KPMG あずさ監査法人

金融機関の危機・RRPフェーズにおける訓練シナリオの追加検討

～サイバー攻撃シナリオの追加投入と流動性等への影響を踏まえた訓練実施～

金融機関の危機・RRPフェーズの訓練

▶ 危機対応の重要性

- ▶ 金融機関は、グローバルには約十年に一度の頻度で大きな財務危機・破綻イベントを経験している。
- ▶ 2009年のリーマンショックを契機とした世界的な金融危機を踏まえ、本邦・海外の当局は、G-SIBs等の大手金融機関に対して、再建・破綻処理計画（Recovery and Resolution Plan、RRP：注）の策定およびその態勢の整備・高度化を求めてきた。
  - 2023年の欧州G-SIBs間の救済合併や米国地銀の破綻を受けて、本邦・海外の当局は、引き続きRRPの高度化を要請している

▶ 訓練の実施

- ▶ 金融機関はRRPの態勢整備・高度化を行うなかで、危機・破綻シナリオを設定して訓練（シミュレーション）を行ってきた。特に、プレイブックと呼ばれる手順書（台本）に基づいて、態勢の実効性やガバナンス・レポーティングに焦点を当てた訓練を実施している。
- ▶ 米欧では、こうした訓練を2020年前後から行ってきたが、本邦では右の金融庁の監督指針（2024年）において危機・RRPフェーズにおける訓練の実施が要請された（訓練の詳細は次ページ参照）。
  - 本邦では、G-SIBs・D-SIBsにRRPに係る対応を求めている

▶ 金融庁の監督指針抜粋

III－11－8 秩序ある処理等の円滑な実施の確保に向けた態勢のテスティング

▶ III－11－8－1 意義

秩序ある処理等の円滑な実施のためには、平時から破綻処理準備態勢等を自己検証（テスティング）することにより、破綻処理の実効性を高めることが重要である。

▶ III－11－8－2 主な着眼点および監督手法・対応

① 本監督指針で金融機関に求められる破綻処理準備態勢等に基づいた危機時における実際の対応手順（例えば、再建計画の実行及び秩序ある処理等に係る金融機関内部の意思決定プロセスや当局・関係者等とのコミュニケーションプロセス等）をプレイブックとして文書化しているか。

② プレイブックに基づき、検証内容に応じて経営陣や海外拠点も含めたシミュレーション形式での演習等を実施したうえで、破綻処理準備態勢等の実行可能性について内部監査部門や第三者等を交えた効果的な検証を行い、その検証を通じて破綻処理準備態勢等の改善点を確認し、高度化を図るといった、いわゆるPDCAサイクルによる継続的な改善を図っているか。

注： 再建計画（Recovery Plan）は、金融機関の財務危機時に、予め策定したリカバリーオプション（有価証券ポートフォリオや事業の売却、貸出回収、子会社売却等）を実行して、資本や流動性を回復させるプロセス（計画）を指す。
破綻処理計画（Resolution Plan）は、金融機関が当局主導の下で秩序ある処理を行うことのできる計画を指す。
詳しくは、田中康浩・野﨑陽光「再建計画・破綻処理計画における訓練（テスティング）実施の重要性」を参照。

出所：金融庁「「主要行等向けの総合的な監督指針」および「金融商品取引業者等向けの総合的な監督指針」の一部改正（案）に対するパブリック・コメントの結果等の公表について」より抜粋
https://www.fsa.go.jp/news/r5/sonota/20240401/20240401.html

訓練のパターン

- 前ページで取り上げた訓練は、英語ではFire DrillやDry Run、Testing（テスティング）といった言葉で呼ばれることが多く、監督指針では「自己検証」と呼ばれているが、基本的にこれらは同じ概念である。
- 危機・RRPフェーズの訓練のパターンは、図表1の3つに分けられる。一般的に、簡易訓練は負担が軽く、マネジメントが参加する訓練であれば、訓練の計画や資料作成、関係部署の巻き込み等に数ヵ月の準備がかかることが想定され、負担が重くなる。実務部署の訓練の負担は、その中間になることが通常である。
- しかし、訓練のパターンに優劣があるわけではなく、金融機関が考える問題意識や課題認識に沿って、適切な訓練を選択・計画することが重要になる。

図表1 訓練のパターン

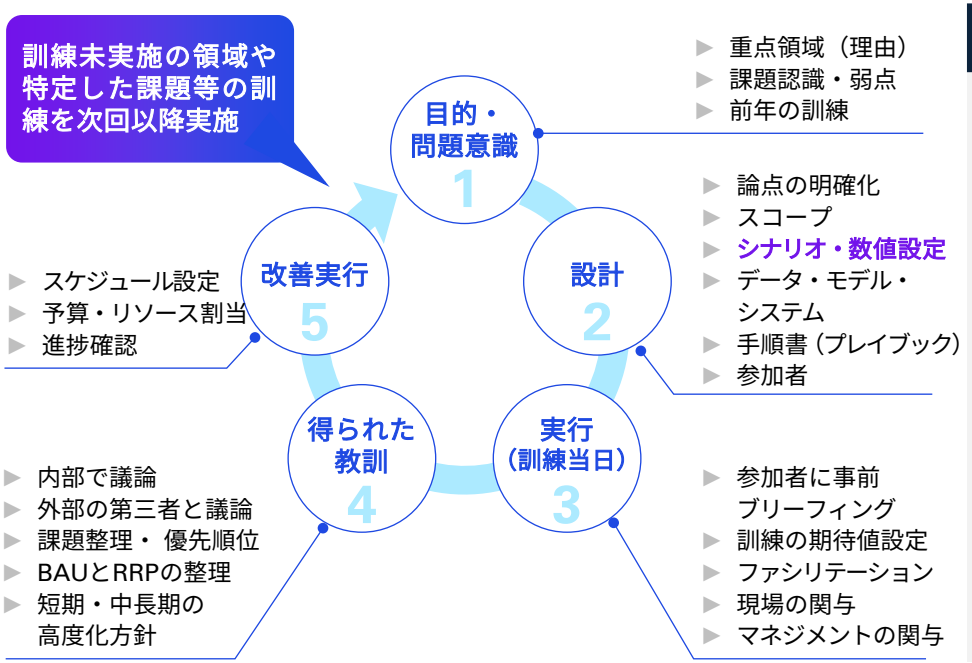
簡易訓練	実務部署の訓練	マネジメントが参加する訓練
策定しているプレイブックやマニュアルの確認・レビュー（机上訓練中心）	プレイブックやマニュアル（の一部）について、現場の部署・担当者が実務やオペレーションを確認・実施する	マネジメントの判断が求められる実務にフォーカスして、プレイブック等を用いながら、意思決定を行う

出所：田中康浩・野﨑陽光「再建計画・破綻処理計画における訓練（テスティング）実施の重要性」を基にKPMGジャパン作成

訓練の流れと設定するシナリオ

- 訓練のサイクルは、図表2のとおりである。このサイクルに基づいて、危機・RRPフェーズに係る自社のリスク管理の実効性やガバナンス・レポーティング態勢を確認し、課題や教訓を特定のうえ、訓練未実施の領域や特定した課題に関する訓練を次回以降実施することが大切になる。
- 図表2の訓練のサイクルのなかで、「シナリオ・数値設定」は特に重要である。金融機関の危機・RRPフェーズの訓練では、景気後退シナリオや固有シナリオ、それらを合わせた複合シナリオを想定することが一般的である（図表3）。

図表2 訓練のサイクル



出所：田中康浩・宇都健太郎・高縁友香「グローバルに要請が強まる「再建・破綻処理計画」の実行性向上」を基にKPMGジャパン作成

図表3 訓練におけるシナリオの例

景気後退シナリオ	固有シナリオ	複合シナリオ
景気後退 • 米国の景気後退 • グローバルで金利急上昇 • 金融危機 **コロナ禍** • 世界的な生産活動停止 **地政学リスク** • 原油価格の暴騰	**格下げ・損失** • 格下げ • 個別取引に紐づく大規模損失 **コンプライアンス** • マネロン事案が発生し、巨額制裁金 • レピュテーショナルリスクの顕在化に伴い預金流出 **その他** • 大災害による固定資産の大規模損失	景気後退シナリオをベースに、固有シナリオを考慮。「複合」という意味では、最も厳しいシナリオになることが一般的

出所：KPMGジャパン作成

サイバーリスク管理の重要性

- 最近、注目が特に高まっているサイバーリスクについては、本邦・海外当局では以下のような取組みがなされている（図表4）。
  - ECB「サイバーレジリエンスストレステスト」でも触れられているとおり、地政学的な緊張の高まりや金融セクターにおけるデジタライゼーションの進展に伴い、サイバーリスクへの備えは極めて重要になっている
- サイバーリスクに係る訓練は、レッドチーム（攻撃側）とブルーチーム（防御側）に分かれてペネトレーションテスト（TLPT）を実施するなどの訓練が行われている。
- 一方、金融機関の危機・RRPフェーズの訓練では、専ら前ページの図表3のような財務リスクの顕在化に関連するシナリオを想定することがほとんどであり、サイバー攻撃をシナリオとして設定することはない。

図表4 本邦・海外当局の取組み例

金融庁「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）

- **概要：**金融庁のサイバーセキュリティに係る基本的な考え方やサイバーセキュリティ管理態勢、経営陣の関与・理解等、金融機関に求められる取組みを説明
- **適用対象：**主要行等、中小・地域金融機関、証券会社、保険会社、清算・振替機関等の幅広い金融機関
- **サイバーセキュリティ管理態勢：**金融機関に求められるサイバーセキュリティの管理態勢を、以下6つのカテゴリーに分けて説明している
  - ① サイバーセキュリティ管理態勢の構築
  - ② サイバーセキュリティリスクの特定
  - ③ サイバー攻撃の防御
  - ④ サイバー攻撃の検知
  - ⑤ サイバーインシデント対応及び復旧
  - ⑥ サードパーティリスク管理

  加えて、金融庁と関係機関の連携強化の必要性についても触れている
- **財務リスクの言及：**特になし

出所： 金融庁「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」
https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdfを基にKPMGジャパン作成

ECB「サイバーレジリエンスストレステスト」（2024）

- **概要：**今後発生しうる深刻なサイバーインシデントの顕在化を踏まえて、金融機関の対応や回復能力を評価するためにストレステストを実施
- **対象：**ECBの監督下にある109の金融機関
  - 対象金融機関は質問票への回答やドキュメントの提出が求められた
  - 109の金融機関のうち、サンプルとして選定された28の金融機関については、より強度の高いテスト（IT回復テストやオンサイト検査等）が求められた
- **シナリオ：**すべての予防措置が失敗し、金融機関のコアシステムのデータベースがサイバー攻撃の影響を受けた状況を想定（サイバー攻撃を事前に防ぐ能力をテストするものではない）
- **評価：**全体としてサイバーインシデントに対する対応や回復能力が示されたが、改善を要する分野も存在。教訓は、監督レビュー評価プロセス（SREP）で活用
- **財務リスクの言及：**本テストは資本の充分性を評価するものではない（監督上の第2の柱に影響しない）。一方で、サイバー攻撃による直接・間接的な損失の推計は重要な論点と指摘

出所：ECB「ECB concludes cyber resilience stress test」を基にKPMGジャパン作成

危機・RRPフェーズのサイバー攻撃シナリオ

訓練の基本的な考え方

RRP　サイバー（TLPT）　不祥事案（SNS）　BCP（災害）　・・・

- 各リスク・イベント単体で実施されることが多い
- 例えば、危機・RRPフェーズの訓練の中で、サイバー攻撃シナリオを考慮することはない

サイバーリスク顕在化による財務への影響

“金融機関が危機に陥っている際にサイバー攻撃が発生すると、流動性等の財務に与える影響は、流動性ニーズに対する反応や資産の投げ売り、資産価格のさらなる下落等を通じて、より甚大になり得る”（右のECBペーパー指摘）

危機・RRPフェーズであるからこそ、**サイバー攻撃を加味した訓練**を実施することに意義がある

危機・RRPフェーズの訓練におけるシナリオの再検討

本稿では、サイバー攻撃と金融機関の財務（流動性）への連関性について触れているペーパーをサーベイし、波及経路を理解する。そのうえで、危機・RRPフェーズの訓練のなかで、サイバー攻撃を追加的に考慮する訓練について提案する

ペーパー① ECB：
Cyber resilience stress testing from a macroprudential perspective
（2025年3月公表、P7-8）

ペーパー② IMF：
Using Simulations for Cyber Stress Testing Exercises
（2025年5月公表、P9）

訓練におけるシナリオ例

景気後退局面で金融危機が発生するなか、**リカバリーオプションの実行**と**財務の回復を行う**必要がある。その過程で**サイバー攻撃**を受け、**追加的な流動性の悪化、システム復旧までの業務制約、復旧のための追加リソースの確保**等、**より厳しくかつ複雑な制約**があるなかで、リカバリーオプションを実行し財務を回復しなければならない

- 金融機関が危機・破綻に至るシナリオとしては、流動性危機の顕在化が最も警戒すべきものと考えられる（2023年のグローバルでのイベントからの示唆）
- 上記ペーパー①・②は、サイバー攻撃による流動性への波及経路を整理しており、通常のストレステストでも参考になる

ペーパー①のポイント

■ 2025年に入り、海外当局からサイバーリスクの顕在化と流動性への波及に焦点を当てたペーパーが複数公表されている。
- ▶ サイバー攻撃の際に金融機関の財務等に影響を与える波及チャネルを示し、サイバーリスクの顕在化と流動性危機との関連性を整理してサイバーストレステストを実施している（ペーパー①は、規制・監督上のツールとして提唱するものではない点に留意）
- ▶ 具体的には図表5のとおり、オペレーション、金融システム、コンフィデンスの3つを波及チャネルとして取り上げている

図表5 サイバーリスクとその波及チャネル

波及チャネル	経路	事例
オペレーション	インフラの相互依存性や少数のサードパーティプロバイダーが提供する重要なソフトウェアを通じて波及	金融取引サービスグループを標的としたランサムウェア攻撃で、米国およびEUの市場参加者が影響を受け、**流動性リスクが顕在化**
金融システム	金融機関間の財務に関する相互連関性を通じて波及	ある金融機関のITシステムがランサムウェア攻撃で麻痺。取引処理や短期国債市場を混乱させ、**流動性リスクが顕在化**
コンフィデンス	システムの一時的な遮断やデータ漏洩が顧客のコンフィデンス喪失を通じて波及	**投げ売り**や**取り付け騒ぎ（バンク・ラン）**が発生し、それらが相乗作業をもたらす**「サイバー・ラン」**に発展

出所：ペーパー①を基にKPMGジャパン作成

- ▶ サイバーストレステストを実施する際には、上記の波及チャネルを考慮のうえ、トップダウンアプローチとボトムアップアプローチの手法が取られる。トップダウンアプローチは金融システムの「全体像」を捉え、ボトムアップアプローチはテスト対象の金融機関の「個別の影響」を明らかにするもの。本ペーパーでは両者を組み合わせることで、より包括的なテストを可能とし、リスク評価もより精緻になるとしている（一方で、金融機関の訓練では、ボトムアップアプローチが中心になると思われる）。
  - トップダウンアプローチ：中央銀行や監督当局が、金融システム全体の視点からモデルを構築し、システム全体の相互連関、行動反応、二次的影響などを分析
  - ボトムアップアプローチ：個々の金融機関が自らのリスク評価やストレステストを実施し、その結果に基づいて健全性を評価

ペーパー①のポイント

▶ ペーパー①では、サイバーストレステストを実施する際に検討すべき点として、以下の6原則を提案している

図表6 サイバーストレステストを実施する際の原則

1	2	3	4	5	6
目的の明確化	対象範囲の明確化	波及チャネルの特定	テールリスクに焦点を当てる	反応の考慮	トップダウン／ボトムアップの両アプローチの結果の補完的な使用
ストレステストの目的を明確にする（資本要件に焦点を当てるのではなく、脆弱性の特定や政策対応の検討などのテストの目的に焦点を当てる）。	サイバー攻撃の影響を受ける範囲（対象金融機関や金融市場インフラなど）を明確にする。	サイバー攻撃がどのように金融システムに波及するか（例：オペレーション停止、信頼喪失など）を分析。	統計分布の「端（テール）」に位置する、発生確率は低いが発生した場合の影響が極めて大きい「テールリスク」に注目する。	金融機関や市場参加者がサイバー攻撃にどのように反応するか（例：資産売却、流動性確保など）をモデルに組み込む。	金融システムの全体像とテスト対象の個別の金融機関をそれぞれ見るアプローチを組み合わせることで、より包括的な分析を実現する。

出所：ペーパー①を基にKPMGジャパン作成

ペーパー②のポイント

■ 2025年に入り、海外当局からサイバーリスクの顕在化と流動性への波及に焦点を当てたペーパーが複数公表されている。
（ペーパー②も、規制・監督上のツールとして提唱するものではない点に留意）
▶ ペーパー②では、図表7のような5つのシナリオを設定し、サイバーリスクの顕在化に伴う決済や流動性への影響をシミュレーションしている

図表7 主なシナリオと影響

	シナリオ	概要	前提	結果
01	ベースライン（通常状態）	大口決済システム（LVPS）は通常通り稼働。中央銀行からの流動性供給も変化なし	（他のシナリオとの比較基準として使用）	ー
02	システム上重要な金融機関への攻撃	大手金融機関がDDoS攻撃を受け、4時間にわたり送金不能に。他の金融機関は、影響を受けた金融機関への送金を締切2時間前に停止	• セキュリティ対策（パスワード、マルウェア対策など）が不十分 • 多層防御アプローチに欠陥	✓ **流動性リスク**が高まり、決済遅延が発生。金融機関が送金不能状態に陥ることによる**流動性悪化のストレスケース**を試算 ✓ サイバーリスクの顕在化が、**流動性を含む深刻な財務リスク**に直結しかねない事を示唆
03	重要なサービスプロバイダー（CSP）への攻撃	5大金融機関にITサービスを提供するCSPが攻撃を受け、4時間にわたり支払い指示不能に	• ランサムウェアによるデータ改ざん • CSPへの依存度が高く、監査体制が不十分	✓ 複数の銀行が同時に影響を受け、未決済の支払いが多数発生 ✓ **金融システムの流動性に深刻な影響**を与えることを示唆
04	中央銀行が内部脅威によって侵害	中央銀行のLVPSが元職員による内部攻撃を受け、10時間の停止。手動処理で一部対応し、深夜まで延長運転	• アクセス権の管理が不十分 • 退職者による不正アクセス	重大な停止にも関わらず、手動処理と延長運転により回復
05	外国為替決済システムへの深刻な持続的脅威	クロスボーダーFX決済システムが攻撃を受け、5時間停止。全金融機関が支払い指示送受信不能に	• ランサムウェアによるデータ改ざん • FX決済の代替手段がなく、金融機関が依存	決済遅延はあるが、システムは回復

出所：ペーパー②を基にKPMGジャパン作成

危機・RRPフェーズにおけるサイバー攻撃の影響

- サイバー攻撃を加味した危機・RRPフェーズの訓練を行ううえで、図表8のような金融機関を取り巻くマクロの状況や個社へのミクロの影響を踏まえた訓練を実施することが考えられる。
  - 例1：通常のRRPの訓練よりも、一層厳しい流動性へのインパクトを想定してリカバリーオプションの実行を検討する
  - 例2：サイバー攻撃を受けたシステムの復旧状況に応じて、実行可能なリカバリーオプションの取捨選択を行う

図表8 金融機関を取り巻く状況と影響

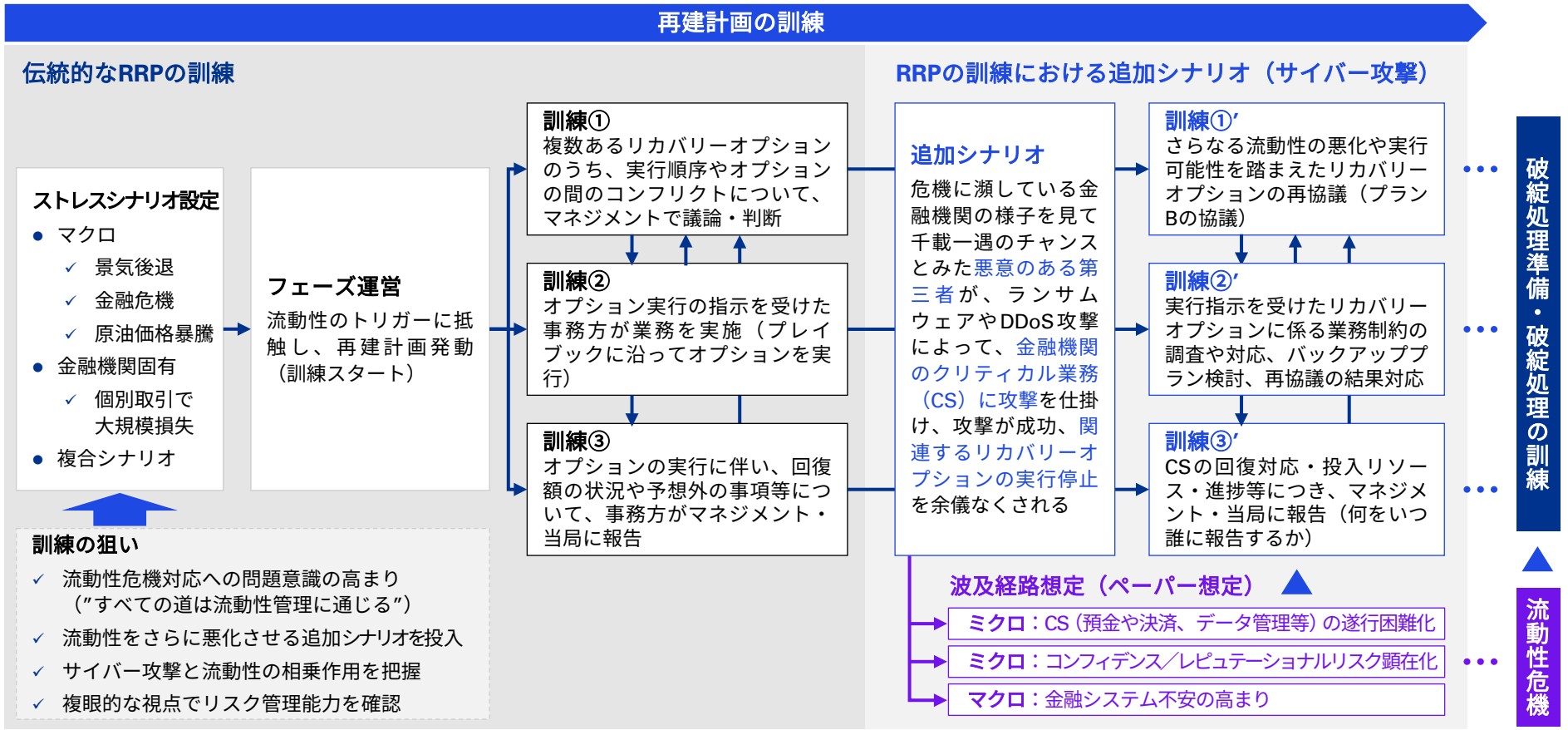
影響範囲	金融機関を取り巻く状況	金融機関への影響
マクロ	• サイバー攻撃により金融市場が混乱し、金融システムが不安定化 • 金融システムの不安定化による投げ売りや株価暴落が発生 • 低流動性資産については、流動性が枯渇し、売却不能に	✓ ビジネスポジションや事業売却が、想定以上の安値で執行せざるを得ない ✓ 低流動性資産については、買い手がつかず売却できない ✓ リカバリーオプションを実行するも、**想定通りに財務が回復しない**
マクロ	• 当局が介入 • 金融市場の安定化のため各種施策を実施	✓ 当局による介入で市場が沈静化するも、時間を要する ✓ その間、当局による各種オペレーションなども模索 ✓ サイバー攻撃からの回復や流動性の状況について、**当局に報告**が必要
ミクロ	• サイバー攻撃により、自社のオペレーションが停止（データにアクセスできない、評価システムが機能しない、など） • クリティカル業務（CS）の停止（決済不能など）	✓ オペレーション停止により、**リカバリーオプションを実行できない** ✓ その結果、急速に**財務状況が悪化（資本、特に流動性）**
ミクロ	• データ漏洩などによる顧客離れ、新規契約停止・取引縮小 • 財務健全性の低下による格下げや自社の株価暴落 • 格下げに伴い早期解約条項抵触、大量の解約が発生	✓ 急速な**財務状況の悪化（資本、特に流動性）** ✓ 予期せぬ解約のため、**資金流出が加速（流動性枯渇）**
ミクロ	• サイバー攻撃の復旧作業を実施	✓ バックアッププランによる**データ復旧**、オペレーションの実行試行 ✓ **サイバー攻撃**を受けたシステムの**復旧進捗**を見ながら、業務継続や**リカバリーオプションを実行** ✓ 復旧作業にリソースが必要（**危機・RRP対応とのバランス**）

出所：KPMGジャパン作成

サイバー攻撃を加味した訓練の例

■ 以上を踏まえると、例えば以下のようなサイバー攻撃を加味したシナリオに基づく危機・RRPフェーズの訓練を行うことが一案である。
  ► 訓練で得られた教訓は、RRP対応とオペレーショナル／サイバーレジリエンス対応の両方で活かすと、訓練のよい振り返りになる

図表9 訓練の例



出所：KPMGジャパン作成

危機・RRPフェーズにおける訓練シナリオの追加検討

01

- 金融機関は危機・RRPフェーズに関わらず、これまでさまざまな訓練を実施してきたが、リスク領域が複数にまたがる形での訓練の実施は少ない。
- 危機・RRPフェーズの財務リスクに焦点を当てた訓練でも、例えば資本と流動性の連関性を意識した訓練は行われてこなかった（最近になって、これらの相乗作用を意識した訓練が行われている状況）。

02

- サイバーリスクについては年々注目が高まっている。金融機関のストレステストでも、サイバー攻撃が財務（流動性）に与える影響について、複数のペーパーが公表されている。
- サイバー攻撃を行う者にとっても、金融機関が危機を迎えている時こそ、攻撃が最も効果的になるという意味で、攻撃すべきタイミングとして危機・RRPフェーズは合理的である。

03

- こうしたことを踏まえると、本邦の金融機関においても、危機・RRPフェーズにおいて、サイバー攻撃シナリオを追加的に投入し、訓練を実施することには意義があると思われる。
- 訓練を通じて、財務リスクのみならず、サイバー攻撃やオペレーショナル／サイバーレジリエンスの観点から管理態勢を見直し、整備・高度化を行っていくことは重要だろう。

04

- 本稿では、危機・RRPフェーズの訓練において流動性と関連の深いサイバー攻撃シナリオを追加的に組み込んだが、ほかの追加シナリオ（SNSを起点にしたデジタル・バンク・ランの顕在化等）を考えてもよいだろう。
- 本邦金融機関には、「危機対応において、リスクは多層的に発生しうる」という前提に立ち、複眼的な視点での訓練実施やリスク管理能力の向上を求めたい。