protiviti®

Face the Future with Confidence

事業継続管理のためのガイド
よくある質問トップ15

2020年8月

Internal Audit, Risk, Business & Technology Consulting

目次

序章

災難やつまずきは人生の一部です。天災、伝染病、データ漏洩、テロ攻撃など、世界中の災害や災難に関する悲鳴を上げるようなニュースが24時間報道されていますが、しばしば、チャンネルを変更したり、音量を下げたり、見出しをスクロールしたくなります。

しかし、ビジネスやプロセスのオーナー、チームリーダー、事業継続の実践者として、私たちは注意を払う必要があります。新たに発生したハリケーン（台風）が来週の出荷にどのような影響を与えるか、一晩で電子商取引を混乱させたクラウドの停止、さらなる業務のボトルネックを生み出す可能性のある新しい規制、報告期限を逃すことに対する市場の反応など、事業継続に影響を与えるあらゆることについて、私たちは日々心配しています。事業継続とは、事象の原因やコントロールできる範囲内であったかどうかに関わらず、さまざまなシナリオと対応手段を検討することを意味します。

COVID-19のパンデミックにより、あらゆる規模や種類のビジネスが前例のない方法で試されている現在の環境では、事業継続性とレジリエンスは、世界中の経営層の間で重要な議論となっています。パンデミックの広範な影響により、組織は事業継続計画（BCP）の見直しを余儀なくされ、BCPの実践を日々の業務にどのように組み込むかを検討することが迫られています。パンデミックによってもたらされた環境の変化を考えるとき、他のビジネスリスクが事業継続を脅かし続けていることを忘れてはなりません。自然災害や人災、技術的なリスクなど、さまざまなリスクが存在します。組織はどのようにしてこれらの事象に備えておくことができるのでしょうか。あらゆる危機のタイプやシナリオに対応する事業継続管理（BCM）プログラムを開発するにはどうすればよいのでしょうか。BCMプログラムを策定し、管理するには、組織内の誰が適しているのでしょうか。また、事業継続方針の重要な要素は何でしょうか。

Protiviti's Guide to Business Continuity Management: Frequently Asked Questions (June 2020)では、BCMやその他の関連実務における多くの喫緊の課題に答えています。段階的にリリースされる第4版の完全版では、以下のような多くの分野をカバーしています。

- COVID-19とパンデミック
- BCMの基本
- プログラム開発と戦略
- オーナーシップとガバナンス
- 規制環境
- 訓練と意識向上
- 検証と維持管理
- コンプライアンスの監視と監査

次の災害やビジネスの混乱がいつ発生するかは誰にも予測できません。唯一確かなことは、計画外かつ破壊的な事象が起こるということです。情報を常に入手しておくことは、未知の事態に備え、レジリエンスを構築するための第一歩であり、持続可能な事業継続プログラムを構築することで、企業がリスクに対するさまざまな準備・対応が行えるように支援します。

プロティビティ

2020年8月

COVID-19とパンデミック

1. パンデミックへの対応計画において、事業継続管理（BCM）プログラムはどのような役割を果たすべきか

パンデミック対策は、事業継続計画の重要な一部です。COVID-19が示しているように、パンデミックへの備えは、その地理的影響が広範囲に及ぶことや、その規模や期間を予測することが困難であることを考えると、企業ごとにさまざまな課題が散在し、幅広い影響を与える可能性があります（例：従業員の配置転換、技術的な制約、生産量の減少、サードパーティの能力に対する課題）。以下に、パンデミックに対する計画と対応においてBCMが果たすことができる重要な役割をいくつか挙げます。

- パンデミック対応の期間、BCMは、特別に定義された手順と危機管理コミュニケーションに関連することから、危機管理機能が継続的に機能していることを確認しなければなりません。混乱した状況下においては流動的な状況にも柔軟に対応可能であると定義された手順に従うことが、対応を成功させる鍵となります。パンデミックが発生すると、労働力が分散し、従業員、チーム、さらにはサードパーティ間で孤立感や断絶感が生じる可能性があるため、危機管理コミュニケーションには、社内外の両方の関係者を対象とした計画策定が必要とあります。

- 事業継続管理（BCM）プログラムは、パンデミックへの対応計画のインプットとして活用できる重要な情報を関係者へ提供します。他の計画（例：事業再開計画やIT災害復旧計画）と同様に、パンデミックへの対応計画の内容は、事業影響度分析（BIA）や継続的なリスクアセスメントのような基礎的な活動から情報を得るべきです。これらの取り組みの成果には、ビジネスプロセスの重要性、中断によって予想されるビジネスへの影響、最大許容可能な停止・中断している期間などの要素が含まれるべきです。また、これらの情報は、企業の対応を整理・体系づけたり、情報を提供するために使用することもできます。

- パンデミック対応に役立つもう1つの重要な情報は、各ビジネスプロセスが機能するために不可欠な重要なサードパーティを特定することです。これらの重要なサードパーティは、事業影響度分析（BIA）の間に、製品やサービスの提供が停止・中断した場合の影響とともに特定することができます。この情報はその後の戦略や計画の検討を進める上での指針となります。

- 事業継続計画では、多くの場合、事業に影響を与える可能性のあるさまざまな事象や災害を想定し、それらの事象や災害の間や後に組織がどのように対応すべきかを概説する規程等を作成する必要があります。これらの規程等は、チェックリストや順序立てられた詳細な手順や計画が記載されたもので、一般的にはシナリオにとらわれない（すなわち、人為災害/自然災害などの災害の種類や原因、規模を問わず、すべての災害に対して同じ原則で行動する手法）ものです。パンデミックやその他の危機や災害の影響を管理するための最も効果的な方法は、成熟したBCMプログラムの一部として開発された規程等で定義された対応を実装することです。

2. パンデミックへの対応を策定する際に、事業継続に関する重要な考慮事項や優先事項は何か？また、COVID-19から考えられる、将来の事業継続計画に反映する教訓は何か？

まず、従業員や顧客の健康と安全の他、人命への配慮が優先されるべきです。事業の継続的な運営、あるいは事業資産の維持・保全は、人命、健康、安全の保全に次ぐものでなければなりません。このような対応がなされることにより、ビジネスを推進する主要な人、プロセス、テクノロジーに焦点を当てた、より伝統的なリスク管理プロセスに注力できます。以下は、パンデミックへの対応を策定する際に考慮すべき重要な事項です。

- 重要なのは、自社において重要な事業目的を理解し、パンデミックに関連するどのリスクが重要な事業目的の達成を阻害する可能性があるかを理解することです。事業目的をしっかりと理解することで、それらのリスクを許容できるレベルまで軽減することに時間、リソース、注意を集中させることができます。

- パンデミックのような長期化する事象では、リスクを特定し、追跡し、管理するための継続的かつ適宜更新するプロセスを持つことが不可欠です。新たなリスクの出現や、既存のリスクについて、企業はその変化を継続的に監視し、変化に応じた対応の検討が必要になります。

- 組織は、特にプロセス間の依存関係、主要な人員のリスク、主要なサードパーティ、および重要なアプリケーションに関連して、パンデミック前に認識した影響度が正確であったかどうかを判断するために、過去の事業影響度分析の結果を再確認する必要があります。

- 以前に確立された影響許容度を、混乱に直面した期間に経験した実際の影響と比較し、組織の真の影響許容度を再調整することで、組織が今後の戦略と計画を強化するのに役立ちます。

事業継続計画自体が常に更新されることが求められます。COVID-19の危機が収束していないにもかかわらず、何が起こったのか、何を学んだのか、そして、危機的な状況が再び訪れた際に効果的に対応するためには何を変えるべきかを理解するために、事後対応の活動を開始している企業もあります。

3. BCMプログラムは、従業員のパンデミック後の生活や働き方をどのように支援すべきか?

優れたBCMプログラムの中核をなす構成要素は、事業再開、危機管理、IT災害復旧(ITDR)です。事象の発生期間を超過する事業継続ライフサイクルの中で、それぞれが重要な役割を果たしており、事象後に組織がどのようにして正常な状態に戻るかについても対応することになります。例えば、危機発生時に形成された危機管理チームは、ビジネス上の重要な意思決定をタイムリーに行い、対応を指示・指導するチームであり、通常業務の復旧活動を指導するチームでもあります。

同時に、全従業員が一斉にリモート環境に移行できるようにインフラや通信等を整備するためにIT災害復旧プログラムの実行を支援するIT専門チームは、従業員が平常時の状態に戻ることを支援する責任を負っています。

BCMの基本

4. 事業継続管理(BCM)とは何か?

BCMは、企業に重大な損害を与えたり、潜在的に重大な損失をもたらす可能性のある活動やビジネスプロセスが中断した場合に、その活動やビジネスプロセスを保護したり、代替的な運用方法を提供したりする戦略、チームや計画を設計、開発、実施、維持することを示すことになります。BCMの進化に伴い、脅威に対する将来の見通しは大幅に拡大しており、内部および外部の事象や、極端でありながらも起こりうるインシデントも含まれるようになっています。

BCMは3つの主要な統制で構成されています。

- **危機管理とコミュニケーション** — この規律は、事象への効果的かつ結束力のある対応を可能にします。危機管理プロセスは、状況の安定化に焦点を当て、業務の代替手段が必要な場合は、効果的な計画、リーダーシップとコミュニケーション手順の連携により事業をサポートしています。

- **ビジネス再開・回復計画** — この規律は、顧客に対する主要な製品やサービスの提供、または支援するビジネス機能およびプロセスが破壊されることに焦点を合わせています。ビジネス再開プロセスは、組織の業務に不可欠な人、プロセス、テクノロジー、その他のリソースの評価に焦点を当てています。事業再開計画の目的は、原因の如何に関わらず、能力が低下した業務の状況を乗り越え、通常通りの業務遂行に向けて人員を導く計画を策定することにより、混乱から生じ得る影響を緩和することです。

- **IT災害復旧(ITDR)** — この規律は、システム、アプリケーション、データベース、ストレージ、ネットワーク資産などの重要なIT資産の復旧について対処します。ITDR戦略はまた、すべての技術的利害関係者が一致していることを保証するために、すべてのテクノロジーサービスプロバイダとの関係(例:クラウドプロバイダ)を網羅する必要があります。

上記の伝統的なBCMの規律に加えて、多くの組織では、全体的なBCMプログラムの一部として、他の密接に関連するプログラムも管理しています。これらのプログラムには、以下が含まれます。

- **インシデント管理(またはインシデント対応)** — この用語は一般的に、破壊的な事象への対応を特定し、分析し、管理することを指します。名称に関わらず、インシデント管理プログラムには、一般的に、施設からの避難、応急対応やその後の追加対応などの緊急対応策が含まれます。

- **サイバーセキュリティインシデント対応** — こちらはデータ侵害、フィッシングの試み、分散型サービス拒否(DDoS)攻撃などのサイバーセキュリティインシデントの計画、対応、復旧に関するものです。

事業継続の性質上、事業継続計画のさまざまな段階で複数の機能が統合されることが一般的です。例えば、施設や物理的セキュリティチームが緊急時の管理活動に従事したり、安全・環境衛生チームが復旧戦略の策定に関与することがあります。一方で、組織や業界によっては、これらの企業に影響を与える機能の統合は、混乱を招く可能性があります。

5. BCMプログラムを設計し、展開することは、組織にとってどのような価値があるか?

BCMの価値はリスク軽減にあり、通常のビジネスの中断に伴うリスクを最小限に抑えることにあります。最近の壊滅的な自然災害やCOVID-19におけるパンデミックを受けて、ビジネスリーダーはビジネスの混乱に対応するための計画の策定、対応する必要性をこれまで以上に意識しています。

ビジネス環境は、事業の継続だけでなく、従業員やブランドの保護、収益の獲得、業務連携の維持、規制の遵守などの企業の経営能力に影響を及ぼすようなリスクに満ちています。企業は、混乱に備えた計画を立て、優れたビジネス慣行を採用し、物事がうまくいかなくなったときに迅速に軌道修正できるように先見性をもって行動するため、優先順位を理解し、リスクを先取りしていく必要があります。

組織は、企業運営にとっての重要なリスクを管理するためのBCMの手法を積極的に設計し、展開することで、企業価値の維持発展を可能にします。例えば、企業は、主要なサプライヤーの損失に備え、コンティンジェンシープランを設計することで、潜在的な財務、業務、レピュテーションに関する影響を軽減することができます。

財務リスク — これは最も明白で定量的なリスクの領域です。企業は下記のものを含む複数の要因に焦点を合わせることによって財務上の損失を最小限に抑えることにより、市場占有率の極端な低下を防ぐことを可能にします。

- 顧客の要求に対応し、実行可能なサプライチェーンの維持
- 役員の責任の理解
- 交換が必要な潜在的な損失（破損した資産の交換費用）の棚卸

サプライチェーンを保護し、顧客の需要に確実に追いつくようにするために、企業は、サプライヤーに対して、自社の業務に影響を与えるサプライチェーンの混乱について責任を求めることが考えられます。例えば、企業は契約条項を利用して、製品やサービスの納期の適時性や、納品された製品やサービスの品質についてサプライヤーに責任を求めることが考えられます。

企業はBCMの手法を導入することで、単一障害点（SPOF）や重要な外部依存に起因する莫大な予想外のコストが発生する可能性を最小限に抑えることができます。例えば、ある企業がある重要なサプライヤーに依存しており、主要な製品やサービスを突然提供できなくなった場合、適切に設計されたBCMの手法は、財務上の損失等不測の事態に備えた対応が可能となります。

業務遂行上のリスク — このリスク領域は、企業が主要な製品やサービスを期待通りに提供できなくなることに起因するリスクの領域です。これには、設備やテクノロジーの陳腐化、内部機能の障害、リーダーシップチームの予期せぬ変更などに関連するリスクが含まれます。その他、通常の業務に直接影響を与える業務遂行上のリスクとしては、以下があります。

- 単一障害点（SPOF）における障害と重要な外部依存性による損失
- 生産性の低下（従業員が相当期間に亘って業務が遂行できない状況）
- 対応損失（混乱に対応するために必要な時間や素材調達のコスト）

企業は、BCMの手法を導入して、異常な状況下でも、運用上のギャップを最小限に抑え、製品やサービスの提供を継続できるようにしなければなりません。BCMプログラムの包括的な導入は、準備、計画、対応に関連するリスクを低減し、全体的な運用リスクを低減することができます。

規制リスク — 規制当局は、検証された能力、チーム、計画を維持することに対する企業の責任を問う傾向が強まっており、BCMプログラムを実施していない企業には罰金を科すこともあります。規制当局にもよりますが、規制対象となる事業体での問題が繰り返し発生し、軽減されていない場合には、対応状況を公開する対象となり、企業の信用力やレピュテーションに影響を与える可能性があります。一般的に、規制やコンプライアンス要件に違反した企業は、以下のようなコンプライアンス要件に直面します。

- 罰則、裁判所の判決
- 要注意事項（MRA）または規制当局からの同様の指摘により、より精密な調査またはより高いパフォーマンスが要請される可能性があります。

レピュテーションリスク — 好ましくない情報に関する外部への報道は、収益の減少、不必要なソーシャルメディアでの注目、時価総額の低下、また長期的には、企業の状況を注視している人々による否定的な評価を引き起こす可能性があります。今日のように、いつの時間帯においても報道されるニュースは、どのような出来事に対しても、慎重に、共感を呼ぶように、迅速に、そして関連性のある対応をすることが、好意的なレピュテーションを維持するために非常に重要となります。成熟したBCMプログラムによって、競争が激化する中で変化し続けるビジネス環境を巧みに管理することで、企業のブランドを保護し、企業価値を高めます。

6. BCMには、見た目は類似している一方で多くの異なる用語が含まれているが、類似点と相違点は何か？

BCMが混乱しやすい理由の1つとして、規制当局や業界団体がBCMに関連する用語をどのように定義し、使用しているのかの類似点や相違点があります。以下にいくつかの例を示します。

危機管理とコミュニケーション

- **業務継続計画** — 政府機関や団体は、幅広い事象や災害に関連した重要な機能のための方針や指針を確立するために、この用語を一般的に使用します。

- **緊急事態管理およびオペレーション** — この用語は医療領域で一般的に使用され、特に臨床（すなわち患者の立場に立った）の側面における緊急時対応計画で使用されます。他の業界では「危機管理」と同義に使われることもありますが、一般的には事象発生直後の初動対応のことを指します。

- **緊急対応** — この用語は、多くの場合、より広範な危機管理プログラムの一部として、人命を保護し、財産や資産を保護するために取られる即時の行動を意味します。建物からの避難計画は、緊急対応行動の一例です。

- **インシデント管理および対応** — この用語は、「危機管理」と代替的な言葉として使用されることがあります。また、一般的には、ハリケーン（台風）、地震、物流業者のサプライチェーンの混乱など、特定の事業体や場所に影響を及ぼすさまざまな事象への対応を指す場合にも使用されます。最近では、企業は危機管理プログラムの一環でインシデント対応計画を策定し、危機的状況におけるエスカレーションや報告に関連する共通のハイレベルな手順として活用しています。この対応により、企業は機能や施設に影響を与える可能性のあるシナリオを想定して、設計された計画を迅速かつ効率的に実行に移すことができます。

- **メジャーインシデント管理（MIM）** — この用語は、事業活動に多大な影響を与える中断に対する対応を指します。「危機管理」と代替的な言葉として使用されることがあります。

- **レジリエンス** — この用語は、事業継続を維持する中で、企業が混乱に耐え、迅速に適応する能力を指す常に進化し続ける概念です。レジリエンスは、事業活動の全体、またはプロセスや機能が、あらゆる状況下で柔軟性を維持する能力を確保するために、事業を維持することに焦点を当て、定期的なメンテナンスが必要となります。最近では、テクノロジー・レジリエンス、ビジネス・レジリエンス、サイバー・レジリエンスといった形で使われることがあります。

事業再開計画

- **事業回復計画** — この用語は、災害時の情報のインプット/アウトプット、人的資源、IT、および物理的な作業場所の計画に関連して、個々のプロセスまたはビジネスラインのために取られるさまざまな手順を指します。この用語は、「事業再開」、「コンティンジェンシープラン」、「事業継続計画」と代替的な言葉として使用されることがあります。

- **事業継続計画（BCP）** — この用語は、事業継続管理（BCM）の計画的側面を表すために使用されます。BCMは通常、包括的なプログラムを指すのに対し、BCPは災害時に事業活動を回復するために取る事前に定義された一連の手順です。この用語は、「事業再開」、「コンティンジェンシープラン」、「事業回復計画」と代替的な言葉として使用されることがあります。

- **事業再開計画** — この用語は、事業機能の回復に焦点を当てています。この用語は「事業回復」、「コンティンジェンシープラン」、「事業継続計画」と代替的な言葉として使用されることがあります。

- **コンティンジェンシープラン** — この用語は、チームや機能が中断した事業を再開するために取る一連の戦術的な手順を指します。この用語は、「事業回復」、「事業再開計画」、「事業継続計画」と代替的な言葉として使用されることがあります。

IT災害復旧（ITDR）

- **災害復旧** — この用語は、災害時における重要なテクノロジー資産の復旧と再開を意味します。災害復旧には、IT環境全体の復旧、個々のシステムの再開が含まれます。災害復旧は、BCMプログラムの構成要素の一部と位置付けられます。

注：上記のリストは包括的なものではありません。特定の業界での慣行や規制状況によっては、BCM用語の使用方法に影響を及ぼす可能性があります。

7. 危機管理と危機におけるコミュニケーションの違いは何か?

危機管理とは、想定外の事象が発生した場合に、その事態を安定化させ、被害の拡大を防ぐための企業の総合的な取り組みのことです。危機管理は、経営陣が管理するすべての組織レベルで行われます。危機管理には、コミュニケーションや広報、法規制、環境・健康・安全(EHS)、人事、法務、企業セキュリティ、およびすべての事業部門など、すべての部門における初動対応が含まれます。

危機におけるコミュニケーションは、危機管理の重要な要素として、従業員、顧客、地域社会、規制機関、株主、取締役会、その他緊急事態によって影響を受ける可能性のあるすべての人を対象とした連絡を含む、事象発生前、発生時、発生後のコミュニケーションを指します。危機におけるコミュニケーションは、製品のリコールからデータセンターでの火災に至るまで、危機とみなされるあらゆる種類の事象発生時に展開することができます。危機におけるコミュニケーションのトレンドとして、社内外のコミュニケーションのために多くの領域に携わるメンバーで結成されたチームが一緒に情報発信に取り組むことが挙げられます。広報、営業、情報システム、人事、IRといった部門が協力して、社内外に向けたメッセージを作成し、配信します。

以下の例は、危機管理と危機におけるコミュニケーションがどのように連携しているかを示しています。

製造業の取締役がCOVID-19に感染していることが確認された後、環境・健康・安全(EHS)に係る部門は、危機管理チームに、役員の体温が1週間を通して上昇していたが、追加の症状が現れるまではウイルスの懸念はなかったことを通知しました。取締役は2つの製造工場を監督しており、会議のために常に本社オフィスにいます。EHSは危機管理チームに、取締役が1週間を通して3つの拠点すべてに出勤していたことを伝えました。危機管理の主要チームは、次のような決定を下します。

- CEOは、追って通知があるまで両工場と本社オフィスを閉鎖することを決定。
- 顧問弁護士は、施設を再開する前に全従業員による検査を要求するようCEOに助言。
- CFOは、操業停止に関わらず、従業員に給与を支払うべきだと判断。
- CROは、感染者確認に起因するさまざまな規制上の影響を指摘。
- 危機におけるコミュニケーションチームは、すべての決定事項を社内に展開し、外部のステークホルダー(顧客、株主、規制機関)に向けて声明を発表。

この例のように、危機におけるコミュニケーションのプロセスは危機管理チームの意思決定に依存しており、事業と社内外の利害関係者との連絡係となります。

プログラム開発と戦略

8. 事業継続計画のベストプラクティス・アプローチは何か？

事業継続管理（BCM）のアプローチや範囲はさまざまであり、ある規模のものが全てを賄えるものではありません。BCMプログラムを推進していくためには、ビジネスの復旧要件（および制約）が必要となります。推奨されるいくつかの付帯要件やプログラムの性質によっては、すべてのBCMプログラムに統合されるべきものがありますが、BCMプログラムに組み込むプロセスはさまざまです。

- **BCMプログラムガバナンス** — BCM運営委員会の特定と正式化、および、BCMプログラム要件を決定するための経営陣レベルでのリスク管理・監督が含まれます。

- **BCMプログラムと導入設計** — 事業継続の取り組みをサポートするための方針、標準、ツールを定めることが含まれます。さらに、効果的なBCMプログラムでは、プログラムの各主要分野（危機管理、事業再開、IT災害復旧（ITDR）など）における責任者と責務を定義することが必要です。また、プログラムのタスクの監視と管理に使用されるテクノロジーツールや定義された主要リスク指標（KRI）と主要業績指標（KPI）を含みます。

- **事業影響度分析（BIA）** — BIAは、BCMプログラムの基礎となるリスクアセスメントの一種であり、組織の混乱によるビジネスへの潜在的な影響（すなわち、業務、レピュテーション、財務、規制やコンプライアンスにおける影響）を把握し、効果的に測定することができます。BIAの目的は、ビジネスプロセスや各プロセスが依存しているリソース（すなわち、テクノロジー、作業場所、機器類、人員、サードパーティ）の復旧における優先順位を確立することです。

- **リスクアセスメント** — BCMの用語では、継続的なリスクアセスメント（CRA）と呼ばれることがあり、組織に対する脆弱性への脅威や障害シナリオの特定や優先順位付けを含みます。継続的なリスクアセスメント（CRA）の範囲は、全社的リスクアセスメント（ERA）ではなく、業務に直接的なリスクをもたらすシナリオ（例えば、サプライチェーンの混乱、テクノロジーの停止、情報漏洩、業務が行われる人口密集地域における悪天候など）が含まれます。

- **戦略の策定と実行** — 費用対効果分析と業務上のリスク許容度に基づいて、組織のニーズを最もよく満たすように継続性のある戦略を策定・実行することは非常に重要です。継続的なリスクアセスメント（CRA）と事業影響度分析（BIA）の結果は、復旧戦略の策定にとって有用な情報となります。

- **計画の文書化** — 特定のリスクにおける実行可能な復旧戦略の策定に続いて、効果的な事業継続運営を可能にするために、対応、回復および復旧手順を文書化しておく必要があります。特に危機管理、事業再開、IT災害復旧（ITDR）といった分野には、文書化した戦略や計画を備えておく必要があります。

- **検証** — 定期的に検証されていないBCMプログラムは、自信を持って信頼することができないものです。事業継続戦略とそれに対応するチームと計画の妥当性を検証し、継続的に改善することが重要です。BCMプログラムの信頼性を確保するためには、各主要分野のチームや計画に対して、個別、または並行で厳密な検証を実施する必要があります。

- **訓練と意識向上** — 従業員が事業継続活動に関するそれぞれの役割と責任について知識を有していれば、組織にとってより良い運営準備になります。訓練は、対応/復旧チームの取り組みに直接責任を持つ者、および復旧チームに直接関与していない者を含め、すべての従業員に提供される必要があります。

- **コンプライアンスの監視と監査** — BCMプログラムの定期的かつ客観的なレビューを実施することで、必要に応じてプログラムを変更することができます。また、レビューにより、内部およびサードパーティの事業継続に関する基準への遵守を維持しやすくなると言えます。

9. 事業継続方針の重要な要素は何か?

BCMプログラムをサポートするために、正式に文書化された事業継続方針を策定する組織が増えてきています。一般的に、事業継続方針の内容や形式は、組織における既存の基準や文化によって異なるものです。以下に、事業継続方針の重要な要素を示します。

- **説明責任** — BCMプログラムの計画と実行に責任のある役員、およびリソースの調達や戦略の意思決定に責任のある役員を特定します。
- **役割と責任** — 災害前、災害中、災害後の計画と活動に関する全従業員の役割と責任を定めます。
- **プログラムの範囲** — 継続的なリスクアセスメント(CRA)と事業影響度分析(BIA)を通じて、プログラムの理念と復旧の優先順位を定義します。さらに、この基本的な取り組みによって、BCMプログラムで対処すべきインシデントの種類や規模の基準を確立します。
- **復旧戦略の策定** — 影響の大きい事象への準備、対応、および復旧を可能とし、関連性のある適正規模の戦略を策定するために必要とされる具体的な行動を特定します。復旧戦略は、主要な人員、主要なプロセスやテクノロジー、主要な作業場や施設などの損失による影響を緩和するために策定する必要があります。
- **計画の策定と維持管理** — すべてのプログラムや計画文書のレビューと維持管理に関する基準を規定しています。
- **検証(演習)** — 検証活動のさまざまな種類、頻度、必要とされる参加者(例えば、社内の従業員、外部のビジネスパートナーやサードパーティのサービスプロバイダなど)を定義します。個別の演習の計画(例えば、範囲、目的、達成基準の定義など)と検証結果の収集は、方針に従って実施する必要があります。
- **訓練と意識向上** — 対応計画および復旧計画に記載された要員の役割に応じた訓練の基準を確立し、事業継続戦略の影響を受ける従業員の一般的な意識向上を図ります。
- **法律、規制、契約上の評価** — 該当する場合は、事業継続要件に影響を与える法律、規制、業界標準、および顧客の契約要件に関して、組織としての理解を把握します。
- **内部監査への参加** — 計画プロセスおよび/または事業継続方針に定められた要件の遵守状況のレビューに係る内部監査の役割を定義します。
- **参考文献** — BCMプログラムで利用している用語集、業界の情報源、標準、ガイドライン、規制、および各種方針へのリンクを提供します。

上記のような事業継続方針における重要な要素は、BCMプログラムを効果的に管理できるように、必要なサポートとリソースを収集する組織の計画策定チームを支援します。

10. 事業継続計画において網羅的なBIAおよびリスクアセスメントを実施する代わりに、どのような選択肢があるか?

事業継続性に影響する短期的な事象を計画する際、組織は、数カ月にも及ぶような正式な事業影響度分析(BIA)やリスクアセスメントに必要な厳密かつ詳細な分析作業を合理化するために、独創的なプロセスを導入するケースが増えてきています。組織にとって、多くの場合、環境、人為的、ビジネスプロセス、サプライチェーン、ITに係る継続性リスクのすべてを網羅的に分析する時間はありません。

リスクを特定し、復旧の必要性に優先順位をつけるための1つの選択肢として、エグゼクティブ・ワーク・セッションを通じ、簡略化された事業影響度分析(BIA)および/またはリスクアセスメントを実施することがあります。ファシリテーターは、ハイレベルの機能横断的なチームを率いて、ビジネス機能やテクノロジーレベルではなく、組織レベルでの影響を定義し、それを基にビジネスプロセスやテクノロジーの優先度、復旧目標、復旧順序の確立を支援します。このプロセスは、組織全体のビジネスリーダーからのインプット情報を利用して、何週間もかけて結論を出すのではなく、数時間で予備的な結論を出すように設計されています。

包括的で継続性のあるリスクアセスメントの代替案として、BCM運営委員会および/またはプロジェクトチームは、現実的なワーストケースのシナリオを定義することで、範囲や計画プロセスを簡略化した情報を提供することができます。このシナリオは、組織全体に影響を与えるべきものであり、計画策定担当が対応・

復旧戦略の策定を支援する際にフレームワークを提供することができます。このアプローチの価値は、混乱の引き金となる事象の種類ごとに分析することなく、混乱による多数の影響を識別する合理化された方法にあります。多くの組織にとって、影響の少ない事象の計画のためにワーストケースのシナリオを使用することは役立つものとされています。

リスクアセスメントや事業影響度分析（BIA）プロセスを簡略化したアプローチで代用しても、組織のすべてのリスクと影響を完全に把握することはできませんが、上記の例は、特に組織が明確な期限に直面している場合や、経営陣がBCMプロセスを正式に承認していない場合に、計画プロセスを迅速に開始するための方法を提供するものです。今後、組織内の複数のレベルからの情報や視点を考慮し、より徹底した分析を行うことで簡略化されたプロセスを更新していく必要があります。

オーナーシップとガバナンス

11. BCMプログラムの管理は、組織内の誰が行うべきか?

組織がBCMプログラムの機能や計画を策定し始めると、「プログラム全体を誰が管理すべきか?」という共通の疑問やジレンマに直面することがあります。BCMプログラムを成功させるためには、組織内でさまざまなレベルの説明責任や責務が必要です。一部の組織では、最終的にプログラムを管理するために別のビジネス機能やユニットの設置を決定する場合もありますが、多くの組織では、既存のリソースや人材を活用することを選択します。

組織は通常、スポンサー、オーナー、BCM事務局(BCMの主導的な役割を果たす管理者)の3つの役割のいずれかを通じてBCMプログラムにおけるリーダーシップを発揮します。

スポンサーは、組織的・財政的な支援を提供・保証します。役員会や経営陣への一貫した可視性が不可欠であることを考えると、スポンサーは経営者であるべきです。

オーナーは、直接的な説明責任を負うか、プログラム全体のサポートや実行を確実にする責務を負います。BCMのオーナーは、戦略を理解し、年間計画を実施し、日常の業務を管理する者との直接的な関係を持つ部門のリーダーです。最後に、BCM事務局(BCMの主導的な役割を果たす管理者)は、組織全体で実行されるBCMタスクを調整することが主な責務となります。

BCM事務局(BCMの主導的な役割を果たす管理者)は、包括的なプログラムの各側面に必要とされるさまざまな役割を理解し、タイムリーで首尾一貫した方法で懸念事項をエスカレーションする権限を与えられています。

上記のような監督の役割は、それぞれのBCM分野に合わせて調整されることは珍しくありません。例えば、CTO、CIO、CISOがITに係る災害復旧プログラムを担当し、マーケティングの責任者が危機管理を担当することもあります。一般的にBCM運営委員会やその他の同様の意思決定・ガバナンスグループが監督機能を有しています。

BCMプログラムには、推奨される単一の構造はありません。企業の業界、リスクプロファイル、文化、業務の意味合いの相違によって、BCMをどこに位置づけるべきかの決定に影響を与える可能性があります。例としては、以下のようなものがあります。

- **財務** — CFOの機能またはライン組織
- **執行委員会** — 上級管理職チームのサブ組織(法務、人事、広報の責任者などが含まれることがあります)
- **業務執行** — COOの機能またはライン組織
- **リスク管理** — CROの機能またはライン組織
  指定された資格要件を満たす事業継続に係る専門職が業務遂行リスクへの対応プログラムにおいて最も直接的に連携するため、最も一般的なものであると言えます。
- **IT** — CTO、CIOまたはCISOの機能またはライン組織

事実上、成熟したBCMプログラムを全面的にサポートしながら、権限者に対して可視化し会社の意思決定に影響を与えるようにするためには、BCMプログラムのオーナーシップを組織内の経営陣レベルで維持することが推奨されます。

12. 内部の事業継続機能や計画チームはどのように構成されているか?

組織の事業継続機能の規模や構成は、以下のように企業のさまざまな特性に依存します。

- 従業員数
- 会社所在地や事業所数や地理的な分散
- 事業部、子会社、組織単位での業務の類似性
- 経営の監督やリーダーシップの体制として、中央集権型か地方分権型かの程度
- 組織のリスクプロファイル(例えば、高度に規制されている、外部の監督機関によって管理されているなど)

組織全体の事業継続の取り組みを数名の個人が担当するのが

一般的になっていますが、多くの企業では、効果的なBCMプログラムを維持するためには、本来は皆の協力が重要であると認識しています。特定の部署やそれぞれの現場の最前線のリーダーやサポートチームのように基盤となるビジネスプロセスの複雑性を知る者はなかなかいません。

このように、部署の事業影響度分析（BIA）や復旧計画が最新で実行可能なものであることを確認するためには、BCMのリーダーは、現場の人々からの意見や関与を求める必要があります。

同様に、BCMのリーダーは、重要な復旧の優先順位をIT組織に伝え、関連するIT災害復旧計画とそれをサポートするテクノロジーが事業の復旧ニーズと一致していることを確認するためのパイプ役としての役割を果たす必要があります。製造業やエネルギー、公益事業のような業界では、業務運営のテクノロジーがIT組織の企業などと同じような方法で管理されていないため、専門的な知識を容易に利用できない場合があります。このような組織や業界では、BCMのリーダーが特定や優先順位付の際に役立つ重要な回復や復旧の要件があるかもしれませんし、後続する復旧計画文書で優先順位をつけた対応に影響を及ぼすことになるかもしれません。

BCMのリーダーは、明確に定義された役割と責任を有し、経営陣による支援と後ろ盾を有する必要があります。さらに、多くの組織では、BCMの責任の一部が複数のレベルの担当者に委譲されていることも珍しくありません。このような場合は、経営陣が関与し、BCMプログラムを全面的に管理する際に、すべての利害関係者に対して組織のニーズに焦点を当てるように調整する必要があります。

運用モデルの観点から、BCMプログラムは、中央集権型、分割型、連合型の3つの主要モデルのうちのいずれかに整理することができます。

- **中央集権型** — このモデルでは、本店事業所が、各ビジネスユニットに対して、方針、ガイダンス、ツール、テンプレート、評価基準、メンテナンスといった情報を提供します。

- **分割型** — 複数の事業所が異なる地域やビジネスラインにサービスを提供します。

- **連合型** — 本店事業所とさまざまな中核拠点とリンクし、さまざまな地域やビジネスラインに専用のサービスを提供します。

13. 組織の事業継続の取り組みを全面的に支援するために、経営陣をどのように説得するか？

BCMプログラムの全般を通じて、計画、訓練、文書化、検証に費やされた時間とリソースの価値は、本当に何か問題が発生するまでは実感できないため、BCMは多くの場合、自由裁量の取り組みとみなされることがあります。規制要件や監査結果、特定の顧客からの要求がない場合、経営陣にBCMの取り組みを全面的に支援するように説得する最も効果的な方法は、リスクを強調する演習（例えば、事業継続リスクアセスメントと事業影響度分析（BIA））を実施し、その結果を共有することです。演習の結果には、通常、復旧の優先順位、対応する推奨事項、業界のベンチマークデータが含まれており、経営陣は、組織の事業継続のニーズを完全に把握することができます。

事業継続の取り組みの価値は、費用対効果分析によっても経営陣に伝えることができます。費用分析では、既存のビジネスやテクノロジー環境の主要な領域において、レジリエンスの保持、レジリエンスの強化のために必要な資金とリソースを投下します。一方、利益分析では、破壊的な事象（例えば、収益機会の損失、事業停止期間、会社財産の毀損、レピュテーションの低下など）の潜在的な影響を回避することに関連しています。

経営陣と共有できるもう1つは、確認済みのBCMプログラムを実施した結果による、組織の保険会社からの事業中断保険料の節約についてです。BCMプログラムの実施は、企業が役員（D&O）賠償責任保険の調達コストの節約を実現するのにも寄与します。受託者の観点からは、役員が事業中断に対する組織の対応に対して、個人的な責任を問われる可能性があることを理解している場合、BCMをサポートし、実施する可能性が高くなります。

規制環境

14. BCMプログラムの開発において、規制や基準をどのように利用すべきか?

BCMの規制や基準は、コーポレート・ガバナンスやリスク管理への関心の高まり、テクノロジーの破壊や壊滅的な事象による影響への対応のために、ますます強化されています。この強化は、脅威の状況が進むことに対して、従業員や組織のサービスに依存しているすべての人々(利用者、顧客、患者など)への保護を強化することを含め、組織が効果的な継続対応を展開できるようにすることを目的としています。

規制や基準は、BCMプログラムの策定を支援し、遵守度を測定し、成熟度を評価するために使用されます。規制や基準は、BCMにおいて焦点を当てるべき、または、推奨される分野やアプローチに関するガイダンスは提供しますが、計画文書の具体的な項目やフォーマット、詳細レベルを指し示すことはほぼありません。最も包括的なガイドラインや基準としては、金融サービスを対象としたものがあります。すべてのベストプラクティスをモデルにしているため、金融以外の業界で、より厳格なガイドラインを使用し、関連するコントロールや戦略に適用することは珍しくはありません。

15. オペレーション・レジリエンスと事業継続管理の関係は何か?

世界中の規制当局は、英国の監督当局が中心となって、金融サービス部門でのオペレーション・レジリエンスの強化を目的とした新たなルールと期待を展開しています。オペレーション・レジリエンスとは、組織が事業環境の不利な変化に耐え、ビジネスサービスや経済機能の提供を継続する能力のことです。以下では、オペレーション・レジリエンスプログラムによる従来のBCMの実践やコンセプトを強化・拡張するためのさまざまなアプローチを紹介します。

- **重要なビジネスサービスの特定** — これらには、ATMのアクセスの中断や支払い処理の低下といった、障害が発生した際に最終消費者に直接影響を与える可能性のある、最も重要な主要製品や基幹業務が含まれます。

- **影響許容度の設定** — 従来のBCMプログラムでは、リスク許容度は容易に定量化できず、リスク許容度に関する記述の多くは、将来の見通しを示す指標や、危機発生時に行動(制御オプションの発動など)を起こすための閾値を文書化していません。オペレーション・レジリエンスの下では、金融機関は、その重要な業務サービスに対する定量的な影響許容度を開発することが期待されています。

- **検証** — BCMプログラムと機能のさまざまな側面を検証することは、通常、IT、業務執行、または危機管理チーム内で個別に行われます。ほとんどの場合、これらの検証は、テスト対象となる機能や業務のすべての側面を検証するような形では行われていません。オペレーション・レジリエンスの下では、組織は、現実的な復旧時間と確立された影響許容度とをよりよく理解するために、極端ではあるが現実的なシナリオを検証することが期待されています。さらに、完全なシナリオ検証は、障害や脆弱性の領域や事業中断事象を引き起こす可能性のある集中リスクを特定する上で重要となります。