

埼玉学園大学・川口短期大学 機関リポジトリ

A Study on IT Internal Control : Practical Use of ISO27001 and ISO9001 as Frameworks

メタデータ	言語: jpn 出版者: 公開日: 2017-07-28 キーワード (Ja): キーワード (En): 作成者: 赤林, 隆仁 メールアドレス: 所属:
URL	https://saigaku.repo.nii.ac.jp/records/845

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 International License.



IT内部統制に関する考察

— ISO27001 ISO9001 の活用 —

A Study on IT Internal Control

— Practical Use of ISO27001 and ISO9001 as Frameworks —

赤 林 隆 仁

AKABAYASHI, Takahito

日本の上場企業はIT化が進展しており、内部統制においてもITを前提としたものが要求される。そのための安価で適用し易いフレームワークとして多くの企業で経験のあるISO 27001（情報セキュリティシステム）、ISO 9001（品質システム）を活用できないかを検討した。その結果この2つを併用するとITを前提とする内部統制の要求事項を網羅できることが判明した。内部統制を意識して2つの基準を適用すれば内部統制に係わる費用の削減につながる事が推測された。

はじめに

企業における一般的な「内部統制」とはリスクマネジメントに基づく全体的な統制活動、監視活動を示すが、2008年4月より施行される金融商品取引法第24条4-4（この部分を「日本版SOX法」と通称する）ではこれを「財務報告類の適正性を確保するために必要なもの」と規定し事業年度毎に体制を評価した「内部統制報告書」としてとりまとめ、公認会計士または監査法人の監査を受けることを義務づけている。法律自体にはITに関する言及はないが、上場企業ではITによる財務会計システムが広く用いられているため、法律で要求される「内部統制報告書」の作成に関しても、ITを前提とした仕組みが必須であると考えられる。

このようなITを前提とする「内部統制」を確立する方法論として一般的には米国COSOフレームワークに基づくCOBITの適用が理想的とされているが、米国における実績では企業に対する費用・人的負荷が非常に大きいことが問題とされている。一方日本企業ではISO 9001品質システム、ISO 27001情報セキュリティシステムの取得件数が米国と比較して多い（例えばISO 9001の場合世界標準機構の発表では2005年末で日本の認証取得件数は53,771件で米国の44,270件を上回っている、またISO 27001の認証取得件数は2007年11月で2,399件で、世界の6割を日本企業が占めている）という特徴がある。本論文では多くの企業でノウハウの活用が期待できるISO 27001及びISO9001のフレームワークがITを前提とした「内部統制」に適用できないかに

キーワード：内部統制、リスクマネジメント、ISO 9001、ISO 27001、日本版SOX法、COBIT
Key words : internal control, risk management, ISO9001, ISO27001, J-SOX Act

ついて考察した。なお本論文における「内部統制」とは前述の通り「日本版SOX法」でいう「財務会計プロセス」を対象としたものを言う。

1. 「日本版SOX法」と「ITへの対応」

「日本版SOX法」の考え方自体は米国の「SOX法」(Sarbanes-Oxley Act) にほぼ準拠しており、その基礎をCOSOフレームワーク(The Committee of Sponsoring Organization of the Tredway Commission) に置いている。COSOフレームワークでは内部統制の基本的要素として、「統制環境」、「リスクの評価と対応」、「統制活動」、「情報と伝達」、「モニタリング」の5要素が定義されている。「日本版SOX法」の実施に当たっては独自の要素としてCOSOフレームワークに加えて「ITへの対応」が2007年2月の「財務報告に係わる内部統制の評価及び監査に関する実施基準」(企業会計審議会)の中で加えられている。

この中では、「ITへの対応」について「ITに大きく依存している場合や組織の情報システムがITを高度に取り入れている場合には、内部統制の目的を達成するために不可欠の要素そして内部統制の有効性に係わる判断の基準となる」として、他の5つの基本要素(統制環境、リスクの評価と対応、統制活動、情報と伝達、モニタリング)の有効性確保のためにITを利用すべきとしている。またITシステムに関しても統制を要求し、その目標として、情報資産に求められる信頼性、可用性、機密性に加えて有効性・効率性、準拠性(法令・基準・規則に合致して処理されること)を要求している。また具体的統制内容として「全般統制」(業務処理が有効に機能する環境を保証する)、「業務処理統制」(業務が正確に処

理・記録されることを確保する)とその両者の経営者による評価を要求している。

2. 上場企業における財務会計システム IT化の現状

2006年にノークリサーチ社が日本の中小企業を対象に調査した結果では、「財務会計システム」は企業に導入されている業務システムの第一位を占め、導入率は74.5%となっている。これは中小企業を対象とした値であるため、「日本版SOX法」の対象となる上場企業についてはほぼ100%に近い導入率と推測される。経済産業省の「企業のICTネットワーク利用状況調査(2006年)」によれば財務会計システムの内訳はパッケージソフトをそのまま利用している率が32.9%、カスタマイズして利用している率が33.6%、専用システムを構築している率が28.6%と全企業ではほぼ1/3づつの比率であるが、上場企業に関しては専用システムの率が更に高くなると推測される。

また2006年に経済産業省が実施した「勤労者ICT利用調査」によると企業の従業員の内、業務専用会計ソフト・データベースソフトによるデータ管理に従事している率が34.6%、表計算によるデータ管理・分析業務に従事している率が77.1%で全従業員の1/3以上が財務会計システムに何らかの関与をしている。

従って実際に「日本版SOX法」の対象となる上場企業は、上述の「財務報告に係わる内部統制の評価及び監査に関する実施基準」でいう「ITに大きく依存している場合」に該当するものと見なされITを前提とした内部統制プロセスが必須なものになると考えられる。

以下ではITを前提とした内部統制の要件について述べる。

3. ITを前提とした内部統制の要件

ITを前提とした内部統制の要件としては「**全社統制**」、「**全般統制**」、「**アプリケーション（業務処理）統制**」の3種類があり、これらは階層構造となっている。

「**全社統制**」は最上位の統制要素であり、ITによる内部統制の前提となる活動である。具体的には企業全体のITに関する方針・計画・手続を示し、企業全体としてITが正しく維持・管理されていることを保証するものである。

「**全般統制**」は「**全社統制**」の下位に位置する概念であり、以下に述べる概念である「**アプリケーション統制**」を有効に機能させる環境を保証提供する活動である。具体的には財務会計システムの開発・保守・運用に係わる管理活動が正しく行われている事を保証する。

「**アプリケーション統制**」は実際のIT業務において、業務（ITアプリケーション）が決められた手順通りに正確に処理され、記録されることを確保するための統制活動であり、財務会計システムにおける正しい入力、正しい処理、正しい出力を保証する活動である。

以下に各要件の詳細とそれを保証するための要求事項について記述する。

4. 全社統制

前述のように、ITを前提とした内部統制プロセスの存在のためには、ITの利用に関して全社にわたり統制が行われていることが条件となる。その事を具体的に示すために内部統制の基本5要素（統制環境、リスクの評価と対応、統制活動、情報と伝達、モニタリング）の各々についてITの役割が定義されている必要がある。これを整理記述すると以下の通りとなる。このうち（1）、（2）は基本的に行

われていなければならない要素であり、（3）、（4）、（5）は利用することで有効性を高める補完的要素である。

（1）統制環境

経営者がIT利用を理解、認識して、IT利用の基本方針を明確にし、それを従業員に周知・教育している。事業活動に必要な権限・職責に応じてITシステムの制御（アクセス権限、ワークフローなど）が可能のようにしている。

（2）リスク評価と対応

ITの持つ脆弱性に関してリスク（入力ミス、故意の改ざんなど）の洗い出し、分析、評価が行われ、それに基づく対応策が正しく検討されている。すなわちIT利用についてのリスクマネジメントが正しく行われている。またリスクの発見、分析、情報の共有にもITを利用することにより効率性を高めている。

（3）統制活動

ITを内部統制機能（承認、検証、記録等の手続き）の中に組み込んで、統制の効率性・有効性を高める手段として活用している。これはIT自体が業務の効率性・有効性を高める手段であるため、「統制活動」という業務にも適用するという考え方であり、プロセス内における入力データの抜け、誤り、見落とし等の防止に大きな効果を発揮する。

（4）情報と伝達

経営者の方針を社内外の関係者に伝達・共有する手段としてweb、電子メール、共有ファイル、グループウェア等のITを活用することで、浸透性、敏速性を高めている。業務システムのアウトプットをこれらとうまく連動さ

せている。

（５）モニタリング

経営者が内部統制の有効性（適正に実施されているか）を確認・評価する場合に、ITを利用して業務システム内に監視プロセスを組み込み、即時的、定量的に把握を行い、モニタリングの精度と効率を高めている。また管理限界値（在庫量、入金期日等）を超えた場合に警告を自動的に発することにより迅速な問題発見が可能となるようにしている。

内部統制上の評価ポイントとしては次の諸点がある。

- ・経営者がITで内部統制を行う方針を有している。
- ・財務情報システムの信頼性についてリスク分析に基づき評価・対応を行っている。
- ・経営者が財務情報システムに関するITへの経営資源（人員、設備、予算）の配分・承認を行っている。
- ・財務情報システムに関する「情報と伝達」、「モニタリング」の仕組みがあり、リスクマネジメントのサイクル（PDCA）が確立されている。
- ・財務情報システムに関する管理・統制の記録を採取・保存する仕組みが確立している。

5. 全般統制

財務情報システムが適正に開発・運用・保守・管理されているかを統制する活動である。内容としては次の4種類の管理についての評価が必要となる。

①開発・保守

- ・ソフトウェアの開発、パッケージやツ

ル等の調達、保守、運用の統制方法が整備され、その通りに運用されている。

- ・開発・保守したソフトウェアの信頼性試験が正しく行われて、結果が承認されている。
- ・効率性・正確性を保証するIT基盤が構築されている。
- ・開発・保守段階のすべてにおいてソフトウェア仕様の変更管理が適正に行われ、承認・記録されている。

②運用・管理

- ・ソフトウェアの運用方法が明確化されており、未承認、不正な処理が排除される仕組みがある。
- ・ソフトウェア、IT基盤のバージョン（構成）が正しく管理、記録されており、容易に識別できる。
- ・入出力されたデータが正確に保持・管理されている。

③システムの安全性

- ・情報セキュリティを経営者が一定の方針に基づき実施している。
- ・情報資産の不正使用や改ざん等を防止するために必要なアクセス管理等の対策が実施されている。
- ・財務情報システムに対する人的災害、自然災害を含むインシデントに対して、適切に対応し、業務が継続、復旧できる仕組みが整備され実行されている。

④外部委託契約の管理

- ・財務情報システムの構築や運用を外部委託する場合に、経営者が受託先の統制状況を把握し、自社の統制に与える影響を

評価して契約している。

- ・外部委託先との契約の際にセキュリティ等を含むサービスレベルについて定義・合意し、遵守されているかを管理している。

6. アプリケーション統制

「IT業務処理統制」とも言う。財務情報システムにおいて、承認された業務が正確に処理され、記録されている事を保証するための内部統制である。すなわち正しい入力データにより、正しい処理が行われ、正当な出力が得られているかを統制する。統制要素としては次の諸点がある。

①入力情報

- ・財務情報システムに入力されるデータの信頼性（完全性、正確性、正当性）の維持・統制（異常値、誤入力、恣意的操作のチェック、例外処理の設定等）がなされている。
- ・自動的にファイル等からデータを入力する場合は、前工程で適正に処理された最新のものかどうかを管理・確認している。
- ・入力データを作成するために前処理として表計算ソフト、データベース管理ソフト等を利用している場合には、その処理内容の正確性、転送時のデータの完全性について確認している。

②例外処理

- ・正しいアルゴリズムや手順（ワークフロー）で処理されていることが管理され、承認・記録されている。
- ・計算式やデータ、出力結果の正当性について敏速に判断できるように（異常値に

はアラームを出す等）管理統制されている。

- ・処理に異常があった場合でも正しく継続・復旧するためのプロセスが予め設定されている。
- ・誤りが発見された場合その時点まで戻って再処理する機能が実装されている。

③マスターデータの維持管理

- ・入出力されたデータが正しく維持され、改ざんされたり、欠落したりする事がない仕組みを作りそれが実証されている。

④システム利用の管理

- ・財務会計システムの利用（入力、処理、出力）が定められた権限の要員によってのみ行われ（データのアクセス権限の付与等）、利用時に認証が行われ操作した確認が記録されている。

パッケージソフトの場合は機能仕様や実績で上記の条件が証明されているものもあるが、これを修正（カスタマイズ）した場合、また独自にソフトウェアを制作（オーダーメイド）した場合にはこれらについて実証する必要がある。

7. COBIT

IT内部統制の評価基準としては米国情報システムコントロール協会（ISACA）によるCOBIT（Control Objectives for Information and related Technology）がある。COBITではIT活動を4つのドメイン（計画と組織、取得とインプリメント、供給とサポート、モニタと評価）と34のITプロセスに分解し、各プロセス毎に主要成功要因（CSF：critical

success factors)、主要目標達成指標 (KGI : key goal indicator)、重要業績評価指標 (KPI: key performance indicator) を7段階 (レベル0 : 存在しない～レベル6 : 最適化されている) の成熟度レベルで示す。この評価の結果がすべての項目についてレベル3 (定義済) 以上であり、更に改善するように管理していることで日本版SOX法の要求水準と判断する。レベル3の内容は「手順は標準化され、文書化され、教育・周知・伝達されている。定義されたプロセスに従うかどうかは個々の人員に任されており、定義プロセス違反が発見しにくい。手順は既存プロセスの公式化に留まる。」である。

これを厳密に適用すると1プロセス当たりのチェック数は136項目となる。財務会計システムに含まれるプロセス数は10-40程度であり、また大企業の場合には事業所の数の分だけこれを実施する必要があるためチェック数の合計は規模の大きな企業では数万項目にのぼる場合さえある。各チェック項目について未達成な場合やリスクが存在する場合には対策を施し、それを文書化することが求められる。米国での調査 (Sarbanes-Oxley Section 404-Costs and Implementation Issues: Survey Update, CRA International 2005/12) によれば全米の企業で社内監査で実際に精査された項目数の平均は992項目、実際に監査された項目数の平均は669項目であった。COBITは網羅性の高い反面これを適用するためには非常に多くの工数を要することがわかる。

8. 内部統制に係わる費用

米国企業では内部統制の整備のために、通常は専門の「内部統制チーム」を編成して財

務会計プロセスに関連する社内部署に関してCOBITに従った調査を行い、手順の徹底的な文書化と、成熟度の改善施策を実行した。調査 (Sarbanes-Oxley Section 404-Costs and Implementation Issues: Survey Update, CRA International 2005/04) によれば、初年度に内部統制にかかった費用は監査コストも含めて大企業1社当たり851万ドル (約10億円)、中企業で124万ドル (約1.4億円)、更に次年度の維持に大企業で477万ドル (約6億円)、中企業で86万ドル (1億円) となっている。

COBITをフレームワークとしたチェック数が多いだけ分析、対策策定、文書化の工数が増大するため、専任人材だけでは不足で、外部にアウトソーシングする必要性が生じ、更にアウトソーシング先でも同様の内部統制が必要になることで費用が増大する構造となっている。

IDC Japanが2006年3月に上場企業100社を対象に調査した結果 (2006年4月26日発表) では、米国と同様の方法を前提とした場合2008年度における日本版SOX対応のIT必要投資額は総額2,607億円で、1社当たり平均は2.6億円となる。

このようにIT内部統制にかかる費用と手間は膨大なものとなり、企業活動に大きな負担となる懸念がある。内部統制はリスクマネジメントの上からも重要な要素であり、法律で定められているため上場企業ではこれを実施する義務があるが、実施に当たった費用対効果については当然考慮・吟味する必要がある。

9. ISO27001とIT内部統制

ISO 27001は情報資産を対象としたセキュリティマネジメントシステム (ISMS: Information

Security Management System) の国際規格であり、2006年の認定開始以来導入する企業が相次ぎ、2007年6月1日現在では認定事業者数は2,191件（日本情報処理開発協会調べ）に達している。

米国情報システムコントロール協会 (ISACA) の「E&Y ISACA Sarbanes Conference」(2004年6月) でKey Vander Wallが報告したところによると、IT内部統制で指摘される問題点の上位10項目の内、7項目が情報セキュリティに関する項目であった。この事からISO 27001を財務情報システム及びそれに関連するシステムを適用する事で、内部統制で要求される諸要件の内実績で7割を占めるセキュリティに関する部分をカバーできると考えられる。ISO 27001では基本的に情報の可用性・機密性・完全性の追求を目的としているが、完全性の定義の中に信頼性や準拠性の要素を加味する事で内部統制のフレームワークとして活用できると考えられる。以下に具体的にISO 27001のどの部分が内部統制のどこに適用可能かを検討する。ISO 27001は「0. 序文」～「8. ISMSの改善」の9章からなる（順守しなければいけない）規格部分と、附属書A「管理目的及び管理表」から構成され、附属書Aに基づいて「適用宣言書」に各項目についての採否とその理由、管理策の詳細を記述が要求される。また各規格に基づく証拠（エビデンス）が文書やファイル等の形で要求される。以下で付番がAの項目は「附属書A」に規定される管理目的及び管理策を示す。

①全社統制

(1) 統制環境

「5. 経営陣の責任」に該当する。

A. 5 セキュリティ基本方針：内部統制

の目的とその具体的内容。

A. 6 情報セキュリティのための組織：関連する内外部の組織とその責任。

A. 8 人的資源のセキュリティ：従業員に対する責任・管理策。

(2) リスク評価と対応

「4. 情報セキュリティマネジメントシステム」の「4.2.1 ISMSの確立」が該当する。規格に基づいて行ったリスクアセスメントの結果、リスク対応が必要と判断した対応策を明示する必要がある。

(3) 統制活動

「4.2.2 ISMSの導入及び運用」が該当する。

(4) 情報と伝達

A. 10.8 情報の交換：情報交換・伝達の手順、方法、管理方法。

(5) モニタリング

「4.2.4 ISMSの維持及び改善」、「6. ISMS内部監査」、「7. ISMSのマネジメントレビュー」、「8. ISMSの改善」が該当する。

A. 6.1.8 情報セキュリティの独立したレビュー：維持改善のために行うレビューの詳細な仕組み。

②全般統制

(1) 開発保守

A. 10.2 第三者が提供するサービスの管理：購買ソフト等のセキュリティの管理策。

A. 10.3 システムの計画作成及び受入れ：故障防止の対策。

A. 12 情報システムの取得、開発及び保守：開発保守に関する全般統制が確実性に行われていることの根拠。

(2) 運用・管理

A. 7 資産の管理：財務会計システム関

連の情報資産を定義。

- A. 9 物理的及び環境的セキュリティ：財務会計システム関連の情報資産の具体的な管理策。
 - A. 11.2 利用者アクセスの管理
 - A. 11.3 利用者の責任：財務管理システムに許可された者だけがアクセスを許され、それ以外のアクセスを防止する対策とその管理策。
 - A. 12.5 開発及びサポートプロセスにおけるセキュリティ：変更管理手順とその遵守、変更過程での情報漏洩の防止策。
- (3) システムの安全性
- A. 5 セキュリティ基本方針：経営者がセキュリティについて定めた方針。
 - A. 9 物理的及び環境的セキュリティ
 - A. 10 通信及び運用管理
 - A. 11 アクセス制御
 - A. 12.4 システムファイルのセキュリティ：ソフトウェアを含む財務会計システムの情報資産の保全対策の実施。
 - A. 13 情報セキュリティインシデントの管理
 - A. 14 事業継続管理：人的災害、自然災害等のインシデントの定義し、その対策、業務を復旧・継続する仕組み。
 - A. 15 順守：日本版SOX法を含めた法的要求事項、その他の項目の識別・順守。
- (4) 外部委託業務の管理
- A. 10.2 第三者が提供するサービスの管理：特に運営等を外部委託した場合の契約、管理、サービスレベル合意。
 - A. 12.5.5 外部委託によるソフトウェア開発：でシステム構築を外部委託した場合の契約、管理、サービスレベル合意。

③アプリケーション統制

- (1) 入力情報
- A. 12.2.1 入力データの妥当性確認
 - A. 12.2.2 内部処理の管理：入力データの信頼性を維持するための対策、方法、それらの機能のシステムへの実装。
- (2) 例外処理
- A. 12.2.3 メッセージの完全性：財務会計システムにおける業務ソフトウェアの真正性を証明するための要求事項とそれを保証するためのメッセージ、それらの実装方法。
 - A. 12.2.4 出力データの妥当性確認：財務会計システムから出力されたデータの正当性を維持、確認する手順、不正出力に対処する手順、実装方法。
- (3) マスターデータの維持管理
- A. 10.7 媒体の取扱：入出力されたデータの維持・管理方法、データ維持の過程での改ざん、漏えいを防ぐ仕組み。
- (4) システム利用の管理
- A. 10 通信及び運用管理：財務会計システムを含むシステム利用の管理、記録。
 - A. 11 アクセス制御：アクセス制御の詳細。
 - A. 12 情報システムの取得、開発及び保守：詳細なレベルの管理の実施。

④文書化

- 4.3.2 文書管理：ISMS上必要とされる文書の承認・更新・改変・保管手順、識別・配布・回収手順。
- 4.3.3 記録の管理：有効な運用を行っている証拠としての記録を文書として管理する。

10. ISO9001とIT内部統制

前述の米国情報システムコントロール協会 (ISACA) Ken Vander Wallの報告による問題点で残り3割を占める (情報セキュリティ以外の) 項目は1) 財務会計システムにおけるデータ入力期間、2) 手作業プロセスの手順がない、3) 実際のシステムとシステムの定義文書が異なる、の3点であった。1) はアプリケーション統制におけるデータの定義、2) は運用における手順の定義、3) はプログラムの変更管理の問題であり、業務プロセスの定義、業務内容の文書化、リスク対応表の作成を徹底的に要求されるが、これらは何れも財務会計システムのアウトプット (財務諸表) の「品質」に関するものである。そこで品質マネジメントシステムISO 9001を財務会計及びその関連システムに適用することで残りの問題点をカバーできないかを検討してみた。

ISO 9001は品質マネジメントの国際規格であり、当初は物理的な製造物に適用されていたが、日本では1993年以降IT (情報技術) を使用した製品及びサービス分野にも広く適用されるようになった。経済産業省産業技術経済局の統計では2005年3月現在で総登録件数は6万件を突破している。ISO 9001は「0.序文」～「8. 測定、分析及び改善」の9章から成り、それぞれの項目 (「5.4.1 品質目標」のように細目に分かれている) に記述された規格に対する適用対象、規格が満たされている事の証明 (エビデンス)、プロセスや規定の文書化が要求される。以下にISO 9001の要求事項と、それに対応する内部統制としての解釈ととるべきアクションについて考察する。

① 全社統制

ISO 9001には「3. 定義」があり、供給者と顧客の定義を要求される。財務会計システムに適用する場合には供給者が担当する組織、顧客が財務報告を利用するステークホルダ (株主等) となる。

ISO 9001における「5. 経営者の責任」は全社統制のほぼ全体に関連する。

- 5.1 経営者のコミットメント：IT利用の基本方針、従業員への周知・教育、等「統制環境」を構成する要素。
- 5.2 顧客重視：財務諸表の品質保持によるステークホルダの満足向上。
- 5.3 品質方針：財務諸表の性質として要求される信頼性、可用性、機密性、有効性、効率性、準拠性の諸点を品質要素とする。
- 5.4 計画：品質方針で述べられた諸要素の具体的目標とそれを達成する仕組みを明らかにする。「リスク評価と対応」の方針を計画の中に入れておく。
- 5.5 責任、権限およびコミュニケーション：「統制活動」における組織やその権限、「情報の伝達」手段やプロセス、特に「5.5.3 内部コミュニケーション」。
- 5.6 マネジメントレビュー：経営者による「モニタリング」のプロセス。

ISO 9001における「8. 測定、分析および改善」は「モニタリング」の全部分と「リスク評価と対応」の一部に関連する。

- 8.1 一般：財務会計システムの改善の仕組みと計画。
- 8.2 監視および測定：財務会計システム自体やそのアウトプットが要求事故を満たしているかの基準、監査。
- 8.3 不適合製品の管理：要求事項を満た

していないプロセスや結果を発見する方法と、その時の措置。

- 8.4 データの分析：どのようなデータ（証拠）を元に適切性や有効性の実証。
- 8.5 改善：継続的改善の仕組み、不適合事項に対する是正措置、「リスク評価と対応」の中で分析された予想される不適合に対する予防措置（対策）、それらの手順、記録。

②全般統制

「システムの安全性」以外の項目に関しては、ISO 9001における「7. 製品実現」の内7.1～7.5が該当する。

- 7.1 製品実現の計画：ここでいう製品を「財務会計システム」のアウトプットとして扱い、要求事項、目標、その合否判定基準等。
- 7.2 顧客関連のプロセス：財務諸表を利用するステークホルダを「顧客」して捉える。財務諸表の正確性を維持するための一般的事項や法令、規制によって定められた事項、外部監査に要求される事項の明確化、それらのレビューと記録。
- 7.3 設計・開発：開発段階での検証、妥当性確認、レビュー、変更管理の各項目のルール、実施記録、承認記録。
- 7.4 購買：外部から購買したソフトウェア（パッケージ、ツール等）、外部に委託した作業（ソフトウェア、要員等）が財務会計システムとしての要求に合致したものである事を証明する手順、実施記録、承認記録。
- 7.5 製造およびサービス提供：正しい財務諸表の提供を「サービスの提供」と

して捉える。「運用・管理」に関して、手順、その妥当性の確認方法、トレーサビリティの維持方法、維持管理の実施記録、承認記録。

③アプリケーション統制

- 7.2.1 製品に関連する要求事項の明確化：入力データのチェック機能、前処理としてのエンドユーザーコンピューティングに要求される機能、連動する他システムに要求される機能、例外処理で要求される機能の記述。

④文書化

内部統制では上記の統制活動に関する手順やルールの文書化が求められているが、これには「4.2 文書化に関する要求事項」が該当する。

- 4.2.1 一般：財務会計システムに関する方針、目標、品質、記録の文書化。
- 4.2.2 品質マニュアル：財務会計システムに要求される品質に関する記述文書（品質マニュアル）。
- 4.2.3 文書管理：文書の承認、レビュー、変更管理、識別管理の方法、手順。
- 4.2.4 記録の管理：各種活動の結果記録を識別・検索可能な状態で保管管理する方法、手順。

11. 結 論

ITを前提とした内部統制で必要とされる項目はISO 27001とISO 9001を財務会計及びその関連システムに対して適切に適用すれば網羅可能な事が検討の結果判明した。日本における上場企業の大半は内部統制の対象部分はIT化されている上に、社内の何れかの部門

でISO 27001やISO 9001を取得しており、それを維持管理する人材も有している。企業によってはこれら2つの規格を技術管理部門内等の同一の人材で行っている場合もある。

そこでISO 27001、ISO 9001の維持管理部門の人間や構築経験のある人間を中心に、財務会計システムとそれに関連するシステムに従事する部門のメンバーを加えたプロジェクトチームを編成して、両規格をフレームワークとした内部統制システムの整備を行う事により、COBIT準拠の専任体制を組んだ場合と比べて構築費用を削減できるものと予想される。対象システムの規模にもよるがISO 27001、ISO 9001の取得には当初から取り組んだ場合では社内対応工数を含めてそれぞれ3000~5000万円の費用が発生する。既に他部門で取得済の場合はこれよりも若干低くなるので、両基準を取得するための費用を合計してもCOBIT準拠の場合の平均予測費用2.6億円を下回ることが期待できる。

また更に以下のような定性的効果が期待できる。

- (1) 既に経験のある担当者が既知のフレームワークで取り組むため、基本的な検討部分の分析や対策の検討に要する時間を削減することができる。
- (2) 外部に依頼せず、関連部門を巻き込んだ活動を展開できるので、全員参加型のリスクマネジメントシステムを構築する事ができ、より実効的な対策が展開できる。
- (3) ISO規格ではPLAN→DO→CHECK→ACTIONのマネジメントサイクルによる継続的改善の仕組みを形成することが求められるので、運用して行くに従い効果が上がって行く事が期待できる

参考資料

1. 内山悟志／浅利浩一 日本版SOX法 IT統制実践法 2007年2月 ソフト・リサーチ・センター
2. システム管理基準 追補版(案) 2007年1月 経済産業省
3. 朝倉忠隆 情報技術分野のISO 9000 2001年5月 日科技連出版社
4. 情報技術－セキュリティ技術－情報セキュリティマネジメントの実践のための規範 2006年 日本規格協会
5. ISMSユーザーズガイド -JIS Q 27001:2006対応- 2006年12月 日本情報処理開発協会
6. Ken Vander Wall, National Quality Leader, E&Y ISACA Sarbnes Onference 2004/4/6