

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
株式会社オーガス総研
ビジネスプロセスモデリング部

米国におけるSOX法適用の背景

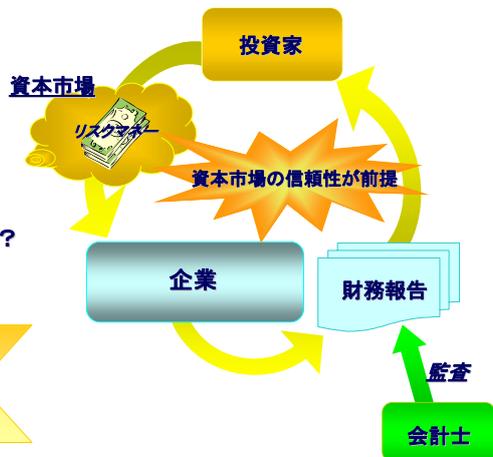
米国における会計不正(エンロン・ワールドコム)

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



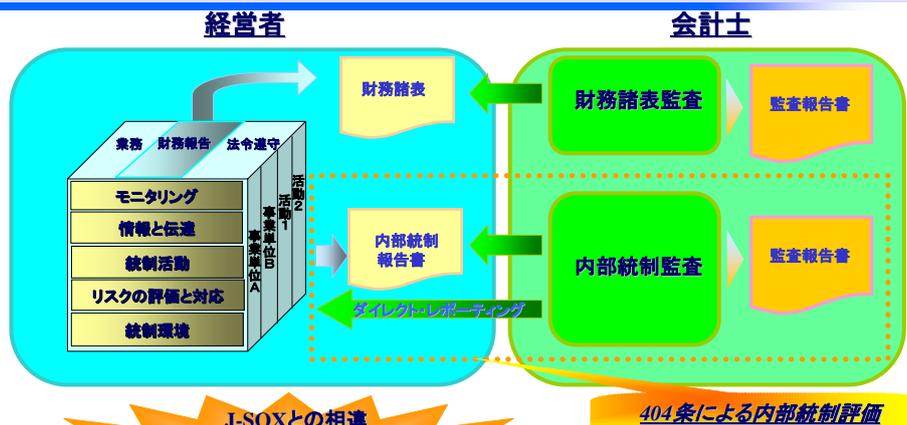
SOX法の内容



Copyright 2006, Osaka Gas Information System Research Institute Co., Ltd

OGIS-RI

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

404条による内部統制評価

Copyright 2006, Osaka Gas Information System Research Institute Co., Ltd

OGIS-RI

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

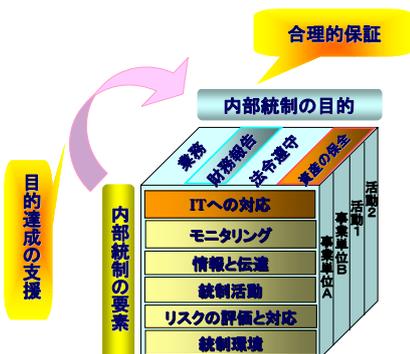
企業会計審議会：内部統制部会の基準案より



Copyright 2006, Osaka Gas Information System Research Institute Co., Ltd

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)

Copyright 2006, Osaka Gas Information System Research Institute Co., Ltd

OGIS-RI

内部統制監査におけるIT統制の重要性

「全般統制は、通常ITに関するインフラ単位で評価することになります。例えば、...、監査人としては、それぞれのアプリケーション・システムがどのような基盤(インフラ)の上で動いているかを把握することがまず必要となります。」
 (IT委員会報告第3号 Q&Aドラフト 日本公認会計士協会)

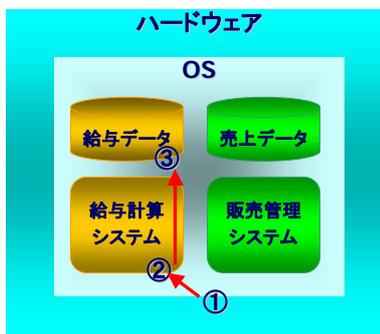
業務プロセスとそれが依存するアプリケーション、さらにそれが依存するITインフラの識別が必要



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

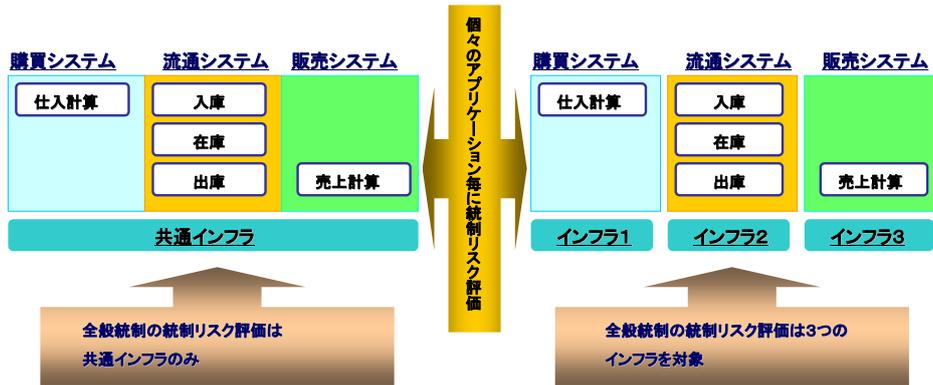


IFAC(世界会計士連盟) Controlling Computers in Business : Logical Access Security より作成

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

Copyright 2006, Osaka Gas Information System Research Institute Co., Ltd

OGIS-RI

内部統制の文書化の全体像とIT



Copyright 2006, Osaka Gas Information System Research Institute Co., Ltd

OGIS-RI

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、GSF (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
 - ✓ GOSOとの整合性
 - ✓ システム監査においても参照

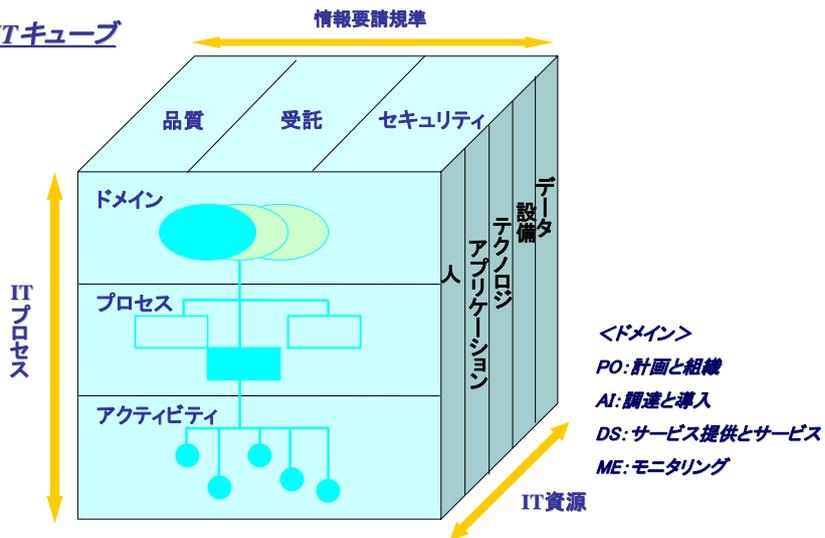
IT全般統制のフレームワークとして利用

会社レベル	COBIT	COBIT構成要素	リスク評価	統制環境	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: 組織アーキテクチャの策定				
		PO3: 業務プロセスの決定				
		PO4: IT戦略とその他のおしりの策定				
		PO5: IT投資の策定				
		PO6: マネジメントの環境と方針の策定				
		PO7: 人的資源の策定				
		PO8: 外部委託管理の策定				
		PO9: IT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: コンピュータ化形質の継続性				
		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: 操作、運用プロセスの作成と維持				
		AI5: システムの導入と変更管理				
		AI6: 変更管理				
		サービス提供とサポート				
		DS1: サービスレベルの策定と管理				
		DS2: サービスレベルのサービスの管理				
		DS3: 資産と損失(キャピタル)の管理				
		DS4: 継続的なサービスの提供				
		DS5: システムセキュリティの策定				
		DS6: コストの調達と削減				
		DS7: 資産の確保と管理				
		DS8: 資産の確保と管理				
		DS9: 資産の確保と管理				
		DS10: 資産の確保と管理				
		DS11: データ管理				
		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: 監査した監査者の策定				
		ME4: 監査計画の策定				

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

COBITの概要 (イメージ)

COBITキューブ



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

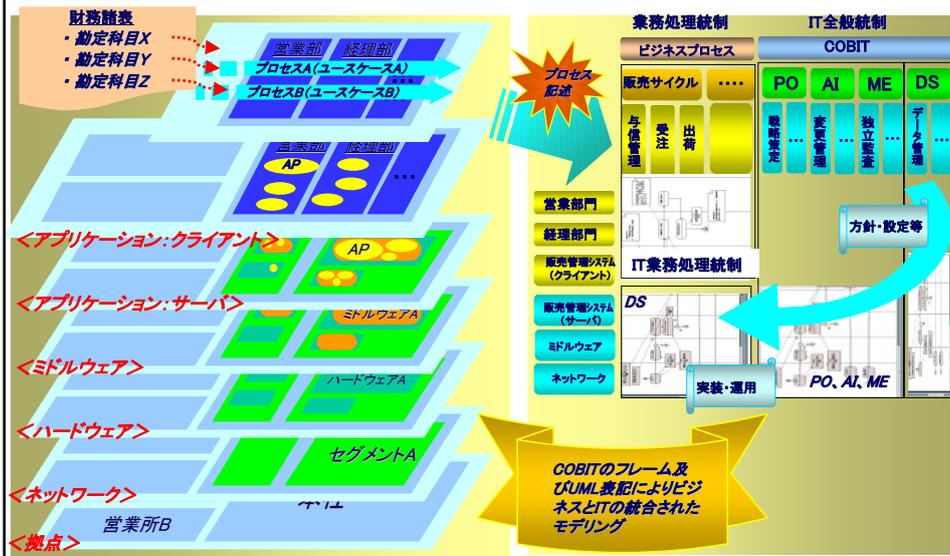
- 限られた人員
- そもそもプロジェクトメンバー以外に理解可能?
- プロジェクトメンバー以外が実践可能?
- 年度内における定期的な監査(あり)
- 成果物の使い回しが可能か?
(業務フローのBPRへの2次利用等)

etc.

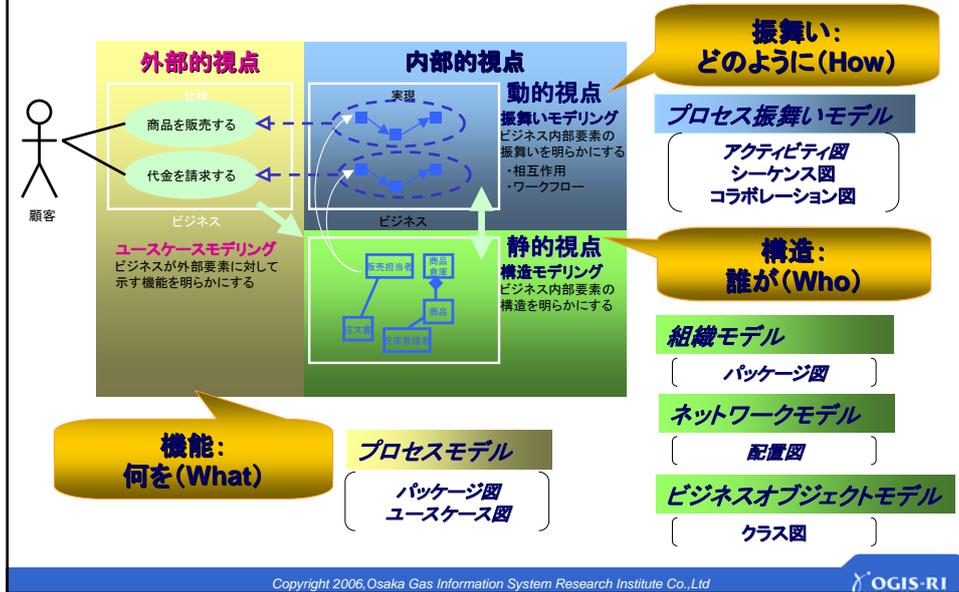
内部統制監査の有効性と効率性の両立

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

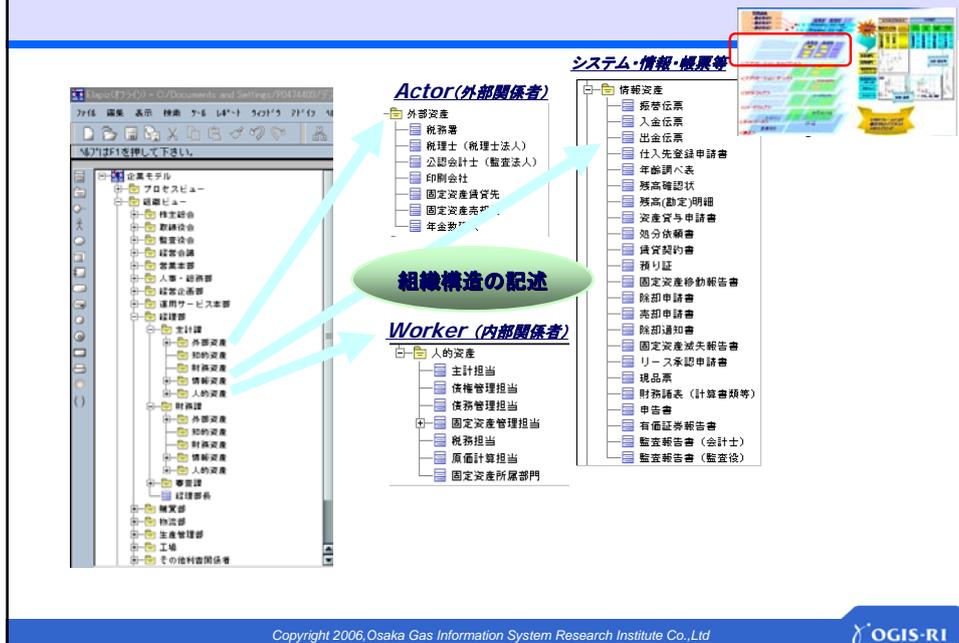
人間系業務とIT系業務の統合的表現 ~COBITとUMLによる~



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

配置図 **ITとビジネスプロセスの依存関係の記述**

システム要素の依存関係

情報資産

＜依存関係の記述＞

ビジネスインパクト図

システム要素	IT資産	業務プロセス	IT資産	業務プロセス	IT資産	業務プロセス
APサーバー	○	○	○	○	○	○
Webサーバー	○	○	○	○	○	○
データベース	○	○	○	○	○	○
ネットワーク	○	○	○	○	○	○
OS	○	○	○	○	○	○
アプリケーション	○	○	○	○	○	○
業務プロセス	○	○	○	○	○	○
外部資産	○	○	○	○	○	○

Copyright 2006, Osaka Gas Information System Research Institute Co., Ltd

OGIS-RI

内部統制の文書化: UMLによるビジネスプロセスの記述

ユースケース図 **業務の整理**

外部資産

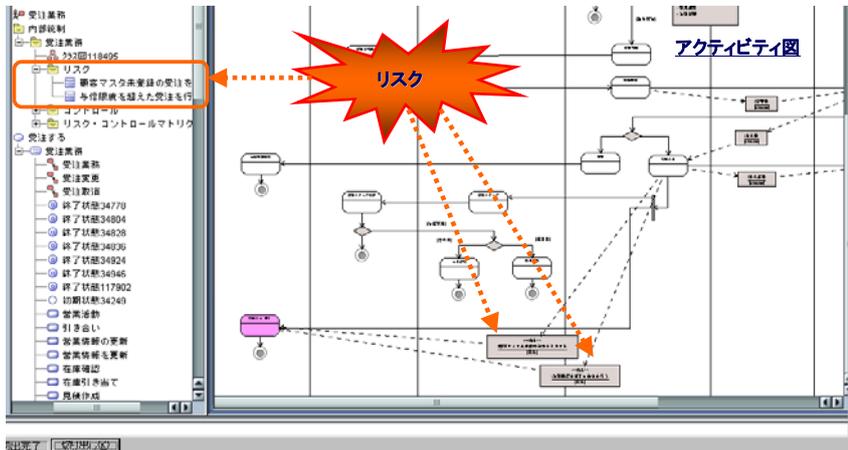
業務一覧等

業務ID	業務名	業務種別	システム	IT資産(業務プロセス)	業務種別(業務)	業務ID
001	業務管理業務	管理	業務管理システム	業務管理システム	業務管理システム	001
002	業務管理業務	管理	業務管理システム	業務管理システム	業務管理システム	002
003	業務管理業務	管理	業務管理システム	業務管理システム	業務管理システム	003
004	業務管理業務	管理	業務管理システム	業務管理システム	業務管理システム	004
005	業務管理業務	管理	業務管理システム	業務管理システム	業務管理システム	005
006	業務管理業務	管理	業務管理システム	業務管理システム	業務管理システム	006
007	業務管理業務	管理	業務管理システム	業務管理システム	業務管理システム	007
008	業務管理業務	管理	業務管理システム	業務管理システム	業務管理システム	008
009	業務管理業務	管理	業務管理システム	業務管理システム	業務管理システム	009
010	業務管理業務	管理	業務管理システム	業務管理システム	業務管理システム	010

Copyright 2006, Osaka Gas Information System Research Institute Co., Ltd

OGIS-RI

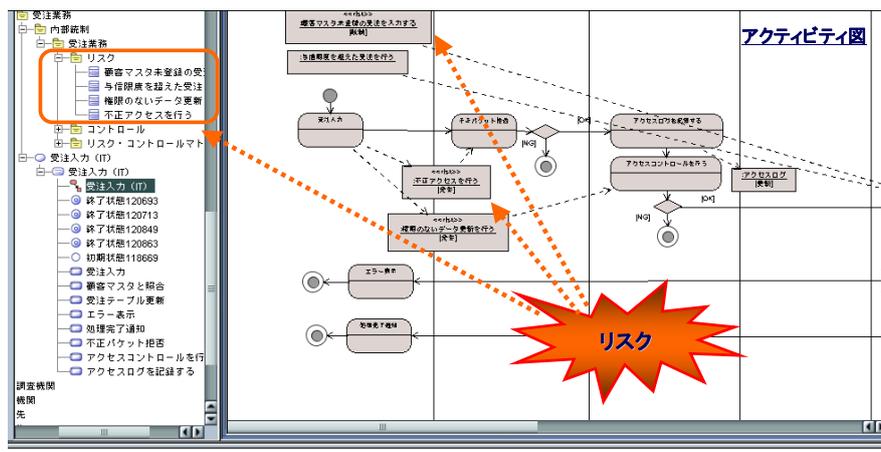
内部統制の文書化: UMLによるビジネスプロセス記述
: リスクの識別(業務)



Copyright 2006, Osaka Gas Information System Research Institute Co., Ltd

OGIS-RI

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)



Copyright 2006, Osaka Gas Information System Research Institute Co., Ltd

OGIS-RI

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

The screenshot displays a UML activity diagram titled 'アクティビティ図' (Activity Diagram) for the process 'Firewall'. The diagram shows a flow of activities including '不正パケット検出' (Detecting malicious packets), 'アクセスログを記録する' (Recording access logs), and '不正アクセスを行う' (Performing unauthorized access). Annotations include:

- 統制の識別** (Control Identification): A green starburst pointing to control elements like '<<risk>>不正パケット検出' and '<<risk>>不正アクセスを行う'.
- アサーション(経営者の主張)** (Assertion/Management's Assertion): A yellow starburst pointing to an assertion element '<<assertion>>不正アクセスを防止する'.
- リスク** (Risk): A red starburst pointing to a risk element '<<risk>>不正アクセスを行う'.

Below the diagram is a table with columns for '業務区分' (Business Division), '大分類' (Major Classification), '中分類' (Sub-classification), 'サイタル' (Saitaru), and '全業務(業務プロセス)の識別' (Identification of all business processes). The table lists various business processes and their classifications.

Copyright 2006, Osaka Gas Information System Research Institute Co., Ltd. OGIS-RI

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

The screenshot displays a UML activity diagram titled 'アクティビティ図' (Activity Diagram) for the process 'Firewall'. The diagram shows a flow of activities including '不正パケット検出' (Detecting malicious packets), 'アクセスログを記録する' (Recording access logs), and '不正アクセスを行う' (Performing unauthorized access). Annotations include:

- 業務の記述** (Business Description): A green starburst pointing to the activity '不正パケット検出'.

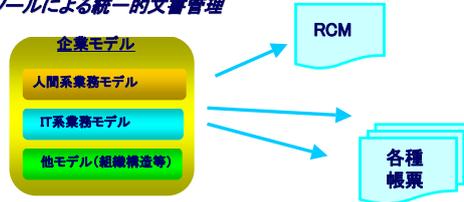
Below the diagram is a table with columns for '業務区分' (Business Division), '大分類' (Major Classification), '中分類' (Sub-classification), 'サイタル' (Saitaru), and '全業務(業務プロセス)の識別' (Identification of all business processes). The table lists various business processes and their classifications.

Copyright 2006, Osaka Gas Information System Research Institute Co., Ltd. OGIS-RI

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



Copyright 2006, Osaka Gas Information System Research Institute Co., Ltd

OGIS-RI

ご清聴ありがとうございました

Copyright 2006, Osaka Gas Information System Research Institute Co., Ltd

OGIS-RI