名古屋文理大学紀要　第6号（2006）

財務報告におけるＩＴ内部統制に関する基礎研究
－米国企業改革法とＣＯＢＩＴとの関係を中心に－

IT Internal Control on Financial Reporting:
The Relationship of Sarbanes-Oxley Act and COBIT

吉　田　　洋
Hiroshi YOSHIDA

米国企業改革法（SOX法）により，企業は今まで以上に内部統制プロセスを強化しなければならなくなった．本稿で取り上げる財務報告及びそれに付随する内部統制報告は，SOX法302条「財務報告に係る企業責任」により経営者は財務報告を適正に表示していること，内部統制の構築及び維持に責任を有していることを宣誓することが求められ，さらに同法404条「経営者による内部統制評価」において経営者によって行われた内部統制の評価について登録会計事務所は証明業務を実施し，報告しなければならないと規定されている．しかし，SOX法では企業活動の基盤となるITに関する内部統制について具体的に示されているわけではない．わが国の企業はこうした問題に対応するため，ITガバナンスに必要な情報システム統制に関してCOSO－ERMやCOBIT 3のフレームワークを取り込んだ現在のシステム管理基準に基づく内部統制を活用することが求められ，このことにより財務報告に伴うIT内部統制に関して，米国のSOX法に十分対応できる体制を作り上げることができると考えられる．

キーワード：　米国企業改革法，公開会社会計監視委員会，ＩＴ内部統制，ＣＯＢＩＴ，システム監査/管理基準
Sarbanes-Oxley Act,　Public Company Accounting Oversight Board（PCAOB），IT Internal Control，COBIT, System Audit / Management Standards

はじめに

2002年7月に制定された米国企業改革法（サーベンス・オクスレー法，以下SOX法とする）により，企業は今まで以上に内部統制プロセスを強化しなければならなくなった．

SOX法とは，2001年末のエンロン事件を契機に多発した不正な財務報告が社会問題化したことで，資本市場に対する米国内外の投資家からの信頼を回復するべく，それまで提起された会計監査およびガバナンスに関連する改革案を包括的に盛り込んだ法律である．本稿で取り上げる財務報告及びそれに付随する内部統制報告は，SOX法302条「財務報告に係る企業責任」において最高経営責任者（CEO）ないし最高財務責任者（CFO）が年次及び四半期報告書の財務報告を適正に表示していること，内部統制の構築及び維持に責任を有していることを宣誓することが求められており，

さらに同法404条「経営者による内部統制評価」において経営者によって行われた内部統制の評価について登録会計事務所は証明業務を実施し，報告しなければならないと規定されている．しかし，そこではIT（情報技術）に関する内部統制について具体的に示されているわけではない．

いうまでもなく今日の企業活動は，ITと密接に関連しており，業務を遂行する上でITを利用することは不可避である．内部統制を強化する場合，情報システム部門は最も重要な部門のひとつであろう．ITガバナンスと情報システム統制については，米国のCOSOフレームワークを基礎に情報システムコントロール協会（以下ISACAとする）からCOBIT第1版（1996年）が公表されている．現在のところISACAの関連団体であるITガバナンス協会が公表する第4版（2005年）が最新のものとなっている（注1）．COBITはITコントロールに焦点をあて，経営者，ユーザー，情報システム監査人を主な利用者としている．

本稿ではSOX法302条及び404条に関連してITガバナンスを確立するためにCOBITの概要及びITプロセスを中心にSOX法の関連性について検討し，さらに2004年に公表されたわが国のシステム監査基準及びシステム管理基準が財務報告のIT内部統制の評価にいかに貢献できるか検討してみたい．

1．企業改革法とIT内部統制

公開企業会計監視委員会（以下PCAOBとする）はSOX法101条によって創設されたものであり，次のような権限を有している．

①公開会社及び会計事務所からの資金拠出によって運営されているが，予算は証券取引委員会（SEC）が監督し，活動内容をSECに報告する義務を負っていることから，民間機関というより準公的機関と位置づけられる．

②従来，米国公認会計士協会（AICPA）が担ってきた監査基準等の基準設定権限を新たに担うことになった．

③SEC登録会社（公開会社）の監査を担当する会計事務所は，PCAOBに登録して，その監督下に置かれ，検査権限や懲戒権限も有する．

PCAOBにより上記の権限に基づいて，現在までに，3つの監査基準が策定・公表されている．

ITの内部統制に関してはPCAOBの監査基準2号（2004年3月9日公表）50条においてITの全般統制を構成する要素について，プログラム開発，プログラムの変更，コンピュータの運用，プログラムやデータのアクセスの4項目が例示されているのみである（PCAOB [2004]）．

財務報告とIT統制との関連について財務報告を行うためにはハードウェア，OS，データベースからなるITインフラがあり，その上に，各種財務アプリケーションシステム，ビジネスプロセス，財務報告といった順に階層化されていることを今一度確認しておく必要がある（IT Governance Institute [2004],p.37）．しかし，PCAOBはIT統制の重要性に触れながらも，その詳細については言及していない．その結果，ITコントロールのフレームワークを最も詳細に分析，記述したCOBITのフレームワークが詳細なIT統制の基礎になっている（IT Governance Institute[2004]p.7）．COBITとはControl Objectives for Information and Related Technologyの下線部の略でISACAの関連団体であるITガバナンス協会（以下ITGIとする）が公表している情報システムの統制目標を示したものである．米国おいてはITマネジメントに関してCOBITを参照する必要が生じる（Ramos[2004]p. 38）．したがってSOX法準拠のためのITコントロール目標についてはCOBITを出版しているITGIから，『SOX法のためのITコントロール目標』（IT Governance Institute [2004]）という資料が公表されており，同協会は経営者がそれに準拠することが望ましいとしている．

2．COBITとITガバナンス

COBITを公表しているISACAでは，ITガバナンスに関して次のように定義している．

「ITガバナンスは取締役会及び経営陣の責任である．それはコーポレートガバナンスの不可欠な部分で，リーダーシップ及び組織的な構造，及び組織のITがその組織の戦略及び目的を保持し拡張することを保証するプロセスから成る．」

したがって，ITガバナンスはコーポレートガバナンスの一部を構成し，COBITはITに関する経営の執行面からの統制，すなわちITのための内部統制のフレームワークを提供するために開発されたものである．COBIT第3版（以下，COBIT 3とする）ではＩＴプロセスを以下のように4つのドメインとその中を34項目に分類している（IT Governance Institute[2000]）．

ドメイン
①計画および組織化（PO）（11項目）
②取得および導入（AI）（６項目）
③提供および支援（DS）（13項目）
④監視（M）（４項目）

図表１，COBIT ３のドメインとプロセス

PO1	IT 戦略の立案
PO2	情報アークテクチャの立案
PO3	技術方針の立案
PO4	ＩＴ組織と相互関連の立案
PO5	ＩＴ投資管理
PO6	経営目標と経営方針の伝達
PO7	人的資源の管理
PO8	外的要因の遵守の保証
PO9	リスクの評価
PO10	プロジェクト管理
PO11	品質管理
AI1	自動化による問題解決領域の識別
AI2	業務ソフトウェアの取得および保守
AI3	技術基盤の取得および保守
AI4	手続の開発および保守
AI5	システムの導入および保証
AI6	変更管理
DS1	サービスレベルの決定
DS2	第三者サービスの管理
DS3	パフォーマンスとキャパシティの管理
DS4	継続的サービスの確保
DS5	システムセキュリティの確保
DS6	コストの識別および割当て
DS7	利用者の教育および訓練
DS8	カスタマーに対する支援および助言
DS9	構成管理
DS10	障害管理
DS11	データ管理
DS12	設備管理
DS13	運用管理
ＭＩ	プロセスの監視
Ｍ２	内部統制の妥当性の評価
Ｍ３	独立的保証
Ｍ４	独立監査の規定

すでに述べたようにPCAOBの監査基準２号（2004年３月９日公表）では，50条においてITの全般統制を構成する要素について，プログラム開発（以下PDとする），プログラムの変更（以下PCとする），コンピュータの運用（以下COとする），プログラムやデータのアクセス（以下APDとする）の４項目が例示されているのみである（PCAOB [2004]）が，COBIT項目との関係を示すと図表２のようになる．表の（ ）内の記号が関連するPCAOBの監査基準２号50条の例示である（IT Governance Institute [2004],p.8）．しかし，内部統制の本質と範囲は企業の業種，規模などから決まるものであるから，ITの全般統制においてもこの例示だけにとどまるものではない．これは最小限の例示であって，COBITに示された項目全体を視野に入れなければならないことはいうまでもないであろう．

図表２，COBIT と PCAOB 第２号50条の例示との関係

AI2	業務ソフトウェアの取得および保守（PD）（PC）（CO）（ADP）
AI3	技術基盤の取得および保守（PD）（PC）（CO）
AI4	手続の開発および保守（PD）（PC）（CO）（ADP）
AI5	システムの導入および保証（PD）（PC）（CO）（ADP）
AI6	変更管理（PC）（ADP）
DS1	サービスレベルの決定（PD）（PC）（CO）（ADP）
DS2	第三者サービスの管理（PD）（PC）（CO）（ADP）
DS5	システムセキュリティの確保（CO）（ADP）
DS9	構成管理（CO）（ADP）
DS10	障害管理（CO）
DS11	データ管理（CO）（ADP）
DS13	運用管理（CO）（ADP）

COBIT ３ではITガバナンスの重要性にかんがみ，成熟度モデル（Maturity Models），重要成功要因（Critical Success Factors：ＣＳＦｓ），主要目標指標（Key Goal Indicators：ＫＧＩｓ），主要業績評価指標（Key Performance Indicators：ＫＰＩｓ）が付け加えられた．その中で特に重要なものが図表３の成熟度モデルである．なぜなら，成熟度モデルによってITガバナンスの成熟度が測定できるからである．

３．システム監査基準・システム管理基準（2004年）

わが国のシステム監査基準・システム管理基準は財務報告に直接的に関連する基準ではない．しかし，す

図表３，成熟度モデル

レベル	種　類	説　明
0	未認識状態	組織として認識できるプロセスが必要なことすら認識されていない．標準のプロセスもない．
1	導入状態	組織としてプロセスの標準が必要なことは認識されているが，標準は確立されていない．個人やその場限りの対応で組織的な対応はない．
2	反復状態	同じ作業を行う異なった人間が同じ手続きを利用する状況にある．しかし，標準的な手続が公式に訓練，伝達されておらず，個人の責任となっている．個人の知識に頼る部分が多く，エラーも起こりやすい．
3	定義化状態	手続きが標準化，文書化され，訓練を通じて伝達がなされている．しかし標準プロセスに従うかは個人任せであり逸脱もありうる．手続自体洗練されておらず，既存のやり方を公式化したものにすぎない．
4	管理実施状態	手続きに従っているか監視し測定することが可能で，プロセスが有効でない場合は是正措置も可能である．プロセスの継続的な改善が実施されており，グッド・プラクティスが実施されている．自動化ツールの利用は部分的である．
5	最適化状態	継続的な改良と他の組織体の成熟度モデルの結果に基づき，プロセスはベストプラクティスの水準まで改良される．ITは自動化されたワークフローに組み込まれ組織がすばやく適応するための品質や有効性のツールとして利用される．

でに述べたように財務報告を行うためにはハードウェア，基本ソフトウェア構成，ネットワーク構成からなるITインフラがそのベースにある．つまりITインフラをいかに統制するか，すなわちIT統制が財務報告に与える影響が大きいことからシステム監査基準・システム管理基準の動向にも注意を払わなければならない．

最新のシステム監査基準では，「システム監査の目的は，組織体の情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを，独立かつ専門的な立場のシステム監査人が検証又は評価することによって，保証を与えあるいは助言を行い，もってITガバナンスの実現に寄与することである（システム監査基準，Ⅱ．システム監査の目的)」とされている．従来からの目的であった情報システムの信頼性，安全性，効率性の向上は後述するリスクに対するコントロールに統合され，保証・助言，ITガバナンスが今回の目的に加わった点であり，その目的は大きく変化している．

(1) 監査人の行為規範

システム監査基準は，システム監査業務の品質を確保し，有効かつ効率的に監査を実施することを目的とした監査人の行為規範である（システム監査基準，前文)。今回の改訂での大きな変更点は今まで著者が指摘したように，「監査人の行為規範」と「情報システム管理の基準」とを峻別したことである(吉田 [2002]p.138)．監査主体の行為規範を定めた基準として「システム監査基準」（一般基準，実施基準，報告基準）が公表され，効果的な情報システム戦略を立てるための実施規範を定めた基準，つまり，監査の際，監査人が行う判断の尺度として「システム管理基準」(情報戦略，企画業務，開発業務，運用業務，保守業務，共通業務）が公表された．システム監査の実施に当たっては，組織体における情報システムにまつわるリスクに対するコントロールの適否を判断するための尺度である（システム監査基準，前文）新たに設けられたシステム監査基準は，従来のシステム監査基準の内で，実施基準として監査対象業務ごとに挙げられていた191項目を287項目に拡張したものである．「システム管理基準」はISACAの関連団体であるITガバナンス協会が公表している前述したCOBIT 3と整合性をとっている(日本情報処理開発協会 [2004b]pp.506-521)．

(2)IT ガバナンス

従来の「システム監査基準」は情報システムのライフサイクル各段階におけるリスクが適切に管理されていたかを監査するための必要な事項を記していたが，今回の改訂ではITガバナンスの観点を考慮している．通産省（現経済産業省）の「ITガバナンススコアカード策定支援プロジェクト」(1998年）ではITガバナンスを次のように定義している．

「企業が競争優位性構築を目的に，IT（情報技術）戦略の策定・実行をコントロールし，あるべき方向に導く組織能力.」

すでに述べたようにISACAではITガバナンスを次のように定義している．

「ITガバナンスは取締役会及び経営陣の責任である.それはコーポレートガバナンスの不可欠な部分で，リーダーシップ及び組織的な構造，及び組織のITがその組織の経営戦略及び目的を保持し拡張することを保証するプロセスから成る.」

戦略を目的とした定義は，経済産業省，ISACAの定義にも見られるところである．

また，コンプライアンス・マネジメントからの定義は次の（社）日本監査役協会ITガバナンス委員会報告「ITガバナンスにおける監査役の役割」(2001年)の定義に見られる.

「主にIT化によって新たに生じるリスクの極小化と的確な投資判断に基づく経営効率の最大化，すなわち，リスク・マネジメントとパフォーマンスマネジメントであり，これらを実施するに当たっての，健全化確保のためのコンプライアンス・マネジメントの確立である.」

コンプライアンス・マネジメントは当然のこととして，組織の経営戦略とIT戦略を整合させ，IT投資を適切に管理し，IT要員やその体制，ITに関するリスクのコントロール等のフレームワークを確立するITガバナンスがきわめて重要になると考える.

(3) 技術革新に伴う新たなリスクへの対応

技術革新に伴う新たなリスクへの対応のための管理項目が追加されている．システム監査は，組織体の情報システムにまつわるリスクに対するコントロールが適切に整備・運用されていることを担保するための有効な手段となる．情報システムにまつわるリスクに対するコントロールを適切に整備・運用する目的として次のようなものを挙げている（システム監査基準，前文）

- 情報システムが，組織体の経営方針及び戦略目標の実現に貢献するため
- 情報システムが，組織体の目的を実現するように安全，有効かつ効率的に機能するため
- 情報システムが，内部及び外部に報告する情報の信頼性を保つように機能するため
- 情報システムが，関連法令，契約又は内部規程等に準拠するようにするため

これらの考え方の根底には，アメリカのトレッドウェイ委員会組織委員会による内部統制の定義すなわち，COSO報告書，COSO-ERM（全社的リスク管理のフレームワーク）のフレームワークを念頭においている．COSO-ERMによれば，リスク・マネジメントの目的を次のように挙げている.

① 戦略
② 業務
③ 報告（財務，非財務を含む）
④ コンプライアンスへの貢献

2004年のシステム監査基準，システム管理基準はこの流れに従って拡充がはかられている（注2）．従来の情報システムの信頼性，安全性，効率性の考え方を発展させながら変更していると考えられる.

むすび

情報システムや情報技術の方向が変わっている現在，ITガバナンスはコーポレートガバナンスの一部を構成し，組織の経営戦略とIT戦略を整合させリスクのコントロール等のフレームワークを確立することが重要になってくる．PCAOBはIT統制の重要性は認識しながらも僅か4つの例示をしただけで多くの言及はない．そこで、COBITによってIT統制のフレームワークを確立し，さらに，その成熟度モデルによって情報システム統制およびITガバナンスの成熟度の測定をはかることが期待されている.

翻ってわが国ではどうであろうか．情報システムや情報技術の方向が変わっている現在，わが国のシステム監査基準によるシステム監査は1985年以来の延長線上でよいか十分検討した結果が今日の姿となっているといえるだろう．現状ではそれぞれの目的に応じて，ITに関連する基準にはシステム監査基準・システム管理基準をはじめ様々な基準が存在している．取締役（会）の内部統制義務の履行という観点から考えればIT関連の内部統制フレームワークを整理・統合化する形で再構成を行い，それによって取締役（会）にとって理解が容易で利用しやすいITガバナンスと内部統制を確立することが望ましいことはいうまでもない．しかし当面はITガバナンスに必要な情報システム統制はCOSO－ERMやCOBIT 3のフレームワークを取り込んだ現在のシステム管理基準の内部統制で十分であると考える．この基準を活用することで財務報告に伴うIT内部統制に関しては，米国のSOX法に十分対応できる体制を作り上げることができると考えられる.

注

(注1) 現在，COBIT第4版(2005年)が公表されている．本稿は第4版公表前の2005年9月に執筆したものであるから第4版の内容は本稿に反映されていないことに注意されたい．COBIT第3版と第4版の相違についてはCOBIT第4版AppendixVのCross-reference（pp.181～188）を参照されたい.

(注2) COSO報告書，COSO-ERMのフレームワークについては以下のホームページを参照されたい.（http://www. coso. org/）

参考文献・引用文献

河合秀敏・盛田良久 [2003]：『21世紀の会計と監査』同文舘.

中央青山監査法人 [2004]：『ＣＯＳＯフレームワークによる内部統制の構築』東洋経済.

日本システム監査人協会（監修）[2004]:『システム監査情報セキュリティ監査ハンドブック』秀和システム.

日本情報処理開発協会 [2004a]:『新版　システム監査基準 / システム管理基準解説書（平成16年基準改訂版）システム監査基準解説書編』日本情報処理開発協会.

日本情報処理開発協会 [2004b]:『新版　システム監査基準 / システム管理基準解説書（平成16年基準改訂版）システム管理基準解説書編』日本情報処理開発協会.

日本情報処理開発協会 [2004c]:『新版　システム監査基準 / システム管理基準解説書（平成16年基準改訂版）関連資料編』日本情報処理開発協会.

吉田 洋 [2002]:『情報システム監査』税務経理協会.

IT Governance Institute [2000]:*COBIT-Governance, Control and Audit for Information and Related Technology,3rd ed.*, IT Governance Institute.

IT Governance Institute [2004]：IT Control Objectives for Sarbanes-Oxley,IT Governance Institute.

Greene, Fredric [2002]：“A Survey of Application Security in Current International Standards,” *Information Systems Control Journal*, Volume 6, pp. 47-51.

Hunton, James E.,Stephanie M. Bryant, Nancy A. Bagranoff [2003]:*Core Concepts of Information Technology Auditing*, John Wiley and Sons.

Moeller, Robert M. [2004],*Sarbanes Oxley and New Internal Auditing Rules*, John Wiley and Sons, Inc.

OECD[2002]: *Guidelines for the Security of Information Systems Networks Towards a Culture of Security*, OECD.

Pargak, Jagdish [2005]: *Information Technology Auditing An Evolving Agenda*, Springer.

PCAOB [2004]: *An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statement*, March 9, PCAOB.

Ramos, Michael[2004]: *How to Comply with Sarbanes-Oxley Section 404, Assessing the Effectiveness of Internal Control*, John Wiley and Sons, Inc.

Weber, Ron[1982]: *EDP Auditing Conceptual Foundations and Practice*, McGraw-Hill.

Weber, Ron[1999]: *Information Systems Control and Audit*, Prentice-Hall.