「盲点」に潜む不正を探り出す

経済犯罪実態調査 2018

pwc

www.pwc.com/jp

概要

Didier Lavion
Principal, Global Economic Crime and Fraud Survey Leader, PwC 米国

不正や経済犯罪の被害を受けたことがある、と答えた組織はわずか49％。しかし私たちは、この数字はもっと高いはずであることを知っている。では、残りの51％はどうなのか？

目の前の不正リスクをしっかりと認識している企業があまりに少ない、というのが実情である。ゆえに、2018年の経済犯罪実態調査では、123の国と地域、7,200名以上から有益な情報を収集し、盲点に潜む不正を探り出すこと、そしてあらゆる組織が直面している極めて重要な戦略的課題に光を当てることを目標としている。

気付かなかった最大の競合相手

今日、不正への対応には大きな注目が集まり、中心的なビジネス課題となっている。たまたまあった悪事、コストのかかる迷惑事、単なるコンプライアンス上の問題―不正をこうした単独的事象と見なしていた時代はとうの昔に終わりを告げた。今日のデジタル社会では、不正の規模と影響があまりに巨大なものになっている。実際、それ自体を一つの巨大なビジネスのようなものとして見ることも可能である―テクノロジーを土台としており、革新的であり、日和見主義的で、波及力があるという意味で。不正を、これまで気付かなかった最大の競合相手と捉えるべきかもしれない。

こういう時代を迎えた理由を知るのは難しいことではない。テクノロジーが飛躍的に進化を遂げたおかげで、不正行為者は目標達成に向け、より戦略的で高度な方法をとることができるようになった。他方、世界の多くの地域で、規制体制はより強固なものとなり、取り締まりが強化され、国境を超えた規制当局同士の協力もしばしば見られるようになった。また、相次ぐ汚職その他企業スキャンダル報道を受け、世界中の人々の間で、透明性および説明責任に関する共通基準の確立に期待が高まってきている。

より多くの企業、組織や国家が、汚職と不正がグローバルな競争の妨げとなっていること、代償の大きさが無視できないレベルに達していることを認識しつつある。

さまざまなリスクへの直面

世間の目がこれまでになく厳しくなっている現在、今日の組織は、不正に関連するリスク―社内、社外、規制、評判に関する各リスク―というさまざまな危機的リスクに直面している。従って、今こそ、不正に関する新たな、より包括的な視点が必要である。すなわち、脅威の本当の姿―不正が事業上のコストであるばかりでなく、あらゆる地域、分野、部門に影響をもたらし得る「影の産業」であること―を認識する視点である。不正は盲点に潜んでいるので、不正に対する認識が欠如してしまうと、非常に危険な状況に陥る可能性がある。

従って、「あなたの組織は不正の被害を受けましたか」というのは重要な問いではない。むしろ、「不正が皆さんの組織にいかに忍び寄っているか、認識していますか」という問いの方が重要である。あなたの組織はそうした不正に目隠しをしたまま挑むのだろうか、それとも、しっかりと両目を見開いて立ち向かうのだろうか？

目に見えない不正は、目に見える不正と同様に重要である

調査結果では、経済犯罪の危険性に関する認識は高まっているものの、直面している各リスクについて十分認識している企業があまりに少ないことを示している。本レポートは、そうした認識のずれを埋めるために作成されたものである。その中で、企業が目に見える不正だけでなく、全体像を把握する妨げとなっている「盲点」を指摘するとともに、それらに対して何ができるか／すべきかを論じている。

不正により効果的に立ち向かうために、今日から始められるステップは何だろうか？

日本企業へのメッセージ

PwCが2年に一度、世界規模で実施している「経済犯罪実態調査」も今回で第9回を迎えました。時代とともに経済犯罪の傾向にも変化があり、それに合わせて調査項目や質問内容も変化させてきました。

特に近年は、マネーロンダリングや贈収賄・汚職といった規制当局の動きが活発な犯罪や目まぐるしい速さで進化するサイバー犯罪に関連する調査項目を増やしています。

これらの犯罪は、被害に遭ったときの損害額（調査費用や訴訟費用などを含む）が大きく、また、企業のブランドイメージを大きく毀損する恐れが高いことから、どのような業種の企業であっても、また企業の大小にかかわらず、防止に多大な力を費やす必要があると言えるでしょう。

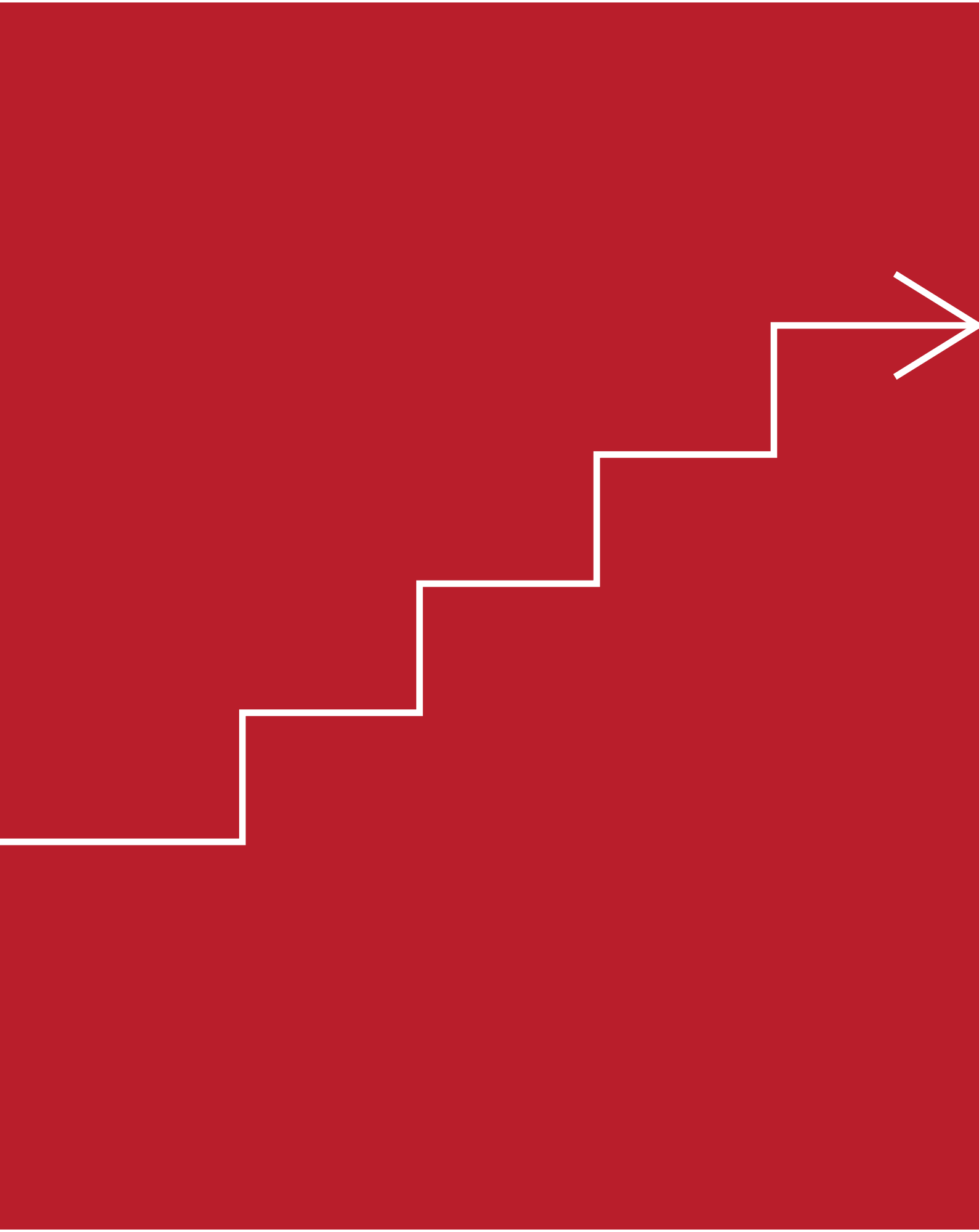
しかしながら、大きな経済犯罪や不正が起こっていない組織では、不正の予防に対してコストをかけることを惜しむ企業が多いのも事実です。今回のレポートでは、予防対策において最新のテクノロジーを活用することによるメリットおよびデメリットなどについても言及しています。

PwCがこれまでに行ってきた同調査で集積された情報と、不正に関する知見を基に作成された本レポートが、日本の皆様の経済犯罪・不正対策において少しでも有益な情報となれば幸いです。

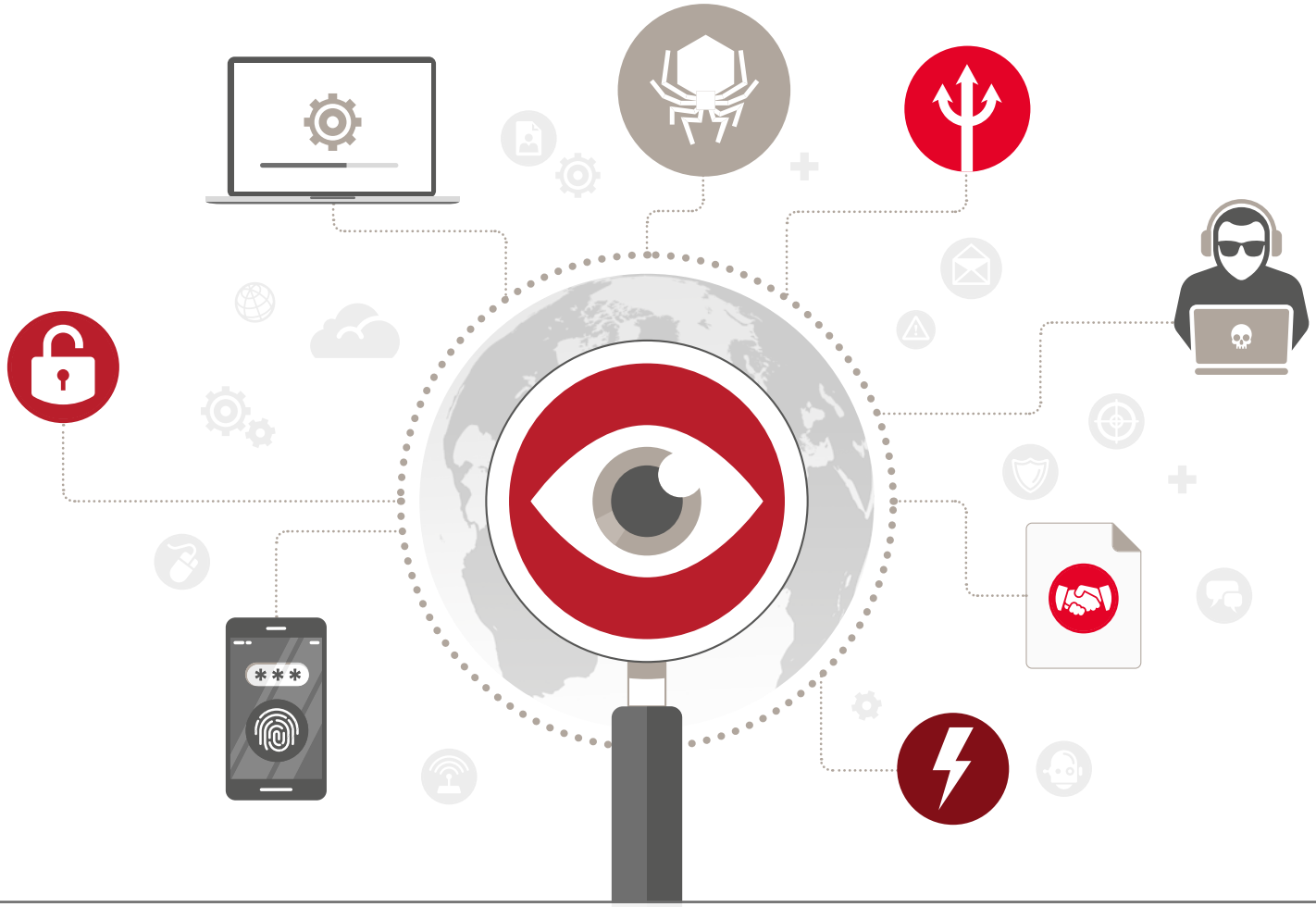
また、本調査をベースに特に日本（全回答数182名）に焦点を当て、日本を含むアジア太平洋地域の結果および世界全体の結果と比較した日本分析版を2018年7月ごろお届けする予定でございます。

大塚 豪
PwCアドバイザリー合同会社
ディレクター

不正に対応するための4ステップ



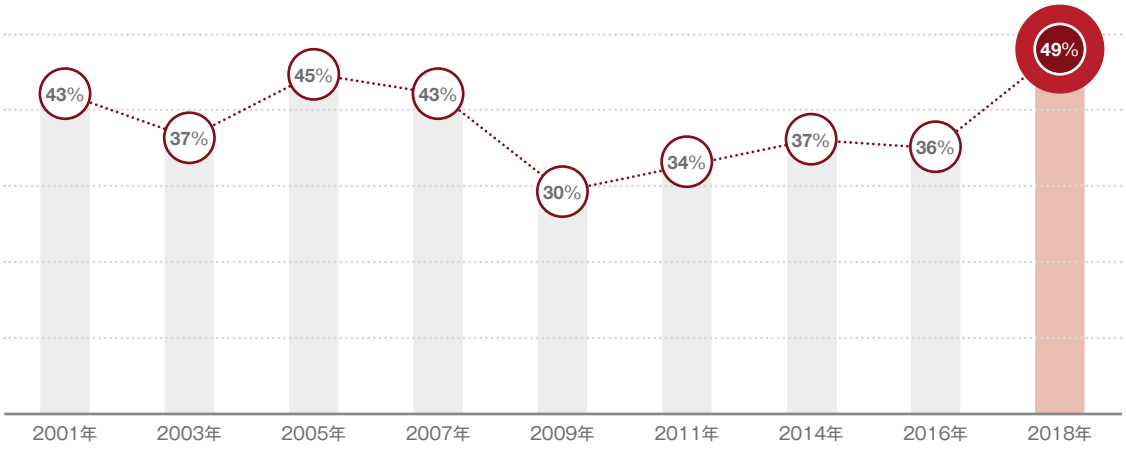
不正は認識されて初めて不正となる



不正は本当に増加しているのか—あるいは不正の認識度が高まっているのか?

2018年の調査において、不正や経済犯罪の被害を受けたことがある、と答えた組織は49%で前回(2016年)調査の36%から増加した。この結果は、世界規模で不正に関する認識が高まっていること、調査回答者が増えたこと、そして、「不正」という言葉の意味がより明確になっていることなど複合的な要因によるものと説明できる。しかし、どれほど警戒していようが、あらゆる組織は、「盲点」には弱いものである。そして、そうした「盲点」は通常、後になって気付くものである。しかし、できるだけ早期に盲点に光を当てることで、不正への対応力を大幅に高めることが可能である。

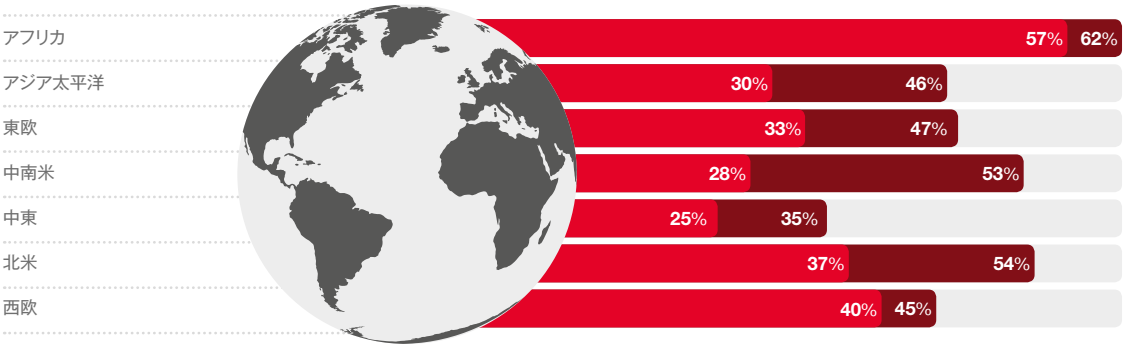
図表1:経済犯罪報告比率は増加傾向



Q. 過去24カ月以内に不正や経済犯罪の被害を受けましたか?

出所:PwC's 2018 Global Economic Crime and Fraud Survey

図表2:経済犯罪報告比率は全地域で増加



Q. 過去24カ月以内に不正や経済犯罪の被害を受けましたか?

出所:PwC's 2018 Global Economic Crime and Fraud Survey

今日の組織は、不正に関連するリスク—社内、社外、規制、評判に関する各リスク—さまざまな危機に直面している

2016年と比べて経済犯罪報告比率の増加とともに、企業の対策費用も増加している。

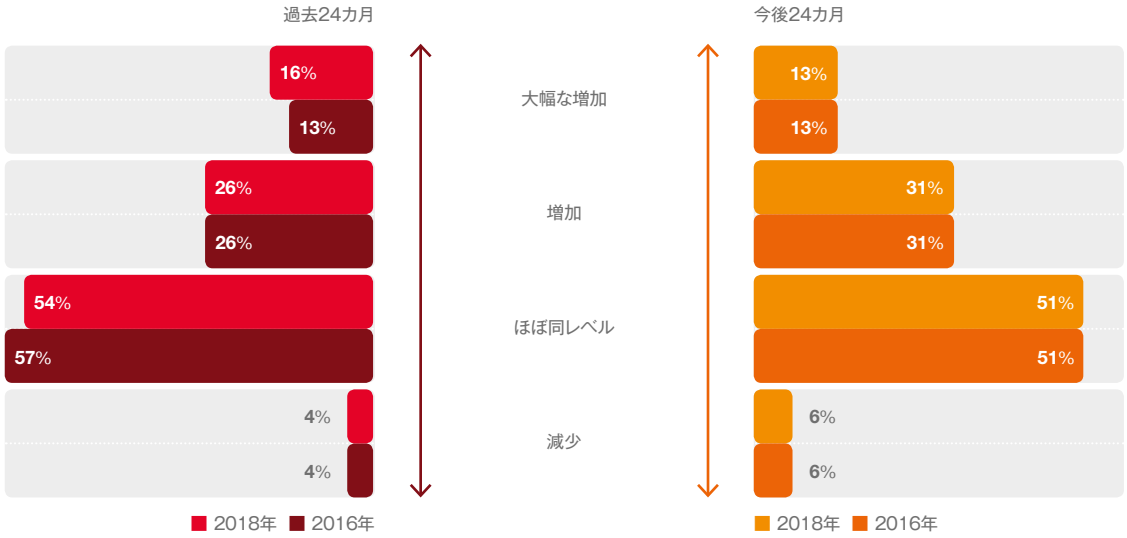
- 回答者の42％が、この2年間で自社の不正・経済犯罪対策費が増加した、と答えている（前回調査では39％）
- 回答者の44％が、今後2年間で同費用を増額する、と答えている

こうした費用は何に使われているのだろうか？組織は、不正に対応するために、これまで以上に強力なテクノロジーとデータ分析ツールを用いている。また、これらのテクノロジーベースの統制に加えて、多くの企業では内部告発プログラムの充実化を進めており、不正の対応について、経営陣へ適切な報告がされるための対策を講じている。

しかし、こうした方策は、不正・汚職に対するより積極的なアプローチへの真の移行を意味するのだろうか？あるいは、厳格化の進む贈収賄・汚職防止法や取り締まりのグローバル化に対する抵抗活動にすぎないのだろうか？別の言い方をすれば、私たちは依然として、不正への対応に不可欠な要素を手にしていないのではないか？

今回の調査結果から、私たちがその不可欠な要素をいまだ手にしていないということが強く示唆された。

図表3：組織は不正対策費を増やし続けている



Q. 不正や経済犯罪の対策費を調整しましたか／調整中ですか？

出所：PwC's 2018 Global Economic Crime and Fraud Survey

59%

のCEOが、あらゆる組織上の不祥事について、リーダーに責任を担わせるよう、組織に対する圧力が高まっていることに同意または強く同意している。

出典：PwC第21回世界CEO意識調査

71%

のCEOが、従業員と組織の上級管理職との信頼関係を図っている。

出典：PwC第21回世界CEO意識調査

不正リスク評価の実施が、不正がはびこる前に防止するための第1ステップ

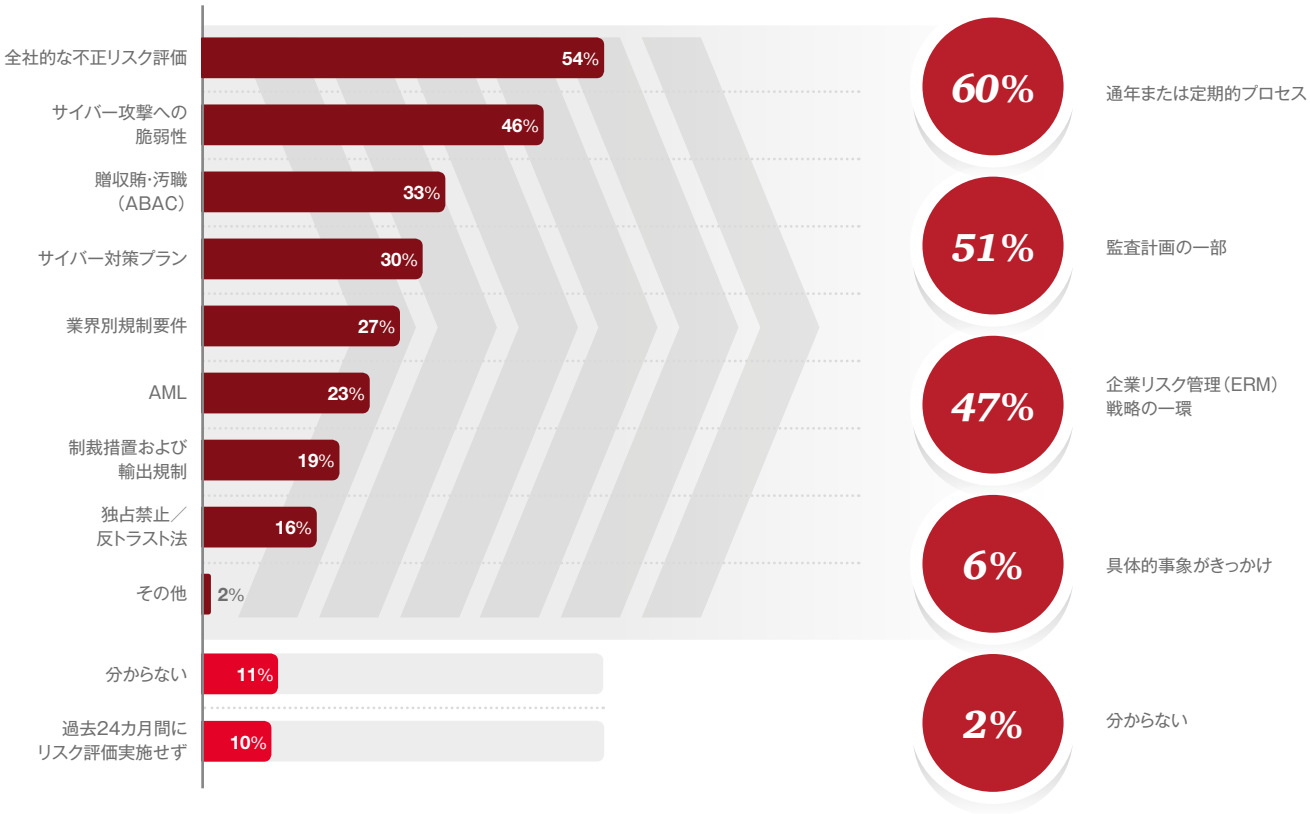
不正対策費は増加しているものの、多くの組織は依然として対症療法的・防御策的なアプローチで不正防止に取り組んでいる。

- 「過去2年間で総合的な不正・経済犯罪リスク評価を実施したことがある」と答えた組織はわずか54%
- 「サイバー犯罪リスク評価を実施した」と答えた組織は半数以下
- 贈収賄・汚職対策（ABAC）、マネーロンダリング対策（AML）、制裁措置、輸出管理といった重要分野でリスク評価を実施した企業は3分の1未満
- 回答者の10人に1人が「過去2年間でリスク評価を全く実施していない」と答えている

しかし、ビジネスのルールは大幅かつ不可逆的に変化している。企業や個人の不正行為に対して、世間は寛容でなくなっており、企業の不正行為に対して、世間の目はかつてないほど厳しくなっている。一部の企業やリーダーは、過去の行為―ビジネスに関する「暗黙のルール」が今とは異なっていた時代の行為―に対する説明責任も負わされている。PwCによる第21回世界CEO意識調査の結果は、このテーマの裏付けとなっており、「信頼」と「リーダーシップの説明責任」を事業の成長に対する2大脅威として挙げている。

これは、不正・経済犯罪が外部に漏れた場合のリスクがより高まっていること、また組織が、不正がはびこる前に先手を打ってそれを防ぐ必要があることを示している。不正リスク評価を行うことにより、懸念されている不正リスクを特定し、不正防止を図るのに役立つ。さらに、こうした評価を行うことで、規制当局による調査の際に企業の不正防止のための努力として評価されることが増えている。

図表4：過去2年間で、目標としたリスク評価を実施した組織は全体の半数



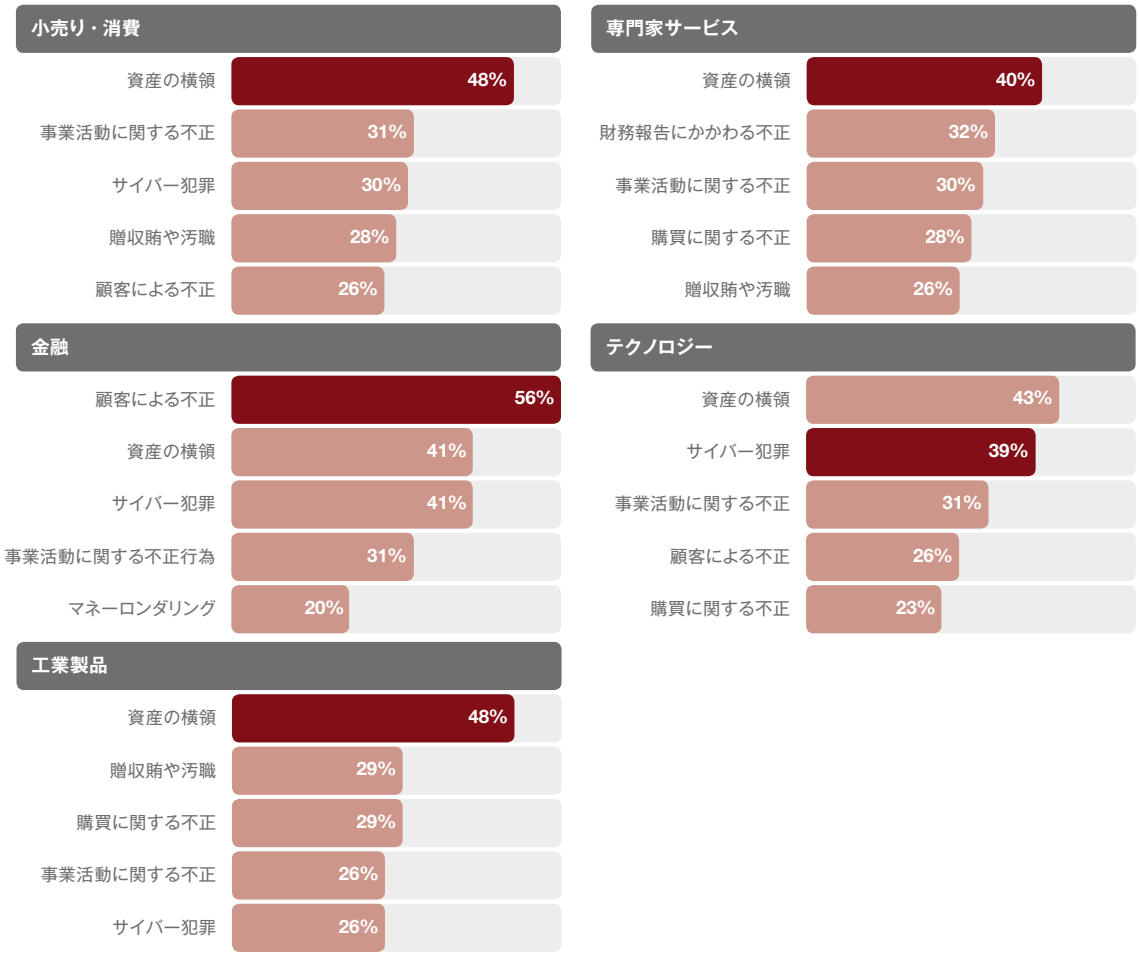
Q. 過去24カ月以内に、以下のいずれかの分野についてリスク評価を行いましたか？

出所：PwC's 2018 Global Economic Crime and Fraud Survey

Q. リスク評価を行った理由は何ですか？

出所：PwC's 2018 Global Economic Crime and Fraud Survey

図表5：全業界を通して最も報告頻度の高い不正は「資産の横領」、「顧客による不正」および「サイバー犯罪」



■ 最も致命的な不正として挙げられた回答

Q. 過去24カ月以内に自国で受けた不正や経済犯罪の種類は？

出所：PwC's 2018 Global Economic Crime and Fraud Survey

「コンダクトリスク」：多くの内部不正の背後にある「隠れたリスク」

今回の調査では、「顧客による不正」と「事業活動に関する不正」という二つの不正行為が大幅に増加してきていることを鑑み、この二つを別の脅威として新たに分類に加えた。過去2年間に自社が不正を経験した、と答えた回答者のうち、29％が「顧客による不正」、28％が「事業活動に関する不正」があったと答えている〔「資産の横領」（45％）、「サイバー犯罪」（31％）に続いて、最も報告頻度の高い不正の第3位、第4位となった〕。「資産の横領」の大幅な減少（前回調査では64％）の背景には、これら二つの不正が新項目として加わったことも一つの要因であることに注意が必要である。

これらの調査手法上の変更は、組織内部の不正リスクである「コンダクトリスク」の幅広いカテゴリーに対する認識が高まっていることを反映したものである。コンダクトリスクとは、従業員の行動によって、顧客が期待する公正な結果の達成や市場の健全性が損なわれるリスクを指す。そして、事業運営の機能不全や外部からの脅威（これらは内部統制によってチェック可能であることが多い）とは異なり、コンダクトリスクは、より包括的な対応および柔軟な姿勢が求められる。

現在、多くの企業が、コンプライアンス、企業倫理、企業リスク管理（ERM）を別々の部門で扱っており、一つの組織内部でそうした各部門が縦割り状態にあることも珍しくない。縦割り化した組織がほぼ全てそうであるように、これらの部門が戦略的に一つの状態としてまとまることはまれである。組織の中で、不正を調査する部門、不正のリスクを管理する部門、役員や規制当局に不正を報告する部門が全て別々という状態になっていることも珍しくはない。

そうなると、運営にもずれが生じて、不正も隠蔽されやすくなるか、しょせんひとごとと見なされるようになってしまい、不正防止の全体的効果、企業の業績や規制当局による評価に害を及ぼしかねない。

より革新的なアプローチは、こうした部門制がコンダクトリスクを生み出す要因であると考えて、見直しを図ることである。それにより、企業はコンプライアンス、企業倫理およびERMを横串で捉え、その評価や管理能力を高めることができ、戦略的意思決定プロセスにそれらを組み込みやすくなる。また、不正および倫理違反について、あらゆる組織が取り組むべき日常的事象として、より冷静で感情を抑えたアプローチをとることができる。コンダクトリスクに対しより体系的かつ現実的な対応を行うことで、倫理―不正―汚職防止コンプライアンスプログラム間のコスト効率化を実現することもできる。不正防止にかかわる主要部門間の縦割り状態を打破し、「盲点」に潜む不正を探り出す上で重要なステップである。

しかるべき場所で不正を探す

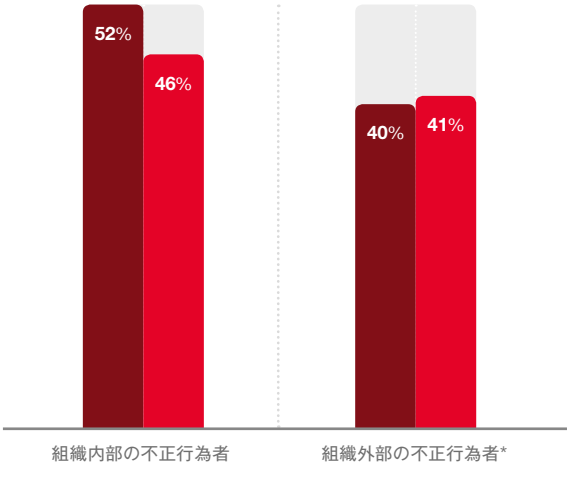
調査によると、組織内部の不正行為者による経済犯罪の割合がかなり増加している〔46%（2016年）から52%（2018年）〕。また、上級管理職による同犯罪の割合も大きく増加している〔16%（2016年）から24%（2018年）〕。実際、最も影響額が大きかった不正の行為者が組織内部の人物だったケースは、組織外部の人物だったケースの3倍に上る。

しかし、不正に関する企業最大の盲点―そして最大の脅威―が、従業員ではなく、取引先であるケースもしばしばある。すなわち、企業が日ごろビジネス上の関係性を有している第三者―代理人、業者、共同事業者、顧客など―である。言い換えると、一定の相互信頼性が見込まれている人や組織が、実際は、その企業に対して不正を働いている可能性もあるということだ。

24%

の組織内部の不正は上級管理職が不正行為者だった。

図表6：主な不正行為者は組織内部の人間



■ 2018年 ■ 2016年

Q. 最も致命的な不正の主犯は誰でしたか？

出所：PwC's 2018 Global Economic Crime and Fraud Survey

***68%**

の外部犯行者は、「友を装った敵」―代理人、業者、共同事業者、顧客―である。

ダイナミックな
アプローチをとる

CEOの説明責任

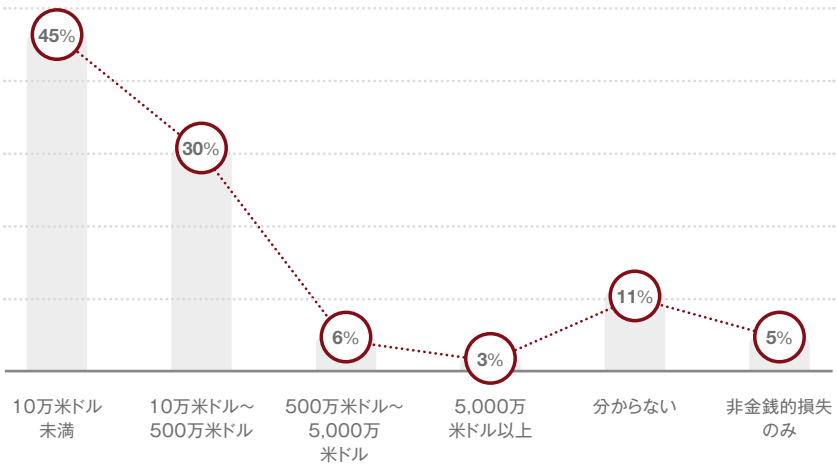
不正およびその後の影響による直接被害額が多額に及ぶ可能性があることは調査でもはっきりしている。しかし、二次的費用（調査その他の派生費用）を含めると、損害額全体が大幅に上昇する可能性もある。

46%

の回答者が、組織が不正により生じた直接損害額と同額またはそれ以上の金額を調査その他の派生費用に費やした、と答えている。

不正の損害が企業収益に影響を及ぼす場合、役員や株主が上級管理職に説明を求めるのは至極当然である。しかし現代社会において、リーダーの責任はそれで終わらない。実際のところ、説明は単なる始まりにすぎないのである。

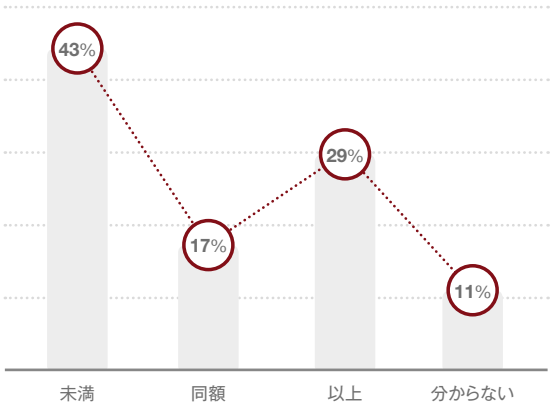
図表7：不正による直接的損害額は多額に及ぶ可能性がある



Q. 過去24カ月に発生した最も致命的な犯罪で被った推定直接損失額は?

出所：PwC's 2018 Global Economic Crime and Fraud Survey

図表8：不正の結果発生した調査費その他の派生費用も大きい



Q. 過去24カ月以内に発生した最も致命的な犯罪の結果、調査費その他の派生費用は、犯罪の損失額を上回りましたか／下回りましたか／同額でしたか?

出所：PwC's 2018 Global Economic Crime and Fraud Survey

CEOは、常に企業文化や事業運営に関するあらゆる側面を正確に把握していると見なされることが多くなっている。従って、企業倫理やコンプライアンスが崩れた時、CEOは、しばしば世間から（また規制当局から）個人としての責任を負わされる。不正で利益を得たか否かにかかわらず、経営陣はもはや「知らなかった」を言い訳にできなくなっているのだ。

調査によると、極めて深刻な不正事象の10件中9件が、上級管理職の耳に届いている。また、回答者の17％は、CEOが組織の倫理・コンプライアンスプログラムの一義的責任を負う、と回答している。これは、経営幹部がいかに危機を管理しているか、また彼らがリスク特性をどの程度適切にコントロールしているか（あるいはしていないか）を浮き彫りにするものである。

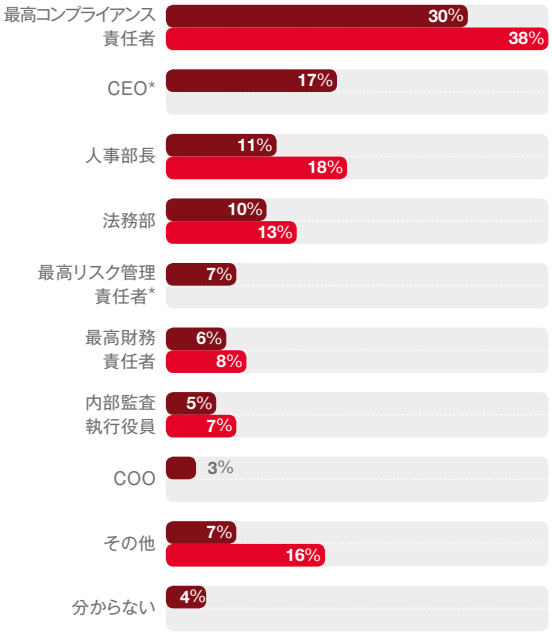
図表9：組織は、深刻な不正を上級管理職に報告している

■ はい ■ いいえ ■ 分からない

Q. あなたが答えた最も致命的な事案は、役員レベルまたはガバナンス担当役員まで報告が上がりましたか？

出所：PwC's 2018 Global Economic Crime and Fraud Survey

図表10：倫理・コンプライアンスプログラムの一義的責任は経営陣にある



■ 2018年 ■ 2016年

*2018年調査から加わった選択肢

Q. 組織において企業倫理・コンプライアンスプログラムの一義的責任を担っているのは誰ですか？

出所：PwC's 2018 Global Economic Crime and Fraud Survey

従来、不正の防止および発見は組織の第二次防御ライン―リスクマネジメント、法務、コンプライアンス部門などの役割―に属するものであったかもしれないが、現代の企業においては、新たに強化した不正防止策を第一次防御ラインに織り込んでいるケースが増えている。

これは、大規模な変化―不正の第一次防御・発見能力が成熟し強化していく大規模な変化の序章にすぎないのかもしれない。そうなれば、第二次防御ラインはより従来型の二次的アプローチであるガバナンスおよび監視、リスク許容度、枠組みおよび方針の設定などに移行することも可能である。

産業、テクノロジーおよび規制当局の境界線が曖昧になりつつある現代社会―不正行為者がこれまで狙ってきたセキュリティが高い金融機関ではなく、セキュリティの脆弱な相手を攻撃しようと探っている社会―において、これは重要な進展である。

「悪事千里を走る」:「評判の毀損」に関するリスクが「規制リスク」を上回る

社会における不正や汚職の捉え方に明らかな変化がでてきたのはここ数年のことである。また、調査データからも、私的・公的部門にわたり、世間と規制当局の両方から説明責任を求める声が強まっていることが分かる。これは、先進国に限られた現象でもない。世界のあらゆる地域やさまざまな文化圏において、透明性の基準や行動規範に関する基準が一つにまとまる兆しも見られる。

これまで法の支配や透明性が脆弱だった国家では、街頭で国民が怒りを爆発させるケースや、政治家やビジネスリーダーが投獄される光景が見られている。また、政府が転覆した例もある。

事態の断片的情報しか得ていない組織にとって、これは、深刻な評判の毀損リスクを意味する。適切な対応力を欠いていると認識された組織は、役員会で対応プランを練る間もなく、各方面から攻撃を受ける可能性がある。

図表11:不正の発見は第一次防御ラインに移行

1 経営管理

CEOおよび管理職は、リスクの管理責任を負うとともに、役員会によって説明責任を負わされる。

2 リスク部門

CROおよびリスク部門は、リスクを管理する責任を負わない。それはマネジメントの職務である。

3 内部監査

内部監査人は独立した立場からの監査責任を持ち、監査・リスク委員会に対する説明責任を持つ。

企業の評判には、管轄地域、法律または法の適正手続きは関係ない

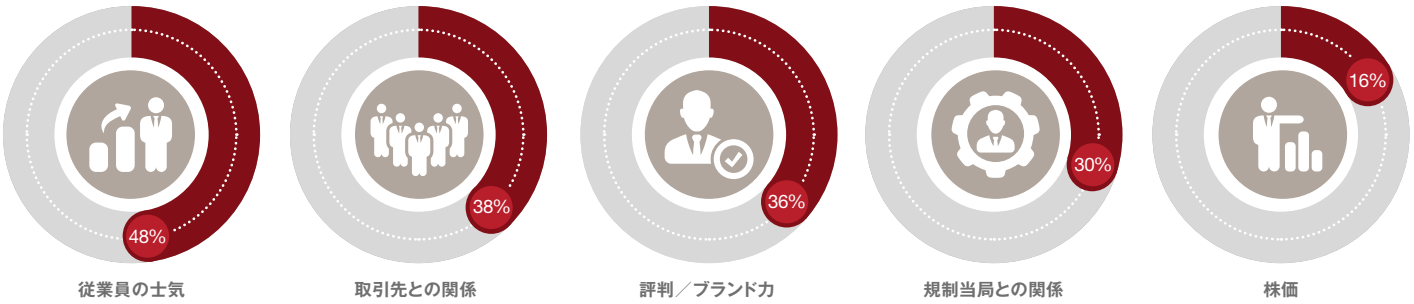
そのため、透明性が急速に高まっているこの時代において、企業が判断する前に問題が危機へと発展してしまうケースもしばしば見られる。一企業が判断するのではなく、世論の審判に委ねられているのだ。また、社会のルールは規制当局の規則よりも変化のスピードが速く、また、そうしたルールを破る者に対して世間は容赦ない。規制当局は、その定義上、限られた管轄内で、明確に定義された規則に従って業務を遂行している。一方、企業の評判には、法管轄や法律、法の適正手続きといったものは関係ない。

調査を行った上級管理職は一貫して、さまざまな形の経済犯罪によるネガティブな影響のうち、「評判の毀損」を1位ないしそれに近い順位としている。具体的には、世間の認知(評判／ブランド力、取引関係、株価)が最も大きな影響を受けるとしており、2016年以降、こうした影響度は高まっている。

規制への順守は、引き続き極めて重要であり、さらなる高まりも見せており、全体的に、法的・倫理的行動に関する規制・報告要件は拡大し続けている。査察や取り締まりも世界的に増加しており、国境を超えた規制当局同士の協力も珍しいものではなくなりつつある。

調査によれば、金融機関、投資信託、マネーサービス業、ブローカーディーラー、保険会社あるいは貴金属・鉱石・宝石取引事業などといった、多額な資金移動を伴う事業者の54％が、過去2年間に、マネーロンダリング(AML)防止に関する法執行または査察を受けた経験があると回答している(2016年から4％増加)。また、同数(54％)の回答者が、最近の地政学的な規制環境の変化により、今後2年間で組織が受ける影響は増大する、と予想している。

図表12：不正および経済犯罪は、事業のあらゆる要素に影響をもたらす

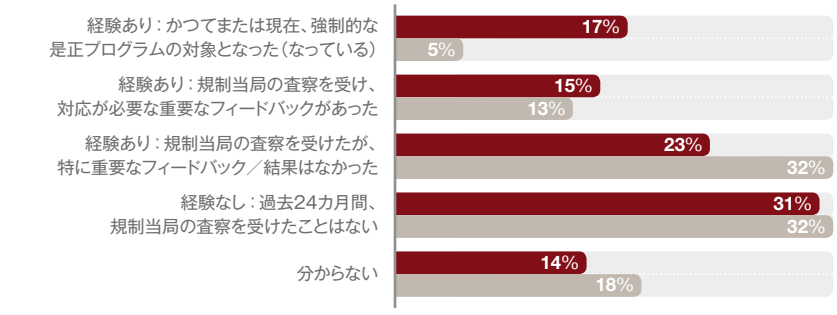


■ 高～中

Q. 最も致命的な不正／経済犯罪が事業運営の各側面に与えた影響の度合いは?

出所：PwC's 2018 Global Economic Crime and Fraud Survey

図表13：規制上の取り締まり・査察数は増加が続く



■ 2018年 ■ 2016年

*金銭の動きに携わる組織および／または、これらに類する事業は以下のとおり。
金融機関、投資信託、マネーサービス業、ブローカーディーラー、保険会社あるいは貴金属･鉱石･宝石取引事業。

Q. 過去24カ月以内に、AML関連の取り締まり／査察を受けましたか?

出所：PwC's 2018 Global Economic Crime and Fraud Survey

54%

が、規制環境の変化により、今後2年間で組織が受ける影響は増大する、と予想している。

経済発展と不正に相関関係はあるか?*

調査の結果、不正に対するグローバルなアプローチについて、いくつか興味深い示唆を読み取ることができる。これは、国家が経済発展を続けていく中で有益な指針となるかもしれない。

新興地域では、金融機関、投資信託、マネーサービス業、ブローカーディーラー、保険会社あるいは貴金属・鉱石・宝石取引事業などといった、多額な資金移動を伴う事業者の58%が、過去2年間に、AMLに関する取り締まりまたは査察を受けた経験がある、と答えている。

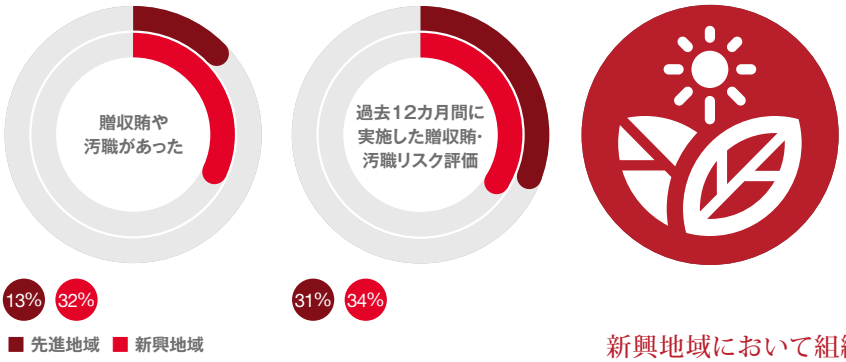
先進地域の同数値は48%であった。

新興地域では、企業の15%が、今後24カ月以内に不正防止への投資額が大幅に上昇すると予想している、と答えた。先進地域の同数値は9%であった。

新興地域では、経済犯罪は組織内部の犯行者によるケースの方が多い、と答えている(59%)。先進地域の同数値は39%であった。

* 先進地域／新興地域の区分は、United Nations Conference on Trade and Developmentの分類に基づく。調査の目的のために、経済移行地域については新興地域に含めた。

図表14:新興地域は汚職リスクの課題を抱え続けている



出所:PwC's 2018 Global Economic Crime and Fraud Survey

新興地域において組織が汚職を経験する可能性は、先進地域の約3倍に達する。しかし、贈収賄・汚職防止策に関するリスク評価を実施している組織は全体の3分の1にすぎない—先進地域の組織での同数値とほぼ同じである。

83%

のCEOが、危機をうまく管理できた場合、収益成長にマイナスの影響が及ぶことはなかった、と報告している。

出典:PwC's CEO Pulse on Crisis

「組織は、トップの姿勢よりもトップの行動に焦点を当てるべきである」

Tania Fabiani、パートナー、PwC米国

小規模な不祥事から学び、より強く成長する

あらゆる組織において、偶発的な機能不全や事故が発生することは避けられない。そして、私たちのデータは、小規模な不祥事から学ぶメリットが多数あることを示唆している。不祥事は一見良くないことだが、実際は、社内システムの改善を図る機会をもたらしてくれるというメリットもある。

企業や国家にとって、プロセスの発展は、嵐を乗り越えることで初めて得られる、という側面もある。危機や不測の事象をうまく管理できた場合、CEOの83%が、収益成長にマイナスの影響が及ぶことはなかった、と回答している。

収益以外でも、マネジメントが危機に陥りそうな状況にいかに対応するか、その手腕はマネジメントを評価する尺度となる可能性が高い。

比較的経験の少ない企業が、不測の危機に対しておざなりな対応をとってしまうのも無理はない。しかし、企業が、小規模な機能不全に効果的に対応する方法を学べば学ぶほど、大規模な危機に対応する備えが高まるのである。一種の「条件反射的」な対応が身に付くことで、充実した倫理・コンプライアンスプログラムや試練で鍛えられた上級管理職の力を生かして、より積極的なアプローチをとることが可能になる。

テクノロジーの防御力を活用する

テクノロジーのスイートスポット（最適解）を見いだす

不正に関して、テクノロジーは「諸刃の剣」である。すなわち、脅威、防御どちらにもなり得る。従って、企業の間で、不正が成長を大きく妨げかねない喫緊のビジネス課題と見なされるようになっている中で、多くの企業が、テクノロジーに対するアプローチを戦略的に変更してきた。これらの企業は、不正の検知、立証、顧客のいら立ち（customer friction）の減少などの分野に対し、着実な投資を新たに行うためのビジネスを展開している。

29%

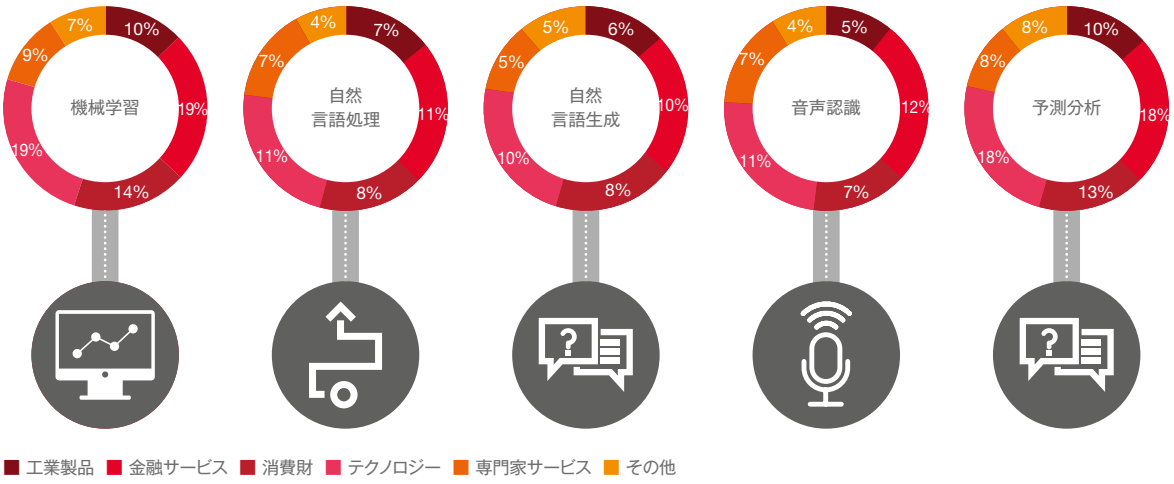
の企業が、最も致命的な経済犯罪による損失額の2倍以上を不正の調査と防止対策費に投じた、と答えている。

42%

の企業が、不正や経済犯罪対策費を増額している、と答えている。

現在、組織は革新的で高度なテクノロジーという資産を利用して、不正から自らを守り、人の行動の監視、分析、学習および予測を行おうとしている。例えば、機械学習、予測分析その他人工知能（AI）を利用した手法などが挙げられる。また、調査から、企業によるこうしたテクノロジーの利用は、所属する業界によって利用度合いが異なることも示されている。テクノロジーを購入し大規模な組織全体に採用するには多額のコストがかかるため、一部の企業にはそうした余裕がない場合もある。また、どのようなテクノロジーをいつ購入するかについての判断は難しい。新しいまたは革新的なテクノロジーに投資したものの、それを組織に最適化できない例もある。逆に、テクノロジーの採用が遅すぎて、周回遅れ状態に陥る例もある。

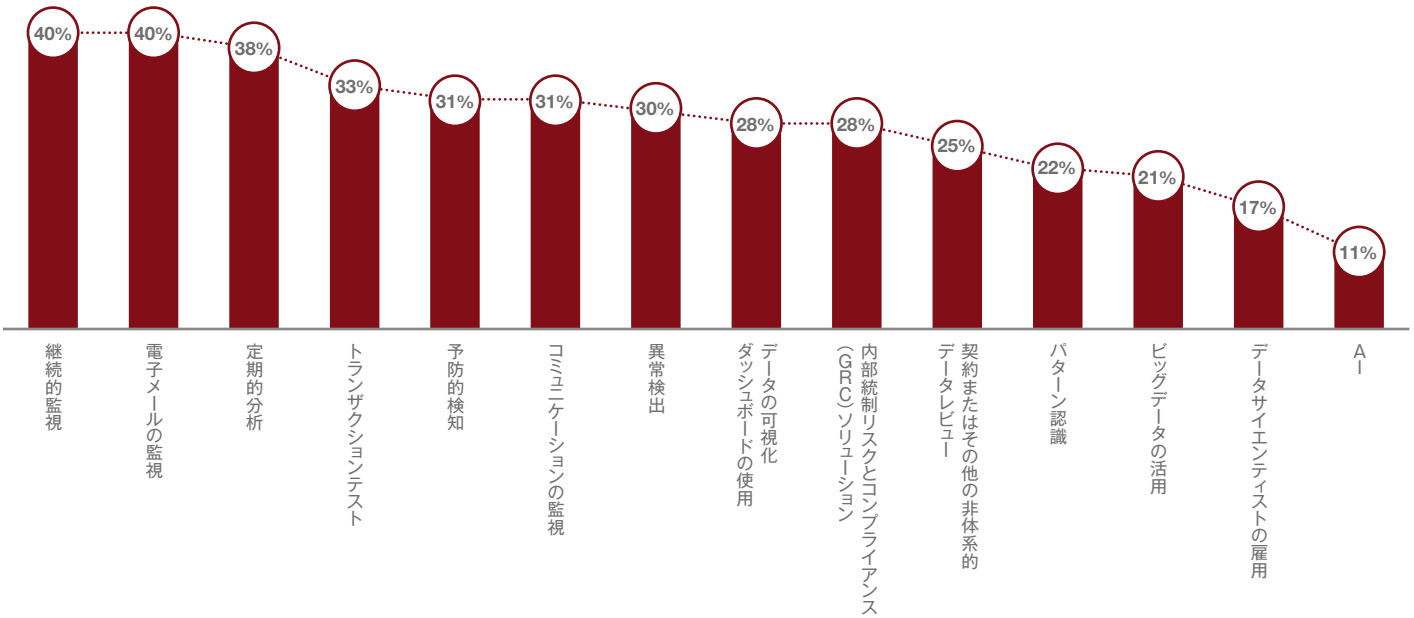
図表15：金融業界およびテクノロジー業界は、「AI」および「高度な分析（Advanced Analytics）」に最も高い価値を見いだしている



Q. 不正その他経済犯罪への対応や監視策として、組織はどの程度「AI」または「高度な分析」を活用していますか？あるいはそれらにどの程度価値を見いだしていますか？（活用し価値を見いだしている、と答えた回答者の比率）

出所：PwC's 2018 Global Economic Crime and Fraud Survey

図表16：組織は、不正対応策として、これまでとは違った革新的なテクノロジーに価値を見いだし始めている



Q. 不正その他経済犯罪への対応や監視策として、組織は統制環境において以下の新たな／革新的テクノロジーおよび手法をどの程度活用していますか？あるいはそれらに価値を見いだしていますか？（活用し価値を見いだしている、と答えた回答者の比率）

出所：PwC's 2018 Global Economic Crime and Fraud Survey

不正対策に革新的なテクノロジーを用いることは、今や全世界的な現象である。実際、調査によると、新興地域の企業は、先進地域の企業以上の速度で、先進技術への投資を行っている。新興地域の企業の27％が、現在、不正対策としてAIを活用しているか、または利用予定である、と答えている（先進地域の企業の同数値は22％）。新興地域にとって、このアプローチは、他国が既に相当のインフラ費を投じている領域において、遅れを取り戻すための効果的方法となり得る。

結局のところ、テクノロジーのユビキタス性によって、あらゆる組織は常に不正行為者より先を行きつつ、テクノロジーの有効性とそのバランスのスイートスポット（最適解）を見いだす必要がある。

顧客のいら立ちとは?

顧客として、まず自分が受けるサービスについて企業が常に不正を監視していると知れば、安心感を得られるだろう。しかし、そうした監視がすぎて頻繁にまたは繰り返しアラートを出されると、そうした安心感はたちまちいら立ちへと変わる。

これが「顧客のいら立ち」と呼ばれるものである。組織が危険信号に適切に行動することと、顧客への警告が過剰になりすぎることとの適正なバランスを模索する中で、顧客のいら立ちは大きな課題となりつつある。

このバランス調整は容易ではない—また誤差の許容範囲も狭い。組織が消極的すぎると、不正な取引を見逃すリスクが生じ、その先には金銭的損害や評判の毀損が待ち受けている。逆に積極的すぎると、顧客との関係が悪くなり、場合によっては顧客を失うリスクが生じる。

新たなテクノロジーの採用に関しては、新興地域が先進地域を上回るスピードを見せている

Philip Upton、パートナー、PwC米国

34%

の回答者が、組織の不正・経済犯罪対策に向けたテクノロジー利用に伴い、誤判定が多すぎると答えている。

顧客はビジネス上の単なる一要素ではない—顧客こそが全て

顧客は、あらゆるビジネスに欠くことのできないものである。しかし、デジタル革命を背景とするビジネスモデルの継続的進化とともに、これらの顧客の多くは支払いにかかわる不正に初めてさらされている。組織がそうした不正をどう処理するかという問題は、その結果に深刻な影響をもたらす。現代のデジタル不正の特性と課題例をいくつか挙げる。

新たなデジタル製品は、新たな攻撃対象を生み出している

企業はこれまで、製品を市場に提供するのに、既に確立したB2Bプロセス（再販業者、流通業者、小売業者）に従っていた。今日の革新的B2Cデジタルプラットフォームでは、不正行為者による攻撃対象が拡大し、不正によってセキュリティが突破される余地も大幅に増えてきている。

業界の境界線が曖昧に

非金融サービス企業が、決済システムへの進出を進めている。こうした比較的新たな参入企業は、従来の金融サービス企業が有する不正防止・AMLにかかわる経験やノウハウに欠けているため、自社および関係者のビジネスが、不正リスク、規制リスクの影響を受けやすくなる場合がある。

組織外部の不正行為者のテクノロジー進化は止まらない

サイバー攻撃はますます高度化し、徹底的かつ壊滅的になっている。たった一つのランサムウェアによる攻撃で、組織の機能を麻痺させることも可能である。また、それにより毎日数十億米ドルを銀行口座間で移動させている。

クレジットカード番号を変更することはできても、生年月日を変えることはできない

不正管理に長く使用されてきたナレッジベースの認証ツールはもはや時代遅れになっており、新たな手法—デジダルデバイスIDや音声生体認証—などが顧客資産の保護に必要とされている。しかし、大部分の企業はまだそれらの採用に至っていない。この点は重要である。なぜなら、大規模なデータ窃盗は、現金のような補填可能な資産の損失とは全く異なるためである。失われるのは個人情報に深くかかわる、一生変えられないID指標（生年月日や社会保障番号）なのである。これはまさしく、ナレッジベースの認証ツールが個人認証や不正防止に用いているデータであり、その窃盗は、不正行為者が個人IDを乗っ取る機会となる。

サイバー犯罪：目的と手段の乖離

サイバー犯罪は、導入期、成長期を既に大きく超えている。現代のサイバー犯罪者は、自らが攻撃対象とする企業に引けを取らない知識と専門性を有している。こうした成熟化により、サイバー犯罪の脅威とそれに伴う不正の多面的性質について、新たな視点が求められている。

多くの場合、組織がシステム上何らかの問題があることに気付くきっかけは、フィッシング、マルウェアまたは従来の総当たり攻撃といったサイバー攻撃の発見である。こうした攻撃の頻度、レベル、破滅性が高まっているために、企業は先手を打つ方法をより熱心に模索するようになっている。こうした先手型のアプローチによって、不正防止により深く焦点を当てられるようになる、というメリットも生まれる。

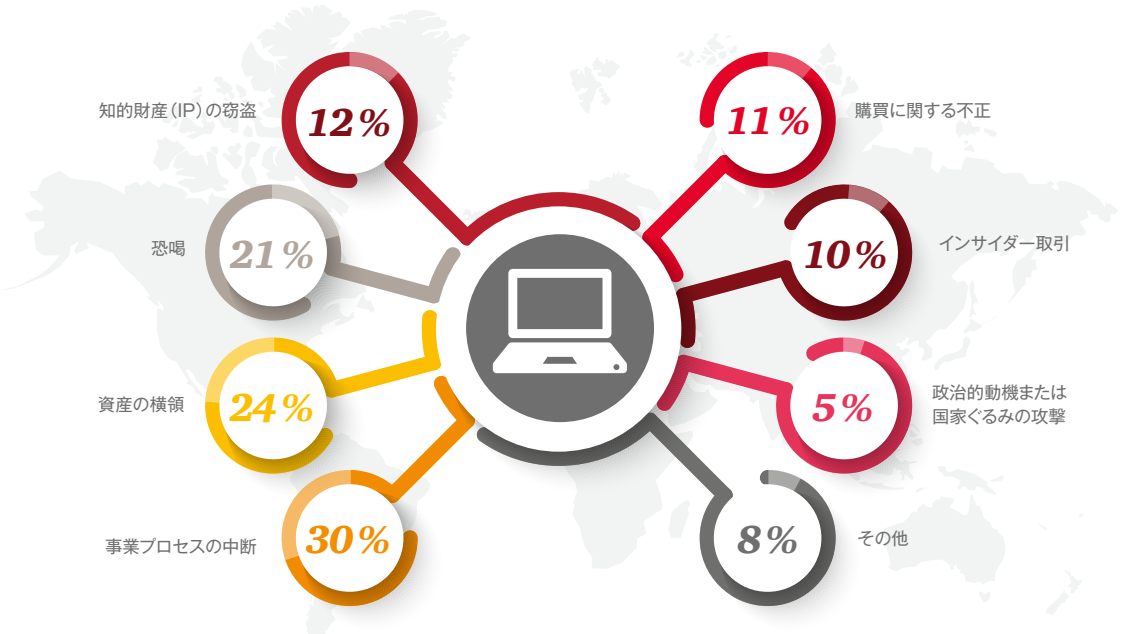
企業がサイバー攻撃による財務的影響を正確に測定することは難しいかもしれないが、サイバー犯罪が最も致命的な不正である、と答えた回答者の14％が、同不正により100万米ドル以上の損害を被ったと述べている。また、1％が、損害額が1億米ドル以上に達したと回答している。

「サイバー犯罪」が今後2年間で組織に影響をもたらす最大の致命的かつ深刻な経済犯罪になる、と答えた回答者は、他の不正の2倍以上に上っている（回答者の26％が、今後2年間にサイバー攻撃があると予想しており、最も致命的な不正になると述べている。また、12％が「贈収賄や汚職」、11％が「資産の横領」と回答している）。実際、サイバー攻撃は、あまりにまん延しているため、その頻度や影響を測定する意義は低下しており、むしろ各ケースについて不正行為者が用いるメカニズムに焦点を当てることの方が役立つと考えられている。

41％

の上級管理職が、サイバー犯罪による損失額の2倍以上を不正の調査と防止費に投じた、と答えている。

図表17：組織がサイバー攻撃の餌食となった不正の種類



Q. サイバー攻撃により、どのような種類の不正または経済犯罪の被害を受けましたか？

出所：PwC's 2018 Global Economic Crime and Fraud Survey

あらゆるデジタル不正は不正に他ならないが、逆にあらゆる不正がデジタル、というわけではない。従って、2種類のサイバー犯罪を区別するのが有用だろう。

(1) デジタル窃盗(モノは盗まれるが物理的な損壊などはない)。この種類の攻撃には、現金、個人情報、IPの窃盗や、恐喝、ランサムウェアその他多くの犯罪が含まれる場合がある。

(2) デジタル不正。この種類の攻撃は、多くの点でより長期にわたり破壊力も大きい。というのも、不正行為者は、開かれたドア(多くの場合、顧客または従業員が使用しているアクセスポイント)から侵入し、企業の事業プロセスそのものを用いて攻撃するためである。この種の不正に対処するためには、組織はワクチン(予防)と治療の両方にデジタルの手法を用いる必要がある。

図表18:組織に対して用いられるサイバー攻撃の手法

Q. 過去24カ月以内に、以下の手法のいずれかを用いたサイバー攻撃の標的となったことはありますか?

出所:PwC's 2018 Global Economic Crime and Fraud Survey

全体の3分の1の回答者が、マルウェアおよびフィッシングによるサイバー攻撃の標的となったことがあると答えた。ビジネスプロセスに深刻なダメージをもたらしかねないこうした攻撃の大部分は、企業に重大な損失ももたらす場合がある。攻撃を受けた回答者の24%が、資産の横領の被害を受け、21%がデジタル上の恐喝を受けた。

顧客への補償の先に…そのお金はどこへ?

顧客に不快な思いをさせないことがビジネスの第一歩であるが、不正防止にかかわる側面はより複雑なものとなっている。これらには、不正を働く地下組織と、それを抑えるための規制・取締制度が含まれる。

仮に、不正行為者が顧客のIDを窃盗し、その名義でクレジットカードを作って使い込んだ場合、銀行または企業がその顧客の損失分を補填し、顧客に対してそれ以上の責任を求めることはない。これまで、外部の不正に対する補償制度はこのようなものであった。全ての関係者—銀行、企業、顧客、当局—は、共に事業上のコストの一部として受け入れてきた。

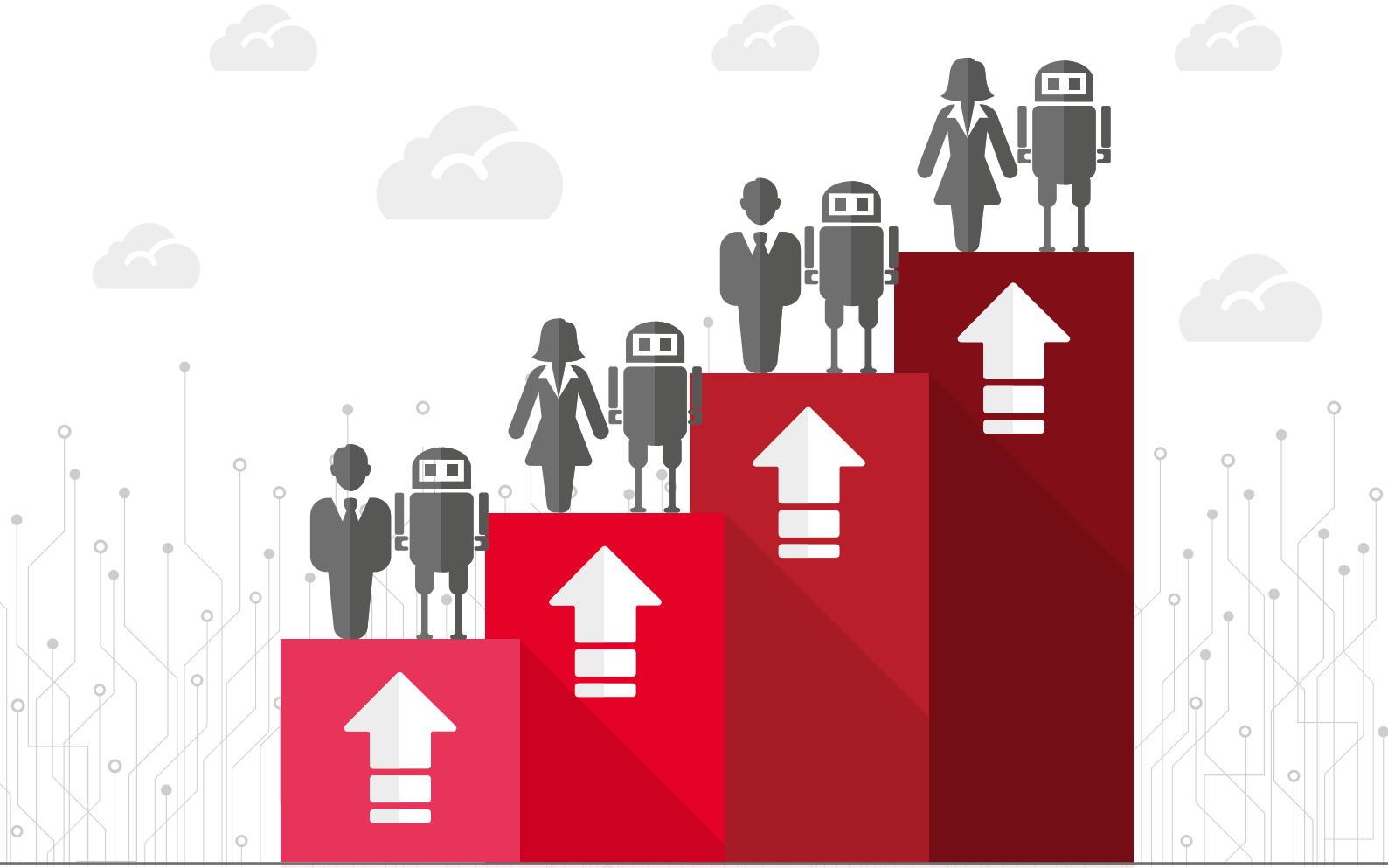
こうした不正行為は、米国銀行秘密法(BSA)や他国の同様の規則に沿って組み込まれた取引監視システムにより発見することが可能であるが、銀行および金融サービス企業(MSB)は、こうした取引がシステムの中にどのように表れているか、うまく見つけられずにいるようである。最近でも、企業が人身売買の取引を見落としていたことをめぐり当局の取り締まりを受けた例もある。

非金融サービス企業は、金融サービス企業と同一の規制上の義務を負ってはいないが、それでも法に抵触する可能性はある。今や、規制当局と法執行機関は、犯罪の第一次影響—例えば、偽造品の売買—のさらに先、つまり、そうした盗品による金銭がどこに流れているのかに目を向けている。そうした機関の権限として、意図的か否かにかかわらず、非金融サービス企業が犯罪行為を助長している兆候が見られた場合、かかわる企業のコンプライアンスや不正防止措置を調査することになる。

投資対効果の検討

不正防止テクノロジーへの投資に関する投資対効果の検討の内容は、評判の毀損、規制上および/または財務的損害から組織を守ること以上の範囲にまで及んでいる。効率化による不正防止コストの削減や、組織がデジタルプラットフォーム上で新たな製品やサービスを安全に構築して販売できるようにすることも含まれる。さらに、企業が顧客のいら立ちを軽減するための不正防止プログラムのバランス調整を図ることも可能になる。これにより、顧客は、プラットフォームや製品をより自由に扱うことができるようになる。

設備だけでなく人材にも投資する



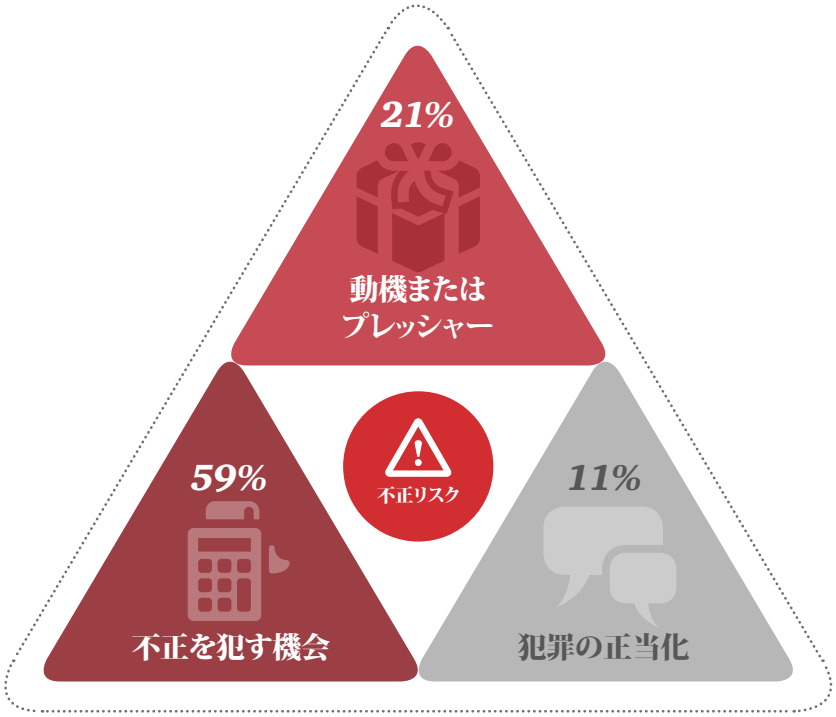
人材への投資抑制が巨額の代償に繋がることも

多くの組織は、不正への対応という難しい問題に直面した後、より多くのリソースをテクノロジーに投資する方針を決めている。しかし、これらの投資は、特に内部不正への対応は、これ以上のリターンが望めない段階に達している。つまり、テクノロジーが不正との戦いに不可欠なツールであることは明白だが、あくまで解決策の一部にしかなり得ないということである。

というのも、不正というのはさまざまな状況や人の動機が複雑に絡んだ結果生じるものであるためである。不正を犯す際の最も重要な要素は、結局のところ人の行動である。これは、不正対策にとっての最良のヒントとなる。ここには組織内部の不正の3要因―不正のトライアングル―を理解し、防止するために、強力な方法が存在する。

不正のトライアングルは、まず「動機またはプレッシャー」（多くの場合、業績に対する組織内部からのプレッシャー）があり、その次に不正を犯す「機会」が続き、最終的にそれを内部で「正当化」するプロセスに至る。これら3要因全てそろって不正が発生するため、各要因について個別に対応する必要がある。

図表19：不正のトライアングル：従業員が不正を犯す理由



Q. 組織内犯行者による不正や経済犯罪について、次の各要因がどの程度寄与しましたか？
（組織内の不正に最も寄与する要因を挙げた回答者の比率）

出所：PwC's 2018 Global Economic Crime and Fraud Survey

図表20：組織内部の不正に対応する上で必要な組織の取り組み度

Q.組織内部の不正や経済犯罪への対応として、組織はどの程度の努力を払っていますか?以下の各カテゴリーについて答えてください

出所：PwC's 2018 Global Economic Crime and Fraud Survey

不正の機会を防止する：統制

近年、組織による不正防止に向けた取り組みの大半は、不正を行う機会を減らすことに集中している。回答者の50％が、内部統制など、不正行為の機会をターゲットとしたビジネスプロセスの構築に多くの努力を払っている、と答えている。そして、59％が、組織内部の犯行者による最も致命的な不正の主因として「機会」と答えているが、これは、2016年の同数値（69％）より10％低下した。これは、テクノロジーが重要な役割を有していること、そしてより重要な点として、企業がおおむねテクノロジーを効果的に採用していることの証左であろう。

しかし残念ながら、企業は「動機」や「正当化」への対策が大幅に欠けている。これらの要因に対して多くの努力を払っていると答えた回答者は34％にすぎなかった。調査では、こうした選択の結果として次のことが浮かび上がっている。組織内部の犯行者による最も致命的な不正の主因を「動機またはプレッシャー」とした回答者は21％で、2016年から2倍に増加した（「不正の正当化」と答えたのは11％で前回並み）。

こうした、企業文化や倫理に関する対策への関心が低いことが、盲点が生じる可能性があることを示している。そして実際に、組織内部の不正がなくならない理由の一つとも考えられる。不正とは人の選択とシステム上の不備が組み合わさった結果発生するものである以上、内部統制がもたらすセキュリティに関する誤った認識に注意することが大切である。どんなに優れた設計の内部統制システムであっても過信してはならない。

実際、テクノロジーを活用した内部統制だけで不正を発見できる、という考え方には根本的な欠陥がある。そうした考え方は、マネジメントは常に倫理的に行動する、という前提に基づいているからだ。過去の実例からも、事実上全ての重大な組織内部の不正は、こうした統制を回避する、または無視するマネジメントが招いた結果であることが分かる。調査でもこのことが裏付けられている：上級管理職が犯した重大な組織内部の不正の割合は、この2年間で50％増と大幅に増加している（前回調査の16％から24％に増加）。こうした構造的問題を克服するために、組織は実際に対象領域における、マネジメントの内部統制の無視や共謀を考慮した統制を策定する必要がある。

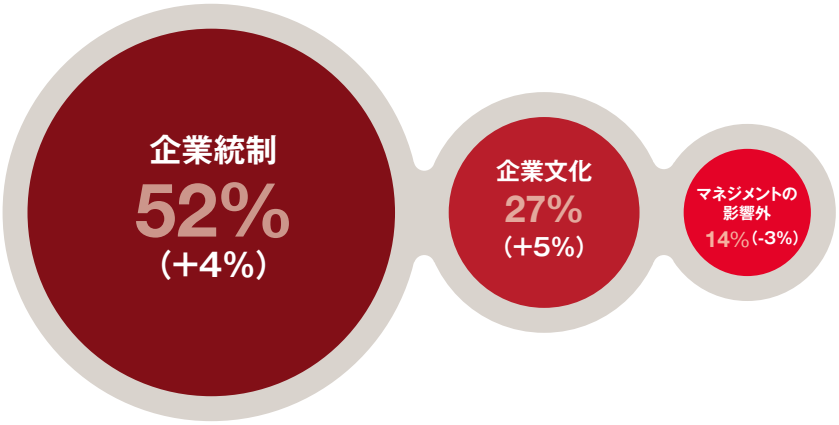
「動機またはプレッシャー」の発生を防ぐ：透明性

企業レベルの不正は、おおむね、企業からのプレッシャーと繋がりがある。また、不正に走らせるプレッシャーは、組織のあらゆるレベルで発生し得る。調査によれば、過去2年間に不正を経験した組織の28％が、業務遂行／職権濫用にかかわる不正（個人の利益のための不正）の被害を受けており、本社以外の地域にオフィスを構える組織の16％が、そうした地域において業務遂行／職権濫用にかかわる不正を経験している。一方、回答者の24％が、最も致命的な犯罪の責任は上級管理職にあったと答えている。

人を不正に走らせる原因を検討する際、金銭的報酬ばかりに目を向けないことが重要である。ミスを犯したことへの恐怖心や困惑といった感情も同じくらい重要である。従って、組織の評価基準についても検証しなければならない。法令遵守や「正しい行動」と、人事評価・報酬制度はどの程度整合性が取れているだろうか。

特別な短期的統制を設けることで、強引な営業プログラムが従業員を不正に走らせる原因となっていないかチェックすることも可能である。また十分に周知した、社内通報／ホットラインポリシーを設けることで、組織において問題が発生しかねない状況を早期に警告するシステムとして活用することも可能である。

図表21：最も致命的な不正の半分以上が企業統制により発覚



含む		含む		含む	
内部監査（定期）	14%	告発（内部）	13%	偶然	8%
不正リスク評価	13%	告発（外部）	7%	法令上の取り締まり	4%
疑わしい活動の監視	13%	告発ホットライン	7%	調査メディア	2%
企業セキュリティ	5%				
データ分析	4%				
配置転換	1%				

Q. 最も致命的な不正や経済犯罪はまずどの方法で発見しましたか？

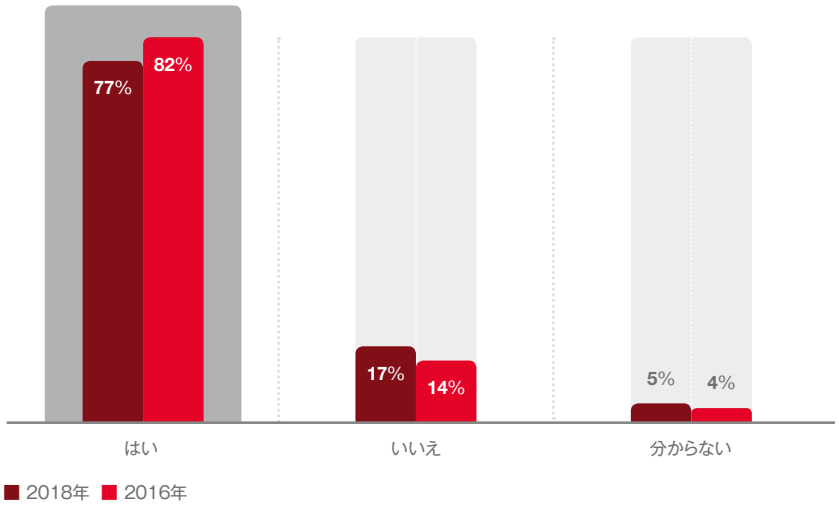
出所：PwC's 2018 Global Economic Crime and Fraud Survey

不正は善意からも生じる

不正は必ずしも、悪意や利己的な行動を必要とするものではない。法的見地からすると不正には2種類存在する―個人的利益を得るために犯した不正（横領や報酬を余分に得るための不正）、そして「企業の利益」に起因する不正（企業存続や労働者保護のための不正）である。後者は、企業としての成功促進を願う「善意」から発生し得る不正である。

例えば、市場シェアおよび収益性増大（従業員の利益のため）を目指して策定した営業戦略のはずだったのが、結局不正な営業機略に変容してしまう可能性もある。スタートはどうあれ、経営陣が責任を取らされる、という結果に変わりはない。

図表22：倫理・コンプライアンスプログラムがある、と答えた企業は減少傾向



Q. 正式な業務上の倫理・コンプライアンスプログラムを設けていますか?

出所：PwC's 2018 Global Economic Crime and Fraud Survey

犯罪の正当化の防止：企業文化

「動機」と「機会」に対しては、さまざまな方法により影響をもたらし、管理することが可能であるが、不正行為の「正当化」を防ぐことは非常に困難である。これは、完全に個人の胸の内の問題であることから、企業の施策により影響をもたらすことが他の二つに比べて難しいためである。

組織内部の不正が他と異なるのは、不正行為者が、しばしばそうした不正を犠牲者のいない行為と考えており、直接的に損害を被る人物を想起できていない、という点である。調査回答者の約4分の3が、以下の最も致命的な経済犯罪の主犯が組織内部の人物であった、と答えた理由もこうした点から伺える―「人事に関する不正」（81％）、「資産の横領」（75％）、「インサイダー取引」（75％）、「財務報告にかかわる不正」（74％）、「購買に関する不正」（73％）。

犯罪の正当化を防ぐ第一歩は、従業員の行動を統治する環境―組織の文化―に焦点を当てることである。そのため、社内アンケートやワーキンググループ、個人面談などを用いて、そうした文化の長所と短所を確認し、評価すべきである。また、一貫性ある研修も重要である。どのような行動をしてはいけないのか、またその理由を明確に理解できるようになれば、不正行為を正当化しづらくなる。

しかし、調査によれば、不正防止に大きな変化をもたらし得るこうした類いの研修に投資する組織数は減少している。正式な業務上の倫理・コンプライアンスプログラムを設けていると答えた回答者は、2016年調査の82％から、77％に減少した。そうしたプログラムを設けていると答えた企業のうち、プログラムに不正全般を対象とする具体的なポリシーがある、と答えたのは58％にとどまった。

経済犯罪や不正の発見や防止が複雑な課題であることは間違いない。これは、不正行為の背後にある動機と発生環境を明確に理解した上で、テクノロジーを用いた施策と人材に焦点を当てた施策とのバランスを図っていくことを意味する。組織は、テクノロジーが唯一の解決策であるという考え方や、ある程度の不正というのは事業上発生するコストの一部にすぎない、という考え方を甘んじて受け入れる必要はない。誠実さやトップダウンによる透明性重視の文化を確立することで、誰もが説明責任について理解し、それを実行できる組織にすること―そして、「盲点」に潜む不正を探り出すこと―が可能になるのである。

結論

不正に備え、不正と向き合い、より強固な組織へ

調査の結果、多くの企業が、内的、外的両方の理由により、不正に向き合うだけの備えが足りてないことが分かった。そのため、組織の不正の盲点に光を当てること、何が不正を構成するのか—それを防ぐためには何をすべきか—明確に理解し共有することが非常に重要となってくるのである。

また、そうした取り組みを通じて、重要な機会を手にすることが可能になる。組織全体で前向きな構造的改善を行うきっかけとなり得、これにより、好不況に関係なく、企業力や戦略性を高めることにも繋がり得る。こうした取り組みには、コンプライアンス、倫理、リスク管理、法務各部門の縦割り状態を解消することも含まれ、それにより前向きで、一貫性があり、団結力に優れ、逆境にも強い企業文化が実現される。

確かに最新の不正プログラムの価値は定量化しづらく、必要な投資を確保するのが難しい場合もある。しかし、コンプライアンスおよび透明性の文化を確立しないことによるコスト—財務、法務、規制、評判にかかわるコスト—はさらに高額になる場合もある。

近年強まっている経済犯罪の脅威だけでなく、全ての利害関係者—規制当局者および一般大衆からソーシャルメディア、従業員まで—もまた、不可逆的な変容を遂げている。現在、透明性と法規則遵守の重要性は、かつてないほどに高まっている。

これは素晴らしいことである。企業の評判が一夜にして一変してしまう「世論」という法廷において、企業は今日起きたことに対して翌日には説明責任を負うのである。従って、企業にとっては、不正事象自体と同じくらい、不正事象やコンプライアンス上の問題が発生した場合の対処方法が重要となってくる。

この原則を理解することで、企業は、急速に進んでいく事象に先手を打ち、問題を掌握していることを内外の利害関係者に示す機会が得られる。透明性を「手にする」ことで組織の評判に大きなメリットがあるだけでなく、わずかな不正も見逃さない環境において上級管理職の業務セキュリティを高めることができる。また同時に、次世代のリーダーに対しセキュリティの重要性を認識させることもできる。予期せぬ事象は、うまく管理しないとすぐさま危機へと発展する。しかし、適切なメカニズム—団結力と透明性を持った高度な統制環境—があれば、企業は、うまく衝撃を吸収し、条件反射的に対応できるようになり、より強固な組織になることが可能である。

すべきことは明らかである。企業目的の中核に透明性を確保すること、それを戦略、ガバナンス、リスク管理、コンプライアンスの統合に用いること、そして、深刻化しそうなビジネス上の課題を、逆に優位に立つ機会へと変えられるような体制を整えることである。

お問い合わせ先

**不正に対処していく上で何ができるか、
さらに詳しく知りたい方はPwCの下記専門家にお問い合わせください。**

Survey Leadership

Didier Lavion
Principal
PwC US
+1 (646) 818 7263
didier.lavion@pwc.com

Forensic Services Leaders

Kristin Rivera
Global Forensics Leader
PwC US
+1 (415) 498 6566
kristin.d.rivera@pwc.com

Dinesh Anand
Partner
PwC India
+91 (124) 330 6005
dinesh.anand@in.pwc.com

Dyan Decker
Partner
PwC US
+1 (646) 313 3636
dyan.a.decker@pwc.com

John Donker
Partner
PwC Hong Kong
+852 2289 2411
john.donker@hk.pwc.com

Ian Elliot
Partner
PwC UK
+44 (0) 771 191 2415
ian.elliot@pwc.com

Trevor Hills
Partner
PwC South Africa
+27 (11) 797 5526
trevor.hills@za.pwc.com

Leonardo Lopes
Partner
PwC Brazil
+55 (11) 3674 2562
leonardo.lopes@pwc.com

Richard Major
Partner
PwC Singapore
+65 6236 3058
richard.j.major@sg.pwc.com

Domenic Marino
Partner
PwC Canada
+1 (416) 941 8265
domenic.marino@ca.pwc.com

Claudia Nestler
Partner
PwC Germany
+49 (69) 9585 5552
claudia.nestler@de.pwc.com

Sirshar Qureshi
Partner
PwC Czech Republic
+420 251 151 235
sirshar.qureshi@cz.pwc.com

Nick Robinson
Partner
PwC United Arab Emirates
+971 4304 3974
nick.e.robinson@ae.pwc.com

Malcolm Shackell
Partner
PwC Australia
+61 (2) 8266 2993
malcolm.shackell@au.pwc.com

日本のお問い合わせ先

PwCアドバイザリー合同会社
〒100-0004 東京都千代田区大手町1-1-1
大手町パークビルディング
Tel：03-6212-6880（代表）

PwCコンサルティング合同会社
〒100-0004 東京都千代田区大手町1-1-1
大手町パークビルディング
Tel：03-6250-1200（代表）

大塚 豪
ディレクター
go.otsuka@pwc.com

ホンマ シン
パートナー
shin.s.honma@pwc.com

平尾 明子
マネージャー
akiko.hirao@pwc.com

上野 俊介
マネージャー
shunsuke.ueno@pwc.com

奈良 隆佑
マネージャー
ryusuke.nara@pwc.com

経済犯罪実態調査 2018について

123の国・地域、7,228名が回答。そのうち、52％の回答者が組織の上級管理職。42％が上場企業に所属し、55％が従業員1,000名以上の企業に所属。

www.pwc.com/jp

本報告書は、PwCメンバーファームが2018年2月に発行した『Global Economic Crime and Fraud Survey 2018』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。
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
オリジナル（英語版）はこちらからダウンロードできます。 www.pwc.com/fraudsurvey
日本語版発刊年月：2018年6月　　管理番号：I201803-1