

日本版SOX法に基づく内部統制を導入する推進者・管理者のための総合的知識入門コースです。IT内部統制に係る全ての基礎知識を網羅しています。

日本版SOX法を実施するための手引書としての金融庁および経産省のガイドラインを理解・活用し、法律の目的に沿ったIT内部統制構築が出来るための知識を習得していただくためのコースです。

IT内部統制とは従来の内部統制をITを駆使して実践する統制の仕組みです。従来の内部統制の適用業務の統制に加えて、ITを活用するためのITに係る業務の統制(IT統制といいます)が必要になります。

金融庁が公表した「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」では、IT統制も含め、内部統制という用語で捉えています。本コースでは、理解を容易にするために「内部統制」、「IT統制」、そしてIT統制を含んだ内部統制を「IT内部統制」と区別して解説します。

(注記)SOX法:“ソックスホウ”とよびます。

目次		頁
第1章 内部統制とは	4
1. 1 内部統制が求められる背景	5
1. 2 日本版SOX法の経緯	6
1. 3 日本版SOX法と新会社法	7
1. 4 内部統制の目的と基本的要素	9
1. 5 日本版SOX法における監査責任	15
まとめクイズ	20
第2章 IT内部統制の構造	21
2. 1 財務報告とアプリケーションシステムの関係	22
2. 2 IT統制の構造	25
2. 3 IT統制と各標準の関係	29
補足資料:IT統制項目に対する各標準の対比	36
まとめクイズ	40
第3章 IT内部統制の業務プロセス	43
3. 1 システム管理基準 追補版とITIL	44
3. 2 IT業務処理統制の考慮事項	51
3. 3 パッケージに対するIT統制考慮事項	54
3. 4 ASP・SaaS向けSLAの考慮事項	58
3. 5 IT統制と評価目標の関係	65
まとめクイズ	69
第4章 IT内部統制の文書化と導入プロセス	70
4. 1 IT内部統制の記載要求事項	71
4. 2 内部統制主要文書例	74
4. 3 導入プロセスにおける重要検討事項	79
4. 4 IT内部統制システムの導入プロセス	95
まとめクイズ	102

Copyright ISM-Research Co.LTD 2

第1章は、内部統制の背景、目的や基礎的な用語や仕組みの解説です。

第2章は、内部統制の仕組みに適用されるIT 統制を取り上げます。

IT統制の経産省ガイドラインである「システム管理基準 追補版」(以降、「追補版」という)からIT統制の意味とその統制に係る標準の位置づけを整理します。

第3章は、IT統制の観点で、業務プロセスに要求される統制事項を整理します。

ITによる業務処理統制やITによる運用業務統制事項を整理しています。

ITの運用業務統制に有効な標準といわれているITILもここで取り上げます。

第4章は、IT内部統制のための要求事項のもとに必要となる文書規定類、考慮点、導入ステップをまとめています。

(注記)ITIL:“アイティル”とよびます。

目次(つづき)		頁
第5章 「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」の要点	103
5.1 「実施基準」の構成	104
5.2 「第Ⅰ部 内部統制の基本的枠組み」の要点	105
5.3 「第Ⅱ部 財務報告に係る内部統制の評価及び報告」の要点	107
5.4 「第Ⅲ部 財務報告に係る内部統制の監査」の要点	110
まとめクイズ	113
第6章「システム管理基準 追補版」の要点 (財務報告に係るIT統制ガイダンス)	114
6.1 「システム管理基準 追補版」概要説明	115
6.2 「システム管理基準 追補版」の構成	117
6.3 「第Ⅱ章 IT統制の概要について」の要点	118
6.4 「第Ⅲ章 IT統制の経営者評価」の要点	119
6.5 「第Ⅳ章 IT統制の導入ガイダンス」の要点	123
6.6 「付録1から付録6」の要点	125
6.7 「付録7から付録9」の要点	128
6.8 IT統制構築と運用・評価の構造	135
まとめクイズ	136


注記: テキストの右上に“★”がマークされているページは補足資料にその拡大図があります。

CopyRight ISM-Research Co.LTD 3

第5章は、金融庁が公表した「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」のガイドラインは内部統制の基本となるガイドラインです。内容は、3部構成となっており、各構成は内部統制の構築、経営者の統制・評価、監査人の監査の観点からの構成となっています。各構成ごとの要点を整理しました。

第6章は、経産省が公表した「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)は金融庁の内部統制ガイドラインに基づいたIT統制の観点でのガイドラインです。4章構成に加え、付録として具体的な記述事項や例を紹介しています。それぞれの構成の要点を整理しました。

それでは、第1章の「内部統制の背景、目的や基礎的な用語や仕組みの解説」から進めていきます。



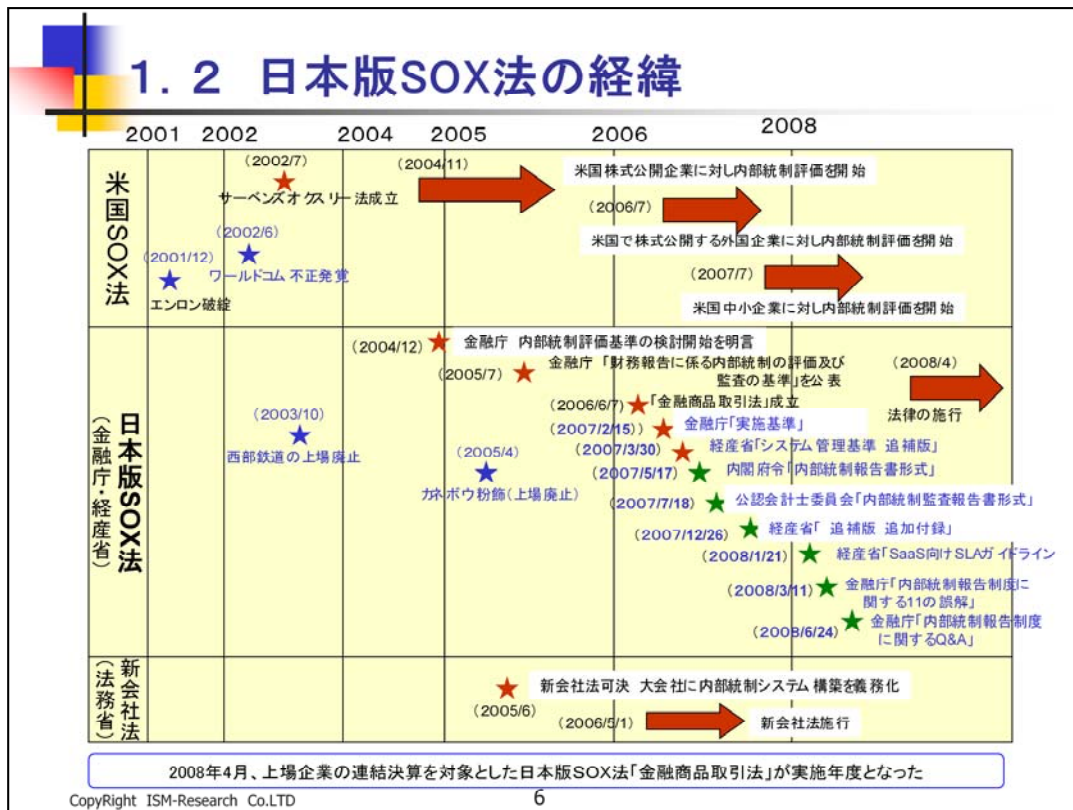
第1章 内部統制とは

- 1.1 内部統制が求められる背景
- 1.2 日本版SOX法の経緯
- 1.3 日本版SOX法と新会社法
- 1.4 内部統制の目的と基本的要素
- 1.5 日本版SOX法における監査責任

CopyRight ISM-Research Co.LTD 4

内部統制が制定されるに至った背景、経緯、および日本版SOX法の構造と仕組みの概要について5つの観点から解説し、日本版SOX法と内部統制の全体像を把握してみましよう。

まず、「1.1 内部統制が求められる背景」、そして「1.2 日本版SOX法の経緯」、「1.3 日本版SOX法と新会社法」、「1.4 内部統制の目的と基本的要素」、「1.5 日本版SOX法における監査責任」の順に進めていきます。



日本版SOX法は米国のサーベンズ・オクスリー法(SOX法)を引用して作成されています。米国SOX法はエンロン、ワールドコムの粉飾決算の発覚により、急遽2002年7月に法制化し、2004年11月より実施しました。

日本でも、西部鉄道の虚偽記載による上場廃止(2003年10月)、カネボウの粉飾(2005年4月)による上場廃止により、日本版内部統制といわれる「財務報告に係る内部統制の評価及び監査の基準」を金融庁が公表し、2006年6月7日の「金融商品取引法」成立へと進みました。

2006年11月21日には、金融庁から「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」(草案)が、2007年2月15日には意見書が内部統制の導入ガイドラインとして公表されました。この意見書が実施基準の公式バージョンとなります。

また、2007年1月19日には、経産省から「システム管理基準 追補版」(試案)がIT統制のガイドラインとして提出され、2007年3月30日に正規版が公表されました。

この2つのガイドラインが内部統制の基本ですが、その後も追加のガイドが公表され続けています。

2007年5月17日には内閣府令「内部統制報告書形式」、同年7月18日公認会計士委員会「内部統制監査報告書形式と記載例」、10月1日金融庁「内部統制報告制度に関するQ&A」、12月26日経産省「システム管理基準 追補版 追加付録」が公表され、会計パッケージのIT統制要件とIT業務処理統制のリファレンス記述が提供されました。

2008年1月21日経産省「SaaS向けSLAガイドライン」によって、外部委託業務のSLAリファレンス記述を提供しました。経産省のIT統制を中心とした整備が充実されていることが分かります。

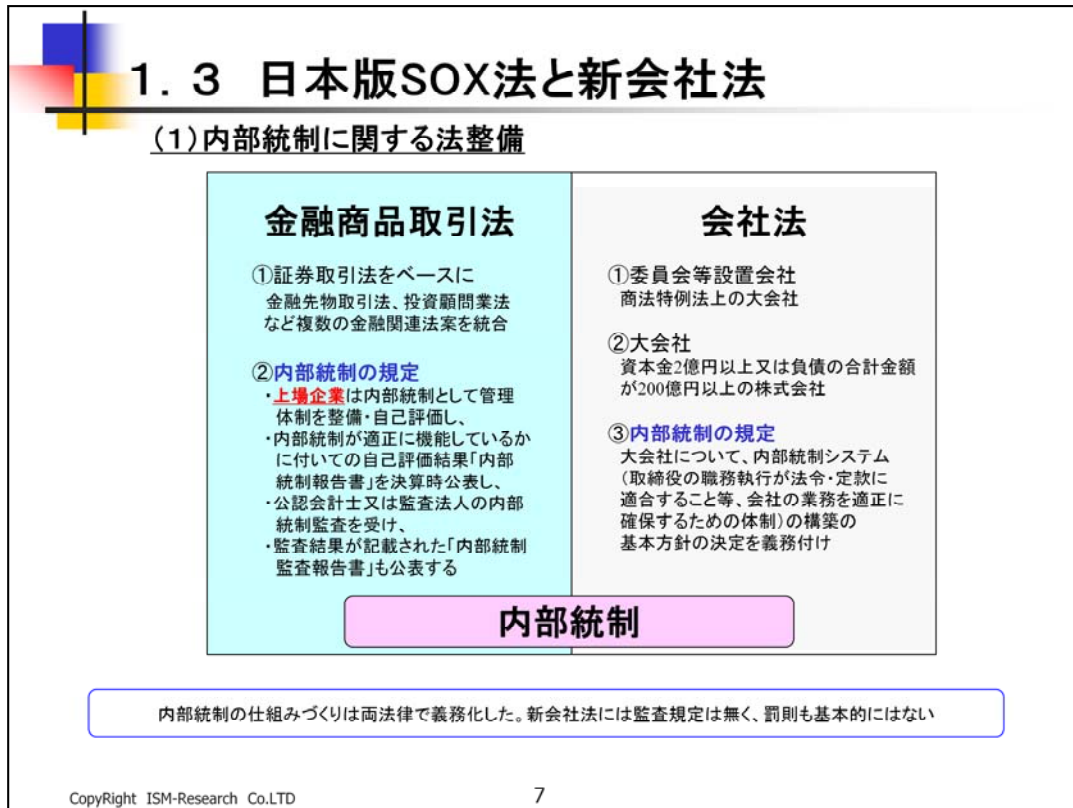
2008年3月11日、金融庁は「内部統制報告制度に関する11の誤解」を公表し、内部統制の構築・評価に“過度に保守的な対応”を戒めました。さらに、同年4月からの実施年度に入り、金融庁は2008年6月24日「内部統制報告制度に関するQ&A」を公表し67個の疑問点に回答をしました。J-SOXの重要視点である「重要な欠陥」を中心として、かなり実践的な回答がなされました。

J-SOX法の対象企業にとって、今後の活動において重要な指針になると思われます。

適用対象企業は異なりますが、会社法(旧来の会社法と区別する意味で新会社法とも言われます。)も法務省の下で2006年5月1日施行されました。

それでは、日本版内部統制のこれらの2法の特徴をみていきましょう。

(注記)これ以降は、金融庁公表の「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」を「実施基準」、経産省公表の「システム管理基準 追補版」(財務報告に係るIT統制ガバナンス)を「追補版」と表現することにします。



内部統制の法整備である日本版SOX法と会社法の違いをみてみましょう。

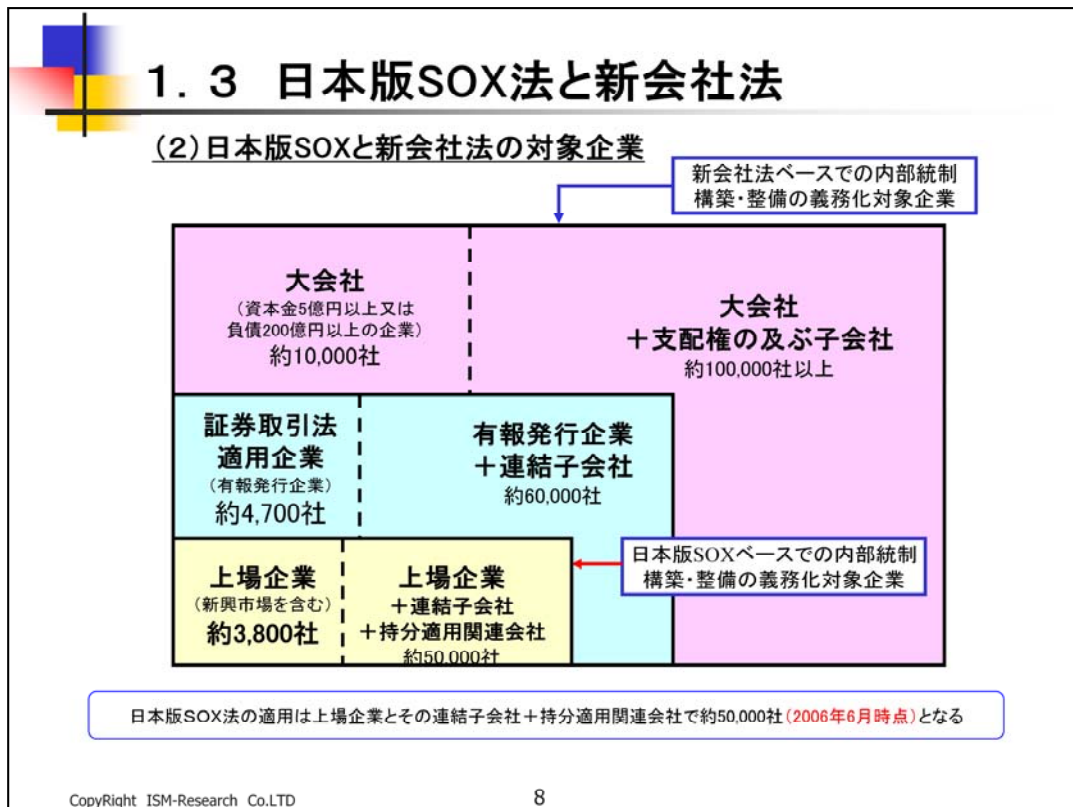
日本版SOX法といわれる「金融商品取引法」は証券取引法をベースに複数の金融関連法案をまとめたもので、その中の条項に上場企業を対象とした内部統制の規定があります。

会社法は商法や有限会社法等を統合し改定を施したもので、その中の条項に内部統制義務化の規定があります。対象企業は「委員会等設置会社」といい、商法特例法上の大会社（資本の額が5億円以上又は負債の合計金額が200億円以上の株式会社）となります。

罰則は、株式会社として「決算報告を行わない場合は、100万円以下の過料に処する（会社法976条）」とありますが、株式会社としては余りにも当たり前の企業行動であり、罰則は無いに等しいと言えます。

これに反して、内部統制で大きく騒がれているのは日本版SOX法です。理由は日本版SOX法には罰則規定があり、個人で1千万円以下、法人では7億円以下の罰金刑となりますが、会社法は罰則規定は無く、義務規定のみだからです。

これらの日本版内部統制の2法の適用企業の範囲を図解で押えておきましょう。



日本版SOX法の対象企業は新興市場も含めた上場企業、約3,800社です。

ただし、連結子会社+持分法適用関連会社があれば連結対象となります。これらの会社も上場企業が対象になることで対象として含まれます。総数は約5万社といわれています。


金融商品取引法が出来るまでの有価証券(有報)発行企業が対象である証券取引法適用企業まで含めると、連結子会社も含めて約6万社でした。

新会社法での対象企業は大会社(すなわち、資本金5億円以上又は負債200億円以上の企業)とその支配権の及ぶ子会社を加えると約10万社と言われていま

す。

このデータは、「金融商品取引法」成立時の2006年6月時点でのデータです。

この数の企業群となると、取引先も含め内部統制は必須の仕組みとなっていくと思われ



1.4 内部統制の目的と基本的要素

- (1) 米国SOX法の全体像
- (2) 金融商品取引法(日本版SOX法)
- (3) COSOのフレームと日本版SOX法
- (4) 日本版内部統制のフレームワーク

CopyRight ISM-Research Co.LTD 9

日本版SOX法は米国SOX法を引用していることから、その違いを4つの事項でみていきましょう。

まず、日本のSOX法の原点である米国のSOX法の全体像です。

(1) 米国SOX法の全体像

	サーベンス・オクスリー法 (SOX法)	PCAOB 監査基準第2号	COSO レポート
正式名称	上場企業会計改革 および投資家保護法	PCAOB監査基準第2号 「財務諸表監査に関連して実施される 財務報告に係る内部統制の監査」	内部統制の統合的枠組み
設定主体	米国議会	PCAOB(公開会社会計監視委員会)	COSO(トレッドウェイ委員会組織委員会)
設定時期	2002年7月成立	2004年3月 公表(2004年6月SEC承認)	1992年 公表

相互関係

PCAOB
の設置

監査基準
の提供

PCAOB監査基準
第2号

- 13項.経営者の評価は適切なフレームワークに基づかなければならない。
- 14項.COSOは適切なフレームワークの1つ。

フレームワーク
の提供

COSO
レポート

(注)COSO: Committee of Sponsoring Organizations of Treadway(監査人を監査する組織)
出典:

SOX法はPCAOB監査基準第2号に準拠し、PCAOBはCOSOフレームワークを推奨している

Copyright ISM-Research Co.LTD 10

米国SOX法の全体像です。

米国SOX法、PCAOB監査基準第2号、COSOレポートの関係を解説します。SOX法の条項には、“PCAOBの設置とPCAOBが監査基準を公表すること”があり、法制化されています。

PCAOB(公開会社会計監視委員会)の監査基準第2号の13項に“経営者の評価は適切なフレームワークに基づかなければならない。”とあり、14項に“COSOは適切なフレームワークの1つ。”と明記されました。

COSOとはトレッドウェイ委員会組織委員会で内部統制フレームワークの事実上の世界標準となる枠組みを公表しているところです。このことから、米国SOX法の監査基準はCOSOレポートの内部統制フレームワークを適用することになりました。

米国SOX法での内部統制の記述は、302条で「経営者の内部統制の義務付け」、404条で「外部の監査人が監査することの義務付け」があり、906条で罰則の規定をしています。

日本版SOX法の内容はどんな法律になっているのでしょうか。

(注記)COSO:“コソ”と呼びます。PCAOB:そのまま“ピーシーオーオービー”と読んでください。

(2) 金融商品取引法(日本版SOX法)

経営者の内部統制を義務付け

24条の4の4

「…第24条第1号に掲げる有価証券の発行者である会社その他の政令で定めるものは、事業年度ごとに、当該会社の属する企業集団及び当該会社に係る財務計算に関する書類その他の情報の適正を確保するために必要なものとして内閣府令で定める体制について、内閣府令で定めるところにより評価した報告書(以下「内部統制報告書」という)を有価証券報告書と合わせて内閣総理大臣に提出しなければならない」

外部の監査人が監査することを義務付け

193条の2の第2項

「金融商品取引所に上場されている有価証券の発行者その他のもので政令で定めるものが、第24条の4の4の規定に基づき提出する内部統制報告書には、その者と特別の利害関係のない公認会計士又は監査法人から監査証明を受けなければならない。ただし、監査証明を受けなくても公益又は投資家保護に欠けることがないものとして内閣府令で定めるところにより内閣総理大臣の承認を受けた場合にはこの限りではない」

罰則規定(197条の2、207条)

- 重要事項に虚偽記載のある有価証券届出書等の提出
懲役:10年以下 罰金:個人1000万円以下、法人7億円以下
- 有価証券届出書等の不提出
懲役:5年以下 罰金:個人500万円以下、法人5億円以下

出典:金融商品取引法(金融庁)

経営者の内部統制義務付けと外部の監査人の監査義務付けがあり、罰則が強化された

Copyright ISM-Research Co.LTD

11

日本版SOX法は、金融商品取引法の中の4つの条項で規定されています。

日本版SOX法では、金融商品取引法の24条の4の4で「経営者の内部統制を義務付け」、193条の2の第2項で「外部の監査人が監査することを義務付け」を上げ、罰則規定を197条の2(個人の罰則)と207条(法人の罰則)によって規定しています。

日本版SOX法では、財務諸表提出と財務計算に関する業務プロセスの統制は経営者の責任であり、「内部統制報告書」として報告書の提出を義務付けています。外部監査人には財務諸表の監査と経営者責任の内部統制報告書の監査を証明することを義務付けました。

罰則は、重要事項に虚偽記載のある有価証券届出書等の提出の場合、最大で、10年以下の懲役、罰金は個人が1000万円以下、法人は7億円以下が課せられることになりました。

この法律に沿って対処するためには、対処すべき要件が分からなければなりませんし、その内容はCOSOを基にして作成された日本版の内部統制(日本版COSOといわれる)の構成を知ることが必要になります。

その内部統制の構成、フレームワークを見てみましょう。