エンタープライズ・レジリエンス

PwC Japan有限責任監査法人
マネージャー　**ト 信慶**

はじめに

近年、業種を問わず、サイバー攻撃によるシステム障害や地政学的リスク増大による原材料調達の一次的な中断等、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増加しつつあります。特に、自社だけでなく、外部委託先を含むサプライチェーンでの障害時に、準備していた対策が有効に機能せず、復旧に想定以上の時間がかかるケースが多く見られます。

レジリエンス（強靭性・復旧力）とは、このような危機が起きても、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のことです。本稿では、組織における既存のリスク管理のフレームワークにレジリエンスの観点を取り入れた態勢を「エンタープライズ・レジリエンス」と定義し、その態勢づくりのアプローチとプロセスの強化について詳しく説明します。

なお、文中の意見は筆者の私見であり、PwC Japan有限責任監査法人および所属部門の正式見解ではないことをお断りします。

1 エンタープライズ・レジリエンスが求められる背景

以前から、金融機関や事業会社は、事業継続管理（BCM）のフレームワークのなかで、地震や感染症等の特定のリスク事象を想定した事業継続計画（BCP）を整備していました。昨今、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やシステム障害等、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、顧客や社会に深刻な影響を与える重要な業務を提供できなくなる恐れがあります。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フレームワークが国際的に議論されています。

日本国内においては、2022年5月に成立した「経済安全保障推進法」において、「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ます[※1]。また、金融業界においても2022年、金融庁が「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）をディスカッションペーパーとして公表し、2023年6月には「主要行等向けの総合的な監督指針の一部改正」においてオペレーショナル・レジリエンスに関する態勢整備の意義について言及し、国際統一基準の適用を受ける金融機関に対してもオペレーショナ

※1　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）」2022年5月
https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/suishinhou.html

ル・レジリエンスの確保に留意する旨を示しています※2。

2 エンタープライズ・レジリエンスのフレームワーク

有効なエンタープライズ・レジリエンスの態勢を構築するには、ガバナンス、組織、プロセス、インフラの各要素にレジリエンスの観点を組み込むことが重要です。以下では、エンタープライズ・レジリエンスを構成する4つの要素を説明します（**図表1**）。

(1) ガバナンス

トップマネジメントは、有事の際にも重要な業務を維持するために、戦略と態勢を構築する必要があります。有事を含むなんらかの緊急事態の発生時にステークホルダーへの影響を最小限にし、早期復旧することはもちろん重要ですが、そのために経営資源を無限に投入することはできません。組織の戦略、ビジネスモデル、オペレーティングモデルを踏まえて、有事の際のステークホルダーへの影響や対応に係るコストを総合的に考慮し、適切な経営資源を確保する必要があります。

そのため、リスクアペタイトのフレームワークを活用し、有事の際に組織のリスクと組織が許容できる最大のリスク（リスクキャパシティ）を考慮したうえで、レジリエンスの目標（有事の際に、いつまでに、どのレベルまで復旧させるか）を達成するための、経営資源の確保といった戦略を考えることが有用です。

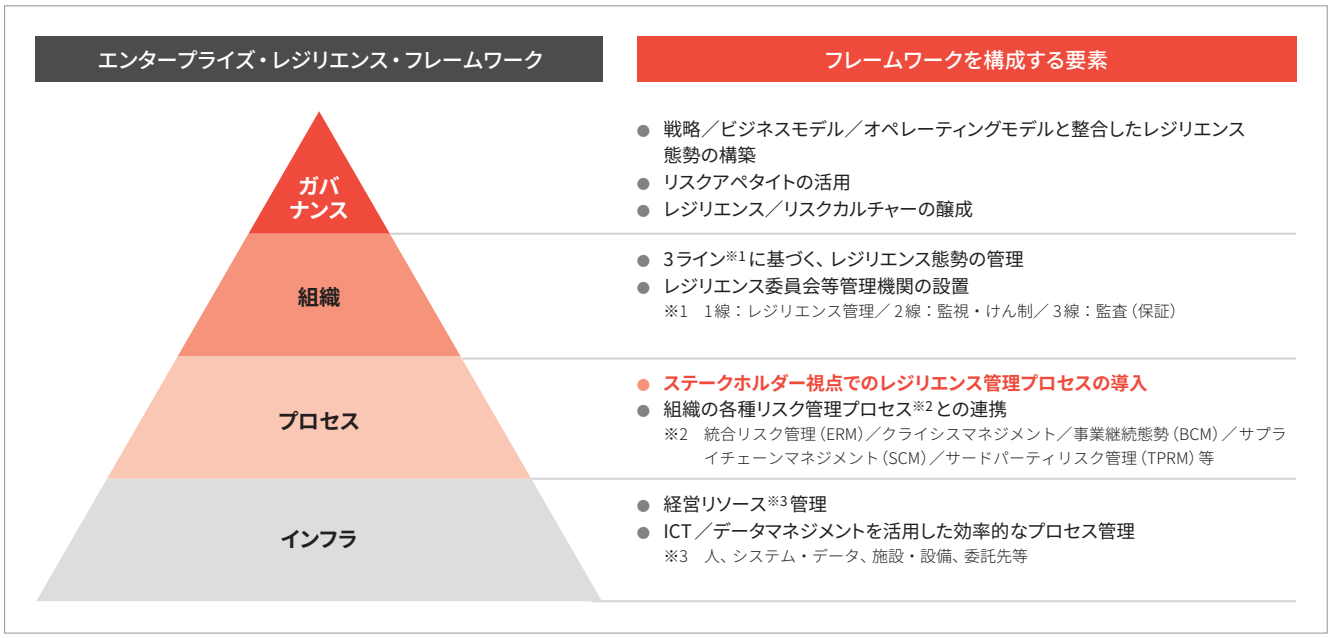
(2) 組織

マネジメントによるレジリエンスの戦略および態勢を機動的に実行するために、組織体制を整備する必要があります。3ラインの考え方に基づき、ビジネス部門（第1線）主導でレジリエンスを管理し、リスク管理部門（第2線）がレジリエンス管理の状況の監視・けん制を行い、内部監査部門（第3線）がフレームワークの有効性を監査・保証することが有用です。

(3) プロセス

エンタープライズ・レジリエンスは全く新しいプロセスを構築するものではなく、既に存在するリスク管理のフレームワークを連携させながら、構築することがポイントとなります。既存のフレームワークとしては、統合リスク管理（ERM）、クライシスマネジメント、事業継続態勢（BCM）、サプライチェーンマネジメント（SCM）、サードパーティリスク管理（TPRM）などが挙げられます。

図表1：エンタープライズ・レジリエンス・フレームワーク



出所：PwC作成

※2 金融庁「『主要行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」2023年6月
https://www.fsa.go.jp/news/r4/ginkou/20230623-2.html

例えば、以下のことが考えられます。

- 既存のBCMにおける復旧目標（RTO/RLO）設定にステークホルダーの観点を入れる。
- 自社だけでなく、SCMの観点でエンドツーエンドでの業務プロセスとリソース情報を収集し、ボトルネックのリソースを検証する（TPRMにおける外部委託先の集中度管理も含める）。
- オペレーショナルリスク管理におけるインシデント管理から、顕在化したリスク事象によるステークホルダーへの影響を確認する。

エンタープライズ・レジリエンスにおけるプロセスの強化およびそのアプローチについては、3 で詳しく説明します。

(4) インフラ

最後に、エンタープライズ・レジリエンスのプロセスを効率的に回し、マネジメントや3ラインの各階層が効果的にレジリエンスに関する情報を管理するため、ICTやデータマネジメントを活用することが有用です。

3 レジリエンス強化のアプローチ

複雑化していくビジネスや変化するリスクに対応するには、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です。既に存在するリスク管理のフレームワークおよび以下のポイントを踏まえて、平時と有事を融合したリスク管理態勢を構築し、トップダウンかつステークホルダーの視点に立ってリスク管理を実施していくことが有用です。ここでは、レジリエンス強化の4つのアプローチを紹介します（**図表2**）。

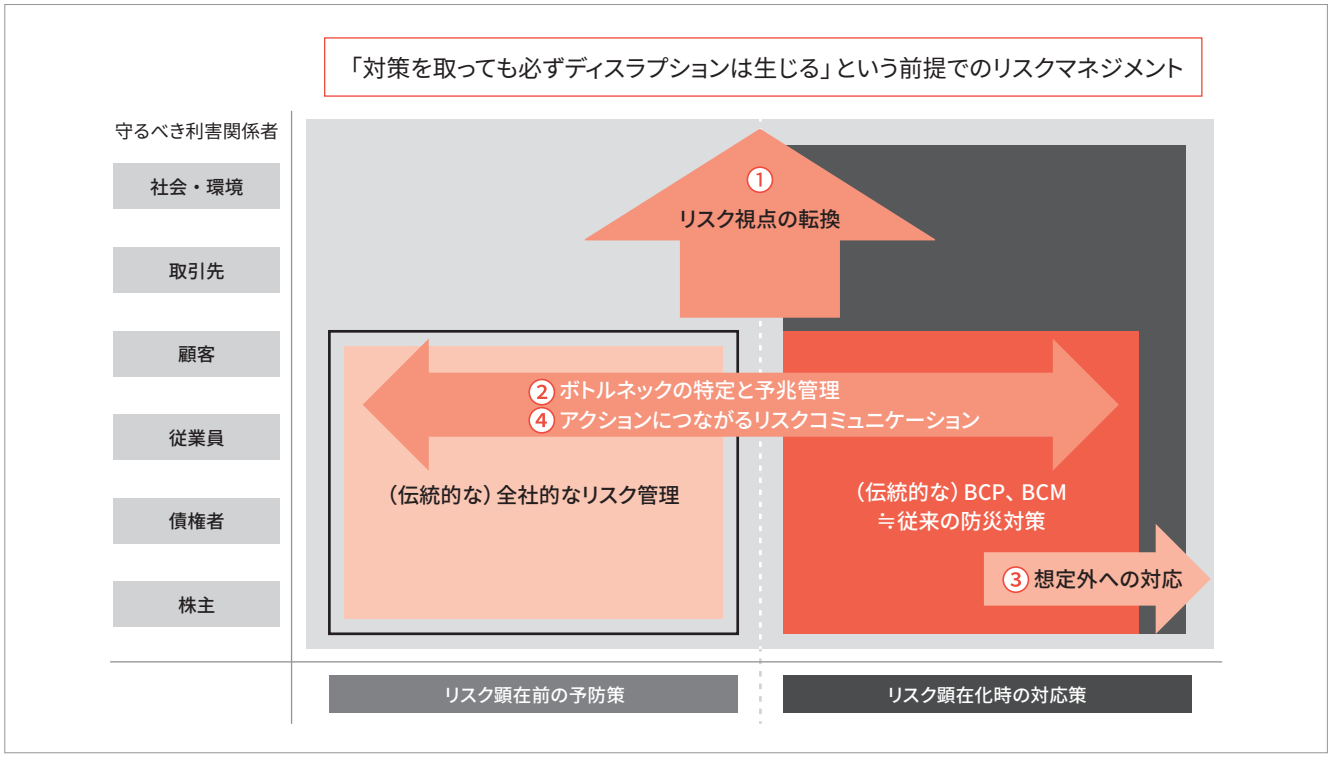
アプローチ①：リスク視点の転換

有事の際に最終的に守るべき者が誰なのかを特定します。伝統的なリスク管理やBCP/BCMのフレームワークでは、自社の従業員や資金調達に関するステークホルダーを念頭に置くことが多かったのですが、これらを顧客やサプライチェーンにおける取引先・委託先、さらに広く社会・環境といった範囲へと拡張し、ステークホルダーごとにリスクの影響を評価します。

アプローチ②：ボトルネックの特定と予兆管理

組織における事業継続計画は一般的に、「〇〇地域におい

図表2：レジリエンス強化のアプローチ



出所：PwC作成

て、最大震度6強の地震が発生した場合」など、特定のリスク事象（シナリオ）を想定しています。ただ、このようなシナリオベースでの対応だけでは、想定外のリスク事象が発生した場合、重要なビジネスおよびサービスを提供できなくなるおそれがあります。そのような事態を避けるには、事業を継続するにあたって不可欠となるリソース（ボトルネックリソース）と、当該リソースに致命的な影響をもたらす要因を特定し、主な要因については可能な限り、その顕在化の予兆を管理することが望ましいと言えます。

アプローチ③：想定外への対応

特定したボトルネックとその要因に対しては、通常、頑健な対策が策定されます。ただし、それらの対策が無効化された場合を想定したPlan B（代替策）についても策定を考慮する必要があります。

アプローチ④：アクションにつながるリスクコミュニケーション

レジリエンスに関する態勢を構築することはとても重要ですが、役職員がレジリエンスの重要性を認識していなかったり、リスクを認識していても声をあげることが難しかったりすると、いくらコストをかけて態勢を整備しても有効に機能しない「絵に描いた餅」となってしまいます。したがって、経営層や現場の従業員が一体となって自律的、能動的な行動を可能とするカルチャーを醸成するようにします。また、フラットな組織構造づくりやコミュニケーションラインの複線化など組織構造・制度の改革と浸透も有効です。

4 エンタープライズ・レジリエンスに関するプロセスの強化

次に、3のレジリエンス強化に向けた4つのアプローチを踏まえた具体的なプロセスについて説明します。

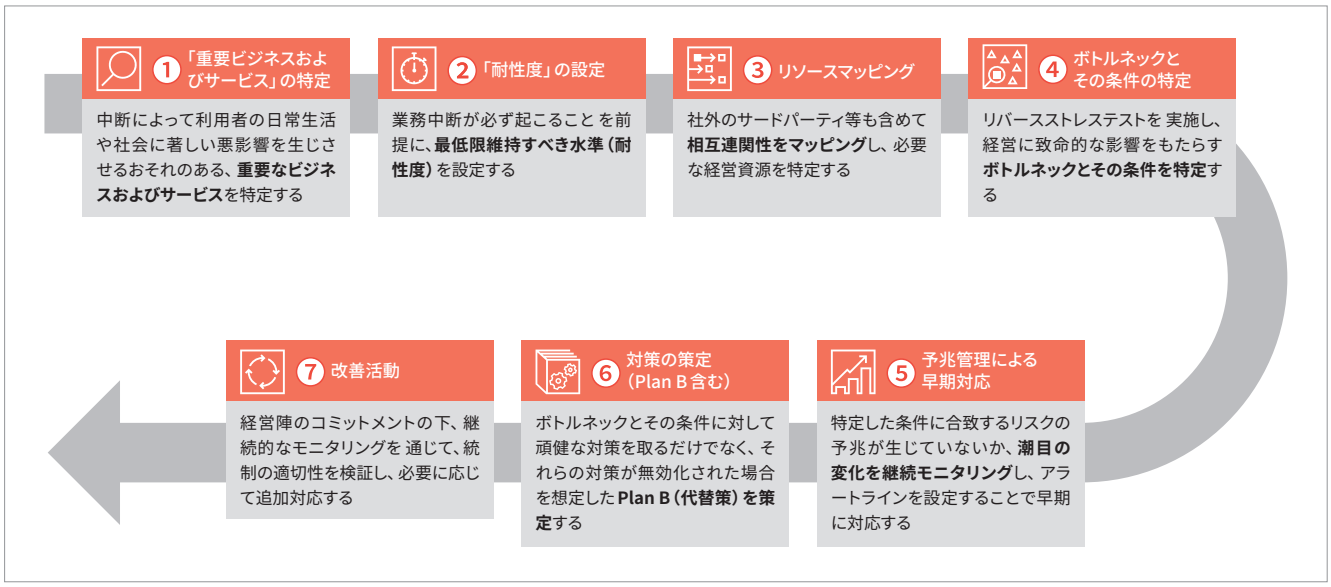
まず、自社が提供するビジネスおよびサービスの重要性を、ステークホルダーに与える影響から評価します。その評価に基づいて、耐性度の設定と経営資源（リソース）の適切性を検証し、管理態勢を継続的に改善していきます。

特に、従来のような特定のリスク事象・原因事象別のリスク対策や発現の蓋然性の高まりを考慮しないリスク管理ではなく、経営に致命的な影響を与えるリスクについての予兆対応およびリスク顕在化時の対応力を高めることが重要です。**図表3**では、エンタープライズ・レジリエンスのプロセスを構成する7つのステップを示しました。7つのステップについて、その概要を説明します。

ステップ①：「重要ビジネスおよびサービス」の特定

3の「アプローチ①：リスク視点の転換」でも述べましたが、自社以外のステークホルダーに対しても、業務中断がもたらす影響を評価し、ステークホルダー目線で重要なビジネスおよびサービスを特定する必要があります。例えば、以下のような観点で、業務中断の影響を評価することが考えられます。

図表3：レジリエンス強化のプロセス



出所：PwC作成

- **自社**：金銭的損失やレピュテーションへの影響はどれほどか。
- **顧客**：重要顧客に対して耐えられないレベルの損失をもたらすか。
- **社会**：重要な国家インフラを提供するサービス等、社会の安定性にリスクをもたらすか。

ステップ②：「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」のことです。BCPにおいて設定する業務中断時の目標復旧時間（RTO）と重なりますが、それだけでなく、社会への影響や利用者の生活への影響を一定の範囲内に収める観点から、業務中断後、時間が経つにつれてステークホルダーにどれほどの影響が生じるかを考慮する必要があります。

ステップ③：リソースマッピング

重要ビジネスおよびサービスやそれらを構成する各業務プロセスを耐性度の範囲内で提供するにあたって必要となる社内外のリソース（人員、システムおよびデータ、施設・設備、原材料・部品、外部委託先等）をエンドツーエンドの業務プロセス全体で特定し、それらの相互連関性※3や相互依存度※4のマッピングを行います（**図表4**）。

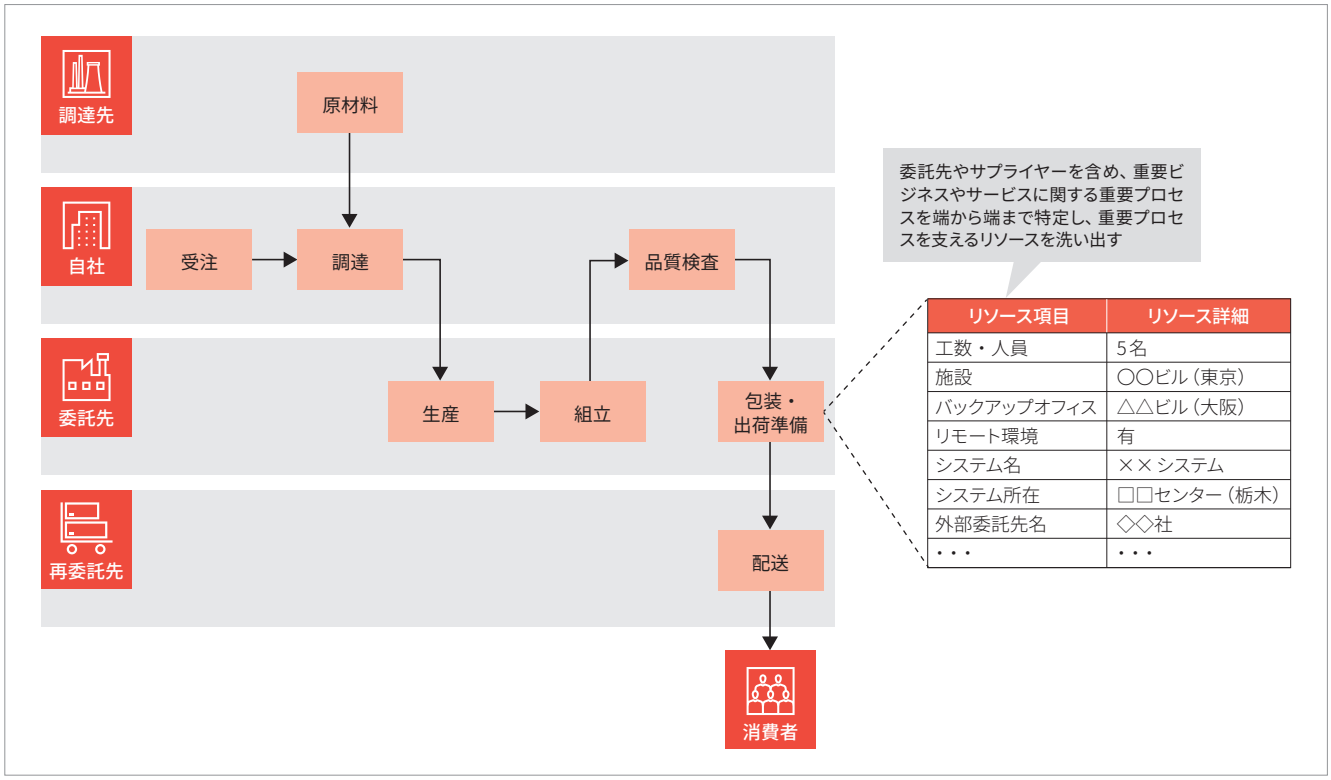
一般的には、フローチャートを作成し、各ステークホルダーの行動を具体化したうえで、関連するリソースを記載します。当該フローチャートをプロセスやリソースを管轄する部門と対話をしながら、具体的に落とし込む必要があります。

ステップ④：ボトルネックと条件の特定

従来の多くの組織では、震災や感染症の流行等、特定のシナリオをベースに、当該シナリオがリソースに対してどのような影響をもたらすかをシナリオの数に応じてリソース制約を仮定して、対応策をテストしてきました（シナリオテスト）。

一方、本稿で紹介するものは、特定されたリソースに対して、シナリオをあらかじめ特定せずに、リソース制約を仮定して、それらを発現させる蓋然性のあるシナリオを想定しま

図表4：リソースマッピング



出所：PwC作成

※3　相互連関性（Interconnectedness）：各リソースが、直接・間接に他のリソースとどのように結びついているかを指す。例：プロセスAのシステムがダウンすると、関連する後続プロセスBやプロセスCの業務全体に影響を及ぼす可能性がある。

※4　相互依存性（Interdependencies）：1つのリソースが他のリソースに依存している度合いや関係を指す。例：生産ラインは原材料供給に依存しており、当該原材料の供給が止まると生産も停止することになる。

す（リバースストレステスト※5、**図表5**）。

リソースマッピングのステップでリソースの相互連関や相互依存を把握することで、業務プロセスを実施するにあたって不可欠となるリソース（ボトルネック）を特定することができます。当該ボトルネックに対して、致命的な影響をもたらす制約条件を社内外のデータ（極端だが起こり得るシナリオの発生条件や発生確率）をもとに整理します。その上で、当該リソース制約を発現させるシナリオを想定します。

ステップ⑤：予兆管理による早期対応

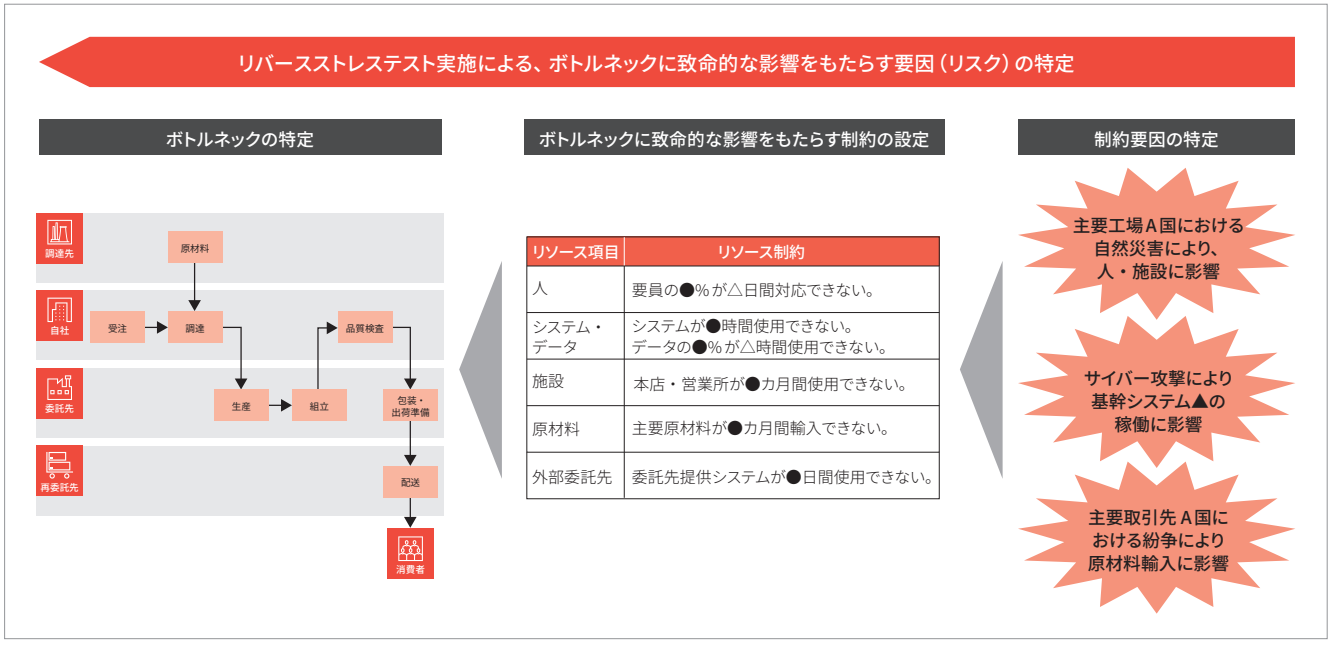
リソース制約をもたらす要因を想定した後は、その予兆が生じていないか、潮目の変化を継続的にモニタリングし、アラートラインを設定することで早期に対応することも重要です。予兆管理としては、以下のようなアプローチが考えられます。

- **リスク変化の捕捉：**固有リスクの高まりと統制の脆弱性を把握するために、リソース制約の要因に対してモニタリング指標（Key Risk Indicator/Key Control Indicator）を設定してからモニタリングします。例えば「サイバー攻撃」という要因に対しては、固有リスクの高まりとして「情報セキュリティアラート件数（不正アクセス件数）」や「同業他社におけるサイバー攻撃報道件数」をKey Risk Indicatorに設定し、統制の脆弱性として「フィッシングテストの違反件数」や「主要システムの脆弱性事項の対応未実施件数」をKey Control Indicatorに設定し、モニタリングすることが考えられます。
- **軽微なインシデント分析：**軽微なインシデント（ニアミス）は、実際の事故に至らなかったものの潜在的なリスクを示します。想定する要因に関してニアミス事象が頻繁に発生する場合、大きな影響をもたらすインシデントに発展する可能性もあるため、トレンドや真因分析（Root Cause Analysis）を実施する必要があります。
- **能動的モニタリング：**インシデント報告等で報告されない場合でも、従業員のプロファイルやアクセスログ、コミュニケーションをインプット情報として、検知ツールを活用してその行動をモニタリングするといった、能動的にリスクを捕捉するアプローチを取ることも考えられます。

ステップ⑥：対策の策定（Plan B含む）

リソース制約をもたらす要因に対しては頑健な対策も重要ですが、それらの対策が無効化された場合を想定したPlan B（代替策）を策定することも重要です。例えば、ボトルネックとなる生産拠点を複線化したり、原材料を調達するサプラ

図表5：リバースストレステスト



出所：PwC作成

※5 リバースストレステストとは、甚大な影響をもたらす結果を先に想定し、それを引き起こすリスクシナリオを分析するもの。

イヤーを分散させたりして、規制やコストを考慮してPlan Bを検討します。

ステップ⑦：改善活動

以上、レジリエンス強化のアプローチを踏まえたエンタープライズ・レジリエンスのプロセスについて紹介しました。これらのプロセスは整備した後も、経営陣のコミットメントの下、継続的なモニタリングを通じて統制の適切性を検証し、必要に応じて追加対応をしていく必要があります。そのためには、役職員がレジリエンスの重要性を認識し、与えられた責任と権限のもとで主体的にプロセスを運用していくことが重要です。

5 おわりに

繰り返しになりますが、エンタープライズ・レジリエンスは全く新しいプロセスを構築するものではなく、既に存在するビジネス戦略やリスク管理のフレームワークを整合させることが大事です。

ナシーム・ニコラス・タレブは、その著書『反脆弱性』において、組織は単に逆境や不確実性に対して耐え抜くだけでなく、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）を備えることが重要と述べています※6。

組織の戦略およびリスク管理にレジリエンスの観点を取り入れることで、不確実な時代を先導する組織へと一層進化できるよう、PwCもエンタープライズ・レジリエンスの態勢構築・高度化に向けたさまざまなサービスをご提供致します。

※6　ナシーム・ニコラス・タレブ『反脆弱性――不確実な世界を生き延びる唯一の考え方（上・下）』望月衛監訳、千葉敏生訳、ダイヤモンド社、2017

卜 信慶（ぼく しんぎょん）
PwC Japan有限責任監査法人　マネージャー
ガバナンス・リスク・コンプライアンス・アドバイザリー部
米国公認会計士（ワシントン州）／GARP Financial Risk Manager（FRM）
信託銀行での海外リスク管理態勢構築および運用の経験を経て現職。国内外のさまざまな業種の事業法人に対して、リスク管理態勢高度化支援、BCP/BCM高度化支援、レジリエンスの態勢評価および導入支援等、リスク管理に関するさまざまなサービスを提供している。
メールアドレス：shinkyung.bok@pwc.com