内部監査人協会（ＩＩＡ）情報／ＣＢＯＫ調査結果（ＣＢＯＫ利害関係者レポート）

戦略リスクの監査
――内部監査のリーダーからの実践的な洞察

著者：Ｊ・マイケル・ジョイス・ジュニア
ＣＩＡ，ＣＰＡ，ＣＲＭＡ

訳者：渡　辺　知　子
プロティビティＬＬＣ　ディレクタ
ＣＩＡ，ＣＣＳＡ，ＵＳＣＰＡ（オレゴン州），ＣＩＳＡ

はじめに

内部監査の国際的共通知識体系（ＣＢＯＫ）は、内部監査の専門職の世界最大規模の継続的調査である。当調査は、主に、「内部監査の実務家」および「その利害関係者」の２つの要素により構成される。内部監査の実務家を対象とした調査は、様々な内部監査の実務を明らかにし、利害関係者への調査は内部監査の成果に関する視点を追究する目的で実施している。利害関係者に対する調査、インタビュー、データ分析は世界中の内部監査人協会（ＩＩＡ）と提携しているプロティビティが実施した。

ＣＢＯＫレポートは、個人、組織体、ＩＩＡ支部、そして世界中のＩＩＡからの厚意により、無料でダウンロードすることができる。全てのレポートはCBOK Resource Exchange（www.theiia.org/goto/CBOK）、そして利害関係者の調査結果はプロティビティのウェブサイト（www.protiviti.com）からも入手可能である。

利害関係者調査に関するデータ	
調査対象者	1,124
インタビュー対象者	112
国	23
言語	13
調査参加利害関係者のポジション	
取締役	34％
最高経営責任者（ＣＥＯ）	15％
最高財務責任者（ＣＦＯ）	18％
その他の経営幹部	33％

目　次

ＣＢＯＫ2015利害関係者への調査：対象23か国

注：ＩＩＡ調査研究財団（訳者注：現・内部監査財団（ＩＡＦ））とプロティビティは、23か国からの参加者の協力を得て、2015年７月から2016年２月にかけて、各地域の利害関係者に対する調査とインタビューを実施した。部分的回答については、回答者属性情報が揃っているものを分析対象としている。当レポートでは、質問１、質問２と示している。地図の色分けはＣＢＯＫ調査で使用された７地域区分を示している。（世界銀行のカテゴリーに準拠）

ＣＢＯＫ2015年グローバルな利害関係者調査について

このレポートは、内部監査財団の2015年共通知識体系（ＣＢＯＫ）グローバルな利害関係者調査の一部である。この調査における重要な発見事項の一つは、取締役会メンバー、ＣＥＯ、ＣＦＯ、ＣＩＯ、ＣＲＯなどの３分の２近い（64％）利害関係者が、「戦略リスクに関して、内部監査による積極的な活動を期待したい」と答えている点である。この継続的な調査のフォローアップ活動として、複数の業界の内部監査部門長（ＣＡＥ）にインタビューを行い、サイバーセキュリティ、ＩＴプロジェクト、およびキャピタルプロジェクトの３つの共通分野に焦点を当てた戦略的リスクにどのように積極的に取り組んでいるかについての洞察を得た。監査リーダーの率直な意見や見解を報告書全体を通して引用し、これらの洞察は、私たちの議論につながっている。

はじめに：戦略的リスクを監査するためのよく知られた興味深い洞察

「我々は前提条件に着目する。戦略的施策をそもそも推進したものと、これらの施策が進展するにつれて施策を推進し続ける前提条件とがある。これらの前提条件は、依然として適切か？」

サイバーセキュリティ、ＩＴプロジェクト、キャピタルプロジェクトは、組織の戦略的リスクの３つの具体的な分野であるが、内部監査機能が経営者や取締役会と連携して、これらにどのように対応しているかについて、ＣＡＥが自由に、次々と共有してくれた先導的な活動についての洞察は、なじみ深くかつ興味深いものであった。

そのなじみ深さは、これらの戦略的リスク分野における監査リーダーのリスクベースのアプローチおよび、取締役、ＣＥＯ、ＣＦＯ、

その他の経営幹部が効果的な「戦略的監査」の基本的な成功要因として内部監査が実施することを奨励する活動によるものである。戦略的施策に対して内部監査が早期に関与すること、リスクベースの監査アプローチ、ビジネスパートナーの視点での内部監査の信頼性、および助言的な方法で成功する能力といったことの重要性をＣＡＥは一貫して指摘している。これらの不可欠な要素は、トップレベルの監査組織においては、かなり前から存在していた。

この対話から出てきた重要な点が他に２つあるが、これらは予期せぬものであった。まず、内部監査機能は、幅広いアプローチ（サイバーセキュリティ、ＩＴプロジェクト、およびキャピタルプロジェクトのセクションで述べたような）を活用することによって、戦略的リスクの監査およびその対処において著しい進展を見せている。第２に、先進的な内部監査機能は、意思決定の場における自らの存在意義、機能の信頼性、および具体的な手法を通じたアドバイザーとして認められるよう（このレポートの最後の部分で要約されている）勤勉かつ独創的に取り組んでいる。

インタビューは２つの目的を持って実施された。先導的な監査幹部は、戦略的なリスクにどのように対処するかを述べることで、機能のビジネス部門の戦略的パートナーとしての役割をはぐくむ方法に加え、何よりもまずコンプライアンスとアシュアランスの責任重視が揺るぎないものであることを強調した。

サイバーセキュリティは隔絶された中に存在しない

「サイバーセキュリティは、脅威から身を守り、効率的に機能させるために、全ての人体の器官および部位とが協力して働くように機能しなければならない。それは独立したプロセスではない。サイバーセキュリティに影響を与えない要素は一つとしてない。」

サイバーセキュリティ監査を戦争で破壊された地域における大規模なキャピタルプロジェクトの監査と比べてどうかと尋ねたところ、とあるＣＡＥは直ちに回答した。「私たちのキャピタルプロジェクトはそこまで複雑ではなく、かつ困難ではない。」

監査委員会は、圧倒的な戦略的リスクであるサイバーセキュリティに対処する組織の能力に関する最新情報を求めている。ＣＡＥは、正式なリスクアセスメント、サイバーセキュリティステアリングコミッティや演習への直接的な関与などを通じて組織のサイバーセキュリティについての見解を磨き、監査計画におけるサイバーセキュリティ関連分野の拡大、リスク管理活動とＩＴ、情報セキュリティ、ＥＲＭ（全体的リスクマネジメント）機能との調和などの複数の手段により対応している。

全体として、インタビューをしたＣＡＥは、サイバーセキュリティ監査の効果を説明する際に、以下の活動とベストプラクティスを最も頻繁に引用している。

戦略的リスク監査のベストプラクティス：サイバーセキュリティ

- **サイバーセキュリティ戦略を策定し、方向付ける人たちと協働する。**
- **サイバーセキュリティリスクの責任について明確にし、他者と連携する。**
- **正式なリスクアセスメントを実施する。**
- **サイバーセキュリティのフレームワーク、基準、ガイダンスについて助言する。**
- **サイバーレジリエンス（対応力）を評価する。**
- **継続的に学ぶ（継続学習）。**
- **サイバーセキュリティのスキルと専門性の課題を自らのものとして認知する。**

●**サイバーセキュリティ戦略を策定し、方向付ける人たちと協働する**：監査の指導者たちは、「サイバーセキュリティ」という言葉が現在の意味と重要性を持つ前から、アイデンティティ管理、パッチ管理および他の多くの形態のサイバーセキュリティ監査をすでに実施していた点を強調しつつ、最近は、組織的なサイバーセキュリティ戦略と能力を設定し、強化する責任を負う委員会への助言的役割を求めている。あるＣＡＥは別の選択肢として次のように述べている。「監査委員会と連携して、重要かつタイムリーなサイバーセキュリティ問題に関連する情報を提供できる外部の専門家からなるサイバーセキュリティ専門の小委員会を編成し、監査委員会に報告する。」

●**サイバーセキュリティリスクの責任について明確にし、他者と連携する**：ＣＡＥはＩＴ、情報セキュリティ、ＥＲＭグループの各パートナーと緊密に連携し、各グループが実施している具体的なサイバーセキュリティ活動を識別する。この連携は、サイバーセキュリティに関する組織内の全ての取り組みを同期させ、サイバーセキュリティリスクに対して客観的で独立したアシュアランスを提供するという内部監査の役割を強化するのに役立つ。あるＣＡＥは「共通のリスク評価アプローチに基づいて協働している」ことを示すために、監査委員会において、ＣＩＯと共にサイバーセキュリティリスクのプレゼンテーションを行っている。

●**正式なリスクアセスメントを実施する**：内部監査あるいは第三者の専門家が行っているかどうかを問わず、正式なリスクアセスメントは、サイバーセキュリティ対応の重要な部分である。これらの評価は、ギャップを識別し、改善および是正の優先順位を明確にし（例えば、フィッシング電子メールの大幅な増加に対処する。）、サイバーセキュリティ側面の監査計画の決定に役立ち、サイバーセキュリティの助言業務に影響を与え、そして組織がサイバーセキュリティリスクと改善目標を合わせるのに役立つ。

●**サイバーセキュリティのフレームワーク、基準、ガイダンスについて助言する**：全てのＣＡＥは、サイバーセキュリティプログラムと関連するアシュアランス活動の構築にあたり、彼らの組織が用いている１つあるいは複数のサイバーセキュリティ基準について言及した。これらの基準には、ＮＩＳＴサイバーセキュリティフレームワーク、ＥＲＭ、ＨＩＴＲＵＳＴ、ＣＯＢＩＴ、ＩＳＯ、ＩＩＡ監査の国際的ガイダンス（ＧＴＡＧ）：サイバーセキュリティリスクの評価：３つのディフェンスライン、ＣＳＣ20、ＦＦＩＥＣなどが含まれる。あるＣＡＥは、一貫性、透明性、およびそれが可能にするサイバーセキュリティリスクへの広範なエクスポージャーなどの点につきＥＲＭフレームワークの多くの利点を称賛したが、一方で「このフレームワークは、インド、オーストラリア、または他の地域では十分ではないかもしれない。これらの地域では、他のサイバーセキュリティリスク管理モデルが使用されている。我々は、全てのモデルの中から最も優れていると考えるものを採用し、グローバルなニーズを満たすために適用した。」と強調している。フレームワークの候補、それぞれの利点と欠点についての議論と評価にＣＡＥが直接関与することにより、組織がフレームワークから最大の価値を引き出すことに内部監査が支援することができる。

●**サイバーレジリエンス（対応力）を評価する**：ＣＡＥは、今日の環境において、侵害は避けられないという事実を受け入れ、侵害が発生した場合の、組織の対応、コミュニケーション、復旧能力を評価する必要が

ある。考慮すべき分野には、事業継続手順だけでなく、コミュニケーションおよび危機管理計画も含まれる。

- **継続的に学ぶ（継続学習）**：外部からの脅威、新たな基準、新しいコンプライアンス要件、さらには心理的プロファイリングについての知識は、サイバーセキュリティ監査の成功にとって不可欠な要因である。あるＣＡＥは「私はＣＩＳＳＰ資格者です。」と告げ、「サイバーセキュリティの学習と研究に多大な時間を費やしている。例えば、Equifaxがどのように情報が流出したのかを正確に知りたい」と述べた。このＣＡＥは、故意もしくは無意識に自社をサイバーセキュリティの脅威に曝す可能性のある広範な利害関係者の考え方を理解する必要性を彼のチームに対して強く説いている。「内部監査は、ハッカーの思考過程とメソドロジを理解する必要がある。」と彼は語った。「内部監査人は、会計士、投資家、弁護士、コンプライアンススペシャリスト、セールスマン、人事エグゼクティブなど企業をサイバーセキュリティの崩壊にさらすリスクを引き起こす可能性のある人のように考えることができなければならない。」そして機能のアシュアランス業務は、組織全体で実施されるサイバーセキュリティトレーニングと意識向上の有効性に関連している。
- **サイバーセキュリティのスキルと専門性の課題を自らのものとして認知する**：ほとんどのＣＡＥは、ＩＴとサイバーセキュリティの専門知識を持つ内部監査人を雇用し、保持することは課題であると認めている。トレーニングや能力開発への投資、外部専門家の活用の他、人事と緊密に連携して、採用、パフォーマンス、人材保持のインセンティブの整備などの人材管理戦略と戦術によってこの課題に対処している。

ＩＴプロジェクト：データ、開発、行動の精緻化

「サイバーセキュリティとＩＴプロジェクトは別物と考えると、誤解を招く。」

より多くの企業がデジタル・トランスフォーメーションを行い、より多くのＩＴシステムとアプリケーションがクラウドに移行するにつれて、あらゆる規模と範囲のＩＴプロジェクトの大規模な収集が戦略的リスクとなる。その結果、より幅広いＩＴプロジェクトやアプリケーション開発活動が監査によって精査される必要がある。

この精査は、内部監査機能にも役立つ。あるＣＡＥは、大規模なソフトウェア導入においてシステムのテストを担当した第三者が、十分な明確さをもってテスト結果を提供しなかったことについてＩＴ監査人が懸念を抱いていたことを思い起こした。「我々は慎重に進み、テスト結果に満足できておらず、サインオフを提供する準備ができていないという主張を裏付ける事実を持っていた。」と説明する。彼のチームの綿密な文書は、システムが稼動する前に追加のテストが必要であることを会社に納得させた。「そのことは、機能として、私たちの存在を確立するのに役立った。」とその経営幹部は続ける。「それ以来、ソフトウェアテストのライフサイクルは改善し続けている。」

同様の詳細な精査と事実に基づく勇気は、監査リーダーがＩＴプロジェクトの監査を有益なものとする上で重要な役割を果たす。

戦略的リスク監査のベストプラクティス：ＩＴプロジェクト

- **複数のフェーズにわたる構造化された評価プロセスを開発する。**
- **行動障壁を取り除く。**
- **アシュアランス業務を補完する提供可能**

な助言業務を開発する。
- アジャイル開発に対処する必要性を認識する。

●**複数のフェーズにわたる構造化された評価プロセスを開発する**：ＣＡＥは、ＩＴプロジェクトの各フェーズにつき構造化された評価を開発し、改善することの価値を強調している。新規導入やシステム変更に伴うデータの量、価値、重要性が増していることを考慮し、セキュリティはプロジェクト評価の出発点として識別されることがよくある。あるＣＡＥは、彼女が率いるＩＴ監査チームがＩＴプロジェクトを現在どのように２つのグループに編成しているかをこう説明した。１つは、財務統制が関係するシステム変更で、ＩＴおよび財務監査人によるが関与が必要となる。第２のカテゴリは、より従来のＩＴプロジェクト管理方法、ガバナンス、効率性に重点を置いている。

●**行動障壁を取り除く**：あるＣＡＥは、ＩＴプロジェクトチームが軽視した、あるいは完全に発見しなかった問題が実際に起きた多くのケースをＩＴ監査チームがどのように多数発見したかを詳述した。その後、内部監査グループは、それらのプロジェクトチームとのコミュニケーションを一新した。「重要な問題を取り上げたくないことがわかったら、我々は彼らがより気軽にできるように働きかけた。」と、監査リーダーは説明した。「赤色、黄色、緑色の評価システムに関しては、『赤色は死んでいない』という新しいマントラを始めた。」また、ＩＴ監査チームは、プロジェクトのライフサイクルにおいて、より早期に問題を浮上させ、解決することの利点について明確に示した。後になると、小さな問題の影響とコストは、はるかに大きくなる可能性がある。

●**アシュアランス業務を補完する提供可能な助言業務を開発する**：あるＩＴ監査グループは、ＩＴプロジェクトの正式な監査を行う際にＩＴ監査人が評価するものよりも概要レベルの基準からなる助言業務を開発した。（例えば、導入戦略はあるか？　スポンサーは誰か？　資金は承認されているか？　既知のプロジェクトリスクは何か？　何らかの緊急時計画が必要か？）ＩＴ監査人とＩＴプロジェクトチームが質問のリストを理解し、合意した後、ＩＴ監査人は正式なマネージメントによる行動計画ではなく、推奨事項を提示する。「それはとても好意的に受け入れられている。」とＣＡＥは言う。「我々が文書化し、共有した手順を、彼ら自身が行うため、今ではこのサービスをほとんど必要としない。」

●**アジャイル開発に対処する必要性を認識する**：我々が話し合った多くのＣＡＥは、現在、より多くのＩＴ機能が採用しているアジャイル開発メソドロジに関連するリスクに対処する方法を決定している。この高度に協調的で反復的で合理化されたソフトウェアの開発アプローチは、新しいアプリケーションの作成に間接的にかかわる時間を大幅に短縮し、組織の俊敏性を向上させ、市場投入をスピードアップするが、アジャイルメソドロジはリスク関連の課題を引き起こす。「監査の観点から、要件のトレーサビリティや、開発チームが設計上の正しい承認を取得しているかどうかなどを把握しなければならない。」と監査幹部は言う。「アジャイル開発は組織に利益をもたらすが、新たなリスクももたらす。」

キャピタルプロジェクト：プロセスが全てである

「我々はプロセスを監査するのであって、人を監査するのではない。」

機能が大規模なキャピタルプロジェクトの監査と評価を行う場合、ＣＡＥは、２つを区別することの重要性を強調する傾向がある。第１は、経営陣の責任である各キャピタルプロジェクトの健全性と進捗状況の監視と、内部監査が提供するアシュアランスを区別することが重要であると彼らは言う。第２に、先導的なＣＡＥは、個々のキャピタルプロジェクトに関する作業と、組織の全体的なキャピタルプロジェクト管理能力を評価する必要性とを区別する。後者は前者に大きく役立っている。

ＣＡＥは、キャピタルプロジェクトのアシュアランスと助言業務の有効性を促進する上で特に役立つものとして、以下の活動とベストプラクティスを挙げた。

戦略的リスク監査のベストプラクティス：キャピタルプロジェクト

- **計画段階の早期に関与する。**
- **投資の基礎となる根拠に焦点を当てる。**
- **専門的なスキルと知識を活用する。**
- **厳密でプロセス重視のプロジェクトレビューを実施する。**
- **キャピタルプロジェクト管理の改善について相談する。**
- **事後監査とレビューを実施する。**

●**計画段階の早期に関与する**：内部監査が戦略的施策に早期に関与することは、組織にとって有益であるが、これは、例えば、地球の反対側で行われる５億ドルの複数年にわたる基礎工事プロジェクトの場合は特に当てはまる。こうした関与は、しばしば、プロジェクトガバナンス体制に重点を置いた初期段階のリスクアセスメントにつながる。こうしたリスクアセスメントによって、エンジニアリンググループ、調達グループ、建設請負業者（および就いた人）の役割など、根本的な変更が生じたことがある、とあるＣＡＥは報告した。

●**投資の基礎となる根拠に焦点を当てる**：多くのキャピタルプロジェクトは完成するまでに数年を要し、投資決定の基礎となる前提は時間とともに変化する可能性がある。キャピタルプロジェクト監査の一環として、ＣＡＥとそのチームは、意思決定の前提条件を検証するために使用されているデータソースを識別する。「我々は、理にかなっていて、かつ合理的にテストできる前提条件を選択してテストする。」と彼は続けている。「『どんな事実に基づいたか？　モデリングを行った場合、モデルが正確であることはどのようにしてわかるか？　数式は整合性がとられていることはどのようにわかるか？　予想投資収益率は確認・検証されているか？』と我々は質問する。」

●**専門的なスキルと知識を活用する**：あるＣＡＥは最近、外部の建設監査人を雇い、これまでにその会社が建設したことのない種類の建造物に関する請負業者からの請求書を精査した。「その投資のおかげで、そのタイプの建設プロジェクトで経験を積んだ人だけができるであろう技術的な質問をすることができた。」と彼は述べた。また別のリーダーたちは、大規模なキャピタルプロジェクトと建設経験がある内部監査人を雇用している。彼らは作業現場を歩き、プロジェクト会議に出席し、進捗レポートを確認する際、探すべき問題を知っており、必要に応じて質問し、議論する。

●**厳密でプロセス重視のプロジェクトレビューを実施する**：ほとんどの場合、キャピタルプロジェクトの監査は包括的で非常にマニュアルである。ガバナンスの評価は、プロジェクトのスティアリングチームが的を射たリスクに焦点を当てているか、正確で完全でタイムリーな情報を受け取っているかどうかを判断する。完了の進捗状況と予算の評価には大量の情報をレビューする必要がある。一般請負業者の支払い申請に付

随する証跡資料は特に分厚い傾向がある。厳密なアプローチが絶対に必要であるが、監査が個人ではなくプロセスに焦点をおいていることをプロジェクト管理者に対して明確にする必要性をＣＡＥは一貫して強調している。このバランスを守るために、監査人は、リスク、内部統制、およびその他の監査用語および考え方を、時間がないプロジェクトマネージャーに浸透する言葉に翻訳する必要がある。

- **キャピタルプロジェクト管理の改善について相談する**：ある内部監査機能は、キャピタルプロジェクトチームが新しい施策の開始時に使用できる助言を提供した。このサービスは、チームが考慮すべき主要な運用の統制、財務統制、プロジェクトリスク、および請負業者の請求行為に関する不正の知識および予防のトレーニングに関するガイダンスを提供する。ＣＡＥは、「この役割における我々の目標は、早期の期日や導入の成功の邪魔をすることなく、リスクアドバイザーかつ戦略的パートナーになることである。」別の内部監査グループは、同社のキャピタルプロジェクト管理能力の向上、具体的には投資収益率の測定および監視を中心とした戦略的施策に参加した。この組織では、内部監査機能の役割は、チームが開発する新しいプロセスに適切な統制が組み込まれていることを担保することである。
- **事後監査とレビューを実施する**：これらの活動の結果、キャピタルプロジェクトを正当化するために使用された元の前提条件の妥当性に関する価値のあるフィードバックを提供し、プロジェクトの早期における内部監査の関与の可能性も含め、将来のプロジェクトのアプローチを強化することができる。

先進的な内部監査機能の４つの成功要因

上記で識別された項目に加えて、ＣＡＥからのコメントと洞察は、戦略的監査活動の成功にとって重要ないくつかの基礎的な要因を明らかにしている。これらの要素は、インタビューされたＣＡＥが担当しているそれぞれの監査機能に存在する。

４つの成功要因：
１．継続的な価値の実証
２．アクセス
３．共通用語（言語）
４．参加

１．継続的な価値の実証：ほとんどのＣＡＥは、内部監査機能がビジネスにとってのアシュアランスと助言の戦略的パートナーとして受け入れられたことのきっかけに関することを記述している。スーパーヒーローがいかに別世界のパワーを手に入れたかを見せる映画の予告編のように、これらの記述は、内部監査の行動が、経営幹部、取締役、プロセスオーナーの内部監査機能に対する見方を変えたことに関する事実や状況を示している。特に、内部監査の指導者は、価値を明確に示し続けることで機能が苦労して勝ち得た評判を育み、維持していかなければならないと強調している。新しいリーダーとプロセスオーナーが組織に継続的に加わってくる。遅かれ早かれ、彼らは内部監査の信頼性が正当であるという証拠を求めてくる。

２．アクセス：内部監査機能の価値および継続的な関係構築に対するＣＡＥのコミットメントを明確に示すことで、これらのリーダーたちは、取締役、経営幹部、およびプロセスオーナーにアクセスするという重要な特権を手に入れることができる。こうしたアクセスができるということは、組織全

体で何が起こっているのか、また今後どのような戦略的な変化や施策があるのかについての貴重な知識が得られることを意味する。

３．共通用語（言語）：「内部統制」という用語をＩＴ部門、ＣＩＳＯ、キャピタルプロジェクトマネージャー、および他のプロセスオーナーが、彼らを取り巻く環境において完全に理解できる用語に変換することの重要性を述べたＣＡＥは非常に多い。ある監査幹部の一人は、「工場、機能、場所などを対象が何であれ、内部統制は、それらを目標に向かって動かすプロセスを意味するという定義に変えている。」と述べた。ＣＡＥは、機能の全ての作業を、実用的で、よく理解され、利害関係者の環境の中で、意義のある用語（言葉）に変換する必要性を強調している。

４．参加：先進的な監査機能は、積極的かつよく関与する傾向があります。彼らは、サイバーセキュリティの侵害を明らかにするために設計された卓上のインシデント対応活動に参加している。彼らは店舗や作業現場で有意義な時間を過ごす。「私たちは監査計画の一環としてネットワーク侵入テストを実施している」と、あるＣＡＥは述べた。リーダーが取締役と共有しているこれらの情報は、サイバーセキュリティリスクについての監査委員会への報告をより具体的なものにするのに役立つ。

最終的な考え方：助言の前にまずアシュアランス

ＣＡＥは、組織が戦略リスクに対処するために機能が提供する助言サービスの興味深いコレクションについて記述しているが、アシュアランス業務が常に最優先であることも強調している。

この逸話が全てを語っている：新たに雇用されたシニア監査人が、業務に就いて数週間後に、ＣＡＥになぜ機能としてより積極的に助言サービスの拡大を進めないのか尋ねた。彼の回答は、機能の優先順位を明らかにした。彼は、「助言サービスでリードするのではなく、アシュアランス業務でビジネスをしてきた顧客を持っており、その顧客は我々の価値観を理解し、助言サービスを依頼している。私はこれが顧客を得る方法だと考えている。」と説明した。

筆者について

Ｊ・マイケル・ジョイス・ジュニア氏は、ＣＩＡ、ＣＰＡ、ＣＲＭＡ、ＦＡＨＭの資格を保持しており、36の独立したコミュニティベースのローカルに運営されているBlue CrossおよびBlue Shield社の連合体であるBlue Cross Blue Shield Association（ＢＣＢＳＡ）の副総裁、チーフ・オーディター、コンプライアンスオフィサーを務めている。Blueシステムは、全米の人工の３分の１にあたる１億700万人以上の会員をカバーする、米国最大の医療保険会社である。ジョイス氏は、内部監査、全国の反不正行為およびコンプライアンススタッフの機能を指揮している。氏は35年にわたる専門家としての経験を持ち、1999年６月からＢＣＢＳＡに在籍している。氏は1989年以来、ＩＩＡボランティアとして活躍している。

内部監査財団について

ＣＢＯＫを運営している内部監査財団は、過去40年間にわたり内部監査の専門職のために革新的調査研究を行ってきた。内部監査財団は、現在の課題、新たな傾向、将来のニーズを探索する取り組みを通して、専門職の進化と発展を支える原動力となっている。

問合せ先：1035 Greenwood Blvd., Suite 401,

Lake Mary, Florida 32746, USA.

プロティビティについて

プロティビティは、企業のリーダーが自信をもって未来に立ち向かえるように、高い専門性と客観性のある洞察力、クライアントに合ったアプローチや最善の協力を提供するグローバルコンサルティングファームである。

20か国、70を超える拠点で、プロティビティと独立したメンバーファームはクライアントに、ガバナンス、リスク、内部監査、経理財務、テクノロジ、オペレーション、データ分析におけるコンサルティングサービスを提供している。

プロティビティはこれまでに、フォーチュン1000（FORTUNE 1000®）企業の60％以上、またフォーチュン・グローバル500（FORTUNE Global 500®）中35％の企業に利用いただいている。プロティビティの人材や職場は、フォーチュン誌やコンサルティング・マガジン誌の「働きがいのある会社ベスト100」などで常に評価されている。

プロティビティは公認会計士事務所としてライセンスまたは登録されておらず、財務諸表やアテステーション・サービスの提供も行っていない。