リーマンショックに立ち向うガバナンス
新COSOの簡単な理解
米国中央政府のGreen　Reportを中心として

日本ITガバナンス協会会長
システム監査学会会長
松尾明

本日の講演の目的

- CLICK
- CHANGE
- OR
- DIE
- の理解

- これが新COSOの本質

新COSO

- ２０１３年５月１４日に最終版公表
- ２０１４年１２月１５日までに移行を求める

- リーマンショツク　２００８年９月１５日

20年ぶりの改訂の理由

- ビジネスおよび業務環境の劇的な変化

- テクノロジー主導的で国際的で複雑になることが
- 組織の事業目的の達成可能性を高め、ビジネスおよび業務環境の変化に適応出来るように
- 内部統制システムの有効かつ効率的な構築および維持が出来るように
- 内部統制システムのインテグリテイ（誠実性と訳されているが本講演ではインテグリテイとする）に関する

いっそうの透明性および説明責任を求めて

利害関係者（Stakeholder）が関与度合いを高めている

Green　Reportの定義　1

- COSO本文に無い、定義の幾つかを示す

- Green book　米国中央政府の内部統制基準、
  （州、市町村、NPO、社団等への適用もあり得る。ただし、これらの事業体の経営者が適切な法規やルールに従い定める。）
- 内部統制（Internal　Control）　内部統制は、有効な内部統制システムを導入するための総括的なフレームワークを示すものであり、事業体の目的の全てをカバーする（業務運用、報告、遵守性）。

Green　Reportの定義　２

- 内部統制システム
  - 方針決定者や事業管理者は、事業体のミツションを達成するための説明責任を高めることに努めている。そのための成功要因は、有効な内部統制システムの導入である。
  - 有効な内部統制システムの導入により、環境変化、ディマンドの展開、新たな優先課題への対応を支援することができる。

Green Reportの定義 3

– 事業の変更が行われ、事業体が事業運用のプロセスを改善し、新たなテクノロジーを導入するのであれば、

経営者は、継続的に内部統制システムを評価し、それが有効で最新化（Update）されていることを確かめること。

Green　Reportの定義　４

- ベースライン（基準点ラインと訳されているが、ベースラインと本講演ではする。）
- 内部統制システムのデザイン時の判断基準とある特定時点の状況との差異
- 課題（Issue）および検出事項（Difficiencies）とも言える。

Green　Reportの定義　５

- 経営者（Management）

事業体の担当者で、直接的にある組織の全ての活動に責任を負う者、

（活動には、内部統制システムのデザイン、導入、有効なその運用も含まれる）。

Green　Reportの定義　６

- 指針（プリンスパル）とは、法規やルールで従わなければいけないもの、従うことが出来るもの

- 原則と訳されているが、この講演では、方向性を共有することに、重みを置き、指針とした。

Green　Reportの定義　7

- 組織（構造）（Organizational Structure）
- 本業ユニット、本業プロセス、その他の目標達成のための構造マネジメント。

１７の指針

- ５要素は変わらず
  - 統制環境　　５指針
  - リスク評価　　４指針
  - 統制活動　　３指針
  - 情報と伝達　　３指針
  - モニタリング活動　　２指針

計　　１７指針

１７の指針　１

- 統制環境

1.　組織は、インテグリテイと倫理観に対する
　コミットメントを表明する。

２．取締役会は、経営者から独立していることを
　表明し、かつ、内部統制の整備および運用状況について
　　監督を行う。

３．経営者は、取締役会の監督の下、内部統制の目的を
　　達成するにあたり、組織構造、報告経路および適切な
　　権限と責任を確立する。

１７の指針　２

- 統制環境
- ４、組織は、内部統制の目的に合わせて、有能な個人を惹きつけ、育成し、かつ、維持することに対するコミットメントを表明する。
- ５、組織は、内部統制の目的を達成するに当たり、内部統制に対する責任を個々人に持たせる。

１７の指針　３

- リスク評価
- ６、組織は、内部統制の目的に関連するリスクの識別と評価が出来るように、十分な明確さを備えた内部統制の目的を明示する。
- ７．組織は、自らの目的の達成に関連する事業体全体にわたるリスクを識別し、当核リスクの管理の仕方を決定するための基礎としてリスクを分析する。

１７の指針　４

- リスク評価
- ８、組織は、内部統制目的の達成に対する

リスクの評価において、不正の可能性について検討する。

９、組織は、内部統制システムに重大な影響を及ぼし得る変化を識別し、評価する。

１７の指針　５

- 統制活動
- １０、組織は、内部統制の目的に対するリスクを許容可能な水準まで低減するのに役立つ統制活動を選択し、整備する。
- １１、組織は、内部統制の目的の達成を支援するテクノロジーに関する全般的統制活動を選択し、整備する。

１７の指針　６

- 統制活動
- １２．組織は、期待されていることを明確にした方針

および方針を実行するための手続を通じて、統制活動を展開する。

１７の指針　７

- 情報と伝達
- １３、組織は、内部統制が機能することを、

支援する関連性のある質の高い情報を入手または作成して利用する。

- １４、組織は、内部統制が機能するために必要な、内部統制の目的と内部統制に対する責任を含む情報を組織内部に伝達する。

１７の指針　８

- 情報と伝達
- 15,組織は、内部統制が機能することに影響を及ぼす事項に関して、外部の関係者との間での情報伝達を行う。

１７の指針　９

- モニタリング活動
- １６、組織は、内部統制の構成要素が存在し、機能していることを確かめるために、日常的評価および・または独立的評価を選択し、整備および運用する。
- １７、組織は、適時に内部統制の不備を評価し、必要に応じて、それを適時に上級経営者および取締役会を含む、是正措置を講じる責任を負う者に対して伝達する。

判断規準のデザイン　1

- 事業情報システムのデザイン
  - 事業体の目的とリスクに対応
- 適切な統制活動のデザイン
  - 事業体の情報システムを事業体の目的とリスクに対応
- 情報テクノロジー基盤のデザイン
  - 情報テクノロジー基盤に対する統制活動をデザイン

判断規準のデザイン　２

- セキュリテイマネジメントのデザイン
  - 事業体の情報システムのセキュリテイマネジメントの統制活動をデザインする
- 情報テクノロジの調達、展開、維持のデザインための
- これらのための統制活動をデザインする。

判断規準のデザイン　３

- 事業体の情報システムのデザイン
- 　業務処理統制の判断規準
- 　完全性
- 　正確性
- 　正当性

判断規準のデザイン　４

- 情報システム活動のデザイン
- 全般統制
  - 完全性
  - 効率性
  - 正当性
  - 効率性

モニタリング

- ベースラインを継続的にモニタリングすることを求めている、
- あるべき姿のデザインとその現状のリアルタイムに近い把握がグローバルな市場では求められている
- TOGAF9があるべき姿のデザインの国際標準です。

オブジェクトとCOBIT

- オブジェクトとは
  - Objectは理解すれば、なぜ理解できないかわからなくなる

- COBITとのかかわり
  - １９９３年パリの会議でのオブジェクトの提案
  - ２００８年LAの会議でのオブジェクトの提案

Objectの定義

- **1.** Something perceptible by one or more of the senses, especially by vision or touch; a material thing.
- **2.** A focus of attention, feeling, thought, or action: an object of contempt.
- **3.** The purpose, aim, or goal of a specific action or effort: the object of the game.
- **4.** *Grammar* **a.** A noun, pronoun, or noun phrase that receives or is affected by the action of a verb within a sentence.
- **b.** A noun or substantive governed by a preposition.
- **5.** *Philosophy* Something intelligible or perceptible by the mind.
- **6.** *Computer Science* A discrete item that can be selected and maneuvered, such as an onscreen graphic. In object-oriented programming, objects include data and the procedures necessary to operate on that data.

論議１　オブジェクト

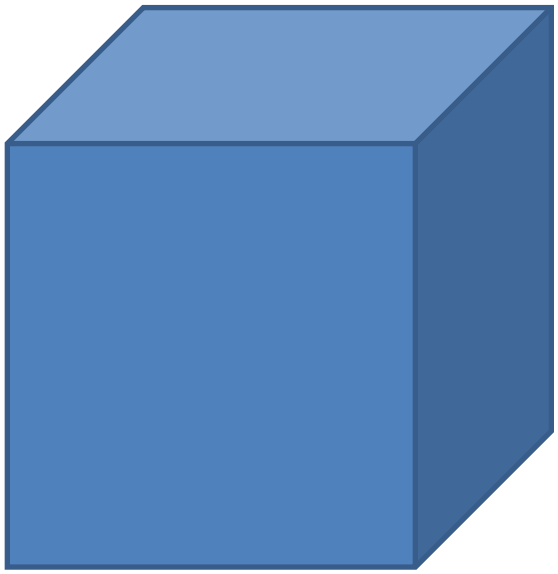
- モノとしてのObject
- コンテンツはObjectか
- ソフトは、ネットはObjectか

COBITの変化

- 1996　COBIT1
- 1998　COBIT2　コントロール
- 2000　COBIT3　マネジメント
- 2005　COBIT4　ITガバナンス
- 2007　COBIT4.1　VALIT.RISKIT
- 2012　COBIT5　Enterprise　IT　ガバナンス
- 2013　COBIT5　ビジネスト統合、エンネイブラー

1993年6月の提案

- まとめの方向性のくくり方としてのObject



COBIT1での対象範囲

・前向き品質の検討

経営の有効性、効率性

・データ管理の本質的な検討

情報、知識への取り組み

有用性
イノベーションについて

- プロダクトイノベーション
- プロセスイノベーション
- 不確かな、人的創造性と機会の膨大なプロセスのなかから生まれる
- 核となる　Intellectual　or　service competencies　廻りに戦略を高める

システム監査学会の取り組み

- ドラッカーの遺言の勉強会
  - 法政大学で開催の予定
- オープングループセミナー
  - ２回目を３月に予定、ソニー所氏
  - １回目は、藤枝氏２月１３日
- ３０周年記念行事
  - 本年に企画、来年度に実施

ISACA・ITGIの予定

- アジアCACS（ISACA）
  - ５月に予定、５月３０、３１日、浅草橋
  - 基調講演　三浦雄大　三浦雄一郎氏長男、
  - インド政府情報戦略コンサルタント　ビタルラジ氏

- ITGIコンファレンス
  - １０月開催は未定
- ３０周年事業

  東京支部は、５月２９日午後、浅草橋で予定

謝辞

- 討議への参加ありがとうございます。

- ご意見、ご連絡は、
  amatsuo@busi.aoyama.ac.jp
  へおよせください。