【法律の基礎知識】

情報管理・情報セキュリティと企業の内部統制

平成 20 年 10 月 13 日
文責　弁護士　六川浩明

1　企業改革と内部統制

一　日米における企業内“内部統制”の動向

【米国の状況】
1929 年　世界大恐慌
1933 年　米国証券法
1934 年　米国証券取引所法
1992 年　米国：COSO「内部統制に関するフレームワーク」
1997 年　米国において、COSO「内部統制に関するフレームワーク」が、企業の内部統制の標準としての地位を得る。世界的にも同様（←1997 年アジア経済危機)。
2001 年（平成 13 年）　米国エンロン社　不正会計、倒産申立事件
2001 年 12 月　エンロン社破綻
2002 年 6 月　ワールドコム社破綻（その他の優良企業の不正な財務報告の問題も顕在化）
米国は直接金融中心の経済であるから、企業が資本市場から資金を集めることができないと経済の血液が止まってしまう、という危機意識。
2002年(平成14年)　米国:「公開会社に関する会計改革･投資者保護法」(Public Company Accounting Reform and Investor Protection Act)（Sarbanes-Oxley 法とも呼ばれる）（以下、S-O 法という）
2002 年以後　S-O 法の委任を受け、米国証券取引委員会（SEC）が、S-O 法に関する SEC 規則を制定
2003 年　SEC　S-O 法 404 条に関連し、「内部統制に関する経営者報告」の規則を公表
・公開会社は、毎年、財務報告に係る内部統制の有効性を評価し、報告することを要求
・会計監査法人が、経営者報告を評価・証明することも要求
2003 年～2004 年　公開会社会計監督委員会（PCAOB）が、以下の監査基準等を作成し、それぞれ SEC によって承認された。
Rule 3100　（2003 年 10 月 31 日、SEC が承認）
Rule 3101（2004 年 9 月 8 日、SEC が承認）
Rule3201T（2004 年 12 月 3 日、SEC が承認）
暫定基準（2003 年 4 月 25 日、SEC が承認）
監査基準第 1 号（2004 年 5 月 14 日、SEC が承認）
監査基準第 2 号（2004 年 6 月 17 日、SEC が承認）

監査基準第3号（2004年8月25日、SECが承認）

2004年11月25日　SECが以下のことを公表

S-O法404条が求めている「財務報告に関する内部統制に関する経営者報告書」の適用期限について：

米国上場会社：2004年11月15日以降終了する事業年度から適用

外国会社：2006年7月15日以降する終了する事業年度から適用

【日本の状況】

2003年　「企業内容等の開示に関する内閣府令」の改正

2004年3月期から、上場企業の有価証券報告書に、次のようなコーポレートガバナンスの事項の記載が必要になった。

① 会社の機関の内容

② 内部統制システムの整備状況

③ リスク管理体制の整備の状況

④ 役員報酬、監査報酬の内容

企業の代表者は、次の内容を記載した確認書を作成・署名し、有価証券報告書に添付して提出する。

① 有価証券報告書の記載内容が適正であることを確認した旨

② 確認を行った記載内容の範囲が限定されている場合、その旨及びその理由

③ 確認を行うにあたり、財務諸表等が適正に作成されるシステムが機能していたかを、確認した旨及びその内容

④ 確認について特記すべき事項

2005年（平成17年）6月「新会社法」成立

2005年（平成17年）7月13日

（１）金融庁　企業会計審議会　内部統制部会

「財務報告に係る内部統制の評価及び監査の基準（公開草案）」公表

内部統制とは、基本的に、①業務の有効性及び効率性、②財務報告の信頼性、③事業活動に関わる法令等の遵守、④資産の保全、の４つの目的の達成のために、業務に組み込まれ、組織内のすべての者によって遂行されるプロセスをいう。

このプロセスは、①統制環境、②リスクの評価と対応、③統制活動、④情報と伝達、⑤モニタリング（監視活動）、⑥IT（情報技術）の利用、の計６つの基本的要素から構成される。

（２）経済産業省　企業行動の開示・評価に関する研究会

「コーポレートガバナンス及びリスク管理・内部統制に関する開示・評価の枠組みについて－構築及び開示のための指針―（案）」公表

2006年（平成18年）5月　新会社法施行予定

現・新会社法と「内部統制」概念

（１） 現行法（商法施行規則 193 条）・・・委員会設置会社

取締役会は、監査委員会の職務執行のため、次の事項を決定しなければならない。

① 執行役の職務執行が法令・定款に適合し、かつ、効率的に行われることを確保するための体制に関する事項

② リスク管理体制に関する事項

③ 情報の保存・管理に関する事項

④ 執行役等が監査委員会に報告すべき事項　等

（２）新会社法

第 362 条 4 項 6 号・5 項に内部統制に関する規定が置かれる。

「取締役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務の適正を確保するために必要なものとして法務省令で定める体制の整備」義務を、委員会設置会社のみならず、大会社一般に義務づけている。

中小会社が内部統制に関する方針を設けることもでき、その場合には、必ず取締役会で審議して決定しなければならないとしている。

雇用の流動化→従来型の以心伝心型の社内内部管理体制の限界→内部統制とリスク管理が必要。

【日米における罰則】

有価証券報告書虚偽記載についての罰則

米国：最高 500 万ドル（約 5 億円）の罰金及び最長 20 年の禁固刑

日本：5 年以下の懲役または 500 万円以下の罰金（証取法 197 条）

二　米国 S-O 法

１　主たる内容

米国の 1933 年証券法及び 1934 年証券取引所法を改正するとともに、公開会社のコーポレートガバナンスを強化するための多くの規律を含む。

（１） 会計制度の改革：

① 公認会計士を監督し、監査基準を策定する自主規制機関として、公開会社会計監督委員会（PCAOB：Public Company Accounting Oversight Board）を創設。

② 会計事務所が、監査対象会社に対し、非監査業務を提供すること等を禁止。

（２） コーポレートガバナンスへの介入

① 公開会社（米国証券取引委員会(SEC)によるディスクロージャー（開示）規制に服する会社）の監査委員会が独立取締役のみから成ること等を求め、監査委員会の権限と責任を強化。

② 公開会社がその取締役・役員に貸し付けを行うことを禁止。

③ 会社の利益が修正された場合に、業績連動型報酬や株式取引による利得を会社に返還するよう役員に義務付け。

（３）ディスクロージャーの強化

①　公開会社の CEO らにディスクロージャーの真実性を担保させるため、誓約書を提出

させる。
② 罰則を強化。
③ 内部統制報告書の提出を求める。

【企業会計】

1　企業会計の種類

（1）　財務会計　株主、銀行、取引先、政府などの企業外部の利害関係者に報告することを目的とした会計である。外部報告会計。共通の会計基準によって作成。定期的に作成開示。

（2）　管理会計　企業の経営者や事業部長あるいは工事長などの企業内部の関係者に報告することを目的とした会計である。内部報告会計。不定期的に作成。

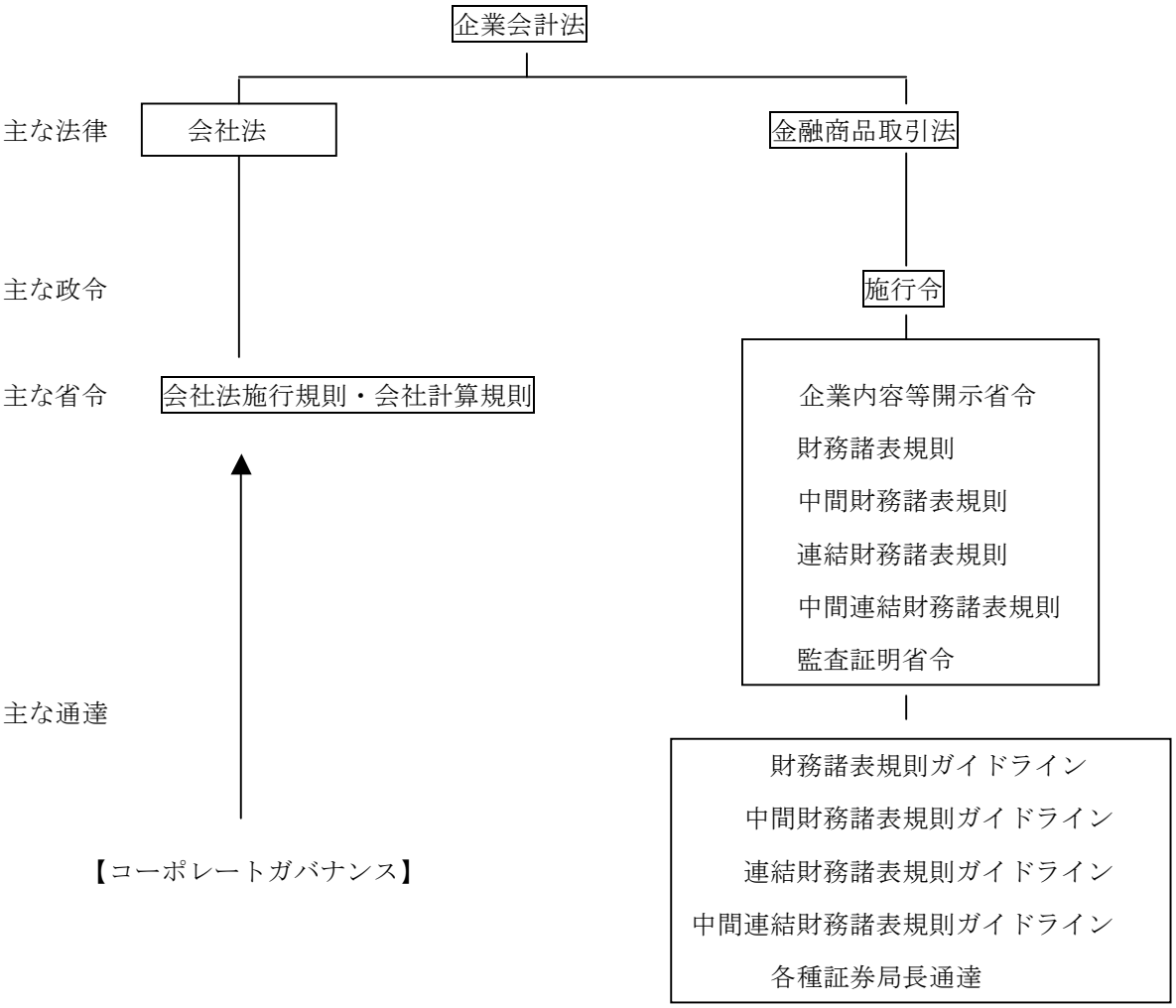
（3）　税務会計

財務会計の目的

1．企業の経営成績を明らかにする。企業の一定期間のフロー情報を提供する。

2．企業の財政状態を明らかにする。企業の一定時点でのストック情報を提供する。

2　企業会計と法（日本）



会社法の会計制度：会社経営者の受託責任の遂行状況、会社の債務弁済能力ないし担保余力を把握するのに役立つ情報を開示。

金融商品取引法の会計制度（金商法 193 条、財務諸表規則）：会社の収益性や配当余力、企業集団の実績という証券投資の意思決定に重要と思われる情報を開示。

会社法「計算書類」:

① 貸借対照表、②損益計算書、③営業報告書、④株主資本等変動計算書、⑤附属計算書

会社法は、資本金、資本準備金、利益準備金など、貸借対照表項目の計算を中心した会計処理の規定。これは、株主は有限責任しか負わないことから、株主に配当する配当可能利益を規制し、もって債権者を保護しようとするため。

金商法 193 条「財務計算に関する書類」及び財務諸表規則 1 条「財務諸表」:

① 損益計算書、②貸借対照表、③キャッシュフロー計算書、④株主資本等変動計算書または損失処理計算書

④ 附属明細表

三　米国 S-O 法の構成
第１章　公開会社会計監督委員会（PCAOB）の設置
101 設立、業務内容
102 会計監査法人による、PCAOB への登録
103 監査基準、品質管理基準、倫理基準、独立性基準の制定
104 会計監査法人への検査
105 会計監査法人に対する調査・懲戒処分
106 外国の会計監査法人への適用
107 証券取引委員会（SEC）による、PCAOB への監督
108 会計基準
109 資金調達
第２章　会計監査法人の独立性の確保
201 非監査業務についての提供の禁止
202PCAOB による事前承認
203 主任会計士等の 5 年ごとの交代
204 会計監査法人から企業内の監査委員会への監査報告
205 改定
206 会計監査法人が監査対象会社の上級役員を雇用した直後における、当該会社に対する監査禁止
207 会計監査法人の強制的変更の調査
208SEC の権限
209 州政府の権限
第３章　企業責任の強化
301 公開会社内の監査委員会（監査委員会メンバーの独立性）
302 財務報告に関する企業責任（CEO 及び CFO の、財務報告に関する「宣誓書」）
303 会計監査法人への不当な影響力の行使の禁止
304 違反行為における CEO 及び CFO によるボーナス及び利益の没収
305 役員に対する罰則
306 年金ファンドの取引規制期間中のインサイダー取引禁止
307 弁護士の専門家責任
308 投資家への公平な資金
第４章　公開会社の財務状況の開示の強化
401 公開会社の定期的報告書の開示
402 取締役及び役員への貸付禁止
403 主要株主の変更報告
404 経営者による内部統制報告書・会計監査法人による評価書
a. 経営者による内部統制の有効性評価に関する報告（経営者が、自社の財務報告に係る内部統制は有効に機能したかどうかについて評価する報告書。）
b. 会計監査法人による監査・・・監査対象は、①経営者が行った財務報告に係る内部統制の有効性評価の妥当性、及び、②財務報告に係る内部統制そのものの有効性
405 免除

1107 情報提供者への報復行為の禁止

四　財務報告に係る内部統制の文書化

１　内部統制の概念

内部統制（internal control）：①業務運営の有効性と効率性、②法令遵守、③財務報告の信頼性、という目的の達成に関連して合理的な保障を提供することを意図した、事業体の取締役会、経営者及びその他の構成員によって遂行されるプロセス

２　財務報告に係る内部統制の文書化

S-O 法第 404 条によれば、経営者は、財務報告に係る内部統制の有効性評価に関する報告書（自社の財務報告に係る内部統制は有効に機能したかどうかについて評価する報告書）を提出し、会計監査法人がこれを監査しなければならないとされている。

会計監査法人は、PCAOB が定め、米国 SEC が 2004 年 6 月 17 日に承認した監査基準第 2 号「Auditing Standard No.2- An Audit of Internal Control over Financial Reporting Performed in Conjunction with An Audit of Financial Statements」に従って監査しなければならない。

○経営者による内部統制の有効性評価報告書において、“財務報告に関する内部統制の文書化”について記載しなければならない事項（監査基準第 2 号 42 項）。

① 重要な勘定項目と注記事項について、それぞれのアサーションと内部統制のコントロールを結びつけること。また、COSO の内部統制フレームワークの５要素（監査基準 49 項）に従って整理すること。
② 重要な取引がいかに起案され、承認され、記録され、処理され、報告されるかが明らかになるような文書化
③ 不正やエラーに基づく重要な虚偽記載が起こる可能性があるのは業務フローのうちどの部分か、ということが明らかになるような文書化
④ ある統制活動が防止的なものであるか或いは発見的なものであるのかの区分、また、誰が統制を実施しているかもしくは職務の分掌等についての情報
⑤ 決算期末の決算書作成手続に関する統制活動の文書化
⑥ 資産の保全に関する統制活動の文書化
⑦ 経営者が行った財務報告に係る内部統制の評価手続とその結果の文書化

○ 文書化の形式に関しては、書類でも電子ファイルでもよく、方法に関してはフローチャート、文書による記述式の説明など様々な方法が考えられ、また、それらを組み合わせて実際の文書化が行われるであろう（監査基準第 2 号 43 項,138 項）。

○ 財務報告に係る内部統制の不適切な文書化は、それ自体が内部統制上の問題とされ、文書化の程度が著しく低い場合には、内部統制上の重要な欠陥となり、会計監査人は不適正意見を表明しなければならない（監査基準第 2 号 45 項）。

五　COSO フレームワーク

COSO(The Committee of Sponsoring Organization of the Treadway Commission=Treadway 委員会支援組織委員会。米国公認会計士協会、米国会計学会、財

務担当経営者協会、内部監査人協会、管理会計士協会の５団体が集まって創立したもの。)の発行するレポート

（１）内部統制に関するフレームワーク：COSO1992 年レポート

内部統制＝「経営活動に携わる人々の行動を統制し、人々が効率よく効果的に業務を行い、信頼できる方法で財務諸表を作成し、法律や規則に違反しない仕組みを提供するもの」・・・内部統制とは、会計に関する統制だけでなく、事業全般にわたる広範囲の概念

３つの目的：

①業務の効率性・有効性、②法令順守、③信頼性のおける財務報告

５つの構成要素：

① 統制環境の整備（Control Environment）：会社経営の基本方針等
② リスク評価(Risk Assessment)：企業目的に影響を与える全ての経営リスクを認識し、その性質を分類し、発生の頻度や影響を評価
③ 統制活動(Control Activities)：権限や職責の付与、職務の分掌等の、様々な統制活動
④ 統制に必要な情報と伝達(Information & Communications)：業務情報と財務情報の社内伝達
⑤ 監視活動（Monitoring)：統制が機能していることを監視するメカニズム、①から④までの機能は常時監視され、是正されることを可能とする監視活動（業務過程における報告等を含む)

	業務の効率性・有効性	法令順守	財務報告の信頼性
統制環境			○
リスク評価			○
統制活動			○
情報と伝達			○
監視活動			○

○印の部分・・「財務報告に係る内部統制の有効性評価に関する報告書」(S-O 法 404 条及び PCAOB 監査基準第 2 号 45 項等）が求めているもの。

（２）企業リスクマネジメントに関するフレームワーク

COSO　2004 年　Enterprise Risk Management Framework（ERM フレームワーク）

1992 年 COSO 内部統制フレームワークを基礎として、そのうち、リスクマネージメントの部分に焦点をあてて、そのリスクマネージメントの評価の部分を相当拡充してつくられたフレームワークである。

（アンダーラインの部分が、1992 年 COSO 内部統制フレームワークに対して新たに加わった)

４つの目的

①業務の効率性・有効性、②法令順守、③財務報告の信頼性、④企業戦略

８つの構成要素

① 内部経営環境の整備（Internal Environment）
② 経営目標の設定（Objective Setting）
③ リスク事象の識別（Event　Identification）
④ リスク評価（Risk Management）
⑤ リスクに対応する経営者の対応（Risk Response）
⑥ 統制活動（Contrrol Activities）
⑦ 統制に必要な情報と伝達（Information and Communication）
⑧ 統制が機能していることを監視するメカニズム(Monitoring)

六　IT の全般統制（Information Technology Genral Controls　PCAOB 監査基準第 2 号 50 項、126 項）

１　IT インフラ　→　ビジネスプロセスシステム　→　財務情報

IT の全般統制＝IT 化に関する経営資源（IT 化された財務情報、財務情報につながるデータ、IT 化されたビジネスプロセス、IT インフラ等）を適切に管理する統制活動

２　IT の全般統制を構成する要素（PCAOB 監査基準第 2 号 50 項）

プログラム開発、プログラム変更、コンピュータ運用、プログラムやデータへのアクセス

２　ＣＯＢＩＴ

（１）COBIT・・・米国 IT ガバナンス協会による「Control Objectives for Information and related Technology 」（情報テクノロジーのためのコントロール目標）

「マネジメントガイドライン」（日本語訳あり）及び「監査ガイドライン」等が公表されている。

（２）IT プロセスと IT マネジメントへの活用

４つの領域、34 の IT プロセス、318 に細分化された管理目標に分けて捉え、それぞれのプロセスについて

- CSF（Critical Success Factors 重要成功要因）
- KGI（Key Goal Indicators 主要目標の達成度評価指標）
- KPI(Key Performance Indicators 主要な業績評価指標）
- 成熟度モデル等が定められている。

COBIT の IT プロセス

計画立案及び組織化

PO1　IT 戦略計画の策定

PO2　情報アーキテクチャの定義

P03　技術指針の決定
P04　IT 組織とその他の組織との関係の定義
P05　IT 投資の管理
P06　マネジメントの意図と指針の伝達
評価視点の一つ：セキュリティと内部統制
提供されるシステムとサービスの品質を左右する哲学･方針･目標が、情報サービス機能の方針と手続により正式に定義され、文書化され、維持されていること。
上級管理者は、セキュリティと内部統制への全体的なアプローチのためのフレームワーク開発に対し全責任をとり続けていること
セキュリティと内部統制フレームワーク文書は、以下について明記すること→セキュリティと内部統制に関する方針、効果と目的、管理構造、組織内の範囲、責任の分担、セキュリティと内部統制方針を遵守しなかった場合の罰則と懲戒処分の定義
正式なセキュリティと内部統制の方針は、組織の内部統制プロセスを明らかにし、以下のコントロールの構成要素を含むこと→コントロール環境、リスク評価、コントロール活動、情報と伝達、監視
特別な活動、アプリケーション、システムまたは技術に関する管理者の決定については、その文書化を要求する明確な方針が存在すること
P07　人的資源の管理
P08　外部からの要求事項に対する遵守性の保証
P09　リスク評価
P010 プロジェクト管理
P011 品質管理

取得及び導入
AI1　自動化された解決案の特定
準拠法テストの一つ:セキュリティと内部統制の問題がシステム設計文書の中で適切に扱われていること
AI2　アプリケーションソフトウエアの取得及び保守
AI3　技術インフラの調達及び保守
AI4　手続の作成及び保守
AI5　システムの導入及び受入れ保証
AI6　変更管理

サービス提供とサポート
DS1 サービスレベルの定義と管理
DS2 サードパーティのサービスの管理
DS3 成果とキャパシティの管理
DS4 継続的なサービスの保証
DS5 システムセキュリティの保証

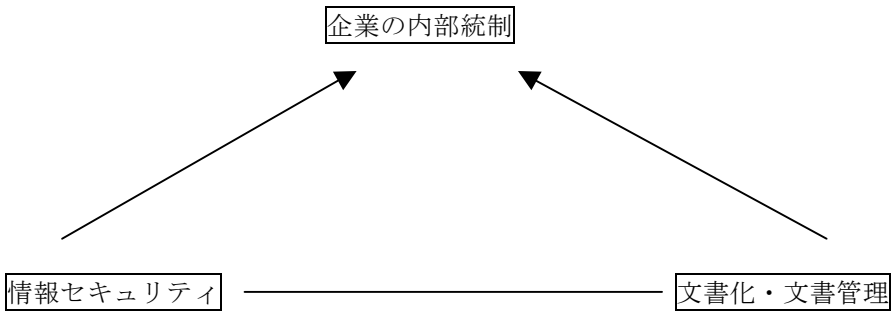
DS6 コストの特定及び適切な配賦
DS7 ユーザの教育とトレーニング
DS8 カスタマに対する支援及びアドバイス
DS9 構成管理
DS10 問題及び事故の管理
DS11 データ管理
DS12 設備管理
DS13 オペレーション管理

モニタリング
M1　プロセスのモニタリング
M2　内部統制の妥当性の評価
M3　独立した第三者による保証の取得
M4　独立監査の実施

（３）2003 年秋「IT Control Objectives for Sarbanes-Oxley」（S-O 法のための IT コントロール目標）・・・S-O 法で求められる財務報告の目標に沿った内容となるよう修正。４つの領域、27 の IT プロセス、136 の管理目標に変更。
IT コントロールは、S-O 法に定める財務報告と情報開示の双方に関連性がある（同報告書 34 頁）。

３　情報セキュリティとの関連

“財務データの正確性”を証明するためには、会計処理手順及び管理が信頼できるものでなければならないが、データの格納・移動・転送する IT システムに対する信頼性も重要である。IT システムとデータベースのプロセス及び管理も、信頼できるものでなければならない。また、データの改ざんなどがあってはならないから、適切な文書管理も重要となる。適切な情報セキュリティ対策（データ管理、文書管理方策を含む）なくして、企業は自社の財務報告や社内管理を自信をもって完了させることはできない。



以上