2018 年 6 月 5 日

コンサルティングレポート

中堅中小企業　組織的経営シリーズ

内部統制システムの構築②　～不祥事・事故を起こさないために(1)～

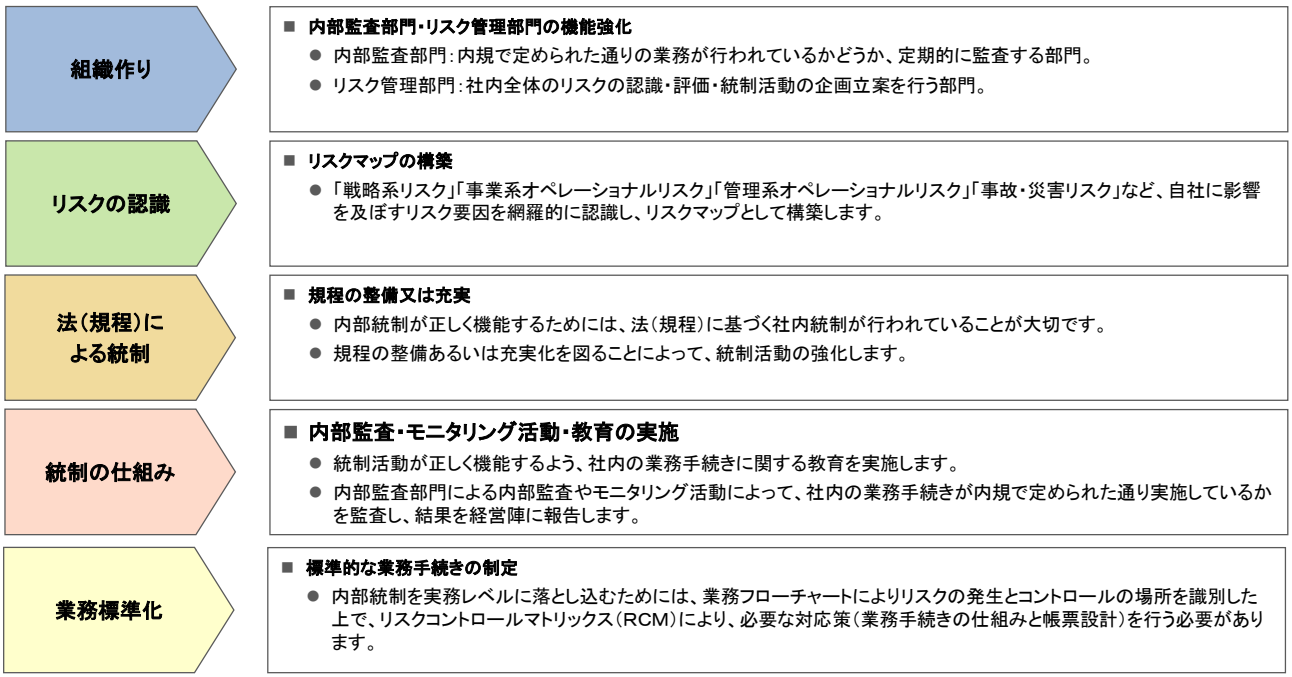
経営コンサルティング部〔大阪〕　部長　細川　達也

1.　不祥事・事故を起こさないための取り組み(フレームワーク)

前稿では不祥事や事故が発生する企業の特徴について考えてきました。ではどうすればこういった企業の不祥事や事故を防止あるいは軽減することができるのでしょうか？　本稿と次稿では不祥事や事故を起こさない企業になるための取り組みについて解説して参ります。

図1は、企業が不祥事・事故を起こさないための取り組みについてまとめたものです。リスクに強い企業を育てるためには「何か一つだけ取り組みをすれば良い」というものではなく、複数の取り組みを継続的に行う必要があります。具体的には「組織作り」「リスクの認識」「法(規程)による統制」「統制の仕組み」「業務の標準化」の 5 つです。これらの取り組みが相互にかつ有効に機能することによって組織をリスクに強い企業に変えていくことができます。利益は短ければ数ヵ月の期間で生み出すことができますが、企業体質を変え内部統制システムを構築するためには数年、具体的には 3～5 年程度の期間が必要と考えられ、腰を据えた取り組みが必要になります。

図 1　不祥事・事故を起こさないための取り組み(フレームワーク)



(お問い合わせ)コーポレート・コミュニケーション室　TEL：03-6733-1005　E-mail：info@murc.jp

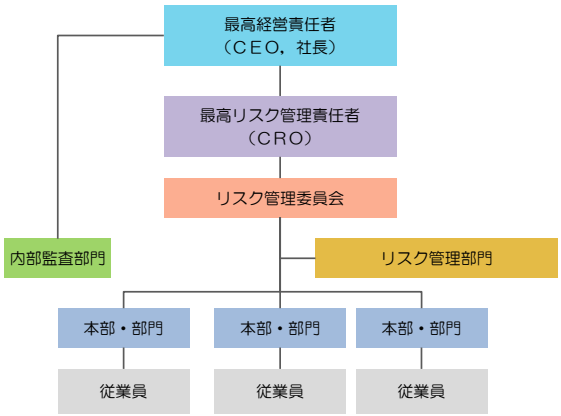
2. 不祥事・事故を起こさないための取り組み（個別論：組織作り・リスクの認識）

（ア）組織作り

内部統制システムを有効に機能させるためには、理論上２つの組織が必要になります。一つはリスク管理全体の企画立案を行うリスク管理部門と、立案されたルール通りに業務執行が行われているかどうかを評価するための内部監査部門です。両組織の役割をもう少し詳しく見て参りましょう。内部統制システムもマネジメントシステムの １ 種であるため、Plan（計画）→ Do（実行）→ Check（評価）→ Action（改善）の考え方を適用することができます。簡略化して示すと、①社内ルールの整備（Plan）→②現業部門への徹底（Do）→③監査（Check）→④ルールの見直し（Action）となります。このうち①②④を担当するのがリスク管理部門（なお労務管理など個別制度については人事部などの所管部門が担当します）、③を担当するのが内部監査部門になります。ルールを作った人が自らを評価することはできませんので管理部門と内部監査部門、2 つの組織が必要になる訳です。ただ中堅中小企業など複数の専門部署を設置することができない場合、リスク管理部門は総務部など他の管理部門が機能的に兼務し内部監査部門だけを独立組織として設置させるのが良いでしょう。なお内部監査部門は監査権限を持たせる必要があるため最高経営責任者（CEO、社長）直轄とすることが一般的です。組織体制の詳細については図 2 をご覧下さい。

なおリスク管理部門を統括する役割として重要なのが最高リスク管理責任者（CRO）です。CRO に指名された役員（兼務）は社内の不正だけでなく海外出張先での事故や他企業との訴訟など、全てのリスクを一元的に管理する役割を担います。また CRO は経営陣で構成されるリスク管理委員会を開催し（実際には経営会議とセットで行われることが多い）、発生した事案を組織内で共有します。あわせて個別事案に対する必要な対応策や組織全体での再発防止策について各部門からの助言も受け、必要な提言を行います。

図 2 リスク管理のための組織体制



主体	主な役割
最高経営責任者	①リスク管理体制構築・運用に関する最終責任 ②リスク管理ビジョンの設定と社内への浸透 ③リスク管理に必要な経営資源の確保 ④リスク管理を最適な状態に保つための全社的なレビュー
最高リスク管理責任者	①リスク管理に関わる全社的な統括 ②リスク管理の有効性を評価し、最高経営責任者へ報告 ③リスク管理全体の是正・改善 ④リスク管理に関連する事項において、外部機関との連絡窓口
リスク管理委員会	①リスク管理に関する重要テーマの議論および意志決定 ②全社的観点からのリスク評価の実施 ③全社的レベルでのリスク対応策の検討および決定
リスク管理部門	①リスク管理の構築・運用に関する事務局 ②全社的なリスク対応に関する対応策の立案 ③各部門からのリスク管理に関する情報のとりまとめ ④各部門にけるリスク管理活動への指導および助言
内部監査部門	①独立した立場から、リスク管理の構築・運用状況の監視 ②リスク管理の状態について、最高経営責任者への適切な報告 ③必要に応じ、リスク管理の有効性の観点からの改善助言
各本部、部門	①リスク管理ビジョンに従った行動 ②日常業務におけるリスク管理活動 ③日常業務でのリスク対応に関するモニタリング ④自部門のリスク管理状況の適切な報告

（イ）リスクの認識

企業の社会的活動に注目が集まるなど、企業を見る社会の目はより一層厳しさを増しています。金銭的な内部不正だけに限らず品質面の不正、個人情報漏洩、外部ハッカーやコンピュータウィルスによるシステム攻撃など、企業は様々なリスクに対処していかなければなりません。しかしながら社内的なリソースも限られている中、全てのリスクに対応することは現実的に不可能です。このため企業は次のような取り組みを行い、自社が管理すべきリスクをうまく絞り込まなければなりません。その巧拙により企業のリスク対応力が大きく変わってくると言っても過言ではないでしょう。

- ✓ 自社を取り巻くリスクの洗い出し
- ✓ リスクの評価と管理対象リスクの選定
- ✓ 管理対象リスクに対する管理方針の策定

まず「自社を取り巻くリスクの洗い出し」ですが、闇雲にリスクを挙げ連ねるだけではどうしても漏れが生じます。リスクを効率よく抽出するためにはチェックリスト（リスクマップ）を利用するのが効果的です。図 3 にそのチェックリストを示します。経営者が検討すべきリスクには「戦略リスク」「事業性オペレーショナルリスク」「管理系オペレーショナルリスク」「事故・災害リスク」の 4 種類があります。このうち「戦略リスク」は事業戦略で検討すべき領域、「事故・災害リスク」は BCP（Business continuity planning ＝ 事業継続計画）で検討すべき領域となり、内部統制システムが取り扱う領域は「事業系オペレーショナルリスク」と「管理系オペレーショナルリスク」の 2 つになります。各オペレーショナルリスクはさらに小分類に分かれ個別のリスクに展開されます。「事業系オペレーショナルリスク」の場合、全社のサプライチェーンを構成する「サービス」「マーケティング」「販売」「製造」「物流」「調達」「取引先」「アウトソーシング」の各分野が対象となります。「製造」における食の安全性や品質不良はマスコミでもよく報道されており、分かりやすい例と言えるでしょう。「管理系オペレーショナルリスク」が対象とするのは「情報システム」「財務」「市場」「株主」「広報・IR」「資産保全」「環境」「労務」「コンプライアンス」「法律・規制・商習慣」「ガバナンス」「コミュニケーション」「人材」「組織・企業文化」といった分野です。「情報システム」におけるウィルス被害や情報漏洩、労務における労基法違反も最近世間を賑わす話題となっています。このようにチェックリストを活用することで、自社が抱えるあるいは管理すべきリスクを効率的かつ網羅的に抽出することができます。経営者は図 3 のチェックリストをひな形として活用しながら過不足を補い、自社に適したチェックリスト（リスクマップ）を完成させると良いでしょう。

「自社を取り巻くリスクの洗い出し」が終わったら、次は「リスクの評価と管理対象リスクの選定」です。例えば発生確率と影響度で評価するのも一つの方法です。各評価項目をH（ハイ）・M（ミドル）・L（ロー）の 3 段階で評価しても構いませんし、5 点満点で評価しても良いでしょう。この評価付けを過度に細かく行う必要はありません。どのリスクに対する評価も主観的なものであるため、あまり精緻に行うことに意味は無いからです。大事なことは方法論ではなく、自社の感覚にあった評価を行うことです。個別の評価を行った後に総合評価を行い、管理対象リスクを選定します。

図 3 企業を取り巻くリスク チェックリスト(リスクマップ)

大分類	小分類	リスク例
戦略リスク	外部環境の不確実性	競合の戦略変更、新規参入
		顧客ニーズ変化、顧客層の変化
		景気変動
	経営計画	経営戦略、経営計画、施策等のリスク
	経営的意思決定	意思決定リスク
	経営情報管理	適切でない経営情報の伝達
事業系オペレーショナルリスク	サービス	代替商品、虚偽表示
	マーケティング	顧客ニーズとのミスマッチ、価格設定、商品構成
	販売	顧客満足低下
	製造	食の安全、品質不良、原価アップ
	物流	物流コスト増大、輸送ルート断絶、誤配・遅配、商品の滅失
	調達	資源の枯渇、調達価格の高騰、余剰在庫、滞留在庫
	取引先	取引先の倒産、調達先・提携先の変化、取引先の姿勢の変化
	アウトソーシング	外注コスト増大、要求水準未達、アウトソーサーへの過度の依存
管理系オペレーショナルリスク	情報システム	システム障害、情報漏洩、ウイルス被害、サイバーテロ、IT技術の陳腐化
	財務	財務諸表虚偽記載、引当金不足、含み損の発生、債権回収不能・遅延
	市場	金利変動、為替変動、株価変動
	株主	株価低下、株主構成の変化、買収
	広報・IR	虚偽情報開示、開示遅延、マスコミ対応失敗、クレーム対応失敗
		アナリストの評価、各種団体からのクレーム・要望の強化
	資産保全(物理的変化、知的財産)	建物・設備の損失、現金・貯蔵品等の滅失、ノウハウ・特許の流出
	環境	CO2排出、不法投棄、土壌汚染
	労務(安全、就業)	労基法違反、ハラスメント、人権問題
	コンプライアンス	法令違反、贈収賄、インサイダー、契約不履行、反社会的勢力との関係、金銭事故
	法律・規制・商慣習	法律・規制の変更、当局の姿勢の変化
	ガバナンス	役員の不正、グループ会社の統制不足
	コミュニケーション	方針の不徹底、組織間の連携不備、重要情報の伝達漏れ
	人材	人材流出、採用難、モチベーション低下
	組織・企業文化	M&A等による社内の混乱、組織の硬直化
事故・災害リスク	自然災害・関連事故	自然災害(地震、風水害等)、天候不順、病気の蔓延
	事故・犯罪	電力等公共サービスの停止、犯罪、事故
	国レベルの紛争・混乱	戦争・紛争、テロ、インフレ・通貨危機、政変

出所)経済産業省 事業リスクマネジメントを参考にMURC作成

管理対象リスクが選定されれば、対象リスク毎に管理方針を決めます。例えば独占禁止法に関する法令違反を犯さないようにするためには「社内研修の充実」が必要かもしれません。コンピュータウィルスによる個人情報の漏洩を防止するためには、社内人材ではスキルが不足しており外部のセキュリティ専門会社に委託(「外部委託」)した方が効果的かもしれません。それ以外にも、「社内申請ルールの整備・強化」「業務上のチェック機能整備・強化」「IT を使った監視機能」「保険の活用」など様々なリスクコントロール手法があります。このように管理対象となったリスク毎にどのようにリスクをコントロールするのか、その方針と方法論を丁寧に考えることが大切です。

3. まとめ

ある顧客はこれまでの実績を買われ、大手流通企業との取り引きを始めました。しかし商品の販売直後、商品パッケージに記載されていた内容に間違いがあることが見つかり、取引先からの信頼を大きく損なうことになりました。さてこれは単なるミスでしょうか? それとも統制不足(仕組みの問題)だったのでしょうか? 「リスクにどう向き合うか」が、今の経営者に求められています。

(お問い合わせ)コーポレート・コミュニケーション室 TEL:03-6733-1005 E-mail:info@murc.jp