外部委託先に求めるシステムリスク管理と保証報告書の活用

金融機関にとって、外部委託管理は重要な経営管理の一つと言っても過言ではない。金融機関が要求するシステムリスク管理を実行可能な委託先か判断する材料として、独立第三者が発行する保証報告書を活用するのも一つの手だ。

2014年2月に起きた地方銀行の外部委託先社員によるカード偽造事件は記憶に新しい。金融機関各社は改めて外部委託管理の重要性を認識していることだろう。金融機関では、自社のシステムリスク管理態勢の整備とともに、外部委託先が金融機関の要求するレベルのシステムリスク管理を実行可能か判断する必要が高まっている。

金融機関に求められるシステム外部委託管理とは

2013年6月12日金融商品取引法等の一部を改正する法律が成立し、銀行等の業務の施行報告徴求・立入検査の対象先が従来の委託先に加え、再委託先（再々委託先など多段階の委託先を含む）まで広がった。また、金融検査マニュアルではシステムリスク管理の観点から適切な委託先を選定することが求められている[1)]。システムリスク管理の観点で留意すべき事項として、例えば①金融機関の合理性の観点からみて十分なレベルのサービスの提供を行い得るか、②委託契約に沿ったサービス提供や損害負担が確保できる財務・経営内容か、③金融機関のレピュテーション等の観点[2)]から問題ないか、などが挙げられる。このうち①に関しては判断が非常に難しい。なぜならば十分なレベルのサービス提供が可能かを判断するためには、委託先のセキュリティ、可用性、再委託先の管理の状況など、システムリスク管理に関する項目を幅広く把握する必要があるからだ。

外部委託先に求めるシステムリスク管理態勢と独立第三者による保証報告書の活用

金融機関が委託先のシステムリスク管理の整備運用状況を判断する材料として、SOC（Service Organization Controls）レポートのような独立第三者による保証報告書を活用するのも選択肢の一つだ。

SOCレポートとは「受託業務に係る内部統制」の保証報告書」のことである。ITサービス事業者など受託会社が、自社のサービスにおける内部統制の有効性や効率性を経営層や顧客に報告するため、独立第三者である監査法人に評価を依頼し発行する保証報告書だ。金融機関はこの報告書を確認することで、委託先のシステムリスク管理の整備状況が自社の基準と比較して許容可能であるか、一定レベルの信憑性の下に確認することができる。

SOCレポートはまた、委託先の直接監査の代替として活用することも考えられる。本来、委託元である金融機関が委託先を直接監査することが望ましいが、共同利用型サービスが増加している中、情報セキュリティの観点から直接監査が困難な場合がある。金融機関が直接監査を実施すると、他の金融機関の情報に触れてしまう可能性があるためだ。こういったケースでは、独立第三者が発行する保証報告書を直接監査の代替手段として利用することも検討してよいのではないだろうか。

米国では、外部委託管理が強化されていく中、リスク管理手法のひとつとして、この保証報告書を有効活用する企業が増加している。金融機関の規制を行うFFIEC（米国連邦金融機関検査協議会）においても、このSOCレポートを発行している委託先会社を選定することをシステムリスク低減の例として取り上げている。

SOCレポート概要

SOCレポートに関しては、AICPA（米国公認会計士協会）によるガイドラインが公表されており、SOC1、

NOTE

1) 金融検査マニュアル（別紙2）Ⅲ．個別の問題点、4.外部委託管理を参照。
2) 例えば、外部委託先と反社会的勢力との関係の有無などを含む（金融検査マニュアル（別紙2）より引用）。
3) SOC3は、サービス事業者がブランディングや競争戦略上、信頼のあるサービスであることを一般に知らせる目的の簡易な報告書。
4) 米国で上場している企業はSOX法により「内部統制報告書」の作成と、「内部統制監査」を義務付けられている。企業は外部委託先の直接監査の代替として外部委託先が発行するSOC1レポートを利用することができる。そのためグローバルな顧客を持つ外部委託先はSOC1レポートを発行しているケースが多い。国内でも、財務諸表に係る内部統制に関する保証基準として日本公認会計士協会発行の "監査・保証実務委員会実務指針第86号「受託業務に係る内部統制の保証報告書」" が存在する。
5) 国内におけるSOC2に相当する基準として、2013年7月に、"IT委員会実務指針第7号「受託業務のセキュリティ・可用性・処理のインテグリティ・機密保持に係る内部統制の保証報告書」" が公表されている。
6) 1992年に米国のトレッドウェイ委員会組織委員会（COSO：the Committee of Sponsoring Organization of the Treadway Commission）が公表した内部統制のフレームワーク。2013年5月14日に改訂版を公表。
7) 可用性、処理の完全性、機密保持の原則に対し、個別に追加となっている基準。
8) 「組織とマネジメント」、「情報伝達」、「リスク管理及び統制のデザインと導入」、「統制のモニタリングの仕組み」、「論理・物理双方のアクセス管理の状況」、「システムの運用」、「変更管理の仕組み」。
9) SOC2レポートの内部統制の項目をFISCの「金融機関等コンピュータシステムの安全対策基準・解説書」の規準項目に対応させた資料を盛り込んでいる点が特徴。

図表　SOCレポート比較

	SOC1レポート	SOC2レポート
目的	委託会社の財務諸表監査に関連する内部統制の評価	以下の内部統制の評価 ・セキュリティ ・可用性 ・処理の完全性 ・機密保持 ・プライバシー
規準及びガイド	SSAE No. 16, Reporting on Controls at a Service Organization	AT 101, Attestation Engagements
報告書の内容	・内部統制記述書 ・受託会社の経営者によるアサーション ・監査人の意見 ・監査人が実施した手続き及びその結果	・内部統制記述書 ・受託会社の経営者によるアサーション ・監査人の意見 ・監査人が実施した手続き及びその結果
利用者閲覧者	限定的 委託会社の経営、監査人 受託会社の経営、監査人	限定的 委託会社の経営、監査人 受託会社の経営、監査人 パートナーなど利害関係者

（出所）AICPA SOC Brochureを基に野村総合研究所作成

SOC2、SOC3[3]の3種類のレポートが存在する。

SOC1レポートとは、従来のSAS70に代わる新基準である米国保証業務基準SSAE16に基づくレポートのことであり、日本でも、J-SOX法という通称で呼ばれている内部統制報告制度において、企業の財務諸表に係る業務プロセスを外部委託する際に、その外部委託先である受託会社が発行したことで知られている[4]。ただし、その目的から報告の範囲が委託会社の財務諸表に係る受託業務の内部統制に絞られるため、外部委託先のセキュリティや可用性などは財務諸表監査等の基準で求められる限定された統制が対象となる。金融機関が委託先のシステムリスク管理態勢を確認する判断材料として活用する場合は、このレポートに加え、委託先のシステムリスク低減に向けた取り組みを更に確認する必要がある。

SOC2レポート[5]は、2011年4月に公表された比較的新しい報告書であり、受託業務の法令順守や運用の内部統制を保証するものである。SOC1レポートで対象にできなかった幅広いシステムリスクに関する統制を報告できるため、金融機関が委託先のシステムリスク管理態勢を確認する上で、判断の手助けとなると考えられる。SOC2レポートでは、COSOフレームワーク[6]のコンセプトに従い整理された共通規準、及び個別の追加規準[7]の遵守状況を確認することができる。共通規準には7つのカテゴリ[8]が定義されており、各カテゴリに遵守すべき統制項目が詳細に定められている。これらの項目に対する遵守状況は、委託先のシステムリスク管理態勢を確認する際の判断材料として利用可能である。

リスクコミュニケーションの重要性

金融庁は金融機関に対し外部委託管理の更なる強化を求めており、今後、システムリスク管理に対する取り組みとして、第三者からの客観的な保証報告を取得するITベンダーの増加が予想される。野村総合研究所もSOC1に加え、2012年よりSOC2レポートを発行している[9]。

金融機関は自社と同等レベルに委託先を管理する必要があるが、よりリスクの高い領域に自社の貴重な管理リソースを集中的に配分し、その他の領域についてはSOCレポートのような保証報告書を活用することで、効果的かつ効率的なシステムリスク管理を実現していくことが望まれる。外部委託管理の重要度の高まりを踏まえ、SOC2に代表される保証報告書を委託先とのリスクコミュニケーションのツールと割り切り、直接管理と併用して活用することを検討してはいかがだろうか。

Writer's Profile

青木 千恵子 Chieko Aoki
ERM事業企画部
主任コンサルタント
専門は監査論
focus@nri.co.jp