Kroll

Global Fraud & Risk Report

不確実性の時代に新たな道を築く

10th Annual Edition - 2017/18

FORRESTER®

Forrester Consultingへの調査委託

調査手法について

2017/2018年版Global Fraud & Risk Reportにおいて、クロールは様々な業界及び地域にまたがる540人の企業幹部に対し、グローバルなオンライン調査をForrester Consultingに委託しました。この調査は2017年6月から8月にかけて行われました。

この調査は、昨年度の不正、サイバー、及び物理的セキュリティリスクの分析に基づいて設計されました。今年は、主にサイバーのセクションにおいて、サイバー上の脅威がどういう形で現れ、こうした脅威に対応するためどのように業界のプロを活用しているのかといった点に関する変化を反映させるため、多くの設問について変更を加えました。本レポートはデータ分析に影響を与える設問の変更部分は強調するようにしています。

以前の調査と同様、回答者は（1）建設、エンジニアリング、インフラ、（2）消費財、（3）金融サービス、（4）ヘルスケア、製薬、バイオ、（5）製造、（6）天然資源、（7）プロフェッショナル・サービス、（8）小売、卸、流通、（9）技術、メディア、テレコム、（10）輸送、娯楽、旅行、といった様々な業界にまたがっています。

回答者はそれぞれの企業の幹部ポストにある方々で、69%の回答者が最高責任者クラス、上級カウンセル、取締役レベルの地位にある方です。84%の対象企業が年商5億ドル以上の企業となっています。

回答者は世界中の主要な地域をすべてカバーしており、ヨーロッパ、アジア太平洋地域、北米からの回答者がそれぞれ20%、サブサハラアフリカからが10%、中東が11%、中南米からが19%となっています。

通貨単位はすべて米ドル表記となっています。

序文

45年前、クロールはビジネス調査業界におけるパイオニアとして始まりました。以来、クロールは、何十年にわたり消えない脅威から、静かに組織にダメージを与え、驚くべき速さで予告なく襲ってくる新たな危険に至るまで、様々な状況を経験し、リスクに関する独実の知見を蓄積してきました。しかし、長きにわたり依然として変わらないこと、それは、リスクは、どんな形であれ、人、財産、企業のレピュテーションに絶えずつきまとい続ける脅威であるということです。

クロールのKroll Global Fraud & Risk Reportの第10版では、これまでと同様、クロール独特の知識とインサイト、そして長年の経験を読者に共有するという姿勢を維持しています。我々の最終目標は、地域やグローバルにおける現実に裏打ちされたフレームワークの中で、こうした複雑なリスクに対する実用的なソリューションの開発やベストプラクティスの選択をサポートすることにあります。

皆様には、このレポートから、世界中のあらゆる業界において、組織がどのようにして現在のリスク環境を切り抜けているのかを是非読み取っていただきたいと思います。また、一線で活躍するクロールの調査、コンプライアンス、サイバー、データ侵害通知、セキュリティコンサルティングそれぞれの分野の専門家による解説は、皆様にとって有益なものであると信じております。

本レポートが伝えたい、組織にとって最も重要な示唆の一つは、「リスクの多くはもはや不正、サイバー、セキュリティなどときれいに分類することはできない」ということです。むしろ、グローバル経済、デジタルなコネクションの発展、依然として変わらぬ人の行動要因を併せ考えると、企業のリスク管理にはホリスティックなアプローチが必要であり、新たな脅威環境に対峙するためには総合的なリスク管理戦略を採用しなければならないとも言えます。

クロールは、お客様がこの新たなリスク環境を理解し、対処していくのを支援するため、多くの分野にわたる専門家のチームを抱え、さらにこれらのチームをデータ分析、言語、技術的なソリューションを使って、いつでもどこでも集約させることができます。我々は、クライアントが、現在および将来のリスクを予期し、検知し、低減し、対処するのをサポートすべく、いつでも知識と情報をご提供します。

David R. Fontaine
クロール　チーフ・エグゼクティブ・オフィサー

目次

調査概要

はじめに

Kroll Global Fraud & Risk Report第10号をご覧いただきありがとうございます。本レポートでは、世界各地の様々な業界で起こっている不正、サイバー、セキュリティそれぞれに関連する課題を取り上げています。このレポートでは、企業の幹部のみなさんが、過去12か月間に自分の組織で経験した事案の性質について、内部からの視点で述べるとともに、犯人やその手口についてのインサイトについても紹介しています。また、年々複雑化し経済的かつレピュテーション上の被害を引き起こす様々なリスクに対してどのように予見し、発見し、被害を最小限に食い止め、実際に対処すべきなのかについても教えてくれています。

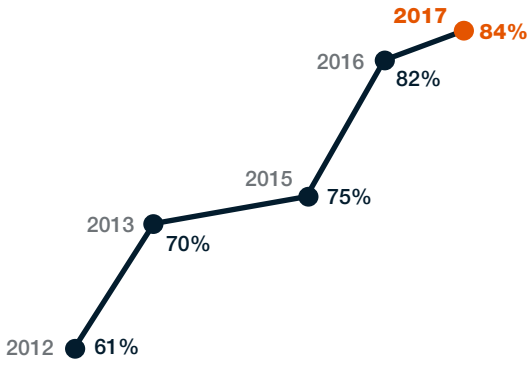
発生率の上昇と実質的な影響

常に起こりうる事件

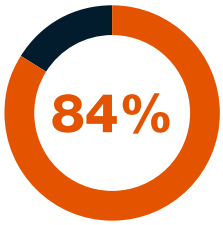
不正

不正事件は今年も増加傾向にある。

過去12ヶ月に、不正事案に少なくとも1回は巻き込まれた企業は、調査対象企業の全体の84%を占め、2016年の82%から上昇した。2012年時点では61%であったが、この数字は年々増え続けている。



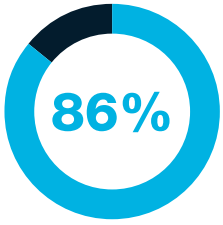
[過去12ヶ月間に不正の被害に遭った割合]



▲ 2% 対前年比

サイバー攻撃

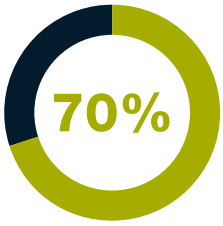
サイバー攻撃やデータ漏洩を過去12ヶ月に経験した企業は、2016年の85%に対し、今年は86%という結果であった。しかし、特定の国や産業では、実に100%に近い数字となっている。



▲ 1% 対前年比

セキュリティリスク

過去12ヶ月間にセキュリティ・インシデントに巻き込まれた経験があるとした回答は、2016年の68%から70%に上昇した 。



▲ 2% 対前年比

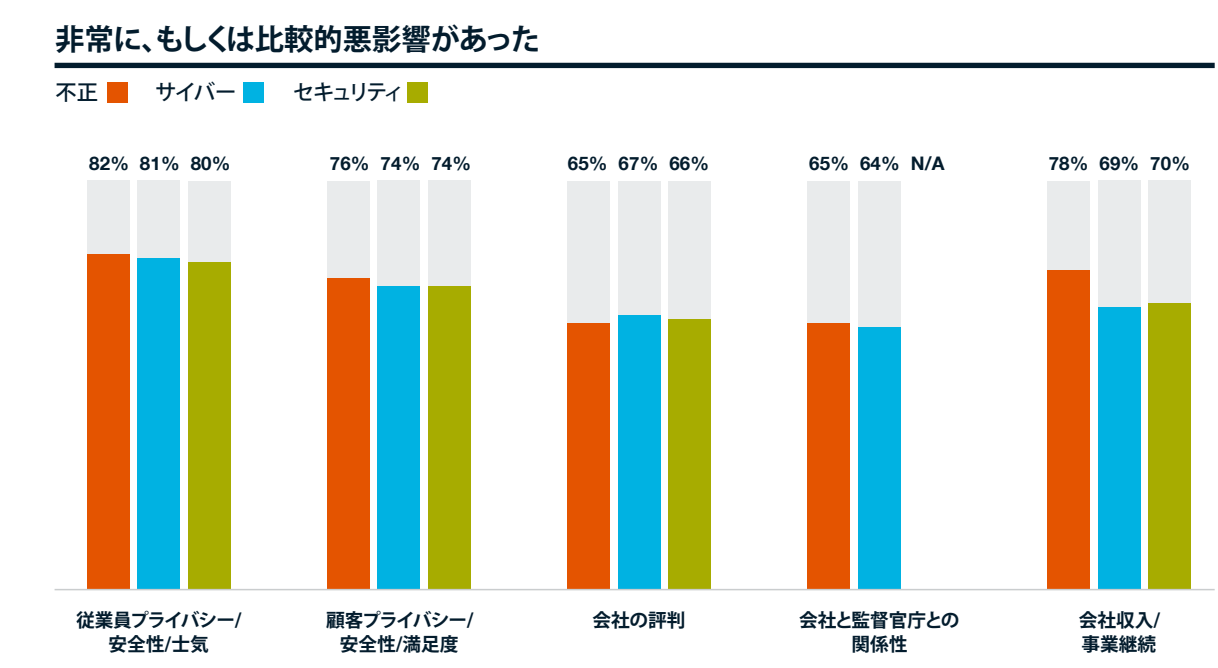
広がる実質的な影響

事案の発生率の高さに加え、その影響は、従業員、顧客、レピュテーション、監督官庁との関係、収益など、金銭的にも範囲的にも広がっている。

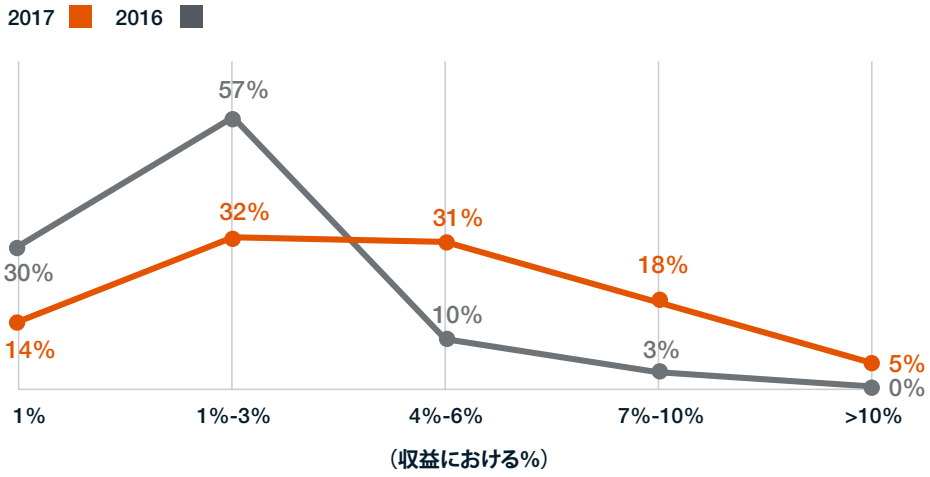
- 驚くべきことではないが、最も重大なものは、**従業員**に対する影響である。不正の被害に遭った企業の82%、サイバー攻撃の被害に遭った企業の81%、そしてセキュリティーインシデントを経験した企業の80%の幹部が、事件によって従業員のプライバシー、安全、士気が損なわれたと回答している。
- 約3分の2の回答者が、不正（76%）、サイバー攻撃（74%）、セキュリティ（74%）の各リスクによって、**顧客**に甚大、若しくは何らかの悪影響を与えてしまったと回答している。
- 約3分の2の経営者が、不正（65%）、サイバー攻撃（67%）、セキュリティ（66%）リスクによって、自社の**評判**を棄損したと回答している。
- 世界的に監督官庁による取締りが強まっている昨今のグローバル環境において、65%の回答者が、不正事件によって、**監督官庁**との関係が悪化したと回答している。
- 不正の被害に遭った78%の幹部が、**収益/事業継続**に、甚大、若しくは何らかの悪影響を与えてしまったと回答している。同様に、セキュリティインシデントの被害に遭った幹部の70%及びサイバーインシデントの被害に遭った69%の幹部が収益や事業継続に悪影響があったと回答している。

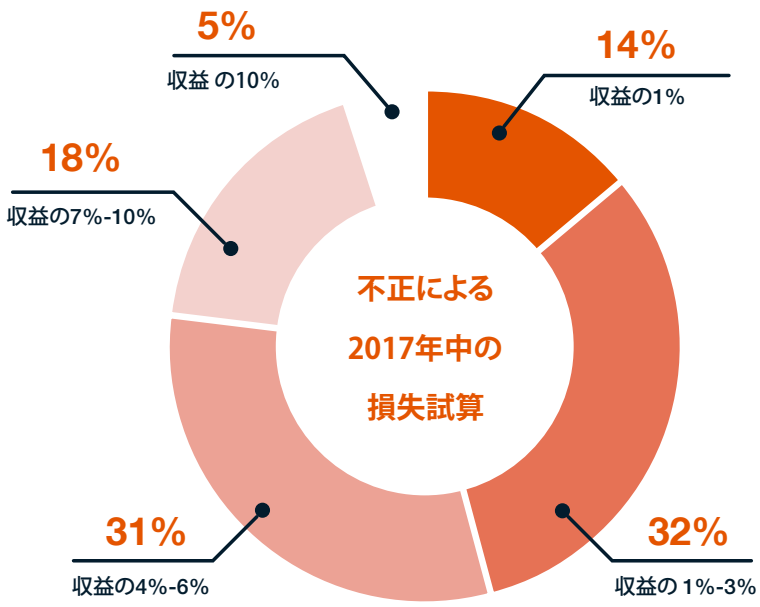
盗まれた資金や資産は、通常、複数の複雑な国々に隠されるため、それらを突き止めて回収することは、昔から非常に困難である。**本レポート24ページの記事では**、Glen Harloff, Dan Karson, Alex Volcicの各氏は、専門家の支援を仰ぐことによって、損失のかなりの部分を、回収困難な国々から取り戻すことができる、と説明している。

自社の[不正/サイバー/セキュリティ]インシデントにおいて次のような悪影響が ありましたか？



不正による過去12ヶ月の損失の試算





回答者たちは不正により甚大な経済的損失を受けたと主張する。

本年の調査では、およそ半数近く（46%）の回答者が、不正により、損失額は企業収益の3%以下と回答している。

特筆すべきは、企業収益の7%以上の損失があったという回答者は、去年は3%であったのが、今年に入っては実に23%にも上ったことである。

7%以上の損失を被った企業のうち、69%の企業が2つの業界で占められている。（小売・卸売・流通業＝35%、建設・エンジニアリング・インフラ業＝34%）

本レポート28ページの記事では、Tarun Bhatia、Reshmi Khurana、Oliver Stern、Brian Weihs の各氏が、サブサハラアフリカ、南米、南アジア等、新興国におけるインフラ投資のリスク並びにリスクを低減するための方策について紹介している。

増大する脅威に晒される秘密情報

ビジネスのあらゆる局面におけるデータ作成、収集及びデータへの依存に特徴づけられるデジタル世界においては、情報はますます重要かつ脆弱なものとなっている。

犯罪者は常に個人情報をはじめとする機密情報をマネタイズする方法を編み出そうとしている。従業員は極めてセンシティブな情報にアクセスでき、これが誤って、あるいは意図的に公開されたり、盗まれたり、削除される。さらに、知的財産や営業秘密が最重要資産である一方、増大する新たな脅威の影響を受けやすい宝であることにも気づいている企業も多い。

不正の種類

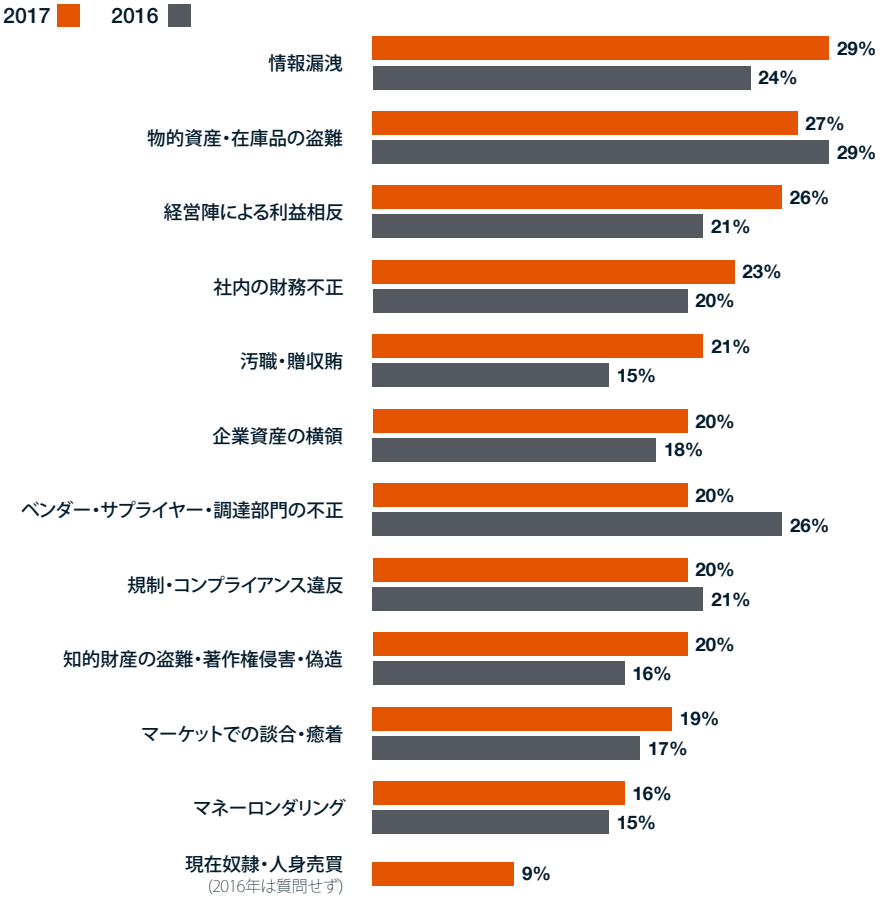
本レポートを発行した過去10年間で初めて、情報の盗難、喪失、攻撃というのが昨年1年間に最も多く被害に遭った不正（回答者の29%）という結果になり、2016年の調査で24%の回答者が答えた頃に比べると5%の増加を示した。

物理的な資産や在庫の盗難は、長い間最も普遍的な不正であったが、今回は2番目に多い27%の回答者が被害を受けたと回答した。

昨年度比で増加率が最も高い不正は腐敗及び汚職であり、21%の回答者が回答しているが、これは昨年度の15%という結果に比べると6%の伸びを示している。過去2年間で腐敗及び汚職の事案がほぼ倍になっていることを考えると、組織におけるリスクはかなり高くなっているともいえる。

21ページの寄稿では、Richard Dailly, Arturo del Castillo及びPaul Nashがどのように世界中の政府が汚職と腐敗撲滅対策を強化しているかについて掘り下げている。

過去12か月間に被害に遭った不正の種類



サイバーインシデントの種類

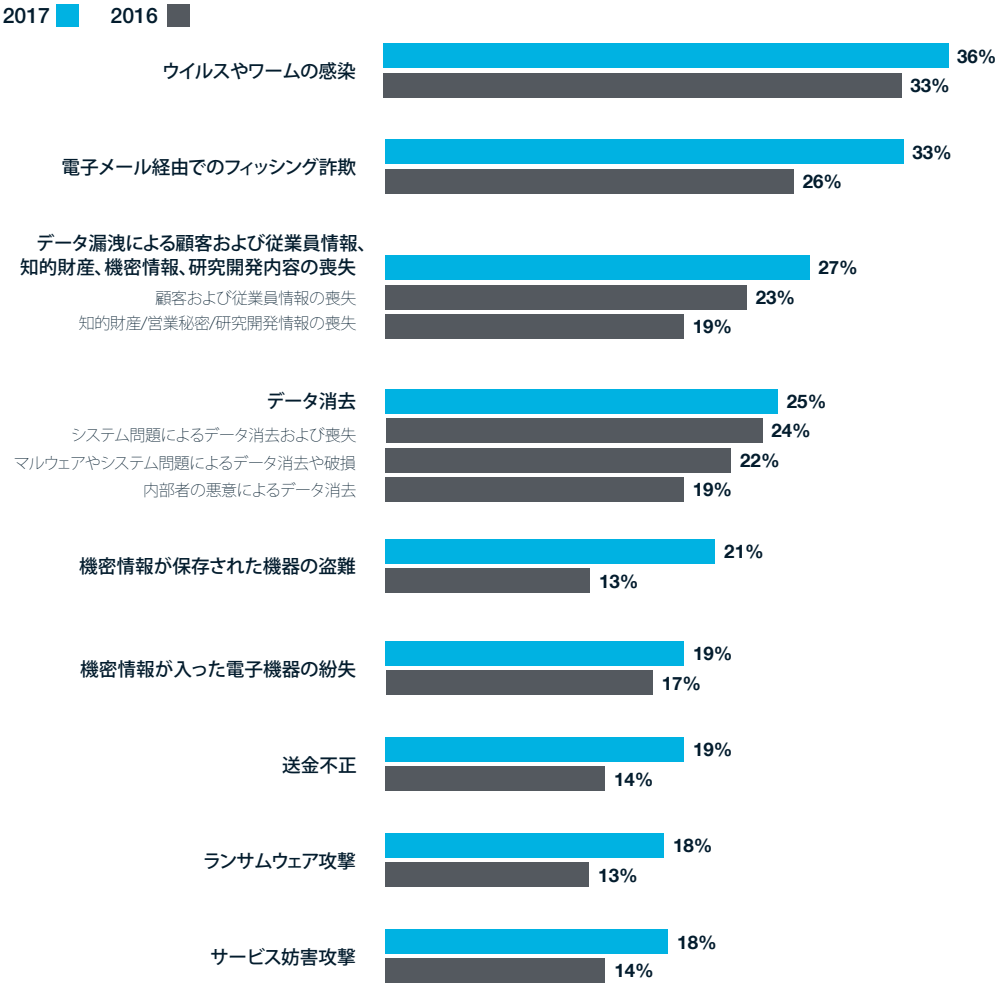
昨年度の回答者は、2016年度の調査に比べ、より多くの種類のサイバーインシデントの被害に遭ったと報告している。

WannaCryやPetyaといった著名なウイルスが世界に蔓延した年、ほぼ4割（36%）の回答者がウイルスやワームの攻撃に遭ったと回答し、前年比ベースでは3%増で、今年のレポートで名前が挙がったサイバーインシデントの中でも最も被害が多いインシデントであった。

昨年の調査では、メール経由でのフィッシング攻撃に遭ったと回答したのは4分の1（26%）であったのに対し、今年は3分の1（33%）の回答者が同様の被害に遭ったと回答している。さらに、今回データ漏洩やデータ消去の被害に遭った回答者はそれぞれ27%及び25%という結果であった。

しかしながら、すべてのサイバー上の脅威がデジタル領域に限定されているわけではない。調査に協力いただいた幹部のうち、機密データが入った機器が紛失したという回答者は19%、盗まれたという回答者は21%であったが、これらは物理的脅威とデジタルの脅威の収斂型ともいえる。

過去12か月間に被害に遭ったサイバーインシデントの種類

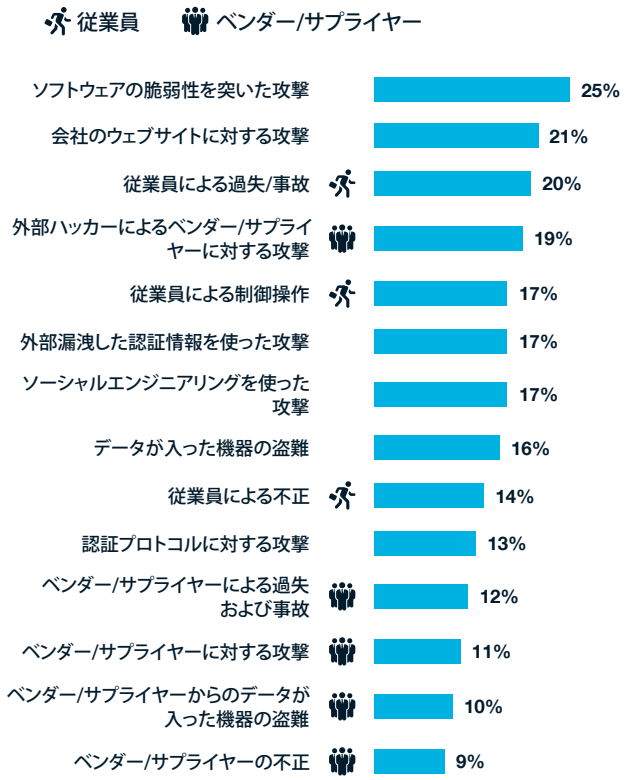


サイバーインシデントはどのように発生するのか

企業が被害を受けた特定のサイバーインシデントについて質問したとき、回答者の多くは、サイバー領域の複雑性を強調しつつ、1つ以上の攻撃区分について言及している。さらに、サイバーインシデントは内部であれ外部であれ悪者による不法行為、あるいは第三者や従業員の過失や事故に起因するしているとみられるという。

- ソフトウェアの脆弱性は最も多い攻撃区分であり、4分の1（25%）の回答者が指摘している。次に多いのは、会社のウェブサイトに対する攻撃であり21%の回答者が回答している。
- 従業員による過失・事故はかなり比重が大きく、5人に1人の回答者（20%）が回答しているのに対し、従業員による制御操作が17%、従業員による不正は14%という結果であった。
  本レポートの28ページでは、Alan Brill, Jonathan Fairtlough,Kenya Mann Faulkner, John Friedlanderが、情報セキュリティにおいて、従業員が実際にどのように働いているかを分析し、そこで得た知識を適切な規則やツール、コンプライアンスメカニズムに活かしていくことによって、組織がいかにして従業員を最重要資産にすることができるかという点について述べている。
- サードパーティもまた脆弱性の一つである。サイバーインシデントの被害に遭った19%の回答者が外部のハッカーによるベンダーやサプライヤーへの攻撃を通じて被害に遭っている。

貴方は自分の会社が過去12か月間にサイバーインシデントの被害に遭ったと回答しています。どのような被害であったか？（最大3つ回答可）

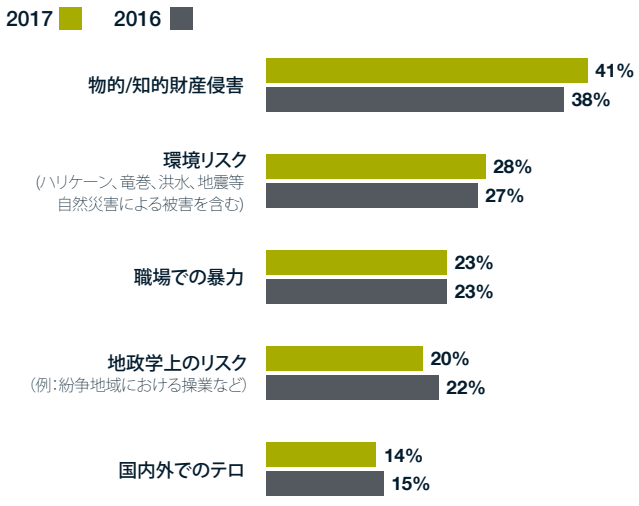


セキュリティインシデントの種類

昨年には、偽造商品から商標権侵害に至るまで、知的財産（IP）侵害の著名な事件や機密情報や芸術作品の盗難といった著名な事件が発生した。こういった事件はサイバー攻撃と物理的な侵入との合わせ技で起こることも多い。今年の調査でも、知的財産の物理的な盗難や喪失はセキュリティ事案の中では最も頻発した種類の事件であり、今年セキュリティに関する事件の被害に遭った回答者の中で、驚くべきことに41%もの人がこの種類の事件の被害に遭ったという。製造業の回答者はこういった物理的な知的財産の盗難及び喪失の最たる被害者で45%という回答であった。

環境リスクもまた大きな被害を与えるものであり、今年は28%の回答者が被害を報告した。これらのリスクは天然資源業界において最も多く（42%）、次に、ヘルスケア、製薬、バイオ（35%）、建設、エンジニアリング、インフラ（30%）と続く。セキュリティ関連事案の被害を経験したほぼ4分の1（23%）の回答者が、職場における暴力を指摘しているが、これは昨年と同じレベルである。

過去12か月間に被害に遭ったセキュリティインシデントの種類



社内外に潜む犯罪者

不正行為者

今回の調査では、企業への脅威として、社内関係者や元社員を挙げる企業が引き続き多い。周到に計画された単独犯によるもの、社内外の関係者との共謀によるもの、悪意のない不運な事故など様々であるが、社内に対する脅威に対処するためのトレーニング、社内ポリシーや手続きの作成は重要だ。

不正調査担当者は、不正であれサイバー攻撃、セキュリティ事案であれ、多くは内部関係者（幹部や中間管理職、一般社員、元社員、フリーランスやパートタイマーなど）　によるものが多いとみられる。

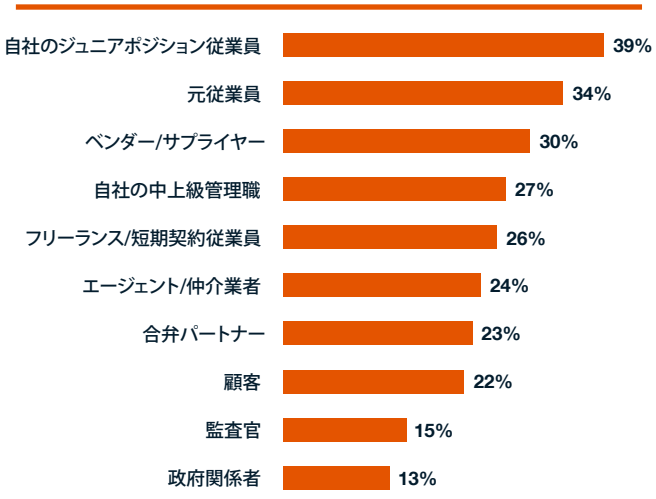
- 不正事案を経験した人々の81%が、単独または複数のインサイダーによるものと回答した。
- セキュリティ事案を経験した人々も、その71%が単独または複数のインサイダーによるものと回答した。
- サイバー事案経験者も、上記に比べるとやや低いがそれでも過半数の58%が単独または複数のインサイダーによるものと回答した。

内部関係者とともに、外部からの脅威についても、不正、サイバー、セキュリティの全てのカテゴリーで、上位を占めている。

不正の行為者

サーベイ回答者は社内関係者による不正行為が最も多いと回答しており、一般社員（39%）、元社員（34%）、幹部・中間管理職（27%）、フリーランス・パートタイマー（26%）となっている。エージェントや仲介者などの準社員も24%となっている。社内関係者が主要な不正行為者と指摘される一方、社内関係者による不正は特定されやすい。約半数（47%）の回答者は内部通報者によって特定され、44%は内部監査によって、35%は管理職によって発見されている。サードパーティも不正行為者として指摘されている。回答者の30%がベンダー・サプライヤー、23%が合弁相手による不正を挙げている。本紙寄稿者のKevin Braine, Julian Grijns, 影山正、そしてCem Ozturkが**30ページで**、サプライチェーンに潜む多くの不正リスクと、このリスクに対して企業がどう能動的に対処すべきかについて解説している。

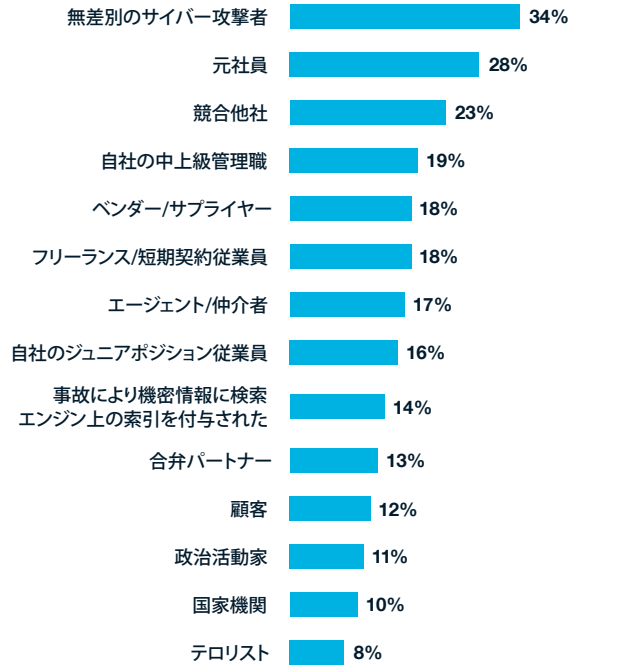
過去12ヶ月の間で、少なくとも1件の不正事案が発生したと回答されましたが、不正行為者は次のうちどれでしたか
（複数選択可）



サイバー犯罪行為者

過去12ヶ月の間にサイバー攻撃を経験した回答者は、外部者による行為が多いと回答しており、無差別のサイバー犯罪者（34%）、競合他社（23%）、ベンダー・サプライヤー（18%）となっている。無差別のサイバー犯罪者は今年のサーベイ結果で示されたサイバー犯罪行為者の中で最多となっている。ウイルスやワームによる攻撃やフィッシングメール攻撃が上位2つの攻撃形態であることを考えれば、サーベイ結果は特に驚くにはあたらない。これらの手口は世界中どこからで大量に攻撃することが出来るという観点からは、賭けにかけるような機会主義的な犯罪と言えよう。また、前述のように、内部関係者による行為の場合、偶然のミスあるいは不正によるものが多い。幹部・中間管理職（19%）、フリーランス・パートタイマー（18%）、一般社員（16%）となっている一方、元社員による行為と回答は28%である。

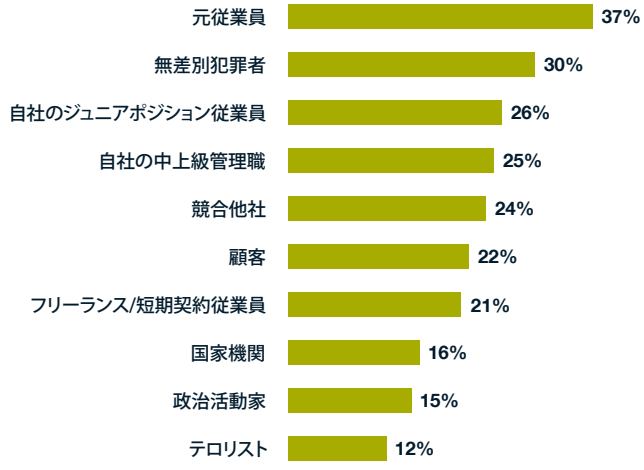
過去12ヶ月の間で、少なくとも1件のサイバー攻撃事案が発生したと回答されましたが、行為者は次のうちどれでしたか（複数選択可）



セキュリティ事案の行為者

セキュリティ事案に関しては、元社員によるものが最多で37%を占め、特にヘルスケア、製薬業、バイオテクノロジー業界には顕著な傾向で、54%と回答している。全業種で見ると、およそ4分の1が一般社員（26%）、幹部・中間管理職（25%）が主な行為者となっている。社外関係者の中では、無差別な行為者は30%を占め、特に運輸、レジャー、旅行業界では38%となっている。次に全業界でいえるのは競合他社（24%）である。ただし、小売、卸売、物流業界では33%と高くなっている。総合すると、顧客（22%）もトップ3に入っているが、消費財、運輸、レジャー、旅行業界からの回答では顧客関連による行為が31%と高くなっている。国家機関、政治活動家、テロリストという回答割合は16%、15%、12%と割合低いが、それでも二桁回答となっていることは注意を要する。

過去12ヶ月の間で、少なくとも1件のセキュリティ事案が発生したと回答されましたが、行為者は次のうちどれでしたか（複数選択可）



脆弱性とリスク軽減への道のり

この調査は企業の不正、サイバー、セキュリティリスクに対する脆弱性を浮き彫りにしている。リスク軽減のための対策を取ったにも関わらず、驚くことに回答者が、かなり、もしくは比較的高い水準で脅威が広まっていると認めている。脅威な材料になりうるリスクの無差別加害者の出現が、他の環境、もしくは地政学上のリスクに関する不安、そして当然、インサイダーや新しい手口など"ランダム(無差別)"なリスクへの不安感を抱かせている。

また、企業が、自分の組織に対する脅威がいつでも発生しうること、及び、現行の軽減策に自信がないことを認識していることを示唆している。リスクへの予測、発見、そして対応を効果的に行うには、新しい手法とリソースを模索しなければならない。

脆弱性の意識の上昇

脅威が増大する中、広範囲に渡って脆弱性の意識が高まったと経営陣が回答するのは予想外ではない。しかしながら、情報関連のリスクが不正、サイバー、そしてセキュリティのすべての部門において最も懸念されるべき事項であるのは着目すべきである。

不正

昨年最も多く報告された不正は情報の盗難・漏えい・攻撃であったが、同様にこれは最も懸念されたものでもあった。大多数の回答者(57%)は、高い、もしくは比較的高い水準で情報窃盗に脆弱性を感じ、同程度の56%が知的財産の盗難・著作権侵害・偽造を懸念していた。物的資産・在庫品の盗難はこれまでから懸念事項のトップであり、依然としてそれは変わらないものの(55%)、今では情報の脆弱性に関する懸念にトップを覆された。

以下の不正のタイプについて、自社の脆弱性はどの程度と認識していますか? (高い、もしくは比較的高いもののみ表示)

	2017	2015*	差異 (+/-)
情報の盗難 (データ漏洩など)	57%	51%	+6
知的財産 (機密情報など) の盗難・著作権侵害・偽造	56%	37%	+19
物的資産・在庫品の盗難	55%	62%	-7
経営陣による利益相反	52%	36%	+16
社内の財務不正	52%	43%	+9
ベンダー・サプライヤー・調達部門の不正	51%	49%	+2
マーケットでの談合・癒着(価格協定など)	50%	26%	+24
汚職・贈収賄	50%	40%	+10
規制・コンプライアンス違反	49%	40%	+9
企業資産の横領	48%	40%	+8
マネーロンダリング	43%	34%	+9
現代奴隷/人身売買	40%	n/a	n/a

*前年では設問されず、前々年との比較のみ。

サイバー

サイバーインシデントの脅威が 常に高い状態にあり、加害者が文字通り日々サイバー攻撃の新たな手口を開発している中、それと比例して被害者側の脆弱性に関する意識の増加が浮き彫りになっている。サイバーインシデントの各種類においては、半数、もしくはそれ以上の経営陣が、自身の企業で高い、もしくは比較的高い脆弱性を有していると認めている。

今日の各サイバーインシデントの種類において、自身の企業の脆弱性がどの程度と認識していますか？(高い、もしくは比較的高いもののみ表示)

	2017	2016	差異 (+/-)
ウィルス/ワームの感染	62%	54%	+8
データ消去	58%	51%	+7
電子メール経由でのフィッシング詐欺	57%	52%	+5
データの不正操作	56%	47%	+9
データ漏洩	55%	53%	+2
ランサムウェア攻撃	55%	44%	+11
機密情報が保存された機器の盗難	55%	52%	+3
機密情報が保存された機器の紛失	53%	49%	+4
サービス妨害攻撃	52%	47%	+5
送金不正 (電子メールアカウントの乗っ取り/詐称)	50%	43%	+7

サーベイの回答者によると、個人情報("PII")、保護された個人健康情報("PHI")、従業員情報、そして知的財産の紛失がマーケット全体より少なくとも15%高い数字が報告されており、ヘルスケア、医療、そしてバイオテクノロジー産業は 危機的な状況に追い込まれている状態である。

34ページの記事では、Devon AckermanとBrian Lapidusが、トレーニング、テクノロジー、そしてトップの姿勢が、ヘルスケア業界において保有しているセンシティブな情報を いかに強固に保護するに資するかについて議論している。

セキュリティ

同様にして、昨年は、物理的なセキュリティ脅威に対して脆弱性を認めた回答者の割合が増大した。物的/知的財産侵害は今年トップに返り咲き、情報関連の脅威に高い、あるいは比較的高い割合で脆弱であると63%の企業が認めている。ヘルスケア、医療、そしてバイオテクノロジー産業の回答者がこの類の脅威に最も脆弱であると感じており、79%が高い、あるいは比較的高い割合であったが、これは、プロフェッショナル・サービス業界の67%より12%高い数字であった。環境リスク(7%増加)、地政学上のリスク(9%の増加)、テロリズム(8%増加)の脆弱性を認識している回答者が増加しているという点も着目すべきである。

今日の各セキュリティインシデントの種類において、自身の企業の脆弱性がどの程度か認識していますか？(高い、もしくは比較的高いもののみ表示)

	2017	2016	差異 (+/-)
物的/知的財産侵害	63%	57%	+6
環境リスク (ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む)	56%	49%	+7
地政学上のリスク (例:紛争地域における操業など)	53%	44%	+9
職場での暴力	50%	49%	+1
国内外のテロリスト	49%	41%	+8

リスク軽減のための要諦

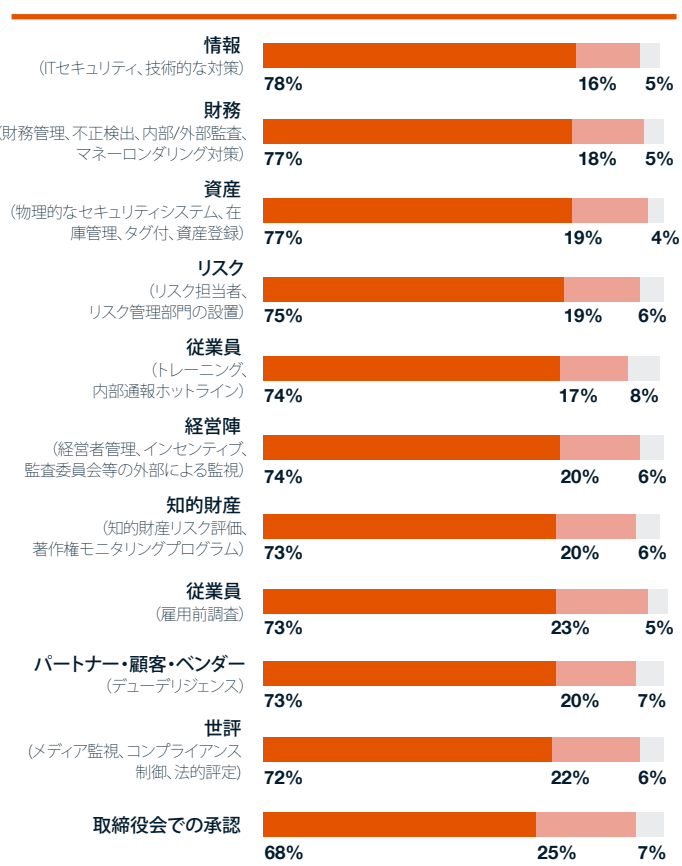
相互接続がより高まっているこの世の中で、企業はリスクというコインの両面を議論しなければならない一例えば、リスクは、いくつもの原因から発生するだけではなく、インシデントの反響も無数の方法があるように感じることがある。オペレーションの寸断、財務上の損失、レピュテーション上のダメージ、そして当局による捜査・調査の全てが、現在そして将来に有益な保護を与えるために、企業に持続可能なプロセスを確立し、支援するよう求めている。

プロアクティブなリスク低減の価値は、変動する昨今の規制環境に対処しようとする企業には明らかである。**36ページの記事では**、投資家が特に対米外国投資委員会の目を引きがちなアジア投資において、投資家がいかにしてプロアクティブに米国の規制及び投資リスクをコントロールしていくかの4ステップをViolet Ho、Lamb-Hale、村崎直子が論じている。

不正

サーベイに明記されたほぼ全ての不正対策は、70%以上の回答者に広く取り入れられている。取締役会の関与だけが68%という唯一低い数値であり、規制の強化、取締り、高い不正の発生率、極端に幅広くコストの大きい反響に直面していることに鑑みれば驚くほど低い結果であった。しかしながら、25%の回答者が1年以内には取締役会の関与を得ると回答している。最も広く取り入れられた不正対策は情報に関するコントロールである　一　例えば、ITセキュリティの78%、財務的コントロールと保護、及び、物的資産の管理が次に並び、共に77%である。内部関係者による脅威に対する対策としては、従業員トレーニング/内部通報ホットライン(74%)、従業員雇用前調査(73%)を実施した企業が4分の3未満であった。ただし、ポジティブな点は、来年以降に向けて、多くの回答者が自社で様々な対策を実行する予定であると答えている。これらが実際に実行されれば、調査回答者の90%以上が、不正をある程度まで軽減する全ての方法を取り入れることになる。

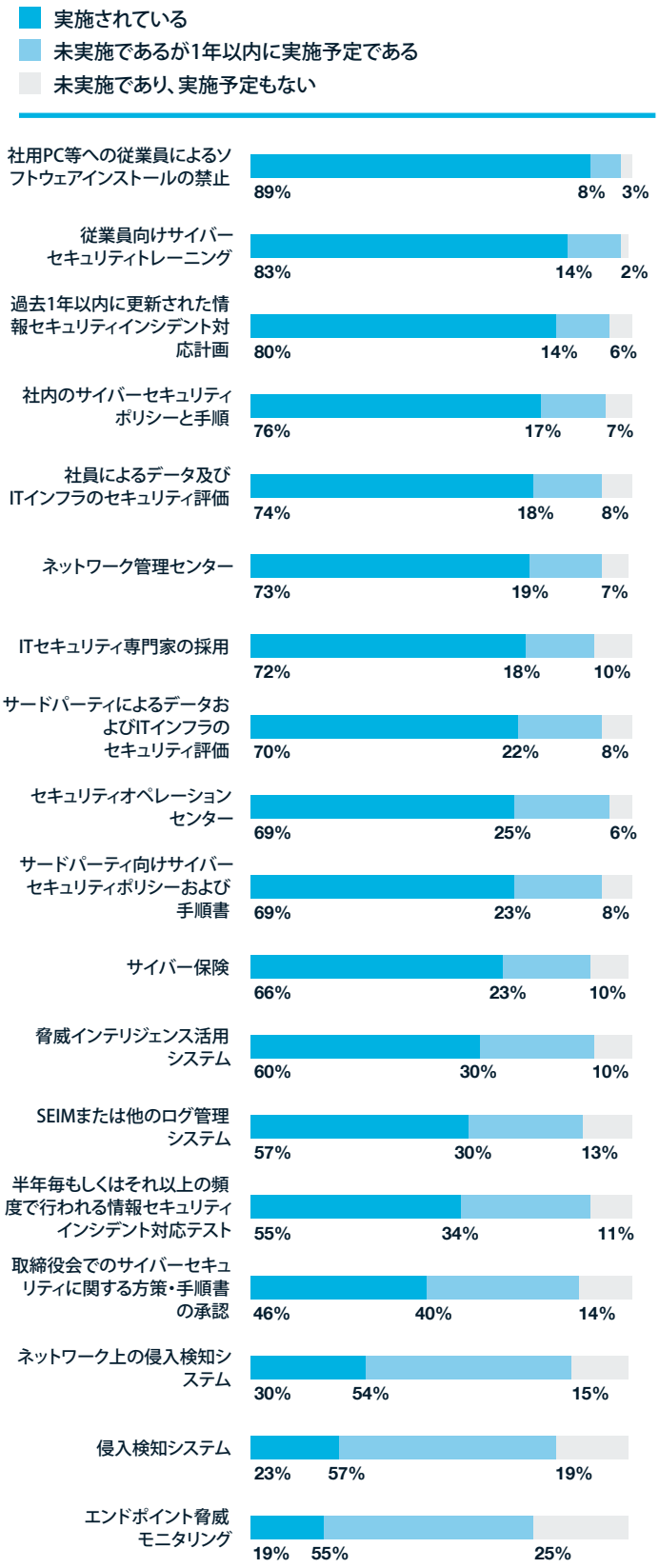
以下のいずれかのうち、どちらがあなたの会社の不正対策の現状をより反映していると思いますか



サイバー

内部関係者がサイバーインシデントの主犯であることを考えると、ほとんどの回答者が従業員にフォーカスしたリスク低減策を既に実行していたのはとても心強い。最も多く実行されたのはソフトウェアのインストールの禁止(89%)、そして従業員向けサイバーセキュリティトレーニング(83%)である。インシデント対応プランもリストの上位にあり、80%の回答者が既に対応プランを適用していた。前述のように、調査回答者はハッキングに脆弱であることを認めており、1年以内に自身の会社で実行を望む対策の上位3つは、侵入検知システム(57%)、エンドポイント脅威モニタリング(55%)、ネットワーク上の侵入検知システム(54%)である。監督官庁の圧力の増加に伴ってインシデントも増加する可能性が高まりつつあることと、データプライバシーに繋がるレピュテーションリスクには大きなコストがかかることから、サイバーセキュリティはものすごいスピードで取締役会へ統制委任される案件となりつつある。回答者の46%がすでに現状で取締役会を巻き込んでおり、40%は向こう1年間でそのようにしていく予定だ。**38ページの記事では**、Andrew Beckett、Paul JacksonとJason Smolanoffがサイバーリスク緩和に向けての施策において、取締役会の実践的な役割を確立し効果的なスタートを切ることが出来るようにするための7つの議論のポイントを提案している。

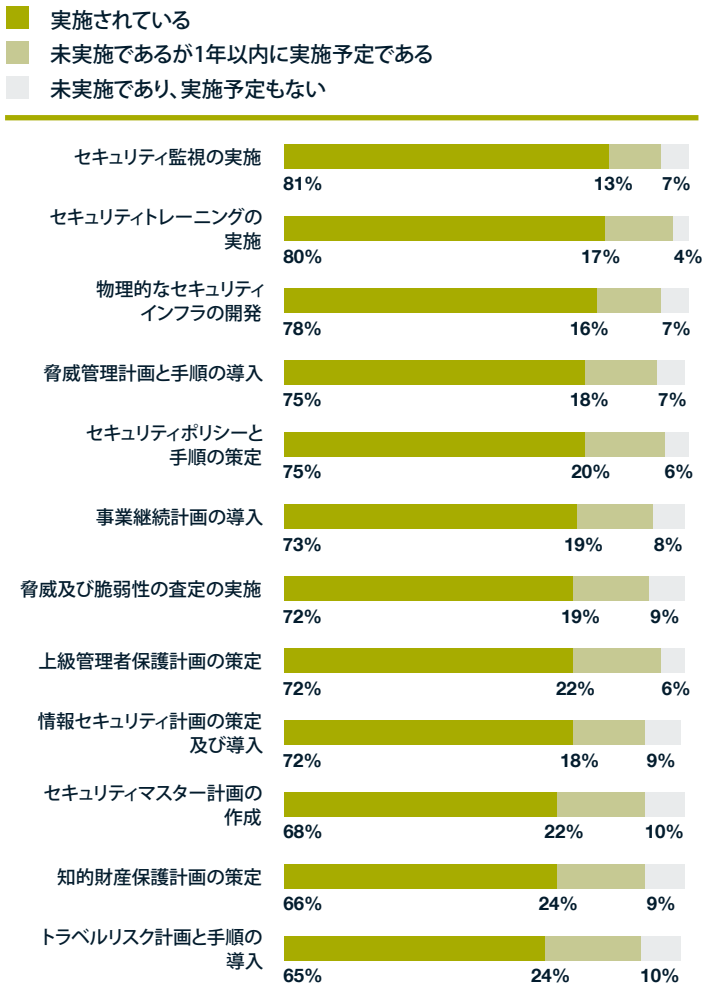
以下のいずれかのうち、どちらがあなたの会社のサイバーリスク軽減策の現状をより反映していると思いますか

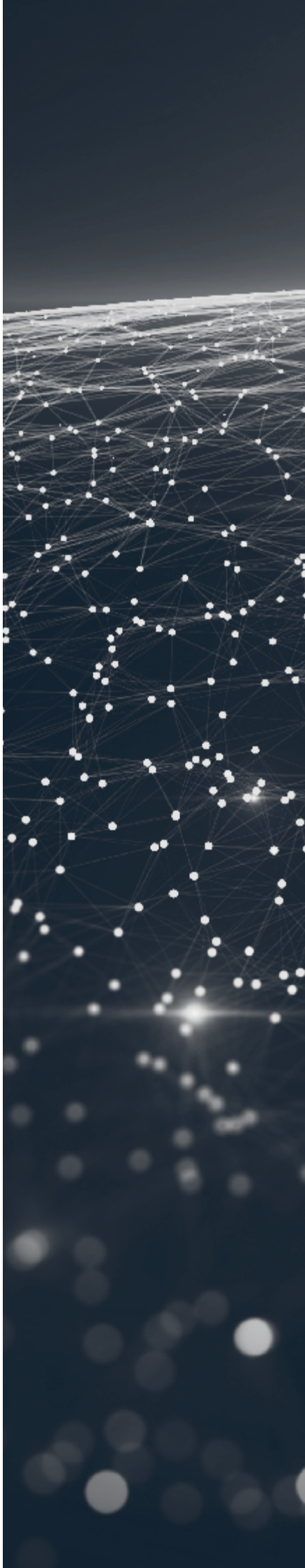


セキュリティ

大部分の回答者は、セキュリティ監査(81%)を筆頭に、セキュリティトレーニング(80%)、そして物理的セキュリティインフラの開発(78%)のリスク軽減対策をとっている。高いインシデント発生数と脆弱性の不安が常に残る物的/知的財産侵害において、驚きなのは知的財産保護対策が66%の最下位、トラベルリスク計画と手順の導入がほぼ同列で65%であった。だが安心材料は、およそ4分の1(24%)の回答者が向こう1年でこれらの対策を実行する予定であることであった。

以下のいずれかのうち、どちらがあなたの会社のセキュリティリスク軽減対策の現状をより反映していると思いますか





後書き

今回で10回目となる"Kroll Global Fraud & Risk Report"は、世界の多くの企業が、不正、サイバー攻撃、セキュリティ侵害に悩まされていることを、改めて浮き彫りに しました。
いまだかつて経験したことのない昨今の脅威に適切に対応するには、経営者は、綿密な計画、導入、適切なリソース確保を、絶えず考えなければ なりません。

昨今のデジタル化されたグローバル市場において、情報は、それが持つ価値と脆弱性のために、最も守るのが難しい経営資源と なりました。

回答者が、情報の国外流出を最も懸念していることは、驚くべきことではありません。

情報に関わる脅威は、不正、サイバー攻撃、セキュリティ侵害といったリスクに共通した最大の懸念事項なのです。

情報に関わる脅威によって、企業が被害にあった場合のコストや影響の大きさを考えた場合、効果的な対策、対応、改善案の策定は、これまでになく必要不可欠なものとなっています。

しかしながら、グローバル経済の集中化、デジタルによる複雑な関係性、何度も繰り返される人的要因は、もはや、不正、サイバー攻撃、セキュリティ侵害といった単独の問題として、リスクを片付けることができないことも表しています。

組織が、今後起こりうるリスクに対して上手く対処するには、今までの分野を超えたアプローチが必要であることを、本調査は明らかにしています。

講評

予測、検知、予防、そして対処

我々は汚職・腐敗との闘いに勝利できるのか？

著者：Richard Dailly, Arturo del Castillo, and Paul Nash

今年のGlobal Fraud & Risk Report実態調査では、汚職・腐敗の発生が2016年の15%から21%に増加し、発生した不正のタイプランキングでは10位から5位に浮上していることが認められた。わずか11%であった2015年の実態調査結果を振り返ってみると、この2年間で汚職・腐敗の報告が倍増していることがわかる。

汚職・腐敗は増加しているようにも見えるが、企業側も、よりそれを検知する力をつけている。また、監督官庁の観点で言うと、世界中の政府もこの問題に取り組むようになってきている。

欧州、中東、アフリカ

フランス、ドイツ、アイルランド、スロバキアなど、いくつかの欧州諸国では、最近新たな汚職・腐敗対策法の導入、または制定に向けての提案が打ち出されている。また、昨年英国では大きな進歩が見られ、重大不正監視局(SFO)が英国贈収賄防止法（UKBA）を使っていくつもの事件の捜査と摘発に成功した。特記すべきこととしては、英国でもいくつかの目立ったケースで、米国式の起訴猶予合意(DPA)が使われたということである。ある大手エンジニアリング会社のケースでは、裁判官の承認が必要とされたケースであるが、インドネシア、タイ、インド、ロシア、ナイジェリアなど7カ国にわたる4年間の汚職・腐敗捜査の集大成となった。その企業の最終的な和解金額は、4.97億ポンドに加え、別途米国にて1.7億米ドル、ブラジルにて2千5百万米ドルにも上った。

SFOの汚職・腐敗告発に対する集中的な取り組みにより、大企業だけでなく中小企業も告発の対象であること、また、英国企業の贈収賄は海外でも行われていたということが明らかとなった。その結果、企業は改めてコンプライアンスシステム見直しを強化し、自社の世界中のオペレーションの贈収賄リスクを検証することとなり、それは新興国市場への投資判断に直接的な影響を与えることになった。

さらに、英国の犯罪財政法は腐敗防止に当たり大きな効果を発揮している。2017年9月30日に成立されたこの法律は、脱税ほう助を防止義務違反という新たな企業犯罪を確立させ、Unexplained Wealth Ordersを導入させた。

ケーススタディ

クロールは、最近アフリカにてある国の検察当局の汚職・腐敗関連の訴訟を支援し、10億ドルの調達契約に絡む犯罪やその他の不正の有無の調査を実施した。この調査は、アフリカ、中東、英国から収集した数々の資料のレビューから始めたが、何年にも渡る疑わしい支払い記録を浮き彫りする為、データアナリティクスの技術も駆使した。またこれらの作業に加え、関係者との現地でのインタビューも行った。

アジア太平洋

中国政府にとって、過去5年間の汚職防止キャンペーンは国内政策の中でも最重要課題であった。20万人以上の官僚の汚職の摘発に成功したことで、現指導者の不動の人気が確立された。

これまで、中国が関わる反汚職条項違反による海外汚職行為防止法(FCPA)執行の成功例は極めて少なかった。汚職を証明することは非常に難しく、管轄権も問題となることが多い。官僚が収賄している証拠を突き止めるのが難しいというのは周知の事実である。しかし今は、中国が自国で官民双方の汚職の捜査に取り組みだしており、過去何年もの間明らかにならなかったた汚職のスキームが露呈されてくる可能性も見えてきた。

アジア太平洋地域のその他の地域では、汚職と腐敗は常に企業が直面する2大リスクとして挙げられている。確認される成果としては、まずインドネシアの汚職撲滅委員会(KPK)がますます成果を挙げており、最近では、国への損害金額が1.4億米ドル以上にものぼった有名なE-KTPの汚職ケースを見事逮捕に導いている。また、フィリピンのドゥテルテ大統領は、地域特有の汚職対策を期待されて選出されている。マレーシアの反汚職アカデミーは、汚職対策に関して当地域で最も評価されるような拠点となるべく、設立された。タイの軍政府は腐敗を撲滅することを約束した。また、ベトナムの新しい指導者たちは、最近腐敗容疑で数多くの著名人を逮捕している。

しかし実際には、この地域の各国政府が果たして政治的に中立なのかどうかを疑う人もいるようだ。KPKは独立しているとは言え、政治的に偏っているという見方も多い。ドゥテルテ大統領の汚職対策のスタンスはどちらかと言うと国家主義や大衆主義のような別物に変形してしまっており、組織的に政府機関を解体していくことで長期的には更なる腐敗を促進することになりかねない。最近のベトナムの官僚の汚職容疑での逮捕は、一部の関係者によると政界最上層部の権力争いによるものだという見方もある。マレーシアの政府機関は 1 MDB スキャンダルの対応について世界中から非難され、国際的なプレッシャーがあったにも関わらず、昨年2016年半ばに、マレーシアの法務長官が不正の証拠は見られなかったと発表した。またタイでは、2016年に新しい汚職対策新法が導入されたにも関わらず、トランスペアレンシー・インターナショナルの2016年版腐敗認識指数では、前年の78から101に悪化し、フィリピンと同位、インドネシアを11位も下回ってしまった。

北米と中南米

2017年初めにFCPAの今後の執行に関して物議が醸されたにもかかわらず、今年はFCPA捜査で大変忙しい年となった。2017年に米国政府が実施したFPCA関連の捜査は38件に及んだ。

近年の大型の贈収賄捜査の一つとして、ブラジルの行政機関がその他数カ国の当局と合同で行った洗車作戦（Operation Car Wash）が挙げられる。この、ブラジルの建設業者Odebrechtとその子会社である石油化学メーカーBraskemに対する捜査では、複雑で巧妙な腐敗のスキームが明るみになり、ブラジル、米国、スイスの行政による合計26億米ドルの罰金が命じられた。このことは、中南米における贈収賄の摘発に確実な変化の到来を告げたのである。

Odebrechtが全11カ国（中南米9カ国、アフリカ2カ国）で贈賄行為を行っていたことが発覚したことで、事件は国際問題に発展した。Odebrechtの一件で分かったことは、贈収賄というのは多くの場合、単なる違法な支払いではないということである。世界経済では、汚職は複雑な金融メカニズムを通じて起こるものである。Odebrechtの関係者達は、（世界中の偽装口座を次々に介して）12カ国以上の政治家の懐へ現金を送っていた。

贈収賄は、その他の犯罪と同じで、犯人に (a) 動機、(b) 機会があり、また、(c) モラルの観点から自分の行いを正当化できてしまう場合に起こる。これらの要素を一つでも除くことができれば犯罪の発生を防止することができる。企業は汚職・腐敗対策プログラムをしっかり活用して準備を整え、事業に大きく有害な影響が及ぶ前に、強固な防御を固め、事態を検知し、対応できるようにしておかなければならない。

[1] Lawler, D. 著 (2012). Frequently Asked Questions in Anti-Bribery and Corruption. Wiley, 326.

RICHARD DAILLY
クロールアジア太平洋地域 調査・訴訟支援部門
東南アジア担当代表
マネジング・ディレクター
rdailly@kroll.com

ARTURO DEL CASTILLO
クロール中南米 調査・訴訟支援部門
アソシエイト・マネジング・ディレクター
arturo.delcastillo@kroll.com

PAUL NASH
クロール欧州・中東・アフリカ 調査・訴訟支援部門
アソシエイト・マネジング・ディレクター
paul.nash@kroll.com

不正調査、仲裁裁定と審判による隠匿資産の解明

著者：Glen Harloff, Dan Karson, and Alex Volcic

今年のGlobal Fraud & Risk Reportの調査から、不正に関連した損失がかなり増大していることが明らかになった

社内不正のケースでは、不正の疑義が申し立てられて調査が行われると、通常は次は被害回復に目を向けることになる。同様に、仲裁裁定者、判決債権者、そして不良債権の債務者を追っている金融機関は、凍結もしくは回復可能な資産を特定するのに、しばしば専門家による支援が必要となる。

ほとんどの債務者は、当初より債務不履行にするつもりで借金をすることはない。また、自分が残した昔の資産の痕跡を消去することはない（もしくはできない）。不正の加害者にも同じことが当てはまると言えよう。では、どのようにして失ったお金を探し出すのか？

資産の痕跡の調査

企業としての戦略は、ターゲットとする債務者の歴史を、ローンや契約の日付けよりかなり以前まで遡って細かくリサーチするところから始めるべきだ。資産調査には、公開情報や情報データベースの包括的検索も含まれる。国や場所にもよるが、これらの資料には、不動産や、株式保有、口座情報、自動車、船舶や航空機その他の資産の証拠や重要なヒントが含まれていることがある。

ソーシャルメディアもまた、資産に関する情報の宝庫である。例えばクロールの調査でも、パスワードで保護されてもいないソーシャルメディアのページ上で債務者やその家族が明らかにしている資産やその証拠を発見したこともある。これは決して珍しい出来事ではない。24時間コミュニケーションをし続けてすべてを語らなければならない現在の我々の世界では、調査対象やその家族は無分別かつ見境なく情報を広めることがある　－　例えば、週末の家庭や贅沢品の写真などを自ら言いふらしているのである。

このような足跡を分析した後は、次の戦略は、外部調査やヒューマンインテリジェンスへとシフトされることになる。

債務者/不正行為者が依然としてアクティブなビジネスに関わっているのは良いニュースである。というのも、売掛金、キャッシュフロー、銀行との関係、クレジットカード、顧客及びサプライヤーが存在していることを意味するからだ。（ローンや信用枠を申請する際、不正行為者は資産と負債のリストが掲載されている純資産計算書をしばしば提供している。）　他の有効な情報源は元従業員、ベンダー（"支払い銀行はどこか？"）、顧客（"支払銀行はどこか？"）、以前の取引先や訴訟相手などである。

GLEN HARLOFF
クロール中南米 調査・訴訟支援部門
シニア・マネジング・ディレクター
gharloff@kroll.com

DAN KARSON
クロール 調査・訴訟支援部門
アメリカ地域会長
dkarson@kroll.com

ALEX VOLCIC
クロール欧州・中東・アフリカ 調査・訴訟支援部門
ロシア& CIS地域代表
シニア・マネジング・ディレクター
avolcic@kroll.com

管轄権の問題

お金と資産は複数の複雑な管轄権に散在している可能性があり、かつ一部は昔から資産回復するのが難しい場所にある可能性もある。全てのステージを通して、ハードルが最も低い場所からフォーカスしていくことが重要である。すなわち、最も執行しやすい場所から調査を始めるべきということである。

安全に資産を隠せる国は少なくなってきている一方、資産を隠匿する方法はますます発達してきている。民間の投資ビークルの激増と電子送金のスピード、マネーロンダリング防止法と銀行の社内規定に関わらず、地域によって行われている銀行幹部の共謀、依然として資産逃避先として利益を得ている国の存在、富裕層のペテン師に対して疑いなく対価を得てシェルターを提供する政府や国家元首の存在などが、資産の隠匿を容易ならしめているのである。

しかしながら、専門家の支援を求めている債権者には、たとえ厳しい管轄地域だったとしても、潜在的に重要な損失回復が出来る現実的な希望を持つことが出来る。事実が公式な刑事捜査に値するならば、債権者は刑事共助条約（"MLAT"）のもとに政府からの支援を検討すべきである。MLATは、とりわけある締約国で得た特定の個人や企業による特定の犯罪の証拠を別の国で得ることができることを容易にする多国籍条約である。救済策は政府のみの利用となる。しかしながら、資産調査の多くは被害者である債権者を援助する裁量を持つ政府による捜査と並行して行われる。昨今のクロールの事案においても、財務記録の精査と外部調査の相互作用が非常に重要となったケースがある。

あるロシアの銀行は、自身のトレーディングフロアで起こった不正で3億ドル以上の損失に至った。クロールは、コンピュータフォレンジックスと公開情報調査で補完しながら、ブルームバーグ取引システムの財務調査とフォレンジックインタビューからなる現地調査を行った。この作業フェーズでは、銀行が不正の被害を受けたことを確認するとともに、資産凍結及び公開に向けてのロンドンでの法的手続きを支援する結果となった。第2フェーズでは、さらなる開示と不正収益を特定するため、クロールはクライアントや法務アドバイザーと協力し、民事・刑事調査戦略を実行した。

MLAT手続を活用し、クロールは資金の流れに関して国際銀行システム経由での資金の流れに関する情報を得るために銀行を支援し、企業の裏の顔を露呈させることに成功した。また、クロールは、公開情報収集と現地における人的情報収集により、中東や北米、南米とともに、ブルガリア、ウクライナ、ジョージア、アゼルバイジャン、タジキスタンといった欧州及びアジアにまたがる資産を割り出した。

クロールは複数の地域における資産を回復させるため、英国で民事不正申立てを支援するための専門家証人報告書を提供した。我々のサイバー・チームは100テラバイト以上の電子データ書類を保全、プロセス、レビューを行い、公判用資料を作成した。クライアントと協力し、金融当局への報告と、当局の調査支援をも行った。英国で行われた民事裁判では、銀行寄りの判決が出され、多額の不正収益を回収することが出来たのである。刑事訴訟手続きでは、主な被告2名は有罪となり、長期服役刑に直面する結果となった。

英国及び前英国領地で適用されるNorwich Pharmacal Order（第三者開示命令）及び/又はMLATに近い民事ツールであり、調査担当者に対して、オフショア企業の口座記録や取締役や幹部、株主の情報を提供してくれる。Norwich Pharmacal Ordersは複数管轄のケースにおいてクロールを支援してくれる手段となった。

クロールが中東のクライアントを支援していた際、会社の口座から500万ドルの流出を確認したことがあった。容疑者は特定されなかったが、調査員がカリブ地域の金融機関に資金が動いたことを確認した。クロールは宣誓供述書を準備し、調査の状況を説明して、現地カリブの法律事務所の力を借りながら当該銀行にNorwich Pharmacal Ordersを適用して、顧客情報（"KYC"）を含めた銀行口座情報の詳細を開示するように求めた。この命令により銀行口座の受益者の特定が出来、まだ400万ドル以上の資金が口座に残されていたことが判明した。法律事務所の支援をさらに借りて、資金はすぐに凍結され、結果的にクライアントに返戻されたのである。

金銭関連の裁判の判決を勝ち取ったり、資産を隠匿して豪勢な暮らしをする債務者や詐欺師を追跡するよりもストレスを感じる状況はそうない。しかし組織化された調査戦略と適切なツールがあれば、その壁を取り払うことは可能だ。ターゲットは逃亡するかも知れないが、資産を隠すのはますます 至難の技になっている。

新興市場におけるインフラ投資ーリスクと闘う

著者：Tarun Bhatia, Reshmi Khurana, Oliver Stern, and Brian Weihs

投資家は、エネルギーや、輸送、通信ネットワークに対する需要の増加に対応するため、サブサハラアフリカ、南アジア、中南米における資本集約型インフラプロジェクトに出資している。

インフラプロジェクトは、成熟市場における利回りを上回る潜在的収益率を背景にしており、投資家にとっては魅力的だ。しかし、特に建設、エンジニアリング、インフラ部門を中心にリスクは付き物であり、我々の調査でも不正事案（前年度比13%増の83%）とサイバーインシデント（前年度比16%増の93%）の数値が前年に比べて最も高くなっている。セキュリティインシデントについてもまた67%に増加している（前年度比4%増）。

この記事では、さまざまな新興市場において投資家がリスクを特定し軽減出来るようにするため我々のチームの知識と経験をご紹介したい。

サブサハラアフリカへのインフラプロジェクト

インフラ投資成功にあたっては、主管区の既存ネットワークの輸送、発電、配電網プロジェクトの統合が必要である。これは単にエンジニアリングの課題ではない。大規模かつ長期的な投資に対応するためには、制度的な能力と機能する法規制の枠組みが必要だ。

多くのサブサハラアフリカ地域には、既存のインフラを新しいプロジェクトにリンクさせるための計画能力とリソースに欠けている。例えば、生産者が固定価格制度を用いて電力を売却するための送電網にアクセスできない限り、発電事業は失敗となる。プロジェクトのフィージビリティをより評価し易くするために規制環境と主要な政府機関の実施能力を理解する上で、投資前のインテリジェンスの収集が有益である。

この地域の多くの新しいプロジェクトは政治的に重要であるため、不透明な干渉や影響を受ける可能性がある。政治家は、自身のプロフィールを高め選挙区内で人気を得るため、インフラプロジェクトを奨励する。そのプロジェクトへの非現実的な期待も、投資の商業実用化に害を及ぼすだろう。例えば、鉄道貨物事業の投資家が政治的・社会経済的優先事項を満たすために旅客輸送提供を期待される場合、投資の経済性は歪む可能性がある。

投資家はこのようなレッドフラッグに気付くべきだが、直接影響を与えることが出来ないこともままある。ただ、出発点として、投資家は国の政治経済の文脈の中で、プロジェクトのモチベーションとインセンティブを理解しておく必要があるのだ。

TARUN BHATIA
クロールアジア太平洋地域
調査・訴訟支援部門
マネジング・ディレクター
tarun.bhatia@kroll.com

RESHMI KHURANA
クロール 調査・訴訟支援部門
東南アジア地域代表
マネジング・ディレクター
rkhurana@kroll.com

OLIVER STERN
クロール欧州・中東・アフリカ
調査・訴訟支援部門
アソシエイト・マネジング・
ディレクター
oliver.stern@kroll.com

BRIAN WEIHS
クロール 調査・訴訟支援部門
メキシコオフィス代表
マネジング・ディレクター
bweihs@kroll.com

南アジアでのインフラ投資に残る課題

南アジアインフラプロジェクトの投資家は、類似した課題に直面している。例えば、企業の拡大したバランスシートや銀行の不良債権増加が重なり、インドの民間部門のインフラ投資は過去3年以上減速している。プロジェクトに関連する様々な政府当局（例えば、土地利用可否や環境浄化問題関連の承認など）の承認のペースも依然として遅い。

投資活動は、南アジアの一部の分野、特にインフラでは高いままだ。このような例の1つとして、インドでの再生エネルギー分野が国内外の投資家から大きな関心を集めている。インド政府にとって再生可能エネルギーの成長は依然として重要な目標であるが、目標（2022年までに175GW）の積極的な推進は、その分野の経験が少ない、もしくは全くない多数のプレイヤーの参入により、太陽エネルギーを中心とした取込価格の急激な低下に終わった。これは、低価格でプロジェクトを納入する計り知れないプレッシャーを地元開発者に与え、結果、資材の質やプロジェクトの持続性に影響を及ぼすことになる。同時に、企業は地方自治体や他のステークホルダーと協力して適切なタイミングで必要な承認を得る必要があるが、汚職のリスクが依然残る。新規プロジェクトのコストが急減すると、既存プロジェクトの電力購入契約（新規プロジェクトのために提案されている価格と比較して1メガワット当たりのコストが大幅に高い）も公共の反発と行政監視の影響を受けやすくなる。

投資家がプロジェクトのコストとパフォーマンスが健全に反映されているかを見極めるには、しばしば苦労を要する。インドにおける企業、政治家、そして官僚間の関係が比較的近いことを考えると、潜在的に不適切なオペレーションがなされていることがしばしばあり、財務報告に直接影響を与えるからだ。報告書の内容と実際のプロジェクトパフォーマンスの大きなギャップが、全体的な品質と財務の整合性に疑問を投げかけている。他のバングラデシュやスリランカのような南アジア市場でも、同様の問題にさらされている。

これらの課題はリスクを伴うが、機会の重要性がリスクのコストに勝ることもある。現地市場の原動力を深く理解することによって、投資家はより大きな自信を持って前進し、サプライズの少ないリターンを期待して投資を行うことが出来る。

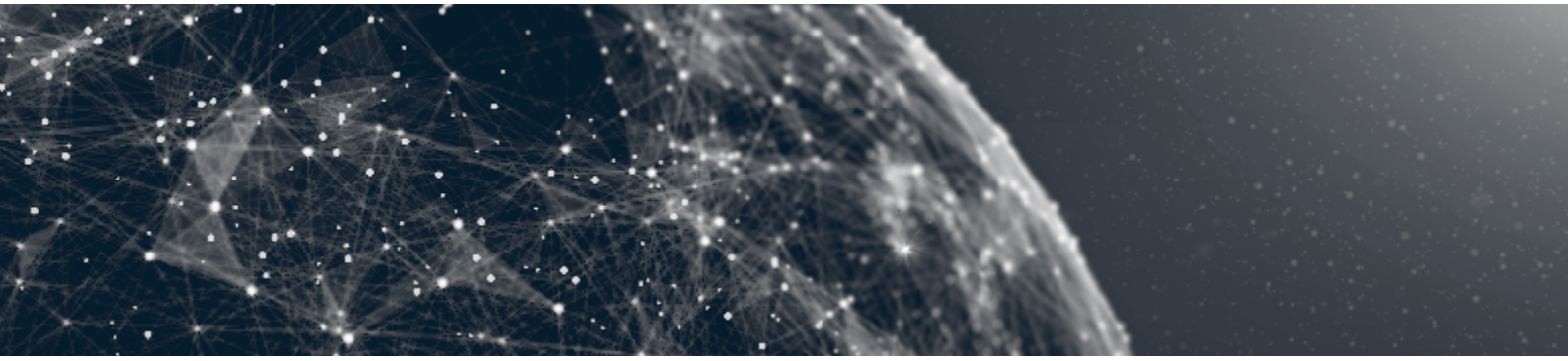
中南米のインフラ投資に関する問題

中南米では、最近の大規模汚職の発覚がインフラプロジェクトに大きな影響を与え、政府への出資を滞らせ、工事途中のプロジェクトを凍結させることとなった。この問題は、最近地元ブラジルの大手建築業者が捜査・訴追されたことで明らかになったのだが、28ヵ国（特にペルー、コロンビア、ベネズエラ、メキシコ）に30億ドル以上の賄賂を政府高官に支払っていたというものであった。

ブラジル、メキシコ、アルゼンチンといった地域最大の国々のエネルギー、輸送、通信プロジェクトもまた、土地の権利取得に苦戦している。前世紀における中南米の国々の土地改革は、共同土地権利と長年の紛争による遺産としてもたらされた。これにより立入りや所有権の交渉に困難と不確実性が生じ、プレッシャーがかかる開発者に手っ取り早い方法を促すことになった。例えば、メキシコシティーの新しい空港開発に向けての努力は土地権利取得に関する紛争で何十年にもわたって阻まれてきた。投資家当事者間で、リスクと、どのように土地アクセスと所有権を取得するかを理解しておく必要がある。土地所有者とコミュニティとの関係の投資前の調査は、投資家が土地権利取得プロセスに関連するリスクを数値化する手助けとなる。

中南米最大の国々の有権者が左派や人民主義の政府から離脱し始めたことから、輸送と公共サービス分野で官民パートナーシップ（"PPP"）投資への新たな関心が高まっている。しかし、PPPへの投資が増えれば、次の政権からの監視にさらされることになり、経済的利益が明確ではない大規模プロジェクトの再評価や解約さえも生じることがある。最近の事例では、コンバインドサイクル発電所の開発に、民間分野の建築業者、および公共分野のスポンサーが関与していた。クロールの調査・分析により、プラント開発の交渉工程のインテグリティに対して民間の投資家に対して安心を与え、投資を進める結果となった。

インフラ投資家は、プロジェクトの資金調達、開発、および運営を成功させるために複雑な一連の課題に対処する必要がある。投資家は、十分な取引前の準備と、プロジェクトサイクルのインテリジェンスを利用することにより、投資戦略において自信を持った決断を下すことが出来るのだ。



情報セキュリティにおいては、従業員は企業にとって最重要資産であるとともに、最大の脅威でもある。

著者：Alan Brill, Jonathan Fairtlough, Kenya Mann Faulkner, and John Friedlander

大規模な情報セキュリティ障害のシナリオは予想できるようになってきた。従業員や信頼していたベンダーがシステムのコンフィギュレーションやデザインを間違えたり、正しいセキュリティ手続に従っておらず、ハッカーなどがそういったミスに便乗する。そして、マスコミや当局、訴訟当事者が、企業やCEOに堂々と被害の弁償をさせることになる。

このような繰り返される企業の悪夢に応じて、企業側も、回避可能なエラーはできるだけ管理できるように力をつけてきた。クロールが行った実態調査では、全体の76%の企業がサイバーセキュリティに関するポリシーや手順書を備えており、すでに74%（昨年76%）の企業が従業員研修や内部告発プログラムを実施している。ITセキュリティ部署では、ユーザーへの信頼を持たないということが当たり前な考え方となってきている。ITマネージャー達は、従業員をいわば"敵"とみなしており、"犯罪を犯しているのはコンピューターじゃない、人だ!"と一同に警戒している。それでも、データ漏洩の件数は止まらない。

持続的な事業発展のためには、セキュリティを業務の一環とすべきである。

データ漏洩が相次ぐと言うことは、セキュリティ関連の教育や方針、規則といったものが機能していないのだろうか。そういうわけではない。ただ、これらは、独立して実施されたのでは充分ではないということなのだ。これらの恩恵に十分に授かる為には情報セキュリティを従業員の業務フローの一部にしてしまうことがポイントである。

クロールが有効だと考える手段は、重要なデータが関わる手続には総合的なリスク評価（ORR）を定めることである。まずは従業員の言動に注目したセキュリティの見直しから始めると良いだろう。これは監査とは別物である。確かに、クロールの実態調査への回答者のうち80%はすでにセキュリティ監査を行っている。しかし監査というものは、既存の管理を一時点でに見直しているだけなのである。

このアプローチは、まず何を守らなければならないかを理解するところから始まる。何に守る価値があるのか？誰がどこからこの情報にアクセスする必要があるのか？何故現行の手続にはリスクがあるのか？リスクの発生確率はどのくらいで、リスクが実際に発生した場合のビジネスへの影響は？これらのリスクを軽減するためにかかるコストは？

あるシナリオを考えてみるとする。ABC社は外注の営業販社の売り上げを頼りにしている。そこの営業マン達は顧客データにアクセスする必要がある。各営業マンは毎日会社支給のパソコンを使ってEメール、カレンダー、書類作成、SNSなどを利用している。そのパソコンは、そのうちに古いデータで一杯になり、更新も満足にされず、バックアップもきちんと取られておらず、また、仕事だけでなく、頻繁に個人使用もされている。そしてそのパソコンが、紛失や盗難、またはハッキングされると情報漏洩が起こってしまう。

別のシナリオも考えてみよう。各営業マンが会社費用でデータにアクセスができるタブレットを持っているとする。顧客データや伝票はクラウドのドキュメント管理システムに保存されており、タブレット本体には保存されていない。そのタブレットには、不要なインターネット閲覧を禁ずるモバイルの端末管理ソフトウェアが入っている。もし紛失した場合でも、そのデバイスは暗号化されており、遠隔操作で情報の消去ができるようになっている。ローカルの保存場所もなく、保存したまま忘れ去られたバンパイアデータや不必要なデータ蓄積もない。誤って何かをクリックして知らずにウィルスに感染してしまうこともない。これが業務フローの一部となっている今、セキュリティは強化されていると言えるだろう。

セキュリティに関する明確な規則を策定し、トレーニングし、一貫してその規則を施行し、従わない者にはそれなりの措置をとることが大事である。

セキュリティリスクの管理を業務フローの一部にすることはスタートとしては良い。セキュリティの規則は明確でなければならない。そしてすべての従業員に守ってもらわなければならない。全員がトレーニングを受講し、規則に沿って練習をしておかなければならない。従わない者にはそれなりの措置をとるべきである。

会社は、全体のセキュリティ態勢の中においての情報リスクにも注目しておかなければならない。物理的な管理ポリシーを持っておくことも不可欠である。結局のところ、データというのはデスクトップからでもクラウドのストレージデバイスからでも同じように簡単に盗まれてしまうのだ。犯罪者はソーシャル・エンジニアリングによって従業員にミスを犯させる方が簡単であることを知っている。犯罪者たちは人間の善意に付け入るのだ。鍵の落とし物の例えを考えてみて欲しい。ある従業員が、会社の敷地内で鍵の落とし物を発見する。それには名札は付いていないがUSBメモリースティックがついている。その社員は親切心からそのUSBメモリを自分のパソコンにつなげ、鍵の持ち主の情報が何かないか見てみる。それにより、その社員は、自分のパソコンにうっかりと会社自体を破滅させかねないようなマルウェアをインストールしてしまったことになる。

こういったことに対する予防は簡単である。 ー 従業員をトレーニングし、そのトレーニングの成果を試してみるのである。有効なセキュリティトレーニングというのは、ただ講義するだけではなく、その結果を試してみることである。偽装のなりすましメールを出してみて、誰が反応するか見てみることだ。外部の人間にピザ配達を装わせて、社内に侵入させてみることだ。

経営陣も同じ規則に従うべきである。社員証をきちんとつけていなかったり、個人のパソコンなどを社内で使用していたり、あらゆるところへアクセス権限を持っている上層部の人間にこそ、セキュリティ規則が意味をなしていない。

そしてまた、経営陣は従業員が規則に従わせるようサポートすべきである。例えば、CFOが経理担当に即時の電子送金を依頼し、その社員が規則違反なので断るとする。もしその社員が罰せられたとしたら、その他の社員は今後規則に従うことを恐れてしまう。

従業員を規則に従わせるためのツールを与えよ。

単純なツールがあることだけでも大きな効果を期待できる。 昼休みや退社前に機密情報を保管しておける鍵付きの引出しはあるか。飛行機内でパソコンの画面を盗み見されないような覗き見防止シートはあるか。何か不審に思った際に従業員がすぐに電話をかけることのできる専用の回線があるか。社内のセキュリティ対策は支持されているだろうか？

従業員がどのような業務を行っているかを把握し、その知識を使って正しい規則やツールやコンプライアンス構造を構築することで、従業員自体を（サイバー面でも物理面でも）セキュリティ対策の一部にすることができる。それを実行することで従業員は会社にとってセキュリティの最重要資産となりえるのである。

ALAN BRILL
クロール サイバーセキュリティ調査部門
シニア・マネジング・ディレクター
abrill@kroll.com

JONATHAN FAIRTLOUGH
クロール サイバーセキュリティ調査部門
マネジング・ディレクター
jfairtlough@kroll.com

KENYA MANN FAULKNER
クロール 調査・訴訟支援部門
マネジング・ディレクター
kenya.faulkner@kroll.com

JOHN FRIEDLANDER
クロール サイバーリスク
マネジメント部門
シニア・ディレクター
jfriedlander@kroll.com

サプライチェーンに潜む脅威

著者：Kevin Braine, Julian Grijns, Tad Kageyama, and Cem Ozturk

自然災害や市民暴動は、サプライチェーンを脅かす最も破壊的でコストのかかるリスクとして看做されているが、これら環境法や人権法に対する侵害は、予測できない地政学リスクよりも、遥かに起こる可能性が高く、より多くの損害を企業に与える可能性が高いと言える。

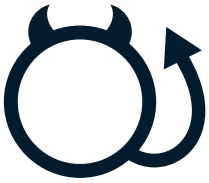
サプライチェーンの潜在リスクが高まっていることは、Krollによる「2017/18 Global Fraud & Risk Report」でも示しているように、グローバル企業にとって、近年益々大きな関心事となっている。

サプライチェーンと調達機能は、通常、グローバル企業の主要プロセスとして既に組み込まれているため、不正や風評被害の温床となり易い。

弊社が実施した調査でも、30%以上の企業が不正の実行犯はベンダーやサプライヤーであったと回答している。

この数字は、昨年の調査より4パーセント上昇している。

本稿では、クロールが過去のプロジェクトで目の当たりにした、最も一般的なサプライチェーンリスクについて幾つか紹介したうえで、事前にリスクを特定し軽減するための、組織としての術を紹介したい。



非倫理的なビジネス慣行

昨年、調査メディアは、国際的なブランド企業のサプライチェーンにおける強制労働、児童労働、土地の権利に関わる問題、劣悪な労働環境について、数多くの現状を公開した。

このことは、時として、長期化する内部調査や企業ブランドの致命的な毀損をもたらした。

例えば、化粧品や自動車メーカーにマイカ（絶縁材料）を供給している化学品メーカーは、インドの違法な鉱山から（マイカの原料となる）児童労働を使って鉱石を採掘している業者を使っているとして、メディアに取り上げられた。

世界を代表する自動車メーカーの半数にあたる6社が、十分に対策を講じていないとして、圧力団体から非難を受けた。

別のケースでは、オーストラリアを代表するメディアが、インドネシア西パプア州において歴史的に環境破壊を続けている韓国の供給業者を使っているとして、数多くのNGOから非難の的とされた。

汚職と贈収賄

汚職や贈収賄は、新興国や後進国のみならず、先進国においても蔓延している。

最近では、FCPAの捜査対象となったクライアントに対して、33カ国に及ぶ政府関係者やエージェントへの支払記録や帳簿をフォレンジック会計によって分析するなどの支援を行った。それに加え、実地（リビア、アンゴラ、ブラジル、ロシア）において、広範囲に及ぶ書類や会計処理について分析を実施した。

組織犯罪や制裁企業との取引

サプライチェーン上の関係やビジネスは、組織犯罪に巻き込まれたり、制裁リストに掲載のある企業や個人との取引につながるリスクを秘めている。

例えば、最近のクロールによる調査で、世界的に使用されている商用船舶の数多くが政治家によって支配され、所有されていることが分かった。また他の商用船舶では、国営企業によって支配されているケースもあり、このことは、制裁リストの掲載企業と取引をしてしまうリスクを潜在的に秘めている。

最近の事例を紹介しよう。日本のコングロマリット企業のシンガポール地域本社で働く内部告発者が、インドのベンダーと従業員の1人が共謀して、存在しない修理のため発注をでっち上げていると、経営陣に通報した。

この不正は、企業に甚大な経済的損失をもたらし、その後、東南アジアやその他地域においても、同様の事態があることが発見された。また、このことは、場合によっては組織犯罪に巻き込まれる可能性をも含んでいる。

製品汚染

ちょっとした契約違反が、企業収益やブランドを損なうといった大きな問題を引き起こすことがある。例えば、アジアのアパレル会社の工場が、欠陥製品や過剰製品を破棄しない場合を考えてみたい。

工場の所有者、マネージャー、従業員が、これらの製品を世界中の販売チャネルを使って、認可のない市場に販売した場合、結果的にブランドオーナーの利益やレピュテーションを毀損することになる。

別のケースでは、供給者がサプライチェーンに不正に馬肉を投入し、牛肉製品に混入させていたことを、英国とヨーロッパの小売業者が発見した。その結果、彼らは大規模なリコールと、緊急かつコストの掛かる再調査を余儀なくされた。

営業秘密と知財漏洩

ベンダーによって使用されている物理的、ITシステム、アプリケーション、および全体的な情報セキュリティを適切に評価できないブランドの所有者は、製品やプロセス技術、およびその他の営業秘密を失うリスクに直面している。

事実、協力会社が将来の競争相手になる可能性がある。高度に設計された特許登録済のラバーブッシュが、ラベルのない同じ製品として製造されるケースなどがそうである。

複雑性と無関心がサプライチェーンリスクを増大させる

これらのインシデントは非常に複雑に見え、各社にとって検知が困難なため、今日の新たなグローバルリスクの課題として、なかなか認識されていない。

事実、この複雑性は、サプライチェーンリスクの新たな傾向のため、日常の業務とサプライヤーとの距離がいかに離れていようとも、グローバルビジネスにおいては、サプライヤーが誰で、どのような活動をしているのかについて、正確に把握する必要がある。

しかしながら、このような環境を取り巻くリスクやチャレンジが存在するにも拘わらず、回答者の4分の1以上が、パートナー、顧客、ベンダーに対するデューデリジェンス等、不正に対する防止策を施していないと答えている。

多くの場合、新興市場、とくに南アジアや東南アジアにおいては、サードパーティであるサプライヤーが正当な理由で関与している。

これらの地域におけるサプライチェーンは極めて不透明といえる。

法律の脆弱性、信頼性の低い企業情報、物議を醸している企業とグローバルサプライヤー間を取り持つ代理会社の日常的な使用、そしておびただしい第三国の下請業者が、比較的リスクの低い国々、例えば、香港、UAE、シンガポールなどにも存在しており、このことがサプライチェーンの不透明感を増大させている。

更に言えば、長期的なベンダーや委託メーカーは、彼らが抱えているリスクを自ら得意先へ明らかにする。そのため、経営陣は、彼らを信じ込み、関係を注意深く監視することに無頓着となる。

一方、ほとんどの企業のサプライチェーン登録プロセスや監査は、これらの問題を検知するには不十分である。特に国をまたがったサプライチェーンや複数の新興国市場で事業を行っている企業においては、それが顕著である。

教訓を先を見越したリスク軽減策に活かす

最近の事案から学んだ教訓は、非倫理的または不正を働くサードパーティを発見することに関して、多くの企業が同じ脆弱性を共有している、という事実である。

彼らは、より効果的なコンプライアンスプログラムを構築するためのロードマップを既に策定している。

- リスクベースのコンプライアンスプログラムを確立すること。汎用的なコンプライアンスプログラムでは、時間を浪費するだけで、重大なリスクを見落とす危険性がある
- ベンダーの誠実性について、自社から完全に独立した検証を行うこと。自社評価への過度な依存は、ベンダーの誠実性について何ら保証していない。所詮、サードパーティがあなたのサプライヤー行動規範に署名したところで、彼らは本当にそれを遵守するだろうか？
- サプライヤーとの関係を継続的に監視する。時間の経過とともに、サードパーティのリスクやコンプライアンスは大きく変わる可能性があるため、継続的なチェックが求められる。
- 監査権限を強化し、厳しい質問を投げかける。このことは、サプライヤーとの関係が悪化した時に、特に重要である
- コンプライアンス・プロセスを一元化する。多くの大企業は、プロセスが一元化されていないため、サードパーティを適切に識別するのに苦労している。
- このことは、重大な事態を招く恐れがあるサプライチェーンの潜在的な不正を検出し、監視するための、一貫したアプローチに繋がる。
- 例えば、私たちは、問題が発見されたサードパーティとの関係を、そのまま維持してしまう事業部門と、関係を断ち切る事業部門との双方を頻繁に見てきた。

組織が一度サプライヤーのことをしっかりと把握したら、不正リスクや風評リスクから身を守ることは、それほど難しいことではない。

法令違反の調査をプロアクティブに実施するためには、良識やリスク・ベースト・アプローチをもって、リスクの高いサプライヤーに対する適切なレベルのデューデリジェンスや分かり易い報告プロセスを確実に導入していかなければならない。

KEVIN BRAINE
クロール コンプライアンス部門
欧州・中東・アフリカ地域代表
マネジング・ディレクター
kevin.braine@kroll.com

JULIAN GRIJNS
クロール北米 調査・訴訟支援部門
マネジング・ディレクター
jgrijns@kroll.com

TAD KAGEYAMA
クロールアジア太平洋地域 調査・訴訟支援部門
アジア・オペレーション　代表
リージョナル・マネジング・ディレクター
tkageyama@kroll.com

CEM OZTURK
クロール太平洋地域 調査・訴訟支援部門
マネジング・ディレクター
cozturk@kroll.com

トレーニング、テクノロジー、幹部の姿勢：ヘルスケア業界におけるステミングデータ損失の救済策

著者：Devon Ackerman and Brian Lapidus

今年のGlobal Fraud & Risk Reportでは、ヘルスケア業界が世界的に厳しいリスクに直面していることを浮き彫りにした。ヘルスケア業界の実態調査で判明したことは、過去12か月間の間に一度でもサイバー関連のインシデントを経験した企業が、その他の一般業界と比べて少なくとも15%高い割合で、個人情報、保護医療情報、従業員情報、知的財産の損失を報告しているということである。

ヘルスケア企業が、患者、消費者、従業員から個人情報を定期的に収集、保管していることは周知の事実だ。この個人情報には、社会保障番号（SSN）や生年月日、クレジットカード番号、医療保険、運転免許証番号などが含まれる。そしてこれらのデータには、患者の医療診断情報や病歴など、さらに機微な情報が含まれていることもあり、サイバー犯罪者達にとっては大変価値の高いデータなのである。

ヘルスケア業界の性質上、適切な治療を提供する為のデータ共有は必須であるが、そのことがリスクを高めている。医療提供者、管理者、スタッフ皆がデータにアクセスし、編集し、大量のデータを送受信しなくてはならない。そしてそれは、不本意なデータ流出や、内部関係者による悪意のあるデータの窃盗など、大きな被害の可能性を広げている。それに加え、近年米国保健社会福祉省へは、外部のハッカーによる被害の報告数が増加している。

このような環境では、セキュリティに注いだせっかくの努力が台無しかのように思えてしまう。以下は、過去にクロールが携わった代表的なケーススタディで、何が起こり、どのように対応したについての例を挙げている。

例えば、**不本意なデータ流出**の例として次のようなケースが挙げられる。ある社員が仕事の締め切りが間に合わなそうだったので、社外からも仕事ができるようにと、10,000人の患者のカルテを暗号化されていないUSBドライブにダウンロードした。そして不幸にもそのUSBドライブを紛失してしまった。クロールは、（外部デバイスが社内ネットワークに接続できないようにポートを無効にするなど）インフラに対するより厳しい管理と、（会社の手順に従って正しく、安全にデータを管理できるよう）従業員教育を行うことを推奨した。

クロールは、ある悪意のある内部関係者の調査も行ったことがある。その人物は、自分が解雇の対象になっているらしいという情報を耳にし、いざという時の"保険"として何百ギガバイトにも及ぶ患者カルテ、従業員情報、ドナー情報、経理情報を社内ネットワークから外付けハードドライブにダウンロードしておいた。その後、その社員が解雇となった際に何かをすることをほのめかすような発言をしたので、担当者は何が起こっているのか疑問に思い始めた。フォレンジック解析の依頼を受けたクロールは、即座に調査を進め、その翌週には何のデータが、どのタイミングで、どのくらいの容量分取られたのかを突き止めた。その企業はそのデータ窃盗に絡むそれ以上の被害を食い止めることができた。

ソーシャル・エンジニアリング / フィッシング詐欺の例としては、ある企業の人事部が納税時期にフィッシング詐欺の標的となったケースが挙げられる。そのメールは社内の幹部からのもので、社員の報酬情報が載ったフォームを送るように依頼されたものだった。担当者は、上層部からの、このまるで本物かのような指示に従い、さらにはその後の送金手配まで完了してしまった。その結果、従業員データの損失だけでなく、何千ドルもの損害も被ることになった。このような脅威を低減するための積極的な対応策として、従業員教育を必須事項とした。また、最近出回っている詐欺行為などに関するアラートを頻繁に従

業員達に知らせるようにもなった。たとえそれが幹部からの指示であってでも、個人情報流出や送金に関する手順はさらに厳しく守るよう徹底することとした。

クロールはまた、ある企業の**ランサムウェア**に対する対応と復旧の支援をしたことがある。その企業はある日自社のデータにアクセスができなくなり、「データは暗号化された。暗号解除用のキー取得のためにはビットコインにて賠償金を払え。」というメッセージだけしか見えない様になってしまった。この対策として、企業はデータ復旧のためには分離されたシステムに保存されているバックアップに頼らざるをえなくなるし、その為には頻繁なバックアップスケジュールが必要になる。また、ランサムウェアはたいてい詐欺攻撃によって広まる為、従業員教育も欠かせない。ランサムウェア攻撃は多くの場合既存の脆弱性を利用してくるため、セキュリティパッチも不可欠だ。多くの企業はランサムウェア被害がデータ漏洩と同じことであるという認識がない。しかしランサムウェア被害では、何にアクセスされ、何が見られ、どのデータが密かに抽出されたのかを把握するのは難しく、必要な事前準備ができていないと大きなデータ漏洩の脅威にさらされてしまう。

経営陣が、情報セキュリティが重要であるというトップダウンの姿勢を示すことは従業員に大きな影響を与える。　特に、最近クロールが対応したある病院システムの顧客の場合はそれが明白であった。その企業の個人情報保護管理責任者は大変な敬意をもって、同社の"神聖なる患者データを保護する義務"について話をした。この責任者は、データの機密性とセキュリティが最終的にいかに良好な顧客対応につながるかを強調し、患者データの機密性の問題に関する従業員の意識を大幅に引き上げ、データセキュリティを彼らの日々の業務に組み込ませることに成功した。

最初から患者をケアするのと同じレベルでデータを繊細に取り扱っているヘルスケア企業は、特異データの監視をしっかり行っており、業界が直面しているような脅威を低減することができる。

DEVON ACKERMAN
クロール サイバーセキュリティ調査部門
アソシエイト・マネジング・ディレクター
devon.ackerman@kroll.com

BRIAN LAPIDUS
クロール ID窃盗・ブリーチ通告部門
プラクティス・リーダー
マネジング・ディレクター
blapidus@kroll.com

アジアによる対米投資-投資機会における規制リスクと商業リスクの高まり

著者：Violet Ho, Nicole Lamb-Hale, and Naoko Murasaki

2017年は、米国ーアジア間の貿易・投資にとって、特別の年となった。アジアの企業にとって、米国市場は最も魅力的な投資先だが、一方、稀に見る不確実性に直面した年でもあった。

米国の新大統領による政権発足以来、2017年の環太平洋パートナーシップ協定（TPP）からの米国離脱に見られるように、（オバマ政権時に掲げた）アジアへのいわゆる「ピボット」の逆転がはじまった。米国のTPPからの離脱は、TPP交渉において米国による市場参入を認めた日本を含む数多くのアジア諸国にとって、貿易のあり方を抜本から見直すよう迫っている。両国間の貿易収支の不均衡を改善するための交渉が、改めてまた始まろうとしている。韓国-米国間（"Korus"）の貿易協定も、貿易収支の不均衡を理由に、抜本的な見直しを迫られている。また、グローバル・サプライチェーンによってコストを管理してきたアジアの多国籍企業にとっても、輸入制限や関税の引き上げは、対米投資の魅力を損なわせかねない不確実要素となり得る。

米国による貿易政策の混乱は、同時に、米国の規制にも不確実性をもたらす。このことは、米国の対米外国投資委員会（"CFIUS"）のような、国家安全保障を守るための"ツール"が積極的に活用されることを意味する。CIFIUSは、外国企業による米国企業の買収において、国家安全保障面からレビューを実施する米国連邦、省庁を跨った委員会である。これらの動向が、米国投資を検討しているアジア企業に対して、規制リスクや商業リスクを生じさせている。なかでも、CFIUSの管轄を広める法案が提出されたことは、CFIUSによるリスクをより一層高める要因となっている。CFIUSによる管轄拡大は、最近国会に提出されたCFIUSの年次報告書を見れば、アジアの投資家にとって特に厄介な問題であることが分かる。[1] この年次報告書によれば、現法案の限られたCFIUSの管轄においてさえ、中国企業と日本企業による買収はCFIUSによってレビューされた全ての取引のなかで上位4位を占めている。

特に中国について言えば、2017年8月に中国政府によって出された海外投資ガイドラインが、外国企業による投資を禁止していることが、このことを更に悪化させている。中国政府は（米国でのM&Aなど）国外への資本流出をコントロールする新しい法案を発効した。このことは、キャッシュを国内に溜め込んでいる中国企業にとっては最大の関心事である。

とは言え、投資が米国の雇用に繋がるならば、アジアの投資家にとっても、大きな機会をもたらす。投資家は、対米投資における規制リスクと商業リスクに対して、どのように立ち向かうべきであろうか。その対策として、例えば、以下のステップを踏むことが考えられる。

[1] http://bit.ly/UnclassifiedCFIUSAnnualReport-2015

1. 取引が国家安全保障上の問題に抵触するかどうかについて専門家の意見を求める

米国内でのビジネスに繋がる取引については、CFIUSへ申請する前に、当該取引が国家安全保障上の問題に抵触するか否かを評価する。CFIUSの承認は、情報技術や防衛関連産業に対して難しいと考えられているが、国家安全保障上の懸念は、実はその他の業界にも及ぶ可能性がある。よって、CFIUSへ出願する前に、専門家の助言を求めるなど、周到な準備が必要である。潜在的な国家安全保障上の懸念は、決して無視されるべきではない。
リスクを低減するための戦略を専門家とよく話し合い、ビジネスへの影響を最小限に食い止める必要がある。

2. 雇用維持と創出という米国の目標に合わせた投資を考える

米国政府は、中国、日本、韓国などアジア諸国との貿易収支不均衡について懸念を示す一方、対米投資が同国の雇用維持や新しい雇用創出に繋がるならば、商業リスクは最小化される可能性が高い。考え方の一つとして、貴社の投資が米国の雇用目標に資するものであると説得できるものであることが肝要である。

3. 投資による地域への影響・地域特性を調査する

対米投資に伴う影響は、連邦レベルだけではなく州、地方、市民社会レベルにも及ぶ。投資先の州や地方の産業への影響を理解したうえで、その影響を最小化するための方策を、よく専門家と検討しながら、市民やコミュニティリーダーと連携してうまく進める必要がある。

4. 他社の経験から学ぶ

デューデリジェンスの一環として、米国の同じ地域に既に投資している外国企業や同業他社の経験を参考にすることは有効である。同じ立場にある企業をケーススタディすることは、余分な費用を省いたり、投資を成功に導くうえで、大変に役立つ。

VIOLET HO
クロール　北京・上海オフィス代表
グレーター・チャイナ代表
シニア・マネジング・ディレクター
vho@kroll.com

NICOLE LAMB-HALE
クロール北米 調査・訴訟支援部門
マネジング・ディレクター
nicole.lamb-hale@kroll.com

NAOKO MURASAKI
クロールアジア太平洋地域 調査・訴訟支援部門
東京オフィス代表
マネジング・ディレクター
nmurasaki@kroll.com

サイバーセキュリティへの経営陣による取り組み

著者：Andrew Beckett, Paul Jackson, and Jason Smolanoff

ANDREW BECKETT
クロール サイバーセキュリティ調査部門
マネジング・ディレクター /
欧州・中東・アフリカ地域リーダー
andrew.beckett@kroll.com

PAUL JACKSON
クロール サイバーセキュリティ調査部門
マネジング・ディレクター / アジア太平洋
地域リーダー
paul.jackson@kroll.com

JASON SMOLANOFF
クロール サイバーセキュリティ調査部門
グローバル・プラクティス・リーダー
シニア・マネジング・ディレクター
jason.smolanoff@kroll.com

サイバーセキュリティは、経営陣にとってはどちらかといえば積極的に関与し続けたり、重要な方針を打ち出しにくいテーマである。その理由は、情報システム（とその周辺のセキュリティの仕組み）がそもそも非常に複雑で難解であること、また理解を超える代物だと見なされてしまっているからである。しかしクロールの前回のGlobal Fraud Reportで指摘されているように、システム上の問題というよりはむしろ人的要素が、サイバー犯罪や情報漏洩問題を引き起こしていることにもっと注目されるべきだろう。この点こそ、企業の役員その他の幹部がもっと積極的に取り組めるし、取り組むべきテーマなのだ。

確かにこのことは組織も認識するようになってきたと言え、クロールGlobal Fraud Reportの最新号でのアンケート調査結果では、回答者の22%がサイバーリスク問題を低減するために取締役会の関与を拡大させる予定とし、また半数近く（40%）が次の12ヶ月の間に取締役会の関与を深めるための新しい試みを行うとしている。

トップのリーダーシップは非常に重要だ。実際のところセキュリティ対応の最前線に立たされる社員は最も弱い立場にいることが多い。経営陣による直接的な関与と模範を示すことは、全社員のマインドセットに大きな影響を与える。データ喪失事案をみると、純粋な技術的な直接的攻撃によるものというよりも、既存の業務プロセスに起因していることが多い。巧妙なサイバー攻撃者が突いてくるセキュリティ上のギャップを見つけ出すためには、技術的な知識とともに優れたビジネス感覚や社員のスキルが必要なのだ。

では、どうすれば取締役会がもっと効果的にサイバーセキュリティリスクに取り組むことが出来るのだろうか？サイバーセキュリティに関するポリシーや手続の包括的な見直しを行っていく中で、取締役会が直接的に関与していくためいくつかのステップを踏むことは、取締役がこの問題を重視していることを示すためには有効だ。

1. 既存のサイバーセキュリティポリシーや手続は理解できているか？

もしNoなら、これらを簡潔で分かりやすいものに書き換える必要がある。ルールは全員がただちに理解でき、運用出来るものであって初めて機能するのだ

2. サイバーセキュリティ体制構築に必要な答えを知っているか。答えを得るための正しい疑問を投げかけているか？

もしITやサイバーセキュリティ対策を担うリーダーが、取締役会レベルで理解可能な情報セキュリティ戦略を適切にあるいは十分に示せていない場合、この件において適切な人物が会を代表しているのかを問う必要がある。取締役会は、株主その他ステークホルダーのためにも、自社の重要な情報資産を守る能力について担当者よりしっかり確認しておく必要がある。

3. ポリシーや手続を策定する際、全ての事業部責任者に関与させているか？

サイバーセキュリティが他の事業から孤立して作られているようなものではいけない。この問題は全社的に取り組むべき問題であり、全ての取締役の意見を考慮すべきで、特に各事業部の業務プロセスにサイバー不正や業務が停滞するようなギャップがある場合はなおさらである。

4. インシデント対応計画は実際にテストさせているか？

どんなに明確で出来栄えのよいポリシーや手続でも、一度も現実的シナリオをもとにテストされていないというのなら、せっかくの計画が現実に即して機能するかどうかは分からない。企業トップを巻き込んだサイバー危機の机上訓練が最も効果的に、現実に起こり得る深刻なギャップを浮き彫りにし、修正することが出来る。どのようなテストであってもITやセキュリティ担当、担当役員だけでなく、法務、IR、人事、外部専門家、社外弁護士、広報の危機対応部門など有事の際に必要とされるステークホルダーを巻き込む必要がある。

5. サイバーセキュリティ対策の費用対効果をどのように測っているか？

取締役会では、サイバーセキュリティ対策の予算や採用の承認権限を持っていることが多いが、予算が有効に使われているかどうかをどのような尺度で測っているだろうか。例えば社内担当部署には知らせず、抜き打ちで外部専門家が現実のハッカーが使う手口でテストを行う、ということを検討してみてはどうだろうか。このような現実の中で試してみることでしか、実際の効果は測れない。テストの他にも、独立した外部専門家にサイバーセキュリティロジェクト、組織、予算を検証してもらうということはどうだろう。クロールのような専門家は、現在起こりえる、業界や　地域のサイバーリスクを熟知しており、顧客のセキュリティ対策の効果を検証したり、同業他社の対応と比較してアドバイスすることが可能である。

6. 模範を示せているか？

サイバーセキュリティ対策が強化されれば、ITツールへのアクセスや使用に様々な制約が課せられることになる。 正しく説明していれば、それが会社全体のセキュリティを守るために有益なことだと分かるはずだ。取締役会や幹部がこれらの対策を受け入れ、対策をきちんと実行に移していれば（利便性のために例外扱いを求めるので　なく）、セキュリティ対策は企業トップから発信されているものであり全員が守るべきものとして浸透していくだろう。サイバーセキュリティに関するトレーニングを自分自身の問題として積極的に支持する個人的なメッセージを発信することことも、会社全体の意識と責任感を高めるうえで有効であろう。

7. 専門家の起用を検討したことはあるか？

最後に、信頼できるセキュリティ専門家より、定期的に取締役会でブリーフィングを受けることは必須である。多くの取締役はこれら専門家を非常勤取締役として招聘している。取締役は情報喪失によって、オペレーション上および法的なコストのみならず株主やブランドも大きく毀損することを理解している。人的な側面を意識し、法的な技術的側面では専門家の助けを得るなど、企業の他のリスクと同様にサイバーリスクに対処することで、経営陣が、様々な規制上またはステークホルダーからの要請に応えて情報資産を守っていくための主導的な役割を担うことが出来るのである。

世界リスクマップ

このマップは過去1年以内に不正、サイバー、およびセキュリティインシデントを経験した企業の各国もしくは地域別に表示されています。

1 カナダ

92% 不正
92% サイバー
79% セキュリティ

3 メキシコ

85% 不正
92% サイバー
60% セキュリティ

5 ブラジル

84% 不正
89% サイバー
63% セキュリティ

2 米国

91% 不正
87% サイバー
73% セキュリティ

4 コロンビア*

61% 不正
72% サイバー
55% セキュリティ

6 英国

97% 不正
94% サイバー
71% セキュリティ

* サンプル少数により、指標データのみ。

7 イタリア

90% 不正
92% サイバー
56% セキュリティ

9 中東

66% 不正
71% サイバー
64% セキュリティ

11 ロシア

89% 不正
80% サイバー
77% セキュリティ

8 サブサハラアフリカ

77% 不正
85% サイバー
72% セキュリティ

10 インド

89% 不正
84% サイバー
74% セキュリティ

12 中国

86% 不正
88% サイバー
75% セキュリティ

カナダ

過去12ヶ月間に不正の被害に遭った割合
- ▲ **4%** 対前年比
- ▲ **8%** 対世界平均

不正

不正事案の被害者数は2016年に88%だったのに対し、今年のリポートでは92%にまで上がり、世界平均の84%を大幅に上回った。この国で最も多くみられた不正の種類は、昨年34%だったのに対し41%にまで上昇した物的資産・在庫品の盗難で、今年の世界平均より14%も高い。すぐ後を追っているのが情報漏洩で、世界平均より9%高い38%の回答者が経験している。

被害を経験した者からは、顧客が一番の加害者になりやすいという報告が上がっている。大体10人中4人(39%)が、フリーランス/短期契約従業員(33%)、及び、ジュニアポジション従業員と元従業員(28%の被害者が両方のカテゴリーに当てはまると答えた)よりも、顧客に責任があると答えた。

著しく高いレベルでの不正が報告されているにも関わらず、カナダの被害者たちは自分たちが特に脆弱だと感じていない。被害者は3つのリスク領域に比較的不安定な感情で報告をすることが多い－情報漏洩、経営陣による利益相反と、社内の財務不正でそれぞれ59%であるが、これらは世界平均の57%、52%、52%とさほど変わらない。

今年の調査で最も多かった不正行為対策は財務統制(83%のうち不正検出をも含む)、管理統制(78%)、そして従業員教育の実施と内部告発ホットライン(75%)もよく取られた戦略であった。

なお、被害経験者のうち、世界平均の47%を上回る半数以上(53%)の者が内部告発によって発覚したと答えている。

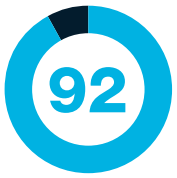
最も多く見られた不正の種類		世界平均
物的資産・在庫品の盗難	41%	27%
情報漏洩	38%	29%
社内の財務不正	31%	23%

主な加害者のタイプ		世界平均
顧客	39%	22%
フリーランス/短期契約従業員	33%	26%
ジュニアポジション従業員	28%	39%
元従業員	28%	34%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
情報漏洩	59%	57%
経営者による利益相反	59%	52%
社内の財務不正 (会計操作)	59%	52%

最も実施されている不正対策		世界平均
財務 (財務統制、不正検出、内部/外部監査、マネーロンダリング対策)	83%	77%
経営陣 (経営者管理、インセンティブ、監査委員会等の外部による監視)	78%	74%

不正発見の経路		世界平均
自社の内部通報	53%	47%



過去12ヶ月間にサイバーインシデントの被害に遭った割合

▲ **7%** 対前年比

▲ **6%** 対世界平均

サイバーセキュリティ

カナダの経営陣による事件増大に関する報告によると、2016年に85%、今年の世界平均では86%だったのに対し、被害者の大多数(92%)が過去12ヶ月にサイバーセキュリティ攻撃に遭ったと回答した。

大部分の他の国と同様、カナダで最も被害の多かった サイバーインシデントは電子メールによるフィッシング詐欺(41%)、ついで、データ漏洩(38%)となっている。頻繁にターゲットになりやすいのは顧客データであり、半数以上がそのように回答した。

カナダの被害者は、サイバーインシデントに対して特に脆弱であるとは感じてはいない。電子メールのフィッシング詐欺やサービス妨害攻撃、そしてウイルス/ワームによる攻撃については57%の回答者がかなり、もしくはある程度、脆弱であると答えている。

カナダの被害者のほぼ3分の1(31%)の回答者が、サイバーセキュリティ事件の責任は元従業員にあると答えた。しかしながら、半分以上(53%)の回答者が加害者は無差別サイバー犯罪者であると回答し、この地域における特に困難な課題であることが浮き彫りになっている。

最も多く見られたサイバーインシデントの種類		世界平均
電子メールによるフィッシング詐欺	41%	33%
データ漏洩 (例:顧客および従業員データの喪失、知的財産/機密情報/研究開発内容)	38%	27%
ウィルスやワームによる攻撃	33%	36%

主な加害者のタイプ		世界平均
無差別サイバー犯罪者	53%	34%
元従業員	31%	28%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
電子メール経由でのフィッシング詐欺	57%	57%
サービス妨害攻撃	57%	52%
ウィルス/ワームによる攻撃	57%	62%

最も多い標的		世界平均
顧客情報	50%	48%

サイバーインシデント発生時の連絡先		世界平均
ITサービス会社	33%	35%
インシデント対応会社(調査、漏洩通知)	14%	11%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▲ **1%** 対前年比

▲ **9%** 対世界平均

セキュリティ

前年の78%から今年の79%へと1%小さく増幅したのはセキュリティ侵害である。比較的緩やかな上昇ではあるが、カナダの被害者がセキュリティインシデントに関して世界水準(今年のレポート時は70%)よりも継続的に報告を行っているということを物語っている。最も多いのは物的/知的財産侵害(56%)で、このタイプの事件は59%の回答者に大きな脆弱さを感じさせるものとして注目されている。

カナダの回答者の45%にあげられる人数がセキュリティインシデントの責任は元従業員にあると報告している。

最も多く見られたセキュリティインシデントの種類		世界平均
物的/知的財産侵害	56%	41%
職場での暴力	26%	23%
環境リスク (ハリケーン、洪水、竜巻、地震といった自然災害による被害を含む)	26%	28%

主な加害者のタイプ		世界平均
元従業員	45%	37%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
物的/知的財産侵害	59%	63%
地政学上のリスク (例:紛争地域における操業など)	48%	53%

米国

過去12ヶ月間に不正の被害に遭った割合

▲ **11%** 対前年比

▲ **7%** 対世界平均

不正

今年は米国における経営陣の91%が不正一般の被害に遭ったと回答しており、不正の発生率が最も高い地域の一つであり、世界平均の84%と昨年の80%を大きく上回った。

米国回答者の半数以上(51%)という最も多くが被害に遭ったのが情報漏洩であり、世界平均の29%を大幅に上回った。最も多かった不正の原因は経営陣による利益相反(33%)とも報告され、物的資産・在庫品の盗難(33%)と同等の数字であった。

彼らの実体験を反映すると、正解平均の57%に対し、米国回答者の73%は情報漏洩について、かなり、もしくはある程度脆弱であると感じている。加えて、経営陣による利益相反は全ての国からの報告において特に脆弱だという結果を示している。

不正の脆弱性増加には何よりもテクノロジー上の問題が問われ、54%がITインフラの複雑さを指摘し、デジタルタッチポイントによる情報露出の増加(45%)と共に世界平均を大きく上回った。

内部監査は、インシデントを経験した半数以上(51%)の回答者が信用する、最も一般的な不正発見の手段である　。

半数近い回答者(48%)が、ジュニアポジション従業員が組織の不正の実行者であると答えており、昨年の36%からかなり上昇していることに大いに考慮すべきである。

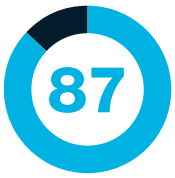
最も多く見られた不正の種類		世界平均
情報漏洩	51%	29%
物的資産・在庫品の盗難	33%	27%
経営陣による利益相反	33%	26%
知的財産の侵害 (機密情報など)・著作権侵害・偽造	31%	20%
社内の財務不正 (会計操作)	27%	23%

主な加害者のタイプ		世界平均
ジュニアポジション従業員	48%	39%
元従業員	41%	34%
中上級管理職	30%	27%
フリーランス/短期契約従業員	30%	26%
ベンダー/サプライヤー (例:技術やサービスのプロバイダー)	30%	30%
エージェント/仲介者 (例:会社の代理で活動する第三者)	30%	24%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
情報漏洩	73%	57%
経営陣による利益相反	70%	52%
社内の財務不正 (会計操作)	63%	52%
知的財産 (機密情報など) の盗難・著作権侵害・偽造	60%	56%
ベンダー・サプライヤー・調達部門の不正	60%	51%

最も実施されている不正対策		世界平均
財務 (財務管理、不正検出、内部/外部監査、マネーロンダリング対策)	84%	77%
資産 (物理的なセキュリティシステム、在庫管理、タグ付け、資産登録)	82%	77%
経営陣 (経営者管理、インセンティブ、監査委員会等の外部による監視)	79%	74%
情報 (ITセキュリティ、技術的な対策)	78%	78%
従業員 (雇用前調査)	78%	73%

不正発見の経路		世界平均
内部監査	51%	44%



過去12ヶ月間にサイバーインシデントの被害に遭った割合

▼ 1% 対前年比
▲ 1% 対世界平均

サイバーセキュリティ

米国の回答者がサイバーインシデントの被害に遭った割合は平均をやや上回った程度(平均86%に対して87%)で、電子メール経由でのフィッシング詐欺がもっとも多かった(39%)。続いて、ウィルス/ワームによる攻撃(37%)、データ漏洩(33%)となっている。

サイバーインシデントの標的として異常に割合が高かったのは従業員情報(平均41%に対し64%)、次いで顧客情報(45%)となっている。

米国では36%が元従業員の加害者によって被害に遭ったと報告しており、無差別のサイバー犯が後に続いている(31%)。

71%の米国の回答者はウイルス/ワームによる攻撃に関しての脆弱性を強く感じており、データ消去やランサムウェアがそれぞれ70%と、そのすぐ後に続いている。

サイバー被害者が最初に連絡するのはITサービスベンダーが一般的で、世界平均の35%に対し、48%がそうすると米国の回答者が答えている。

最も多く見られたサイバーインシデントの種類		世界平均
電子メール経由でのフィッシング詐欺	39%	33%
ウィルス/ワームによる攻撃	37%	36%
データ漏洩 (顧客/従業員データ、知的財産/機密情報/研究開発情報の喪失など)	33%	27%

主な加害者のタイプ		世界平均
元従業員	36%	28%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
ウィルス/ワームによる攻撃	71%	62%
データ消去	70%	58%
ランサムウェア攻撃	70%	55%

最も多い標的		世界平均
従業員情報	64%	41%
顧客情報	45%	48%

サイバーインシデント発生時の連絡先		世界平均
ITサービス会社	48%	35%
連邦法執行機関	12%	4%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▲ 15% 対前年比
▲ 3% 対世界平均

セキュリティ

米国の被害者は物理的なセキュリティ被害を報告する割合が最も高く(73%)、うち天災を含む環境に起因するインシデントもそれに含まれる(39%)。

物理的なセキュリティ被害に関しては、不正やサイバーインシデントなどと異なり加害者がわからないことが多い。米国での無差別加害者による被害の割合が37%であることに対し、競合他社による被害の割合は35%である。

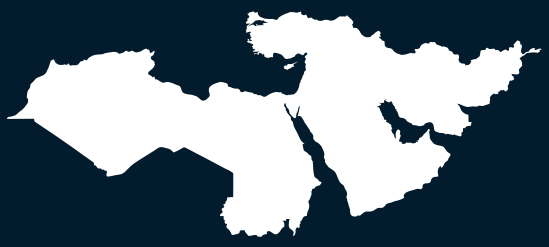
米国の回答者は、昨年よりも今年のセキュリティリスクに対して特に脆弱さを感じている。69%の回答者がかなり、もしくは比較的高い割合で、昨年よりも24ポイント高い環境リスクに対しての脆弱性を報告している。

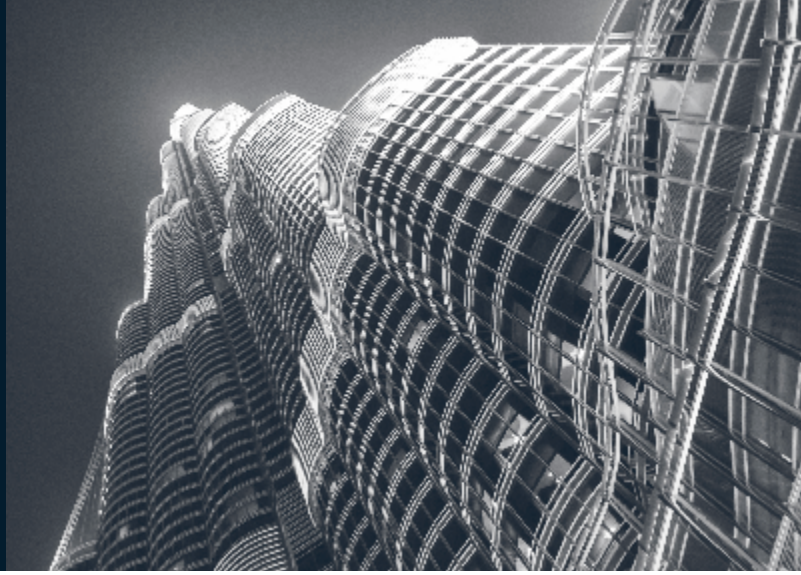
最も多く見られたセキュリティインシデントの種類		世界平均
環境リスク (ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む)	39%	28%
物的/知的財産侵害	37%	41%
地政学上のリスク (例:紛争地域における操業など)	34%	20%

主な加害者のタイプ		世界平均
無差別加害者	37%	30%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
環境リスク (ハリケーン、洪水、竜巻、地震といった自然災害による被害を含む)	69%	56%
地政学上のリスク (例:紛争地域における操業など)	67%	53%
物的/知的財産侵害	65%	63%

中東





過去12ヶ月間に不正の被害に遭った割合

- ▼ **22%** 対前年比
- ▼ **18%** 対世界平均

不正

中東で過去12ヶ月の間に不正事案を報告した回答者は昨年の88%から66%にまで減少した。

最も多い不正事案は規制・コンプライアンス違反で、回答者の24%が挙げており、経営陣の利益相反（22%）、物的資産・在庫品の盗難（19%）となっている。

中東における不正加害者としてジュニアポジション従業員があげられる割合が高く、昨年の34%だったのに対し、62%であった。加害者のカテゴリーで次に高いのは当局で、正解平均15%の2倍以上である。

中東の回答者によると、不正は経営陣により発覚することが多い。半数以上（54%）が経営陣により不正が摘発されたとし、昨年の38%が外部による監査、36%が内部監査によるものであった。一部の回答者からは通報者による摘発も報告されており、2016年度では1位（50%）であったが今年の報告では4位（31%）まで転落した。

中東の経営幹部は特に、企業資産の横領と同様に汚職・贈収賄に脆弱性を感じており、どちらも61%で世界平均の50%と48%であるそれぞれをはるかに上回っている。

最も多く見られた不正の種類		世界平均
規制・コンプライアンス違反	24%	20%
経営陣による利益相反	22%	26%
物的資産・在庫品の盗難	19%	27%

主な加害者のタイプ		世界平均
ジュニアポジション従業員	62%	39%
監督官庁	36%	15%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
汚職・贈収賄	61%	50%
企業資産の横領	61%	48%
情報漏洩	58%	57%
知的財産（機密情報など）の盗難・著作権侵害・偽造	58%	56%
社内の財務不正（会計操作）	58%	52%
ベンダー・サプライヤー・調達部門の不正	58%	51%

最も実施されている不正対策		世界平均
財務（財務管理、不正検出、内部/外部監査、マネーロンダリング対策）	69%	77%
資産（物理的なセキュリティシステム、在庫管理、タグ付け、資産登録）	69%	77%
情報（ITセキュリティ、技術的な対策）	69%	78%

不正発見の手段		世界平均
自社の幹部	54%	35%

過去12ヶ月間にサイバーインシデントの被害に遭った割合

▼ 19% 対前年比
▼ 15% 対世界平均

サイバーセキュリティ

中東の回答者のうち、サイバーインシデントの被害に遭ったという回答の割合は2016年度の90%から今年は71%にまで下がった。

中東の経営幹部は、競合他社がサイバーインシデントの加害者になりうると指摘しており(33%)、次いでエージェント/仲介者(31%)、そして無差別のサイバー犯罪者(29%)となっている。サイバーインシデントで最も標的になりやすいのは顧客情報と企業/従業員個人情報がそれぞれ45%と挙げられている。昨年最も多く標的にされたのが物的資産/現金(47%)で、今年は5位であった。

この地域の回答者は、ウイルス/ワームによる攻撃(80%)、データ消去(76%)、そして不正送金(65%)にかなり、もしくは比較的高い脆弱性を感じており、全てが世界平均を上回っている。

最も多く見られたサイバーインシデントの種類		世界平均
機密情報が保存された機器の紛失	31%	19%
データ消去	27%	25%
電子メール経由でのフィッシング詐欺	25%	33%

主な加害者のタイプ		世界平均
競合他社	33%	23%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
ウィルス/ワームによる攻撃	80%	62%
データ消去	76%	58%
送金不正 (電子メールアカウントの乗っ取り/詐称)	65%	50%

最も多い標的		世界平均
顧客情報	45%	48%
企業・従業員のID	45%	35%
機密情報・研究開発情報・知的財産	43%	40%

サイバーインシデント発生時の連絡先		世界平均
ITサービス会社	33%	35%
インシデント対応会社	17%	11%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▼ 18% 対前年比
▼ 6% 対世界平均

セキュリティ

昨年の82%に比較すると、今年は中東の3分の2の回答者(64%)が過去12ヶ月間にセキュリティインシデント被害に遭ったと回答している。

セキュリティインシデントは元従業員によるものが多いと中東の回答者の39%が回答している。物的/知的財産侵害は最も一般的なセキュリティインシデント(34%)だが、ほぼ同等(32%)が自然災害による被害を含む環境リスクだも報告している。

中東の経営陣は、物的/知的財産侵害(一般的な世界平均の63%と大体同等である61%)に高い 、もしくは比較的高い脆弱性を感じており、その次に環境リスク(56%)を挙げている。

最も多く見られたセキュリティインシデントの種類		世界平均
物的/知的財産侵害	34%	41%
環境リスク (ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む)	32%	28%

主な加害者のタイプ		世界平均
元従業員	39%	37%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
物的/知的財産侵害	61%	63%
環境リスク (ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む)	56%	56%

イタリア

過去12ヶ月間に不正の被害に遭った割合

▲ **13%** 対前年比
▲ **6%** 対世界平均

不正

イタリアの回答者が報告した不正発生率は90%で、これは世界平均の84%よりも6%ポイント高く、また昨年の77%よりも大幅な増加となった。

3つの最も一般的な不正のタイプは、知的財産侵害（28%）、物的資産・在庫品の盗難（26%）、そして情報漏洩（26%）であった。規制・コンプライアンス違反は今年の不正事案報告トップ3から外れた。

被害に遭ったというイタリアの回答者のうち3分の1を少し上回る回答者（34%）が、元従業員が不正事案の主犯と挙げており、ついで中上級管理職（31%）、そしてフリーランス/短期契約従業員（26%）を挙げた。昨年の報告では現行のジュニアポジション従業員（50%）が不正の主犯だと報告されていたが、今年はその可能性がかなり低い数値となった（20%）。

イタリアの回答者の多く（62%）は、知的財産侵害に対して高い、もしくは比較的高い脆弱性を感じており、世界平均の56%よりも6%上回った。情報漏洩も大きな懸念事項であり、この脅威に対しても54%が高い、もしくは比較的高い脆弱性を感じている。

不正発見の手段については内部通報者（46%）は依然として最も一般的であったたが、昨年の数値（53%）よりは大分減少し、今年の世界平均の47%をわずかに下回っている。

最も多く見られた不正の種類		世界平均
知的財産の盗難（機密情報など）、著作権侵害、偽造	28%	20%
物的資産・在庫品の盗難	26%	27%
情報漏洩	26%	29%

主な加害者のタイプ		世界平均
元従業員	34%	34%
中上級管理職	31%	27%
フリーランス/短期契約従業員	26%	26%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
知的財産の盗難（機密情報など）、著作権侵害、偽造	62%	56%
情報漏洩	54%	57%

最も実施されている不正対策		世界平均
リスク（リスク担当者、リスク管理部門の設置）	83%	75%
資産（物理的なセキュリティシステム、在庫管理、タグ付け、資産登録）	75%	77%
情報（ITセキュリティ、技術的な対策）	74%	78%
取締役会の関与	74%	68%
従業員（トレーニング、内部通報ホットライン）	69%	74%

不正発見の手段		世界平均
自社の内部通報者	46%	47%

過去12ヶ月間にサイバーインシデントの被害に遭った割合

▲ **13%** 対前年比
▲ **6%** 対世界平均

サイバーセキュリティ

イタリアの回答者の大多数(92%)は、過去12ヶ月間にサイバー・インシデントを経験した。これは昨年の79%からの大幅な増加であり、また、今年の世界平均の86%を上回っている。

電子メールによるフィッシング攻撃は最も一般的なサイバーインシデントとして報告されており、イタリアの回答者の49%が回答している。これは驚くべき結果で、世界平均よりも16%高く、また昨年の21%の2倍以上の数値を記録している。

サイバーインシデントの主犯については、昨年の結果と同様に、元従業員が多く挙げられており(28%)、世界平均(28%)と同等であった。

イタリアは他の地域の回答者と比較するとサイバーインシデントに特に脆弱だと感じている経営陣が多い。ランサムウェア攻撃とウイルス/ワームによる攻撃(それぞれ64%)に高い、もしくは比較的高い脆弱性を感じており、データの不正操作とデータ消去(それぞれ62%)がすぐ後に続いている。

サイバーインシデントとして最も狙われやすいものは顧客情報(39%)で、企業/従業員のID(36%)が続いている。

最も多く見られたサイバーインシデントの種類		世界平均
電子メール経由でのフィッシング詐欺	49%	33%
ウイルス/ワームによる攻撃	44%	36%

主な加害者のタイプ		世界平均
元従業員	28%	28%

過去12ヶ月間にサイバーインシデントの被害に遭った割合		世界平均
ランサムウェア攻撃	64%	55%
ウイルス/ワームによる攻撃	64%	62%
データの不正操作	62%	56%
データ消去	62%	58%
データ漏洩 (顧客/従業員のデータ、知的財産、機密情報、研究開発情報の喪失など)	61%	55%

最も多い標的		世界平均
顧客情報	39%	48%
企業/従業員のID	36%	35%

サイバーインシデント発生時の連絡先		世界平均
ISP/通信プロバイダー	17%	7%
IT サービス会社	14%	35%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▼ **12%** 対前年比
▼ **14%** 対世界平均

セキュリティ

イタリアのセキュリティインシデント報告は前年度より減少し、今年の報告では68%から56%に下がり、世界平均の70%を下回った。

報告された3つの最も一般的なセキュリティインシデントは、物的/知的財産侵害(33%)、紛争地域における操業などの地政学上のリスク(21%)、そして自然災害を含む環境リスク(同じく21%)だ。

イタリアの回答者の67%がテロ脅威に高い、もしくは比較的高い脆弱性を感じており、世界平均の49%を18%上回った。次いで物的/知的財産侵害で、65%とそれに近い数値である。

最も多く見られたセキュリティインシデントの種類		世界平均
物的/知的財産侵害	33%	41%
地政学上のリスク (例:紛争地域における操業など)	21%	20%
環境リスク (ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む)	21%	28%

主な加害者のタイプ		世界平均
無差別犯罪者	36%	30%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
国内外でのテロ	67%	49%
物的/知的財産の侵害	65%	63%

「今年の調査によるとイタリアの大部分の回答者はサイバーインシデントの被害に遭っており、企業が情報セキュリティにおいて直面している課題が大きくなっていることを示しています。経営陣は政府の努力と新しい汚職対策規制があるにもかかわらず、特に贈収賄と汚職に脆弱性を感じています。内部通報者の保護を改善し、従業員に不正の疑惑があれば早期に報告するよう促すことが進むべき第一歩となり、それにより、こういった増大する複雑な問題に対処するにあたって、企業が有利な立場を保つことが出来るようになります。」

- Marianna Vintiadis
クロール　調査・訴訟支援部門
南欧州地域代表
マネジング・ディレクター

ロシア

過去12ヶ月間に不正の被害に遭った割合

- ▲ **7%** 対前年比
- ▲ **5%** 対世界平均

不正

ロシアの回答者の89%が、過去12ヶ月間に組織が不正を発見したと報告しており、この数値は前年（82%）に比べ7%増加し、世界平均の84%より5%上回っている。

ロシアの回答者が被害に遭った不正の種類トップ3は社内の財務不正（34%の回答者）、経営陣による利益相反（26%）、そして物的資産の盗難と情報漏洩（いずれも23%）である。

被害に遭ったロシアの回答者のうち39%が、ベンダー/サプライヤーが最も一般的な不正の加害者であると回答している。これは世界平均の30%より明らかに高い（＋9%）数値である。次に挙げられたのは中上級管理職（32%）と元従業員（29%）であった。他の地域と比較するとジュニアポジション従業員が主犯となる割合は、世界平均の39%よりは少ない16%の回答者が答えている。

ロシアの経営陣は、マーケットでの談合・癒着に高い、もしくは比較的高い脆弱性を感じており、世界平均よりも10%高い60%となっている。回答者は現代奴隷/人身売買（平均の40%に対して51%）にも高い、もしくは比較的高い脆弱性を感じている。

最も多く見られた不正の種類		世界平均
社内の財務不正 (会計操作)	34%	23%
経営陣による利益相反	26%	26%
情報漏洩	23%	29%
物的資産・在庫品の盗難	23%	27%

主な加害者のタイプ		世界平均
ベンダー/サプライヤー (例：技術やサービスのプロバイダー)	39%	30%
中上級管理職	32%	27%
元従業員	29%	34%
エージェント / 仲介者 (例：会社の代理で活動する第三者)	26%	24%
顧客	26%	22%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
マーケットでの談合・癒着 (価格協定など)	60%	50%
物的資産の盗難	51%	55%
現代奴隷/人身売買	51%	40%

最も実施されている不正対策		世界平均
情報 (ITセキュリティ、技術的な対策)	94%	78%
資産 (物理的なセキュリティシステム、在庫管理、タグ付け、資産登録)	87%	77%
従業員 (トレーニング、内部通報ホットライン)	87%	74%
パートナー・顧客・ベンダー (デューデリジェンス)	87%	73%

不正発見の手段経路		世界平均
自社の内部通報者	74%	47%

過去12ヶ月間にサイバーインシデントの被害に遭った割合

▼ **2%** 対前年比
▼ **6%** 対世界平均

サイバーセキュリティ

サイバーインシデントの被害を報告しているロシアの回答者は、前年度の82%よりわずかに下がり80%となった。この最新の数値は、世界正解平均の86%と比べて6%下回っている。

機密情報が保存された機器の盗難は、ロシアで最も多く普及が報告されているサイバーインシデントの1つであり、電子メール経由でのフィッシング詐欺と同程度の数値になっていると、回答者の3分の1ををちょうど超えた数(34%)が強調した。

ロシアの回答者は他の国よりも機密情報が保存された機器の盗難の報告が多い傾向にあり、英国だけが32%というそれに近い32%という数値であったを出している。なお、世界平均は21%である。

顧客情報は、ロシアでは他国よりもサイバー犯罪の標的になりやすい傾向がみられる。半数以上(57%)の回答者が顧客情報がサイバーインシデントの標的にされたと報告しており、世界平均の48%よりも高い数値となっている。

ロシアのサイバーインシデントでもう1つ大きな脆弱性と認識されているものがある。電子メール経由でのフィッシング詐欺(71%)について、高い、もしくは比較的高い脆弱性を感じており、ウイルス/ワームによる攻撃(69%)、そしてデータ漏洩(60%)となっている。

最も多く見られたサイバーインシデントの種類		世界平均
機密情報が保存された機器の盗難	34%	21%
電子メール経由でのフィッシング詐欺	34%	33%
主な加害者のタイプ		世界平均
無差別のサイバー犯罪者	39%	34%
過去12ヶ月間にサイバーインシデントの被害に遭った割合		世界平均
電子メール経由でのフィッシング詐欺	71%	57%
ウイルスやワームによる攻撃	69%	62%
データ漏洩 (例:顧客/従業員のデータ、知的財産、機密情報、研究開発情報の喪失など)	60%	55%
最も多い標的		世界平均
顧客情報	57%	48%
物的資産・/現金	46%	34%
サイバーインシデント発生時の連絡先		世界平均
IT サービス会社	29%	35%
監督官庁	21%	6%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▲ **18%** 対前年比
▲ **7%** 対世界平均

セキュリティ

今年の調査で、セキュリティサイバーインシデントを報告したロシアの回答者はのうち、劇的に増加し(18%)した数値があり、77%がセキュリティ問題に影響を受けたと77%が回答した。これは世界平均(70%)よりも7%高い数値である。

被害を受けたというにあった回答者によると、元従業員(41%)がセキュリティインシデントの主な加害者主犯であったと回答しており、次いで無差別の犯罪者、中上級管理職、そしてジュニアポジション従業員となっている。

ロシアの経営陣は環境リスクについて、高い、もしくは比較的高い脆弱性を感じており、世界平均より7%高い63%の回答者がそのようにこれを指摘し挙げた。職場での暴力(54%)もまた、大きな懸念事項である。

最も多く見られたセキュリティインシデント		世界平均
環境リスク (ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む)	37%	28%
物的/知的財産侵害	31%	41%
職場での暴力	26%	23%
主な加害者のタイプ		世界平均
元従業員	41%	37%
セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
環境リスク (ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む)	63%	56%
職場での暴力	54%	50%

サブサハラアフリカ

過去12ヶ月間に不正の被害に遭った割合

- ▼ **12%** 対前年比
- ▼ **7%** 対世界平均

不正

サブサハラアフリカは基本的に不正の発生が多い地域であるが、今年の77%は前年の調査よりも12%下がり、世界平均の84%を7%下回った。

それにもかかわらず、この地域は依然として経営陣の利益相反(34%)、マネーロンダリング(26%)、そして規制・コンプライアンス違反(25%)が最も高い発生を示している。

サードパーティは一般的にリスク要因に挙げられ、合弁パートナーと顧客が折半でインシデントの加害者なっている(それぞれ34%)。元従業員も34%の回答者が加害者として挙げている。しかしこの地域で最も一般的な加害者はジュニアポジション従業員(44%)であった。

脆弱性の感じ方は世界平均と大体同じであり、世界平均の57%と比較すると、53%の回答者が高い、もしくは比較的高い脆弱性を感じているのが情報漏洩である。物的資産の盗難(49%)も脆弱性が高いものとして挙げられ、経営陣の利益相反、ベンダー・サプライヤー・調達部門不正、そして企業資産の横領、それぞれが47%の回答者によって指摘された。

自身の会社が「全く脆弱性がない」と信じている回答者はほかの地域に比べて幅広い不正について多くみられ、現代奴隷(49%)、社内の財務不正(38%)、企業資産の横領(32%)、マーケットでの談合・癒着(32%)、汚職・贈収賄(28%)、そしてベンダー・サプライヤー・調達部門不正(23%)という不正についてそのような回答がみられた。

最も多く見られた不正		世界平均
経営陣による利益相反	34%	26%
物的資産・在庫品の盗難	28%	27%
マネーロンダリング	26%	16%
規制・コンプライアンス違反	25%	20%
ベンダー・サプライヤー・調達部門の不正	23%	20%

主な加害者のタイプ		世界平均
ジュニアポジション従業員	44%	39%
元従業員	34%	34%
合弁パートナー (例:製造・その他ビジネス機能担当、フランチャイズ)	34%	23%
顧客	34%	22%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
情報漏洩	53%	57%
物的資産・在庫品の盗難	49%	55%
経営陣による利益相反	47%	52%
ベンダー・サプライヤー・調達部門の不正	47%	51%
企業資産の横領	47%	48%

最も実施されている不正対策		世界平均
知的財産 (知的財産リスク評価、著作権モニタリングプログラム)	85%	73%
財務 (財務管理、不正検査、内部/外部監査、マネーロンダリング対策)	80%	77%
パートナー・顧客・ベンダー(デューデリジェンス)	80%	73%

不正発見の手段		世界平均
自社の内部通報者	56%	47%
内部監査	51%	44%

過去12ヶ月間にサイバーインシデントの被害に遭った割合

▼ **6%** 対前年比
▼ **1%** 対世界平均

サイバーセキュリティ

この地域の回答者の85%が今年の調査でサイバーセキュリティに遭ったことを報告しており、世界平均（86%）とほぼ同じ数値である。

最も多かったサイバーインシデントはウイルス/ワームによる攻撃で、ほぼ半数（47%）の回答者が挙げており、世界平均の36%を11%も上回っている。データの不正操作もこの地域では一般的で、世界平均22%に対し30%という結果であった。これは脆弱性の感じ方が反映されており、59%の経営陣がこの種のサイバーインシデントにかなり、もしくは比較的高い脆弱性を抱いている。データ漏洩（59%）と電子メール経由でのフィッシング詐欺（58%）も大きな懸念事項である。

サブサハラアフリカで報告されたサイバーインシデントの3分の1（33%）が無差別サイバー犯罪者によるものであった。報告された全てのサイバーインシデントの半分が、顧客情報を標的にしたものであり（51%）、44%が従業員情報を標的とされたという回答であった。

最も多く見られたサイバーインシデントの種類		世界平均
ウイルス/ワームによる攻撃	47%	36%
データの不正操作	30%	22%

主な加害者のタイプ		世界平均
無差別サイバー犯罪者	33%	34%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
データの不正操作	59%	56%
データ漏洩（顧客/従業員データ、知的財産/機密情報/研究開発情報の喪失など）	59%	55%
電子メール経由でのフィッシング詐欺	58%	57%

最も多い標的		世界平均
顧客情報	51%	48%
従業員情報	44%	41%

サイバーインシデント発生時の連絡先		世界平均
サービス会社	40%	35%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▼ **2%** 対前年比
▲ **2%** 対世界平均

セキュリティ

この地域の回答者のうち、セキュリティインシデント被害に遭った回答者の割合は昨年の74%に比べるとわずかに72%に下がっただけで、世界平均の70%をわずか2%上回った。

報告されたセキュリティインシデントの種類トップ3を挙げると、物的/知的財産侵害（45%）、環境リスク（34%）、そして職場での暴力（26%）であり、全てが世界平均の、それぞれ41%、28%、23%を上回っている。

セキュリティインシデントの最も一般的な加害者は元従業員で、世界平均の37%に対しこの地域は39%であった。

物的/知的財産侵害は最も多く報告されているセキュリティインシデントであるだけでなく、この地域では高い、もしくは比較的高い脆弱性を有していると考えられている（68%）。約半数（51%）の回答者は地政学上のリスクについても、高い、もしくは比較的高い脆弱性を感じている。

最も多く見られたセキュリティインシデント		世界平均
物的/知的財産侵害	45%	41%
環境リスク（ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む）	34%	28%

主な加害者のタイプ		世界平均
元従業員	39%	37%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合		世界平均
物的/知的財産侵害	68%	63%
地政学上のリスク（例：紛争地域における操業など）	51%	53%

英国

過去12ヶ月間に不正の被害に遭った割合

▲ **7%** 対前年比
▲ **13%** 対世界平均

不正

英国の回答者は今年の調査で97%という最も高い不正発生率を報告し、昨年の数値の90%から7%上昇し、今年の世界平均(84%)からも13%も高い結果であった。

マネーロンダリングはどの国よりも英国回答者が最も多く挙げた。3分の1以上(35%)がマネーロンダリングが関わる不正被害に遭ったと回答しており、それは世界平均の16%を2倍以上上回るものである。

同じ割合の英国の回答者(35%)は、物的資産・在庫品の盗難の被害に遭った報告をしており、世界平均(27%)より8%高い。次に英国回答者に最も多い不正は情報漏洩(32%)で、それも同じく世界平均(29%)より高い。

英国回答者によると、元従業員が不正の加害者になる確率が最も高い。約半数(45%)がフリーランス/短期契約従業員(36%)とジュニアポジション従業員(33%)と比較しても元従業員によるものが最も多いと回答している。

英国の回答者は、知的財産の盗難・著作権侵害・偽造、経営陣による利益相反、規制・コンプライアンス違反、そしてマーケットでの談合・癒着に、高い、もしくは比較的高い脆弱性を抱いている。それぞれの脅威は68%の回答者に指摘された。

英国回答者の企業で最も多く実行された不正対策は従業員に向けたものであった。従業員に対する雇用前調査(88%)と従業員トレーニング/内部通報ホットライン(81%)は最も上位で、共に世界平均を上回っている(それぞれ73%と74%)。

不正は内部監査で発覚することが多く、世界平均(44%)よりも4%多い48%の英国回答者が答えている。

最も多く見られた不正		世界平均
マネーロンダリング対策	35%	16%
物的資産・在庫品の盗難	35%	27%
情報漏洩	32%	29%

主な加害者のタイプ		世界平均
元従業員	45%	34%
フリーランス/短期契約従業員	36%	26%
ジュニアポジション従業員	33%	39%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
知的財産(機密情報など)の盗難・著作権侵害・偽造	68%	56%
経営陣による利益相反	68%	52%
規制・コンプライアンス違反	68%	49%
マーケットでの談合・癒着(価格協定など)	68%	50%

最も実施されている不正対策		世界平均
従業員(雇用前調査)	88%	73%
従業員(トレーニング、内部通報ホットライン)	81%	74%
資産(物理的なセキュリティシステム、在庫管理、タグ付け、資産登録)	81%	77%
パートナー・顧客・ベンダー(デューデリジェンス)	79%	73%
情報(ITセキュリティ、技術的な対策)	78%	78%

不正発見の手段		世界平均
内部監査	48%	44%

過去12ヶ月間にサイバーインシデントの被害に遭った割合

▲ **2%** 対前年比
▲ **8%** 対世界平均

サイバーセキュリティ

英国回答者の大部分（94%）が昨年サイバーセキュリティインシデント被害に遭ったと回答しており、昨年の92%の数値よりわずかに上昇しているが、世界平均の86%を大幅に超えている。

最も多いサイバーセキュリティインシデントの種類はウイルス/ワームによる攻撃だと、英国回答者の41%が報告した。2番目に多いのは電子メール経由でのフィッシング攻撃で、38%が報告している。

英国回答者は、機密情報が保存された機器の盗難に対して高い、もしくは比較的高い脆弱性を感じている割合が68%であるが、実際の被害報告（32%）とは調和がとれていない。送金不正も大きな懸念事項であり、68%という数字は世界平均よりも18%高い。

英国回答者の3分の2以上（69%）がサイバーインシデントで従業員情報が標的にされたとし、世界平均の41%を28%上回るという記録的な数値を出している。

最も多く見られたサイバーインシデントの種類		世界平均
ウイルス/ワームによる攻撃	41%	36%
電子メール経由でのフィッシング詐欺	38%	33%
データ漏洩（顧客および従業員データ、知的財産/機密情報/研究開発情報の喪失など）	35%	27%
機密情報が保存された機器の盗難	32%	21%

主な加害者のタイプ		世界平均
フリーランス/短期契約従業員	31%	18%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
機密情報が保存された機器の盗難	68%	55%
送金不正（電子メールアカウントの乗っ取り/詐称）	68%	50%
ウィルス/ワームによる攻撃	65%	62%
機密情報が保存された機器の紛失	62%	53%

最も多い標的		世界平均
従業員情報	69%	41%
顧客情報	47%	48%

サイバーインシデント発生時の連絡先		世界平均
ITサービス会社	31%	35%
インシデント対応会社（調査、違反通知）	16%	11%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▼ **11%** 対前年比
▲ **1%** 対世界平均

セキュリティ

英国回答者からの今年のセキュリティインシデント報告は少なく、前年の82%と比較すると71%が経験したと答えている。

英国で最も一般的なセキュリティインシデントは他の地域と同様、物的/知的財産侵害（44%）、次いで地政学上のリスク（32%）となっている。その結果といえようが、これらのリスクに英国回答者が高い、もしくは比較的高い脆弱性を感じており、71%がテロに、70%が物的/知的財産侵害に心配を寄せている。

セキュリティインシデントでは元従業員が主な加害者のトップだと回答者の38%が挙げた。昨年は世界平均（37%）と同程度だった数値が10%も急増した。

最も多く見られたセキュリティインシデントの種類		世界平均
物的/知的財産侵害	44%	41%
地政学上のリスク（例：紛争地域における操業など）	32%	20%

主な加害者のタイプ		世界平均
元従業員	38%	37%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
国内外のテロ	71%	49%
物的/知的財産侵害	70%	63%
地政学上のリスク（例：紛争地域における操業など）	67%	53%

中国

過去12ヶ月間に不正の被害に遭った割合

= 前年と同等

▲ **2%** 対世界平均

不正

中国の回答者の86%が、過去12ヶ月間に不正を経験しており、それは世界平均の84%を2%上回っている数値になる。最も経験の多かった不正の種類は、ベンダー・サプライヤー・調達部門の不正と、汚職・贈収賄であり、いずれも29%で世界平均の20%と21%をそれぞれ上回っている。中国での回答者に次に多い最も経験されている不正の種類は経営陣の利益相反と情報漏洩で、ともに28%である。

ベンダー/サプライヤー(39%)と中上級管理職(25%)が最も多い不正加害者だと調査回答者が報告している。元従業員も不正事案には深く関わっており、中国の回答者地域の経営陣の21%に指摘摘発されている。

中国の回答者は知的財産の盗難・著作権侵害・偽造(48%)、マーケットでの談合・癒着(47%)、経営陣の利益相反と汚職・贈収賄(いずれも46%)に高い、もしくは比較的高い脆弱性を感じている。

不正防止対策についての質問に対しては、中国の回答者は財務管理(82%)、内部通報ホットライン(81%)、そして資産保護(80%)を、自身の企業で既に実行している対策トップ3として挙げた。

これら3つの対策全てがそれぞれ、世界平均の77%、74%、そして77%を上回っている。

最も多く見られた不正の種類		世界平均
ベンダー・サプライヤー・調達部門の不正	29%	20%
汚職・贈収賄	29%	21%
情報漏洩	28%	29%
経営陣による利益相反	28%	26%

主な加害者のタイプ		世界平均
ジュニアポジション従業員	50%	39%
ベンダー / サプライヤー	39%	30%
中上級管理職	25%	27%
エージェント / 仲介者 (例:会社の代理で活動する第三者)	23%	24%
元従業員	21%	34%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
知的財産の盗難 (機密情報など)、著作権侵害、偽造	48%	56%
マーケットでの談合・癒着 (価格協定など)	47%	50%
経営陣による利益相反	46%	52%
汚職・贈収賄	46%	50%

最も実施されている不正対策		世界平均
財務 (財務管理、不正検出、内部/外部監査、マネーロンダリング対策)	82%	77%
従業員 (トレーニング、内部通報ホットライン)	81%	74%
資産 (物理的なセキュリティシステム、在庫管理、タグ付け、資産登録)	80%	77%
情報 (ITセキュリティ、技術的な対策)	79%	78%

不正発見の手段		世界平均
内部監査	48%	44%

過去12ヶ月間にサイバーインシデントの被害に遭った割合

▲ **2%** 対前年比
▲ **2%** 対世界平均

サイバーセキュリティ

中国の回答者のうち、自身の会社が過去1年間にサイバーインシデントを経験した(88%)数値は、世界平均の86%よりわずかに高い。

サイバーインシデントの種類でデータ漏洩が最も一般的であり、世界平均が27%であるのに対し、中国の回答者の38%が報告している。それにもかかわらず、中国の回答者の15%しか自身の会社がデータ漏洩にかなり脆弱だと信じておらず、世界平均の21%を下回っている。

競合他社がサイバーインシデントの加害者であると32%が挙げており、世界平均の23%より特に高い。

中国の回答者も、電子メールによるフィッシング攻撃(55%)、データ漏洩(53%)、そして送金不正(52%)に対してかなり、もしくは比較的高い脆弱性を感じていると報告している。

機密情報、研究開発情報、そして知的財産はサイバー攻撃の主な標的であり、中国でのサイバー関連被害者の61%がそれらの資産を標的にされたと回答しているが、これは世界平均の40%を大きく上回り、全ての国々の中で最も高い数値であった。顧客情報が2番目に多い標的で、サイバーインシデント被害者の42%が挙げていた。

最も多く見られたサイバーインシデントの種類		世界平均
データ漏洩 (顧客/従業員データ、知的財産/機密情報/研究開発情報の喪失など)	38%	27%
ウイルス/ワームによる攻撃	31%	36%
データの不正操作	25%	22%
機密情報が保存された機器の紛失	25%	19%

主な加害者のタイプ		世界平均
競合他社	32%	23%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
電子メール経由でのフィッシング詐欺	55%	57%
データ漏洩 (顧客/従業員データ、知的財産/機密情報/研究開発情報の喪失など)	53%	55%
送金不正 (電子メールアカウントの乗っ取り/詐称)	52%	50%

最も多い標的		世界平均
機密情報/研究開発内容/知的財産	61%	40%

サイバーインシデント発生時の連絡先		世界平均
ITサービス会社	26%	35%
インシデント対応会社 (調査、違反通知)	18%	11%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

= 前年と同等
▲ **5%** 対世界平均

セキュリティ

中国の回答者の75%が過去1年間にセキュリティインシデントの影響を受けており、これは世界平均の70%より5%上回っている。

中国の回答者が経験したセキュリティインシデントで最も多かった2つの種類は物的/知的財産侵害(48%)、そして洪水や地震のような環境リスク(31%)である。しかしながら、どのセキュリティインシデントがかなり、もしくは比較的高い脆弱性を感じるか問いかけたところ、環境リスクが最も大きな懸念事項という回答であった(60%)。

セキュリティインシデントを経験した3人に1人(33%)が、元従業員が主犯であった事案を経験したと答えた。

最も多く見られたセキュリティインシデントの種類		世界平均
物的/知的財産侵害	48%	41%
環境リスク (ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む)	31%	28%

主な加害者のタイプ		Global Avg.
元従業員	33%	37%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		Global Avg.
環境リスク (ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む)	60%	56%

インド

過去12ヶ月間に不正の被害に遭った割合

▲ **21%** 対前年比

▲ **5%** 対世界平均

不正

インドにおいては昨年の報告よりも不正が大きく増加しており、前年の68%と今年の世界平均84%に対し、インド企業の89%が過去1年の間に不正を経験している。

物的資産・在庫品の盗難はインドが世界で最も高い割合を示しており、4割（40%）がこの種類の不正を経験したというのは、カナダ（41%）に次いで2番目に多い数字である。回答者によると、知的財産侵害（36%）とマーケットでの談合・癒着（36%）もインドの不正の中で高い割合を占めている。

インドでは、合弁パートナー（45%）が不正の主な加害者になることが多いと回答しており、次いでジュニアポジションの従業員（43%）、ベンダー・サプライヤー（40%）となっている。

実際の被害を体験して、インドの回答者は複数のリスクに高い、もしくは比較的高い脆弱性を感じている。実のところ、不正の脆弱性を測るこの調査において、ベンダー・サプライヤー・調達部門の不正を除いた全てのカテゴリーにおいて、インドは、世界的のトップ3ヵ国に入っている。世界平均の57%を30%も上回る9割に近い（87%）回答者が、情報漏洩を最も懸念している。社内の財務不正（85%）と知的財産の盗難・著作権侵害・偽造（80%）も世界平均の52%と56%を、それぞれ大幅に上回っている。

インドにおいては、他の国よりも多くの回答者が、合弁パートナー（45%）が不正増加の主な理由と挙げた。インドの企業はリスクにますます敏感になっており、回答者によると、財務管理（83%）や物理的なセキュリティシステム（83%）といった防止対策を施している。

最も多く見られた不正の種類		世界平均
物的資産・在庫品の盗難	40%	27%
知的財産（機密情報など）**の盗難・著作権侵害・偽造**	36%	20%
マーケットでの談合・癒着（価格協定など）	36%	19%

主な加害者のタイプ		世界平均
合弁パートナー（例：技術やサービスのプロバイダー）	45%	23%
ジュニアポジション従業員	43%	39%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
情報漏洩	87%	57%
社内の財務不正（会計操作）	85%	52%
知的財産の盗難（機密情報など）、**著作権侵害、偽造**	80%	56%
物的資産・在庫品の盗難	78%	55%
マネーロンダリング	76%	43%
マーケットでの談合・癒着（価格協定など）	73%	50%
汚職・贈収賄	71%	49%
ベンダー・サプライヤー・調達部門の不正	71%	51%

最も実施されている不正対策		世界平均
財務（財務管理、不正検出、内部/外部監査、マネーロンダリング対策）	83%	77%
資産（物理的なセキュリティシステム、在庫管理、タグ付け、資産登録）	83%	77%
リスク（リスク担当者、リスク管理部門の設置）	81%	75%
世評（メディア監視、コンプライアンス制御、法的評定）	80%	72%
知的財産（知的財産リスク評価、著作権モニタリングプログラム）	80%	73%

不正発見の手段		世界平均
自社の幹部	55%	35%
自社の内部通報者	55%	47%

過去12ヶ月間にサイバーインシデントの被害に遭った割合

▲ **11%** 対前年比
▼ **2%** 対世界平均

サイバーセキュリティ

インドの回答者の84%が昨年のうちにサイバー攻撃を経験しており、前年（73%）よりも11%高い結果である。これらの回答者の半数近くが電子メール経由のフィッシング攻撃（44%）を経験した。ウイルス/ワームによる攻撃は2番目に多い事案であった（36%）。

実体験を考慮すると、インドの回答者の80%が電子メール経由のフィッシング攻撃に高い、もしくは比較的高い脆弱性を感じていることになる。他の大きな懸念事項はデータ消去（78%）、データの不正操作（77%）、そしてウイルス/ワームによる攻撃（72%）であった。

インドのサイバー攻撃で最も標的にされているのは従業員情報（55%）、機密情報/知的財産（55%）、そして顧客情報（55%）であった。機密情報/知的財産と顧客情報は昨年よりも大きく上回っている。無差別サイバー犯罪者がサイバーインシデントの加害者として最も多く報告されている（45%）。

今年のインドの回答者は、サイバーインシデントにより、顧客のプライバシー・安全性・満足度、および企業評判（84%）と共に、従業員の安全性・プライバシー・士気に悪影響を受けた（84%）と報告している。

最も多く見られたサイバーインシデントの種類		世界平均
電子メール経由でのフィッシング詐欺	44%	33%
ウイルス/ワームによる攻撃	36%	36%

主な加害者のタイプ		世界平均
無差別サイバー犯罪者	45%	34%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
電子メール経由でのフィッシング詐欺	80%	57%
データ消去	78%	58%
データの不正操作	77%	56%
ウィルス/ワームによる攻撃	72%	62%
サービス妨害攻撃	71%	52%

最も多い標的		世界平均
顧客情報	55%	48%
従業員情報	55%	41%
機密情報/研究開発内容/知的財産	55%	40%

サイバーインシデント発生時の連絡先		世界平均
ITサービス会社	55%	35%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▲ **2%** 対前年比
▲ **4%** 対世界平均

セキュリティ

インドの4分の3（74%）の回答者が過去1年間にセキュリティインシデントを経験しているが、これは前年（72%）の数値より増え、世界平均70%よりも高い。

インドで最も多く発生しているセキュリティインシデントは物的/知的財産侵害（47%）で、職場での暴力（33%）が後に続いている。この現実は脆弱性が世界平均を大きく上回る結果に表れている：80%が物的/知的財産侵害（世界平均63%より17%高い）を高い、もしくは比較的高い脆弱性を感じており、　一方で78%が職場での暴力を心配している（世界平均50%より28%高い）。また、インドの回答者はテロに対する懸念が世界平均の49%に対して74%とさらに高かった。

インドの組織にとって従業員は大きなリスクであり、回答者の半数以上（52%）がセキュリティインシデントの主犯に中上級管理職を、回答者の3分の2（42%）が加害者に元従業員を挙げた。

大多数（91%）の回答者は、セキュリティインシデントが従業員のプライバシー・安全性・士気に悪影響を及ぼすと答えた。顧客のプライバシー・安全性・満足度も、75%の回答者から影響があったと報告された。

インドの回答者の半数以上（53%）が、セキュリティリスクの懸念から他の地域や国々での操業を断念していると報告している。主に挙げられたのは南アジア周辺国である　-　パキスタン、バングラデシュ、そしてスリランカ（22%）　-　日本はそのすぐ後に続いている（20%）。

最も多く見られたセキュリティインシデントの種類		世界平均
物的/知的財産侵害	47%	41%
職場での暴力	33%	23%

主な加害者のタイプ		世界平均
中上級管理職	52%	25%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
物的/知的財産侵害	80%	63%
職場での暴力	78%	50%
国内外のテロ	74%	49%

ブラジル

過去12ヶ月間に不正の被害に遭った割合

▲ **16%** 対前年比

= 世界平均と同等

不正

ブラジルは昨年不正が大幅に増加し、前年度が68%であったのに対し、回答者の84%が過去1年間の不正を報告した。ブラジルの回答者が経験した最も広範囲に渡った不正の種類は規制・コンプライアンス違反（29%）と社内の財務不正（29%）である。前年度ブラジルの不正の種類で最も多かったのは物的資産・在庫品の盗難であった。

ブラジルの組織では元従業員が深刻な不正リスクであると報告されている。実のところ、国内の半分以上の回答者（53%）が、元従業員が不正の主犯であると挙げており、すべての地域を通じて二番目に高い。回答者が挙げたもう1つの主犯グループは、中上級管理職（41%）である。

ブラジルの組織の不正は人々に大きな影響を与える – それが従業員のプライバシー・安全性・士気（81%）であっても、顧客の安全性・満足度・プライバシー（81%）であってもだ。アウトソースと海外への外注が増加することにより、ブラジルの半数の組織（50%）が、他のどの国よりも不正増加の主要因になりうると答えた。

ブラジルの回答者は、経営陣の利益相反（63%）、続いて財務不正（58%）、そしてベンダー・サプライヤー・調達部門の不正（58%）に高い、もしくは比較的高い脆弱性を感じている。

回答者によると、ブラジルの組織はリスクに敏感になっており、財務管理（84%）と物理的セキュリティシステムのような資産制御（82%）を含む、不正防止対策を実行している。

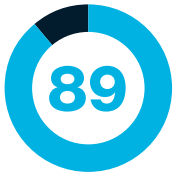
最も多く見られた不正の種類		世界平均
規制・コンプライアンス違反	29%	20%
社内の財務不正（会計操作）	29%	23%
情報漏洩	26%	29%
経営陣の利益相反	24%	26%
企業資産の横領	21%	20%

主な加害者のタイプ		世界平均
元従業員	53%	34%
中上級管理職	41%	27%
フリーランス/短期契約従業員	28%	26%
ベンダー / サプライヤー（例：技術やサービスのプロバイダー）	25%	30%
エージェント / 仲介者（例：会社の代理で活動する第三者）	19%	24%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
経営陣の利益相反	63%	52%
社内の財務不正（会計操作）	58%	52%
ベンダー・サプライヤー・調達部門の不正	58%	51%

最も実施されている不正対策		世界平均
財務（財務管理、不正検出、内部/外部監査、マネーロンダリング対策）	84%	77%
資産（物理的なセキュリティシステム、在庫管理、タグ付け、資産登録）	82%	77%
情報（ITセキュリティ、技術的な対策）	76%	78%
従業員（雇用前調査）	76%	73%
リスク（リスク担当者、リスク管理部門の設置）	76%	75%

不正発見の手段		世界平均
内部監査	66%	44%



過去12ヶ月間にサイバーインシデントの被害に遭った割合

▲ **13%** 対前年比
▲ **3%** 対世界平均

サイバーセキュリティ

ブラジルの回答者はここ1年でサイバーインシデントの増加を報告しており、前年の76%に比べると今年は89%が攻撃に遭ったという結果であった。半数近くの回答者がウイルス/ワームによる攻撃(45%)を経験している。

この経験が、回答者の63%がウイルス/ワームによる攻撃に高い、もしくは比較的高い脆弱性を感じている結果に置き換えられている。61%が同様に、電子メール経由でのフィッシング攻撃に対する懸念を高めている。

ブラジルのサイバーインシデントの標的は顧客情報(47%)で、機密情報や知的財産の研究開発情報も同様である。

元従業員が昨年のうちに起きたブラジルでのサイバーインシデントの主な加害者として挙げられており、次いで競合他社(21%)となっている。サイバー犯罪の影響は大きな損害をもたらす。ブラジルの回答者は、従業員の安全性・プライバシー・士気と共に、顧客のプライバシー・安全性・満足度(80%)にも悪影響を及ぼしたと報告している。

最も多く見られたサイバーインシデントの種類		世界平均
ウイルス/ワームによる攻撃	45%	36%
電子メール経由でのフィッシング詐欺	37%	33%

最も多い加害者のタイプ		世界平均
元従業員	32%	28%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
ウィルス/ワームによる攻撃	63%	62%
電子メール経由でのフィッシング詐欺	61%	57%
データの不正操作	55%	56%
データ漏洩 (顧客/従業員のデータ、知的財産、機密情報、研究開発情報の喪失など)	55%	55%
ランサムウェア攻撃	55%	55%
サービス妨害攻撃	55%	52%

最も多い標的		世界平均
顧客情報	47%	48%
機密情報・研究開発内容・知的財産	44%	40%

サイバーインシデント発生時の連絡先		世界平均
ITサービス会社	47%	35%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▲ **10%** 対前年比
▼ **7%** 対世界平均

セキュリティ

ブラジルの3分の2の回答者(63%)が昨年のうちにセキュリティインシデントに影響を受けたとし、世界平均の70%よりはまだ低い数値ではあるが、前年の回答者(53%)よりも10%の増加であった。最も多かったセキュリティインシデントの種類は、2位の職場での暴力(16%)よりもかなり高い物的/知的財産侵害だった(42%)。

これらの経験を反映して、ブラジルの回答者は物的/知的財産侵害(69%)に高い、もしくは比較的高い脆弱性を感じている。

前述の通り、元従業員がセキュリティインシデントの主な加害者であると報告したのは回答者の3分の2(42%)で、フリーランス/短期契約従業員がすぐ後に続いている(38%)。

潜在的なセキュリティインシデントの脅威に対応するため、回答者の大部分が、セキュリティポリシーと手順を策定し(92%)、セキュリティトレーニングを実施し(88%)、事業継続計画を実行し(88%)、そしてセキュリティ監査を実施した(88%)。

最も多く見られたセキュリティインシデントの種類		世界平均
物的/知的財産侵害	42%	41%
職場での暴力	16%	23%
地政学上のリスク (例:紛争地域における操業など)	13%	20%
環境リスク (ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む)	13%	28%

主な加害者のタイプ		世界平均
元従業員	42%	37%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
物的/知的財産侵害	69%	63%
環境リスク (ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む)	60%	56%
地政学上のリスク (例:紛争地域における操業など)	53%	53%

コロンビア

過去12ヶ月間に不正の被害に遭った割合*

不正

コロンビアの回答者のうち60%をわずかに上回った人数が、今年になって不正事案を経験したと報告した（61%）。回答者が経験した最も多い不正の種類は情報盗難（33%）であり、これはメキシコの回答者が報告した数値に近い（38%）。企業資産の横領が次に多く挙げられた事案で、回答者の22%が報告した。

世界的な回答者とは対照的に、世界平均の34%と比較すると、コロンビアの回答者は元従業員を不正の主な加害者と指摘している（55%）。

コロンビアでは67%の回答者が知的財産の盗難・著作権侵害・偽造に高い、もしくは比較的高い脆弱性を感じており、ラテンアメリカの中では最も大きい数値である。同様に、コロンビアの回答者はブラジル（42%）やメキシコ（33%）の回答者に比較して、規制・コンプライアンス違反（55%）に大きな懸念を持っている。

回答者が経験したうち、3分の2近い（64%）事案では、組織の内部通報によって不正事例が発覚した。回答者はまた、不正検出には内部監査が最も一般的な方法だと報告している。

コロンビアの回答者は他国よりも従業員のプライバシー・安全性・士気が不正によって強い影響を受けたと述べている（世界平均34%に対して55%）。コロンビアの回答者の半数以上が企業の不正に対する脆弱性の背後にある理由として高い離職率を挙げており（56%）、それが最も多い要因となっている。全世界では、34%の回答者が高い離職率を不正に対する脆弱性の要因と述べている。

最も多く見られた不正の種類		世界平均
情報漏洩	33%	29%
企業資産の横領	22%	20%
経営陣の利益相反	17%	26%

主な加害者のタイプ		世界平均
元従業員	55%	34%
ジュニアポジション従業員	36%	39%
フリーランス/短期契約従業員	36%	26%
顧客	27%	22%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
知的財産の盗難（機密情報など）、著作権侵害、偽造	67%	56%
規制・コンプライアンス違反	55%	49%
物的資産・在庫品の盗難	50%	55%
汚職・贈収賄	50%	50%

最も実施されている不正対策		世界平均
リスク（リスク担当者、リスク管理部門の設置）	91%	75%
取締役会の関与	81%	68%
経営管理（経営者による管理、インセンティブ、監査委員会等の外部による監視）	81%	74%

不正発見の手段		世界平均
自社の内部通報者	64%	47%

* サンプル少数により、指標データのみ。

過去12ヶ月間にサイバーインシデントの被害に遭った割合*

サイバーセキュリティ

コロンビアの72%の回答者が、自身の会社が過去1年間に経験したサイバーインシデントにおいて顧客情報を主に標的にした攻撃が多かったと述べた（46%）。

最も多く報告されたサイバーインシデントの種類はウイルス/ワームによる攻撃（回答者の44%）、次いでデータ消去（33%）であった。今年は、サイバーインシデントの加害者として元従業員と無差別サイバー犯罪者が同等の数値で挙げられている（31%）。ウイルス/ワームによる攻撃を経験した回答者が多かったにもかかわらず、データ消去（56%）、機密情報が保存された機器の盗難（56%）、そしてデータ消去と機密情報が保存された機器の紛失（それぞれ回答者の50%）のようなリスクに、高い、もしくは比較的高い脆弱性を感じている。

世界的には、サイバーインシデント被害への最も一般的な対応はITサービス会社に連絡することとなっている（35%）。しかしながら、コロンビアでは、これを選択したのはわずか15%であった。インシデント対応会社への連絡が最も多く選ばれた選択肢であった（23%）。

最も多く見られたサイバーインシデントの種類		世界平均
ウイルス/ワームによる攻撃	44%	36%
データ消去	33%	25%
主な加害者のタイプ		**世界平均**
元従業員	31%	28%
無差別サイバー犯罪者	31%	34%
サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		**世界平均**
データの不正操作	56%	56%
機密情報が保存された機器の盗難	56%	55%
データ消去	50%	58%
機密情報が保存された機器の紛失	50%	53%
最も多い標的		**世界平均**
顧客情報	46%	48%
機密情報/研究開発情報/知的財産	38%	40%
物的資産/現金	38%	34%
サイバーインシデント発生時の連絡先		**世界平均**
インシデント対応会社	23%	11%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合*

セキュリティ

コロンビアでは、半分をわずかに超えた数の回答者（55%）が、自身の組織が過去1年間にセキュリティインシデントを経験したと述べた。物的/知的財産侵害が最も多く経験されたセキュリティインシデントであり、回答者の39%が挙げている。この経験からか、回答者の56%がこの脅威に対して高い、もしくは比較的高い脆弱性を感じている。

サイバーセキュリティと同様に、コロンビアの回答者は無差別加害者と元従業員をセキュリティインシデントの加害者として挙げている（それぞれ40%）。なお、80%の回答者が、これらの事案は企業の収益と事業の継続性に影響を与えていると述べている。

コロンビアの回答者が自社の脅威及び脆弱性のアセスメントを実施している割合は平均よりも低く（世界平均の72%に対して50%）、同時に、そのようなアセスメントに基づいて何等かの計画を立てていないとする回答も平均以上であった（世界平均の9%に対して20%）。5分の1が、セキュリティ監査、セキュリティ基本計画、知的財産保護計画、幹部保護計画、脅威統制計画と手順、情報セキュリティ計画、もしくは事業継続計画を未実施、もしくは実施の予定もないと報告している。

最も多く見られたセキュリティインシデントの種類		世界平均
物的/知的財産侵害	39%	41%
主な加害者のタイプ		**世界平均**
元従業員	40%	37%
無差別加害者	40%	30%
セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		**世界平均**
物的/知的財産侵害	56%	63%
職場での暴力	50%	50%
国内外のテロ	50%	49%

メキシコ

過去12ヶ月間に不正の被害に遭った割合

▲ **3%** 対前年比

▲ **1%** 対世界平均

不正

自社が不正事案を経験したとするメキシコの回答者が、今年の報告では前年の82%よりわずかに増加した。

米国やカナダの回答者と並んで、メキシコでは情報漏洩(38%)が世界平均(29%)より高い。また、3分の1の回答者が汚職・贈収賄を挙げている。特に前年52%のメキシコの回答者に報告されたベンダー・サプライヤー・調達部門の不正は、今年の調査ではわずか17%であった。

メキシコの回答者は世界平均よりも高い、もしくは比較的高い脆弱性を物的資産・在庫品の盗難に感じている(世界平均の55%に対し、58%)。回答者の半数以上が汚職・贈収賄(54%)と知的財産の盗難・著作権侵害・偽造(51%)に大きな懸念を抱いている。

回答者は自身の組織がITセキュリティと技術対策を導入することで、増加する不正行為の潮流に対処していると述べている;従業員トレーニングや内部通報ホットライン、そして経営管理とインセンティブである。

不正事案を経験したメキシコの調査回答者の半分(49%)が、準従業員が主な加害者であり、元従業員とベンダー・サプライヤーが後に続くと示した。

最も多く見られた不正の種類		世界平均
情報漏洩	38%	29%
汚職・贈収賄	31%	21%
物的資産・在庫品の盗難	29%	27%
経営陣の利益相反	27%	26%
企業資産の横領	23%	20%

主な加害者のタイプ		世界平均
ジュニアポジション従業員	49%	39%
元従業員	37%	34%
ベンダー/サプライヤー (例:技術やサービスのプロバイダー)	34%	30%
フリーランス/短期契約従業員	24%	26%
エージェント / 仲介者 (例:会社の代理で活動する第三者)	24%	24%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
物的資産・在庫品の盗難	58%	55%
汚職・贈収賄	54%	50%
知的財産の盗難 (機密情報など)、著作権侵害、偽造	51%	56%

最も実施されている不正対策		世界平均
従業員 (トレーニング、内部通報ホットライン)	86%	74%
情報 (ITセキュリティ、技術的な対策)	83%	78%
経営陣 (経営者管理、インセンティブ、監査委員会等の外部による監視)	80%	74%
財務 (財務管理、不正検出、内部/外部監査、マネーロンダリング対策)	78%	77%
資産 (物理的なセキュリティシステム、在庫管理、タグ付け、資産登録)	73%	77%

不正発見の手段		世界平均
内部監査	54%	44%

過去12ヶ月間にサイバーインシデントの被害に遭った割合

▲ **10%** 対前年比
▲ **6%** 対世界平均

サイバーセキュリティ

メキシコでは、過去1年間でサイバーインシデントの被害に遭ったとする回答が前年の82%から92%にまで増加した。組織が直面している最も大きな壁はデータ消去であるであり、回答者の35%という結果であるが、これは全地域の中でデータ消去の割合が最も高い。

メキシコの回答者が高い、もしくは比較的高い脆弱性を感じているのはウイルス/ワームによる攻撃（53%）で、データ消去の懸念（50%）後に続き、この不正の増加する被害の経験や認識が反映されているようだ。半分以上（55%）の回答者が、自社が経験したサイバーインシデントの標的になったのは顧客情報だと述べた。次に標的に挙がったのは、従業員情報、次いで物的資産/現金であった。

昨年、メキシコの回答者は、サイバーインシデントの際には連邦法執行機関に通報する可能性が高いと述べたが、今年は回答者の3分の1が、ITサービス会社に連絡すると回答した。

最も多く見られたサイバーインシデントの種類		世界平均
データ消去	35%	25%
ウイルス/ワームによる攻撃	33%	36%
電子メール経由のフィッシング攻撃	29%	33%
機密情報が保存された機器の盗難	27%	21%

主な加害者のタイプ		世界平均
無差別サイバー犯罪者	45%	34%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
ウイルス/ワームによる攻撃	53%	62%
データ消去	50%	58%

最も多い標的		世界平均
顧客情報	55%	48%
従業員情報	45%	41%

サイバーインシデント発生時の連絡先		世界平均
ITサービス会社	34%	35%
保険会社ホットライン	11%	3%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▲ **12%** 対前年比
▼ **10%** 対世界平均

セキュリティ

メキシコの回答者は、今年は昨年よりさらに高いレベルでのセキュリティインシデントを報告している（前年の48%に比べて60%）。しかしながら、この数値は世界的な平均値（70%）からみるとまだ低い。

メキシコの回答者が経験した最も多いセキュリティインシデントは、物的/知的財産侵害であり、38%という結果であった。昨年メキシコにおいてに最も多く報告されたセキュリティインシデントである職場での暴力は23%と、世界的な数値と同等であった。

メキシコの回答者が高い、もしくは比較的高い脆弱性を感じているのが物的/知的財産侵害（58%）で、次いで職場での暴力（40%）である。

元従業員はセキュリティインシデントの要因になる可能性が高いと報告されている。10人のうち4人以上（41%）が加害者になりえるとした（世界平均は37%、昨年値は31%）。

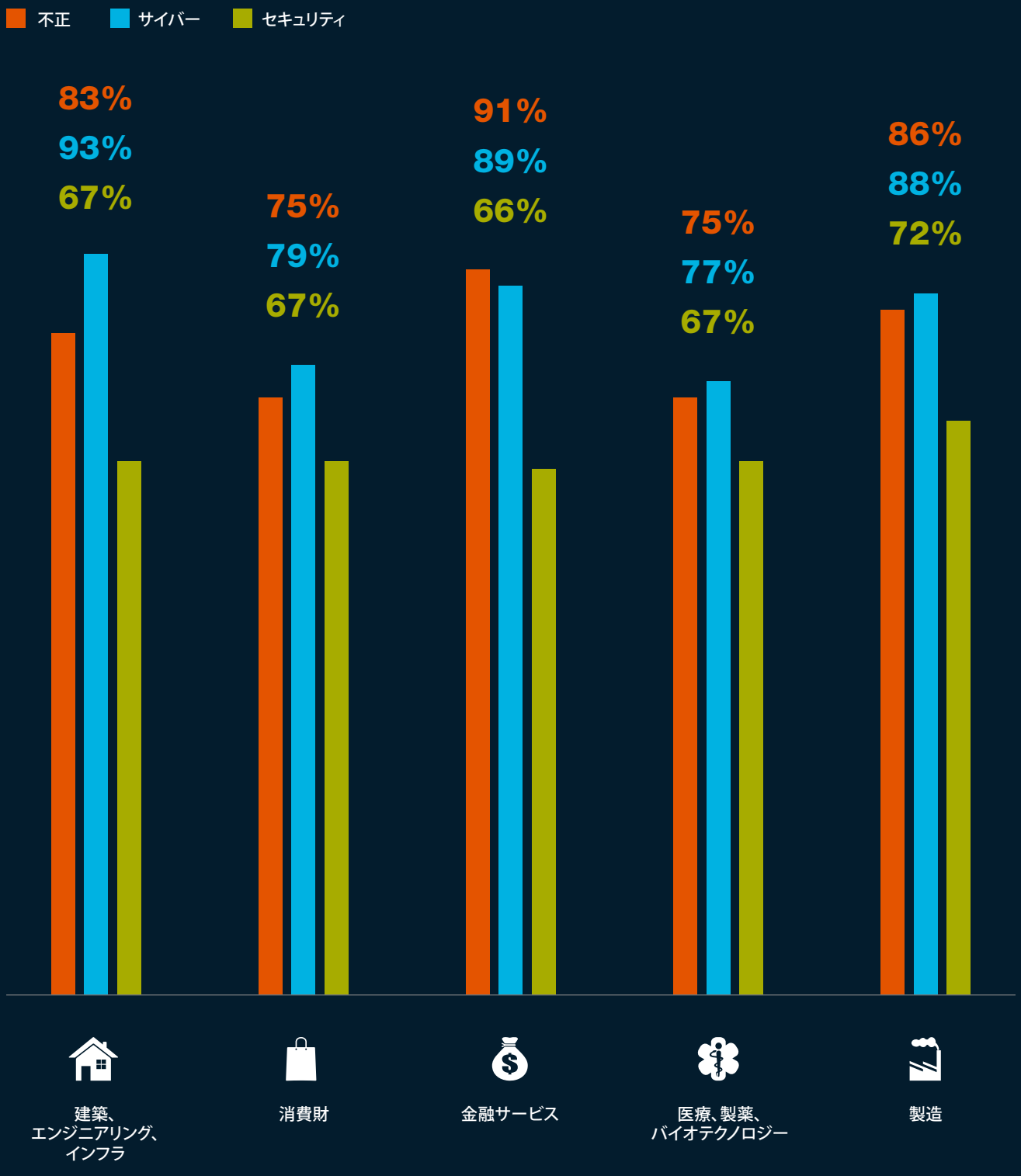
最も多く見られたセキュリティインシデントの種類		世界平均
物的/知的財産侵害	38%	41%
地政学上のリスク（例：紛争地域における操業など）	25%	20%
職場での暴力	23%	23%
環境リスク（ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む）	15%	28%

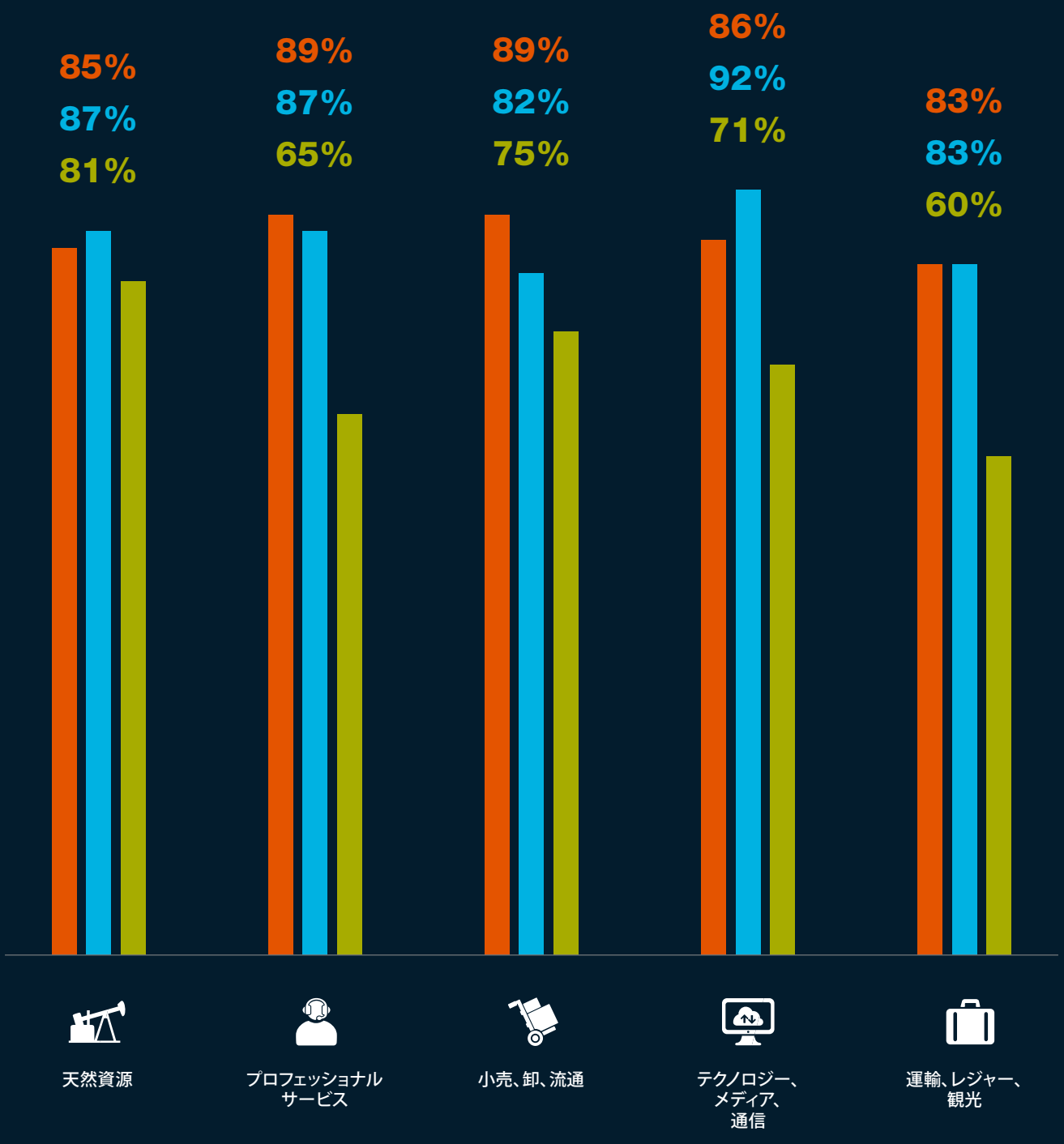
主な加害者のタイプ		世界平均
元従業員	41%	37%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
物的/知的財産侵害	58%	63%
職場での暴力	40%	50%

業界リスクマップ

この図は、過去12か月間に不正、サイバー、およびセキュリティインシデントの被害に遭った経験を有する企業の割合を業界ごとに示したものです。




85%
87%
81%
89%
87%
65%
89%
82%
75%
86%
92%
71%
83%
83%
60%
天然資源
プロフェッショナル サービス
小売、卸、流通
テクノロジー、メディア、通信
運輸、レジャー、観光

建築、エンジニアリング、インフラ

過去12ヶ月間に不正の被害に遭った割合

▲ **13%** 対前年比
▼ **1%** 対世界平均

不正

建築、エンジニアリング、インフラ業界の不正事案は、前年比で最も高い数値を記録した。5分の4（83%）の回答者が今年何らかの不正を報告しており、前年の70%より13%高かった。

不正の種類としては情報漏洩が最も多く（33%）、規制違反とベンダー/サプライヤー不正が30%と続いている。

不正の主な加害者として最も多かったのはジュニアポジション従業員である（47%）。業界内の不正事例の多くは、内部通報者により発覚したものであった（53%）。

半数以上の回答者（54%）が知的財産(機密情報など)の盗難・著作権侵害・偽造に高い、もしくは比較的高い脆弱性を感じており、2年前より21%高くなっている。また、ほとんどの回答者（52%）は経営陣の利益相反に懸念を持っており、2年前より22%高く、規制・コンプライアンス違反が後に続いている（50%）。財務管理（不正検出と内部監査を含む）が、最も多く実行された不正防止対策であった（82%）。

最も多く見られた不正の種類		世界平均
情報漏洩	33%	29%
規制・コンプライアンス違反	30%	20%
ベンダー、サプライヤー、調達部門の不正	30%	20%
物的資産・在庫品の盗難	28%	27%
経営陣の利益相反	28%	26%
汚職・贈収賄	28%	21%

主な加害者のタイプ		世界平均
ジュニアポジション従業員	47%	39%
ベンダー/サプライヤー（例：技術やサービスのプロバイダー）	38%	30%
中上級管理職	38%	27%
フリーランス/短期契約従業員	36%	26%
合弁パートナー（例：製造・その他ビジネス機能担当、フランチャイズ）	29%	23%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
知的財産の盗難（機密情報など）、著作権侵害、偽造	54%	56%
経営陣の利益相反	52%	52%
規制・コンプライアンス違反	50%	49%

最も実施されている不正対策		世界平均
財務（財務管理、不正検出、内部/外部監査、マネーロンダリング対策）	82%	77%
従業員（雇用前調査）	76%	73%
経営陣（経営者管理、インセンティブ、監査委員会等の外部による監視）	74%	74%
パートナー・顧客・ベンダー（デューデリジェンス）	73%	73%
リスク（リスク担当者、リスク管理部門の設置）	73%	75%

不正発見の手段		世界平均
自社の内部通報者	53%	47%

過去12ヶ月間にサイバーインシデントの被害に遭った割合

▲ 16% 対前年比
▲ 7% 対世界平均

サイバーセキュリティ

今年の報告では、建築、エンジニアリング、インフラ業界は他のどの業界よりもサイバーインシデントを経験し、93%の回答者が過去1年間に自社が被害を受けたと報告している。この業界は前年比最も高い数値を出しており、前年より16%高い。

サイバー攻撃で最も多かったのはウイルス/ワームによる攻撃(39%)で、電子メール経由のフィッシング攻撃(37%)、送金不正(31%)、そしてデータ漏洩(31%)が後に続いている。これらの事例の52%において、顧客情報が標的にされている。

回答者は、被害は無差別サイバー犯罪者によるもの(38%)と報告している。この業界の回答者はウイルス/ワームによる攻撃(65%)とデータ漏洩(55%)に対して高い、もしくは比較的高い脆弱性を感じている。

最も多く見られたサイバーインシデントの種類		世界平均
ウイルス/ワームによる攻撃	39%	36%
電子メール経由のフィッシング攻撃	37%	33%
データ漏洩 (顧客/従業員データ、知的財産/機密情報/研究開発情報の喪失など)	31%	27%
送金不正 (電子メールアカウントの乗っ取り/詐称)	31%	19%

主な加害者のタイプ		世界平均
無差別サイバー犯罪者	38%	34%
競合他社	30%	23%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
ウイルス/ワームによる攻撃	65%	62%
データ漏洩 (顧客/従業員データ、知的財産/機密情報/研究開発情報の喪失など)	55%	55%
データ消去	52%	58%
機密情報が保存された機器の盗難	52%	55%

最も多い標的		世界平均
顧客情報	52%	48%
顧客/従業員のID	46%	35%
物的資産/現金	46%	34%
従業員情報	46%	41%

サイバーインシデント発生時の連絡先		世界平均
ITサービス会社	36%	35%
インシデント対応会社(調査、違反通知)	16%	11%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▲ 4% 対前年比
▼ 3% 対世界平均

セキュリティ

3分の2以上(67%)のこの業界の回答者が、自身の組織がセキュリティインシデントを経験をしたことがあると述べた。最も多かったセキュリティインシデントは物的/知的財産侵害で、43%の回答者から報告されており、自然災害のような環境事案が後に続いている(30%)。

中上級管理職、元従業員、そして無差別の加害者が、それぞれ同じ数の回答者(36%)からセキュリティインシデントの主な加害者であると挙げられている。

この業界においては、6割近くの回答者(57%)が、物的/知的財産侵害と地政学/環境のリスクに対して自社が高い、もしくは比較的高い脆弱性を感じている(それぞれ55%と52%)。地政学上のリスクの懸念においては、昨年の25%から倍以上となった。

最も多く見られたセキュリティインシデントの種類		世界平均
物的/知的財産侵害	43%	41%
環境リスク (ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む)	30%	28%
地政学上のリスク (例:紛争地域における操業など)	28%	20%

主な加害者のタイプ		世界平均
中上級管理職	36%	25%
元従業員	36%	37%
無差別加害者	36%	30%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
物的/知的財産侵害	57%	63%
地政学上のリスク (例:紛争地域における操業など)	55%	53%
環境リスク (ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む)	52%	56%

消費財

過去12ヶ月間に不正の被害に遭った割合

- ▼ **7%** 対前年比
- ▼ **9%** 対世界平均

不正

消費財業界では、自社が過去1年間に不正を経験したという回答者は少ない傾向にあり（75%）、世界平均（84%）より9%低い。また、前年の調査よりも7%少ない数値でもある。

この業界で最も多かった不正は物的資産・在庫品の盗難（23%）であり、そのすぐ後に情報漏洩（21%）とベンダー/サプライヤー不正（21%）が続いている。

回答者の4割(41%）が、不正事案はジュニアポジション従業員によるものであるとし、36%は元従業員が不正の主な加害者であるとした。不正事案の最も一般的な手法は内部監査であった（54%）。

この業界の回答者は物的資産・在庫品の盗難（48%）、ベンダー・サプライヤー・調達部門の不正（48%）、そして情報漏洩（46%）に高い、もしくは比較的高い脆弱性を感じている。

この業界の回答者が報告した最も一般的な不正防止対策は、ITセキュリティと技術的な対策（72%）、内部通報ホットラインを含む従業員トレーニング（69%）、そして知的財産リスク評価、著作権モニタリングプログラム（69%）であった。

最も多く見られた不正の種類		世界平均
物的資産・在庫品の盗難	23%	27%
情報漏洩	21%	29%
ベンダー・サプライヤー・調達部門の不正	21%	20%
汚職・贈収賄	19%	21%
経営陣の利益相反	15%	26%

主な加害者のタイプ		世界平均
ジュニアポジション従業員	41%	39%
元従業員	36%	34%
ベンダー/サプライヤー	26%	30%
フリーランス/短期契約従業員	26%	26%
中上級管理職	18%	27%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
物的資産・在庫品の盗難	48%	55%
ベンダー・サプライヤー・調達部門の不正	48%	51%
情報漏洩	46%	57%
知的財産の盗難（機密情報など）、著作権侵害、偽造	42%	56%

最も実施されている不正対策		世界平均
情報（ITセキュリティ、技術的な対策）	72%	78%
従業員（トレーニング、内部通報ホットライン）	69%	74%
知的財産（知的財産リスク評価、著作権モニタリングプログラム）	69%	73%
従業員（雇用前調査）	67%	73%
パートナー・顧客・ベンダー（デューデリジェンス）	66%	73%

不正発見の手段		世界平均
内部監査	54%	44%

過去12ヶ月間にサイバーインシデントの被害に遭った割合

▼ **4%** 対前年比
▼ **7%** 対世界平均

サイバーセキュリティ

消費財業界の回答者の大多数(79%)が、昨年自社がサイバーインシデントの犠牲者となったと述べているが、前年は83%であった。これらの事案のほとんどはウイルス/ワームによる攻撃(29%)と、電子メール経由のフィッシング攻撃(23%)である。

ほとんどの回答者が、サイバーインシデントは元従業員によるものであると回答した(27%)。また、ほとんどのサイバーインシデントは顧客情報(41%)、および物的資産・在庫品(37%)をターゲットにしたものであった。

実際の経験を反映して、回答者はウイルス/ワームによる攻撃(59%)に高い、もしくは比較的高い脆弱性を感じている。半数以上の回答者はデータ漏洩(55%)とランサムウェア攻撃(52%)に高い、もしくは比較的高い脆弱性を感じていると報告した。ランサムウェア攻撃の懸念は昨年より19%上昇し、この脅威に対して33%の回答者が高い、もしくは比較的高い脆弱性を感じたとも述べている。

最も多く見られたサイバーインシデントの種類		世界平均
ウイルス/ワームによる攻撃	29%	36%
電子メール経由のフィッシング攻撃	23%	33%
データの不正操作	19%	22%
機密情報が保存された機器の紛失	19%	19%
データの消去	19%	25%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
ウイルス/ワームによる攻撃	59%	62%
データ漏洩 (顧客/従業員データ、知的財産/機密情報/研究開発情報の喪失など)	55%	55%

最も多い標的		世界平均
顧客情報	41%	48%
物的資産/現金	37%	34%

サイバーインシデント発生時の連絡先		Global Avg.
ITサービス会社	34%	35%
ホームページ/ウェブサイトプロバイダー	10%	8%
保険ポータル	10%	5%

主な加害者のタイプ		世界平均
元従業員	27%	28%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▼ **8%** 対前年比
▼ **3%** 対世界平均

セキュリティ

消費財業界のセキュリティインシデントは、昨年の調査報告に比べると2%の増加があった(前年65%に対して今年は67%)。物的/知的財産侵害が最も多く経験されたセキュリティインシデントであり(40%)、次いで職場での暴力(27%)、そして環境リスク(25%)が続いた。

この業界の回答者はセキュリティインシデントの主な加害者は元従業員(49%)だと挙げており、物的/知的財産侵害(57%)に高い、もしくは比較的高い脆弱性を感じていると報告する傾向がある。前年比で最も増加したのは脆弱性を感じている職場での暴力で、昨年の37%より15%も高い52%であった。

最も多く見られたセキュリティインシデントの種類		世界平均
物的/知的財産侵害	40%	41%
職場での暴力	27%	23%
環境リスク (ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む)	25%	28%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
物的/知的財産侵害	57%	63%
職場での暴力	52%	50%
環境リスク (ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む)	47%	56%

主な加害者のタイプ		世界平均
元従業員	49%	37%

金融サービス

過去12ヶ月間に不正の被害に遭った割合

▲ **2%** 対前年比

▲ **7%** 対世界平均

不正

金融サービス業の9割（91%）の回答者が、今年不正事案を経験しており、今年の報告の中ではどの業界よりも高い結果であった。これは昨年の数値（89%）より2%高く、今年の世界平均（84%）よりかなり高い。

金融サービス業の回答者は、主に経験した不正は経営陣の利益相反（27%）と情報漏洩（27%）と述べている。元従業員（39%）は不正の主な加害者に挙げられ、次いでジュニアポジション従業員（33%）とベンダー/サプライヤー（33%）であった。これらの不正事例の半数以上が内部監査で発覚している（53%）。

今年の回答者は2年前と比較するといくつかのリスクに対してさらに脆弱性を感じている。回答者は社内の財務不正（64%）と知的財産侵害（62%）に高い、もしくは比較的高い脆弱性を感じており、前回の報告よりそれぞれ25%と29%高い。

物的資産・在庫品の盗難も同様に61%と高い。今年はマーケットでの談合・癒着と企業資産の横領といった2種類のリスクは最大の懸念としては挙がって来なかったが、それにもかかわらず、2年前と比較して24%と25%と最も高い伸び率を記録した。

不正防止対策で何を実行したかという質問に対しては、84%の回答者がITセキュリティと技術的な対策を、そして同等の割合で内部通報ホットラインも含めた従業員トレーニングが挙げられた。これらの割合は世界平均のそれぞれ78%と74%よりもかなり高い。

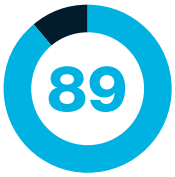
最も多く見られた不正の種類		世界平均
情報漏洩	27%	29%
経営陣の利益相反	27%	26%
汚職・贈収賄	23%	21%
規制・コンプライアンス違反	21%	20%
ベンダー・サプライヤー・調達部門の不正	21%	20%
マーケットでの談合・癒着 (価格協定など)	21%	19%
マネーロンダリング	21%	16%

主な加害者のタイプ		世界平均
元従業員	39%	34%
ジュニアポジション従業員	33%	39%
ベンダー/サプライヤー(例：技術やサービスのプロバイダー)	33%	30%
中上級管理職	24%	27%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
社内の財務不正 (会計操作)	64%	52%
知的財産の盗難 (機密情報など)、**著作権侵害、偽造**	62%	56%
物的資産・在庫品の盗難	61%	55%
経営陣の利益相反	59%	52%

最も実施されている不正対策		世界平均
情報 (ITセキュリティ、技術的な対策)	84%	78%
従業員 (トレーニング、内部通報ホットライン)	84%	74%
パートナー・顧客・ベンダー (デューデリジェンス)	80%	73%
財務 (財務管理、不正検出、内部/外部監査、マネーロンダリング対策)	80%	77%
資産 (物理的なセキュリティシステム、在庫管理、タグ付け、資産登録)	80%	77%

不正発見の手段		世界平均
内部監査	53%	44%



過去12ヶ月間にサイバーインシデントの被害に遭った割合

= 昨年と同等
▲ 3% 対世界平均

サイバーセキュリティ

金融サービス業の回答者からは、今年は平均以上のサイバーインシデントが報告され、世界平均の86%に対し、89%がサイバー攻撃を経験していた。金融サービス企業より報告された、主なサイバーインシデントは電子メール経由のフィッシング攻撃（41%）で、今回の報告で全業界の中で2番目に多かった。

ほとんどの回答者がサイバーインシデントの標的は顧客情報（44%）、機密情報/研究開発情報/知的財産（38%）、そして物的資産・現金（38%）と回答した。これらの攻撃の加害者については、回答者の38%が無差別サイバー犯罪者を挙げた。

サイバーリスクについては、およそ7割の回答者が、データ消去（67%）に高い、もしくは比較的高い脆弱性を感じており、これは昨年よりも19%高い数値であった。

回答者の多くが潜在的なウイルス/ワームによる攻撃（62%）、機密情報が保存された機器の盗難（61%）、サービス妨害攻撃（61%）を懸念しており、特にサービス妨害攻撃は昨年より22%も上昇した。およそ半数の回答者が電子メール経由のフィッシング攻撃を経験したと報告しているが、この脅威にはたったの23%しか脆弱性を感じていないということに着目すべきである。

最も多く見られたサイバーインシデントの種類		世界平均
電子メール経由のフィッシング攻撃	41%	33%
データ漏洩（顧客/従業員データ、知的財産/機密情報/研究開発情報の喪失など）	34%	27%

最も多い標的		世界平均
顧客情報	44%	48%
機密情報・研究開発情報・知的財産	38%	40%
物的資産/現金	38%	34%

主な加害者のタイプ		世界平均
無差別サイバー犯罪者	38%	34%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
データ消去	67%	58%
ウイルス/ワームによる攻撃	62%	62%

サイバーインシデント発生時の連絡先		世界平均
ITサービス会社	36%	35%
ISP/通信プロバイダー	12%	7%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▲ 9% 対前年比
▼ 4% 対世界平均

セキュリティ

金融サービス業の回答者が報告したセキュリティインシデントは今年9%増加しており、昨年の57%だったことと比較すると、3分の2（66%）がセキュリティインシデントの犠牲になっている。しかしながら、これはまだ世界平均71%より低い数値であった。

金融サービス業の5分の2（41%）の回答者が物的/知的財産侵害を報告しており、29%が環境リスク事案を経験している。加害者として最も多かったのは元従業員であった（49%）。

回答者が高い、もしくは比較的高い脆弱性を感じているセキュリティリスクについては、65%が物的/知的財産侵害、62%が環境リスク、そしてほぼ同数（61%）が地政学上のリスクを挙げた。環境と地政学上のリスクは昨年に比べそれぞれ22%と17%上昇した。

最も多く見られたセキュリティインシデントの種類		世界平均
物的/知的財産侵害	41%	41%
環境リスク（ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む）	29%	28%
地政学上のリスク（例：紛争地域における操業など）	18%	20%

主な加害者のタイプ		世界平均
元従業員	49%	37%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
物的/知的財産侵害	65%	63%
環境リスク（ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む）	62%	56%
地政学上のリスク（例：紛争地域における操業など）	61%	53%

医療、製薬、バイオテクノロジー

過去12ヶ月間に不正の被害に遭った割合

- ▼ **5%** 対前年比
- ▼ **9%** 対世界平均

不正

医療、製薬、バイオテクノロジー業界の回答者の4分の3（75%）は、過去1年間に不正事案を経験したと報告した。これは今年のどの業界よりも少なく、世界平均より9%下回っている。複数の種類の不正を経験している回答者は、物的資産の盗難、知的財産侵害、そして企業資産の横領について、同等の数値（29%）を報告した。

ジュニアポジションの従業員は不正の加害者として多く挙げられるが（56%）、今回の報告では、あらゆる業界の中で最も多く報告されており、世界平均より17%高い。

この業界では、経営陣（49%）が不正事案を発見したという割合が高い。また、多くのリスクについて脆弱性の感情が非常に高い。およそ4分の3（73%）の回答者は、知的財産の盗難・著作権侵害・偽造に高い、もしくは比較的高い脆弱性を感じており、この割合は、わずか2年で41%も増加を示している。汚職・贈収賄（39%＋の71%）のみならず、社内の財務不正（34%増加の70%）、そして情報盗難（25%増加の70%）についても高い脆弱性を感じている。マーケットにおける談合・癒着への懸念は2年前の14%の数値が今年は急激に62%へと4倍以上に上昇した。

この業界で最も多かった不正防止対策は従業員雇用前調査（85%）、次いでITセキュリティ、技術的な対策（80%）であった。

最も多く見られた不正の種類		世界平均
物的資産・在庫品の盗難	29%	27%
知的財産(機密情報など)の盗難・著作権侵害・偽造	29%	20%
企業資産の横領	29%	20%
経営陣の利益相反	27%	26%
情報漏洩	23%	29%
社内の財務不正 (会計操作)	23%	23%

主な加害者のタイプ		世界平均
ジュニアポジション従業員	56%	39%
エージェント / 仲介者(例：会社の代理で活動する第三者)	41%	24%
元従業員	38%	34%
監督官庁	38%	15%
合弁パートナー (例：製造・その他ビジネス機能担当、フランチャイズ)	36%	23%
中上級管理職	36%	27%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
知的財産の盗難 (機密情報など)、著作権侵害、偽造	73%	56%
汚職・贈収賄	71%	50%
社内の財務不正 (会計操作)	70%	52%
情報漏洩	70%	57%

最も実施されている不正対策		世界平均
従業員 (雇用前調査)	85%	73%
情報 (ITセキュリティ、技術的な対策)	80%	78%
財務 (財務管理、不正検出、内部/外部監査、マネーロンダリング対策)	79%	77%
世評 (メディア監視、コンプライアンス制御、法的評定)	79%	72%
資産 (物理的なセキュリティシステム、在庫管理、タグ付け、資産登録)	77%	77%

不正発見の手段		世界平均
自社の幹部	49%	35%

過去12ヶ月間にサイバーインシデントの被害に遭った割合

▼ 9% 対前年比
▼ 9% 対世界平均

サイバーセキュリティ

この業界で調査した4分の3以上（77%）の幹部が、サイバーインシデントの被害を報告した。これは昨年の数値（86%）からも、今年の世界平均（86%）からもそれぞれ9%減少している。

最も多かった被害はウイルス/ワームによる攻撃である（38%）。今回の調査でどの業界よりも多く報告された機密情報が保存された機器の紛失（33%）が後に続き、世界平均19%を大きく上回っている。主な加害者として多く挙げられたのは競合他社であった（43%）。

この業界における82%の回答者が、データ消去において高い、もしくは比較的高い脆弱性を感じており、昨年より23%高い結果となった。高い脆弱性で目立った他の分野はウイルス/ワームによる攻撃（27%増加の78%）、機密情報が保存された機器の盗難（73%）、サービス妨害攻撃（26%増加の73%）、そして電子メール経由のフィッシング攻撃（20%増加で73%）であった。

顧客情報と従業員情報はサイバー攻撃の主な標的（それぞれ63%と58%）として挙げられた。業界の専門性からすると想定範囲内であるのが、半数（55%）以上の回答者が、サイバーインシデントで標的にされたのは機密情報・研究開発情報・知的財産であったと報告している。

最も多く見られたサイバーインシデントの種類		世界平均
ウイルス/ワームによる攻撃	38%	36%
機密情報が保存された機器の紛失	33%	19%
電子メール経由のフィッシング攻撃	31%	33%

最も多い標的		世界平均
顧客情報	62%	48%
従業員情報	57%	41%
機密情報・研究開発情報・知的財産	55%	40%

主な加害者のタイプ		世界平均
競合他社	42%	23%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
データ消去	82%	58%
ウイルス/ワームによる攻撃	78%	62%

サイバーインシデント発生時の連絡先		世界平均
ITサービス会社	45%	35%
インシデント対応会社（調査、違反通知）	15%	11%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▲ 2% 対前年比
▼ 3% 対世界平均

セキュリティ

医療、製薬、バイオテクノロジー業界の3分の2（67%）の回答者から、過去1年間にセキュリティインシデントの被害に遭ったという回答があった。これは、この業界では不正とサイバーセキュリティに関するインシデントが減少しているにもかかわらず、昨年の65%をわずかに上回ったことを示している。

被害が多かったのは、物的/知的財産侵害（40%）、職場での暴力（35%）、そして環境リスク（35%）であった。実際に被害に遭った経験から、彼らは物的盗難（79%）と環境リスク（66%）に高い、もしくは比較的高い脆弱性を感じている。この業界で最も多く挙げられた主な加害者は元従業員であった。

最も多く見られたセキュリティインシデントの種類		世界平均
物的/知的財産侵害	40%	41%
職場での暴力	35%	23%
環境リスク（ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む）	35%	28%

主な加害者のタイプ		世界平均
元従業員	54%	37%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
物的/知的財産侵害	79%	63%
環境リスク（ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む）	66%	56%
地政学上のリスク（例：紛争地域における操業など）	60%	53%

製造

過去12ヶ月間に不正の被害に遭った割合

▼ **3%** 対前年比

▲ **2%** 対世界平均

不正

今年、製造業の回答者が世界平均以上の不正を報告しているが（世界平均84%に対し86%）、これでも昨年よりは3%低い数値であった。

この業界で最も多かった不正として挙げられたのは、3分の1（33%）が情報漏洩、次いで汚職・贈収賄（28%）、経営陣の利益相反（26%）、そして社内の財務不正（26%）であった。

多くの回答者は、ジュニアポジション従業員が不正事案の加害者であると報告し（42%）、元従業員が後に続く（34%）。不正発見の手段は、内部通報者によるものが最も多かった（46%）。

現況の脆弱性については、回答者は情報漏洩（62%）、社内の財務不正（57%）、そしてベンダー・サプライヤー・調達部門の不正（56%）に高い、もしくは比較的高い脆弱性を感じている。5分の4以上の回答者（84%）が、不正防止のために会社が財務管理（不正検出、内部監査を含む）を行っていると述べている。同等の割合で資産統制（物理的なセキュリティシステム、在庫管理、タグ付け、資産登録）を報告している。

最も多く見られた不正の種類		世界平均
情報漏洩	33%	29%
汚職・贈収賄	28%	21%
経営陣の利益相反	26%	26%
社内の財務不正（会計操作）	26%	23%

主な加害者のタイプ		世界平均
ジュニアポジション従業員	42%	39%
元従業員	34%	34%
ベンダー/サプライヤー（例：技術やサービスのプロバイダー）	30%	30%
フリーランス/短期契約従業員	26%	26%
エージェント / 仲介者（例：会社の代理で活動する第三者）	22%	24%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
情報漏洩	62%	57%
社内の財務不正（会計操作）	57%	52%
ベンダー・サプライヤー・調達部門の不正	56%	51%
知的財産の盗難（機密情報など）、著作権侵害、偽造	52%	56%

最も実施されている不正対策		世界平均
財務（財務管理、不正検出、内部/外部監査、マネーロンダリング対策）	84%	77%
資産（物理的なセキュリティシステム、在庫管理、タグ付け、資産登録）	84%	77%
情報（ITセキュリティ、技術的な対策）	80%	78%
経営陣（経営者管理、インセンティブ、監査委員会等の外部による監視）	80%	74%
従業員（トレーニング、内部通報ホットライン）	80%	74%
リスク（リスク担当者、リスク管理部門の設置）	80%	75%

不正発見の手段		Global Avg.
自社の内部通報者	46%	47%

過去12ヶ月間にサイバーインシデントの被害に遭った割合

▼ **3%** 対前年比
▲ **2%** 対世界平均

サイバーセキュリティ

製造業の回答者がサイバーインシデントにおいて平均よりも高い被害を報告をしているが(88%)、それでも昨年より3%改善している(91%)。製造業の回答者が最も多く経験したサイバーインシデントはウイルス/ワームによる攻撃で(38%)、電子メール経由のフィッシング攻撃とデータ消去が後に続いている(それぞれ26%)。

約半数(49%)の回答者がサイバー攻撃による被害を経験し、顧客情報、次いで機密情報(45%)と従業員情報(35%)が標的となった。

半数以上の回答者(57%)が、データ消去について自身の企業が高い、もしくは比較的高い脆弱性を感じていると考えており、それと同じくらい多くの回答者が電子メール経由のフィッシング攻撃(55%)とウイルス/ワームによる攻撃(55%)も主な脆弱性であると述べている。送金不正の脆弱性も急上昇しており、昨年より19%増加した。

最も多く見られたサイバーインシデントの種類		世界平均
ウイルス/ワームによる攻撃	38%	36%
データ漏洩(顧客/従業員データ、知的財産/機密情報/研究開発情報の喪失など)	26%	27%
電子メール経由のフィッシング攻撃	26%	33%
データ消去	22%	25%

最も多い標的		世界平均
顧客情報	49%	48%
機密情報・研究開発情報・知的財産	45%	40%
従業員情報	35%	41%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
データ消去	57%	58%
電子メール経由のフィッシング攻撃	55%	57%
ウイルス/ワームによる攻撃	55%	62%

主な加害者のタイプ		世界平均
無差別サイバー犯罪者	41%	34%

サイバーインシデント発生時の連絡先		世界平均
ITサービスベンダー	25%	35%
インシデント対応会社(調査、違反通知)	18%	11%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▼ **9%** 対前年比
▲ **2%** 対世界平均

セキュリティ

製造部門の回答者より報告されたセキュリティインシデントは昨年の合計81%から今年は72%へ低下した。この数値は世界平均の70%よりはまだ高いが、全ての部門において前年比より最も大きい減少だった。

回答者によると、物的/知的財産侵害は最も多いセキュリティインシデントの種類だ(45%)。2番目に頻繁に発生しているセキュリティインシデントは環境リスクである(24%)。回答者によると、攻撃は概ね無差別加害者によるものである。

回答者は物的/知的財産侵害(53%)にかなり、もしくは比較的高い脆弱性を感じている。テロ(47%)の懸念が最も増加しており、昨年より21%の増加となった。

最も多く見られたセキュリティインシデントの種類		世界平均
物的/知的財産侵害	45%	41%
環境リスク(ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む)	24%	28%
職場での暴力	19%	23%
地政学上のリスク(例:紛争地域における操業など)	19%	20%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
物的/知的財産侵害	53%	63%
国内外のテロ	47%	49%
地政学上のリスク(例:紛争地域における操業など)	45%	53%
環境リスク(ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む)	45%	56%

主な加害者のタイプ		世界平均
無差別加害者	31%	30%

天然資源

過去12ヶ月間に不正の被害に遭った割合
- ▲ **5%** 対前年比
- ▲ **1%** 対世界平均

不正

天然資源業界の85%の回答者が、昨年不正の被害に遭っているが、これは世界平均の84%をわずかに上回り、且つ、昨年より5%多い数字であった。

不正の種類については、この業界の回答者は経営陣の利益相反（35%）とマーケットでの談合・癒着（29%）が最も多いと報告した。4人に1人（27%）が、過去1年間に知的財産侵害の被害に遭ったと述べた。これらは全て世界平均の26%、19%、20%をそれぞれを大幅に上回っている。

この部門ではジュニアポジションの従業員が不正の主な加害者であると報告されており（45%）、元従業員（41%）と中上級管理職（34%）が後に続いている。内部通報はこの業界では不正検知に重要な役割を果たしており、不正事案の70%は内部通報者による発覚だ。ただし、これは世界平均よりも23%高いのだが、内部通報による発見はいずれの業界においても最も不正多く報告された手段であった。

天然資源業界の回答者は2年前より21%も多く報告された経営陣の利益相反（68%）に、高い、もしくは比較的高い脆弱性を感じている。回答者たちは情報漏洩（65%）と企業資産の横領（61%）にも、同様に脆弱性を感じている。

不正事案のリスクを低減させるため、5人中4人（80%）の回答者が、自社で知的財産リスクのアセスメントを行っていると報告しており、4分の3（75%）が不正検知を含む財務管理を行っていると述べている。

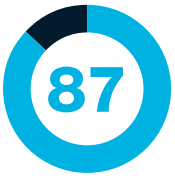
最も多く見られた不正の種類		世界平均
経営陣の利益相反	35%	26%
マーケットでの談合・癒着（価格協定など）	29%	19%
知的財産(機密情報など)の盗難・著作権侵害・偽造	27%	20%
物的資産・在庫品の盗難	25%	27%
マネーロンダリング	23%	16%

主な加害者のタイプ		世界平均
ジュニアポジション従業員	45%	39%
元従業員	41%	34%
中上級管理職	34%	27%
ベンダー/サプライヤー(例：技術やサービスのプロバイダー)	32%	30%
合弁パートナー（例：製造・その他ビジネス機能担当、フランチャイズ）	32%	23%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
経営陣の利益相反	68%	52%
情報漏洩	65%	57%
企業資産の横領	61%	48%
物的盗難・在庫品の盗難	60%	55%

最も実施されている不正対策		世界平均
知的財産（知的財産リスク評価、著作権モニタリングプログラム）	80%	73%
財務（財務管理、不正検出、内部/外部監査、マネーロンダリング対策）	75%	77%
経営陣（経営者管理、インセンティブ、監査委員会等の外部による監視）	73%	74%
パートナー・顧客・ベンダー（デューデリジェンス）	73%	73%
世評（メディア監視、コンプライアンス制御、法的評定）	68%	72%

不正発見の手段		世界平均
自社の内部通報者	70%	47%



過去12ヶ月間にサイバーインシデントの被害に遭った割合

▲ **1%** 対前年比
▲ **1%** 対世界平均

サイバーセキュリティ

この業界の大多数（87%）の回答者が、自社の組織が前年のうちにサイバーインシデントを経験したと述べており、種類としては電子メール経由のフィッシング攻撃が最も多かった（38%）。そのほか、ウイルス/ワームによる攻撃（37%）とデータの不正操作（31%）も一般的である。

回答者によると、元従業員がサイバー攻撃の加害者であったケースが多く（33%）、続いてフリーランス/短期契約従業員（29%）と競合他社（27%）である。

この業界の回答者はサイバーインシデントの主な標的は機密情報・研究開発情報・知的財産（47%）であり、続いて従業員情報（42%）、そして企業もしくは従業員のIDであった（42%）。

実際の被害に即して、この業界の回答者は電子メール経由のフィッシング攻撃（69%）に最も脆弱性を感じており、これは昨年より21%高い。これらの回答者は、ウイルス/ワームによる攻撃（64%）や送金不正（59%）に高い、もしくは比較的高い脆弱性を感じている。

最も多く見られたサイバーインシデントの種類		世界平均
電子メール経由のフィッシング攻撃	38%	33%
ウイルス/ワームによる攻撃	37%	36%
データの不正操作	31%	22%

最も多い標的		世界平均
機密情報・研究開発情報・知的財産	47%	40%
従業員情報	42%	41%
顧客/従業員のID	42%	35%

主な加害者のタイプ		世界平均
元従業員	33%	28%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
電子メール経由のフィッシング攻撃	69%	57%
ウイルス/ワームによる攻撃	64%	62%
送金（電子メールアカウントの乗っ取り/詐称）	59%	50%

サイバーインシデント発生時の連絡先		世界平均
ITサービス会社	24%	35%
保険ブローカー	11%	4%
州法執行機関	11%	6%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▲ **11%** 対前年比
▲ **11%** 対世界平均

セキュリティ

天然資源業界の回答者はセキュリティインシデントの大幅な広がりをみている。81%が少なくとも昨年に一度は影響を受けており、これは昨年度より11%増加している上、世界平均よりも11%上回っている。

物的/知的財産侵害は最も多いインシデント（44%）で、その後に環境リスクが続く（42%）。5人に2人の回答者（40%）が中上級管理職がセキュリティインシデントの主な加害者と挙げた。

およそ4分の3の回答者は、環境リスク（71%）に高い、もしくは比較的高い脆弱性を感じているが、このリスクに関しては実際の被害経験とは比例していないようだ。同様に、職場での暴力は実際の被害の上位3つのカテゴリーに入っていないにも関わらず、64%の回答者が脆弱性を感じている。

最も多く見られたセキュリティインシデントの種類		世界平均
物的/知的財産侵害	44%	41%
環境リスク（ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む）	42%	28%
地政学上のリスク（例：紛争地域における操業など）	27%	20%

主な加害者のタイプ		世界平均
中上級管理職	40%	25%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
環境リスク（ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む	71%	56%
職場での暴力	64%	50%
物的/知的財産侵害	58%	63%

プロフェッショナルサービス

過去12ヶ月間に不正の被害に遭った割合

▲ **5%** 対前年比

▲ **5%** 対世界平均

不正

プロフェッショナルサービス業界では、不正事案の被害に遭った回答者は昨年より5%増加し、前年の84%から89%に上昇した。情報漏洩(33%)と社内の財務不正(29%)が、主な不正である。

回答者によると、不正の主な加害者はジュニアポジション従業員(37%)で、次に中上級管理職(31%)、そして元従業員(31%)と続いている。これらの不正の発見は、主に内部通報や経営陣によりなされている(43%)。

ITセキュリティと技術的な対策はプロフェッショナルサービス業界では最も多く実行されており、88%の回答者が回答している。他に共通して報告されている不正防止対策はリスク担当者、リスク管理部門の設置であった(82%)。これらは両方とも世界平均の77%と75%をそれぞれ上回っている。

この業界の回答者は、物的資産・在庫品の盗難(56%)、知的財産侵害(56%)、そして情報漏洩(51%)について、高い、もしくは比較的高い脆弱性を感じている。

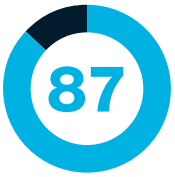
最も多く見られた不正の種類		世界平均
情報漏洩	33%	29%
社内の財務不正(会計操作)	29%	23%
ベンダー・サプライヤー・調達部門の不正	27%	20%
汚職・贈収賄	27%	21%
物的資産・在庫品の盗難	25%	27%
経営陣による利益相反	25%	26%

主な加害者のタイプ		世界平均
ジュニアポジション従業員	37%	39%
中上級管理職	31%	27%
元従業員	31%	34%
ベンダー/サプライヤー (例:技術やサービスのプロバイダー)	29%	30%

最も実施されている不正対策		世界平均
情報 (ITセキュリティ、技術的な対策)	88%	77%
リスク (リスク担当者、リスク管理部門の設置)	82%	75%
資産 (物理的なセキュリティシステム、在庫管理、タグ付け、資産登録)	80%	77%
財務 (財務管理、不正検出、内部/外部監査、マネーロンダリング対策)	79%	77%
従業員 (トレーニング、内部通報ホットライン)	78%	74%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
物的資産・在庫品の盗難	56%	55%
知的財産(機密情報など)の盗難・著作権侵害	56%	56%
情報漏洩	51%	57%

不正発見の手段		世界平均
自社の内部通報者	43%	47%
自社の幹部	43%	35%



過去12ヶ月間にサイバーインシデントの被害に遭った割合

▲ 3% 対前年比
▲ 1% 対世界平均

サイバーセキュリティ

サイバーインシデントはプロフェッショナルサービス業界でも増加しており、回答者によると、昨年の84%に対し今年は87%が被害を経験している。サイバーインシデントの種類で最も多いのはウイルス/ワームによる攻撃（38%）で、次がデータ消去（29%）であった。

サイバーインシデントに直面したプロフェッショナルサービス業界のおよそ半数の回答者が、従業員情報（52%）と顧客情報（46%）がサイバー攻撃の主な標的であったと報告している。これらの攻撃の主な加害者は元従業員（33%）と中上級管理職（25%）であった。

高い、もしくは比較的高い脆弱性を感じるサイバーリスクは、機密情報が保存された機器の盗難（67%）であり、昨年より16%増加している。また、サービス妨害攻撃（64%）とデータ消去（63%）にも懸念を抱いている。

最も多く見られたサイバーインシデントの種類		世界平均
ウイルス/ワームによる攻撃	38%	36%
データ消去	29%	25%
データ漏洩（顧客/従業員データ、知的財産/機密情報/研究開発情報の喪失など）	27%	27%

最も多い標的		世界平均
従業員情報	52%	41%
顧客情報	46%	48%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
機密情報が保存された機器の盗難	67%	55%
サービス妨害攻撃	64%	52%
データ消去	63%	58%

主な加害者のタイプ		世界平均
元従業員	33%	28%

サイバーインシデント発生時の連絡先		世界平均
IT サービス会社	40%	35%
ホームページ/ウェブサイトプロバイダー	10%	8%
インシデント対応会社（調査、違反通知）	10%	11%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▲ 2% 対前年比
▼ 5% 対世界平均

セキュリティ

プロフェッショナルサービス業界の回答者のうち3分の2以上（65%）が、過去1年間にセキュリティインシデントを経験している。これは前年の63%よりも増加しているが、世界平均の70%よりは低い。セキュリティインシデントの主な種類は物的/知的財産侵害（38%）と環境リスク（65%）である。

3分の1以上の回答者が、元従業員がセキュリティインシデントの加害者であると指摘している（36%）。実体験に基づいて、回答者が高い、もしくは比較的高い脆弱性を感じていると報告しているのは、物的/知的財産侵害であった（67%）。地政学上のリスク（55%）と環境リスク（56%）にも、同程度に脆弱性を感じている。

最も多く見られたサイバーセキュリティインシデントの種類		世界平均
物的/知的財産侵害	38%	41%
環境リスク（ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む）	29%	28%
職場での暴力	24%	23%

主な加害者のタイプ		世界平均
元従業員	36%	37%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
物的/知的財産侵害	67%	20%
地政学上のリスク（例：紛争地域における操業など）	57%	25%
環境リスク（ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む）	56%	21%

小売、卸、流通

過去12ヶ月間に不正の被害に遭った割合
- ▲ **6%** 対前年比
- ▲ **5%** 対世界平均

不正

小売・卸・流通業界の回答者のうち、89%が過去1年間に不正事案を経験しており、世界平均より5%、昨年より6%の増加となっている。また、その業界の回答者は情報盗難の被害も平均値より多い(39%)。

さらに物的資産の盗難(33%)、経営陣の利益相反(32%)、そして社内の財務不正(28%)も後に続いている。

その業界で昨年最も多かった不正は資産の横領で、依然として課題にはなっているが、贈収賄と汚職と並んで、最も多い不正の種類の5位についている(同じく23%)。

この業界では、不正の加害者として顧客が最も多く(31%)、物的盗難が多くみられた。合弁パートナーとフランチャイジー、ベンダー/サプライヤーは共に31%の回答者に主な加害者として報告されている。

この業界でおよそ3分の1の回答者(74%)は、情報盗難に高い、もしくは比較的高い脆弱性を感じており、2年前より30%増加している。同様な増加傾向がマーケットでの談合・癒着にも見られ、63%という数値は2年前の3倍以上である。知的財産侵害(2倍以上の67%)と規定・コンプライアンス違反(ほぼ2倍の62%)も同様である。

この業界で物的資産盗難が多く報告されたことを考慮すると、86%が、物理的なセキュリティシステム、在庫管理を含め、資産に対する不正防止対策実施を進めたことは驚くにあたらない。この数値は世界平均の77%より大幅に高い。この業界では外部監査が最も多く不正を発見した手段であった(41%)。しかしながら、内部通報や内部監査、経営陣による検知など(全て39%)を含む他のチャネルでも、不正発見の手段として多く報告された。

最も多く見られた不正の種類		世界平均
情報漏洩	39%	29%
物的資産・在庫品の盗難	33%	27%
経営陣による利益相反	32%	26%
社内の財務不正(会計操作)	28%	23%

主な加害者のタイプ		世界平均
顧客	31%	22%
合弁パートナー (例:製造・その他ビジネス機能担当、フランチャイズ)	31%	23%
ベンダー/サプライヤー(例:技術やサービスのプロバイダー)	31%	30%
中上級管理職	29%	27%
元従業員	29%	34%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
情報漏洩	74%	57%
物的資産・在庫品の盗難	68%	55%
知的財産(機密情報など)**の盗難・著作権侵害・偽造**	67%	56%

主な加害者のタイプ		世界平均
資産 (物理的なセキュリティシステム、在庫管理、タグ付け、資産登録)	86%	77%
経営陣 (経営者管理、インセンティブ、監査委員会等の外部による監視)	84%	74%
従業員(雇用前調査)	80%	73%
情報(ITセキュリティ、技術的な対策)	78%	73%
財務 (財務管理、不正検出、内部/外部監査、マネーロンダリング対策)	78%	77%
知的財産 (知的財産リスク評価、著作権モニタリングプログラム)	78%	78%

不正発見の手段		世界平均
外部監査	41%	35%

過去12ヶ月間にサイバーインシデントの被害に遭った割合

▼ **5%** 対前年比
▼ **4%** 対世界平均

サイバーセキュリティ

この部門で大多数（82%）の回答者が、過去1年間にサイバーインシデントを経験しているが、この数値は昨年より5%減少している（87%）。電子メール経由のフィッシング攻撃が最も多く報告されたサイバーインシデントで、40%の回答者であったが、これは世界平均の33%よりもかなり高い数値であった。

サイバーインシデントを低減するための対策にかかわらず、72%の回答者がウイルス/ワームによる攻撃と、61%がランサムウェア攻撃に高い、もしくは比較的高い脆弱性を感じていると報告した。

この業界の回答者が直面したサイバー攻撃で、最も標的になったのは従業員情報だ（53%）。次いで顧客情報（38%）と機密情報（同じく38%）となっている。

無差別サイバー犯罪者が加害者として最も多く挙げられ（34%）、次いで競合他社（28%）となっており、顧客情報と機密情報により得るものが多いといえる。

サイバーインシデントが発生した場合、この業界の調査回答者はインシデント対応会社に連絡し、調査とブリーチの通告を依頼する傾向が最も強い。世界平均11%に対し、19%の回答者がそのように答えている。

最も多く見られたサイバーインシデントの種類		世界平均
電子メール経由でのフィッシング詐欺	40%	33%
データ漏洩（顧客/従業員データ、知的財産/機密情報/研究開発情報の喪失など）	33%	27%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
ウィルス/ワームによる攻撃	72%	62%
ランサムウェア攻撃	61%	55%
データ消去	56%	58%
機密情報が保存された機器の紛失	56%	53%

最も多い標的		世界平均
従業員情報	53%	41%
顧客情報	38%	48%
機密情報・研究開発情報・知的財産	38%	40%

主な加害者のタイプ		世界平均
無差別サイバー犯罪者	34%	34%

サイバーインシデント発生時の連絡先		世界平均
ITサービス会社	43%	35%
インシデント対応会社（調査、違反通知）	19%	11%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▼ **4%** 対前年比
▲ **5%** 対世界平均

セキュリティ

小売・卸・流通業界の4分の3の回答者によると、昨年セキュリティインシデントの被害に遭ったと述べており、世界平均の70%より高いものの、昨年の数値よりは4%低下した。物的/知的財産侵害（回答者の42%）、環境リスク（26%）、地政学上のリスク（21%）に関連するセキュリティインシデントが多くみられた。

この業界では、元従業員がセキュリティインシデントの加害者として最も多く（35%）、次いで競合他社となっている（33%）。被害の経験が最いことに鑑み、物的/知的財産侵害に高い、もしくは比較的高い脆弱性を感じていると回答者が報告している（65%）。

最も多く見られたセキュリティインシデントの種類		世界平均
物的/知的財産侵害	42%	41%
環境リスク（ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む）	26%	28%
地政学上のリスク（例：紛争地域における操業など）	21%	20%

主な加害者のタイプ		世界平均
元従業員	35%	37%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
物的/知的財産侵害	65%	63%
地政学上のリスク（例：紛争地域における操業など）	54%	53%
国内外のテロ	50%	49%

テクノロジー、メディア、通信

過去12ヶ月間に不正の被害に遭った割合

▲ **7%** 対前年比

▲ **2%** 対世界平均

不正

テクノロジー、メディア、通信業界では、86%の回答者が過去1年間に不正事案を経験した。世界平均（84%）をわずかに上回り、昨年報告された79%よりも7%増加していることになる。

この業界では、情報漏洩（35%）の被害が世界平均（29%）と比較すると高い。次に多い不正が物的資産・在庫品の盗難（31%）と、規制・コンプライアンス違反（29%）である。

主な加害者としては、フリーランス / 短期契約従業員が最も多く（41%）回答されており、これは世界平均の26%より大幅に高い。ジュニアポジションの従業員（同じく41%）も同様で、元従業員と 、ベンダー/サプライヤーも挙げられている （いずれも31%）。この業界では、内部関係者が不正発見の主な情報源であり、内部通報が最も一般的な不正発見手段であった （59%）。

この業界の回答者は、経営陣の利益相反（63%）に高い、もしくは比較的高い脆弱性を感じており、2年前の数値に比べると2倍以上であった（31%）。同様に、彼らの大きな懸念であるマーケットでの談合・癒着についても、2年前に比べて3倍以上になり、2年前の17%に対し55%という結果になった。

不正防止対策として最も多いのは、物理的なセキュリティシステム、在庫管理、タグ付けなど、資産に関するものであると88%が回答している。この業界のITセキュリティ等情報に関する不正防止対策を取っているという回答者は、わずかに少ない（84%）。

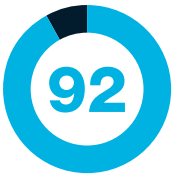
最も多く見られた不正の種類		世界平均
情報漏洩	35%	29%
物的資産・在庫品の盗難	31%	27%
規制・コンプライアンス違反	29%	20%
知的財産（機密情報など）の盗難・著作権侵害・偽造	27%	20%
経営陣による利益相反	27%	26%

主な加害者のタイプ		世界平均
フリーランス・短期契約従業員	41%	26%
ジュニアポジション従業員	41%	39%
元従業員	30%	34%
ベンダー / サプライヤー（例：技術やサービスのプロバイダー）	30%	30%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
経営陣による利益相反	63%	52%
情報漏洩	62%	57%
知的財産の盗難（機密情報など）、著作権侵害、偽造	59%	56%

最も実施されている不正対策		世界平均
資産（物理的なセキュリティシステム、在庫管理、タグ付け、資産登録）	88%	77%
情報（ITセキュリティ、技術的な対策）	84%	78%
リスク（リスク担当者、リスク管理部門の設置）	82%	75%
知的財産（知的財産リスク評価、著作権モニタリングプログラム）	82%	73%

不正発見の手段		世界平均
自社の内部通報者	59%	47%



過去12ヶ月間にサイバーインシデントの被害に遭った割合

▲ **15%** 対前年比
▲ **6%** 対世界平均

サイバーセキュリティ

世界平均が86%であるのに対し、この業界の回答者の大多数（92%）が前年にサイバーインシデントを経験したと報告している。前年比より増加している（15%）のは建築、エンジニアリング、インフラ業界である。電子メール経由のフィッシング攻撃が最も多いサイバーインシデントであり（43%）、全ての部門において最も回答が多かった。次にウイルス/ワームによる攻撃（41%）が続いている。これらの割合は世界平均よりかなり高くなっている（それぞれ33%と36%）。

この業界の回答者は、元従業員がサイバーインシデントの加害者であるケースが多いと報告している。世界平均の28%と比較すると、4割以上（43%）が、元従業員が主な加害者であると述べている。

今年、テクノロジー、メディア、通信業界の幹部は、電子メール経由のフィッシング攻撃（67%）に最も高い脆弱性を感じていると回答している。また、昨年より21%多いランサムウェア攻撃（65%）についても脆弱性を感じているという回答であった。

テクノロジー、メディア、通信業界で、最もサイバーインシデントの標的になりやすいものは顧客情報であった（回答者の53%）。

最も多く見られたサイバーインシデントの種類		世界平均
電子メール経由でのフィッシング詐欺	43%	33%
ウイルス/ワームによる攻撃	41%	36%
データの不正操作	35%	22%

主な加害者のタイプ		世界平均
元従業員	43%	28%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
電子メール経由でのフィッシング詐欺	67%	57%
ランサムウェア攻撃	65%	55%

最も多い標的		世界平均
顧客情報	53%	48%
従業員情報	51%	41%

サイバーインシデント発生時の連絡先		世界平均
ITサービス会社	38%	35%
ISP/通信プロバイダー	17%	7%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▼ **1%** 対前年比
▲ **1%** 対世界平均

セキュリティ

この業界の71%が、自社でセキュリティインシデントが発生したと回答している。最も多かったセキュリティインシデントは物的/知的財産侵害である（39%）。しかしながら、回答者は職場での暴力（35%）も世界平均（23%）に比べると多い。

本調査では、ジュニアポジションの従業員（42%）が加害者であるケースが多いと回答されている。回答者は物的/知的財産侵害（66%）に高い、もしくは比較的高い脆弱性を感じており、職場での暴力（64%）と同様に19%増加している。

最も多く見られたセキュリティインシデントの種類		世界平均
物的/知的財産侵害	39%	41%
職場での暴力	35%	23%
環境リスク（ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む）	25%	28%

主な加害者のタイプ		世界平均
ジュニアポジション従業員	42%	26%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
物的/知的財産侵害	66%	47%
職場での暴力	64%	49%
環境リスク（ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む）	59%	51%

運輸、レジャー、観光

過去12ヶ月間に不正の被害に遭った割合

▼ **2%** 対前年比
▼ **1%** 対世界平均

不正

運輸、レジャー、観光業界の回答者の大多数（83%）が、自社が昨年不正事案を経験したと報告しているが、これは昨年より2%の減少となっている（85%）。

この業界の回答者は物的資産・在庫品の盗難（34%）と情報漏洩（34%）を経験したと述べており、共に世界平均の27%と29%より高い。これらの後に社内の財務不正（23%）が続いている。不正の加害者としては、元従業員（36%）、顧客（27%）、そして中上級管理職（27%）の順番で報告された。

この業界の調査回答者は、不正は社内で発見していることが多く、内部通報や内部監査などが最も一般的な手段と報告している（それぞれ39%）。

回答者は物的資産・在庫品の盗難（53%）と汚職・贈収賄（51%）に高い、もしくは比較的高い脆弱性を感じていると述べた。加えて、多数が懸念していたマーケットでの談合・癒着が2年前に報告された数値よりも3倍近くになり、2年前の18%に対して今年は51%であった。

この業界の組織で最も多く実行されている不正防止対策は、回答者の報告によるとリスク関連の対策導入が多く、リスク担当者（82%）、知的財産（78%）、メディアモニタリングのような世評、パートナー・顧客・ベンダーのデューデリジェンス（78%）、そして財務管理（78%）だ。

最も多く見られた不正の種類		世界平均
物的資産・在庫品の盗難	34%	27%
情報漏洩	34%	29%
社内の財務不正(会計操作)	23%	23%
経営陣による利益相反	19%	26%
マネーロンダリング	19%	16%

不正リスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
物的資産・在庫品の盗難	53%	55%
汚職・贈収賄	51%	50%
マーケットでの談合・癒着(価格協定など)	51%	50%
経営陣による利益相反	49%	52%
マネーロンダリング	49%	43%

主な加害者のタイプ		世界平均
元従業員	36%	34%
中上級管理職	27%	27%
顧客	27%	22%
ジュニアポジション従業員	20%	39%

最も実施されている不正対策		世界平均
リスク(リスク担当者、リスク管理部門の設置)	82%	75%
知的財産 (知的財産リスク評価、著作権モニタリングプログラム)	78%	73%
世評(メディア監視、コンプライアンス制御、法的評定)	78%	72%
パートナー・顧客・ベンダー(デューデリジェンス)	78%	73%
財務 (財務管理、不正検出、内部/外部監査、マネーロンダリング対策)	78%	77%

不正発見の手段		世界平均
自社の内部通報者	39%	47%
内部監査	39%	44%

過去12ヶ月間にサイバーインシデントの被害に遭った割合

▼ 4% 対前年比
▼ 3% 対世界平均

サイバーセキュリティ

83%の回答者が昨年サイバーインシデントを経験しているが、これは世界平均をわずかに下回っており（86%）、昨年の報告と比較しても同程度の減少が見られた（87%）。

最も多かった攻撃はウイルス/ワームによる感染であった（43%）。この後に電子メール経由のフィッシング攻撃（28%）とデータ消去（25%）が続いている。

顧客情報（55%）と企業/従業員ID（39%）は、サイバーインシデントの標的として挙げられた上位2つであった。無差別サイバー犯罪者（32%）と元従業員（27%）が、主な加害者として報告されている。

回答者はデータの不正操作（58%）に高い、もしくは比較的高い脆弱性を感じており、ランサムウェア攻撃とウイルス/ワームによる攻撃（いずれも56%）がその後に続く。

最も多く見られたサイバーインシデントの種類		世界平均
ウイルス/ワームによる攻撃	43%	36%
電子メール経由でのフィッシング詐欺	28%	33%
データ消去	25%	25%

最も多い標的		世界平均
顧客情報	55%	48%
企業/従業員のID	39%	35%

主な加害者のタイプ		世界平均
無差別サイバー犯罪者	32%	34%

サイバーリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
データの不正操作	58%	56%
ランサムウェア攻撃	56%	55%
ウイルス/ワームによる攻撃	56%	62%
データ漏洩（顧客/従業員データ、知的財産/機密情報/研究開発情報の喪失など）	55%	55%

サイバーインシデント発生時の連絡先		世界平均
ITサービス会社	34%	35%
インシデント対応会社（調査、違反通知）	11%	11%
ホームページ/ウェブサイトプロバイダー	11%	8%

過去12ヶ月間にセキュリティインシデントの被害に遭った割合

▼ 10% 対前年比
▼ 10% 対世界平均

セキュリティ

運輸、レジャー、観光業界の60%の回答者のみが過去にセキュリティインシデントを経験をしたと述べ、世界平均の70%を大幅に下回る数値は、どの業界よりも低い。

最も一般的なセキュリティインシデントは、物的/知的財産侵害であった（40%）。これはこの業界の継続的な懸念事項であり、63%の回答者は物的/知的財産侵害において、高い、もしくは比較的高い脆弱性を感じている。

最も多く見られたセキュリティインシデントの種類		世界平均
物的/知的財産侵害	40%	41%
職場での暴力	17%	23%
環境リスク（ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む）	17%	28%

主な加害者のタイプ		世界平均
元従業員	38%	37%
無差別犯罪者	38%	30%

セキュリティリスクに対して脆弱性が高い、もしくは比較的高いと回答している割合		世界平均
物的/知的財産侵害	63%	63%
環境リスク（ハリケーン、竜巻、洪水、地震といった自然災害による被害を含む）	60%	56%
地政学上のリスク（例：紛争地域における操業など）	51%	53%

クロール　ミッションとバリュー

クロールとは

クロールはリスクとコンサルティングサービスのリーディング・グローバル・プロバイダーです。

私たちのミッション

お客様のリスクに対する予測、検知、軽減、そして対応を支援しています。

クロールの特徴

45年以上前、クロールはビジネス調査業界のパイオニアとして誕生し、時代と共に変化してまいりました。私たちは絶えず変化するリスクと脅威の状況に対応するために、常に進化し、適応できるスキルとサービスを提供しています。

- 私たちはグローバル・ファームです。当社の専門家は、成熟市場と新興市場の両方において、幅広い業界および国における経験を有しています。この多様性を活用して、専門性、データ、言語、そして技術のいずれにおいても多分野にわたるマルチなチームを結集することができます。私たちは、法律事務所、政府機関、非営利団体、そして個人まで、グローバルなお客様にサービスをご提供致します。
- 私たちは事実への絶え間ない追及、確固たるフォレンジックの専門知識、洞察力のある分析、そして独自経験に基づいた見識に裏付けされた調査アプローチにより認められてきました。この基本的なフォーカスが、私たちそのものであり、私たちのDNAでもあるのです。
- 私たちは、うわべだけでの情報では、確かな情報に基づく健全な決定につながるわけではないことを理解しています。私たちは、お客様に情報のアドバンテージを提供するため、専門性、グローバルな展開と技術を活用します。より深く、より洗練され、より文脈に沿った情報は、結果的により確かな意思決定をもたらします。
- **私たちのクライアントは、自信を持った選択を行うために知識とインテリジェンスを求めています。**

私たちのバリュー

- お客様の信頼と自信を得るために、根気強く努力します
- 私たちは責任とプライドを持ってお客様のニーズを理解します
- 私たちは、他の人に見えない答えを見つけるために、当たり前のものの先をみます
- 私たちは世界中で協力し、人々の起業家スピリットを大切にします
- 私たちは変化をもたらします

お問合せ先

クロールのサービスに関するご質問は下記担当者、もしくは
www.kroll.comまでお気軽にお問合せください

お問合せ先

600 Third Avenue, New York, NY 10016

北米

ボストン
Daniel Linskey
T +1 617 210 7471
daniel.linskey@kroll.com

シカゴ
Baltazar Vallenilla
T +1 312 345 2767
bvallenilla@kroll.com

ロサンゼルス
Jason Smolanoff
+1 213 700 4312
jason.smolanoff@kroll.com

ナッシュビル
Marc Brawner
T +1 615 577 6765
mbrawner@kroll.com

ニューヨーク
Dan Karson
T +1 212 833 3266
dkarson@kroll.com

フィラデルフィア
Mark Ehlers
T +1 215 568 8305
mehlers@kroll.com

レストン
Mari Davies-DeMarco
T +1 571 521 6160
mdavies@kroll.com

サンフランシスコ
Betsy Blumenthal
T +1 415 743 4825
bblument@kroll.com

トロント
Peter McFarlane
T +1 416 813 4401
pmcfarlane@kroll.com

ワシントンDC
David Fontaine
T +1 202 833 6866
david.fontaine@kroll.com

中南米

ボゴタ
Pablo Iragorri
T +57 1 742 5556
pablo.iragorri@kroll.com

ブエノスアイレス
Juan Cruz Amirante
T +54 11 4706 6024
jcamirante@kroll.com

グレナダ
Glen Harloff
T +1 786 340 6753
gharloff@kroll.com

メキシコシティ
Brian Weihs
T +52 55 5279 7250
bweihs@kroll.com

マイアミ
James Faulkner
T +1 786 801 8214
jfaulkner@kroll.com

サオ・パウロ
Fernanda Barroso
T +55 11 3897 0907
fernanda.barroso@kroll.com

欧州・中東・アフリカ

ロンドン
Neil Kirton
T +44 20 70 29 5000
nkirton@kroll.com

ドバイ
Amine Antari
T +971 4 449 6700
amine.antari@kroll.com

マドリード
Marcelo Correia
T +34 91 2747974
marcelo.correia@kroll.com

ミラノ
Marianna Vintiadis
T +39 02 86998088
mvintiadis@kroll.com

モスクワ
Alex Volcic
T +7 495 9692898
avolcic@kroll.com

パリ
Béchir Mana
T +33 1 42678146
bmana@kroll.com

アジア太平洋

香港
Paul Jackson
T +852 2884 7763
paul.jackson@kroll.com

北京、上海
Violet Ho
T +86 10 5964 7600
vho@kroll.com

ムンバイ
Reshmi Khurana
T +91 22 6724 0504
rkhurana@kroll.com

シンガポール
Richard Dailly
T +65 6645 4521
rdailly@kroll.com

日本
Naoko Murasaki
T +81 3 3509 7103
nmurasaki@kroll.com

kroll.com