内部監査人協会（ＩＩＡ）情報

グローバルな視点と洞察　第５号
最新動向
「内部監査の国際的動向」調査より

内部監査人協会（ＩＩＡ）
訳者：堺　　咲　子
内部監査人協会（ＩＩＡ）国際本部　理事
Internal Audit Foundation（内部監査財団）　理事・評議員
インフィニティコンサルティング　代表
ＣＩＡ，ＣＣＳＡ，ＣＦＳＡ，ＣＲＭＡ，ＣＰＡ（ＵＳＡ）

目　次

実施方法と回答者属性

内部監査人協会（ＩＩＡ）の「2016年内部監査の国際的動向」調査（国際的動向）が、2016年５月９日から５月27日までオンラインを通じて実施された[1]。ＩＩＡには世界中の現役の内部監査の専門職から2,254件の回答が寄せられた。回答者の52％が、内部監査部門の最高位の方または内部監査部門長（ＣＡＥ）またはＣＡＥ直属のディレクターやシニア・マネージャーであった。この報告書では、これらを「内部監査のリーダー」と呼ぶ。回答者にはまた、ディレクター直属のマネージャー（16％）、監査実務に従事する監査部門スタッフ（28％）、およびサービス・プロバイダー等（4％）が含まれている。

回答者は、111の国や地域に及び、組織体の種類、産業、収益規模、従業員数および内部監査部門の規模の面で様々な内部監査部門を代表している。

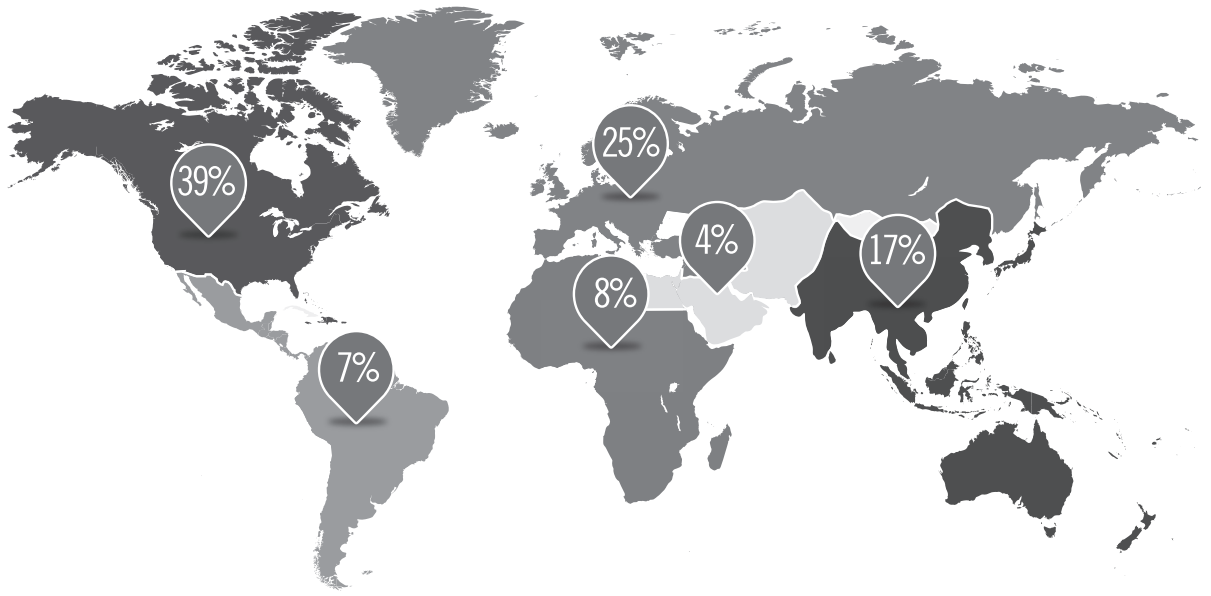
回答者の主な所属先は、上場会社（34％）、公共部門（27％）、および非上場会社（25％）である。

回答者が属する主な産業は、金融サービス（32％）、製造業（12％）、行政機関（11％）、医療産業（６％）、および公益事業（６％）である。

調査結果は、地域別のＩＩＡ会員の国際分布をうまく反映するように調整（正規化）されている。（以下地図参照）

はじめに

世界中で内部監査のリーダーは、卓越性に向けて動き出している。すなわち、組織体のガバナンス、リスク・マネジメントおよび戦略目的を進める上でのかけがえのない人材となるために、ビジネス感覚、技術的専門知識、および関係構築のスキルを示している。世界の多くの地域において今後内部監査スタッフの人数や予算の増加が予想されるが、このことは、経営陣や取締役会が内部監査の価値の向上を認識し支援していることを反映しており、これにより内部監査部門は、リスク・マネジメントのアシュアランス、戦略的ビジネスリスクおよびITといった重要な領域に時間を費やすことが可能になっている。しかし、内部監査人は向上し続ける必要があると考え

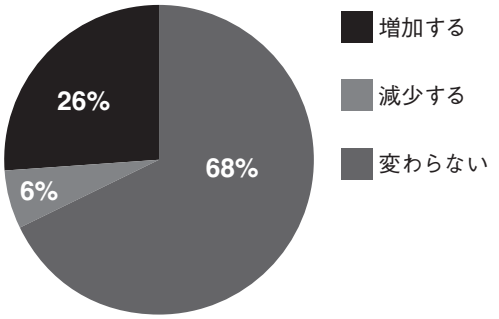


[1] 限られた数の質問については、2015年10月20日から11月10日の間に北米の回答者を対象に調査を行った。

ている者は多い。

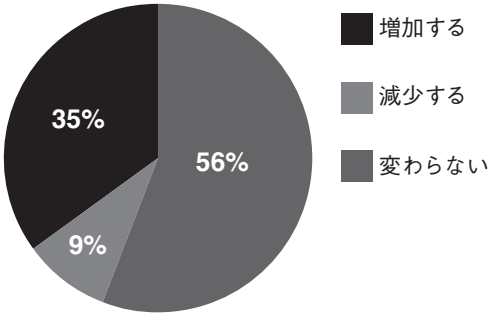
世界の多くの地域において今後内部監査スタッフの人数や予算の増加が予想されるが、このことは、経営陣や取締役会が内部監査の価値の向上を認識し支援していることを反映している。

＜図表１＞内部監査部門人員予測



備考：設問49：これからの１年の間に、あなたの所属する内部監査部門では、フルタイムのスタッフの数はどのようになるとお考えですか。

＜図表２＞内部監査部門予算予測



備考：設問50：これからの１年の間に、あなたの所属する内部監査部門の予算はどのようになるとお考えですか。

卓越性を追求するために講じられている措置を探るために、国際的動向調査では、内部監査を管理する上での新たな課題と実務を世界的に査定して内部監査の実態を評価した。

この報告書では次の２つの新たな課題について探っている。それらは、組織文化を監査することと、テクノロジー（サイバーセキュリティとビッグデータ）についていくことである。ここではまた、内部監査がどのようにして信頼されるアドバイザーのレベルまで向上できるか（ほぼ間違いなく向上しなければならないのだが）についても探っている。

本報告書は、内部監査が重要で新たな課題と実務に焦点を当て続けようとしていることを裏づけていると考えている。今ほど内部監査への期待が膨らみ続けている時はない。確かに、内部監査人は専門職として大きな進歩を遂げてきたが、まだやるべきことも多い。これが、内部監査をこのように難しいがやりがいのある職業にしている理由である。

組織文化の監査

組織文化が組織体の財務、業務および風評に直接的で悪い影響を及ぼすことを、歴史は示している。取締役会、経営陣、およびその他の利害関係者は、内部監査が組織体による組織文化のモニターと強化を支援するようなアシュアランスとアドバイザリーを行うことを、さらに、異変があるかもしれない時に警鐘を鳴らすことを期待すべきである。

確かに、内部監査はこれまでも長い間ソフトコントロールの監査を行っており、「トップの姿勢」がよく使われる語句になってからは、多くの組織体が「トップの姿勢」を少なくとも非公式には評価している。しかし、正式に組織文化を監査するために次の段階に進んでいる組織体がある一方で、大多数の組織体には次の段階へ進むことを阻む多くの要因がある。

組織文化は、全従業員の活動や態度を通して示される組織の信念や価値観を具象化している。端的に言うと、組織文化とは組織体全体で物事が行われる方法であり、物事が行われる方法、および物事を成し遂げる方法である。

望ましい組織文化は、トップによって確立されるものであり、組織体の主たる価値観や倫理綱要に表れ、許容できる行動や許容でき

ない行動を示している。容認できず非倫理的でさえある、つまりやってはいけない方法は、組織体をリスクにさらし、極端な場合には、不正、汚職およびその他の違法行為を伴う有害な組織文化をもたらす。注目に値するいくつかの事件は、経済危機さえもたらして人々の信頼を損ねた。2015年には、東芝による不正会計、ＦＩＦＡ（国際サッカー連盟）における贈収賄と汚職疑惑、フォルクスワーゲン社による排ガス試験の偽装問題、エクソン・モービル社の気候変動の影響に関する疑わしい報告書など、世界は組織文化の失策を示す一連の深刻な事件を目の当たりにした。これらの事例だけでも、組織文化が企業の主たる価値観に整合しているかどうか、また組織文化が倫理的な行動や法規制の遵守を奨励しているかどうかについて、アシュアランスを提供するよう内部監査を促すものになるはずである。しかしながら、内部監査のリーダーの72％は、現在、企業文化の監査を行っていないと回答している（図表３）。

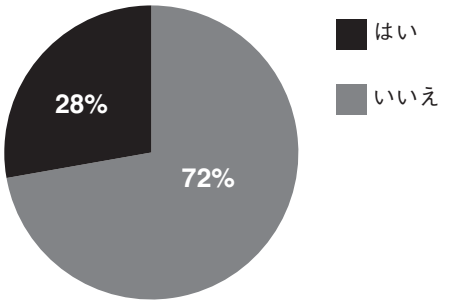
「組織文化を監査することは科学のようにはいかない。多くの組織体は、自らの組織文化を定義することに苦労しているのだから、組織文化を効果的にリスク評価プロセスに組み込むことには言うまでもなく苦戦している。それでも組織文化を監査することは不可欠である」

英国勅許ＩＩＡ（ＩＩＡ英国＆アイルランド支部）　最高経営責任者
イアン・ピーターズ博士[2]

組織体の気風は一般的に組織のトップによって決められ、組織体の規模や複雑さに関係なく期待される組織文化はリーダーによって示されるが、組織文化は、組織体全体で必ずしも均一ではない。トップダウンによる全組織的文化、つまり「マクロ文化」は、望ましい行動を定義する際の起点となる。しかしどんな組織体にも、特定の地域、部署、部門および何らかの共通点を持った従業員のグループを反映した、多くの個別の小規模な文化、つまり「ミクロ文化」が存在する。このミクロ文化の増殖が、組織文化の監査を難しくすることがある。しかし、内部監査は組織体に対する包括的かつ客観的な視点を備えているので、各ミクロ文化、そのミクロ文化が組織体のマクロ文化に与える影響、およびそれらが組織体に与え得るリスクを検証する潜在能力がある。もしも内部監査が、後でミクロ文化を評価して経営者が望んでいる姿と実際に組織で起こっていることとの違いを見つけようとするのであれば、まずは望ましいマクロ文化というものを深く理解しなければならない。

幸い、内部監査のリーダーの大多数（89％）は、所属する内部監査部門が組織文化に関連するリスクについて理解していると回答している。しかし一方で、内部監査部門がどのように組織文化を監査すればよいかを本当に理解していると回答しているのは、約半数（53％）にとどまる。興味深いことに、図表４が

＜図表３＞組織文化の監査を実施する内部監査部門の割合



備考：設問5：あなたの所属する内部監査部門は、組織文化の監査を行っていますか。

[2] CCH Daily, “FRC calls for greater emphasis on corporate culture,” 20 Jul 2016 https://www.cchdaily.co.uk/frc-calls-greater-emphasis-corporate-culture（accessed Aug. 24, 2016）.

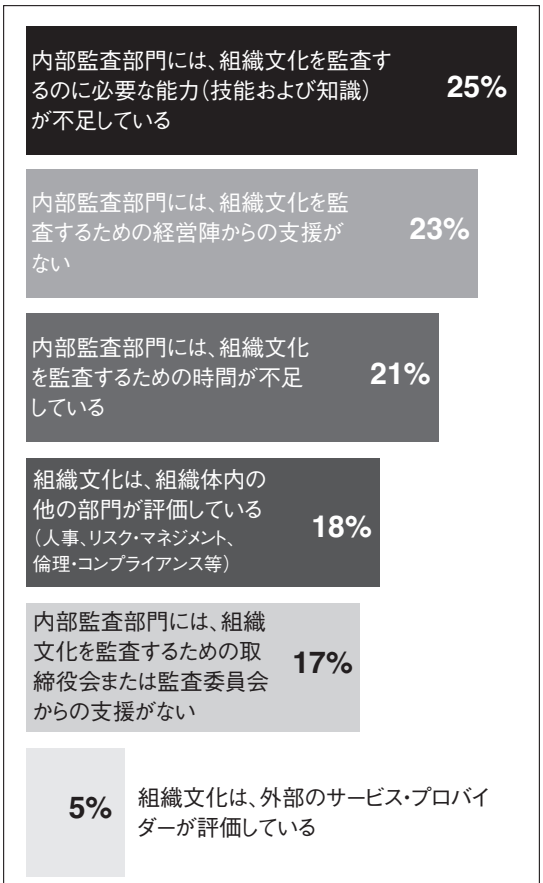
示すように、18％は他部門がこの分野の評価をしているので文化を監査していないと回答しているが、一方で文化を監査していない理由の上位は、能力不足（25％）、必要とする組織的支援がない（23％）、または時間が不足している（21％）であった。

> 内部監査は組織体に対する包括的かつ客観的な視点を備えているので、各ミクロ文化、そのミクロ文化が組織体のマクロ文化に与える影響、およびそれらが組織体に与え得るリスクを検証する潜在能力がある。

ＩＩＡマレーシアのエグゼクティブ・ディレクターであるヌル・ハヤティ・バハルディン氏は、「組織文化の監査に関するスキルや知識が不足している内部監査部門は、内部監査が得意なこと、すなわち、組織体の組織文化に関連する活動の評価と改善に向けて体系的で規律ある方法を用いることから始めればよい」と述べている。例えば、ＩＩＡが2016年に公表した「グローバルな視点と見識：組織文化の監査　ーソフトなことをハードに調べる」が示すように、３つのディフェンスライン（またはリスクとコントロールの義務や責任および報告経路について説明したその他の適切なモデル）[3]を理解することは、標準的な監査業務の支援に有効であるのと同様に文化の評価においても有効である。組織文化の監査をする際に各ラインに期待される責務には、次のようなものがある。

1．第１のディフェンスラインである現業部門の経営管理者は、望ましい価値観と行動を定め、伝達し、モデル化する。
2．第２のディフェンスラインは倫理室のような監督部門であり、倫理プログラムを策定し、文化に関連するリスクおよび文化に関連する方針と手続への遵守状況をモニタリングし、さらに第１のディフェンスラインに助言する。
3．第３のディフェンスラインである内部監査は、組織の基準および望ましい基準への遵守状況を評価し、組織文化が組織体の目的、戦略、およびビジネスモデルを支持しているかを評価する。内部監査は組織文化全体を評価して、文化の弱い分野を特定する[4]。

＜図表４＞内部監査部門が組織文化の監査を実施しない理由



備考：設問6：あなたの所属する内部監査部門が組織文化の監査を行っていない理由について、以下の文章のうち当てはまるものをすべて選択してください。（組織文化の監査を行っていないと回答した方）

[3] The IIA's Position Paper, "The Three Lines of Defense in Effective Risk Management and Control," 2013, www.theiia.org/positionpapers（accessed Sept. 29, 2016）.（訳者注：本レポートの日本語訳は、『月刊監査研究』2015年10月号に掲載）

「組織文化の監査に関するスキルや知識が不足している内部監査部門は、内部監査が得意なこと、すなわち、組織体の組織文化に関連する活動の評価と改善に向けて体系的で規律ある方法を用いることから始めればよい」

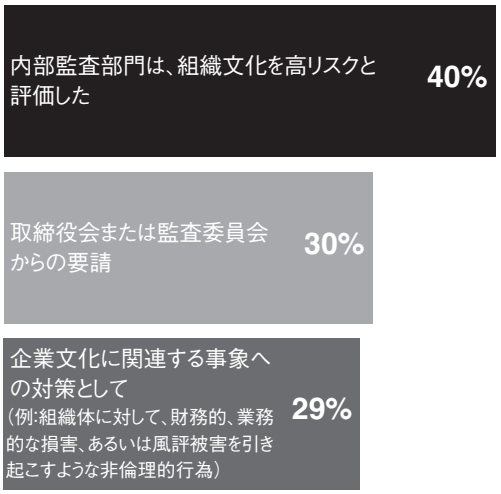
ＩＩＡマレーシア　エグゼクティブ・ディレクター
ヌル・ハヤティ・バハルディン氏

しかし、監査能力の有無にかかわらず、内部監査人は組織文化の監査に注目している。プロティビティ社の2016年内部監査部門の能力調査によれば、組織文化の監査は、内部監査のリーダーにとっての優先事項の上位５つに含まれている。そして、ＩＩＡの国際的動向の調査に回答した内部監査のリーダーの89％が、組織文化に関連するリスクを理解していると回答していたことを思い出して欲しい。組織文化の監査を実施する主な動機には、組織文化が内部監査で高リスクと評価されていること、取締役会や監査委員会の要請があること、および組織文化に関連する事象への対策として、などがある（図表５）。

ＣＡＥは、リスクベースの監査計画の策定でリーダーシップを発揮し、取締役会や監査委員会との関係を構築することを通して、組織体が戦略的使命を達成し関連する事業および業務の目的達成に必要な、健全で望ましい組織文化の維持を支援するという重要な役割を果たさなくてはならない。

組織文化の監査を行う者は、先進的な取り組みをしている。ＩＩＡ国際本部理事会2016－17年会長であるアンゲラ・ウィッツァーニ氏は、「組織文化の監査は、あらゆる監査業務に組み込まなければならず、組織体が継続的

＜図表５＞内部監査部門が組織文化の監査を実施する理由



（上位３つ）

備考：設問7：あなたの所属する内部監査部門が組織文化の監査を行う理由について、以下の文章のうち当てはまるものをすべて選択してください。（組織文化の監査を行っていると回答した方）

モニタリングをするための基礎を提供しなければならず、内部監査人が早期の警戒信号を見つけられるものにしなければならない」と述べている[5]。

組織文化の監査には、少なくとも次の３つの方法がある。それらは、組織体全体に対して独立して評価する、（すべての監査ではなくても）多くの監査の一部として個々に監査する、長期間をかけた一連のミクロ文化の監査を集約して報告する、である。これらの方法を組み合わせてもよい。現在組織文化の監査を行っている少数派は、おそらく組織体の文化そのものを反映した様々な方法を用いている（図表６）。

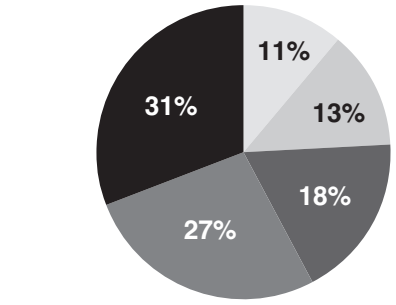
[4] The IIA, “Global Perspectives and Insights: Auditing Culture – A Hard Look at the Soft Stuff,” 2016, 5 www.theiia.org/gpi（accessed Aug. 24, 2016）.

[5] The IIA, “Global Perspectives and Insights: Auditing Culture – A Hard Look at the Soft Stuff,” 2016, 3 www.theiia.org/gpi (accessed Aug. 24, 2016).

「組織文化の監査は、あらゆる監査業務に組み込まなければならず、組織体が継続的モニタリングをするための基礎を提供しなければならず、内部監査人が早期の警戒信号を見つけられるものにしなければならない」

ＩＩＡ国際本部理事会　2016 - 17年会長
アンゲラ・ウィッツァーニ氏

＜図表６＞組織文化の監査への取り組み



備考：設問8：あなたの所属する内部監査部門が、企業文化を監査する方法に関して、以下の文章のうち最もよく当てはまるものを選択してください。(組織文化の監査を行っていると回答した方)

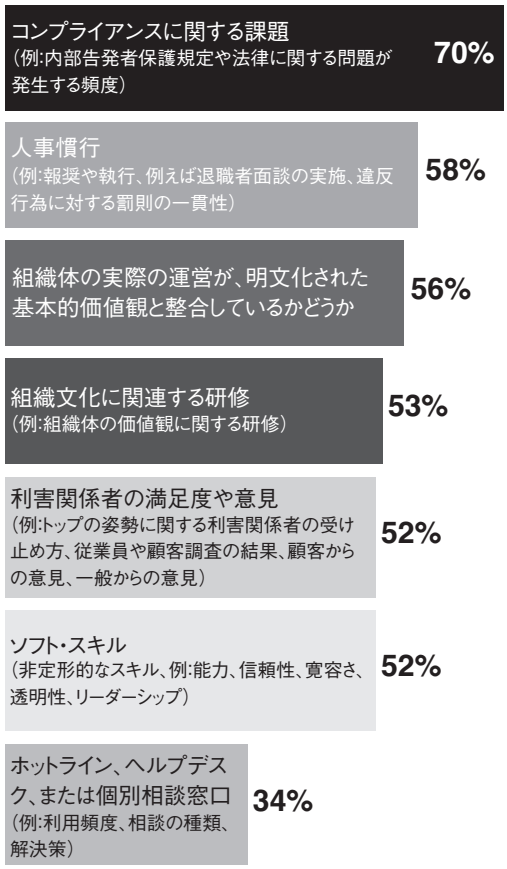
時には独立した組織文化の監査が理に適っている。すなわち、大規模なスキャンダルの後、企業合併や買収の準備として組織体の相性を評価する時、または特定のコンプライアンス違反案件の根本原因調査のような、ある時点のスナップショットが必要な時である。しかし、独立した組織文化の監査だけでは十分ではない。内部監査があらゆる監査業務において組織文化を考慮すれば、望ましい組織体全体の文化から逸脱したり有害化する可能性のあるミクロ文化を経営陣や取締役会が発見して対処するのにより一層役立つことができる。そのため、マクロ文化および様々に異なるミクロ文化の両方の評価を行う余地がある。

組織文化の監査が最も有効なのは、組織文化に関連した要素の包括的なリストが考慮されている場合であり、内部監査は、この分野における改善の機会が多い。内部監査のリーダーの約半数は、この調査で示した７つの要素のうち少なくとも４つを考慮していると回答している（図表７）。組織文化に関連するあらゆる監査で最も考慮されているのは、コンプライアンス上の問題、人事慣行、および組織の行動と組織のコアバリュー（基本的価値観）との整合である。

組織文化に関連するあらゆる監査で最も考慮されているのは、コンプライアンス上の問題、人事慣行、および組織の行動と組織のコアバリュー（基本的価値観）との整合である。

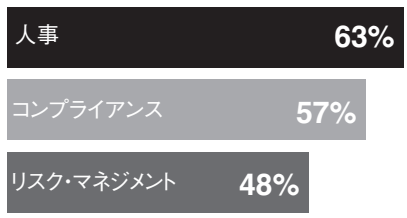
興味深いことに、組織文化を監査する者の60％以上が、組織文化を監査する他の部門と連携している。内部監査が組織文化を監査する際に最もよく連携している部門は、人事、コンプライアンスおよびリスク・マネジメントである（図表８）。組織体内の他の重要な部門と連携することは賢明であり、おそらく先進的な実務である。しかしながら、内部監査にとって重要な独立的な役割からすると、組織文化の監査を主導していると認められ、自らの結論を導き、独立的に意見と発見事項を報告すべきなのは、内部監査である。

＜図表７＞監査実施時に考慮する組織文化に関連する要素



備考：設問12：これまで実施してきた内部監査業務において、組織文化に関連する要素として考慮したことのある項目は何ですか。以下の文章のうち当てはまるものをすべて選択してください。(組織文化の監査を行っていると回答した方)

＜図表８＞内部監査が組織文化を監査する際に最もよく連携している部門（上位３つ）



備考：設問11：どの部門と共に組織文化の監査に取り組みましたか。該当するものをすべて選択してください。（他部門と取り組んでいると回答した方）

組織文化を監査する者の60％以上が、組織文化を監査する他の部門と連携している。しかし内部監査は自らの結論を導き、独立的に意見と発見事項を報告すべきである。

他の監査よりも組織文化の監査の方が内部監査にとって結果の報告が難しい理由は、組織文化に捉えどころのない側面があるからではないかと推測している。実際に、組織文化の監査を行っている内部監査のリーダーの約半数しか内部監査部門が組織文化の報告方法を理解していると回答しておらず、５分の１は組織文化に関する監査報告を全くしていないと回答している。監査結果を報告する場合に最も一般的な形式は書面による報告であり、時には口頭による報告も併用される。

ためらいがあるのは理解できるが、内部監査人は組織文化の監査への取り組みを躊躇してはならない。内部監査があらゆる監査に組織文化を組み込めば、組織文化は各監査の結論と最終報告書で考慮すべきもう１つの要素となる。

組織文化の監査を行っている内部監査のリーダーの約半数しか内部監査部門が組織文化の報告方法を理解していると回答しておらず、５分の１は組織文化に関する監査報告を全くしていないと回答している。

結論

内部監査が組織文化の問題を、組織体に長期的に害を及ぼす要因になり得るものとしてより強く意識するようになっていることを示す証拠が出始めている。本調査に回答した内部監査部門の約４分の３は組織文化の監査を実施していないが、内部監査のリーダーの少数はこの分野で一歩先を進んでいる。内部監査の専門職全体がこのようなリーダーに追随

するためには、以下を行うとよい。
■組織体のマクロ文化をよく理解する。
■確立されたリスクおよびガバナンスのフレームワークを、マクロ文化およびミクロ文化の両方の評価に適用する。
■組織文化に関連する様々な要素を念頭に置いて、あらゆる監査業務で組織文化を考慮する。
■組織文化に関して継続的に報告する。

テクノロジーについていく

急速に変化する複雑なテクノロジーの進化の動きについていくために内部監査はいくつかの措置を講じているが、国際的動向調査の結果によると、内部監査はテクノロジーリスクに包括的に対応するために依然として苦労しているようである。この苦労をしているのは内部監査だけではない。事実、ヒューレッド・パッカード社の2016年のセキュリティ・オペレーションの現状報告によれば、2015年はセキュリティ・オペレーション・センターの成熟度が対前年比で低下した。ヒューレッド・パッカード社によると成熟度の低下原因は、クラウド、モバイル、ソーシャル、ビッグデータの各コンピューティングによるサイバー防御に対する圧力、およびサイバー攻撃集団の高度化である。取締役に対するどのような調査でも、大多数がテクノロジーリスク、特にサイバー攻撃を（最高ではないとしても）懸念事項リストの上位であると評価している。

内部監査はこれらに対して何ができるだろうか。広い見識を持った内部監査のリーダーが増えており、彼らはサイバーセキュリティやビッグデータのようなＩＴ問題の知識を身に付けて熟達度を示し、さらにこれらの問題に関するあらゆる種類の内部監査サービスを（直接またはコ・ソーシングを通して）提供することによって、組織の信頼されるサイバー・アドバイザーとして位置づけられるようにと踏み出している。しかし他方で国際的動向調査は、内部監査がこの分野で卓越性を示すのを阻む要因があることも示している。

サイバーセキュリティ

サイバーセキュリティとは、コンピューター・ベースのシステムに存在する企業データを、想定外の者による紛失、破壊、不正アクセスまたは誤用から保護するための対策を指している。ＩＩＡの2016年『グローバルな視点と見識：信頼されるアドバイザーとしての内部監査』は、「サイバーセキュリティに失敗した場合の影響は、基本的な業務が遂行できなくなることから知的財産権の喪失や甚大な風評被害の可能性に及ぶため、サイバーセキュリティは総合的かつ体系的に検討しなければならない。これは単にテクノロジーリスクではなく、ビジネスリスクなので、内部監査人が果たすべき重要な役割がある」[6]と述べている。

幸いなことに、内部監査のリーダーの圧倒的多数（93％）は、内部監査部門がサイバーセキュリティに関連するリスクを理解していると回答している。このような楽観論とは対照的に、アーンストヤングは2016年の報告書『デジタルの世界で信頼を築く』の中で、サイバーセキュリティ・リスクが過小評価されており、あまりにも多くの組織体がその場しのぎのリスク対策で脆弱性を悪化させていると警告している。国際的動向調査でもこれを確認しており、組織体がサイバーセキュリティに対応するフレームワークを利用していると回答しているのは半数超（55％）だけであ

[6] The IIA, “Global Perspectives and Insights: Internal Audit as Trusted Cyber Adviser,” 2016, 5, www.theiia.org/gpi (accessed Aug. 24, 2016).

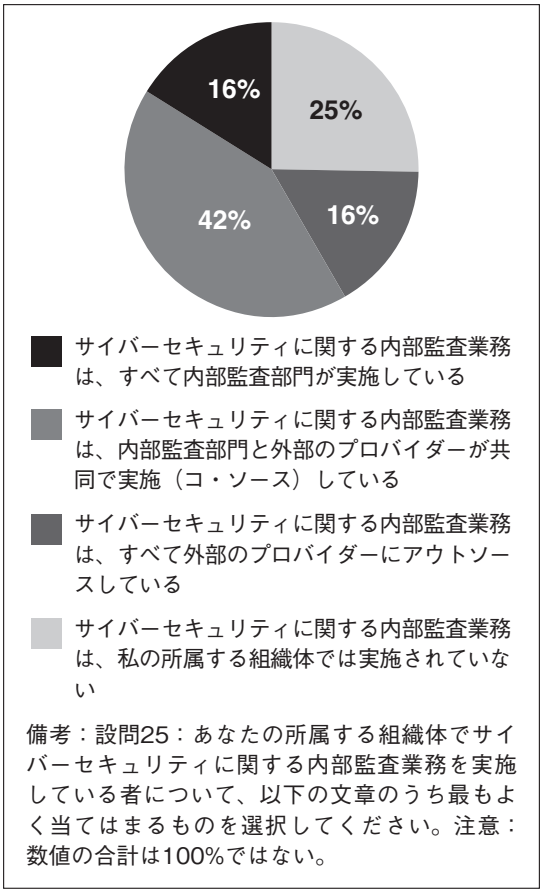
る。これは図表９が示すとおり、サイバーセキュリティ関連の内部監査業務を単独（16％）またはコ・ソーシング（42％）で行っているという回答とほぼ同じ割合（58％）である。

「サイバーセキュリティに失敗した場合の影響は、基本的な業務が遂行できなくなることから知的財産権の喪失や甚大な風評被害の可能性に及ぶため、サイバーセキュリティは総合的かつ体系的に検討しなければならない」

つまり、内部監査部門の大多数はサイバーセキュリティ・リスクを理解していると主張しているにもかかわらず、その理解を組織体が必要とするサイバーセキュリティの内部監査業務の実施という行動に完全に移しているのはほんの少数である。しかしもっと憂慮すべきなのは、内部監査のリーダーはサイバーセキュリティ・リスクおよび有名なサイバー攻撃による注目度と被害を理解していると回答しているのに、彼らの４分の１（25％）は組織体のサイバーセキュリティ関連の内部監査業務を行っていないと回答していることである。残りの16％は、すべてのサイバーセキュリティ関連の内部監査業務が完全にアウトソースされていると回答している（図表９）。

サイバーセキュリティ関連の内部監査業務を行っていない理由の上位は、内部監査の能力（スキルおよび知識）不足と、サイバーセキュリティの監査を実施するためのツールの不足である（図表10）。ＣＡＥは、これらの不足を補うための対策を講じている。2016年のＩＩＡ調査研究財団のＣＢＯＫレポート[7]によれば、情報技術およびデータマイニング／分析は、ＣＡＥが内部監査部門内外から獲得しようとしている７つのスキルの内の２つである。またＣＡＥは、能力やツールの不足を、コ・ソーシングやアウトソーシングを通じて補っている。

＜図表９＞誰がサイバーセキュリティ関連の内部監査を実施しているか



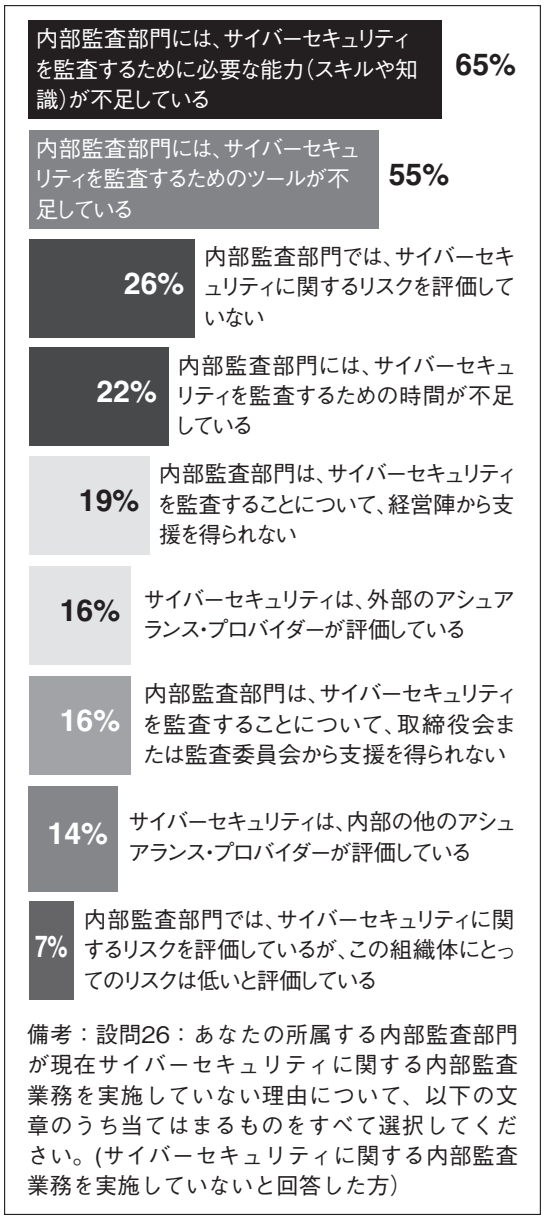
備考：設問25：あなたの所属する組織体でサイバーセキュリティに関する内部監査業務を実施している者について、以下の文章のうち最もよく当てはまるものを選択してください。注意：数値の合計は100%ではない。

内部監査のリーダーの４分の１は組織体のサイバーセキュリティ関連の内部監査業務を行っていないと回答している。

内部監査人がこの分野で進歩するためには何ができるだろうか。まず、サイバーセキュリティの監査の実施に必要な能力やツールを獲得することがすべての起点になる。調査結果から、これらがこの重要な分野の監査をうまく行うための上位２つの課題であることが明らかになっている。次に、組織体のトップからの支援が必要であることを認識することである。「信頼されるサイバーアドバイザー

[7] James Rose, “The Top 7 Skills CAEs Want,” (Altamonte Springs: The IIA Research Foundation, 2016) p 2, http://theiia.mkt5790.com/CBOK_2015_Top_Skills_CAEs_Want.

＜図表10＞内部監査部門がサイバーセキュリティの監査を実施しない理由



備考：設問26：あなたの所属する内部監査部門が現在サイバーセキュリティに関する内部監査業務を実施していない理由について、以下の文章のうち当てはまるものをすべて選択してください。(サイバーセキュリティに関する内部監査業務を実施していないと回答した方)

としての内部監査」に書かれているとおり、事実上あらゆる組織体のあらゆる主要プロジェクトにおいて、トップの賛同は不可欠である。取締役会は、サイバーセキュリティに関して最も懸念する事項について、リスクに見合った行動をしていない可能性がある。例えば、米国における最近の調査では、調査対象者の26％は、自社の最高情報セキュリティ責任者（ＣＩＳＯ）または最高セキュリティ責任者（ＣＳＯ）が、年に１回しか取締役会に対してセキュリティの報告を行っておらず、ほぼ同数（28％）は、全く報告がされていないと回答していた。さらに、約３分の１は、取締役会の委員会や取締役の誰もサーバーリスクに携わっていないと回答しており、わずか15％が、監査委員会がサイバーリスクに携わっていると回答していた[8]。

おそらく内部監査がサイバーセキュリティを評価する十分な能力がないという認識と現実の両方の結果として、内部監査がこの不足を補っているという自信も欠けている。その格好の例として、国際的動向調査では、サイバーセキュリティを監査するように取締役会もしくは監査委員会またはその両方から求められていると回答したのは、内部監査のリーダーのわずか56％であった。では、何をすべきなのだろうか。第１に、内部監査のリーダーが持つ取締役会と監査委員会への特権的なアクセスおよびサイバーセキュリティ・リスクに対する理解を利用して、サイバーセキュリティを常に議題に含め、サイバーの脆弱性について議論し、組織体がサイバーセキュリティのリスク選好を設定するプロセスを支援しようと申し出るべきである。サイバーセキュリティ・リスクの重要性を理解していない者は、サイバーセキュリティの有効なリスク・マネジメントとコントロールよりもテクノロジーの絶え間ない進歩の方が早いことからサイバーセキュリティ・リスクは重要なリスク要因として確実に一層深刻なものになる、ということを理解すべきである。実際にフォーブス誌は2016年初めに、サイバー犯罪対策コストは2019年までに２兆ドルに達するとの見通しを示した[9]。

第２に、サイバーセキュリティには連携し

[8] PwC, “US cybersecurity: Progress stalled, Key findings from the 2015 US State of Cybercrime Survey,” July 2015, http://www.pwc.com/us/cybercrime (accessed Aug. 24, 2016).

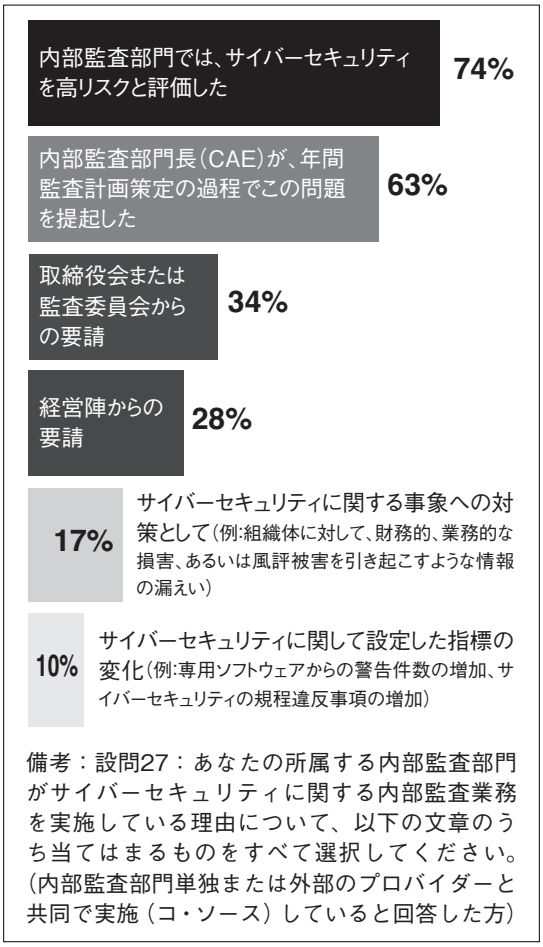
た取り組みが必要であるが、これはＣＡＥが示すリーダシップ感覚にかかっていることを認識すべきである。ＩＩＡオランダの最高責任者ハンス・ニューランド氏は、「ＣＡＥは経営陣と信頼されるパートナーシップ関係を構築し、サイバーセキュリティ・リスクを許容範囲内に管理または低減するための助言と解決策を提供し、最高情報責任者（ＣＩＯ）、最高情報セキュリティ責任者（ＣＩＣＯ）およびプライバシー・法務責任者と協力的な関係を構築しなければならない。」と述べた。

第３に、この分野の先覚者に倣うべきである。前述のように、内部監査のリーダーの半数以上（58％）は、サイバーセキュリティ関連の内部監査業務を単独（16％）またはコ・ソーシング（42％）で行っていると回答している。サイバーセキュリティ監査を行う理由の上位は、サイバーセキュリティを高リスクと正しく評価したことと、ＣＡＥが年間監査計画策定の過程でこの問題を提起したことである。これは、組織体がサイバーセキュリティの重要性のかつてない高まりを適切に重視するために、内部監査のリーダーが触発者（カタリスト）になる必要があり得ることを証明している（図表11）。

重要なのは、サイバーセキュリティの監査を実施する内部監査部門が、幅広く価値ある業務を行い始めているということである。サイバーセキュリティの監査として最もよく行われている業務は、インターネットに接続されたシステムによるデータの処理、格納、転送に関わるコントロール手段の評価、事業継続計画の評価、およびサイバーセキュリティ・リスクの評価プロセスの評価である（図表12）。内部監査のリーダーにとって明らかに機会となり得るのは、プロジェクトチームに助言をし、サイバーセキュリティの導入や実施の計画にガイダンスを提供することによって、プロセスの初期段階にもっと関与するようになることである。

> 内部監査のリーダーが持つ取締役会と監査委員会への特権的なアクセスおよびサイバーセキュリティ・リスクに対する理解を利用して、サイバーセキュリティを常に議題に含め、サイバーの脆弱性について議論し、組織体がサイバーセキュリティのリスク選好を設定するプロセスを支援しようと申し出るべきである。

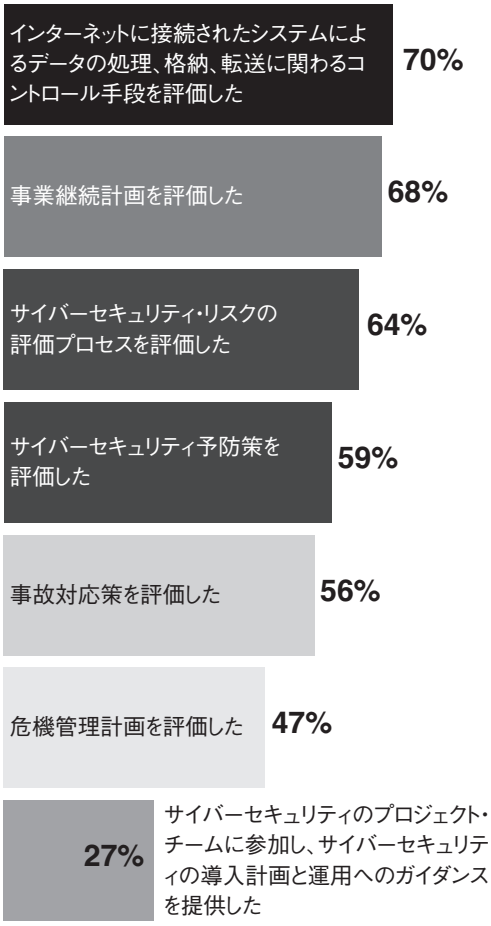
＜図表11＞内部監査部門がサイバーセキュリティの監査を実施する理由



備考：設問27：あなたの所属する内部監査部門がサイバーセキュリティに関する内部監査業務を実施している理由について、以下の文章のうち当てはまるものをすべて選択してください。（内部監査部門単独または外部のプロバイダーと共同で実施（コ・ソース）していると回答した方）

[9] Steve Morgan, “Cyber Crime Costs Projected to Reach $2 Trillion by 2019,” http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#6b96d1ae3bb0

＜図表12＞内部監査部門のサイバーセキュリティの監査の実施方法

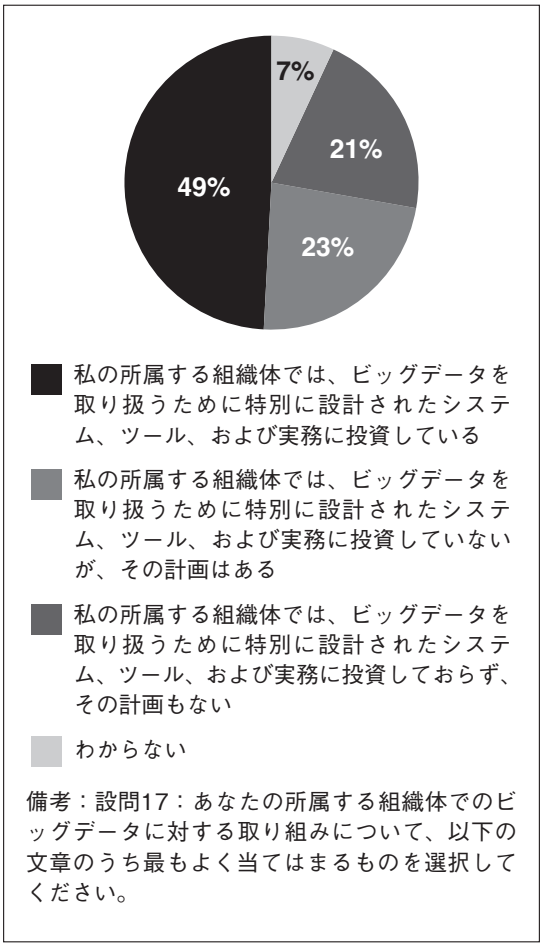


備考：設問28：あなたの所属する内部監査部門は、サイバーセキュリティにどのように関わってきていますか。以下の文章のうち当てはまるものをすべて選択してください。（内部監査部門単独または外部のプロバイダーと共同で実施（コソース）していると回答した方）

ビッグデータ

ビッグデータには、単に大量のデータという以上の意味がある。ビッグデータとは、組織体内に存在する大量で多種で高速で可変性が高いデータ（情報）であり、組織体はビッグデータを扱うための特別なシステム、ツール、業務に投資しなければならない。世界的にみると、内部監査のリーダーの約半数（49％）は、所属する組織体がこのような投資を既に行って（そしてビッグデータをある程度効果的に処理するためのシステムをおそらく既に導入して）いると回答しており、23％は、所属する組織体には（未整備ではあるが）システムを整備する計画があると回答している（図表13）。この結果から、内部監査はリスクベースの監査計画の中で、ビッグデータに取り組んでいるか取り組もうとしていることが予測される。

＜図表13＞ビッグデータを導入している組織体



備考：設問17：あなたの所属する組織体でのビッグデータに対する取り組みについて、以下の文章のうち最もよく当てはまるものを選択してください。

2016年にニュー・バンテージ・パートナーズ社が行ったフォーチュン1000企業の業務とテクノロジーに関する意思決定者に対する調査では、以下の事項が明らかになった。

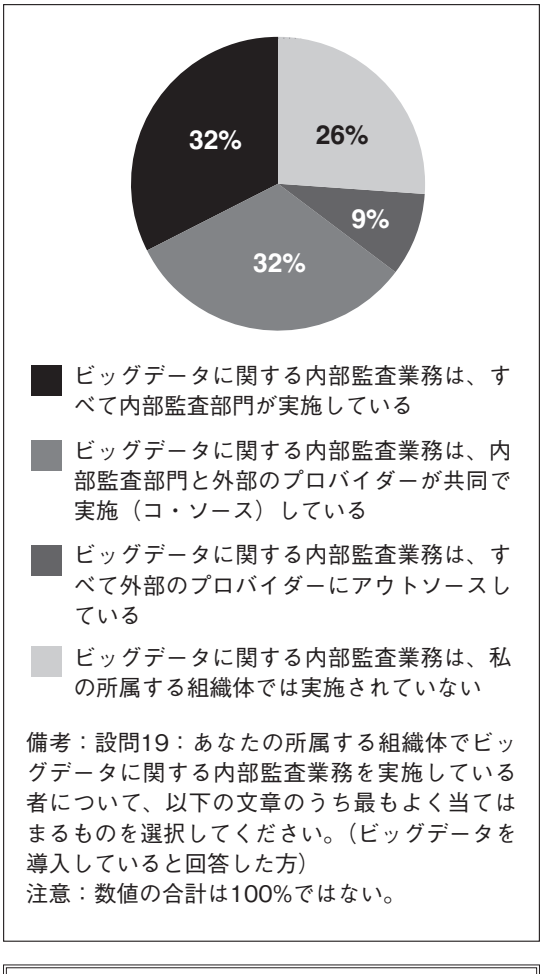
- ビッグデータは、主流が導入するところとなっている。
- 新しい組織体の役割として、最高データ責任者の役割が十分確立してきている。
- 業務とテクノロジーの連携は、ビッグデータの導入に不可欠であるとみられている。

■ビッグデータへの投資の主要なビジネス上の推進力となっているのは、ビジネスへの洞察とスピードである。
■ビッグデータへの投資の背景にある技術的推進力として、（データの）多様性が、量や速度より影響力を持ち続けている[10]。

世界的にみると、内部監査のリーダーの約半数は、所属する組織体がビッグデータへの投資を既に行っていると回答しており、23％は、所属する組織体にシステムを整備する計画があると回答している。内部監査はリスクベースの監査計画の中で、ビッグデータに取り組んでいるか取り組もうとしていることが予測される。

図表14のとおり、ビッグデータに投資している組織体の内部監査のリーダーの64％はビッグデータに関する内部監査業務を行っていると回答しており、そのすべてを内部監査部門が実施している（32％）、または外部のプロバイダーとのコ・ソーシング（32％）で実施しているのいずれかである。また、サイバーセキュリティの場合と同様に、内部監査のリーダーは、ビッグデータのリスク・マネジメントとコントロールの課題に注意を向けるようにと、組織体に働きかけることがよくある。内部監査のリーダーがビッグデータを監査する理由の上位２つは、ともにリスクに対する見方に関連している。（サイバーセキュリティのところで）既に述べたのと同様に、その理由は、ＣＡＥが年間監査計画策定の過程でこの問題を提起したことと、ビッグデータを高リスクと正しく評価したことである。

＜図表14＞誰がビッグデータ関連の内部監査を実施しているか



備考：設問19：あなたの所属する組織体でビッグデータに関する内部監査業務を実施している者について、以下の文章のうち最もよく当てはまるものを選択してください。（ビッグデータを導入していると回答した方）
注意：数値の合計は100%ではない。

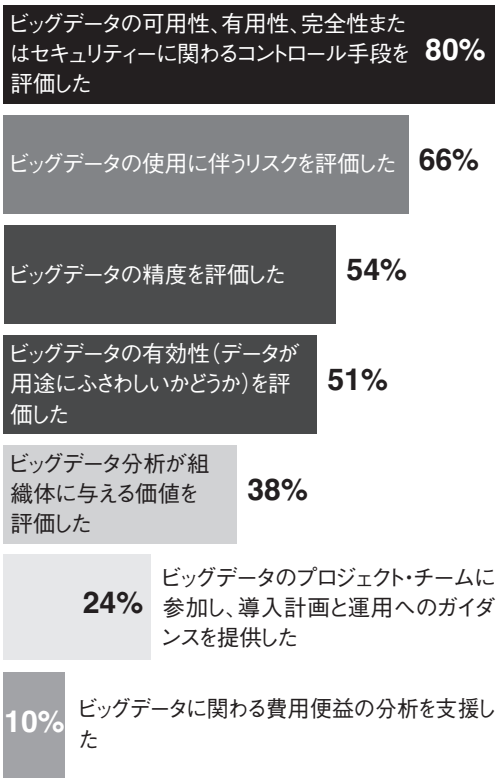
内部監査のリーダーがビッグデータを監査する理由の上位２つは、ともにリスクに対する見方に関連している。既に述べたのと同様に、その理由は、ＣＡＥが年間監査計画策定の過程でこの問題を提起したことか、ビッグデータを高リスクと正しく評価したことのどちらかである。

ビッグデータを調べている内部監査部門は、組織体にビッグデータに関する価値のある幅広い業務を提供している。最もよく行われる業務には、データの可用性、有用性、完全性またはセキュリティについてのコントロールの評価、ビッグデータの使用に伴うリス

[10] New Vantage Partners LLC, “Big Data Executive Survey 2016,” 2016, http://newvantage.com/wp-content/uploads/2016/01/Big-Data-Executive-Survey-2016-Findings-FINAL.pdf (accessed Aug. 24, 2016).

クについての評価、およびビッグデータの精度の評価がある（図表15）。

＜図表15＞－内部監査部門のビッグデータの監査の実施方法



備考：設問22：あなたの所属する内部監査部門はビッグデータにどのように関わってきていますか。以下の文章のうち当てはまるものをすべて選択してください。（内部監査部門単独または外部のプロバイダーと共同で実施（コ・ソース）していると回答した方）

おそらくこれらの内部監査業務は、ニュー・バンテージ・パートナーズ社の調査の重要な結果にそれぞれ関連付けることができる。例えば、ボツワナ国際科学技術大学の内部監査ディレクターであるレセディ・レセテディ氏は次のように説明している。「ニュー・バンテージ・パートナーズ社の調査で、ビッグデータに対応するための支出が増加傾向であることが明らかになった。内部監査が費用対効果分析を手伝えば、経営陣と取締役会は、ビッグデータへの投資が組織体への潜在的利益に基づいて判断されているという確信が持てる。」また、バージニア大学のCAEであるキャロライン・セイント氏は、「内部監査がプロジェクトチームに参加すれば、データの完全性、セキュリティ、プライバシー要件のようなテーマに対して、業務とテクノロジーの両方の観点を備えた示唆に富んだ議論を促すことができる。」と付け加えた。

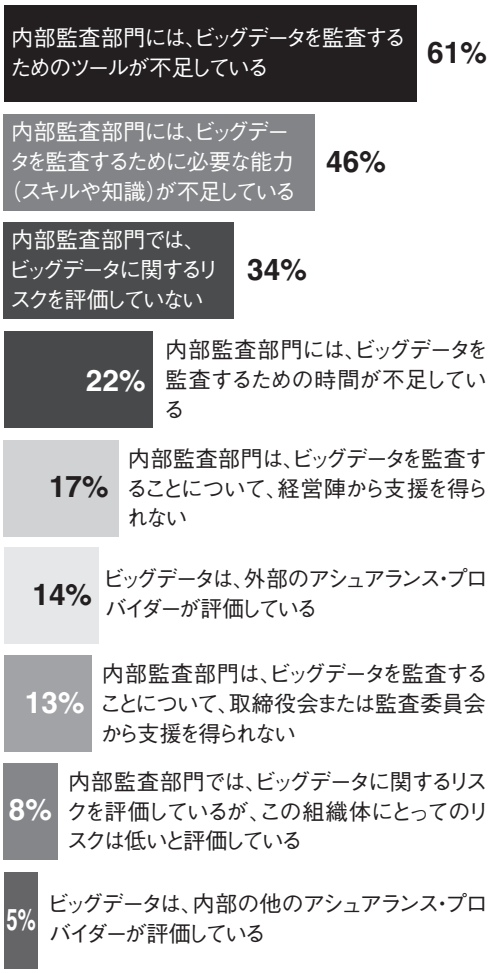
しかし、内部監査のリーダーの92％が、内部監査部門はビッグデータに関するリスクを理解しており、さらに内部監査は組織体のビッグデータ施策に貢献できる無数の方法があると回答しているにもかかわらず、ビッグデータに投資している組織体の内部監査のリーダーの４分の１（26％）は、ビッグデータに関する内部監査業務を行っていないと述べている。これらの内部監査のリーダーは様々な理由を挙げているが、ほとんどの者が、ビッグデータの内部監査をしない理由として、ツールと能力（スキルと知識）の不足を挙げている（図表16）。

> 「内部監査がプロジェクトチームに参加すれば、データの完全性、セキュリティ、プライバシー要件のようなテーマに対して、業務とテクノロジーの両方の観点を備えた示唆に富んだ議論を促すことができる」
>
> バージニア大学　ＣＡＥ
> キャロライン・セイント氏

結論

サーバーセキュリティやビッグデータに関連するテクノロジーリスクは多くの取締役会の最優先事項だが、これらに関する内部監査業務を行う多くの内部監査部門は、そのリスクに対応するのにふさわしいレベルに達していないようである。しかし、これらの業務を行う内部監査部門は、組織体をサイバーセキュリティやビッグデータに関連する重要なリスクとコントロールの課題に目を向けさせるのに役立っていることが多い。内部監査にとっての課題は、刻々と変化するダイナミック

＜図表16＞内部監査部門がビッグデータの監査を実施しない理由



備考：設問20：あなたの所属する内部監査部門が現在ビッグデータに関する内部監査業務を実施していない理由について、以下の文章のうち当てはまるものをすべて選択してください。(ビッグデータに関する内部監査業務を実施していないと回答した方)

なリスク環境において、スキル、知識、人材およびツールを確実に入手できるようにすることである。コ・ソーシングによってしかるべき専門家を活用することは、今後多くの内部監査部門にとって不可欠となるかもしれない。

内部監査がこの分野で卓越性を伸ばすための手段には、次のようなものがある。

■テクノロジー関連のリスクと、リスクが業務および戦略目的の達成に与える可能性のある影響に関して、よく理解する。

■組織体によるテクノロジーへの投資を活用して、サイバーセキュリティとビッグデータの監査に必要なツールを確保する。

■必要となる内部監査の能力を開発する。

■テクノロジーと業務の連携を進める手助けをする。

■プロジェクトマネジメントチームに参画することから始まり、テクノロジーに関連したリスク・マネジメントとインターナル・コントロールについてのアシュアランスを取締役会に提供することまでに至る、テクノロジーに関する包括的な内部監査業務を行う。

サイバーセキュリティとビッグデータに関する内部監査業務を行う多くの内部監査部門は、そのリスクに対応するのにふさわしいレベルに達していないようである。

信頼されるアドバイザーの地位を得ること

捉えどころがなく難しいことではあっても、内部監査は高まり続ける利害関係者の期待に応えようと進歩し続けてきた。これは、多くの者にとっては永遠の挑戦であるが、他方で、高まり続ける要求と期待の少なくとも一歩か二歩先を行くだけのことだと捉えている者もいる。

間違いなく時代遅れの会計コントロール重視から真の全社的リスクベースの監査へと進化し続けていることは、専門職にとって大躍進である。同様に、専門職の次の成熟度段階は、内部監査の計画が組織体の戦略的優先事項に整合するようにＣＡＥが大きく前進することであり、組織体が戦略目的をうまく達成することができるか（あるいはできないか）に関してＣＡＥが見識を提供することである。

では、次のステップは何か。今や多くの者が、内部監査が真に有効であるためには「信頼されるアドバイザー」として組織体全体か

ら見なされるように一層向上する必要がある、と語っている。しかし多くの場合、内部監査は組織体が最も切迫した問題を議論し経営陣が決断を下す場に（もし１つも得ていなければ）念願の「席」を得ることを未だに求めている状態である。これに対して真の信頼されるアドバイザーは、その価値を誰もが当然のものとして受け入れているので、席を得ているのである。関与させてほしいと頼むのではなく、招かれるのである。利害関係者から組織体の目的達成を促進する上でのかけがえのない人材として認められるためには、信頼されるアドバイザーとしてビジネス感覚、技術的専門知識および関係構築スキルをしっかりと身に付けなければならない。ＣＡＥとそのチームにとって、信頼されるアドバイザーとは、組織体の目的達成の促進に資する何か重要な価値のあるものを常に備えていることを意味する。

ＰｗＣ社は、『2016年内部監査全世界実態調査　リーダーシップの重要性：利害関係者の高まる期待に応えるための内部監査の「真北（真に重要な目標のたとえ)」を目指して進む』という報告書の中で、専門職が目指す姿と現状とのギャップを明らかにした。このギャップは、一般的な見解と一致している。期待があることを認めながらも、ＰｗＣ社の調査のわずか16％の回答者（ＣＡＥとその利害関係者）が、今日の内部監査は監査計画の効果的かつ効率的な実施にとどまらない付加価値のあるサービスとプロアクティブな戦略的助言を提供している、と回答している一方で、62％が今後５年以内に内部監査がよりプロアクティブな信頼されるアドバイザーとなることを期待している。同様に、デロイト社は「グローバルCAE（内部監査執行役員）サーベイ2016『進化か、衰退か？』岐路に立つ内部監査」において次のように報告した。「自部門が組織内で強い実効性と影響力を有していると回答したＣＡＥはわずか28％である。内部監査の実効性と影響力はほぼないとする割合は16％と懸念すべき値を示した。一方、今後数年間では内部監査の強化が重要と答えた割合は３分の２近くある。」[11]

> 真の信頼されるアドバイザーは、その価値を誰もが当然のものとして受け入れているので、「席」を得ているのである。関与させてほしいと頼むのではなく、招かれるのである。

内部監査はこの顕著なギャップを埋めて信頼されるアドバイザーとなるよう前進することが出来るだろうか。期待されていることを考慮すれば、プロアクティブで精力的な対策を講じなければならない。

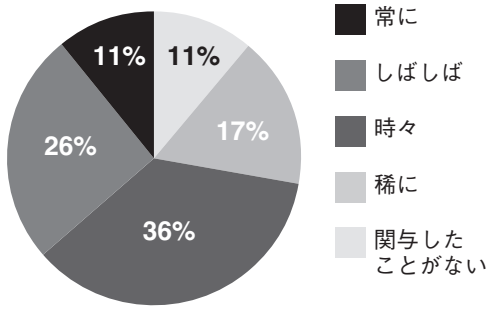
タワズン社のＣＡＥであるカレム・トウフィック・オベイド氏は、「ギャップを埋めるには、経営陣や取締役会と信頼関係を構築する必要がある。信頼は、内部監査の業務が単に頼りになり約束したことを実施するというだけではなく、先見的で洞察力に優れている場合に構築される」と述べている。残念ながら、内部監査のリーダーの大半はまだ、最高経営責任者、経営陣および監査委員会の委員長と、必要に応じて頻繁にではなく事前に取り決めた指定された時にだけ面談している。また、トップとの強固な関係の必要性を踏まえると、鋭いビジネス感覚と技術的専門知識を考慮に入れて必要な洞察力を併せ持つことはかなりの難題であろう。しかし、これは当然のことになりつつあるようである。ただ一方で、内部監査のリーダーの大部分（66％）は、組織体の主要な組織改編構想に関与するよう依頼されることはあまりないと報告しており

[11] Deloitte, “Evolution or irrelevance? Internal audit at a crossroads,” 2016, 5, http://www2.deloitte.com/global/en/pages/audit/solutions/global-chief-audit-executive-survey.html（accessed Aug. 24, 2016）.

(図表17)、３分の１近くの者は、取締役会に全く出席を依頼されていない（図表18)。結果として、少なくともこの時点では、信頼されるアドバイザーの地位は多くの者にとって「鋭意努力中」の願望のままである。

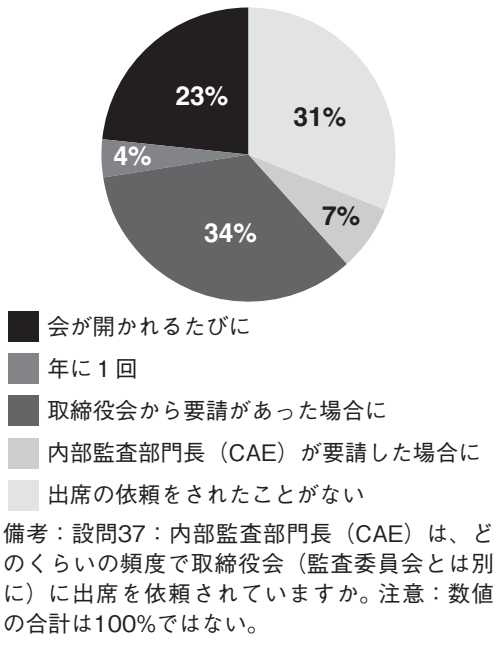
内部監査のリーダーの大部分（66％）は、組織体の主要な組織改編構想に関与するよう依頼されることはあまりないと報告しており、３分の１近くの者は、取締役会に全く出席を依頼されていない。

＜図表17＞内部監査が組織改編構想に関与する頻度



備考：設問38：内部監査部門は、どのくらいの頻度で主要な組織改変構想に関与していますか。
注意：数値の合計は100%ではない。

＜図表18＞ＣＡＥが取締役会に出席を依頼される頻度



備考：設問37：内部監査部門長（CAE）は、どのくらいの頻度で取締役会（監査委員会とは別に）に出席を依頼されていますか。注意：数値の合計は100%ではない。

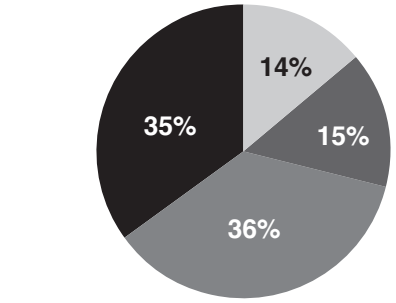
内部監査のリーダーやスタッフは、ＣＥＯ、経営陣および監査委員会委員長との関係に加えて、上級および中間管理職との関係も構築する必要がある。多くの者にとってこの関係構築は、構造的かつ反復的な関わり合いを意識的に計画することを通して、深く持続的な関係の構築に向けて取り組むことによって、最もうまく達成できる。しかし内部監査のリーダーの65％は、内部監査人が組織体内の面談したい相手と継続的に面談する正式なプログラムがないと回答している（図表19)。こうしたプログラムがなければ、内部監査のリーダーやスタッフが信頼されるアドバイザーと見なされるようにと向上するために必要な関係性のベースラインを構築し維持することは、どんな規模の組織であってもその殆どにとっては不可能ではないまでも困難であろう。

ギャップを埋めるには、経営陣や取締役会と信頼関係を構築する必要がある。信頼は、内部監査の業務が単に頼りになり約束したことを実施するというだけではなく、先見的で洞察力に優れている場合に構築される。

タワズン社　ＣＡＥ
カレム・トウフィック・オベイド氏

内部監査人と組織体の人々との交流を促す正式なプログラムがあると、内部監査が知名度を上げ、知識を豊富にし、実際に組織体内で起こっていることにより精通するのに役立つ。ＩＩＡコロンビアのＣＥＯ兼プレジデントであるアナ・クリスティーナ・ザンブラノ・プレシアド氏は、「ＣＡＥが自分をどのようにアピールするかは、組織体内でどのように認識されるかに影響を与える。」と説明している。そして、認識が現実を動かすことは誰もが知っている。しかし、調査結果によると経営陣の１人として認識されていると思っているのは、ＣＡＥのわずか26％である。明らかに残りの74％は、経営陣から同格と認識

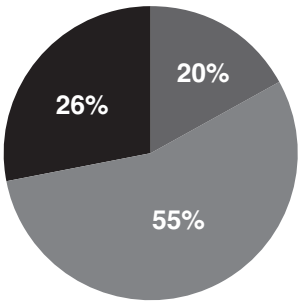
＜図表19＞内部監査人が組織体内の面談したい相手と面談する正式なプログラム



備考：設問31：内部監査部門には、内部監査人が組織体内の面談した相手と継続的に面談する正式なプログラムはありますか。

されているとは思っていない（図表20）。非常に多くのＣＡＥが組織体の経営陣として認識されていないと思っていることは、問題ある調査結果であり、信頼されるアドバイザーの地位と知名度を獲得する上での潜在的障害と考えられる。

＜図表20＞ＣＡＥに対する認識

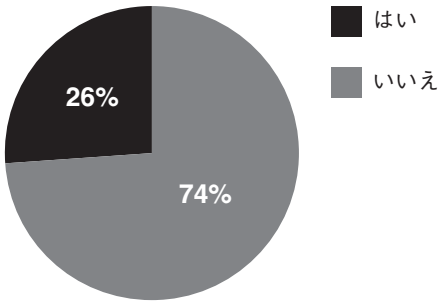


備考：設問35：内部監査部門長（CAE）は、以下のどの立場の1人として認識されていますか（CAEによる回答のみ参照）。注意：数値の合計は100%ではない。

内部監査のリーダーが組織体内で知名度と地位を強化するためのもう一つの要素は、課題はあるものの、内部監査以外の責任を負うように求められるようになることである。内部監査のリーダーの４人に１人（26％）は、内部監査以外の機能の責任を負っていると回答している（図表21）。最も頻繁に名前の挙がる機能は、リスク・マネジメントおよびコンプライアンスといった第２のディフェンスラインに焦点を合わせた機能である。

経営陣の１人として認識されていると思っているのは、ＣＡＥのわずか26％である。

＜図表21＞内部監査以外の機能の責任を負っているＣＡＥの割合



備考：設問39：あなたの所属する組織体の内部監査部門長（CAE）は、内部監査部門以外の部門の責任も有していますか。

内部監査以外の責任を負う場合は、当然、内部監査のリーダーは課題に直面する。一番の関心事は、報告経路によって左右される独立性に伴う問題だけでなく、外見上も実質上も客観性を維持することである。確かに、第２のディフェンスラインと第３のディフェンスラインの境界が曖昧になるリスクがあるので、ＣＡＥは内部監査の主な職務が何らかの形で抑えられたり損ねられたりする方向へ引っ張られないように強力に防御しなければならない。しかし、内部監査の枠を超えて権限を拡大するよう要求されることは、内部監査の知識、スキルおよび貢献が、部門を超えて組織体全体にとって意味があるものになり得る、またはなっていることをＣＡＥに示すシグナルかもしれない。

最適な報告経路、すなわち部門運営上はＣＥＯに直属し職務上は監査委員会に報告する

という多くの組織体にとって新しい考え方は、内部監査のリーダーが組織上の独立性を維持しつつ信頼されるアドバイザーとしての可能性を最大化するのに役立つ。国際的動向調査は、内部監査のリーダーの45％が、部門運営上ＣＥＯ（またはＣＥＯと同等の立場の者）に直属しており、73％が職務上取締役会または監査委員会（またはそれと同様の組織）[12]に報告していることを明らかにしている。内部監査が主に会計および財務の課題にのみ焦点を当てる型どおりの役割から脱し続けるに連れて、この比率は年々増加している。

例えばコンプライアンスまたはリスク・マネジメントの責任から内部監査の枠を超えて権限を拡大するよう要求されることは、内部監査の知識、スキルおよび貢献が、部門を超えて組織体全体にとって意味があるものになり得る、またはなっていることをＣＡＥに示すシグナルかもしれない。

結論

まず、コントロールベースの監査からリスクベースの監査へ、そして今ではボトムアップのリスク評価から内部監査の優先事項を組織体の戦略的優先事項へ整合させることへと、信頼されるアドバイザーの地位に向上するための次の波は来ている。前途では、献身的な努力と同様に評価されるスキルや求められる才能の変化への対応が求められている。しかし、これが内部監査の利害関係者が求め始めている道であり、数少ない先覚者が既に到達している場所である。

ＩＩＡの事務総長兼ＣＥＯリチャード・チャンバース氏は『インターナル・オーディター』誌のブログの中で、ＣＡＥや内部監査の貢献が評価されていないことを示す兆候を紹介した。

- 年間を通して、監査依頼があるとしてもわずかである。
- 内部監査の年間リスク評価プロセスにおいて、最小限の情報しか入ってこない。
- 事業戦略が議論または策定される会議に出席を求められない。
- 監査報告書の受領者が、無関心であるか結論や勧告に抵抗する。
- 重大なリスクが識別された際、経営者がＣＡＥではなくコンサルタントに意見を求める[13]。

最後に

大多数にとって内部監査の重要な活動を支える予算とスタッフの水準が現状維持または増加していることから、内部監査にとって利害関係者の高まる期待に応えさらに超えるために必要なもう一歩を踏み出す機会はこれまでになく大きいだろう。資源の支援がある今こそが、この機会をつかむ絶好の時かもしれない。

また、卓越性と信頼されるアドバイザーの地位を求め続けていくには、内部監査は組織体の重要な課題に取り組むために最前線にいなければならない。2016年の国際的動向調査が示すように、組織文化、サイバーセキュリティおよびビッグデータといった差し迫った課題は、内部監査の貴重な時間と労力と注目を、増やさないまでも費やす必要のある新た

[12] 部門運営上の報告先は、予算管理、人事管理、コミュニケーション、内部方針と手続の管理等、日常的な監督を行う。職務上の報告先は、内部監査基本規程の承認、監査計画の承認、ＣＡＥの業績評価、ＣＡＥの報酬の決定等、内部監査機能の責任の監督を行う。

[13] Chambers, Richard. June 14, 2016. Forensic Examination May Explain Why You Aren't a Trusted Advisor. https://iaonline.theiia.org/blogs/chambers/2016/Pages/Forensic-Examination-May-Explain-Why-You-Arent-a-Trusted-Advisor.aspx（accessed Aug. 24, 2016）.

な課題の一部である。

内部監査のリーダーは大きな前進を遂げてきたが、専門職全体としては明らかにそのペースを上げる必要があり、もちろん失速している余裕はない。

より詳しい情報の参照先

組織文化の監査

■Chartered Institute of Internal Auditors, “Organizational Culture: Evolving approaches to embedding and assurance,” May 2016, https://iia.org.uk/policy/publications/culture-evolving-approaches-to-embedding-and-assuranceboard-briefing/ (accessed Aug. 24, 2016).

■CCH Daily, “FRC calls for greater emphasis on corporate culture,” 20 Jul 2016 https://www.cchdaily.co.uk/frc-calls-greater-emphasis-corporate-culture (accessed Aug. 24, 2016).

■Financial Reporting Council, “Corporate Culture and the Role of Boards,” July 2016, https://www.frc.org.uk/Our-Work/Corporate-Governance-Reporting/Corporate-governance/Corporate-Culture-and-the-Role-of-Boards.aspx (accessed Aug. 25, 2016).

■The IIA, “Global Perspectives and Insights: Auditing Culture – A Hard Look at the Soft Stuff,” 2016, www.theiia.org/gpi (accessed Sept. 29, 2016).

テクノロジーについていく

■EY, “Creating trust in the digital world,” 2015 http://www.ey.com/Publication/vwLUAssets/EY-creating-trust-in-the-digital-world/$FILE/EY-creating-trust-inthe-digital-world.pdf (accessed Aug. 24, 2016).

■KPMG, “Global profiles of the fraudster: Technology enables and weak controls fuel the fraud,” May 2016, https://home.kpmg.com/xx/en/home/insights/2016/05/global-profiles-of-the-fraudster.html (accessed Aug. 24, 2016).

■New Vantage Partners LLC, “Big Data Executive Survey 2016,” 2016, http://newvantage.com/wp-content/uploads/2016/01/Big-Data-Executive-Survey-2016-Findings-FINAL.pdf (accessed Aug. 24, 2016).

■PwC, “US cybersecurity: Progress stalled, Key findings from the 2015 US State of Cybercrime Survey,” July 2015, http://www.pwc.com/us/cybercrime (accessed Aug. 24, 2016).

■Steve Morgan, “Cyber Crime Costs Projected to Reach $2 Trillion by 2019,” http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costsprojected-to-reach-2-trillion-by-2019/#6b96d1ae3bb0

■The IIA, “Global Perspectives and Insights: Internal Audit as Trusted Cyber Adviser,” 2016, www.theiia.org/gpi (accessed Sept. 29, 2016).

■The IIA’s Global Technology Audit Guide (GTAG), “Assessing Cybersecurity Risk: Roles of the Three Lines of Defense,” 2016, www.globaliia.org/standards-guidance (accessed Sept. 29, 2016).

信頼されるアドバイザー

■Chambers, Richard. June 14, 2016. Forensic Examination May Explain Why You Aren’t a Trusted Advisor. https://iaonline.theiia.org/blogs/chambers/2016/Pages/Forensic-Examination-May-Explain-Why-You-Arent-a-Trusted-Advisor. aspx (accessed Aug. 24, 2016).

その他

■Deloitte, “Evolution or irrelevance? Internal Audit at a crossroads,” 2016, http://www2.deloitte.com/global/en/pages/audit/solutions/global-chief-auditexecutive-survey.html (accessed Aug. 24, 2016).

■Protiviti, Arriving at Internal Audit’s Tipping Point Amid Business Transformation, 2016, http://www.protiviti.com/en-US/Pages/IA-Capabilitiesand-Needs-Survey.aspx (accessed Aug. 25, 2016).

■PwC, “2016 State of Internal Audit Profession Study, Leadership matters: Advancing toward true north as stakeholders expect more,” 2016, https://www.pwc.com/ca/en/risk/publications/pwc-state-of-internal-audit-professionstudy-2016-03-en.pdf (accessed Aug. 24, 2016).

■James Rose, “The Top 7 Skills CAEs Want,” (Altamonte Springs: The IIA Institute of Internal Auditors Research Foundation, 2016) p 2, http://theiia.mkt5790.com/CBOK_2015_Top_Skills_CAEs_Want.

■The IIA’s Position Paper, “The Three Lines of Defense in Effective Risk Management and Control,” 2013, www.theiia.org/position-papers (accessed Sept. 29, 2016).