KPMG

アメリカ大陸で発生している3つの脅威

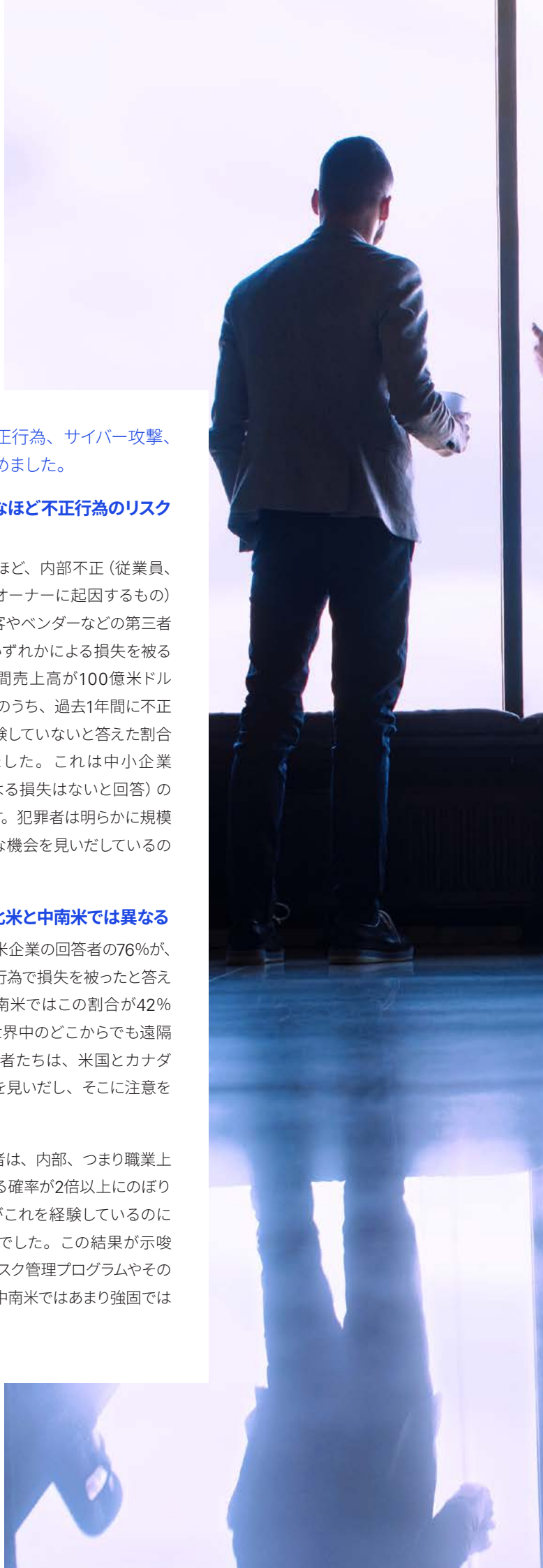
2022 KPMG Fraud Outlook

2022年11月

kpmg.com

目次

はじめに



KPMG[1]は、アメリカ大陸（北米および中南米を含む）における不正行為、サイバー攻撃、コンプライアンス違反について、今後の展望を2022年11月にまとめました。

さまざまな業界にわたる600人以上の企業幹部を対象とした調査では、新型コロナウイルス感染症（COVID-19）のパンデミックが関連する3つの脅威への影響について、具体的な事例が確認されました。不正行為、コンプライアンス違反、ならびにサイバー攻撃の影響は、拡大するとともにその深刻度が増しており、今後はさらに多く発生することが予想されます。

アメリカ大陸の企業は、これら3つの脅威を回避できているのでしょうか。今回の調査では、多くの企業において限定的にしか対策を講じておらず、部分的な在宅勤務からリモートワークへの完全移行といった勤務形態の変化によって、既存の対策では効果が出ないことが示唆されています。

北米および中南米の企業の過半数が、不正行為、コンプライアンス違反、サイバー攻撃で損失を被ったと報告しています

調査回答者の83%は、自社が過去12ヵ月間に少なくとも1回のサイバー攻撃を受けたと答えています。自社で不正行為が発覚したとの回答は71%にのぼりました。また、回答者の半数以上は、コンプライアンスリスクが軽減されていないことが原因で、自社が制裁金を支払った、もしくは、財務面で損害を被ったと回答しています。

これはすべて多大なコストにつながります。回答者は、過去1年間に不正行為やコンプライアンス関連の制裁金によって利益の平均1%を失ったと報告しています。

企業規模が大規模なほど不正行為のリスクが高い

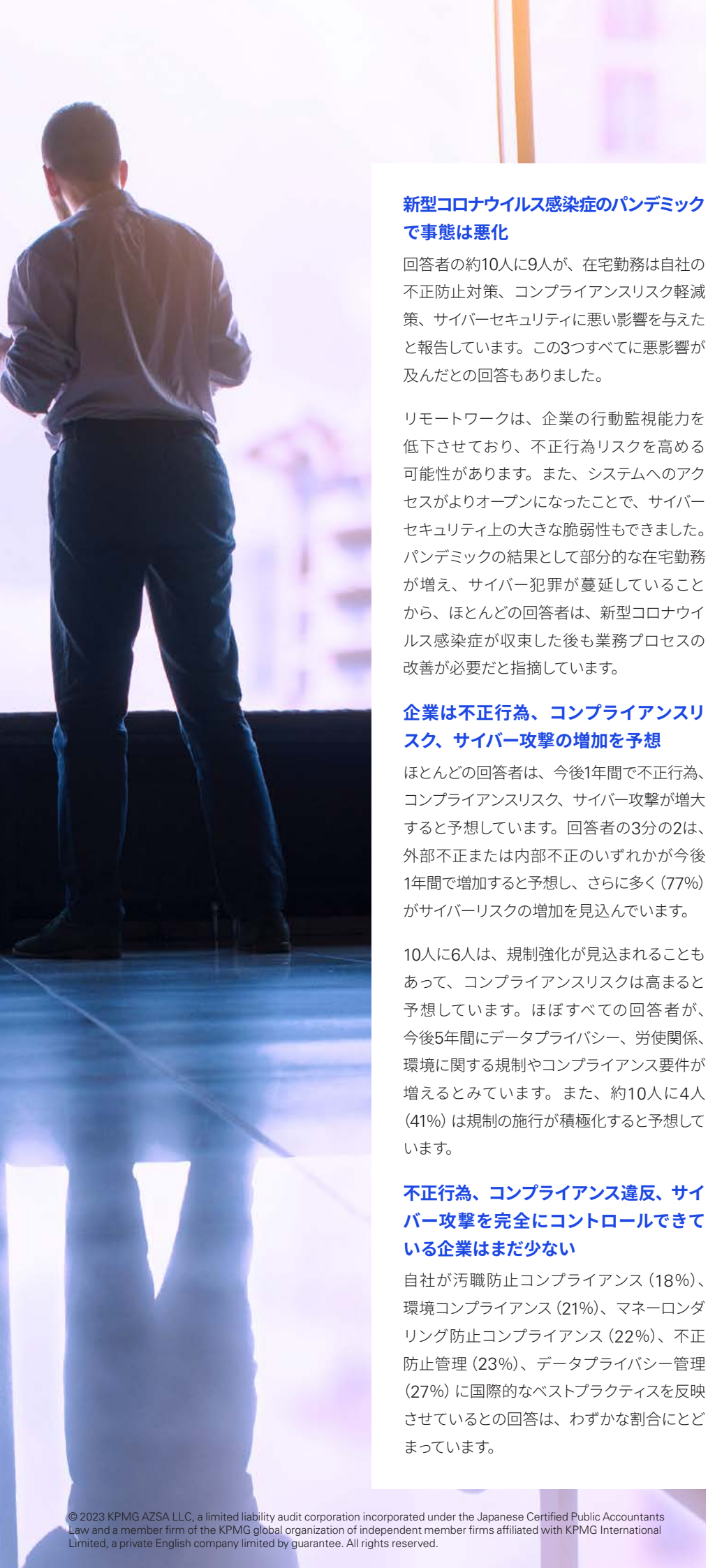
大企業になればなるほど、内部不正（従業員、マネジャー、役員、オーナーに起因するもの）または外部不正（顧客やベンダーなどの第三者に起因するもの）のいずれかによる損失を被る傾向があります。年間売上高が100億米ドル以上の企業の回答者のうち、過去1年間に不正行為による損失を経験していないと答えた割合は15%にとどまりました。これは中小企業（29%が不正行為による損失はないと回答）のほぼ半分にあたります。犯罪者は明らかに規模の大きな組織に大きな機会を見いだしているのです。

不正行為の脅威は北米と中南米では異なる

今回の調査では、北米企業の回答者の76%が、外部の関与する不正行為で損失を被ったと答えているのに対し、中南米ではこの割合が42%にとどまりました。世界中のどこからでも遠隔操作で活動する犯罪者たちは、米国とカナダの企業に大きな機会を見いだし、そこに注意を向けているようです。

ただ、中南米の回答者は、内部、つまり職業上の不正行為を経験する確率が2倍以上にのぼります。半数（49%）がこれを経験しているのに対し、北米では17%でした。この結果が示唆しているのは、不正リスク管理プログラムやその他の内部不正対策が中南米ではあまり強固ではないということです。

1 本レポートにおけるKPMGとは、調査による洞察を提供するための、中南米、米国、カナダのKPMGメンバーファームが該当します。



新型コロナウイルス感染症のパンデミックで事態は悪化

回答者の約10人に9人が、在宅勤務は自社の不正防止対策、コンプライアンスリスク軽減策、サイバーセキュリティに悪い影響を与えたと報告しています。この3つすべてに悪影響が及んだとの回答もありました。

リモートワークは、企業の行動監視能力を低下させており、不正行為リスクを高める可能性があります。また、システムへのアクセスがよりオープンになったことで、サイバーセキュリティ上の大きな脆弱性もできました。パンデミックの結果として部分的な在宅勤務が増え、サイバー犯罪が蔓延していることから、ほとんどの回答者は、新型コロナウイルス感染症が収束した後も業務プロセスの改善が必要だと指摘しています。

企業は不正行為、コンプライアンスリスク、サイバー攻撃の増加を予想

ほとんどの回答者は、今後1年間で不正行為、コンプライアンスリスク、サイバー攻撃が増大すると予想しています。回答者の3分の2は、外部不正または内部不正のいずれかが今後1年間で増加すると予想し、さらに多く（77%）がサイバーリスクの増加を見込んでいます。

10人に6人は、規制強化が見込まれることもあって、コンプライアンスリスクは高まると予想しています。ほぼすべての回答者が、今後5年間にデータプライバシー、労使関係、環境に関する規制やコンプライアンス要件が増えるとみています。また、約10人に4人（41%）は規制の施行が積極化すると予想しています。

不正行為、コンプライアンス違反、サイバー攻撃を完全にコントロールできている企業はまだ少ない

自社が汚職防止コンプライアンス（18%）、環境コンプライアンス（21%）、マネーロンダリング防止コンプライアンス（22%）、不正防止管理（23%）、データプライバシー管理（27%）に国際的なベストプラクティスを反映させているとの回答は、わずかな割合にとどまっています。

不正行為、コンプライアンス違反、サイバー攻撃に関連する一連の防止策の実施に関して、回答者が自社をどのように評価しているか具体的に見てみると、関連する施策の少なくとも半分をしっかりコントロールしている（これを「半分以上」の基準とする）と報告した割合はごく一部でした。回答者のうち、自社がサイバーセキュリティ対策の半分以上でしっかり対応していると答えた割合はわずか24%、不正の防止・検知では17%、コンプライアンスリスクへの対応では13%にとどまっています。3つの分野すべてで自社が優れているとの回答はわずか4%でした。

企業にとって緊急性が高い優先事項

不正行為：

内部犯行の可能性を軽視してはいけません。回答者の31%が、過去1年間に内部者による不正行為の被害を受けたと答えています。

コンプライアンス違反：

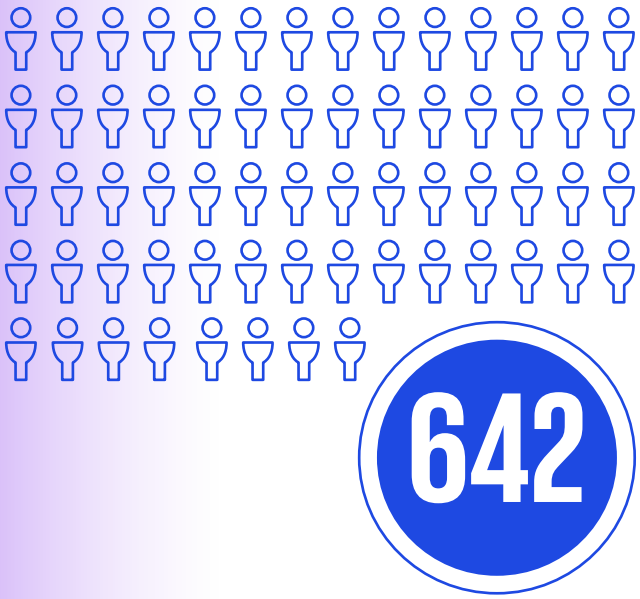
コンプライアンスは今や風評にかかわる問題です。回答者の多くが、罰金や強制執行よりも、風評被害を考慮してリーダーがコンプライアンスに注意を払うようになったと答えています。

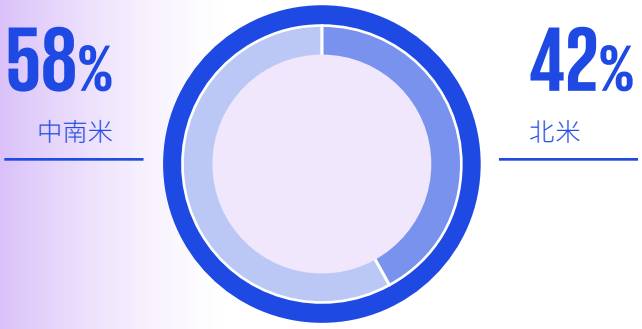
サイバー攻撃：

のんびりとした対応では、サイバーセキュリティの競争に勝つことはできません。回答者によると、サイバー攻撃を完全に封じ込めるまでに平均で約1ヵ月かかるとのことですが、大半は自社の対応に満足しているようです。これは危機感が致命的に欠けている可能性を示唆しています。

調査について

本レポートは、642人の企業幹部を対象とした調査に基づいています：





対象者は以下7つの業界にほぼ均等に分かれています：

産業機械製造　消費財・小売　エネルギー・天然資源

金融サービス　保険　ライフサイエンス・医薬

通信・メディア・娯楽・テクノロジー

回答者は、主に上級管理職**（半数以上は取締役、経営幹部、または部門長）**で構成されています。

調査について（続き）

所属企業の規模はさまざま：

年間売上高が
10億米ドル未満

年間売上高が
10億米ドル以上
100億米ドル未満

年間売上高が
100億米ドル以上

各地域の企業幹部・専門家6人へのインタビューを実施：

José Calderón
Chief Global Auditing Officer, Grupo Bimbo

Larissa Galimberti
Partner, Pinheiro Neto Advogados

Carlos García Jiménez
Regional Director of Ethics and Compliance LATAM, Uber

Ariel Nowersztern
Cybersecurity Specialist, Inter-American Development Bank

Beth Rose
Chief Compliance, Ethics and Integrity Officer, Ford Motor Company

Pascal Saint-Amans
Director, Center for Tax Policy and Administration, Organisation for Economic Co-operation and Development

知見を共有してくださった皆様に感謝いたします。

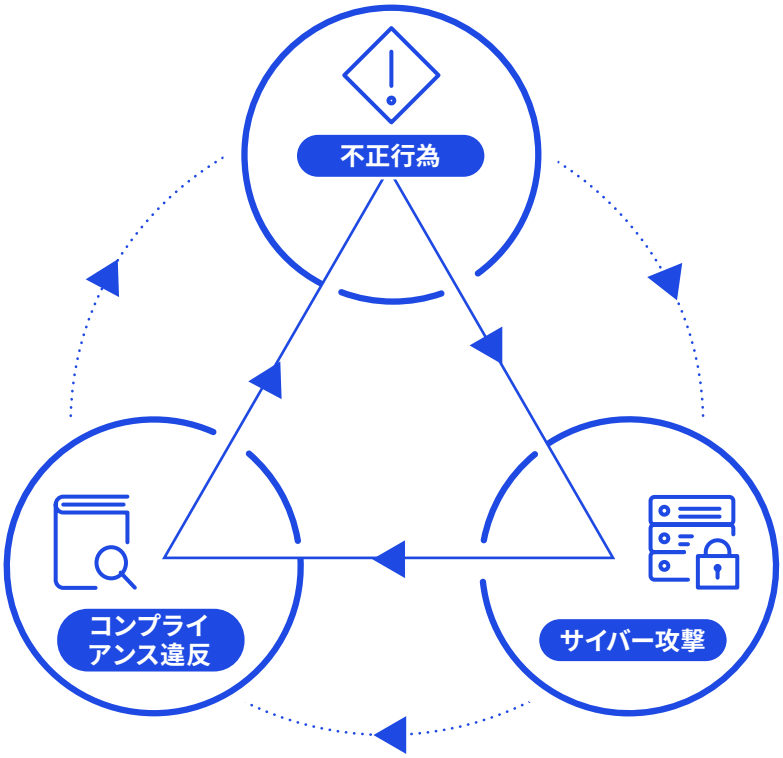
3つの脅威に対抗するための共同防衛

不正行為、コンプライアンス違反、サイバー攻撃のリスクは、北米・中南米の企業に広く存在し、増大する危険性があります。

これらの脅威は相互に絡み合っています。例えば、従業員が在宅勤務中に会社から顧客データを盗むというケースを考えてみましょう。これは3つの脅威を同時に高めるケースであり、企業は1つの脅威として対処する必要があります。

企業は、KPMGが「脅威のループ」と呼ぶ、不正行為、コンプライアンス違反、サイバー攻撃の3つの脅威を軽減する必要があります。脅威のループから身を守るには、相互に連携した総合的な取組みが必要です。企業はそれぞれの脅威が単独でもたらすリスクだけでなく、複数の脅威がもたらす影響を総合的に考える必要があります。

KPMGが考える3つの脅威のループ



米州開発銀行（IDB: Inter-American Development Bank）のサイバーセキュリティ専門家であるAriel Nowersztern氏は、一部の企業はすでにこれらのリスクに対する総合的な防御策を開発していると指摘しています。「サイバーセキュリティ、内部統制、監査のいずれかを実施して、他の対応の有効性を高めることが可能である」と説明しています。

物的資産やデジタル資産の監視を、不正防止やその他の内部統制と組み合わせている企業もあります。ある分野でのアラートが、別の分野で何か問題が起きていることを教えてくれる場合もあるかもしれません。

企業はこの脅威のループに対応する準備ができているか、また、準備ができていない場合はどの程度の作業が必要なのかについて探るため、KPMGは北米・中南米エリアの企業における上級管理職を対象にした調査を実施しました。本レポートは、彼らが語った内容を紹介し、「アメリカ大陸における各企業は脅威への準備ができているのか」と問いかけるものです。

> “サイバーセキュリティ、内部統制、監査のいずれかを実施して、他の対応の有効性を高めることが可能です
>
> **Ariel Nowersztern**
> Cybersecurity Specialist at the
> Inter-American Development Bank

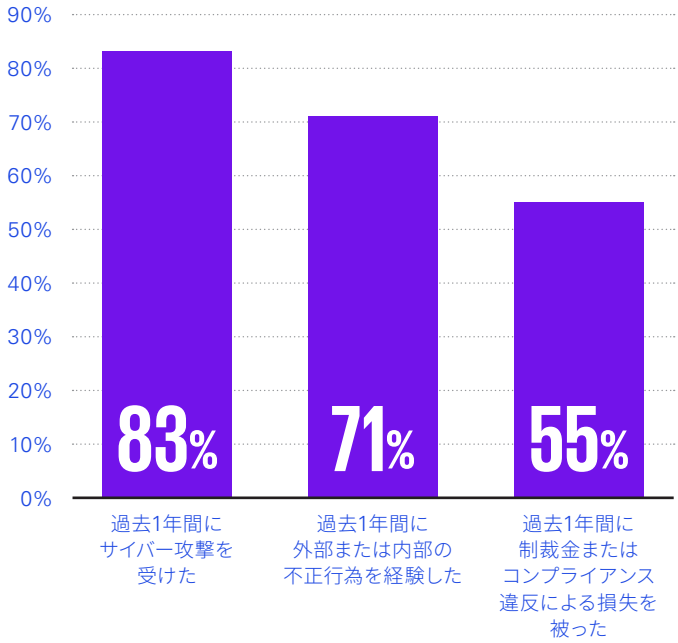
高額の対応費用がかかる、不正行為・コンプライアンス違反・サイバー攻撃

ブラジルの法律事務所Pinheiro Neto Advogadosでテクノロジー問題を専門とするパートナーのLarissa Galimberti氏は「サイバー攻撃は今や『起きるかどうか』ではなく、『いつ起こるか』の問題」と述べています。今回の調査回答者も同意見で、アメリカ大陸の企業にとって不正行為やコンプライアンスの欠如は避けられない事象と認識しています。

今回の調査では、3つの脅威のなかで、自社がサイバー攻撃を受けたとの回答割合が最も高くなりました。アメリカ大陸全体における調査対象者の83%は、自社が過去12 ヵ月間に少なくとも1回のサイバー攻撃を受けたと回答しています。この調査では、ビジネスに顕著な影響を与えたインシデントについてのみコメントするよう回答者に依頼したため、サイバー攻撃の総数は報告数よりも多い可能性があります。

不正行為も憂慮すべき頻度で指摘されています。回答者の71%は、過去12ヵ月間に自社で不正行為が発覚したと報告しています。この割合は、年間売上高が100億ドル以上の企業では85%にのぼります。一方、回答者の55%は、自社が過去1年間にコンプライアンス違反で制裁金を支払った、または財務面で損害を被ったと認めています。不正行為やコンプライアンス違反は発覚しない場合もあるため、これらの数字は代表的なものではない可能性が高く、根本的な問題はさらに大きいかもしれません。

3つの脅威の現実



回答者は、不正行為、コンプライアンス問題、制裁金による自社の損失を合わせると、平均して利益の1%に達すると回答しています。さらに、回答者の58%は、自社がサイバー攻撃による直接的な経済的損失を被ったと回答しています。

一方、回答者の20%は自社が風評被害を受けたと回答し、32%は自社がコンプライアンス調査への対応を余儀なくされたと答えています。これらのインシデントは、特に中小企業の存続にかかわる脅威をもたらす可能性があるとNowerszstern氏は警告しています。資本の大幅な損失、深刻な信用の失墜、あるいは重要な業務情報（顧客リストなど）の流出はいずれも、企業の倒産につながる可能性があります。

これらの分野のコストは、企業規模が大きくなるほど増大します。大企業（ここでは年間売上高100億ドル以上と定義）の回答者は、自社が過去1年間に不正行為によって純利益の平均0.7%を失い、コンプライアンス違反の制裁金として純利益の0.8%を支払い、合計で1.5%になったと回答しています。

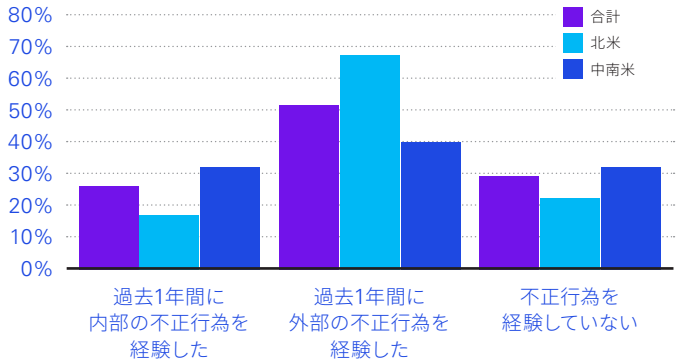
Ford Motor CompanyでChief Compliance, Ethics and Integrity Officerを務めるBeth Rose氏は、企業にとってコンプライアンスや不正防止、サイバーセキュリティが重要である理由はこうした数字だけではないと強調しています。優良企業にとっては、評判と誠実さはきわめて重要な考慮事項です。しかしそれと同様に、これほどの規模のコストは企業とそのステークホルダーにとって重要な事項になります。「当然ながら、経営幹部は経済的な影響の方に目を向ける傾向がある」とRose氏は述べています。

Uber社のEthics and Compliance LATAMのRegional DirectorであるCarlos Garcia Jiménez氏も同意見で、これらのリスクに対する効果的な防御策は、すべての企業の基準とされる平均損失の「数分の1のコスト」で済むと指摘しています。

地域ごとの不正行為の違いと企業規模が重要である理由

表面上、北米と中南米の回答者が報告する不正行為の発生状況は、以下のように著しく異なっています。

北米と中南米における不正行為の比較

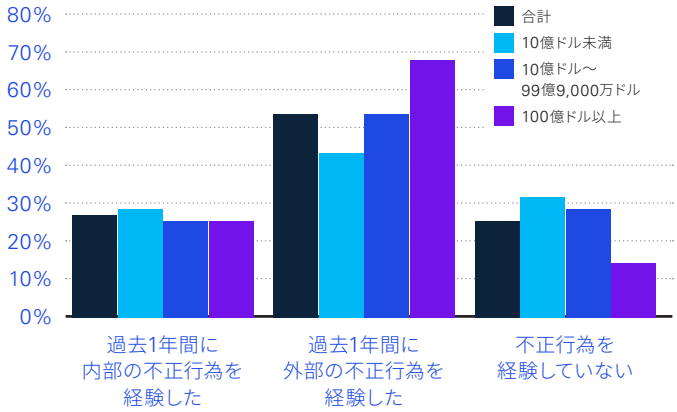


注目すべきは2つの点です。第一に、不正行為は北米企業にとってより広範な問題であることが回答から考察できます。第二に、リスク環境は地域間で異なっています。中南米企業は、内部関係者が関与した不正行為を報告する割合が、北米企業の2倍近くに達しています。北米では、外部の不正行為がはるかに大きな問題となっています。

1.5%：大企業が不正行為やコンプライアンス違反で失っている利益の割合

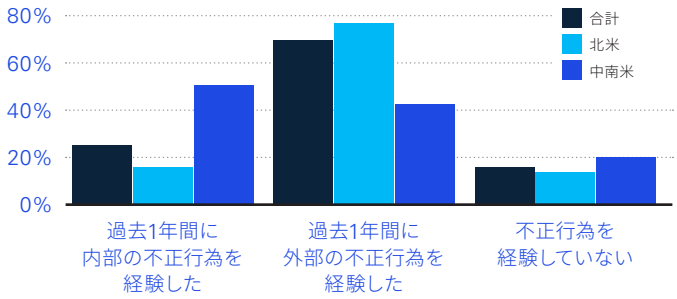
ただし、これらの数字には、両地域の平均的な企業規模が大きく異なることが影響している可能性があります。調査対象となった北米企業の多くはかなり規模が大きく、年間売上高の中央値が29億ドルであるのに対し、中南米企業では8億4,600万ドルです。今回の調査では、大規模で裕福な企業ほど、外部の不正行為の標的になりやすいことも明らかになっています。

企業規模による不正行為の比較



しかし、このような地域差は、企業規模に起因するのでしょうか。その答えは、北米と中南米の大企業（年間売上高100億ドル以上）だけを比較することで見えてきます。

年間売上高100億ドル以上の企業における不正行為の比較



何らかの不正行為の影響を受けた企業の数を地域別に比較してみると、大企業の回答者ほど、その差が近づく傾向にあります。何らかの不正行為を経験した北米企業の割合（77%）と中南米企業の割合（67%）の差は10ポイントです。しかし、大企業の回答者のうち、過去12ヵ月間の不正行為を報告した割合は北米の86%に対し、中南米では80%と、その差は明らかに小さくなっています。

それでも、不正行為の種類によっては、地域別の回答結果は著しく異なります。中南米の大企業の調査対象者のうち、49%は過去1年間に内部の不正行為が少なくとも1回発生したと回答しており、この割合は北米の約3倍となります。これは、北米企業が内部の不正行為と決して無縁ではない一方で、中南米企業は内部の不正行為リスクに対処するために内部統制の導入を優先すべきであることを示しています。

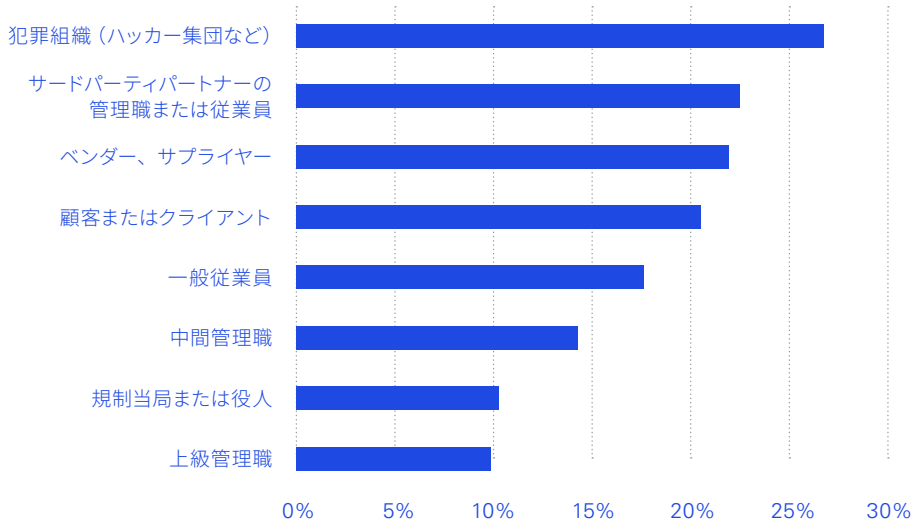
しかし、外部の不正行為を経験した北米企業の割合（76%）が（中南米企業の42%と比較して）はるかに多いことをどう考えるべきでしょうか。その理由は、サイバー犯罪の経験の違いにあると思われます。中南米の大企業の回答者のうち、過去1年間にサイバー攻撃を受けたと回答したのはわずか7%でした。この割合は、北米では実に43%にのぼりました。

北米企業は売上高が多いだけでなく、デジタル化が進んでいるため、晒されるリスクが大きいとNowersztern氏は指摘しています。一方で、北米の企業は中南米の企業に比べ、サイバー攻撃が起きた際の検知能力が優れている可能性が高いため、実際の侵入未遂の比率は、回答に反映されているよりも近いかもしれません。

北米企業がサイバー防衛の強化を必要としていることは明らかですが、中南米企業も現状に甘んじてはいられません。会社が成長するにつれて、サイバー攻撃のより大きな標的となる可能性があるのです。

データのスナップショットI：不正行為の実行者群

過去12ヵ月間に自社で不正行為や不祥事（単独または共謀）に関与したことが判明した人物は、以下のどの種類ですか？

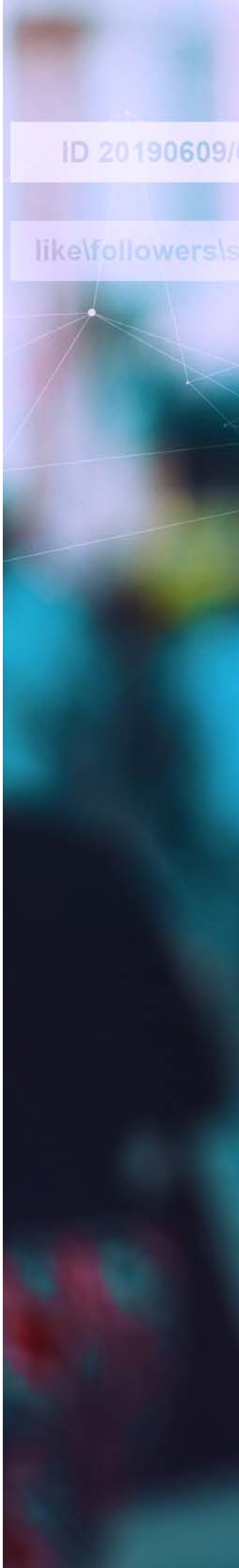


企業はさまざまな不正行為の被害を受けやすい状況にあります。Grupo Bimbo社のChief Global Auditing OfficerであるJose Calderón氏は、さまざまな不正行為に関するリスクを低減することを目的に、同社はグローバルな枠組みを導入したと説明しています。「多くのサプライヤーからの原材料の調達から、生産、販売・実行に至るまでのプロセスに影響し得るすべての事柄」が、不正行為リスクを生み出す可能性があると同氏は言います。「また、社内外の関係者、環境・労働規制、データプライバシーなど、コンプライアンスと不正行為に関する課題もあり、リスクは非常に広範にわたっている。」

今回の調査によると、企業に最も頻繁に侵入する（あるいは、少なくとも最も頻繁に発覚する）犯罪者の種類は、デジタル技術を駆使する外部の窃盗犯です。そのすぐ後に、パートナー、ベンダー、サプライヤーが続きます。企業の現地事業が統制されておらず、サードパーティサプライヤーを多く利用している国では、ベンダーによる不正行為や癒着の可能性がそれ相応に大きくなります。

内部にも脅威は潜んでいます。回答者の31%は、過去1年間に自社で内部の不正行為（従業員、管理職、役員、オーナーによるもの）が行われたと回答しています。

犯人は地域によっても異なります。北米の回答者の43%が、外部の犯罪組織（ハッカー集団など）による不正行為を報告しているのに対し、中南米ではわずか14%となっており、北米でサイバー犯罪のレベルが高まっていることと一致しています。反対に、中南米の回答者の36%が自社で内部の不正行為があったと回答しているのに対し、北米では23%にとどまっています。



パンデミックで状況はどう変わったか

新型コロナウイルス感染症のパンデミックとそれに伴うロックダウンにより、脅威に関する環境は複雑化しています。

あらゆる分野でリスク環境は悪化し、リモートワークの拡大によって既存の防御力は弱まっています。全体として、回答者の86%は、リモートワークが自社の不正防止、コンプライアンス違反、サイバーセキュリティプログラムの少なくとも1つの要素に悪影響を及ぼしていると回答しています。

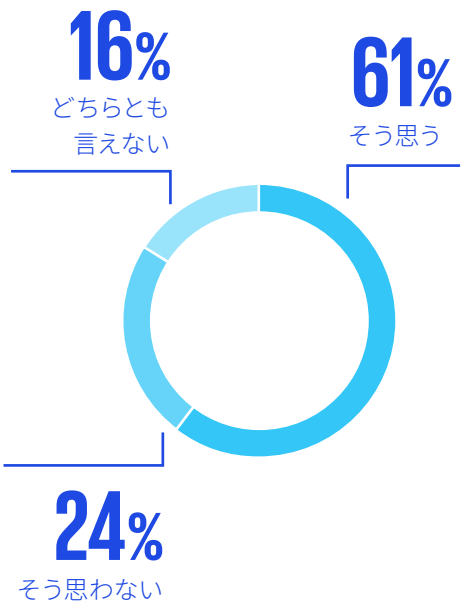
86%：リモートワークが自社の不正防止、コンプライアンス違反、サイバーセキュリティプログラムの少なくとも1つの要素に悪影響を及ぼしていると回答した割合

不正行為の防止

ビジネスにおける不正行為の機会は、そのオペレーションの産物であると言えます。例えば、Grupo Bimbo社のJose Calderón氏は、原材料やスペアパーツを迅速に入手する必要がある場合、大きなリスクが生じると指摘しています。

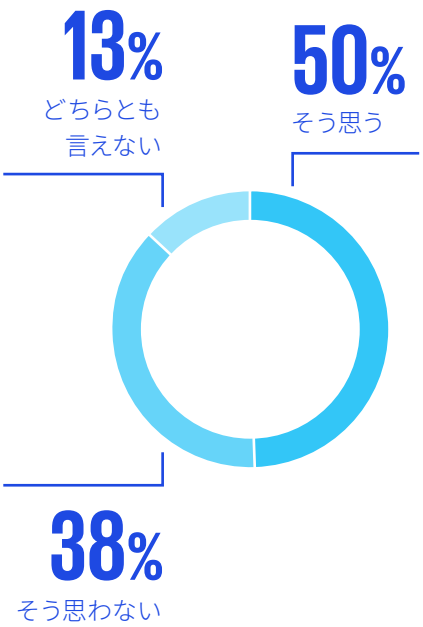
これは、企業が原材料をできる限り早急に入手するため、既存の管理（第三者のデューデリジェンスなど）を迂回する可能性が高まるからです。これはパンデミックの最悪期にも、2021年後半に世界の多くでサプライチェーン問題が発生した際にも、多くの企業にとって特筆すべきリスクとなりました。

リモートワークへの移行で不正行為を監視・制御する能力が低下し、不正行為リスクが高まった[2]



2　グラフの合計値は四捨五入の関係で100%になりません。

在宅勤務はビジネスにおける不正行為への適切な対応能力に悪影響を及ぼした[2]

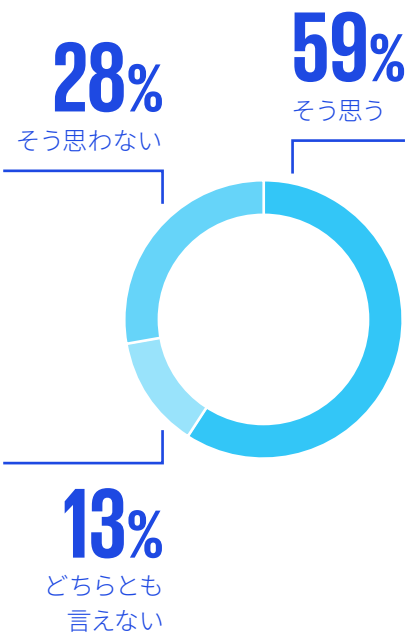


一方、リモートワークの急増は、不正の防止、特に監視と原因調査の面でも課題をもたらしています。調査対象者の61%が、従業員の行動を監視する能力の低下により、不正行為リスクが高まったと回答しています。これは一般従業員だけに関連するものではありません。回答者の28%は、リモートワークによって経営管理や監督に支障が出ていると回答しています。この問題は、従業員が新しいリモートワークの職場を持つことだけにはとどまりません。例えば、Garcia Jiménez氏によると、多くの従業員がミレニアル世代で、会社とは関係のない人とアパートでルームシェアをしています。これにより、従業員以外が会社のシステムにアクセスできないようにすることは一段と難しくなりました。

同様に、回答者の半数は、在宅勤務が自社の不正行為への対応能力に悪影響を与えたと答えています。Garcia Jiménez氏は、基本的な不正対策さえ変えざるを得なかったと指摘しています。通常のオフィス環境以外では、もはやオフィス内と同じレベルの物理的な統制はききません。「情報を収集したり、ファイルや電子メールを取り込んだりするのは非常に困難です。面談を実施するのも大変です。ロジスティクスの面では、部屋の予約はもちろん、従来とは異なる手配をする必要があります。」 一部の従業員は、別の州や国からリモートで仕事している場合さえあります。

部分的な在宅勤務がますます普及すると予想されるなか、これらの課題が解消される可能性は低いでしょう。アメリカ大陸の企業の大半は、こうしたリスクに対応する準備が現在もできていません。

コロナ前に導入された不正防止策は、新しい働き方を反映するべく効果的に更新されていない。

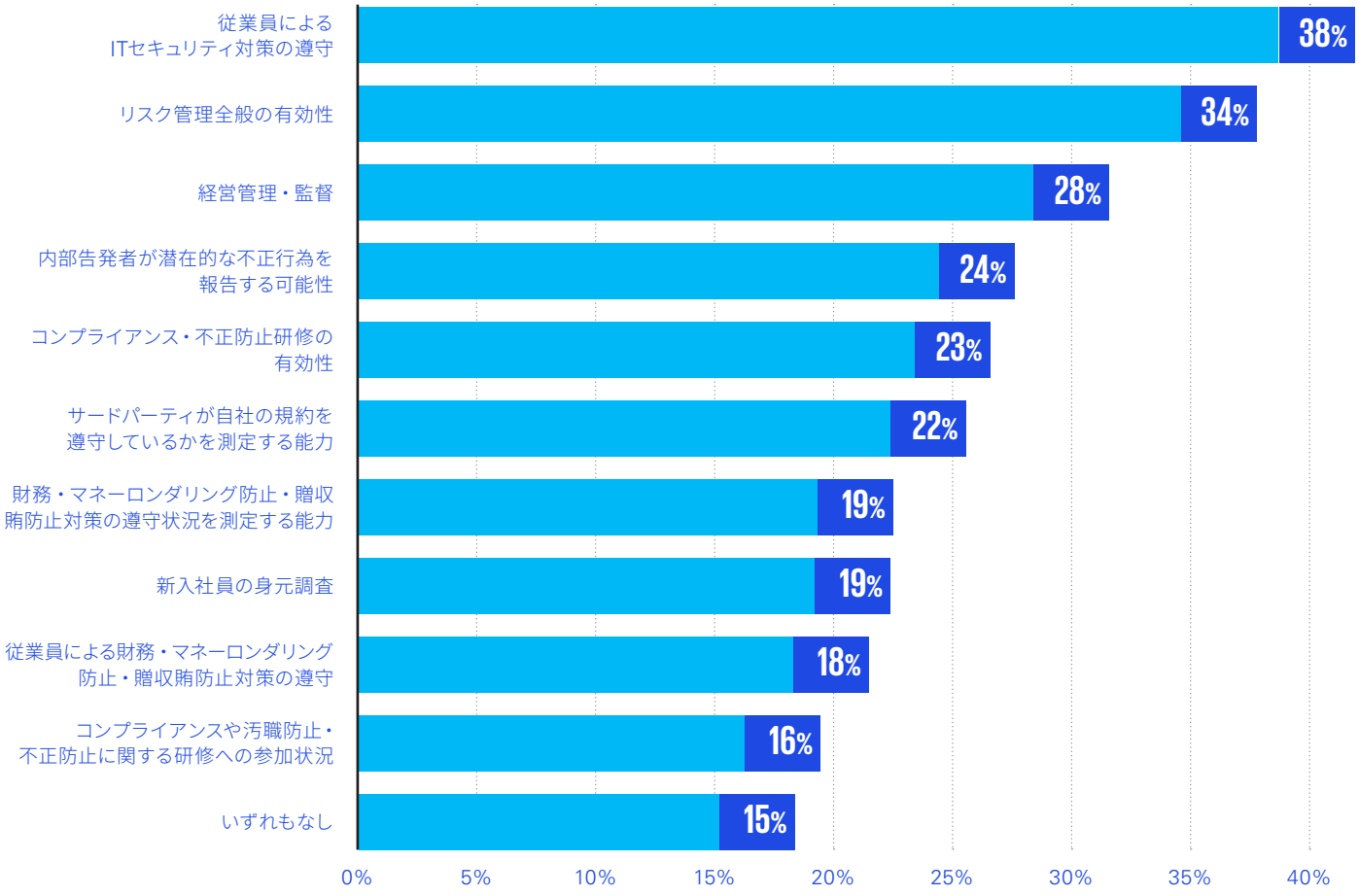


回答者の**59%**は、コロナ前に導入された不正防止策が、新しい働き方を反映するべく効果的に更新されていないと感じている

コンプライアンス違反

77%もの調査対象者が、進化するコンプライアンスの要求に対応するため、自社はパンデミック中に新しい戦略を立てる必要があったと答えています。これは現状の新たな課題を反映している場合もあります。Ford Motor CompanyのBeth Rose 氏は「コロナ禍ではすべてのコンプライアンス部門が大きな転換を迫られた」と振り返ります。当初の問題は「健康と安全をどのように遵守するか」でした。同様に、Ford社が初めて人工呼吸器や保護マスクの製造に着手したとき、これらの製品に関連するコンプライアンス要件を理解し、実施する必要がありました。

以下のうち、在宅勤務の従業員が増加したことで過去1年間に悪影響を受けたのは？



リモートワークへの配慮は、コンプライアンスの面でも重要な役割を担っています。Garcia Jiménez氏によると、対面式の研修がオンラインに移行するなど、コンプライアンス研修が最大の影響を受けています。これは単なる媒体の変化にとどまりません。多くの企業では、研修資料を大幅に見直すとともに、指導する側と学ぶ側でさまざまなコミュニケーションスキルを身につける必要がありました。これにかかる時間を考えると、多くの企業は研修の長期的な空白期間を余儀なくされているでしょう。

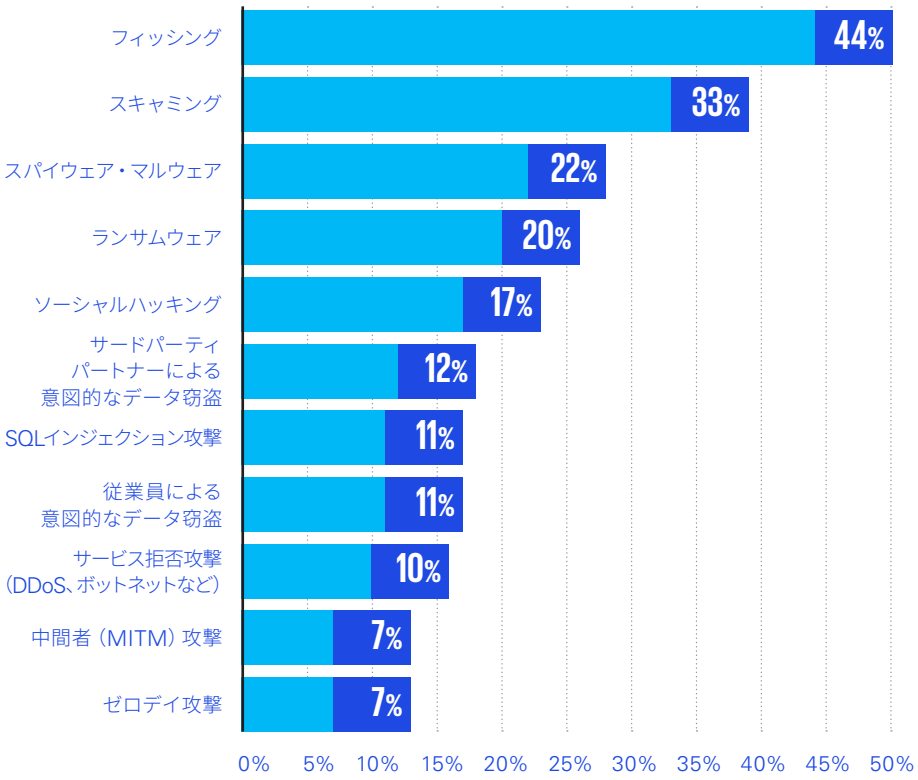
また、リモートワークの増加によって大きな文化的変化も求められました。「リスクがどこにあるかを感知するため、何が起きているかを見極めることはコンプライアンスの一部です。バーチャルになると、それが課題になります」とRose氏は言います。多くの回答者も同意見で、19%がリモートワークによって財務、マネーロンダリング防止、贈収賄防止対策の遵守状況を測定するのが難しくなったと回答しています。

新しいコンプライアンス環境への適応は依然として進行中です。前述のFord社は現在の部分的な在宅勤務モデルを継続する計画だとRose氏は報告しています。コンプライアンスへの影響を把握することは「非常に難しい問題です。研修、意識向上、チームとリスク評価についてこれまでとは違った考え方をしなければなりません」と同氏は断言します。業界ごとに異なるニーズがあるでしょう。

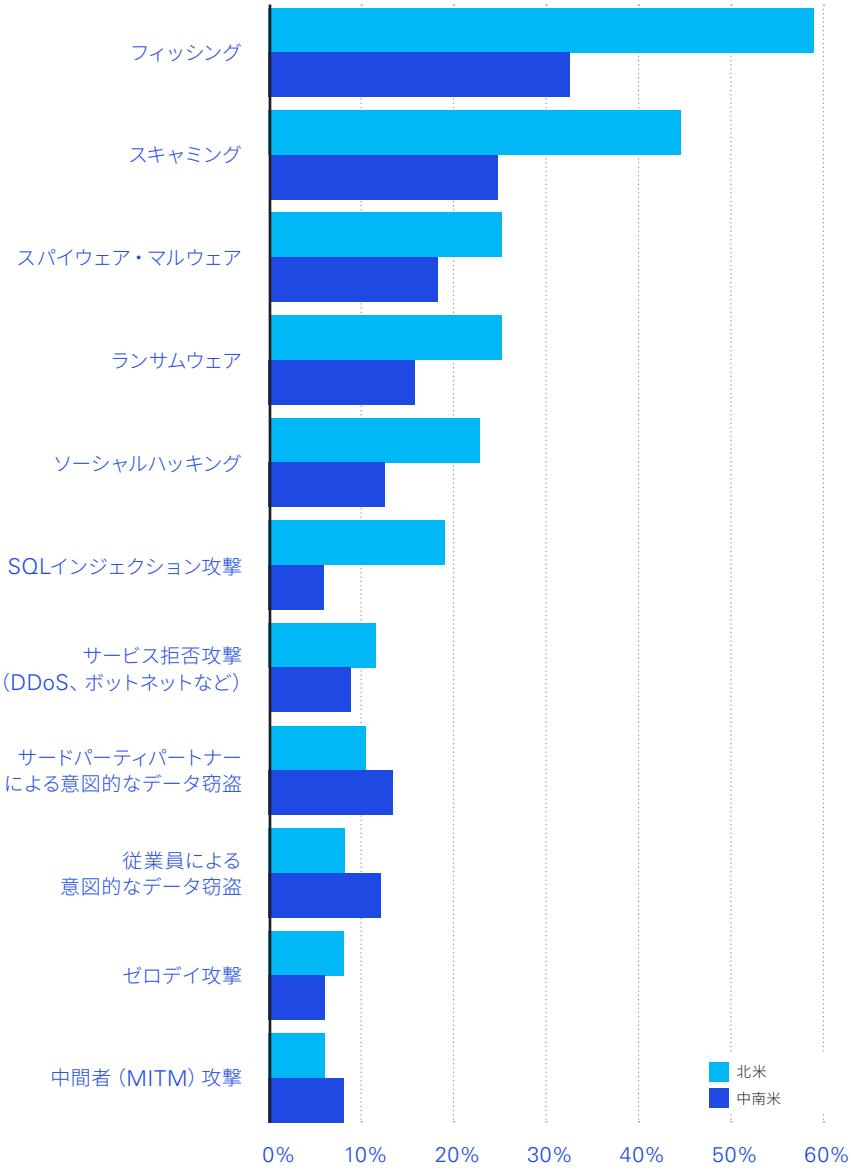
サイバーセキュリティ

サイバー犯罪はパンデミック中に増加し、現在もその勢いは衰えていません。以下のグラフでわかるとおり、本レポートの調査対象企業はフィッシング（44%）、スキャミング（33%）、マルウェア（22%）、ランサムウェア（20%）など、さまざまな種類の攻撃の頻度が増していると回答しており、多くの企業にとってますます課題となっています。全体として、回答者の79%が、本調査の対象とされる攻撃の種類のうち少なくとも1つは増加したと答えています。

以下のうち、過去1年間に自社で増加したサイバー攻撃はどの種類ですか（もしあれば）？



地域比較：以下のうち、過去1年間で増加したのはどれですか？



個々のインシデントであっても、結果的に大きな影響を及ぼすことがあります。その一例として、パイプラインを狙った2021年5月のランサムウェア攻撃により、米国南部の複数の州で石油不足が発生しました。Galimberti氏は、かなりの影響が出たもう1つの例として、2021年初頭にブラジルで起きた大規模なデータ盗難事件を挙げています。「2億2,000万人のブラジル人のファイルが、あらゆる情報とともにダークウェブ上で公開された」と言います。

Nowersztern氏は、パンデミック前から存在するものの、パンデミックによって加速したいくつかの傾向が犯罪活動の増大を後押ししたと指摘しています。例えば、フィッシングメールは話題性の高い新型コロナをテーマにし、不安を抱える消費者を誘い込みました。そのうえ、企業や社会がデジタル資産や機器への依存度を高めるにつれ「私たちは以前よりもますます脆弱になっている。犯罪者はそれに気づいている」と同氏は警告しています。

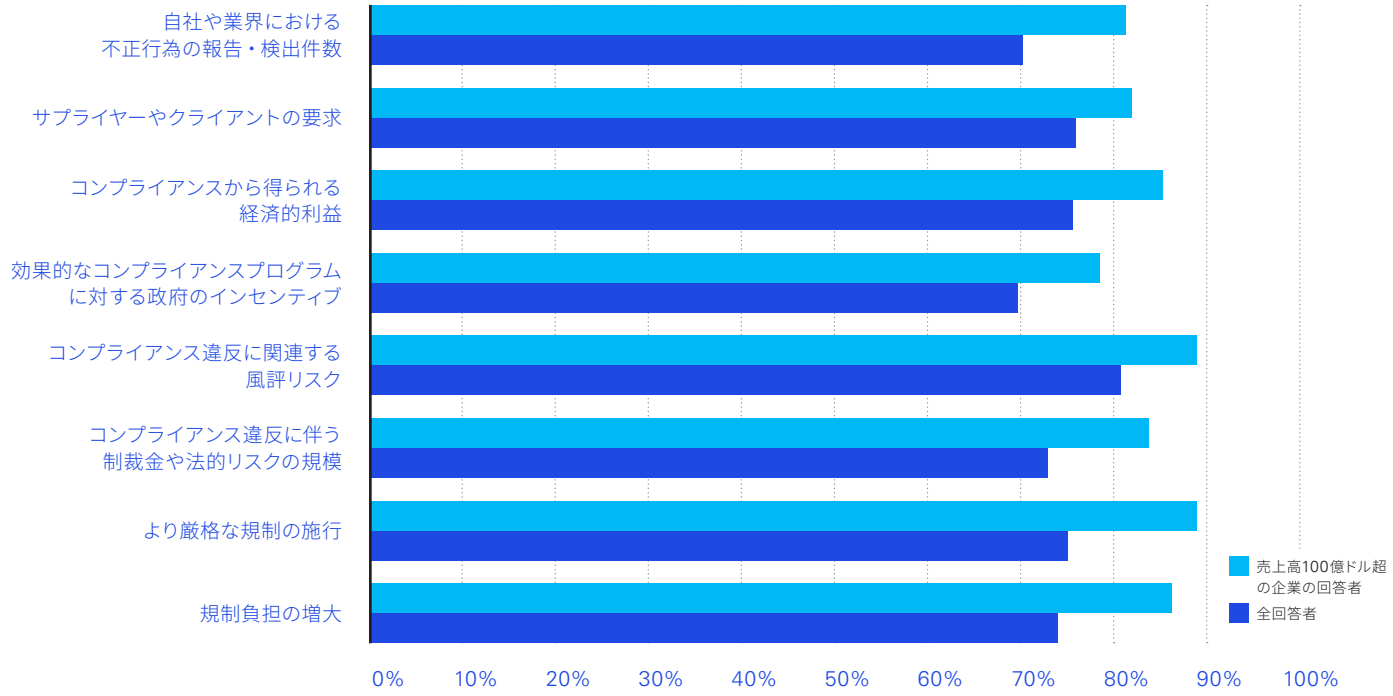
調査対象者のほぼ全員が、自社は二要素認証の導入（55%）、ネットワークセキュリティの改善（54%）、研修の強化（47%）など、サイバーセキュリティリスクに対処するための措置を講じたと回答しています。こうしたサイバーセキュリティの課題に対応するために必要とされる投資は、結果的にかなりの額にのぼる可能性があります。Calderon氏によると、Grupo Bimbo社では「取締役会がサイバーセキュリティ予算を5倍以上に増やしました。さらに増えるかもしれません。」在宅勤務をするGrupo Bimbo社の従業員は全体の5分の1未満であるにもかかわらず、これほどの増額が必要でした。

> 調査対象者の**69%**が、リモートワークは自社のビジネスにとってサイバーセキュリティ上の大きな課題になっていると回答している

新型コロナウイルス感染症の流行と、それに伴うリモートワークへの移行は、企業のサイバーセキュリティ対策を一段と難しくしています。回答者の67%は、部分的な在宅勤務の環境がもたらすサイバーリスクに依然として懸念を抱いています。パンデミック、あるいは少なくともロックダウンの終了は、一部企業の視野には入っているかもしれませんが、アメリカ大陸における労働形態の恒久的な変化は、脅威のループのあらゆる側面における各種の取組みが緊急の注意を要するものであることを意味しています。

データのスナップショットII：コンプライアンスはビジネス全体の関心事項

自社のリーダーがコンプライアンス問題に費やす時間と注意は、以下によってどの程度増えていますか？[3]



コンプライアンスはもはや（かつてはそうだったとしても）単に法律に違反しないようにするだけの問題ではなくなっています。グラフからわかるとおり、全回答者の70%以上、大企業の回答者の80%以上が、厳格な規制施行、規制負担の増大、制裁金の可能性によって、自社のリーダーがコンプライアンス問題に費やす時間と注意は増えていると報告しています。

しかし、利害関係者の要求、経済的利益、風評も同様に、リーダーの注意をコンプライアンスに向けさせる可能性があります。調査対象者の64%は、サプライヤーや顧客がデータプライバシー規制に対する適合性について証拠を求めるようになっていると報告し、52%が汚職やマネーロンダリング関連の法律についても同様な適合性に関する証拠が求められると回答しています。

Ford社のBeth Rose氏は当然のことだと言います。「ソーシャルメディアが進化し、評判やブランドについて意見する人が急増するなか、コンプライアンス活動を徹底することに気を配らなければならない。」

また、規制の厳格な施行と、第三者との提携や合併を通じたコンプライアンス違反行為との不用意なつながりを避けることは重要です。

このように幅広い検討事項があるため、コンプライアンス機能の役割は広がっています。Garcia Jiménez氏は、コンプライアンスが依然としてリスクの軽減を目的とする一方で、今や「社内外でのストーリーづくり」を目指すものでもあると述べています。

規制当局や他の利害関係者、社会全体に対し、自社のビジネスが地域社会に提供する経済的、社会的、環境的な利益を示すことも企業活動の一部です。

こうした幅広いストーリーづくりは、企業に副次的なメリットをもたらします。特に、優れたコンプライアンス活動は、規制当局、投資家、パートナー、顧客など、他の利害関係者に対して会社の信頼性を伝えるのに役立ちます。

3　このグラフは、1を「まったくない」、3を「多少ある」、5を「大いにある」と定義した1から5までの選択肢のうち、4または5を選択した回答者の割合を示しています。

脅威のレベルは高まるばかり

リモートワークがはらむ課題は、不正行為、コンプライアンス、サイバーセキュリティ関連の困難が増すという、幅広いパターンの一部にすぎません。回答者の69%が、今後1年間で外部または内部による不正行為のうち、少なくともどちらか1つのリスクが増加すると予想しており、29%は両方の不正行為リスクが高まると回答しています。

サイバー犯罪の拡大に対する懸念が広がっています。回答者の77%は、今後12ヵ月間でサイバーセキュリティのリスクが高まると回答する一方で、サイバーセキュリティリスクが減少すると予測したのはわずか7%でした。Galimberti氏も同意見で、「企業はますます多くのハッカー、ランサムウェア、フィッシングなどの攻撃に直面している」と述べています。

不正行為とサイバー攻撃の事例が増加していることは、必ずしも関連しているわけではありませんが、Calderón氏は、経営モデルに圧力がかかると、不正行為リスクは高まる可能性があると指摘します。例えば、食品・飲料業界では、低価格でより健康な製品に対する消費者の関心が、需要のあり方を変えています。この新しい需要に対応するために低コストのサプライヤーを利用する方向にシフトするには、そうしたパートナーのビジネス慣行に関するデューデリジェンスが必要です。これには、契約交渉の方法や、不正を疑われるような方法で価格交渉をしない、といった考慮事項も含まれます。

それでも、不正行為とサイバーセキュリティの不備は重複の度合いがますます高まっています。過去1年間で増加したと回答した人が最も多かったサイバー攻撃の種類には、フィッシング（44%）、スキャミング（33%）、スパイウェア（22%）、ランサムウェア（20%）が含まれます。

> 回答者の**69%**が、今後1年間で外部または内部による不正行為のうち、少なくともどちらか1つのリスクが増加すると予想しており、29%は両方の不正行為リスクが高まると回答

現在のビジネストレンドは、不正の実行者に新たな機会を提供することで、不正行為とサイバーリスクの融合を不注意にも増加させています。例えば、Calderón氏は「プロセスのデジタル化、クラウドへの移行、モバイル端末の利用拡大」はすべてリスクを伴うと指摘します。Rose氏は「誰もがリモートでコンピューターを使うようになるなか、悪意のある人はより創造的な手法を見いだしている」とし、こうした試みがすべてオンラインで行われているわけではないとも述べています。データもそれを裏付けており、回答者の17%は、サイバー犯罪者がソーシャルエンジニアリングと人間行動の操作を駆使してシステムにアクセスする「ソーシャルハッキング」の増加を報告しています。

62%
今後5年の間に新しいデータプライバシー規制の導入を予想

47%
今後5年の間に新しい環境規制を予想

46%
今後5年の間に新しい労働規制を予想

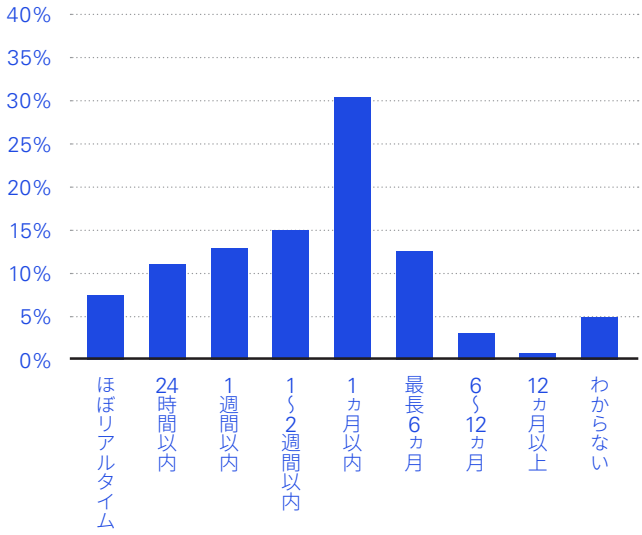
41%
今後5年の間に既存規制の施行強化を予想

調査対象者の60%は、一般的なコンプライアンスリスクも今後1年間で増加する可能性があると回答しており、コンプライアンスリスクが減少すると予測したのは回答者のわずか17%でした。Ford社のRose氏が説明するように、この課題は多面的なものであり、既存規制が多い領域におけるコンプライアンス要件の増加、新しい分野へのルール導入の可能性、コンプライアンス担当者による積極的な施行などが含まれます。上記の結果が示すように、かなりの数の回答者が、今後5年の間に新しいデータプライバシー規制、環境規制、労働規制が導入されると予想しています。全体として、回答者の89%が、今後1年間にこれらの分野の少なくとも1つで新たなコンプライアンス要件が発生すると回答しています。Rose氏は、「米国の現政権は施行を強化し、すべての分野で規制を拡充しています。それには環境・社会・企業統治（ESG）規制も含まれます。サイバー分野は成長し続けるでしょう。すべてが一緒に影響を受けるのです」と述べています。

中南米でも同様の規制強化が進んでいます。Galimberti氏によると、2020年9月に施行されたブラジルの一般データ保護法は、大小の企業によるコンプライアンス活動を後押ししています。この法律は、データへのアクセス権など実質的な権利をデータ主体に与えているほか、データを処理するすべての企業にデータ保護責任者の任命を義務付けています。Calderón氏は、水の消費や廃棄物管理などの分野で環境面の要件が増えていると付け加えています。これらは「課題であると同時に、消費者のニーズに応える機会でもあります」と同氏は述べています。

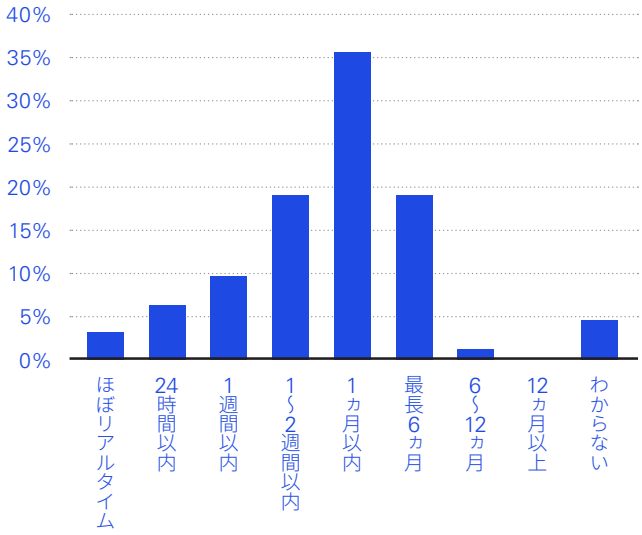
データのスナップショットIII：遅い反応、不十分な懸念

自社でサイバー攻撃や侵入行為を特定するのに通常どれくらい時間がかかりますか？



中央値：約2週間

自社でサイバー攻撃や侵入行為が特定された場合、通常はその封じ込めにどれくらい時間がかかりますか？



中央値：約2.5週間

IDBのAriel Nowersztern氏は、サイバーインシデントが発生すると「データは数分ないし数秒で失われる可能性があります。その意味で、どのような対応速度も十分ではありません」と述べています。同様に、悪意のある人はネットワークへのアクセス権を一度取得すると、さまざまな方法で企業に損害を与えることが可能です。

このため、自社がサイバー攻撃をリアルタイム、または24時間以内に特定して封じ込められると回答した人の割合はごくわずかにとどまった、という調査結果は特に憂慮されます。

サイバー攻撃の特定にかかる時間の中央値は2週間とかなり長く、封じ込めにはさらに2週間半を要します。今回の調査を総合すると、企業へのサイバー攻撃が始まってから、その企業が攻撃を封じ込めるまでには、通常約1ヵ月かかります。

それに対して回答者は驚くほど意に介していないようです。回答者の81%は、自社がIT攻撃を認識するまでの時間にややまたは完全に満足しており、76%は対応の速さに満足しています。

Nowersztern氏は、訓練を受けた専門家の不足や、サイバーセキュリティは投資ではなくコストであるという一般認識の面での問題など、サイバーセキュリティの向上には多くの障壁があると説明しています。しかし、結局のところ、今回の調査で示された関心の薄さという事実が最大の障壁となっています。「基本的に、解決策はサイバーセキュリティに一層の重点を置くことから始まります。そうしなければなりません。たとえ導入が困難であったり、費用が高くついたりしても、ツールはあるのです」とNowersztern氏は付け加えています。

包括的な軽減策は依然として限定的

北米企業は自社の基準を高く評価しており、北米企業の回答者の多くは、自社が国際的な基準を満たしている、あるいは国内基準でうまくやっていると考えています。

対照的に、これらの質問に対して中南米の回答者から最も多く上がった回答は、自社は法的義務を果たしているが、国内外の基準で見て優れているわけではないというものでした。

実際、汚職とマネーロンダリングの規制に関しては、中南米の回答者の4分の1以上が、現地のルールさえも完全に満たしているかどうかわからないと回答しています。

この調査では、細部にわたる実態を把握するため、不正防止（11分野）、コンプライアンス違反（7分野）、サイバーセキュリティ（6分野）の個々の側面について、回答者が自社をどの程度評価しているかを掘り下げています[4]。企業は必ずしも、脅威のループ全体に及ぶ26分野のすべてにおいて優れている必要はないのかもしれませんが、Rose氏が指摘するように、「コンプライアンスはリスクベースであるべき」です。リスクの低い分野に労力を傾けすぎると、リソースの不適切な浪費につながります。とはいえ、財務・経営管理やデータ盗難の防止など、今回の調査で取り上げられた問題は、ほとんどの企業が管理の改善に努める上で十分に重要な事象です。

複雑化する不正行為、コンプライアンス違反、サイバーの脅威に対して企業はどのような防御策を講じているのでしょうか？

特に中南米では、どの観点から見ても、ほとんどの企業に大幅な改善の余地がありますが、北米企業の対応も満足できない状況です。

調査対象者のうち、自社が汚職防止コンプライアンス（18%）、環境コンプライアンス（21%）、マネーロンダリング防止コンプライアンス（22%）、不正防止管理（23%）、データプライバシー管理（27%）の活動において、国際的なベストプラクティスを模範にしているとの回答は、全体として少数派にとどまりました。

4　具体的な対象分野は以下のとおり：
不正防止 — 財務管理、物的資産のセキュリティ、ITセキュリティ、経営管理・監督、社員の経歴審査、内部告発などの報告の仕組み、サプライヤー・パートナー・顧客に関するデューデリジェンスのプロセス、不正防止方針・不正行為マトリックス、リスク評価、社員研修、不正対応計画。
コンプライアンス — コンプライアンス違反の防止、コンプライアンス違反事例の発見・調査、コンプライアンス違反事例を軽減するための措置、企業リスク・制裁金・罰則を最小化する方法での当局への不正報告、新しい規制要件へのタイムリーな適応・遵守、潜在的な第三者におけるコンプライアンス・不正行為リスクの特定、上記の分野でパフォーマンスを高めるための新テクノロジーの導入。
サイバーセキュリティ — 外部ハッカーによるデータ盗難の防止、従業員によるデータ盗難の防止、従業員の過失によるデータ損失・盗難の防止、ベンダー・サプライヤー・パートナーによるデータ盗難の防止、ランサムウェア攻撃の防止、ネットワークや資産に対する他の攻撃の防止。

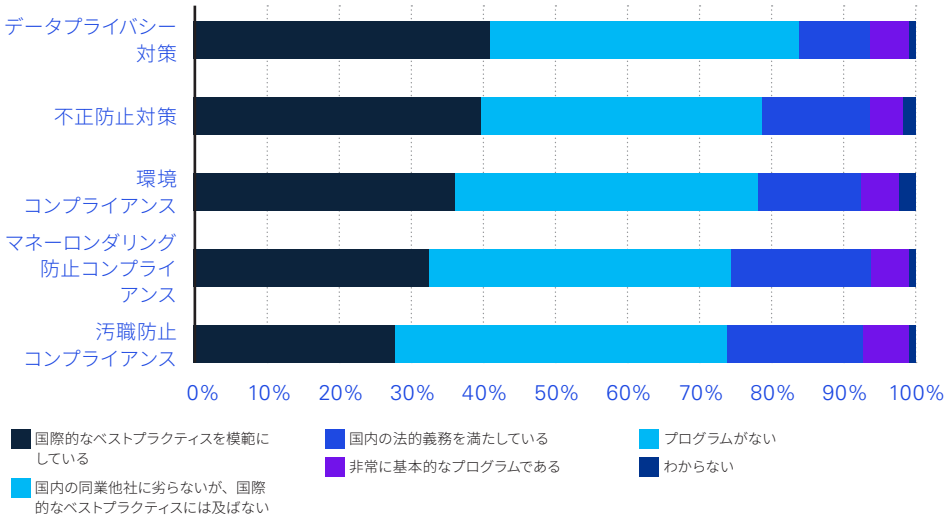
明るい面としては、不正防止、コンプライアンス違反、サイバーセキュリティのそれぞれについて、回答者の85 ～ 95%が、調査対象分野の少なくとも1つの点で自社が優れていると評価しました。しかし、自社のパフォーマンスの質が全体的に高いと評価した回答者はごくわずかでした。調査対象者のうち、各カテゴリーの対象分野の少なくとも半分で自社が優れている（これを「半分以上」の基準とします）と評価した人数を算出しました。

全体として、自社がサイバーセキュリティ関連で半分以上の基準を達成したと評価した回答者は24%、不正防止関連では17%、コンプライアンス関連では13%にとどまりました。

さらに、3つの分野すべてで自社が基準の半分以上を達成したとの回答はわずか4%でした。つまり、ほとんどの企業は不正行為、コンプライアンス違反、サイバーリスクに対する取組みの質を高める必要があるのです。

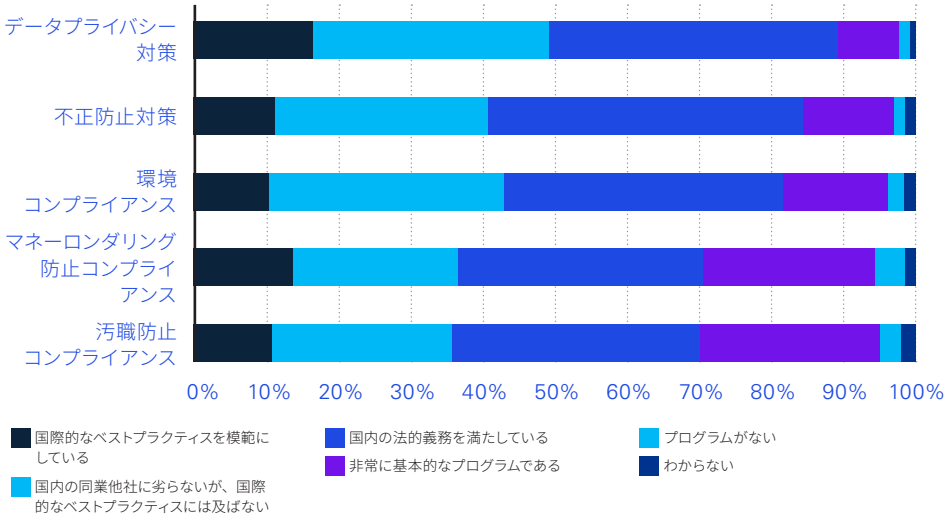
以下の分野における自社のプログラムの成熟度は？

北米企業の回答



以下の分野における自社のプログラムの成熟度は？

中南米企業の回答



この問題は中南米でより広範に及んでおり、自社がサイバーセキュリティ関連で半分以上の基準を満たしていると評価した回答者は20%、不正防止関連では11%、コンプライアンス関連では9%にとどまりました。この弱みの影響は他の調査結果でも明らかです。例えば、内部監査によって不正行為やコンプライアンス違反、サイバーセキュリティ違反が明らかになったとの回答は、北米企業で43%にのぼりましたが、中南米企業ではわずか27%でした。

同様に、他の内部統制によってこうした問題が表面化したとの回答は、北米企業の41%に対し、中南米企業では31%にとどまりました。

中南米企業の内部統制の洗練度が低いことも、中南米企業の回答者が高い割合で内部の不正行為に直面していることを説明するのに役立つかもしれません。

多くの回答者の所属企業のリーダーは、防御策を強化する必要性を理解しているようです。調査対象者の約65%は、今後1年間でサイバーセキュリティへの支出が増えると予想しており、53%は不正防止への支出増を、44%はコンプライアンスへの支出増を見込んでいます。この3分野への支出が今後1年間で減少すると予測している回答者は、いずれも7%未満と、ごくわずかにとどまっています。

企業がこれらの支出を決定する際に、今回インタビューした専門家たちが最も重要なアドバイスとして挙げるのは、従業員を忘れてはならない、ということです。Calderón氏は「優秀な従業員の育成とつなぎ留めは、不正行為を防ぐうえで最も重要なことの1つです。これにより正しい文化が広まります」とみています。Rose氏も「最大の問題は文化である」と同意しています。

これを徹底するには、育成だけでなく、パンデミックの影響で疲弊した従業員のケアも必要だとRose氏は付け加えています。「人は1日の限界、あるいは完全な限界に達しつつあるかもしれず、それがミスや不祥事につながる可能性がある。どうすれば、従業員が安心してサポートを受けていると実感できるのか。それが大きな課題である。」

半分以上の基準を満たしている企業の割合

北米

31% サイバーセキュリティ

27% 不正防止

18% コンプライアンス対策

中南米

20% サイバーセキュリティ

11% 不正防止

9% コンプライアンス対策

結論：

あなたの会社は3つの脅威に備えていますか？

新型コロナウイルス感染症のパンデミック以前から、不正行為、コンプライアンス違反、サイバー攻撃はすでにアメリカ大陸の企業に多額の犠牲を伴う脅威をもたらしていました。今やこれらはより広範かつ複雑になっています。

企業幹部は今後、3つの脅威全体でリスクがさらに広範囲に増加すると予想しています。

ほとんどの企業は何らかの防御策を講じていますが、包括的に優れた対策が取られている企業は限られています。特に中南米ではそれが顕著で、例えば、効果的な統制の欠如が内部の不正行為の多さにつながっていることが、今回の調査で示唆されています。北米企業はうまく対応していますが、ほとんどの企業はまだ不十分です。

大多数の企業は、これらの分野への支出を増やすとともに、経営陣の集中力を高めるとみられています。KPMGは3つの脅威の軽減策として、次の5つを推奨します。

01

トップが正しい姿勢を見せる

上級管理職と取締役会は、倫理的な行動とコンプライアンスへの取組みを奨励する企業文化を確実に推進すべきです。その一環として、不正行為を防止・検知し、コンプライアンス違反やサイバーセキュリティのリスクを軽減するための基準や手順を確立し、そうした基準を遵守しているか監視する必要があります。これを支援するため、企業は取締役会がコンプライアンスと倫理について十分な知識を持ち、合理的な監視を行えるようにするためのプロトコルを整備しなければなりません。

02

リスクを見直す

企業は、不正行為・不祥事、コンプライアンス違反、サイバーセキュリティのリスクを網羅し、仮想リスクではなく実際のリスクに焦点を当てた包括的なリスク評価プロセスを実施すべきです。これは、経営陣、取締役会、内部監査、コンプライアンス、オペレーション、その他の利害関係者が協力して主要なリスク領域を特定し、その軽減策を策定する必要があることを意味します。

03

効果的にコミュニケーションする

企業はリスクに関するメッセージが組織全体に最も効率的に流れる方法を見極めるべく、研修やコミュニケーションの既存のプロトコルを評価すべきです。すべての関係者は、上級管理職から、統制の責任を真剣に受け止めなければならないという明確な意思伝達を受けている必要があります。これを後押しするためには、目的を絞った研修を実施することで、従業員は会社資産の保護や内部統制システムの強化における自分の役割や、自分の行動が他の社員の仕事とどのように関連しているかを理解できるでしょう。

04

検知能力を強化する

重大な不正行為や不祥事を発見するうえでは従業員の存在が欠かせません。従業員が自分には手を挙げて不祥事を報告する責任があると考えている組織は、不正行為や不祥事を早期に発見する可能性が高まります。このような組織では、従業員が安心して通報し、報復を恐れることはなく、経営陣の素早い対応に期待しています。組織は従業員や関連する第三者が不正行為の疑いを報告し、法規制や会社の行動規範に関する助言や説明を求める方法を開発し、公表する必要があります。

05

施行と説明責任を果たす企業文化を醸成する

企業は自社のポリシーとプロトコルを強化し、施行と説明責任の懲罰的でない要素を盛り込むことを検討すべきです。例えば、倫理的な原則や誠実さ、行動を業績評価の一部とし、倫理関連の目標や業績目標に関連するゴールを達成した場合にインセンティブや報酬を提供することが考えられます。これにより、不正行為やコンプライアンス違反があった場合、懲戒処分が階級や在職期間、職務に関係なく一貫して実施されるというメッセージが伝わります。

執筆者

Marc Miller
Partner, Global & U.S. Forensic Network Leader
T: 212-872-6916
E: marcmiller@kpmg.com

Emerson Melo
Partner, KPMGブラジル
Forensic South America Leader
emersonmelo@kpmg.com.br

Ana Lopez Espinar
Partner, KPMGアルゼンチン
Forensic South America Leader
ablopez@kpmg.com.ar

Enzo Carlucci
Partner, Risk
KPMGカナダ
ecarlucci@kpmg.ca

Luis Preciado
Lead Partner, Risk Advisory, KPMG メキシコ
Forensic Mexico and Central America Leader
luispreciado@kpmg.com.mx

お問合せ先

KPMGジャパン
セクター統轄室
Sector-Japan@jp.kpmg.com

本冊子で紹介するサービスは、公認会計士法、独立性規則および利益相反等の観点から、提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。詳しくは有限責任 あずさ監査法人までお問い合わせください。

kpmg.com/jp/socialmedia

本冊子は、KPMGインターナショナルが2022年11月に発行した「A triple threat across the Americas 2022 KPMG Fraud Outlook」を、KPMGインターナショナルの許可を得て翻訳したものです。翻訳と英語原文間に齟齬がある場合は、当該英語原文が優先するものとします。