内部統制入門
～ XMLの視点で考える内部統制 ～

2006.08.31

株式会社 NTTデータ
梅田 伸明

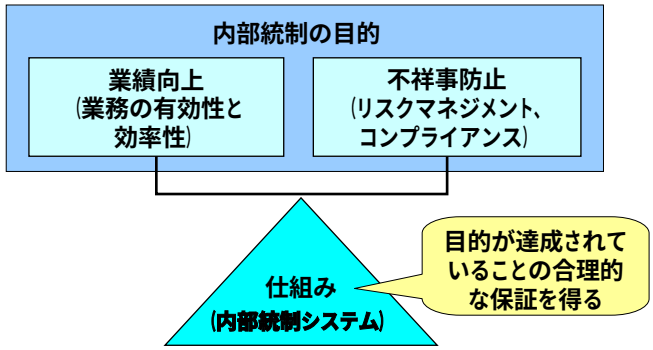
XML Consortium

(1) 内部統制とは？

Copyright©2006 NTT DATA Corporation

内部統制の目的

内部統制とは、企業がその業務を適正かつ効率的に遂行するために、組織内に構築され、組織内のすべての者によって遂行されるプロセスである



企業環境の変化

仕組みやプロセスが必ずしも明確化されていなくても、業務毎に関係者間で自主的取組や調整が行われることが期待されていた

従来の日本企業の状況

●高いモラル、終身雇用等を背景とし、経営者と従業員が高いレベルでの情報共有や意思疎通を図り、ボトムアップ方式、あるいはコンセンサス方式で意思決定を実施
- ✓経営者から明確な指示がない状況でも、従業員等が自律的に判断し、目的達成のために自主的に行動
- ✓職務及びその権限と責任の範囲が不明確／重複していても、当事者間の調整によって問題の多くは解消

株主、従業員、顧客、取引先等の多様なステークホルダーへの責務を適切に果たすことに対して、国内外の市場が迅速に評価を行うようになってきた

最近の状況

リスクマネジメント及び内部統制の構築と運用に失敗し、リスクの特定、評価や対応を怠った場合、広範なステークホルダーに損失を与え、市場の信頼を失い、企業自らも厳しいペナルティを受ける

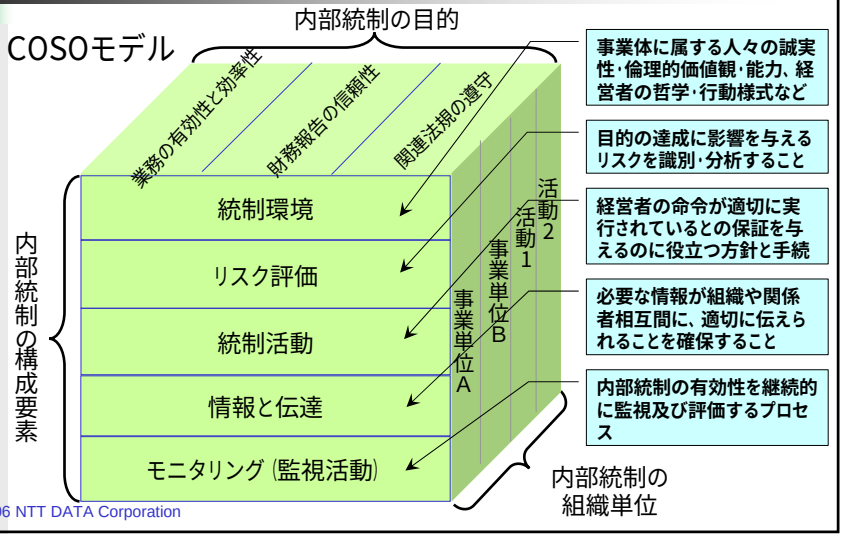
内部統制の必要性

- 内部統制は、市場経済社会における企業において、経営者が各ステークホルダー等に対する責務を果たしつつ、企業価値を維持・向上するために不可欠なものである
- 企業を取り巻くリスクが多様化し増大している中で、経営者は、強固なリスクマネジメント及び内部統制を構築・運用することにより、より適切で大胆な経営判断を行い、収益を上げていくことが可能となる
- 適切な内部統制が構築・運用されることにより、企業に対する顧客、投資家等の信頼感を高めることができ、これにより、企業価値をより向上させていくことが可能となる
- 強固なリスクマネジメント及び内部統制の構築・運用は、取締役会、監査役及び監査委員会が、経営者に対し適切なガバナンスを働かせるための前提ともなる

米国における内部統制の流れ

- 1970 年代：不安定な経済状況の中で、ウォーターゲート事件に代表される多くの企業の違法支出や粉飾決算等の不祥事が問題に
- 1985年6月：会計5 団体（米国公認会計士協会、米国会計学会、内部監査人協会、管理会計士協会及び財務担当経営者協会）が「不正な財務報告に関する全国委員会（通称トレッドウェイ委員会）」を組織し、検討を開始
- 1987年10月：トレッドウェイ委員会が報告書を公表「トップマネジメントは、不正な財務報告を防止又は摘発することの重要性を認識し、財務報告に関する総合的な統制環境を確立すること」が必要であることを指摘
- 1992年：トレッドウェイ委員会組織委員会（Committee of Sponsoring Organizations of the TreadwayCommission）が、「内部統制の包括的フレームワーク」（通称COSO レポート）を公表
- COSO レポートの考え方は、BIS（国際決済銀行）ガイドライン、米国・日本の監査基準等でも参照され、現在、内部統制のあり方に関して、世界のデファクトスタンダードと見なされている。

内部統制のためのフレームワーク



内部統制ができていない例

法令遵守を含む行動規範等が確立されていない、あるいは、行動規範が存在したとしても、経営者自らによる率先垂範と従業員への周知徹底が不足している。

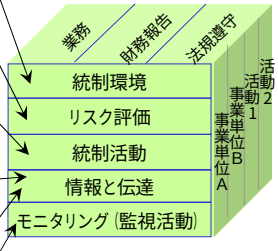
企業価値に影響を与える広範なリスクを特定できていない、あるいは、リスクを認識しても、それに対応するための仕組みを社内に構築できていない。

職務権限に関し、範囲が明確でない、あるいは、適切な牽制が機能していない。このため、特定の従業員が広範な権限や裁量を有している。

通常の業務上の経路以外の情報伝達ルートが存在せず、問題意識を経営者まで伝えることができない。本来、社内で自浄作用を働かせるべき行為が、社外への告発というかたちで、初めて対処・是正される。

事故等が発生した場合の社内及び社外への情報伝達経路が確立していない。

必要な専門性を有し、通常の業務執行部門から独立した内部監査機能が存在しない、あるいは、体制の不備や能力不足、内部監査の重要性への認識の低さ等から、その機能が十分に発揮されていない。



米国SOX法の直接の契機

- エンロン事件
  - 1985年に設立された米国最大のエネルギー会社
  - 1990年代には利益の急増に伴って、株価を急上昇させ、経済雑誌や証券アナリストから優良企業として絶賛されていた。
  - 2001年半ば頃から急速に業績を悪化させ、同年12月2日には、チャプター11（米連邦破産法11条）を適用し破綻。
  - 米国最大級の会計事務所アーサーアンダーセンと共謀の上、簿外で巨額の負債隠しを行っていたという不正会計事件であった。
- その他の事件
  - 2002年7月には通信大手のワールドコムが破綻。同社もそれ以前は低価格の通信料金で業界をリードし、エンロンと同様に、優良企業ともてはやされていたが、実際には経費を資産勘定に入れ込んでコストを安く見せかけるという手法で好業績に見せかけてきたものである。
  - 2002年はこの他にもグローバルクロッシング、アデルフィアコミュニケーションズ、タイコインターナショナルなどの破綻が相次いだが、いずれも経営陣主導による不正会計処理を伴うものであった。

米国SOX法とは？

- 正式名称は、Public Company Accounting Reform and Investor Protection Act of 2002
  「上場企業会計改革および投資家保護法」
  - 法案提出議員の名にちなんで、サーベンス・オクスリー法と呼ばれる（法の趣旨から「企業改革法」とも呼ばれる）
  - エンロン事件（2001年12月）など、一連の企業スキャンダルを受けて、2002年7月制定
- 立法目的
  - 会計制度の見直し
  - 監査人の独立性強化とその行動規範の厳格化
  - 経営者のアカウンタビリティとコーポレートガバナンスの向上
- 株式時価総額が7500万ドルを超え、SECに年次報告書を提出している米国企業に限定して開始

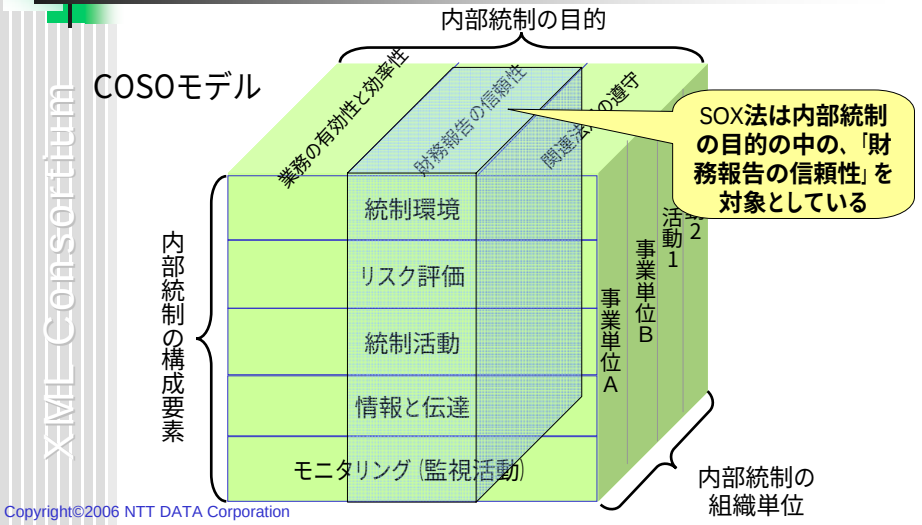
米国SOX法の構成

- 第1章（第101～109条）：公開会社会計監視委員会ーPCAOB
- 第2章（第201～209条）：監査人の独立性
- 第3章（第301～308条）：会社の責任
- 第4章（第401～409条）：財務情報ディスクロージャーの強化
- 第5章（第501条）：証券アナリストの利益相反
- 第6章（第601～604条）：証券取引委員会の財源と権限
- 第7章（第701～705条）：調査および報告
- 第8章（第801～807条）：企業不正および刑事的不正行為説明責任
- 第9章（第901～906条）：ホワイトカラー犯罪に対する罰則強化
- 第10章（第1001条）：法人税申告書
- 第11章（第1101～1107条）：企業不正および説明責任

米国SOX法の主要条文

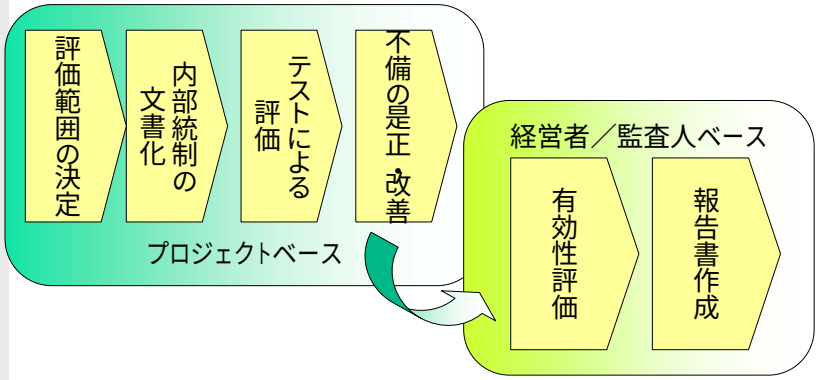
- 302条
  - 四半期報告書・年次報告書における財務諸表の適正性と、内部統制の構築と維持に関する経営者の宣誓
- 404条
  - 年次報告書における内部統制報告書の開示
    - 経営者は内部統制の構築・維持に関する責任を負う
    - 事業年度末における内部統制の有効性に関する評価実施を義務付け
    - 外部監査人に対しては、経営者評価を客観的に検証し、別途報告書を提出することを義務付け（ダイレクト・レポーティング）
- 906条
  - 罰則規定
    - 故意・過失にかかわらず、財務報告の内容に違反があった場合には、100万ドル以下の罰金または10年以下の懲役（もしくはその両方）
    - 虚偽報告と知っていて故意に署名した場合は500万ドル以下の罰金または20年以下の懲役（もしくはその両方）

SOX法の対象範囲



財務報告の内部統制報告の流れ

- 以下のサイクルを継続的に実施する
- 一般的には、業務プロセスおよび内部統制の整備状況を文書化して、内部統制の有効性を評価、不備の是正・改善につなぐもの



文書化の作業に負荷がかかる

- 文書化に先立って決めるべきもの
  - 重要な勘定科目
  - 対象とする組織、業務プロセス
  - 推進体制の整備、スケジュールの策定
- 「文書化」の対象になるもの
  - 業務記述書
    - 個々の業務における作業内容や手順を記述した文書。管理方針や職務分掌なども含まれる
  - 業務フローチャート
    - 業務の流れをフローチャートの形式で記述した文書
  - リスク・コントロール・マトリクス（RCM）
    - 業務プロセスのどこにリスクがあり、それをどのようにコントロール（統制）しているのかを記述した文書
- 評価対象は、連結ベース
- 委託先のプロセスも評価対象となる

内部統制が有効であるとは

- 「財務報告に係る内部統制」が有効であるとは、内部統制に「重大な欠陥」がないことを意味する。
- 302条で「重大な欠陥」があれば報告することが規定されており、違反した場合は906条の罰則が適用される。
- 1年目は16%、2年目は7%の企業が内部統制の重大な欠陥を報告
- 重大な欠陥の例（2005年5月の企業報告内容）
  - 有識者がおらず、適正な処理が行われていない
  - 担当者が、取引の入力から承認まで一人で完了できる状態にあった
  - 一般ユーザーに権限を変更するための権限が与えられていた
  - ユーザーID、パスワードが共有されていた
  - 改ざんに対するセキュリティ対策が不十分であった
  - 自社の未払い金や、顧客への請求が管理できていない

米国SOX法対応状況（1）

- SOX1年目を終了して
  - 多くの企業が準備不足で、「取りあえず」の対応に終わる
    - 「財務報告の内部統制」対応に膨大な稼動と多額の費用
  - 実施の範囲について明確な基準がなくプレイヤーによって意見が食い違う
  - 経営者向けガイドがなく、PCAOBの監査基準第2号（AS2）が唯一の拠り所
  - 一般的に明確なガイダンスが無い中で、監査人は監督当局の対応を怖れて専門職的判断をせず、便益の乏しい詳細なコントロール活動の検証に入り込んでしまう
  - 経理部門に比べて、IT部門での対応遅れ
    - SOX法は財務の話でありITとは関係がないと思っていた経営者が多かった
    - 現実には、ITの活用は不可欠でプロセス、モニタリング等、自動化しないと厳しい
    - 会計・監査ツールのみではなく、総合的な対応が必要
  - 内部統制は組織全体の課題という認識（IT部門、経理部門）
    - 人間・組織・企業文化の維持、継続的な取り組み、継続的な教育と訓練
  - コスト削減の要請を背景にプロジェクトからプロセスへ
    - 法令遵守支援のための内部統制の自動化

米国SOX法対応状況（2）

- SOX2年目を終了して　～今後の動向
  - 適用初年度に問題となった膨大なコスト負担は、企業や監査人が経験を積むことにより多少低下したが、期待したほどではなかった。
    - Financial Executive Internationalの調査では平均16%の低下で、期待値の約半分
  - コストダウンには、トップダウン型リスクアプローチの適用による、評価対象の絞込みが不可欠
    - 2005年5月にトップダウン・リスクアプローチのガイドライン提示→　監査人の監査基準に反映されていなかったため機能せず
    - SECは経営陣向けのトップダウン・リスクアプローチによる財務報告に係る内部統制評価の実施のためのガイドラインを提示する予定
    - 監査基準も改定予定→高リスク領域へのフォーカスを目指す

日本版SOXとは?

- 金融商品取引法
  - 平成18年6月7日　第164国会で法案可決、成立
  - 財務情報のディスクロージャーは金融庁「財務報告に係る内部統制の評価及び監査の基準のあり方について」がベース
  - 実施基準を金融庁の企業会計審議会内部統制部会が策定中
- 「日本版SOX」を考えるには、米国SOXだけでなく、会社法を意識した内部統制であることが重要
- 会社法における「内部統制に関する義務」
  - H14改正：委員会等設置会社に
  - H17改正：大会社に拡大＝内部統制整備に関する事項を取締役会決議事項に
- 法律が具体的に求めているもの
  - 金融商品取引法
    - 経営者確認書と内部統制報告書の提出
    - 内部統制報告書の監査証明
  - 会社法
    - 内部統制に関する事項の取締役会決議

金融商品取引の概要

- 金融商品取引法

  【経営者確認書】

  第24条の4の2　（有価証券報告書の記載内容に係る確認書の提出）

  ＜有価証券報告書の記載内容が金融商品取引法令に基づき適正であることを確認した旨を記載した確認書を有価証券報告書と併せて内閣総理大臣に提出＞

  【内部統制の評価】

  第24条の4の4　（財務計算に関する書類その他の情報の適正性を確保するための体制の評価）

  ＜事業年度ごとに財務計算に関する書類その他の情報の適正性を確保するために必要なものとして内閣府令で定める体制について、内閣府令で定めるところにより評価した報告書（内部統制報告書）を、有価証券報告書と併せて内閣総理大臣に提出＞

  【内部統制の監査】

  第193条の2　2項　（公認会計士又は監査法人による監査証明）

  ＜内部統制報告書には、その者と特別の利害関係のない公認会計士又は監査法人の監査証明を受けなければならない＞
- 証券取引法等の一部を改正する法律

  【適用時期】

  附則15条　平成20年4月1日以降に開始する事業年度から適用する

会社法の内部統制

- 会社法　(取締役会の権限等)

第三百六十二条

4項　取締役会は、次に掲げる事項その他の重要な業務執行の決定を取締役に委任することができない。

六　取締役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務の適正を確保するために必要なものとして法務省令で定める体制の整備

5項　大会社である取締役会設置会社においては、取締役会は、前項第六号に掲げる事項を決定しなければならない。

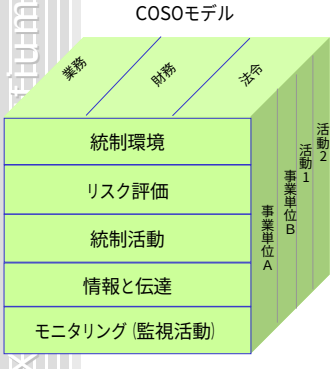
- 会社法施行規則　(業務の適正を確保するための体制)

第百条　法第三百六十二条第四項第六号に規定する法務省令で定める体制は、次に掲げる体制とする。

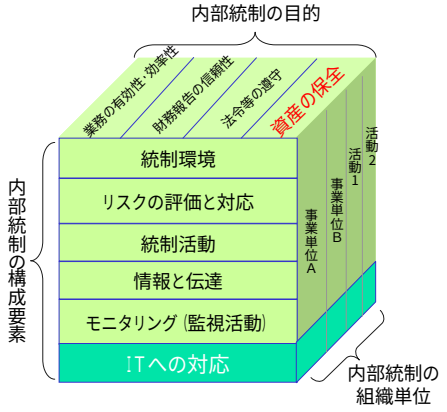
一　取締役の職務の執行に係る情報の保存及び管理に関する体制
二　損失の危険の管理に関する規程その他の体制
三　取締役の職務の執行が効率的に行われることを確保するための体制
四　使用人の職務の執行が法令及び定款に適合することを確保するための体制
五　当該株式会社並びにその親会社及び子会社から成る企業集団における業務の適正を確保するための体制

日本版COSOキューブ

米国COSOキューブ



日本版COSOキューブ



金融庁企業会計審議会内部統制部会で審議

日米SOXの比較

米国	日本
●適正性を保証する内部統制すべてを評価対象 ●評価の当初から、財務諸表に至る一連のプロセスを評価 ●ダイレクトレポーティングを採用 ●内部統制の不備は3段階（「重大な欠陥」「重要な不備」「不備」） ●内部統制監査と財務諸表監査の区分実施	●トップダウン型リスクアプローチを適用し「絞込み」を実施 ●全社的内部統制の評価を踏まえて、業務プロセスに係る内部統制の評価へ至る2段階構成 ●ダイレクトレポーティング不採用 ●内部統制の不備は2段階（「重大な欠陥」「不備」） ●内部統制監査と財務諸表監査の一体的実施

日本版SOX＆内部統制対応の考え方

- いわゆる「日本版SOX」＝財務報告に関する内部統制の構築・整備状況の問題
  - 財務報告に関しては、現実的な対応がポイント
  - ITは有力なツールになるが、万能薬ではない
    - 「One Fits All Solution」は存在しない
- 会社法が要求する「内部統制全般」については、「業務改善」の側面にも注目すべき
  - 業務の可視化・標準化がプロセスの効率化を促進
  - ビジネスリスクのコントロールとしての側面、ＢＣＰの観点
  - 重要リスクにフォーカスし、ＰＤＣＡによるマネジメントプロセスを導入して、そのリスクを管理する「システム」を作る
  - IT環境を前提としたITへの対応
    - 金融庁基準案「ITへの対応」＝情報化社会におけるリスクマネジメントも想定している

(2) 内部統制と情報システムの関係

XML Consortium

内部統制におけるIT

- 現在の企業の業務プロセスの多くはITに依存
  →内部統制を考える場合ITを無視できない
  - 内部統制の項目自体、ITの利用に関連するものが多い
  - 日本版COSOでは、構成要素のひとつとして「ITへの対応」を導入
- 内部統制におけるITの位置付け
  - 内部統制システムの対象範囲としてのITシステム
  - ITを利用して内部統制システムを整備
- 米国でのSOX対応を見ていると、膨大な会計監査対応を少しでも省力化しようとの考えから、ITへの期待が高まる
  - 様々な「SOX対応ツール」
  - 正しく設計・運用されていることが示せれば、評価コストを大幅に削減することが可能

米国SOX法におけるIT

- SOX 施行後の2005 年の状況に関するＫＰＭＧの調査結果
  (年商10 億ドル以上の102 社を対象)
  1) トップキーコントロール (キーとなる内部統制項目)
  - IT コントロール 20%
  - 売上関連 13%
  - 財務報告関連 12%

  2) 重大な欠陥
  - IT コントロール 21%
  - 人事関連 15%
  - 財務報告関連 13%

- ITコントロールの中で、特に不備が目立つものは以下の2つと言われている
  - ITシステムへのアクセスコントロール、ID管理
  - システムの開発・変更時の環境と、運用時の環境の切り分け

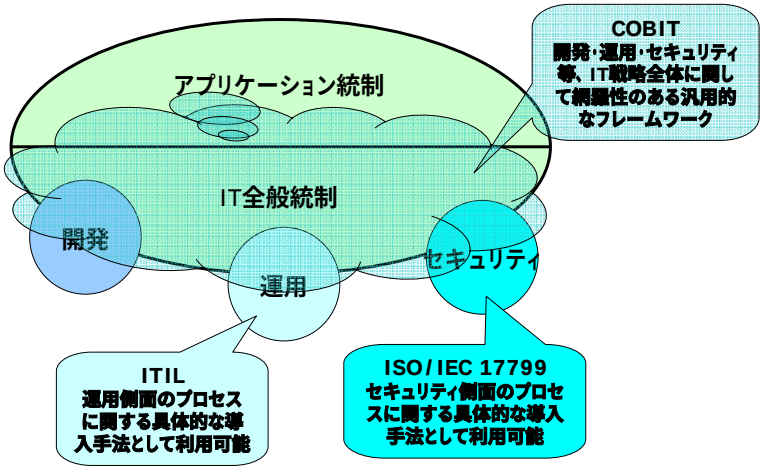
COBITとは

- COBIT(Control Objectives for Information and related Technology
- 組織のITガバナンス能力を内部統制することを支援するシステム管理のガイドライン
- ITガバナンス協会 (ITGI) が作成し、情報システムコントロール協会 (ISACA) と共同で発表し普及を図っているITを管理するためのオープンスタンダード
- COSOフレームワークとの関連が深く、SOX法対応におけるIT統制の強化の際に、そのフレームワークとして利用されるケースが増加している
- 現在の最新版は、2005年に公開された第4版
- SOX法への対処として，SOX法遵守のためのIT統制目標 (IT Control Objectives for SOX) というガイドラインを発表している

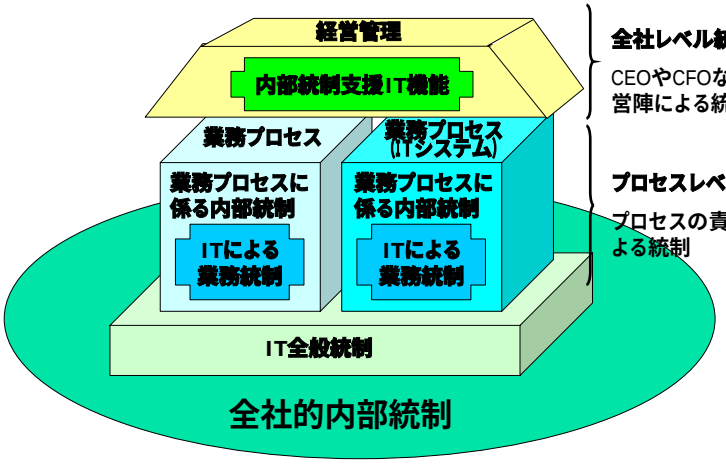
COBITの領域とCOSOの構成要素

IT CONTROL OBJECTIVES FOR SARBANES-OXLEY日本語訳より

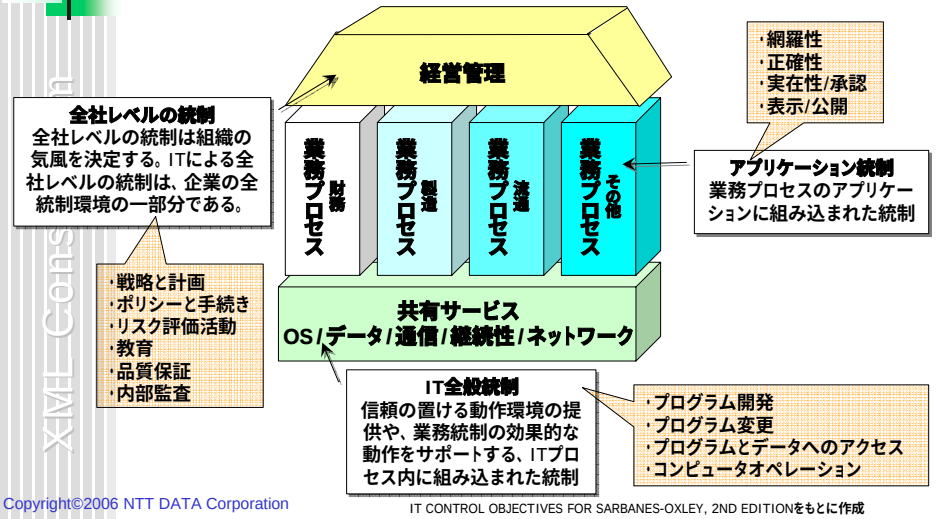
COBITとその他フレームワークとの関係



内部統制におけるITの位置付け



ITに関する統制の種類



IT CONTROL OBJECTIVES FOR SARBANES-OXLEY, 2ND EDITIONをもとに作成

IT全般統制とアプリケーション統制

- IT全般統制
  - 情報処理センター業務に対する統制
    - ジョブの段取りと割り付け、オペレータの業務、データのバックアップとリカバリーの手続きなどの統制
  - システムソフトウェアに対する統制
    - システムソフトウェアやデータベース管理システム、通信ソフトウェア、セキュリティソフトウェア、ユーティリティの効果的な調達、導入、保守管理に関する統制
  - アクセスセキュリティに対する統制
    - システムの不適切で不正な使用を防ぐための統制
  - アプリケーションシステムの開発と保守管理に対する統制
    - アプリケーションシステムの設計と導入、文書化の要件、変更管理、システムの設計または保守計画を統制する際の承認とチェックポイントを含む、開発手法に関する統制
- アプリケーション統制
  - 不正な取引を防止または発見するため、ソフトウェアプログラム内に組み込まれている
  - 他の統制と併用された場合、必要に応じて、取引処理の完全性、正確性、承認、有効性を確実にする
  - アプリケーション統制の例は以下の通り
    - 誤入力防止のための画面インタフェース、入出力データチェック、入力データの連続性や合計値のチェック、権限者による承認とその記録の保存　等々
  - 自動化されたアプリケーション統制の増加により、IT全般統制はより重要になってきている

COBITとIT全般統制との対応

CobiT の統制目標	PCAOB IT全般統制			
	プログラム開発	プログラム変更	コンピュータ・オペレーション	プログラムとデータへのアクセス
1. アプリケーションソフトウェアの調達と開発	●	●	●	●
2. 技術インフラの調達と保守	●	●	●	
3. 方針、運用手続きの作成と維持	●	●	●	●
4. アプリケーションソフトウェアと技術インフラの導入とテスト	●	●	●	●
5. 変更管理		●		●
6. サービスレベルの定義と管理	●	●	●	●
7. サードパーティサービスの管理	●	●	●	●
8. システム・セキュリティの保証			●	●
9. 構成の管理			●	●
10. 問題と事故管理			●	
11. データ管理			●	●
12. オペレーション管理			●	●

IT CONTROL OBJECTIVES FOR SARBANES-OXLEY日本語訳より

SOX法対応ツール

- SOX法対応のツール（ソフト）は大きく2種類
  - 1．SOX法対応活動自体を支援するもの
    ＝　全社レベルの統制を実現するためのもの
    - 「文書化・評価支援ソフト」、「ドキュメント管理ソフト」、「内部監査支援ソフト」など
  - 2．SOX法の目的である「財務報告の信頼性向上」に関わる個々の業務プロセスに内部統制の仕組みを実装するもの
    - 業務処理統制に関しては、「ERPソフト」、「データ保護ソフト」、「ワークフロー支援ソフト」、「ドキュメント管理ソフト」など
    - IT全般統制に関しては、「開発管理ソフト」、「開発支援ソフト」、「運用管理ソフト」、「ID/アクセス管理ソフト」など
- 「One Fits All Solution」は存在しない
- 企業情報システムの拡張性と柔軟性や、規制及びその解釈の変更への迅速な対応に備えておく必要がある

IT利用による効果（1）

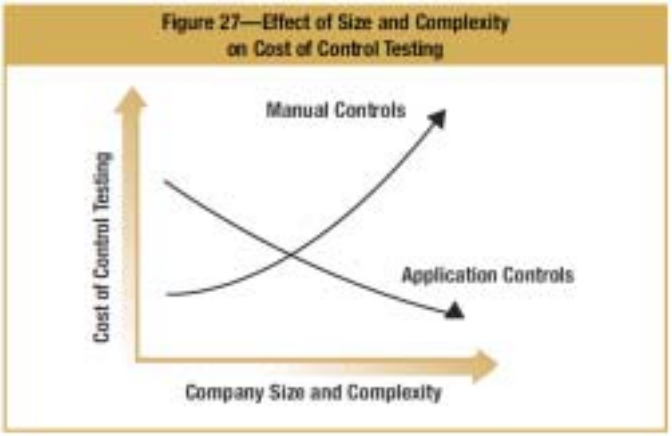
Figure 26—Comparison of Manual and Application Control Approaches

Manual Control Approach		Automated Control Approach	
Total controls	500	Total controls	500
Effort to document per control	1 hour	Effort to document per control	3 hours
Total effort to document	500 hours	Total effort to document	1,500 hours
Average sample size per control	10	Average sample size per control	1 ※
Total sample items to test	5,000	Total sample items to test	500
Effort to test per sample	30 minutes	Effort to test per sample	30 minutes
Total effort to test	2,500 hours	Total effort to test	250 hours
Total effort	**3,000 hours**	**Total effort**	**1,750 hours**

※IT全般統制が効果的に機能していることが前提

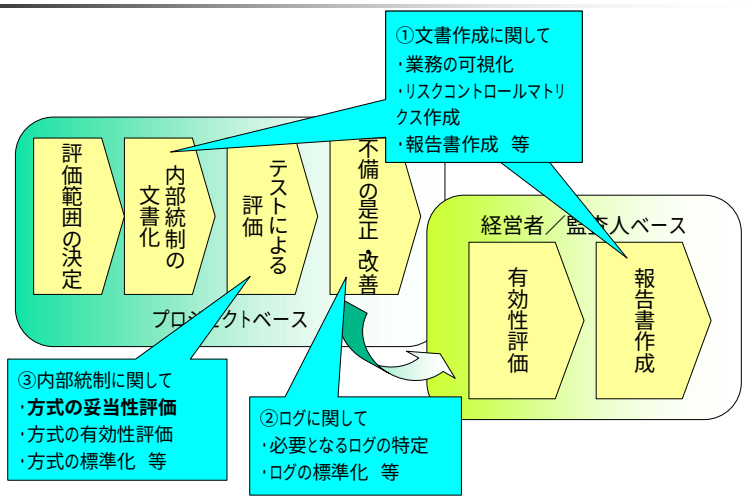
IT CONTROL OBJECTIVES FOR SARBANES-OXLEY, 2ND EDITIONより

IT利用による効果（2）



IT CONTROL OBJECTIVES FOR SARBANES-OXLEY, 2ND EDITIONより

最後に　～XML適用の可能性について



ご清聴ありがとうございました

XML Consortium

参考資料

Copyright©2006 NTT DATA Corporation

財務報告における内部統制の評価･監査の流れ

金融庁 企業会計審議会 第11回内部統制部会資料から引用