2020

終わりなき不正との戦い

PwC経済犯罪実態調査2020
日本語翻訳版

www.pwc.com/jp

pwc

新聞やニュースなどを見ると、崩壊した建物の建設工事における贈収賄、ハッキング被害による何百万人分もの医療関連データや財務データの外部流出、会社側の不正行為が引き起こした製品の欠陥、内部通報によって明るみに出た不正による株価の急落など、毎日必ずと言っていいほど経済犯罪や不正に関する報道を目にしているであろう。

経済犯罪や不正は増え続けており、それがこれまで以上に多様な形で、より多くの企業に影響を与えている。そのような現状を踏まえ、企業は次のような問いに答えなければならない。

- 自社に対する経済犯罪の脅威を適切に評価しているか
- 現状の体制が不十分または非網羅的で、必要以上にリスクにさらされていないか
- これまで構築してきた不正対策のテクノロジーは、期待した価値を提供しているか
- インシデントが発生した際に正しい対応を取っているか

これらは今回の「経済犯罪実態調査」で中核となる質問の一例である。

不正がこれまで以上に深刻化し、不正対応にかかる費用が高額化する中で、組織として、有事に向けた態勢の評価、有効な不正対策の策定および有事発生時の迅速な対応が不可欠となっている。

不正

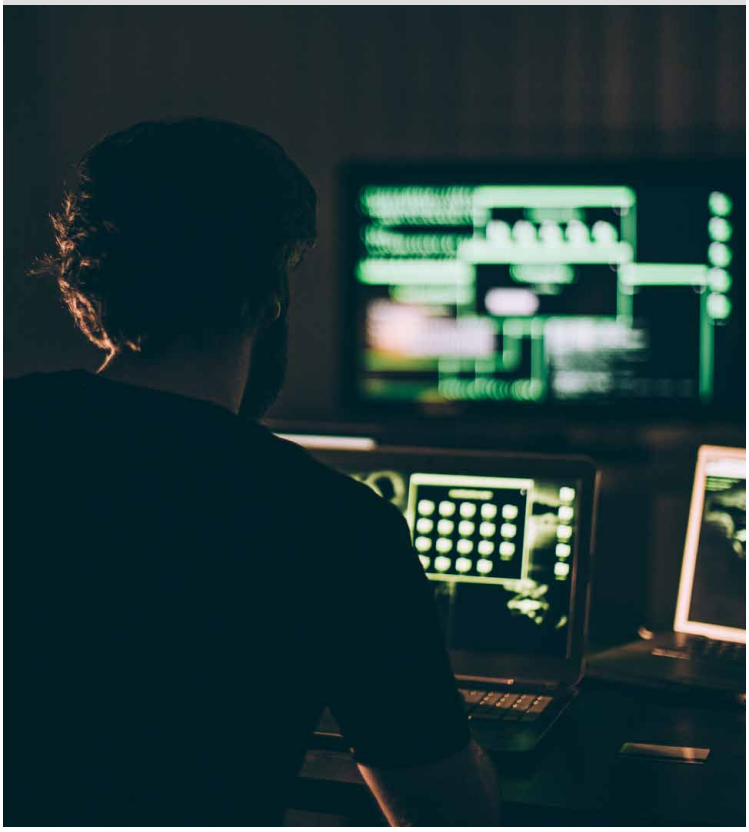
20年以上にわたり、PwCのグローバル経済犯罪実態調査では、次のような犯罪を調査している。

- 財務報告に関する不正
- 競争法・反トラスト法違反
- 資産の横領
- 贈収賄・汚職
- 顧客による不正
- サイバー犯罪
- 事業活動に関する不正
- 人事に関する不正
- インサイダー取引
- 知的財産の侵害
- マネーロンダリング
- 購買に関する不正
- 税金に関する不正

経済犯罪実態調査2020の概要

不正の実態に迫る：**不正の類型**

今回、5,000社以上の回答者のうち半数近くが、過去2年間で経済犯罪・不正の被害を受けたと回答している。得られた回答に基づき、経済犯罪・不正の種類、不正の関与者、不正対応に成功した会社の事例などの実態について詳細を見ていこう。



5,000以上
の組織が回答

62% 回答者のうち62%は上級管理職

72% 全世界売上高が10百万ドル以上の企業の割合

99
の国と地域からの回答

420億米ドル
経済犯罪・
不正にあった企業が
被った被害総額

47%

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は**過去20年間で2番目に高い水準**

6件の不正被害

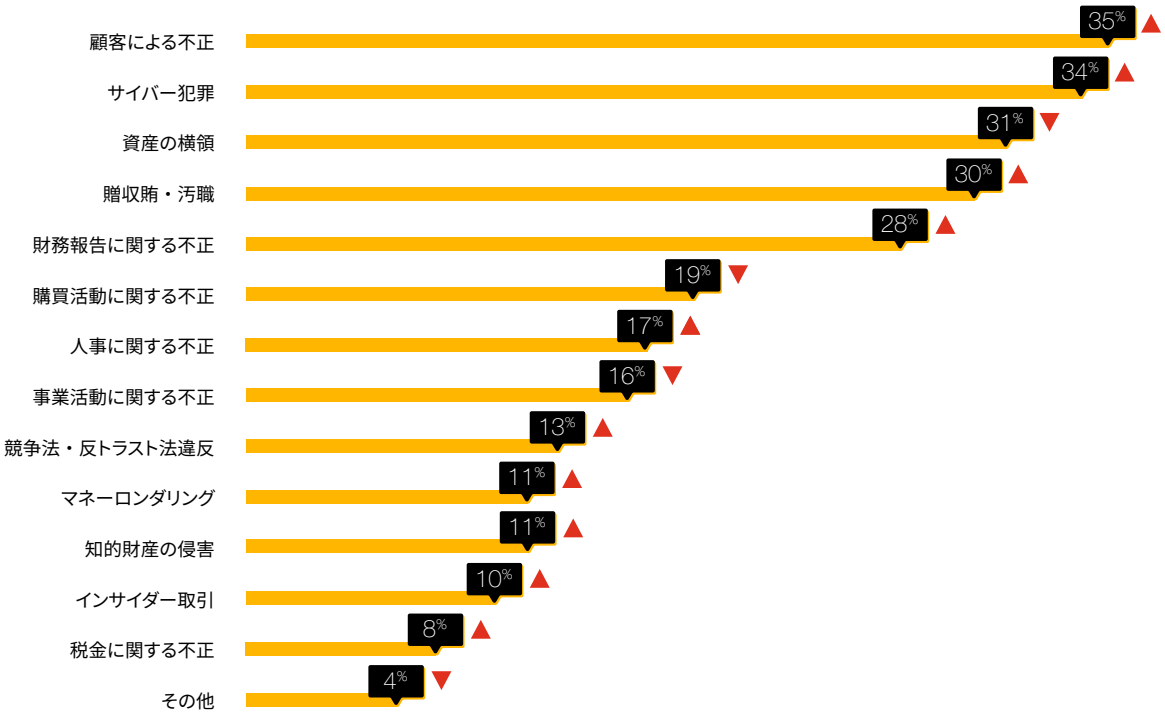
過去2年間に経験した不正・経済犯罪の数（平均値）

上位4位の不正の種類は？

1. **顧客による不正**
2. サイバー犯罪
3. 資産の横領
4. 贈収賄・汚職

顧客による不正、財務報告に関する不正、競争法・反トラスト法違反、人事に関する不正、贈収賄・汚職などの不正が今回の調査では大きく増加した。

過去2年間で被害に遭った経済犯罪



出典：PwC「2020年世界経済犯罪・不正調査」

最も被害が大きかった不正ランキング-業種別

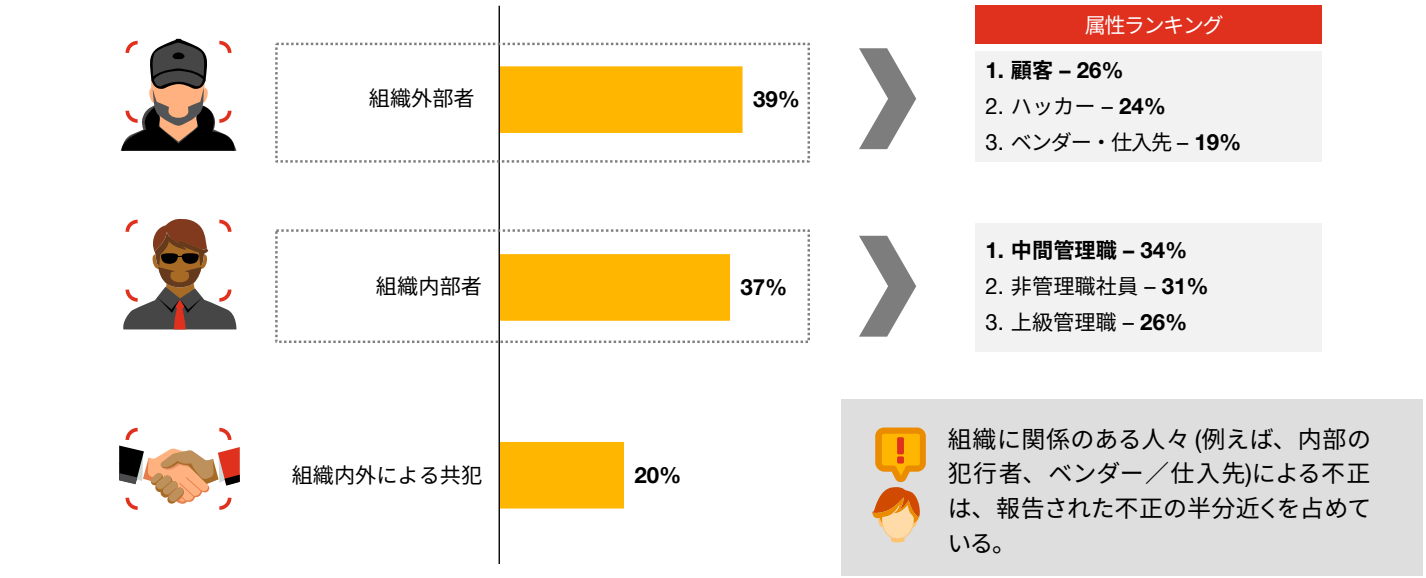
	消費財市場	エネルギー・ユーティリティ・資源ビジネス	金融サービス	政府・公共セクター	ヘルスケア産業	工業製品・製造	テクノロジー、メディア&電気通信事業
1	顧客による不正 **18%**	贈収賄・汚職 **17%**	顧客による不正 **27%**	サイバー犯罪 **17%**	サイバー犯罪 **16%**	資産の横領 **21%**	サイバー犯罪 **20%**
2	資産の横領 **17%**	資産の横領 **16%**	サイバー犯罪 **15%**	財務報告に関する不正 **17%**	財務報告に関する不正 **13%**	サイバー犯罪 **15%**	財務報告に関する不正 **16%**
3	サイバー犯罪 **16%**	財務報告に関する不正 **13%**	財務報告に関する不正 **14%**	贈収賄・汚職 **16%**	顧客による不正 **13%**	贈収賄・汚職 **14%**	顧客による不正 **13%**

出典：PwC「2020年世界経済犯罪・不正調査」

経済犯罪・不正の実行者

不正は、あらゆる角度からやってくる　経済犯罪・不正の実行者や関与者は、組織の内部者、外部者、また内部者と外部者の共犯によるものとも多い。取引先などのビジネスパートナーによる不正リスクは依然として高く、組織のマネジメントが関与した不正は増加傾向にあることが分かった。

不正の主な関与者は外部か内部か、それとも共犯か



出典：PwC「2020年世界経済犯罪・不正調査」

顧客による不正（26%）　顧客による不正は、組織外部者による不正の中で1位（26%）となるだけでなく、被害に遭った不正の内容調査の中でも2018年調査より増加して上位になった（2018年調査より35%増加）

- 金融サービスや消費者市場の業界では、顧客による不正が特に目立っている。これは直接顧客対応をする業界では当然の結果とも言える。一方で、昨今より多くの業界が、消費者に対する直接戦略を取る傾向となっているため、同様のリスクが他業界に広がる可能性が高い。
- 一方、「顧客による不正」に関しては、専任のリソースや強固な内部統制、テクノロジーの活用が、予防に有効であることが証明された。

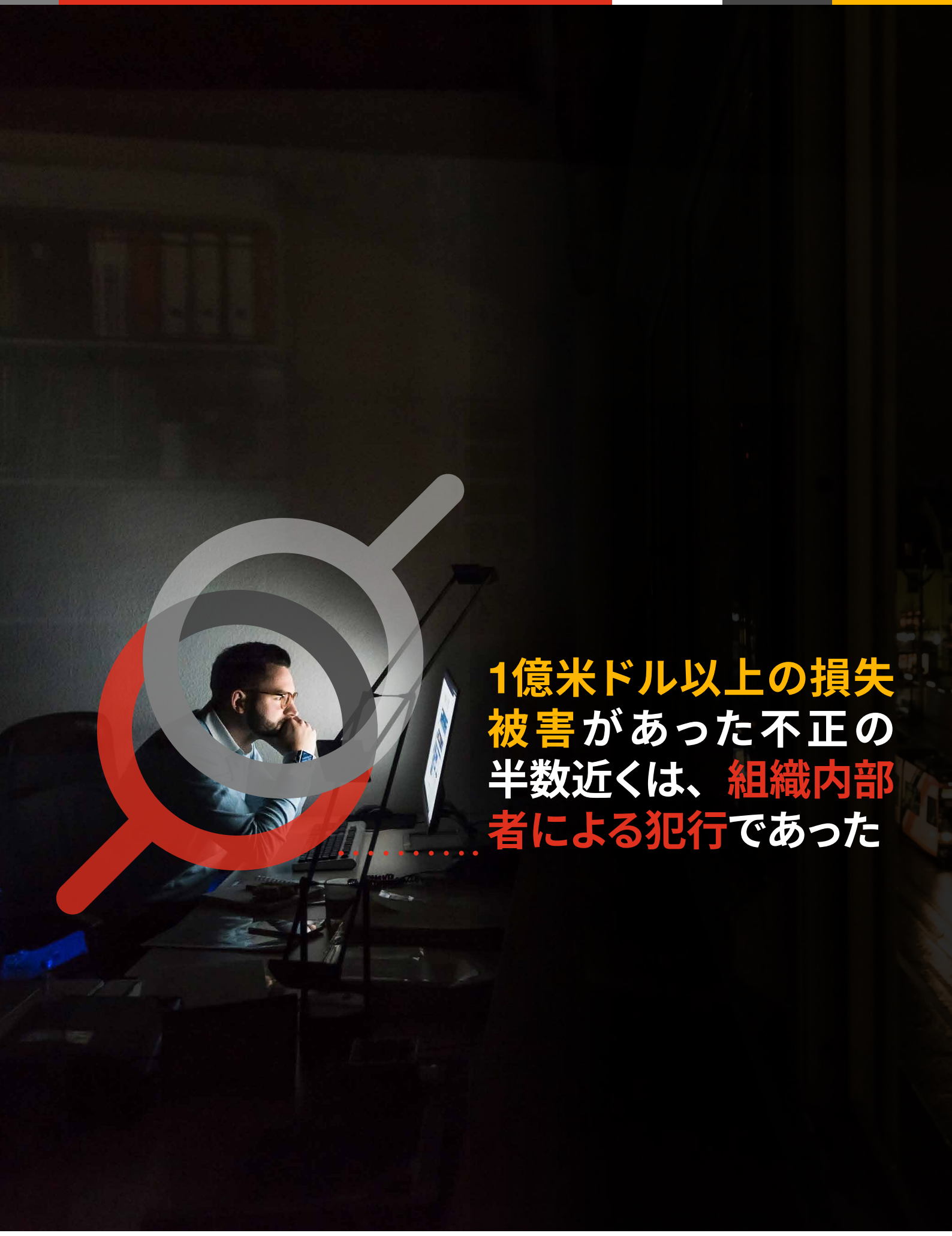
第三者（サードパーティー）による不正（19%）　多くの企業がコスト削減のために、非中核事業にかかる業務を外部に委託している。しかし、自社の業務に外部のビジネスパートナーを利用する場合には不正のリスクはつきものである。多くの企業がそのリスクを適切に管理できていない。

- 回答者の5社に1社が、「ベンダー・仕入先」を最も被害の大きかった外部不正の原因として挙げた。
- 回答者の半数は、第三者（サードパーティー）リスク管理に関する強固なプログラムを持っておらず、21%は第三者（サードパーティー）に対するデューデリジェンスや管理・モニタリングを全く行っていないと回答した。

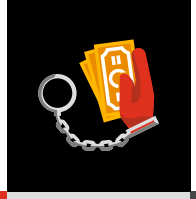
マネジメントによる不正（26%）　いわゆる「マネジメントによる不正」は、委任された権限レベル、システムへの知識や影響力を介して、内部統制を無効化しうるため、最も厄介で潜行的であることが多い。

不正の告発　今回の調査では、初めて、不正の被害を経験した回答者に対して、「自らの組織も不正行為を行ったとして責任を問われたか」と尋ねた。その結果、10社に3社近くが、犯罪・不正行為の自らの組織の関与について責任を問われたと回答した。

- ほぼ同じ割合の回答者が、組織による不正を訴追するのは、競合他社、規制当局、従業員および顧客が多いと回答している。
- 各種規制の強化や、一部の地域で施行されている内部通報者に対するインセンティブ（報酬）制度が、この傾向に寄与している可能性がある。



1億米ドル以上の損失被害があった不正の半数近くは、**組織内部者による犯行**であった



コスト面から見る不正の被害

不正が及ぼす損失は複雑である　罰金、不正対応や再発防止にかかる費用など、直接的な財務上の損失や費用については定量化できる。しかし、企業ブランドの毀損、市場での地位の逸失、従業員の士気の低下、将来の機会損失などは、容易に定量化することができない。

420億米ドル

過去2年間で経済犯罪・不正に遭った企業が被った被害総額

組織の外部者による不正は、通常の取引の中で発生することが多く、積極的なモニタリングなどの適切な管理により、財務上の影響を軽減することができる可能性がある。一方、贈収賄や汚職、組織内部者による不正は、いわゆるダウンサイドリスクの回避とリスク管理がより重要な要素となる。

後者の不正は、一般的に、予測や監視が難しく、高額の罰金に加えてビジネス機会の損失やブランド価値の毀損といった付随的な損害を伴う傾向がある。

今回の調査で、過去2年間に不正を経験した組織の**約13%が、不正により5,000万米ドル以上の損失があったと回答した。**

最も費用のかかる不正のTOP5　競争法・反トラスト法違反、インサイダー取引、税金に関する不正、マネーロンダリング、贈収賄・汚職は、直接的な損失額が大きな不正として上位にランクインした。これらの不正は、不正の対応・改善および罰金の支払いによって、多大な費用が発生するケースもある。

組織内部者による不正は、組織外部者による不正よりもはるかに被害が大きい可能性がある　これは単に財務上の損失が大きい可能性が高いというだけではない。1億米ドル以上の損失があったと報告された不正のうち、43%が組織内部者によるものであった。組織内部の人間による不正の場合、組織や関与した従業員に対する刑事訴追や民事訴訟、企業のレピュテーションの毀損、経営の混乱、事業の喪失なども同時にもたらす可能性がある。

贈収賄と汚職は依然として大きな課題である
回答企業の3分の1が、賄賂の支払いを求められたことがある、あるいは賄賂を支払ったと思われる競合他社にビジネスの機会を奪われたことがあると回答している。

今回の回答の中には、いくつかの盲点や驚くべき事実があった

- **10社中6社において、贈収賄・汚職リスクに対応するコンプライアンスプログラムが整備されていない。**
- 全回答企業の半数近くが不正リスクの評価を実施していないか、限定的にしか実施していない。
- 全回答企業の半数が、サードパーティーに対するリスクベースのデューデリジェンスや継続的なモニタリングを全く実施していないか、限定的にしか実施していない。
- 内部統制の運用の有効性について限定的なテストを行っている会社は10社に3社に満たず、12%の企業は全く行っていない。

有事に向けた準備

あなたの組織では、不正の防止・検出のために何を行っているだろうか。不正の防止・検出の目的において機能しているプログラム、方法、テクノロジーは何で、機能していないのは何か。現状どのような認識のギャップがあり、今後どのような改善の機会があるか。

不正に立ち向かう努力には意味がある。しかし、今行っていることで十分だろうか　不正リスクを緩和するためのプログラムは、一組織あたり、平均で4つ有している（従業員数が1万人以上の組織ではそれ以上）。約3分の2の組織が不正防止に関する規定や手続きを整備し、過半数（10社中6社）が研修やモニタリングを実施していると回答した。しかしそれでも、リスク評価、ガバナンス、第三者（サードパーティー）管理に十分なリソースを割いている会社は半分にも満たないという結果となった。

では、どのような対策が最も効果的だろうか

1. **あらゆるリスクを特定し、重要度に応じた対応を行う。**企業は、全ての事業部および事業を行う全ての地域の従業員からの情報収集を通じて、自社の有するリスクを特定し、そのリスクの緩和策を評価する適切なリスク評価を実施すべきである。これには様々な外的要因も取り入れるべきである。公開情報から入手できる情報は豊富にあり、その情報を無視すると重大なミスにつながってしまう可能性がある。不正リスクの評価は、一度きりではなく、定期的に実施するべきである。
2. **テクノロジーを適切なガバナンス、専門知識、モニタリングによって補完する。**1つのツールで全ての不正に対処することは不可能である。また、テクノロジーだけで組織を不正から守ることはできない。テクノロジーは、専門知識を有する人材、データ管理と可視性、強固な統制、および定期的なモニタリングと一緒に存在してこそ、その存在意義を発揮する。
3. **効果的な不正防止プログラムで特に重要なことは、不正の発生時に、いかに迅速に初動対応ができるか、という点である。**適切な人員、手続き、テクノロジーを同時に素早く展開することにより、潜在的なダメージを軽減することができる。影響の大きな不正は、結果的に広範な組織変革の機会を引き起こし、組織戦略上の変換点となる場合も多い。

テクノロジーは解決策の1つにすぎない

近年、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いるが、今回回答した多くの企業が、そうしたテクノロジーを展開することに対する懸念を示している。

- 不正対策のためのテクノロジーの導入やアップグレードができたと回答した企業は3割に満たなかった。これは費用の問題や、リソース不足およびシステムの限界が原因となっている。
- 従来の技術に代わるテクノロジーとして 昨今普及している人工知能（AI）を活用している企業はわずか25%である。ただし、そのうちの約40%は、AIを不正対策ツールとして活用する価値を見出せていない。

単一のツールやテクノロジーだけでは、不正防止プログラムとは呼べない。適切なルールと要件に基づいて適切な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。情報の分析結果を既存の不正防止プログラムに照らし合わせて、より強固なプログラムへと改善しているだろうか。新たな不正対策のテクノロジーの導入に苦慮する組織が多い中、人工知能などのツールを適切に導入した組織は、不正対策における価値を見出している。

有事の際の正しい対応

実際にあなたの組織で不正が起きてしまったらどうするか。不正発生後に、事実解明のための調査を実施した企業の60%近くは、結果的に不正が起こる前より、組織として良い状態になったと回答をした。しかしながら、回答者の半数近くは調査を全く実施していなかった。また、取締役会に不正を報告した企業も3分の1に留まった。

昨今、ひとたび不正が起きると、規制当局だけでなく、世間一般も企業側へより多くの対応を求めるようになっている。初動対応の遅れは、直接的な被害だけでなく、より広範囲に悪影響を及ぼしかねない。

PwCが2019年に実施したグローバルクライシスサーベイによると、従業員5,000人以上の企業は、**サイバー犯罪（26%）、自然災害（22%）、経営者のによる不正行為（17%）、そして、詐欺や汚職、企業の不正行為を含む倫理上の不正（16%）**の被害に遭う可能性が最も高いことが分かった。

PwC「2020年CEO意識調査」によると、58%のCEOが、自社の危機対応の準備状況について不安を抱いている

不正という危機を乗り越えてより良い状況になったと回答した組織が取った不正対応の中で、鍵となった施策は何だったのか

実態解明のための調査を実施（71%） さらなる被害を防ぐためには、不正の根本原因を特定・分析することが重要である。調査にあたって客観性が求められる場合や、組織内に調査に必要なリソースや専門的な知見がない場合は、外部専門家を起用して調査を行うことが多い。

内部統制および規程・手続きの強化（>50%） 一部の規程や手続きを見直すことは比較的容易なことであるかもしれない。しかし重要な点は、海外子会社などを含む全社レベルで運用を評価し、不足している領域を特定することである。

従業員への懲戒処分（44%） 規制当局のガイダンスにもあるように、コンプライアンスプログラムは全ての組織における構成員に適用されるべきであり、上位の役職者や特定の従業員が優遇され、処分から免除されるような例外は認めるべきではない。コンプライアンスプログラムを忠実に実行することが、その有効性を高める鍵の1つである。

最も被害が大きかった不正について「調査」を実施したのは、回答企業のうちわずか

56%

出典：PwC「2020年世界経済犯罪・不正調査」

取締役会に報告したのはわずか3分の1以下

90%近くの企業が不正発生後にネガティブな感情を持ったと回答した

42%
ポジティブな感情

89%
ネガティブな感情

出典：PwC「2020年世界経済犯罪・不正調査」

不正事案を規制当局に報告（37%） 不正の事実を規制当局に早期に開示することが、会社にとって有利な結果をもたらす場合がある。

研修の実施（32%） コンプライアンス研修の実施は、従業員に対して社内の新たな規程や手続きを周知する以外にも、不正防止に向けた意識の向上や社内文化の醸成にも寄与する。

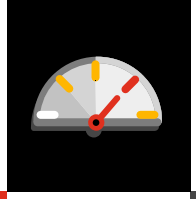
驚くことではないが、大半の企業（89%）は、不正を経験した後にネガティブな感情を抱いている。しかし、不正発生後に組織が良くなったと回答した企業は、次のような共通点がある。

- 不正の首謀者は、組織の内部者ではなく、組織の外部者であった（48%）。
- 組織として、自分たちの価値観に忠実であり、チームとして行動し、計画を策定し、その計画に沿って行動した。

状況の把握・整理

誰しも、不正の被害者となること（あるいは最悪の場合不正に関与していたと責められること）などは望んでいない。反面、こうした重大な事案を別の視点で見てみると、不正は組織変革のターニングポイントにもなる。不正事案がプラスに作用するかマイナスに作用するかどうかは（例えば市場で不正事案前より良い地位にポジショニングできるケースや、逆に本格的な危機に陥ってしまうケース）、いかに不正対応の準備がよくできていたか、また不正発生後にそれがどのように運用されたかにかかっている。

今回、インシデント発生時に状況を把握、整理することの大きなメリットを示すデータが得られている。不正を経験したことがある全回答者の半数近く（45%）が、統制環境の強化、事業の合理化、損失の減少、従業員のモラルの向上などの側面において危機発生前よりも組織がより良い状態になったと回答している。大企業では、同様の回答をした割合がさらに高く（52%）、良くなった分野として、事業環境の改善と事業の合理化に加え、新技術の採用、インシデント再発件数の減少などを挙げた



より強い組織になるための**成功例**

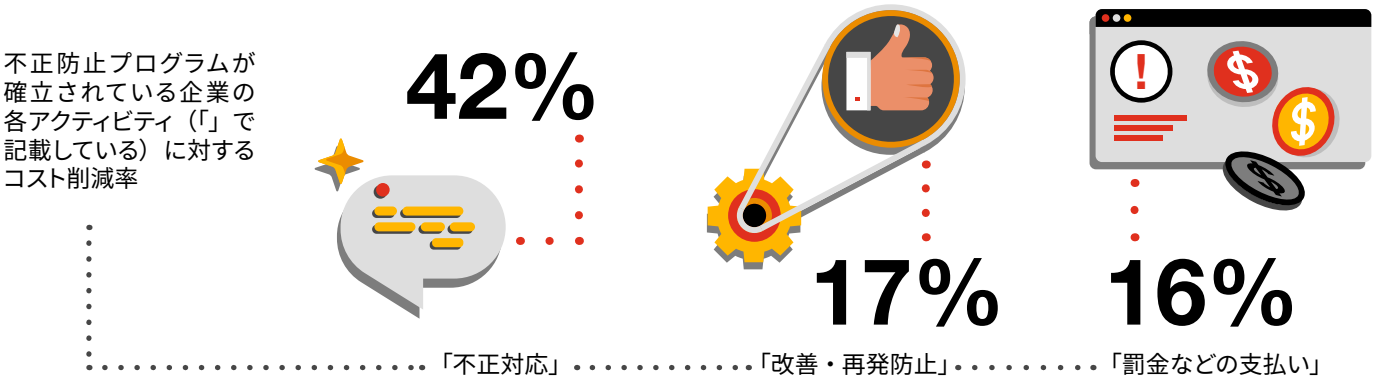
不正対応に関連する部署は、新しいテクノロジーへの投資や、新しいプログラムの導入・実施、追加の人員の採用等に関する予算の確保に苦労していることが多い。今回、回答者の40%近くが、今後2年間で不正防止に関する支出を増やす予定であると回答している。しかし、そういった対策は実際に機能しているのだろうか。また、投資に見合った成果や見返りは期待できるのだろうか。そして、こうした投資の正当性を、いかに組織のリーダーに説明できるのだろうか。

この点、不正対策ツールの利点を定量化するのは難しい場合がある。効果的な不正防止プログラムは、将来の不正の件数や不正が発生した場合の被害額を抑制させると考えるのは当然であろう。今回、不正防止対策への投資と不正が発生した場合のコストの削減には、明確な相関関係があるという、興味深い調査結果が得られた。

不正防止に特化したプログラムを導入・実施している会社は、不正が発生した際の対応、改善・再発防止、罰金などの支出が（売上高に対して）、そういったプログラムがない会社よりも少ないのである。

- 不正防止プログラムを導入・実施している会社は、プログラムが実施されていない会社に比べて、不正の対応費用が42%、改善・再発防止費用が17%少なかった。
- 贈収賄や汚職が発生した場合、贈収賄・汚職に対する不正防止プログラムを導入・実施している会社は、導入・実施していない会社よりも、改善・再発防止にかかった費用が58%少なかった。

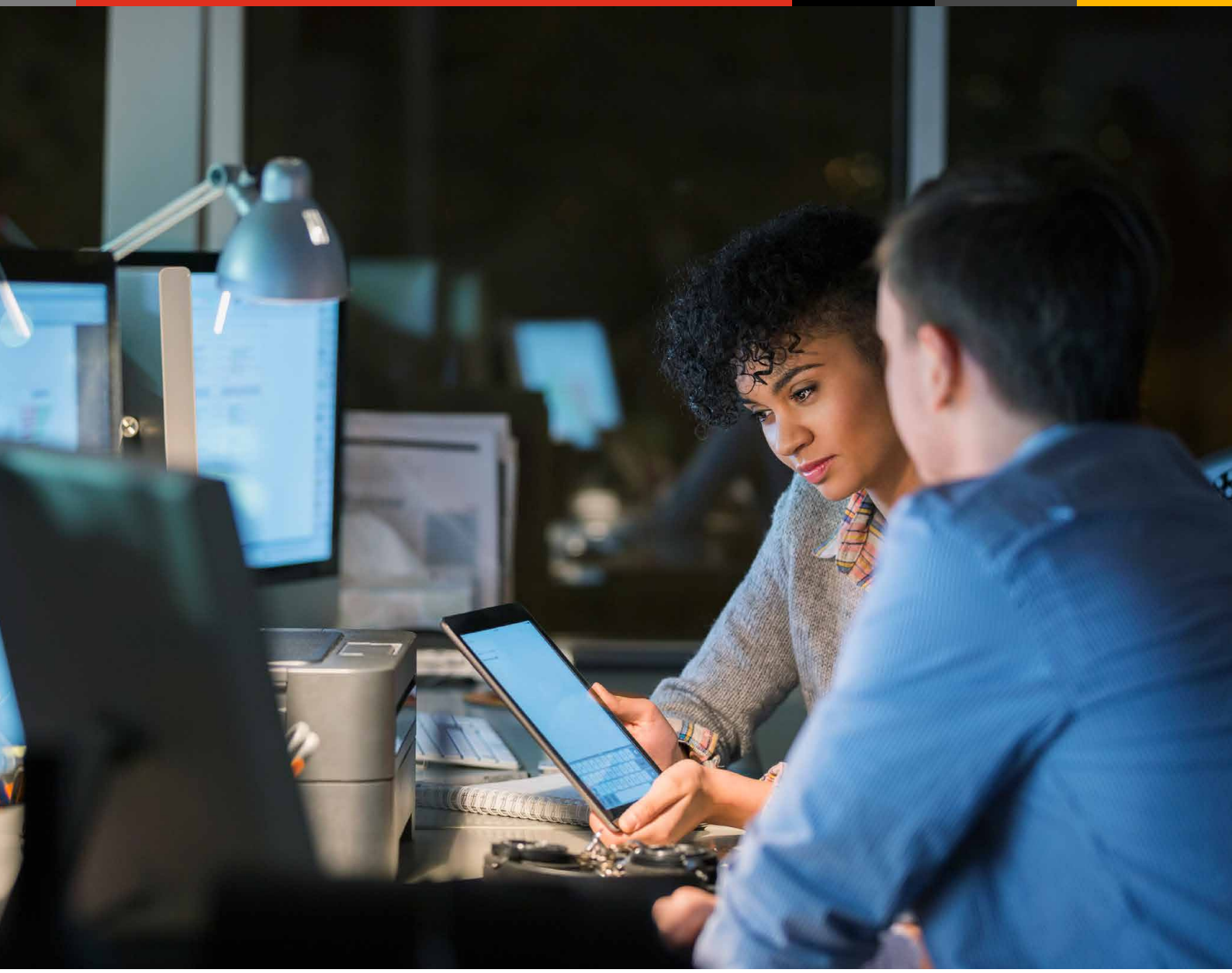
不正防止に投資している会社は、不正発生時の費用支出が少ない



出典：PwC「2020年世界経済犯罪・不正調査」

不正防止プログラムの導入後は、定期的な評価と改善が鍵となる。その理由は？

- 企業のビジネスモデルは流動的であることが多く、リスクプログラムが確立または強化される前に、ビジネスモデル自体が変わると、結果的に会社は予期せぬリスクにさらされることがある。
- IT・テクノロジー関連企業が金融サービスを提供するようになったり、ヘルスケア関連企業が消費者市場に参入するなど、業界のコンバージェンスが進んでおり、リスク管理プログラムは、そういった新しい事業やマーケットに対応することが肝要である。
- 組織内外からのホットラインを通じた通報や、外部監査などの結果から、以前は考慮されていなかったリスクが発見される可能性がある。



最も重要なのは、規制当局が昨今、これまで以上に企業のコンプライアンスプログラムに着目していることである。企業に対して、自社のコンプライアンスプログラムの有効性を示す証拠となる情報を提供するよう要求し始めている当局もいる

多くの規制当局は、コンプライアンスプログラムは、各社のリスクに基づき適切な規模感で構築されており、必ずしも全ての不正行為を検知できるものではないということは認識している。コンプライアンスに対するいわゆる「紋切型のアプローチ」は存在せず、大手通信会社のコンプライアンスプログラムは、小規模小売業者のそれとは異なっていて当然である。プログラムが異なっていても、両者はそれぞれの組織が直面する特定のリスクに対処するには適切な場合もある。

同様に、有効性を評価する規定の方法は存在しない。不正防止におけるコンプライアンス研修の有効性について研究した論文などの文献は多く存在するが、例えば第三者（サードパーティー）管理プログラムの有効性の評価などについては、情報量が少ない。

規定の方法が存在しないということは、逆に言えば、各企業が自社にとって有効な評価システムを独自に定義する機会でもあるということだ。例えば、ベンダー・取引先の集約に関するデータや取引成否に関するデータ、各種教育研修プログラムへのベンダー・取引先の参加、ベンダー・取引先による誓約、および第三者（サードパーティー）に対する監査における発見事項の減少などについて評価の対象とすることも有用かもしれない 。**重要なのは、不正防止プログラムの各領域が、適切な検証を経て、将来の不正の発生を防止および検知するのに有効なものであることを証明できる取り組みを行うことである。**

おわりに

本調査結果を見て、ご自身の組織の状況と比較してどう感じただろうか。不正行為の防止、発見および対応に関する取り組みにおいて、組織の中でリーダーの役割を果たしているだろうか。また、緊急の課題として取り組むべき改善点があるだろうか。

いずれにしても、行動を起こすのは今である。どんなに素晴らしい不正防止プログラムであっても、継続的な評価と改善を行う必要がある。不正の実行者や内容が日々複雑化する中で、不正防止プログラムも新たなリスクに応じて変わっていかなければならない。

逆に、不正防止プログラムが十分でないと、不正リスクや不正対応コストの増大を招いてしまうだろう。

組織として事業を継続する限り、不正のリスクはつきまとう。そして、実際に不正が発生してしまった場合、外部からの厳しい追及に対して、「不正防止への意識や洞察力が足りなかった」という言い訳は通用しない。

今こそ、あなたの組織が不正に対してどれほど準備ができているかを確認するときである。本調査におけるカスタマイズされた調査結果を参考にすれば、自社の市場、業界、グローバルの同業者に対して自社がどのような状況で、不正防止のために今何をすべきかが分かるかもしれない。

お問い合わせ先

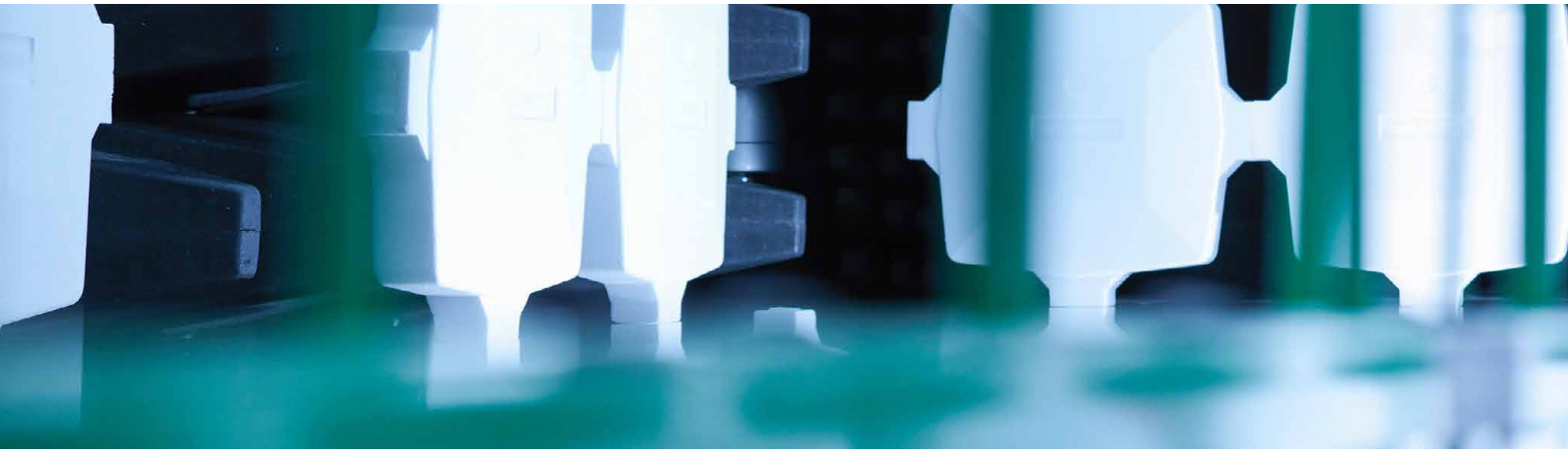
今回本調査にご協力頂いた全社の回答と比較して、あなたの会社の経済犯罪や不正のリスクや不正防止プログラムの評価結果をご提供します。ご希望の方は、下記担当者までご連絡ください。

Kristin Rivera
Global Leader, Forensics,
PwC United States
kristin.d.rivera@pwc.com
+1 415 302 3428

John Donker
Partner, APA Forensics Leader,
PwC Hong Kong
john.donker@hk.pwc.com
+852 91962726

Chris Rohn
Principal, Global Economic Crime and Fraud Survey 2020 Leader,
PwC United States
chris.rohn@pwc.com
+1 312 714 7463

Chris Butter
Partner, EMEA Forensics Leader,
PwC U.K.
christian.butter@pwc.com
+44 7841 498581



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

大塚 豪
パートナー

池田 雄一
パートナー

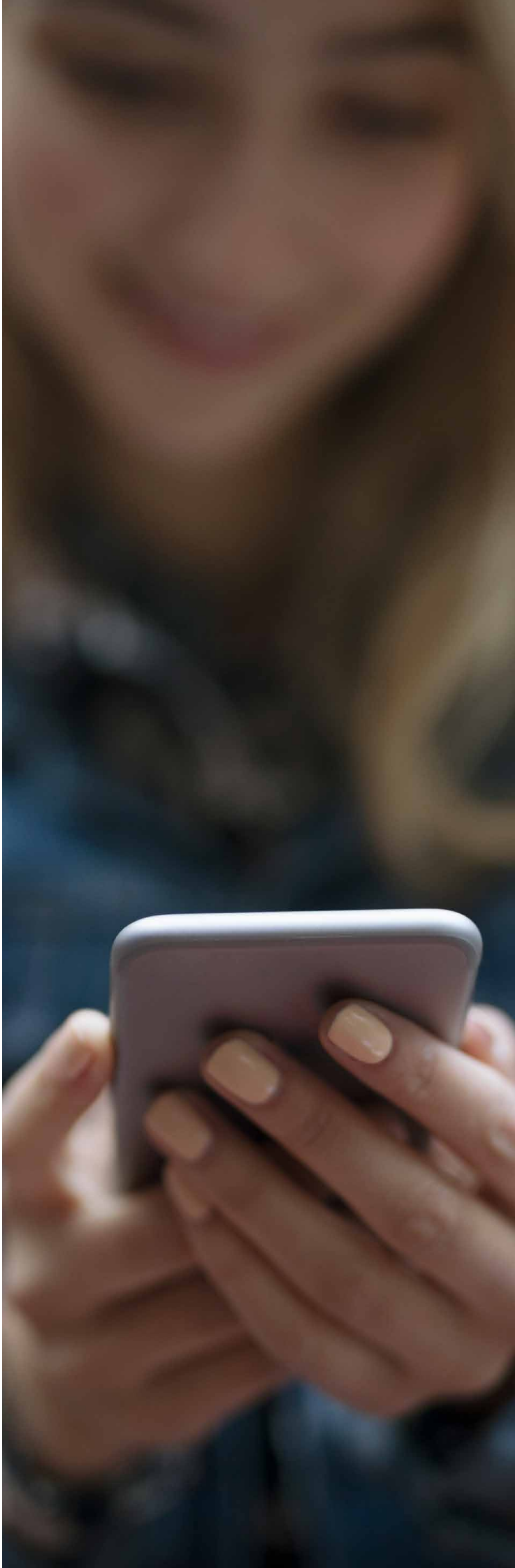
迫田 宜生
パートナー

那須 美帆子
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

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8,100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築き、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157カ国に及ぶグローバルネットワークに276,000人以上のスタッフを有し、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2020年3月に発行した『Fraud and Economic Crime – a seemingly never-ending battle PwC's Global E conomic Crime and Fraud Survey』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。
https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html
日本語版発刊年月：2020年6月　管理番号：I202005-07