『ITアウトソーシングで失敗しない SLAチェックポイント294』

2007年11月29日

ソリューションサービス事業委員会
IT内部統制専門委員会

委員長
NEC　川井 俊弥

JEITA

2006年度の委員会活動から

- 『IT内部統制の為の統制項目表』の活用について
- 内部統制に関わる2006年度の市場動向

JEITA

2006年度「IT内部統制専門委員会」の活動

- 企業において関心が高い‘内部統制’をテーマとして、新たに「IT内部統制専門委員会」を設置。
- 2006年度は、以下のテーマで活動を開始。

1. 「IT内部統制の為の統制項目表」の作成
   情報システム部門の重要業務にフォーカスし、
   そのリスクに応じた‘統制項目’を整理

2. 内部統制に関わる市場動向調査
   内部統制への取り組み関する企業動向を調査。
   2007年度以降も経年での調査を実施予定

JEITA

「IT内部統制の為の統制項目表」(*)の作成目的

(*)以下、「IT内部統制項目表」と略す

目的

- 企業に向けたIT内部統制におけるリファレンスの提示。
  「アプリケーションソフトウェアの調達と保守」、「変更管理」、
  「システムセキュリティの保証」、「データ管理」の4プロセスを対象。
  79管理項目、132統制項目を提示。

対象

- ITサービスの改善、品質向上を目指すIT部門
- ITに関わる業務部門

JEITA

「IT内部統制項目表」の活用対象とメリット

(1)「IT部門」における活用メリット

- 特に重要と考えられる4つのプロセス「アプリケーションソフトウェアの調達と保守」「変更管理」「システムセキュリティの保証」「データ管理」を対象としており、社内のITサービスの改善、品質向上活動に向け、効率的な統制項目洗い出しの際の参考として活用できる。
- 統制を実現するための業務プロセスや規程、ルール作りの参考として活用できる。
- ITツール利用による効率化のヒントとして活用できる。

(2)「業務部門」における活用メリット

- 業務部門の役割/責任分担や、実施項目の明確化の参考として活用できる。
  (システム要件の明確化、設計内容のレビュやテスト結果の承認など)

「 IT内部統制項目表」 項目の説明

#	項目名		説　明
1	システム管理基準 項目番号		「システム管理基準」に記載されている項目番号。 わかりやすくするため、項目番号の下に内容を追記
2	管理項目		「システム管理基準」の管理項目の内容
3	発生リスク		管理項目に記述された活動がなされない場合に発生が予想されるリスクの例
4	統制活動	統制項目	IT内部統制における統制項目の例
5		統制のタイプ	統制活動にITツールが適用可能な場合は「自動」に〇。人手を介する場合は「手動」に〇
6		利用ITツール	統制活動に利用することが出来るITツールの名称
7		規定類等	統制のための基準、ルールなどを記述するドキュメント例
8		実施基準対応	実施基準との対応付け

JEITA

「IT内部統制項目表」(サンプル)

(1)アプリケーションソフトウェアの調達と保守

統制項目の洗い出しの参考

利用できるITツールは何か？

統制のために作成が有効なドキュメントは何か？

			統制活動									
				統制のタイプ						基準との対応		
		生リスク		自動	手動	IT		守	用	確保 安全性	契約管理	外部委託
Ⅱ-03-0-(01)(企画)調達	調達の要求事項は、開発計画及び、ユーザニーズに基づき作成し、ユーザ、開発、運	構築する情報システムの機能、性能、品質等の要求が、計画とおりに達成 とが きない。	調達要求事項は開発計画やユーザーニーズを基に作成する。		○		・システム開発規定 ・システム計画書 ・要求定義書 ・保守/運用規定	○	○			
			調達要求事項は、ユーザー部門責任者及び、システム部門責任者(企画/開発／保守運用)のレビュ・承認を受ける。	○	○	・文書管理 ・ワークフロー ・ID管理		○	○			
			調達要求事項レビュ実施記録を作成し、保存する。	○	○	・文書管理 ・ワークフロー ・ID管理 ・ログ管理		○	○			

業務(ユーザ)部門の役割を例示

ご参考　利用ITツール（サンプル）

名称	ヨミ	意味
文書管理	ブンショカンリ	文書（情報、データ、ドキュメント、ファイル等）に対する更新履歴、承認、最新版の管理、公開（配布）を管理し、体系的に保管するツール。
ワークフロー	ワークフロー	文書作成、承認、回付、文書保管等の業務の流れをサポートするツール。
ID管理	アイディー カンリ	利用者を特定する為の番号、パスワードおよび権限等の発行・変更・削除等の管理を実行するためのツール。
ログ管理	ログカンリ	情報（データ）、ソフトウェア、ネットワーク等に対するアクセス及び、システムの運用の履歴を収集・集計・参照・分析するためのツール。
コーディング チェック	コーディング チェック	ソースコードの静的な正しさをチェックするツール。
開発テスト	カイハツテスト	開発したプログラムのテストを支援するツール
プロジェクト 管理	プロジェクト カンリ	プロジェクトの管理運用（進捗、リソース、時間等）支援を行うツール
バックアップ	バックアップ	ソフトウェア、データを自動的にバックアップを保存し、業務継続性をサポートするツール。
暗号化	アンゴウカ	情報の盗難・悪用を防止するために、データの暗号化（並べ替え）を行うツール。

JEITA

ご参考　規程類等（サンプル）

名称	ヨミ	意味
システム開発規程	システムカイハツキテイ	システムを開発するにあたり、その開発プロセス（要件定義、システム設計、プログラム設計、単体テスト、結合テスト、総合テスト、保守/運用、システム移行など）や手順について組織として守るべき方針やステップを規定した文書 。
要求定義書	ヨウキュウテイギショ	システム化要件を記述したドキュメント。主にシステム化目標、システム化対象範囲、費用対効果、適用業務要件、処理要件、品質要件や他システム要件、ハードウェア／ソフトウェア要件、システム設計の全体条件などが記述した文書
システム計画書	システムケイカクショ	要件定義書に基づいてシステム全体の概要を記述した文書。システム設計書に記載される内容を大枠で記述している。実際には、システム設計書で代用される事もある
プロジェクト計画書	プロジェクトケイカクショ	プロジェクトにおけるシステム化の目標／対象業務とその機能、システム構成の方針、開発範囲と開発スケジュールの大枠、開発の推進体制や開発方法／管理方法など、当該プロジェクトの基本方針や全体構想および開発方針といった基本的な計画を記述した文書
システム設計要綱	システムセッケイヨウコウ	要求定義書に基づいて、システムの構造を決定し、各サブシステムとの人間業務処理とのインタフェースを記述する手法を定義した文書。システム設計を行う上で、考慮すべき事項（フェールセーフ設計、二重化など）の定義を含む。
システム設計書	システムセッケイショ	要求定義書に基づいて、システムの構造を決定し、各サブシステムとの人間業務処理とのインタフェースを詳細を記述した文書。システム移行･運用方針を示し、結合テスト、総合テスト、システム移行の計画を記述した文書を含む
プログラム設計書	プログラムセッケイショ	システム設計書に基づき、各サブシステムのコンピュータの処理のソフトウェア仕様（プログラム構成、プログラムの基本仕様、実行形態など）を記述した文書

JEITA

内部統制に関わる2006年度の市場動向

調査方法：民間企業にアンケートを実施し全体傾向を把握(定量)、
更に個別企業へのヒアリングによって詳細状況を調査(定性)

■アンケート（定量調査）

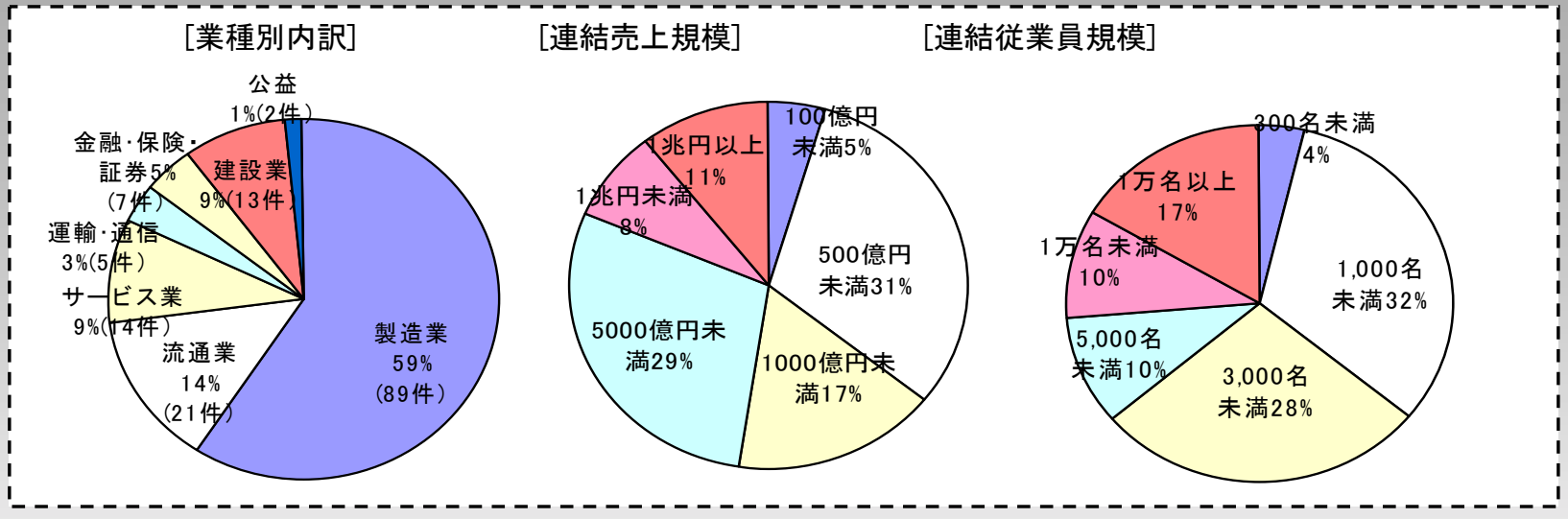
✓期間：2006年10月下旬～2006年12月下旬
✓方式：アンケート依頼書の送付
✓対象企業数：送付552社（有効回答151社）
✓主なアンケート項目：
　企業プロフィール
　内部統制全般への取り組み状況
　IT内部統制全般への取り組み状況
　ITベンダへの期待・要望

■ヒアリング（定性調査）

✓期間：2006年12月下旬～2007年1月下旬
✓方式：面談によるヒアリング
✓対象企業数：6社
✓主なヒアリング項目：
　内部統制全般への取り組み状況
　IT内部統制全般への取り組み状況
　ITベンダへの期待・要望

JEITA

【アンケート】回答先の基本属性：有効回答数151件



●本調査対象の母集団は国内株式市場上場全企業（3,870社）に対し、無作為抽出による
アンケート調査を実施。最終的な有効回答は151社。

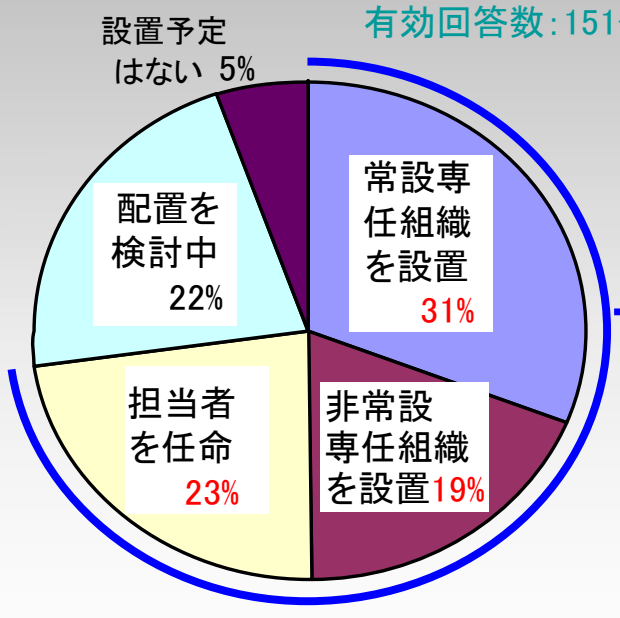
●ユーザの属性は、以下の通り。

- 業種区分では全上場企業の構成比と同様、製造業及び流通業で過半数を占める。
- 連結売上規模、同従業員規模については、特に大規模企業に集中することなく
バランスのとれた構成であった。

JEITA

【アンケート】内部統制関連組織・担当設置状況

「内部統制関連組織設置」と「担当者任命」を合わせると、
7割強の企業で、すでに何らかの組織的な対応を行っている。



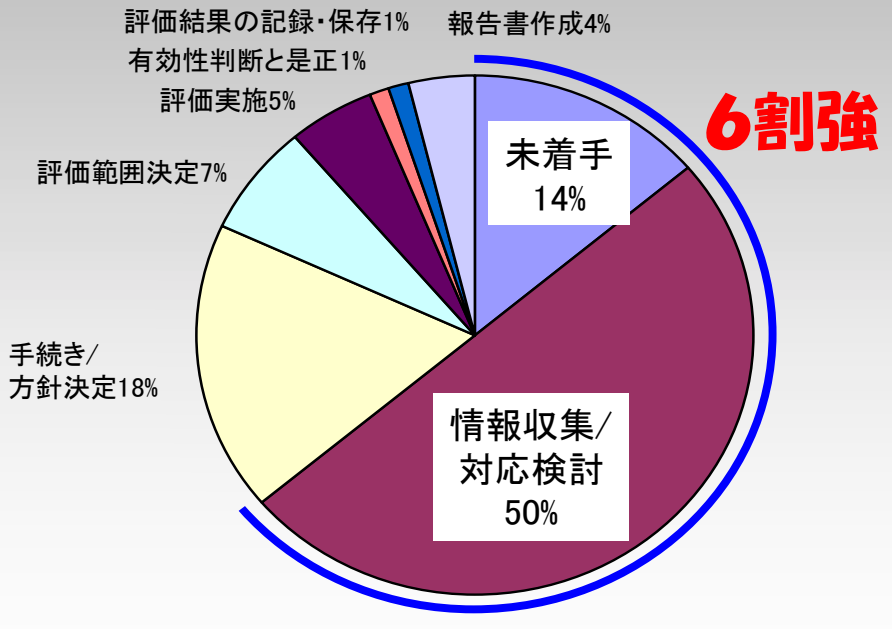
組織的対応（7割強）

- 常設選任組織を設置
- 非常設選任組織を設置
- 担当者を任命

【アンケート】IT部門のIT内部統制に関する取り組み状況

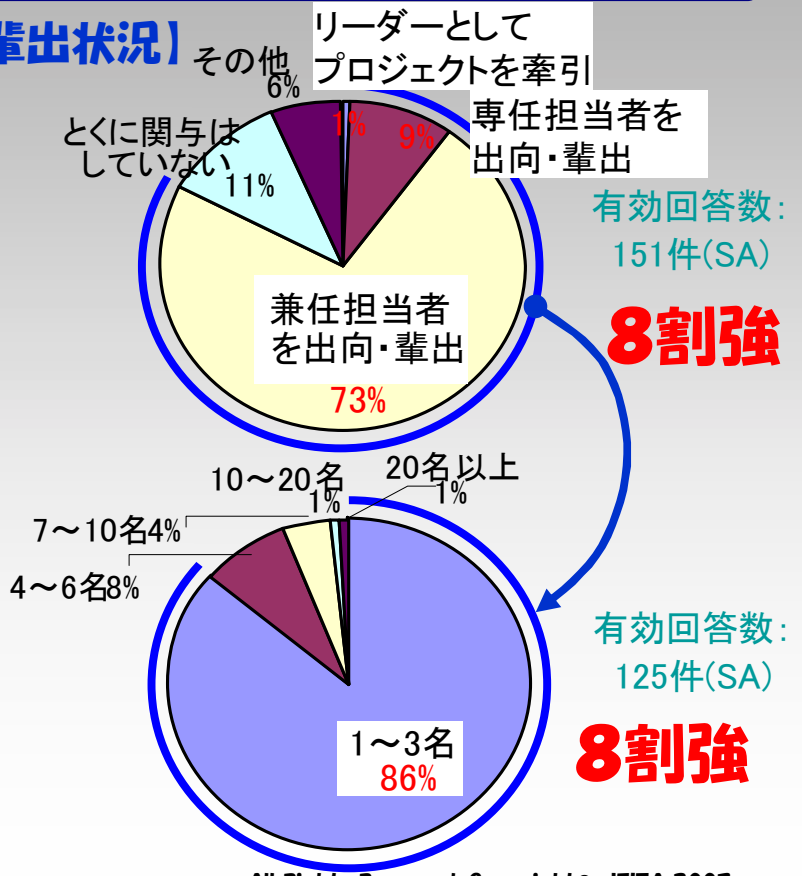
IT部門のIT内部統制に関する取り組み状況は、6割強の企業が「未着手」もしくは「情報収集・対応検討」段階。但し、8割強の企業では全体の内部統制強化活動にIT部門が関与しており、その出向・輩出人員数は「1～3名程度」が8割強となる。

【IT内部統制取り組み状況】



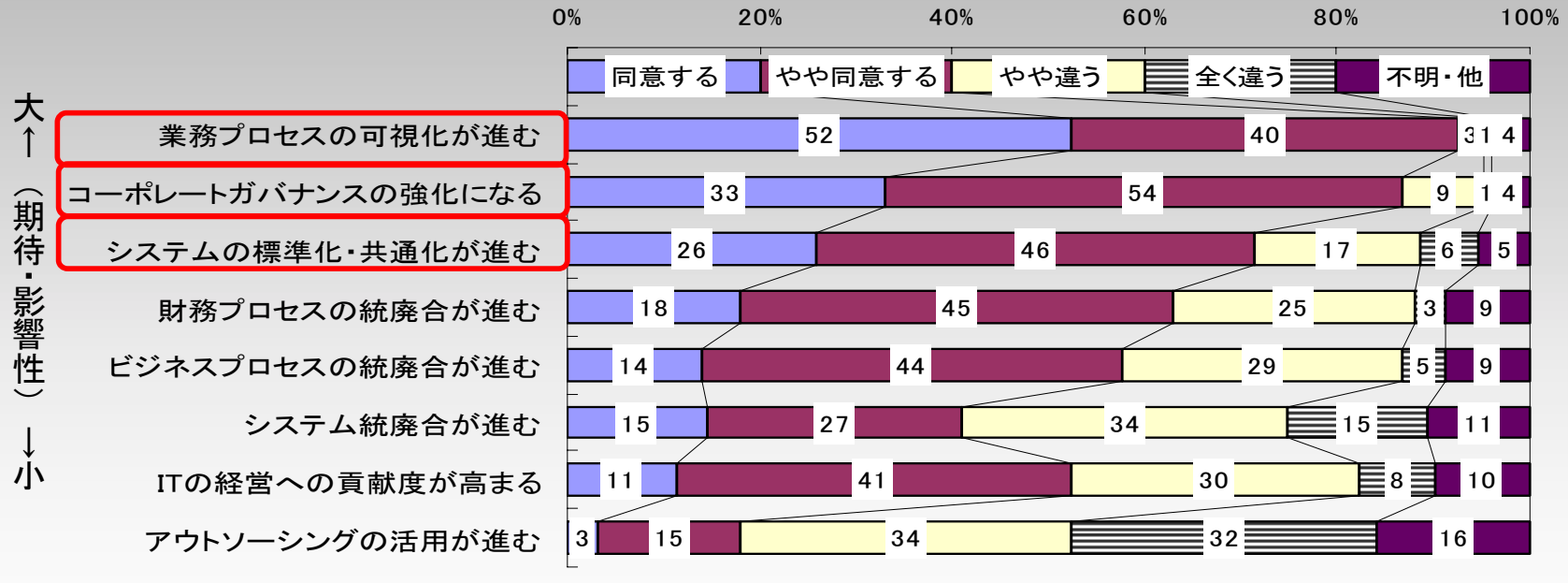
有効回答数：151件(SA)

【IT人員輩出状況】



【アンケート】日本版SOX対応に関する期待・影響予想

「業務プロセスの可視化」「コーポレートガバナンス強化」に対する期待が大きい。「システムの標準化・共通化推進」がそれに続く。

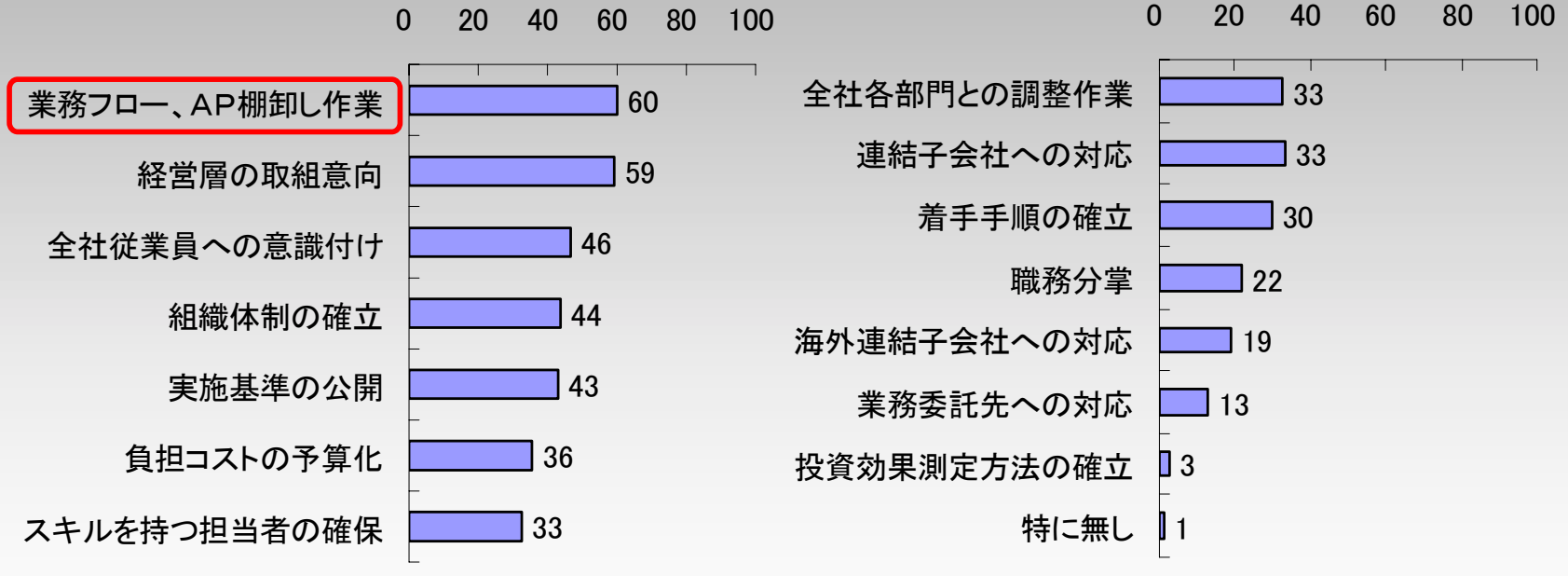


n=151単位：%(SA)

JEITA

【アンケート】IT内部統制推進上での阻害要因

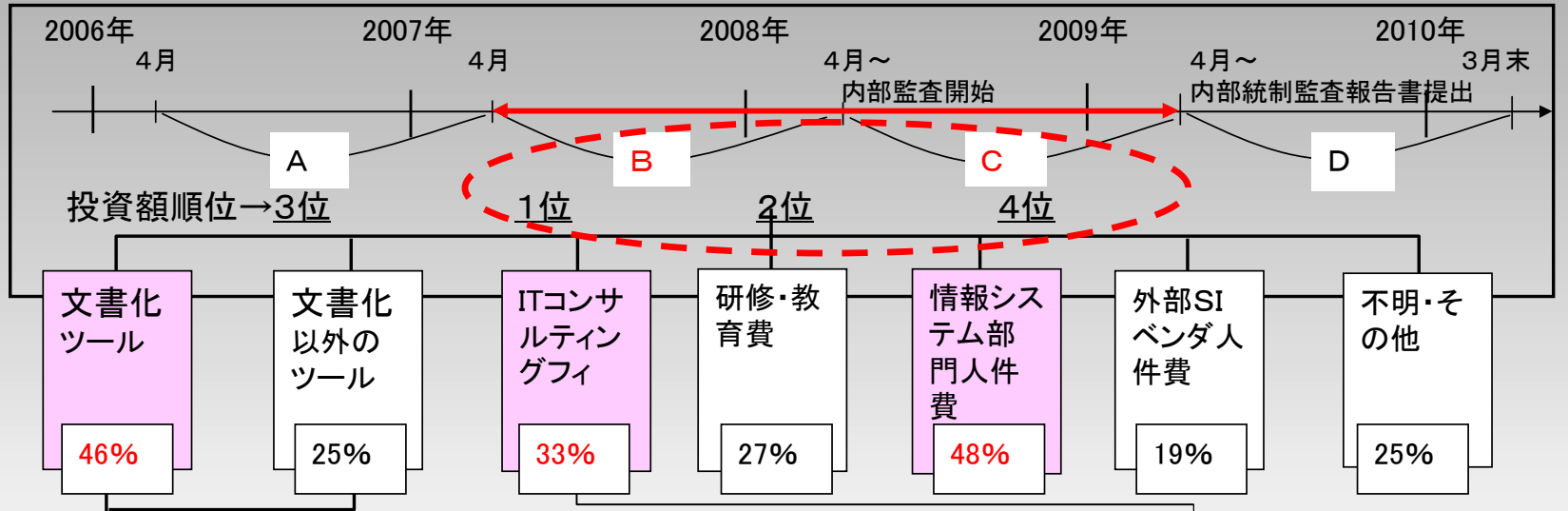
業務フロー作成や、アプリケーションの棚卸し等といった、
「現状把握」を課題として認識している企業が多い。



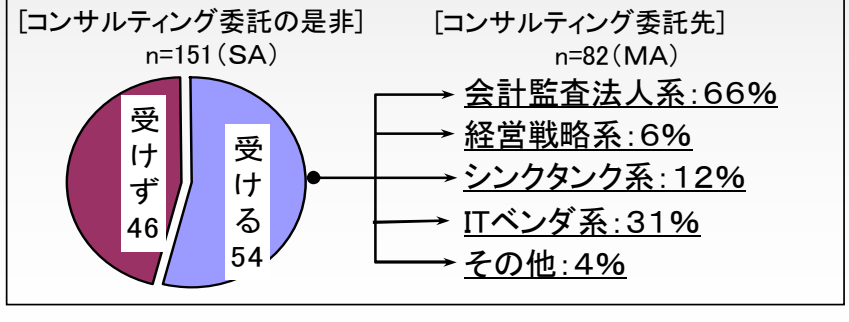
n=151単位：%(MA)

【アンケート】IT内部統制関連の投資意向

IT内部統制関連投資は、2007年度を1位、2008年度を2位とする意見が多い。



- 導入有望性：1位「文書化ツール」
- 導入有望性：2位「運用管理ツール」
- 導入有望性：3位「セキュリティ関連ツール」
- 導入有望性：4位「ERP」
- 導入有望性：5位「開発支援ツール」



JEITA

【ヒアリング】実施先の基本属性

対象企業（業種）	連結売上高／連結従業員数	上場市場	連結子会社数（国内／海外）	内部統制対応組織状況		
				専任組織	統括部門	担当者数
流通・サービス業	500～1,000億円未満／1,000～3,000名未満	国内	―（―）	担当者のみ任命	経営層	約10名
製造業（A）	1兆円以上／1万名以上	国内、米国、その他、海外	約380社（約190社）	常設専任部門設置	内部監査部門	100名以上※兼任含
製造業（B）	1兆円以上／1万名以上	国内	約80社（約30社）	常設専任部門設置	経営層	12名
製造業（C）	1,000～5,000億円未満／5,000～10,000名未満	国内	約30社（約20社）	常設専任部門設置	内部監査部門	8名
製造業（D）	100～500億円未満／300～1,000名未満	国内	1～5社（1～5社）	常設専任部門設置	経営層	1～3名
製造業（E）	100～500億円／1,000～3,000名未満	国内	1～5社（―）	非常設専任部門設置	経理部門	7～10名

JEITA

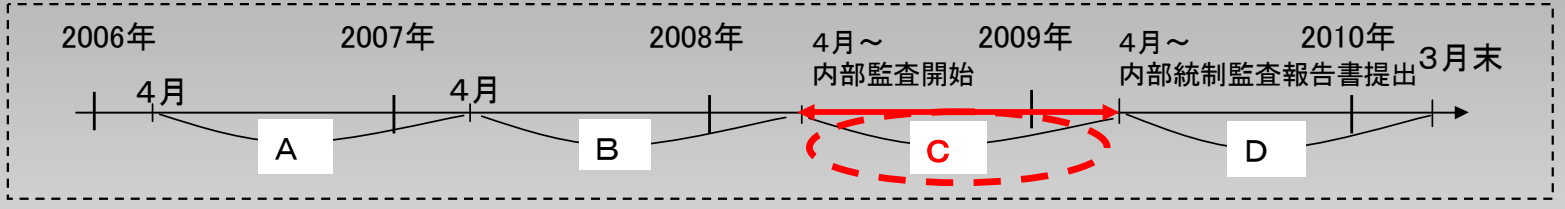
【ヒアリング】ITへの対応に関する進捗状況

ITへの対応に関する進捗は、ほとんどの企業がStep3(手順・方針決定)以降のフェーズに入っている。

日本版SOX対応フェーズ	Step1	Step2	Step3	Step4	Step5	Step6	Step7	Step8
	未着手	情報収集・検討	手順・方針決定（パイロット含）	評価範囲決定	評価実施（文書化・評価）	有効性判断と是正	評価結果記録・保存	内部統制報告書作成
流通・サービス業								○
製造業(A)								○
製造業(B)				○				
製造業(C)			○					
製造業(D)		○						
製造業(E)			○					

【ヒアリング】IT内部統制関連投資に関する見解

ヒアリング結果では、IT内部統制関連投資は2008年度を1位とする意見が多い。



	投資コストの多い順				主な理由・コメント
	1位	2位	3位	4位	
流通・サービス業	C	D	B	A	米SOX法に対応済みで投資の山は小さくPDCAを回せば以下の通り。ただ日本の企業は全般的にプロセス・ドキュメント整理でBが山となる感。
製造業（A）	C	B	A	D	CはB、Aのサンプリングテストなどで発生するシステム改訂費が主に発生する。なお、波形はCが100ならA＋Bで10程度の差がある。
製造業（B）	C	B	A	D	内部統制開始初年度までの3年間が準備として投資拡大するとみている。
製造業（C）	B	C	A	D	BとCの順位は逆転の可ありだが、Bで仕組みを作る必要がある。なお、AとDはAの方が工数が多いという点でこの順位となった。
製造業（D）	C	B	A	D	準備を行っても本番一年目のCが、色々な不具合の修正コストで膨らむとみる。故にA，Bは文書化ソフト、Cはシステム修正での投資となる。
製造業（E）	B	C	A	D	Bで既に投資を行うことを決定済み。また、その見直しが入るとCも増加。

JEITA

2007年度の委員会活動から

・内部統制に関わる2007年度の市場動向
・米国SOX法対応企業から学ぶ（米国視察結果より）

「IT内部統制専門委員会」 2007年度の活動方針

2007年度は、「IT内部統制専門委員会」の2006年度成果をさらに充実させる。
主な活動内容としては、以下のとおり。加えて、活動成果の普及活動も展開する。

1)「IT内部統制の為の統制項目表」の対象プロセスの拡充

2006年はCOBIT for SOXをベースに、特に重要性が高いと考えられる「アプリケーションソフトウェアの調達と保守」「データ管理」「変更管理」「システムセキュリティの保証」の4つにフォーカスして『IT内部統制の為の統制項目表』を提供した。
2007年度は、その他のプロセスについての提供を予定。

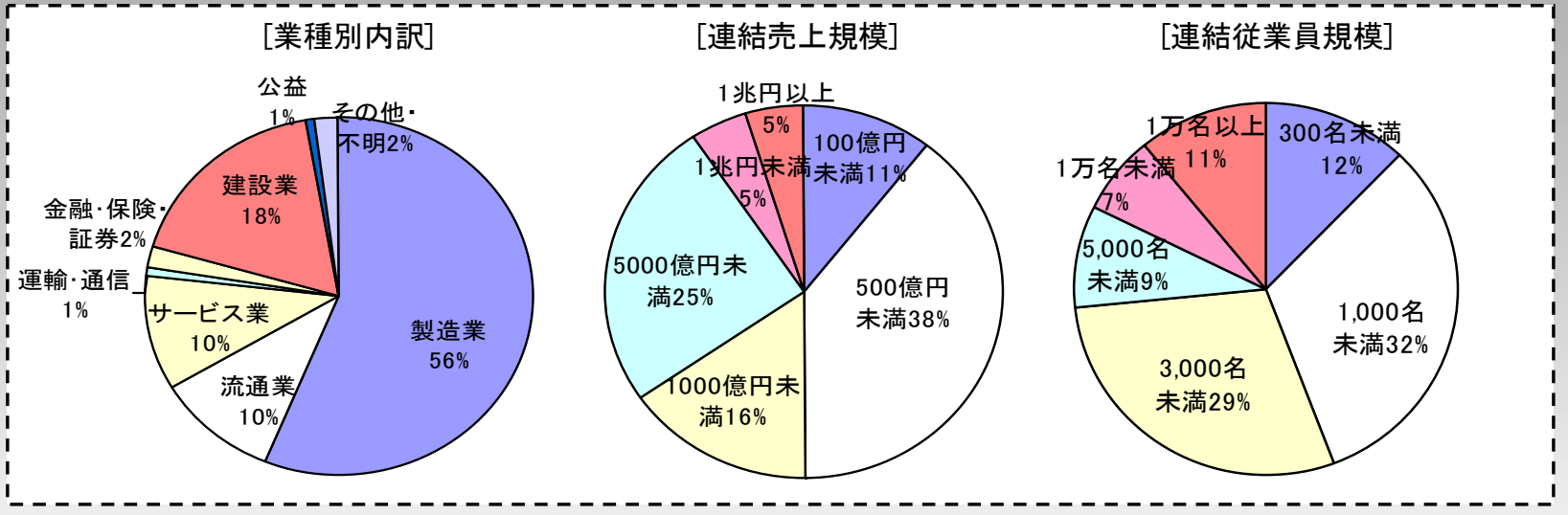
2)「内部統制に関わる市場動向調査」の継続と拡充

2006年度に実施した本調査については、内部統制に関する企業の動向の変化を把握する為に、**2007年度も継続して調査を実施**する。
また、**「米国SOX法対応企業の状況」**など、調査内容の拡充を予定。

JEITA

【速報】2007年度の市場動向

回答先の基本属性（有効回答数147件）



●本調査対象の母集団は国内株式市場上場全企業（3,870社）に対し、無作為抽出によるアンケート調査を実施。最終的な有効回答は147社（昨年調査は151社）。

●ユーザの属性は、昨年度の調査同様バランスのとれた構成となった。

- 業種区分では全上場企業の構成比と同様、製造業及び流通業で過半数を占める。
- 連結売上規模、同従業員規模については、特に大規模企業に集中することなくバランスのとれた構成であった。

JEITA

【速報】2007年度市場動向トピックス(1/2)

- 【IT内部統制取り組み状況】
  - ✓未着手は殆どなく、文書化フェーズ以降に進む企業が約半数に増加している。
    2006年度調査：11% → 2007年度調査：約50%
    ＊しかし、中堅以下の企業の進捗遅れがやや目立ち始める。
- 【IT内部統制関連の投資意向】
  - ✓昨年の調査同様に「2007年度の投資額が最も大きくなる」との意見が多いが、「2008年度の投資額が最も大きくなる」という意見も増加している。
    2006年度調査：19% → 2007年度調査：35%
- 【IT内部統制関連ツール（ソフトウェア）導入状況】
  - ✓文書化ツールは昨年の調査に比べ、「導入済み」の企業が大きく増加している。
    2006年度調査：19% → 2007年度調査：46%
  - ✓内部統制PJ進捗管理ツールは「導入済み」企業は全体では15%と低いが、大手企業は「導入済み」または「１～２年以内での導入可能性あり」の比率が高い傾向にある。
  - ✓ID管理などのセキュリティ関連ツールは、昨年の調査同様に「導入済み」または「１～２年以内での導入可能性あり」の企業は半数を超えている。

JEITA

【速報】2007年度市場動向トピックス(2/2)

- 【監査人との協議の頻度】
  - ✓監査人との協議の頻度は1回／月が約40%と一番多く、意思疎通についても「ほぼ満足」している企業が多い。
    - ＊しかし、小規模企業は監査人との関係について満足度は低い傾向にある。
- 【文書化範囲】
  - ✓文書化範囲を「連結売上高の２／３以上」としている企業は約60%となる。
    - ＊この傾向は、特に大手企業ほど顕著となる。
- 【海外子会社の内部統制】
  - ✓海外の事業所や子会社の内部統制強化推進・モニタリングについて本社が行う企業は66%となる。
  - ✓作成文書の言語は、「日本語」と「英語」がそれぞれ半数を占める。「中国語」や「その他の言語」は15%前後。
    - ＊海外の事業所や子会社を持つ企業は全体の１／３程度

JEITA

米国企業調査の目的

目的

- 米国企業のSOX法対応から学ぶ
  インタビューの結果は米国SOX法対応後の参考事例として、IT内部統制に関する今年度のJEITA報告書でまとめる。
- SOX法対応後に取り組むべき次の課題の整理
  企業がSOX法本番対応で直面した課題や、企業価値向上の為に次に取り組むべきテーマを整理する際の参考とする。

米国企業調査結果の抜粋(1/2)

- 【SOX法対応の効果】
  - ✓販売プロセスは9つあり、セールス・財務・IT部門で異なっていた。
    中には90%のディスカウントも可能なプロセスがあったが、SOX法対応することでガバナンスを強化することができた。
  - ✓ITが重要視されるようになった。
    誰がどの業務を担当し、ITを使っているかを整理した。その結果管理職までが業務とITの関連を把握できるようになった。

- 【SOX法対応の課題】
  - ✓事業部門とIT部門と監査部門の連携。
  - ✓外部監査を入れるとお金と時間がかかる。
    →財務関連の850システムから監査対象250へ絞り込むことで効率化。
  - ✓SOX法への対応が大変で、上場を廃止を検討する企業が出てきている。
    →2007年6月に規則の変更を行っており、その結果を待つ状況(商務省)

JEITA

米国企業調査結果の抜粋(2/2)

●【監査ポイント】
- ✓職務分離 / アクセス管理 / 変更管理 / 開発と運用の分離 / セキュリティの脆弱性対応

＊APの認証をして本番へ適用する正式な開発サイクルがあると、外部監査対応は楽。導入していない企業は大きな負担。

●【CIOの役割】
- ✓CIOは、戦略や全体の状況などを主に見ていればよかったが、SOXが導入されてからは事業のオペレーションや管理に重点が移り、より細かく見る必要が出てきた。
- ✓CEOではなく、CFOへレポートすることが多くなってきている。

●【IT投資】
- ✓当初SOX法に関わるIT投資は多く、新規ITプロジェクトのうちSOX法対応に関連するプロジェクトは50%以上を占めていた。(コンサル会社談)

●【外部委託管理】
- ✓売上1億ドルを超えるアウトソーサには、SAS70のタイプ2を導入してもらった。

JEITA

ご清聴ありがとうございました。

今回ご紹介したIT内部統制専門委員会の報告書（有償）は、
下記問合せ先にてお申し込み頂けます。

社団法人 電子情報技術産業協会（JEITA）
インダストリ・システム部
〒101-0062　東京都千代田区神田駿河台３丁目１１番地
三井海上別館ビル
電話：03-3518-6426　　FAX：03-3295-8724
Eメール：itt3@jeita.or.jp
JEITAホームページ：http://www.jeita.or.jp/japanese/index.htm