コンプライアンス態勢の高度化と内部監査

PwCあらた有限責任監査法人
ガバナンス・リスク・コンプライアンス・アドバイザリー部
パートナー　**竹内 秀輝**

はじめに

近年、企業を取り巻く環境が複雑化し、その変化もめまぐるしくなっています。これらの環境変化を背景に、従来は「法令遵守」と捉えられていたコンプライアンスの概念が拡大しています。また、コンプライアンス事案が発生した場合には行政処分に至らない場合であっても、報道等により企業ブランドが毀損するケースも少なからずあります。一方で、経営資源は有限であるため、コンプライアンス態勢の整備・運用に資源を無尽蔵に投入することは現実的ではありません。このため、いかにコンプライアンス態勢の整備・運用を効果的・効率的に行うかが重要な経営課題の1つとなっています。

本稿では、コンプライアンスの概念がどのように拡大しているかについて解説した後、コンプライアンス態勢の整備・運用を行う上でのポイントに触れます。その上で、このような状況下における内部監査に求められる役割を説明します。

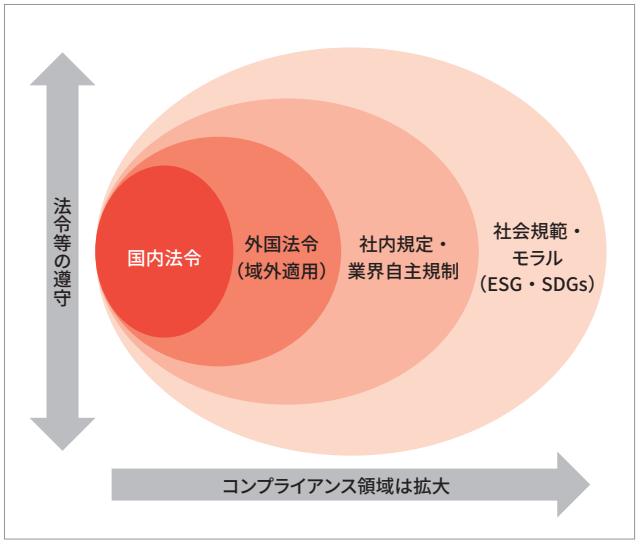
なお、文中の意見に係る記載は筆者の私見であり、PwCあらた有限責任監査法人および所属部門の正式見解ではないことをお断りします。

1 拡大するコンプライアンス領域

はじめに、「Compliance（コンプライアンス）」という言葉の意味を確認しておきましょう。「コンプライアンス」とは「法令遵守」と考えている方も多いかもしれませんが、英語辞書では「法令遵守」という訳を見つけることはできません。一般的には、「withを伴い『～を遵守する』」という語義が挙がっています。つまり、「with」の後に「laws and ordinances（法令）」以外の単語を加えてもよいことから、コンプライアンスという言葉は法令遵守よりも広い意味を持っていると考えることができます。

次に、コンプライアンスの範囲について考えてみます。**図表1**に示すとおり、今日のコンプライアンスは、国内法令はもとより、米国の海外腐敗行為防止法（Foreign Corrupt Practices Act：FCPA）に代表される法域をまたいで適用される域外法令、業界自主規制、さらには「社会規範・モラル」

図表1：拡大するコンプライアンス領域



出所：PwC作成

を含んでいると考えられています。近年、「ESG・SDGs」に社会的な関心が集まっていますが、「持続可能な社会の実現を目指すべき」という社会規範を企業が遵守するのであれば、「ESG・SDGs」もコンプライアンスの範疇に収まると考えることもできます。

コンダクトリスクとは

数年前から、日本を含む各国の金融監督当局はコンダクトリスク管理を金融機関に求めています。コンダクトリスクに関するグローバル共通の定義を金融監督当局は示していませんが、あえて定義すれば、「企業の行動が法令に遵守していても、社会の価値観と相容れないことから生じるリスク」となります。

ここで留意しなければならないのは、「相容れないかどうかを判断する」のは社会・市場・顧客といった企業を取り巻くステークホルダーであり、企業ではありません。上述の「ESG・SDGs」も日本では法令として明確には定められていません。このため、「ESG・SDGs」を念頭に置かない経営を行ったとしても直ちに法令違反に問われることはありませんが、「持続可能な社会の実現を目指すべき」という社会規範と相反する行動をとったと社会がみなした場合には、糾弾・非難を受ける可能性もあります。

社会の価値観が急速に変化することと相まって、企業に求められるコンプライアンスを一層複雑化させています。

2 企業に求められる対応

(1) リスクベースでのコンプライアンス態勢の整備・運用

拡大するコンプライアンス領域に対して企業はどのように対応していくべきでしょうか。経営資源は有限であることから、リスクベースでコンプライアンス態勢の整備・運用を企業が行う必要があります。つまり、自社（あるいは自グループ）にとって、リスクが高いと評価したコンプライアンス領域を特定し、そこに経営資源を重点的に投下して態勢を整備・運用し、事案の発生低減を図ります。逆に、リスクが低いと評価した領域については、相応の態勢を整備・運用すれば足りることになります。

ここで、リスクが低い領域であってもコンプライアンスは当然に求められることを忘れてはいけません。繰り返しになりますが、リスクが低い領域については、相応の態勢を整備・運用することも許容され得る、ということを述べている点にご留意ください。

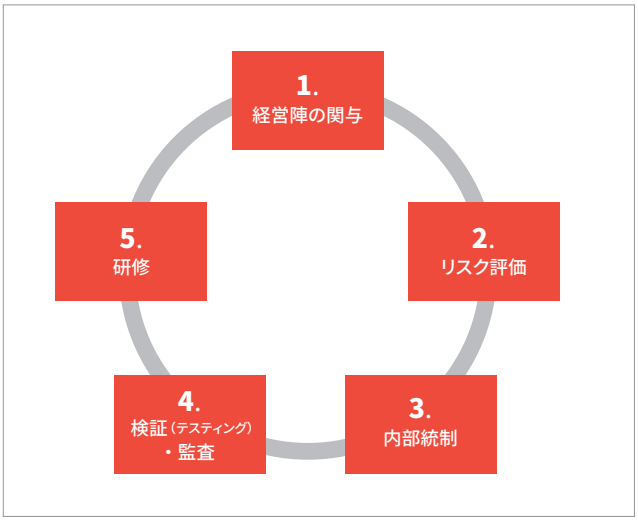
(2) コンプライアンス態勢の構成要素

前述の「コンプライアンス態勢」を組織が「コンプライアンスを実現する仕組み」と定義した場合、どのような仕組みを考えなければならないのでしょうか。この点に関しては、米国財務省の外国資産管理局（Office of Foreign Assets Control：OFAC）の公表文書※1が参考となります。OFACは違反企業に対する処分を下す際、**図表2**に示す5つの要素に着目することを明らかにしており、逆に考えれば、これらの要素はコンプライアンスを実現する仕組みと考えることもできます。

以下、各構成要素の要点を解説します。

1. **経営陣の関与**：コンプライアンス事案に対する毅然とした態度を示すこと等を通じたコンプライアンスに関するカルチャー醸成と、コンプライアンス態勢の整備・運用に向けた経営資源の確保と配分を行う。
2. **リスク評価**：コンプライアンス領域に関するリスクの特定と評価の実施。評価結果に対する経営陣の承認に加え、定期的に見直しを行う。
3. **内部統制**：リスク評価結果に基づく、リスク低減策として

図表2：コンプライアンス態勢に求められる構成要素



出所：PwC作成

※1 OFAC「A Framework for OFAC Compliance Commitments」2019年5月
https://home.treasury.gov/news/press-releases/sm680

の内部統制の整備・運用を行う。

4. **検証（テスティング）・監査**：内部統制はリスクベースで整備・運用するため、整備・運用する内部統制が有効であることを事後的に検証・監査する必要がある。このため、内部統制の整備・運用を担う担当者から独立した立場の担当者がその有効性を定期的に検証・監査し、リスク評価結果を事後的に確認する仕組みが必要となる。
5. **研修**：法令等の理解、カルチャー醸成あるいは内部統制の一環として整備された規程・手順書等の周知等を目的に、研修対象（例：経営陣、新入職員）を意識した研修を企画・実施する。あわせて、未受講者等に対するフォローを実施する。

（3）コンプライアンス態勢の説明責任

コンプライアンス態勢が十分であることの説明責任はガバナンス機関と当該機関から委任を受けた経営陣が一義的に負っていると考えるのが自然です。これは、ガバナンス機関の監視の下、経営陣の裁量（リスクベース）でコンプライアンス態勢の整備・運用が行われているからです。

つまり、「コンプライアンス態勢をどの水準で整備・運用したらよいか？」という問いに対する一律の回答はありません。さながら、「……のようなリスク評価の結果に基づき、……の整備を行うことが妥当と判断し、当該内部統制を設計し、運用してきました」といった記述式の試験問題に回答することが経営陣等に求められます。

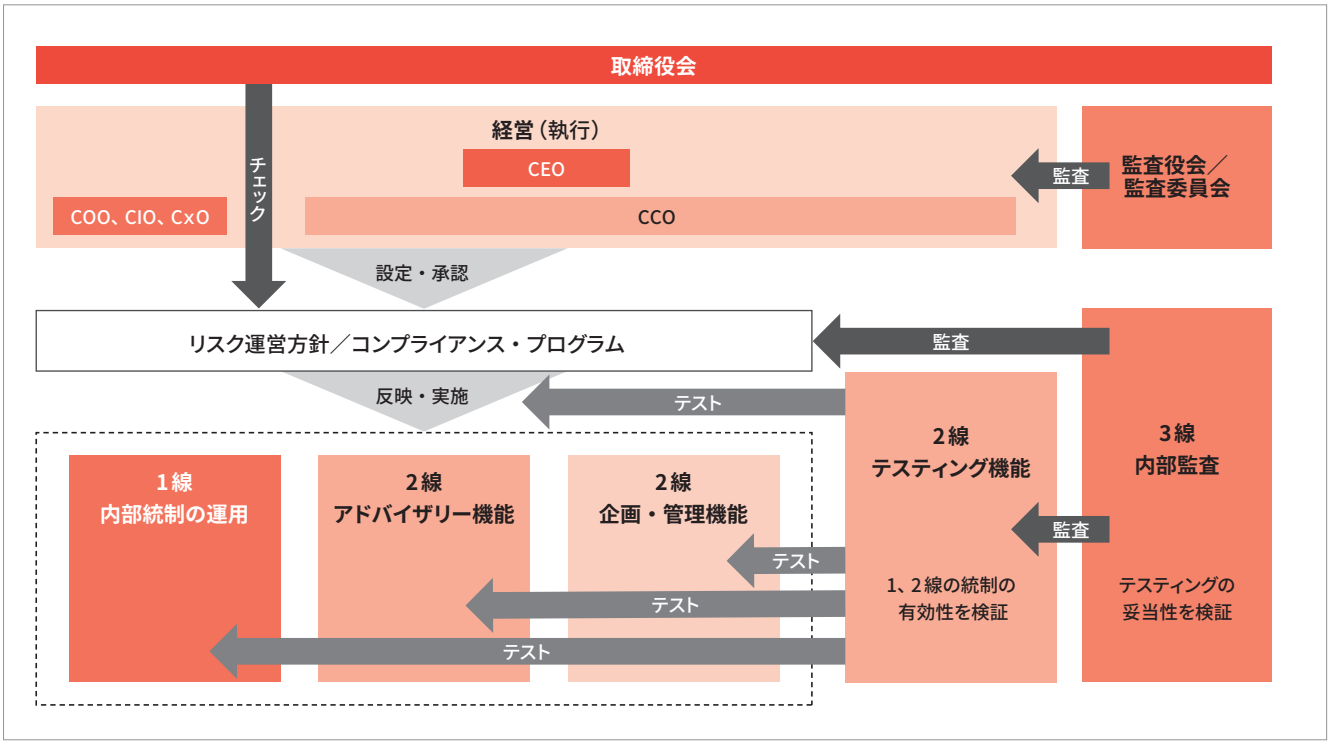
3 内部監査に求められる役割

ここでは、「3つのラインモデル（Three Lines Model）」[※2]における2線の役割変化を解説した上で、3線である内部監査に求められる役割について説明します。

（1）3線モデルにおける2線の役割変化

従来、2線は1線である業務執行部門から独立した立場で業務執行部門の監視を行うことが役割と言われてきました。しかし 1 で述べたように、コンプライアンス領域が拡大したこと、新技術の採用、新規事業への参入といった要因により、

図表3：2線であるコンプライアンス部門の役割



出所：PwC作成

※2 IIA「IIAの3ラインモデル：3つのディフェンスラインの改訂」2020年7月
https://www.iiajapan.com/leg/pdf/data/iia/2020.07_1_Three-Lines-Model-Updated-Japanese.pdf

コンプライアンス態勢の整備・運用はコンプライアンスを含むリスクオーナーである第1線の業務執行部門が担うべきと考えられています[※3]。なお、リスクオーナーである1線の業務執行部門がコンプライアンス管理の責任を負うことが明確にされただけで、独立の立場としての2線の監視機能は残ります。

その結果、2線であるコンプライアンス部門のアドバイザリー機能とテスティング機能に重点が置かれるようになりました。アドバイザリー機能とは、コンプライアンスは組織全体で実現することが求められる以上、コンプライアンスの専門家としての立場から1線である業務執行部門に対して助言を行うことを言います。また、テスティング機能とは、前述のとおり、整備・運用したリスク低減策（内部統制）の有効性をコンプライアンスの専門家の立場から定期的に検証することを言います。

一方、2線であるコンプライアンス部門が担う役割が多様化し、利益相反が生じかねない状況となりました。このため、**図表3**のように、2線の役割を細分化している企業もあります。

(2) 3線に求められる役割

コンプライアンス態勢が実現した際には、3線である内部監査はさらに経営目線で監査を行うことが求められるようになります。すなわち、2線のアドバイザリー機能とテスティング機能も含むコンプライアンス態勢を俯瞰した内部監査が期待されます。具体的には、内部統制が整備されたとおりに運用されているかといった準拠性の監査に加え、下記の観点で内部監査を行うことが求められるようになります。

1. 経営陣の発信しているコンプライアンスに関するメッセージと、発生したコンプライアンス事案に対峙する姿勢に整合性はあるか（もし、不整合であるとの心証を得ている場合には、経営陣ではなく、取締役・監査役等のガバナンス機関に直接報告する必要がある）
2. リスクの高いコンプライアンス領域を特定する方法は妥当か、また定期的な見直しを行っているか
3. 整備した内部統制は、コンプライアンス領域のリスク低減策として適切に設計されているか（設計したリスク低減策がリスクを適切に低減するために機能しているか、実現できる効果と投入する経営資源がバランスを欠いたものになっていないか）
4. 内部統制を周知する研修は有効に機能しているか（欠席者へのフォローアップはなされているか、受講対象者を念頭に置いた内容となっているか）
5. 2線が実施したテスティング結果は適切にフォローがなされ、フォロー結果も確認がされているか

上記の視点で内部監査を行うには、監査対象となっているコンプライアンス領域に関する知見に加え、IT分野での知識も必要となります。例えば、内部統制に機械学習を利用している場合、機械学習導入時の検討、さらにはインプットデータの品質についても監査対象になり得るかもしれません。この他、設計された内部統制が高度な判断を必要とせず、かつ反復継続的に行われるものであれば、RPA（Robotic Process Automation）あるいは外部委託の検討を提言することも考えられます。

4 おわりに

本稿では、コンプライアンス領域の拡大に伴い、コンプライアンス態勢の整備・運用の高度化のポイントや、内部監査に求められる役割の変化について解説しました。今回は紙幅の都合でリスクの高いコンプライアンス領域の特定方法については説明を割愛しましたが、機会があれば稿を改めて解説したいと思います。

本稿が、コンプライアンス態勢高度化の必要性を感じているコンプライアンス部門あるいは内部監査部門等が検討を進める上での一助になれば幸いです。

※3 リスクオーナーは、必要なリスク低減策（内部統制）を講じた上で、残存するリスクが許容できるか否かを判断する立場にあるため、必要なリスク低減策（内部統制）の整備・運用もリスクオーナーの役割と考えることができます。

竹内 秀輝（たけうち ひでき）
PwCあらた有限責任監査法人
ガバナンス・リスク・コンプライアンス・アドバイザリー部　パートナー
1999年に中央監査法人に入所。中央青山監査法人、あらた監査法人、 PwCあらた有限責任監査法人（以下、PwCあらた）にて保険会社に対する監査業務および各種アドバイザリー業務を幅広く経験した後、2011年から2014年にかけて、金融庁監督局保険課および総務企画局（現・総合政策局）総務課国際室で勤務。金融庁在籍期間中は、保険監督者国際機構（IAIS）のメンバーとして国際保険規制に関する検討に携わった他、国内外の監督カレッジへの参画を通じたクロスボーダーでの監督にも従事。PwCあらたに復職後、規制およびコンプライアンス関連のアドバイザリー業務に従事。現在、金融機関などに対し、FATF（金融活動作業部会）をはじめとする国際的な要請や国内関連法規制などを踏まえたAML/CFT（マネーロンダリングおよびテロ資金供与対策）態勢強化に関する支援を提供している。