健全な成長を支える事業基盤としてのGRC（ガバナンス・リスク・コンプライアンス）
取組事例からの示唆

中野浩志
SAPジャパン株式会社
早稲田大学大学院非常勤講師
日本CFO協会 主任研究委員
米国公認会計士 公認内部監査人

日本企業のグローバル展開に伴う海外子会社ガバナンスの重要性の高まり、M&Aなどによる異文化・異人種との共働機会増加、そして労働市場の流動性の高まりや帰属意識の希薄化。従来、社員の阿吽の呼吸や高い帰属意識に依存してリスクの予防をしてきた日本企業であるが、直面するグローバル化やリスクの多様化を踏まえると、「人」への過度な依存には限界がある。日常業務プロセスの中にリスクを予防する仕掛けを組み込むこと。システムの利用を通して、国や法人の枠を超えてルール遵守がナビゲートされる仕組み作りと工夫が、各社取組事例から伺える。本稿では、企業価値に大きな毀損をもたらす不正の予防・発見に着目して、各社取組事例をご紹介する。

事業活動とリスク管理の融合

A社は急速なグローバル事業展開に伴うリスクの多様化、遵守すべき法規制の増大への対応が急務であった。場当たり的なリスク対応では変化対応力、コストの両面で限界がある。そこで、同社はガバナンス・リスク・コンプライアンスを一貫化したGRCフレームワークのもと、「ポリシー」、「組織」、「プロセス」、「レポーティング」およびそれを支える「GRCシステム」の整備を段階的に推進した。経営理念や事業目的に照らして経営に重大な影響を及ぼすリスクを経営者が認識・評価して対応するプロセスを構築し、地域・法人・事業等の各責任者は、事業管理の一環としてKRI（Key Risk Indicator）等をダッシュボードやモバイル端末で継続的にモニタリングしている。一定金額以上の引合いがシステム入力されると、潜在リスクとしてリスク管理部門に通知され、リスク管理部門のレビューなしでは社内承認プロセスを進めることができなくなる。また、不正リスクのある取引が検知されると、内部監査部門に通知され調査要否の判断を促すなど、リスク管理を日常業務プロセスに組み込む工夫も行っている。

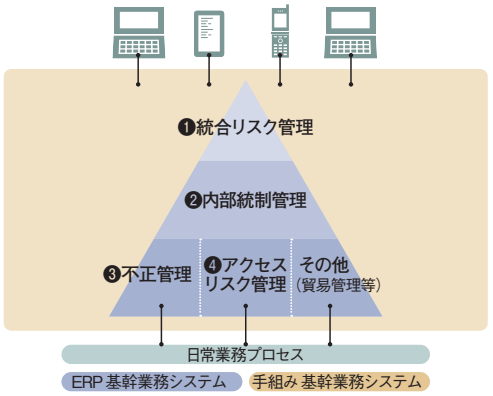
A社のようにシステムを利用して業務プロセスの中にルールを組み込む意味は大きい。システムの利用を通してリスク検知やコンプライアンスを遵守する図式ができあがるからだ。例えば、新興国取引先からの大量注文オファー判断に際して、システムが利用可能在庫、製造拠点別生産能力の照会を行うのみならず、仕向け国の環境規制をチェックして注意を促す。また、受注担当者が受注入力を行うと、受注単価・数量などの入力異常値や利用可能在庫、与信限度額のみならず貿易コンプライアンスがチェックされ、取引相手が懸念取引先と検知されると、受注ブロックがかかり安全保障貿易部門に通知されるという具合だ。

ルールに基づいて例外事象を検出し、担当者に通知することは業務負荷軽減のみならず、現場に気づきを与え、考えることを促す。うっかりミスやつい魔がさしてしまうことは誰にでもありえる。国により不正の捉え方も異なり、認識GAPが事故に繋がるケースも少なくない。社員とそのご家族を不測の事故やリスクから守る基盤。そして、経営トップの意思やリスク管理ポリシーを確実に業務プロセスに組込み、グループ全体の健全な成長を支える基盤にITは進化している。

不正リスクへの対応～職務分掌リスク～

日本企業がグローバル展開を進める中、海外子会社ガバナンスの共通課題の1つが、不正の防止である。ほとんどの業務がシステムを通して実行される中、そもそも不正を実行できるような権限の

●GRCシステム概要



❶ 統合リスク管理 (Risk Management)
- リスク管理やリスク指標の集約・分析
- 全社横断的なリスク可視化 (ダッシュボード)

❷ 内部統制管理 (Process Control)
- 統制の一元管理 (統制文書・社内規定)
- 統制自己評価 (サーベイ)
- 管理プロセスの自動化
- 「持続的統制モニタリング」自動化

❸ 不正管理 (Fraud Management)
- 不正リスク検知・予兆の発見
- 調査・結果の記録
- 不正検知ルールのシミュレーション(誤検知減少)

❹ アクセスリスク管理 (Access Control)
- 職務分掌 (SoD:Segregation of duties) 分析
- 職務分掌リスク事前テンプレート(約260リスク)
- 特権ユーザー管理 (貸出運用・モニタリング)等

与え方をしないという職務分掌の視点が大切になる。一方、業務ユーザーが必要な権限を申請し、情報システムは間違いなく権限付与を行うという業務プロセスの中で職務分掌リスクを検知するのは難しい。人が網羅的にアクセス権限レベルの職務分掌リスクチェックを行うのも限界がある。そこで、GRCシステムを利用して職務分掌リスクの検知、運用の自動化・効率化を実現したグローバル製造業B社の事例を見てみよう。同社はまず、ツールの中に事前定義されている職務分掌リスクテンプレートを利用し、網羅的にリスクの洗い出しを行った。例えば、ある社員に仕入先マスター登録権限と支払処理権限が割り当てられていると、架空送金リスクのある社員という形でレポートされる。そして、現状のリスクを分析し、業務分担と権限設定の見直しを行った。兼務が避けられない場合は補完的統制を組み入れリスクの軽減を図った。さらに、組織変更や異動の権限変更時には、職務分掌リスクを事前に自動チェックする予防的統制、毎月職務分掌リスクレポートを出力してリスク責任者がレビューする発見的統制を業務プロセスに組み込み、統制の持続可能性を高めている。ただし、各国独自にツールを導入したため国ごとにリスク定義の仕方、使い方に一貫性がなかった。そこで次のステップとして、同社リスク管理フレームワーク／セキュリティフレームワークに準拠する形でグローバル共通職務分掌リスクテンプレートを構築して欧州地域へパイロット導入したのを皮切りに、地域単位で順次展開を行った。地域横断で一貫性のある職務分掌リスク検知の仕組みを整備することで、監査効率と監査品質の向上、職務分掌リスク検知・メンテナンス業務集約化(SSC化)などを実現している。

大量取引明細データから不正リスクを炙り出す

IT技術の進化を活かし、取引明細データや取引マスターデータなどの大量データの中から不正リスクを検知・予防する取り組みも進んでいる。日系グローバル製造業C社の取り組みを見てみよう。同社はグループ全体最適化を目指し、M&Aを積極的に進める中でグローバル経営体制の強化を図っている。その中で、M&Aで買収したグループ企業のガバナンス強化の必要性、グループ拡大に伴う決算にインパクトを与える不正取引リスク増大が顕在化してきた。現状の監査リソースでますます増えるグループ企業のガバナンスを強化するためには、不正監査のカバー率・精度の双方の向上が必要となり、ITを高度に利用した改革が不可欠である。そこで同社は不正検知ルールに基づいて取引データ全件をチェックし、不正リスクを洗出すGRCシステムを試行した。架空売上(期末押し込み、翌月戻し)なら期首返品率・額、出荷から返品までの期間が短く決算期を跨いでいる等を不正検知ルールとして設定し、ルールに抵触する取引データを持つ取引先が架空売上リスクありとしてアラートされ、不正調査の経緯と結果をアラートに紐づけて記録・蓄積するという具合だ。システムで全ての不正検知ができるわけではない。しかし、システムでできるところはシステムに任せ、人でしかできないところに限られた人財を投入して監査カバー率と精度を高める意味は大きい。システムを利用した全件チェックによる網羅性確保、人に依存しない監査品質平準化、全件見られているという牽制効果に加え、熟練社員の経験に基づく不正発見手法を不正検知ルールとしてシステムに埋め込み、資産化・継承できる点も見逃せない。

海外に目を向けると不正検知の仕組みは、ソフトウエア企業のライセンス不正利用、損害保険会社における不正請求チェック、通信企業における携帯電話不正利用・代理店不正請求、税務当局における不正申告洗い出しなど、さまざまな用途で活用されはじめている。海外子会社ガバナンス施策としても検討の余地がある仕組みであろう。

●

リスク管理は知識でなく意識と言われる。グループ企業一人ひとりへの啓蒙活動が最重要であることは言うまでもない。ジョブローテーション、内部統制制度の確立などの従来からの取組に加えて、システムを利用したリスクコントロールの日常業務への組み込みと継続的モニタリング体制の整備は、グローバル市場を土俵に事業を健全に成長させていく上で、今後ますます重要になると思われる。