統合的なITマネジメントにつなげるIT全般統制

金融商品取引法に対応するための内部統制構築が本格化するなか、内部統制評価の実施基準が発表され、IT統制のフレームワークの整備も進んでいる。本稿では、本番運用の開始まであと半年を切った内部統制について、そのために必要な備えを確認しておくとともに、内部統制を通じたIT分野の統合的なマネジメントを志向することの意義について提言する。

金融商品取引法が求める2つのIT内部統制

金融商品取引法にいう内部統制評価のより所のひとつに、2007年２月に発表された金融庁の「実施基準」がある（http://www.fsa.go.jp/singi/singi_kigyou/tosin/20070215.html）。

そこでは、内部統制は①経営者による内部統制、②全社的な内部統制、③業務プロセスに係る内部統制の３つに区分されている。このうち②と③はITの利用に関わる部分があり、②ではIT全般統制、③ではITアプリケーション統制という２種類のITの内部統制を構築・評価することが求められる。

IT全般統制の構築にあたって

ITアプリケーション統制が、企業内の各業務プロセスの統制を通じて会計上の虚偽記載につながるリスクを低減させるのに対し、IT全般統制は、システム開発、システム変更、システムの保守・運用、トラブル対応などITに係わる全般的な活動への統制となっている。IT全般統制は、個々の業務のあり方に左右されるITアプリケーション統制とは異なり、システムの構成や内容によって若干の違いはあるものの、企業のIT運用に係わる全社的な内部統制という意味で汎用性が高い。

IT全般統制の構築にあたっては、米国で導入されているCOBIT for SOXを参考にすることが第一義的には有効であると考えられる。COBIT for SOXは、世界的な標準であるCOSOフレームワーク（内部統制全般のフレームワーク）の観点から、IT統制評価のフレームワークであるCOBITの内容を整理し、SOX法に対応するIT統制の目標を定めたものである（http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=32586）。

COBIT for SOXでは、IT戦略策定から調達（開発）・運用・評価までのITマネジメントプロセスを「計画と組織」「調達と導入」「サービス提供とサポート」「モニタリングと評価」という４つの領域と、それぞれに対応した合計34の項目で定義している。

日本でも経済産業省から2007年３月に「システム管理基準 追補版（財務報告に係るIT統制ガイダンス）」が公表されている（http://www.meti.go.jp/press/20070330002/system kijun-tsuiho.pdf）。実施基準の管理項目と統制目標の対応関係が記載されているため、IT全般統制の構築に関してIT部門担当者の

レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。
Copyright © 2007 Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.

野村総合研究所
システムコンサルティング事業本部
ERMプロジェクト室
上級コンサルタント・技術士（経営工学部門、総合技術監理部門）
姫野桂一（ひめのけいいち）
専門はリスクマネジメント、内部統制構築支援

表1　IT分野の国際標準規格（ISO規格）の概要

規格名称	概要
ISO 15504：システム開発（2006年）	CMM（Capability Maturity Model）をベースに発展したシステム開発の品質管理に関する国際規格。
ISO 12207：開発プロセス（2004年）	システム開発プロセスに関する国際規格で、ソフトウェアライフサイクルモデルのプロセス群が盛り込まれ、文書化プロセスや構成管理プロセスなどが記載されている。
ISO 20000：ITサービスマネジメント（2005年）	ITILをベースに発展したシステム運用に関する国際規格。 日本ではJIPDEC（日本情報処理開発協会）が2007年4月よりITSMS（ITサービスマネジメントシステム）適合性評価制度を開始し、22の事業者が認定されている（2007年10月14日時点）。インシデント管理、問題管理、変更管理、構成管理などのプロセスに分けられる。
ISO 27001：情報セキュリティマネジメントシステム（2005年）	英国のBS7799をベースに発展した情報セキュリティの国際規格。 日本ではJIPDECが2002年よりISMS（情報セキュリティマネジメントシステム）適合性評価制度を開始し、2,359の事業者が認定されている（2007年10月19日時点）。
ISO 19770：ソフトウェアの資産管理（2006年）	ソフトウェアの資産管理に関する国際規格で、ISO 20000との整合も図られている。

注）規格名称欄の括弧内の年は最新版の発行年

参考となる。

統合的なITマネジメント構築に向けて

上場企業では、金融商品取引法に対応した内部統制は2008年4月から本番に入り、内部統制の点検・整備の段階から、その運用の有効性を評価する段階へと移行する。

上述した金融庁の「実施基準」では、金融商品取引法で求められる内部統制について、「経営者による評価及び報告と監査人による監査を通じて財務報告に係る内部統制についての有効性を確保しようとするもの」であって、「財務報告の信頼性以外の他の目的を達成するための内部統制の整備及び運用を直接的に求めるものではない」としている。しかし、金融商品取引法への対応を契機に本格化した内部統制の活用範囲を“他の目的”に拡張し、将来的に全社的なIT分野の統合的なマネジメントへと発展させることは大きな意義があると考えられる。それは、企業のリスクマネジメントへの対応能力を高め、既存の統制活動との重複をなくすことにつながるからである。

そのような統合的なマネジメントを実現するにあたっては、国際標準規格（ISO規格）が参考になる（表1参照）。近年、IT分野のISO規格は、システムの開発・運用、情報セキュリティ、ソフトウェア資産管理というように、情報システムのライフサイクルに沿った形で各種の規格が策定されている。それぞれの規格に盛られた詳細な管理策を分析した上で、必要な部分を組み合わせていけば、統合的なマネジメント構築を効率的に進めていくことが可能である。■

レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。
Copyright © 2007 Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.