内部監査人協会（ＩＩＡ）情報／ＣＢＯＫ調査結果

金融サービス監査のグローバルな展望
― 課題、機会、将来 ―

著者：ジェニファー F. バーク（CPA, CRP, CFF, CFS）
クロウ・ホーワス社　金融サービス・リスク・プラクティス　パートナー

スティーブン E. ジェームソン（CIA, CFSA, CRMA, CPA, CFE）
コミュニティ信託銀行　エグゼクティブ・ヴァイスプレジデント
最高内部監査兼リスク管理責任者

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

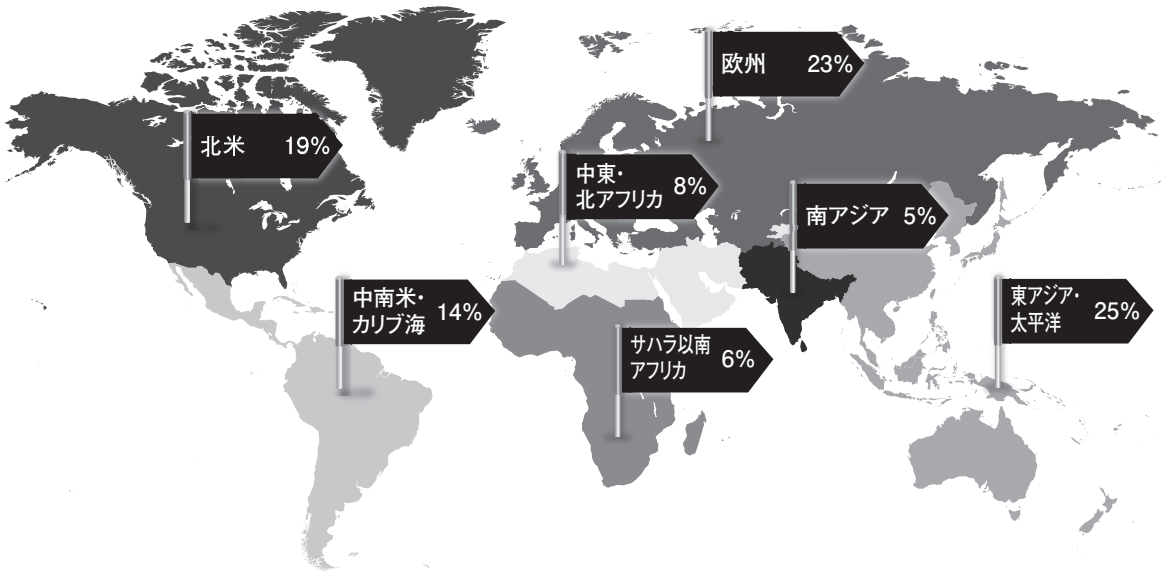
これらのレポートは、テクノロジー、リスク、素質等の８つの異なる側面から研究されている。

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

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

現在以上に課題が多い時代はなかったと、金融サービス業界の多くの人々が思っているだろう。金融機関の内部監査人は多くの課題に直面しているが、本レポートは以下の重要課題に焦点を当てている。

1．通常、金融機関のほとんどがリスクリストの上位に掲げている、規制上の要件
2．増え続けるガバナンス関連委員会の議題の管理
3．内部監査人への期待の高まり
4．サイバー犯罪者が防衛策を突破する新たな方法を見つけるたびに増えるテクノロジーリスク
5．３つのディフェンスライン間での連携
6．リソース配分管理

法規制の遵守という課題は、優先順位リストを上昇し続け、バックオフィスから役員室に至るまでの各種の議論の出発点となることが多い。新たな規則の制定や既存の規則の改正は、スタッフの増員、新たなテクノロジー、プロセスの見直しなどのための支出の増加と、手数料や収益の削減さえも金融機関に求めてきた。このような変更は極めて包括的であり、金融機関の間接的なパートナーやベンダーにも著しい影響を与えている。

ガバナンス活動や監督に携わる者は、自身の業務量が増してきていると感じている。大量の議題をカバーするためにより長く多くの会議を行う時間が必要になったため、金融機関は討議すべき増え続ける諸問題に十分な時間を充てるために、一層の効率性が求められている。出席者数の増加も、ガバナンス関連会議を長引かせる一因となっている。

内部監査人は長年、自身が所属する金融機関でその存在を認められ戦略的討議に加わるよう要請されることを念願してきたが、内部監査部門の地位を高めたさまざまな利害関係者からの期待の高まりは、独自の難題ももたらした。問題、弱点、コントロールされていないリスクに焦点を当てるという内部監査の性質上、このような期待の高まりは内部監査人に正しい決断を下すようにと一層のプレッシャーをかけ、また、誤った決断を下す者への影響も大きくなった。

内部監査人は、限られたリソースを有効に活用しながら広範囲な監査対象領域をカバーするために、テクノロジーを利用することが多い。現在、テクノロジーは急速に広がっているので、有効なコントロールを維持するのはほとんど不可能である。このような試練に追い打ちをかけて、犯罪者は今やテクノロジーを金融機関とその顧客に対するグローバルな継続的攻撃に悪用している。

金融機関の内部監査人が直面する多くの難題に立ち向かうための新たなディフェンスモデルが作成され採用されていることから、希望の光もいくらか射している。３つのディフェンスラインは、近年、世界中で広く受け入れられ採用されているモデルの1つである。金融機関の内部監査人には、自身が所属する組織に役立つようにこのモデルを効果的に導入する方法を見いだすことが求められている。小規模な金融機関では、第２と第３のディフェンスラインの境界が曖昧なことが多いので、内部監査人には役割と責任を明確にすることが課せられている。

世代的な相違、求められるスキルセットの拡大、リソースプールの縮小、内部監査部門長（ＣＡＥ）のローテーションプログラムは、内部監査のリソース管理に課題をもたらしている。このような課題は、昔からずっとＣＡＥの職務の一部である。それ自体は新たな課題ではないが、リソース管理のためにかつて用いていた方法が今でも常にうまく機能するわけではないので、将来のためにリソースの獲得と管理の新たな方法を策定しなければならない。

１．金融サービスの内部監査人にとっての規制上の課題

金融サービスの内部監査人に安眠を妨げるものは何かと尋ねたら、彼らの多くは数ある重要リスクの上位に掲げる規制上の課題であると答えるだろう。法規制の遵守が主に法務部とコンプライアンス部に委ねられていた頃は、内部監査人は財務と業務の問題に専念していたが、今や法規制の遵守は、金融機関のあらゆる機能に関係している。

2015年に内部監査部門が最も焦点を当てるリスク分野上位５つを世界中のＣＡＥに尋ねたところ、コンプライアンスリスクと規制上のリスクがトップになった。コンプライアンスリスクと規制上のリスクの次は業務（オペレーショナル）リスクであった（図表１参照）。金融セクターのＣＡＥは、監査計画ではコンプライアンスに集中するよりは業務リスクにより多くの割合を充てているが、コンプライアンスリスクと規制上のリスクにも着目している（図表２）。

＜図表１＞ＣＡＥが2015年に焦点を当てるリスク分野

リスク分野	回答割合
コンプライアンス・規制当局	83%
業務（オペレーショナル）	78%
リスクマネジメントのアシュアランス・有効性	68%
情報技術	67%
戦略的ビジネスリスク	53%

注：質問66「あなたの内部監査部門が2015年に最大の焦点を当てている上位5つのリスクを特定してください。」CAEのみ回答。金融セクターのみ抽出。回答数＝582。

「規制の変更は必要以上の複雑性をもたらすので、今や事前準備がより重要であり、組織は規制変更による減収も見込まなければならない。」

オレゴン州ポートランド、ユニタス地域信用組合　最高リスク責任者
ジェームス・アレクサンダー氏

＜図表２＞2015年の監査計画で高い割合を占めるリスク分野

リスク分野	回答割合
業務（オペレーショナル）	25%
コンプライアンス・規制当局	16%
リスクマネジメントのアシュアランス・有効性	14%
情報技術	11%
戦略的ビジネスリスク	10%

注：質問49「あなたの2015年の監査計画は、以下の一般的なリスクカテゴリーについて何パーセントを占めていますか？（合計で100％にしてください。）」CAEのみ回答。金融セクターのみ抽出。回答数＝558。

世界中の新たな規制機関と法律

かつては、規制の変更の影響はそれほど大きくなかったようで、消費者へのディスクロージャーの内容、方法、書式の改訂などに影響を及ぼすくらいものであった。しかし、ここ数年の規制の変更は、ディスクロージャー書類上で何をどのように発表するかに影響するだけでなく、システムやプロセスの根本的な運用変更も求めている。これらの変更は、複数のシステムや業務ユニットに無限連鎖的な影響を及ぼしているようである。今日の規制の変更は、以前に比べてより大きくより重く銀行業務にのしかかっている。

金融機関を監督しモニタリングするために、大きな権限を持った規制機関が新設された。インドネシアの金融サービス機構、英国の金融行動監督機構と健全性（プルーデンス）規制機構、米国の消費者金融保護局は、世界中の新設統治機構のほんの一例である。

新たな法律や規則の制定は、その量も頻度も増加の一途をたどっている。規則の制定や改正の例には、国際決済銀行のバーゼル委員会が公表した、規制、監督、リスクマネジメントを強化するための包括的改善策であるバーゼルⅢや、EUの金融商品市場指令の見直し（MiFID Ⅱ）と金融商品市場規制（MiFIR）などがある。

以前は、法律や規則の制定や改正には、制定や改正の影響を受ける者が効果的に導入で

きるように、パブリックコメントのための公開草案、合意形成、十分な導入準備期間が含まれていた。しかし、このようなアプローチは、どんな代償を払っても消費者と投資家を守るというスローガンの下で便宜を重視したプロセスによって一掃された。多くの人々はこの新たなアプローチを「取り締まりによる規制（regulation by enforcement)」と表現する。過去数年間で金融機関に課された罰金は、数十億ドルにも達する。

従来、金融サービス業界の内部監査人は、法規制遵守関連の監査にあまり携わってこなかった。法規制遵守関連の監査やレビューは、通常、内部監査とは別のコンプライアンスグループが行っていた。しかし最近は、特に規制変更による業務への影響や法規制を遵守しないリスクの増加により、内部監査グループが法規制遵守問題に一層関与するようになっている。内部監査の関与の仕方には、コンプライアンス監査、コンプライアンスグループの監査、法規制遵守状況の追跡とモニタリング、コンプライアンス変更による業務への影響評価、消費者の苦情をモニタリングするシステムの確認、従業員向けの法規制研修の適切性評価、立ち入りまたは常駐する大勢の検査官と自社との連絡調整役などがある。

> ウォール街および世界の大手金融機関は、金融危機以降１千億米ドルを罰金と和解金として支払っており、半分以上が過去１年以内のものである。
>
> 2014年３月25日付フィナンシャル・タイムズ電子版

内部監査人に対する規制当局の期待もまた著しく高まっているが、金融機関の規模や所管する個々の規制当局により期待は異なる。多くの場合、金融機関に対する規制当局の期待は、ＩＩＡの『内部監査の専門職的実施の国際基準（基準)』をはるかに超えており、特に独立性、報告体制、監査対象範囲、監査報告書、経営者への異議申し立てなどの分野がそうである。また、組織内のリスクとコントロールの文化について内部監査がレビューし意見を出すように規制当局が求める国もある。このような期待は、「内部監査は規制当局と正式で直接の報告関係を持つべきかもしれない」という提言を耳にするほどに高まってきた。さまざまな間接的報告関係が既に整っている国もある。

かつてないほどの規制当局の権限拡大の中で、金融機関のベンダーまでもが規制当局の監視対象になっている。金融規制当局は通常、金融機関以外の組織を直接規制することはできないが、金融機関のベンダーに対して「法規制に従うか、あるいはベンダーとしての資格をはく奪されるリスクを取るか」と迫る形で、新たな法規制が金融機関に対して制定・施行されている。ベンダーに本業とは関係ない問題があった場合の評判リスクであっても、金融機関に対する規制当局の監視が強まることがある。

金融機関にとって法規制の遵守は、かつては主にコストの問題であったが、今では法規制の制定・施行は収益源に影響するようになっている。法規制遵守に関連するリスクのリストは、コストの増加、収益の減少、主な業務やテクノロジーの変更、ベンダーとの関係、罰金の可能性、刑罰、顧客手数料の返還などを既に満載している。しかし、より厳しい見方をするならば、このリストに戦略リスクと評判リスクを加えることが可能である。法規制遵守の問題は、集団訴訟、投資家による訴訟と委任状争奪戦、消費者擁護団体からの要求、規制当局からの公開覚書、問題解決のための取締役会からのプレッシャーなどの核心になっている。法規制の負担は単独の組織で対応するには大きすぎるため、合併を模索する金融機関もある。

「銀行を監視するために規制当局は内部監査への依存を強めているので、多くの銀行が当局対応専門の監査チームを作ることを検討している。これは監査チームが直面している人員数の制約という問題を緩和するだろう。」

南アフリカ、ファーストランド社ＣＡＥ
ジェニサ・ジョン氏

２．監査委員会とリスク委員会での数多くの議題

さまざまな方面から課せられるさらなる責任に対処するために、監査委員会とリスク委員会の議題は拡大し続け、会議時間は貴重なものになっている。株主と投資家の期待は増え続け、規制当局の期待も減る気配はない。取締役会は、監査委員会とリスク委員会が取締役会の受託者責任の遂行を支援してくれることや訴訟や規制措置への賠償責任にある程度の制限を設けてくれることを求めている。

監査委員会とリスク委員会の開催頻度と開催時間がともに増え続けている。調査回答者によると、金融セクターは年平均6.7回正式な監査委員会を開催しており、他のあらゆる種類の組織より多い（図表３参照）。

金融セクターは、より多く会議を開催していることに加えて議題数と会議参加者数が増え続けているため、各議題に割り当てられる時間は減っている。対処すべき問題がより複雑になっているので、より長い討議が必要になっている。監査委員会とリスク委員会の委員に対する要求事項が増えているため、委員はより多くの質問をし、会議ではより多くの説明と討議が必要になっている。監査委員会の委員が関与と交流を深めるのは一般的には良いことであるが、一層の時間と労力が必要になる。

会議の出席者は増えており、最高経営責任者（ＣＥＯ）、最高財務責任者（ＣＦＯ）、内部監査部門長（ＣＡＥ）、最高リスク管理責任者（ＣＲＯ）、最高コンプライアンス責任者（ＣＣＯ）、最高テクノロジー責任者（ＣＴＯ）、最高プライバシー責任者（ＣＰＯ）、法律顧問、議題の対象となる事業部門の経営者、ローンレビュー管理者、セキュリティ責任者、反マネーロンダリング責任者、米国銀行秘密法責任者、外部監査人、外部のアドバイザーやコンサルタント等が含まれる。さらに、内部・外部監査人との個別の会議と併せて委員会の常設エグゼクティブ会議もあるため、会議がぎっしり詰まって慌ただしく感じるのは当然である。

＜図表３＞１年間で正式な監査委員会が開催される回数

組織の種類	平均回数
金融セクター（株式非公開と株式公開）	6.7
株式公開（金融セクターを除く）	6.4
非営利組織	6.2
公共部門・政府機関（国、地方自治体、諸官庁、国有組織等）	5.9
その他の種類の組織	5.6
株式非公開（金融セクターを除く）	5.3

注：質問78「昨年度、（対面会議、電話会議、オンライン会議等を含む）正式な監査委員会会議は約何回開催されましたか？」CAEのみ回答。回答数＝1,894。

多くの金融機関は多数の議題に対応するために、委員会と委員会の間に会議を設けたり増やしたり、委員長とＣＡＥが電話会議を行ったり、会議を迅速に進められるように委員に会議事前資料を送付したりしている。会議資料の量は、追加説明を必要とするような複雑な議題のせいで、爆発的なものになっている。

ＣＡＥは、異なるレベルの詳細さを求める複数の参加者に宛てた監査報告書を書くのに苦労し続けている。例えば、

- 取締役は、ハイレベルの戦略的リスクに焦点を当てた報告書を必要としている。
- 経営幹部は、是正措置が特定できるような、より詳細な報告書を必要としている。

●業務部門の経営者は、システムやプロセスを見直して複雑な変更を適切に実施するために、極めて詳細な報告書を必要としている。

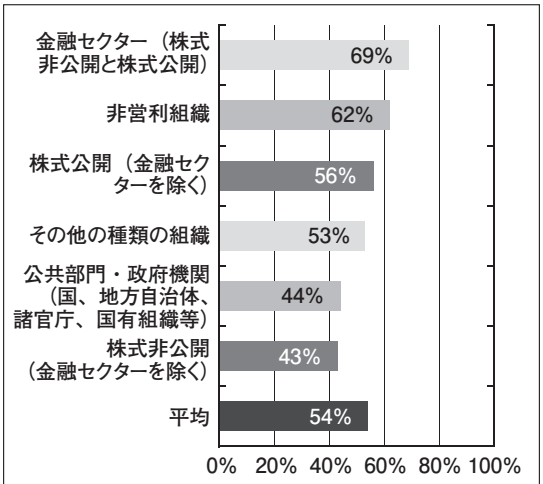
監査委員会とリスク委員会にとって、期待が高まる現在の環境下で有効性を発揮するのは非常に難しい。議題の広がりや討議時間の超過に備えて、予備の時間を割り当てておかなければならない。ＣＡＥにとって不可欠なのは、監査委員会を最も重要な議題に集中させることと、経営者や監査委員会にとって懸念となる問題に対処するようなリスクベースの監査計画を策定することである。簡潔でインパクトのある監査報告書があれば、経営者と監査委員会は効率的に時間を活用して会議中により有効な討議を進めることができる。

３．内部監査への期待の高まりに起因する課題

ＣＡＥの長年の念願は、独立性を高めるために組織内の高い地位に就き認められること、監査による改善提案に重要性が置かれること、経営幹部や取締役とより頻繁に交流すること、より生の情報を入手して戦略的施策へインプットを提供することである。多くのＣＡＥにとって「願い事は慎重に」という警告は現実的なものになっており、先に掲げた念願は機会と課題の両方をもたらしている。ＣＡＥは、考えられるほぼすべての問題の真っ只中に自らが置かれていると感じている。

経営者、取締役、規制当局、外部監査人からの期待によって、内部監査が達成すべき業績水準が引き上げられている。これら内部監査の利害関係者は、内部監査への期待について意見がぶつかり合うことが多く、矛盾する利害関係者に仕える内部監査を難しい立場に立たせている。金融機関の内部監査人は利害関係者の期待に応えるために、ガバナンス、戦略への関与、報告、経営者の決定事項への異議申し立てなどに関して『基準』を超えなければならないことが多い。また、金融サービスの監査人は他の業界の内部監査人に比べて、監査委員会に直接報告することが多い。調査回答者によると、金融サービスの内部監査人の69％は監査委員会に直接報告しているが、全業界平均はわずか54％である（図表４参照）。内部監査への期待の高まりによって内部監査の業務量と監査スケジュールは増えており、リソースの制約がより厳しくなっている。

＜図表４＞ＣＡＥが職務上監査委員会に報告している割合



注：質問74「あなたの組織の中で、内部監査部門長（CAE）または同等の職位の者の職務上の主な報告先はどこですか？」CAEのみ回答。回答数＝2,634。

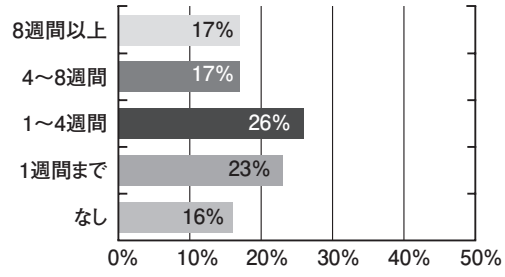
外部監査人の支援

従来、内部監査人は、外部監査人の補完や支援にかなりの時間を割くことが多かった。これは今でも続いているが、今や内部監査グループは、外部監査人のために費やしたのと同じかそれ以上のリソースを規制当局の検査官の補完と支援にも費やさなければならない。一部の例では、新たな会計規制当局が内部監査人の業務への依拠に制限を設けたために、外部監査人の業務と費用が追加されることになった。これにより、外部監査人と規制当局にも追加的費用を払わなければならなくなったので、内部監査に対するリソース配分

について経営者と取締役は疑問を投げかけている。調査回答者によると、他業種に比べて金融・保険業界は外部監査人の支援をより多く行っており、全く支援していないのはわずか16％である。さらに、金融サービスセクターは外部監査人の支援に最も時間を割いており、34％が４週間以上、17％が８週間以上を支援に費やしている（図表５参照）。

監査による改善提案の実施を確実にすることは、内部監査のフォローアッププログラムの形式としてより重視されている。フォローアップは、単に改善提案の実施状況を経営者に尋ねる以上のことをしなければならない。改善提案が適時に実施されたかを検証するためにテストを行うことがより重要になっているため、監査の労力が増えて限られたリソースにさらに負担がかかっている。調査回答者によると、他の業界では業務プロセスのオーナーがフォローアップの一義的責任を負っていることが多いが（金融サービスの19％に比べて全平均は25％）、金融サービスの内部監査人はフォローアップの責任を業務プロセスのオーナーと共有していることが多い（全平均50％に比べて金融サービスは54％）。（質問52、回答数＝3,216）。繰り返しになるが、金融サービスセクターの内部監査リソースは、このような追加的責任のせいでギリギリの状態である。

＜図表５＞１年間で内部監査部門が外部監査の支援に費やした期間



注：質問51「あなたの組織の内部監査部門は昨年、約何週間外部監査の支援に費やしましたか？」CAEのみ回答。金融セクターのみ抽出。回答数＝560。

内部監査人が経営者に異議を唱えることを規制当局が要請

内部監査の重要性に対する規制当局の期待が高まったことにより、金融検査の範囲は単にいくつかの監査報告書と監査調書を調べることから内部監査のあらゆる側面のより包括的な評価へと拡大している。一部の例では、規制当局は内部監査グループを彼らの延長線上に置こうとしているようであり、内部監査人が経営者に異議を唱える通常のまたは伝統的な解決プロセスを回避して取締役会に報告することや、問題を規制当局に直接報告することさえも求めている。内部監査人の多くは、自らの業務の結果が規制当局の検査報告書の中で追加の不備として引用されることを懸念している。オレゴン州ポートランドのユニタス地域信用組合最高リスク責任者のジェームス・アレクサンダー氏は、「監査報告書の意見に対する適切なフォローアップシステムがあれば、内部監査報告書の意見が金融検査の発見事項として引用される可能性を減らせる。」と考えている。従来の意見相違解決プロセスでは、通常、意見相違項目が取締役会や規制当局に報告される前にほとんどが解決された。規制当局は内部監査に高度の期待をしているため、意見の相違があった場合に内部監査人が経営者に「異議申し立て」することを期待しており、その状況が監査委員会や取締役会に上申された証拠を探し求めている。

内部監査への期待の高まりは内部監査にとって確実にプラスになるが、課題もある。内部監査人への期待および報告や責任が増加すれば、独立性、客観性、デューデリジェンス、あらゆる関係者とのコミュニケーションを適切に確保するための要件も増加する。

４．テクノロジーリスクの増加

テクノロジーは、組織が理解し、解釈し、評価し、機密データへのアクセスをコントロ

ールするよりも速く進歩している。テクノロジーを使えば、犯罪者は組織がアクセスを制限し保護するより速く脆弱性につけ込むことができる。今どきの銀行強盗は、銃の代わりにテクノロジーで武装して襲って来る。彼らは世界中のあらゆる場所で暗躍できる。彼らによる金融機関の機密データへの不正アクセスの企ては、１日24時間休むことなくコンピュータ上で行われている。その結果、金融セクターの内部監査人は、他業界に比べてはるかに広範囲にＩＴリスクに関する監査業務を行っている（図表６参照）。

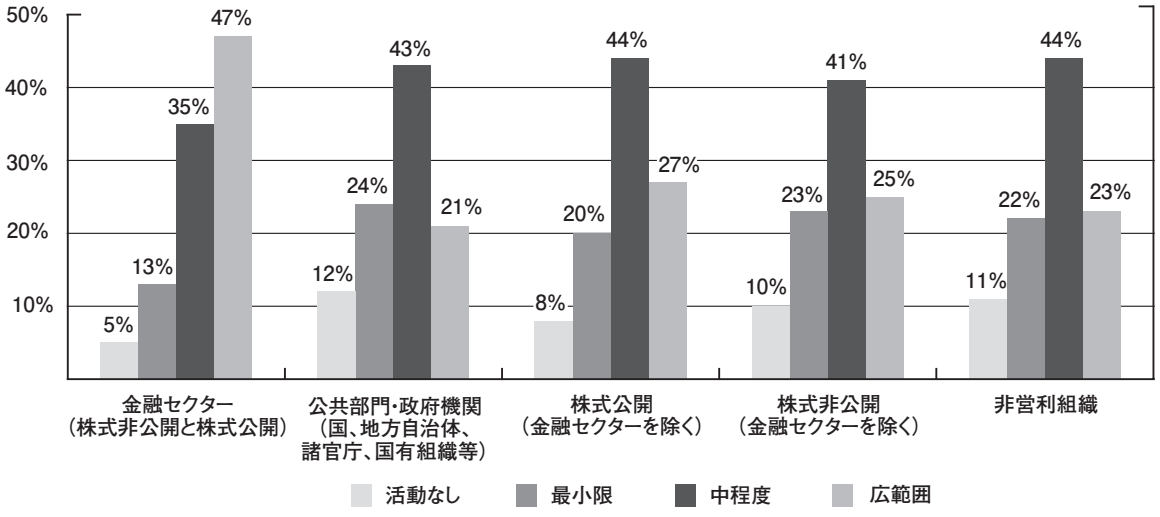
サイバーセキュリティリスクの大規模な影響

サイバーセキュリティ、ＡＰＴ攻撃[1]、プライバシー保護は、内部監査人のリスクレーダー内で最も注目されている話題の１つになっている。図表１と図表２が示す通り、情報技術（ＩＴ）リスクは、ＣＡＥが焦点を当てるリスク分野および監査計画で高い割合を占めるリスク分野のともに第４位である。また、これらの話題に注目しているのは内部監査人だけではなく、上級経営者、取締役会、規制当局、投資家も、これらのリスクに懸念を示している。データ侵害が大々的に公表されていることから、誰もがこれらの侵害がもたらす評判リスクと悪影響を十分承知している。復旧作業は膨大な時間と費用を要し、結果として大掛かりな組織的再編が起こり得る。「もし侵害されたら」ではなく「いつ侵害されるか」なので、侵害が起こる前に復旧計画を念入りに策定しテストすべきである、と多くの人々が言う。金融セクターの内部監査人（43％）は他のセクター（34％）に比べて、データ侵害のリスクをより広範囲であると考えている（図表７参照）。

準備と復旧活動

事業の継続、再開、復旧は、データ侵害の防御や制限の試みと同じかそれ以上に重要になってきている。より広範で総合的なデータとプライバシーの管理と、準備、発見と分析、封じ込め、撲滅から事後処理までの全領域をカバーするプログラムが必要である。内部監査人が積極的に準備計画に関与すれば、不可

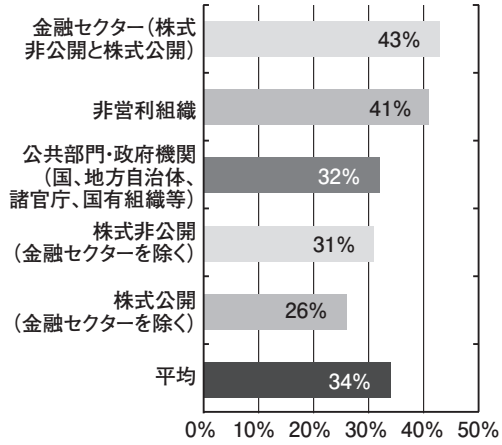
＜図表６＞ＩＴ全般リスクに関する内部監査業務



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「情報技術（IT）全般リスクの監査」。回答数＝9,747。

[1] 訳者注：ＡＰＴ（Advanced Persistent Threats）攻撃とは、インターネットにおいて特定のターゲットに対して継続的に攻撃・潜伏を行い、さまざまな方法で執拗にスパイ行為や妨害行為を行うサイバー攻撃の総称。

＜図表７＞データ侵害のリスクが「広範囲」と回答した割合



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？」のうち「組織のブランドを傷づけ得るデータ破壊」。回答数＝9,426。

避な事態が起こった時に大きな実を結ぶことができる。準備状況のテストは、内部のリソースとわずかなベンダーで行うところから、サイバー脅威と物理的脅威の情報分析と共有を目的とした金融サービス業界のリソースである『金融サービス情報共有センター（ＦＳ－ＩＳＡＣ）』のような組織を含めるところにまで発展している。

「内部監査のデータ分析能力と積極的な継続的モニタリング能力は向上中であり、これは能力開発計画を検討すべき分野の１つである。」

南アフリカ、ファーストランド社　ＣＡＥ
ジェニサ・ジョン氏

ビッグデータのリスクを監査計画に加える

莫大で増加の一途を辿るビッグデータをどのように保存、管理、保護、利用するかが組織にとって課題となっている。2013年に報告されたところによると、世界中のあらゆるデータの９割は、過去２年間で生成されているという（2013年５月22日付、サイエンス・デイリー電子版）。リスクデータの集約と情報ガバナンスは、内部監査人がリスクベースの監査計画を策定する際に考慮すべきテーマである。

つながりとモバイル機器

新たなテクノロジーは、組織と内部監査グループに独特の課題をもたらしている。アクセスコントロールは、もはやワークステーションのロックダウン[2]だけに限らない。インターネット、ソーシャルメディア、モバイル機器、リモートアクセス、その他の機器や方法は、コントロールすべきより多くの侵入ポイントを開いている。組織中のユーザーは、大抵、通常のコントロール手続を経ずに未承認のソフトウエアを導入できる。多くの金融機関が利用しているレガシーシステムと新たなテクノロジーを統合する場合、金融機関の情報のモニタリングと管理に追加的な課題が生じる可能性がある。

これらのテクノロジー上の課題は、金融セクターの内部監査部門に多くの難題を課している。変わり続けるテクノロジーリスクに対応するために内部の専門家を監査部門に配置するのは費用が掛かるし、また、この分野の専門家の数が限られていることから実現は難しい。情報システム監査の資格を保持しているのは世界中の調査回答者のわずか１割であり、ＩＴセキュリティの資格保持者はたったの３％である（質問13、回答数＝12,540）。テクノロジー監査にコンサルタントを用いるのも費用が掛かるし、追加的な監督と管理も必要になる。テクノロジーの変化の速度のせいで金融機関のテクノロジーリスクプロファイルは変化し続けるので、内部監査部門は動く標的を監査することが求められている。

[2] 訳者注：ロックダウンとは、システムの機能制限、リソース制御やアクセス制御など、特定の用途にだけシステムを使用できるようにすること。

５．３つのディフェンスライン

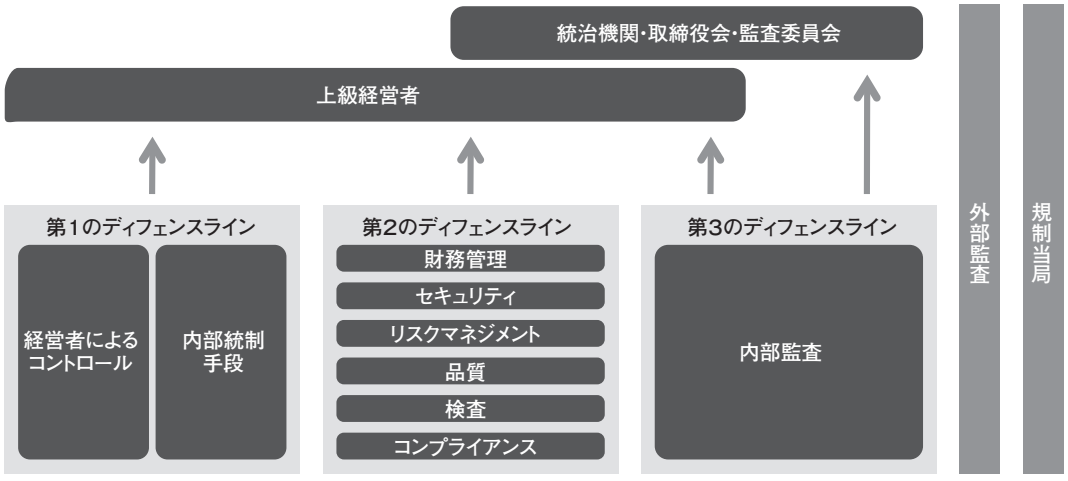
３つのディフェンスラインモデル（図表８参照）は好評で、世界中の内部監査人に広く利用されている。調査回答者によると、世界中の金融セクターの78％は「３つのディフェンスラインモデルに従っており内部監査は第３のディフェンスラインである」と回答している（図表９参照）。これは、他の種類の組織に比べてはるかに高い割合である。このモデルがより一般的になり、理解され、受け入れられる一方で、このモデルがどの程度柔軟であるべきかという疑問が起こっている。３つのすべてのディフェンスラインは、組織の規模や複雑性を問わず、何らかの形ですべての金融機関に存在すべきである。リスクマネジメントは通常、３つの別々で明確なディフェンスラインがある場合に最も強固である。しかし実際には、特に中小規模の金融機関では混合型アプローチが導入されている。例えば、第２のディフェンスラインの一部を内部監査と統合している金融機関がある。

内部監査人は、独立したコンプライアンス部門がない場合にはコンプライアンス監査の実施、独立したローンレビュー部門がない場合にはローンレビューの実施、全社的リスクマネジメント（ＥＲＭ）業務の調整、物理的セキュリティやＩＴセキュリティの担当を、要請されたりそれらの責任を割り当てられることがある。３つのディフェンスラインモデルを適切かつ有効に導入する方法を模索しているＣＡＥもいる。

混合型の３つのディフェンスラインの安全対策

内部監査は、客観性を保ち日常業務の管理者の不当な影響を受けずに業務を行うことが重要である。内部監査と第２のディフェンスラインの一部を含むすべての内部のアシュアランスグループが、部門運営上１人の経営幹部に報告する組織もあり得る。このような混合型の部門運営上の報告関係では、ＣＡＥが監査委員会に職務上直接報告することを妨げないように報告体制を設計すべきである。３つのディフェンスラインの異なる機能が部門運営上同一の経営幹部に報告する場合は、内部監査が職務上監査委員会に直接報告する体制を確保することが重要である。内部監査の独立性と客観性の維持に役立つ追加的な安全対策を講じることも可能である。安全対策には、内部監査の品質評価、第三者によるコンプライアンス、ローンレビュー、セキュリテ

＜図表８＞３つのディフェンスラインモデル



注：出典－IIAのポジションペーパー『有効なリスクマネジメントとコントロールにおける3つのディフェンスライン』（2013年1月）の中の『ECIIA/FERMA Guidance on the 8th EU Company Law Directive, article 41』。

ィ、ＥＲＭのレビュー、およびコンプライアンス、ローンレビュー、セキュリティ等の管理者に対する取締役会の委員会へのアクセス提供などがある。

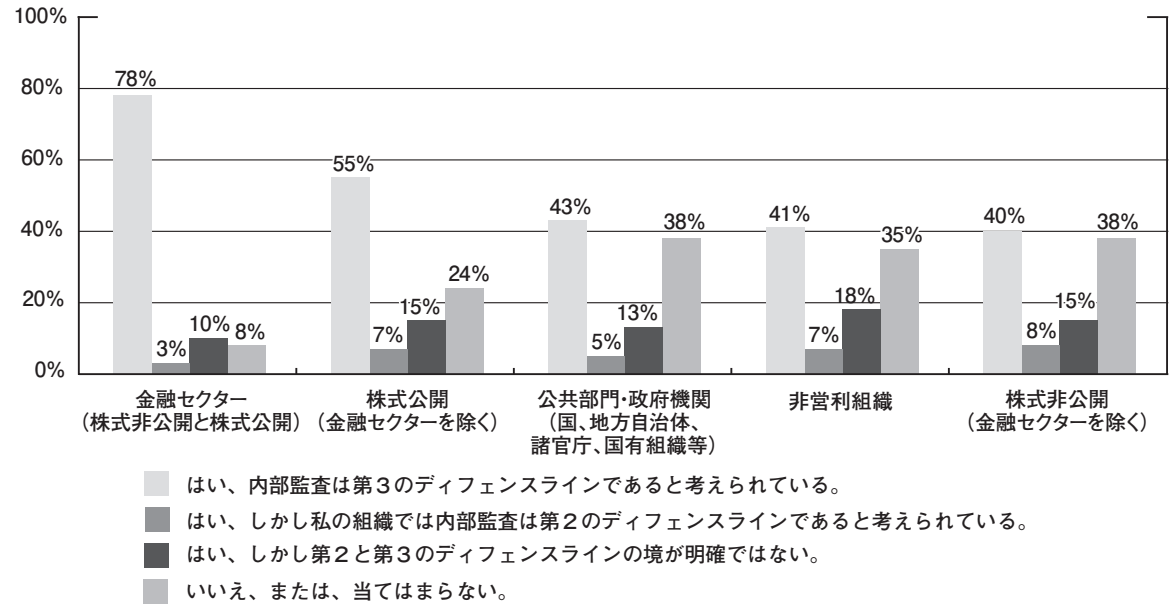
内部のアシュアランスグループが業務運営上または経営上の意思決定責任を負っておらず、内部監査の基本規程や報告書等で適切に開示され透明性が確保されていれば、３つのディフェンスラインモデルの下での混合型の部門運営上の報告関係において独立性と客観性を裏付けることができる。高度に規制された金融サービス業界では、このような混合型の報告関係および独立性と客観性を強化する安全対策の整備状況をレビューする当局検査を、この体制の適切性の検証に役立てることができる。

内部のアシュアランスグループが１人の経営幹部に直接報告する体制は、これらすべてのグループの独立性と客観性を強化する安全対策にもなり得る。このアプローチでは、複数のアシュアランスグループ内のコミュニケーションと連携を一層深めることができるので、情報の活用と重複業務の最小化を可能にし、結果的に効率性と有効性が増す。

ＩＩＡのポジションペーパー『有効なリスクマネジメントとコントロールにおける３つのディフェンスライン』は、「どの組織も固有であり置かれた状況もさまざまなため、３つのディフェンスラインを連携する唯一の『正しい』方法というものはない。」と述べている。さらに、「特に小規模組織のような例外的な状況では、あるディフェンスラインが兼務されることもある。このような状況では、内部監査は統治機関と上級経営者に対して、兼務の影響を明確に説明しなければならない。もし二重の責任が単一の個人または機能に課される場合には、３つのディフェンスラインを確立するために、後でこれらの職務の責任を分けることを検討することが適切である。」とも述べている。

ＣＡＥは、各組織のリスクとコントロールを有効に管理するために、情報が共有され業務が連携されることを確実にすべきである。正式な方針と手続を策定すれば、この取り組みを促進できる。

＜図表９＞３つのディフェンスラインの利用割合



注：質問63「あなたの組織は、IIAが明示した３つのディフェンスライン（３本の防衛線）モデルに従っていますか？」のうち「このモデルを良く知らない」と回答した者を除く。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＝9,093。

６．内部監査のリソース

内部監査に対する経営者、取締役、規制当局の期待は、すべての内部監査人の伝統的特徴であった典型的な会計と財務の知識の枠を超えて拡大している。今や内部監査人は、テクノロジー、事業運営、金融サービス、コミュニケーション、法規制の遵守、サイバーセキュリティ、プライバシー、ベンダー管理、事業継続、法的事項、定量分析などに関連する知識を持つことが期待されている。これらのスキルを獲得するために単により多くの人々を採用し続けるのは、ほとんどの組織にとって不可能である。調査に回答したＣＡＥによると、金融サービス業界は他の業界と比べて異なるスキルの優先順位があり、業界特有の知識、ファイナンス、リスクマネジメント、ＩＴをより重視している（図表10参照）。興味深いことに、会計スキルはあまり重視されていない。多才な監査人がさまざまな分野の監査を行えるように、個々の監査人のスキルセットを伸ばさなければならない。

これらの新しいスキルを身につけた内部監査人を育成することに課題がないわけではない。例えば、ＩＩＡの2015年監査管理者大会（General Audit Management Conference）での報告によると、北米の監査人と会計士の失業者数は史上最低であり、また、会計を専攻する学生はより少なくなっている。ＣＡＥは、伝統的な会計以外の学歴にも幅を広げて求人の検討をしている。

世代的な相違は労働環境を再形成し、従来からの報酬制度や管理手法に課題をもたらしている。若い世代は福利厚生を検討する際に、仕事と生活のバランスをより重視している。融通の利く仕事のスケジュールや多くの休暇が、より一般的になってきている。幸いにも、テクノロジーのおかげで監査スタッフは自宅で働ける機会が増えている。

テクノロジースキルは、就労するあらゆる監査人にとって今や必須条件である。テクノロジーは、組織が内部のリソースを補完するために外部や第三者のリソースを必要とすることが多い分野でもある。内部監査リソースを補完するためには、新たなシステムやソフトウエアツールも必要かもしれない。幅広いテクノロジー監査を効果的に行うためには、

＜図表10＞金融セクターのCAEがスタッフに求めるスキルの上位

スキル	金融セクター	非金融セクター	差
分析的・批判的思考	66%	64%	2%
コミュニケーションスキル	52%	51%	1%
リスクマネジメントアシュアランス	48%	41%	7%
業界特有の知識	45%	33%	12%
情報技術（一般）	43%	37%	6%
会計	36%	45%	-9%
データマイニングと分析	32%	31%	1%
ファイナンス	30%	21%	9%
ビジネス感覚	26%	27%	-1%
不正監査	21%	23%	-2%
サイバーセキュリティとプライバシー	16%	13%	3%
フォレンジックと調査	13%	15%	-2%
法務知識	10%	12%	-2%
品質管理（シックスシグマ、国際標準化機構）	4%	8%	-4%
その他	3%	4%	-1%

注：質問30「あなたの内部監査部門で最も採用または開発しているスキルは何ですか？（５つまで選んでください。）」CAEのみ回答。回答数＝3,288。

「金融サービスの監査機能のニーズが財務リスクから業務（オペレーショナル）リスクに変化していることを踏まえて、当社が採用する人材の経歴も変化している。当社が現在求めているのは、ファイナンス、組織的戦略、統計、サプライチェーンマネジメントなどを大学で専攻した人々である。」

テキサス州サンアントニオ、ＵＳＡＡシニアヴァイスプレジデント、ＣＡＥ
マーク・ハワード氏

予算と研修の増加が必要となるだろう。

内部監査部門長を一定期間務めるローテーション制のＣＡＥは、監査手法を拡大する一方で、監査手法の継続性や独立性の問題をもたらしている。また、ローテーション制のＣＡＥがＩＩＡの『基準』や品質評価などを理解しているのか、あるいは注意を払っているのかといった問題もある。内部監査の研修や資格に対するコミットメントも不足している可能性がある。組織的な人材育成は、ローテーション制のＣＡＥにとって、有利な転出や業務ユニットへの復帰のタイミングと機会に影響を及ぼす可能性がある。しかし、ＣＡＥのローテーション制は、多くの利点ももたらし得る。例えばローテーション制のＣＡＥは、既に実証され認められているリーダーシップ、ビジネスに対するより幅広い見識、既に構築されたビジネス部門との関係などを持っているので、それらを内部監査機能の価値の付加と自信の増加に活用することができる。

結論

金融サービス業界の内部監査人には、常に課題がある。課題は、長年にわたり似たようなテーマであり共通の種類にまとめることができるが、対処する者の創造性を試すような異例の課題も常にある。環境は変化し続け、課題に対処するための革新的な戦略を策定する新たな機会をもたらしている。

直面する課題に効果的に対処し進歩する内部監査人は、組織に積極的な貢献を示すことができる。彼らは有能なリーダーとして認められ、ひいては職場で地位と評価を高め続ける。このような評価に連動して組織内での彼らの役割は重要性を増し続けるため、さらなる難題を背負う可能性がある。最も成功する内部監査人は、過去の経験から学び、さらに革新的手法と実践、プロ意識、継続的能力開発、内部監査の専門職への献身を通して、改善のための努力を続けるだろう。

著者について

ジェニファー・Ｆ．バーク氏は、公認会計士、Certified Risk Professional、Certified in Financial Forensics、Certified Fraud Specialistの資格を有し、クロウ・ホーワス社の金融サービス・リスク・プラクティスのパートナーであり、クロウ社での19年間を含めて25年以上金融サービス業界の顧客にサービスを提供している。数十億ドル規模の金融機関の戦略的プロジェクトを主導し、内部監査、コンプライアンス、ローンレビュー、全社的リスクマネジメント（ＥＲＭ）を行っている。また、ＩＩＡの金融サービスアドバイサリーボードとノースカロライナ州ＥＲＭイニシアティヴ・アドバイザリーボードで委員を務めている。彼女は、銀行、内部監査、ＥＲＭなどのテーマの講演者として米国内および国際的に著名である。クロウ社に勤務する前は、数十億ドル規模の金融機関のシニアヴァイスプレジデントでありＣＡＥを務めていた。

スティーブン・Ｅ．ジェームソン氏は、公認内部監査人、公認金融監査人、公認リスク管理監査人、公認会計士、公認不正検査士の資格を有し、コミュニティ信託銀行で内部監査、ＥＲＭ、ローンレビュー、コンプライアンス、セキュリティの機能を担当するエグゼクティブヴァイスプレジデントであり最高内部監査兼リスク管理責任者である。金融サービス業界の内部監査の専門家として28年以上、会計事務所で３年、ＩＩＡの専門職的実施グループのヴァイスプレジデントとして４年以上の経験がある。彼は、ドレッドウエイ委員会支援組織委員会（ＣＯＳＯ）の2013年版『内部統制の統合的フレームワーク』および2004年の『全社的リスクマネジメント』の諮問委員会委員を務めた。

ＣＢＯＫプロジェクトチーム

ＣＢＯＫを運営しているＩＩＡ調査研究財団（ＩＩＡＲＦ）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。ＩＩＡＲＦは、現在の課題、新たな傾向、将来のニーズを検討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。

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

ジェームス・アレクサンダー（U.S.A.）
デスポイナ・チャザガ（ギリシャ）
キヴィルシム・グンバティ（トルコ）
キャシアン・ジェイ（U.S.A.）
ジェニサ・ジョン（南アフリカ）
マイケル・パーキンソン（オーストラリア）
デボラ・ポーラリオン（U.S.A.）
ニコラ・リマー（英国）