ＩＴＣ江東主催　平成１８年度ＩＴＣセミナー資料

内部統制によるＩＴガバナンスの向上

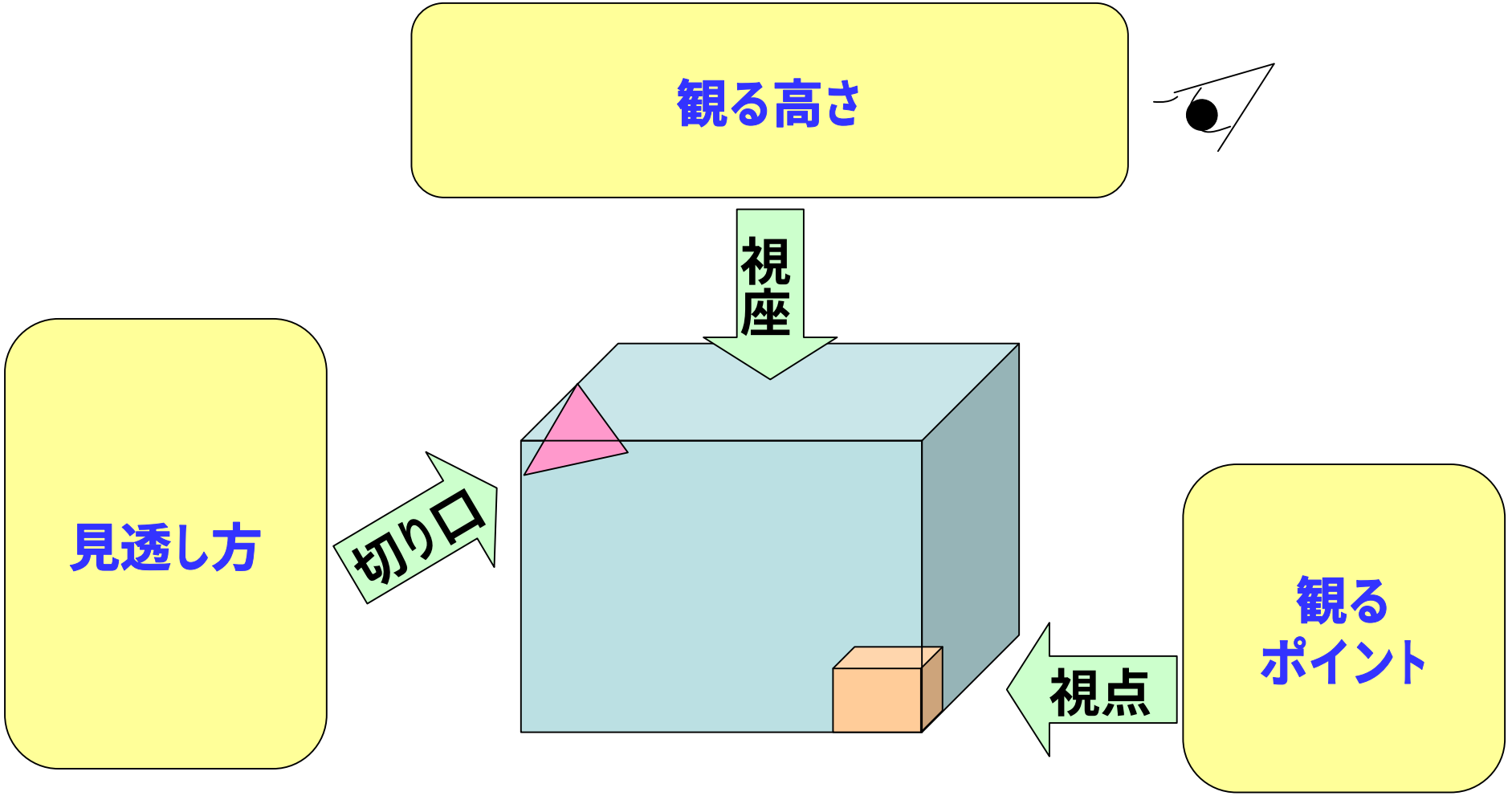
２００７年　３月２７日

ＮＥＣソフト株式会社　営業本部
中小企業診断士／ＩＴＣ　斎藤　尚志

目　　次

時代の潮流を読む！

・同じ事象を見ても人それぞれに感じ方は違う。
・常識的に見れば常識的な問題点や結論しかでてこない。
・物事をいかに観るか？



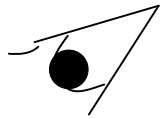
問　　い

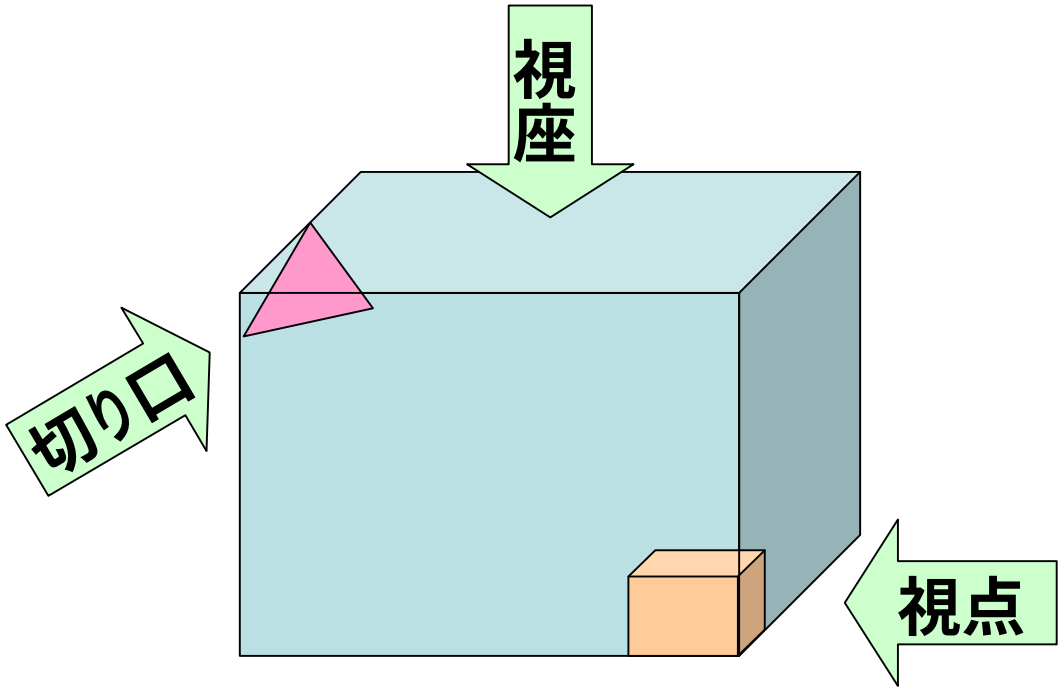
●少年ジャンプは、１９７３年～１９９５年の間、
その永き絶頂期を謳歌した。

●少年ジャンプはなぜ強かったのか？

内部統制導入をどう読むか？

1993年11月に成立、公布・施行された「環境基本法」についで超大型の法律である。今後、10年このような法律は成立しないであろう。ということは、千載一遇のチャンス！



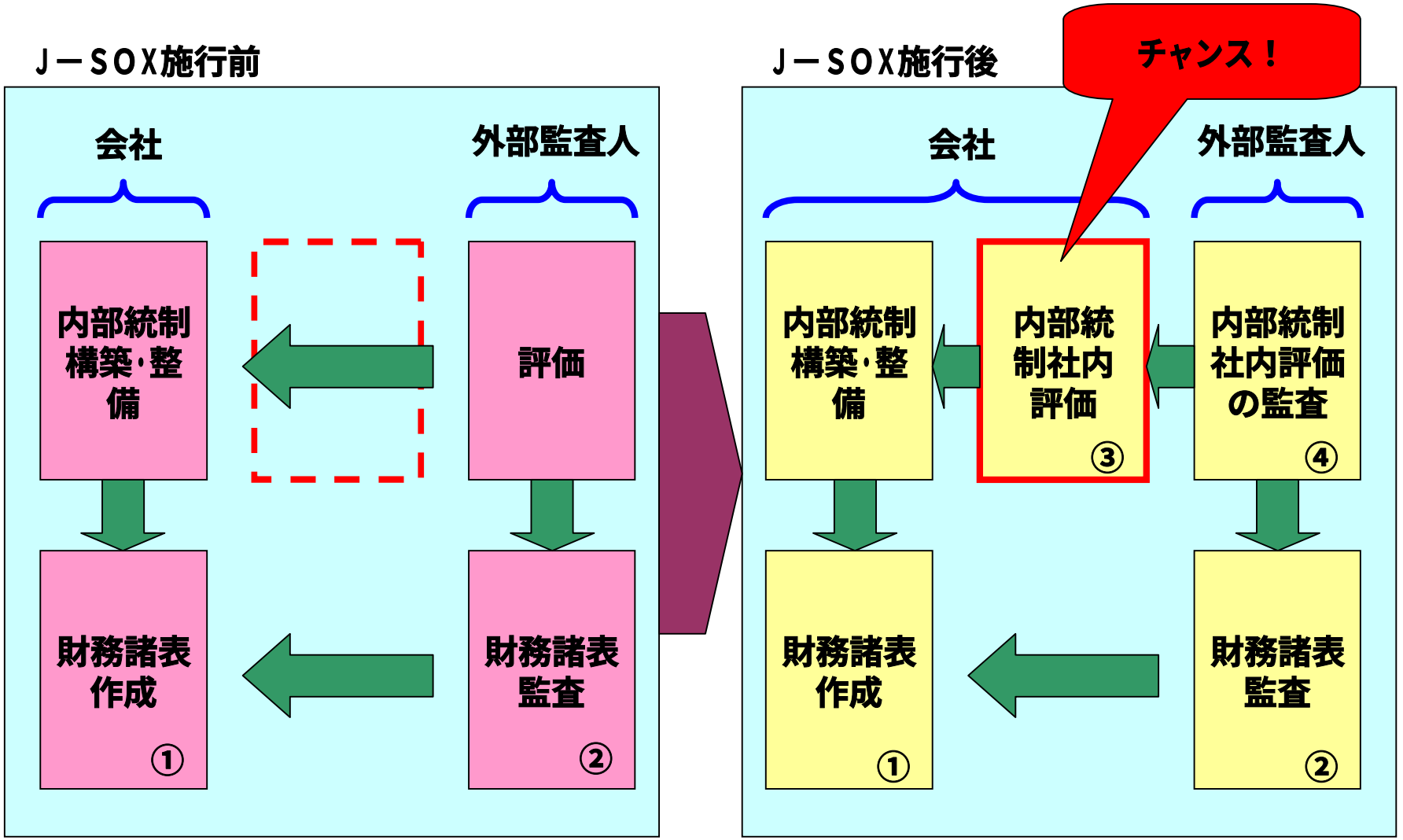


内部統制評価（ISOの内部監査）を継続的に、ご支援することにより、お客様のITガバナンス向上に資することができる。

・内部統制プロセス（構築→評価→会計士監査）
・後工程（評価プロセス）も着眼点。

Ｊ－ＳＯＸ施行前と後で何が変わるか？

●現行制度では、外部に対して、①と②を報告しているが、Ｊ－ＳＯＸ施行後は、①②③④を報告することになる。



金融商品取引法

VALWAY NECソフト

●２００６年6月７日国会で可決！

第２４条の４の４

第二十四条の四の四第二十四条第一項の規定による有価証券報告書を提出しなければならない会社（第二十三条の三第四項の規定により当該有価証券報告書を提出した会社を含む。次項において同じ。）のうち、第二十四条第一項第一号に掲げる有価証券の発行者である会社その他の政令で定めるものは、事業年度ごとに、当該会社の属する企業集団及び当該会社に係る財務計算に関する書類その他の情報の適正性を確保するために必要なものとして内閣府令で定める体制について、内閣府令で定めるところにより評価した報告書（以下「内部統制報告書」という。）を有価証券報告書（同条第八項の規定により同項に規定する有価証券報告書等に代えて外国会社報告書を提出する場合にあたっては、当該外国会社報告書）と併せて内閣総理大臣に提出しなければならない。

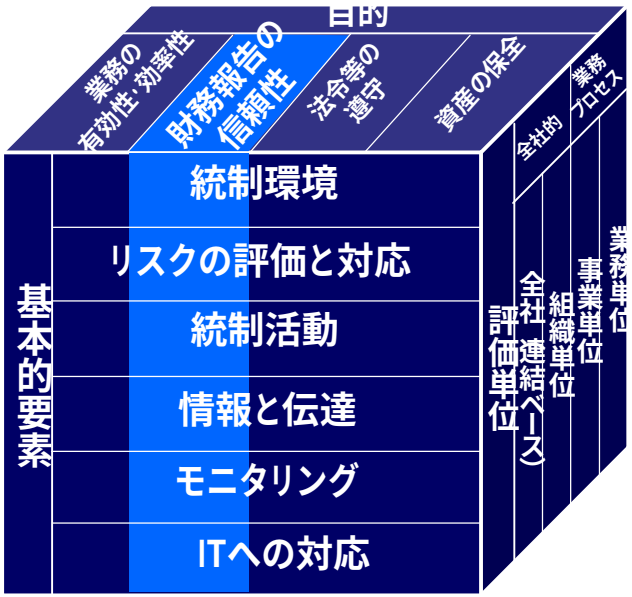
第１９３条の２第２項

金融商品取引所に上場されている有価証券の発行会社その他の者で政令で定めるものが、この法律の規定により提出する貸借対照表、損益計算書その他の財務計算に関する書類で内閣府令で定めるものには、その者と特別の利害関係のない公認会計士又は監査法人の監査証明を受けなければならない。ただし、監査証明を受けなくても公益又は投資者保護に欠けることがないものとして内閣府令で定めるところにより内閣総理大臣の承認を受けた場合は、この限りでない。

財務報告に係る内部統制の評価及び監査の基準

●2007年2月15日実施基準を確定

Ⅰ．内部統制の基本的枠組み



【出典：金融庁・企業会計審議会
「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」を基に作成】

Ⅱ．財務報告に係る内部統制の評価及び報告

記録及び保存

整備及び運用の方針及び手続

評価の範囲の決定 ― 評価範囲の制約

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

内部統制の重要な欠陥の是正

経営者による報告

Ⅲ．財務報告に係る内部統制の監査

監査計画の策定 ― 監査役等との連携 ／ 他の監査人等の利用

評価範囲の妥当性の検討

全社的な内部統制の評価の検討

業務プロセスに係る内部統制の評価の検討

内部統制の重要な欠陥等の報告と是正 ― 不正等の報告

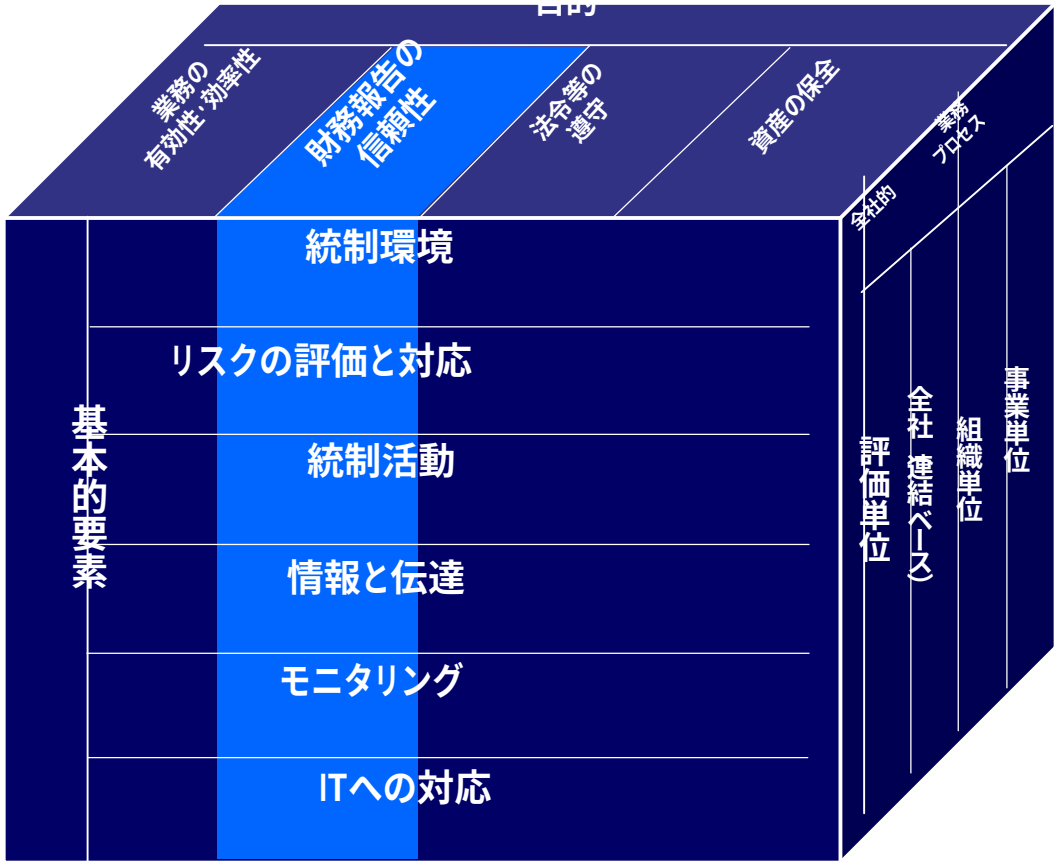
意見の表明 ― 監査範囲の制約

監査人の報告

米ＳＯＸ法とＪ－ＳＯＸ法の比較

項	米ＳＯＸ法	Ｊ－ＳＯＸ法
1	経営者による内部統制の評価基準がない	経営者による内部統制の評価基準の明確化
2	評価対象が広範	評価対象の絞り込み
3	内部統制の不備区分が複雑	内部統制の不備区分の簡素化
4	監査人監査におけるダイレクト･レポーティングの採用	監査人監査におけるインダイレクト･レポーティング方式の採用
5	財務諸表監査と内部統制監査との担当監査法人等の分離	財務諸表監査と内部統制監査は同一の監査法人等でよい

内部統制のフレームワーク



出典：金融庁・企業会計審議会
「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」を基に作成

内部統制の4つの目的

◆内部統制が達成しようとする目的
- 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
- 資産の保全

この内、金融商品取引法により評価及び監査の対象となるのは、「財務報告の信頼性」を確保するための内部統制である。
しかしながら、経営上のプレッシャーから黒字を装う誘惑に駆られる脅威に対し、業務の有効性及び効率性を高め、黒字を計上できるよう企業努力することは、結果として財務報告の信頼性を確保することにつながる。

内部統制の基本的要素

・内部統制の基本的要素とは、内部統制の目的を達成するために必要とされる内部統制の構成部分をいい、内部統制の有効性の判断の規準となる。

基本的要素	内容	備考
統制環境	統制環境とは、組織の気風を決定し、組織内のすべての者の統制に対する意識に影響を与えるとともに、他の基本的要素の基礎をなし、リスクの評価と対応、統制活動、情報と伝達、モニタリング及びITへの対応に影響を及ぼす基盤をいう。	誠実性・倫理観、経営者の意向・姿勢、経営方針・経営戦略、取締役会・監査役の有する機能、組織構造・慣行、権限・職責、人的資源に対する方針・管理
リスクの評価と対応	リスクの評価とは、組織目標の達成に影響を与える事象について、組織目標の達成を阻害する要因をリスクとして識別、分析及び評価するプロセスをいう。 リスクへの対応とは、リスクの評価を受けて、当該リスクへの適切な対応を選択するプロセスをいう。	リスクへの対応…回避、低減、移転、受容
統制活動	統制活動とは、経営者の命令及び指示が適切に実行されることを確保するために定める方針及び手続をいう。	・権限及び職責の付与、職務の分掌等の広範な方針・手続 ・方針・手続は、業務のプロセスに組み込まれ、遂行されること
情報と伝達	情報と伝達とは、必要な情報が識別、把握及び処理され、組織内外及び関係者相互に正しく伝えられることを確保することをいう。	・情報の識別、把握、処理、伝達 ・情報は共有されること
モニタリング	モニタリングとは、内部統制が有効に機能していることを継続的に評価するプロセスをいう。モニタリングにより、内部統制は常に監視、評価及び是正されることになる。	・日常的モニタリング ・独立的評価
ITへの対応	ITへの対応とは、組織目標を達成するために予め適切な方針及び手続を定め、それを踏まえて、業務の実施において組織の内外のITに対し適切に対応することをいう。	組織の業務内容に依存orITを高度に取り入れている場合等は不可欠の要素 (1) IT環境への対応 (2) ITの利用及び統制

財務報告の重要な事項に虚偽記載が発生するリスク

◆粉飾は機械やシステムが引き起こす物ではない

◆財務報告の重要な事項に虚偽記載が発生するリスクは、粉飾にかかわる可能性が高い人に付け入る脅威と、脅威を引き起こしてしまう脆弱性によって現実の物となる

リスク　＝　脅威　×　脆弱性

粉飾にかかわる可能性が高い人に付け入る脅威

- ◆ 経営上のプレッシャーから黒字を装う必要に迫られている
  - ・配当維持
  - ・金融機関に対し返済能力があるように見せ掛け
  - ・信用の維持、経営基盤が強固であるように見せ掛け
- ◆ 企業環境の悪化
  - ・過度の競争又は市場が飽和状態
  - ・顧客の需要が著しく減少
  - ・技術、製品陳腐化
- ◆ 財務目標を達成するために、経営者や営業担当者に対する過大なプレッシャー
- ◆ 個人的な借金があり、返済に充てる金を捻出する必要に迫られている
- ◆ 取引の失敗などで与えた損失を隠蔽する必要に迫られている
- ◆ 裏金を捻出する必要に迫られている

脆弱性（1）

★脅威を引き起こしてしまう弱さ　⇒　脆弱性

◆利益を生まない経営、戦略、体質
◆不正を自ら正そうとしないモラルの低い経営体質
　・不適切な企業価値又は倫理基準が横行
　・内部統制における重大な欠陥を発見しても適時に是正しない企業体質
◆従業員の企業に対する不満
◆悪魔のささやきが聞こえる業務の特質
　・取り扱う現金が多額
　・棚卸資産が高価で需要が多く、容易に換金可能

脆弱性（2）

◆誰のチェックも受けずに独断で不正操作ができる環境
- 通常の取引過程からはずれた取引の存在
- 監査を受けていない取引先の存在
- 内部統制に重要な関わりをもつ従業員に強制休暇を取得させていない
- 不適切な財務上の影響力を行使できる仕入先や得意先の存在
- 財務報告プロセスと内部統制に対する監視が効果的でない
- 職務の分離又は牽制が不十分な場合
- 資産に関する帳簿記録が不十分
- 会計及び情報システムに内在する内部統制の重大な欠陥

◆自動化された記録に対するアクセス管理が不十分

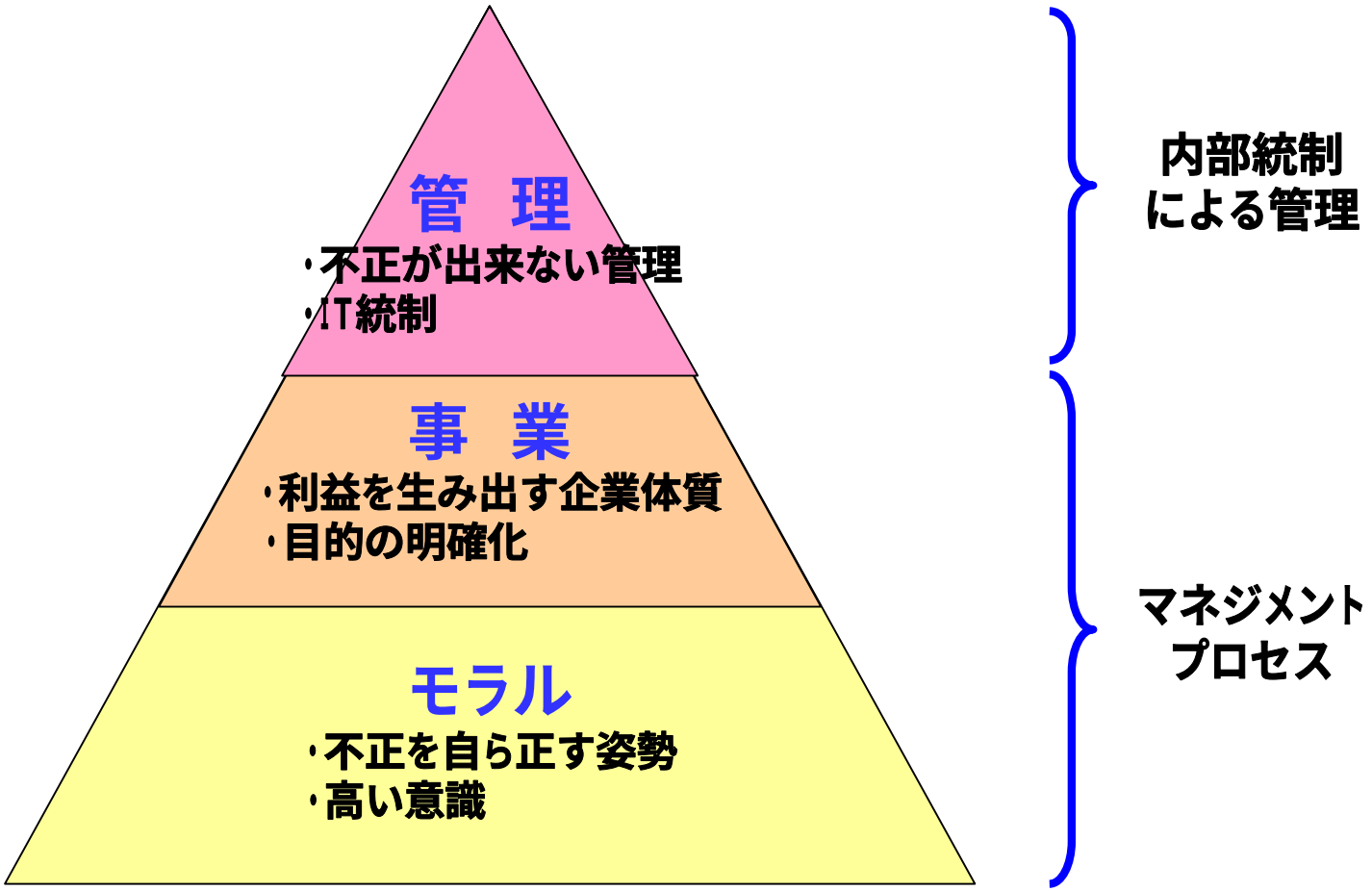
内部統制とマネジメントプロセス（1）

◆内部統制は、マネジメントプロセスのうち、経営者の判断や、目的の設定、計画の立案、リスク管理そのもの、是正措置といった要素は含まれないというのが一般的な考え方である。

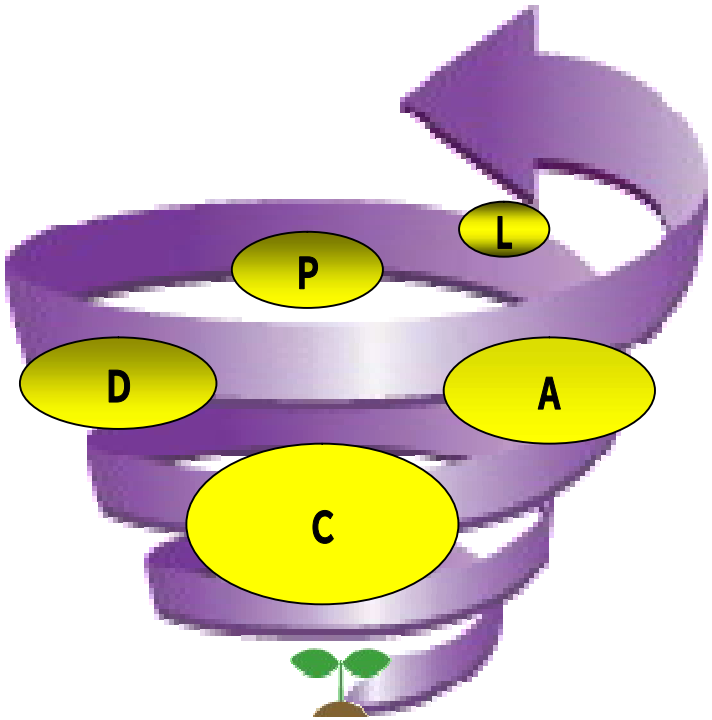
◆しかし、企業の体質の改善を効果的に行うためには、マネジメントプロセスのコアとなるＰ－Ｄ－Ｃ－Ａサイクルの存在は欠かせない。上記のＰ－Ｄ－Ｃ－Ａサイクル要素をまわすことにより得られる健全な企業体質の上に内部統制は築かれるべきであろう。

内部統制とマネジメントプロセス（2）

●ベースに健全なマネジメントプロセスなくして内部統制の構築・運用はありえない。

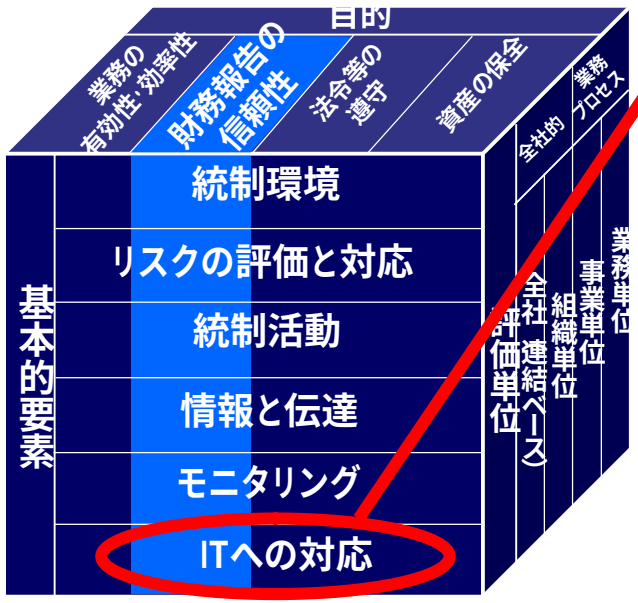


内部統制を確実なものとするＰＤＣＡ＋Ｌサイクル



・安全な情報システム構築
・情報を処理し続ける情報システム
（可用性、事業継続性）
・リソースの管理
・構成を管理
・情報セキュリティ
・インシデントへの対応

ITへの対応（1）



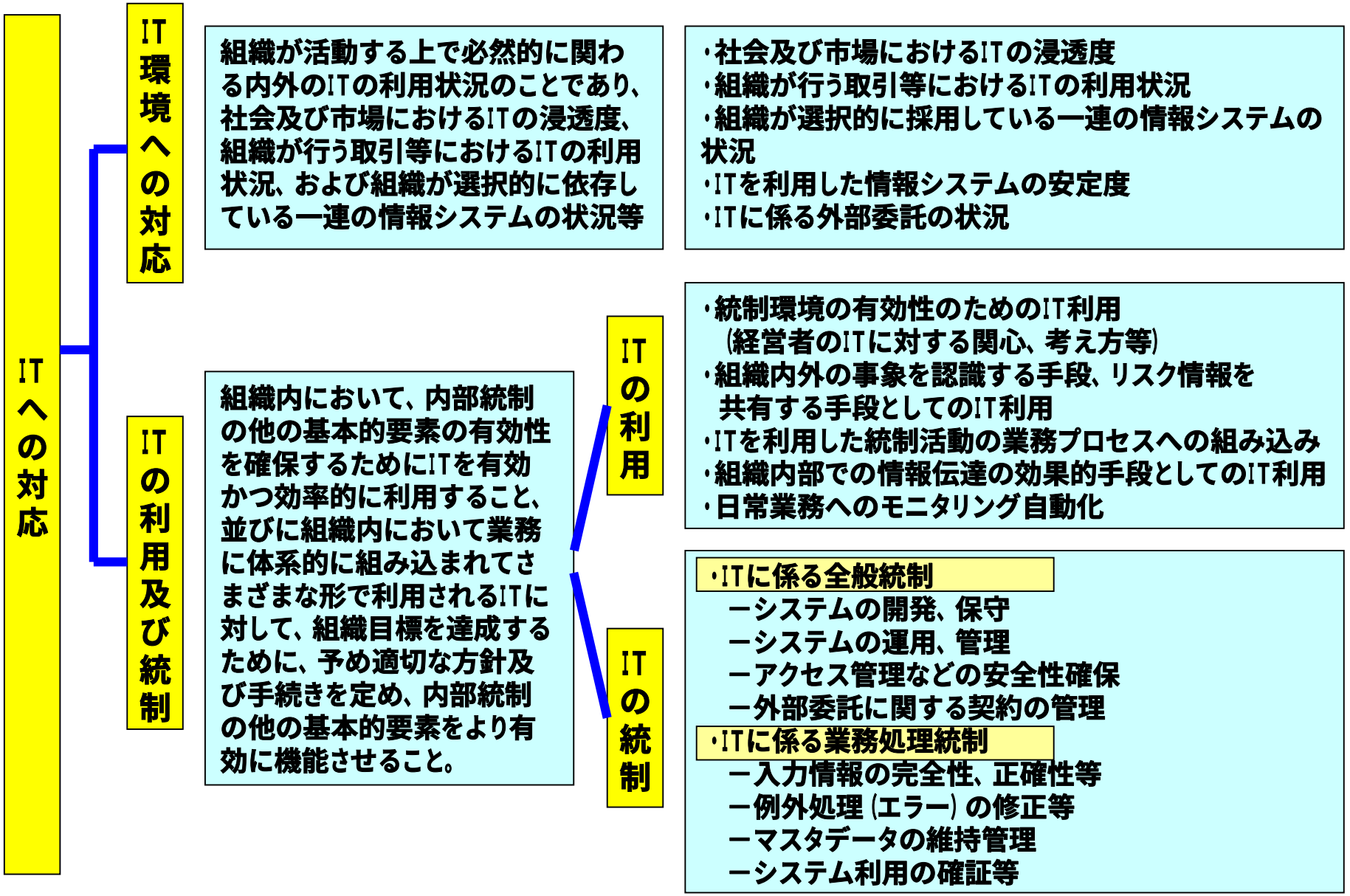
【出典：金融庁・企業会計審議会
「財務報告に係る内部統制の評価及び
監査の基準のあり方について」を基に作成】

ITへの対応

組織目標を達成するために、予め適切な方針及び手続きを定め、それを踏まえて、業務の実施において組織の内外のITに対し適切に対応すること。

「ITへの対応」は、内部統制の他の基本的要素と必ずしも独立に存在するものではないが、組織の業務内容がITに大きく依存している場合や組織の情報システムがITを高度に取り入れている場合等には、内部統制の目的を達成するために不可欠の要素として、内部統制の有効性に係る判断の規準となる。

ITへの対応 (2)


ITへの対応
IT環境への対応
組織が活動する上で必然的に関わる内外のITの利用状況のことであり、社会及び市場におけるITの浸透度、組織が行う取引等におけるITの利用状況、および組織が選択的に依存している一連の情報システムの状況等
・社会及び市場におけるITの浸透度
・組織が行う取引等におけるITの利用状況
・組織が選択的に採用している一連の情報システムの状況
・ITを利用した情報システムの安定度
・ITに係る外部委託の状況
ITの利用及び統制
組織内において、内部統制の他の基本的要素の有効性を確保するためにITを有効かつ効率的に利用すること、並びに組織内において業務に体系的に組み込まれてさまざまな形で利用されるITに対して、組織目標を達成するために、予め適切な方針及び手続きを定め、内部統制の他の基本的要素をより有効に機能させること。
ITの利用
・統制環境の有効性のためのIT利用
(経営者のITに対する関心、考え方等)
・組織内外の事象を認識する手段、リスク情報を共有する手段としてのIT利用
・ITを利用した統制活動の業務プロセスへの組み込み
・組織内部での情報伝達の効果的手段としてのIT利用
・日常業務へのモニタリング自動化
ITの統制
・ITに係る全般統制
－システムの開発、保守
－システムの運用、管理
－アクセス管理などの安全性確保
－外部委託に関する契約の管理
・ITに係る業務処理統制
－入力情報の完全性、正確性等
－例外処理 (エラー) の修正等
－マスタデータの維持管理
－システム利用の確証等

IT統制で何が出来るか

◆電子化された記録に対するアクセス管理
- ・職務上の責任に見合った特権の付与
- ・アクセスの監視
- ・ログの分析による不正の検知、抑止

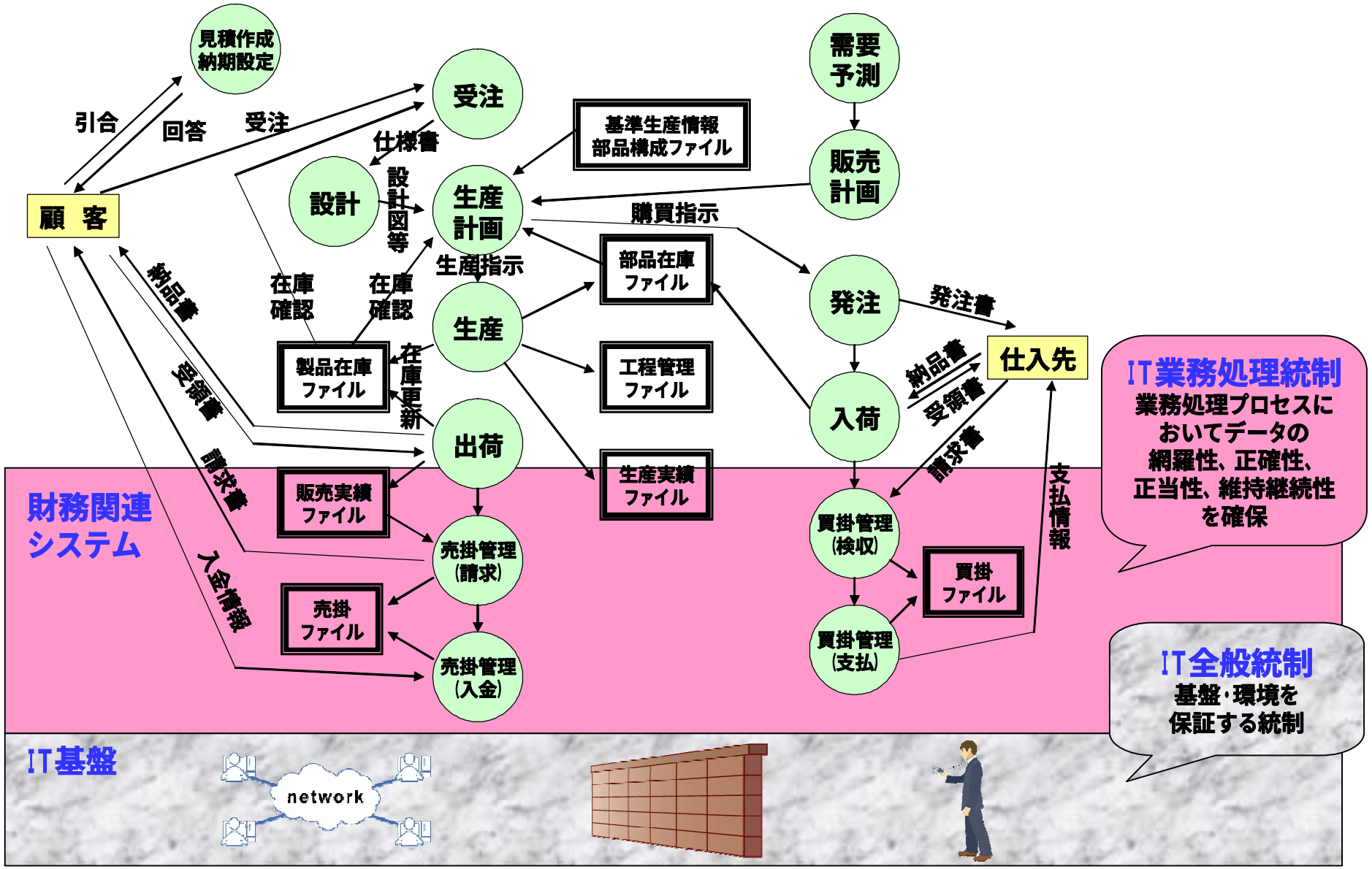
◆正確なデータ処理

◆入力ミスの防止
- ・二重入力チェック
- ・限度チェック

◆暗号化による機密情報の保護

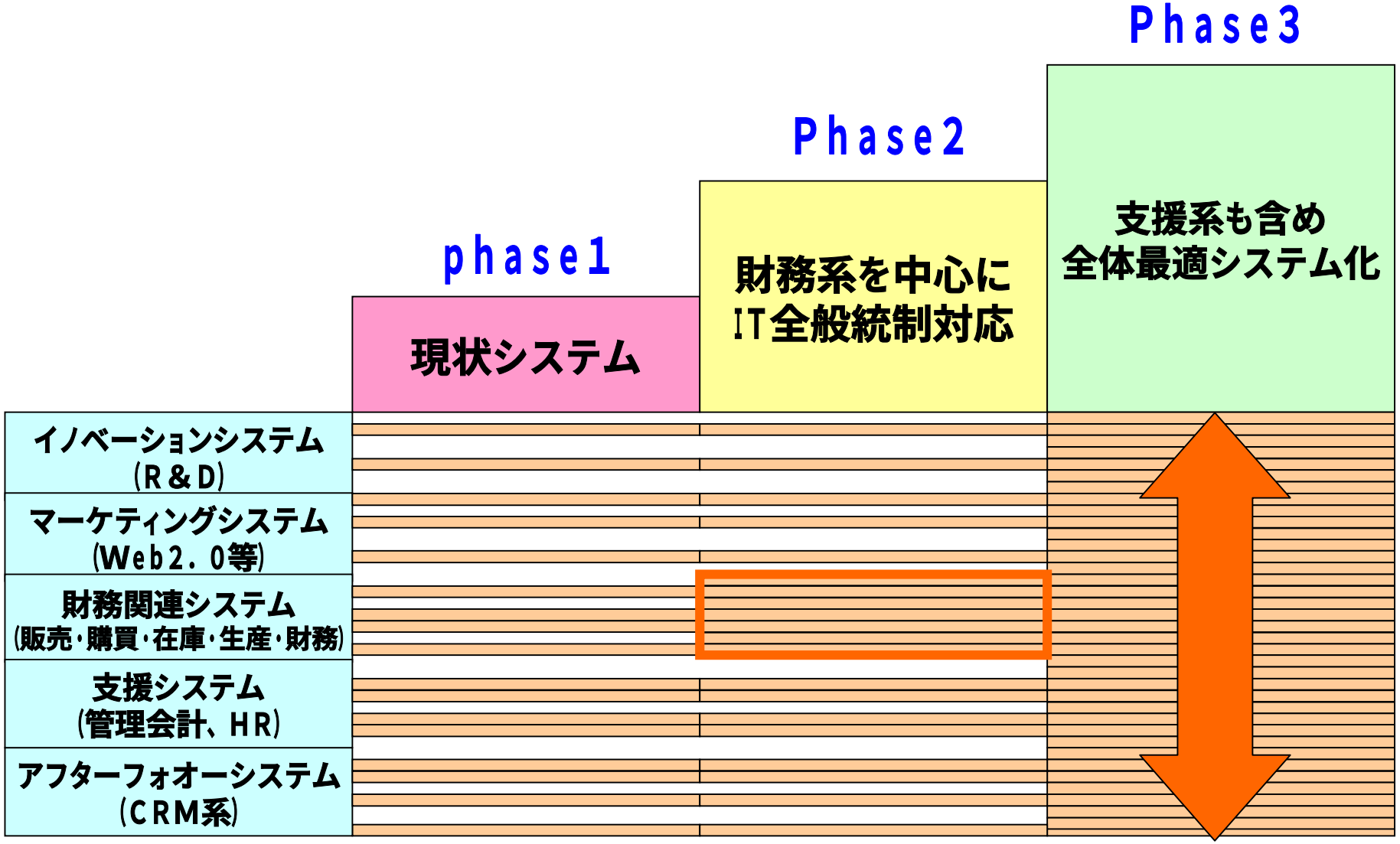
◆職務の分離又は牽制

IT統制のイメージ図

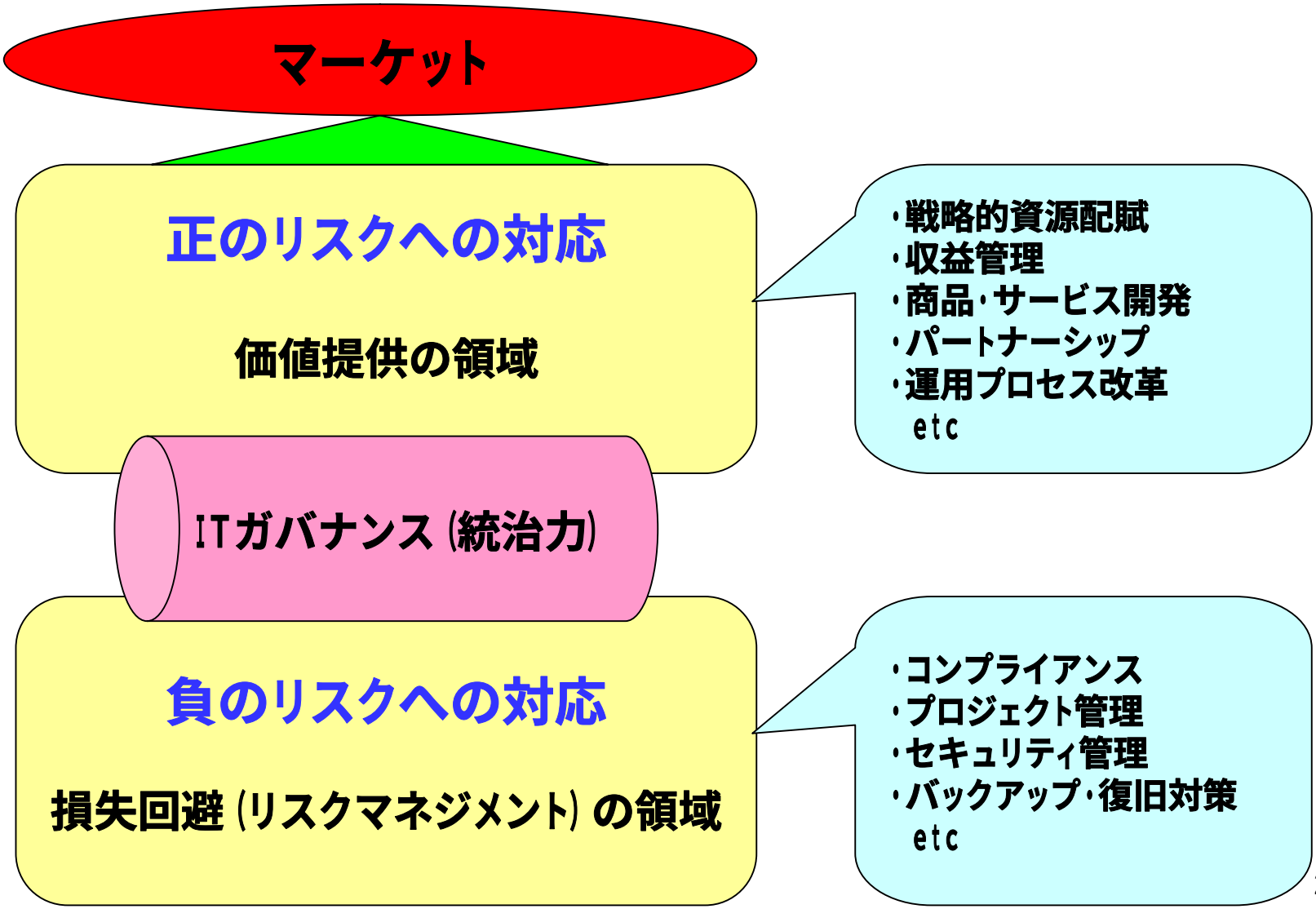

見積作成
納期設定
引合
回答
受注
顧 客
受注
仕様書
設計
設計図等
生産計画
基準生産情報
部品構成ファイル
需要予測
販売計画
購買指示
部品在庫ファイル
生産指示
在庫確認
在庫確認
生産
製品在庫ファイル
在庫更新
工程管理ファイル
出荷
生産実績ファイル
発注
発注書
仕入先
納品書
受領書
入荷
納品書
受領書
請求書
支払情報
販売実績ファイル
売掛管理(請求)
売掛ファイル
売掛管理(入金)
入金情報
買掛管理(検収)
買掛ファイル
買掛管理(支払)
財務関連システム
IT業務処理統制
業務処理プロセスにおいてデータの網羅性、正確性、正当性、維持継続性を確保
IT全般統制
基盤・環境を保証する統制
IT基盤
network

内部統制（IT統制）から全体ITガバンンスへ

●内部統制で強化されたIT統制の次は支援系システムも含めた全体最適システムへ



ITガバナンス強化による企業価値の向上



ITガバナンス強化の絶好の機会

J－SOX対応プロジェクトが、企業グループ全体を巻き込んだ、大規模プロジェクトとなる。
また、時限的なプロジェクトとなる。

J－SOX対応プロジェクトが、財務諸表の信頼性の確保に収斂した「内部統制評価・改善・文書化」活動になりうる。

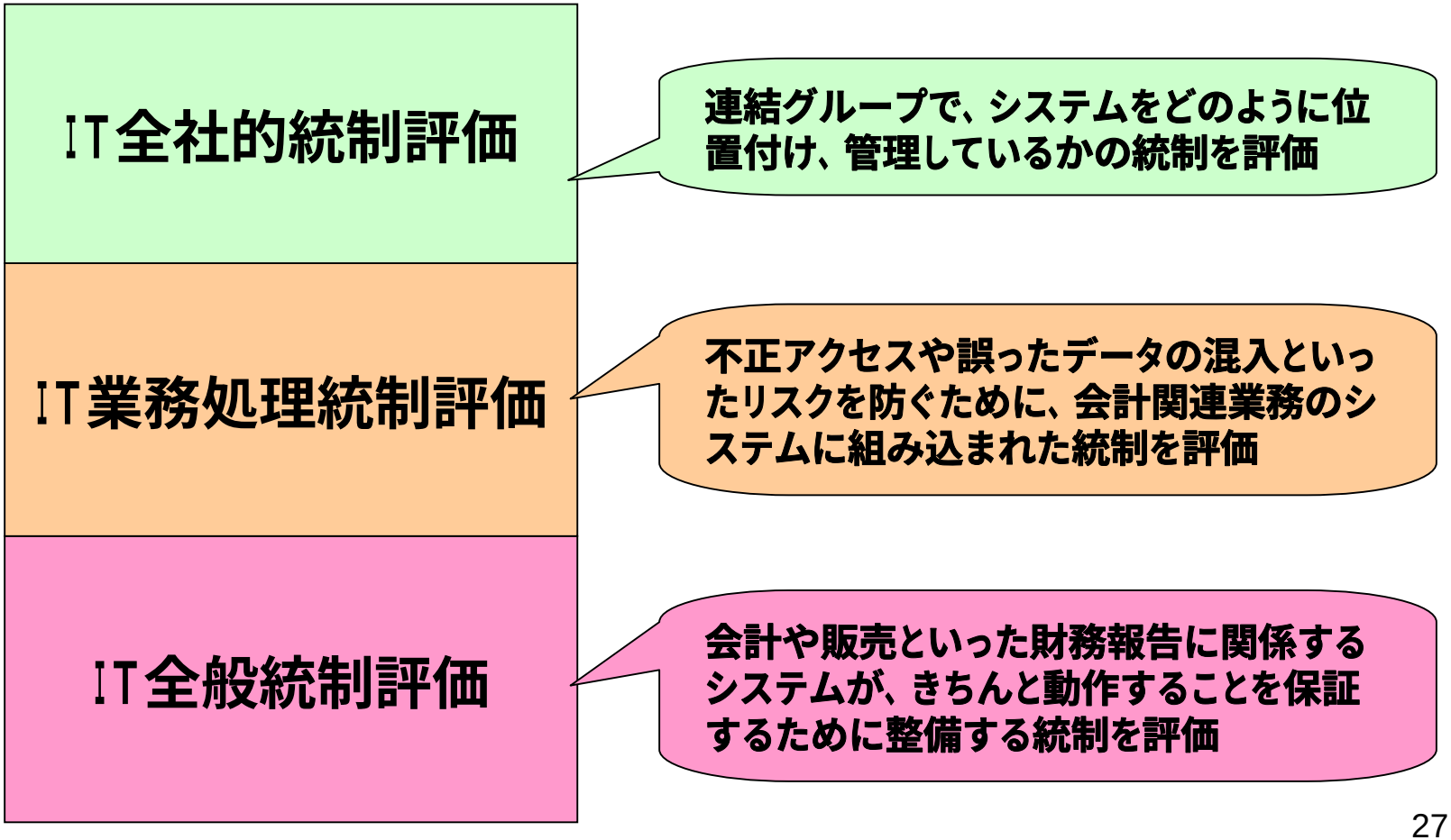
内部統制あるいはJ－SOX対応を「旗印」「スローガン」とし、これまで経営資源を配賦できなかったITガバナンス強化を行うことが可能な“絶好の機会”である。

ITを取り巻く環境は、時々刻々と変化しており、要求事項も高度化してきている。

従来、ITガバナンスについて問題認識はあっても、必要な予算を獲得できない。
あるいは、関係者の理解が得られなかった経験を有している。

システム管理基準　追補版（案）の3種類のIT統制の評価

●「IT全般統制評価」をしっかり行い、それを拡充していくことが全体でのITガバナンス向上につながる。



システム管理基準　追補版案ｖｓ　ＩＳＯ等（1）

部	章	節	項目	マネジメントシステム内容	CobiT4.0	ISO9001	ISO20000	ISO27001
Ⅰ			情報戦略					
	1		全体最適化					
		1.1	全体最適化の方針･目標	経営陣の責任	PO	○	○	○
		1.2	全体最適化計画の承認	計画承認	PO	○	○	○
		1.3	全体最適化計画の策定	計画立案	PO	○	○	○
		1.4	全体最適化計画の運用	導入及び運用	PO	○	○	○
	2		組織体制					
		2.1	情報システム化委員会	監視･測定･レビュー･継続的改善	DS	○	○	○
		2.2	情報システム部門	プロセス規程	DS	○	○	○
		2.3	人的資源管理の方針	力量･認識及び教育･訓練	DS	○	○	○
	3		情報化投資	資源の提供	PO	○	○	○
	4		情報資産管理の方針	資源の運用管理	PO	○	○	○
	5		事業継続計画	事業継続管理	PO		○	○
	6		コンプライアンス	順守	ME			○
Ⅱ			企画業務					
	1		開発計画	計画立案と導入	AI	○		○
	2		分析	容量･能力管理	AI	○		○
	3		調達	購買	AI	○		○
Ⅲ			開発業務					
	1		開発手順	製品実現･情報システム開発	AI	○		○
	2		システム設計	製品実現･情報システム開発	AI	○		○
	3		プログラム設計	製品実現･情報システム開発	AI	○		○
	4		プログラミング	製品実現･情報システム開発	AI	○		○
	5		システムテスト･ユーザ受入れテスト	システムの受入	AI	○		○
	6		移行	製品実現･情報システム開発	AI	○		○
Ⅳ			運用業務					
	1		運用管理ルール	手順･記録	DS	○	○	○
	2		運用管理	インシデント･問題･変更･リリース	DS		○	○
	3		入力管理	入力データの妥当性の確認	DS		○	○
	4		データ管理	内部処理の管理	DS		○	○
	5		出力管理	出力データの妥当性確認	DS		○	○
	6		ソフトウェア管理	構成管理	DS		○	
	7		ハードウェア管理	構成管理	DS		○	
	8		ネットワーク管理	構成管理	DS		○	
	9		構成管理	構成管理	DS		○	
	10		建物･関連設備管理	物理的･環境的管理	DS	○	○	○

システム管理基準　追補版案ｖｓ　ＩＳＯ等（2）

部	章	節	項目	マネジメントシステム内容	CobiT4.0	ISO9001	ISO20000	ISO27001
V			保守業務					
	1		保守手順	情報システムの保守	AI	○	○	○
	2		保守計画	情報システムの保守	AI	○	○	○
	3		保守の実施	情報システムの保守	AI	○	○	○
	4		保守の確認	情報システムの保守	AI	○	○	○
	5		移行	情報システムの保守	AI	○	○	○
	6		情報システムの廃棄	物理的･環境的管理	AI	○	○	○
VI			共通業務					
	1		ドキュメント管理					
		1.1	作成	文書管理	PO	○	○	○
		1.2	管理	文書管理	PO	○	○	○
	2		進捗管理					
		2.1	実施	監視･測定･レビュー	ME	○	○	○
		2.2	評価	監視･測定･レビュー	ME	○	○	○
	3		品質管理					
		3.1	計画	問題管理	DS	○	○	○
		3.2	実施	問題管理	DS	○	○	○
	4		人的資源管理					
		4.1	責任･権限	経営資源の運用管理	DS	○	○	○
		4.2	業務遂行	経営資源の運用管理	DS	○	○	○
		4.3	教育･訓練	経営資源の運用管理	DS	○	○	○
		4.4	健康管理	経営資源の運用管理	DS	○	○	○
	5		委託･受託					
		5.1	計画	外部委託	AI	○	○	○
		5.2	委託先選定	外部委託	AI	○	○	○
		5.3	契約	外部委託	AI	○	○	○
		5.4	委託業務	外部委託	AI	○	○	○
		5.5	受託業務	外部委託	AI	○	○	○
	6		変更管理					
		6.1	管理	変更管理	AI	○	○	○
		6.2	実施	変更管理	AI	○	○	○
	7		災害対策					
		7.1	リスク分析	事件･事故管理	PO		○	○
		7.2	災害時対応計画	事件･事故管理	PO		○	○
		7.3	バックアップ	事件･事故管理	PO		○	○
		7.4	代替処理･復旧	事件･事故管理	PO		○	○

ＣＯＢＩＴ４.０（Control Object for Information Technology）の領域

計画と組織（IT環境）

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プロセスと組織及びその関わりの決定
ＰＯ５	IT投資の管理
ＰＯ６	マネジメントの意図と指針の周知
ＰＯ７	IT人材の管理
ＰＯ８	品質管理
ＰＯ９	ITリスクの評価と管理
ＰＯ１０	プロジェクト管理

モニタリングと評価（IT環境）

ＭＥ１	IT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
ＭＥ３	規制遵守の確実化
ＭＥ４	ITガバナンスの提供

調達と導入（プログラムの開発と変更）

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	運用の促進
ＡＩ５	IT資源の調達
ＡＩ６	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

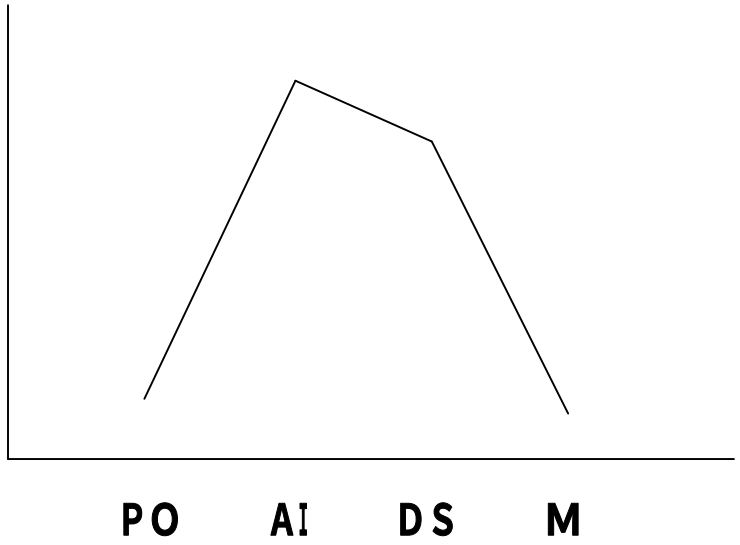
サービス提供とサポート（コンピュータ･オペレーションおよびプログラムとデータへのアクセス）

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	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
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
ＤＳ１０	問題管理
ＤＳ１１	データ管理
ＤＳ１２	物理的環境の管理
ＤＳ１３	オペレーション管理

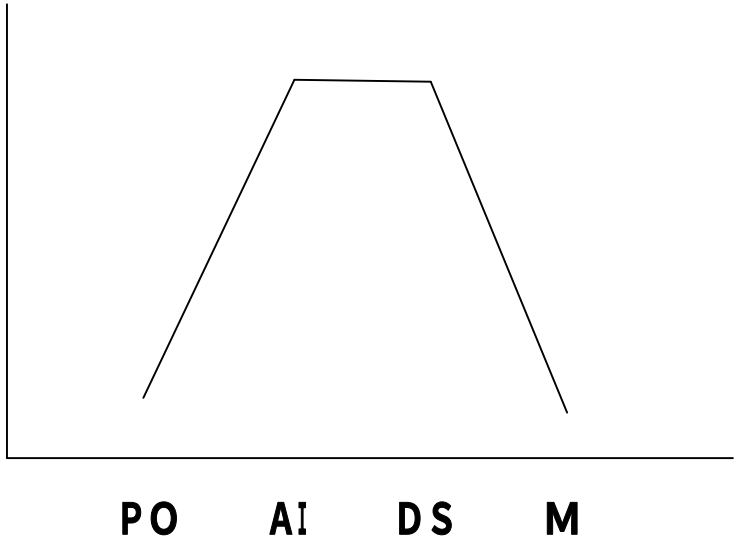
ITガバナンスの成長過程

●内部統制は成熟度レベル3を求めている！

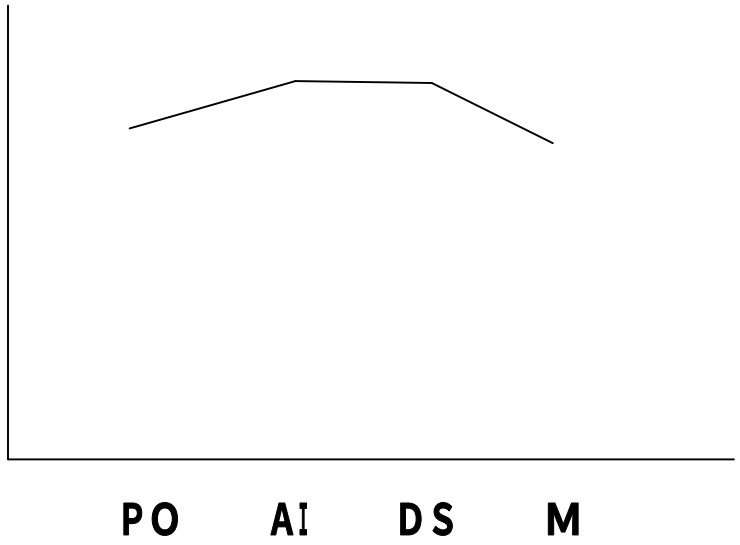
初期段階



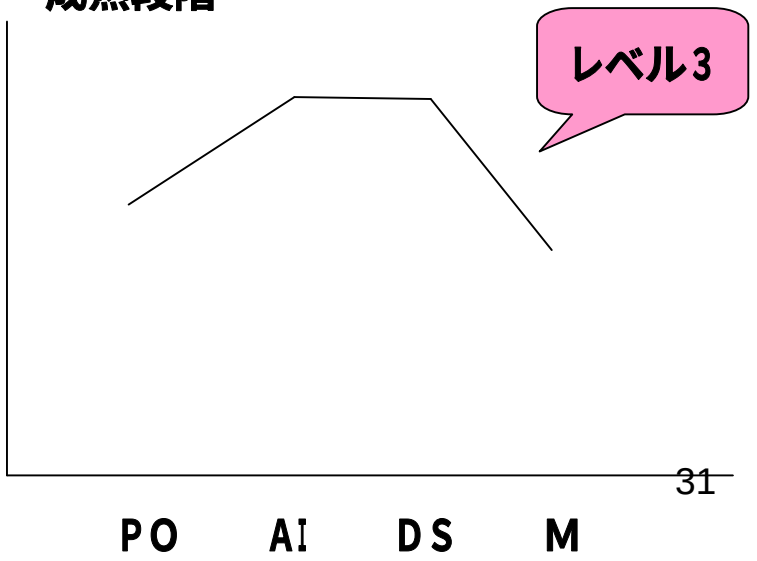
成長段階



円熟段階



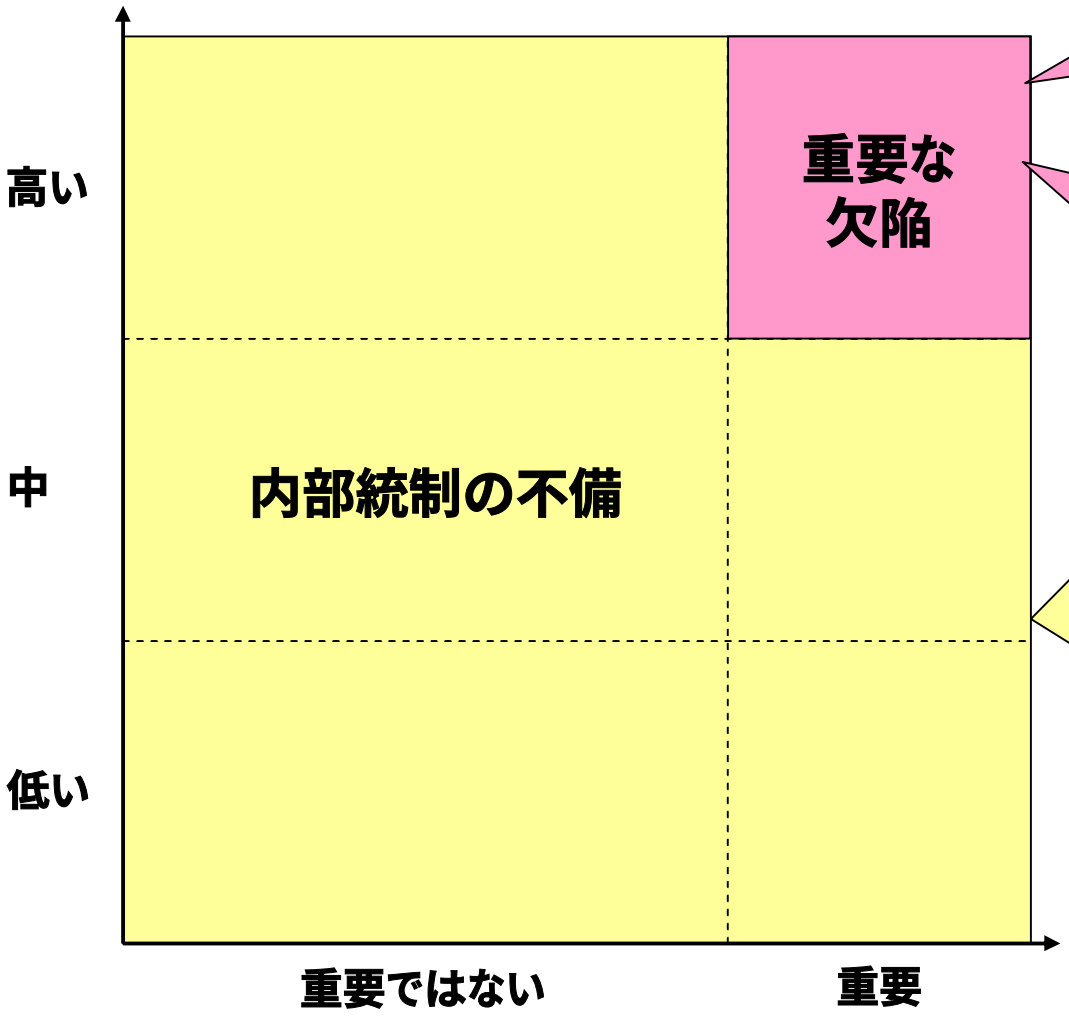
成熟段階



ITに係る内部統制の評価

項	評価単位	評価内容	備考
IT全般統制	・業務管理システムを支援するIT基盤 ex) 販売・購買管理ｼｽﾃﾑ…IS部 会計ｼｽﾃﾑ…経理部	以下の4項目の有用性を判断 ・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のシステムの安全性の確保 ・ITに関する外部委託に関する契約の管理	IT全般統制は信頼性を確保し、IT業務処理統制の継続的な運用を間接的に支援するものである。よって、IT全般統制の不備が直ちに重要な欠陥と評価されるものではない。
IT業務処理統制	・個々の業務システム	以下の4項目の有用性を判断 ・入力情報の完全性、正確性、正当性等が確保されること ・エラーデータの正確性が確保されること ・マスタ・データの正確性が確保されること ・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こと	IT業務処理統制に不備がある場合、影響と発生可能性を検討し、重要な欠陥に該当するかどうかを判断する

内部統制の不備と是正



財務報告に重要な影響を及ぼす可能性が高い内部統制の不備

「重要な欠陥」が発見された場合であっても、それが報告書における評価時期（期末日）までに是正されていれば、財務報告に係る内部統制は有効であると認めることができる

1．整備上の不備

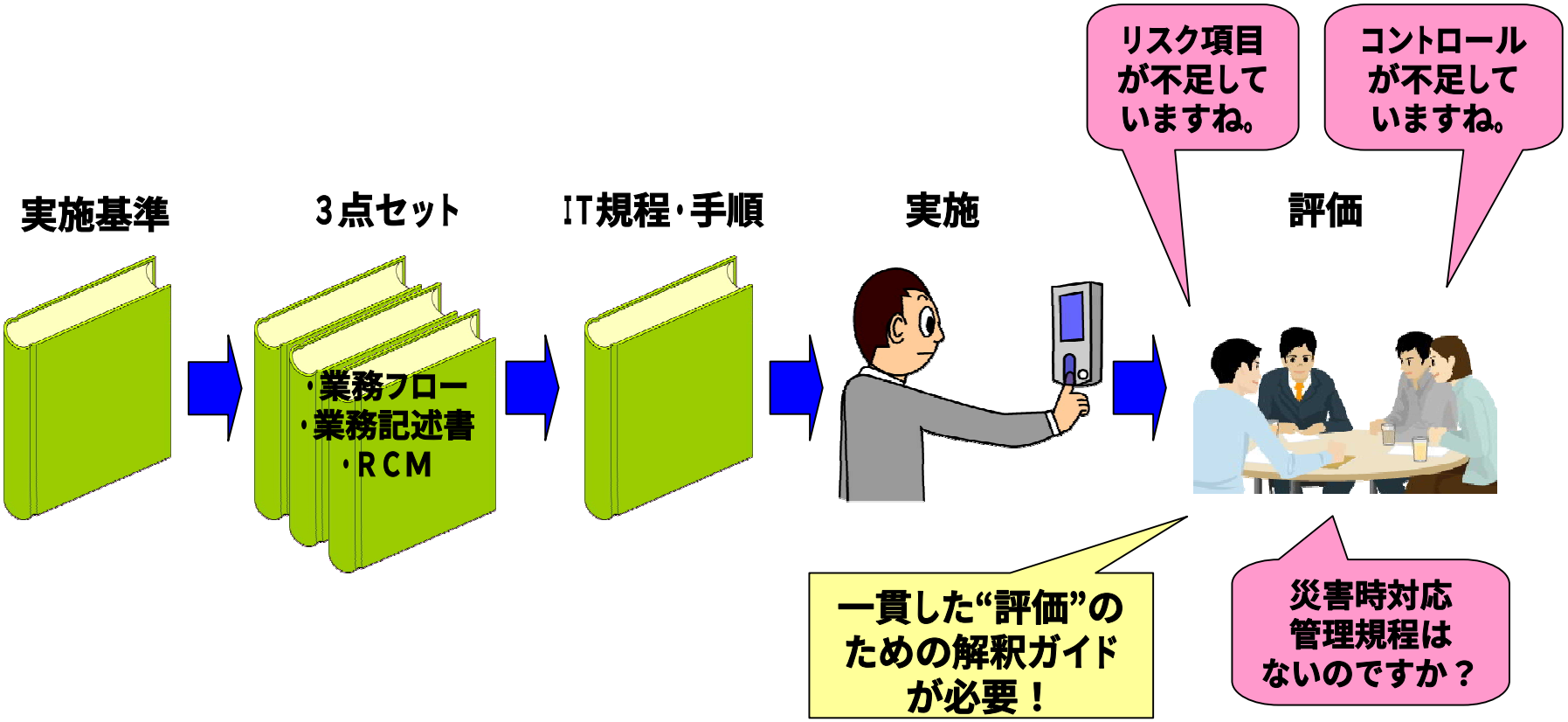
・内部統制が存在しない
・規定されている内部統制では内部統制の目的を十分に果たすことができない

2．運用の不備

・整備段階で意図したように内部統制が運用されていない
・運用上の誤りが多い
・内部統制を実施する者が統制内容や目的を正しく理解していない

ＩＴ全般統制のｺﾝﾄﾛｰﾙと規程・手順書化の関係

・評価時に「ITの規程・手順書」の不足をどこまで指摘するか？
・「IT全般統制評価支援」では、作業者が一貫して指摘できるように「システム管理基準　追補版」の「コントロール」評価項目が「実施基準」の「どの項目」に照らして指摘できるかのガイドを作成しておく必要がある。



監査人の心証を良くするノウハウ（1）

NO	監査人		被監査組織	
	質問項目	その心	悪い回答	良い回答
1	内部統制構築運用方針はありますか？説明して下さい。	・トップとして内部統制に取り組む姿勢を知りたい ・特にWhy？ ・従業員にどうして欲しいと思っているか？	・特にありません。ＪーＳＯＸ法律を義務として実施するだけです。 ・財務に関する完全性は重要なので、全てルール化して見える化しています。	・方針書は明文化してます。 ・我が社が何故、内部統制を構築運用するかと言うと・・・ ・よって、評価も大変重視しています。特に、IT全般統制はＮＥＳさんにお願いしています。
2	内部統制全体の構築状況はどうですか？	・どこまでが有効で、どの辺が有効でないと判断しているか？ →トップダウンに解決しているか？	・実施基準により求められていることは、人的承認行為を強化し対応しました。従来のITはこの１０年間問題なく動いているので、今回定めたルールで運用していくつもりです。よって、１００％対応したと考えています。	・初年度としては、従来から使用している基幹システムに人的コントロール（承認など）を追加しまずは対応した。 ・しかし、業務・作業の負荷が増大しており、人的ミスの残留リスクは残る。 ・よって、将来的にはITで対応できる箇所はIT化したい。3年計画で段階的にIT化による統制を計画している。

監査人の心証を良くするノウハウ（2）

NO	監査人		被監査組織	
	質問項目	その心	悪い回答	良い回答
3	内部統制を構築・運用した前と後で変化はありますか？従業員の変化はありましたか？	・内部統制を構築・運用して、組織文化がどのように変えていきたい、そして変わってきたかと感じているか？	・従業員が全内部統制の規定を遵守するよう教育も徹底しており、ルールを守る組織文化ができています。	・今回のＪ－ＳＯＸ対応は組織の成熟度の向上、企業価値向上の良い機会と捉えています。財務処理の健全性を高めることによって、透明度の高い組織文化を構築でき、管理会計情報も（トップ）に迅速に伝わることができます。 ・さらに、財務を中心にしたITガバナンス向上を、イノベーションプロセスや支援プロセスへ拡大し全体最適のIT活用に向け推進していく所存です。
4	今後、継続改善したい課題はありますか？	・全体的に有効であるが、細かいレベルで課題が残っていることを認識しており、今後とも改善していく姿勢が見られるか？	・文書規定は確実に出来ており、従来のITに対し人的対応を充実することにより進めていきたい。	・IT化が間に合わず、承認行為を文書ベースの人的対応で行っているが、業務効率の向上を考えて、IT化できるところを拡大していく予定です。

監査人の心証を良くするノウハウ（3）

NO	監査人		被監査組織	
	質問項目	その心	悪い回答	良い回答
5	評価の実施状況はどうですか？	・定量的に全体を把握しているか？ ・統計的にＯＫか疑ってかかるか？	・業務処理統制は監査部門に、IT全般統制はＩＳ部により評価しました。 報告によると数件の観察事項があったと聞いています。	①全体で、５００項目評価し、重要２件、不備２８件、観察４２件でました。内訳は ②全般的な内部統制の評価で△件 ③業務プロセスに係る内部統制の評価で△件 ④ITを利用した内部統制の評価で△件 ⑤委託業務の評価で△件です。
6	対応状況はどうなってますか？	・取組み姿勢ができているか？ ・隠そうとしていないか？	1	・１０月の評価で７２件、２月の評価で２７件でた指摘に対し、重大なものは、このように抜本的対策を行い、再確認させました。また機微なものも同様に対策し、内5件を7月までに対応する計画になっています（予算割当、責任者設定済み）。観察も・・・

監査人の心証を良くするノウハウ（4）

NO	監査人		被監査組織	
	質問項目	その心	悪い回答	良い回答
7	今後の計画（年間計画）はどうなっていますか？	・漏れを、放っていないか？	・部門の判断で対応し、実施結果を報告することになっています。	・評価による是正計画および現場からの申告による不具合の真の原因を追究に、○○件を今後このように1年計画で是正していく計画になっています。 ・それまでの間は、計画部門により常時監視し、緊急時は直ぐに、少なくとも月例会議で監視状況の報告が挙がって来る仕組みになっています。また、責任者はこのメンバです。
8	評価後の是正計画と実施はどうなっていますか？	・是正指示を適切に出して、フォローしているか？	・是正の指示は出しています。確認は責任部門が行っているはずです。	・是正計画は責任分担部門で、即刻作成し委員会によりトップ承認しています。 ・是正処置の実施後フォローは評価Gが行い、報告が毎月あがり、委員会の討議を経て、承認しています。

監査人の心証を良くするノウハウ（5）

NO	監査人		被監査組織	
	質問項目	その心	悪い回答	良い回答
9	ＲＣＭによって、事前にリスクに気づいてコントロール活動をしているか？	・ＲＣＭ＝予防処理と認識しているか？ ・事故になる前に、未然に予防を発見し、対策を取っているか？	・ＲＣＭはコンサルの協力を得て実施しました。 ・コントロールは想定できる範囲で対応しています。	・ＲＣＭの結果抽出したリスクに対し、コントロールをベストプラクティスに照らし当てはめて、その結果リスクがどこまで減るか検証しています。 ・全てのコントロールは対応計画の立案、役割分担を決め、実施・評価し、効果の確認をシステム監査も導入し実施しています。
１０	販売管理業務で似ているが、異なるフローがいくつかあるが、どのように考えているか？	・１つの場合は疑ってかかる。 ・ｎ個有る場合はシンプル化の検討を行っているか？	・既存の業務フローを全て文書化しました。毎年見直しをして、現実の業務フローと合致するようにしています。	・販売管理業務にいくつかのパターンがあることが、業務フローを書いて分かりました。 ・今年度はこれで行きますが、来年度はここととここは統合する計画です。 ・残りは、３年くらいを見て統合した方が、経営効率が良いと考え、答申していく予定です。

監査人の心証を良くするノウハウ(6)

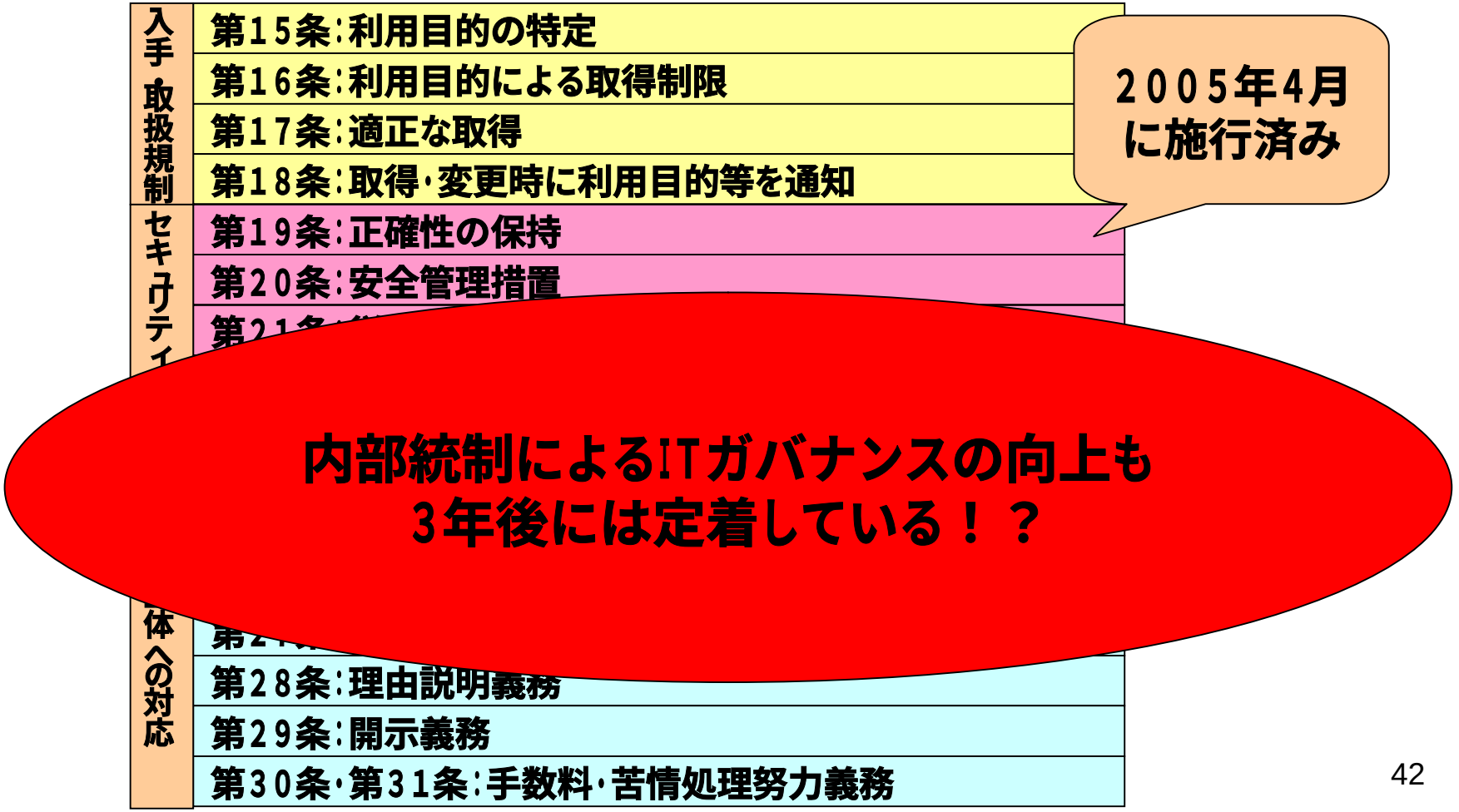
NO	監査人		被監査組織	
	質問項目	その心	悪い回答	良い回答
11	いつから本格的に運用を始めましたか？	・準備・運用の時期は妥当か？	・えっと、2006年12月からPjを発足させてましたので、2007年1月に本格運用を開始したことになります。	・正直申しますと、2007年4月にPjスタート、外部の協力を得て9月までに構築、10月15日本格運用を開始したので、当面評価、見直しを2ヶ月単位に行っていく予定です。
12	1年間運用してみて、不具合が発生して見直しした箇所はありますか・	・非効率になった点はないか、現場からの意見を取り込んでいるか、評価での指摘は妥当で見直しているか？ ・将来に亘って、継続改善する意思、体制はあるか？	・いいえ、特にありませんでした。 (監査人：本当かな？これは、詳しく見る必要がありそうだ．．．)	・運用してみて、計画部門から、いくつかの不具合の声が挙がってます。 ・内部評価をして見て、不具合の指摘が挙がってます。 ・一覧表はこれです。内部評価の不具合は是正計画を立て、進捗はこうなってます。 計画部門からの声の集計はこれで、現在、当面の対応と抜本的改善(是正)を検討しています。議事録はこれです。

監査人の心証を良くするノウハウ（7）

NO	監査人		被監査組織	
	質問項目	その心	悪い回答	良い回答
13	構築に当たり、コンサルタント等の支援はありましたか？	・本質的に理解しているか試そう。 ・まず、過大になっているだろう、重たい部分に気づいていて、改善していく予定があるだろうか？	・監査人には相談しましたが、後は実施基準等で行いました。特に支援は受けてません。	・監査人への事前の充分な相談、業務処理統制は○○コンサル会社、IT全般統制は当社のベンダーであるＮＥＣソフトさんに協力を得て対応しました。 ・今後の改善もあるので、今後1年間は支援を受けていきます。 ・評価作業は業務処理統制の評価は自社で、IT全般統制評価はＮＥＳさんの支援を受け、確実に自社のものとして取り込んで評価作業を継続的に実施していきます。

個人情報保護法は定着した！？

この法律は、高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることにかんがみ、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。



ま と め

Ｊ－ＳＯＸ法への対応

法令遵守として最低限実施しなければならないことを、確実に実施する。

株主／投資家に対する社会的責任の一部をまっとうする。

上場企業（ユーザ企業）

自らの統制環境や統制活動等の現状を見直し、ITガバナンス強化に向けた本質的な活動と認識する。
また、ITベンダーとの関係を見直し、監督・牽制を強化するなどの対応を行う。

ITベンダー

自らのIT提供能力・統治能力を示し、説明責任を果たす。
また、ユーザ企業との関係構築・強化を図る絶好の機会であり、競争力強化を左右する取組みである。

法令遵守対応の先にある、ビジネス機会創出やITガバナンスのあり方などを追求した取組みとして、企業の価値観形成や現場のモチベーション向上につなげていく。

VALWAY
NECソフト

END