

米国の保証業務基準改訂がもたらす効果

SOX法、J-SOX法により財務報告に係る内部統制の有効性評価が義務付けられ、関連業務を外部委託している委託先企業の評価も必要となった。評価には外部委託先が発行する第三者の保証報告書を受領することが多いが、今回その保証報告書の基準が改訂された。委託元企業はこれを機に外部委託先とのリスクコミュニケーション活性化を図るべきだろう。

外部委託先の内部統制有効性評価に係る基準の変遷

米国において2002年に企業改革法（日本では2006年に金融商品取引法）が制定され、上場企業は財務諸表監査に加え、経営者による財務報告に係る内部統制の有効性の評価・証明の監査（内部統制監査）が義務付けられた。いわゆるSOX法（2004年12月期から適用）・J-SOX法（2009年3月期から適用）である。財務報告に影響を及ぼしうる業務（コンピュータシステム含む）を外部委託している企業は、外部委託先における内部統制の有効性の評価が必要となった。しかしながら、企業が外部委託先を評価すること、また外部委託先が複数の委託元企業からの評価に対応することは、双方にとって大きな負担となった。そのため、企業が外部委託先から内部統制の有効性に関する第三者保証報告書を受領し、その内容を確認することにより、外部委託先評価の代替とするという方法が注目された。これが米国監査基準書70号に基づく報告書（いわゆる「SAS70報告書」）である。

「SAS70報告書」は委託元企業に対する監査の基準に基づいた外部委託先の保証報告書であったが、その後、外部委託先の内部統制の有効性評価の基準は、外部委託先の経営者自らが評価・証明し、第三者が保証する保証業務（SSAE：Statement on Standards for Attestation Engagements）の体系に組み込まれた。こうして定められたのが保証業務基準書第16号である。2011年6月以降終了する期間に係る第三者保証報告書については「SSAE16保証報告書」に移行されることとなった。

図表 外部委託業務の内部統制評価基準の変遷

第三者保証報告書の基準	説明
米国監査基準書70号 (SAS70報告書)	Statement on Auditing Standards No.70 委託元の監査の基準に基づく、外部委託業務の内部統制の有効性を評価する基準。
保証業務基準書第16号 (SSAE16保証報告書)	Statement on Standards for Attestation Engagements No. 16 (AT section 801 "Reporting on Controls at a Service Organization" ^(注1)) 外部委託業務の内部統制の有効性に関する保証業務の基準。(AT 801基準「外部委託業務に関する統制の報告書」)
保証業務基準書第18号 (AT-C 320基準)	Statement on Standards for Attestation Engagements No. 18 AT-C section 320 "Reporting on an Examination of Controls at a Service Organization" ^(注2) Relevant to User Entities' Internal Control Over Financial Reporting" いくつかの主題・目的の保証業務の体系を整理した基準。 AT-C 320基準 ^(注2) 「委託元の財務報告に係る内部統制に関する、外部委託業務の統制に関する保証業務の報告書」

(注1) "a Service Organization" は受託業務と訳されることが多いが、本文と整合するよう外部委託業務と訳した

(注2) 保証業務の主題・目的により、AT-C 3nn基準と表記される

(出所) 米国公認会計士協会 (AICPA) 発行の各基準書を基に野村総合研究所作成

「SSAE16保証報告書」の適用から5年が経過したが、より適正な財務報告を実施し投資家からの一層の信頼を得るべく、その他の保証基準との体系整理や各規準の具体化明瞭化が求められるようになった。その結果、複数の主題・目的を持つ保証業務が保証業務基準書第18号として体系整理され、その中で、財務報告に係る業務の外部委託先の内部統制に関する保証業務はAT-C 320基準として改訂された。2017年5月1日以降発行の第三者保証報告書からは当該基準が適用されることとなった。

新しい評価基準の変遷点

保証業務基準書18号 (AT-C 320基準) の要求事項について、従来の「SSAE16保証報告書」から変更された点は主に以下の三つである。

- ① 外部委託先の経営者がどのようにリスクを認識しているかがより一層問われており、独立監査人は経営

NOTE

- 1) 具体的には、独立監査人が経営者にヒアリングを行いリスク認識を把握し、内部監査室等に内部監査結果報告等で統制状況を確認する、というような手続きが想定される。
- 2) 外部委託先が再委託先を含めて統制評価する場合と、再委託先から第三者の保証報告書をもらう場合の二つのケースが想定される。
- 3) 具体的には、サンプリング評価での母数が評価目的全体を網羅しているかの確認、統制運用の証跡（アクセスリスト等）については補正や不適切な選択等が行われていないことの確認、などが想定される。

者とのディスカッション等を通じ、委託先企業におけるリスク統制活動を理解することが求められる¹⁾。

②外部委託先は再委託会社に対する統制活動を求められる²⁾。

③外部委託先の評価に使用する情報の信頼性を担保するため、その情報の網羅性と正確性の観点により求められる³⁾。

これらの改訂内容は、委託元企業にとって以下のような効果をもたらすと推察される。委託元企業の財務諸表監査・内部統制監査では、財務報告上の重要な虚偽表示リスクに注目して監査が行われる。委託元企業が、財務報告に影響を及ぼしうる業務を外部委託している場合、委託先企業における重要な虚偽表示は当然委託元に大きな影響を与える。外部委託先の経営者がしっかりとしたリスク認識を持っていれば、ガバナンスを効かせることにより委託先企業における虚偽表示を抑制でき、結果的に委託元企業のリスク低減に寄与することになる。

また、外部委託先が第三者保証報告書を発行するということは、外部委託先自らが再委託先も含めてリスクを評価し、リスクに対応した内部統制を適切に構築して有効に運用することによりリスクを低減し、その上で業務（コンピュータシステム含む）を委託元企業に提供していることを意味すると言える。

求められるリスクコミュニケーションの活性化

金融機関では、各種のITサービスの利用にとどまらず、クラウドサービスベンダやFintech企業等の利活用が進展し、業務の外部委託範囲が拡大するとともに、外部委託形態も複雑化している。それに伴い、外部委託管

理のあり方や外部委託によるリスクの管理という課題も同様に拡大・複雑化している。こうした状況下では、外部委託先が発行する第三者保証報告書の利活用なしには、効果的かつ効率的なリスク管理・外部委託管理を行うことは難しいと推察する。

ところが、第三者保証報告書の利用にあたっては、委託元企業が一方的に外部委託先の発行する報告書を受領するだけで、それをもって委託元における内部統制評価の代替とするケースも少なからず存在しているのが現状である。金融機関を含め委託元における外部委託先の内部統制評価には、委託元と外部委託先とが互いに共通のリスク認識を有することが欠かせず、そこで初めて有効性のある評価が可能となるのである。今回の基準改定を、委託元・委託先がコミュニケーションを図り、リスクに対する共通認識を醸成する機会とすべきだろう。具体的には、金融機関は自身のリスク認識を外部委託先へ伝え、外部委託先は経営陣自らリスクを識別し金融機関と共有する。外部委託先は共有したリスクを低減する内部統制を構築・運営し、第三者からの保証を得て、金融機関に保証報告書を提供する。金融機関は、外部委託先の経営陣のリスク認識が相違している場合には、積極的に牽制していく。

外部委託の形態がここまで複雑多様化した金融業界においては、このような活動を通してリスクコミュニケーションを活性化していくことが、リスク管理の課題解決に必要なのではないだろうか。

Writer's Profile



小谷 良則 Yoshinori Kotani

金融システムリスク管理部
上級コンサルタント
専門は内部統制
focus@nri.co.jp