バーゼル銀行監督委員会による市中協議文書「健全なサードパーティリスク管理のための諸原則」について

2024年８月

金融庁／日本銀行

＊当資料は、バーゼル銀行監督委員会による公表文書の理解促進の一助として作成されたものです。公表文書のより詳細な内容については必ず原文をご確認ください。

目次

1. 本諸原則の全体像と主なポイント
2. 銀行向けの各原則の内容
3. 今後の予定

1. 本諸原則の全体像と主なポイント

（1）全体像

- バーゼル銀行監督委員会（以下「バーゼル委」）は、本年7月9日、標記の市中協議文書を公表。本諸原則は、デジタル化に伴い銀行がサードパーティへの依存を深めていることを踏まえ、2005年2月公表の銀行・証券・保険の業態横断的な文書「金融サービスにおけるアウトソーシング」（原題：Outsourcing in Financial Services）を銀行業態についてアップデートするものとして策定。
  - 本諸原則におけるサードパーティ（TPSP：Third-Party Service Provider）は、従来の外部委託先に加え、調達先やサービス連携先等を含む。
- また、本諸原則は他の基準設定主体等が公表した以下をはじめとする文書を補完するものとの位置づけ。
  - 金融安定理事会（FSB）「サードパーティリスクの管理とオーバーサイトの向上：金融機関と金融当局のためのツールキット」（2023年12月）
  - 保険監督者国際機構（IAIS）「保険業態のオペレーショナル・レジリエンスに関する論点書」（2023年5月）
  - 証券監督者国際機構（IOSCO）「アウトソーシングに関する原則」（2021年10月）

（1）全体像 （続）

- バーゼル委は、本諸原則の策定により、銀行がサードパーティリスク管理の実効性を高め、オペレーショナル・リスク管理及びオペレーショナル・レジリエンスの向上をプリンシプル・ベースで促進することを企図。このアプローチは、以下をはじめとするバーゼル委の他の公表文書に基づいている。
  - 「健全なオペレーショナル・リスク管理のための諸原則の改訂」（2021年４月）
  - 「オペレーショナル・レジリエンスのための諸原則」（2021年４月）
- 本諸原則は、主な対象を国際的に活動する大手銀行（The Principles are primarily directed to large internationally active banks）としつつ、より小規模な銀行も恩恵を受けることができるほか、銀行業態以外の金融機関にとっても有益な可能性があるとしている。
- 銀行のサードパーティリスク管理について、銀行向け（９つ）と監督当局向け（３つ）の計12の原則を提示。

（2）本諸原則の主なポイント

①比例原則及び重要なサードパーティの取扱い

- 本諸原則は、銀行の規模、複雑性、リスク・プロファイル、TPSPとの取決めの内容（性質と期間、重要なサービスの提供に対する貢献度合い等）に応じて、比例的に（on a proportionate basis）適用される。
- TPSPの重要性を評価する際、銀行は、取決めの財務上、オペレーション上又は戦略上の重要性、混乱に対する銀行の許容度、TPSPと共有するデータ又は情報の性質、サービスの代替可能性等の要素を考慮すべきとしている。
- リスクベース・アプローチに基づき、銀行が柔軟に対応することを企図。
  - 重要なTPSPとの取決めに対しては①銀行とTPSP間の契約、②業務継続、③出口計画及び戦略について最低限対応すべき項目を提示している一方、その他のTPSPについては考慮事項として示している。
  - 銀行の一部の対応（台帳の完備・更新、定期的及び環境の変化に応じた取決めのレビュー、予期しない終了のための出口戦略の維持）については、全てのTPSPに適用されることを明示。

（2）本諸原則の主なポイント （続）

②nthパーティとサプライチェーン

- TPSPが銀行へサービスを提供するにあたっては、4thパーティを含むnthパーティに依存していることがあり、銀行に追加的なリスクをもたらす可能性があるため、サプライチェーン全体を俯瞰する必要性が意識されている。本諸原則では、銀行とnthパーティに直接的な契約関係がないことを踏まえ、銀行にとってのサービスの重要性に応じて、nthパーティについてもTPSPを通じて適切に管理すること等を要請。
- 例えば、銀行への重要なサービスの提供に関与、または銀行にとって秘匿性の高い情報にアクセス可能なnthパーティ（key nth party）については、継続的なモニタリングの対象とすること、TPSPとの契約において（インシデント報告を含めた）情報取得権を含めることを求めている。

（2）本諸原則の主なポイント （続）

③集中リスク

- 本諸原則では、集中リスクについて、個別行レベルとシステミックの２種類に分類。個別行レベルの集中リスクのモニタリング・管理は当該銀行の責任であるとしているほか、システミックな集中リスクについても、利用可能な情報をもとにTPSPのシステム上の重要性を理解することが重要であるとしている。

④監査（audit）と保証（assurance）

- 本諸原則では、銀行がTPSPの入口審査や継続的なモニタリングにおいて、監査・保証を活用できることを指摘。
- 保証に関しては（ISOのような）業界標準基準等が有益としている。もっとも、単一の保証が銀行にとって必要な事項を全て提供するとは限らないため、監査や他の保証の必要性を排除する訳ではないとしている。

2. 銀行向けの各原則の内容

(1)ガバナンス、リスク管理及び戦略

原則1: 取締役会等の責任	取締役会は、全てのサードパーティとの取決めを監督する最終的な責任を有し、銀行のリスクアペタイトと混乱(disruption)に対する許容度の範囲内で、サードパーティとの取決めに関する明確な戦略を承認すべき。
原則2: リスク管理枠組みの実施	取締役会は、上級管理職が、サードパーティの実績並びにサードパーティとの取決めに関するリスクの報告及び低減措置を含む戦略に沿って、サードパーティリスク管理の枠組みの方針及びプロセスを実施することを確実にすべき。

- 銀行は、**全ての**TPSP及び重要なnthパーティについて、台帳(register)を完備し最新の状態に更新すべき。
- 高リスクまたは重要な取決めについて、相互依存性・相互連関性のマッピングを行い、台帳を監督当局に共有可能にしておく必要がある。
- 銀行は、自行に関する個社レベルでの集中リスクを評価し、集中リスクが回避できない場合はモニタリング等を強化すべき。

（2）リスク評価とデュー・デリジェンス

原則3： リスク評価	銀行は、サードパーティとの取決めを締結する前及び取決めを結んでいる間を通じて、特定されたリスク及び潜在的なリスクを評価し管理するために、サードパーティリスク管理の枠組みの下で包括的なリスク評価を行うべき。
原則4： デュー・デリジェンス	銀行は、サードパーティとの取決めを締結する前に適切なデュー・デリジェンスを行うべき。

- 銀行は、TPSPとの取決めを締結する前に、また契約締結後も反復的に、その重要性とリスクを特定・評価する必要がある。重要性を評価する際、銀行は、取決めの財務・運営・戦略上の重要性、混乱に対する銀行の許容度、サードパーティと共有するデータ又は情報の性質、サービスの代替可能性等の要素を考慮すべき。

（3）契約

原則5： 契約	サードパーティとの取決めは、すべての当事者の権利、責任及び期待を明確に記述した法的拘束力のある書面による契約によって管理されるべき。

- 銀行は、TPSPとの契約において、（パラ41に定める）TPSPからの情報取得権等の18項目を考慮すべき。また、重要なサービスについては、上記の18項目に加えて、重要なnthパーティからの情報取得権を含む7項目を最低限契約に含めることが求められる。

（4）オンボーディングとモニタリング

原則6： オンボーディング	銀行は、デュー・デリジェンスや契約条項の解釈の過程で特定されたあらゆる問題の解決を優先させるために、新たなサードパーティとの取決めに円滑に移行するための十分な資源を投入すべき。
原則7： モニタリング	銀行は、サードパーティとの取決めのパフォーマンス、リスクの変化、及び重要性を継続的に評価・監視し、その結果を取締役会や上級管理職に報告し、必要に応じて問題に対応すべき。

- 銀行は、TPSP（重要なnthパーティを含む）の能力や問題点・懸念事項等を継続的に確認する。**全ての**取決めは、定期的又は内部・外部環境の変化に応じてレビューされるべき。
- 重要なTPSPに関するBCP（Business Continuity Plan）やDRP（Disaster Recovery Plan）について、定期的にレビューされ、訓練も実施されるべき。
- 銀行は、TPSPと契約したサービスについて、外部監査の結果やその他の保証を利用することができるが、重要なサービスについては、単一の保証に依存するのではなく、複数の保証を利用すべきである。

（5）業務継続管理

原則8： 業務継続管理	銀行は、サードパーティのサービスが中断した場合に業務を継続する能力を確保するために、堅固な業務継続管理を維持すべき。

- TPSP関連の業務継続管理については、①銀行内部のBCP・DRPの策定・更新、②定期的なBCP・DRPの訓練、③代替候補先となるTPSPの定期的な更新を考慮すべき。
- また、重要なTPSPとの間の契約には、上記に加えて以下を最低限含むべき。
  - TPSPによる、明確かつ測定可能なRTO（Recovery Time Objectives）・RPO（Recovery Point Objectives）を含むBCPの策定・更新。
  - TPSPのBCPが頑健であることを保証するためのテストの実施。

（6）終了

原則9： 終了	銀行は、サードパーティとの取決めの計画的な終了のための出口計画及び計画外の終了のための出口戦略を維持すべき。

- TPSPとの取決めの計画的な終了のための出口計画では、①移行期間、②契約上の権利の完全な行使、③適切な予算、④責任範囲の特定を考慮すべき。
- また、重要なTPSPとの取決めの出口計画には、上記のほか、①論理的資産（データ等）、有形資産、人的リソースの適切・適宜の移転、②全てのステークホルダーとの調整に必要な措置を最低限含める必要がある。
- 計画外の終了のための出口戦略については、銀行の規模、複雑性及びリスク特性並びにTPSPのサービスの重要性等を考慮しつつ、**全ての**サードパーティ取決めに対して適切かつ比例的に維持すべき。
- また、重要なサードパーティ取決めに対する出口戦略には、①資産移転のプロセス、②緊急時に対応を行う人員の定期的な更新、③追加コストを確保するための予算承認のプロセスを最低限含める必要がある。

3. 今後の予定

- 本市中協議文書に対するコメントは、令和6年（2024年）10月9日までに以下のBISのウェブサイトに英文でご提出ください。

  https://www.bis.org/bcbs/commentupload.htm

- コメントは特段の断りが無い限り、すべてBISのウェブサイトに掲載されます。

Annex.諸原則の抄訳

原則1： 取締役会等の責任	取締役会は、全てのサードパーティとの取決めを監督する最終的な責任を有し、銀行のリスクアペタイトと混乱（disruption）に対する許容度の範囲内で、サードパーティとの取決めに関する明確な戦略を承認すべき。
原則2： リスク管理枠組みの実施	取締役会は、上級管理職が、サードパーティの実績並びにサードパーティとの取決めに関するリスクの報告及び低減措置を含む戦略に沿って、サードパーティリスク管理の枠組みの方針及びプロセスを実施することを確実にすべき。
原則3： リスク評価	銀行は、サードパーティとの取決めを締結する前及び取決めを結んでいる間を通じて、特定されたリスク及び潜在的なリスクを評価し管理するために、サードパーティリスク管理の枠組みの下で包括的なリスク評価を行うべき。
原則4： デュー・デリジェンス	銀行は、サードパーティとの取決めを締結する前に適切なデュー・デリジェンスを行うべき。

Annex.諸原則の抄訳

原則5： 契約	サードパーティとの取決めは、すべての当事者の権利、責任及び期待を明確に記述した法的拘束力のある書面による契約によって管理されるべき。
原則6： オンボーディング	銀行は、デュー・デリジェンスや契約条項の解釈の過程で特定されたあらゆる問題の解決を優先させるために、新たなサードパーティへ円滑に移行するための十分な資源を投入すべき。
原則7： モニタリング	銀行は、サードパーティとの取決めのパフォーマンス、リスクの変化、及び重要性を継続的に評価・監視し、その結果を取締役会や上級管理職に報告し、必要に応じて問題に対応すべき。
原則8： 業務継続管理	銀行は、サードパーティのサービスが中断した場合に業務を継続する能力を確保するために、堅固な業務継続管理を維持すべき。
原則9： 終了	銀行は、サードパーティとの取決めの計画的な終了のための出口計画及び計画外の終了のための出口戦略を維持すべき。

Annex.諸原則の抄訳

原則10: 銀行のリスク評価	監督当局は、サードパーティリスク管理を銀行の継続的評価の不可欠な部分として考慮すべき。
原則11: システム全体の集中リスク	監督当局は、銀行セクターにおける1つまたは複数のサードパーティサービスプロバイダの集中がもたらす潜在的なシステミック・リスクを特定するために、利用可能な情報を分析すべき。
原則12: 当局間の協調	監督当局は、セクターや国境を越えて銀行にサービスを提供する重要なサードパーティサービスプロバイダがもたらすシステミック・リスクをモニターするために、協調と対話を促進すべき。