ITガバナンスの継続的な維持・改善
―COBITに基づく体系的なフレームワークの確立―

金融機関では、金融庁の指導のもと主にシステムリスク対応の観点からITガバナンス（統治）の整備が進められているが、仕組みを支えるルールの度重なる改定により管理プロセスが煩雑化しているものと考えられる。本稿では、金融機関がこうした煩雑化を避けてITガバナンスを継続的に維持・改善していく上で有効な、体系的なフレームワークの確立方法について紹介する。

見えにくくなるITガバナンスの仕組み

コーポレートガバナンスや内部統制の強化が叫ばれるなか、企業はITを経営戦略に沿って正しくかつ効率よく活用することを求められている。そのためには、全社的にITの投資・効果を最適化し適切なリスク管理を行うITガバナンスの仕組みを作り、これを維持・改善していく必要がある。特に金融機関は、さまざまな分野に与える影響の大きさから、金融庁の検査・指導が徹底されてきている。その結果、金融機関のITガバナンスは、システムリスクへの対応という点では高いレベルに達しているところが多い。

しかし、そこには2つの懸念事項がある。1つは、ITガバナンスの仕組みを維持するためのルールがたびたび改定されることから、既存の社内規定や業務マニュアルなどの中にルールが分散し、埋没していくおそれがあることである。もう1つは、システムリスクへの対応が重視されるあまり、IT活用の本来の目的であるビジネスへの価値提供に対する評価を適切に行うための統制活動にはなかなか目が向かないことである。

そうなると、組織全体としてITガバナンスの仕組みを維持・改善していく上で、以下のような問題が発生する可能性がある。

①どのような目的のもとで個々のルールが整備されているのかが見えにくくなるため、統制活動を改善していく際にルール改廃の適否を判断しにくい。

②システムリスク対応に傾きすぎることで、IT投資や効果を評価する能力が低下するなどバランスの取れない統制活動となる。

COBITによる体系化の有効性

ITガバナンスは包括的な管理の仕組みであるため、実務的には何らかのフレームワークに準拠することが非常に有効である。そのフレームワークとして事実上の国際標準となっているのがCOBITである。COBITはITIL®（ITサービス管理のフレームワーク）やISO/IEC 27001（情報セキュリティマネジメントシステムに関する国際標準規格）、ISO 9001（品質マネジメントシステムに関する国際標準規格）など他の国際標準規格とも密接に関連しており、米国SOX法との関連で整理されたCOBIT for SOXも作成されるなど、網羅性の高いフレームワークとなっている。

従って、COBITの体系に沿って統制に必要

野村総合研究所
システムコンサルティング事業本部
社会ITコンサルティング部
上級システムコンサルタント
山下　晃（やましたあきら）
専門はITガバナンス態勢整備、システム基本構想策定など

なルールを整理すれば、個々のルールの目的や他の規格との関係が明確化できるため、上記のような問題を解決することが容易になる。ただし、COBITはもともと欧米の組織を対象として作成されたものであることや、ボリュームも大きいことから、効果的かつ適切に導入するためには種々の工夫が必要になる。

ルール整備上の工夫・留意点

以下では、COBITに基づいてITガバナンスのルールを整備していく上での工夫や留意点について述べる。

(1) 優先順位づけと計画的な導入

COBITは、網羅性が高い半面、実施事項も膨大になっているため、すべてを一度に取り込むことはきわめて困難である。従って、統制領域と対象システムの優先順位を決めて計画的に導入することが必要である。金融機関では、金融庁や監査機関に指摘を受けた事項や、金融庁の検査マニュアルなどの指針類の中で、COBITとの関連が密接な事項を優先させることになる。管理対象となる情報システムが多数ある場合には、投資規模や経営に与える影響の大きさから優先度を判断する。

(2) 組織と実行者を明確にするルールを作成

COBITは、現場の担当者から経営者まで、さまざまな立場の者が活用することを前提に作られている。そのため、そのまま導入すると誰が実施するのかが不明確なルールになりかねない。そこで、ルール作成の際には、ITガバナンスに関係する組織を明確化し、組織構成員の業務や責任が明確になるルール体系とする必要がある。通常、ITガバナンスの組織階層は、経営層、ITを管理する担当部門、システム開発・運用を担当する部門に分けられる。それぞれの視点で、いつ誰が何を実行すべきかまで規定することが、ルールの実効性を担保するためには有効である。

(3) 既存の社内規定・基準の有効活用

金融機関の場合、すでに一定以上のレベルで統制のルールが整備されていることが多い。また既存のルールは、各現場がすでに順守しているものであり、現場の業務実態に適合していると想定される。従って、既存のルールをできる限り体系的なフレームワークの中に取り込んで有効に活用することが、効率性、実効性の観点から得策である。そのためには、ITガバナンスに関係しそうな既存の社内規定を棚卸しして、COBITの体系と照らし合わせ、漏れや重複を整理することが有効である。

合併や再編の加速、金融庁による規制強化、消費者庁・消費者保護法への対応などを背景に、金融機関は自社のITガバナンスの見直しを迫られている。COBITのような体系的なフレームワークの活用は、そのための非常に有効なアプローチとなるであろう。ここでは主に金融機関を念頭に述べてきたが、ITガバナンス整備の考え方は他の企業においても同じように適用できるはずである。 ■