企業リスクに備える

統合的GRC（ガバナンス、リスク、コンプライアンス）構築に向けて

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
米国公認会計士、公認内部監査人
日本CFO協会 主任研究委員

ここ数年の企業不祥事の頻発、法制度の改革、レピュテーションリスクの増大により、企業リスクへの関心が高まっている。一方、リスク予防においてきわめて重要な役割を担ってきた社員一人一人の負担は、人員削減や法制度対応に伴う社内管理徹底の流れの中で重くなるばかりだ。社員の帰属意識の希薄化や企業の説明責任の増大を踏まえると「人」への過度な依存には限界がある。「業務プロセス」の中にリスクを予防する仕掛けを組み込み、「IT」を利用して社員の業務負荷を軽減しつつ統制の持続可能性を高める取り組みが改めて問われて来ているといえる。

「人」を軸にした「業務プロセス」「IT」の整備

昨年秋に上場企業財務担当役員に対して実施した財務マネジメントサーベイ(*1)では、内部統制強化にあたり最も重要と考えるポイントとして「人」に加えて「業務プロセス」「IT」があげられた。多様化する法制度や企業リスクを前に、どのように「人」「業務プロセス」「IT」を整備していけばよいのであろうか。金融商品取引法等、ここ数年相次いで導入された法制度の多くはリスク管理を中心とするものといえる。どのような見地からリスクを評価して対応すべきなのかという点が各制度の目的によって異なっているに過ぎない。形は違っていても、リスクを軽減する仕掛けをルール化して「業務プロセス」に組み込み、「人」を教育してルール遵守を動機付け、それが遵守されているかを点検・内部監査して改善していくという点では大枠で大差がない。そこに取り組みのポイントがある。場当たり的な法制度対応でなく、基本的枠組みを押さえて一貫性を持ちながらリスクの統合管理を行うこと。そして、「IT」を利用して日常業務プロセスの中にルールを組み込むことが、社員の業務負荷を軽減しつつ統制の持続可能性を高める鍵になる。

「IT」を利用してルールを業務プロセスに組み込む

一貫性を持った取り組みには、健全なコーポレートガバナンスのもと、経営理念や事業目的等に照らして経営に重大な影響を及ぼすリスクを企業経営者が認識・評価して対応するプロセスを構築し、教育やITを通して日常業務プロセスの中に浸透させる仕組みを作ることが大切になる。「IT」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業務プロセス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。業務の効率化だけでなく、プロセスの流れやルールを人が忘れてもシステムが気づかせてくれる。例えば、受注担当者が受注処理を行うと、受注単価・数量などの入力異常値や利用可能在庫、与信限度額のチェックのみならず、仕向け国法制度に基づいた貿易コンプライアンスがチェックされ、受注ブロックがかかるという具合だ。ルールに基づいて例外事象だけを検出し、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る。社員とご家族を不測の事故やリスクから守る基盤。そして、トップの意思とポリシーを確実に業務プロセスに組み込み、実行を徹底する基盤にITは進化している。

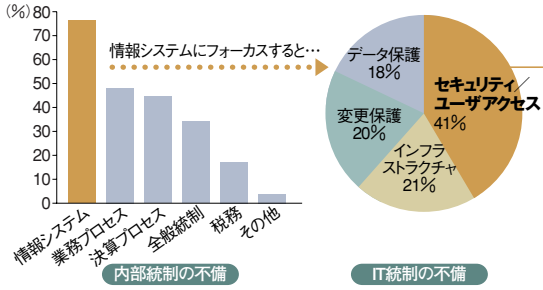
企業リスクを防ぐ前提条件――職務分掌

ITを利用して業務プロセスに統制を組み込む時の留意点として職務分掌がある。米国における状況（図

図1●内部統制の信頼性を高める前提―職務分掌

米国事例から、セキュリティー／ユーザーアクセス、そして職務分掌はIT統制における最重要課題であることが伺えます。

●米SOX法財務報告に係る内部統制の有効性評価に関して、重大な修正が必要となった分野



●ユーザーアクセス／セキュリティ分野における10大統制欠陥

1	不完全な職務分掌
2	会計システムのOSに関するアクセスコントロール不備
3	会計システムのデータベースに関するアクセスコントロール不備
4	開発要員が本番環境で本番処理を実施できる
5	多くのユーザが「特権ユーザ」処理を実施できる
6	退職職員・コンサルタントによるシステムへのアクセスが可能
7	財務アプリケーションへのデータ入力期間に制限なし
8	カスタムプログラムやテーブル、インタフェースがセキュアでない
9	人手による業務手順が明確に存在していない、守られていない
10	システム文書が実際のプロセスに合格していない

【出典】Ernst & Young ISACA Sarbanes Conference

【出典】Emerging Trends in Internal Controls
U.S.-Listed Foreign Private Issuers Second Survey and Section 404 Reference （Ernst & Young）

1）や特定個人への権限集中が不祥事の原因となった過去の事例を見ても、職務分掌が内部統制の信頼性を高める前提となるのは明らかだ。例えば、売上計上と滞留売掛金チェックが一つの部署で完結している場合は、架空売上げの計上に対する牽制は弱いといえる。「職務分掌」された状態で各人が業務を行うことにより統制の実効性を高めることができる。一方、職務分掌規定というルールだけあり、「破ろうと思えば破れる」状態では社員を不正や過ちから守ることはできない。適切な範囲で「IT」を利用して「職務分掌」をアクセス権限という形で業務プロセスに組み込み、統制の実効性を高める必要がある。

事例――ITを利用して業務プロセスに職務分掌を埋め込む

ある外資系メーカー日本法人での取り組み例を見てみよう。同社は、会計、在庫管理、購買管理にERP（統合基幹業務システム）を採用しており、グループレベルのリスクマネジメント・内部統制に対する意識も高い。ERPで権限は詳細に設定できるが、それでは十分でなかった。米国SOX法で外部監査法人から求められるのは、詳細に設定した権限の組み合わせにリスクがないこと、つまり、ユーザーに付与された権限の組み合わせが職務分掌上適切かどうかである。組織変更や異動など変化への対応も考慮すると、権限設定の妥当性チェックを人手で行うには限界がある。そこで、同社はIT（ツール）を利用した職務分掌リスクの洗い出し、運用の自動化・効率化に踏み切った。まず、事前定義されているリスクライブラリを利用し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、三ヵ月間かけて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。

●

職務分掌を例にとりご紹介したが、「人」「業務プロセス」「IT」の整備は、自社の「戦略」やグループ各社の状況を踏まえて段階的に行っていく必要がある。多様化する企業リスクに対してガバナンス、リスク、コンプライアンス（GRC）の一貫性を保ちつつ、事業をより健全に成長させるためにいかにGRCを活用するかという視点での取り組みが、持続的に企業価値を向上させていく上で今後ますます大切になる。

（*1）CFO FORUM 一八号（二〇〇六年九月発刊）

図2●統合GRC（ガバナンス・リスク・コンプライアンス）と職務分掌リスク