protiviti®
Global Business Consulting

第三者（サードパーティ）の重要なリスクの特定と管理

「アウトソーシングやその他の第三者との関係は、金融機関に、オペレーションの耐性の強化、金融商品やサービスをより迅速かつカスタマイズすること、コスト削減、イノベーションの拡大、内部プロセスの改善など、さまざまなメリットをもたらします。しかし、アウトソーシングや第三者との関係は、金融機関や潜在的に金融の安定性に、新たなまたは異なるリスクを生じさせることがあり、適切に管理することが必要である。」[1]

1990年代以前は、金融機関において第三者リスク管理（TPRM）といえば、外部委託しているテクノロジー提供者が経済的に存続できるか、評判が良いか、信頼できるか、プライバシーや情報セキュリティの保護措置は適切かといった監視を意味していました。サイバーセキュリティという言葉が英語の辞書に載るようになったのは1989年のことですから、サイバーセキュリティの管理はこうした初期の議論には含まれていませんでした。アウトソーシングテクノロジープロバイダーとの契約は、金融機関全体に広く分散していることが多く、金融機関の第三者テクノロジープロバイダーの完全なリストを作成しようとしても、無駄に終わることが多いのです。

この30年で多くのことが変わりました。今日、金融機関に対する第三者提供者は、テクノロジーやその他のサービス提供者を幅広く含み（普遍的な定義の欠如は、コンプライアンスの取り組みを複雑にしていますが）、これらの提供者のリスクを特定し管理するためには、協力的かつ継続的な取り組みが必要であると一般に理解されています。また、長年認識されてきたリスクは依然として重要ですが、集中リスクなど、他の多くのリスクにも注意を払う必要があります。リスクの状況、そして大規模な金融機関では5万社近い取引先[2]があることを考えると、TPRMが業界や規制当局の世界的な優先事項であることは少しも驚くに値しません。

サードパーティ・サービス・プロバイダーの「新しい」リスク

金融サービス企業では、2021年第4四半期に1週間あたり703件のサイバー攻撃が報告されていること、前年比53％増となっていること[3]、顧客の信頼回復を含むサイバー攻撃の対応関連するコストが発生していることから、金融機関は第三者との関係における情報セキュリティおよびプライバシーリスクの管理の重要性を改めて認識する必要はないでしょう。また、プロバイダーの財務的な余裕や評判を考慮する必要もないでしょう。しかし、今日の環境では、テクノロジーの継続的な進歩と依存、データプライバシーとデータ取り扱い要件の複雑なグローバルな枠組み、パンデミック時に学んだ教訓、さらには世界政治の状況などにより、いくつかの既存のリスクが高まり、次のような新たなリスクが発生しています。

サードパーティプロバイダーに共通するリスク

- プライバシーと情報セキュリティ
- データのローカライズ（現地化）
- オペレーショナル・レジリエンス
- デリバリー
- 代替性
- コンプライアンス
- 法務/契約書
- ESG
- 地政学的リスク
- 戦略的
- ソルベンシー
- 集中
- レピュテーション 顧客への影響
- N番目の事業者のリスクマネジメント
- グループ内リスク

1 Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Discussion Paper, Financial Stability Board, November 9, 2020, https://www.fsb.org/wp-content/uploads/P091120.pdf.

2 Managing When Vendor and Supplier Risk Becomes Your Own," by Hamid Samandari, John Walsh and Emily Yueh, McKinsey & Company, July 1, 2013, https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/managing-when-vendor-and-supplier-risk-becomes-your-own.

3 "Spike in Destructive Attacks, Ransomware Boosts Banks' Cybersecurity Spending in 2022," by Sherry Fairchok, Insider Intelligence, May 3, 2002, https://www.insiderintelligence.com/content/spike-destructive-attacks-ransomware-boosts-banks-cybersecurity-spending-2022.

- **データのローカライズ（現地化）** — 国境を越えた非公開データのフローを制限または禁止する、いくつかの法域における厳格なデータのローカライズの規則。

- **オペレーショナル・レジリエンス** — サードパーティプロバイダーが悪条件下で事業を行うことができなくなること。このリスクは、パンデミックによって表面化し、一部のプロバイダーがリモートワークに容易に移行できないことが明らかになった。

- **デリバリー** — 新規市場参入者（例：フィンテック）が受託サービスを提供する際の持続可能性が証明されていないこと。

- **代替性** — 代わりのサービス提供者をコスト効率よく、かつタイムリーに探し出すことの困難さ。特に後発市場だけでなく、提供者の数が限られているハイテク市場においても同様である。

- **ESG** — 第三者の環境・社会・ガバナンス（ESG）に対するコミットメントと実践を、サービス利用者のものと一致させること。

- **地政学的なもの** — 地政学的な緊張のために、第三者であるプロバイダーのサービス提供が中断または排除される可能性がある。

- **集中** — 利用可能なプロバイダーの数が限られている（例：クラウドサービスに関連するもの）。

- **N番目の事業者のリスク** — 第三者機関の下流業者が、サプライチェーンリスクを含む不当なリスクにさらされる可能性、および／または、オペレーションの回復力を危うくする可能性があること。

グループ内リスクとは、関連する企業がサービスを提供する際に発生するエクスポージャーのことです。金融機関は、グループ内プロバイダーが関連企業であることを理由に、そのリスクを小さく見積もることがあまりにも多いです。グループ内リスクの評価方法については、ある程度の柔軟性を持たせるべきでしょう（例：グループ内プロバイダーのソルベンシーは、一般的に独立した第三者と同程度の精査を必要としないであろう）。しかし、グループ内プロバイダーにとって、他のリスク（デリバリーやコンプライアンスなど）は、特にクロスボーダーでサービスを提供する場合に限られたものではなく、経験上重要であり、そのため、これらのリスクを慎重に評価する必要があります。

これらのリスクの中には、金融機関がますますテクノロジーに精通し、デジタル主導のサービスを提供するために、第三者のテクノロジー、データ、クラウドサービスを利用することを反映したものもあります。このような第三者との取り決めによるリスクも同様に構成されていますが、非常に限られた数の業者に集中していること、業者の代替が困難なこと、効果的な契約交渉ができないこと、アクセス権や監査権が限られていることなどから、これらのリスクの一部は非常に大きく、最近の世界各国での発表に見られるように、多くの規制当局から注目しています。後述するように、多くの国の規制当局は、重要な IT サードパーティ・サービス・プロバイダーに対する関心を高めています。金融安定化機構（FSI）は、2022年8月発行のFSI Briefs「Safeguarding Operational Resilience : The Macrorudential Perspective」において、この監督や監視を実現するためのさまざまなアプローチについて考察しています。

TPRMへの規制対応

世界各国の規制当局は、TPRMに対する期待値をあげ続けています。金融安定理事会（FSB）が2020年11月に公表した「アウトソーシングと第三者関係に関連する規制・監督上の問題」とこれに関して提出されたコメントは、複数の規制制度にまたがるさまざまなサードパーティを管理するという業界の課題について、良い全体像を提供しています。各規制当局は多くの共通した期待を持っていますが、その期待の提示と執行の方法には大きな違いがあります。これは古典的な80/20ルールです。80% の期待値はグローバルな規制機関間で一貫していますが、20% は厳格化要件で、そのうちのいくつかはグローバルプログラムにとって対処が容易なものです。以下では、いくつかの主要な金融市場における現状の概観を説明します。

米国

2021年7月、通貨監督庁（OCC）、連邦預金保険公社（FDIC）、連邦準備制度は、第三者リスク管理に関する省庁間ガイダンス案（Proposed Interagency Guidance on Third-Party Relationships: Risk Management）をコメント用に発表しました。TPRMに関する各機関の足並みを揃えることを目的として、提案されている枠組みは、以前に発表されたOCCガイダンスに基づいており、TPRMに対するリスクベースのアプローチの開発に引き続き重点を置いています。2021年9月21日に意見募集期間が終了しましたが、最終ルールはまだ発行されていません。

提案されたガイダンスは、金融機関（具体的には、この例では銀行）が第三者の監督に責任を持ち、金融機関が依然として法律や規制を遵守していることを確認することを引き続き強調しています。また、金融機関が第三者の評価を正確

に行っていないと規制当局が判断した場合に発生する第三者に対する監督上のレビューにも対応しています。クラウドアウトソーシングの取り決めは、このガイダンスでは特に扱われていません。しかし、これまでも、そしてこれからも、米国の審査プロセスの焦点となり、連邦金融機関審査委員会（FFIEC）のIT審査ハンドブック（Federal Financial Institutions Examination Council（FFIEC）IT Examination Handbooks）で扱われています。

カナダ

2022年4月、金融機関監督庁（OSFI）は、TPRMの期待に関連するものとして、ガイドラインB-10の改訂に関するコンサルテーションペーパー（consultation on revisions to its Guideline B-10）を発表しました。2022年9月に締め切られるこのコンサルテーションペーパーでは、拡大した第三者エコシステムの中でより包括的な第三者リスクを反映するためにガイドラインB-10を強化し、ガバナンスとリスク管理プログラムを重視し、連邦規制金融機関（FRFI）に成果を重視した原則ベースの期待を設定することを提案しています。

改訂版ガイドラインB-10は、より広範な第三者の取り決めに適用されます。従来のアウトソーシング契約によってもたらされるリスクだけでなく、重要な下請け業者を含む商業ベースまたは戦略ベースで従事する外部事業者によってもたらされるリスクも管理することを提案しています。提案されているリスクベースアプローチは、評価すべきリスクを広げると同時に、金融機関に対し、アレンジメントのリスクレベルに見合ったTRPMのライフサイクルアプローチを採用することを求めるものです。

イギリス

英国の規制当局は、重要なアウトソーシングの取り決めについて、その締結前の通知など、長年の要求事項を設けています。Prudential Regulation Authority（PRA）は最近、TPRMとアウトソーシングに対する規制を強化しています。金融セクターの業務回復力を向上させ、第三者への「依存」に起因する脆弱性を軽減する手段として、PRAは監督指針2/21（Supervisory Statement 2/21）を2021年3月に発表しました。

この指針では、アウトソーシングの取り決め、アウトソーシング以外の第三者との取り決め（例：重要または高リスクのハードウェア、ソフトウェア、その他の情報通信テクノロジー（ICT）製品）、規制要件の対象となる第三者との取り決めに関するさらなる定義と要件の概要が示されています。外部委託していない第三者が「重要」または「高リスク」とみなされる場合、金融機関は、同等のリスクまたは重要性のある外部委託の取り決めに適用されるものと同等の強固なリスクベースのコントロールを実施することが期待されます。PRAは、規制要件の対象となる第三者の取り決め（例：清算、決済、保管サービス）はアウトソーシングの定義を満たさないが、適切なモニタリングとリスクベースでコントロールすべきであると金融機関に注意を促しています。

2022年7月、PRAとFCAは共同でディスカッション・ペーパー（Discussion Paper）を発表しました。 英国における重要な第三者機関（CTP）（クラウドサービスプロバイダーなど）を直接監督する意向を示しています。直接監督は、CTPがもたらすシステミックリスクを監督当局が管理する上で、現行の規制枠組みの限界を克服することを目的としており、最低限のレジリエンス基準の設定、レジリエンスのテスト、世界の他の規制機関との協調を含むことになります。

欧州連合（EU）

欧州銀行協会（EBA）のアウトソーシングの取り決めに関するガイドライン（Guidelines on outsourcing arrangements）は、2019年9月に施行され、しばらくの間、欧州の金融機関に対する規制要件の重要な発信源となっています。これらのガイドラインは、2020年6月にEBAの「ICTとセキュリティリスク管理に関するガイドライン」（Guidelines on ICT and security risk management）によって強化されました。このガイドラインは、第三者を巻き込む可能性のあるICTリスクに関するさらなる要件とガイドラインを定めています。

金融サービスにおけるクラウド導入が一般的になるにつれ、クラウドサービスプロバイダーへのアウトソーシングのリスクが高まっていることを認識した上で、欧州証券市場庁（European Securities and Markets Authority, ESMA）や欧州保険・職業年金機構（European Insurance and Occupational Pensions Authority, EIOPA）含む他の欧州監督当局も、クラウドサービスプロバイダーへのアウトソーシングを推奨しています。そして、クラウドサービスプロバイダーへのアウトソーシングに関するガイドライン（guidelines on outsourcing to cloud service providers）を発表しました。

2020年9月、欧州委員会（EC）はある提案書（proposal）を発表しました。それは、デジタル・ファイナンス・パッケージ（digital finance package,DFP）の一環として、デジタル・オペレーショナル・レジリエンス法（DORA）と呼ばれる金融セクターのデジタル・オペレーショナル・レジリエンスに関する規制のためのものです。DORAは、EUの金融セクターにおけるデジタルオペレーションレジリエンスとICTリスクマネジメントの規制と監督の調和を図ることを目的としています。規制が確定すれば、この監視の枠組みは、クラ

ウドサービスプロバイダーを含む第三者の業務回復力とリスク管理に大きな影響を与えることが予想されます。

オーストラリア

オーストラリア健全性規制庁（APRA）の長年にわたるプルデンシャル・スタンダードCPS231(Prudential Standard CPS 231) は、重要な第三者および関連企業とのアウトソーシングの取り決めを対象としています。この基準は、APRAの規制下にある企業に対し、適切なデューデリジェンス、承認、継続的な監視を行うことを要求しています。

2020年7月、APRAのプルデンシャル・スタンダードCPS234(Prudential Standard CPS 234)に が発効されました。CPS234は、APRAの規制対象事業者が第三者との取り決めを通じてさらされる可能性のある情報セキュリティリスクを管理するための要件に焦点を当てています。この要件には、第三者に対する保証・監査に関する契約上の権利、第三者の適切な監視・管理、経営幹部による報告・監視が含まれます。

さらなる展開として、2022年7月、APRAはディスカッション・ペーパー230(Discussion Paper 230)を公表しました。 オペレーショナルリスク管理を強化するために、重要な業務やAPRAの規制下にある企業が重大なオペレーショナルリスクにさらされるような重要なサービス提供者すべてに要件を拡大し、TPRMを強化する新基準を提案しています。提案された新基準は、プルデンシャル基準CPS231とプルデンシャル基準CPS232(Prudential Standard CPS 232)を統合し、置き換えるものであり、事業継続マネジメントに関わるものです。提案された基準は、調達プロセスから生じるリスクと、運用面で弾力的な金融機関を維持するための期待について、現代的な見解を示すものです。最終的な要件は2024年に発効する予定です。

香港

2022年7月、香港金融管理局（HKMA）は、第三者による監視とリスクマネジメントのために「レグテック導入実践ガイド」(Regtech Adoption Practice Guide)を発行しました。このガイドの目的は、第三者監視とリスク管理に使用されるレグテックソリューションの概要を提供し、導入時に観察される共通の課題を概説し、業界の事例を紹介することです。戦略やオペレーションモデル、人材調達、ガバナンス、組織、テクノロジー、データなど、サードパーティから生じるリスクに対処するためのベストプラクティスや先進的な銀行が行っている方法を紹介しています。

レグテック・プロバイダーに焦点が当てられていますが、原則と事例は、他の第三者関係における規制上の期待に貴重な洞察を与えてくれます。HKMAは、銀行に対し、重要な業務プロセスおよびサービスを明確に把握し、これらの分野で第三者が果たす役割を特定することを求めています。さまざまな規制やガバナンスの優先順位の中で、リスク評価のアプローチは一貫して適用されるべきであり、規制要件を遵守する必要があります。

シンガポール

2021年1月、シンガポール金融管理局（MAS）は、「テクノロジーリスク管理ガイドライン」(Technology Risk Management Guidelines)を改訂しました。 これは、金融機関が健全なテクノロジーリスクガバナンスと監視を確立し、サイバー耐性を維持することを支援しようとするものです。改正後のガイドラインでは、金融機関が第三者を利用することは必ずしもアウトソーシングとは言えないが、第三者との関係については、契約前の適切なデューデリジェンスと、継続的なモニタリングが必要であることを指摘しています。アウトソーシングに関するMASガイドライン（MAS Guidelines on Outsourcing）は、2016年に発行され、2018年に改訂されましたが、引き続き有効であり、クラウドコンピューティングを対象としています。

最近の規制当局の発表では、金融サービス部門以外の第三者（すなわち規制対象外）および契約書以外のアウトソーシングの取り決めに関連するリスクが強調されています。世界の規制当局は、外部に委託しない第三者の取り決めが、重大なオペレーショナルリスクやオペレーションの回復力に重大な影響を与える可能性があり、より強力な管理と監視を必要とすることを認識しています。クラウドサービスのアウトソーシングを進める業界動向は、さらなる規制強化の推進要因となっています。このような分野では、世界的にさらなる規制の強化が予想され、要件がきびしく、そして期待が高まっています。

TPRMのためのフレームワーク

アプローチの違いはあるにせよ、世界の規制当局は、第三者の利用は、金融機関に、第三者のパフォーマンスに対する責任があることを認めています。つまり、金融機関は第三者との関係を積極的に管理する必要があるのです。第三者との取り決めに関する健全なリスク管理の枠組み（以下に示す）は、金融機関が以下のことを行っており、また行っていることを証明することを目的とした多くの活動の詳細を示し、権限を付与するものです。

- 第三者の選定と機関のビジネスニーズとの整合性を慎重に検討すること（**計画**）。この検討には、戦略や計画の

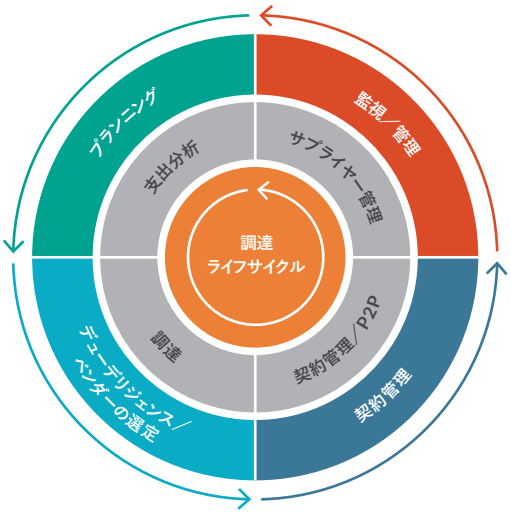
プロセスに第三者の評価を組み込むことや、製品やサービスの革新が第三者との協働を促し、顧客価値を創造し、リスクを管理することを確実にすることなどが含まれます。新たな第三者との関係が想定される場合、第三者の戦略的意味合いと明確な要件を考慮した上で、正式なビジネスケースを作成する必要があります。契約前に、新製品・新サービスの承認やIT変更管理プロセスの一環としての検討を含む、適切なリスク評価とデューデリジェンス（以下に詳述）を実施する必要があります。重要な第三者との関係については、上級管理職による監督と承認が必要となります。

- リスク評価と第三者に対する金融機関にもたらすリスクに見合った徹底的なデューデリジェンスを実施（**デューデリジェンスとベンダーの選定**）。リスク評価には、（第三者が提供するサービスに基づく）固有のリスク評価、第三者との取り決めに関するリスク評価、全体的な残存リスクとリスク軽減計画が含まれます。各サードパーティについては、特定された主要なリスクに焦点を当て、第4者の使用、データの流れ、および計画された活動を超えてデータを共有できる可能性のある共同所有権とネットワークの検討を含む詳細な評価が必要となります。ビジネスのステークホルダーは、業務に対する重要性と、第三者がレジリエンス・プランニングにどのような影響を与えるかも考慮する必要があります。適切なリスクベースのデューデリジェンスプログラムは、第三者のリスクを管理するための効果的なプログラムの基礎となるものです。

- 第三者と契約し、役割、責任、期待を明確に定めたサービスレベル合意書（SLA）を制定すること（**契約管理**）。アウトソーシングを成功させ、規制当局の期待に応えるためには、契約要件を定め、第三者との契約交渉を成功させることが重要です。主な検討事項には、問題および違反通知の要件、データセキュリティ、回復力計画および監視、下請け業者および第4者の要件、アクセス権および監査権、適用される法律、規制およびその他のビジネス要件への準拠が含まれる必要があります。撤退計画、代替可能性、混乱の扱い、事業継続の条項も重要です。さらに、金融機関は、第三者への業務の円滑な移行、金融機関の方針と手続き、モニタリングと報告のプロトコルと要件がすべて確立され、定着することを確認する必要があります。

- 第三者のパフォーマンスを継続的に監視し、必要に応じて、第三者の終了および代替のための措置を講じること（**監視および管理**）。第三者との関係については、金融機関の TPRM およびガバナンスの枠組みに従って、（契約条件、合意されたパフォーマンス閾値およびリスク評価に従って）定期的かつ継続的に監視、評価 および レビューを実施する必要があります。審査および情報管理の要件の性質と頻度は、リスクベースのアプローチを用いて決定されます。金融機関はまた、課題管理、契約の再交渉や関係における重要な変更、第三者との関係を終了させるためのリスクとプロセスの管理に関する方針とプロセスを持つことになります。

プロティビティTPRMフレームワーク



TPRMプログラムのガバナンスは、その有効性を高めるために非常に重要です。今日、規模の大小を問わず、ほとんどの金融機関は、第三者リスクを一貫して管理し、TPRMプログラム全体のリスクを確実に監視するTPRM機能またはセンターオブエクセレンスを有しています。大規模な金融機関では、多くの場合、日常業務をサポートする第一線のチームと、サービスを共有する第二線の専門チームが存在します。小規模な金融機関では、第一線と第二線を兼務することが多いようです。TPRM部門は、他のリスク関係者（コンプライアンス、サイバーセキュリティなど）と密接に連携し、第三者が金融機関や規制当局の期待に応えていることを確認します。より成熟したリスクフレームワークは、アプローチの一貫性を確保し、基準を確立し、潜在的な重複やギャップを最小化するために、全体のリスク機能の中でTPRMプログラムを調整します。

経営者が問うべき質問

上記のような健全なTPRMリスク管理の枠組みを有する金融機関の経営者および取締役会は、TPRMプログラムに関する定期的な報告を受けます。しかし、十分な情報が得られていないと感じている経営陣や、金融機関の枠組みに異議を唱えたい経営陣は、次のような質問をするとよいでしょう。

1. TPRM に関する規制要件や期待事項を理解しているか、また、グローバル金融機関については、自国とホスト国の要件の違いをどのように調整してきたか。

2. 第三者のさまざまなリスクを理解し、そのリスクを評価・軽減できる、十分かつ適切な訓練を受けたスタッフや上級管理職がいるか。

3. 第三者との関係を管理するための、統一された、全社的な、リスクに基づいたプログラムがあるか。

4. すべての第三者との関係、関連する場合は分類化して、特定していることに自信があるか。

5. 第三者デューデリジェンスプログラム（導入時および継続的）が、リスクベースで適切に実施されているか。

6. 業績不振のベンダーやリスクをもたらすベンダーを特定するための効果的なエスカレーションプロセスがあるか。

7. 第三者との関係の取り決めの管理に、オペレーショナル・レジリエンスを織り込んでいるか。

TPRM サービスについて

プロティビティは、ビジネスパフォーマンスインプルーブメント、リスク・コンプライアンス、セキュリティ・プライバシーなどの専門家からなるサードパーティ管理センターオブエクセレンスを通じ、あらゆる規模の金融機関に対し、ベンダーやサードパーティを管理する効果的なプログラム作成を支援してきました。TPM は、戦略とプログラムの評価、設計と導入・変革、BCM、IT セキュリティ、プライバシー、PCI、コンプライアンスなど個々のリスク領域の改善、第三者監査（IT セキュリティ/共有評価、運用、コンプライアンス）、テクノロジー導入、ターゲット課題の修正とインシデント対応に及んでいます。

プロティビティは、すべてのエンゲージメントにおいて、適切な業務、規制、コンプライアンス、リスク管理、IT の専門知識を提供するための統合的なソリューションを提供しています。私たちは、お客様のサードパーティおよびコンプライアンスニーズに対応するチームとソリューションを構成するための、奥行きと俊敏性を提供します。

protiviti®