ディスカッション・ペーパー

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

令和５年４月

金融庁
Financial Services Agency

目 次

BOX 一覧

BOX 番号	タイトル
BOX1	オペレーショナル・リスク管理
BOX2	システムリスク管理とサイバーセキュリティ
BOX3	業務継続計画（BCP）と再建・処理計画（RRP）
BOX4	稼動目標（Service Level Objective）と耐性度（Tolerance for disruption）
BOX5	相互連関性のマッピングの範囲・粒度
BOX6	サードパーティリスク管理①（個別金融機関によるモニタリングの強化）
BOX7	サードパーティリスク管理②（代替手段・出口戦略の確保）
BOX8	サードパーティリスク管理③（内製化）
BOX9	サードパーティリスク管理④（業界横断的な取組の強化）
BOX10	必要な人的資源確保のための人事制度（メンバーシップ型／ジョブ型）
BOX11	リスク管理文化の醸成①（ジャストカルチャー）
BOX12	リスク管理文化の醸成②（心理的安全性）
BOX13	コンプライアンス・リスク管理（コンダクトリスク管理）

I. はじめに

1. なぜ今オペレーショナル・レジリエンスか

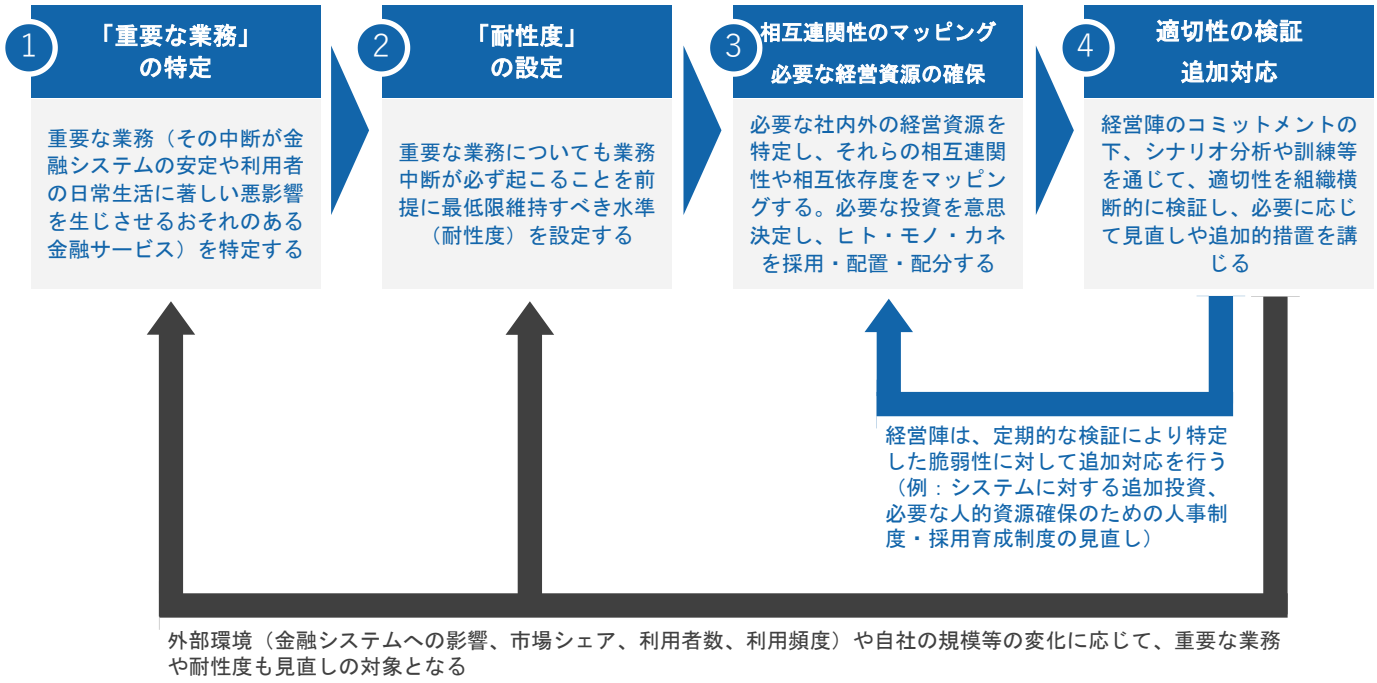
金融機関を取り巻く環境は急速に変化している。IT システムへの依存の高まり、大規模システム障害の発生、感染症の拡大、サイバーセキュリティ上の脅威の高まり、クラウドサービスの利用の広がり、FinTech 企業等との連携による相互依存度の高まりなど、リスク環境は複雑化する一方である。

こうした中、既存のリスク管理（未然に事故や障害を防ぐための態勢整備）や、BCP（地震などの特定のリスク事象を想定した対応計画）だけでは、想定外の事象が生じた場合に、決済サービスなどの金融システムにとって重要な業務を提供し続けることができないおそれがある。未然防止策を尽くしてもなお、業務中断は必ず起こることを前提に、利用者目線に立ち、代替手段等を通じた早期復旧や影響範囲の軽減を担保する枠組みを確保することが重要である。外部委託業務や連携サービスを含めた業務プロセス全体の包括的な態勢整備によって、オペレーショナル・レジリエンス（業務の強靭性・復旧力。以下「オペレジ」）を確保することは、国際的にも重要視されている。

2021 年3月にバーゼル銀行監督委員会が策定した国際原則を踏まえ、本文書では、オペレジを、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する。金融機関がオペレジを確保するためには、重要な業務を特定した上で、業務中断後（危機時）の金融システムや利用者への影響を耐性度（最終防衛ライン）内に収めるよう、平時から社内外の業務プロセスの相互連関性をマッピングし、必要な経営資源（ヒト・モノ・カネ）を確保し、訓練・テスト等を通じて適切性を検証し、定期的に見直し続けることが、経営陣に求められる。（【図表1】参照）

このように、オペレジを実効性のある形で確保するためには、オペレジに対する組織横断的な理解の浸透や、経営陣のトップダウンによるコミットメントが不可欠である。もっとも、現状ではベストプラクティスを探求している段階にある論点も多い。また、オペレジは画一的な基準を課す趣旨ではなく、金融機関の規模・リスク選好度・金融システムへの影響に応じた、比例原則に基づく対応が求められる。そこで本文書は、国際的な動向を概観した上で、オペレジ確保に向けた基本的な枠組みを示し、考慮すべき論点・課題を整理することを目的とした。（【図表2】参照）

図表1:オペレジの基本動作



（資料） 金融庁

図表2：課題の例と、オペレジの確保によって期待される効果

	課題の例	期待される効果
利用者目線の金融サービス	未然防止策に重点が置かれ、結果的に業務中断が発生してしまった後（危機時）の対応が不十分。	**利用者目線で危機時の影響を極小化**（早期復旧や代替手段の確保、迅速な広報により、利用者目線で影響を限定的にする）。
業務プロセス全体の合理性	ゼロリスク志向（zero tolerance）により、未然防止策のマニュアルやチェックリストが際限なく増加し、業務効率が悪化し、現場が疲弊する。 リスク管理・危機管理の枠組みが林立し、部署ごとの縦割りで、全体として非効率な業務プロセスとなってしまう。	ヒューマンエラーや想定外の事象はゼロにはできないとの認識の下、現実的な耐性度（重要な業務の最低限維持すべき水準）を設定し、**包括的に態勢を再構築する**（既存の枠組みを活用しつつ、メリハリをつけて業務プロセス全体を合理化・効率化する）。
リソース配分の実効性	業務継続計画（BCP）の実行に必要な経営資源（ヒト・モノ・カネ）が実際には配置されていない。 サードパーティを含めた社内外の経営資源の相互連関性がマッピングされておらず、脆弱性を特定できていない。	重要な業務の最低限維持すべき水準（耐性度）での遂行に**必要な社内外の経営資源を特定し、実際に採用・育成・配置する**（含むガバナンス・人事制度見直し）。
経営陣のコミットメント	枠組みの適切性の検証が形骸化し、環境変化への適応が遅れるなど、PDCAサイクルが機能していない。	必要な経営資源が実際に配置されているか、監督当局を含めたステークホルダーに対して、**経営陣が説明責任を果たす。**
企業文化	ゼロリスク志向や過度な減点主義により、現場が委縮し、懸念が経営陣まで報告されず、部門間の連携も悪い。	**リスク管理文化の醸成**（Bad News First の徹底、自由闊達な対話、組織の縦割りを超えた連携）。

（資料） 金融庁

2. 本文書の位置づけに関する留意事項

金融庁では、検査・監督全般に共通する基本的な考え方と進め方を整理した「金融検査・監督の考え方と進め方（検査・監督基本方針）」（2018 年6月公表）を踏まえ、個々のテーマ・分野ごとのより具体的な考え方と進め方を、議論のための材料であることを明示した文書（ディスカッション・ペーパー）の形で示すこととしている。本文書の位置づけは、金融機関がオペレジを確保していく際の論点・課題をディスカッション・ペーパーとして整理したものである。

本文書は、主として銀行を対象にしているが、これ以外の金融システム上重要な業務を担う企業においてもオペレジの確保は重要な課題であり、より良い実務の構築に向けた金融庁と金融機関との対話の材料として活用することを念頭に置いたものである。

また、本文書については、現時点での金融庁としての考え方・進め方を整理したものであるが、オペレジに係る実務や手法は発展途上にあり、国際的な議論も継続中であることから、今後こうした実務や手法が確立していくにつれて改訂されるべきものである。本文書に記載する事例等についても、ベストプラクティスを示すという位置づけではなく、あくまで本文書作成時点の参考事例を示すものである。

金融庁が本文書を材料に金融機関と意見交換を行うにあたっては、金融機関が提供しているサービスの金融システムにおける重要度・市場シェア・利用者への影響等、その規模・特性に応じて、オペレジ確保に必要な対応や経営資源（ヒト・モノ・カネ）は異なることを十分に踏まえた議論を行う（すなわち、金融システムにおける重要度が相対的に小さい金融機関に対して、不必要に複雑な議論を求めるものではない）。従って、検査・監督において、本文書の個々の論点を形式的に適用したり、チェックリストとして用いたりするものではない。

本文書については、2022 年 12 月 16 日から 2023 年2月 16 日までの間、広く意見を募集した。コメントの概要及びそれに対する金融庁の考え方は、金融庁のウェブサイトで公表している[1]。今後も国際的な議論や実務等の進展も踏まえながら、金融機関や利用者をはじめとした幅広い関係者との間で議論を行い、金融庁による金融機関との対話の継続的な改善に努めていく。

[1] 金融庁（2023）「「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」（案）に対するパブリックコメントの結果等について」

II. オペレーショナル・レジリエンスを巡る議論・背景

1. 国際的な議論の動向

（1） バーゼル銀行監督委員会の国際原則

オペレジに関する国際原則として、バーゼル銀行監督委員会（BCBS：Basel Committee on Banking Supervision）が 2021 年3月 31 日に最終化した「オペレーショナル・レジリエンスのための諸原則」（以下、オペレジ原則）[2]及び「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」（以下、オペリスク原則）[3]がある。

両原則は、プリンシプル・ベースであり、他のバーゼル枠組みと同様、連結ベースで適用される。再建・処理計画（RRPs：Recovery and Resolution Plans）との整合性確保の観点はグローバルなシステム上重要な金融機関（G-SIFIs：Global Systemically Important Financial Institutions）等を対象とするが、その他の内容は G-SIFIs 以外についても比例原則の下での適用が想定される。

オペレジ原則は、7原則（ガバナンス、オペリスク管理、BCP とテスト、相互連関性の特定、サードパーティ依存度の管理、インシデント管理、サイバーを含む ICT セキュリティ対応）で構成される。原則2「オペリスク管理」についての詳細は、「オペリスク原則」によって規定されており、両原則を実質的に一体のものとして捉え、オペレジの実効性確保を進めていく必要がある。

このほか、金融安定理事会（FSB：Financial Stability Board）では、サードパーティ依存度や外部委託先の管理に関するディスカッション・ペーパー[4]を市中協議文書として公表し、金融機関一般がサードパーティリスク管理において直面している課題を整理している[5]。主な課題としては、技術やサービスのサプライチェーンの複雑性・不透明性、グローバルに活動する金融機関グル

---

[2] Basel Committee on Banking Supervision (BCBS) (2021a) "Principles for operational resilience"

[3] BCBS (2021b) "Revisions to the principles for the sound management of operational risk"

[4] Financial Stability Board (FSB) (2020) "Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Discussion paper"

[5] FSB (2021) "Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Overview of Responses to the Public Consultation"

ープ内のリスク管理の整合性、集中リスク、代替手段の確保、規制・監督や業態ごとの実務の断片化、データローカライゼーション、サイバーセキュリティ・データ保護、スキルを備えた人的資源の不足が挙げられている。こうした中、FSB の「2022 年の作業計画」[6]においてもオペレジの強化は重要事項とされており、具体的には、金融機関のサードパーティリスク管理に関する監督当局の目線や、用語・定義の統一化に関する議論が進展している。

また、証券監督者国際機構（IOSCO：International Organization of Securities Commissions）[7]においても、外部委託先の管理や、新型コロナウイルス感染症発生下で得られたオペレジの教訓に関して議論が進んでいる他、保険監督者国際機構（IAIS：International Association of Insurance Supervisors）もオペレジに関するイシューペーパー[8]を市中協議文書として公表している。

（2） 主要海外当局の動向

BCBS におけるオペレジ原則・オペリスク原則の最終化の検討に並行して、英・欧・米の監督当局よりオペレジに関する規制やガイダンスが示されている。各監督当局が使用する用語に細かい差異はあるものの、概念としては BCBS の国際原則と整合的なものとなっており、グローバルに活動する金融機関に対する規制・監督の断片化は避けるべきという共通認識がある。以下は、各国の動向の概要である。

先行する英国においては、2018 年7月に英当局が共同でディスカッション・ペーパー[9]を公表後、市中協議を経て 2021 年3月に最終化された新規制[10]を公表した（同時にサードパーティリスク管理にフォーカスした新規制[11]も公表した）。当該規制の実施スケジュールとしては、2022 年3月末から段階的に適

6 FSB (2022) “FSB Work Programme for 2022”
7 International Organization of Securities Commissions (IOSCO) (2021) “Principles on Outsourcing”
IOSCO (2022) “Operational resilience of trading venues and market intermediaries during the COVID-19 pandemic & lessons for future disruptions”
8 International Association of Insurance Supervisors (IAIS) (2022) “Issues Paper on Insurance Sector Operational Resilience”
9 Bank of England (BOE), Prudential Regulation Authority (PRA), and Financial Conduct Authority (FCA) (2018a) “Building the UK financial sector's operational resilience”
10 BOE, PRA, and FCA (2018b) “Operational resilience: Impact tolerances for important business services”
11 BOE and PRA (2021a) “Outsourcing and third party risk management”

用開始され（重要な業務の特定、耐性度の設定、必要な経営資源の特定、適切性の検証）、2025 年3月末までには検証の結果を踏まえた改善（必要な経営資源の追加投資など）が完了している必要がある。英当局は、第三国支店（例：邦銀ロンドン支店）に対しては、当該規制を直接適用せず、母国当局の監督レジーム（例：監督指針）の同等性評価により代替する方針である[12]。また、監督当局に重要なサードパーティを直接監督する権限を付与する法改正案が検討されており、関連して 2022 年7月に英当局共同でディスカッション・ペーパー[13]が公表されている。

欧州では、欧州委員会が 2020 年9月にオペレジに係る規制案（DORA：Digital Operational Resilience Act）[14]を公表し、市中協議を経て 2022 年5月に欧州連合理事会と欧州議会において組織間合意[15]に達した。英国の法改正案と同様、監督当局が重要なサードパーティ（ICT プロバイダ）を直接監督できるようになっている。

米国では、2020 年 10 月に米当局共同でガイダンス[16]を公表している。これは新たな規制を課すものではなく、規模が一定以上の銀行に適用される既存の規制やガイダンス、業界のスタンダードを包括的に取りまとめたものである。

12 BOE and PRA (2021b) “International banks: The PRA’s approach to branch and subsidiary supervision”
13 BOE, PRA, and FCA (2022) “Operational resilience: Critical third parties to the UK financial sector”
14 European Commission (EC) (2020) “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014”
15 Council of the European Union (2022) “Digital finance: Provisional agreement reached on DORA”
16 Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), and Federal Reserve Board (FRB) (2020) “Sound Practices to Strengthen Operational Resilience”

2. 国内外の環境変化

金融サービスにおけるテクノロジーの利用拡大は、利用者の利便性向上や、金融機関のコスト削減、業務効率化、イノベーションなど多くの便益をもたらしてきた一方、業務における IT システムへの依存度も高めてきた。

近年、不確実性の高い経営環境を背景に、IT システム開発のアプローチにも変化が見られている。従来の大規模システム開発においては、オンプレミス環境でウォーターフォール型開発方式[17]を採用し、システム開発を外部の IT ベンダー（システムインテグレーター）へ委託することが（とりわけ日本では）主流であった。もっとも、実際の取引量の変動に対して過剰投資や過少投資になりやすく、取引量が変化した際の迅速な対応に課題があったことから、現在は適材適所でクラウド環境やアジャイル開発方式を採用し、投資の適正化や、取引量の変化に対して迅速に対応することを通して、利用者のニーズにより沿ったアプローチを採用する動きも見られている。

こうした、利用者への価値提供の最適化を目指した業務プロセスの再構築は、新技術の利用に留まらず、社内のマネジメント手法や人事制度の変革、内製・外注の領域の再整理、FinTech 企業等とのサービス連携などを伴いうる。すなわち、デジタル化に伴う環境変化は、社内外の経営資源の相互連関性をより一層複雑化させる可能性がある。

金融サービスを利用者に提供し続けるために必要な社内の人員、設備、IT システム、社外のサードパーティ（外部委託先、サービス連携先、サービス利用先、調達先など）、フォースパーティ（サードパーティの再委託先など）の間の相互依存度が高まる中、金融機関が業務プロセス全体を見通して脆弱性を特定し、ある部分の障害や不具合がどの部分に波及するかを把握・管理すること――サードパーティリスク管理・フォースパーティリスク管理――は、国際的にも重要な課題と認識されている。

加えて、分散型台帳技術（DLT）を活用したイノベーションも進展している。例えば、証券トークン（デジタル証券）やステーブルコインの発行・流通プラットフォームによる証券決済インフラの効率化・安全化（T＋0決済）やポストトレード事務の標準化を目指す動きが金融機関や FMI で見られている。また、伝統的な資

[17] ウォーターフォール型開発では、要件定義・仕様、外部設計、内部設計、開発・システム実装、テスト、運用といった開発工程を順に進めていくのに対し、アジャイル開発では開発工程を小さな機能単位で繰り返し、段階的に機能をリリースし、利用者からのフィードバックを得ながら柔軟にニーズを反映することを目指す。

産のデジタル化・効率化のほかにも、資金決済法上の暗号資産、分散型金融（DeFi）、非代替性トークン（NFT）等に関連した新規事業（カストディ、マーケットプレイス等）も検討が進んでおり、金融機関が直面するリスクプロファイルはますます多様化しつつある。

新型コロナウイルス感染症（COVID-19）の感染拡大については、金融機関が BCP（業務継続計画）によって想定してきたシナリオ（新型インフルエンザ）に近いこともあり、これまでのところ、在宅勤務、時差出勤、フレックスタイム制、人員のスプリットなどの創意工夫が奏功し、金融サービス提供に大きな支障は生じていない。しかしながら、潜在的にはテレワーク等外部から内部への接続ニーズ（グループ企業やサードパーティによる接続を含む）が高まることで、外部から内部への侵入リスクも高まっている。ロシアによるウクライナ侵略を受け、サイバーセキュリティ上の脅威や地政学リスクの高まりについても、引き続き注意が必要である。

感染症以外にも、東日本大震災、多くの水害など、我が国は度重なる自然災害に直面してきた。今後も、南海トラフ巨大地震、首都直下地震、激甚化する水害による被害が想定される中、そのような危機時においても決済サービスなど金融システム上重要な業務を継続するために、冗長性の確保が課題となっている。こうした中、IT システムのメインセンタを首都圏に置いているインフラ企業が、バックアップセンタを首都圏から関西圏に移転する動きも見られている。

III. 金融機関に期待される役割

前述のとおり、環境が急速に変化し、不確実性が高い時代にあっては、従来のリスク管理（未然に事故や障害を防ぐための態勢整備）や、BCP（地震などの特定のリスク事象を想定した対応計画）では、想定外の事象が生じた場合に、金融システムにとって重要な業務を提供できないおそれがある。

このため、未然防止策を尽くしてもなお業務中断は必ず起こることを前提に、利用者目線に立ち、その影響を耐性度内に収めるための態勢整備が必要になる。すなわち、BCP のように事前にリスク事象を想定してその対策をまとめるといった従来のアプローチに留まらず、リスク環境の変化に適応し、想定外の事象にも対応するため、より能動的で、リバース・ストレステスト的なアプローチ（一定の業務中断が発生したと仮定して、当該業務中断という結果から原因を逆算し、どこに脆弱性が潜んでいるか、あるいは、どの程度の耐性度が確保できているかを検証するアプローチ）が求められる。

具体的には、様々な部署で分掌されている既存の枠組み（オペレーショナル・リスク管理、BCP、RRP、システムリスク管理、ITガバナンス、サイバーセキュリティ、サードパーティリスク管理、コンダクトリスク管理等）を活用しつつ、新たな視点から包括的に態勢を整備し、業務中断後の影響の軽減・早期復旧のために不可欠な社内外の経営資源が実際に確保されているかを検証する PDCA サイクルを回す必要がある。そのような包括的な枠組みが、オペレジの条件である。

とりわけ、縦割りの組織においては、個別の態勢整備だけでは、経営資源の配分に過不足が生じかねないところ、オペレジという視点を採用することにより、不必要なプロセスの合理化・廃止や、必要なプロセスへのヒト・モノ・カネの配分につなげていくことも期待される。

オペレジの基本動作ともいうべきポイントを整理すると、以下のとおり、①「重要な業務」を特定した上で、②業務中断後の金融システムや利用者への影響を一定の範囲内に収めるべく、重要な業務の最低限維持すべき水準（耐性度）を設定し、③社内外における業務プロセスの相互連関性のマッピングにより、必要な経営資源（ヒト・モノ・カネ）を確保し、④訓練・テスト等を通じて適切性を検証し、必要に応じて追加対応を実施するなど、定期的に見直し続けるという4点に集約される。

BOX1：オペレーショナル・リスク管理

オペレーショナル・リスク（以下、オペリスク）とは、金融機関の業務の過程、役職員の活動若しくはシステムが不適切であること、機能しないこと又は外生的な事象に

より損失が生じるリスクをいう。そして、オペレーショナル・リスク管理（以下、オペリスク管理）は、主要な商品や業務プロセス、システムに内在するオペリスクを特定し、評価し、把握し、管理し、かつ、削減・移転するための戦略を策定することをいう。

経営陣が、役職員の人事管理を含むオペリスク管理態勢の確立に主体的に関わり、定期的にその適切性を点検することは、オペレジの実効性確保にとっても重要な要素である。オペリスク管理態勢の確立のためには、オペレーションの実行部門（1線）、リスク管理部門（2線）、内部監査部門（3線）による3線防衛態勢等を用いつつ、十分に牽制機能が発揮されるよう、オペリスク管理に関する方針、報告・モニタリングの体制、役職員のインセンティブ設計、リスク管理と倫理規範に関する教育・研修体制を整備する必要がある。また、業務フローやオペリスク管理態勢に係る諸規程を明確に定める必要がある。

バーゼルⅢの自己資本比率規制（1柱）の枠組みでは、オペリスクは信用リスク・市場リスクと並ぶ主要なリスクカテゴリーの一つ[18]であり、オペリスク相当額は資金損益や役務損益から計算される事業規模要素に、過去 10 年間の内部損失の実績値から計算される内部損失乗数を掛け合わせることで算出される。金融機関は、オペリスクを正確かつ包括的に捕捉し、リスクが顕在化した際の損失を自己資本で吸収できるだけの財務の健全性を維持することに加えて、損失の原因を分析し再発防止策を策定するなど、オペリスクの削減にも取り組む必要がある。

もっとも、外部環境の変化により、これまで未然防止策を策定してこなかったような想定外の事象が生じたときには、オペリスク管理の枠組みだけで対応することは難しい。リスクの定量化についても、過去 10 年間の内部損失をバックワードルッキングに計測し、過去と同じような事象が同じような頻度で将来も起こり得るという仮定を置いている点には留意が必要である。この点、サイバー攻撃、人工知能（AI）・機械学習（ML）、暗号資産、気候変動など、新しい技術・環境変化に伴うリスクについては、バックワードルッキングなリスク計測では十分ではなく、フォワードルッキングな対応が必要との議論が国際的にも広まりつつある。

一般的に、変化が激しく、実務上のベストプラクティスも確立していない領域については、規制による画一的な対応ではフィージビリティに欠けるおそれや、過度な規制によりイノベーションを委縮させる可能性もあることから、監督による柔軟な対応が望ましい。オペレジという視点は、監督当局が金融機関のオペリスク管理をモニタリングし、その高度化を促していく上で、既存の枠組みを補完する側面もある。

[18] 2022 年３月末における銀行業態のオペレーショナル・リスクアセットは、25 兆円程度（リスクアセット全体に占める割合は５％程度）。

BOX2：システムリスク管理とサイバーセキュリティ

オペレジと不可分一体のオペリスク管理の重要な要素として、システムリスク管理やサイバーセキュリティがある。金融庁は、既にこれらの分野に関してディスカッション・ペーパーや詳細なレポートを公表している[19]。

とりわけ、サイバーセキュリティについては、外部委託の拡大等により、IT 資産管理が拡大し複雑化する中、安全性の高い IT 環境を維持するには、境界型セキュリティや特定のセキュリティ製品だけに依存することなく、風邪予防における手洗い、うがいなどの公衆衛生活動と同様に、IT 環境においても、例えば、IT 資産の適切な管理、速やかなセキュリティパッチ適用などの基本的な行動を組織全体に浸透させる取組（いわゆるサイバーハイジーン）を強化することが重要である。

また、サイバー攻撃が巧妙化する中、未然防止策に加えて、インシデント発生時の早期復旧や影響範囲の軽減を担保する枠組み（いわゆるサイバー・レジリエンス）も課題である。

オペレジの実効性確保のためには、こうしたシステムリスク管理やサイバーセキュリティのほか、自然災害時の業務継続も含めて、危機時の柔軟な対応や、平時からの経営資源の配分を行う必要がある。例えば、自社 ATM の故障により現金の受払ができなくなった場合には、システムの早期復旧自体も当然に重要であるものの、利用者目線では、迅速にウェブサイト、アプリ、SNS 上で障害状況や代替手段（他社 ATM やオンラインバンキング）が案内される広報もまた重要である。

オペレジの観点からは、利用者目線で、サービスの提供途絶の影響を極力一定の範囲内に収めることが重要である。

[19] 金融庁（2019）「金融機関の IT ガバナンスに関する対話のための論点・プラクティスの整理」
金融庁（2022a）「金融機関の IT ガバナンス等に関する調査結果レポート」
金融庁（2022b）「金融機関のシステム障害に関する分析レポート」
金融庁（2022c）「金融分野におけるサイバーセキュリティ強化に向けた取組方針（Ver. 3.0）」

1.「重要な業務」の特定

金融機関は「重要な業務」（Critical Operations）を特定する必要がある。**重要な業務とは、その中断が金融システムの安定や利用者の日常生活に著しい悪影響を生じさせるおそれのある金融サービスをいう。**

金融機関が重要な業務を特定する際には、利用者目線で、既存の BCP や RRP を活用することが想定される。具体的には、当該業務の中断又は不具合が金融システムの機能の維持に与える影響や、当該金融機関の規模、サービスの市場シェア・利用者数・利用頻度、当該金融機関の収益や市場での信認、他の金融機関による代替可能性等を考慮することが想定される。

例えば、既存の BCP の枠組み[20]において「金融システムの機能の維持にとって必要最低限の業務」として例示されている、インターバンク市場や銀行間決済システムを通じた大口・大量の決済の処理、個人に対する現金払出や送金依頼の受付、手形交換等は、重要な業務に該当しうる。

ちなみに、金融機関における BCP の取組状況[21]をみると、資金決済だけでなく、融資、市場シェアの著しく高いサービスなども、金融システムや利用者に与える影響が大きいことから、危機時においても業務継続の対象として選定されていることが多い。オペレジ上の重要な業務の検討を進める上でも、こうした既存の枠組みを活用することは有益である。

BOX3：業務継続計画（BCP）と再建・処理計画（RRP）

（業務継続計画（BCP））

金融機関は、危機発生時において、迅速な復旧対策を講じ、必要最低限の業務の継続を確保する等適切な対応を行うために業務継続体制（BCM：Business Continuity Management）を構築し、危機管理（CM：Crisis Management）マニュアル、及び業務継続計画（BCP：Business Continuity Plan）の策定等を平時から行う必要がある。

BCP はオペレジの重要な要素であり、BCP をベースにオペレジの検討を進めている金融機関も多い。もっとも、BCP については、以下のような特定の危機（特に地震）

20 金融庁（2023）「主要行等向けの総合的な監督指針」
21 日本銀行金融機構局（2015）「業務継続体制の整備状況に関するアンケート（2014 年 9 月）調査結果」

を想定した上で、個別の危機対応プロセスを整備するという側面が強くなる。

① 自然災害(地震、風水害、異常気象、伝染病等)
② テロ・戦争(国外において遭遇する場合を含む。)
③ 事故(大規模停電、システム障害等)
④ 風評(口コミ、インターネット、電子メール、憶測記事等)
⑤ 対企業犯罪(サイバー攻撃、脅迫、反社会的勢力の介入、データ盗難、役職員の誘拐等)
⑥ 営業上のトラブル(苦情・相談対応、データ入力ミス等)
⑦ 人事上のトラブル(役職員の事故・犯罪、内紛、セクシャルハラスメント等)
⑧ 労務上のトラブル(内部告発、過労死、職業病、人材流出等)

すなわち、リスク環境が急速に変化する中で、極端だが起こり得る想定外の事象が発生したときに BCP だけでは十分な対応ができないおそれがある。このため、BCP を含めた既存の枠組みの機能度を組織横断的かつ総合的に検証し、必要に応じて態勢を強化する包括な枠組み(オペレジ)が求められている。

また、危機時の対応計画である BCP の実効性を確保するためには、何らかの事象により業務が中断した際に、その影響を軽減し、初動対応や早期復旧を行うために必要な社内外の経営資源(ヒト・モノ・カネ)を特定し、実際に投資・配分する必要がある。ただ対応計画を策定するだけでなく、その適切性を検証し、経営資源の配分が十分でないことが判明した場合には、経営陣が必要な追加投資を意思決定することまでやり切って初めて、オペレジの確保につながる[22]。

なお、危機の種類(業務中断の原因)ごとに策定する従来型(原因事象型)の BCP をアップデートし、特定の危機のみを想定せず、業務中断という結果を前提に、初動対応や復旧対応の手順や代替手段を確保するオールハザード型(結果事象型)の BCP の検討を進めている先も見られる。こうしたオールハザード型の BCP のための実務上の対応は、オペレジと重なる部分もより一層多い。

[22] BCP の実効性を高めるために、事業影響度分析（BIA：Business Impact Analysis）を行うことも、オペレジの確保に貢献しうる。一般に、BIA では、企業は災害時に優先的に復旧すべき重要な業務を特定し、当該業務が中断したときのステークホルダーへの影響を踏まえて最大許容停止時間（MTPD：Maximum Tolerable Period of Disruption）や、それよりも短い目標復旧時間（RTO：Recovery Time Objective）を設定した上で、必要な経営資源を特定する。この際、目標復旧時間においてどの程度のレベル（水準）まで復旧させるかを目標復旧レベル（RLO：Recovery Level Objective）として設定したり、復旧の際に過去のどの時点のデータまで復旧させるかを目標復旧時点（RPO：Recovery Point Objective）として設定することもある。危機時においても最低限提供し続ける業務・サービスのレベル（水準）については、業務中断直後において目標復旧レベルと定義されるが、より長期的には最小事業継続目標 （MBCO：Minimum Business Continuity Objective）と定義される。

（再建・処理計画（RRP））

先般発生したグローバル金融危機の反省を踏まえて、グローバルなシステム上重要な金融機関（G-SIFIs：Global Systemically Important Financial Institutions）及び破綻時に金融システムの安定性に影響を及ぼす可能性があると母国当局によって判断された金融機関においては、堅牢かつ信頼性のある「再建・処理計画（RRPs：Recovery and Resolution Plans）」の整備が国際的に求められている。

RRP の目的は、世界規模で活動している巨大金融機関が無秩序に破綻すれば、各国の金融・経済システムに極めて深刻な悪影響（システミック・リスク）が生じることが予想されるために、これらを破綻させることができず、公的資金の注入によってかかる金融機関を救済せざるを得ないという、いわゆる「大きすぎて潰せない問題」（too big to fail）を解決することにある。金融機関は平時から、そもそも危機から破綻に至ることを防ぐための再建計画の策定のほか、破綻に至った場合の破綻処理可能性（resolvability）を高めるための態勢整備を求められる。具体的には、金融システムの著しい混乱を回避しつつ、当該金融機関が行う金融システム上重要な業務の継続性を確保し、納税者を損失の危険にさらすことなく、当該金融機関の破綻処理を行うことが実現可能であり、その信頼性が高い状態の確保が求められる。

RRP の策定において、金融機関はその中断又は混乱が、金融システムの安定に著しい悪影響を生じさせるおそれのある業務（クリティカル・ファンクション）を特定する必要がある[23]が、オペレジにおいても利用者目線で同様の作業が求められる。BCP と同様に、RRP をベースとしてオペレジの対象となる重要な業務の特定などの検討を進めている先も見られる。

[23] FSB (2013) “Guidance on Identification of Critical Functions and Critical Shared Services”

2.「耐性度」の設定

金融機関は、リスク選好度（リスクアペタイト）[24]を設定した上で、重要な業務と特定した金融サービスについて、未然防止策を尽くしてもなお、業務中断が必ず生じることを前提に最低限維持すべき水準を「耐性度」（Tolerance for disruption）として設定する必要がある。

耐性度は、典型的には BCP において設定する**業務中断時の目標復旧時間**（RTO：Recovery Time Objective）と重なるが、それ以外にも、**金融システムへの影響や利用者目線で生活への影響を一定の範囲内に収める観点から、業務中断が生じる範囲、影響を受ける取引数、取引額及び利用者数**（例えば、業務中断時の利用者からの苦情数）なども考慮要素となりうる。

既存の BCP の目標復旧時間については、「インターバンク市場や銀行間決済システムを通じた大口・大量の決済の処理等、特に重要な金融決済機能に係る業務については、当日中に再開する計画とされているか」[25]が最低ラインとなる。

この点、BCP の実務上は、危機時において最優先で復旧すべき資金決済・現金受払について「4時間以内」から「当日中」の目標復旧時間を設定している金融機関が多い[26]。オペレジ上の耐性度の検討を進める上でも、こうした既存の枠組みを活用することは有益である。

なお、金融システムや利用者の生活への影響を軽減することは、必ずしも自社のシステム復旧だけにこだわることを意味しない。システムの早期復旧自体も当然に重要であるものの、利用者目線では、迅速な代替手段の案内や広報もまた重要である。

もっとも、金融機関の多くが特定の代替手段に依存している状態では、広域災害により、当該代替手段も含めて業務中断してしまう可能性に留意が必要である（業界横断的な特定のサードパーティへの集中リスクの管理については、【BOX9：サードパーティリスク管理④（業界横断的な取組の強化）】参照）。

---

24 リスク選好度（リスクアペタイト）とは、自社の戦略目標や事業計画を実現するために、リスクキャパシティ（組織が許容できる最大のリスク量）の範囲内において、進んで受け入れるリスクの種類と総量をいう。

25 金融庁（2023）「主要行等向けの総合的な監督指針」

26 日本銀行金融機構局（2015）「業務継続体制の整備状況に関するアンケート（2014 年 9 月）調査結果」

BOX4：稼動目標（Service Level Objective）と耐性度（Tolerance for disruption）

金融機関の中には、どのようなサービスに利用者の需要があるのか予見しがたい不確実性の高い経営環境を背景に、取引量の変化に柔軟に対応しやすいクラウドを採用する先も見られる。こうしたクラウド環境上の金融サービスについて、その稼動目標（Service Level Objective）を高く設定すると、それだけコストもかかるトレードオフがあるため、利用者目線でより好ましいコストと利便性のバランスを模索する観点から、金融サービスごとに、その重要度に応じて稼動目標と稼動実績を公表している先も見られる。稼動目標については、可用性や停止時間の形で設定されることが想定される。

例えば、可用性 99.99%を 99.999%にしたときにコストが 10 倍になるとしたら、利用者はそのコストを負担してまで高い可用性を本当に望むのか、それとも多少はダウンタイム（停止時間）があったとしてもそれが許容できる範囲内なのであれば、むしろ低価格を選好するのか、あるいはアクセスの容易性などの別の利便性を重視するのか、というのがここでの論点である。このような論点については、正解を事前に予見することは不可能であり、企業が多種多様な金融サービスを実際に提供し、競争していく中で、市場によって事後的に発見されるものである。

こうした稼動目標は耐性度とは異なるが、利用者目線で金融サービスを提供し続けるという観点からは密接に関連する概念であると言える。

3. 相互連関性のマッピング・必要な経営資源の確保

金融機関は、**重要な業務の耐性度での提供に必要な社内外の経営資源（ヒト・モノ・カネ）を端から端まで（end to end の業務プロセス全体で）特定し、それらの相互連関性や相互依存度をマッピングする**必要がある。その上で、**必要なスキル・専門性を持った役職員を採用・配置し、適切な施設、システム、サードパーティ等を調達・確保し、保守・改善のための十分な投資を行う**必要がある。

なお、金融機関とサードパーティ等との相互連関性が複雑化している現状を踏まえ、金融機関が重要なサードパーティ等の利用状況について定期的に監督当局に報告・情報共有し、監督当局が特定のサードパーティに対する集中リスクを把握した上で、そのような重要なサードパーティとも対話を進めていくことが、金融システム全体のレジリエンスを確保する上で一定の意義があると考えられる。

BOX5：相互連関性のマッピングの範囲・粒度

金融機関が、重要な業務の最低限維持すべき水準（耐性度）での提供に必要な社内外の経営資源を特定し、それらの相互連関性や相互依存度をマッピングするにあたっては、その範囲や粒度が論点となる。

例えば、銀行の IT システムにおいては、勘定系、情報系、外部接続系、その他社内の窓口系など、様々なモジュールが複雑に絡み合って相互依存しており、CIO やCTO などの経営陣がそれらのシステム構成を把握していないと、ワーストシナリオとしてどのようなシステム障害が起こり得るか理解することは難しい。重要な業務の耐性度を設定するにあたり、こうした自社システム内のモジュール間の相互依存度を把握することは不可欠である。こうした相互依存性をシステム開発のテスト工程で十分に検証しきることが、システム障害を未然に防ぐ上で重要であることは言うまでもないが、収益環境が厳しい中、どうしてもコストやスケジュールが優先されてしまい、オペレジの実効性確保という点では不十分な例も散見されるのが現状である。

またシステム面だけでなく、オペレーション面での相互連関性のマッピングも必要である。まず、業務プロセス全体の中で、平時においてどの施設でどの部署のどのスキル・能力を持つ人員が何人必要か（専担が何人で、兼任が何人で、手作業に切り替える場合の BCP 要員は何人か）、危機時に IT システムが止まった場合には、バックアップセンタへの切替をどのような意思決定プロセスで行うか、そのために必要な経営資源を明文化することが前提になる。その上で、業務プロセスの中である部分の経営資源の欠如（被災による人員の欠如、施設の損壊、ハードウェアの故障

等）が、他の部分にどのように波及するかを平時から把握する必要がある。その際は、リバース・ストレステスト的なアプローチも有益である。

相互連関性のマッピングの実務上の課題となるのは、社外の経営資源についてである。金融サービスの提供には、社外のサードパーティ（外部委託先、サービス連携先、サービス利用先、調達先等）、フォースパーティ（サードパーティの再委託先等）との連携が不可欠である。国際的な議論では、重要なサードパーティとして、システム開発・運用を外部委託されている IT ベンダーや、サービス利用先であるクラウド事業者が挙げられることが多い。このほか、FinTech 企業が提供する外部サービスとの API 連携も進み、SMS 本人認証を行う外部連携先におけるシステム障害等も、モバイルアプリ利用者にとっては金融サービスの途絶をもたらす要因となりうる。通信や電力の途絶も業務継続に与える影響は甚大であり、通信回線の冗長化や、自家発電機の設置といった対応が取られている。サービス利用先としては、金融市場インフラ（例：日銀ネット、全銀システム）、現金輸送を担う警備保障会社も挙げられる。また、N 次委託先（再委託先、再々委託先、再々々委託先…）との相互連関性の把握も重要である。

マッピングの手法についても、様々な実務がありうる。業務プロセスのフローチャートを作成し、関連する経営資源を列挙することは基本的な手法である。このほか、IT システムのメインセンタ、バックアップセンタ、サードパーティの拠点を地図上でマッピングし、その集中度を可視化することで、地震、水害、感染症、テロ、戦争などの地理的な影響を見積もることも考えられる。

なお、こうした相互連関性のマッピングは、金融機関の経営陣がオペレジ確保のために必要な経営資源（ヒト・モノ・カネ）を特定するために行うものであり、その範囲や粒度はそれに必要な程度であればよいと考えられる。

BOX6：サードパーティリスク管理①（個別金融機関によるモニタリングの強化）

社内外の経営資源の相互連関性のマッピングにより、重要な業務の最低限維持すべき水準（耐性度）で提供するために重要なサードパーティを特定した後は、そのサービス品質を確認・維持することや、代替手段の確保、出口戦略の策定などの依存度の管理（サードパーティリスク管理[27]）が必要となる。

[27] BCBS (2021a) “Principles for operational resilience” の「サードパーティ依存度の管理（原則５）」においては、サードパーティリスクを当該サードパーティの業務中断が金融機関の「重要な業務」の提供に影響を与えるリスクとして定義し、当該サードパーティが金融機関と同等のオペレーショナル・レジリエンスが確保されているか検証すべきとしている。

とりわけ、特定のサードパーティへの集中リスクへの対応としては、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業界横断的な取組の強化に分類することができる。

現状においても、金融機関は IT ベンダーなどのサードパーティに対して契約締結前の情報取得・開示、業務中断時の適時・詳細な情報取得・開示、業務継続性やデータセキュリティの確保、訓練・テストの定期的な共同実施等を求めるなど、一定のモニタリングを行っている。特に、フォースパーティとの契約関係（再委託先やクラウドサービスの利用の有無）の確認は、再委託や再々委託による権限外の行為や情報漏洩などのリスクを軽減する上で重要である。このほか、金融機関側でも、不芳情報のチェック等や、潜在的なリスクの軽減策の策定も行われている。

もっとも、大規模な金融機関においては外部委託先だけでも数千先に及び、重要なサードパーティに絞っても数十先から数百先程度となることが想定される。こうした先全てについて、一律の基準を要求することは実務上困難であり、重要度やリスク評価の区分に応じたメリハリのあるモニタリングで対応せざるを得ない部分もある。

契約締結前の適切な情報取得という点では、サードパーティがどの程度までサービスのレベル（定義、範囲、内容、品質、ダウンタイムなど）を保証するかを明示した SLA（Service Level Agreement）を締結し、耐性度との整合性を図ることが重要である。例えば、クラウド事業者の SLA 上の可用性が 99.99%である場合には、当該インフラの上に乗る金融サービスの可用性はそれ以下にならざるを得ない。利用者目線で、どこまでの可用性が求められているのか、コストとの見合いでバランスを図る必要がある。

また、契約締結後のサービスのレベルを確認するためには、机上訓練や書面でのチェックリストや財務情報の確認のほか、ランサムウェア被害などの共通テストシナリオを設定した上での共同 BCP 訓練や、定期的な実地検査も考えられる。

もっとも、大手クラウド事業者に対しては、委託先の IT ベンダーと比べて、業務中断時に適時・詳細な情報開示に応じてもらうことが契約やセキュリティ上の理由で難しい場合もあるとの声も聞かれている。個別金融機関がいかにモニタリングを強化しようと努力しても、一定の水準までしか達することができないなど、統制に限界がある。

国際的な議論においても、大手クラウド事業者は、市場における寡占度や、勘定系システムのインフラとして採用された場合の重要な業務に与える影響が重大であることから、重要なサードパーティとして見なされることが多い。一つのクラウド事業者に利用が集中するリスクについては、当該事業者の障害が潜在的にシステミック・

リスクに波及しうるため、留意すべき課題の一つである。

個別金融機関によるモニタリング強化というアプローチの本質的な課題は、そもそも外部委託されている業務は自社の経営資源が十分でなかったり、効率的ではないと経営判断されたりしたからこそ外部委託されているのであり、外部委託先の業務を把握し、問題を検知し、対応できる人的資源を抱え続けるだけのインセンティブが欠如しやすい、という点である。こうしたインセンティブ構造を前提にすると、形式的には実地検査を行っていても、そもそも社内の人材にノウハウが無いため、モニタリングが形骸化していくおそれがある。

この点、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、地銀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が挙げられる。また、モニタリングの効率化・高度化に関する好事例として、銀行 OB・研究者・セキュリティコンサルタントで構成される第三者機関が日常的な牽制（例：規程類のチェックや BCP 訓練のシナリオについての助言）を図る事例も見られる。なお、個別金融機関がそれぞれ監査する非効率性を解消するために、外部監査により一括してモニタリングする方法としては、クラウドを含む委託業務の内部統制を対象とした SOC（Service Organization Control）報告書[28]の利用や、監査対象が SaaS である場合には「政府情報システムのためのセキュリティ評価制度（ISMAP）」[29]への登録状況が参考情報として利用される例も聞かれている。

このほか、金融情報システムセンター（FISC）が「金融機関等コンピュータシステムの安全対策基準・解説書」・「金融機関等におけるコンティンジェンシープラン策定のための手引書」を策定・改訂するなど、業界の自主的な取組も進展している。

BOX7：サードパーティリスク管理②（代替手段・出口戦略の確保）

金融機関が特定のサードパーティへの依存度を減らすために取り得るアプローチとしては、代替手段や出口戦略を確保することも考えられる。

この点、既に金融機関はシステム障害や自然災害等に備えて、クラウドに載せている業務ごとにどのような冗長構成を採用するかを決定している。例えば、勘定系

[28] ある特定の業務を企業（受託会社）が外部者から受託、提供する場合に、当該業務に係る受託会社における内部統制の有効性について、監査法人や公認会計士が独立した第三者の立場から客観的に検証した結果を記載した報告書。

[29] ISMAP（イスマップ）は、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度。内閣サイバーセキュリティセンター・デジタル庁・総務省・経済産業省が運営している。

システムをクラウド上に構築している銀行は、局所障害発生時のバックアップ（マルチゾーン）に加え、大規模障害 （広域災害時等） に対応するためのバックアップ（マルチリージョン、具体的には東阪体制）を採用している先もある。この際、可用性が求められる程度、コスト、サービスの速度（冗長性を高くするほど速度が低下する側面もある）間においてトレードオフがあるので、バランスを図る必要がある。

クラウド事業者レベルの冗長化例が、プラットフォームのマルチクラウド化（二つ以上のパブリッククラウドを組み合わせて利用する体制）である。もっとも、マルチクラウドはクラウドごとに異なる仕様に対してそれぞれ対応できる人員の育成・採用コストがボトルネックとなり、現状では困難との声が多く聞かれている。

このほか、地理的な集中リスクも課題である。日本においては、主要なクラウド事業者のサーバの拠点は、データセンタ内で従事するエンジニアを確保するために東京近郊にならざるを得ないが、その中でも災害リスクが比較的低い特定の立地は限られており、結果として地理的な集中が生じやすい構造がある。日本のどの場所も災害とは無縁ではないことは言うまでもない。なお、このような地理的な集中リスク（災害や感染症への脆弱性）については共同システムを運営する IT ベンダーにも当てはまる。

他方で、システムのオープン化やクラウドシフトに伴うリスクよりも、オープン化せず、クラウドを使わないことにより、外部環境の変化に取り残され、システムが劣化し続けるリスクについて留意すべきとの声も聞かれている。すなわち、金融機関がソフトウェアを活用して業務を行うにあたっては、技術や人材などの外部環境の変化に応じて定期的にシステムを更改し、品質の悪化を防ぐ必要がある。この点、一般的な仕様や公開された技術を用いたオープン系システムやシェアの高い大手クラウド事業者の運営するクラウドサービスは、汎用性や可搬性が高く、外部環境の変化に適応しやすいと評価する声も聞かれている。

BOX8：サードパーティリスク管理③（内製化）

金融機関が特定のサードパーティへの依存度を減らすために取り得るアプローチとしては、外部委託先の業務の内製化も考えられる。そもそも、重要な業務の耐性度での提供に必要な社内外の経営資源を特定するためには、一定のスキル・専門性を持った人材の判断を要する。ある程度専門人材を社内で確保しておくことは、オペレジの実効性確保のために不可欠である。

とりわけ、IT システム開発について自前で判断できる体制（コントローラビリティ）を確保することが重要である。具体的には、そもそも何を作るのか、ソフトウェアの設計

をどうするか、どの技術を使うか、どのサービス構成とするか、誰に開発（コーディング）してもらうかを金融機関が主体的に決定し、IT ベンダーから納品されたコードを見てその品質を判断・管理する必要がある。IT ベンダーに言われるがまま開発するというよりは、IT ベンダーに対しても対等にコミュニケーションができる状況になって初めて、自社のシステムをコントロールしたと言える。

一部の金融機関においては、コントローラビリティを確保するために、IT 人材の内製化を進めている。こうした先では、年功序列・メンバーシップ型の賃金体系では高度 IT 人材を採用できないとの問題意識のもと、本社と異なる人事制度を採用した子会社を設立し、年俸制、裁量労働制、フレックス、フルリモート可能、という条件で、IT 企業との採用競争に打ち勝ち、必要な人的資源を確保しようとしている。

このほか、いわゆるレガシーシステムの保守・運用にアサインされた若手エンジニアが、より市場価値の高い技術・スキルを磨ける IT 企業に転職してしまいがちであり、当該レガシーシステムを扱えるエンジニアの高齢化・定年退職とともに、システム更改ができる人材が社内にもベンダーにもいなくなる、という危機が迫っている。エンジニアの調達のしやすさという観点でシステムを採用することや、優秀なエンジニアを採用できる賃金体系・人事制度を用意することは、DX やイノベーション推進の文脈だけでなく、オペレジの実効性確保という文脈でも喫緊の課題である、との声も聞かれている。

なお、金融機関が IT システムの開発・運用を共同システムに外部委託することにも一長一短があり、プロパーIT 人材の採用・育成が困難になりやすい一方で、スケールメリット・コスト削減という経営戦略上の意義があることも事実である。また、BCP の実効性やシステムの安定性についても、単独ではコスト的に難しいバックアップセンタの設置を共同化によって実現するという点では貢献してきた。ベンダーへのモニタリングについても、共同実施することで効率化できた面もある。

BOX9：サードパーティリスク管理④（業界横断的な取組の強化）

個別の金融機関がサードパーティリスクの軽減を図るために取り得るアプローチとしては、①モニタリングの強化、②代替手段・出口戦略の確保、③内製化が考えられるが、いずれも効率性には課題がある。必要な人的資源・ノウハウが社内で枯渇している先については、実効性についても大きな課題がある。

また、個別の金融機関のオペレジの実効性確保（いわば、ミクロ・オペレーショナル・レジリエンス）という視点に加えて、個別の経済主体の合理的な行動がかえって金融システム全体の安定性を損なうような合成の誤謬にも目を向

ける必要がある。

例えば、大手サードパーティの提供するサービスへの利用が集中することは、個別の金融機関にとってはコスト削減や DX 推進といったメリットがあるものの、当該サードパーティのシステム障害や被災の影響がシステミック・リスクに波及しかねない、という点には留意すべきである[30]。個別の金融機関が金融システム上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ためには、クラウド事業者含めた IT ベンダー、FinTech 企業、金融市場インフラ、警備保障、通信、電力、その他重要なサードパーティを含めたエコシステム全体でのオペレジの実効性確保（いわば、マクロ・オペレーショナル・レジリエンス）もまた重要である。

こうした中、金融庁としても、金融機関に対するモニタリングを通じて、その委託先を捕捉し、委託に伴うリスクの理解・把握に努めてきた。また、金融機関のシステム障害発生時には、必要に応じ、システム開発・運営の委託先に対して銀行法に基づく報告徴求命令を発出することで、原因分析や再発防止策を把握し、サードパーティも含めたリスク管理態勢の適切性を確認してきた。さらに一歩進んで、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、金融庁としても対話を進めていくことに一定の意義があると考えられる。

海外の動向をみると、監督当局が金融機関からサードパーティ利用状況の報告を収集し、業態別や地域別にサードパーティ集中リスクを把握する実務が多くの主要国で採用されている[31]。とりわけ、英・欧においては、監督当局が重要なサードパーティを直接監督する新規制の導入を検討しており、個別金融機関がそれぞれサードパーティ集中リスクを独自に管理するよりも社会全体として効率的である可能性も指摘されている。また、グローバルに活動する大手クラウド事業者に対して、各法域の規制・監督が断片化することを避けるため、SWIFT（Society for Worldwide Interbank Financial Telecommunication）に対する協調オーバーサイトのように、主要国の監督当局が国際協調する枠組みの必要性も議論されている[32]。

---

30 Juan Carlos Crisanto, Johannes Ehrentraud, Marcos Fabian and Amélie Monteil(Financial Stability Institute of the Bank for InternationalSettlements) (2022) "Big tech interdependencies - a key policy blind spot"

31 BOE and PRA (2021a) "Outsourcing and third party risk management"
EBA (European Banking Authority) (2019) "Guidelines on outsourcing arrangements"
United States Congress (1982) "US Code Tittle 12 Chapter 18 Section 1867 (Bank Service Company Act)"

32 Jermy Prenio and Fernando Restoy (Financial Stability Institute of the Bank for

もっとも、監督当局における人的資源・ノウハウの確保という実務上の課題もある。また、一般的に、変化が激しく、実務上のベストプラクティスも確立していない領域については、規制による画一的な対応はイノベーションを委縮させる可能性もあることから、対話を通して民間のステークホルダーとともにベストプラクティスを探求していく柔軟なアプローチの方が望ましいと考えられる。

なお、金融システム全体のオペレジ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である。例えば、日本銀行では、3市場(短期金融市場、証券市場、外国為替市場)合同で市場レベル BCP 訓練[33]を定期的に実施している。この際、日本銀行金融市場局は短期金融市場の参加者からの要望に基づき、訓練を目的とする即日スタートの共通担保資金供給オペも実施し、災害時の業務フロー(例:東阪通信途絶時におけるバックアップ拠点からの資金供給オペの入札や資金繰り)を実際に確認できる機会を設けている。

このような業界横断的な訓練については、全国銀行協会などの業界団体が主催するものもあるが、俯瞰的な視点を持つ公的セクターが果たす役割も多いと考えられる。

BOX10:必要な人的資源確保のための人事制度(メンバーシップ型/ジョブ型)

オペレジでは、経営陣主導で外部環境の変化に応じて IT システムを改善し続け、現実的な耐性度を設定し、必要なヒト・モノ・カネが不足していたら追加投資を意思決定し、監督当局を含めたステークホルダーに対しても説明責任を果たしていくことが求められる。例えば、コードを読み書きできるレベルで自社システムを理解し、リスクを把握できる専門人材を CIO や CTO として配置し、その下で必要な高度 IT 人材を採用・育成することが考えられる。

もっとも、日本全体で高度 IT 人材が不足する中、必要な人的資源確保は容易ではない。専門性を有さない人材が CIO として配置されてしまう事例も見られ、一部では、目先のコスト削減が優先され、システム保守のための予算が十分に割り当てられず、結果として大規模なシステム障害の発生に至った事例も見られる。

経営陣が必要な経営資源の確保を怠ることは、一義的にはガバナンスの欠如が原因であるが、メンバーシップ型の人事制度が遠因ではないかと指摘する有識者の声もある。例えば、ジョブディスクリプション(職務記述書)及び職務遂行に必要なス

InternationalSettlements) (2022) "Safeguarding operational resilience: the macroprudential perspective"

[33] 日本銀行金融市場局 (2021)「市場レベル BCP・3市場合同訓練を実施」

キル・専門性を定義せずに、新規学卒者を一括採用して現場が OJT で育成するため、経営陣が業務遂行に必要な人的資源を明確に定義するという慣行がそもそも無い。また、定期人事異動により、数年で職務が変わるため専門性を育てづらいといった課題もある。

他方で、ジョブ型の人事制度では、労働者が遂行すべき職務（ジョブ）は雇用契約に明確に規定される。職務を特定して雇用するため、ジョブディスクリプションを定義したうえで、その職務を遂行できる人だけを採用する。このような人事制度は、経営陣が重要な業務の耐性度での提供に必要な経営資源を定義した上で、要件を満たす人員を採用・配置するというオペレジの考え方と親和性が高い。

もっとも、エンジニアを採用・育成しやすくするためにキャリアパス・報酬体系を見直す、という漸進的な取組を進めている先もあるため、現時点ではベストプラクティスを探求している段階の論点であると言える。

4. 適切性の検証・追加対応

金融機関は、**経営陣のコミットメントの下、極端だが起こり得るシナリオを想定した分析や訓練等を通じて、リスク選好度、重要な業務、耐性度、必要な経営資源に関する設定及び配分が適切であるかを定期的かつ組織横断的に検証し、必要に応じて見直しや追加的措置を講じる**必要がある。

典型的には、定期的な検証により特定した脆弱性に対して、ヒト・モノ・カネの追加投資を行うことが想定される。外部環境の変化に応じて、一度特定した重要な業務や耐性度も増減させる見直しもありうる。このほか、採用育成制度を含めた人事制度や企業文化の見直しも追加的措置に含まれ得る。

この点、オペリスク原則で規定される「リスク管理文化の醸成」（原則1）は、被害拡大につながりうる懸念材料や不具合を放置することなく、迅速に経営トップ・関連部署に報告（Bad News First）し、率直に意見交換して利用者目線で柔軟に危機対応する上で不可欠な要素である。例えば、「縦割りで、部署間や階層間の連携が悪い」、「ケアレスミスが頻発する」、「退職者・休職者が毎月のように出る」、「部下が育たず、上司がプレイング・マネージャー化する」、「経営企画部門は奮闘して毎年のように改革や組織再編はするも、現場は何も変わらない」、「結論ありきで大方針が決まるため、現場は忖度した情報しか上げてこない」といった風通しの悪い企業風土を放置していては、いくら追加的措置を講じても形骸化してしまい、オペレジの実効性確保につながらないおそれがある。

オペレジの実効性確保のためには、システムの開発・運用から、オペレーション、広報、代替手段の確保に至るまで、利用者目線で組織が部署間の縦割りを超えて協力し、社外のサードパーティとも連携し、早期復旧に向けた態勢整備と経営資源の配分の PDCA を回し続ける必要がある。こうした調整や協業を円滑に行うためには、異なる価値観・専門性・バックグラウンドを持つ人員・組織同士が、お互いの違い（多様性）を認め合い、相互理解を深めていく自由闊達な対話が不可欠である。

もっとも、様々な手法の中でベストプラクティスを探求している段階の論点であることには留意すべきである。どのようなインセンティブ設計や倫理規範、具体的行動が必要かについては、実務家も試行錯誤を繰り返しており、以下に例示するのはあくまでも参考事例である。

BOX11：リスク管理文化の醸成①（ジャストカルチャー）

実務上は、同じインフラ企業として他業界（航空・鉄道・医療）のリスク管理文化（ジャストカルチャー）を参考にする動きも見られている。

ヒューマンエラーをインシデントの原因として捉え、関与した特定の個人にペナルティ（減給・停職・再教育・告訴）を課す減点主義では、かえって現場の懸念や違和感などの潜在的なリスクに関する情報共有を委縮させ、危機時の初動対応も遅れかねない。むしろ、ヒューマンエラーを組織の問題（人員不足、教育不足、風通しの悪さ、部門間の連携の悪さ等）から生じた症状として捉え、当該インシデントやヒヤリハット（重大な災害や事故には至らなかったものの、直結してもおかしくない一歩手前の事例）を組織全体の学習・適応のための教訓として活用するべき、という人間工学の知見のもと、事務ミス発生時の担当者個人へのペナルティ・人事評価上の減点をあえて廃止した先も見られる。

事務ミスの隠蔽行為や、故意による内部不正に対しては、引き続きペナルティが必要であるものの、インシデントや懸念を報告した担当者個人に過度に責任を帰着させずに、現場が迅速・率直に上司や関連部署に報告するインセンティブを確保することは、オペリスクを正確かつ包括的に把握し、所要自己資本を正確に見積もって財務の健全性を維持する観点からも重要である。（【BOX1：オペレーショナル・リスク管理】参照）

BOX12：リスク管理文化の醸成②（心理的安全性）

迅速な情報共有・率直な意見交換が根付いているなど、健全で風通しの良い企業文化が醸成されているためには、職場環境として心理的安全性（一人ひとりが不安や不利益を感じることなく、率直に質問・発言・行動できる場の状況や雰囲気）が確保されていることも重要である。

一般に、ノルマ至上主義、心理的プレッシャー、不明瞭な指示、といった要素は職場の心理的安全性を損ない、利用者保護に違反する不正の遠因となりやすい。また、心理的安全性の欠如した企業文化は、組織間連携の欠如（いわゆるポテンヒット）にもつながりやすい。危機時においては、原因や利用者への影響を完全に把握できているわけではない不確実性のもとで、たとえ間違っていたとしても積極的・自発的に行動し、組織の縦割りを超えて声を上げ、利用者目線で連携して被害の拡大を防ぐ行為が褒められる企業文化やインセンティブ設計があるべきである。

もっとも、過度な減点主義が蔓延した組織においては、こうした積極的・自発的姿

勢は加点されず、間違いがあれば大きく減点されるため、現場の人員にとっては自発的に声を上げることの不利益・危険性が非常に高く、かえって何もしない選択の方が合理的となってしまう。危機時の組織間連携の実効性を確保する上でも、職場の心理的安全性は重要な要素と考えられる。

心理的安全性を確保し、風通しのよい企業風土を醸成するための具体的方法は様々である。一例として挙げられるのは、官民や業種を問わず導入が進んでいる「1on1ミーティング」（1on1）である。1on1は、マネージャーとメンバーが一対一で行う対話であり、一方的な指示・説教ではなく、メンバーの問題意識や違和感を掘り下げる質問・傾聴を通して、メンバーの主体性・自発性を育てることが期待されている。

このほか、2on2やトライアローグなど、煮詰まりやすい一対一の関係を第三者（オブザーバー）による傾聴とフィードバックによって解きほぐしていくコミュニケーション手法（リフレクティング・プロセス）も、官民で導入が進んでいる。一対一の関係だと権力勾配により、どうしても一方的に相手を評価してフィードバックする側と、忖度する側に分かれてしまい、フラットな意見交換が難しい面がある。異なる知識・前提・価値観、対立する利害関係を持つ人員同士が、あえて結論を急がずに、相互理解の前段階として、お互いがいかに違うかを深掘りしていく対話を通じて、縦割りを超えた連携につながることが期待される。

BOX13：コンプライアンス・リスク管理（コンダクトリスク管理）

オペレジと不可分一体のオペリスク管理と密接に関わる分野に、コンプライアンス・リスク管理（コンダクトリスク管理）がある。一般に、金融機関に期待されるコンダクトとは「利用者の正当かつ合理的な期待に応えることを金融機関がまず第一に自らの責務としてとらえて、利用者への対応や金融機関同士の行動や市場での活動で示すこと」である。また、利用者保護・市場の健全性・有効な競争に対して悪影響を及ぼす行為が行われるリスクをコンダクトリスクという。典型的には、LIBOR 不正などの市場操作、相場操縦、利益相反行為、インサイダー取引、顧客説明義務違反、適合性原則違反が挙げられる。

狭義のコンプライアンス・リスクは法令・規則違反を指すが、法令・規則に違反していなくても、社会規範に違反している場合にはコンダクトリスク（広義のコンプライアンス・リスク）に該当する。また、バーゼル規制上のオペリスクと異なり、自社において直接損失は発生しないが、利用者などの外部のステークホルダーに損失が発生する（自社にとってはレピュテーション・リスクの顕在化という形で間接的に損失が発生するにすぎない）場合にも、コンダクトリスクに該当する。

コンプライアンス・リスク管理（コンダクトリスク管理）の観点からは、収益至上主義あるいは権威主義（上意下達）の傾向を有する企業文化は利用者保護に違反する問題が生じやすく、健全で風通しの良い企業文化の醸成が求められる。オペレジにおいても、このようなリスク管理文化の醸成は重要な要素である。コンプライアンス・リスク管理（コンダクトリスク管理）の詳細について、金融庁は既にディスカッション・ペーパー[34]や事例や課題を整理した資料[35]を公表している。

[34] 金融庁（2018）「コンプライアンス・リスク管理に関する検査・監督の考え方と進め方（コンプライアンス・リスク管理基本方針）」
[35] 金融庁（2020）「コンプライアンス・リスク管理に関する傾向と課題」

IV. 今後の対話の進め方

各金融機関のオペレジ対応状況は、その業態や規模、リスク選好度、金融システム内における役割によって様々である。また、技術の発展や外部環境の変化によって、オペレジ確保に必要な実務や課題も変わり得ることが想定される。

従って、金融庁が金融機関と対話していくにあたっては、チェックリストの適用といった形式的な手法は用いない。むしろ、それぞれの金融機関の規模・特性も踏まえつつ、サーベイの実施や経営陣等との対話を通して足もとの取組状況や問題意識を丁寧に把握し、国際的な議論の進展も見据えつつ更なる取組を進めていく上での課題を特定していく。その上で、課題の解決に向けた好事例集の共有等を通じて、金融機関におけるベストプラクティスの探求を実質的に促していく。

金融庁では、金融システムの安定と金融サービスの利用者の保護・利便性確保の観点から、引き続き、金融機関を含めた幅広いステークホルダーや有識者と建設的な対話を継続し、国際的な議論の深化にも貢献していく。

以　上