内部統制を分かるために必要な基本的視点・考え方

２００７．１１．７

弁護士法人　エルティ総合法律事務所
所長弁護士／システム監査技術者／
公認システム監査人
藤　谷　護　人

1.「仕事」としての「内部統制」

(1)「仕事」とは？

□□を○○することである。

(2)「問題」とは？

ＡＡＡＡＡとＢＢとのＣＣＣＣである。

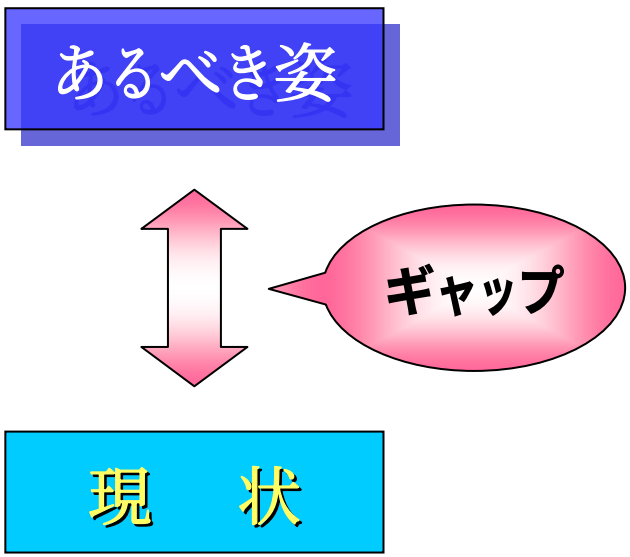
(3)「解決」とは？

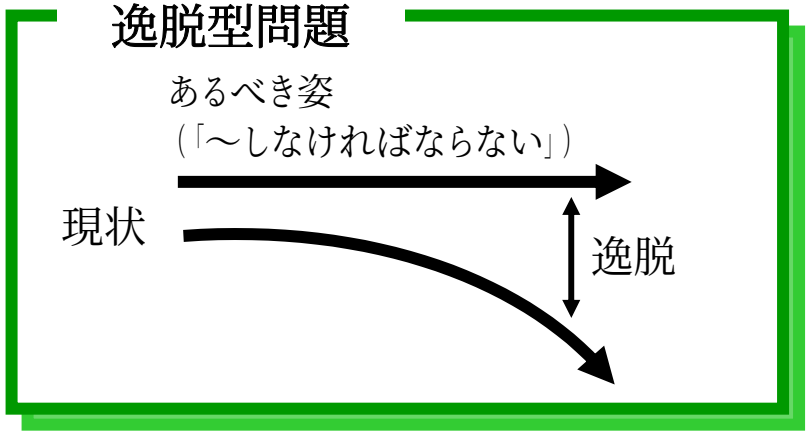
□□をＤＤし、ＥＥし、ＦＦし、ＧＧすることである。

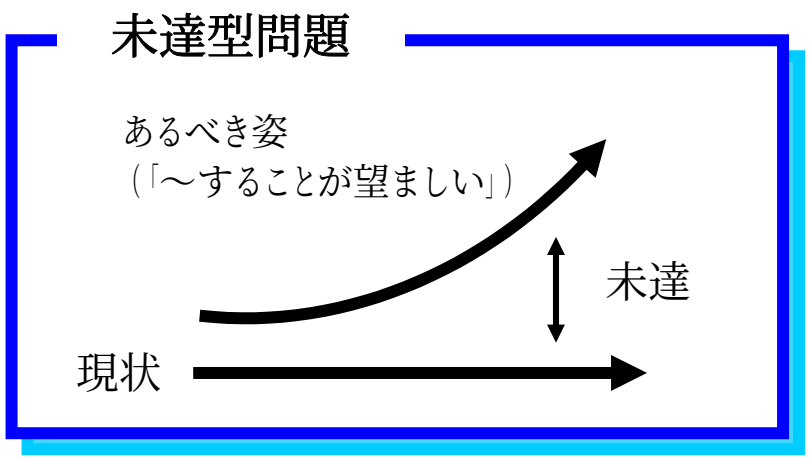
(4)「内部統制業務」とは？

逸脱型問題と未達型問題

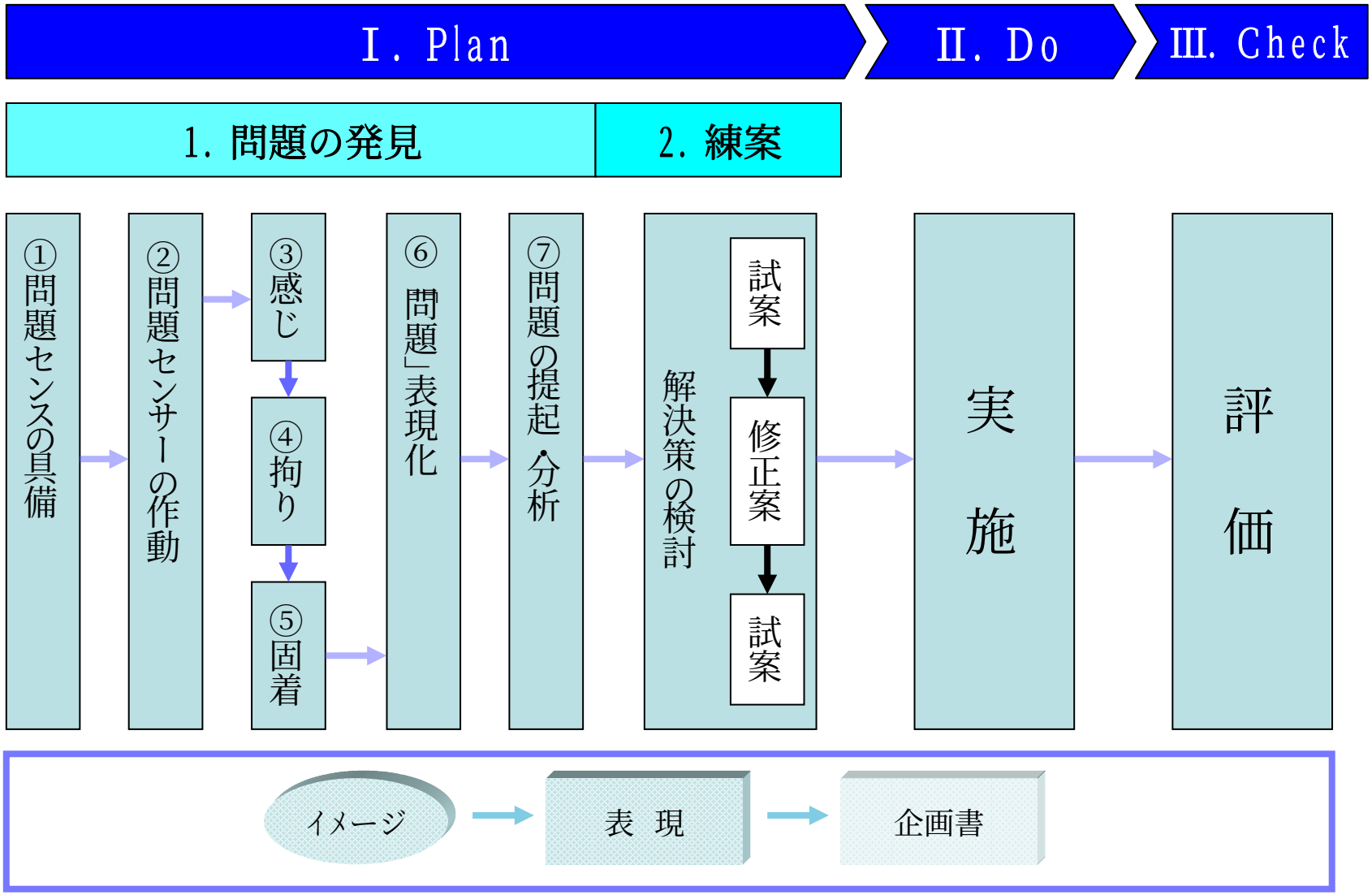
問題とは・・・・・・



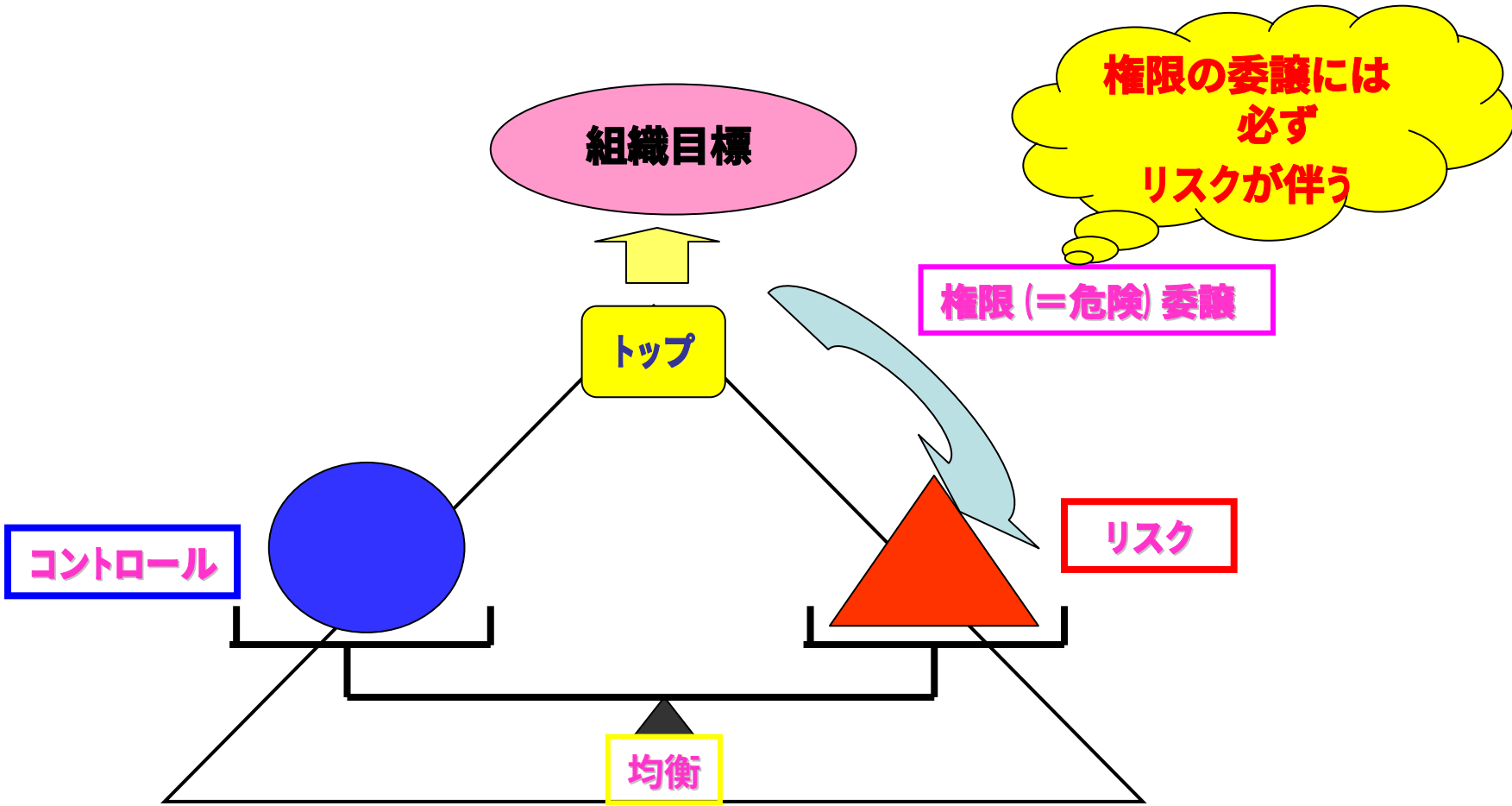




問題解決のプロセス



2.「内部統制原理」



全組織的リスクマネジメント（ERM）

内部統制原理とは

■組織とは、組織目標の実現のために、人的資源と物的資源を有機的に結合して、諸活動を行う社会的存在である。

■人的資源の有機的結合は、トップから下位への権限委譲によって行われる。

■この権限委譲によって、個人活動を遙かに超えた組織的活動が可能になり、大きな成果を実現することが可能になる。

■しかし「権限委譲には必ずリスクが伴うものである」（権限の付与はリスクの付与でもある）ことに気付かなければならない。

■リスクの大きさと均衡のとれた管理策（コントロール）を実施（リスクマネジメント）しなければ、リスクが顕在化してしまう。

■組織が社会的存在として許されるためには、様々に社会（あるいは組織に対するスタークホルダー）に対して、迷惑を掛けかねない組織のリスクをマネジメントする仕組み（エンタープライズ・リスクマネジメント＝内部統制システム）を整備することが要件である（社会的に許す法理）。

■以上の社会的理を組織の「内部統制原理」と言い、内部統制を実現するシステムとはＥＲＭそのものに他ならないのである。

3.「コーポレートガバナンス原理」－組織統治原理－

□権限分離原則

- ・権力集中による恣意的経営の排除
- ・チェック（抑制）＆バランス（均衡）

□会社民主主義

- ・所有と経営の分離
- ・株主主権

4. エンタープライズリスクマネジメント（ERM）

□「リスクマネジメント」とは

「リスク分析」

「リスクコントロール」

・抑制／防止→検出→回復

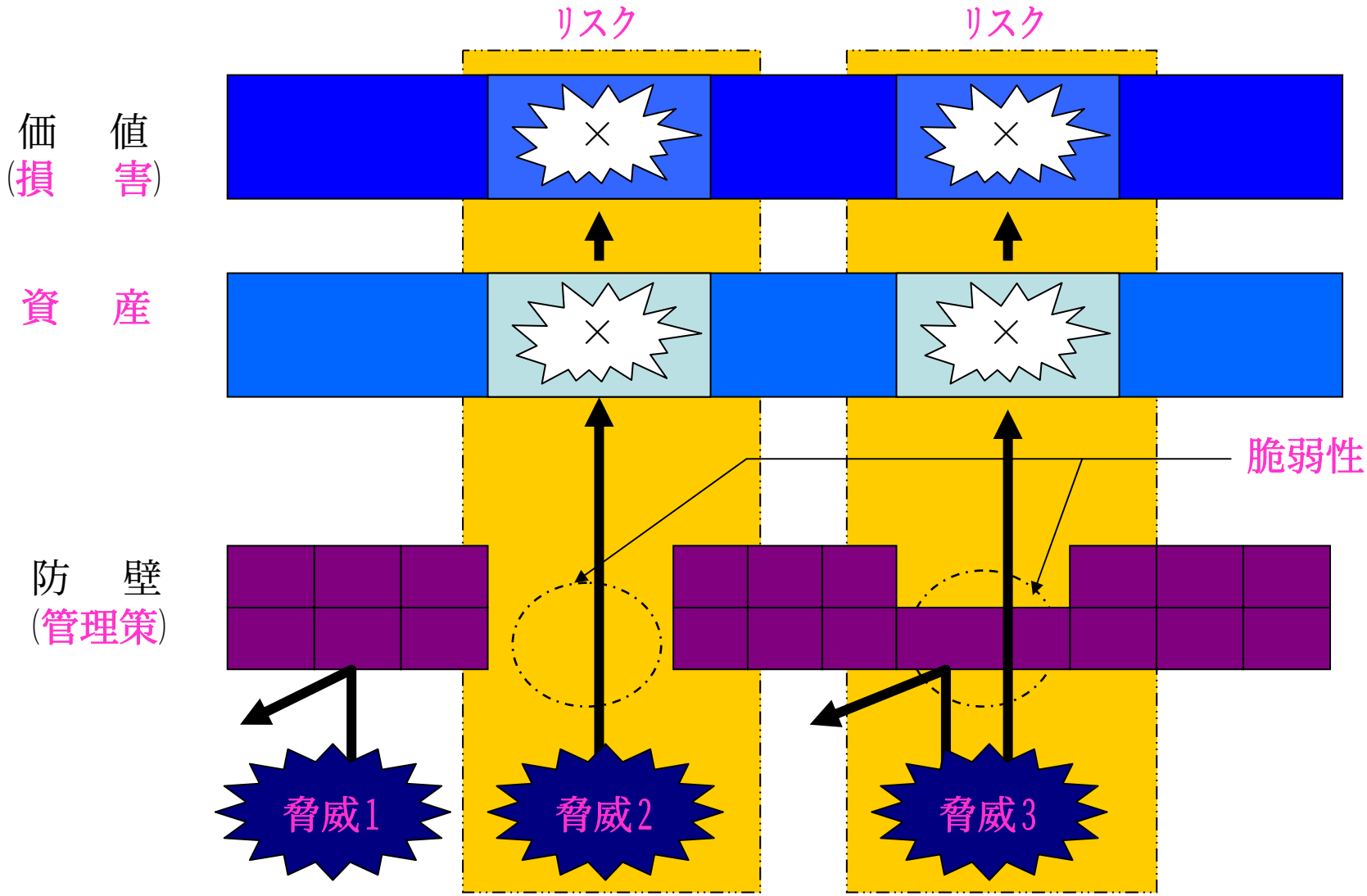
・低減／移転／回避／保有（監視）

「数値化ーベースラインアプローチ」

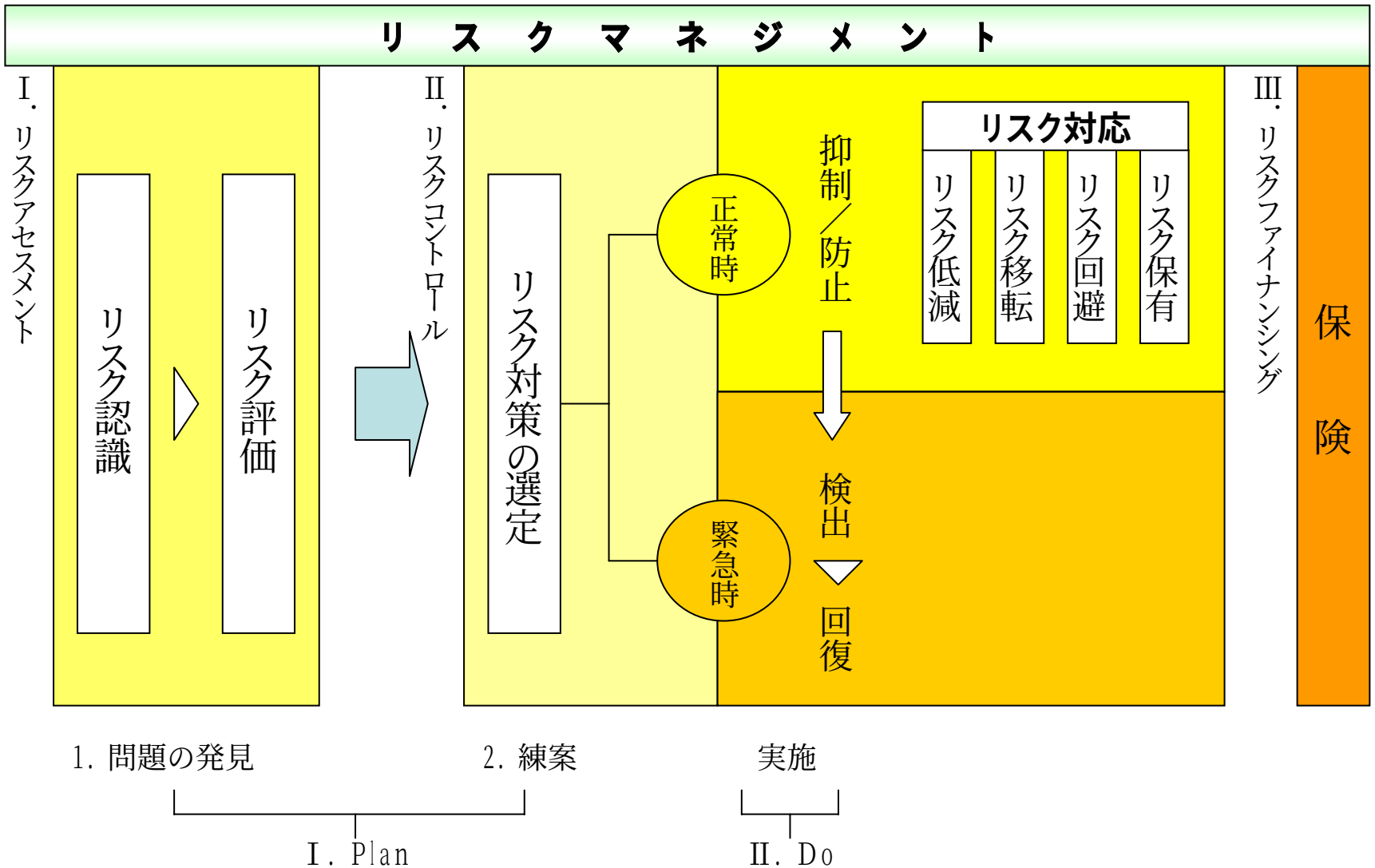
□「ERM」とは

企業経営における全社的リスクマネジメント（COSO2004）

＜資産と管理策と脅威と脆弱性とリスクの相関関係＞



リスクマネジメント技法



リスク値算出早見表ーベースラインアプローチ

	脅威								
	1			2			3		
	脆弱性								
資産価値	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2		4	6	4	8	12	6	12	18
3		6	9	6	12	18	9	18	27
4		8	12	8	16	24	12	24	36

許容リスク値は「8」以下の例。資産価値4、リスク値「24」を許容リスク値「8」にするには、2つの方法がある。

5．情報セキュリティ・問題解決技法としての「情報セキュリティ・リスクマネジメント」とは？

□「情報セキュリティ」とは
「情報資産」について、CIA+ACを図ること

①機密性Confidenciality　②完全性Integrity　③可用性Availability

④説明責任性Accountability　⑤法令遵守性Conplianciality

□情報セキュリティ・「リスク」とは
「管理策」の「脆弱性」を「脅威」が突破して、
「情報資産」の「価値（CIA）」が損なわれる危険性

5－2．情報セキュリティは「何故必要」なのか

- 情報システムは「技術」である。デメリットを伴わない技術はない。
- 「社会的に許す法理」＝技術の「有用性」を社会的に必要としており、技術のデメリットによる「リスクをコントロール」できる場合には、その技術の使用を認める、という考え方。
- 「自動車技術」には、毎年交通事故死者が1万人というリスクがある。だから自動車技術を使用することは「原則として禁止」されている。「運転免許」とは、交通法規の理解と安全運転技術の修得を条件として「禁止を解除」すること。
- 「コンピュータやインターネット技術」にも情報漏えいやネット自殺などデメリットがあるが。その使用は「原則として自由」である。しかしそれを安全有効に使用するためには「情報セキュリティ（機密性（C）・完全性（I）・可用性（A）・説明責任性（A））」が不可欠である。
- ＪＳＯＸ法により「内部統制システム整備義務」として「情報セキュリティ」が法的義務化。

6．「企業法人」という「社会的技術」を「社会が許す法理」

□ソーシャルエンジニアリングとしての「企業法人」

◇虚構性に対するリスクコントロール

□ソーシャルエンジニアリングとしての「株式市場」

◇信頼性（粉飾・不正確）に対するリスクコントロール

□「ＥＲＭ」が必要とされる理由

◇＝内部統制原理

6-2. J-Sox法のルーツ①（商法・会社法的リスク）

○経営者の「内部統制（不作為）責任」を問う株主代表訴訟
＝「取締役の善管注意義務違反」判例ルール

①H12.9.20 大和銀行株主代表訴訟事件、大阪地裁判決
「健全な会社経営を行うためには、～リスク管理が欠かせず、会社が営む事業の規模、特性に応じたリスク管理体制（いわゆる内部統制システム）を整備することを要する」として、現・元取締役らに総額８３０億円の賠償命令。

②H15.4.5 神戸製鋼所株主代表訴訟事件、神戸地裁和解所見「取締役は違法行為などがなされないよう、内部統制システムを構築すべき法律上の義務がある。企業トップは、社内の違法行為について知らなかったという弁明だけでその責任を免れない」として元会長らが3億1０００万円払うとの和解成立。

H15.6.27　経済産業省、リスク管理・内部統制に関する研究会報告書「リスク新時代の内部統制　－リスクマネジメントと一体となって機能する内部統制の指針－」公表。

H15.7.30　旧商法特例法において、委員会設置会社における取締役会に「内部統制システム整備義務」を規定。<資料3>

H17.6.29 会社法の中に、委員会設置会社と大会社の取締役会に「内部統制システム整備義務」を規定<資料1・2>。それら以外の会社には判例ルール。

6－3．J-Sox法のルーツ②（金融商品取引法的リスク）

米国	エンロン	ワールドコム
	2001.10 新聞報道（不正会計）	2002.6　2002.7 粉飾露見　破綻 監査法人コンサル部門が結託

日本	カネボウ	西武鉄道	ライブドア
	2005.4 粉飾露見	2004.10 有価証券報告書虚偽記載	2006.1 偽計取引 風説流布

Sox法
§303
§404

2005.12.8
「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」
企業会計審議会

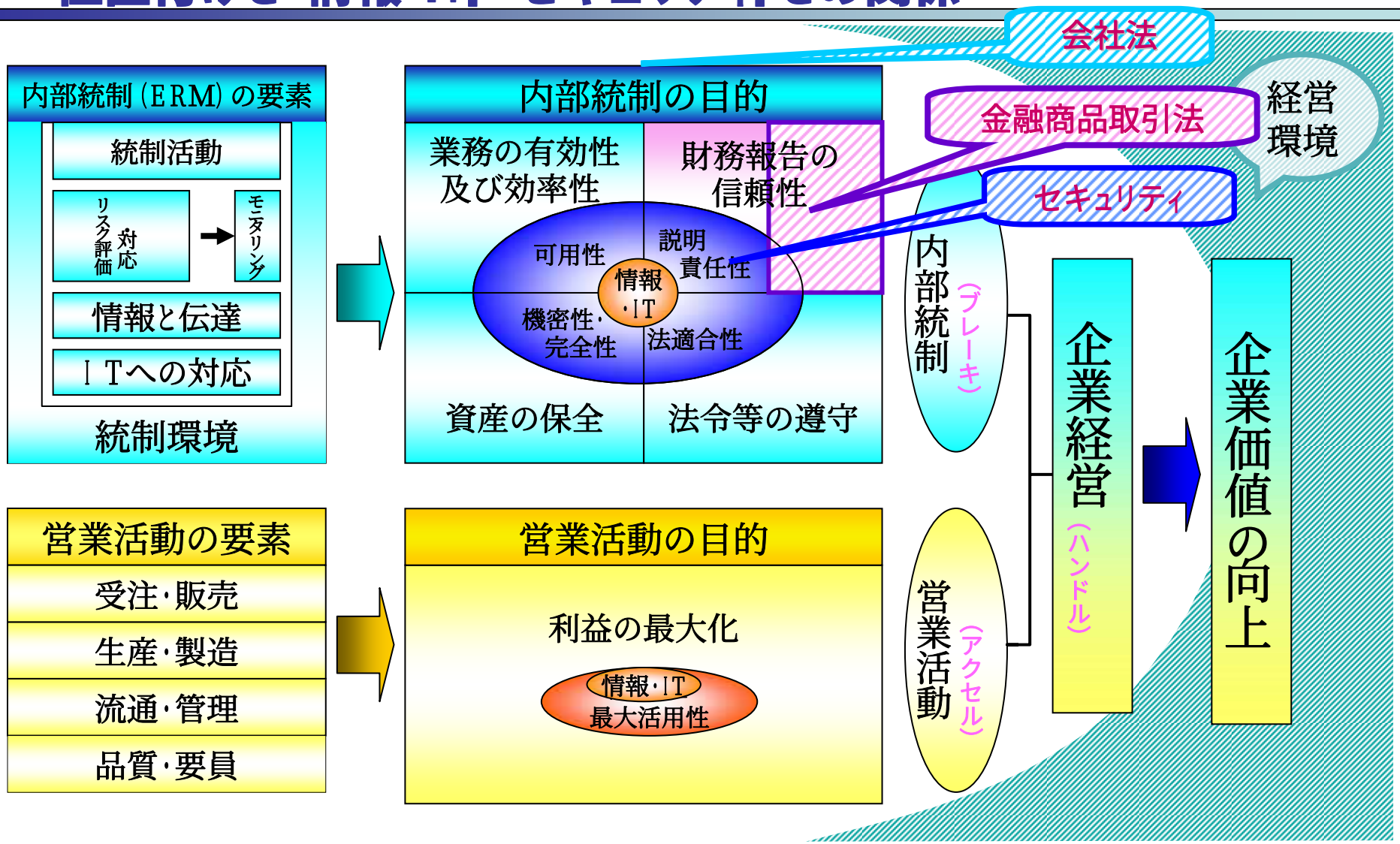
金融商品取引法
2006.6.7における
「第2章 企業内容等の開示」
<資料4>

2006.11.7
「実施基準（案）」
企業会計審議会

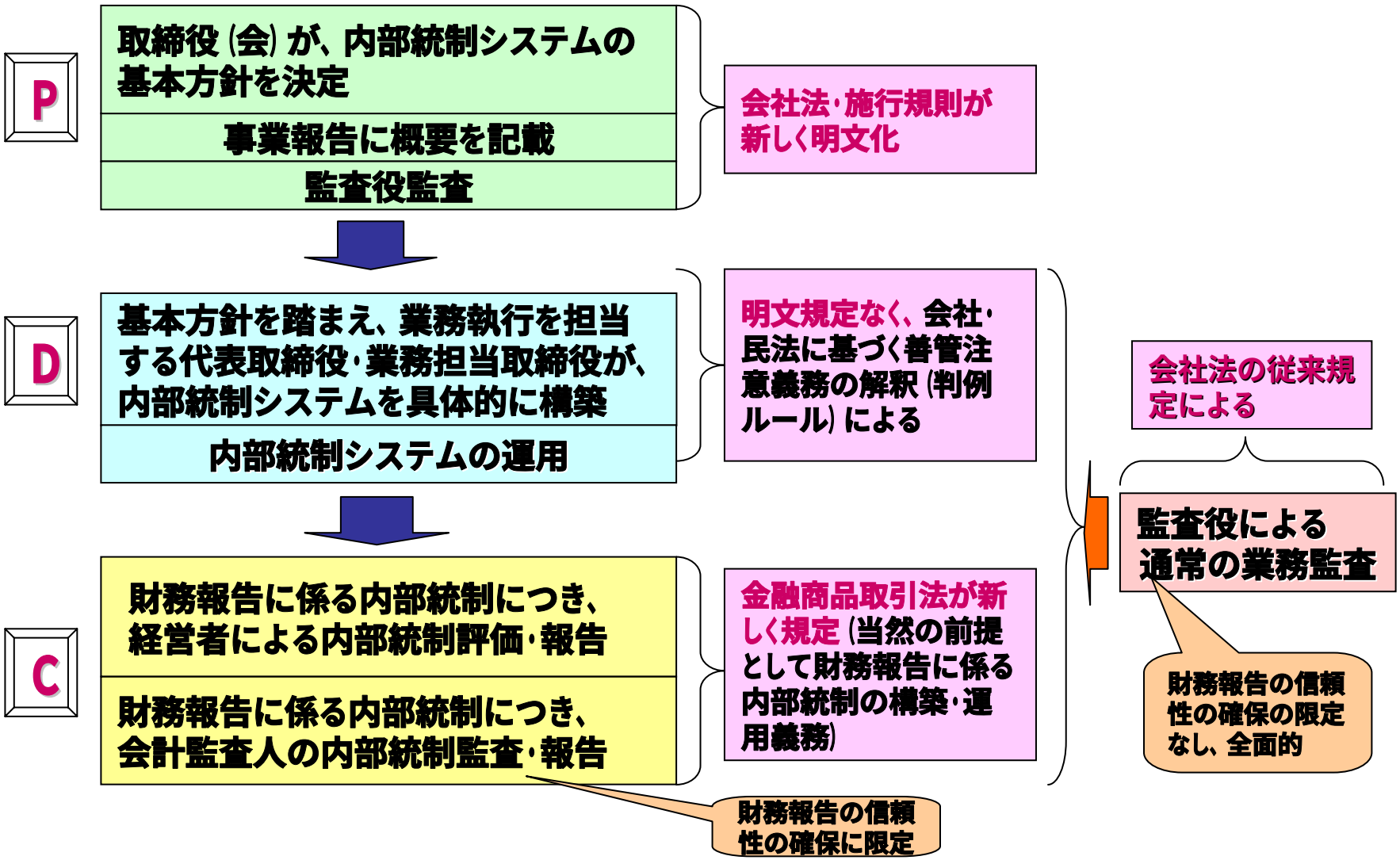
従来の
コーポレートガバナンス
が
機能不全

「内部統制システム」整備の義務化
→「業務プロセスの可視化」による
株式市場の信頼性の確保

7．会社活動の全体構造における「会社法」「金取法」の内部統制の位置付けと「情報・IT」「セキュリティ」との関係



8.「内部統制システム・マネジメントサイクル」と「対応法令・ルール」



会社法における内部統制システム規定の概要

内部統制システムの決定（法３４８条４項等）

２００６年５月１日以降の最初に開催する取締役会の終結時までに決定する必要（会社法の施行に伴う関係法律の整備等に関する法律の施行に伴う経過措置を定める政令１４条

議決の概要を事業報告で開示（施行規則１１８条２号）

事業報告での開示は、２月決算会社の２００７年５月総会、３月決算会社で２００７年６月総会以降（施行規則附則６条１号）

内容が「相当でないと認めるときは、その旨及びその理由」が、事業報告の監査にかかる監査役（会）監査報告の必要的記載事項（施行規則１２９条１項５項）

上記総会以降の監査役の監査報告に、左記の記載が必要（施行規則附則６条１号）

金融商品取引法における内部統制システム規定の概要

経営者

経営者が内部統制を整備・運用	この法律の対象は、財務報告に係る内部統制に限られる。
経営者による内部統制評価	財務報告に係る内部統制につき、経営者が内部統制の有効性を自己評価。
財務報告に係る内部統制の報告	財務報告に係る内部統制につき、経営者が自己評価結果を記載した「内部統制報告書」を作成・提出。

監査人

公認会計士又は監査法人が内部統制の評価結果を監査	内部統制報告書を、公認会計士又は監査法人が監査。
監査結果を記載した「内部統制監査報告書」を作成・提出	公認会計士又は監査法人が、内部統制報告書に対する意見を、内部統制監査報告書により表明。

金融商品取引法における「ITへの対応」に関する検討

◆「セキュア・ジャパン2006」（2006年6月15日　情報セキュリティ政策会議決定）

第2章　第4節

ウ）情報セキュリティ関連制度と内部統制制度等との整合性確保

（内閣官房、金融庁及び経済産業省）

「政府が推進する情報セキュリティに関する取組みについて、政府全体としての整合性を確保するため、現在構築が検討されている内部統制制度のIT統制に係る部分において、情報セキュリティ関連制度との関連を考慮しつつ、2006年度に検討を進める。」

■　金融商品取引法（金取法）の成立により、上場企業は、財務報告に係る内部統制の構築が求められることとなる。

■　「セキュア・ジャパン2006」に掲げられた上記の項目については、例えば、経済産業省が展開している既存の情報セキュリティ関連制度と内部統制制度のIT統制部分との間の整合性確保に係る検討があり得るのではないか。

	米国	日本
法律	SOX法	金融商品取引法
内部統制フレームワーク	PCAOB監査基準第2号（COSOフレームワーク）	財務報告に係る内部統制の評価及び監査の基準（企業会計審議会） 金融商品取引法
IT統制フレームワーク	COBT（その他ITIL、ISO/IEC17799等）＋IT Control Objectives for SOX	システム管理基準＋システム管理基準追補版

検討内容

■ITを利用した情報システムにおいて、業務処理統制が財務情報の信頼性を直接保証する役割を果たすことから、上場企業等は、財務報告に係る内部統制に対応したIT統制を構築するにあたり、業務処理統制を含めた統制例を適切に選択することが求められると推察。
(参考) IT統制＝(IT全社的統制+) IT全般統制+IT業務処理統制
ーIT全般統制＝IT業務処理統制が有効に機能する環境を保証する統制活動
ーIT業務処理統制＝個々のアプリケーションシステムにおける、データの網羅性･正確性･正当性･維持継続性を確保するIT統制活動

企業がIT統制を構築する際に参照する代表的なフレームワーク

◆IT統制全般
- COBIT (米国ITガバナンス協会) (→IT Control Objectives for SOX (同左))
- システム管理基準 (経済産業省)

◆ITシステムの運用管理
- ITIL (英国政府)

◆その他
- 自社で開発した基準　等

主にIT統制のために策定した基準であるが、情報セキュリティ関連部分についてはISO/IEC17799等との整合性を確保

SOX法対応のためにCOBITをベースにIT統制目標を整理し、統制を例示したもの

状況分析

◎ほとんどのフレームワークは全般統制にしか言及がないため、財務情報の適正性を確保する観点からIT統制を構築する際、企業は具体的に何をすべきかが明確ではない。

◎また、海外のフレームワークは、欧米の商習慣を前提としているので、我が国の企業にそのまま適用しづらい面もある。(我が国企業がシステム監査の際に参照している基準について調査した結果では、約75%の企業が「システム監査基準」(改定前) を参照している)

検討内容

◎企業がIT統制を構築する際に具体的に何をすべきかが判断できるよう、「システム管理基準 (平成16年10月改正)」をベースに、金融商品取引法に則したIT統制の具体的な例示集を検討。

◎この検討のために、経済産業省から情報通信総合研究所に委託を行い、「企業のIT統制に関する調査検討委員会」において、「システム管理基準追補版 (財務報告に係るIT統制ガイダンス) (案)」を策定。

イメージ

「金融商品取引法」

「財務報告に係る内部統制の評価及び監査基準」
（企業会計審議会内部統制部会）

＝

【構成】
①枠組み
②経営者評価
③監査

内部統制の構築

「実務基準」を踏まえ、企業に置かれた環境や事業の特性等に応じ、適切な内部統制を構築する

「財務報告に係る内部統制の評価及び監査の実施基準」（企業会計審議会内部統制部会）
「基準」を実務に適用していく場合のより詳細な実務上の指針

経営者評価

財務報告に係る内部統制の有効性を評価
（内部統制報告書）

監査

経営者による財務報告に係る内部統制の評価が適正なものかどうかを監査
（内部統制監査報告書）

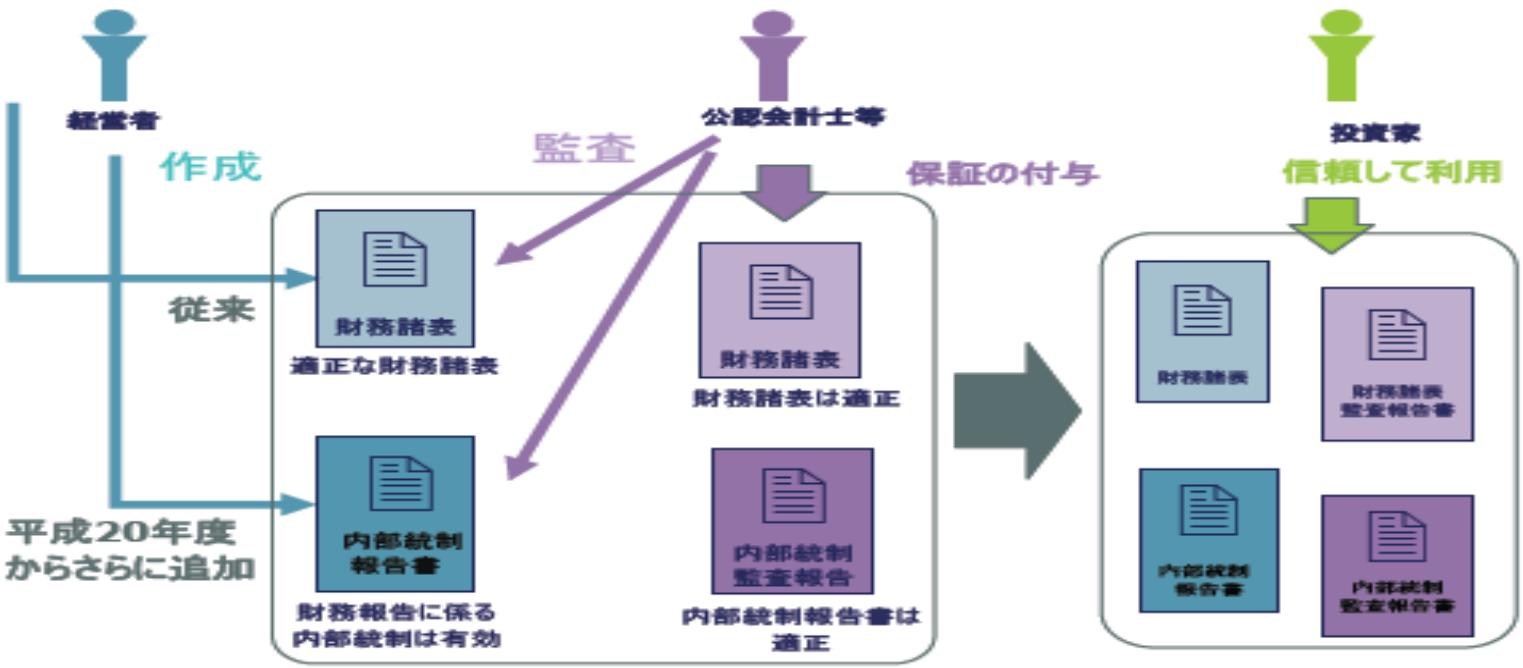
システム管理基準追補版（財務報告に係るIT統制ガイダンス　by METI）
システム利用活動を前提とした内部統制構築のためのガイドラインであり、構築のポイントを明確にすることで、同時に、経営者評価の際の着目点を理解するための利用も期待できる。システム監査と内部統制を再結合した。

実務指針
（日本公認会計士協会）
外部監査人による内部統制監査を行う上での留意事項等をとりまとめたもの

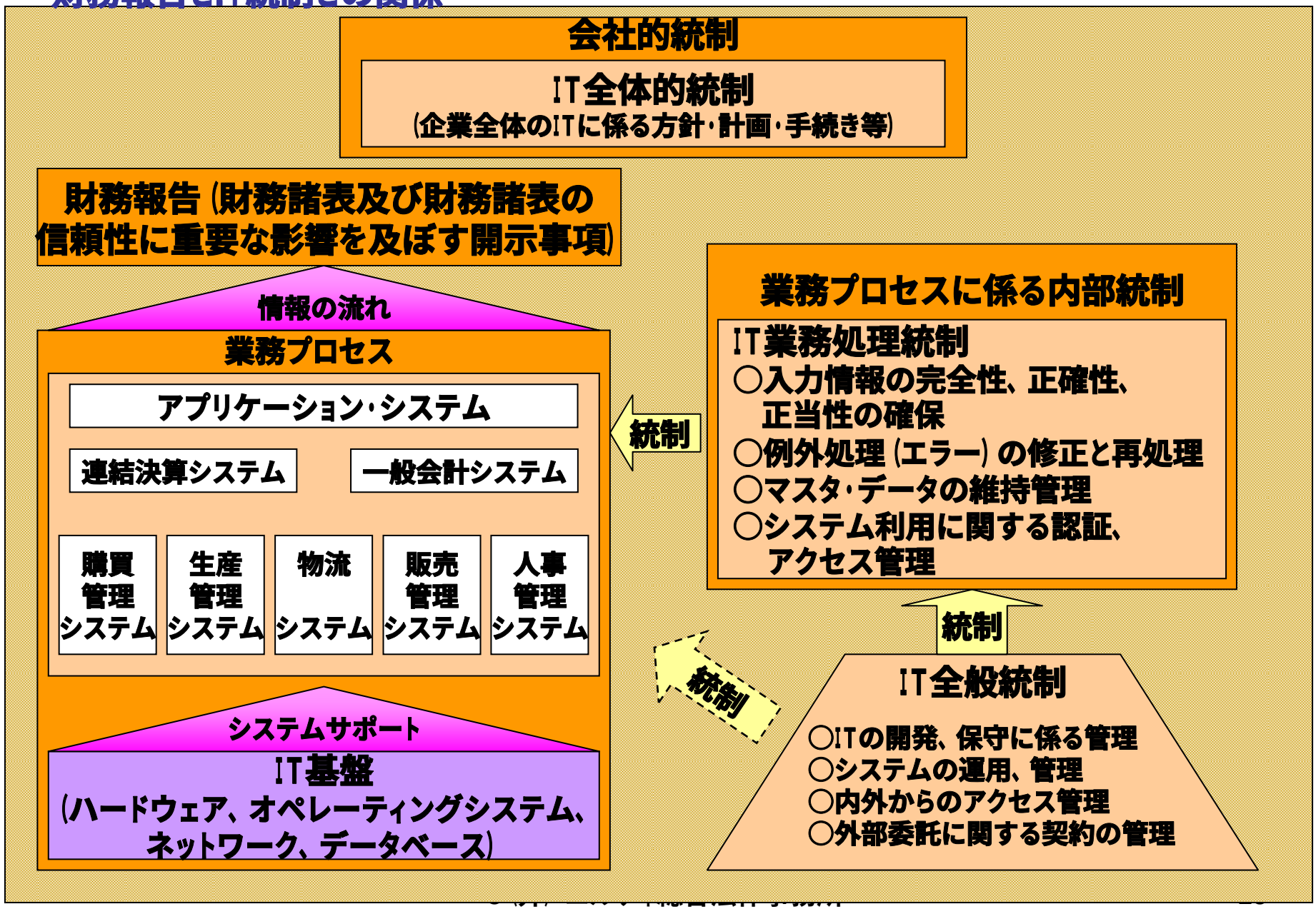
（企業サイド）

（監査人サイド）

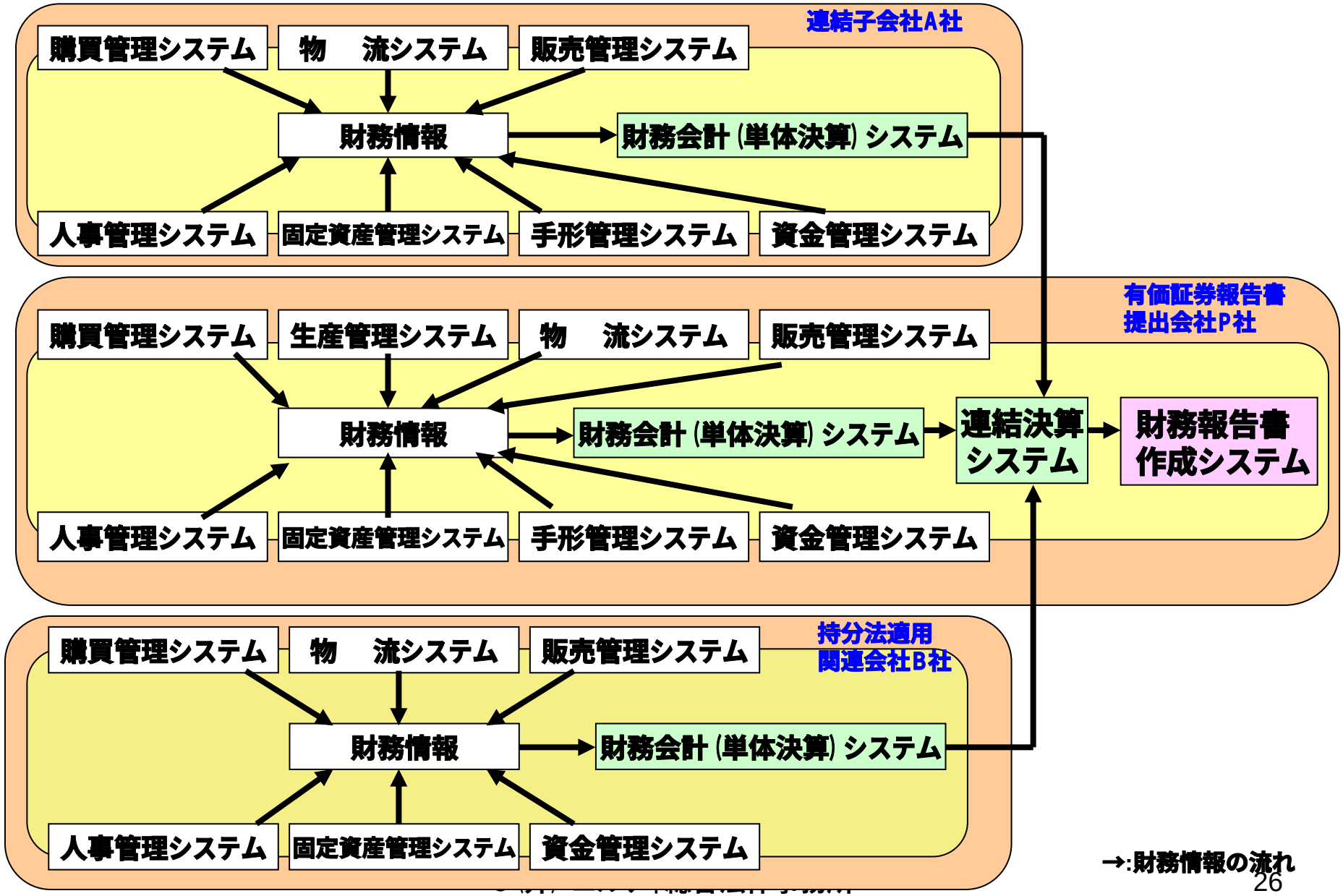
図表Ⅱ．１－１　財務諸表監査と内部統制監査について



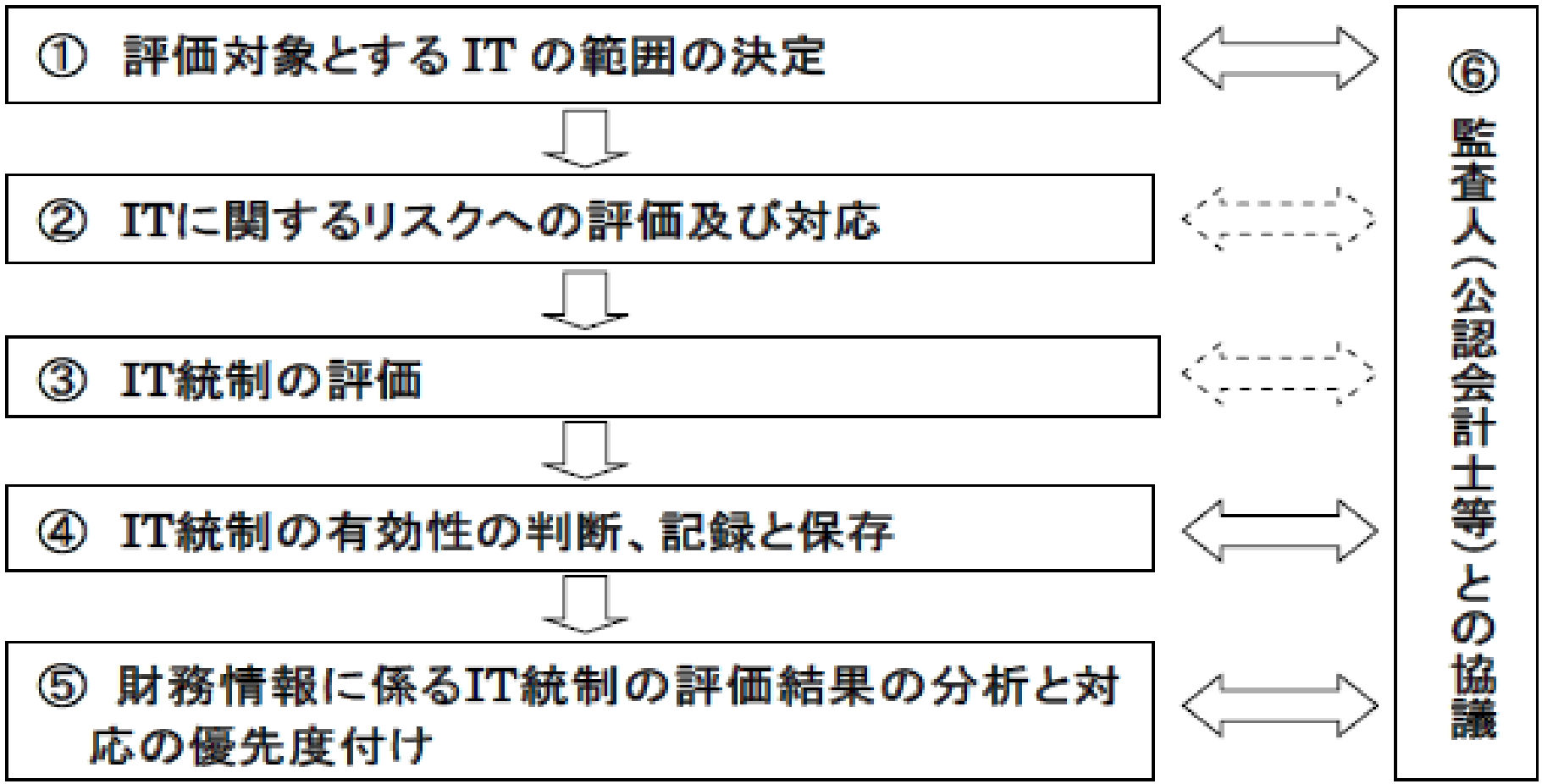
財務報告とIT統制との関係



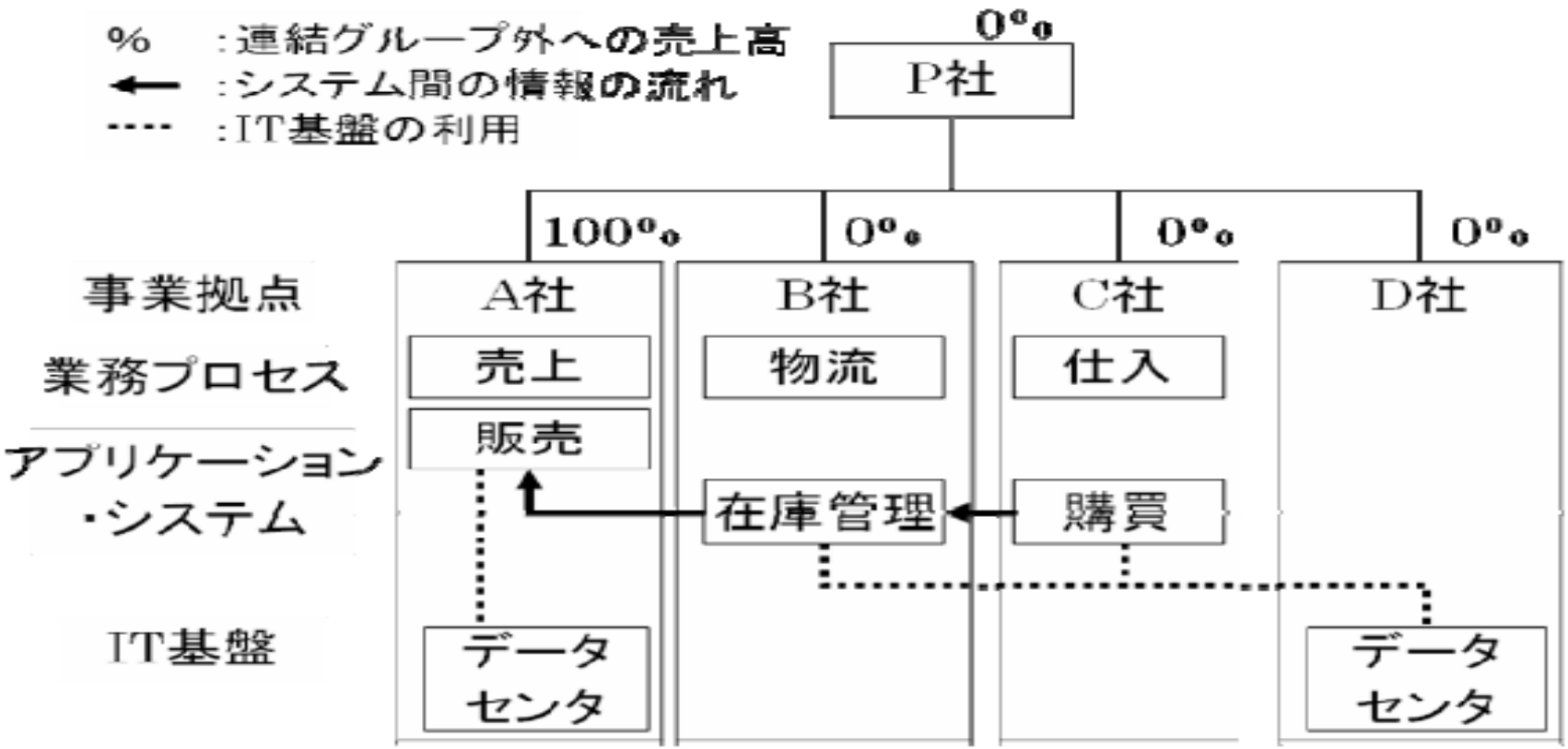
財務報告とアプリケーション･システムの関係



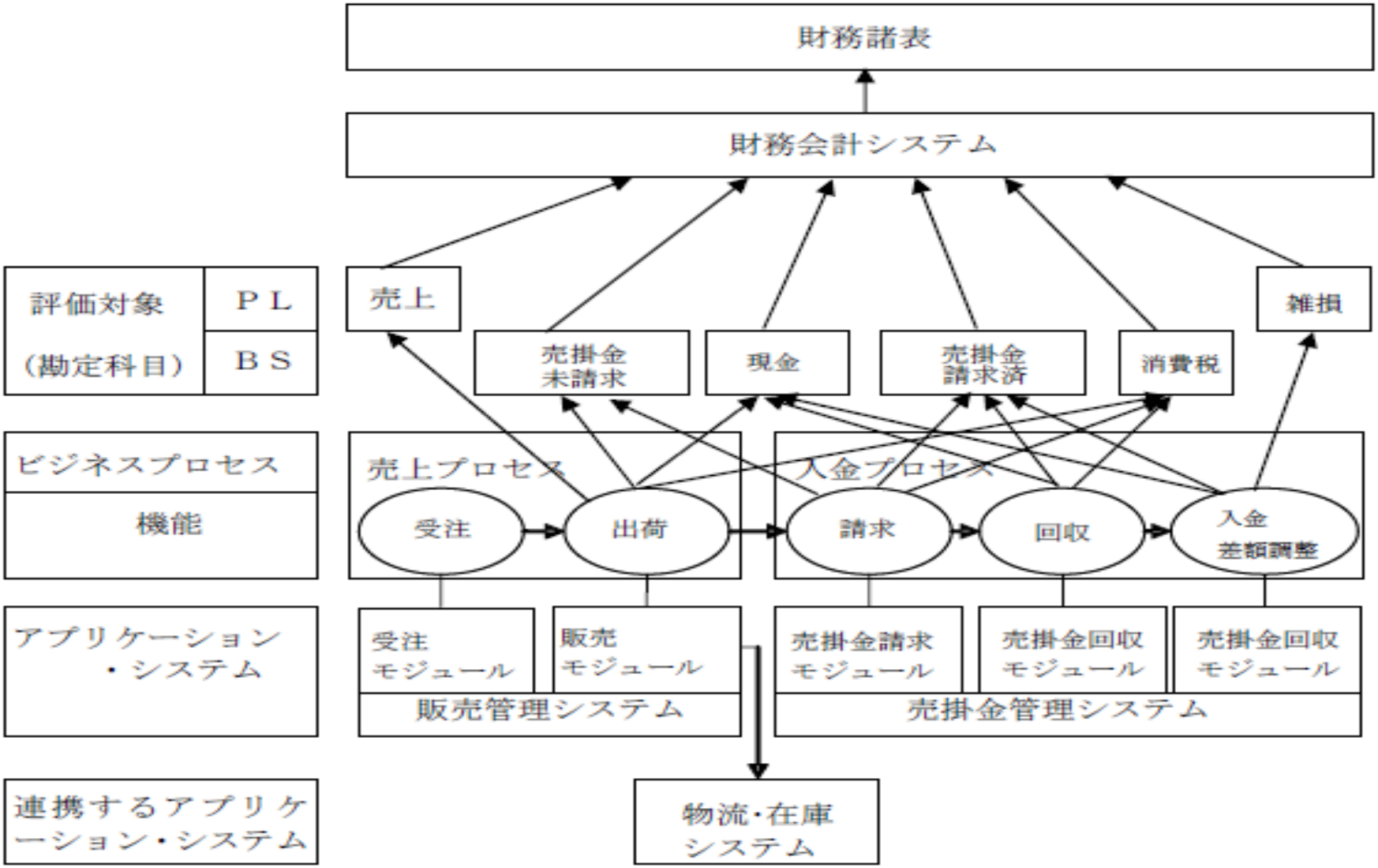
図表Ⅲ．１－１　IT 統制の評価のロードマップ



図表Ⅲ．２－２　IT の評価範囲の例



図表Ⅲ．４－３　勘定科目とアプリケーション・システムの関係



「ITの統制目標」と「アサーション」の関係

IT の統制目標	アサーション（適切な財務情報を作成するための要件）
完全性 (Integrity)	網羅性、期間配分の適切性
正確性	実在性、評価の妥当性、期間配分の適切性、表示の妥当性
正当性	実在性、権利と義務の帰属、評価の妥当性

「アサーション」には存在しない「ITの統制目標」

- **機密性(Confidentiality)**
- **可用性(Availability)**

「アサーション」の上位に位置する「ITの統制目標」

- **説明責任性(Accountability)**
- **法適合性(Compliancy)**

付録２．システム管理基準の統制目標の使い方

３　システム管理基準の統制目標（例）

システム管理基準の統制目標（例）の利用方法は次のようになる。

① 管理項目および管理項目の主旨を理解する

② 対応する統制項目（例）を明確にして、ガイダンスの管理項目のリスクを理解する

③ 該当するリスクが低減したいと考えているものであれば、統制項目の候補となる

④ 統制項目（例）をリストアップして、企業のリスクを低減できることを確認する（リスクコントロールマトリックスの利用など）

システム管理基準の統制目標の利用は企業や業種によって大きく異なっている。したがって、システム管理基準の統制項目（例）の利用にあたっては、各企業の実情に合わせた適用を行うこと。

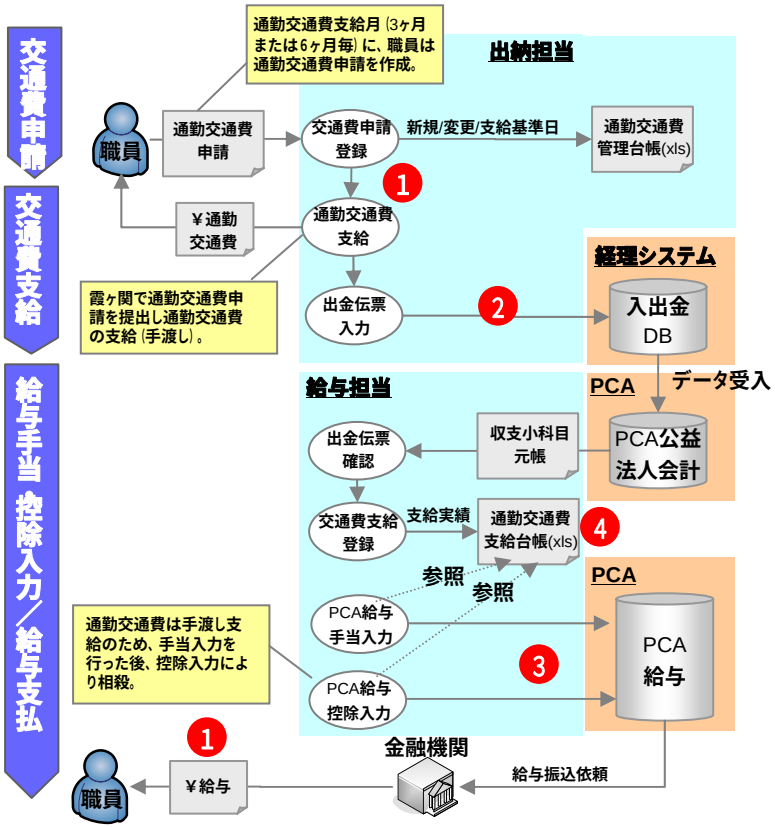
付録2－1　　システム管理基準の管理項目と統制目標の対応（例）

項番	システム管理基準の管理項目	統制種別	統制目標（例）	ガイダンス項番	C/S種別	システム管理基準の趣旨
I	情報戦略					
1	全体最適化					
1.1	全体最適化の方針・目標	全社				
(1)	ITガバナンスの方針を明確にすること。	全社	ITガバナンスの方針（計画）を策定する	2-(1)-①	C	ITガバナンスの確立に際し、その方針を明確にしておく必要がある。
(2)	情報化投資及び情報化構想の決定における原則を定めること。	全社	経営戦略にあわせた情報化計画を定める	2-(1)-①	C	首尾一貫した全体最適化計画を策定するため、情報化投資及び情報化構想の決定における原則を定めておく必要がある。
(3)	情報システム全体の最適化目標を経営戦略に基づいて設定すること。	全社	情報システムの最適化計画を経営戦略と整合させる		S	経営目的を実現する情報システムを企画するため、最適化計画の目標は、経営戦略との整合性を考慮して策定する必要がある。
(4)	組織体全体の情報システムのあるべき姿を明確にすること。	全社	全体最適化計画を策定する	2-(1)-①	C	組織体全体の情報システムは、個別の情報システムが有機的に関連し、整合性が相互に保たれて効率的かつ効果的に目的を達成するものであるため、全体最適化計画は、情報システムのあるべき姿を明確にする必
(5)	システム化によって生ずる組織及び業務の変更の方針を明確にすること。	全社	全体最適化計画は、システム化する組織や業務の変更について示す	2-(3)-①	C	全体最適化計画では、情報システムの（再）構築と同期して行われる組織及び業務の新設、改変及び廃止の方針を明確にする必要がある。
(6)	情報セキュリティ基本方針を明確にすること。	全社／全般	全体最適化計画を、情報セキュリティ基本方針と整合させる	2-(1)-⑤ 2-(3)-① 3-(3)-①-イ	C	不正防止、機密保護、プライバシー保護等は、健全な経営活動推進の基盤であるため、情報セキュリティ対策の方針を全体最適化計画で明確にする必要がある。
1.2	全体最適化計画の承認	全社				
(1)	全体最適化計画の立案体制は、組織体の長の承認を得ること。	全社	全体最適化計画は、経営幹部の承認を得る		S	全体最適化計画は、経営戦略に基づき情報システムの中長期計画として策定する必要があるため、立案体制を組織的に確立し、組織体の長が承認する必要がある。
(2)	全体最適化計画は、組織体の長の承認を得ること。	全社	全体最適化計画は、経営幹部の承認を得る		S	経営戦略に基づいて組織体全体で整合性かつ一貫性を確保した情報化を推進するため、全体最適化計画は、組織体の長が承認する必要がある。

(サンプル) 機能差報告書
ー 通勤交通費支給業務の改善 ー

定性的効果	■ 緊張・単調作業の排除 ■ 情報の正確性向上 ■ セキュリティの向上
定量的効果	-10.75時間/年

合計 10.8時間/年

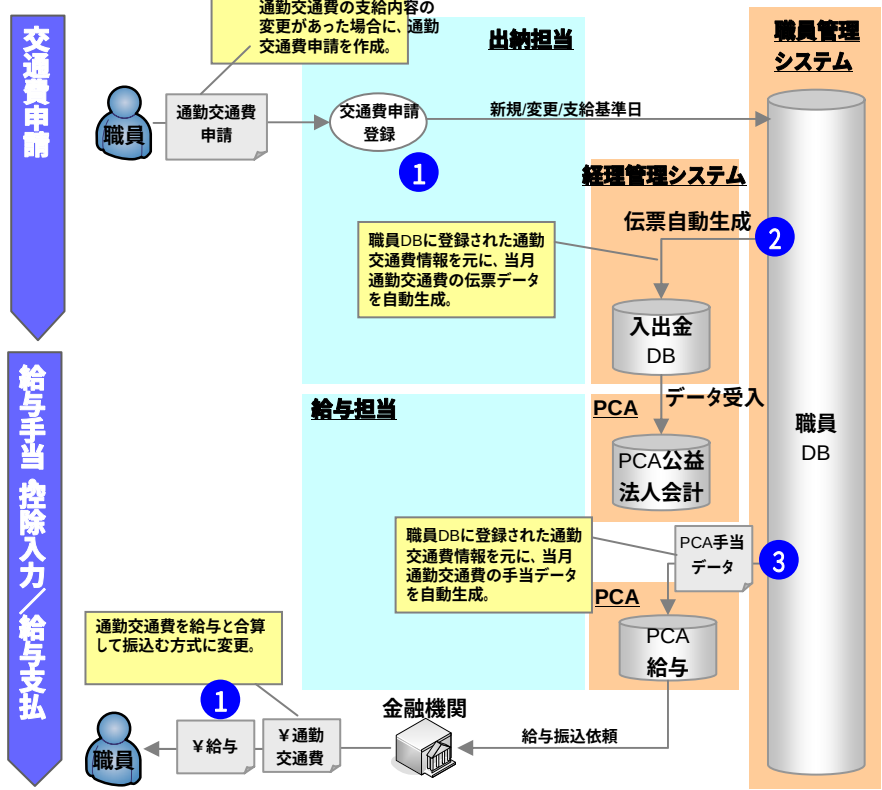


① 職員は指定月に通勤交通費申請を作成のうえ霞ヶ関に出頭し通勤交通費の支給（手渡し）を受ける必要があるため、作業負荷が高く、出納が高額の手許現金を用意するためセキュリティレベルも低い。 0.01時間×80人×2 = 1.6時間/年

② 通勤交通費の支給に応じて、職員の通勤経路毎に伝票入力をする必要があるため、作業負荷が高く、ミスも発生しやすい。 0.02時間×80人×2 = 3.2時間/年

③ PCA給与に通勤交通費支給実績を反映させるために、手当入力後に控除入力で相殺するため、作業負荷が高く、ミスも発生しやすい。 0.5時間×12回 = 6時間/年

合計 0.05時間/年



① 職員は交通費の支給内容に変更があった場合のみ申請し、通勤交通費の支給は給与と合算して振込みにより行う。このことにより、作業負荷の低減とセキュリティレベルの向上を図る。 0.01時間×5人 = 0.05時間/年

② 職員管理システムから、登録された通勤交通費の支給内容に応じて、伝票を自動生成することにより、作業負荷低減と正確性確保を図る。 0時間×80人×2 = 0時間/年

③ 職員管理システムから、PCA給与への手当データを自動生成することにより、作業負荷低減と正確性の向上を図る。 0時間×12回 = 0時間/年

付録6-2

IT全般統制評価記述書

会社名	
決算期	
事業拠点	
対象システム	販売システム

作成者・作成日	◇◇◇◇ 2007/1/23
質問への回答者（実施部署）	

リスク	統制目標 留意事項	No.	統制の状況	整備 運用	予防 発見	手作業 自動化	整備状況 文書	整備状況 プロセス	整備状況 システム実装	頻度	統制評価手続	評価並びに検出事項 （検出事項がある場合、その影響）	調書番号	評価結果
財務情報の信頼性に係わるシステムが適正に開発、関連されずに、処理結果の財務情報に信頼を置くことができない	開発	システムを開発する際に意図的な不正プログラムが埋め込まれていないか、また、処理に誤りがないか		システムを開発するための標準化された方針および手続があり、これに基づいて、ITが開発され、更改されている	整備	予防	手作業	○	○	NA	四半期	対象とするシステムの開発は標準化された手順、文書で実施されていることを確かめた	なし	記載省略	低
		システムの開発プロセスにおいて、意図的な不正や、処理に誤謬がないか		システムの開発プロセスにおいて、財務情報の信頼性に係る正当性、完全性、正確性の統制が確実に実現できるようになっている	運用	予防	手作業	○	○	NA	四半期	開発の仕様書、基本設計書（概念設計書）等で財務情報の信頼性確保の統制機能が織り込まれていることを確かめた	なし	記載省略	低
		以下省略												
保守が適切に実施されないと業務処理統制の信頼が失われる	保守	プログラムが改ざんされたり、承認なく変更されていないか		システムの変更および保守管理については、変更管理手続に従っている（標準化され、記録され、承認され、文書化されている）	整備・運用	発見	手作業	○	○	NA	月週	変更管理手続の規定があることを確かめた。変更管理規定通りに変更管理を実施していることを25件テストした	25件のうち1件、承認漏れがあったが、責任者の押印漏れであり、実際には、承認されているとの説明を受けた。25件の追加テストの結果、押印漏れはなく、単なる押印漏れのミスであると判断した	記載省略	低
				以下省略										

付録6-3

IT業務処理統制評価記述書

会社名	○○株式会社
決算期	平成○○年3月
場所	受注センター
取引サイクル	販売サイクル
ファンクション	受注
関連する勘定科目	売上、売掛金

作成者・作成日	○○○○　2006/12/23
確認者・確認日	□□□□　2007/1/24

リスク	統制目標	留意事項	No.	主要な統制活動	自動化手作業	頻度	要件：網羅性	実在性	期間配分	権利と義務	評価	表示	種類	実施	統制評価手続	評価及びに検出事項（検出事項がある場合、その影響）	証書番号	評価結果
財務情報に漏れや重複が生ずる	網羅性	全ての受注は漏れなく重複なく記録されているか	1	ＥＤＩによる受注はＪＣＡ手順によって制御され異常な伝送があればシステム担当者にメールが送信される	自動化	四半期	○	NA	○	NA	NA	NA	種類・運用	特定の月を選び、システム運用報告をレビューしＪＣＡ手順による異常終了が担当者に報告され、フォローされていることを確かめる	なし	記載省略	他
			2	ＦＡＸ受注はコールセンタで受信後に連番を記入し、一人が入力した後で、ブルーフリストを出力し、他の一人が内容をＦＡＸと照合する	自動化・手作業	日	○	NA	NA	NA	NA	NA	運用	特定の月の２５件を選び、ブルーフリストが照合されていることを確かめる	なし	記載省略	他
			3	在庫引当された受注のみが当資物図ファイルに登録される。未引当の受注情報は、受注残ファイルに記録され営業担当者がフォローして消し込んでいる	自動化・手作業	日	○	○	NA	NA	×	NA	種類・運用	受注残ファイルが営業担当者により、消し込まれていることを確かめる	なし	記載省略	他
財務情報が正確に記録されない	正確性	受注の登録に誤りがないか	4	ＥＤＩで受信した受注データは得意先マスタ、商品マスタと存在性のチェックをし、エラーについてはエラーファイルが作成され、エラーデータについては、得意先に返信し、再送を依頼する。エラーファイルは訂正データが再送されるまで保存される	自動化	日	NA	○	NA	○	○	NA	種類・運用	特定の月のエラーファイルの処理状況を２５件確かめる	なし	記載省略	他
			5	2と同じ。ＦＡＸ受注はコールセンターで受信後に連番を記入し、一人が入力した後で、ブルーフリストを出力し、他の一人が内容をＦＡＸと照合する	自動化・手作業	日	NA	○	NA	○	○	NA	種類・運用	2と同じ。特定の月の２５件を選び、ブルーフリストが照合されていることを確かめる	なし	記載省略	他
			6	受注日付は端末日付で登録される	自動化	日	NA	○	○	NA	NA	NA	種類・運用	売上日付の設定を確かめ、売上データの日付が端末日付であることを確かめる	なし	記載省略	他
			7	得意先コードにより、得意先マスタから得意先名がロードされる	自動化	日	NA	○	NA	○	○	NA	種類・運用	得意先コードにより得意先名が登録されることを画面で確かめる	なし	記載省略	他
			8	単価は得意先ごとにマスタに登録された単価が自動的にロードされ、受注端末から変更入力はできない	自動化	日	NA	○	NA	NA	○	NA	種類・運用	単価が自動的に登録され変更入力はできないことを確かめる	なし	記載省略	他
正当でない財務情報が記録される	正当性	正当でない受注が登録されていないか	9	得意先マスタに登録された得意先以外は登録できない	自動化	日	NA	○	NA	○	NA	NA	種類・運用	マスタに登録された得手先しか登録できないことを確かめる（設定はマスタ登録で確かめる）	なし	記載省略	他
			10	単価は得意先ごとにマスタに登録された単価が自動的にロードされる	自動化	日	×	○	NA	○	○	NA	種類・運用	単価は登録単価が登録され、単価入力ができないことを確かめる（単価登録はマスタ登録で確かめる）	なし	記載省略	他
			11	受注入力は、担当者のＩＤとパスワードで統制されている	自動化	日	NA	○	NA	NA	NA	NA	種類・運用	担当者のＩＤとパスワードでしか受注画面が開かないことを確かめる　（注）シングルサインオンの場合はパスワード設定は、全般統制で確かめる。ただし、販売システムへのアクセス権限は、業務の権限と一致して設定されいることは、業務処理統制で確かめる	なし	記載省略	他
			12	得意先の与信限度を超える受注は入力できない	自動化	四半期	NA	○	NA	NA	NA	NA	種類・運用	与信限度を超える入力ができないことを確かめる	なし	記載省略	他
			13	以下省略										以下省略			
財務情報が長期的に使用できない	継続性	受注ファイルが不当に変更されていないか	14	受注ファイルへの変更は、担当者のＩＤとパスワードで統制されている	自動化	四半期	○	○	○	○	○	NA	種類・運用	受注ファイルは担当者しかアクセスできないことを確かめる（ＤＢＡが統合されている場合は全般統制でアクセス権限を確かめる場合がある）	なし	記載省略	他
			15	受注ファイルへのアクセスログはモニタされている	自動化・手作業	四半期	NA	○	NA	NA	NA	NA	種類・運用	マスタへのアクセスログが一定の条件でモニタされていることを確かめる（アクセスログのモニタは全般統制で実施することもあるが、業務処理統制で実施する方が整理する範囲が絞り込まれる場合がある）	なし	記載省略	他
			16	在庫マスタは、流通センターのマスタと毎晩、夜間バッチで照合され、不一致が起きないように管理されている	自動化	四半期	○	○	NA	NA	NA	NA	種類・運用	在庫マスタが置き換えられていることを確かめる（バッチ処理が正常に実施されていることは全般統制で確かめる場合もある）	なし	記載省略	他

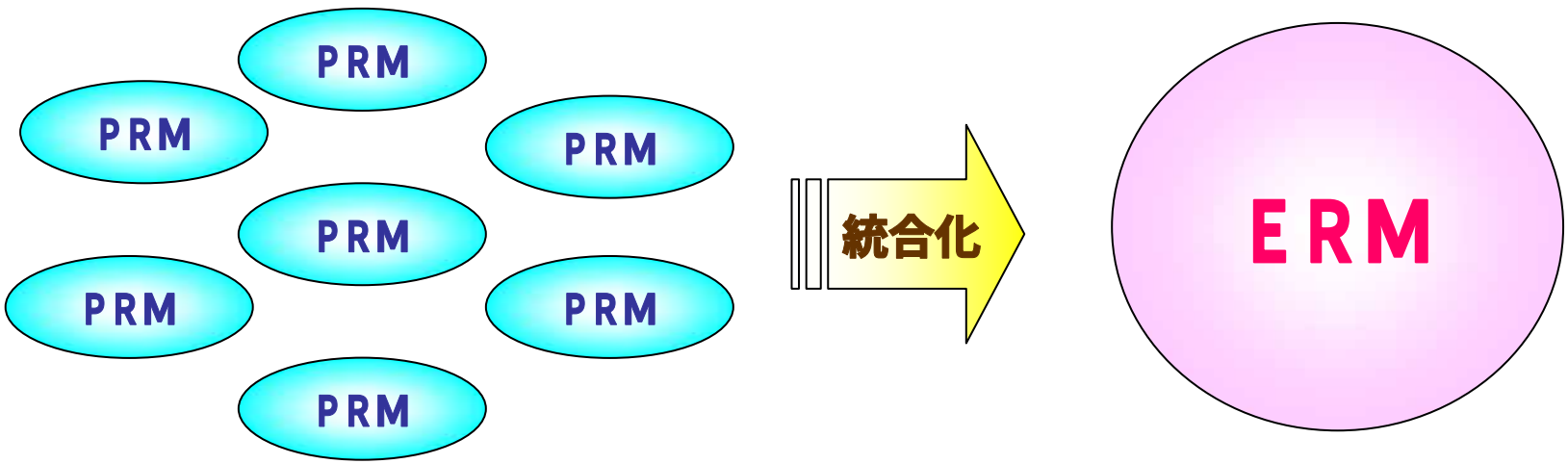
社員一人ひとりからの内部統制システムの整備

■「トップマネジメント」としての内部統制システム整備の重要性

■内部統制事故＝たった一人の職員の「0のかけ算」

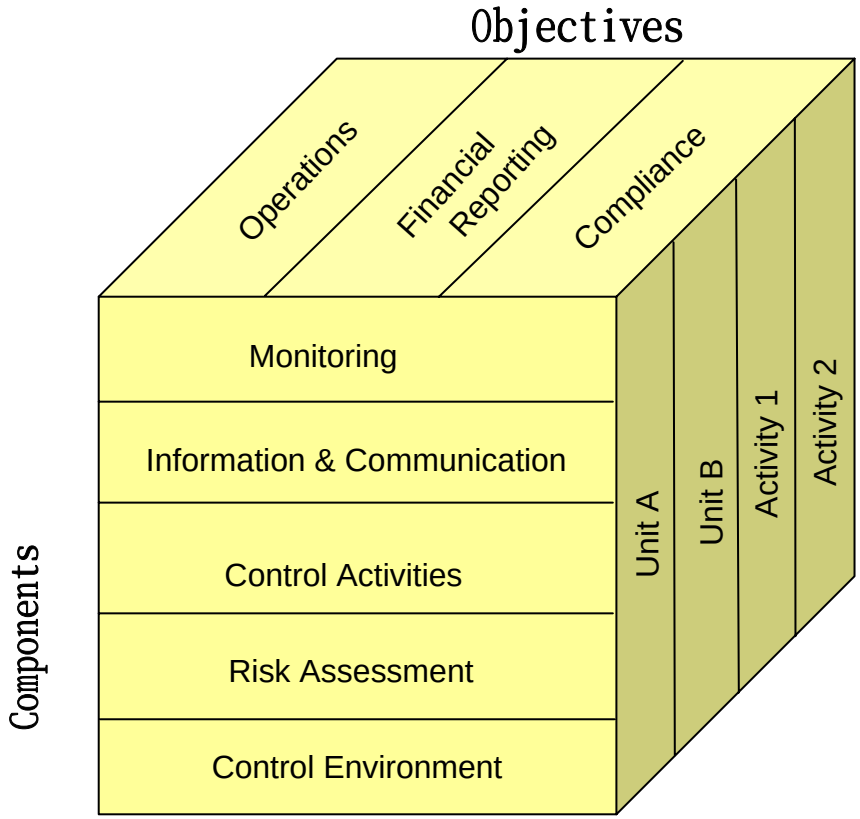
■「社員一人ひとりからの内部統制システム整備への取り組み」が重要

PRM(ﾊﾟｰｿﾅﾙﾘｽｸﾏﾈｼﾞﾒﾝﾄ)からERM(ｴﾝﾀｰﾌﾟﾗｲｽﾞﾘｽｸﾏﾈｼﾞﾒﾝﾄ)へ



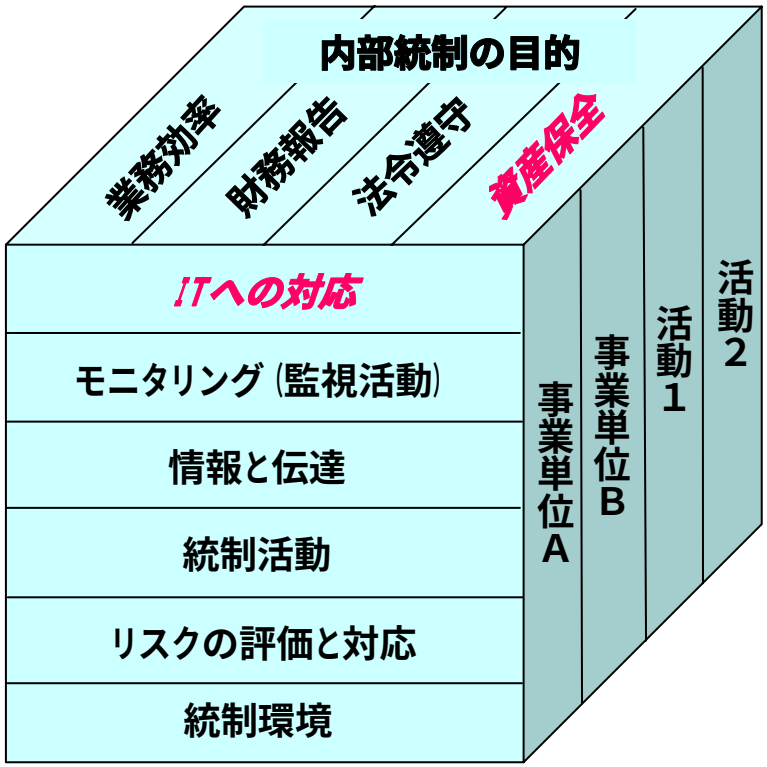
内部統制のフレームワーク

COSO1992フレームワーク



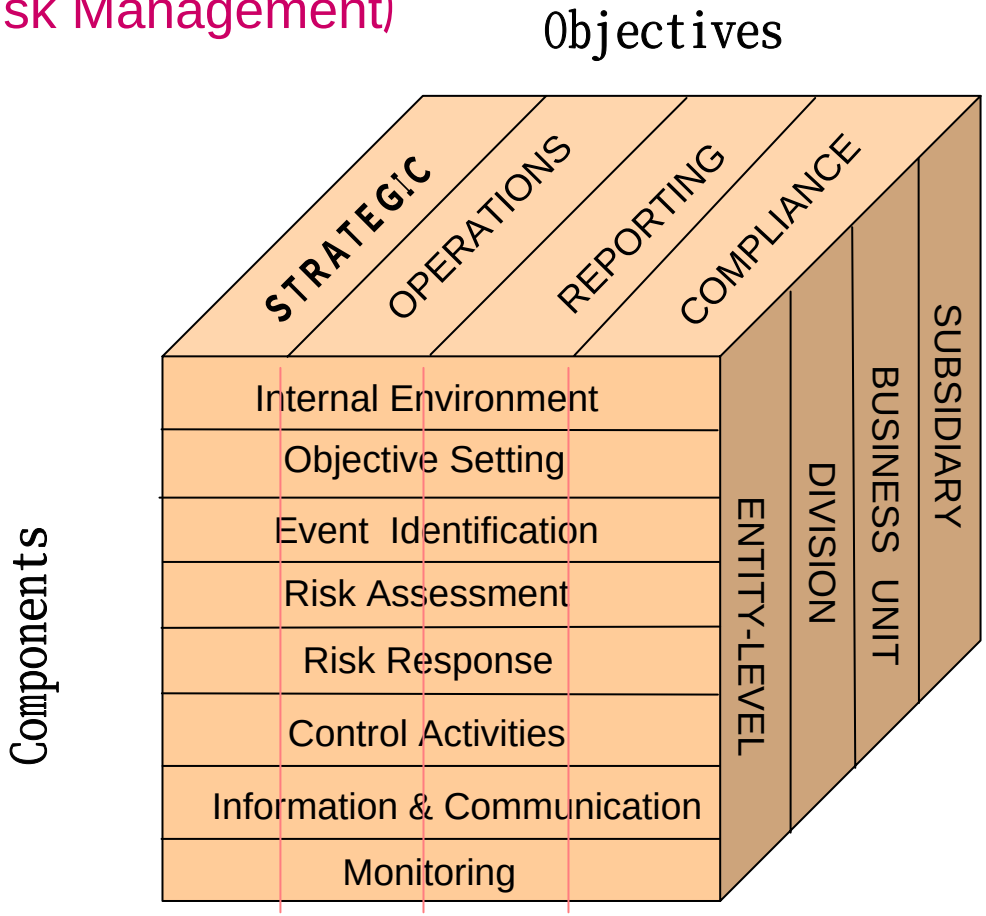
内部統制の基本要素

日本「基準案」フレームワーク



内部統制のフレームワーク

COSO２００４フレームワーク
(Enterprise Risk Management)



フレームワークの差違

COSO1992	CSO2004 (ERM)	基準案
☐Objectives		
・Operations ・Financial Reporting ・Compliance	・STRATEGIC ・OPERATIONS ・REPORTING ・COMPLIANCE	・業務効率 ・法令遵守 ・財務報告 ・*資産保全*
☐ Components		
・Monitoring ・Information & Communication ・Control Activities ・Risk Assessment ・Control Environment	・Internal Environment ・Objective Setting ・Event Identification ・Risk Assessment ・Risk Response ・Control Activities ・Information & Communication ・Monitoring	・*ITへの対応* ・モニタリング（監視活動） ・情報と伝達 ・統制活動 ・リスクの評価と対応 ・統制環境

フレームワークの差違

- 「Risk assessment」→「Control Activities」
- 「Risk assessment」→「Risk response」
  cf.「Control Activities」？
- 「リスクの評価と対応」cf.「統制活動」
- 「Strategic」ー「Objective Setting」
  ／「Event Identification」
- 「Operating」cf.「業務効率」　cf.「有効性」
- 「Reporting」cf.「財務報告」

「内部統制とIT」の2局面

2局面の共有化による効率化

①「内部統制システム整備のためのIT活用」と
②「IT活用業務に対する内部統制システム適合化」

①重要な勘定科目に関する全業務プロセスについて内部統制システム監査のための「文書化」におけるIT活用【所管：管理部門】

A.「内部統制マトリックス」
＝「現行業務フロー図
＋【リスク評価＋リスク対応】」

無関係・断絶

■「問題点」＝「あるべき姿」と「現状」との「ギャップ」
■「あるべき姿」＝「内部統制の4つの目的」

共有化

共有化

② IT活用業務についてのシステム開発における内部統制システムへの適合化
【所管：IT企画部門】

B.「機能差報告書」
＝「現行業務フロー図＋【問題点】」
＋「新業務フロー図＋【改善策】」