

デジタル技術の活用とサードパーティリスク管理 —日米欧における制度対応の進展状況—

富永 健司

■ 要 約 ■

1. 昨今、金融市場でデジタル技術の活用が進む中、サードパーティに関連するリスク（TPR）管理への関心が高まっている。この背景には、金融サービスにおける AI（人工知能）の活用拡大に伴うサードパーティへの依存度の増加がある。
2. TPR 管理を巡っては、1980～1990 年代の情報技術（IT）の発展に伴うアウトソーシングの一般化を契機に注目され始め、近年ではオペレーショナル・レジリエンス強化の観点から、金融監督当局による国際的な議論が一層活発化している。
3. こうした状況を踏まえて、日米欧では TPR 管理に関する制度対応が進展している。加えて、生成 AI の導入によって、TPR 管理に関する課題がより複雑かつ高度化する傾向にあり、欧州を中心に金融監督当局による重要なサードパーティに対する監督や対話の枠組みを構築する動きが進んでいる。他方、金融監督当局からは、デジタル技術の活用において、少数のサービスプロバイダーに市場シェアが集中する構造は、ビジネスにおける規模の経済性の観点から、一定程度避けがたい傾向であるとの見解も示されている。
4. こうした状況下で、デジタル技術の恩恵を最大限に享受するためには、リスクが顕在化した際のシステム障害や業務中断といった影響を最小限に抑えるべく、リスクを適切に管理するための体制を整備・強化していくことが重要だと言える。今後、AI の活用が一層普及していくことが見込まれる中で、金融市場において、効率的かつ効果的な TPR 管理がどのように進展していくのか注目される。

野村資本市場研究所 関連論文等

- ・ 富永健司「金融市場における責任ある AI（RAI）への取り組み—オーストラリアによる RAI の推進事例—」『野村サステナビリティクォーターリー』2025 年春号。
- ・ 富永健司「AI ウォッシングへの監督と金融市場による対応—米 FINRA が示す規制対応に関する検討事項を中心に—」『野村サステナビリティクォーターリー』2025 年冬号。

I 重要性が高まるサードパーティリスク（TPR）管理

昨今、金融市場でデジタル技術の活用が進む中、サードパーティ¹に関連するリスク（TPR）²管理への関心が高まっている。例えば、2024年7月に発生した、サイバーセキュリティ分野における主要企業である米クラウドストライクのセキュリティソフトに起因する大規模なシステム障害は、金融分野を含む幅広い業界の企業活動に深刻な影響を及ぼした³。このような事案は、デジタル関連サービスへの依存が強まる中で、特定のサービスプロバイダーに関連する障害が社会全体に広く影響を及ぼすリスクが増大していることを示唆している⁴。

金融市場では従来、TPRに関する規制やガイダンスが整備されてきたが、特に最近では生成 AI（人工知能）をはじめとする AI の普及が進む中で、金融安定の観点から TPR 管理の重要性が一層増している。さらに、TPR 管理は、安全で、信頼性が高く、倫理的な方法で AI を開発・評価・導入する「責任ある AI（RAI）」の取り組みを推進する上で、金融監督当局からの要請事項に含まれるケースも見られる⁵。

本稿では、TPR が注目される背景と金融監督当局による国際的な議論を概観するとともに、日米欧における制度対応の進展状況を紹介した上で、今後の注目点を論考する。

II 金融市場において TPR が注目される背景

金融市場において TPR への注目度が高まっている背景には、金融サービスにおける AI の活用拡大に伴うサードパーティへの依存度の増加が挙げられる。

近年、金融セクターによる AI 活用は広範囲にわたり、事例も多様化している。こうした動きは、非構造化データの処理能力向上や、モデルの学習と計算を実行するために必要な GPU（画像処理装置）等の活用によって後押しされている。

これらの技術革新は、業務効率や利便性の向上、新たなサービスの創出を可能とする一方で、金融市場におけるサードパーティへの依存度と TPR を一層高める要因となっている。具体的には、（1）ハードウェア、（2）クラウドサービス、（3）モデル、の領域において少数の AI 関連のサービスプロバイダーに市場のシェアが集中する構造が顕在化している（図表 1）。

ハードウェアの観点では、GPU や ASIC（特定用途向け集積回路）といった半導体への依存度が高まっている。クラウドサービスの導入は、様々な処理、AI ツールへのアクセ

¹ 外部委託（アウトソーシング）先、サービス提携先、サービス利用先等の外部事業者を指す。

² 国際決済銀行（BIS）はサードパーティリスクを、サードパーティの業務中断により、金融機関の重要な業務の提供に支障が生じるリスクと位置付けている（Bank for International Settlements[BIS], “Principles for operational resilience,” March 31, 2021）。

³ “Global IT failure puts cyber firm CrowdStrike in spotlight,” *Bloomberg*, July 20, 2024.

⁴ “CrowdStrike outage is another warning for banks,” *Bloomberg*, July 23, 2024.

⁵ 詳細は、富永健司「金融市場における責任ある AI（RAI）への取り組み—オーストラリアによる RAI の推進事例—」『野村サステナビリティクォーターリー』2025 年春号、を参照されたい。

図表 1 金融機関の AI 関連サードパーティへの依存度が上昇する要因

要因	詳細
ハードウェア	・ GPU や特定用途向け集積回路 (ASIC) 等の高速計算チップの活用
クラウドサービス	・ LLM の学習、AI ツールを提供するクラウドサービス事業者を利用
モデル	・ LLM を展開しようとする際に、サードパーティが提供する事前学習済みモデルを使用

(出所) Financial Stability Board, “The Financial Stability Implications of Artificial Intelligence,” November 14, 2024、より野村資本市場研究所作成

スの容易さ、大規模言語モデル (LLM) の活用を通じて推進されている。モデルに関しては、金融機関が AI 関連のアプリケーションを導入する際に、サードパーティが提供する事前学習済みのモデルを購入することが一般的となっている。その結果、サービスプロバイダーが提供する AI モデルが広範囲に拡大する状況が見られている。このような状況において、主要なサービスプロバイダーに関連する障害等が、金融機関の業務運営に大きな影響を及ぼす可能性が高まっている。

Ⅲ 金融監督当局の国際的な議論の動向

歴史的には、1980～1990 年代に、情報技術 (IT) の発展に伴い、IT サービスのアウトソーシングが一般的となったことで、金融監督当局の TPR に対する認識が高まった。こうした中、バーゼル銀行監督委員会 (BCBS) は 2005 年 2 月、銀行・証券・保険分野の金融機関によるアウトソーシングに関する原則を公表した⁶。本原則では、金融機関がアウトソーシングを実施する際の責任のあり方や金融監督当局の役割が示されている。アウトソーシングに関しては、BCBS が示すオペレーショナル・リスク管理の枠組みにおいても、リスク管理上の対応が求められている⁷。

近年では、システム障害や自然災害を含む様々なリスクに対する包括的な枠組みである、オペレーショナル・レジリエンス⁸の強化という観点からも TPR 管理の取り組みが進められている。オペレーショナル・レジリエンスに関する国際原則としては、BCBS が 2021 年 3 月、「オペレーショナル・レジリエンスのための諸原則」がある。同文書には、業務の混乱時においても重要な業務を継続できる能力向上を目的とした原則がまとめられている。

また、BCBS は 2024 年 7 月、デジタル化に伴い銀行がサードパーティへの依存を強めている状況を踏まえ、「健全なサードパーティリスク管理のための諸原則」と題する市中協議文書を公表した (図表 2)。同文書は、銀行のサードパーティリスク管理について、銀行及び金融監督当局に向けた原則を示している。

⁶ BIS, “Outsourcing in financial services,” February 2005.

⁷ BIS, “Revisions to the principles for the sound management of operational risk,” March 2021.

⁸ 金融庁はオペレーショナル・レジリエンスを、「システム障害、テロやサイバー攻撃、感染症、自然災害等の事象が発生しても、金融機関が重要な業務を、最低限維持すべき水準 (耐性度) において、提供し続ける能力」と定義している (金融庁「オペレーショナル・レジリエンス確保に向けた基本的な考え方」2023 年 4 月)。

図表 2 BCBS の市中協議文書で示された TPR 管理に関する原則

原則	分野	詳細
1	ガバナンス・リスク管理・戦略	取締役会は、全てのサードパーティ・サービスプロバイダー (TPSP) との契約の監督に最終責任があり、リスク許容度と混乱への耐性に鑑みて、同契約に関する戦略を承認すべき
2		取締役会は、シニアマネジメントが、TPSP のパフォーマンス及び契約上のリスクに関する報告と軽減策等、TPR 管理フレームワーク (TPRMF) のポリシー及びプロセスを実施することを確保すべき
3	リスク評価	TPSP との契約において、TPRMF の下で包括的なリスク評価を実施すべき
4	デューデリジェンス	TPSP との契約締結前に適切なデューデリジェンス (適正評価手続き) を行うべき
5	契約	TPSP との契約は、契約に関連する当事者の権利と義務、責任、期待を明確に記述した法的に拘束力のある書面で管理されるべき
6	オンボーディング	新しい TPSP との契約の円滑な移行を支援するために、十分なリソースを割り当て、問題の解決を優先すべき
7	継続的な監督	TPSP との契約の状況、リスクの変化、重要性を継続的に評価・監督し、その結果は取締役会及びシニアマネジメントに報告されるべき
8	事業継続管理	TPSP のサービスが中断した場合に運営を継続できるように強固な事業継続管理を維持すべき
9	契約の終了	TPSP との契約の計画的な終了に向けた退出計画と、予期しない終了に備えた退出戦略を保持すべき
10	金融監督当局の役割	監督当局は、TPR 管理を銀行の継続的な評価に不可欠と考えるべき
11		監督当局は、入手可能な情報の分析を通じて、銀行セクターにおける TPSP の集中によって引き起こされるシステムリスクを特定すべき
12		監督当局は、銀行にサービスを提供する重要な TPSP によって引き起こされるシステムリスクを監視するためにセクターや国境を越えた連携と対話を推進すべき

(出所) BIS, “Principles for the sound management of third-party risk,” July 9, 2024、より野村資本市場研究所作成

さらに、前述の通り AI の活用が進む中で、AI サービスプロバイダーの管理に関する観点から、TPR の新しい側面が浮上している。例えば証券監督者国際機構 (IOSCO) は、金融市場における AI の活用に関するリスク及び課題に関連して、少数の AI サービスプロバイダーへの集中リスクを指摘している⁹。

IV 日米欧における制度対応の進展状況

本章では、日米欧において進展する TPR 管理に関連する制度対応の状況について示す。

1. 欧州 (EU 及び英国)

欧州連合 (EU) での TPR 管理に関する制度として、2025 年 1 月より適用が開始されたデジタル・オペレーショナル・レジリエンス法 (DORA) がある。DORA は、金融機関に対してサイバーセキュリティの脅威や業務の中断リスクに対応するために、オペレーショナル・レジリエンスを強化することを目的とした規則である。特に、ICT (情報通信技術) 関連の包括的なリスク管理に重点が置かれていることが特徴である。DORA の適用対象に

⁹ The Board of the International Organization of Securities Commissions, “Artificial intelligence in capital markets: Use cases, risks, and challenges,” March 2025.

は、金融市場参加者に加えて、サードパーティ・サービスプロバイダー（TPSP）をはじめとする多様な組織が含まれている¹⁰。

DORA は特に、ICT の観点からの TPR 管理（ICT TPR 管理）について要件が定められており、金融機関は同管理を、ICT リスク管理の不可欠な要素として考慮することが求められている（図表 3）。具体的には、ICT TPR に関する戦略の策定と定期的な見直しが義務付けられると共に、ICT サービスに関する契約情報の登録簿については維持・更新が必要とされている。また、ICT サービスの利用前にはその重要性や監督上の条件についての評価を実施し、ICT TPSP の情報セキュリティ、アクセス・検査・監査の権利行使についての事前の取り決めが求められている。さらに、契約の終了条件や出口戦略の策定が求められている。加えて、ICT 集中リスクの予備評価が必要とされる。

DORA は、ICT TPSP に関連する集中リスクへの対応を目的として、重要な ICT サードパーティ（CTPP）の指定及び監督の枠組みを定めている。CTPP の指定は、（1）情報登録簿の収集、（2）重要性評価、（3）最終決定、の 3 つのステップで構成されている¹¹。

（1）では、欧州監督機構（ESAs）が各国の監督当局と連携し、金融機関による ICT サードパーティとの契約情報を収集する。（2）では、ESAs が収集した情報を基に ICT サードパーティの重要性評価を行い、同評価結果の通知を行う。（3）では、通知された結果を

図表 3 DORA が規定する ICT TPR 管理の概要

項目	詳細
戦略と方針	・ ICT TPR を、サードパーティとの関係の性質・規模・複雑さ・重要性や契約上のリスク等を考慮して、ICT リスク管理の不可欠な要素として管理 ・ ICT TPR に関する戦略を策定し、定期的に見直し
情報の登録・報告	・ ICT サービスに関する契約情報の登録簿への記録と維持・更新 ・ 新規契約件数やサービス内容を年 1 回以上監督当局に報告
契約締結前の評価	・ 重要性の評価、監督上の条件、関連リスクの特定・評価、デューデリジェンス、TPSP の利益相反の特定・評価
情報セキュリティ	・ 契約は適切な情報セキュリティ基準に準拠した TPSP と締結。重要機能に関連する場合は最新かつ高品質の基準を確認
アクセス・検査・監督の権利行使	・ ICT TPSP に対して、リスクベースの手法に基づき、監査及び検査の頻度及び範囲を事前に設定し、アクセス・検査・監査に関する権利を行使
契約終了条件及び出口戦略	・ ICT TPSP による法令違反又は契約違反等により契約が終了できる条件を設定 ・ ICT TPSP におけるリスク、破綻の可能性、サービスの質の低下、事業の中断等を考慮した出口戦略を策定
ICT 集中リスクの予備評価	・ 重要な機能又はそれをサポートする ICT サービスに関する契約において、代替可能性等を考慮して、リスクを特定・評価

（出所）“Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011,” *Official Journal of the European Union*, December 27, 2022、より野村資本市場研究所作成

¹⁰ 信用機関、決済機関、口座情報サービスプロバイダー、電子マネー機関、投資会社、暗号資産サービスプロバイダー及び資産参照トークンの発行者、中央証券保管機関、中央清算機関、取引所、取引情報蓄積機関、オルタナティブ投資ファンドの運用会社、資産運用会社、データ報告サービスプロバイダー、保険及び再保険会社、保険・再保険仲介業者等、企業年金機関、格付会社、重要なベンチマークの管理者、クラウドファンディングサービスプロバイダー、証券化情報蓄積機関に加えて、ICT TPSP が対象となる。

¹¹ European Securities and Markets Authority, “The ESAs provide a roadmap towards the designation of CTPP under DORA,” February 18, 2025.

踏まえ、異議申立期間（6 週間）を経た後に ESAs が CTPP の最終指定を行う。ESAs によれば、2025 年 7 月までに重要性の評価の通知が行われる予定となっている。

一方、英国では健全性規制機構（PRA）が 2021 年 3 月、金融機関のオペレーショナル・レジリエンスの強化に関する監督指針を公表している¹²。本指針は、重要な業務サービスに対する影響許容度（Impact tolerance）¹³の設定を通じて、業務上の障害に対する金融機関及び金融セクター全体のレジリエンスを向上させることが目的とされる。当該監督指針の中で、TPR に関連して、重要な業務サービスの実施に必要なリソースを特定する「マッピング」を、サードパーティによるサービス提供を含めて実施することが明記されている。

また、PRA は同年同月、アウトソーシング及び TPR 管理の規制要件及び期待事項に関する監督指針を公表した。そしてその後、2024 年 11 月に同指針が改訂された¹⁴。改訂後の指針においては、ガバナンス及び記録管理の項目において、取締役会による関与や企業とサービスプロバイダーによる責任の明確化等が示されている（図表 4）。また、アウトソーシング実施前の検討事項として、アウトソーシング及びサードパーティ契約の重要性に関する判断等が必要とされている。さらに契約においては、重要なアウトソーシング契約についての機能説明等に関する明示が必要との内容が示されている。そして、データセキュリティについては、機密性及び機微性に基づくデータの分類やデータに関するリスクと影響の特定等が求められている。

加えて、PRA は 2024 年 11 月、重要なサードパーティに関する監督指針及び規則文書を公表した¹⁵。これらは、EU における DORA 同様、重要なサードパーティの指定とその規制要件を示すものとなっている。

図表 4 英国のアウトソーシング及び TPR 管理に関する規制要件及び期待事項の例

項目	詳細
ガバナンス及び記録管理	- 取締役会によるアウトソーシングに関する許容度の設定、リスク管理の責任等に関する明確化 - 企業は自社及びサービスプロバイダーの責任を定義し、文書化し、理解すること - アウトソーシングに関する規制上の義務をシニアマネジャーに割り当て - 企業は文書化されたアウトソーシングに関するポリシーの承認、定期的な見直し、及び実施
アウトソーシング実施前の検討事項	- アウトソーシング及びサードパーティ契約の重要性に関する判断 - サービスプロバイダーに対する適切かつリスクに応じたデューデリジェンス - 全てのアウトソーシングのリスク評価
契約	重要なアウトソーシング契約についての機能に関する説明、開始・更新・終了及び解約通知期間、準拠法、財務上の義務、再委託等についての明示
データセキュリティ	機密性及び機微性に基づくデータの分類、データに関するリスクと影響の特定、データの可用性・機密性・完全性についての合意、規制要件を満たして収集・処理されていることを示す保証・文書の取得
アクセス・監査・情報に関する権限	イングランド銀行及び PRA は情報収集及び調査権限を持っており、その一部は金融機関と共にアウトソーシング先のサービスプロバイダーに直接適用されるとの認識

（出所）Bank of England, “SS2/21 Outsourcing and third party risk management,” November 15, 2024、より野村資本市場研究所作成

¹² Bank of England, “SS1/21 Operational resilience: Impact tolerances for important business services,” March 29, 2021.

¹³ 「時間的な長さを含む指標によって測定される、重要な業務サービスにおいて最大限許容される水準」と定義される。

¹⁴ Bank of England, “SS2/21 Outsourcing and third party risk management,” November 15, 2024.

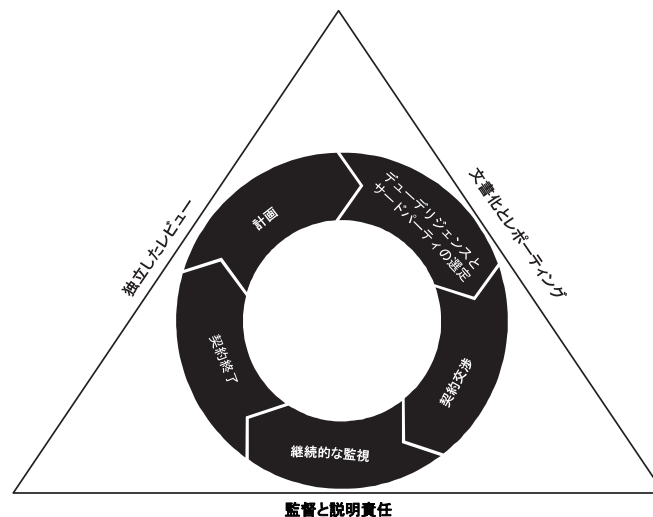
¹⁵ Bank of England, “SS6/24 Critical third parties to the UK financial sector,” November 12, 2024.

2. 米国

米国では、金融規制当局（連邦準備制度理事会〔FRB〕、連邦預金保険公社〔FDIC〕、米国通貨監督局〔OCC〕）が共同で 2023 年 6 月、TPR 管理に関する最終ガイダンス（以下、ガイダンス）を公表した¹⁶。本ガイダンスは、2021 年 7 月から開始された意見募集の結果を受けたものであり、銀行が TPR の特定と管理を支援することを目的として策定された。さらに 2024 年 5 月には、本ガイダンスに関連する具体的な検討事項・情報源・事例を示した補完的なガイドが公表されている。

これらの文書の特徴は、TPR 管理をサードパーティとの関係におけるライフサイクルの視点でとらえ、各ステージにおける考慮事項が示されていることである（図表 5）。具体

図表 5 米国金融規制当局のガイダンスの概要
ライフサイクルのイメージ図



各ライフサイクルの項目に関する概要

項目	詳細
計画	・ 契約締結前にリスクの評価と管理方法を検討。その際、(1)戦略上の目的の理解と目標・リスク許容度・リスク特性・ポリシーとの整合性の把握、(2)メリットの認識とリスク管理方法の決定、(3)取引関係の把握、(4)人員やシステムに関するコストの推定、(5)従業員への影響や移行手段の把握、等を考慮
デュエリジェンスとサードパーティの選定	・ 契約締結前にサードパーティへのデュエリジェンスを実施。その際、(1)戦略と目標、(2)法令遵守、(3)財務状況、(4)事業実績、(5)人材、等を考慮
契約交渉	・ 契約交渉時に、(1)権利と責任の範囲、(2)業績評価指標、(3)情報提供・受領・保持の責任、(4)監査及び是正要求権利、(5)法令順守の責任、等を考慮
継続的な監視	・ サードパーティの管理体制や契約履行能力の確認、重大な問題の特定と迅速な対応を目的として、(1)サードパーティの業績・管理体制に関するレポートの確認、(2)定期的な面談や会議を通じた状況把握、(3)リスク管理体制のテスト、等を実施
契約終了	・ 契約違反、契約の切り替え、内製化、事業の中止等の理由で契約終了に至る場合、(1)サービス移行の選択肢、(2)必要なリソースや期間、(3)費用、(4)リスク管理、(5)知的財産の取り扱い、等を検討

（出所） Board of Governors of the Federal Reserve System, “Agencies issue final guidance on third-party risk management,” June 6, 2023、より野村資本市場研究所作成

¹⁶ Board of Governors of the Federal Reserve System, “Agencies issue final guidance on third-party risk management,” June 6, 2023.

的には、計画の段階では、契約締結前にリスク評価と管理手法が検討される。デューデリジェンスとサードパーティの選定の段階では、サードパーティに対して戦略と目標をはじめとする内容に関するデューデリジェンスの実施が求められている。契約交渉では、契約交渉時に権利と責任の範囲、業績評価指標等に関する項目を考慮することが必要とされる。また、継続的な監視においては、サードパーティの管理体制及び契約履行能力の確認、重大な問題の特定や対応といった取り組みが示されている。加えて、契約終了の際には、サービス移行の選択肢、必要なリソースや期間等を検討することが必要とされる。

米国においてはこの他、FINRA（金融取引業規制機構）が 2025 年度の規制監視レポートにおいて、近年証券会社が様々な業務や機能に関するサードパーティへの依存度が高まっているとの見方を示すと共に、会員証券会社に対して、TPR 管理の強化を求めている¹⁷。

3. 日本

日本では金融庁が 2023 年 4 月、IT システムへの依存度の高まり、大規模システム障害の発生等、リスク環境が変化・複雑化する中で、オペレーショナル・レジリエンス確保に向けた基本的な考え方を公表した¹⁸。本文書の中では、オペレーショナル・レジリエンスに関する基本動作において、「相互関連性のマッピング・必要な経営資源の確保」を示している。この中で特定のサードパーティへの集中リスクへの対応として、（1）個別金融機関によるサードパーティへのモニタリング強化、（2）代替手段・出口戦略の確保、（3）内製化、（4）業界横断的な取り組みの強化、が示されている。

（1）については、モニタリングの効率性や実効性を高めるための実務上の工夫としては、地域金融機関向け共同システムを運営する IT ベンダーに対する共同監査等が挙げられている。（2）については、システム障害等に備えて、システムのバックアップ体制の構築や冗長化¹⁹の対応が言及されている。（3）については、特定のサードパーティの依存度を減らすために取り得るアプローチとして、アウトソーシング業務の内製化があり、IT システム開発について自前で判断できる体制を確保することが重要、との見方が示されている。（4）については、金融システム全体のオペレーション・レジリエンスの実効性確保の観点から、業界横断的な訓練や演習も有益とされている。また、金融機関向け共同システムの運営者を含めた大手ベンダーのような重要なサードパーティについては、その集中リスクを把握する観点から、金融庁として対話を進めていくことに一定の意義があるとの考え方が示されている。

なお、金融庁が 2024 年に実施した金融機関等の AI の活用実態に関するアンケート調査によれば、AI の検討・導入・利用時の課題について、「適切なサードパーティ（外部事

¹⁷ FINRA, “2025 FINRA Annual Regulatory Oversight Report,” January 28, 2025.

¹⁸ 金融庁「オペレーショナル・レジリエンス確保に向けた基本的な考え方」2023 年 4 月。

¹⁹ システムやネットワークを多重化して障害に備える仕組み。

業者)の選択」を課題として選択した先が4割強に達したことが明らかになった²⁰。具体的な課題として、「LLMの完全内製は不可能であるため何らかの外部サービスとの接続を要するが、外部サービスとのセキュアな通信手段の確立は課題」といった見解や、「生成AIは従来型AIとは異なり性能の評価方法や評価軸が確立しておらず、また汎用性も高いため、客観性を持って性能検証をすることが難しい。その結果、体系的評価に基づき適切なサードパーティを選定することも現状困難」といった意見が示されている。

V 今後の注目点

世界ではAIの活用拡大に伴い、AI関連のサービスプロバイダーに市場シェアが集中する構造が生まれており、TPR管理の重要性が高まっている。歴史的には、1980～1990年代におけるITの発展に伴ってアウトソーシングが一般的化したことを契機に、TPR管理の必要性が認識されるようになった。近年では、オペレーショナル・レジリエンス強化という観点からもTPR管理の議論が進んでいる。また、責任あるAIの考え方においても、TPR管理が取り上げられている。こうした状況を踏まえて、日米欧においては、TPR管理に関する制度対応が進展している。

加えて、生成AIの導入によって、TPR管理に関する課題がより複雑かつ高度化する傾向にあり、欧州を中心に金融監督当局による重要なサードパーティに対する監督や対話の枠組みを構築する動きが進んでいる。

他方、金融監督当局からは、AIをはじめとするデジタル技術の活用が進展する中で、少数のサービスプロバイダーに市場シェアが集中する構造は、ビジネスにおける規模の経済性の観点から、一定程度避けがたい傾向であるとの見解も示されている²¹。こうした状況下で、デジタル技術の恩恵を最大限に享受するためには、リスクが顕在化した際のシステム障害や業務中断といった影響を最小限に抑えるべく、リスクを適切に管理するための体制を整備・強化していくことが重要だと言える。

今後、AIの活用が一層普及していくことが見込まれる中で、金融市場において、効率的かつ効果的なTPR管理がどのように進展していくのか注目される。

²⁰ アンケート調査は、2024年10月から11月にかけて金融分野の幅広い業種を対象に実施されたもので、合計130社が回答（金融庁「AIディスカッションペーパー（第1.0版）―金融分野におけるAIの健全な利活用の促進に向けた初期的な論点整理―」2025年3月）。

²¹ Financial Stability Board, “The Financial Stability Implications of Artificial Intelligence,” November 14, 2024.