第 129 回月例研究会報告

報告者 No.966　斎藤　淳

日　時：2007 年 6 月 19 日（火）18：30～20：30
場　所：総評会館
演　題：「米国 SOX 法対応の IT 内部監査の課題と対応」
講　師：NEC 株式会社　システム・サービス事業推進本部
　　統括マネジャー：　清水　美欧　氏

1. はじめに

多くの上場日本企業ではいわゆる J-SOX 対応プロジェクトが進行中である。J-SOX 対応では大きく業務処理統制と IT 統制の 2 つに分かれ、IT 統制の中の IT 全般統制（ITGC）のためのコントロールとして COBIT4、COBIT for SOX、システム管理基準、同追補版、FISC、ITIL、ISMS（ISO27001）、CMMI などが参考にされている。

講師の所属する NEC では J-SOX より先行して US-SOX 対応に取り組んでおり、今回はその主力メンバーとして活動された講師に、SOX 法 404 条対応内部監査の実施課題について、ITGC を中心としたマルチ・レギュレーションに対する考え方を交えながら、ご経験をご紹介いただいた。

2. 講演要旨

(1) 米国 SOX の最新トピックス

SEC（米国証券取引委員会）に年次報告を提出している日本企業は 26 社あり、開示した 6 社中 3 社に「重大な欠陥」が見つかったようである。NEC 自身も米国での追加的な監査手続きが遅れ、2006 年 3 月期の年次報告が未提出の状況である。日本では 2008 年度に内部統制ルールの導入が控えており、その対応に拍車がかかりそうである。

SEC の経営者評価指針（ガイダンス）が改定された。特徴的な点はフレキシビリティとスケーラビリティ（経営者の判断領域拡大）、コスト・ベネフィットの改善、アサーション方式の廃止、トップダウン・リスクベースドアプローチの提唱などである。

PCAOB 監査基準 5 号がリリースされた。これは PCAOB 監査基準 2 号を置き換えるものである。その内容は、監査人による「経営者評価プロセス」の評価を廃止、SEC ガイダンス案と用語を統一、トップダウンアプローチ、不正対策の強調、企業レベル統制、ウォークスルーの考え方、第三者の利用、監査のスケーリングなどである。

(2) SOX 法対応 IT 統制 内部監査の事例

講師の所属する NEC における US-SOX 対応活動を一例としてご紹介する。

NEC グループは 342 社、従業員 15.5 万人の規模であるが、スコープとしては連結決算売上高の約 80%をカバーし、要した工数は約 4,000 人月、作成したドキュメントは 9,000 枚以上となった。内部監査は監査部門の 54 名のスタッフが中心となって対応した。

対応作業は 2004 年から開始したが、外国企業に対する US-SOX 適用が 1 年延期となったため、トライアル、リハーサル、初年度本番と 3 段階となった。

リスク分析は実際に起こった（または発生が想定される）事故について、各部署にお願いしてリスク分析シートに記入してもらい、原因と対策をまとめていった。

ITGC では特に変更管理に着目して活動したが、IT 統制の内部監査の現状は総じて「職務分離」、「個人の特定」、「組織としての管理」が重要であり、本番プログラムの変更（特に緊急リリースのプロセス）とアプリケーション・ユーザ ID の管理が問題となることが多い。

編集・発行　NPO 法人 日本システム監査人協会　月例研究会・会報編集部
事務局　tel. 03-3666-6341　Fax.03-3666-6342　saajjk1 (at) titan.ocn.ne.jp

(3) SOX 法対応 IT 内部監査の課題

A. プロジェクト管理としての課題

プロジェクト管理としての課題としては 4 つ取り上げる。

1 つ目はプロジェクト体制に関するものであり、IT 統制のオーナが不在というケースが多かった。これに対しては RACI（Responsible、Accountable、Consult、Inform）表を利用して明確にした。

2 つ目はスコーピングの問題であり、監査対象の特定方法（予備調査が重要)、サブシステム／スプレッドシートの追及（統制が不在のアプリケーションの発見）を確実にすると、スコーピングから外れた無駄な作業を防止できる。

3 つ目は業務チームと IT チームのコミュニケーションの問題であり、文書化の粒度と品質や統制（マニュアル統制と自動化統制）の実装タイミングに差が出てしまう。これについてはステアリング・コミッティの役割が重要となる。

4 つ目は改善課題へのフォローアップに関する問題である。職務分離の改善要求に対しては現場の理解がなかなか得られず、業務委託先の内部統制評価については SAS70 のような仕組みを利用するにしても、統制項目、報告書をもらうタイミング、費用に課題が残る。

B. 技術的な課題

技術的な課題としては 2 つ取り上げる。

1 つ目は ITGC のアプローチと評価手法についてものであり、特にベンチマーク（チェックリスト）方式はコントロールが増加し、負担が増大する。マルチ・レギュレーションともなるとさらに増えてしまう。これを防止するにはリスクアプローチを徹底することが重要であり、現場で実施されていることを洗い出す必要がある。

2 つ目はマルチ・レギュレーションの問題である。以前より利用していた ISO/IEC9000、同 27001、ITIL、CMMI、PMBOK 等とどのように折り合っていくのかが課題となった。NEC では仕事柄部署ごとに得意なレギュレーションが存在し、マッピングしておくと話がしやすいという面がある。しかし、マッピング作業をしている最中にレギュレーションのバージョンアップが行われ、キャッチアップに工数がかかってしまう。マッピングは COBIT を核に作業をすすめるのが効率的である。

3. 所感

私も昨年から US-SOX 対応支援、今年 4 月以降は J-SOX 対応支援の仕事をしているが、US-SOX 対応プロジェクト立上から初年度本番まで通してのご経験は日本では大変貴重であり、深い関心を持ってその紹介を聴講させていただいた。ご紹介いただいた情報の中には、開示することが躊躇された内容のものもあり、配布資料にもご苦心の跡がうかがえた。

私の経験から US-SOX 対応ダイレクトレポーティングのための監査法人による監査において、その指摘事項から推測されるコントロールは COBIT ベースのもののようであるが、監査法人によって異なる部分が見られ、その他のスタンダードも参考にしているとも感じる。これに対応しようとするとコントロールが増加してしまい、必然的に運用テストの対象となるキーコントロールも増えるので、企業はその負担に喘ぐことになる。これを防止するにはリスクアプローチを徹底して、キーコントロールを絞り込むという講師の意見に全く同感である。

J-SOX 対応プロジェクトが本格化している日本企業で、その仕事に携われている方が多く参加されていたのではないかと想像するが、大変参考になるお話をお聞かせいただき、改めて深く感謝したい。

以上

編集・発行　NPO 法人 日本システム監査人協会　月例研究会・会報編集部
事務局　tel. 03-3666-6341　Fax.03-3666-6342　saajjk1 (at) titan.ocn.ne.jp