東京海上日動リスクコンサルティング（株）
情報グループ
主任研究員　　小芝　正敬

内部統制の構築とセキュリティ

本稿は、日本実務出版株式会社発行の『月刊「安全と管理」』2008年11月号「ビル・オフィス―内部統制とセキュリティ―」の特集に掲載された「内部統制の構築とコンサルティング」を許可を得て転載しています。

内部統制の概略（2 つの内部統制）

内部統制とは

内部統制とは「Internal Control」を日本語に翻訳した言葉で、主に、経営者がどのようにして従業員を管理すれば、事務ミスや不正・不祥事などから会社の財産を守ることができるか、また事業を有効的・効率的に行うことができるかについて論じられています。そして近年では、企業を取り巻くあらゆる環境を考慮して、企業が持続的に発展するために経営者はいかにリスク管理を行うべきかの議論に発展しています。

会社法が求める内部統制

現在、日本では会社法と金融商品取引法において内部統制が要求されています。会社法では「業務の適性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」として、取締役会議事録や稟議書、決裁書などの管理体制、全社的・一元的なリスク管理体制、経営体制の最適化や職務分掌に沿った権限委譲、コンプライアンス体制、子会社も含めた内部統制の体制、の構築を求めています。会社法が求める内部統制の特徴は、おおよそ経営全般について内部統制の構築を求めている点です。また、構築の具体的な方法についての言及はなく、それぞれの企業の判断で行うことになります。

金融商品取引法が求める内部統制

一方、内部統制を要求する金融商品取引法の条項は一般に J-SOX と呼ばれており、この J-SOX の指針として金融庁企業会計審議会から「財務報告に係る内部統制の評価及び監査に関する基準」（以下『基準』）が発行されています。この基準では、内部統制全体の枠組みとして、経営者に求められる内部統制の 4 つの目的とそれぞれの目的を達成するための 6 つの基本的要素が示されています。

4 つの目的	6 つの基本的要素
① 業務の有効性及び効率性	1. 統制環境
② 財務報告の信頼性	2. リスクの評価と対応
③ 事業活動に関わる法令等の遵守	3. 統制活動
④ 資産の保全	4. 情報と伝達
	5. モニタリング
	6. IT への対応

J-SOX では内部統制の 4 つの目的のうち「②財務報告の信頼性」を達成する、つまり粉飾決算のリスクを予防するための 6 つの基本的要素が社内できちんと機能しているかについて、経営者が毎年確認を行い、その結果を内部統制報告書として公表することを要求しています。一方で、前述したように会社法は経営全般についての内部統制を求めており、この『基準』の枠組みに準拠すれば、会社法は 4 つの目的にある①～④の全てを達成するために内部統制を行うことを求めているといえます。

2 つの内部統制の違い

このように、会社法と J-SOX では内部統制を求めている範囲が異なります。他にも、会社法は全ての企業に内部統制の構築を要請しているのに対して、J-SOX は上場企業等に限られます。また、会社法は内部統制の構築義務を課しているものの罰則規定がないのに対して、J-SOX は内部統制報告書を偽った個人又は法人に対して刑事罰が規定されているという違いがあります。

内部統制とセキュリティ

セキュリティ対策の注意点

内部統制では『基準』の 6 つの基本的要素にもあるように「2. リスクの評価と対応」がポイントとなります。対象となる様々なリスクを評価し、評価に応じて低減・移転・回避・保有の対策を選択し対処します。そしてリスクの低減対策の一つとしてセキュリティがあります。セキュリティには様々なレベルがあるので、全てのリスクに対して万全なセキュリティ対策を行うのではなく、費用対効果を見ながら様々なリスク対策を検討する必要があります。

J-SOX とセキュリティ

J-SOX の内部統制では、様々な経理プロセスにおいて、経理上の数値の、実在性、網羅性、権利と義務の帰属、評価の妥当性、期間配分の妥当性、表示の妥当性の担保が要求され、会計監査人の監査時にこれらが担保されていることを証明する必要があります。一方、大量のデータを繰り返し処理する経理業務は IT と親和性が高く、大多数の企業では経理システムや連結決算システム、受発注システムなど様々な IT が導入されています。このことから『基準』では内部統制の基本的要素の一つとして「6. IT への対応」が求められており、間違いや不正処理を防止するための IT による経理業務の統制と共に、IT システム自体の信頼性を確保する IT 統制が重要です。

IT 統制では、情報セキュリティの 3 要素である「可用性」「機密性」「完全性」の確保を考慮して、

ユーザー認証・アクセス制御、ログの管理・監視・分析、情報漏えい対策などの様々な対策が行われています。

会社法とセキュリティ

一方、会社法は財務報告に限らず企業活動全般に関する内部統制を求めており、情報セキュリティはもちろんのこと、様々な悪意や不正に対するセキュリティが求められています。個人情報や機密情報の漏えいは経営に深刻な影響を与える可能性があります。食品業界では工場や流通過程での異物・毒物混入対策が重要です。また、小売業では店舗での盗難・万引き対策が重要な場合もあります。業態と企業を取り巻く社会環境によって求められるセキュリティは多種多様であるといえます。

内部統制構築の現状と今後の課題

J-SOX の現状

J-SOX は 2008 年 10 月現在、構築段階を終え運用・検証段階に移りつつあります。しかし、新興企業や中小規模の企業を中心に人材不足やコスト負担の重さを背景に対応が遅れているとの報道もあります（2008 年 3 月 28 日、日本経済新聞朝刊）。

また、J-SOX 対応のために様々なシステムを導入した企業も多く、やはり中小規模の企業を中心に IT 関連の設備投資が経営上の負担となっている企業もあります。

会社法内部統制の現状

会社法上の大企業（資本金 5 億円以上、負債 200 億円以上）は法に従い「内部統制システム構築の基本方針」を取締役会で決議し何らかの内部統制体制の整備を行っています。全社的・一元的にリスク管理体制を構築し内部統制を進めている企業がある一方で、ノウハウ不足のため、上手く体制が活用できていない企業もあります。

また、期限が定められ罰則もある J-SOX 対応を優先し、罰則規定のない会社法の対応を先送りしている企業も見受けられます。

今後の課題

J-SOX 対応が遅れている企業に関しては、人材・予算等の経営資源の不足を乗り越えて如何に J-SOX の求める内部統制を軌道に乗せるかが課題です。J-SOX 対応は 1 回限りの対応でなく上場を維持する限り永遠に続くため、その場しのぎには限界があります。

J-SOX 対応が軌道に乗ったあとは、より広範囲の内部統制を求める会社法の規定を視野に入れて、粉飾決算のリスク以外の企業を取り巻く様々なリスクや、従業員が原因となるリスクだけでなく外部要因によるリスク、さらに経営戦略に内包するリスクに至る、全社的・一元的なリスク管理体制を構築し運用していく必要があります。

コンサルティングの紹介

東京海上日動リスクコンサルティング㈱は内部統制の整備やリスクマネジメント体制の構築・運用について、体制整備の助言、リスク評価の実施、対策への助言、内部統制・リスクマネジメント

http://www.tokiorisk.co.jp/

の有効性評価などに関する多くの経験とノウハウを基に、様々なご要望にお応えするコンサルティングを提供しております。

（第213号　2008年12月発行）