急務のサイバーレジリエンス、外部委託先BCP検証への対応

NRIの事業継続マネジメントに関するアンケート調査で、「業務中断時の対応策」「外部委託先全体のBCP検証」への取り組みについて課題があることが明らかになった。経済安全保障推進法による審査も迫っており、BCP強化への取り組みがさらに重要となっている。

事業継続マネジメント（BCM）調査を実施

企業がビジネスコンティニュイティ（BC）に取り組む上では、事業継続計画（BCP）を策定するだけでなく、その導入・運用・見直しという継続的改善を含む、包括的かつ統合的な事業継続マネジメント（BCM）が重要である。NRIは、サイバー攻撃の多様化やコロナ禍による勤務環境の変化など、昨今の企業を取り巻く環境変化に伴う事業継続に対する危機意識、およびBCMの取り組み状況を調査する目的で、2023年1月、国内の金融機関（銀行、証券、資産運用、保険、その他金融）を対象に「事業継続マネジメント（BCM）に関するアンケート調査」を実施し、122社から回答を得た。

アンケートはBCMの国際規格ISO22301が示すPDCAサイクルを基に、図表1に示す5領域に分類して行った。

また、アンケート回答結果を、NRIが開発したBCM成熟度モデルを用いてスコア化し、レベル1（最低）～レベル5（最高）の5段階で評価した（図表2参照）。

図表1　BCM成熟度モデルにおける5領域

領域	領域の観点	質問例
組織内外の状況認知	BCP策定の前提となる組織内外の状況等について把握、整理をしているか	•自社の事業継続の使命や義務を認識しているか。 •事業継続に関して、どのような危機意識をもっているか。
BCM推進態勢	BCMを推進する組織体制、仕組みが確立されているか	•BCMを運用するために、必要な役割を明確にした上で部署や担当者を割り当てているか。 •適切なBCPの見直しのタイミングを設けているか。
BCP対策	BCP策定において、実効性のある計画、適切な対策が講じられているか	•「オフィス・会社設備」のBCP対策として、どのような施策を講じているか。 •「重要システム」のBCP対策として、どのような施策を講じているか。
BCP評価・継続的改善	BCPの有効性検証、適切なパフォーマンス評価、継続的改善を実施しているか	•どのようなBCP訓練を採用しているか。 •どのようなパフォーマンス評価を行い、改善活動を行っているか。
経営陣のリーダーシップ	BCPの整備促進に経営陣によるリーダーシップ(積極的な関与)が発揮されているか	•BCMおよびBCPの有効性および妥当性について、経営陣による定期的な確認（マネジメントレビュー）を行っているか。 •経営陣はどのような訓練に参加しているか。

（出所）野村総合研究所

図表2　BCM成熟度モデルにおける成熟度指標

BCM成熟度モデル		成熟度指標の基準	
高	成熟度指標	段階	概要
	レベル5	成熟度80%-100%	BCMおよびBCPの適切性、妥当性、有効性を検証する機会があり、継続的改善が行われている
	レベル4	成熟度60%-79%	事業継続の優先順位とそれに対する自部門のとるべき対応を理解し、全社的なテスト・訓練を充分に行っている
	レベル3	成熟度40%-59%	組織で合意された事業継続方針に基づき、重要業務が定義されており、それに対する事業継続計画が構築されている
	レベル2	成熟度20%-39%	事業継続計画の重要性について、少なくとも1つ以上の事業部門で理解がされていて、経営への啓蒙を進めている
	レベル1	成熟度20%未満	事業継続計画の重要性について、理解がされていない
低			

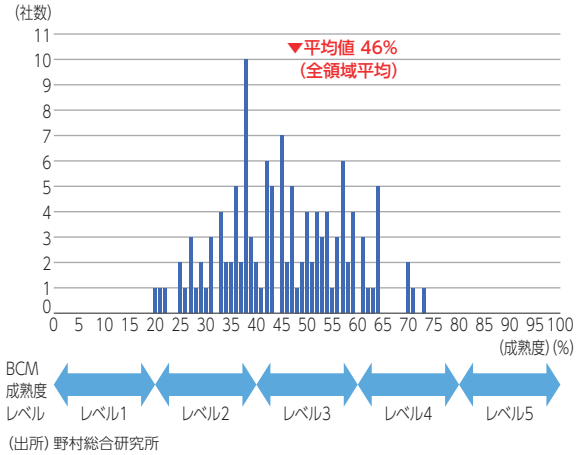
（出所）野村総合研究所

全体のBCM成熟度レベルは中間レベル

回答企業全体のBCM成熟度は、「組織内外の状況認知」「BCM推進態勢」について各企業ともに態勢整備が進んでいることが伺われたが、「BCP対策」「BCP評価・継続的改善」については相対的に成熟度が低く、全体としての成熟度指数の分布をみるとほぼ中間のレベル3（平均46%）であった（図表3）。

レベル4以上の企業をみると、「経営陣が主体となり中長期的なBCMが具体的に計画されている」「人・建物・システム・データ・サイバーセキュリティなど各経営リソースへの対策が偏りなく整備されている」「経営陣や外部委託先等を巻き込んだ大規模なBCP訓練が計画実施されている」「訓練結果を踏まえた評価改善活動まで実施されている」など、PDCAサイクルが定着している様子が伺えた。

図表3　BCM成熟度スコア分布と該当社数



(出所) 野村総合研究所

一方、レベル2以下の企業をみると、「各領域の対策に大きな偏りがある」「特定の分野における対策レベルが著しく低い」など、BCMの実効性が低い例が散見された。

BCP対策に課題

BCP対策については、自社の経営リソースや近年のリスク動向といった組織内外の状況認知を行った上で、BCP策定の検討が進められている。しかし、「バックアップオフィスの設置」「システム構成の冗長化」「自家発電の導入」などの対策は、予算や人員リソースなどの確保が必要かつ整備に時間を要するため、対応の優先度が後回しとなっている傾向が見て取れた。

また、回答企業のうち約8割がBCP訓練として安否確認や標的型メール対応訓練を採用している一方、社内外を巻き込んだ初動対応訓練を行う企業は全体の約2割、重要業務の継続訓練を行う企業は全体の約1割に留まっていた。

最近のサイバー攻撃の頻発を受け、BCPの大きな課題として、とりわけ「業務中断時の対応策」「外部委託先全体のBCP検証」への関心が高まっている。

しかし、アンケート結果からみると、業務中断に対する未然防止措置に加え、業務中断した場合の早期復旧・影響範囲の軽減策まで整備している企業、また、外部委託先のBCP状況の確認、外部委託先と共同のBCP訓練を行っている企業は少数だった。

経済安全保障法施行は24年春と迫る

2023年2月、経済安全保障法制に関する有識者会議において、経済安全保障法制に関する基幹インフラの基本指針が示された。この中でリスク管理の実施状況について事前審査することが示され、前述の業務中断時の対応策（サイバーレジリエンス）や、外部委託先全体のBCP検証も事例として挙げられている。

今後、金融庁より、この指針に基づいた政省令、ガイドラインが公表される。法の施行開始は2024年春と迫っており、早急な体制整備が求められている。

事前審査は、主務省令で定める基準に該当する企業を対象としたものだが、それ以外の外部委託先企業も含めた課題の解決が求められる。検討対象範囲が広いことを念頭に事前審査開始に備え、BCP訓練計画策定などの取り組みを推奨したい。

Writer's Profile

斎藤 亜美 Ami Saito
金融ガバナンスプラットフォーム企画部
コンサルタント
専門はBCP、システムリスク、証券業務
focus@nri.co.jp