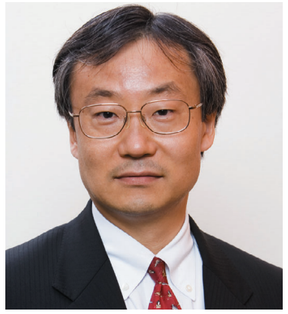
内部統制整備で進めるITの再構築

～日本の企業情報システムに見られる課題と対策～

内部統制の整備は、企業によっては対策が広い範囲に及び、対応に苦慮しているところもあるかもしれない。しかし、経営者にとっては自社内の仕組みを、ITを含めて根本から見つめ直す良いチャンスである。具体的には、職務分掌の必要性、アウトソーシング先の役割、ERP（統合基幹業務システム）やレガシーシステムが持つリスク――を再考したい。



金山 尚弘
新日鉄ソリューションズ株式会社
産業ソリューション事業部　営業第四部長

着々と進んだ日本国内における内部統制に関連する法律の整備

日本では企業における内部統制環境の構築と強化を意図した法令の制度化は、2003年から始まった。まず2003年4月に商法が改正され、委員会等設置会社の内部統制システム構築が義務となった。また、同時に施行された内閣府令第28号では、コーポレートガバナンス、内部統制事項の開示を義務化、代表者確認書の任意添付、といったことへの対応が求められた。

その後も2006年5月施行の会社法など内部統制環境の構築/強化を目的とした法整備は続いた。特に2006年6月には「金融商品取引法（証券取引法の一部を改正する法律）」によって財務報告に係る内部統制報告制度が上場企業に対して義務化されたことは大きい。影響の大きさや求める内容が米国のSOX（サーベンス・オクスリー）法に似ているため、金融商品取引法は「日本版SOX法」や「J-SOX」という通称で呼ばれる。

財務報告に係る内部統制報告制度は、2008年4月以降に始まる会計年度の決算期から提出と監査が必要になる。いま、国内の多くの企業は内部統制環境の構築に注力しているはずだ。

日本が独自に明確化したIT統制 全般統制と業務処理統制から成る

金融商品取引法では、企業が整備すべき内部統制の姿が、業務とITの二つに大きく分けて示された。米国のSOX法との大きな違いは、「ITへの対応」が基本要素として明確化されたことだ。「ITに係る全社的内部統制」「ITに係る業務処理統制」、そして「IT全般統制」の仕組みを整えることが求められている。

日本が独自に明確化した「IT統制」について、少し詳しく触れておく。それぞれの項目が何を意味し、どんな統制活動を求めているのかを知っておかなければ、効果的な内部統制環境を構築できないからだ。

まず、「ITに係る全般統制」。これは、後述するIT業務処理統制が有効に機能する環境を保証するための統制活動だ。少し簡単に言うと「情報システムに不正や誤りが起きないようにする」システム業務のことである。具体的には、システムの開発・保守管理、運用管理、システムの安全を確保するセキュリティ管理、外部委託先の契約管理などを行う必要がある。

同時に、システムの可視化を推進することも重要となる。システム全体、そして各部分が、何をどう行っているのか、チェックが容易でなければならない。システム横断的に、標準化したIT全般統制を行うことがIT業務の効率化にもつながる。

もう一つの「ITに係る業務処理統制」は、システムにおいて、業務が正確に処理・記録・監視できるようにすることが目的になる。具体的には、入力されたデータの多重チェック、データの信頼性担保、エラーデータの制御、改竄を防ぐアクセス制御といった機能をシステム内に用意し、それぞれの機能が正常に機能することを保証する作業が重要になる。

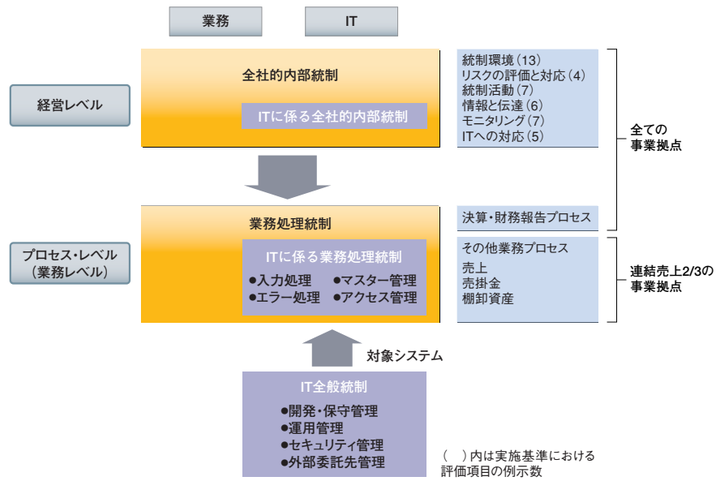
内部統制環境を構築する代表的なメソッドは四つある

金融商品取引法が求める内部統制環境を構築するには、いくつかの標準的なメソッド（方法）がある。代表的なものは、①フローチャート、②RCM（リスク・コントロール・マトリックス）、③整備・運用評価、④監査――だ。

フローチャートは、企業が行う業務プロセス全体をいくつかのサブプロセスに分割し、その流れを図式化したものだ。業務項目を縦軸に、実施部門を横軸に、それぞれ配置するのが一般的である。業務の流れをチャートによって「見える化」した上で、それぞれに存在するリスクとコントロールを明示し、業務プロセスのどこにリスクが集中しているかを見極める。こうすると、リスクの識別と内部統制でコントロールする部分の検討が可能になる。

もう一つのRCMは、業務プロセス内に潜在するリスクを徹底的に洗い出す手法である。リスク内容とアサーション（統制目的）、そしてリスクをコントロールするために必要な手段を列挙し、それぞれのリスクへの対応策を網羅的に検討する。

■日本版SOX法が求める内部統制の概要



フローチャートもRCMも、企業の業務内容や規模によって検討すべき項目数は変動する。例えば新日鉄ソリューションズの「業務プロセス」は、60のサブプロセスに分かれたが、このうち受注サブプロセスでは「受注入力」にリスクが集中していることが判明した。また、RCMで検討した結果、約450のリスク要因と約1400のコントロール項目が挙がった。グローバルに事業を展開する大企業では、コントロール数は1万以上にも上るという。

内部統制の整備の基本には職務分掌の考え方が不可欠

フローチャートやRCMによって、業務プロセス内に潜在するリスクを把握できたら、こうしたリスクをコントロールできるような内部統制環境を構築する段階になる。

内部統制の基本は、職務分掌（SoD）にある。業務プロセス全体を複数のサブプロセスに分類し、それぞれにかかわる担当者と業務範囲を明確化する。そして、プロセスごとにチェック役を設けると同時に、プロセス受け渡し時のチェックも行っていく。例えば、システム開発なら、ユーザー部門、情報システム部門、外部委託先のそれぞれで明確に職務分掌をすると同時に、部門の責任者などがチェックを行う。

この考え方を推し進めることにより、相互牽制と多重チェックが働くようになる。一つひとつのプロセスは厳密に定義されており、個々のプロセスに存在するリスクをあらかじめチェック/コントロールすることによって、業務全体のリスクを低減できるからだ。

ただし、職務分掌の手法で業務に係るすべてのプロセスをコントロールするのは現実には難しい。SoDの基本は「他人を信頼しない」ことであり、組織内の人間関係に悪影響を

与える危険もある。リスクを予防する効果は高いが、導入の仕方には工夫を凝らす必要があると言える。

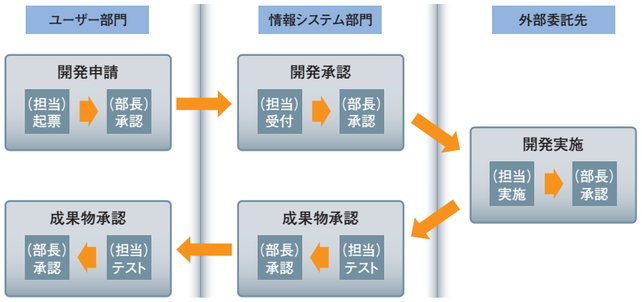
職務分掌が正しく行われると開発ベンターとの関係が健全化

職務分掌という考え方は、自社内の内部統制のみでなく、ユーザー企業とITベンダーの関係にも適用できる。これまでシステム開発の分野においては、RFP（提案依頼書）による「顧客ビジョン」が明確でない場合も多かった。細部の仕様決定をベンダー任せにしたり、要件定義が行われなかったり――といった問題だ。また、開発プロセスについても仕様やスケジュールが硬直化していたり、開発基準が標準化されていなかったり、といった問題もあった。

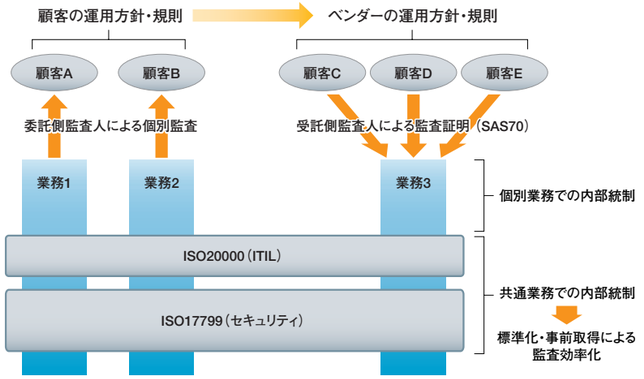
職務分掌という考え方をここに導入することによって、顧客側がなすべきこと、開発ベンダーがなすべきことが明確に見えるようになる。それぞれが主体的に行うべきプロセスが明確に見え、より健全なシステム開発ができるようになる。

SLC（システムライフサイクル）をトータルでカバーする標準方法論を保有する新日鉄ソリューションズでは、こうした開発プロセスのモデルを「V字モデル（NSVICTORYモデル）」と呼び、顧客ビジョンを実現できる仕組みとして用意している。このように、職務分掌という考え方を効果的に導入することで、内部統制活動の実効性を上げるだけでなく、システム開発プロセスの改良にもつながる。

■職務分掌（SoD）による相互牽制と多重チェックの仕組み（システム開発の例）



■アウトソーシングにおける迅速な日本版SOX法対応のポイント



ERPやレガシーシステムの抜本的な見直しが必要になる

内部統制環境の構築に役立つ手法として再び注目を集めているのが「ERPの見直し」だ。ERPは、1990年代に広まった概念をもとに作られたシステムである。企業内に存在するすべての経営資源を統合的に管理し、最適な配分と配置を行うというコンセプトに基づく。

実はERPには、内部統制を効率的に行う仕組みが盛り込まれている。先に挙げた職務分掌や、個々のプロセスに内在するリスクのコントロールといった諸要素を既に備えているのである。

しかし、日本ではそうしたERPの仕組みが効果的に利用されているとは言えない。日本でのERPは使い勝手や業務の効率化を重視してアドオンを多用してきた。それは内部統制の観点からは、ERP本来の統制機能を殺していることにほかならない。

同様の問題点は、レガシーシステムを使い続ける企業にも当てはまる。内部統制機能が不十分なレガシーシステムを継続して利用することは、内在するリスクをそのまま放置することにつながりかねない。

そこで必要なのが、ERPやレガシーシステムの抜本的な見直しだ。業務の基幹を担うERPやレガシーシステムを、内部統制という観点から見直すことが不可欠になる。

内部統制環境の整備によってアウトソーシング先も変化

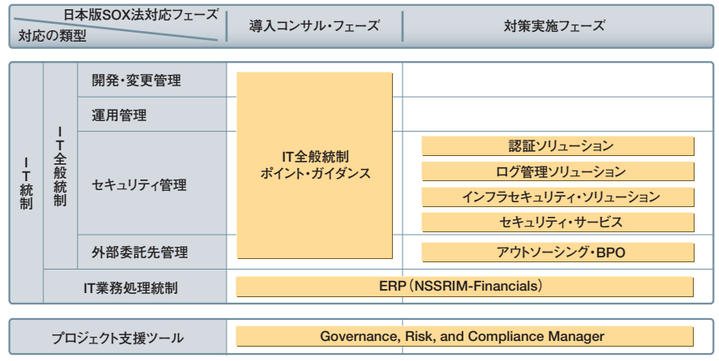
金融商品取引法では、自社の内部統制環境を構築/強化することに加え、業務委託（アウトソーシング）先の内部統制についても重視している。同法の内部統制に関する実施基準では「委託業務の内部統制は、委託者が責任を有する」とされている。このことにより、アウトソーシングのあり方にも大きな変化が見られそうだ。

アウトソーシングには、特定業務を委託することで自社のコアビジネスに集中できるというメリットがある。しかし、内部統制という観点から考えると、きちんとリスクがコントロールされている委託先を選ばなければ、より多くのリスクを背負う危険性がある。委託側にとっては監査に耐える内部統制を整備した委託先を見つけることが必要だ。

こうした変化とニーズを受け、受託側企業で内部統制環境を整備する動きが広がってきた。中でも重視されているのがISO20000（ITサービス・マネジメントに関するベストプラクティス集のITILに対応するITサービス・マネジメントの標準）やISO17799（情報セキュリティに関する標準）に対応する動きだ。

企業の共通業務における内部統制の大部分は、この2種類の認証を受けていることでカバーできる。ただし、各企業における個別の業務は、委託側の監査人による個別の監査となる。

■新日鉄ソリューションズの内部統制ソリューション体系



企業の個別業務も標準化し、複数の顧客から同一業務を受託できれば、SAS70（受託業務にかかわる内部統制に関する監査基準）監査報告書で効率化できる。今後、SAS70対応の事例は増えて行くに違いない。

内部統制環境の構築は経営の質を高めるチャンス

このように内部統制の整備は、企業によっては対策が広い範囲に及び、対応に苦慮しているところもあるかもしれない。しかし、経営者にとっては自社内の仕組みを、ITを含めて根本から見つめ直す良いチャンスである。職務分掌の重要性、アウトソーシング先の役割の再検討、ERPやレガシーシステムが持つリスクの評価――は、どれもいずれは着手しなければならない経営課題であることに異論はないだろう。

ERPを見直したり、新たに導入したりすることは確かに大きな投資が必要になる。レガシーシステムについて、システムトランスフォーメーションを実施する場合も同様である。しかし、内部統制は一度やれば終わりというものではなく、継続的に運用していく必要がある。2～3年後を見据えた上で、そうしたIT環境を見直していけば、BPR（ビジネスプロセス・リエンジニアリング）が実現でき、“経営の質”を高めることができるだろう。

国内でも既に、内部統制環境の構築が経営の質を高め、会社自体の価値を向上させることに早くから気づき、施策を実施している企業がある。例えば、株式会社ノーリツ（p.22参照）がそうだ。内部統制環境の構築が持つ「チャンス」に、いかに早く気づいて実施できるか。経営者としての対応力が問われている。

新日鉄ソリューションズでは、内部統制環境を構築するためのソリューションを数多く用意する。必要な部分を抽出し、ピンポイントで対応するソリューションも、全体を統一的に見るソリューションも用意する。そうすることで、いち早く気づいた企業が、経営の質を高めることをサポートしていく。