

PwC 世界経済犯罪 実態調査 2016 - タイ版 -







Contents

- 4 序文(ご挨拶)
- 6 タイにおける経済犯罪の実態
- 16 サイバー犯罪: 逼り寄る脅威
- 21 不正行為者とは
- 23 不正の検出方法
- 28 倫理とコンプライアンス
- 32 資金洗浄防止: アンチ・マネーロンダリング
- 42 求められる行動



序文(ご挨拶)



経済犯罪は、依然として、タイ国内で事業を展開する多くの企業にとって最大の脅威であり、対処しなくてはならない最重要な課題である。

この度発表しましたPwC世界経済犯罪実態調査2016年版の結果は、如何に不正がビジネスや国益を蝕み続けているかを物語っており、この不都合な事実に対して大きな警鐘を鳴らしています。

本調査の目的は、財政界のリーダーを始めとした、多くの皆様に対して、経済犯罪リスクが比較的に高いタイという国の年々複雑化する脅威の概観をお伝えすることであり、今までも同様に隔年で実施して参りました。

本調査の結果からも、4社に1社で不正が発生しており、経済犯罪は、依然として企業にとって重要な懸念事項であることが見て取れます。

また、約80%の不正は、企業内部に端を発しており、世界平均の46%と比べても高くなっています。これは、内部の人間に不正が行えてしまう環境があることの裏返しではないでしょうか。

不正の種類としては、資産の横領、サイバー犯罪、汚職・賄賂が最も多く、金額的には、購買不正やマネーロンダリングによる被害が大きくなっています。そして、それら不正の全てが、財務的な損害のみならず、従業員のモラルや風評に大きな影響を与えます。

タイでは、政府や民間団体が日々複雑化する不正リスクと戦う為の取り組みを強化しております。その中で、企業には、実行可能な計画を策定し、何をすべきかを明確にし、そしてこの難題に立ち向かう為に必要な人材・技術に投資することが求められています。

最後に、本調査にご協力いただきました皆様にはこの場を借りて心から御礼申し上げます。本調査の内容が、皆様が不正と戦う上で一助となりましたら幸いです。

Sira Intarakumthornchai
Chief Executive Officer, PwC Thailand



序文(ご挨拶)



タイにおけるPwC世界経済犯罪調査は250社を越す企業からの回答、その過半数は執行役員以上から直接ご回答を頂き、大きな成果を挙げることが出来ました。

この高い回答率は、皆様の多大なるご協力によるものであると同時に、より多くの企業が不正リスクについて真剣に考え始めているという事実の表れだとも感じております。タイにおける不正事案の件数は年々増加傾向にあり、その原因は、企業内部の防止・検出メカニズムの脆弱性にあるとも分かっております。例えば、東南アジアの中でも、タイは従業員が声を上げて会社を改善していくという文化・環境の醸成という点で大きく後れをとっています。従業員から効果的に情報を得るというのは、不正を早い段階で発見する上で非常に重要であり、有効的な通報プログラムを持たないということは、不正の兆候を見逃し、悪事を野放しにしているといっても過言ではないでしょう。

最近、特に金融業界では、サイバー犯罪による脅威が高まっています。成長著しいオンラインバンキングやeコマースビジネス等はその急速な成長に対して、会社のリスク管理体制が追いついておらず、その隙を突いて国内外の犯罪者が金融機関やその顧客を脅威に晒しています。銀行は、閉塞的な金融市場において、かつてない成長ならびにコスト削減へのプレッシャーを受けており、つい不正防止プログラム構築への投資を後回しにしているのが現状です。しかし、その一時的なコスト削減が結果的に、重大なサイバーリスクを抱えるということについては是非今一度考え直す必要があるのではないのでしょうか。

最後に、貴社が不正と対峙する上で、本調査の内容が少しでも参考になりましたら幸いです。

Vorapong Sutanont
Partner
Forensic services, PwC Thailand



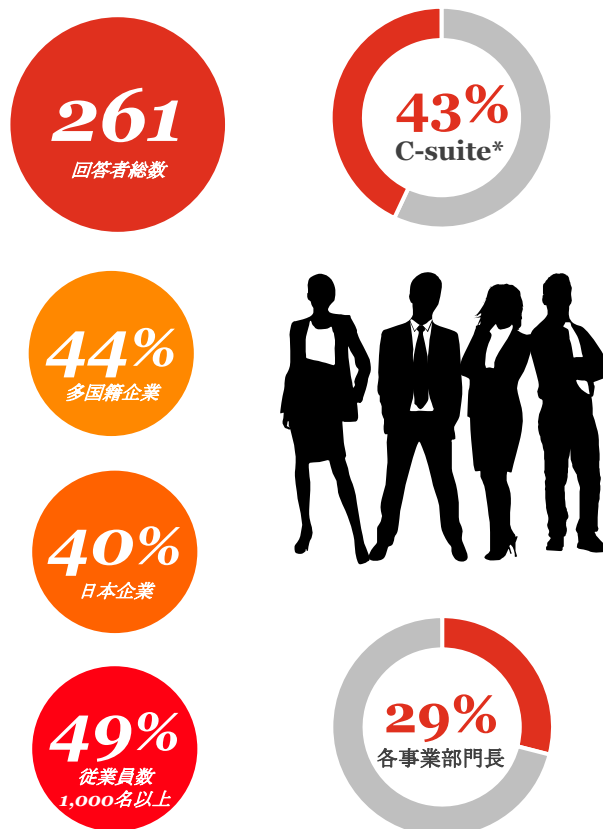
タイでは、上場企業10社の内、
4社が不正を経験している。

タイにおける経済犯罪の実態

PwC世界経済犯罪実態調査2016ータイ版(以下、「本調査」)は、261名からのサーベイ回答結果に基づき作成されている。前回2014年版の76名から大幅に増加しており、また、回答者の多くが重要な意思決定に関する役職者であった。その内訳は、43%が経営幹部であり、29%が各事業部門長である。

企業属性についても上場非上場を問わず多岐に亘り、44%が多国籍企業、40%が日本企業、49%が従業員1,000名以上の企業に該当する。業界としては、自動車を含む製造業が最も多く、金融、小売と続いている。これはタイの産業構成を反映した結果となっている。

回答者の分布

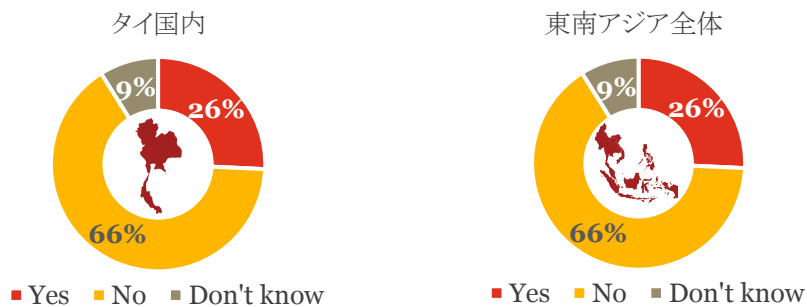


業界



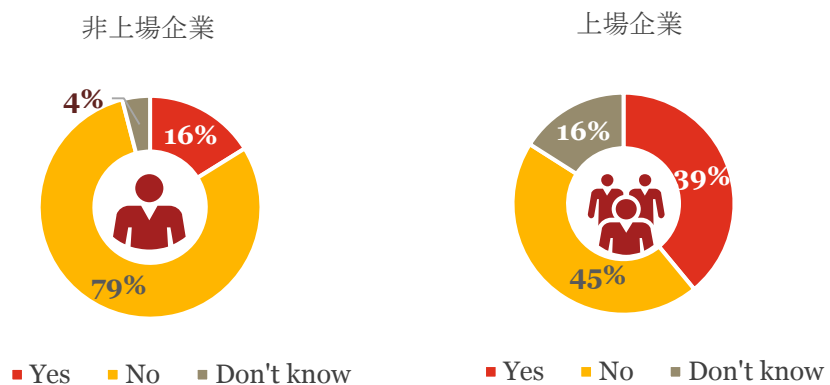
*CEO, CFO, COO等の経営幹部

2014年および2015年において不正が発生したと回答したタイ国内の企業の割合



過去2年間に、タイで不正が発生したと回答した割合は26%となっており、東南アジア全体と同じである。一方で、多くの企業が、現在の自社の内部統制では不正を発見できているとは限らず、実際の不正の発生割合はより高いであろうと認めている。

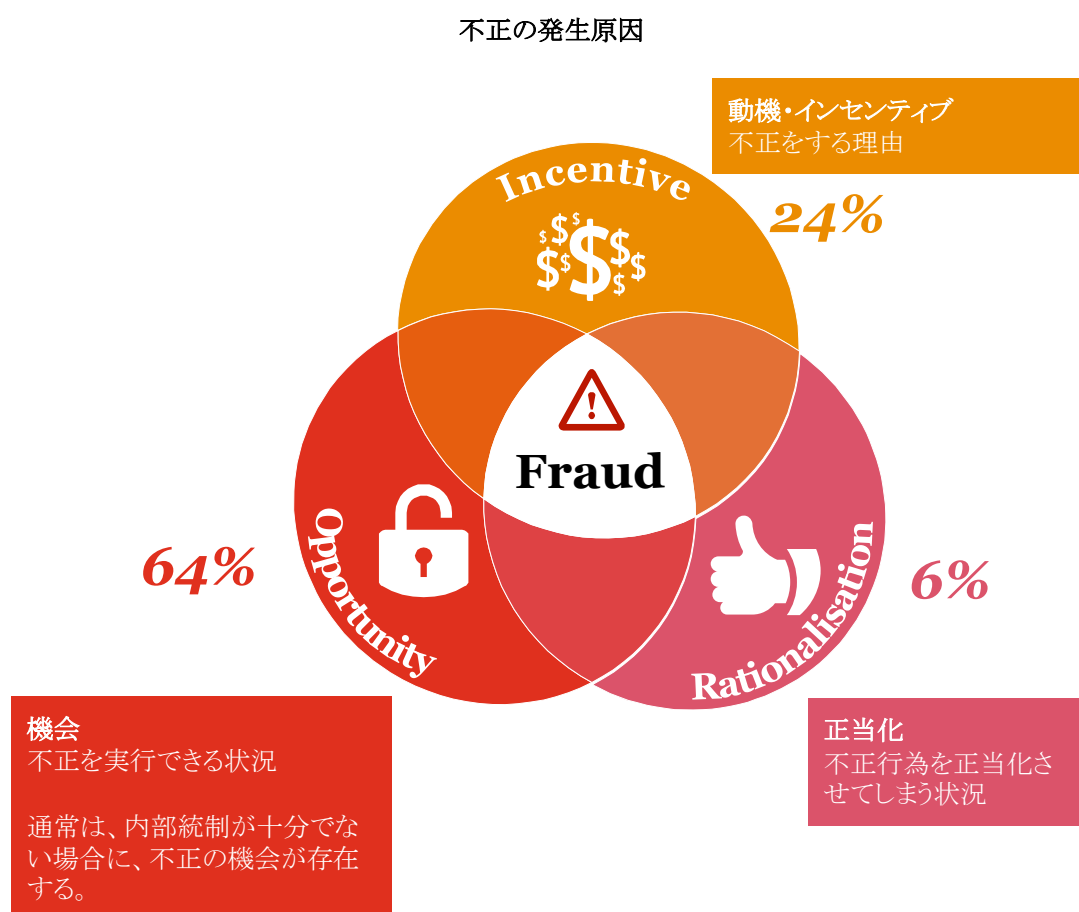
2014年および2015年において不正が発生したと回答したタイ国内の企業の割合 (上場・非上場別)



タイ国内では上場企業の39%が不正を経験しており、非上場企業の16%を大きく上回っている。この上場企業の不正発生割合が多いという傾向は、世界全体の傾向(上場企業41%、非上場企業30%)と共通しており、タイ国内の上場企業は、より不正に対する認識を高めていることが見て取れる。タイでは、タイ王国国家警察庁(「タイ警察」)経済犯罪制圧課(the Economic Crimes Suppression Division of the Royal Thai Police)による企業の対応能力強化イニシアチブや、拘束力はないものの、タイ取締役協会(Thai Institute of Directors (IOD))による反汚職集团的行動連合(Collective Action Coalition against Corruption (CAC))等の民間機関による提言など、ここ数年、国内企業の不正を防止するためのイニシアチブが活発に行われている。これらの活動により、より不正への認識が高まり、非上場企業における不正も表面化していくと考えられる。また、業界別では、金融業界の約過半数(48%)が企業内で何らかの不正が発生したと回答しており、その他業界の平均33%より高くなっている。

約80%の経済犯罪は企業内部の犯行によるものである。通常、従業員による犯行は、巧妙に社内
で隠蔽されている場合が多く発見が難しいことが多い。

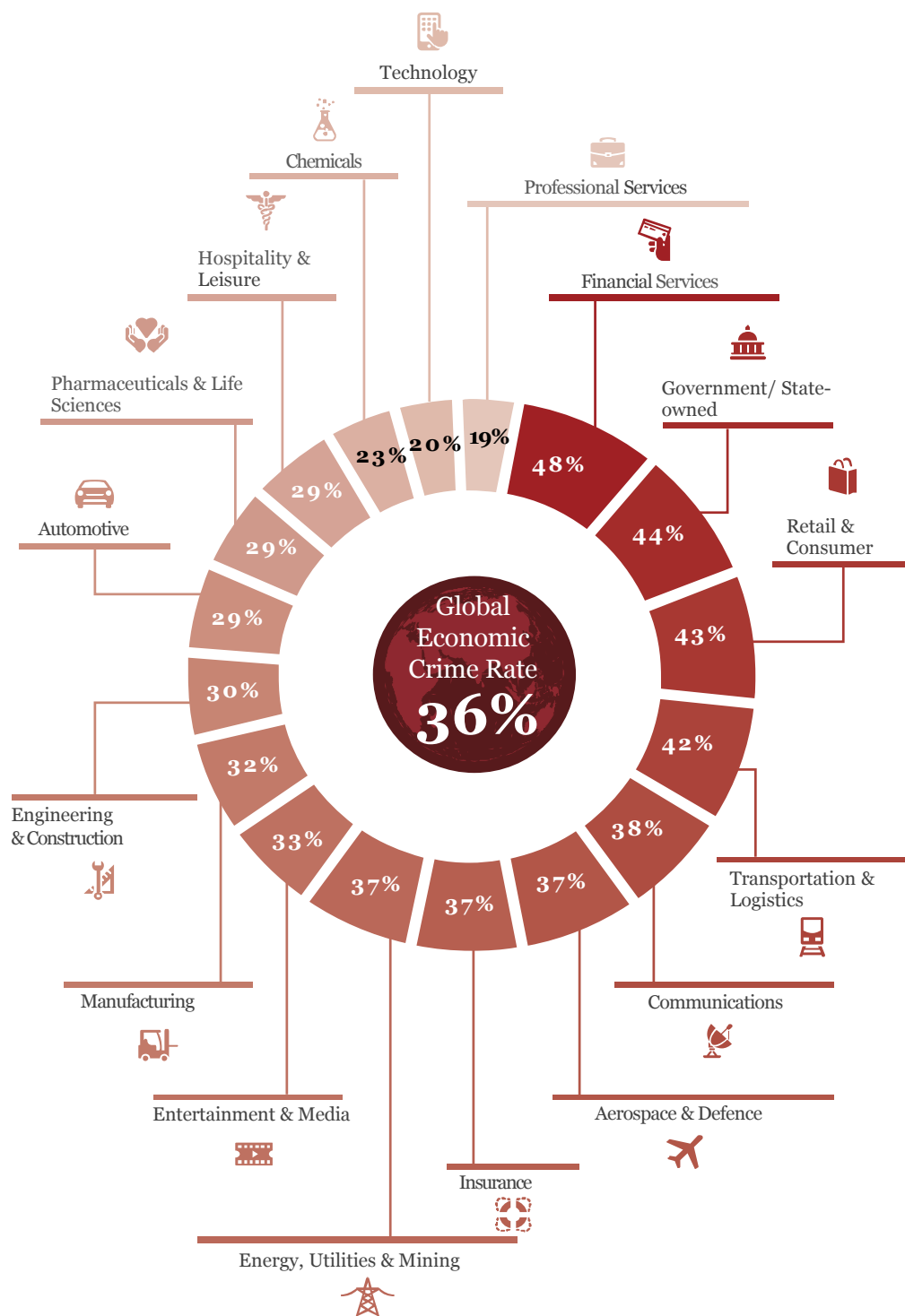
また、回答者の約3分の2(64%)が、不正の発生は、それを容易に行えてしまう機会があることに起
因していると考えており、不正防止には何よりも強固な内部統制構築および不正防止対策が必要
であることを強調している。さらに、従業員のモラルの向上および維持も重要であり、不満のある従
業員は、往々にして不正行為者に変貌することが多いのも事実である。





グローバルの視点

業種別の不正の発生状況



世界全体では、**2,251**社が経済犯罪の被害にあったと回答している。業界別では、金融機関が**48%**と多く、その金銭的規模からも経済犯罪被害を受けやすいという結果になっている。一方で、上図からも見て取れるように、ほとんどの業界において約**3割超**の企業が不正を経験していることを鑑みると、不正は業界を選ばずに発生していると言えるだろう。

しかしながら、やはり金融業界における経済犯罪を他業種のそれと同一視することは出来ない。例えば、自動車業界、小売業、通信などいくつかの業種を例に挙げてみても、そのビジネス活動において金融サービスとの連携は切り離すことが出来ないものである。

金融業界は、厳格な規制環境の下、過去数十年に亘り、高度な業務統制と不正防止プログラムを構築してきたが、急速に変遷するコンプライアンスを取り巻く環境下でリスクを管理するにあたって、金融機関規制と総合的な不正対策の両方への効果的な対応に苦慮している。この点については、後述のアンチ・マネーロンダリング (AML) の章で掘り下げている。



グローバルの視点

金融業界における不正トップ5



資産の横領



サイバー犯罪



マネーロンダリング



会計不正



住宅ローン不正

金融業界以外における不正 トップ5



資産の横領



汚職・贈収賄



購買不正



サイバー犯罪



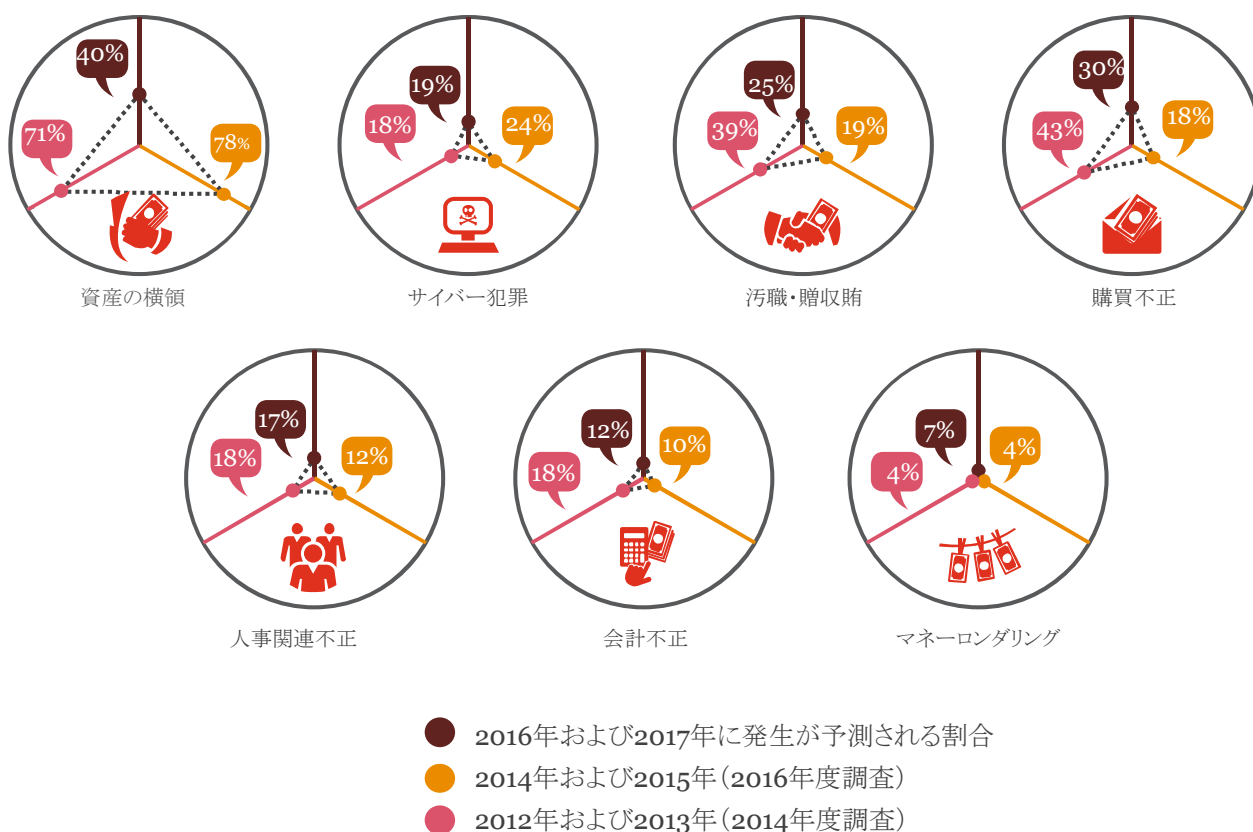
会計不正

ここでは、金融機関とそれ以外の業界それぞれにおける不正の特徴を見て行きたい。まず、金融機関を除くその他業界では、資産の横領、汚職・贈収賄および購買不正等が主な不正となっている一方、金融業界では、資産の横領がやはり最も多いものの、次いでサイバー犯罪、マネーロンダリングといった金融業界の特性を表した結果となっている。

また、ガバナンス、リスク管理およびコンプライアンス・プログラムへの情報システムやデータアナリティクスの導入が汚職・不正リスクを軽減させるとの結果も出ている。PwC USが2015年に発行したPwC's 2015 State of Compliance surveyによると、28%の金融機関がリスク管理の手法として、コンプライアンス情報の自動トラッキングや疑わしい取引のモニタリングなどを含む分析手法・テクノロジーを採用しており、特にリスク管理部門がハイリスクと定義した領域に対する内部監査手続きの一環としても実施しているとのことである。

過去のタイにおける主な不正と今後2年間の予測

2014年度調査vs. 2016年度調査 – 全業界



資産の横領

資産の横領は、依然としてタイにおける最も一般的な不正で78%となっており、世界平均の64%、東南アジアの平均69%と比較しても発生率が高い。前回調査においても、資産の横領がこの2年間で最も大きな課題になるとの回答が集まっており、本調査の結果に反映されている。一方で、本調査においては、今後2年間に資産の横領が発生すると回答したのは40%と少なくなっている。しかしこの数字は、ここ数年で資産の横領を含む不正対策に力を入れ始めたことによる企業の楽観視である可能性は否めない。



サイバー犯罪

サイバー犯罪は、資産の横領に続き2番目に多く、回答者の4分1がサイバー攻撃を経験したと回答している。これは、グローバルの結果の32%と同じ傾向である。実際に、我々のタイにおける調査経験からも、2011年以降急速に増加していると実感している不正の種類である。

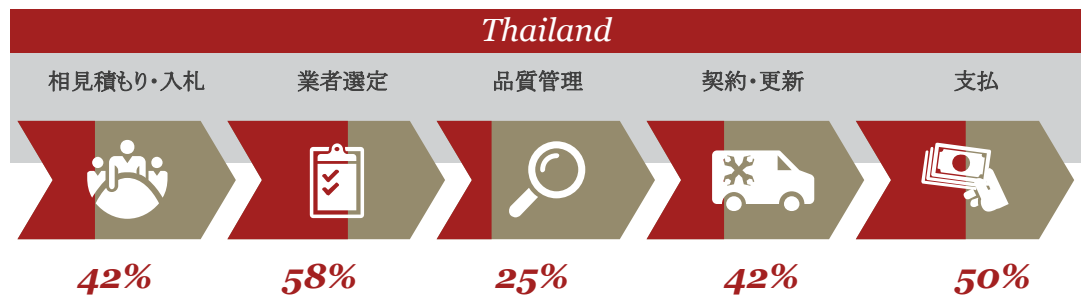
汚職・贈収賄

汚職・贈収賄が発生したと回答した企業は19%であり、2011年の54%、2014年の39%から大幅に減少した。一方で、約4分の1の企業は汚職・贈収賄を認識していないものの発生している可能性があると回答し、他の4分の1は、必ずしも発生していないとは言い切れないと回答している。つまり、約半数の回答企業が汚職・贈収賄リスクを少なからず認識していると言えるだろう。

タイには、汚職事件を防止・調査することを目的とした、国家汚職行為防止委員会 (the National Anti-Corruption Commission) があり、過去にはタイの上級国家公務員の資産状況に関する報告書等も発表している。また、タイの現政権は汚職撲滅を目的とした施策を打ち出しており、直近では、公務員の汚職および不正行為に特化した裁判所を設立する法案が可決し、さらには、2016年末までに、法制委員会 (the Council of State) にて汚職に関する法令が可決される予定であると発表している。現在、メディア、財界、国際監視機関は、これらタイ国内の反汚職に対するイニシアチブを注視しており、各施策・機関の有効性について積極的に議論を交わしている。

2010年、民間企業における不正リスクに対する認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、反汚職集团的行動連合 (Collective Action Coalition against Corruption "CAC") を設立した。2016年3月現在、548社 (内、316社が上場会社) がCACネットワークに加盟しており、152社がCAC認定を受けている。

購買不正



購買不正

購買不正が発生したと回答した企業は前回調査の43%から18%と大幅に減少している。前回調査では、購買不正がタイにおける最も多い不正としてあげられており、我々も、この2年間、ベンダー選定基準、バックグラウンド調査や適切なデューデリジェンスの実施等を含め購買プロセスの強化をすることを各企業に推奨しており、また実際多くの企業が不正防止施策を導入し始めている。これら購買関連における不正防止策の導入などが本調査の結果に影響している可能性は高いが、我々は、依然としてタイで事業を行う企業にとって最も起こり得る不正の種類であると考えている。実際に30%の企業が、今後2年間で購買不正が発生すると考えていると回答している。

また、各購買プロセス毎に見ていくと、ベンダー選定時が58%と最も多くなっている。これは、財務報告目的の内部統制の枠外においてベンダーとの癒着が多いことに起因している。また、注目すべきは、支払時における不正の割合が前回調査の25%から50%と倍増している点である。これは、従来の小切手による支払からオンラインバンキングによる支払が増加している一方、例えば、支払先の変更、入力と承認の職務分掌の欠如など、その新しいプロセス対しての統制が必ずしも十分でないことなども原因であると考えられる。

さらには、契約・更新時における不正も前回調査の25%から42%と増えている。これも、ベンダー選定と同様、従業員とベンダーとの癒着による馴れ合いや合理性のない契約更新等が主な理由であろう。

人事関連不正

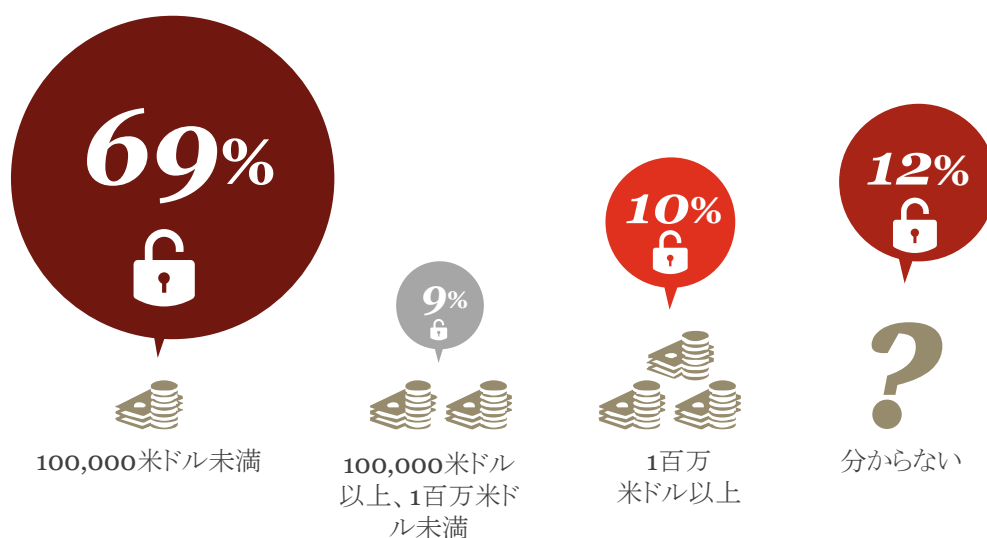
ここ2年間で、12%の企業が採用時および給与支払に関する人事関連不正が発生したと回答している。また、調査結果によると、最も多いのがペイロールに架空の従業員を載せて給与を不正に払いだす幽霊社員 スキーム(38%)と経歴詐称(38%)であった。不適切な給与の支払による財務的影響は勿論のこと、経歴詐称などによる資格の不備は、品質・サービスの低下並びに対外的な信用の毀損などの原因となりうる。

我々の過去の経験から、ある一定役職以上の採用については、前職、前々職への問い合わせや、採用時の誓約書への署名などルール化が必要である。実際、不正を行った従業員が解雇された数ヶ月後に同じビルの別会社に相応のポジションで採用されたという事例もある。また、幽霊社員については、入退社などの情報がペイロールに適時反映されていない企業も多く見られるため、プロセスを改めて見直していただきたい。

会計不正

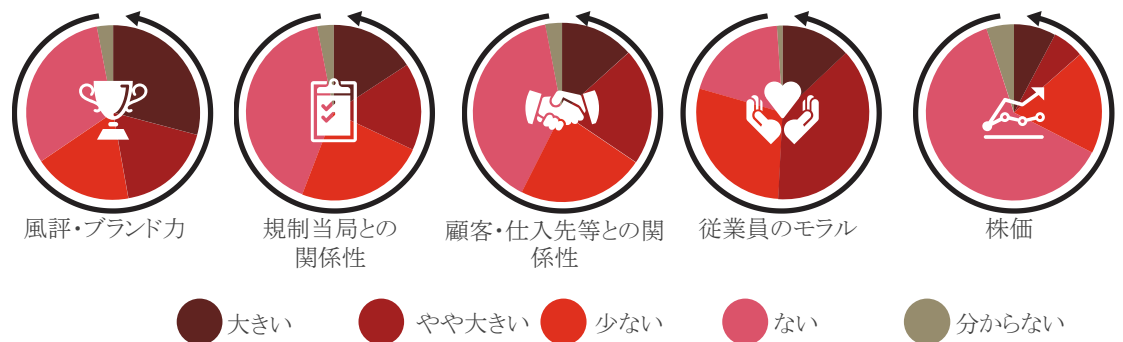
本調査によると、過去2年間で会計不正を経験した企業は10%で、その主な種類は、架空の売上計上、原価付替え等であった。しかしながら、実際にはこの数字より多いと考えられている。通常、会計不正には、架空の取引を捏造したり、不正の事実を隠蔽するために財務データの改ざん等を伴うが、横領や購買に付随する財務数値の改ざん等は、それぞれ資産の横領や購買不正に分類されていると考えられる。

2014年および2015年に発生した不正による財務的被害



過去2年間で不正を経験した企業の約10分の7(69%)において金額的被害額は100,000米ドル以下(3.5百万バーツ)以下であり、一つ一つの不正は比較的小規模である一方、約20%の企業では100,000米ドル以上、内10%で1百万米ドル(35百万バーツ)以上の金額的被害を経験している。不正の約5分の1が、100,000米ドル以上の金額的被害を被るというのは、タイ国内において事業を展開する日本企業にとっては看過できない事実なのではないだろうか。

2014年および2015年に発生した不正による非財務的被害



本調査では、財務的被害のみならず、風評やブランド力の毀損、従業員のモラル低下、規制当局や取引先との関係性等、非財務的な影響についても調査した。不正は単に直接的に金銭的被害を与えるだけではなく、非財務的な被害により短長期的にビジネス全体に影響を与えるためである。

回答企業によると、企業内における不正の発生は、主に、従業員のモラル、および風評・ブランド力へ影響を与えており、被害が大きい又はやや大きいと回答した企業は、それぞれ50%と49%となっている。一方で、株価への影響が大きいと回答した企業は少なく見えるが、これは回答企業の約40%がタイ国内で事業を展開する日本企業(タイ国内において非上場)であることも影響していると考えられる。

いずれにせよ、不正の与える非財務的被害はタイ国内で事業を展開する企業にとって極めて重大な課題であり、規定類の整備、不正リスク評価、コミュニケーション、不正・内部統制に関するトレーニングおよびモニタリング等をカバーする包括的な不正防止プログラムの構築を検討することが望まれる。

タイ国内の企業は、サイバー犯罪のリスクを軽視すべきでない。

サイバー犯罪： 逼り寄る脅威

タイにおけるサイバー犯罪の発生率は急速に増加している。22%の企業は過去数年内にサイバー攻撃による被害を受けたと回答している。企業内で報告されたサイバー犯罪の被害は2014年から2015年にかけて大幅に増加し、2012年および2013年を対象とした前回調査の4位から2位へと躍り出ている。

今後より多くの企業が「モノのインターネット (Internet of Things)」事業へ進出するに伴い、サイバー犯罪のリスクはさらに増加するものと考えられる。

10件中4件がサイバー犯罪を認識している



しかし、サイバー犯罪者による攻撃は10件中2件である



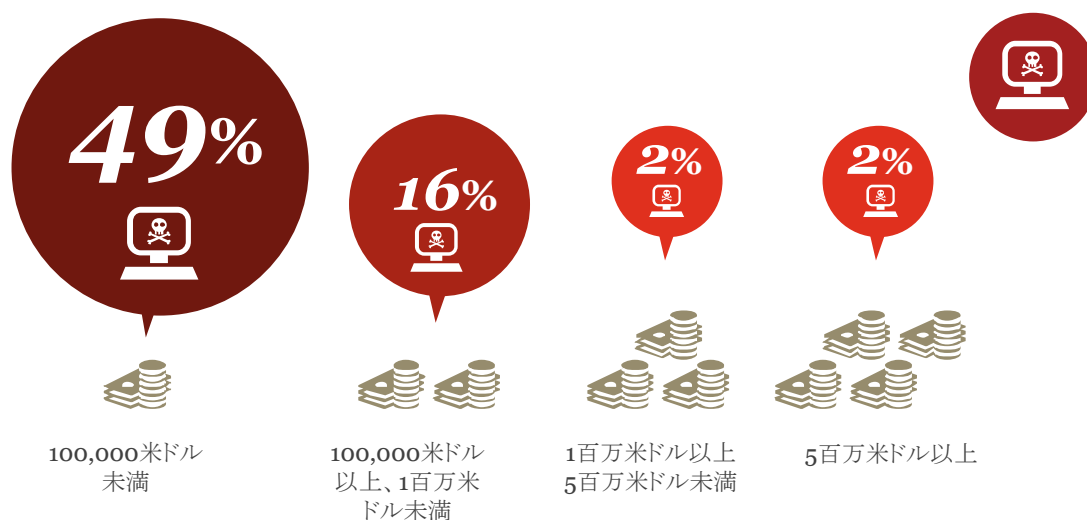
誰が影響を受けるのか？

本調査によると、全ての業界がサイバーリスクに晒されているという結果が出ており、特に金融業界のリスクが高くなっている。また、2016年に発表されたPwCの「グローバル情報セキュリティ調査」によると、2015年は小売業におけるサイバー犯罪が最も増加している。

企業内外からの脅威

内部による犯罪が多いタイにおける伝統的な不正とは異なり、**44%**の回答者が外部からの攻撃による被害、**34%**が内外の両方から攻撃を受けたと回答している。これは、グローバルの経済犯罪の不正行為者のトレンドと同じ傾向になっている。我々のタイにおける過去の調査経験では、やはり攻撃者は、企業内外や国内外からを問わずインターネット回線を介して攻撃していることが多い。従って、タイ国内の企業も、これらの脅威に対抗するために、世界水準の強固なITポリシーおよびシステムを構築することが求められている。

2014年および2015年のサイバー犯罪による財務的被害



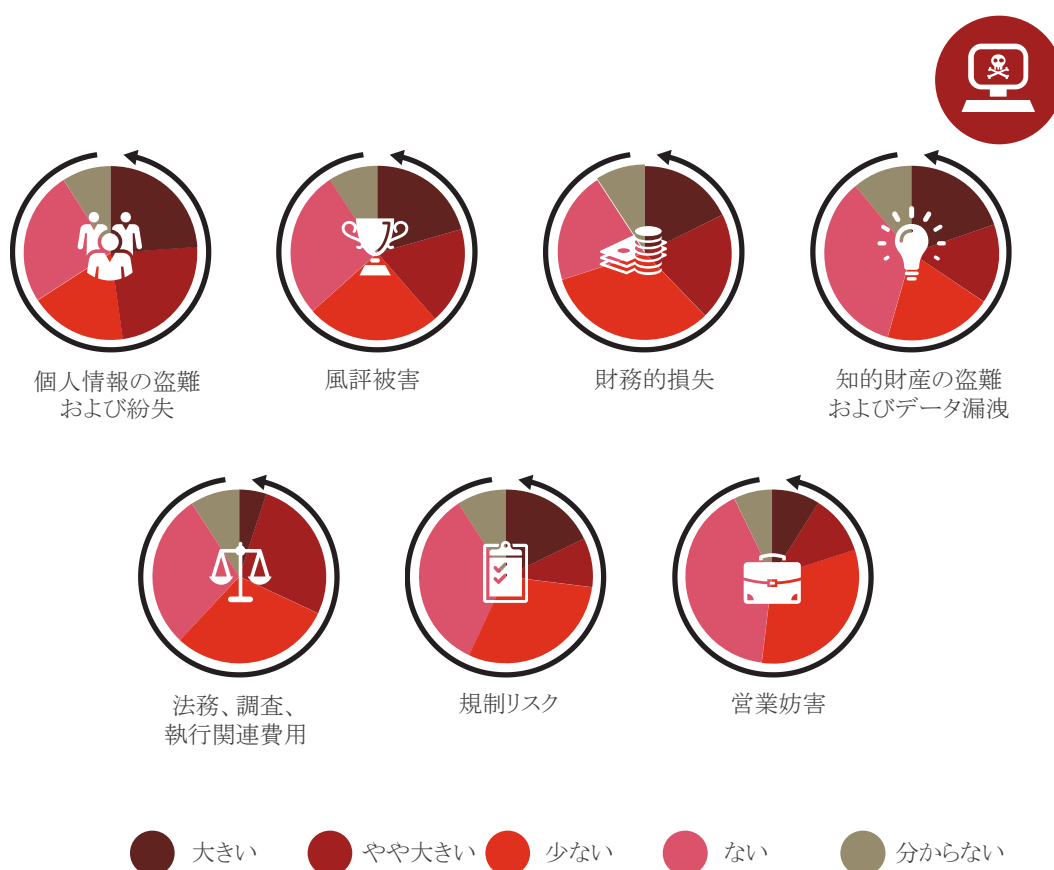
サイバー犯罪による財務的被害

サイバー攻撃を受けたことのある企業の約5分の1が**10万米ドル(約3.5百万バーツ)**以上の被害を被っている。内、**4%**は**1百万ドル(約35百万バーツ)**以上の損失とその被害額も高額である。その被害額の大きさに加え、金融業界に限らず様々な業界を標的にしている点、攻撃者の所在地を選ばない点、昨今の被害件数の急増からも今後無視出来ない不正であることは間違いない。

最大の被害は個人情報漏洩

数あるサイバー犯罪の中で、企業にとって最も被害が大きかったのが個人情報の漏洩である。続いて、風評被害、知的財産の盗難との調査結果となっている。なお、必ずしもサイバー犯罪ではないが、我々の過去の調査において、知的財産や機密事項の持ち出しは、しばしば行われており、多くの日本企業が直面するリスクとなっている。

2014年および2015年のサイバー犯罪による非財務的被害

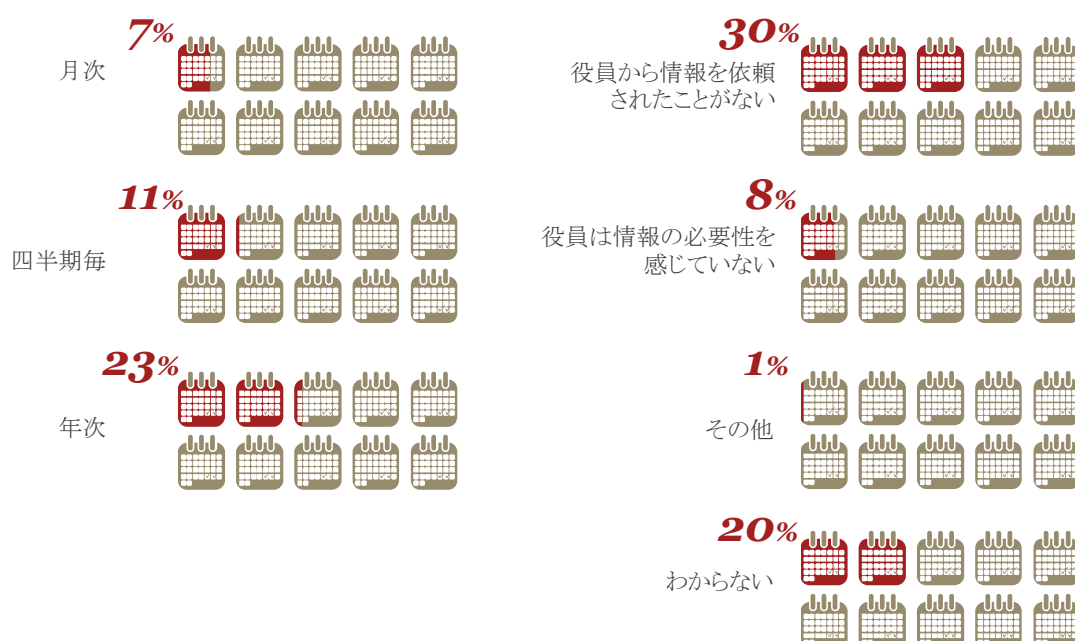


タイ国内の企業はサイバー犯罪に対しどのような対応を行っているか？

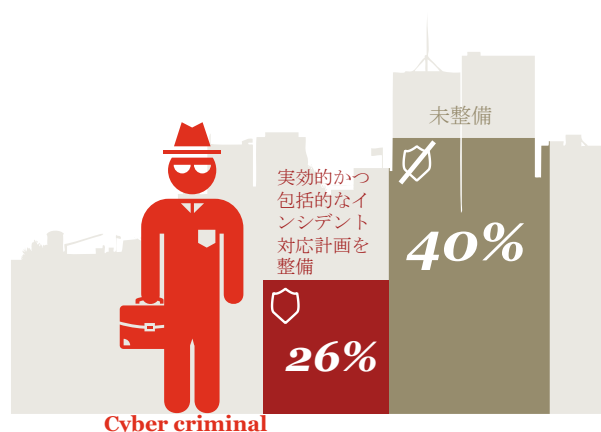
グローバル企業は、積極的なサイバーリスク評価・分析技術を用いサイバー攻撃を認識した際の調査や改善の迅速化を図っている一方、タイでは39%の回答者がサイバーリスクを認識していると回答しているにも拘らず、積極的なサイバーリスク対応への投資が行われておらず、日々企業のウェブサイトやシステムが脅威に晒されている。

昨今グローバルでは、サイバー犯罪との戦いは、IT部門内で解決すべき問題ではなく、会社を代表する役員レベルが企業資産を守るために責任を負うべきとの見方が大半になっている。しかしながら、タイでは、サイバー犯罪に対する有事への即応性について、役員が定期的に確認している企業は41%のみであった。

役員はどのくらいの頻度で、サイバー犯罪に対する即応性の現状について、情報の確認を行っていますか？



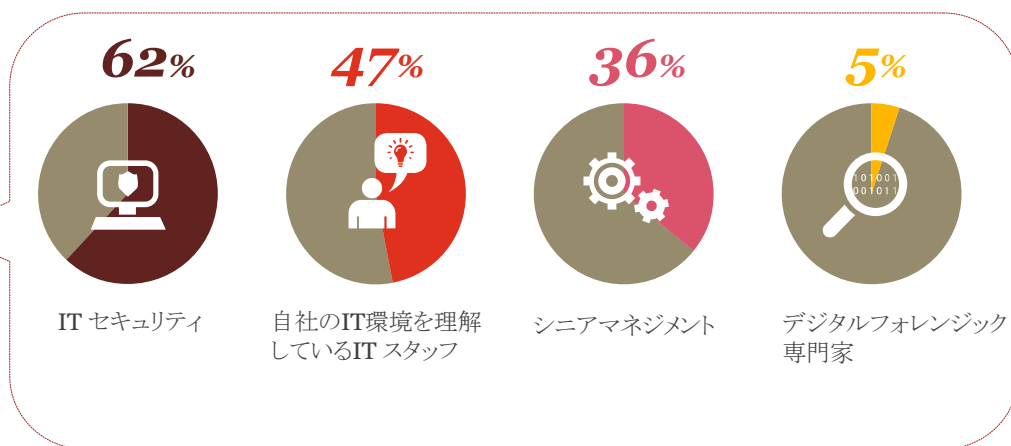
グローバルでは37%の企業(主に規制の厳しい金融業界)が、サイバー攻撃に即応するための実効的かつ包括的なインシデント対応計画を整備しているが、タイでは26%に留まっている。さらに、40%の企業は、基本的な計画等も全く整備しておらず、そのうち半数は必要性も感じていないとの回答であった。



タイ国内では約80%の企業が、サイバー攻撃に対しての緊急初動対応チームを有していないと回答している。サイバー攻撃への緊急対応チームを有する23%の企業のうち、その主な構成メンバーはITセキュリティ担当が62%で最も多く、自社のITスタッフが47%と続いている。デジタルフォレンジック専門家を採用している企業はわずか5%にとどまっている。

緊急対応チームの構成メンバー

緊急対応チーム
を有する企業



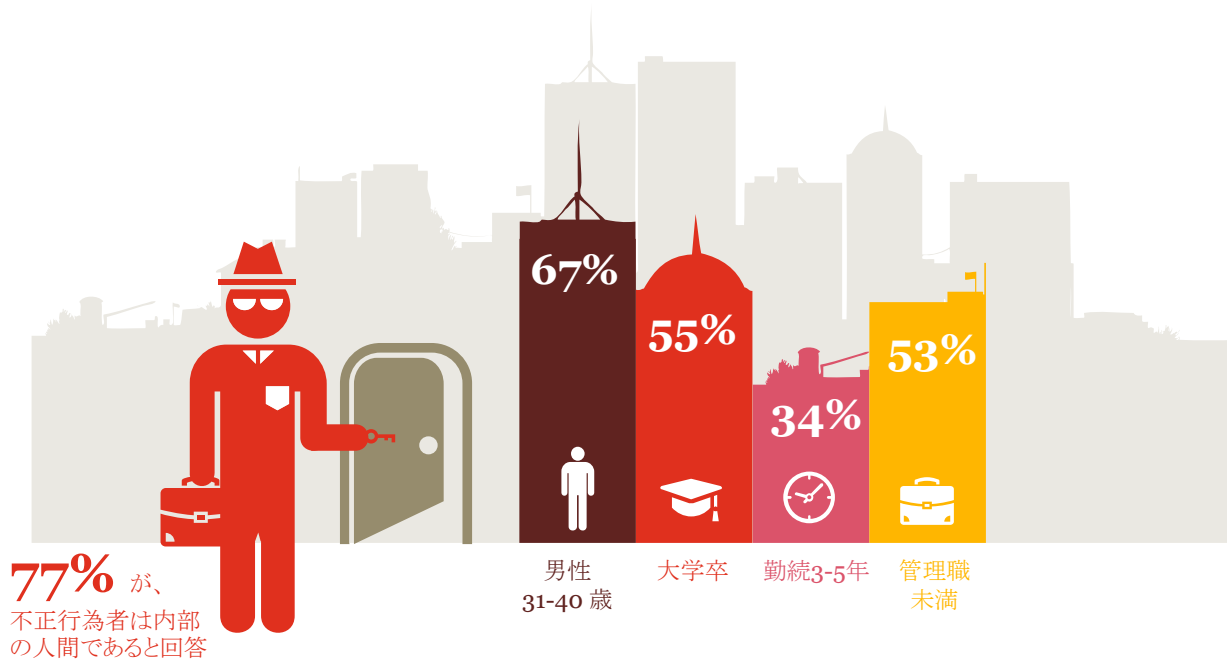
企業の約30%は、タイの法執行機関がサイバー犯罪の調査に必要なスキル、人員および技術を十分に有しておらず、結果的に立件できないのではないかと考えている。さらに約40%は、そもそも法執行機関のそれらの能力について分からないと回答しており、サイバー犯罪に関する国内の法執行機関への信頼度は低いことが窺える。

法執行機関への信頼度



回答者の過半数以上が、自社の従業員（役職者未満）に不正を行っている者があると回答した。

不正行為者とは？



タイの不正行為者の特徴

77%と前回調査の89%から12%減少したものの、依然として従業員が主な不正行為者という結果になっている。また、興味深いのは、不正行為を行った者の役職が、中間管理職（前回調査にて56%）から管理職未満の従業員へシフトしており、同割合は前回の36%から53%へ大幅に増加している。

また、外部からの不正を経験した企業の31%は、ビジネスパートナーまたは代理店・エージェントによるものであると回答しており、内、33%の企業が、その犯罪を警察に報告したとのことである。しかし、この通報実績の割合は世界平均の53%から見ると大幅に少ない。さらに、そのようなビジネスパートナー間での不正に対して、取引関係を中止したと回答した者は17%に留まっており、これも東南アジア全体の27%よりも低くなっている。

これらの事実からも、タイでは、不正への認識が高まってきてはいるものの、外部との取引関係においてある程度の不正行為は当然なものとし、重要視していない悪しき慣習が残っていることが分かる。しかし、それは社会的責任を負う企業にとって何らその慣習を正当化すべきものではなく、新規取引先との取引開始の際には適切なデューディリジェンスを実施することが改めて求められている。

不正が発生する原因

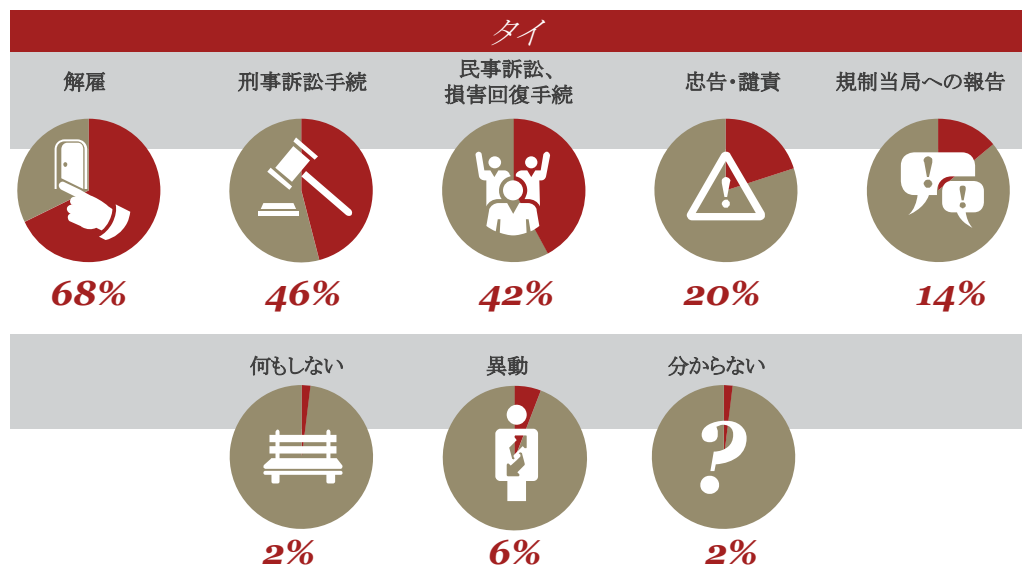
グローバルの傾向と同様に、大半の回答者は、内部統制の欠如による不正が行える機会と、不正行為者に実行するだけの知識があることが大きな原因と考えている。また、そのような環境において、従業員のモラルの低下、悪意の欠如等が相まって不正が起きている。現に、労働環境、給与、評価に満足をしていない従業員による不正が多いのも事実である。これらの結果からも、内部統制、内部通報制度、取引モニタリング等の不正防止や発見に関する統制の継続的な強化は必然的に求められている。

不正行為者への対処

不正の事実・疑義が発生した際は、企業は、その事実を真剣に受け止め対応しなければならない。まずは、最終的な処遇如何に拘らず、事実認定を行う必要があり、その結果に基づき、解雇・減給等の社内対応や民事訴訟・刑事訴訟などの法的手続きを検討していくことになる。これら調査や法的手続きは、しばしば専門家のサポートが必要となり時間も要するが、会社としての不正に対する厳格な姿勢を示すことで、不正が起りにくい企業風土が醸成されていくことになる。

68%の企業が不正行為を行った従業員を解雇している。刑事訴訟と民事訴訟は、それぞれ46%と42%となっているが、この数字が近似しているのは、不正行為者に対して刑事訴訟と民事訴訟をセットで行うことが多いためである。

内部不正行為者に対する懲罰



不正リスクの管理に於いてタイ企業は未だグローバル基準を満たしておらず、高リスクな要素に対しても容認的である。

不正の検出方法

本調査の結果、最も多かった不正の発見経路は、「疑わしい取引報告」の17%であり、次いで「内部監査」と「偶然」が続いており、それぞれ15%であった。また、単純合算にはなってしまうが、企業内外からの告発やホットラインによる不正の発見は13%となっており、東南アジアの23%、グローバルの17%と比較して下回っている。

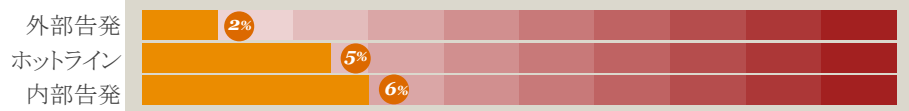
グローバルの傾向と比較して、告発や内部通報による不正の発見は少ない結果になっており、それはタイ人の国民性に由来するところでもある。一方で、そのような状況下において、効果的な内部通報制度の導入・高度化は進んでおらず、従業員が声をあげるという企業文化の醸成も追いついていないのが実態であり、企業が丸丸となって不正を防止するという仕組み・雰囲気を持つことが今求められている。

経済犯罪の発見経路

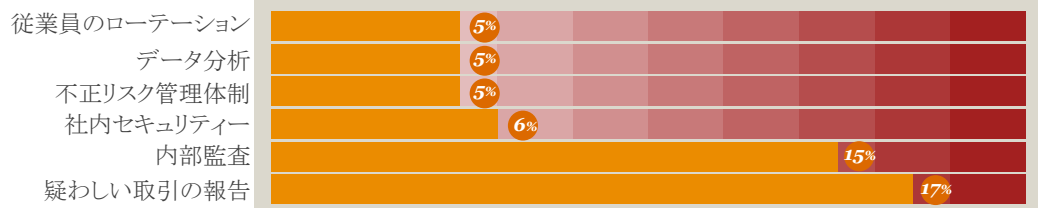
経営者の影響力以外の要素



企業文化



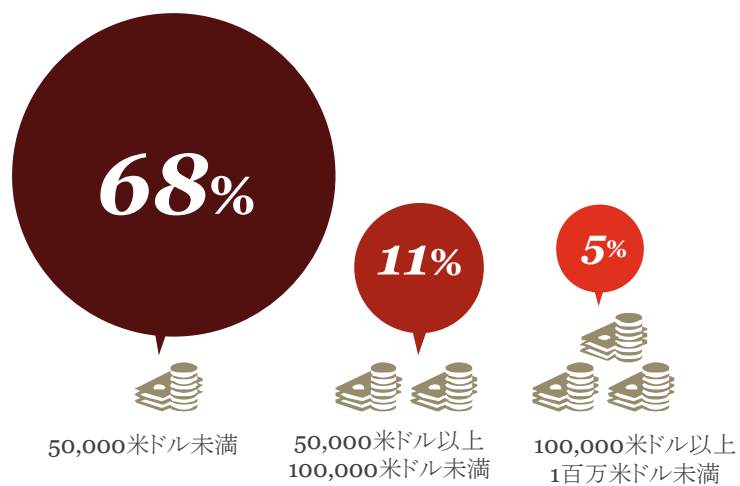
内部管理



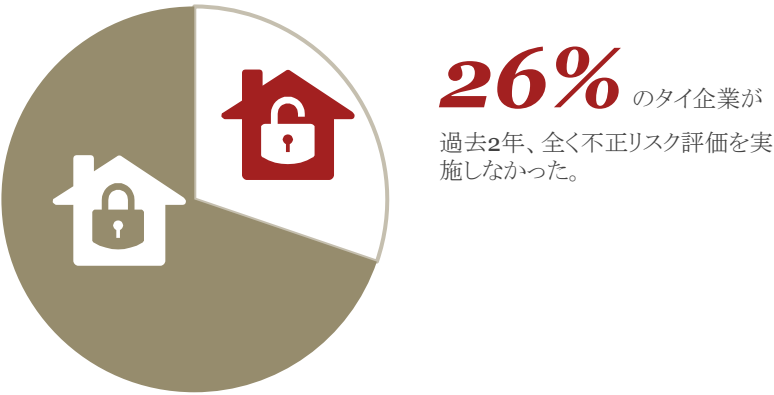
我々の経験上、強固かつ効果的な内部通報制度は、従業員の疑わしい行動、非倫理的行動、違法行為などの情報を得る上で非常に有益であることが分かっている。企業には、既存の内部通報制度やポリシーが十分に理に適っているものであり実効性のあるものか、また、その存在、意義、安全性などが従業員と十分に共有できているか今一度見直していただきたい。例えば、社長からのメッセージ、ポスターの掲載、ホットラインのオペレーター向けのワークショップやインタビュー・トレーニング等も利用者提供者双方に対する促進方法である。

過去2年間に発生した経済犯罪事案に要した調査費用は、約70%の企業において50,000米ドル未満であり、これは発生した不正の平均金額的被害に比例しているといえる。一方で、5%の企業で調査費用が100,000米ドルを超えており、この2年間に一定規模以上の不正調査が必要とされる大規模な不正が発生したことを物語っている。

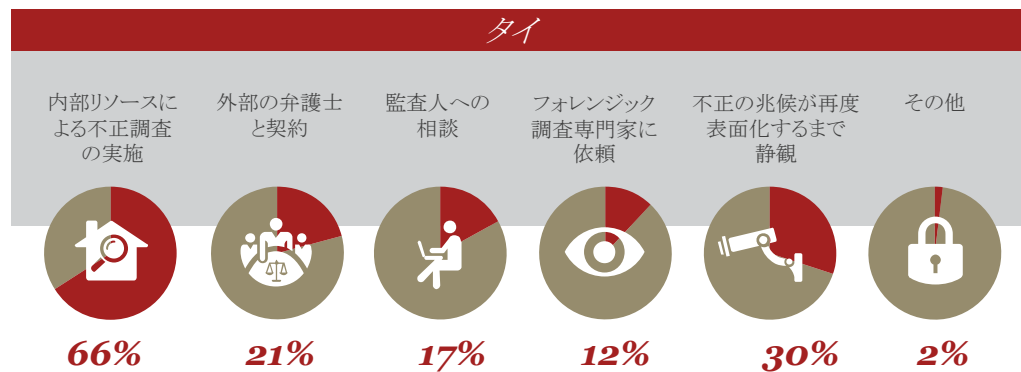
2014年～2015年に発生した経済犯罪に対する調査費用



約6割の企業が、少なくとも過去2年間に1回以上、不正リスク評価を実施していると回答した一方、全体の約4/1の企業がこの2年間で全くリスク評価を実施していないと回答している。不正リスク評価を実施している企業の内、1年間に2回以上行っている企業は15%となっており、この数値はグローバル平均の20%を下回っている。



不正発見後の対処



不正発見時の企業の対応

不正リスク管理そして迅速かつ効果的な対応という側面において、タイ国内企業の態勢は、グローバル基準に達しているとは言いがたい。その一つの傾向として、不正調査による実態解明およびその後の対応の重要性に対する認識に違いがあり、不正疑義が発覚した場合でも、**66%**の企業は、外部専門家ではなく社内のリソースによって調査を行っている。

外部専門家を活用する場合は、「社外の弁護士との契約」が**21%**、「監査人への相談」が**17%**、「フォレンジック調査専門家に依頼」が**12%**となっている。驚くことに、**30%**の企業が再度表面化するまで静観すると考えている。

タイ法執行機関の経済犯罪調査能力に対する信頼度

「タイの法執行機関が経済犯罪の調査および不正行為者の起訴において十分に訓練された人材を有しているか」という質問に対して、**33%**が「いいえ」、**44%**は「わからない」と回答している。一方で法執行機関を信頼していると考えている企業は**23%**にとどまっている。

法執行機関に対する信頼



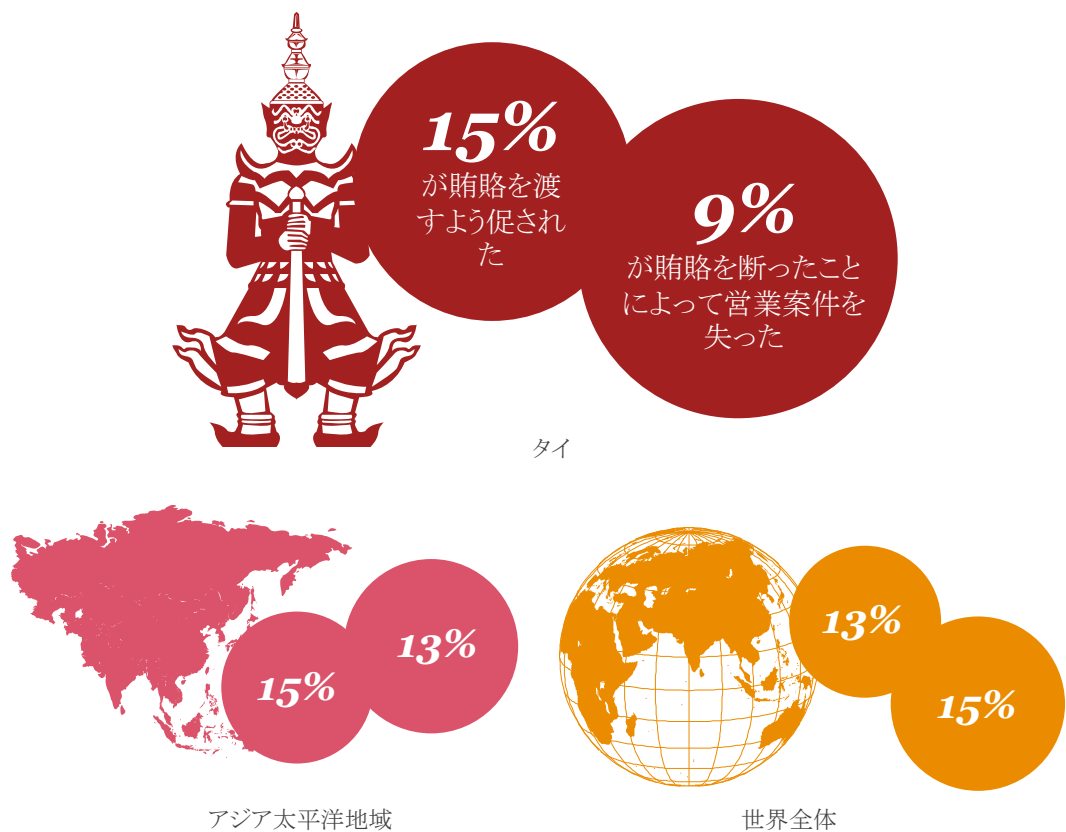
タイ国内で事業を展開する企業の
15%が賄賂を要求されたことがある。

倫理とコンプライアンス

タイ国内で事業を展開する企業の15%が過去2年間に賄賂を要求されたことがあり、9%が賄賂を支払った競合他社にビジネス機会を奪われたと回答している。この汚職・贈収賄はタイにおける大きなリスクであり、25%の企業が今後2年間も汚職・贈収賄を経験するだろうと考えている。

このような現実に対して、回答企業の75%が、政府に国として積極的に汚職・贈収賄を取締まることを期待している。

過去2年間で賄賂を要求されたことがあるか？



コンプライアンス・プログラムは効果的に機能しているのか？

本調査によると、コンプライアンス・プログラムを導入・構築していない企業が20%に上る結果になっている。会社規模の大小により必要とされるプログラムのレベルは異なるものの、コンプライアンスという言葉が紙面で見ない日がない昨今において、5分の1もの企業が何の対策を取っていない事実は驚きである。

コンプライアンス・プログラムの責任者は誰か？



46% の企業がチーフ・コンプライアンス・オフィサーをプログラム責任者としている

どのようにコンプライアンス・プログラムをモニタリングしているのか？



70% の企業が内部監査にてプログラムの有効性を評価している

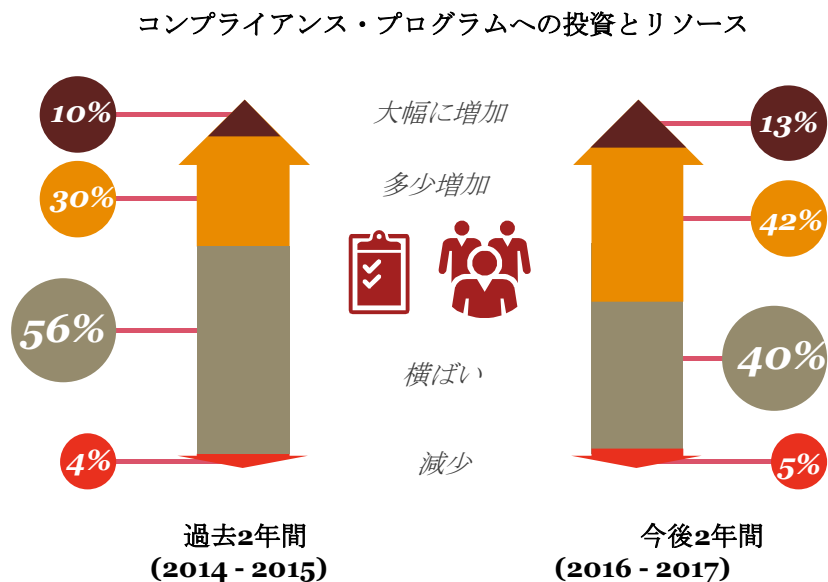
コンプライアンス・プログラムを設けていると回答した企業の46%は、プログラムの責任者としてチーフ・コンプライアンス・オフィサー (CCO) を任命している。比較的小規模な企業では、人事担当者、内部監査人または財務担当役員がその職責を担っているのが一般的である。

また、70%の企業が、内部監査の一環でプログラムの有効性を評価をしているとのことである。

不正の発見には内部監査だけで本当に十分なのか？

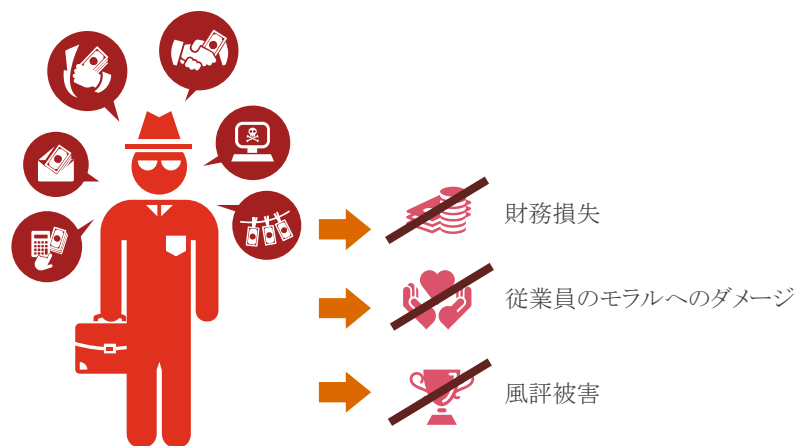
内部監査は、定期的に経営諸活動の運用状況を合理性かつ合法性の観点から評価するもので、経営目標の達成のみならずコンプライアンスの有効性を評価する上でも非常に重要である。また、内部監査の効果的な遂行は不正の抑制という観点からも有効であることに疑いはない。しかしながら、巧妙に隠された不正の発見または適時検出という点では、内部監査手続きの枠内で果たして十分なのだろうか。

不正を積極的に特定・発見するためには、不正リスク評価に基づく監査対象領域の選定と集中、データ分析による不正の兆候検出、取引テストの拡大、証拠の信憑性の確認など、リスクに応じて監査範囲・手続きを拡大する必要がある。さらに、取引量が多い企業においては、取引モニタリングによる高リスク取引を特定することが不正の早期発見という点で非常に有効であるが、現在採用している企業は全体の8%に留まっている。

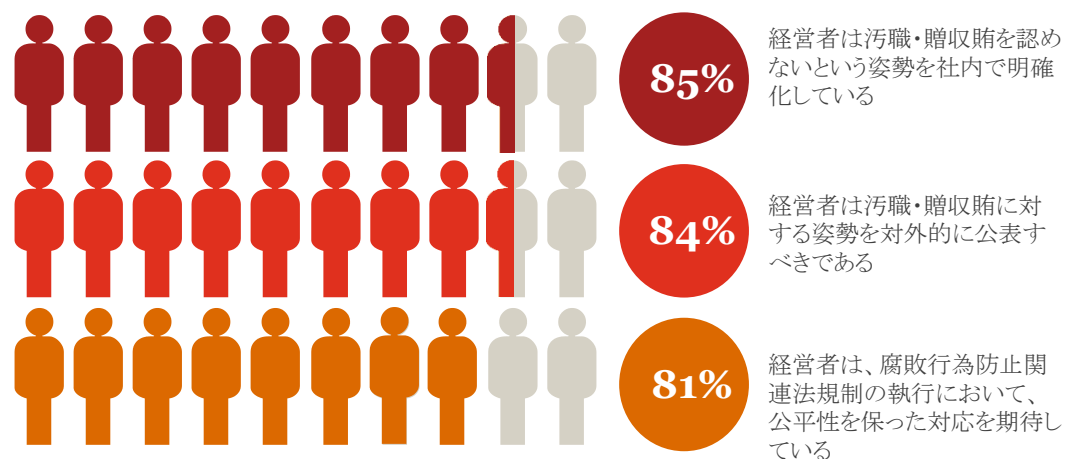


上図からも、企業のコンプライアンスプログラムへの投資とリソースは年々増加していることが分かり、過去2年間で40%の企業が増加したと回答しており、55%が今後2年間でさらにコンプライアンスプログラムを強化していくと回答している。

前述した通り、経済犯罪による影響は直接的な金銭的被害はもちろんのこと従業員のモラル低下や風評被害といった影響も甚大であり、会社に対してこれに何らかの影響があったと回答した企業はそれぞれ50%および49%であった。いずれの場合も、企業の内外からどのように認識されるかという点でビジネスに影響があるということを鑑みると、改めて倫理や価値観が企業運営において重要な役割を担うことを示す結果になっている。



企業の姿勢という観点では、85%の企業は、経営者が汚職・贈収賄は不正行為であり認めないという姿勢を社内で明確にしていると同時に、ほぼ同数の84%が、その汚職・贈収賄に対する姿勢を対外的に公表すべきだと回答している。社内では汚職・不正は許されないとの姿勢を持ちながらも、会社として対外的には発信しておらず、コンプライアンス・プログラムの高度化には依然として改善の余地があることが分かる。



資金洗浄が疑われる活動の特定に
当たって、金融機関の大半が、依然
として人間的報告手段に大きく依存
している。

資金洗浄防止：アンチ・マネーロンダリング

政府による改革

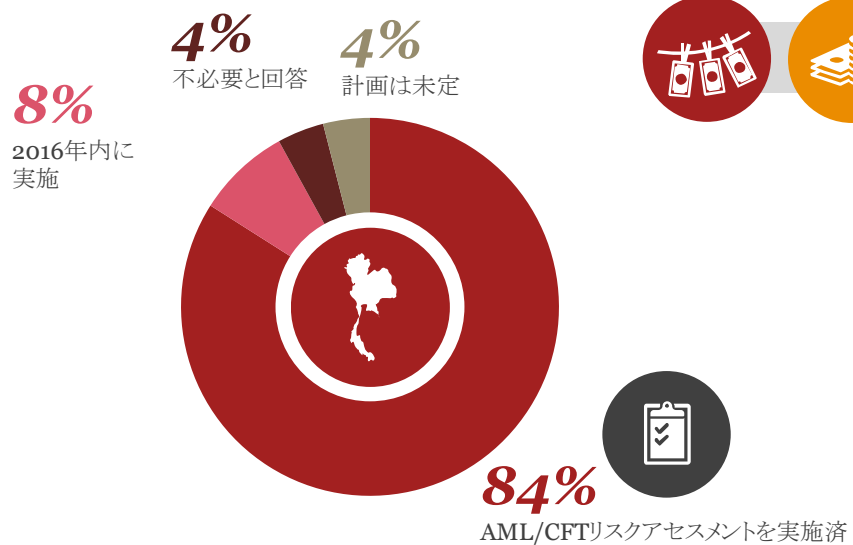
タイ政府は、数々の改革を実行し、資金洗浄防止(AML)およびテロ資金供与対策(CFT)を強力に推進してきた。これらは、タイの規制当局(AMLO)を初めとする国内からの圧力に加えて、タイが2001年に加盟したアジア太平洋マネー・ロンダリング・グループ(Asia/Pacific Group on Money Laundering)による資金洗浄防止規制など国際的な義務を履行するために行われてきた。

タイ政府は、2015年第3四半期から取組みに着手し、AML規制を強化してきた。これには例えば、税制の施行を強化するための歳入局による法律制定、無記名債券のクロスボーダーでの取引に係る対策強化、テロ資金供与対策執行における外務省との協力強化などの改善が行われてきた。また、2016年2月には、現軍事政権である国家平和秩序維持評議会(National Council for Peace and Order (NCPO))がより広範な汚職の取締りを実施する旨を発表しており、AML対策に影響を与える可能性がある。



CURRENCY EXCHANGE RATES			
DATE: 12 APR 2016 TIME: 2:03 PM PAGE: 2/2			
CURRENCY	BUYING		SELLING
	BANK NOTES	T/C	BANK NOTES
USD 1-2	33.95	0.00	35.22
USD 5-20	34.35	0.00	35.27
USD 50-100	34.71	0.00	35.32
GBP	49.22	0.00	50.56
JPY	32.05	0.00	33.25
MYR	8.05	0.00	9.15
SGD	25.64	0.00	26.29
HKD	4.43	0.00	4.57
EUR	39.44	0.00	40.40
KRW	2.79	0.00	3.44
CNY	5.11	0.00	5.61

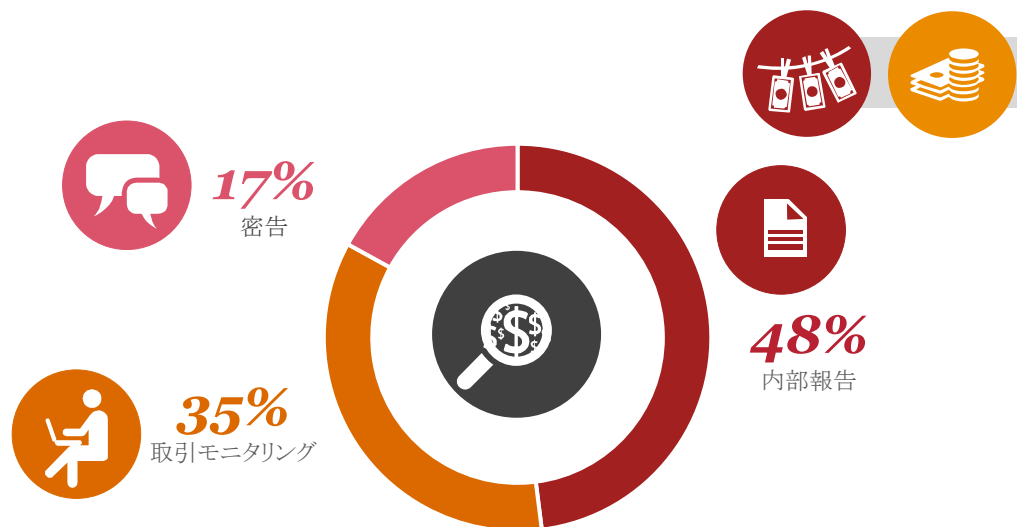
タイで活動する金融機関における
AML/CFTリスクアセスメントの実施状況



タイでAML関連規制を徹底的に運用するにあたっては、常に同地域固有の課題が伴ってくる。まずは、電子的取引が急増しているものの、経済活動の主流が依然として現金ベースであり、それが国内外で支払経路を追跡・モニタリングすることを困難にしている。また、汚職や政治的問題も大きな問題であり、政治的にコネクションを有する者が、規制の隙をすり抜け、その適用を逃れる可能性も未だ排除できてない。

このような課題はあるものの、タイでのAML関連規制の実施状況は改善してきていると言えるだろう。タイ王国国家警察庁の経済犯罪抑制課(Economic Crimes Suppression Division)が国内対策を強化していることに加え、タイはマネー・ロンダリングに関する金融活動作業部会(Financial Action Task Force on Money Laundering: FATF)による立入検査を受けている。FATFの検査結果は、特に金融サービスに対する信頼性という点で、政治的かつ経済的両方において、タイという国の国際的立場に大きく影響を与えるため、AML関連規制の徹底に大きく拍車がかかると考えられる。本調査結果には、このような規制実施強化が反映されており、84%の回答企業が資金洗浄防止およびテロ資金供与対策(AML/CTF)に係るリスクアセスメントを実施したと回答している。

資金洗浄／テロ資金供与の疑わしい取引の特定方法



タイにおけるAML活動に対する注目は益々高まっている。本調査では、タイの金融機関がどのような方法で資金洗浄に関連する問題を検出しているかを質問しているが、約半数の回答者が内部報告を主な発見手段としており、依然として人的な報告手段に大きく依存していることが分かる。

一方、顧客の取引行動パターンを体系的に評価できる取引モニタリングのシステム対応を実施済の企業は35%であった。取引モニタリングは、顧客の取引傾向を分析し、資金洗浄や不正取引の疑いがある場合に警報が発せられるようになっている。

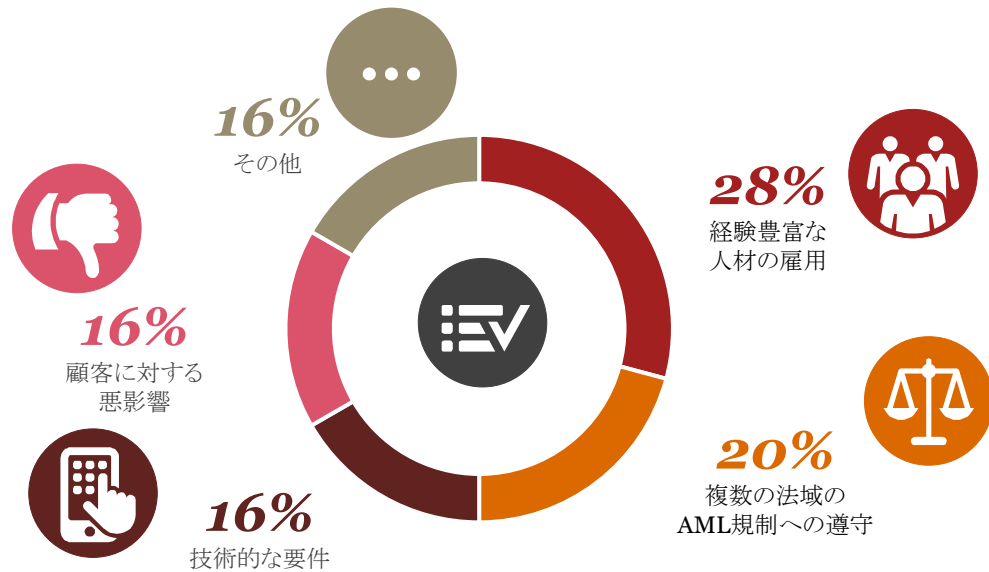
不正の早期検出・解決には何よりもリアルタイムに不正の兆候を検出することであり、その兆候に対して経営陣が速やかに対応し、不正が拡大・悪化する可能性を軽減することが求められており、継続的な取引モニタリングの導入は必須である。

金融機関が直面する課題

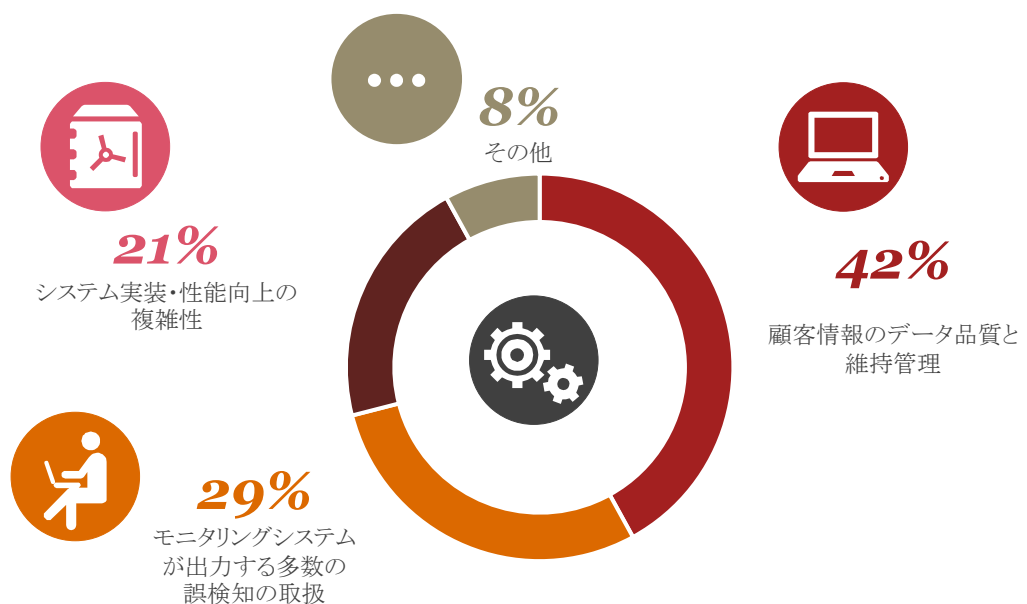
AML/CFT関連規制を遵守する体制を構築するにあたり金融機関が抱える最大課題として、経験豊富なリソースの不足が挙げられる。その他にも、複数の法域のAML規制への対応、技術的な要件、顧客に対する悪影響等も指摘されている。

また、AMLのシステムに関する課題として、42%の金融機関がデータ品質を挙げており、次いで、モニタリングシステムにおける誤検知への対応(29%)、システム実装・性能向上の複雑性(21%)が挙げられている。

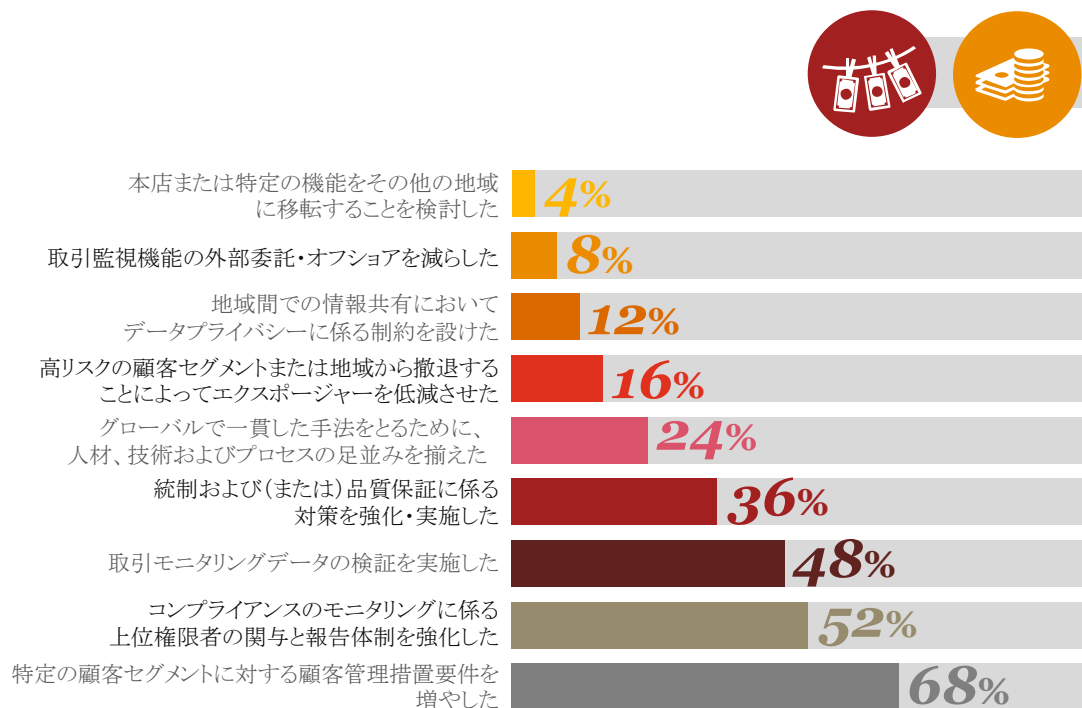
AML/CFT関連規制遵守に関連する課題



AML/CFTシステムを運用する際の課題



AML/CFTリスク軽減のためにタイの金融機関が実施した活動



AML/CFTリスクを軽減するため、タイの金融機関の68%が特定の顧客セグメントに対する「顧客管理措置(know your customer(KYC))」の要件を引き上げ、約半数が遵守状況モニタリングに係る上位権限者の関与・報告体制を強化した。

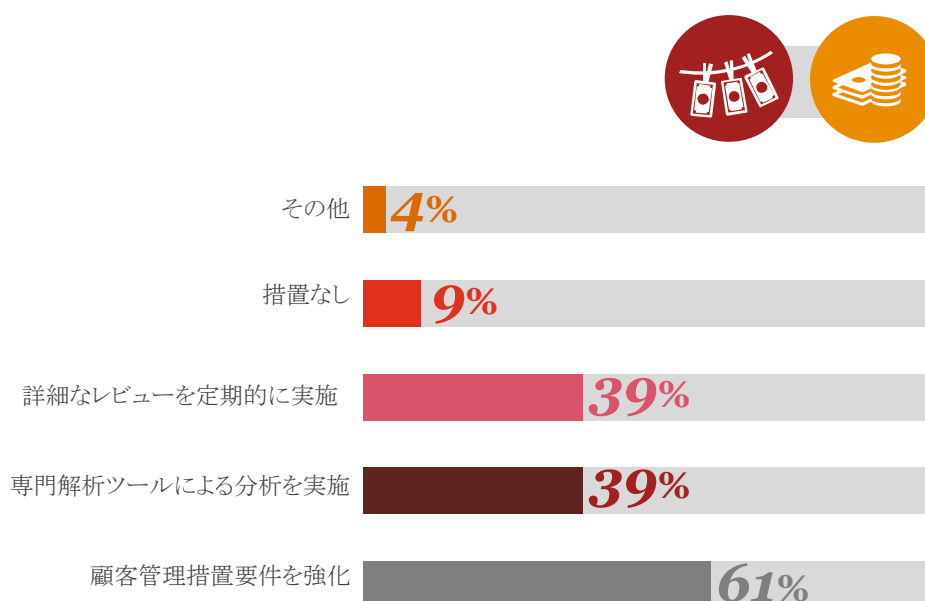
また、人材、技術またはプロセスについてグローバルでの足並みを揃えた会社もある(24%)。実際、これはコンプライアンス上重要な要素であり、まだ実施していない企業においては、ギャップ分析の実施、差異の特定・改善を行い、全社的に一貫したプロセスおよびシステムを確保することが推奨される。

確かにAML対策プログラムの厳格化によって直接収益が生み出されるわけではないが、国際的な規制強化の流れにおいてコンプライアンスの徹底は金融機関の責務であり、その不徹底による信頼喪失は防がなくてはならない。さらに、効果的なプログラムは高リスクの顧客への無担保エクスポージャーなどを減少させ、貸倒引当金の減少にもつながることにもなる。

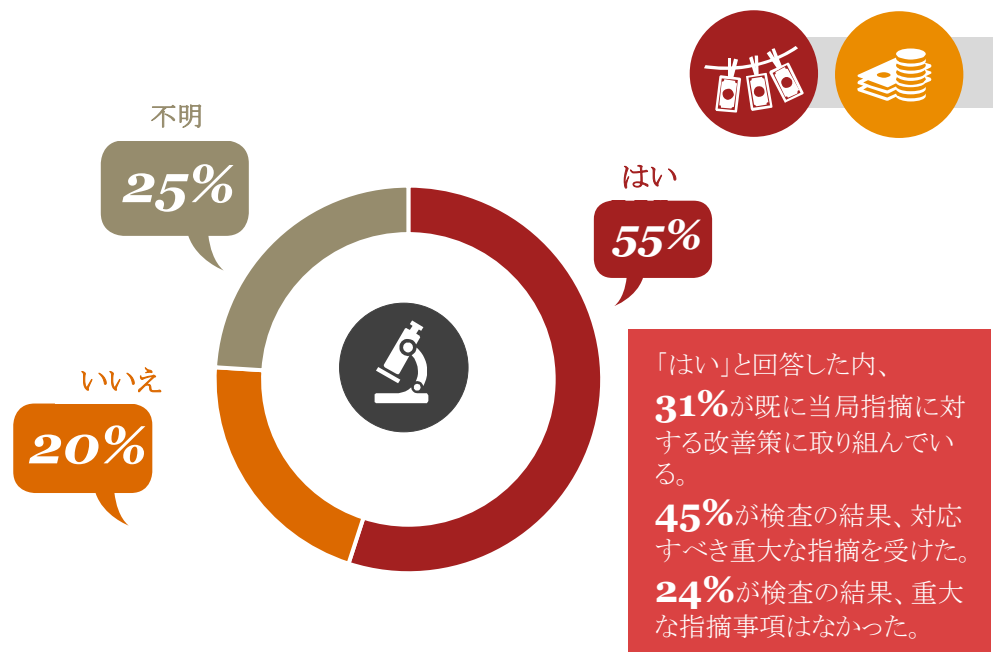
タイの金融機関の多くが、規制当局の監視が強まっている業界に対する顧客管理措置を強化することで、資金洗浄の検出・防止を図っている。一方で非定型的な取引慣行やパターンを特定するために専門解析ツールを利用している会社、並びに、高リスクの事業や国に関与する顧客の活動全般に係る詳細なレビューを定期的実施している会社は、それぞれ約40%にとどまった。また、約10%の会社は何ら措置を講じておらず、当該リスクを認知していない会社も存在することを示している。

顧客管理措置はリスク管理の重要な要素の一つであり、関連当事者の精査や最終的な真の受益者の特定を含むべきである。不法資金が流入する可能性が高い国境沿いの地域など高リスクの地域で活動する会社にとっては、このような手続きが特に重要となる。それら問題に対応するには専門解析ツールを活用し、商取引の非定型的な取引内容やパターンを特定することが推奨される。

貿易取引を利用した資金洗浄活動の検出・防止のための措置

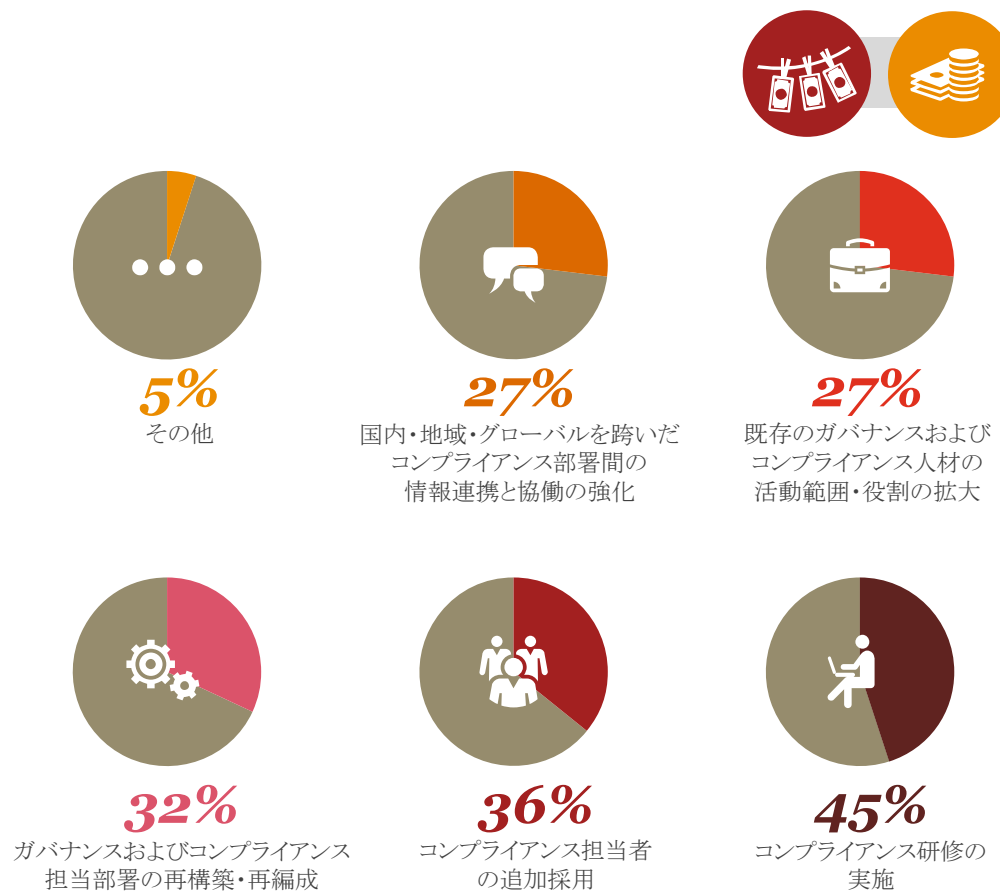


過去2年間で規制当局によるAMLに関する検査を受けたか？



回答企業の55%が規制当局による検査を受け、その内、76%が重大な指摘を受けている。検査を受けた金融機関の内、31%が既に当局指摘に対して既に改善策に取り組んでいるが、重大な指摘を受けている残りの45%についても、今後迅速な改善対応が求められている。

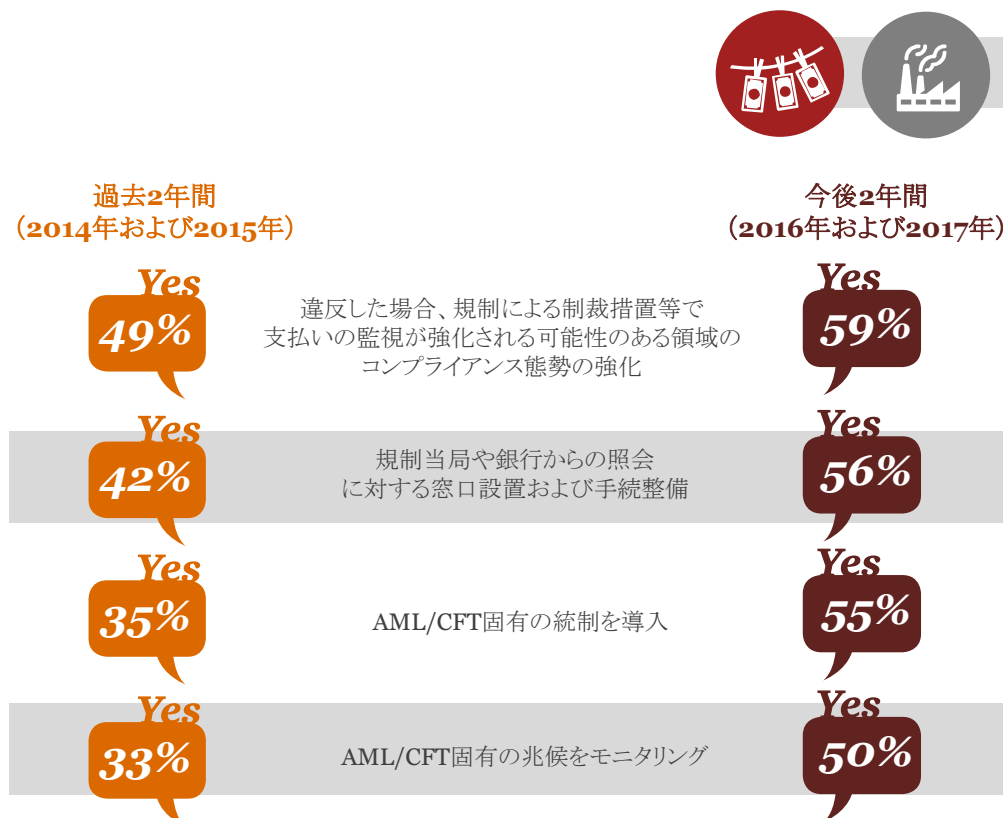
規制強化に対応するために過去2年間に新たに導入した
貿易取引を利用した資金洗浄活動の検出・防止策



近年の規制強化を受けて半数近くの45%が、コンプライアンス研修を実施していると回答している。また、36%の回答者が、AML／CFT、贈収賄防止、汚職防止や制裁措置など特定の規制に係るコンプライアンスを担当する人材を追加雇用した。

貿易取引を利用した資金洗浄関連取引を検出・防止するため、32%の金融機関がガバナンスおよびコンプライアンスを担当する部署を再編しており、それぞれ27%が、社内の情報連携または協働体制を改善し、現行のガバナンスおよびコンプライアンス担当者の活動範囲および役割を拡大したと回答している。

タイの非金融機関が実施した／実施する予定の対応策



金融機関以外についても、不動産業や宝石商を中心にAML/CFT対策への取り組みを強化している傾向にある。回答者の50-60%の企業が、今後2年間で、規制対象領域におけるコンプライアンス態勢強化、規制当局や銀行への対応手続き整備、AML/CFTに関連する統制を整備し、さらには疑わしい取引・活動のモニタリングをすると回答しており、これは過去2年間の実績から10-20%多くなっており、その注目度の高さが窺える。

貿易取引を利用した資金洗浄へのエクスポージャーを抑制するために
非金融機関で導入されている対応策



貿易取引を利用した資金洗浄のエクスポージャーを抑制するため特別に採用された対応策はない



インボイス・注文書および(または)送金の指示・送金内容の詳細など、第三者への支払い・第三者からの支払いに関連する統制を整備



特に明確なビジネス上の目的をもたない異常に複雑なディール・取引・支払いを禁止



取引関係開始時点でデュー・デリジェンスを実施



すべての取引先に関連するネガティブな情報をリアルタイムでモニタリング



貿易取引を利用した資金洗浄によりビジネスはリスクに晒されているかもしれないが、特段、措置は講じられていない。

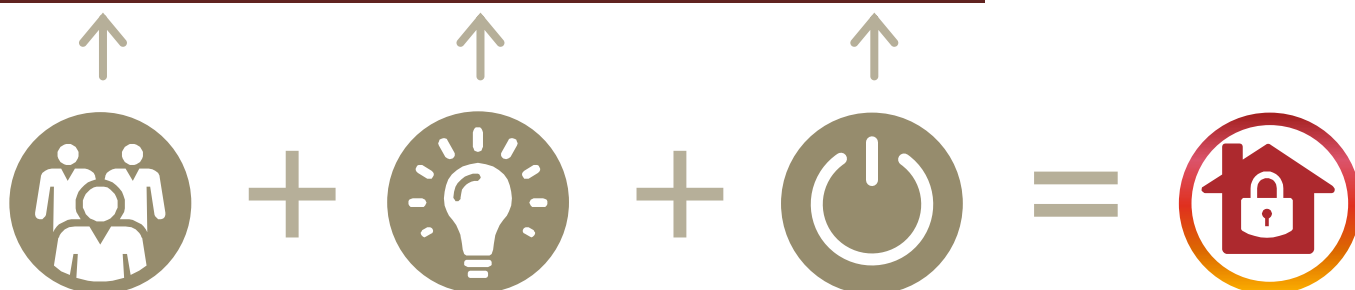
タイの非金融機関のうち34%が、貿易取引を利用した資金洗浄リスクを軽減するための対応策を講じていない。一方で、半数近くが、第三者との支払いに関連する内部統制を整備し、約3分の1が、異常に複雑な取引の禁止、取引開始時点でのデュー・デリジェンスを実施している。

AML規制上、すべての非金融機関が関連省庁の規制に規定される閾値を超える取引の報告を要求されているわけではなく、宝石商、自動車販売業者および不動産ブローカーのみが当該規制の対象となっている。しかしながら、その他の非金融機関についても、資金洗浄が経済犯罪を助長し、ビジネスの成長を阻害する可能性があることを認識し、自社のビジネスにおける当該リスクを検討してみてはいかがだろうか。

1. 明確な不正・汚職防止プログラムの整備
2. プログラムの導入・監視のための独立性のあるスタッフの任命
3. ポリシー・対応策の社内への通知徹底
4. 調査並びに不正対応のための情報の収集・精査
5. リスクマネジメント・コンプライアンスチームの強化
6. タイ固有の不正リスクにカスタマイズしたポリシーと組織
7. 公式な緊急有事対応策並びに是正対応策の整備

求められる行動

不正に対抗するための
7つのステップ



お問い合わせ先

Vorapong Sutanont

Partner

Tel: +66 (0) 2344 1429

Fax: +66 (0) 2286 4440

Email: vorapong.sutanont@th.pwc.com

魚住篤志 / Atsushi Uozumi

Partner

Tel: +66 (0) 2344 1157

Fax: +66 (0) 2286 2666

Email: atsushi.uozumi@th.pwc.com

www.pwc.com/th