内部監査人協会（ＩＩＡ）情報／ＣＢＯＫ調査結果

テクノロジーのトップ10リスクの舵取り
― 内部監査の役割 ―

著者：フィリップ・E. フローラ（ＣＩＡ，ＣＩＳＡ，ＣＦＥ，ＣＣＳＡ）
フロビズ＆アソシエイト, LLC　代表兼マネージングメンバー

サジャイ・ライ（ＣＰＡ，ＣＩＳＳＰ，ＣＩＳＭ）
セキュアリー・ヨアーズ, LLC　共同設立者兼オーナー

訳者：堺　　咲子
内部監査人協会（ＩＩＡ）国際本部　理事
内部監査人協会（ＩＩＡ）調査研究財団　理事・評議員
ＣＢＯＫ2015運営委員会委員　　実務家調査小委員会委員
インフィニティコンサルティング　代表
公認内部監査人（ＣＩＡ）　　内部統制評価指導士（ＣＣＳＡ）
公認金融監査人（ＣＦＳＡ）　　公認リスク管理監査人（ＣＲＭＡ）
米国公認会計士（ＣＰＡ（ＵＳＡ））

ＣＢＯＫについて

内部監査の国際的共通知識体系（ＣＢＯＫ）は、内部監査の実務家とその利害関係者を対象にした内部監査の専門職の世界最大規模の継続的調査である。2015年ＣＢＯＫ調査の主な内容の1つは、世界中の内部監査人の業務と特徴を包括的に調べた実務家調査である。この実務家調査プロジェクトは、内部監査人協会（ＩＩＡ）調査研究財団が2006年（回答数9,366）と2010年（回答数13,582）に実施した同調査を礎にしている。

本プロジェクトのレポートは、2016年７月まで毎月のペースで発表され、個人、専門家組織、ＩＩＡ支部からの寄付のおかげで、無料でダウンロードできる。次の３つの形式で25以上のレポートが発表される予定である。

１）コアレポート：広範なテーマを扱うレポート
２）詳細レポート：重要なテーマを深掘りするレポート
３）早わかり：特定の地域やテーマを扱うレポート

これらのレポートは、テクノロジー、リスク、素質等の８つの異なる側面から研究されている。

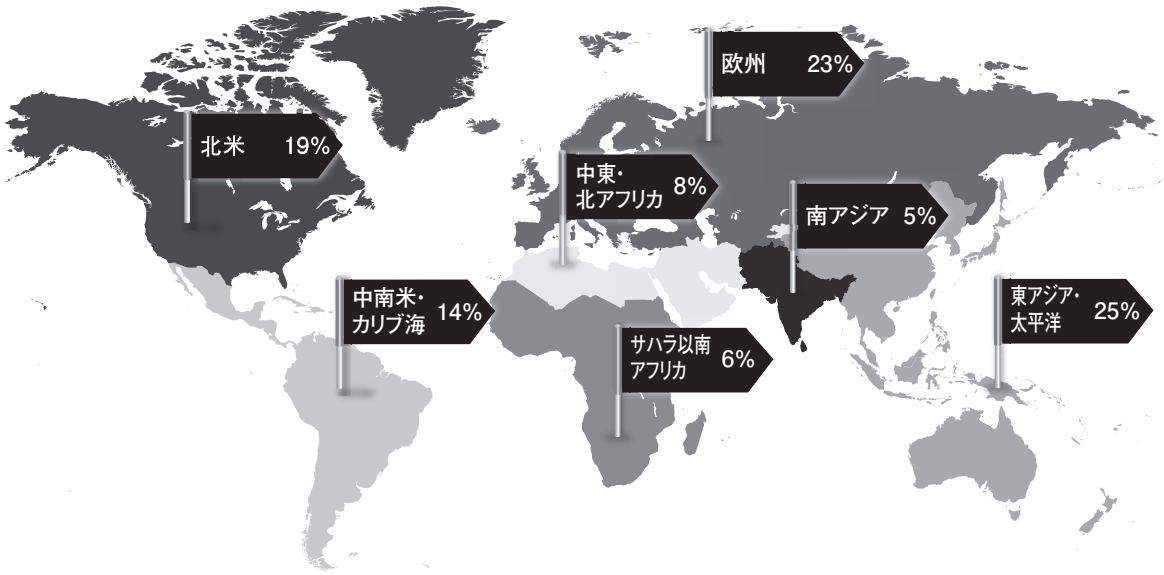
本調査の質問と最新のレポートは、ＩＩＡのホームページ内のCBOK Resource Exchange（英語）からダウンロードできる。

調査データ	
回答者数	14,518*
回答国数	166
調査言語数	23

回答者階層	
内部監査部門長（ＣＡＥ）	26％
ディレクター	13％
マネージャー	17％
スタッフ	44％

＊回答率は、質問によって異なる。

2015年ＣＢＯＫ実務家調査：地域別参加状況



注：地域区分は、世界銀行の分類によるものである。欧州には、中央アジアからの回答（１％未満）を含めている。調査回答期間は、2015年２月２日から４月１日までであった。オンラインによる調査ページへのリンクは、ＩＩＡ支部の電子メールリスト、ＩＩＡのホームページ、ニュースレター、ソーシャルメディアなどから配信された。回答者の基本情報が完全に回答されている限り、部分的な回答であっても分析に含めている。2015年ＣＢＯＫレポートの中では、具体的な質問は質問１、質問２のように表示している。本調査の全質問は、ＩＩＡのホームページ内のCBOK Resource Exchange（英語）からダウンロードできる。

目次

エグゼクティブ・サマリー …… 32
１．サイバーセキュリティ …… 32
２．情報セキュリティ …… 33
３．ＩＴシステム開発プロジェクト …… 35
４．ＩＴガバナンス …… 37
５．アウトソースしたＩＴ業務 …… 39
６．ソーシャルメディアの利用 …… 41
７．モバイルコンピューティング …… 42
８．内部監査人のＩＴスキル …… 44
９．新たなテクノロジー …… 46
10．取締役会と監査委員会のテクノロジー認識 …… 47
結論 …… 48

ＣＢＯＫの課題分野別のマーク

将来　グローバルな視点　ガバナンス　マネジメント　リスク　基準と資格　素質　テクノロジー

エグゼクティブ・サマリー

組織内の最も重要なテクノロジーリスクや新たに発生するテクノロジーリスクを適切に識別し管理しているか？　これはあらゆる組織の監査委員会や取締役会が自問している重要な質問の１つである。本レポートは、内部監査人、取締役、監査委員会に、現在の最も重大なテクノロジーリスクの舵取りに役立つ重要情報を提供する。

本レポートでは、以下について説明する。

- テクノロジーのトップ10リスク
- これらのリスクに関して内部監査人が尋ねるべき重要な質問
- テクノロジーリスクに対処するための重要な業務

トップ10リスクは、アフリカ、南米、中東、欧州、カナダ、米国の内部監査部門長（ＣＡＥｓ）と情報技術（ＩＴ）専門家へのインタビューをもとに決定した。また、テクノロジーリスクに関する全体像は、内部監査人の世界最大規模の調査である2015年ＣＢＯＫ内部監査の実務家国際調査に基づいている。リスクの順位については、ビジネスを行う市場によって優先順位が異なる場合がある。

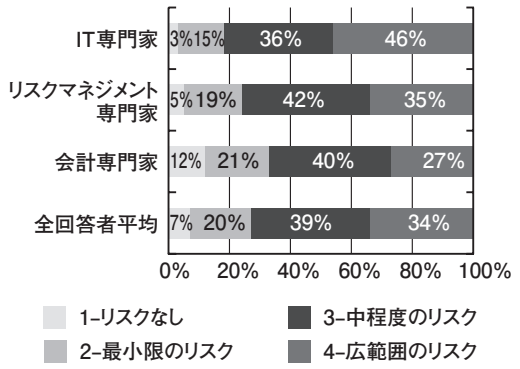
本レポートは、現在の、そして新たに発生する複雑なテクノロジー問題の迷路を案内するだけでなく、内部監査部門内のＩＴスキルの低さや取締役会の認識の欠如を原因とするリスクの組織的な面も検討する。

１．サイバーセキュリティ

サイバーセキュリティリスクは、経営幹部、内部監査人、監査委員会、取締役会の間で恐らく最も議論されているＩＴのテーマであるため、テクノロジーのトップ10リスクの第１位とする。

組織が直面する最大のサイバーセキュリティリスクの１つは、外部の攻撃者が機密データを盗む可能性である。大抵の組織は、そのようなデータ侵害が引き起こす組織のブランドや評判への損害を認識している。図表１はこのような心理を裏付けており、回答者の７割以上がデータ侵害のリスクを中程度または広範囲のリスクであると回答している。注目に値するのは、ＩＴ専門家がこのリスクをさらに高い（82％）と考えていることである。これは、ＩＴ専門家がテクノロジーをよく理解しており悪用され得る隙を知っているためだろう。

＜図表１＞組織のブランドを傷つけ得るデータ侵害のリスク水準



注：質問93「下記の新たな情報技術（IT）の分野について、あなたの組織の固有リスクの水準はどの程度ですか？」「該当なし・わからない」と回答した者は除外。四捨五入の関係で合計が100%にならないものもある。回答数＝1,038（IT）、1,139（リスクマネジメント）、1,678（会計）、9,426（全回答者）。

内部監査人の役割

内部監査人は、サイバーセキュリティリスクに適切に対処することを確実にするために、組織内で重要な役割を果たすことができる。行う業務や尋ねる可能性のある質問という観点での内部監査人の役割は、組織の規模によって異なることがある。小規模組織（従業員1,500人未満）では、５割の内部監査部門がサイバーセキュリティ関連の監査業務を全くまたは最小限しか行っていないのに対し、大規模組織では、４割の内部監査部門がサイバーセキュリティ関連の監査業務を広範囲に行っている（質問92、回答数＝9,929）。

多くのリーダーは、サイバーリスクに関して自らがどの程度のリスクを負っているかを理解していない。

米国、フューチャー・ポイント・オブ・ビュー，ＬＬＣ、パートナー
スコット・クロソスキー氏

内部監査人は、自社が社内外の経験を活かすためのプロセスを持つことを確実にすべきである。例えば、サイバーセキュリティや関連脅威と闘うための情報共有を目的として金融業界で広く利用されている『金融サービス情報共有分析センター』という国際組織を通じて、社外との協調が起こっている。

オレゴン州ポートランド、ユニタスコミュニティー・クレジットユニオン、最高リスク責任者、ＣＩＡ、ＣＦＥ、ＣＩＳＡ
ジェームス・アレクサンダー氏

内部監査人が尋ねるべき重要な質問

1．組織は不審なネットワーク侵入をモニターできるか？
2．組織は攻撃が起こっているかを識別できるか？
3．組織は攻撃を隔離して潜在的損害を抑えられるか？
4．組織は機密情報が無くなっているかを知ることができるか？
5．インシデント発生に備えて、危機管理計画文書は整備されているか？　また、計画はテストされており組織のリスクに合ったものになっているか？
6．インシデントが発生した場合、組織はインシデント対応を支援するフォレンジック（デジタル鑑識）スキルが利用できるか？
7．インシデント対応チームがあるか？彼らは役割と責任を理解しているか？

内部監査が行うべき重要な業務

1．外部に接続しているネットワークの脆弱性スキャンと侵入テストを独立的に毎年行う。
2．実際のインシデントにインシデント対応チームが備えるために、組織の危機管理計画に関するシミュレーションが行われているかを検証する。
3．ネットワークの方針と手続の遵守状況を判断するために、ネットワークアーキテクチャーの監査を行う。
4．直近のインシデントについて監査を行い、方針、手続、ツールが予定通りに適用されたか、また、インシデント中にフォレンジックの専門家が利用されたかを判断する。

２．情報セキュリティ

サイバーセキュリティはメディアの注目をかなり集めているが、情報セキュリティも同様に重要なので、テクノロジーのトップ10リスクの第２位とする。情報セキュリティとは、組織にとって重要な情報の機密性、完全性、可用性の保護を指している。

かつては、大抵の組織はネットワークペリメータ（境界）の保護に焦点を当て、セキュリティ予算のかなりの部分をペリメータ防御に費やし、ファイヤーウォール、侵入検知、侵入防止、コンテンツフィルタリング、ネットワークモニタリングなどのネットワークペリメータ機器へ投資した。しかし、最近の大規模なデータ侵害に関するあらゆるニュースから、ネットワークペリメータにのみ焦点を当てるのが正しい戦略でないことは明らかである。外部の攻撃者が組織のネットワークに侵入したいと思えば、彼らが方法を見つけて侵入してくるのは目に見えている。現在は、ネットワークペリメータに対するシングルレ

イヤーの防御ではなく、重要情報のマルチレイヤーの防御に重きを置いている。

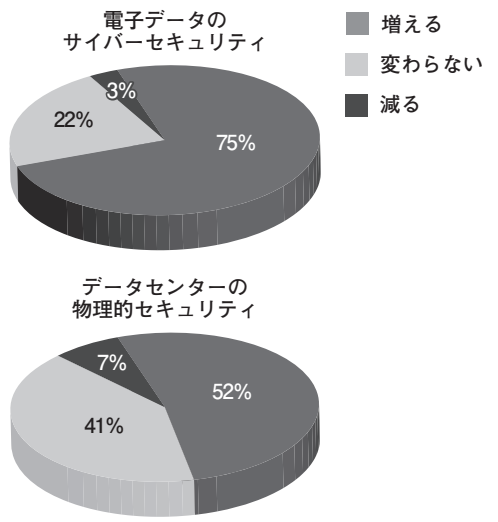
組織に優れた情報セキュリティプログラムがあれば、通常、プログラムに責任を負う最高情報セキュリティ責任者（ＣＩＳＯ）のような経営幹部を選任している。情報セキュリティプログラムには、最低でも次のことを盛り込むべきである。

- 厳格なリスク評価プロセス
- 効果的なガバナンスとコンプライアンスの手続
- 情報セキュリティ方針および基準の文書化と伝達
- 効果的なセキュリティ意識向上研修プログラム
- 効率的なアクセスコントロール手続
- テスト済みの災害復旧、事業継続、インシデント対応のプログラム
- 業務資産管理、ネットワーク管理、パッチ管理、変更管理のプロセス
- 厳重な物理的セキュリティ

内部監査の役割

内部監査は、組織の情報セキュリティプログラムが有効かつ効率的であることを確実にするための重要な役割を担っている。サイバーセキュリティ業務は恐らくより急速に増えるだろうが、内部監査計画には物理的セキュリティとサイバーセキュリティの両方を含め続けるべきである。図表２の通り、サイバーセキュリティ業務を増やす予定なのは回答者の75％以上であるのに対し、物理的セキュリティ業務を増やすのは52％である。

＜図表２＞



注：質問94「今後2～3年間で、これらの技術分野に関する内部監査業務は、増える、減るまたは変わらない、のどれだと思いますか？」回答数＝11,163。

従業員がリスク管理について知らされ措置を講じる権限を与えられない限り、組織的な情報セキュリティとリスクマネジメントによって重要なリスクを封じ込めることはできない。

ワールドビジョン・インターナショナル社、ＩＴ監査テクニカルディレクター
グレース・ルワンガ氏

内部監査人が尋ねるべき重要な質問

1．情報セキュリティ方針がレビューされ更新された直近の時期はいつか？
2．情報セキュリティ意識向上研修の成功率はどの程度か？　研修は強制参加か？　研修を修了していない者にはどのような影響があるか？
3．リスク評価を行った直近の時期はいつか？　新たな外部の取引先すべてについてリスク評価を実施したか？
4．組織はインシデントに対する準備状況を判断するためにシミュレーションを行ったか？
5．災害復旧計画のテストを行った直近の時期はいつか？　それは成功した

か？　どのような課題があったか？

6．組織が遵守しなければならない要件には何があるか？　例えば、米国医療保険の携行性と責任に関する法律（ＨＩＰＡＡ）、2002年サーベンス・オクスリー法（ＳＯＸ）、クレジットカードの国際セキュリティ基準は該当するか？

7．外部の攻撃者はソーシャルエンジニアリングを使って物理的パラメータに侵入できるか？（この種の侵入の例には、攻撃者が建物の外で従業員と気楽な会話を始め、その従業員が入館バッジをスキャンして建物に入る時に従業員の後に続いて建物に侵入するなどがある。）

8．組織は特権ユーザ（ＩＴ環境を管理するための管理者権限を持つユーザ）の活動を記録しモニターしているか？

内部監査が行うべき重要な業務

1．内部ネットワークの脆弱性スキャンを実行する。

2．アクセスコントロールのレビュープロセスをレビューする。オーナーは実際にアクセスリストをレビューしているか？　あるいはレビューは実際にリストを見ずに「承認」するという形骸化したコンプライアンス儀式になっているか？

3．第三者を使って攻撃のシミュレーションを行い、結果を監査する。例えば、フィッシングメールを使って意識向上研修プログラムの有効性を判断する（中・大規模組織）。

4．重要情報のバックアップ状況を監査し、バックアップが定期的に行われているかを検証する。

5．特権ユーザの活動を監査し、承認された者のみが特権機能を持っているかを検証する。さらに、特権ユーザの活動が記録されモニターされているかを検証する。

6．組織の重要資産にアクセスを持つ第三者を監査する。または、第三者の保証業務基準（ＳＳＡＥ）第16号[1]の報告書をレビューする（大規模組織）。

３．ＩＴシステム開発プロジェクト

ＩＴ予算の大部分はシステム開発プロジェクトに費やされるため、テクノロジーのトップ10リスクの第３位とする。ほぼすべての組織が生き残りのためにテクノロジーシステムの開発や更新を必要としている。しかし残念ながら成功率は低い。スタンディッシュ・グループが発行するＣＨＡＯＳレポートによると、ＩＴシステム開発プロジェクトの長期間の実績は以下の通りである。

- 全体の成功率：16.2％
- 重大な問題が発生したプロジェクト：52.7％
- 障害（中止）：31.1％

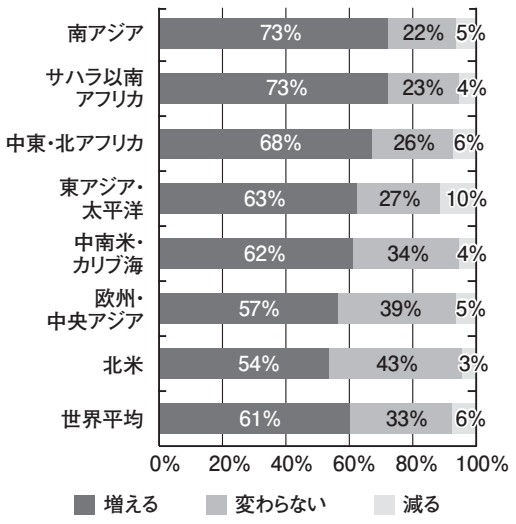
また、ある研究の予測によると、ソフトウエア開発失敗のコストは年間500～800億ドルにもなる[2]。

調査回答者の大部分は、主要プロジェクトの監査やプロジェクトマネジメントのアシュアランスの継続や増加の重要性を認識しており（図表３参照）、全回答者の６割が、これらの監査の増加を予測している。

[1] 訳者注：米国公認会計士協会が策定した受託業務を行う会社の内部統制の有効性を評価する保証業務基準書第16号のこと。日本においては日本公認会計士協会が監査・保証実務委員会実務指針第86号を定めている。

[2] *CIO Journal*, January 2014. *The Wall Street Journal*からの引用。

＜図表３＞



注：質問94「今後2～3年間で、これらの技術分野に関する内部監査業務は、増える、減るまたは変わらない、のどれだと思いますか？」のうち「主要プロジェクトの監査・プロジェクトマネジメントのアシュアランス」に回答した者。回答数＝11,019。

主要システムプロジェクトの目的は、開発期間中および導入後もモニターされなければならない。多くの組織で達成されなかったプロジェクト目的の例には、期限に間に合わない、費用超過、期待通りの効率性が達成されていない、導入前にテストされなかったソフトウエアの不具合、当初の計画から削減された統合範囲、プロジェクト承認時にビジネスケースで特定した機能が十分に装備されていない、などがある。

最後に、もう１つの重要な問題はリーダーシップの弱さであり、これはさまざまな段階でプロジェクトを弱体化させ得る。リーダーシップが弱くなる一般的な要因には、次のようなものがある。

- 経営幹部レベルのプロジェクトチャンピオンの支援が限られているか積極的な関与がない。
- ビジネスアナリストの能力が低いか適切に訓練されていない。
- リスクマネジメントの能力が低いか不十分。
- プロジェクトマネジャーまたは経営者の能力が低いか経験不足。
- プロジェクト運営委員会が効果的でない。

内部監査人の役割

内部監査は、システム開発ライフサイクル（ＳＤＬＣ）の各段階の監査実施を検討すべきである。ＳＤＬＣの代表的な内容には、実現性検証、要件検証、要件定義、詳細設計、プログラミング、テスト、インストール、導入後レビューが含まれる[3]。

> 組織は、あらゆるシステム開発の失敗から素早く学習する必要があり、そうすれば事業体の主要アプリケーションの開発と導入をもっとうまくできるようになる。
>
> オハイオ州内部監査室ＩＴ監査主任
> エドワード・カー氏

期待ギャップ

ＩＴシステム開発プロジェクトが経営者の期待に応えられない一般的な理由には、以下のようなものがある。

- 導入期限の強制（プロジェクトチームが適切な計画やプロジェクト予測技法を実施する前に、プロジェクト完了日が設定されている）
- 非現実的な期待
- 期待とリソースが釣り合わない
- プロジェクトの実績低迷の影響が常に当てはまるわけではない
- 不規則・不正確な状況報告（アーンドバリュー法が用いられていない）

内部監査人が尋ねるべき重要な質問

１．プロジェクトは組織内でどのように承認されているか？

２．プロジェクトは組織内でどのように

[3] ISACA Glossary of Terms 参照。www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

開始されているか？
3．プロジェクトは組織内でどのように管理されているか？
4．主要プロジェクトには経営幹部のチャンピオンがいるか？
5．プロジェクト運営委員会があり、定期的に会議が行われているか？
6．プロジェクト開発にベンダーが関与している場合、契約管理プロセスはどうなっているか？
7．月次状況報告書は作成されているか？
8．プロジェクト予算の超過または期限の延長の場合、組織内で取るべきプロセスは何か？
9．プロジェクトの目的が達成されない場合に、プロジェクトを中止するプロセスが組織内にあるか？
10．ＩＴ組織は、ＩＴプロジェクトの結果とコストに対するユーザの満足度調査を行っているか？

内部監査が行うべき重要な業務

1．主要ＩＴシステム開発プロジェクトのライフサイクルを通した監査を行う。ライフサイクルには、契約遵守、プロジェクト管理、コスト（ベンダーの要員配置・請求など）、プロジェクト進捗、変更注文、インセンティブ・ボーナスプログラム等が含まれる。
2．監査回数を減らしたり追加知識を得るために、ベンダーの監査・品質チームとともにプロジェクト監査に参加する。これによりプロジェクトの中断も最小になる。
3．組織のプロジェクト管理手法についての監査を行う。
4．プロジェクトのポートフォリオをレビューし、特に予算超過または期限延長のプロジェクトについて、管理手法に従っているかを監査する。
5．プロジェクトの範囲および成果物の変更に関して、ユーザが関与しているかを検証する。
6．プロジェクト完了後、ＩＴ組織が行ったユーザ満足度調査の結果をレビューする。あるいは、ＩＴ組織が提示した結果を検証するために、独自のユーザ満足度調査を行う。
7．事後分析や教訓を生かす活動が行われ、今後のプロジェクトプロセス改善に利用されているかを判断する。

詳細は、ＩＩＡのホームページ内のStandards & Guidance の *GTAG12: Auditing IT Projects*, 2009を参照。

4．ＩＴガバナンス

昨今の企業スキャンダルを受けて、コーポレートガバナンスだけではなくＩＴガバナンスも激しい非難に晒されているため、テクノロジーのトップ10リスクの第４位とする。

多くの組織で経営者はＩＴに費やした金額に疑問を抱いており、ＩＴコストのモニタリングの重要性が高まっている。ＩＴ側が考えるビジネスニーズとビジネス側が考えるＩＴにできることのギャップが広がっていることも、モニタリングの重要性が高まっている理由である。優れたＩＴガバナンスには、最低でも次の３つの要素がなくてはならない。

- ビジネスとの明確な調和
- 測定可能な価値のビジネスへの提供
- リソース、リスク、実績、コストの責任ある管理

回答者の３割は、ＩＴガバナンスに関連する内部監査活動を全くまたは最小限しかしていないと回答しており、懸念される分野である（図表４参照）。テクノロジーにかけた費用と顧客や業務に対する影響を考えると、ほ

ぼすべての内部監査部門がＩＴガバナンスに関連する活動を最低でも中程度はすべきである。回答者の中で最も広範囲にＩＴガバナンスに関連する活動を行っているのは南アジアであり、回答者の８割が中程度または広範囲に活動していると回答している。

内部監査の役割

内部監査は、ＩＴがうまく機能しており組織のリスク許容度に基づいてリスクを低減する適切なコントロールが整備されているというアシュアランスを提供することによって、組織に役立つことができる。同様に重要なもう１つのビジネス目的は、ビジネスを推進する機会を活かすようなＩＴインフラが整備されることである。

小規模な内部監査部門は、ＩＴガバナンスに関連するレビューに時間を割くことが難しいようである。３名以下の内部監査部門では、４割がＩＴガバナンスに関連する活動を全くまたは最小限しかしていないと回答している（図表５）。

ＩＴガバナンスの定義

全社的な情報技術（ＩＴ）が組織体の戦略や目標を支援することを確実にするリーダーシップ、組織構造、プロセスから構成される。

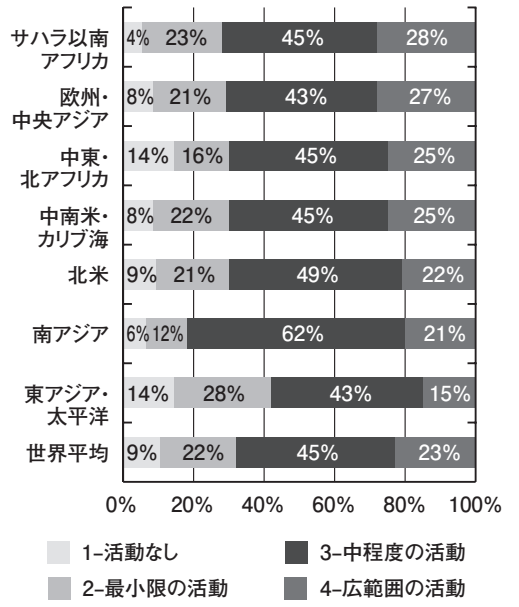
―専門職的実施の国際フレームワーク 2013年版より

有効なＩＴガバナンスの構成要素

- 組織体制とガバナンス体制
- 経営幹部のリーダーシップと支援
- 戦略計画と業務計画
- サービス提供と業績測定
- ＩＴ組織とリスクマネジメント

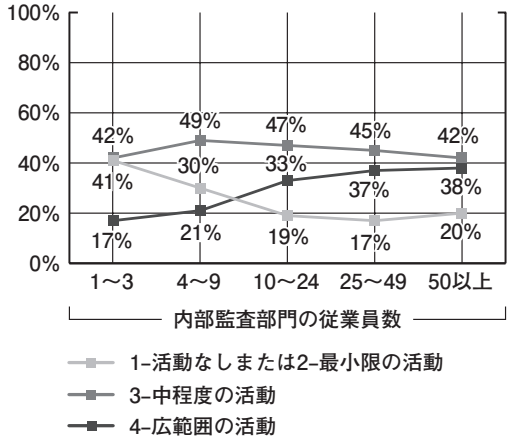
―*GTAG 17: Auditing IT Governance* (Altamonte Springs, FL: The Institute of Internal Auditors, July 2012).

＜図表４＞ＩＴガバナンスに関連する活動



注：質問72「あなたの内部監査部門がガバナンスレビューに関連する活動に関わる範囲はどの程度ですか？」のうち「特に組織の情報技術（IT）利用に関連するガバナンスの方針および手続のレビュー」に回答した者。CAEのみ回答。「該当なし・わからない」と回答した者は計算から除外。回答数＝2,545。

＜図表５＞内部監査部門の規模と比較したＩＴガバナンスに関連する活動



注：質問72「あなたの内部監査部門がガバナンスレビューに関連する活動に関わる範囲はどの程度ですか？」のうち「特に組織の情報技術（IT）利用に関連するガバナンスの方針および手続のレビュー」に回答した者。CAEのみ回答。「該当なし・わからない」と回答した者は計算から除外。回答数＝2,497。

ＩＴガバナンス監査の計画方法

ＩＴガバナンス監査の範囲を決定し実施するために内部監査実施チームがすべ

きことは次の通りである。

- ＩＴ機能が組織の目的と戦略に整合しているか、また理解しているかを判断する。
- ＩＴリソースと業績管理の有効性を判断する。
- ＩＴ環境に不利な影響を及ぼす恐れのあるリスクを評価する。

—*GTAG 17: Auditing IT Governance* (Altamonte Springs, FL: The Institute of Internal Auditors, July 2012), 15.

内部監査人が尋ねるべき重要な質問

1．ビジネスと調和するためにＩＴはどのような活動をしているか？　ビジネスニーズを理解するためにＩＴがビジネス側と会う頻度はどのくらいか？
2．ＩＴの能力と実績についてビジネス側はどのように見ているか？
3．ビジネスに提供している価値についてＩＴはどのように判断しているか？
4．ＩＴ担当役員は、ＩＴに雇う適正人数をどのように決定しているか？
5．ＩＴは、ＩＴリスク評価を定期的に行っているか？
6．ＩＴは自らの業績測定のための主要業績評価基準を持っているか？
7．ＩＴはコストをどのように管理しているか？

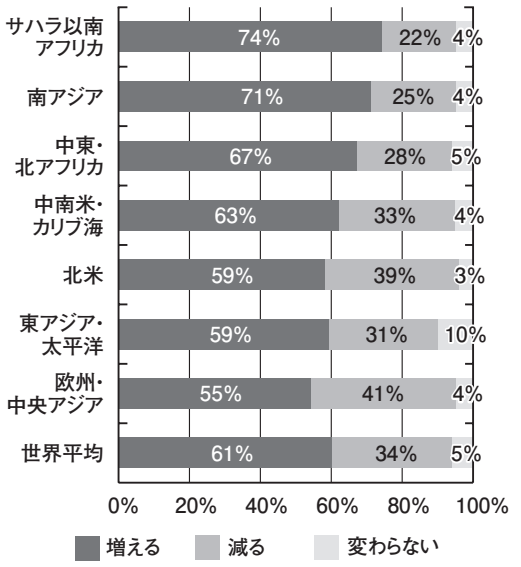
内部監査が行うべき重要な業務

1．企業文化、定められた業績評価基準や期待、サービス内容合意書（ＳＬＡｓ）、顧客サービス等に関するＩＴ組織の「トップの気風」を評価する。
2．ＩＴ機能が組織の戦略的優先順位と整合しているか、また理解しているかを判断するために、定期的に監査する。
3．ＩＴリソースと業績管理の有効性をレビューする。
4．ＩＴ環境に好ましくない影響を及ぼす恐れのあるリスクを評価する。
5．ＩＴ環境内で用いられているコスト指標を監査する。
6．ＩＴの能力と実績についてビジネスリーダーがどのように見ているか調査する。
7．組織内のコンプライアンスプログラムと次のような確立されたフレームワークを必要に応じて比較する（大規模組織）。
   - ✓Control Objectives for Information and Related Technology（COBIT）
   - ✓トレッドウェイ委員会支援組織委員会（COSO）
   - ✓National Institute of Standards and Technology（NIST）
   - ✓国際標準化機構（ISO）27001, 27002

５．アウトソースしたＩＴ業務

前章で述べた通り、ＩＴコストへの注目が増した結果、主要なＩＴ業務のいくつかはアウトソースされた。そのためＩＴガバナンスが一層注目され、テクノロジーのトップ10リスクの第５位にアウトソースしたＩＴ業務が押し上げられた。アウトソースしたＩＴ業務は、障害が発生するまで発見できないというリスクに組織を晒し得る。アウトソースによって、組織の不可欠なテクノロジープロセスが直接管理外に置かれることもある。平均して調査回答者の６割が、今後ＩＴ業務のアウトソースが増えるだろうと回答している（図表６）。増えると回答した割合が最も高いのはサハラ以南アフリカであり、最も低いのは欧州である。

＜図表６＞アウトソースしたＩＴ業務の今後の監査



注：質問「今後2～3年間で、これらの技術分野に関する内部監査業務は、増える、減るまたは変わらない、のどれだと思いますか？」のうち「第三者またはアウトソーシングサービスを含むITの調達の監査」に回答した者。回答数＝11,020。

内部監査の役割

内部監査人は、アウトソースの早い段階で関与することでアウトソースの問題のいくつかを防止することができる。例えば内部監査は契約締結時に、監督、モニタリング、監査、物理的・論理的セキュリティ、適切な人員配置、担当者、情報へのアクセス、事業継続計画・災害復旧、ＳＬＡｓ、報告などが契約書に適切に盛り込まれるようにすべきである。

> ＩＴ業務をアウトソースするということは、あなたの王国への鍵を誰かに渡して、彼らがあなたと同じように情報を管理することを期待し信頼するのと同じことである。
>
> アシュランド社、ＩＴコンプライアンス・マネージャー、ＣＩＳＳＰ、ＣＩＳＡ
> ドリュー・ペリー氏

内部監査人が尋ねるべき重要な質問

１．アウトソースした業務は、組織にとって重要なものか？
２．組織には明確に定義されたアウトソース戦略があるか？
３．アウトソースした業務に関するガバナンス体制はどのようなものか？　役割と責任は明確に定められているか？
４．アウトソース時に詳細なリスク分析は行われたか？　また、定期的にリスク分析を行っているか？
５．アウトソースした業務について、正式な契約書またはＳＬＡｓが締結されているか？
６．アウトソース先の業績をモニタリングするための主要業績指標（ＫＰＩｓ）は、ＳＬＡに明確に定められているか？
７．契約書またはＳＬＡへの遵守状況はどのようにモニターされるか？
８．ＳＬＡを遵守していない場合に対応するために用いる仕組みはどのようなものか？
９．データシステム、通信システム、オペレーティングシステム、ユーティリティソフトウエア、アプリケーションソフトウエアの所有責任は明確に定められサービスプロバイダーと合意されているか？
10．サービスプロバイダーの内部統制の有効性に関するアシュアランスを得るプロセスはどのようになっているか？

内部監査が行うべき重要な業務

１．アウトソース契約プロセスの初期段階に関与する。
２．外部のサービスプロバイダーの監査を行い、彼らのＳＬＡとＫＰＩｓをレビューする。
３．契約や合意への非遵守があったアウトソース先の業務をレビューし、適切な措置が講じられたかを判断する。

4．アウトソース先が提供したすべてのソースコードにマルウエアがないかスキャンすることを確実にする。
5．アウトソースすべきＩＴ要素を組織が決めるための意思決定プロセスを監査する。
6．既存の主要なサービスプロバイダーを選定し、サービスプロバイダー選定前に実施したリスク評価をレビューする。

参考文献

Auditing Outsourced Functions, 2nd Edition, by Mark Salamasick（Altamonte Springs, FL: The Institutes of Internal Auditors Research Foundation, 2012）.

GTAG 7: Information Technology Outsourcing, 2nd Edition（Altamonte Springs, FL: The Institutes of Internal Auditors, 2012）.

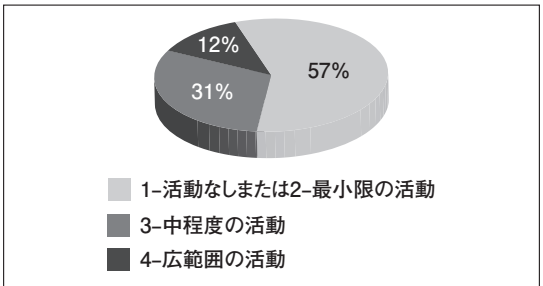
６．ソーシャルメディアの利用

ソーシャルメディアがメッセージを拡散するスピードは、組織によるソーシャルメディアの方針と手続の制定を促した。そのため、ソーシャルメディアの利用をトップ10リスクの第６位とする。ソーシャルメディア方針は、主として従業員が利用できるソーシャルメディアツールの利用方法とソーシャルメディアで共有できる内容の制限に主眼を置いている。従業員が方針に違反して有害なメッセージを投稿すると、組織には次のようなリスクがある。

- 名誉棄損、ハラスメント、プライバシーの侵害などの法的責任のエクスポージャー
- 競争力に影響し得る機密情報等の漏洩
- 虚偽の、抽象的な、または不注意なコミュニケーションを通じた組織の評判の毀損

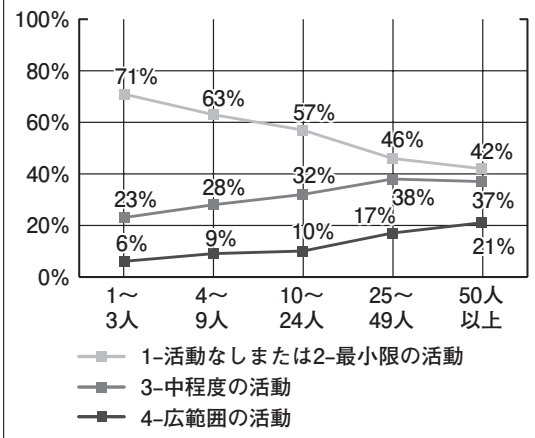
図表７の通り、従業員のソーシャルメディアの利用についてのアシュアランス活動は、現在極めて低い割合でしか行われていない。回答者の約６割は、活動を全くまたは最小限しか行っていない。広範囲に活動しているのは、回答者のわずか１割である。大規模な内部監査部門の方が、ソーシャルメディアのアシュアランス活動をより多く行っているようである（図表８参照）。とは言っても、大規模な内部監査部門の４割は、この分野の活動を全くまたは最小限しか行っていない。

＜図表７＞従業員のソーシャルメディア利用についてのアシュアランス



注：質問92「特に情報技術（IT）のセキュリティについて、下記の分野に関連する内部監査業務の範囲はどの程度ですか？」「該当なし・わからない」と回答した者は計算から除外。回答数＝9,747。

＜図表８＞内部監査部門の規模と比較したソーシャルメディア利用についてのアシュアランス



注：質問92「特に情報技術（IT）のセキュリティについて、下記の分野に関連する内部監査業務の範囲はどの程度ですか？」のうち「従業員が組織に関するソーシャルメディアを利用する方法についての組織の手続の監査」に回答した者。「該当なし・わからない」と回答した者は計算から除外。回答数＝8,980。

参考文献

Auditing Social Media: A Governance and Risk Guide by Peter Scott and Mike Jacka（John Wiley & Sons with The IIA, 2011）.[4]

ソーシャルメディアのリスクに対処するには、組織はソーシャルメディア手続の一部に次のステップを含めなければならない。

1．ソーシャルメディアのビジネス利用に関する適切な方針を定める。
2．セキュリティ意識向上研修のプログラムを通じて方針を伝達する。
3．Web 2.0のようなテクノロジー用の「コンテンツフィルタリング」ソフトウエアの利用を通じて方針を実施する。
4．方針が守られることを確実にするために結果をモニタリングする。
5．方針に違反した者に対して方針の遵守を強制する。

内部監査の役割

内部監査人は、ソーシャルメディアに関するリスク管理において重要な役割を果たすことができる。内部監査人は、組織が上記のステップを実施する際に、コンサルタントの役割が果たせる。また、内部監査は、年間監査計画の一部としてソーシャルメディア監査を含めることを検討すべきである。

内部監査人が尋ねるべき重要な質問

1．組織は取引先や顧客との連絡にソーシャルメディアをどのように利用しているか？
2．ソーシャルメディアサイトに投稿を許可しているコンテンツは何か？
3．ソーシャルメディアサイトに実際に投稿されたコンテンツのモニタリング（ソーシャルメディアサイトのスキャン実施）に責任を負うグループまたは個人はいるか？
4．「コンテンツフィルタリング」ソフトウエアでモニタリングしているのはどのようなコンテンツか？　ソフトウエアが発する警告をモニターするのは誰か？
5．ソーシャルメディア方針に違反した従業員は、どのような処分を受けるか？

内部監査が行うべき重要な業務

1．ソーシャルメディアの方針と手続の監査を行う。
2．ソーシャルメディアの話題が確実に盛り込まれるように、意識向上研修プログラムの妥当性をレビューする。
3．コンテンツの出入りをモニターする「コンテンツフィルタリング」ソフトウエアの利用状況とその有効性を理解する。
4．利用可能な組織のコンテンツを見つけるために、ソーシャルメディアサイトの独立的なスキャンを実施する。

7．モバイルコンピューティング

モバイル機器の普及およびテクノロジー、外観、アプリケーションの向上は、労働力に大変革をもたらし「モバイルコンピューティングとモバイルワーカー」という言葉に新たな意味を持たせた。したがって、モバイルコンピューティングをトップ10リスクの第７位とする。以前のモバイルワーカーは、ラップ

[4] 訳者注：櫻井通晴・伊藤和憲・吉武一監訳『ソーシャルメディア戦略－ガバナンス, リスク, 内部監査－』日本内部監査協会、2013年

トップを組織のネットワークにリモート接続して仕事をするのが一般的であった。現在のモバイルワーカーは、ビジネス用に開発されたアプリケーションを搭載したスマートフォンやタブレット端末のようなモバイル機器を活かして仕事をするのが一般的である。

モバイル機器は業務用ユーザに、携帯コンピュータ、Wi-Fiや携帯電話によるインターネットアクセス、公私兼用端末をもたらした。同時に、私物か会社貸与かを問わずモバイル機器は、リスク管理に対するＩＴ部門の伝統的なアプローチに難題を与えるような多種多様な機器やネットワークコンフィギュレーションのリスクをもたらした。

セキュリティリスク

モバイル機器に保存されている情報には、個人データと組織のデータが含まれ得る。この機器が紛失または盗難に遭う、ユーザが機器から組織のデータを削除せずに離職する、適切なセキュリティコントロールが整備されていないか意図した通りに運用されていない、といった場合には、情報漏えいが起こる可能性がある。

コンプライアンスリスク

個人所有の機器持ち込み（ＢＹＯＤ）の到来とともに、組織はユーザが方針と手続を遵守することに大きく依拠している。方針と手続には、ソフトウエアやオペレーティングシステムのアップデートのガイドラインのようなものがある。アップデートが頻繁すぎるとか機器のパフォーマンス低下になると考えるユーザは、アップデートをしないまたはコントロールを無視する可能性がある。

プライバシーリスク

ＢＹＯＤｓは組織と従業員という双方の観点で、プライバシー侵害の懸念を増す恐れがある。例えば、スマート機器に個人情報が保存されていたりその情報にアクセスされたりする場合には、組織が利害関係者のプライバシーを保護することが一層難しくなるだろう。反対に、従業員はスマート機器が組織によって侵害的な監視をされる、または、組織が組織情報を個人の機器から削除する際に誤って個人の情報（例えば、写真や連絡先など）を削除してしまうなどのプライバシー上の懸念を持つ可能性がある。

管理リスク

ＢＹＯＤｓは、広範囲なＩＴサポートサービスの管理を必要とする。機器の種類が増えるにつれて、ネットワークの潜在的な脆弱性も増してくる。さらに、機器がアップグレードされると、機器を適切に廃棄するための管理リスクも増える。ＢＹＯＤｓが外部のサービスプロバイダーにも適用される場合には、サービスプロバイダーのＢＹＯＤ機器上にある組織データの管理も、管理リスクの増加につながる。

法的リスク

組織は、スマート機器に保存されたデータに関して、どのように訴訟が行われどのように電子証拠開示要件が適用されるかといった法的要件を理解する必要がある。

内部監査の役割

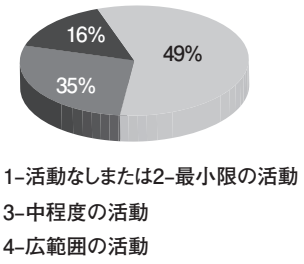
図表９の通り、内部監査部門の51％しかモバイル機器のアシュアランス業務を中程度または広範囲に行っておらず、約半数はこの分野について全くまたは最小限の活動しかしていないことを意味している。

> 情報はユーザとともに移動するため、モバイル機器内のセキュリティ・データは本社のものと同様に厳重に扱われなければならない。タブレット端末、パソコン、携帯電話、スマート時計等は、会社

の戦略情報の大部分が保存されている小さなデータセンター（または、中央サーバを攻撃するのに十分なデータ）である。紛失や盗難に遭った機器の量が事態を悪化させている。

テレフォニカ・デ・アルゼンチナル社、内部監査部門長
アレジャンドロ・レンバド・メンディサーバル氏

＜図表９＞モバイル機器の利用についてのアシュアランス



注：質問92「特に情報技術（IT）のセキュリティについて、下記の分野に関連する内部監査業務の範囲はどの程度ですか？」

内部監査人が尋ねるべき重要な質問

1．組織にはすべてのモバイルコンピューティング機器の棚卸をするプロセスがあるか？
2．組織はモバイルコンピューティング機器の紛失や盗難をどのように管理しているか？
3．組織はＢＹＯＤｓをどのように管理しているか？
4．組織は従業員離職時にモバイル機器のコンテンツをどのように管理しているか？
5．モバイル機器は暗号化されているか？

内部監査が行うべき重要な業務

1．モバイルコンピューティング機器の棚卸プロセスを監査する。
2．モバイルコンピューティング機器の紛失や盗難の管理方法を監査する。
3．モバイル機器に保存できる情報の種類を組織が決める方法を理解する。
4．機密情報がモバイル機器に保存されていないか、または、機密情報が暗号化されているかを検証する。

アフリカと中東の一部ではオンラインバンキングに携帯電話が広く利用されているため、他の地域に比べてオンラインバンキングのリスクが高い。

ワールドビジョン・インターナショナル社、ＩＴ監査テクニカルディレクター
グレース・ルワンガ氏

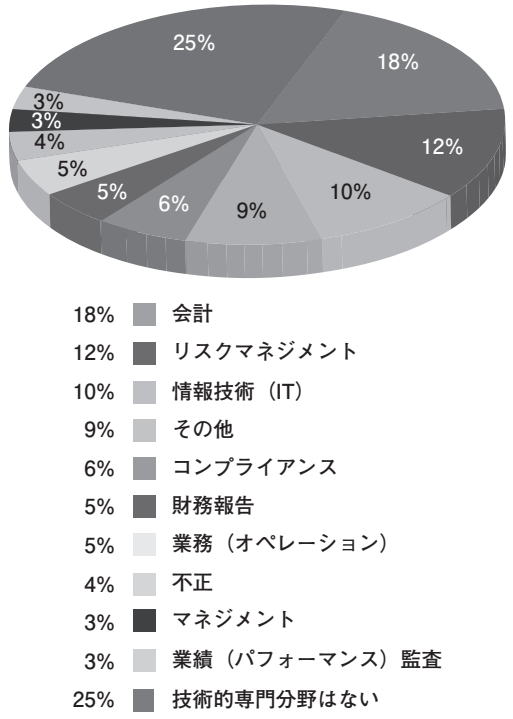
８．内部監査人のＩＴスキル

有能なＩＴ監査人の数の確保は内部監査にとって継続的な課題であるため、テクノロジーのトップ10リスクの第８位とする。回答者のうちＩＴの専門家はわずか１割である（図表10参照）。これには多くの理由があるが、「一般的な理由としては、ＩＴの専門家は新たなテクノロジーを活かしてＩＴ監査人よりも高い給料を要求する機会があるからだ。」とテキサスシステム大学監査学術研究機関エグゼクティブディレクターのマーク・サラマンシック氏は語る。「テクノロジーの経歴や専門知識のある監査人の給料は一般的にＩＴ職より低いので、多くの組織でＩＴ監査スキルのある監査人が不足している。」

ＩＴスキルのある監査人を増やす方法の１つは、ＩＴの適性のある業務・財務監査人にＩＴの研修をすることである。しかし、内部監査部門内で訓練された監査スタッフにとってＩＴ部門や経営陣の信頼を得ることは難しいかもしれない。プロティビティ中東ＩＴコンサルティングサービスのマネージングディレクター、スダーサン・ジャヤラマン氏は、

「ＩＴ監査人は、ハイリスクの監査業務をうまく実施するために、より専門的なスキルが必要である。ＩＴ専門家としての経験を含む高度なスキルをＩＴ監査人が持っていなければ、経営陣はＩＴ監査人のスキルや監査結果に大抵不安を感じる。」とコメントした。

＜図表10＞調査回答者の技術的専門分野



注：質問11「一般的な内部監査業務に加えて、正式な研修受けておりあなたの仕事の大部分を費やしている技術的専門分野はありますか？」回答数＝13,144。

内部監査の役割

内部監査は、部門内のＩＴスキルの不足への対策を講じることができる。そのためにはまず、以下に従って部門内で不足しているＩＴスキルの棚卸をする。

1．組織内で利用しているテクノロジーの種類を理解する。
2．組織内で利用しているテクノロジーと部門内のテクノロジースキルのマッピングをする。
3．内部監査がカバーしていないすべてのテクノロジーについて、スキルギャップを特定する。

ギャップが特定できれば、内部監査にはギャップを埋めるための選択肢がある。

選択肢１：適切に予算を配分して研修を行い、部門内でスキルを磨く。

選択肢２：最高情報責任者（ＣＩＯ）とともに、ＩＴスキルを持つ人材をローテーションするプロセスを導入する。

選択肢３：外部のサービスプロバイダーにアウトソースまたはコソースして、ＩＴスキルギャップを埋める。

内部監査人が尋ねるべき重要な質問

以下の６つの措置は、内部監査とＩＴ部門の関係構築およびＩＴプロセス全般に対する意識向上に役立つ。

1．主要なＩＴスタッフと関係を構築し、ＩＴ監査が組織にどのような価値を与えるかを実証する。
2．重要なＩＴの課題とリスクをよりよく理解するために、主要なＩＴ会議（例：ＩＴシステム開発運営委員会、情報セキュリティ最新情報伝達会、新たなテクノロジー会議等）に出席する。
3．最高テクノロジー責任者（ＣＴＯ）やＣＩＳＯを含め、ＩＴの主要メンバーと定期的に会合を持つ。
4．ＩＴスキルの向上と経営陣からの信頼を得るために、テクノロジーの経歴を持つ監査人を採用する。
5．ＩＴガバナンス監査を行う。
6．業務の重複を減らしＩＴスタッフへの業務の妨げを最小にするために、リスク管理、ガバナンス、コントロール、コンプライアンスの分野と、組織のリスク情報を共有し協働する。

最後に、上記６つの措置の進捗状況を取締役会に報告する。これにより、取締役会と監査委員会はテクノロジーに対する理解を深め、内部監査はＩＴ監査の有効性を向上するための説明責任を負う。

９．新たなテクノロジー

テクノロジーの変化と発展の速度は驚異的であり、組織に新たなリスクを急速にもたらし得る。したがって、テクノロジーのトップ10リスクの第９位は新たなテクノロジーとする。新たなテクノロジーの意味は、組織によって異なるだろう。ある組織にとっては、スマート機器の利用は新たなテクノロジーかもしれないが、別の組織では既に定着している可能性がある。ここでの議論では、新たなテクノロジーを、組織内で今日利用されていないが近い将来利用されそうなテクノロジーと定義する。例には次のようなものがある。

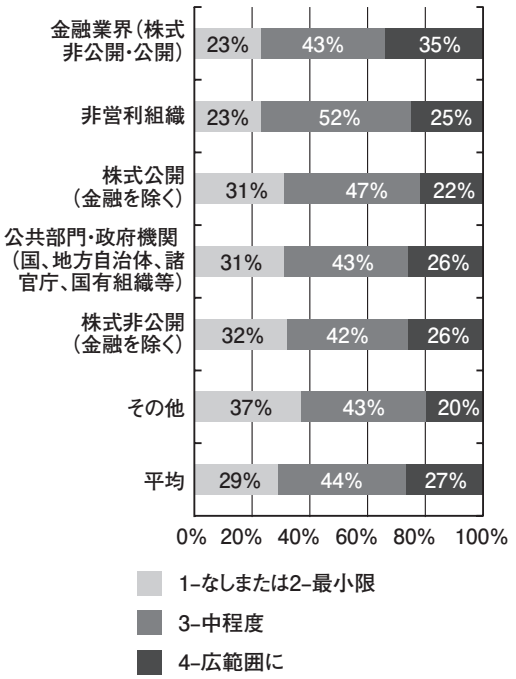
- 予測的データ分析
- ビッグデータ
- フォグ・コンピューティング（クラウド・コンピューティングが事業体のネットワークの境界まで拡張したもの）
- ３Dプリンター（３次元の物体を出力するようにプログラムされたプリンター）
- インターネット・オブ・シングス（冷蔵庫や電子レンジのような毎日使うモノがネットワークに接続してデータのやり取りができる）
- ロボット工学

ある業界内では既に利用されているが（例えば、金融業界におけるビッグデータ）、他の業界ではまだ利用されていないテクノロジーもあり得る。このような違いは、リスクの認識水準にも影響する。図表11の通り、金融業界は、ビッグデータの信頼性リスクが広範囲に及ぶと考えている割合が最も高い。

内部監査の役割

内部監査人は、組織内の新たなテクノロジー採用において重要な役割を果たすことができる。内部監査は、新たなテクノロジーの評価プロセスの早い段階で関与すれば、リスクとコントロールの要件についてガイダンスを提供することができる。例えば、組織が初めてクラウドコンピューティングサービスの採用を検討している場合、内部監査はそのような環境がもたらす追加的リスク（リスクの低減の場合もある）を判断するためのテクノロジータスクフォースの一員となることができる。

＜図表11＞ビッグデータの信頼性リスク（組織タイプによる比較）



注：質問93「下記の新たな情報技術（IT）の分野について、あなたの組織の固有リスクの水準はどの程度ですか？」「該当なし・わからない」と回答した者は計算から除外。四捨五入の関係で合計が100％にならないものもある。回答数＝9,373。

内部監査人が尋ねるべき重要な質問

1．組織には新たなＩＴテクノロジーを評価するチームがあるか？
2．組織には新たなテクノロジーを評価する正式なプロセスがあるか？
3．組織は新たなテクノロジーがもたらすリスクをどのように識別しているか？
4．本番環境内で新たなテクノロジーが利用される現在進行中のプロジェクトは何か？

内部監査が行うべき重要な業務

1．現在利用中のテクノロジーの一覧表を入手する。
2．新たなテクノロジーが利用される可能性のある新規プロジェクトについて理解する。
3．新たなテクノロジーのリスクプロセス（新たなテクノロジーの評価中にリスクがどのように識別されるか）を監査する。
4．新たなテクノロジーを採用するＩＴ戦略を理解するために、ＩＴテクノロジーチームと議論する。

10. 取締役会と監査委員会のテクノロジー認識

多くの組織では、取締役会にＩＴ専門家はわずかしかいない。したがって、取締役会と監査委員会のテクノロジー認識を、テクノロジーのトップ10リスクの第10位とする。ＩＴ部門に業績の責任を持たせるためには、取締役会が適切な水準のＩＴ知識を持つ必要がある。istaインターナショナル社コーポレート・インターナルオーディット・コンプライアンス担当シニアヴァイスプレジデントのグンター・メグジェネダー氏は、「取締役会と監査委員会は財務知識を向上させてきたのと同様に、今後はＩＴの専門知識を一層増やすことが重要である。」と述べている。

ＩＴはビジネスの可能性を広げるが、多大な投資が必要なため、取締役会にＩＴの知識が不足しているのは危険である。

「今後４～５年以内に、取締役会はＩＴ技術者を取締役にするか諮問委員会にＩＴ専門家を入れるべきである。」とフューチャー・ポイント・オブ・ビューＬＬＣのパートナー、スコット・クロソスキー氏は言う。

内部監査の役割

内部監査は、取締役会と監査委員会にテクノロジーに対する認識をもたらす主なルートであり重要な役割を果たす。内部監査は、監査委員会のテクノロジーの知識を評価し、監査委員会の啓発役やコンサルタントとしての役割を果たす責任がある。

問題を事後分析する中でよく見られる根本原因には、自身のビジネス―仕組みや起こり得る事態―を理解していなかったことがある。この問題を克服し手遅れになる前に措置を講じる機会を当事者に与えるためには、自らの状況と選択肢をしっかり理解できるような環境を作ることが不可欠である。

バリューブリッジ・アドバイザーズ代表、ＯＣＥＧフェロー
ブライアン・バーニャー氏

内部監査人が尋ねるべき重要な質問

1．テクノロジーの変更を計画する際の組織のＩＴ戦略はどのようなものか？
2．監査委員会はＩＴリスクを理解しており、その理解は全社的リスクに照らしたものであるか？
3．監査委員会は、全社的リスクとテクノロジー認識という観点からの自らの責任と役割を理解しているか？

内部監査が行うべき重要な業務

1．監査委員会との会議にテクノロジー認識が含まれることを確実にする。
2．組織が新たなテクノロジーに関する意思決定をする場合に、助言者となる（例えば、組織が機密情報をクラウドに移すことを計画している時、または、機密情報を外部のサービスプロバイダーで保管している時）。

結論

内部監査人は、戦略的に考え、ビジネスを理解し、価値を付加するために熱心に働いてきた。これからは、内部監査人は組織に影響を及ぼし得る新たなテクノロジーを識別するために積極的になる必要がある。専門家は以下を推奨している。

1．状況に応じた認識を持つためのプロセスを導入する。
2．業界または組織が置かれた環境における危険信号に注意する。
3．「起こりうる事態」を考える。
4．新たなテクノロジーのリスクと機会の影響を判断するためのレビュー用に、新たなテクノロジーのリスクと機会のリストを保持する。
5．リスクや機会を識別した時に、それに応じてフォローアップするための措置を講じる。

将来を予測することは不可能であるが、テクノロジー・ランドスケープが変化することは確かである。内部監査人は変化に対応するための準備をすべきである。

ＣＢＯＫプロジェクトチーム

ＣＢＯＫ開発チーム

ＣＢＯＫ共同委員長：ディック・アンダーソン（U.S.A.）、ジャン・コロラー（フランス）
実務家調査小委員会委員長：マイケル・パーキンソン（オーストラリア）
ＩＩＡ調査研究財団ヴァイス・プレジデント：ボニー・ウルマー
主任データ分析官：ポージュー・チェン博士
コンテンツ開発者：デボラ・ポーラリオン
プロジェクトマネジャー：セルマ・クーストラ、ケーラ・マニング
編集主任：リー・アン・キャンベル

レポートレビュー委員会

ウーリッヒ・ハーン（ドイツ）
スティーブ・ハント（U.S.A.）
リチャード・マーティン（U.S.A.）
マイケル・パーキンソン（オーストラリア）
カート・レディング（U.S.A.）
デイブ・ウイリアム（U.S.A.）

スポンサー

本レポートはＩＩＡオースチン支部がスポンサーの一部となっている。ご支援に感謝する。

著者について

注：本レポートはフィリップ・フローラ氏とサジャイ・ライ氏が共同で執筆した。フローラ氏は、トップ10リスクの決定、世界中の専門家へのインタビュー、初稿を担当した。ライ氏は、最終稿および各章の尋ねるべき重要な質問と行うべき重要な業務を担当した。

フィリップ・Ｅ．フローラ氏は、ＣＩＡ、ＣＩＳＡ、ＣＦＥ、ＣＣＳＡの資格を保持しており、フロビズ＆アソシエイト, LLCの代表兼マネージングメンバーであり、ＹＣＮグループのメンバーであり、また、ＩＩＡの研修コンサルタントを務めている。30年以上の監査経験を持ち16年以上にわたって非営利公共企業のＣＡＥを務め、未来の監査リーダー50名以上の育成を支援する内部監査リーダーシップ開発プログラムの作成を支援した。現在はＩＩＡ調査研究財団の評議委員も務めており、2000年以来、ＩＩＡの国際委員会の委員長、ＩＩＡ調査研究財団の研究・教育助言委員会（ＣＲＥＡ）、ＩＩＡの国際委員会メンバーなどを歴任した。過去10年間は、様々な州、地域、国内外のカンファランスや研修会で講演している。フィルは、バージニア・

コモンウエールズ大学で会計の学位を取得している。

サジャイ・ライ氏は、ＣＰＡ、ＣＩＳＳＰ、ＣＩＳＭの資格を保持しており、セキュアリー・ヨアーズ，ＬＬＣの共同設立者兼オーナーである。30年以上のＩＴ経験があり、情報セキュリティとリスク、ＩＴ監査、事業継続、災害復旧、プライバシーなどに精通している。セキュアリー・ヨアーズを始める前は、アーンスト・アンド・ヤングＬＬＰのパートナーとしてデトロイトのメトロ地区で情報アドバイザリーに従事し、また、アーンスト・アンド・ヤングのセキュリティおよびリスクの米国リーダーとして活躍した。アーンスト・アンド・ヤングの前はＩＢＭ社に勤務し、情報セキュリティと事業継続を担当した。ＩＩＡでは専門職課題委員会（ＰＩＣ）委員およびデトロイト支部の理事を務めた。彼は、ワシントン大学セントルイス校で情報管理の修士号を、フォントボーン大学セントルイス校でコンピュータサイエンスの学位を取得している。