保険・年金フォーカス

サードパーティーリスクへの対応

保険会社は、外部委託に係るリスクを、どのように管理すべきか?

保険研究部 主席研究員　篠原　拓也
(03)3512-1823　tshino@nli-research.co.jp

1――はじめに

保険会社のERM [1]において、リスク管理の対象範囲は、自社やグループ会社だけにとどまらない。業務の外部委託取引などから生じる、さまざまなリスクも管理の対象となる。このリスクは、「サードパーティーリスク」と呼ばれており、よく業務の一部をアウトソーシングする金融・保険業界では重視されている。ここで、サードパーティーとは、商品・サービスを提供するために、業務上の関係や契約があり、その提供に不可欠な事業者を指す [2]。

近年、特に、デジタルトランスフォーメーション(DX)の流れのなかで、IT技術を用いるフィンテックやインシュアテックの導入が隆盛となっており、銀行や保険会社から、サードパーティーへIT業務を委託したり、サードパーティーが提供するクラウドサービスやAPI接続サービス [3]を利用したりする機会が増えている。その結果、サードパーティーリスク管理の重要性がさらに高まっている。

サードパーティーリスクは、サードパーティーに関する諸リスクをすべて含む。そのため、その管理方法を詳細に記述していくと、長大なものとなりがちである。2008年に、アメリカ連邦預金保険公社(FDIC)は、金融機関向けに、サードパーティーリスクの手引き [4](以下、「手引き」)を公表している。この手引きは10ページ程度の分量ながら、リスク管理の内容が簡潔にまとめられており、わかりやすい。保険会社向けのものではないが、今日の保険ERMにも、十分活用可能な内容と考えられる。

本稿では、その内容を参考にしつつ、サードパーティーリスクについて、みていくこととしたい。

---

[1] ERMは、Enterprise Risk Managementの略。リスク管理活動に関する、全社的な仕組みやプロセスを意味する。

[2] 日本では、IT分野で、サードパーティーという言葉がよく用いられている。他社のパソコンやOSに対応するソフトウェアや周辺機器を提供する企業を、メーカーと消費者以外の第三者という意味で、サードパーティーと呼ぶ。サードパーティーが開発・販売する製品は「サードパーティー製品」と呼ばれ、パソコンメーカーやOSの開発会社自身が提供する「純正品」とは区別されることがある。本稿では、日本のIT分野での意味にとどまらず、外部委託先等をサードパーティーと呼ぶ。

[3] APIはApplication Programming Interfaceの略。あるアプリケーションの機能や管理するデータ等を、他のアプリケーションから呼び出して利用するための接続仕様等を意味する。自己のソフトウェアの仕様を一部公開して、他のソフトウェアと機能を共有できるようにし、サービス利用者の利便性を向上させることなどを指す。一例として、電子決済代行業者とAPI接続することで、電子決済のセキュリティの向上を図るケースがあげられる。

[4] “Guidance for managing Third-Party Risk” (FDIC, FIL-44-2008, June 6, 2008)

2――サードパーティーリスクとは

まず、サードパーティーリスクとはどういうものか、簡単にみていこう。

1｜新興企業と初めて取引をする場合、サードパーティーリスクへの注意が必要

ひと口に、サードパーティーといってもさまざまなものがある。典型的なものは、業務の一部を外部委託するときの委託先だ。近年は、クラウド事業者、API 接続する電子決済代行業者、業務ライセンス利用許諾先、決済サービスを提供する先の加盟店など、その範囲が拡大している。

サードパーティーリスクの軽重は、サードパーティーによって異なる。たとえば、特定顧客向けに商品関連のサービスを提供するために、同じ委託先に、長年、継続的にサービス業務を外部委託しているような場合は、これまでの豊富な委託実績からみて、リスクは限定的といえるだろう。

一方、初めて取引する新興企業と、顧客の個人情報をやり取りするようなケースは、リスクが大きいとみられる。手引きでは、サードパーティーリスクを重視する必要がある場合が示されている。

図表 1. サードパーティーリスクを重視する必要があるケース

- サードパーティーとの関係が、新たな関係である場合、または新たな金融活動の実施を伴う場合
- サードパーティーとの関係が、金融機関の収益又は費用に重要な影響を及ぼす場合
- サードパーティーが、重要な機能を果たす場合
- サードパーティーが、顧客の機密情報を保管・アクセス・送信し、取引を行う場合
- サードパーティーが、銀行の商品やサービスを販売する場合
- サードパーティーが、サブプライムローンやカード決済取引などの商品・サービスを提供する場合

※ 「手引き」をもとに、筆者作成

2｜サードパーティーの関与により、新たに発生したり高まったりするリスクもある

金融機関がサードパーティーを活用する際には、さまざまなリスクが伴う。これらのリスクのなかには、金融機関が直面するリスクと同様に、事業活動そのものに起因するものがある。一方、サードパーティーが関与することにより、新たに発生したり、高まったりするリスクもある。これらのリスクの管理が不十分な場合、金融機関は当局の規制措置、財務上の損失、訴訟の提起、風評の悪化等に直面する恐れがある。さらに、新規顧客の開拓や、既存顧客への対応に支障が出る可能性もある。

3――サードパーティーリスクの例

それでは、サードパーティーリスクにはどのようなものがあるのか？ 手引きをもとに、みていこう。

1｜戦略リスク ： 目標達成に役立たない商品・サービスの提供にサードパーティーを活用

戦略リスクとは、事業に不利益となる意思決定を行うことや、戦略目標に整合した適切な意思決定を行わないことから生じるリスクをいう。投資収益率の向上には役に立たない商品・サービスを提供するために、サードパーティーを活用すると、銀行や保険会社が戦略リスクにさらされることとなる。

2｜風評リスク ： 顧客の苦情を招くような委託先との関係がリスクを引き起こす

風評リスクとは、世間における否定的な論調から生じるリスクをいう。たとえば、顧客の苦情を招くような委託先との関係、金融機関の経営方針に反する提携先との関係、顧客に対する不適切な商品・

サービスの推奨、顧客情報の流出につながるセキュリティ違反、各種の法令等遵守違反などは、金融機関の風評と地位の毀損を引き起こす可能性がある。また、サードパーティーについて、マイナスイメージとなる情報が流布すると、実際にそのサードパーティーの活用に関するものかどうかにかかわらず、風評リスクが生じる可能性がある。

3｜オペレーショナルリスク ： 業務プロセスの統合により業務の複雑さが増してリスクが増大することも

オペレーショナルリスクとは、 業務プロセス、人材活用、システム運用が、不適切であったり、機能しなかったり、何らかの外部の事象を引き起こして損失を招いたりするリスクをいう。サードパーティーとの関係により、金融機関と他の事業者の業務プロセスが統合されることで、業務の複雑さが増して、オペレーショナルリスクの増大につながることもある。

4｜取引リスク ： 技術面の障害などから期待どおりにサードパーティーが機能しない

取引リスクとは、商品・サービスや提供に関連して発生するリスクをいう。能力不足、技術面の障害、人為的ミス、詐欺行為のために、顧客や金融機関の期待どおりにサードパーティーが機能しないと、金融機関は取引リスクにさらされる。また、効果的な業務再開プランや、適切なコンティンジェンシープラン[5]がないと、取引リスクは増大することとなる。さらに、サードパーティーが提供する技術への管理が弱いと、セキュリティや、システム・リソース面の問題も生じる。これらの問題により、不正な取引が行われたり、予定どおりに事業処理ができなかったりすることもある。

5｜信用リスク ： サードパーティー自身の財務状況に関連する

信用リスクとは、サードパーティーやその他の債権者が、金融機関との契約上の取決めを履行できなかったり、合意していた通りに財務パフォーマンスを達成できなかったりするリスクをいう。信用リスクの基本形態は、サードパーティー自身の財務状況に関連する。一部の契約では、サードパーティーが、ローンの組成プログラムなど、一定の債務履行を保証することを規定している。このような状況では、サードパーティーの財務状況が信用リスクを評価するための要素となる。また、信用リスクは、特定ローンのマーケティングや組成、顧客の勧誘や紹介、引受分析の実施、金融機関の商品設計において、サードパーティーを利用することからも発生する。信用リスクを把握し、その水準を取締役会の承認限度にとどめるために、サードパーティーの活動を適切にモニタリングする必要がある。

6｜法令等遵守リスク ： サードパーティーによる欺瞞的商品や顧客情報保護基準違反

法令等遵守リスクとは、法令・規則等に違反することにより発生するリスクをいう。これには、委託等の契約、業務プロセス、組織の事業基準を遵守しないケースも含まれる。たとえば、サードパーティーが、法令違反の欺瞞(ぎまん)的商品のマーケティングを行ったり、差別的な貸付を行ったりする場合が該当する。また、サードパーティーが顧客の個人情報の保護や開示を適切に実施するかどうかも、法令等遵守に関する懸念事項となる。サードパーティーが、顧客情報保護基準に反してセキュリティ違反を犯した場合、その責任が金融機関に及ぶ可能性がある。法令等遵守リスクは、金融機関に対する監督や監査が不十分な場合には悪化する傾向がある。

---

[5] 予期せぬ事態に備えて、あらかじめ定めておく緊急時対応計画のこと。企業は、この計画を定めておくことで、災害や事故など、不測の事態が生じたときに、事業が中断する範囲を最小限にとどめるとともに、迅速かつ効率的に業務を復旧することが可能となる。

4――サードパーティーリスクの管理プロセス

サードパーティーリスクを適切に管理するには、どうすればよいだろうか。手引きでは、(1)リスク評価、(2)サードパーティー選定におけるデュー・デリジェンス、(3)契約の構成と確認、(4)監視 の4つの要素をあげている。それぞれ、順番にみていこう[6]。

1｜リスク評価 ： サードパーティーによる欺瞞的商品マーケティングや顧客情報保護違反

リスク評価は、そもそもサードパーティーと関係を持つかどうかを決めるための基本となる。その関係が、金融機関の戦略計画や全体的な事業戦略と整合的であることが、最初のステップとなる。次に、サードパーティーに関連する収益、費用、法的側面、リスク等を分析する。商品・サービスが、金融機関にとって新しいものである場合、より幅広い分析が求められる。経営者が、その関係により達成されるものや、サードパーティーの利用により利益が最大化される理由を、十分に理解することがカギとなる。その際、重要な項目については、サードパーティーとの関係を、他の事業者の活用や、社内組織での実行等の他の方法と比較して、分析すべきである。

リスク評価を担当する職員は、分析を適切に行うために、必要な知識とスキルを持つ必要がある。あるリスク評価の局面では、内部監査役、コンプライアンスオフィサー、テクノロジーオフィサー、弁護士を活用する場合もある。この局面では、リスクの継続的な評価と管理に必要なパフォーマンス基準、内部統制、報告ニーズ、契約要件も定めることが求められる。たとえば、その活動が顧客の商品・サービスに関するものである場合、経営者は、パフォーマンスの評価と途中での修正を可能にするよう、戦略を確立すべきである。さらに、この段階では、情報セキュリティを保持し、顧客のプライバシー要件を満たすための評価を見落としてはならない。

組織の全体的な戦略計画に関連する一般的なリスク評価を終えた後、経営者は、サードパーティーとの関係を継続して適切に監視し、管理していく能力について確認すべきである。サードパーティーに関するリスクを特定し認識することは当初から重要だが、その関係を長期的に管理していくことは、成功に不可欠となる。サードパーティーとの重要な関係について、取締役会は、デュー・デリジェンス、履行、継続的な監視、および取締役会への定期的な報告などの責任者として、上級管理職を任命することがある。この上級管理職は、サードパーティーとの関係のあらゆる側面を批判的に検討するのに必要な知識と技能を有すべきである。また、サードパーティーとの関係に効果的に対処し、新たに生じた問題や法令等遵守上の不備に適切に対応するために、金融機関のコンプライアンス管理システムが適用されることを保証すべきである。

初期リスク評価段階の最後には、サードパーティーとの関係の長期的な財務面の影響を、慎重に見積もることが含まれる。取締役会は、関係の長期的な可能性のあらゆる側面と、サードパーティー活用の決定から生じる経営上の専門知識およびその他の関連費用を考慮に入れるべきであり、短期的な費用削減の取り組みを過度に見積もりに影響させるべきではない。初期費用の会計処理が不十分であ

[6] 手引きによると、これらの4要素は、あらゆるサードパーティーに適用されるが、このプロセスの適切な使用は、サードパーティーとの関係の性質、活動の範囲と影響度、特定されたリスクに依存する。さらに、これらを含む包括的なリスク管理プロセスにより、自己資本が金融機関のベースとなるリスク・エクスポージャーを支えるのに十分であることや、サードパーティーが顧客保護を含めて各種法令等を遵守しつつ業務を遂行していることを確保できる、とのことである。

ったり、収益の過大評価があったりして、長期的な財務リスクが生じると、リスク管理プロセスの他の段階において、適切な意思決定が損なわれる可能性がある。

2｜サードパーティー選定におけるデュー・デリジェンス ： 事業者選定時の評価

経営者は、活動や計画を実施しうる事業者を選定しなければならない。サードパーティーとの関係が金融機関の戦略目標と財務目標の達成や、リスクの軽減に役立つかどうかを判断するために、デュー・デリジェンスを行う。デュー・デリジェンスは、サードパーティーの選定時だけでなく、契約の更新の際にも、定期的に実施する必要がある。

デュー・デリジェンスを行う範囲と深度は、サードパーティーとの関係の重要性や規模に関係する。たとえば、大規模で世間の注目を引く事業や、機密データを取り扱う計画では、詳細なデュー・デリジェンスが求められる。一方、サードパーティーの活動が低リスクだったり、リスクが限定的であったりする場合、包括的なデュー・デリジェンスは不要といえる。

包括的なデュー・デリジェンスには、企業の財務状況、業務関連の実績、適用法令に関する認識、企業の風評、業務管理の範囲と有効性に焦点を当てながら、すべての情報を確認することが含まれる。評価には、つぎの項目を含めることが考えられる。

図表 2. サードパーティーの評価項目の例

- 監査された財務諸表、年次報告書、証券取引委員会(SEC)への提出書類、その他の利用可能な財務指標
- サードパーティーの財務状況に対する提案された契約の重要性
- 提案された活動の実施とモニタリングにおける経験と能力
- 事業の風評
- 会社トップの資格と経験
- サービス理念、品質イニシアチブ、効率化、雇用政策などの戦略と目標
- 会社に対する重大な苦情や訴訟、または規制措置の存在
- 現在のシステムを使用して提案された機能を実行する能力、または追加投資の必要性
- サードパーティーによる他者や下請業者の使用
- 内部統制、システムおよびデータセキュリティ、プライバシー保護、および監査の範囲
- 事業再開戦略とコンティンジェンシープラン
- 関連する顧客保護及び市民権に関する法律及び規則に関する知識
- 経営情報システムの適切性
- 保険の補償範囲

※ 「手引き」をもとに、筆者作成

3｜契約の構成と確認 ： 必要事項の契約書への記載

サードパーティーを選定した後、金融機関とサードパーティー双方の、期待と義務が契約書に具体的に記載されていることの確認が必要となる。契約締結前には、取締役会の承認や、弁護士による確認を行うべきである。なお、デュー・デリジェンス基準に合致しない場合、サードパーティーから他者への義務の譲渡、移転、下請契約を禁止する必要がある。

契約条項の詳細は、サードパーティーとの関係の範囲とリスクによって異なる。以下の諸点が、契約の構成項目となる。これらは、サードパーティーとの関係性と重要性に依存する。

(1) 範囲

契約書には、次の事項を含め、契約の各当事者の権利及び責任を明確に記載すべきである。

図表 3. 契約書に記載すべき事項

- 契約が適用される期間
- 提供する商品・サービスの頻度、形式、仕様
- ソフトウェアのサポートとメンテナンス、従業員のトレーニング、カスタマサービスなど、サードパーティーが提供するその他のサービス
- サードパーティーが、適用されるすべての法律、規制、および規制ガイダンスを遵守することの要件
- 法令や規制の遵守を評価するために必要又は適切な場合に、金融機関や適切な連邦・州の規制機関がサードパーティーの記録にアクセスすることを認めること
- 必要な顧客情報の開示について責任を負う当事者の特定
- サードパーティーによって維持される保険適用範囲
- 銀行の施設、設備または従業員の使用に関する条件
- 契約に関する義務を履行するためにサードパーティーが下請契約を締結し、又はサードパーティーを使用することの許可/禁止、及び通知/承認要件
- 金融機関がサードパーティーを監視し、その契約の遵守について定期的に確認を行うための権限
- 補償

※ 「手引き」をもとに、筆者作成

(2) 費用と報酬

契約書は、金融機関とサードパーティーの双方について、固定報酬、変動手数料、経常外項目や特別な要求に対して支払われるべきものなど、いかなる手数料の概要も示しておく必要がある。事業活動に関連する装置、ハードウェア、ソフトウェアその他を購入、維持するための費用や責任がある場合には、その他の項目として対処すべきである。また、法定費用や監査費用を支払う責任についても、明らかにしておくことが必要となる。

金融機関は、健全な銀行の慣行や顧客保護法制に合致した報酬制度を採用すべきである。報酬体系は、安全かつ健全な方法で良好な長期的業績を促進するよう構成される必要がある。一方、定量的で短期的なインセンティブ報酬については、厳格な品質管理の対象とすべきである[7]。

(3) パフォーマンス基準

サードパーティーのパフォーマンスを測定するための基礎として、パフォーマンス基準を明確に定義して、契約書に含める必要がある。これを、報酬取り決めの要素として、使用することもありうる。なお、特定の機能のために参考として業界標準を用いたり、サードパーティーと金融機関の間の特定の関係を反映するように基準を設定したりすることもできる。経営者は、全体目標との整合性を確保するために、パフォーマンスを定期的に確認すべきである。

(4) 報告

契約書には、サードパーティーから受け取る報告書の種類と、報告頻度を明記すべきである。通常の報告には、パフォーマンス報告、監査、財務報告、セキュリティ報告、ビジネス再開テスト報告などがある。また、経営者は、取引関係の性質に影響を及ぼしたり、金融機関にリスクをもたらす可能性があったりする変更や問題の通知のための、不定期の報告を義務付けることを検討すべきである。

[7] このことは、特に、融資を組成する事業分野に当てはまる。FDIC は、サードパーティーが、借り手を不適切に高額な費用の商品に誘導することを助長するような報酬制度を、明確に禁止している。

(5) 監査

契約書には、金融機関がサードパーティーから受け取る監査報告書の種類と頻度に加えて、契約の下でのパフォーマンスを監視するために、必要に応じて、金融機関がサードパーティーを監査する権利(または会計監査人を置くこと)を明記すべきである。経営者は、金融機関に提供される商品・サービスに関して、サードパーティーの内部統制が十分に監査されていることを保証すべきである。契約上重要な場合には、サードパーティーが維持すべき具体的な内部統制を契約書に定める必要がある。

(6) 機密性とセキュリティ

契約で指定された機能を行う場合を除いて、サードパーティーやその代理人が、金融機関の情報を使用したり、開示したりすることは禁止しなくてはならない。金融機関の顧客に関する非公開の個人情報は、金融機関自身の個人情報保護方針と、適用される個人情報保護関連法令に従って、取り扱われなくてはならない。情報のセキュリティや機密性の侵害(不正侵入よる潜在的な侵害を含む)が生じた場合、金融機関は、完全かつ迅速に、そのことを開示することが求められる。

(7) 顧客の苦情

契約書には、金融機関やサードパーティーが、顧客から受けた苦情に対する責任を負うか否かを明記しなくてはならない。サードパーティーが責任を負う場合は、苦情や対応を金融機関に連携しなくてはならない。契約書には、苦情の状況と解決策を詳述した定期的な要約報告書についても記載すべきである。

(8) 事業の再開とコンティンジェンシープラン

人為災害と自然災害の両方を含む、業務上の障害が発生した場合、契約上の取り決めに規定されたサービスを継続するためのサードパーティーの責任に対処すべきである。サードパーティーは、情報をバックアップするための適切な保護を準備しておく必要がある。また、詳細な運用手順を備えた災害復旧プランとコンティンジェンシープランを保持しておく必要もある。これらのプランのテスト結果は、金融機関に提供されなくてはならない。

(9) 債務不履行と契約終了

債務不履行や契約終了に伴うリスクを軽減するために、契約は両方の問題に対処すべきである。契約書には、どのような状況が債務不履行を構成するかを明記し、改善策を特定し、それを是正するための妥当な機会を考慮すべきである。

特に重要なサードパーティーとの取り決めや、急速に変化する技術や状況に関連する関係については、契約の中に、契約終了権を明記しておく必要がある。契約終了権には、管理の変更、費用の大幅な増加、履行基準の不履行、契約上の義務の不履行、法令違反防止の不能、破産、会社の閉鎖、支払不能など、さまざまな条件を盛り込んでおくことが求められる。契約書には、過度の費用をかけずに他の事業体への秩序ある移行を可能にするための要件と期間とともに、契約終了と通知要件を記載しておく必要がある。また、金融機関のデータ、記録、その他リソースの返却についても記載しておくべきである。

(10) 紛争解決

金融機関は、問題を迅速に解決するために、紛争解決手続を契約に含めることを検討すべきである。また、紛争中の当事者間の取り決めの継続についても、記載すべきである。

(11) 所有権と使用許可

契約には、所有権の問題や、データ、機器、ソフトウェア、知的財産(金融機関の名称、ロゴ、商標、その他の著作権等)といった金融機関の財産を使用するサードパーティーの権利について、規定をおく必要がある。また、サードパーティーによって作成されたすべての記録の所有権と管理についても記載すべきである。

(12) 損害賠償

損害賠償規定は、サードパーティーの過失により、金融機関に損害を与えないことを求めるもので、その逆も同様である。これらの規定を契約に組み込むことにより、サードパーティーの過失から生じた賠償請求について金融機関が責任を負う可能性を低減することができる。しかしながら、そのような規定があるからといって、安全かつ健全に、法令や健全な銀行原則を遵守して銀行業を行っている金融機関の最終責任をサードパーティーに転嫁できるわけではないことを、繰り返して認識しておく必要がある。また、損害賠償規定があるからといって、是正が必要な欠陥が軽減されるわけでもない[8]。

(13) 責任の制限

サードパーティーは、金融機関との関係の結果、生じる可能性のある負債の額を、契約により制限するよう望むことがある。このような契約を締結する際には、金融機関の経営者は、提案された損害限度額が、サードパーティーが適切に履行しなかった場合に金融機関が被る可能性のある損失額と比較して妥当であるかどうかを慎重に検討すべきである。

4｜監視 ： サードパーティーの活動の監視

金融機関は、サードパーティーの活動に対する適切な監視と、サードパーティーとの取り決めを通じて提供される商品・サービスに対する適切な品質管理を維持し、重大な財務上の損失、風評被害、監督措置の発生を最小限に抑える必要がある。取締役会は、少なくとも年に1回、重要なサードパーティーとの取り決めを承認、監視、確認する。また、計画に重要な変更があったときは、これらの取り決めと、書面による合意を確認する。経営者は、定期的にサードパーティーの業務を確認し、リスクが契約書の条件と整合的に管理されていることを確かめる。金融機関のコンプライアンス管理システムは、連邦法、州法、規則、規制、内部の方針や手続きの継続的な遵守を保証する必要がある。

経営者は、重要なサードパーティーとの関係を監視し、必要な監督を行うために、十分な資格を持つ職員を配置すべきである。特に、重要な関係については役員を指名すべきであり、法令等遵守はも

[8] 手引きでは、顧客保護その他の法令、規則、健全な銀行の原則に対する違反がある場合や、銀行業及びそれに関連する活動が安全かつ健全に行われていない場合には、損害賠償命令を含む救済措置についてのFDICの検討は、サードパーティーとの契約における補償条項の有無にかかわらず行われる、としている。

とより、必要に応じて、監査や IT 技術のような他の業務分野を監視プロセス含めるべきである。サードパーティーの監視の程度は、潜在的なリスクと、契約の範囲及び規模に依存する。

監視内容には、通常、サードパーティーのサービス品質、リスク管理慣行、財務状況、適用可能な管理および報告の監視が含まれる。重要なサードパーティーとの取決めに対する監視活動の結果は、金融機関の取締役会や指定された委員会に定期的に報告される必要がある。また、特定された弱点は、文書化して、迅速に対処すべきである。

パフォーマンスの監視には、必要に応じて、以下を含めるべきである。

図表 4. サードパーティーに対するパフォーマンス監視項目

- サードパーティーとの関係の全般的な有効性と、金融機関の戦略目標との関係の一貫性を評価する。
- サードパーティーが合法的にサービスを実行可能であることを確認するために、免許や登録状況を確認する。
- 少なくとも年 1 回、サードパーティーの財務状況を評価。財務確認は、貸付時の信用リスク分析と同様に包括的に行う。重要なサードパーティーとの関係については、監査済みの財務諸表が必要。
- サードパーティーの保険の補償範囲の妥当性を検討する。
- サードパーティーの他者に対する金銭的義務が履行されていることを確保する。
- サードパーティーの監査報告書またはその他の報告書を確認し、必要な是正措置を求める。
- 内部統制およびセキュリティ問題に関するサードパーティーの経営政策の妥当性と遵守状況を確認する。
- 適用される法律、規則、規制への遵守状況を監視する。
- サードパーティーのビジネス再開のための緊急時対応計画とテストを確認する。
- 金融機関との関係に関与する主要なサードパーティーの人員の変更の影響を評価する。
- 契約要件と基準に照らして、サードパーティーのパフォーマンスを確認。必要に応じて適切なフォローアップを行う。
- 金融機関とサードパーティーの従業員を対象とする研修の適切性を判断する。
- 顧客と直接のやり取りがあるサードパーティーとのテストプログラムは、すべて管理する。
- サードパーティーが提供する商品・サービスに関する顧客の苦情と、苦情の解決策を検討する。
- パフォーマンスや業務上の問題について、必要に応じてサードパーティーの代表者と話し合う。

※ 「手引き」をもとに、筆者作成

適切な文書化を行うと、サードパーティーリスクの監視と管理が容易になる。したがって、金融機関は、有効な契約、事業計画、リスク分析、デュー・デリジェンス、監視活動(取締役会または委任された委員会への報告を含む)などの、サードパーティーとの関係のあらゆる面で、文書と記録を保持しておく必要がある。また、いかなる紛争解決に関する文書も保管しておくべきである。[9]

5――おわりに（私見）

金融機関や保険会社では、以前からサードパーティーリスクが存在している。特に、DX が進むなかで、デジタル技術を有する新興の IT 会社等との関係が必要となってくると、サードパーティーリスクの影響も多様化する可能性がある。

本稿で取り上げた FDIC の手引きは、10 年以上前に公表されたものではあるが、いまでも活用できる部分が多いものと考えられる。こうした手引きなどを参考に、実際に、サードパーティーリスクへの対応がどのように進められていくか、引き続き、注視していくこととしたい。

[9] 手引きでは、この後に「FDIC によるサードパーティーとの関係の監督」という節を設けて、監督方針等をまとめているが、本稿では割愛する。