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

2026年２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

（1）全体像

- バーゼル銀行監督委員会（以下「バーゼル委」）は、2025年12月10日、標記の文書を公表。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）「外部委託に関する原則」（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、実効的なサードパーティリスク管理のためのプリンシプル・ベースのアプローチを促進し、銀行におけるオペレーショナル・リスク管理を補完するとともに、オペレーショナル・レジリエンスを強化することを企図。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３月）
  - 「オペレーショナル・レジリエンスのための諸原則」（2021年３月）
- 本諸原則は、銀行のサードパーティリスク管理について、リスク評価、デュー・デリジェンス、契約締結、オンボーディング・継続的なモニタリング、契約終了という、TPSPに係る一連の「ライフサイクル」に関連付けるかたちで、銀行向け（９つ）と監督当局向け（３つ）の計12の原則を提示。
- 銀行向け原則の対象は、国際的に活動する大手銀行（large internationally active banks）としている。

（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、ビジネスモデル、リスク・プロファイル、TPSPとの取決めのリスクや重要性に応じ、比例的に（on a proportionate basis）適用される。
- TPSPとの取決めのリスクのタイプ・レベルを評価する際、銀行は、銀行レベルの集中リスク、長大・複雑なサプライチェーンに起因するリスク、新技術や高度な技術に関連するリスク、その他財務的・非財務的リスクを考慮すべきとしている。また、重要性を評価する際、銀行は、TPSPが提供するサービスの中断に対する許容度、TPSPと共有するデータ・情報の性質、サービスの代替可能性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含める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リスクや重要性に応じて、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、重要なTPSPとの取決めの中で、銀行への重要なサービスの提供を支え、不可欠な役割を果たす主要なnthパーティ（key nth party）については、TPSPに対する義務と同等の契約上の義務を適切に適用するほか、完全かつ最新の台帳を維持することや、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、信頼できる情報（公開情報やTPSPから直接得た情報等）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のデュー・デリジェンスやオンボーディング、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。
- 監査には、銀行単独または複数銀行共同の依頼に基づく独立した第三者の監査、（銀行による批判的レビューが前提であるが）TPSP自身による監査が含まれるとしている。保証に関してはISO認証などの業界標準等が含まれるが、重要なサービスに関する完全な保証を提供するものではないことから、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. 市中協議の結果

（1）コメントの概要

- 2024年7月～10月にかけて実施した市中協議で寄せられたコメントの主な内容は以下の通り。
  - オペレーショナル・レジリエンスを超える幅広いリスクや、個別のTPSPとの取決めの（重要性のみならず）リスクに応じた管理策が必要。
  - 既存の諸原則（「健全なオペレーショナル・リスク管理のための諸原則」、「オペレーショナル・レジリエンスのための諸原則」）や、FSBによる「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」との整合性を確保するべき。こうしたもと、TPSPとの取決めが過度に「重要な取決め」に分類されることがないようにするべき。
  - 特に小規模なTPSPやグループ内の取決めに関しては比例適用が必要。
  - 銀行が（個別行レベルを超えて）システミックな集中リスクを把握することは困難。
  - nthパーティに関しては、主要な先に焦点を当てたリスクベース・アプローチがとられるべき。
  - 取締役会はTPSP戦略の監督に集中すべきであり、個別の取決めの監督は不要。

（2）市中協議文書からの主な修正点

（重要＜critical＞の定義）

- 「重要（critical）」の範囲として、従前のオペレーショナル・レジリエンスにおける「重要性」に加えて「リスク（タイプ・レベル）」の概念が追加された。これにより、「重要な取決め」に係る追加的な要件は、重要性の高い取決めのみならず、リスクの高いものにも柔軟に適用されることとなる。
- 他方、「重要な」取決めへの過度な分類を回避すべく、「重要なサービス」、「nthパーティ」、「主要なnthパーティ」の定義が精緻化され、「重要なTPSP」の定義は削除された（「重要なTPSPとの取決め」の定義は残存）。

（比例適用等）

- 「より小規模な銀行も恩恵を受けることができる」旨の記載は削除された。
- 銀行が「リスク（タイプ・レベル）」と「重要性」に応じてリスク管理策を柔軟に適用できることが文書全体を通じて明確化された。
- nthパーティに係る要件は主要な先に限定された。

（集中リスク）

- 銀行が対応を求められる集中リスクが、原則「個別行レベル」であることが明確化された。

（2）市中協議文書からの主な修正点（続）

（重要なTPSPとの取決めに係る要件）

- 重要なTPSPとの取決めに関して、①銀行とTPSP間の契約、②業務継続、③出口計画・戦略で含めるべきとされる事項について、当初の「最低限含めるべき」との表現は削除された。ただし、重要なTPSPとの取決めに関しては、市中協議文書と同様、全てのTPSPとの取決めにおける考慮事項に加え、複数の「追加的」な事項についても対応すべきであるとされている。

3. 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、銀行のサードパーティリスクの監督に対して最終的な責任を負い、明確な戦略を承認し、銀行のリスクアペタイトとサービス中断(disruption)に対する許容度を定義すべき。
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、銀行のサードパーティ戦略に沿ったサードパーティリスク管理枠組みに基づく方針及びプロセスを実施することを確実にすべき。これらの方針及びプロセスには、TPSPの実績・TPSPとの取決めに関連するリスク・低減措置について、取締役会へ報告することが含まれる。

- 銀行は、**全ての**TPSP及び主要な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、集中リスクが存在する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、TPSPとの取決めを締結する前及びライフサイクル全体を通じて、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、TPSP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、またライフサイクル全体を通じて反復的に、リスクのタイプ・レベルと重要性を特定・評価する必要がある。リスクのタイプ・レベルを評価する際、銀行は、銀行レベルの集中リスク、長大・複雑なサプライチェーンに起因するリスク、新技術や高度な技術に関連するリスク、その他財務的・非財務的リスクを考慮すべきとしている。また、重要性を評価する際、銀行は、TPSPが提供するサービスの中断に対する許容度、TPSPと共有するデータ・情報の性質、サービスの代替可能性も考慮すべきとしている。

（3）契約締結

原則5： 契約締結	TPSPとの取決めは、すべての当事者の権利・義務、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40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TPSPとの取決めについては、上記の18項目に加えて、主要なnthパーティからの情報取得権を含む6項目を追加的に契約に含めることが求められる。

（参考）TPSPとの契約において考慮ないし含めるべき項目（附番は金融庁・日本銀行による）

全ての契約における考慮事項/重要な契約で含めるべき事項

①KPI
②銀行が正確・包括的・タイムリーな情報を受け取る権利
③TPSPの権利
④銀行がTPSPにアクセス（施設を含む）、監査、関連情報を取得する権利
⑤監督当局がTPSPにアクセス（施設を含む）、監査、情報取得する権利（ただし、各法域の法令等による）
⑥業務継続・災害復旧に関する義務と責任
⑦コスト構造
⑧論理資産（データ等）及び物理資産に関する所有権、アクセス権、利用権、ならびに契約終了時も含む適時適切な権利移転の容易性
⑨セキュリティ、レジリエンス、その他技術構成に関する義務と責任
⑩業務実施および関連データの処理・保存が行われる場所（国・地域等）
⑪銀行が保有する専有的・戦略的情報の機密性および秘密保持契約の活用
⑫銀行の情報がTPSPの他の顧客情報と混在するリスクへの対応
⑬銀行が特定の状況で補償を受ける権利
⑭顧客苦情対応および紛争解決の仕組み
⑮紛争時の準拠法および管轄（可能であれば、銀行の法人所在地または営業法域の法律を適用することを優先）
⑯デフォルトおよび契約終了に関する条件
⑰規制・監督要件の変更等の理由により既存の取決めを修正するための枠組み
⑱契約終了に備えた銀行の出口戦略を支援する条項

重要な契約で追加的に含めるべき事項

i. 主要なnthパーティに関する条件（例：利用または変更の事前通知、インシデント報告）
ii. KPIの追加指標と測定方法（例：SLAとサービス基準、BCPテスト結果、統制有効性テスト結果、顧客苦情情報）
iii. SLAに記載された情報を銀行が正確・包括的・タイムリーに受け取る権利（TPSPや主要なnthパーティのサービスに関するインシデントや重要な変更情報を含む）
iv. 銀行が主要なnthパーティにアクセス、監査、関連情報を取得する権利
v. 監督当局が主要なnthパーティにアクセス、監査、情報取得する権利（ただし、各法域の法令等による）
vi. 業務継続計画および災害復旧計画に関する義務と責任（最低稼働時間、最大停止時間、RTO〔復旧時間目標〕、RPO〔復旧時点目標〕を含む）

（4）オンボーディングと継続的なモニタリング

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解決への対応を含め、新たなTPSPのオンボーディングを円滑に進めるための十分な資源を投入すべき。
原則7： 継続的なモニタリング	銀行は、TPSPとの取決めのパフォーマンス、リスク及び重要性の変化を継続的に評価・モニタリングし、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（主要な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**取決めは定期的に、および内部・外部環境やTPSP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）についてレビューし、TPSPによる定期的な訓練の実施を確保すべき。
- 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・定期的なレビュー・更新、②定期的なBCP・DRPの訓練、③インシデントや定期的な訓練の結果から得られた教訓、④緊急時代替候補先となるTPSPの定期的な更新を考慮すべき。
- また、重要なTPSPとの取決めには、上記に加えて以下を追加的に含むべき。
  - TPSPによる明確かつ測定可能な指標（例：RTO（Recovery Time Objectives）・RPO（Recovery Point Objectives））を含むBCPの策定・定期的なレビュー・更新。
  - TPSPの業務継続管理プロセスが頑健であることを保証するための銀行によるテストの実施。

（6）契約終了

原則9： 契約終了	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（予期せぬ）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性、③適切な予算配分、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論理資産（データ等）、物理資産、人的リソースの適時適切な移転に関するプロセス、②全てのステークホルダーとの調整に必要な措置を追加的に含めるべき。
- 計画外の終了のための出口戦略については、妥当なシナリオと合理的な前提に基づき、TPSPから提供されるサービスの重要性と代替可能性を考慮しつつ、全てのサードパーティとの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TPSPとの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含めるべき。

４. 今後について

- ここ数年、ソフトウェアの変更管理に起因する問題でわが国を含めて金融業界が大きな影響を受けた事例があるほか、国内でもサードパーティへのサイバー攻撃を通じた深刻な個人情報漏洩事案等が発生しており、サードパーティリスク管理はより一層重要性を増している。

- 従前から、わが国金融機関には、委託先管理やサイバーセキュリティにとどまらず、法令・監督指針等に基づき、サードパーティリスク管理について適切な対応が求められているところ。改めて、「金融分野におけるサイバーセキュリティに関するガイドライン」（2024年10月）や、今回新たに策定された本諸原則を、さらなるリスク管理の高度化に活用することが期待される。

- 本諸原則を踏まえた先行きのサードパーティリスク管理に関する監督・モニタリングのあり方については、金融機関との対話も踏まえ、適切に検討していく方針。