金融業界にとっての脅威

pwc

www.pwc.com/jp

目次

ハイライト
金融業界の調査結果

魅力的な標的…金融業界を除く全業種の経済犯罪報告比率がわずか34％だったのに対し、金融業界では45％が調査対象期間中に経済犯罪の被害にあったと回答した。

被害はさまざまなかたちで発生する…金融業界は依然として犯罪者の主要な標的であり、資産の横領が引き続き主要な経済犯罪となっている。サイバー犯罪や贈収賄・汚職の頻度が高まっている。

経営幹部の姿勢…組織内部者による不正の大半は若手社員や中間管理職によるものであるが、5件に1件は経営陣が関与したものだった。

セキュリティの妄想…サイバー犯罪リスクが高まっているにもかかわらず、組織内の役割や部門によってリスクに対する認識は大きく異なる。

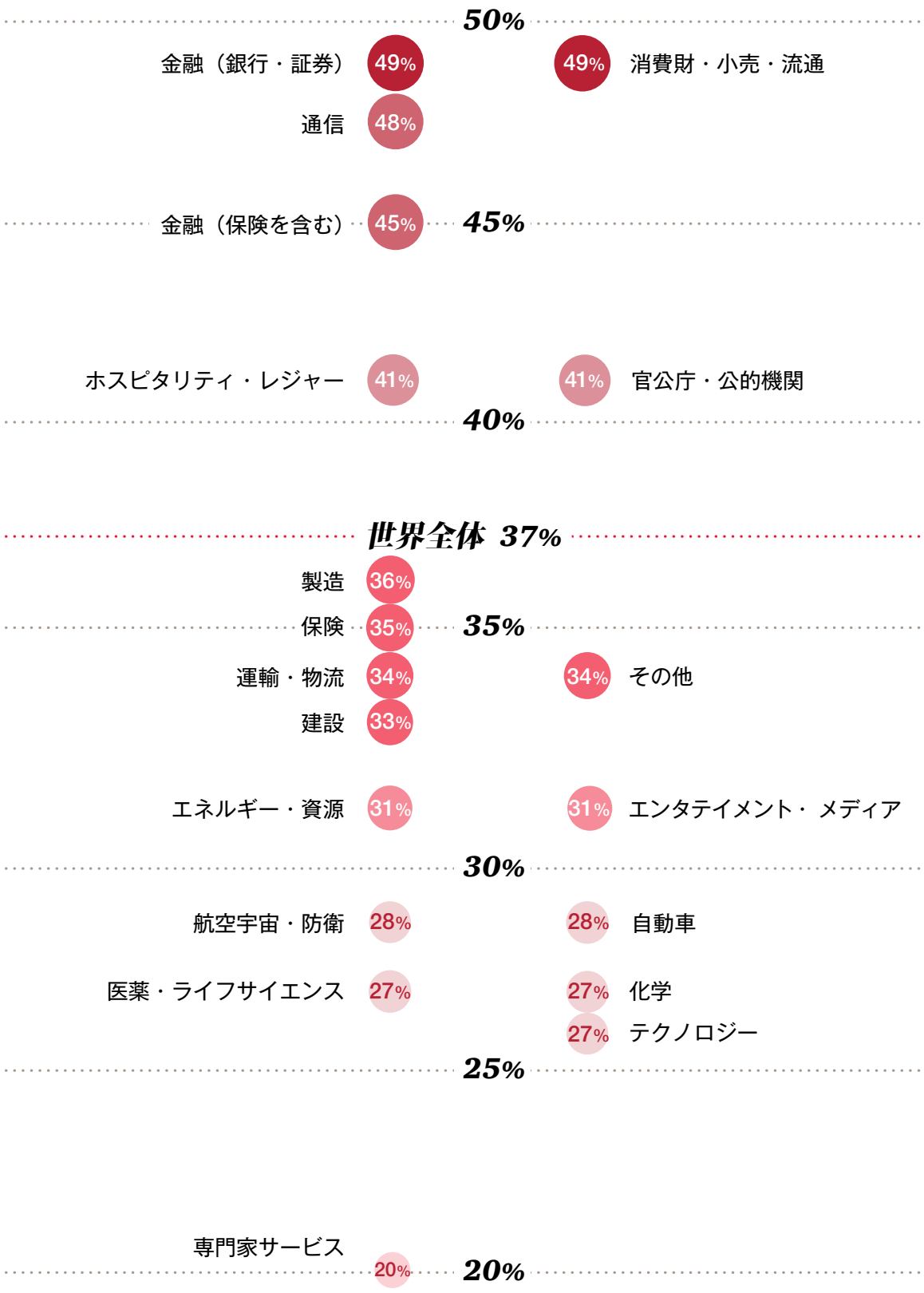
お金があるところに…マネーロンダリングは相変わらず金融業界で一番の話題となっており、その発生確率は他業界のほぼ5倍である。

名指しされ面目を失う…金融機関はマネーロンダリングに巻き込まれることを恐れている。金融機関のほぼ30％が自社の評判への影響が最も大きいと考えている。

通報…内部通報の仕組みの導入は以前より進んでいるようであるが、実効性には疑問が残っている。

リスクの過小評価…金融機関の4分の1は年次不正リスク評価を実施していなかった。調査対象期間中に不正リスク評価を行わなかった金融機関の過半数は、不正リスク評価がどういうものか理解していないか、不正リスク評価に価値を見いだせていなかった。

図表1：業種別経済犯罪報告比率



調査対象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（%）

経済犯罪報告比率が金融業界を上回ったのは、消費財・小売・流通業界と通信業界のみだった。保険業界の経済犯罪報告比率が金融業界全体の経済犯罪報告比率を下回っているが、これは予想外のことではない。銀行などの金融機関は現金を保有しており、不正行為者にとってより魅力的と考えられるためである。

序文

金融業界を除く全業種の経済犯罪報告比率がわずか34%だったのに対し、金融機関の45%が調査対象期間中に経済犯罪の被害にあったと回答した。

PwCの第7回経済犯罪実態調査でこのほど明らかになった金融業界[1]に関する調査結果は、これまでで最も包括的で興味深いものである。金融業界だけで1,330社から回答が寄せられ、全業種[2]合わせた回答企業5,128社の26%を占めた。これらの金融機関の所在地は世界79カ国に及び、金融業界に関する本報告書は、実にグローバル[3]で、不正やサイバー犯罪からマネーロンダリング、贈収賄・汚職まで、さまざまな形態の経済犯罪に関する見解を示すものとなった。

調査の質問項目は、現下の経済環境においての経済犯罪に対する各企業の姿勢、調査対象期間に発生した不正の種類、サイバー犯罪が増えているか否か、各企業が経験した贈収賄や汚職、マネーロンダリング、反競争的行為の程度を評価できるように設定されている。

金融業界は、多くの点で、他の業界の調査結果に見られる動向から乖離しており、興味深い結果となっている。一部の調査項目については、世界的に厳しい検査と規制の対象になっている業界とは思えないような結果が得られた。本報告書では、金融業界における経済犯罪、企業文化、個人の行動の相関関係に焦点をあて、誠実性およびコンダクトリスクの脅威について理解を深める必要のある金融機関が数多く存在することが、今回の調査でいかに明らかになったかを説明する。

調査結果から得られた主な結論は、金融機関は経済犯罪の防止・発見という点において他の業界より進んでいるかもしれないが、さらなる取り組みが可能であり、なされるべきであるということである。とりわけ懸念されるのは、不正リスク評価、内部通報（もしくはそれに相当する「スピークアップ・スピークアウト制度」）の仕組み、広範かつ継続的なサイバー犯罪の脅威に対する意識について明確な脆弱性が認められる金融機関が存在することである。

本報告書では、調査結果に加えて、「ベスト・イン・クラス（業界最高）」の取り組みの達成もしくは維持を目指す金融機関が実行すべき行動項目も提示する。

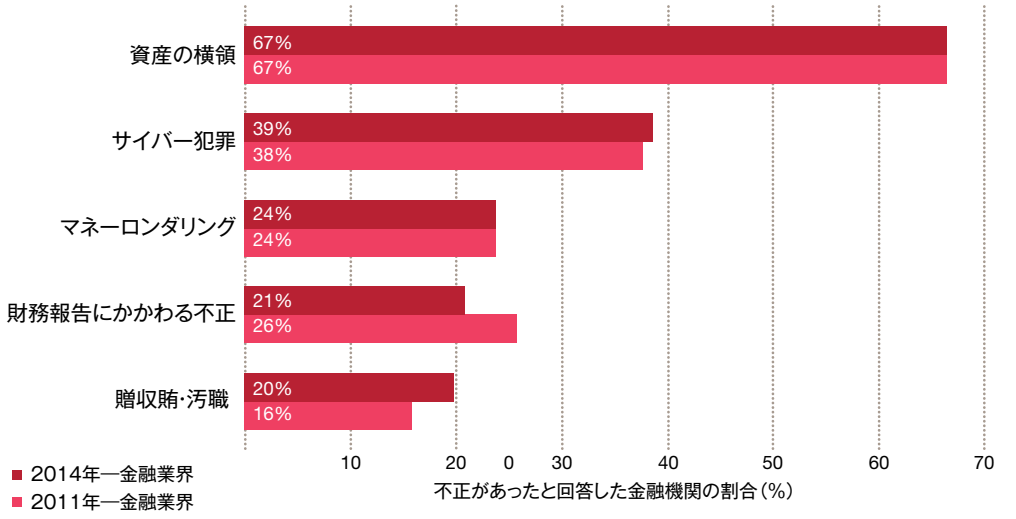
1. 金融業界：リテール金融、投資金融、保険、資産運用、証券、未公開株式投資を含む。本調査において回答企業は、（図表1に見られるように）自社の業種を「金融」と区別して、「保険」と特定することができた。本報告書において、「金融」という場合、その両者を指す。
2. これに対し、2011年の調査では、全業種合わせて3,877社から回答が寄せられ、うち878社（23%）が金融業界だった。
3. 世界79カ国の金融機関から回答が寄せられ、2011年調査の56カ国から大きく（ほぼ41%）増えた。

第1章—今日の金融経済犯罪
発生件数および被害金額

調査対象期間中に経済犯罪の被害にあったと回答した金融機関の約半数が、経済犯罪の発生件数と被害金額が増加していると報告している（他の業界より顕著な傾向）。状況は地域によって異なり、アジア太平洋地域では少なくとも半数の金融機関が増加と回答したのに対し、中南米地域ではほぼ40%の金融機関が減少と回答している。

主要な脅威

図表2：調査対象期間中に金融機関が被害にあった五つの主要経済犯罪



金融業界では資産の横領が引き続き最も多い経済犯罪となっている（67%）。これは、金融機関が現金を取り扱う機関であり、不正行為者にとって資産横領は換金コストの低い犯罪であることを踏まえれば、予想外の結果ではない。次に多いのがサイバー犯罪で、贈収賄や汚職と同様に、発生頻度が高まっている。財務報告にかかわる不正の被害にあったと回答した金融機関は、（前回調査では4分の1だったのに対し）5分の1にとどまったが、これは、社内統制の改善によるものと考えられる[4]。

不正の定義はさまざまであるが、ほとんどの場合、不当な手口によって金銭上の利益や個人的利益を得ようとするものである。さまざまな経済犯罪がある中、「従来型」の不正（資産の横領など）から第三者によるマネーロンダリングまで幅広い経済犯罪が金融機関にとって大きな脅威となっている。

4. 社内統制：内部監査、不正リスクマネジメント、人員ローテーション、技術的・物理的なセキュリティ管理手続きなど、リスクの監視と対処のために組織内で実施される一連の活動のこと。

内部不正行為者と外部不正行為者

過半数の金融機関（2011年の60%に対して2014年は57%）において、経済犯罪は依然として、主に外部の不正行為者によって引き起こされている。

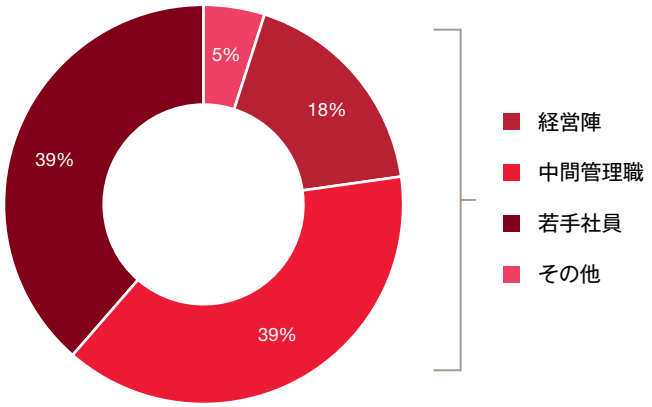
金融機関は、横領できる金額が大きく、重要性や機密性の高いデータ（クレジットカード情報、詳細な個人情報など）を保有していることから、外部者による不正行為の格好の標的となっている。サイバー犯罪は、ほとんどの場合、金銭目的だけでなく貴重な個人情報の入手を目的として、外部者によって引き起こされていることを明記しておく（金融機関もそう考えている）。例えば、保険会社は、機密性の高い情報や著名な人物のセキュリティ情報を保有しているかもしれない。

また、金融業界は一般的に他業界より厳しく規制されており、その結果、多くの業務手順や職務に社内統制が行き届いている。そのため、内部者が周りに気付かれずに不正を働くのは困難になっている。このことは、経済犯罪がどのように発覚したかを認識していると答えた金融機関のうち61%が社内統制を挙げており、他業界の56%を上回っていることにも示されている。

不正行為者の職位と人物像

2008年の不況突入後、金融業界の経済犯罪は、経営陣が関与（主たる動機はボーナスその他の利益のための業績や株価の操作である可能性がある）したものが2009年（12%）から2011年（18%）にかけて50%増加したことが前回の調査でわかった。2014年についても、経営陣の経済犯罪への関与は前回と同水準（18%）となっており、金融危機を受けて政府当局によって規制強化が図られたものの、誠実性やコンダクトリスク（誰からも見られていないときに正しいことを行わないリスク）を十分管理することはできなかったということを示している。

図表3：金融業界における内部不正行為者の職位



とはいえ、金融業界における内部不正は、依然として、若手社員や中間管理職によるものがほとんどである。他業界では、内部不正の64%が中間管理職や経営陣によるものであるが、金融業界では57%となっている。また、金融業界の内部不正行為者は、他業界に比べて大学卒以上の学歴を有している場合が多いが、これは採用時の学歴要件を反映しているものと考えられる。

調査結果が示しているのは、金融業界の平均的な内部不正行為者は組織内の職位がかなり低い段階から不正を働くことができるということである。これは、金融業界が扱う商品の仕組みや機能が複雑であり、その結果、（社内統制や監視体制が整っているにもかかわらず）「取り締まる」のが難しいためかもしれない。

金融機関としては、こうした調査結果をそのまま「現状」として受け入れるのではなく、不正対策を進めるにあたり、今回の調査結果が何を意味しているのかを探るべきである。

・各個人の誠実性や倫理的行動が十分重視されているか。

・従業員に対して、他者への影響を顧みることなく組織の利益や個人的利益を追求するよう日常的に奨励していないか。

・日々の業務においてどのように方針や手続きが実行されているかを示す証拠はあるか。

・倫理的行動に対する称賛や好ましくない行動に対する処罰は、一貫性を持って、公正かつ透明性のあるかたちで行われているか。

・従業員は、他者の行動に対して疑問を持ったり、開かれた討議の場で質問したりすることを奨励されているか。

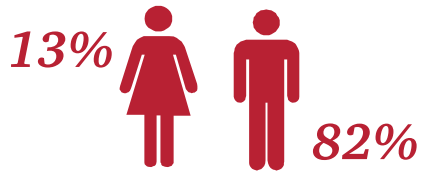
金融業界は、手順と規則とコンプライアンスを重視することで知られている。それでも、従業員に不正な行為を問いただすための教育と動機と支援が提供されなければ、服従が不正行為につながる可能性もある。

従業員の多様性

回答を寄せた金融機関によると、内部不正行為者は一般的に31～50歳である場合が多い。

調査対象期間中に各金融機関で発覚した不正のうち重大な事例について尋ねたところ、男性従業員による不正が82％（2011年の75％より増加）だった。女性従業員による不正の占める割合は減少（20％から13％へ）しており、特に大きな変化が見られなかった他業界とは対照的な結果となった。残りの5％については、不正行為が男性によるものか女性によるものか確認できなかった。

女性の社会進出に関する一部の調査研究によると、金融業界は女性従業員数が減少傾向にある。金融業界は他業界に比べて女性の進出度が低く、その実態が平均的な内部不正行為者の人物像にもある程度、反映されているものと考えられる。



何ができるか？

・倫理的行動に向けた組織としての戦略的目標を設定する。明確なビジョンを打ち出し、組織内の全ての人員に周知徹底されるようにする。

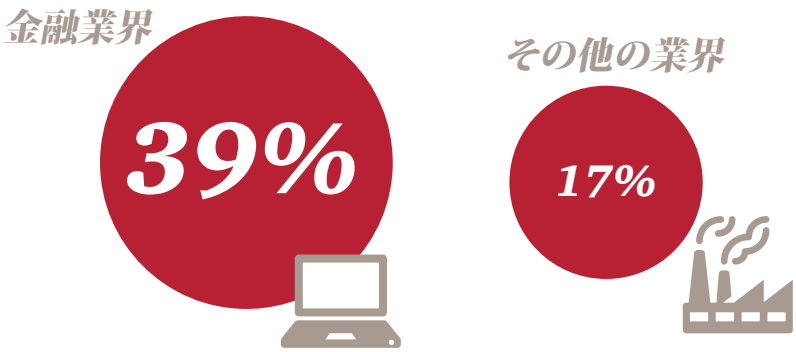
・現在、組織がどの程度の誠実性リスクにさらされているかについて（例えば、意図された行動と宣言された行動と実際の行動の不一致についてギャップ分析を行うことによって）評価し、許容できるリスクレベルを決める。

・組織内の好ましくない行動を生み出す要因を特定し、対処する。例えば、組織の人員採用方針および「精神」、リスクと見返りについての周知状況、その他の行動のきっかけとなる誘因について調査する。

第2章—サイバー犯罪
ITリスクだけではない

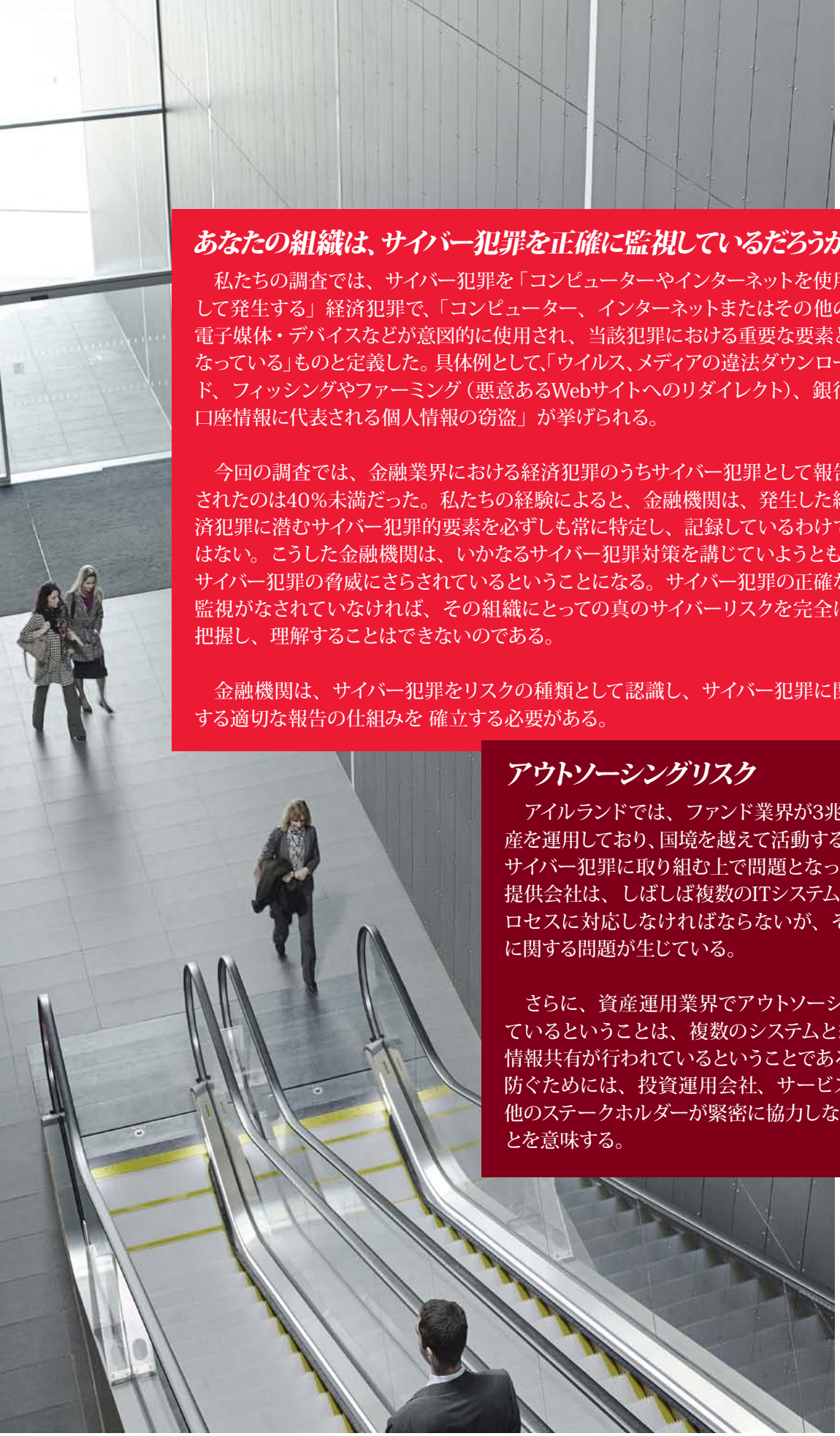
金融業界は、サイバー犯罪の標的として最初に狙われた業界の一つである。銀行のコンピューター化された業務プロセスや社内統制を破壊することによって得られる潜在的な金銭上の利益は常に大きいことを考えれば、これは驚くことではない。

今回の調査では、サイバー犯罪は依然として、金融機関にとって（資産の横領に次ぐ）2番目に多い経済犯罪という位置付けとなっており、被害にあったと回答した金融機関の割合は、2011年が38%だったのに対して2014年は39%だった（他業界では、2011年は16%、2014年は17%の企業がサイバー犯罪の被害にあったと回答）。しかし、私たちは、この数値はあまりにも低すぎると考えている。私たちの経験によると、金融機関（特にリテール銀行）の大半が調査対象期間中にサイバー犯罪の被害にあっている。



今後24カ月以内にサイバー犯罪の被害にあう可能性が高いと回答した金融機関は41%（アフリカ地域とアジア太平洋地域はそれぞれ約45%と36%）にとどまった。他業界は26%だった。この他、金融機関の19%はサイバー犯罪の被害にあう可能性が高いか低いかわからないという回答だった。

サイバー犯罪のリスクが高まっていると考えている金融機関の割合（57%）は、他業界（45%）に比べて高くなっている。2011年調査でサイバー犯罪のリスクが高まっていると回答した金融機関は半数だけだった。明らかに、金融機関はサイバー犯罪がより大きな脅威となりつつあるという認識を持っているが、それにもかかわらず、多くは自らの組織が実際に被害にあうとは考えていない。



あなたの組織は、サイバー犯罪を正確に監視しているだろうか

私たちの調査では、サイバー犯罪を「コンピューターやインターネットを使用して発生する」経済犯罪で、「コンピューター、インターネットまたはその他の電子媒体・デバイスなど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」ものと定義した。具体例として、「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」が挙げられる。

今回の調査では、金融業界における経済犯罪のうちサイバー犯罪として報告されたのは40%未満だった。私たちの経験によると、金融機関は、発生した経済犯罪に潜むサイバー犯罪的要素を必ずしも常に特定し、記録しているわけではない。こうした金融機関は、いかなるサイバー犯罪対策を講じていようとも、サイバー犯罪の脅威にさらされているということになる。サイバー犯罪の正確な監視がなされていなければ、その組織にとっての真のサイバーリスクを完全に把握し、理解することはできないのである。

金融機関は、サイバー犯罪をリスクの種類として認識し、サイバー犯罪に関する適切な報告の仕組みを 確立する必要がある。

アウトソーシングリスク

アイルランドでは、ファンド業界が3兆ユーロを超える資産を運用しており、国境を越えて活動する同業界の特徴が、サイバー犯罪に取り組む上で問題となっている。サービス提供会社は、しばしば複数のITシステムと矛盾した組織プロセスに対応しなければならないが、その結果、統一性に関する問題が生じている。

さらに、資産運用業界でアウトソーシングが広く行われているということは、複数のシステムと組織にまたがって情報共有が行われているということである。サイバー犯罪を防ぐためには、投資運用会社、サービス提供会社、その他のステークホルダーが緊密に協力しなければならないことを意味する。

昔ながらの手口と新たな手法

脅威の中には、一時的に高まって消えていくものもある。例えば、2012年から2013年にかけて繰り広げられた米国のいくつかの大手金融機関に対する中東からのサイバー攻撃は、影を潜めたようである。全体でみると金融機関の約5%が（サイバー犯罪の）リスクが軽減したように思うと回答しているが、これは上記のようにかつて大きく注目されたサイバー攻撃が、沈静化したことによるものかもしれない。

その一方で、サイバー犯罪は増えており、その手法は進化し続けている。銀行のインフラに対する攻撃はおさまる気配がない。最近では、銀行の支店のシステムにハードウェアをインストールし、モバイルネットワーク経由で取引を操作できるようにした事例があった。米国では、DDOS攻撃（複数のネットワークに分散する大量のコンピューターから一斉に接続要求を行うことによって処理能力を麻痺させるもの）による機能停止から、組織犯罪グループによるATMでの多額の現金引き出しまで、金融機関を標的とした経済犯罪が急増している。

米国では、Chip & PINシステム（ICカードと個人識別番号による本人認証システム）がまだ普及していないため、クレジットカードの不正使用が増加している。日本では、銀行の顧客のパソコンを標的として、偽のポップアップ画面や正規のインターネットバンキングのインターフェースを装った電子メールで顧客に個人情報を入力させ、預金を不正に引き出すウイルスを使ったフィッシング詐欺が発生している。

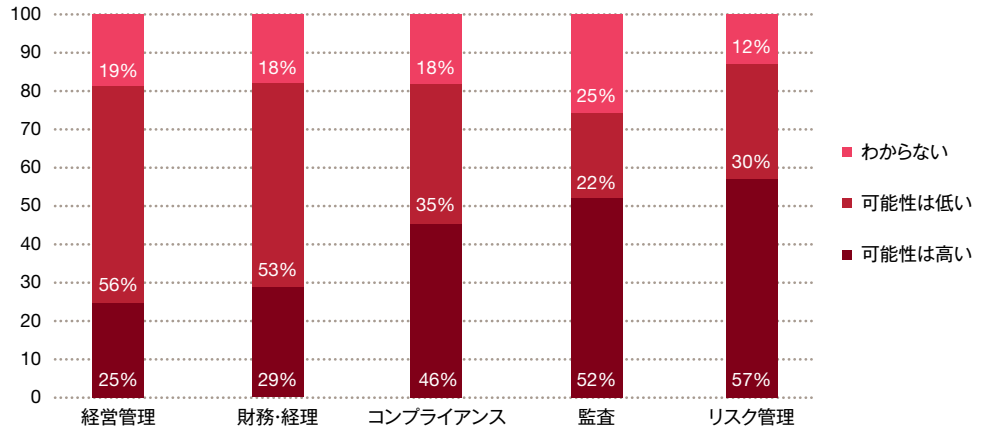
サイバー犯罪の景観は、その文字どおりの意味でも変貌を遂げつつある。例えば、当社のサイバーセキュリティ専門家は、アフリカ地域でサイバー犯罪が増加すると予想しているが、これは、同地域で各国政府が大規模なブロードバンド計画を打ち出していることによる。業界筋も（欧州連合(EU)域内各国の捜査当局間の連携が強化されたことから）サイバー犯罪者が欧州から、南アフリカ共和国に拠点を移しつつあると述べている。

サイバー犯罪に関する認識の温度差

今後24カ月以内にサイバー犯罪の被害にあう可能性が低いと考えている金融機関が40%もあるのは、憂慮すべき事態である。回答者の職位別に分類して回答を見てみると、驚くべきことに、最高経営責任者（CEO）もしくは同等者の54%と最高財務責任者（CFO）もしくは同等者の49%が可能性は低いと回答し、CEOの5人に1人は可能性が高いか低いかわからないと回答した。それでもなお、サイバーセキュリティに関する不安が主要な脅威であるという認識をCEOは持っている。PwCの第17回世界CEO意識調査によると、銀行・証券業界では、他業界を上回る70%超のCEOがサイバーセキュリティに関する不安を成長への脅威と見なしている。

各金融機関内部のサイバー犯罪リスクに関する認識には大きなずれが存在する。内部監査部門、コンプライアンス部門、リスク管理部門に属する回答者は、サイバー犯罪の被害にあう可能性が高いと考えているが、財務・経理部門や経営管理部門の回答者は逆の認識を示した。

図表4：今後2年以内にサイバー犯罪の被害にあう可能性が高いと思いますか



最高責任者レベルの回答者の見解はさまざまであるが、CEOやCFOは全般的に、自らの組織でサイバー犯罪が起こる可能性にあまり気付いていないようである。これは、一部の金融機関で最高責任者にサイバー犯罪に関する実質的な報告がなされていないということかもしれない。

内部監査、コンプライアンス、リスク管理といったリスクを注視する部門に属する回答者は、サイバー犯罪のリスクについても比較的しっかり認識しているが、その一方で、サイバー犯罪が起こる可能性は低いという回答の割合は、憂慮しなければならないほど高い。

金融業界はサイバー犯罪への取り組みで最先端を行っているというのが一般的な認識である。しかし、今回の調査は、金融機関の内部ではかなり油断が生じていることを示唆している。おそらく、脅威はたいてい一歩先を行っているという認識がないまま、経営陣はサイバーセキュリティ対策がかつてより改善していることに満足しているのだろう。あるいは、特定の部門（財務・経理を含む）は依然として、サイバーセキュリティを（重要な事業リスクというよりも）IT問題と捉える傾向があるのかもしれない。

「現在のインシデントに過去の戦略で対応――金融サービスにおけるデジタルチャネルが進化し続ける中、サイバーセキュリティは、もはや単なる技術的なリスクを超えて、事業リスクになった」

グローバル情報セキュリティ調査®
（PwC、CIO Magazine、CSO Magazineが毎年実施する世界的調査）

金融機関は、適切な防衛措置を実施しているか否かにかかわらず、サイバー攻撃の被害にあう可能性が高まっていることを認識すべきである。上記の調査結果と不正リスク評価に関する調査結果（後述）をつなぎ合わせると、金融機関が依然として、基本的なITセキュリティ方針を確立し、その方針を事業目的と事業リスクに結びつけることの重要性に気付いていないように思われる。

反撃する規制当局

一方、世界各国の規制当局は、特にリテール銀行や商業銀行が絡む場合、サイバー犯罪が社会全体に及ぶような危険をもたらすことに気付きつつある。金融機関は、さまざまな他業界の企業や個人の金融資産や機密性の高い情報を預かっている。つまり、金融業界におけるサイバー犯罪の影響は、標的となった金融機関だけの問題にとどまることはほとんどないということである。

サイバー脅威に対する規制上の圧力

英国では、サイバー犯罪が金融機関にとって重大なリスクであることをイングランド銀行（BOE）が宣言した。さらに、2013年11月には、イングランド銀行と英国金融規制当局が共同でWaking Shark II作戦と呼ばれる大規模なサイバー攻撃演習を実施し、英国の銀行がサイバー攻撃のストレスにどの程度耐えられるかを試した。イングランド銀行は、この演習に関する報告書の中で、業界内の協調体制を強化するとともに、各金融機関に対して重大な事件について規制当局に報告する必要があることを周知徹底する必要があると指摘している。同じく2013年11月、米国ではニューヨーク州当局が、管轄下の銀行のサイバーセキュリティに関する方針や手続きを評価するために、リアルタイムで実施するオンラインテストで当局の質問に答えることを銀行に義務付けると発表した。

さらに、米国では、重大な影響をもたらしたサイバー事件について上場企業報告書への記載を義務付けることによって、サイバー犯罪の可視性を向上させた。その結果、いくつかの大手金融機関は、過去にサイバー攻撃の標的になっていたことを米証券取引委員会（SEC）に提出する年次報告書（10K）で開示させられることとなった。 オンラインバンキングがそれほど発展しておらず、銀行がサイバー犯罪を重大なリスクと見なしていないレバノンにおいてさえ、金融業界がサイバー犯罪による多額の損害を被った。レバノンの銀行規制委員会（Banking Control Commission）は、サイバー防衛の強化を目指して、銀行のITセキュリティの調査に着手した。

知識は力である。金融機関は長年にわたり、脅威に関する情報共有に協力して取り組んでいる。サイバー脅威に関するデータ共有を進めることによって、各金融機関は迅速に、先を見越してサイバー犯罪に対処することができる。金融業界が主要産業であるルクセンブルクでは、こうした協力は経済全体にとって戦略的に重要である。

最大手の金融機関もサイバー犯罪を（単に発見するのではなく）阻止する必要性を認識しつつある。また、世界的な大手銀行において、重大性いかんにかかわらずオンラインバンキングに関する不正は全て阻止するというゼロ容認方針が打ちたてられた。

何ができるか？

- あらゆるレベルの従業員（最高責任者から新米管理職まで）を対象にサイバー脅威に関する教育を行う。サイバー犯罪は、単にIT・ネットワークセキュリティ部門の範疇におさまるものではない。サイバー犯罪には、ハクティビズム（政治的ハッカー活動）からデータ窃盗まで多種であり、銀行のさまざまな機能に多様な方法で影響を及ぼす。
- 潜在的にどのような犯罪者がどのような動機でサイバー攻撃をしかけてくるか理解する。
- 実効性あるサイバーセキュリティのための主要な予防対策措置を確実に講じる。継続的モニタリング、最新の個人・機密データ目録、バックアップ体制に関する方針、および事業継続計画を含む。
- 継続的に規制当局と連絡をとり、他の金融機関がどのようなサイバー犯罪対策を講じているか情報を入手し、「ベスト・イン・クラス（業界最高）」の手法を取り入れる。
- サイバー犯罪によって金融機関が被ったグロスとネットの財務損失を区別し、活動レベルと回復レベルがわかる指標として経営陣に報告する。

第3章—不正
被害はさまざまなかたちで発生する

金融業界は、特定の種類の経済犯罪（マネーロンダリングなど）に特にさらされており、その結果、規制面でも独特の課題がある。

マネーロンダリング

マネーロンダリングは相変わらず金融業界で一番の話題となっている。マネーロンダリングは、金融機関が財務損失を直接被るわけではないという点において、他の経済犯罪と明確に異なる。マネーロンダリングの影響は、（一般市民と規制当局両方から見た）評判の喪失を通して感じられ、規制当局によって課せられる巨額の罰金によってさらに増幅する。西欧およびアフリカ地域の金融機関の少なくとも50%は、世界的に事業展開する上で最もリスクが高いものとして、贈収賄・汚職や反競争的行為禁止法よりマネーロンダリングを選んでいる。

今回の調査で、マネーロンダリングは、金融機関にとって資産の横領とサイバー犯罪に次いで多く発生する経済犯罪であることがわかった。金融機関におけるマネーロンダリングの発生確率は、他の業界のほぼ5倍となっている。

金融機関は、マネーロンダリングが評判に与える影響について（業務上の混乱や財務損失よりも）特に大きな憂慮を示している。金融機関の評判重視姿勢は、多くの銀行がマネーロンダリング防止（AML）規制違反でマスコミの批判を招いた経験に基づくものである。

金融機関の29%は、マネーロンダリングがもたらす最も重大な影響は評判に対する影響であると考えている。

この数年間の世界各地における規制当局による法の執行活動によって、マネーロンダリング防止において規制当局が何を期待しているかが明確になった。世界的な金融機関にとっては、顧客本人確認（KYC: Know Your Customer）情報を組織全体で、特に複数の部署や管轄地域にまたがって複数の担当窓口で取引のある顧客に関して、どのように活用するべきかが課題となる。規制当局は金融機関に対して、時代遅れのITシステムの限界や国境をまたぐデータの機密保護法制の複雑さにかかわらず、顧客関係を統合的に把握することを期待するとの姿勢を明確にしている。

その期待を確実に満たすためには、金融機関はマネーロンダリング防止のための技術に投資する必要があるという認識が広がりつつある。マネーロンダリング防止に関する基準を設定する政府間組織FATF（Financial Action Task Force）は、金融機関がマネーロンダリング防止要件を満たしているか否かよりも、講じられているマネーロンダリング防止措置が実際に効果を発揮しているか否かを重視するという方針を先ごろ打ち出した。

守勢に立たされるマネーロンダリング防止策

多くの銀行は、業務や顧客ベースの規模が大きく複雑であるため、マネーロンダリング防止に向けた改善に悪戦苦闘している。規制当局（アイルランドからイスラエルまで世界各国の中央銀行を含む）は引き続き説明責任の強化を求めており、さらなる課題が生み出されている。

最近、英国の金融行為規制機構（FCA: Financial Conduct Authority）からマレーシアの中央銀行（Bank Negara Malaysia）まで世界各地の規制当局によって、金融機関のマネーロンダリング防止システムおよび管理体制に関する課題別検証報告書が発表された。FCAが発表した資産運用会社およびプライベートエクイティが初期投資を行うプラットフォーム会社に関する検証報告書（TR13/9）は、「優れた（good）」取り組みと「不十分（poor）」な取り組みの具体例を示した上で、経営陣の監督体制について以下のように述べている。

「繰り返し発生する問題について経営委員会に報告されているにもかかわらず、封じ込めや解決に向けた責任の所在が不明確なまま放置され、その結果、マネーロンダリングや贈収賄・汚職のリスクの管理が「後手」にまわっている事例を特定した。一部の金融機関の経営陣は、マネーロンダリングや贈収賄・汚職のリスク管理がどのように行われているかを明確に述べることができなかった」

南アフリカ共和国では、違法薬物取引による収益のロンダリングを特定および阻止するために、金融情報機関が1980年代に設置された。今日では、より広範な取り組みが行われており、金融情報センター（FIC: Financial Intelligence Centre）が同国内または同国経由で活動する世界的な犯罪組織の動き、大規模な汚職、政治的影響力を有する者が民間部門に及ぼす影響などを監視している。FICでは、ビッグデータの分析が必要とされる場面が増えており、今後、膨大な量のデータの処理・分析が可能な技術システムへの投資が必要になるだろう。

何ができるか？

- 顧客本人確認（KYC）手続きとマネーロンダリング防止プロセスが「シングル・カスタマー・ビュー（一元化された顧客情報）」を通してくまなく効果的に実施されるようにする。あらゆる関連システムと記録データをつなぎ合わせて、データの整合性を確保する。
- 規制要件ならびにマネーロンダリング組織の新たな手口に対応するため、時代遅れのITに起因する諸問題を解決する。

海外における贈収賄・汚職への対応

今回調査対象となった金融機関の47%は、汚職リスクの高い市場で事業展開している[5]。また、金融機関の約40%は、贈収賄・汚職、マネーロンダリング、反競争的行為禁止法といった各種経済犯罪について、結果的に被った被害額の推定値を提示することができなかった。

今回の調査結果は、こうしたリスクを財務損失というかたちで数値化することが依然として困難であることを示している。また、金融機関がこうした地域で事業展開することのリスクに十分取り組んでいないことも明らかになった。規制当局は、マネーロンダリングや贈収賄・汚職に対して引き続き厳しい目を向けており、その対象は、組織だけでなく個人も含まれる。英国では、2010年贈収賄法（Bribery Act）で取締役の個人的責任が強調され、2013年の金融サービス法（Financial Services Act）では、（贈収賄や汚職を回避するためにしかるべき措置を講じたことを示す）立証責任が個人に課せられた。

先見の明のある多くの金融機関が業界に先んじようとしている

私たちは最近、ある世界的な投資銀行と仕事をしたが、その際、いくつかの他の銀行（競合他社）の協力を得て、贈収賄・汚職・不正防止のための管理体制を比較評価した。その結果、上記投資銀行は、自らの組織構造がどうなっているか、また、組織内の役割分担、経営資源、責任分担がかかるリスクや事件の対処にどのように向けられているかについて、外側から客観的に見ることができるようになった。

金融機関は、新興市場でどういう相手と手を結ぼうとしているのか注意し続ける必要がある。2013年6月、米国司法省（Department of Justice）は、南米の国営経済開発銀行の幹部への贈賄容疑で、米証券会社のマネジングパートナーを逮捕したと発表した。より最近の事例では、複数の世界的な銀行が、アジアで著名な政府関係者を雇い入れていることが原因で贈収賄や汚職の嫌疑をかけられ、英国と米国の規制当局の捜査を受けた。こうした慣行は現地の企業の間では一般的に行われていることであるが、外国の規制当局は別の見方をする可能性がある。規制当局の最近の発表資料によると、金融機関に対する米国連邦海外腐敗行為防止法（FCPA: Foreign Corrupt Practices Act）やその他の類似法規制に基づく当局の監視が厳しくなりつつあるようであるが、これを踏まえればなおさら、金融機関としては事件が発生した後で規制当局と争うより、十分な情報に基づいて慎重に新興市場で事業を展開するほうがはるかに賢明だろう。

何ができるか？

- 不正発見メカニズムの実効性を高める方法を見いだすとともに、汚職リスクの高い地域で事業展開する際の規制違反リスクを軽減するために、不正や贈収賄・汚職に関するリスク評価を実施する。
- 贈収賄や汚職の起こりやすさを示す潜在的な「危険信号」を見つける手助けとなる、第三者に関する包括的なデューデリジェンス計画を実施する。こうした危険信号には、政治的影響力のある人物との関係、批判的なメディア報道、訴訟事件への関わりなどが含まれる。

5. 汚職リスクの高い地域とは、2012年腐敗認識指数（CPI: corruption perceptions index）が50未満の国を指す。http://www.transparency.org/cpi2012/results

内部通報―改善しているものの十分に利用されず、過小評価されている

内部通報の仕組みは、金融業界では依然として十分に用いられていない。金融業界がプロセスによる不正発見に大きく依存してきたことがその一因と考えられる。こうした手法がとられた結果、油断が生まれ、個々の従業員の誠実性や責任感の必要性が薄らぎ、十分に認識されなかったのかもしれない。あるいは、内部通報は従業員にとって懸念や問題を報告する「最後の手段」となりがちであることによるものかもしれない。

今回の調査では、一部において大幅な改善が図られたことが明らかになった。内部通報の仕組みがまったく存在しないと回答した金融機関はわずか19%にとどまった（2011年は45%だった）。内部通報の仕組みがあると答えた金融機関の半数以上（53%）は、その仕組みが効果的または大変効果的であると答えている（2011年調査では27%だった）。とはいえ、内部通報方針の実効性に関する懸念は依然として残る。内部通報の仕組みが効果的か否かわからないという回答が16%もあり、このうち内部通報の仕組みが効果的でないと答えた金融機関が7%あった。その地域別内訳は西欧が10%、アジア太平洋およびアフリカが6%となっている。

実際、最も重要な経済犯罪で情報提供や内部通報によって発見されたのはわずか16%で、社内統制の57%を大きく下回っている。他業界では、情報提供や内部通報による発見が26%を占めている。

教訓

ロンドン銀行間取引金利（LIBOR）不正操作事件では、複数の異なる銀行の従業員が不正に関与した競争法違反が明らかになり、内部通報者が違法行為や不正行為の「ふたを開ける」必要性が注目された。

LIBOR事件のように、従業員が人間関係の調和を崩してでも立ち向かうよう奨励されていなければ、単に内部通報の仕組みの利用を奨励するだけでは不十分である。同事件では、多くの従業員は、LIBORの操作が不正行為であるという認識すら持っていなかったようである。一部の金融機関では、経営幹部が姿勢を変える必要がある。多くの銀行は、近年、評判や社会的信頼を損ねた。「正しいことをする」企業文化を強固に確立することが求められている。

また、この分野における取り組みは経営陣が率先して行う必要がある。規制当局からより大きな説明責任を問われ、説明責任が果たせない場合は刑事責任を問われる恐れがあることを踏まえれば、その必要性はなおさら明らかである。

内部通報を奨励するために相当大胆な措置を講じている金融規制当局もある。例えば、米証券取引委員会による制裁に至った事件について、そのきっかけとなる情報を提供した人々は、その事件に関する制裁金などの100万米ドルを超過した額の一定割合を報奨金として支払われる可能性がある。2012年には、UBSの元行員が同行の脱税計画を暴露して、米内国歳入庁（IRS: Internal Revenue Service）から1億4,000万米ドルの報奨金を受け取った。ドイツでは、金融機関は、適切な内部通報の仕組み（その実効性と適切性は年次監査の対象）を設けることが法律で義務付けられている。

情報提供者に支払われる報奨金の額については、従業員の行動をゆがめるのではないかと懸念する人々から疑問の声が上がっている。その結果、内部通報の仕組みが乱用されることになるのか否かは、現時点ではわからない。さらに、歴史的・文化的理由から、内部通報は好ましい行為と見なされない地域もある。金融機関は、内部通報をめぐる問題と結果が事業にどのような影響を及ぼすことになるのか、また、どの程度目に見える結果が得られるのかについてよく検討し、内部通報の仕組みと組織内の他のフィードバックプロセスの連携が十分図られるようにする必要がある。

全体として、金融規制当局は内部通報を好ましい行動と見なしているようである。しかし、金銭的なインセンティブと肯定的な認識だけでなく、内部通報の仕組みの明らかな乱用に対するペナルティを伴うといった、バランスのとれたアプローチが求められている。さらに、内部通報が唯一残された手段になるほど事態が悪化する前の段階で、従業員が問題を特定し、報告できるようにすべきである。

何ができるか？

- 従業員の統合的なフィードバックメカニズムの一環として、内部通報の仕組み（もしくは類似の効果を持つ「スピークアップ」宣言のような制度）を設ける。
- 既存の内部通報の仕組みが近年あまり使われていなかったり、効果が認められなかったりする場合は、これを刷新する。
- 好ましく、報われ、認められる業務の一環として内部通報の仕組みの利用を促す（「告げ口」ではなく「正しいことをする」ということであることをはっきりと伝える）。

不正リスク評価

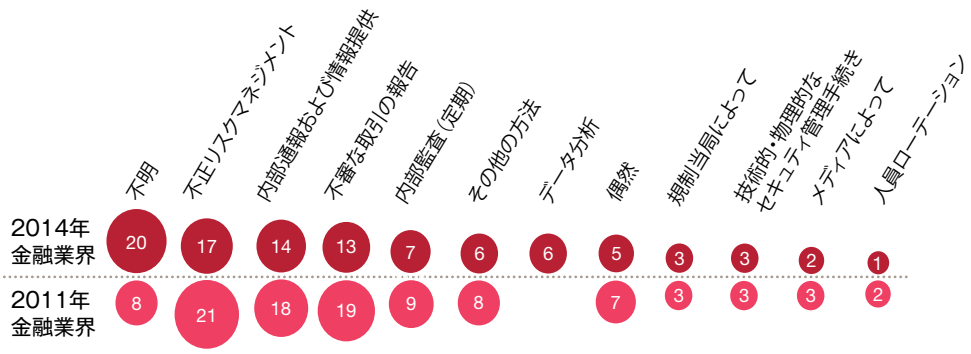
一部の国・地域では、マネーロンダリングや不正といった特定のリスク分野に関する金融規制要件が設けられている。今回の調査では、不正リスク評価について尋ねたが、その結果、驚くほど多くの金融機関で不正リスク評価が一切行われていないことがわかった。不正リスク評価がより定期的に行われていれば、もっと多くの経済犯罪が発見されていたかもしれない。贈収賄や汚職、マネーロンダリングのような他の経済犯罪についても、全社的なリスク評価を実施することによって好ましい影響が得られるだろう。

年次不正リスク評価を実施しなかったと答えた金融機関の割合は18%から25%に上昇した。この結果は、他業界（43%が年次不正リスク評価を実施していない）に比べてましに見えるが、金融規制当局はこうしたリスク評価が行われることを期待する傾向にあり、義務付けている国・地域も相当数あることを踏まえると、この割合はかなり高いと考えられる。

さらに、調査対象期間中に不正リスク評価が組織内で実施されたか否かを把握していない回答者も12%いた。その理由を尋ねたところ、不正リスク評価がどういうものかわからないという回答が32%に上った（これに対する2014年調査の他業界の数値は30%、2011年調査における金融業界の数値は36%だった）。また、27%は不正リスク評価に価値が見いだせないという理由だった。

調査期間中に不正リスク評価を実施しなかったと回答した金融機関の50%超は、不正と職場環境、組織文化、社内統制の実効性の相関関係を見いだせていないようである。それでもなお、最も深刻な不正のほぼ5分の1が不正リスクマネジメント（FRM）によって発見されている。今回の調査でも、不正リスクマネジメントが最も効果的な不正発見方法という結果となった（金融機関で起きた深刻な不正の17%はこの方法で発見された）。不審な取引に関する通報によって発覚した不正は13%にとどまった（2011年は19%だった）。データ分析による発見（2011年では選択肢に含まれていなかった）は6%だったが、今後、この手法は重要性が増すと思われる。驚くべきことに、不正発見方法を特定しなかった回答者（「不明」）が、2011年はわずか8%だったのに対して、今回は5人に1人もいた。

図表5：金融機関における経済犯罪の発覚原因



金融業界の回答者に占める割合（%）

保険業界の問題を探す

私たちの経験によると、多くの保険会社は、効果的なリスク評価体制が整っていないことにようやく気付き始めたところである。しかし、中には先進的な取り組みを行っている保険会社もある。ある保険会社は、（特定の既知の不正に重点をおくのではなく）未知の不正を積極的に見つけ出すための不正発見プログラムを設けている。

このようなプログラムは、不正や違法行為が偶然発見されることを期待して実施される抜き打ち検査や無作為調査とは対照的に、明確な方法と実施計画（データ分析も適宜利用）に基づいて実施することによって最も大きな効果を発揮する。

何ができるか？

- 不正リスク評価は事業にとって不可欠な要素であり、多くの場合において、規制当局との衝突を避けるために必要であることを認識する。金融機関は、十分な情報に基づいて、どのような不正防止・発見の仕組みが必要か決定する必要がある。
- 新たな不正発見方法を検討する。データ分析によって、金融機関は「異常値」基準（ありそうにない取引や支払い日など）に基づいて不正を特定することができる。

お問い合わせ先

経済犯罪実態調査および調査方法に関するさらなる詳細については、
http://www.pwc.com/jp/ja/japan-knowledge/archive/economic-crime-survey2014.jhtmlをご参照ください。

本報告書の記載内容についてさらなる情報の入手をご希望の場合、あるいは経済犯罪に関する問題について当社の担当チームがどういうサービスを提供できるかご相談をご希望の場合は、以下のお問い合わせ先までご連絡ください。

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

上野　俊介
マネージャー
Tel: 080-1014-6320
Email: shunsuke.ueno@jp.pwc.com

フォレンジックサービス

PwCのフォレンジックサービスのネットワークは、フォレンジック会計士、経済専門家、統計専門家、元規制当局者・捜査官、不正検査士、フォレンジック技術者、企業情報専門家で構成されています。私たちは、経済犯罪に関する重大な財務リスクや評判リスクに立ち向かうお手伝いをします。財務上の不正を特定し、業務上の複雑な問題を分析し、将来の不正リスクを軽減します。

www.pwc.com/jp

PwCは、世界157カ国に及ぶグローバルネットワークに195,000人以上のスタッフを有し、高品質な監査、税務、アドバイザリーサービスの提供を通じて、企業・団体や個人の価値創造を支援しています。詳細は www.pwc.com/jp をご覧ください。

PwC Japanは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（あらた監査法人、京都監査法人、プライスウォーターハウスクーパース株式会社、税理士法人プライスウォーターハウスクーパース、PwC弁護士法人を含む）の総称です。各法人は独立して事業を行い、相互に連携をとりながら、監査およびアシュアランス、アドバイザリー、税務、法務のサービスをクライアントに提供しています。

本報告書は、PwC メンバーファームが2014年9月に発行した『2014 Global Economic Crime Survey: Threats to the Financial Services sector』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。

電子版はこちらからダウンロードできます。 www.pwc.com/jp/ja/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/gx/en/financial-services/publications/global-economic-crime-survey-2014-financial-services.jhtml

日本語版発刊月：2015年4月　　管理番号：M201410-5