Deloitte.

システム監査の現状と未来

2010年01月23日

デロイト トーマツ リスクサービス株式会社
公認会計士 公認情報システム監査人
丸山 満彦

トーマツ

Agenda

- システム監査の歴史を振り返ってみる
- システム監査の現状を踏まえてみる
- システム監査、監査人の在り方はどうあるべきか

システム監査の歴史を振り返ってみる

過去の本を読んでみる

書名	著者・訳者	出版社	出版
EDPシステム監査　その理論と手続・ケーススタディ	W.Tohmas Porter.Jr著　伏見章、前川良博訳	日刊工業新聞社	1969年05月24日
セキュリティ コンピュータ・システムの機密保護マニュアル	米興情報処理学会システム改善委員会編 横山保、萬代三郎監訳	秀潤社	1977年02月15日
コンピュータ安全管理マニュアル	岡本行二、田口孝弘著	オーム社	1980年10月20日
コンピュータセキュリティ　犯罪対策と災害対策	ドン・パーカー著、日本情報処理開発協会監訳	企画センター	1982年05月31日
高度情報化時代のシステム監査の方法 コンピュータ・セキュリティ対策のあり方	青山監査法人システム監査部編	中央経済社	1984年11月10日
システム監査ガイドライン 管理目標と監査実施基準	EDP監査人協会東京支部　編	日経マグロウヒル社	1985年02月21日
システム監査人のための情報セキュリティ入門	Barry J.Wilkins著、渡部一元、宇佐美博、富山茂訳	日刊工業新聞社	1986年04月01日
情報システムのコントロール設計	Jerry FitzGerald著、鈴木勝彦監訳、堀内一、木戸恭彦、生田英輔	日経マグロウヒル社	1986年06月30日
データ資源管理 企業内データの有効活用を目ざして	William R.Durell著、味村重臣監修、IRM研究会訳	日経マグロウヒル社	1987年01月27日
コンピュータセキュリティ アクセス管理によるハッカー対策	ジェローム ローベル著 与那嶺桂子訳	マグロウヒルブック	1987年03月25日
管理者のためのコンピュータ・セキュリティ戦略　セキュリティ管理に不可欠な全社的管理体制	William E.Perry著、長谷川定吉、伊藤茂文、大和田淳	日経マグロウヒル社	1987年10月29日
システム監査の運用事例	社会経済生産性本部編　遠藤昇他	生産性出版	1987年12月25日
情報システム監査講座③情報システム監査の技法	石崎純夫監修、川野佳範、萩生光紀編著	オーム社	1988年05月20日
システム監査用語辞典	ビジネス・ブレイン太田昭和	中央経済社	1988年07月05日
情報システム監査講座②情報システム業務の管理・統制	石崎純夫監修、浅輪壽男、堀内一、諸岡節生、良永順	オーム社	1988年07月25日
システム監査実施の手引	松田武彦他	日本情報処理開発協会	1989年09月13日
コンピュータウイルス対策基準 解説書	通商産業省機械情報産業局監修	日本情報処理開発協会	1990年04月20日
コンピュータ犯罪と現代刑法	日本弁護士連合会、刑法改正対策委員会編	三省堂	1990年05月25日
システム監査基礎辞典	岩崎尚人、上園忠弘、大久保丈二、神田良、瀬野和泉、遠山暁、鳥居壮行	コンピュータ・エージ社	1990年10月01日
システム監査の基礎と実際　システムの健康度をチェックする	日本システム監査人協会 編著	東京電機大学出版局	1992年12月20日
システム監査の理論	堀江正之	白桃書房	1993年03月06日
情報システム管理者心得帳	監査法人トーマツ 小浜健二	中央経済社	1993年11月25日
コンピュータ環境下の内部統制監査	アメリカ公認会計士協会コンピュータサービス執行委員会 (著), 石原 俊彦, 林 隆敏 (翻訳)	晃洋書房	1994年12月01日
情報システムのコントロールと監査Q&A	日本公認会計士協会 情報システム委員会編	中央経済社	1998年02月25日
システム監査技術者合格完全対策　'98年版	梅津尚夫編著	経林書房	1998年04月24日
システム監査の基本	森實、森靖之	白桃書房	1998年09月26日
情報システムの内部統制 ITに対応した評価の計画と手続	石島隆著	中央経済社	2005年02月20日

【参考】システム監査，EDP監査の「古書」をアマゾンで検索してみる

No	書名	著書・訳者	発行年
1	監査業務とEDP	ウエイン・S.バウテル、今井 敬二、吉村 成弘、大橋 周治	(1967)
2	EDPシステム監査ーその理論と手続・ケーススタディ	W.Tohmas Porter.JR.、伏見 章、前川 良博	(1969/5)
3	EDP監査	ハリー・L.ブラウン 富島 一夫	(1971)
4	EDP監査の実際	伏見 章	(1972)
5	会計情報とEDP監査	(研究叢書〈16〉) 中野 勲、大矢知 浩司、神戸大学経済経営研究所	(1972)
6	銀行のEDPシステム監査	(アメリカの銀行監査シリーズ〈2〉) アメリカ銀行経営研究所情報会計研究所	(1976)
7	システム監査体制確立への道	日本情報処理開発協会	(1977/3)
8	システム監査の現状と問題点ー情報化社会の健全なルール確立をもとめて	日本情報処理開発協会	(1978/5)
9	システム監査の実態とその推進ーシステム監査の普及・定着をめざして	日本情報処理開発協会	(1979/3)
10	システム監査実施への道標	日本情報処理開発協会	(1980/3)
11	EDPシステム監査ー安全性信頼性採算性の総合点検	ジェーエムエーシステムズ アーサー・アンダーセン公認会計士共同事務所	(1981/5)
12	システム監査/セキュリティ訪米実態調査団報告書	日本情報処理開発協会	(1982/8)
13	システム監査入門	レスリー・ボール 松尾 明	(1984/9)
14	システム監査基準解説書	日本情報処理開発協会	(1985/8)
15	コンピュータ・セキュリティに関するリスク分析調査報告書	日本情報処理開発協会	(1985/12)

日本のシステム監査年表 (1)

システム監査年表

（参考資料１）

年　月	実施主体	内　容
1974年 4月	日本情報開発協会	システム監査の研究に取組むこととし、「渡米システム監査研修団」の派遣を発表
1975年 4月	日本情報開発協会	渡米システム監査研修団の報告書「システム監査」発表
1975年 6月	日本情報開発協会	「システム監査委員会（金子佐一郎委員長）」設置
1975年11月	日本経済新聞	11月7日付の社説で「システム監査の徹底を」と訴える
1976年 3月	日本情報開発協会	1975 年度システム監査委員会の報告書「わが国におけるシステム監査のあり方」発表
1976年10月	EDPﾕｰｻﾞｰ団体連合会	「システム監査の実施に関する要望書」を通産大臣に提出
1976年11月	日本公認会計士協会	「企業内部における EDP システム監査に関する要望書」を通産大臣に提出
1977年 3月	日本情報処理開発協会	1976 年度システム監査委員会の報告書「システム監査体制確立への道」発表
1977年度	通商産業省	一般会計でシステム監査の調査費が確定
1977年10月	日本情報処理開発協会	第二次渡米システム監査研修団派遣
1978年 5月	日本情報処理開発協会	「システム監査の現状と問題点」発表
1979年 3月	日本情報処理開発協会	「システム監査の実態とその推進」発表
1980年 3月	日本情報処理開発協会	1979 年度システム監査研究委員会の報告書「システム監査実施への道標」発表。この報告書には、「システム監査の実施に関する提言」および「システム監査基準（試案）」を収録
1981年 6月	産業構造審議会	情報産業部会：「システム監査基準やシステム監査人の養成が必要」と答申で指摘
1982年 4月	日本情報処理開発協会	「システム監査／セキュリティ訪米実態調査団」派遣
1982年10月	通商産業省	コンピュータセキュリティ研究会：「システム監査士等の資格創設も考えられる」と指摘
1983年12月	産業構造審議会	情報産業部会：「システム監査基準の策定と試験の実施」答申
1984年 6月	通商産業省	「情報化対策委員会システム監査部会」設置
1985年 1月	通商産業省	「システム監査基準」公表
1985年 8月	日本情報処理開発協会	「システム監査基準解説書」発行
1986年10月	日本情報処理開発協会	「システム監査実務の進め方」というテーマで情報化国際後援･討論会開催
1986年10月	通商産業省	第１回「システム監査技術者試験」実施
1987年 3月	日本情報処理開発協会	「システム監査学会」設立
1987年 9月	日本情報処理開発協会	「システム監査Q&A110」発行

システム監査研究の黎明期
鳥居 壮行
駿河台大学文化情報学部紀要
駿河台大学 15(2)
(20081200)

日本のシステム監査年表 (2)

年　月	実施主体	内　容
1989年 5月	システム監査学会 日本情報処理開発協会	「システム監査白書」発行
1989年 9月	日本情報処理開発協会	「システム監査実施の手引き」発行
1990年11月	システム監査学会	「システム監査の普及に関する要望書」を通産大臣へ提出
1991年 3月	通商産業省	「システム監査企業台帳制度」創設
1994年 1月	日本情報処理開発協会	「システム監査技術者育成カリキュラム」発行
1994年10月	システム監査学会 日本情報処理開発協会	「システム監査の理論と実践」発行
1994年 5月	日本情報処理開発協会	「システム監査技術者テキスト」発行
1996年 1月	通商産業省	「システム監査基準」改訂
1996年 7月	日本情報処理開発協会	改訂基準に基づく「システム監査基準解説書」発行
2000年 3月	日本情報処理開発協会	「プライバシーマーク制度における監査ガイドライン」発表
2002年 3月	日本情報処理開発協会	「システム監査の普及と基準のあり方に関する報告書」発表
2003年 4月	経済産業省	「情報セキュリティ監査基準」および「情報セキュリティ管理基準」告示
2003年 7月	経済産業省	「情報セキュリティ監査企業台帳制度」創設
2003年10月		「日本セキュリティ監査協会」設立
2004年 4月	システム監査学会	「専門監査人資格認定制度」創設
2004年10月	経済産業省	「システム監査基準」改訂 新基準は「システム監査基準」および「システム管理基準」の二本立
2005年 1月	日本情報処理開発協会	「システム監査基準／システム管理基準解説書」発行
2007年 3月	経済産業省	「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）」公表
2007年12月	経済産業省	「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）追加付録」公表
2008年 1月	システム監査学会 日本情報処理開発協会	「システム監査の理論と実践（第２集）」発行

本表にとりまとめた内容は、システム監査に関する調査研究を主導してきた経済産業省および㈶日本情報処理開発協会の活動を中心としたものである。

システム監査研究の黎明期
鳥居 壮行
駿河台大学文化情報学部紀要
駿河台大学 15(2)
(20081200)

1966年当時のEDP監査の手続き (1)

4.1.1 組織面のコントロール

監査人は，取引の承認，記録ファイルの保管あるいは資産の管理などの機能が分離して行われているかどうかを判定しなければならない。その判定のために組織計画やそれぞれの機能ごとの責任などについてチェックすることになる。

この機能分離の原則は，EDPシステムにおいては，システムアナリストとプログラマーの機能，オペレーターとテープ係あるいはデータの保管管理などの諸機能が分離独立していることによって達成されるわけである。

4.2.2 運営管理面のコントロール

運営管理面におけるコントロールの評価は，システムデザインとプログラミング及び電子計算機オペレーションに関する業務ごとの諸資料を点検することによって行われる。

（略）

4. プログラム変更について次のことが手順として明確にされているか。

a.プログラマーが自由勝手に修正変更するのではなく，権威ある管理者の許可，指示によって行われる。

b.適切なプログラム修正変更書類に基づいて行われる。

c.修正，変更後のプログラムテストのやり方が示されている。

（略）

10. コンソールによって印刷されたログシートは，対象業務処理に精通した（オペレーター以外の）責任ある人によって区分整理され，コントロールされ，点検されているか？

EDPシステム監査　その理論と手続・ケーススタディ　W.Tohmas Porter.JR.、伏見 章、前川 良博　1969

1966年当時のEDP監査の手続き (2)

4.1.3　手続のコントロール

監査人が内部統制のあり方を評価する場合に，データ処理システムの実態を調べて，データを記録し，処理し，提供するシステムの効果と能率について調査することも重要なことである。
そのような検討を行うことによって，財務と会計上の手続が，確立しているかどうかを判定することができる。
その場合，つぎにあげるような手続きが確実に行われなければならない。

1.取引の記録が適切かつ正確に処理されるために，十分な内容の点検が行われる。
2.データ処理の過程で実績報告や会計データの誤りを発見したり，訂正したりする。そして，そのような誤りの取扱を経営者の許しているレベルにまで引き下げる
3.財務，会計上の取引について，その承認，実施，検閲の責任を反映するようなリポートが要求され，準備される。

（略）

処理方法を観察したり，それについての質問は，2章で述べた三つのコントロールのタイプについて行われるのである。三つのコントロールというのは原始データのコントロール，処理手続のコントロールおよびアウトプットのコントロールであって，・・・

（略）

（プロセッシングのコントロールに関する質問）
1．プログラムには，インプットデータに脱漏や未処理があれば検出するチェックが組み込まれているか。

EDPシステム監査　その理論と手続・ケーススタディ　W.Tohmas Porter.JR.、伏見 章、前川 良博　1969

1983年のEDPAA（現ISACA）発行のControl Objectivesの項目

Ⅰ		マネジメントコントロール
	A	組織と情報システムの計画
	B	方針，基準及び手続き
	C	組織の責任と人事管理
	D	情報システムの品質保証
	E	内部監査
	F	外部からの規制事項
Ⅱ		情報システムの全般コントロール：システム設計，開発，保守のコントロール
	G	システム開発ライフサイクルの方法論と責任
	H	システム開発ライフサイクルのプロジェクト開始の段階
	I	システム開発ライフサイクルのフィージビリティスタデイの段階
	J	システム開発ライフサイクルの設計段階
	K	システム開発ライフサイクルの開発および導入の段階
	L	システム開発ライフサイクルの運用と保守の段階
	M	システム開発ライフサイクルの導入後の段階
Ⅲ		情報システムの全般コントロール：運用
	N	情報システム資源計画と管理
	O	情報システムの品質保証運用
	P	システムソフトウェア
	Q	アクセスコントロールと物理的セキュリティ
	R	バックアップと回復
Ⅳ		アプリケーションコントロール
	S	データ起票のコントロール
	T	データ入力のコントロール
	U	データ処理のコントロール
	V	出力データのコントロール
Ⅴ		テクノロジー
	W	データベースを利用するシステム
	X	分散処理とネットワーク運用
	Y	マイクロコンピュータ
	Z	タイムシェアリング

システム監査ガイドライン 管理目標と監査実施基準　EDP監査人協会東京支部　編

システム監査制度導入を阻む大きな壁 in 1985年

通産省が83年6月に実施した「コンピュータ・システムのセキュリティ対策に関するアンケート調査」によると対象企業のうちシステム監査制度を導入している割合はまだ10.4%と少ない，未導入のなかで「導入の予定がある」と回答した企業は17.9%しかない。

内部監査部門がない企業が多い

- 日本ユニバックのUNIVACコンピュータのユーザー・グループであるユニバック研究会の「システム監査に関するアンケート調査」（81年10月に調査）によれば資本金1億円以上の企業で内部監査部門がない企業は4割を超える（42.1%）。
- 日本には株式上場をする際に証券取引所が上場予定企業の内部統制状況を提出させ，2年間その運用状況を調べる。このために上場前には必ず内部監査部門ができるという良い制度がある。ところが，上場後には証券取引所はフォローしないため，いつの間にかに内部監査部門を消滅させてしまう企業も多い。（霜垣日本内部監査協会専務理事）

企業内ではシステム監査人が育ちにくい

- 日本の場合，監査部門に配属された人材のローテーション期間が短く，平均で約4年未満である。しかも再び監査部門に戻ってくるという例が少ないため，外資系企業のようなシステム監査の専門家が育つ仕組みができていないところが多い。（霜垣日本内部監査協会専務理事）

システム監査技術は幅広く不明確

システム監査ガイドライン 管理目標と監査実施基準　EDP監査人協会東京支部　編

システム監査制度を導入するための課題 in 1985年

- **経営トップに監査の必要性を認識させよ**
  - 信頼性や安全性監査については，・・・TQC（全社的品質管理）の一環として経営トップにアピールしてはどうか。その場合，選任のシステム監査人ではなく社内プロジェクト・チームによる監査活動になると思うが，それでも効果が上がればやがてシステム監査人の設置につながる。（モービル石油の鈴木勝彦課長）
- **国家試験を実施し長期教育コースを設けよ**
  - 大学や専門学校に内部統制やシステム監査講座の設置が必須（宇佐美博EDPユーザー団体連合会システム監査専門員会）
  - システム監査の実務ができるようにするには事例研究を中心とした教育コースがいる。期間は最低でも半年は欲しい。（システム監査コンサルタントの富山茂氏）
- **コンピュータ業界は監査人を育成せよ**

システム監査ガイドライン 管理目標と監査実施基準　EDP監査人協会東京支部　編

見えてくること

- コンピュータが利用されたと同時にシステム監査が始まった
- 汎用機からクラウドの時代の現代まで
  - 変わらないもの
    - コントロールの要件（目標）は変わらない
  - 変わるのもの
    - コントロールの具体的な実施手法
    - それに応じた具体的な評価手法

そして・・・

相変わらずシステム監査はあまり「はやっていない」？

システム監査の現状を踏まえてみる

(1) どのような状況なのか？

現在の課題意識

- **内部統制報告制度**の導入により、上場企業グループでは、財務報告の信頼性を確認するための内部監査がより精緻に行われるだろう。
- 財務報告の信頼性を確保する上では、情報システムに係る内部統制も重要である。
- したがって、**情報システム監査もより精緻に行われる必要がある**。
- 業務プロセスに係る内部統制の評価については社内の人材の活用が比較的容易であるが、外部委託が進んでいる情報システムの内部統制の評価については、情報システムの開発、運用、セキュリティ等に精通している人材が社内に不足し、**情報システム監査が十分にできていない**可能性がある。
- 米国企業の事例等を見ると、**情報システム監査を外部委託**している企業も多いように聞く。
- しかし、本来的には**社内でも情報システム監査ができる人材を育てていく必要**もある。
- 内部統制報告制度の対応のためではなく、企業の発展、企業価値向上のためにも情報システムの活用が重要であり、そのために有効な内部統制の整備、運用が必要だからである。

概要把握に利用したデータ

- 情報システム監査の実施状況についての主な調査として

日本情報処理開発協会 「システム監査普及状況調査（平成19年3月）」

（以下、普及状況調査）

- 2006年9月から11月に実施
- 母集団40業種、4000事業体を対象として質問書を発送し、417社から回答を得ている。

日本内部監査協会 「監査総合実態調査　2007監査白書」

（以下、総合実態調査）

- 2007年10月から11月に実施
- 内部監査協会の会員1885社と非会員2411社の総数4296社に対して質問書を発送し、1473社から回答を得ている。

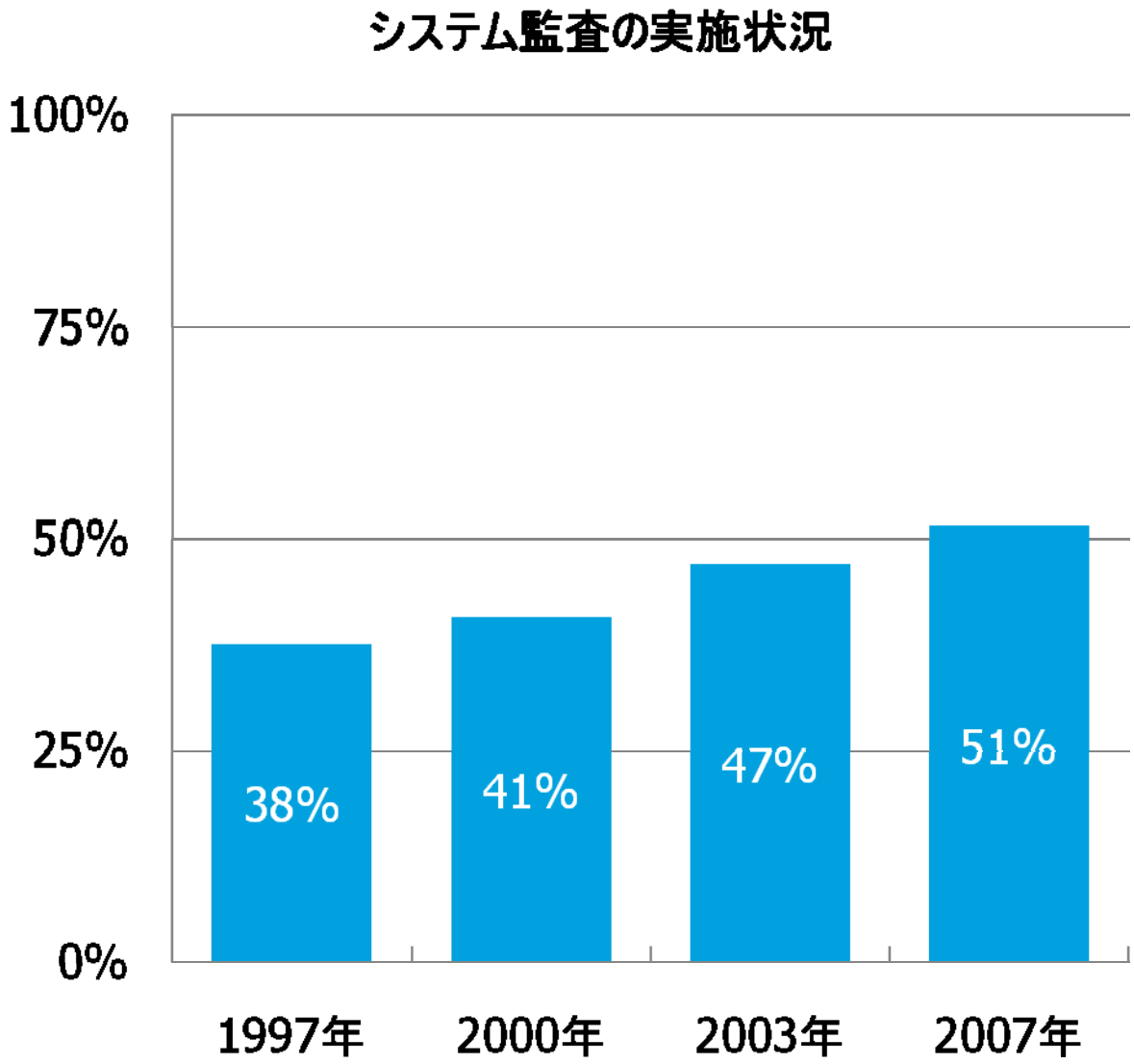
二つのデータをもとに現状を検討した。

- 経年データについては質問項目の変動があるため、必ずしも経年データが取れていない場合があることに注意していただきたい。

システム監査を実施している企業は「2社に1社」?

システム監査を実施している企業は全体の約半分である。
10年前の1997年では約40%であり、年々増加している傾向にある。

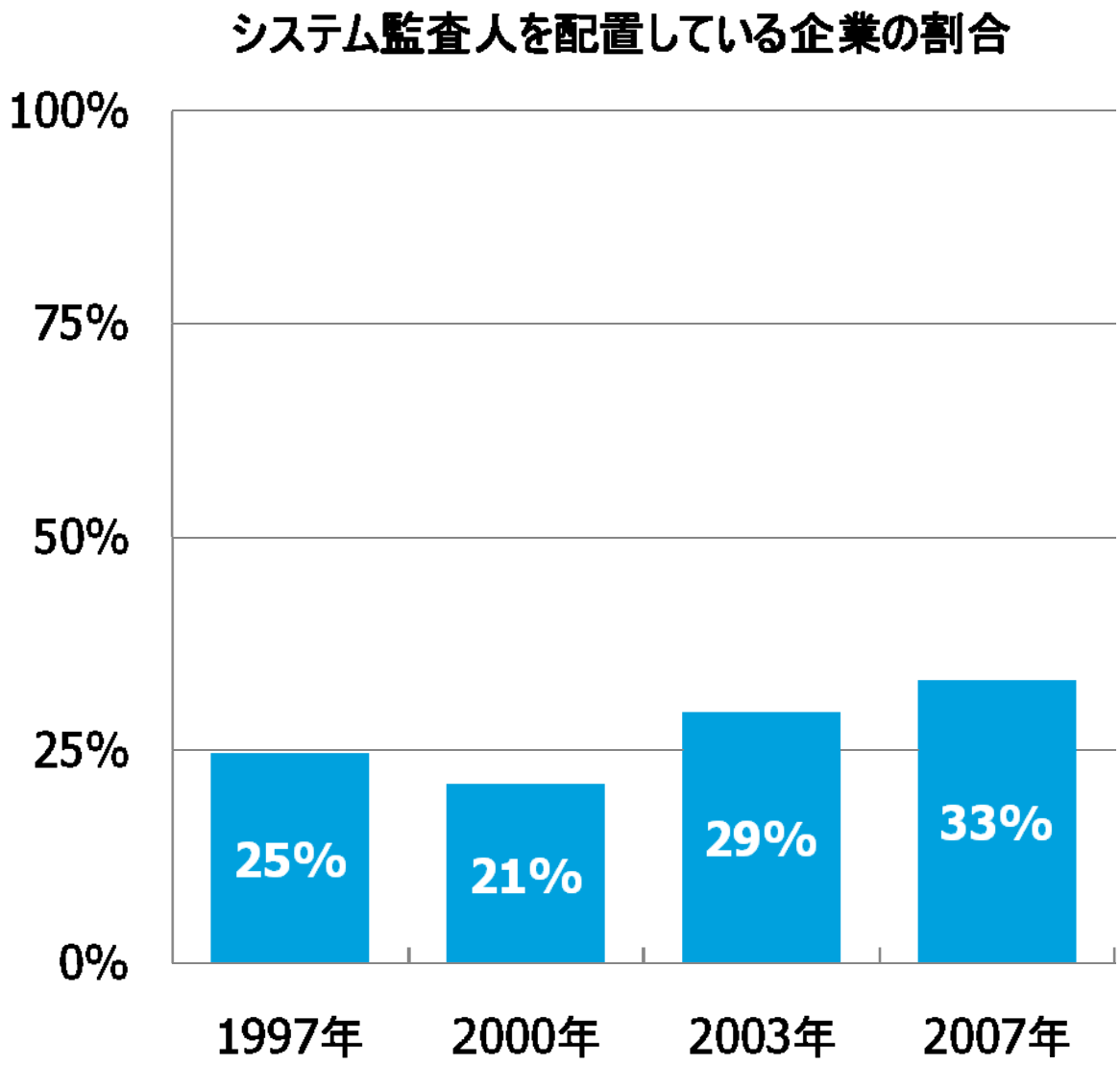
【参考】
1983年6月の通産省の調査では10.6%



「総合実態調査」より

システム監査人を配置している企業は「3社に1社」?

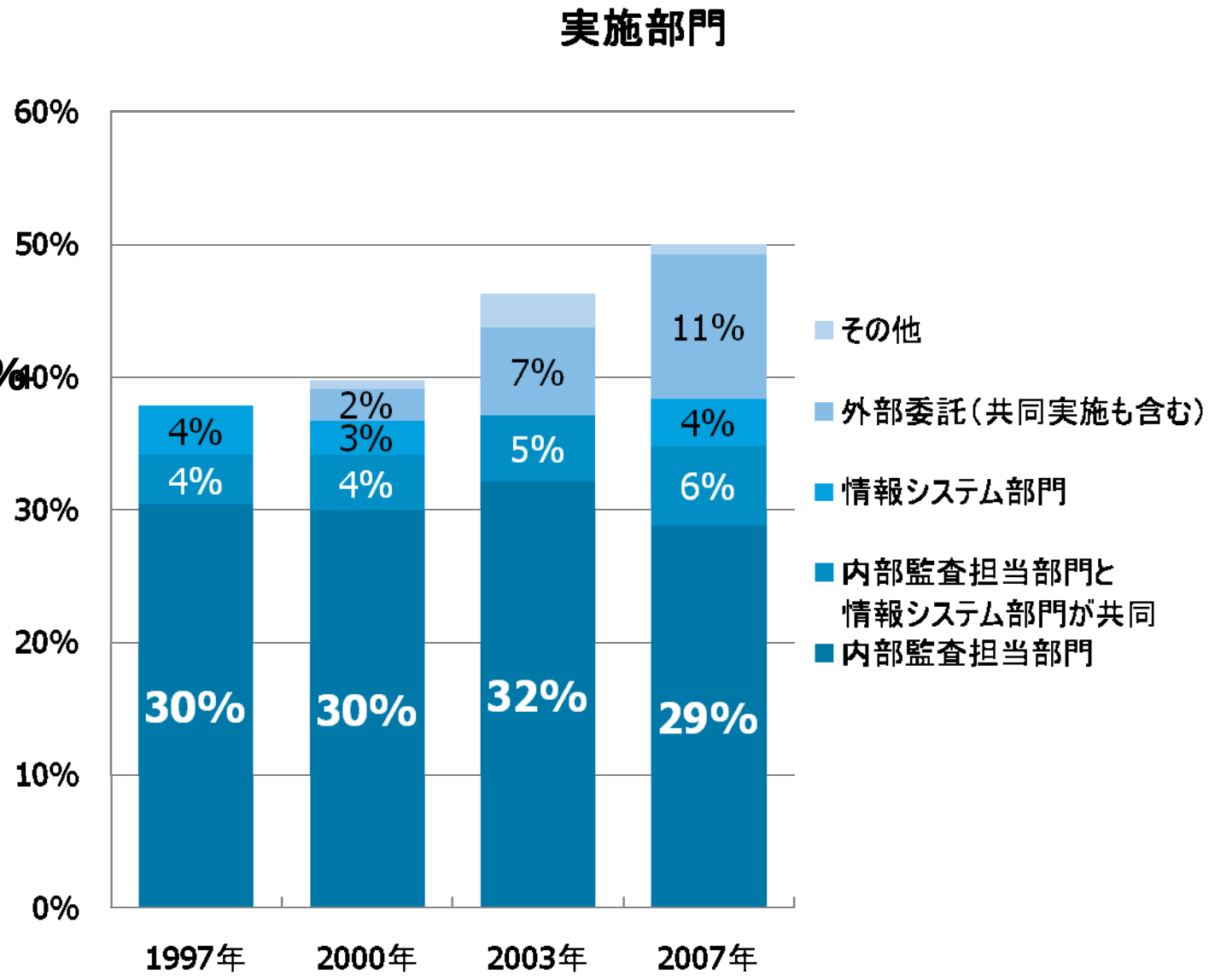
システム監査人を配置している企業は約3社に1社である。
10年前でも4社に1社であり、若干の増加が認められるものの大きな変化がない 。



システム監査を実施している部門

システム監査を実施していない組織も含め割合を示すと、**内部監査部門が実施している組織が約30％**である。

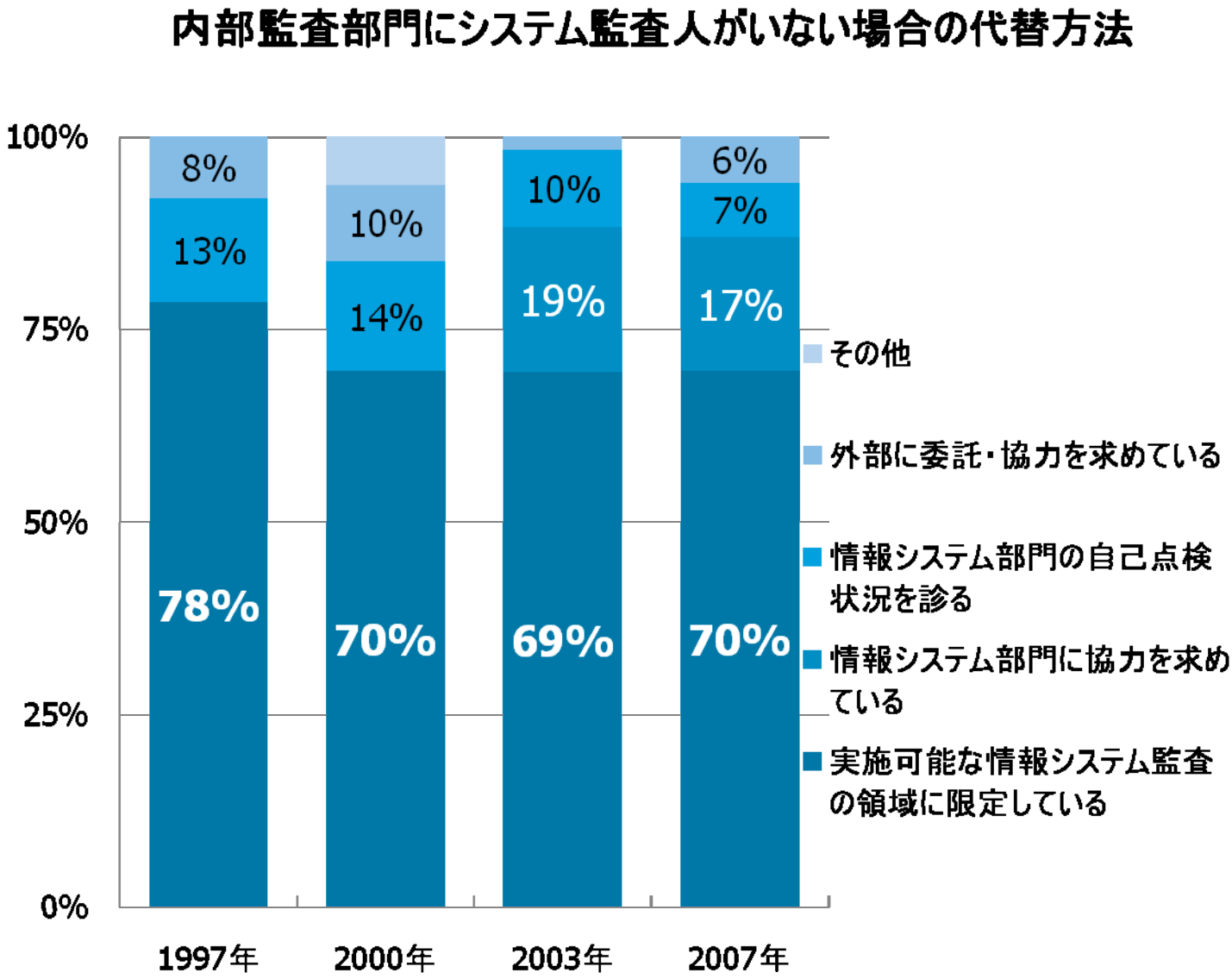
外部委託の利用は大幅に増加している。



「総合実態調査」より

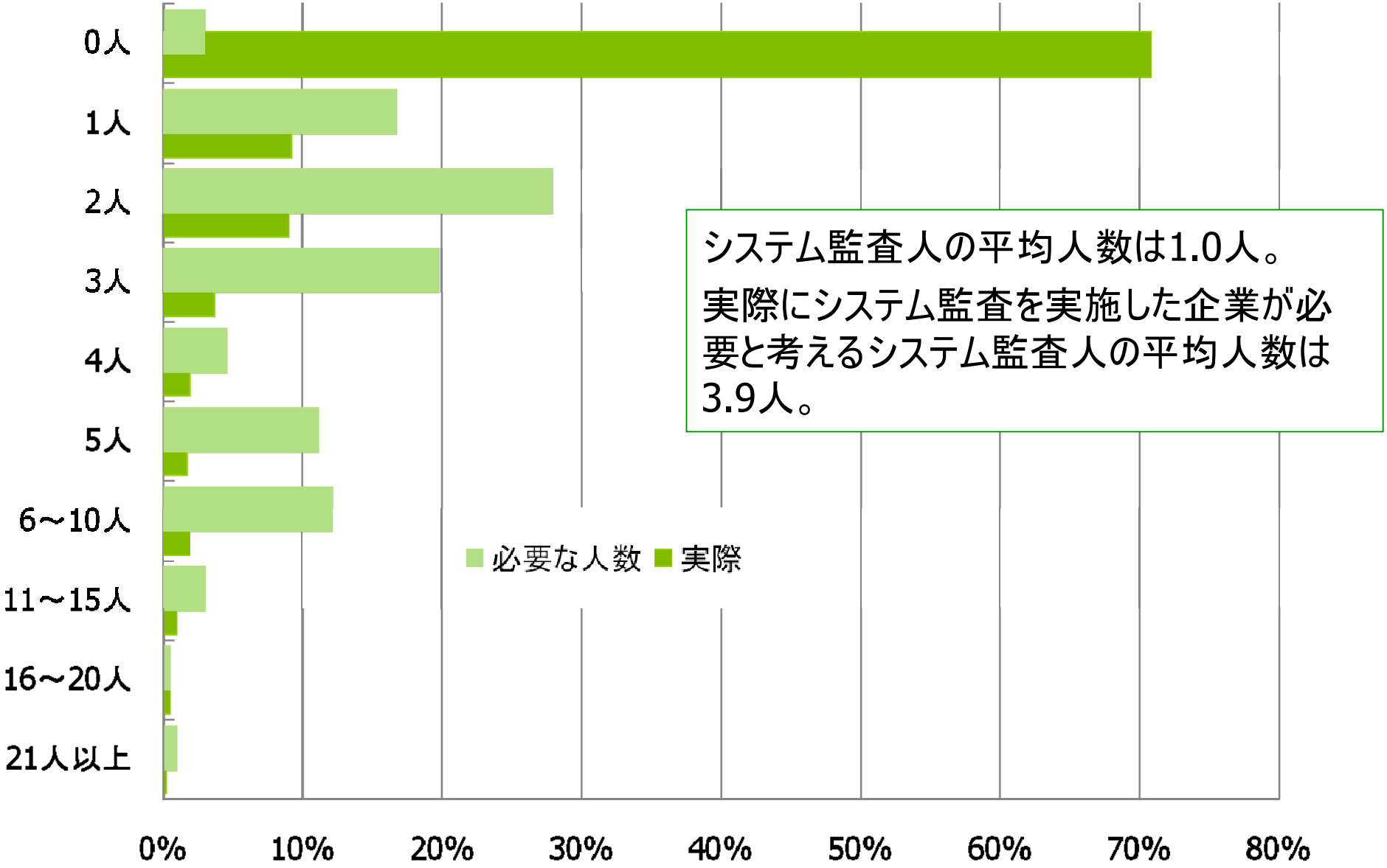
内部監査部門にシステム監査人がいない場合は「できることだけする」?

できることしかしていない組織が70%。
リスクに応じた内部監査が実施されていない可能性が高い。



「総合実態調査」より

システム監査人の人数 （1.0人 vs 3.9人）



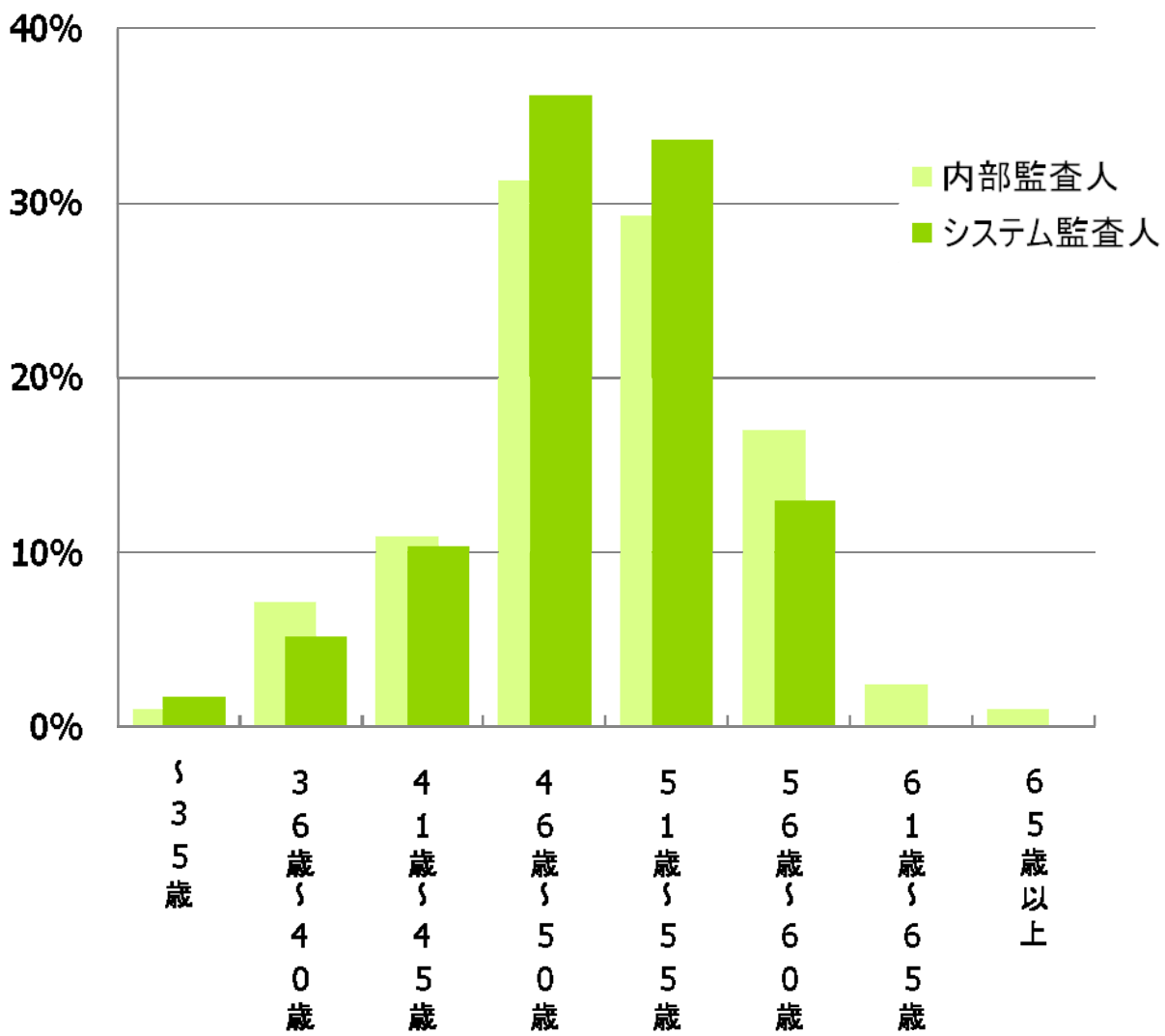
システム監査人の平均人数は1.0人。
実際にシステム監査を実施した企業が必要と考えるシステム監査人の平均人数は3.9人。

「普及状況調査」より

（閑話休題）システム監査人の年齢

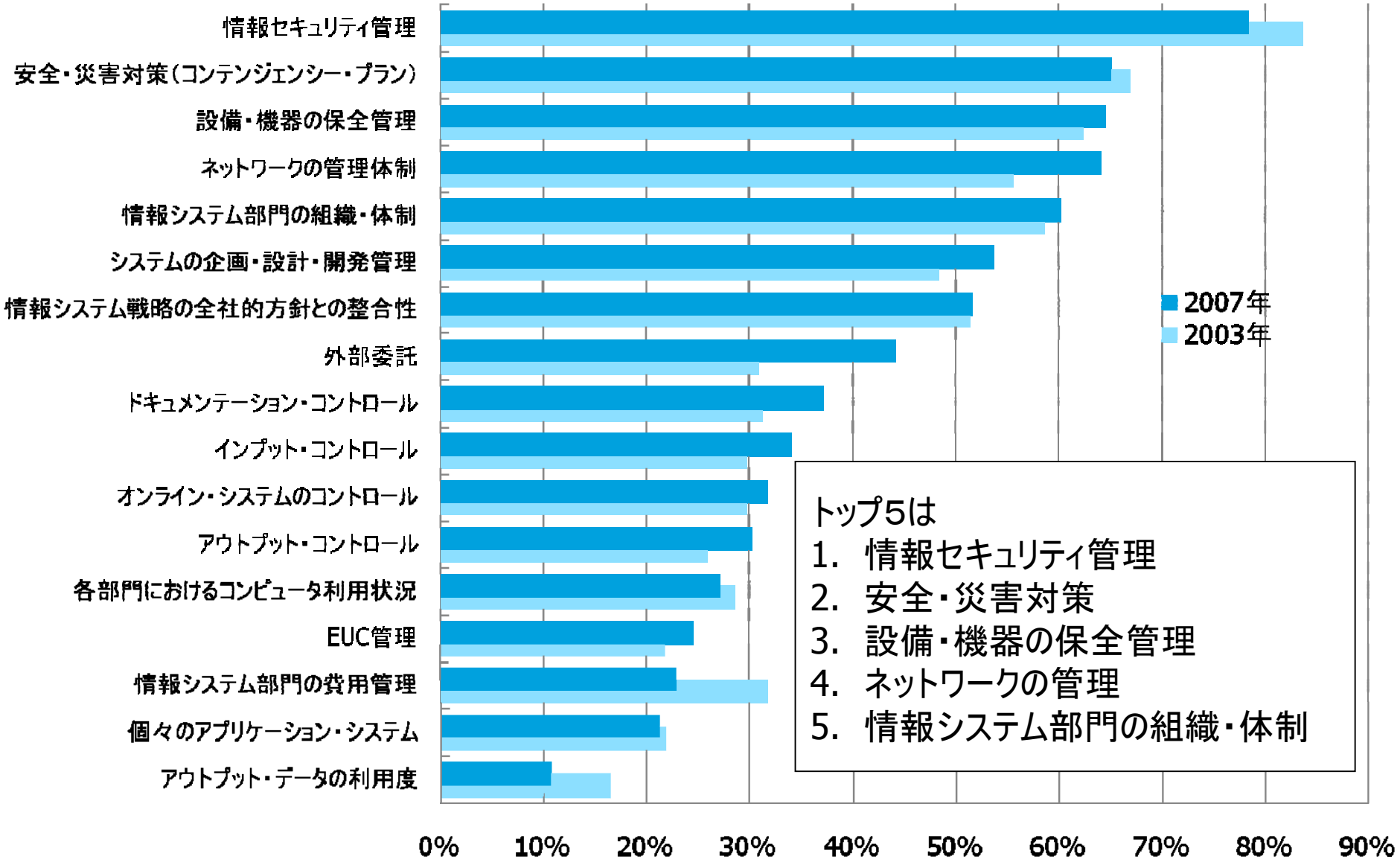
各組織における監査人の平均年齢。

システム監査人も内部監査人も同じく、約50歳。



「普及状況調査」より

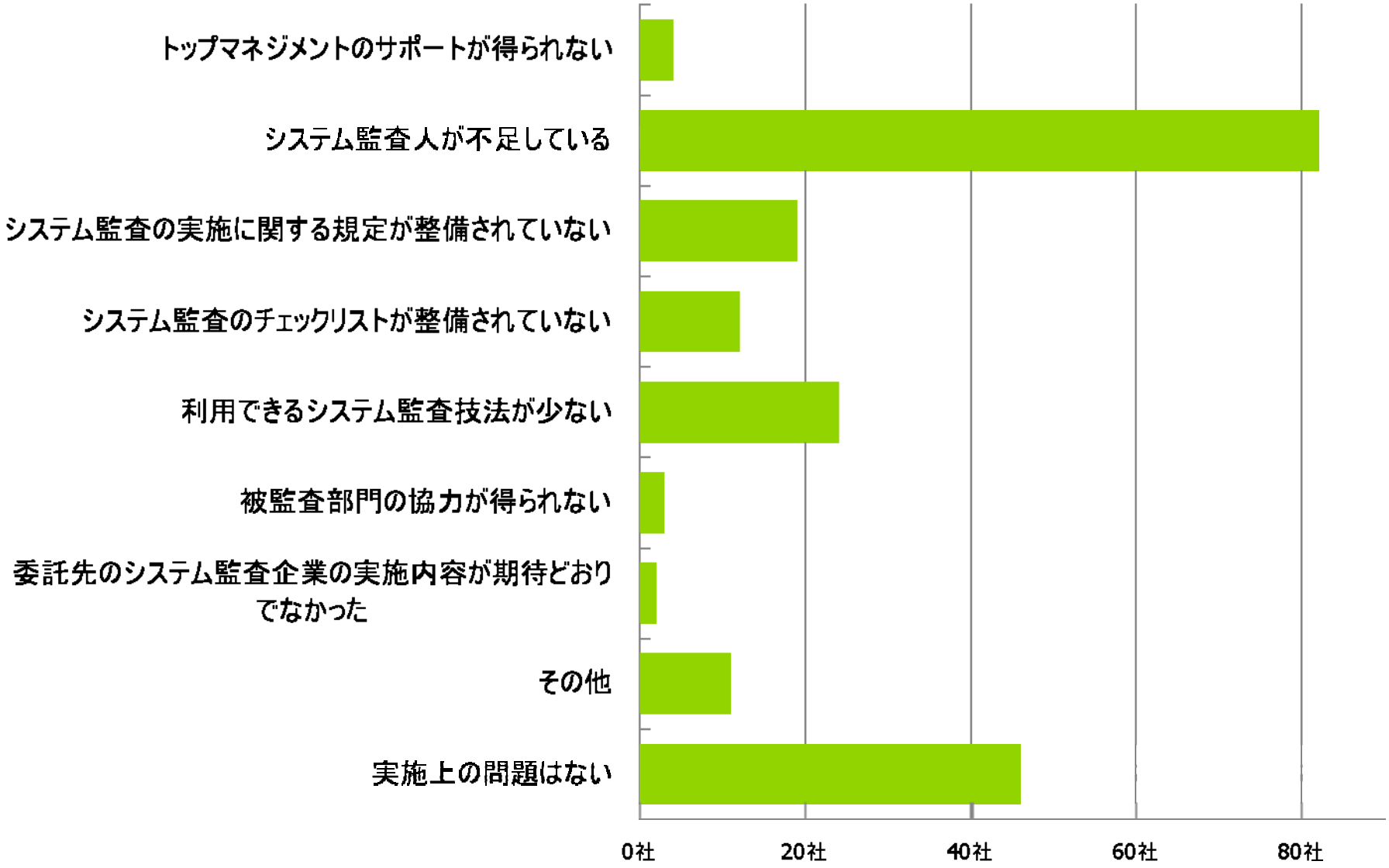
システム監査の実施領域



トップ5は
1. 情報セキュリティ管理
2. 安全・災害対策
3. 設備・機器の保全管理
4. ネットワークの管理
5. 情報システム部門の組織・体制

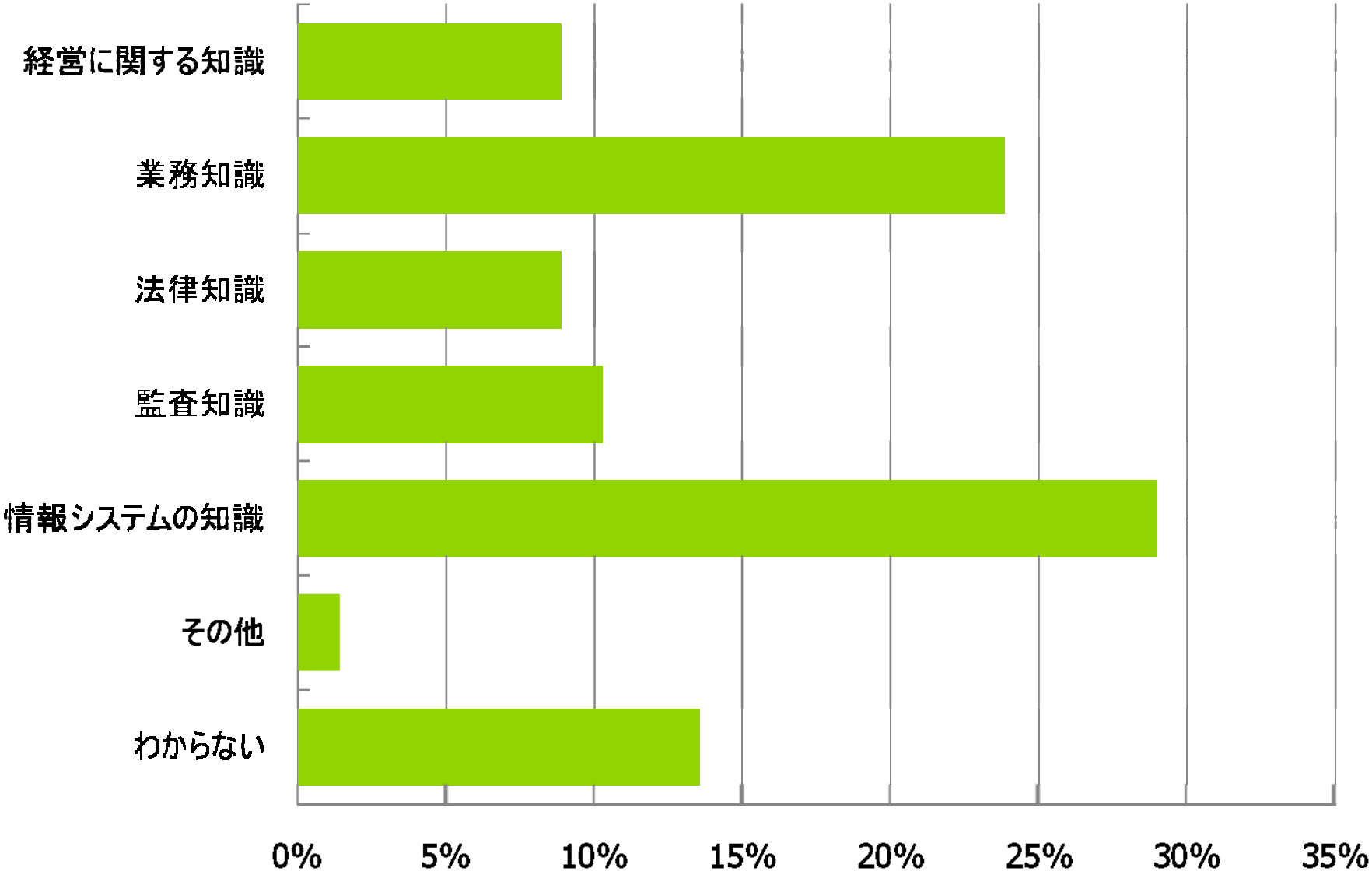
「総合実態調査」より

システム監査実施上の問題は「システム監査人が不足」していること



「普及状況調査」より

情報システム監査人に不足している知識は「情報システムの知識」

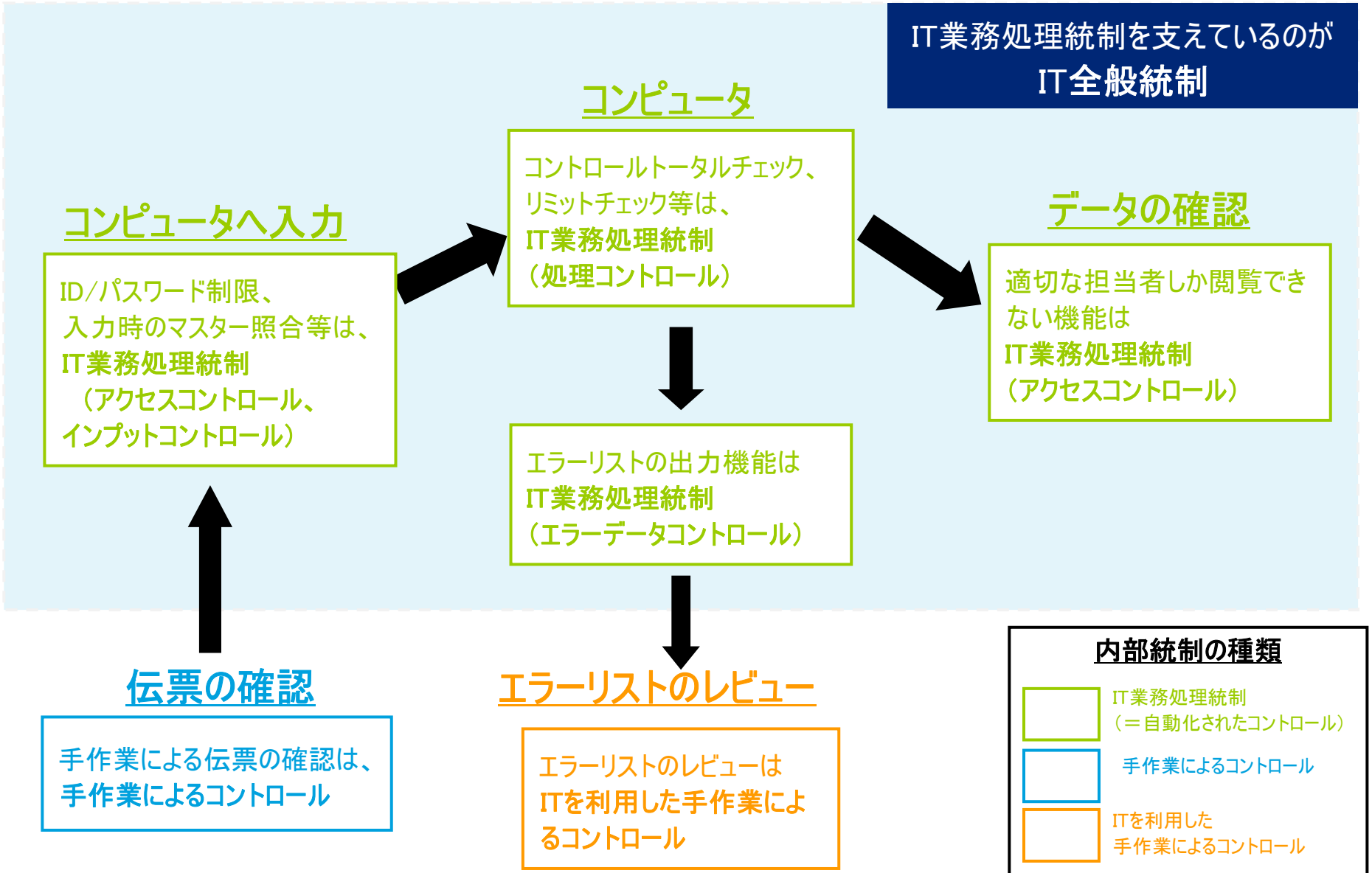


「普及状況調査」より

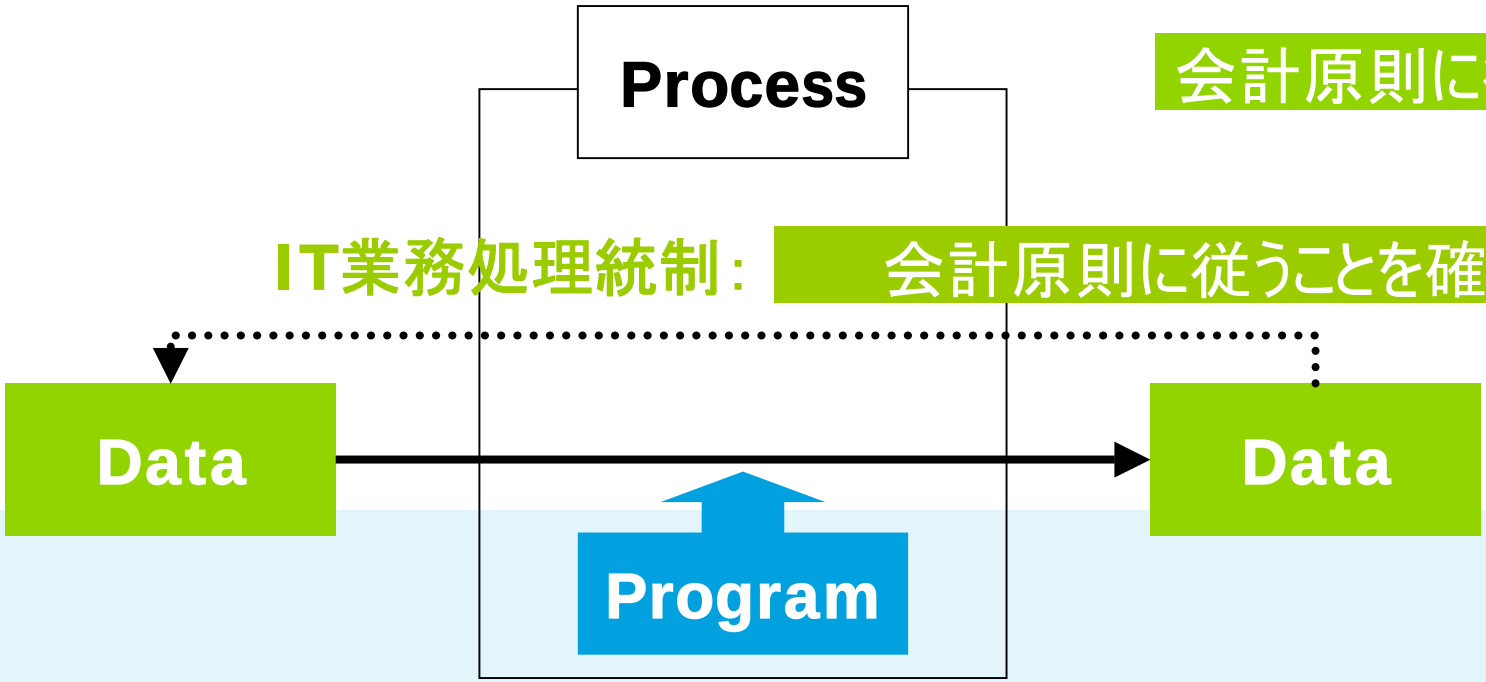
システム監査の現状を踏まえてみる

(2) 今，何をしているのか？

IT業務処理統制のイメージ図



IT全般統制のイメージ図



IT全般統制 **IT Processは期待したとおりに機能する**

1. 期待したProgramのみが実装される
2. Programは期待したとおりに実行される
3. ProgramやDataは改ざんされない

IT全般統制の評価項目

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 ）

「下線、太字は筆者による」

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。

※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

IT全般統制の評価項目

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）

「下線、太字は筆者による」

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

※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

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。

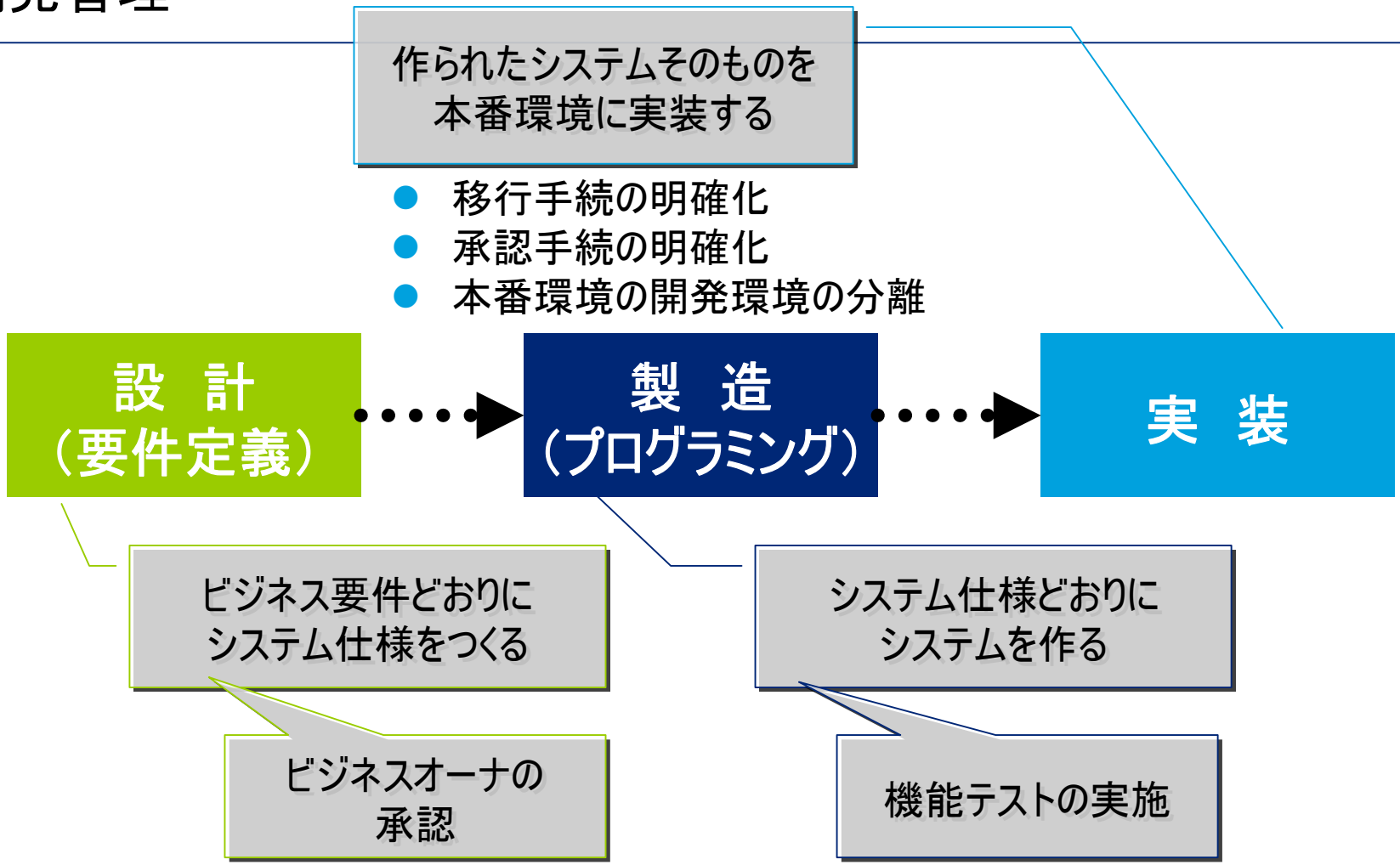
d. 外部委託に関する契約の管理

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。

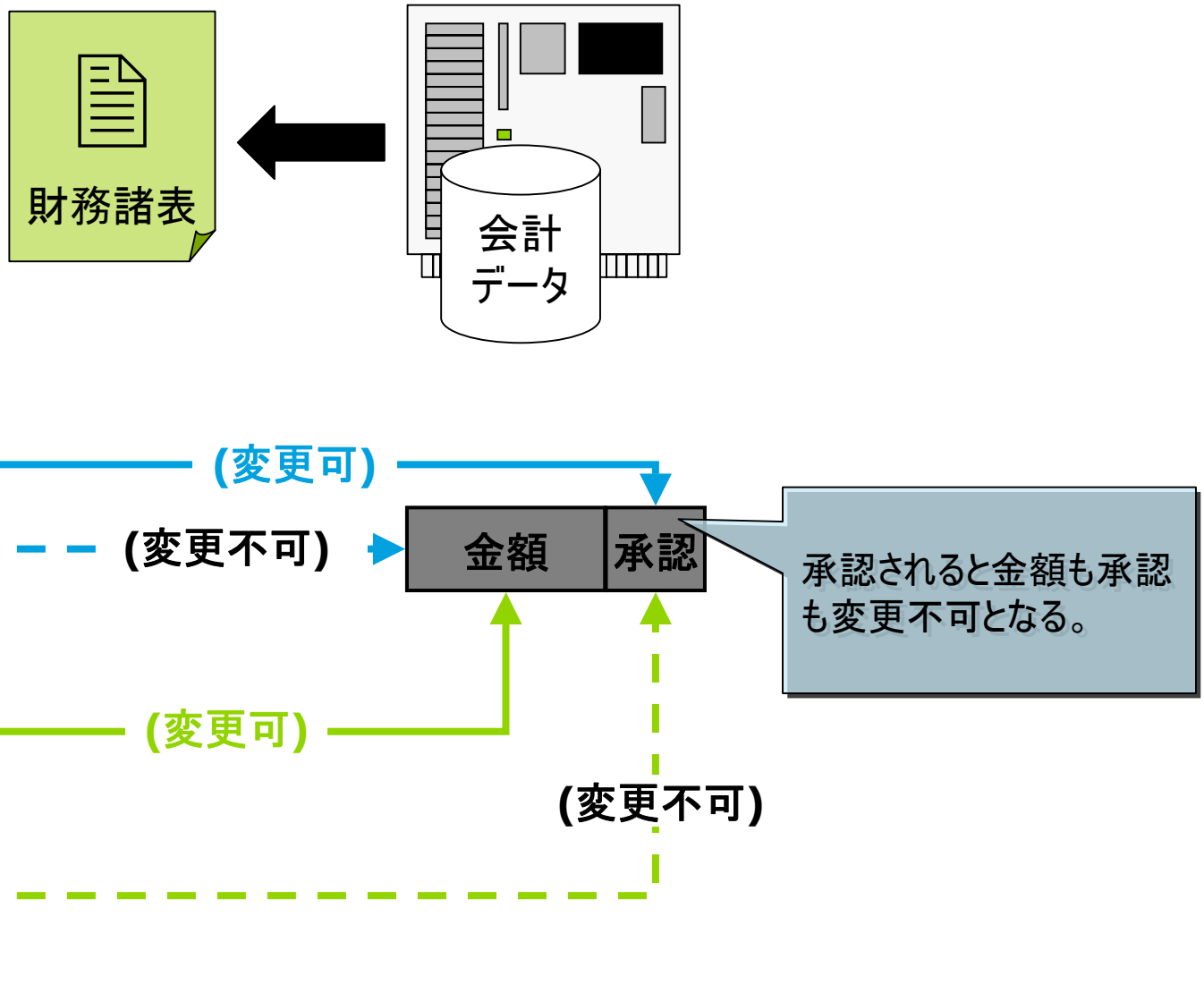
（パッケージ・ソフトウェアをそのまま利用するような比較的簡易なシステムを有する企業の場合）
ITに係る全般統制に重点を置く必要があることに留意する。

※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
「下線、太字は筆者による」

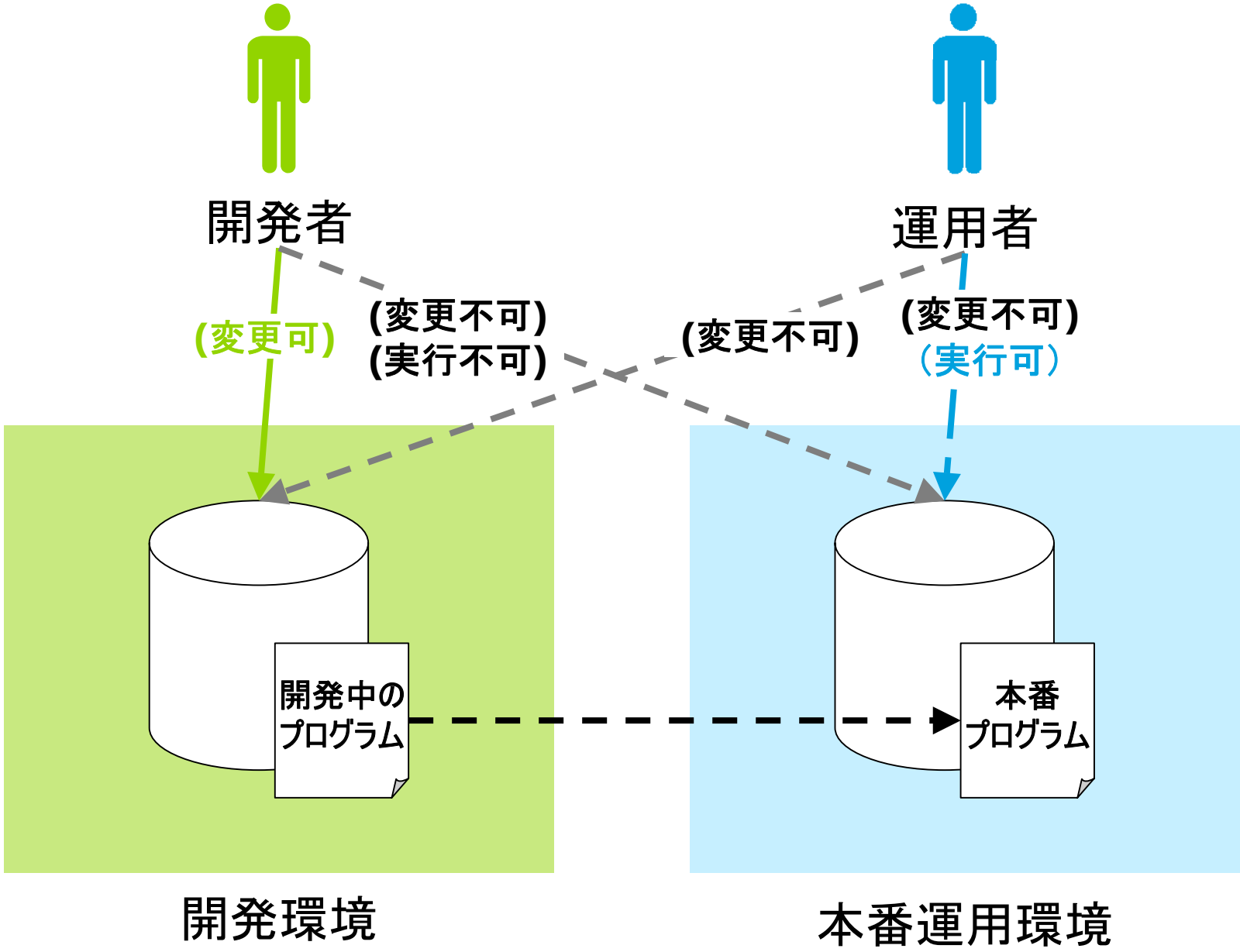
開発管理



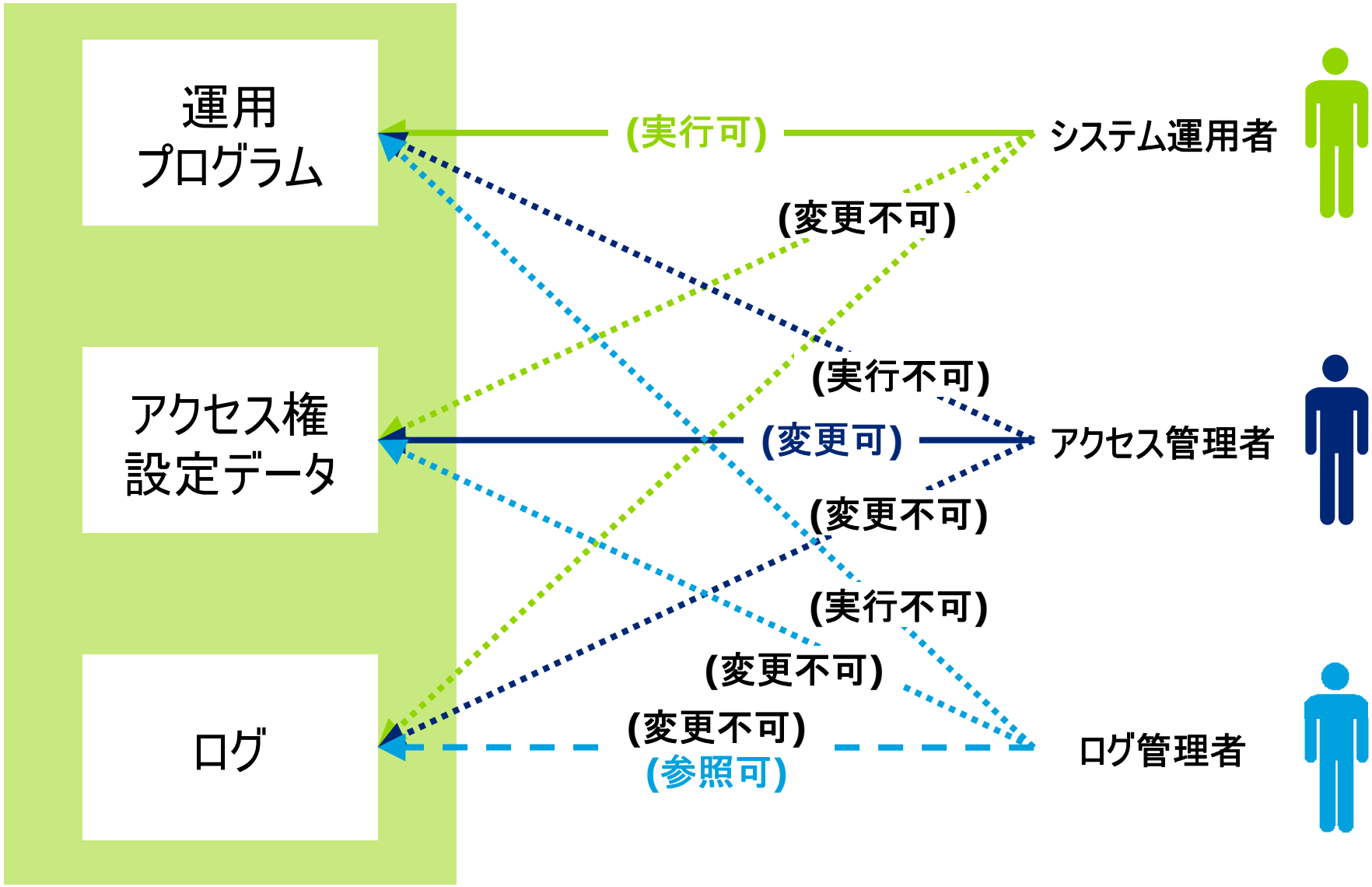
アクセス管理（会計データのアクセス管理）



アクセス管理（情報システム部門の職務分掌）



アクセス管理（特権ユーザの分離）

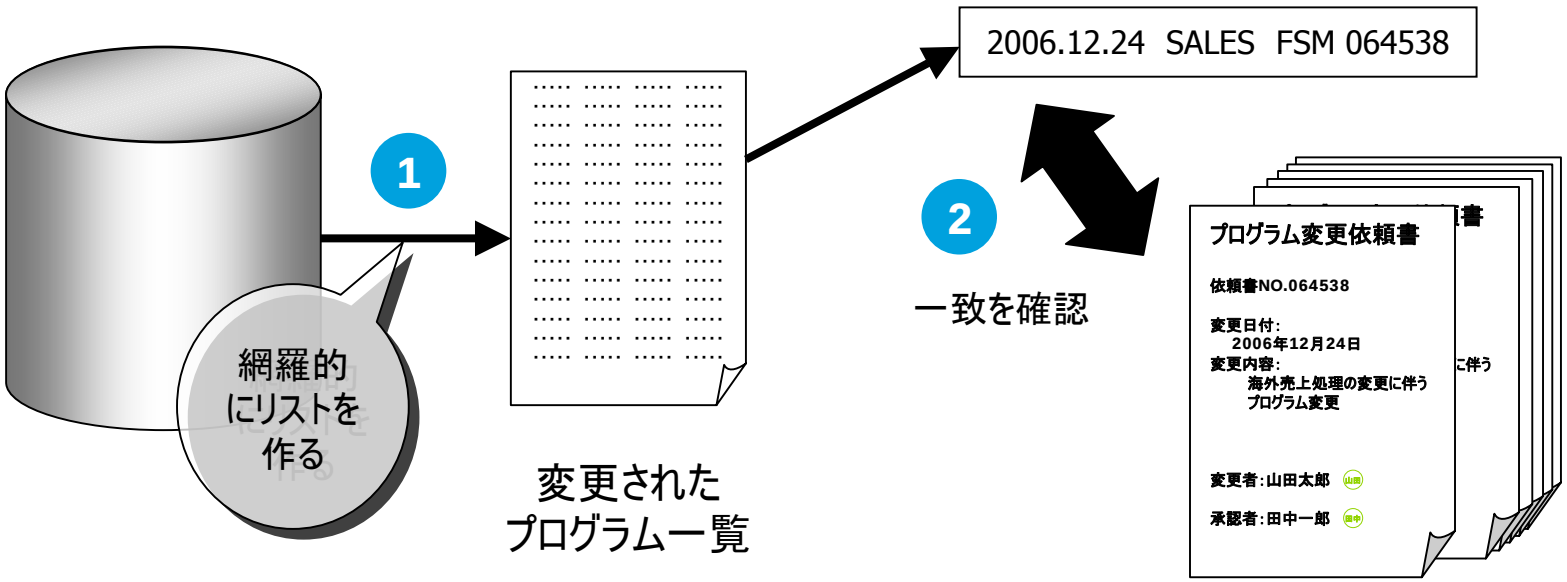


同じ目的を達成するための手段は複数ある。。。

本番環境のプログラムは、承認なしに変更されていない

手段1 開発環境と本番環境は分離され、開発者が本番環境のプログラムを変更できないようになっている。

手段2 変更されたプログラムはすべて、承認されている。



設定をみなければわからない場合も多い

- 例えば、アクセス権の設定が適切に行われているか？
- 汎用機
  - ACF2、TOP secret、RACFなど
- UNIX、Windows
  - 3rdパーティのアクセス管理ソフトの設定を確認する場合もある。
- データベース
  - Oracle DB、SQL server、Informix、DB2等の設定

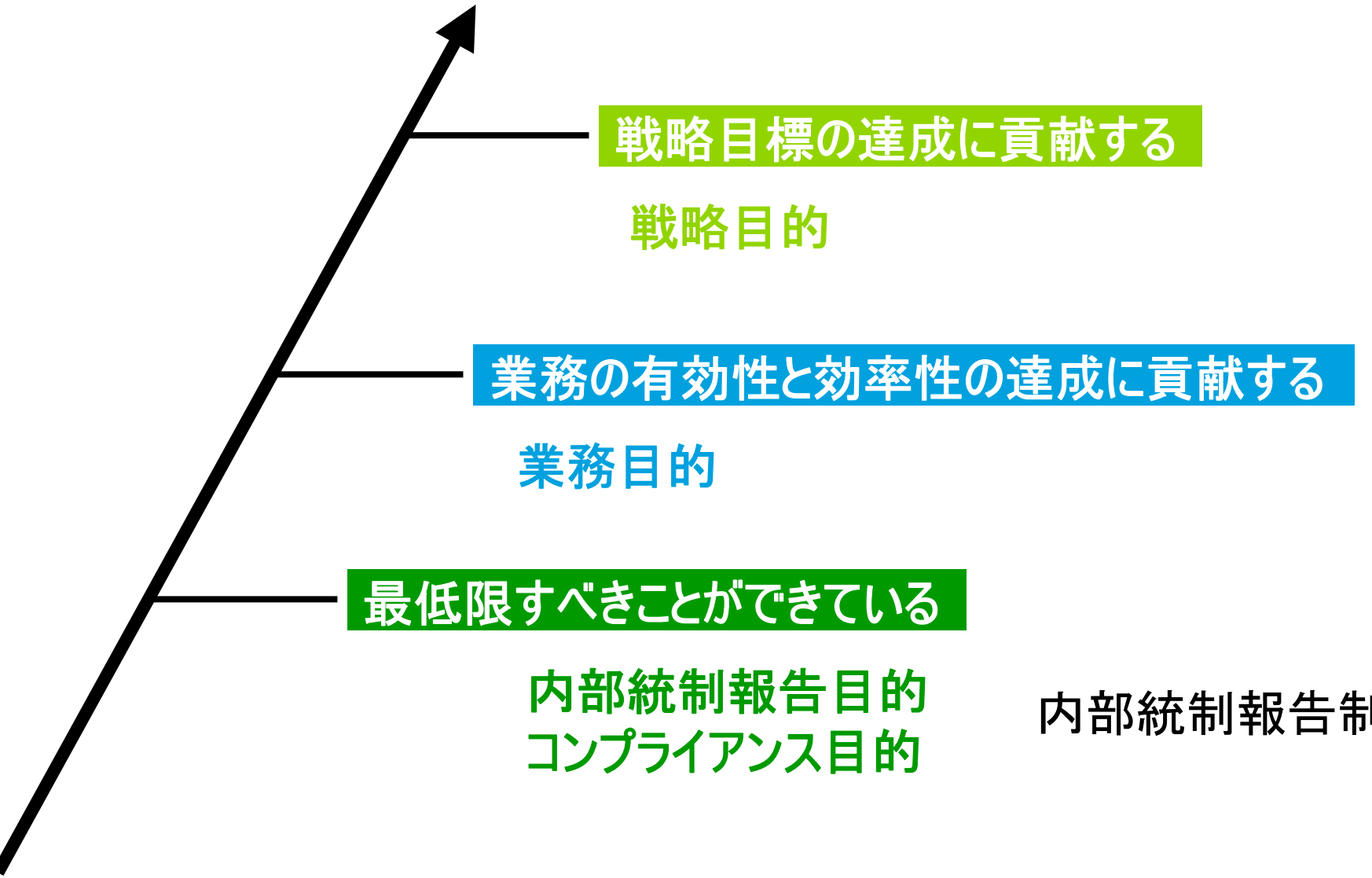
システム監査の未来を考える

内部統制報告制度の導入でシステム監査の重要性が認識された？

- 内部統制報告制度の導入により
  - 上場企業には財務報告に係る内部統制の評価が義務付けられた
  - システム監査の必要性が認識された？

  - CISA等のシステム監査の資格保有者が増加した！

有効性の監査？（企業価値の向上に向けて）



内部統制報告制度

業務の有効性及び効率性の評価のポイント

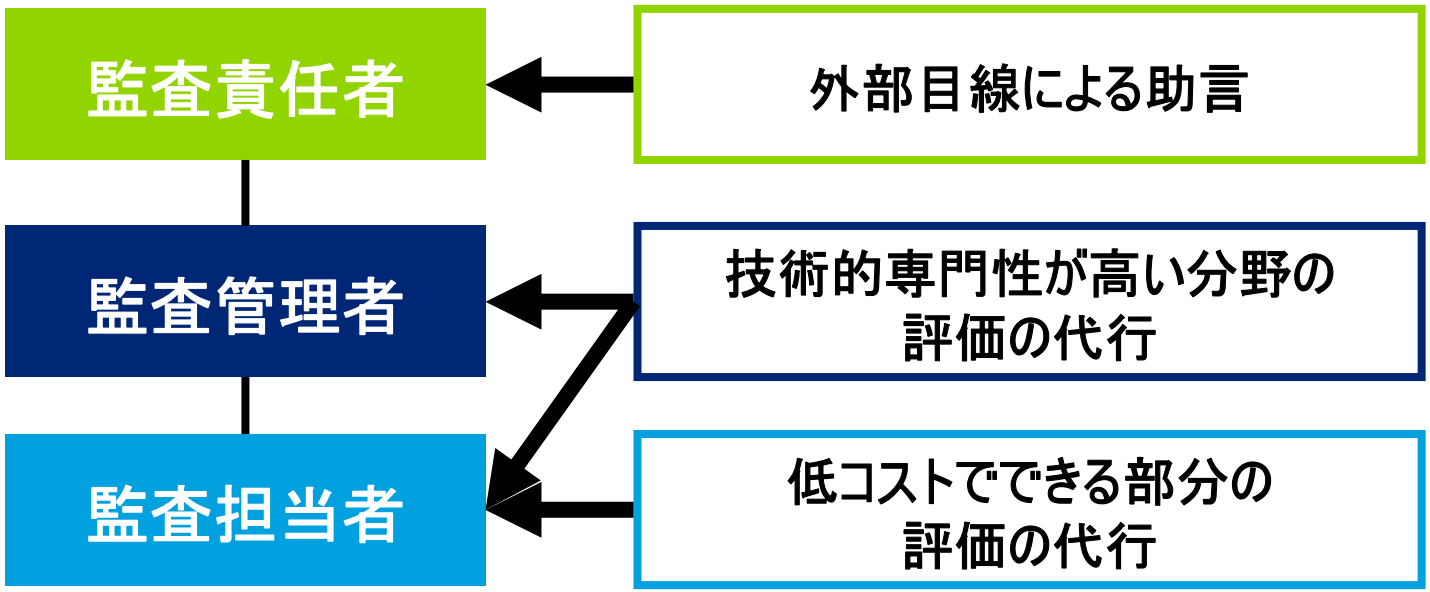
- 主にオペレーションに主眼を置く
  - 同じ目標を達成するための手段には複数の手段がある
    - より効率的か（インプットとアウトプットの関係）
    - 例：手作業により、個々のシステムにIDを登録するよりも複数システムに同時にIDが登録できるようにするほうが、同じ目標を達成するための作業コストは少ない。
  - より効果的な目標を達成する。
    - 例：きめ細かなアクセス権の設定により、リスクをより低減することができる。
    - 注意：効果を高めるためには、より多くのインプットが必要となることが多い。そのためには、同時に効率性も追求することが重要となる。

戦略目的の達成の評価のポイント

- 主に計画に主眼を置く
  - 企業の戦略目標を達成することができるシステムとなっているか
    - 「顧客の細かいニーズに対応できるようにする」
    - システムがそのような目標を達成できるアーキテクチャーとなっているか？
  - 環境変化に柔軟に対応できるシステムとなっているか
    - 「新たな顧客ニーズに迅速に対応できるようにする」
    - システムが環境変化に応じて柔軟に対応できるアーキテクチャーとなっているか？
- 戦略はシステムに従い、システムは戦略に従う？

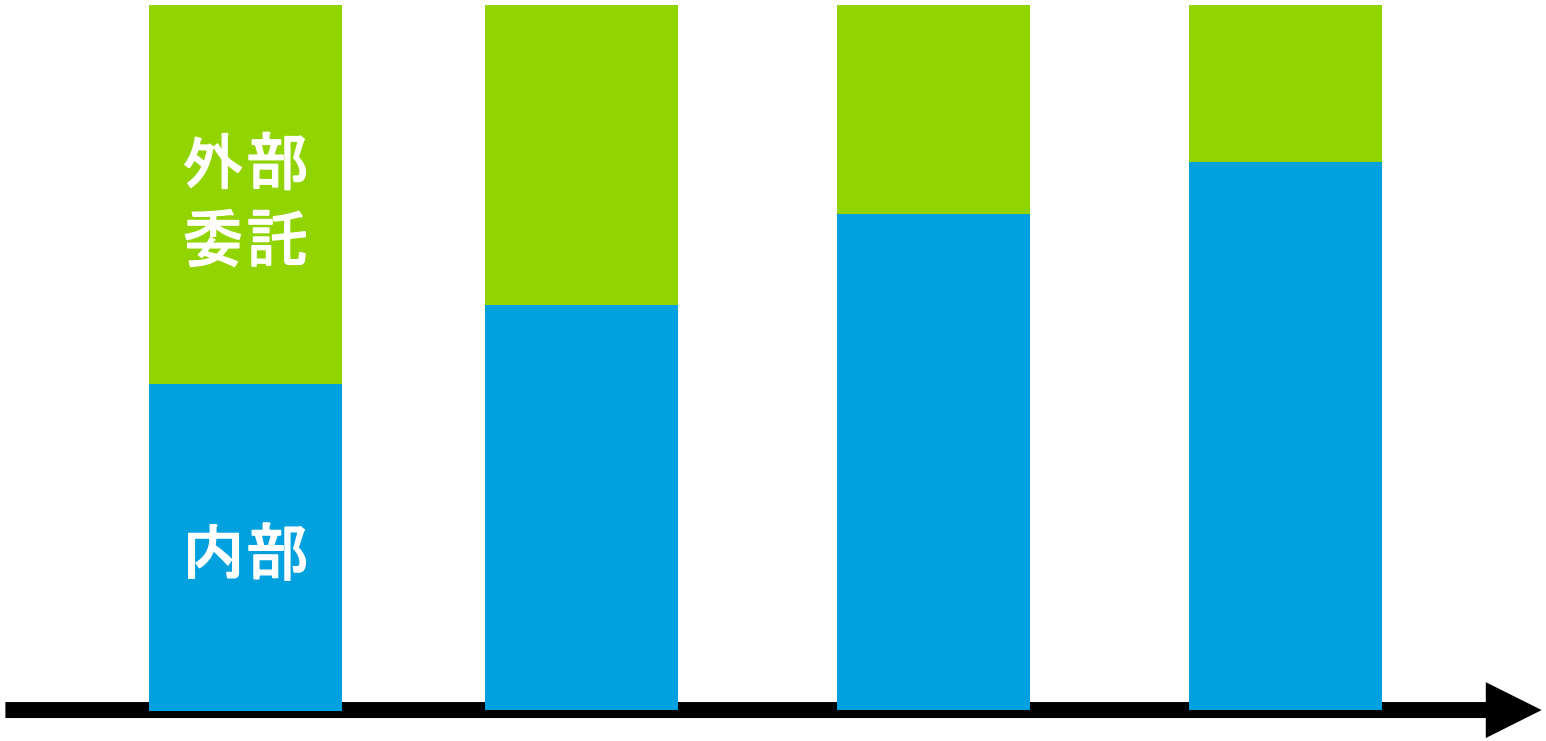
しかし現実は，質・量とも不足しているシステム監査の要員

- 外部委託の上手な使い方の例示
  - 低コストでできる部分は外部に委託
  - 技術的な専門性が高い分野は外部に委託
  - 外部目線が必要な部分は外部に委託



「丸投げではない」。監査の主体は監査部門側に！

スキル移転をしながら内部実施と外部委託の最適配分へ

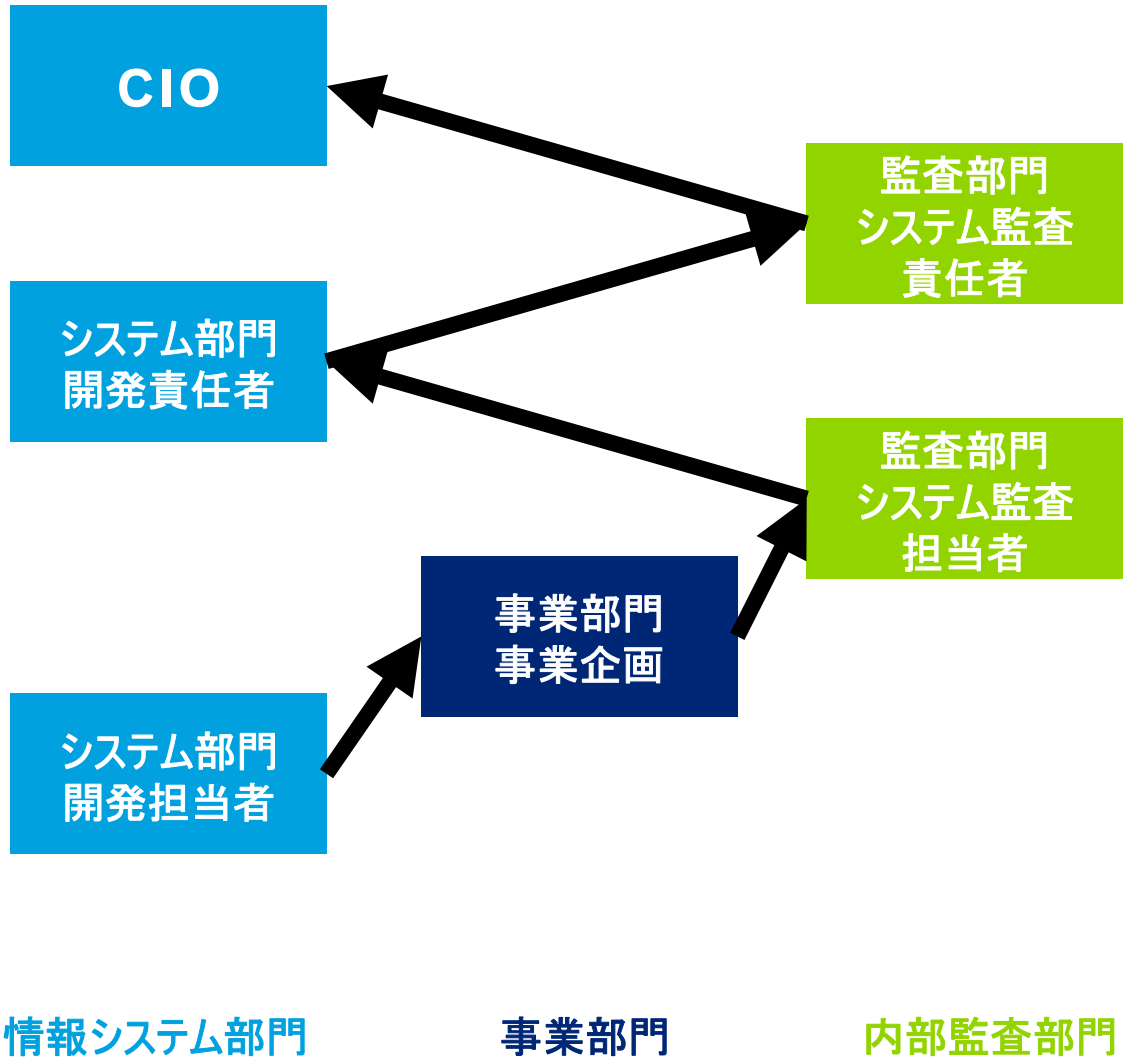


当初は外部委託が多くなる可能性が高いが、
スキル移転等を通じて
最適配分を目指すべきだろう

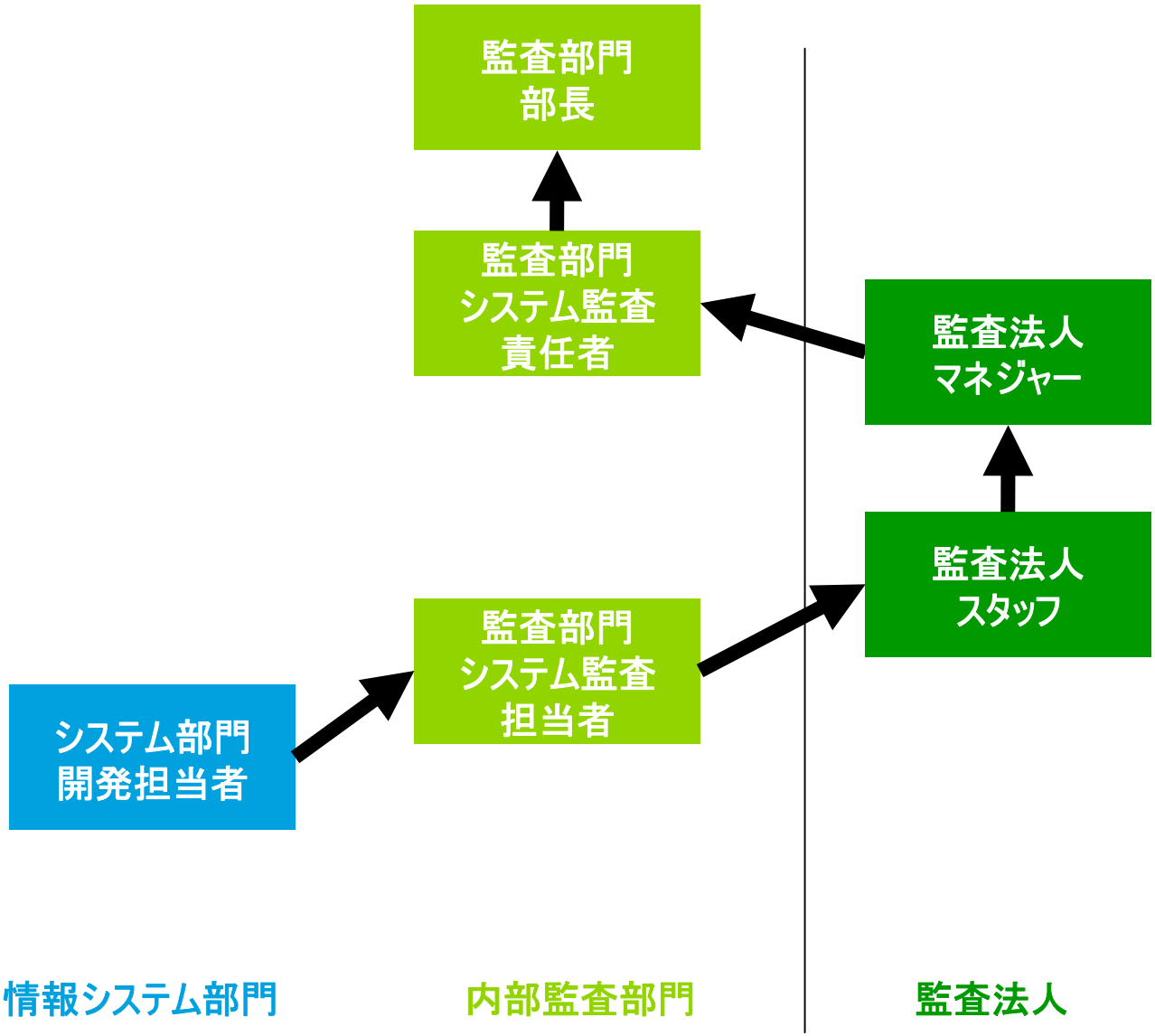
これから重要となる外部委託先のシステム監査

- 中小企業を中心にパブリッククラウドの活用が進む可能性がある
- パブリッククラウドに対するシステム監査をどのようにすべきか？
- 契約に監査をできる条項がはいっているのか？
- 入っている場合でも海外にセンター等がある場合はどのようにするのか？
- パブリッククラウド事業者がシステム監査の報告書を提出してきたらその内容を理解できるか？内容を納得できるか？

システム監査人のキャリアパスを考える（1）



システム監査人のキャリアパスを考える (2) 監査法人の活用？



経営者の皆様

- 内部統制報告制度の導入で**内部監査機能の重要性**が認知された。
- システム監査人は質・量とも不足している可能性が高い。
- 外部のリソースを積極的に活用する必要がある。
- 制度対応のみならず、企業価値向上に向けた視点がこれから重要となる。
- システム監査人を育てる環境が必要

今こそ、内部監査、システム監査の機能強化のための投資を！

ご静聴ありがとうございました・・・

トーマツグループはデロイト トウシュ トーマツ（スイスの法令に基づく連合組織体）における日本のメンバーファーム各社（有限責任監査法人トーマツと税理士法人トーマツ、およびそれぞれの関係会社）の総称です。トーマツグループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各社がそれぞれの適用法令に従い、監査、税務、コンサルティング、ファイナンシャル アドバイザリーサービス等を提供しております。また、国内約40都市に約6,700名の専門家（公認会計士、税理士、コンサルタントなど）を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はトーマツグループWebサイト（www.tohmatsu.com）をご覧ください。

Deloitte（デロイト）は監査、税務、コンサルティング およびファイナンシャル アドバイザリーサービスをさまざまな業種の上場・非上場クライアントに提供しています。全世界140ヵ国にわたるメンバーファームのネットワークで、ワールドクラスの品質と地域に対する深い専門知識により、いかなる場所でもクライアントの発展を支援しています。デロイトの165,000人におよぶ人材は"standard of excellence"となることを目指し、"誠実性"、"卓越した価値の提供"、"相互信頼"、"文化的多様性"といった価値観を共通するカルチャーで結ばれています。継続的な知識習得、チャレンジングな経験、豊富なキャリア形成の機会といった環境を生かしながら、Deloitteのプロフェッショナルは企業責任(CSR)を強化し、社会からの信頼を築き、各々の地域社会に貢献していきます。

Deloitte（デロイト）とは、スイスの法令に基づく連合組織体のデロイト トウシュ トーマツおよび相互に独立した個別の法的存在であるネットワーク組織のうちのメンバーファームのひとつあるいは複数を指します。デロイト トウシュ トーマツとメンバーファームの法的な構成についての詳細はwww.tohmatsu.com/deloitte/をご覧ください。

有限責任監査法人トーマツ東京事務所エンタープライズ リスク サービスは、2006年2月8日、監査法人として初めて情報セキュリティマネジメントシステムの国際規格であるISO/IEC27001の認証を取得しました。

ISMS_UKAS_JIPDEC

IS 501214 / ISO (JIS Q) 27001