ITベンダーに対する内部統制評価の考え方

3年目に入った米国のSOX法では、対象企業を段階的に広げることが規定されており、いよいよ日系企業もその対象に含まれる運びとなっている。これらSOX法の対象となる企業では、委託先のITベンダーの内部統制の評価も適切な方法で実施する必要がある。本稿では、そのための委託側企業の考え方について述べる。

ITベンダーの内部統制をどう評価するか

企業の粉飾決算を発端として、2002年にSOX法（サーベンス・オクスリー法。いわゆる企業改革法）が施行された米国では、2006年7月以降の決算から第3グループも対象に加わることになっている。

第3グループとは、日本を含む非米系のSEC（証券取引委員会）登録企業のことで、日系企業ではトヨタ自動車、松下電器産業、野村ホールディングスなど30数社が対象となっている。

SOX法404条で求めている内部統制は、全社レベルの統制、業務処理統制、IT全般統制の3つである。SOX法への対応が義務付けられる企業（以下、SOX法対応企業）は、この3つの統制の有効性を評価する必要があるが、問題はIT全般統制である。

いま、多くの企業は自社のシステムをITベンダーにアウトソーシングしており、システムの開発から運用・保守を自社のシステム部門だけで実施しているケースは非常に少ない。したがって、企業がIT全般統制の有効性を評価するためには、自社のシステム部門のプロセスの有効性を評価するだけでは、SOX法の要求を満たすことはできない。そこでIT全般統制の有効性評価を補完するため、委託先のITベンダーに対して内部統制強化を求めることになる。

内部統制評価の手法

ITベンダーの内部統制の評価方法には、顧客企業自身が評価を行う方法と、外部の第三者が監査を実施して評価を行う方法の2つがある。ITベンダーにはシステム委託元の内部統制の要求を拒否するという選択肢もないわけではないが、継続的な関係を前提にすれば、それは現実的にはあり得ない選択であろう。

顧客企業自身が監査を行う方法は、ITベンダーがASP（アプリケーションサービスプロバイダー）事業を展開している場合や、複数のSOX法対応企業を顧客にもつ場合、すべての顧客の個別監査を受け入れることは現実的に不可能であろう。顧客企業の側も、複数のITベンダーに委託していることが多いため、それぞれに個別監査を実施するのは大きな負担である。

したがって、顧客企業とITベンダーの双方にとって、外部の第三者による監査を実施

野村総合研究所
品質監理本部
品質監理部
主任専門スタッフ
森田太士（もりただいじ）
専門は品質プロセス改善など

するほうが利点が多いと考えられる。

米国で多く採用されるSAS70号監査

米国では、標準的な外部監査の方法としてSAS70号監査というものがよく用いられる。SAS70号監査とは、独立した会計監査人（外部監査人）が、米国公認会計士協会が策定した監査基準書第70号に基づいて企業の内部統制の整備状況および有効性を評価し、その監査意見を表明するものである。

企業がSAS70号監査を実施することは、外部監査人による内部統制の有効性を評価する手続を実施することで、企業内の意思決定プロセスを第三者へ説明できる、内部統制組織の整備およびその運用状況を確認できる、内部統制上の問題点を発見し改善につなげることができるなどの利点がある。

SAS70号監査は、TYPEⅠ監査とTYPEⅡ監査によって構成される。TYPEⅠ監査は内部統制の設計（時点監査）、TYPEⅡ監査は内部統制の運用（期間監査）についての監査を範囲とする。

SAS70号監査は、元来SOX法対応のために作られたものではないため、評価基準の全体がSOX法に準拠しているとは言えない。しかし、独立監査法人による監査という“お墨付き”が得られるので、ITベンダーは内部統制の有効性を顧客企業に示しやすく、またSOX法対応企業でも、ITベンダーに対する客観的な評価が得られることになる。

なお、米国公認会計士協会の基準によるSAS70号監査以外に、日本公認会計士協会基準による評価を実施する18号監査と呼ばれるものもある。両者は英語と日本語という言語の違いはあるものの、ほぼ同様の基準となっている。

野村総合研究所（NRI）もSOX法対応企業を顧客にもつITベンダーとして、以下のように内部統制の評価を実施している。

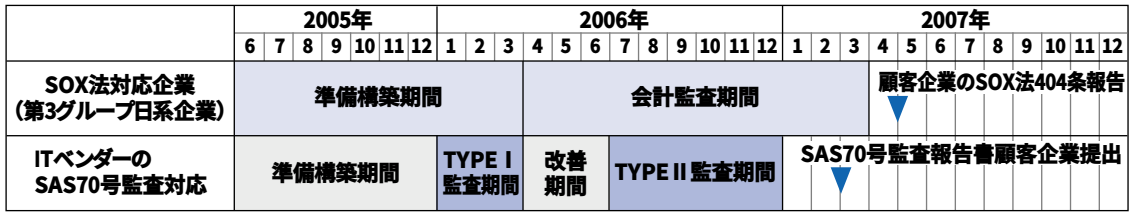
①システムの受託開発事業の内部統制評価
顧客：日系SEC登録金融業
サービス内容：基幹系システムの受託開発・保守・運用
監査基準：日本公認会計士協会基準18号
監査期間：計画準備　3カ月
　　TYPEⅠ監査　3カ月
　　TYPEⅡ監査　6カ月（予定）

②ASP事業の内部統制評価
顧客：金融業数十社（欧州系SEC登録企業）
サービス内容：ASPとしての金融情報の提供
監査基準：SAS70号
監査期間：計画準備　2カ月
　　TYPEⅠ監査　2カ月
　　TYPEⅡ監査　6カ月（予定）

ITベンダーへのSAS70号監査（18号監査）の問題点

ITベンダーにとって顧客企業が1社だけの場合、両者の結び付きが強いためにITベンダーの内部統制は顧客企業の内部統制の影

図１　顧客企業とITベンダーの内部統制の取り組みスケジュール



響を強く受ける。そのため実質の業務はITベンダー内で行っているにもかかわらず、顧客企業の統制下に入るプロセスと、自社内で統制すべきプロセスの境界があいまいになることが多い。この傾向は顧客との関係が密であるほど顕著である。ITベンダーと顧客企業に資本関係があれば、すべてを顧客企業の統制プロセスに含めることも考えられるが、そうでないにもかかわらず、顧客企業との関係が非常に親密で、役割分担（業務分掌）が不明確な場合がある。このような場合、SAS70号監査では、役割分担を明確にしなければ内部統制の有効性評価は得られない。

また、評価対象の時間的設定がSOX法とSAS70号監査（18号監査）で異なっている点にも注意が必要である。SOX法は、一会計期間での内部統制の有効性を求め、会計年度末時点の有効性を評価すればよいとされている。しかしSAS70号監査（18号監査）のTYPE Ⅱ監査では、監査期間を通じての有効性評価が求められているため、監査期間内で重大な指摘が発生した場合、監査法人から統制の有効性の評価は得られない。また、顧客企業の会計年度末を３月とした場合、ITベンダーの内部統制の有効性評価の報告はそれ以前に求めなければならない。したがって顧客企業のSOX法対応よりも前倒しの活動が求められ、実質的には12月末までをSAS70号監査（18号監査）期間とする必要がある（図１参照）。

日本版SOX法でも同様の対応が必要

日本版SOX法（金融商品取引法）が施行された場合、対象となる上場企業約3,800社も米国と同様にIT全般統制の有効性を評価する必要がある。当然ながら自社のシステム部門だけでIT全般統制の有効性を示せる企業は少ないため、ITベンダーの内部統制の有効性を評価しなければならない。企業にとってITベンダーの内部統制強化は、もはや対岸の火事（米国SEC登録企業の問題）ではなく、近いうちにすべての上場企業が対応しなければならない問題なのである。そしてITベンダーもその要求に応える必要がある（図２参照）。

信頼性の高い内部統制評価のために

日本版SOX法への対応に際しても、内部統制の有効性評価方法は基本的に米国SOX

法と変わらないため、ITベンダーはSAS70号監査または18号監査を利用した内部統制を構築することになるだろう。SAS70号監査（18号監査）はさまざまな問題をはらみながら、制度として一般に知られ、採用する企業も増える傾向にある。SOX法対応企業およびITベンダーは、それらの問題を理解した上で、以下のような考え方で内部統制を構築・評価する必要がある。

①自社の内部統制をもつ

内部統制は自社内で検討・決定・構築するのが基本である。有効性評価を実施する監査法人の言いなりなる必要はなく、自社のリスク分析に基づく内部統制を構築することが大切である。

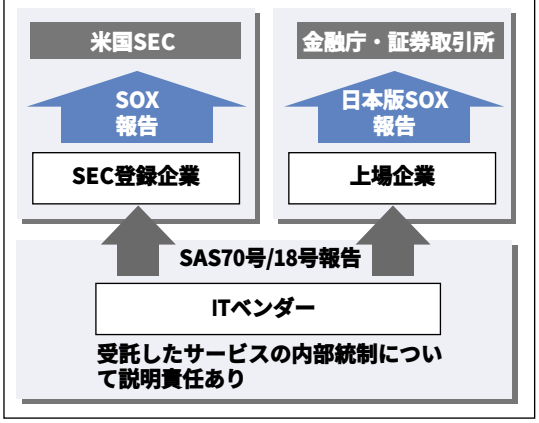
②内部統制の“構築”がゴールではない

内部統制はいったん構築すれば終わりというものではない。継続的な内部統制活動と、環境の変化に応じた内部統制の改善が必要になる。中・長期的な方針に則り、継続的な運用が行えるような統制の体制づくりが必要である。

③統制に関するコミュニケーション

顧客企業はSOX法対応のためにリスク分析を行い、リスクを軽減するためのプロセスを構築し、内部統制を構築する。ITベンダーもまた、自社のリスクに応じた内部統制を構築する。これらの活動は必ずしも足並みがそろうわけではない。そのため、互いに相手の統制が出来上がるのを待つのではなく、自社の内部統制を早期に構築し、積極的に情報を交換しながら調整していくことが必要である。

図２　SOX法とITベンダーの関係



ITベンダーの選別が必要な時代に

SOX法への対応（内部統制の整備）が不可避であることは、内部統制先進国の米国では周知の事実であり、日本でもその認識は強まっている。

企業のSOX法への対応にはITベンダーの内部統制整備が不可欠であり、ITベンダーもまた、その要望に応えなければならない。ITベンダーに対する企業のニーズは、サービスレベルに関するものだけでなく、内部統制という企業のガバナンスにまで広がっている。ITベンダーは、この幅広いニーズに柔軟に対応できなければ、顧客から選ばれる企業になることはできない。顧客企業もまた、幅広いニーズに柔軟かつ確実に対応できるITベンダーを選ばなければならない時代になってきている。■