

要求開発と内部統制 J-SOX

要求開発アライアンス
定例会

Requirement Development Alliance



要求開発とSOX

- 要求開発とJ-SOXの関係は？
 - 関係あるのか??
 - 本当にあるのか??
 - 時流に乗ってるだけなのか???
 - J-SOX対応って「開発」なのか???

J-SOXとは何か

- 巷に溢れる“J-SOX対応”

- いったい「何が」対応なんだ？

- そもそもJ-SOX対応って何なのだ

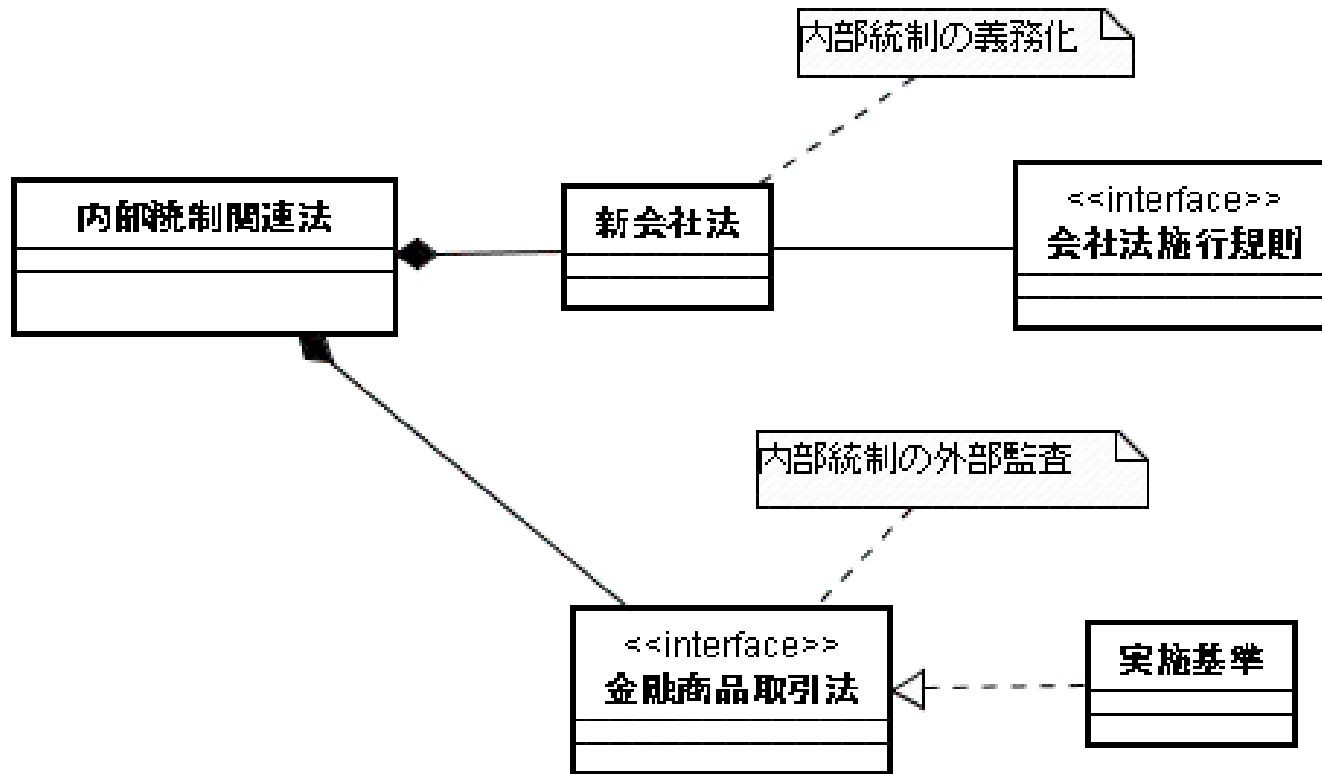
The screenshot shows a web browser window with the URL <http://fpronk-le.jp.co.jp/sox/index.html>. The page content includes:

- データ** (Data) section:
 - 日本版SOX法関連市場は975億円に63.7%の企業が対策プロジェクトを重要視**
2006年における日本版SOX法関連市場規模は975億円となる見込みであり、2005年にピークを過ぎて2607億円に達するもよがた。IDC Japanが国内の有形公開企業100社のSOX（最高情報責任者）およびIT部門マネジャーを対象とした調査による。(2006/05/30)
 - 上場企業の6割強が何らかに着手、日本版SOX法への対応**
日本版SOX法の導入の検討が進められていることについて、86.1%の企業が認識しており、既に数社の企業が実際に何らかの対応に着手している。野村総合研究所が東証1部・2部・東証マザーズ・JASDAQ上場企業を対象にした調査による(有効回答数は380社)。(2006/04/06)
 - 日本版SOX法、情報システム担当者の2割が関心を示す**
2006年にも施行予定の日本版SOX法(企業改革法)について、国内企業の情報システム担当者のうち2割が関心を示している。日経マーケットアクトが国内企業の情報システム担当者を対象にした「企業情報システムの利用実態2005-2006(第3回)」による(有効回答数は505社)。(2006/03/07)
- 米国レポート** (US Report) section:
 - SOX法が招くIT現場の混乱**
米国のSOX法(サーベインズ-オクスリー法)が、米国のシステム管理者や開発者にも与える影響をレポートした2004年の記事。「監査役がSQL Serverの管理者権限を多く奪って混乱を招いている」といった状況を報告する。

On the right side of the page, there is a sidebar with various news items and an RSS feed section titled 'Enterprise アクセルランニング' (Enterprise Acceleration) with a date of '2006年05月26日' (May 26, 2006). The RSS feed includes links for 'ニュース(総合)', 'ニュース(国内)', 'ニュース(海外)', and '記者の眼'.

だいたいJ-SOX法なんて法律はない！！

- 内部統制に関する法律はあります！
でも一本ではありません

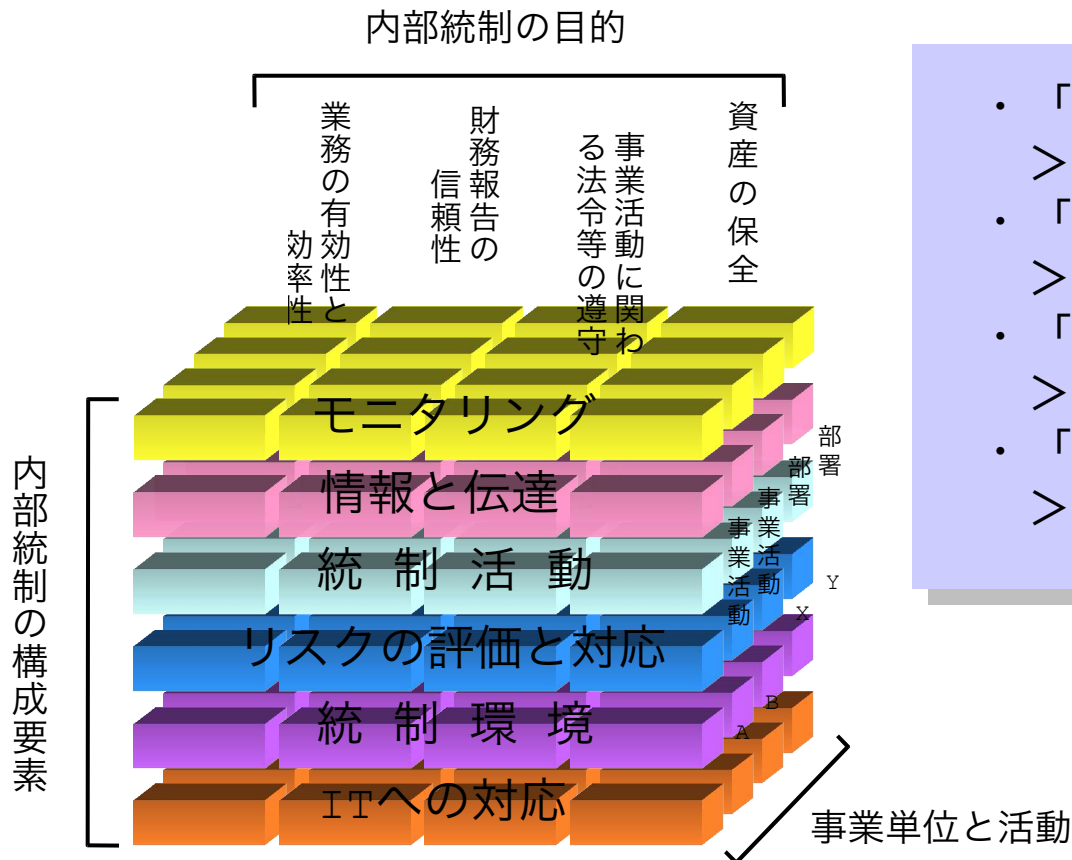


そもそも内部統制なんて新しい言葉なのだ

- 内部統制という単語が判例に初登場したのは・・・
 - 2000年（平成12年）9月20日大阪地方裁判所
「大和銀行ニューヨーク支店事件」
 - 取締役は、取締役会の構成員として、また、代表取締役又は業務担当取締役として、リスク管理体制を構築すべき義務を・・・・・・・・
- 「企業やってるなら、きちんとしてね！」ということ
 - 「きちんと」＝リスク管理を確実に行う
 - リスク＝犯罪などの人がする悪いこと + 災害などの自然の脅威
- なぜ？今、言われるのか
 - 正しい、財務「報告」が市場を守るから！

何をもって「正しい」というか

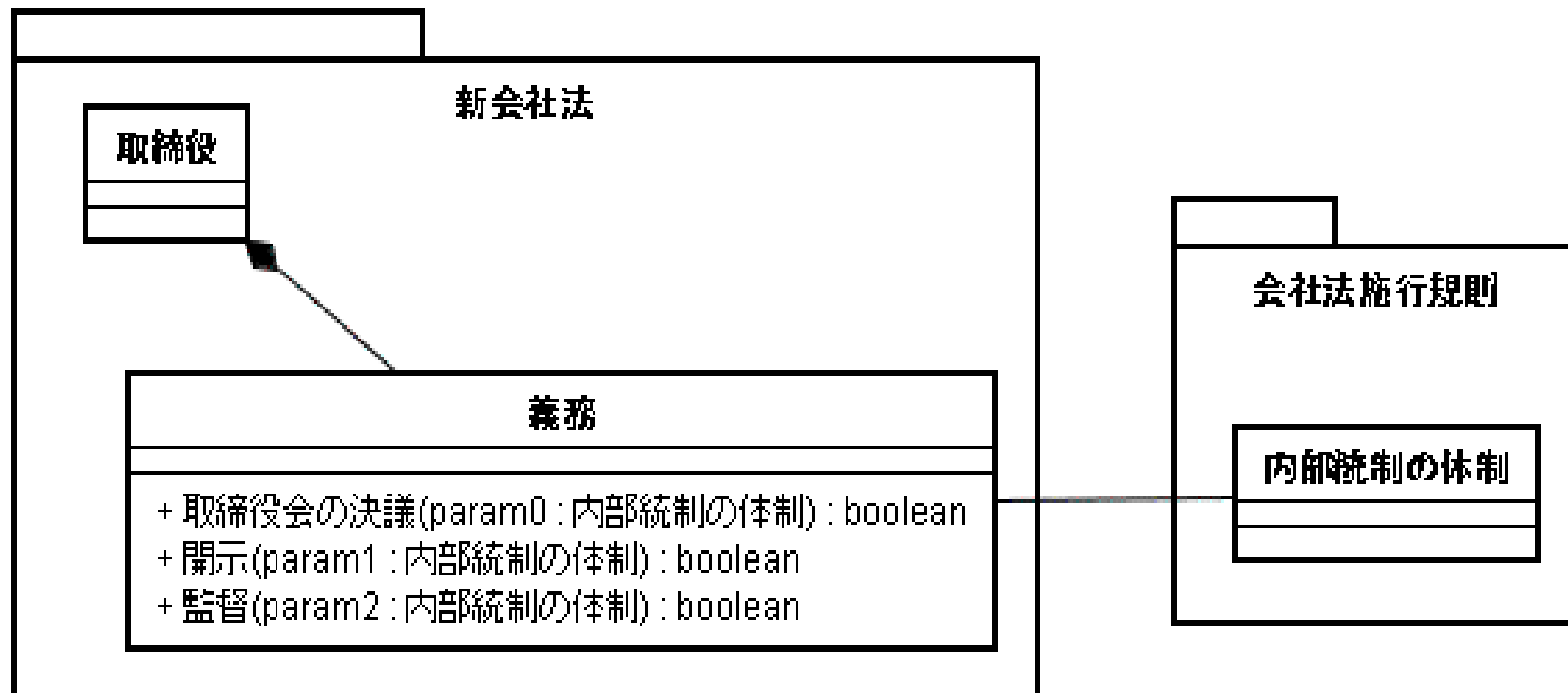
「内部統制」という視点



- ・ 「業務活動」
＞無駄で無益なことはしていない
- ・ 「財務報告」
＞うそや間違いをしていない
- ・ 「法規制準拠」
＞悪いことはしていない
- ・ 「資産の保全」
＞資産を浪費・放置していない

(株)豆蔵 内部統制サービス資料より引用

会社法はこういうことです



「知らない」では済まされない

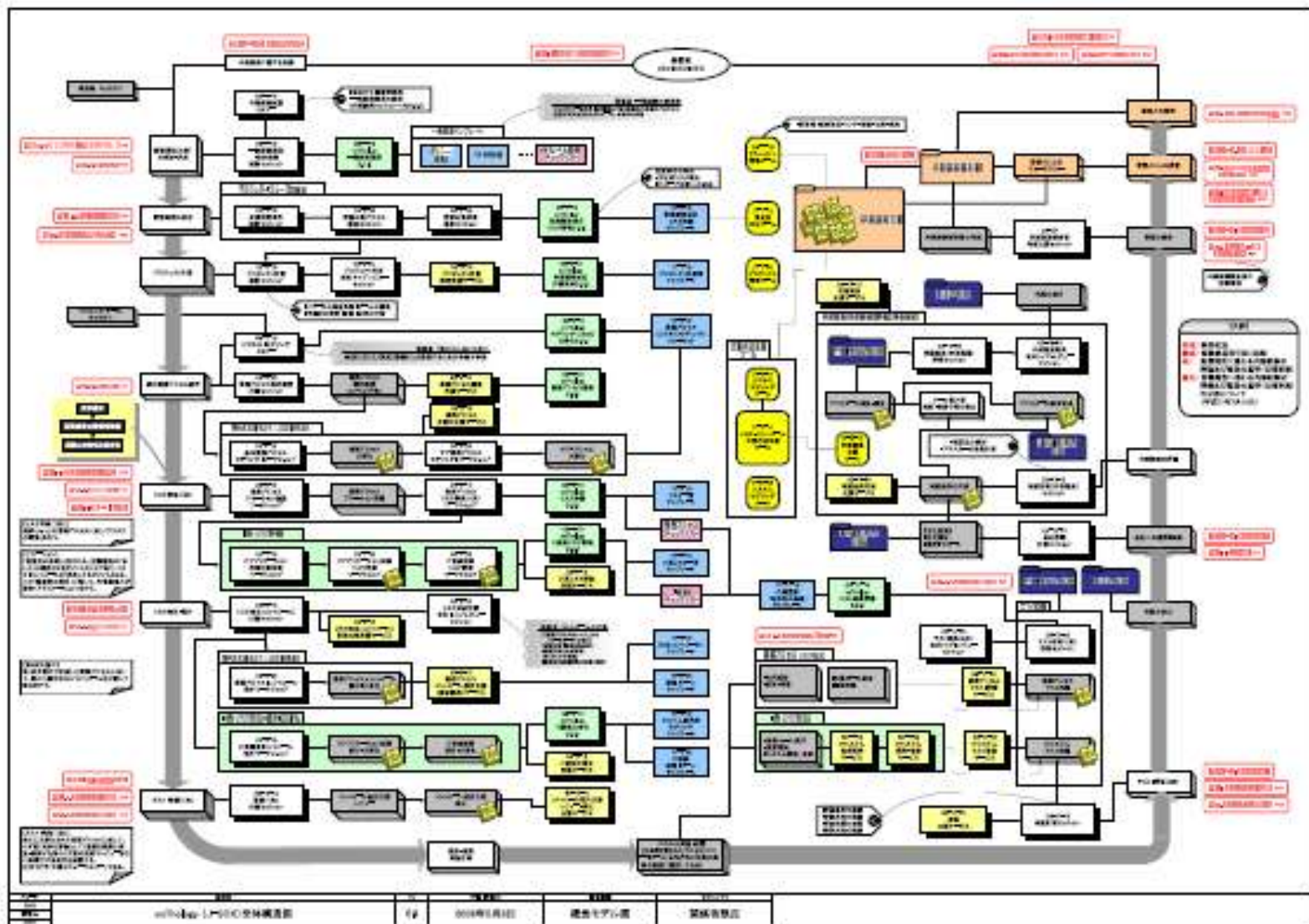
それで、いったい何が「法対応」なのか

- 可監査性
 - 監査とは
 - 証明の保証
 - 見えること
 - 監査対象は「内部統制報告書」（経営者の作るもの）
 - ダイレクトレポーティング方式の否定
 - 仕事のやり方、が「正しい」ことを証明する
- 内部統制報告書に使用できるような資料を提供すればよい＝法対応

JSOX対応は「大きくて」「大変な」プロジェクト

- 膨大な資料の作成・・・かも？
 - 業務プロセスがマニュアルなどで文書化されていない
 - 職務権限規定などが完璧に揃えられていない
 - 情報システムと業務プロセスの関連が文書化されていない
 - 経理システムなどの関連アプリケーションの開発文書が残っていない
 - アクセスログなんてディスクの無駄だから残していない
 - システムの運用規則やマニュアルが完備されていない
- これでは、監査のしようがありません！！
 - 不適格へまっしぐら
 - 社長に言いつけてやる！！

J-SOX対応プロジェクトの規模



重要なことは「何を監査するか」ということ

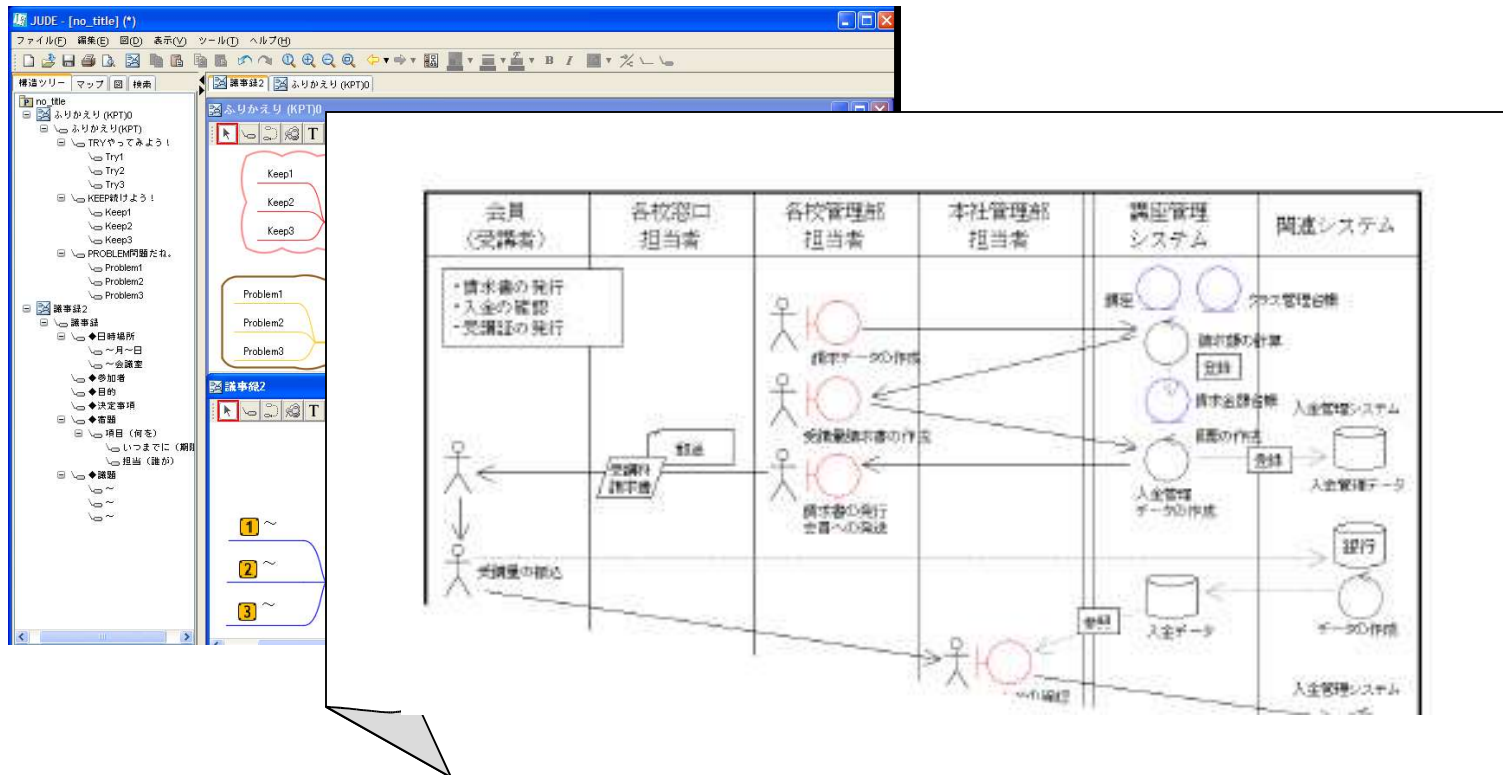
- 「当たり前前のことを、当たり前前にやる」ことで企業の健全性や競争力を伸ばす、とか言うけれど
- そのために「当たり前前、以上のこと」を要求してどうする。本末転倒
- これが「正しい」ものならそれでよい
 - 財務諸表の計算と根拠との整合性
 - 財務諸表の数値を「生成」する業務プロセス

内部統制監査のための三種の神器

- 業務フロー
 - こればかり注目されていますが・・・
- リスク・コントロール・マトリックス (RCM)
- 業務記述書

業務フロー図

- ビジネスモデリングによる文書化



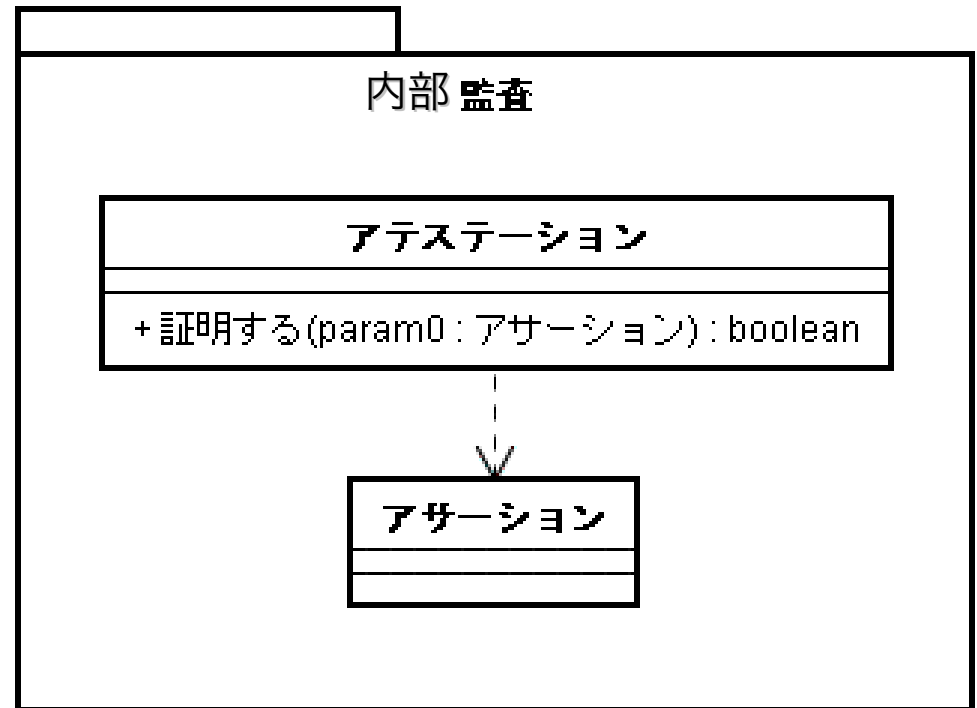
スコープが重要

- まずは「正しさ」を証明しなければならない科目を特定する
 - 連結決算
- その科目の数値に関与する業務プロセスを特定する
- その業務プロセスを構成する情報システムを特定する
- その情報システムを開発・運用するための体制に関する問題を特定する

監査要点 全てが、これを前提とする

- アステーション

- アサーション



- 監査の対象になるのは

- アサーションあつてのリスク
 - リスクあつてのコントロール
- リスクを正しく認識したうえで
コントロールを有効に機能
させているか

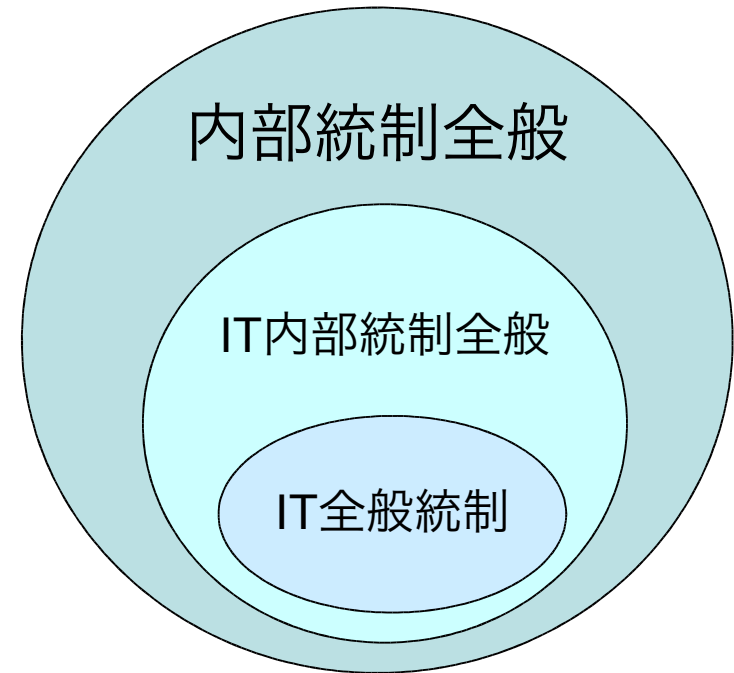
業務プロセスとモデリング

- 何を「証明」するのか
 - アサーション
 - リスクとコントロール
- 単にフロー図が出来ればよいわけではない
 - ビジネス・モデリングの「前提」 (目的)
 - アステーションが可能であること (可能であればよい)
- 「前提」なければ「価値」もなし

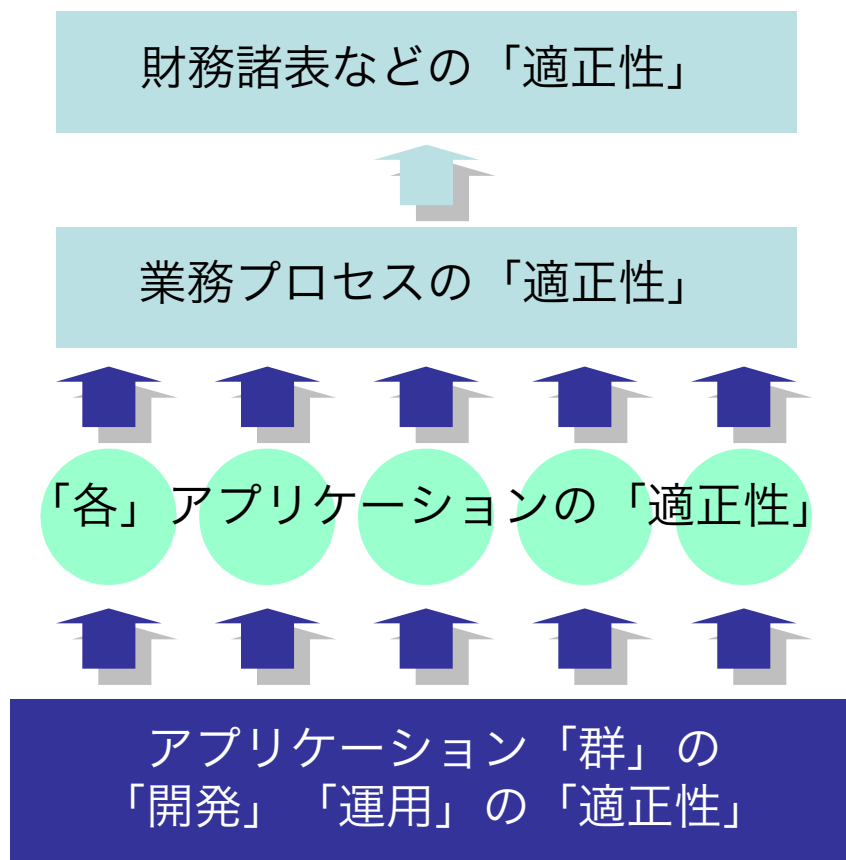
- 業務リスク分析や文書化
 - 「目的」（視点）を重視したモデリング
 - データだけではない。人の介在も含めたモデリング
 - ビジネスモデリングによるAs Isのモデリング
 - コントロールの立案におけるTo Beのモデリング
 - システム化範囲の明示化
- 内部監査・アテスタ体制の設計・構築
 - 新業務モデルの設計に等しい
- プロジェクト推進
 - プロセス・セルの考え方

IT全般統制と要求開発

- ITに関する内部統制の3つのスコープ
 - IT全般体制
 - IT全般統制の部分だけ
 - IT内部統制全般
 - IT業務統制+IT全般統制
 - 内部統制全般
- 要求開発はIT全般統制に関わる



IT全般統制



を確保するためには・・・

を確保しなければならないが、
そのためには・・・

を確保しなければならないが、
そのためには・・・

を確保しなければならない=
「IT全般統制」

「何をすればよいか」という基準を網羅すると・・・

- COBIT (Control Objectives for Information and related Technology)
 - ■計画と組織
 - 1.戦略的IT計画の定義
 - 2.情報アーキテクチャの定義
 - 3.技術指針の決定
 - 4.IT組織の関係の定義
 - 5.IT投資の管理
 - 6.運用目標と指針の伝達
 - 7.IT人的資源の管理
 - 8.品質管理
 - 9.リスクの査定と管理
 - 10.プロジェクト管理
 - ■取得とインプリメント
 - 1.自動化されたソリューションの検証
 - 2.アプリケーションソフトの調達・保守
 - 3.技術基盤の調達・保守
 - 4.プロセスの開発・保守
 - 5.IT資源の調達
 - 6.変更管理
 - 7.ソリューションと変更の導入・認定
 - ■供給とサポート
 - 1.サービスレベルの定義と管理
 - 2.サードパーティサービス管理
 - 3.性能やキャパシティの管理
 - 4.継続的サービスの保証
 - 5.システムセキュリティの保証
 - 6.識別とコスト配賦
 - 7.ユーザーの教育・訓練
 - 8.サービスデスクとインシデント管理
 - 9.構成管理
 - 10.問題管理
 - 11.データ管理
 - 12.物理環境管理
 - 13.運用管理
 - ■モニタと評価
 - 1.ITパフォーマンスのモニタと評価
 - 2.内部統制のモニタと評価
 - 3.コンプライアンス遵守の保証
 - 4.ITガバナンスの提供

企業におけるシステム開発と内部統制

開発前	【要求開発】 システム企画（効率性・有効性）
開発中	【プロジェクト管理】 権限者による承認
開発後	【テスト】 処理の適正性の確認

Appendix

Requirement Development Alliance



内部統制導入

(新会社法における) 内部統制システムの構築に関する決定・開示

新法362条第4項

内部統制システムの構築に関する決定・開示

内部統制システムの構築の基本方針については、
取締役が設置された株式会社では取締役会の
専決事項→個々の取締役に委ねることはできない

会社法施行規則 第100条

業務の適正を確保するための体制

企業集団、取締役、監査役及びその補助者、使用人が業務の適正を確保するための体制

内部統制上の監督義務と責任

取締役及び監査役の監視・監督義務

- 取締役は、取締役会の構成員として、また、代表取締役または業務担当取締役として、**内部統制を構築すべき義務を負う**とともに、代表取締役及び業務担当取締役が**内部統制を構築すべき義務を履行しているか否かを監視する義務を負う**。
 - 善管注意義務
 - 忠実義務（新会社法355条）
 - 監視・監督義務（新会社法362条2項）
- **他の取締役の職務執行に対する監視・監督義務**
- 監査役は、業務監査の職責として取締役が内部統制の整備を行っているか否かを監視すべき職務を負う。