UMLビジネスプロセスモデリングによる内部統制の可視化

2006年3月14日

株式会社オージス総研
ビジネスプロセスモデリング部

OGIS-RI

米国におけるSOX法適用の背景

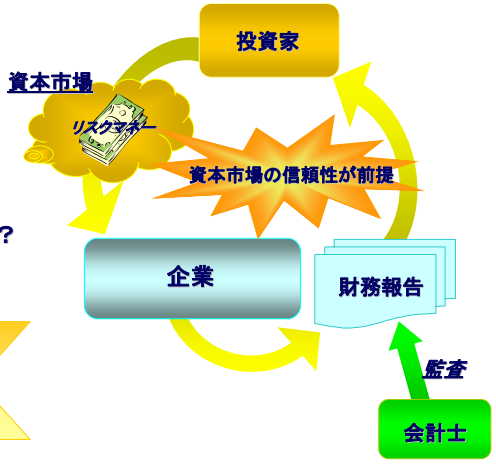
米国における会計不正（エンロン・ワールドコム）

資本市場の信頼性が揺らいだ

資本市場の信頼性回復の必要性

財務報告の信頼性をどのように担保？

従来の財務諸表監査に加え
財務諸表作成プロセスである
*内部統制監査*を制度化



OGIS-RI

SOX法の内容

不正な財務報告防止のための集大成

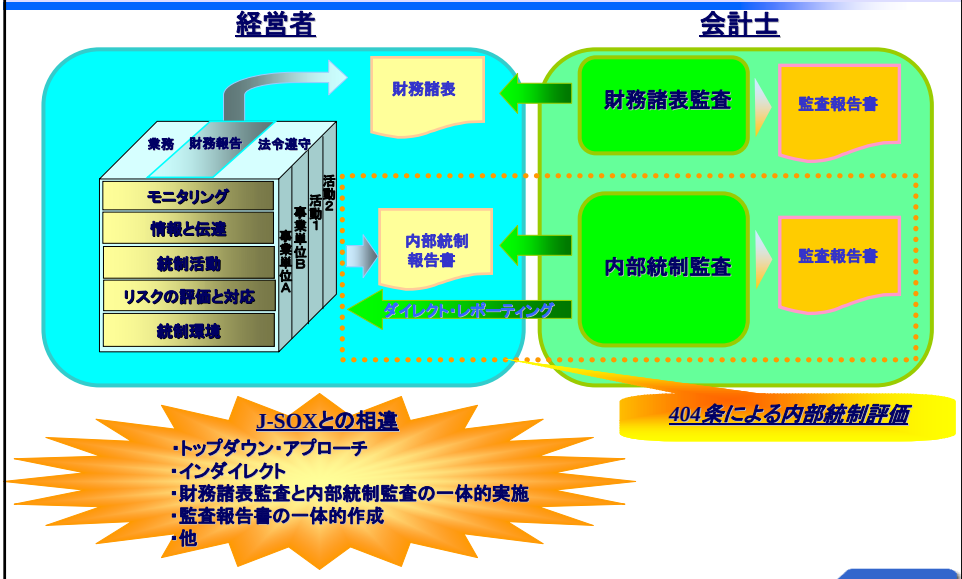
✓PCAOB（公開会社会計監視審議会）の設置
✓外部監査人の独立性強化
✓会社の機関責任強化
✓財務開示制度の強化
✓証券アナリストの利益相反
✓SECの権限強化
…etc.

302条：財務報告に対する会社責任（民事）
906条：財務報告に対する会社責任（刑事）
404条：経営陣による内部統制評価

PCAOB　監査基準第2号
“An audit of internal control over financial reporting performed in conjunction with an audit of financial statements”

内部統制監査

SOX法による監査制度の概要



J-SOXとの相違
・トップダウン・アプローチ
・インダイレクト
・財務諸表監査と内部統制監査の一体的実施
・監査報告書の一体的作成
・他

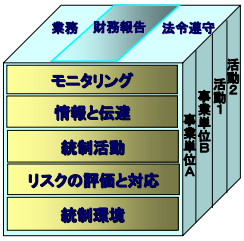
内部統制の文書化の範囲

"internal control over financial reporting"

財務報告に係る内部統制とは？

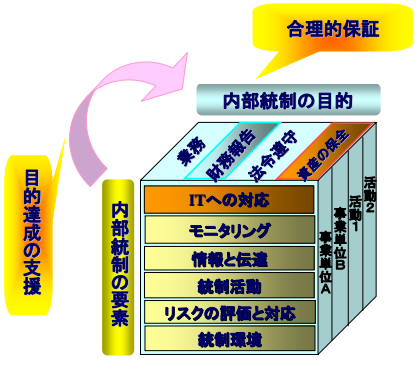
「財務報告に係る内部統制」とは、財務報告の信頼性を確保するための内部統制をいう

企業会計審議会：内部統制部会の基準案より



OGIS-RI

内部統制の意義



内部統制の定義

内部統制とは、基本的に、業務の有効性及び効率性、財務報告の信頼性、事業活動に関わる法令等の遵守並びに資産の保全の4つの目的が達成されているとの合理的な保証を得るために、業務に組み込まれ、組織内のすべての者によって遂行されるプロセスをいい、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（監視活動）及びIT（情報技術）への対応の6つの基本的要素から構成される

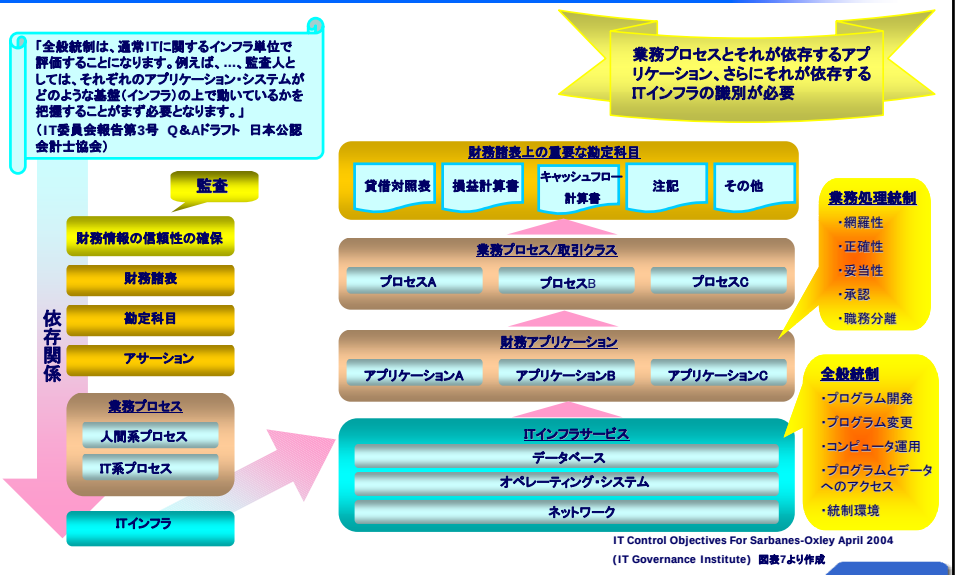
企業会計審議会：内部統制部会の基準案より

COSOと日本版COSOの相違点

- *目的：資産の保全*
- *要素：ITへの対応（ITの利用）*

OGIS-RI

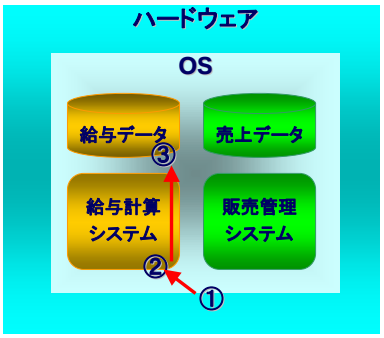
内部統制監査におけるIT統制の重要性



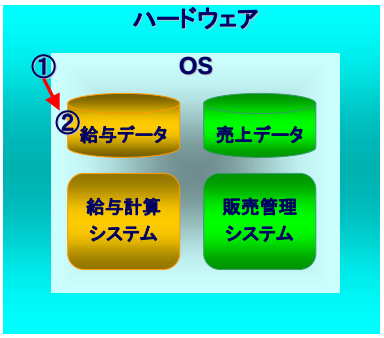
IT Control Objectives For Sarbanes-Oxley April 2004
(IT Governance Institute) 図表7より作成

全般統制と業務処理統制

OSが適切に設定されている場合



OSが適切に設定されていない場合

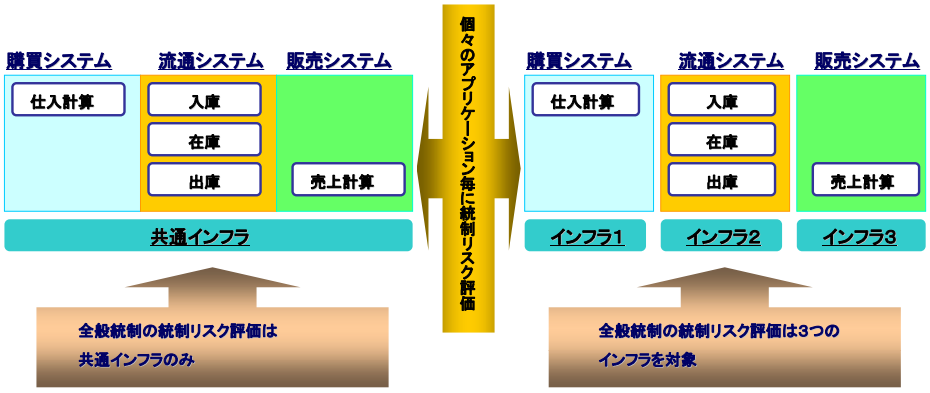


IFAC（世界会計士連盟） Controlling Computers in Business : Logical Access Security より作成

IT統制の評価

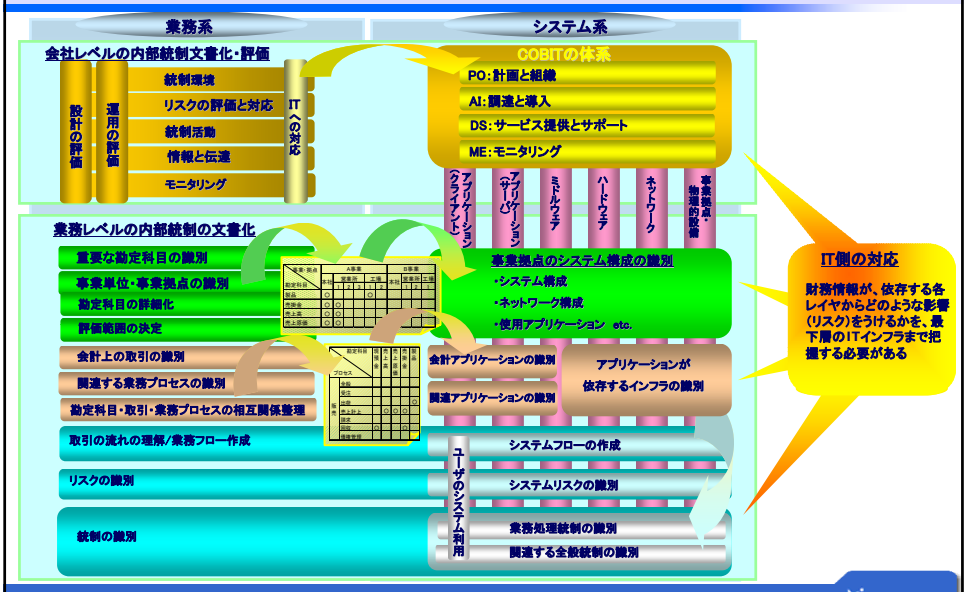
全般統制は通常ITに関するインフラ単位で評価

業務処理統制は個々のアプリケーション・システム毎に評価



IT委員会報告第3号　Q＆Aドラフト　日本公認会計士協会より

内部統制の文書化の全体像とIT



COBITを採用するメリット

- ✓ *COBIT（ Control Objective for Information and related Technology ）とは？*
  - ✓ 米国の情報システムコントロール協会（ISACA：Information Systems Audit and Control Association）が提唱するITガバナンスの成熟度を測るフレームワーク
  - ✓ ITの企画から運用に至るまでのフローを4つの管理プロセスと34のITプロセスとして定義
  - ✓ それぞれのプロセスについて、CSF（critical success factor：重要成功要因）／KGI（key goal indicator）／KPI（Key Performance Indicator）と、その成熟度レベルを6段階で定義
  - ✓ リスク・コントロールモデルを採用
- ✓ *COBITを利用するメリット*
  - ✓ 事実上の世界標準
  - ✓ PCAOBにおけるIT全般統制との整合性
  - ✓ COSOとの整合性
  - ✓ システム監査においても参照

IT全般統制のフレームワークとして利用

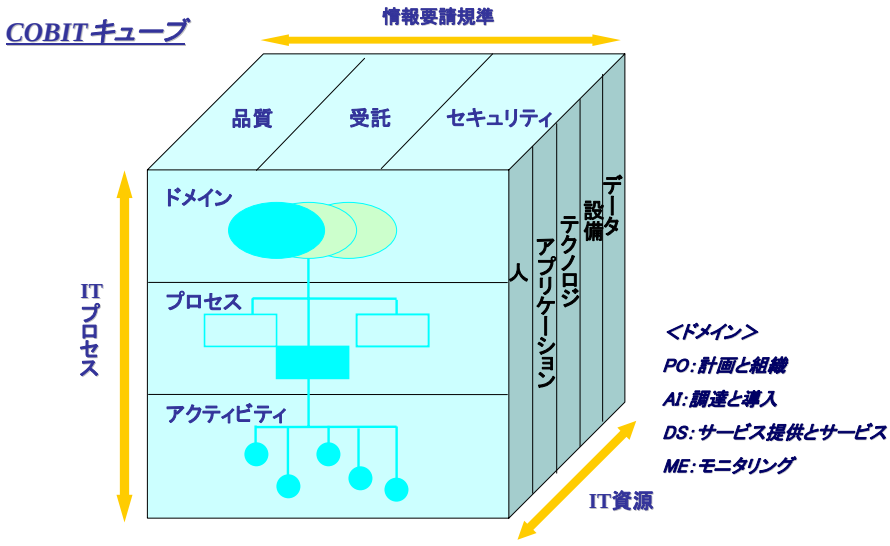
会社レベル	業務レベル	COSO構成要素 / COBIT	統制環境	リスク評価	統制活動	情報と伝達	モニタリング
		計画と組織					
●		PO1:IT戦略計画の策定	●	●		●	●
●		PO2:情報アーキテクチャの定義			●	●	
		PO3:技術指針の決定					
●		PO4:IT組織とそのかかわりの定義	●			●	
		PO5:IT投資の管理					
●		PO6:マネジメントの実現と指針の展開	●			●	●
●		PO7:人的資源の管理	●			●	
●		PO8:外部要求事項の遵守				●	●
●		PO9:リスク評価		●			
		PO10:プロジェクト管理					
●		PO11:品質管理	●		●	●	●
		調達と導入					
		AI1:コンピュータ化対応策の明確化					
	●	AI2:アプリケーションソフトウェアの調達と保守			●		
	●	AI3:技術インフラの調達と保守			●		
	●	AI4:運用、利用手順の作成と維持			●	●	
	●	AI5:システムの導入と導入責任			●		
	●	AI6:変更管理			●		●
		サービス提供とサポート					
	●	DS1:サービスレベルの定義と管理	●		●		●
	●	DS2:サードパーティのサービスの管理	●	●	●		●
●		DS3:成長と能力（キャパシティ）の管理			●		●
		DS4:継続的なサービスの確保					
	●	DS5:システムセキュリティの保証			●	●	●
		DS6:コストの特定と配賦					
●		DS7:利用者の教育と研修	●			●	
		DS8:利用者に対する支援と助言					
	●	DS9:構成管理			●	●	
	●	DS10:問題と障害の管理			●	●	●
	●	DS11:データ管理			●	●	
●		DS12:施設管理		●			
		モニタリング					
●		ME1:プロセスのモニタリング				●	●
●		ME2:内部統制の十分性の評価					●
●		ME3:独立した第3者の保証	●				●
●		ME4:独立監査の実施					●

IT Contorol Objectives For Sarbanes-Oxley April 2004 (IT Governance Institute) より作成

OGIS-RI

COBITの概要（イメージ）

COBITキューブ



<ドメイン>

PO：計画と組織

AI：調達と導入

DS：サービス提供とサービス

ME：モニタリング

OGIS-RI

明確な導入方法論の必要性

J-SOX法への適用初年度対応段階

比較的リソースが潤沢

しかし

- 人的
- 予算的
- 時間的

監査が続く限り対応が必要

導入初年度以降

リソースが限定的

- 限られた人員
- そもそもプロジェクトメンバー以外に理解可能？
- プロジェクトメンバー以外が実践可能？
- 年度内における定期的な監査（〆あり）
- 成果物の使い廻しが可能か？
（業務フローのBPRへの2次利用等）

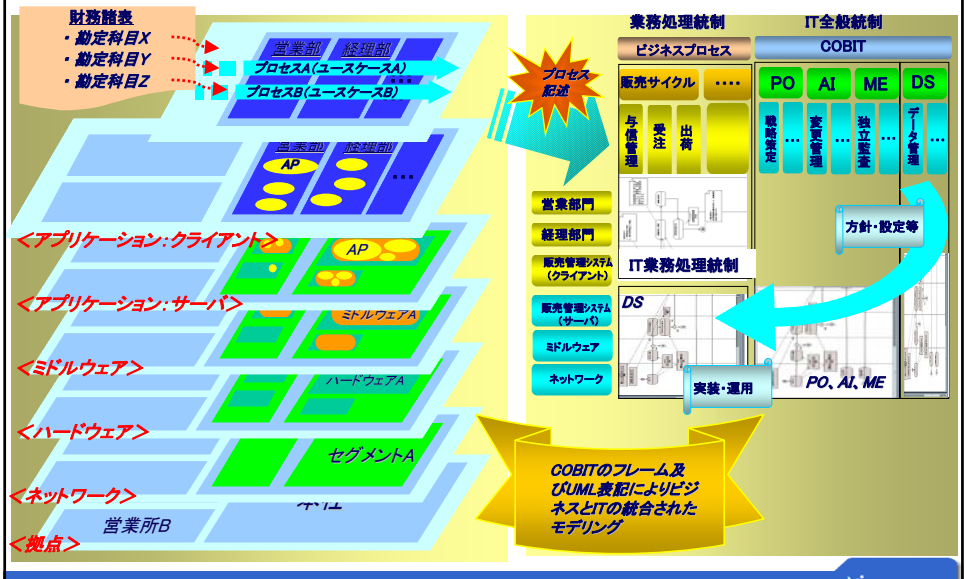
etc.

内部統制監査の有効性と効率性の両立

導入以降の運用を見据えた体系的かつ明確な方法論の必要性

OGIS-RI

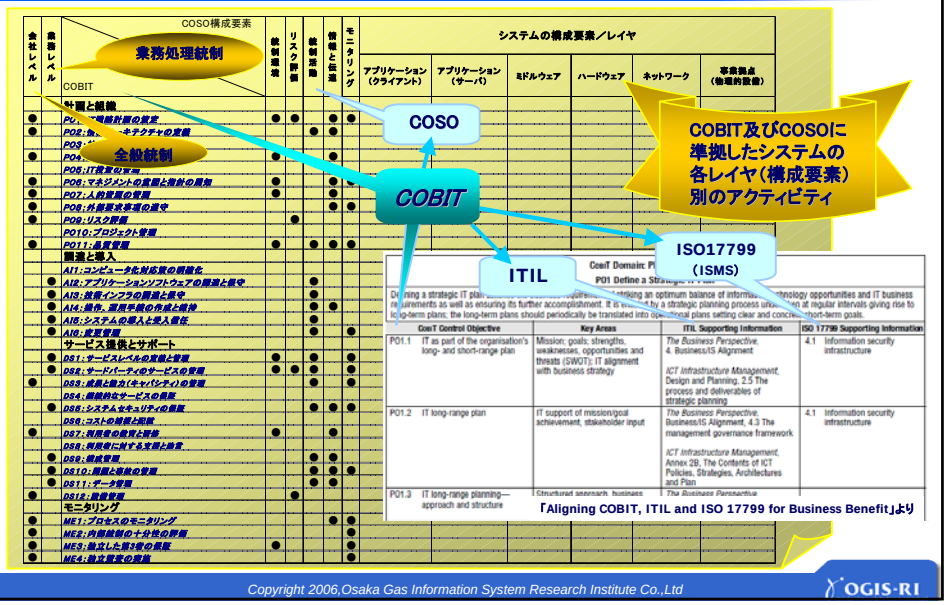
人間系業務とIT系業務の統合的表現
～COBITとUMLによる～



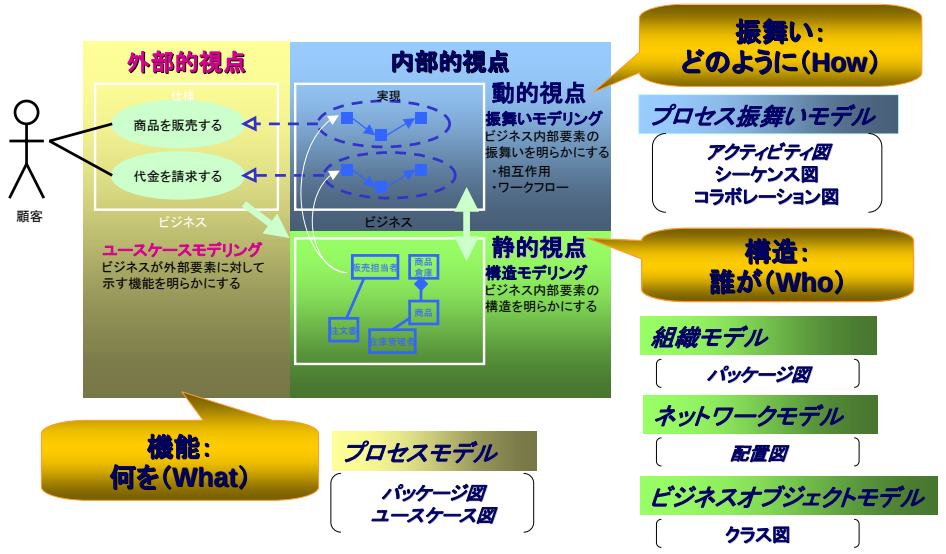
OGIS-RI

IT系業務の全般統制の記述

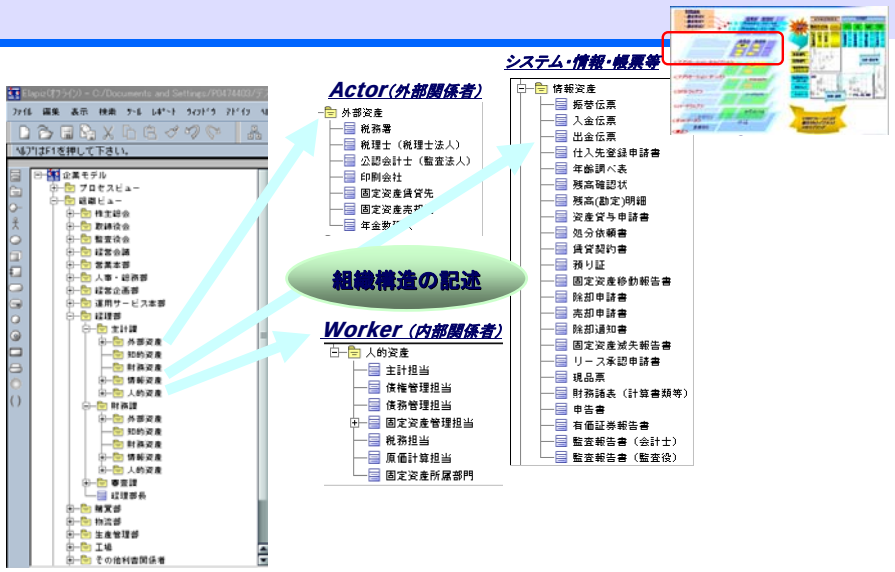
IT系業務の全般統制の整備



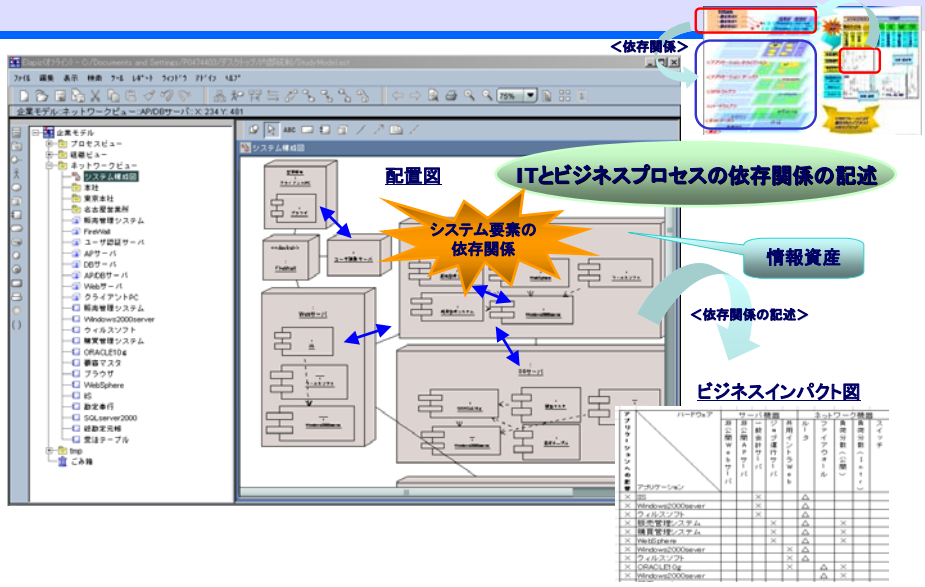
UMLによるビジネスプロセスのモデリング（文書化）概要



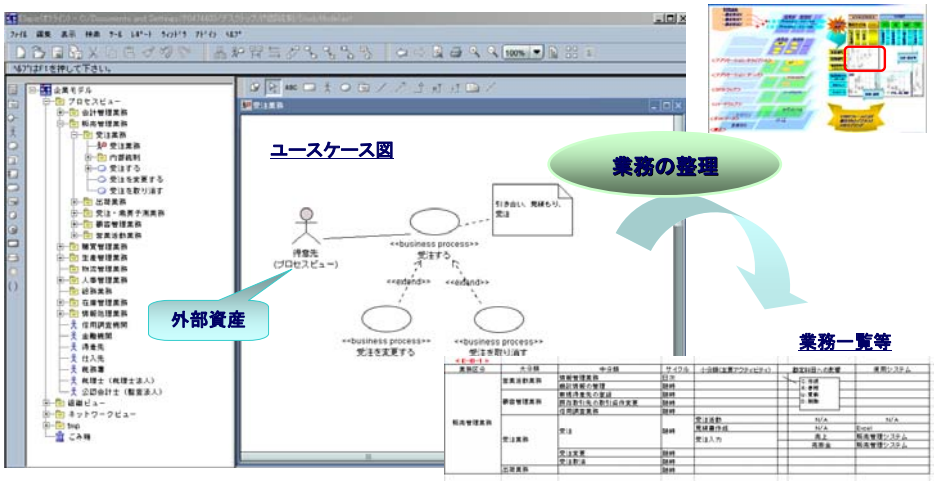
内部統制の文書化：UMLによる組織構造の記述



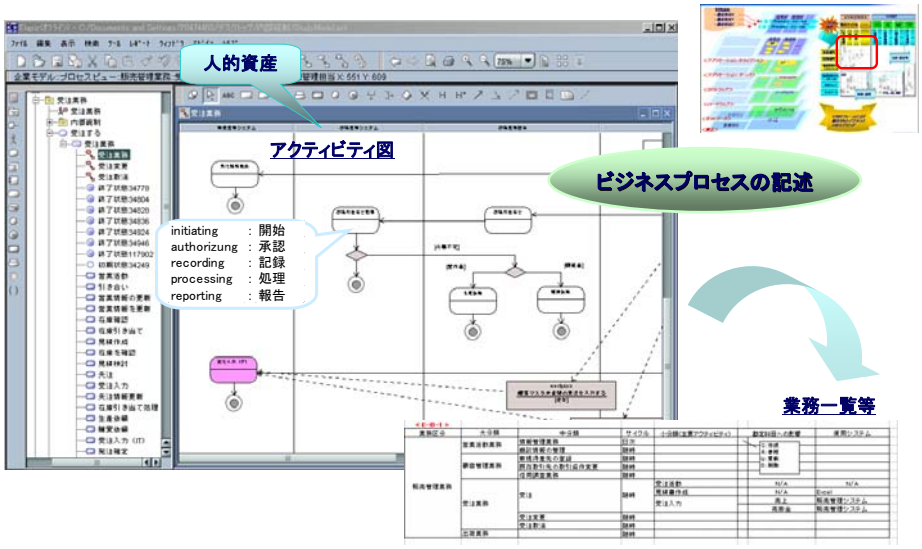
内部統制の文書化：UMLによるシステム構成の記述



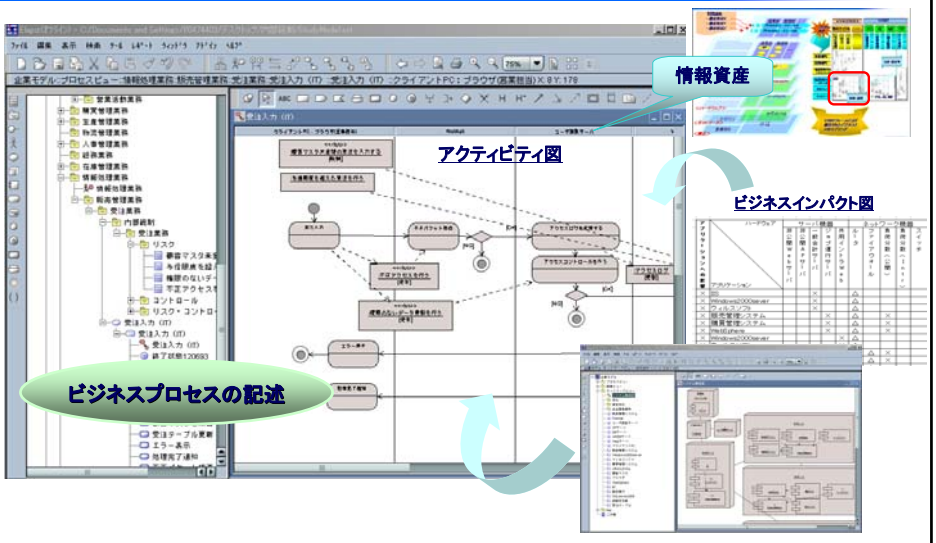
内部統制の文書化：UMLによるビジネスプロセスの記述



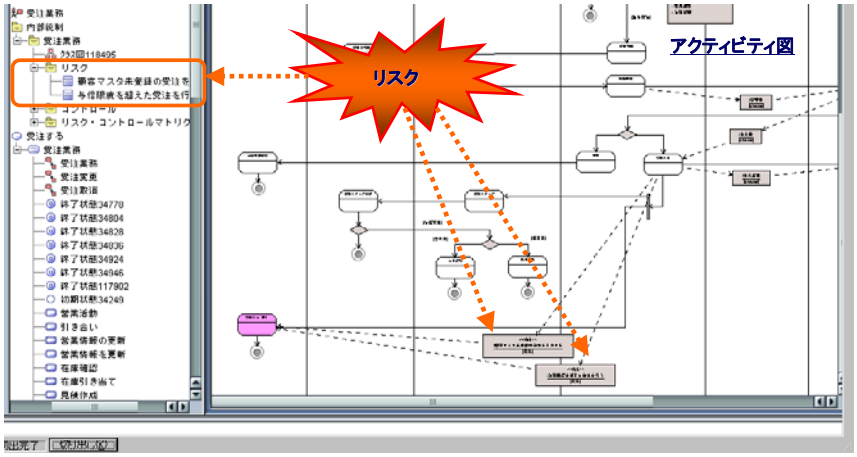
内部統制の文書化：UMLによるビジネスプロセスの記述



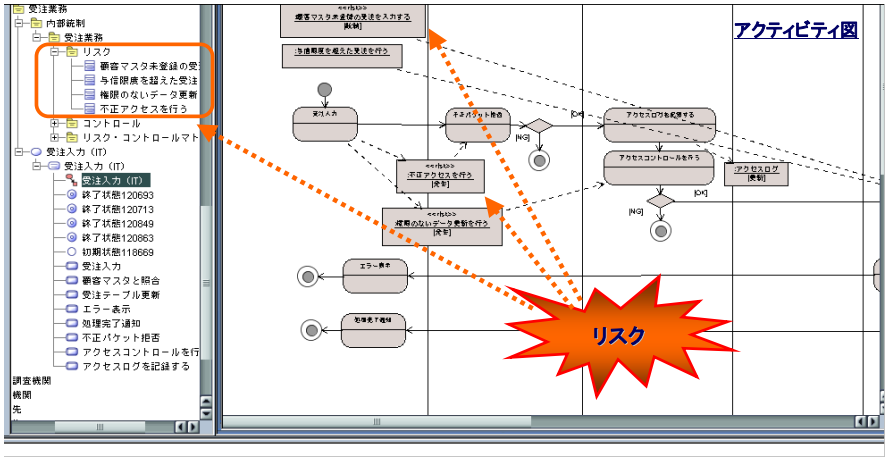
内部統制の文書化：UMLによるビジネスプロセス（システム）の記述



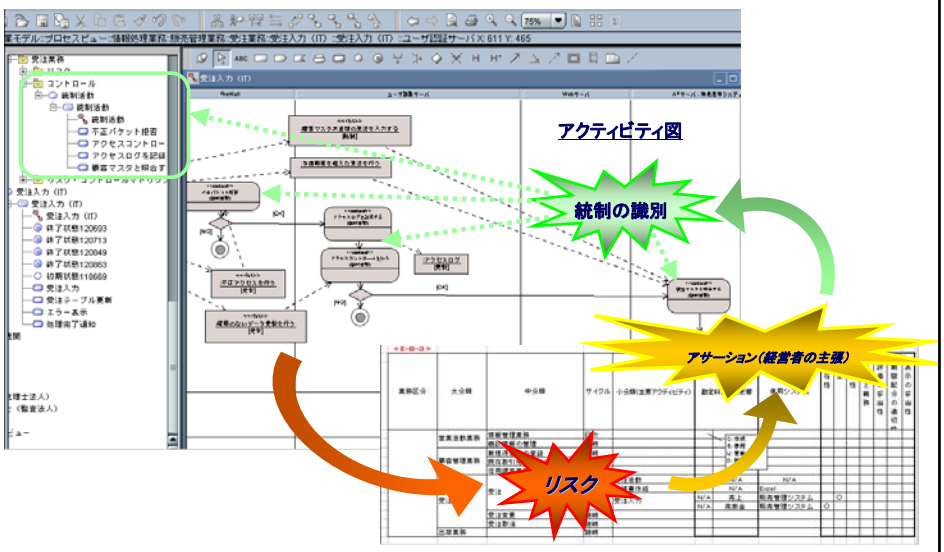
内部統制の文書化：UMLによるビジネスプロセス記述 ：リスクの識別（業務）



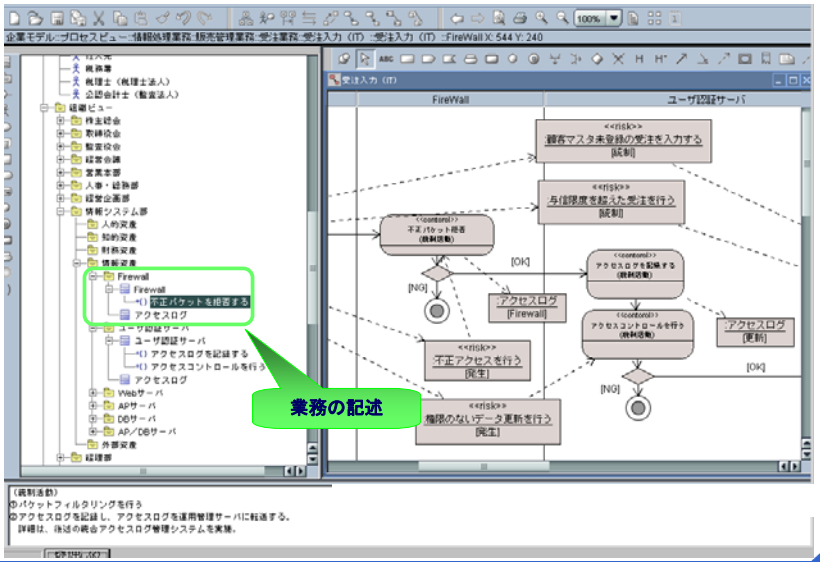
内部統制の文書化：UMLによるビジネスプロセス記述 ：リスクの識別（システム）



内部統制の文書化：UMLによるビジネスプロセス記述 ：統制の識別



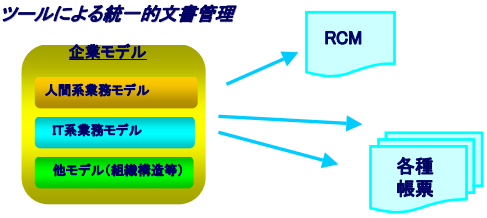
内部統制の文書化：UMLによるビジネスプロセス記述 ：職務の記述



要求される文書管理機能（現在作業中）

- ✓ ***RCM（リスク・コントロール・マトリクス）出力機能***
  - ✓ 作成したモデルからのRCMの出力が可能（CSV出力→EXCEL取り込み）
- ✓ ***その他の機能***
  - ✓ 特定の指定したリスクが潜在する業務活動の一覧出力
    ⇒架空受注というリスクはどこの誰の業務活動に潜在しているか　etc.
  - ✓ 特定の帳票や情報を作成・参照・更新・削除する業務活動の一覧出力
    ⇒受注情報を更新している業務活動は、誰がどのように行っているか　etc.
  - ✓ 勘定科目を更新する業務活動の一覧出力
    ⇒売掛金は、誰が（システムを含む）どのように行っているか　etc.

ツールによる統一的文書管理



ご清聴ありがとうございました