ITガバナンス協会　CIO ITガバナンスセミナー

CIOはIT統制にどう取り組んでいるか

～　したたかに、そして真剣に　～

社団法人日本情報システム・ユーザー協会　主席研究員
東京海上日動火災保険（株）　特別任命参与
GIULIANI COMPLIANCE JAPANシニアアドバイザー
髙　橋　秀　敏

なお、本日の講義の内容は、個人の見解であって上記企業・団体の公式見解ではありません。

この講演を聞くと、何が分かるのか－１

Ⅰ－1

50分間の講演を聞くことで、何が分かるか、（と云うよりも何を理解していただきたいか）を挙げたのが、以下の５点。

■ **ＣＩＯとは何か（機能は？　何が必要か）**

JUASの実態調査結果および個人的な経験を踏まえての見解をお話しする。

■ **全社的な取り組み課題が続々と現れるが、どう整理したら良いのか。**

◎全体像のモデルをベースに、課題を整理するためのポイントを探る。
◎全社的な取り組み課題が、CIOの役割にどう影響しているのかを考察する。

■ **内部統制等の経営課題の取り組みを社内に浸透させていく工夫は何か。**

異文化の持つ多面性を理解して、自社に適した使い分けをする。

この講演を聞くと、何が分かるのか－２

Ⅰ－2

■ＪＵＡＳのアンケート結果に見る内部統制等の動向はどうか。

◎全社的な取り組み課題は、業界や他社との横並びの対応では済まされない。
◎身の丈に合った取り組みが、会社を支えていく。

■ＪＵＡＳのＣＩＯインタビューに見るＩＴ統制への取組の状況はどうか。

◎「したたかに、そして真剣に」というのが、率直な印象である。
◎アンケートでは、微妙な本音は見えてこない。その本音に迫りたい。

とは言っても、全企業に適用できる回答を出せない課題であり、**考えるヒント**の提供に留まる。
元々、回答は一つではなく、業種、業態、企業規模、そして企業文化によって異なる。後は、自分で考えるしか無く、この講演では、今後のアクションプランのための「**気づきの眼（芽）**」を持っていただければと思う。

自己紹介－１

■東京海上火災保険（株）に入社し、システム部門において、大規模プロジェクトの企画・開発に携わる。システム開発・運用の専門グループ会社への出向経験も持つ。

■2000年以降は、情報システム部門の専門職として、システムリスク管理、品質管理に従事する。その後、活動の範囲を広げ、IT企画部の専門次長以外に、ホールディングカンパニーの文書管理部、東京海上日動火災保険（株）の経営企画部、文書法務部、リスク管理部の各部署を兼務する。

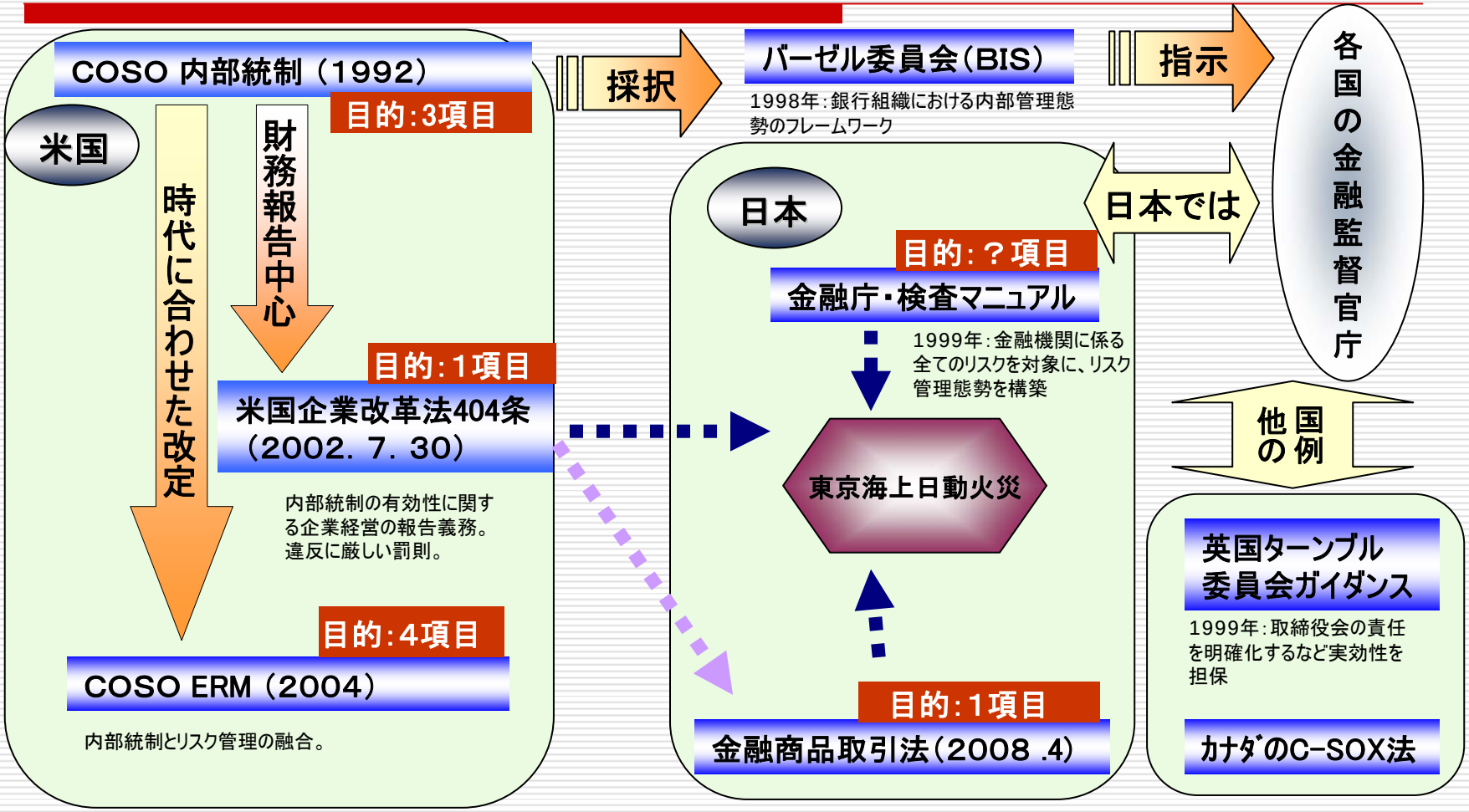
■2006年6月末で退職したが、2007年1月からは、同社の「特別任命参与」として、社長の経団連活動などの支援に従事。

■（社団法人）日本情報システム・ユーザー協会（JUAS）の主席研究員
企業情報マネジメント研究会の部会長、調査部会の委員
JIPDECのITSMS（ITサービスマネジメントシステム）技術専門部会の委員

■著書　：「システムリスクに挑む」（共著：社団法人金融財政事情研究会発行）
システムリファレンスマニュアル（SRM）第2巻」（第5章）「リスク管理内部統制」

COSOフレームワークの展開の流れ

自己紹介ー2



CIOとは何か（機能は？何が必要か）

Ⅱ－1

2005年、CIOの機能に関する経産省からのヒアリングに対して、東京海上日動火災保険の考え方を、以下の2点について、説明した。

- CIOの機能・・・　他のラインや経営層との連携と調整

- CIO的立場として必要なもの

CIOの機能
他のラインや経営層との連携と調整

Ⅱ－2

システムがブラックボックスなのではなく、縦割りの商品や社内規定がブラックボックスを生む。
全取締役が、担当分野の透明性を上げていくことが、それを支えるシステムの透明性に繋がり、コンセプトの明確なシステムに結実していく。

ITのことはIT担当役員に任せるということでは、実効ある経営戦略の策定が出来ない時代。縦割りの判断に横串を入れた経営判断が出来るように、
取締役全員がCIOという認識が大切

部門毎（アプリケーションオーナー）の精緻主義によってシステム化の要件が肥大化する。過剰な開発を抑止するためには、精神論だけでなく、仕組みが大切。(例として、プロジェクト策定時の第三者による審査・評価のスキーム導入、予算のしばり　など)

ＣＩＯ的立場として必要なもの

Ⅱ－３

IT＝経営を掛け声だけで横串の入った経営体制を作るのは至難の技
如何に、このコンセプトを、全経営陣の「肚に落とし、実行する」かがCIOの最大の使命

IT技術よりも、まず経営の課題に対する幅広く深い見識を持つことが前提
その上に、経営とITを結びつける洞察力と理解力が重要
有能な技術者からのヒントを生かせるセンスがあれば、IT技術の専門的知識を自ら持つ必要はない

絡み合った分かりにくい問題を、自分の言葉で分かり易く納得させる能力
現状をビジュアルに説明することで初めて「肚に落とす」ことが可能

企業IT動向調査2007の概要

Ⅱ－4

アンケート調査

定点観測＋重点テーマ（11月に実施）

- ユーザー企業IT部門3962社対象
- 有効回答：802社（有効回答率20%）
- 経営企画部門：4180社対象
- 有効回答：805社（有効回答率19%）

インタビュー調査

重点テーマで12月～1月に実施

- ユーザー企業IT部門長：40社
- 情報子会社役員、ベンダー：10社
- 内部統制担当部門：5社

調査委員会、調査部会による分析

JUAS調査の特徴

- 94年度以来過去13年間継続して実施、経年変化をふまえた分析
- アンケートとインタビューの複合効果
- IT部門だけでなく、利用部門にも調査
- 年度別に、重点テーマを設定

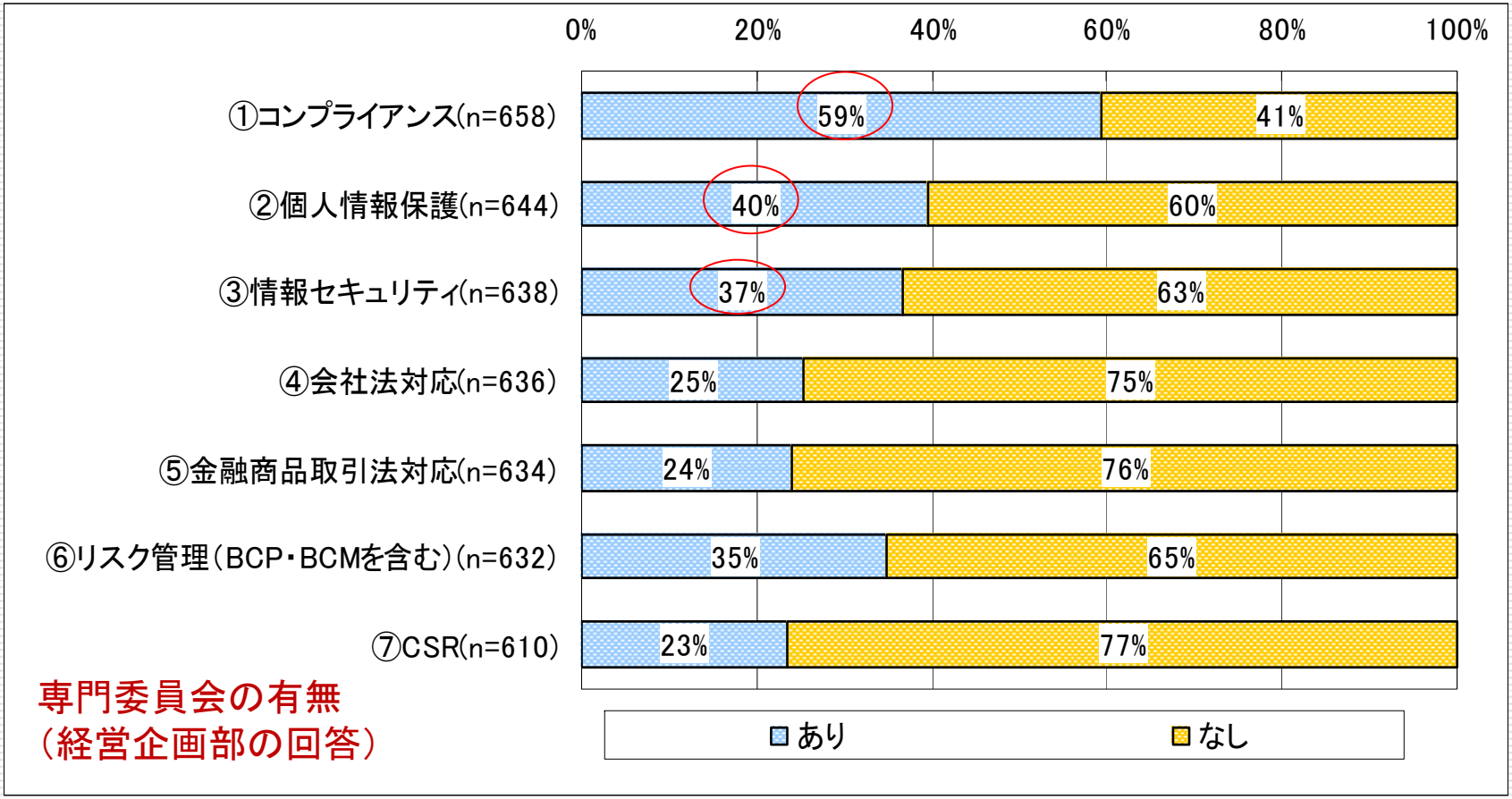
調査報告
2007年4月発表

＜重点テーマ＞

- 情報システムの信頼性
- 内部統制・リスクマネジメント

リスクマネジメントの課題については、専門委員会の形態が日本企業に浸透し始めている

Ⅱ－5



専門委員会の有無
（経営企画部の回答）

IT部門はリスクマネジメント課題の推進部隊の常連の脇役に納まる

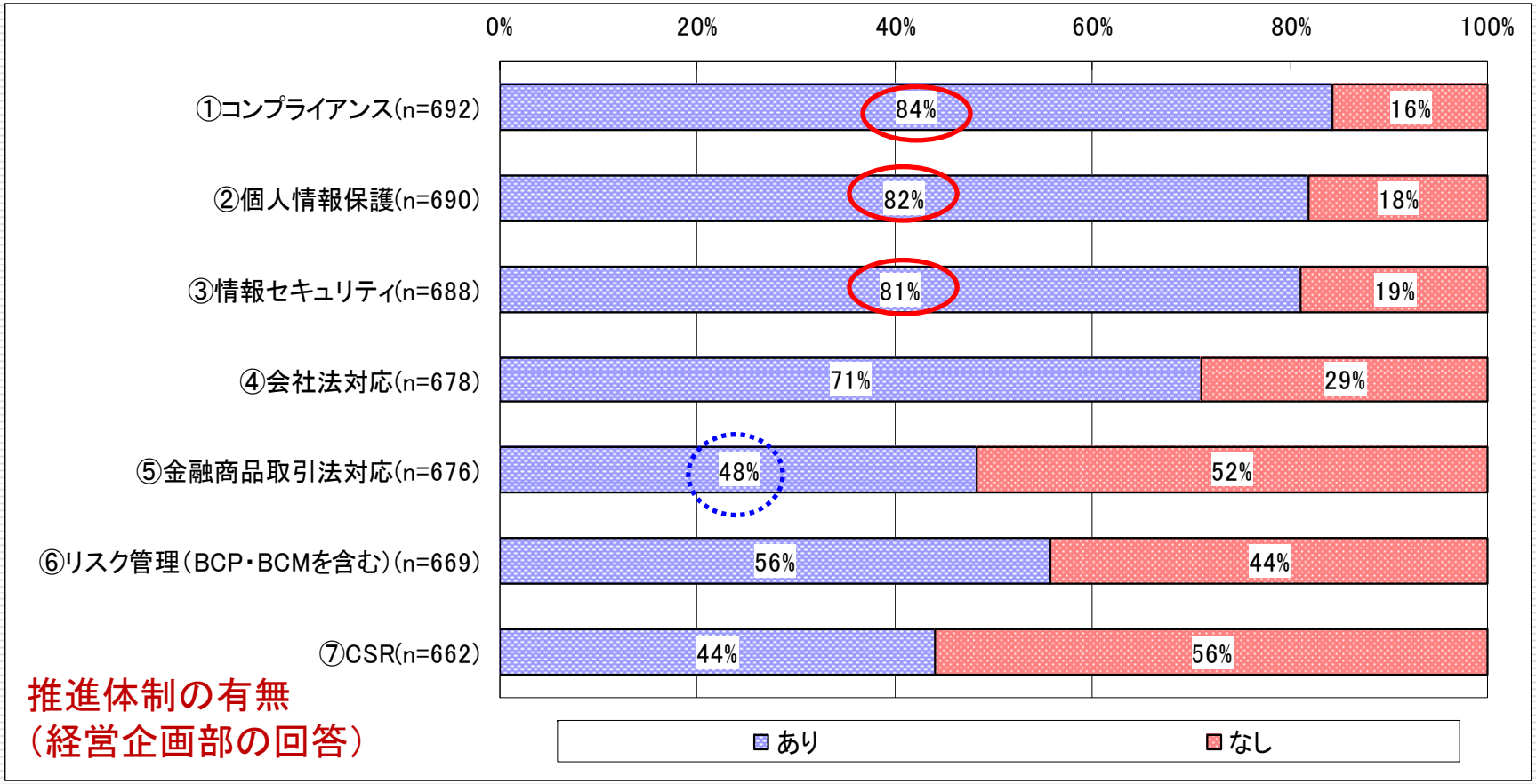
Ⅱ－6

主管部門とともに推進する部門

	IT部門の回答	経営企画部門の回答
コンプライアンス	第1位（32％）	第4位（16％）
個人情報保護法対応	第1位（57％）	第1位（40％）
金融商品取引法対応	第1位（42％）	第3位（30％）
会社法対応	第1位（31％）	第3位（17％）
リスク管理	第1位（41％）	第2位（24％）

「金融商品取引法対応」の推進体制を設けている企業はまだ半数

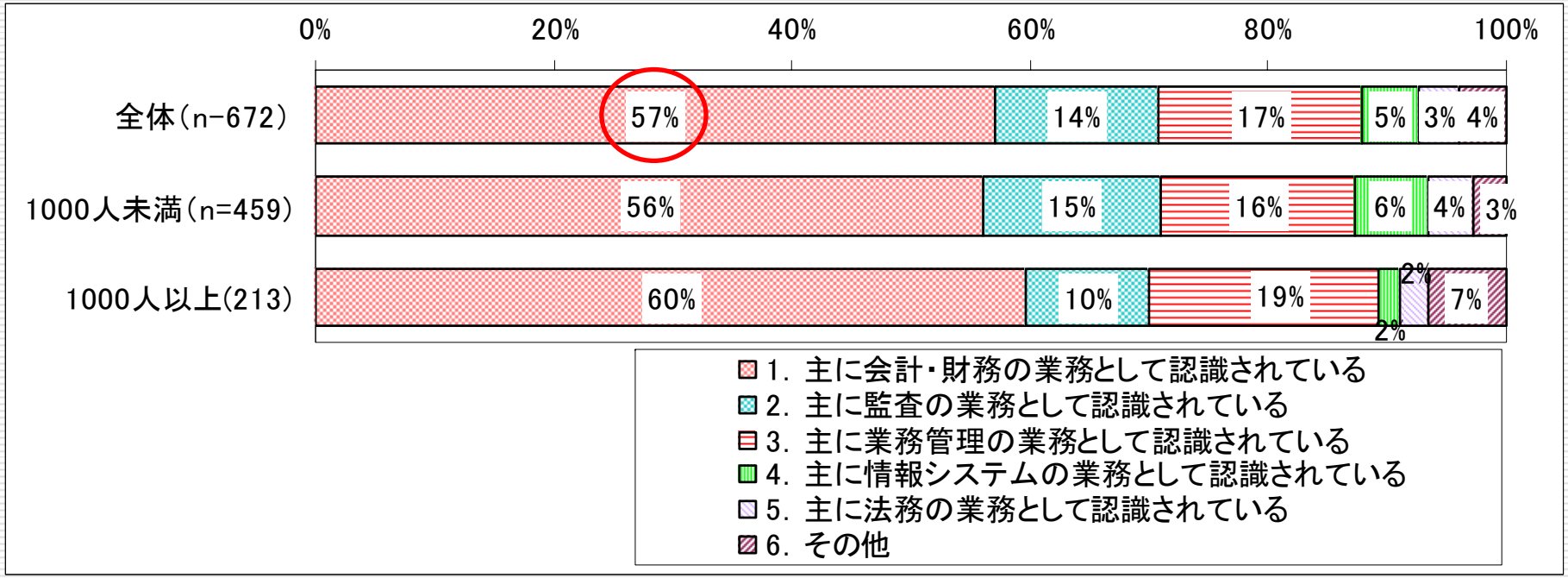
Ⅱ－7



推進体制の有無
（経営企画部の回答）

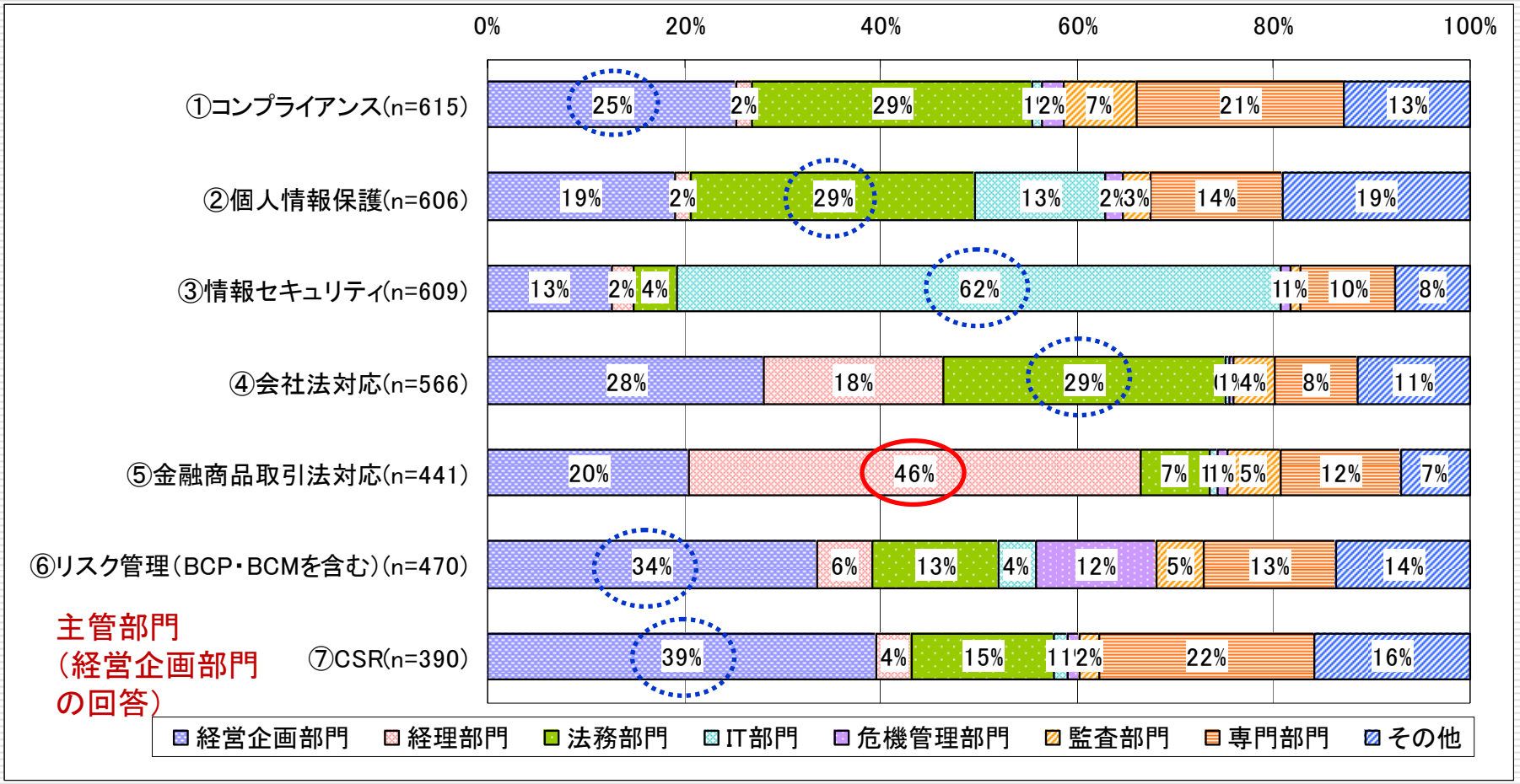
金融商品取引法対応は「主に会計・財務の業務」との認識

Ⅱ－8



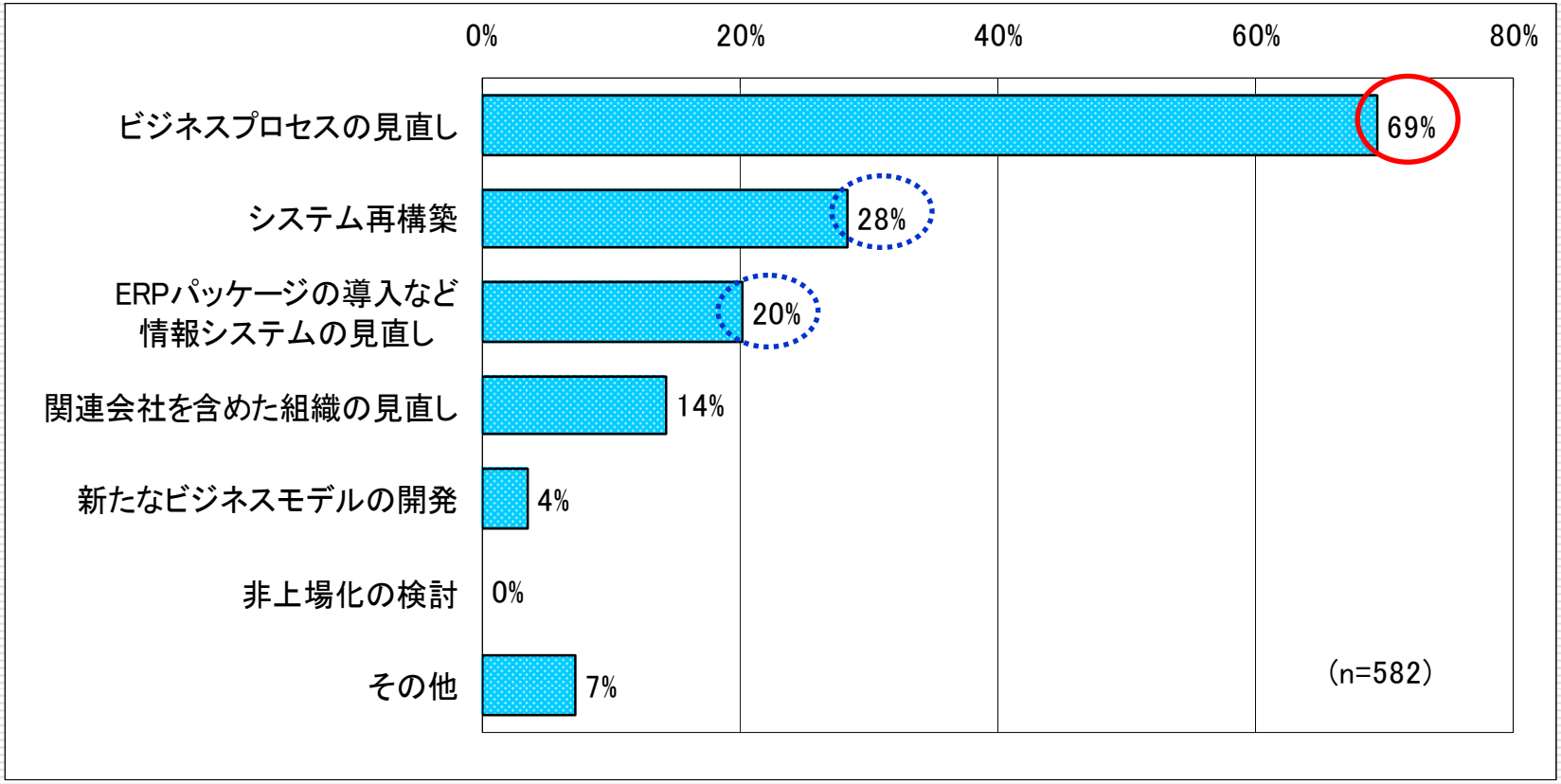
金融商品取引法対応の主管部門は経理が半数
経営企画部門が全てのテーマに目を光らせる

Ⅱ－9



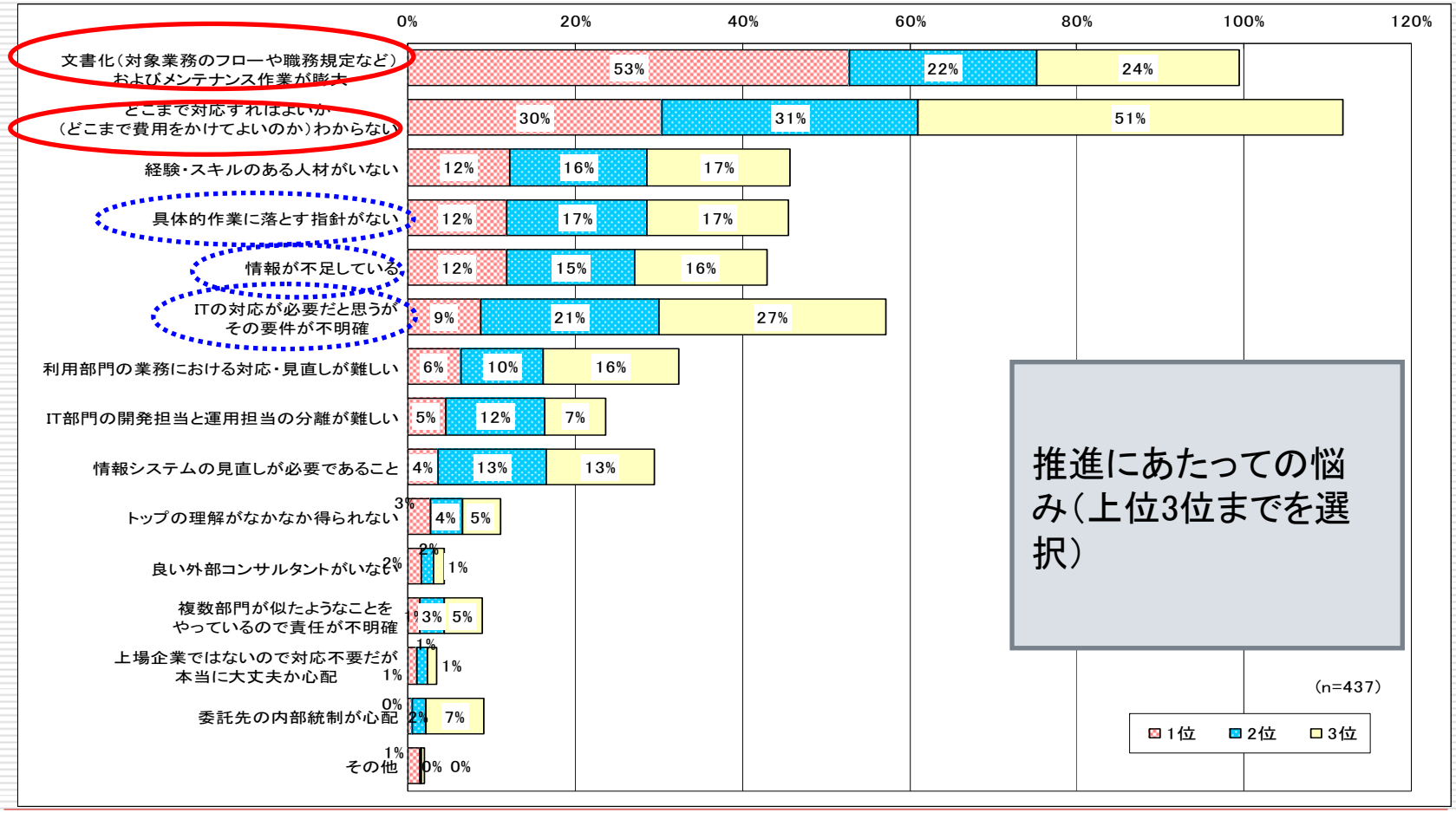
日本版SOX法対応と同時進行の施策は
ビジネスのプロセスの見直しが7割と１位

Ⅱ－10



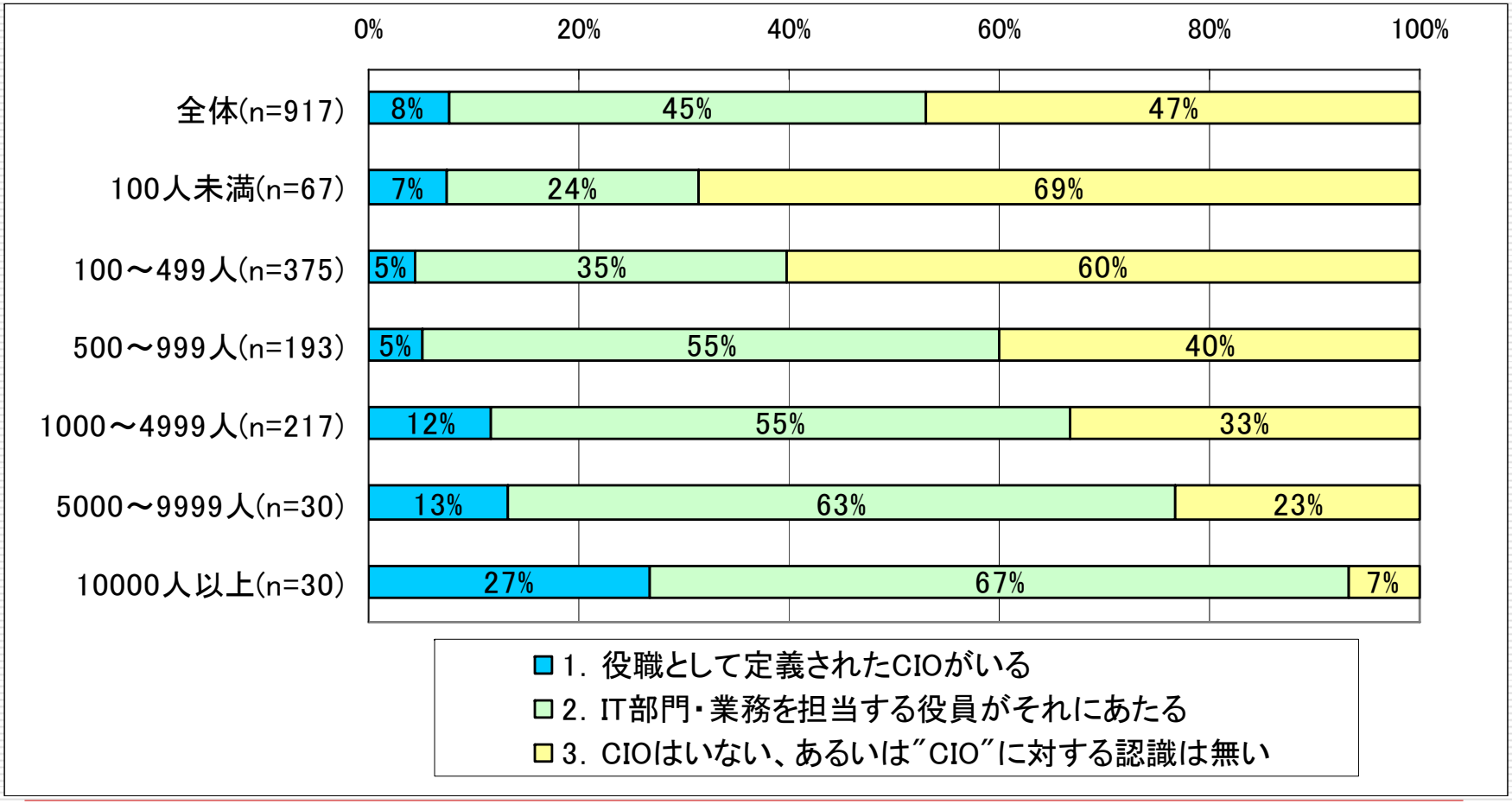
各企業の進行状況にバラツキはあっても、根源の悩みは「どこまで対応すればよいか分からない」

Ⅱ―11



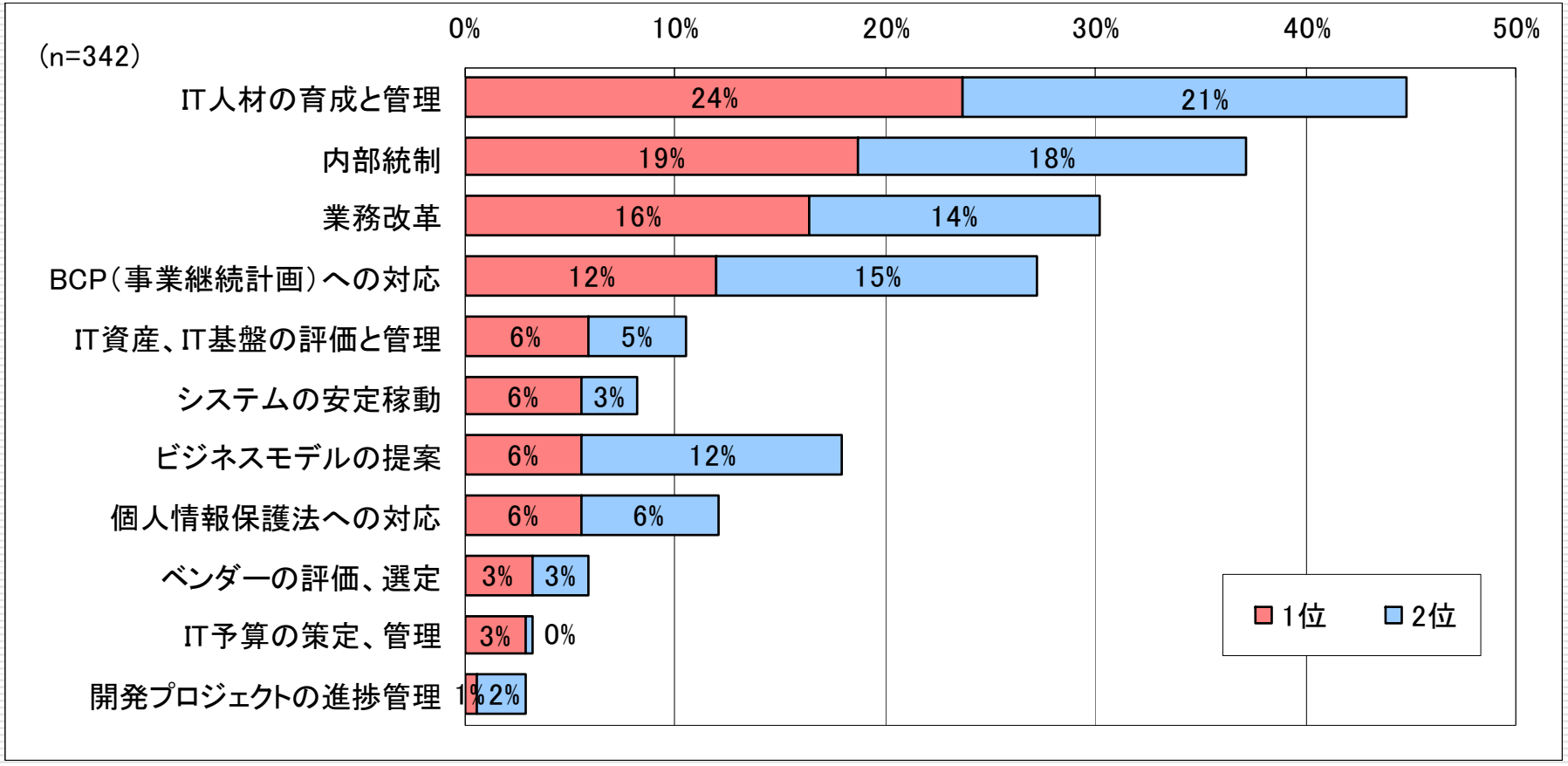
企業規模別CIOの有無（企業IT動向調査2006）

Ⅱ－12



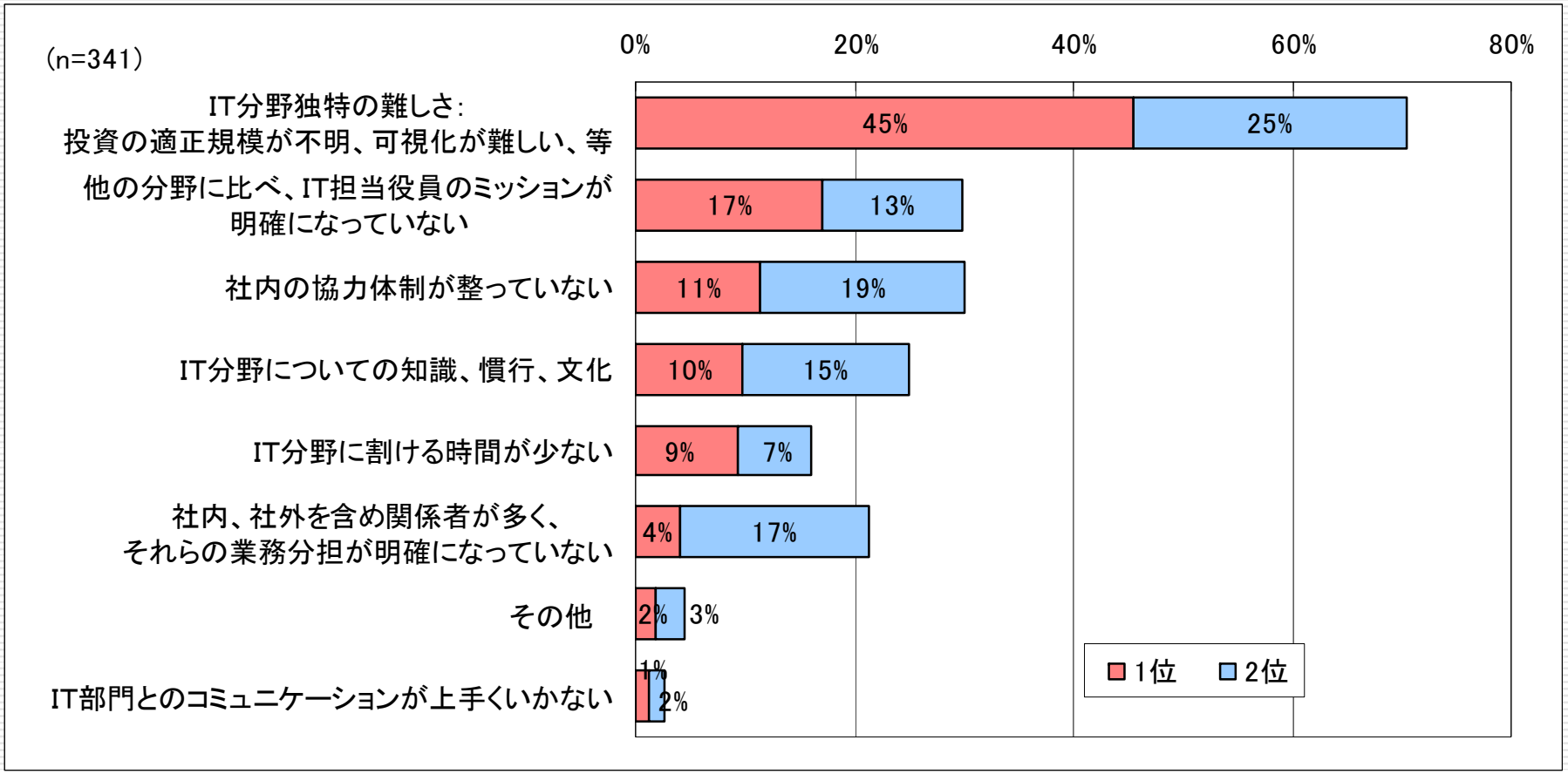
（企業IT動向調査2006）
CIOが不安に感じている点

Ⅱ－13



（企業IT動向調査2006）
CIOとしての責任を果たす上で悩んでいる点

Ⅱ－14



インタビュー結果 ： リスクマネジメント課題におけるIT部門の役割と課題（1）

Ⅲ－1

主管部と共に推進する部隊として大きく位置づけられるのは良いが、職責を果たすべく、経営的な観点から、リーダーシップをとれる人がIT部門には非常に少ない。

共に推進するというよりも、主管部から言われたことを忠実に実行する優秀な部隊というのが、まだまだ実状である。

内部統制・リスク管理に従事してきた人は、地味な人が多く、かつ団塊の世代の退職などもあって、体制から外れていっている。そういう人材が圧倒的に少なくなっている現状に反比例して、経営からのニーズが急速に高まってミスマッチが発生している。

求められるのは、IT部門の従来の業務とは異質で、SE的なことよりも、法的な素養である。監査法人の人材育成が喫緊の課題として話題になるが、企業内のキーパーソンの育成の遅れの方が、企業にとっては深刻である。

インタビュー結果 ： リスクマネジメント課題におけるIT部門の役割と課題（2）

IT部門が全般統制について責任を持ち、ビジネスプロセスについては、プロセスオーナーが責任を持つという分担にしている。しかし、ビジネスプロセスが全部分かっているプロセスオーナーはいないし、システムとの絡みは更に分からないので、IT部門が全面的にサポートしなければいけない局面の割合が極端に多い。

こうした背景から、先行実施したパイロット業務を通して、IT部門がプロセスの不備などを指摘できるようになってきた。更に、COBITやITILなどのワールドワイドのフレームワークをIT部門は持っており、どのあたりに過不足があるのか、自社のプロセスはかくあるべきという観点から、海外拠点も含めて内部統制を随分と見直した。今や、IT部門は、主役に変われる脇役としての実力を備えてきたと考えている。

インタビュー結果 ： 対応における悩み

日本版SOX法がスタートする局面では、経営としても初期の投資を認めてくれるが、この課題は積み残しを抱えながら、それ以降毎年改善を図って充実していかなければならないと考えている。却って、初期費用に多額のものを積むよりもIT部門への総額の投資を数年間で山崩しして経営の承認を得ておくことが、経営からのリクエストに真に応えられるものと考える。

過熱した日本版SOX法投資の風潮に踊らず、控え目にしていく。

そのためには、IT部門が自力で出来るものは実施する姿勢を示していくことにしている。

主管部は経理部なので、経理部と監査法人との打ち合わせ結果を踏まえた指示が出されれば、IT部門としてその対応をすると思えば、敢えて悩む必要は無いと考えている。

その分、限られたソースをより効果的に投下するためには、IT部門が責任部門となる他の経営課題（例えば情報セキュリティなど）にもっと検討のロードを注力したい。

インタビュー結果 ： 先進企業は「したたかに、そして真剣に」取り組んでいる

Ⅲ－4

システム側の投資については、日本版SOX法のための投資ではない。

今までの流れでずっと階段を上がってきたところの最終段階を、少し前倒しで 実施できるようになったということである。

元々、やらなければならない課題があったが、日本版SOX法が見直しのきっかけとなり、必要があれば「錦の御旗」として使えることがメリットである。

各社各様であるが、例えば、「開発・運用の標準化」「ドキュメント整備」「セキュリティ、ログ監視、データ保存」、「EAの導入」「COBITの導入」「ITILの導入」など。

時間が無いのは大きな悩みではあるが、今後の展開に不安を持っていないのは、既に、監査法人・コンサルタントと打ち合わせを持って、IT全般統制に致命的な欠陥は無い、有ったとしても、緊急の要員・大きなコストにはならないという感触を得ているからである。

IT部門から見た場合に、以下のプラスがあった。

「業務とシステムの意味づけが明確になった」「改善案の創出の情報源になった」「基幹業務再構築時の改善のネタにつながる項目が出てきた」等

私からのメッセージ　－１

Ⅳ－1

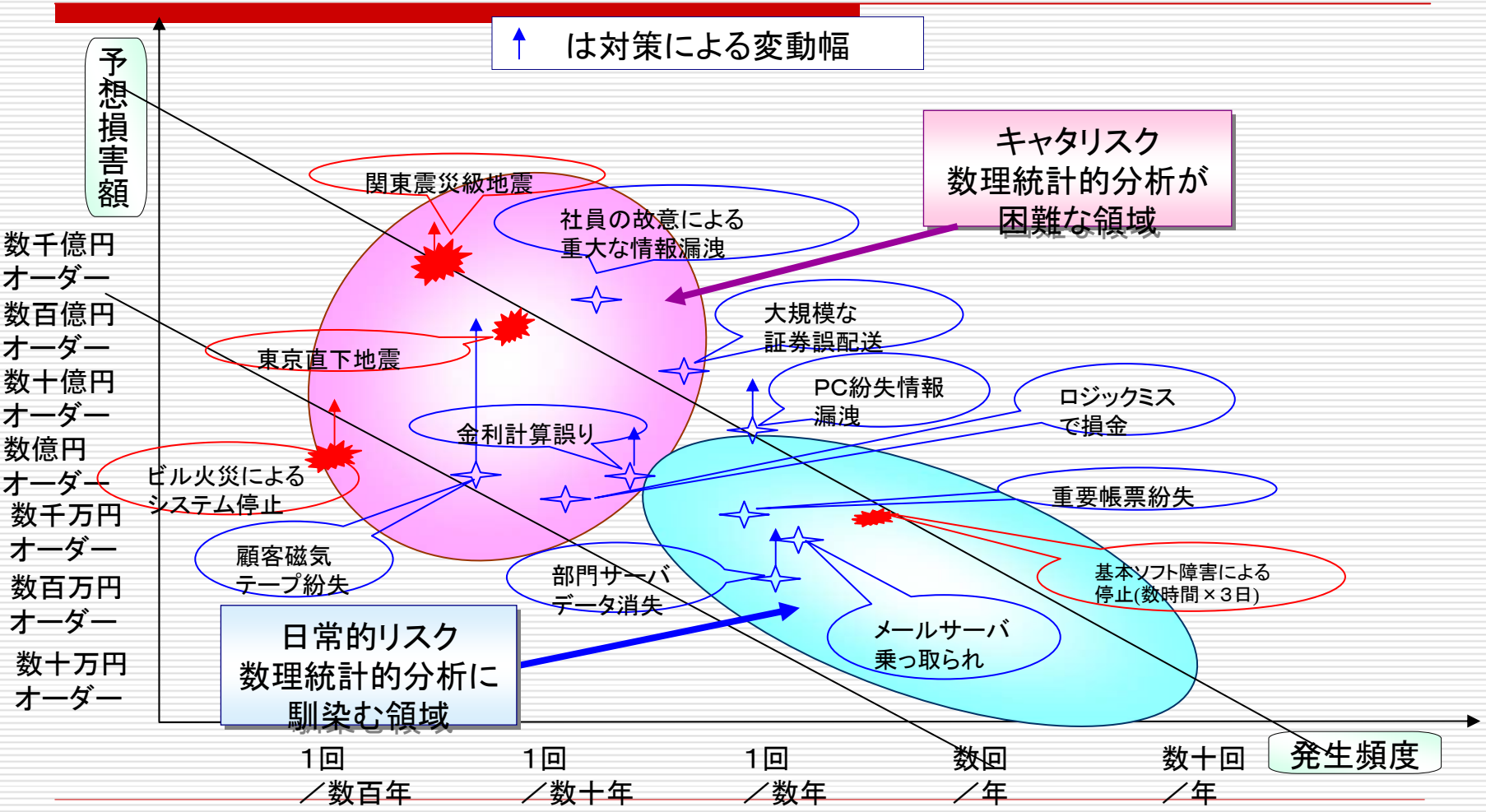
■日頃からリスクを認識・分析・評価する訓練をする。

◎リスク管理は難しい話ではない。
必要なのは、「リスク認識の感性を磨くこと」、「素因数分解の思考パターンを身につけること」、「リスクシナリオの作り方を学ぶこと」、「１枚の絵でリスクの全体像を描いてみること」などの訓練で育っていく。
→　企業のシステムリスクの全体像を描いてディスカッションすると、企業としての共通の認識が生まれる。

◎経営には、日頃から、リスクに関する情報を提供して、身近に感じてもらう。
日々新聞報道される事件などは、検討の宝の山である。
例　：　ジュリアーニ（元ニューヨーク市長）のリーダーシップの発揮の仕方

ITリスクマップによる全体像(シナリオ分析結果)

Ⅳ−2



私からのメッセージ　－２

Ⅳ－３

■「身の丈に合った」内部統制で「全体最適」を目指す。

◎各企業が培ってきた良き企業文化を失わないためには、どうしたら良いかを工夫する。

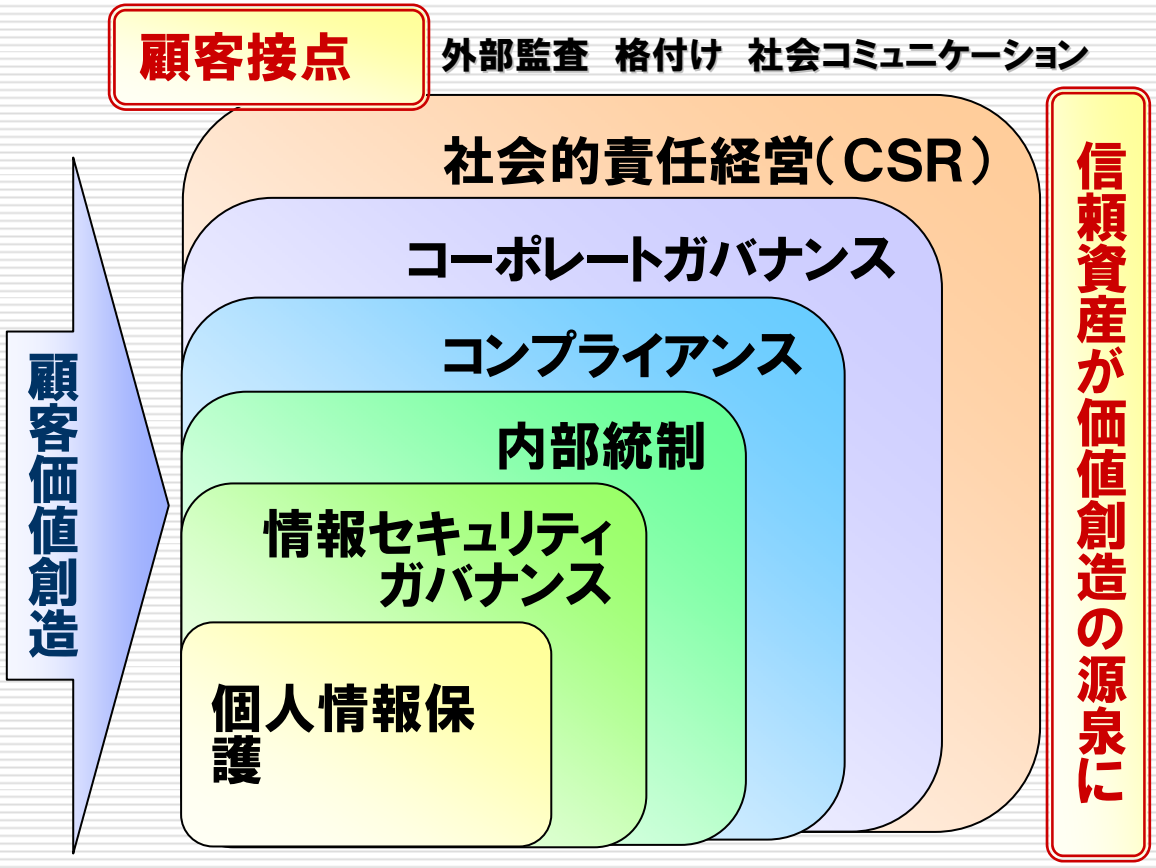
◎CIOインタビューで良く耳にする、監査人からの「重箱の隅をつつく指摘」への対応をこのまま続けていくのか。切磋琢磨とは、磨き合って成長していくことから、磨り減らして駄目になっていくことになっている。

◎相互に依存している委員会や様々な組織が、経営課題の解決に当たると、「現場への複数の指示による混乱」、「対策の重複感・度重なる変更」、「兼務者の負担感」などで、本来の業務改革のスピードが発揮できなくなる。
→　次の図で、経営課題の整理をするポイントを説明する。

◎自主点検が自社の身の丈に合ったリスク管理の原点になる。
自主点検は、自社の現状を見ることから始まる。まずは、「直面する課題に即して考える」ことから始め、「外部監査の指摘を受けてのレベルアップ」まで、順次拡大していく。→　内部統制は進化していく。そのスタートに立つ。

【経営課題の全体像】自社の企業風土に合った概念を定義して「信頼のガバナンス」の全体像を1枚で描く

Ⅳ－4



出典：野村総合研究所　村上輝康理事長の東京大学での講義資料

- 包含関係を理解し、
- バラバラな活動ではなく、
- 企業として整理された活動
- 　が必要。

- あらゆるリスクをERM戦略に統合していく。
- 「リスク管理文化」を定着させないと、スピード経営が行なえない。

- 目の前にある気がついた欠陥の応急措置だけを繰り返していても、企業を本質的に改革することは出来ない。

私からのメッセージ　－３

Ⅳ－５

■内部統制を進化させていく仕組みを構築する。

◎内部統制進化論　・・・　日本はどれだけ米国から遅れているのか。（進んでいるのか？）　具体的に数値で示してほしいという質問にどう答えるか。
既に、スパイラルを回しながら、米国は進化している。

◎JUASの研究部会の今年度のテーマを、問題意識の共有を目指したディスカッションに置いた。　→「自ら考える」「情報を発信する」「共有する」

◎リスク管理の原点は、Y2Kにある。
イソップの「ウサギとカメ」に譬える。「愚直に取り組む」カメではなく、器用にこなしていく日本の企業はうさぎの状態。或る意味では頭は良いが、結局は、「ピーク性のお祭り騒ぎ」、「トータルでは却ってコストがかかる」、「社員は疲弊する」などのマイナスが大きい。

◎標準化していくことが、将来の負荷軽減には大切である。
COBIT、ITILなどは、グローバル企業で導入され始めている。

◎「システムリスクに挑む」のときには、COBITを事務プロセスにまで適用できないかという問題意識もあった。（事務とITは裏腹の関係にある）　→理想

私からのメッセージ　－４

Ⅳ－6

■経営との懸け橋となるシステムリスク管理の専門家を育成する。

◎IT人材の育成が、CIOの最大の課題であるのと同じで、リスク管理の人材育成も喫緊の課題になっている。

◎求められるのは、複数の分野にまたがる事案を見る「複眼を持つ」人材。

→ 技術のみのプロではなく、ビジネスプロセスを見渡せることも大切。このため、分かりやすいプロセス・フローを描くことの訓練等も必要。

◎孤独で理解してくれる人も少なく、孤独で疲れる業務なので、トップの支援が大切である。

→ 優秀できちっとした仕事をする人を割り当てるが、生真面目だと、際限のない指摘に過剰反応して精神的な弱さが露呈。部門長には、愚痴・悩みを聞くことの大切さを再認識してもらう必要がある。

◎九州大学大学院（工学部）で、システムリスク管理からみた「企業の社会的責任とコンプライアンス」を講義して感じたこと。

→ テレビゲームのRPGで育ったこともあって、シナリオ分析でシミュレーションする感性は若い人達の方が磨かれているかも知れない。

最後に：CIOはIT統制にどう取り組んでいるか

Ⅴ－1

■CIOは多岐に渉る経営課題を抱えている・・・「全体最適の仕組み」を考える。

課題は常に複数（内部統制も一つ）ある。先進企業は、関連する経営課題と絡ませて、工夫しながら「元々やらなければならない課題」を実現しようとしている。

■IT統制とは　・・・　科学的なアプローチで経営の数値化を推進する。

◎リスク管理の基本は難しくない。「リスクベース・アプローチ」、「全体像を1枚で描く」、「素因数分解」、「数値化」等の基本的な考えで、問題を明らかにしていく。

◎現場にとっては、IT統制によって、不祥事件が起きても「説明責任を果たせて身を守れる」仕組みを構築する。

■取り組む・・・　自社の「身の丈に合った仕組み」を考える。

講習会やセミナーでの情報を鵜呑みにして、自社に導入しようとしても、大量の輸血をするようなもので、経営も現場も担当者も拒否反応で病気になる。自分の口から栄養のある食材を取って咀嚼して力をつけていくしかない。

ITガバナンス協会　CIO ITガバナンスセミナー

CIOはIT統制にどう取り組んでいるか

～したたかに、そして真剣に～

講師への連絡先

takahashi.hidetoshi@juas.or.jp