

「実施基準公開！JSOXプロジェクト成功へのカギ」セミナー

JSOX及び実施基準の動向とその対応

注：資料作成時点では実施基準が公開されていなかったため、この資料は草案をベースとしています

2007年2月6日

株式会社 NTTデータ経営研究所
パートナー 小野寺 清人

PROFILE

- 現在
 - ・株式会社 NTTデータ経営研究所 パートナー **認定SOXアドバイザー**
 - ・経営及びIT双方に関わるテーマを中心に、経営戦略、ITガバナンス、ITマネジメント、BPM(ビジネス・プロセス・マネジメント)、EA(エンタープライズ・アーキテクチャー)、戦略的IT活用、ITアウトソーシング、BPR、ITポートフォリオ(投資対効果)、パフォーマンス評価、情報セキュリティ等に関するコンサルティングを実施。また、ハイテク、ヘルスケア、小売・流通等の分野における新規事業立案等のコンサルティングにも従事。最近では、新会社法対応やJ-SOX法対応などの内部統制(マネジメントシステム)構築に関連したコンサルティングにも携わっている。
- 学歴
 - ・1982年東京大学卒
 - ・1993年ペンシルバニア大学ウォートン校卒、経営学修士(MBA)
- 職歴
 - ・1982年 日本電気株式会社入社
運輸、製造、マスコミ、公益企業等の大手日本企業および公共機関を顧客として、人工知能、意思決定支援、マルチメディア等の先端技術を応用した情報システムの構築や、営業系、経理系等各種業務システムの構築に従事。MBA取得後、ERPパッケージやその他ソフトウェアツール等、IT分野における企画立案及びマーケティングを担当。
 - ・1996年 株式会社 NTTデータ経営研究所 入社 現在に至る
- 主要論文・著書
 - ・統計学大系シリーズ 『シックスシグマ』(共訳)エコノミスト社(2006年)
 - ・『情報システム投資の基本がわかる本』(共著)日本能率協会マネジメントセンター(2003年)
 - ・『CNCネットワーク革命』(共編著)東洋経済(2002年)
 - ・「最新IT活用による公的保険医療費請求業務フロー改革構想」『経営情報学会誌』(2000年)
 - ・「経営者のためのITアウトソーシングABC」シリーズ第2, 3, 6回『ロジスティクス・ジャーナル』(2001年)
 - ・“Cockpit Crew Scheduling and Supporting System” *Operational Expert System Applications in the Far East*. Pergamon Press(1991年)

会社案内

会社概要

社名： 株式会社エヌ・ティ・ティ・データ経営研究所
設立： 1991年(平成3年)4月12日
資本金： 4億5000万円 ((株)NTTデータが100%出資)
売上： 約35億円(2005年度)
従業員数： 約135名(2005年度)
本社： 〒150-0011 東京都渋谷区東1-32-12渋谷プロパティ―東急ビル6階
TEL： 03-5467-6311(代表)
URL： <http://www.keieiken.co.jp/>
取締役会長 武藤 英二
代表取締役社長 佐々木 崇
取締役所長 齋藤 精一郎

事業内容

1. 企業経営および行政に関する調査研究ならびにコンサルティング業務
2. 情報および通信システムの企画・開発に関する調査研究ならびにコンサルティング業務
3. 経済、社会、産業、文化等に関する調査研究ならびにコンサルティング業務
4. 前各号に関連する教育研修・セミナーの実施・運営、情報の提供ならびに刊行物の出版
5. 前各号に付帯する一切の業務

はじめに・・・コンプライアンス／内部統制／SOX法の関係

1. 米国の動向

2. 日本版SOX法(JSOX)の概要

3. 全社的な内部統制の進め方

4. IT全般統制の進め方

5. 投資対効果を上げる方法

おわりに 教育・資格の紹介

はじめに・・・コンプライアンス／内部統制／SOX法の関係

1. 米国の動向
 2. 日本版SOX法(JSOX)の概要
 3. 全社的な内部統制の進め方
 4. IT全般統制の進め方
 5. 投資対効果を上げる方法
- おわりに 教育・資格の紹介

最近の経済犯罪

(空白ページ)

背景

『ブランド力向上』

『顧客満足度向上』

『スキルアップ』

『品質向上』

『環境対策』

『セキュリティ強化』

パフォーマンス向上への期待

コンプライアンスの強化

内部統制の確立／向上

業務が不正なく適切に遂行されるシステムの確立が必要

企業内部において不正が容易に行われ得る状況が存在

『牛肉偽装事件』

『欠陥隠し事件』

『記録改ざん事件』

『個人情報漏洩事件』

『新薬副作用死亡事件』

『有価証券報告書の虚偽記載発覚』

コンプライアンスの範囲

『コンプライアンス』とは狭義の場合『法令順守』となるが、広義の場合は『企業倫理等の観点から定められた企業ルールや明文化されていないルールの遵守』も含まれる。



内部統制の対象を、狭義のコンプライアンスレベルから広義のコンプライアンスレベルへ、更にコンプライアンスの枠を超えてパフォーマンスの向上レベルへ引き上げることが望ましい。

内部統制の目的と実現する仕組み

内部統制の目的の範囲は後述のCOSOフレームワーク、SOX法、会社法によってそれぞれ異なっている。

目的は大きく

- ①パフォーマンス向上
- ②コンプライアンス確保に分けることができる。

目的

パフォーマンス向上

ブランド価値の向上

⋮

製品・サービスの品質維持・向上

業務の有効性・効率性向上

(狭義の)コンプライアンス確保

商法

金融商品取引法

独占禁止法

個人情報保護法

⋮

企業内ルール

意思決定・実行・モニタリング
の適正性と透明性を確保する

仕組み

(=『マネジメントシステム(MS)』)

ブランドマネジメントシステム

⋮

QMS(品質マネジメントシステム)

⋮

コンプライアンス マネジメントシステム

財務(報告)マネジメントシステム

ISMS(情報セキュリティマネジメントシステム)

EMS(環境マネジメントシステム)

COSO

会社法

SOX法

各目的達成のため内部統制は『マネジメントシステム』として構築される。

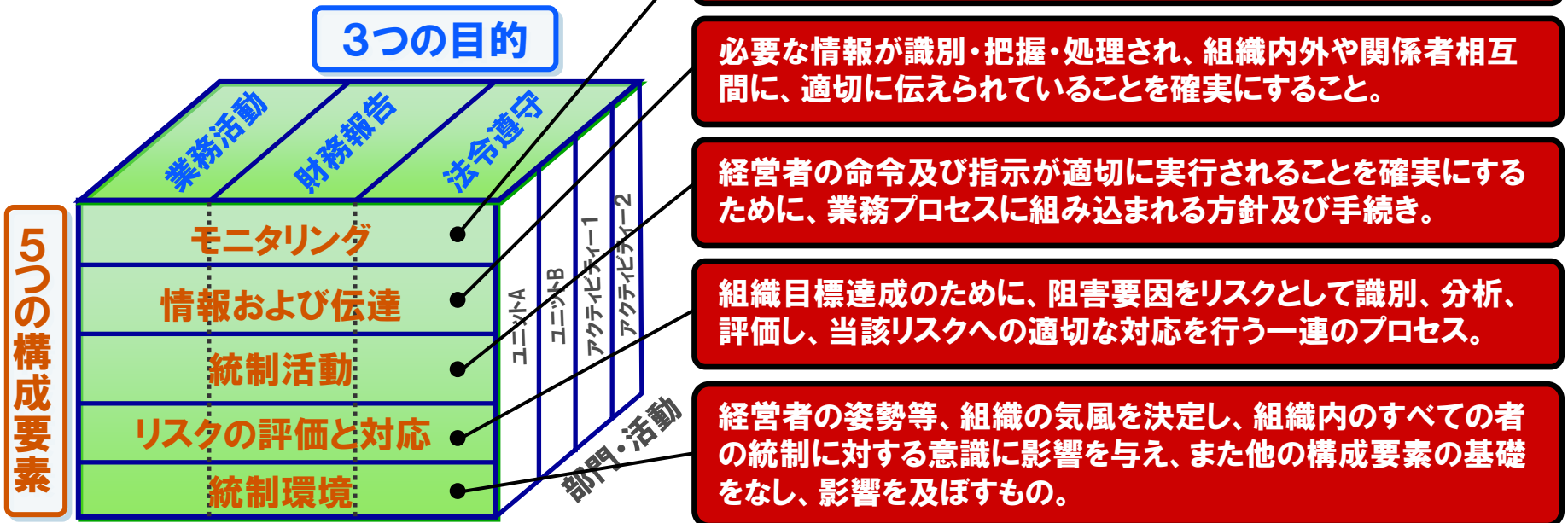
SOXは、財務(報告)マネジメントシステムであり、管理の仕組みの一部ではない

COSOフレームワーク

組織が内部統制を構築または評価・改善するにあたっての枠組みとしてCOSOフレームワークがある。米国SOX法もJ-SOX法基準案も、COSOフレームワークをベースにしている

- COSO : トレッドウェイ委員会支援組織委員会(The Committee of Sponsoring Organization of the Tread Commission)の略称。倫理、内部統制、コーポレートガバナンスを通して財務報告の質の向上を図るために、1985年設立された米国の民間団体。
- COSOフレームワーク : 1992年にCOSOが発表した「内部統制－統合的枠組み」のこと。

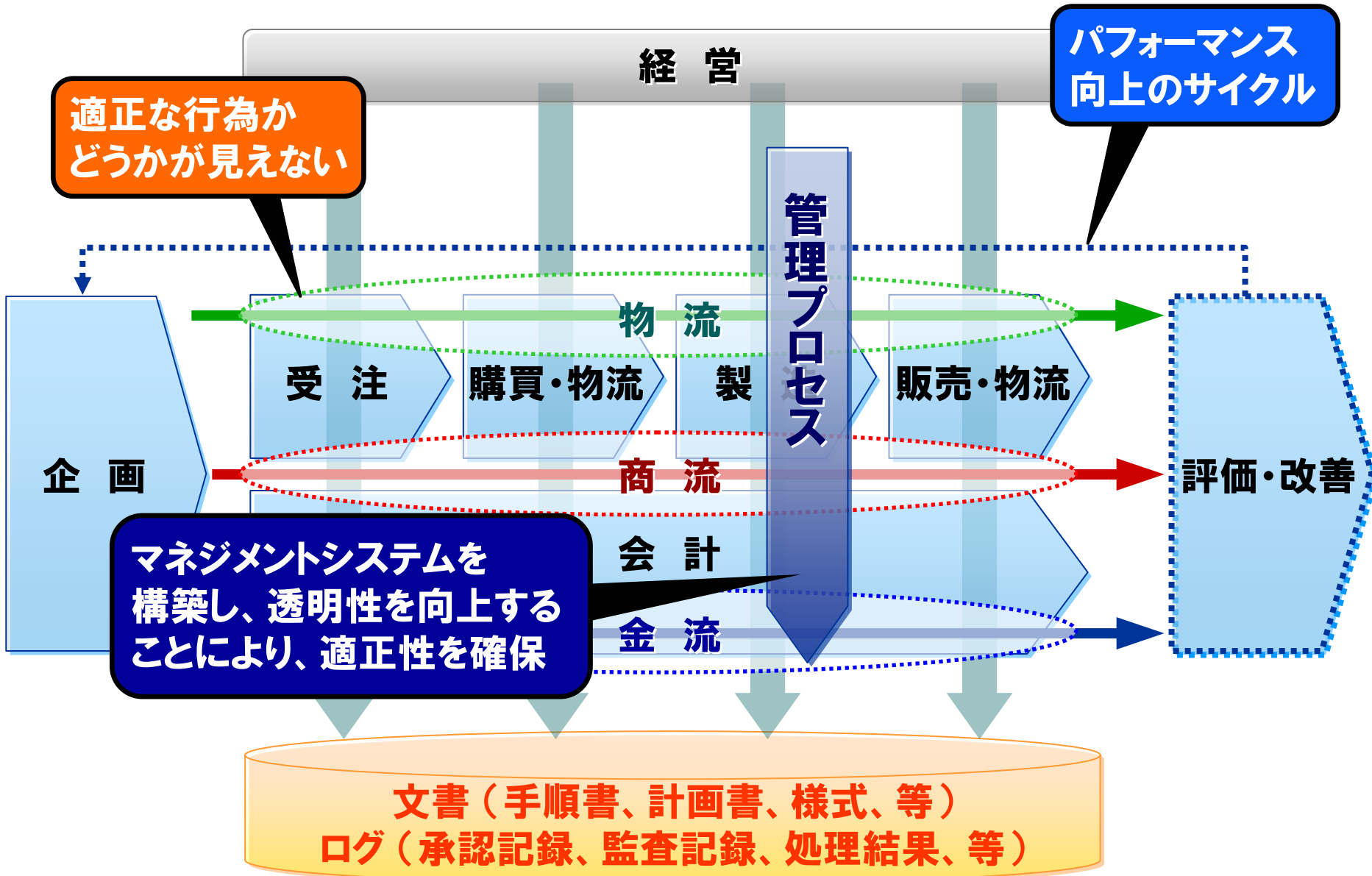
内部統制の3つの目的と5つの構成要素、およびそれを実現する部門・活動の関係



(補足)・COSOフレームワークはあくまで枠組みとして内部統制の目的と構成要素を整理しているにすぎない。
・内部統制を実現する方法や内部統制を評価するポイントは組織が個別に検討・設計する必要がある

出典:「財務報告に係る内部統制の評価及び監査の基準のあり方について」平成17年12月8日 企業会計審議会内部統制部会 を元に編集

業務プロセスとマネジメントシステムの関係



マネジメントシステムの成熟度

すべての組織にマネジメントシステムは存在している。ただ、その成熟度(平たく言えば巧拙)が異なるだけである



ISO9001等の認証を取得していることが、成熟度の高さを示すわけではない。実際には、このような国際規格の認証を取得していても、成熟度が低い企業が少なからず存在している

はじめに・・・コンプライアンス／内部統制／SOX法の関係

1. 米国の動向

2. 日本版SOX法(JSOX)の概要

3. 全社的な内部統制の進め方

4. IT全般統制の進め方

5. 投資対効果を上げる方法

おわりに 教育・資格の紹介

米国企業のコンプライアンス状況

(空白ページ)

米国企業改革法(SOX法) 成立までの経緯

1992年 COSOレポートの公表

COSOレポート：トレッドウェイ支援組織委員会(COSO)が公表した「内部統制に関する統合的フレームワーク」
米国で不正経理が多発。そのため、当時のAICA(米国公認会計士協会)やIIA(内部監査協会)が内部統制について調査し発表。制度化までは到らず。

2001年～2002年 大規模な会計不祥事の多発

大規模な会計不祥事事件の頻発により、証券・金融市場に対する不信感が高まった。

例)・**エンロン事件**

⇒大手エネルギー企業エンロンが、業績不振会社の連結外し等の手口により、大規模な粉飾決算を行った。

・**ワールドコム事件**

⇒長距離電話会社ワールドコム社が、費用や損失とすべき項目を資産と計上することにより、巨額の損失を隠蔽した。

2002年7月 企業改革法(SOX法)可決、成立

証券・金融市場への信用回復を目的とし、コーポレートガバナンス、財務報告等に関する規制からなる企業改革法が成立。下院423-3、上院99-0。上院では30分足らずで審議終了。

・SOX法は1992年に公表されたCOSOレポートをベースにしている。

【主要規定】

・**財務報告への企業責任(302条)**：CEO、CFOは開示した財務報告の内容、その内部統制手続きに責任を負うことを四半期毎に宣誓することを義務化。

・**内部統制の経営者評価(404条)**：経営者が内部統制とその手続きを毎年評価し、外部監査法人がこの評価の中身を客観的に検証し、別途報告書を提出することを義務化。

米国企業改革法(SOX法) 現状

SOX法規定の適用

- ◆財務報告への企業責任(302条) ⇒ 2002年8月より適用
- ◆内部統制の経営者評価(404条) ⇒ 2004年11月15日以降の年次決算より適用

企業における404条への対応結果

- 対応するため多大なコストと労力を強いられた。
- ◆外部監査人・コンサルティング会社への支払い費用
数億円以上(最高100億円を超える)
 - ◆従業員等が内部統制の整備や評価に費やした時間
数万時間(平均2~3万時間程度?)

404条の適用結果

- 2004年12月決算
⇒ 適用対象企業のうち **十数%もの企業** が
内部統制に『**重大な欠落**』

SEC(証券取引委員会)の対応

- ◆ 経営者から事務負担が大きいという指摘を受け、『内部統制報告規定の実施に関する委員会報告』、『財務報告に係る内部統制について経営者報告書に関するスタッフ報告』を公表(2005年5月16日)
- ◆ 内部統制報告制度改善に向けて下記の動きがある
⇒ 『トップダウン型リスク重視アプローチの採用』、『財務諸表監査と内部統制監査の統合』、
『小規模企業のためのCOSOのガイダンス策定』、『経営者と監査人の独立性規定違反の限度』

米国の今後の法適用(緩和)予定

■ 内部統制報告の段階的適用延期

米国において、内部統制報告実務が以下のように段階的に適用延期となった。

	米国企業	外国企業
大規模早期適用企業	2004年11月15日以降 適用(済)	2006年7月15日以降 適用に延期
早期適用企業		2007年7月15日以降 適用に延期
早期適用企業以外の会社	2007年7月15日以降 適用に延期	

(注)大規模早期適用企業：普通株式の市場価格7億ドル以上

早期適用企業：普通株式の市場価格75百万ドル以上7億ドル未満

■ 中小規模企業に対する適用緩和策の提案

SEC中小規模公開企業諮問委員会が中小規模企業に対する緩和策を提案した

小規模企業 (Microcap Companies)	中規模企業 (Smallcap companies)
SOX法302条の適用のみで 404条適用除外	経営者による評価のみで 404条に基づく監査人の監査を免除

(注)小規模企業：発行済株式の時価総額1.282億ドル以下で、直近事業年度の売上高1.25億ドル以下の場合

中規模企業：発行済株式の時価総額1.282億ドル～7.871億ドルで、直近事業年度の売上高2.5億ドル以下の場合

■ 新規公開会社(国内・外国)への適用緩和

新規公開会社の公開後、初年度の決算においては、経営者評価と内部統制監査の双方を免除

SOXの効果

1 不正やミスの削減

特に大企業の場合、効果>コスト

なぜ、ここをコントロールしていなかったのか、という発見もある

2 業務の標準化の推進

例:グローバル企業の場合、ローカルルール削減につながっている

3 業務の改善(部分的ではあるが)

特に、自分たちで文書化作業を行った場合、問題への**気づき**がある

4 IT資産の集約によるコスト削減

IT統制の向上によって、IT資産(データセンター、HW、業務ソフト)の集約が進展

SOX適用企業のコストと効果の関係

SOX費用／売上額
(%)

売上額がおよそ5億ドル以下(またはSOX対応コストが売上の0.3~0.4%以上)の企業では、**コスト>効果**の危険がある。この規模の企業の場合、大企業よりも取り組み方に工夫が必要となる。なお、SOX2年目では、前年比10~20%程度、コストが削減している。

危険ゾーン
コスト>効果

安全ゾーン
コスト<効果

SOXの一般的な効果

- 不正やミスの予防・早期発見による効果
- ITガバナンスの向上によるコスト削減
- ビジネスプロセスの標準化／改善(部分的)

0.3~0.4%が分岐点

0.05以下 売上額

\$50M

\$100M

\$500M

\$1B

\$5B

\$30B

注: 上記の数値は、各種調査、ヒアリング及びテレビ報道等から推測

企業規模別に必要とされるSOX内部統制1

(SOX対応した場合)

(26ページ参照)

従業員数
売上金額

極小規模

50人以下
10億円以下

効果<コスト

小規模

150人以下
100億円以下

中規模

1000人以下
500億円以下

効果>コスト

大企業

1000人以上
500億円以上

経営者の内部統制
把握水準

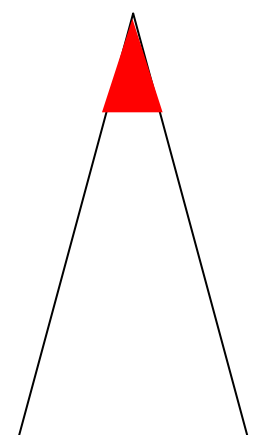
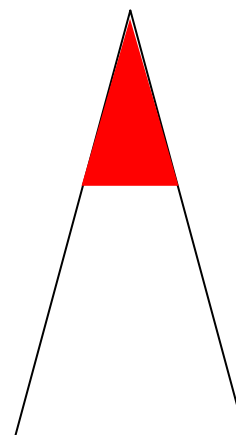
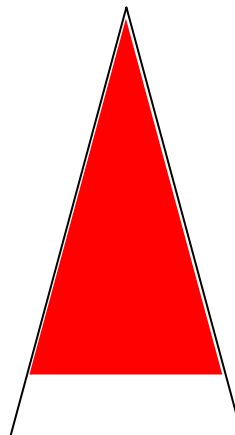
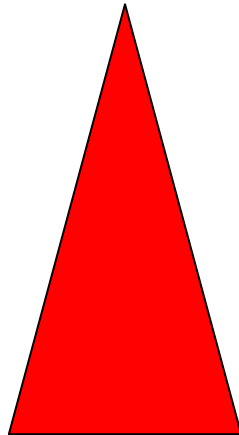
経営者が、従業員
全員(**who**)が何
(**what**)をどのように
している(**how**)か、
把握可能

経営者が、従業員
全員(**who**)が何
(**what**)をしているか
把握可能。Howは
多少、不透明

経営者が、組織単
位で何(**what**)をして
いるか把握可能。
Whoとhowは不透
明。

権限が各組織に移
行しており、組織が
何をしているか、多
少不透明。Whoと
howは不透明。

経営者の内部統制
把握のイメージ
(赤が把握部分)



注:企業規模に関しては、イメージとして考えていただきたい。特に統計的な根拠があるわけではなく、インタビューや各種資料からの推測を基にしている

企業規模別に必要とされるSOX内部統制2

(SOX対応した場合)	効果<コスト			効果>コスト
	極小規模 従業員数 50人以下 売上金額 10億円以下	小規模 150人以下 100億円以下	中規模 1000人以下 500億円以下	大企業 1000人以上 500億円以上
財務統制の必要性	小	中	大	大
業務プロセスが定義可能か	定義困難 ←			→ 定義可能
職務分掌可能か	困難 ←			→ 容易
必要な財務統制	現状でほぼOK	Howの把握。職務記述書、分掌規定、ID管理等。	SOX対応、但し、範囲を限定、フローチャートを簡易化。	SOX対応

注:企業規模に関しては、イメージとして考えていただきたい。特に統計的な根拠があるわけではなく、インタビューや各種資料からの推測を基にしている

SOXの課題

1 投資対効果が得られない？(小規模企業の場合)

企業が受ける効果よりもコストの方が大きい
通常の手組み方では改善につながらない

→改善につながるケース

・良いBPMツールを使用し、自分たちで文書化を行った場合

2 膨大な紙・・・ペーパーレスに逆行

特に手作業で対応した企業の場合

3 業務へのインパクトが大

永続的に続く作業

4 人によって判断が異なる

監査法人、テスター

5 外部業者への委託・・・どう証明するか？

米国ではSAS70があるが、米国以外では？

6 ITの不備を補う必要

最後は目視チェック

IT全般統制(ITガバナンス)の向上が容易ではない

SOXの課題

1 投資対効果が得られない？(小規模企業の場合)

企業が受ける効果よりもコストの方が大きい
通常の手組み方では改善につながらない

→改善につながるケース

・良いBPMツールを使用し、自分たちで文書化を行った場合

2 膨大な紙・・・ペーパーレスに逆行

特に手作業で対応した企業の場合

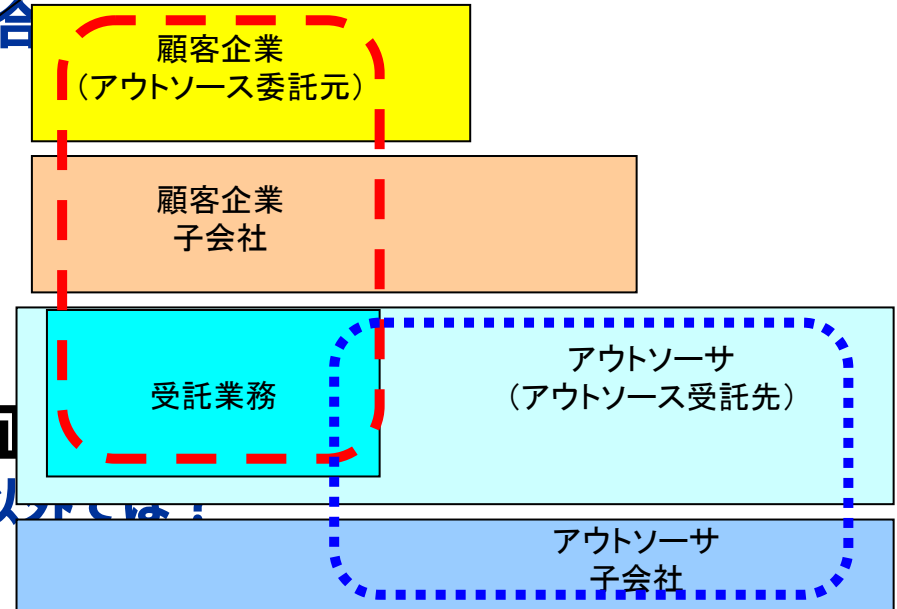
3 業務へのインパクトが大 永続的に続く作業

4 人によって判断が異なる 監査法人、テスター

5 外部業者への委託・・・どう証 米国ではSAS70があるが、米国以外では

6 ITの不備を補う必要 最後は目視チェック

IT全般統制(ITガバナンス)の向上が容易ではない



アウトソーシング業務は18号監査か委託企業の監査を受けることとなる
(点線が文書化(業務処理統制)の範囲)

はじめに・・・コンプライアンス／内部統制／SOX法の関係

1. 米国の動向

2. 日本版SOX法(JSOX)の概要

3. 全社的な内部統制の進め方

4. IT全般統制の進め方

5. 投資対効果を上げる方法

おわりに 教育・資格の紹介

SOX法とJ-SOXの関係

米国のSOX法がしばしば引き合いに出されるが、SOX法が企業の財務に関する内部統制の強化を主眼としているのに対して、J-SOXは金融商品取引法の一部として位置づけられるという違いがある。

米国SOX法

目的

財務報告の適正性、透明性を向上することによる**投資家の保護**

金融商品取引法

証券取引法の改正版。金融商品を縦割りではなく包括的に取り扱うことによる**投資家の保護**

財務内部 統制に 関する 記述

11章69条からなる財務内部統制の強化に関する法

- PCAOB: Public Company Accounting Oversight Boardの設置
- 監査人の独立性
- インサイダー取引の制限
- 内部統制の義務化
- 経営者への罰則強化
- 内部告発者の保護等

米国SOX法の**404条**に対応する部分を法令化。但しダイレクトレポーティングの不採用など違いがある。

経営者に対する罰則も最大で懲役5年、罰金500万円と米国に比較して軽い

J-SOXにおける内部統制の基本的枠組み—内部統制の定義

内部統制とは、

- ① 業務の有効性及び効率性、
- ② 財務報告の信頼性、——→ (J-SOXの目的)
- ③ 事業活動に関わる法令等の遵守並びに
- ④ 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、

- ① 統制環境、
- ② リスクの評価と対応、
- ③ 統制活動、
- ④ 情報と伝達、
- ⑤ モニタリング(監視活動)及び
- ⑥ 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。

J-SOXにおける内部統制の評価

評価範囲の決定

財務報告の範囲

- 企業活動を構成する事業又は業務
- 財務報告の基礎となる取引又は事象
- 主要な業務プロセス

金額的及び質的影響の観点から重要性を検討し、評価範囲を決定

評価範囲の決定方法及び根拠等を適切に記録

評価の方法

全社的な内部統制の評価

業務プロセスに係る内部統制の評価

内部統制の有効性の判断

重要な欠陥の是正

評価手続きの記録及び保存

報告

内部統制報告書の記載事項

- ① 整備及び運用に関する事項
- ② 評価の範囲、評価時点及び評価手続
- ③ 評価結果
- ④ 付記事項

1. 財務報告及び財務報告に係る内部統制に責任を有する者の氏名
2. 経営者が、財務報告に係る内部統制の整備及び運用の責任を有している旨
3. 財務報告に係る内部統制を整備及び運用する際に準拠した一般に公正妥当と認められる内部統制の枠組み
4. 内部統制の固有の限界

1. 財務報告に係る内部統制の評価の範囲(範囲の決定方法及び根拠を含む。)
2. 財務報告に係る内部統制の評価が行われた時点
3. 財務報告に係る内部統制の評価に当たって、一般に公正妥当と認められる内部統制の評価の基準に準拠した旨
4. 財務報告に係る内部統制の評価手続の概要

- 財務報告に係る内部統制は有効である旨
- 評価手続の一部が実施できなかったが、財務報告に係る内部統制は有効である旨、並びに実施できなかった評価手続及びその理由
- 重要な欠陥があり、財務報告に係る内部統制は有効でない旨、並びにその重要な欠陥の内容及びそれが是正されない理由
- 重要な評価手続が実施できなかったため、財務報告に係る内部統制の評価結果を表明できない旨、並びに実施できなかった評価手続及びその理由

J-SOXにおける内部統制の監査と報告

監査

目的

一般に公正妥当と認められる**内部統制の評価の基準**に準拠して、内部統制の有効性の評価結果をすべての重要な点において**適正に表示**しているかどうかについて、監査人自らが入手した**監査証拠**に基づいて判断した結果を意見として表明すること

財務諸表監査との関係

同一の監査人により、財務諸表監査と一体となって行われる

監査手順

監査計画の策定

評価範囲の妥当性の検証

全社的な内部統制の評価の検証

業務プロセスに係る内部統制の評価の検証

内部統制の重要な欠陥等の報告と是正

不正などの報告

報告

監査人は、無限定適正意見を表明する場合には、**内部統制監査報告書に次の記載を行うものとする。**

① 内部統制監査の対象

- イ. 内部統制監査の範囲
- ロ. 財務報告に係る内部統制の整備及び運用並びに内部統制報告書の作成の**責任は経営者**にあること
- ハ. 内部統制監査に対する監査人の責任は独立の立場から内部統制報告書に対する意見を表明することにあること
- ニ. 内部統制の固有の限界

② 実施した内部統制監査の概要

- イ. 内部統制監査に当たって、監査人が一般に公正妥当と認められる内部統制の監査の基準に準拠して監査を実施した旨
- ロ. 内部統制監査において実施した監査手続の概要
- ハ. 内部統制監査の結果として意見表明のための合理的な基礎を得たこと

③ 内部統制報告書に対する監査人の意見

- イ. 内部統制報告書における経営者の評価結果
- ロ. 内部統制報告書が一般に公正妥当と認められる内部統制の評価の基準に準拠し、財務報告に係る内部統制の評価結果について、すべての重要な点において適正に表示していると認められること

J-SOXにおける考慮事項

『財務報告に係る内部統制の評価及び監督の基準案』における考慮事項

- 1 トップダウン型のリスク・アプローチの活用
- 2 内部統制の不備の区分(不備と重要な欠陥)
- 3 **ダイレクト・レポーティングの不採用**
- 4 内部統制監査と財務諸表監査の一体的実施
- 5 内部統制監査報告書と財務諸表監査報告書の一体的作成
- 6 監査人と監査役・内部監査人との連携

米国からの教訓を汲み取っているため米国SOX法と異なる点もある。

J-SOXにおける内部統制の限界

内部統制は、下記のような固有の限界を有するため、その目的の達成にとって絶対的なものではないが、各基本的要素が有機的に結びつき、一体となって機能することで、その目的を合理的な範囲で達成しようとするものである。

1

内部統制は、判断の誤り、不注意、複数の担当者による共謀によって有効に機能しなくなる場合がある

2

内部統制は、当初想定していなかった組織内外の環境の変化や非定型的な取引等には、必ずしも対応しない場合がある

3

内部統制の整備及び運用に際しては、費用と便益との比較衡量が求められる
(投資対効果?)

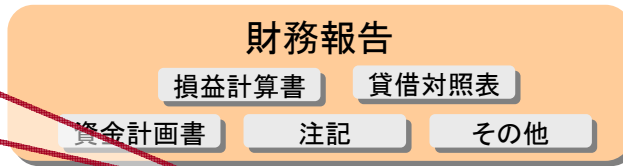
4

経営者が不当な目的の為に内部統制を無視ないし無効ならしめることがある
(社会的影響が大きい経営者の犯罪をどう防ぐか?)

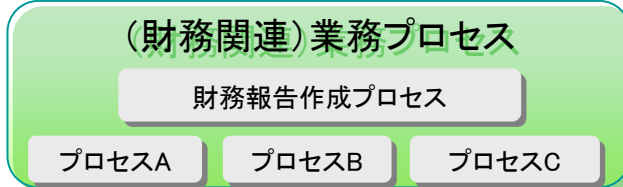
JSOXが要求する財務報告に係る内部統制

日本版SOX法では、財務報告に係る内部統制を『全社的な内部統制』、『業務処理統制』、『IT業務処理統制』、『IT全般統制』の4つと捉え、これらを整備・運用することを求めている

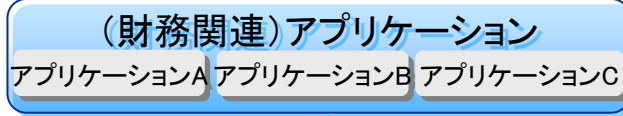
「実在性」、「網羅性」、「評価の妥当性」等の財務諸表項目の残高が適切であるための条件（アサーション）の達成を妨げる可能性があるか、という視点でリスクを分析する



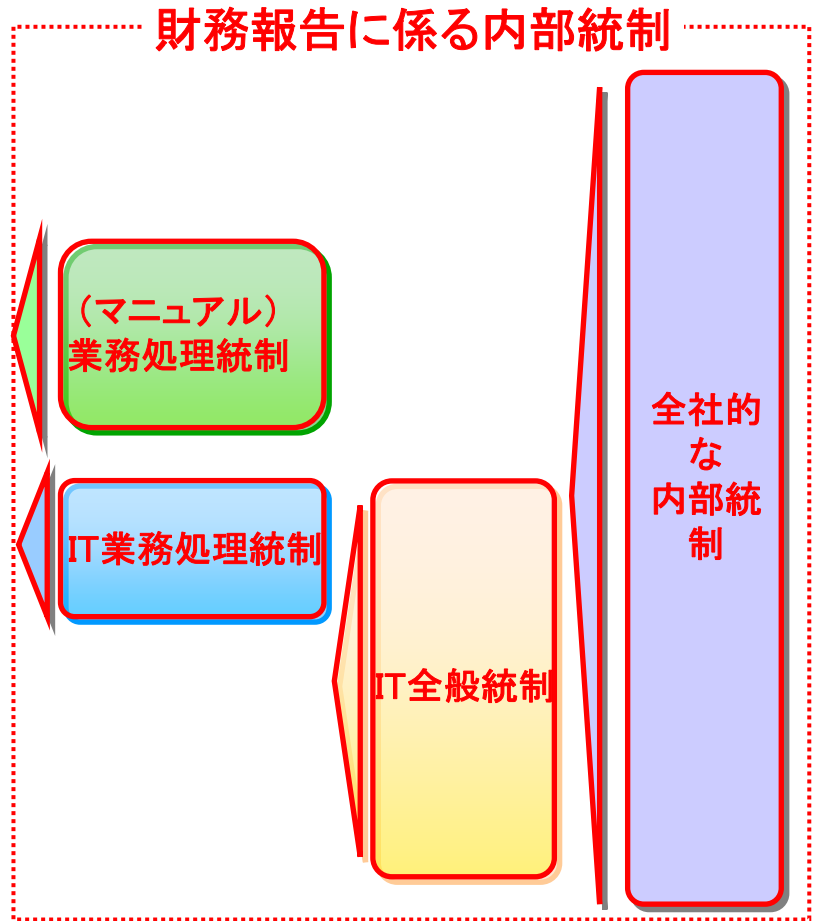
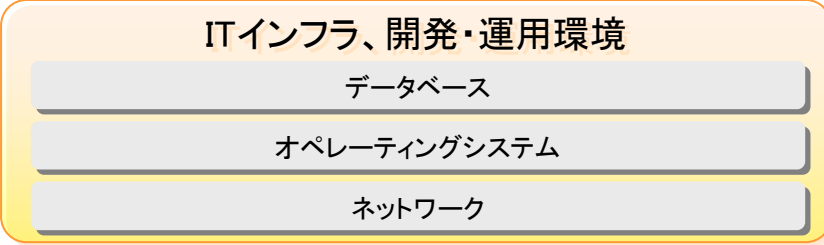
無関係なプロセス



無関係なアプリ



無関係なインフラ等



※ITガバナンス協会「サーベインズ・オクスリー法（企業改革法）遵守のためのIT統制目標」をもとに作成
http://www.itgi.org/Template_ITGI.cfm?Section=Information_Technology1&CONTENTID=24230&TEMPLATE=/ContentManagement/ContentDisplay.cfm

全社的な内部統制

『全社的な内部統制』は、企業全体に広く影響を及ぼす組織の基本的な統制として、『業務処理統制』など他の3つの統制が機能するための基盤となる

財務報告

(財務関連)業務プロセス

(財務関連)アプリケーション

ITインフラ、開発・運用環境

全社的な内部統制の例

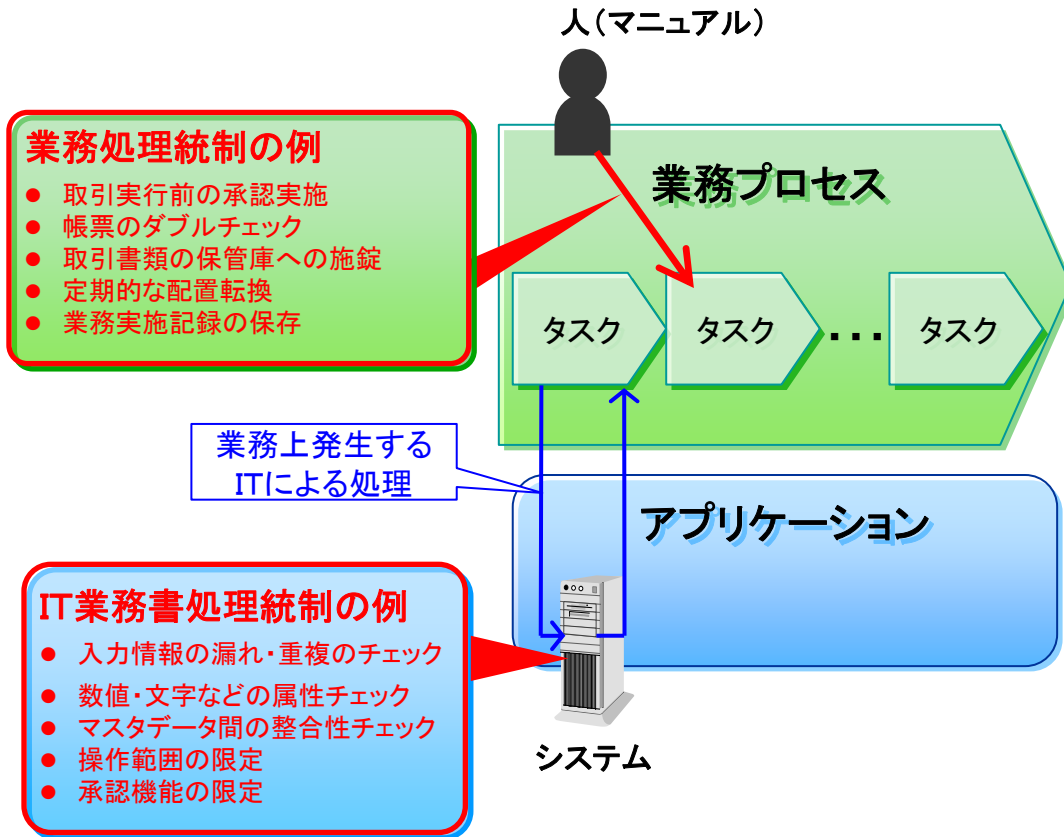
- 経営者が、信頼性ある財務報告を重視し、財務報告に係る内部統制の役割を含め、財務報告の基本方針を明確にしていること
- 取締役会、監査役または監査委員会が、財務報告とその内部統制に関し経営者を適切に監督・監視する責任を理解し、実行していること
- 信頼性のある財務報告作成のため、適切な階層の経営者、管理者を関与させる有効なリスク評価の仕組みが存在すること
- 経営者が、信頼性ある財務報告の作成に関し、職務の分掌を明確化し、権限や職責を担当者に適切に分担させていること
- 内部通報の仕組みなど、通常の通報経路から独立した伝達経路が利用できるように設定されていること
- 日常的なモニタリングが、企業の業務活動に適切に組み込まれていること
- 経営者が、内部統制を整備する際に、IT環境を適切に理解し、これを踏まえた方針を明確に示していること

■ 全社的な内部統制

経営理念、組織慣行、責任・権限等の企業全体に広く影響を及ぼし、企業全体を対象とする内部統制

業務処理統制とIT業務処理統制

『業務処理統制』と『IT業務処理統制』は、業務プロセス上で財務報告の適正性に影響を及ぼし得るリスク(アサーションの達成を妨げる可能性)に対するコントロールとして両者が一体となって機能し、財務報告の適正性を確保する



■業務処理統制

・マニュアルでの業務実施ポイントにおいて、承認された業務をすべて正確に実施、記録されることを確保するために、管理業務として業務プロセスに組み込まれる統制

■IT業務処理統制

業務を管理するシステムにおいて、承認された業務がすべて正確に処理、記録されることを確保するために、アプリケーションに組み込まれる統制

・【実施基準案で提示された評価項目】

- 入力情報の完全性・正確性・正当性を確保
- エラーデータの修正と再処理の機能の確保
- マスタデータの正確性の確保
- システム利用に関する認証・操作範囲の限定

IT全般統制

『IT全般統制』は、IT業務処理統制が有効に機能するためのIT環境を整える役割を担うことにより、財務報告の適正性の確保に対して間接的に寄与する

IT業務
処理統制

アプリケーション



システム

ITインフラ、開発・運用環境

IT全般統制の例

- システム開発工程での管理者によるレビュー・承認
- 業務分担の明確化による担当者間の相互牽制
- 臨時オペレーションにおける承認申請
- 業務委託先のサービス内容の評価手続き
- ネットワーク上のデータ量の監視
- 情報システムに関する内部監査の実施

■IT全般統制

・業務処理統制が有効に機能するIT環境を保証するための統制活動を意味しており、通常、複数の業務処理統制に関係する方針と手続きとして整備される統制

【実施基準案で提示された評価項目】

●ITの開発・保守

－「事前の承認」、「目的に適合した開発手法」、「導入に関する十分な試験とその結果の承認」、「開発・調達・変更の過程の記録・保存」、「従業員への教育・研修」

●システムの運用・管理

－「誤謬・不正等の防止策」、「障害や故障等によるデータ消失等への対策」、「障害・故障発生時の状況把握、対応」

●内外からのアクセス管理等システムの安全性確保

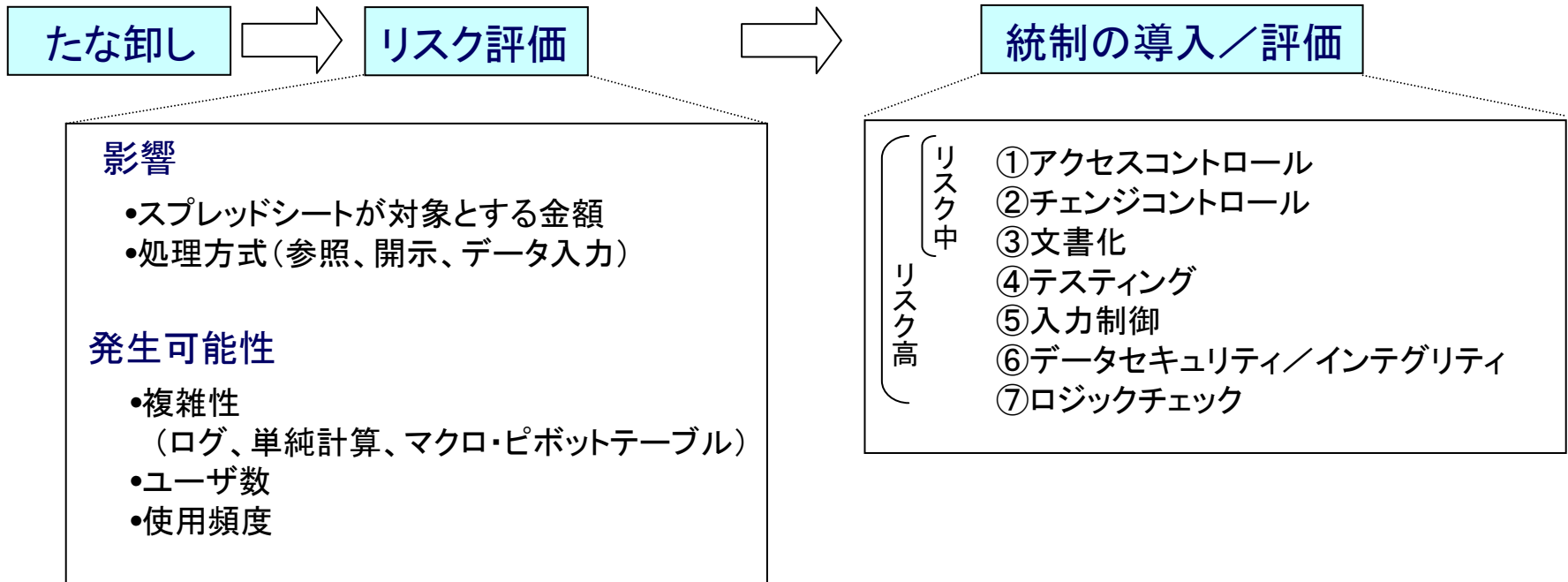
－「適切なアクセス管理等の方針を定めているか」

●外部委託に関する契約の管理

－「適切に外部委託に関する契約の管理を行っているか」

スプレッドシート統制

財務諸表作成にスプレッドシートを利用する企業はかなり多い。ある調査によれば、73%の米国企業が、スプレッドシートを財務報告プロセスの重要な部分に使用している。スプレッドシートは、簡単にデータ操作できるだけでなく、そのログ取得にも問題がある。ITガバナンス協会からは、以下のガイドラインがでている



影響・・・対象金額が大きく(重要性の50%以上)、処理方式がデータ入力であれば、高リスク
発生可能性・・・複雑性が高く、ユーザ数が多く(5以上)、さらに、使用頻度が頻繁であれば、高リスク

リスクとコントロール

監査人は、経営者が評価した個々の統制上の要点について、内部統制の基本的要素が適切に機能しているかを判断するため、**実在性、網羅性、権限と責任の明確性、記録の十分性等の監査要点**に適合した監査証拠を入手しなければならない。

出典:「財務報告に係る内部統制の評価及び監査の基準のあり方について」
平成17年12月8日 企業会計審議会内部統制部会

アサーション

- 実在性
- 網羅性
- 権利と義務
- 評価
- 発生
- 表示と開示

リスク

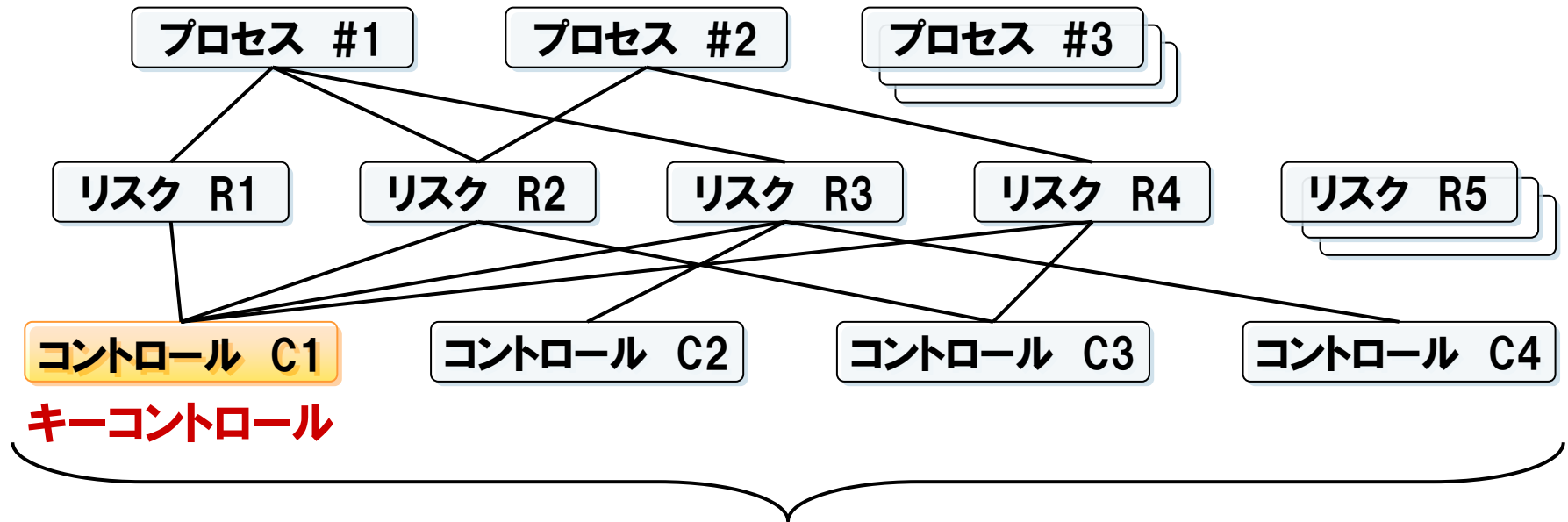
アサーションが
成立しなくなる
(破壊される)
可能性

コントロール

リスクの消失や軽減
を図ることにより、
アサーションを確保

取引の変換、移動が起こる場所で主に発生
(開始、承認、記録、処理、報告)

プロセス／リスク／コントロールの関係

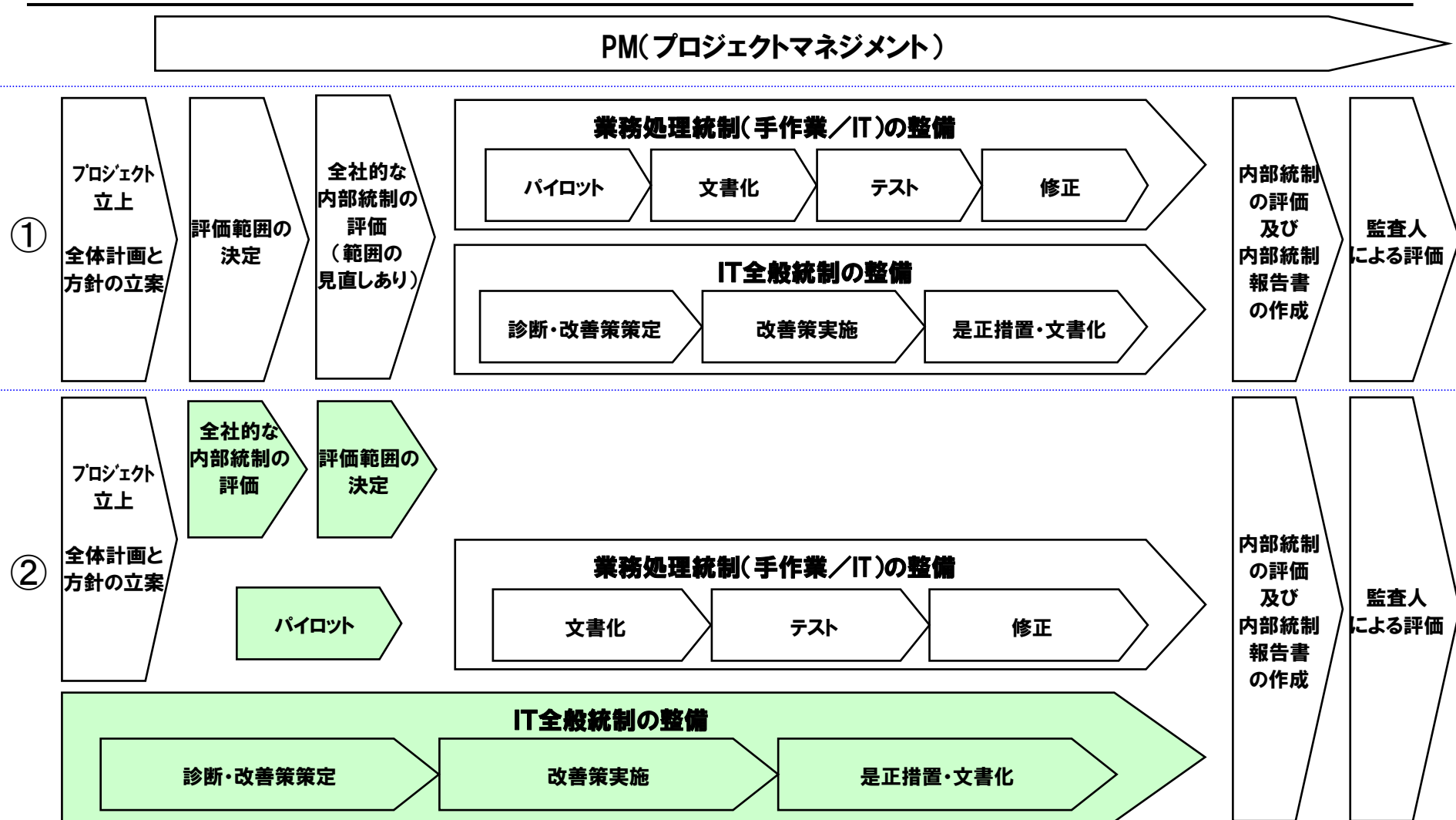


全部を実施する必要はない

以下の観点から、重要なコントロール(キーコントロール)を特定

- **複数のリスクをカバー可能**
- **予防的コントロールである**
- **比較的实现が容易**

JSOX対応計画の例(1)

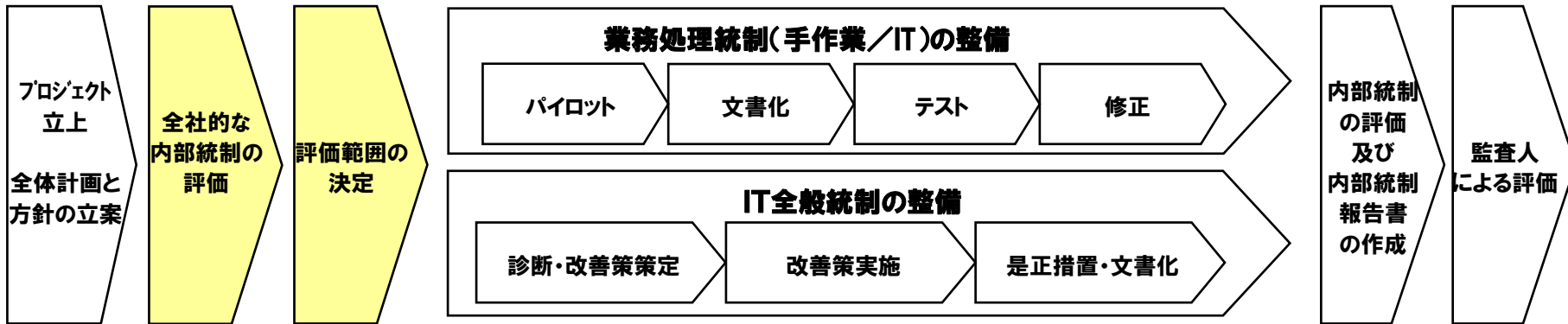


対応期間を考えた場合、②がベスト。

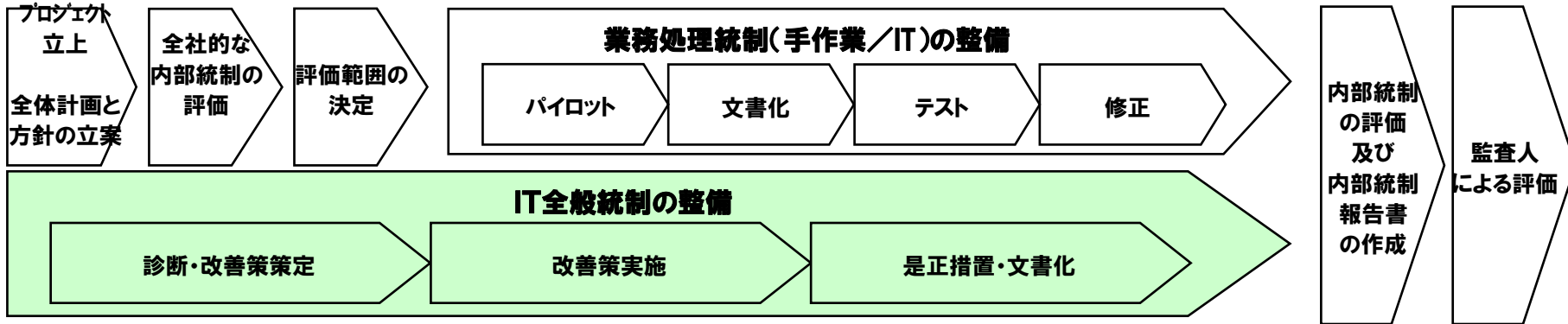
JSOX対応計画の例(2)



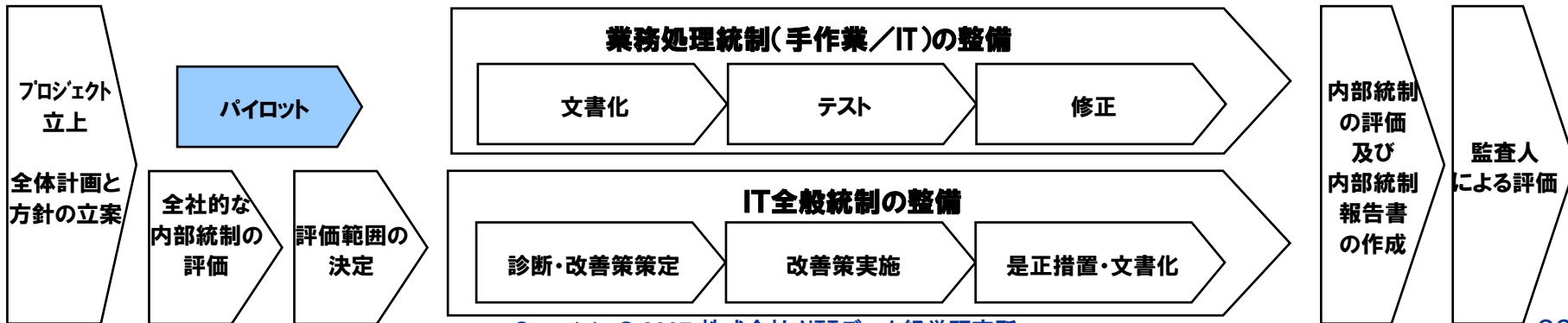
③



④



⑤



(参考) 全体計画と方針の立案・・・「財務報告」の定義

「財務報告」とは、財務諸表及び財務諸表の信頼性に重要な影響を及ぼす開示事項等に係る外部報告をいう

「財務諸表の信頼性に重要な影響を及ぼす開示事項等」とは、有価証券報告書等における財務諸表以外の開示事項等で次に掲げるものをいう。

①財務諸表に記載された金額、数値、注記を要約、抜粋、分解又は利用して記載すべき開示事項(以下「財務諸表の表示等を用いた記載」という。)

例えば、**有価証券報告書の記載事項中**、「企業の概況」の「主要な経営指標等の推移」の項目、「事業の状況」の「業績等の概要」、「生産、受注及び販売の状況」、「研究開発活動」及び「財政状態及び経営成績の分析」の項目、「設備の状況」の項目、「提出会社の状況」の「株式等の状況」、「自己株式の取得等の状況」、「配当政策」及び「コーポレート・ガバナンスの状況」の項目、「経理の状況」の「主要な資産及び負債の内容」及び「その他」の項目、「保証会社情報」の「保証の対象となっている社債」の項目並びに「指数等の情報」の項目のうち、**財務諸表の表示等を用いた記載**が挙げられる。

②関係会社の判定、連結の範囲の決定、持分法の適用の要否、関連当事者の判定その他財務諸表の作成における判断に密接に関わる事項

例えば、有価証券報告書の記載事項中、「企業の概況」の「事業の内容」及び「関係会社の状況」の項目、「提出会社の状況」の「大株主の状況」の項目における**関係会社、関連当事者、大株主等の記載事項**が挙げられる。

(参考) 全体計画と方針の立案・・・計画と方針

、経営者は、取締役会の決定を踏まえて、財務報告に係る内部統制を組織内の全社的なレベル及び業務プロセスのレベルにおいて実施するための基本的計画及び方針を定める必要がある。

基本的計画及び方針の例

- 適正な財務報告を実現するために構築すべき内部統制の方針・原則、範囲及び水準
- 内部統制の構築に当たる経営者以下の責任者及び全社的な管理体制
- 内部統制の構築に必要な手順及び日程
- 内部統制の構築に係る個々の手続に関与する人員及びその編成並びに事前の教育・訓練の方法等

(参考)内部統制の対象企業

すべての連結対象企業(組合等も含む)と委託業務先が対象となる

上場子会社・・・当該子会社の評価結果を利用可能

持分法適用子会社・・・全社統制の対象となる。

すでに内部統制監査を受けている場合、上場子会社に準じる
子会社と同様の評価が行えない場合、質問書の送付、聞き取り、
報告等の閲覧等より評価

在外子会社等・・・対象。ただし、所在地国に適切な内部統制報告制度がある場合には、
それを利用可能(第3国の制度も含まれる)

委託業務先・・・サンプリングによる検証
委託先の評価結果の利用

(参考)全社的な内部統制(1)

全社的な内部統制の評価項目と方法

評価項目・・・例:実施基準草案に例示されている評価項目(基本的要素ベース)

評価方法・・・評価対象となる内部統制全体を適切に理解及び分析した上で、**関係者への質問や記録の検証**などにより実施

評価項目例

統制環境

- ・経営者は、信頼性のある財務報告を重視し、財務報告に係る内部統制の役割を含め、財務報告の基本方針を明確に示しているか。
- ・適切な経営理念や倫理規程に基づき、社内の制度が設計・運用され、原則を逸脱した行動が発見された場合には、適切に是正が行われるようになっているか。
- ・経営者は、適切な会計処理の原則を選択し、会計上の見積り等を決定する際の客観的な実施過程を保持しているか。
- ・取締役会及び監査役又は監査委員会は、財務報告とその内部統制に関し経営者を適切に監督・監視する責任を理解し、実行しているか。
- ・監査役又は監査委員会は内部監査人及び監査人と適切な連携を図っているか。
- ・経営者は、問題があっても指摘しにくい等の組織構造や慣行があると認められる事実が存在する場合に、適切な改善を図っているか。
- ・経営者は、企業内の個々の職能(生産、販売、情報、会計等)及び活動単位に対して、適切な役割分担を定めているか。
- ・経営者は、信頼性のある財務報告の作成を支えるのに必要な能力を識別し、所要の能力を有する人材を確保・配置しているか。
- ・信頼性のある財務報告の作成に必要なとされる能力の内容は、定期的に見直され、常に適切なものとなっているか。
- ・責任の割当てと権限の委任がすべての従業員に対して明確になされているか。
- ・従業員等に対する権限と責任の委任は、無制限ではなく、適切な範囲に限定されているか。
- ・経営者は、従業員等に職務の遂行に必要な手段や訓練等を提供し、従業員等の能力を引き出すことを支援しているか。
- ・従業員等の勤務評価は、公平で適切なものとなっているか。

リスクの評価と対応

- ・信頼性のある財務報告の作成のため、適切な階層の経営者、管理者を関与させる有効なリスク評価の仕組みが存在しているか。
- ・リスクを識別する作業において、企業の内外の諸要因及び当該要因が信頼性のある財務報告の作成に及ぼす影響が適切に考慮されているか。
- ・経営者は、組織の変更やITの開発など、信頼性のある財務報告の作成に重要な影響を及ぼす可能性のある変化が発生する都度、リスクを再評価する仕組みを設定し、適切な対応を図っているか。
- ・経営者は、不正に関するリスクを検討する際に、単に不正に関する表面的な事実だけでなく、不正を犯させるに至る動機、原因、背景等を踏まえ、適切にリスクを評価し、対応しているか。

(参考)全社的な内部統制(2)

評価項目例(続)

統制活動

- ・信頼性のある財務報告の作成に対するリスクに対処して、これを十分に軽減する統制活動を確保するための方針と手続を定めているか。
- ・経営者は、信頼性のある財務報告の作成に関し、職務の分掌を明確化し、権限や職責を担当者に適切に分担させているか。
- ・統制活動に係る責任と説明義務を、リスクが存在する業務単位又は業務プロセスの管理者に適切に帰属させているか。
- ・全社的な職務規定や、個々の業務手順を適切に作成しているか。
- ・統制活動は業務全体にわたって誠実に実施されているか。
- ・統制活動を実施することにより検出された誤謬等は適切に調査され、必要な対応が取られているか。
- ・統制活動は、その実行状況を踏まえて、その妥当性が定期的に検証され、必要な改善が行われているか。

情報と伝達

- ・信頼性のある財務報告の作成に関する経営者の方針や指示が、企業内のすべての者、特に財務報告の作成に関連する者に適切に伝達される体制が整備されているか。
- ・会計及び財務に関する情報が、関連する業務プロセスから適切に情報システムに伝達され、適切に利用可能となるような体制が整備されているか。
- ・内部統制に関する重要な情報が円滑に経営者及び組織内の適切な管理者に伝達される体制が整備されているか。
- ・経営者、取締役会、監査役又は監査委員会及びその他の関係者の間で、情報が適切に伝達・共有されているか。
- ・内部通報の仕組みなど、通常の報告経路から独立した伝達経路が利用できるように設定されているか。
- ・内部統制に関する企業外部からの情報を適切に利用し、経営者、取締役会、監査役又は監査委員会に適切に伝達する仕組みとなっているか。

モニタリング

- ・日常的モニタリングが、企業の業務活動に適切に組み込まれているか。
- ・経営者は、独立的評価の範囲と頻度を、リスクの重要性、内部統制の重要性及び日常的モニタリングの有効性に応じて適切に調整しているか。
- ・モニタリングの実施責任者には、業務遂行を行うに足る十分な知識や能力を有する者が指名されているか。
- ・経営者は、モニタリングの結果を適時に受領し、適切な検討を行っているか。
- ・企業の内外から伝達された内部統制に関する重要な情報は適切に検討され、必要な是正措置が取られているか。
- ・モニタリングによって得られた内部統制の不備に関する情報は、当該実施過程に係る上位の管理者並びに当該実施過程及び関連する内部統制を管理し是正措置を実施すべき地位にある者に適切に報告されているか。
- ・内部統制に係る重要な欠陥等に関する情報は、経営者、取締役会、監査役又は監査委員会に適切に伝達されているか。

ITへの対応

- ・経営者は、ITに関する適切な戦略、計画等を定めているか。
- ・経営者は、内部統制を整備する際に、IT環境を適切に理解し、これを踏まえた方針を明確に示しているか。
- ・経営者は、信頼性のある財務報告の作成という目的の達成に対するリスクを低減するため、手作業及びITを用いた統制の利用領域について、適切に判断しているか。
- ・ITを用いて統制活動を整備する際には、ITを利用することにより生じる新たなリスクが考慮されているか。
- ・経営者は、ITに係る全般統制及びITに係る業務処理統制についての方針及び手続を適切に定めているか。

出典:「財務報告に係る内部統制の評価及び監査に関する実施基準 一公開草案一」平成18年11月21日 企業会計審議会内部統制部会 を元に編集

(参考) 業務プロセス評価の範囲

決算・財務報告プロセスで評価すべきプロセスは、全社統制に準じて、すべての事業拠点について全社的な観点で評価する。その他は、以下の方法で範囲を決定

重要拠点の選定

例えば、全社統制が良好であれば、**売上高**で上位から**全体の2/3**までを選定。全社統制の状況により、範囲は異なる。なお、下記の②で特定のプロセスのみ対象となる拠点が追加される場合がある。

評価対象プロセスの選定

- ①企業の事業目的に大きく関わる勘定科目 (**売上、売掛金及び棚卸資産等**)に至る業務プロセスは原則としてすべて対象
- ②上記以外で重要性の大きい業務プロセス、なお、重要性により一部だけでもよい
 - a. リスクが大きい取引を行っている事業又は業務に係る業務プロセス
 - 例えば、金融取引やデリバティブ取引を行っている事業又は業務や価格変動の激しい棚卸資産を抱えている事業又は業務
 - 複雑な会計処理が必要な取引を行っている事業又は業務
 - b. 見積りや経営者による予測を伴う重要な勘定科目に係る業務プロセス
 - 例えば、引当金や固定資産の減損損失、繰延税金資産(負債)など見積りや経営者による予測を伴う重要な勘定科目に係る業務プロセス
 - c. 非定型・不規則な取引など虚偽記載が発生するリスクが高いものとして、特に留意すべき業務プロセス
 - 例えば、期末に集中しての取引や過年度の趨勢から見て突出した取引
 - 売上は小さいが期末棚卸資産が非常に大きくなっている場合

経営者は、評価の範囲を決定した後に、その決定した方法及びその根拠等について、必要に応じて、監査人と協議を行っておくことが適切である。

(参考) 業務処理統制(1)

評価対象となる業務プロセスの把握・整理

- ・業務プロセスにおける取引の開始、承認、記録、処理、報告を含め、取引の流れを把握
- ・取引の発生から集計、記帳といった会計処理の過程を理解
- ・把握された業務プロセスの概要は、必要に応じ図や表を活用して整理・記録することが有用

業務プロセスにおける虚偽記載の発生するリスクとこれを低減する統制の識別

①業務プロセスにおける不正又は誤謬により、虚偽記載が発生するリスクの識別

適切な財務情報を作成するための要件

- a. 実在性－資産及び負債が実際に存在し、取引や会計事象が実際に発生していること
- b. 網羅性－計上すべき資産、負債、取引や会計事象をすべて記録していること
- c. 権利と義務の帰属－計上されている資産に対する権利及び負債に対する義務が企業に帰属していること
- d. 評価の妥当性－資産及び負債を適切な価額で計上していること
- e. 期間配分の適切性－取引や会計事象を適切な金額で記録し、収益及び費用を適切な期間に配分していること
- f. 表示の妥当性－取引や会計事象を適切に表示していること

②虚偽記載が発生するリスクを低減するための統制上の要点の識別

・特に**取引の開始、承認、記録、処理、報告**に関する内部統制を対象に、上記の要件を確保するために、どのような内部統制が必要かという観点から識別

・個々の重要な勘定科目に係る個々の統制上の要点について、内部統制が適切に機能し、上記の要件を確保する合理的な保証を提供しているかを判断することを通じて、財務報告に係る内部統制についての基本的要素が有効に機能しているかを判断する。

(参考) 業務処理統制(2)

整備状況の有効性の評価

- ・重要な勘定科目に関係する統制上の要点が適切に整備
 - ・内部統制要件を確保する合理的な保証
- を提供できているかについて、

関連文書の閲覧、従業員等への質問、観察等を通じて判断

この際、内部統制が規定の方針に従って運用された場合に、財務報告の重要な事項に虚偽記載が発生するリスクを十分に低減できるものとなっているかにより、当該内部統制の有効性を評価する。

その際には、例えば、以下のような事項に留意する。

- ・内部統制は、不正又は誤謬を防止又は適時に発見できるよう適切に実施されているか。
- ・適切な職務の分掌が導入されているか。
- ・担当者は、内部統制の実施に必要な知識及び経験を有しているか。
- ・内部統制に関する情報が、適切に伝達され、分析・利用されているか。
- ・内部統制によって発見された例外事項に適時に対処する手続が設定されているか

(参考) 業務処理統制(3)

運用状況の有効性の評価

① 運用状況の評価の内容

関連文書の閲覧、当該内部統制に係る適切な担当者への質問、業務の観察、内部統制の実施記録の検証、各現場における内部統制の運用状況に関する自己点検の状況の検討等により、業務プロセスに係る内部統制の運用状況を確認

② 運用状況の評価の実施方法

・サンプリングが基本

・サンプリング数は会計士に相談。全社統制が良好である場合、サンプリングの範囲を縮小可能

・評価対象とする営業拠点等については、計画策定の際に、一定期間で全ての営業拠点を一巡する点に留意(基本は無作為抽出)

③ 運用状況の評価の実施時期

・評価時点(期末日)における内部統制の有効性を判断するには、適切な時期に運用状況の評価を実施することが必要。通常、期末の3ヶ月以内。

④ 評価の実施方法の決定に関する留意事項

・サンプル件数、サンプルの対象期間等・・・内部統制状況により、増減が必要。監査法人等が統計的に割り出した数値を持っている。

・決算・財務報告プロセス・・・財務報告の信頼性に関して非常に重要な業務プロセスであること、その実施頻度が低いことから、他の内部統制よりも**慎重に運用状況の評価を行う必要がある。**

(参考)IT統制の概要(1)

ITを取り入れた情報システムに関する統制

- ・自動化された統制が中心
- ・一部、手作業による統制

財務報告の信頼性を確保するためのITの統制目標

正当性・・・取引が組織の意思・意図にそって承認され、行われること

完全性・・・記録した取引に漏れ、重複がないこと

正確性・・・発生した取引が財務や科目分類などの主要なデータ項目に正しく記録されること

IT全般統制

IT全般統制とは、業務処理統制が有効に機能する環境を保証するための統制活動を意味しており、通常、複数の業務処理統制に関係する方針と手続をいう。

ITに係る全般統制の具体例としては、以下のような項目が挙げられる。

- ・ ITの開発、保守に係る管理
- ・ システムの運用・管理
- ・ 内外からのアクセス管理などシステムの安全性の確保
- ・ 外部委託に関する契約の管理

例えば、システムの変更の段階で必要な内部統制が組み込まれなかったり、プログラムに不正な改ざんや不正なアクセスが行われるなど、全般統制が有効に機能しない場合には、適切な内部統制(業務処理統制)を組み込んだとしても、その有効性が保証されなくなる可能性がある。

こうした問題に対応していくためには、例えば、

- ① システムの開発又は変更の際して、当該システムの開発又は変更が既存のシステムと整合性を保っていることを十分に検討するとともに、開発・変更の過程等の記録を適切に保存する
- ② プログラムの不正な使用、改ざん等を防止するために、システムへのアクセス管理に関して適切な対策を講じるなど、全般的な統制活動を適切に整備することが重要となる。

(参考)IT統制の概要(2)

IT全般統制(続)

IT全般統制は、通常、業務を管理するシステムを支援するIT基盤(ハードウェア、ソフトウェア、ネットワーク等)を単位として構築。

例えば、購買、販売、流通の3つの業務管理システムが1つのホスト・コンピュータで集中管理されており、すべて同一のIT基盤の上で稼動している場合、当該IT基盤に対する全般統制を構築することになる。逆に別々のIT基盤で構築されている場合、それぞれに対する全般統制を構築する必要がある。

IT業務処理統制

IT業務処理統制とは、業務を管理するシステムにおいて、承認された業務がすべて正確に処理、記録されることを確保するために業務プロセスに組み込まれたITに係る内部統制である。

IT業務処理統制の具体例としては、以下のような項目が挙げられる。

- ・ 入力情報の完全性、正確性、正当性等を確保する統制
- ・ 例外処理(エラー)の修正と再処理
- ・ マスタ・データの維持管理
- ・ システムの利用に関する認証、操作範囲の限定などアクセスの管理

これらの業務処理統制は、手作業により実施することも可能であるが、システムに組み込むことにより、より効率的かつ正確な処理が可能となる。

(参考)ITを利用した内部統制の評価(1)

評価範囲

IT業務処理統制の範囲は、業務処理統制の対象業務プロセスが利用している情報システムである

IT全般統制の場合、上記の情報システムに加えて、それを支援するIT基盤の概要も把握する

- ・ITに關与する組織の構成
- ・ITに關する規程、手順書等
- ・ハードウェアの構成
- ・基本ソフトウェアの構成
- ・ネットワークの構成
- ・外部委託の状況

評価単位の識別

IT業務処理統制・・・各業務システム単位
IT全般統制・・・基本的にはIT基盤単位

IT全般統制の評価

例えば、以下の点について有効に整備・運用されているか評価

- ・ITの開発、保守
- ・システムの運用・管理
- ・内外からのアクセス管理などシステムの安全性の確保
- ・外部委託に關する契約の管理

業務処理統制の運用状況の評価の実施範囲を拡大することにより、全般統制の運用状況の評価を実施せずに、内部統制の運用状況の有効性に関して十分な心証が得られる場合もある。

(参考)ITを利用した内部統制の評価(2)

IT業務処理統制の評価

識別したIT業務処理統制が、適切に業務プロセスに組み込まれ、運用されているかを評価する。具体的には、例えば、次のような点について、業務処理統制が有効に整備及び運用されているかを評価する。

- ・入力情報の完全性、正確性、正当性等が確保されているか。
- ・エラーデータの修正と再処理の機能が確保されているか。
- ・マスタデータの正確性が確保されているか。
- ・システムの利用に関する認証・操作範囲の限定など適切なアクセス管理がなされているか。

前年度の評価結果を利用できる場合

自動化された内部統制が前年度に内部統制の不備が発見されずに有効に運用されていると評価された場合、

- ・評価された時点から内部統制が変更されていないこと、
- ・障害・エラー等の不具合が発生していないこと、
- ・関連する全般統制の整備及び運用の状況を確認及び評価した結果、全般統制が有効に機能していると判断できる場合

これらの結果を記録することで、前年度に実施した内部統制の評価結果を継続して利用することができる。

はじめに・・・コンプライアンス／内部統制／SOX法の関係

1. 米国の動向

2. 日本版SOX法(JSOX)の概要

3. 全社的な内部統制の進め方

4. IT全般統制の進め方

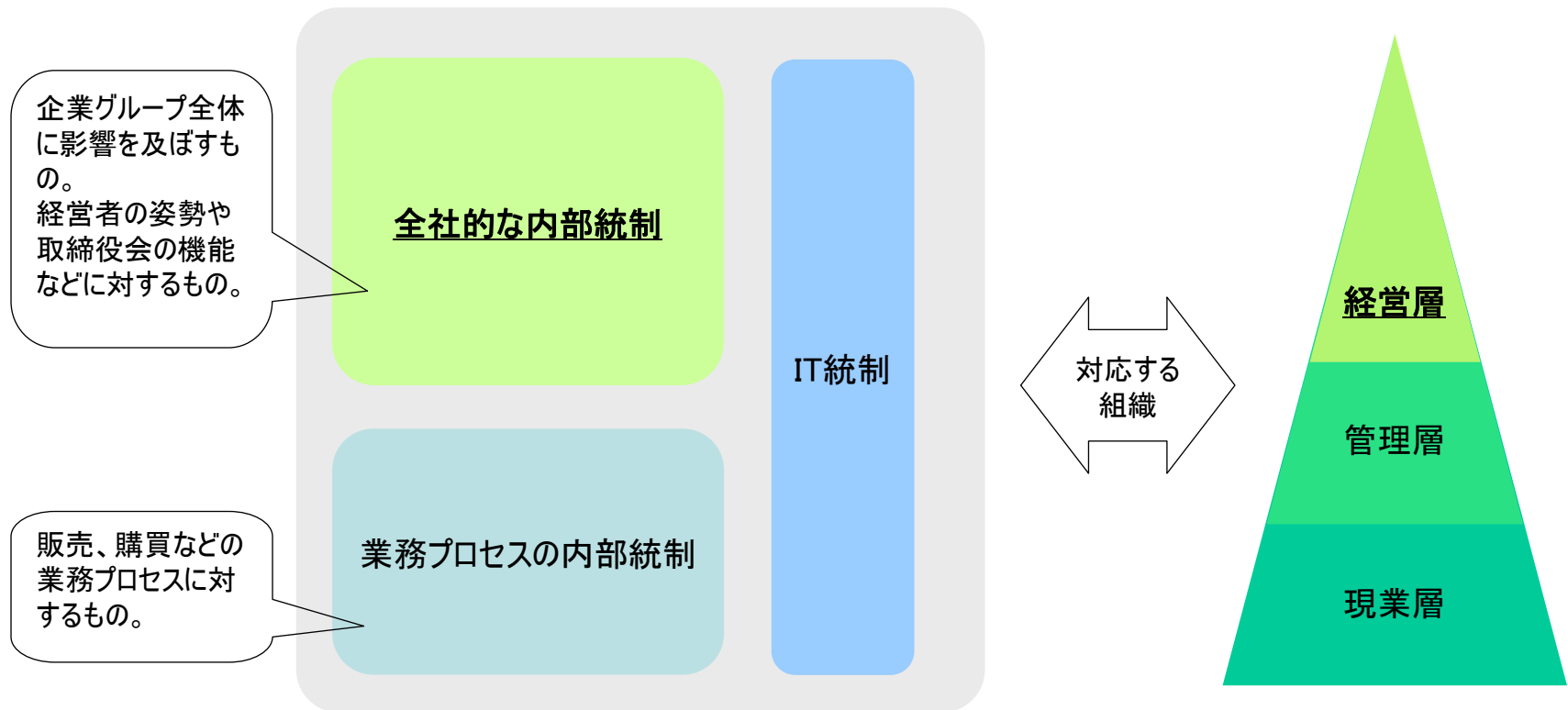
5. 投資対効果を上げる方法

おわりに 教育・資格の紹介

日本版SOX法 の構成要素

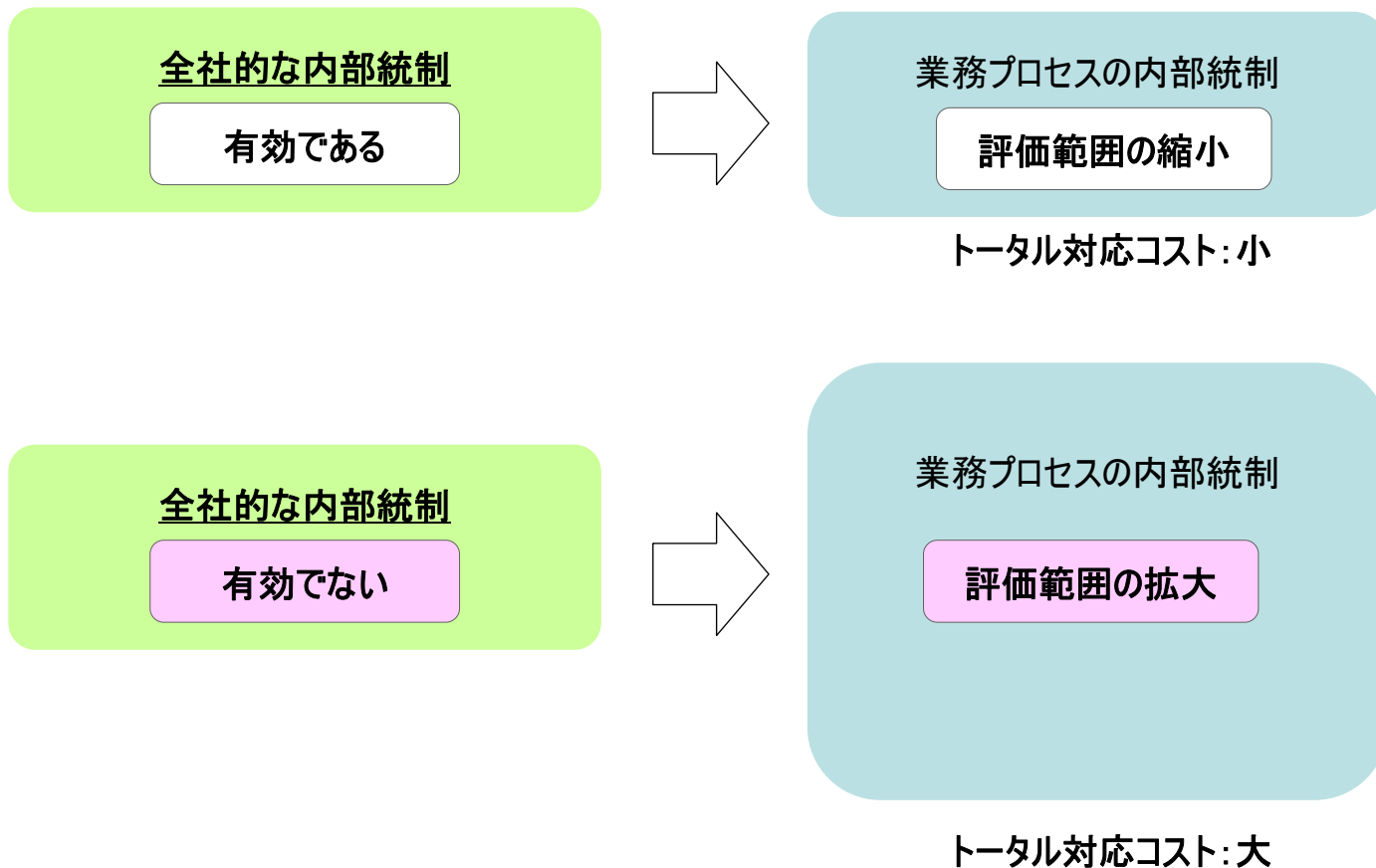
「金融商品取引法」に盛り込まれた内部統制制度（日本版SOX法）の実施基準は、企業グループ全体に影響を及ぼす「全社的な内部統制」と業務プロセスに対する「業務プロセス統制」、「IT統制」部分から構成されている

「全社的な内部統制」とは、内部統制に対する経営陣の取り組みや、全体を通じての整備状況のことであり、実施基準に評価項目の例が記載されている



「全社的な内部統制」と「業務プロセスの内部統制」の関係

日本版SOX法の実施基準では、「全社的な内部統制」の有効性に応じて、「業務プロセスの内部統制」の構築範囲が決まる



全社的な内部統制の不備の例

- a. 経営者が財務報告の信頼性に関するリスクの評価と対応を実施していない。
- b. 取締役会又は監査役若しくは監査委員会が財務報告の信頼性を確保するための内部統制の整備及び運用を監督、監視、検証していない。
- c. 財務報告に係る内部統制の有効性を評価する責任部署が明確でない。
- d. 財務報告に係るITに関する内部統制に不備があり、それが改善されずに放置されている。
- e. 業務プロセスに関する記述、虚偽記載のリスクの識別、リスクに対する内部統制に関する記録など、内部統制の整備状況に関する記録を欠いており、取締役会又は監査役若しくは監査委員会が、財務報告に係る内部統制の有効性を監督、監視、検証することができない。
- f. 経営者や取締役会、監査役又は監査委員会に報告された全社的な内部統制の不備が合理的な期間内に改善されない。

「全社的な内部統制」対応への課題

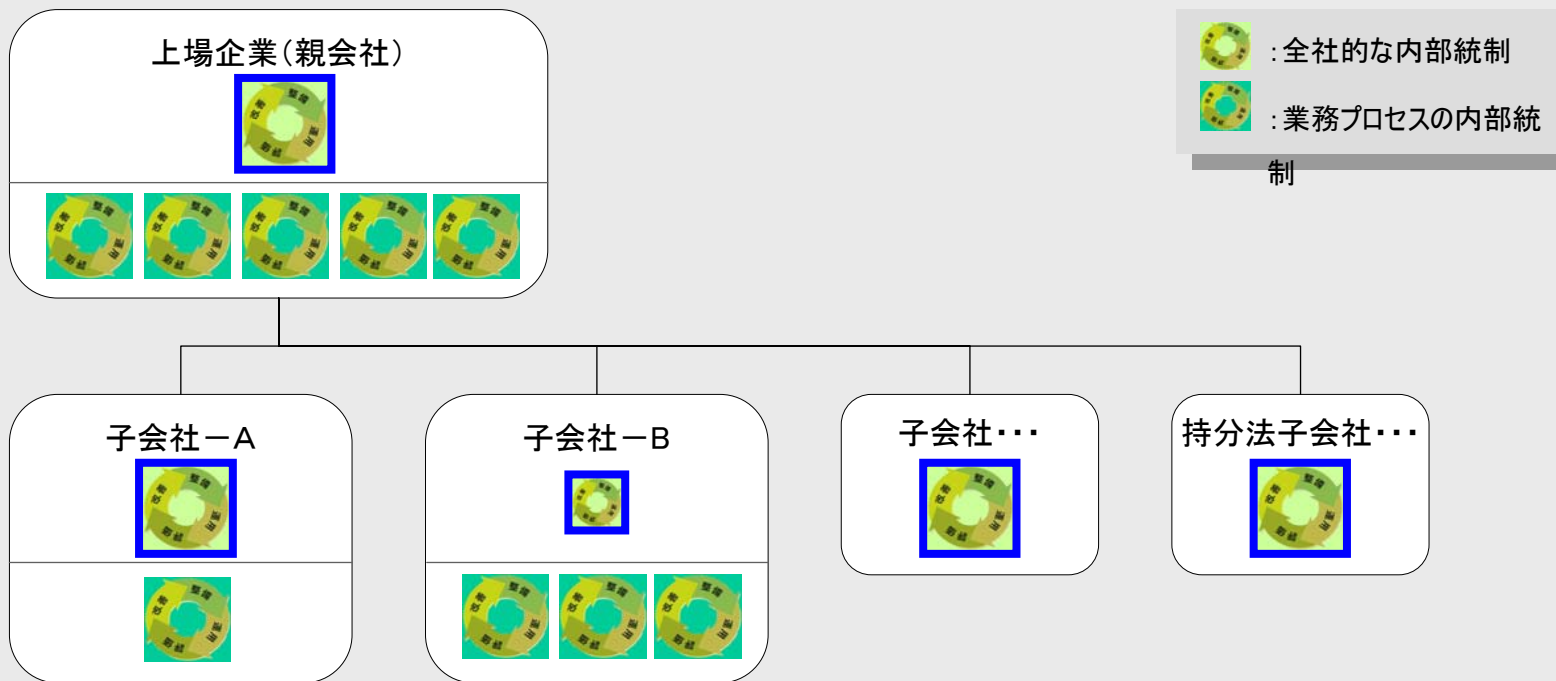
- 評価項目例から具体的な作業が把握しにくい
- 企業の組織構造や規模により、評価項目、方法が異なる
- 業務処理統制とのバランスをどう取るのか
- 評価基準があいまい。

「全社的な内部統制」対応への課題

統制要素	金融庁「実施基準」の例示	例示を具体化した評価ポイント	統制事項に対応する規程・文書名
統制環境	<p>経営者は、信頼性のある財務報告を重視し、財務報告に係る内部統制の役割を含め、財務報告の基本方針を明確に示しているか</p>	<p>取締役会・経営者は、決算財務諸表(案)を査閲している。</p> <p>取締役会・経営者は、月次財務諸表を査閲している。</p> <p>経営者は、監査人から提案された修正をレビューした後、フィードバックしている。</p> <p>経営者は、財務数値の内容を会計方針を含めて十分に理解している。</p> <p>取締役会・経営者は、関連子会社・支店(海外子会社を含む)の財務諸表を入手し、業績分析結果などを検討している。</p>	<ul style="list-style-type: none"> ・取締役会規程 ・関係会社管理・報告規程

「全社的な内部統制」の現状を把握

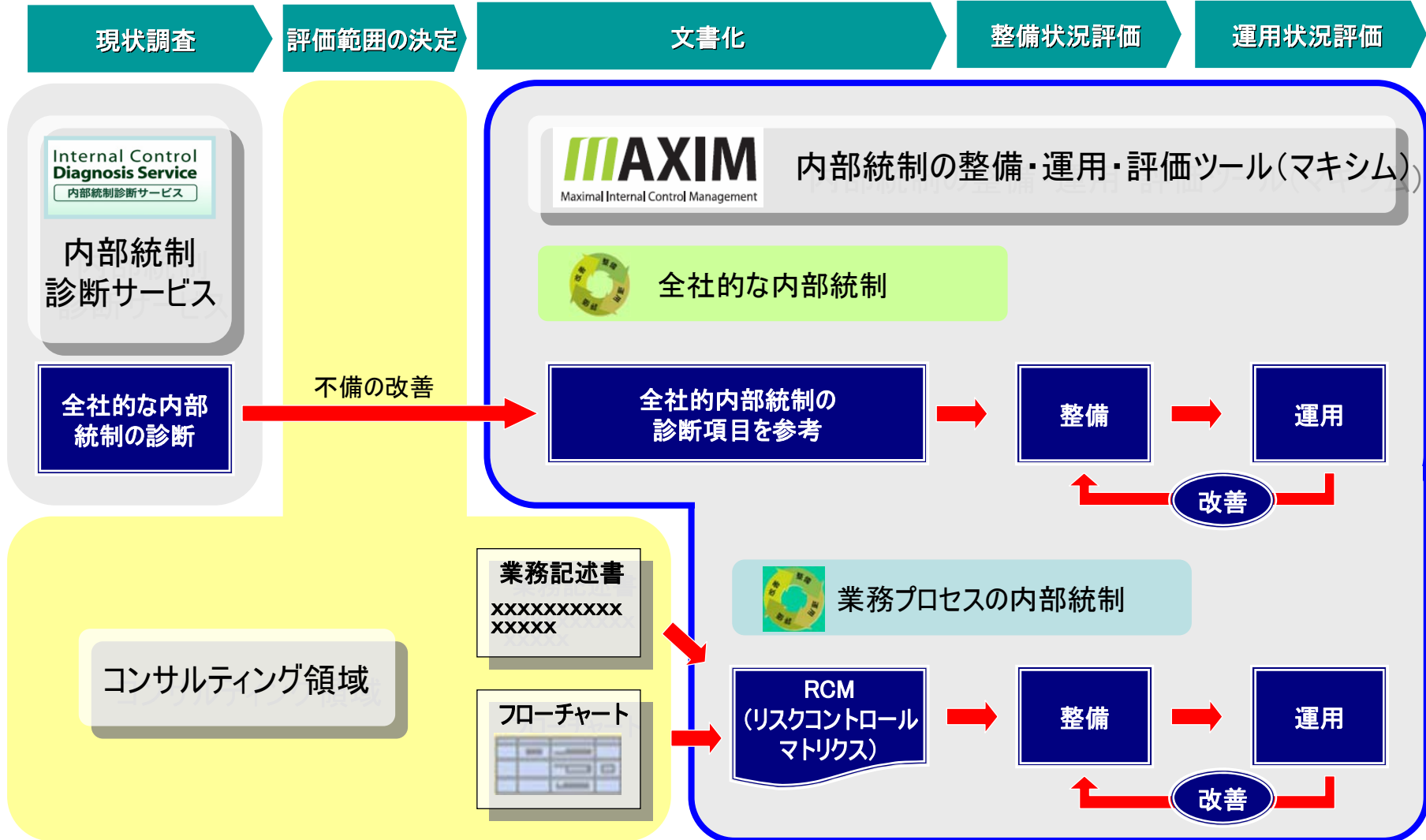
「全社的な内部統制」の評価範囲は、基本的に「親会社」、「子会社」、「持分法子会社等」が対象となる。経営者は、企業グループ全体の「全社的な内部統制」の整備・運用状況を把握する必要がある



(参考) 内部統制構築におけるツールの活用

★ 不備に対する改善コンサルティング

★ 「全社的な内部統制」の診断した項目を、内部統制の整備・運用ルーツ(マキシム)で継続管理



はじめに・・・コンプライアンス／内部統制／SOX法の関係

1. 米国の動向

2. 日本版SOX法(JSOX)の概要

3. 全社的な内部統制の進め方

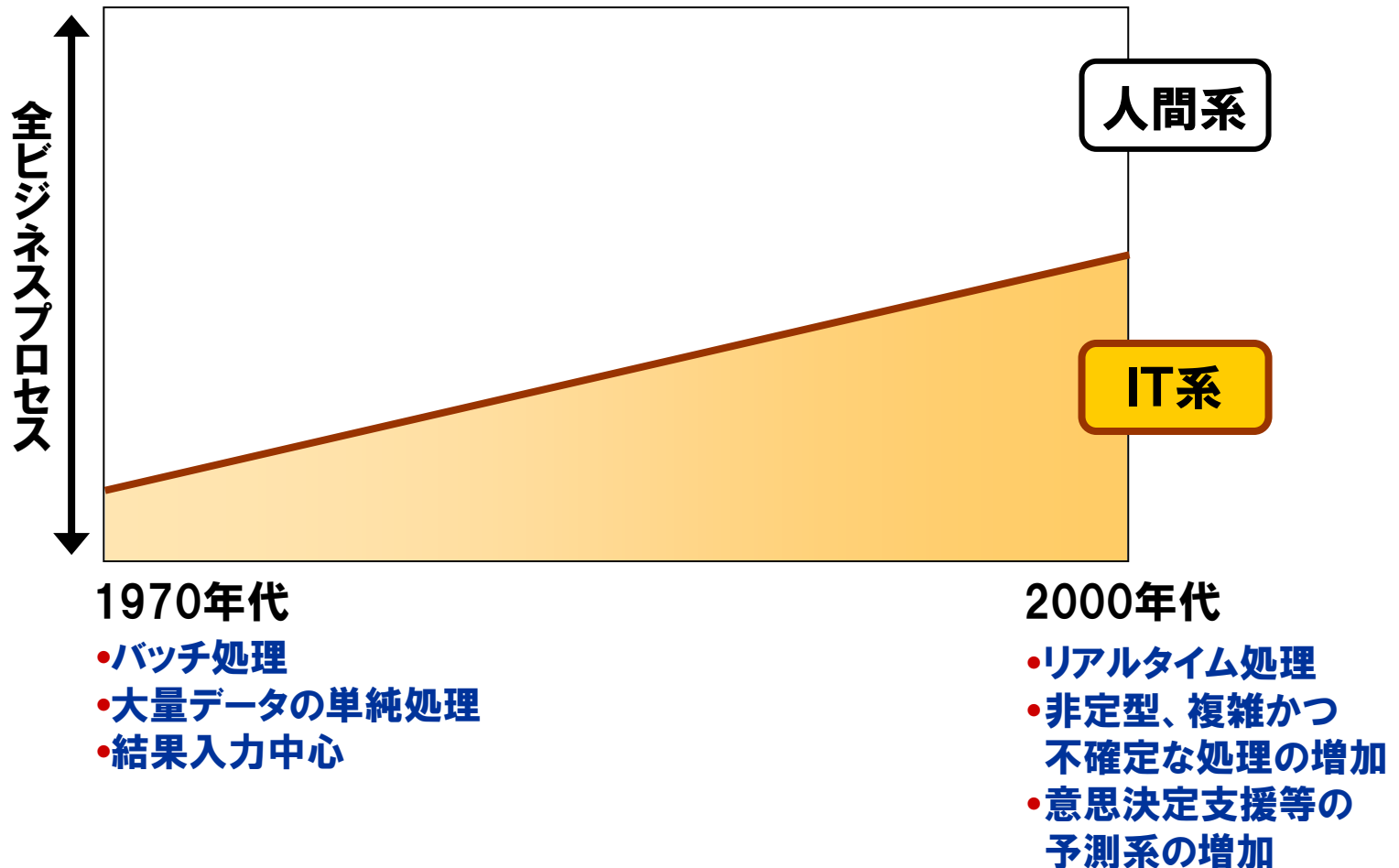
4. IT全般統制の進め方

5. 投資対効果を上げる方法

おわりに 教育・資格の紹介

ITプロセスの位置づけ

ITプロセスが全ビジネスプロセスに占める割合は上昇しており、現在では、重要な位置づけを担うようになっている。したがって、内部統制を向上するためには、ITプロセスの対応にますます力点を置く必要が高くなってきている。



ITガバナンスの必要性

1970年代

現在

企画・管理機能は貧弱

企画・管理機能の強化が必要

標準化(EA)

プレゼンテーション機能

プレゼンテーション機能

プレゼンテーション機能

プレゼンテーション機能

WEBサービス、メール等

アプリケーション

アプリケーション

アプリケーション

アプリケーション

アプリケーション

アプリケーション

データ

データ

データ

データ

インフラ

インフラ

インフラ

インフラ

- ITの発展
- ITプロセスの比重大
- 情報系のニーズ増加

IT全般統制の重要性

米国におけるSOX法対応の事例から見ると、IT全般統制の不備・欠陥が発見され、改善対策が必要である例が多い。IT全般統制の認識の低さ、対応の難しさが原因と想定される

米国におけるSOX法対応の事例

(空白)

IT全般統制の特徴

● アウトソース先への依存

- ITスキルの専門性から、自社の業務プロセスに対する統制と比較してアウトソース先への依存度が高く、管理統制が十分に行きとどいていないことが多い

● 改善に必要な時間の長期化

- 自社要員がオーナーとなっている業務プロセス上のコントロールの改善と比較して、IT全般統制の改善(ID管理ツールの導入、運用業務の標準化、等)には時間を要する

● 改善対象の広範化

- IT全般統制は、情報システムの戦略・企画／開発・調達／運用・保守というライフサイクル上に必要なマネジメントプロセスの全てを対象としているため、改善対象範囲が広い

米国の大手企業はITガバナンスの成熟度(水準)が比較的高いが、それでも、これだけの不備・欠陥が指摘されている

各企業体において、日本版SOX法が要求するIT全般統制は最優先課題といえる

IT全般統制への取組

IT全般統制を確立していくには、ITに関わる広範囲のマネジメントプロセスに対し、統制の整備(現状診断、改善策策定、改善策実施)、統制の運用(テスト、是正措置)という多くの作業が必要であり、特に改善策の実施においては多大な作業と時間を要する

対象となるマネジメントプロセス(※)
アプリケーションソフトウェアの調達と開発
技術インフラの調達と保守
方針、運用手続きの作成と維持
アプリケーションソフトウェアと技術インフラの導入とテスト
変更管理
サービスレベルの定義と管理
サードパーティーサービスの管理
システム・セキュリティの保証
構成の管理
問題と事故管理
データ管理
オペレーション管理

IT全般統制に関するタスク

[統制の整備]

● 診断

⇒ 対象プロセスにおける問題点を把握

● 改善策策定

⇒ 問題点に対する改善策を策定

● 改善策実施

⇒ ドキュメント・体制の整備、インフラ改善などの各種改善策を実施

● 文書化

⇒ RCMなどの文書の作成

[統制の運用]

● テスト

⇒ 整備されたとおりに統制が実施状況を確認

● 是正措置

⇒ 必要に応じて統制に関する是正措置を実施

例1)

システムへのアクセスを制御しているID管理に不備(共有IDの利用、等)があった場合、ID管理ツールの改修やID体系の見直し(付与規則、等)などの多くの作業と時間を要する

例2)

データを分散保管しており、保護対策が不十分であった場合、データの集中管理(ストレージ導入、等)、データ暗号化対策などの多くの作業と時間を要する

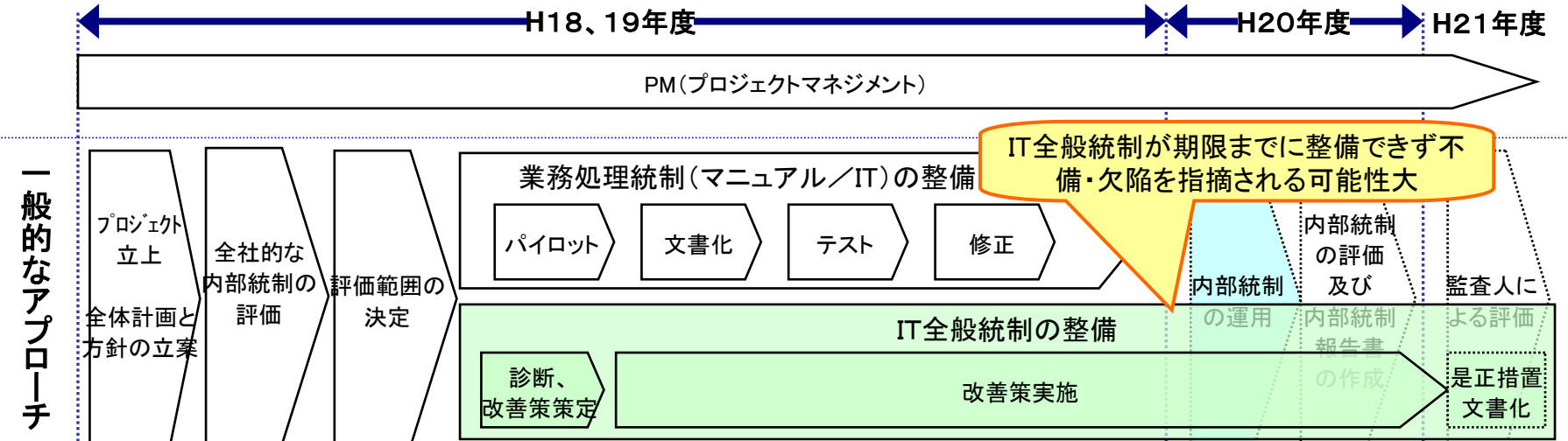
一方、業務処理統制では・・・

『受注伝票の権限者による承認が実施されていないので、権限管理規定に基づき、権限者による承認を行うよう業務マニュアルを修正する』などのようにIT全般統制の改善と比較して作業と時間は少ない

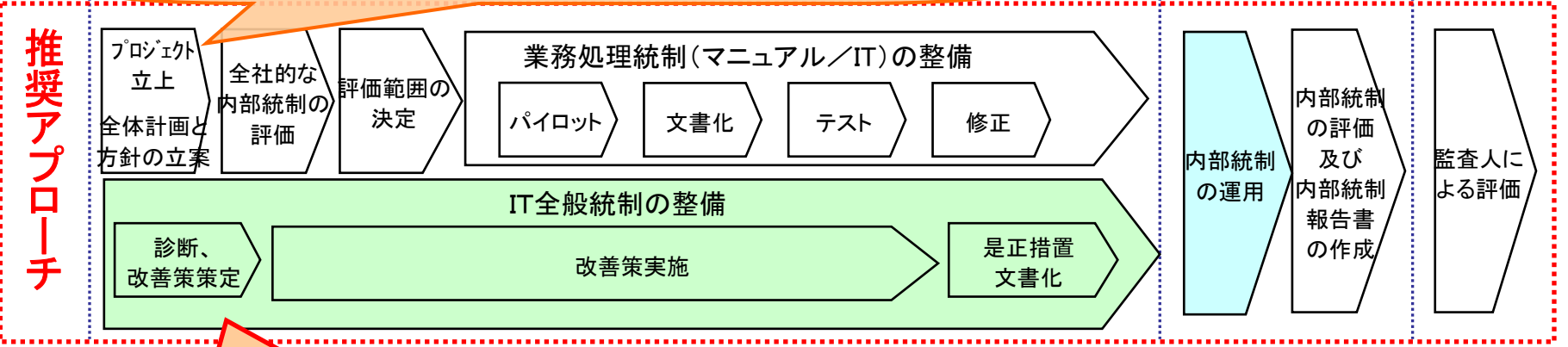
※ 対象プロセスとして、COBITにおけるITガバナンスの34プロセスのうち、SOX法のIT全般統制に関連する12のプロセスを記載
出展: IT Governance Institute「サーベインズ・オクスリー法(企業改革法)遵守のためのIT統制目標」

プロジェクトの進め方

IT全般統制は、業務処理統制の整備とは独立した活動であり『評価範囲の決定』として対象範囲を絞り込めるものではないため、先行して整備を進めることが可能であることから、改善策実施期間を考えると、早急に開始すべきである



「実施基準」等が公になった後に整備を開始した方が手戻りが少ない



IT全般統制を先行着手

IT全般統制を強化するために活用可能な管理手法、方法論

COBIT

COBIT: Control Objectives for Information and related Technology.
IT Governance InstituteとInformation Systems Audit and Control Foundation
の登録商標。

米国の情報システムコントロール協会が提唱する組織のITガバナンスの水準(成熟度)を評価するフレームワーク

エンタープライズ・アーキテクチャ (EA)

ビジネスとITのアーキテクチャを構築し管理・運営する方法論

ISO9001

品質マネジメントシステムの国際規格

ISMS / BS7799 / ISO27001 & ISO17799

情報セキュリティ管理に関する日本版標準規格 / 英国規格 / 国際規格

PMBOK

PMBOK: the Project Management Body Of Knowledge.
米国プロジェクトマネジメント協会 (PMI: Project Management Institute) の商標

米国プロジェクトマネジメント協会が提唱するプロジェクトマネジメント用フレームワーク。米国プロジェクトマネジメント協会の商標

ISO20000 / BS15000 / ITIL

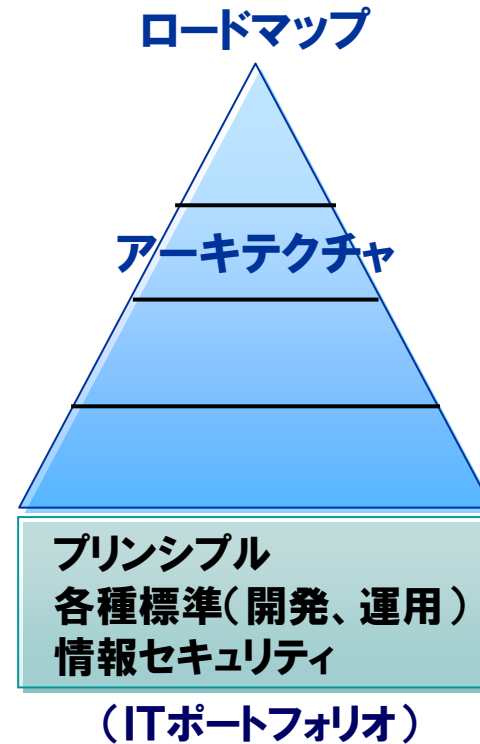
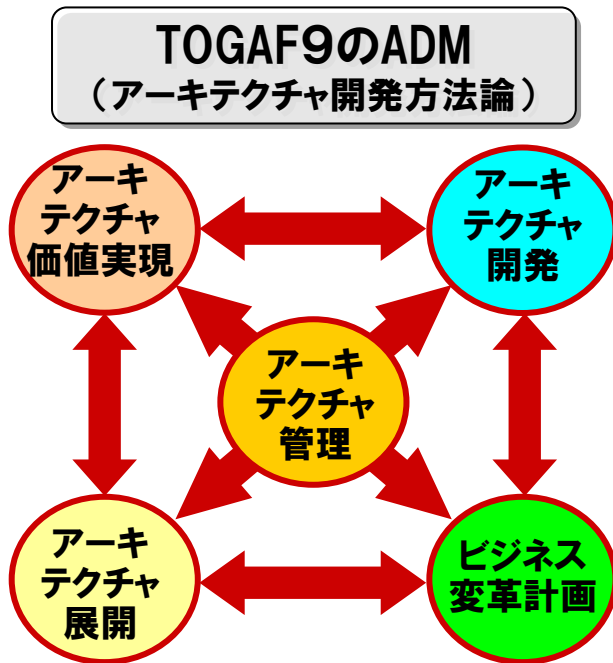
ITシステムの運用・管理業務に関する国際規格 / 英国規格 / ベストプラクティス

ITIL: Information Technology Infrastructure Library.
英国商務省 (Office of Government Commerce) の登録商標

いずれも、SOXが要求している範囲を超えている点に注意が必要である。従って、SOX対応だけであれば、例えばCOBITを全面適用する必要はない

IT全般統制実現の土台となるITアーキテクチャ（EA）の構築

EAを構築することにより、標準化、ITの方向性、ITアーキテクチャの可視化と共有等、ITを利用する上での基盤が整備される。一見、遠いようだが、SOX法対応を行う上でも重要である



IT統制のさまざまな部分で、統制水準の向上に貢献する

TOGAF: The Open Group Architecture Framework.
The Open Groupの登録商標

COBITの概要 – 成熟度

COBITで定義されたプロセスにはそれぞれにおいて統制の観点としてCSF(重要成功要因)が整理されており、このCSFにより各プロセスの成熟度レベルを6段階で診断できるようになっている

成熟度の定義

成熟度	定義
0: 不在	コントロールが存在せず、課題があることも認識されていない状態
1: 初期状態	課題が認識されているが標準が存在せず、担当者ベースで対応している状態
2: 再現性	公式な手続は定められていないが、担当者が概ね同一の手続を再現できる状態
3: 定義	手続が標準化、文書化されており、研修等により周知されている状態
4: 管理	プロセスに対してPDCAサイクルが適用されている状態
5: 最適化	プロセスが最適化され、ベストプラクティスのレベルまで高められている状態

成熟度の評価例



出典: IT Governance Institute "COBIT 3rd Edition Executive Summary" COBIT 第3版 マネジメントガイドラインを元に編集

COBIT: Control Objectives for Information and related Technology.
 IT Governance InstituteとInformation Systems Audit and Control Foundation
 の登録商標。

COBITの概要 – COBITと米国SOX法の関連

ITガバナンス協会のガイドラインによれば、COBITの12のITプロセスにおける統制目標を達成することで、米国SOX法におけるIT全般統制を実現できるとされている

COBITのITプロセス		米国SOX法におけるIT全般統制			
		プログラム開発	プログラム変更	コンピュータ運用	プログラムとデータへのアクセス
調達と導入 (A I)	AI2: アプリケーションソフトウェアの調達と開発	●	●	●	●
	AI3: 技術インフラの調達と保守	●	●	●	
	AI4: 操作、運用手続の作成と維持	●	●	●	●
	AI5: システムの導入と受入信認	●	●	●	●
	AI6: 変更管理		●		●
	DS1: サービスレベルの定義と管理	●	●	●	●
提供と支援 (D S)	DS2: サードパーティのサービス管理	●	●	●	●
	DS5: システム・セキュリティの保証			●	●
	DS9: 構成管理			●	●
	DS10: 問題と事故の管理			●	
	DS11: データ管理			●	●
	DS13: オペレーション管理			●	●

COBIT: Control Objectives for Information and related Technology.
IT Governance InstituteとInformation Systems Audit and Control Foundation
の登録商標。

■ ※ITガバナンス協会「サーベインズ・オクスリー法(企業改革法)遵守のためのIT統制目標」をもとに作成
http://www.itgi.org/Template_ITGI.cfm?Section=Information_Technology1&CONTENTID=24230&TEMPLATE=/ContentManagement/ContentDisplay.cfm

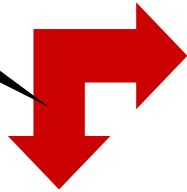
IT統制構築上の注意点

範囲	財務情報の開始・記録・処理・報告に関わるIT(システム、アプリケーション、ITロケーション)。直接、業務プロセスと関係があるITアプリケーション統制は、範囲を確定しやすい。間接的な IT全般統制はかなり範囲が広がる 。
地理的な条件	ITの設備、リソースの物理的な配置を考慮
アウトソーサ	アウトソーシングしている場合には、 アウトソーサの内部統制の証明 が必要
成熟度	日本企業は、ITガバナンス(COBIT)の 成熟度が低い 。成熟度が向上するにはそれなりに時間がかかる。
ITプロセスの可視化とテスト	ITプロセスが可視化可能かどうかも重要である。また、テスト方法も十分検討すべきである。
現状資産の有効活用(次頁)	まず、現状の資産(ドキュメント等)の調査を行い、完成度を確認すべきであろう。また、QMS等の マネジメントシステムを構築 している場合には、そのドキュメントや仕組みも活用すべきである
構築時間	半年から1年以上 、IT統制の文書化・評価作業に費やされる。

COBIT: Control Objectives for Information and related Technology.
IT Governance InstituteとInformation Systems Audit and Control Foundation
の登録商標。

(参考) IT全般統制・・・対応状況の確認

カバレッジ、
内容の深さ
等を確認



既存文書

- 外部委託先管理
- 情報セキュリティ規定
- 情報セキュリティ対策基準
- 情報危機管理計画書
- 運用管理手順
- 開発維持保守手順

COBITのITプロセス		米国SOX法におけるIT全般統制			
		プログラム開発	プログラム変更	コンピュータ運用	プログラムとデータへのアクセス
調達と導入(AI)	AI2: アプリケーションソフトウェアの調達と開発	●	●	●	●
	AI3: 技術インフラの調達と保守	●	●	●	●
	AI4: 操作、運用手続の作成と維持	●	●	●	●
	AI5: システムの導入と受入信認	●	●	●	●
	AI6: 変更管理	●	●	●	●
	提供と支援(DS)	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管理		●	●	●	●
DS5: システム・セキュリティの保証		●	●	●	●
DS9: 構成管理				●	●
DS10: 問題と事故の管理				●	●
DS11: データ管理				●	●
DS13: オペレーション管理				●	●

カバーされている
かどうか不明
(おそらく不十分)



COBIT: Control Objectives for Information and related Technology. IT Governance InstituteとInformation Systems Audit and Control Foundationの登録商標。

COBITのSOX法対応への適用例

ある調査では、90%の企業が、SOX法対策に際して、COBITを何らかの形で使用。

(空白)

IT全般統制構築上のポイント

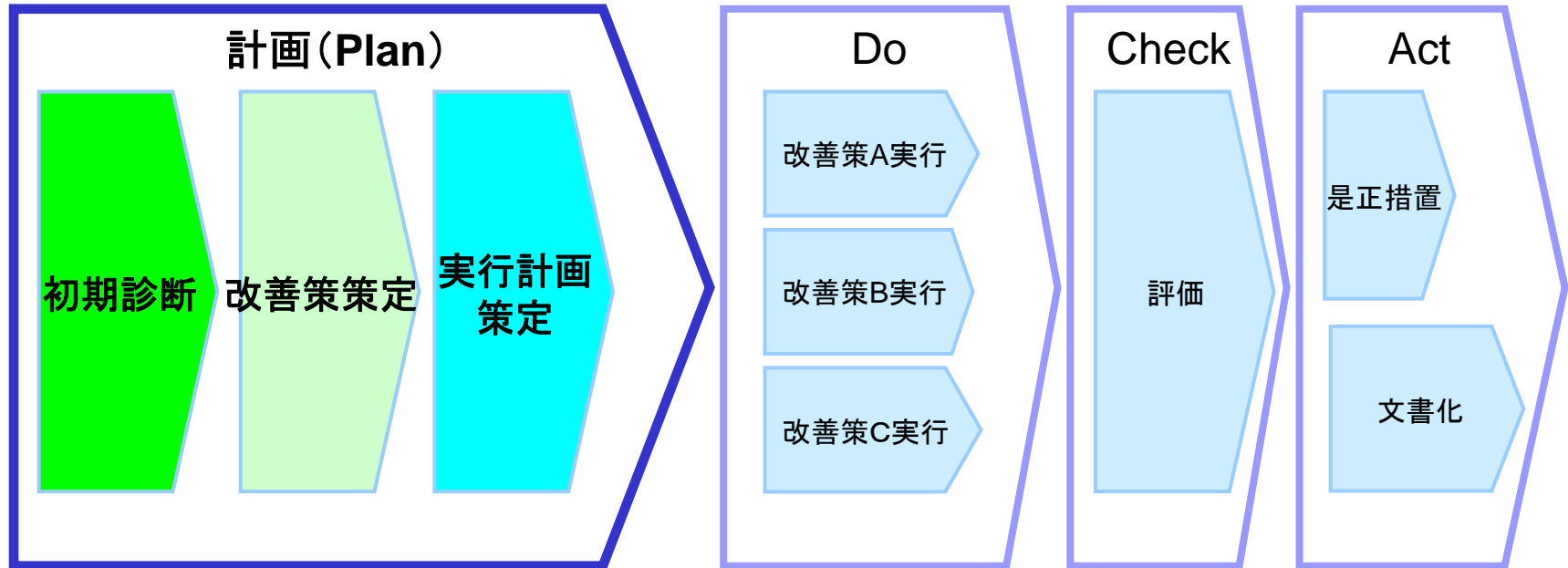
- 1 方法論、フレームワークを効果的に活用
- 2 運用段階におけるコストも考慮し、IT化を推進
- 3 ITツールの選択、システムの更新を決定する場合には、全体観が不可欠
- 4 成熟度が低い企業でも、何らかの仕組み・基準等を保有しているはず。既存の財産を有効活用することを検討すること

検討の流れ ー全体像

IT全般統制の強化は、現状把握とそれにもとづく改善策の策定(Plan)→策定した改善策の実施(Do)→改善策の事後評価(Check)→事後評価結果にもとづく是正措置(Act)といった、PDCAサイクルを通して行うことが一般的である

2006年度(1月～3月)

2007年度以降



- 予備調査と本調査により、現状の統制状況を診断
- 改善策を策定し、実施すべき策を選定
- 改善策の実施手順の詳細化と計画策定

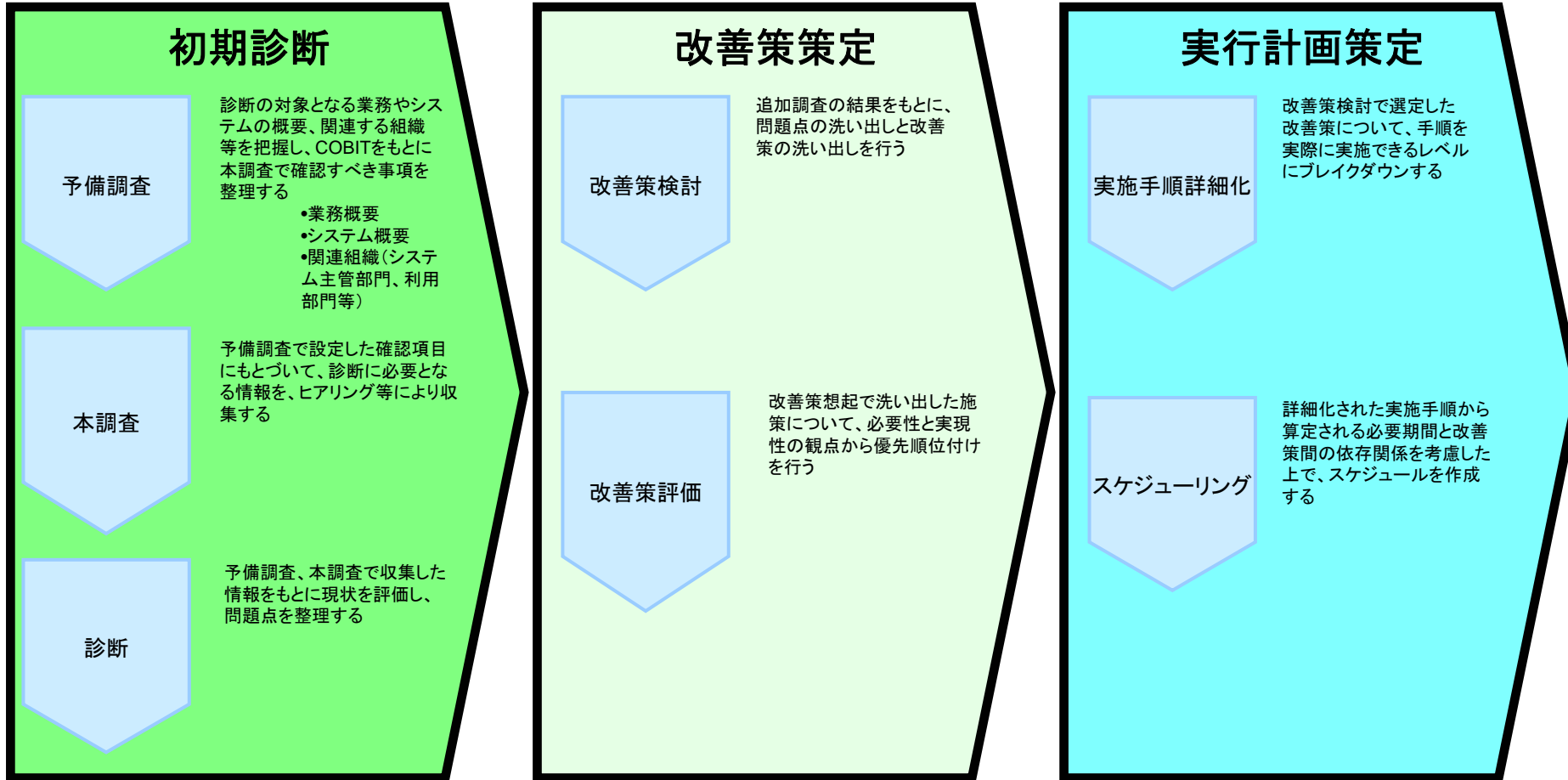
- 実行計画にもとづく各改善策の実施
- かなり時間がかかる

- 改善策実施後の状況の評価

- 評価で確認された問題の是正措置
- 必要となる文書の作成

計画段階における作業

計画段階では、現状を分析し、診断後に、必要な改善策を検討し、それらの実施計画の策定を行う



はじめに・・・コンプライアンス／内部統制／SOX法の関係

1. 米国の動向

2. 日本版SOX法(JSOX)の概要

3. 全社的な内部統制の進め方

4. IT全般統制の進め方

5. 投資対効果を上げる方法

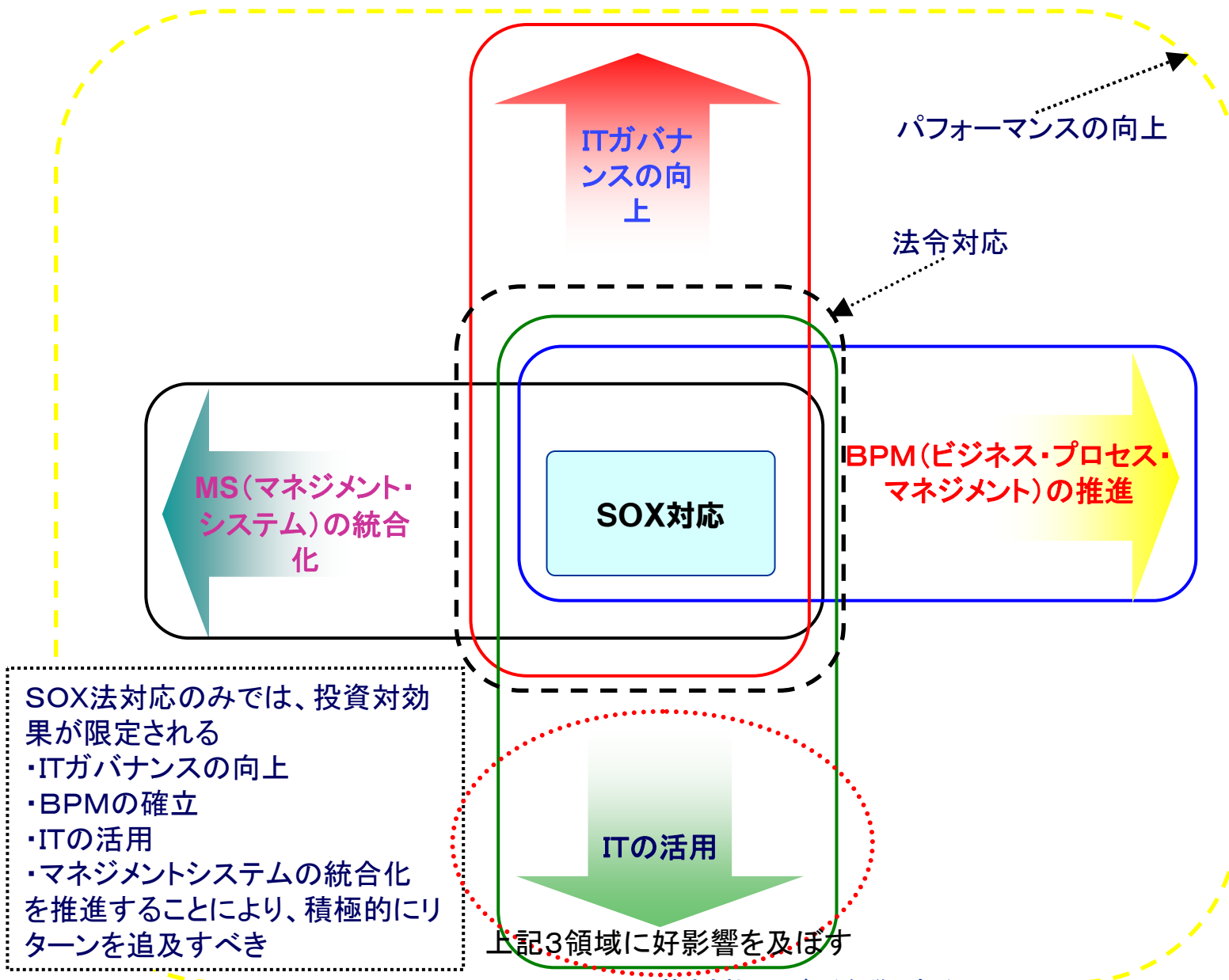
おわりに 教育・資格の紹介

法令対応のみで効果を上げる方法

SOX(JSOX)対応において、最低限の対応(法令対応)のみを行う場合、いわゆる作業の効率化以外での効果を上げるための選択肢は少ない。

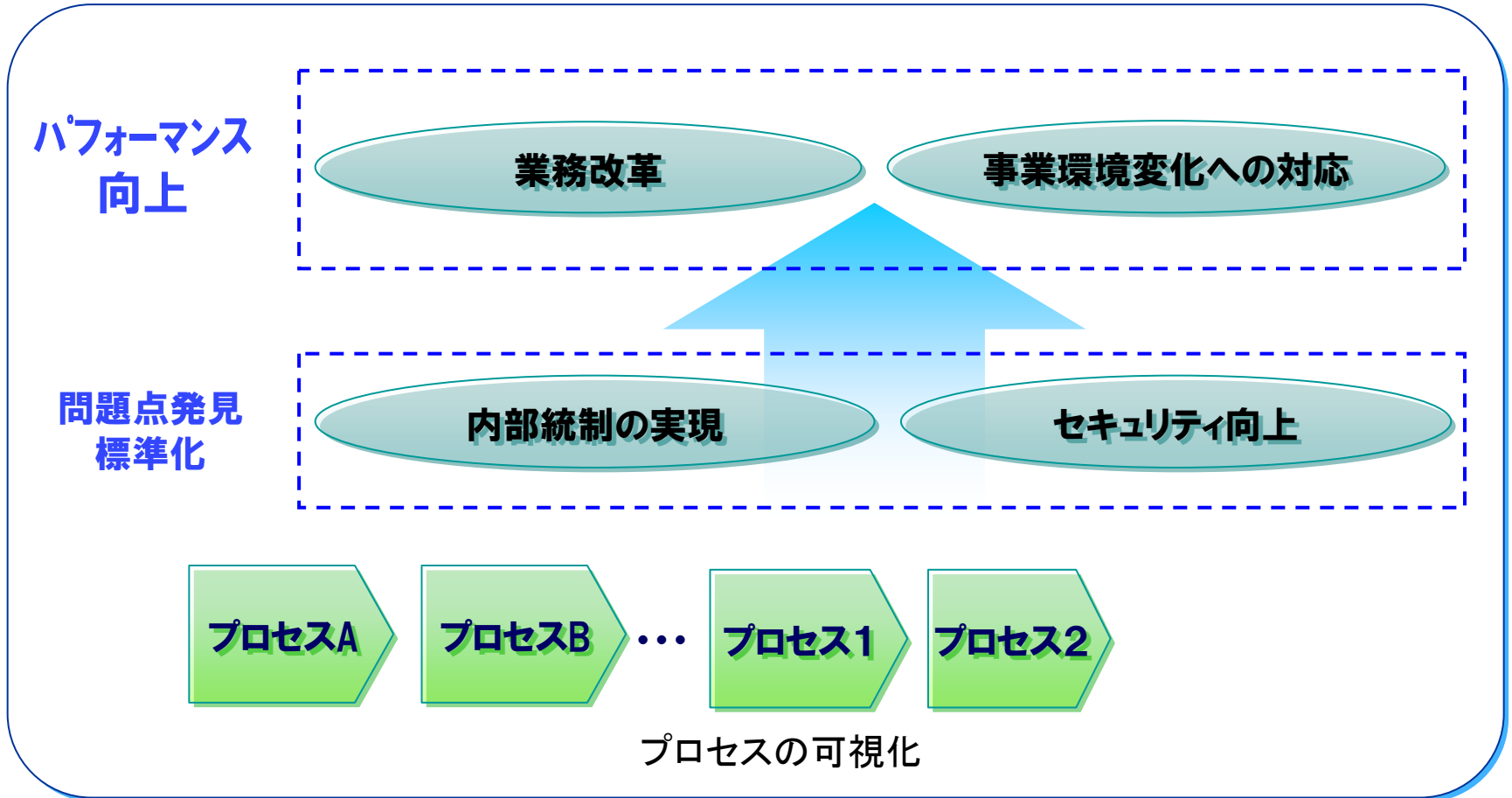
- 1 **できるだけ自社(業務部門)で作成**
自分でやる→問題に気がつく→改善につながる
- 2 **標準化の推進が必須**
用語、表現方法、粒度など
- 3 **適切なツールの選択**
表現力・・・書きやすいこと
メンテしやすいこと
SOX対応などの機能があること
共用が容易なこと
文書管理能力があること・・・体系化、文書ファイル等のリンク等
シミュレーション機能
ワークフローへの連携

効果上げるための視点と対象領域



BPMの推進

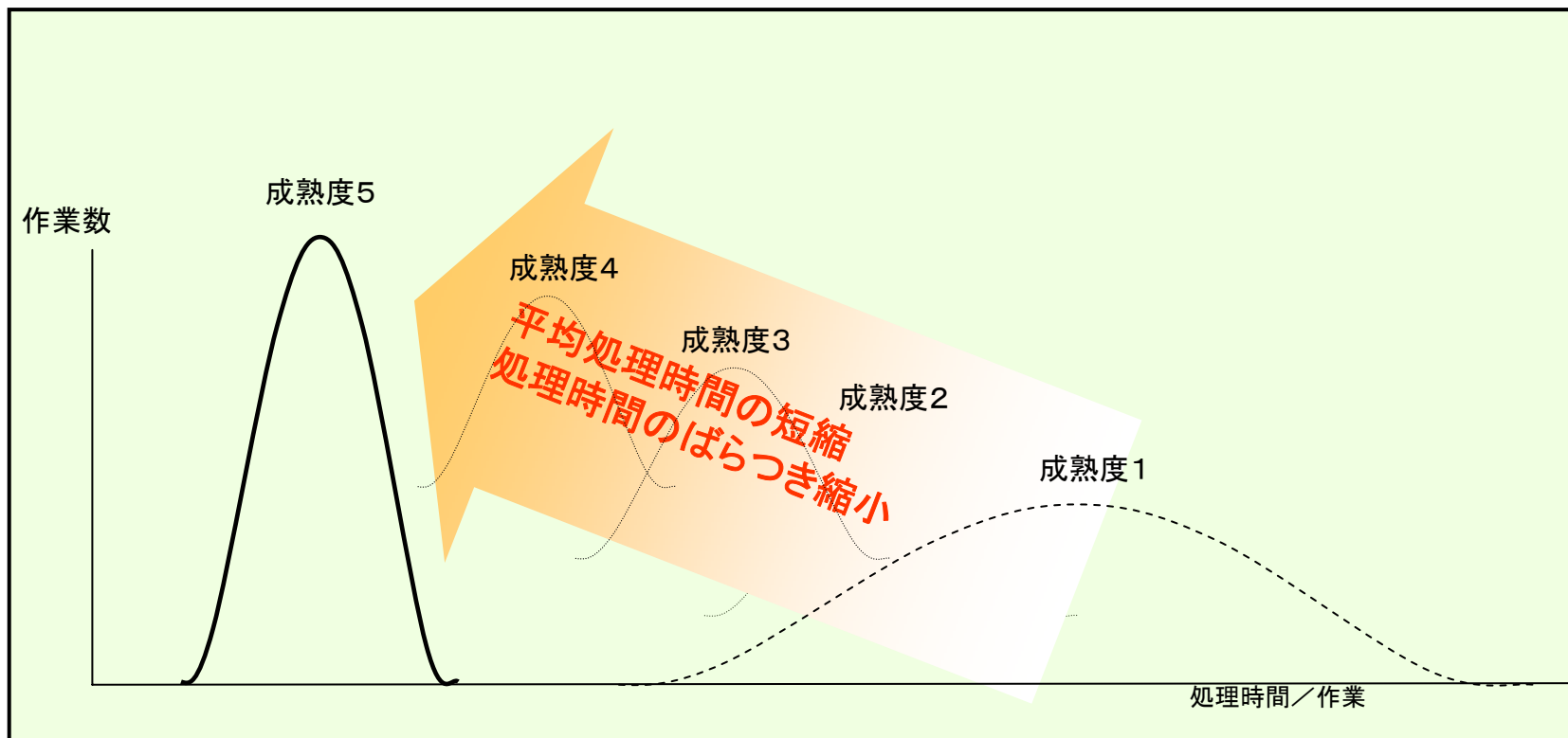
BPMを推進すれば、セキュリティ向上や内部統制(SOX)への対応が可能となるだけでなく、継続的な業務改革の実現や事業環境変化への迅速な対応が可能となる。



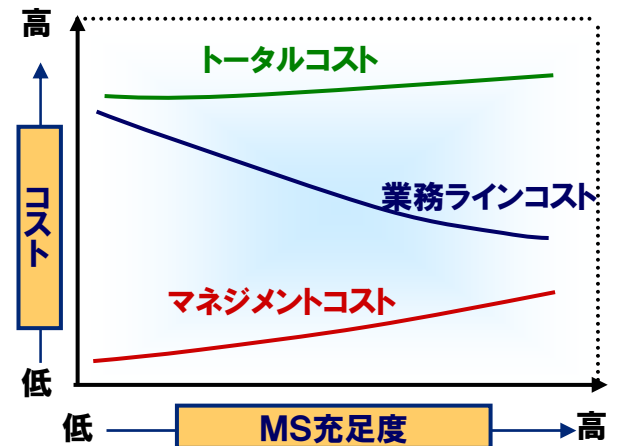
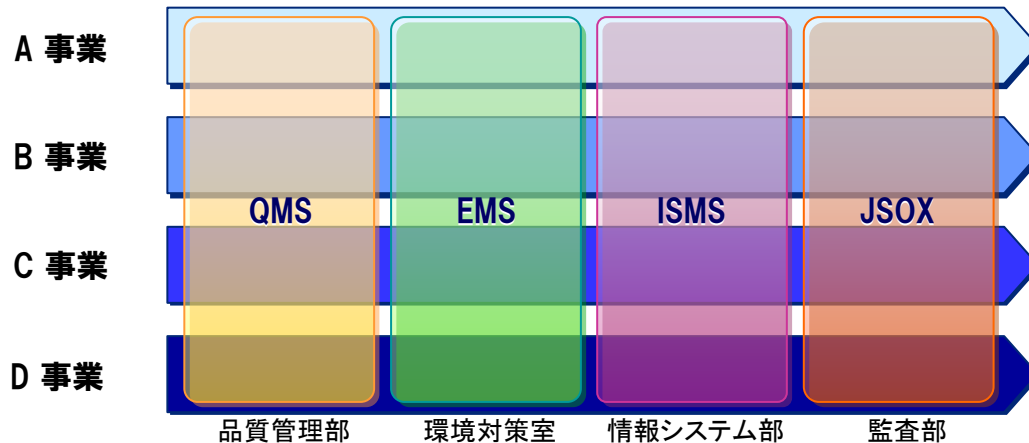
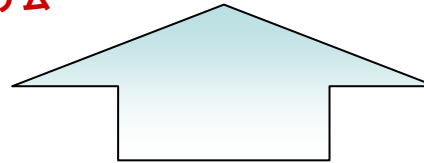
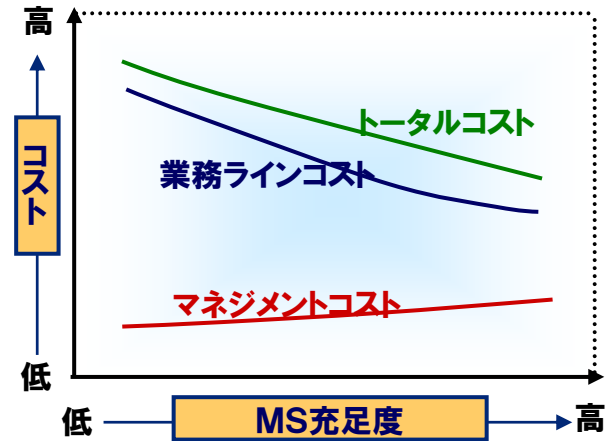
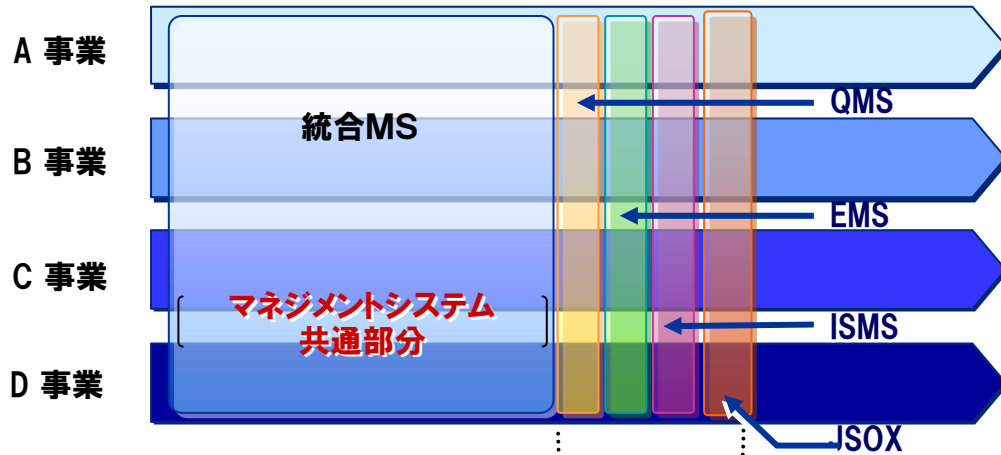
成熟度向上による効果

イメージ

成熟度が高くなると、平均処理時間が短縮され、処理時間のばらつきも小さくなる。

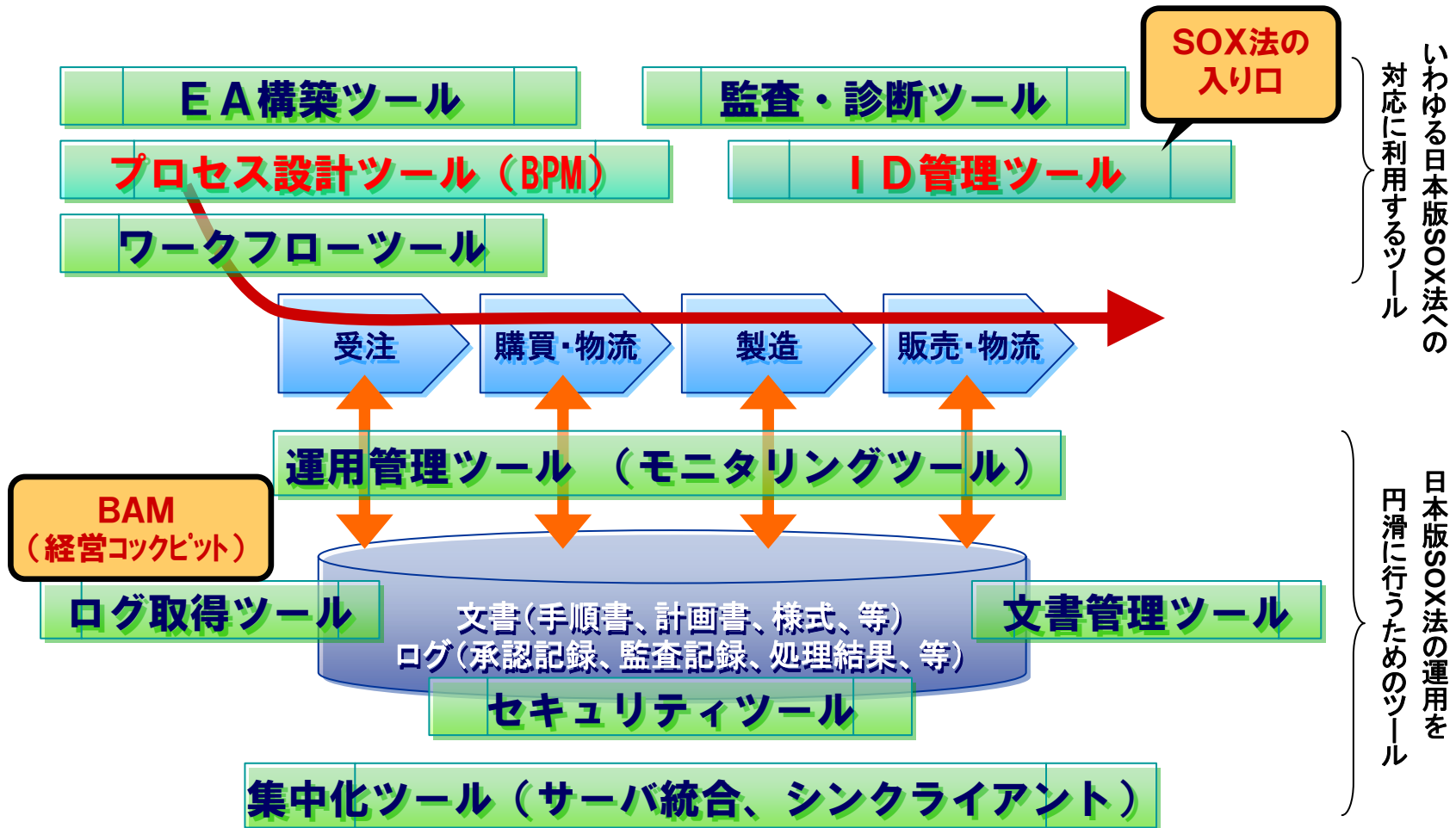


マネジメントシステムの統合化とその効果



ITの活用

日本版SOX法対応を効率的かつ実効的に行なうためには、必要に応じて、例えば以下にあるようなIT(ツール)を有効に活用していくことを推奨する



ITツールの有効活用は、単に日本版SOX法に対応するのみではなくパフォーマンス向上やセキュリティ向上等の効果が得られる

IT活用による効果

一般に、ITは業務の効率化に寄与するが、日本版SOX法対応においても同様のことがいえる。下記は、マニュアルコントロールとアプリケーションコントロールのコスト比較である。下記のように、ITアプリケーション統制は整備に時間がかかるが、それ以降のテストにおいては、格段に投資対効果が高い。

(空白)

企業規模によるIT統制効果の差異

もつとも、企業規模によって、その効果はかなりの差異がある

(空白)

目的と範囲の再設定

パフォーマンスの向上へ

ITの活用

マネジメントシステムの統合化

ITガバナンスの強化

BPMの推進

SOX→新会社法、COSOを目標

SOX法のみへの遵守

コスト上昇
後ろ向きの姿勢
手作業中心

多くの企業が、SOX対応のみで済まそうと考えているが、それだけでは、投資対効果は得にくい。今後の法規制の増加も考えた場合、重複投資になる危険もある。マルチコンプライアンスに対応可能で、パフォーマンス向上も狙える仕組みづくりを目指すべきである。

はじめに・・・コンプライアンス／内部統制／SOX法の関係

1. 米国の動向
2. 日本版SOX法(JSOX)の概要
3. 全社的な内部統制の進め方
4. IT全般統制の進め方
5. 投資対効果を上げる方法

おわりに 教育・資格の紹介

教育・資格のご紹介～認定SOXアドバイザー

認定SOXアドバイザー資格養成講座は、米国のSOX Instituteの協力を得て、グローバルマネジメントアカデミーが日本国内で提供する、内部統制支援を行うための唯一の専門家養成講座です。

日本版SOX法は半ば永続的な作業を必要とすることから、お客様ご自身が主体的に日本版SOX法に取り組む必要があります。そのため、自社内に専門家を育成し、会計士やコンサルタントと協力しながら、文書化、評価、改善等の各種活動を実施する体制を築くことが不可欠となります。

この講座は、このようなニーズを満たすべく、米国SOX法の経験を踏まえつつ、金融商品取引法や実施基準の内容を踏まえた構成となっております。

なお、株式会社NTTデータ経営研究所は、この講座に協力をしており、講座申し込みの窓口やオンサイトでの講座実施に関する企画・支援も行っております。

この講座は、3日間(全日)で実施され、最後に認定試験を行い、合格すると資格が与えられます。詳細は、

<http://www.keieiken.co.jp/events/2007/0123/index.html>

をご覧ください。幸いです。

短期間での対応のポイント

適切な人員配置(量)と短期間での育成(質・・・認定SOXアドバイザー資格等の取得)

IT全般統制、パイロットを並行した計画立案

ツールの活用

監査人の協力を取り付ける(範囲の設定等)

外部リソースの有効活用(立ち上げ時、全社統制、パイロット、IT全般統制)

業務処理統制の構築・・・内部リソース中心(パイロットで要員育成)

外部委託部分→将来的な内製化を計画(ブラックボックスのホワイトボックス化)

(必須)トップの十分な理解と承認とリーダーシップ

ご清聴ありがとうございました