

新たなITリスクに立ち向かう 連載シリーズ 第18回 システム関連業務における再委託先管理の 実務

金融機関に限らずシステム開発やシステム運用の現場においては、高度なITスキルの享受や短期間でのシステム開発の実現のために外部への業務委託が盛んに行われている。

一方で、外部委託先がかかわる情報漏えいや情報の不正利用などの問題も発生しており、外部委託先管理の重要性はより高くなっている。

このような状況のもと、金融庁は平成27年4月に「主要行等向けの総合的な監督指針」、「金融検査マニュアル」等を改正した。

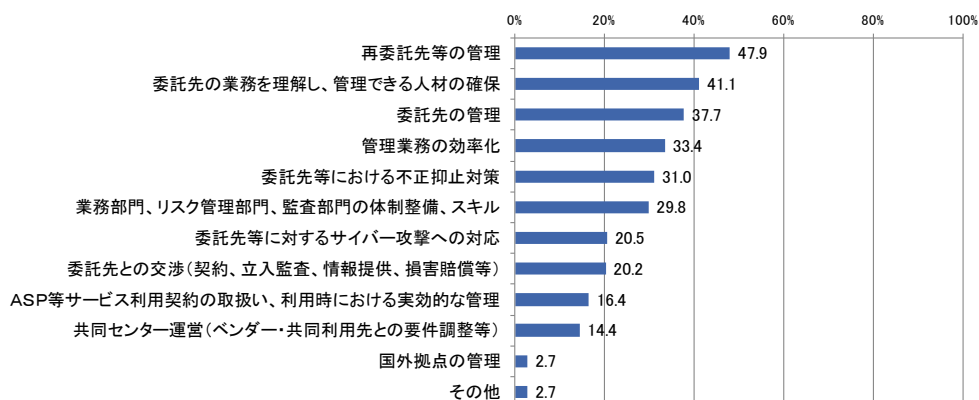
本稿では金融庁の改正を踏まえ、外部委託先管理における再委託先管理の具体的な対応について考察する。

1. 改正のポイントと現状

今般の金融庁の各種ガイドライン改正のうち、外部委託先管理にかかわる点としては、再委託を含む外部委託業務のリスク管理の適切性確保、定期的なモニタリングが挙げられる。これまでは再委託先等の2段階以上の委託先に対し明確な記載がなかったが、今回明示されたことで、2段階以上の委託先に対しても、委託の計画・委託先選定におけるリスク評価と選定後の定期的な評価が求められた。

また最新の金融情報センター（FISC）の調査でも、外部委託先管理にかかわる現在直面している課題として、半分近くの金融機関が「再委託先等の管理」を挙げており、再委託先についての効果的な管理の重要性が伺える。

【図表1】外部委託先管理にかかわる現在直面している課題



出所:公益財団法人 金融情報システムセンター「金融情報システム」(平成27年10月 増刊79号)平成27年度金融機関アンケート調査
結果 36ページを基に筆者作成



2. 再委託先管理の取組み

一般的にシステム開発やシステム運用の現場において、再委託に伴い発生する代表的なリスクとして、以下が挙げられる。

- 再々委託など委託が繰り返されることにより、実際に業務を担う企業の審査が疎かになり、反社会勢力や業務遂行能力のない企業に委託することになる。
- 管理者や監督責任者が曖昧になり、情報セキュリティ管理機能が機能せず、不正／ミス等による情報セキュリティインシデントが発生する。

これらのリスクに対応するために、外部委託先の管理プロセスにおいて各企業ではさまざまなコントロールを実施している。以下に具体的な例を挙げる。

【図表2】外部委託先の管理プロセスにおけるコントロール例

プロセス	コントロール例
再委託に関する方針・規定の作成	• 再委託先についてルールの策定 • 委託業務内容についての再委託によるリスク評価を行い、再委託の禁止や再委託階層の上限を設定する • 「丸投げ」による再委託の禁止
再委託先の審査	• 再委託先に対する審査 － 反社会的勢力チェック － 財務状況 － 免許、資格等の業務遂行能力 － 情報セキュリティ管理体制
委託契約の締結	• 再委託先の責任・義務の明確化 － 1次委託先が委託元に対して負う責任および義務と同等のレベルを再委託先にも求めるため、委託先・再委託先間の契約に明記することを委託元と委託先の契約に定める • 再委託先への立入監査 － 業務内容や状況に応じて、再委託先が負うべき責任・義務について委託元が立入監査、モニタリング等を実施する権利を委託元と委託先の契約に定める • 損害賠償 － 再委託先が何らかの問題を発生させた際には、委託先が賠償責任を負うことを委託元と委託先の契約に定める • 再委託の中止 － 再委託先の業務遂行能力等に対し問題が発生した場合、委託元は委託先に対し、再委託の中止を求めることができることを委託元と委託先の契約に定める
委託契約の管理	• 再委託先の業務状況、情報セキュリティの管理状況を1次委託先から書面で報告させ、それらが十分であることを確認する • 1次委託先から再委託先への情報の受け渡し履歴を作成させる • 委託元による再委託先への立入監査、モニタリングを実施する
委託先の評価	• 定期的な再委託先の審査 • 委託期間終了後の委託先の評価

出所：公益財団法人 金融情報システムセンター「金融機関におけるクラウド利用に関する有識者検討会報告書」20ページを基に筆者まとめ

このようなコントロールの定着には、柔軟な運用も必要になってくる。たとえば、再委託を行う理由として、専門性の高いスキルやノウハウを持った人材が必要であるのに条件を満たす要員が1次委託先にいない、プロパーメンバーでは単価がマッチしないということがあり得る。このような場合には合理性があると判断し、再委託階層の上限の超過についても一時的に許可することや、委託元による再委託先への直接的な立入監査・モニタリングの際には、1次委託先によるモニタリングと重複することのないよう、役割分担やタイミングを調整する。

このような対応を取り入れつつ、再委託先に対しても委託元による積極的な関与を図ることが肝心である。

最近では他に留意、懸念すべき事項として、以下のようなケースが挙げられる。

クラウドの利用: クラウド事業者が実務作業を外部に委託しているケースが見受けられるが、利用企業が多岐にわたるため、利用企業からの直接的な立入監査やモニタリングに応じない場合がある。

EUCシステム: ユーザ部門が外部委託先と直接契約し、EUCシステムの開発業務を委託しているケースが多い。EUCシステムは本番データに直接触れることも多く、その管理の重要性は基幹系のシステムと比較しても変わらないが、日常的に外部へのシステム開発業務を委託している情報システム部門と比較して、ユーザ部門による委託先管理は甘くなりがちである。

モニタリング: 作業負荷等を鑑み、年に1回程度のYes/No形式のアンケートを行う程度に留まっており、実態やリスクを把握できていないとも言えない。委託先も取引を中止にしたいため甘い評価になっている可能性がある(両者が形式を整えることを目的としている)。

これらの固有リスクに対応するためには、これまでの一般的な取組みの他に、より実践的な管理が必要となっている。以下にその例を示す。

【図表3】個別事象における取組み例

個別事象	取組み例
クラウド	- 再委託の条件などについて、契約時に個別に交渉する。再委託先への直接的な立入監査が難しい場合も、外部監査報告書やペネトレーションテストの報告書の閲覧などについて規定する - 海外事業者の場合、審査時に確認できる情報が限られることがあるため、その場合の代替情報を検討しておく
EUC	契約部門に管理を任せるとはせず、リスク管理部門等が全社横断的に関与する仕組みとする
モニタリング	- アンケートによるモニタリングを行う際には、記述式のアンケートとし、その回答内容から質問に対する委託先の理解度を評価する。理解度が足りていない場合は追加の質問を行い、正確な回答を得る 例として以下のような項目が挙げられる <u>企業としての取組み</u> - 情報セキュリティ管理態勢: 想定するリスク、規定、管理責任体制等について - 過去のセキュリティインシデント: 発生有無とその対応、再発防止策について - 内部での立入監査・モニタリング: 方法、頻度、これまでの指摘事項について - 最新動向についての勉強会: 具体的な内容、方法、頻度について <u>受託業務の取組み</u> - 受託業務において想定するリスクとそのコントロール。または現状での抜け道があれば改善策など - 新規参画者や参画終了者を含むメンバーへの教育や、具体的な内容、方法、頻度について。弱点や今後の課題などを含む - 回答において現状は不十分な点があった場合にも、不可と一律に評価をせず、リスクに応じた中長期的な改善指導やリスク受容の選択を含め検討、交渉を行う

3. まとめ

委託先、再委託先はプロジェクトの目標を達成するための重要なステークホルダーであり、外部委託を抜きにしたシステム開発やシステム運用は考えられないのが現状である。またビジネス環境の変化やユーザーニーズの多様化、FinTechに代表される先進的なテクノロジーへの取り組みなどで、今後も外部への依存は高くなると想定される。

そのため将来を見据え、早い段階で経営層が主体となり、再委託先を含めた外部委託先への実行的なガバナンスの仕組みを構築し、規律を促すことが重要となっている。

KPMGコンサルティング株式会社
シニアマネジャー 磯野 央也

KPMGコンサルティング株式会社

東京本社
〒100-0004
東京都千代田区大手町1丁目9番5号
大手町フィナンシャルシティ ノースタワー
TEL : 03-3548-5305
FAX : 03-3548-5306

大阪事務所
〒541-0048
大阪市中央区瓦町3丁目6番5号 銀泉備後町ビル
TEL : 06-7731-2200

名古屋事務所
〒451-6031
名古屋市中区牛島町6番1号 名古屋ルーセントタワー
TEL : 052-571-5485

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供するように努めておりますが、情報を受け取られた時点及びそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

©2016 KPMG Consulting Co., Ltd., a company established under the Japan Company Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.