Deloitte.

DB セキュリティからみた内部統制報告制度について

2008年02月05日

監査法人トーマツ
公認会計士
丸山満彦

トーマツ

要旨

- 内部統制報告制度が平成20年4月1日開始事業年度から、上場企業に適用される。

- そこで、内部統制や内部統制報告制度の要点を説明し、内部統制報告制度で重要な一部となるIT統制、とりわけデータに対するアクセス管理のポイントを説明する。

- 最後に、制度対応後に重要となってくる管理と評価の効率化について説明をする。

アジェンダ

1．内部統制って？

2． 内部統制評価制度の概要

3．IT全般統制（会計データの保護が重要）

4．今後の課題（自動化による評価の効率化）

Deloitte.

1．内部統制って？

トーマツ

内部統制の基本

内　部　統　制

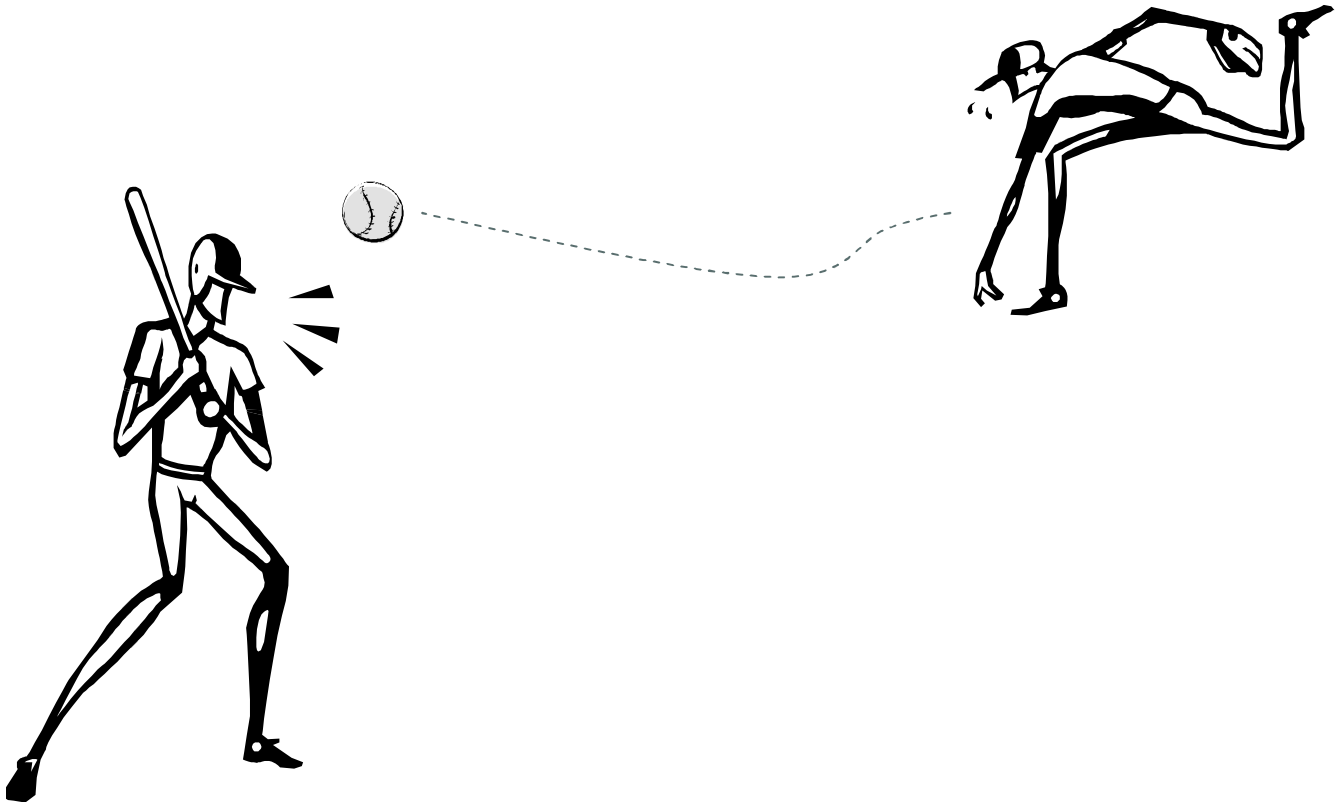
内　部	**組織内部による自主的なもの**

⇔　**外部＝組織外部（ex.行政機関）による強制的なもの**

統　制	**コントロール＝目標達成を支援するプロセス**

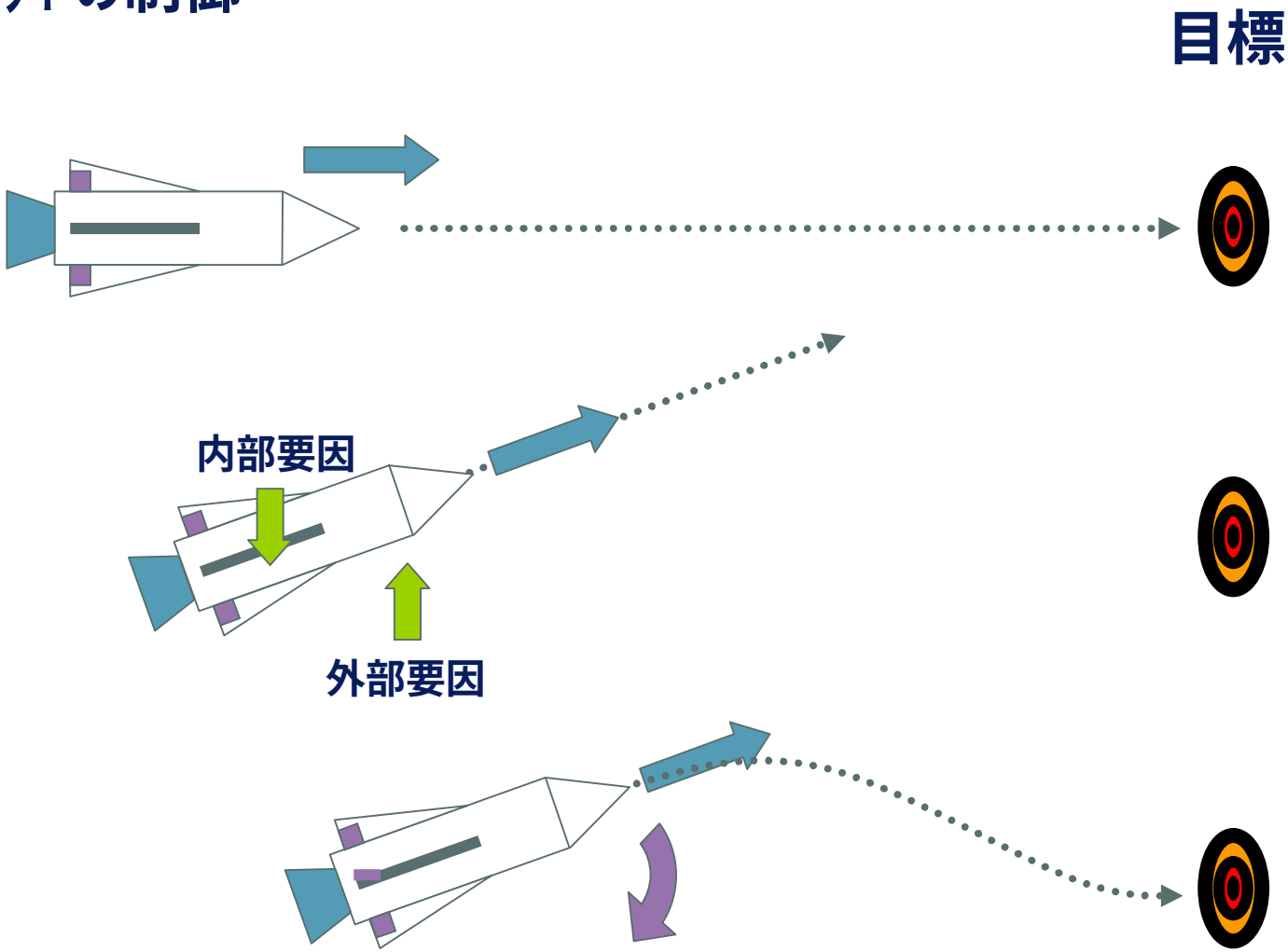
日常生活の中の統制

- 今日の松坂のコントロールは悪かったな。。。

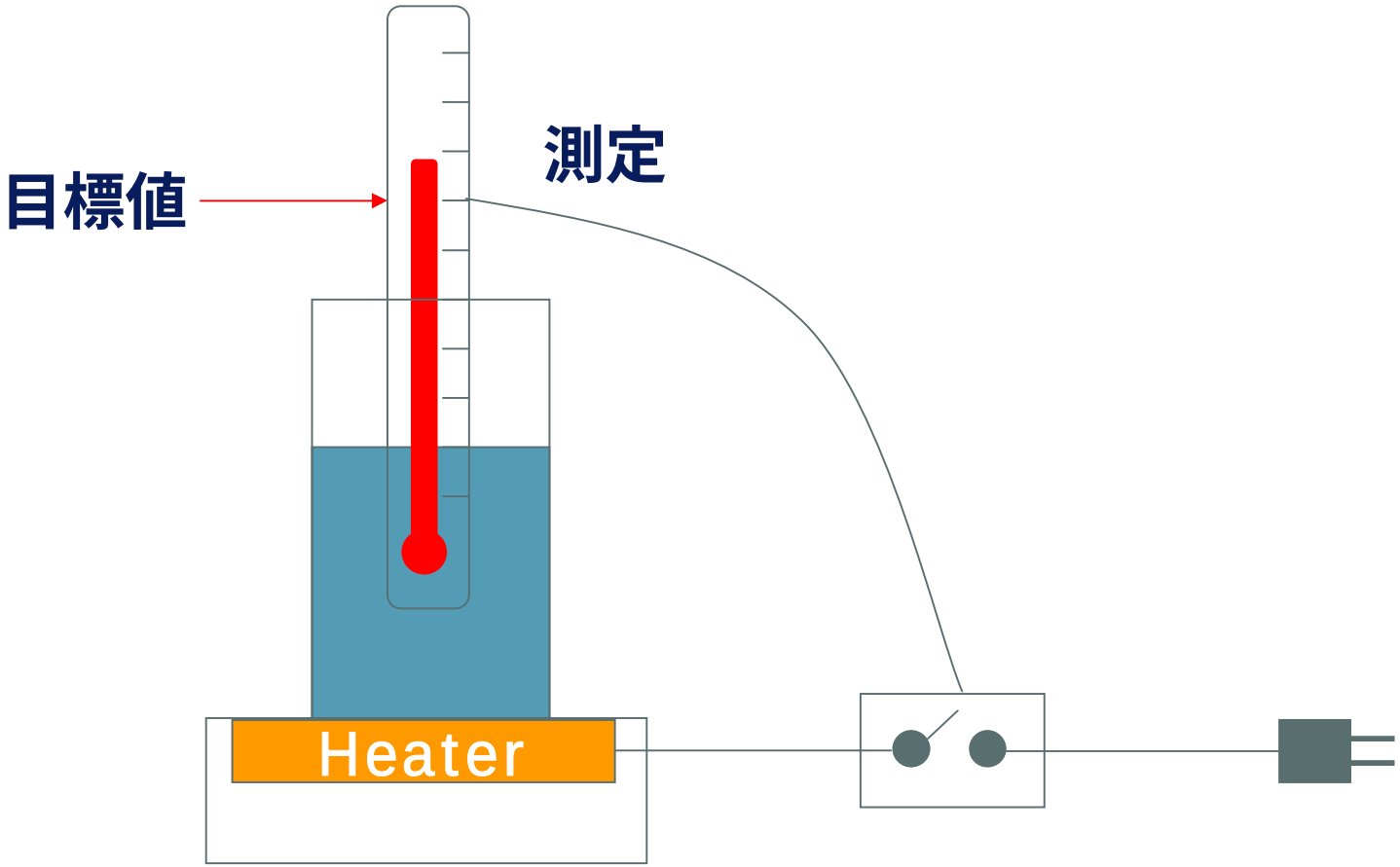


工学の世界の統制 (1)

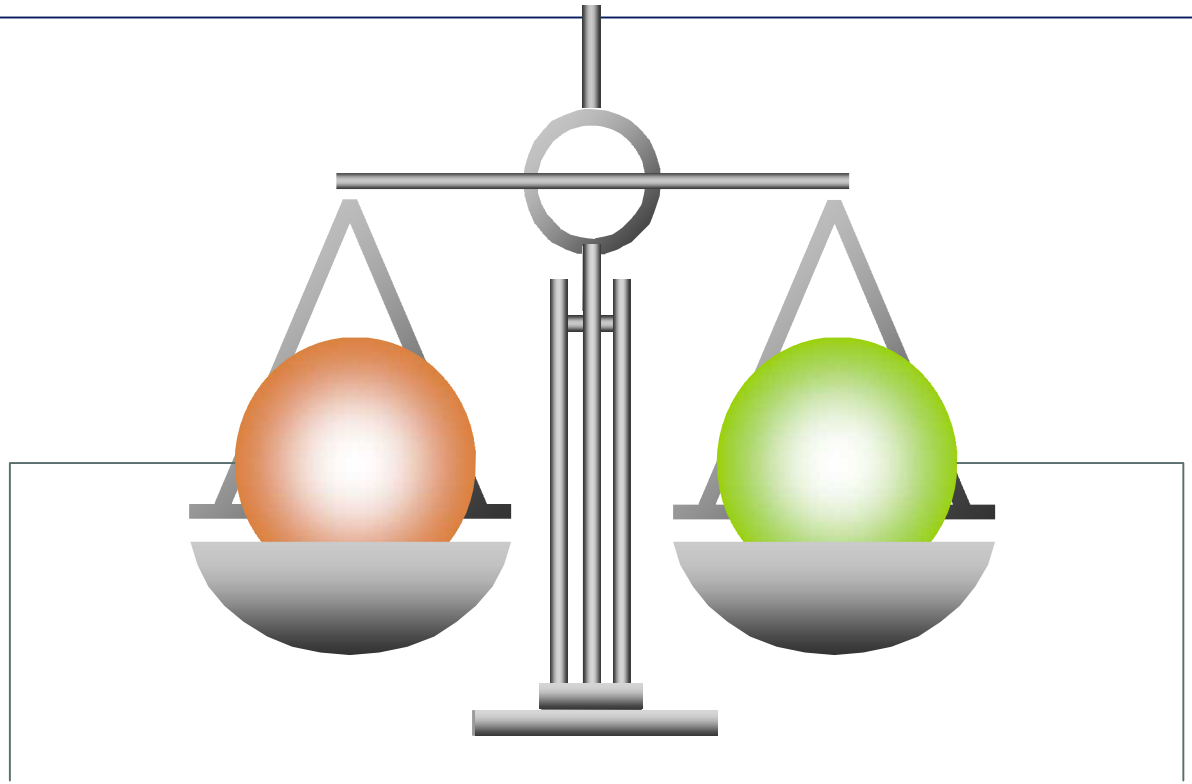
- ロケットの制御



工学の世界の統制 (2)



目標達成って・・・



- 業務の有効性及び効率性

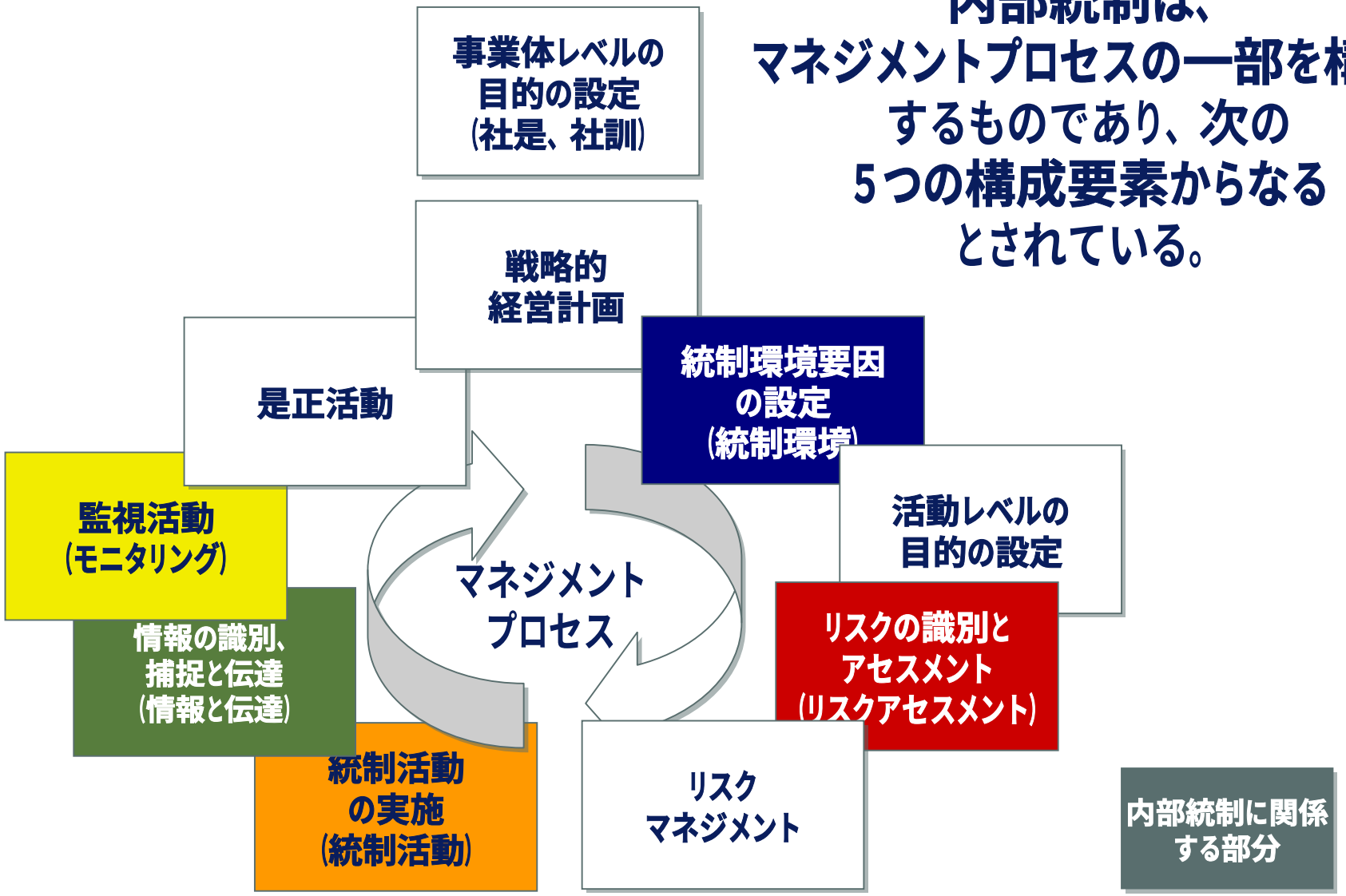
内部統制

- 財務報告の信頼性
- 事業活動に関わる法令等の遵守

ちゃんと金儲けをしましょう
利害関係者には説明責任を果たしましょう
法律は守りましょう

内部統制は何からなるか？？？

内部統制は、マネジメントプロセスの一部を構成するものであり、次の5つの構成要素からなるとされている。



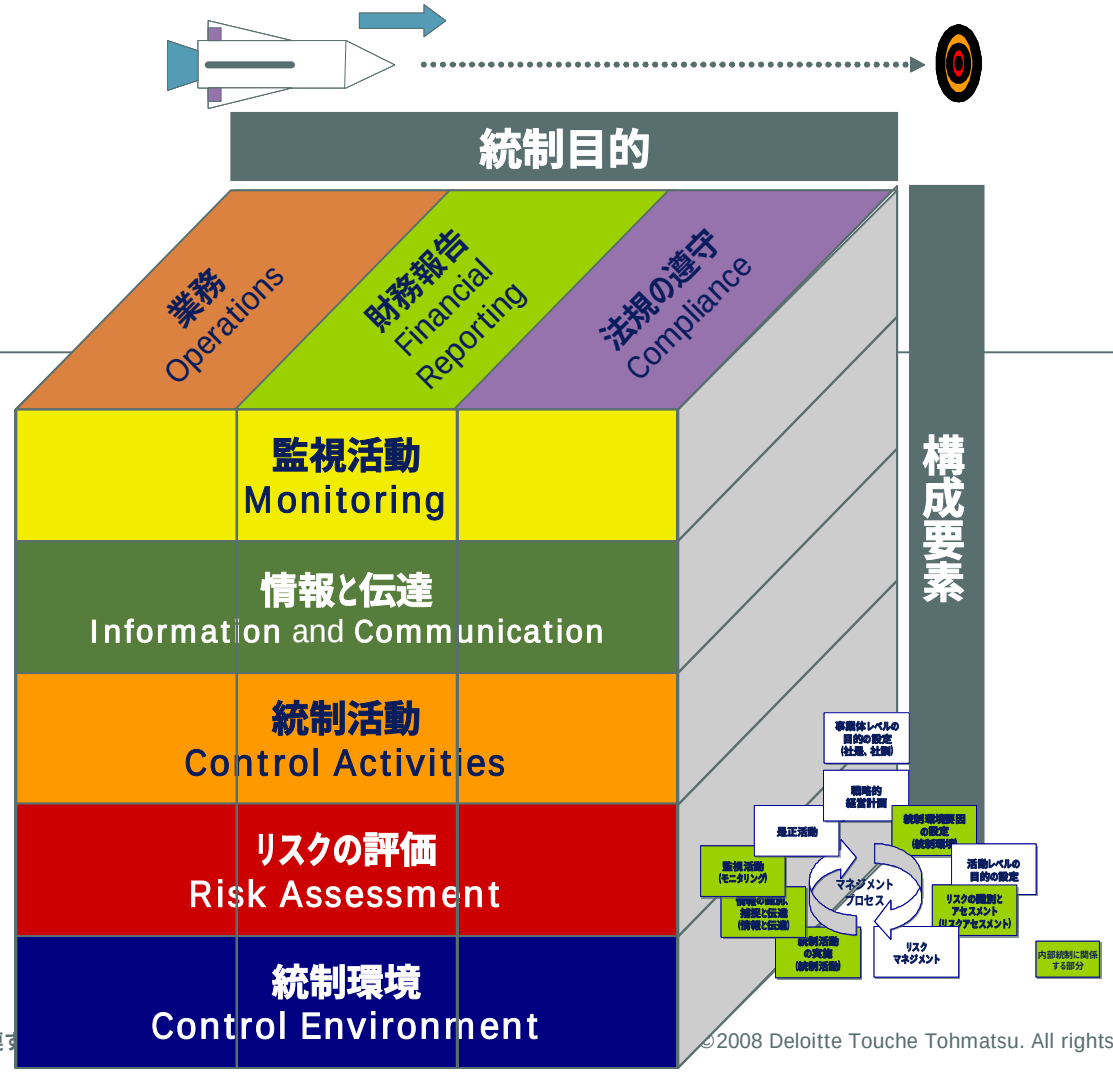
5つの構成要素の内容

統制環境	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、他の構成要素の基礎となるもの。
リスクの評価と対応	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、分析及び評価し、当該リスクへの適切な対応を行う一連のプロセス 。
統制活動	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 。
情報と伝達	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 。
モニタリング	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 。

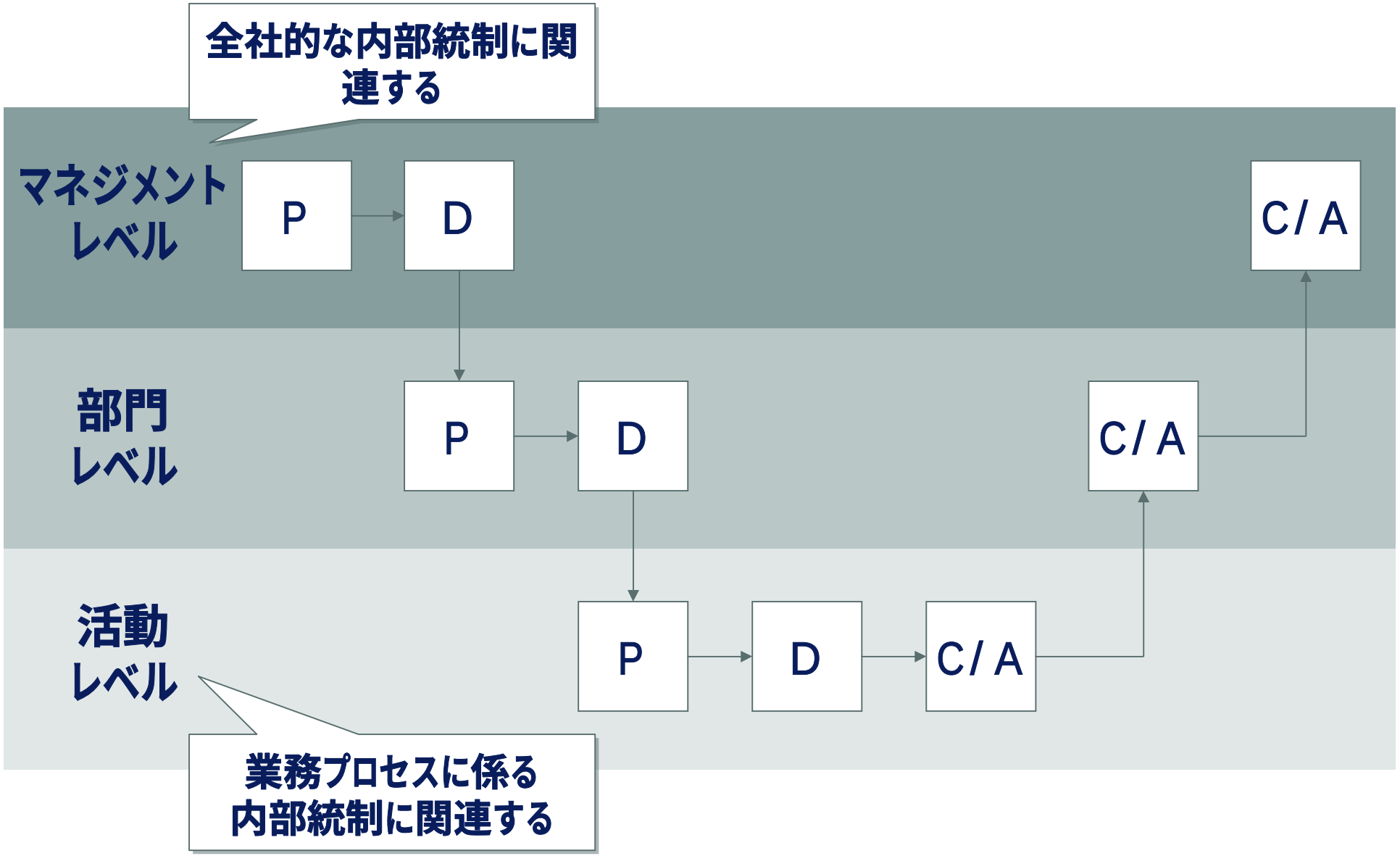
って結局内部統制とは・・・(COSOの内部統制の定義)

内部統制とは、以下の範疇に分けられる目的の達成に関して合理的な保証を提供することを意図した、事業体の取締役会、経営者およびその他の構成員によって遂行される一つのプロセスである。

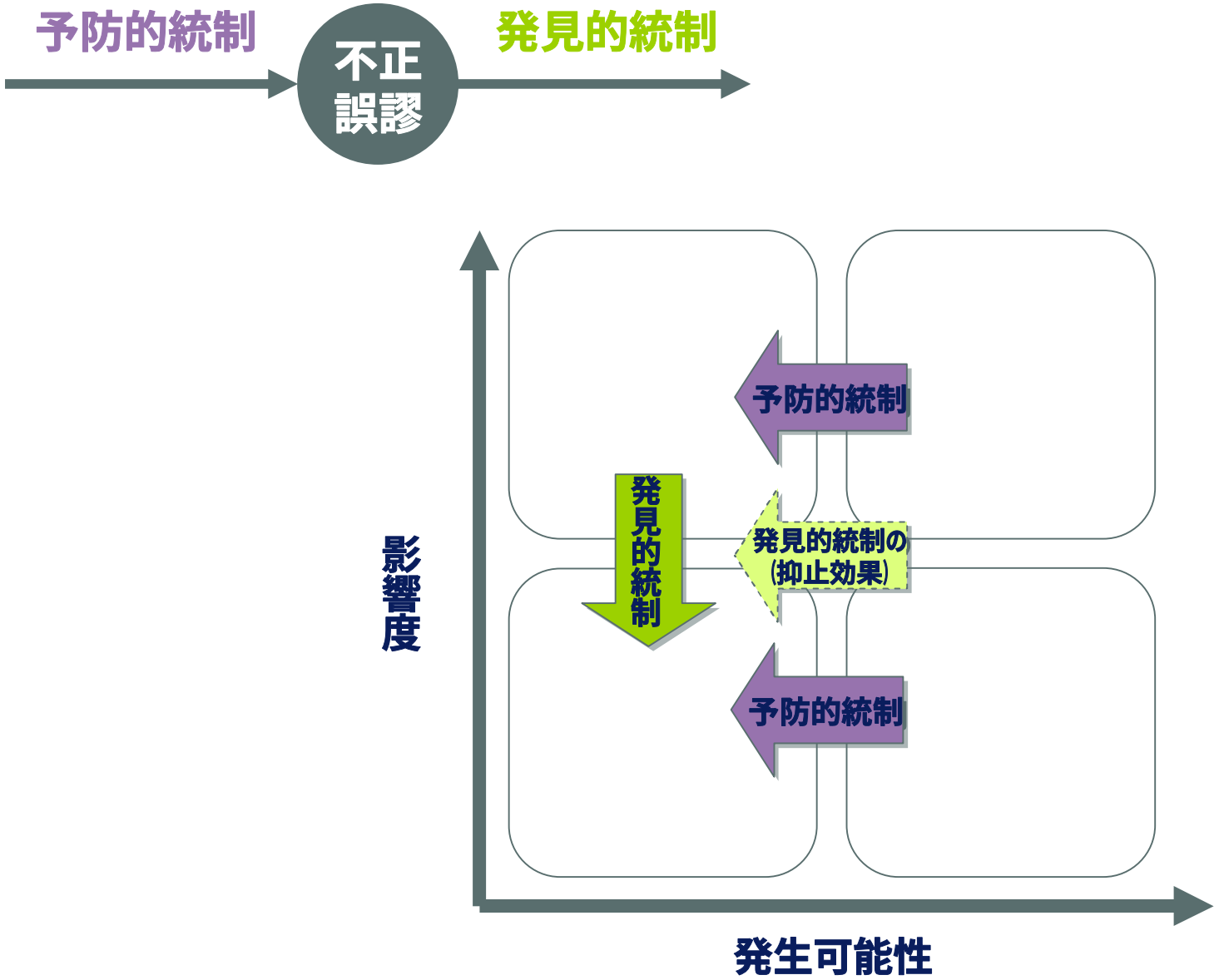
- 業務の有効性と効率性
- 財務報告の信頼性
- 関連法規の遵守



マネジメントレベル～活動レベルのリスクマネジメントPDCA



予防的統制と発見的統制



Deloitte.

2．内部統制評価制度とIT統制

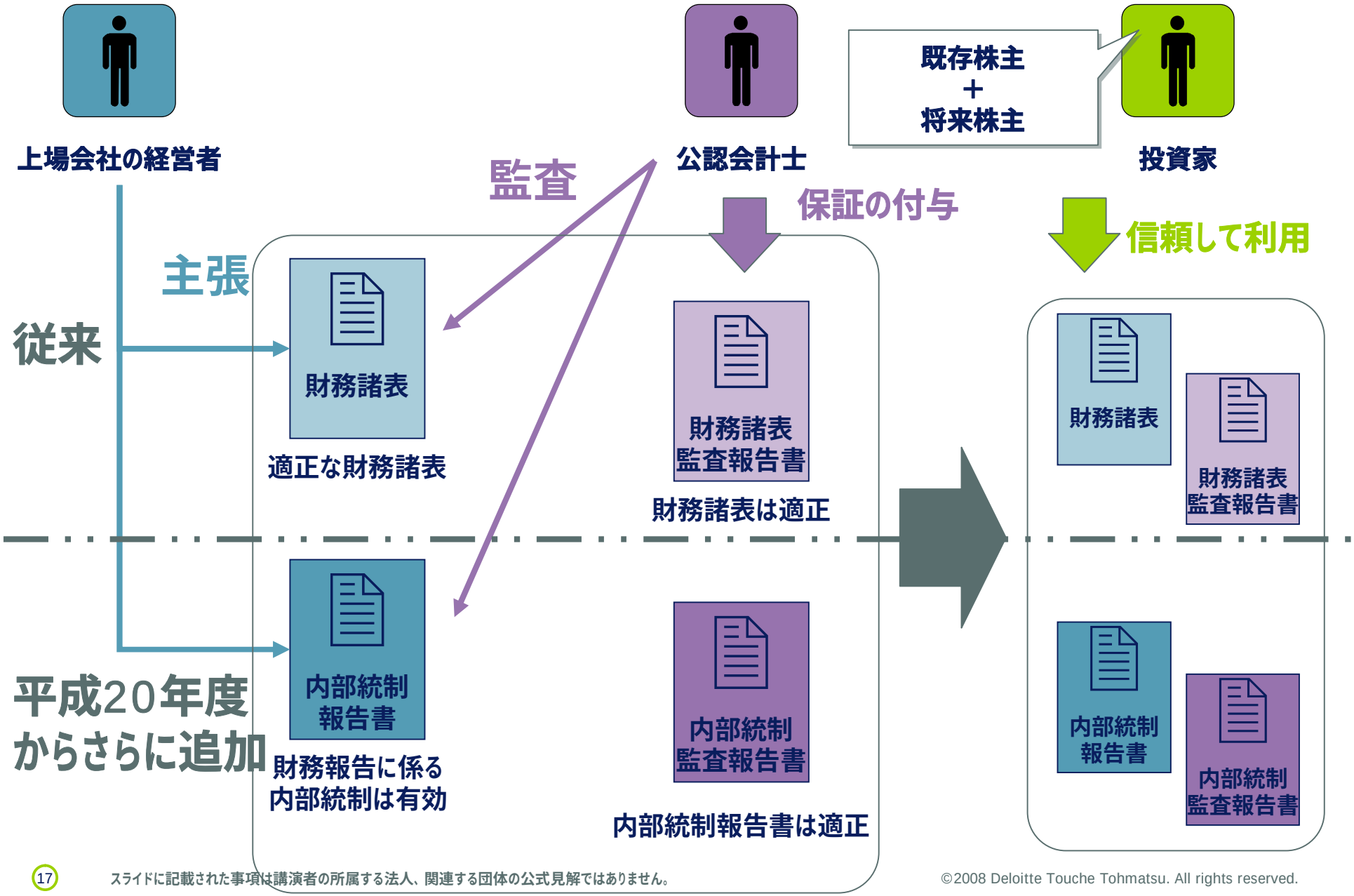
トーマツ

J-SOXってなんだ・・・

- J-SOX法という法律はない。。。
- SOX法404条に類似した制度を日本に導入したことから、J-SOXといわれている。

- 日本では、金融商品取引法
  - 第24条の4の4　　財務報告に係る内部統制の経営者評価と報告（内部統制報告書の提出）
  - 第193条の2第2項　　内部統制報告書の監査

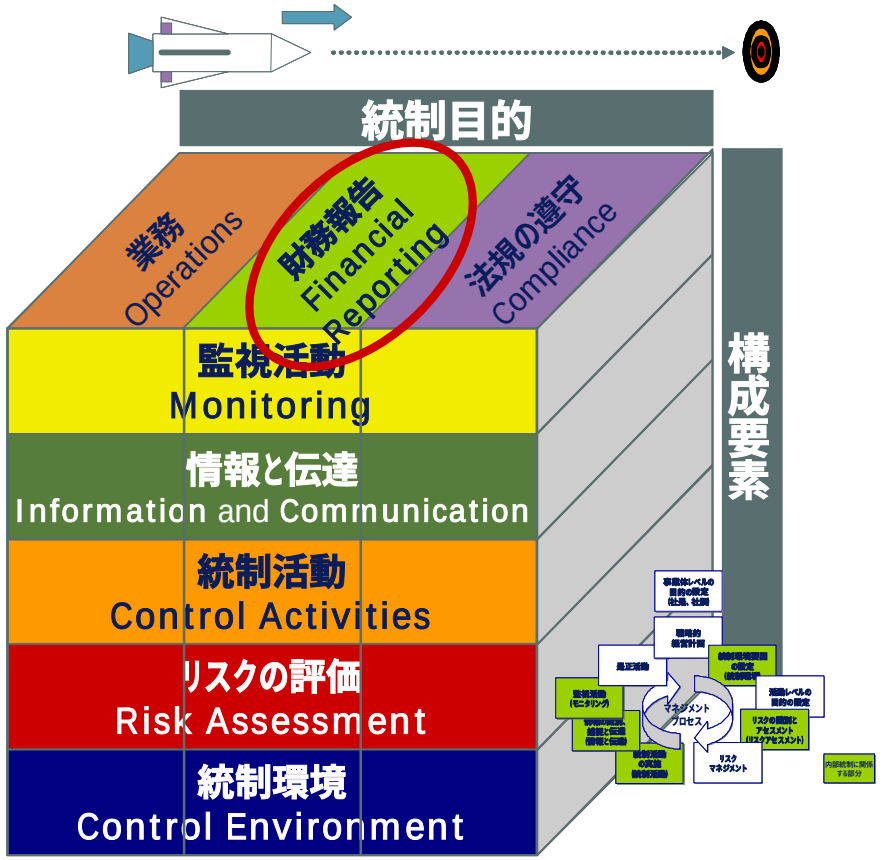
金融商品取引法第24条4の4と第193条の2第2項による制度の概要



内部統制評価制度

財務報告の信頼性のみ

- ポイント
  - 財務報告の信頼性のみ
  - 法律上は評価をして内部統制報告書を提出することが義務付けられている
  - 従って、内部統制が有効でなくても法律違反とはならない
  - ただし、内部統制が有効でないのに有効であると報告すれば、虚偽報告で刑事罰の対象となる
  - 評価するためにはルール（基準及び実施基準）がある



それを評価するためのルールとしての基準及び実施基準

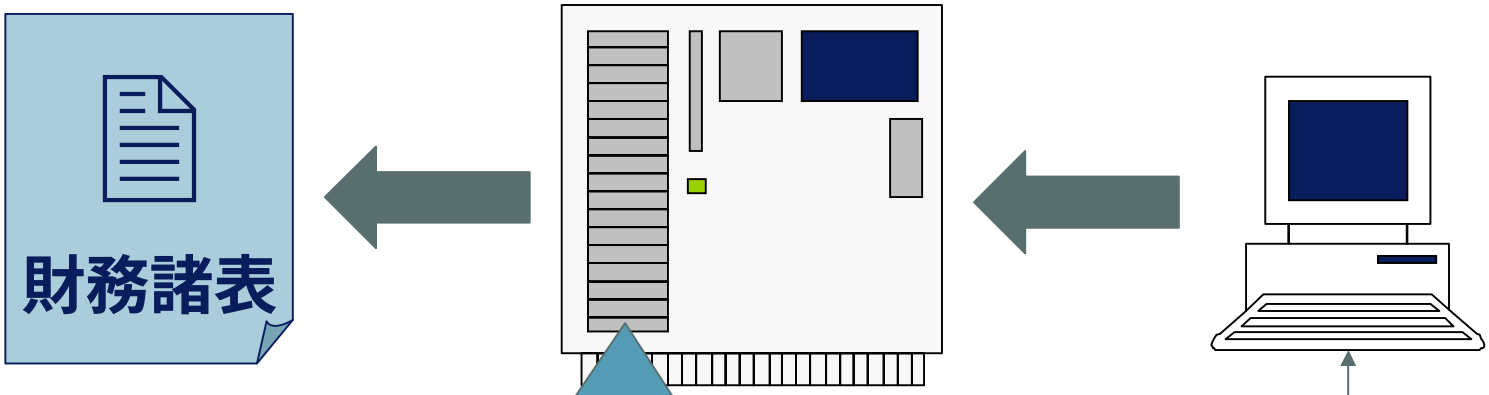
	内部統制部会	実施基準
	前　文	
内部統制を理解するための概念	Ⅰ．内部統制の基本的枠組み 1. 内部統制の定義 2. 内部統制の基本的要素 3. 内部統制の限界 4. 内部統制に関係を有する者の役割と責任	Ⅰ．内部統制の基本的枠組み 1. 内部統制の定義（目的） 2. 内部統制の基本的要素 3. 内部統制の限界 4. 内部統制に関係を有する者の役割と責任 **5. 財務報告に係る内部統制の構築**
経営者による評価基準	Ⅱ．財務報告に係る内部統制の評価及び報告 1. 財務報告に係る内部統制の評価の意義 2. 財務報告に係る内部統制の評価とその範囲 3. 財務報告に係る内部統制の評価の方法 **4. 財務報告に係る内部統制の報告**	Ⅱ．財務報告に係る内部統制の評価及び報告 1. 財務報告に係る内部統制の評価の意義 2. 財務報告に係る内部統制の評価とその範囲 3. 財務報告に係る内部統制の評価の方法
外部監査人による監査基準	Ⅲ．財務報告に係る内部統制の監査 1. 財務諸表監査の監査人による内部統制監査の目的 2. 内部統制監査と財務諸表監査の関係 3. 内部統制監査の実施 4. 監査人の報告	Ⅲ．財務報告に係る内部統制の監査 1. 内部統制監査の目的 2. 内部統制監査と財務諸表監査の関係 **3. 監査計画と評価範囲の検討** 4. 内部統制監査の実施 5. 監査人の報告

Deloitte.

3．IT全般統制（会計データの保護が重要）

トーマツ

IT統制がなぜ財務報告に係る内部統制に関係するのか？



IT業務処理統制

コンピュータ上で会計処理漏わがないかなどのチェック

伝票

受注書

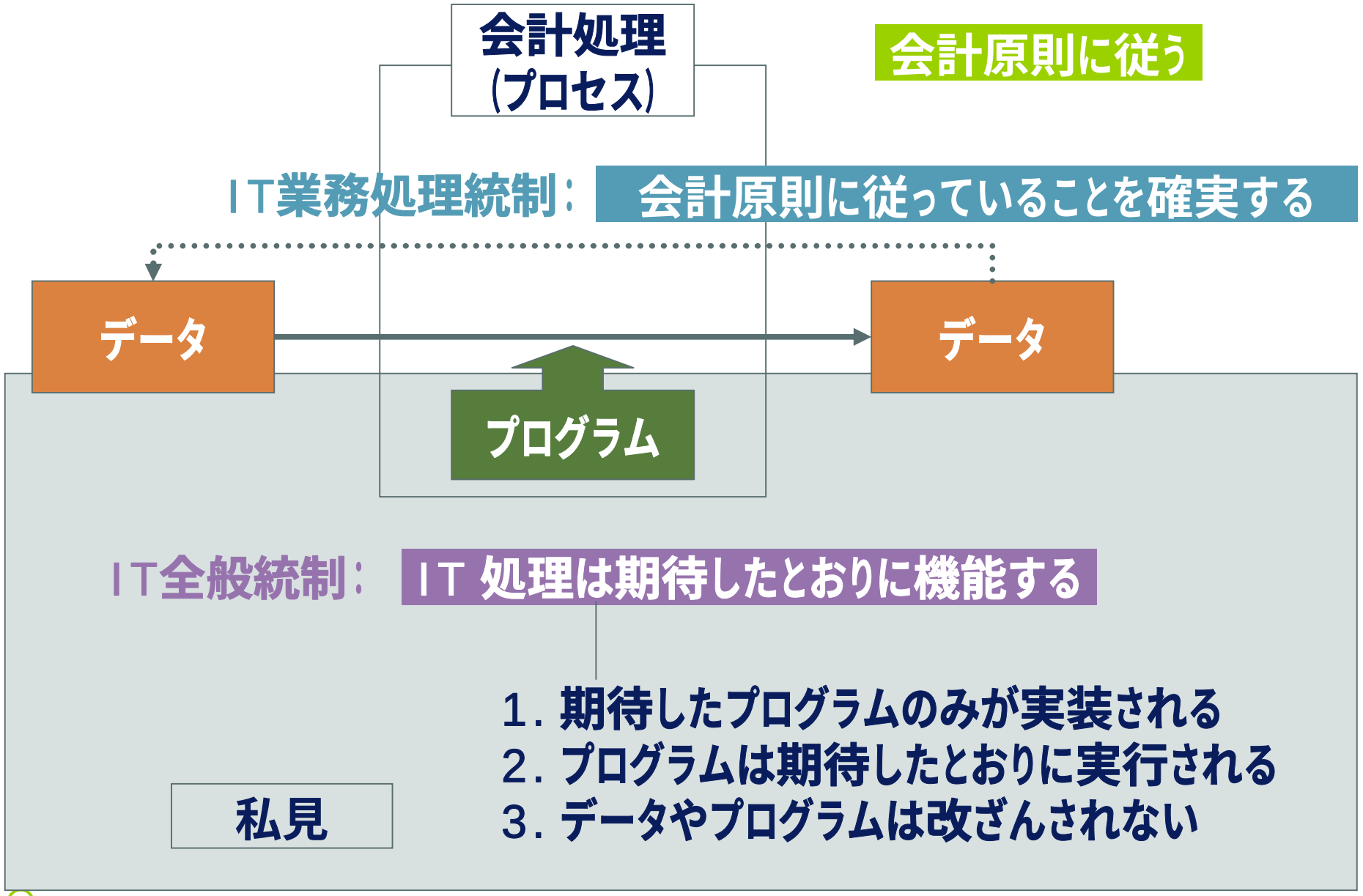
会計システムが信頼できないと財務諸表も信頼できない。

IT全般統制

会計システムの信頼性を保証

スライドに記載された事

IT業務処理統制とIT全般統制の関係



IT全般統制の評価項目

監査人の実施基準の中で、経営者も留意すべきIT全般統制の評価項目の例示が示されている。

(Ⅲ. 4. (2) ② ロ)

a.	システムの開発、変更・保守	監査人は、企業が財務報告に関連して、新たにシステム、ソフトウェアを開発、調達又は変更する場合、**承認**及び**導入前の試験**が適切に行われているか確認する。
b.	システムの運用・管理	監査人は、財務報告に係るシステムの**運用・管理**の有効性を確認する。
c.	システムの安全性の確保	監査人は、企業がデータ、システム、ソフトウェア等の不正使用、改竄、破壊等を防止するために、財務報告に係る内部統制に関連するシステム、ソフトウェア等について、適切な**アクセス管理**等の方針を定めているか確認する。
d.	外部委託に関する契約の管理	企業が財務報告に関連して、ITに係る業務を外部委託している場合、監査人は、企業が適切に**外部委託に関する契約の管理**を行っているか検討する。

太字は私がつけました。

IT全般統制の評価項目

監査人の実施基準の中で、経営者も留意すべきIT全般統制の評価項目の例示が示されている。

(Ⅲ. 4. (2) ② ロ)

a. システムの開発、変更・保守

監査人は、企業が財務報告に関連して、新たにシステム、ソフトウェアを開発、調達又は変更する場合、**承認**及び**導入前の試験**が適切に行われているか確認する。 その際、監査人は、例えば、以下の点に留意する。

- システム、ソフトウェアの開発、調達又は変更について、事前に経営者又は適切な管理者に**所定の承認**を得ていること
- 開発目的に適合した適切な**開発手法**がシステム、ソフトウェアの開発、調達又は変更に際して、適用されていること
- 新たなシステム、ソフトウェアの導入に当たり十分な**試験**が行われ、その結果が当該システム、ソフトウェアを**利用する部門の適切な管理者**及び**IT部門の適切な管理者により承認**されていること
- 新たなシステム、ソフトウェアの**開発、調達又は変更**について、その**過程が適切に記録及び保存**されるとともに、変更の場合には、変更前のシステム、ソフトウェアに関する内部統制の整備状況に係る記録が更新されていること
- 新たなシステム、ソフトウェアにデータを**保管又は移行**する場合に、**誤謬、不正等を防止する対策**が取られていること
- 新たなシステム、ソフトウェアを利用するに当たって、利用者たる従業員が適切な計画に基づき、**教育研修**を受けていること

太字は私がつけました。

IT全般統制の評価項目

b. システムの運用・管理

監査人は、財務報告に係るシステムの**運用・管理**の有効性を確認する。その際、例えば、以下の点に留意する。

- システムを構成する重要なデータやソフトウェアについて、障害や故障等によるデータ消失等に備え、その内容を**保存し、迅速な復旧**を図るための対策が取られていること
- システム、ソフトウェアに障害や故障等が発生した場合、**障害や故障等の状況の把握、分析、解決等**の対応が適切に行われていること

c. システムの安全性の確保

監査人は、企業がデータ、システム、ソフトウェア等の不正使用、改竄、破壊等を防止するために、財務報告に係る内部統制に関連するシステム、ソフトウェア等について、**適切なアクセス管理等の方針**を定めているか確認する。

d. 外部委託に関する契約の管理

企業が財務報告に関連して、ITに係る業務を外部委託している場合、監査人は、企業が適切に**外部委託に関する契約の管理**を行っているか検討する。

太字は私がつけました。

（パッケージ・ソフトウェアをそのまま利用するような比較的簡易なシステムを有する企業の場合）
ITに係る全般統制に重点を置く必要があることに留意する。

「IT全般統制に重点を置く」という趣旨が不明だが、パッケージについては個別の機能検証等（IT業務処理統制）まで踏み込まなくても、IT全般統制が有効であれば十分ということか？

IT全般統制の不備が重大な欠陥となった事例

- USSOXの場合は、IT全般統制（会計データに対するアクセス権が不十分）の不備が重大な欠陥となった事例がある。

2005年3月31日時点で、同社は会計に関連するアプリケーションプログラムとデータに対する有効なコントロールを維持していなかった。

特に、特定の何名かは他者が代行できない業務を行っており、その職務上の責任に必要な権限を越えて、会計関係のアプリケーションプログラムとデータに**無制限のアクセス権**を与えられていた。さらに、ユーザが不適切なプログラムの使用及びデータのアクセスを行っていないことを**モニタリング**する有効なコントロールもなかった。

これらの不備が北米、ヨーロッパおよびアジアのいくつかのシステムとプロセス（現金、売掛金、固定資産、その他の資産、買掛金、未払費用、給与勘定、在庫及び関連損益計算書勘定を含む）に存在した。

この**統制の不備は、同社の連結財務諸表の記載ミスを引き起こしているわけではなかったが、年次および四半期の財務諸表に、防止又は発見されない重要な記載ミスにつながる可能性のあるものである。**したがって、同社のマネジメントは、この統制上の不備は重要な欠陥を構成すると判断した。

AVX社の2005年Form10kの経営者による内部統制報告書及び監査報告書の重要な欠陥についての記載内容を仮訳した。

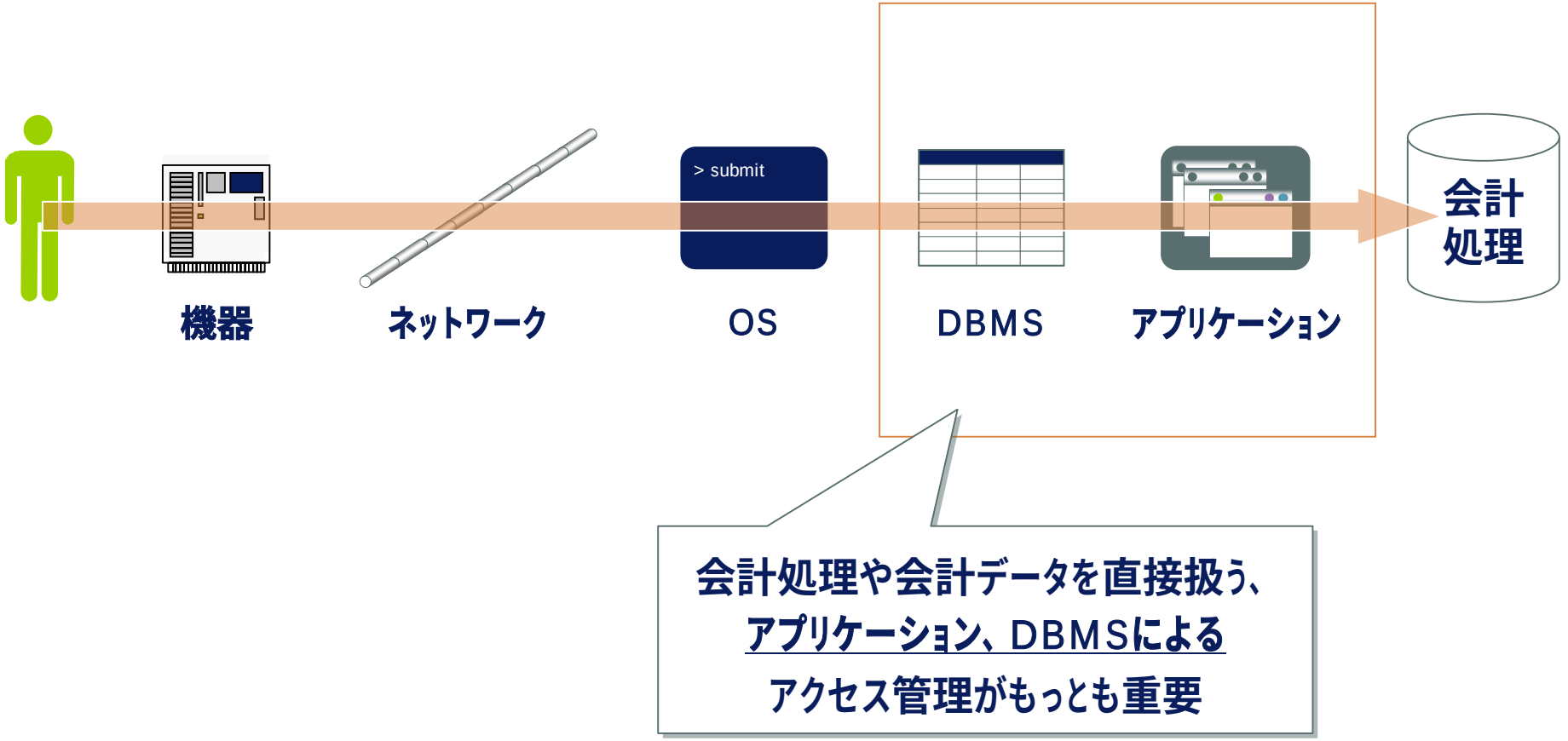
予防的統制と発見的統制のどちらかは最低必要

重要な記載誤りにつながる「可能性」が高ければ、実際に記載誤りがなくても重要な欠陥となり、非有効意見となる。

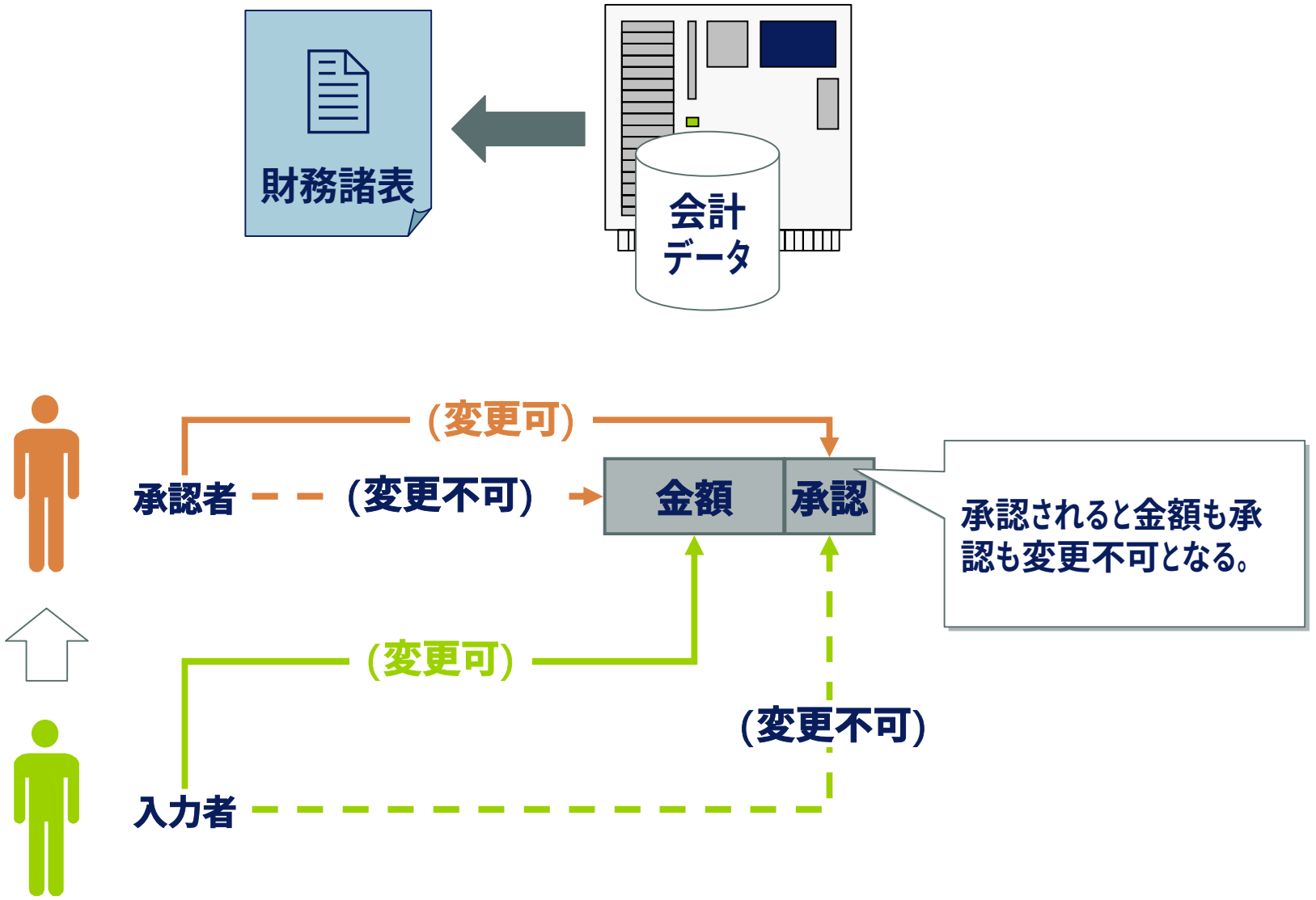
ITに係る全般統制の不備は、財務報告の重要な事項に虚偽記載が発生するリスクに直接に繋がるものではないため、**直ちに重要な欠陥と評価されるものではない。**
しかし、ITに係る全般統制に不備があった場合には、たとえITに係る業務処理統制が有効に機能するように整備されていたとしても、その有効な運用を継続的に維持することができない可能性があり、**虚偽記載が発生するリスクが高まる**こととなる。

⑦ http://library.corporate-ir.net/library/10/101/101602/items/156400/AVX10K2005.pdf

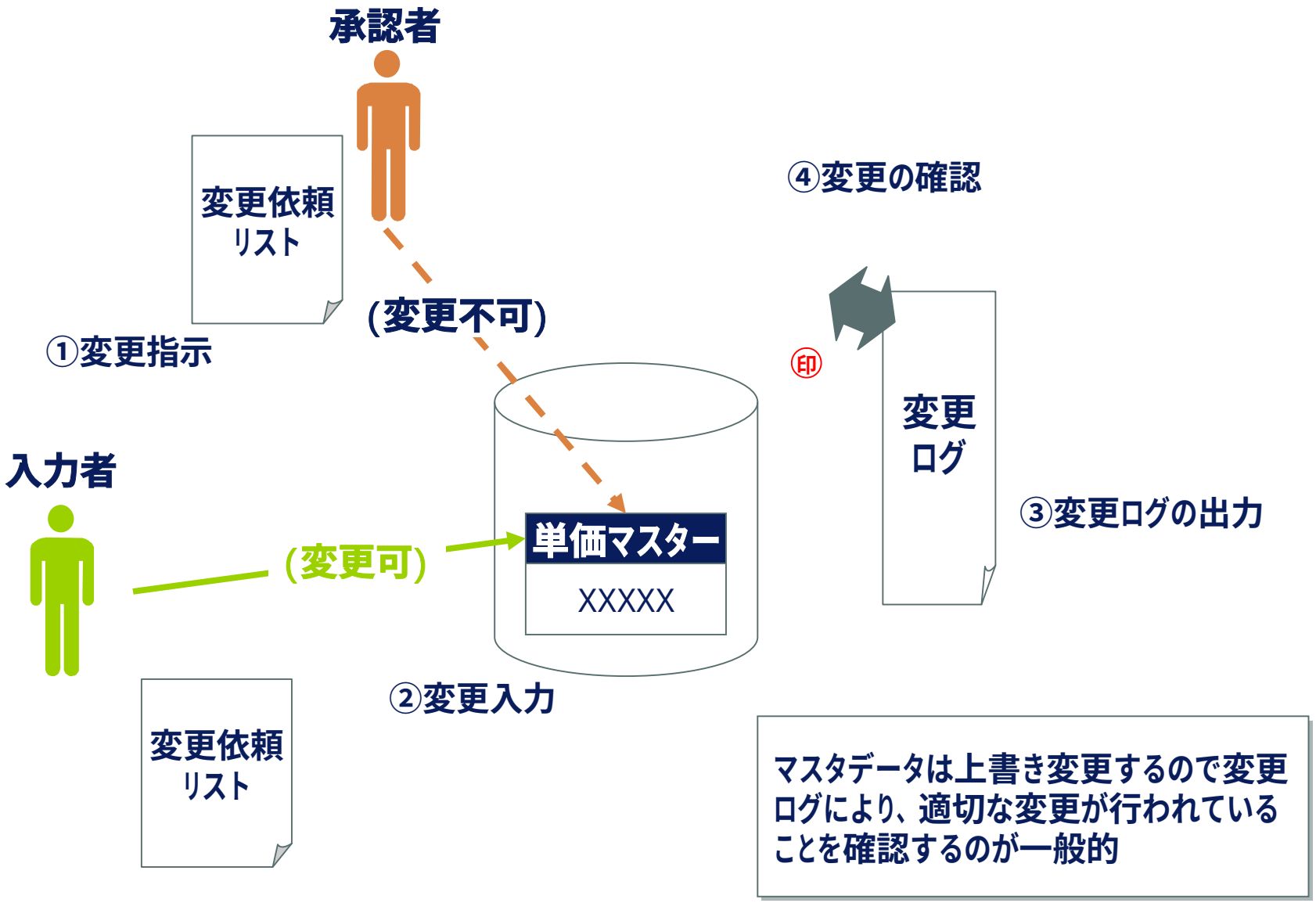
財務報告とアクセス管理



会計データ（トランザクションデータ）のアクセス管理



マスタデータのアクセス管理

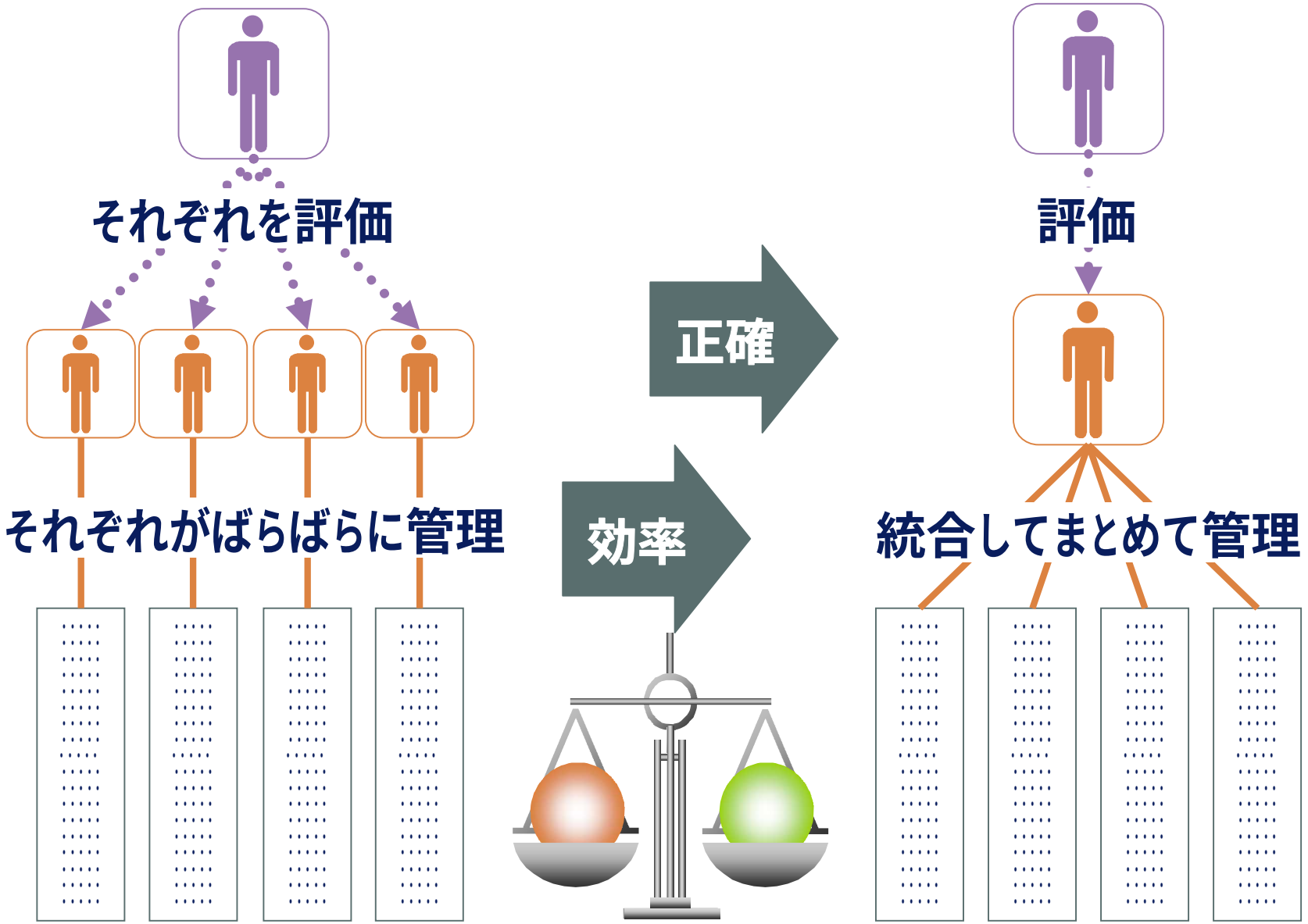


Deloitte.

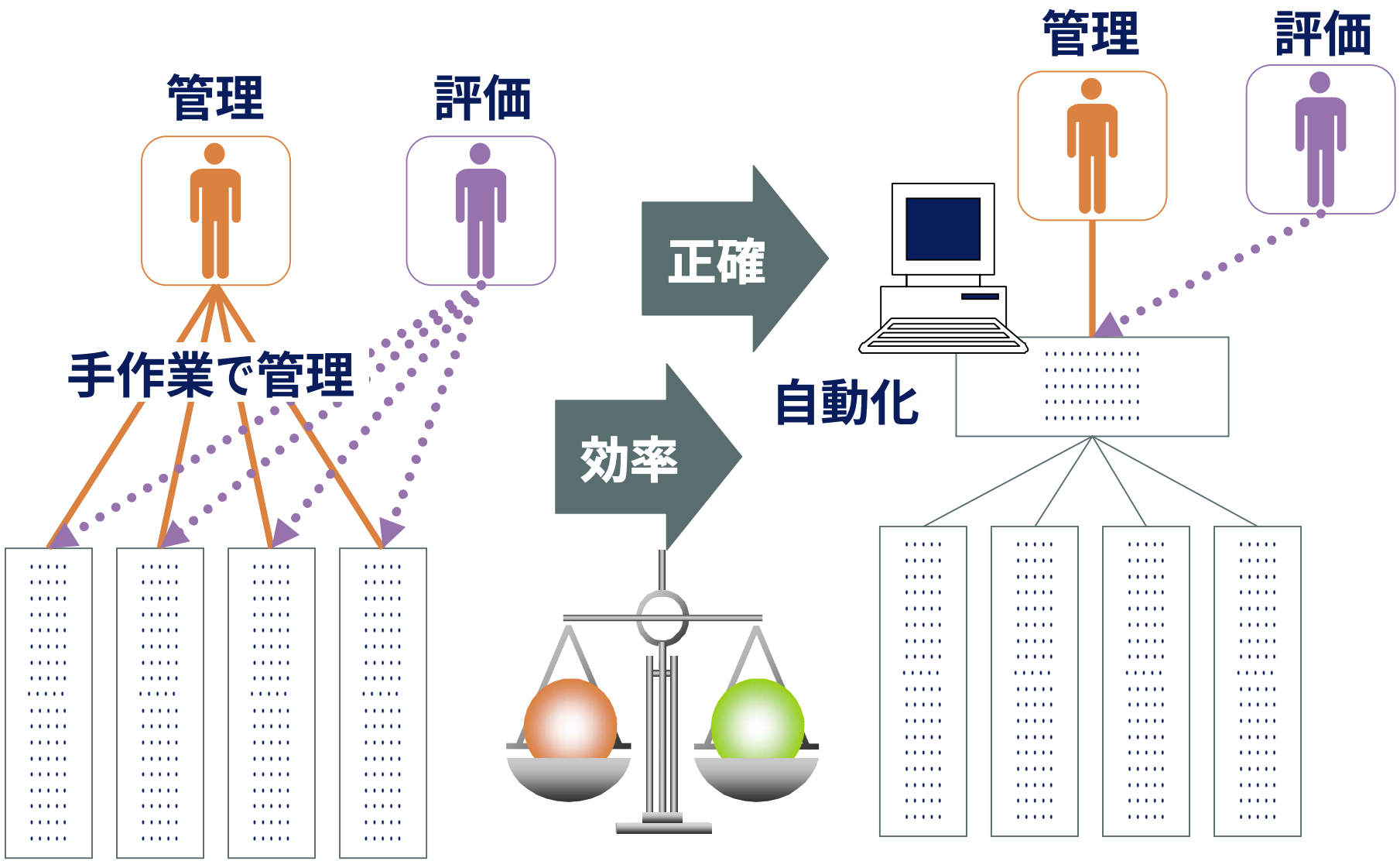
4．今後の課題
（自動化による管理と評価の効率化）

トーマツ

統合による効率的な管理と評価



自動化による効率的な管理と評価



Deloitte.

さいごに・・・

トーマツ

DBセキュリティからみた内部統制報告制度

- 内部統制は、目標達成を支援する手段
- 内部統制報告制度では、IT全般統制も重要である。
- 会計データ（データベース）へのアクセス管理は重要
- 管理や評価の効率化のために「統合＋自動化」が重要

ご静聴ありがとうございました・・・

If you have any questions...

mitsuhiko.maruyama@tohmatsu.co.jp

Thank you <(_ _)>