プログレス・ウェビナー

オペレーショナルレジリエンス・BCP の実践ポイント

2026年3月19日（木）
PwC Japan有限責任監査法人
早道友詩・小平秀明

Agenda

1. オペレーショナルレジリエンスが求められる背景
2. 内外の監督当局の動向と期待事項
3. オペレーショナルレジリエンス概要
4. オペレーショナルレジリエンスを考慮したBCP/BCM
5. BCP/BCMの取り組み

※ 本講義内容に含まれる意見は講師の私見であり、PwCおよび所属部門の正式見解ではありません。

1

オペレーショナルレジリエンスが求められる背景

金融機関のビジネスやステークホルダーを脅かす危機事象（1/2）

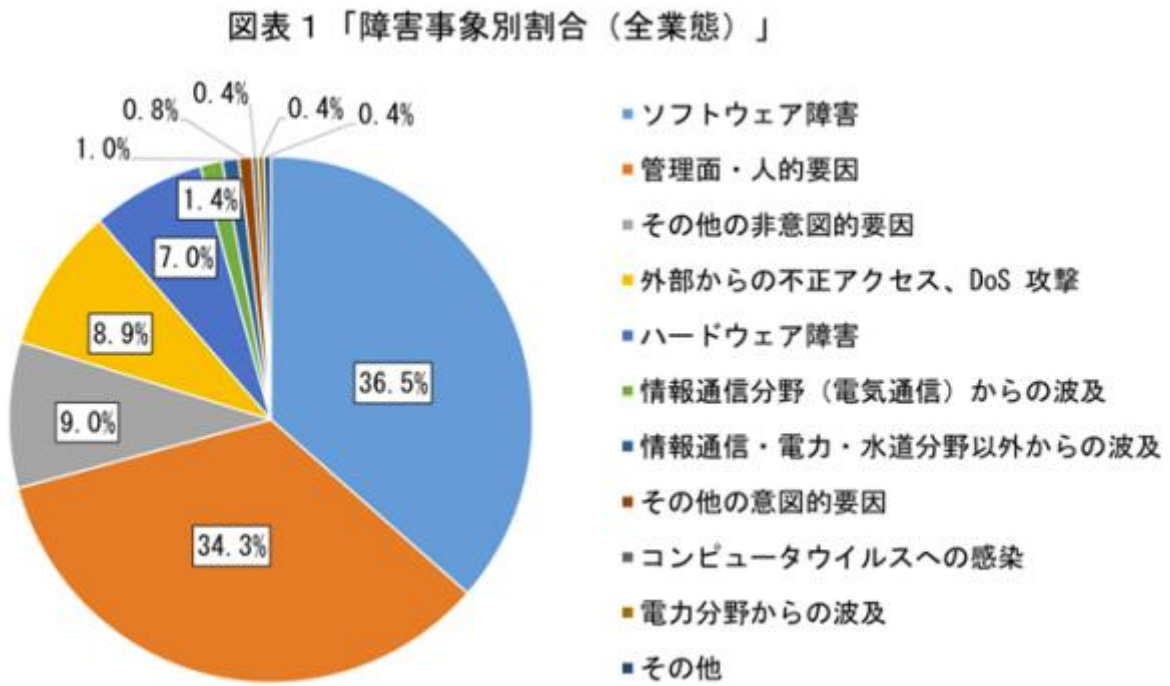
近年、金融機関は、ビジネスの多角化に向けたオペレーティングモデルの変更や外部依存、積極的なグローバル進出を推し進めています。ビジネス・オペレーティングモデルや展開する地域が変容する中で、危機事象に対する組織的な対応能力とその持続可能性がステークホルダーより求められています。

金融機関のビジネスやステークホルダーを脅かす危機事象（2/2）

- 金融庁が2025年6月に公表した「金融分野におけるITレジリエンスに関する分析レポート」によると、2024年度に金融機関から報告を受けたITシステム障害の 件数は約1,800件です。
- レポートにおいては、従来型のソフトウェア障害や、人的要因に加え、サイバー観点での事案を主な障害として挙げています。
- 防御策だけではなく、インシデント発生時の顧客目線での対応、影響の最小化、重要業務の早期復旧等を実現させるための態勢整備等を求められています。

障害事象別割合（全業態）

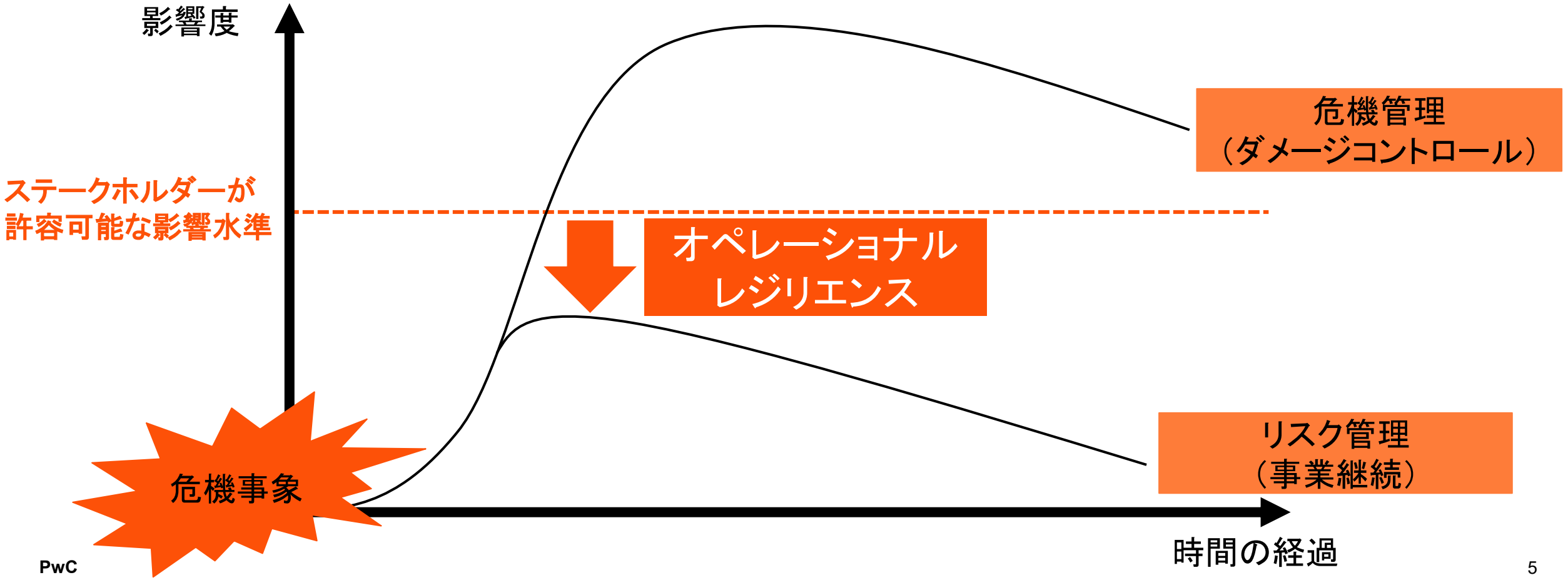
【出所】
金融庁, 2025『金融分野におけるITレジリエンスに関する分析レポート』
https://www.fsa.go.jp/news/r6/sonota/20250630-2/01.pdf



オペレーショナルレジリエンスとは

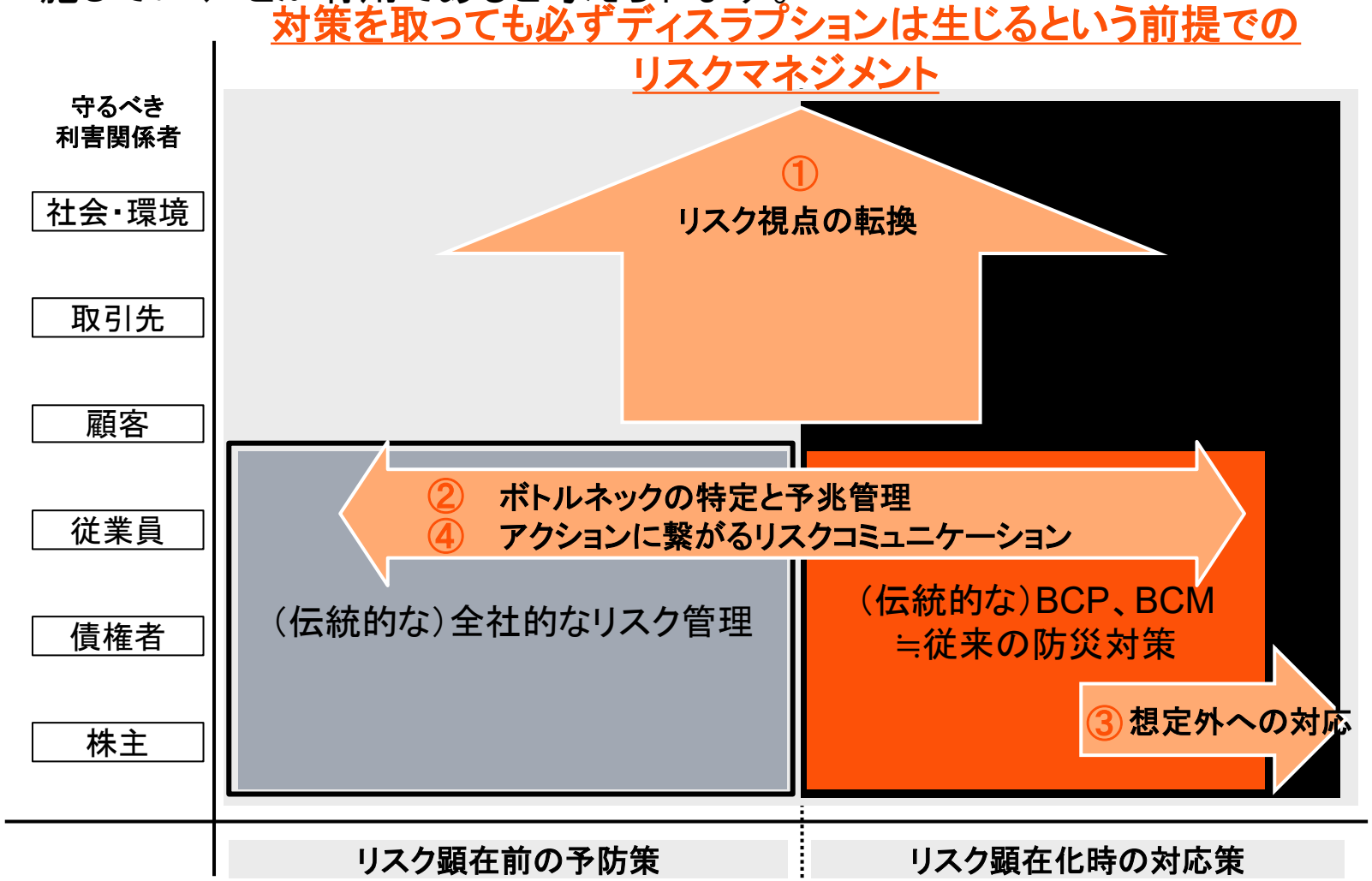
オペレーショナルレジリエンス（業務の強靭性・復旧力、オペレジ）とは、システム障害、サイバー攻撃、自然災害等が 発生しても、リスクを吸収し、速やかに回復する組織の能力をさします。

企業は従来の事業継続の取り組みや危機管理、オペレーショナルリスク管理にオペレーショナルレジリエンスの観点を取り入れることで、枠組みを発展させ、複雑化するリスク環境に対応できる態勢を整える必要があります。



オペレーショナルレジリエンスに対するアプローチ

複雑化していくビジネスや変化するリスクに対応するために、リスクの顕在化を前提としたレジリエンスの強化が重要となっています。平時と有事を融合したリスク管理態勢を構築し、トップダウン、ステークホルダーの視点でリスク管理を実施していくことが有用であると考えられます。



レジリエンス強化のポイント

① リスク視点の転換
最終的に守るべき主体を特定
（リスクの影響を受ける主体を特定、評価）

② ボトルネックの特定と予兆管理
（ストレステストによるボトルネックの特定。パフォーマンスモニタリング実施、エマージングリスクの捕捉による早期対応、平時と危機時のシームレス管理）

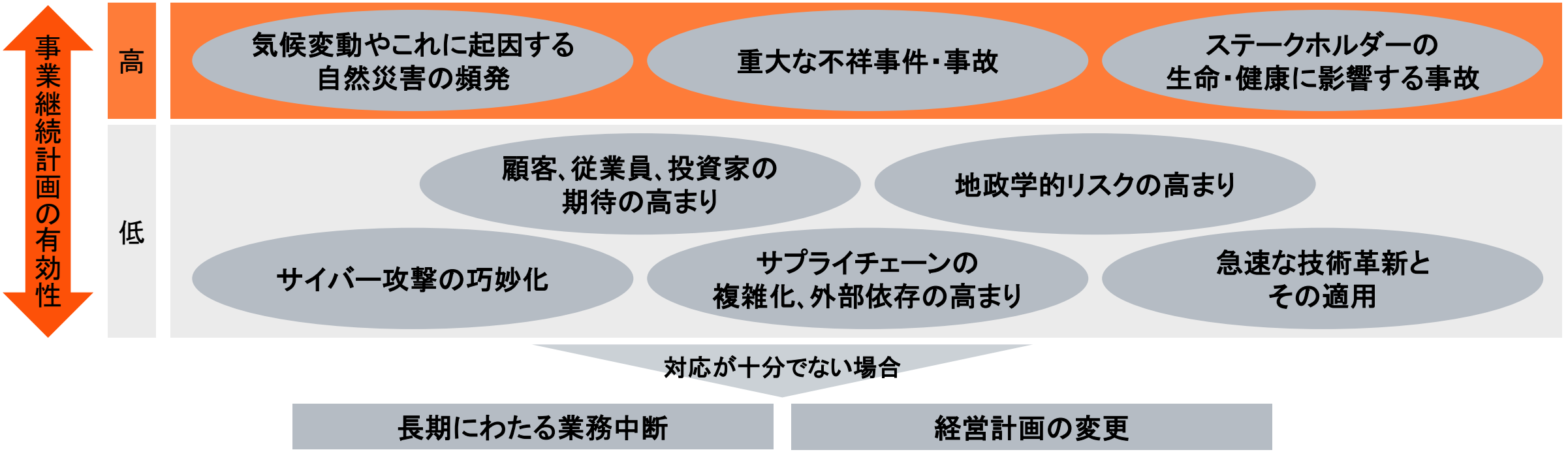
③ BCPが有効に機能しない場合でも対応を可能とする想定外への対応（Plan B）
（事前のシナリオテスト、ストレステスト）

④ リスクコミュニケーション

従来の管理方法とその限界

従来、金融機関や事業会社は事業継続計画（Business Continuity Management 、BCM）の枠組みのなかで、地震などの特定のリスク事象を想定した対応計画（Business Continuity Plan、BCP）を整備していた。一方、業務効率化や提供サービスの多様化、イノベーションの推進のため、企業におけるITシステムや外部ベンダーが提供するサービス（クラウドサービス等）への依存度は高まり、サイバーセキュリティの脅威、システム障害等、企業が直面するリスク環境は複雑化しつつあります。

既存のBCM／BCPで想定していなかった事象が生じた場合、顧客や市場に深刻な影響を与える重要な業務を提供できなくなるおそれがあります。未然防止策を尽くしてもなお、業務中断が生じることを前提に、利用者目線で早期復旧・影響範囲の軽減を確保する枠組みが国際的に議論されています。



2

内外の監督当局の動向と期待事項

オペレーショナルレジリエンスに関する本邦監督当局の動向

金融庁は、2022年8月「2022事務年度金融行政方針」において、オペレーショナルレジリエンスの対応について言及し、2023年4月「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」のディスカッションペーパーを発出しました。

金融庁による オペレーショナルレジリエンスの定義	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
ディスカッションペーパーの概要	• オペレーショナルレジリエンスとして求められる対応はBCBSや英国の要請事項と凡そ、共通。 • サードパーティリスク、サイバーセキュリティに触れるのは当然として、オペレーショナルリスク、BCP／BCM、再建・処理計画（RRP）、更にはコンプライアンスリスク（コンダクトリスク）についても言及。 • 主たる対応として4つのステップに係るプロセスを提示。 ① 「重要な業務」の特定 ② 「耐性度」の設定 ③ 相互連関性のマッピング、必要な経営資源の確保 ④ 適切性の検証、追加対応 • また、オペレーショナルレジリエンス態勢の確立においてトップマネジメントのコミットメントから顧客等へのコミュニケーション、人事制度（採用・育成・評価・異動）、リスクカルチャーの醸成（リスクコミュニケーション、心理的安全性）まで態勢全般について触れている。

オペレーショナルレジリエンスに関する本邦監督当局の動向

金融庁のディスカッションペーパーにおいて、実効性あるオペレーショナルレジリエンスのために必要となる周辺要素について紹介しています。

トップマネジメントのコミットメント

- オペレーショナルレジリエンスの枠組みが形骸化し、PDCAサイクルが機能しないことを防止するため、経営陣のコミットメントと積極的な関与により、ステークホルダーへの説明責任を果たすことが重要で ある。

人事制度（採用・育成・評価・異動）

- 明確な人材要件を定義せず、定期異動で人材を配置するメンバーシップ型の人事制度は、必要なスキル・専門性を有するリソースの確保を阻害する要因となり得る。
- 他方で、ジョブ型の人事制度では、遂行すべき職務が雇用契約に 明確に規定されるため、「重要業務の耐性度に必要なリソースを定義した上で、要件を満たす人員 を採用・配置する」というオペレーショナルレジリエンスの考え方と親和性が高い。

リスクカルチャーの醸成（リスクコミュニケーション）

- インシデント（ヒューマンエラー）に関与した個人にペナルティを科す減点主義は、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から生じた症状として捉え、インシデントやヒヤリハットを組織全体の学習・適応のための教訓として活用する考え方のもと、事務ミス発生時の担当者へのペナルティをあえて廃止したケースもある。

リスクカルチャーの醸成（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れば、危機時においても、積極的に声を上げ、組織間で連携することで被害の拡大を防止することができる。
- そのためには、職場環境として心理的安全性が確保されていることも重要であり、1 on 1等の対話活動を行うことで、メンバーの問題意識や違和感を傾聴し、主体性・自発性を育てる取り組みが導入されつつある。

出典: 金融庁「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」（概要）

オペレーショナルレジリエンスの管理プロセス

金融庁のディスカッションペーパーで提示された、オペレーショナルレジリエンスの管理プロセスは下記のとおりです。

オペレーショナルレジリエンスの統合的な管理プロセス

①「重要業務」の特定	②「耐性度」の設定	③相互連関性のマッピング 必要な経営資源の確保	④適切性の検証 追加対応
• 金融システムの安定・利用者の日常生活上の重要な**金融サービス**を特定	• 業務中断が必ず起こることを前提に、最低限維持すべき**水準（耐性度）**を設定	• 社外のサードパーティ等も含めて**相互連関性をマッピング**し、必要なヒト・モノ・カネを特定して採用・配置・配分	• 経営陣のコミットメントの下、シナリオ分析やBCP訓練を通じて、**適切性を検証**し、必要に応じて追加対応

個々の機能ではなくビジネスサービスごとの検討

顧客・自社・社会の観点での耐性度設定

End To Endでのリソースの可視化

リソース配分の実効性を確認

経営陣は、定期的な検証により特定 した脆弱性に対して追加対応を行う（例：システムに対する追加投資、必要な人的資源確保のための人事制度・採用育成制度の見直し）

外部環境（金融システムへの影響、市場シェア、利用者数、利用頻度）や自社の規模等の変化に応じて、重要な業務 や耐性度も見直しの対象となる

出典: 金融庁「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」（概要）

オペレーショナルレジリエンスに関する各国の状況

オペレーショナル レジリエンスについては世界各国の当局及び多国籍企業が検討を開始しており、様々な高度化アプローチが提案されつつあります。世界に先駆けて英国Bank of Englandが規制化を念頭に包括的な枠組みを提案しており、これまでにディスカッションペーパーや市中協議文書が複数発行されています。

バーゼル銀行監督委員会 （BCBS）

- 2018年にOperational Resilience Working Groupを設立。同年12月にはCyber Resilienceに関するRange of Practicesを公表
- 2020年8月にオペレーショナル レジリエンスとオペレーショナルリスクに関する原則を公表し、各国中銀の関連する取り組みを強化するための、原則的なアプローチを紹介している
- 2021年3月に上記の原則文書を改定する形で、「オペレーショナル レジリエンスのための諸原則」最終文書を公表

保険監督者国際機構 （IAIS）

- 2022年オペレーショナルレジリエンスにかかる市中協議文書を公表し、2024年8月には、実務文書（案）を公表
- 監督実務を示す「ツールキット」は、2025年前半に市中協議を実施予定

英国（イングランド銀行、PRA、FCA）

- BoE、FCA、PRAは、2018年に共同でディスカッションペーパー（DP）を公表。また市中協議文書を2019年12月に公表した。それ以降、継続して検討が進められているが、英国では、従来業務継続の領域に重点が置かれていたレジリエンスを、企業だけでなく顧客および市場の視点から検討する方法について積極的に変革が進められている。
- 2021年3月に最終文書を公表。政策的枠組みの導入にあたり、3年の移行期間が設定
- 2022年7月にレジリエンス観点を含めた重要外部委託先（CTP）管理についてのDPを公表
- 2025年3月、オペレーショナルレジリエンス整備に関する移行期限が到来

米国（FRB、FFIEC）

- FRBは2020年10月に「オペレーショナル レジリエンス強化のための健全なプラクティス」を発表、ガバナンスやリスク管理高度化のアウトラインを示した
- FFIECは、2019年11月に発行したITハンドブックにおいて事業継続に関するガイダンスを変更し、レジリエンスの概念（ビジネスインパクトアナリシスによる重要業務の特定、最大許容停止時間の設定など）を導入
- 2023年6月、FDIC, FRB, OCCは、レジリエンスの観点を含めた外部委託先管理についての最終ガイダンスを公表

EU（欧州委員会）

- ICTに焦点を当てたDORAを発表

シンガポール（シンガポール通貨監督庁）

- 2022年6月BCMに係るガイドラインが発表
- 顧客向かいの重要ビジネスサービスに関して、Timelyな復旧とサービス中心のアプローチの導入
- End to End で重要ビジネスサービスに関し依存性を確認し、効果的な復旧を阻害する要素を特定
- 定期的なモニタリングと外部環境の変化の取り込み

香港（香港金融管理局）

- 2026年5月末までに金融機関に対してオペレーショナルレジリエンスの導入が求められており、直近では2023年3月31日までに下記の達成を各金融機関に要求

1) 下記の含めてオペレーショナルレジリエンスのフレームワークの構築
   - オペレーショナルレジリエンスのキーパラメターの特定
   - 基本的なマッピングの完了
2) オペレーショナルレジリエンス構築のタイムラインの設定

経済安全保障推進法

2022年5月に成立した「経済安全保障推進法*」は、下表の4つの制度を新たに創設しました。
うち、「②基幹インフラ役務の安定的な提供の確保」に関する制度の対象となる事業には、金融・クレジットカード事業が含まれ、事業の停止を予防することへの期待が示され、有事の際でも、事業のオペレジを発揮することが強く求められています。

経済安全保障推進法　4つの制度	
① 重要物資の安定的な供給の確保	③ 先端的な重要技術の開発支援
半導体等、民間事業者が供給確保計画を作り、国が資金面などを支援	量子やAIなどの分野を想定する先端技術について、官民の協議会を立ち上げ、国が情報提供や資金面で研究開発を支援。機微情報には守秘義務を課す
② 基幹インフラ役務の安定的な提供の確保	④ 特許出願の非公開
14の基幹インフラ事業において、設備導入の際、サイバー攻撃等の「役務の安定提供への妨害」に備え、国が事前審査	核や武器関連など、国や国民の安全を脅かす恐れのある技術の流出を防ぐため、特許出願を非公開とする

14の基幹インフラ事業とは、

- 郵便
- ガス
- 石油
- 水道
- 電気
- 外航貨物
- 航空
- 鉄道
- 空港
- 貨物自動車運送
- 放送
- 電気通信
- 金融
- クレジットカード

よって、基幹インフラ事業は、

- **顧客へ甚大な影響を与える停止を避ける**義務を負う（欧米発祥の考え方）
- 国外から、安定提供の**妨害手段として利用され得るため、安全保障上も重要**である（本邦の考え方）

*出典: 内閣府 「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）」

バーゼル銀行監督委員会（BCBS）のオペレーショナルレジリエンスに関する諸原則

1. ガバナンス

- リスクアペタイト、リスクキャパシティ、リスクプロファイルを考慮したレジリエンスレベルの設定
- リスク強度は強いが蓋然あるシナリオ（“Severe but plausible”）の想定

2. オペレーショナルリスク管理

- PSMORのフレームワークの上にレジリエンスを確立
- オペレーショナルレジリエンスに関連する管理フレームワークの協調の必要性（例：BCP、サードパーティ管理、RRP等）
- 脅威と脆弱性の特定・評価および改善プロセスの必要性
- チェンジマネジメントの強化、拡張

3. BCPとテスティング

- 重要業務（Critical operations）の特定
- 重要な依存関係の特定
- 相互連関と相互依存を考慮したBCPの策定と管理
- RRP（再建・処理計画）との整合

4. 重要業務に係る相互連関と相互依存の把握

- 重要業務に関連する人材、テクノロジー、プロセス、情報、ファシリティ、サードパーティ、グループ会社（機能提供会社）とその関連性の把握（マッピング）

5. サードパーティー管理

- 重要業務の提供に関わるサードパーティやグループ会社のレジリエンス能力の評価と管理
- 上記について自社と同等の水準の管理を有しているか検証する必要

6. インシデント管理

- インシデントのライフサイクル管理（インシデントの影響度評価とリソース配分、インシデント管理プロセス、コミュニケーション）

7. 情報通信技術（ICT）のレジリエンス

- 情報資産、インフラの管理
- サイバーセキュリティ

出所：「オペレーショナルレジリエンスの諸原則」協議文書（2020年8月）をもとに、PwCが作成

内外の監督当局の動向と期待事項：導入状況

日本

- **主要行**においては、全重要業務にに対してのオペレジのプログラムの導入が完了。いわゆる二周目の取り組みや、一周目の課題の打ち取りに向けて検討中
- 一部の金融機関においては経済安保推進法の対象となるケースもある。オペレジと並行して対応しているケースも存在する
- **大手証券会社**もオペレジの導入に着手し、プログラムの構築および、トライアルは完了
- **保険会社**：IAIS の2025-2029 年戦略計画の戦略テーマとしてデジタルイノベーション、及びサイバーリスクが挙げ られ、その中でオペレーショナルレジリエンスへの監督強化の方針が示されている
- 金融庁は「金融分野におけるITレジリエンスに関する分析レポート」において、本邦のオペレジの事例の取り組みの紹介

英国

- 英国では、各金融機関におけるオペレジプログラムの導入は完了
- 当局は各金融機関に対して、オペレジに関しての定期的な自己評価を指示
- また、当局はオペレジを補強するため、関連領域であるサードパーティ、サプライチェーン、サイバー、非金融機関に対しての集中リスク対応等に着手
- 昨今の状況を踏まえサイバーによる長期停止については、適切性の検証においての取り組みが求められている
- 一方、各金融機関は耐性度内での運用を開始しているが、金融機関において、下記の観点において運用上の課題が発生している
    - リソースマッピングの更新
    - サードパーティへのオペレジの対応依頼
    - レガシーシステムの取り扱い

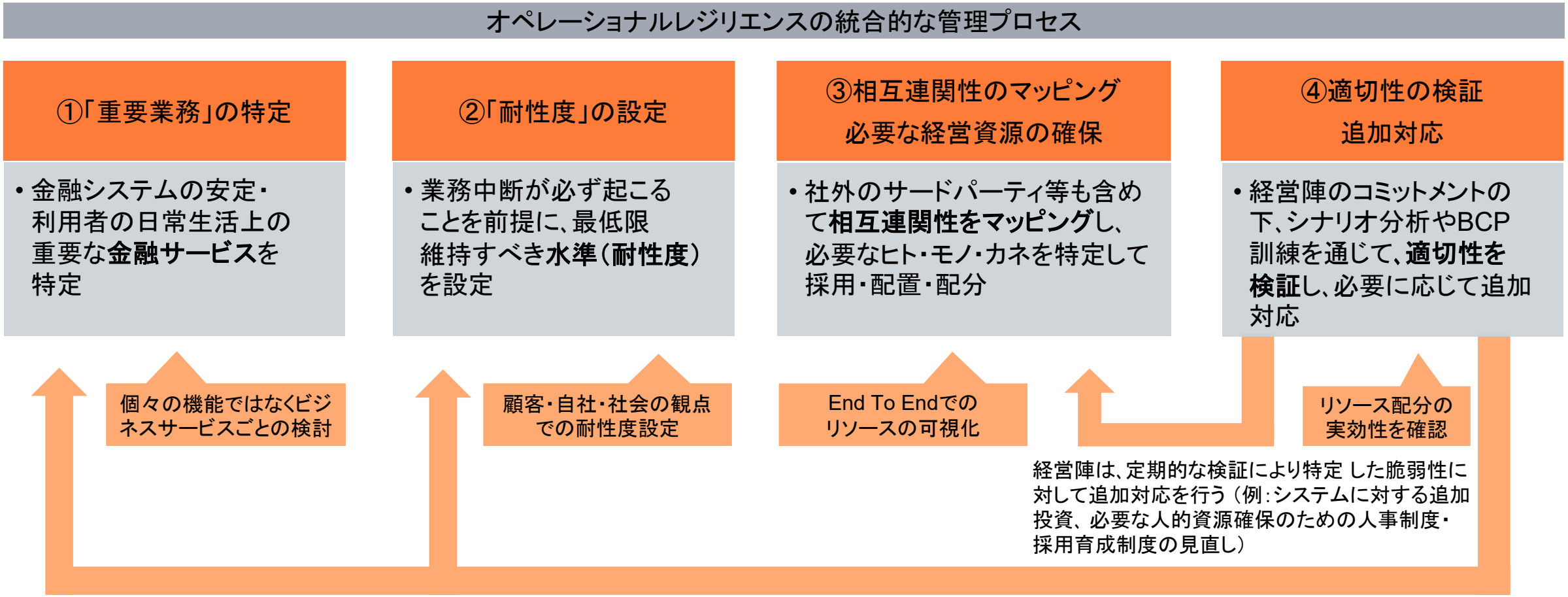
3

オペレーショナルレジリエンス概要

オペレーショナルレジリエンスの管理プロセス

再掲

金融庁のディスカッションペーパーで提示された、オペレーショナルレジリエンスの管理プロセス。



出典: 金融庁「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」（概要）

① 重要ビジネス・サービスの特定

中断・停止により顧客に耐えがたい損害を与えたり、システムの安定性や当社の安全性・健全性を害するサービスを、「重要ビジネス・サービス」として特定します。例えば、銀行の決済業務、ATM現金引出機能、投資銀行の通貨ヘッジサービス等が挙げられます。

①選定基準の策定

ビジネス・サービスの性質×規模

性質

観点	評価項目	評価
顧客	生活や企業活動への影響	有／無
	(機会)損失の発生	有／無
市場	システミックリスクへの影響	有／無
	流動性機能への影響	有／無
自社	風評被害の発生	有／無
	当局処分の可能性	有／無

✖

規模

取引の規模
顧客数
取引残高(ストック)
取引量(フロー)

②タクソノミーの整備

ビジネス・サービス、商品のタクソノミー(一覧)を整備の上
左記の選定基準により、重要ビジネスサービス(IBS)を選定

ビジネス・サービス	商品	評価軸			規模	IBS
		顧客	市場	自社		
A サービス	a-1	✓		✓	H	◎
	a-2	✓			M	
	a-3		✓		L	
B サービス	b-1			✓	H	◎
	b-2		✓		M	
	b-3			✓	M	
C サービス	c-1	✓			L	
	c-2			✓	L	
	c-3		✓		M	

① 重要ビジネス・サービスの特定

重要ビジネス・サービスの特定における主な論点・課題は以下の通りです。

1. 自社のビジネス・サービスや商品が一覧化されていない（標準化されたタクソノミーの不在）。

   - まずは、自社がステークホルダー（外部・内部）に提供しているサービスを整理する。
     業務プロセスではなく、業務プロセスを繋ぎ合わせたビジネス・サービス全体が望ましい。

ビジネス・サービス	商品	プロセス
保険金支払	生命保険	保険金請求、受付、審査、保険金算定、支払等
有価証券売買	外国上場株	発注、約定、決済（証券・資金）、レコンサイル等

   - 他の枠組みにおけるビジネス・サービスの区分があれば、参照する。
     （但し、オペレーショナルレジリエンスにおけるビジネス・サービスは部門毎の業務プロセス単位でないことに留意）
     - ✓ BCM/BCPにおける優先業務区分
     - ✓ ORMのRCSAやEvent報告の際の業務区分
     - ✓ IAのAudit Universe、Auditable Entityを援用
   - オペレーショナルレジリエンスのPDCAを回していくため、1線における責任部署（オーナー）を定めておくことが望ましい。

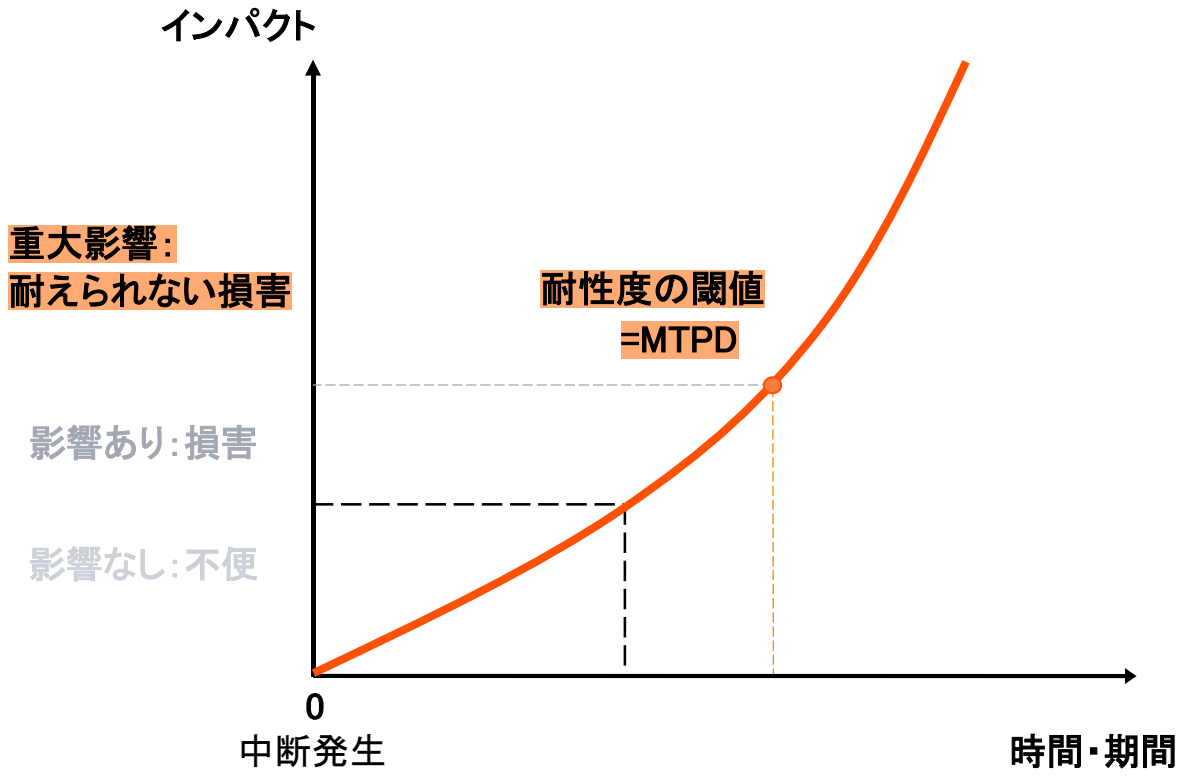
2. 多くのビジネス・サービスが重要なものとして選定されてしまっており、優劣がつかない。

   - ステークホルダー毎の評価観点に加えて、代替可能性や時限性といった評価軸を入れているケースがある。
   - 重要業務のなかでも評価結果から最重要、重要とTierを分け、段階的にオペレーショナルレジリエンスの取り組みを行うことが考えられる。

② 耐性度の設定

中断の時間に伴い、顧客、市場、当社に与える影響は不便程度から徐々に損害の発生に発展し、さらに耐えられない損害に達するポイントです。
耐性度の閾値（=最大許容停止時間：MTPD）は耐えられない損害が発生する時点に設定することが求められます。

＜耐性度のイメージ＞



影響度の目線	
重大影響	サービス提供できないことで多数の顧客や、業界のステークホルダーないし社会・市場全体に耐えられないレベルの損害を与え、または自社の収益に耐えられない損害をもたらし、謝罪会見を開き、社会にお詫びするレベル
影響あり	サービス提供できないことで一部の顧客やステークホルダーに損害を与え、顧客からの苦情が入り始め、現場から個別にお詫びを入れるレベル。または自社の収益に損害をもたらすが、受け入れ可能な程度
影響なし	サービス提供できないものの、顧客、自社、社会と市場への損害はなく、リカバー可能なレベル

② 耐性度の設定

各国の規制・ガイドラインにおいて、耐性度は、業務中断に対するステークホルダーにおけるMTPDを時間軸で表現する事が求められています。時間軸については、取引量、売上高等も考慮して判断する事が求められています。

①耐性度設定に関する計測指標の収集

計測指標	具体的なデータ例		
	顧客観点	自社観点	市場観点
影響ステークホルダー数	・顧客数		・顧客数からみた市場シェア
中断取引量	・当社⇔顧客の取引後に発生する取引量	・当社⇔顧客の直接的な取引量	・取引量ベースで見た市場シェア
損失、逸失収益	・中断により顧客が被る損失金額	・営業中断による逸失収益、売上	
…	…	…	…

② 耐性度の設定

各国の規制・ガイドラインにおいて、耐性度は、業務中断に対するステークホルダーにおけるMTPDを時間軸で表現する事が求められています。時間軸については、取引量、売上高等も考慮して判断する事が求められています。

②耐性度基準の設定

影響度	影響度設定基準（目線）		
	顧客	当社	市場
指標	影響を受ける顧客数	損失金額	市場シェアへの影響
重大影響	多数の顧客に影響あり（目安：〇〇人以上）	当社業務への重大な影響 （〇〇億円以上の損失発生・収益剥落可能性等）	（顧客側のサービス代替による） 〇〇%以上の市場シェア低下
影響「あり」	一定の顧客に影響あり（目安：〇〇人以上）	当社業務への影響 （〇〇億円以上の損失発生・収益剥落可能性等）	〇〇%未満の市場シェア低下
影響「なし」	①顧客・事業等への影響なしor軽微	当行業務への影響なし or 軽微	市場シェアに対する影響なし

②耐性度の設定

顧客、自社、市場それぞれの観点で、各計測指標の定量データを収集、もしくは定性的な判断により、業務中断による時間軸上の影響度を特定

観点	基準	1日	2日	3日	・・・	1週間	2週間	1カ月
顧客	影響顧客数							
自社	当社の損失							
市場	市場シェアの低下							

各観点の影響度から、最も早く重大影響が生じる時点をMTPDとして設定（RTOはMTPDの範囲内で設定）

② 耐性度の設定

耐性度の設定における主な論点・課題は以下の通りです。

1. 耐性度の設定に際して、「重大影響」が発生する閾値を設定することが難しい場合、（適切なデータが存在しない、或いは入手が難しい）どのようにすれば良いか。

   ➢ 以下のような観点で閾値を設定することが考えられる。

   ＜保険会社における保険金支払＞

#	「重大影響」の閾値設定の検討方法	説明	例
①	**業界・ビジネス慣習や有識者の経験に基づく判断**	業界・ビジネス慣習として持っている数値や有識者の経験を踏まえて設定	• ビジネス上の経験値や法令対応等から、〇人以上の顧客に△日以上の支払遅延が発生すると深刻な影響を与える可能性がある
②	**過去のリスク事象の数値を基に設定**	他業界・他社のリスク事象（システム障害等）から設定	• 〇年の△△証券の事象では■日間、支払サービスが停止している。
③	**既存の枠組みにおける閾値を準用**	既存の枠組み（規制当局や業界団体の基準、或いは社内のBCP、RCSA等）において設定されている閾値（目線）などを準用して設定	• 監督当局あるいは協会において、システム障害の報告基準は「契約者数の〇%以上又は〇件以上の契約（いずれか少ない方以上となる場合）に影響を与えた場合」としている

2. RLOの設定は必要か

   ➢ ディスカッションペーパーではRLOの必須とは記載されていないが、長期の停止や、復旧を想定しない代替手段においては、通常時と同様の水準での業務提供は難しい。

   ➢ 必ずしも、定量的な数字のみならず、定性的な「新規入力は受けつけない」などの定義を行うことも可能である。

③ 相互連関性のマッピング

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します。マッピングの目的は、リソースのうち、脆弱性（代替不可能性）のある箇所を特定し、シナリオテストの際、ストレスをかけて検証する箇所を特定するために行います。

ステークホルダー		重要プロセス						
		請求	受付		審査		送金	
顧客	顧客	保険請求						受取
当社	カスタマーサービス部			受付				
	審査部				審査			
	商品部					保険金算定		
当社（グループ）	決済部						送金	
	・・・							
サードパーティー（グループ外）	コールセンター		受理					
	・・・							
リソース種別		**リソース確認**						
必要人員		-	20名	5名	10名	5名	10名	-
施設		-	横浜	東京	東京	東京	豊洲	-
リモート環境		-	×	○	○	○	×	-
システム		-	受付管理システム	契約者管理システム	契約者管理システム	アクチュアリーシステム	銀行送金システム	-
バックアップシステム		-	×	○	○	○	○	-
・・・		-						-

③ 相互連関性のマッピング

既存の台帳の情報を活用し、相互連関性のマッピングを行うことで、マッピングやフロー図の乱立を防ぐことが可能です。
これらの台帳をシステム上で管理を行うことにより、マッピングのメンテナンスが可能になります。

重要ビジネスサービス一覧A

ステークホルダー		重要プロセス						
		請求	受付		審査		送金	
顧客	顧客	保険請求						受取
当社	カスタマーサービス部			受付				
	審査部				審査			
	商品部					保険金算定		
当社(グループ)	決済部						送金	
	・・・							
サードパーティー(グループ外)	コールセンター		受理					
	・・・							
リソース種別		リソース確認						
必要人員		-	20名	5名	10名	5名	10名	-
施設		-	横浜	東京	東京	東京	豊洲	-
リモート環境		-	×	○	○	○	×	-
システム		-	受付管理システム	契約者管理システム	契約者管理システム	アクチュアリーシステム	銀行送金システム	-
バックアップシステム		-	×	○	○	○	○	-
・・・		-						-

- ビジネスサービス一覧
- 業務一覧
  業務フロー図（概要）
- 部門台帳
- ｻｰﾄﾞﾊﾟｰﾃｨ台帳
- オペレーション一覧
  業務フロー図（詳細）
- システム管理台帳
- BCP・コンチプラン
- 施設一覧

③ 相互連関性のマッピング

相互連関性のマッピングにおける主な論点・課題は以下の通りです。

1. 相互連関性のマッピングを行う部署において、プロセスやリソースに関する断片的な情報しかない。
   - ビジネス・サービスに関する所管部署において、End to Endにおける業務プロセスを全て対応していることは考えにくく、社内で個々のプロセスを所管している部署や一部プロセスを外部委託先へアウトソースしている場合もある。
   - また、システム（システムフロー、サーバーやバックアップシステムの所在等）やインフラ（電力・通信環境等）に関するリソースについても、ビジネス・サービスの所管部署ではなく、ITや総務で管理をしているケースが多い。
   - まずは、所管部署において有している断片的な情報から、マッピングを行い、ワークショップや個別インタビューを開催し、関連部署と情報のギャップを埋めていくことが望ましい。

2. マッピングをどの粒度まで細かく整備すればよいかわからない。
   - 本件の目的は、全てのプロセス及びリソースを網羅的に洗い出すものではなく、End to Endで、特に脆弱性のあるリソース（代替不可能、オペレーションの集中）を洗い出すものである。
   - ビジネス・サービスの目的（例.顧客への保険金支払、投資家への証券解約代金の支払、投資信託の受益権の発行等）を踏まえ、主要プロセスを並べたうえで、緊急時に業務量の観点で内製化が難しいもの、他の方法で代替が難しいものを洗い出すことに主眼を置く。

④ 適切性の検証

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、重要ビジネス・サービス、耐性度、必要な経営資源に関する設定およ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、見直しや追加的措置を講じます。

①シナリオの定義とデータ収集

内外の情報をもとに極端だが起こり得るシナリオという想定の下、リソース種別ごとに、制約を設定

＜自然災害・感染症＞

リソース	制約の詳細（例）
人	人員が、2週間、50%未満
システム・データ	–
施設	施設が、1ヶ月、利用不能
サードパーティ	上記制約に準ずる

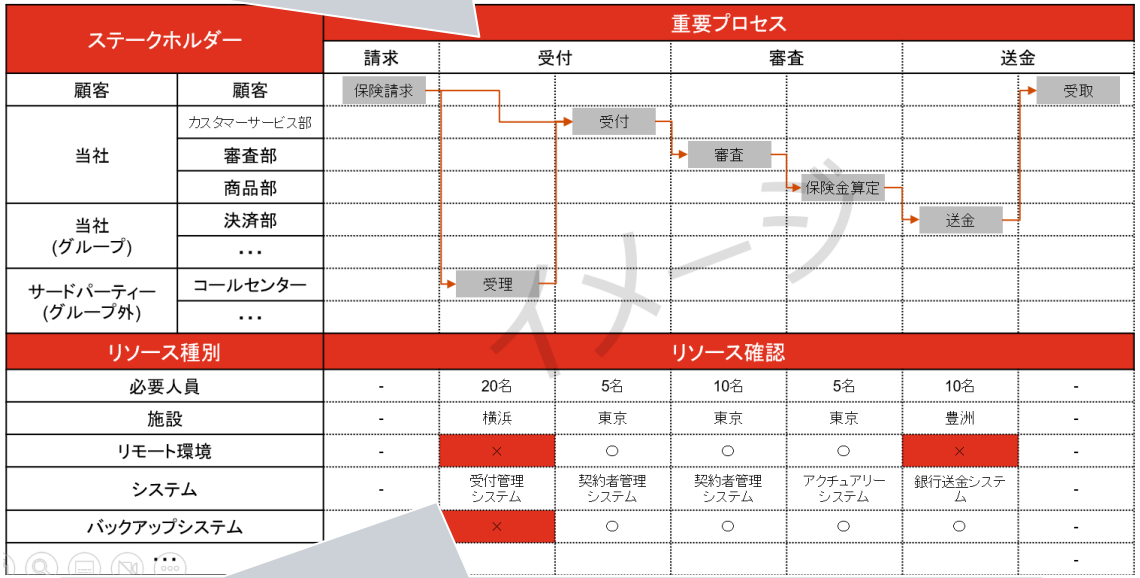
＜システム障害＞

リソース	制約の詳細（例）
人	–
システム・データ	システムが、5日間、利用不可
施設	–
サードパーティ	当該委託サービスが、5日、利用不能

②テストと改善の実施

左記シナリオとリソース制約のもとで、既存のリソース、BCPの対応により、ビジネス・サービスを耐性度の範囲内で維持できるか確認。テスト結果を踏まえて改善を実施

リソース制約から、耐性度の範囲内で対応が可能か（RTOを満たせるか）検討



必要に応じてリソース・BCPの追加検討あるいは、Plan Bとして復旧に限らない代替手段を検討

④ 適切性の検証

適切性の検証における主な論点・課題は以下の通りです。

1. シナリオとリソース制約をどのように設定すれば良いかわからない。
   - 金融庁のディスカッションペーパーでは、極端だが起こり得るシナリオを想定することが求められている。
     以下の情報を踏まえて、いくつかのシナリオとリソース制約を設定する。
     - ✓ 既存のシナリオ（BCP, IT-BCP等）
     - ✓ 自社または業界の過去事故
     - ✓ 当局指針・ガイダンス、自治体公表情報等
   - 但し、上記シナリオベースで適切性を検証すると、シナリオ毎にリソース制約を設定し、適切性の検証をシナリオ毎に実施しなければならない。このことから、オールハザード（特定のシナリオは記載せず、リソース制約のみに着目）ベースで適切性の検証を行うケースもある。

2. 適切性の検証の結果、BCP・リソースの補強だけでは、耐性度の範囲内でのビジネス・サービスの維持が難しいことが判明した。
   - 復旧だけでなく、他社との協業等による新たな代替手段の確保やステークホルダーへの情報発信等、Plan Bを予め設定しておくことが考えられる。
     （例）
     - ✓ 震災時におけるATM同時開放
     - ✓ 衛星通信契約による更なる通信手段の確保
     - ✓ 店頭電子掲示板やWebsiteによる障害に関するメッセージ発信

4

オペレーショナルレジリエンスを考慮したBCP/BCM

オペレーショナルレジリエンスと事業継続計画の違い

オペレジは、顧客等の期待を踏まえ自社のビジネス・サービスの維持すべき水準を定め、ビジネス・オペレーティングモデルにその水準を維持するための仕組みを組み込むためのフレームワークです。

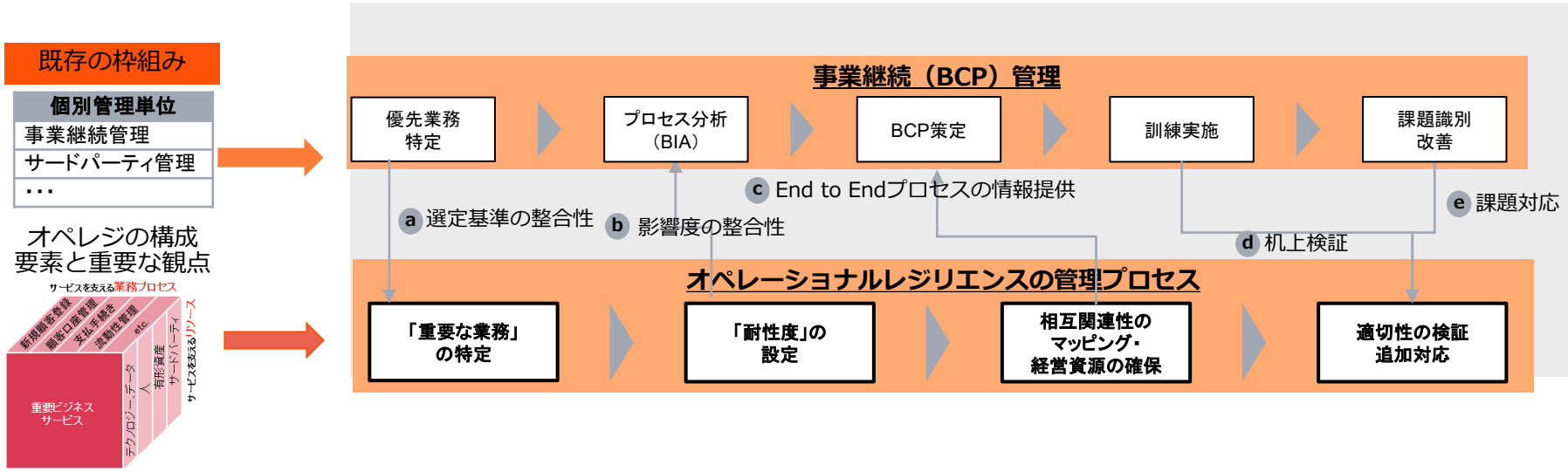
	事業継続計画（BCP）		オペレーショナルレジリエンス	
アプローチ	ボトムアップ	組織・機能の観点による取り組み	トップダウン	経営目線での取り組み（リスクアペタイト）
影響の捉え方	組織	自社への影響中心	社外	顧客・マーケットへの影響中心
戦略視点	戦術的	復旧のための活動	戦略的	ビジネス上の戦略と整合
単位	業務・機能	詳細な業務・プロセス等のレベル	ビジネス・サービス	重要サービスの全体の観点
体制	垂直型	機能別／部・課別等の組織構造に依存	水平型	組織横断的なEnd-to-Endの業務プロセス全体
レポーティング	コンプライアンス	機能復旧状況	ビジネス上の意思決定	顧客サービス品質
アウトカム	機能維持・復旧		顧客サービスの維持・復旧	

事業継続計画（BCP）は誰（Who）がどのように（How）業務を継続させるかという具体的行動計画

オペレジはどういう理由（Why）で誰（Whom）のために、どのビジネスサービス（What）をいつまで（When）に回復・維持するかという、あるべき姿の整理

オペレーショナルレジリエンスと事業継続計画の関連性

あるべき姿として、オペレジでは旧来のBCPの情報を継承し、活用しつつ、特に顧客目線と社会目線で再度検証する必要があります。また、オペレジで整理した重要な経営資源に対して、BCPを通して、耐性度までの達成可能性の検証をおなう必要があります。



BCPとオペレジの関連性

ⓐオペレジの重要業務を選定する際に、旧来のBCPで選定された重要業務を継承することが可能だが、顧客、市場、自社の観点で再検証する必要

ⓑオペレジの耐性度を設定する観点として、顧客、社会と自社の目線が挙げられる。オペレジの耐性度を検討できたら、関連するBCPにおける業務中断の影響を把握するために、ビジネス影響度分析にも反映可能

ⓒオペレジで相互連関性のマッピングを整理し、必要な重要経営資源を洗い出したあと、それぞれの経営資源または複数の経営資源をまとめる部署あるいはシステムのBCPに紐づける必要

ⓓ適切性検証としては、BCPで規定されたRTOの等の復旧指標が耐性度以内に設定しているかどうかを検証

ⓔBCP訓練を通して発見した課題を解決しつつ、オペレジでは耐性度を守る代替策なども考える必要

オペレーショナルレジリエンスと事業継続計画の論点

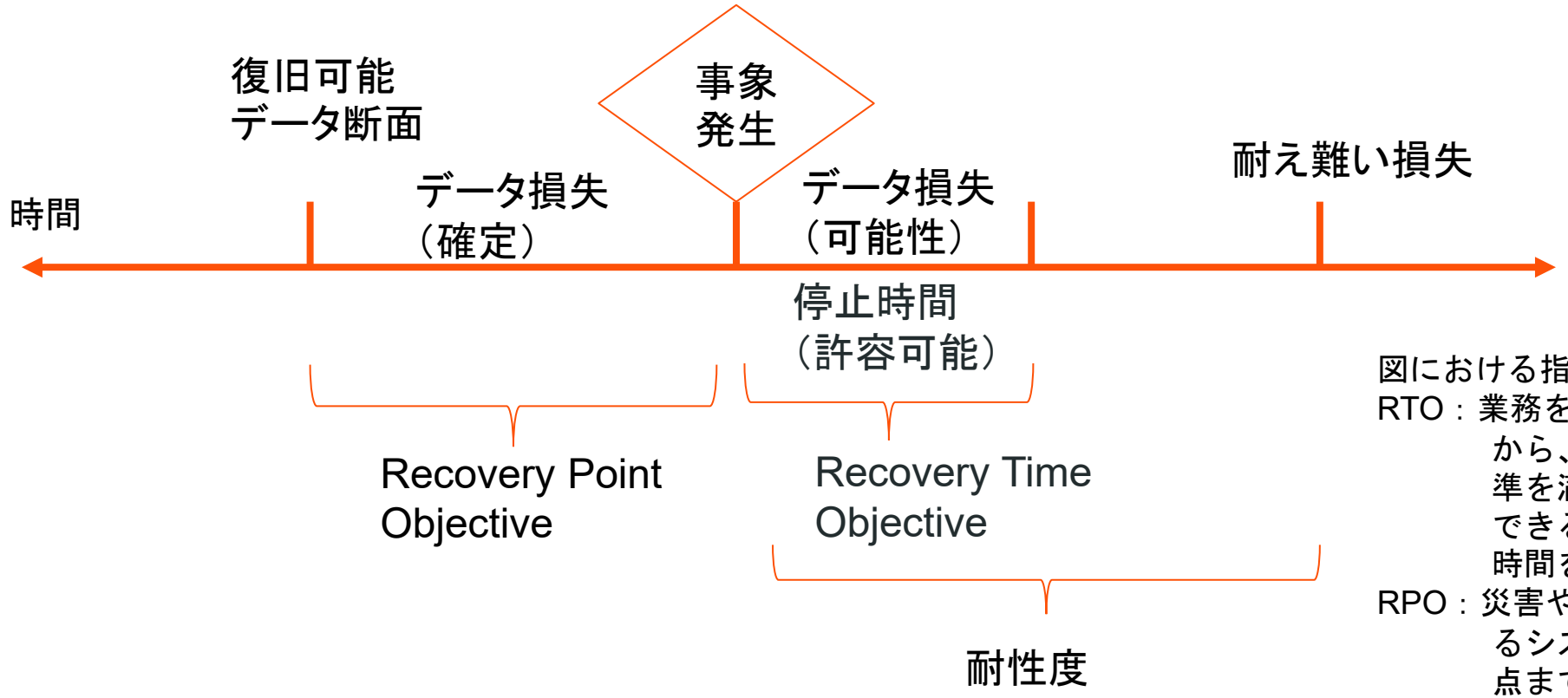
あるべき姿を明確化するオペレジに対して、復旧の具体的計画であるBCPはオペレジに向けて、重要業務のインパクト分析と選定理由や、コンチプランの対象とその目標復旧時間の設定を整合する必要があります。

BCPとオペレーショナルレジリエンスの論点と整合性

	BCPにおける論点	整合性	オペレーショナルレジリエンスにおける論点
「重要な業務」の特定	1. ビジネスインパクト分析（BIA）によってどの業務がBCP重要業務の対象か？	オペレジの重要業務はBCPの対象業務と整合しているか	1. どの業務がどのように重要業務（または重要ビジネスサービス）に選定されたか？
「耐性度」の設定	2. BCPの対象となる重要業務の目標復旧時間（RTO）はいつまでか？	BCPで設定されたRTOはオペレジの耐性度に収められているか？	2. 重要業務の耐性度（または重要ビジネスサービス）はいつまでか？
相互関連性のマッピング・経営資源の確保	3. BCPに規定しているコンテンジェンシープランの対象（人・部署、施設、システム）はだれか？どういう手順で復旧作業を実施するか？	BCPのコンチプランはオペレジ重要業務のリソースをカバーしているか？	3. 重要業務を構成するリソース（人・部署、施設、システム、サードパーティ）は何か？リソース間の関係は何か？
			4. 各リソースの中断から復旧または代替手段への切り替えができるまでの時間は耐性度に収められるか？
適切性の検証追加対応	4. BCPのテスト・訓練でRTOの有効性を検証できているか？	耐性度を満たすための手段やリソースは十分か	5. 重要なリソースについては、BCPの復旧のみならず、代替手段や広報などの対応は準備されているか？

耐性度を踏まえたRTOの関係性

途絶と復旧のタイミングを決めて、途絶許容度に対してのテストを実施することはBCBS、FFEICなど各国当局で求められています。
今後のRTOの設定のためには耐性度をその検討要素として含める必要があります。



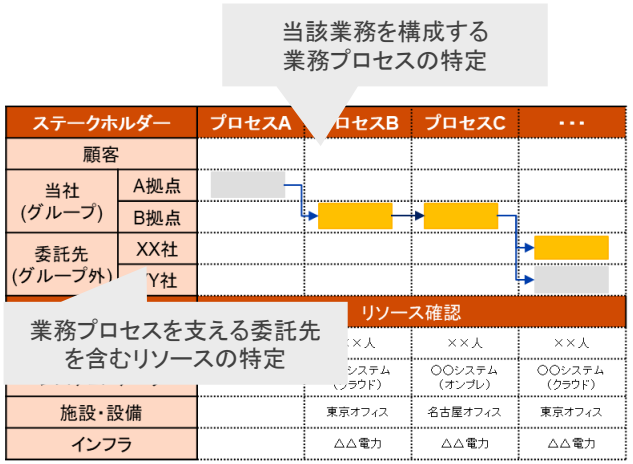
図における指標
RTO：業務を停止させる事態の発生から、目標としている復旧基準を満たし、重要な業を再開できるようになるまでの目標時間を指し示す指標。
RPO：災害や事故、障害の発生によるシステム停止時に、どの時点までさかのぼってデータを回復させるかを示す指標。

サードパーティーを踏まえた業務継続の考え方

システムに関わる外部委託や、事務オペレーションの外部委託など事業の提供に関わるリソースの複雑化が進んでいる。一方、こうしたリスクへの対策はまだ十分でない企業が多いです。
危機管理とサードパーティリスク管理を連動させて、リスクベースで対応を検討する必要があります。

リソースマッピング

選ばれた重要業務を構成する業務プロセス、拠点、リソースを特定



委託先の**業務遂行上の重要性に応じたリスクベースで**の重要性評価を行い、サードパーティ可用性に関わる関与を行う必要がある

可用性に関わる評価の方法としては下記があげられる

- 重要度に応じたオンサイトの監査
- 契約書やSLAなどのサードパーティとの関わる合意（復旧水準関係先への連絡方法等）
- サードパーティの訓練のモニタリング
- サードパーティとの合同の訓練実施
- SOCIIの可用性に関わる保証

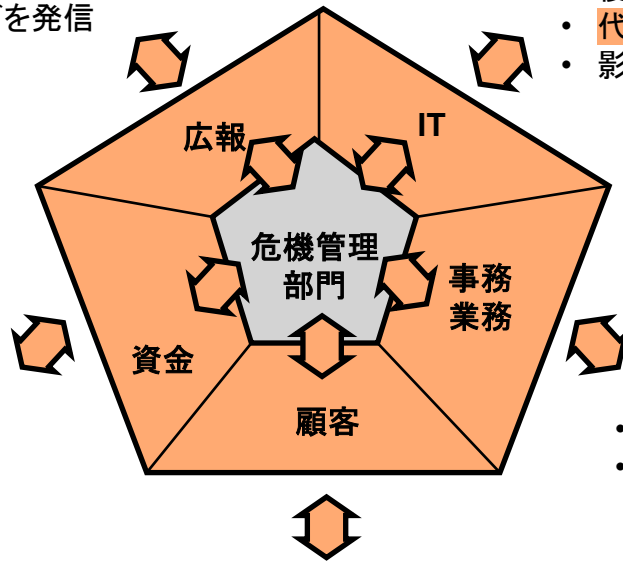
継続計画であり、復旧計画ではない

従来のBCPでは、機能の「復旧」に焦点があたることが多いが、復旧のみならず、マニュアル作業での代替手段や、外部発表などの様々な手段を活用し、耐性度を満たす必要がります。
近年のサイバーセキュリティインシデント事案のように、復旧手段が機能しない、対応が長期化するケースが増えており、代替手段や広報等の対応方針がより求められています。

【有事の社内ステークホルダーの動き方イメージ】

- 現地から公開情報、連絡事項を収集
- 被災状況、対応進捗などを発信
- 外部発信当の検討

- 復旧、原因追及
- 代替・暫定手段の提供
- 影響特定（事務、業務部門との連携）



- 現地から資金の不足に対する情報収集
- 資金を調達し、各拠点に配送

各部署からそれぞれ業務の遂行可能性など、事務手続きに関する情報を収集
- 代替手段の提供等の提示
- 業務等の復旧について指示

- 現地顧客からの苦情、要望などを収集
- 営業可否や、顧客対応を指示
- 顧客への謝罪、お詫び（返金等）の検討

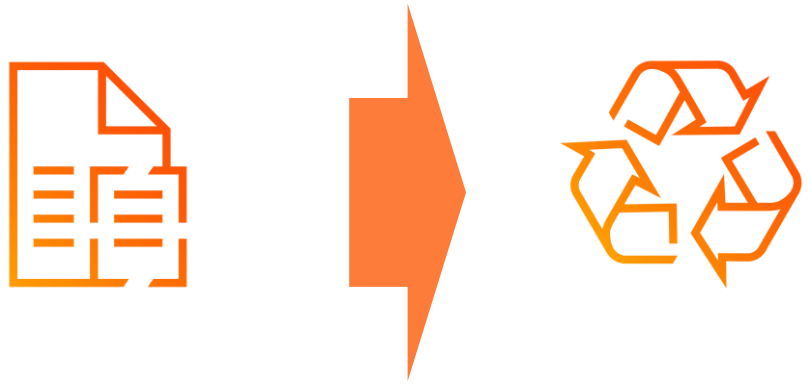
5

BCP/BCMの取り組み

BCPを"文書"から"動く仕組み"へ

BCPは作るだけでは十分ではありません。訓練と評価を回し、改善し続ける仕組み（BCM）にして初めて、業務継続の実効性が上がります。

- ✓ 昨今、金融機関で起きているインシデントは、サイバー、外部委託、クラウド、サプライチェーンなどが重なりやすく、原因も影響も一つに固定できません
- ✓ だからこそ、事象ごとに手順書を積み上げるより、重要業務が止まる状態を前提にして、止まった後にどう判断し、どう縮退し、どう復旧するかを“回せる形”にすることが重要となります



本章における3つのポイント

1.BCP/BCMの規制動向・潮流

規制や潮流の要点を押さえつつ、「BCMとして何が追加で求められているか」に絞って整理します。

2.リスクシナリオ策定・訓練高度化

シナリオと訓練の作り方を、事例を交えながら明日から自社で実施できるように落とし込みます。

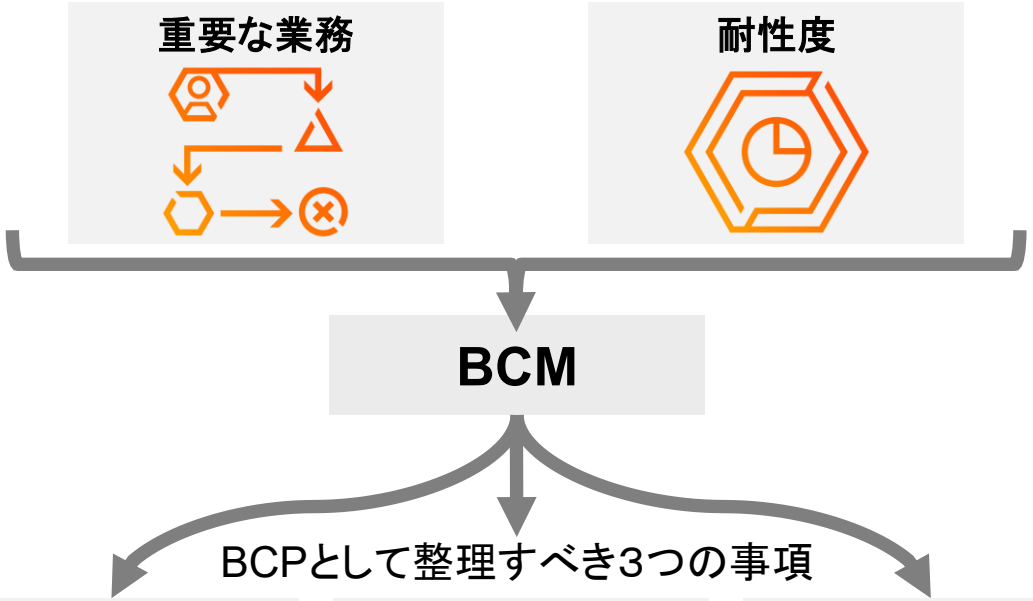
3.BCPの有効性評価と継続的改善

「できた/できない」ではなく、実測と目標の差分を分析し、具体的な改善計画の策定まで具体化します。

オペレーショナルレジリエンスからBCPへの“変換"を担うBCM

オペレジとBCP/BCMはそれぞれ独立したものではありません。オペレジ側で決めた「守るべき重要な業務」を、BCPが実装できる形に変換するのがBCMの役割です。

- ✓ オペレーショナルレジリエンスでは、守る対象を「重要な業務（サービス）」として特定し、許容できる停止の範囲や時間（耐性度）を決めます。BCMは、この上流の決定をBCPの実務として落とし込むことです
- ✓ これが曖昧なままだと、訓練で議論が散り、実際の障害時に意思決定が止まります。BCMは「計画書を整える」ことではなく、「判断できる状態を作る」ことを主語に置きます



何が起きたらBCPを発動するのか(停止の兆候、顧客影響の閾値、対外説明要否など)

どの業務を先に戻すのか(顧客影響、法令対応、市場影響、二次被害の観点など)

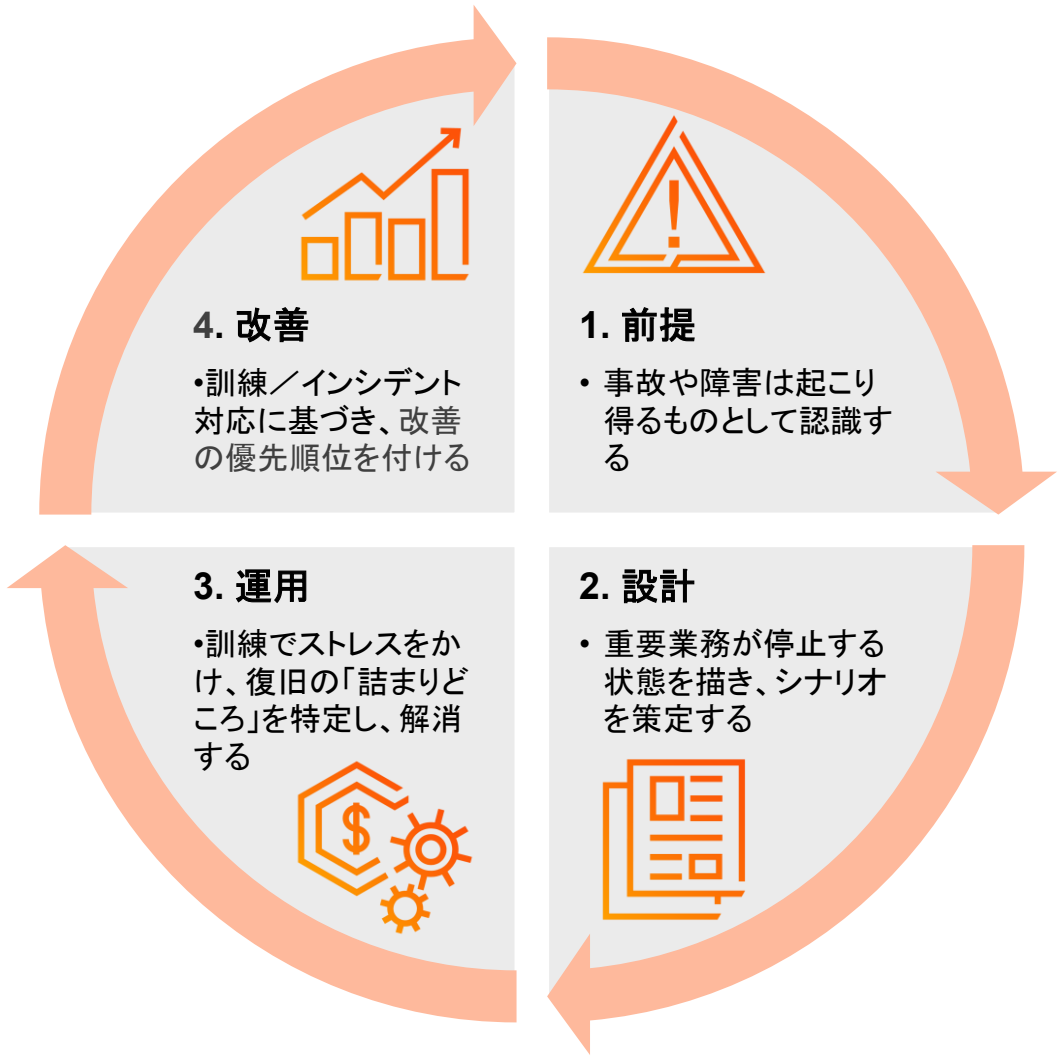
縮退運用、取引制限、対外公表、委託先切替などを、誰がどの情報で決めるのか

国内の監督目線：重大障害は"起きる前提"での運用（BCM）が求められる

金融機関に対するFSAの期待は、BCPの策定から、平時から回して更新する運用（BCM）へ比重が移っています。サイバーリスクを含め、重大障害はゼロにはできないという前提に立った動きです。

- ✓ 国内における監督の目線では、BCPの有無そのものよりも、BCPが実際に動くか、動いた結果が改善されるかが重視されています。
- ✓ これはBCP/BCMを「危機管理部門の仕事」に閉じず、IT、サイバー、外部委託、顧客対応、広報、法務、経営判断が同時に動く横断の運用設計と捉えるべきことを示唆します。

金融庁のレポートでも「対策を講じてもインシデントが発生することを前提としてITレジリエンスを強化する必要がある」と明記されており、このサイクルを回す実効性が問われます。



FSAレポートから見るインシデントの“パターン"：自社のBCPシナリオへの変換

FSAの「ITレジリエンスに関する分析レポート」は、実際に起きた事案からBCMが学ぶべき「止まる状態」と「復旧の詰まりどころ」の宝庫です。ITに関する事例が中心ではあるものの、BCPのシナリオを強化するため、事象を以下のような“パターン"に分類し、自社の計画に反映させます。

1

外部・第三者要因が混ざる

事例：委託先のランサムウェア感染による情報漏えい、セキュリティソフトの不具合による業務端末停止

BCPへの反映：「委託先からの情報提供が遅延する」「原因が特定できない」状況をシナリオの初期条件とする

2

防御を前提とした攻撃・妨害

事例：DDoS攻撃によるサービス遅延、フィッシングからの不正アクセス

BCPへの反映：防御策が機能している中でもサービス影響が出ることを想定し、縮退運用や顧客への告知手順を検証する

3

変更が事故を起こす

事例：システム更改時の設定誤り、パッチ未適用による冗長構成の機能不全

BCPへの反映：変更作業そのものがインシデントのトリガーとなり得ることを想定し、切り戻し手順や判断基準を訓練する

4

手順・体制の不備が被害を拡大

事例：復旧手順の欠落による対応遅延、障害発生時の連絡体制の不備

BCPへの反映：「手順書がない」「担当者が不在」といった状況を訓練に組み込み、アドホックな対応能力を検証する

出典：金融庁「金融分野におけるITレジリエンスに関する分析レポート」

海外の潮流：第三者リスク管理に組み込まれたBCM（継続・出口・集中）

BCBSなどの国際的な潮流では、第三者リスク管理は、外部委託管理の延長ではなく、業務継続、代替先への切替、集中リスクを含む運用の枠組みに広がっており、第三者リスク管理の議論が調達や契約の話だけでは完結しなくなっています。BCP/BCMの観点からは、以下の問いに「運用として」答えられる状態が求められます。

1 業務継続性の確保

- ✓ 主要な委託先やクラウドが停止した際に、業務を継続するための選択肢（縮退運用、手作業、別チャネル）が具体的に定義され、訓練されているか

2 出口戦略の現実性

- ✓ 代替先の有無だけでなく、代替先切替の実行可能性（手順/データ移行/権限/所要時間）が具体化されており、実際に切替が可能か
- ✓ 契約条項だけでなく、運用として切替できるか

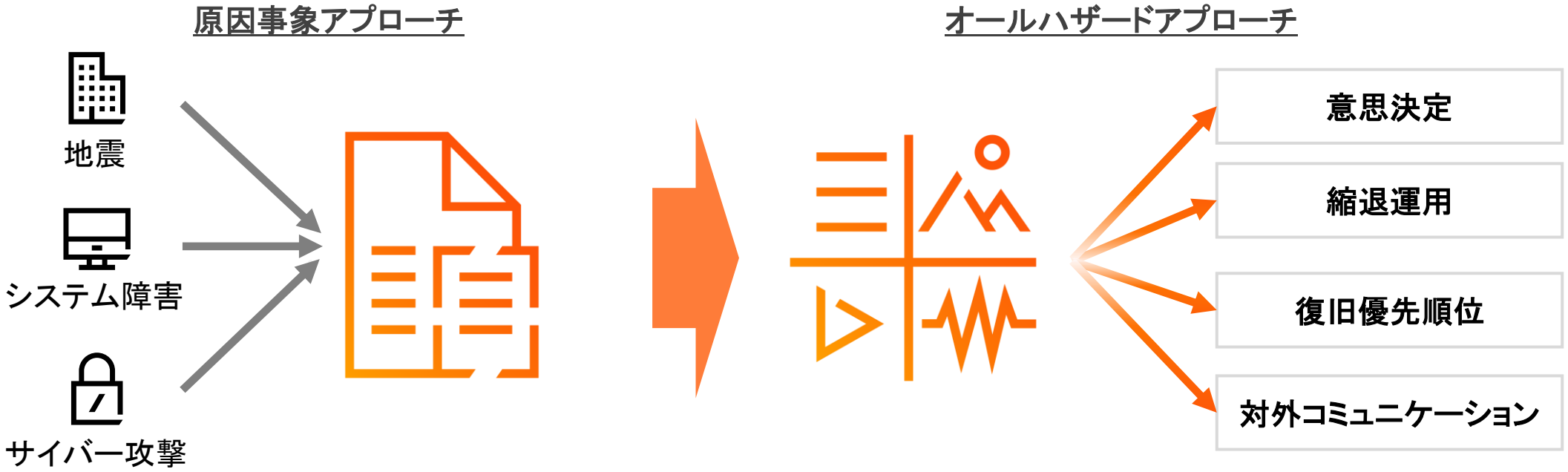
3 集中リスクへの備え

- ✓ 同じクラウド、同じSaaS、同じベンダーへの依存が原因で、複数業務が同時に停止する可能性を前提にできているか
- ✓ その際の復旧優先順位が定められているか

訓練を通じて一度検証してみることで、"代替策が実は動かない"といった問題が可視化され、そこが改善の起点となります

オールハザードへの転換：事象別BCPから「重要業務が止まる状態」を基準に

「地震」「システム障害」「サイバー攻撃」など、原因（事象）別に手順書を整えるだけのアプローチには限界があります。現実の危機は原因が複合し、特定に時間がかかるためです。そこで、「オールハザード」アプローチでは、原因を問わず「重要業務が停止した状態」を起点に、そこから逆算して対応を設計します。



本アプローチは、原因を問わず停止時に動く共通骨格を整えるのに有効です。
一方で、現実の災害との接点が弱くなりやすいため、次頁で紹介するハイブリッドモデルでは、結果事象の土台に原因事象のストレステストを重ねて検証します。

ハイブリッドモデルで「想定外」に備える

ハイブリッドモデルのBCPでは、第1層：結果事象（共通骨格）と第2層：原因事象（ストレステスト）の二層で構成します。
第1層で共通プレイブックを整備し、第2層で南海トラフ／首都直下等を当てるストレステストを実施します。

原因事象アプローチ

「地震」「サイバー攻撃」など、BCPの起点となる特定の原因を想定して対応策を設計する従来型の手法

◎：具体的で実践的、現場が理解しやすい
◎：被害進展や対応フェーズを時系列で描ける
◎：実際の警報と連動した運用設計がしやすい
△：想定外のシナリオには対応しにくい
△：シナリオが増えるほど維持・更新の負担増大
△：依存関係の抜け漏れを見落とす可能性

ハイブリッドモデルの二層構造

結果事象アプローチで土台を作り、原因事象アプローチでその強度を検証することで、両者の視点を補完し合う

第1層：結果事象（共通骨格）
原因問わずに発生する機能損失に備え、代替策や初動手順といった共通部品を整備し、事業継続能力を確保

第2層：原因事象（ストレステスト）
第1層で作った土台が、南海トラフ地震のような大規模複合災害という現実に耐えられるか具体なシナリオを検証

結果事象アプローチ

「重要拠点が使えない」「人員が不足する」など、業務継続を阻害する要因に着目して対応策を設計する手法

◎：網羅的で汎用的。原因を問わず適用可能
◎：人・拠点・IT等の依存関係を横串で整理
◎：対応策を共通化でき、維持・更新が効率的
△：抽象的になりがちで、現場がイメージしにくい
△：実際の災害警報等との連動設計が難しい
△：大規模複合災害への具体性が不足

ハイブリッドモデル導入のための5ステップ

重要業務を"サービス"として確定する
組織単位ではなく「顧客に提供する重要サービス」を切り出し、社会影響や復旧目標（RTO/RPO）を定める

結果事象の設計図を作る（依存関係の見える化）
各サービスが「何を失うと停止するか」を人・拠点・IT・外部委託・インフラに分解し、結節点と単一障害点（SPOF）を洗い出す

共通プレイブックを作る（統制と現場の機能）
「誰が・いつ・何を判断し・どう動く」を標準化。特に対策本部運営、情報収集、外部・対外連絡の手順を明確にする

原因事象シナリオで"ストレステスト"をする
南海トラフ地震のような広域複合化・本社機能損失シナリオを使い「計画の前提が崩されないか」を確認する

改善を"能力"として定着させる
発見した課題を文書修正で終わらせず、訓練・教育・規程・制度・変更管理の仕組みが落とし込み、実効性を確保する

訓練設計：状況付与型から「判断主導型」へ

訓練の質はシナリオの細かさではなく、「何を判断させるか」の設計精度で決まります。プロセスを逆転させ、問いを先に定義することがよりよい訓練設計の一歩となります。

従来型の訓練設計アプローチ（状況先行型）

シナリオを時系列で細かく作り込むことに注力しすぎる傾向がある

台本の読み上げや手順の確認のみに終始してしまい、予定調和な対応になりがち

結果として、想定外の事態における「判断力」が養われる機会がほとんどない

詳細なシナリオ → 手順の確認 --> × 思考停止..

新しい訓練設計アプローチ（判断主導型）

1. 判断（Decision）を先に設計する
   - 「誰が、何を、どの情報で決めるか」を訓練のゴールとして固定（情報不全下でのサービス停止判断など）
2. 状況（Situation）を後から作る
   - その判断を難しくするための阻害要因（情報の欠落、二律背反、優先順位）をシナリオとして肉付けする

判断の定義 → 状況の付与 → ✓ 意思決定力の強化

シナリオ設計のフレームワーク：目的・判断・問い・成果物の4要素

訓練シナリオは読み物ではなく「設計図」となります。次の4つの要素をセットで固定することで、再現性と評価可能な品質を担保することができます。

1. 目的の固定

- 抽象的な「対応力向上」ではなく、目的を具体に定義
- 例：復旧見込み不明下でのトレードオフ判断

2. 場面構成

- 時系列を4～5場面に分割
- 「与える情報」と「隠す情報」を制御し、意図的な情報の非対称性を作る

3. 判断点の設計

- 判断事項：何を決めるか
- 判断者：誰が決めるか
- 判断材料：必要な情報は何か
- 選択肢：A案／B案の葛藤

4. 成果物の定義

- 議論だけで終わらせない
- 「決定メモ」「告知骨子」「方針案」など、その場でアウトプットを作成させる

このシナリオ設計のフレームワークにより、シナリオ作成における属人性を極力排除し、サイバー攻撃や広域災害などあらゆる危機テーマにおいて一定の品質を維持した訓練が可能となる

訓練の高度化：目的別に分け、必ずAARで改善に繋げる

訓練を単一の方法で済ませると、検証できる範囲が限られます。目的別に訓練を設計し、必ず振り返り（AAR）で具体的な改善アクションに接続することが、BCMを機能させる鍵です。

目的別の訓練アプローチ

（1）机上訓練（テーブルトップ）

目的：経営判断（意思決定）、復旧の優先順位付け、部門間の情報共有、対外説明の妥当性を検証する

焦点：情報が不完全な中で、どこまで意思決定できるか

（2）実地訓練（切替・復元）

目的：手順書の実効性を「時間」で測定する

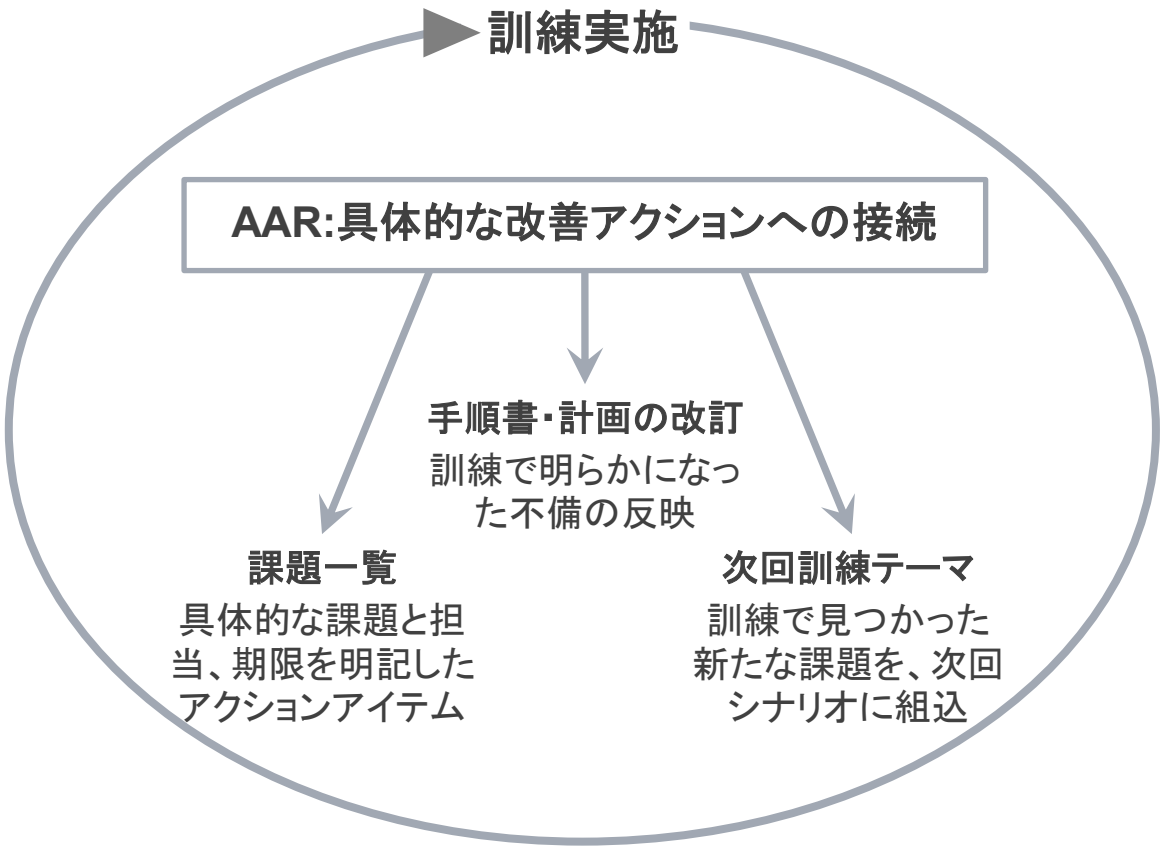
焦点：復旧に必要な権限、環境、依存関係、実際の作業時間を計測し、計画上のRTOのギャップを明らかにする

（3）合同訓練（委託先・関係機関を含む）

目的：組織の境界で発生する連携の課題を特定する。

焦点：連絡経路、役割分担、判断の連鎖、切替時の実務的な問題を洗い出す

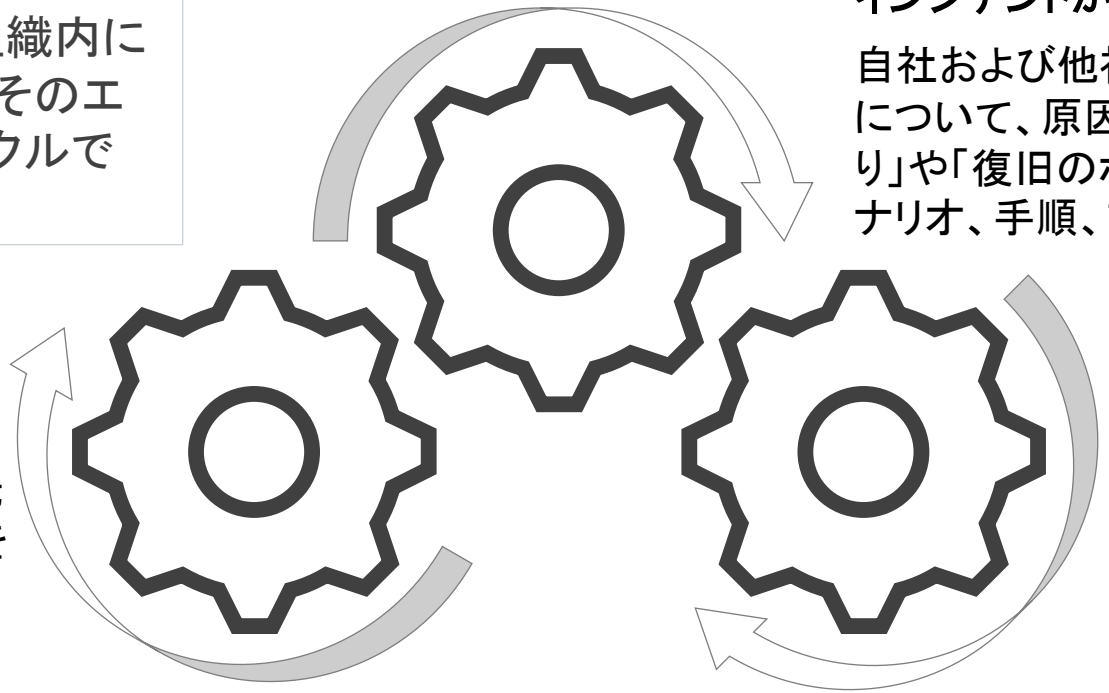
After Action Review（AAR）



継続的改善：BCPの陳腐化を防ぎ、"生きている仕組み"として回し続ける

BCPは一度作れば終わりではなく、環境変化とともに陳腐化します。インシデントからの学び、定期的な見直し、そして第三者との連携のサイクルを回し続けることこそが、BCMの本質となります。

真に実効性のあるBCMは、改善を続けるための「エンジン」を組織内に組み込むことで実現します。そのエンジンは、以下の3つのサイクルで構成されます



インシデントからの学習

自社および他社で発生したインシデントや障害について、原因究明だけでなく、「判断の詰まり」や「復旧のボトルネック」を分析し、自社のシナリオ、手順、訓練テーマに反映させる。

変化起点の見直し

連絡先、権限、依存関係は常に変化する。組織変更、システム更改、委託先の変更、クラウド環境の変更などをトリガーとして、BCPへの影響を評価し、更新するプロセスを業務に組み込む。

第三者との連携

重要な委託先やサービスプロバイダーとは、平時から障害発生時の連絡・連携体制を確認。連絡経路、エスカレーション手順などをテーマに、合同訓練や机上確認を実施する。

このサイクルを回すことで、オペレジ（守るべきものを決める）、第三者リスク管理（委託先を管理する）、BCP/BCM（具体的な対応を準備する）が分断されず、同じ「重要業務の継続」という目的のために一貫して機能するようになります

ご清聴ありがとうございました。

PwC Japan有限責任監査法人
ガバナンス・リスク・コンプライアンスアドバイザリー部

Manager
早道　友詩
yuta.hayamichi@pwc.com　070-5465-8029

Manager
小平 秀明
hideaki.kodaira@pwc.com　080-9151-3799

pwc.com