

日本版SOX法に向けた18号監査（日本版SAS70）の活用

欧米の金融機関は、その特性・限界を理解した上で、SAS70を有効に活用している。日本の金融機関も、18号監査については、その特性・限界を十分に見極め、さらに欧米と日本の制度・環境の違いを意識した上で、有効に活用していく必要がある。

日本版SOX法（金融商品取引法）により、内部統制報告書の提出が義務付けられる中、外部委託業務の内部統制を評価する手段としてSAS70や18号監査に注目が集まっている。SAS70や18号監査を、どのように捉えたらよいのだろうか？本稿では、欧米の金融機関におけるSAS70活用の考え方を参考に、SAS70や18号監査の位置づけを考察する。

SOX法で重要性を増したSAS70

SAS70（Statement of Auditing Standards No.70）は、米国公認会計士協会が1992年に策定した監査基準であり、90年代より活用されてきたが、2002年の米SOX法¹⁾施行後、その利用は一層増加した。

米国では、80年代前半の粉飾決算多発を受けて、80年代後半より不正会計防止に向けた監査基準強化が行われ、外部委託業務も含めた内部統制評価が要請されるようになった。

外部委託業務の内部統制評価については、主に2つの方法がある。

1. 委託者が、受託者を直接監査する。
2. 委託者が、受託者の内部統制監査の結果を利用する。

複数の委託者を抱える受託者にとって前者の直接監査はあまりにも負荷が大きいと、後者の一手段として、SAS70は準備された。

SAS70は、90年代から、信託、年金管理、資産運用、給与計算、データセンター等の財務諸表に大きな影響を与える外部委託業務を

中心に活用されてきた。そして、2002年米SOX法の施行によりすべての上場企業に内部統制評価が義務付けられた結果、SAS70の利用はさらに増加した。

欧米の金融機関におけるSAS70活用の考え方

ただ、欧米の金融機関にヒアリングしてみると、外部委託業務の内部統制を評価するにあたって、必ずSAS70を利用するわけではなく、その特性、限界を理解した上で、選択肢の一つとして、活用していることがわかる。活用にあたっての考え方をいくつか紹介したい。

まず、SAS70は万能でないことが理解されている。SOX法対応では、委託者が内部統制を評価する必要があるが、SAS70報告書は、監査人向けの報告書であり、委託者自らが評価する報告書としては、テスト内容および結果、情報セキュリティ等に関する記述が不十分になりがちである。また、受託者が決めた内部統制範囲が、委託者が評価したい範囲と合致しないケースも起こりうる。

こうした状況に対して、欧米の金融機関は、様々な対策を行っている。例えば、金融機関が、ITベンダーに重要な業務を外部委託しているケースで、情報セキュリティに関する記述が不足する場合は、別途ペネトレーションテスト²⁾を要請したり、テスト内容や結果の記述が不足する場合には、追加の報告書³⁾を要請したりしている。

また、選択肢は、SAS70だけではないこと

Writer's Profile



河合 孝
Takashi Kawai

金融ITイノベーション研究部
上級研究員

専門は金融市場動向調査
focus@nri.co.jp

を常に意識している。前述のとおり、受託者を直接監査する、あるいはSAS70以外の監査結果³⁾を利用することも可能である。受託者側の状況（SAS70取得有無や直接監査受け入れ方針等）を確認した上で、期間、ワークロード、コスト等を総合的に勘案し、ケースバイケースで最も効率的な手段を選択しているようだ。

英国版SAS70の動向

SAS70を参考に、よりよい監査基準を模索する動きもある。英国版SAS70であるFRAG21は、2006年にAAF01/06⁴⁾へと改定されたが、SAS70を参考に、より使いやすくする工夫が盛り込まれている。

例えば、統制目的のミニマムセットが事前に定義されているため、受託者が決めた内部統制範囲と委託者が監査したい範囲が異なるといったことは起こりにくい。また、記述内容不足を防止するために、テスト内容と結果を詳細に記述することが規定されている。

残念ながら、現時点では、利用実績も少なく、AAF01/06がすべてを解決するわけではない。英国上場のみであれば、AAF01/06が活用できるが、米国上場時にはSAS70を考慮せざるを得ない現実がある。

しかしながら、AAF01/06の動向は、SAS70のみならず、各国の監査基準へ影響を与える可能性がある。AAF01/06が成功し、各国の監査基準が進化することを期待したい。

日本版SOX法に向けて


日本でも、2006年6月に日本版SOX法（金融商品取引法）が成立し、上場企業は、2008年度の本番年度に向け、内部統制報告書の提出を義務付けられることとなった。日本では、日本公認会計士協会が、SAS70と同内容である18号監査（日本版SAS70）を発表済みであり、この18号監査に注目が集まっている。

日本版SOX法の実施基準⁵⁾を見ると、「受託

会社の評価結果の利用」について、18号監査という記述はなく⁶⁾、「委託業務に関連する内部統制の評価結果を記載した報告書等」を「評価の代替手段とすることが考えられる」という表現になっている。文言どおり解釈すれば、「経営者」および「監査人」が認めれば、18号監査でなくても良いこととなる。

一方で、日本の公認会計士数は、図表のように、米国および英国と比べ圧倒的に少ない。金融庁は公認会計士・監査法人制度の充実・強化の方針を打ち出している⁸⁾ものの、急激に増加するわけではない。18号監査を取得したくとも、監査法人あるいは公認会計士がなかなか確保できないという状況に陥ることは十分に考えられる。

「委託業務に関連する内部統制の評価結果を記載した報告書等」の実務上の取り扱いは、金融機関をはじめとする企業経営者、監査法人、行政の動向や個々の実務を通して、今後徐々に決まってくると想定されるが、公認会計士の数が圧倒的に少ないという日本の環境を考慮すると、この「報告書等」については、18号監査報告書だけに限定されず、各社の内部監査資料等を活用できる方向へ向かうべきではないだろうか。

日本版SOX法に向けて、日本の金融機関は、外部委託業務の評価手段として何が最適なのかを十分吟味した上で、18号監査の利用を判断すべきである。そして、18号監査を利用する場合には、受託者側と十分に協議して、内部統制範囲の不一致や記述内容不足といった事態を防止し、有効に活用すべきである。 

図表

	米国	日本	英国
公認会計士概数	約33万人	約1.7万人	約13万人
上場会社概数	約5,000社	約4,000社	約3,000社

（出所）公認会計士数：AICPA（米国公認会計士協会）、日本公認会計士協会、ICAEW（イングランド・ウェールズ勅許会計協会）データよりNRI作成。（米国、英国は2005年、日本は2007年）
上場会社数：国際取引所連合データ等よりNRI作成。（2005年）

NOTE

- 1) Sarbanes-Oxley Act of 2002
- 2) セキュリティ上の弱点を発見するために、システムを実際に攻撃して侵入を試みるテスト。
- 3) 公認会計士が提供する、SAS70とは別の監査報告書。名称は、Agreed Upon Procedures（略称AUPs）で、合意された手続きどおりに行われていることを証明する監査報告書。公認会計士の意見は表明されない。
- 4) ICAEW（イングランド・ウェールズ勅許会計士協会）が発行した外部委託業務の内部統制を評価するための監査基準
- 5) 「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準」2007/2/15
- 6) 米SOX法の実施基準（AS2⁷⁾）には、手段の一つとして、SAS70が明記されており、これが、SAS70が脚光を浴びた原因のひとつと考えられる。
- 7) 「Auditing Standard No.2」PCAOB（公開会社会計監督委員会）が策定した監査人向けルール。現在、内容の見直しが進んでいる。
- 8) 金融審議会公認会計士制度部会の中で、公認会計士・監査法人制度の充実・強化が検討されており、平成14年12月17日報告の中で、2018年に5万人という目標数字の例が挙げられている。