実務指針 6.2 リスク･マネジメント

［根拠とする内部監査基準］

第 6 章　内部監査の対象範囲

第 2 節　リスク・マネジメント

6.2.1 内部監査部門は、組織体のリスク・マネジメントの妥当性および有効性を評価し、その改善に貢献しなければならない。

(1) 内部監査部門は、以下の視点から、組織体のガバナンス・プロセス、業務の実施および情報システムに関するリスク・エクスポージャーを評価しなければならない。

① 組織体の全般的または部門目標の達成状況

② 財務および業務に関する情報の信頼性とインテグリティ

③ 業務の有効性と効率性

④ 資産の保全

⑤ 法令、方針、定められた手続および契約の遵守

(2) 内部監査部門は、組織体のリスクの受容水準に沿った適切な対応が選択されているかを評価しなければならない。

(3) 内部監査部門は、識別されたリスクの情報が適時に組織体の必要と認められる箇所に伝達されているかを評価しなければならない。

(4) 内部監査部門は、組織体が不正リスクをいかに識別し、適切に対応しているかを評価しなければならない。

(5) 内部監査人は、アドバイザリー業務の遂行過程において、業務執行部門の個々の業務における目標と密接に結び付いたリスクに対応するとともに、その他の重要なリスクの存在についても注意を払わなければならない。

(6) 内部監査人は、アドバイザリー業務を通じて得られたリスクに係る知見を、組織体のリスク・マネジメントに対する評価プロセスに組み入れなければならない。

(7) 内部監査部門がリスク・マネジメントの確立や改善について経営管理者を支援する場合には、内部監査部門は、経営管理者のリスク・マネジメントに係るいかなる責任も負ってはならない。

［キーワード］

リスク・マネジメント・プロセスに係る役割分担とそのプロセスの評価

［目的］

本実務指針の目的は、内部監査部門による組織体のリスク・マネジメントの妥当性および有効性の評価に関して、以下の点を明らかにすることにある。

① リスク・マネジメント・プロセスに係る役割分担

② リスク・マネジメント・プロセスの整備状況の評価

③ リスク・マネジメント・プロセスの運用状況の評価

④ 不正リスクのマネジメントの評価

⑤ 改善のための提言のあり方

［指針］

1. リスク・マネジメント・プロセスに係る役割分担

組織体のリスク・マネジメント・プロセスにおける内部監査部門の役割は組織体によって異なるが、内部監査部門長は、それについて最高経営者および取締役会との間で合意しなければならない。ただし、内部監査部門は、経営管理者のリスク・マネジメントに係るいかなる責任も負ってはならない。

なお、内部監査部門がリスク・マネジメント・プロセスの妥当性および有効性に係るアシュアランスの提供を超え、当該プロセスに積極的かつ継続的に参加する場合等にあっては、その独立性および客観性が維持されるよう、以下の条件を満たさなければならない。

- 経営管理者がリスク・マネジメントに対する責任を負い続けること、および内部監査部門は経営管理者に代わっていかなるリスクも管理しないことについて、明確にされていること。
- 内部監査部門の役割は、リスク・マネジメントに関する意思決定を行うのではなく、最高経営者ないし経営管理者の意思決定に対する助言、異議申立および支援の提供にとどめること。

2. リスク・マネジメント・プロセスの整備状況の評価

組織体のリスク・マネジメント・プロセスは、組織体の事業活動の規模および複雑さによって異なり（**注１**）、その文化やマネジメント・スタイル、事業の目的等に基づいて整備されるが、内部監査部門は、その整備内容が組織体の活動に比して十分に包括的かつ適切なものであるかを評価し、改善のための提言を行う（ただし、提言のあり方については「5.改善のための提言のあり方」を参照）。

なお、組織体が正式なリスク・マネジメント・プロセスを有していない場合には、内部監査部門長は、その必要性について最高経営者および取締役会と話し合わなければならない。

3. リスク・マネジメント・プロセスの運用状況の評価

内部監査部門は、リスク・マネジメント・プロセス（**注２**）にしたがい、以下の視点から、その妥当性および有効性を評価し、改善のための提言を行う（ただし、提言のあり方については「5.改善のための提言のあり方」を参照）。

（1）事象の識別

- 組織体の目標の達成に影響を与える事象が、マイナスの影響を与える「リスク」とプラスの影響を与える（またはマイナスの影響を打ち消す）「機会」（**注３**）とに的確に識別されているか。
- 識別されたリスクの情報が、最高経営者および組織体内の適切な部署に適時に伝達されているか。

（2）リスクの分析・評価

- リスクをどのように管理するかを判断する基礎として、それぞれのリスクが分析・評価されているか（リスクの分析・評価のイメージについて、（**注４**）参照）。

（3）リスクの管理

- リスクを受容可能な水準にまで低減するための管理方針が決定されているか。すなわち、それぞれのリスクについて、回避、低減、共有、受容のいずれかの対応策を的確に選択しているか（**＜図表** 6.2.①＞）。

＜図表 6.2.① リスク対応＞

リスク対応	定義
回避	リスクをもたらす行動を止めること。
低減	リスクの発生可能性または影響の大きさを低減する行動をとること。
共有	リスクの一部を移転または共有することによって、リスクの発生可能性または影響の大きさを低減する行動をとること。
受容	リスクの発生可能性または影響の大きさを低減する行動を一切とらない（すべてを受け容れる）こと。

（4）リスクのコントロール

・当事者によってとられる具体的な行動によって、組織体のリスクが受容可能な水準にまで低減され、組織体の目標やゴールが効率的かつ経済的に達成されようとしているか（内部監査基準 6.3.1 参照）。

（5）定期的なリスク評価および環境変化への対応

・組織体において、少なくとも年に１回は、リスクの識別からリスクのコントロールまでの一連のプロセスが実施され、関連するコントロールの運用状況が最高経営者および取締役会に報告されているか。

・組織体の内外の環境（経済、産業、規制、または組織もしくは業務の運用状況等）に著しい変化が生じた場合には、適時かつ適切にリスク・マネジメント・プロセスが見直されているか。

4. 不正リスクのマネジメントの評価

内部監査部門は、潜在的な不正および違法行為の発生可能性を識別、評価するプロセス、ならびに不正および違法行為に関するコントロールの整備状況および運用状況を評価しなければならない。

なお、内部監査部門は、内部監査の実施を通じ、不正の兆候（例えば、標準化されたマニュアルの欠如や職務の分離が不十分な状態、記録されていない取引、記録の紛失など）を把握した場合には、その内容をリスク・マネジメント・プロセスにフィードバックしなければならない。

5. 改善のための提言のあり方

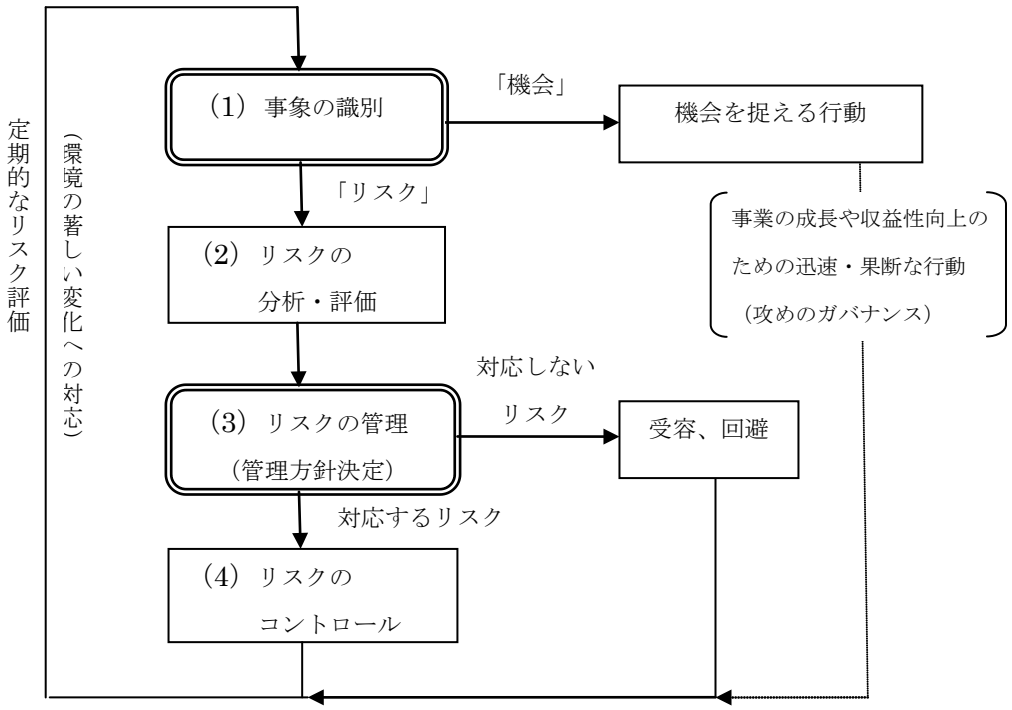
内部監査部門は、リスク・マネジメント・プロセスの評価を通じて把握されたコントロール上の課題に係る本質的な問題の解消を図る改善策について、最高経営者および組織体内の適切な部署に提言を行うことが望ましい。

この場合、内部監査部門は、そのような改善（関連するルールの改善など）に関与し過ぎることで、該当するコントロールの整備および運用に係る責任を負うようなことがあってはならない。

（注１） リスク・マネジメント・プロセスが専門の委員会（「リスク・マネジメント委員会」や「内部統制委員会」など）や専門の部門（「リスク管理部門」など）を中心に実行される場合がある一方、その他の委員会や部門等でリスク・プロファイルを議論し、必要なアクションを起こす場合があるかもしれない。

（注２）　リスク・マネジメント・プロセスのイメージについては、次のとおりである。

＜図表 6.2.②リスク・マネジメント・プロセスのイメージ＞



（注３）　識別した事象を「機会」と捉える行動とする例としては、次のようなものが挙げられる。

・計画外の大型案件の受注で要員不足が懸念されたが、組織をまたがる人員の最適配置のほか採用計画の見直しを通じ、契約通りに納品し得た。

・新製品の評判がＳＮＳや口コミで広がり、生産が追い付かない事態が懸念されたが、生産プロセスの効率化などによって拡大する需要に対応し得た。

（注４）　リスクの分析・評価の例（イメージ）については、次のとおりである。

＜図表 6.2.③＞リスクの分析・評価の例（イメージ）

注）図表中の各項目はあくまでも表示例であり、実際とは異なる。

※網掛け部分は、高リスクと考えられる範囲を表す。