ITGI Japan

GOVERNANCE INSTITUTE

J-SOX対応とシステム監査の課題
～COBITの視点から～

2007.6.20

CISA,CIA
島田裕次

アジェンダ

- COBIT／COBIT for SOXの意義
- IT統制整備における実務上の課題
- ITガバナンスとIT統制の関係
- ITガバナンスの向上に向けて

COBIT/COBIT for SOXの意義

COBIT/COBIT for SOXの意義

- COBIT for SOXは、J－SOX対応で広く利用されている。
  - 米国SOX対応の影響
  - 監査法人、コンサルタントによる利用
- 経済産業省『システム管理基準』、『同追補版』でも参照されている。
- COBITは、ITガバナンス確立のためのグローバルスタンダードとしての意義がある。

COBIT/COBIT for SOXの活用状況

業務プロセスの見直しに当たって参考にした公的基準・フレームワーク		参考にした割合
1位	COSOフレームワーク	56．6%
2位	情報セキュリティ管理基準、同監査基準	50．3%
3位	システム管理基準、同監査基準	45．5%
4位	COBIT	45．4%
5位	COBIT for SOX	43．5%
6位	JIS Q 15001:2006	34．6%
7位	JIS Q 27001:2006(ISO/IEC:27001:2005)	30．3%
8位	ITIL	27．0%
9位	FISCのガイドライン	9．9%
10位	CMMI	9．9%

回答数491社の合計

（財）日本情報処理開発協会「ITと内部統制に関する調査研究報告書」2007年3月。

大企業での利用が進むCOBIT

業務プロセスの見直しに当たって参考にした公的基準・フレームワーク		参考にした割合
1位	COSOフレームワーク	68．0%
2位	COBIT for SOX	57．4%
3位	COBIT	57．2%
4位	情報セキュリティ管理基準、同監査基準	54．2%
5位	システム管理基準、同監査基準	50．0%
6位	ITIL	39．0%
7位	JIS Q 15001:2006	34．3%
8位	JIS Q 27001:2006(ISO/IEC:27001:2005)	32．3%
9位	FISCのガイドライン	13．6%
10位	CMMI	13．5%

1000人以上の企業（回答数199社）

（財）日本情報処理開発協会「ITと内部統制に関する調査研究報告書」2007年3月。

業種別に見たCOBITの利用状況

COBITの利用状況		
製造業	3位	49．4%
流通・物流業	2位	48．6%
金融・保険業	6位	42．9%
サービス業	6位	44．6%
建設業・その他	5位	28．6%
COBIT for SOXの利用状況		
製造業	4位	48．6%
流通・物流業	5位	42．5%
金融・保険業	4位	60．9%
サービス業	7位	37．5%
建設業・その他	6位	26．5%

（財）日本情報処理開発協会「ITと内部統制に関する調査研究報告書」2007年3月。

カスタマイズされるCOBIT

- 公的基準・フレームワークを自社プロセスに導入する場合には、カスタマイズして採用する企業が大半を占める。
  - COBIT
    - 回答147社のうち　66．7%はカスタマイズして採用
    - 9．5%は、ほぼ全編を採用
  - COBIT for SOX
    - 回答141社のうち、71．6%はカスタマイズして採用
    - 9．9%は、ほぼ全編を採用

（財）日本情報処理開発協会「ITと内部統制に関する調査研究報告書」2007年3月。

IT統制整備における実務上の課題

実施基準の課題

- 実施基準で求める内容やレベルが分からない。
  - 実施基準では、例が示されているが、会計監査人はどこまで拡大して解釈するのか。解釈の根拠が明確でない解釈は、適切ではないのではないか。
  - 実施基準の統制項目に示していない統制項目についても、企業側に求められる可能性がある。
- 実施基準には、財務統制以外の統制項目も含まれているのではないか。
  - 財務統制に必要な統制項目を適切に示しているわけではない。（そんなことは現実に難しいが・・・）
  - 財務統制では、アクセス管理と変更管理が重要である。
  - バックアップは、財務統制（財務情報の信頼性）と関係するのだろうか？今まで紙の帳簿、帳票のバックアップは取得していたのか？
- しかし、J-SOX対応では、実施基準が経営者評価および内部統制監査の拠り所となるので、実施基準をベースにIT統制項目を議論すべきでなはないか。
- ただし、後で説明する価値向上のためのIT統制項目（ITガバナンス）については、J-SOX対応とは一線を画して整備することが必要になる。

J-SOX対応の留意点

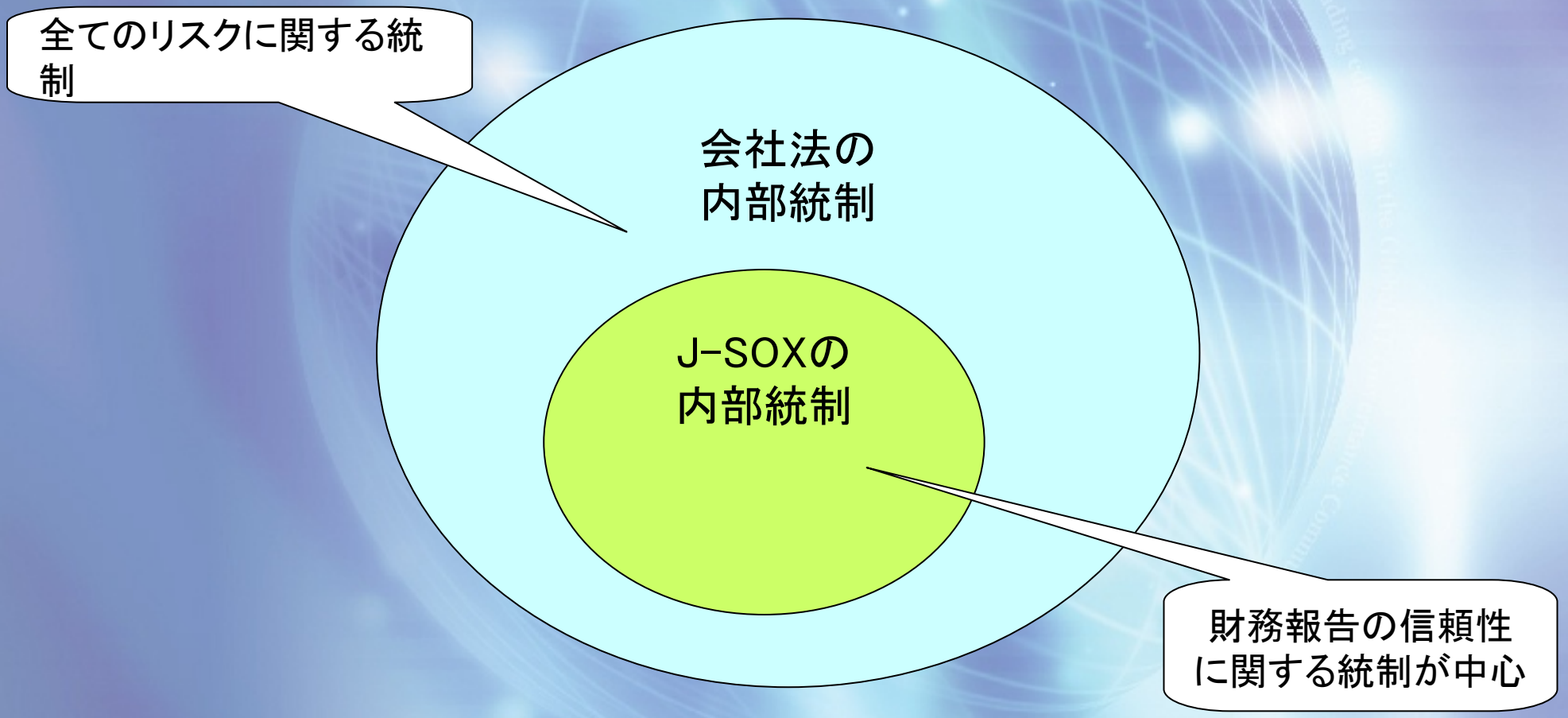
- 実施基準が求めるIT統制項目と、企業が本来整備すべきIT統制項目（ITガバナンスのための統制項目）を整理する。
  - IT統制を財務統制と財務統制以外に整理し、財務統制に絞る。
  - 実施基準で求めるIT統制項目に絞る。
  - ITガバナンスのためのIT統制項目は、経営者評価とは別のもとのする。
- IT統制項目の評価基準を決める。
  - 企業としてはどの程度の水準のIT統制を整備するのか、リスクとの関係を明確にした基準を決める。
  - 連結ベースでのリスクの把握・分析とコントロールの水準の統一
  - 代替コントロールの理解
  - 会計監査人との判断の違いは、リスクに基づいて対等の立場で議論する。
- リスク及びコントロールの標準化
  - コントロール水準の統一
  - IT統制の効率化
- 内部統制監査に上手に対応してゆくことも重要である。
  - 会計監査人が納得しやすい資料や記録を作成・保管する。
  - 財務統制以外のIT統制項目への質問に対しては、会計監査人の意図を確認する。
  - 内部統制に関する社内の教育も必要である。

実施基準と本来のIT統制項目

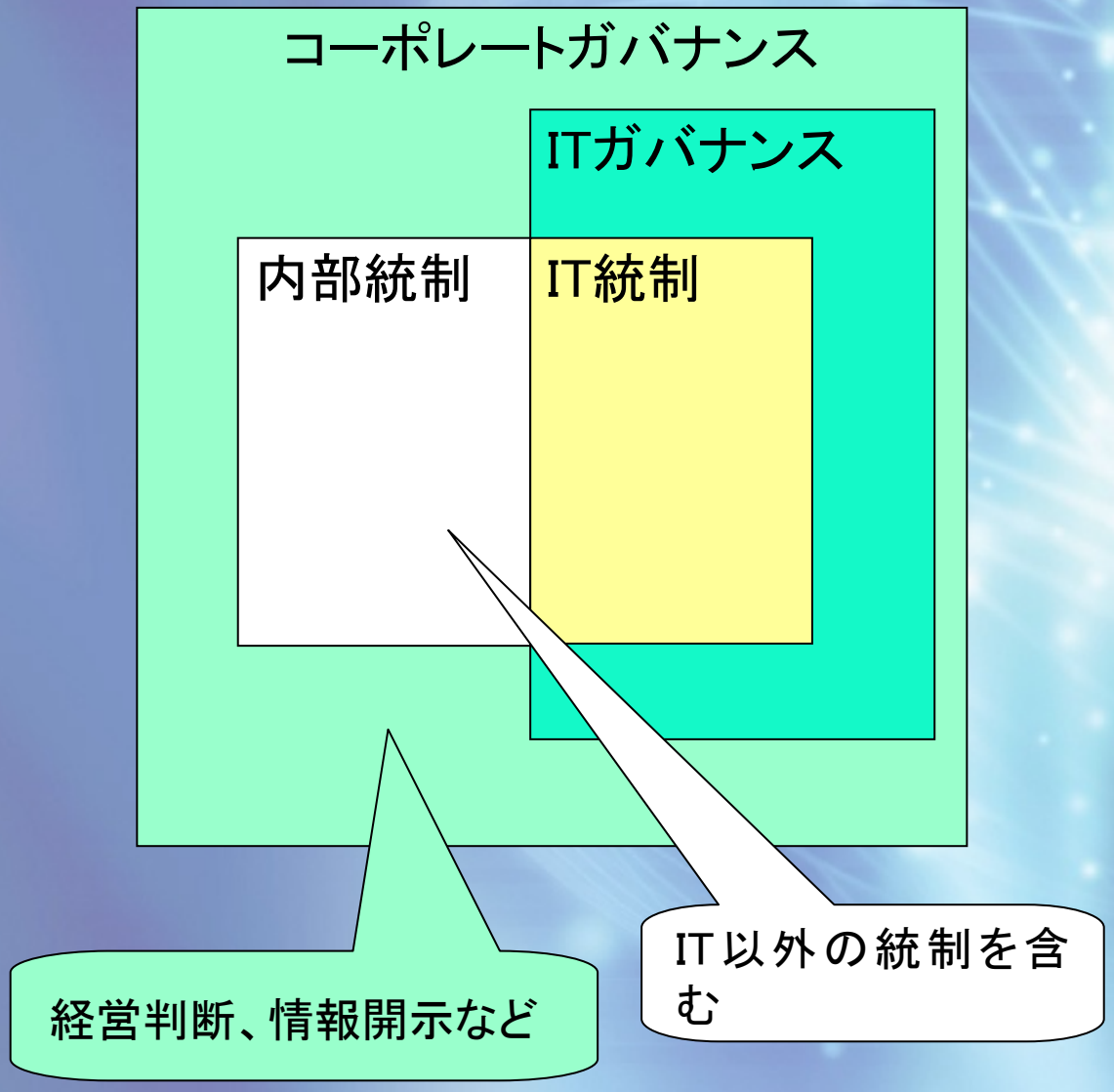
- 実施基準が求めるIT統制項目と、本来のIT統制項目を整理する。グレーゾーン（実施基準であいまいな部分、拡大解釈される部分）については、会計監査人との議論が必要ではないか。
- 実施基準を超える部分は、企業の努力部分である。この部分の不備は、内部統制報告書の根拠とはいえないのではないか。

ITガバナンスとIT統制の関係

J-SOXと会社法の内部統制



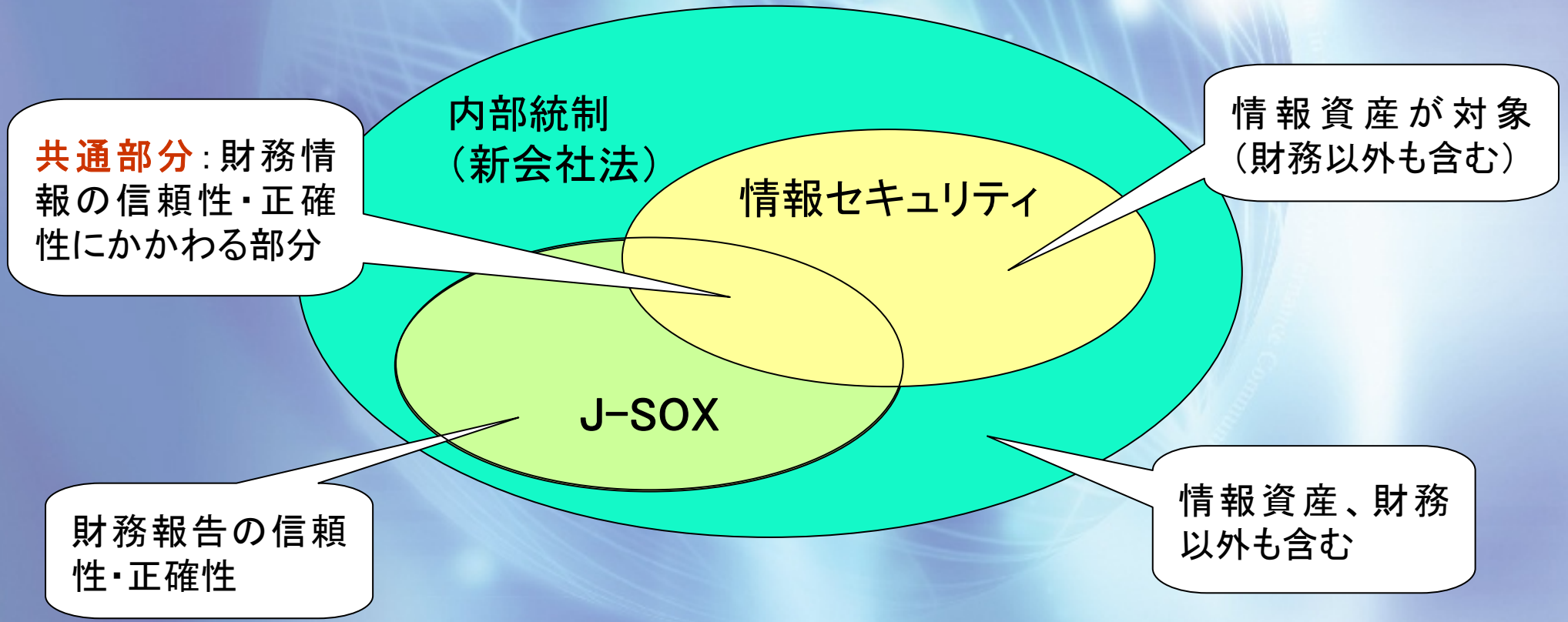
ITガバナンスとIT統制



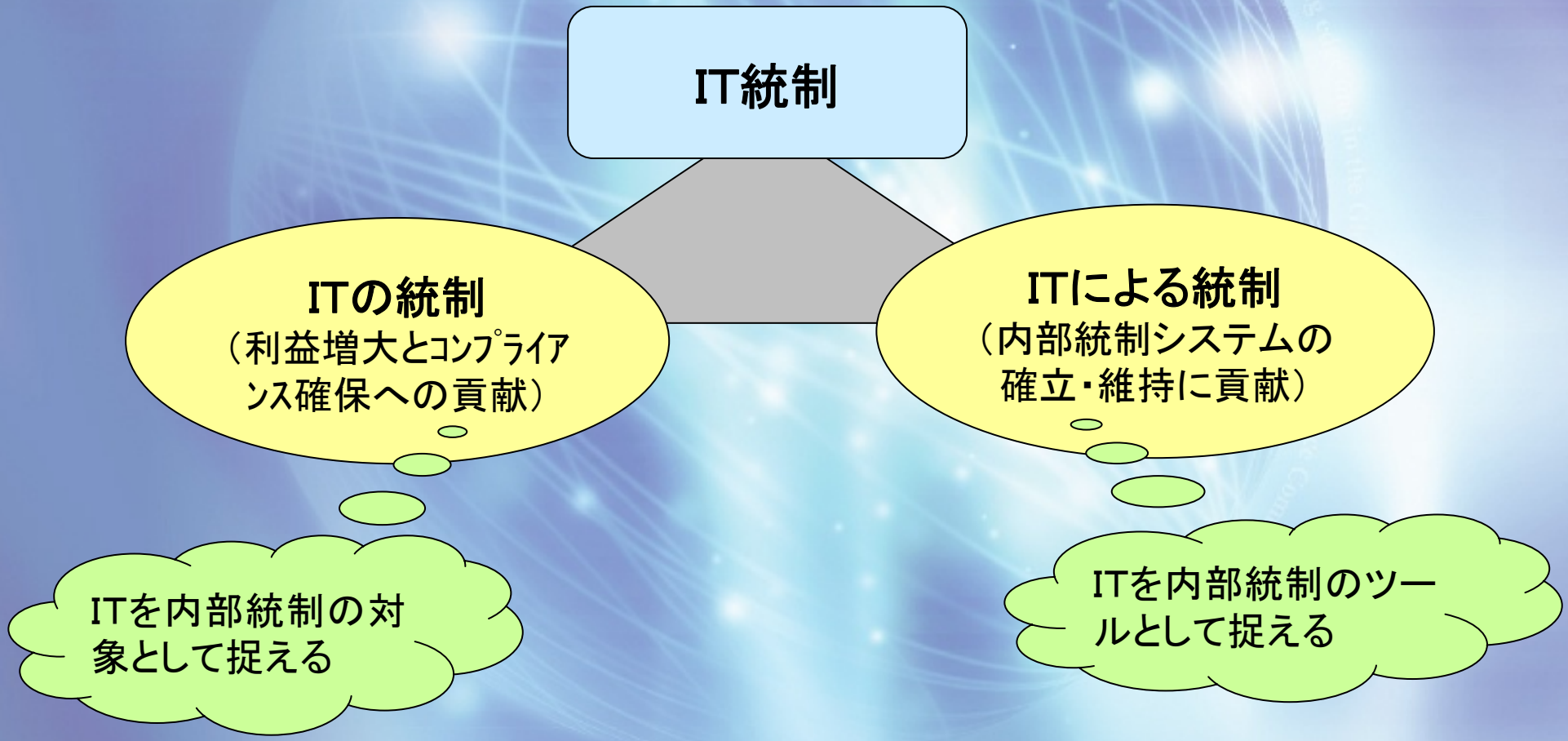
- ITガバナンス
  - コーポレートガバナンスの一部
  - ビジネスとの関係を重視
  - ITによる企業目標の達成への貢献
  - ITはガバナンスの対象
  - ディスクロージャーも関係
- IT統制
  - ITを利用した統制とITを対象とした統制
  - J-SOX（ITへの対応）では、ITを利用した統制＆財務統制が中心。ただし、ITを対象とした内部統制も含む。
  - IT統制は、ITガバナンスを構成する一部分

情報セキュリティとIT統制

- 会社法の内部統制、J－SOX、情報セキュリティでは、範囲が少しずつ異なる。



IT統制の概念整理


IT統制
ITの統制
（利益増大とｺﾝﾌﾟﾗｲｱﾝｽ確保への貢献）
ITによる統制
（内部統制システムの確立・維持に貢献）
ITを内部統制の対象として捉える
ITを内部統制のツールとして捉える

IT統制概念の疑問？？？

- ITを利用して内部統制を整備することは分かる。しかし、なぜ、内部統制の対象としてITだけが取り上げられるのか？
  - 他の投資案件も同じでは？
  - ITが内部統制の有効性に影響を及ぼすから？
- 財務に係るITを統制の対象とするのは分かるが・・・。（ただし、開発中のシステムのIT統制が不十分であっても稼動するまでは内部統制上の不備にはならないのではないか）
- 財務報告の視点からみると、ITによる統制の方が重要ではないか？

ITGI Japan

GOVERNANCE INSTITUTE

ITガバナンスの向上に向けて

COBIT for SOXがCOBITではない

- COBIT for SOXを参照した内部統制の整備と、COBITによるITガバナンスの整備は同じものではないことに注意しなければならない。
- COBIT for SOXは、財務統制に関わるIT統制を整備するものである。
- 両者の項目を比較すれば、その違いが分かるのでは・・・。

COBITとCOBIT for SOXの比較

	COBIT 4.0	COBIT for SOX
PO1	IT戦略計画の策定	IT戦略の策定
PO2	情報アーキテクチャーの定義	
PO3	技術指針の決定	
PO4	ITプロセスと組織及びそのかかわりの定義	ITプロセス、組織および関係
PO5	IT投資の管理	
PO6	マネジメントの意図と指針の周知	マネジメントの意図と指示の周知
PO7	IT人材の管理	IT人的資源の管理 利用者の教育と研修
PO8	品質管理	品質管理
PO9	ITリスクの評価と管理	ITリスクの評価と管理
PO10	プロジェクト管理	

COBITとCOBIT for SOXの比較（続き）

	COBIT 4.0	COBIT for SOX
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	アプリケーションソフトウェアの調達と保守
AI3	技術インフラストラクチャの調達と保守	技術インフラストラクチャの調達と保守
AI4	運用と利用の促進	運用の促進
AI5	IT資源の調達	
AI6	変更管理	変更管理
AI7	ソリューションおよびその変更の導入と認定	ソリューションおよびその変更の導入と設定
EUC		エンド・ユーザ・コンピューティング

COBITとCOBIT for SOXの比較（続き）

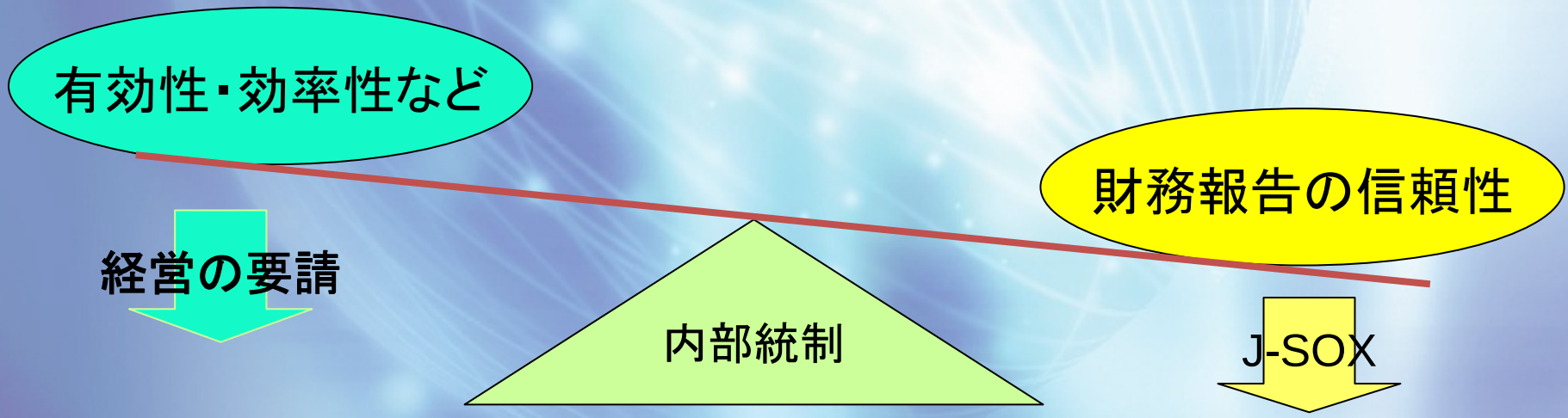
	COBIT 4.0	COBIT for SOX
DS1	サービスレベルの定義と管理	サービス・レベルの定義と管理
DS2	サードパーティサービスの管理	サードパーティのサービスの管理
DS3	性能とキャパシティの管理	
DS4	継続的なサービスの保証	
DS5	システムセキュリティの保証	システムセキュリティの保証
DS6	コストの捕捉と配賦	
DS7	利用者の教育と研修	
DS8	サービスデスクとインシデントの管理	
DS9	構成管理	構成管理
DS10	問題管理	問題とインシデントの管理
DS11	データ管理	データ管理
DS12	物理的環境の管理	
DS13	オペレーション管理	オペレーション管理

COBITとCOBIT for SOXの比較（続き）

	COBIT 4.0	COBIT for SOX
ME1	IT成果のモニタリングと評価	成果のモニタリングと評価
ME2	内部統制のモニタリングと評価	内部統制のモニタリングと評価
ME3	規制に対するコンプライアンスの保証	
ME4	ITガバナンスの提供	
業務処理統制		決算における業務処理統制の目標
		総勘定元帳における業務処理統制の目標
		販売における業務処理統制の目標
		購買における業務処理統制の目標
		棚卸資産に関する業務処理統制の目標
		固定資産管理における業務処理統制の目標
		人事部における業務処理統制の目標
		税務における業務処理統制の目標

J－SOXの悪影響？

- J-SOXは、財務統制に焦点が当てられている。つまり、財務報告に偏った内部統制が改善・強化されることになる。
- システム監査も、J-SOXに偏っていく可能性がある。つまり、財務報告に偏ったシステム監査が盛んになるおそれがある。
- 付加価値のあるシステム監査は、企業の目標達成（価値向上）につながる監査である。財務統制以外の内部統制を対象とした内部監査の重要性を忘れてはならない。



「攻めのIT統制」とは何か

- 「内部統制の整備の結果として期待される業務処理品質の向上や内部統制プロセスから生み出されるデータや情報を活用していくことにより、次のような効果が期待できます。」（平野雅章教授）
  - 業務プロセスの効率化
  - 経営の効率化
  - リスク耐性の強化
  - 経営革新
  - 資本市場や社会の信頼向上

  ＊出所：経営情報学関連学会「内部統制」タスクフォース、『内部統制Q＆A』、日経BP社、2006年、pp.18−20。
- 「内部統制への取組みにおいては、企業価値の向上を目的として、企業戦略の一環としてそれを行う「攻めの姿勢」が重要です。（中略）内部統制への取組みにあたっては、内部統制に関する法令への対応や、内部統制報告書のような文書の作成が目的化してしまわないように留意する必要があります。」（村田潔教授）

  ＊出所：経営情報学関連学会「内部統制」タスクフォース、『内部統制Q＆A』、日経BP社、2006年、p.26。

J-SOX対応と価値向上

- J-SOX対応による価値
  - J-SOX対応は、ITガバナンスの確立に向けたスタートであり、ITガバナンスの基盤
  - 財務情報に関するアクセス管理、変更管理などのIT統制レベルの向上
  - プロセスの明確化
  - 文書化によるプロセス、リスク及び統制の透明性の向上
  - 説明責任の意識向上
- J-SOX対応での不足事項
  - システムのビジネスへの有効性、効率性などに関する統制は対象外
  - 財務以外のアクセス管理、変更管理などのIT統制は対象外
  - 内部統制監査において、オーバーコントロールは内部統制の不備にはならない。

COBITをどのように利用してゆくか

- COBITは、「攻めのIT統制」の整備に役立つ。
- COBITの項目を全てそのまま適用するのは現実的ではない。
  - 自社のIT環境や企業環境に応じた取捨選択
  - リスクを考慮した導入
- COBITの考え方は有益
  - KPI、KGI、KSFの視点を監査で利用
  - CMMを監査で利用する際の工夫が必要
  - メトリックスの概念はアクティビティ、プロセス、IT、ビジネスの関係のせり入りに役立つ。
- 監査で利用する場合、経営者が利用する場合、管理者が利用する場合で、利用の仕方が異なる。
  - 監査の場合には、判断尺度の設定が必要になる。また、内部監査の場合と、外部監査の場合でも利用方法が異なる。

COBITをどのように利用してゆくか続き

- 企業の主体性が必要
  - 何のためにCOBITを導入するのか（導入目的の明確化）
  - COBITの自社向けのカスタマイズ
  - 成熟度の目標レベルの決定
- 効率性の考慮
  - CMMの効率性についても考慮が必要
  - KPI、KGI、CSFを設定すればマネジメントが効率的になるのか（指標導入の目的の明確化）
- 品質
  - システム監査（IT保証）の品質確保

おわりに

- ビジネスとコントロールをセットで考える。
  - ビジネスの枠組みや、ビジネスプロセスを考えるときには、ントロールを一体のものとして検討する。
  - COBITは、その際に参考になる。
- ITガバナンスの成熟度レベルだけではなく、それを達成するためのコストを考える。
  - 成熟度レベルを高めることは良いことだが、コストも増加する。
  - ITガバナンス構築・運用の効率性の視点を忘れない。
- IT以外のリスクも忘れない。
  - ITリスクの重要性は増大しているが、IT以外のリスクも複雑化し増大している。
  - ERM（Enterprise Risk Management）が注目されている。