FinTechで露呈する「外部委託先」管理の限界

FinTechの進展によって、金融機関の提携先・関係会社が増え、「リスクの外部割合が高まる」傾向にある。その際、いざ提携先で障害が発生すると、事業継続が困難になることにより、金融機関側まで直接的な影響や風評被害を受けることになる。こういった広義の外部委託先管理の巧拙が、ビジネスの成否に潜在的な影響を及ぼすと考える。

伸び切る兵站 －「外部委託先」管理の限界－

この数年、当局の指針や指導などで金融機関における外部委託先管理は強化される傾向にあり、現在では末端の再委託先まで管理することが一般的になっている。それでも現在の外部委託先管理では、FinTechで広がるビジネス戦線を『包括的』に管理できていないと考える。

その原因の一つは、「対象による管理態勢の濃淡」にある。今後増加が見込まれる提携先は、厳密な意味では金融機関からの委託契約による「外部委託先」に当たらない。そのため通常の外部委託先管理とは異なる主管部署で異なる手法で管理されることが多い。関係会社なども同様である。管理態勢に濃淡があることで、経営の目線から見て、包括的に外部委託先を比較することができなくなっている。

また、実施部署レベルで見ると、同じ外部委託先カテゴリーであったとしても、「本社機能がサイロ型で機能」しているため、総合的な観点が不足していると思われる。調達管理部は各企業を財務の観点で、情報セキュリティ部は情報漏えいの観点で、リスク管理部は事業継続の観点でなど、それぞれに外部委託先を管理している。しかし、「それらの観点をすべて集約して総合的に評価をし、経営に報告」はされていないのではないだろうか。

より大きな課題は、「リスク評価プロセスの不足」である。多くの金融機関はある意味真面目であり、“お上”が定める基準を満たしているか否かを確認することは怠らない。安全対策基準や検査マニュアルをもとにしたチェックリストでの確認やヒアリングは行っている。だがそのチェックリストの良し悪し以前に、外部委託先を活用している現場部門にチェックリストの記載を依頼した場合、当該委託先を活用したい立場の現場部門が「問題がない」と記載することも危惧される。そもそも、統制を実施しているか否かのチェックリストでは、提携先がどのようなリスクが内在する業務・機能を実施しているか確認することはできない。

リスクベースでの「サードパーティ」管理へ

伸び切った兵站を立て直すためには、VMO（Vendor Management Office）と呼ばれる、包括的に外部委託先管理を行う組織を設置、もしくは役割を誰かに持たせ、ライフサイクルのすべてにおいて、そのフェーズに応じた評価・モニタリングに関与させることが必要だと考える。

米国で金融機関のリスク管理担当者と話をすると、米国通貨監督庁（Office of the Comptroller of the Currency）の規制強化以降、外部委託先の定義を委受託の契約関係だけでなく自らの組織の事業上の合意関係にまで広げ、提携先や関連会社・子会社さらには合弁会社までを対象として、それらを包括的に管理するVMO機能を強化してきている（これ以降、委託先として提携先や関係会社・子会社さらには合弁会社まで対象を広げたカテゴリーを、所謂「外部委託先」と区別するために「サードパーティ」と呼ぶ）。日本でも、金融機関によってはIT部門の中にVMO組織を構築・運営している例はあるようだが、対象を米国のように全社視点でサードパーティまで広げている例はあまり聞いたことがない。

新たに設置されたVMOの最も重要な仕事は、当然のことながら包括的な視点でのサードパーティのリスク評価である。サードパーティまで広げると相当数の企業が

NOTE

1) OCC 2013-29, Third-Party Relationships, Risk Management Guidance.

対象となるのだが、VMOを中心に包括的なリスク評価を行い、リスクレベルごとにサードパーティの重要度を区分けしている。

リスク評価にあたっては、まず情報セキュリティや事業継続など個別のリスク主管部署が固有リスクと残存リスクという二つの観点について評価を行い、それをVMOでとりまとめて重要度の区分けを行っている。固有リスクについては、「どのサードパーティに業務を任せるか」ではなく、金融機関内部の「どの業務・機能を外部化するか」が大切だと担当者は力説していた。実際にサードパーティと仕事を行う現場のIT部門や事務部門の責任者がどのような業務・機能を外部化するのかを明確に定め、その業務・機能がOCCガイダンス[1)]に謳う「重要活動」に該当するか否かを判断する。その上で、当該業務・機能を任せるサードパーティの情報セキュリティや事業継続など各リスクカテゴリーの統制状況を確認し、残存リスクを見極めている。VMOではそれらを総合して包括的に判断を行い、サードパーティを3〜5つの重要度に分類し、それに応じた管理を行っている。最も重要度の高いサードパーティ群については、契約等を締結する前の精査をVMO自身がオンサイトに出向くなどして行い、サービス開始後も統制状況のモニタリングだけでなくサービス内容の変化・リスクの変化について「対話」を欠かさないようにしているようである。

日本の金融機関の方にこうした話を紹介すると、「そこまでやるのですか・・・」という反応が返ってくることが多い。しかし実は、サードパーティを1000社も抱える金融機関でも、最重要に区分けされるサードパーティは5社〜10社程度しかいない。リスク評価を徹底する事が、その後のモニタリングを効率的かつ効果的なものとしている。当局などがリスクベースアプローチを徹底していくと言うと、一見、外部委託先管理の負荷を増やすようにも思えるが、長い目で見ればそうしたアプローチは外部委託先管理を効率的に運用するために大切なプロセスなのだ。

今後は、より早期にVMOをFinTech検討に巻き込むことが必要になると考える。最近では金融機関でも、FinTechベンチャーと提携開始する前に、PoC（Proof of Concept）もしくはプロトタイプと称して、サービスの実現可能性を共同で検証する場合も多い。仮に当該サービスにリスクが存在した場合、そのリスクを受容しないとするとリスク低減の対策実装には時間とコストがかかる。そのため、PoC／プロトタイプ検討の極めて初期段階からVMOを巻き込みリスク評価を行うことが大切になってくる。Regulatory Sandbox（もしくは単にサンドボックス）と呼ばれる仕組みは、極めて初期の段階から監督当局をもリスク評価の観点で巻き込んだ有効なリスク評価活動だと言える。

昨今、金融機関とFinTechベンチャーとの動き、特にリスク管理面の議論を見ていると、APIチェックリスト等の統制実施状況を確認する際の細かさや厳格さにばかり焦点が当たり過ぎているように感じる。そこだけに議論を集中せず、リスクベースという言葉を今一度確認し、外部委託先管理のあり方を抜本的に見直すことが重要なのではないだろうか。

Writer's Profile

能勢 幸嗣 Koji Nose
金融システムリスク管理部
部長
専門はリスクマネジメント
focus@nri.co.jp