見えない不正をスポットライトの下へ

「知ること」が経済犯罪と闘うための第一歩となる

pwc

www.pwc.com/crimesurvey


35%
37%
26%
2011
2014
2016

目次

序文

近年、世界的に不正、汚職と言った経済犯罪に関連する報道が過熱しています。そのような時流の中で、世界中で事業を展開する多くの企業が、経済犯罪リスクが自社の競争力・持続性に与えうる影響の重要性を認識し始めています。また、国家レベルにおいても、市場の透明性確保、不正のないビジネス環境の整備が国外からの投資を誘致する上で不可欠であるという認識が高まっています。

その中で、タイが、経済犯罪リスクに対する意識という点において、先進的立場にあると言えるのは、私にとって非常にうれしいことであります。事実、PwCの「経済犯罪実態調査2018」に参加した企業数は、全世界中でタイが最も多く、タイ国内においてこの問題が非常に重要視されていることを示唆しています。

本書で後述しておりますが、リスクを認識し、それについて語っていくことが、経済犯罪を防止するための第一歩であります。不正・不祥事に対する意識を持ち、認識を高めることで、例え防御ラインが破られ経済犯罪が発生したとしても、より迅速かつ効果的に対応することが出来るようになるのです。それは、適切な調査および法的措置による損害回復といった直接的な金銭的メリットのみならず、事態の混乱による事業運営への影響、株価への影響、風評被害、規制当局からの課徴金や行政処分等の副次的影響を最小限に抑える上でも非常に重要になります。

タイ国内において経済犯罪に関する議論が活発化した主な背景として、政府が、グローバル化、市場開放、透明性の向上に力を入れており、それに伴いビジネス環境および文化が変化していることが考えらます。

私は、このような変化の中で、PwCが積極的な役割を果たしてきたことを誇りに思っております。2009年、不正および経済犯罪の防止、発見、調査を主な任務とするタイ国内初の不正対応専門家チーム（Forensics）を発足しました。以来、同チームは、会議やセミナー、メディア、個別企業との打合わせの場と言った様々な機会を活用し、企業を取り巻く経済犯罪リスクの大きさや対策の重要性についての啓蒙を行い、意識の向上を図ってきました。

そして同チームは、年間40件を超える案件（財務諸表の不正、資産の横領、贈収賄、キックバック、サイバー犯罪に関する調査や腐敗行為防止法やマネーロンダリング防止に係るコンプライアンス支援）を経験することで、実用的な専門性および知識を蓄積してきました。

読者の皆様も、ぜひ本書をお読みいただき、経済犯罪と不正に関する話合いに参加して頂ければと思います。知っている、認識しているからこそ、私たちはともに経済犯罪と闘うことができるのです。

Sira Intarakumthornchai
Chief Executive Officer, PwC Thailand

はじめに

「タイ経済犯罪実態調査2018（以下、「本調査」）」では、多くの企業が経験した経済犯罪およびその傾向に加え、見えないリスク、盲点となりやすい論点に焦点を当てております。

本調査結果によると、過去2年間に何かしらの経済犯罪被害にあったと回答したタイ国内の回答者の割合は48%と、2016年の26%からほぼ倍増しております。

一見すると、この2年間に経済犯罪の発生が爆発的に増加しているように見えますが、実際には、それらの犯罪や不正は以前から企業内部に潜んでおり、これまで明るみに出てこなかったものが、不正への認識の向上により表面化されたというのが実情ではないかと思います。

しかし、この傾向は非常に良いことで喜ぶべきことであります。

不正の防止、発見、調査の最前線にいる私たちは、日々目に見えない敵と闘っています。例え姿が目の前に見えなくても、不正行為者がすぐそこにいるという事実を認識して受け入れることこそが、闘いに勝つ第一歩となるのです。本調査結果からも、企業は今、この重要な第一歩を踏み出しつつあることが見えてきました。

pwc

しかし、実際にはその認識レベルはまちまちです。例えば、不正や汚職等を含む経済犯罪を容認することが、犯罪社会への加担となり、一企業内の問題ではなく、国、業界に影響を及ぼす可能性があるということを認識している企業は、人材、業務プロセス改善、および最新技術を含めた不正防止態勢構築に投資し、経済犯罪の発生リスクを効果的に最小化するよう努めています。一方で、これらの犯罪収益に関する認識が希薄な企業は、知らず知らずのうちに、自社を危険な立ち位置に晒していることになるのです。

従って、今自問すべきは　「不正の被害を受けたことがあるか」ではなく、「不正が組織にどのような影響を与えるか、そのリスクを十分に理解した上で対応しているのか」という質問です。

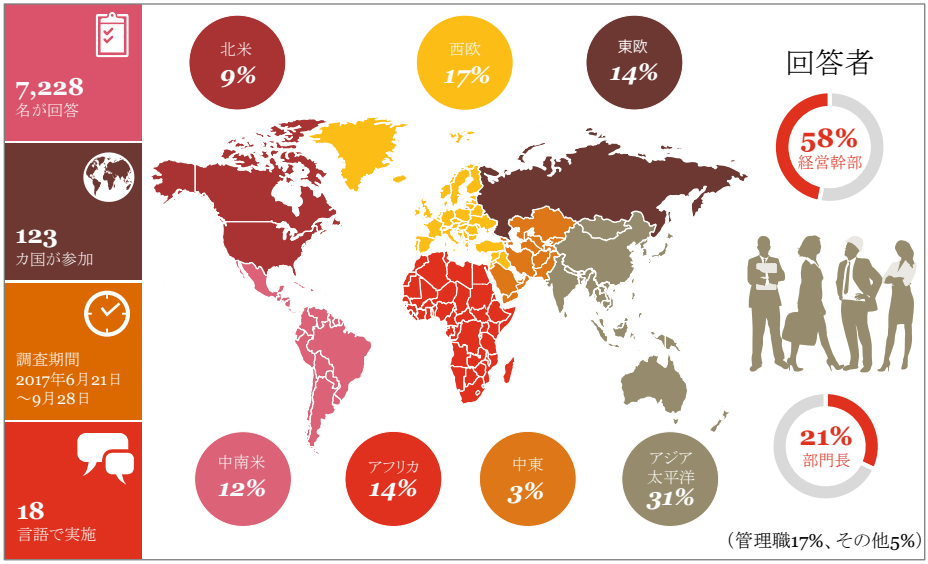
不正には、まだ影響が表れていないものが数多く潜んでおります。本書では、企業が組織内の不正を発見するのを妨げている盲点や、そうした盲点について今企業は何ができるのか、また何をすべきかについて考察していきます。

Vorapong Sutanont
Partner
Forensic Services, PwC Thailand

第1章

タイにおける経済犯罪の実態
―認識の高まりと対応の実情

2018年グローバル調査の概要

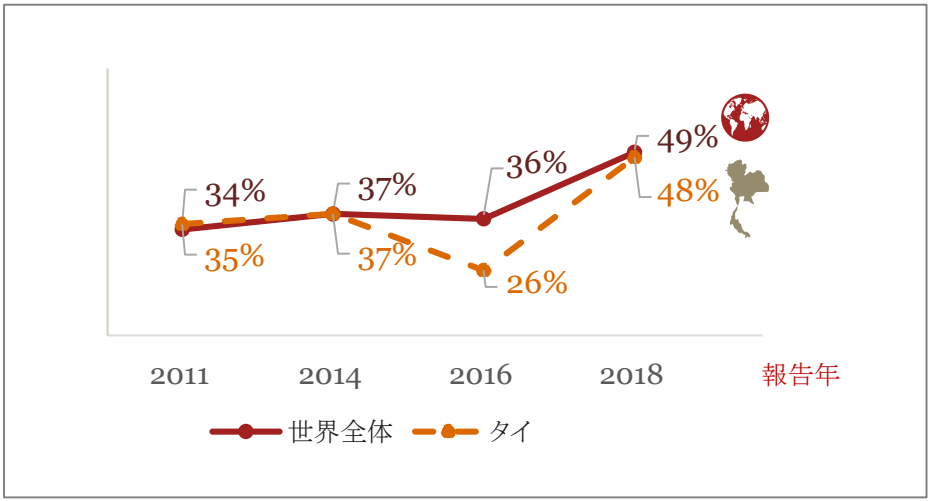


タイにおけるPwC「経済犯罪実態調査2018」の調査結果によると、過去2年間に経済犯罪を経験したと答えた回答者は全体の48%であり、2016年からほぼ倍増した。世界的にも、経済犯罪を経験した企業の割合は36%から49%と大幅増になっている。

しかし、本当にこの数字が示すほど経済犯罪そのものが増加したのだろうか。それとも水面下に潜んでいた不正が、ここに来てやっと目に見える形として表面にはっきりと表れ始めた結果なのだろうか。

経済犯罪や不正との闘いの最前線で得た我々の経験からいうと、おそらく後者であろう。前回の調査結果との違いは、サイバー犯罪などの新たな脅威により経済犯罪や不正の発生数が増加したことが理由であることも否定できないが、それら新しい脅威を含めて不正に対する認識が向上したことが原因だと考えられる。

経済犯罪報告率 – 世界とタイの比較



企業は不正と対峙する上で、何らかの形で経済犯罪被害を受けている可能性があるという認識を持つことが重要である。しかし、依然として多くの不正リスクが発見または報告されることなく看過されてしまっているのも事実である。その理由として、損害額が微少であること等が挙げられるが、被害の大小にかかわらず不正を見過ごすことは、不正行為者を次第に大胆にしていき、共謀者を巻き込み大規模な不正に発展し、やがて長期間に亘り企業に多大な損害をもたらす可能性がある。

不正に対する意識が向上しているのは非常に良い兆候であり、個々の企業のみならずタイ全体にとって、不正と対峙する上での闘い方に根本的な変化をもたらすだろう。それは、不正の早期発見に対する会社の姿勢でありメカニズムの導入であり、そして、不正の報告率がさらに上昇したときに、真に意識が向上し、その仕組みが結実したといえるのではないだろうか。

近年、タイ企業、外国企業に限らず、タイ国内で事業を運営する企業は、不正や経済犯罪についてオープンに語るようになってきた。そのような意識をもたらした一因として、タイのグローバル化、市場開放、透明性の向上に伴う、ビジネス環境及び文化の変化が挙げられる。

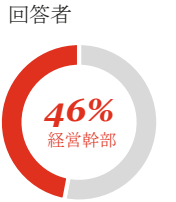
実際、その意識の高さは、タイにおける調査参加者数が全世界で最も多かったことからも明らかである。そのおかげで、私たちはタイ国内における経済犯罪や不正の規模とその影響、また企業がどのような対策を講じているかについて、貴重な知見を得ることができた。本調査において、全123カ国から得た回答数7,228件の内、522件がタイからのものであった。これは、第2位の米国の約350件を大幅に上回っている。

その内訳を見ていくと、タイの回答者のほぼ半数（46%）が経営幹部、22%は財務、監査、コンプライアンス、リスク管理などの担当部門長となっており、多くの高位役職者から回答頂いている。これは、経済犯罪に対する懸念、対策というのが企業の経営課題として優先的な位置付けとして捉えられていることを示唆しているとも考えられる。

業界別には、約半数（46%）が産業部門と最も多くなっており、これは製造および輸出産業が中心となるタイの産業構造を反映していると言える。産業部門の内訳は、自動車が6%、化学が3%、電力/公益事業/鉱業が5%、建設が4%、ヘルスケアが2%、交通/運輸が5%、その他製造業が21%となっている。

2018年における調査の回答者属性（タイ）

回答者



71%
財務、経営管理、
監査、コンプライアンス、
リスク管理、不正・金融犯罪部門

42%
多国籍企業に勤務

55%
従業員1,000名超の企業
（32%が従業員5,000名超の企業）

51%
上場企業

33%
非公開企業

業界

46%
産業部門

19%
金融サービス

6%
保険

6%
小売・消費材

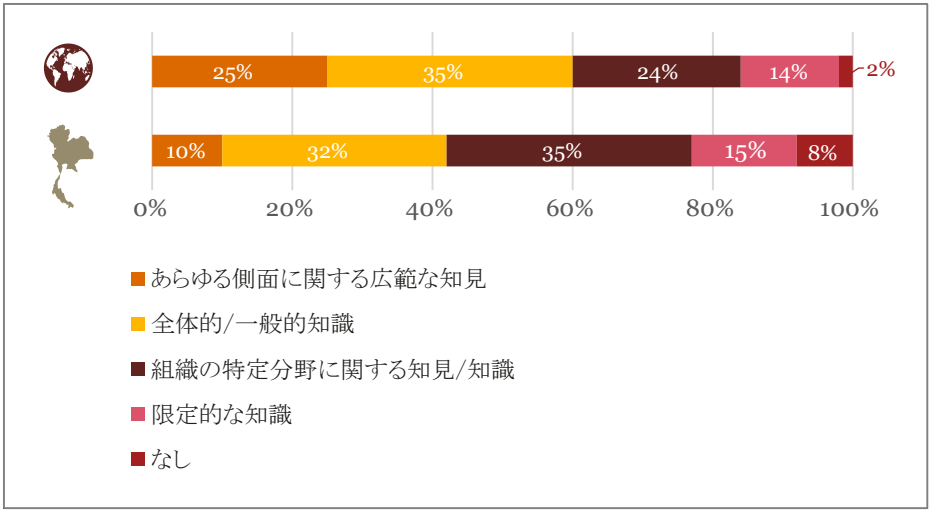
6%
テクノロジー

（管理職25%、その他7%）

続いて、金融サービスと保険会社が全体の4分の1を占めている。この金融保険部門が占める割合は2016年の調査よりも減少しているが、これは単に産業部門の回答数が大幅に上昇し母数が拡大したためであり、金融保険部門の回答者数も実際には増加している。タイ国内の産業構造を鑑みると、依然として、金融サービス企業や保険会社は、同業界が不正行為者に最も狙われやすいという認識を持っていることが見て取れる。

ここで次のような疑問が生じる。企業は、経済犯罪対応の必要性を議論するだけでなく、実際に、従来の受動的で有事対応的な姿勢から、より積極的に不正を防止・検出する姿勢へと移行しているだろうか。それとも、不正との闘いに欠かせない極めて重要な何らかの要素がまだ不足しているのだろうか。

経済犯罪に関する知識 – 世界とタイの比較



意識は向上しているが、全体像の理解が欠けている

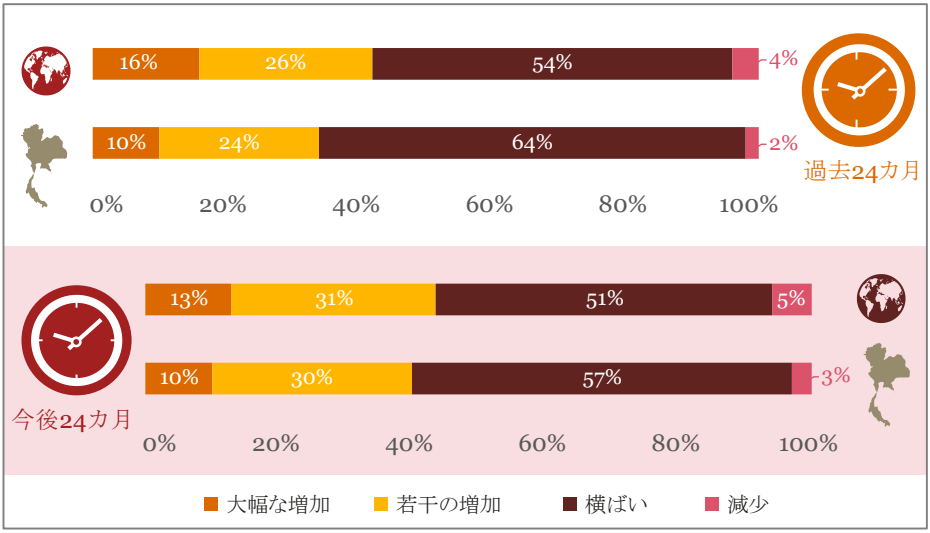
本調査の結果から、タイ企業全体として、不正や経済犯罪に対する意識は向上しているものの、多くの企業が経済犯罪について依然として限定的な知見しか持っていないことが分かる。驚くべきことに、組織内の経済犯罪リスクについて広範な知見を有していると回答したのは、回答者の10%（世界平均25%）と少数であった。全体として見ると、タイ企業は、経済犯罪に関する最新知識、および自身の事業活動の中で実際に何が起こっているのかの認識という点で、依然として世界の平均水準に達していないことが見て取れる。

話題として不正や経済犯罪を意識していても、知見不足により目の前にあるリスクや犯罪を見逃してしまう可能性があるため、今後2年間でこれらの数値が大きく改善することを期待したい。

また、組織内の特定分野についてのみ知見を有すると述べた回答者は35%あり、これは、コンプライアンス、倫理、およびリスク管理という議論をする際に、各部門が個別に対応しており、情報が部門間で共有されたり全社的な対応がなされていない可能性もある。

臭いものに蓋をするではないが、不正は、担当部門内で隠蔽されたり、「他人事」とみなされ易いため、不正との闘いに勝つためには、縦割り的に対応するのではなく、全社的な姿勢をもって広範かつ包括的なアプローチをとることが必要である。

不正・経済犯罪防止策への投資 – 世界とタイの比較

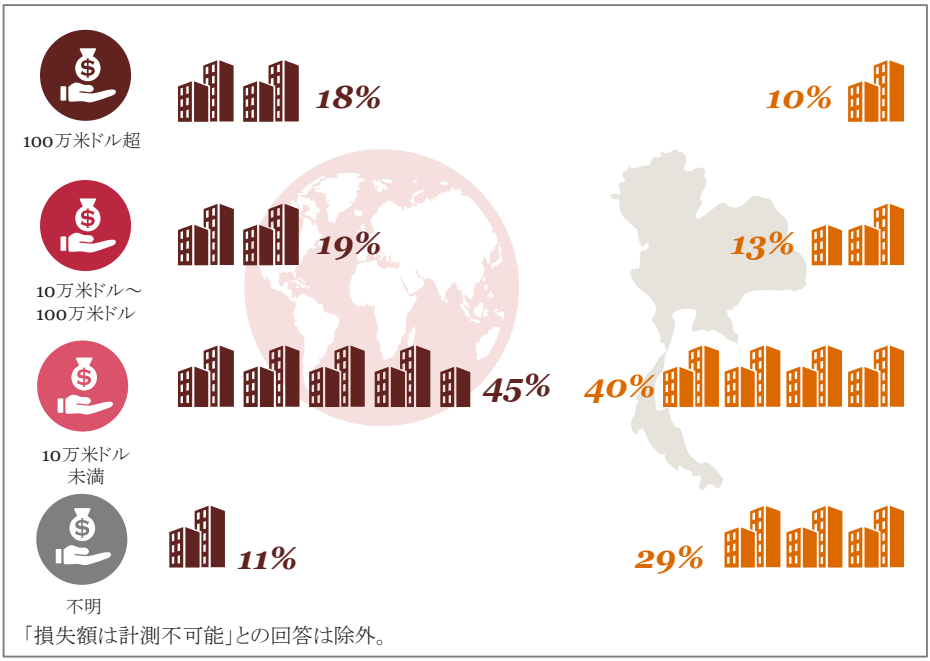


経済犯罪による損失額が拡大する可能性があるにも拘わらず、なぜ防止策への投資が遅れているのか

経済犯罪がもたらす損失額の大きさを考えると、経済犯罪防止策に追加投資を検討している企業の数はあまりにも少ない。回答者の64%は、不正や経済犯罪対策に配分する予算の額は過去2年間にわたって増えていないと答え、57%が今後2年間は増やす予定もないと答えている。

過去2年間に予算を大幅に増やした回答者の割合はわずか10%であり、今後2年間に大幅増加を予定している回答者も10%のみである。なお、ある程度予算を増強すると答えた回答者は過去2年間の24%から30%に上昇している。

最も致命的な経済犯罪による直接的な損失額 – 世界とタイの比較

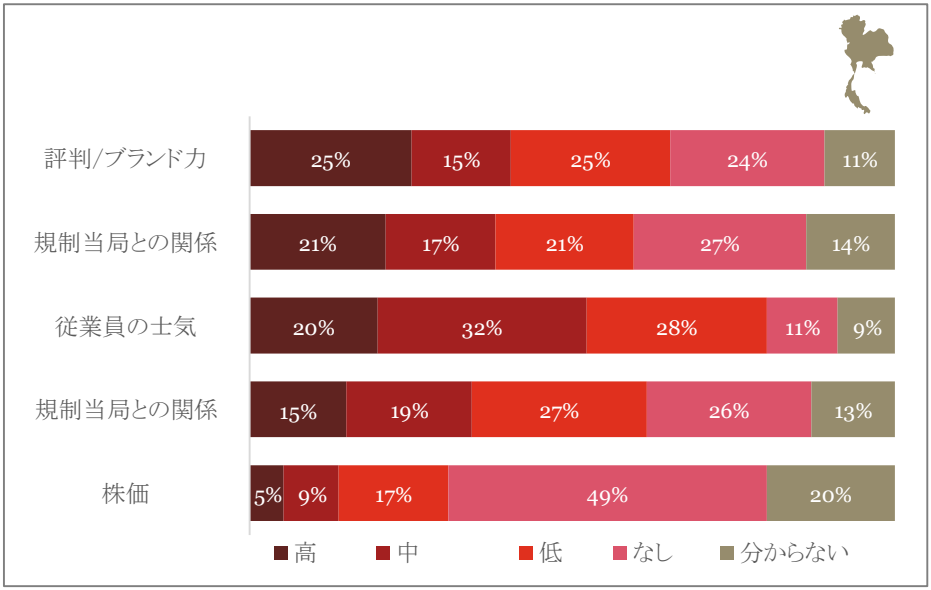


経済犯罪がもたらす損失の広範さと大きさを考えると、その対策に費用を投じることの投資効果は非常に高いはずである。タイでは、10%の回答者が、過去2年間に発生した最も重大な経済犯罪被害による被害額はが少なくとも100万米ドル以上と答えている。その内訳は、1億米ドル以上が1名、5,000万米ドル～1億米ドルが4名、100万米ドル～ 5,000万米ドルが21名であった。

また、13%が10万米ドル～100万米ドルの被害があったと回答してる。しかしながら、全体の29%が実際どの程度被害があったのか分からないとのことである。

不正および経済犯罪防止対策への投資が加速しないのは、想定被害額の特定と防止策導入の費用対効果が、なかなか企業として、見えにくく予算化しずらいのも一因なのであろう。

経済犯罪による非財務的影響（タイ）



風評への影響

しかし、損失は必ずしも財務的なものに限らず、間接的被害も決して無視できるものではない。非財務的な影響として、過去2年間に経済犯罪を経験した回答者の40%が自社の評判とブランド力に大きな又は中程度の影響を与えたと回答している。

世界的にも評判やブランド力などへの風評被害が重大な間接的被害と認識されており、それが結果として取引先との関係や株価にも影響していると考えられる。これらの、経済犯罪による二次的被害は2016年と比較しても増加傾向にある。

ブランドや地位、評判を確立するには何十年という歳月がかかる。一方で、一つの不祥事の発生や、その際の対応が不十分かつ不適切である場合、それまで築いた信用が崩れ去るのは一瞬である。「悪事千里を走る」というが、経営陣が損害の範囲や程度を特定し、対応策を立てている間に、ブランドの毀損は始まっている。

それらのリスクに迅速に対応するためには、企業は危機管理計画を策定し、有事にどう行動すべきか備えておく必要がある。責任者、関与すべき部署を定め、危機の際のシナリオ、役割を全てのステークホルダーが認識しておくことが重要である。

対応の正当性への説明責任

経済犯罪被害の事実が規制当局との関係に致命的な影響を与えたとの回答が**21%**、中程度の影響を与えたとの回答が**17%**となっており、企業の規制に対するコンプライアンス意識や態勢構築の程度等が、規制当局の企業を見る目に影響を与えていることが見て取れる。規制当局による監視が強化されていく中で競争に生き残るには、自社が前広に危機管理を行っていることを当局に説明し理解してもらう必要がある。

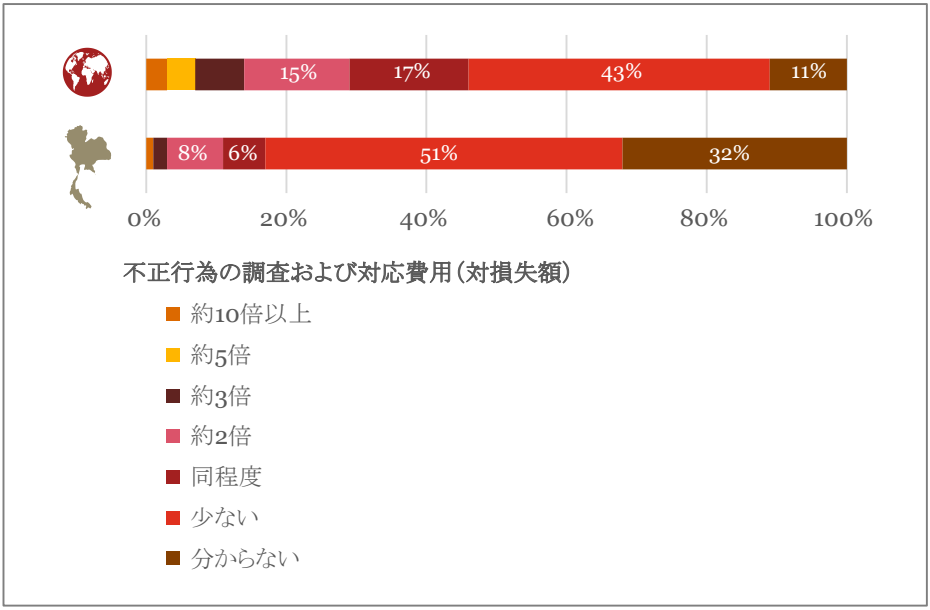
従業員のモラルと会社への信頼

不正や経済犯罪の発生は従業員の士気に大きな影響を及ぼす。回答者の**52%**が、経済犯罪の発生が会社に対する従業員の士気に影響を与えたと述べている。

一部の高い倫理観を持った善意の従業員にとっては、不正を容認してしまう企業文化や脆弱な内部統制が、不満や不公平さを感じる要因になり、また、経営陣に対する信頼の失墜や失望につながることになる。また、それらの従業員は、自らの社内での立ち位置や生活と言った現実と正義感の狭間で、内部通報をすべきか黙っているべきかで迷い、ストレスを感じることになる。

倫理感が確立されていない従業員などは、不正やその行為者に対する対処が不十分で放置されていると、不正というのはその程度の軽微なものであると思い込み、自らも不正に手を染めてしまう可能性がある。

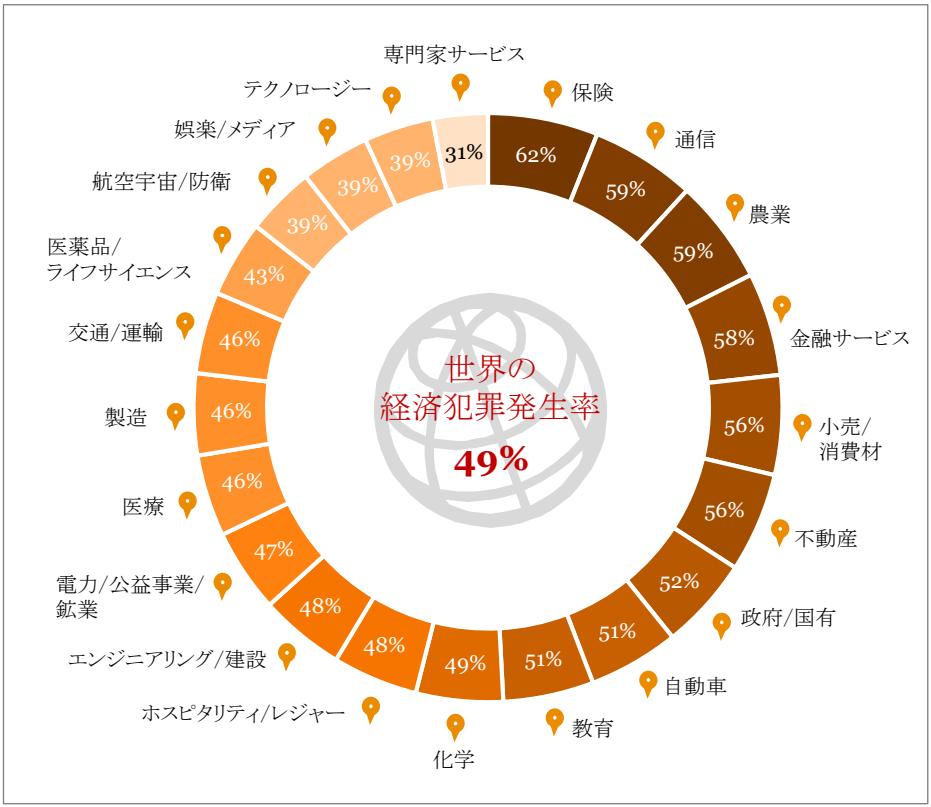
経済犯罪事象の調査及び対応費用：世界とタイの比較



不正調査には人的にも金銭的にもコストがかかるが、しっかりと実施することが肝要である。もちろん調査の結果、資産または費用を回収できる場合もあるが、最も重要なのは、犯罪規模の大小に関わらず、その事象からの教訓を得ると共に、根本的な原因を把握し、統制環境および内部統制を強化することで、将来に向けての被害の縮小、防止につなげることである。

世界的には、過去2年間で不正を経験した回答者の46%が、被害額と同程度または、それ以上の調査費用がかかったと回答している。一方、タイではわずか17%に留まっている。これは、不正発生時の対処法として、世界的には、公平な第三者調査機関を活用することが一般的であるのに対して、タイ国内では専門家による本格的調査というのが、まだ浸透しきっていない可能性がある。また、タイでは32%が費用対効果について分からないと回答しており、被害額の算出や調査費用への意識が低いという特徴も見られた。尚、10倍以上の金額を支払ったと答えた回答者は1%、2~3倍の金額を支払ったと答えた回答者は10%となっている。

業界別・世界の経済犯罪発生率



第2章
経済犯罪・不正を知る

経済犯罪や不正は、常に身の回りに潜んでおり、財務的・非財務的の両面において企業活動に多大な影響を与えている。それらのリスクと対峙するためには、まず、どのような経済犯罪・不正が発生しているかを知ることが重要である。

資産の横領

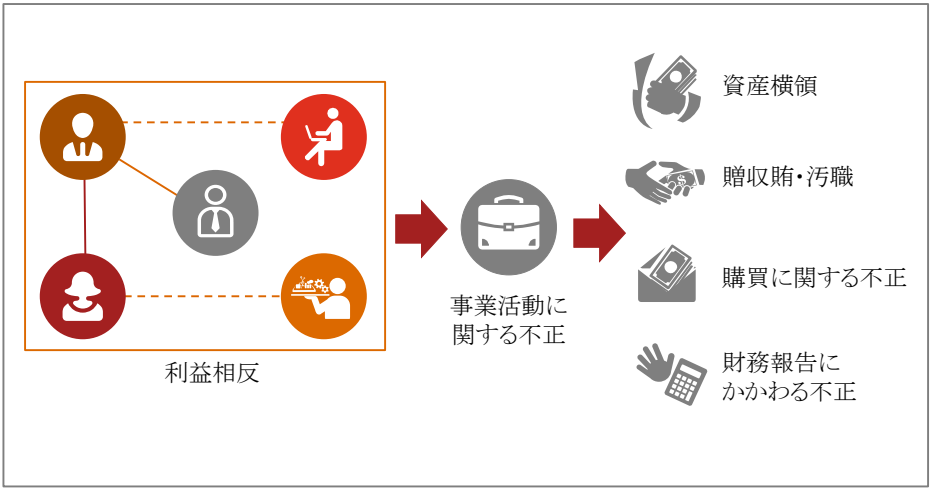
タイで最も一般的な不正は資産の横領であり、回答者の62%が過去2年間に被害を受けたと答えている。当該数値は、2016年の調査結果の78%から62%に減少しているが、世界全体の45%と比較すると高い数値になっている。その理由としては、タイの産業構造上、原材料などの有価資産を敷地内に有する製造業が多く、同業界からの回答者が大半を占めることに起因すると考えられる。それと関係してか、最も深刻な被害をもたらした不正として資産の横領を挙げた回答者も27%と最も多く、モノをとるという原始的な不正が依然としてタイにおける大きなリスクになっていることが分かる。

事業活動に関する不適切な行為

事業活動に関する不適切な行為とは、タイムシートへの虚偽記入や友好関係にある当事者への便宜等の様々な不適切な行為を指し、2018年の本調査から新たに回答項目に加えられた不正の種類である。そして、この種の不適切行為は、贈収賄、資産の横領、財務報告不正、購買に関する不正など、より深刻な不正の発生の兆候となる場合が多い。

そして、本調査の結果、40%の回答者が過去2年間で事業活動に関する不適切な行為を経験したと回答しており、これは、世界平均の28%を大きく上回っており、同行為がタイ企業内で蔓延していることが伺える。その大きな理由として、タイの文化的背景や倫理観の未熟性があり、それを律する行動規範や不正防止関連規定が不在である場合、善悪の区別が不明瞭な状況のまま行われてしまっていることが多い。この点については、第4章で後述する。

タイにおいて最も目にする事業活動に関する古典的な不正行為の一つに、従業員やその縁故者の関連企業に便宜を図り取引をするという利益相反関係があり、多くのタイ企業において、その管理・統制が脆弱である。このような不適切行為は、見積価格の漏洩による不適切な業者選定や水増し発注などの購買不正につながっている。



購買に関する不正

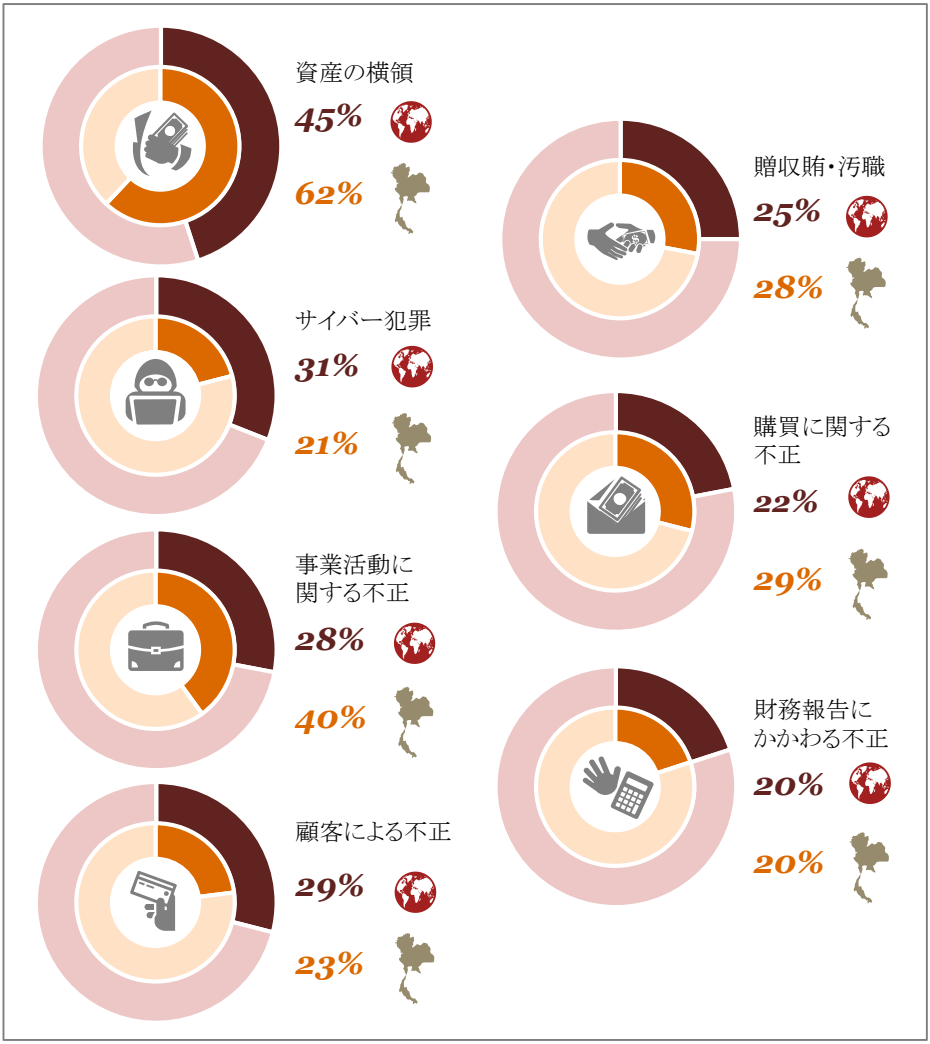
3番目に多い不正として挙げられたのが、29%が回答した購買に関する不正であり、2016年の18%から大きく増加している。この種の不正は、副資材や一般購買など、比較的に経営陣の目が届きにくい非製造プロセスにおける副資材、建設、IT、メンテナンス、一般購買において発生しやすい。実際、業者との共謀による水増し発注や架空発注などの相談が後を絶たない。

顧客による不正

顧客が、企業を欺く目的で働く不正行為であり、本調査によると、タイで23%、全世界で29%の回答者が、同不正の被害にあったと答えている。

顧客による不正には、住宅ローンやクレジットカードに関する不正など、会社の製品やサービスの不法な利用、またはそれらに関連する不正行為が含まれる。

企業が最も頻繁に経験する不正および経済犯罪：世界とタイの比較

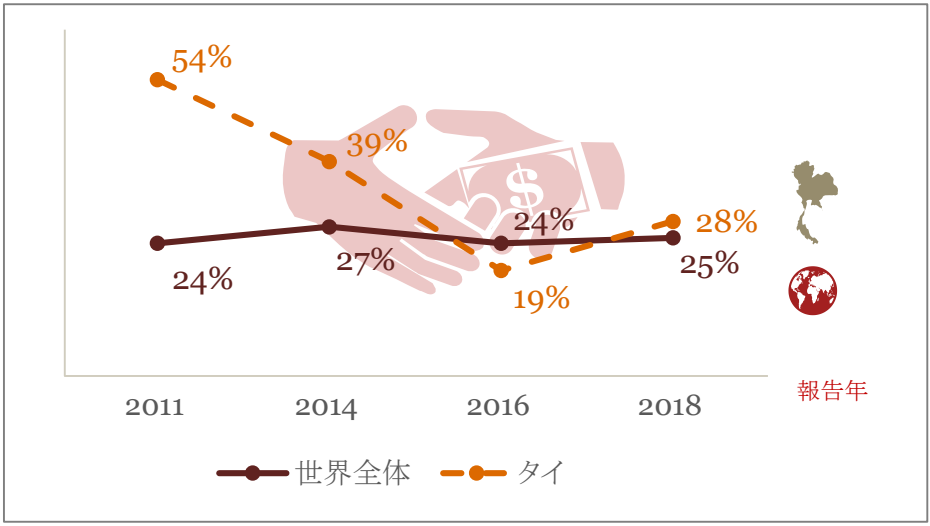


贈収賄・汚職

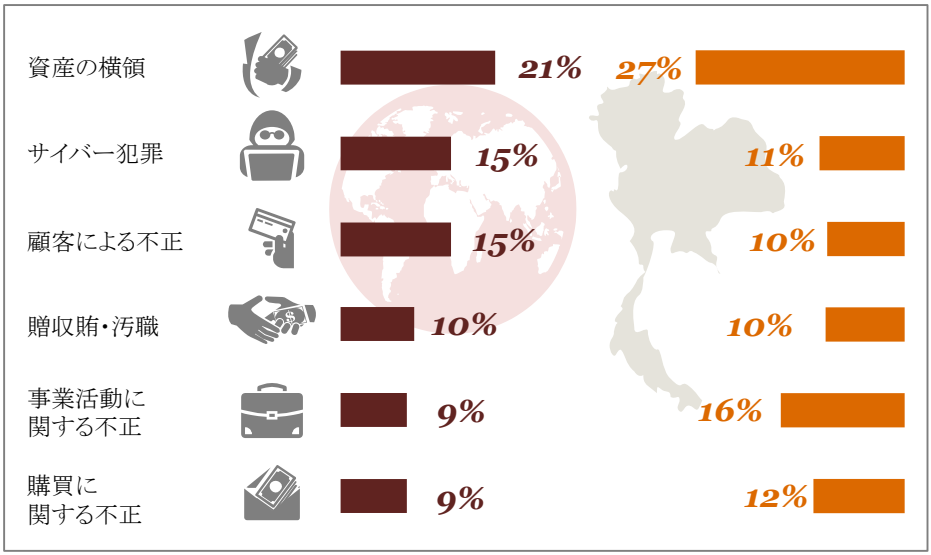
タイでは、依然として贈収賄と汚職が深刻な問題となっており、過去2年間にその影響を受けたと答えた回答者は4分の1を超えて（28%）いる。

近年、この問題は国家レベルでも認識が高まっており、タイ政府も民間と連携して反汚職・贈収賄に全力を挙げて取り組んでいる。2010年、民間企業における不正リスクに対する意識の向上並びに汚職・贈収賄を防止するためのポリシーやメカニズムの導入を目的に、民間団体であるタイ取締役協会（Thai Institute of Directors）は、反汚職集団的行動連合（Collective Action Coalition against Corruption"-CAC"）を設立した。また、2018年7月22日に、贈収賄規制に関する新法として、Act Supplementing the Constitution Relating to the Prevention and Suppression of Corruption B.E. 2561（2018）が施行された。主な改正点は、1）贈賄者の定義が外国法人に拡大、2）国家汚職防止委員会（National Anti-Corruption Commission（'NACC'））が他国の調査機関や司法機関と協力して調査出来る点である。

贈収賄・汚職を経験した企業の割合：世界とタイの比較



企業が経験した最も深刻な経済犯罪：
世界とタイの比較



サイバー犯罪

過去2年間にサイバー犯罪を経験したとの回答は21%であった。内、最も致命的な犯罪としてサイバー犯罪を挙げたタイの回答者はわずか11%であったものの、回答者の約3分の1（32%）が、サイバー犯罪は今後2年間で最も致命的な経済犯罪になるだろうと回答している。

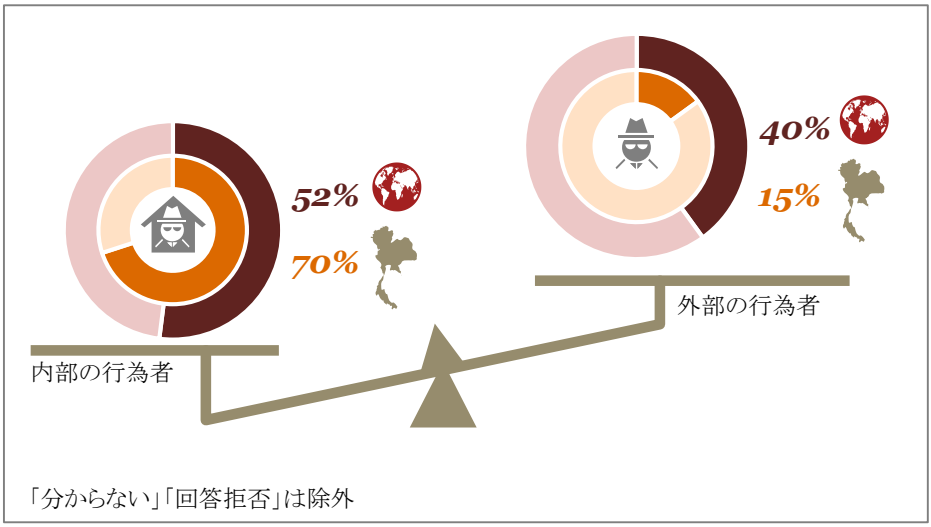
従来の資産の横領や購買不正、贈収賄に加えて、新たな脅威としてこれから企業に襲いかかってくる経済犯罪である。サイバー犯罪については、第3章にてより詳細に論じる。

不正行為者は必ずしも社内にいるわけではない

多くの企業が見逃してしまい盲点となりやすい点に、外部いわゆる第三者による不正がある。本調査の結果、タイにおける最も致命的な不正・経済犯罪の70%が内部による犯行であり、外部者によるものは15%に留まっている。一方で、世界的に見ると、外部者による犯行が40%と、必ずしも内部の不正行為者による犯行だけではないことが見て取れる。それら外部不正行為者の属性は、ハッカーが50%(世界平均は31%)、顧客が42%(世界平均は39%)、サプライヤー、代理店、仲介業者などの取引先が33%(世界平均は29%)、組織犯罪が28%(世界平均は22%)となっており、前述したサイバー犯罪や購買周りおよび顧客による不正などが脅威となっていることが分かる。

経済犯罪、企業のリスクという観点では、パートナーを知る、取引先を知るというのは非常に重要である。例えば、贈収賄は自身で賄賂を支払っていなくても、代理店やコンサルタントが支払っていれば企業の責任となる。また、関税における輸出規制においても、販売先の実態、販売した製品・材料の使途を知らなければ課徴金対象となってしまう可能性もある。

最も致命的な経済犯罪の主な不正行為者:世界とタイの比較



「分からない」「回答拒否」は除外

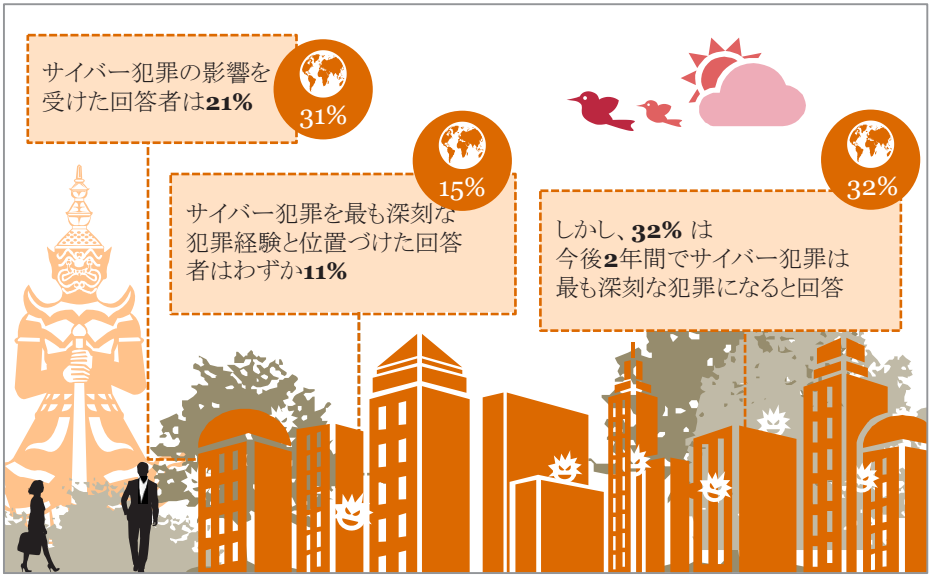
第3章

迫り来るサイバーリスク
ー見えない脅威

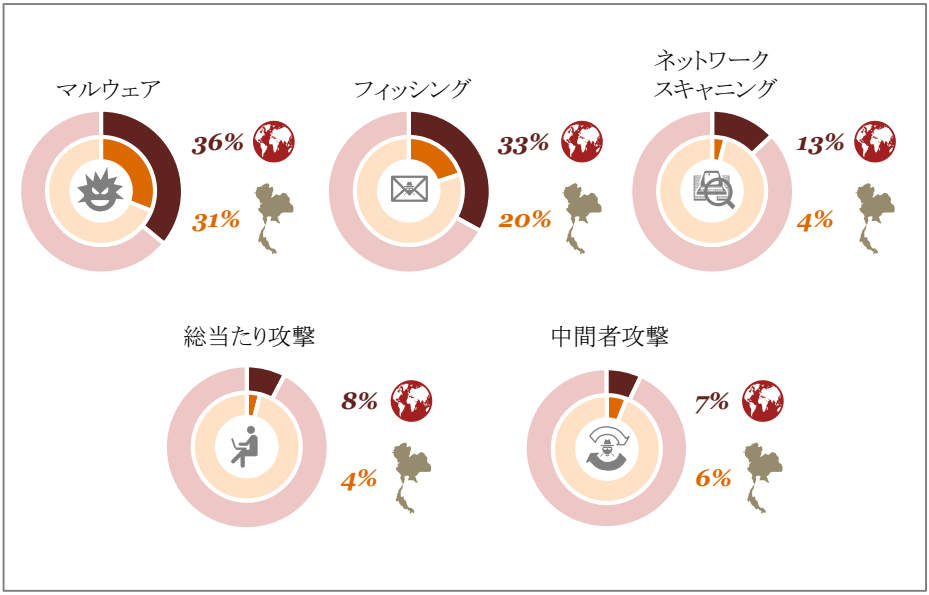
タイにおいて、過去24カ月間にサイバー被害を受けたと答えた回答者は約5人に1人（21%）いたものの、サイバー犯罪が最も致命的な不正であると答えたのは約10人に1人（11%）に留まっている。一方で、回答者の約3分の1（32%）は、サイバー犯罪が今後2年間で最も深刻な犯罪になると予測している。

世界中で、サイバー攻撃被害の報告は年々増加しており、今最も注視すべき経済犯罪の一つである。それはタイも例外ではない。実際に国家レベルでの「Thailand 4.0」の推進により、多くの在タイ企業が、業務のデジタル化、クラウドソリューションの活用など、業務モデルの変革に取り組んでおり、サイバーリスクへの対応が喫緊の課題となり、今後の最大の懸念となっている。

サイバー犯罪の経験と将来的な懸念：
世界とタイの比較

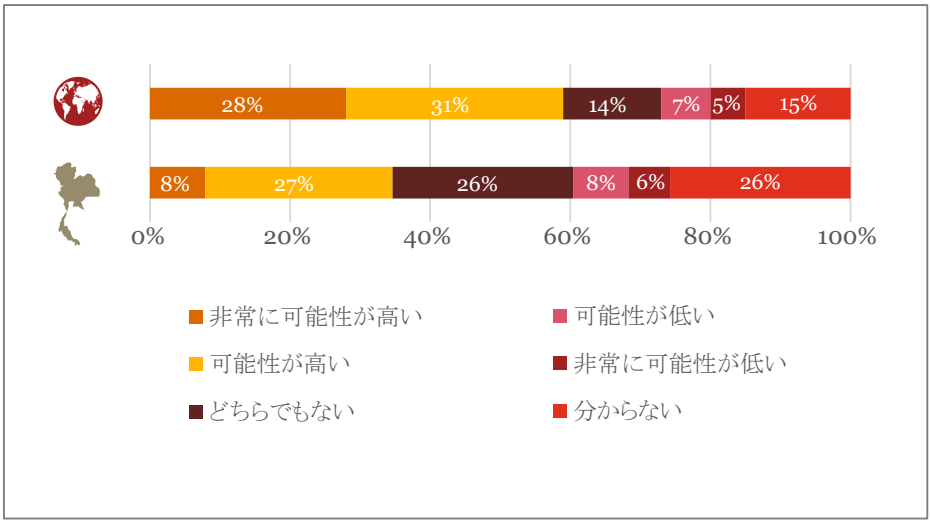


最も報告件数の多いサイバー攻撃：世界とタイの比較



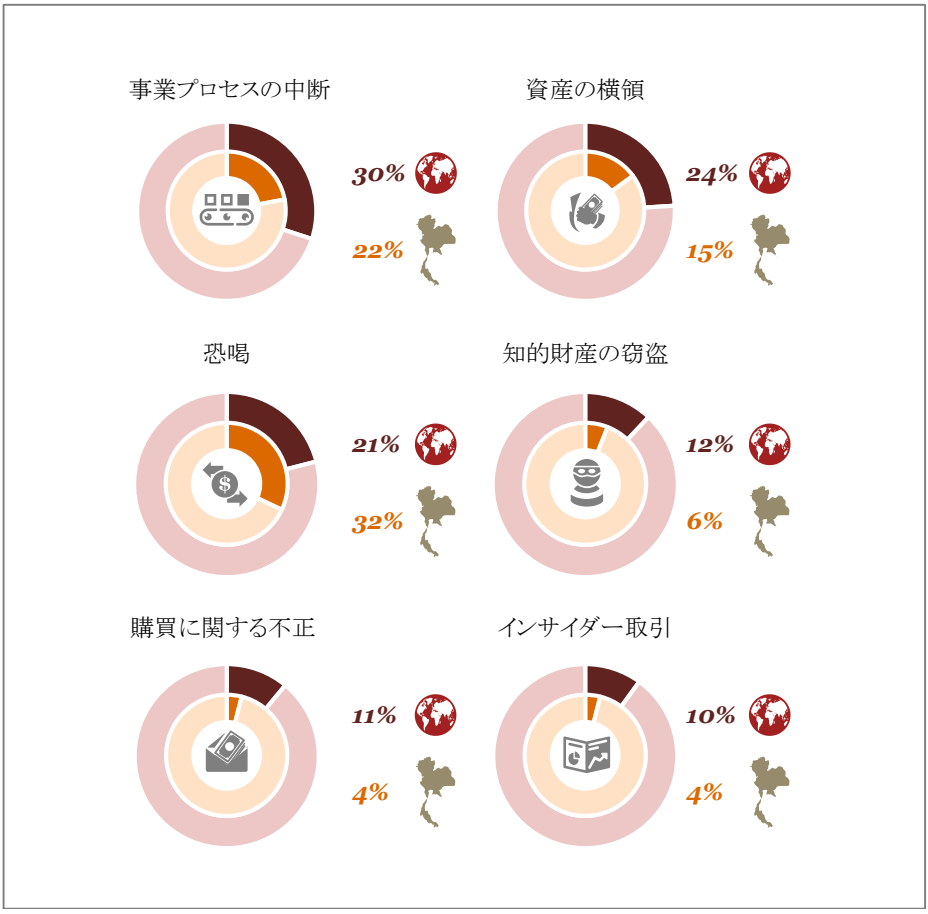
近年、タイ国内においても、サイバー攻撃に関する相談が増加しているが、そのほとんどが、マルウェア感染による情報流出とその情報に基づく、取引先や社内の上長からのなりすましメールによる被害である。本調査においても、最も報告件数の多い攻撃手法としてマルウェア（31%）が挙がっており、続いてフィッシングメール被害（20%）となっている。

サイバー攻撃情報を政府または法執行機関と共有する可能性
– 世界とタイの比較



サイバー攻撃を受けたまたはその疑いがある際に、その情報を政府や法執行機関と共有するか否かとの問いに対して、世界平均では約6割が高い可能性で情報共有すると回答している一方、タイではわずかに35%に留まっている。情報共有するか分からない、または可能性が低いと回答した者の理由として、無秩序に情報が公開され、自社の信頼性や評判が損なわれる懸念があるとの回答が最も多くなっている。

サイバー攻撃の標的となった不正および犯罪の種類
－ 世界とタイの比較



現代のデジタル不正の主な特徴と課題

デジタル化は、新たな攻撃対象を生み出している

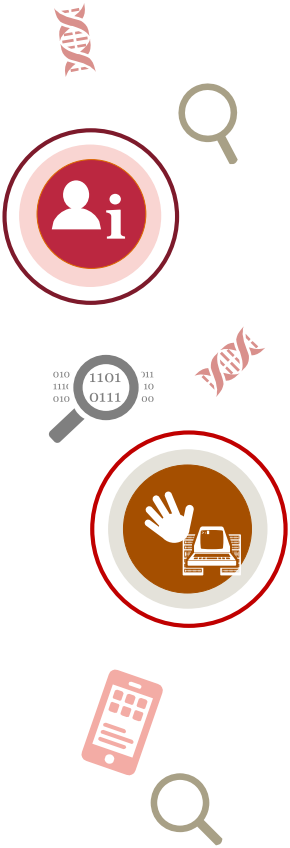
企業は従来、製品を市場に提供するにあたり、既に確立したB2Bプロセス（再販業者、流通業者、小売業者）を介して行っていた。近年拡大しているB2Cデジタルプラットフォーム等によって、不正行為者による攻撃対象が拡大している。

業界の境界線が曖昧に

昨今、非金融サービス企業が、電子決済システム事業等に進出をしている。従来の金融サービス企業は不正やマネーロンダリング防止のための先進的な技術や管理態勢を有している一方、こうした比較的新しい参入企業には、蓄積された経験やノウハウが欠けているため、不正リスクや規制リスクの影響を受けやすい状況にある。

不正行為者の技術の進化が止まらない

サイバー攻撃はますます高度化し、徹底的かつ破壊的になっている。2017年には、たった一つのランサムウェアが、英国の国民健康保険サービスを麻痺させ、人命を危険にさらした。また、2016年には、不正行為者がSWIFT口座（他の銀行との間で毎日何十億ドルもの金額をやり取りするためにあらゆる銀行が利用している国際送金システム）を機能停止にし、バングラデシュ中央銀行から1億米ドル近くを盗んだ事件も起きている。



クレジットカード番号を変更することはできても、生年月日を変えることはできない

不正管理に長く使用されてきたナレッジベースの認証ツールはもはや時代遅れになっており、新たな手法－デジタルIDや顔・音声認証－等が顧客資産の保護に必要とされている。しかし、大部分の企業はまだそれらの採用に至っていない。もし、政府機関や大企業等のセキュリティが破られた場合、盗まれるのは必ずしも現金などの代替可能な資産ではなく、生年月日や国民識別番号などの個人情報である。これはまさしく多くのナレッジベースの認証ツールが個人認証や不正防止に用いているデータそのものであり、このようなサイバー攻撃により個人IDが乗っ取られてしまう可能性がある。

いったん侵入を許すと、いつ攻撃を受けるか分からない

常に外部からの脅威に注意を払うことがサイバー攻撃を防止する鍵であることに議論の余地はない。しかし、新たな侵入だけを警戒するだけでは不十分である。APT（Advanced Persistent Threat）攻撃型マルウェアは、政府および企業のITシステムや各端末内に、監視ソフトウェアの目をかい潜り、検出や削除されることなく潜む特性を持っている。そして、知らず知らずのうち拡散し、継続的な攻撃を仕掛けたり、または、期が熟すのを待ち、結果的に多大な損失を及ぼす可能性がある。

それでは今何ができるか

タイでは、サイバー攻撃に特化したモニタリングツール、または全社的な監視プログラムの一部としてテクノロジーを利用していると答えた回答者は61%と、世界平均の72%を下回っている。

サイバーセキュリティ態勢を構築することは、全ての組織にとって必要不可欠である。これは単に新たなテクノロジーソリューションを導入することだけを意味しているのではなく、サイバー人材育成、プロセスの導入、明確なガバナンス等、包括的に態勢強化していく必要がある。組織規模が小さく、こうした取り組みに十分なリソースを確保するのが困難な企業は、外部の専門会社にアウトソースすることを検討すべきである。専門リソースを活用することで、サイバー脅威の評価、監視、発見、対応、是正の仕組みを比較的容易に確立することが出来る。最も重要なのは、仮にサイバー犯罪事象が発生した際に、内外のリソースの如何に拘らず、迅速に対応出来るよう万全な準備をしていることである。

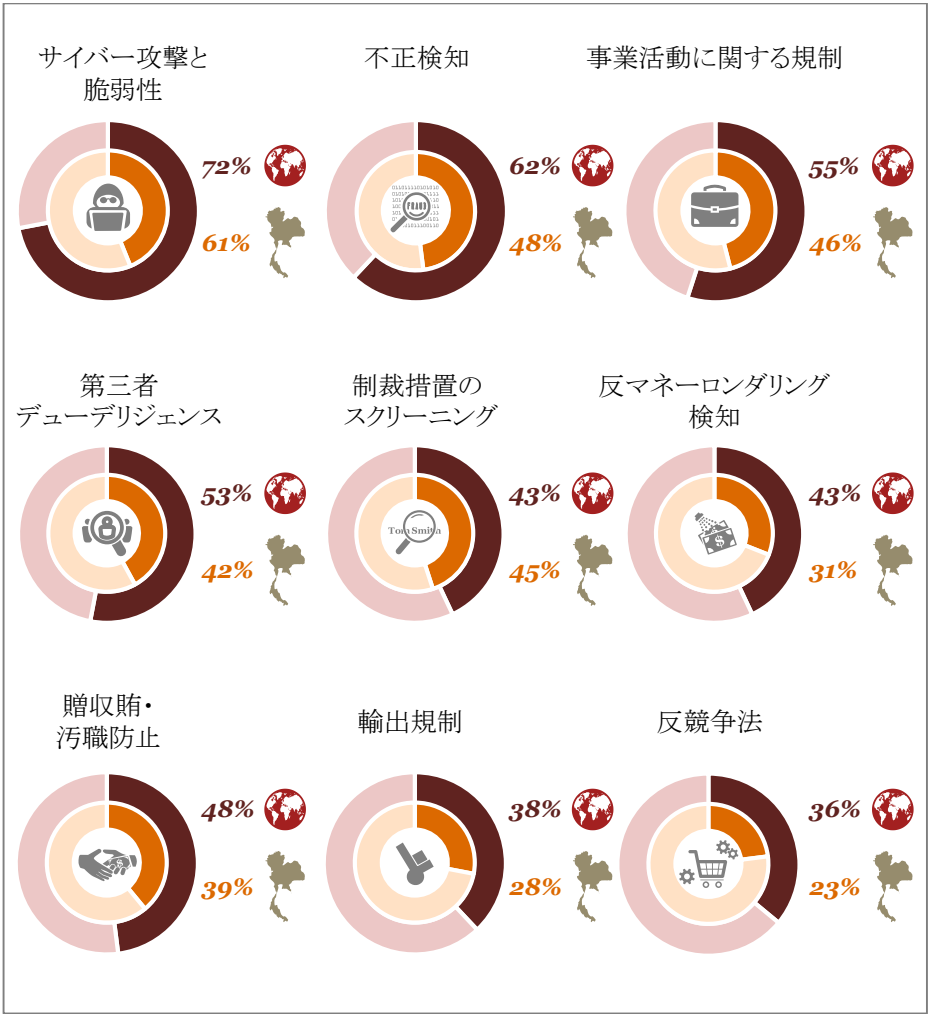
サイバーリスクを知る

サイバーリスク耐性を強化するためにまず最初にすべきことは、現状を知ることである。セキュリティ規定等の統制環境が整備されているか、アプリケーションやネットワークセキュリティーは十分か、サイバー人材や教育はされているか、それを判断するためにITサイバーリスクアセスメントを実施することが必要である。そして、いわゆるサイバーセキュリティプログラム（CSP）を導入・運用していくことになる。

タイ国内では、社内でCSPを整備し、運用していると答えた回答者は46%であった。これは2016年の26%から大幅に増加しているものの、世界全体の59%と比較すると遅れをとっている。しかしながら、回答者の10%は、CSP自体は策定したものの実際の導入に至ってない、16%は導入可能性について評価中であると答えている。

また、プログラムを策定していないまたはあるかどうかわからないと回答したのがそれぞれ7%と21%であり、全体の約3割でCSPの整備が全く進んでいないという結果になっている。

不正や経済犯罪の監視手段としてのテクノロジーの活用状況
– 世界とタイの比較



人材を配置する

マルウェアが添付されているメールがたった一通あれば、企業内部に入り込み、ネットワーク中に拡散し、業務を混乱させることや事業上の機密データを盗むことが出来るこの時代、いかに優れたCSPが整備されていても、しっかり運用されておらず、有事の際に迅速な対応ができるよう組織に浸透していなければ意味がない。

特にサイバー人材の確保および育成が非常に重要である。CSPのみ整備し、経験豊富な情報セキュリティマネージャーおよび専門チームがいないということは、小学生が専門書を持っているようなものである。

タイ国内では、最高情報セキュリティ責任者（CISO）がいると答えたのはわずか16%であり、世界全体（38%）の半分にも満たない。さらに、私共の経験から、例えCISOまたは同様の役職名を名乗っていたとしても、組織内の立場上、経営幹部レベルではなく、取締役会や経営陣への報告ラインを持たない場合も多く、サイバー人材が必ずしも戦略的に配置されていない場合も多い。

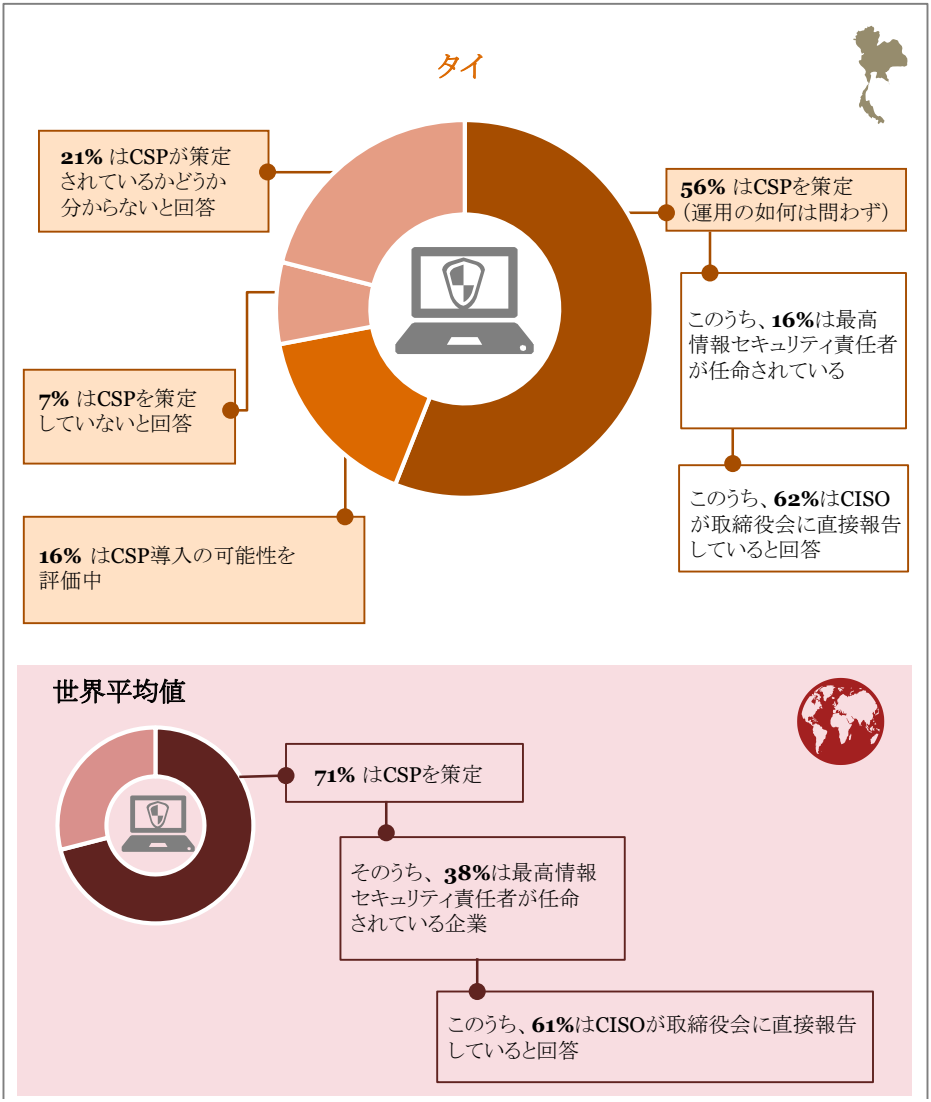
サイバーインシデントへの対応策を理解する

CSPにおいて効果的な発見・防止・対応のサイクルを回すためには、定期的にテストを実施し、有事に備えることが重要である。特に、サイバーインシデント対応計画に即した定期的な訓練をすることで、実際にサイバー攻撃を受けてセキュリティが突破された際に、慌てて混乱することなく迅速かつ適切な対応を行えるようになる。そして、結果的に初期被害を最小限に抑え、二次被害の抑制にもつながるのである。

全従業員への教育

最後に、おそらく最も重要な要素になるが、従業員への教育が、プログラムや技術と同様に非常に大切である。多くのサイバー攻撃が、従業員のちょっとした注意や意識の欠如によって発生したり、被害の範囲が拡大している。例えば、見知らぬ相手からのメールの添付ファイルを開いてしまったり、なりすましメールに反応して多額の支払いをしてしまったり等である。したがって、企業は、社内ネットワークを利用する全ての従業員に対して定期的な研修を行い、サイバー攻撃に対する認識を高める必要がある。また、経営陣は、サイバー攻撃シミュレーション研修等の、有事対応の訓練も受けることを推奨する。

サイバーセキュリティプログラムの有無：
世界とタイの比較



第4章

不正のトライアングル
－企業文化の醸成が
不正を抑制する

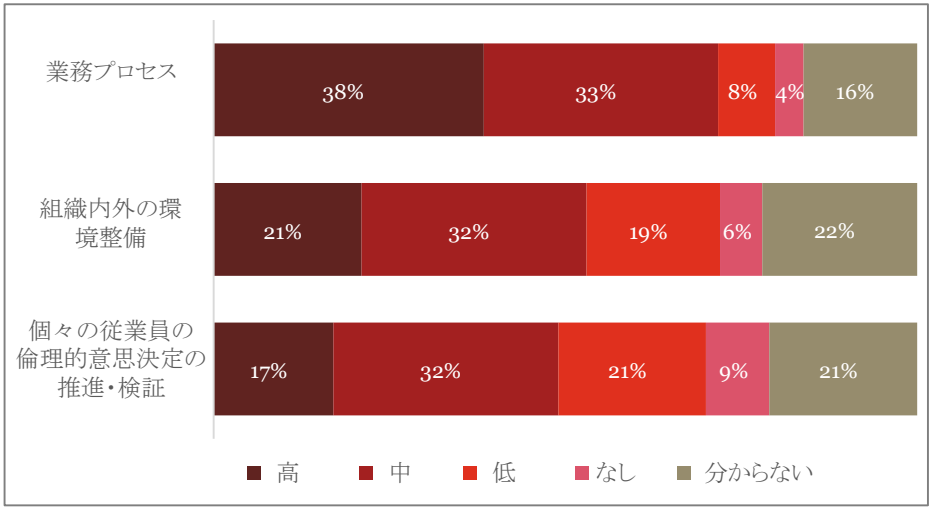
不正防止効果を最大化するためには企業文化や従業員の倫理意識向上への投資が欠かせない。

不正リスクを効果的に抑制するためには、業務プロセス改善やテクノロジーへの投資に加えて、社内環境の整備や企業文化の醸成、ならびに従業員の能力および意識向上への投資を合わせて行う必要がある。本調査の結果、一部の企業では全体的な投資を行っているものの、やはり業務プロセス改善、いわゆる内部統制の強化という効果が分かりやすい領域での取り組みに偏ってしまっていることが見て取れる。

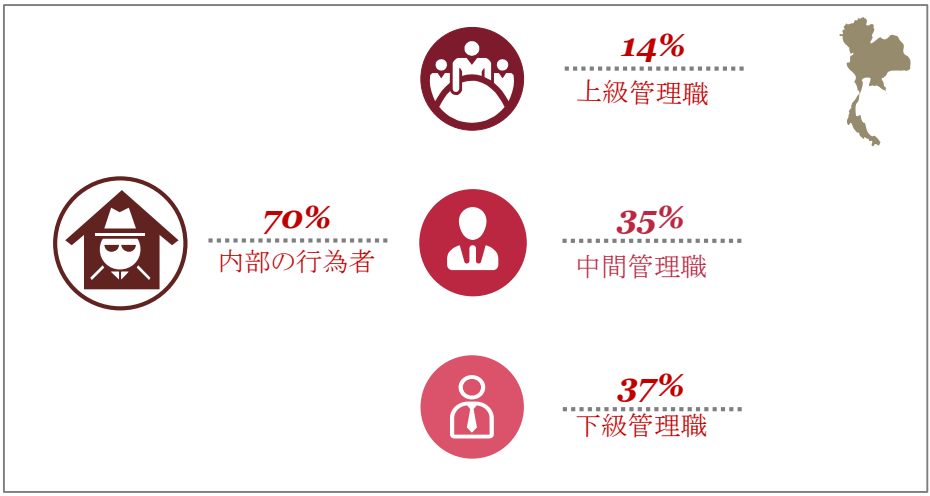
不正や経済犯罪に対応するために実施している取り組みとして、回答者の71%が、内部統制などの業務プロセスの構築に一定度以上の努力をしていると答えている。しかしながら、経営者の姿勢や文化醸成等を含む組織内外の環境整備や研修・教育等の従業員の倫理観向上への施策に取り組んでいるのは50%程度にとどまっている。内、積極的に取り組んでいるのはわずかに全体の20%程度である。

また、業務プロセスへの取り組みでに関しても、世界平均の83%より低くなっており、タイ国内の多くの企業にとって、社内施策への取り組み余地が十分にあると言える。

社内の不正や経済犯罪と闘うための取り組み



タイにおける不正・経済犯罪の主犯格の職階内訳



前述の通り、過去2年間に経済犯罪を経験したタイの回答者の70%が、最も深刻な経済犯罪は内部の行為者による犯行であると答えており、外部者による犯行は15%に過ぎなかった。世界的には、内部による犯行が52%、外部犯行が40%と内外の不正行為者の割合は拮抗しており、タイにおける内部犯行の多さが際立っている。これは内部環境の整備が未だ整っていないことを示唆する結果となっている。

まずは、不正を断固として許さない(zero-tolerance-for-fraud)企業文化を創り上げるための環境整備および人材教育へ優先的に投資していくことが必要である。不正の存在は、従業員の士気・モラルに多大な影響を与える。しかし、逆を言えば、適切な企業文化に支えられることによって、従業員は不正防止に大きな役割を果たすことができるのである。

業務プロセスや内部統制強化のみならず、人や企業文化への投資の重要性を理解するためには、経済犯罪や不正の発生原因を理解する必要がある。不正は、条件と動機が複雑に絡み合った結果発生するものであり、決して、業務プロセス、内部統制の強化のみによって防止されるものではない。

不正は、人が判断し、意思決定することによって起こるものである。したがって、人間の行動に焦点を当てることが、不正の防止、抑制につながる。倫理的な意思決定を促す環境整備など、人に関する取り組みに投資することによって、統制強化や検出のためのテクノロジーへの投資効果が高まるのである。

不正のトライアングル

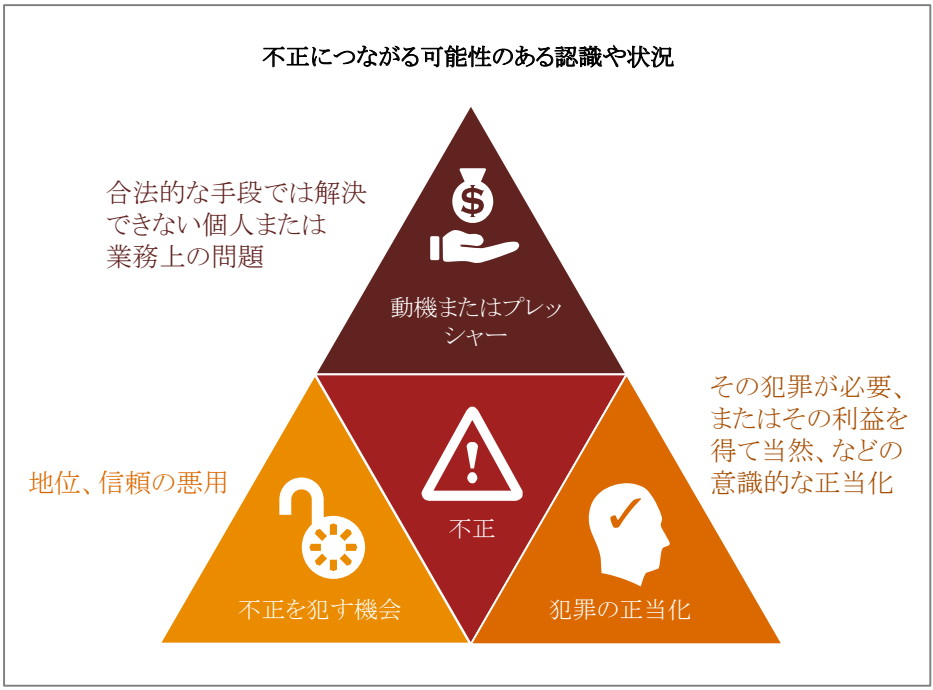
不正を防止するためには、まず不正の発生要因を理解することが重要であり、そのための理論として不正のトライアングルというものがある。不正のトライアングルは、不正を働く「動機またはプレッシャー」、不正を可能にする 「機会」、不正行為そのものの「正当化」という三つの要素から構成されており、これら三つの要因が全てそろって初めて不正が発生すると定義している。この理論は、不正につながる人間の行動や認識を理解し、防止策を策定するために非常に有用である。

まず、プレッシャーや動機であるが、これは従業員の個人的な金銭需要の場合もあれば、業績や評価への過度のプレッシャーなど様々であり、職階やポジションに限らず個々の事情を抱えていることが多い。例えば、管理職や営業職が業績達成へのプレッシャーから数字を改ざんする場合もあれば、エンジニアが品質問題を報告しない場合もある。これらは、自己の責任逃れという場合もあれば、会社のためにという歪んだ責任感の場合もある。もちろん、個人的な金銭的需要で言えば、ギャンブル、医療費、麻薬、女性関係など、人それぞれで挙げればきりがない。他には、人事評価制度や報酬への不満や不公平感などの要因も挙げられる。

しかし、動機は必ずしも金銭的なものや業務上のプレッシャーだけではなく、文化的な要因に帰することもある。タイでは、過ちを認めることを恐れたり、屈辱だと捉える文化的な特徴がある。そして、最初についた小さな嘘を隠すためにさらに、不正を重ねていき、やがて大きな嘘となり重大な不正になってしまうことも少なくない。

次に、不正行為の実行を許してしまう機会の有無であるが、これはいわゆる内部統制である。

内部統制の強化など業務プロセスの向上に対して、一定度以上の努力を払っていると答えた回答者が71%に達することから分かるように、不正防止のための努力および施策の大部分は、不正のトライアングルの三つの要因のうち、不正を犯す「機会」をなくすために費やされてきた。



業務プロセスの改善や新しい技術の導入による内部統制の強化は、不正を防止する観点から最重要な要素の一つであることは疑いの余地もない。しかし、内部統制を強化したことで、自社の不正防止策として満足してしまうケースも多い。内部統制は、経営陣を含む権限者が、倫理的に行動し業務手順に厳密に従うという前提に基づいている。そして、その最大の弱点は、悪意を持つ者による共謀（従業員間の場合や従業員と第三者間による場合もあり）や権限者による越権行為があった場合に、無効化されてしまうことである。

実際、上級または中間管理職による不正は、2016年の34%から49%へと大幅（約50%）に増加している。こうした根本的かつ構造的な問題を克服するには、前述の動機やプレッシャーなどの根本的な要因の解決を図るとともに、経営陣による内部統制の越権行為や共謀が発生する可能性を考慮した上で、そのリスクを最大限抑制するような包括的な不正防止態勢を構築する必要がある。

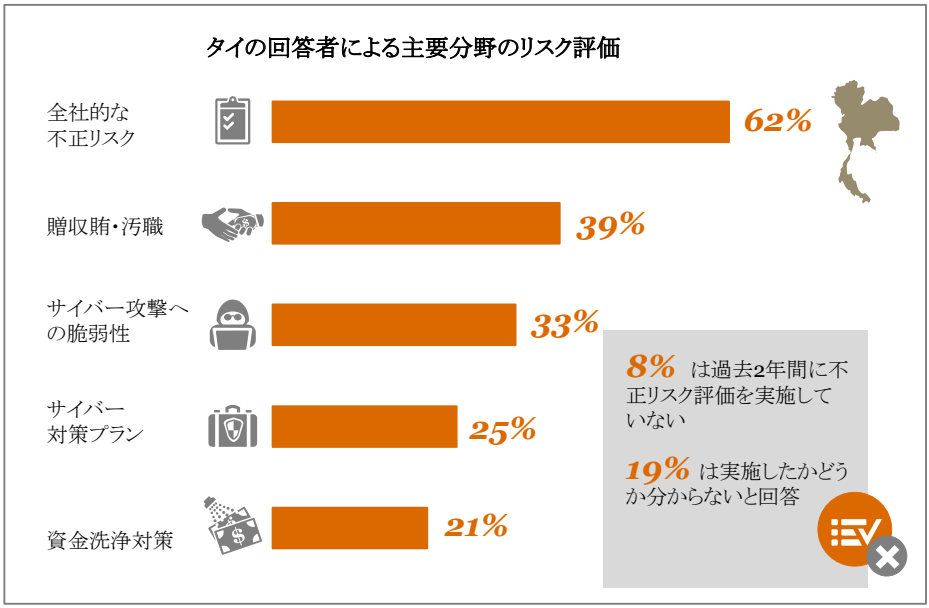
最後に、不正行為者が（多くの場合、自己の個人的な倫理観と折り合いをつけることによって）自ら犯した行為に対して言い訳をする、自己の正当化である。

不正行為を働いた者は、しばしば、その行為が誰かを傷つけた訳ではない、また会社のためや誰かのために行ったものである等と、自分自身を納得させている。また、その行為自体が、見つからないだろう、また、発見されそうになったとしても大事になる前に解決できると信じている場合も多い。

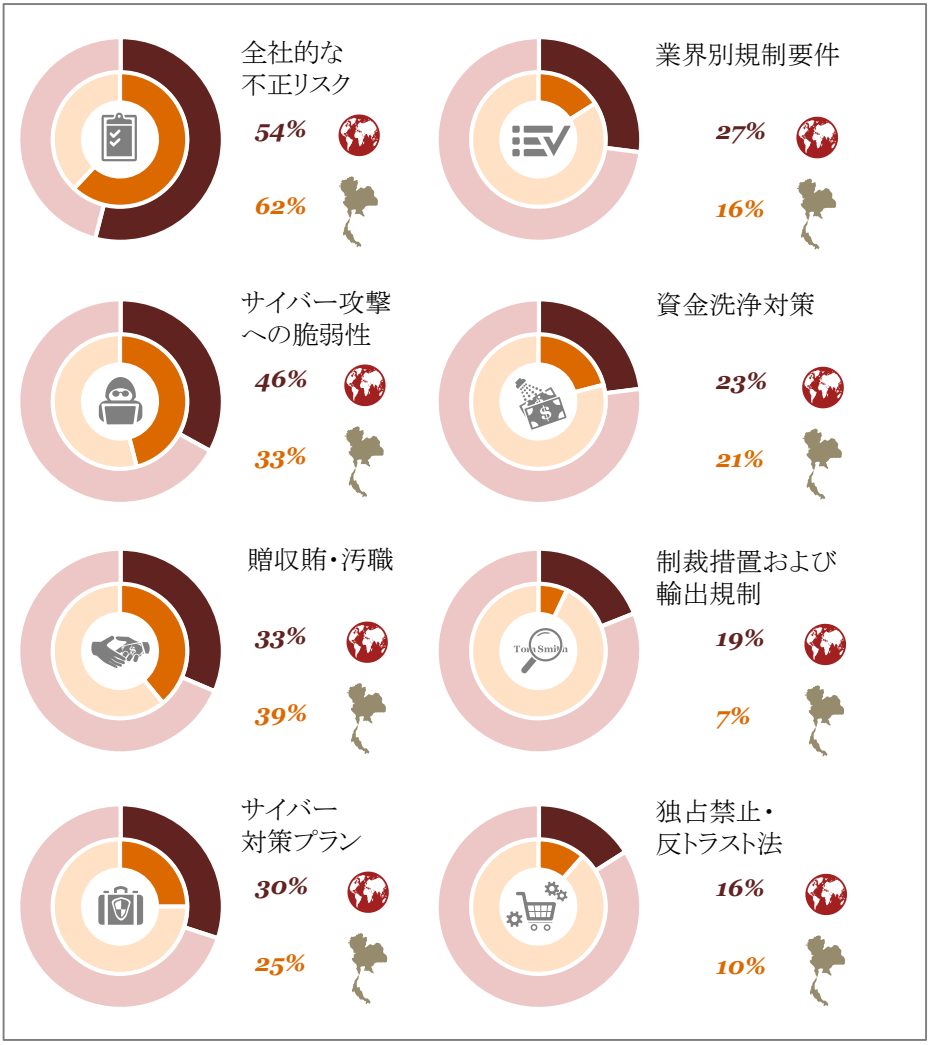
どう対応すべきなのか

それでは、その不正のトライアングルが示す不正の要素に対してどのように対応すべきなのか。その第一歩は、組織の不正リスクを事前に評価し、自社が抱える脆弱性を理解することである。これにより、想定される不正スキームを特定して、それから初めて、あるべき統制環境や統制活動を検討すべきである。

しかし、必ずしもすべての企業が、不正リスク評価を実行しているわけではない。本調査によると、過去2年間に全社的な不正リスク評価を実施したのは、回答者の62%であり、贈収賄・汚職防止の重要分野では39%、サイバー攻撃に対する脆弱性に対しては33%であった。また、過去2年間に一度も不正リスク評価を行わなかったと答えた回答者は、8%となっている。

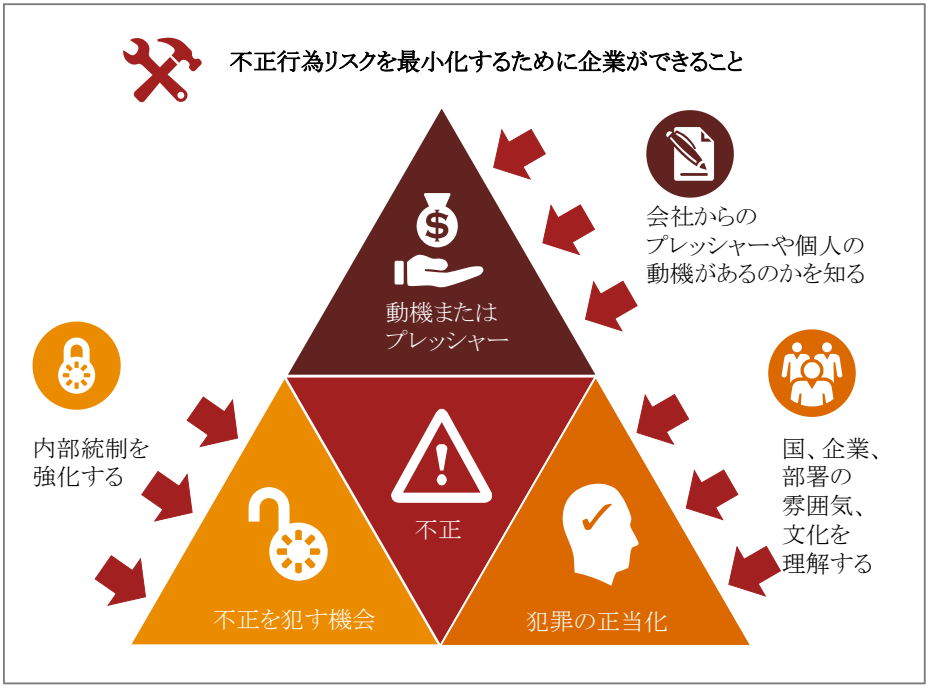


リスク評価を実施した分野：世界とタイの比較



まずは、上司部下の関係など社内的なプレッシャーや動機付けるものがないか、または従業員が抱えている問題等について知ることが重要である。この機会に、以下のような質問を自身に問いかけてみよう。従業員は精神的なプレッシャーを抱えていないか。それらのプレッシャーは社内規則、法規制に反していないか。顧客・取引先や社員の正しい行動につながる行為か。部下は個人的な問題を抱えていないか。

そして、不正の正当化の主因となる従業員の倫理観を形成する企業文化についても理解する必要がある。ここでも、改めて、経営者が、不正を許容しない姿勢を従業員に伝えているか、不正行為を見過ごしていないか、不正行為者に対する適切な対処がなされているか、コンプライアンスに関する研修がされているか等を自問してもらいたい。



また、自社の企業文化が従業員に影響を与えているかを知るためには、従業員との対話が必要である。まずは、主要なプロセスにおいて一程度の権限を有している従業員から始めるのが良いだろう。ワークショップやフォーカスグループ、または匿名アンケート等も活用して、より広範な従業員からの情報を収集するのも良い。

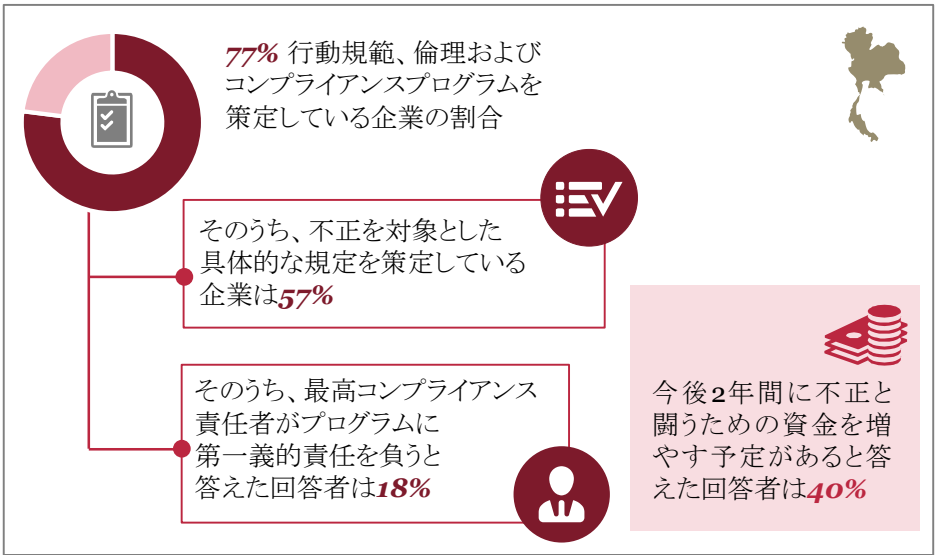
その活動過程において、容認できない行動とは何か、その結果どのような法的または社内規則上の罰則があるのか、そして周りの同僚や家族からどういう目で見られるのか等について、従業員がしっかりと理解していることを確認することが重要である。

タイ国内の企業においては、未だ明確な不正防止規定や行動規範を策定していないことが多いため、一部の従業員にとっては、不正の定義そのものが曖昧であり、それを正当化の理由に使われることもしばしばである。したがって、不正意識向上を目的としたコンプライアンス研修を実施し、それを定期的に繰り返すことで、不正行為の正当化や弁明の原因となる未成熟な倫理観を是正していくことが重要である。

また、行動規範や関連社内規定を理解し、遵守することを確認する誓約文書への定期的な署名を義務づけさせることでその理解と同意を担保することが出来る。このように、具体的なルールを定め、しっかりと教育をし、署名をさせるという一連の流れは、例えば、紹介手数料や謝礼を受け取ることを通常の権利として捉え何の疑問も持たないタイにおいては、特に重要である。さらに、コンプライアンス関連の文書は、監査証跡としても利用することができ、規則違反による懲罰や解雇の際に有用である。

しかし、行動規範およびコンプライアンスプログラムを策定・導入していると答えた回答者は、77%であり、その内、不正を対象とした具体的なポリシーを有しているとの回答は57%のみであった。タイにおける不正防止プログラムの標準化は未だ道半ばであると言えるであろう。

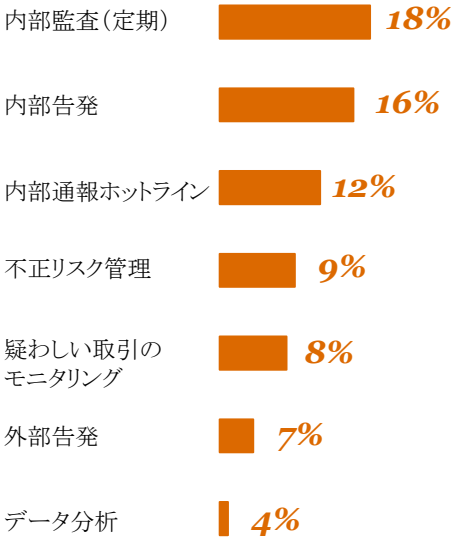
タイにおける倫理とコンプライアンス



不正は常に私たちの周りに存在しているが、不正を容認しない企業文化の醸成に投資することが、組織内部の不正リスクエクスポージャーの最小化を図る鍵になる。特に、既に内部統制の整備が進んでいる場合、この投資によるリターン効果は高い。

タイにおいては、過去2年間に発生した最も致命的な犯罪の35%は、内外部からの告発により発覚している。その内訳は、内部告発が16%、内部通報ホットラインが12%、外部告発が7%である。従って、従業員の不正に対する意識を向上し、かつ、適切な内外からの通報制度を整備することも、不正の防止および迅速な発見をする上で重要である。是非、内部統制の強化、内部監査プログラムの充実、モニタリングシステムなどの導入と併せて推進して行くことが望まれる。

最も致命的な不正や経済犯罪が発見された方法:タイ



今、問うべき質問

最近、不正リスクの評価を実施したか？
していない場合、それはなぜか？

自身の業界に関連する規制、コンプライアンス基準を把握しているか？

自社の行動規範やコンプライアンスプログラムは、不正を明示的に対象としているか？

従業員は精神的なプレッシャーを抱えていないか？それらのプレッシャーは社内規則、法規制に反していないか？それは、顧客・取引先や社員の正しい行動につながる行為か？

組織内部の不正を早期に発見するための内部通報ポリシーまたはホットラインが整備されているか？

潜在的な問題を把握するために、自社の企業文化を見直したことはあるか？また、問題を抱えている従業員はいないか？

第5章

テクノロジーの活用
ー高度な不正防止機能の導入と課題

ここ数十年の間、企業活動におけるほぼ全ての業務プロセスが新しいテクノロジーの導入によって劇的に変化してきた。それらテクノロジーは、業務プロセスを迅速かつ容易にし、かつ人為的ミスを軽減するのに大幅に貢献してきた。

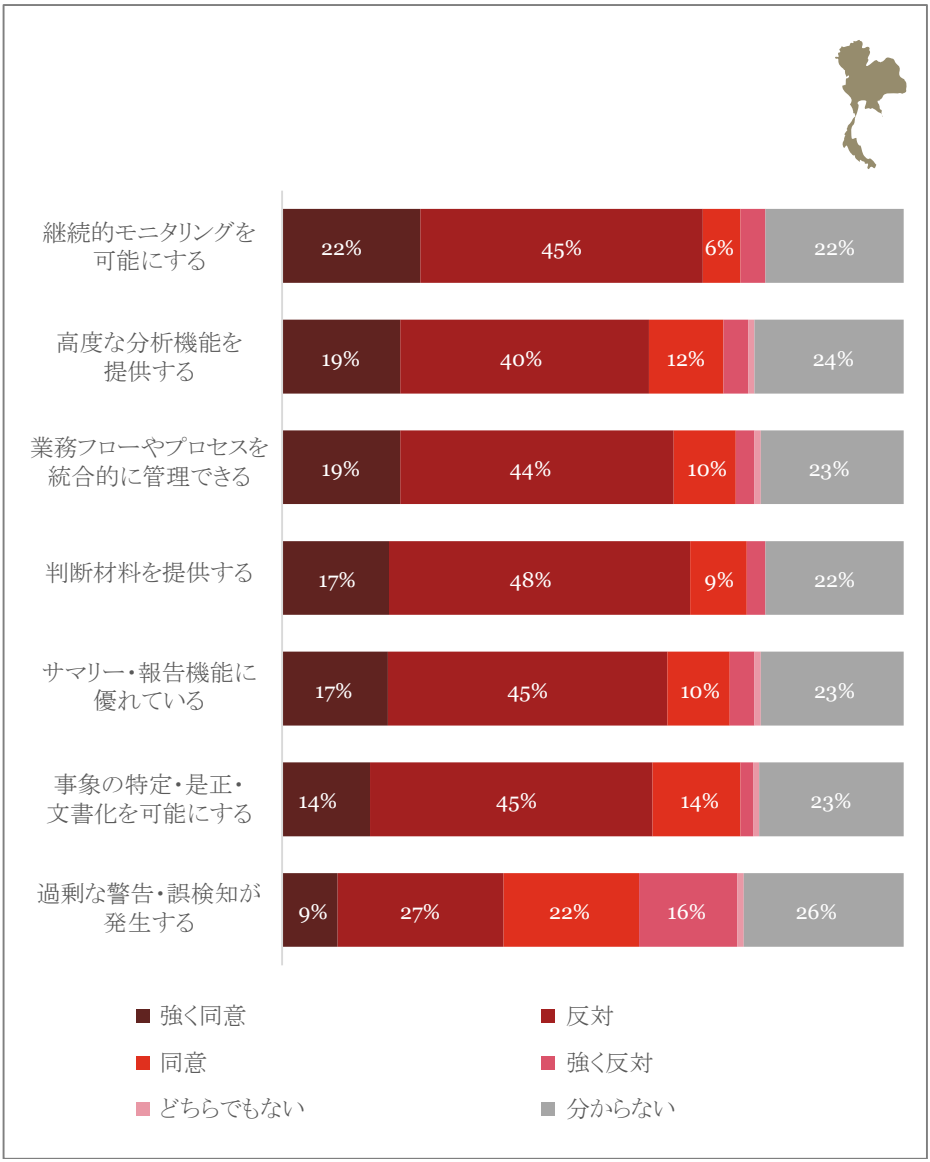
また、多くの不正や経済犯罪が何らかの形で記録上の痕跡に残ることを考えると、適切にテクノロジーを活用し管理している企業にとっては、証跡を追いやすく不正や経済犯罪に関する証拠を確保しやすいという利点もある。

しかし、タイの回答者の大半は、新たなテクノロジーの活用が不正の防止・発見プログラムを強化することを認めているものの、実際には約50%が、当該目的のためにテクノロジーを活用していない、または利用しているかどうか分からないと回答している。

一方で、単に新しいツールや技術を導入すれば良いわけではなく、いかに有効的に活用するかが非常に重要である。本調査によると、回答者の36%が、導入した不正検出システムまたはツールには過剰な警告や誤検出（false positive）が多いと回答している。この場合、不正検知機能の信頼性が損なわれるだけでなく、警告の重要性が失われ、人々が無視する原因になる可能性がある。

従って、企業は、活用するテクノロジーが適切に機能し、その投資効果を最大限に高めるよう、適切な人材を配置し、日々その効果を改善することが重要である。

不正・経済犯罪対応におけるテクノロジーの活用に関するタイ企業の認識



我々のタイ国内おける不正防止メカニズム構築サポートの経験からも、継続的な監査とテクノロジーを活用したモニタリングの両輪を並行して実施し、継続的なフィードバックを反映させる仕組みを構築させることが、誤検出を減らし、真の不正の兆候を判別するために必要であると実感している。不正検出のアルゴリズムやリスク指標を迅速に調整できるか否かは、日々進化する不正スキームに適応するために欠かせない機能である。このためには、まず、初期の不正リスク評価の結果によって、検出ルールの妥当性を検証し、その検出アルゴリズムを可能な限り精緻化していることが前提である。そして、最終的には予測モデリングや人工知能を駆使し、継続的監査で収集された各種フィードバックや過去の事象や取引のパターンからより高度な不正の兆候分析を行うことも不可能ではない。

不正への認識は高いものの技術への投資を含む不正防止態勢の構築で後れを取っているタイ国内の企業にとって、今がまさに国際水準まで高める過渡期にある。しかしながら、大規模なシステムやツールを購入し、全社的に採用するとなると多額な費用を要するし、どのテクノロジーを採用するかの選択も一筋縄でいくものではない。また、導入したとしても、最大限に活用できない場合もある。しかし、二の足を踏んでると、その間に手遅れになり、不正の被害が拡大してしまう可能性がある。

このように、水面下での不正および経済犯罪の蔓延に対する早急かつ有効的な対策への投資判断という課題に多くの企業が直面している。唯一の解答はないが、企業文化の構築、プロセスにおける内部統制の構築、テクノロジーを用いた統制および検出メカニズム、従業員の教育、内部通報制度の充実などの、様々な施策を検討し、効果、効率性と費用の適切なバランスを見極めて、絶えず進化する不正・経済犯罪と対峙することを真剣に考えることが求められている。

第6章
最後に

不正に備え、不正と正面から向き合い、より強固な組織へ

全てのタイ企業は、経済犯罪や不正という目の前にある脅威と対峙していかなければならない。そのための最善の方法は、目を光らせ、組織のあらゆる片隅にスポットライトを当て、不正行為者に狙われる穴、「盲点」がないかを見つけ出すことである。

本調査の結果からも、不正と対峙する姿勢・備えが必ずしも十分でないことは見えている。しかし、欠点を認識し是正することが出来れば、不正防止・検出防止態勢強化の大きな一歩となる。特に、日々変動するビジネス環境の中で形を変えながら襲い掛かってくる経済犯罪に対応するためには、従業員の意識を向上させ、倫理観の高い企業文化を醸成することが重要である。それによって、業績が良い時も悪い時も、より不正耐性の強い組織を造ることができる。

不正防止プログラムはその価値、投資効果を定量化しづらく、必ずしも社内における予算確保が容易ではないかもしれない。しかし、何も行動をとらず、脅威に身をさらし続けるコストは、財務的、法規制的、そして風評リスクという観点から見ても、重大なものになる可能性があるので、是非、全ての企業において、マネジメントによる陣頭指揮のもと、不正と戦う姿勢を打ち出していくことを期待したい。

お問い合わせ先

Vorapong Sutanont
Partner
Forensic Services, PwC Thailand
Tel: +66 (0) 2844 1000
Email: vorapong.sutanont@pwc.com（新）*
vorapong.sutanont@th.pwc.com（旧）

Eiichi Yoshikawa（吉川　英一）
Senior Manager
Forensic Services, PwC Thailand
Tel: +66 (0) 2844 1249
Email: eiichi.yoshikawa@pwc.com（新）*
eiichi.yoshikawa@th.pwc.com（旧）

*弊社は2018年12月17日に新Eメールアドレスに移行致します。
ご不便をおかけ致しますが、ご協力のほどよろしくお願い致します。

www.pwc.com/th