、消費財メーカーであり、国内数か所に倉庫・物流施設を有している。例年であれば決算期末である3月末日に、会計監査人の「立会」の下、実地棚卸を行う。しかし、C社は、知事による外出自粛要請を理由に、会計監査人に対し、棚卸作業自体の中止を申し出た。C社は継続記録法を採用していたため、実地棚卸を中止する代わりに、期末の在庫残高を算定するために、「出庫証明書」の提出を提案した。会計監査人は、諸般の事情を勘案し了承した。しかしながら、この出庫証明書は、配送業者の協力のもと偽造されており、実際の出庫数量より過大に報告していた（すなわち、実際には売れておらず、倉庫に残ったままになっている製品について、売れたように見せかけていた）。これにより、利益の過大計上が行われた。C社CFOは、COVID-19による経済活動縮小により業績が振るわず、業績予想未達成の状況について悩んでいた。利益を業績予想どおりに見せるために、CFOは経理部、工場在庫管理担当者に対し上記スキームによる在庫および売上高の調整、証憑の改ざんを指示した。さらに会計監査人に対しては、自ら代替手続きの提案を行った。

- D社はソフトウェア開発企業である。経理担当者は、受注したソフトウェア開発案件について開発原価の各種証憑の日付や案件名を改ざんした。そして、原価を本来計上すべきでないプロジェクトに計上し、結果的に原価計上の時期を繰り延べた。その結果、当期の利益は過大計上された。D社のCEOを含む経営陣はCOVID-19による経済活動の停滞により、他の案件進行が中断するなど、当初業績予想が未達となることを懸念しており、経理部に対して利益捻出の指示を行っていた。リモート対応していた会計監査人は、改ざんが行われた原価証憑について、原本ではなくメール送付されたPDFファイルにて確認しており、改ざんは看過された。

- E社は投資ファンドを経由して多くのアライアンス企業やベンチャー企業に投資を行っている。しかし、2020年3月決算において、投資先のベンチャー企業の事業は事実上ストップしてしまっている状態であり、今後事業を継続できる見込みもない。E社としても、そのような状況を把握している。本来であれば、投資先の事業に関する無形固定資産（のれん）の減損を実施する必要があるところ、会計監査人に対しては、虚偽の事業計画を説明し、無形固定資産の減損処理を回避し、同会計期間の利益が過大計上された。COVID-19による経済活動の停滞により、事業計画を十分に検討することが困難な状況の下、減損の先送りは看過された。

- F社は、製造業である。COVID-19による経済活動の停滞による業績悪化で、経費削減を進めており、加えて健康への配慮から、海外駐在員を帰任させることにした。そこで、駐在員たちが担っていた日本本社の連結パッケージソフトウェアと連携するための複雑なマニュアル作業（現地独自のシステムAからデータを切り出して加工し、連結パッケージシステムBに入力する作業）を、現地の経理担当者に任せることにした。後任のスタッフは不慣れであるため、現地子会社CFOの指示のまま経理処理を行った。その中に、「陳腐化した棚卸資産の評価損レポート」があったが、CFOは「評価損を計上する状況にない」と虚偽の報告をしていた。経理担当者は言われるがまま連結パッケージソフトに虚偽の報告内容を入力した。結果的に、実態より業績をよく見せる決算処理が行われた。会計監査人は、F社海外子会社の経理担当者の変更を知らされておらず、担当者変更後の内部統制の状況を検証していなかった。

厳しい経営状況から人員削減をはじめとする社内体制の変更を行った場合、内部統制の脆弱化を招くことが多い。以下の例のように手続きを簡略化した場合は、統制機能の不備が生じていないかについて点検し、変化の隙間を突いた不正を防止したい。

・G社の海外子会社では、リモートワーク移行に伴うネットワーク構築を緊急で行う必要が生じた。自社のリソースでは対応できないと判断し、一部の業務をアウトソーシングすることにした。通常G社では、このような委託業者の選定に関して、コンプライアンスプログラム上、3社以上から「相見積もり」を取り、価格上の選定を行った上で、委託企業の事業継続性、サービスの品質、業界での風評など、数十項目をリスク評価する。しかし、COVID-19の混乱の中で本来あるべき「相見積もり」や「リスク評価」を行う時間が確保できず、海外子会社社長主導で「今すぐ対応が可能な」業者として、社長親族が経営する企業と相場よりもはるかに高い金額で契約した。このようにコンプライアンスプログラムに定められた手続きを行わなかった結果、市場価格と比して、不当に高い金額が委託費として支払われ、会社資産の流出を招いた。

③品質不正

COVID-19感染拡大により生じた「危機」は、会社や社会のルールを逸脱してよいという不可抗力にはならない。危機への対応に追われている状態が、緩んだ内部統制やコンプライアンス体制を是正しないことの正当化に結びつきやすい状況になっている。製造現場や品質管理工程においても、現状を的確に把握し最低限守るべきラインを組織として認識し補正していくような体制を構築したい。

・H社では、一定期間ごとに、業務で必要な資格や免許（自動車運転免許や、外国人在留資格などの各種免許）の更新状況をモニタリングしている。緊急事態宣言下で、各規制当局は、更新の延期や有効期間の延期措置を講じた。その後、緊急事態宣言が解除され、免許・資格更新申請ができるようになったにも関わらず、資格更新を行わなかった従業員が存在した。この把握を品質管理部は失念していた。結果的に、免許更新をしない状態で一定期間、法律で定められた免許が必要な業務に従事させていた。

④贈収賄

緊急事態宣言下の制限により、当初の予定通り業務が進まず、取引に影響が出ているケースも多い。このような中、業績が悪化した企業においては、ルールを逸脱してまで目標を達成しようというインセンティブが生じやすい。特に以下のような贈収賄や汚職に関しては注意が必要だ。

・I社はヘルスケア業界に属しており、COVID-19感染拡大の状況下において、X国にある海外子会社が、X国政府で必要とするマスク等の医療関係の製品やサービスを提供している。X国の海外子会社では、COVID-19下の各種制限により業績に大きな悪影響が出ていた。そこで海外子会社のCEOは、損失補填のため、購買業務に従事する公務員らに賄賂を渡し、その見返りとして、製品供給契約を獲得した。

・J社は、オンラインでの教育サービス提供をグローバルで展開している。COVID-19により諸外国でも軒並み学校が休校となり、自社のサービスを売込む絶好の機会と考えた。しかし、Y国においては、既にオンライン授業は概ね普及しているため、同サービスを提供する事業者間の競争は激しい。そこで、国立学校法人Yとサービス導入契約を締結できるようコンサルティング会社Zに働きかけた。うまく契約が成立したため、コンサルティング会社Zの役職者や国立学校法人Yの校長らにキックバックとして、取引合計金額の5%相当の金品を渡した。

⑤情報漏洩

短期間のうちに全社的なリモートワークを迫られた結果、システム管理および情報保護に対する取り組みの検討プロセスを省略ないし未実施のままリモートワークへの移行がされていないだろうか。今一度点検しておくことが重要だと考えられる。

リモートワークでの業務遂行により、従業員が自宅のネットワークからアクセスを行う、または、私用のPC端末などから仕事を行うなどの機会が増えるため、セキュリティ対策の必要性が各所から指摘されている。しかしながら、リモートワークに即した慎重な対策導入検討手続きを踏めず、通常時と変わらぬ態勢のままで、相応の維持管理予算および体制が確保できていない企業もあるのではないだろうか。そのような状態を放置すれば、情報漏洩が発生してしまう隙を広げてしまう可能性がある。

・K社では、リモートワーク開始にあたり、従来から貸与していた出張用のモバイルルーターを経由して、社内システムを利用することを想定していた。ところが、既存の通信契約ではデータ通信量がキャパシティを超えてしまい業務遂行が困難となったため、従業員の自宅の回線の利用を条件付きで許可することになった。しばらくすると、セキュリティ設定が不十分であった従業員の自宅のネットワークが外部から侵入され、業務用のPCが乗っ取られた。

・L社はセキュリティ対策を重視しており、万が一の不正アクセスに備え、アクセス状況が分析可能な仕組みを導入するなどの対策をCOVID-19拡大当初から着手していた。しかし、IT部門のメンバー自身もリモートワークに移行し一部業務に制約が出たため、実際のアクセス監視方法および危機対応方法の精査、それに見合った体制確立や試験運用については、部分的に延期せざるを得ない状況であった。ようやく通常業務への落ち着きを取り戻した頃、過去のアクセス状況の調査を進めていくと、社内の技術情報に対する不審なアクセスが多発していたことが判明した。

また、リモートワークの推進で急遽不慣れなツールの利用が増加したことで情報漏洩リスクが高まる可能性もある。本来であれば早期に重要情報の取扱いポリシーの見直しを行った上で、利用者に向けた適切な情報管理教育と操作訓練が必要である。ところが、それらが徹底できない状況が続き、不用意に情報漏洩が広がってしまうケースもあるだろう。

・M社では、リモートワーク推進のため新たに手軽なビデオ会議ツールの利用を開始することとなった。ところが、急なリモートワーク要請の中で、情報取扱規程の詳細な見直しに時間を割くことができず、従業員に簡易的なツール操作マニュアルを配布しただけで利用が開始された。セキュリティに対する危機意識の醸成が後手に回ったこともあり、ビデオ会議後に接続を切り忘れ、別顧客との会議の内容が漏洩したり、ビデオ/電話会議の目的に適合しない参加者が含まれることにより、情報が漏洩していたことが判明した。

トップがすべきこと

先が見えない脅威にさらされる中、「緊急対応」と「事業継続」という課題に向き合うためにトップがすべきことは何であろうか。

まず、COVID-19への感染リスクを下げ、従業員が安全に働ける環境を確保しなければならない。業種や業態により制約は異なるが、可能な限りリモートワーク環境を推進し、安全かつ衛生的な就業環境を構築する必要があるだろう。加えて、この数ヶ月間のリモートワーク環境下で露わになった業務プロセス上の不備を踏まえた就業規則の改定、情報管理規程の整備、セキュリティ環境の構築、業務プロセスの改善などが求められる。この機会に改めて統制の見直しをすることにより、不正の機会を減らしていくことに繋がるだろう。

そして、組織としての新たなリスク認識をトップダウンで共有することをはじめとして、適切な組織風土・リスクカルチャーを醸成することに注力したい。具体的には、それぞれの事業において想定される「難しい判断が求められる場面」をいくつか取り上げて、そのような場面における「あるべき行動指針」について組織の構成員へ伝達し、繰り返しコミュニケーションをとる必要があるだろう。全従業員のリスクに対する認識を高め、それを実際の行動にまで落とし込むことで、いかなる場合であっても不正が正当化できるものではないことを組織に徹底することが可能となるだろう。

今後多くの企業で業績不振が予想されるところ、組織に芽生え得る不正の動機の芽を早めに摘んでおくことも大切かもしれない。設定した目標の見直しを行うことはもとより、状況に鑑みて現実的でないコミットメントが放置されていないか、評価基準や賃金制度はそぐわないものになっていないか、人員配置は適切かを確認していく必要がある。これは組織の構成員に対してのみでなく、サプライヤーなど他のステークホルダーとの関係においても同様である。つまり、事業継続あるいは業績回復に向けて財務・事業リスク分析を実施し、リソースの配分を見直すことが不正を予防し早期回復するためのキーとなる。

最後に、ビジネス上のステークホルダーに加え、国内外の政府当局等の関係性の維持も重要となってくる。必要なタイミングでの各種優遇措置を迅速に受けるためにも、情報の収集に加え、説明責任を果たし、常に事業の透明性を確保しておくことが重要である。

本レポートが皆様にとって、困難に立ち向かい、with コロナ時代の「New Normal」への移行に繋がるヒントになれば幸いである。

2020年7月
PwCアドバイザリー合同会社
フォレンジックチーム

調査結果の要旨

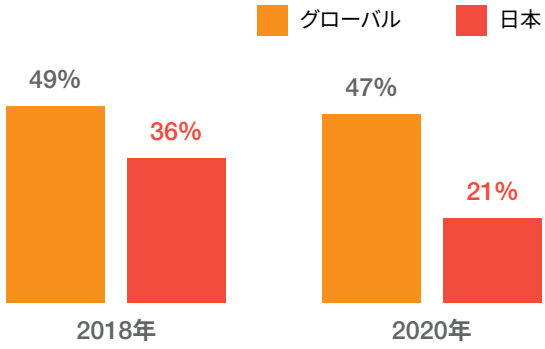
経済犯罪・不正の実態について、PwCでは2年に1度、グローバル規模でオンラインによるアンケート調査を行っており、今回で10回目を迎えた。今回は、グローバル全体では5,018社からの回答があり、日本では172社から回答が寄せられた。本報告書では、得られた回答を基に、特に日本とグローバルの結果を比較しながら、日本企業の置かれている状況や考えられる対策について論じている。

今回、過去2年間で経済犯罪・不正の被害に遭ったと回答した日本企業は21%で、前回調査時（2018年）に比べて15%減少した結果となった。グローバル全体でも、47%の組織が経済犯罪・不正の被害にあったと回答しており、前回調査より2%減少したものの、依然として約2社に1社が被害に遭った結果となっている。また、過去2年間に報告された不正の損失は、グローバル全体で総額420億米ドルにも上り、その内容は財務上の損失のみならず、ブランドの毀損、マーケットによる競争優位の喪失、従業員の士気の低下など、容易に数量化できない損失も含まれている。

経済犯罪の被害に遭ったと回答した日本企業のうち、不正行為に関与した主犯格は、従業員などの組織の内部者が53%であったのに対して、組織の外部者は44%であった。前回調査までは圧倒的に組織の内部者による不正の割合が高かった（2018年調査では72%）が、今回調査では、組織の外部者の割合が大きく増加する結果となった。一方、グローバルにおいては外部者の割合の方が内部者より高くなっており、組織の内部者が37%、外部者が39%であった。この理由は、次に述べる「不正の内容の変化」にあると考えられる。

被害に遭った経済犯罪・不正の類型について、グローバルでは「顧客による不正」が最も回答が多く、次いで「サイバー犯罪」「資産の横領」が多かった。他方、日本では、例年「資産の横領」および「財務報告に関する不正」が最も多い不正として常に上位に並ぶ傾向にあったが、今回初めて「サイバー犯罪」が第1位となった。ニュースなどではたびたび目にする「サイバー犯罪」であるが、急速に日本企業を取り巻く環境に大きな影響を与えていることが本調査からも読み取れる。先述した主犯格との関係からも分かるとおり、日本ではサイバー犯罪の割合が相対的に増加していることが、ハッカーなどの社外の組織・人物による犯罪が増加している要因の一つになっていると考えられる。

図表1：過去2年間に経済犯罪の被害にあったと回答した企業の割合



調査概要

アンケート調査実施期間	調査方法	有効回答数	経営幹部レベル（C-suite）からの回答
2019年 9月～10月	オンライン による選択式 アンケート方式	世界99の国と地域 グローバル全体で 5,018企業 日本は172企業から回答	グローバル 62% 日本 66%

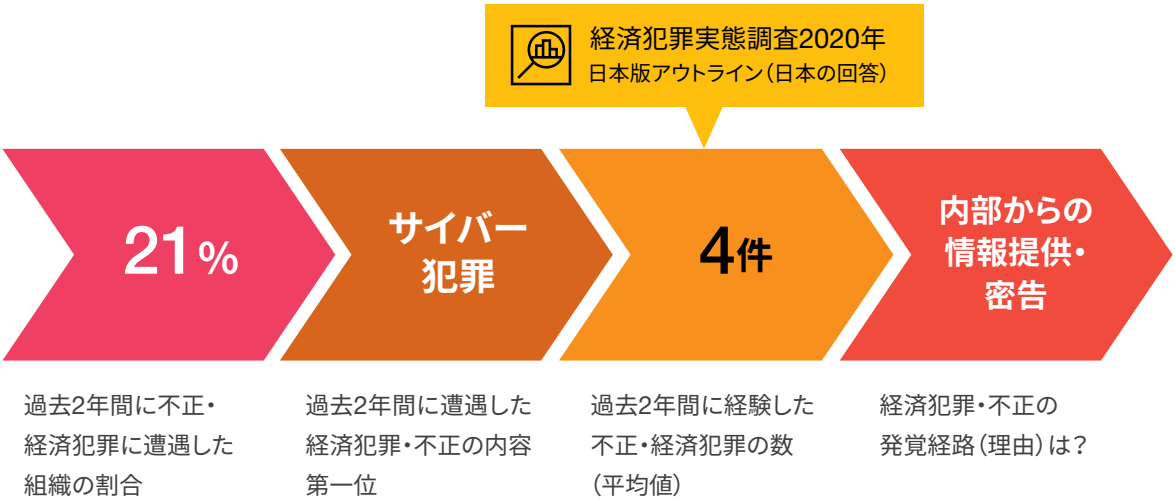
公開企業の割合	1,000人以上の従業員数の企業割合	年間収益が10億米ドル以上の企業割合
グローバル 26% 日本 36%	グローバル 48% 日本 50%	グローバル 29% 日本 38%

経済犯罪・不正の発覚理由については、「内部からの情報提供・密告」と回答した組織が19%と最多で、続いて「不正リスク管理」や「コーポレートセキュリティ」によると回答した組織が同率で14%であった。日本で従来割合が高かった「偶然」による発見は、今回の調査で大幅に減少しており（2018年：11% → 2020年：3%）、不正に対するモニタリングシステム、情報・伝達の仕組みの構築の結果、それらが効果的に機能していることの表れとみることができるのではないだろうか。一方で、「内部通報・ホットライン」経由の不正の発覚は、日本企業に関しては全くない結果となった。近年、内部通報制度を整備し、独立した社外弁護士事務所をホットライン窓口に設置している組織が増えているが、今回の結果を見ると制度自体が当初意図したとおりに機能していない実態が強くうかがわれる結果となった。通報者の保護や、提供された情報の客観性のある取り扱いなど、利用者にとっての懸念点を洗い出すとともに、計画から導入、対応までの運用を具体化し、より実用的で有効的なものに見直すことが必要である。

今回大幅に増加したサイバー犯罪についても、各種テクノロジーを導入し運用することにより、サイバー犯罪を未然に防いだり、早期に検知するための施策を導入する意欲がグローバル・日本ともにみられる。しかしながら、具体的な時期やその内容などに躊躇している回答も多くみられた。新しいテクノロジーの導入にあたっては、その価値が見いだせず費用対効果の面で疑問が残る、当初の想定どおりに活用できない、といった消極的な回答もあった。金融業界などを中心にサイバーセキュリティ対策の導入が進んでいる業界からの示唆を異業種に展開し、浸透させていくことが必要であろう。

多くの不正に共通するのは、取引先やベンダーなどの第三者（サードパーティ）の関与であるが、約3割の日本企業が取引先やベンダー等の第三者（サードパーティ）管理を全く行っておらず、グローバル全体でも、回答者の約半数が成熟した第三者（サードパーティ）管理プログラムが存在しないという結果となった。特に贈収賄については、自社の従業員による直接的な贈賄より、取引先を経由して政府系組織や公務員に渡るケースの方が圧倒的に多いため、第三者（サードパーティ）の起用にあたっては、リスク評価をした上で、専門家によるバックグラウンド調査やツールを用いたデューデリジェンスを行うといった施策を導入するべきである。

経済犯罪自体の変化に応じて、組織は新たな対策を講じる必要が出てくる。適切な対策を講じるためには、私たちが置かれている状況とその変化について情報を適時に収集、把握し、その状況に合わせて定期的に内部統制や社内ルールの強化・見直しを図る努力を続けていくことが肝要といえる。こういった平時の取り組みに加え、予防から有事対応までの一貫した体制構築が引き続き求められる。



1

日本企業における経済犯罪・不正の概要

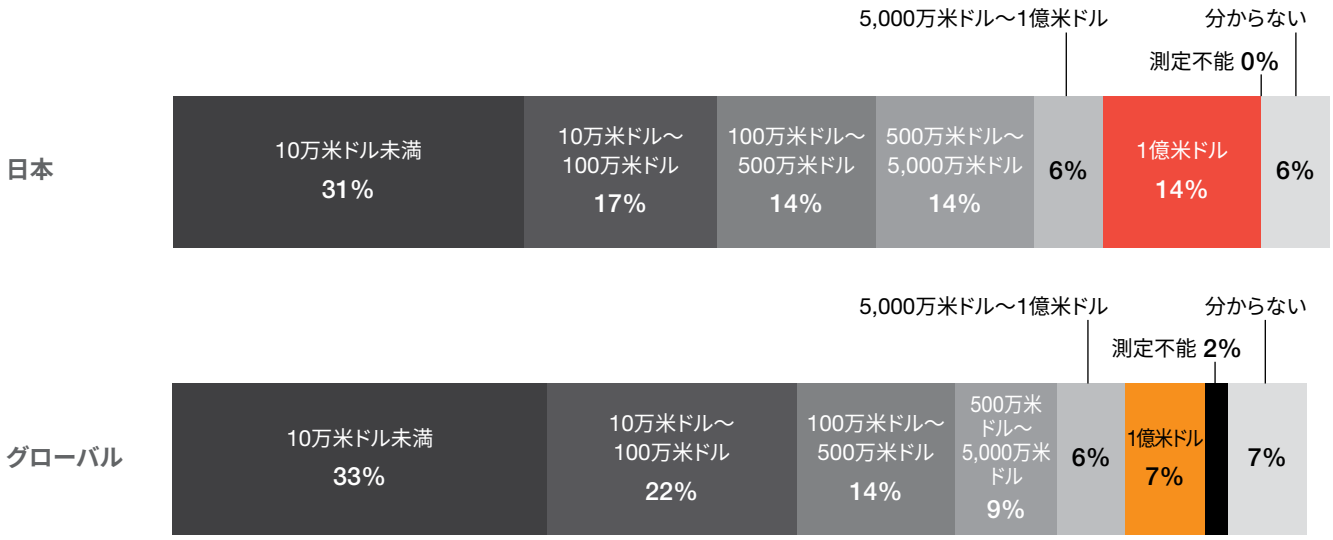
最新の経済犯罪・不正の傾向

過去2年間に不正を経験したかとの問いに対して、グローバルでは47% の組織、日本では21% が「経験した」と回答した。グローバルの結果は2018年調査とほぼ変わらないが、日本においては大きく減少している（2018年：グローバル49%、日本36%）。また、過去2年間に経験した経済犯罪の件数（図表3）を見ると、グローバルの平均は約6回であるのに対し、日本では約4回と、グローバルに比して少ない結果となっている（中央値比較でも同様）。

上記の結果を見ると、一見、経済犯罪の件数が減ったことで、安心できる結果と映るかもしれない。しかし、不正の影響は、単に件数だけで測れるものではない。実際に被った被害という観点から考えると、今回の調査は決してポジティブな結果とは言えない。

今回の調査では、最も被害額が大きかった経済犯罪の直接被害額、調査費用や弁護士費用など事案対応にかかった金額、管理体制の改善や再発防止にかかった金額、規制当局等からの罰金や課徴金の支払い額についてそれぞれ質問をし、組織にとっての経済犯罪・不正による被害の実態把握を試みた。その結果、過去2年間の経済犯罪による直接的な被害総額（図表2）に関しては、14% の日本企業が1億米ドル以上であったと回答している。これは、グローバルの回答（7%）と比較して、約2倍の数値である。

図表2：過去2年間に遭った経済犯罪・不正による被害総額全額

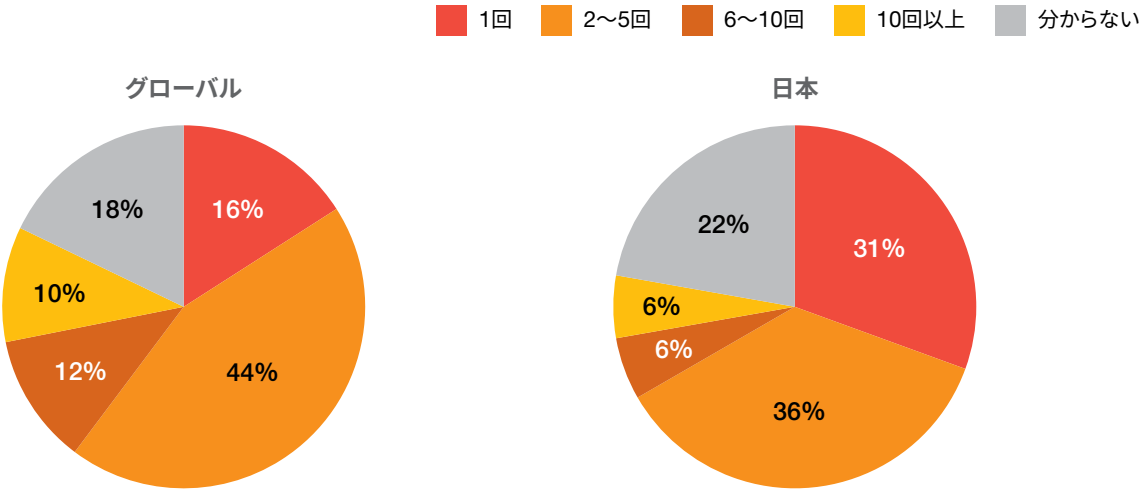


※構成比は小数点以下第1位を四捨五入しているため、合計しても必ずしも100とはならない。

不正の調査費用や弁護士費用など、不正の対応に100万米ドル以上の費用を費やした組織の割合（図表4）を見ると、日本企業は22%となっており、グローバルの15%と比較すると多く、また費用がかからなかったという組織をみてもグローバルの14%に比較すると6%と少ない結果となっている。

上記の結果に鑑みると、日本企業は不正の被害に遭う機会は少ないが、被害額が大きいということが分かる。つまり、日本では1件当たり事案でより大きな損失を被っているということであり、被害に遭った割合が減少していることをもって安心するのは早計である。また、実際に事案が発生した場合も、多額のコスト支出により、より大きな損害を被るため、予防や早期発見のための体制構築をきちんと確立しておくことが肝要であると言える。

図表3：過去2年間に経験した経済犯罪の件数

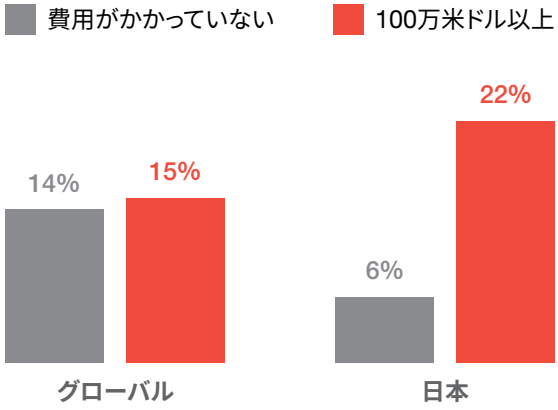


※構成比は小数点以下第1位を四捨五入しているため、合計しても必ずしも100とはならない。

過去2年間に経験した経済犯罪・不正の数（統計値）

	平均値	中央値	最低値	最高値	レンジ
日本	3.86	2	1	28	27
グローバル	5.95	3	1	50	49

図表4：不正対応にかかった費用

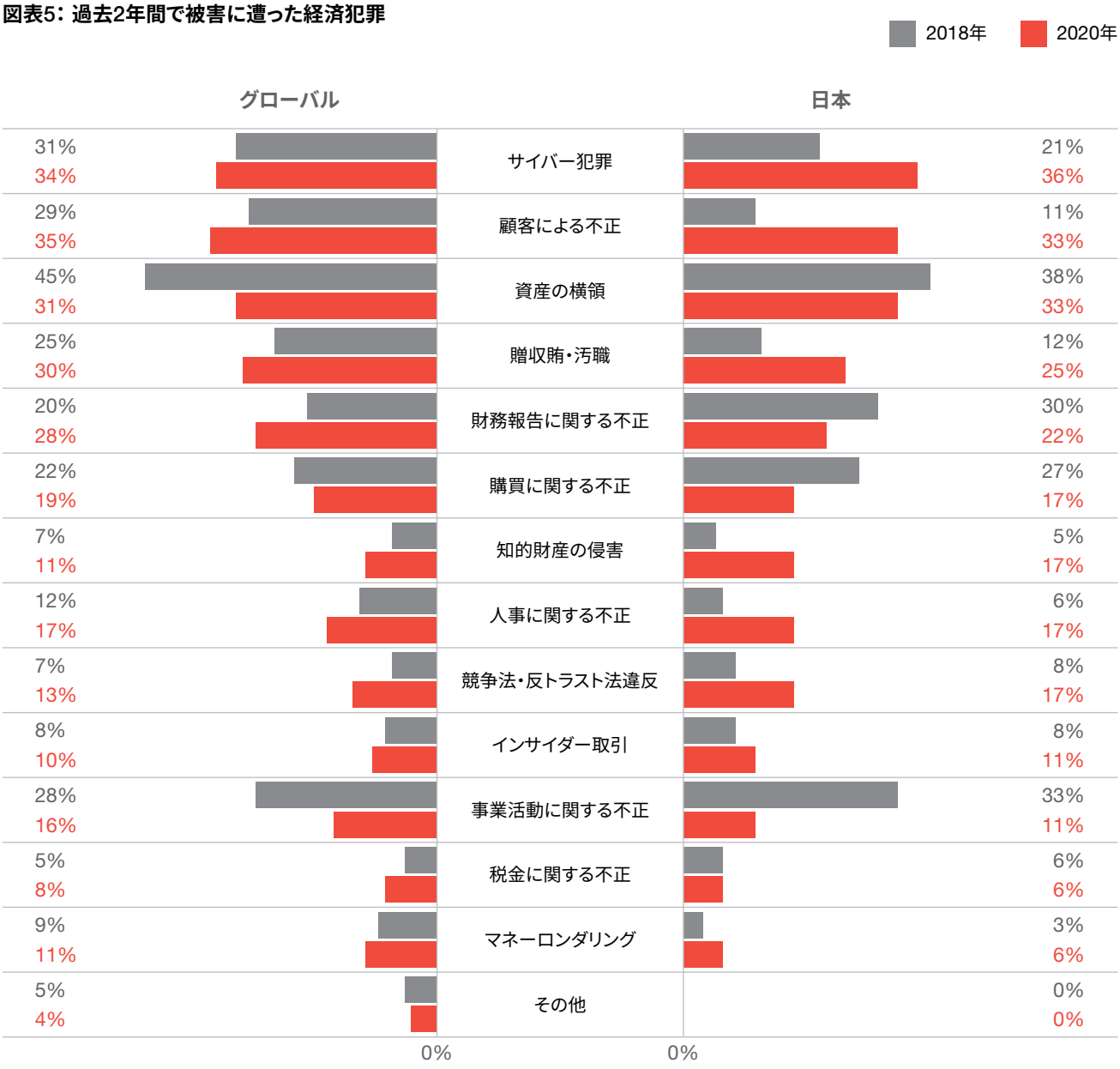


経済犯罪・不正の類型

過去2年間で、経済犯罪・不正の被害に遭ったと回答した組織が、どのような経済犯罪・不正の被害に遭ったかを示しているのが図表5である。

グローバルでは、「顧客による不正」が前回調査から6% 増加して第1位となり、次いで、「サイバー犯罪」「資産の横領」の順で上位となった。「顧客による不正」は、近年増加しているクレジットカードの不正利用や不動産ローンにかかわる不正融資・詐欺などを含んでおり、特に日本ではより顕著な増加傾向がみられた（前回調査の11% から3倍の33%）。この増加要因の一つとして考えられるのが、Eコマース市場の拡大である。テクノロジーの進化により、個人レベルでのビジネス・取引が容易になったため、個人が企業・組織のシステムに触れる機会が多くなったことに加え、クレジットカード等の不正利用の機会が増加した。また、対面ではない融資審査などにより、虚偽申告によるローン借り入れなどが可能となった。このようなテクノロジーを通じた商流の変化により、顧客による不正が増加したと考えられる。

図表5：過去2年間で被害に遭った経済犯罪



各国規制当局が強化をすすめる「贈収賄・汚職」規制および取り締まり

日本企業が経験した経済犯罪の中で特筆すべき点として、「贈収賄・汚職」の割合が、前回調査時と比較して倍増（12%→25%）している点が挙げられる。これについて考えられる要因の一つとして、アジアの経済活動が一段と活発になってきている国・地域の規制当局が、摘発を強化していることが挙げられる。

具体的には、タイでは、贈収賄規制に関する新法が2018年7月から施行され、外国法人も贈賄の主体として処罰の対象になり、捜査機関による取り締まりの権限も強化されている。また、マレーシアでもこれまで個人に限られていた処罰対象が法人に対しても適用されることになった（2020年6月より施行）。日本企業が関与したアジアでの贈賄案件としては、2019年に、日本版司法取引制度が初めて適用された外国公務員の贈収賄事案は日本国内でも大きく報じられていたため、認知している方も多いだろう。

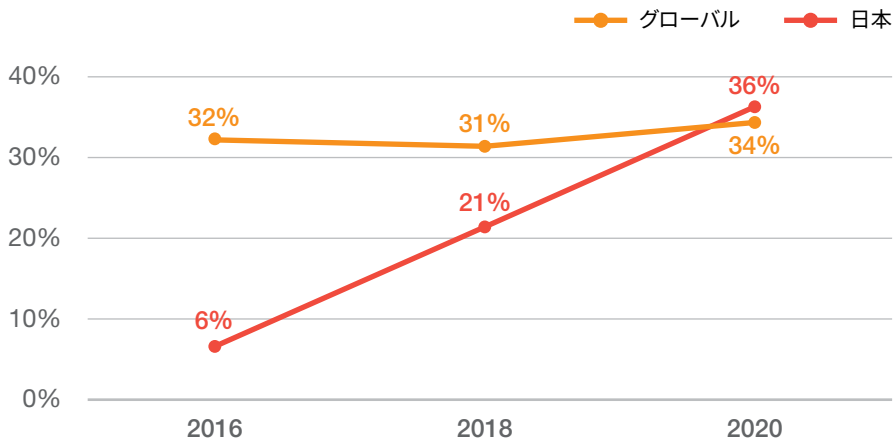
各国の文化・商慣習に沿うような形でのビジネスの進め方と、既に確立している本社（国内）のコンプライアンスプログラムをどのように現地レベルで適用させるかという論点は、海外で事業を展開する多くの組織が頭を抱える課題である。自社の反贈収賄・汚職コンプライアンスプログラムを一律に活動拠点全体に展開することは、贈賄や金品要求が根付いた国・地域では、事業展開を進めるうえでの足かせになると捉える人もいるだろう。しかしながら、上記のように、ここ数年で法改正などで贈賄・汚職の取り締まりが厳格化してきていることからも、最新の法令に基づく現地での対応をとることが、ビジネスをする上での必要不可欠である。

既に多くの組織は、米国のForeign Corrupt Practices Act（FCPA：連邦海外腐敗行為防止法）や、英国のBribery Act（UKBA：英国贈賂防止法）の域外適用に対応するための規程や手続きの整備および運用を行っているが、既存の規定・手続きでも自社が直面するリスクや事業内容に合わせて、定期的に見直さなければならない。とりわけ、グローバル展開する組織は、拠点を置いている各国の法規制の改正内容、そして文化や慣習をよく理解したうえで、子会社向けに展開しているルールの見直しを定期的に行い、現地従業員に対し適切な研修を実施し、ルールの徹底を図ることが肝要である。

サイバー犯罪の台頭

グローバル、日本ともに増加しているのが「サイバー犯罪」である。グローバルでは34%（前回比+3%）で第2位、日本では36%（前回比+15%）で第1位と、これまで経済犯罪の種類別で上位にランクインしていなかったサイバー犯罪が日本企業でも首位に位置する結果となった。サイバー犯罪は、グローバルでは4年前から3割前後で推移しているが、日本企業では近年顕著に増加傾向にある（図表6）。このサイバー犯罪の台頭に関しては、第4章で詳しく述べることとする。

図表6：「サイバー犯罪」の被害にあったと回答した組織の比率の推移



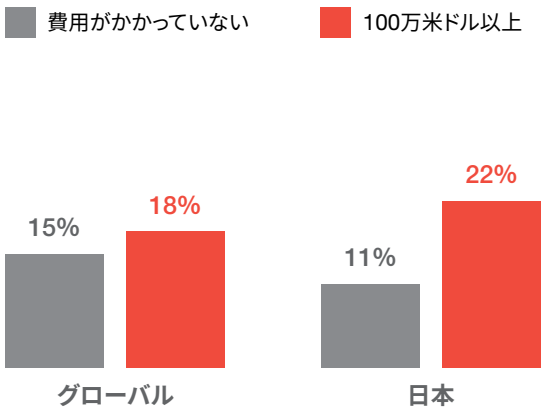
コスト面から考える不正対応

前述のとおり、日本企業では、不正対応にかかる費用がグローバルと比較して高額になる傾向がみられた。また、図表7の通り、事案発生後の再発防止策などの「改善」にかけた費用についても、若干ながらも、日本の方が100万米ドル以上費やした会社がグローバルより多い結果となった（日本：22%、グローバル：18%）。これにはさまざまな理由が考えられるが、今回の調査のトレンドに鑑みると、不正の種類として「サイバー犯罪」が上位にきており、対応すべき不正の質の変化に伴って改善にかけた費用にも影響がでていることが大きな要因の一つであると思料される。サイバー犯罪への対応にはシステム投資など多額の費用が掛かるだけでなく、せっかく対応策を講じてもまた直ぐに新しい攻撃手法が台頭し、新たな対応策を講じることが必要になるという、いたちごっこになってしまうケースが多い。

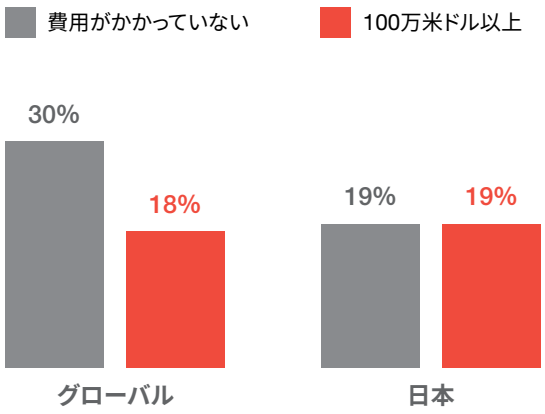
罰金や当局からの課徴金などの支払いにかかった金額（図表8）については、100万米ドル以上の金額を支払った組織が日本もグローバルも約2割となっており、経済犯罪の被害にあった組織の約5社に1社が高額な罰金・課徴金を支払っているという結果となった。近年、日本企業が海外の規制当局から摘発を受けたり課徴金を支払った例も相次いでおり、米国の連邦反トラスト法違反で2019年に2件、2018年にFCPA違反などで制裁金を科され合意したケースが1件あった。

また、昨年はEUにおいて欧州競争法違反で制裁金を科されたケースや、英国において競争法違反で制裁金が科されたケース、また、オーストラリアでの競争・消費者法違反で刑事上の有罪判決が出て罰金が科されたケースなどもあり、本社のある日本から離れた活動拠点において規制当局からの取り締まりがなされている。本拠地の法規制のみならず、各活動拠点におけるルールにも準拠したコンプライアンス体制の構築と適切な運用を図る必要がある。

図表7：不正対応後の改善費用

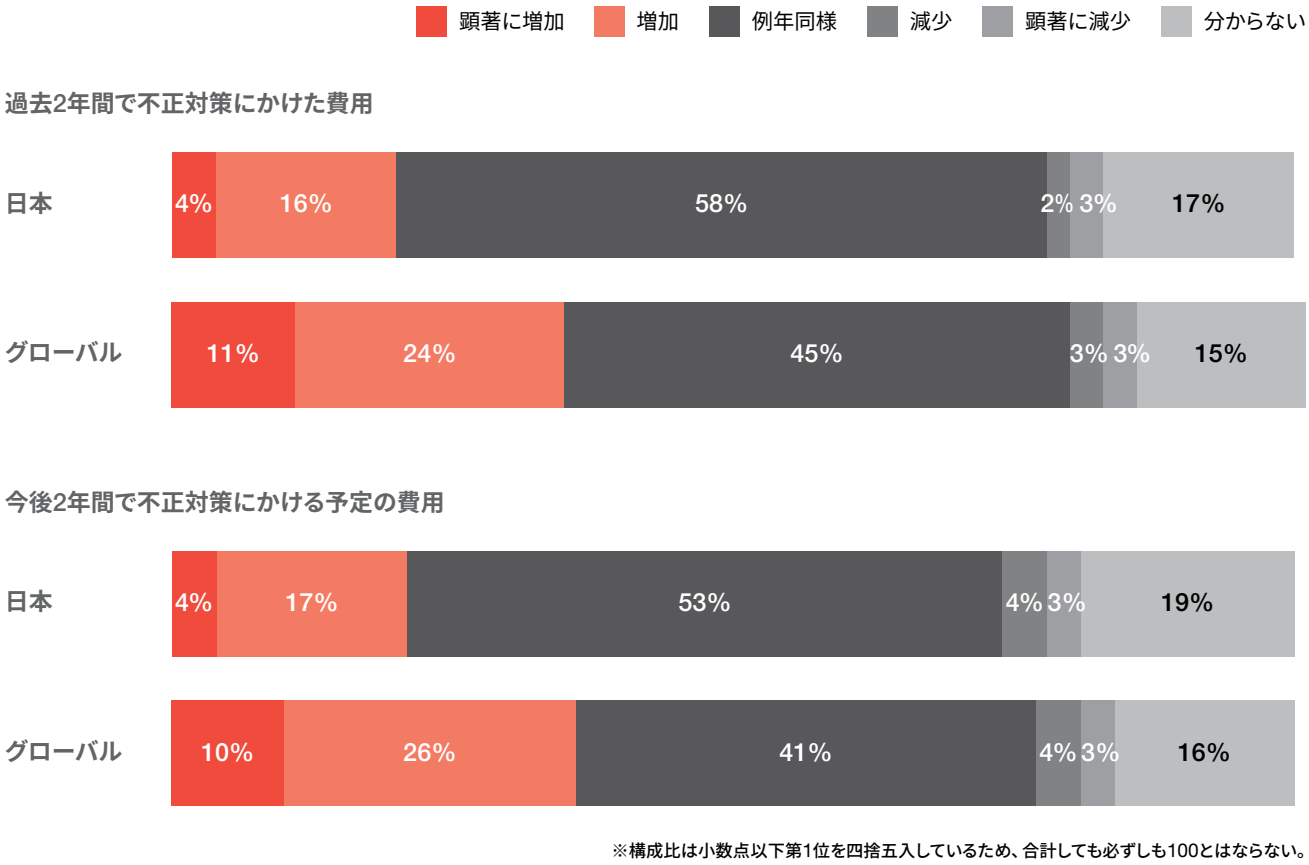


図表8：支払った罰金額



日本においては、過去2年間で予防策や事後対応などの不正対策にかけた費用と、今後2年間で不正対策にかける予定の費用について、半数以上の組織が、いずれも例年同様の金額規模を維持した（する予定である）と回答した（図表9）。将来の不正発生に備えた予算については、予算や投資を拡大したからといって、不正リスクは減少するものではない一方で、近年の経済犯罪の類型・内容が変化してきていること踏まえると、組織としてもその変化に見合った予算や投資面の見直しは必要であろう。新たな不正リスクに対応できるようなリソースの確保、サイバーセキュリティの導入・更新や、不正の早期発見に役に立つデータ分析やモニタリングなどのテクノロジーへの投資など、新たなリスクへの対応策の具現化を図りたい。

図表9：過去2年間と今後2年間における不正対応費用（予防策・事後対応を含む）

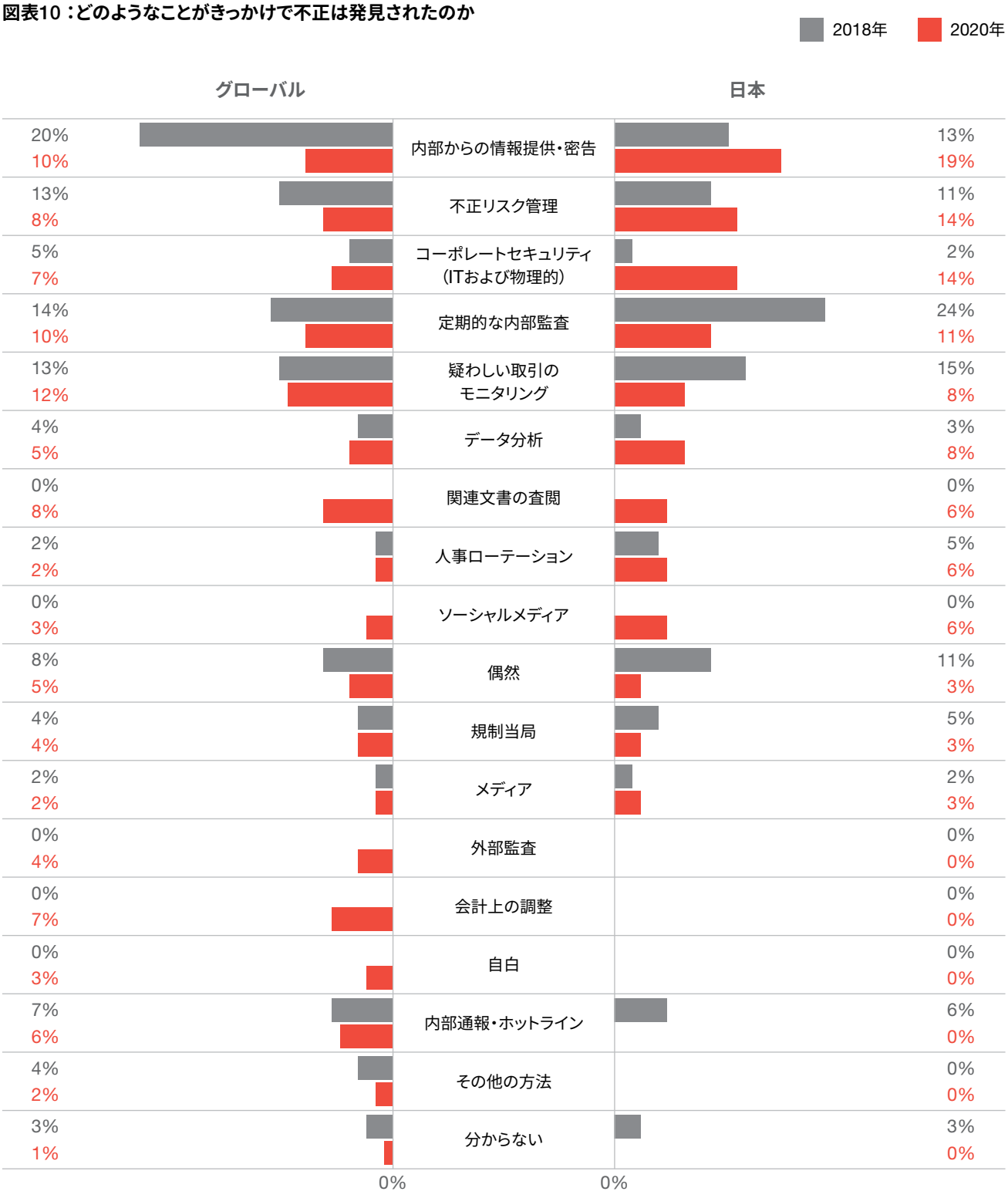


※構成比は小数点以下第1位を四捨五入しているため、合計しても必ずしも100とはならない。

経済犯罪・不正の発覚理由

今回、日本において不正が発覚した経緯として最も多かったのは、「内部からの情報提供・密告」の19%で、次いで「不正リスク管理」および「コーポレートセキュリティ」の14%であった（図表10）。「定期的な内部監査」は、前回調査（2018年）から大きく減少しているが（24%→11%）、グローバルと合わせて、不正検知の手法としては依然有効な手段の一つとなっている。

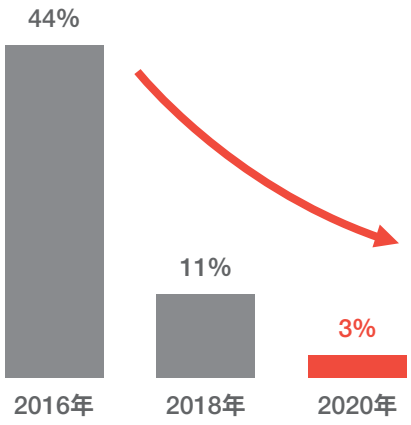
図表10：どのようなことがきっかけで不正は発見されたのか



また、不正が「偶然」発見されたケースは、前回（2018年）および前々回調査（2016年）から顕著な減少傾向にあり（図表11）、会社が不正防止・発見の意図をもって積極的な対応を講じている会社が増えてきていることがうかがえる。

一方、今回最も多かった「内部からの情報提供・密告」と比較して、「内部通報・ホットライン」を通じた不正発見は全くない結果となった。「内部通報・ホットライン」と「内部からの情報提供・密告」は、何れも社員などの内部関係者からの情報提供に基づいた不正発覚であり、一見すると同じように受け止められがちである。しかし、制度として内部通報窓口を設置し、然るべきルートで体系的に報告される前者とは異なり、後者はそうした制度を通さずに社内外の関係者に直接、社内の不正に関する情報が持ち込まれる（考えられる例として、社内外の利害関係者への告発文の送付、管轄する規制当局への相談、週刊誌などの報道機関への情報提供などが挙げられる）。

図表11：「偶然」による発見の割合（日本における調査）



近年、コンプライアンス意識の高まりとともに、内部通報制度を整備し、独立した社外弁護士事務所をホットライン窓口に設置するなどしている会社が増えてきているが、今回の結果を見ると、制度自体が有効的に機能していない実態が浮き彫りになっている。内部通報自体の存在や具体的な運用方法が周知されていない、通報者が報復など自身に対する不利益を危惧している、提供された情報に基づく会社の対応の欠如・不備が疑われているなど、客観性も含めた制度に対する不信感および懸念が、内部通報制度が活用されていない理由となっている可能性がある。

社内の不正行為に対して危機感を抱き、行動を起こす勇気ある社員が増えてきているということは、喜ばしいことである。しかし、内部通報制度を通さず、一度外部関係者に情報が渡ってしまうと、情報の真偽の確認も含めて、会社として効果的な対応が困難になってしまう可能性がある。今後新しく内部通報制度の導入を検討している会社も、既存の制度を引き続き運用していく会社についても、計画から導入、対応までの運用を具体化し、利用者へ周知徹底することが重要である。具体的には、①客観性・独立性を持つ社内および（または）社外の受付窓口の設置、②秘匿性の担保および通報者の保護に関する規定、③情報に基づく社内調査の要否判断の基準、通報後の対応（調査プロセス、調査実施者などを含む）、調査結果に基づく報告（通報者、取締役会、その他利害関係者）、および事後対応（不正行為者の懲戒処分など）に関する方針の明確化、④不正関与者・社内規定違反者に対する懲戒処分の明文化とルールに基づいた処分の実施 、⑤過去の通報内容および調査結果に基づく再発防止策などの策定・見直しなど、制度としての仕組みをより実用的かつ有効的なものにするための努力が必要であると考える。

2 経済犯罪・不正の主犯者のプロフィール

経済犯罪・不正の主犯者の概要

経経済犯罪・不正の主犯者の特徴とはどのようなものだろうか。グローバルと日本を比較した場合、グローバルにおいて不正の主犯者が組織の内部者であるのは37%であるが、日本では53%となり、日本の方が内部者が不正の主犯者である割合が高い結果となった（図表12）。しかし、日本のアンケート結果の2018年と2020年の比較では、内部者が不正の主犯者である割合が72%から53%と減少している一方、外部者が不正の主犯者である割合が、19%から44%と著しく増加している。その原因の一つとしては考えられるのは、「サイバー犯罪」の増加である。サイバー犯罪は、基本的に組織外部の人間により行われる行為であり、組織のセキュリティの脆弱な部分に付け込んで攻撃される。この傾向は2018年調査時点でも存在していたが、今回の2020年調査においてより顕著となってきている。

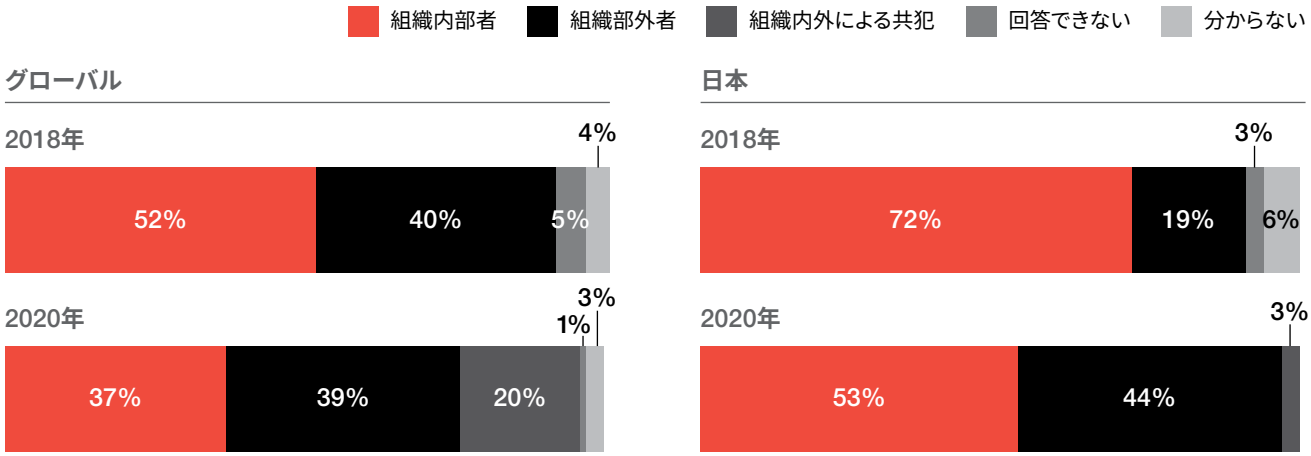
また、組織の内部者と外部者が共犯して関与している犯罪の割合は、日本では3%であるのに対して、グローバルでは20%と非常に高い結果となっている。日本企業においては、組織の外部者と共謀する不正が非常に少ないといえるが、組織内外による共犯・共謀はどのようなリスクが潜んでいるのであろうか。

組織の内部者による不正は、権限集中により内部統制が無効化されたり、属人的な業務プロセスにより事後的な検証が不可能になることを悪用して行われることが多い。また、組織の外部者による不正は、ビジネスフロー上の欠陥（例えば、取引先など第三者（サードパーティ）管理や、物理的・IT面へのセキュリティ対策などの欠陥）が原因となるケースがある。

一般的に、経営者や管理者が不正目的のために内部統制を無視することは、「内部統制の固有の限界」として知られている。前述のような、組織の外部者（取引先の担当者など）に、組織内部から経営者などの役職者が加わって「共謀による不正」を行うと、内部統制の有効性がさらに低下し、不正の発見がより一層困難な状況となる。この点が、共犯・共謀による不正の厄介な特徴である。

共謀の結果としては、収益の期間帰属の意図的な変更（例えば、売上の前倒し計上）や、組織の財政状態または経営成績を偽るために仕組まれた複雑な取引（例えば、循環取引やスルー取引）などが代表例としてあげられる。また、共謀による「資産の横領・流用」は、組織が提供を受けていない財やサービスに対する支払い（例えば、架空の相手先に対する支払い、水増しされた価格と引き換えに売主から組織の購買担当者に対して支払われるキックバック）や、物的・知的財産の窃盗・窃用（組織の競争相手と共謀して報酬と引換えに技術的情報を漏らすこと）などが挙げられる。

図表12：不正への主な関与者は外部か内部か



※構成比は小数点以下第1位を四捨五入しているため、合計しても必ずしも100とはならない。

今回、日本の回答結果を見ると、外部との共謀のケースは少ないが、グローバルの傾向を見ると、日本でも外部との共謀のケースが今後増加していくことが予想される。そのため、組織はあらゆる角度からガバナンス体制の定期的な評価を行うとともに、取引先の管理（サード・パーティ管理）の徹底や内部通報制度の整備などを通じて、そうした不正の予防と早期発見の努力が必要である。

マネジメント関与の不正

内部主犯格の職階に関する特徴

経済犯罪・不正の主犯者の職階についてグローバルと比較した結果、マネジメント（中間・上級管理職）が主犯者の割合が、グローバルが約60％に比して日本では75％と高い結果となった。前回調査（2018年）では、日本でマネジメントが関与した不正は69％であり、前回調査と比べてもさらにマネジメントが主犯者である割合が増加している。

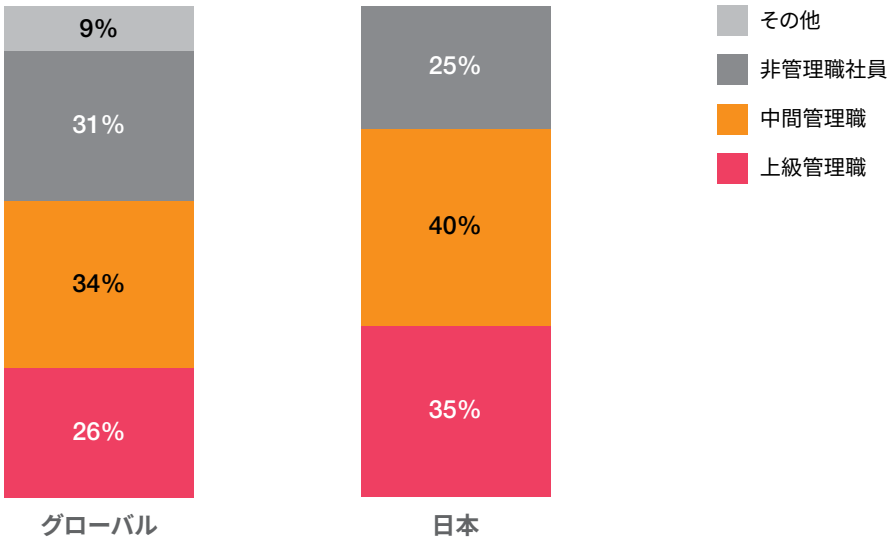
従前から、「海外に比べ日本では勤続年数が長く、年齢・職位が高い社員による経済犯罪が多い」という調査結果が出ているが、この傾向がより強くなった。マネジメントによる不正については、内部統制が有効に働かないことから防止・発見することが難しく、不正が長期にわたり行われることが多くなるため、被害額が大きくなるケースが多い。また、調査においても、社内調査ではなく、外部の調査委員を含めた客観的な調査が必要になるケースが多く、調査費用も高額になる傾向がある。

マネジメント関与の不正の抑止

マネジメントが関与する不正を抑止するためには、やはりガバナンスの整備が重要な要素になる。昨今トレンドとなっている社外取締役の選任により、経営に第三者の目を入れることはもちろんであるが、特定の人員に権限を集中させていないかを、定期的に確認することも重要である。具体的な方法として、会計監査や税務調査への誠実な対応や、社内外の通報や相談体制の充実が考えられる。これらは、組織に「第三者の視点を受け入れる風土」があることの裏返しであり、経営トップが日ごろから発するメッセージや態度で醸成される。経営層が自らチェックの目を受け入れる体制を作ることが、経営者による不正の減少に資するだけでなく、中間管理職含むマネジメント層全体のモラル向上にもなる。

また、内部統制の拡充も必須要件である。一般的に不正は3段階のディフェンスライン（現場レベル、管理部門レベル、内部監査などの独立的な部門レベル）で予防の設計図を描く。各層のディフェンスラインでどういったモニタリングを行っているか、何が漏れているか、具体的なリスクが今後組織のどの箇所に潜んでいるかを、昨今の組織を取り巻く状況や業界の動向なども勘案したうえで、該当リスクに対する最適な統制活動を定期的に見直したい。各層のディフェンスラインでの統制に、さらなる有効性の向上を図るための発見的統制として、データ分析や異常値検知などのテクノロジーの力を用いることは、特に人的リソースの確保や意思決定の速度に苦慮する場合に有効である。各種内部統制制度の要請に従い、既存の仕組みが整っている日本企業においては、定期的な評価・検証の際に、発見的統制の充実という観点からも検討するとよいだろう。

図表13：不正に関与した内部者の職階レベルは？



3 増加するサイバー犯罪

サイバー犯罪と想定される被害

サイバー犯罪と想定される被害

第1章で、日本ではサイバー犯罪が増加していると述べた。ところで「サイバー犯罪」と聞いて具体的に何を思い浮かべるであろうか？　日本ではネットワークやコンピュータを利用した犯罪を「サイバー犯罪」と呼んでおり、次の3つに分類される。

不正アクセス行為

他人のアカウントを用いたアクセス、システムの脆弱性（セキュリティホール）を用いた他者のコンピュータへの侵入など

コンピュータ犯罪

データの改ざん、マルウェアの配布など

ネットワーク利用犯罪

違法薬物や他者の著作権物の販売、特定個人の中傷、わいせつ画像の頒布など

さらに、重要インフラなどの機能不全を起こす「サイバーテロ」や、組織の機密情報を窃取する「サイバーインテリジェンス活動」なども含めて、「サイバー攻撃」と呼ばれることがある。本章ではこれらを総称して「サイバー犯罪」と呼ぶことにする。

組織に対してサイバー犯罪の被害を受けると、多大な経済的損害が発生し、場合によっては組織の存続にも関わる事態にも発展し得る。組織が巻き込まれるサイバー犯罪として、例えば次のような例が挙げられる。

- 外部の犯罪集団による組織内ネットワークへのサイバー攻撃を受け、社内資料や提案書類の他、取引先の情報が流出した可能性が発覚。情報管理への信頼を失い、受注額が大幅に減少。
- 業務委託先の従業員が顧客の個人情報を窃取。顧客にダイレクトメールが送り付けられたことから発覚し、ブランドの信頼が失墜。売上が大幅に減少。
- ランサムウェアに社内の多数のコンピュータが感染。データを人質に身代金を要求され、最終的にデータが消失。業務プロセスが麻痺。
- インターネットショッピングサイトに大量のアクセスを行うことでサイトがダウン。攻撃を受けている間は注文を受けることができず機会損失が発生。
- 自社が製造・販売する機械にスマートフォンから侵入して不正な操作を行うことができる、セキュリティ上の欠陥が発覚。プログラムを外部から修正できる設計になっていなかったことから、機械を回収してのリコールが必要になり、多額のリコール費用が発生。
- 取引先から支払の振込先口座が変更になった旨のメールを受信したため、指定された口座に代金を振込。その後、取引先から支払いがなされていないとの連絡があったためメールを改めて確認したところ、振込先口座変更のメールは取引先からのメールを巧妙に真似た詐欺メールだった。

サイバー犯罪は不特定多数を狙ったものだけではなく、特定の企業の特定の部署・人を狙ったものもある。人間の心理的な隙や行動のミスに付け込んで秘密情報を得る「ソーシャルエンジニアリング」の手法（例：役員を名乗って従業員に電話をかけて情報を聞き出す、捨てられた紙資料から情報を盗み見る）も駆使しながら事前に入念な調査を行い、取引先や関係者からのメールを巧妙に真似て、ウイルス入りのメールを開くように誘導したり（標的型攻撃）、金銭の振り込みを要求したり（ビジネスメール詐欺）する手口が近年増えている。これらは周到に準備されていることから、このような手口があることを知らないと見抜くのが難しい。

さらに、自社が被害者になるだけではなく加害者になる例もある。自社のコンピュータがマルウェアに感染し、他社への攻撃の踏み台として利用された場合、自社のコンピュータが他社を意図せず攻撃することになる。

このようにサイバー犯罪は多岐にわたり対策方法も異なるため、全てのケースに備えた対策を整えるのは困難である。しかし、コンピュータやネットワークの利用が必要不可欠となっている現代においては、組織が事業活動を行う上でサイバー犯罪への対策は必要不可欠である。また、サイバー犯罪は対策が不十分な点を突いて狙われることから、全ての従業員・役職員が情報セキュリティについての十分な知識を持つように継続的な教育を行うほか、テクノロジーの力を積極的に利用して対策を行うのが望ましい。

「サイバー犯罪」における不正関与者

組織外部者によって行われた不正関与者の詳しい調査に関しては、日本では「ハッカー」が47％と1位である。対して、グローバルでは「顧客」が1位（26％）で、「ハッカー」は2位（24％）であった。

テクノロジーの進歩は目覚ましいものがあり、新たなサイバー攻撃手法が次々と編み出される中で、それを100％未然に予防することは不可能に近い。

しかしながら、例えば従業員に対してフィッシングやマルウェアによる攻撃に引っ掛からないよう教育・研修を徹底したり、万が一攻撃に遭った場合に素早く検知するためのシステムに投資することやシステム専門部署に高度な専門知識を持った人材を採用すること、あるいは外部の専門業者と平時から密にコミュニケーションをとり、事案が発生した場合に調査および対応を迅速に依頼できる体制を整備するなど、できる限りの手だては打っておくべきであろう。

図表14：不正の外部関与者の内訳は？

グローバル			日本		
1位	顧客	26%	1位	ハッカー	47%
2位	ハッカー	24%	2位	顧客	29%
3位	ベンダー・サプライヤー	24%	3位	競合他社	24%

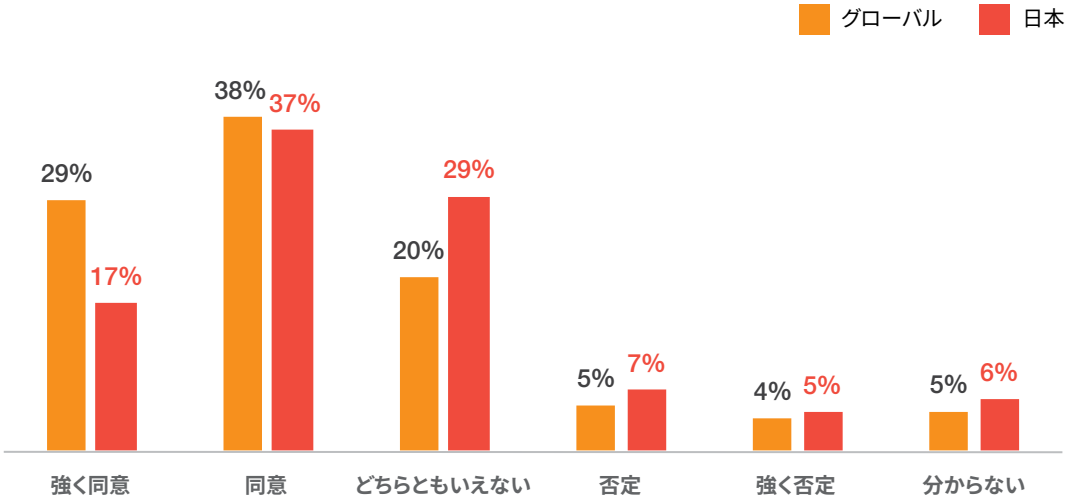
サイバー犯罪を予防するために

テクノロジーは、サイバー犯罪を防ぐ手段の一部に過ぎない

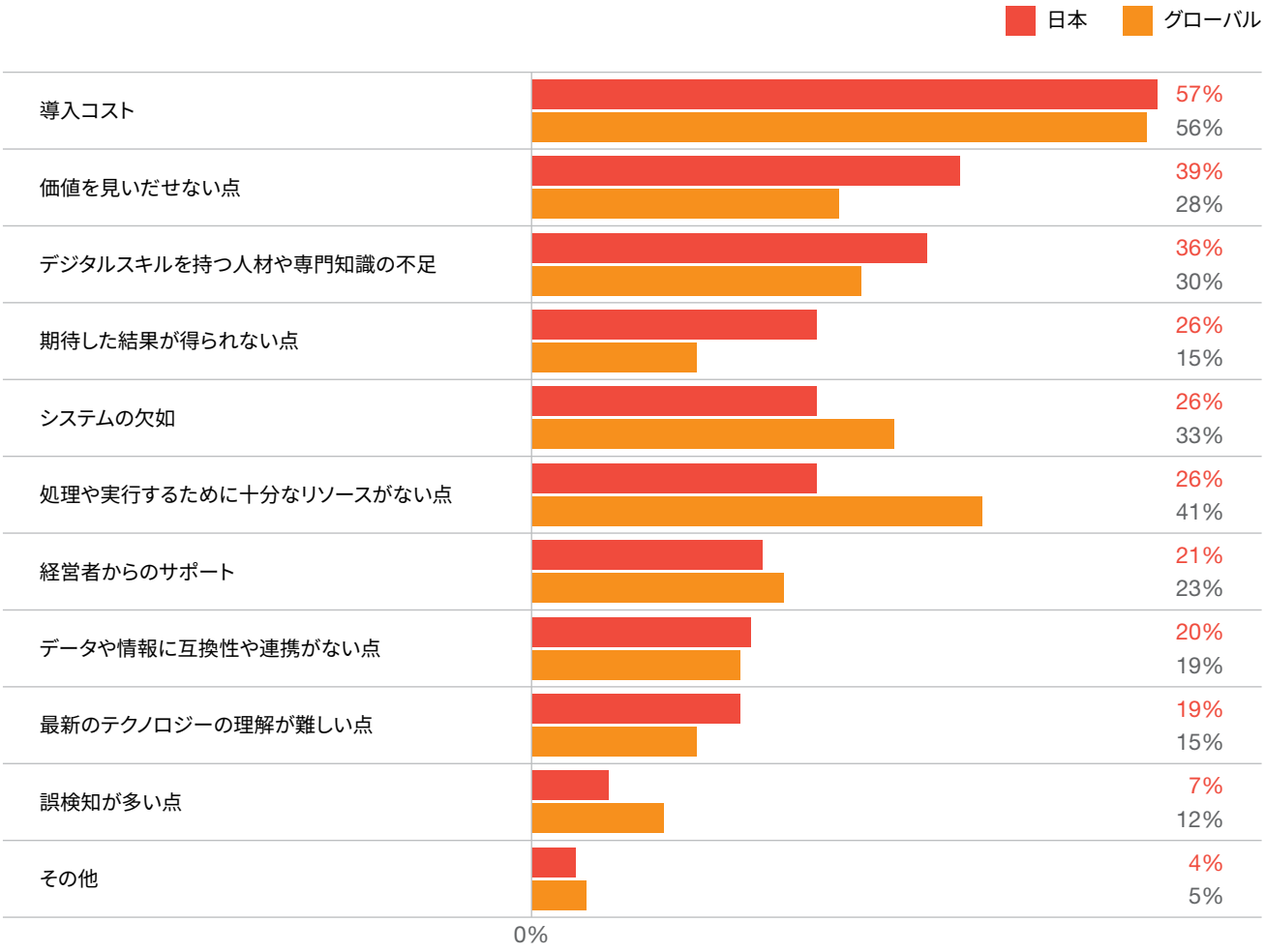
近年、サイバー犯罪のリスクや対策用のツールに関する認識が徐々に高まってきていることに伴い、多くの組織が新しいツールやテクノロジーに多額の投資を行ってきた。一方で、今回の調査で回答した多くの組織は、テクノロジーの利用に対して懸念を抱いていることも、下記のような設問の回答より判明した。

- サイバー犯罪対策のためにテクノロジーを導入またはアップグレードができたと強く感じているとの回答は、グローバルでは30% 弱にとどまり、日本ではわずか17%であった（図表15）。何がテクノロジーの導入やアップグレードの障害となっているかという質問に対しては、グローバル、日本ともに導入コストが障害となっているとの回答が半数を超えた。それ以外にも、リソースやシステムの不足、デジタルスキルを持つ人材や専門知識の不足が障害となっているとの回答も多かった。また、価値を見いだせないとの回答が、日本で約40%、グローバルでも約30%あり、サイバー犯罪対策のためのテクノロジーに投資する価値を見いだせないとする回答者が一定数いることが分かった（図表16）。
- 人工知能（AI）は近年さまざまな分野で使われている。これをサイバー犯罪対策のために使用している組織は、日本・グローバルとも25% 前後に過ぎない。また、人工知能を使用していると回答した組織のうち40% 近くは、価値を見いだせていない（図表17）。

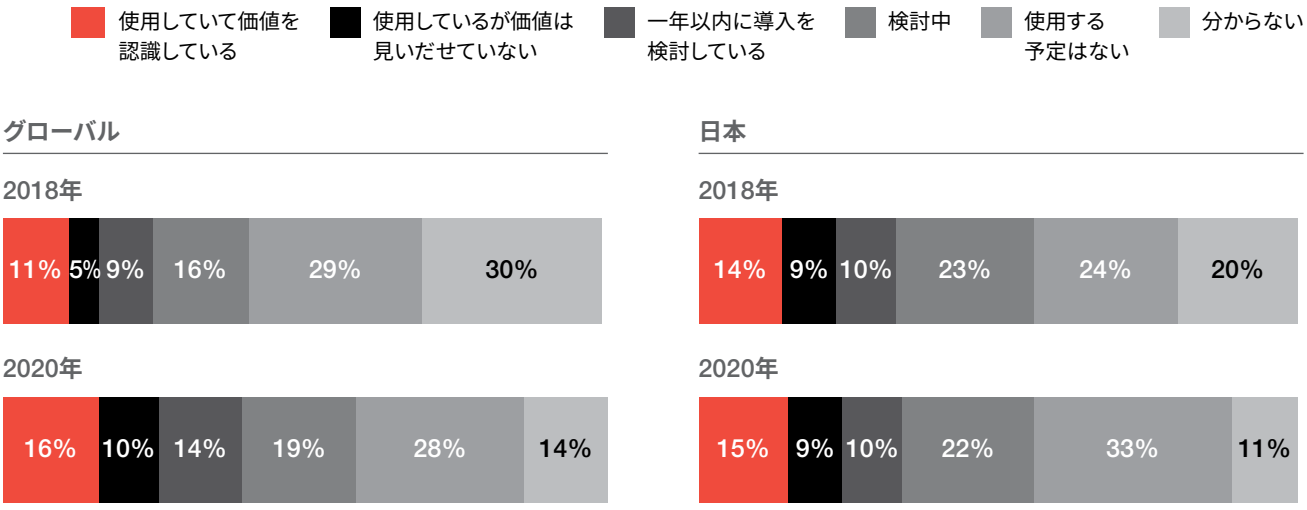
図表15：過去2年間の不正対応を経て、「サイバー犯罪対策のためにテクノロジーを導入またはアップグレードができた」という点についてどの程度同意するか



図表16：テクノロジーの導入やアップグレードを妨げているのは何か？



図表17：AIの導入に関して組織としてどう考えているか



※構成比は小数点以下第1位を四捨五入しているため、合計しても必ずしも100とはならない。

単一のツールや技術だけでは、サイバー犯罪防止プログラムとして十分とはいえない。データ分析をサイバー犯罪防止プログラムだけでなく、組織内の各種オペレーションや統制活動に取り入れている組織があるが、ここで以下のような論点が盛り込まれているかを確認し、分析手法も見直したい。

- 適切なルールおよび要件に基づいてデータを収集しているか
- 収集したデータをどのように分析しているか
- 分析における発見事項をサイバー犯罪防止プログラムにフィードバックし、サイバー犯罪防止プログラムをより頑強なものにしているか

組織内に、これらの問いに対応、管理するための適切な資源や専門知識を持つ者がいない場合、テクノロジーの価値を見落としてしまう。

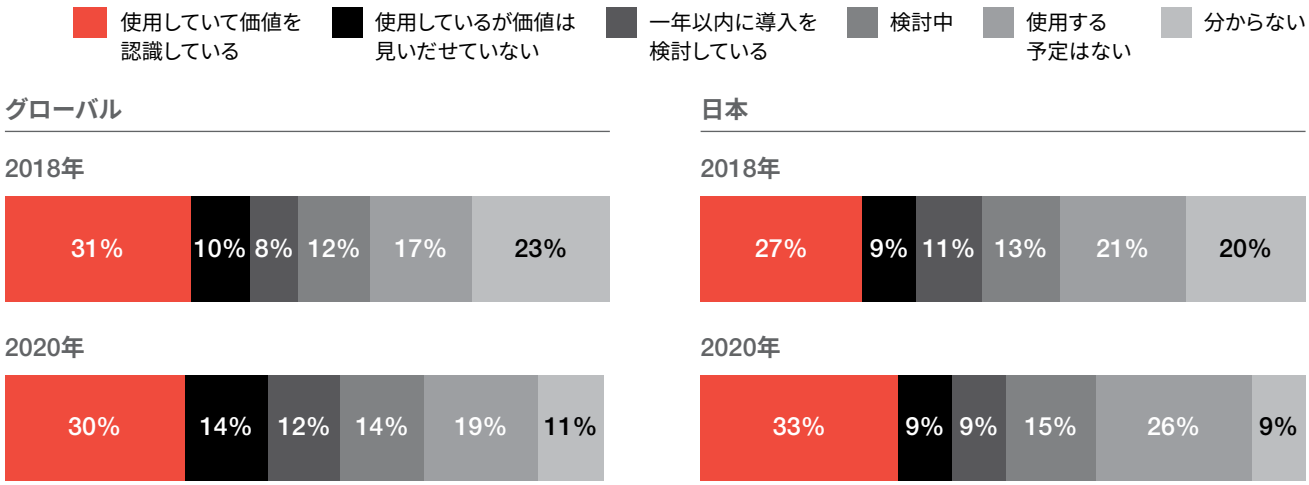
サイバー犯罪を防ぐには、新しいツールやテクノロジーを導入するだけではなく、実際にそれらを使いこなす必要がある。これには高度な専門知識が必要であり、平均的なITエンジニアを担当者に選任したとしても、能力不足であるケースもある。常任の専門家を雇用することが困難な場合は、外部の専門家を積極的に活用することで効果的な対応が可能になる。コミュニケーションモニタリングを導入することに対する組織の回答（図表18）も前回調査と比較するとポジティブな回答がみられ、いわゆるリスクモニタリングとして、組織にまつわるコミュニケーション（社内外・SNSなど）を監視し、不正の兆候について確認のスピードやその質を高めることも可能だ。サイバー犯罪の抑止だけでなく、競争法違反やその他さまざまな従業員不正の発見にもつながる可能性がある。

一方で、サイバー犯罪による被害が顕在化しない限り、テクノロジーの導入に十分な予算を割り当てる社内のインセンティブが働かないことも多く、設備投資を行う価値を見いだせないことがテクノロジーを導入していない理由の一つだと考えられる。しかし、現実には外部からの不正アクセスといったサイバー犯罪は組織の規模を問わず常に行われている。特に防衛機密など重要な情報に対しては、潤沢な資金と多数の専門家を抱える犯罪集団や他国の軍隊などが組織的に攻撃を行うという事例もある。また、特定の組織の情報を狙って、サプライチェーン内のサイバー犯罪対策が不十分な他社を使って間接的に攻撃を行うというケースも考えられる。

サイバー犯罪の被害を受けたときの経済的な損害が甚大であることを考えると、人とテクノロジーの両面で普段からサイバー犯罪対策に投資を行う方がはるかにコストは低い。サイバー犯罪対策にはさまざまなものがあるが、下記に一例を挙げる。

- サイバー犯罪の予兆（ブロックした不正アクセスの件数・不自然な大量のデータ転送等）を定期的に告知し、サイバー犯罪が身近に起こり得ることを従業員・役職員に認知させる。
- サイバー犯罪に関する訓練を行う。簡易的なものでは、ビジネスメール詐欺に使われる類のメールを社内向けに発信し適切に対応されるかを追跡する方法がある。高度な機密を扱う組織の場合は、外部の専門家（レッドチーム）による疑似攻撃テストを行うことも考えられる。
- 万全の対策を行っていても、サイバー犯罪を100%防ぐことは不可能である。システム障害、情報漏洩等が起きたときに行う手順を事前に策定する。これには関連するログの保全、社内での報告体制の確認のほか、社外に向けた情報発信も含む。

図表18：コミュニケーションモニタリングの導入への組織としての態度



※構成比は小数点以下第1位を四捨五入しているため、合計しても必ずしも100とはならない。

4

日本企業が取り組むべき不正対応

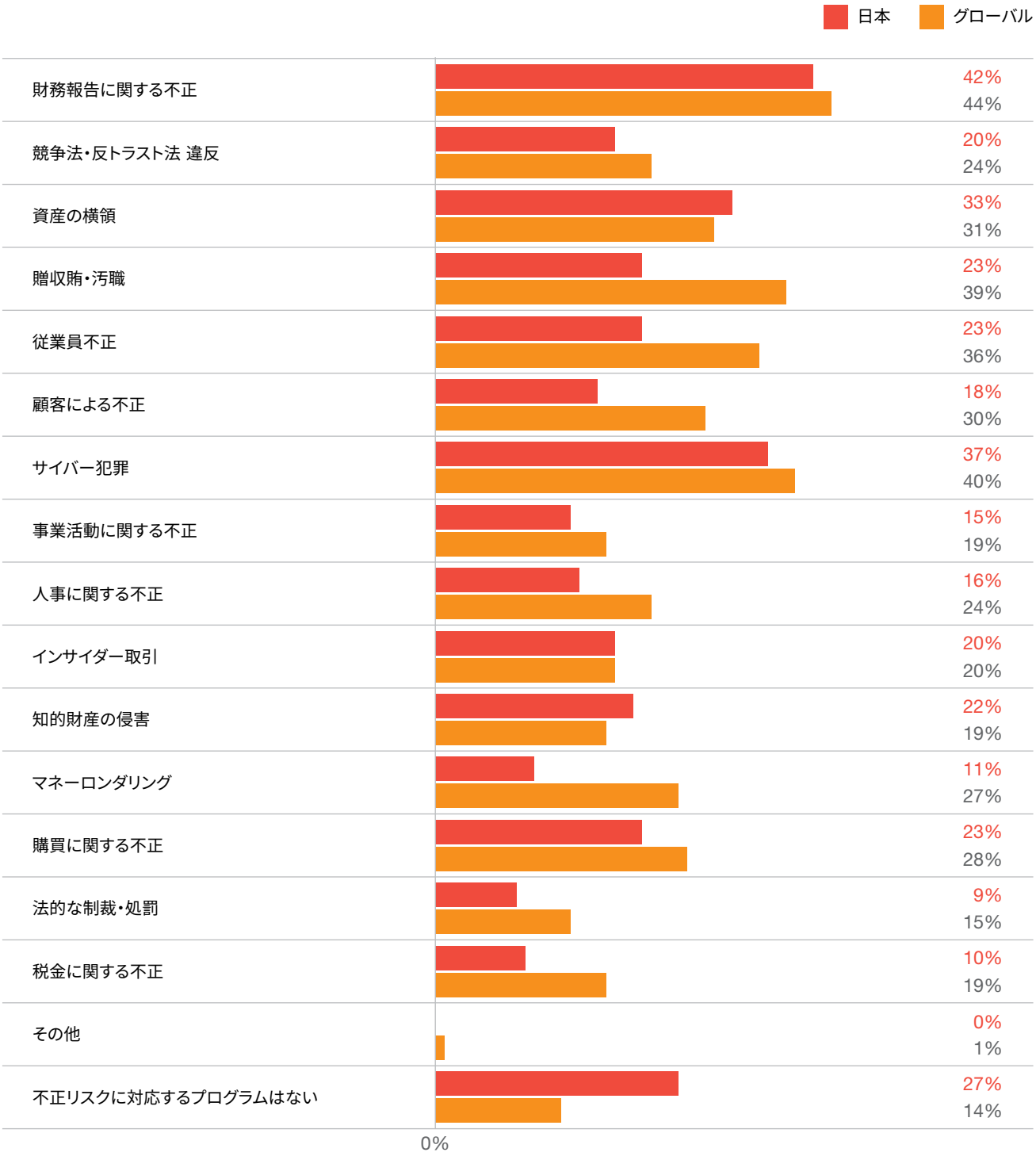
リスクの認識と対応の現状

多くの会社が潜在的な不正のリスクへの認識を持つ、または実際に不正事案に直面する一方で、そうした不正リスクに見合った態勢の構築など、「リスクに備えた準備」はできているのだろうか。

例えば、今回の調査では、社内で贈収賄・汚職に関する不正が実際に発生したと報告した日本企業は25%で、前回調査から大きく増加しており、グローバルの割合（30%）と比較しても大差ない。そのような状況において、80%近い日本企業が、「贈収賄・汚職リスク防止に関するコンプライアンスプログラムが整備されていない」と回答している（図表19）。また、「顧客による不正」に対応したプログラムが「ある」と回答した日本企業は18%と、グローバル回答（30%）との差が大きい。同じく、今回最も被害として顕著だったサイバー犯罪についても、グローバル、日本ともに半数以上の組織が、同領域に特化した対策を講じていない結果となった。さらに、コンプライアンスプログラムが全くないと回答した日本企業は約30%と、グローバル比較で倍近く多い。特に、偽造クレジットカードの使用やローン借入の際の情報詐称などの「顧客による不正」については、日本で被害にあった会社が前回調査時（2018年）から3倍（11%→33%）に急増しているため、新たな不正への対応策を講じることは、組織にとって喫緊の課題である。特に、技術の進歩や手口の巧妙化に伴い、クレジットカードなどの偽装やインターネットを経由した詐欺行為は今後増えていくと考えられ、不正の予防や検知のハードルも高くなっていく一方である。そうした中でも、金融や不動産の取引においては、取引時の顧客および取引目的の確認を徹底することで、不正をある程度未然に防ぐことができる。また、インターネットを介した取引についても、認証ステップを強化するなどの工夫が不正リスクの軽減には有効的だと考えられる。

少なくとも年に一度は組織として不正リスク評価を行い、自社を取り巻くさまざまな不正リスクの把握と、それに対応する施策の策定および見直しを実施する事で、常に自社の不正リスクを最小化する努力を行う事が肝要である。

図表19：次のリスクに対応するための不正対応プログラムが組織に存在すると回答した割合（%）

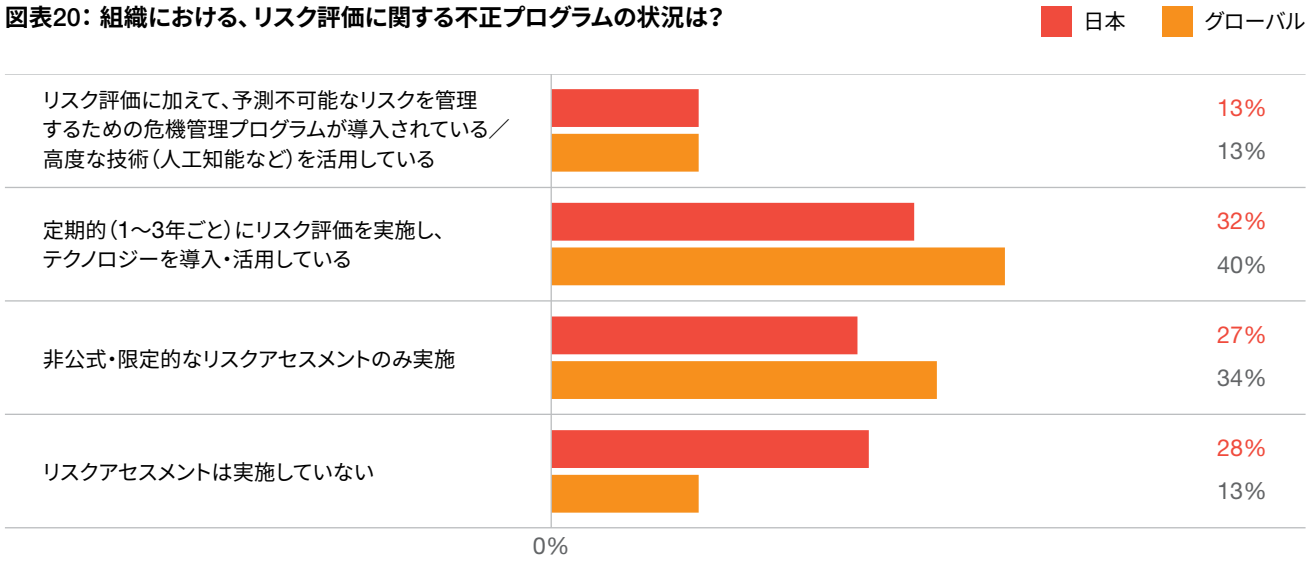


図表20の結果は、組織が抱えるリスクが必ずしも会社の体制および実態に反映されていない可能性を示唆している。原因と考えられることは、まず、不正リスクの評価が十分できていないことが挙げられる。今回の調査では、多くの日本企業が、自社における不正リスク評価を「行っていない（28%）」、または「非公式かつ限定的にしか行っていない（27%）」と答えている。一方、正式なリスク評価体制に基づく評価に加えて、テクノロジーを駆使した潜在的なリスクの管理を行っているという会社はグローバル、日本ともに13% にとどまった。

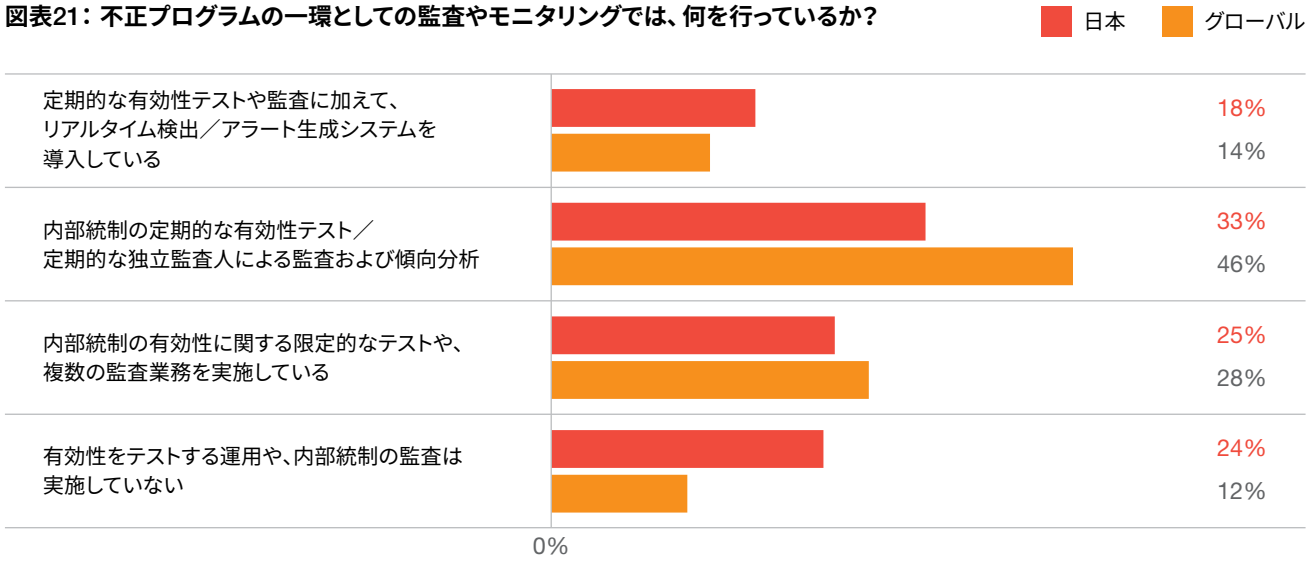
組織が抱えるリスクとリスク対応のずれが生じている原因のもう一つは、実際のオペレーションにおける自社の内部統制状況およびその効果が十分に把握されていない点だと考える。グローバルの倍の約24% の日本企業が、コンプライアンスに係る社内統制の運用に関するテストや監査を「全く行っていない」と回答している。また、限定的にテスト・監査を行っている組織（25%）と合わせると、約半数（49%）に上る。

当然、限られたリソースで全ての不正をカバーする網羅的かつ十分なコンプライアンス体制を構築するというのは現実的ではない。自社の事業内容、業界、ビジネスモデル、主要活動拠点などの要素を総合的に判断し、各種不正リスクの洗い出し、および既存の不正防止プログラムの有効性のテスト、見直し、改善を定期的に繰り返すことにより、リスクベースでより賢く、効率的かつ最大限の備えをしよう。

図表20：組織における、リスク評価に関する不正プログラムの状況は？



図表21：不正プログラムの一環としての監査やモニタリングでは、何を行っているか？



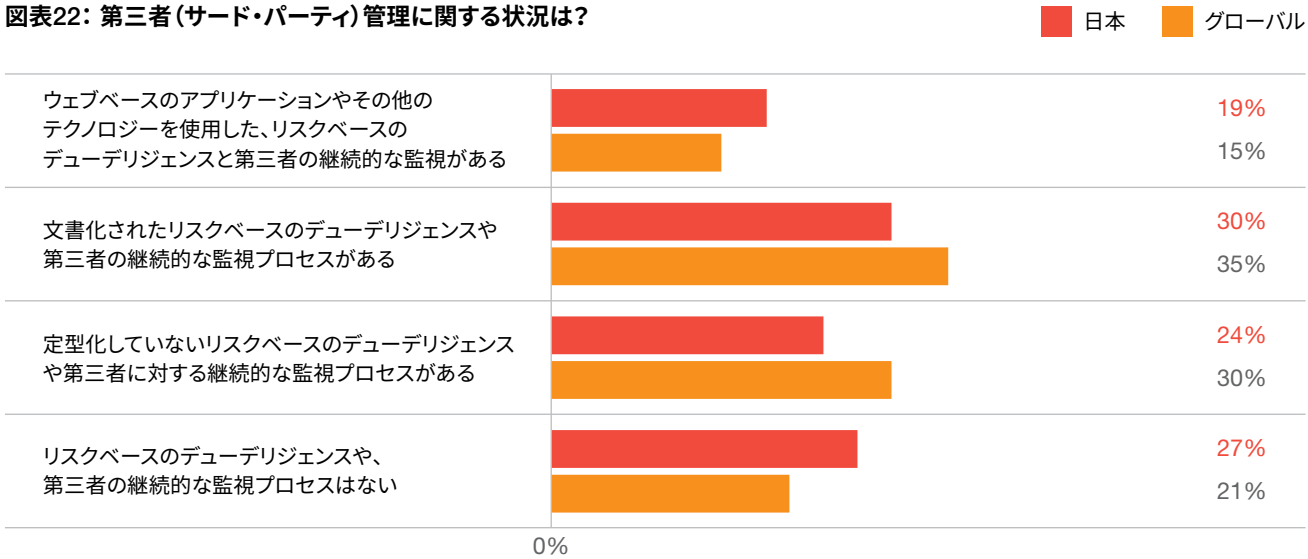
第三者（サード・パーティ）管理

多くの不正に共通するのは、取引先やベンダーなどの第三者（サードパーティ）の関与である。特に贈収賄のケースでは、自社従業員による直接的な贈賄行為より、自社のコンサルタントやエージェントなどが間接的に贈賄行為を行うことの方が圧倒的に多いということは今日一般的に認識されているだろう。また、循環取引やキックバックなどが原因の不適切会計も、取引先の協力を得て行われることが少なくない。サイバー犯罪では、取引先などの外部関係者を通じて情報の漏洩やハッキングの被害に遭うことも考えられる。

取引先との契約やベンダーなどの起用に際して、不正リスクを適切に把握するために事前のバックグラウンド調査および継続的なステータスの確認・更新を行うことで、上記のような取引先、特にコンサルタントやエージェントが絡む不正を未然に予防することが重要である。実際にサードパーティが関与する不正が発生した場合でも、そうした適切なサードパーティ管理は効果的な自己防衛策となる。例えば、贈収賄、マネーロンダリング、輸出入管理などに関する不正では、多くの国の規制当局が、バックグラウンド調査の実施や継続的なサードパーティモニタリングの有無およびその内容を、起訴や量刑判断、和解条件の決定に係る考慮要件としている。つまり、いずれの形にしても、コンプライアンス体制および不正防止を考える際には、十分なサードパーティ管理が必要不可欠なのである。

今回の調査では、サードパーティ管理について、約半数（49%）の日本企業が、自身の取引先（サードパーティ）に対して、テクノロジーを使用した体系的なリスクベースのデュー・デリジェンス（19%）や継続的なモニタリングを実施（30%）しており、その他24%が簡易的なデュー・デリジェンスおよびモニタリングを行っている結果となった。サードパーティ管理の重要性がある程度認識、反映される結果となっている。その一方で、約3割（27%）は全くサードパーティ管理を行っていないとの回答であった。当該結果は、グローバルと比較して大差はないが、日本企業が直面する不正リスクが多様化してきている昨今、効果的なサードパーティ管理は、組織として整備しなければならない基本的な要素であることを認識しなければならない。

図表22：第三者（サード・パーティ）管理に関する状況は？



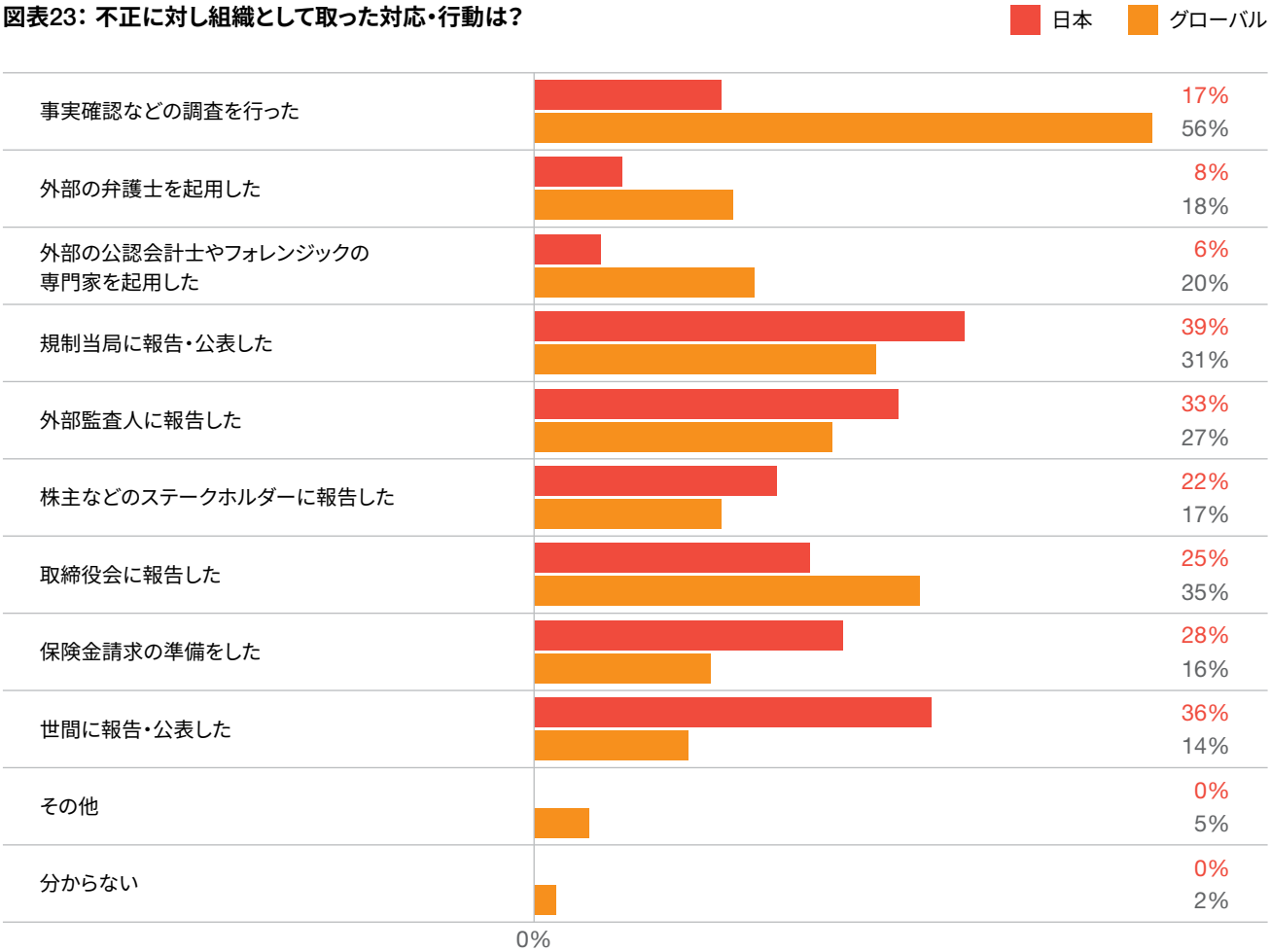
不正が発生した時の組織としての対応

初動対応

不正が起こった際に取った対応・行動に関する質問について、所管の規制当局（39%）、外部監査人（33%）、株主（22%）および世間（36%）に不正を報告・公表したと回答する日本企業は、いずれもグローバルよりも顕著に多い。一方で、事実確認などの「調査」を行ったとする日本企業は17%しかおらず、取締役会に報告した会社も25%で、グローバルと比較すると非常に低い。さらに、弁護士やフォレンジック、会計の専門家を起用した会社は10%に満たない。不正調査を行う場合、まず調査全体の枠組みを検討するために、ある程度の実態を掴むべく予備調査を行う事が多い。予備調査は、少人数で短期間で行うのが一般的であるが、日本では、社内の一部関係者（法務、コンプライアンス部門など）だけで担う場合が多い。しかし、特に過去に不正を経験したことがない組織では、予備調査の段階で何をすべきか明確でないまま調査を行ってしまい、逆に社内や対外的な対応で混乱をきたし、レピュテーションなどの2次的被害が拡大してしまうケースに陥ることも少なくない。初期の調査の段階で、本番の調査体制および各種ステークホルダーへの対応を見据えて、主要メンバーに専門家を入れ、戦略的な対策を講じることで初動失敗のリスクを軽減できる。

日本では、不正発生時に第三者委員会や特別調査委員会など、外部調査主体を起用するトレンドが目立ってきているが、本調査の段階になってから外部の専門家を起用するのではなく、平時の段階からこういった専門家とモニタリング体制などのアドバイスを得て、万が一の有事の際には即座にコンタクトし予備調査から関与させることは、こういった有事対応の失敗リスク軽減にもつながる。起きてしまった不正を、組織の未来のための「改善」のきっかけにするためにも、平時に行っている活動も見直したい。

図表23：不正に対し組織として取った対応・行動は？



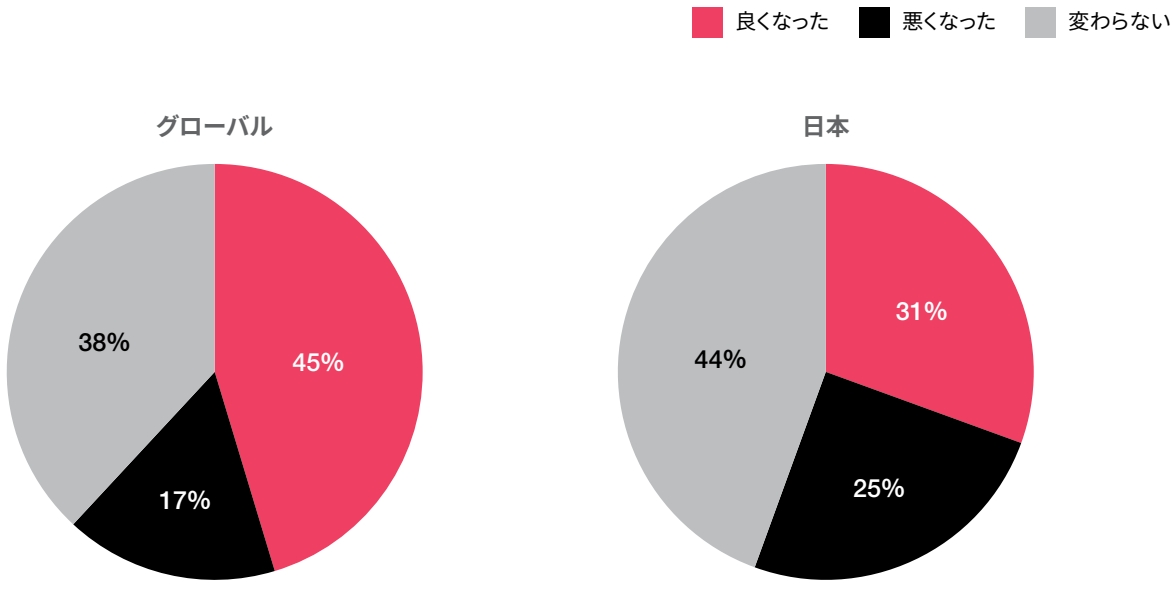
不正対応とその後

今日、不正に関しては、取引先や顧客、規制当局だけではなく世間の目も日々厳しくなってきている。それは、会社が被害を受けた立場（例えば、外部からのハッキング）であっても同様で、「情報の管理者」としての会社の責任を問われてしまう。また、不正発生時の初動対応の遅れは、直接的被害の拡大だけではなく、2次的、3次的な被害を引き起こしてしまう可能性もある。

一方で、不正への適切かつスピーディーな対応は、会社への被害を最小限に留めることはもちろん、長期的な企業価値やレピュテーション向上に資することもある。実際、今回の調査のグローバル結果では、不正事案を経験した会社の45% が、危機的状況を経て「会社がより良くなった」と回答している。日本企業で、危機的状況を経て「会社がより良くなった」と回答したのは31% であり、「会社の状況が悪くなった」と回答したケースは25%と、グローバルの17% に比し多い割合となった（図表24）。この差の原因は何だろうか。これまで本レポートで見てきたように、日本企業が「リスクに対する準備」として強化すべき点が明らかになった。すなわち、サードパーティ管理や、内部通報制度、サイバー犯罪に対するプログラムなど、「リスクに対する準備」の課題について、実際に不正が起こっていなくても、取り組むべき課題と認識するかどうかは、有事の際の「差」になる。万が一不正が発生してしまったとしても、起きた不正を多角的に調査・分析、組織の見直しから次につなげるというサイクルを今後より一層強化していけば、不運と見られていた不正は、組織としては変革のきっかけとなり得る。不正を経験してより強い組織となるためには、平時の準備と有事の際の迅速かつ的確な対応、そして適切な再発防止策の策定が非常に重要である。

自社のことを誰よりも一番知るのは会社であり、率いる経営者および働く従業員である。そして何よりも効果的な再発防止策は、会社が一体となった改善に向けた姿勢である。専門家を交えた不正調査による事実解明や原因分析に基づき、自社に最も合った有効的かつ戦略的な再発防止策の策定やコンプライアンス体制の見直しを行うことが重要である。不正対応に係るコストや罰金額の増加や日々厳しくなるステークホルダーからの期待などにより、不正からの立ち直りにかかる負担も増えてきている今こそ、危機的状況を乗り越えて成長した成功者となるために、会社を主体とする真の「有事・不正対応」の在り方を再考する絶好のタイミングではないだろうか。

図表24：危機を乗り越えて組織としてどう変わったか？



おわりに

今回の調査を振り返ると、日本企業が長年取り組んできた組織のコンプライアンスに対する努力が随所にみられる結果となったと評価することができる。

誰もがテクノロジーの力を誰もが等しく享受できる時代となり、事業や活動の幅が広がっている。一方で、テクノロジーを悪用した外部からの攻撃など、経済犯罪が多様化・複雑化することに伴い、組織として不正発生時により迅速かつ高度な対応が求められる時代となった。加えて、不正防止の観点からは、有事の影響範囲の予測が難しくなっている。ますます不確実性が高まる状況の中で、グローバル企業にとって、不正リスク評価を始めとした組織の多方面からのリスクの把握がより一層重要な要素となったことも、今回の調査で明らかになった。

不正行為の防止、発見、対処において、リーダーとしての役割はどこにあるだろうか。現時点で「最良の」不正防止プログラムや内部統制が存在したとしても、継続的に評価、見直しをする必要がある。犯罪の内容や方法が進化するのを見てきたように、組織、そしてそれを取り巻く人々を守るためには、「防衛策」も変わらなければならない。そして、その「防衛策」のベースにあるのが「不正行為を正当化しない文化」と「失敗を許容し次につなげる前向きな姿勢」である。こういった組織風土を確立するには、リーダーの姿勢が何よりも重要である。「Tone at the top（経営陣の姿勢）」はさまざまなところで謳われているが、リーダー自身が率先して「誠実で公正な姿勢」を体現し、それを全社員に広げていくことが、長期的には最善の「防衛策」となる。従業員のコンプライアンスに対する姿勢を人事評価に取り入れたり、コンプライアンス体制の強化に資するような働きをした従業員を奨励するような仕組みを取り入れたり、コンプライアンス部門や内部監査部門等、不正リスクと戦うリソースを増やす、不正の早期発見に資するデータ分析やモニタリングなどのテクノロジーに投資するなど、リーダーの本気度が客観的に測れるような施策を打つことが重要である。

私たちは組織の課題解決に向けた変革の基盤を築き、発展させていきたいと考えている。本レポートがこのような課題に取り組む組織の方々にとっての道標となり、より良い明日へのヒントにつながることを願っている。

2020年7月

大塚 豪
PwCアドバイザリー合同会社
パートナー

お問い合わせ先

PwC Japanグループ
https://www.pwc.com/jp/ja/contact.html

大塚 豪
PwCアドバイザリー合同会社
パートナー

池田 雄一
PwCアドバイザリー合同会社
パートナー

迫田 宜生
PwCアドバイザリー合同会社
パートナー

那須 美帆子
PwCアドバイザリー合同会社
パートナー

サイバーセキュリティについてのお問い合わせ先

外村 慶
PwCコンサルティング合同会社
パートナー

綾部 泰二
PwCあらた有限責任監査法人
パートナー

www.pwc.com/jp

電子版はこちらからダウンロードできます。www.pwc.com/jp/ja/knowledge/thoughtleadership.html
発刊年月：2020年7月　管理番号：I202005-08