

オペレーショナルレジリエンスの 基本的な考え方と内部監査

2023年12月



本資料および説明は一般情報であり、特定の目的に対する助言を提供するものではありません。

資料上の記載、説明は特定の組織、事案について言及するものではありません。

本資料および説明は説明者が所属する組織の公式な見解を表すものではなく、記載の正確性について保証するものではありません。

本資料および説明の利用は利用者の責任においてなされるものであり、説明者およびその所属する組織は一切の責任を有するものではありません。

本資料の無断の引用、転載は許容されません。

目次

- 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のフレームワーク
- 各国当局の動向
- オペレーショナルレジリエンスのプロセス
- レジリエンスカルチャー

オペレーショナルレジリエンスとは ~いまオペレーショナルレジリエンスが求められる理由

ビジネスやステークホルダーを脅かす不芳事例(1/2)

業種を問わず、サイバー攻撃やシステム障害等、ビジネスやステークホルダーに多大な影響を与える事象が発生している。

- ・システム障害によるATMや予約システムなどの機能停止

- ・サイバー攻撃による鉄道の運休や工場の稼働停止

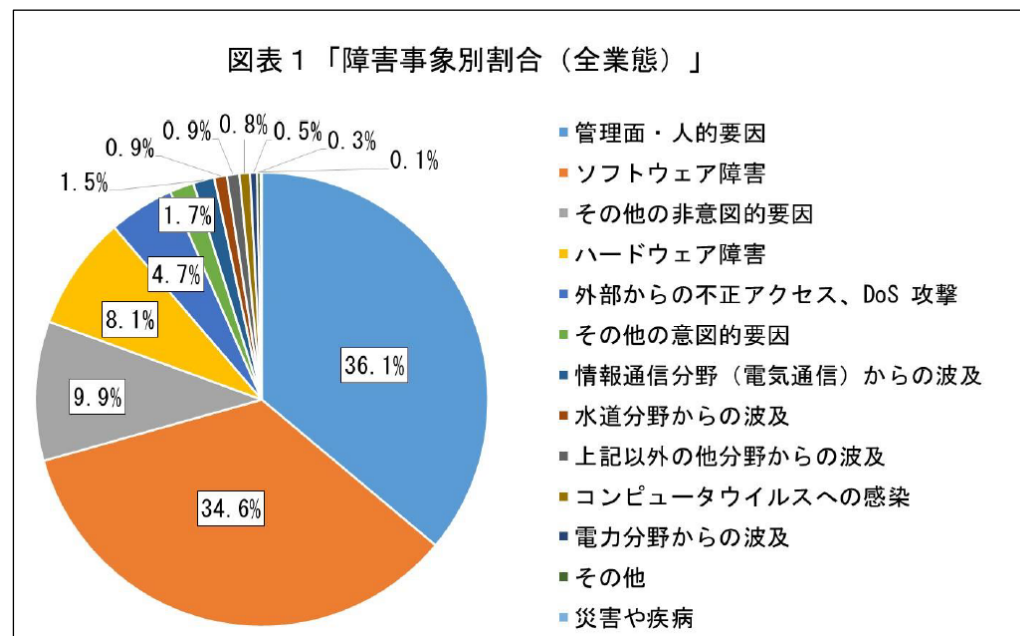
- ・サーバーへのアクセス急増やアプリの不具合によるサービス断絶

ビジネスやステークホルダーを脅かす不芳事例(2/2)

- 金融庁が2023年6月に公表したシステム障害分析レポートによると、2022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1,900件(前年度比 +200件)。
- 外部委託先含む金融機関へのサイバー攻撃やデータセンターの障害によって、サービスが一時的に停止しており、障害発生時に準備していたシステムの冗長構成が機能せず復旧に想定以上の時間を要した不芳事案も多数発生している。
- レポートでは、障害の未然防止にとどまらず、障害発生時の業務の早期復旧や顧客影響の軽減の強化を一層求めている。

金融機関全体における障害事象の内訳(2022年度)

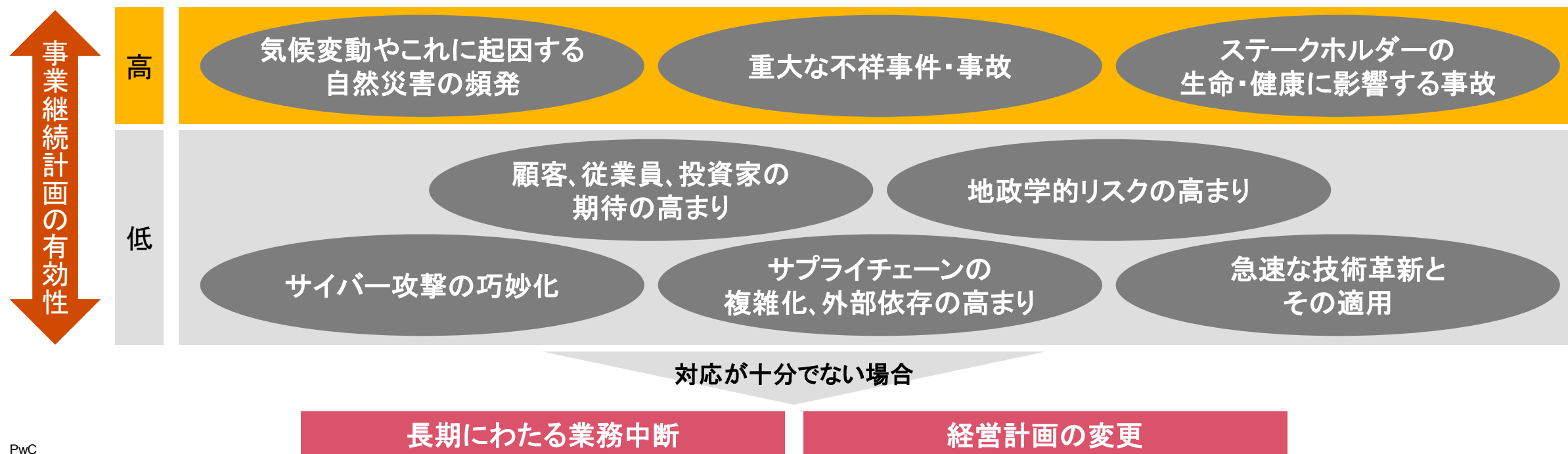
【出所】
金融庁, 2023, 『金融機関のシステム障害に関する分析レポート』
<https://www.fsa.go.jp/news/r4/sonota/20230630-2/20230630-2.html>



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る。

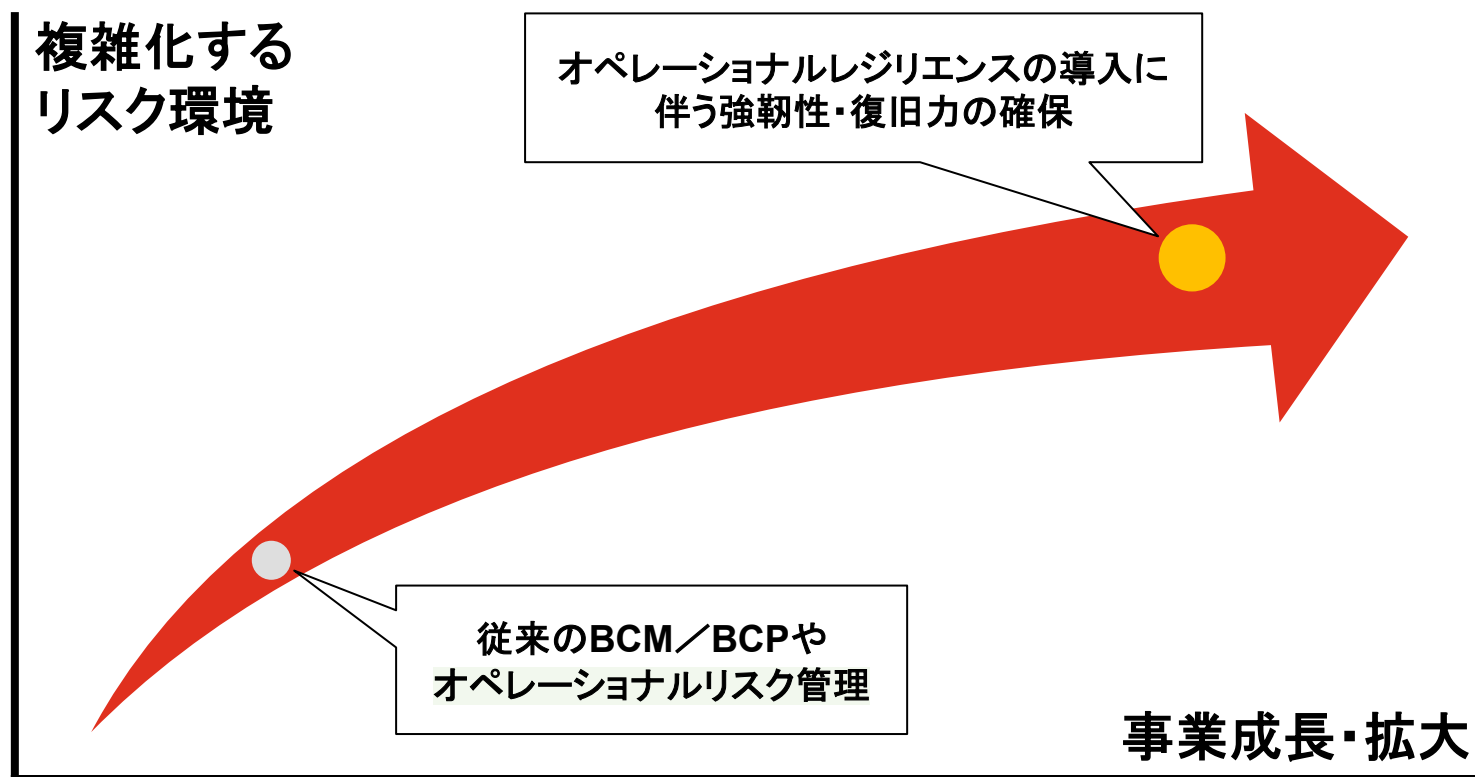
既存のBCM/BCPで想定していなかった事象が生じた場合、顧客や市場に深刻な影響を与える重要な業務を提供できなくなるおそれがある。未然防止策を尽くしてもなお、業務中断が生じることを前提に、利用者目線で早期復旧・影響範囲の軽減を確保する枠組みが国際的に議論されている。



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(業務の強靱性・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、重要な業務を、最低限維持すべき水準において、提供し続ける能力をいう。

企業は従来のBCM／BCPの取り組みや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る。



オペレーショナルレジリエンスが求められる背景

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、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、事業のレジリエンスを発揮することが強く求められている。

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 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	③ 先端的な重要技術の開発支援 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 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	④ 特許出願の非公開 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、



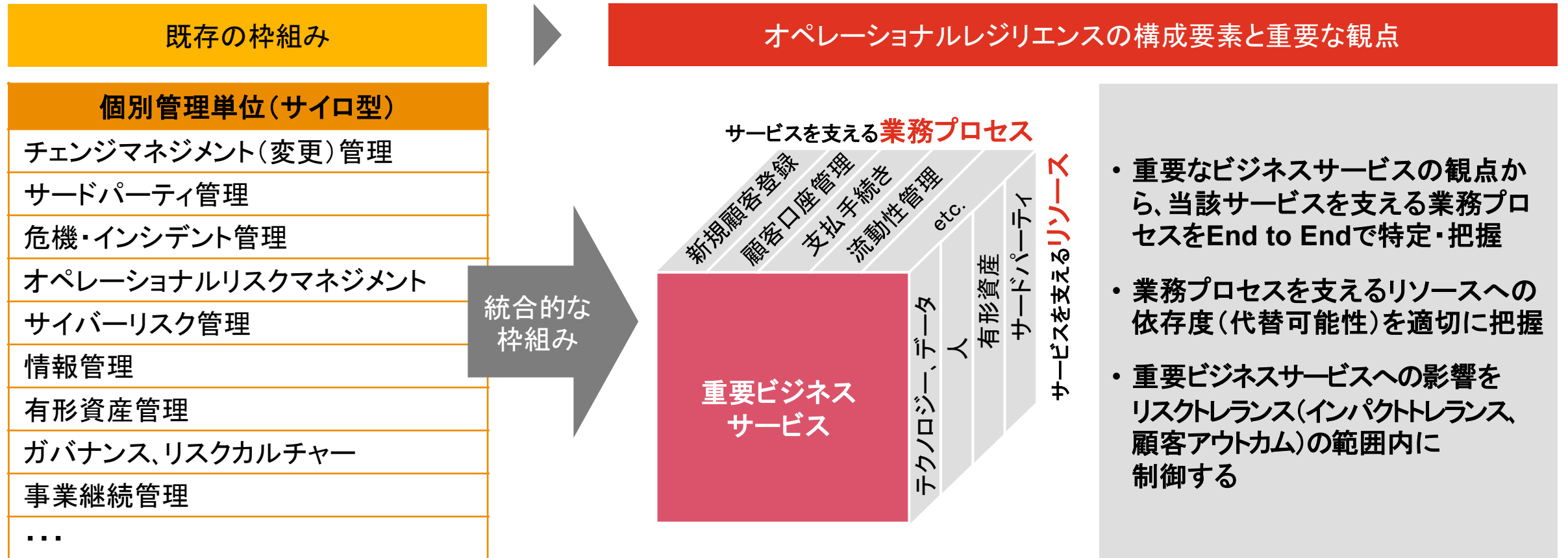
よって、基幹インフラ事業は、

- **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）

オペレーショナルレジリエンスのフレームワーク ~今までのBCP／BCMでは何が足りないのか

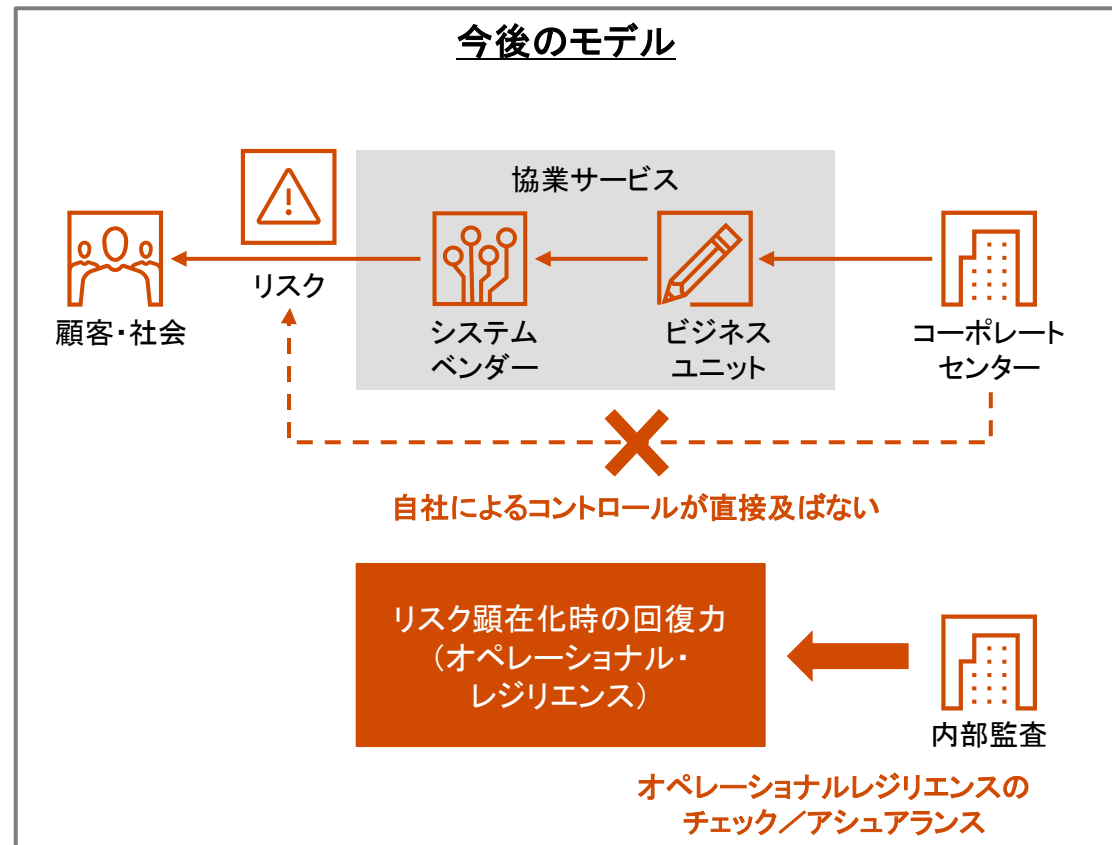
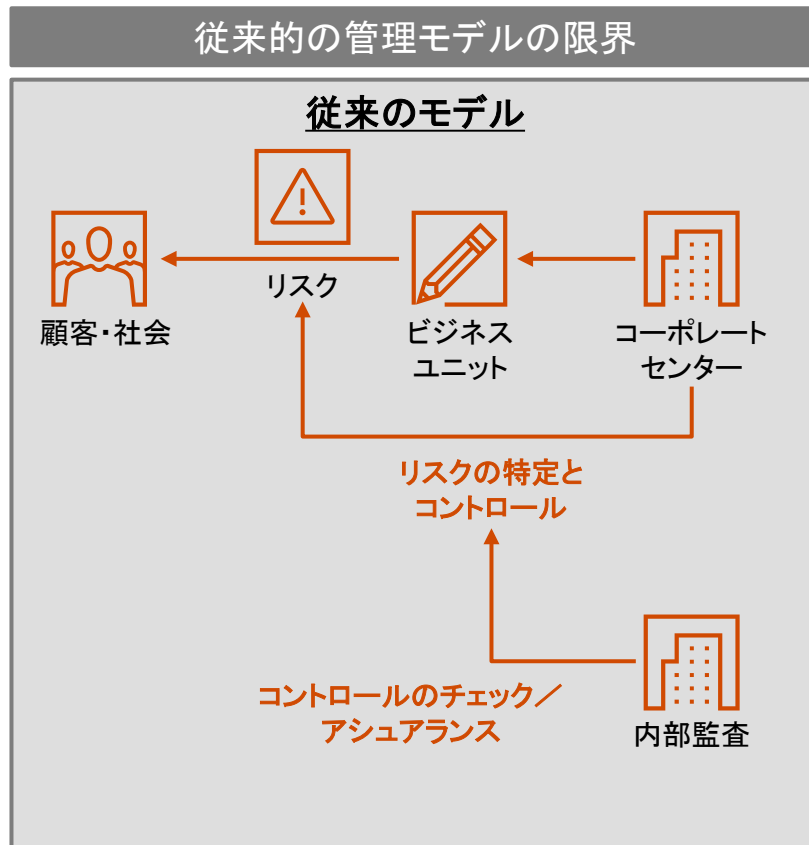
オペレーショナルレジリエンスに対するアプローチ

これまで金融機関や各事業体は、主にシステムなどの自社機能や部門単位に基づいて、個別管理単位で回復プロセスを策定してきた。しかし、オペレーショナルレジリエンスの観点からは個別管理単位ではなく、統合的な枠組みで取り組む必要がある。その枠組みでは、ステークホルダー、顧客、市場全体にとって重要なビジネスサービスという視点から、サービスを支える業務プロセスとリソースを構成要素として整理できる。



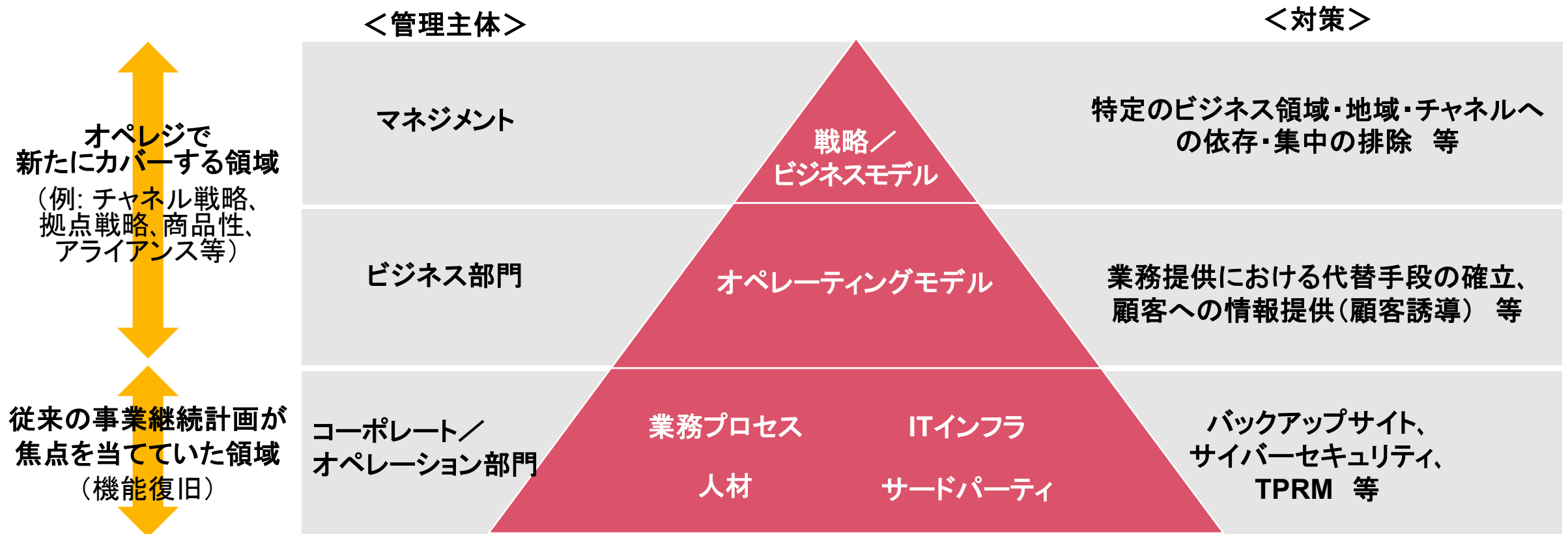
オペレーショナルレジリエンスに対するアプローチ

Fintech企業などとの協業によるサービス提供に関するリスクは自社の外にも広がっており、従来の自社のコーポレートセンターによるコントロールおよびそのモニタリングを中心とした統制では十分とは言えない。このようなリスクについては、顕在化を前提に、いかにサービスを回復、継続するか(=レジリエンス)が大切になる。



オペレーショナルレジリエンスに対するアプローチ

戦略／ビジネスモデル、オペレーティングモデルに内在する、オペレーショナルレジリエンスに係るリスク(リスクドライバー)を考慮し、また戦略／ビジネスモデル、オペレーティングモデル自体にレジリエンスの打ち手を組み込むことが重要である。特に機能復旧に焦点を当てるのではなく、冗長性の観点で代替措置を整備することが重要となる。



オペレーショナルレジリエンスとリスク管理の関係

オペレーショナルレジリエンスは危機事の対応のみを想定したものではなく、平時(事前対応)からの延長としてリスク発生時(危機事対応)の重要サービス提供の継続性を担保するための仕組みになる。そのため、平時と危機時をシームレスに結びつけたフレームワークの構築が重要となる。

	平時		危機事	
	リスク管理		重要サービスの中断	著しい財務状況の悪化と業務中断
目的	中断を発生させるリスクの識別、抑止	業務の継続	中断時のレスポンス、復旧	破綻リスクの対応
ケーパビリティ	オペレーショナルリスク管理	オペレーショナルレジリエンス		リカバリープラン
管理単位	リスクタクソミー	重要ビジネスサービス		重要機能
プライオリティ	損失やレピュテーション毀損を抑える	顧客、市場の利益の保護		財務安定性

オペレーショナルレジリエンスとBCP／BCMの違い

オペレーショナルレジリエンスはトップダウンアプローチであり、経営の意思決定(リスクアペタイトを考慮した顧客へのサービス提供に係るレジリエンスの程度)を支援する管理フレームワークに位置付けられる。

	BCP／BCM		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
影響の捉え方	組織	銀行・株主への影響中心	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・機能ベース	詳細な業務・プロセス等のレベル	ビジネスサービスベース	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したアプローチ	水平型	組織横断的なEnd-to-Endの業務プロセス全体
レポートイング	コンプライアンス	方針・規程に従った報告	ビジネス上の意思決定	データを用いてレジリエンスに関する能力を報告
アウトプット	BCP		リスクプロファイル(リスクアペタイトとの整合、変更)	
目的	備える(ことによる安心・安全)		顧客への提供価値に関する意思決定	

監督当局の動向

~オペレーショナルレジリエンスの対応はグローバルにも求められている

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る。その多くは概念的な議論が中心だが、一部サイバーセキュリティや外部委託管理面で規制として具体化している例もある。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る。

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。

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、1年間の移行期間を設けるほか、企業がインパクト・トレランスの範囲内で業務を継続させるための、最長3年の追加移行期間が設定された。
- 2022年7月にレジリエンスの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

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BCMI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

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

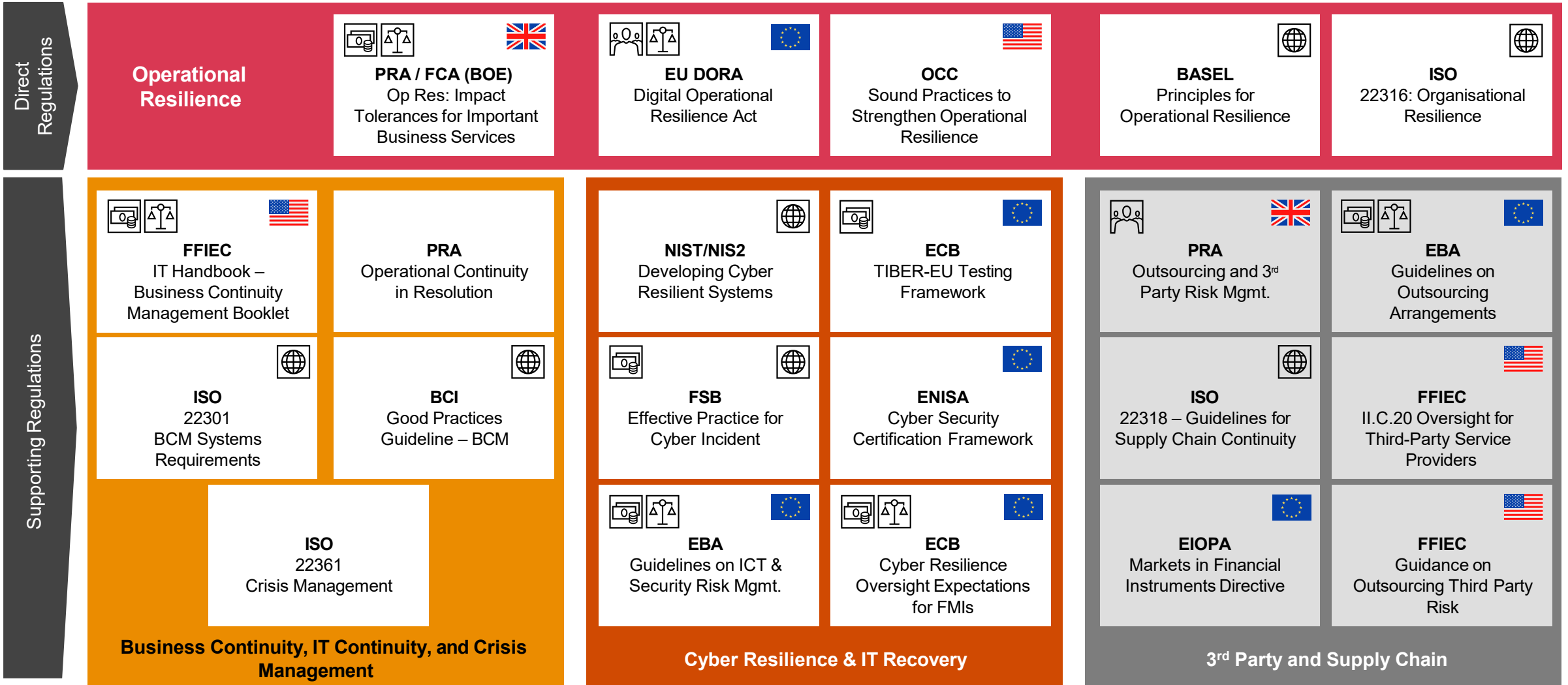
香港(香港金融管理局)



- 2026年5月末までに金融機関に対してオペレジ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ジのフレームワークの構築
 - オペレジのキーパラメーターの特定
 - 基本的なマッピングの完了
- 2) オペレジ構築のタイムラインの設定

オペレーショナルレジリエンスに関する海外監督当局の視点

 International Only
  Legally Binding
  FinServ
  Consultation Paper



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とテストング

- 重要業務(Critical operations)の特定
- 重要な依存関係の特定
- 相互関連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関連と相互依存の把握

- 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

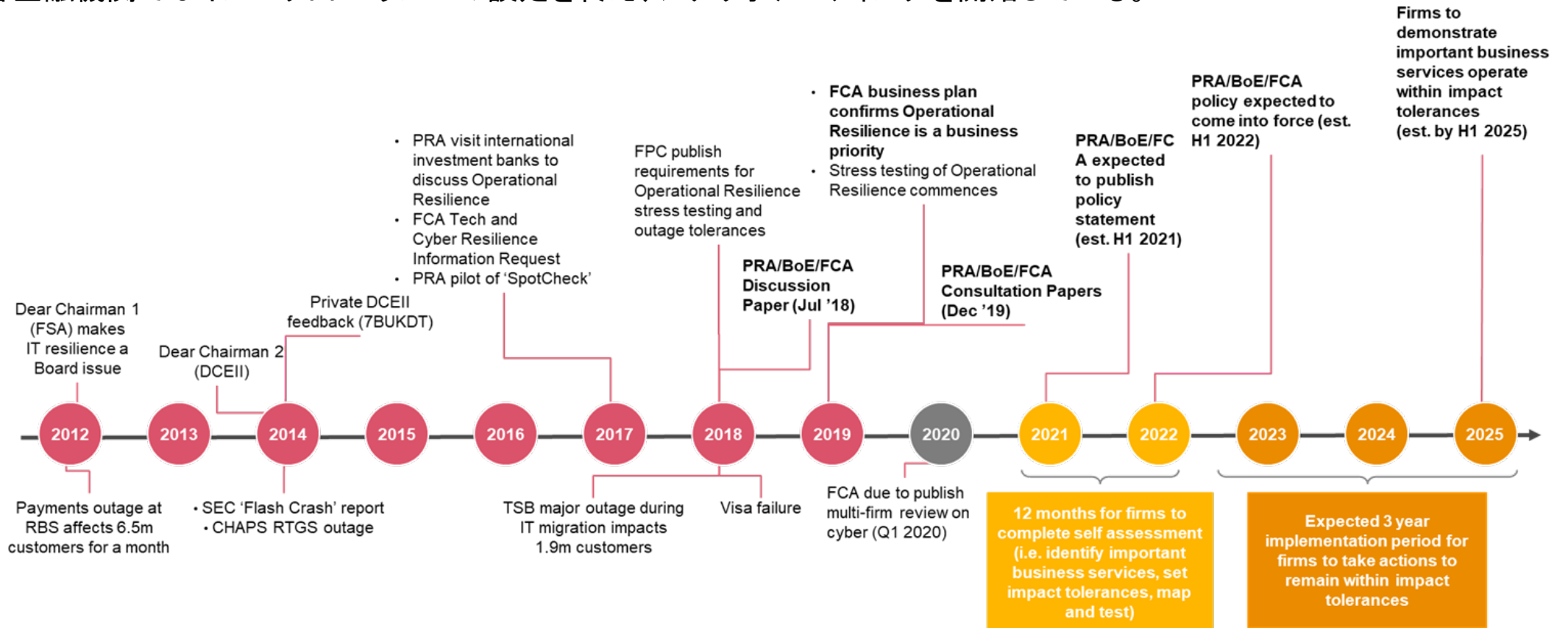
- 情報資産、インフラの管理
- サイバーセキュリティ

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

オペレーショナルレジリエンスに係る海外監督当局の動向(英国)

英国当局PRA/BoE/FCAは、2018年7月に最初のオペレーショナルレジリエンスに関するディスカッションペーパーを発売し、2019年12月に協議文書を公表した。

2021年にオペレーショナルレジリエンスに関する規制化が行われ、2022年に規制の効力が発生している。3年の移行期間を設け、2025年3月には各行が検討してインパクトトレランス内での活動を求められている。現在、各金融機関ではインパクトトレランスの設定を終え、シナリオテストを開始している。



オペレーショナルレジリエンスに係る海外監督当局の動向(EU)

Digital Operational Resilience Act(DORA)の概要

EUの金融業界のデジタルオペレーショナルレジリエンスに関する新しい規制である。

日本企業であってもEU内に拠点を置いている 金融機関、EUの金融機関にサービスを提供しているICTサービスプロバイダーも対象となり、2025年初頭までに本規制に準拠する必要がある。

1. 目的

DORA(デジタルオペレーショナルレジリエンス法)は、EUレベルでデジタルオペレーションレジリエンスのための詳細かつ包括的な規制を定義している。

目的:

EU加盟国間の金融分野における現地規制を調和させ、それによって:

- 金融機関およびICTサードパーティ(TPP)が、あらゆる種類のICT関連の混乱に適時かつ適切に対応し、回復することを確保する
- ICTリスクマネジメントの向上
- 金融監督当局が、金融機関とそのICTサードパーティをより厳格に監視・監査する権限を付与する
- ナレッジシェアを含めた統一的な事故報告の仕組みの導入

2. コントロールエリア

ガバナンス要件:特にマネジメントボードの役割

ICTリスク管理:識別、保護・予防、検知、対策・復旧、学習、高度化・コミュニケーション

ICT関連インシデントを当局に報告する

デジタル運用のレジリエンステスト:少なくとも年に1回実施される独立したテストに使用される評価基準、テスト、方法、手順、ツールの定義

ICTサードパーティのリスク管理:金融機関によるICTサードパーティのリスク監視の要件、重要なICTサードパーティへの監督的枠組みの適用

情報共有:サイバー脅威に関する情報を金融機関間で共有すること

3. 対象事業者



信用機関、保険会社、職業的退職金提供機関、資本管理会社、市場インフラなどを含むEU内の約22,000の金融会社、およびICTサービスプロバイダーなど

オペレーショナルレジリエンスに係る海外監督当局の動向(EU)

DORAのフォーカス分野

DORAがフォーカスする分野は、以下の5つである。

ICTリスク管理

- ICTリスク管理の枠組みは詳細であり、企業戦略や目標に沿ったものでなければならない
- デジタルレジリエンスの戦略を定める必要がある
- 以下に重点を置いて脅威の検知から対応、復旧、通信に至るまで、第一線の防衛能力を強化する:
 - ❖ 脅威のシナリオ・モデリング
 - ❖ サイバー保護と予防
 - ❖ 事業継続・災害復旧コミュニケーション(例:顧客とのコミュニケーション)

ICT関連インシデント報告

- ICT関連インシデント(重要なサイバー脅威)の報告
- ICT関連の重大インシデント(重大なサイバー脅威)に関する初報、続報、最終報告書の提出
- ICT関連インシデント後の根本原因解析の実施
- 必要な改善点の洗い出しと報告

レジリエンステスト

- すべての重要なICTシステムの年次テスト
- 3年に一度の高度な脅威ベースのペネトレーションテスト
- ICTサードパーティプロバイダの参画

ICTサードパーティのリスク管理

- ICTリスクマネジメントのフレームワークへの統合
- マルチベンダー戦略
- 契約上の必須要件
- ICTサードパーティが提供するすべてのサービスの情報登録を行うこと
- 重要なICTサービスの利用状況の変化を報告する
- ICT集中リスクとサブアウトソーシングの評価
- 第三国のICTサードパーティの利用制限

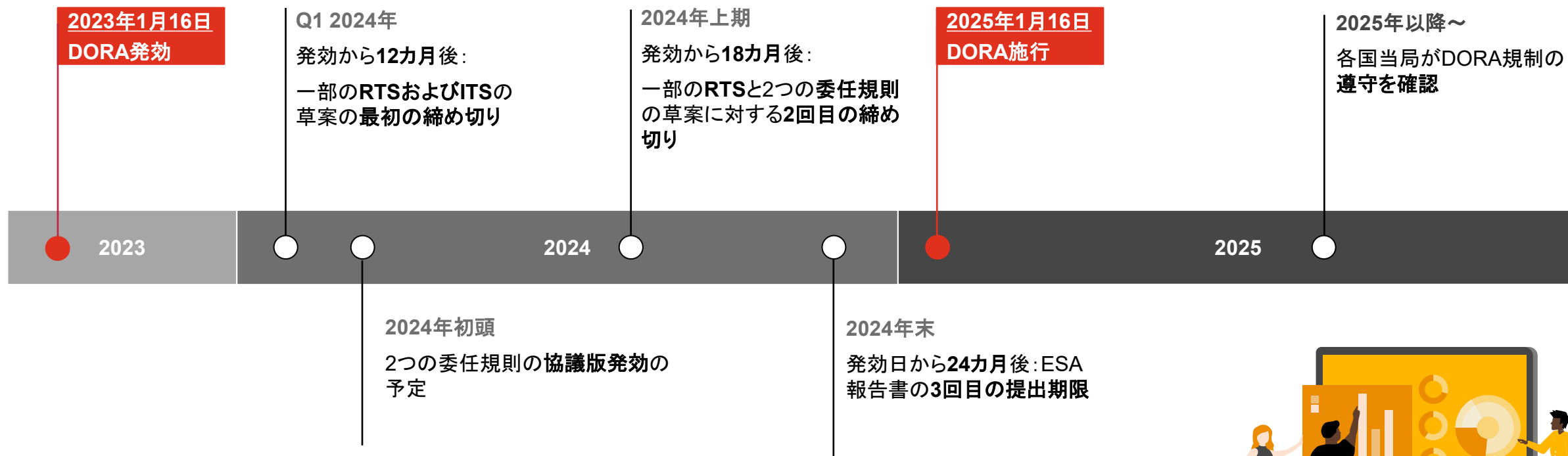
情報共有

- サイバー脅威のインテリジェンスとインサイトを共有し、デジタルオペレーションのレジリエンスを向上させる
- 情報交換に関する協定書(参加条件を含む)
- 当局が共有する情報を検証し、対策を講じる仕組みの導入

オペレーショナルレジリエンスに係る海外監督当局の動向(EU)

DORA施行までのタイムライン

EU(欧州委員会)は、DORAを2023年1月16日に発効した。今後、RTS、ITSといった標準仕様が策定される予定。



*RTS: 技術規制標準仕様 (Regulatory Technical Standards)、
ITS: 技術導入標準仕様 (Implementing Technical Standards)

*Note: 記載されている将来の日付は推定であり、基本的な時間枠を提供することのみを目的としています。

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。

金融庁による オペレジの定義

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 相互関連性のマッピング、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のプロセス

~オペレーショナルレジリエンスのプロセスを経営管理に組み込む

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。

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

- 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

②「耐性度」の設定

- 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

③相互関連性のマッピング 必要な経営資源の確保

- 社外のサードパーティ等も含めて相互関連性をマッピングし、必要なヒト・モノ・カネを特定して採用・配置・配分

④適切性の検証 追加対応

- 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)

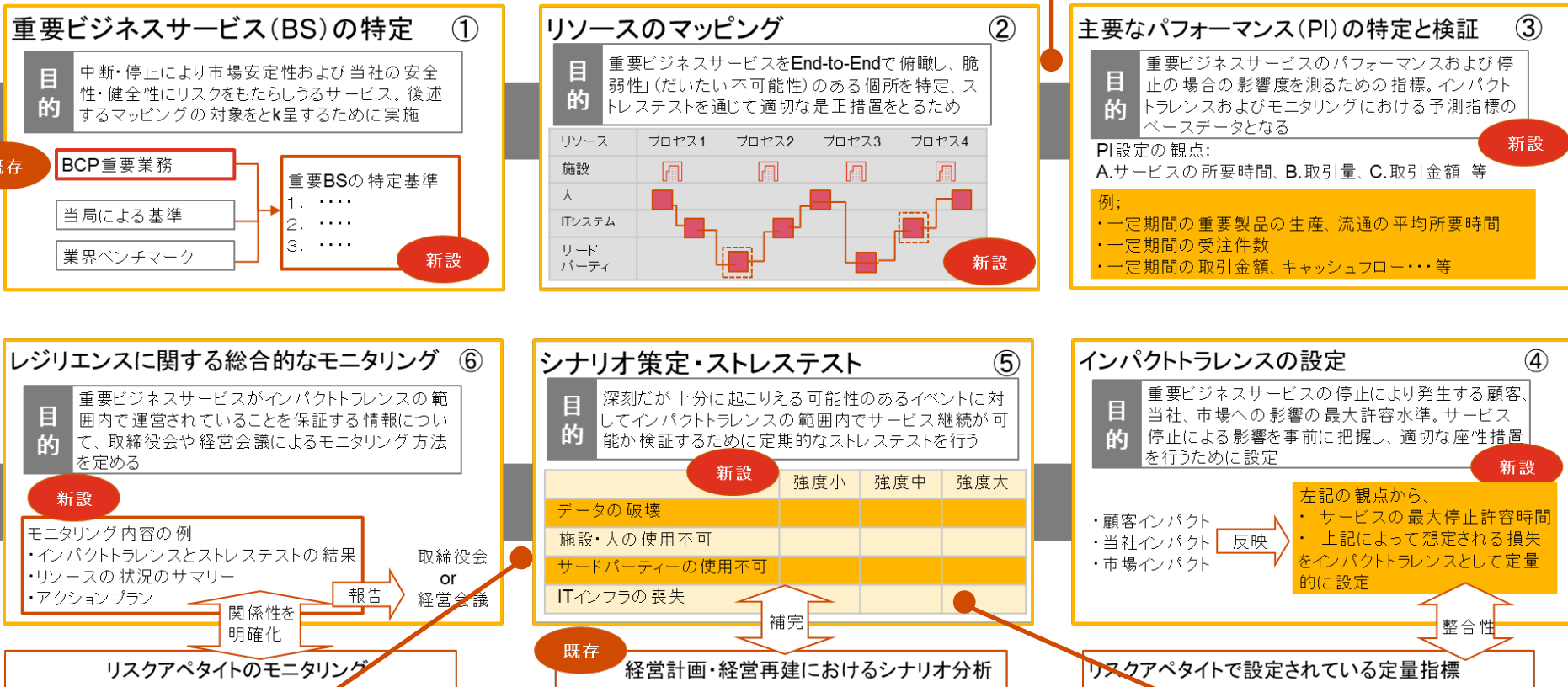
外部環境(金融システムへの影響、市場シェア、利用者数、利用頻度)や自社の規模等の変化に応じて、重要な業務や耐性度も見直しの対象となる

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の管理プロセス

英国監督当局が求めるオペレーショナルレジリエンスの管理プロセス。

BCBSでは、PIの設定に関する記載はないものの、BCPIにおけるRTO等の指標設定、オペレーショナルレジリエンスに係るインシデント管理の中で「パフォーマンス指標」の設定について言及がある



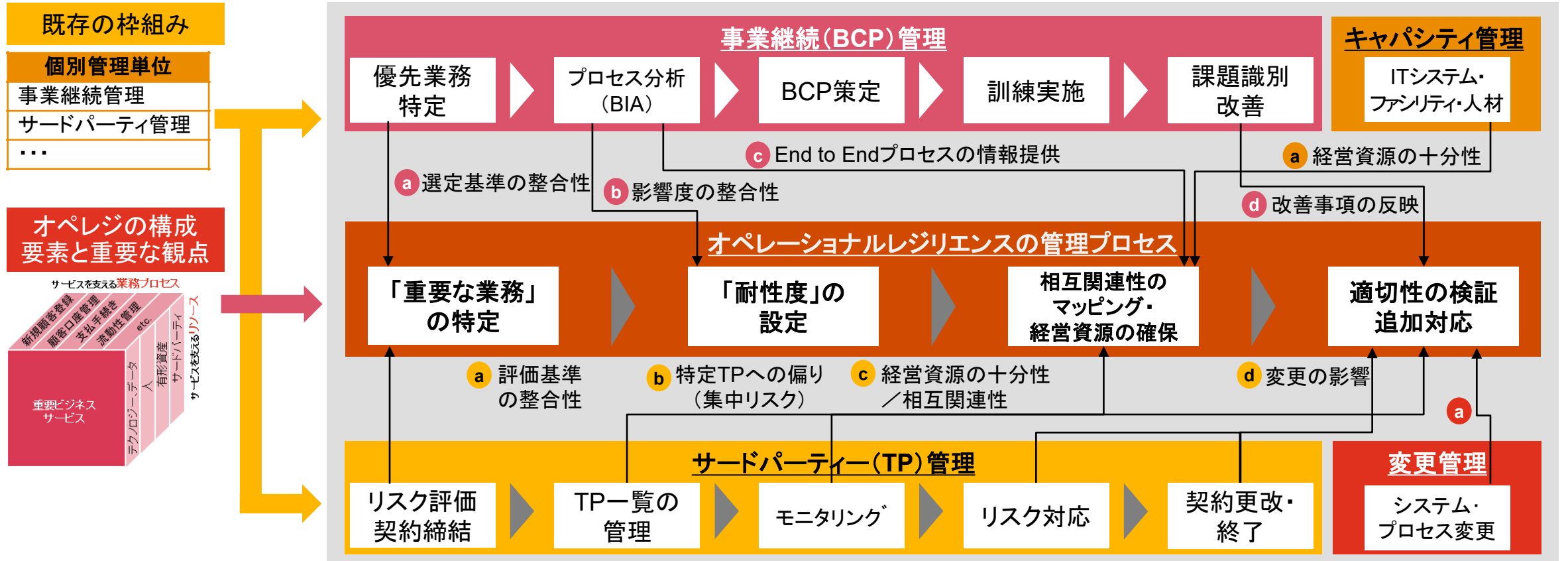
BCBSの諸原則に、シナリオ策定およびストレステストが明確に含まれていないが、「健全なオペレーショナルリスク管理のための諸原則」の中で、オペレーショナルリスク管理のシナリオ分析をオペレーショナルレジリエンスのテストに活用すると言及

FCAは、顧客・市場の観点からトラレンスの設定を求めるのに対して、BCBSは業務中止に対するトラレンスとリスクアペタイト・トラレンスとの整合性を強調する

管理プロセスの構築事例①

大手金融機関にて、金融機関が既存(サイロ型)リスク管理からオペレジが目指す統合的リスク管理への見直しを検討

————— オペレジを機能させるための情報



見直しの観点:

① リスク評価基準が部門により不揃いであり、個別管理単位によって異なる重要性評価がなされる懸念はないか？

② 前提としたTPや業務プロセスを全社網羅的に収集できておらず、業務中断時の影響度分析において欠陥が生じていないか？

③ ④ 策定した復旧策やリスク対応策の実効性が全社横断的に検討されず、想定外の要因(4th Partyの集中、代替策や対応者のキャパシティオーバー等)で失策する懸念はないか？

⑤ 特定された復旧策等の欠陥、各部門や各管理単位で実施された追加対応・経営資源の再配分の内容が全社横断的に共有されず、部分最適に留まっていないか？

管理プロセスの構築事例②

オペレーショナルレジリエンスの観点を取り入れBCPを再整備

課題

従来運用していたBCPは、詳細なシナリオ設定に基づく具体的な対応が業務別に定められているものの、想定していない事象が発生した場合の対応力に課題があった。

対応

業務種別と最大停止許容期間を踏まえ、重要業務を選定し、業務概要や障害発生時の顧客影響、対応方針を整理することで、想定外の事象が発生しても、経営レベルで迅速な対応を可能とした。

重要業務については、既存の個別システムの継続計画と業務の継続計画を融合させ、障害発生時の多層的な対応力強化を図った。

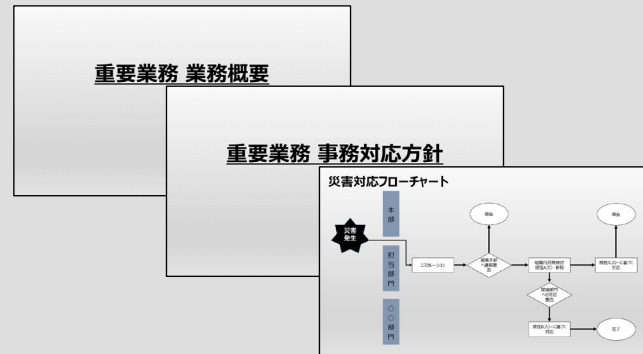
重要業務の選定

業務種別と最大停止許容期間を踏まえ、一定以上の影響度の領域を重要業務として選定し、業務別方針書の作成必須領域とする。

最大停止許容期間 \ 業務種類	重要	通常	その他
	決済業務	決済業務	業務
原則停止不可	影響度A	影響度A	影響度B
半日		影響度A	影響度B
1日		影響度B	影響度B
3日		影響度C	影響度C

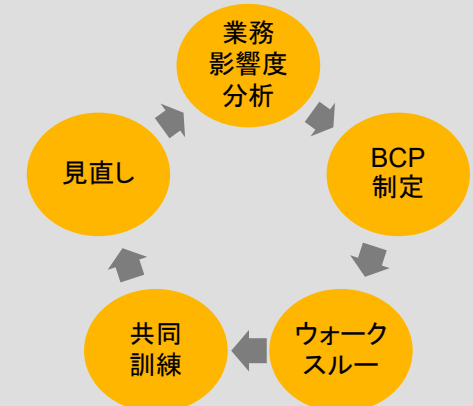
対応方針の整備

重要業務については、業務概要やシステムフロー図を整備し、基本的な事務対応、システム対応、および顧客対応方針を整理する。



PDCAの整備

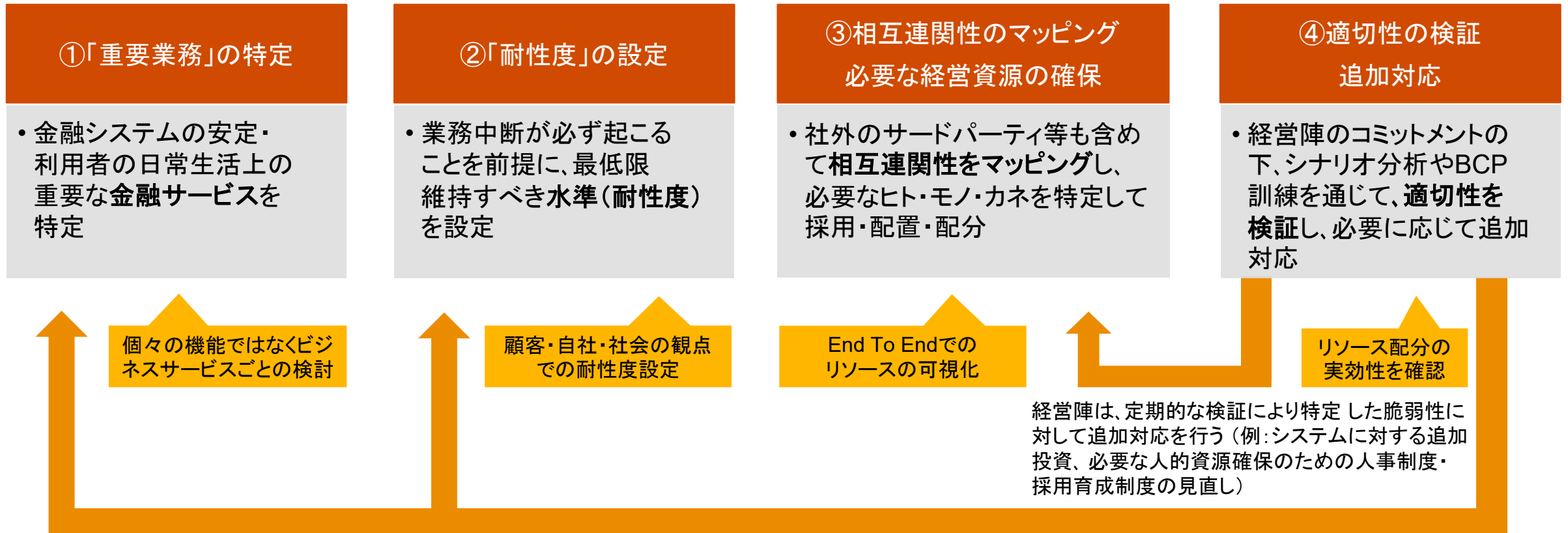
訓練を実施し、年度でのPDCAを通じ、継続的に実効性を向上させる。



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。

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



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)

「重要業務」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自社の安全性・健全性を害したりするサービスを、「重要業務」として特定する。

例えば、銀行の決済業務、ATM現金引出機能等が挙げられる。

特定基準の例

顧客観点：顧客に耐えられないレベルの危害を引き起こす

- 顧客ベースの規模
- 顧客の性質を考慮

社会・市場観点：国の金融システムの安定性へのリスクをもたらす

- 経済全体機能への阻害
- 金融市場インフラや重要な国家インフラを提供する
- カウンターパーティへの影響

自社観点：自社の安全性と健全性にリスクをもたらす

- 企業の損失
- 風評被害
- 法的または規制上の処分

耐性度の設定

耐性度とは、「業務中断が必ず生じることを前提に設定された、重要業務の最低限維持すべき水準」を意味する。金融庁によれば、「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、取引額および利用者数（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」とされている。

重要業務を、業務中断時の影響が異なるプロセスに細分化し、各プロセスにおける耐性度を時間軸で設定した上で、それが現行のBCPで実現できるのかを検証するアプローチが考えられる。

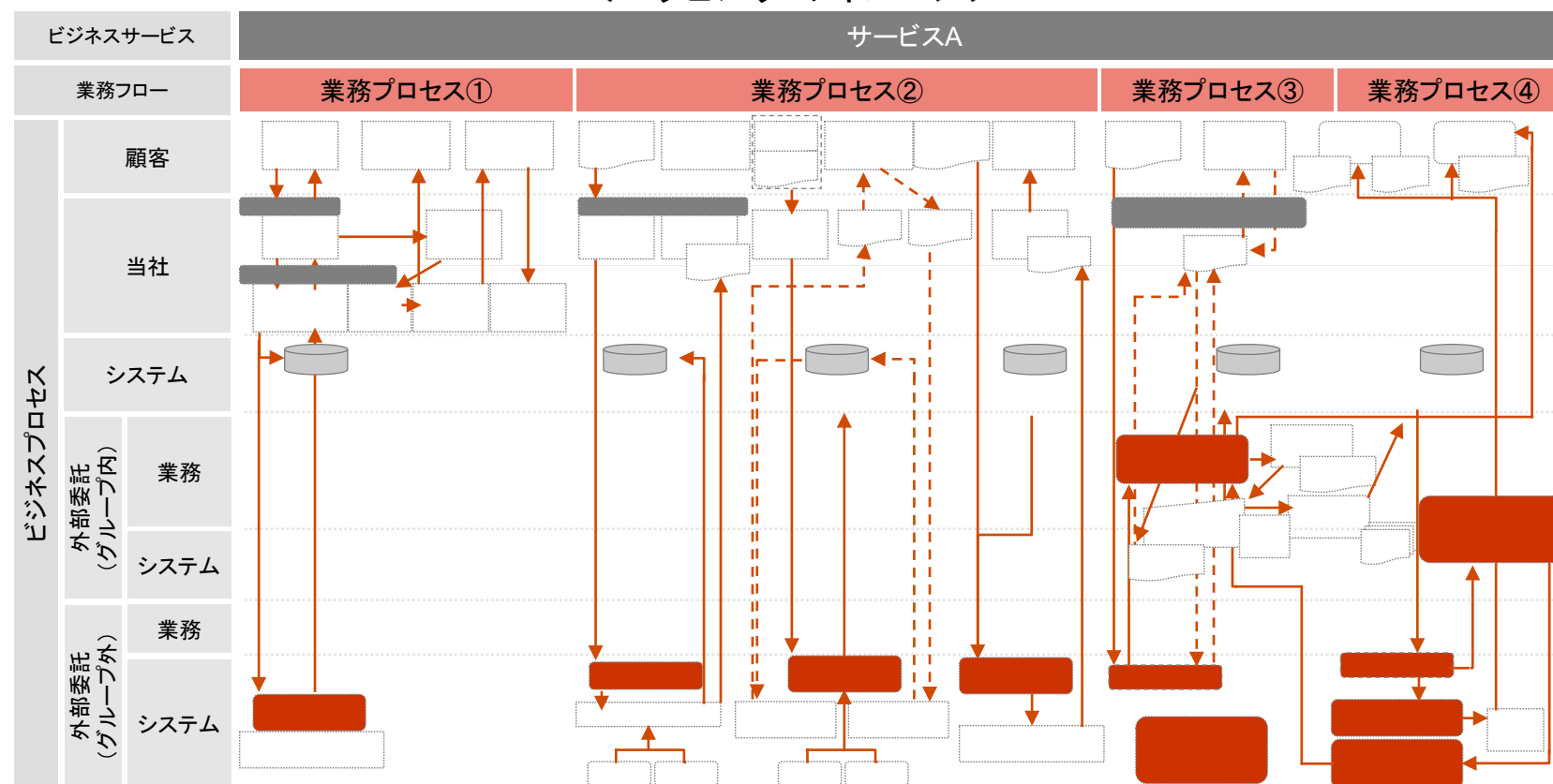
重要サービス	影響度の観点	重要度	時系列での影響度の評価					耐性度
			X時間	X+12時間	X+3日	X+7日	X+14日	
サービスA	顧客	M	影響なし	影響なし	影響なし	影響なし	影響なし	X+14日
	当社		影響なし	影響なし	影響なし	影響あり	重大な影響	
	市場		影響なし	影響なし	影響なし	影響なし	影響なし	
サービスB	顧客	H	影響あり	重大な影響	重大な影響	重大な影響	重大な影響	X+12時間
	当社		影響あり	重大な影響	重大な影響	重大な影響	重大な影響	
	市場		影響あり	重大な影響	重大な影響	重大な影響	重大な影響	
サービスC	顧客	L	影響なし	影響なし	影響なし	影響なし	影響なし	-
	当社		影響なし	影響なし	影響あり	影響あり	影響あり	
	市場		影響なし	影響なし	影響なし	影響なし	影響なし	

相互関連性のマッピング・必要な経営資源の確保

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、それらの相互関連性や相互依存度のマッピングを行う。

マッピングは、重要ビジネスサービスを支えるリソースのうち、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う。

＜マッピングのイメージ＞



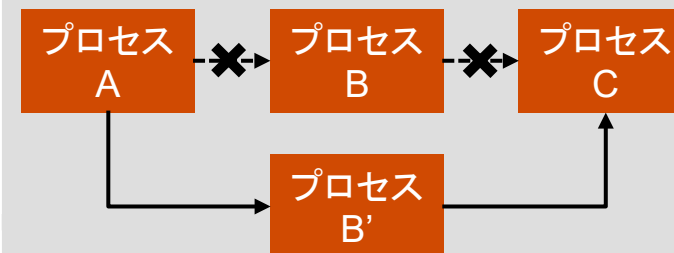
＜冗長性のイメージ＞

重要な業務を継続する為、代替手段として、ネットワークやプロセスの**冗長性**も考慮する必要がある。

単一のプロセス

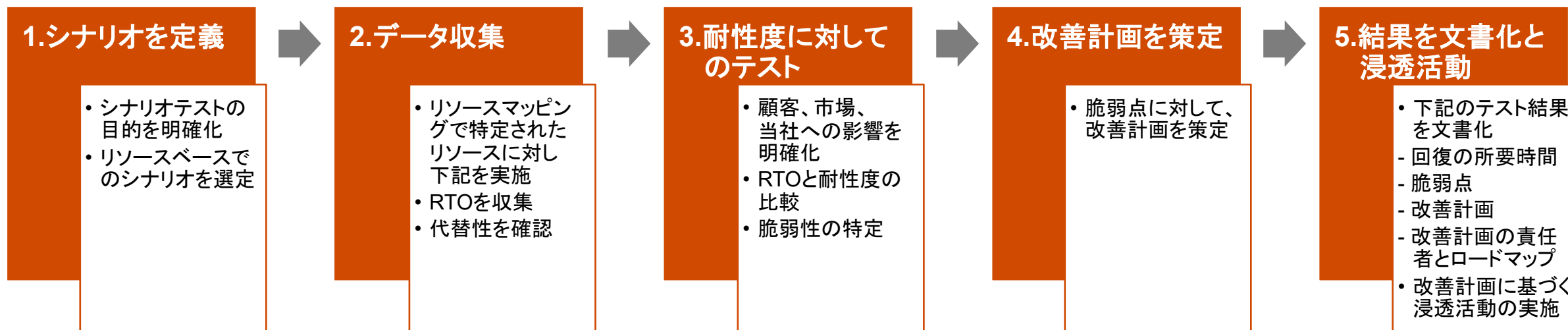


プロセスの冗長化



適切性の検証・追加対応

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、必要に応じて見直しや追加的措置を講じる。



実効性あるオペレーショナルレジリエンスに必要な周辺要素

金融庁のディスカッションペーパーにおいては、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も、紹介している。

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」というオペレジの考え方が親和性が高い。

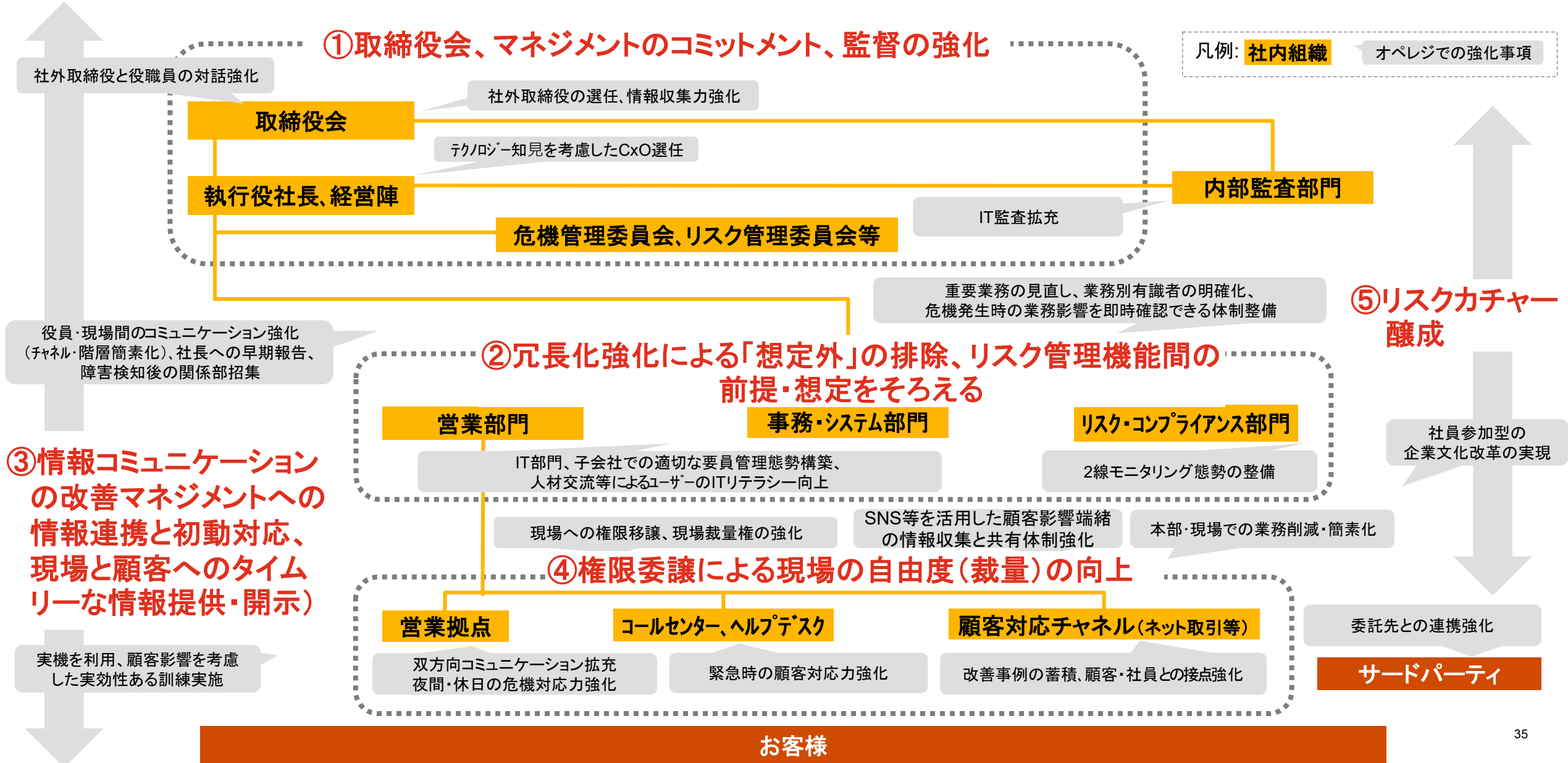
リスクカルチャーの醸成(リスクコミュニケーション)

- 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。

オペレーショナルレジリエンスを踏まえた事業継続管理の見直し例

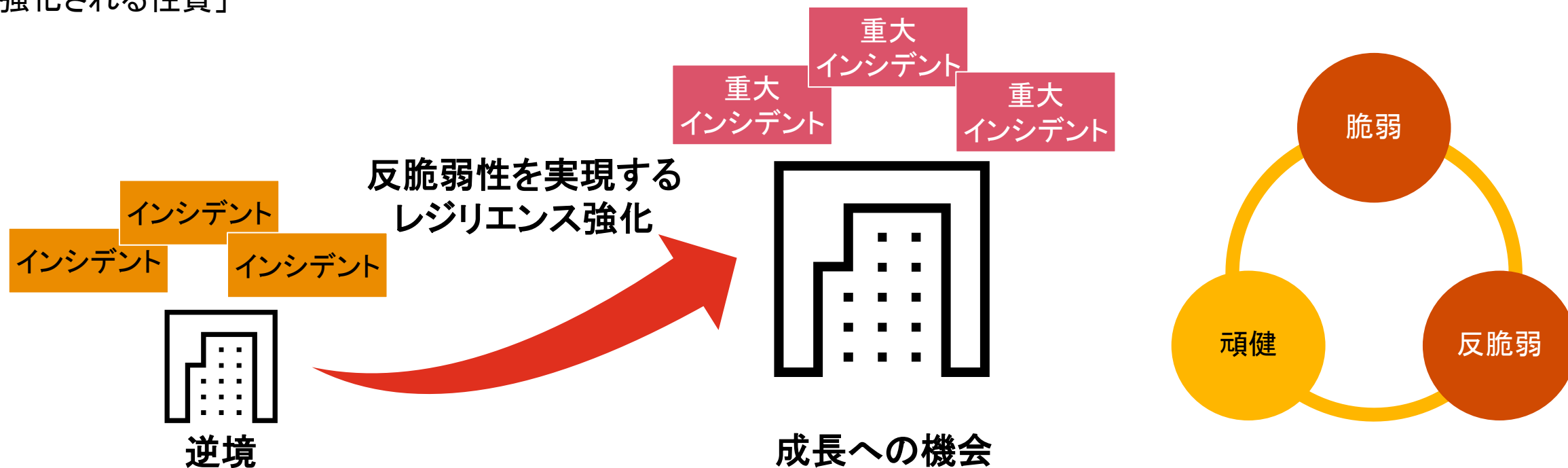


レジリエンスカルチャー ~レジリエンスカルチャーを浸透させる

レジリエンスカルチャー：反脆弱性について

反脆弱性 (Antifragility) とは

ニューロン・ニコラス・タレブによって提唱された概念で、「システムや組織がストレスや混乱に晒されることで、強化される性質」

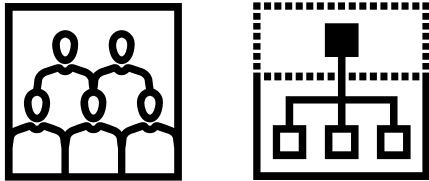


オペレーショナルレジリエンスの取り組みを通じて、単に逆境や不確実性に対して耐え抜くだけでなく、そのような危機を糧にして学び、成長する能力（逆境を機会に変え成長し、より大きな逆境や不確実性に対しても耐える）が重要

レジリエンスカルチャー：反脆弱性について

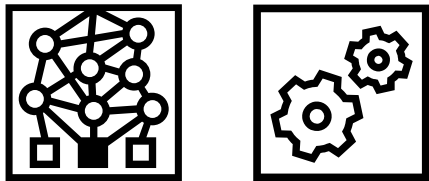
柔軟・強靱(レジリエント)な組織、サービス・業務・システムをイメージすると以下の様になる

組織・体制



- 階層が少ないフラットな組織
- 関与者が限定されている
- 動的に対応が可能（権限含め、意思決定プロセスが硬直的でない）
- 多様性（同質性の排除）

サービス・業務・システム



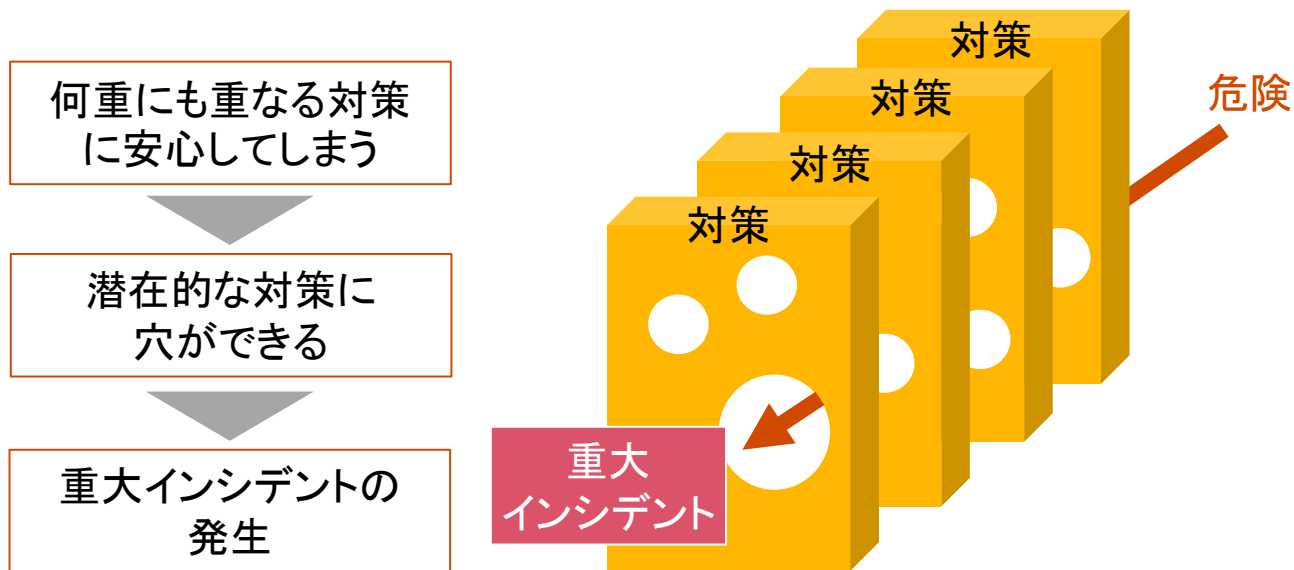
- 相互依存が低い(フィードバック・ループ)
- 分離可能性が高い
- 結果（帰結）の予測可能性
- パラメーターが少ない
- メカニズムが可視化されている
- 直接コントロールができる
- 特定のリソース、技術に依存しない
- 汎用性（代替可能性）が高い

レジリエンスカルチャー：平穩無事に潜む危険と安全文化について

複雑な技術(システム)が絡む組織においては、安全のため、さまざまな対策が何重にも講じられることから、構成員は「平穩無事」な時間が続いているように感じる。しかし、構成員は嚴重な対策が複数用意されていることに安心してしまい、小さな問題を見過ごしてしまう可能性もある。英国の心理学者J・リーズンは、このような安心感(潜在的な対策の穴)の連鎖が、表面的な平穩を崩し、重大なインシデントを起こしてしまうとした。

また、安全向上を組織全体で常に求めようとする「安全文化」こそ、「平穩無事に潜む危険」を防ぐ良好な組織文化としている。

<平穩無事に潜む危険>



<安全文化の5つの要素>

- ①情報に基づく文化 (Informed Culture)
安全に関する情報を分析・収集し、積極的に発信する文化
- ②報告する文化 (Reporting Culture)
問題や脅威に関する情報を安心して共有できる文化
- ③公正な文化 (Just Culture)
行動の是非についての境界線が明確な文化
(故意ではないエラーまで非難されない)
- ④柔軟な文化 (Flexible Culture)
変化について、効果的に適応できる文化
- ⑤学習する文化 (Learning Culture)
失敗から学び、変化を促す文化

レジリエンスカルチャー：リスクの本質、実態をとらえた対応

リスクに対する考え方としてフレームワークを作り厳格に管理するタイプ1の考え方がある。一方で、リスクに対して柔軟性をもって対応する考え方として、人が現場で時々の状況に即した対応をとることで実効性を高めるタイプ2によるリスク管理の考え方も存在する。

レジリエンス工学における安全の考え方

	タイプ1	タイプ2
安全の定義	悪い方向へ向かう物事ができるだけ少ないこと	できるだけ多くのことが正しい方向へ向かうこと
安全管理の原則	何かが起こったときに、反応し、応答する	事前対策的、発展や事象を予期するように努める
事故の説明	事故は失敗や機能不全が原因で起こる	結果によらず、物事は同じ方法で起こる
ヒューマンファクターの見方	責任	資源

リスクカルチャーのフレームワーク

リスクカルチャーとは「従業員のリスクに対する考え方や認識、行動の全体」のことを言い、以下の要素から構成される。

プロセスと統制の確立

ビジネスプロセスが有効に管理され、統制がビジネスの複雑さや変化に対応している

リスクの特定・評価

リスクを特定・評価する明確なプロセスがあり、リスクがどう評価され、管理されるか明確なフレームワークがある

能力の確保

スタッフは自らの役割を担うのに必要な知識、経験、能力を有しており、継続的に改善している

情報とコミュニケーション

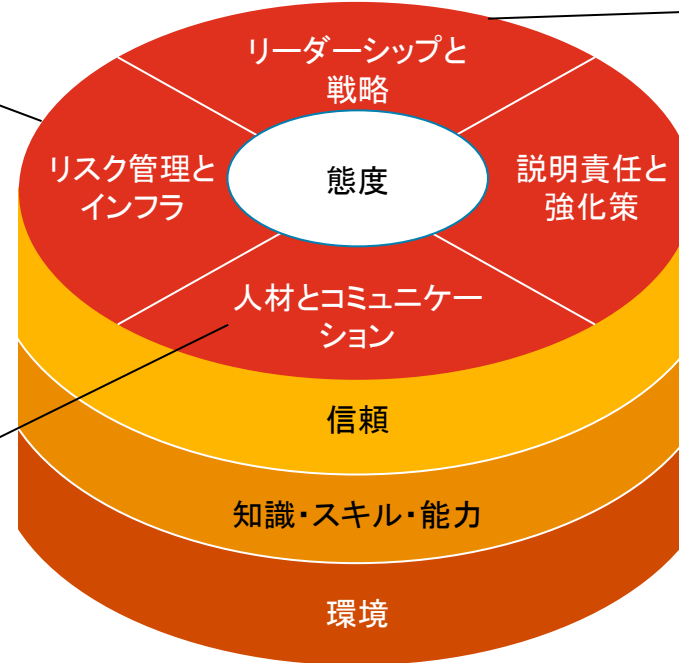
コミュニケーションとシンボルは組織の価値、倫理観、態度を強化する
部門間コミュニケーションが有効

成熟度レベル

環境: 組織は、リスクにどう対応するかを示すために、方針・プロセス・システムなど適切なインフラを備えている

知識・スキル・能力: リスク管理方針や手続きが何を意味するかを的確に理解している。リスクを特定し対応するスキル・能力を有する

信頼: リスク管理が信用でき価値のあるものと理解されている。知識を持ち、リスク管理において正しいことが何を示すプロセス・手続きが自然に運用されている



誠実性・倫理感

倫理感や価値観は態度に表れる
それらはマネジメントにより強化される

ミッションと目的の伝達

戦略が明確で伝達もされている。スタッフは自らの目標が組織の戦略や事業部門にどう関連するか理解している

権限・責任

役割と説明責任が明確に定義され、全てのスタッフに伝わっている
スタッフは何を意思決定でき、何は上程が必要かを理解している

人事方針・手続きおよび評価手法

リーダーとスタッフは自らへの期待値と自らの目標を持っている
リーダーはスタッフを監督・育成し、適切な態度に向けて指導する

オペレーショナルレジリエンス(OR)を内部監査の視点で捉えると

- 監査ユニバースにおいて、重要業務(重要ビジネスサービス)を取り込む
少なくとも〇年に一度は重要業務をカバーすることによる保証提供など
- リスクアセスメント(残余リスク)において耐性度(リスクトレランス)の考慮
耐性度の範囲内に残余リスクが収まっているのかを確認。(監査評定、意見に反映)
通常のコントロールの有効性を超えた負荷(ストレス)をかけたときの残余リスクを想定する必要
- 監査テーマ、対象設定においてEnd to Endで監査スコープを設定
プロセスフローチャートなどを作成する際には重要なリソースもカバー
- ORに関連するリスク管理フレームワークの監査の際にはORの視点を含める
サイバーセキュリティ、TPRM、BCP/BCMなどの監査においてORの視点を入れる
逆にORを大きなテーマとして連携させる形で各リスク管理フレームワークの監査を設定する
- ORをテーマ監査として実施する際にはガバナンス(権限、情報伝達含む)、人事制度、カルチャー、PoGも含めて監査
ORのピラミッド(P12)の上位階層への対応
- レジリエントかという視点の監査をする際には「反脆弱性」(P38)の視点を考慮する
DXで解決することは理想であるが、TP/BP含めマニュアル対応も重要

過去BCのインシデント(および「失敗からの学び」)は真因分析に活用

PwC Japan有限責任監査法人

パートナー 辻田 弘志

090-1424-3247 hiroshi.tsujita@pwc.com

www.pwc.com/jp

© 2023 PricewaterhouseCoopers Japan LLC. All rights reserved.

PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.