内部統制

●内部統制の目的は、米国の COSO フレームワークによると、「業務の有効性及び効率性」、「財務報告の信頼性」、「関係法令等の順守」である。日本はこれに加えて、「資産の保全」を追加している。

●つまり、内部統制とは、組織内部において、上記目的を達成するための手続き、仕組み、プロセス等を整備し、それを組織全体で遂行することにより、組織の活動全般を適切にコントロールすることである。

●内部統制の法整備として、米国では SOX 法、日本も模倣して金融商品取引法等で規定

IT への対応

●内部統制の基本的要素の中に「IT への対応」（← 日本独自）があり、業務の実施において、組織の内外の IT に対して適切に対応することであり、「IT 環境への対応」、「IT の利用」、「IT の統制」がある。

●IT 環境への対応とは、組織内外の IT 環境に対して適切な対応をとることである。

●IT の利用とは、「IT への対応」以外の基本的要素の有効性を確保するために、IT を有効かつ効率的に利用することである。

●IT 統制とは、IT が有効かつ適正に利用されるよう監視・統制するために「IT への対応」以外の基本的要素を機能させること。つまり、「IT の利用」と「IT の統制」は共存又は相互牽制しているようなもの。

IT 統制

●IT 統制は以下の 2 つに大別される。

①IT 業務処理統制：業務プロセスに組み込まれた情報システムの処理工程において、データの欠落や重複等が発生することなく、その正当性や正確性等を確保するために行う各種コントロール。具体的には、入力データのチェックの認証機能、マスターデータの維持管理、システム利用のアクセス管理等がある。

②IT 全般統制：IT 業務処理統制が有効かつ適正に機能するために必要な組織全体の IT 基盤、施策、体制等からなる各種コントロール。具体的には IT 戦略、ISMS（各種セキュリティ対策等）がある。

IT ガバナンスと IT 統制

●IT ガバナンスと IT 統制は全く関係ない。「IT ガバナンス」は「コーポレートガバナンス(企業統治)」つまり「会社は経営者ではなくステークホルダのものという考えのもと、社外取締役の配置、監査の実施、取締役と執行役の分離等によって企業経営を監視する仕組み」から派生した言葉である。

●そのため「IT ガバナンス」とは「経営陣がステークホルダのニーズに基づき、組織の価値を高めるために実践する行動であり、情報システムのあるべき姿を示す情報システム戦略の策定及び実現に必要となる組織能力である」と定義している。わかりやすく言うと「IT システムを戦略的に活用し、その効果を最大化するための組織の仕組み」である。

●「IT ガバナンス」における経営陣の具体的な役割として「EDM モデル」があり、IT マネジメントとそのプロセスに対して、経営陣が、Evaluate（評価）、Direct（指示）及び Monitor（監視:モニタ）を行うことである。

●ガバナンスの中核である IT システムに対する監査は、システム監査基準とシステム管理基準を使用。