『IT内部統制のための統制項目表の活用』
『内部統制に関する市場動向調査結果』

2008年 7月18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
社団法人 電子情報技術産業協会

2007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2007年度の市場動向調査
- 米国企業調査

JEITA
社団法人 電子情報技術産業協会

2007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、2006年度より「IT内部統制専門委員会」を設置。
- 2007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」の拡充
   情報システム部門の業務毎のリスクに応じた
   ‘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に関する企業動向を調査。
   2008年度も経年での調査を実施予定

JEITA
社団法人 電子情報技術産業協会

「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。
  COBIT for SOXの全12プロセスを対象。
  134管理項目、225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
社団法人 電子情報技術産業協会

「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

- COBIT for SOXの全12プロセスを対象としており、
  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）

JEITA
社団法人 電子情報技術産業協会

「 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
社団法人 電子情報技術産業協会

「IT内部統制項目表」(サンプル)

■DS9 構成管理

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？

業務(ユーザ)部門の役割を例示

			統制活動									
		生リスク		統制のタイプ		IT				基準との対応		
				自動	手動				用	安全性	契約管理	外部委託
Ⅳ-06-0-(01) 運用(ソフトウェア管理)	ソフトウェア管理ルールを定め、遵守すること。	ソフトウェアを適切に利用できず、不正を防止できない。	ソフトウェアの管理項目、管理サイクルなど管理事項を明確にするためのソフトウェア管理ルールを明文化する。		○		IT資産管理規程		○			
			ソフトウェア管理ルールは、ユーザ部門責任者および、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	IT資産管理規程		○			
			ソフトウェア管理ルールのレビュ／承認の実施記録を作成し、保存する。	○	○	・文書管理 ・ワークフロー ・ID管理	IT資産管理規程		○			

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。

ご参考　規程類等（サンプル）

名称	ヨミ	意味
構成管理規程	コウセイカンリキテイ	構成管理対象物（対象物の構成及び、最新の状態）を管理するための手続きを規程した文書 ※「IT資産管理規程」に含まれる場合もある。
全社情報管理憲章	ゼンシャジョウホウカンリケンショウ	会社が要請する個人情報、知的財産権、著作権等の情報管理水準（経営的観点での水準／ビジネス遂行の観点での水準／ISO／ISMS等の認証取得等）が定義された文書
情報管理規程	ジョウホウカンリキテイ	「全社情報管理憲章」に基づいて、具体的な手続きや実現するための基準を規程した文書 ・知的財産権、著作権、個人情報等の保護手続き ・各情報のアクセス制限及び利用手続き ・情報管理に対する役割と責任（職務分離）
セキュリティ管理規程	セキュリティカンリキテイ	情報の漏洩や不正利用防止のための手続きを規程した文書（ISMS／ISO、情報漏洩 ）
IT資産管理規程	ITシサンカンリキテイ	情報システム資産に関する利用、取り扱い、構成管理、保守等の手続き規程した文書 ・ライセンス管理の手続き ※「構成管理規程」に含まれる場合もある。
職務分掌規程	ショクムブンショウキテイ	職務上の独立性を保証するための職務分離を規程した文書
記録の保管規程	キロクノホカンキテイ	作成したドキュメントや媒体などを記録するときに守るべき共通の基準を規程した文書
ネットワーク管理規程	ネットワークカンリキテイ	ネットワークに対する運用管理の手続きを規程した文書 ※「セキュリティ管理規程」」に含まれる場合もある 。

JEITA 社団法人 電子情報技術産業協会

内部統制に関わる2007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)
（2006年度より経年で調査）

■アンケート（定量調査）

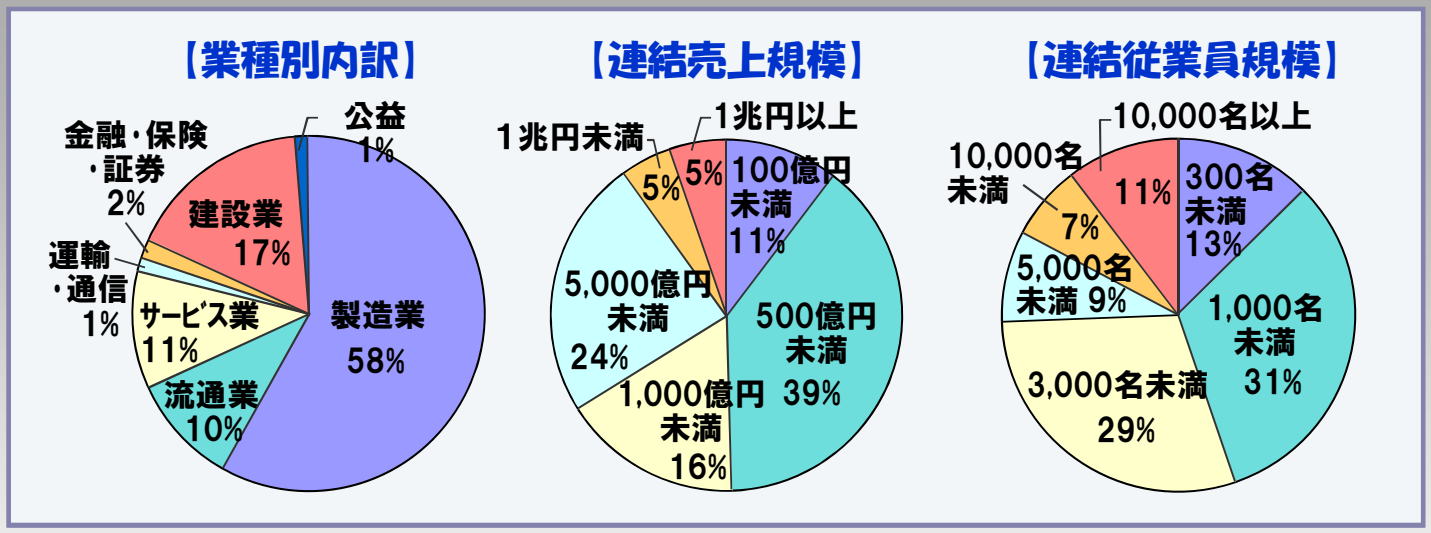
✓期間：2007年10月下旬～2007年12月下旬
✓方式：アンケート依頼書の送付
✓対象企業数：送付530社（有効回答152社）
✓主なアンケート項目：
- 企業プロフィール
- 内部統制全般への取り組み状況
- IT内部統制全般への取り組み状況
- ITベンダへの期待・要望

■ヒアリング（定性調査）

✓期間：2007年12月下旬～2008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 社団法人 電子情報技術産業協会

【アンケート】回答先の基本属性：有効回答数152件

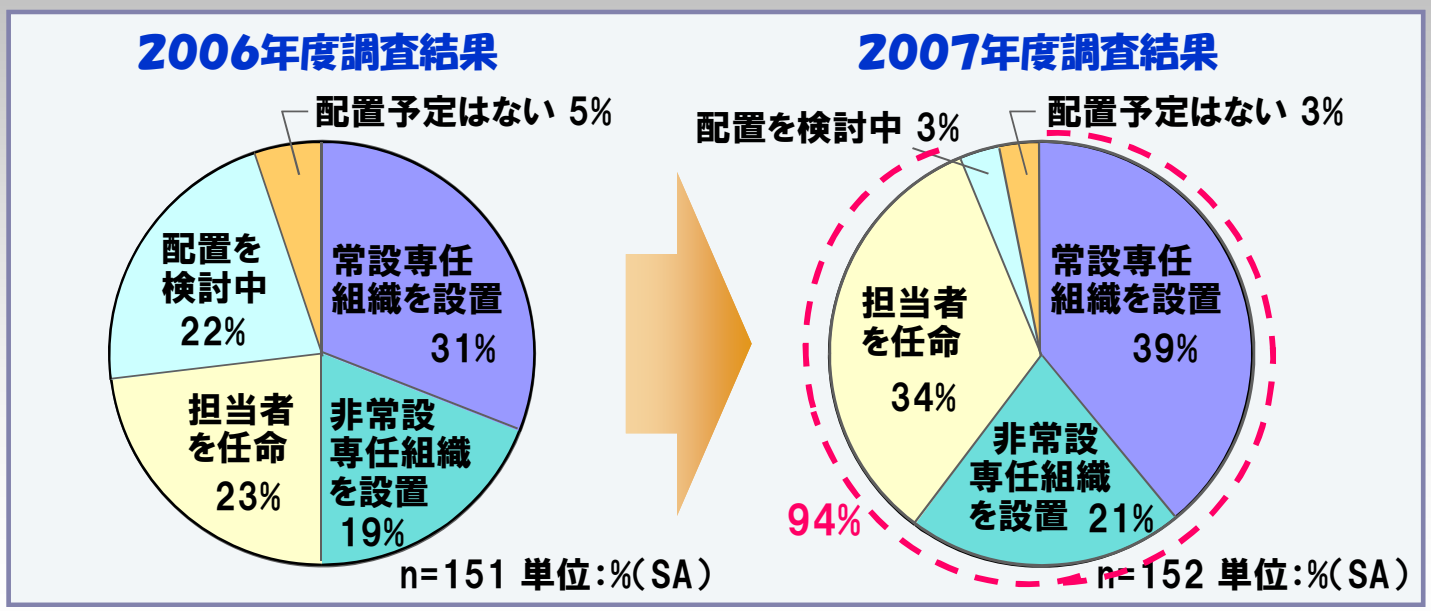


- 本調査対象の母集団は国内株式市場上場全企業（3,947社）に対し、無作為抽出によるアンケート調査を実施。最終的な有効回答は152社。
- ユーザの属性は、以下の通り。
  - 業種区分では全上場企業の構成比と同様、製造業及び流通業で過半数を占める。
  - 連結売上規模、同従業員規模については、特に大規模企業に集中することなくバランスのとれた構成であった。

JEITA 一般社団法人 電子情報技術産業協会

【アンケート】内部統制関連組織・担当設置状況

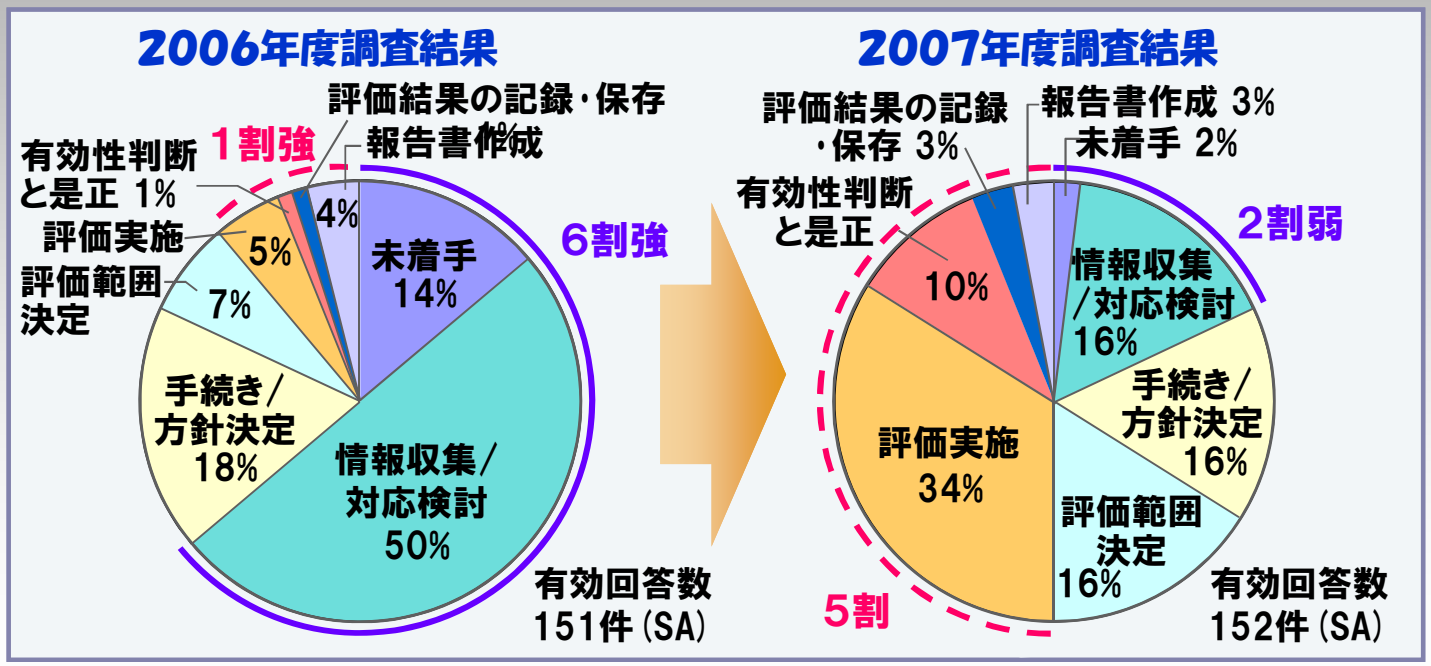
「内部統制関連組織設置」と「担当者任命」を合わせると、
9割強の企業で、すでに何らかの組織的な対応を行っている。



JEITA 一般社団法人 電子情報技術産業協会

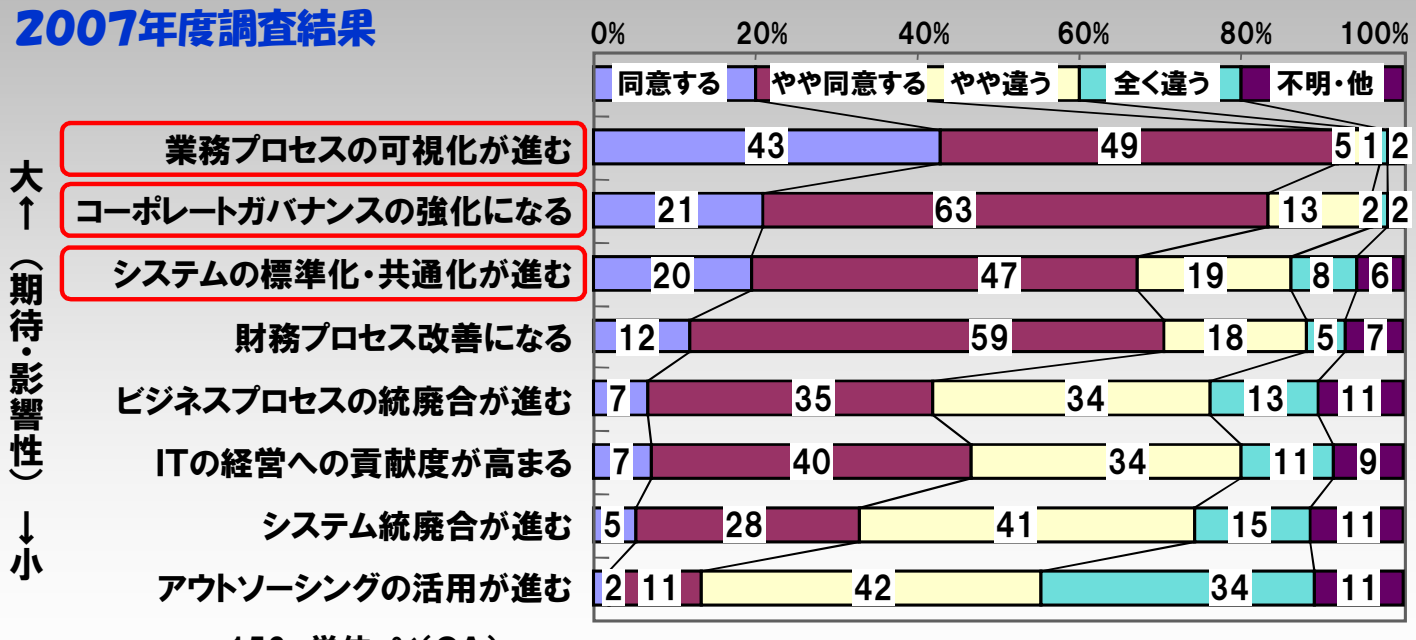
【アンケート】IT部門のIT内部統制に関する取り組み状況

「未着手」「情報収集・対応検討」段階は、6割強⇒2割弱に激減
「評価の実施」以降の段階は、1割強⇒5割に激増



【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。

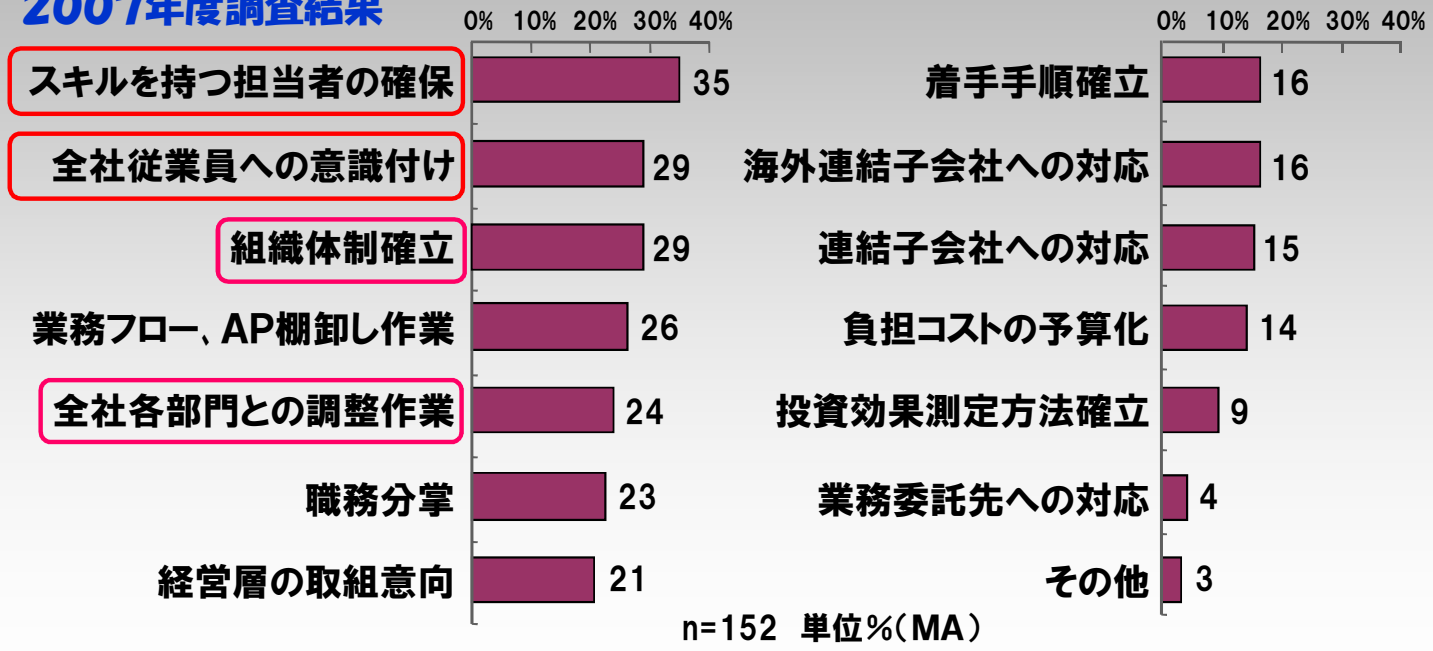


n=152　単位:%(SA)

【アンケート】IT内部統制推進上での阻害要因

経営者に対する啓蒙や情報収集の段階を終え、実施フェーズにおける課題に直面している企業が多い。

2007年度調査結果

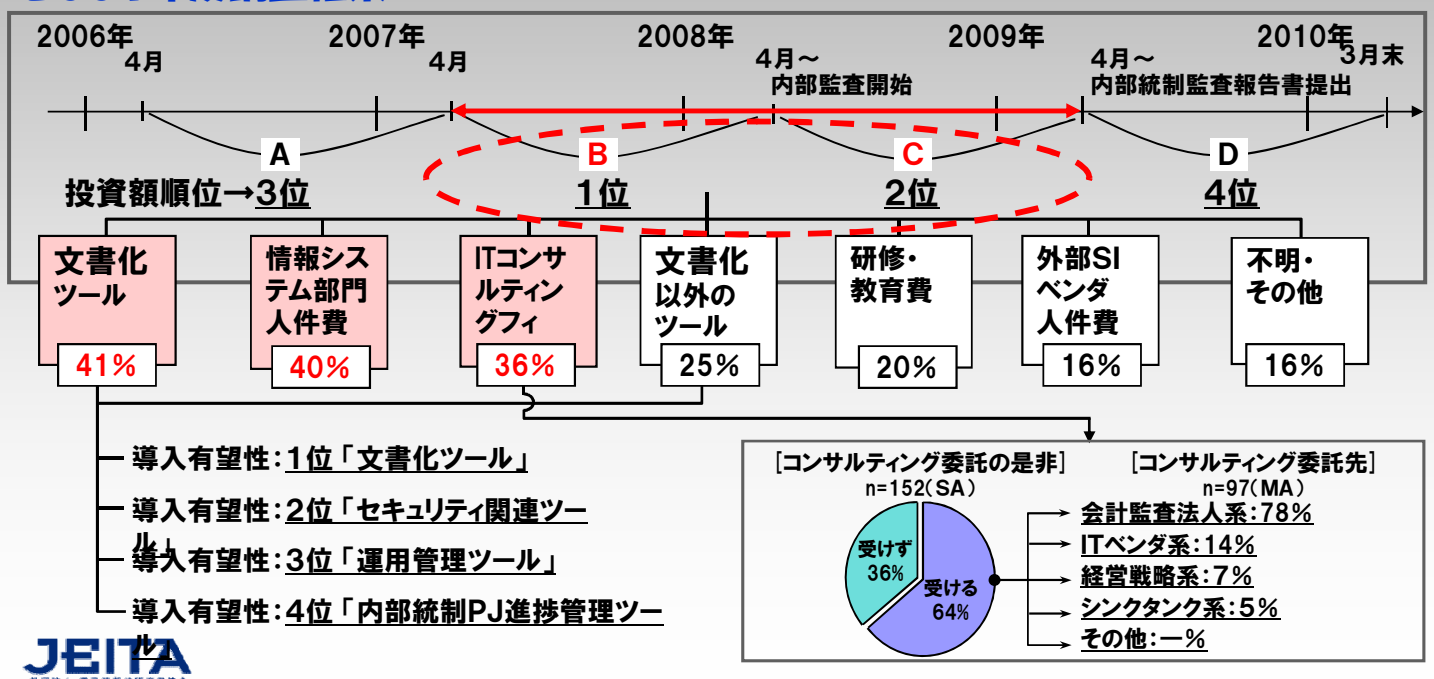


JEITA 社団法人 電子情報技術産業協会

【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。

2007年度調査結果



JEITA 社団法人 電子情報技術産業協会

【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、海外）	内部統制対応組織状況			本番以後の体制
				専任組織	統括部門	担当者数	
製造業（A）	5,000億～1兆円未満／1万名以上	国内、米国	100社以上（60～70社）	常設専任部門設置	内部監査部門	約15名	変更なし
製造業（B）	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	3名	変更なし
金融機関（A）	100～500億円未満／300名未満	国内	1社（—）	担当者のみ任命	内部監査部門	約6名	増員の予定
流通・サービス業（A）	1,000～5,000億円未満／10,000名以上	国内	1～5社（—）	担当者のみ任命	経理部門	4～6名	現状通り
流通・サービス業（B）	500～1,000億円未満／300～1,000名未満	国内	5～10社（—）	担当者のみ任命	経理部門	3名	各部門に担当設置
流通・サービス業（C）	100～500億円／1,000～3,000名未満	国内	10～50社（10～50社）	非常設専任部門設置	経営企画部門	7名	当面は現状通り

JEITA 一般社団法人 電子情報技術産業協会

【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。

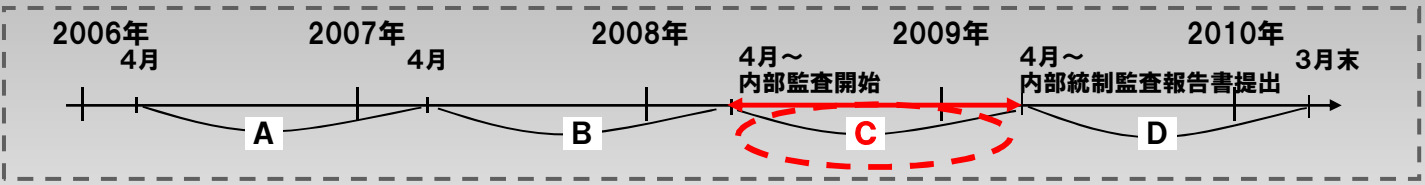
対象企業/本番開始時期	J-SOXへのIT対応に於ける現段階							
	Step1	Step2	Step3	Step4	Step5	Step6	Step7	Step8
	未着手	情報収集・検討	手順・方針決定（パイロット含）	評価範囲決定	評価実施（文書化・評価）	有効性判断と是正	評価結果記録・保存	内部統制報告書作成
製造業（A）/08.4～								⇒
製造業（B）/09.3～			⇒					
金融機関（A）/08.4～				⇒				
流通・サービス業（A）/09.3～		⇒						
流通・サービス業（B）/08.4～			⇒					
流通・サービス業（C）/08.4～					⇒			

JEITA 一般社団法人 電子情報技術産業協会

【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。

2007年度調査結果



対象企業	投資コストの多い順位				主な理由・コメント
	1位	2位	3位	4位	
製造業(A)	C	B	D	A	一般論では本番一年目で工数を含めてタイトになりコストも増大すると思う。ただ、当社は既に米SOX対応を行っている手前、A、Bの期間が最も投資が多かった
製造業(B)	B	C	A	D	当社は会計年度の点で他社の事例を多く収集できる時間的猶予もあり、極力本番前年度中に必要な準備を行うため、コストは「B」期間が最も掛かる
金融機関(A)	B	C	D	A	「B」が最大だが、アドバイザリ契約を活かし業務プロセス数を絞込めたことが大きい。また、07年度内に導入した関連ツールが最もコストを要したという背景もある
流通・サービス業(A)	C	D	B	A	本番稼動してみて初めて分かる点が出てくると予想しており、やはり本番1年目、2年目のコストが増加するのではないかとみている
流通・サービス業(B)	C	B	A	D	幾ら準備段階で周到に事前テストを行っても、本番で想定外の事態も含め対応すべき点が出てくると予想しており本番1年目(C)が最もコストが掛かるように思う
流通・サービス業(C)	C	D	B	A	「C」の本番初年度でどういったコストが発生するかまだ予見できない。ただ、仮に、初年度がコスト面でピークになれば次年度もある程度、コストは発生すると思う

JEITA 社団法人 電子情報技術産業協会

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。

JEITA 社団法人 電子情報技術産業協会

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 一般社団法人 電子情報技術産業協会

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 一般社団法人 電子情報技術産業協会

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
〒101-0065　東京都千代田区西神田３－２－１
千代田ファーストビル南館
電話：03-5275-7261　　FAX：03-5212-8122
Eメール：itt3@jeita.or.jp
JEITAホームページ：　http://www.jeita.or.jp/japanese/index.htm

JEITA
社団法人 電子情報技術産業協会