情報セキュリティ管理を起点とした内部統制強化へのアプローチ

企業は日本版SOX法への対応として、2006年度中には内部統制について何らかの体制構築に着手する必要があると言われている。とはいえ、どこから手を付けたらいいのか迷っている企業も多いことであろう。本稿では、内部統制体制を情報セキュリティ管理を起点として構築することの有効性と、そのための具体的なアプローチのポイントについて概説する。

多くの企業で必須の内部統制の強化

企業の内部統制の体制強化については、2006年５月に施行された新会社法や、日本版SOX法（2008年に導入予定の金融商品取引法）により、とくに上場企業にとって、もはや逃れられない取り組みになっている。とくに日本版SOX法で財務報告に係る内部統制の有効性が焦点であることから、財務報告に関連する対策を最優先としている企業も多いであろう。また、日本版SOX法の適用対象は上場企業となっているが、連結子会社（海外子会社も含む）が対象になることも予想され、さらにそのアウトソーシング先にも影響が及ぶと考えられるため、システムの開発や運用を受託する企業は、かなりの割合で対応が求められることになりそうである。

では、日本版SOX法への対応として、何から手を付ければいいのだろうか。ここでは、情報セキュリティ管理を起点とした内部統制の体制強化について考えてみたい。

内部統制の基礎は情報セキュリティ管理

今日では、日々の取引から財務会計処理に至るあらゆる企業活動において、ITが関係しない業務はほとんどない。そのため、必然的に内部統制はITの統制なしには成り立たない。そのITの統制には、情報セキュリティ管理が必要不可欠なことは言うまでもない。

ITの統制は、各々のビジネスプロセスに適用される「業務統制」と、すべてのシステム構成要素やプロセスやデータに適用される「全般統制」に区分できる。情報セキュリティ管理はその双方に大きく関与している。とくに「全般統制」の管理策として、情報セキュリティポリシーの策定、アクセス管理、職務と権限の分離、システム導入・変更管理、ログの取得などは、すべて情報セキュリティ管理の基本的要素である。情報セキュリティ管理は内部統制の有効性を支えており、必須の対策である。

企業全体のリスクに関連する情報セキュリティリスク

情報セキュリティ管理が内部統制の体制強化の起点となるもう１つの理由として、情報セキュリティ管理が企業全体のリスクコントロールの基礎になっている点があげられる。

内部統制の基本的要素のひとつは「リスクの評価と対応」であり、監査法人による内部

NRIセキュアテクノロジーズ
情報セキュリティ調査室
主任セキュリティコンサルタント
長谷川　剛（はせがわごう）

専門は情報セキュリティ全般に関するコンサルティング、セキュリティ診断

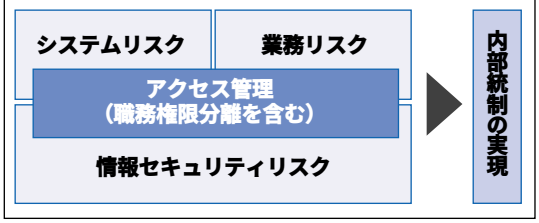
統制の監査では、企業のリスクコントロールが適切に行われているかどうかが大きなポイントとなることが考えられる。

一般に企業におけるリスクは、「人や組織に潜む業務リスク」と「IT基盤に関連するシステムリスク」の2つに大別される。この2つのリスクにともに深く結び付いているのが情報セキュリティリスクであり、そのリスクコントロールが企業全体のリスクコントロールを支えるものとなる。したがって内部統制体制の強化には、情報セキュリティリスクへの対策の強化が必須であり、なかでもアクセス管理（利用者認証、識別による制御、管理者による承認）を強化することが必要である（図1参照）。

情報の“完全性”を実現するための各種アプローチ

では、具体的に何を基準に、どのように情報セキュリティ管理を行えばよいだろうか。2005年4月の個人情報保護法の施行に際しては、多くの企業が個人情報を中心とした情報セキュリティ管理体制や対策の強化に取り組んでいると思われる。この対応を内部統制に対しても活用することが可能である。ただし大きな違いもある。個人情報保護法への対応ではおもに情報の“機密性”に焦点が当てられているのに対して、財務報告に係る内部統制対応においては情報の“完全性”、つまり情報が正確に処理・表示・受け渡しされること

図1　企業の内部統制を脅かすリスク要因の関係



を保証することが重要である。

また、ISMS適合性評価制度（組織全体のセキュリティ管理体制を第三者が評価認定する制度）の考え方を内部統制にそのまま適用することもできる。その場合、経営層を巻き込んだ情報セキュリティ管理体制を構築し、文書化・セキュリティ対策・監査・是正という一連のPDCA（Plan—Do—Check—Action）サイクルによって内部統制の強化を図ることになる。

米国では、SOX法対応を行った企業が最も参考にした基準に、ISMSとほぼ同一の内容をもつBS7799（英国の標準。現在はISO/IEC 27002）をあげる企業が多いという報告もある。日本版SOX法における情報セキュリティ管理の対策においても、この基準を超えることは考えにくいため、ISMSやBS7799が対策の基準として参考になるであろう。

また、COBIT（IT統制に関する標準のフレームワーク）についても、システム監査的な観点から参考になると思われる。BS7799で対策を立案・実施し、実施水準のチェックや文書化体系の整備はCOBITをベースに実施するという方法も有効であろう。 ■