ERM と BCM の連携が
組織のレジリエンスをいかに強化するか

WTW ブローカージャパン　シニアリスクマネジメント コンサルタント　桐原憲昭

ポイント

○ ERM（全社的リスクマネジメント）と BCM（事業継続マネジメント）の統合により、リスクの早期察知から危機対応、復旧までの一貫したサイクルを確立できる。

○ 統合の効果として、リスクの全体像の可視化、意思決定の質とスピード向上、リソース最適配分、組織のアジリティ向上の 4 つが実現し、レジリエンスが受動的防御から能動的な意味合いへと転換する。

○ 多くの組織で統合が進まない要因として、部門間のサイロ化、異なる評価指標や報告ライン、重複作業などのグローバル共通の課題に加え、日本企業では縦割り構造や規格別管理の問題が存在する。

○ WTW が提唱する 5 つの統合ステップ（統一リスクプロファイル策定、部門横断的協働、ERM 視点の演習、対応プロトコル標準化、継続的改善）により、段階的かつ体系的な統合が可能となる。

○ 日本企業特有の課題として、J-SOX、ISO22301、ISO31000 など複数の管理体系が独立運用され、経営層の関与不足と地震対策偏重の傾向があるが、近年は統合への機運が高まりつつある。

○ 不確実性の時代において、ERM-BCM 統合による戦略的レジリエンスの構築は、もはや選択肢ではなく必須要件であり、リスクを成長機会に転換し、持続的競争優位を確立する鍵となる。

はじめに：レジリエンス[1]強化の新たな潮流

今日の企業経営を取り巻く環境は、かつてないほど複雑かつ不確実性に満ちている。パンデミック、地政学的緊張、サイバー攻撃、気候変動、サプライチェーンの混乱、米国の関税措置など、従来の想定を超えた規模と速度でリスクが顕在化し、相互に連鎖しながら企業活動に影響を及ぼしている。

このような環境下において、企業に求められるのは単なる「生存」ではない。混乱や変化を新たな成長機

[1] 困難な状況に直面した際に、それらに適応し、回復する力

会へと転換し、競争優位性を確立する能力、すなわち「戦略的レジリエンス」の構築が不可欠となる。

従来、多くの企業では、ERM（Enterprise Risk Management：全社的リスクマネジメント）と BCM（Business Continuity Management：事業継続マネジメント）が別々の部門で管理され、それぞれ独立した活動として運営されてきた。ERM は取締役会や経営層に近い位置で戦略的・財務的リスクを評価し、BCM は現場に近い位置で、災害対応や業務復旧を担当するという分業体制である。

しかし、我々は、この分断された状態を「レーダーはあるが救命ボートがない」「救命ボートはあるがレーダーがない」状態に例え、両者の統合なくして真のレジリエンスは実現できない、と警鐘を鳴らしたい。ERM がリスクを早期に察知する「レーダー」の役割を果たし、BCM が実際の危機に対応する「救命ボート」として機能するとき、初めて組織は予測から対応、復旧から学習までの一貫したリスクマネジメントサイクルを確立できるのである。

実際、ERM-BCM 統合に取り組んでいる企業では、リスク対応時間の短縮、コスト削減、意思決定の迅速化など、具体的な成果が見て取れる。本ニュースレターでは、なぜ ERM-BCM 統合が必要なのか、統合を阻む要因は何か、そして、どのように統合を進めるべきかを考えていきたい。

ERM と BCM の基礎理解

組織のレジリエンスを高めるためには、ERM と BCM それぞれの役割と機能を正確に理解することが出発点となる。両者は異なる視点からリスクにアプローチするが、本質的には相互補完的な関係にある。

ERM（全社的リスクマネジメント）とは

ERM は、組織全体のリスクを包括的に識別、評価、管理する戦略的フレームワークである。その特徴は、個別のリスクを部門ごとに管理するのではなく、組織横断的な視点から統合的にリスクを捉える点にある。

ERM の中核を成すのが「三層防衛モデル」である。第 1 層は、事業部門がリスクを所有し日常的に管理する。第 2 層は、リスク管理部門やコンプライアンス部門が、リスク管理プロセスの設計と監視を担当する。第 3 層は、内部監査部門が独立した立場から評価と保証を提供する。この構造により、リスク管理の実効性と客観性が担保される。

ガバナンス体制においては、CRO（最高リスク責任者）が中心的役割を果たす。CRO は四半期ごとに取締役会へリスク状況を報告し、経営陣によるリスク統制の最高レベル委員会と協議しながら、重要リスクの調整と評価を行う。

BCM（事業継続マネジメント）とは

BCM は、重大な混乱が発生した際に、事業の継続性を確保するための包括的な管理プロセスである。自然災害、サイバー攻撃、パンデミック、サプライチェーンの途絶など、あらゆる脅威に対して組織が迅速に対応し、重要業務を継続または早期復旧させることを目的とする。

BCM の中核となるのが BIA（Business Impact Analysis：事業影響分析）である。BIA は、各業務プロセスが中断した場合の影響を時系列で分析し、優先的に復旧すべき重要業務を特定する。この分析により、RTO（Recovery Time Objective：目標復旧時間）と RPO（Recovery Point Objective：目標復旧時点）が設定される。

図表 1 ：ERM と BCM の比較

比較項目	ERM	BCM
主な目的	戦略目標達成を阻害するリスクの予防・管理	業務中断時の継続性確保と早期復旧
対象範囲	組織全体の戦略的・財務的・評判リスク	重要業務とそれを支える経営資源
時間軸	中長期的視点（年次～複数年）	短期的・即応的視点（時間～日単位）
アプローチ	トップダウン（経営層から現場へ）	ボトムアップ（現場から経営層へ）
主要ツール	リスクレジスタ、リスクマップ、KRI	BCP、BIA、RTO/RPO
評価方法	発生可能性×影響度のマトリクス	時間経過による業務影響度分析
管理サイクル	識別→評価→対応→モニタリング	分析→計画→訓練→改善
報告先	取締役会、リスク委員会	危機管理委員会、対策本部
主管部門	リスク管理部、経営企画部	総務部、IT 部門、施設管理部

この比較表が示すように、ERM と BCM は異なる特性を持ちながらも、組織のレジリエンス構築という共通目標に向かって機能する。ERM が「何が起こりうるか」を予測し備えるレーダーの役割を果たし、BCM は「起きたときにどう対応するか」を実行する救命ボートとして機能する。

重要なのは、この 2 つが別々に運用されるのではなく、統合されたフレームワークの中で相互に情報を共有し、補完し合うことである。次章では、なぜ多くの組織でこの統合が進まないのか、その要因を見ていく。

なぜ ERM-BCM 統合が進まないのか

ERM と BCM の統合がもたらす効果は明白であるにもかかわらず、多くの組織では依然として両者が分断された状態で運用されている。この分断は、グローバル共通の構造的課題と、日本企業特有の事情が複雑に絡み合って生じている。

クローバル共通の課題

最も根深い問題は、組織内の「サイロ化（縦割り）」である。多くの企業では、ERM 部門が財務・戦略リスクに集中し、BCM 部門が災害対応・業務復旧に特化するという、分業体制が確立されている。両部門は異なる報告ラインを持ち、使用する言語や評価指標も異なるため、情報共有や協働が困難となっている。例えば、ERM 部門が識別したサイバーセキュリティリスクの情報が、BCM 部門の IT 復旧計画に反映されないケースは珍しくない。逆に、BCM の訓練で発見された脆弱性が、ERM のリスク評価に組み込まれないこともある。このような情報の分断は、組織全体のリスク対応力を著しく低下させる。ほかにも下表に示す問題が散見される。

図表 2 ：分断による問題の具体例

問題カテゴリ	ERM 側の活動	BCM 側の活動	結果として生じる問題
情報の分断	サイバーリスクを「高」と評価	IT 復旧計画でサイバー攻撃を想定せず	実際の攻撃時に対応が後手に
重複作業	全社リスク評価を実施	独自に BIA を実施	同じ部門に 2 回ヒアリング、現場の負担増
優先順位の不一致	財務リスクを最優先	業務継続を最優先	リソース配分で対立、経営判断の遅れ
言語・指標の相違	リスクスコア、KRI で管理	RTO、RPO で管理	相互理解が困難、統合評価ができない

日本企業特有の障壁

日本企業においては、これらのクローバル共通の課題に加えて、独自の構造的問題が存在する。

図表 3：日本企業における縦割り構造の実態

管理体系	主管部門	主な活動	他部門との連携状況
J-SOX 対応	内部統制部門	財務報告の信頼性確保	BCM は「IT の全般統制」の一部として部分的に考慮
ISO22301	総務部門	BCMS の構築・運用	独立して運用、ERM との連携なし
ISO9001	品質管理部門	品質マネジメント	品質リスクに特化、全社リスクとの統合なし
情報セキュリティ	IT 部門	ISMS 運用	独自のリスク評価、BCP との連携不足
ISO31000 (ERM)	経営企画部門	全社リスク評価	上記すべてと連携不足

このような縦割り構造は、それぞれの規格や規制への対応としては機能するものの、組織全体のレジリエンス強化という観点では大きな障害となっている。

また、経営層の関与不足も深刻である。日本では、「BCM＝災害対応」、「ERM＝内部統制の一部」として捉えられる傾向が強く、戦略的な経営課題として認識されていない。このため、統合に必要な経営資源の配分や組織横断的な権限付与が行われず、部門レベルでの部分最適に陥りやすい。

さらに、日本企業の多くは、地震対策に偏重した災害対応体制を構築してきた歴史があり、サイバーリスク、地政学リスク、気候変動リスクなど、多様化する脅威への統合的なアプローチが遅れている。

WTW が提唱する ERM-BCM 統合の意義

統合がもたらす 4 つの戦略的効果

WTW は、ERM-BCM 統合により、以下の 4 つの戦略的効果が得られると分析している。

1. 第 1 に、リスクの全体像の可視化である。 ERM で識別された戦略的リスクと BCM で分析された業務影響が統合されることで、リスクの相互関連性と連鎖的影響が明確になる。例えば、地政学的リスクがサプライチェーンの混乱を引き起こし、それが財務リスクへと波及するといった複合的なシナリオを、統合的に評価・対応できるようになる。
2. 第 2 に、意思決定の質とスピードの向上である。 統合されたリスク情報と事業影響分析により、経営層は包括的な視点から迅速に判断を下せる。ある金融機関では、統合ダッシュボードの導入により、危機対応の初動判断が大幅に改善されたという例もある。
3. 第 3 に、リソースの最適配分である。 ERM と BCM が別々に予算を確保し、重複した対策を実施する非効率が解消される。統合により、リスクの優先順位に基づいた戦略的なリソース配分が可能となり、同じ予算でより高い効果を実現できる。
4. 第 4 に、組織のアジリティ（機敏性）の向上である。 統合された体制では、新たなリスクの出現や環境変化に対して、組織全体が一体となって迅速に適応できる。COVID-19 パンデミックにおいて、統合体制を持つ企業が他社に先駆けて事業モデルの転換を実現できたのは、この機敏性の証左である。

戦略的レジリエンスへの転換

WTW が最も強調するのは、ERM-BCM 統合により、レジリエンスが「受動的な防御策」から「能動的な戦略資産」へと転換することである。統合された組織は、リスクを単に回避・軽減するだけでなく、変化や混乱を新たな機会として活用できる。

例えば、ある小売企業は、ERM で特定した「消費者行動のデジタルシフト」というリスクと、BCM で準備していた「店舗閉鎖時のオンライン販売体制」を統合的に活用し、コロナ禍において競合他社が苦戦する中、売上維持に成功した。これは、統合によりリスクが機会に転換された典型例である。

WTW は、このような戦略的レジリエンスこそが、不確実性の時代における持続的競争優位の源泉になると結論づけている。単なるリスク管理を超えて、組織の適応力と成長力を高める統合アプローチは、もはや選択肢ではなく必須要件となっている。

統合プロセス：5 つのステップ

WTW が提唱する ERM-BCM 統合[i]は、段階的かつ体系的なアプローチにより実現される。以下、各ステップの詳細な実施方法と具体的なアクションを見ていく。

ステップ 1：統一されたリスクプロファイルの策定

ERM と BCM の統合における第一歩は、両フレームワークから得られた知見を統合した包括的なリスクプロファイルの構築である。このプロファイルは、ERM が特定する戦略的リスクと、BCM が重視する業務継続性の観点を融合させ、組織が直面する脅威の全体像を提供する。

例えば、ある大手製造業のケースでは、ERM チームが特定したサプライチェーンの地政学的リスクと、BCM チームが実施した事業影響分析（BIA）で明らかになった特定部品の供給途絶による生産ライン停止リスクを統合することで、より実践的な対応策の立案が可能となった。具体的には、BIA の結果、ある電子部品の供給が 72 時間以上停止した場合、主力製品の生産が完全に停止し、1 日あたり約 5 億円の機会損失が発生することが判明。この情報を ERM の戦略的リスク評価と組み合わせることで、代替サプライヤーの確保だけでなく、在庫戦略の見直しや製品設計の変更といった多層的な対策を講じることにつながった。

また、リスクプロファイルの定期的な更新も重要である。一定期間ごとに BIA を見直し、新たに特定された重要業務や変化した依存関係を反映させることで、リソース配分の優先順位を適切に調整できる。金融機関の例では、デジタル化の進展に伴い、従来は補助的だったオンライン・バンキングのシステムが、基幹業務となったことを BIA で特定し、サイバーセキュリティへの投資を大幅に増強した。このように、統一されたリスクプロファイルは、戦略的な意思決定と業務レベルの対応策を結びつける重要な基盤となる。

ステップ 2：部門横断的な協働の促進

ERM と BCM の効果的な統合には、組織の縦割り構造を超えた強固な協働体制の構築が不可欠である。これは単なる情報共有にとどまらず、リスク認識の共通化と対応戦略の一体化を実現する継続的

なプロセスである。

ある国際物流企業では、半期ごとに開催される「統合リスク委員会」を設置し、ERM 担当役員、BCM 責任者、各事業部門のリスクオフィサー、IT 部門、人事部門、法務部門の代表者が参加する体制を構築した。この委員会では、ERM が特定した戦略的リスクがどのように現場の業務継続性に影響を与えるかを具体的に検討する。例えば、気候変動リスクの議論では、ERM チームが長期的な規制変更リスクを提示し、BCM チームが異常気象による物流拠点の操業停止リスクを共有、現場の物流管理者が実際の代替ルート確保の課題を説明することで、包括的な対応計画を策定できた。

ステップ 3：ERM 視点を反映した統合演習・訓練

BCM の訓練や演習に ERM で特定されたリスクシナリオを組み込むことで、より現実的で効果的な危機対応能力を構築できる。これは単なる手順の確認を超えて、組織全体の危機対応力を向上させる戦略的な取り組みである。

ある大手銀行グループの事例では、ERM チームが特定した「複合的サイバー攻撃と物理的テロの同時発生」というシナリオを基に、全社規模の危機対応演習を企画した。この演習では、まず BIA で特定された重要業務（決済システム、ATM 網、コールセンター）への影響を詳細にシミュレートし、段階的にエスカレーションする状況を再現した。第 1 段階では支店への物理的攻撃、第 2 段階では基幹システムへのランサムウェア攻撃、第 3 段階では偽情報の拡散によるレピュテーション危機という複合シナリオを展開した。

また、演習の設計において重要なのは、ERM の分析に基づく「想定外」要素の組み込みである。例えば、電力会社を例にとると、ERM が特定した気候変動リスクと地政学的リスクを組み合わせ、「記録的猛暑による電力需要急増時に、主要発電所でサイバー攻撃による制御システム障害が発生し、同時に天然ガス供給国との外交問題で燃料調達が困難になる」という複合シナリオで訓練を行うことも考えられる。この訓練では、通常の対応手順では対処できない状況を意図的に作り出し、創造的な問題解決能力と部門間連携の重要性を体験的に学習する状況を作り出す。

ステップ 4：対応プロトコルと手順の標準化

ERM と BCM の真の統合を実現するには、組織全体で一貫性のある統合対応プロトコルの策定が不可欠である。このプロトコルは、リスクの種類や規模に関わらず、迅速かつ効果的な危機対応を可能にする統一的なフレームワークとして機能する。

統合プロトコルの中核となるのは、明確なエスカレーション基準と意思決定権限の定義である。ある総合商社では、「統合危機管理プロトコル」を導入し、インシデントを 5 段階の深刻度レベルで分類した。各レベルには具体的な判断基準が設定され、例えばレベル 3（事業部対応）は「想定損失額が 10 億円以上 50 億円未満」「複数拠点での同時障害発生」「メディア報道の可能性あり」のいずれかに該当

する場合と明確に定義されている。この基準により、現場担当者も迷うことなく適切なエスカレーションを実施できるようになった。

また、役割と責任の明確化も重要な要素である。RACI マトリックス[2]を活用し、危機対応における各ステークホルダーの責任を詳細に定義する。例えば、データ漏洩インシデントでは、CIO が技術的対応の実行責任（R）、CRO が全体統括の説明責任（A）、法務部門が規制対応の協議対象（C）、影響を受ける部門が情報共有対象（I）として事前に定められている。この明確な役割分担により、大規模なランサムウェア攻撃では、検知から 2 時間以内に全ての初動対応を完了し、被害を最小限に抑えることができた。

ステップ 5：定期レビューと継続的改善

リスク環境の急速な変化に対応するため、ERM と BCM 戦略の継続的なレビューと改善プロセスの確立は、組織のレジリエンス維持に不可欠である。これは単なる定期的な文書更新ではなく、組織の学習能力と適応力を高める戦略的な取り組みである。

例えば、先進的な製造業企業では、「アダプティブ・リスク・マネジメント・サイクル」を導入し、3 層構造のレビュー体制を構築している。第 1 層の「週次リスクパルス」では、KRI の変動を AI がリアルタイムで監視し、異常値を検出すると自動アラートを発信する。第 2 層の「月次統合レビュー」では、ERM と BCM の合同チームが、新たに顕在化したリスクや変化したリスクプロファイルを評価し、必要に応じて対応策を調整する。第 3 層の「四半期戦略レビュー」では、経営層を交えて、リスクアペタイトの見直しや重大な戦略変更を検討する。

まとめ：取り組みに向けて

今日の複雑かつ不確実な経営環境において、ERM（全社的リスクマネジメント）と BCM（事業継続マネジメント）の統合は、組織の持続的成長と競争優位確立のための必須要件となっている。本論にて指摘した「レーダー（ERM）と救命ボート（BCM）」の比喩が示すように、リスクの早期察知から実際の危機対応、復旧から学習までの一貫したサイクルの確立が重要である。

統合により得られる効果は、①リスクの全体像の可視化による相互関連性の把握、②意思決定の質とスピードの向上、③リソースの最適配分による効率化、④組織のアジリティ向上による環境変化への迅速な適応である。これらにより、レジリエンスは受動的な防御策から能動的な戦略資産へと転換し、リスクを新たな成長機会として活用することが可能となる。

---

[2] RACI マトリックスは、タスクごとに実行責任(R)、説明責任(A)、協議対象(C)、情報共有(I)の 4 つの役割を明確化する責任分担表である

実装においては、統一リスクプロファイルの策定、部門横断的な協働体制の構築、ERM 視点を反映した統合演習、対応プロトコルの標準化、継続的な改善プロセスの確立という 5 つのステップを着実に進めることが重要である。

日本企業においては、縦割り構造や規格別管理といった特有の課題があるものの、統合への取り組みは着実に進展している。不確実性の時代において、ERM-BCM 統合による戦略的レジリエンスの構築は、組織の持続可能な成長を実現する鍵となる。

参考文献

[i] How bridging ERM and BCM can strengthen your organisational resilience? https://www.wtwco.com/en-gb/insights/2024/11/how-bridging-erm-and-bcm-can-strengthen-your-organisational-resilience