デジタル・ガバナンス改革
FinTechを停滞させるリスク管理の呪いを解く

能勢幸嗣

CONTENTS

要　約

1　日本の金融業界におけるリスク管理のあり方が「呪い」となって企業のFinTech推進を停滞させているのではないか。

2　関連するプレイヤー別にリスク管理に影響を及ぼしそうな変化を整理してみると、リスク管理部門は3つの重要な問題に直面していることが明らかになってきた。

—対策基準やガイドラインが後追いであるために「未知のリスクとの遭遇」の可能性が高い

—外部との提携が増えることによって、これまで以上に「リスクが顕在化する可能性が高い」

—提携先が増加することで、それらの「提携先のリスク管理レベルに差異」が生じる

3　それらの問題に対処しFinTechを加速させるために、「リスクに対する経営の認識を高める」「現場と共に業務を機能軸で考えるリスク管理組織へ」「社外も含めた系全体での危機管理体制強化」「顧客へのリスク・インフォーム」という4つの観点で改革を進め、現場と共に攻めと守りのバランスを取ることのできる『デジタル・ガバナンス』組織へと変化することが必要となってくる。

4　また、提携先が増加し、かつそれらのリスク管理レベルの差異に対処するために、「外部依託先」の概念を提携先や関係会社まで拡大し、それらを全社で一元的・包括的に管理を行うVMO（Vendor Management Office）の新設もしくは既存VMOの変革も必要である。

Ⅰ 端緒となる問題意識

FinTechという言葉がはやり出して数年経つが、なかなか売上規模の大きな金融サービスが登場しない。その原因の一つには、他国に比較して、日本の金融サービスが既に低コストで多くの人に使われているという背景・環境があるのかもしれない。ただ、リスク管理を生業とする立場から見ると、日本の金融業界におけるリスク管理のあり方が呪いとなって、企業を縛り付けているのではないか、リスク管理が変われば利便性が高く・低コストのサービスを後押しできるのではないか、と思うことがある。

金融庁などの監督官庁およびその関係者も、FinTechを推進・普及させるために、FinTechサポートデスク、FinTech実証実験ハブ、銀行のAPI開放といったさまざまな施策を打ち出している。しかしながら、今まで事細かにルールを設定してきたことが、既存の金融機関には「待ち・当局依存」の体質として染み込み、それが呪いとなって自発的に先取りして対策を講じることをためらわせていることが考えられる。適用するガイドラインがないために、新しい技術を採用する際にリスクが放置されていたり、また提携先が多く、かつ動的に変化することで実は大きなリスクを抱えているにもかかわらず、リスクの存在に気づけていなかったりすることも考えられる。

Ⅱ リスク管理包囲網

では、FinTechを加速しようとする事業部門に対して、後押し・伴走するようなリスク管理部門とはどのような変化を遂げるべきなのだろうか。それを検討する前に、そもそもリスク管理がFinTechの進展によってどのような影響を受けているかについて、「顧客」「新規金融業参入者」「金融機関」「外部委託先」「規制当局」そして「外敵」という関連プレイヤー別にリスク管理に影響を及ぼしそうな変化を整理してみたい。

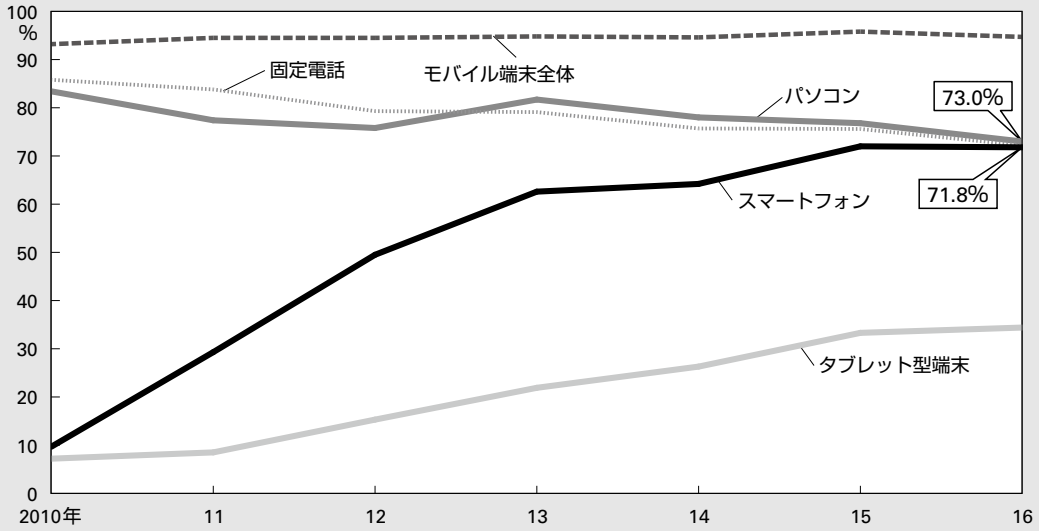
1 顧客＝入り口が変化

FinTechを後押しする顧客の変化要素は複数存在する。少子高齢化や大都市への人口集中などの人口動態の変化や、共働き世帯の増加や電子取引の増加によるライフスタイルの変化などさまざまな要素が考えられる。その中で、最も大きな要因を挙げるとすれば、「スマートフォン・タブレットなどモバイルの普及」であると考える。

既に以前よりインターネットや携帯電話の普及に伴い、店舗に行かなくても取引できるインフラは整備されていた。確かに店舗に行く必要性は低下したが、その使い勝手やインターフェースの面から、主に家庭内における使用が多く、その結果、インターネットバンキングの普及率はここ数年思ったほど伸びていなかった。そこにスマートフォン・タブレットといったモバイル端末が登場することによって、その使い勝手やインターフェースが大幅に改善されたために、「いつでも、どこでも」型の金融取引が加速している。

これにより、「『金融サービス』が『日常生活』に組み込まれる」ものになっていく。今までは、極端な言い方をすると、買物や旅行といった消費行動（＝日常生活）を行うと、そのために「別途、改まって」金融機関に出

図1　スマートフォン・タブレット端末の普及率



出所）総務省「平成28年通信利用動向調査」より作成

向いてお金を引き出したり、借りたりする必要があった。ところが、モバイル端末の普及・使い勝手の改善によって、金融サービスが日常生活と密接に連動することが可能となり、消費者は金融サービスを「意識せず」にその場で利用することが可能となる。

利便性の向上は消費者としてはうれしいが、金融サービスを提供する企業のリスク管理側の視点で考えてみると、自らの管理権限が及ばない場所が取引の入り口となっていくともいえる（図１）。

2　新規金融業参入者＝提携先の増加

では、競合環境はどうだろうか。新規のFinTechベンチャーの登場に伴い、既存金融機関が淘汰されるシナリオも想像されたが、実は共存共栄が進み、金融機関の提携先・関連会社が増える傾向にある。

既存金融機関と機能的に重複するために、当初FinTechベンチャーは金融機関と競合するとも考えられていた。しかし、顧客基盤を持たないために、ビジネス拡大にあたってFinTechベンチャーによる単独展開では苦戦することが想定され、結果としては彼らの多くが金融機関との提携という道を選択している。金融機関側も、自らFinTechサービスを立ち上げることを模索するが、人材面・インフラ面、そして何より会社のカルチャー面などから、自社内部で立ち上げることが難しく、提携や関係会社化などを選択することが多々見られる。アンバンドリング化から、既にリバンドリングが進行しているともいえる。

このように、FinTechの進展に伴って提携先や関係会社が増えることで、リスクの「外部割合が高まる」傾向にもある。最近の提携の特徴は、リスク管理体制にギャップがある企業同士の提携が増えている点にある。金融機関は、金融庁を中心とする監督当局の指針・ガイドライン・マニュアルなどに従い、

内部統制面の体制整備を行ってきた。

一方、FinTechベンチャーは監督官庁が金融庁ではない場合も多く、内部統制面の体制整備についても、金融機関とレベル差が生じている。さらにFinTechベンチャーが起業段階であるほど、リスクという守りに対する組織文化や人員数・専門性といった体制面が脆弱であることが考えられるため、そのレベル差はさらに大きくなる。

加えて、提携という対等な関係や関係会社・子会社という資本関係にあることが、その差を埋めることを難しくしている。外部委託のように委託・受託の関係ではないために、委託元が委託先にその「上下関係」から半ば強制していたようなことは難しくなる。むしろ最近の金融機関とFinTechベンチャーとの提携では、FinTechベンチャーの方が顧客からの依頼・承認を受けて、顧客の代理として金融機関に保管されている顧客本人の情報を引き出したり、取引を行ったりしており、逆に金融機関の方が「委託先」ともいえる状況にある。

このような関係の下、どのように互いにリスクを管理していくのだろうか。ビジネスが順調な際には陰に隠れているが、いざ提携先で障害発生により事業継続が困難になることや、情報漏えいを生じることで、直接的な事業継続面での影響や風評被害を受けることも考えられる。こういった広義の外部委託先管理の巧拙が、潜在的なビジネスの成否に影響を及ぼすと考える。

3　金融機関＝社内のリバンドリング

前述のように、既存金融機関にとって脅威となるような新サービスは少ないように感じる。脅威も少ないが、見方を変えると、金融機関にとっても「新規事業」といえる規模の事業も見つかっていないともいえる。そのため、昨今の金融機関におけるプレスリリース状況を見ると、RPA（Robotic Process Automation）やAI（人工知能：Artificial Intelligence）を活用した社内の業務改革の方にFinTechの効果を求めている感がある。

RPAやAIを活用した業務改革は、社内のリバンドリングともいえる。つまり、業務から人をアンバンドリングし、RPAやAIと業務をリバンドリングすることによって、コスト削減効果を期待するものである。RPAやAIを導入することで業務改革が成し遂げられる可能性も高いが、内在するリスクも変化

表1　大手金融グループにおける業務改革目標

	みずほ	三菱UFJ	三井住友
店舗	2024年度末までに500拠点のうち100拠点を削減	2023年度末までに516店のうち最大100店を「セルフ型」に転換	2019年度末までの3年間に500億円以上を投じ、全店舗のデジタル化を推進
人員	2026年度末までに1万9000人を削減	同6000人程度の自然減	同4000人分の業務量を削減
効果	1000億円台半ば	2000億円	中期で1000億円

出所）『日本経済新聞』2017年12月26日より作成

する可能性が高いということも忘れてはならない（表1）。

たとえばRPA導入を活用した業務改革を想像してほしい。RPA導入により、人手による事務処理がシステム（RPA）に置き換わり、事務ミスによるオペレーショナルリスクは低減する。しかし一方で、RPAを導入することでRPA自身の改ざんリスクやセキュリティリスクを管理する必要が生じてくる。つまり、リスクの所在が事務からシステムにシフトし、リスク顕在化の頻度は下がるが、発生した場合の影響度は格段に大きくなる。このように社内のリバンドリング化の影響は、大きく、かつ動的である。しかも、後述するように、一般的にそれらのリスク管理のガイドラインとなるべきものの整備が追いついていないのが実状である。

4　外部委託先＝所有から利用への流れ

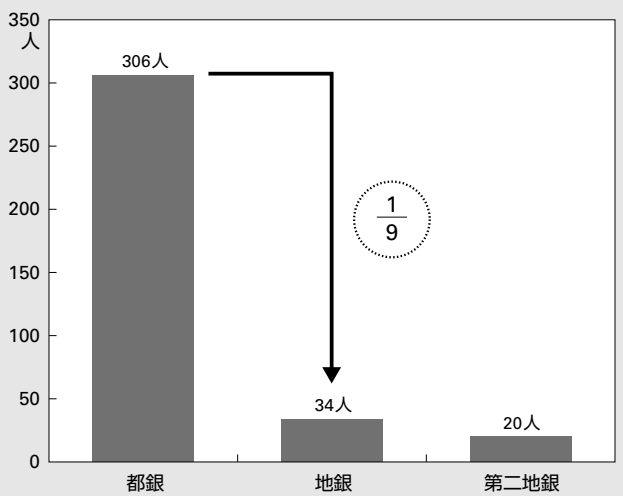
サービス提供の手段となるシステムについて、所有から利用への流れが加速している。所有から利用へとシフトすることでメリットも大きい一方、FinTechと提携する、もしくは迎え撃つ守備側ともいえる金融機関、特に中小金融機関において人材不足という構造的な弱みが生じている。

所有から利用への流れは、サービスを開始したてのFinTechベンチャーにとって、メリットは大きい。彼らは、クラウドサービスなどを活用することで、自前のデータセンターを保有しなくても、事業規模に応じて適宜適切にサーバーなどのインフラ面を拡張、場合によっては縮小することが可能となる。会計などの間接部門機能についても外部化を行うことができる。そのため、自社にいる社員は、自らのコア領域であるアプリケーション開発やマーケティングに専念できる状況がつくられている。

一方の金融機関はどうだろう。当然、金融機関にとってもメリットはある。ノンコアともいえるバックオフィスシステムについては、共同利用型システムの利用が進みつつある。それに伴い、毎年の運用コストや法制度改革対応などのコストの低減が図られている。しかし一方で、地銀などの中小金融機関にとっては、基幹系を中心に共同利用化が進むことで、IT人材が少なくなってきている。正確には卵とニワトリのような関係であり、どちらが最初の原因であるかは不明だが、共同化が人材不足を加速しているのは確かだと考える。

日本銀行の調べによると、勘定系システムの共同利用は、2013年段階で67％弱まで進んでいる。そのためか、地方銀行におけるIT関連部門社員数は平均34名にとどまってい

図2　中小金融機関におけるIT関連部門社員数（2017年）



出所）金融情報システムセンター「平成30年版　金融情報システム白書」より作成

る。国内金融機関のIT部門における通常の業務運用（RTB：Run The Bank）と業務改革（CTB：Change The Bank）費用では、前者が8～9割を占めるとされていることから考えると、FinTechのような新しいテーマに取り組むことができる社員は5名もいないと思われる。そのような少数のIT人材でFinTechに挑むとすれば、自行とFinTechベンチャーに加えて共同利用型サービスを提供する大手SI会社の三者で、システム要件や接続様式、さらに責任分解点などについて検討・対応することが求められる（図2）。

5　規制当局＝新法・ガイドライン検討のタイムラグ

行政もFinTechを推進するために、積極的に動き出している。銀行法を改正し、同時にAPI開放を推進している。また、FinTechサポートデスクの設置やFinTech実証実験ハブを設けることで、より具体的に企業を支援しようと試みている。監督局と検査局の一体化や検査マニュアルの廃止も、FinTech推進の一助となると考える。

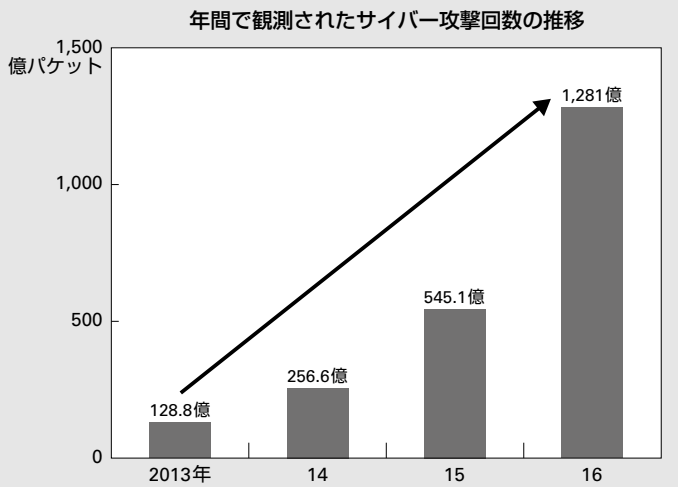
ただし、それらのサポートも十分ではない。新サービスの検討や新技術の活用にあたっては、どの法律やガイドラインが適用されるのか、多くの企業が迷っている。確かに、野村総合研究所（NRI）でも、顧客金融機関から、「新技術適用や新サービス検討時にどのようにリスクを考えるべきか」という、いわゆる正解のない問い合わせが増えつつある。

金融機関のそのような迷いを低減させるためにも、金融庁は機能別・横断的な金融規制の見直しに着手し始めている。また、複数の業界団体などでもAIやブロックチェーンなどの技術に対するリスクやガイドラインの検討を開始している。ただし、それらの活動はどうしても後追い的なものとなり、たとえば法制度の統合にはスタディグループやワーキンググループにおける検討と具体的な法制化、およびその施行までの準備期間を考えると、早くても3年はかかるものと思われる。その検討の間にも新しい技術やサービスが出現することが考えられる。それらの新技術やサービスを顧客向けに提供することで、どのようなリスクが新たに生じるかは未知数である。

6　外敵＝サイバー攻撃増加

昨今、サイバー攻撃による不正送金やシステムを人質とした身代金事件が確実に増加傾向にある。その手口も徐々に巧妙になり、確実にこれまで述べたようなサービスネットワークの弱点を突いてきている。たとえば、地銀の場合、その取引先である中小企業の安全

図3　サイバー攻撃の増加



出所）国立研究開発法人 情報通信研究機構「NICTER観測レポート2016」より作成

対策が脆弱であるため、地銀自体がしっかりとシステムを管理していても、その取引先中小企業のパソコンを乗っ取り、IDやパスワードを盗み、利用者になりすまして不正送金を行うような事例が多発している。前述のように提携先が増えていくことは、そのような弱点が増えることを意味している（図３）。

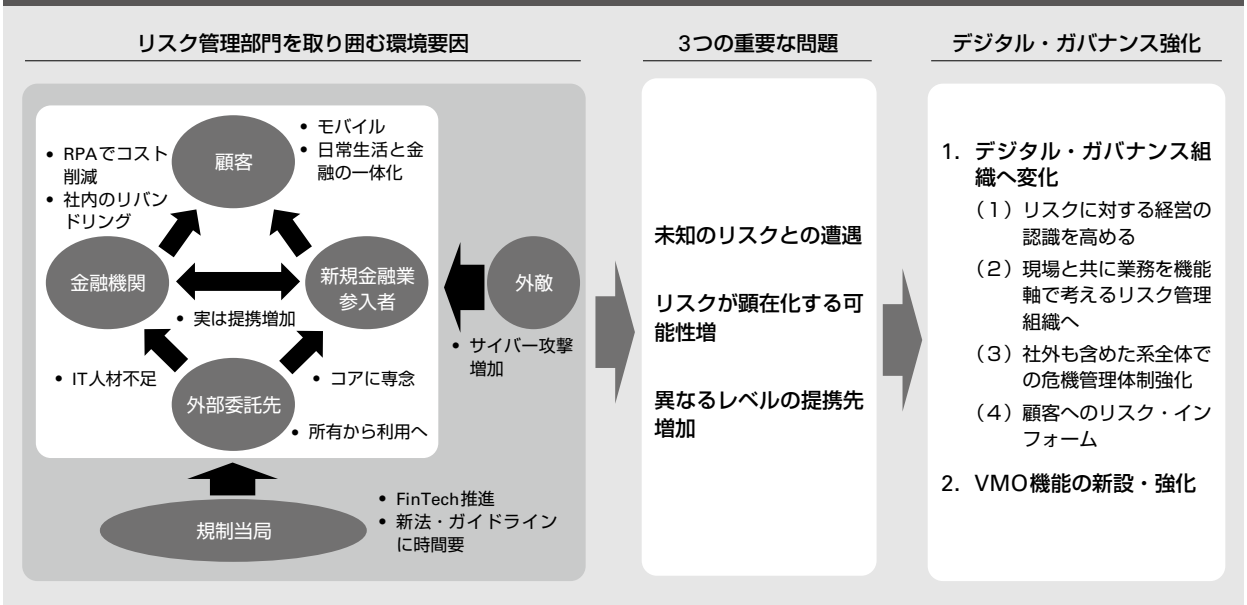
Ⅲ リスク管理からデジタル・ガバナンスへ

前章において、リスク管理を取り囲む要素をプレイヤー別に整理することで、デジタル時代のリスク管理における３つの重要な問題が浮き彫りになってきた。

一つ目は、対策基準やガイドラインが後追いであるために「未知のリスクとの遭遇」となることである。新しい技術・新しいサービスモデルが登場するが、それらに適用すべき業法を選択することや、具体的な業法の解釈が難しかったり、統制面でのガイドラインとなるべき検査マニュアルやFISC（金融情報システムセンター）安全対策基準などが未整備であったりする状況が頻発するものと想定される。そのような未知のリスクと遭遇した場合の対応方法を整備する必要がある。また、ビジネスモデルの変革頻度が今までよりも高まるために、リスクの所在や影響度、発生確率なども常に変化することとなる。

二つ目は、外部との提携が増えることによって、これまで以上に「リスクが顕在化する可能性が高い」という点である。昨今のサイバー攻撃の増加傾向は今後も継続するものと思われる。そこに、未成熟な企業との提携が増加、さらには自社・提携先の業務がダイナミックに変化することを考慮すると、構造的な脆弱性が大きくなるため、残存するリスクが顕在化して事業継続に影響が生じることや、提携先から情報が漏えいすることを前提とした対応も必要になってくる。

図4　デジタル・ガバナンス強化



最後の三つ目は、提携先が増加することで、それらの「提携先のリスク管理レベルに差異」が生じる点である。外部委託先もあれば、ジョイントベンチャー形式の関連会社もあれば、単なる提携先の場合もある。しかも、それらが同じ金融業界の成熟した企業であったり、まったく異業種のスタートアップで統制面が未熟な企業であったりする場合も考えられる。また、提携に際して、システム部門が契約する場合もあれば、本社が契約するような場合もある。提携先だけでなく自社側においてもリスク管理体制が異なり、かつそれらの提携先が増加する実状に対して、提携先の残存リスクに応じた管理が必要となってくる。

リスク管理部門は単に3つの問題に対応するだけでは不十分である。十分条件として、ビジネス創出のスピードを落とすことなく、現場と共に動きながら、攻めと守りのバランスを取る役割を担う「デジタル・ガバナンス」組織へと変革しなければならない。デジタル・ガバナンス機能としては、既存のリスク管理組織を、アクセルとブレーキのバランスを念頭に置きつつ、4つの観点で変革することが必要となると考える。また、異なるレベルの提携先を包括的に管理するために、VMO（Vendor Management Office）という新組織を構築することが必要になってくると考える（図4）。

1　デジタル・ガバナンス組織へ変革するための4つの視点

（1）リスクに対する経営の認識を高める

未知のリスクと対峙するためには、COO、CTOなど、経営レベルの人間がリスクの有無を認識し、サービス検討開始からサービス終了までの間、適切なタイミングでそのリスク動向についての収支状況や戦略リスクと共に判断を行うような会議体などを設定し運営することが必要となってくる。

経営レベルのガバナンス体制といっても、金融機関と非金融機関では、その対応に若干の差がある。金融機関においては、新サービスや新技術の導入時に、リスクについても考慮されている場合が多い。ただし、2点ほど見直すべき点がある。

一つは、あたかもリスクがゼロにできることを前提としているが、実際にはそうはいかないという点である。現状、金融機関のシステムリスク管理は、当局などが定めた検査マニュアルやFISC安全対策基準に従った「統制チェック」となっている場合も多いのではないだろうか。多くの場合においては、経営側を忖度した現場が、すべての項目に「○。実施しています」と素直に統制を実装している、もしくは単にそのように回答している。

それはあたかも、「すべて統制し対応しています。リスクはゼロです」と主張しているかのように見える。「リスクはない」ということが暗黙の前提となっているともいえる。しかし、現実には○と回答している項目に関しても、事務ミスやシステム障害などは発生している。今後、新サービスや新技術導入においては、提携先が増えることで構造的な脆弱性が増え、未知のリスクに遭遇する可能性も高まると考えられるため、今までと同様のリスク対策を実装できるとは思いにくい。つまり、現実にリスクは残存するということが前提であり、そのような報告が必要となってくる。

もう一つは、タイミングの問題で、サービス開始のタイミングだけでなく、その後のリスク管理も重要ということである。サービス開始時には収支・戦略と一緒にリスク管理が徹底して行われているとして、サービス開始後には収支・戦略面のレビューはあったとしても、リスク面の変化について確認されていることは少ないと思われる。この点についても改善が必要だと考える。

異業種が金融サービスへ参入する場合、金融機関と比較すると、どうしても新サービス開始時のリスク認識が不足している場合が多い。特に非金融機関にとっては、金融業界の厳しい法律への対応およびモニタリング体制などを整備し適切に運用することは一つの壁になっている。法律の実務指針やガイドラインの例示などを厳格に適用し、残存リスクがゼロとなるように対策を講じようとすると、サービスが高コストになったり、柔軟性がなくなったりする。金融独特の法律に対応し、かつ低コストで革新的なサービスを提供するためには、法律の立法主旨や背景を理解・咀嚼した上で、自ら説明責任を果たせる「良い塩梅」のリスク管理水準を見極めることが求められる。

(2) 現場と共に業務を機能軸で考えるリスク管理組織へ

リスクに関して経営レベルに適切な報告を行い、正しい意思決定を行ってもらうためには、現場のリスク管理部門についても、機能軸で現場と一緒に考える組織へと変革することが求められる。

以前は、新事業をスタートするために時間をかけて戦略を立案し、人や不動産などの経営資源に投資することが求められた。しかし、デジタライゼーションの進展は戦略に自由度を与えた。

デジタル化投資は人や不動産のように比較的流動性の低い経営資源への投資があまり必要でないという特徴があるために、戦略を深く検討するよりも、PoC（Proof of Concept）という形でデジタル技術を活用したシステムおよびサービスモデルを、実際に構築して試行してみるというやり方が主流となっている。

その際、今まで取引のない新しい企業との提携や、既存システムや業務プロセスとの連携が必要不可欠になってくる。社内と社外を分け、またシステムと人手による事務を分けてリスク管理を行うのでは、十分にリスクを認識できない恐れがある。

これについては、「機能ベース」という言葉が一つのヒントであると考えている。平成29事務年度金融行政方針でも、今後アンバンドリング化が進むと、金融機関などの組織を単位とした「業態ベース」に規制をかけるのではなく、預金・決済といった「機能」のどこにリスクが存在するかを見極め、規制していく必要があると述べられている。

現状、金融機関のシステムリスク管理は、金融庁監督指針や検査マニュアルの構成に倣ったのか、事務リスク管理と分別して管理されている。そのため、機能全体での管理が弱くなる懸念がある。

サービス・業務の設計時には、多くの金融機関で、顧客に対するサービス・業務プロセスについて、人手による事務処理やシステム処理、外部委託を一気通貫してオペレーション機能全体として把握し、その中で業務継続・情報漏えいといったリスクの所在や、そ

れらに対する統制をトータルな目線で検討している。

しかし、いったんサービスの提供が開始されると、プロセスの中に境界線が構築され、システムリスク管理担当部門は「システムだけ」、あるいは「システム外部委託先だけ」を分別して管理している。このため、サービス開始から数年経過すると、サービス・業務プロセス全体のリスクについて語れる人が少なくなってしまうというのが現状かと思われる。

今後は、金融機関でも、送金や決済、融資など、顧客にサービスを提供するオペレーションの「機能」を一体として、頭から尻尾まで定常的に管理する体制に戻る必要を感じる。業務プロセスを社内と提携先・外部委託先やシステムまで含めて記述し、そのどこにどのようなリスクが存在するかを図示・記述するようなオーソドックスなリスク抽出を徹底することが求められる。

確かに、システムは専門性が高く特殊な知識が必要である。しかし、時代の変化・環境の変化を見ると、オペレーショナルリスクを事務リスクとシステムリスクとに二分し、システムリスクだけを特殊な括りで管理する時代は、終わりを迎えているのではないだろうか。

もう一点、付け加えるとすれば、リスク管理組織のスタンスを、より現場寄りに変更することだと考える。一般に企業のリスクに対する守備体制を語る際に、3ライン・ディフェンスという考え方がある。サービスを提供しつつ同時に統制を行う現場を一線（1stライン）とすると、リスク管理部門を二線（2ndライン）、監査部門を三線（3rdライン）と呼ぶ。

リスク管理部門は、現場ではないが、現場を支援する二線の立場であるにもかかわらず、現実的には第三者的な、ともすれば三線である内部監査的な発言をする人も多い。事業検討やサービスの迅速さを追及するのであれば、より現場に近い「1.5線」的な活動こそが求められるはずである。そのために、現場である一線と二線とのローテーションや、攻めを考える事務企画機能と、守りを考えるリスク管理機能の統合などを検討することも必要であると考える。

（3） 社外も含めた系全体での危機管理体制強化

新技術や新サービスであるからリスクが残るだけでなく、サイバー攻撃が増加し、かつその手口が高度化していくため、情報漏えいを中心としたリスクが顕在化する可能性が高い。また、提携先が増えるに伴い、それぞれのサービスをつなぎ合わせる「接点」が増えるため、情報漏えいのリスクが高まる。さらに、一社のサービス停止が全体としての業務停止につながるというリスクが高まり、いったん停止した場合の原因究明や復旧に時間がかかることが想定される。

残存するリスクが顕在化して事業継続に影響が生じることや提携先から情報が漏えいすることを前提とすると、社外も含めたサービスの系全体での危機発生時の連絡体制や事業継続プラン立案、さらにはそれらを前提とした訓練が今まで以上に重要となってくる。

（4） 顧客へのリスク・インフォーム

特に金融機関の場合、前述の（1）～（3）の

視点でリスク管理機能の強化を図り、企業として善管注意義務を尽くした対応をしたとしても、いざリスクが顕在化すると消費者はクレームの声を上げる。古くから存在する金融機関に対して消費者は、あまりリスクがなかった時代の信頼を引き続き持ち続けている。そのため、FinTechベンチャーが問題を起こしただけでも、提携先である当該金融機関へ、とばっちり的にクレームが寄せられる可能性や、風評被害が生じる可能性が考えられる。

その解決のヒントは、金融庁の森長官がある講演の中で使った「インフォームドコンセント」という言葉にある。FinTechが加速するということは、利便性の高いサービスが低コストで利用可能になる、つまり、消費者にとってのリターンが大きくなるということである。しかし、リターンが大きくなるということは、当然リスクが増える可能性も高くなるということになる。それを消費者にしっかりと知らせる、つまり「インフォームドコンセント」の重要性を挙げている。これは、もともと医療現場で使われるようになった概念だが、医療現場においても医療事故訴訟が増加してから一層徹底されるようになっている。FinTechにおいても、自らのサービスが抱えるリスクおよびそれに対する自社の考え方を整理し、分かりやすい形で説明することが重要になってくる。

2　VMO機能の新設・強化

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、増殖する異なるレベルの提携先までを「包括的」に管理することは難しい。新しく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。

現状の外部委託先管理では不都合な理由は幾つかあるが、その原因の一つは、「対象による管理体制の濃淡」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。管理体制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、同じ外部委託先分類として管理されていたとしても、「本社の各リスク主管部署がサイロ型で機能」しているため、総合的な観点が不足すると思われる。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」されては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、当局が定めるガイドラインや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基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。

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（OCC：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含め、いわゆる「外部委託先」と区別するためにOCCに倣い「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にまで広げている例はあまり聞いたことがない。

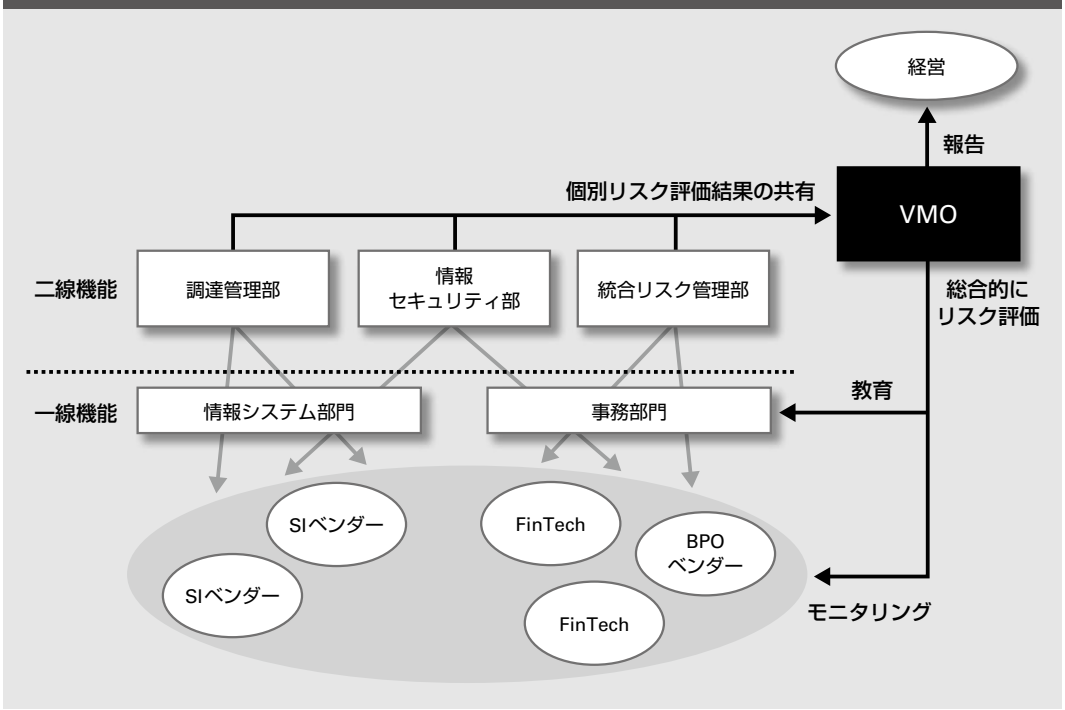
欧米において企業内に設置されているVMOの最も重要な仕事は、当然のことながら包括的な視点でのサードパーティのリスク評価である。サードパーティまで広げると相当数の企業が対象となるのだが、VMOを中心に包括的なリスク評価を行い、リスクレベルごとにサードパーティの重要度を区分けしている。

リスク評価にあたっては、まず財務リスク、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[注]にうたう「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リスク分類ごと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、契約などを締結する前の精査において、VMOのメンバー自身が当該企業の現場に出向くなどして、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。

日本の金融機関の人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５～10社程度しかない。すべてのサードパーティについて包括的なリスク評価を徹底して行うことが、その後のモニタリングを効率的

図5　VMOの位置づけと機能



かつ効果的なものとしている。当局がルール・ベースからルールとプリンシプルのバランス重視へと舵を切り、検査マニュアルの一律適用を廃止し、各企業のリスクに応じたモニタリングを徹底していくというと、一見、外部委託先管理においても管理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考え方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、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いえる（図５）。

Ⅳ　やはり鍵は経営者

事業を推進する人の多くは、「リスク管理」という単語や部署が好きではないといわれる。後ろ向きで事業にとってブレーキとなるイメージがあり、定型的・形式的なニュアンスを醸し出しているのがその理由だという。現場に貢献したいという思いも込めて、「リスク管理」という言葉ではなく、あえて「デジタル・ガバナンス」という言葉を使ってみた。

FinTechも、やっとこれからRPA、ブロックチェーンやAIなどの新技術を活用したサービスが登場してくるステージにある。当然、デジタル・ガバナンスについても、これから検討事例が増えてくるものと考える。NRIにも、意識の高い企業からの問い合わせやプロジェクト依頼が少しずつ増えつつある。ある非金融の企業からは金融サービスを立ち上げた後に、危機管理体制・事業継続計画の立案などの依頼がある。さらにFinTechにとどまらずデジタル・ビジネスを多産しているような企業からは、戦略リスクと共にいわゆるリスク管理体制を整備してほしいという依頼もある。

「デジタル・ガバナンス」については、リスクベースで経営レベルの関与が重要となる点は、どのような企業にも共通となる。だが、金融機関、FinTechベンチャー、異業種から金融サービスに参入する企業と、それぞれの会社のホームグラウンドである業種や歴史、そこで培われた会社制度・文化のレベルにより、どのように対応すべきかが異なってくる。大別すれば、金融へ新規参入する企業は組織・ルール的な手当てが必要だし、既存金融機関は仕組みよりも経営を巻き込んだ企業のメンタリティ・文化的な変革が必要不可欠だと考える。金融機関の方が、歴史のあるが故に、既存の組織や今までの慣習が「呪い」となって企業を縛り付けているのではないかと思うことがある。呪いを解くのも、FinTechを推進するのも、やはり経営者しかいない。

注

https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

著者

能勢幸嗣（のせこうじ）
金融システムリスク管理部長
専門はリスクマネジメント、チェンジマネジメント