経済犯罪
ビジネス への脅威

37%
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

53%
「世界CEO意識調査」で回答したCEOの半分以上が贈収賄や汚職について懸念を示した

48%
回答者の半数近くがサイバー犯罪のリスクが増加したと報告。2011年の調査から23%も増加した

pwc

www.pwc.com/jp

経済犯罪は、あらゆる産業、地域、規模の企業にとって主要な懸念事項であり続けている。

目次

調査対象の内3社に1社（37%）が経済犯罪の被害にあったと報告している。

序文

不正行為、知的所有権侵害、汚職、サイバー犯罪あるいは不正会計といった経済犯罪が、あらゆる産業や地域における全ての組織にとって主要な懸念事項である、ということは周知の事実である。

今回実施した2014年経済犯罪実態調査はその事実を裏付ける結果となった。本調査では世界のあらゆる地域から調査に貢献いただき、5,000を超える回答を入手することができた。その結果私たちがこれまで行ってきた調査の中で、最も広範囲で包括的な経済犯罪の実態に関する調査になった。

経済犯罪が依然発生し続けることだけが問題なのではない。 経済犯罪が、企業の業務プロセスを脅かし、従業員の品位をおとしめ、企業の評判を傷つけることが問題なのである。そこで今年の報告書は、経済犯罪が各企業にどのような影響を与えているかに焦点を当てている。本調査が各企業にとって、予防の観点や戦略的観点から経済犯罪に取り組む一助となれば幸いである。

経済犯罪による脅威は進化しつづける。経済犯罪は、ウイルスのように世の中の動きに応じて形を変えながら、あらゆる企業に対して影響を及ぼしている。特に昨今の動きの中で影響の大きいものは、テクノロジーへの依存、あらゆるビジネスにおいてテクノロジーが使用されるようになったこと、また、経済的な活力が新興市場に移ってきていることが挙げられる。

企業・組織がますますテクノロジーへの依存を高める中で、サイバー犯罪の件数や頻度が増加し、巧妙化が進んでいることは驚くことではない。当社による調査の全回答のうち四分の一は、サイバー犯罪に巻き込まれた経験があると報告している。一方、見落とされがちな購買関連の不正、マネーロンダリングや人事関連の不正といった分類の経済犯罪も、資産の横領、贈収賄や汚職、不正会計といったこれまでの一般的な脅威と比較して増加傾向となっている。

経済犯罪は、全ての企業に共通の売買、支払いや代金の回収、雇用および解雇といった基本的なプロセスを脅かす。全ての組織は、日々の活動を通して他の組織と共に価値を生み出したり、価値を交換したりする中で、その活動を脅かすさまざまな種類の経済犯罪の脅威にさらされている。

経済犯罪が、経営者の大きな関心事であることはそれほど不思議なことではない。そして、私たちの最新の「2014年世界CEO意識調査」によると、協力を得た経営者の半数以上は、贈収賄や汚職に関して大きな懸念を抱いている。

本調査が、各組織の経営者を含むあらゆる関係者にとって、絶え間なく続く企業活動を振り返り、また将来を考えるきっかけとなり、また日々の企業活動を支える一助となれば幸いである。

Steven L. Skalak

ハイライト

- 経済犯罪は、ビジネスとビジネスプロセス（業務プロセス）にとって常に脅威である。—37％の回答者が経済犯罪に被害にあったと報告した。
- 使われる手口は地域によってさまざまではあるが、経済犯罪に対する脅威は世界中に存在する。—79 の地域の回答者が経済犯罪を経験したことがあると報告した。
- 贈収賄や汚職、マネーロンダリングや競争法違反などの「構造的な問題」という性質を持つ経済犯罪は、頻繁に規制当局によって調査されるため、一過性の不正行為よりもリスクがより高いと言える。
- 最も悪質な経済犯罪は、組織にとって重要かつ基本的な目標である「利益」と「コンプライアンス」の間の葛藤につけ込んで犯罪をすることである。リスクの高い市場で活動している組織は、そうでない組織に比べて、賄賂の支払いを求められた経験があるとの報告が2倍近くみられた。
- 経済犯罪は、下記表内のプロセスを含むさまざまな業務プロセスにとって脅威となる。

経済犯罪は下記を含むさまざまな業務プロセスにとって脅威である。

図表1：経済犯罪により脅威にさらされる主な業務プロセス

▪ 営業 （または販売）	▪ 顧客獲得
▪ マーケティング	▪ 国際的業務拡大
▪ 入札	▪ 税務
▪ 購買	▪ 施設管理
▪ 支払い	▪ 雇用と求人
▪ 業者選定	▪ 不審な取引の報告
▪ 流通	▪ 知的財産の開拓と普及
▪ 物流	▪ データセキュリティとプライバシー
▪ 商品や資産の管理	▪ ITネットワーク管理
▪ サプライチェーン業務	▪ 従業員の経費精算

- サイバー犯罪は増加の一途をたどっており、今年の調査にて4番目に発生件数の多い分類の犯罪であると報告されている。サイバー犯罪は、テクノロジーの問題というだけでなく、ビジネス戦略上の問題でもある。
- 私たちが実施してきた経済犯罪実態調査の14年間の間で、経済犯罪を発見するための内部統制の有効性は向上してきている。今年の調査の回答によると、55％の経済犯罪は、内部統制が機能することで予防的または事後的に発見されており、その割合は2011年の50％よりも上昇している。
- 経済犯罪は、世の中の大きな流れに応じて変化する。例えば、先進国から新興国への富の移動や、ビジネスにおけるあらゆる場面でのテクノロジーへの依存の高まりなどが昨今の大きな流れとなっている。
- 私たちの前回の調査と比べて、今回の調査では、贈収賄や汚職の事例の報告件数が13％増加している。また、第17回世界CEO意識調査にて半数以上のCEOが贈収賄や汚職について懸念しているという結果となった。

回答者の37％が本調査期間内に自分が属する組織で経済犯罪が少なくとも一回は発生していると回答しており、これは2011年の調査から3％増えている。

2014年の経済犯罪について
概要

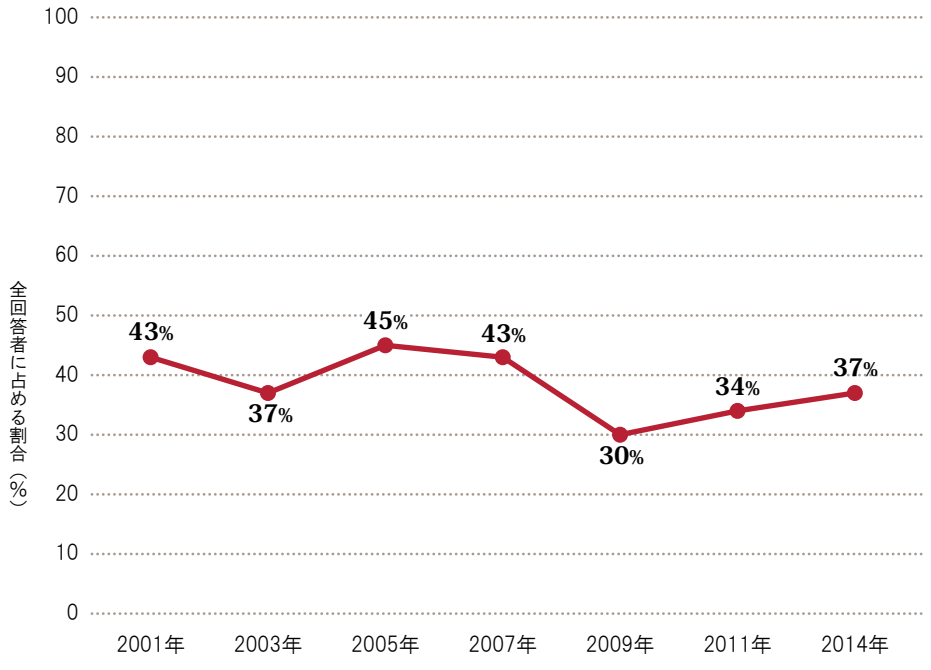
2014年の調査は95カ国以上から5,128の回答を得た。半数以上（54％）の回答者は1,000人以上の従業員を抱える組織で働いており、約3分の1（35％）の回答者は上場企業に所属している。

本調査を通して、経済犯罪はあらゆるグローバルビジネスの分野において、いまだ厳然と存在する根本的な問題であることが確認された。回答者の37％が本調査期間内に自分が属する組織で経済犯罪が少なくとも1回は発生していると回答しており、これは2011年の調査から3％増えている。

経済犯罪にはさまざまな種類があり、それぞれ特徴や脅威、企業に与える影響も異なる。本報告書では、主だった不正の種類について詳細に分析している。経済犯罪の実態と今後の予測について、回答者の意見や、経済犯罪が各組織に対してどのような影響を与えたかについて分析を加えるとともに、実際に発生した事例を取り上げて考察を加えている。

調査時期によって、経済犯罪の規模や種類は違えども、私たちの14年間の調査データから言えることは、どの調査期間においても、常に約3分の1の回答者が経済犯罪の被害を受けた経験を持つということである。

図表 2：経済犯罪報告比率の推移（GECS）



不正の種類

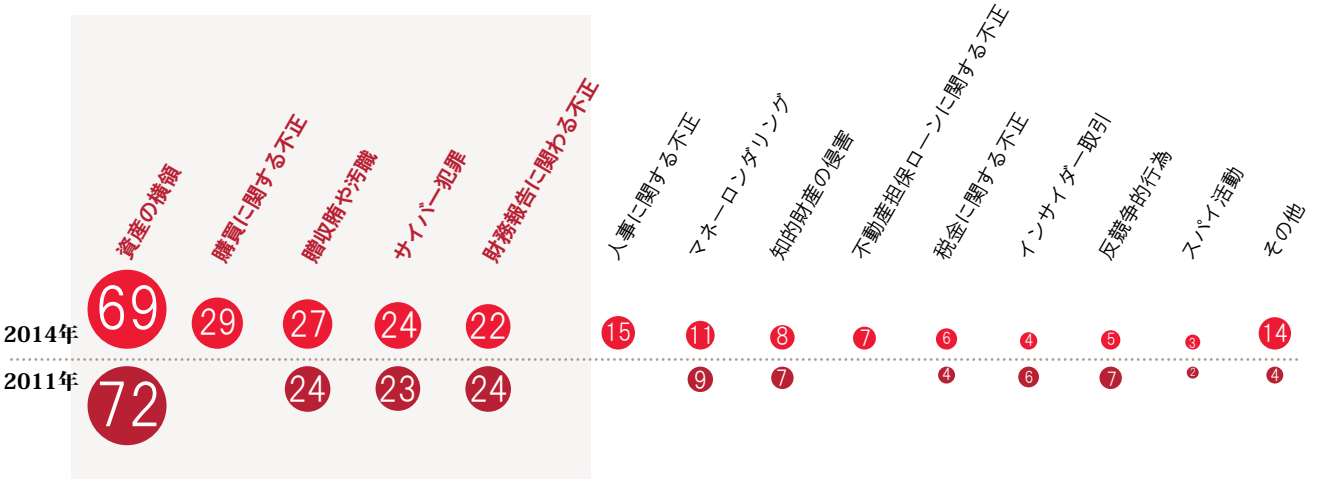
2001年に初めて実施した経済犯罪実態調査以降、資産の横領（通常最も多い）、贈収賄や汚職、および財務報告に関わる不正の三つの不正が常に上位に入っている。また、2011年よりサイバー犯罪を個別の不正の分類として加えている。

また、それに加え今年は新たに購買に関する不正という分類を追加した。大きな流れとして、政府や国営企業による入札での競争が激化していることや、さまざまな組織においてサプライチェーンの統合が主要な事業活動となってきていることなどが背景としてあげられる。購買に関する不正は今回の調査で29％と、全体で2番目に高い結果となった。長年上記の三つの不正の分類が一般的（回答者全体のうち20％以上の回答が得られたものを一般的とする）だったものの、2014年調査ではサイバー犯罪と購買に関する不正を加えた五つの不正の分類が20％を超えるものとなった。

さらに上記の購買に関する不正に加え、今年は人事に関する不正と不動産担保ローンに関する不正という分類も追加した。「その他」の分類の中には保険詐欺、融資不正、クレジットカード詐欺などさまざまな不正が含まれている。

図表3では経済犯罪の種類別報告件数をまとめている。

図表3： 分類別　経済犯罪報告比率



調査期間中に経済犯罪の被害にあったと回答した回答者の割合（%）

地域による傾向

地域別の傾向としては、2011年調査と比べると他地域との差が歴然ではないが、アフリカの回答者から最も多く経済犯罪が発生しているという回答を得た。

北米については、例年同様経済犯罪は高い割合で報告されているが、これは同地域でグローバルな企業展開を進めている企業が多いことや、不正を発見するための仕組みや方法論が比較的整備されていることが理由であると考えられる。また、西欧については、報告の比率が高くなってきているが、これは後述するように、EUを含む規制当局による不正に対する意識が、金融業界を中心として高くなっていることが背景にある。

しかしながら、中東は他地域とは異なる傾向が見られた。全体的な報告の割合は全地域の中でもっとも低いものの、不正の種類や事例は多岐にわたるものであった。

図表4：地域別　経済犯罪　報告比率

地域	2014年	2011年
アフリカ	50%	59%
北米	41%	42%
東欧	39%	30%
中南米	35%	37%
西欧	35%	30%
アジア太平洋	32%	31%
中東	21%	28%
新興8カ国*	40%	35%
世界全体	**37%**	**34%**

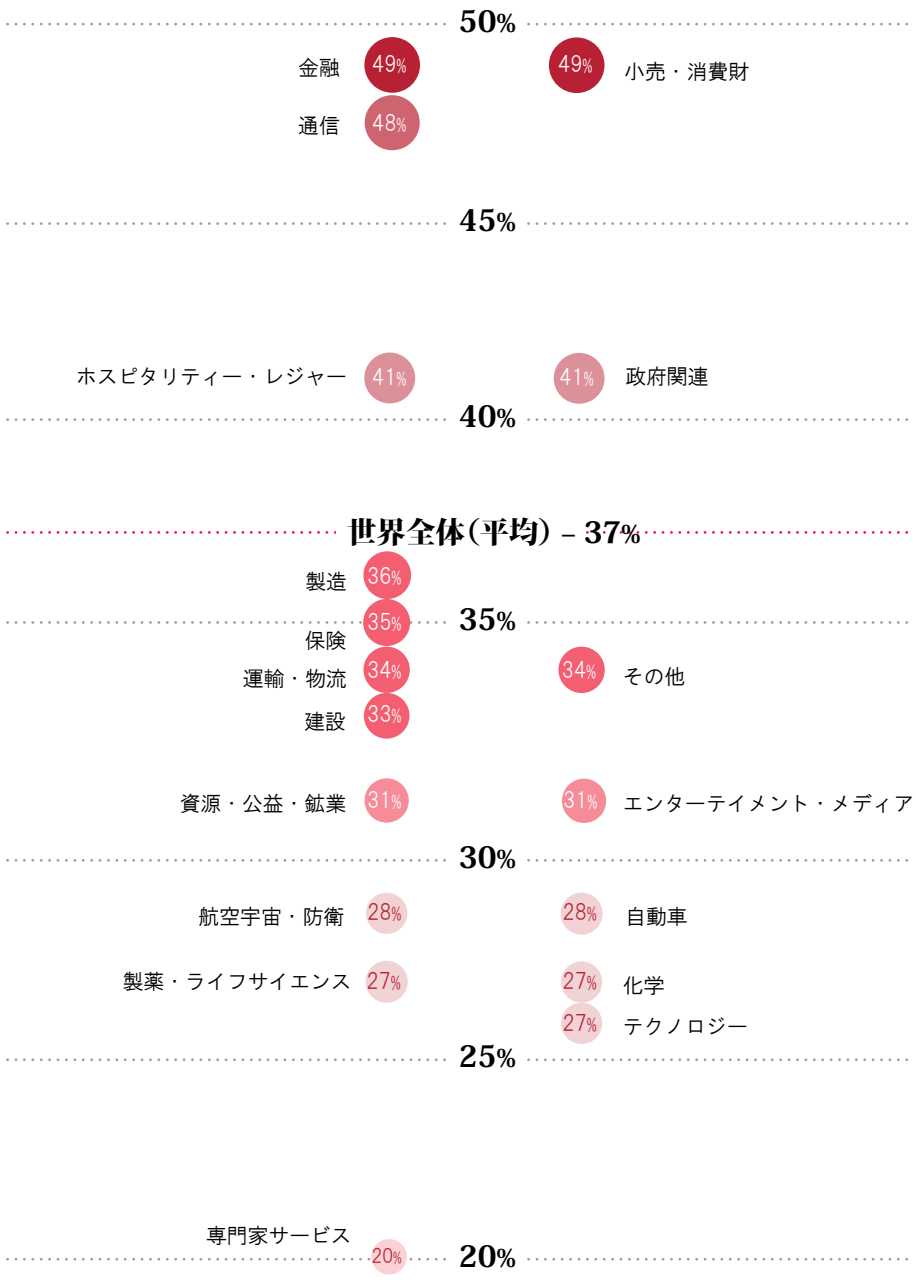
*新興8カ国：ブラジル、中国、インド、インドネシア、メキシコ、ロシア、トルコ、南アフリカ

業界による傾向

業界別の傾向としては、金融、小売・消費財および通信業界の三つの業界が群を抜いて経済犯罪の報告が目立っている。金融業界における不正については、サイバー犯罪やマネーロンダリングの影響が大きいものと思われる。また、小売業および通信業界では、予想どおり資産の横領の割合が高くなっている。

不正の報告の割合が、27％から36％の範囲に多くの業界が集まっている。またこの報告の割合は世界全体平均を下回る反面、この範囲に含まれる多くの業界のうち、特に建設、運輸・物流などは贈収賄や汚職、購買に関する不正などの経済犯罪の被害に遭いやすいようである。

図表5：業界別の経済犯罪報告比率



調査期間中に経済犯罪の被害にあったと回答した回答者に占める割合（%）

特定の人間の行動による一過性の経済犯罪からも被害は受けるが、構造的な経済犯罪の影響の方が企業にとって大きい。

二つの脅威

なぜ経済犯罪はあらゆる地域、あらゆる業界の企業の隅々まで影響を与えるのだろうか。序文にもあるとおり、基本的なビジネスプロセスは、商品の流通、資本調達、知的財産の活用、取引相手の選定、決算報告、コンプライアンスに準拠している組織の経営、ブランド価値の確立など、第三者と現金やその他の価値を取引することを基盤としている。これらの第三者との接点が経済犯罪の脅威にさらされやすいところなのである。

さらに分析をしていくと、脅威の種類が二つに分類できる。

資産の横領を、スリや窃盗といった特定の人間の行動による一過性の事件に例えるなら、連邦海外腐敗行為防止法（FCPA）や2010年贈収賄法（UK Bribery Act）のような贈賄防止法令に背くような重大な違反、または自社組織でのマネーロンダリングなどは、企業の構造的な問題である。

一過性の経済犯罪からも被害を受けるが、構造的な経済犯罪の影響の方が企業にとって大きい。規制当局から課徴金を課せられ、評判が失墜することはもちろんのこと、それ以外のさまざまな長期的損害も引き起こされる。社員の品位が損なわれ、企業の営業、マーケティング、物流、コンプライアンス、サプライチェーン、支払い処理、政府関連機関との関係や財務報告などの分野の内部統制の脆弱（ぜいじゃく）性を露呈する。

贈収賄や汚職が業務プロセスに与える脅威

さまざまな業務プロセスに潜んでいる経済犯罪の脅威をより強調するため、下記に私たちの経験を踏まえたシナリオをまとめた。

グローバル企業が成長を期待している市場は、比較的汚職リスクの高い国であることが多い。ある企業が現地で営業チームを設立し、積極的に法人顧客、教育機関や政府機関と幅広い顧客層に営業、販売を推進するプログラムを導入したとしよう。

営業チームは直ちにミーティングやイベント、実演を行い、市場での認知度を高める。また、戦略的に重要な顧客や、マーケットに影響力を持つ人物とコネクションのある人間を主要スタッフとして雇用する。さらには、顧客からの物流関連のニーズや期待を参考に、流通ネットワークを確立する。つまり、企業は自社の目標達成のために体系的かつ効率的な方法で、また精力的に市場に参入するのである。このような一般的な新規市場開拓の過程においても、企業はさまざまな課題に直面する。

課題は比較的平凡な支払いプロセスの問題から、新規業者との関係に関わる複雑な問題に至るまでさまざまである。例えば、支払プロセスに関する問題であれば、ミーティング、接待、実演やイベントの出席者確認の記録はしっかりとっているか、政府関係者は出席していたか、提供した食事や贈答品の金額は社内規則、現地法にしたがっているか、などが挙げられる。また、新規業者との関係に関する問題であれば、当該業者が政府関係者とつながっているか、といった潜在的な問題を検知できる適正なデュー・デリジェンス・プロセスが存在するかも課題となる。

その一方で、人事プロセスにおいては、現地市場で有益なコネクションを持つ人物の採用に課題があると言える。例えば、その人物の中には、親族が政府関係者の人間がいるかもしれない。通関業者は、企業やその顧客から迅速な通関手続きを期待され、定期的に税関職員に接待をしているかもしれない。技術チームは自社製品の承認およびライセンス認可プロセスを手伝ってもらえるように、政府推奨のコンサルタントや退職した元規制局員を雇っているかもしれない。繰り返しになるが、こういった場合においても、業者選定のデュー・デリジェンス・プロセスと支払いプロセスが課題となってくる。

営業チームは常に競争にさらされ、売上を増やすため、販売業者に通常より何パーセントか多めの値引きを提供するかもしれない。企業の顧問弁護士事務所は労務関連の問題対処のために一カ月単位で現地労働法弁護士を雇うだろう。最後に、税務チームは自社での輸入品の関税上の取り扱いや現地子会社の利益に関わる移転価格税制について現地税務当局と頻繁に相談することになる。

経済犯罪を業務プロセスを脅かす存在としている理由として、上記のさまざまな活動が、それ自体は不適切というものではない、ということが挙げられる。だがその活動をしていく間には、従業員の品位を試し、また従業員に対し売上目標を達成することと、さまざまな社内規則や規制を遵守しつつ業務にあたることとの両立で大きなプレッシャーを与えることが起こりうる。現地の政治状況やビジネス文化の特徴によっては、賄賂の支払が要求されることもあるのである。

不正による損害

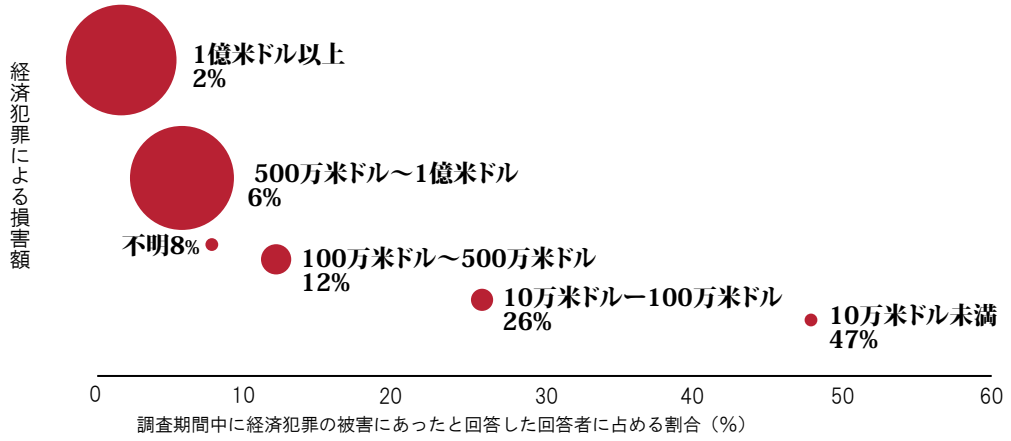
実際にその不正の事象が発生するまでは、各組織はそれが実際にどれくらい財務的な影響を与えるかについて、通常正確に把握することはできない。また、事象が発生してしばらく時間がたったあと、ようやくその影響の全容が分かってくるという場合も珍しくはない。これまでの過去の報告書内でも強調されているように、組織における不正の代償は甚大であり、金銭面だけではその影響を推し量ることはできない。

財務的な損害

図表6で見られるとおり、5社に1社（18％）は100万米ドルから1億米ドルの損害を被っている。さらに、損害額が1億米ドル以上の組織は2％と2011年調査の1％の2倍に膨れ上がった。

損害額の1億米ドル以上に当てはまる回答者は30と少なく感じるが、全体の比率として前回の調査の倍であることには変わりなく、不正の影響は深刻である。この増加は贈収賄や汚職に関する不正の件数増加の影響である可能性が高いと思われる。贈収賄や汚職の場合、規制当局の罰金、弁護士費用、裁判費用、補償費用などの総計が1億米ドルを超えることもありうる。

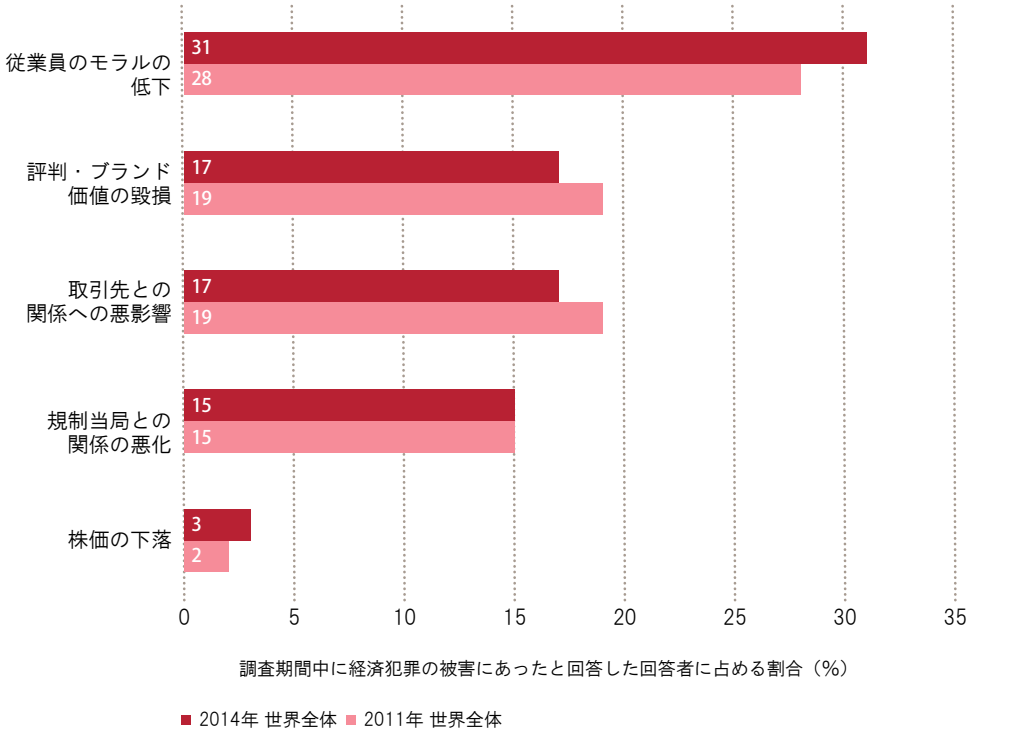
図表6：組織における財務的な損害



副次的な損害（直接財務的な影響はないが重大な損害）

不正の代償は経済的損害だけにとどまらない。調査結果によると、不正による財務的な影響以外の大きな損失としては、従業員のモラルの低下、組織の評判やブランド価値および取引先との関係への悪影響などが主な回答として挙げられる。

図表7：経済犯罪による副次的な損害



前述した副次的な影響を考慮すると、不正の代償の大きさは計り知れない。万一、世間から注目される不正事件が発覚した際、次のような悪影響が考えられるであろう。顧客離れによる収益減、規制対応によるマーケット進出の遅れ、株価の暴落、従業員の士気低下と離職率増加による生産性の低下などが挙げられる。

幸い、2014年世界CEO意識調査では回答者である組織の経営者の半分（2013年の37%からの増加）が、「ビジネスで信頼を失うこと」は市場において大きな問題の一つであるとしており、財務的な影響以外の悪影響について理解しているようである。また、その中の多くの経営者が、企業の社会的役割は株主価値を上げるだけにとどまらないと考えている。

副次的な損害：最悪のケース

私たちは一つの事件をきっかけに企業全体が崩壊したケースを多々目の当たりにしてきた。

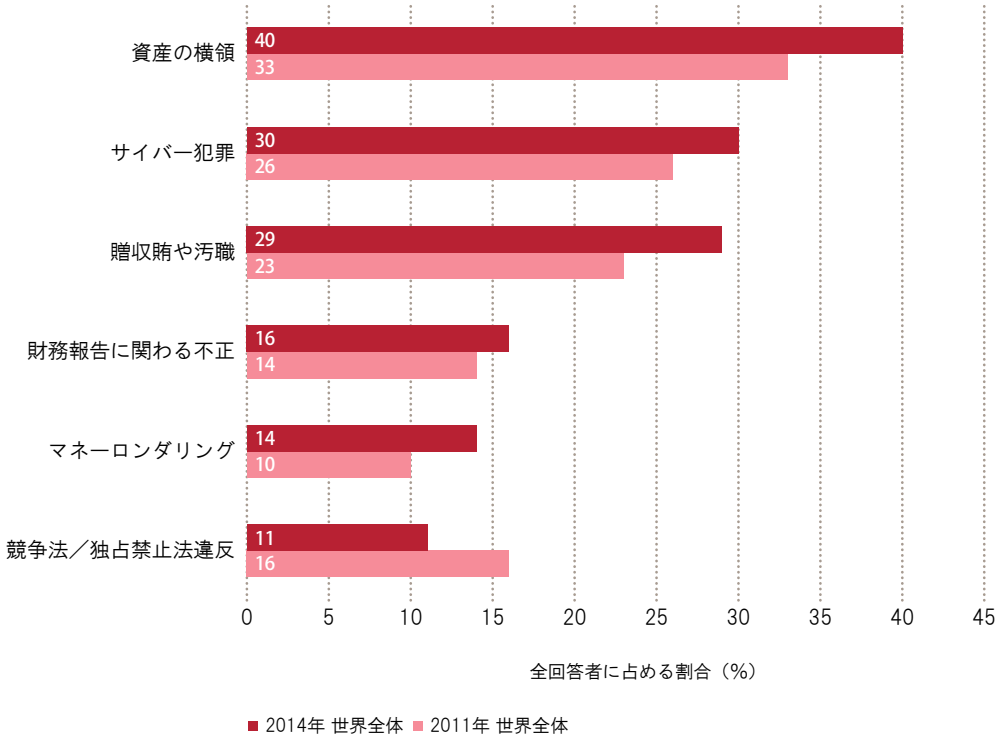
例えばインサイダー取引や財務諸表不正のような事件は一見、特定の口座、特定の部署または特定の顧客にだけ関係しているかのように見える。だが競争の激しい市場において、顧客、取引先や投資家にとって、不正を抱える企業と取引関係を維持する利点はあまり見受けられない。また今後の企業活動が規制当局から強制的に制限される可能性もある。そして、顧客、資本、従業員や投資家が企業から離れていく。その結果、企業活動の見通しが立たなくなり、内部から企業は崩壊する。

今後の見通し

これまで過去に発生した経済犯罪とその影響を見てきたが、それに加えて回答者には、今後組織を発展させていく上でどういった部類の不正のリスクが最も顕在化する可能性が高いと思うかについても回答してもらった。ほぼ全ての分類で、今後は不正のリスクの増加とともに、これまで以上に不正に巻き込まれる可能性が高いと考える回答が多く見受けられた。

図表8ではその2014年調査の回答結果について、2011年調査の結果と比較している。

図表8：今後の経済犯罪発生傾向　見通し



上記結果は、発展途上国への進出の大きな流れや、ビジネスのあらゆる分野にテクノロジーが導入されたことによるサイバー犯罪の脅威の増加を反映しているようである。

競争法や独占禁止法の分類では5%ほどの減少が見られる。また後半で、この独占禁止法関連の犯罪についての意識が若干薄れつつある状況について分析を加えたいと思うが、ここで一点だけ例外を補足すると、この傾向はヨーロッパ地域の結果にだけは当てはまらない。考えられる理由としては、ヨーロッパ規制当局の摘発に向けた活発な動きと昨今の関連ニュースなどの影響が、ここでの回答にも反映されているものと考えられる。

経済犯罪の中には、他と比べて著しく政府当局の関心を引く類のものがある。

政府当局による規制の影響

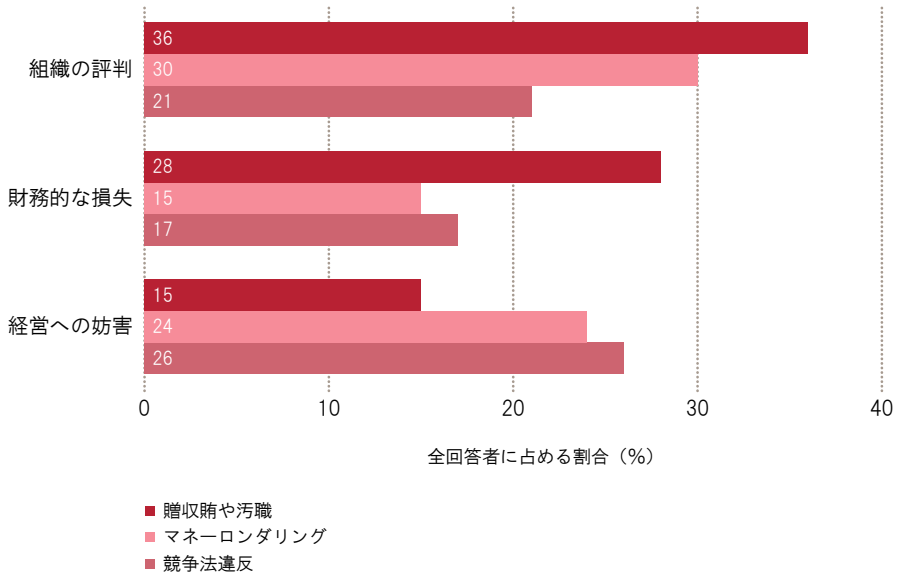
経済犯罪の中には、他と比べて著しく政府当局の関心を引く類のものがある。こういった状況を鑑み、贈収賄や汚職、マネーロンダリング、競争法違反といった経済犯罪について、ここで一章を設けて解説をする。

これらの三つの犯罪の特徴としては、各国で定められているビジネスにおける行動規範から逸脱してしまったことにより発生するということである。また、米国や英国のように、著しく厳しい基準のもと、非常に高額な罰金を科す法律を適用している国も存在している。

相互依存が高まる世界において、これらに分類される経済犯罪はグローバル企業にとって新しい脅威となる。高額な罰金を科されたり、当局に起訴されたりするだけでなく、それらの犯罪はさらに大きな組織的な問題として取り扱われることがある。（例．内部統制の不備、業務プロセスにおける欠陥、企業文化の腐敗、経営陣の姿勢の問題など）それだけでなく、それらの犯罪は副次的な悪影響をももたらすことがある。例えば、ソーシャルメディア上で当該組織の批判が広まる、既存メディアによって心外な報道をされる、訴訟に巻き込まれる、株式市場で株価が大きく下落するといったことで会社の評判が傷つけられる可能性がある。また、財務的な損失だけでなく、経営計画を実施する上で大きな妨害になることや、優秀な人材を失うこともまた副次的な悪影響であると言える。

私たちの調査でも実証されているように、規制当局によって頻繁に摘発されるこれらの三つの経済犯罪について、回答者は自社の評判が傷つけられるリスクと、経営計画を実施する上で大きな妨害となるということを最も大きな影響として回答している。

図表9：経済犯罪により最も影響を受ける項目

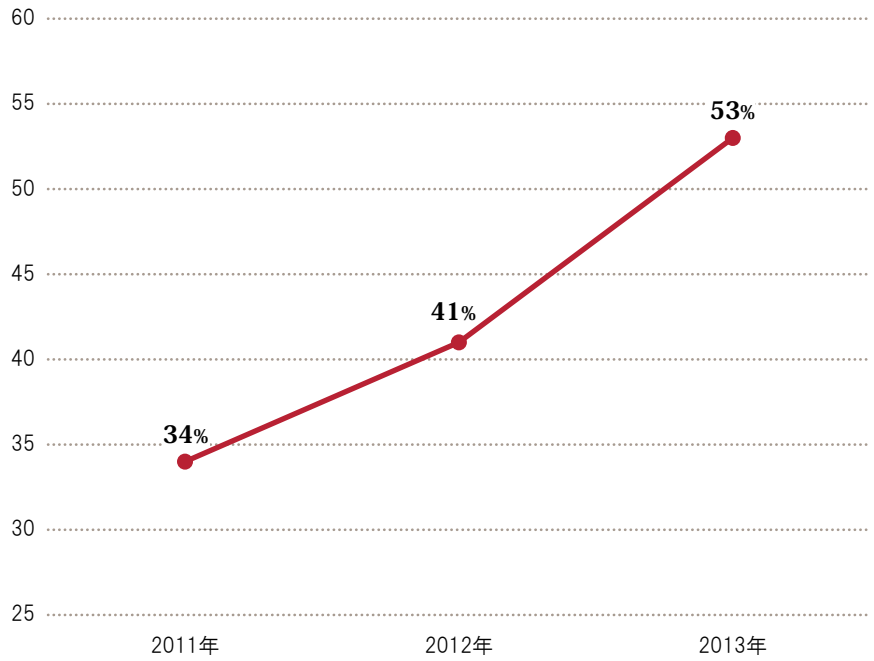


贈収賄や汚職に対する経営陣の認識

最も一般的な犯罪というわけではないが、私たちの調査に登場するあらゆる種類の不正の中で、贈収賄や汚職はグローバルビジネスにおいて最も大きな脅威であるかもしれない。なぜならば、これは営業、マーケティング、販売、支払い、海外展開、経費申請、税務申告、そして施設や工場の運営に至るまであらゆる業務プロセスに関連するからである。

どの地域においても多くの贈収賄や汚職の発生件数が報告されている。調査期間中に贈収賄や汚職に関わる事象を経験したと報告した人は全回答者の27%を占め、2011年の24%に比べ13%増加している。またその割合は多くの不正の分類の中で3番目に高い割合となった。

図表10：増加する贈収賄と汚職に対する経営者の懸念



PwC世界CEO意識調査より（%）

経済犯罪が企業をさまざまな形で脅かす昨今において、本年度の世界CEO意識調査を見ても分かるように、贈収賄や汚職のリスクに対する経営陣の関心は著しく高まっている。

27%

調査期間中に経済犯罪の被害にあったと回答した企業の27％が汚職があったと報告した。

脅威にさらされる営業やマーケティング

贈収賄や汚職のリスクはさまざまなビジネスにとって脅威である一方、企業が政府機関や国営企業を含む政府関係者と協働する際には、特に大きな懸念事項となる。

一例を挙げると、例えば、ある製薬会社が、新しく開発した薬を公的医療プログラムを実施している国に販売しようとしているとする。その場合、薬剤販売の認可、購入の可否と支払価格は、政府当局者の手中にあるようなものである。

別の例として、機器販売会社が自社製品を、役員が現職の与党の国会議員である国営企業に販売しようとしているとしよう。その場合、入札書類に記載する仕様書の内容、予算、研修に必要な追加サポート、予備の部品、保守、入札に向けた提案書に対する評価に至るまで、全て政府関係者によって決定されることになるだろう。

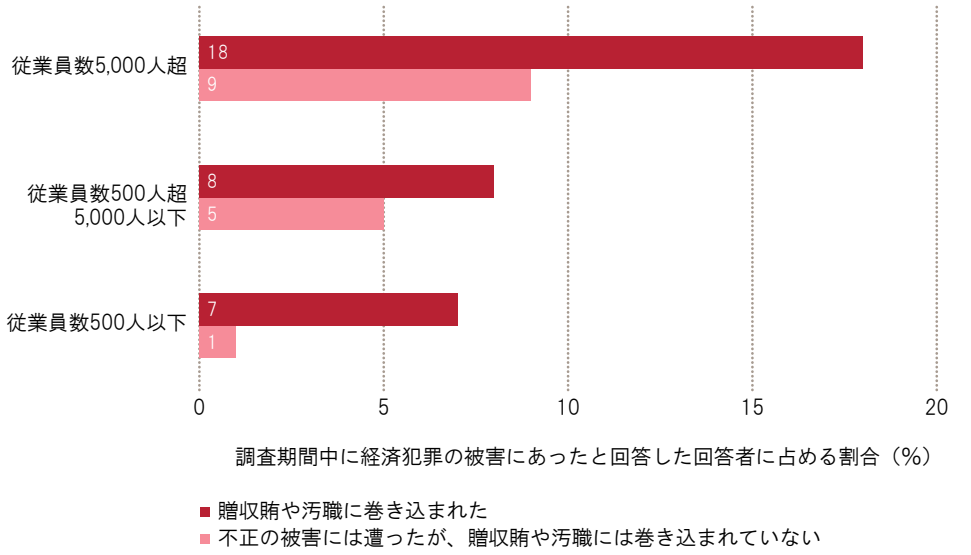
もしその地域が比較的贈収賄や汚職に厳しくない地域であれば、政府当局者は賄賂を期待しているか、少なくとも賄賂に対して寛容な考えを持つ傾向にあるかもしれない。そういった状況は、成長市場に新製品を展開する使命を担っている製薬会社の営業およびマーケティングスタッフにとって、賄賂あるいはキックバックまたはより良い価格を確保するために認可プロセスを不正操作することを正当化するプレッシャーとなる。

営業担当者やマーケティング担当者にとって、利益獲得のために行動をすることは当然のことではあるが、汚職に巻き込まれやすい環境下において、そのリスクが潜んでいることは看過されがちだ。FCPA（海外腐敗行為防止法）やその他の規制適用はしばしば甚大な財務的かつ非財務的な損失をもたらす。それは例えば、売り上げプロセス、売り上げ実績によるインセンティブの考え方、販売網、マーケティング活動や他の支払いに関する承認権限、代理店の選定などを変えてしまうだけでなく、時には特定の国でそもそもビジネスができなくなってしまう場合も起こり得る。

しかしながら、経営者の贈収賄や汚職に対する不安が高まる一方で、それに対応するための業務プロセスの強化は、多くの組織においていまだ発展途上となっている。

贈収賄や汚職による財務的な損失や副次的な損失は、積極的に腐敗防止に取り組む政府によって科せられる罰金の観点からも甚大なものになり得る。下記の図表によると、従業員の数に関わらず、贈収賄や汚職に巻き込まれた企業は500万米ドル以上の損失を報告するケースが多くなっていることが分かる。

図表 11: 企業規模別、500万米ドル以上の贈収賄や汚職関連損失



先進国から発展途上国へ

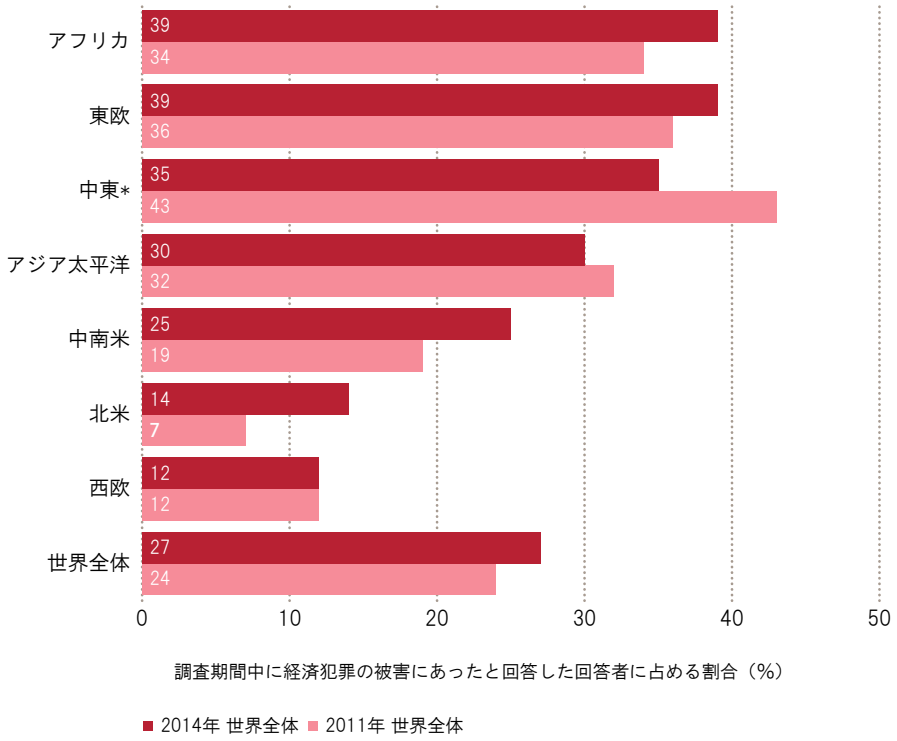
世界経済は基本的に回復基調にあり、企業のビジネス拡大への意欲を再び活性化させるとともに、それに伴うリスクへの関心も高めている。私たちの調査の結果、多くの企業（50%）が汚職のリスクが高いとされる地域において企業活動を行っていることが分かった。さらに、今後2年間でそういった地域への進出を考えている企業は8%に上る。また、データによると[1]、これらの地域に属する国々において、贈収賄や汚職の不正全体に占める割合は36%となっており、世界全体の平均27%を上回っている。

贈収賄や汚職の報告件数が多くなっている大きな要因の一つとしては、欧米を始めとする先進国から、成長目覚ましい新興地域であるアフリカ諸国やアジアの一部の地域への、構造的な富の移動があることは間違いない。これらの地域では、贈収賄や汚職について、文化的にも異なった価値観を持っており、またそれらについての規制も少なく、またその規制自体も欧米のものと比べてそれ程厳しいものではない。したがって、これらの地域や国々では贈収賄や汚職についてのリスクが高いという結果になる。

図表12に示したとおり、贈収賄や汚職については、アフリカと東欧が39%と最も高い割合の報告となり、それに中東が35%と続いていて、どちらも全世界平均を上回っている。とりわけ中東は、豊富な資源を有し、またインフラ整備や建設に依存する経済であるため、それらの産業がこれまでも不正や汚職の温床となっていた経緯がある。

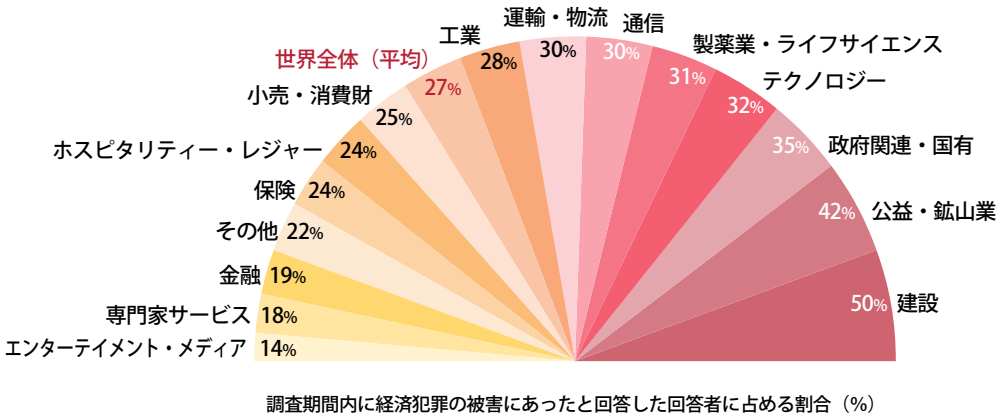
1. 2012年 トランスペアレンシー・インターナショナルによる腐敗認識指数（“CPI”）に基づき、各組織がリスクの高い地域で活動しているか、または活動予定があるかについて回答を得た。”CPI”は汚職に関するさまざまな分析を行っている非営利組織のトランスペアレンシー・インターナショナルによって毎年開示されている。

図表12：地域別の贈収賄や汚職の報告状況



*中東は2011年調査では「アジア太平洋」地域に含まれていた

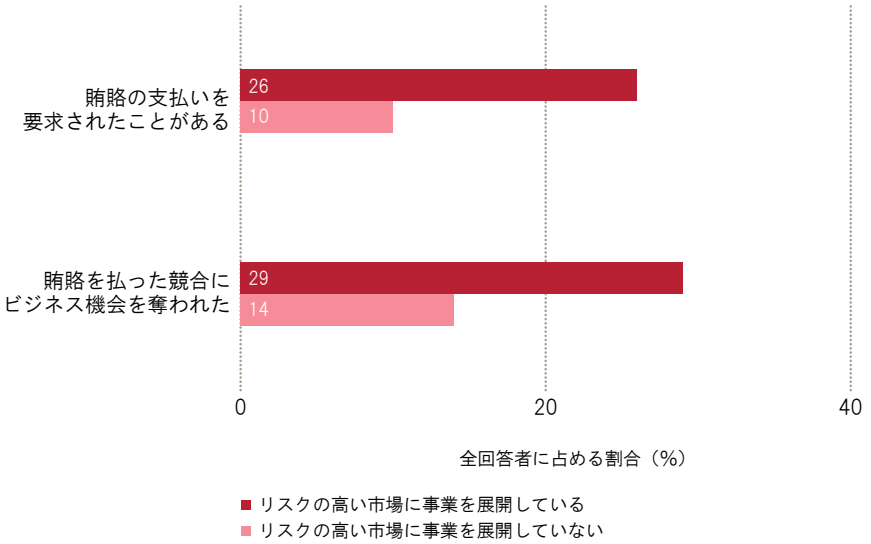
図表13：業界別の贈収賄と汚職の報告状況



2012年の腐敗認識指数（CPI）によると、北米は世界の他地域よりも汚職のリスクが低いという結果になった。しかしながら、2011年から2014年にかけて、同地域の贈収賄や汚職に関する事象の発生件数の割合は2倍になっている。この結果は、北米地域に属する回答者の企業が、よりリスクの高い地域への事業拡大を進めていることを表している。実際に48％の回答者が本調査期間中に自社が汚職のリスクが高い地域への進出を検討したと回答しており、その割合はアフリカの50％に次いで2番目に大きいものであった。

図表14を見ると、贈収賄や汚職のリスクが高い地域において活動する企業の方が、そうでない企業に比べて、賄賂を支払うように要求される可能性や、賄賂を支払わなかったことによって実際に賄賂を支払った競合他社にビジネス機会を奪われるなどの可能性が、著しく高くなっていることが分かる。競合他社が公正にビジネスを行っていない場合、その競合他社の行動に倣わざるを得ないプレッシャーは相当なものだと言える。

図表14：贈収賄と機会損失



贈収賄や汚職は規制当局によって国境を越えて摘発されることも少なくないため、各企業が成長著しい新興国で企業活動を行う場合には、そのリスクに十分留意しなければならない。それは、たとえ現地の規制や慣習が比較的緩い場合でも同様のことである。実際、北米や西欧地域における贈収賄や汚職に関する報告件数は規模としてはそれ程大きくはなく、それらの国々の政府当局の関心はアフリカやアジアなどのリスクが高い国々に向いている。

現地特有の課題

比較的汚職が身近ではない社会で生まれ育った人たちは、賄賂が要求されるという文化を過小評価する傾向がある。賄賂が横行しやすい文化において、売り上げの達成やビジネスでの成功を目指している従業員たちは、賄賂が要求または期待されているのか、どれくらいの注意を払うべきかなど、汚職のリスクについて認識していない可能性が高い。

そして、彼らは、企業方針に反し、地域の慣習に従うために自分たちの行動をさまざまな方法で正当化する傾向にある。

企業が従業員に期待することと、地域の慣習が要求することの間に生まれる恒常的なジレンマを克服することは、多くの人が考えているほど容易ではない。こういった状況は、さまざまな形を通じて企業の営業やマーケティング活動を脅かすことになる。例えば、従業員に不適切な契約を結ぶプレッシャーを与える、流通経路の中に不必要に多くの利害関係者を巻き込む、顧客の役員の親族を雇用する、顧客の特定の従業員のためにアドバイザー業務などの仕事を提供する、裏金のプールを作るために代理店に対してのディスカウントを増やす、などがある。

各地域の慣習からの要求や誘惑を乗り越えて、会社の方針や法律を遵守するためには、全ての従業員に対して、今までの人生で培った適切な倫理観を保つよう、強く一貫したメッセージを発信し続ける必要がある。

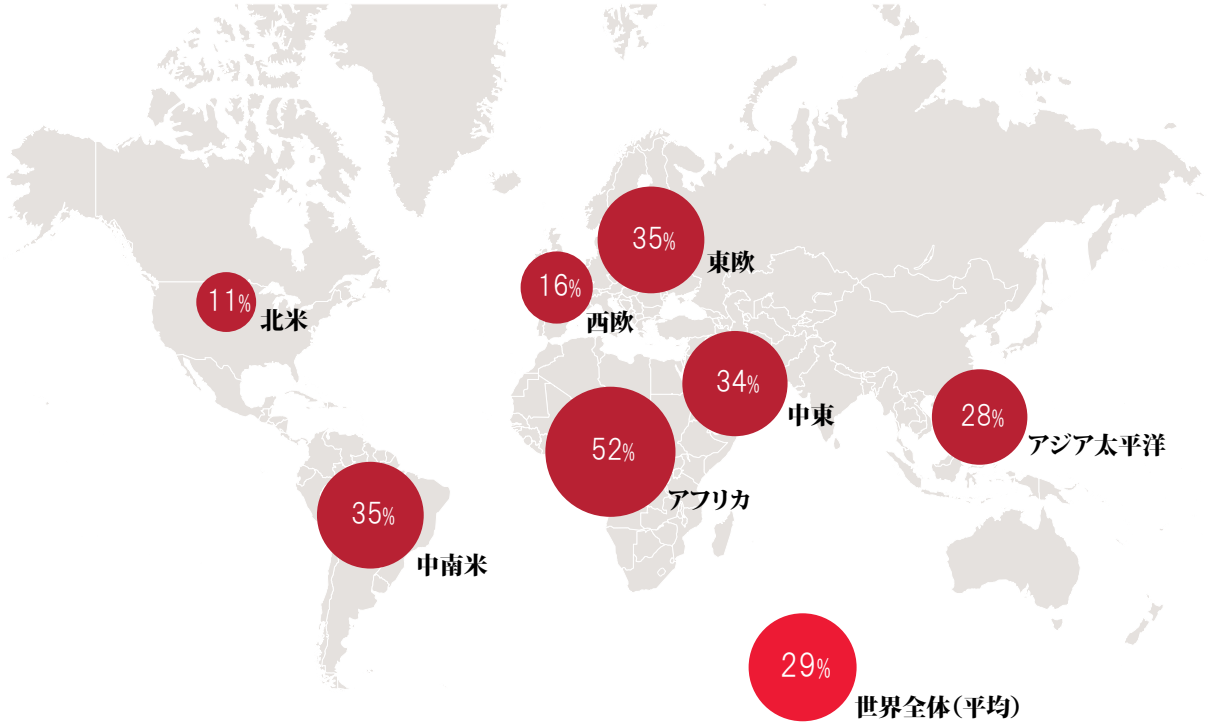
現状の認識と今後の見通し

本調査における回答者の回答を見ると、他のほとんどの経済犯罪の分類よりも、贈収賄や汚職の脅威に対する認識が急激に高くなってきていることが分かる。29%の回答者が、自社が贈収賄や汚職に巻き込まれる可能性があると回答しており、2011年の23%と比べても大きく増加している。またこれは、組織が将来巻き込まれる可能性があると回答している分類の中で、2番目に位置付けられているサイバー犯罪と似た傾向となっている。

贈収賄や汚職は、それに対する脅威の認識が高まっているだけでなく、あらゆる産業で発生している。例えば、比較的発生率の低いエンターテインメント・メディア産業における21%から、37%と高い資源関連、電力などの公益事業、鉱業など多岐にわたる。

図表15に示したとおり、地域別で見ると、地域ごとに傾向があることが分かる。世界全体では今後の脅威に対する予測の程度は、これまでの認識の程度に近いものであった。しかしながら、アフリカや南米では、現状のリスクを認識している程度（それぞれ39%および25%）に比べて、将来の脅威に対する認識の程度が大きくなっている。（それぞれ52%および35%）

図表15：地域別の贈収賄や汚職の将来の脅威に対する認識



全回答者に占める割合（%）

マネーロンダリング：金融業界にとっての脅威

金融業界に所属している回答者は、最も懸念している経済犯罪について、他の業界の回答者と全く異なる見解を持っている。彼らが最も懸念している経済犯罪は「お金の実際の出どころを偽ることにより、犯罪による収益を正当化しようする行為」とされるマネーロンダリングである。

マネーロンダリングは、金融機関にとって、もしそれを報告する義務を怠った場合リスクとなる。つまり、もし何かマネーロンダリングに関する事件が起きたとしても、その組織が法律にしたがって、顧客との取引を精査するなど、法令遵守に真摯（しんし）に対応している場合には、その金融機関は規制当局によって罰せられない可能性が高い。

金融業界に属する回答者のうち4分の1を超える27％の回答者が、本調査期間にマネーロンダリングに巻き込まれたことがあると回答しており、この比率は2番目に比率が高かった保険業界の11％の2倍以上となっている。さらに、金融業界に属する回答者の58％が、贈収賄や汚職、競争法違反よりも、マネーロンダリングに対して大きなリスクを認識しており、それは上記三つの分類の中で最大であった。

マネーロンダリングの形態はその巧妙さや複雑さにおいてさまざまである一方、必ず金融機関の設備やサービス自体にアクセスする必要がある。したがって、顕在化する現実的な脅威としては、マネーロンダリングは人間の弱みに付け込んだ犯罪といえる。そういった脅威に直面することは、少なくとも、問題を抱える市場から退場でもしない限りは、決して避けることはできない。したがって、日常の業務プロセスにおいて常にこの脅威と向き合う必要がある。

マネーロンダリングは、金融機関における下記のような業務プロセスを主に脅かす。

- **顧客獲得プロセス**　新しい顧客獲得に向けたマーケティング活動や、新しい顧客取り込みは、マネーロンダリングの脅威の影響を直接受ける。
- **コンプライアンス**　上記同様重要なのが、マネーロンダリングは金融機関における法令遵守のプロセスにとっても脅威であるということだ。出納窓口や資金送金、小切手振出や決済プロセスに至るまであらゆるプロセスで脅威となる。
- **リスク管理**　マネーロンダリングは金融機関の債権評価や、疑いのある取引の報告、リスク管理などにとっても脅威となる。共通管理されているローンや犯罪者によって使用されている口座、または、監視システムが使用されているシステムを、適切に監視できていない時などは、特に大きな脅威となる。

先進欧米経済で確立された厳しい法規制を受けつつ、ありとあらゆる文化や法環境のもとで業務を行っている金融機関が直面する困難を考えよう。例えば、その金融機関は窓口の出納係に対して、金額や通貨、預金の頻度、預金者の情報、または取引の目的をどのように特定するかなどについて、しっかりとした研修を実施しなければならない。

その金融機関は、非協力的な個人に対して暴力や脅しを使う文化、利益を得るためには手段を選ばないといった文化、または汚職がはびこっている環境において業務を行っているかもしれない。また、その金融機関は、顧客と銀行の従業員の間に比較的大きな所得格差があるような地域で業務を行っているかもしれない。そういった状況下においては、贈答品や脅しといった手段を使って、取引の実施や承認、報告の役割を持つ銀行員を惑わし、金融機関を不適切に使用しようとする人間が出てくる。

マネーロンダリングは副次的な脅威ももたらす。法執行機関による罰則だけでなく、この犯罪は組織の評判を傷つけ、規制当局との関係にも悪影響を与える。その上、法令遵守や継続した経過監視、その他の業務プロセスの刷新等に伴う費用もかさむ。

最近では、新しい形態のマネーロンダリングの脅威が台頭している。それは、「架空」の通貨を使った代替支払ネットワークである。これらの取引は架空である一方で、世界中の金融機関で実際の預金として取り扱うことができる。そういった不適切な資金を特定することは、銀行の法令遵守や業務システムの観点からも新しい課題になっている。

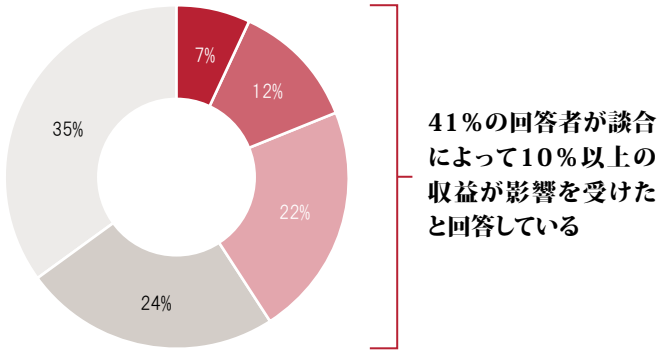
したがって、あらゆる業務プロセスに対してマネーロンダリングの脅威のある環境で業務をすることは、金融機関にとって特有の課題になっている。マネーロンダリングの形態が多様化し巧妙になっているだけでなく、利益を生み出す顧客を獲得しサービスを提供することと、さまざまな法を完全に遵守して業務を行う事という間にある種の緊張感を生み出すことにもつながる。

競争法／独占禁止法

競争法や独占禁止法の分野において、私たちの調査ではヨーロッパ地域に着目している。贈収賄や汚職、競争法違反、マネーロンダリングといった政府当局により規制されている主な三つの不正の分類のうち、西欧と東欧の回答者の4分の1が、競争法に抵触する行為が他の二つの分類よりもリスクが高いと回答している。また、これはアジア太平洋地域、アフリカ、北中南米アメリカなどの他の地域よりも高くなっている。

欧州委員会は、注目度の高いカルテル、価格協定、昨年報道されたLIBOR案件の他、市場操作に関連する案件に着目しており、EU諸国を拠点に活動をする企業にとって、その意識や業務に大きな影響を与えている。

図表16：談合による収益への影響



PwCドイツが行った2013年経済犯罪調査結果
談合によって影響を受けた収益の割合（%）

■ 30%以上 ■ 20-29% ■ 10-19% ■ 5-9% ■ 5%以下

上記を裏付ける情報が最近のPwCドイツによる経済犯罪調査で明らかになった。調査の中で、10人中約4人（41%）の回答者が、市場のひずみ（ここでは2社以上の企業の談合と定義）が原因で10%以上の収益が影響を受けているのではないか、と回答した[2]。

もう一つ同じドイツでの調査で分かったことは、10人のうち7人の回答者（71%）が、競争法に関するコンプライアンスプログラムをまだ導入していないということだ。しかしながら、既に腐敗防止プログラムを実施している企業の47%については、そのプログラムを応用して反競争法の対策にも使用している傾向が見受けられた。逆に、腐敗防止プログラムを実施していない企業については、競争法に関するコンプライアンスプログラムを導入している企業は、たったの9%にとどまった。

残念ながら、同調査によると両コンプライアンスプログラムには似た欠点があるようだ。例えばドイツでは、約2割の競争法に関するコンプライアンスプログラムには社員への研修が組み込まれていない。また約3割の組織では、同プログラムに通常含まれる取引業者、市場や業界のリスクを体系的に調査する仕組みが導入されていなかった。さらに内部監査（71%）や内部通報プログラム（67%）などの同プログラムにおいて重要な仕組みの強化の必要性も見受けられる。

[2]PwCドイツはドイツを拠点とする603企業を対象に過去2年の経験についての調査を行った。

10社中4社のドイツ企業が、談合によって10%以上の収益が影響を受けたと報告した。

これらの結果自体はドイツが対象であったが、傾向としては欧州全体の状況を表していると言える。また、ここで取り上げたリスクについては欧州の回答者によって共有されていたが、実際は欧州委員会の動きは世界中の企業に影響を与えることになる。

LIBOR スキャンダル

本調査実施の最中に、競争法に触れる大事件として、多数の銀行が共謀しロンドン銀行間取引金利（LIBOR）を操作していた疑惑が世間を騒がせていた。

LIBOR は何兆米ドルにものぼる有価証券、債券や他金融契約を支えている国際的に使われている利率のスタンダードである。その利率が世界規模の大手金融機関によって操作されたとの発覚後、欧州委員会がその規制当局として調査を始めた。

2012年に行われた世界規模の調査で、多数の大手金融機関の従業員が虚偽の利率を報告することによってLIBORを操作していた事実が発覚した。人為的に操られた利率で有利になる投資をすることによって、利益が生まれ、その結果、高い報酬も得ていたと思われる。また、人為的に低いLIBORを出すことによって、金融機関の安全性と安定性に対する市場の印象を良くしようとしていた可能性もある。

2014年1月時点で、米国、英国と欧州委員会は利率操作の罪で80億米ドル以上の罰金を科し、スイス、カナダと日本では調査が続いている。興味深いことに、各国の規制当局が不正に調査の重点を置く中、欧州委員会は違法カルテルによる競争法違反を中心に調査を進めていた。

業務プロセスのどこに問題があったのだろうか。何年にもわたって銀行同士で規制を免れ、競合であるはず銀行同士が共謀する環境の中、この事件はコンプライアンス、リスク管理および内部統制の重大な脆弱性を明らかにした。また、これによって世界各国の組織の主要な財務および資本機能が大きな影響を受けた。

多くの専門家は、LIBOR 事件をきっかけに、将来競争法違反の事案が発生した場合には、欧州委員会による調査はさらに厳しいものになるだろうと予想している。

規制当局による監視：今後の見通し

最後に、私たちは回答者に対して、この項で取り上げた三つの経済犯罪（贈収賄や汚職、マネーロンダリング、競争法違反や独占禁止法違反）についてリスク認識の観点から順位づけをしてもらった。

結果としては、半分以上の回答者（53%）が、贈収賄や汚職を世界中でビジネスを行う上で最もリスクが高い犯罪であると位置づけた。また、マネーロンダリングが22%、競争法違反や独占禁止法違反が21%でこれに続いた。

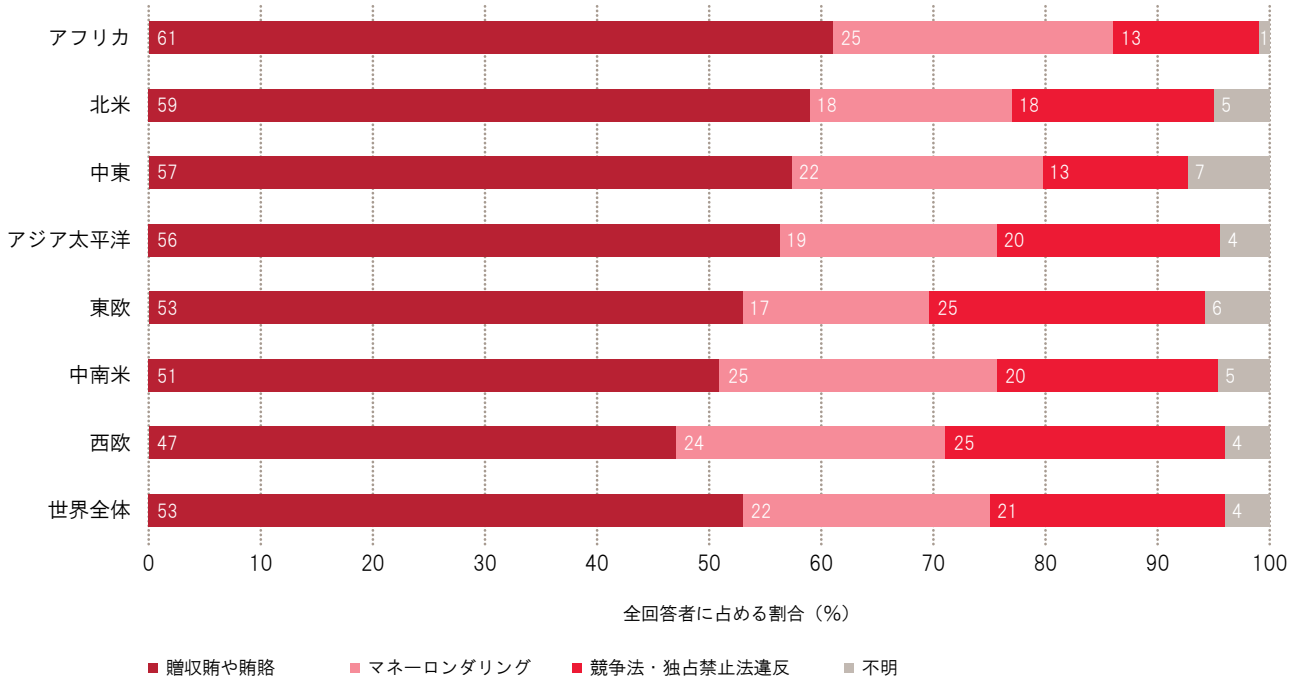
図表17：リスクが高いと認識されている経済犯罪

全回答者に占める割合（%）

図表18に示したとおり、どの地域においても、贈収賄や汚職が、上記の三つの分類の犯罪の中で相対的に最もリスクが高いという結果になった。

北米地域（59%）は、アフリカの61%と中東地域の57%の間で第2位につけているが、これはアメリカの回答者が、FCPAやその他の反汚職法を違反することによって被る甚大なコストを警戒してのことであると考えられる。

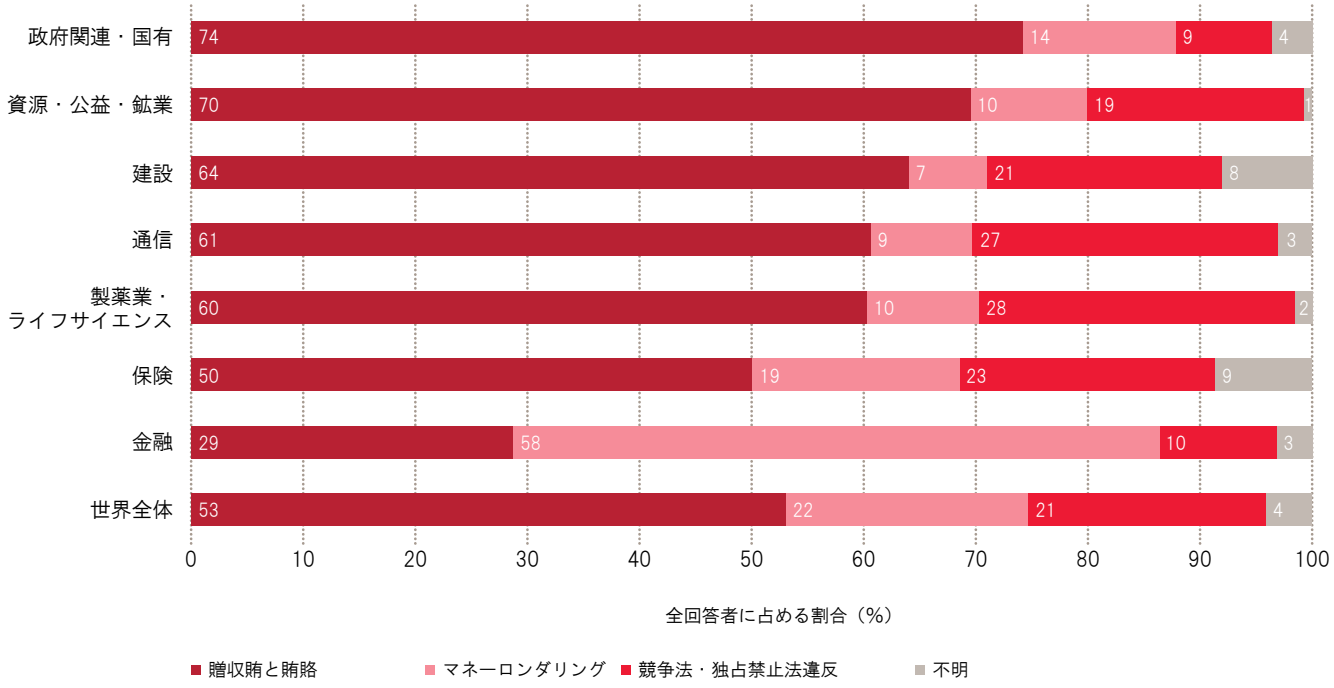
図表18：リスクが高いと認識されている経済犯罪（地域別）



産業／業界別に見ると、基本的には全体を含むほとんどの産業／業界において、贈収賄や汚職が世界中でビジネスをする上で同三つの経済犯罪の分類の中で最もリスクが高いと位置付けられている。しかしながら、金融業界（29％）だけは、前項で解説したとおり、マネーロンダリングを最もリスクが高いと位置づけている。

他の業界と比べると、政府関連組織や国有企業（74％）は贈収賄や汚職に関するリスクを相対的に最も高く認識しており、次いで資源・電力などの公益事業・鉱業（70％）、建設業等（64％）となっている。上記のような重厚長大産業ではないが、最近アジア地域で規制当局による摘発が見られたように、製薬業やライフサイエンスの業界も60％とかなり高い比率となった。

図表19：リスクが高いと認識されている経済犯罪（業種別）



テクノロジーの進化によるネットワークやデータへの容易なアクセスには、影の部分も存在しており、そこではずる賢く恐ろしい犯罪者が背後で暗躍している。

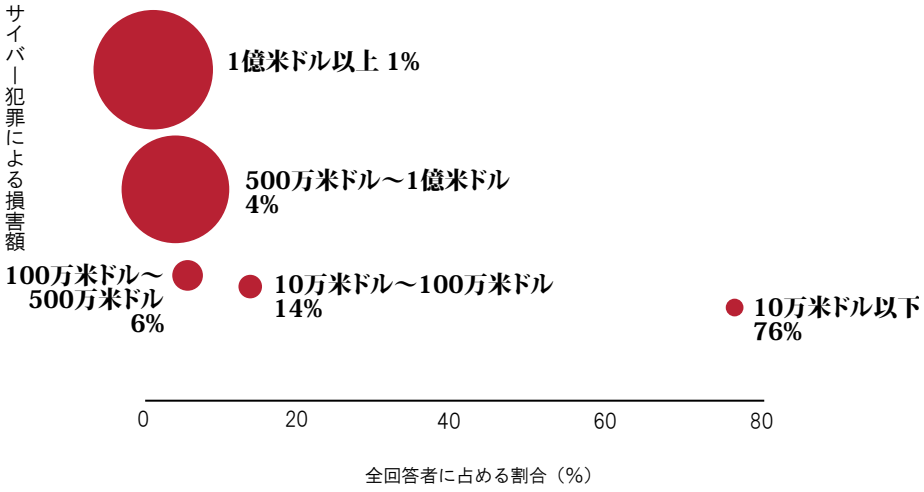
サイバー犯罪：
ネットワーク化された世界のリスク

ビジネスにおけるテクノロジーの進歩は、ソーシャルメディアやデータによる管理の著しい成長と相まって、これまでの企業と消費者の構図を根底から変えたと同時に、さまざまな場面での両者のつながりやすさを生み出した。

しかし残念なことに、こういったインターネットやサイバー上でのネットワークには影の部分も存在しており、そこではずる賢く恐ろしい犯罪者が私たちの見えないところで暗躍している。また、基本的にサイバー犯罪は人知れず行われるため、企業は自分たちが狙われていることに気付くこともなく、たとえ気が付いたとしても、損害を被ってから長い期間がたってから、ということになるかもしれない。

そのため、インターネットに関連するさまざまな手口の不正が、あらゆる経済犯罪の中でも最も危険なものの一つとなっている。

図表20：サイバー犯罪による財務的損失

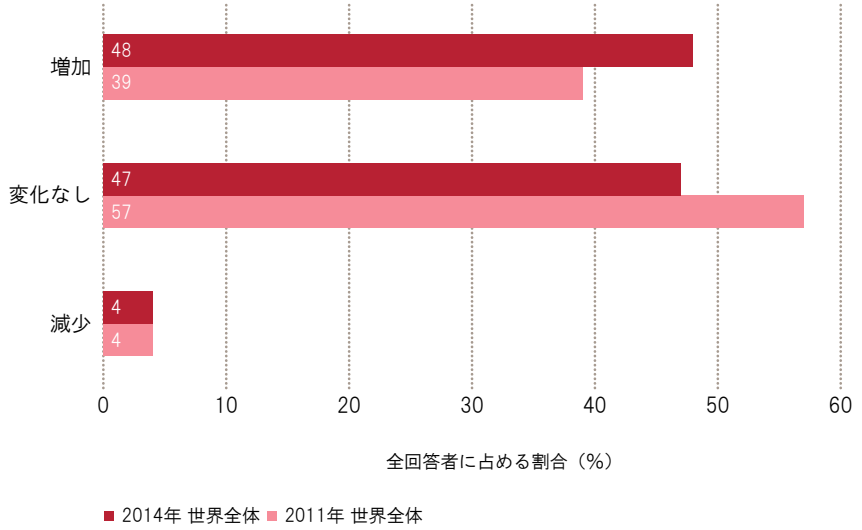


私たちの2011年調査で、初めてサイバー犯罪が企業にとって大きな脅威であることを取り上げた。本年度の調査においても、4人に1人の回答者がサイバー犯罪に巻き込まれたことがあると回答している。また、財務的な損失被害を受けたと答えた回答者の11％以上が100万米ドル以上の被害を受けており 、サイバー犯罪がビジネスへ与える深刻かつ継続的な影響が確認された。

組織がサイバー犯罪の脅威をより深刻に捉えている兆候として、私たちの調査によると、実際に報告された事例の増加よりもさらに速いペースでサイバー犯罪への意識が高まっているということが挙げられる。本年の調査でも、全回答者のうち48％が、自社内におけるサイバー犯罪のリスクへの意識は高まっていると回答している。2011年の同内容の調査結果は39％だった。

これを強調するかのように、私たちの最新の世界CEO意識調査では上記と同パーセント（48％）のCEOが、機密データの保護が不十分であると感じていたり、サイバー犯罪の脅威を懸念していた。

図表21：サイバー犯罪のリスクに対する認識



サイバー犯罪：目に見えない脅威

25％の回答者がサイバー犯罪に巻き込まれたことがあるという事実もさることながら、サイバー犯罪に実は巻き込まれていたかもしれないが、そのことに気付いていない人が大勢いることも忘れてはいけない。

多くの企業は自身のネットワークおよびそこにあるデータが侵害され、その際どのような資料が盗まれ、どのような損害を被ったかを把握していない。これがサイバー犯罪の脅威である。

さらに状況を複雑にしている要因として、サイバー犯罪の場合、たとえ事件が発覚しても、未報告のままにされてしまうことが多くあるということが挙げられる。個人情報漏えいのように報告が義務付けられている分野以外では、公表が義務付けられている分野はほとんどない。また、重要な知的財産の盗難のケースのように、他社との競争上の理由で、そのような事実を社外秘として取り扱わざるを得ない状況も多く存在する。

例えば、機密事項である入札計画の情報がサイバー犯罪者にアクセスされ、その情報が競合他社に有利に使用された場合、組織は公開するだろうか。企業はそのようなサイバー犯罪に対して十分な予防策をとれているのだろうか。また、もしそういった事実が発見された場合、どのようにして損失を計上するのだろうか。

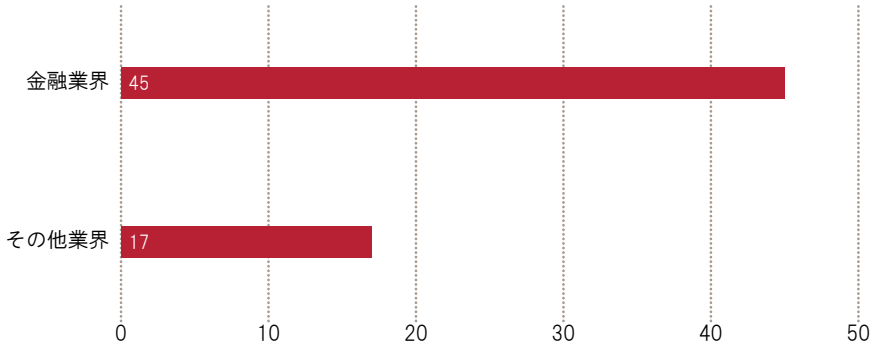
最も重要なことは、このように綿密に計画された攻撃による被害のほとんどが、人知れず行われたり、定量化することが困難であったり、共有されることがないため、公表されないことが多いのである。当然ながら、このような問題点は、テクノロジーや知的財産への依存が増加しており、また透明性が重要なグローバルビジネス環境において大きなリスクとなっている。

盗まれた重要な無形資産の価値を算出し、公表し、またそもそもその損失があったことに気付くこと自体よりも、実はそれを盗む方が簡単かもしれない状況というのは、非常に危険だと言えるだろう。

金融業界とサイバー犯罪

金融業界において、不正の被害にあった企業の45％がサイバー犯罪の被害にあっており、これは他業界の約3倍である。

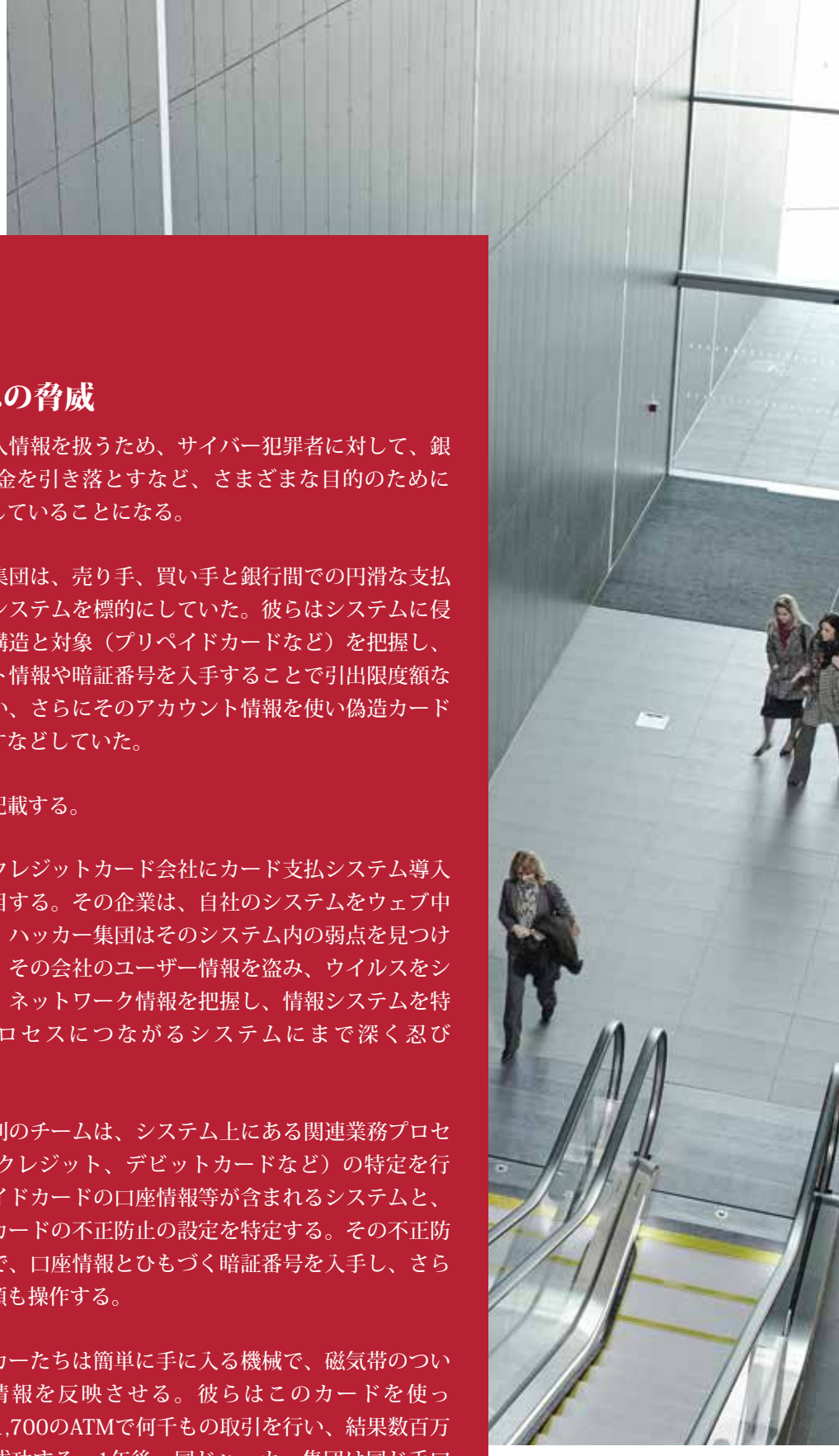
図表22：金融業界におけるサイバー犯罪



調査期間中に経済犯罪の被害にあったと回答した回答者に占める割合（％）

なぜ金融業界ではこれほどサイバー犯罪の被害が突出しているのか。さまざまな規制に準拠しなければならない大規模の金融機関は、システムやセキュリティが適切に構築されているため、ネットワーク侵害を発見できる環境にある可能性が高い。また、金融機関はそもそも現金を扱っているので狙われやすい業界だともいえる。

金融機関は、大量の顧客情報および財務情報をオンラインでやり取りするため、そのような情報にアクセスし、非合法の市場で売買を行おうとする、ツールやスキルを有するサイバー犯罪者にとって格好の標的となっている。



データの機密性への脅威

データ収集と保全は個人情報を扱うため、サイバー犯罪者に対して、銀行口座にアクセスして現金を引き落とすなど、さまざまな目的のためにデータを盗む機会を提供していることになる。

東欧で有名なハッカー集団は、売り手、買い手と銀行間での円滑な支払いを仲介するカード支払システムを標的にしていた。彼らはシステムに侵入することで、システム構造と対象（プリペイドカードなど）を把握し、そこに含まれるアカウント情報や暗証番号を入手することで引出限度額などの口座情報の操作を行い、さらにそのアカウント情報を使い偽造カードを発行して現金を引き出すなどしていた。

下記によくある手口を記載する。

ハッカー集団は銀行やクレジットカード会社にカード支払システム導入を提供している企業に着目する。その企業は、自社のシステムをウェブ中心で行っていることから、ハッカー集団はそのシステム内の弱点を見つける。その弱点につけ込み、その会社のユーザー情報を盗み、ウイルスをシステムに流す。その上で、ネットワーク情報を把握し、情報システムを特定することで、業務プロセスにつながるシステムにまで深く忍び込む。

次に、ハッカー集団の別のチームは、システム上にある関連業務プロセスや対象（プリペイド、クレジット、デビットカードなど）の特定を行う。彼らはまず、プリペイドカードの口座情報等が含まれるシステムと、その中で設定されているカードの不正防止の設定を特定する。その不正防止の設定を無効にした上で、口座情報とひもづく暗証番号を入手し、さらには口座の引き出し限度額も操作する。

その情報を元に、ハッカーたちは簡単に手に入る機械で、磁気帯のついた未使用カードに口座情報を反映させる。彼らはこのカードを使って、36時間の間に世界の1,700のATMで何千もの取引を行い、結果数百万米ドルを引き出すことに成功する。1年後、同じハッカー集団は同じ手口で、今度はより効率的に、実際に現金引き出しを行ういわゆる運び屋を雇って、12時間の間で数千万米ドルを引き出した。

動く標的

テクノロジーを取り巻く環境が変化する中で、ずる賢い犯罪者たちは新しい弱みを攻撃することでさらに進化を続ける。その被害を食い止めるためにも、各組織は少なくともその犯罪者たちの進化についていかなければならない。

たとえ企業が直面するさまざまなサイバー犯罪における脅威を一般的に認識していても、大半の人はサイバー犯罪者の能力や、彼らが何を標的にしようとしているか、またその標的にどれくらいの価値があるかを本当の意味では理解できていない。そうであるにもかかわらず、その実用性や利便性は非常に魅力的なため、企業は相変わらず重要なデータを経営陣、従業員、取引業者、また顧客に対して、リスクの高いモバイルやクラウドといったさまざまなプラットホームを通じて共有し続けている。

誰もがこの利便性が失われるとは思わず、また組織に蓄積されたデジタルデータがなくなるとは思わない一方、プラットホーム上のデータとアクセス数の増加により、重要なデータが危険にさらされていることは明らかであり、セキュリティ侵害によるコストは増える一方となっている。どの地域においても、4社に1社ないし3社に1社の企業が、自社が近い将来サイバー犯罪の被害に遭うであろうと確信していると回答している。

戦略的な問題であるサイバー犯罪対策

結論から言うと、サイバー犯罪はテクノロジーだけの問題ではない。企業の戦略に影響する問題であり、人間の問題であり、組織の問題である。

結局、企業はコンピューター自身に攻撃されているわけではなく、それを駆使した人間によって、ネットワークやシステムの弱点、また人間誰しもある弱みにつけこまれて攻撃されている。結果、テクノロジーの底上げだけでなく、企業戦略に見合った全体のプロセス、アクセス権限、委譲プロセス、管理と社内意識向上が必要となる。

このことは、これから挙げる四つの点が如実に表している。一つ目に、ハッカーはセキュリティの仕組みの中で最も脆弱（ぜいじゃく）とされる人間を標的にし、その無知につけこむ手段として、銀行など信用している発信源からの偽装メールを使って銀行情報などを取得しようとする「フィッシング詐欺」と呼ばれる手口などを使う。あるいは、最新のコンピューターを使い、データの暗号化を解除する、簡単なパスワードであれば自分たちで推測する、盗む、お金を払って違法にパスワードを入手するなどの手段がある。18カ月ごとにデータ暗号化の機密性は倍になるが、その一方で、人間が複雑なパスワードを書きとめずに覚えておける記憶力は1万年前からあまり変わっていない。

二つ目に、ハッカー集団はテクノロジー技術だけを強化しているわけではないということである。実際に起こった事件を元にした偽造カードの事例を上記で紹介したが、そこではハッカー集団が生産性や効率性を高めることで被害総額が前年の4倍近くに増えている。これは、ハッカー集団のテクノロジー技術が大幅に進化したことによるのではなく、いわゆる「運び屋」を雇い、人間をうまく組織化したことによるものである。

三つ目に、サイバー犯罪対策を行う上では、テクノロジー面以外の観点もしばしば必要になる。その例として、研修と社員の意識向上に加え、法務や情報保護の専門家との連携、メディア対応、危機管理と防止策の策定などがある。

最後に、データセキュリティにおいては、組織にとって最も重要なデータを守ることに主眼が置かれるべきである。自社ネットワーク内で適切にデータを管理できている組織は、どれが自社にとって重要な資産であるかということついて理解できている。そして、限られたサイバーセキュリティのための予算を賢く使うことができる。

したがって、サイバーセキュリティの本質を考える上で重要なことは、単に技術的なことを情報技術部門のスタッフが考えるのではなく、何をどう守るのかを経営陣が戦略的に考えなければいけないのである。確かに、情報技術部門は業務に必要なソフトウエアを始めとする技術をよく理解しているはずだが、そもそもそれを使って間違ったデータ資産を守ることに注力しているかもしれない。

テクノロジー重視のビジネスプロセスに潜むサイバー犯罪の脅威

さまざまなところでテクノロジーが使われている現在、サイバー犯罪はあらゆる業務にとって現実的な脅威となっている。当社の経験上多く見られるのは、金融資産へ直接アクセスできる情報を管理するシステムに侵入されるケースや、個人情報を入手し、そこから金融資産を盗まれるケースなどがある。

テクノロジーが活用されているビジネスプロセスで、特にサイバー犯罪に狙われやすい項目の例として下記が挙げられる。

- 一般的な販売で使われるデビットカードやクレジットカードの日々の販売時点情報（**POS**）
- 日々利用される**ATM**取引
- 顧客情報の保全および保護：これは身元、金銭状況、保険制度や健康状態といった膨大な個人情報を扱う保健医療業界では特に大切である。
- 電子商取引（**eコマース**）：基本的には上記のPOSと同様の課題があるが、電子商取引はオンライン上の取引であることが異なる。
- **Email**でのコミュニケーション：企業のメールシステムに外部のサイバー犯罪者が侵入し、ビジネスにおける重要な情報や、知的財産や経営陣間のやりとりなどが盗まれる危険がある。
- システム構造の脆弱（ぜいじゃく）性：例えば、比較的セキュリティの弱いWifiのアクセスポイントに侵入する、またはそのWifi環境でやりとりされる電子メールを傍受するといった手口がある。それ以外にも、プロバイダーによって管理されているサーバー環境に侵入し、いわゆるクラウド上の業務システムを攻撃するといった手口がある。
- 顧客への特典プログラム：ポイントプログラムなどの顧客への特典プログラムは顧客の個人情報および消費性向といった情報が含まれているため、個人情報の盗難に遭いやすく、さらなるサイバー犯罪の標的にされる。
- **M&A**：多くの企業において、合併や買収完了後、情報セキュリティに関しての方針、システムなどの統合が先延ばしにされるケースが散見される。ハッカー集団はこの状況を利用する。例えば、重要な知財情報やそれ以外の重要データを含む、M&A以前に使用されていた過去のシステムに侵入するなどの手口を利用する。
- サプライチェーン・仕入れ先、受託業者や販売業者は企業全体の一部と見なしてもよく、多くの場合、自社へのシステムや重要な情報などにもアクセス権限をもつ。そういった外部の業者のリスクは自社へのリスクでもあり、サプライチェーン上の不備はそのままネットワークセキュリティに影響を与えることになる。最悪の場合、重要情報にアクセスされてしまうことも考えられる。
- 研究開発：独占所有権のある技術、競合情報および知的財産は国家や国営企業、非倫理的な組織に狙われている。ハッカーによる侵入や、知的財産に精通する内部関係者による競合他社への情報横流しなどにより、企業は何十億米ドルという損害を被っている。
- 新しい市場への進出：企業が新しい地域に進出することにより、企業の技術、顧客リストまたはマーケティング計画などが進出国の政府や現地競合他社に狙われる可能性がある。他国での事業であるがゆえに、内部関係者の不祥事は社員にとどまらず、設備業者、人材派遣業者、清掃業者や政府や地方自治体の関係者にまで範囲は及ぶ。

約5分の3の回答者が、購買に関する不正が業者の選定過程で発生したと回答し、また約半分が、公開入札への申し込みの過程で不正が発生したと回答した。

その他、影響が大きい経済犯罪
購買に関する不正：増加する脅威

先に述べたとおり、今回私たちの報告書では購買に関する不正という新しい分類を追加したが、29%の回答者がこの分類の不正があったと回答した。

一般的に、組織が公開入札に関わる過程や、自社のために製品やサービスを調達しようとする過程において購買に関する不正は起こり得るが、その過程はあらゆる産業において共通するものである。この種の不正を考える上で、押さえておきたいポイントが三つ挙げられる。

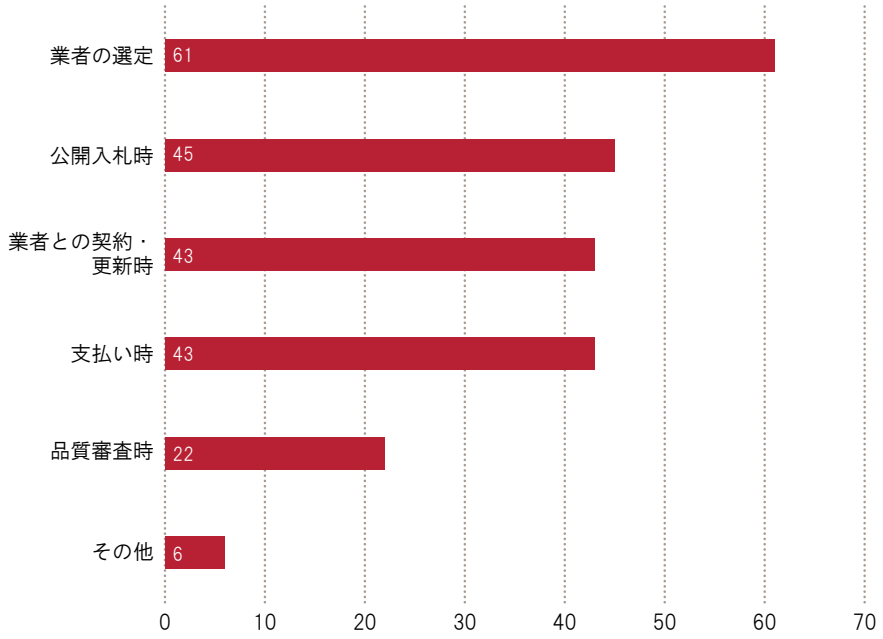
一つ目に、政府や国有企業によって、より競争が激しい公開入札が実施される頻度が高くなっており、代理人やその他の第三者による不正行為が行われる可能性を大きくしているということである。当然のことながら、過去の調査においては、購買過程でのキックバックや談合およびそれに準ずる不正は汚職としてこれまで報告がなされていた。しかし、購買に関する不正が主にどの過程で発生したかという調査によって、その状況は明らかになった（図表23）。約5分の3の回答者が、購買に関する不正が業者の選定過程で発生したと回答し、また約半分が、公開入札への申し込みの過程で不正が発生したと回答した。

二つ目に、2014年世界CEO意識調査でも取り上げたとおり、大多数の企業が世界全体の潮流に対応するように、自社のサプライチェーンの改革に取り組んでいるといったことが挙げられる。多くの企業が各サプライチェーンにおける相互関係を強化し、全世界にまたがったサプライチェーンを構築しようとしている。そういった中で、供給業者（サプライヤー）はより一層組織の日々の経営の中に組み込まれているため、通常業務が遮断され、財務的な損失を被る脅威が高まっている。

三つ目に、経済環境が近年の経済危機から回復基調にある中で、企業内の雇用慣習に変化が見られる点が挙げられる。短期的な観点では、これまでは終身雇用であった社内の従業員が担っていた仕事を、代替可能で調整しやすい外部の労働力に置き換える傾向が続いている。

これらの回答を見ると、購買に関する不正には二つの脅威があると考える。自社で製品やサービスの調達を行う際に不正に巻き込まれる脅威と、公開入札の過程で公平に正しく競争が行われない脅威が存在していると言えるだろう。

図表23：購買に関する不正が発生した業務プロセス



「購買に関する不正を調査し摘発するのは国家主権レベルだけではない」ということを追記しておこう。近年では、世界銀行（国際復興開発銀行）が不正全般に対してより積極的な姿勢をとっており、2012年には79のケースが確認されている。世界銀行のような国際機関は概して発展途上国におけるインフラなどの経済基盤の構築に対して出資していることが多いため、購買や調達過程に対しては特段の注意を払っている。世界銀行を敵に回すことは、多くの制裁措置を受け、将来の契約を拒否され、また他の国際機関からも締め出されることにもつながる。

購買に関する不正の業界別・地域別の傾向

予想どおり、購買に関する不正が目立つ業界は、政府関連組織や国有企業（46%）資源、電力などの公益事業や鉱業（43%）、建設業等（42%）、運輸や物流（39%）など、入札過程などの業務上重要な部分を、政府や政府関機、元請業者などとの緊密な連携に依存している業界である。

贈収賄や汚職、マネーロンダリングなどの経済犯罪のように、購買に関する不正は自社の従業員の品位をむしばむ。なぜならば、従業員を利益の実現とコンプライアンス遵守という二つの果たすべき目標のはざまに立たせているからである。

地域別の分析では、アフリカ（43%）や中東（33%）のように大きな政府機関、重要な資源や鉱業、建設業、インフラ需要の大きい地域で購買に関する不正が起こりやすいという結果が出ている。前段で述べた業界がリスクの高い業界であることは、この地域別の分析からも明らかである。

購買プロセスに対する脅威

これまでの私たちの議論は入札過程や外部の第三者についての内容が中心であったが、内部に潜む脅威についても看過することはできない。私たちの経験では、物品の調達は不正のリスクが高い領域である。特にリスクが高い企業文化としては、家族や同僚、所属する地域社会や国家への忠誠心の影響が大きいような文化が挙げられる。そういった文化は、会社の方針や、法的な条文に即した行動規範などを定めるような文化よりも、おそらくリスクが高いといえる。

購買や販売の部署に所属する個人が、その個人が属する組織との契約を勝ち取りたいと考える業者と、個人的な関係を築いているかもしれない。その個人は、その懇意にしている業者が有利になるように、競合他社の入札金額などの入札過程の情報をその業者に渡すこともあるかもしれない。または、その個人は業者からの購入価格を必要以上に高くして承認をするかもしれない。

そして、会社に適切な統制があったとしてもそれが機能しないかもしれない。私たちはこれまで、いわゆる「上司」からのプレッシャーに嫌々従い、定められた方針や手続きに違反して支払いを承認し手続きを進めてしまう、といった事例を数えきれないほど見てきた。経営陣の会社に対する忠誠心と、現地社会との絆の間に存在する葛藤は、企業の内部統制にとって脅威であり続けるのである。

会計不正

会計不正は私たちの調査において報告されている主な犯罪の一つであり、2005年以降、経済犯罪の被害にあったことがあると回答した回答者の20%以上が会計不正を経験したと回答している。今年も前年同様、22%の回答者が会計不正の被害にあったと回答している。

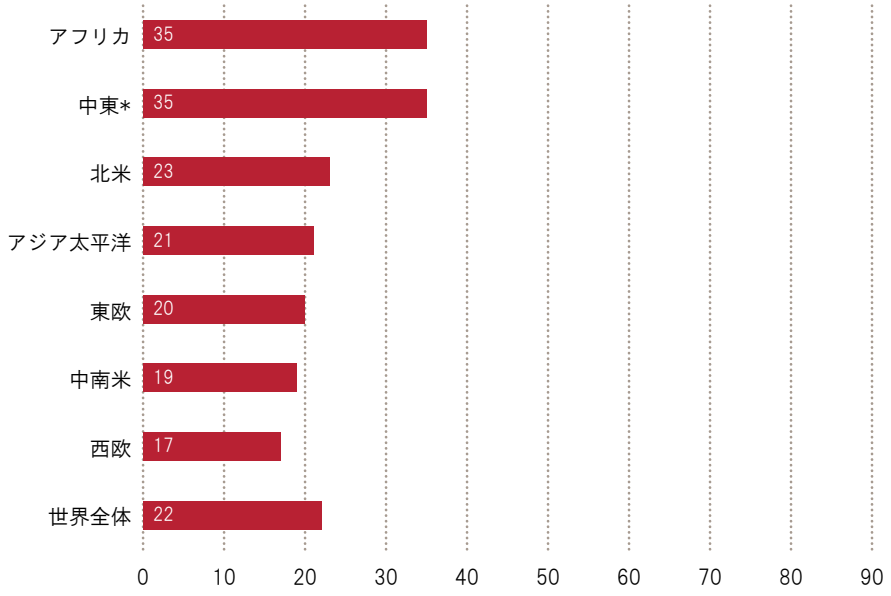
財務諸表はビジネスにおける基本的な指標であり、以前から与信判断、契約獲得、株式市場での資金調達などのための基本的な分析資料であった。会計不正は、誤解を招くような記載や虚偽の表示によって、銀行、債権者、業者、投資家などにリスクが高い間違った判断をさせることになる。財務諸表や業務における財務データの汎用性を考えると、会計不正がビジネスに与える影響は大変大きいものになる。

海外での上場

最近では会計不正は、さまざまな外資系企業が米国ナスダック、香港、シンガポールなどの株式市場に上場している中、誤解を招くような記載や虚偽の財務諸表を公表するといったことで注目されてきた。投資家に対して損失を与えるだけでなく、その後規制当局によって一連の調査が行われたり、各対象会社や監査人に対してどの規制当局が責任を持つかについて、中国と米国の間で長期間にわたる議論がなされているのである。

中東やアフリカでは特に会計不正に関する報告が多くなっており、全世界平均の22%を大きく超えて3分の1以上の割合である。また、アジア太平洋地域や北米地域の回答については、全世界平均の22%に近いものであった。昨今では、多くのビジネスや未公開株式投資ファンドが新興市場経済に対して投資を行っており、この状況は、先進国から新興国への富の移動の大きな流れを反映していると言える。

図表24：地域別の会計不正の報告



*中東は2011年調査では「アジア太平洋」地域に含まれていた

業界別の観点で見ると、会計不正の事象が平均以上の頻度で報告されている業界は、建設関連業界（39%）と運輸・物流業界（31%）であった。

この業界別の結果の背後にある理由の一つとして、贈収賄や汚職が挙げられる。賄賂やそれに準ずる支払いは、たいてい適切に財務諸表に記録されていないため、汚職に関する不正は同時に会計不正でもありうる。さらに、建設関連のプロジェクトでは収益計上の際にしばしば複雑な会計処理を行うため、不正行為が行われる可能性をはらんでいると言える。

不正会計（続き）

合弁事業

投資を考える個人・企業にとって、合弁事業の形態はよくとられる市場参入方法である。合弁事業が適切に管理されているかどうかは、財務情報が正確であるかどうかによるといっても過言ではない。

例えば、欧米の会社が新興市場の会社と合弁事業を立ち上げた場合を考えてみよう。通常、欧米側の企業は財務的なパートナーとなり、新興市場側の企業は事業のオペレーターとしてその合弁事業の人・モノの整備に責任を持つことになるケースが多い。そういった状況下の多くの場合、月次の会計報告は海外の事業パートナーに対してビジネスの進捗を報告する手段となる。もし問題が見つかった場合、その問題の報告を遅らせたり、そうでなければ、その問題を報告せずに財務諸表を改ざんすることで、隠蔽（いんぺい）を図ることもあるかもしれない。

こういった不正のパターンの背後には、より深刻な状況が潜んでいることが多い。例えば、欧米側のパートナー企業の出資金を使って、合弁事業で保有する工場と競合する工場を勝手に設立したり、発生するコストを自身が管理する他の事業部に不当に配分していたり、さまざまな不正の手口でその合弁事業を台無しにしてしまうケースが考えられる。

資産の横領

資産の横領はもっとも発生率の高い経済犯罪で、調査では回答者の69％が経験していると回答している。この回答率は同質問の2位の購買に関する不正（29％）の2倍以上の回答率である。資産の横領の個々の被害は、サイバー犯罪や政府当局によって取り締まりが行われる不正と比べれば、金額こそ低いものの、その脅威の影響を考えると注意する必要がある。

欧米では、資産の横領を婉曲（えんきょく）的に表現する方法として、英語で、「falling off the back of the truck」という表現が使われている。これは、ビジネスプロセスの中で重要な位置づけである、企業の運輸、物流、倉庫等が狙われ資産の横領の被害にあうということを比喩的に表している。

例えば、全世界で小売業を展開する企業の倉庫の在庫を考えてみよう。在庫は企業の従業員だけでなく、多くの外部業者にもその管理販売業務が委託されており、その供給プロセスや販売プロセスにある種の脆弱（ぜいじゃく）性がもたらされることになる。脆弱（ぜいじゃく）性をついて、例えば、従業員が在庫を無断で倉庫から持ち出したり、一般在庫を意図的に勝手に廃棄処分扱いにし、市場に横流しするなどの不正が起こり得る。

一般的に、資産の横領によって脅かされるもう一つの業務プロセスとしては、経費精算のプロセスが挙げられる。この場合、特に現金支出について大きな影響があるが、副次的な影響として帳簿が適切に管理されないという影響もある。

知的財産の侵害 – 重要な資産が脅威にさらされている

知的財産権の侵害は、しばしば大きな被害をもたらす経済犯罪であり、経営者にとっても大きな関心事となっている。直近の世界CEO意識調査のよると、43％の回答者が自社の知的財産を保護できているかどうか心配であると回答している。

本報告書のサイバー犯罪の項で、組織は、サイバーセキュリティについて単にネットワーク環境を守るということではなく、自社が持つ情報などの資産そのものを守ることに注力すべきだ、ということを述べた。業界によっては、知的財産が、会社が市場を制するために必要な、まさにその守るべき資産である場合もある。

回答者の18％が、今後24カ月の間に知的財産に関する経済犯罪の被害にあうと思うと回答しており、これは本調査期間に実際に報告された比率8％の2倍以上となっている。

上記の認識の差は、この知的財産権に関する経済犯罪においてよく見られる傾向である。また、資産への攻撃や窃盗といった犯罪が成功するということは、つまりそれらの犯罪が見つからなかったということに他ならない。回答者たちが懸念しているのは、知的財産が例え脅かされていたとしても、自分たちの統制ではその攻撃を見つけられないのでは、ということなのである。

全体の平均では56％が組織内の人物による犯行で、40％が組織外の人物によるものという結果だったが、金融業界においては、59％が組織外の人物が主犯であったと報告し、ほぼ正反対という興味深い結果がでた。

不正行為者の特徴

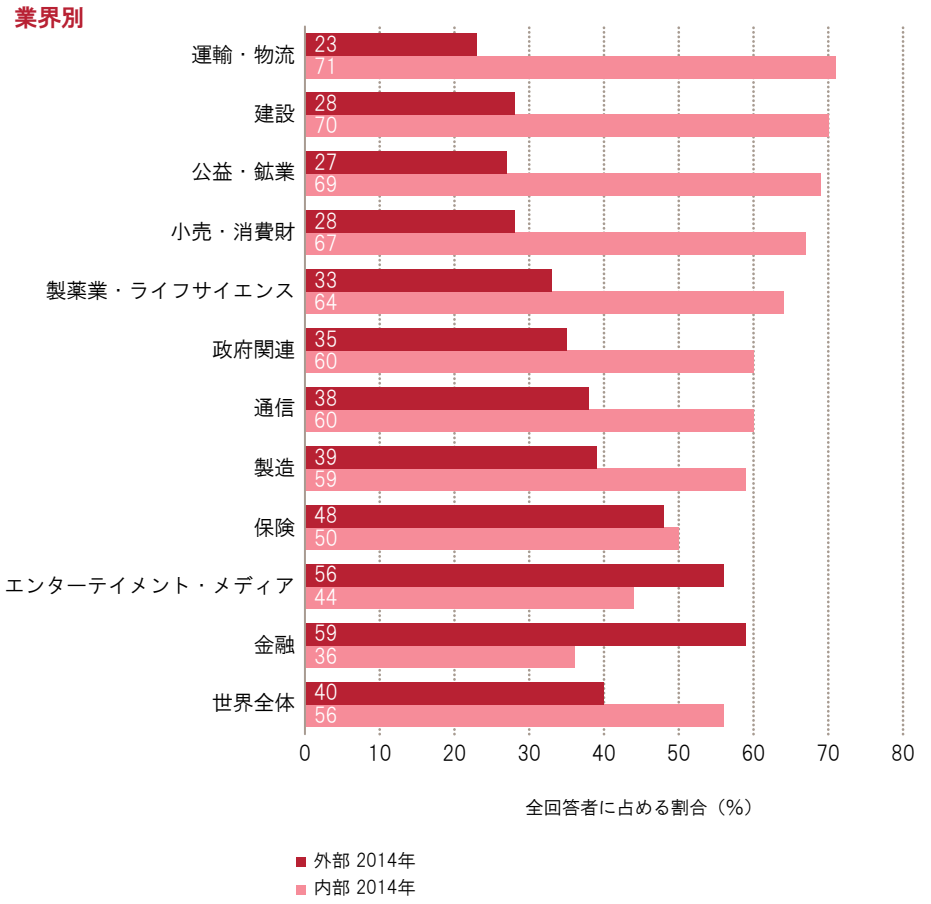
私たちの調査では、経済犯罪被害にあった組織に属する回答者に対し、彼らが直面した最も深刻な不正行為の主犯が、外部の人物であったか内部の人物であったかについても調べた。結果は過年度の結果と似たようなものとなり、56％が主犯は組織内の人物だと回答し、40％が外部の人物であると報告した。

しかしながら、もう少し分析を進めてみると、業種によって傾向が異なることが明らかになってきた。

前述のとおり、全体の平均では56％が組織内の人物による犯行で、40％が組織外の人物によるものという結果だったのが、図表25にあるように金融業界においては、59％が組織外の人物が主犯であったと報告し、ほぼ正反対という興味深い結果がでた。しかも、この傾向は2011年の調査においても同様であった。これは、金融業界がサイバー犯罪の標的となる確率が偏って高いということもあり（全体平均が17％のところ45％）、またサイバー犯罪が基本的には組織外の人物による犯行となる傾向があるということに起因しているかもしれない。

しかしながら、もう少し分析を進めてみると、業種によって傾向が異なることが明らかになってきた。

図表25：不正行為者（内部または外部）



一方、これとは逆の傾向が顕著にみられる業界もあった。例えば建設業では70%、資源、電力などの公益事業、鉱業では69%が組織内の人物による犯行であると報告している。本報告書内でも既に触れたように、贈収賄や汚職および購買に関する不正の説明の際にもこれらの業界区分が登場していた。それらの結果を踏まえると、下記2点を示唆しているのではないであろうか。まずは、これら重厚長大産業に属する組織はそもそもこれらの類いの不正に巻き込まれやすいということ、そして、組織内の人物に常に目を配っていることが、不正に巻き込まれるリスクを少しでも下げる上で重要であるということである。

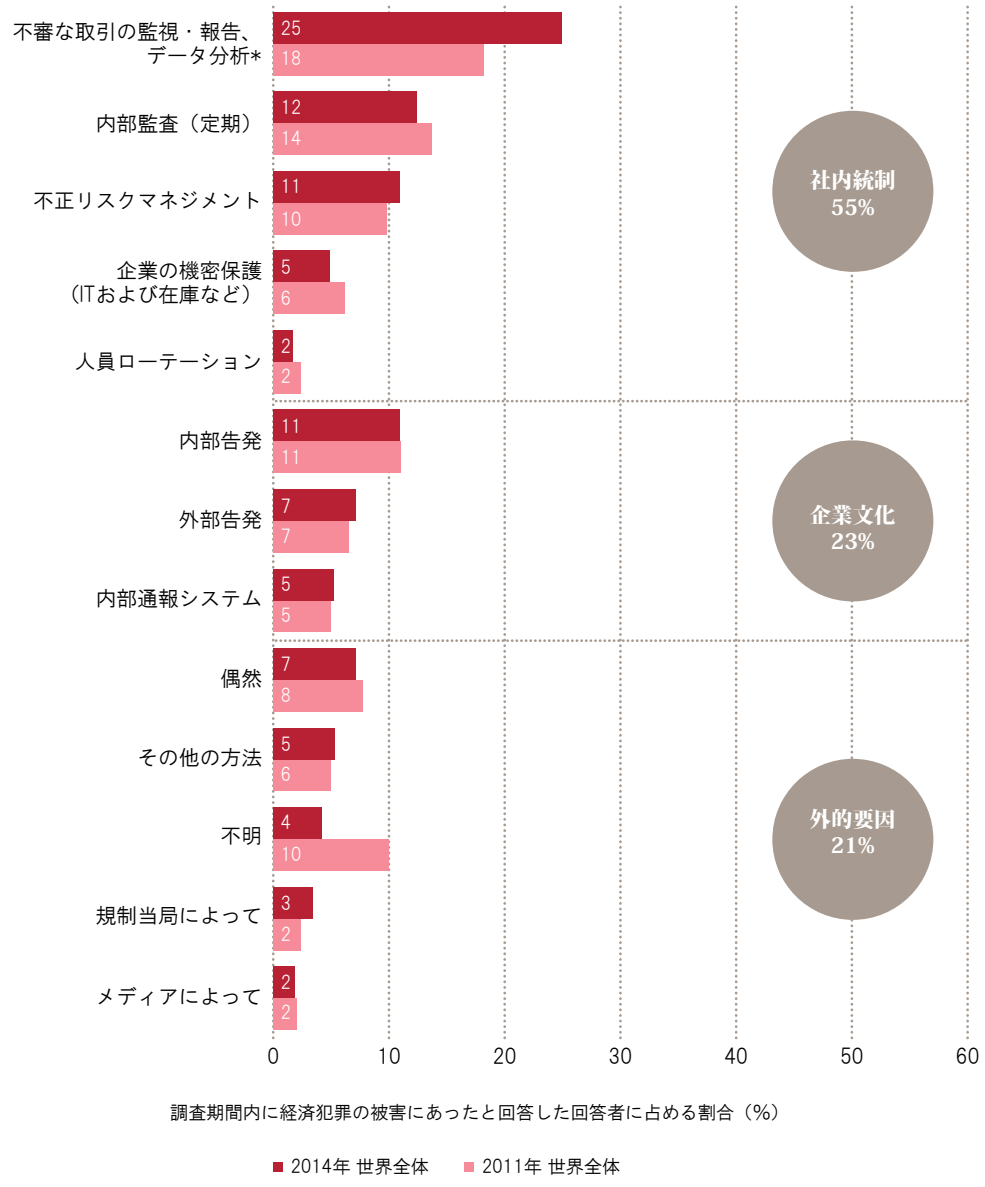
ほとんどの不正による損害が組織内の人物によってもたらされる状況の中で幸いなのは、どのような人物が不正を犯したかをいくらかは把握できるということであり、社内の方針、業務プロセス、統制などの改善によって、これらのリスクを軽減できる可能性があるということである。これは、組織外の人物の場合、いつもこのような可能性がある訳ではない。

不正を発見するために

それでは、どのように経済犯罪を未然に防ぐ、もしくは食い止めることができるのであろうか。

不正の発見の方法は大きく分けて次の3種類に分類できる。それは①社内統制②企業文化③外的な要因である。図表26は、どのような方法で大規模な社内不正が発見されたかを示している。回答者の報告によると、本年度の結果では、不審な取引の監視・報告とデータ分析による不正発見が18%から25%に上昇している。

図表26：重大な経済犯罪が発覚した要因



*データ分析は2014年の調査から追加された

図表27：経済犯罪が発覚した要因

	2005年		2007年		2009年		2011年		2014年	
社内統制	36	67	34	77	46	80	50	73	55	78
社内文化	31		43		34		23		23	
外的要因	33		23		20		28		21	

経済犯罪がどのようにして発覚したか、過去の調査結果の割合（%）

データ分析の主流化

近年、データ分析や不審な取引のモニタリングによる不正事件の発覚が急増しているが、具体的にはどういったことを行っているのかを下記に示した。

データ分析は体系的にデータを収集し、分析できる形式にした上で、データを標準化する手順から始まる。現代の技術を使えば、さまざまな種類の膨大なデータを効率的に分析することで、組織内に存在するデータへの理解も深まり、結果として潜在的なリスクを浮き彫りにすることもできる。

効果的な分析プログラムは、調査のために必要なさまざまな取引や取引の相手先を、そのリスクに応じて分類することができる。また中には、リスクの高い取引先との隠れた関係性を浮き彫りにする場合もある。さらには、統計的な手法や、キーワード検索、異常値に着目した分析などを用いることで、不審な取引の傾向を識別することもできる。

反汚職、不正予防のためのデータ分析は常に進化、改善を続けている。企業もまたこれまでに得られた知見や過去の調査経験を生かすことで、より体系的なデータ分析を行うとともに、分析による発見事項を最大限活用することができる。

今後これらの事例が、データ分析を利用する上で、より多くの企業の不正の防止や発見に役立つと予想される。

もう一つの心強い兆候として、私たちの2011年調査の結果と比べ、「どのようにして不正が発覚したのか分からない」と回答した人数が減少したということである。どのようにして不正が発覚したか原因を把握できることで、より効果的な社内プロセスの策定にも寄与するためである。

内部通報

駅などでよく良く耳にする「不審物などを見かけた際はお近くの駅係員にお知らせください」といったフレーズのように、周りに注意を呼びかけて潜在的な目撃者の数を増やすことで、犯罪を予防し発見することにつながる。これと同様の考え方で、内部通報システムも不正発見のための一つのツールとして効果的である。多くの国々では内部通報の重要性を理解し、内部通報者を報復などから保護するプログラムを導入している、または導入を検討している。

同時に、私たちの調査では興味深い対照的な回答もあった。10社中6社が内部通報の仕組みを導入しており、かつその約半数がその仕組みを効果的または大変効果的と回答しているにも関わらず、内部通報の仕組み自体が実際に不正発見につながったと答えた企業はたった5％だった。

この結果はいくつかの点を示唆している。まず、高いレベルの内部通報の仕組みを持つことは、不正発見のための当面の企業努力として必要かもしれないが、それだけで全てが解決するわけではないということである。企業を不正から守るためには不正を見逃さない社内風土の醸成と適切な内部統制の構築が必要である。

次に、内部通報があまり活用されない理由として考えられるのは、効果的な内部統制や不審な取引の分析などの不正発見・防止手法が構築されているため、従業員が内部通報する前にそういった手法により不正が摘発される、ということである。他に考えられる理由としては、通報者が通報することで自分が不利な立場に置かれるのを恐れて通報しないという場合である。

また、内部通報についての慣習は国によってさまざまである。例えばインドでは約5社中4社は内部通報の仕組みを導入しており、最近になって政府機関での不正の告発を促すために設立した不正に関する相談窓口の回線には、何千もの問い合わせが殺到し、処理が大変であったという事例もある。

組織内の不正-日常の中に潜む脅威

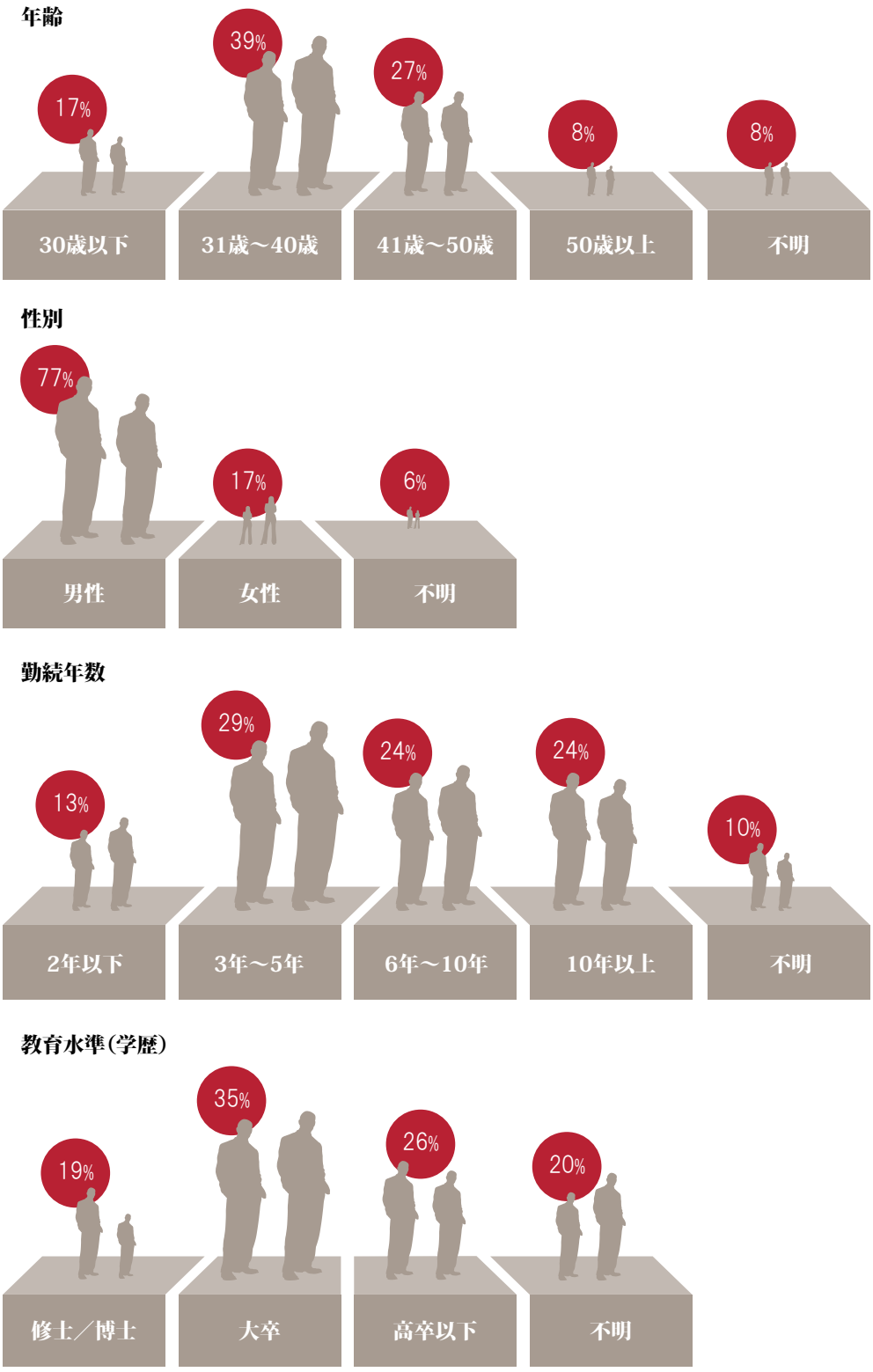
専門家はよく「不正のトライアングル」を引用する。これは犯人が不正を犯す際に引き金となる三つの要素のことをいい、「動機」、「機会」、そして「正当化」の3点から成り立っている。

約4人中3人（73％）の回答者が、組織内の人物による不正行為を考える上で、その「機会」もしくは「能力」という要素が最も重要であると回答している。3要素の中で「機会」というのは、組織が最もコントロールできる要素であるということを頭に入れておくことが重要である。これは、たとえ普段の生活のプレッシャーによる動機や、行動の正当化というものが従業員の頭の中に巡ったとしても、もし組織がその機会を制限することができれば、不正を未然に防ぐことができるかもしれないということである。

図表28にあるように、私たちは組織内で不正を行った人物の特徴について調査をした。結果、組織内で不正を犯した人物の全体的な特徴は2011年の調査結果と同じで、大学以上の教育を受け、勤続年数が3年から10年の中年男性となった。また、世界の全体平均では、約半数の不正は勤務年数が6年以上の従業員によって行われ、約3人に1人（29％）は3年から5年の勤務年数の従業員によって行われていた。

しかしながら、地域ごとの結果に着目すると、さまざまな傾向が見られた。例えばイギリスでは、組織内で不正を犯した人物のうち、前回の調査の2倍にあたる約4人に1人が女性との回答であった。

図表28：年齢、性別、勤続年数と教育水準（学歴）



経済犯罪の主要な犯行者が内部の人物だったと回答した回答者に占める割合（%）

● 2014年 世界全体

経営陣と不正の被害

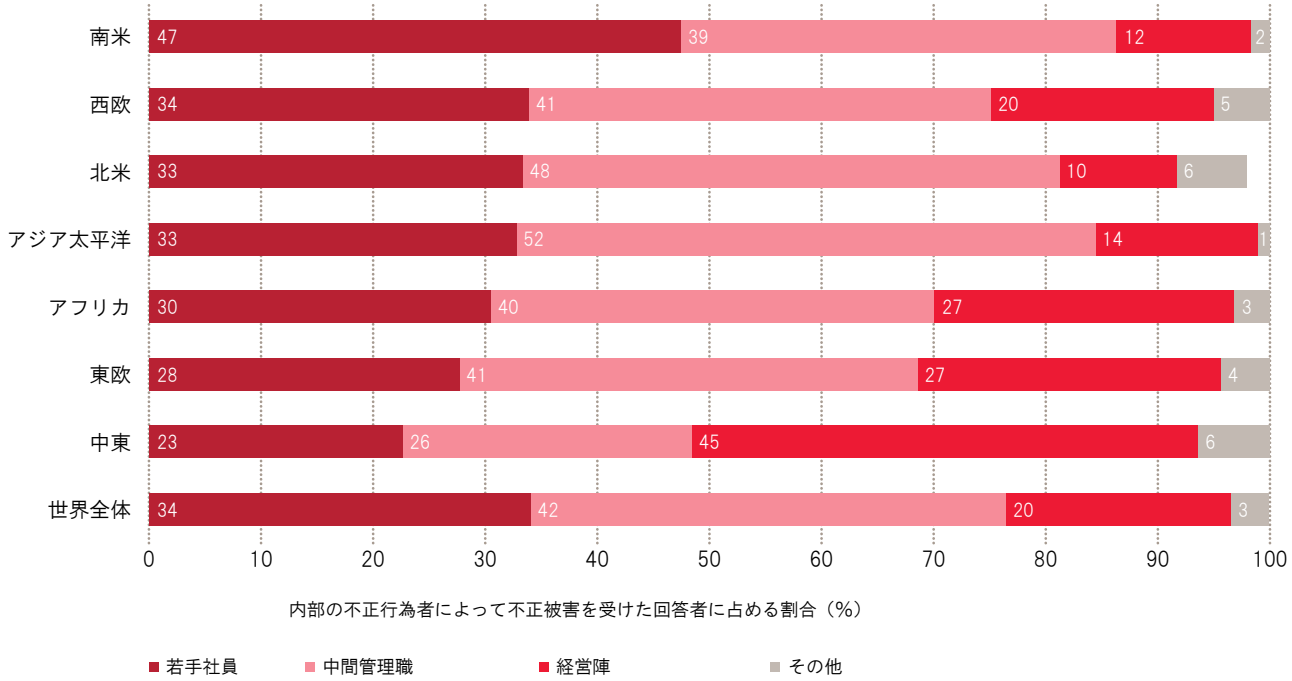
私たちの経験上、組織内の不正においてはその犯人の年齢および勤続年数が比較的大きな影響を持っている。その理由としては、勤続年数が長い管理職は、比較的社内でも大きな権限を持っているため、内部統制で定められていない例外事項をも認めさせてしまう傾向があるからである。

例えば、本来であれば銀行において送金担当者が担当をするところを、古株の銀行員がその担当者に、自分が直接支払いに関する顧客対応をする旨を言い出す。または、上司が支払いを裏付ける証憑を直々にまとめると提案する。もしくは、支店長が自分で資金を横領するために予算を水増し、偽の請求書を使い、金庫の中から金を盗み取る、などのケースがある。

これらの事例は、アジア、北米と欧州で実際にあった事件であり、経営陣や責任者が持つ権限が特別であることを改めて認識させられる。彼らは内部統制における管理者であるがゆえに、他従業員が持つことができない権限を持つ。また、彼らは企業風土を醸成する張本人でもある。従って、そのような立場の人物によって行われる不正や犯罪によってもたらされる損害は単なる財務的損害に留まらず、甚大なものになるかもしれない。

不正行為者についての詳細は、付記の「不正行為者の特徴の詳細」参照

図表29：内部の不正行為者の職位（地域別）



2014年経済犯罪実態調査では95カ国以上から5,128の回答を得た。

付記
地域・業界詳細データ

2014年経済犯罪実態調査では95カ国以上から5,128人の回答を頂いた。回答者には過去2年間で経済犯罪に巻き込まれた経験の有無を回答してもらった。図表30は、経済犯罪に関する報告が相対的に多かった地域について挙げている。

図表30：経済犯罪の報告の割合が高い国々

国名	経済犯罪報告 2014年	経済犯罪報告 2011年
南アフリカ	69%	60%
ウクライナ	63%	36%
ロシア	60%	37%
オーストラリア	57%	47%
パプアニューギニア	57%	NA
フランス	55%	46%
ケニア	52%	66%
アルゼンチン	51%	45%
スペイン	51%	47%
世界全体	**37%**	**34%**

上記図表で見受けられるように、発展途上国での回答は増加傾向にある。先進国の中にも上位に位置している国もあり、この場合にはおそらく、その国がむしろ不正行為を発見する体制が整っているとも言えるであろう。

図表31：経済犯罪報告の割合が低い国々

国名	経済犯罪報告 2014年	経済犯罪報告 2011年
マレーシア	24%	44%
イタリア	23%	17%
トルコ	21%	20%
ペルー	20%	35%
香港・マカオ*	16%	NA
日本	15%	5%
ポルトガル	12%	NA
デンマーク	12%	29%
サウジアラビア**	11%	NA
世界全体	**37%**	**34%**

*2011年調査では中国の一部として報告されていた　** 2011年調査では中東の一部として報告されていた

逆に比率が低い場合にもその理由として多くのことが考えられる。例えば、「回答者が不正の被害にあったことを申告すること自体に消極的である、資産の横領（最も頻繁に発生する不正分類）の事例が少ないまたは不十分な内部統制体制のためそもそも不正が発見されなかった」などの理由が挙げられる。

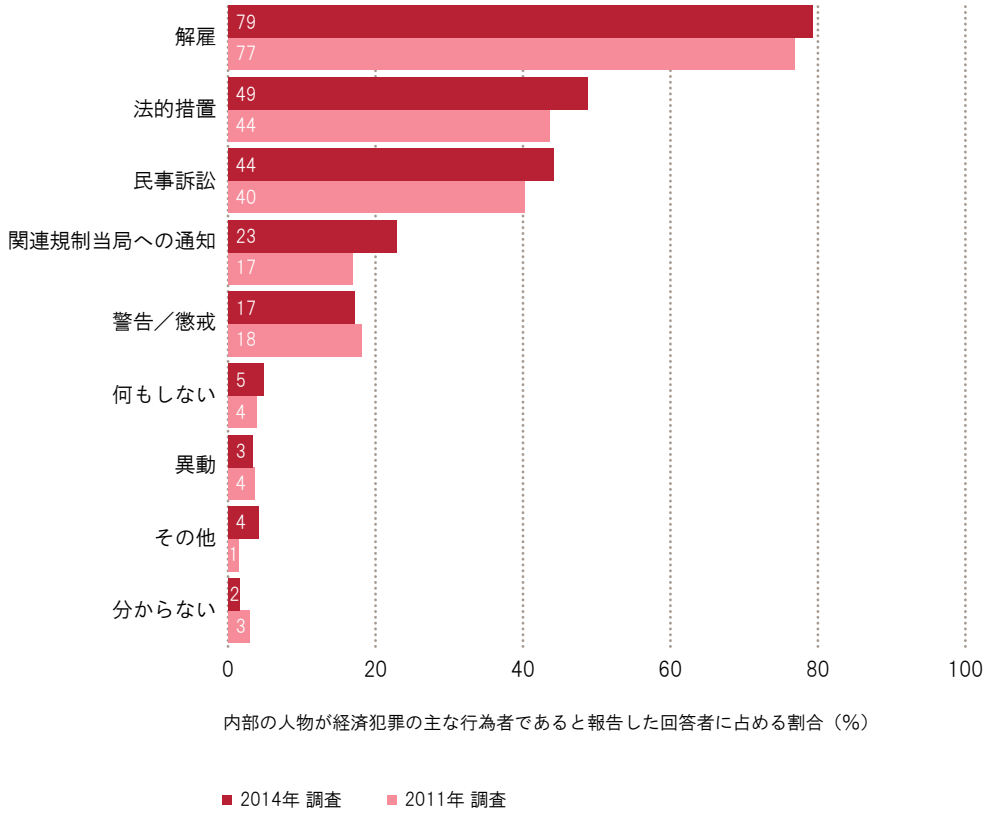
図表32：主要新興8カ国の経済犯罪報告状況

国名	経済犯罪報告 2014年	経済犯罪報告 2011年
ブラジル	27%	33%
ロシア	60%	37%
インド	34%	24%
中国*	27%	NA
南アフリカ	69%	60%
トルコ	21%	20%
メキシコ	36%	40%
インドネシア**	NA	16%
世界全体	**37%**	**34%**

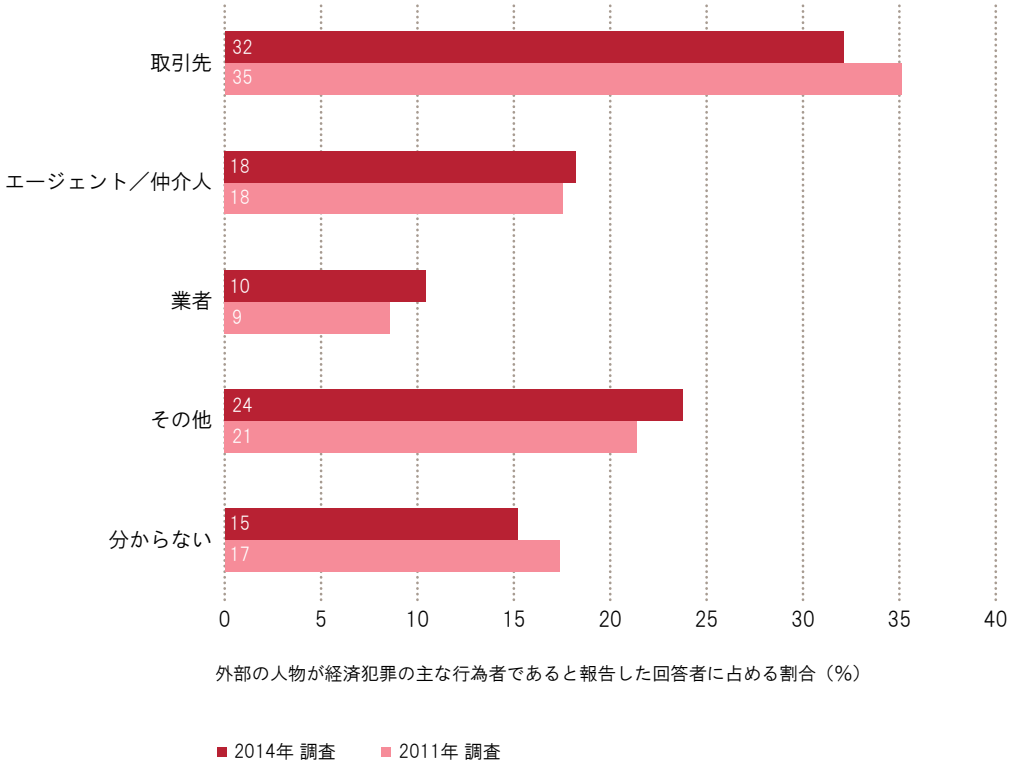
*2014年の中国の結果は香港・マカオを除く、2011年は中国（香港除く）の数値は不明
**2014年は回答が得られなかった

不正行為者の特徴の詳細

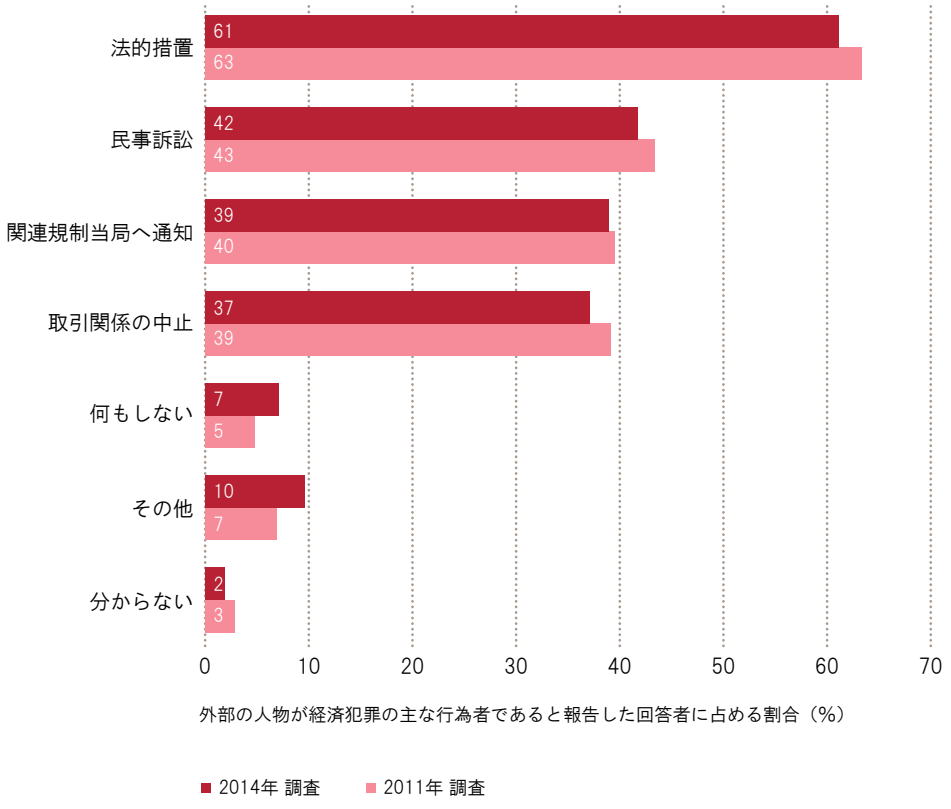
図表33：内部の不正行為者に対して取られた措置



図表34：外部の不正行為者のプロフィール



図表35：外部の不正行為者に対して取られた措置



調査手法

この第7回経済犯罪実態調査は2013年8月から2014年2月にかけて行われた。

本調査は4セクションに分かれている。

- 回答者の所属などを含む 一般的な質問
- どのような経済犯罪の被害にあったことがあるかに関する質問
- サイバー犯罪の脅威に関する質問
- 贈収賄や汚職、マネーロンダリング、反競争法および独占禁止法に関する質問

本調査について

2014年経済犯罪実態調査は95カ国において5,128の回答を得た（2011年の回答数は78カ国3,877件）。回答者の内、50％が組織を代表する上級経営幹部、35％が上場企業、54％が従業員1,000人以上の企業であった。

調査手法

1. 各組織の経営幹部に対して調査を実施した。本調査は、回答を得た経営幹部の所属組織における経済犯罪に関する経験に基づいている。私たちは、さまざまなタイプの経済犯罪について、組織への影響（発生した財務的、副次的な重大な損害について）、犯罪の首謀者、組織が講じた対応等の情報を収集した。

2. サイバー犯罪、贈収賄や汚職、マネーロンダリング、反競争法および独占禁止法に関して調査を実施した。本調査では、組織全体に対して影響が大きく、長期的な被害となりうるこれらの脅威について着目した。

3. 過年度の調査結果との比較分析を実施した。本調査は2001年から開始し、多くの主要な質問に、その時代に合わせて調査時に重要と思われる質問を組み合わせることで、調査内容は世界中の組織に影響を及ぼすと思われる問題に対応している。過去の調査結果と合わせて分析をし、現在の主要な問題点やその推移を図示化して分析することで、問題の傾向を捉えることができる。

他資料

- PwC – 第17回世界CEO意識調査
  [http://www.pwc.com/jp/ja/japan-news/2014/ceo-survey2014.jhtml]
- PwC - 変化の時にこそ信頼を：年間グローバルレビュー2013（英語）
  [http://www.pwc.com/gx/en/annual-review/megatrends/index.jhtml]
- PwC – ドイツ経済犯罪実態調査：経済犯罪と企業文化 2013 （ドイツ語）
  [http://www.pwc.de/de/risiko-management/wirtschaftskriminalitaet-2013.jhtml#]
- PwC – グローバル情報セキュリティ調査2014
  [http://www.pwc.com/jp/ja/advisory/press-room/news-release/2014/information-security-survey140205.jhtml]

図表36：本調査への参加地域一覧

地域	2014年	2011年
アジア太平洋	**906**	**669**
オーストラリア	79	79
中国 （香港含む）[1]	N/A	22
香港／マカオ	116	N/A
中国 （香港除く）	85	N/A
インド	115	106
インドネシア	4	84
日本	75	73
マレーシア	110	93
ニュージーランド	82	93
パプアニューギニア	81	1
シンガポール	82	18
台湾	0	2
タイ	76	79
ベトナム	1	19
アフリカ	**604**	**259**
アルジェリア	2	0
アンゴラ	22	1
ボツワナ	5	1
カメルーン	6	0
コンゴ民主共和国	1	0
ガーナ	3	29
ギニア	2	0
コートジボワール	3	0
ケニア	124	91
レソト	1	0
リベリア	0	5
マラウイ	1	0
モロッコ	17	0
モザンビーク	4	0
ナミビア	26	2
ナイジェリア	82	3
シエラ・レオネ	1	0
南アフリカ	134	123
スワジランド	4	1
タンザニア	12	0
チュニジア	17	2
ウガンダ	12	0
ザンビア	83	1
ジンバブエ	42	0

地域	2014年	2011年
中東[2]	**232**	**128**
下記以外の中東諸国	N/A	127
バーレーン	2	N/A
エジプト	7	N/A
ヨルダン	9	N/A
レバノン	8	N/A
オマーン	1	N/A
カタール	12	N/A
サウジアラビア	74	N/A
スーダン[3]	1	1
シリア	1	N/A
アラブ首長国連邦	117	N/A
西欧	**1,555**	**1,317**
アンドラ	0	1
オーストリア	6	8
ベルギー	68	84
キプロス	88	5
デンマーク	118	116
フィンランド	34	61
フランス	131	112
ドイツ[4]	10	38
ギリシャ	11	92
アイルランド	78	80
イスラエル	31	–
イタリア	101	127
ルクセンブルグ	12	3
オランダ	75	41
ノルウェー	92	67
ポルトガル	75	0
スペイン	79	85
スウェーデン	91	79
スイス	83	140
イギリス[5]	372	178
北米	**215**	**209**
カナダ	100	53
アメリカ合衆国	115	156

1）中国と香港は2005年-2011年の間は合計されていたが、2014年では別々に表記している。

2）中東は前回アジア太平洋地域に含まれていた。

3）スーダンは前回アフリカ地域に含まれていた。

4）PwCドイツは2013年に別途603の回答者からの回答者を元に独自に調査を実施した。

5）イギリスにはガーンジー島所属とした回答者の回答を含んでいる。

図表36：本調査への参加地域一覧

地域	2014年	2011年
中東欧	**877**	**804**
ブルガリア	79	58
クロアチア	0	1
チェコ共和国	94	84
エストニア	0	1
ハンガリー	91	85
カザフスタン	1	0
リトアニア	1	7
モルダビア	0	1
モンテネグロ	0	1
ポーランド	94	79
ルーマニア	77	76
ロシア	111	126
セルビア	52	14
スロバキア	76	84
スロベニア	33	48
トルコ	78	55
ウクライナ	90	84

地域	2014年	2011年
中南米	**711**	**483**
アルゼンチン	82	77
バハマ	2	0
バルバドス	1	0
ボリビア	0	3
ブラジル	132	115
チリ	75	1
コロンビア	1	1
キューバ	2	0
ドミニカ共和国	1	0
エクアドル	22	11
メキシコ	211	174
ペルー	82	17
ベネズエラ	100	84
それ以外の国、地域	**28**	**8**
合計	**5,128**	**3,877**

図表37：参加組織の業種別割合

回答者率（%）

業種	2014年	2011年
航空宇宙／防衛	1%	1%
化学	2%	2%
情報	3%	3%
エネルギー資源、公益、鉱山	7%	7%
土木建築	6%	5%
エンターテイメント、メディア	2%	3%
金融サービス	19%	18%
政府関連組織／国営企業	5%	5%
ホスピタリティ／娯楽	2%	2%
保険	7%	5%
製造	9%	12%
製薬、 生命科学	5%	5%
専門家サービス	6%	6%
小売・消費財	7%	8%
技術	5%	5%
運輸・物流	5%	4%

図表38：参加者の所属組織内での（主な）職務

回答者率（%）

業種	2014年	2011年
監査	14%	16%
アドバイザリー／コンサルティング	4%	3%
コンプライアンス	6%	5%
カスタマーサービス	1%	1%
経営管理	18%	17%
財務／経理	28%	29%
人事	1%	1%
情報技術	2%	4%
法務	4%	4%
マーケティング／営業	3%	2%
生産管理	2%	3%
購買	1%	0%
研究開発	1%	1%
リスク管理	6%	6%
セキュリティ	3%	4%
税務	1%	1%
その他	6%	2%

図表39：参加者の組織内の職位

	回答者率（%）	
	2014年	2011年
上級役員	**50%**	**53%**
取締役	4%	4%
CEO／代表取締役／業務執行取締役	12%	10%
業務執行責任者（COO）	2%	2%
最高財務責任者（CFO）／財務部長／会計監査役	23%	23%
最高情報責任者／技術責任者（CIO）	1%	3%
最高セキュリティ責任者*	2%	
その他の経営幹部	6%	10%
非上級役員	**49%**	**47%**
上席副社長／副会長／取締役	7%	8%
事業部門長	4%	7%
部長	15%	15%
人事部長*	1%	
マネージャー	22%	17%
その他	2%	0%

*本調査より区分追加

図表40：参加組織の種別

	回答者率（%）	
	2014年	2011年
上場企業	35%	36%
非上場企業	50%	51%
政府関連／国営企業	9%	10%
その他	6%	3%

図表41：参加者の所属する組織の規模（従業員数）

	回答者率（%）	
	2014年	2011年
1,000人以下	44%	43%
1,001人以上 5,000人以下	20%	20%
5,000人以上	34%	34%

用語

不正会計

財務諸表、その他の書類が、改ざんされ、またはその価値や財務活動を正確に反映しない報告がなされること。 会計操作、不正借入・資金調達、不正な与信申請、無権限の取引や不正トレードを含む。

資産横領（従業員による詐欺や横領を含む）

役員やその他受任者としての義務を負う地位にいるもの、もしくは従業員が、自己の利益のために、資産（金銭資産・現金・事務用品・機器を含む）を盗取すること。

贈収賄や汚職（利益供与や恐喝を含む）

公職にあるものが、職務に違反しその地位を利用して、自分にとって有利なものを得ること。経済的利益やその他特取り計らいらいの約束、脅迫・ゆすりを含む。また、それらの誘引を容認することを含む。

反競争的行為

市場における支配的地位を乱用した、もしくは他社との共謀によるカルテル行為（例えば、価格協定、入札談合、企業間協定に基づく市場分割、購入したい商品を買うに当たり、違う商品もまとめて購入することを買い手に義務付ける行為）など、市場での競争を阻害する行為。

サイバー犯罪

コンピューター犯罪としても知られ、コンピューターやインターネットを使用して発生するもの。サイバー犯罪の典型的な例は、ウイルス、メディアの違法ダウンロード、フィッシングやファーミング（悪意のあるWebサイトへのリダイレクト）、銀行口座情報に代表される個人情報の窃盗などが挙げられる。

サイバー犯罪には、犯罪を行うにあたりコンピューターを使用したというような通常の不正行為は含まない。ただコンピューター、インターネットまたはその他の電子デバイス等が意図的に使用され、当該犯罪における重要な要素となっているような場合にはサイバー犯罪に含むものとする。

経済犯罪・不正

他人の金銭、所有物、もしくは法的権利を奪うために虚偽行為や策略を実行すること。

スパイ活動

秘密情報を得るためにスパイ行為をすること、またスパイを使うこと。

財務的な損失

不正による財務的損失を推定する場合、直接的および間接的な損失の両方を含めるべきである。直接的な損失は不正による損失の実際発生額であり、間接的な損失は、通常、問題の調査や修正に関わる費用や、規制当局による課徴金、訴訟費用、風評による被害を含む。ただし間接的な損失からは「ビジネスチャンスの喪失」に起因する機会損失の見積もり額は除外する必要がある。

不正リスク評価

組織が下記の（i）から（v）の事項を確かめるために行う評価指標。

（i） どの業務が不正リスクにさらされているか

（ii） 最も脅威となるリスク（重要性と可能性の評価）

（iii） 重要なリスクを緩和するための統制の特定と評価

（iv） 組織内部の一般的な不正防止策や統制の評価

（v） 統制が不十分な場合の救済措置

人事に関する不正（雇用や人件費に係る不正）

給与支払いに関する不正、架空の社員のでっちあげ、日当に関する不正、友人や親族への優遇的な採用や不適切な人物の独断での採用、また採用書類の偽造など、採用に関わる不正。

用語（続き）

不正行為の動機やプレッシャー

個人が財政的なトラブルを合法的な手段では解決できない場合、非合法な手段で解決を図ろうとするといった状況。財政トラブルは職業的（失業の危機など）の場合や、個人的（借金など）な場合がある。

インサイダー取引

一般的に、忠実義務や他の秘密保持義務に違反して、重要な公開前の情報を利用して有価証券を売買すること。情報漏えいすることや、その情報を得たものが有価証券を売買すること、また、そのような情報を利用して有価証券を売買することを含む。

知的財産の侵害（商標、特許権、模造品や模造サービスを含む）

違法コピー、特許権や著作権侵害にあたる模造品の販売や流通、通貨の偽造を含む。

汚職リスクの高い市場

汚職リスク自体は主観的なものではあるが、本調査においては、2012年のトランスペアレンシー・インターナショナルによる腐敗認識指数（CPI）で50点以下の地域を汚職リスクが高い市場とした。

マネーロンダリング

犯罪等から得た利益を、出どころ出所を偽装するなどして、正当化しようとする行為。

不動産担保ローンに関する不正

不動産取引に関して、重大な虚偽表示、不当表示、報告漏れによって取引当事者を欺く行為。

機会または能力

個人が自分自身の財政的問題を解決する際に悪用する、自身の役職や役割。不正行為が発見されづらい機会が悪用されるケースが多い。

購買に関する不正

自己の利益のために、自社への責任を逃れまた自社へ損害を与えるような不正行為。行為者としては、企業の購買プロセスに関与する従業員、社長、役員、公務員、業者等が考えられる。

正当化

犯罪行為に対して行為が容認可能であると弁明を図る行為。

税金に関する不正

正しい納税義務を意図的に避ける不正行為。

フォレンジックサービス
PwCフォレンジックサービスはフォレンジック会計士、経済学者、統計学者、元規制局員、不正検査士、フォレンジック技術者で構成されている。私たちは組織の不正行為によって引き起こされる重大な財務的損失、風評被害へ対応を手助けしている。財務データの不規則性の特定、複雑なビジネス問題分析、不正リスクを軽減するためのサービスを提供している。

お問い合わせ先

Survey Leadership and Editorial Board

Steven Skalak
Partner, United States
+1 (646) 471 5950
steven.skalak@us.pwc.com

Darshan Patel
Partner, India
+ 91 22 6689 1670
darshan.patel@in.pwc.com

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

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

Survey Management Team

Matthew Curry
Manager, United States
+1 (646) 415 2994
matthew.j.curry@us.pwc.com

Forensic Services Leaders

Chris Barbee
Partner, USA, Global Leader
+1 (267) 330 3020
chris.barbee@us.pwc.com

John Donker
Partner, Hong Kong, East Cluster Leader
+852 2289 2411
john.donker@hk.pwc.com

Survey Marketing Team

Anjali Fehon
Marketing Director, United States
+1 (973) 236 4310
anjali.t.fehon@us.pwc.com

Shannon Schreibman
Global Marketing Senior Manager, United States
+1 (845) 489 8473
shannon.schreibman@us.pwc.com

日本のお問い合わせ先

プライスウォーターハウスクーパース株式会社
フォレンジックサービス

佐々木　健仁
パートナー
Tel: 080 3473 8478
Email: takehito.sasaki@jp.pwc.com

ホンマ　シン
ディレクター
Tel: 080 9441 7458
Email: shin.s.honma@jp.pwc.com

平尾　明子
マネージャー
Tel: 080 3414 2756
Email: akiko.hirao@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/report.jhtml
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/crimesurvey

日本語版発刊月：　2014年3月　　管理番号：I201401-11