OPENTHOLOGY

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

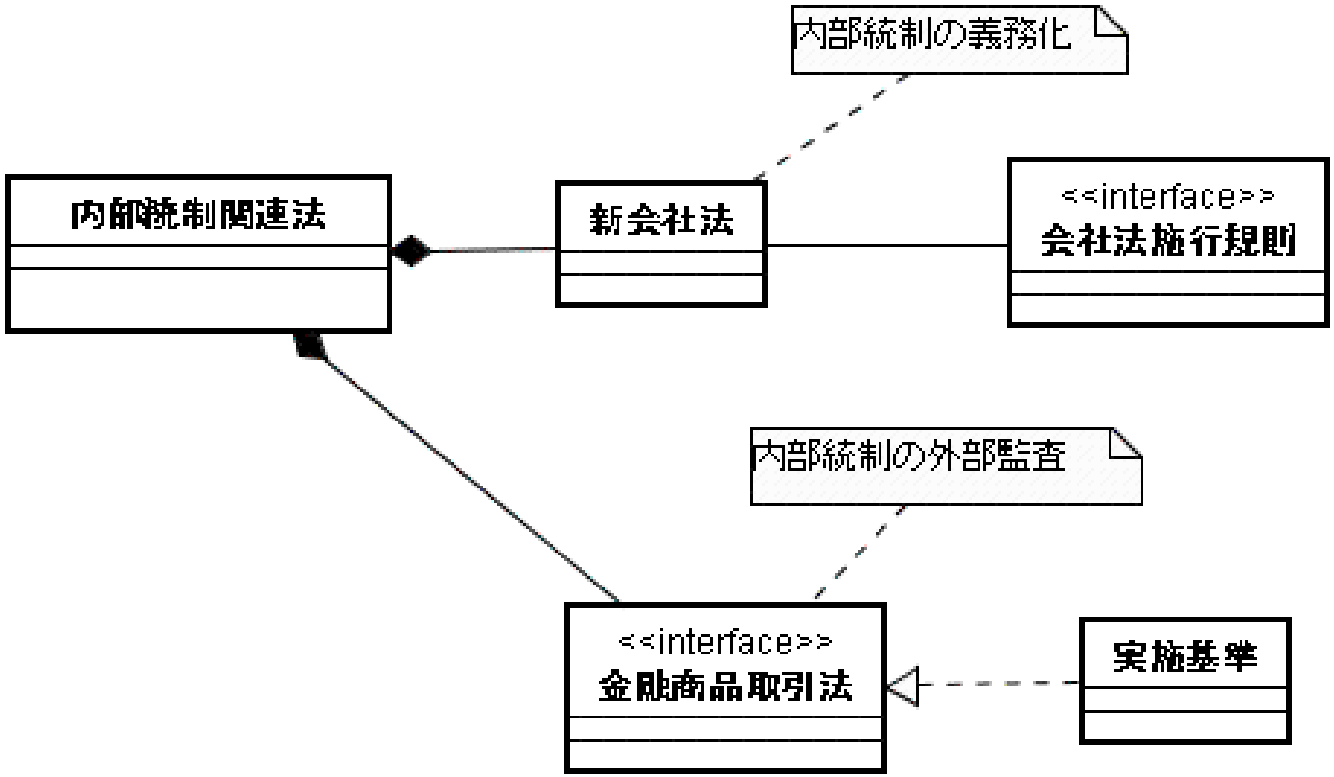
- 要求開発とJ-SOXの関係は？
  - 関係あるのか？？
  - 本当にあるのか？？
  - 時流に乗ってるだけなのか？？？
  - J-SOX対応って「開発」なのか？？？

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

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

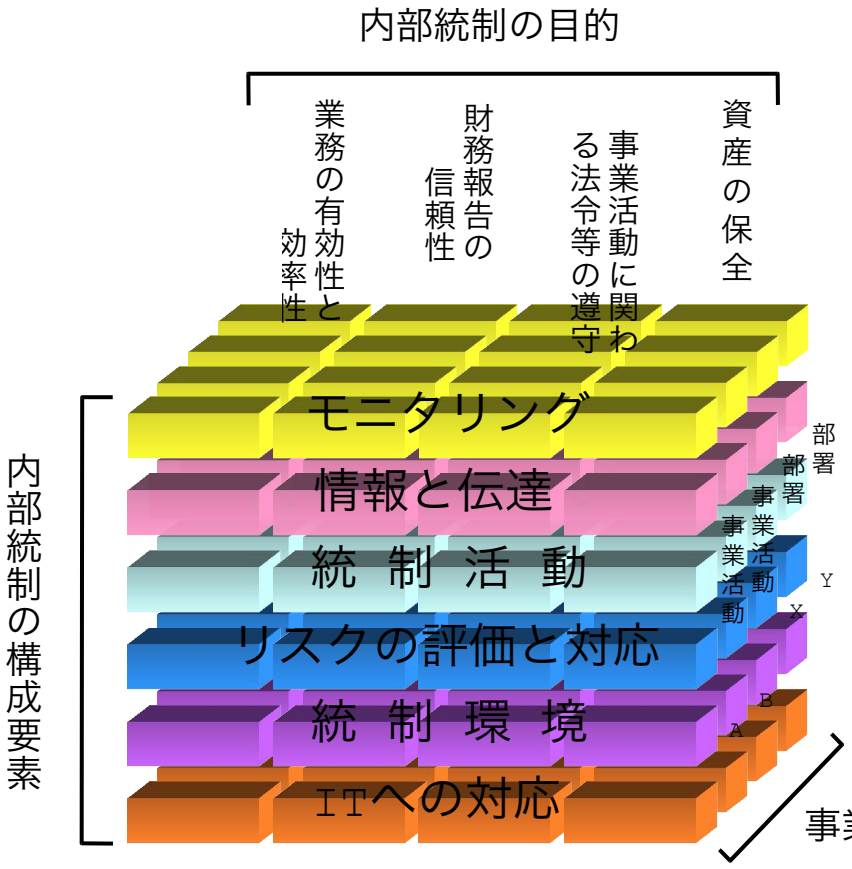


そもそも内部統制なんて新しい言葉なのだ

- 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

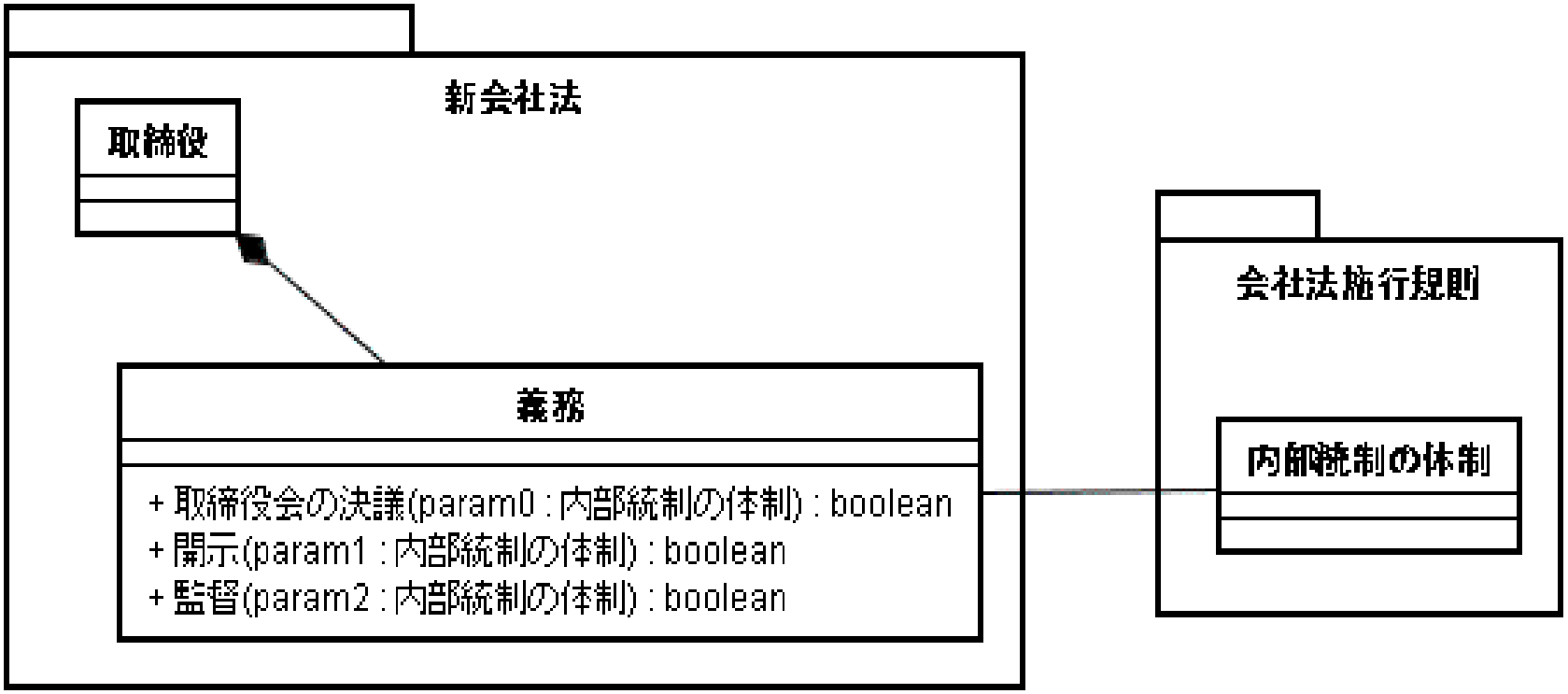
- 「内部統制」という視点



- 「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

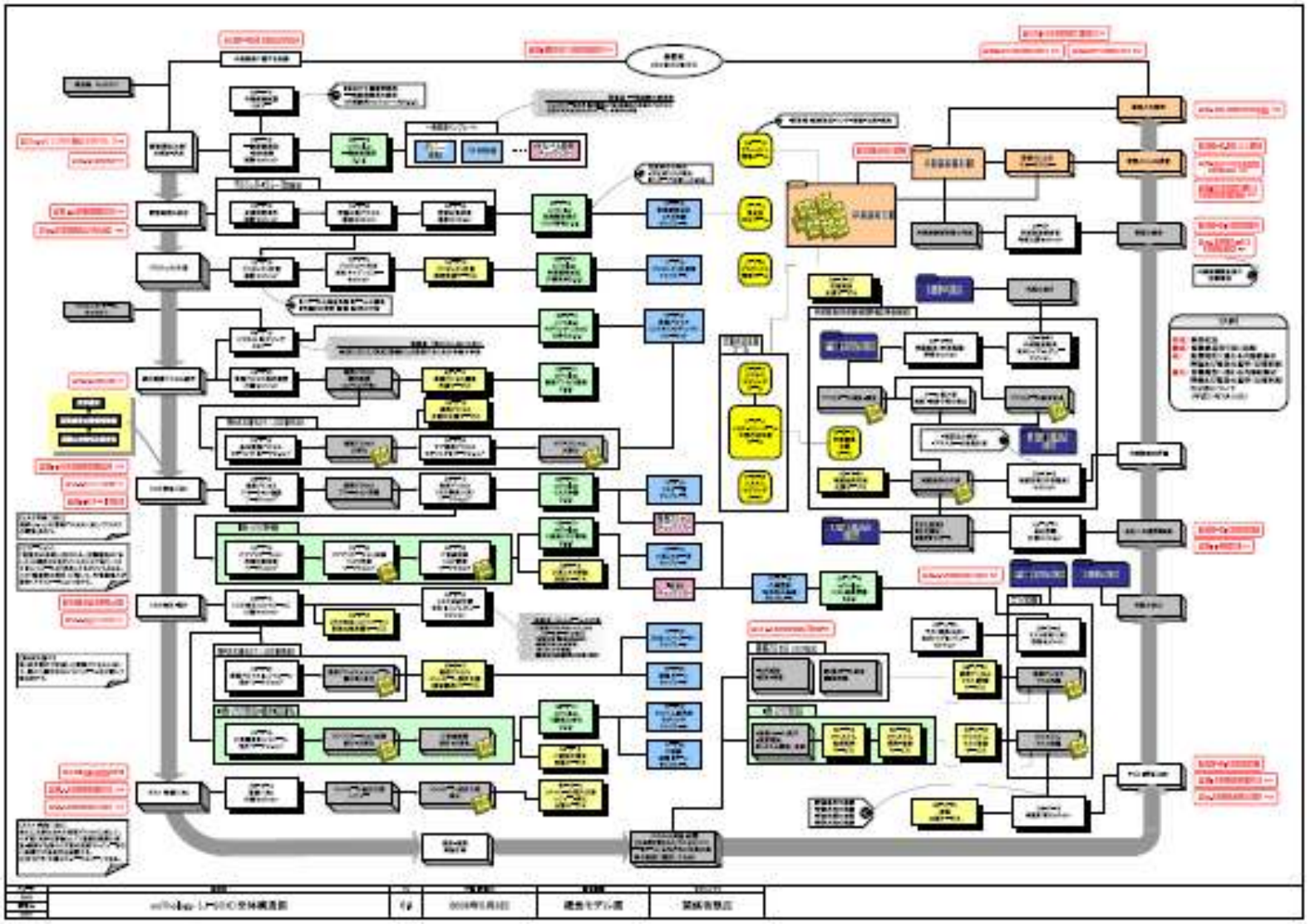
それで、いったい何が「法対応」なのか

- 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

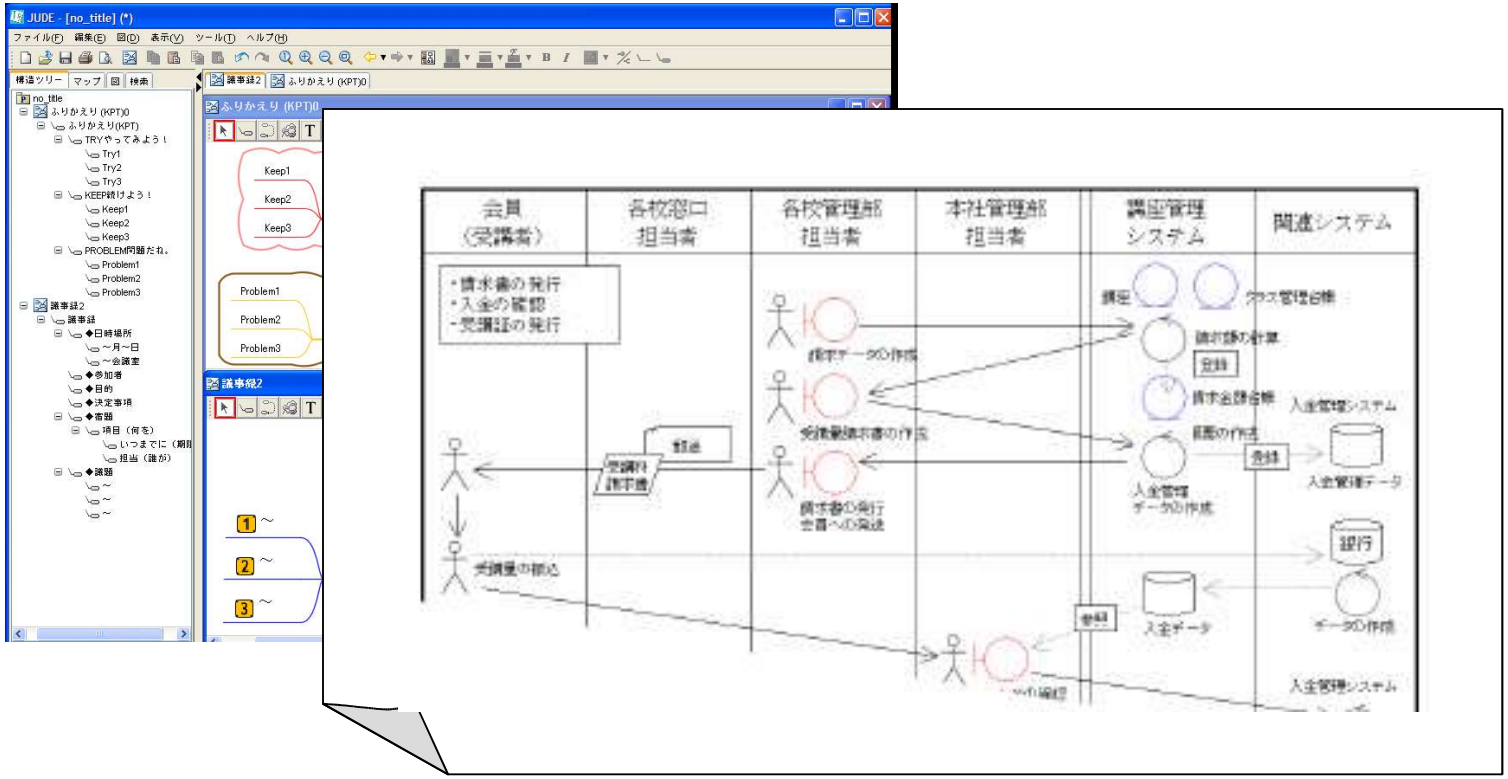
- 「当たり前のことを、当たり前にやる」ことで企業の健全性や競争力を伸ばす、とか言うけれど
- そのために「当たり前、以上のこと」を要求してどうする。本末転倒
- これが「正しい」ものならそれでよい
  - 財務諸表の計算と根拠との整合性
  - 財務諸表の数値を「生成」する業務プロセス

内部統制監査のための三種の神器

- 業務フロー
  - こればっかり注目されてますが・・・
- 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

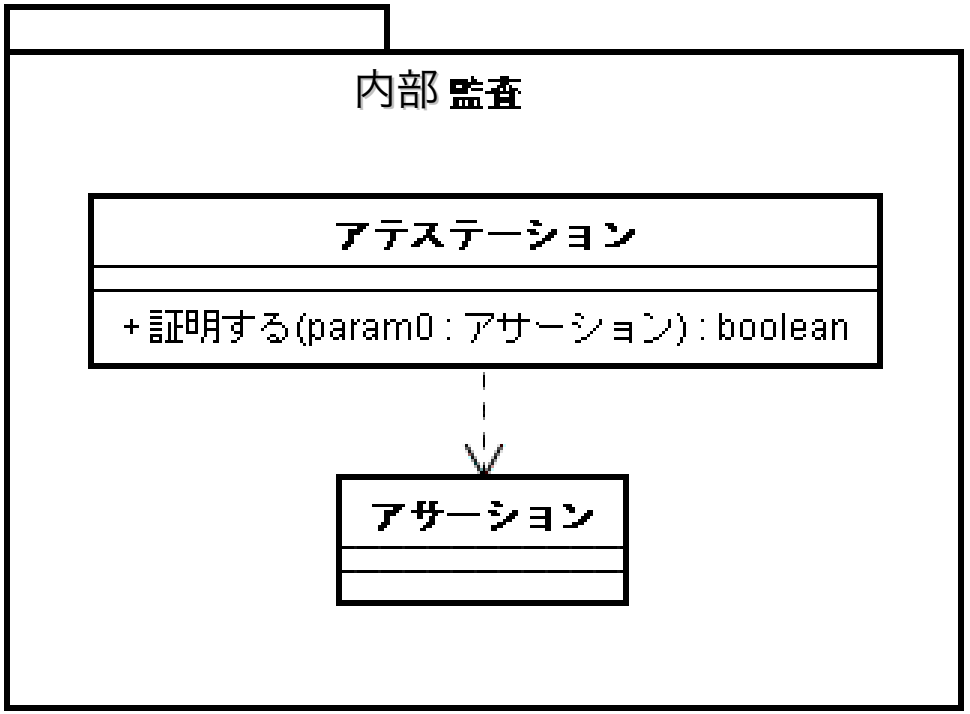


スコープが重要

- 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

- アテステーション
- アサーション



- 監査の対象になるのは
  - アサーションあってのリスク
  - リスクあってのコントロール

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

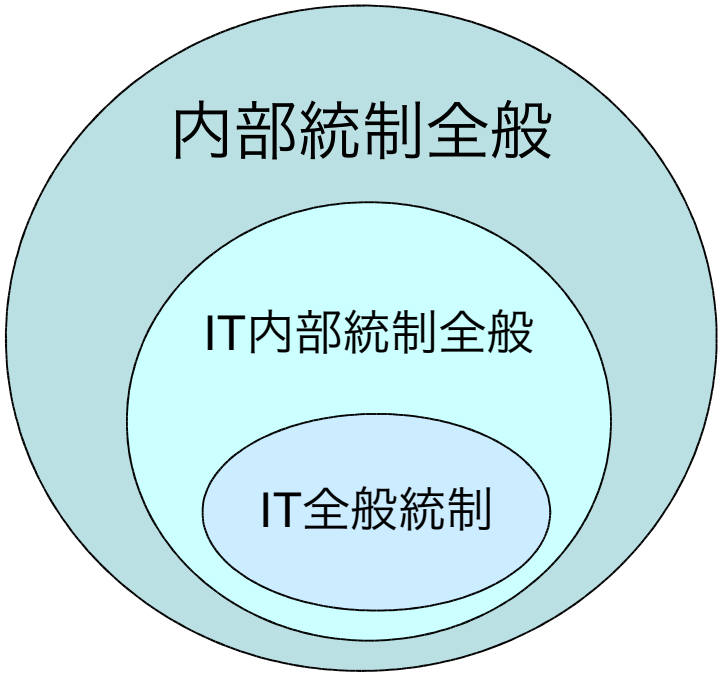
- 何を「証明」するのか
  - アサーション
  - リスクとコントロール
- 単にフロー図が出来ればよいわけではない
  - ビジネス・モデリングの「前提」（目的）
    - アテステーションが可能であること（可能であればよい）
- 「前提」なければ「価値」もなし

要求開発の手法や考え方

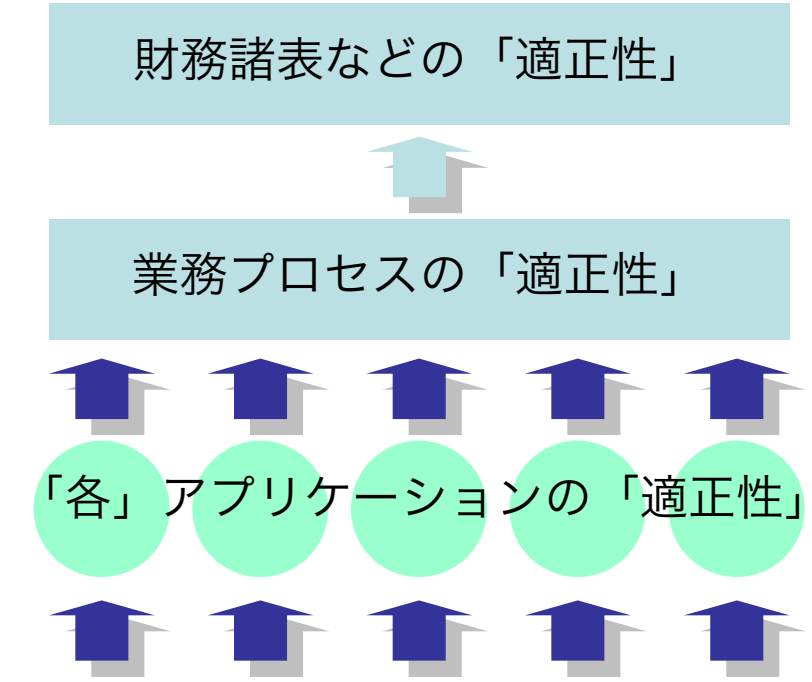
- 業務リスク分析や文書化
  - 「目的」（視点）を重視したモデリング
  - データだけではない。人の介在も含めたモデリング
    - ビジネスモデリングによるAs Isのモデリング
    - コントロールの立案におけるTo Beのモデリング
    - システム化範囲の明示化
- 内部監査・アテスタ体制の設計・構築
  - 新業務モデルの設計に等しい
- プロジェクト推進
  - プロセス・セルの考え方

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

OPENTHOLOGY

Appendix

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る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。