内部統制マネジメントモデルの構築

－わかりやすい IT 全般統制をめざして－

アブストラクト

1. 研究の背景と目的

国際的な内部統制強化の流れの中、通称日本版 SOX 法が制定された。先行した米国事例の膨大な対応費用の反省を受け、日本では効率的な対応が議論されているが、具体的な対応策は明確でなく、各企業は実際の対応方法に困惑していると考えられる。情報システムの適正管理として従来からシステム管理基準があり、また、ITIL、情報セキュリティ管理基準、ISMS、PMS、CMMI など、すでに様々な基準・規格を利用しながら適正管理を図っている。このような複雑な状況の中で、当分科会はわかりやすい IT 全般統制の対応をめざすべく、有効かつ効率的な仕組みの構築をテーマとした。

2. 研究の進め方

当分科会では以下の手順で研究を行った。

(1)トライアル

IT 全般統制とは何かを実感するために、米国での基準である「COBITforSOX」で IT 全般統制の RCM(リスクコントロールマトリクス)を擬似的に作成し、課題・問題点を抽出、共通認識する。その際には、既存の様々な“IT に係るマネジメントシステム”も参照する。

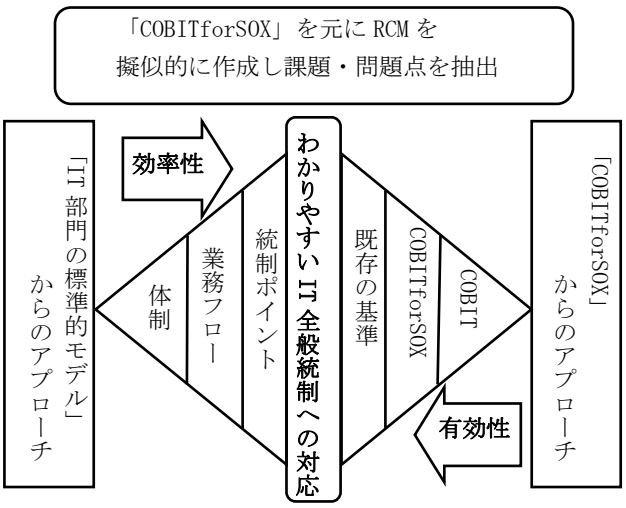
(2)わかりやすい IT 全般統制への対応

効率性および有効性から検証する。

・「IT 部門の標準的モデル」からアプローチすることで、既存の統制活動の仕組みを検証する。（効率性）

・「COBITforSOX」からアプローチすることで、IT 全般統制要件の網羅性を検証する。(有効性)

図表 1-1　アプローチのイメージ



3.研究内容・成果

(1) トライアル

「COBITforSOX」の分類は、日本で馴染みが薄く容易には理解できなかった。そのため当分科会では以下の理由によりシステム管理基準を中心に研究を進めることにした。

・企業の業種に影響されない（汎用性が高い）基準である。

・企画、開発、運用、保守という日本企業が慣れ親しんでいる区分で記載されている。

・入手が容易で広く公開・参照されている。

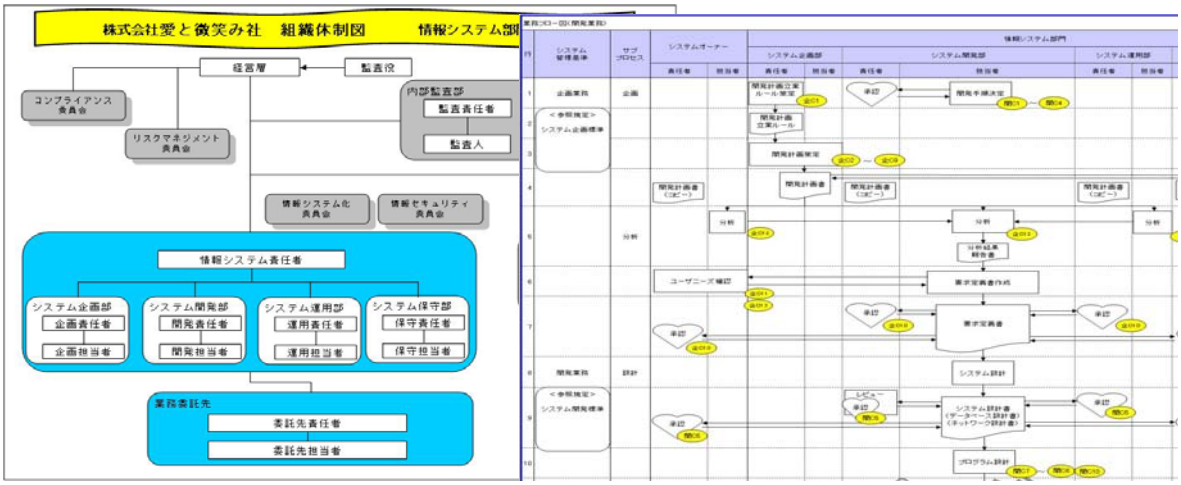
次に RCM 作成にあたり、リスクはコントロール（統制）の裏返しの表現になるので、統制項目のみ記載したコントロール集で十分との結論を出した。

(2)「IT 部門の標準的モデル」からのアプローチ

IT 部門は既に何らかの統制活動があり、それは現在のシステムライフサイクル（企画～開発～運用～保守）の中に組み込まれている。そこで IT 部門の標準的なモデルとして組織体制図、職務分掌、関連組織、関連規程、業務フロー（企画、開発、運用、保守など）を作成し、その業務フローにシステム管理基準のコントロールをマッピングした。その過程でシステム管理基準を利用してコントロール集を作成する場合、特にセキュリティ面で統制項目が不足するが、情報セキュリティ管理基準で補う

だけで効率的に IT 全般統制への対応が可能であることを確認した。

図表 1-2　体制図および業務フロー



(3)「COBITforSOX」からのアプローチ

「COBITforSOX」の統制例のわかりづらさを解消するために、既存のマネジメントシステムが充当できる場合はその表現をもってコントロールとした。充当できない場合はわかりやすい表現をコントロール集に追加した。その結果、システム管理基準と情報セキュリティ管理基準の項目で、IT 全般統制要件のおよそ 9 割の網羅性を確認でき、有効であると判断した。

図表 1-3　コントロール集の抜粋

COBIT for SOX の統制の例	COBITforSOX の統制の例が要求している成熟度	実施すべき内容	実施すべき内容が必須か？○:必須 △:二次的		実施すべき内容の成熟度	実施すべき内容の引用元	引用元の項番
Ⅱ．2．アプリケーションソフトウェアの調達と開発		統制目標－財務報告の要件を効果的にサポートするアプリケーションおよびシステ					
組織のシステム開発ライフサイクル方法論(SDLC)は、セキュリティ、可用性、および処理の万全性(インテグリティ)といった組織の要件を含む。 (第二版) 組織は、セキュリティ、および処理のインテグリティといった組織の要件を含むシステム開発ライフサイクル方法論(SDLC)を有する。	3	開発担当者は、データのインテグリティを確保すること。 開発方針、システム設計マニュアルに基づいてデ のインテグリティ確保の計をしていること。	○		4	システム管理基準	Ⅲ.2.(5)
		開発担当者は、情報シムの障害対策を考慮し計すること。 情報システムの可用性ベイラビリティ)目標を していること。					

図表 1-4「COBITforSOX」に対するカバー率

カバーしている基準	項目数	カバー率	
システム管理基準	140	73%	88%
情報セキュリティ管理基準	30		
その他既存基準	3		
分科会オリジナル	19		

4. 評価・提言

システム管理基準に一部のセキュリティ管理項目を追加すれば、十分に IT 全般統制への対応が可能であることを検証でき、結果的に効率性・有効性を持つコントロール集が完成した。この成果は、IT 部門が具体的にイメージできる「わかりやすい」IT 全般統制への対応の仕組みにつながる。ぜひその仕組みを推進するために、本コントロール集を活用して頂きたい。

多くの企業には情報システムの適正管理の仕組みは既に存在し、2007 年 2 月公開された実施基準では、内部統制対応の詳細は各企業の自主的判断に委ねられている。そこで本活動を通して得られた知見により、以下の「内部統制マネジメントモデル対応の三か条」を提唱したい。

＜内部統制マネジメントモデル対応の三か条＞

・米国 SOX 法対応を安易に模倣せず、自ら考えて内部統制マネジメントの仕組みを検討すること
・情勢に過剰反応せずに、既存の仕組みの有効性も考慮すること
・受身的に対応せず、自らの仕組みで「不正と誤謬の低減の確保」および「IT の業務の有効性を確保している」ことを主張すること。

最後に、内部統制の整備を IT ガバナンス強化の機会と捉え、積極的に取り組んでいただきたい。