バーゼル銀行監督委員会による「オペレーショナル・レジリエンスのための諸原則」の公表について

2021年5月

金融庁／日本銀行

＊当資料は、バーゼル銀行監督委員会の公表文書の内容への理解促進の一助として、作成されたものです。公表文書の内容については必ず原文を当たって御確認下さい。

目次

1. 概要

- バーゼル銀行監督委員会（バーゼル委）は、2021年3月31日に以下の２つの原則を公表した。

  ①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・レジリエンス諸原則）

  ②オペレーショナル・リスク管理のための諸原則

- 本資料はこのうち①オペ・レジリエンス諸原則について解説するもの。

2. オペレーショナル・レジリエンスの解説

オペレーショナル・レジリエンスとは何か

- オペレーショナル・レジリエンス（以下、オペ・レジリエンス）とは、テロやサイバー攻撃、自然災害等の発生時においても、銀行が重要な業務を継続できる能力を言う。

（1） 業務中断が起こり得ることを前提に、その影響が許容水準内に収まるよう態勢整備を求めるもの。

（2） BCP等の個別のプロセス整備だけではなく、業務中断による影響の軽減・緩和、初動・回復に繋げるキャパシティの確保等、包括的な検証と態勢整備を求めるもの。

（3） 想定する問題事象とその対策を纏めるといったリスク管理的アプローチだけでなく、失敗に至る原因を事前に想定し、因果関係を遡りながら脆弱性を除去するリバース・エンジニアリング的アプローチに基づくもの。

（4） 組織横断的な取り組みにあたり、経営陣のトップダウンによるコミットメントを求めるもの。

2. オペレーショナル・レジリエンスの解説

（1） なぜオペ・レジリエンスが必要か？

- ITシステムへの依存度の高まりやサイバー攻撃の増加、大規模システム障害やパンデミックの発生等、近年のオペレーショナル・リスク（以下、オペリスク）を取り巻く環境変化
- 業務プロセスの相互依存度、ひいては金融システム全体の相互連関性の高まり

⇒ これらを踏まえると、未然に事故や障害を「防ぐ」ための態勢整備だけでは不十分であるため。

- ✓ オペリスク管理を尽くしてなお、業務中断が発生し得る現実に向き合う必要がある。
- ✓ 非現実的な”zero tolerance”に拘泥するのではなく、現実的に甘受可能な許容水準を検討・設定することが重要。

2. オペレーショナル・レジリエンスの解説

（2） 既往のBCPで十分では？

- リスク環境がめまぐるしく変化する中、既存のBCP等の機能度を統合的かつ適時に検証・アップデートできる枠組みの整備が必要。

- すなわち、下記のような様々な部署／ラインで分掌している既存枠組みを包括的に検証できる不断のプロセスが必要。
  - サイバー・セキュリティを含むオペリスク管理
  - BCP、緊急時対応計画
  - 再建・破綻処理計画（RRP）
  - サードパーティ依存管理等

⇒ BCPや手順書等による個別の危機対応プロセスを都度、整備しても、リスク環境が変わり想定外の事象が起これば対応できない。

⇒ 業務中断による影響の軽減・緩和、初動・回復に繋げるキャパシティの確保等について、組織横断的かつ総合的な検証と態勢整備が必要。

2. オペレーショナル・レジリエンスの解説

（3） 具体的に何をすればよいのか？

- オペ・レジリエンス諸原則は、下記の取り組み等を通じた頑健性の向上を提唱するもの。
  - 「重要な業務」とその遂行に不可欠な経営資源※を特定する。またそれらの相互依存関係を整理する

    （※）人員・テクノロジー・プロセス・情報・施設等を想定
  - 重要な業務に関して、業務中断やその影響時の許容可能な水準※を設定する

    （※）業務中断の時間や範囲、影響を受ける取引数・取引額・顧客数等に対する水準を想定
  - シナリオ分析や訓練を通じて、上記水準が適切であるかを検証し、必要に応じ追加的措置を講じる
  - 以上を経営陣のコミットメントの下、組織横断的に反復継続する

⇒ 想定する問題事象とその対策を纏めるといった旧来のリスク管理的アプローチに基づきBCPを策定する現状に加えて、より動態的でリバース・エンジニアリング的なアプローチで補完

2. オペレーショナル・レジリエンスの解説

（4） 何をどこまで取組むべきか？

- オペ・レジリエンス諸原則は、当局が各金融機関に対して画一的な基準を押し付けることを提唱するものではない。

- 自行のビジネス・モデルや外部環境がめまぐるしく変化する中にあって、自行のリスク特性や金融システム全体の中での役割を勘案しつつ、どの程度の業務中断やその影響までなら甘受可能かという許容水準を自ら設定した上で、その達成状況を検証し、改善サイクルを回す態勢を確立する必要。

⇒ オペ・レジリエンスの期待水準に関しては、経営陣による組織横断的・包括的な検証、トップダウンによるコミットメントが求められている。

3. 諸原則のポイントと抄訳

- 7の原則を提示。
- プリンシプル・ベースの原則である旨を明記。
- 本原則は、オペリスク管理諸原則ほか既存のバーゼル文書を活用しつつ、統合的に適用されるべきものとしている。
- 本原則は他のバーゼル枠組みと同様、連結ベースで適用される。RRPとの整合性確保の観点はSIBsを対象とするが、その他の内容は比例原則の下で全金融機関に適用可能なもの。
- 「重要な業務」は銀行の性質や金融システムの中での役割を勘案して特定されるべきものとしている。

3. 諸原則のポイントと抄訳

市中協議の結果

- プリンシプル・ベースの原則である点等を踏まえ、本原則を支持する声が大半を占めた。
- 各国が既に発出している指針類等との平仄を取るべきとの指摘等を踏まえ、主として下記の点が修文された。
  - 許容水準に関する文言をめぐり、 市中協議段階で用いていた“risk tolerance for disruption”から“risk”を削る一方、“risk appetite”との併記は残し、リスク管理の枠組みを積極的に活用することを明示。
  - 各行において連結ベースで適用されるべき旨を明示。
  - サードパーティや関連会社との間で、オペ・レジリエンスの確保に関する措置を取り決めた書面契約（SLA等）の締結を求める記述を削除。

3. オペ・レジリエンス諸原則・抄訳

① ガバナンス	銀行は、業務中断時にも重要な業務の提供に及ぼす影響を最小限に抑えられるよう、既存の体制を活用し、オペ・レジリエンスに係る方針を確立、監督、実施すること。
② オペリスク管理	銀行は、オペリスク管理のための機能を応用することで、業務プロセス、人的資源、システムに対する組織内外の脅威や潜在的なリスクを常に把握すること。また、自行のオペ・レジリエンスに係る方針に沿って、重要な業務の脆弱性を速やかに評価し、リスクを管理すること。
③ BCPとテスト	銀行は、BCPを整備すること。また、深刻であるが起こり得るシナリオを想定した訓練を実施し、障害時でも重要な業務を継続できるか確認すること。
④ 相互連関性の特定	銀行は、重要な業務を特定したうえで、オペ・レジリエンスの方針に沿って、重要な業務の提供に係る組織内外の相互連関性や相互依存関係をマッピングすること。
⑤ サードパーティ依存度の管理	銀行は、重要な業務の提供に関わるサードパーティやグループ内組織への依存度を管理すること。
⑥ インシデント管理	銀行は、リスクのアペタイト（選好度）や許容度に沿って、重要な業務の提供を阻害しうるインシデントを管理するための初動・回復計画を策定・実施すること。また、実際に発生したインシデントからの教訓を踏まえて、同計画を継続的に更新していくこと。
⑦ サイバーを含むICTセキュリティ対応	銀行は、侵害の検知や防御、初動・回復プログラムにかかる、サイバー関連を含む頑健なICTセキュリティを確保すること。またこれらプログラムは定期的にテストされ、周囲の状況を適切に認識し、重要な業務をサポートするためのリスク管理や意思決定プロセスのための情報を提供するものでなければならない。