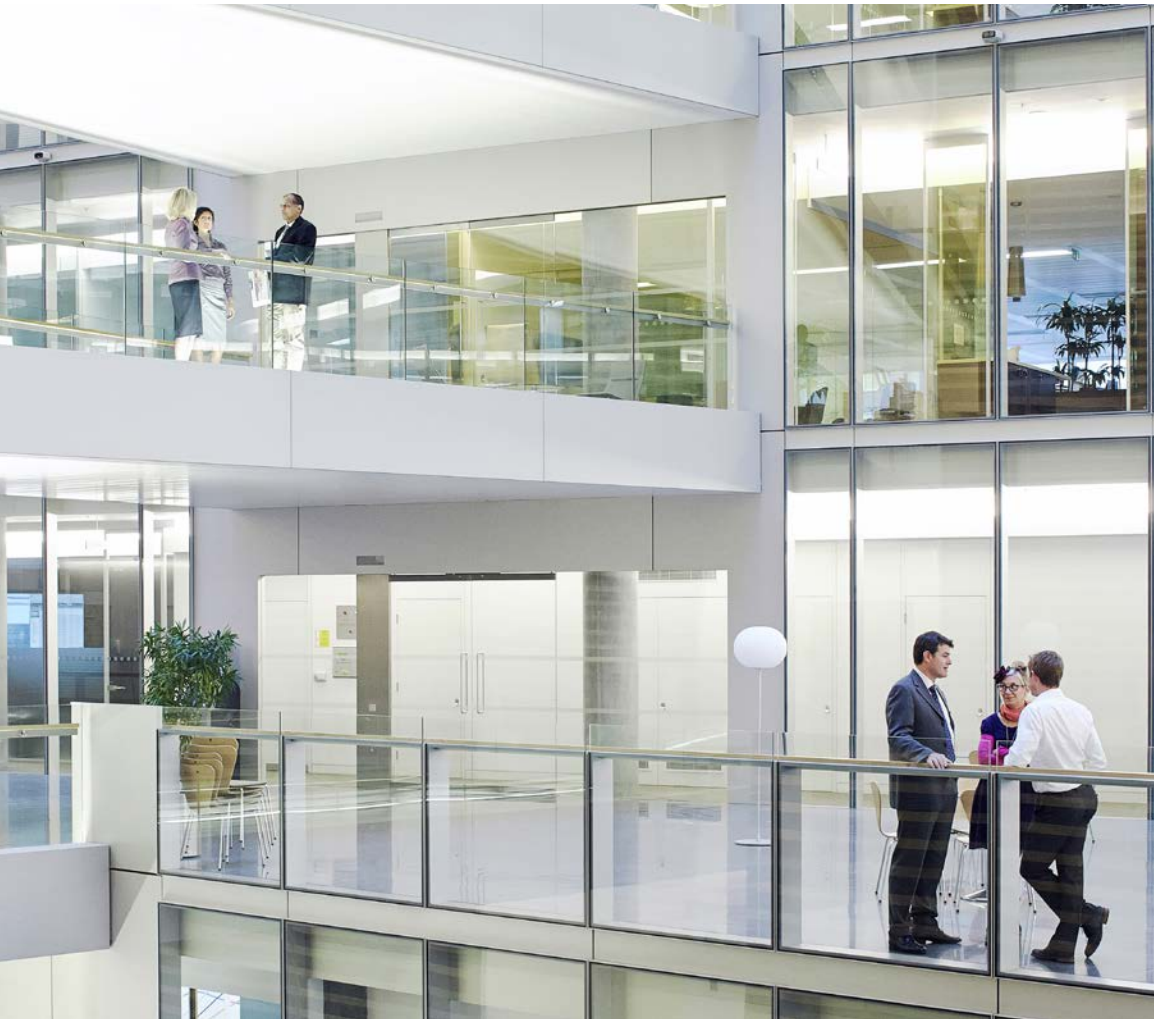
経済犯罪
リスクに対する焦点を変える
備えがもたらすチャンスを見据えて



36%

回答企業の3分の1以上が経済犯罪の被害にあったと報告

32%

サイバー犯罪は、企業に影響を及ぼす経済犯罪としてランキングの2位に上昇

44%

回答企業の半数近くが、自国の規制当局では経済犯罪を捜査・摘発するためのリソースが不十分であり、経済犯罪と戦う責任は企業が負っていると考えている

pwc

ハイライト

1 経済犯罪は手強い脅威

・回答企業の3分の1以上（36%）で経済犯罪の被害が発生している
・先進国と新興国のどちらにおいても被害が発生している
・経済犯罪の発見方法・技術が現状に追いついていない

経済犯罪を事前に食い止める手立てはあるのか

経済犯罪は多様化したグローバルな課題

2 組織の文化に統制（コントロール）を組み込む必要がある

・不正行為者の組織内外による差がなくなりつつある
・回答企業の5社中1社が、不正リスク評価を一度も行ったことがない

会社が直面するリスクを把握し、脆弱な部分を積極的に特定しようとしているか

金銭的損害が何億米ドルにも上る場合がある

3 サイバー犯罪の脅威は高まるが、企業の対策が追いついていない

・回答企業の32%が、サイバー犯罪の被害に遭い、このサイバー犯罪は、経済犯罪の種類別発生ランキングの中で2位になった。
・ほとんどの企業は、直面するリスクに対して十分な準備がまだできていないか、理解すらできていない：サイバー犯罪への備えがある企業はわずか37%
・マネジメントの積極的関与は極めて重要。しかし、自社のサイバー対策の状況について情報を要求する役員は半数未満

サイバー犯罪にはどのように対応すべきか

サイバー防衛は企業のストレステストとして見るべき

4 マネジメントと現場のギャップ

・回答者の5人に1人は、正式な倫理・コンプライアンスプログラムの存在を把握しておらず、その多くが、誰が社内のコンプライアンス責任者であるのか理解していない
・重大な経済犯罪の半数近くが内部犯行
・経済犯罪の弊害として従業員の士気低下（44％）と評判の失墜（32％）が上位に挙げられている

組織の価値基準と整合したビジネス戦略になっているか

人と文化が第一次防御ライン

5 迷走を続けるマネーロンダリング対策

・銀行の5行に1行は規制当局による査察を経験している。不正な商取引の抑止に失敗すると、個人的な賠償責任を負うおそれがある
・金融機関の4分の1以上が、海外拠点全体に対してマネーロンダリング対策（AML）／テロ資金供与対策（CFT）に関するリスク評価を実施していない
・回答者の33％がデータの品質を技術的な課題として挙げている
・AML／CFTの熟練スタッフがいないことが重要な課題である

規制当局の査察を受けた場合に、どのように対応するのか

コンプライアンス遵守のコスト（およびコンプライアンス違反によるコスト）は増加の一途をたどっている

目次

序文

ビジネスの世界における多くの有望な機会にはリスクという現実が付きまとう

この法則は、ビジネスの構築と維持に努める人々にとって真実であるだけでなく、経済犯罪を行う側の人々にとってもまた真実である。

2016年経済犯罪実態調査で示された結果は、これまでも幾度となく語られてきた内容である。経済犯罪は次々と新たな方法で企業に忍び寄っており、厳格な法規制の遵守は企業の負担を増加させている。さらに、脅威を巡る環境の複雑化が進み、対応のためのリソースと成長の間のバランスが危うくなっている。

この話は目新しいものではないが、目まぐるしく進化する今日のグローバル市場での成功を急ぐあまり、私は事の重要性を忘れているのかもしれない。

このレポートは、経済犯罪というリスクに対する焦点を変え、ビジネスチャンスにたどり着く道筋に再び焦点をあてられるよう、問題を提起する内容になっている。

本稿の内容は企業の日々の意思決定の中に組み込み、また、確固たる企業倫理によって裏付けされるべきものである。経済犯罪に対する綿密な計画を立てるものの、バインダーに綴じられたまま取締役の棚で誰にも顧みられることなく埃をかぶっている―こんなことでは、今日の世界で持続的成功を収めていくための備えがあるとは言えない。必要な備えとは、絶えず行う呼吸のようなものである。すなわち、脅威が現実のものとなったときに即応できるように、絶えず調整し、訓練し、目を配っておかねばならないのである。

自社のビジョンを深く理解しているか、そして、企業ごとに異なる脅威の状況や特徴に基づいた成長計画と防御計画を戦略的に構築できるか―これらが、チャンスを現実のものとするのか、会社を餌食にしようと狙っている人々の企みを許してしまうかの分かれ道となるのである。

Trevor White
パートナー、
経済犯罪実態調査 リーダー
PwC南アフリカ

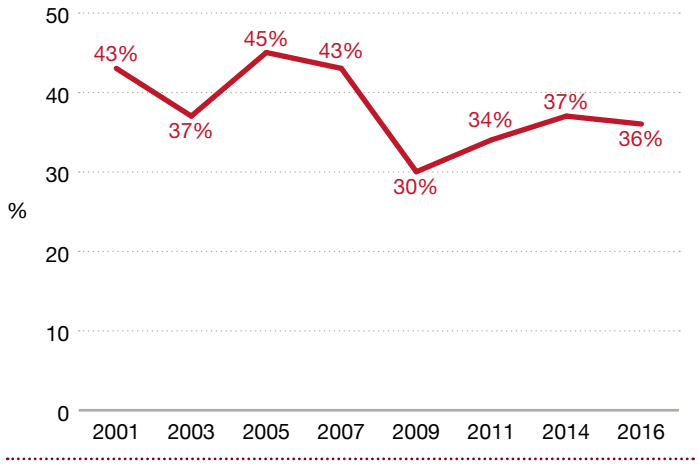
経済犯罪の進化

2016年：進化する経済犯罪、追いつかない予防策

経済犯罪実態調査 2016への6,000を超える回答の結果、回答企業の3分の1以上が、過去24カ月で経済犯罪の被害にあっていることが判明した。本年度の結果には、経済犯罪の発生がわずか1%とはいえ、2008年～ 2009年の世界金融危機以降初めて減少したことが示されている。

これは一見、企業がここ数年にわたって行ってきた予防策への投資が実を結んだことの証拠に見えなくもない。しかし、データを吟味すると、このわずかな減少の裏側には、実は悩ましい傾向が隠れている可能性もある。すなわち、経済犯罪が大きく変化しつつある中、発見と統制のプログラムが犯罪の変化のペースに遅れをとっているかもしれないのである。さらに、各不正行為がもたらす財務費用は増加しつつある。

図表1：経済犯罪報告比率の推移



本年度のレポートでは、経済犯罪の過去2年での変貌と、業界や地域に応じた違いについて説明している。

脅威が進化しつつあるにもかかわらず、内部統制による発見件数は7%減と、マネジメント主導の手法による犯罪の発見件数は減少している。さらに、5社中1社（22%）は、過去24カ月以内に不正リスク評価を一度も実施していない。第19回PwC世界CEO意識調査では、CEOの3分の2が、自社の成長を脅かす要因はかつてないほどに増えているとの見解で一致している（2015年の59%と比べて急増）。この結果を踏まえて先ほどの数字を見ると、悩ましい傾向が生じている可能性があることが分かる。すなわち、経済犯罪の発見が偶然の結果、という側面が非常に強いという点である。事実、調査結果によれば、経済犯罪の10件のうち1件が偶然に発見されている。

> ***調査結果によれば、経済犯罪のうち10件に1件は偶然に発見されている。***

経済犯罪の発見と防止への消極的な取り組みが多大な損害につながる可能性は、かつてないほどに高まっている。調査結果から、地域や経済発展のレベルとは関係なく、自国規制当局の法的措置や取り締まりに対する不信感の蔓延が明らかになったことは、この事実を浮き彫りにしている。

これが何を物語っているかは明らかである。すなわち、経済犯罪の防止、保護、対応の責任は、企業自体に負わされているのである。

本年度の調査は、サイバー犯罪、倫理・コンプライアンスプログラム、マネーロンダリング対策の3つの領域を中心としている。また、技術の普及と関連するリスクの管理、拡大するビジネス環境下で事業責任を果たすことの意味、意思決定に倫理的行動を組み込むことなど、共通のテーマを探っている。

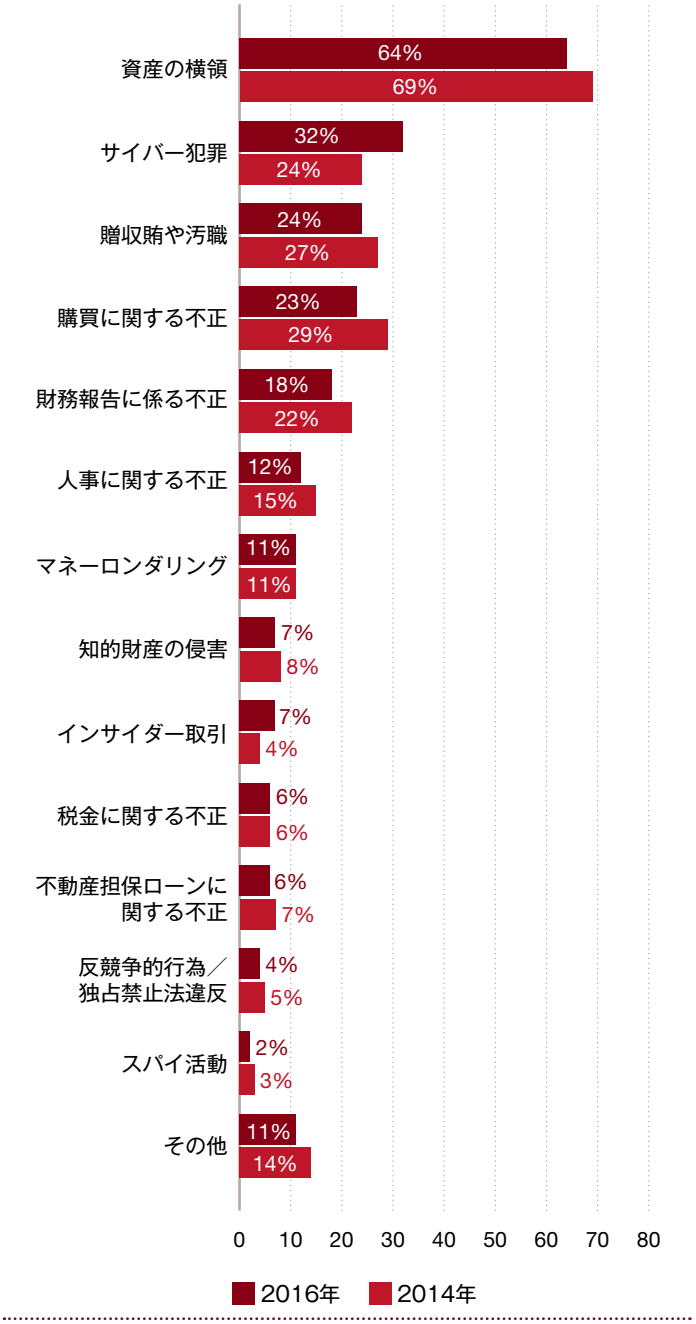
さらに本報告書は、企業のリスクの低減だけでなく、変化する世界の中で自社の防御に自信を持ち、脅威をより意識しつつビジネスで利益をもたらすような、より高度で効果的な方策の実施に重点を置いている。

2016年に報告件数が最も多い経済犯罪の上位三種類

昔ながらの犯罪が上位を占めているが…

2016年調査において回答企業にて発生した経済犯罪の種類別ランキングは、下記のグラフに示すとおりである。

図表2：発生分類別 経済犯罪報告率



従来上位を占めてきた資産横領、贈収賄や汚職、購買に関する不正および会計不正がいずれも本年は対2014年比で微減している。一方、サイバー犯罪は2011年に調査に初登場して以来、どの国でも着実に増えており、今回の調査では一躍二位に浮上している。

資産横領は歴史的に発見が最も容易な不正と見られており、調査で報告されているこの犯罪の割合は、以前は予想がかなり容易だった。しかし、2011年以降、同犯罪に関しては、報告比率が低下する傾向が見られる。これは、組織の内部統制が強化されたためと考えられる。つまり、企業は従来型の経済犯罪の防止に熟練してきたといえる。裏を返せば、経済犯罪は、サイバー犯罪を含むより多大な影響をもたらす別の種類の不正に姿を変えつつあるとも解釈できる。

サイバー犯罪が蔓延し、社内統制・管理による不正の発見比率が低下していることから、これらの犯罪の発見が難しくなっているのか、あるいは直面する脅威の変化を企業が認識できていないのかについて再考する必要がある。そして、どのような対策を講じるべきなのか、今一度検討すべきである。

回答企業の約20%が、今後24カ月の間にこうした主要な経済犯罪が発生する可能性が高いと考えており、リスクへの対処方針を見直すべきときが来ていると言える。

地域別 経済犯罪報告率

地域	2016年	2014年
アフリカ	57%	50%
西欧	40%	35%
北米	37%	41%
東欧	33%	39%
アジア太平洋	30%	32%
中南米	28%	35%
中東	25%	21%
世界全体	**36%**	**37%**

一部の地域では経済犯罪の報告率は低く、また、世界的な傾向は一定であった。しかし、アフリカ、西欧および中東は2016年の調査で大幅な増加を示した。アフリカにおける経済犯罪の報告率が高く、かつ上昇した主因は、南アフリカ（69%、2014年以来横ばい）、ケニア（61%、2014年以降17%増加）、ザンビア（61%、2014年以降35%増加）にある。他方、中東では、サウジアラビアの回答者は、経済犯罪の報告率が2014年の11%から2016年には24%と、2倍以上である。

西欧はフランス（68%）と英国（55%）が上位を占め、どちらも2014年比で25%増加している。
フランスの大幅な増加は、組織外の不正が急増したことによる。これは主としてサイバー犯罪で、2014年の28%から2016年には53%とほぼ倍増した。英国の増加は、サイバー犯罪の報告件数が対2014年比で83%増加したことによる。

サイバー犯罪の件数はほとんどの地域で増加しているが、東欧では2%減少している（全世界平均よりも10%低い）。また、サイバー犯罪はアフリカ、アジア太平洋、東欧の上位3種類の経済犯罪の中には登場しない。これらの地域では逆に、贈収賄や汚職、購買に関する不正の発生が全世界平均よりも高い。

ほとんどの先進国では規制による監視の目がより厳しくなっており、サイバー犯罪、マネーロンダリング、贈収賄や汚職など、慎重な取り扱いが求められる問題については特にその傾向が強い。犯罪に国境がなくなりつつあることで、規制と査察における国際協力の向上が求められている。

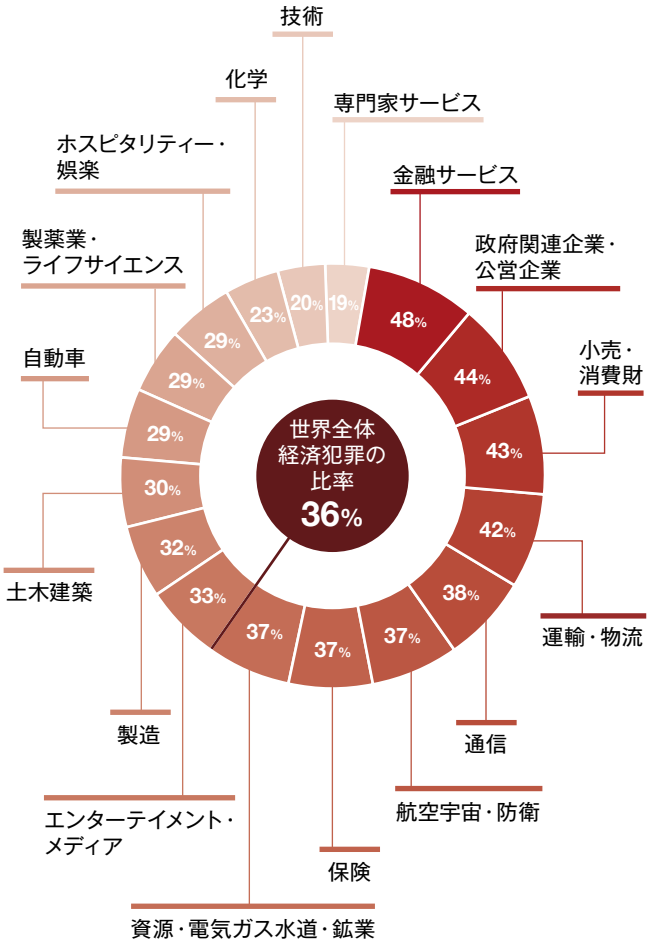
この統計数値が示しているように、経済犯罪は、犯罪の種類の面でも、新興国と先進国のどちらでも発生しているという点でも、非常に多様化が進んだグローバルな課題である。こうした犯罪の種類を理解することで、企業はその地域に効果的・効率的な犯罪防止の取り組みに集中することができる。

従って、規模や地理的な多様性と関係なく、全ての組織がグローバルな視野を持ち、経済犯罪対策に国際標準を設定し適用する必要があると言える。

あなたの業界が経済犯罪から受ける影響は？

金融業界は、その他の業界全てに金融サービスを提供するため、従来から最も経済犯罪の標的にされやすい産業であることが明らかになっている。

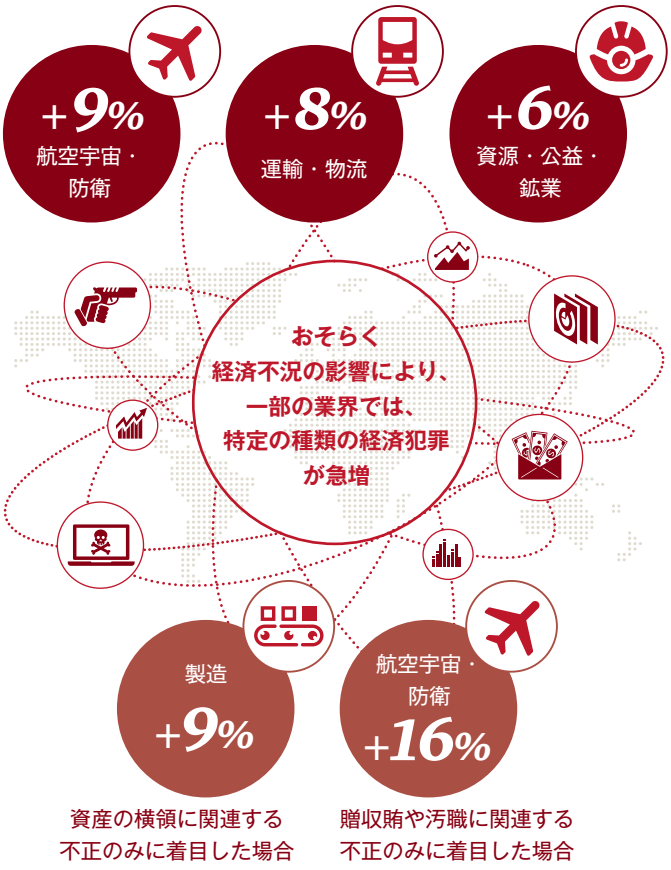
図表3：業界別の経済犯罪の報告率比較



しかし、市場が総合ビジネスソリューションの方向に進みつつあるため、金融業以外の多くの企業が、従来は銀行が行っていた業務を行うようになっている。自動車、小売・消費財、通信をはじめ、非金融業の企業は、金融業者と提携しているか、自ら銀行業務の認可を取得するケースもある。現金を付け狙う不正行為者にとっては、犯罪の手段が増えたのである。

金融業界は厳格な規制環境により、数十年にもわたり、高いレベルの内部統制、発見手法、リスク管理ツールを構築することができた。しかし、他業種から参入してきた企業は一般に、リスクにせよ急速に変化するコンプライアンス環境にせよ、確実に管理できるレベルには到達していない。

以下で示す業界が過去24カ月で経済犯罪の増加を経験



市況が変われば、脅威の状況も変化する。
定期的に再評価を行うことが、経済犯罪防止の鍵である。

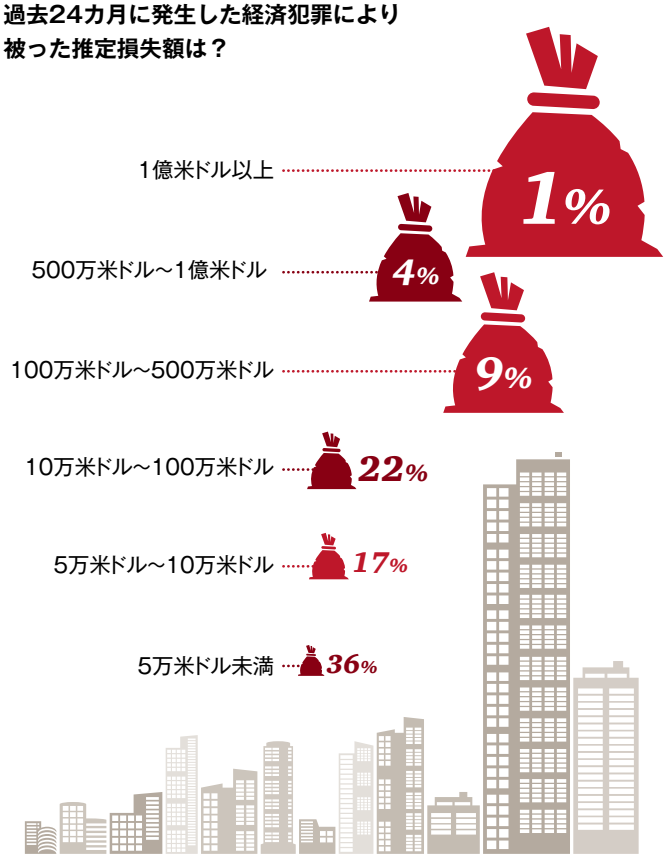
増える財務的損失と副次的損失

財務的損失は極めて高額になるおそれがある。回答企業の4分の1近く（22%）が10万米ドル～ 100万米ドル、14%が100万米ドル超、1%（主に北米とアジア太平洋）が1億米ドル超の損失を報告している。損失額は大きく、個々の犯罪のコストが増える傾向にあることが分かる。

それでは、世界経済は経済犯罪によってどのくらいのコストを負担しているのか。重大な経済犯罪の場合、犯罪による直接の財務的損害が、副次的影響による損害に比べわずかである場合が多いことを考えると、正確な数字を見積ることは難しい。回答企業は、事業の混乱、是正策、調査や予防、規制当局からの罰金、訴訟費用を含め、副次的な損害の方が大きいと一様に述べている。 そして重大なのは、士気と評判が損なわれ、長期的な業績に多大な影響が及ぶことである。この種の損失は当然ながら、いつでも定量化が可能なわけではない。しかし、いずれは財務的損害の短期的影響が小さく見えるほどに増大する可能性がある。

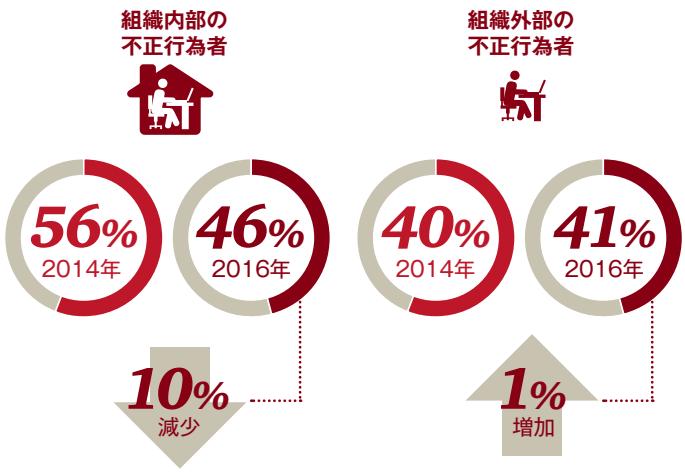
図表4：経済犯罪による財務的損害

過去24カ月に発生した経済犯罪により被った推定損失額は？



不正行為者のプロフィール

前回の調査以来、組織内外の不正行為者の差がなくなりつつあることが確認できた。



今回の調査結果でも内部犯行者の半数以上が中間・上級管理職であったが、それらに加え幹部補佐が内部犯行の多数を占めている地域もあった。これは、内部統制に潜在的な弱点があることを示すものである。つまり、内部統制が、企業の文化に組み込まれた効果的なプロセスではなく、チェックボックスにチェックをつけるだけの、単純作業に等しい状態となってしまっている可能性がある。さらに、回答者の22%が不正リスク評価を一度も実施したことがなく、31%はリスク評価を年に一度しか実施していないという事実からも、そうした状態が伺える。

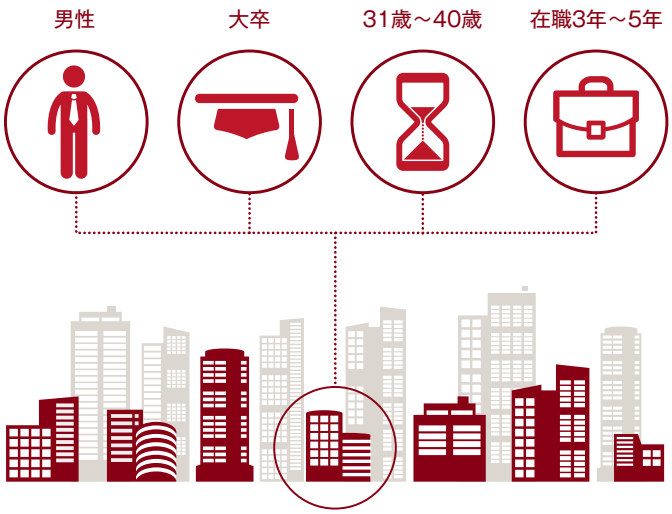
アジア太平洋など、一部の地域では、上級管理職の不正が急増している。これらは発見が最も困難で、影響も非常に大きい場合が多い。

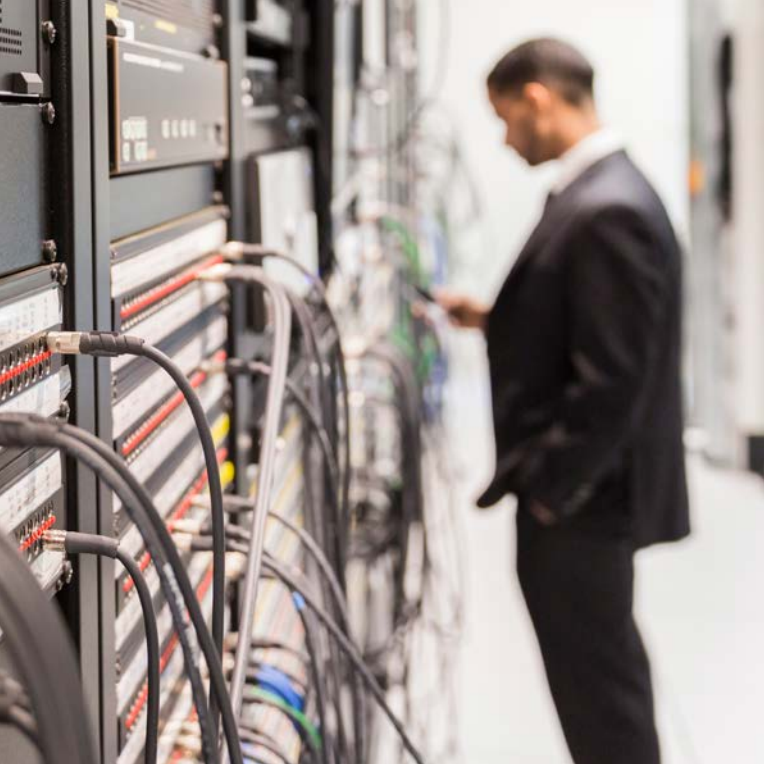
地域単位では犯行は組織内部の人物によると答えた回答者が大幅に減っているにもかかわらず、地域別で見ると、アフリカ（全世界平均よりも7%高い）、アジア太平洋（9%高い）、および中南米（9%高い）では、組織内の人物が依然として不正の主役である。

逆に、組織外の人物による不正の件数は、全世界平均の41%に対して、東欧（44%）、西欧（49%）、北米（56%）ではより高いという結果が得られている。

不正行為者の種類の最も根本的な変化が生じたのは北米で、内部犯行者の減少と外部犯行者の増加が非常に顕著であった。

組織内部における不正行為者の特徴



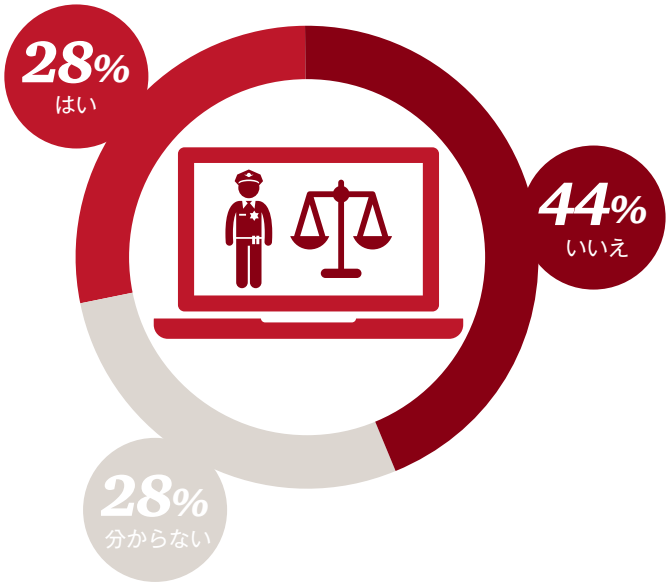


取り締まりは万全か

自国の規制当局に十分なリソースがあり、経済犯罪の捜査と起訴ができるように訓練されていると思うかどうかについて意見を求めたところ、回答企業の44％が自国の規制当局能力に疑問を抱いており、28％が分からないと答えた。

この数字は、複数の異なる要因―例えば、国の経済犯罪率、サイバー犯罪などの特定領域に対する専門能力を各国の規制当局がどの程度重視（または軽視）しているか、規制当局がどの程度政治的干渉をうけないか―の影響を受けているものと考えられる。

図表5：自国の規制当局は、経済犯罪の捜査と起訴ができるような十分なリソースを持ち、訓練を受けていると思う回答者の割合



自国の規制当局には経済犯罪を取り締まるのに十分なリソースがないと考える上位15カ国

1	ケニア	79%
2	南アフリカ	70%
3	トルコ	60%
4	フィリピン	58%
5	ブルガリア	58%
6	ポーランド	58%
7	ウクライナ	57%
8	メキシコ	56%
9	ザンビア	55%
10	ナイジェリア	54%
11	オーストラリア	52%
12	米国	52%
13	フランス	51%
14	ベネズエラ	50%
15	インド	49%

備えを固め、前へ進む

経済犯罪は絶えず進化しており、企業や国にとって益々複雑な問題になりつつある。規制の状況も変わりつつあり、ビジネス慣行に多くの課題を突きつけている。自国の法的措置が必ずしも実質的な力を発揮できるとは思われていないため、自らとその関係者を経済犯罪から保護する責任は各国経済界の肩に重くのしかかっている。

以降の3つのセクションで、サイバー犯罪、倫理・コンプライアンスプログラム、マネーロンダリング対策という戦略的に極めて重要な領域について論じていくが、調査結果の統計数値はトレンドを示すだけではなく、前向きな思考の企業が新たな課題に取り組む際の重要な指標としても役立つ。

サイバー犯罪

軍需物資はセキュリティや管理が強固であると思われている。しかし、ハッカーは、「低リスク」のサプライヤーはセキュリティや管理水準にばらつきがある事を知っており、その穴を突くことで容易に物資納入先の特定が可能である。

国境なき脅威

デジタル技術はビジネスの世界に革新的な変革をもたらし続け、企業にとってはチャンスにも脅威にもなりうる。従って、サイバー犯罪が拡大の一途をたどるのは当然であり、本年は経済犯罪の種類別報告件数の中で2番目に多い経済犯罪タイプとなっている。

ビジネス活動全般と同様、経済犯罪もデジタル化が進んでいる、というのが2016年の状況である。複数の国と地域にまたがることの多い高度にネットワーク化された今日のビジネス環境では、サービスプロバイダー、取引業者、政府当局などの第三者を含め、システムのどの接点で問題が発生しても、企業のデジタル環境はさまざまな悪影響を受ける可能性がある。それだけではない。サイバーリスクは今や従来のコンピューター観を超えている。あらゆる物のインターネット化が進み、自動車や家庭用機器といった物にまで対象とする攻撃が急増している。

昨今の企業は、新しいデジタル接続、ツール、プラットフォームにより、顧客、サプライヤー、パートナーとリアルタイムでつながることで、かつてないほどに取引の範囲が広がり、しかも迅速に処理できるようになっている。しかし、同時に、サイバー犯罪がそのポテンシャルを制限する強力な対抗勢力となっている。これがデジタルパラドックスである。

ビジネスリーダーはその足かせに悩んでいる。第19回PwC世界CEO意識調査では、CEOの10人に6人が、サイバー犯罪の脅威とテクノロジーの進化速度を、成長を脅かす上位の存在として挙げている。

本年の経済犯罪実態調査結果でも、上級管理職やその他の要職にある者が適切な介入もサポートもせずに、初期対応を情報技術部門にまかせきりにしている企業が非常に多いという穏やかならぬ事実が示されている。さらに、対策チームの構成に根本的な欠陥があることも多く、データ侵害への対応に決定的な影響を及ぼすことになる。

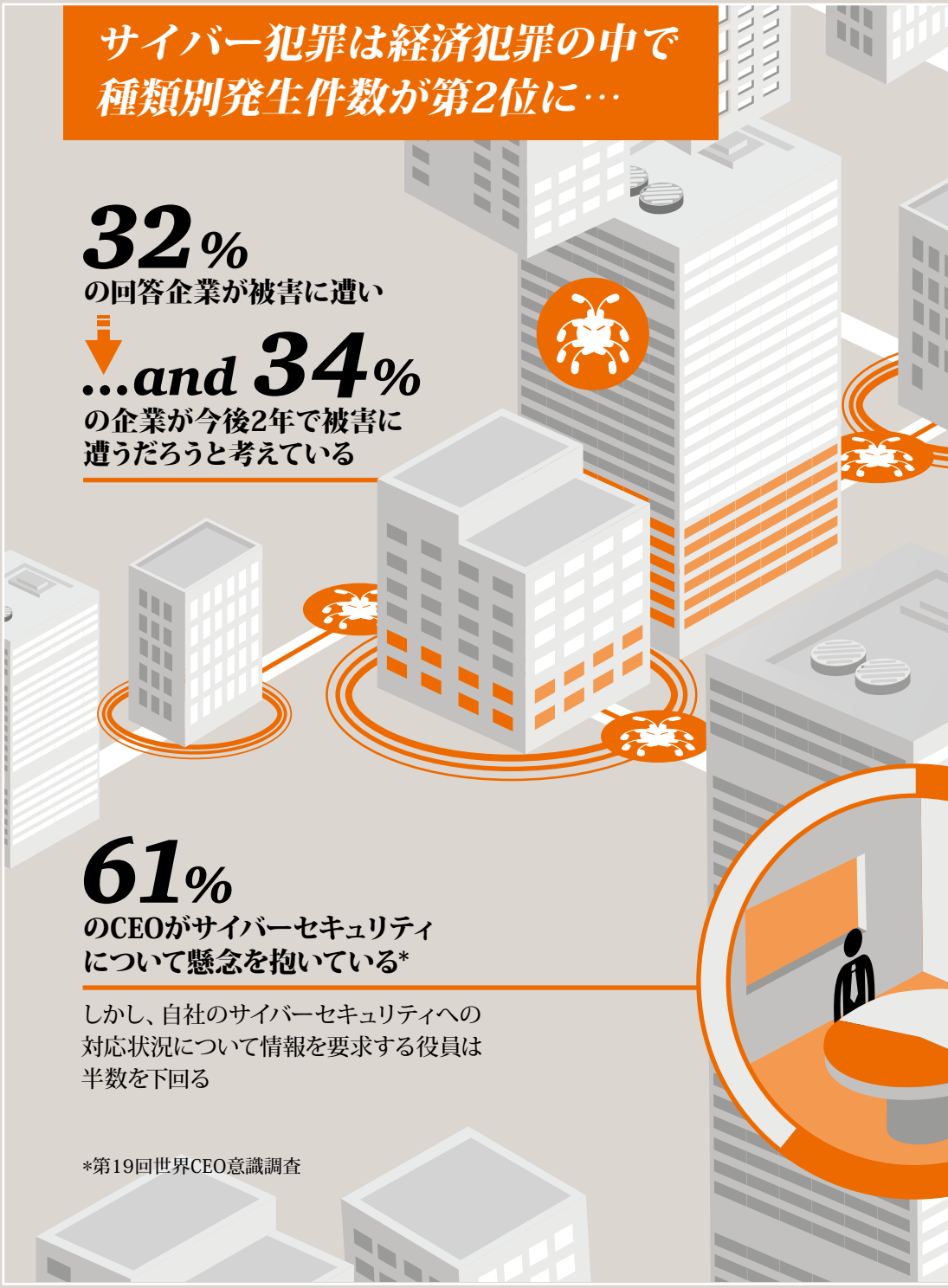
デジタル戦略に対する全社的な取り組みと世界中の何千もの企業との共同作業を通じて、PwCはデジタル時代のリーダーがとるべき行動は何かを特定した。その代表的な一つは、「サイバーセキュリティとプライバシーに対する積極的な姿勢」である。これは、役員と経営幹部レベル、中間管理職から時間給労働者に至るまで、組織の全員が自らの責任として捉える必要がある。

高度にネットワーク化されたビジネス環境の中で、サイバー犯罪の拡大は留まるところを知らず、経済犯罪の中で発生件数第2位に躍り出ている

サイバー犯罪は経済犯罪の中で種類別発生件数が第2位に…

32%
の回答企業が被害に遭い

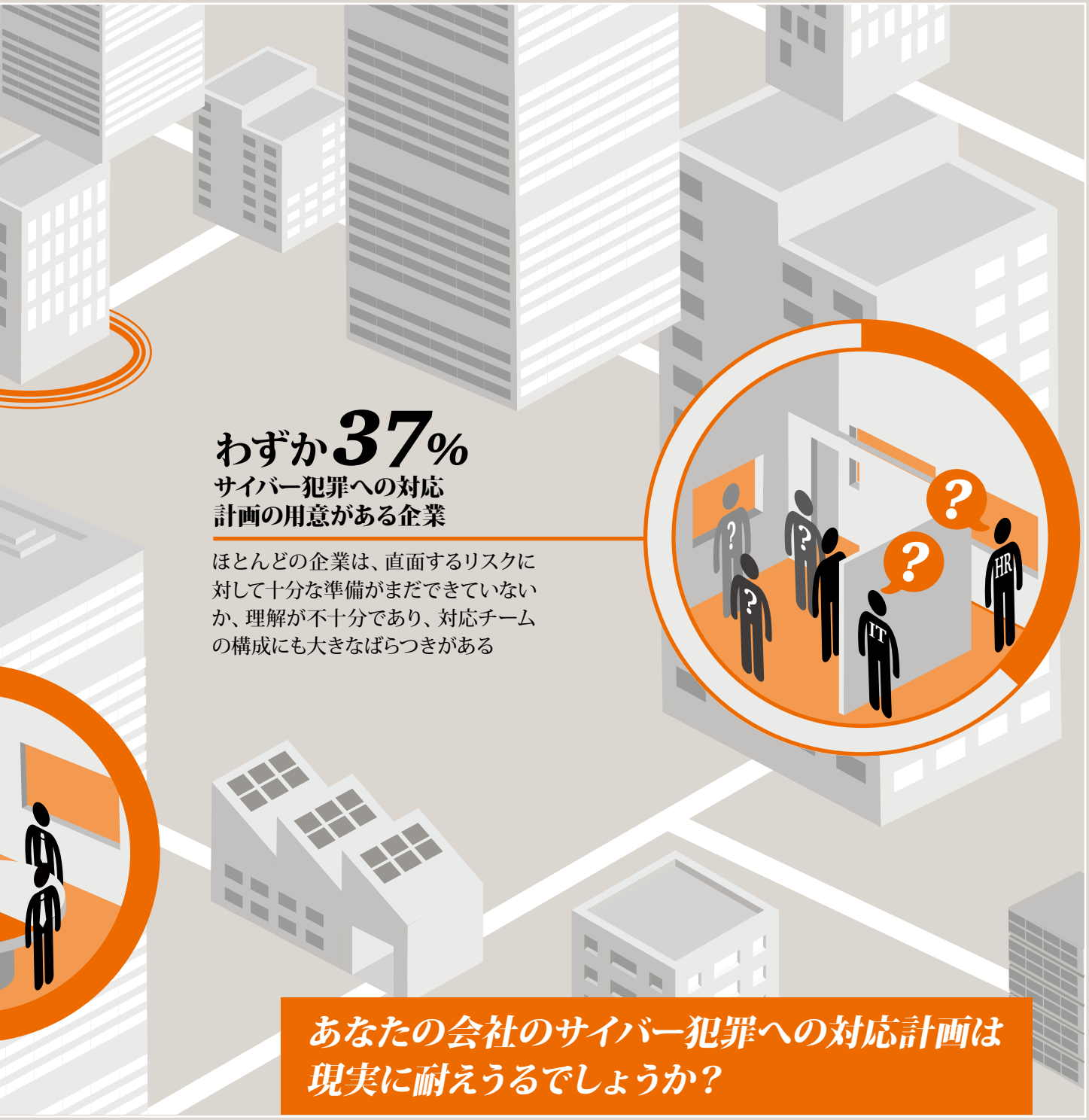
…and 34%
の企業が今後2年で被害に遭うだろうと考えている



61%
のCEOがサイバーセキュリティについて懸念を抱いている*

しかし、自社のサイバーセキュリティへの対応状況について情報を要求する役員は半数を下回る

*第19回世界CEO意識調査



わずか37%
サイバー犯罪への対応計画の用意がある企業

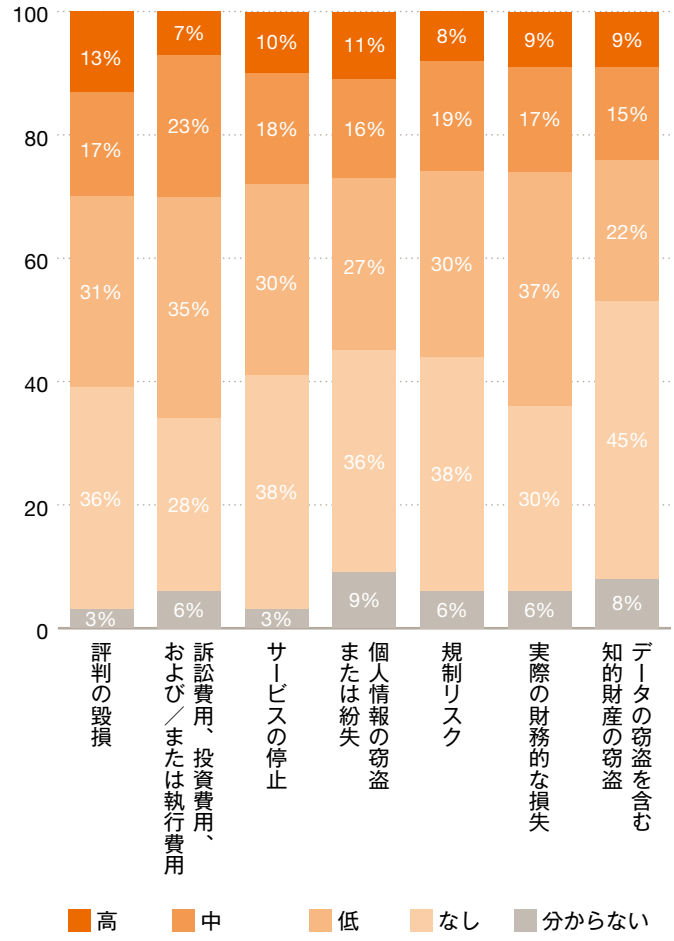
ほとんどの企業は、直面するリスクに対して十分な準備がまだできていないか、理解が不十分であり、対応チームの構成にも大きなばらつきがある

あなたの会社のサイバー犯罪への対応計画は現実に耐えうるでしょうか？

調査結果：サイバー犯罪は増加が続いている

サイバー犯罪は今年になって急増し、経済犯罪の中で種類別発生件数が第4位から第2位に躍り出た。サイバー犯罪が主な経済犯罪の中でも唯一増加した傾向にあったことは特筆すべきである。回答企業の4分の1以上が、サイバー犯罪の被害に遭った経験があると答えている。また、被害にあったかどうか分からないとの回答が18%あった。

図表6：サイバー犯罪による被害の傾向



損失は多額になる可能性がある。一部の企業（約50社）では、500万米ドルを超える損失を被り、そのうちの3分の1近くが、サイバー犯罪に関係する損失が1億米ドルを超えたと報告している。

回答企業は、サイバー攻撃による最大の被害は評判の毀損であると考えており、わずかな差で訴訟費用、投資費用、執行費用が続く。

この脅威の恐ろしい点は、被害にあっていないと答えた56%の回答企業のうち、多くが気づかずに被害を受けていた可能性が高いことにある。懸念すべきは、ハッカーが企業のネットワークに長期にわたって気づかれずに留まることに成功していることである。

攻撃者は、より被害の大きい活動を隠すために陽動作戦を繰り広げることも知られている。陽動作戦の一つに、注意をそらす手段としてサービス妨害攻撃を分散的に行う方法がある。分散攻撃はいわばノイズのようなもので、その間にゆっくりと気づかれないように本命の攻撃を展開するのである。通常、その種のシナリオでは、攻撃者は自らにとって価値のないシステムに攻撃を仕掛ける。これは緊急対応チームの注意をそむけている間に、攻撃者はその裏で、本命として狙っていた情報を密かに引き出すためである。

サイバー攻撃を受けるリスクがある業界

今日では、全ての業界がリスクにさらされている。かつては標的にされる可能性が低いと考えられていた業界も例外ではない。PwCのグローバル情報セキュリティ調査2016によると、2015年にサイバー犯罪が最も顕著に増加した業界は小売である。金融業は依然として狙われやすい業界の一つではあるが、横ばい状態で、過去3年にわたり、攻撃の回数はほとんど増えていない。

企業と国家がなぜ知的財産を盗むのか

- 多くの先進国では、IP（知的財産）を中心とする大規模なデータ侵害の傾向がみられる。個別の企業をランダムに攻撃するのではなく、戦略的に組織化された大規模な作戦の一部として行われるのである。
- こうした大規模な攻撃の一部には、国家が裏で糸を引いている可能性があるが、これは重要なインフラを破壊しようとするテロリズム的問題ではなく、経済犯罪の問題である。
- 他社の知的財産を盗むことには、経済的行動原理があり、自前で研究開発を行うよりも、経費と時間を節約できるためである。
- アドバイス：同業他社が攻撃を受けた際は、次は自社が標的にされる番だと考えるのが賢明である。

二種類のサイバー犯罪とその意味

若いハッカーが銀行カードを盗んでいた頃からは、随分と時代が変わった。認知度の面でも、攻撃者の身元や出所を検出する技術レベルにおいても、称賛に値する大幅な向上があった。しかし、不正行為者と企業の戦いの激しさに変わりはない。企業側から見ると、戦いに本当の勝利が訪れることは永久にない。

過去数年で、サイバー経済犯罪は次の二つにはっきりと分けることができるところにまで進化した。一つは、金銭を盗み、企業の評判を傷つけるタイプ、もう一つはIP（知的財産）を盗んで事業全体の存続を揺るがすタイプである。

- **サイバー不正**：IDやクレジットカードの窃盗など、金銭に還元できるサイバー犯罪は、多額の損失や多くの被害者が出るため、世間の注目を浴びやすい事件である。この種の犯罪は注目を集めるものの、企業の存在を脅かすことはほとんどない。
- **IP（知的財産）の侵害**：企業が直面する、より深刻な経済犯罪は、国際サイバースパイの犯罪、すなわち、重要なIP、企業秘密、製品情報、交渉戦略などの窃盗である。サイバー専門家の間では、これらの犯罪は「壊滅レベル（extinction-level）の事件」と呼ばれているが、それにはもっともな理由がある―損害が極めて多額になる可能性があり、事業レベル、会社レベル、さらにそれをも超えるレベルの損害が生じる可能性すらあるためである。こうした種類の攻撃は発見が困難なだけでなく、企業の脅威を感知するレーダーでは検知できない場合もある。

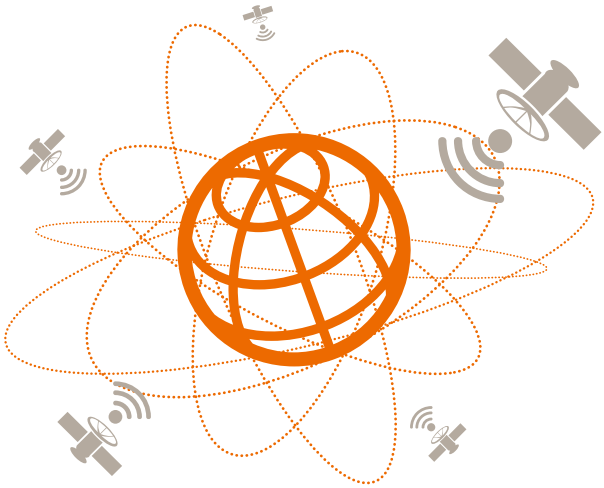
組織と経済の両方に対する長期的な損害は、IP（知的財産）の侵害の方が遥かに大きくなる可能性がある一方で、クレジットカード情報や個人情報の漏えい・窃盗は社会の耳目を集め、メディアの監視や法規制の対象となる可能性がある。

脅威のベクトル：5つの種類

国家
サイバー戦争が含まれる。また、被害者には、政府機関、インフラ、エネルギー、有力な知財保有企業などが含まれる。

インサイダー
社員に限らず、会社の直接管理下にないものの、重要情報にアクセス可能な第三者も含まれる。

テロリスト
現時点では比較的初期段階の脅威。脅威には混乱やサイバー戦争などが含まれ、被害者には、政府機関、インフラが含まれる。



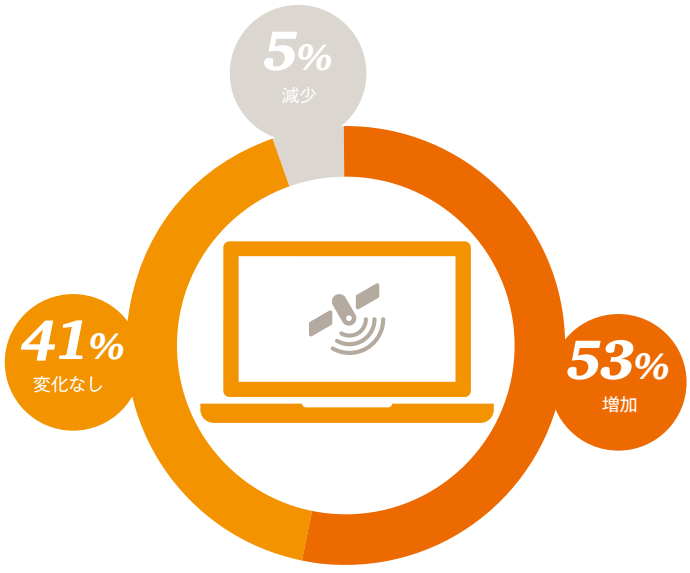
組織的犯罪シンジケート
犯罪組織の脅威には財務情報や個人情報の窃盗（インサイダーの共謀による場合もある）が含まれる。被害者には、金融機関、小売業者、医療法人、ホスピタリティー企業が含まれる。

社会的・政治的主張を目的とするハッカー
脅威には、サービスの停止、または評判の毀損が含まれる。被害者には、注目度の高い組織や政府が含まれる。被害者にはあらゆる種類の組織が含まれる。

備えはできているか

回答企業の半数以上（53%、対2014年比で）が、サイバー犯罪の脅威にさらされるリスクが増えていると見ている。おそらく、サイバー犯罪に関する報道が著しく増えているためと思われる。しかし、調査によると、企業はそれでも現在のサイバー犯罪の脅威に対応する備えが十分にできていない。

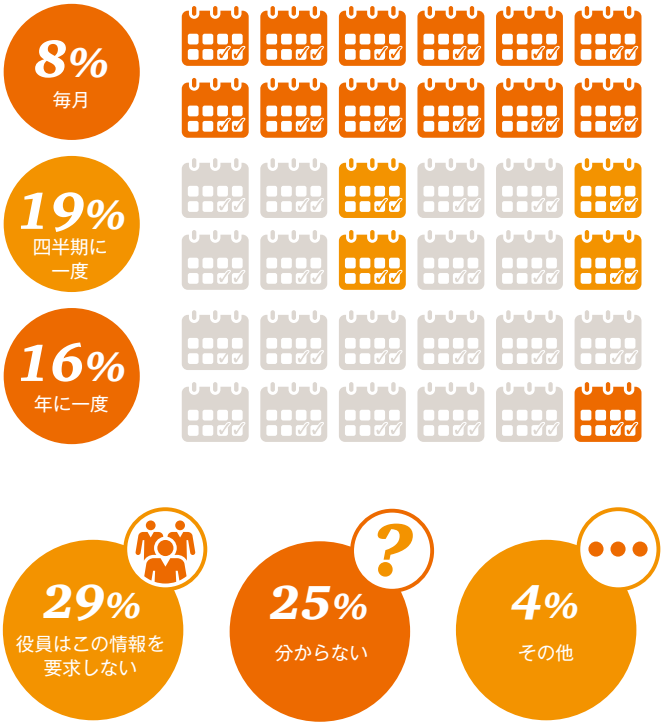
図表7：サイバー犯罪のリスクに対する認識



サイバー脆弱性を正す第一の責任はトップにある。しかし、調査によれば、いくつかの国では取締役にはサイバーリスクに関して株主に対する受託者責任があるにもかかわらず、多くの取締役はサイバー犯罪の脅威に関して積極的な姿勢が欠けており、リスクを適切に評価できるほどに自社のシステムを十分に理解していない（例えば、米国証券取引委員会は、今後の検査では会社のサイバー対応能力を考慮するとの警告を発している[1]）。驚くべきことに、自社のサイバー犯罪への対応状況について情報を要求する役員は半数を下回る。

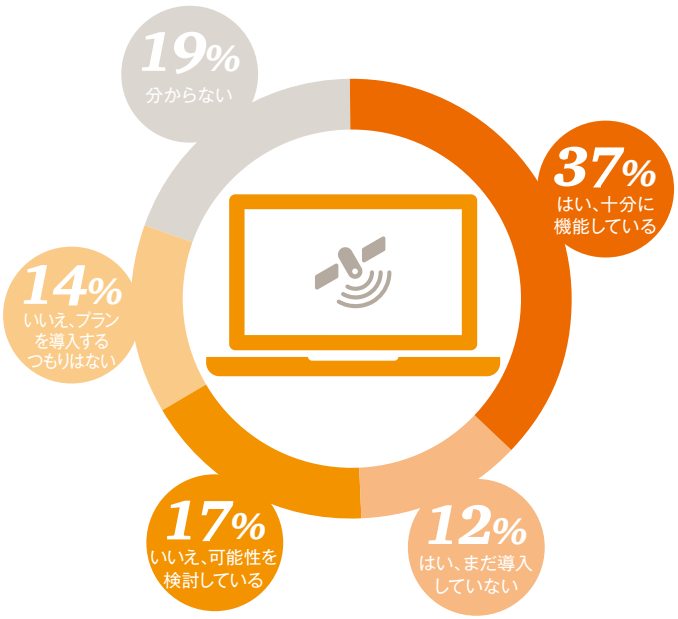
1）https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

図表8：組織のサイバー危機対応能力に関して取締役が情報を要求する頻度



十分に機能する危機対応計画を立てているのは、回答企業のわずか37％（そのほとんどが規制の厳しい金融業界に属している）である。10社中3社は計画を一切立てておらず、そのうち半分近くは必要性を感じていない。

図表9：企業はサイバー攻撃に対応する危機対応計画を立てているか



サイバー危機が発生した際に初期対応が可能な「十分に訓練された」人員を備えている企業は、10社に4社しかない。その人員のうち、圧倒的大多数（73%）がITセキュリティスタッフである。

「企業のリーダーであれば、自社の防衛能力の程度を把握しているべきであり、重大なセキュリティ侵害が発生した場合の対応計画が準備されているのかどうかを確認しておくべきである。また、サイバーセキュリティが破られる脅威と、その脅威に自社がどんな対応をしているかについて、定期的な報告を受けている必要がある」

アメリカ合衆国財務長官 Jacob Lew、2014年7月

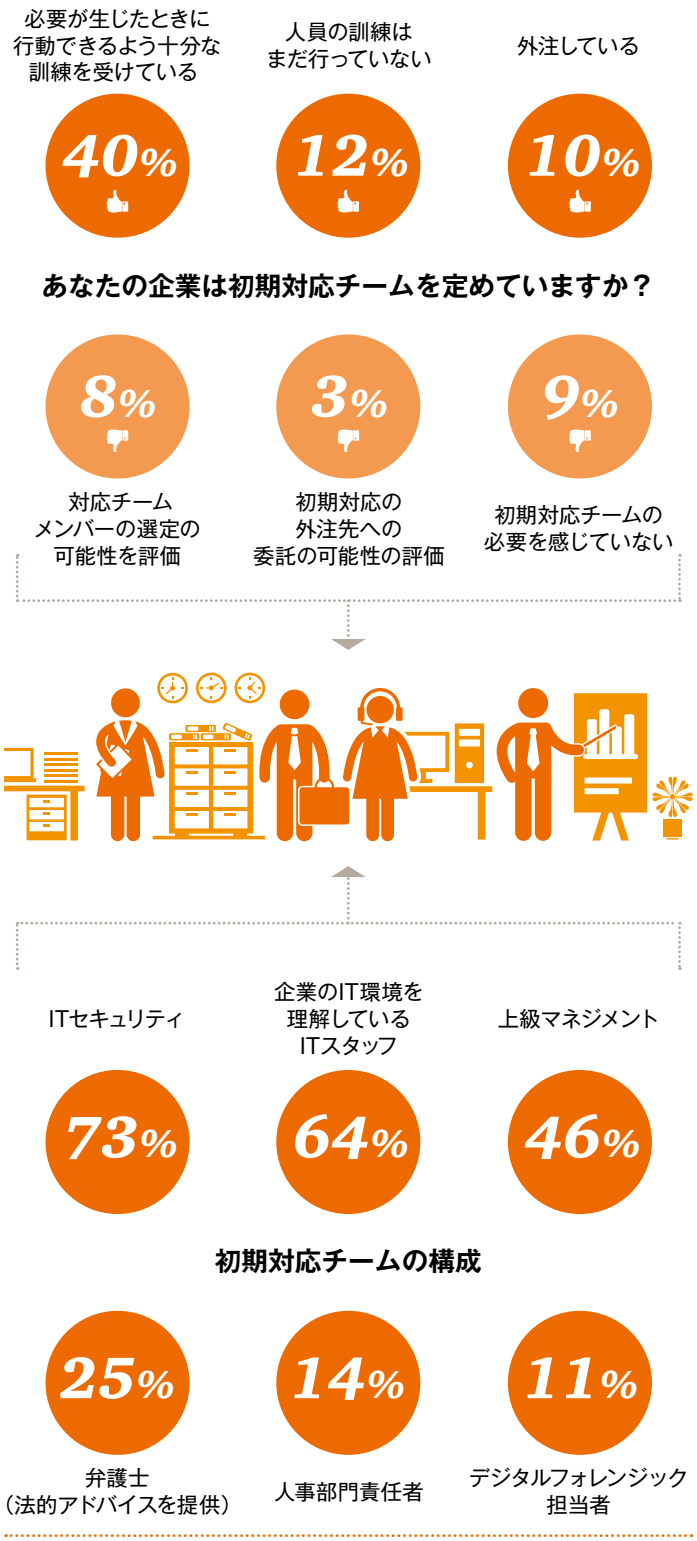
サイバー攻撃の発見と回避に重要な役割を果たすのはITスタッフであるものの、上級管理職（46%）、法務（25%）、人事（14%）など、上位レベルの危機管理を担当するメンバーが含まれている初期対応チームは半数以下であったことは注目に値する。デジタルフォレンジック担当者が含まれている緊急対応チームは、10チーム中1チームのみであった。

こうした結果は、仮にサイバー犯罪が起きた場合に、多くの企業が攻撃を抑えシステム復旧を急ぐあまりに、重要な証拠となり得る情報を見落とし、後に法廷で争う際に不利となる状況に陥る可能性を示している。さらに重要なことは、セキュリティが破られた原因を解明する手がかりが失われるおそれもある。

対応時の連携が不十分であると、実際に攻撃された全ての領域について調査する能力が不十分となる場合がある。これは、ハッカーが陽動作戦を頻用することを考えると特に重要である。

最後に、攻撃への対応を急ぎすぎると、会社は攻撃の総合的な影響を十分に理解することができず、メディアを含め、会社内外の関係者への適切な説明ができなくなるおそれがある。これは評判の失墜につながる可能性がある（本年度の調査で、サイバー攻撃による最大の被害として挙げられている）。

図表10：サイバー犯罪初期対応チーム



犯行の発見：危機管理

犯行に気付いた時に社内で何を行うか。効果的な発見から対応までの間隔を短縮し、事業への悪影響を可能な限り素早く食い止めることが極めて重要である。初期対応チームを招集した後に行うべき手順として以下が想定される。

- 犯行に関する重要事実を把握し、まだ進行中なのかどうかを確認する。ネットワークが複雑化しているため、犯人がネットワークに侵入した方法を突き止めることは困難な場合もある。高度なフォレンジックおよびデータ分析ツール（外部の専門家から入手できるものも、規制当局から入手できるものもある）は、この段階で極めて重要である。
- 発見された攻撃が、ときには組織へのさらに深い侵入を隠すためのものである可能性を考慮する。状況によっては、犯行を発見し、損害を食い止めるまでに、数時間ではなく数週間かかる場合もある。
- 規制当局の介入を求めるべきか、求めるならどこまで求めるべきか、地方と中央政府のどちらが適切かを判断する。考慮すべき要因は多数あり、攻撃の種類と規模によっても異なる。回答企業の半数近くが政府のサイバー犯罪調査能力を信用していないことは、重大な問題である。
- 二次的リスクを検討する。例えば、電子メールが傍受されただけでも相手に企業秘密が漏れる場合がある。ネットワークが不正侵入を受けると、会社がVoIPやネットワークによる電話サービスを利用している場合、電話も被害を受ける可能性が高い。
- 最後に、データ侵害が発生したら、サイバー捜査であろうとも基本的には捜査であること、犯罪捜査の原則が適用されることを覚えておく必要がある。進行中の攻撃を阻止して復旧することに注力する一方で、捜査と次の攻撃の防止に役立つ可能性のある証拠をうっかり破壊してしまわないよう注意することが非常に重要である。

重層的な防御体制の重要性

サイバー犯罪の脅威とその軽減は企業全体の責任である。全員がそれぞれ果たすべき重要な役割を担っている。しかし、前回の調査以来、サイバー攻撃に対する意識が高まっている一方で、ほとんどの企業において、直面しているリスクを理解する点においても、事件を予測し、効果的に管理する点においても十分な準備ができていない。

サイバー犯罪での損害を被る企業が非常に多いのは、基本的な部分に不備があるためである。役員の積極的取り組みが不十分である、システム構成が貧弱である、ネットワークにアクセスできる第三者の管理が不十分である―企業は、こうした基本的問題点により苦しんでいるのである。これは、侵入者のために機密情報のドアを開けたままにしているようなものである。

取締役が日常のリスク評価にサイバー犯罪を組み込み、計画を組織の全体に伝え、不正侵入があったらどの段階で通知を受けるようにしたいかをIT部署と具体的に話し合って決めておくことが非常に重要である。

サイバー犯罪の脅威は、事業に影響を与える可能性のあるその他の潜在的な脅威や混乱（テロや自然災害）と同じように理解し、対応計画、役割と責任の明確化、監視とシナリオの計画といった対策を立てておく必要がある。 一流企業が危機管理演習をサイバーセキュリティとインシデント対応戦略の中心要素に組み込んでいるのは、そのためである。一流企業は、定期的に演習を実施し、具体的なシナリオを検討し、対応計画のストレステストを行い、ギャップや不足点を特定するのである。

ITの脅威とその対応策は企業全体の責任である

マネジメントレベル：

- 健全なサイバーセキュリティ戦略を定める
- 質の高い情報が届き、それを消化できるようにする
- ユーザーのセキュリティ意識を高めるプログラムを導入する
- 戦略に基づくセキュリティ投資をサポートする

監査と各種リスク対応チーム：

- 技術上のリスクを徹底的に理解する
- 事前のデューデリジェンスを実施し、第三者に関連するリスクを軽減する
- (非財務の)運用システムに関連するリスクに対応する
- 基本的なIT監査の問題に対応する

法務：

- 進化するサイバー規制環境を理解する
- サイバー事件に対して規制当局が下した決定をモニタリングする
- サイバー保険を無効にしかねない要因に配慮する

IT：

- フォレンジック調査への対応準備状況を評価する
- 変化する脅威の状況と攻撃に目を配る
- インシデント対応計画をテストする
- 効果的な監視プロセスを導入する
- 新たな戦略を採用する：サイバー攻撃シミュレーション、セキュリティ研修、ゲーミフィケーションによる研修およびセキュリティデータ分析

企業のサイバー危機は、組織が直面し得る最も複雑で困難な課題の一つである。サイバー犯罪に対応するには、相当なフォレンジック・分析能力を含め、高度な通信および調査戦略が必要とされ、この戦略を正確・迅速・冷静に遂行しなければならない。

防御力の強化に向けた取り組みは面倒な部分もあるが、良い面もある。企業のストレステストとして捉えればよいのである—これは、プロセスの改善につなげることができ、またつなげるべきテストなのである。今日のリスク環境においては、会社のサイバー危機への準備状況は、競争優位性、究極的には企業存続のバロメーターともなり得る。

「サイバー犯罪に対する防御の基本が欠けているのは、侵入者のためにサイバーセキュリティのドアを開けたままにしているようなものである」

PwCグローバル・米国担当サイバーセキュリティリーダー、David Burg

計画づくりもよいが、実践こそ最重要

多くの企業が、労をいとわずにさまざまな演習を行い、サイバーインシデントに確実に備えようとしている。

だが残念ながら、事が発生した最初の段階で計画どおりに行くことは希であり、初期対応チームも危機管理者も不測の事態に見舞われることが多い。

危機に効果的に対応するには、幅広い部門—法務、人事、システム、法律顧問、監査、リスク、財務、セキュリティ、広報、さらには、現場の事業ユニットや地域統括部門などのスキルや知識が必要である。

定期的な演習プログラムによる「計画の計画を立てる」プロセスは、結果的に策定される計画そのものよりも遥かに価値がある。これにより、インシデントの対応が無意識下で構築され、プロセス、環境への対応、そして意思決定を反射的に実行できる。それによって、危機時にプレッシャーを受けても、目の前の問題の解決に集中できるようになる。

主なお問い合わせ先

David B. Burg
PwCグローバル、米国アドバイザリ
サイバーセキュリティ、プライバシーリーダー
電話：+1 (703) 918 1067
電子メール：david.b.burg@us.pwc.com

Kris McConkey
パートナー
PwC英国
電話：+44 (0) 77 2570 7360
電子メール：kris.mcconkey@uk.pwc.com

Junaid Amra
アソシエイトディレクター
PwC南アフリカ
電話：+27 (31) 271 2302
電子メール：junaid.amra@za.pwc.com

倫理とコンプライアンス

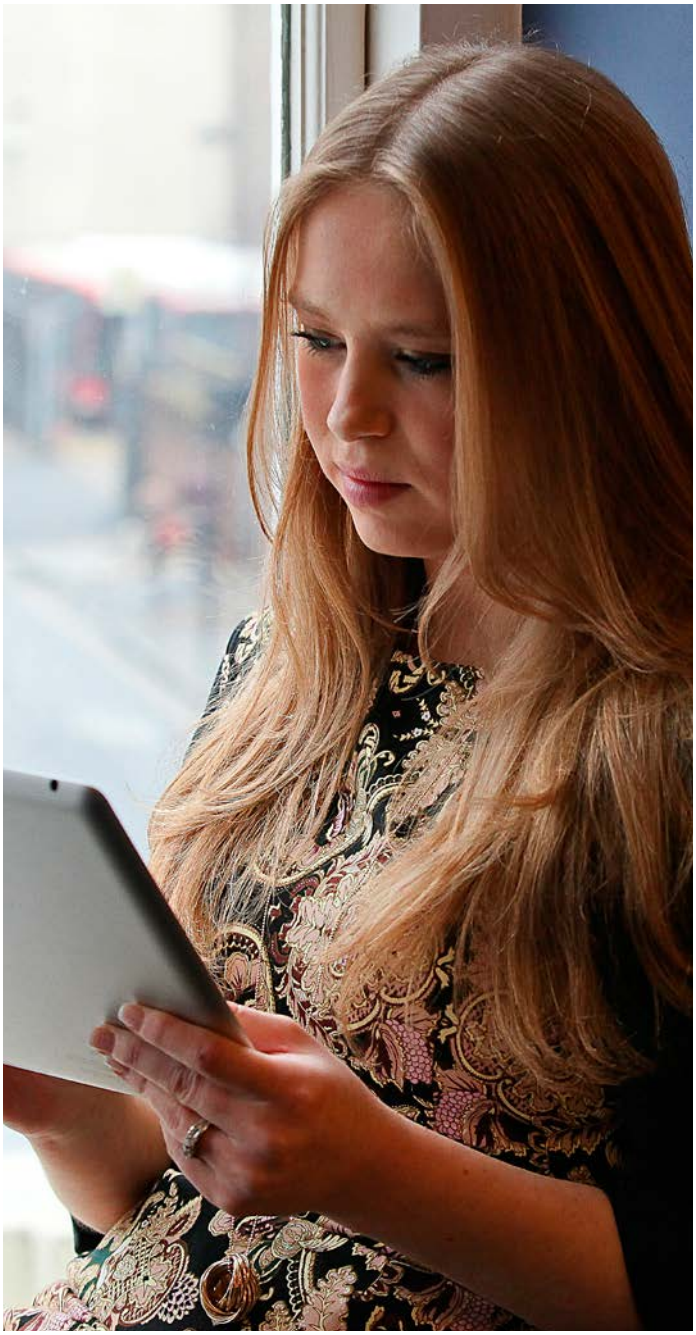
信頼とコンプライアンスのバランスを維持できるかどうかで、優秀な人材を保持できるか失うかの差が生じる。絶えず進化する今日の市場にあっては、倫理・コンプライアンスと事業リスクの整合化を図る戦略が決定的に重要である。

経営判断と組織の価値観との整合

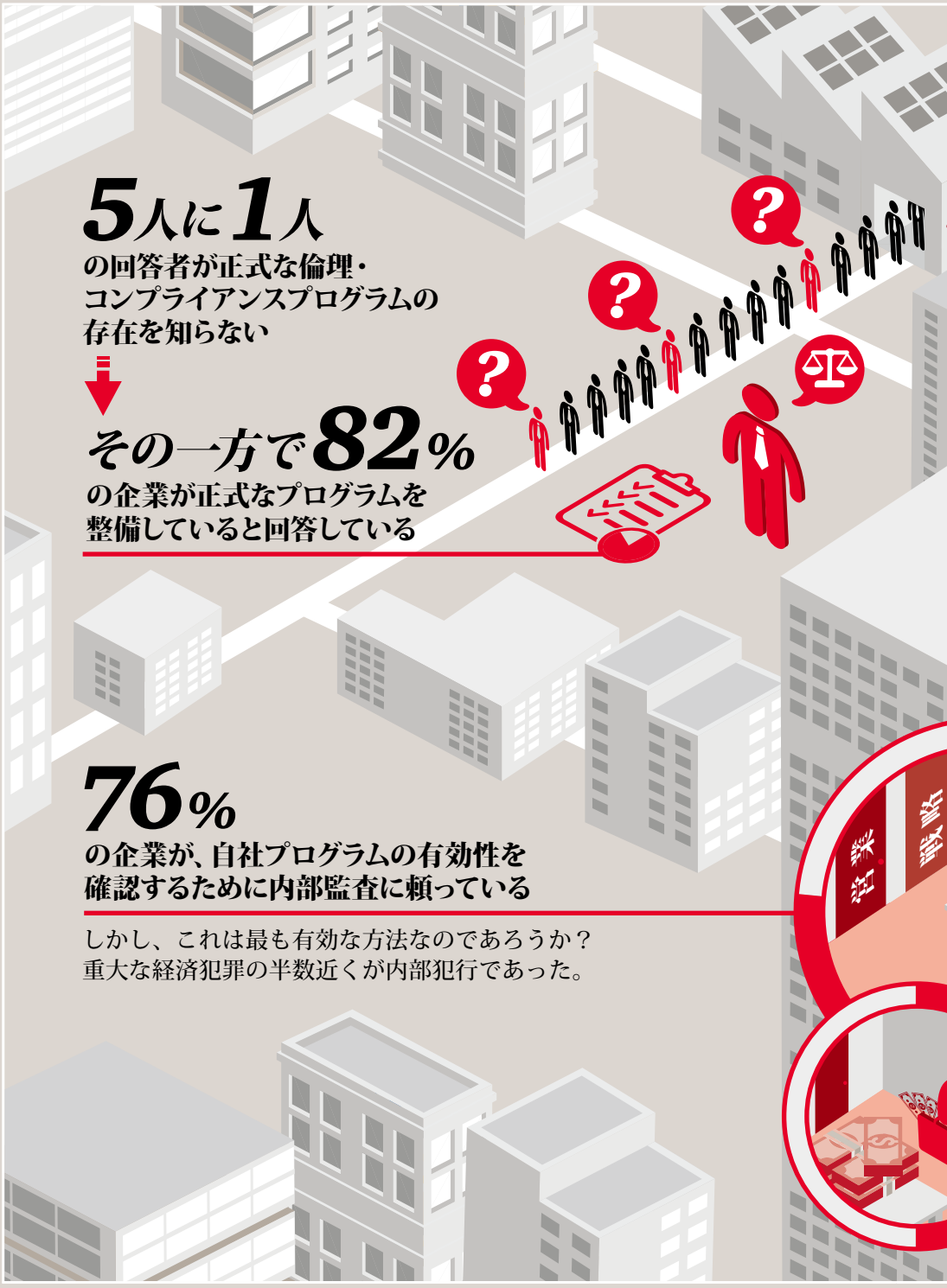
調査の結果、経済犯罪のリスクが増大している事に加えて、リスクの複雑性とテクノロジーに求められる役割が明らかになった。グローバル化が進み、説明責任と慎重な業務執行が求められているビジネス環境において、これは決して驚くべきことではない。

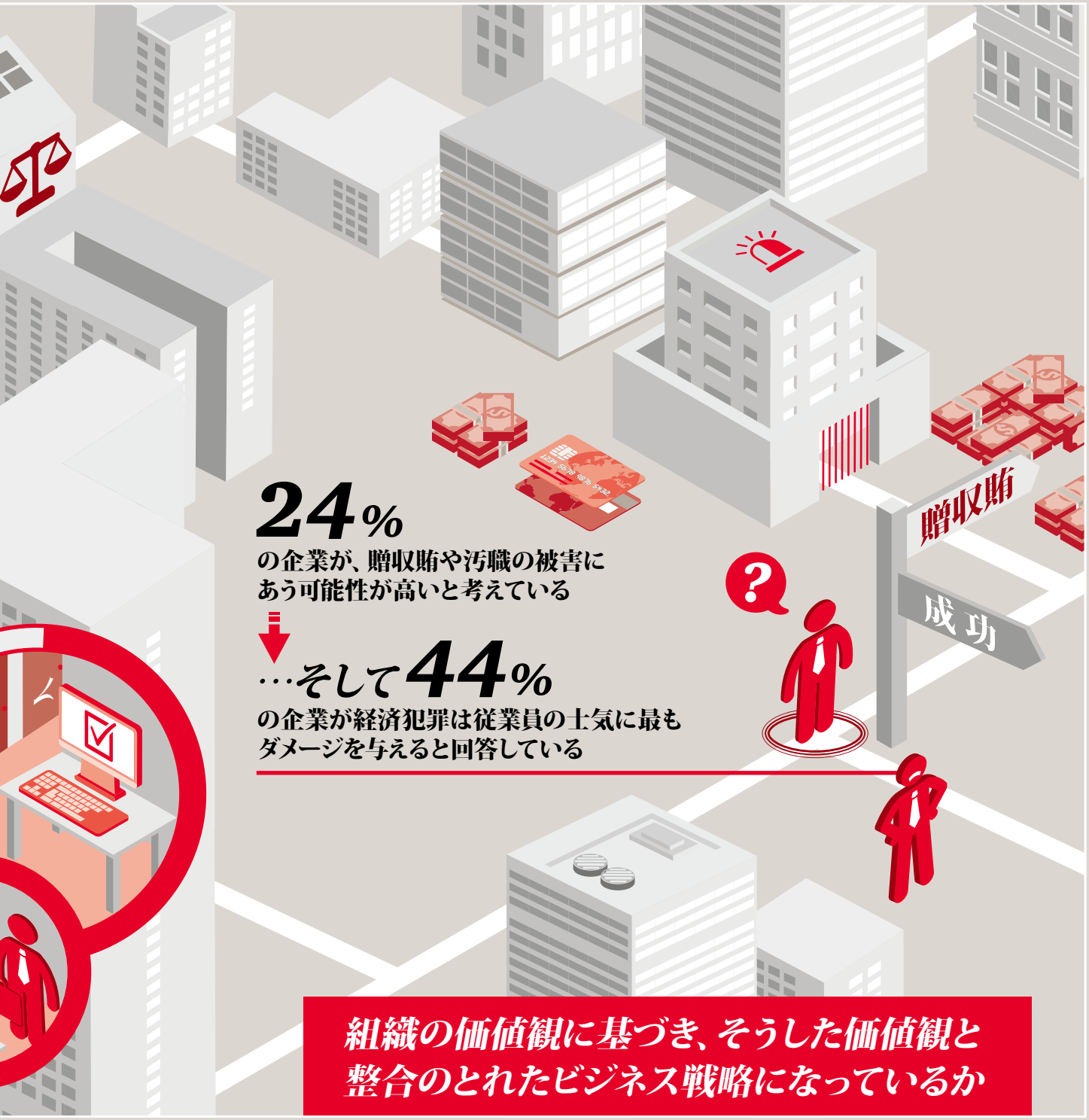
上述の理由から、コンプライアンス関連のリスクを特定し、軽減する能力を急ぎ高めていく必要がある。倫理とコンプライアンスに対するリスクベースのアプローチ（経済犯罪リスクの総合的理解と、コンプライアンスの弱点がどこにあるかについての理解を出発点とする）は必要不可欠である。こうした明確なポジションをとることで、リスクを軽減し、事業目標を達成できる体勢へと企業を導く効果的プログラムを策定することが可能になる。しかし、リスクに悩む22%の企業が、過去24カ月以内に不正リスク評価を一度も実施したことがないと答えている。

不正を報告している企業の数は、全体で36%と近年大きな変化は見られていない。しかし、データを綿密に読み解いていくと、重要な意味合いが明らかになる。ほとんどの「従来型」の不正（資産横領、会計不正、贈収賄や汚職など）は、2014年のレベルからやや減少している。その他の犯罪（とりわけ、サイバー犯罪、マネーロンダリング、インサイダー取引）は横ばいか増加のどちらかで、サイバー犯罪はわずか2年で3分の1も急増している（24%から32%）。



責任感のある人は責任感のある会社、つまり倫理的信念を貫き、言行が一致している会社に勤めたいと思っている。




24%
の企業が、贈収賄や汚職の被害にあう可能性が高いと考えている
…そして44%
の企業が経済犯罪は従業員の士気に最もダメージを与えると回答している
贈収賄
成功
組織の価値観に基づき、そうした価値観と整合のとれたビジネス戦略になっているか

前回の調査との比較から、従来型の不正の件数がわずかに減少していることは、誤った安心感を与えるかもしれない。企業が経済犯罪の被害件数の増加に気づいていない場合、倫理・コンプライアンスプログラムに投入するリソースを増やすことに価値はない、と判断してしまうリスクがある。

実際、多くの企業が人員数と研修の両面でコストを削減しているか、既存のコンプライアンスチームの担当範囲を広げて職務を増やしているが、これは誤った戦略となる可能性がある。多くの業界と地域で経済犯罪のリスクは減少しておらず、企業の短期的な経験に頼ることは危険である。リスクや脅威は常に変化するものだが、優れたコンプライアンスプログラムの本質は、進化するリスク環境を予見し、対応できることにある。

ギャップ

グローバル企業が関与し、ニュースになった事件を何か思い浮かべてみればいい―そうした企業には定評ある倫理・コンプライアンスプログラムがあったはずなのに、なぜそうした事件は起こったのだろうか。変化していく事業リスクに対して、そうしたプログラムが追いついていないことを示しているのだろうか。プログラムの内容に一貫性を欠いていたのだろうか。あるいは、このギャップにはもっと深い理由があるのだろうか。

数字は、CEOや取締役が想像している状況と、事業、特に上級・中間管理職の間で実際に発生している事柄との間にズレがあることを示している。調査によると、中間管理職は不正を行う可能性が依然として最も高い（ただし、地域でばらつきはある）。彼らは、組織内で倫理基準が明確に規定されていない、または奨励給制度が公平でないと感じる可能性が最も高い層である。

第19回PwC世界CEO意識調査では、マネジメントの意図と実際の行動の間にあるギャップというテーマの分析を行っている。企業が直面する上位の脅威のうち、CEOによる贈収賄や汚職を挙げている割合の増加が最も多く、51%から56%への上昇となった。報告されたもう一つの主要な脅威が「ビジネスで信頼を失うこと」だった。これは、マネジメントが高度で信頼できる企業倫理プログラムを用意することの重要性を浮き彫りにしている。

コンプライアンスプログラムは目的と適合しているか

それでは、経営幹部レベルは、自らの支持する内容がマネジメントによって実際に実行に移されるようにするために、どのような方法を用いているのだろうか。コンプライアンス意識の向上はどのようにして行われ、どのように測定されているのだろうか。

以下は、倫理・コンプライアンスプログラムの効果を高めるための4つの重点領域である。本セクションではこの4領域について考察する。

- **人と文化**：企業の価値観に基づくプログラムを維持し、望ましい行動を測定し、奨励を与える
- **役割と責任**：現在のリスクとの整合性を確認する
- **高リスク領域**：リスクの高い市場と部門において、同プログラムの履行を推進し、テストを実施する
- **テクノロジー**：ビッグデータの分析を含む、発見と防止ツールをより有効に用いる

コンプライアンスプログラムの効果を高めるために―プログラム実行中の5つのステップ

1. プログラムが企業戦略に則していることを確認し、全社員に伝達する
2. リスクと脅威が絶えず変化する環境に適応できるように、コンプライアンス部門の独自性を評価し、場合によっては再考する
3. コンプライアンス義務を持つ者全員が、会社全体にわたるコンプライアンスの「全体像」と、その中における自らの責任範囲を十分に理解していることを確認する
4. 方針や価値に関する教育だけでは不十分であることを忘れない：会社組織全体を通じた、信頼できる、一貫性ある関与が不可欠である
5. リスクが高まっている環境において、プログラムの規模を縮小しない

人と文化：第一次防御ライン

経済犯罪の中心には、人の行動によって引き起こされる不適切な判断がある。従って、まずとりかかるべきは人から、というのは当然である。つまり、スタッフに明確なプロセスと原則を教育するだけでなく、コンプライアンスが、価値や企業全体に適用される戦略としっかり結びついて文化を構築していくことが必要である。

回答者によると、経済犯罪がもたらす最大の損害は、株価への影響でも、規制当局との関係でもなく、最大の損害は、従業員の士気の低下に表れたという。44%の回答者が、その影響を中または大として答えている。また評判の失墜も、32%の回答者が重大な影響があるものとして挙げている。どちらの場合も、外部のみならず内部からも、会社がどう認識されているかが最大の関心領域だった。これは、成功するビジネス戦略において価値が重要な役割を果たすことを如実に物語っている。

金融業界の倫理行動の促進に関してPwCとロンドン・ビジネス・スクールが最近行った調査によると、業績管理に対する強硬なアプローチを元に、おそれの企業風土が生まれ、その結果、非倫理的な行動につながることが示されている。

この調査で、こうした「非難の文化」は不安を招き、それが正しい判断を下す能力を阻害し、前向きな結果に動機付けられた人と比べて、行動の質が低下する場合が多いことが分かった。

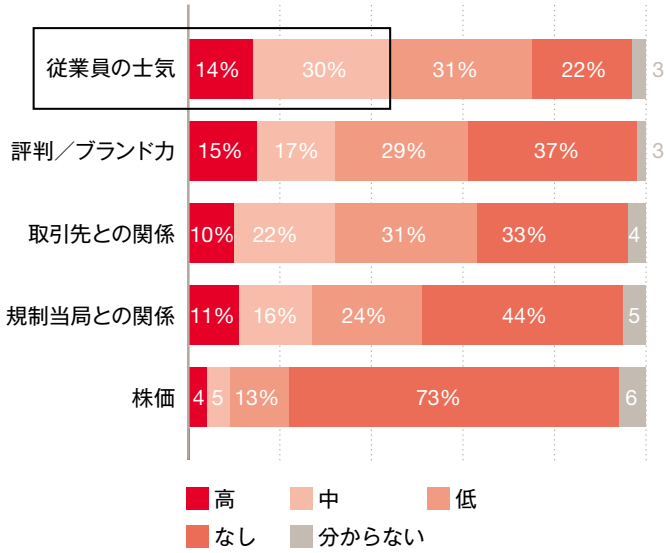
刊行：'Stand out for the right reasons' – PwC and London Business School research, June 2015.

リスクにスポットライトを

多くの組織は、リスク行動を積極的に監視し、対応するための有意義なデータを収集しようと苦労している。こうした内部の圧力に加えて、外部の圧力もある。すなわち、世間の目がいっそう厳しくなり、情報を誰もが容易に入手できるようになることで、投資家、消費者、サプライヤー、あらゆる種類の第三者が、企業が健全な事業活動に向けて注力する事をいっそう強く要求するようになっている。

最近盛んに報道された多くの事例から明らかなように、倫理とコンプライアンスに対する静的アプローチでは、組織全体に倫理行動を浸透させるのには不十分である。PwCのウェブベースのツール、Spotlightでは、行動リスクを定量化して、倫理・コンプライアンスプログラムの有効性を評価することができる。Spotlightは、インターネット調査や、面接、フォーカスグループ、文書レビューを含むその他の主観的・客観的尺度を用いて、期待する行動と実際の行動の整合性を測定する。

図表11：経済犯罪の影響



価値に基づくコンプライアンスプログラムは、最も聡明な人材を会社に引き入れるのに役立つ。責任感のある人は、責任感のある会社、すなわち倫理的信念を貫き、言行が一致している会社に勤めたいと思っている。

優れたコンプライアンスプログラム（倫理的行動の支援に重きを置くことを土台とする）は、事業に明確な戦略的利点をもたらすことができる。

しかし、コンプライアンスプログラムが効果的であるためは、最新の行動規範、ポリシー、数時間の研修以上の価値を持つものでなければならない。まず、価値－行動－意思決定間の深い結びつきを踏まえたプログラムである必要がある。

より洗練されたアプローチは、リスクが顕在化する前の予測段階でも、事後対応段階であっても個々のリスクを個別に取り扱うのではなく、特定の状況で正しい判断を下すための土台となる力をスタッフに与えることである。このアプローチが必要であることは、調査結果によって裏付けられている。不正の犯行に上級管理職が関与している事例が多かった地域（アジア太平洋、東欧、北米、西欧など）では、最大の誘因の一つが、業績に対するインセンティブまたはプレッシャーであった。つまり、コンプライアンスプログラムが浸透しておらず、この上級管理職達は最も重要なときに、間違った判断をしてしまったのである。

ギャップの認識と測定

調査回答者のほとんど（86%）が、企業としての価値基準が明文化され十分に理解されていると答えており、CEOとCFOはそれを特に力説している。しかし、調査の結果、上級管理職と取締役の理解と、中間管理職の理解に差異があることに気づいていないことも分かった。CEOの90%が、価値は明瞭で理解されていると考えていたのに対し、マネージャーレベルでは84%に留まっている。

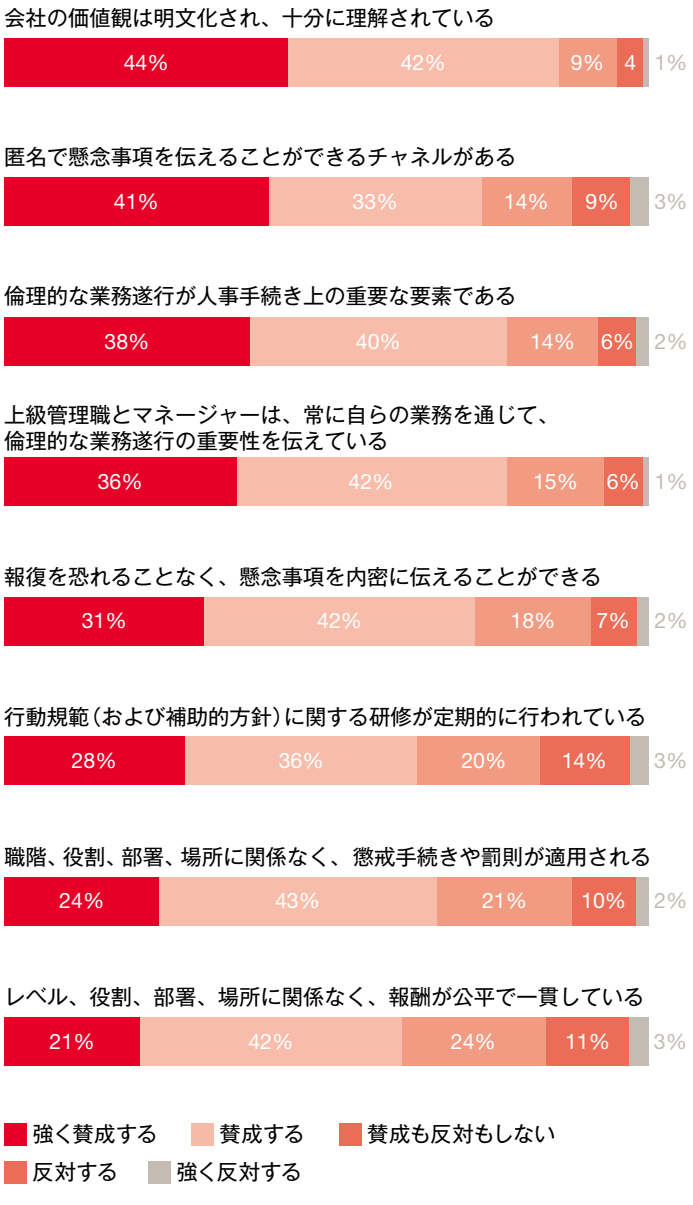
これは統計的に重要なギャップである。こうしたギャップから意識のギャップが生まれ、善意に基づく取り組みを導入したつもりでも、倫理違反行動に陥る可能性がある。

認識ギャップ

調査結果でいつもテーマとして取り上げられるのが、認識ギャップというテーマである。これは望ましくない結果につながるおそれがある。認識のギャップは次の3つの基本カテゴリーに分類することができる。

- 取締役が信じて推進していることと、組織内の人々が日々実際に見て、信じて、実行していることとのギャップ。
- 意図とそれを遂行するためのリソースとのギャップ。
- コンプライアンスを監督する際の上級管理職と中間管理職のギャップ。

図表12：企業倫理とコンプライアンスの認識



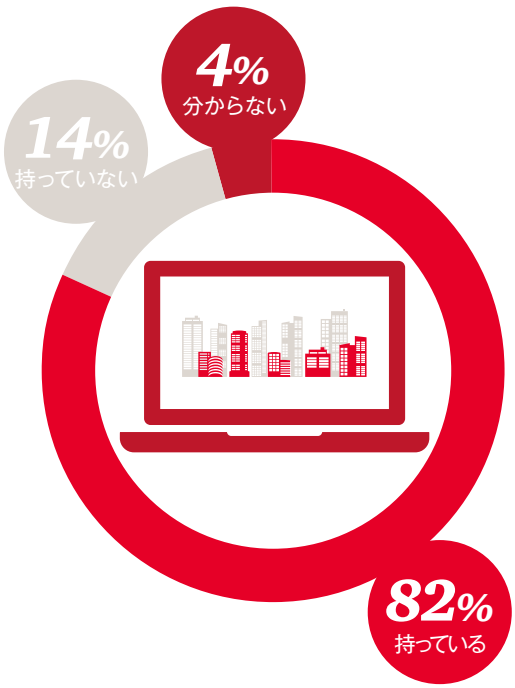
役割と責任の一致：責任者は誰なのか

調査によれば、全回答者の約5分の1（18%）が、自社に正式な倫理・コンプライアンスプログラムがあることを知らないと答えている。興味深いことに、正式な倫理・コンプライアンスプログラムの存在を知らないと答えたCEO、取締役、COOが23%存在した。

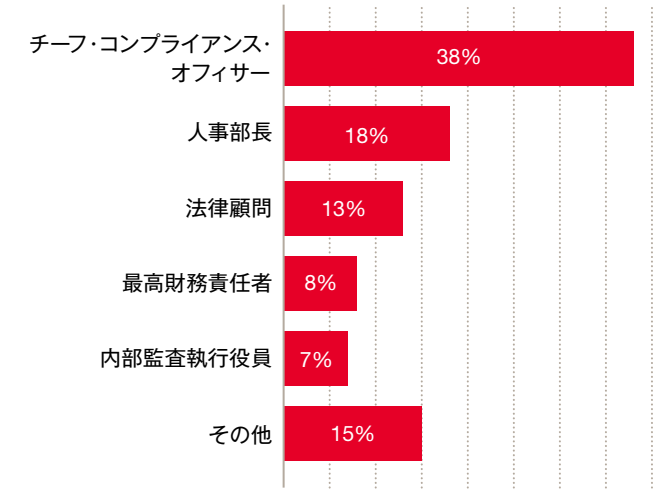
企業の82%が正式な企業倫理・コンプライアンスプログラムを定めていたが、そのプログラムに対する責任の所在は役職間で分散していた。

従業員が1,000人を下回る企業は一般に、正式な倫理・コンプライアンスプログラムを持たない場合が多い。「あれもこれも」というアプローチではなく、事業上の実際的なニーズに絞っているためかもしれないが、こうした企業は困難に直面するおそれがある。その多くが、大企業と同様のリスク環境に直面するケースがあるためである。

図表13：正式な企業倫理・コンプライアンスプログラムがある企業の比率



図表14：企業倫理・コンプライアンスプログラムの責任者



責任の所在―リスクベースアプローチの採用

会社が一つになることができるように、また、倫理・コンプライアンスプログラムと優先順位を守ることができるように、コンプライアンスの専門家だけでなく、社内の全員がその役割と責任を理解しておくことが重要である。依然として、多くの企業において、誰がどの部分の責任を持っているのか、混乱が見られる。

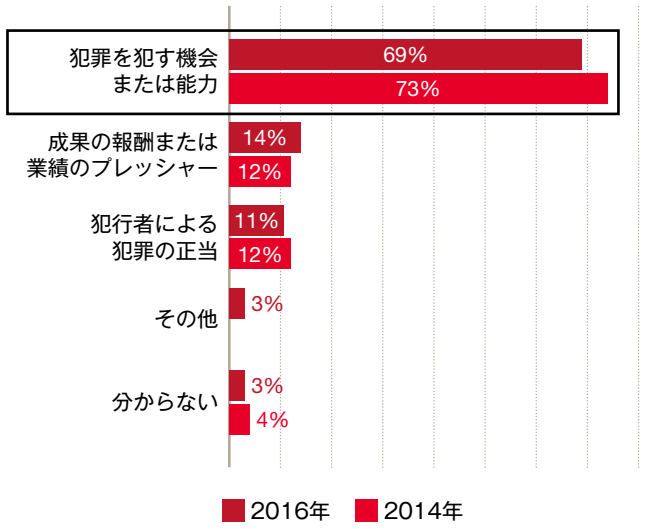
プログラムの「責任」は、第一線（事業ユニットのマネジメント）が持つべきである。その責任とは、リスクを理解し、リスクの発生原泉と誘因を特定する事である。他方、コンプライアンス部門の役割は、監督とガイダンスである。しかし、一部の企業ではコンプライアンス部門を保険として、責任を受動的に負うものとして見る傾向がある。

最終的には、企業の全員が同じコンプライアンスの目標に取り組んでいるべきである。前向きな考え方を持つ企業は、広い「コンプライアンスコミュニティー」を作っている。そこでは、倫理・コンプライアンスの役割と責任が、全員にとって日常業務の一部となっている。

犯罪の機会に誰が気づくのか

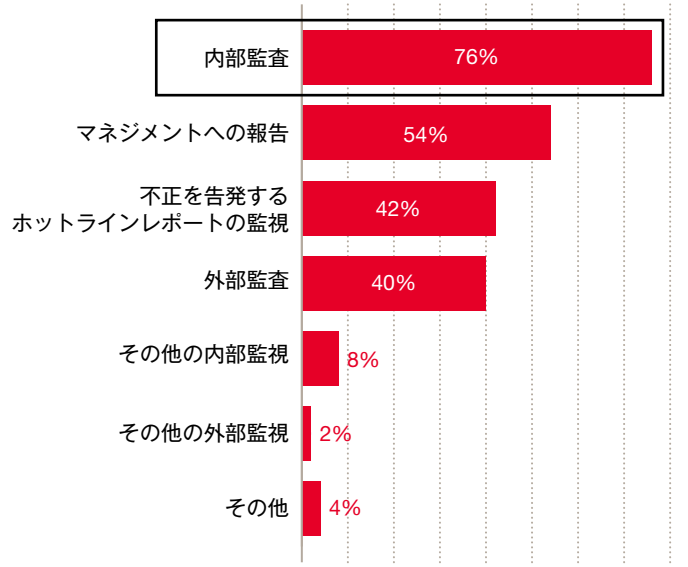
10社中7社が、社内で発生する経済犯罪の主因は犯罪を犯す「機会」であると考えている。これは、不正のトライアングル（不正の3要因）における他の2要素を遥かに上回る重要性を持つ。他の2要素とは、成果の報酬または業績のプレッシャー「動機」および犯罪の「正当化」である。

図表15：組織内犯行者による経済犯罪に寄与する要因



大多数が、こうした機会を減らす手段として統制環境を強化することに賛成している。しかし、調査結果によれば、企業の統制環境が経済犯罪を防止・発見する効果は、2年前と比べて7%低下している。また、回答者の4分の3以上（76%）が、コンプライアンスプログラムの有効性を評価するのに、内部監査機能に頼っていると答えている。

図表16：企業倫理・コンプライアンスプログラムの有効性をどのような方法で確保している



大企業は依然として、購買に関する不正と贈収賄や汚職の被害に合いやすい傾向にある

内部監査はコンプライアンスプログラムの有効性を評価する重要な枠組みではあるが、内部監査の取り組みは断続的かつ過去の環境の分析であるために、それ自体ではコンプライアンスを保証する十分な手段とはならない。さらに、不正の内容が変化しており（例えば、サイバー犯罪などの新しい犯罪が増えている）、特定の種類の犯罪の件数が一部の組織において増えたり、根強く続いていたりする場合もある。

例えば、従業員が1,000人を超える大企業は依然として購買に関する不正と贈収賄や汚職に弱い（購買は5%、贈収賄や汚職は2%全世界平均よりも高い）。これは不正行為者が既存の統制フレームワークの抜け穴を見つけ出すためである。事実、ハッカーと不正行為者は、一般的な統制フレームワークをすり抜ける方法を編み出している。

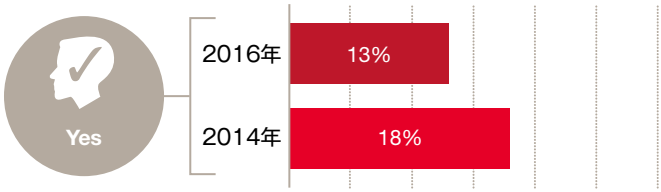
理想的には、犯罪防止策はマネジメントの意思決定と同時に行われる必要があるため、問題の発見と防止がどちらも機能するためには、社内で、内部監査メカニズムがマネジメント報告およびリアルタイムな監視と統合されている必要がある。 金融業界の回答者は特に、コンプライアンスプログラムの有効性を確保するための要として、マネジメント報告を挙げており、回答者の60%が活用している。現在、すり抜けることがさらに難しいデータ分析や予測分析など、より有効な内部監視手法を使用していると答えた回答者は、わずか8%だった。

高リスク地域における導入：危険は細部に潜む

倫理的行動をグローバル企業内に浸透させるには、研修の改善、一貫したコミュニケーション、マネジメント報告が必要である。しかし、リスクの高い地域であっても、地域リスクと部門リスクは等しくはないという見識も加えておくことが必要だろう。従って、高度なグローバル・コンプライアンス・プログラムは現場の個別の実情に合わせて微調整する必要がある。

よく見られる国境を越えた贈収賄や汚職のリスクについて考えてみたい。規制当局は、本社から遠く離れた場所で行われる非倫理的行為についても、積極的に企業の責任を問うようになっている。従って、マネジメントは全従業員が常に正しく行動していることを確認する方法を見出さなければならない。

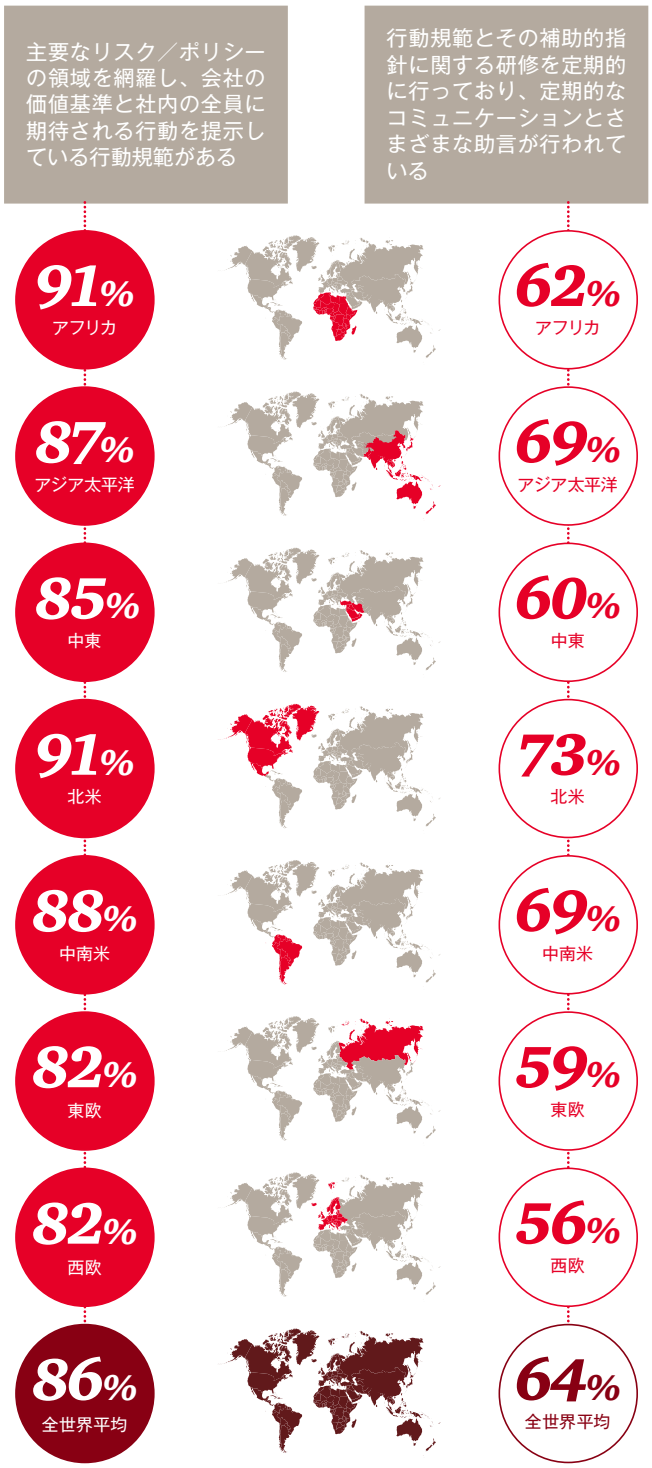
図表17：賄賂の支払いを要求されたことのある企業比率

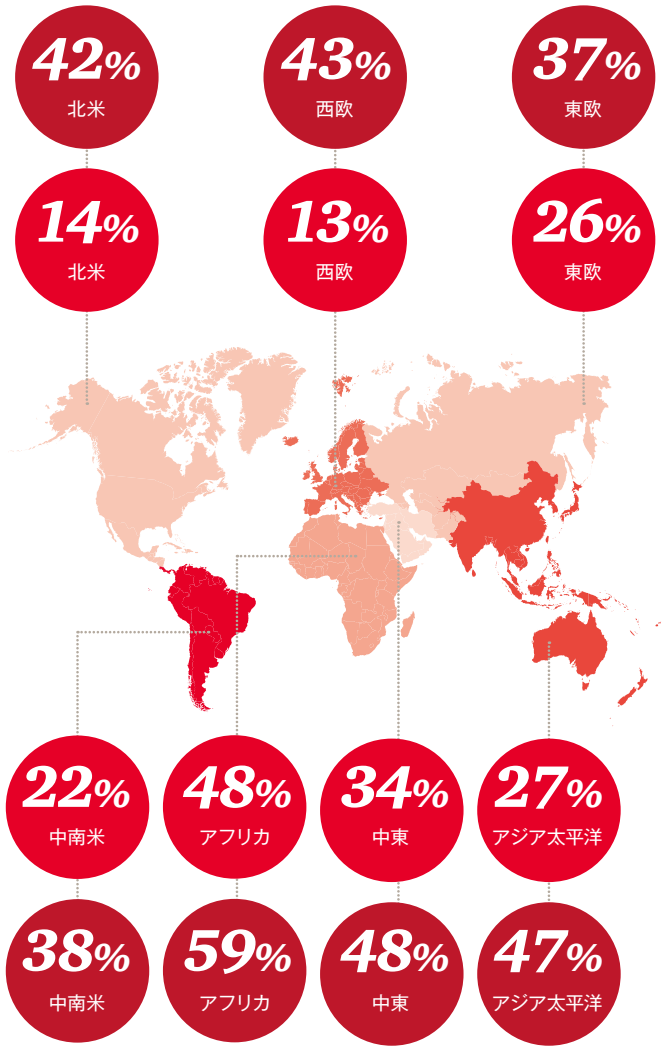


企業はこのリスクにどう対応すべきだろうか。認知された行動規範を持っていることが最初の一歩ではあるが、従業員が日々の意思決定にそれを使う方法を知らなければ、コンプライアンスリスクの軽減にはほとんど役に立たない。行動規範やその他の方針は、研修、定期的なコミュニケーション、良好な意思決定がなされた場合の報奨・表彰、悪い意思決定がなされた場合の懲戒手続きを通じて、組織に組み込む必要がある。

世界中の企業の86％が、行動規範を持っていると回答したが、研修を定期的に行っており、定期的なコミュニケーションとアドバイスによってサポートしているとの回答は64％に留まった。このギャップは、アフリカ、西欧、中東、東欧の回答者の間で特に顕著である。

図表18：研修と行動規範





回答者全体の91％が、自社のトップマネジメントは賄賂をはっきり非合法行為としていると回答している。

この回答は、地域・業界の違いを問わず一貫している。しかし、報告される犯罪の件数は依然として多く、多数の地域では、今後24カ月の間に贈収賄や汚職の被害を受けるだろうと予想する企業がこれまでになく増えている。

テクノロジー：万能薬ではないが、強力な薬

今日では、非常に効果的な監視が可能なビッグデータ分析をはじめ、さまざまな構造化データと非構造化データを処理することでコンプライアンスと実際の業務のギャップを縮められる高度なツールがいくつもある。

取引モニタリングシステム（主に金融業界の顧客が利用する）は別として、経済犯罪の防止と発見にこの種の技術を用いている企業は非常に少ない。現在、データ分析など、その他の内部監視手法を使用していると答えた回答者は、わずか8%である。

ただし、テクノロジーに関して失策に陥る可能性もあるので注意が必要である。リスク評価プロセスにムラがあるために、監視の多すぎる場所（効果は限定される）があればゼロの場所もあるという具合に偏りができる場合がある。気づかぬまま、複数のツールに出費を重ねてしまう企業もある。さらには、コンプライアンスが慣例化された作業になってしまい、正しいデータの収集や使用を必ずしも常に行っていない企業もある。データ分析作業の価値を検証する前に廃止を促してしまう場合も少なくない。

これまで、最初に手を付けるのに最適なのは、取引モニタリングの「ビッグデータ」ではなく、むしろリスク評価の「スモールデータ」にあることを示す事例を見てきた。最も重要なのは、一貫した比較可能なデータを収集することである。これは簡単なように聞こえるが、実際にはそうではない。

最適なモデルは企業が直面するあらゆるリスクに適用でき、事業単位別、地理別ごとの報告が可能である。これを達成するには、次の3つが必要とされる。

- リスク定義の一貫した手法
- リスク計測の透明性
- 共通のデータプラットフォーム

こうした条件は、集中型ガバナンスやオペレーティングモデルと組み合わせることで、現在の取引モニタリングの有効性を評価するための糸口となり得る。また、会社にとっての本当の脅威に集中的に取り組むための助けとなる。最終的に重視するのは、テクノロジー自体ではなく、テクノロジーによって何が可能になるか、ということである。データがそれだけで万能薬となることはあり得ない。しかし、データを効果的に使えば、コンプライアンスリスクに負けない能力が確実に備わる。

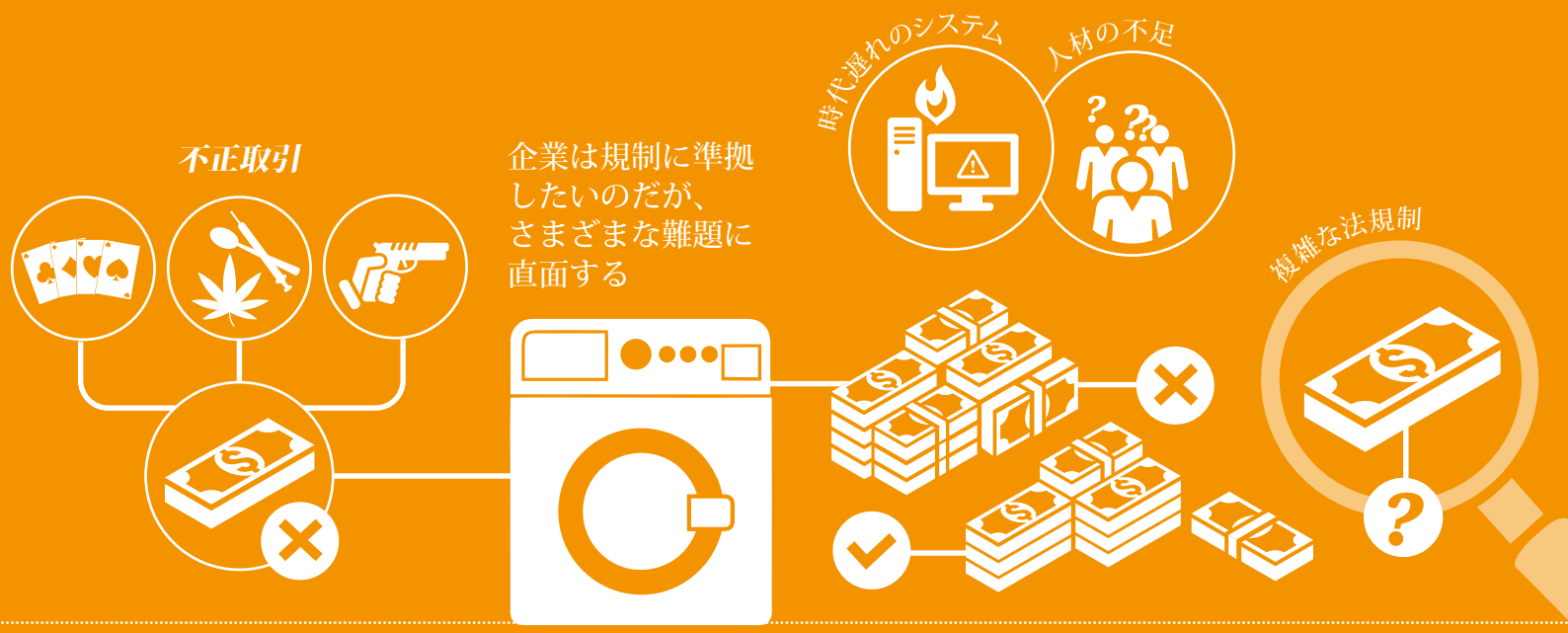
主なお問い合わせ先

Mark Anderson
パートナー
PwC英国
電話：+44(0) 20 7804 2564
電子メール：mark.r.anderson@uk.pwc.com

Manny Alas
パートナー
PwC英国
電話：+1 (646) 471 3242
電子メール：manny.a.alas@us.pwc.com

Martin Whitehead
パートナー
PwCブラジル
電話：+55 11 3674 2141
電子メール：martin.j.whitehead@br.pwc.com

マネーロンダリング対策



企業価値を破壊するマネーロンダリング

マネーロンダリングは企業価値を破壊する。犯罪に必要な資金を保有したり移動したりすることで、経済犯罪や、汚職、テロ、脱税、麻薬、人身売買などの違法な活動を助長する。組織の評判とビジネスに悪影響をもたらす可能性がある。

世界中のマネーロンダリング取引は毎年、世界全体のGDPの2%～5%、または約1兆米ドル～2兆米ドルに上ると推定されている。しかし、国連薬物犯罪事務所（UNODC）によると、世界中の不正な資金の流れのうち、当局が現在把握しているのは1%未満だという[2]。

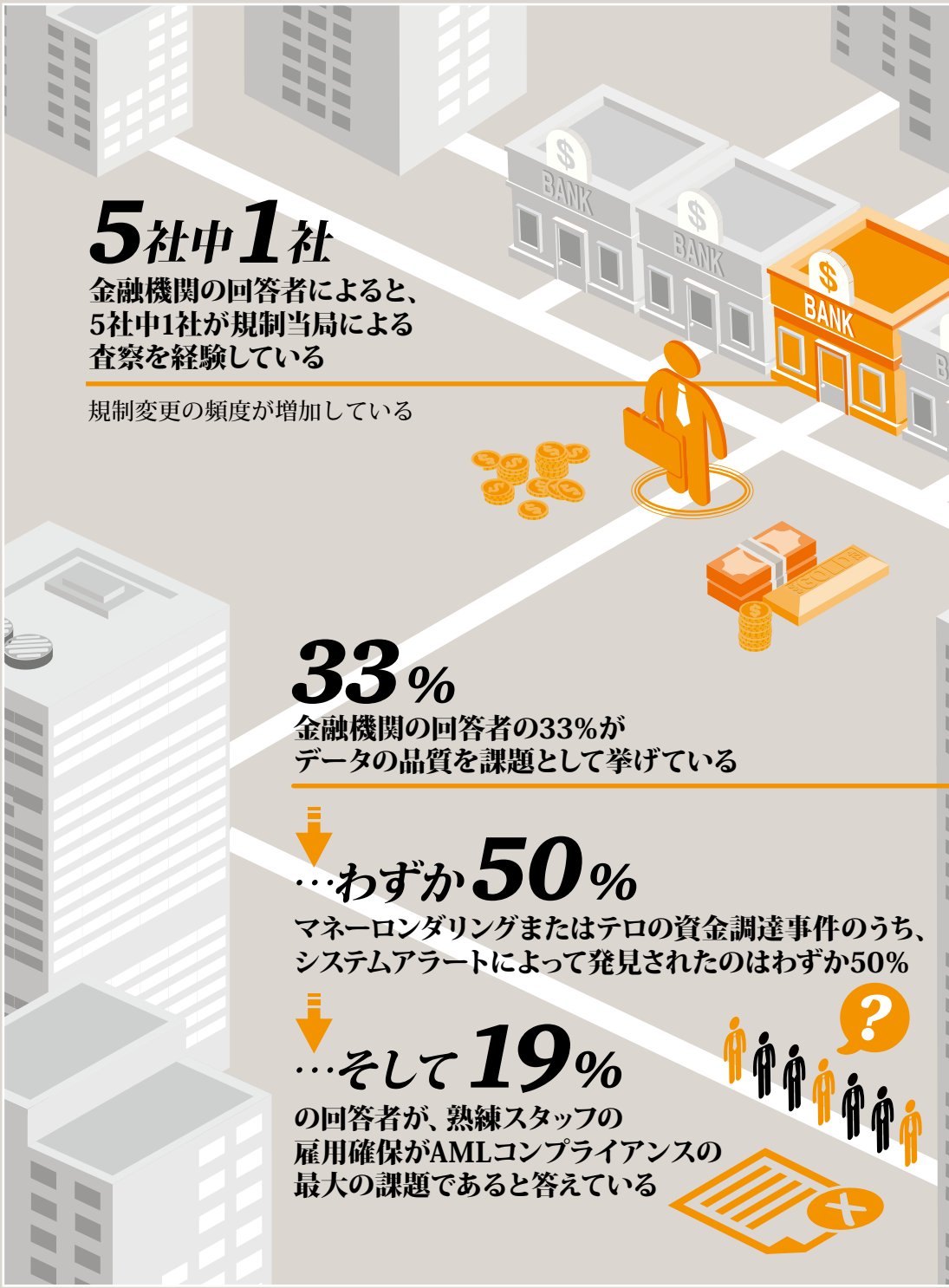
テロ活動が目立つ昨今、マネーロンダリングとテロリストの資金調達は、世界中の政府が優先課題として取り上げている問題である。過去数年にわたり、米国だけでも多数の大手グローバル金融機関が、マネーロンダリングや承認違反で数億米ドルから数十億米ドルの罰金を科せられた。その他の国もこれに倣って規制と執行を強化する方向に進むであろうことを示す確かな兆候も見られる。

しかし、これは金融機関に限った話ではない。金融取引をサポートする組織（デジタル／モバイルの決済サービス、生保会社、小売業者、その他諸々のノンバンクマネーサービス業を含む）も、マネーロンダリング防止（AML）法の視野に入りつつある。不安なことに（しかし、驚くべきことではないが）、こうした新たな参入者の多くは、満たすべき規制事項、または必要とされるコンプライアンスプログラムについて十分な知識を有していない。

規制が益々複雑化し、範囲が広がるとともに、コンプライアンスのコストも上昇する。WealthInsightの新しい統計によると、AMLコンプライアンスに対する全世界の支出は、2017年までに80億米ドルを超えることになる[3]（9%近くの年平均成長率になる）。しかし、規制に違反した場合には、査察時のコストや課徴金が莫大なものになるのにもかかわらず、多くの企業は増加するコンプライアス対策への支出に二の足を踏んでいる。

2）‘Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes’（国連薬物犯罪事務所）より。
3）統計はWealthInsightの承諾を得て転載

規制の厳格化に伴い査察が急増している



5社中1社

金融機関の回答者によると、5社中1社が規制当局による査察を経験している

規制変更の頻度が増加している

33%

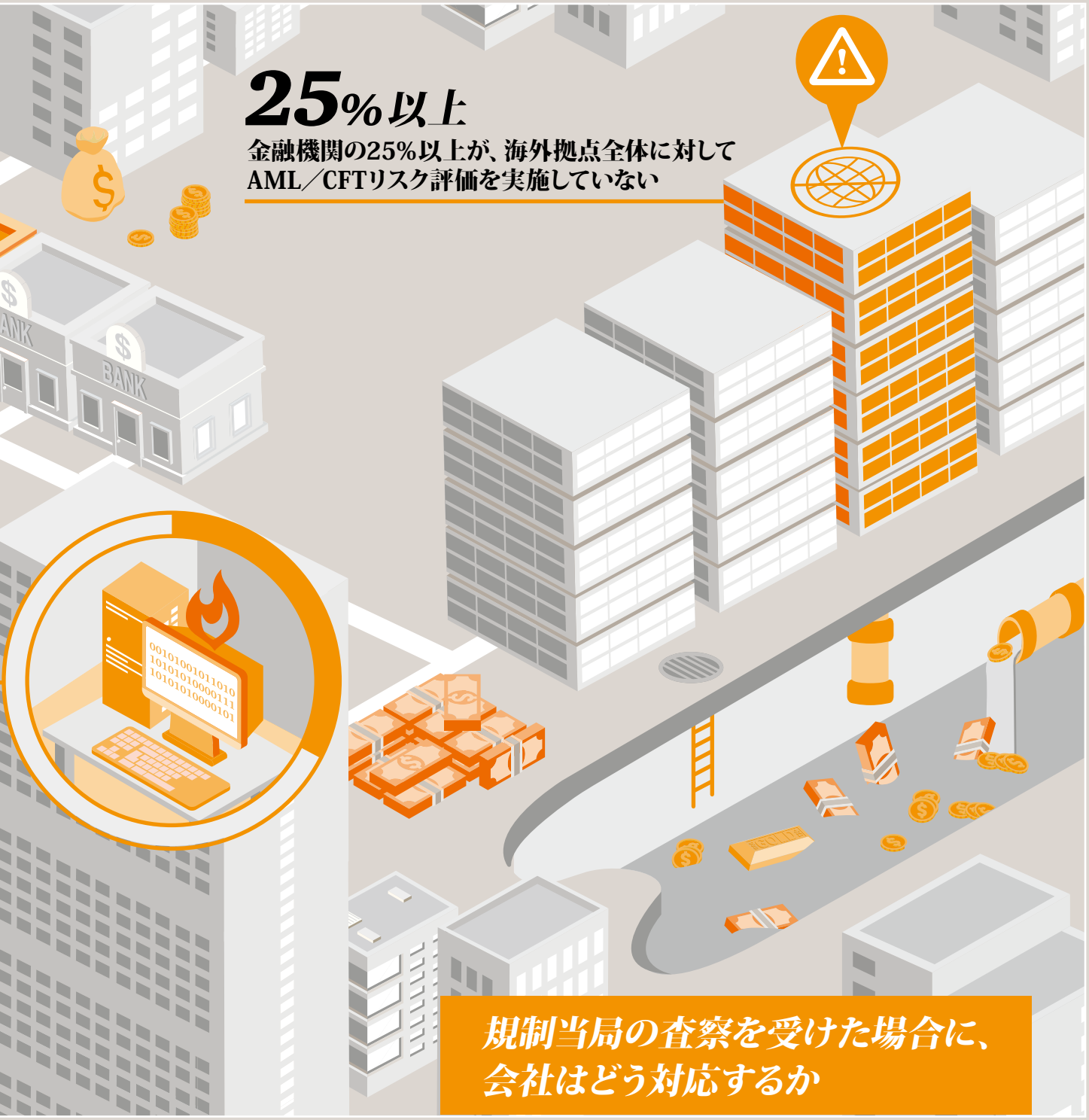
金融機関の回答者の33%がデータの品質を課題として挙げている

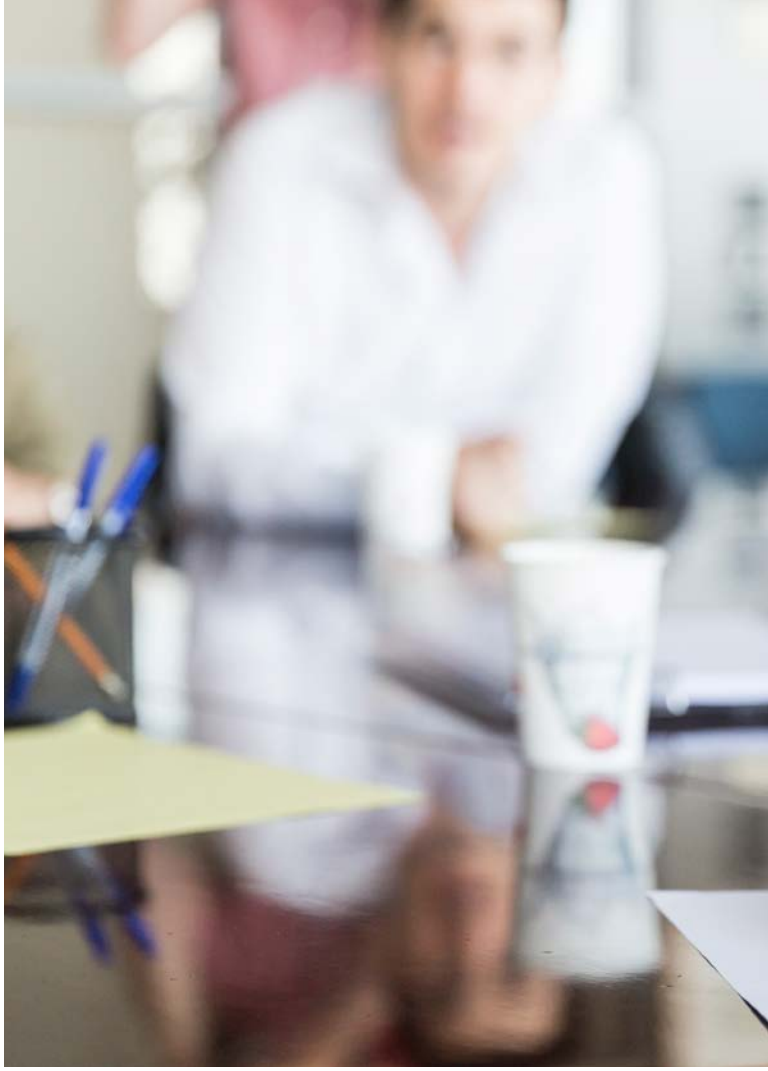
…わずか50%

マネーロンダリングまたはテロの資金調達事件のうち、システムアラートによって発見されたのはわずか50%

…そして19%

の回答者が、熟練スタッフの雇用確保がAMLコンプライアンスの最大の課題であると答えている

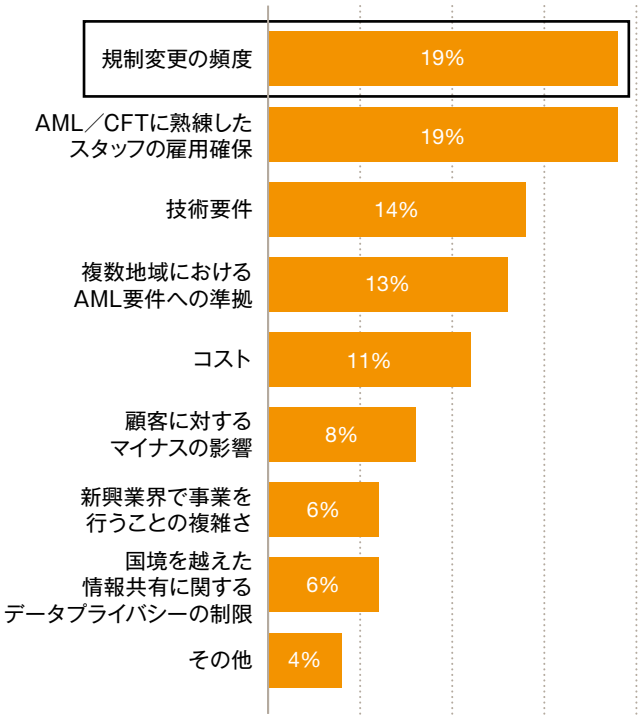

25%以上
金融機関の25%以上が、海外拠点全体に対して
AML／CFTリスク評価を実施していない
BANK
BANK
規制当局の査察を受けた場合に、
会社はどう対応するか



検査に基づく規制

規制基準が厳しくなったことで、摘発が急増している。調査の結果、マネーロンダリング対策（AML）とテロ資金供与対策（CFT）の執行レベルが引き上げられたことで、対応に十分に取り組んできた金融機関ですら困難を覚える状況になっていることが分かった。

図表19：AML／CFT要件へのコンプライアンスに対する最大の課題

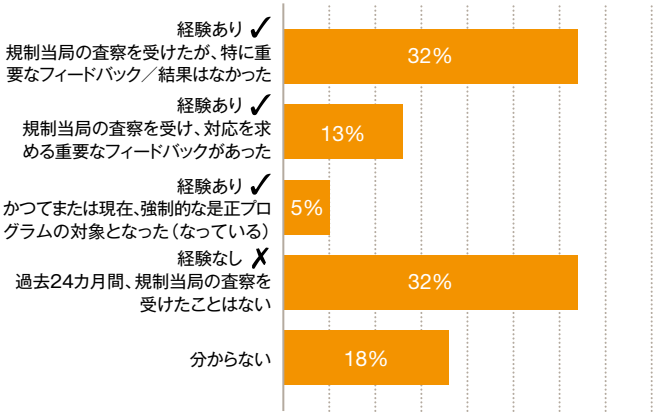


一部の政府は、グローバルな取引を監視するための十分な措置を導入していない金融機関に罰金を（場合によっては刑事訴訟も）科した。金融機関の中には、ある国での不正な商習慣を理由に、別の国の規制当局による処分対象となったケースもある。金融機関が別の国で制裁を受けると、どこで合法的に営業できるのかについて混乱が生じることが多い。

AMLの監視人と規制当局

- **マネーロンダリングに取り組む金融活動作業部会（FATF）**は、マネーロンダリングとテロの資金調達を取り締まる政策を推進することをミッションに掲げる、政府間の政策立案・基準設定組織であり、グローバルなAMLとテロ資金供与対策（CFT）の傾向をモニタリングし、国際標準を設定している。FATFが提出した「40の提言」は、34の加盟国がマネーロンダリング対策の規制と法律の一部として現在採用している、効果的なマネーロンダリング対策システムに向けたグローバルな最低限遵守すべき基準である。
- **国連安全保障理事会**は、既知のテロ組織など、制裁の対象とされた人物とグループのリストを記載した決議を発表している。リストは多くの場合、加盟国政府のテロ対策に活用されている。
- 米国財務省管轄の**外国資産管理室（OFAC）**は、米国の経済制裁プログラムと通商停止措置を管理している。

図表20：規制当局による査察の経験



査察と是正の件数が増えている。近年、多くの金融機関が買収によって巨大化しているが、グループの業務プロセスやさまざまな基準の統合は困難な場合が多い。また、規制当局の制裁とその是正措置への対応に苦慮している組織も多い。これらの要因はAMLに関する査察の増加要因として作用している。今回の調査によると、銀行の18％が、最近、規制当局による指摘や是正指導を受けている。（これは非常に高い数値である）。

不公平な実施？

ほとんどの国がAML検査のメカニズムを持っているが、検査の度合いには大きなばらつきがある。

米国をはじめとする先進国の幾つかには、AMLと制裁の専任検査スタッフがいる。だが、その他の多くの国ではAMLの専門家ではなくコンプライアンスまたはリスク管理部門が対応し、検査の実施頻度も低い。

グローバルなAML／CFTコンプライアンスに取り組む企業にとって、もう一つの難題は、規制当局の期待が明確な法的要求に取って代わりつつあることである。これは、顧客のデューデリジェンスと取引モニタリングの領域で最も顕著である―これらの領域では、査察官がある金融機関に別の金融機関の慣行に基づいて基準を適用する場合がある。このいわゆる「査察に基づく規制」は、よく知られた（企業とその関係者が適用することを期待される）リスクベースアプローチのコンセプトと異なるものである。

FATF：評価の焦点が有効性に

FATFは全世界のAML／CFT基準の評価尺度を、「テクニカルなコンプライアンス」から「有効性」へと切り替えた。後者の基準では、全ての組織が同様の尺度で測定される。

有効性が新たな焦点になったことで、一部の発展途上国はAML／CFTの基準に合わせて実務慣行を変更せざるを得なくなり、その変更は金融機関に浸透してゆく。AMLの新構想がグローバルな性質を持つことを考えると、これは他の国や地域にも広がっていくと考えられる。また、「有効性」の意味の捉え方に、成熟市場と発展途上市場の間で一時的なズレが生じる可能性もある。

グローバルコンプライアンスとは、一つの地域の法律に従えばそれで済むというものではない。母国の法域に関係なく、組織はAML／CFTの事柄をグローバルな規制対象と見なすべきである。それには次の3つの理由がある。

- FATFはAML／CFTのリスク管理と実施の国際標準を設定している。よって、それが米国外の国内規制のベースとなり、銀行その他、規制を受ける機関の義務となる。
- OFACは、英財務省などの財務監督官庁とともに、海外および国境を越えた商品、サービス、およびファンドの移動を網羅する経済制裁プログラムを管理している。
- 金融機関が、米ドル、英ポンド、ユーロなどの主要グローバル通貨を管理する国や地域の法律を避けて通ることは、ほぼ不可能である。米国で、または米ドルを使用して単一の取引を清算する行為や、米国内の人物に電話や電子メールで連絡を取るだけの行為でも、つながりが生じ、米国での訴追理由となるのに十分である。

例えば、香港、シンガポール、ロンドン、ニューヨークなど、主要な金融の中心地の規制枠組みは集中化が進んでおり、金融機関は国内外問わず、最高レベルの基準を組み込むことが求められている。

金融機関が今後直面する将来の規制環境を予想しようとする中で、このように急速に変化する予測不能な展開が続くと、企業にとって戦略の硬直化（strategic inertia）につながる可能性がある。ここに一つ非常に明確なことがある―金融犯罪コンプライアンスプログラムの策定においては、相当な判断力が必要とされるということだ。

あなたの企業にとってこれは何を意味するか。

AML／CFT基準のグローバル化により、高度に整備された国際的なコンプライアンス基準によってあなたの会社も裁かれる可能性があることを覚えておくことが重要である。考慮すべきアクションポイントは次の3つである。

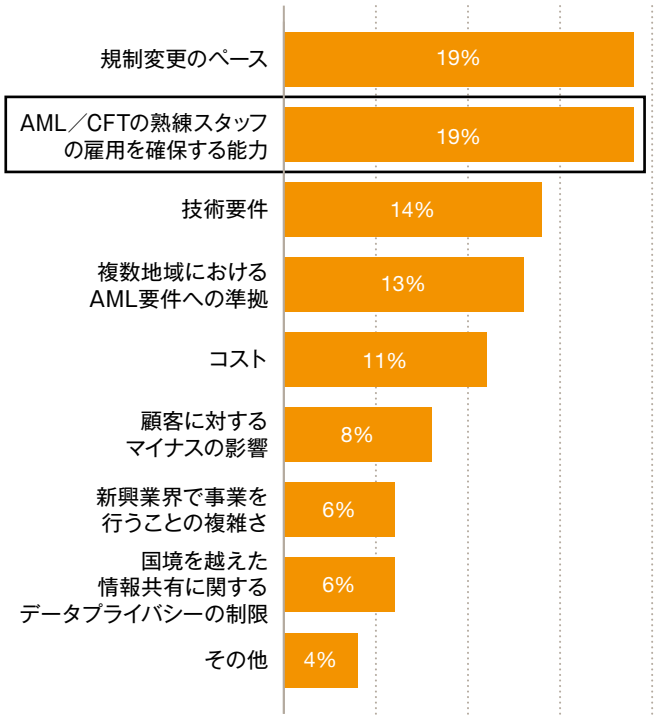
- **規制の実情を正確に把握しておく**。現在の法律に機械的に従うのではなく、その先に注意を払う。今後の法律制定の傾向に従えるように、適切な体制づくりを検討する。この領域の未決定の規制を積極的に追跡調査する部門を組織内に設置する。
- **後手に回らず、先頭に立つ**。「普通」にしていては、規制の後手に回ってしまうリスクが生じる。規制の変化を完全に掌握することができるように、戦略的に迅速かつ革新的でいる。
- **他社の過ちから学ぶ**。規制当局が特定した重要な問題の根本原因を積極的に調査している企業は非常に少ない。是正は、規制当局の調査結果に対応するための手っ取り早い解決策として役に立つことも多いが、違反の是正コストが、規制当局が課す課徴金を上回るケースもよくある。ほとんどの取引には多国籍間の財務的な取引の要素が含まれているため、他に事情がなければ、可能な限り常に最も厳しいグローバルスタンダードに準拠し、より厳格なAML／CFT自己評価を実行することが「優れた実践（good practice）」と言える。地理的な違いを越えて一貫性を確保するために、「企業全体」としての要件を確立するべきである。

自社の人材、自社のプロセス

調査によると、AML対応で直面する最大の課題は、熟練スタッフの雇用である。これは、規制変更の頻度に対する懸念と並んで19%だった。

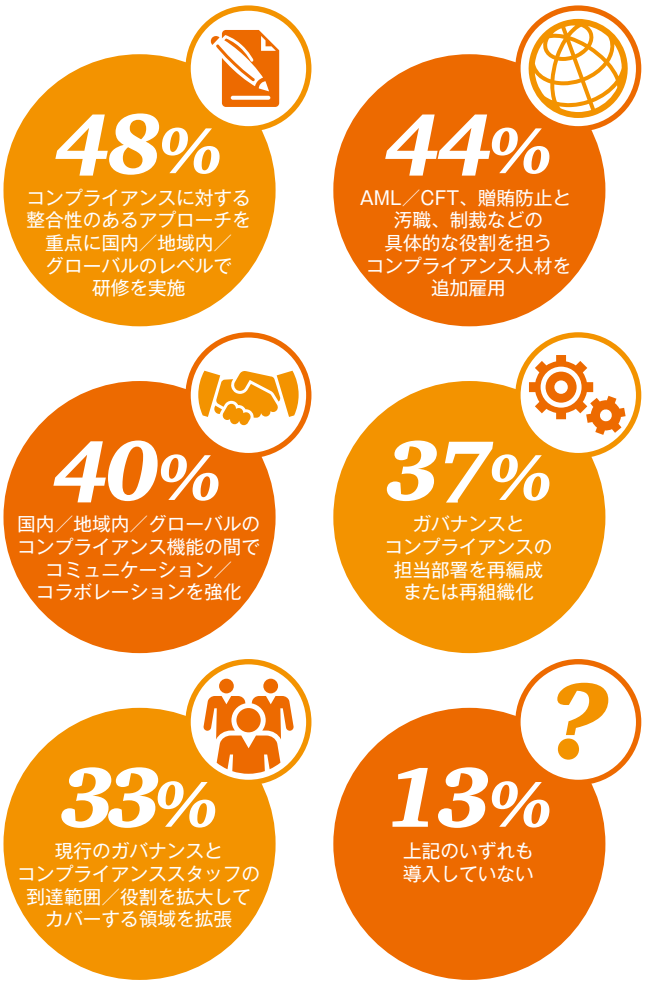
残念ながら、優秀な人材の供給は常に需要を下回っている。AMLとコンプライアンス担当者の人材回転率は高く、金融機関と非金融機関のどちらにおいても、トップクラスの人材を巡る競争は厳しい。

図表21：AML／CFT要件へのコンプライアンスに対する最大の課題



一部の組織は、AML／CFTと贈賄防止の両方のリソースに的を絞り、社内人材への研修を強化することで、人材確保の課題に対応している。

図表22：規制当局に対応するために導入されている人材対策



リスク評価が極めて重要である。過去10年にわたり、正式な金融システムにおけるマネーロンダリング対策が改善されたため、不正行為者は犯罪で上げた利益を「移転」する新たな方法を探さざるを得なくなった。

定期的なリスク評価が決定的に重要なのは、そのためである。そうすることで、企業は、どこで誰と取引する場合も、マネーロンダリングとテロの資金調達リスクを特定し、対応することができる。

明らかにメリットがあるのにもかかわらず、この調査に参加した金融機関の4分の1以上が、海外拠点全体に対してAML／CFTリスク評価を現在行っていないか、行っているかどうかを把握していない。

マネーロンダリングの高度化が進む中、これは先延ばしにはできない対策である。例えば、貿易ベース・マネー・ロンダリング（TBML）は、偽造文書を用いる複雑なシステムで、不正行為者は合法的な貿易を装い、世界中で資金を稼ぎ、移動することができる。これは、従来の取引モニタリングシステムでは発見が難しくなってきている。

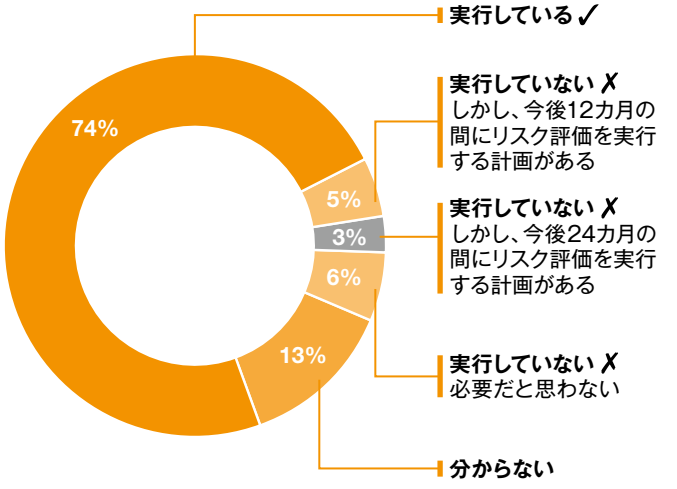
リスク評価は定期的に実施する必要がある。また、業務を行う国の業務環境、グローバルスタンダード、規制など、状況の変化に合わせて調整すべきである。とりわけ、評価には顧客のプロファイリングを行って、異なるマネーロンダリングやテロの資金調達リスクといったカテゴリーに分類する作業も含める必要がある。これは、脅威を防ぐためにFATFと規制当局が推奨するグローバルスタンダードでもある。

適材適所。どんなスキルを必要としているか

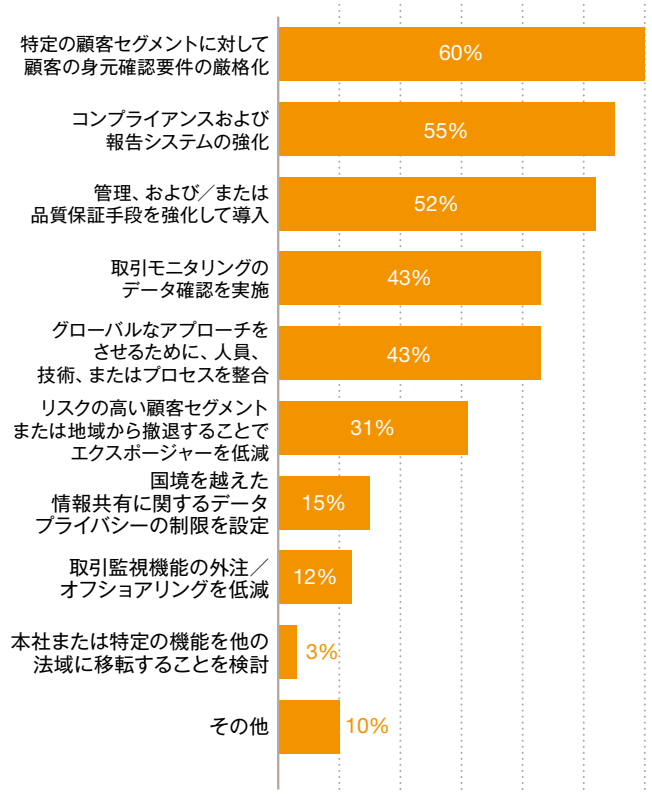
最良のAML防衛線に適切なスキルを持つ人員を適材適所に配置するためには「適材」に求められる素養を知っておく必要がある。高度な専門知識とスキルに対する需要は非常に高い。

- グローバルスタンダードと要求事項の理解
- 法域の規制と義務に関する知識
- グローバルな規制環境の理解
- 顧客のデューデリジェンス
- 取引モニタリングの技術的専門知識
- データ分析

図表23：AML／CFTリスク評価を実行している割合



図表24：AML／CFTリスクを低減する手段



現在、そして将来にも目を向けた顧客管理。顧客ベースの透明性とは、単に提供される情報を特定し、検証することに留まらない。静的ではなく、動的な行為でなければならない。危険信号と疑わしい活動の定期的な監視を続けることが不可欠であり、顧客の取引先との取引には特に注意を払うべきである—AML規制が弱いか不十分な国の居住者と取引を行う場合には、特に重要である。

テクノロジー

あらゆる産業に属する企業が苦境に陥っているように思われる。ほとんど企業（特に金融機関）が、進化するグローバルな規制環境の中で変化するビジネスに合わせてAMLプログラムを「ライトサイジング（適正規模化）」する難題に直面している。にもかかわらず、多くの企業が、負担が大きい上に調整／確認／維持コストが高すぎると判明しつつある従来のモニタリングシステムに、不自由さを感じている。

残念ながら、高度な新しいデータ分析プラットフォーム（取り扱いが難しい取引ベースから、より戦略的・効率的なアプローチへの移行に役立つ可能性がある最先端のアルゴリズム）の一部は、導入コストが高く複雑であるため、多くの企業では導入が困難であると思われる。金融機関の回答者はこうしたシステム上の難題を十分に認識していると見られ、3人に1人がデータの品質を最も重大な技術的課題として挙げている。

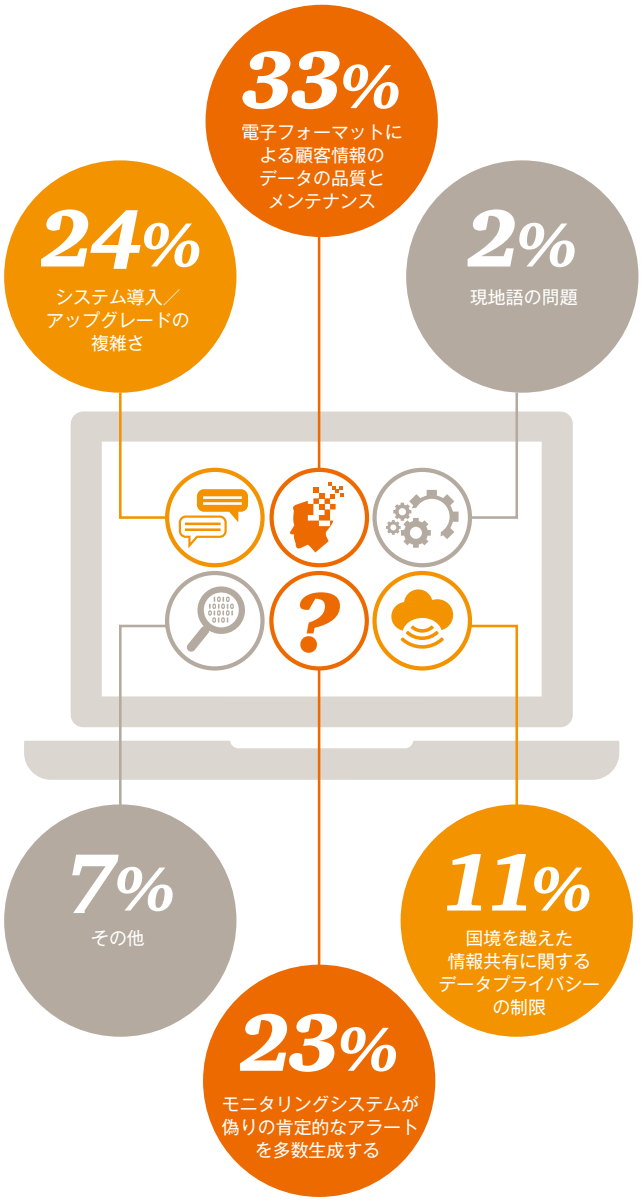
企業が新技術へ移行するきっかけはなにか？

新技術への移行は、規制当局の制裁による是正、または合併、買収、その他の取引で、旧システムが目的に適さなくなったことが明らかになり、それがきっかけになる場合が多い。または、新たな破壊的な競争相手が参入し、どの業者も対応の変更を余儀なくされた場合である。

しかし、組織が転換点に達するかどうかだけの問題である場合もある。転換点とは、新技術のプラットフォームに移行することで予想される投資収益が、投資とメンテナンスに莫大な費用を要したシステムを廃棄するコストを上回るとの認識に至るポイントである。

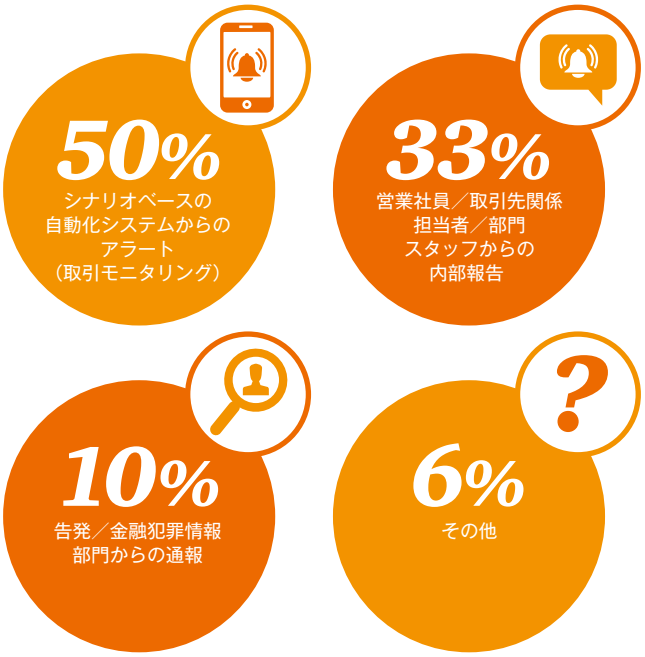
また、新技術で別の利益が得られる場合もある。AMLコンプライアンス以外にも、贈賄防止、輸出制裁、不正監視と対応、財務管理および調査など、他の重要なコンプライアンス機能を高めることができる。また、これらにより、総合的なガバナンスが強化される可能性もある。

図表25：AML／CFTシステム：直面している最重要課題



問題をさらに複雑にしている要素がある：AMLアラートモニタリングのパフォーマンスがあまり良くない、という点である。調査によると、特定された不審なマネーロンダリングやテロ資金供与のうち、取引モニタリングシステムがフラグを立てたのは半分でしかない。現在のAML類型論では、リスクの高い取引を特定するのに必要な、微妙な違いや複雑な構造を読み取れていない可能性がある。

図表26：不審な活動の特定に用いられた手法



新たな分析モデルとプラットフォームへの転換は、これまでのところ、それほど進んでいない。これは、企業が従来の検出システムの非-有効性について、ある程度織り込み済みである（そして、おそらく不利益につながっている）ことを示すものといえる。

主なお問い合わせ先

Didier Lavion
プリンシパル
PwC米国
電話：+1 (646) 471 8440
電子メール：didier.lavion@us.pwc.com

Andrew Clark
パートナー
PwC英国
電話：+44 (0) 20 7804 5761
電子メール：andrew.p.clark@uk.pwc.com

Malcolm Shackell
パートナー
PwCオーストラリア
電話：+61 (2) 8266 2993
電子メール：malcolm.shackell@au.pwc.com

参加者データ

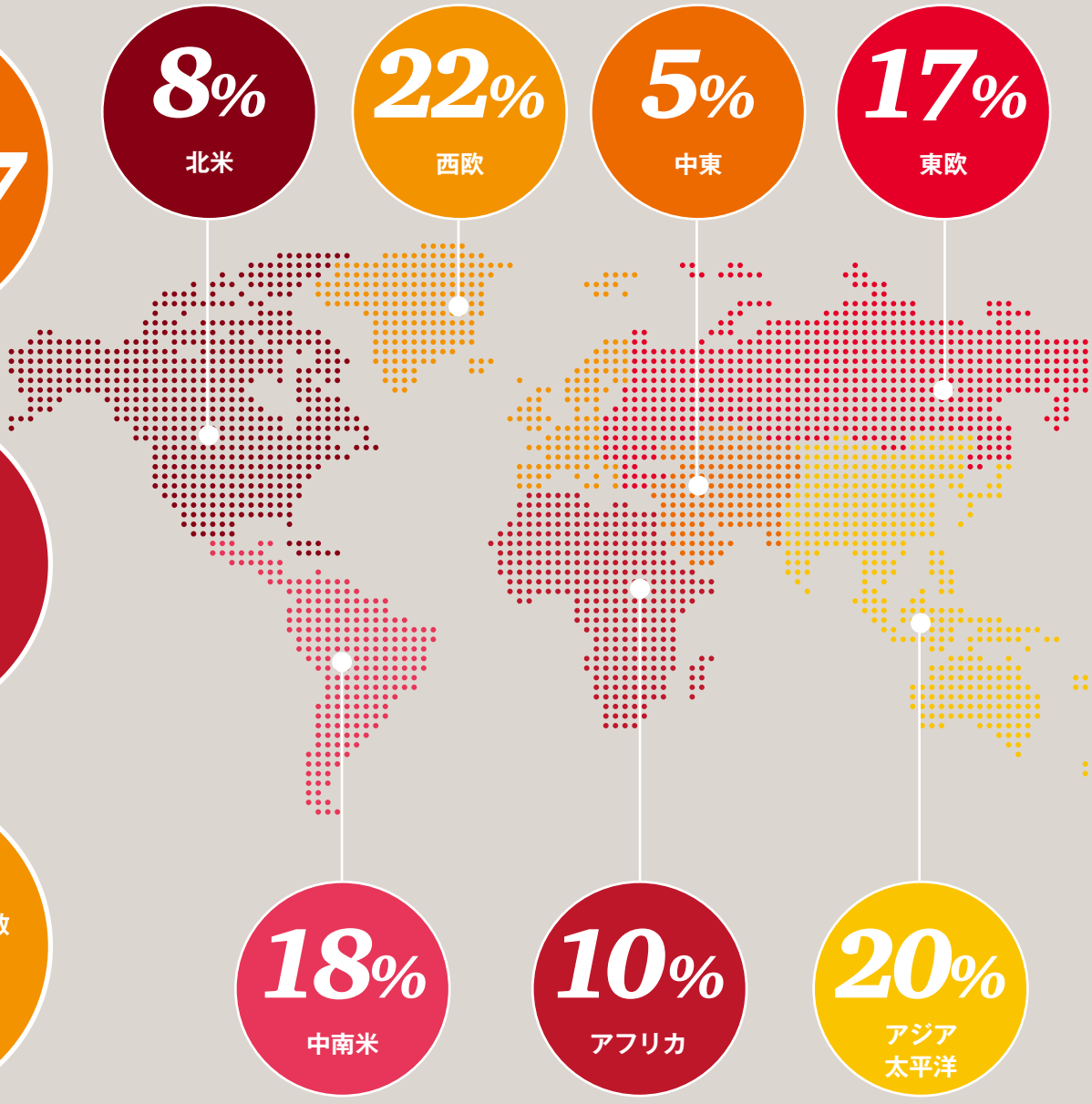
参加者データ

6,337
名が回答

115
カ国

調査に使用した言語数
17

地域別



回答者

70%
の回答者が、財務、経営管理、監査、コンプライアンス、リスク管理の業務を担当

54%
の回答者が、従業員1,000人以上の企業に雇用されており、それらの参加企業のうち、

48%
が従業員10,000人以上を擁している

37%
の回答者が上場企業の代表であり

59%
の回答者が多国籍企業に属している

業界

35% 工業

24% 金融

14% 消費財

7% テクノロジー

6% 専門サービス

13% その他

データリソース

さらに詳しい情報を希望される方に

犯罪実態調査ウェブサイトwww.pwc.com/crimesurveyは、本調査の拡大版として設計されており、調査データについてより詳しく知りたい皆様のために、以下をはじめとする、興味深い有用なリソースを提供しています。

・調査方法

・用語

・国別の比較

・参加企業に関する追加情報

本年度の調査データはGlobal Data Explorerと呼ばれる画期的なツールで表示されており、サイトの訪問者は、個々のニーズに応じてデータ分析をカスタマイズすることが可能です。

執筆者

Survey Leadership Team

Trevor White
Partner, South Africa
t: +27 (31) 271 2020
e: trevor.white@za.pwc.com

Mark Anderson
Partner, United Kingdom
t: +44 (0) 207 8042564
e: mark.r.anderson@uk.pwc.com

Didier Lavion
Principal, United States
t: +1 (646) 471 8440
e: didier.lavion@us.pwc.com

Editorial Board Members

Alex Tan
Executive Director, Malaysia
t: +60 (3) 2173 1338
e: alex.tan@my.pwc.com

Claudia Nestler
Partner, Germany
t: +49 (69) 9585 5552
e: claudia.nestler@de.pwc.com

Martin Whitehead
Partner, Brazil
t: +55 (11) 3674 2141
e: martin.j.whitehead@br.pwc.com

Antoinette Lau
Partner, China
t: +86 (21) 2323 5533
e: antoinette.yy.lau@cn.pwc.com

Dinesh Anand
Partner, India
t: +91 9818267114
e: dinesh.anand@in.pwc.com

Survey Management Team

Moazam Fakey
Senior Manager, South Africa
t: +27 (11) 797 4750
e: moazam.fakey@za.pwc.com

Anjali Fehon
Forensics Strategy Leader,
United States
t: +1 (973) 236 4310
e: anjali.t.fehon@us.pwc.com

Survey Marketing Team

Gemma Peart
Global Marketing Manager, United Kingdom
t: +44 (0) 771 1589 331
e: gemma.peart@uk.pwc.com

Kate Glenn
Forensics Marketing Leader,
United States
t: +1 (202) 312 7542
e: kate.n.glenn@us.pwc.com

Survey Research & Data Team

Colin McIlheney
Research Director, Northern Ireland
t: +44 (0) 289 0415719
e: colin.mcilheney@uk.pwc.com

Sabrina McCotter
Manager, Northern Ireland
t: +44 (0) 289 0415598
e: sabrina.c.mccotter@uk.pwc.com

Forensic Services Leaders

Andrew Gordon
Global Leader, United Kingdom
t: +44 (0) 20 7804 4187
e: andrew.gordon@uk.pwc.com

Andrew Palmer
EMEA Leader, United Kingdom
t: +44 (0) 20 7212 8656
e: andrew.palmer@uk.pwc.com

Erik Skramstad
US & APA Leader, United States
t: +1 (617) 530 6156
e: erik.skramstad@us.pwc.com

日本のお問い合わせ先

PwC Japanグループ フォレンジックサービス

PwCアドバイザリー合同会社
03 3546 8480（代表）

PwCコンサルティング合同会社
03 6250 1200（代表）

佐々木 健仁
パートナー
takehito.sasaki@jp.pwc.com

ホンマ シン
ディレクター
shin.s.honma@jp.pwc.com

平尾 明子
マネージャー
akiko.hirao@jp.pwc.com

上野 俊介
マネージャー
shunsuke.ueno@jp.pwc.com

奈良 隆佑
マネージャー
ryusuke.nara@jp.pwc.com

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/japan-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/gx/en/services/advisory/consulting/forensics/economic-crime-survey/cybercrime.html

日本語版発刊月：2016年7月　　管理番号：I201602-9