経済犯罪実態調査 2018
日本分析版

過去2年間で経済犯罪・不正の被害に遭った企業の割合

36%
日本

46%
アジア太平洋

49%
世界全体

pwc

www.pwc.com/jp

はじめに

過去2年間における経済犯罪・不正の実態について、PwCでは2年に一度、グローバル規模でオンラインによるアンケート調査を行っており、今年で9回目を迎えた。

今回は今までで最高となる、世界123の国と地域から7,228名の回答が寄せられ、うち日本からは182名の回答を得た。

時代とともに経済犯罪・不正の傾向も変化しているため、それに合わせて調査の質問や選択肢も変化させてきているが、今回の大きな変更点としては、経済犯罪・不正の種類として、「顧客による不正」と「事業活動に関する不正」という二つの類型を追加したことである。これは、近年増加しているクレジットカードの不正利用や顧客の虚偽申告によるローンの借り入れに代表される「顧客による不正」や、検査工程の省略・検査データの改ざんによる品質不正や過大広告などの景品表示法違反などに代表される「事業活動に関する不正」が、従前からある不正の類型では対応できないためである。

調査概要

調 査 期 間 ：2017年6月21日～9月28日

調 査 方 法 ：オンラインによる選択式アンケート調査

有効回答数：世界123の国と地域から7,228名（うち、アジア太平洋2,218名、日本182名）

回答者の特徴：【世界全体】回答者の56%が組織を代表する経営幹部、42%が上場企業、55%が従業員1,000人超の企業

【日本】回答者の34%が組織を代表する経営幹部、57%が上場企業、68%が従業員1,000人超の企業

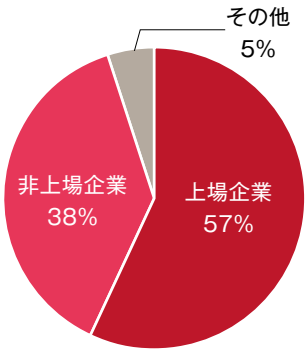
※レポート中の数値は、小数点以下四捨五入

業界別	%
工業	43%
金融サービス	18%
消費財	23%
テクノロジー	4%
プロフェッショナルサービス	2%
その他	11%

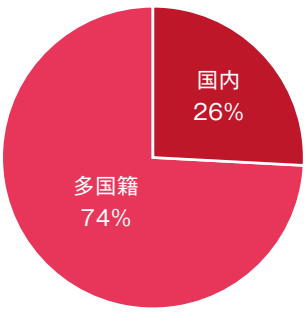
世界全体では、「顧客による不正」が、「資産の横領」、「サイバー犯罪」に続いて3位、「事業活動に関する不正」が4位という結果となったが、日本においては、「事業活動に関する不正」が「資産の横領」に次いで2位、「顧客による不正」は7位という結果であった。昨今の報道をみても分かるとおり、日本においてはデータの改ざんによる品質不正といった「事業活動に関する不正」が顕著に多い結果となっており、世界全体との差が垣間見えた。

これ以外にも、犯罪者のプロファイルや経済犯罪・不正への対応策などに関しても、日本と世界全体との違いがみられており、本冊子ではそれらの違いや、逆に世界との共通項などについて論じている。

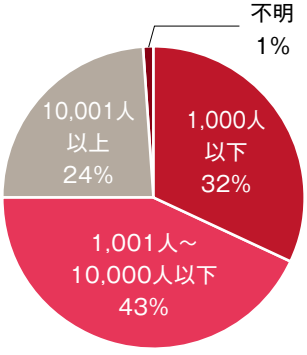
上場／非上場



事業展開領域

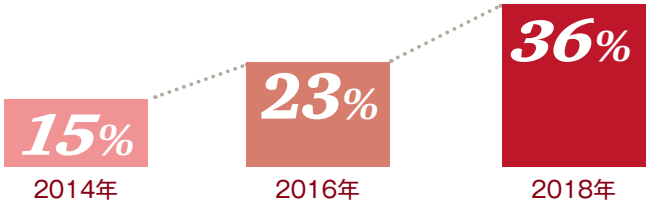


従業員数



目次

過去2年間で経済犯罪・不正の被害に遭った企業は増加傾向



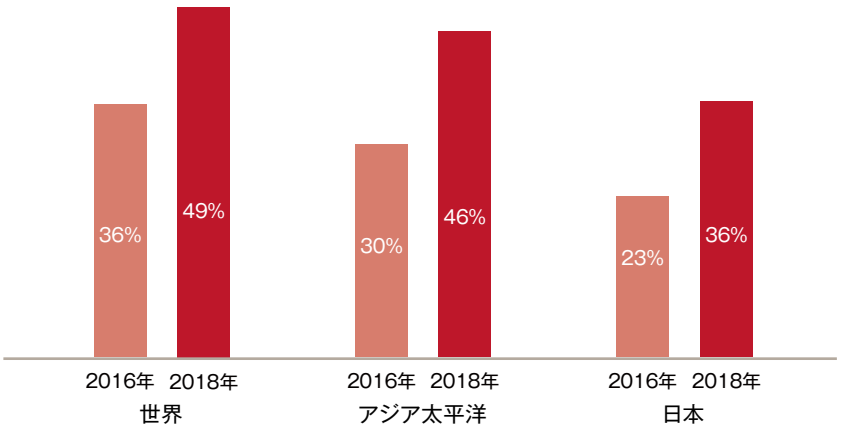
日本企業における経済犯罪・不正の概要

前回と今回の調査結果を比較すると、「過去2年間で経済犯罪・不正の被害に遭った」と回答した企業が世界的に増加していることが分かる（図1）。世界全体では回答企業の約半数にあたる49％（前回比+13％）、アジア太平洋では46％（+16％）、日本では36％（+13％）が被害に遭ったという結果が出た。この調査結果だけをみれば、日本企業の被害遭遇率は相対的に低いといえるかもしれない。一方で、前々回調査時から4年間を通じて増加傾向にあること（世界的には前々回から前回にかけては減少傾向であった）、経済産業省や経団連からアナウンスまで出る事態となった品質不正問題などを考慮すれば、今回の調査結果をみて安心するのは危険であると考えられる。

経済犯罪・不正の類型とコンダクトリスク

過去2年間で経済犯罪・不正の被害に遭ったと回答した回答者が、どのような経済犯罪・不正の被害に遭ったかを表しているのが図2である。冒頭でも述べたように、近年クレジットカードの不正利用などの「顧客による不正」や、検査工程の省略・検査データの改ざんなどによる品質不正などの「事業活動に関する不正」が増加していることを背景に、今回の調査では新たにこの二つの不正類型を追加した。結果としては、日本においては、過去2年間で被害に遭ったことのある経済犯罪・不正として、「顧客による不正」を挙げた企業は11％（第7位）、「事業活動に関する不正」を挙げた企業は33％（第2位）となり、世界全体の結果と比較すると、「事業活動に関す

図1　過去2年間で経済犯罪の被害に遭ったと回答した企業



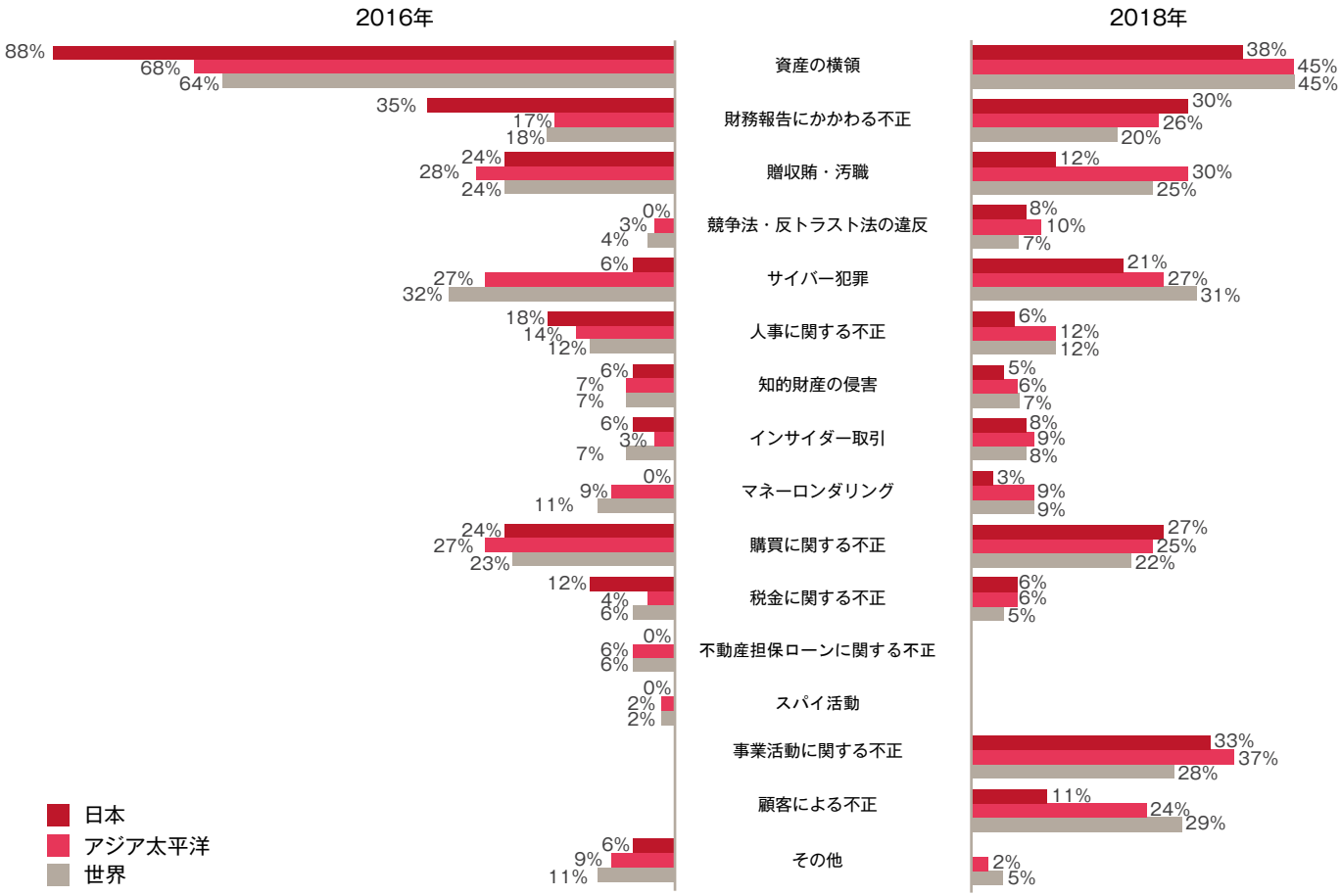
報告件数が多い経済犯罪・不正上位三種類

る不正」の割合が高く（世界全体：28％）、顧客による不正の割合が低い（世界全体：29％）という結果となった。なお、前回と今回の調査結果を比較した際に、資産の横領に遭ったと回答した企業の割合が大きく減少した要因として、上記二つの不正が新類型として加えられたことがある点には注意が必要である。

上記を踏まえた上で今回の調査結果をみると、前回調査から継続して、世界全体やアジア太平洋と比べ、日本では財務報告にかかわる不正の割合が多く、贈収賄・汚職の割合が少ない傾向がみられた。サイバー犯罪についても世界全体やアジア太平洋と比較すると少ないが、前回調査と比べると3倍以上に増加している点は特筆すべきだろう。

また一方で、組織内部の不正リスクである「コンダクトリスク」についての関心が高まっている。コンダクトリスクとは、従業員の行動によって、顧客が期待する公正な結果の達成や市場の健全性が損なわれるリスクを指す。コンダクトリスクは、企業文化や組織風土に起因するといわれていることから、内部統制などによるチェックが効かないことが多く、組織としてより柔軟で包括的な対応をとることが求められている。現在多くの企業でとられている、コンプライアンス・企業倫理・企業リスク管理（ERM）がそれぞれ別の部門で扱われるような、縦割りの組織体制をとっていると、運営のすれ違いや各組織間における責任領域の認識のずれなどによって、不正の隠蔽が容易になってしまう。この事態を打破する方法の一つとしては、コンプライアンス・企業倫理・ERMに横串を通し、企業として一体化したコンダクトリスクへの対応策を構築することである。これにより企業として、より包括的な視点からリスク低減の方策をとることができ、コスト効率化も同時に進めることができるのである。

図2　過去2年間で被害に遭った経済犯罪



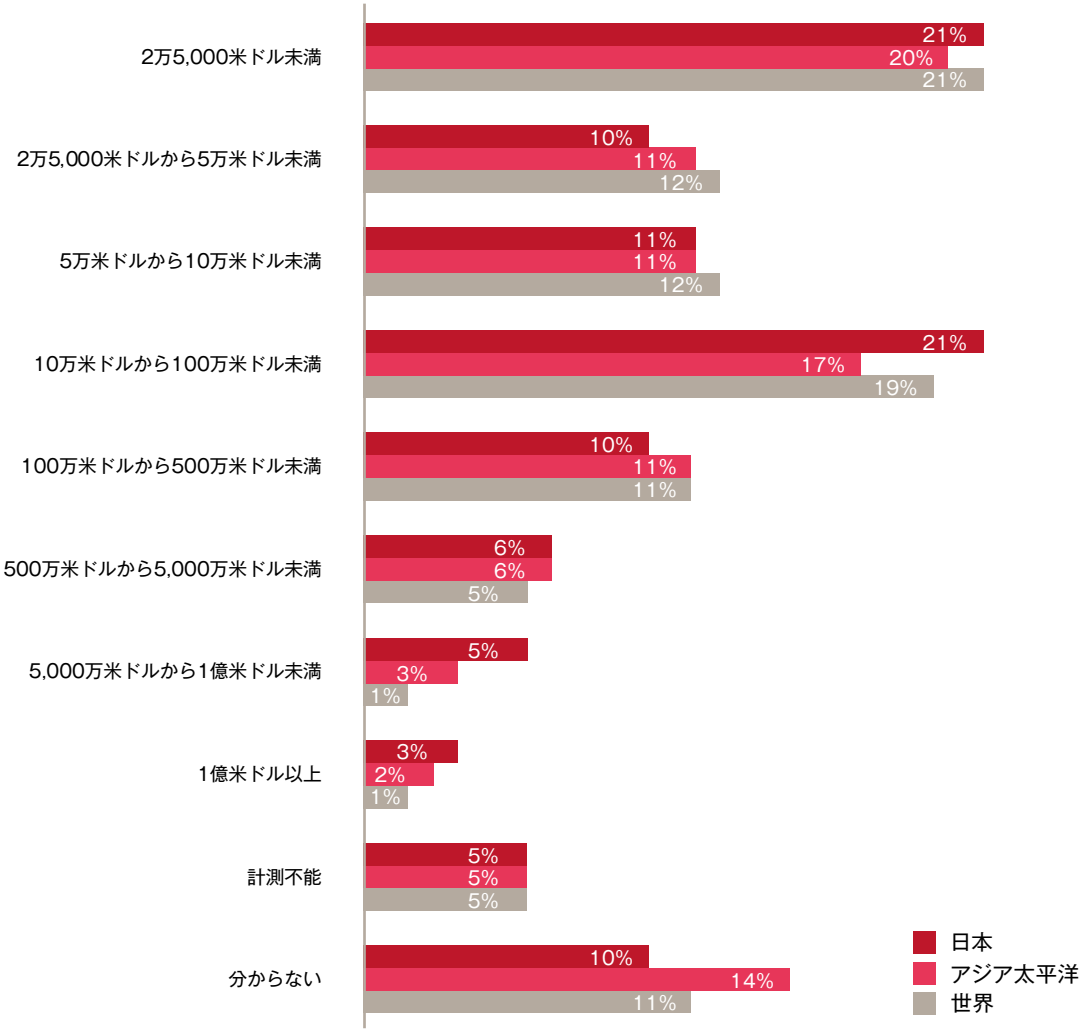
経済犯罪・不正の被害規模

調査では、過去2年間で被害に遭った経済犯罪・不正のうち、最も被害が大きかったものの直接的被害額、およびその調査など事後対応に際して発生した費用についての質問を行い、企業にとっての経済犯罪・不正による被害の実態の把握を試みた。

直接的な被害額に関しては、100万米ドル以上の高額被害であった割合は24％であり、世界全体（18％）と比較すると、前回と同様、日本では経済犯罪自体は世界平均と比べて少ないが、ひとたび経済犯罪に遭った場合の被害額は大きいという結果が出た（図3）。

事後対応の費用については、直接的な被害額との比較を求める質問を実施しており、日本と世界全体・アジア太平洋とでは傾向に大きな違いが出た（図4）。

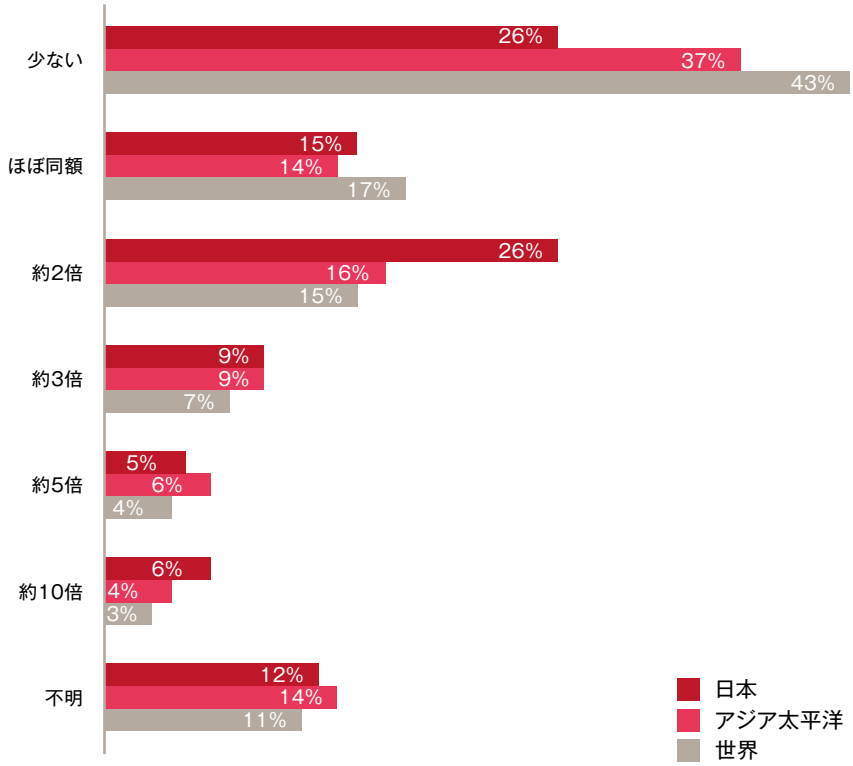
図3　過去2年間で被害に遭った最も深刻な経済犯罪被害額



世界全体・アジア太平洋では、調査などの事後対応にかかった費用の方が直接的な被害額より低い、または同等と答える企業が半数以上を占めた。一方、日本では直接的な被害額よりも事後対応費用の方が高いと答えた企業が46％にも上った（世界全体：28％、アジア全体：34％）。中には約10倍と回答した企業が6％もあった。一般的に、不正は期間が長く、また複数の事業部をまたがって行われているほど、調査にも時間および費用が掛かる傾向がある。従って、不正があったとしても早期発見することにより、事後の費用は少なくて済むといえる。

日本企業においては、不正が長期にわたっているケースや、また全社的に行われているケースが多いことから、経済犯罪による直接的な被害および事後対応にかかる費用が高額になる傾向が高いといえ考えられる。つまり、積極的に経済犯罪への予防策を実施し、不正を早期発見できる体制を構築するインセンティブがあるといって良いのではないだろうか。

図4　過去2年間で最も深刻な被害を受けた経済犯罪の被害額を基準とした際の当該事案にかかる調査などの対応費用の金額



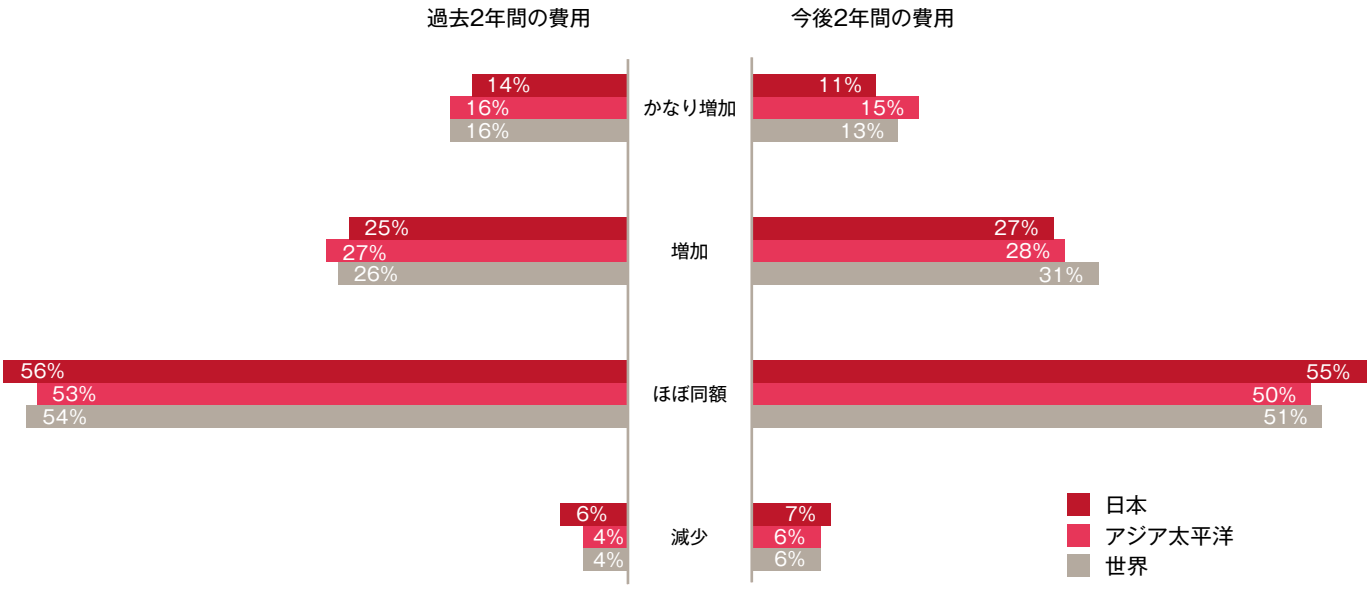
過去2年間で不正リスク評価を実施した企業は**44%**

経済犯罪・不正対応関連の費用

では、企業が経済犯罪・不正対応にかける費用（予防策と事後対応を含む）は、どうなっているだろうか。日本の回答をみると、過去2年間の実績では半数弱が増加傾向にあり、この先2年間の計画においてもその傾向は変わらない（図5）。世界全体やアジア太平洋と比較すると、かなり増加、増加と回答した比率は若干少ないものの、同じ傾向がみられる。一方で、過去2年間において実施されたリスクアセスメントに関する質問への回答をみてみると、

- 全社的な不正リスク評価を実施した企業は44%
- 贈収賄・汚職（ABAC）、マネーロンダリング（AML）、制裁措置および輸出管理といった重要分野でリスク評価を実施した企業は4分の1以下（最も高い「贈収賄・汚職（ABAC）」でも22%）
- サイバー犯罪に関するリスク評価を実施した企業は40%以下
- 約16%の企業が「過去2年間でリスク評価をまったく実施していない」と回答（世界全体・アジア太平洋と比較した際に約1.5倍の比率）

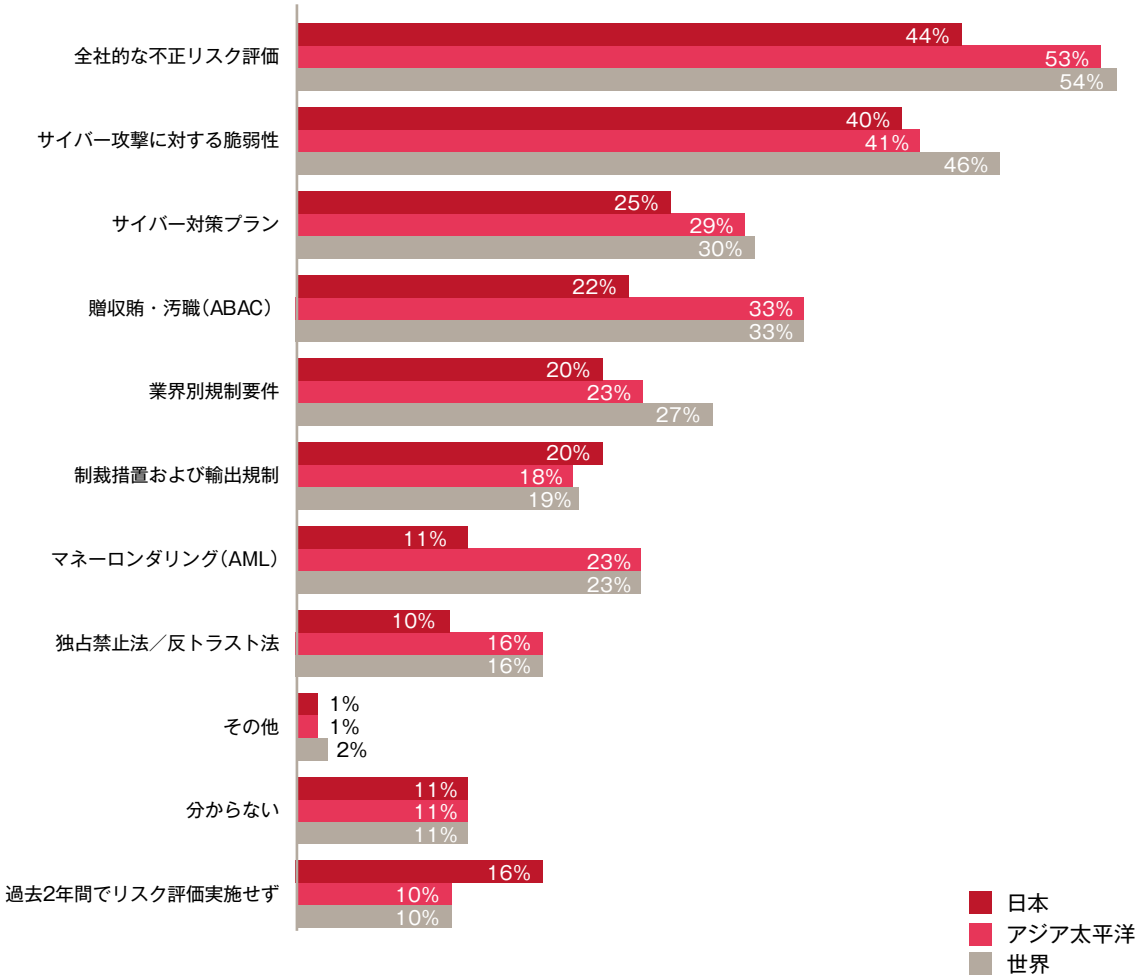
図5　企業の経済犯罪対応への費用（予防策と事後対応を含む）



となっており、企業として能動的・包括的な経済犯罪予防策を実施するための第一歩となるはずのリスクアセスメントを適切に実施している企業は、それほど多くないという結果となった（図6）。実施状況が最も良い「全社的な不正リスク評価」の結果をみても50％以下であることを考えると、増加する経済犯罪に対して十分に対応できているとはいえず、日本企業にとって大きな課題といえるだろう。

先ほども触れたとおり、特に日本企業においては、経済犯罪の直接的な被害額も、調査費用など事後的に発生する費用も高額になる傾向にあるため、適切なリスクアセスメントを実施し、その結果に基づいて予防策を構築・実行するメリットは大きいといえる。

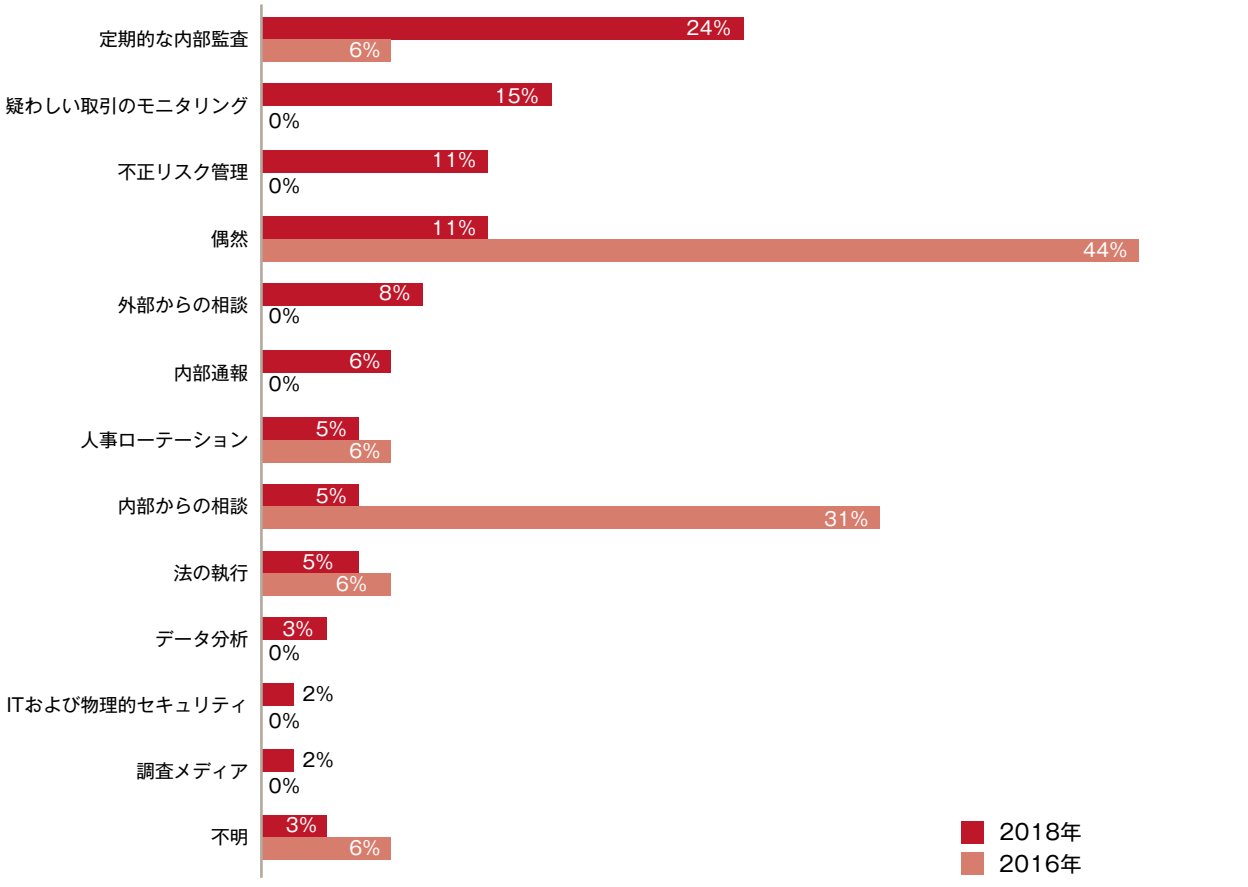
図6　過去2年間で実施したリスクアセスメント



経済犯罪・不正の発覚理由

次に、経済犯罪・不正の発覚理由についてみてみよう。前回の調査結果と比較すると、今回の調査では日本企業における経済犯罪・不正の発覚理由について大きな変化があった。前回調査では発覚理由として「偶然」との回答が目立ったが、今回の調査では「定期的な内部監査」が6％から24％、「疑わしい取引のモニタリング」が0％から15％、また「不正リスク管理」が0％から11％と上昇した（図7）。「偶然」による発見から、不正検知プログラムの一環による不正の発見にシフトしてきていることは、大きな進歩といえる。これは、先ほどの「経済犯罪・不正対応関連の支出」の箇所でもみたとおり、過去2年間で半数近くの企業が経済犯罪・不正対策として何らかの対応をとってきたことが、功を奏しているとも考えられる。昨今、データ改ざん、安全品質、入札談合を始めとした企業の不正に対する摘発事案が頻繁に取り上げられているが、これらの摘発を受け、今後企業による不正に対する意識がさらに向上し、企業が積極的に内部監査、モニタリング、リスク管理などの体制を見直し、さらなる強化を行うきっかけとなることを望む。

図7　最も被害が深刻だった経済犯罪の発覚理由



経済犯罪・不正の主犯者のプロファイル

それでは、経済犯罪・不正の主犯者の特徴はどのようなものだろうか。世界全体やアジア太平洋と比較すると、日本においては組織の内部者による犯行の割合が高い結果となった。しかしながら、前回の調査と比較すると、日本における内部者による犯行の割合は88％から72％と大きく下がっている（図8）。その原因の一つとして考えられるのは、サイバー犯罪の増加だろう。サイバー犯罪は、基本的に組織外部の人間が、組織のセキュリティの脆弱な部分につけ込んで攻撃を行うものであるからである。

また、世界全体との比較で目立つのが、主犯者の所属である。日本の場合、27％が「営業部」の人間となっており、世界全体の14％、アジア太平洋の15％と比較して2倍近い結果となった（図9）。これは、最初にみた「経済犯罪・不正の種類」において、日本では財務報告の不正が多いという事実と表裏一体である。つまり、営業部所属の従業員が、売上目標達成のプレッシャーから、架空売上や売上の前倒しを行った結果、財務報告に関する不正が多くなっていると考えられるためだ。

図8　経済犯罪の主犯格（2016年、2018年）

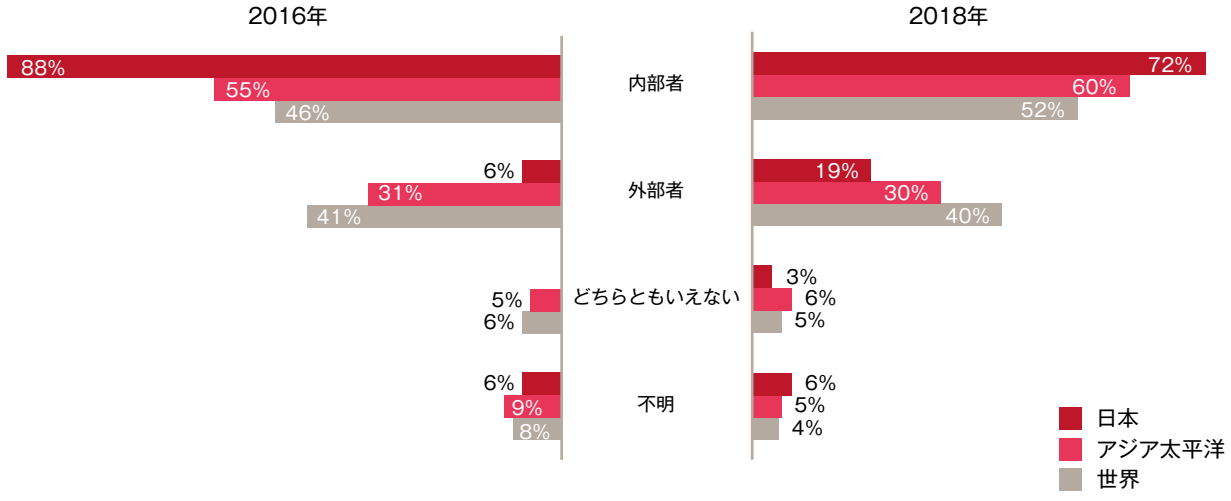
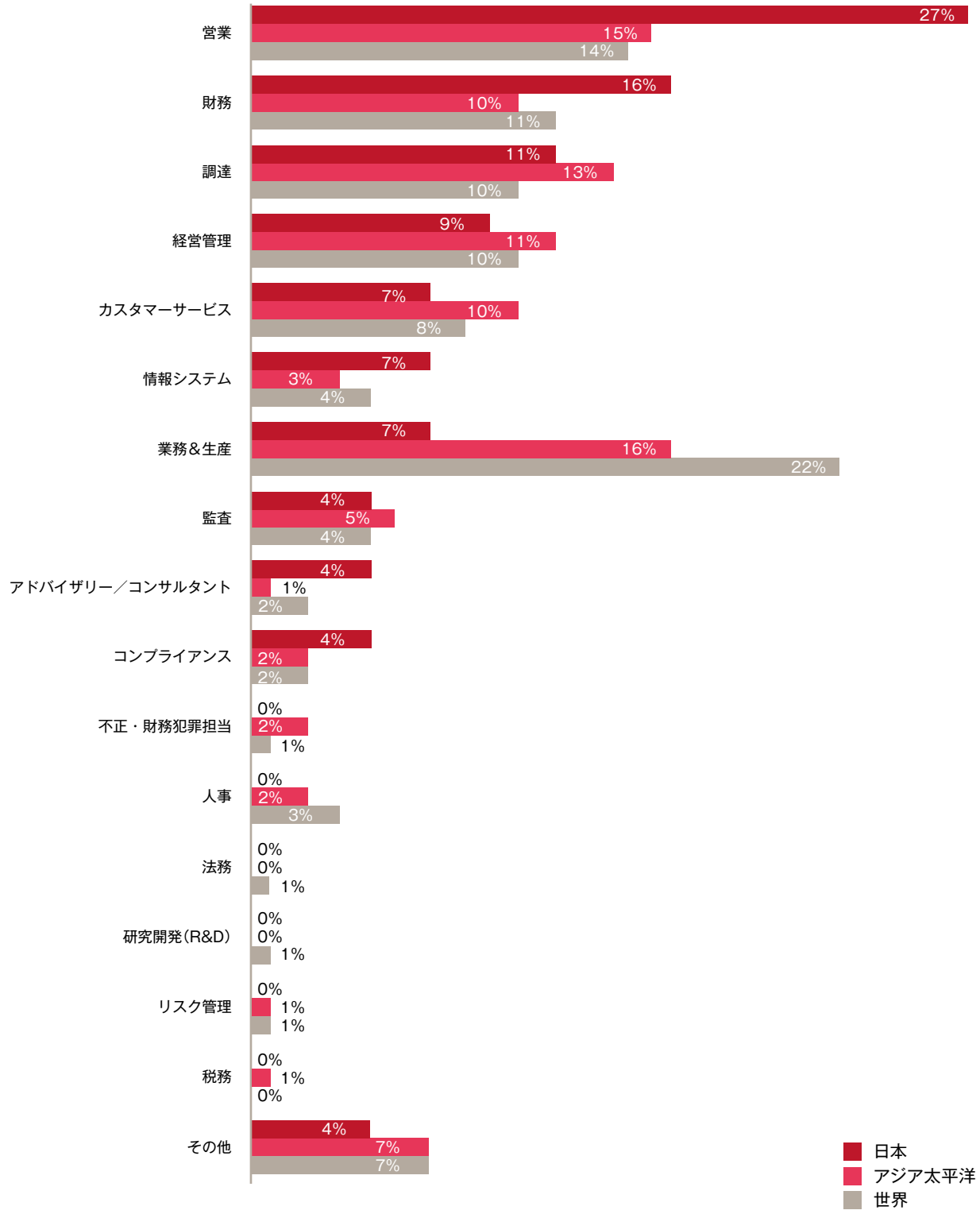
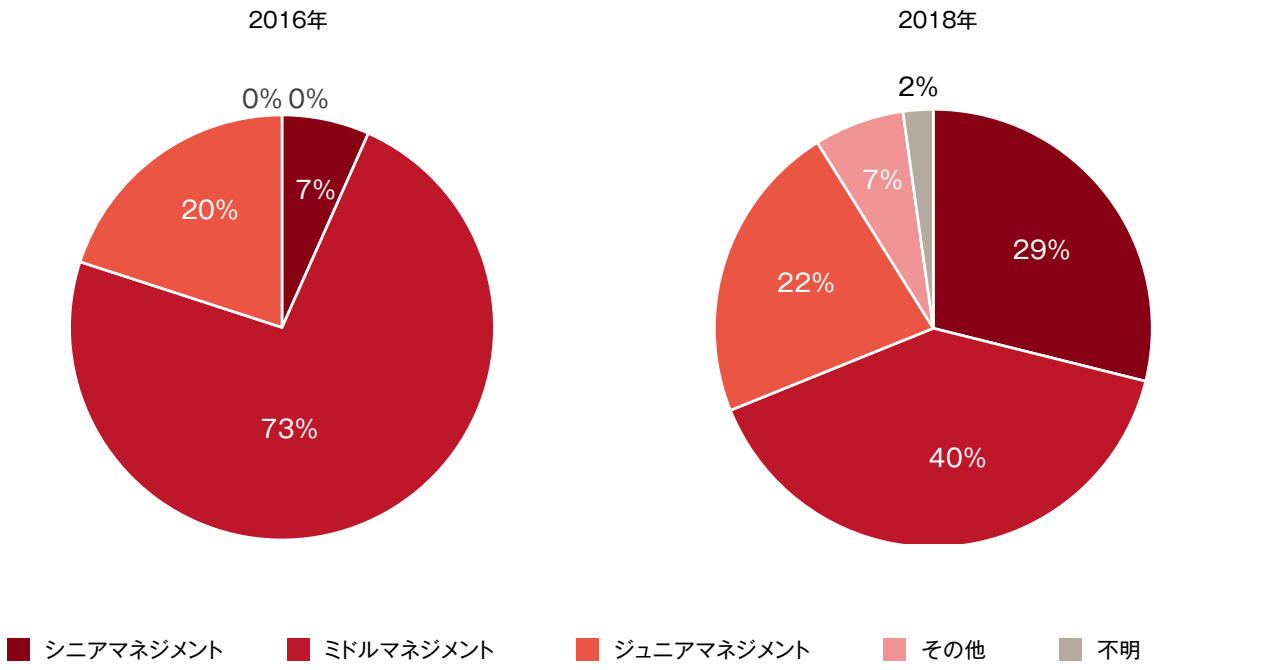


図9　経済犯罪の内部主犯格の所属内訳（2018年）



また、日本における経済犯罪・不正の主犯者の職階について前回の調査時と比較すると、「ミドルマネジメント」による経済犯罪が73％から40％に減少し、「シニアマネジメント」が7％から29％と増加した（図10）。この結果から、経済犯罪の主犯格がマネジメント層の中でもより高い職階に推移していることが分かる。従前から、「海外に比べ日本では勤続年数が長く、年齢・職位が高い社員による経済犯罪が多い」という調査結果が出ているが、この傾向がより強くなった。経営陣による不正については、内部統制が有効に働かないことから防止・発見することが難しく、不正が長期にわたり行われることが多くなるため、被害額が大きくなるケースが多い。このことも、日本で1件あたりの被害額が大きくなる理由の一つといえるだろう。

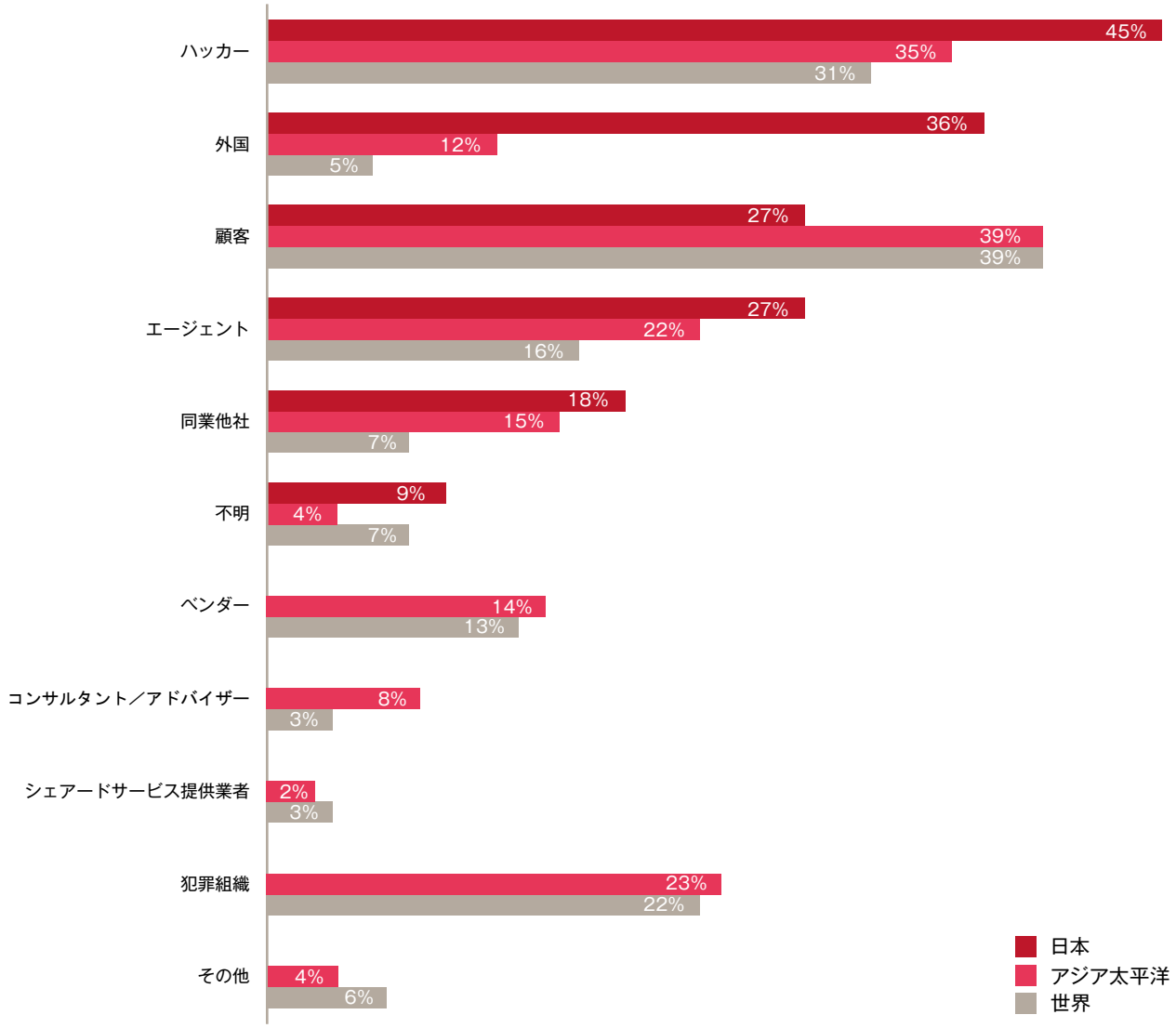
図10　日本における経済犯罪・不正の内部主犯格の職階内訳（2016年、2018年）



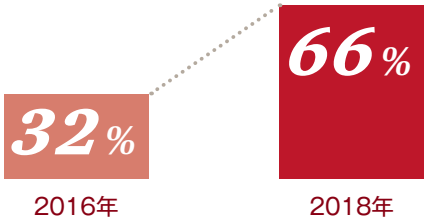
さらに、「外部」の主犯格の特徴をみてみよう。既にみたように、「外部」から経済犯罪の被害に遭ったと回答した日本企業は6％から19％と増加した。その内訳は、「ハッカー」が45％、次いで「外国」が36％、さらに「顧客」「エージェント」がそれぞれ27％で3位という結果になった（図11）。

テクノロジーの進歩は目覚ましいものがあり、新たなサイバー攻撃手法が次々と編み出される中で、それを100％未然に予防することは不可能かもしれない。しかしながら、例えば従業員に対してフィッシングやマルウェアによる攻撃に引っ掛からないよう教育を徹底したり、万が一攻撃に遭った場合に素早く検知するためのシステムに投資したりするなど、できる限りの手だては打っておくべきであろう（サイバー犯罪についての詳細は次章参照）。

図11　経済犯罪の外部主犯格の内訳（2018年）



サイバーセキュリティプログラムを完全に運用している

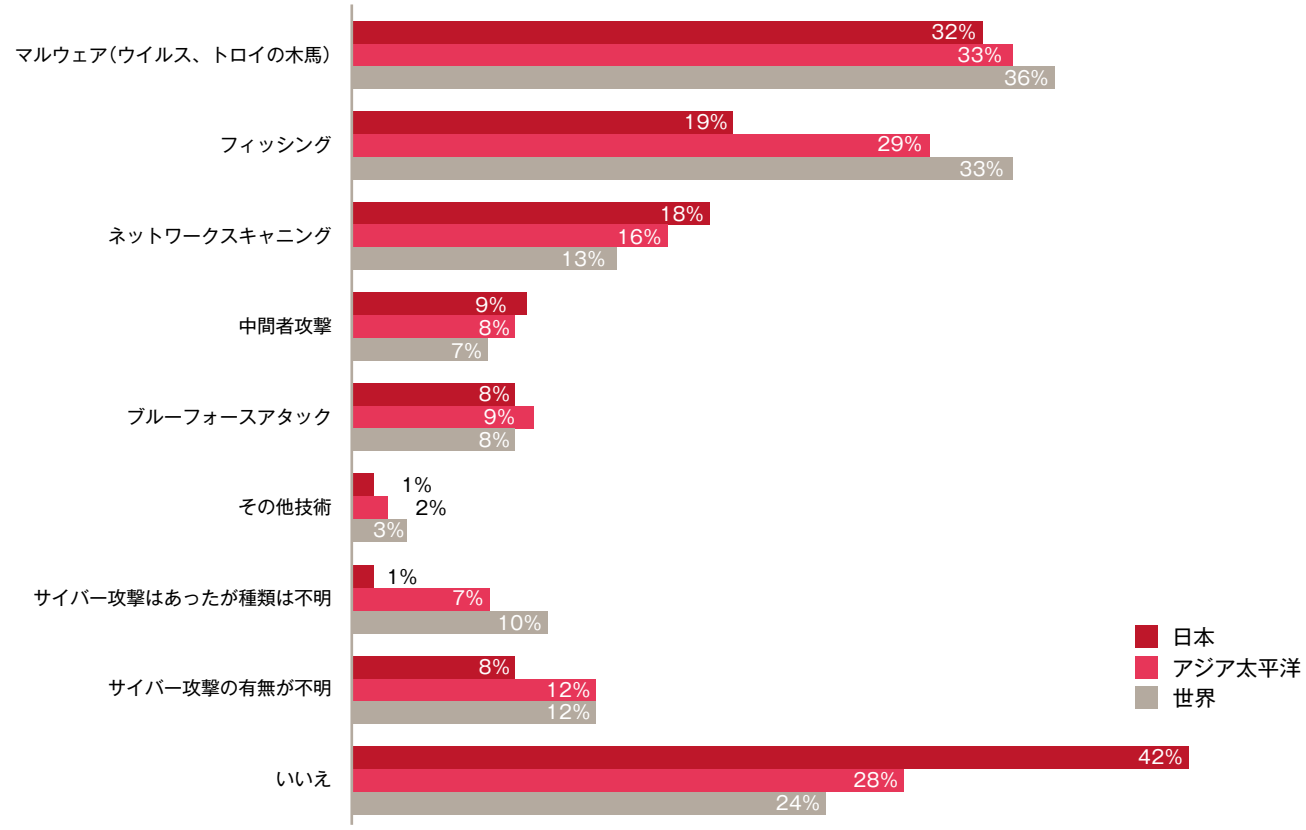


サイバー犯罪：目的と手法の乖離／テクノロジーの防御力を活用

日本企業におけるサイバー攻撃の被害は年々増加しており、過去2年間でサイバー攻撃の対象になったことがあると回答した日本企業は全体の約半数に上り、その手法もさまざまとなっている。本調査ではマルウェアによる被害を受けたと回答した企業が最も多く、全体の32％を占め、次にフィッシングの19％、ネットワークスキャニングの18％と続いている（図12）。

企業がサイバー攻撃による財務的影響を正確に測定することは難しいかもしれないが、「サイバー犯罪が最も致命的な不正である」と答えた回答者の13％が、同不正により100万米ドル以上の損害を被ったと述べている（図13）。サイバー攻撃によって個人情報や技術情報などが漏えいした場合、場合によっては巨額な損害賠償を支払わなければならないケースもあるため、損害金額は計り知れないものになると考えられる。

図12　過去2年間のサイバー攻撃の有無とその種類



サイバー攻撃の狙いとなった不正の類型としては、「サイバー恐喝」と回答した企業が最も多く31％、次に知的財産（IP）の盗難が25％となっている（図14）。

ランサムウェアなど、データを人質に身代金を要求するような「サイバー恐喝」は、一見無害なEメールやウェブサイト経由で一気に感染が広がりやすく、さらに共有リソースを介して二次、三次的な被害も発生することが多い。最近では、個人ユーザーの被害に加え、企業や組織における被害も増えている。特に日本企業では従業員のセキュリティ意識が低いため、社内での情報セキュリティ教育強化などの対策をしっかりと行っていくことが重要である。

図13　サイバー犯罪による被害金額（日本）

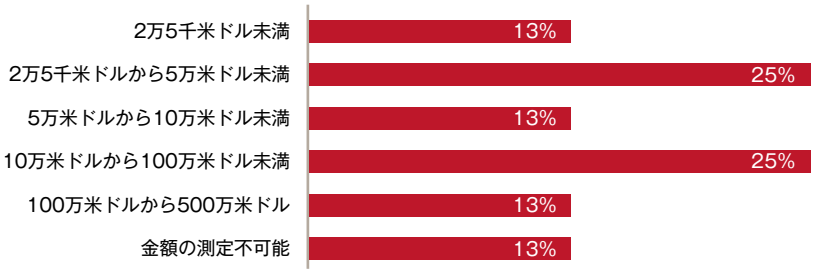
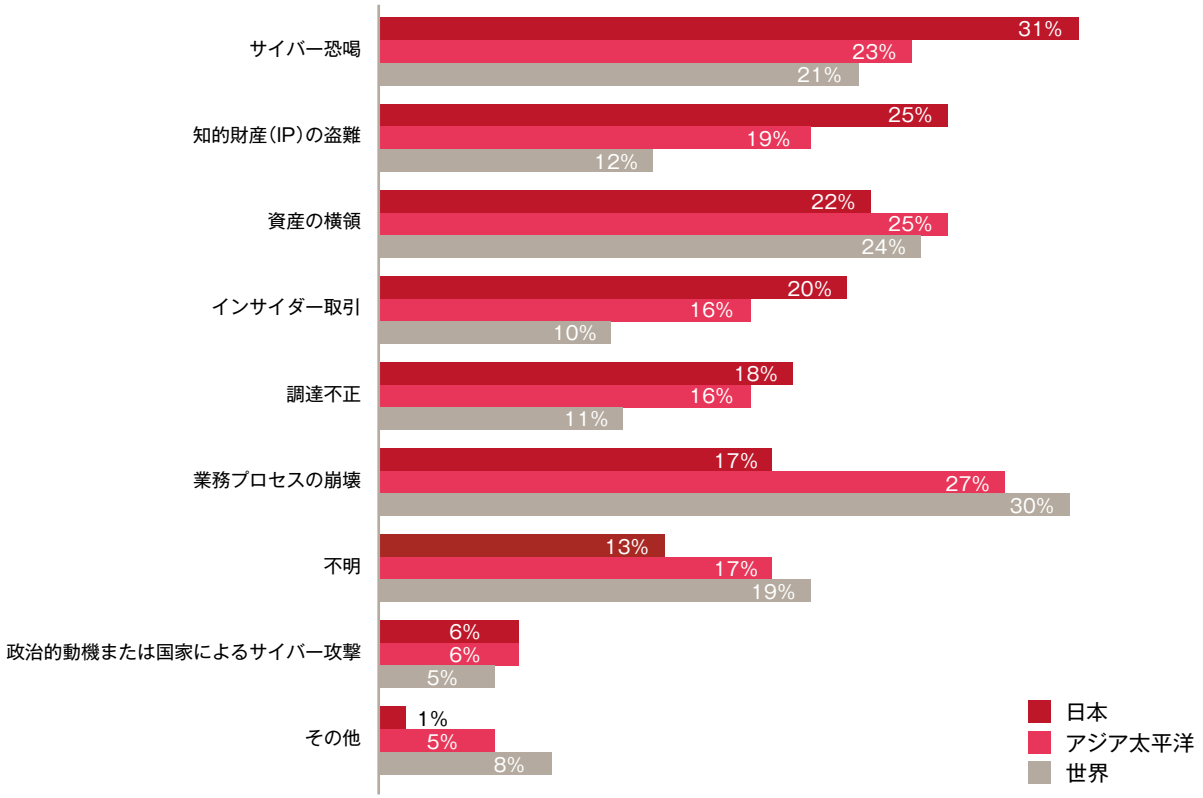


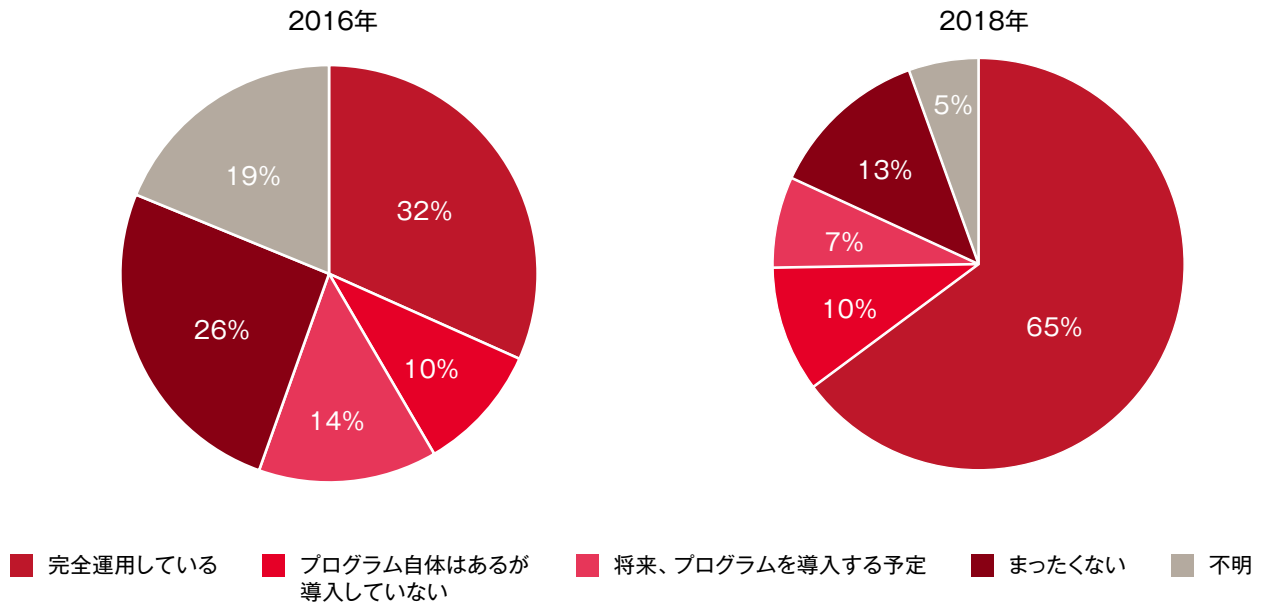
図14　組織がサイバー攻撃の狙いとなった不正の種類



知的財産（IP）の盗難については、世界全体の結果である12％と比べると日本では顕著に多いという結果になった。これは日本企業の知的財産（IP）の重要性に対する認識が低く、従業員が企業のネットワーク外のパソコンへ情報を共有するなど情報管理が適切でないことや、そもそも知的財産（IP）を含めた情報セキュリティシステム全般が脆弱であることが要因であると考えられる。実際、サイバー攻撃は年々増加しており被害も拡大しているため、未然に防ぐためには不正行為者が用いるメカニズムに焦点を当て、手法を分析し、それを上回る対抗措置をとる必要がある。しかしながら、テクノロジーの進歩は目覚ましいため、企業がどれほど対抗措置に費用と時間を費やしても、新たなサイバー攻撃を全て防ぐことは難しい。そのため、防御だけでなく、攻撃を受けた時にいかに早くそれを検知し、被害を最小限に食い止めるか、という部分についても注力し、バランスよくリソースを配分することが肝要と考える。

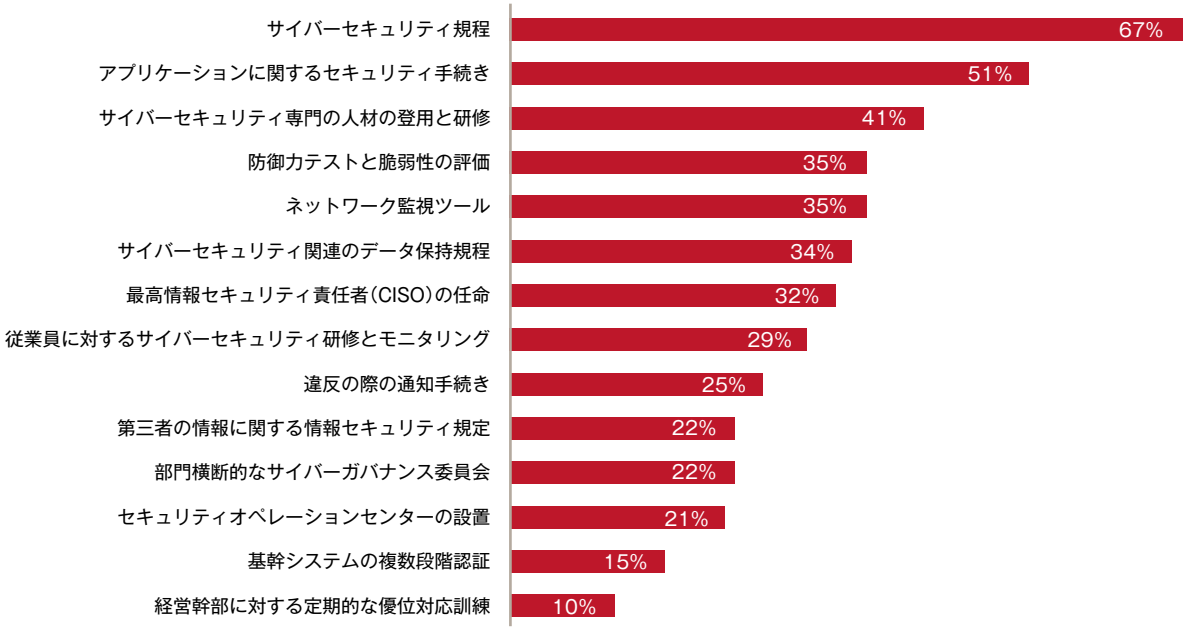
サイバー攻撃の被害の増加を受けて、実際に社内でサイバーセキュリティプログラムを整備し、運用していると回答した日本企業は65％となり、2016年の前回調査からは33％増加している（図15）。これは、図2（7ページ）で示したようにサ

図15　サイバーセキュリティプログラムの有無について



イバー攻撃の被害に遭ったと回答した企業が3倍になっていることから、当然の結果と受け取れる。各企業が整備・運用しているプログラムの例としては、サイバーセキュリティ規程の制定やアプリケーションセキュリティの管理、サイバーセキュリティ人材および研修などが含まれている（図16）。

図16　サイバーセキュリティプログラムの内容



また、サイバー攻撃を受けた際に、被害に関する情報を政府・行政機関と共有する可能性については、日本は世界全体と同様の結果となっており、約6割の企業が情報を共有すると回答している（図17）。その反面、情報共有するか分からない、あるいはその可能性が低い場合の理由として、「無秩序に情報が公開される懸念がある」あるいは「政府機関の専門性に懸念がある」という回答が高くなっている（図18）。

図17　サイバー攻撃（やその疑い）があったことについて政府や行政機関に共有する可能性は？

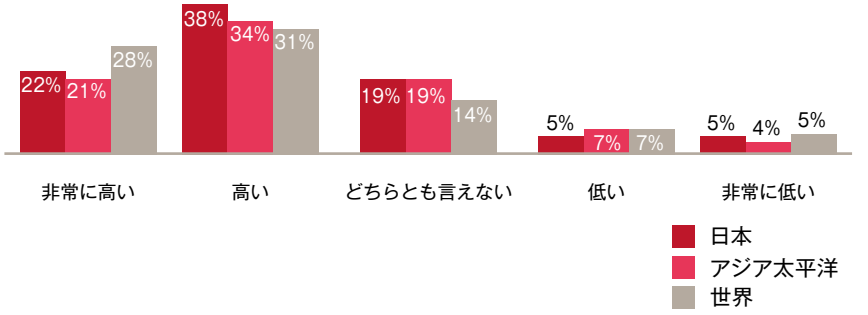
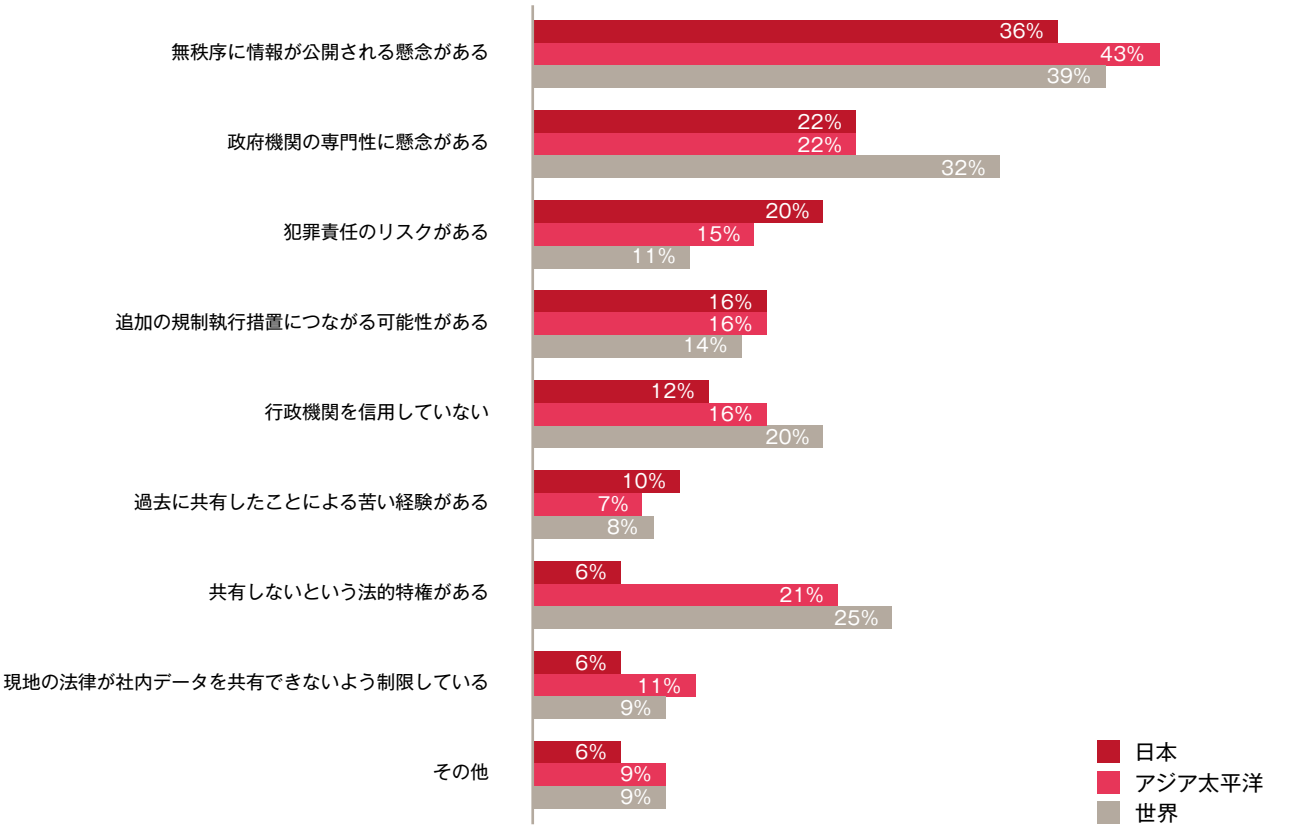
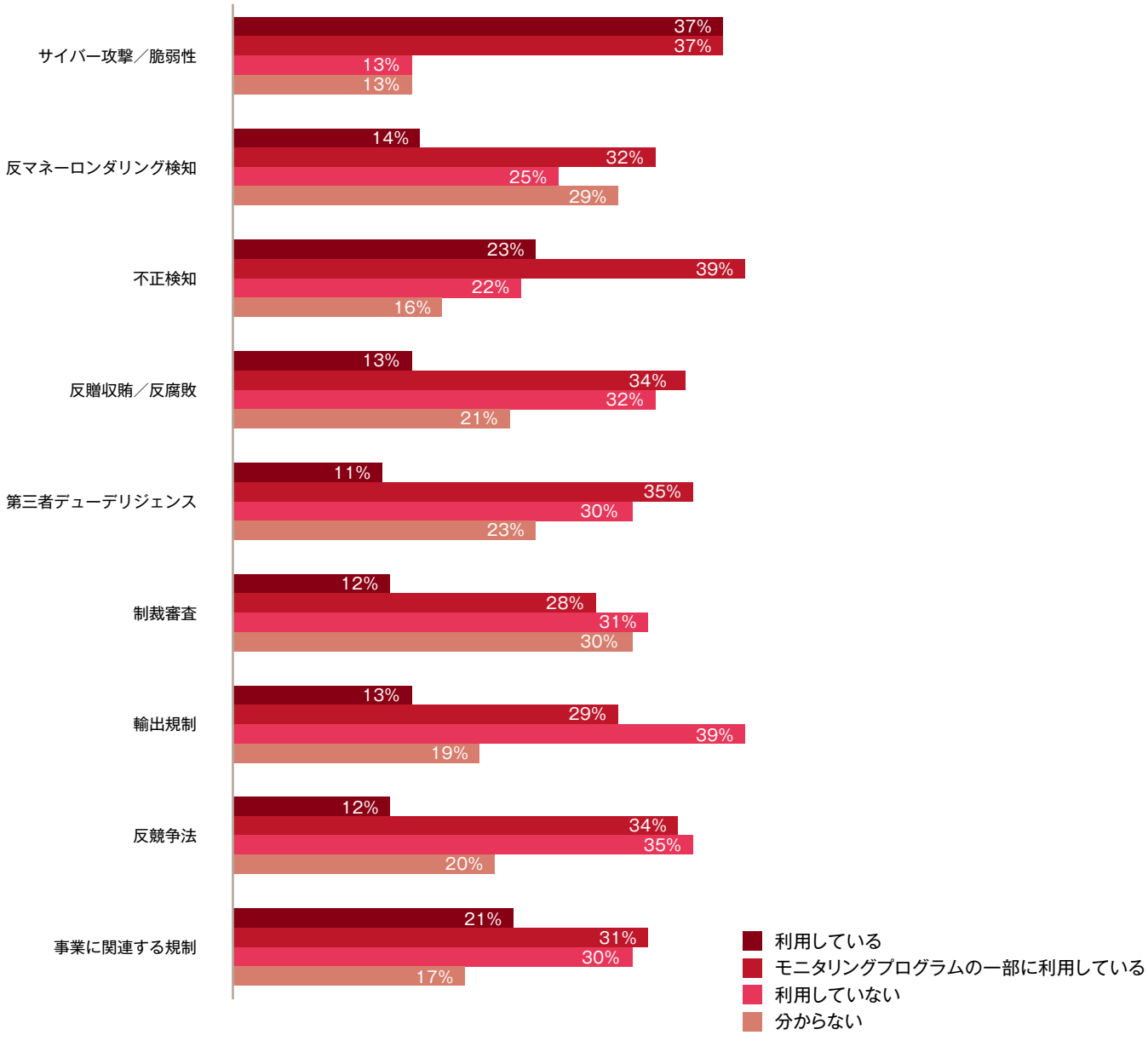


図18　政府および行政機関に情報を共有しない要因



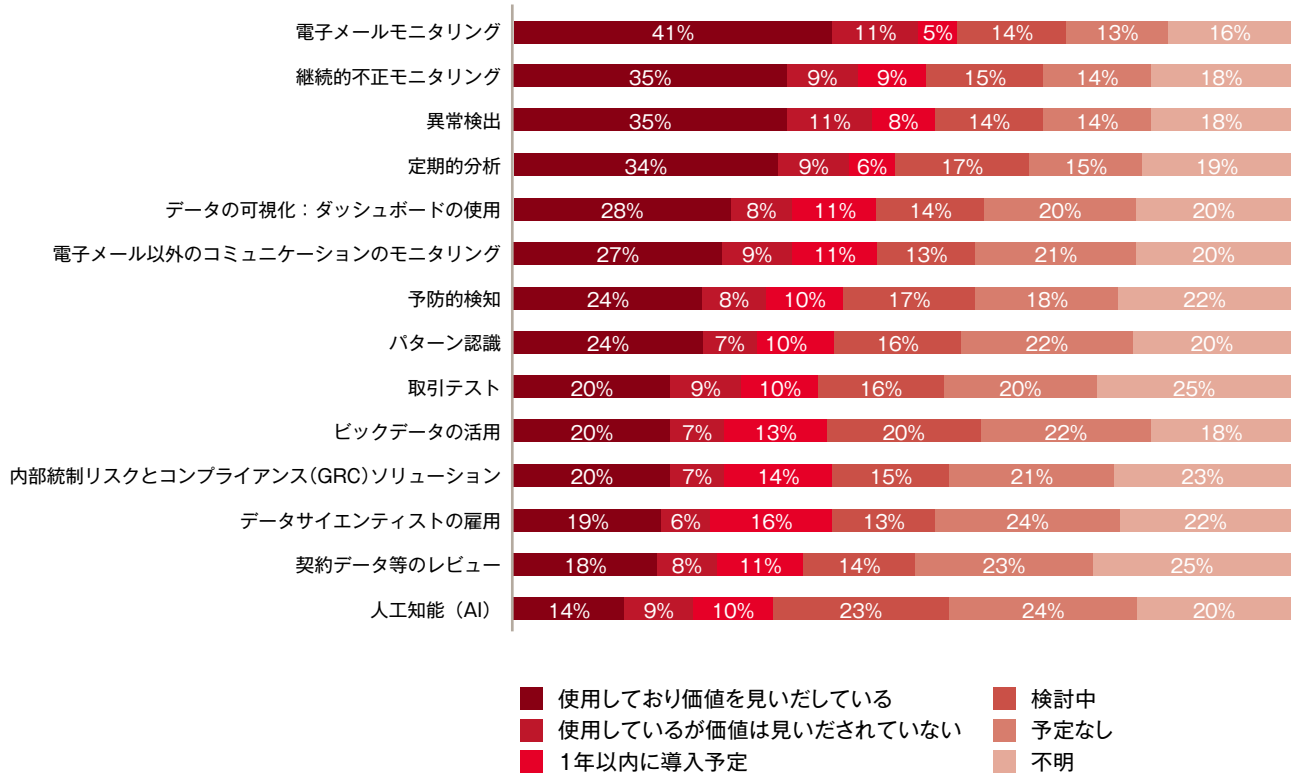
現在、企業は革新的で高度なテクノロジーを利用して、サイバー攻撃だけでなく、不正全般から自らを守り、行動の監視、分析、学習および予測を実施しようとしている。その手法として近年話題となっている、機械学習、予測分析、その他人工知能（AI）などを利用したものが挙げられる。その実例の一つとしてAIなどのテクノロジーを使用した不正のモニタリングがある。モニタリングによって不正を検知する項目の中ではやはりサイバー攻撃や脆弱性への対応など、テクノロジー依存型の不正に対して利用しているという回答が一番多く37％という結果になっているが、他方一般的な不正の検知としてもその効果が期待されていることが読み取れる結果となった（図19）。

図19　テクノロジーを利用した不正監視の状況（日本）



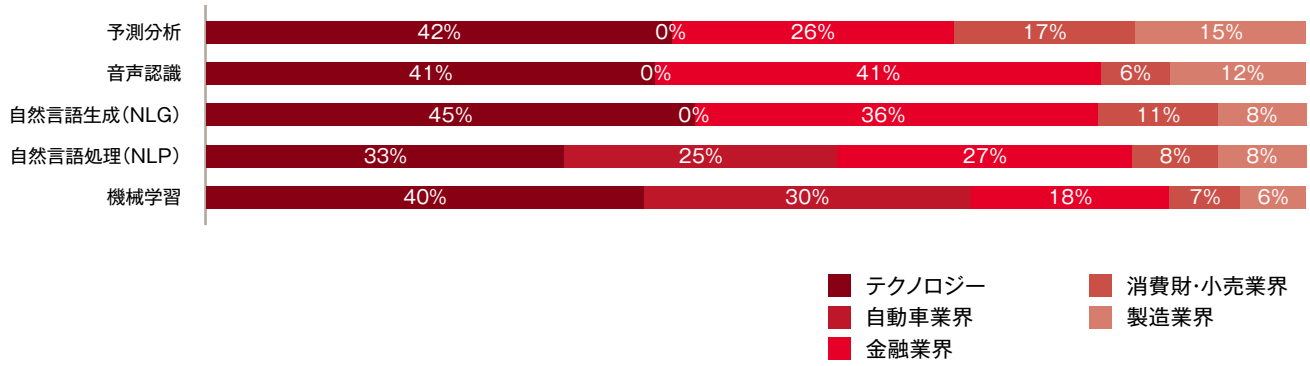
また企業は不正対策として、統制環境においても革新的なテクノロジーを活用してきており、その中でも電子メールのモニタリングに関しては、活用し価値を見いだしていると答えた回答者は41％にも上った。また、昨今話題となっているビッグデータの活用が20％、人工知能（AI）の活用が14％という結果であった（図20）。ただし、使用しているが価値が見いだされていないとの回答も一定割合を占めるため、今後導入予定の企業は、既にうまく活用ができている企業の事例を参考にして、自社においてどうすればうまく活用できるかを慎重に検討した上で導入すべきであろう。

図20　不正対策として活用している（活用予定の）テクノロジー（日本）

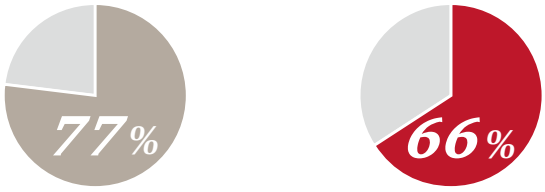


テクノロジーを導入し、運用するには多額のコストがかかるため、一部の企業ではそれらに投資する余裕がない場合があり、また、導入するテクノロジーの種類や導入時期を判断するのも難しい。不正の事前防止の観点から革新的なテクノロジーに対して投資したものの、それをうまく活用できない可能性も考えられる。業界別の活用状況を鑑みると、やはりテクノロジーや金融業界においては活用されている割合が高いが、消費財・小売業界や製造業界など、現状では新しいテクノロジーを活用しきれていない業界へ、いかに浸透させていくかが注目すべきポイントといえる（図21）。

図21　不正その他経済犯罪犯罪への対応や監視策としてのテクノロジーの活用状況業界別（日本）



コンプライアンスプログラムを有する企業

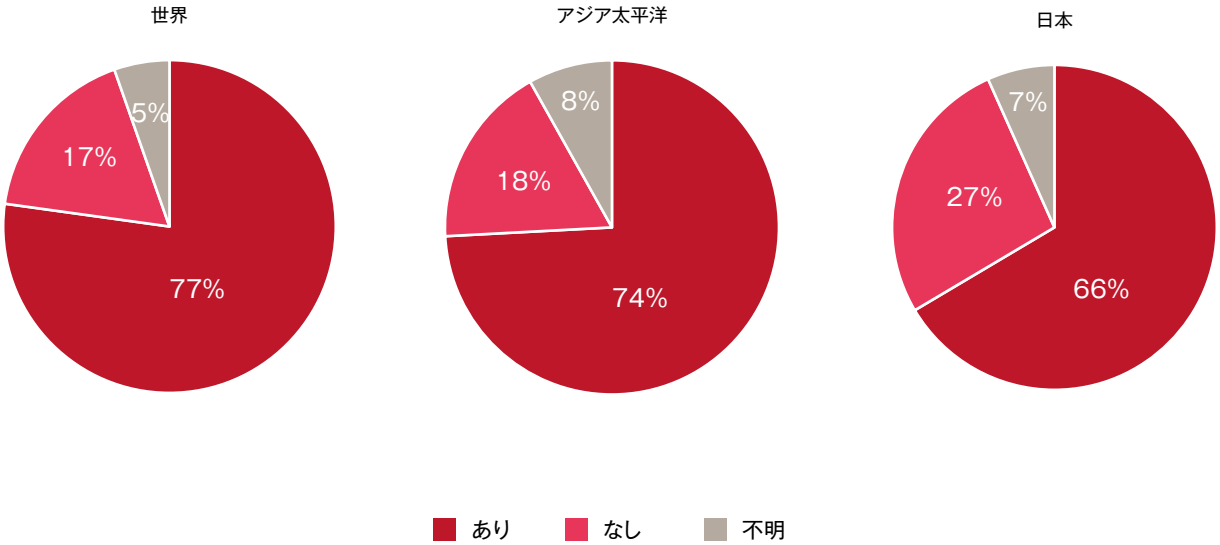


企業を取り巻く不正リスクの把握および対応

贈収賄などの不正への危機意識は高い水準にある一方、経営層の関与が低い

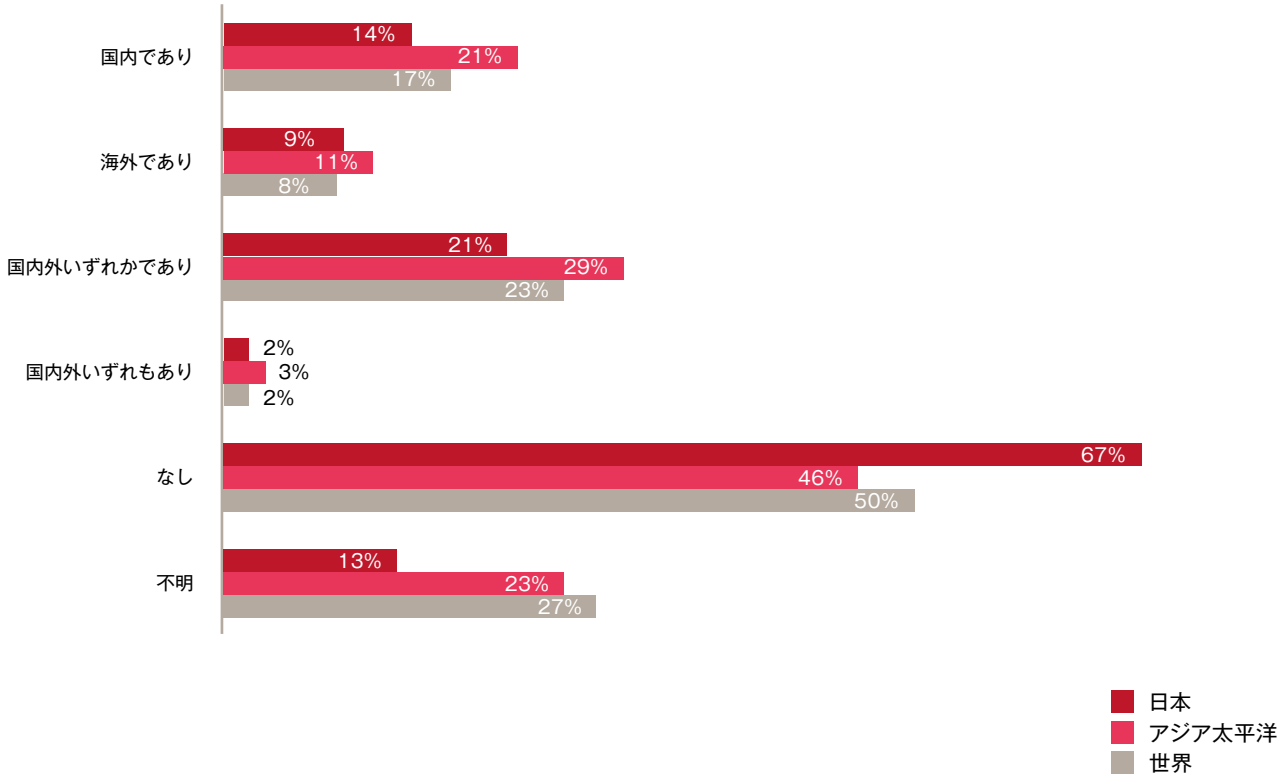
今回の調査で、約66％の日本企業が企業倫理およびコンプライアンスに関する社内プログラムを有していると回答したが、アジア太平洋地域の約74％、世界の約77％と比較すると若干低い水準にとどまった（図22）。また、コンプライアンスプログラムがないと回答した企業は約27％と、世界・アジア太平洋地域と比べて高い水準となっており、経済犯罪の被害に遭う企業が増えている中で、コンプライアンスプログラムの整備が後手に回っている状況が読み取れる結果となった。他方、約36％の日本企業が過去2年間に不正あるいは経済犯罪の被害に遭っており、その中で過去2年間に国内外で賄賂を要求されたと回答した企業は、約21％と前回調査時の5％を大きく上回った（図23）。これらの結果は世界の水準と比較しても決して低くなく、また特に海外規制当局による取り締まりが厳しくなっ

図22　企業倫理およびコンプライアンスに関する社内プログラムの有無（2018年）



ていることから、日本企業においても相当程度の管理体制の整備が求められているといえる。

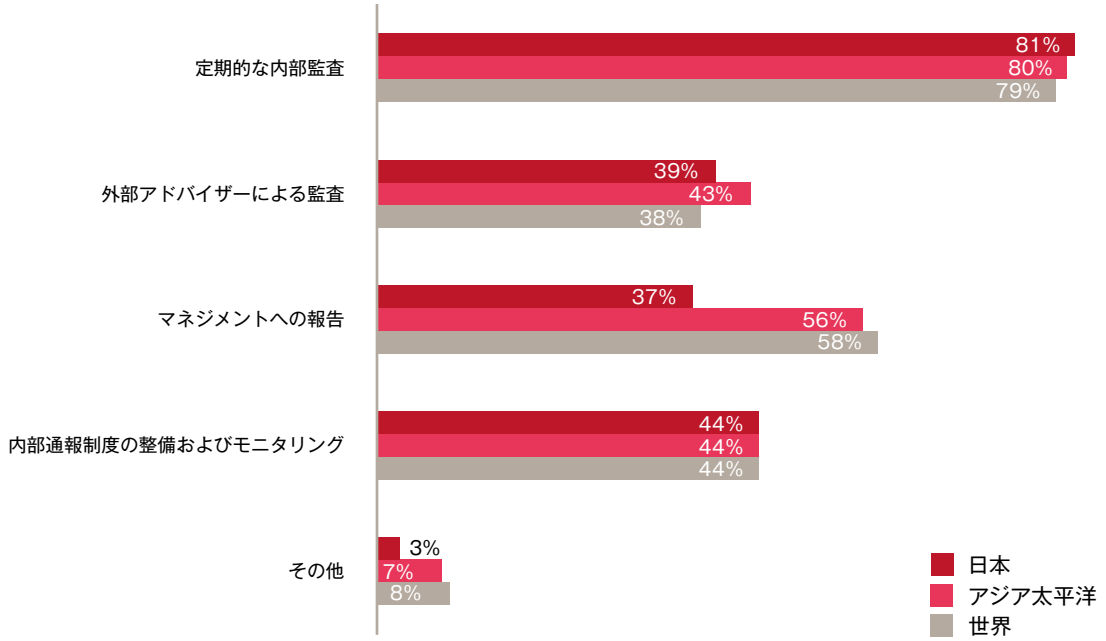
図23　過去2年間に国内外で賄賂の要求を受けたか（2018年）



倫理・コンプライアンスプログラムがあると回答した日本企業については、主に定期的な内部監査（約81％）、内部通報制度の整備およびモニタリング（約44％）、外部アドバイザーによる監査（約39％）、によりプログラムの有効性の確認を行っているという集計結果が出た（図24）。

一方で、経営陣に対して倫理・コンプライアンスプログラムの有効性に関する報告を行っている日本企業は約37％にとどまり、世界・アジア太平洋地域と比べても低い水準となっている。経営層がプログラムの有効性の担保に向けた活動に関与していない実態がうかがえる。近年、日本の大手企業における会計不正やデータ改ざんなどの不正が表面化しているが、経営陣の不正に関する認識の甘さや対応の不備・遅れなどが問題視されている。不正の監視、社内のコンプライアンスの周知徹底に最終的な責任を持つ経営陣が、コンプライアンスプログラム策定および周知のみだけではなく、現状のプログラムへの有効性の確認とその結果に基づく改善策の検討などに積極的に関与する姿勢が重要である。

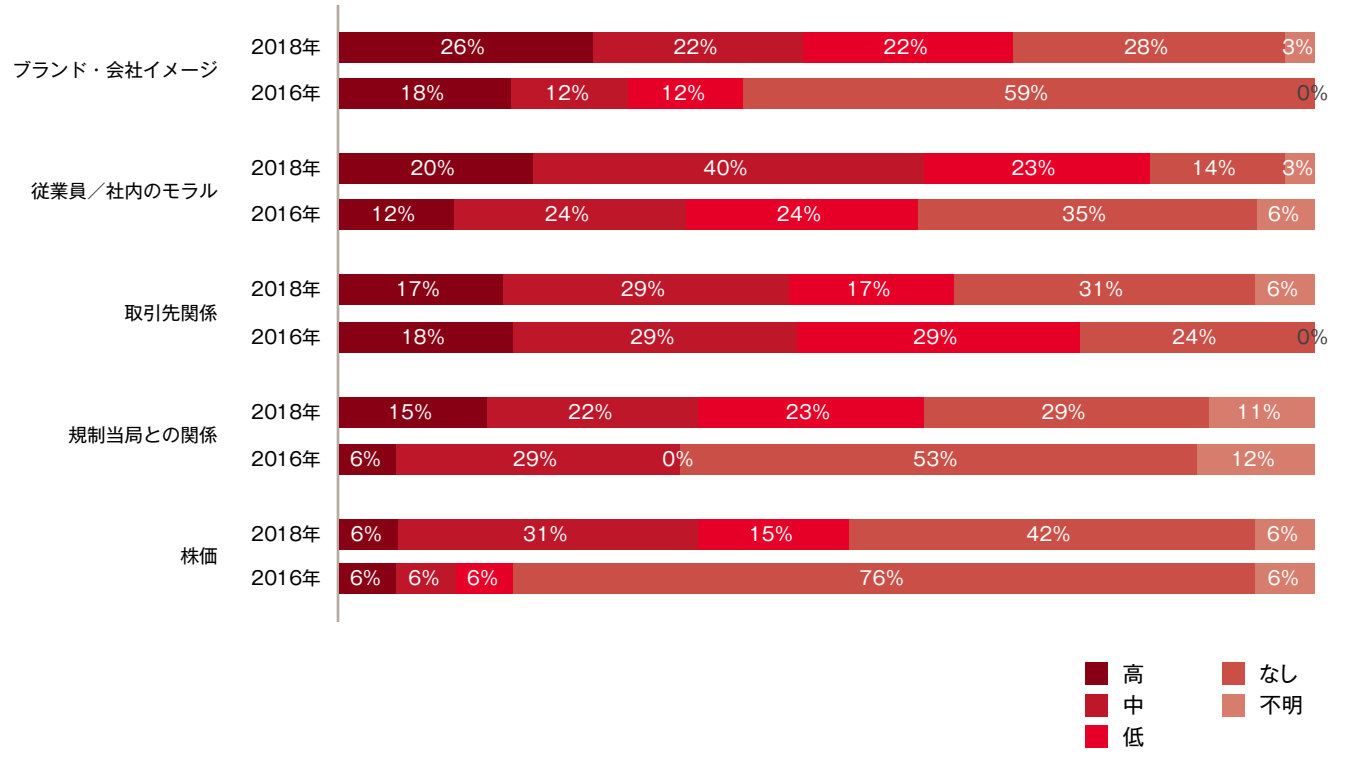
図24　企業倫理およびコンプライアンスに関する社内プログラムの有効性の確認方法（2018年）



経済犯罪・不正の発生によりどのような影響を受けたかという質問に対して、前回と比較して大きな変化があった。特に、2016年には、ブランドや会社イメージへの影響は「ない」との回答が約6割だったのが、今回調査では7割が「ある」と回答し、そのうちの3分の1は影響度が高いと回答している（図25）。また、株価への影響をみても、前回調査では76％が「ない」と回答していたが、今回「ない」と回答したのは42％に減少している。昨今では、企業で不祥事が起こるとマスコミなどで大々的に報道され、世論からも厳しい目が向けられることが多いことからこのような結果になったと推察される。

長年かかって築いてきたブランドや企業イメージは、一つの不祥事によって大きく毀損する可能性がある。そしてそれを回復するには多大な努力と時間がかかる。組織としては、不正を未然に防ぐシステムの構築、不正が起きた場合にできる限り早く検知するシステムを構築するだけでなく、不正を検知した場合にいち早くその中身を精査し、経営陣に対して迅速に報告し、経営陣はそれを隠蔽しようとしたり過小評価せずに、適切に開示などの対応をとることが肝要である。それにより、不正や不祥事がたとえ起きたとしても、直接的な被害額以上の損害を会社に与えることなく、被害を最小限に食い止めることができるのではないだろうか。その点において、経営陣の役割は非常に大きいといえる。

図25　経済犯罪･不正の発生に伴い、下記の項目にどの程度影響を及ぼしましたか?



過去2年間で当局の査察により、反マネーロンダリング体制の不備・脆弱性に関する指摘を受けた企業：**40%**

厳格化するマネーロンダリング規制

近年世界では、依然続く国際的テロ組織によるテロ活動や金融犯罪の複雑化、北朝鮮やイランなどの核開発問題などを受けて、以前にも増してマネーロンダリング対策（Anti-Money Laundering／AML）やテロ資金供与対策（Counter-Financing of Terrorism／CFT）にかかわる規制および取り締まりが強化されている。また、ビットコインなどの仮想通貨を用いた違法資金の取引の増加が懸念されており、多くの政府機関が仮想通貨を対象とした新たな規制の整備を進めている。日本でも、2017年4月に、仮想通貨を扱う取引業者に対して取引時の取引目的や顧客の確認などを義務付ける旨の法改正が行われた。

2014年、FATF（Financial Actions Task Force／資金洗浄に関する金融活動作業部会）は、日本のAML／CFTへの対応の遅れを指摘した。日本では、FATFからの指摘および世界における取り締まりの強化を受けて、2016年10月に犯罪収益移転防止法（犯収法）を改正した。犯収法は、銀行などの金融機関だけではなく、不動産や宝石・貴金属の売買を行う者、電話受付・転送サービス業者、弁護士、会計士など幅広い業界・業種に対して適用される。この改正では、取引の目的や職業・事業内容などの既存の取引時確認の要件に加え、顧客の本人確認の際に用いる書類および確認方法の厳格化、法人顧客の場合は個人にまでさかのぼった実質的支配者（Ultimate Beneficiary Owner／UBO）の確認が義務付けられた。また、新たに外国で重要な公的地位を有する者（Politically Exposed Person／PEP）との取引がハイリスク取引として厳格な取引時確認の対象となり、外国為替取引を行う金融機関に対しては、コルレス契約の締結先となる海外の金融機関へのAML／CFT体制に関するデューデリジェンスを義務付けている。さらに犯収法の対象となる企業には、犯罪収益移転危険度調査書などを用いたリスク評価を実施する義務が新たに定められたほか、AML／CFT関連規定の策定や統括管理者の選任など社内の体制整備に向けた努力義務が設けられた。

今回の調査では、金融機関などの対象日本企業のうち、70％以上が日本国内あるいは海外のAML法の規制対象となっていると回答した（図26）。しかし、実際に過去2年間でAML／CFTにかかわるリスク評価を行った企業は全体の36％にとどまり、世界・アジア太平洋地域に大きく後れをとっている（図27）。また、40％の企業が過去2年間に当局の査察を受け、現状の体制に関する重大な指摘があった、あるいは是正に向けた対応を行っていることが判明した（図28）。犯収法などの国内AML／CFT関連法・規制の厳格化を踏まえ、国内における査察・取り締まりが活発化していくと予想されるほか、米国の財務省（Department of Treasury）を中心とした海外当局の取り締まりも強化されていることから、日本企業においても社内のAML／CFT体制の構築と整備が急務となっている。今回の調査では、今後1年間から2年間でリスク評価を行う予定としている企業が他の地域と比較しても多いほか、リスク評価を「必要ない」と回答した企業も前回の調査時から大幅に減少（50％→9％）しており、問題意識が高まっていることがうかがえる。ただし、AML／CFT規制は流動的な部分もあり複雑であるため、体制の構築・整備においては専門家を交えた協議、対応を行っていくことが重要である。

図26　国内外のAML規制の対象となっているか否か

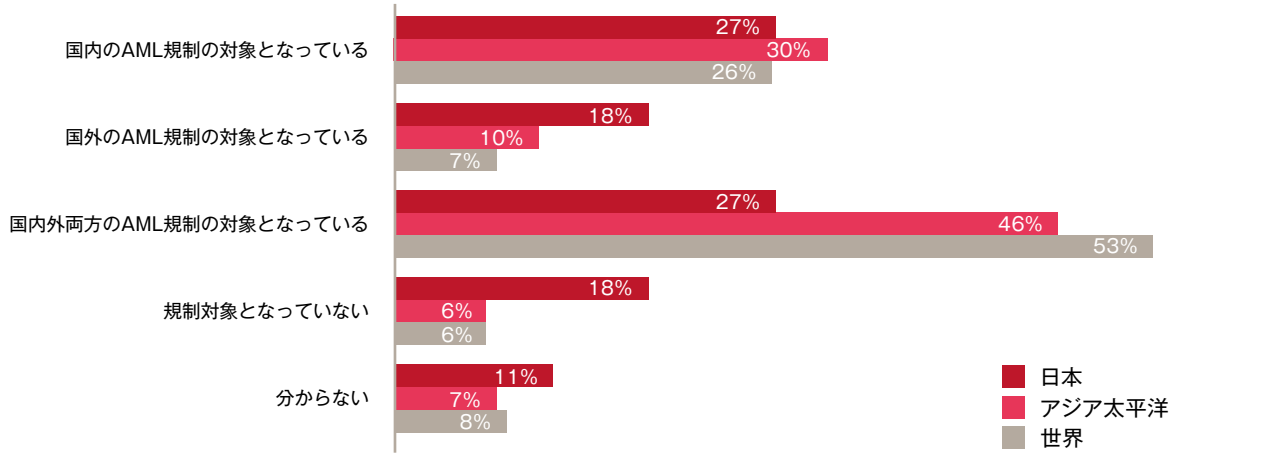


図27　過去2年間に、AML／CFTに関してリスク評価を行ったか否か

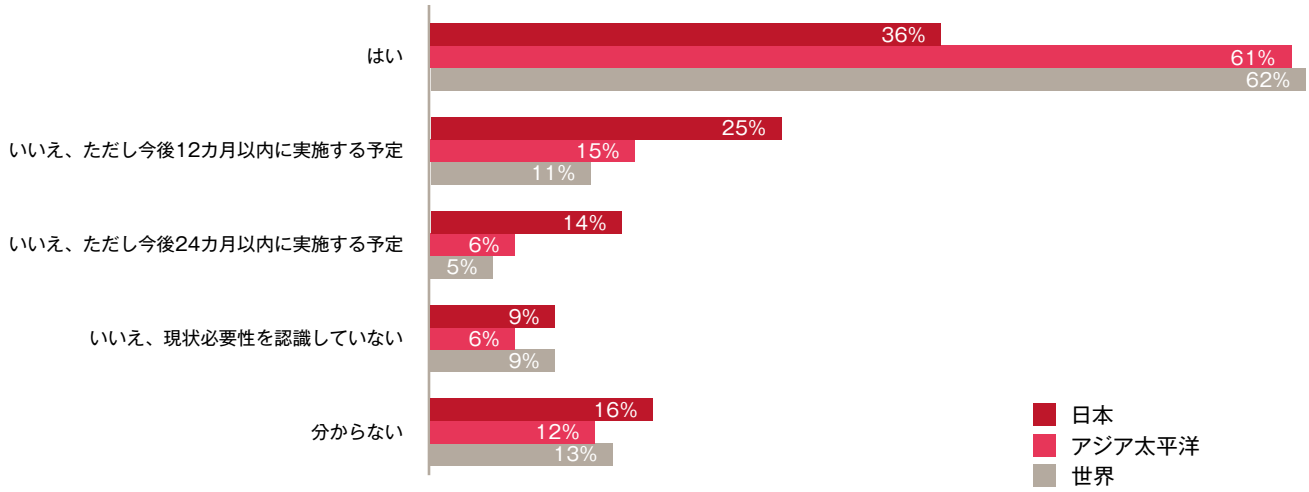
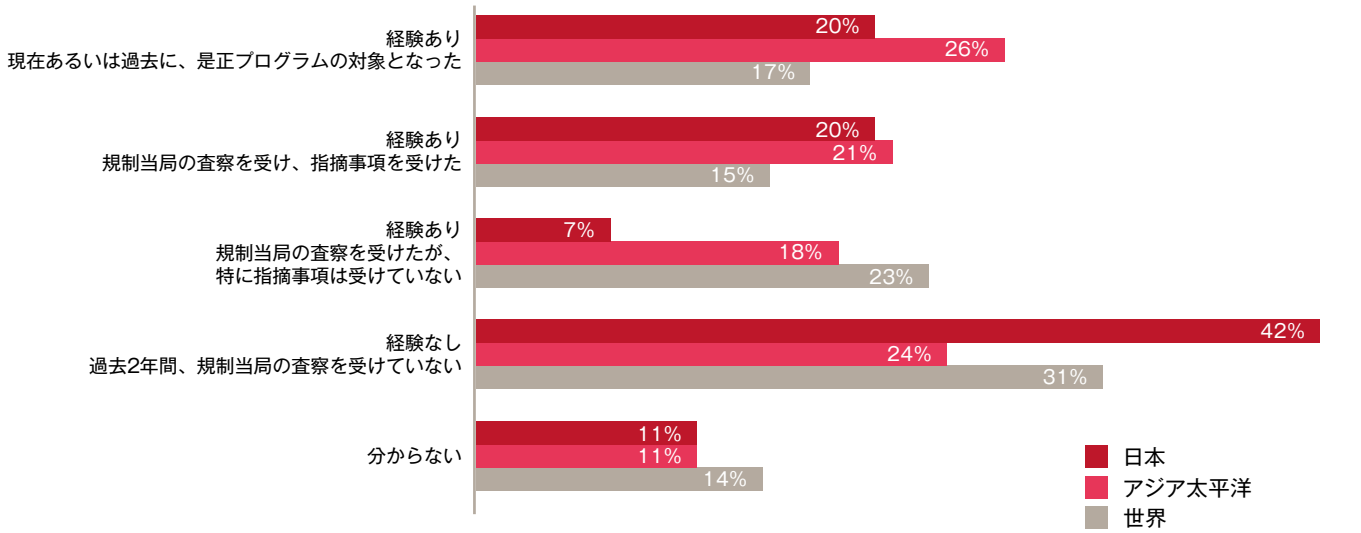


図28　過去2年間に、AML関連の取り締まり／査察を受けたか否か



おわりに

経済犯罪・不正は年々増加しています。被害にあった場合、その不正による損害額だけでなく、弁護士や調査会社に支払う調査費用や、取引先や顧客からの訴訟費用なども多額となります。また、金銭的な損害だけでなく、これまで築き上げた会社のブランド価値や信頼が、一気に毀損される可能性もあります。

特に、今日まで大きな不正や不祥事がなく、対応策を整備してこなかった日本企業にとっては、何かが起こった場合にどのような対応をとるか、またそれをどのようにステークホルダーに説明し、理解を得るか、といった事についてお手本となる事例がなく、手が付けられていないのが現状です。どんなにリスク緩和の手段を講じたとしても、ビジネスを行っている限りリスクが顕在化することはあります。その時のために、平時から有事のための体制構築を怠らないことが重要であると考えます。このレポートが、有事体制構築のためのきっかけとなれば幸いです。

大塚 豪
PwCJapanグループ
フォレンジックサービスリーダー
PwCアドバイザリー合同会社
パートナー

経済犯罪実態調査2018 グローバル翻訳版
～「盲点」に潜む不正を探り出す～

目次

https://www.pwc.com/jp/ja/knowledge/thoughtleadership/economic-crime-survey1805.html

参考情報

2014年改正犯罪収益移転法（2016年10月施行）における主な追加事項

- 顔写真のない本人確認書類による本人確認の際の追加的措置
- 自然人（個人）までさかのぼった実質的支配者の特定・確認
- 外国PEPs（重要な公的地位を有する者）に対する厳格な取引時確認
- 外国所在外為取引業者とのコルレス契約締結に際する相手の体制確認義務
- 疑わしい取引の判断方法および必要なリスク評価の実施の義務
- 関連規定の策定、統括管理者の選任など、体制整備の努力義務

お問い合わせ先

PwCアドバイザリー合同会社
Tel：03-6212-6880（代表）

大塚 豪
パートナー
go.otsuka@pwc.com

平尾 明子
シニアマネージャー
akiko.hirao@pwc.com

上野 俊介
シニアマネージャー
shunsuke.ueno@pwc.com

奈良 隆佑
シニアマネージャー
ryusuke.nara@pwc.com

PwCコンサルティング合同会社
Tel：03-6250-1200（代表）

ホンマ シン
パートナー
shin.s.honma@pwc.com

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwCあらた有限責任監査法人、PwC京都監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立して事業を行い、相互に連携をとりながら、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、法務のサービスをクライアントに提供しています。
PwCは、社会における信頼を築き、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界158カ国に及ぶグローバルネットワークに236,000人以上のスタッフを有し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細はwww.pwc.comをご覧ください。

電子版はこちらからダウンロードできます。 www.pwc.com/jp/ja/knowledge/thoughtleadership.html
日本語版発刊年月：2018年7月　　管理番号：I201804-6