

事業継続マネジメントシステム(BCMS) 事始め

社団法人日本工業技術振興協会
事業継続マネジメントシステム(BCMS)研究会

2010年9月15日 発表

目次

第 1 章	BCMS の考え方	3
第 2 章	BCMS 導入の前にすること	9
第 3 章	目標の設定	17
第 4 章	リスクアセスメントとビジネス影響度分析 (BIA)	20
第 5 章	インフラの脆弱度と影響度評価	28
第 6 章	関係要員の脆弱度と影響度評価	31
第 7 章	外部から購入して部品・材料・サービスの脆弱度と影響度評価	39
第 8 章	IT システムの脆弱度と影響度評価	45
第 9 章	重要な経営資源への対応	50
第 10 章	予防対策	52
第 11 章	緊急時対策	61
第 12 章	継続対策	66
第 13 章	復旧対策	68
第 14 章	訓練	72
第 15 章	BCMS 構築のための組織	76
参考文献		79

第 1 章 BCMS の考え方

多くの方には「事業継続マネジメントシステム」は見慣れない用語と思います。事業継続マネジメントシステムは英語では Business Continuity Management System (BCMS)と言います。これは、企業が抱える災害・事故・事件(以下「災害など」の対策を総合的に管理する手法である事業継続マネジメント(BCM)に、品質 ISO や環境 ISO で知られている PDCA サイクルを含めた考え方です。BCM で企業の防災力などの改善を、PDCA サイクルで改善するシステムの整備を目指しています。

なお、この資料では IT 関係の事業継続性も取り上げていますが、ISO の技術委員会では一般的な BCMS (ISO 検討文書 22300 シリーズ)とは別の文書 (ISO 検討文書 27031)で IT 関係の事業継続性に対処する方向で検討が進められています。

- ISO 検討文書 22300 BCMS の用語
- ISO 検討文書 22301 BCMS の要求事項
- ISO 検討文書 22399 BCMS のガイドライン
- ISO 検討文書 27031 ICT の事業継続ガイドライン

1.1 企業防災との違い

BCMS はたびたび企業防災と比較されます。両者の一番の違いは、BCMS は全社的な立場で考え、企業防災は拠点の立場で考えることにあります。例えば、工場や店舗が不幸にして地震や火災などで大規模に被災した場合ですが、企業防災の立場ではその被災した工場または店舗をなるべく早く復旧し、事業や業務の再開を目指します。これに対して BCMS は、被災した工場や店舗の事業を他の工場や店舗で代行出来ないかを考えます。ここが違います。

なお、この他の工場や店舗での代行活動を「継続対策」といいます。

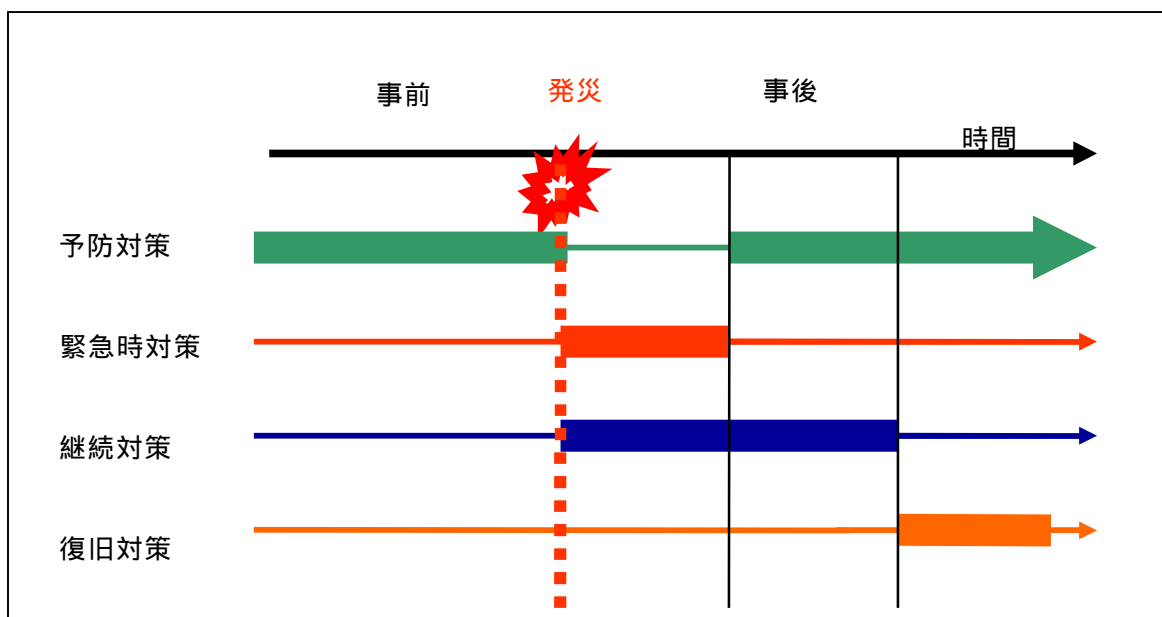
- 企業防災 = 予防対策 + 緊急時対策 + 復旧対策
- BCMS = 予防対策 + 緊急時対策 + **継続対策** + 復旧対策

1.2 予防対策、緊急時対策、継続対策、復旧対策

図表 1 は、各対策の活動状態を表したもので、太線の部分は実際に活動をしている期間、細線の部分は活動の準備期間です。災害・事故・事件の被害程度により、緊急時対策・継続対策・復

旧対策の活動期間(図表中の太線部分)は長くなったり、短くなったりします。

図表 1 時間と各対策との関係



(注1) この図は地震や事故など突発的な発生事象の場合で、台風や噴火のように事前に被害の発生が予見できるものは、予見可能時から緊急時対策が開始される

(注2) 被害の拡大を抑える対策は緊急時対策に含める

(1) 予防対策

予防対策は、発災前と緊急時対策の終了後に活動をします。発災から緊急時対策が終了するまでの期間は次の災害・事故・事件(以下「災害など」)に備えた準備期間になります。また、復旧対策の活動期間中は、予防対策を復旧対策に組み込む活動を行います。

(2) 緊急時対策

緊急時対策は、緊急事態対策とも呼ばれます。活動期間は、発災直後から災害などの被害の詳細な調査が終了するまでです。なお、台風や噴火などある程度事前に予兆があるものは、予兆の時点で緊急時対策を始めることもあります。更に、テロや窃盗などの事件は予兆時点で、犯人逮捕などの事件解決を見るものもあります。

(3) 継続対策

継続対策の活動期間は、緊急時対策の発令後に被害の状況を見て経営者が発令し復旧対策が終了するまでの期間です。継続対策とは、通常と異なる装置・部品・材料やサービスを活用し、

事業・業務を継続することです。この中には、次が含まれます。

- 備蓄材料・商品の活用
- 代替部品・材料・サービスの活用
- 代替駐車場、代替会議室、代替倉庫の活用
- セカンドサプライヤーの活用
- 代替サーバー、バックアップサイトの活用
- 代替物流ルート、代替通勤経路・手段の活用
- 非常用発電機、非常用井戸の活用
- 自社の他工場・他店舗・他事務所などでの事業再開
- 他社の工場・店舗・事務所などでの事業再開
- その他

(4) 復旧対策

復旧対策には、一時的な応急復旧対策と、恒久復旧対策があります。これはともに、被災した工場・研究所・事務所・店舗を復旧し、事業や業務を再開することです。復旧対策の活動期間は緊急時対策の終了後から事業・業務を本格的に再開するまでです。ただし、緊急時対策の活動中に復旧計画書の作成準備をします。

1.3 BCMS 担当者の役割

BCMS 担当者は次の業務を担うことになります。業務範囲が広いですので、担当者は複数名が望ましいと思います。

(1) 防災・防火・防犯対策

BCMS 担当者は、全社または担当する施設の防災・防火・防犯対策などの現状と改善を担当することになります。この中には、リスク排除対策およびリスク低減対策(減災対策)も含まれます。これは今までの企業防災と同じです。

(2) 継続対策を考える

BCMS 担当者は、全社または担当する施設の継続対策を担当します。このためには、全社または担当施設の事業・業務で使用している経営資源の日常的な使用状況と在庫、その代替部品・材料・サービスについて理解し、代替部品などの認定に責任を持ちます。

また、全社または担当施設の事業・業務を自社の他施設または他社の施設に低コストで委託する方法について理解し、実証する責任があります。この中には、代替サーバーやバックアップサイトの活用など、IT システムの事業継続対策も含まれます。

(3) インフラ経由、サプライチェーン経由の被害を考える

電力や通信などのインフラが停止すると自社の事業は停止します。サプライヤーからの部品や材料の供給が停止しても、自社の事業が停止します。BCMS 担当者は、インフラ経由、サプライチェーン経由の被害についても理解し、対策を講ずる責任があります。

(4) マネジメントシステムを推進する

BCMSは2011年秋または2012年春にISOの新しいマネジメントシステム規格になりますので、BCMS 担当者はマネジメントシステムについても、内部監査が出来る知識と力量が必要になります。

1.4 災害別 BCP と汎用 BCP

BCMSは成果物としてBCP(事業継続計画書)を策定しますが、このBCPには地震用や新型インフルエンザ用など災害別BCPと、災害などを特定しない汎用BCPがあります。英国や米国は汎用BCPが一般的ですが、我が国の場合は2005年頃から地震用BCPの普及が始まり、次いで2009年に新型インフルエンザ用BCPが普及しましたので、災害別BCPが広く存在しています。

災害別BCPと汎用BCPのどちらを選ぶかは、各企業が決めることになります。災害別BCPは、想定する災害などが増えるに従い数が増えることになります。また、震度7の場合、震度6強の場合、震度6弱の場合など、被災のレベルでもBCPの数が増えます。

汎用BCPは、災害などを想定するのではなく、ある施設が使用不可能になり復旧に1ヶ月かかるケース、通常の物流ルートが使えないケース、ITシステムが1週間止まるケースなどを想定してBCPを構築します。

首都圏の場合は地震用(震度7、6強、6弱、5強)、水害用(最大規模、大規模、中規模)、火災(最大規模、大規模、中規模)、労災事故、感染症(欠勤率が40%または20%を超える場合)の災害別BCPを作成し、それに社長が誘拐された場合、電力が24時間停止した場合やサプライチェーンが途絶して部品または材料の供給が1週間停止した場合などを含めると良いと思います。

1.5 災害などで企業が困ること

災害などで企業が困るのは、その経営資源であるヒト・モノ・カネ・情報が途絶したり、中断したり、傷ついたり、混乱するからです。この経営資源の途絶・中断・損傷・混乱をディスラプションといいます。災害などが発生しても、ディスラプションにならなければ、企業は困りません。

しかし、自社が被災しなくとも、顧客・協力会社・物流会社が被災するとディスラプションは発生します。また、電力・水道・道路・通信などのインフラ系の中断もディスラプションを発生させます。

近年は材料や部品を中国・ベトナムなど海外から輸入することが著しく増加していますし、製品の輸出も増加しています。従って、海外の顧客・協力会社・物流会社の被災に起因するディスラプションの発生が増加しています。

- ディスラプション = 経営資源の途絶・中断・損傷・混乱

BCMS は、ディスラプションに備えるものといえます。予防対策は、ディスラプションの発生を防ぐまたはディスラプションの規模を最少化し、緊急時対策はディスラプションの拡大を抑止し、継続対策はディスラプションの代替を容易にし、復旧対策はディスラプションを通常に戻す作業です。

更に、地震や台風など多くの災害などは緊急事態が発生したことを多くの関係者がほぼ同時に認識することが出来ますが、インフラ経由やサプライチェーン経由のディスラプションは多くの関係者が同時に被災を認識することが困難になります。このため、緊急時対策本部の設置が遅れ、かつ緊急時対策や継続対策の始動が遅れますので、ご注意ください。

1.6 BCP の数

災害別、汎用に関わらず施設毎に必要な BCP の数は 10 を超えます。これを効率的に少なくすることが必要です。

(1) 予防対策書

予防対策書は施設毎に一つ以上必要になります。これを、地震用、水害用、火災用、感染症用などに分ける場合もあります。また、連絡網および IT 関係を別の BCP として整備することもあります。

(2) 緊急時対策書

緊急時対策書は施設毎に、また災害など毎に作成する必要があります。従って、対象とする災害などが異なると装備する BCP も異なります。以下は首都圏の一般的な災害別 BCP の場合です。

- 地震では「震度 7+ 震度 6 強」、震度 6 弱、震度 5 強の 3 種類
- 水害では最大規模、大規模、中規模の 3 種類
- 火災では最大規模、大規模、中規模、小火の 4 種類
- 感染症では欠勤率 20%程度、40%以上の 2 種類
- 労災事故
- IT 関係のディスラプション
- サプライチェーンの途絶
- インフラ(電力)の途絶
- それぞれの教育・訓練

なお、汎用 BCP の場合は次のようになります。

- 被災拠点に現地対策本部が設置可能な場合
- 被災拠点に現地対策本部の設置が困難な場合
- 代替施設での継続対策が必要な場合
- 代替施設での継続対策が不要な場合
- IT 関係のディスラプション
- ヒト関係のディスラプション
- サプライチェーンの途絶
- インフラ(電力)の途絶
- それぞれの教育・訓練

(3) 継続対策書

継続対策書は施設毎に次の 4 種類が必要になります。

- 自施設内で継続対策を行う場合
- 自施設の事業・業務を他施設で行う場合
- 他施設の事業・業務を自施設で行う場合
- それぞれの教育・訓練

(4) 復旧対策書

復旧対策書は施設毎に次の 4 種類から一つまたは二つ選ぶことになります。

- 自施設を整理する場合
- 自施設を原状に復旧する場合
- 自施設を縮小復旧する場合
- 自施設を拡充復旧する場合

第 2 章 BCMS 導入の前にすること

この章では、BCMS の導入前に自社の防災力、防火力、防犯力、セキュリティ力を把握する方法を解説しています。なお、防災力や防火力などに大きな欠陥が見つかった場合は、BCMS を導入する前にその部分を改善する必要があります。

また、BCMS の導入前に自社のマネジメントシステムの現状についても把握する必要がありますが、こちらは第 3 章で解説致します。

2.1 準備作業

BCMS を策定する場合は、導入作業対象となる全社または施設の現状調査が必要です。この調査には海外にある施設も含めます。

- 施設がある地域の災害などの発生状況
- 施設の周辺環境の現状
- 施設の建物の現状
- 施設の防災力・防火力・防犯力・セキュリティ力の現状
- 施設のマネジメントシステムの現状

ここで、～ は企業の外部要因の調査です。 と は、企業の内部要因の調査になります。この調査を元に、BCMS 導入の目標を設定します。

2.2 施設がある地域の災害などの発生頻度

BCMS 担当者は、施設毎に外部要因による災害などの発生頻度をチェックします。同じ市区町村の場合は、まとめて一つにすることも可能です。ただし、地域の特性が異なる場合は分けて発生頻度を洗い出します。

災害などの発生頻度は都道府県または市区町村の危機管理担当部門に聞くとある程度の情報を得ることができます。行政から得られない情報については自社で収集することになりますが、始めは精度が低くとも毎年少しずつ高くすることになります。

図表 2 は、A 県 A 市、B 県 B 市、C 県 C 市に施設がある場合です。施設の数が増えるに従いこの表は横に伸びていきます。海外に拠点がある場合も、この表に含めます。

また、図表 1-2 の災害などの項目は必要に応じ、項目を増加させて下さい。ちなみに、海外を含めると、誘拐、放火、強盗など事件の項目が増加します。なお、インフラ関係については第 2 部で

解説しますので、この図表の項目には含めないで下さい。

この図表では5段階評価ですが、3段階評価や9段階評価もあります。評価段数は標準化がされていませんので、自社で決めることになります。

図表 2 災害などの発生頻度評価表

災害など	説明	A市	B市	C市
地震	首都直下など地震毎に分ける	5		
津波	原因となる地震毎に分ける	2		
河川の氾濫	河川毎に分ける	3		
内水氾濫	下水道の逆流など	3		
風害	道路・鉄道線路はインフラで取り扱う	2		
土砂災害	道路・鉄道線路はインフラで取り扱う	1		
干魃	上水道不足	2		
雪害	道路・鉄道線路はインフラで取り扱う	1		
落雷	物損事故、人身事故	2		
噴火・火山灰	火山毎に分ける	2		
感染症	新型インフルエンザ等	5		
火災・爆発		4		
窃盗	部内者の犯罪は除く	4		
テロ	部内者の犯罪は除く	2		
サイバーテロ	部内者の犯罪は除く	2		
その他	具体的に()			
災害などポイントの合計		39		

【災害などの評価ポイント (Disaster Point)】

- Dポイント 5: 繰り返し発生している
- Dポイント 4: 過去に発生したが、被害は大規模であった
- Dポイント 3: 過去に発生したが、被害は中程度であった
- Dポイント 2: 過去に発生したが、被害は軽微であった
- Dポイント 1: 過去に発生したことがない

図表 2 で、施設がある地域毎に発生頻度の高い災害などを把握します。九州地方は、地震より河川氾濫と噴火のポイントが高くなります。東海地方は地震と河川氾濫のポイントが高くなります。窃盗は日本では低いポイントになると思いますが、東南アジアや南米では高くなります。感染症はアフリカで高くなります。

2.3 施設の周辺環境

これも施設毎にチェックします。災害などの発生頻度と同様に、同じ市区町村の場合はまとめて一つにすることも可能です。また、周辺環境の項目は必要に応じて追加をお願いします。

「評価の説明」は、あくまでも参考例です。これは自社で検討し、決めることとなります。なお、脆弱度の評価の際には行政やインフラ系企業の対策は含めますが、自社の対策は含めません。評価は過去のデータを収集・整理・分析して書き込むものですが、まず分かる範囲で記入し、後日、過去のデータなどを調べ、精度を上げる作業をすることをお勧めします。この評価結果は新しく施設を設置する場合の参考資料としても活用が可能です。

なお、幼稚園・保育所、病院や介護施設が近くにあると脆弱度が上がるのは、自社の火災や事故にそれら施設を巻き込むと企業のブランドイメージを大きく損なうからです。更に、地震や水害などの広域災害の場合も自社への対応よりもこれら施設への対応を優先すべきケースがあります。

図表 3 周辺環境の脆弱度評価

項目		評価の説明 【周辺環境の脆弱度評価の参考例】	A市	B市	C市
A 群	河川	10m 以内:5、 10-100m:4、	2		
	海岸	100-1,000m:3、 1,000-10,000m:2、	1		
	山・崖	10,000m 以上離れている:1	1		
	その他	具体的に()			
B 群	幼稚園・保育所		2		
	病院・介護施設	10m 以内: 5、 10-100m: 4	3		
	商業施設	100-250m: 3、 250-1,000m: 2	5		
	娯楽施設	1,000m 以上離れている: 1	4		
	危険物工場		2		
	住宅密集地		2		
	その他	具体的に()			
周辺環境の脆弱度ポイント (V)の合計			22		

この脆弱度ポイントと先の災害などの評価ポイント(Dポイント)と組合せ、図表 4 を作成します。図表 4 では、地震と感染症、次いで火災・爆発と窃盗の脆弱度が高く、土砂災害と雪害の脆弱度が低いこととなります。

図表 4 周辺環境を含めた施設の脆弱度評価表【A市にある施設の例】

災害など	発生頻度 [Dポイント]	周辺環境の脆弱度 [Vポイント]	積算ポイント [D・Vポイント]
地震	5	22	110
津波	2	22	44
河川の氾濫	3	22	66
内水氾濫	3	22	66
風害	2	22	44
土砂災害	1	22	22
干魃	2	22	44
雪害	1	22	22
落雷	2	22	44
噴火・火山灰	2	22	44
感染症	5	22	110
火災・爆発	4	22	88
窃盗	4	22	88
テロ	2	22	44
サイバーテロ	2	22	44

2.4 施設の建物外部

自社の各建物を診断します。まずは分かる範囲で記入し、後日データを見て精度を上げる作業をします。また、必要に応じて項目を追加して下さい。

図表 5 建物外部の脆弱度評価表

項目	説明 [脆弱度ポイントの参考例、これは日本の場合]	A工場 第1号棟	A工場 管理棟	A工場 第1倉庫
築年数	1972年以前：5、1981年以前：4 1998年以前：3、築10年以内：2 築5年以内：1 (注意) 法令の変更に注意が必要です。	2	2	3
階数	30階以上：5、20階以上：4 10階以上：3、5階以上：2 4階以下：1	1	2	1

	(注意) 低層階は防犯には弱くなります。			
用途	大幅な変更がある: 5 変更がある: 3 変更がない: 1 (注意) 住居を事務所へ転用、事務棟を工場へ転用することです。	3	1	3
その他	具体的に()			
建物の脆弱度ポイントの合計		6	5	7

図表 6 は部屋の種類と積載荷重です。荷重が増える方向への用途変更が建物の耐震性を弱くします。

図表 6 地震力算出用の積載荷重

部屋の種類		地震力算出用の積載荷重
(1)	住宅の居室、住宅以外の建築物の寝室または病室	600N/m ²
(2)	事務室	800N/m ²
(3)	教室	1100N/m ²
(4)	百貨店または店舗の売場	1300N/m ²
(5)	劇場、映画館などの客席または集会室	1600N/m ²
	固定席 その他	2100N/m ²
(6)	自動車車庫および自動車通路	2000N/m ²
(7)	屋上広場又はバルコニー	(1)の数値による。ただし、学校又は百貨店の用途に供する建物にあっては、(4)の数値による。

2.5 施設の建物内部

この現状調査は、地震の際に落下や転倒が生じる可能性があるもの、火災の際に避難路を妨げる可能性があるもの、水害の際に水に浸かる可能性があるもの、外部から侵入しやすい窓や扉などのチェックです。チェックは、建築士、消防官、警察官などの専門家の支援を受けて行います。

図表 7 建物内部の脆弱度評価表

災害など	A 工場 第 1 号棟	A 工場 管理棟	A 工場 第 1 倉庫
地震	3	3	4
津波	2	1	3
河川の氾濫	2	1	2
内水氾濫	2	2	3
風害	3	2	3
土砂災害	2	1	2
干魃	建物と無関係	建物と無関係	建物と無関係
雪害	1	1	2
落雷	2	2	3
噴火・火山灰	1	1	1
感染症	建物と無関係	建物と無関係	建物と無関係
火災・爆発	3	2	3
窃盗	2	2	3
テロ	2	3	3
サイバーテロ	建物と無関係	建物と無関係	建物と無関係

【建物内部 の脆弱度ポイント (Vulnerability point of Facilities)】

F ポイント 5: 脆弱度が高い (地震や火災などの際に、危険度が高い)

F ポイント 4: 5 と 3 の間

F ポイント 3: 脆弱度が中程度

F ポイント 2: 3 と 1 の間

F ポイント 1: 脆弱度が低い (地震や火災などの際に、危険度が低い)

図表 5 と図表 7 を組合せると、災害など別に建物内部と外部を掛けあわせた脆弱度の評価表 (図表 8) になります。BCMS 導入の対象になる全ての工場・研究所・事務所・店舗・倉庫毎に図表 8 を作成します。

図表 8 建物内部と外部の脆弱度評価表

災害など	A 工場第 1 号棟 【建物: 6 ポイント】	A 工場管理棟 【建物: 5 ポイント】	A 工場第 1 倉庫 【建物: 7 ポイント】
地震	18	15	28
津波	12	5	21

河川の氾濫	12	5	14
内水氾濫	12	10	21
風害	18	10	21
土砂災害	12	5	14
干魃	0 (建物と無関係)	0 (建物と無関係)	0 (建物と無関係)
雪害	6	5	14
落雷	12	10	21
噴火・火山灰	6	5	7
感染症	0 (建物と無関係)	0 (建物と無関係)	0 (建物と無関係)
火災・爆発	18	10	21
窃盗	12	10	21
テロ	12	15	21
サイバーテロ	0 (建物と無関係)	0 (建物と無関係)	0 (建物と無関係)
合計	156	105	224

2.6 施設の防災力・防火力・防犯力・セキュリティ力の現状

事故・事件について、過去の発生頻度を施設毎に図表 9 を作成します。ただしこの図表には、次の事故・事件は含みません。

- 停電や断水などインフラ経由のもの
- 部品納入遅れやサービス中断などサプライチェーン経由のもの
- 株式・商品・金融市場の変化に起因するもの
- 会計・税務・会計監査関係のもの
- 法律や条例などの変更にとまなうもの

上記のと は本資料の第 2 部で概説します。 ~ は BCMS での対処が困難または他のマネジメントで対処した方が効率的なものです。(本章末を参照下さい。)

図表 9 事故・事件の発生頻度評価表

事故・事件	A 工場第 1 号棟	A 工場管理棟	A 工場第 1 倉庫
労働災害	3	1	2
安全衛生管理不良	2	1	3
操作ミス・事務ミス	4	3	3
設備故障	4	2	5
輸送中の事故	2	1	4

交通事故	2	1	3
小火	1	1	2
職場内暴力	1	2	1
セクハラ	2	2	1
パワハラ	2	3	2
労使問題	2	2	1
地域住民とのトラブル	1	1	2
各種感染症	2	2	2
情報漏洩	2	2	1
情報システム誤作動	4	3	3
ネットワーク中断	4	3	3
コンピュータウイルス	5	5	5
土壌汚染	2	1	1
水質汚染	2	1	1
廃棄物処理	2	1	1
盗難	2	1	3
放火	2	1	2
異物混入	2	1	1
合計	55	41	52

【インシデント評価ポイント (Incident Point)】

- Iポイント 5: 繰り返し発生している
- Iポイント 4: 過去に発生したが、被害は大規模であった
- Iポイント 3: 過去に発生したが、被害は中程度であった
- Iポイント 2: 過去に発生したが、被害は軽微であった
- Iポイント 1: 過去に発生したことがない

【BCMS の効率性】

BCMS は、予想被害表を作成し、次にリスク低減対策表、更にリスク低減実施表を作成します。先に記述した、「株式・商品・金融市場の変化に起因するもの」に対しても BCMS は有効ですが、BCMS よりも金融マネジメントの方が作業効率が高いと思います。

「会計・税務・会計監査関係のもの」は、事務的ミスと意図時ミス(粉飾決済)があります。事務的ミスは予想被害表並びにリスク低減対策表の作成が可能ですが、会計監査や税務監査を厳格化の方が効率的と思います。意図的ミスは予想被害表とリスク低減対策表の作成が困難です。

「法律や条例などの変更にとまなうもの」は、予想被害表が作成できないため、BCMS では対処が出来ません。

第 3 章 目標の設定

ここでは、BCMS の導入作業を始める前に行う自社のマネジメントシステムの把握と、BCMS 導入の目標設定を解説します。

3.1 施設の防災・防火・防犯・セキュリティ力の評価

図表 3(周辺環境の脆弱度評価)、図表 8(建物内部と外部の脆弱度評価表)と図表 9(事故・事件の発生頻度評価表)をまとめ施設毎に図表 10を作成します。図表 10は施設の防災力などの現状を表します。防災力などの改善はこの数字を低くすることになります。

図表 10 施設の防災・防火・防犯・セキュリティ力評価表

項目	A 工場 第 1 号棟	A 工場 管理棟	A 工場 第 1 倉庫
周辺環境の脆弱度評価	22	22	22
建物内部と外部の脆弱度評価	156	105	224
事故・事件の発生頻度評価	55	41	52
合計	233	168	298

(注意) 単純に点数だけで評価すると、項目数の増減により見かけの防災力などが変化します。これに対処するためには、点数/満点の割合などを活用します。

3.2 施設のマネジメントシステムの現状

次に、マネジメントシステムの現状を確認します。品質 ISO (ISO9001) や環境 ISO (ISO14001) の認証を取得している企業は高い成熟度にあると言えます。しかし、未取得の企業はこの成熟度が不明ですので専門家に診断をお願いすることになります。

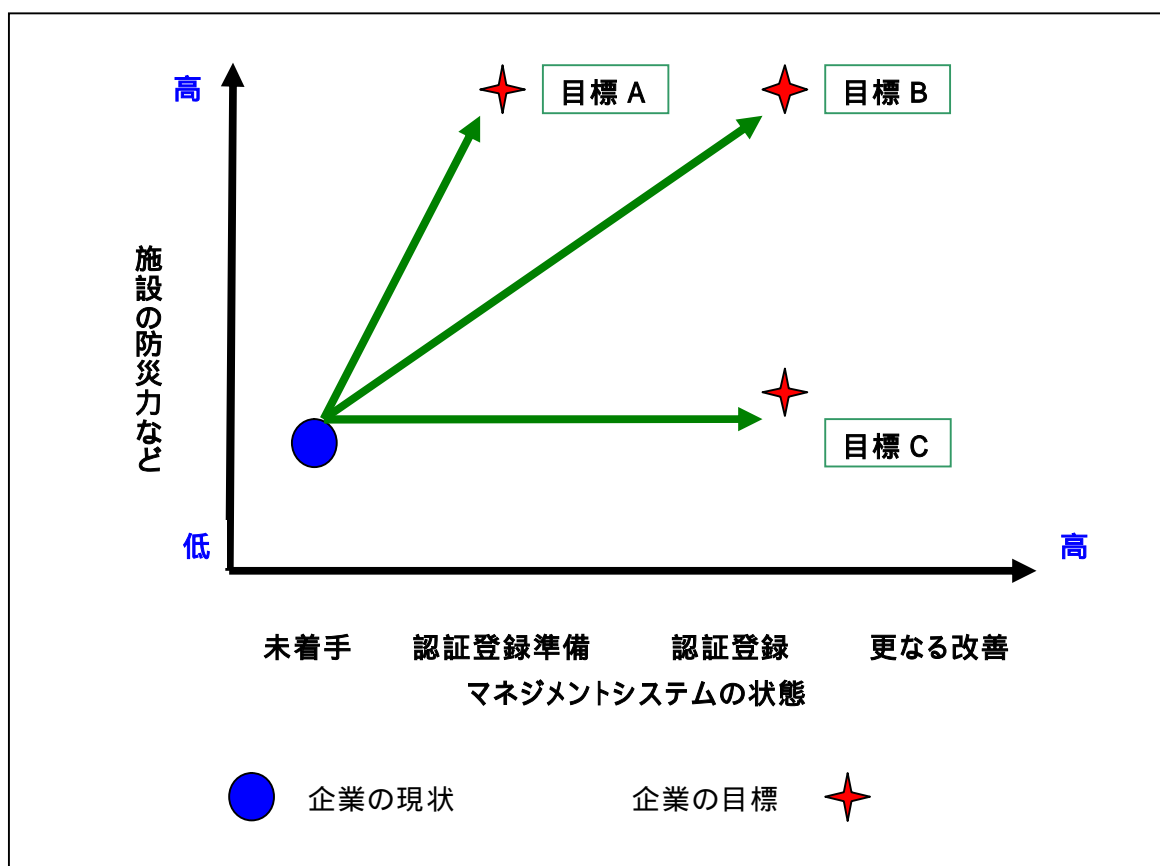
マネジメントシステムの現状評価は、未着手、認証登録の準備、認証登録、更なる改善の 4 段階とします。

3.3 目標の設定

施設毎のマネジメントシステムの現状評価と防災力などの評価表(図表 10)から図表 11 に現状

をプロットします。プロット後に、施設の BCMS 導入目標をプロットします。

図表 11 施設の防災力などとマネジメントシステムの状態



図中、「目標 A」は施設の防災力などの改善に力点があり、「目標 C」は BCMS の認証登録に力点があるケースです。「目標 B」は防災力の改善とマネジメントシステムのレベルアップの両方を目標とするケースです。

BCMS の全社または事業部の目標設定は次の手順が良いと感じています。

- 各施設の現状調査
- 全社または事業部の目標設定
- 各施設の目標設定

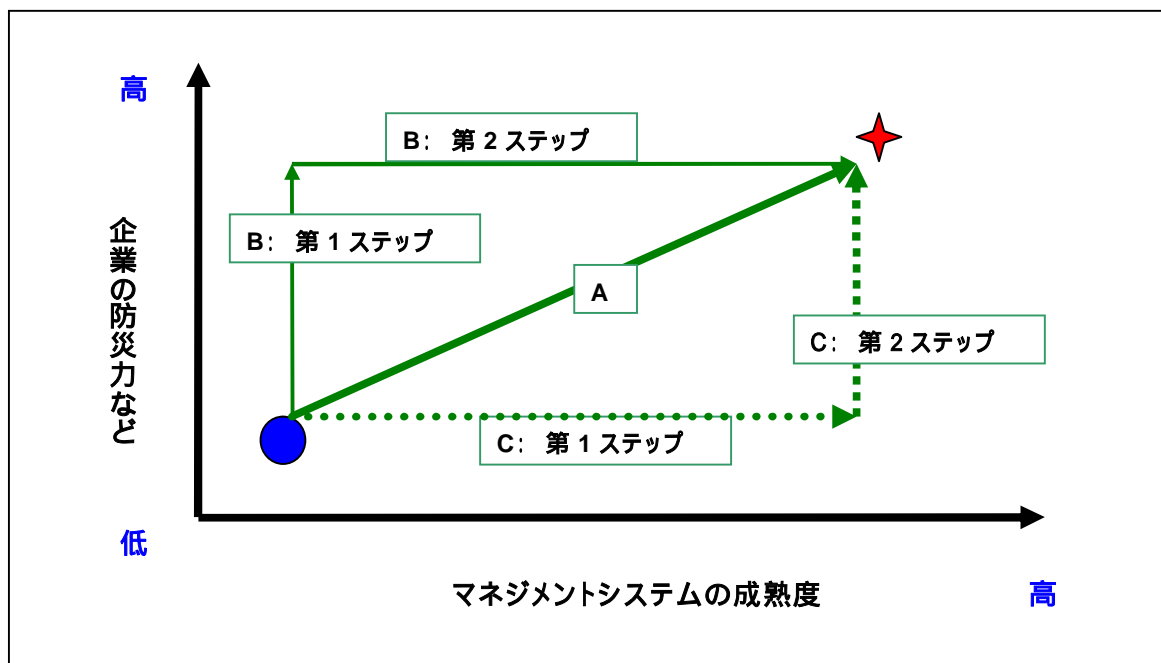
3.4 目標までの手順

図表 12 は、目標に到達する手順を表しています。防災力などの改善を優先して作業する方法と、

マネジメントシステムの改善を優先して作業をする方法、両方を並行して進める方法があります。

方法を選択するのは経営者になりますが、顧客から認証登録を求められている場合はマネジメントシステムの改善を優先し、東海地震や首都直下地震への対処を優先する場合は防災力などの改善を先に行うことになります。

図表 12 目標までの手順



第 4 章 リスクアセスメントとビジネス影響度分析 (BIA)

BCMS はリスクアセスメントとビジネス影響度分析 (BIA) を必要とします。この第 4 章では、両者の目的の違いとそれぞれの手法を概説します。

4.1 リスクアセスメントの目的と BIA の目的

リスクアセスメントと BIA の目的は、次のとおりです。違いは、「災害など」と「ディスラプション = 経営資源の途絶・中断・損傷・混乱」のみです。

リスクアセスメントの目的は、自社の経営に影響を与える災害・事故・事件 (以下「災害など」) の発生頻度を把握し、その被害額を予測することです。

BIA の目的は、自社の経営に影響を与えるディスラプションの発生頻度を把握し、その被害額を予測することです。

(1) 自社の場合

リスクは顕在化すると災害などになります。災害などは経営資源であるヒト・モノ・カネ・情報を途絶・中断・損傷・混乱させ、企業の経営に影響を与えます。従って、企業経営のためには、経営資源の途絶などが生じないように災害などの原因となるリスクを排除し、排除出来ない場合は減災対策を講ずることになります。また、発生頻度や影響度からリスクを受容する選択もありますが、今回は、除きます。

(2) インフラ経由、サプライチェーン経由のディスラプション

電力や通信などのインフラ経由および他社から購入する部品・材料・サービス経由の被害の場合は、リスクアセスメントからのアプローチは困難になります。無論、インフラ系企業や協力会社に対して災害などの原因となるリスクの排除対策および減災対策の実施をお願いすることは出来ますが、実施とそのレベルについて自社が責任を持つことは出来ません。

そこに登場するのが BIA です。インフラ系企業や協力会社に対して自社が必要とするのは、「決められたものを、決められた品質で、決められた数量、決められた時間」に納品されることです。BIA は、この「決められたものを、決められた品質で、決められた数量、決められた時間」を評価することを目的にしています。BIA の利点は、国内のみならず海外の協力会社、物流会社などに対しても部品・材料・サービスの安定供給について評価ができることです。

また、BIA は自社内における事業で活用する経営資源の途絶・中断・損傷・混乱が全社の経営に与える影響度も評価できるという利点があります。

4.2 リスクアセスメントから導かれる対策と BIA から導かれる対策

リスクアセスメントは災害などの発生頻度を下げするために、リスクの洗い出しを行い、リスクを排除する対策を導きます。例えば、河川の氾濫に備え堤防を高くする。活断層を見つけ、その直上には建物を設置しない、などです。企業でいえば、氾濫しそうな河川や活断層の近くには施設を設置しない、などです。次に、排除出来ないリスクには減災対策を施します。地震では免震・制震システムなどであり、河川氾濫においては重要機材を 2 階、3 階に上げることです。

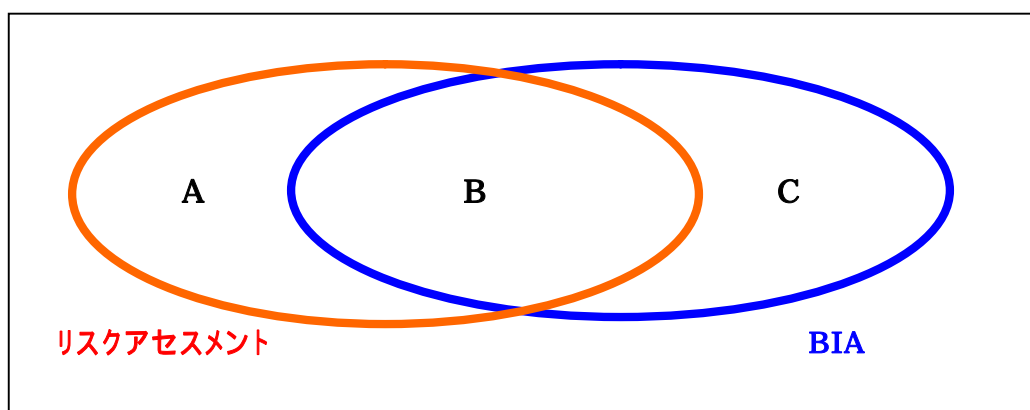
これに対し BIA は「決められたものを、決められた品質で、決められた数量、決められた時間」を守ることで、自社内では部品や材料の在庫量積み増し、代替部品・代替材料・代替サービス・代替オフィス・代替生産ライン・代替要員の確保、物流ルートの二重化、代替サーバーの設置など二重化を中心とした対策を導きます。協力会社に対しては、災害などで被災しても安定して部品・材料・サービスを提供することを求めるとともに、自社では代替サプライヤーの活用も検討します。

図表 13 は、両者から導かれる対策を図示したものです。「A」の部分は、自社の人命や重要な経営資源に対して行うリスク排除対策およびリスク低減対策です。

「B」の部分は、自社ですが「A」に含まれない経営資源に対するものでリスク排除・リスク低減対策と、二重化対策から選ぶことができます。

「C」の部分は、同一のサプライチェーン上にある協力会社・物流会社・インフラ会社など経由でのディスラプション対策で、二重化対策です。

図表 13 リスクアセスメントと BIA から導かれる対策



4.3 被害予想とリスクアセスメントの実務

ここではリスクアセスメントの実務を少し説明いたします。第 2 章で、脆弱度の評価を行いました。BCMS 担当者が次に行う作業は災害など毎の被害の予想です。図表 14 は、「台風」を想定しています。被害は、「最大規模」、「中程度」の二つですが、必要に応じ「大規模」や「小規模」を追

加して下さい。この図表は、施設毎・災害毎に必要なになります。

この作業の次に BCMS 担当者が行う作業は減災対策(リスク低減対策)ですが、これは第 10 章の予防対策で解説致します。

図表 14 想定被害表

対象施設	A 市地区	
対象リスク	台風 (平成16年台風18号規模)	
被害が最大規模の場合		
予想される 直接被害	建物外部	
	建物内部	要員
		IT機器
		業務機器
	インフラ	
予想される 業務中断	IT関係の中断時間	
	その他業務の中断時間	
	協力会社の中断時間	
	全体の業務中断時間	
予想される 直接被害額	建物外部の復旧費用	
	建物内部の 復旧費用	要員
		IT機器
		業務機器
	その他	
予想される 間接被害額	業務中断による A 市地区の被害額	
	業務中断による 全社の被害額	
	その他	
保険関係	関係支払保険額	
	関係受取保険額	
被害が中規模の場合		
予想される 直接被害	建物外部	
	建物内部	要員
		IT機器

		業務機器	
		材料・部品	
	インフラ		
予想される 業務中断	IT関係の中断時間		
	その他業務の中断時間		
	協力会社の中断時間		
	全体の業務中断時間		
予想される 直接被害額	建物外部の復旧費用		
	建物内部の 復旧費用	要員	
		IT機器	
		業務機器	
		材料・部品	
その他			
予想される 間接被害額	業務中断による A市地区の被害額		
	業務中断による 全社の被害額		
	その他		
保険関係	関係支払保険額		
	関係受取保険額		

4.4 予想被害額の算出

ここではリスクアセスメントの後半である予想被害額の算出を行います。第1部で参考例としたA市にあるA工場第1号棟、管理棟、第1倉庫について、予想被害額を算出します。まず、施設の建物、生産設備、IT設備などが被災した場合にその部分を原状に復旧するための額を調査し、算出します。これを予想直接被害額といいます。

次に、生産設備などが止まることにより本来生産または販売できた逸失額を調査・算出します。これを予想間接被害額額(施設)といいます。予想直接被害額と予想間接影響額(施設)は災害毎、施設毎に異なりますので、それらを算出し、図表15A・Bを作成します。

この図表では、事業再開までの期間が、地震では3ヶ月と1ヶ月、新型インフルエンザでは2ヶ月と1ヶ月ですが、必要に応じて2週間、1週間などを追加して下さい。

図表 15A 各施設の予想被害額【地震の場合】 単位:100万円

項目	A工場	A工場	A工場
----	-----	-----	-----

		第1号棟	管理棟	第1倉庫
事業再開まで 3ヶ月	予想直接被害額	150	40	15
	予想間接被害響額(施設)	510	100	150
	合計額	660	140	165
事業再開まで 1ヶ月	予想直接被害額	160	50	15
	予想間接被害響額(施設)	170	33	50
	合計額	330	83	65

図表 15B 各施設の予想被害額【新型インフルエンザの場合】 単位:100万円

項目		A工場 第1号棟	A工場 管理棟	A工場 第1倉庫
事業再開まで 2ヶ月	予想直接被害額	0	0	0
	予想間接被害響額(施設)	340	66	100
	合計額	340	66	100
事業再開まで 1ヶ月	予想直接被害額	0	0	0
	予想間接被害響額(施設)	170	33	50
	合計額	170	33	50

図表 16A は、一般的な予想直接影響額を算出する考え方です。図表 16B は、食品会社における産地や食材偽装、老舗や高級店における品質偽装など企業イメージ、ブランドイメージを著しく傷つける場合です。

図表 16A 予想直接影響額の算出(一般的)

項目	
失われる予想生産額・販売額	A
不要となる予想経費額	C
予想直接影響額	A-C

図表 16B 予想直接影響額の算出(無形財の影響が強い場合)

項目	
失われる予想生産額・販売額	A
失われる無形財の予想額	B
不要となる予想経費額	C
予想直接影響額	A+B-C

次に、中断期間毎に各施設の予想直接被害額と予想直接影響額を全社の年間販売額で除すと、図表 17 のとおりそれぞれの影響度が算出できます。これを簡単な BIA 評価といいます。

図表 17 簡単な BIA 評価【地震の場合】 単位:100 万円

項目		A 工場 第 1 号棟	A 工場 管理棟	A 工場 第 1 倉庫
事業再開まで 3 ヶ月	予想直接被害額	150	40	15
	予想間接被害額(施設)	510	100	150
	合計額	660	140	165
	全社の年間販売額	18,000		
	影響度(簡易)	3.7%	0.8%	0.9%
事業再開まで 1 ヶ月	予想直接被害額	160	50	15
	予想間接被害額(施設)	170	33	50
	合計額	330	83	65
	全社の年間販売額	18,000		
	影響度(簡易)	1.8%	0.5%	0.4%

4.5 一般的な BIA

図表 17 に、施設が中断することによる全社の予想間接被害額(全社)を加えます。例えば、本社にある各種データが紛失したために生産部門や販売部門の活動停止による被害額や、倉庫にある原材料の紛失による工場の生産中止による逸失生産額などです。これを含め図表 18 を作成します。

この予想間接被害額の算出は、多くの場合大変込み入っています。また、BIA の作業は難しいといわれる原因でもあります。しかし、工程フロー図、IT フロー図、資金フロー図などのチェックを行い、可能な限り正確に予想間接被害額を算出して下さい。

図表 18 間接被害額(全社)を含めた BIA 評価【地震の場合】 単位:100 万円

項目		A 工場 第 1 号棟	A 工場 管理棟	A 工場 第 1 倉庫
事業再開まで 3 ヶ月	予想直接被害額	150	40	15
	予想間接被害額(施設)	510	100	150
	予想間接被害額(全社)	750	1,000	500

	合計額	1,410	1,140	665
	全社の年間販売額	18,000		
	影響度	7.8%	6.3%	3.7%
事業再開まで 1ヶ月	予想直接被害額	160	50	15
	予想間接被害額(施設)	170	33	50
	予想間接被害額(全社)	250	333	167
	合計額	580	416	232
	全社の年間販売額	18,000		
	影響度	3.2%	2.3%	1.3%

この作業を自社の全施設に対して行くと、災害などによる各施設の中断が経営にあたる影響度の順位が出てきます。この順位は、予防対策など各種対策を講ずる際に重要な指標となり参考になります。

なお、全ての災害に対して施設毎に図表 18 を作成することが必要ですが、災害などが経営資源にあたる影響を図表 19 のようにタイプ別に整理し、各タイプに対応する方法もあります。

図表 19 大規模な災害などと経営資源の関係

影響を受ける経営資源		大地震 大火災 大事故	重度の感染症	顧客の倒産	重度の IT 障害
ヒト	経営者				
	管理者				
	作業員				
モノ	建物				
	生産設備				
	搬送設備				
カネ	人件費				
	部材費				
	研究費				
情報	生産データ				
	顧客データ				
	経理データ				

……直接被害

……間接被害

4.6 全施設を比較する

施設毎に 図表 18 を作成し、その後それを図表 20 のような一覧表にします。ここでは、各施設の全経営資源の被害により 1 ヶ月中断した場合の影響度を比較しています。

図表 20 各施設の影響度(業務中断:1 ヶ月、地震) 単位:100 万円

地区	施設名	直接 被害額	直接 影響額	間接 被害額	合計	影響度
A 市地区	工場第 1 号棟	20	170	250	440	2.4%
	工場第 2 号棟	15	60	90	165	0.9%
	管理棟	10	33	333	376	2.1%
	倉庫第 1 号棟	5	50	167	222	1.2%
	倉庫第 2 号棟	20	77	200	297	1.7%
B 市地区	工場	160	320	540	1,020	5.7%
	研究所	120	10	10	140	0.8%
	管理棟	80	220	410	710	3.9%
	倉庫	60	140	320	520	2.9%
C 市地区	工場	50	260	310	620	3.4%
	管理棟	50	80	225	355	2.0%
	倉庫	40	80	280	400	2.2%

図表 20 では、B 市地区工場の影響度が一番高いこととなります。予防対策と緊急時対策は一般的にこの影響度に関係なく高いレベルが求められますが、継続対策と復旧対策はこの影響度により対策レベルに違いが出てきます。

第 5 章 インフラの脆弱度と影響度評価

この章では、各施設のインフラの脆弱度と影響度を評価する方法を概説します。評価は施設毎ですが、同じ市区町村の場合はまとめて一つにすることも可能です。ただし、地域の特性が異なる場合は分けて評価します。

5.1 インフラの脆弱度

ここでは、インフラの脆弱度を 5 段階でチェックします。この脆弱度の評価の際には、行政とインフラ企業の対策は含めますが、自社の対策は含めません。なお、本来は、データを収集分析して記載するものですが、始めは「おおよその感覚」で記入し、後日精度を上げる作業をします。また、ここでも必要な項目を追加します。

図表 21 インフラの脆弱度評価

項目	名称	区間など	A 市地区	B 市地区	C 市地区
高速道路			3		
主要道路			3		
搬入出道路			3		
貨物用鉄道			1		
通勤用鉄道			3		
港湾			1		
電力			1		
上水道			3		
下水道			1		
ガス			2		
通信			2		
その他	具体的に()				
インフラの脆弱度ポイントの合計			24		

【インフラの脆弱度ポイント】

まず、原因を問わず途絶・中断・損傷・混乱を半日(12 時間):1 回とする。従って 14 時間の場合は 2 回になる。期間は過去 5 年間。

ポイント 5: 半日程度の中断などが 11 回以上発生 (災害に弱い)

ポイント 4: 半日程度の中断などが 5-10 回発生

ポイント 3: 半日程度の中断などが 2-4 回発生

ポイント 2: 半日程度の中断などが 1 回発生

ポイント 1: 全く中断等が発生していない (災害に強い)

5.2 インフラの影響度

ここでは、インフラの影響度を 5 段階でチェックします。なお、本来は、データを収集分析して記載するのですが、始めは「おおよその感覚」で記入して下さい。後日、データを見て、精度を上げる作業を行います。

図表 22 インフラの影響度評価

項目	名称	区間など	A 市地区	B 市地区	C 市地区
高速道路			3		
主要道路			4		
搬入出道路			5		
貨物用鉄道			2		
通勤用鉄道			4		
港湾			3		
空港			2		
電力			5		
上水道			5		
下水道			4		
ガス			2		
通信			5		
その他	具体的に()				
インフラの影響度ポイントの合計			44		

【インフラの影響度】

ポイント 5: 途絶・中断すると施設の事業への影響度が高い

ポイント 4: 5 と 3 の間

ポイント 3: 途絶・中断すると施設の事業への影響度が中程度

ポイント 2: 3 と 1 の間

ポイント 1: 途絶・中断すると事業への施設の影響度が低い

5.3 インフラの脆弱度と影響度

脆弱度と影響度からインフラの重要度を算出し、代替プランを書き込みます。

図表 23 の代替プランは参考例ですが、積算ポイントの大きい順に詳しく検討する必要があります。ことに、影響度が「5」で脆弱度が「1」または「2」のものは、過去の途絶・中断事例が少ないので、対策が疎かになっていることが予想されます。このインフラについては要注意です。

図表 23 インフラの脆弱度と影響度評価 (A 市地区)

項目	名称	区間など	脆弱度 V	影響度 I	V*I	継続対策 (代替プラン)
高速道路			3	3	9	迂回路あり 国道 N1 号線 実証試験済み
主要道路			3	4	12	迂回路あり 高速道路 + 県道 N2 号線 実証試験済み
搬入出道路			3	5	15	迂回路なし 要検討
貨物用鉄道			1	2	2	代替はトラック B11 会社と契約済み 要実証試験
通勤用鉄道			3	4	12	代替は徒歩など 徒歩 + 自家用車など 要駐車場 要実証試験
港湾			1	3	2	代替港湾 C12 物流会社と契約済み 要実証試験
電力			1	5	12	非常用電源 6 時間程度、要検討
上水道			3	5	4	代替プランなし 要検討
下水道			1	4	4	代替プランなし 要検討
ガス			2	2	10	代替プラン 要検討
通信			2	5	4	代替通信設備あり 要実証試験

第 6 章 関係要員の脆弱度と影響度評価

この章では、各施設に勤務する正規および非正規従業員が果たしている職務機能の脆弱度と影響度を評価する方法を概説します。

6.1 関係要員との連絡

(1) 安否確認

災害などが発生すると一番先に必要なのが、関係要員の安否確認です。安否確認システムは各種が市販されていますので、それらの活用を検討することになります。

広域地震や水害のように数時間から数日に多くの安否確認が必要となる場合と、感染症のように数週間から数ヶ月にわたり安否確認が必要となる場合があります。また、関係要員の家族を含める場合もありますし、通常は当該施設に勤務していない協力会社の担当者または役員を含めるケースもあります。

経験的ですが、平常時の勤務時間内に安否確認システムを使わずに訓練を実施すると出張中や休暇中の要員を除き 6 時間以内に確認が出来ます。出張中や休暇中の要員との連絡は連絡方法を取り決めて置くと確認が早くなります。

次に、同様に安否確認システムを使わずにこの訓練を休日に実施すると、90%以上の関係者と確認が取れるのに 12 時間から 24 時間かかり、100%に至には 48 時間程度かかります。また、平日の夜間は 6 時間から 12 時間かかります。これも、夜間や休日の連絡方法を取り決めて置く必要があります。

更に、災害時の電話連絡は一時に集中し、連絡が困難になり、対策本部の整理も難しくなります。これに対しては、対策本部へのメール送信が有効です。

(2) 現住所と通勤経路の確認

従業員などの現住所と通勤経路を把握することは、近くに住む人や同じ通勤経路の人でチームを組むことを可能にし、広域災害が発生した場合の連絡を容易にします。従業員などが全てこのチームに参加するとは思いませんが、80%位の参加率でも効果があります。

(3) 連絡が取れない時間と代行者への権限委譲

次に、連絡が取れない場合に代行者へ権限を委譲する時間を決める必要があります。図表 2-12 はその参考です。

図表 24 連絡途絶時間と代行者への権限委譲

役職名	第 1 代行者	第 2 代行者	連絡途絶時間	委譲する権限の概要
代表取締役	専務取締役	常務取締役	1 時間	全社の緊急時対策と 継続対策に関する業務
施設長	施設次長	総務部長	1 時間	施設の緊急時対策と 継続対策に関する業務
部門長	部門次長	○○課長	1 時間	部門の緊急時対策と 継続対策に関する業務

6.2 各業務が経営に与える総合的な影響度

各業務が経営に与える影響度をチェックします。影響度が高い業務は中断すると経営へ大きな影響を与えますので、災害などへの対策を厚くする必要があります。

(1) 代行要員の要件

災害などが発生した場合には、本来の担当者が自宅の被災や通勤経路の途絶で勤務できない場合があります。また感染症で 2～3 週間程度入院することも考えられます。このような場合には、代行要員が必要になります。ここでは代行要員の確保の困難度を評価します。代行要員の条件が高度なものは、代行要員の確保が難しくなり、結果として経営への影響度を高めます。

関係要員を内部の役職・職制、知識、経験、各種外部資格(医師、建築士、英検一級、一級販売士、その他)で区分します。この区分の目的は、代行要員の条件を明確にするためです。図表 2-13 は代行要員の条件例です。

図表 25 代行要員の条件例

担当業務	職制・役職	知識	経験	資格	研修期間	代行要員 確保の困難度
A 業務 (主任)	主任以上	TOEIC 500 点以上	業務経験 3 年以上	一級販売士	2 週間	2
B 業務	全社員	不問	社歴 1 年以上	不問	1 週間	1
C 業務(IT)	主任以上	C 言語	業務経験 1 年以上	応用情報 技術者	4 週間	3
D 業務 (課長)	主任以上	ロジスティック 要員管理	業務経験 5 年以上	ロジスティック 経営士	6 週間	3
E 業務	主任以上	冶金	業務経験	不問	24 週間	4

(専門職)			20年以上			
-------	--	--	-------	--	--	--

【代行要員確保の困難度】

- ポイント 4: 極めて困難
- ポイント 3: 困難
- ポイント 2: 普通
- ポイント 1: 容易

(2) 業務毎に代行要員確保の困難度を評価する

部または課内の個々の要員について、代行要員確保の困難度を調査し、それを平均化して部または課の代行要員確保の困難度とします。

(3) 業務の脆弱度

業務の脆弱度を評価します。図表 26 はそのサンプルで、各セルには過去 5 年間に発生した事故・事件の数を記入します。総合評価は、4 段階または 5 段階で行います。

図表 26 業務の脆弱度

	労働災害	作業ミス	情報漏洩	セクハラ	その他	合計	総合評価
総務課							
経理課							
IT 支援部							
契約管理課							
業務企画課							
契約推進課							

(4) 業務の影響度

業務の影響度は、図表 27 で評価します。この表は、5 段階評価(1:小さい、5:大きい)ですが、3 段階評価、4 段階評価などもあります。対顧客、対社内などのポイントに係数を掛けて、総合ポイントを算出します。ここでは、それぞれ 3、2、1、3 を係数としています。係数は経営者が決めます。

- 総合ポイント = 対顧客 x3 + 対社内 x2 + 対社会 x1 + 対収益 x3

図表 27 業務の影響度

部署名	経営への影響度					総合評価 ポイント
	対顧客 (3)	対社内 (2)	対社会 (1)	対収益 (3)	総合	

総務課	2	5	4	1	28	3
経理課	2	5	2	1	22	3
IT 支援部	5	5	1	3	34	4
契約管理課	5	1	2	5	47	5
業務企画課	4	1	2	5	44	5
契約推進課	4	1	2	5	44	5

(5) 各業務が経営に与える総合的な影響度評価

代行要員確保の困難度、業務の脆弱度と影響度から、各業務が経営に与える影響度を評価します。影響度が高い業務は、代行要員の確保を容易にする、脆弱度を低くする、影響度を低くするなどの対策が必要になります。

図表 28 業務の総合的危険度

	代行要員確保の 困難度 (D)	脆弱度 (V)	影響度 (I)	合計 (D*V*I)	経営に与える 影響度評価
総務課					
経理課					
IT 支援部					
契約管理課					
業務企画課					
契約推進課					

6.3 新型インフルエンザ流行時の問題

2009年4月27日にWHO(世界保健機構)が警戒態勢を「フェーズ4」と宣言し、2010年8月11日に同機構が「最盛期後」(ポスト・パンデミック)を宣言したメキシコ、米国での豚由来の新型インフルエンザでは、企業の従業員への対策について検討すべき課題が幾つか明らかにされました。

(1) 対策の三要素

新型インフルエンザ対策は、次の三要素から構成されています。

- 感染拡大防止対策
- 社内制度の整備
- 事業継続マネジメントシステム(BCMS)

この三要素の内容が始めは整理されず、対策部門に混乱が見られました。対策の内容と担当を整理すると図表 29 になります。

図表 29 新型インフルエンザ対策の内容と担当部門

部門名など	担当分野		
	感染拡大防止対策	社内制度の整備	BCMS
産業医			
弁護士			
BCMS エキスパート			
総務部長			
人事部長			
財務部長			
ICT 部長			
営業部長			
製造部長			
研究開発部長			
物流部長			

○ : 担当する △ : 助言を行う

(2) 感染拡大防止対策

感染の流行が始まった 2009 年 4 月末から 5 月にかけては、テレビ・新聞などで、マスク着用・手洗いとうがい励行が推奨されましたが、感染拡大防止対策の目的は次の二つです。

- 新型インフルエンザにかからないようにする
- 新型インフルエンザの感染拡大を防止する

(3) 社内制度の整備

こちらは、各社が新型インフルエンザ対策を構築する中で浮かび上がってきた疑問点で、就業規則の整備が中心です。以下は、代表的な疑問点と対処の考え方です。(監修者: 弁護士 北周士)

【疑問点】

- Q1. 感染を恐れて出社を拒否している従業員に対し、出社命令を出すことはできるか。
- Q2. パンデミック期において、従業員の多数が有給休暇を同時に申請した場合には、会社として有給休暇の取得に制限をかけることができるか。

- Q3. 感染の疑いがある従業員に、出社拒否命令を出すことができるか。
- Q4. 出社拒否命令を出した場合の給与はどうすべきか。
- Q5. 出社拒否命令を出す期間はどうか。
- Q6. 新型インフルエンザの流行により、契約の内容を履行できなくなった場合に、会社は債務不履行責任を負うのか。
- Q7. 新型インフルエンザに感染した従業員が、取引先や顧客と接触し感染を拡大させた場合は、会社に法的責任(損害賠償責任)が発生するか。

【対処の考え方】

- A1. 会社として、適切な新型インフルエンザ対策を取っている場合においては、出社命令を出すことも可能である。
- A2. 原則として、有給休暇の申請を制限することはできない。例外として、「事業の正常な運営を妨げる場合」に限り、会社は時季変更権を行使し、他の時期に有給休暇を申請するように指示をすることができる。
- A3. 使用者には、他の労働者に対する健康配慮義務と職場の安全配慮義務が課せられている。この義務を履行するために、新型インフルエンザに感染した可能性のある社員に対し、以下の条件のもとで、出社拒否命令を出すことも可能である。
- 新型インフルエンザ対策を策定し、適切な健康管理体制を構築していること
 - 専門家(医者)などの判断を求めるなどの客観的な判断資料を収集すること
 - 同資料に基づいて判断をすること
- A4. 労務を提供していない以上、その際の給与についても、支払義務は発生しない。もっとも、会社が適切なインフルエンザ対策をしていない場合には、「債務者の責めに帰すべき事由によって債務を履行することができなかつた場合」(民法536条2項)又は「使用者の責めに帰すべき事由」(労働基準法26条)に基づいて、給与の支払義務が発生する。なお、法律的には、給与の支払義務が発生しないとはいえ、従業員に賃金を払わないことはその生活への影響が大きいことから、暫定措置として、一定の賃金の支給を検討することも考えられる。
- A5. 適切なインフルエンザ対策の元においては、無給の出社禁止命令が認められる以上、その期間は、適切な期間でなければならない。その際には、単なる自己申告と診断書のみによるのではなく、産業医などの意見を聞き、客観的な判断資料に基づいて、その期間等を決定しなければならない。かかる義務を怠った場合には、出社禁止期間中の賃金を支払う義務が発生する。
- A6. 債務不履行責任は、その債務の不履行について「帰責事由がない」場合でない限り免れることはできない(金銭債務除く)。新型インフルエンザは、未知の感染症ではあるものの、一定の対応策をとるべき指針が示されている(予見可能性があり、結果回避義務がある)。従って、事業者としては、パンデミックに備え、臨時の雇用をする・流行に至っていない地域の事業所に事業を委託する、商品の備蓄をするなど、契約の履行に向けた努力をするべきであって、例え新型インフルエンザの流行によるものであっても、債務不履行責任を

免れるものではない。

- A7. 病気を感染させる行為は、不法行為(民法709条)及び傷害罪(刑法204条)を構成しうるのであるから、理論上、従業員が新型インフルエンザを感染させた場合には、会社には不法行為責任が発生しうる(民法717条)。もっとも、実際には、感染ルートの特定は困難であること及び故意・過失の立証が困難であることなどから、会社が損害賠償を請求される可能性はそれほど高いものとは言えない。しかしながら、会社が新型インフルエンザ対策を全く取っておらず、漫然と被害を広げた場合や、従業員が新型インフルエンザに罹患していることを認識しつつ業務に従事させていた場合などにおいては、会社の法的責任が認められることも考えられる。

(4) 事業継続マネジメントシステム(BCMS)

感染流行(パンデミック)時にどのように病院・診療所・保健所など医療機関の維持、食料・日用品の輸送・販売の維持、さらに警察・消防・行政機能の維持をどうすべきか、との論議がありBCMSが注目されました。

中でも、BCP(事業継続計画書)の発動準備時点と発動時点は特に注目されました。図表 2-18 は、従業員や関係者の欠勤率とBCPの状況を示しています。

図表 30 欠勤率と対策レベル

	新型インフルエンザの対策レベル			
	感染注意	感染警戒	感染嚴重警戒	部分休業
欠勤率の目安	10%未満	10%以上、20%未満	20%以上、30%未満	30%以上
対策準備室など	設置しない	対策準備室の設置	対策本部の設置	
BCPの発動	発動しない	BCPの発動準備	BCPの発動	

図表 31、32 は企業の施設別従業員数とBCPレベルとの関係を表したもので、従業員数が多くなるとBCPのレベルも高くなることを示しています。

図表 31 BCPレベルの内容

BCPのレベル	代行要員の確保	優先事業の維持	社外連絡の維持	社内連絡の維持
高				
中	×			
低	×	×		

○：実施する ×：実施しない

図表 32 従業員数とBCPのレベル

施設単位	従業員数	BCPのレベル
本社(東京)	多	高
仙台支店	中	中
大阪支店	中	中
北陸営業所	少	低
福岡支店	中	中
那覇営業所	少	低
中央研究所	中	中
関東工場	中	中
九州工場	多	高
東京コールセンター	多	高

2010年8月31日に人に感染すると高い致死率になる可能性が高い、鳥インフルエンザウイルス(H5N1)が、豚の体内で人に感染しやすく変異していることが確認されたと報道されています。今後に、注意が必要です。

第 7 章 外部から購入して部品・材料・サービスの脆弱度と影響度評価

第 5 章でインフラの脆弱度と影響度を評価しましたが、ここではインフラ以外に外部から購入している部品・材料・サービスの脆弱度と影響度を評価します。鍵となる部分は、一社購買です。一社購買は、その一社が災害・事故で生産が停止すると部品・材料・サービスの供給停止を経て自社の生産や販売に影響を及ぼします。

7.1 サプライチェーンを途絶させない

2008 年 9 月 5 日に発生した新潟県中越沖地震で柏崎市に二つの工場を持つ自動車部品会社が被災し、自動車製造に必須の部品であるピストンリングの生産が止まり、これを起因として地震の被害が全くなかった自動車生産会社の製造ラインが停止したのを記憶している方も多いと思います。これは、部品の供給が停止したことによるサプライチェーンの途絶事例です。

2007 年 3 月 20 日に化学会社の直江津工場爆発火災事故により医薬品のカプセルに使われているメチルセルロースの材料供給が国内消費量のうち 95%が停止し、医薬品の供給懸念が生じたため海外から緊急輸入を厚生労働省が決めたこともあります。こちらは材料の供給が停止したことによるサプライチェーンの途絶事例です。

海外の取引先を含めるとサプライチェーンの途絶事例は多くなります。例えば、四国にある特殊材料製造工場の火災が、米国中西部にある半導体工場のラインを止めることもありましたが、米国西海岸の港湾ストライキが日本の自動車会社の米国工場を減産に追い込んだこともあります。

このサプライチェーン経由で発生するディスラプションを防ぐには、以下の ~ を実施し、との対策を講ずることになります。

- 協力会社毎に納品している全ての部品・材料・サービスを明確にすること
- 一社購買の部品・材料・サービスを明記すること
- 全ての部品・材料・サービスの要件、仕様、認定手順が明記され、定期的に更新されていること
- 全ての部品・材料・サービスについてセカンドサプライヤーを明記すること
- 協力会社が災害・事故・事件で被災しても関係する部品・材料・サービスの納品に滞りがないような計画を策定すること
- 協力会社に災害・事故・事件を低減させる対策を構築し、実行を要請すること

ここで、の対策は自社が行う二重化対策です。具体的には在庫の積み増しや代替部品・材料・サービスの活用、セカンドサプライヤーの活用、代替部材の使用による製品仕様の変更などになります。

は協力会社をお願いするリスク排除・低減対策で、自社が要請し、要請が聞き届けられない

場合は、他社との取引に代えるものです。

7.2 部品・材料表を作成する

施設毎にインフラを除いた購入部品・材料・サービスの一覧表を作成します。要員・材料・部品については1日の必要数量、生産設備については稼働台数と保守のレベル、各種サービスについて保守のレベルを概要に明記します。

図表 33 外注部品・材料・サービス一覧表

項	目	コード 番号	数量 / 日	概要	供給会社
要員	受入検査員	H-01	2名	技術習得に2ヶ月	H1社
	警備員	H-02	8名	技術習得に2日間	H2社
	清掃作業員	H-03	4名	技術習得に2日間	H3社
材料	A1材料	M-01	2t	主要材料	M1社
	A2材料	M-02	1t	主要材料	M2社
	A3材料	M-03	400Kg	補助材料	M3社
	A4材料	M-04	100Kg	パッケージ材料	M4社
部品	B1部品	P-01	800個		P1社
	B2部品	P-02	2,400個		P2社
	B3部品	P-03	2,400個		P3社
	B4部品	P-04	800枚	説明書	P4社
項	目	コード 番号	稼働数	概要	供給会社
設備	K1検査装置	N-01	2台	保守レベル4	N1社
	K2検査装置	N-02	2台	保守レベル3	N2社
	K3加工機	N-03	8台	保守レベル5	N3社
	K4加工機	N-04	8台	保守レベル4	N4社
サービス	通信系	S-01	一式	保守レベル4	S1社
	警備システム	S-02	一式	保守レベル5	S2社
	事務機器	S-03	一式	保守レベル2	S3社
	空調システム	S-04	一式	保守レベル2	S4社

【保守レベル:参考】

レベル5: 供給会社の保守要員が常時待機

レベル4: 異常時は供給会社の保守要員が2時間以内に点検・保守

- レベル3: 異常時は供給会社の保守要員が6時間以内に点検・保守
 レベル2: 異常時は供給会社の保守要員が12時間以内に点検・保守
 レベル1: 上記以外

次に在庫、予備設備、セカンドサプライヤーとその認定状況を確認し、図表 34 を作成します。ここで重要なのは、代替の品質や納期の認定と、認定年月日です。認定は毎年更新が必要です。また、セカンドサプライヤーがない場合は、在庫の積み増しなどの検討が必要になります。

図表 34 在庫およびセカンドサプライヤー表

コード 番号	数量/日	在庫	供給会社	セカンド サプライヤー	認定	認定 年月日
H-01	2名		H1社	H21社	済	10-08-01
H-02	8名		H2社	H22社	未	
H-03	4名		H3社	H23社	済	10-07-01
M-01	2t		M1社			
M-02	1t		M2社			
M-03	400Kg		M3社			
M-04	100Kg		M4社			
P-01	800個		P1社			
P-02	2,400個		P2社			
P-03	2,400個		P3社			
P-04	800枚		P4社			
コード 番号	稼働数	予備設備	供給会社	セカンド サプライヤー	認定	認定 年月日
N-01	2台		N1社			
N-02	2台		N2社			
N-03	8台		N3社			
N-04	8台		N4社			
N-05	4台		N5社			
S-01	一式		S1社			
S-02	一式		S2社			
S-03	一式		S3社			
S-04	一式		S4社			

7.3 脆弱度と影響度

外部から購入している部品・材料・サービスの脆弱度は、過去の事故数(供給途絶・中断・損傷・混乱)と代替サプライヤーの確保の容易度・困難度から算出します。影響度は、その部品・材料・サービスが施設の事業に与える影響度で見ます。これを図表 35 にまとめます。

なお、対策としては、事故数を下げる、セカンドサプライヤーの確保を容易にする、影響度を下げる、になります。過去の事故数が少なく、セカンドサプライヤーの確保が難しく、かつ影響度が高いものは要注意です。

図表 35 関係要員の脆弱度と影響度

コード番号	過去の事故数 A	セカンドサプライヤーの確保 B	影響度 I	評価値 A*B*I
H-01				
H-02				
H-03				
M-01				
M-02				
M-03				
M-04				
P-01				
P-02				
P-03				
P-04				
N-01				
N-02				
N-03				
N-04				
N-05				
S-01				
S-02				
S-03				
S-04				

【過去の事故数】

まず、原因を問わず部品・材料・サービスの途絶・中断・損傷・混乱を数える。各種保守サービスは 6 時間の中断を 1 回とする。従って 8 時間の場合は 2 回になる。期間は過去 5 年間。

ポイント 5: 途絶などが 100 回以上

ポイント 4: 途絶などが 30 回以上、100 回未満

ポイント 3: 途絶などが 10 回以上、30 回未満

ポイント 2: 途絶などが 5 以上、10 回未満

ポイント 1: 途絶などが 5 回未満

【セカンドサプライヤーの確保】

ポイント 5: セカンドサプライヤーがない、または認定していない

ポイント 4: セカンドサプライヤーを認定している

ポイント 3: 毎年 1 回活用している

ポイント 2: 毎年 2 回以上活用している

ポイント 1: 常に活用している

【部品・材料・サービスの影響度】

ポイント 5: 高い

ポイント 4: 5 と 3 の間

ポイント 3: 普通

ポイント 2: 3 と 1 の間

ポイント 1: 低い

7.4 一社購買についてのマネジメントシステム

部品・材料・サービスが特殊なため、またはコストの関係で一社購買をせざるを得ないケースがあります。この場合は、次のマネジメントシステム項目を整備します。

一社購買の必要性を認定する手順が整備されていること

当該部品と当該サプライヤーの供給履歴書、供給能力書、在庫計画書が整備されていること

当該部品についてリードタイムの確認手順が整備されていること

当該部品について供給履歴と需要予測が利用可能なこと

当該サプライヤーの長期および短期的な供給能力について緊急時の柔軟性が追跡調査されていること

7.5 新製品開発の際のマネジメントシステム

新製品の開発の際は、次のマネジメントシステム事項を整備します。

関係するサプライヤーの継続供給能力についてチェックする手順と文書が整備され、関係する技術者や製品開発者に手順が周知されていること

関係する主要な治工具、製造装置、部品・材料・サービスの安定供給についてサプライヤーの能力を評価する手順と文書が整備されていること

関係するサプライヤーに要求する事業継続項目を決める手順と文書が整備されていること

関係するサプライヤーに必要な事業継続項目が通知され、確認されていること

第 8 章 IT システムの脆弱度と影響度評価

情報技術 (IT) システムは、企業内の基礎インフラとして電気や水と同様に基礎的経営資源になっています。IT システムが停止すると、製造ラインや販業務、各種事務が止まる企業が一般的です。したがって、BCMS は、この IT システムを止めないことを求めます。

なお、本章は 2008 年に共立出版社から刊行された「事業継続マネジメントシステムの構築と実務」第 4 章を大幅に修正したものです。

8.1 IT システムの特徴

IT システムはソフトウェアとハードウェアから構築されています。ソフトウェアは、新しいシステムを開発する過程での不具合を除けば、誤動作で業務を中断させることはほとんどありません。ただし、運用テストが不十分な場合と、想定した処理能力を超えた場合にはシステム中断を招きます。従って、システムの移行に当っては、開発フェーズのテスト(単体テスト、結合テスト)、運用フェーズのテスト(データテスト、平行運用)を厳密に行い、システムが事業中断の主因にならないことを BCMS は求めます。

運用テストが不十分でシステムが停止した事例は、金融機関が合併し、IT システムを統合する際に発生しています。2002 年 4 月 1 日の M 銀行、2008 年 5 月 12 日の T 銀行などです。また、想定した処理能力を超えたためシステムが停止した事例は、2006 年 1 月 18 日に東京証券取引所で発生しています。

これに対し、ハードウェアの異常は、一定時間内に確率的に発生し、事業中断を招く原因のひとつです。この解決方法は、冗長性をシステム構築の中に組み込むこととなります。

8.2 ハードウェアのチェック

電源・通信ネットワークを含めたハードウェアの問題は、火災・落雷・経年劣化・ウィルス攻撃など数多く発生し、IT システムを中断させています。中断が発生すれば、再稼動するための修復が必要になります。オンサイトの保守サービスに加入した場合も、復旧サービスを依頼してから担当者が来社し、作業を終了するまでの時間は、最低でも 2 時間から 4 時間は必要になります。2 時間以上 IT システムが止まると困る業務が多数ありますから、この中断時間を短くする方策が必要になります。BCMS は、いかなるディスラプションに対しても、この IT システムの中断時間を短くするシステムを構築することを求めます。

落雷で中断が発生し、ハードウェアの一部を入れ替える必要が生じてから、必要な器材を購入しては時間がかかります。この時間を短くする必要がある場合は、必要な器材のスペアを確保し

て、中断時間を短縮します。しかし、どの器材が入れ替えを必要とするかは不明ですから、全ての器材のスペアを持つこととなります。ただし、この方法は設備費に加えて、保管スペースや管理などのコスト的な問題を引き起こします。

地震など広域災害を考えると、現用システムと同じシステム(代替システム)を遠隔地に持つ以外に、BCMS が求める解答はないのです。この代替システムの保持には以下のような種類があります。

- 遠隔地の施設に代替システムを置く
- 遠隔地の他社に代替システムを置く
- 遠隔地に施設がなく、他社との協力も困難な場合は、遠隔地にバックアップサイトを設置する

8.3 遠隔地

ここでの「遠隔地」とは、「同一の地震、台風などで被災しない」程度に離れた場所を指しますが、具体的に「何キロ」という固定解はありません。米国は、国土が大きいので、遠隔地を「1600km 以上」とすることがありますが、これも「1000 マイル = 遠く」の意味で、1600km という数値に科学的な根拠があるわけではありません。

日本では、東京と大阪(600km)という事例がいくつかあります。この距離ですと、地震の原因となるプレートが異なりますし、同一台風で被災する可能性も低くなりますので、効果が期待できません。

また、米国では「2 社以上の電力会社から電気の供給を受けていること」が、バックアップサイトの要求事項になっていますが、日本では二つ以上の異なる変電所からの受電が、達成可能限界とします。

主に英語を使う顧客を持つ企業の場合は、米国設備のバックアップサイトをイギリスやスイスに置く事例や、インドに置く事例もあります。日本語の顧客を対象とする場合は、入力については漢字圏である中国を活用出来ますが、会話を必要とする業務は国内にバックアップサイトを設置することになります。

8.4 バックアップサイト

バックアップサイトは次のように区別されます。自社または他社の遠隔地施設に代替システムを置きバックアップサイトとすることが出来る場合は、そのサイトには関係者が常に通常業務を行っていますので、ホットサイトにする事は容易であると考えられます。

- ホット・バックアップサイト(ホットサイト)
常に、現用システムと同じシステムが稼働しており、定期的に現用システムのデータをコピーしている。

- ウォーム・バックアップサイト(ウォームサイト)
スペースと必要な器材がすべて確保されている状態。ただし、平時は稼働しておらず、緊急時にのみシステムを起動する。データやシステムは、緊急時になってから、保管場所から再導入される。
- コールド・バックアップサイト(コールドサイト)
スペースのみ、または、スペースとある程度の器材が確保されている状態。緊急時には、器材の組立てや追加器材の調達・搬入が必要になる。

ホットサイトは、常時稼働していますから、現用システムが停止した場合も、即時に代替運用が可能となります。しかし、ウォームサイトは、常時稼働していませんので、緊急時に備え、関係要員の移動を含め稼働訓練が必要になります。さらに、コールドサイトは、稼働訓練ができませんから、緊急時の稼働に疑問が残ります。

8.5 各種データの評価

BCMS は、各種データについても他の業務と同様に、影響度を考慮することを求めます。これは、影響度により保管場所を 3 箇所または 2 箇所に決めるためと、更新時間を毎秒・毎時・6 時間・12 時毎などに決めるためです。

図表 36 各種データの評価表

データ名	RPO	脆弱度 V	影響度 I	V*I	管理責任者	更新日
人事関係						
勤務時間/出勤状況						
業務・評価						
履歴・賞罰						
財務						
為替業務						
帳票管理						
財務諸表						
事故履歴						
文書						
管理文書						
更新履歴						

保管場所						
事故履歴						
顧客情報						
受注商品						
受注実績						
事故履歴						
サプライヤー情報						
発注商品						
発注実績						
倉庫管理						
事故履歴						
生産管理						
製造						
サービス						
その他						

【脆弱度】

データの紛失、改竄、漏洩などの過去 5 年の事故数から算出する。

ポイント 5: 事故数が 10 件以上

ポイント 4: 事故数が 5～9 件

ポイント 3: 事故数が 2～4 件

ポイント 2: 事故数が 1 件

ポイント 1: 事故数が 0 件

【各種データの影響度】

ポイント 5: 高い

ポイント 4: 5と3の間

ポイント 3: 普通

ポイント 2: 3と1の間

ポイント 1: 低い

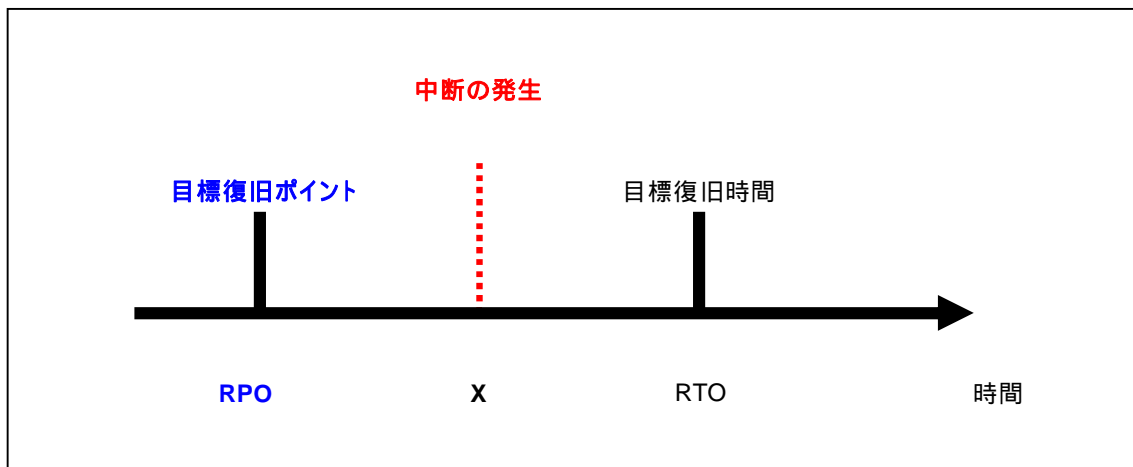
8.6 目標復旧ポイント(RPO)

RPO は Recovery Point Objective の略語で、ディスラプションにより IT システムが中断した場合に、失われたデータを中断の発生時点から何時間(何秒)前のポイントまで回復できるかという目標です。

金融機関では、なにが起きても「RPO はゼロ秒」が基本です。これは、災害・事故・事件が発生し

でも、直前までの情報を使えるように運営することです。金融機関でIT障害が発生し、現金自動入出金機械(ATM)が停止することも問題ですが、数秒前に行った入出金情報が喪失することは、ATM停止以上に大きな問題になります。

図表 37 目標復旧ポイント(RPO)



RTO: Recovery Time Objective、目標復旧時間

(注意) 目標復旧時間は、継続対策を含めて事業を再開するまでの時間で、被災施設を復旧する目標時間ではありません。

第9章 重要な経営資源への対応

重要な経営資源とは、その会社に代替となるものがなくかつ当該会社の経営に高い影響力がある資源のことで、次のものです。

- 最新鋭の生産装置や検査装置
- 既にメーカーが生産を取りやめた生産装置
- 熟練した職人、独創性の高い技術者や研究者
- 鉄道会社の主力鉄道路線
- 百貨店やスーパーの主力店舗
- 金融機関の本支店
- メーカーの主力工場、中心的な研究所
- その他

社会的に重要な経営資源もあります。これは次のものです。

- 都道府県庁、市町村の役所・役場
- 地域の中心的な病院
- 道路、港湾関係、空港関係
- 中心的な駅
- 通信施設
- 電力供給施設
- 上下水道施設
- ガス供給施設
- 学校施設
- 警察署、消防署
- その他

重要な経営資源については、全体的な二重化対策は取れませんのでリスク排除対策とリスク低減対策に依存することになります。ただし、当該資源を機能、サブシステム、部品、材料、サービスに分解し、可能な限り部分的な二重化対策を取ります。

なお、重要な経営資源に対しては以下の文書が必要になります。また、これら文書を毎年更新する必要があります。

(1) 各種施設(鉄道路線、主力店舗など)

該当施設が全社に与える影響度の分析書

該当施設の責任者と次席責任者、および責任内容と範囲が明記されている文書

該当施設と周辺環境の脆弱度の評価表

該当施設を機能毎に分け脆弱度と影響度を評価した文書
各機能をさらに部品・材料・サービスに分け脆弱度と影響度を評価した文書
部品・材料・サービス毎の供給源とその入手方法を明記した文書
該当施設のリスク低減対策書
該当施設の緊急時対策書、継続対策書、復旧対策書
該当施設の訓練計画書

(2) 各種装置(最新鋭の生産装置など)

該当装置が全社または施設に与える影響度の分析書
該当装置の責任者と次席責任者、および責任内容と範囲が明記されている文書
該当装置の操作と保守の手順書
該当装置の操作と保守要員の訓練書
該当装置の部品・材料・サービス毎の供給源とその入手方法を明記した文書
該当装置と周辺を含むリスクアセスメント
該当装置と周辺のリスク低減対策書
該当施設の緊急時対策書、継続対策書、復旧対策書
該当装置の将来的な代替戦略を明記した文書

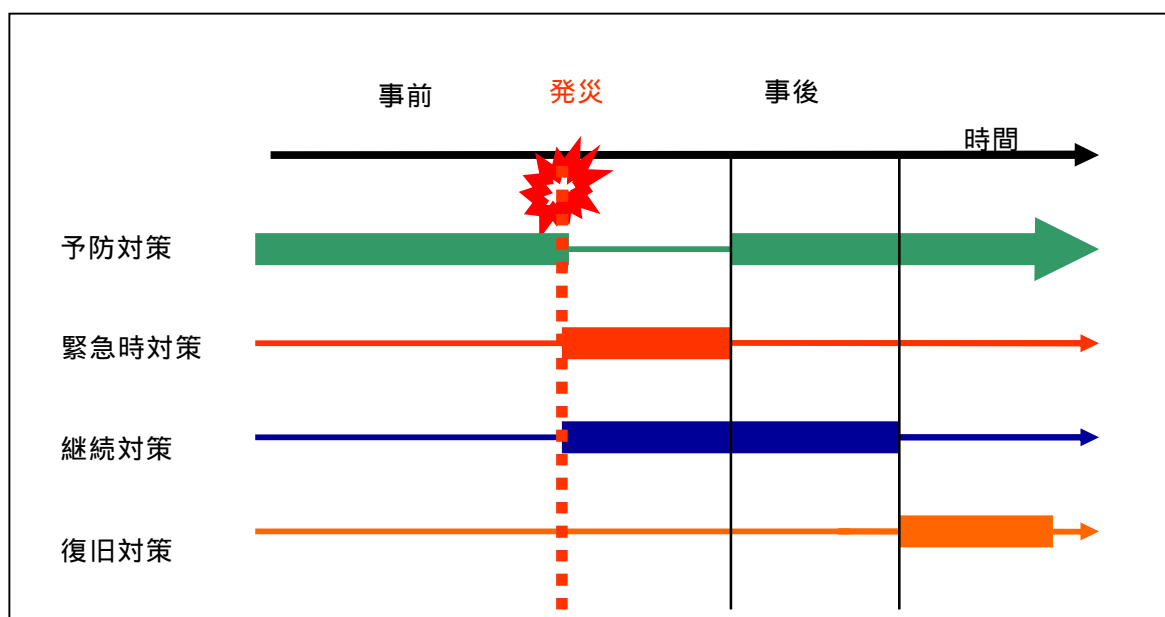
(3) 該当する要員

該当要員が全社または施設に与える影響度の分析書
該当要員の責任者と次席責任者、および責任内容と範囲が明記されている文書
該当要員に必要な知識、経験、資格、意欲、その他を明記した文書
該当要員の後継者の育成に必要な手順と期間を明記した文書
該当要員のリスクアセスメント
該当要員のリスク低減対策書
該当要員の緊急時対策書
該当要員が担当する業務の将来的な代替戦略を明記した文書

第 10 章 予防対策

第 1 章で概説した各対策と時間との関係を思い出して下さい。実際は、発災と緊急時対策の関係はこれほど単純ではなく、台風のようにかなり前から発災が予見出来るもの、金属の経年劣化やテロのように事前に予見できる場合は発災を防ぐことも可能なもの、感染症のように事前に予見できるが発災を防ぐことが困難なもの、などがあります。

図表 38 時間と各対策との関係



10.1 二つの予防対策

第 4 章で触れましたが、予防対策には大きく分けて二つあります。ひとつはリスクアセスメントから導かれる対策で、リスク排除対策やリスク低減対策です。今ひとつは BIA から導かれる対策で、二重化対策です。これを自社の人命および重要な経営資源、その他の経営資源、サプライチェーン経由やインフラ経由と組み合わせると次の三つになります。

- 自社の人命および重要な経営資源 → リスク排除・低減対策
- 自社のその他の経営資源 → リスク排除・低減対策と二重化対策から選択
- サプライチェーン経由またはインフラ経由 → 二重化対策

ただし、自社の重要な経営資源については、機能やサブシステムなどに分解することにより部分的な二重化は可能になります。

10.2 リスク排除・低減対策

第2章で既に以下の作業をしていますが、本章ではこのデータを元に作業を進めます。

施設がある地域の外部に起因する災害・事故・事件の発生頻度

施設がある地域の周辺環境の脆弱度評価

施設毎に建物内部と外部の脆弱度評価

施設毎に内部に起因する事故・事件の発生頻度評価

リスク排除対策を取ることは理想ですが、これは大変難しい問題を抱えています。コストです。例えば、今の科学技術であれば絶対に落ちない飛行機を製造することは可能です。しかし、このコストは大変高くなります。また、絶対に爆発しない化学工場を建設することも可能ですが、この場合は、生産量を著しく小さくするか、防爆対策を極めて厳重に実施することになり、投資効率は極めて悪くなります。そこで、ここではリスク低減対策を概説することにします。

施設毎に人命が関係する可能性がある災害・事故・事件(以下「災害など」)の発生頻度を見ます。これは、上記の「施設がある地域の外部に起因する災害などの発生頻度」と「施設毎に内部に起因する事故・事件の発生頻度評価」で分かります。

発生頻度が高い災害などの順にまず図表 39 を作成します。この図表 39 の目的は、予想被害を可視化することです。なお、この想定被害表は毎年更新します。

図表 39 想定被害表

対象施設	A 市地区		
対象リスク	台風 (平成16年台風18号規模)		
被害が最大規模の場合			
予想される 直接被害	建物外部		
	建物内部	要員	
		IT機器	
		業務機器	
	材料・部品		
インフラ			
予想される 業務中断	IT関係の中断時間		
	その他業務の中断時間		

	協力会社の中断時間		
	全体の業務中断時間		
予想される 直接被害額	建物外部の復旧費用		
	建物内部の 復旧費用	要員	
		IT機器	
		業務機器	
		材料・部品	
その他			
予想される 間接被害額	業務中断による A市地区の被害額		
	業務中断による 全社の被害額		
	その他		
保険関係	関係支払 保険額		
	関係受取 保険額		
被害が中規模の場合			
予想される 直接被害	建物外部		
	建物内部	要員	
		IT機器	
		業務機器	
		材料・部品	
インフラ			
予想される 業務中断	IT関係の中断時間		
	その他業務の中断時間		
	協力会社の中断時間		
	全体の業務中断時間		
予想される 直接被害額	建物外部の復旧費用		
	建物内部の 復旧費用	要員	
		IT機器	
		業務機器	
		材料・部品	
その他			
予想される 間接被害額	業務中断による A市地区の被害額		

	業務中断による 全社の被害額	
	その他	
保険関係	関係支払 保険額	
	関係受取 保険額	

次に、最大規模の被害を想定して、図表 40 を作成します。図表 40 の目的は、各種あるリスク低減対策の効果とコストを検討し、実行する対策を決めるためのものです。なお、この作業表は毎年更新します。

図表40 リスク低減検討表

施設名	A 市地区	対象リスク名	台風	
全体の対策名	A 市地区の台風対策			
全体の対策の目標	平成16年台風第18号規模の台風が来襲し、A 市に最大規模の被害を与えても、業務の中断時間を2日間以内にする			
個別対策(1)	建物に対する対策			
(1)の目標	被害が全くないこと			
実施のための手順	現状での被害予測 修理・修繕箇所の洗い出し 費用の算出 実行レベルの決定			
選択肢	低減対策の 実施期間	リスクが顕在した場合の 結果(予測)	予想される 費用	予想される 排除率
1: 何もしない	0 日			
2: 20%実施:				
3: 40%実施:				
4: 60%実施:				
5: 80%実施:				
6: 全てを実施				
個別対策(2)	ITシステムに対する対策			
(2)の目標	中断がないこと			

実施のための手順	現状での被害予測 脆弱部分の洗い出し 費用の算出 実行レベルの決定			
選択肢	低減対策の実施期間	リスクが顕在した場合の結果(予測)	予想される費用	予想される排除率
1: 何もしない	0日			
2: 20%実施:				
3: 40%実施:				
4: 60%実施:				
5: 80%実施:				
6: 全てを実施				
個別対策(3)	要員の確保			
(3)の目標	必要な要員を確保すること			
実施のための手順	必要な要員数の洗い出し 宿泊などが出来る要員の確認 宿泊費用、各種手当の算出 実行レベルの決定			
選択肢	低減対策の実施期間	リスクが顕在した場合の結果(予測)	予想される費用	予想される排除率
1: 何もしない	0日			
2: 20%実施:				
3: 40%実施:				
4: 60%実施:				
5: 80%実施:				
6: 全てを実施				

次に図表 40 で検討し、実施した対策を元に図表 41 を作成します。図表 41 の目的は、次回の予防対策を検討する際に、その効率を上げるためです。

図表41 リスク低減実施表

施設名	A 市地区	対象リスク名	台風
対策名			
対策の目標			

対策の概要	
全体の費用	
実施した手順	
実施した度合い	
必要な資源（社内）	
必要な資源（社外）	
開始年月	
終了年月	
排除率（予想）	
参考となる利点	
参考となる欠点	

10.3 自社または他社のディスラプションの確認

自社または他社で対象リスクが顕在化した場合は、図表42を作成します。図表42の目的は、経営資源の途絶・中断・損傷・混乱、業務中断時間、直接的な被害額（有形財と無形財）、緊急時対策・継続対策・復旧対策の費用を含めた間接被害額（有形財と無形財）、支払保険額と受取保険額などを含めて、ディスラプションの全体像を把握することです。

図表42 ディスラプション発生報告書

対象リスク			
発生日時		発生場所	
災害などの概要			
被害の経過			
被害の結果			
途絶などした経営資源			
二次的に中断した業務			
その他の影響（社内）			
その他の影響（顧客）			
その他の影響（協力会社）			
緊急時対策	実施概要		
	評価		
緊急時対策	実施概要		
	評価		

復旧対策	実施概要	
	評価	
直接被害額	有形財	
	無形財	
間接被害額	有形財	
	無形財	
保険関係	関係支払 保険額	
	関係受取 保険額	
今後の対策への参考		

10.4 ヒヤリハットの調査

予防対策のひとつにヒヤリハットの調査があります。これは従業員および関係者に対して、インタビュー形式で行います。この聞き取りには、図表43が参考になります。図表43の目的は、顕在する可能性が高いリスクと途絶。中断などを起こす可能性がある経営資源を洗い出すことです。

図表43 ヒヤリハット報告書

インタビュー者		被インタビュー者	
聞き取り日時		聞き取り場所	
対象となるリスク			
途絶・中断の可能性 がある経営資源			
二次的に中断する 可能性がある業務			
その他の影響			
リスク顕在化 の結果	最悪の場合		
	かなり悪い場合		
	上記以外		
各種対策への参考			

10.5 経営資源の二重化対策

二重化対策はBIAから導かれる対策で、自社の人命と重要な経営資源を除く資源のディスラプションと、インフラ経由やサプライチェーン経由のディスラプションに対応します。対策の内容は、生産ライン、販売、倉庫、部品、などの二重化です。なお、以下は二重化対策について概説した章と個別の経営資源です。

- 第5章：インフラ関係
- 第6章：代行要員
- 第7章：外部から購入している部品・材料・サービス
- 第8章：IT関係

10.6 複合的な経営資源の二重化対策

ここでは、各種の経営資源を持つ工場と販売の二重化について概説します。主力工場や百貨店・スーパーの主力店舗の場合は、全てを二重化することは難しいですが、一部の生産商品・販売商品・業務を二重化することにより企業の事業継続性を上げることが出来ます。また、研究所・役所・病院の一部業務も二重化が可能ですので、ご検討下さい。

(1) 生産ラインの二重化

ひとつのラインが停止しても、他のラインで生産を継続させるには以下の方法があります。BCMSが推奨しているのは、「C」と「D」です。

同一建屋内に、同じ商品を生産するラインを複数設置するもの

- 要員・部品などの供給および管理が容易
- 建屋が火事や地震で被災した場合は、関係する生産ラインが全て停止する

同一敷地内の別の建屋に同じ商品を生産するラインを複数設置するもの

- 要員・部品などの供給および管理が容易
- 地震や水害、インフラ中断などの際には、複数のラインが同時に停止する

離れた施設に、同じ商品を生産するラインを複数設置するもの

- 要員・部品などの供給および管理も二重化が必要になる
- 地震や水害、インフラ中断などの際にも、複数のラインが同時に停止することはない

遠隔地の他社に委託生産

- 要員・部品などの供給および管理が複雑になる。製造ノウハウが流出する
- 地震や水害、インフラ中断などの際にも、複数のラインが同時に停止することはない

(2) 販売の二重化（消費者対応）

店舗販売の場合は、店舗に顧客がついているため代替店舗の活用が難しくなりますが、それでも、被災店舗から代替店舗に専用バスを運行することにより、ある程度二重化は可能になります。

一部商品を通信販売にすると更に二重化のレベルは上がります。このためには、平時に継続対策書を作成する必要があります。

通信販売の場合は、受注センター、倉庫・配送センター、IT システムを二重化することにより、被災時の事業継続性が上がります。こちらも、平時に継続対策書を作成する必要があります。

(3) 販売の二重化（企業間取引）

こちらは、相手先企業に自社の関係部署が被災した場合の対抗策と平時に通知することにより二重化が可能となります。例えば、東京支店が担当していた業務は、新潟支店と仙台支店が代行することです。ただし、代行支店はひとつでなく、二つ以上必要です。これは代行支店の業務量を著しく増加させないためです。このためには、平時に継続対策書を作成する必要があります。

第 11 章 緊急時対策

緊急時対策は、緊急事態対策、クライシスマネジメント、危機管理とも呼ばれます。また、時間経過とともに、次のように分けられます。

発災が確認されるまで

発災の確認

現地対策本部および本社対策本部が設置されるまで

現地対策本部および本社対策本部の設置

現地対策本部および本社対策本部の活動

被害の拡大縮小の調査

詳細な被害調査

事後の検討

対策本部の解散

11.1 発災の確認

まず、施設毎に従業員 10 名当たり 1 名程度を発災確認者に委嘱します。発災確認者の業務は、発災を確認し、対策準備室長または本社および施設の対策本部長に通報することですが、発災の確認は容易ではありません。

台風や火山噴火は、気象庁から事前に情報が出ますので、発災確認者の作業は不要になります。これは一番簡単な発災の確認です。次は、火災・爆発です。これは、周辺のものを含め容易に発災を確認できます。次に容易なのは、地震や水害です。これは、震度 5 弱以上もしくは近隣の河川に洪水注意報が出たら対策本部を設置することを、平時に決めると発災の確認は容易になります。

火災や事故は、発災の基準を明確にしないと発災確認者により判断の違いが出てきます。更に、インフラ経由、サプライチェーン経由のディスラプションは発災の確認が施設内や近隣ではありませんから、発災の基準が明確でないと、発災確認が大きく遅れます。

図表44 発災の基準

災害など	基準
地震	気象庁が震度 5 弱以上を発表した場合
津波	気象庁の津波警報を出した場合
河川の氾濫	近隣の河川に洪水注意報が出された場合

内水氾濫	自社で判断する
風害	自社で判断する
土砂災害	気象庁が注意報を出した場合
干魃	自社で判断する
雪害	自社で判断する
落雷	自社で判断する
噴火・火山灰	気象庁が注意報を出した場合
感染症	欠勤率が 20%を超えた場合
火災・爆発	小火でも発生を確認した場合
窃盗	予兆もしくは犯行が明らかになった時点
テロ	予兆もしくは犯行が明らかになった時点
サイバーテロ	予兆もしくは犯行が明らかになった時点
電力	中断の予兆もしくは中断が明らかになった時点
通信	中断の予兆もしくは中断が明らかになった時点
部品	決めてあるサプライヤーの被災が確認された時点
材料	決めてあるサプライヤーの被災が確認された時点
サービス	決めてあるサプライヤーの被災が確認された時点
社内暴力	自社で判断する
セクハラ	自社で判断する
その他	

また、発災確認者以外の方が発災または発災らしいものを見かけた時の行動を決める必要があります。基本は発災確認者や対策本部要員への通報ですが、これを明確にしないと、二次災害に巻き込まれることがあります。

初期消火、事故への初期対応は、被害の拡大を防ぐ上で大変重要です。しかし、この初期行動は、関係者および警察・消防への通報を遅らせ、第一発見者を被害者にする危険性があります。米国のカリフォルニア州では三人集まるまで初期対応をしてはいけないと教育しています。これは、一人が初期対応を行い、一人がそれを見守り、一人が関係者および警察・消防と常時連絡を取ることを想定しています。

11.2 現地対策本部および本社対策本部が設置されるまで

発災確認者から対策本部長に通報があった場合は、速やかに対策準備室を立ち上げます。これは全ての通報に対して立ち上げます。準備室長は、その通報の真偽と被害の拡大縮小傾向を確認し、警察、消防、その他の関係先に通報するとともに、対策本部設置の有無、施設内の全て

の発災確認者への通知の有無を判断します。

なお、災害などは、「軽微な被害」で済むものと、「重大な被害」に至るものがあります。軽微な被害とは、次の条件を全て満たすもので、それ以外は全て重大な被害になります。

- 人への被害がない
- 近隣への影響がない
- 二次災害がない

軽微な被害と準備室長が判断した場合は、対策本部は設置しませんが、速やかに発災報告を作成し対策本部長に報告します。また準備室の解散は、対策本部長が行います。

マネジメントシステムとしては、軽微な被害の判断基準と対策本部の設置基準、警察・消防などへの通報基準、発災確認者への通知基準を文書化し、毎年更新することが必要になります。

11.3 軽微な被害

具体的に軽微な被害をもたらす災害などは次のようなものですが、各項目の金額、数量、時間、また影響度などは自社で基準を作成する必要があります。

- 小火
- 部品・材料・商品の小量(金額または量を決めます)の紛失
- 機器・設備の異常(異常時間の長さを決めます)
- 照明機器や各種工具の異常(影響度を決めます)
- 施設内のセクハラ、パワハラ(影響度を決めます)
- IT 障害(時間と影響度を決めます)
- パソコンの異常(数量、異常時間、影響度を決めます)
- 警報システムの異常(異常時間、影響度を決めます)

11.4 現地対策本部および本社対策本部の設置

対策準備室から対策本部への変更は、準備室長が提案し対策本部長が実行します。本社対策本部長は社長が、現地対策本部長は施設長が就任するのが一般的です。各対策本部要員は平時に各対策本部長が決めますが、図表 45 はその参考です。

図表 45 対策本部の要員

業務名	現地・本社	業務内容
対策本部長	両者	対策本部を指揮する

対策副本部長	両者	対策本部長を補佐する
対策準備室長	両者	軽微な被害の場合に、全てを指揮、管理する
財務担当	両者	緊急時対策、継続対策に必要な財務を担当する
法務担当	両者	緊急時に法令違反がないように監視、助言する
調査担当	両者	被害の拡大縮小を調査する。詳細な被害調査を担当する
広報担当	本社	株主、近隣住民、隣接会社、メディアなどへの連絡を担当する
連絡担当	両者	警察、消防、行政、病院などとの連絡を担当する
情報担当	両者	安否確認と従業員との連絡を担当する。
ITシステム担当	本社	ITシステムを担当する
顧客担当	本社	顧客への連絡を担当する
協力会社担当	本社	協力会社への連絡を担当する
教育・訓練担当	両者	次回の緊急時に備え、訓練計画を検討、作成する
危機対応チーム リーダー	現地	自衛消防隊の隊長など
予防対策責任者	両者	必要に応じ、防災用品などの配布を担当する
継続対策責任者	両者	継続対策の実施、その期間、それに関する業務
復旧対策責任者	両者	復旧対策を担当する
書記	両者	緊急事態の推移と対策を把握し、記録する

11.5 現地対策本部および本社対策本部の活動

両対策本部は、次の3点を守り、各種活動を行います。

- 関係者の安全と健康を最優先する
- 法令と企業倫理を遵守する
- 企業の社会的責任を果たす

現地対策本部の活動は、当該施設とその近隣に限定します。他の施設との連絡は、本社対策本部が担当します。また、ITシステムのハードウェア・ソフトウェア・データ維持管理は、本社対策本部が担当します。これらを簡潔に文書化し、毎年更新します。

11.6 被害の拡大縮小の調査

被害が拡大傾向にあるのか、縮小傾向にあるかを調査します。そのためには「判断のトリガー」が必要になります。「判断のトリガー」は河川氾濫の場合は川上の雨量、火災の場合は延焼状況、地震の場合は機器の転倒などです。

11.7 詳細な被害調査

被害の拡大が停止し、二次被害の危険がなくなってから詳細な被害調査を行います。この調査結果は図表4-5の「ディスラプション発生報告書」に準じ様式を作成し、記録します。

11.8 事後の検討

詳細な被害調査を元に緊急時対策の検討をします。これは、防災力などを改善するために大変重要な活動です。

第 12 章 継続対策

継続対策は「代替対策」とも呼ばれます。具体的な行動は以下のようなものですが、これ以外にも多数の行動があります。これらの行動と付随する業務を合理的に整理し、緊急時に無理なく行動を起こせるようにし、自社の事業や業務の停滞を最少化するのが継続対策です。

- 自社または他社の代替生産ラインでの生産
- 自社または他社の代替事務所で業務
- 自社または他社の代替店舗での販売
- 自社または他社の代替 IT システムの活用
- 代行要員の活用
- 代替機器の活用
- 代替会議室(倉庫や駐車場)の活用
- 代替サプライヤー(セカンドサプライヤー)の活用
- 代替部品・代替材料・代替サービスの活用
- 代替電力(非常発電など)、代替水(井戸水など)の活用
- 代行物流ルート of 活用
- 代替港湾、代替空港の活動

12.1 災害などと継続対策の関係

継続対策の基本は二重化ですが、これは大変幅広くどこの会社でも日常的に行っています。コピー用紙のトナーの予備在庫、入場用 ID カードの予備、車の予備タイヤ、予備のパソコン、予備の駐車場、予備の車両、食料の備蓄、これらも実は軽微な事故や事件に対応した継続対策です。

この継続対策が不十分な場合は、大量の複写、ID カードの紛失、突然のパソコンの動作不良などの事故・事件には対応が出来なくなります。われわれは、軽微な事故・事件への対応は無意識に二重化を実施しているのです。

ある程度規模が大きい災害などの場合は、途絶・中断・損傷・混乱する経営資源が増えますので、日常的な継続対策では対応が困難になります。この場合は、改めて継続対策と意識した統制の取れた行動が必要になります。このための簡潔な文書を整備し、毎年更新するとマネジメントシステムになります。

12.2 注意すべき事項

既に、第 5 章から第 8 章で各種経営資源の二重化を概説していますので、ここでは継続対策を

考える際に注意すべき事項について概説します。

(1) 重要な経営資源に対する継続対策

重要な経営資源(第9章)については全体的な継続対策を構築することができません。しかし、機能や構成する部品などに分け、部分的な二重化の比率を高くすることが出来ます。

(2) 代替工場、事務所などを使用する際の注意事項

他社に代替工場や代替事務所をお願いする場合も、自社の他工場や他事務所を使用する際も次の事項を継続対策書に明記する必要があります。これ以外にも必要な事項は明記します。

- 必要な部品・材料・サービスの移動手順
- 必要な部品・材料・サービスの保管、管理手順
- 製品などの管理、搬送手順
- 工場、事務所の使用料、光熱水費、諸管理費、関係事件費
- 関係文書、データの管理手順書
- 各種保険

(3) 要員が移動する際の注意事項

代替工場や代替事務所に必要な要員を移動する場合は、次の事項および追加事項を継続対策書に明記します。

- 代替行動のための訓練手順
- 移動手順
- 移動の経費
- 移動先の宿泊設備、食事、健康管理
- 各種手当
- 移動先の連絡網
- 社会保険

(4) IT 関係の注意事項

- 代替システムへの移行手順と検査確認手順
- 元のシステムへの移行手順と検査確認手順
- 消失データまたは損傷データの復旧手順
- 鍵類、パスワード、セキュリティコードの保安と管理手順
- 事故・事件の被害査定方法と手順
- 各種費用の算出方法と手順

第 13 章 復旧対策

復旧対策は、警察・消防・行政などの現場検証と自社による詳細な被害調査の終了時点から始めることができます。

継続対策がない場合または機能や部品などの二重化の比率が低い場合は、自社の事業を継続するために復旧を急ぐこととなります。しかし、急ぎ過ぎますと、不十分な被害調査と次の災害などに対する予防対策の不十分な検討となり、脆弱度を低減させることを難しくさせるとともに、近隣住民や取引先に「企業エゴ」の強い会社というマイナスのイメージを与えることとなりますので、注意が必要です。

BCMS では、一般的に「目標復旧時間 (RTO) は短い方が良い」としていますが、この「目標復旧時間」は被災した施設や被災した部分の再開目標時間ではなく、継続対策を活用した事業の再開目標時間です。ある部品を製造している工場が被災した場合に、その被災工場である部品の生産を再開するための目標時間ではなく、代替する工場である部品の生産をするための目標時間です。

13.1 復旧対策の種類

復旧対策には、「軽微な被害」用と「重大な被害」用の二つがあります。軽微な被害とは、次の条件を全て満たすもので、それ以外は全て重大な被害になります。

- 人への被害がない
- 近隣への影響がない
- 二次災害がない

軽微な被害の場合の復旧対策は、現状への回復が基本です。しかし、重大な被害の場合は、次にある基本方針から選ぶこととなります。

- 現状に戻す
- 該当する施設または経営資源の一部または全部を整理する
- 該当する施設または経営資源の一部または全部を改善する

例えば、単線の鉄道線路があるとして、は元の単線に戻す、はその線路を廃線にする、はその線路を複線化する、になります。この基本方針の決定は大変重要ですから、本社対策本部長である社長が決めることとなります。

13.2 現状に戻す

これが一番多い復旧対策です。この方針は、途絶・中断・損傷・混乱した経営資源を正常な経営資源で置き換えることになります。従って、次の手順を明確にし、簡潔に文書にします。

- 再利用可能な資源と、廃棄する資源を評価する手順
- 廃棄方法の手順
- 置き換える経営資源の入手方法と検査方法
- 経営資源を交換する手順
- 最終的な機能テストの手順と評価方法

最終的な機能テストで多いのは、「通常の操作手順で、正常に機能する」です。また、次の手順も明確にし、簡潔に文書にします。

- 復旧対策の終了を確認する手順
- 復旧対策の終了を関係者に連絡する手順
- 復旧対策の終了を宣言する前に、一部の業務を再開する手順
- 復旧対策費の算出方法
- 保険金の請求手順
- 事後の検討

13.3 該当する施設または経営資源の一部または全てを整理する

一部の施設や装置を整理することは、良くある事例です。この場合は、前節「現状に戻す」の拡大版ですから、廃棄する資源が多くなりますが前節の手順がそのまま使えます。ただし、整理された部分の作業手順や二重化は不要になりますから、その部分の修正が必要になります。

ただし、施設を全て整理する場合は、従業員や関係者並びに近隣への対応が必要になることもありますので、慎重な手順を取る必要があります。

13.4 該当する施設または経営資源の一部または全てを改善する

一部の装置や施設を災害などを契機に改善することも、良くある事例です。これにも「現状に戻す」の手順が使えます。なお、削除と追加する作業手順や二重化が発生しますので、その部分の修正が必要になります。

施設の全てを改善する場合は、新たに施設を作るのと同じ手順になります。

13.5 ITシステムの復旧対策

ITシステムの復旧対策は、コアシステムの特定と、コアシステムへの依存度を明確化することから始まります。また、優先順位の高いデータ類を、必要に応じて複数の施設で同時に復旧させることも必要になります。更に、重要な文書・データや作成中の文書類、特殊な文書類を保管する手順を明確に規定することも必要になります。

なお、本節は、2008年に共立出版社から刊行された「事業継続マネジメントシステムの構築と実務」(小職編著)第10章を大幅に修正したものです。

(1) 目標復旧時間(RTO)の要件

ディストラクションによる中断の発生後、いつまでにIT業務を復旧すべきかを規定します。全てのIT業務ごとに業務要件とRTOを明確に規定します。IT関係のディストラクションは、災害などの二次的被害のほか、IT独特のウィルス被害、情報ネットワーク障害、不正アクセス等も考えられます。被害の深刻さと範囲によっては、IT専門家による分析と対策評価が必要になります。実際の復旧には不確定要素があり、期待されるRTOより、はるかに大きな時間がかかる危険性があります。

(2) 復旧対策の始動とITトリガー

復旧対策を始動する責任者と代行者の詳細な連絡先情報を明記します。さらに、復旧対策を始動させる事業上のITトリガーを明確にします。ITトリガーとは、中断後に建物に入りIT業務が再開できるまでの時間、主要サーバーの予想されるダウンタイムの時間、コンピュータウィルスに感染した情報端末の数、情報インフラが復旧するまでの時間、などです。

(3) 始動手順

ITの復旧対策には、始動手順が必要になります。ITトリガーと始動手順を定める目的は、業務の優先順位と活用可能なリソースを明確にすることです。

ITシステムの中断発生時には、通常の連絡手段や代替連絡手段が使えない場合もあります。ITシステムに依存しない緊急連絡網が必要になります。

多くの場合、復旧対策の始動は、電気・通信回線・高速ブロードバンドなどインフラ系の復旧や費用と関連します。中断からIT以外の業務を再開させるため、ITに依存しない手段による対策も必ず検討します。電気などのインフラ系がディストラクションにより中断した場合は、ITシステムの復旧は、自力ではできないか、できても非常に大きな出費になります。

明確に規定されたITトリガーは、意思決定プロセスにおける指針となり、ITシステムの復旧を敢えて待たずに業務の再開を促すこともあります。また、ITトリガーと「容認できない業務上の影響」が発生するまでの時間を関連付ける必要もあります。

(4) 復旧対策の優先順位

ITシステムの復旧対策の適用範囲内で業務、アプリケーション、インフラに関する復旧の優先順位を明確にします。復旧手順はこの優先順位に従います。

(5) 協力会社など

通常利用しているソフトウェアやハードウェア、情報セキュリティサービスの納入業者を明確にしておきます。具体的な連絡先情報や注文書番号を適宜明確にしておきます。認可や支援等を受けるのに必要な協力会社の連絡先情報も盛り込みます。

セキュリティ事件や不正アクセス等の発生時には、事故・事件の管理責任と障害の発生経緯を明確にし、文書化します。契約違反もしくは法令違反では、証拠を明確にし、行政機関または司法機関へ連絡することが必要になります。更に、実際に被害を受けた場合は、サービスあるいはソフトウェアの提供者との間で補償問題が起きることも想定できるため、管理責任と発生経緯の文書化は重要になります。

(6) 事後検討

ITシステムの復旧対策終了後は、速やかに次のような項目を検討し、文書化します。これは、企業の事業継続性を向上させるために大変重要です。

- ITシステムのBRTの召集、始動、終了
- IT始動トリガー
- 代替システム
- 問題の特定
- 解決策の構成要素
- 鍵類、パスワード、セキュリティコードなど
- ハードウェア、ソフトウェアの調達
- 社外保管データからの復旧
- 事前訓練の効果
- その他

第 14 章 訓練

緊急時対策の妥当性を確認するためには、訓練を実施することが必要になります。訓練には、施設毎の机上訓練と実地訓練、全社の机上訓練があります。

14.1 訓練計画を立案する際の注意点

効果的な訓練は、適切な計画立案から始まります。計画立案の早い段階で訓練に関係する主な関係者を明確にし、立案にも参加してもらいます。具体的には、警察・消防・行政、隣接会社、協力会社、顧客、病院などです。

次に、訓練の目的と内容、成功判定基準、特定訓練、そして全ての訓練用メッセージを明確にします。訓練計画を立案する際は以下の点に注意してください。

- 訓練の日程、目的、内容、予想される影響を関係者に周知する
- 該当する施設の訓練に対する成熟度と訓練内容とのバランスをとる
- 会議室、パソコン、白板、固定電話、携帯電話、その他訓練に必要な経営資源を事前に検討し、調達する
- 事前に、訓練の背景と関係するデータ(例えば、火災が A 点で発生し、B 点、C 点が延焼し、D 点で鎮火する)を決定し、現実感を保つようにする
- 製造ラインを止める場合は、再開手順を明確に周知
- 机上訓練には全ての対策本部要員とその代行者を参加させる
- 実地訓練には全ての対策本部要員とその代行者および発災確認者と指定した従業員などを参加させる
- 訓練参加者には、予め訓練スケジュールを伝えるが、訓練の目的が驚きの要素を必要とする場合は、この限りではない
- 訓練の成功判定基準には主要な習得事項を盛り込む。
- 緊急時対策書と訓練で生じたギャップは、調査し、緊急時対策書に盛り込む

14.2 訓練計画に含む諸点

訓練計画には次の諸点を含みます。

- 対策本部の指示系統と報告系統の確認
- 対策本部と警察、消防、行政との連絡方法の確認
- 被害の拡大縮小の調査方法の確認
- 傷害 / 死亡発生時の対応(確認、報告方法を含む)

- 途絶・中断・損傷・混乱した経営資源の確認、報告、対処方法
- ユーティリティーの確認、報告、対処方法
- 安全上の問題の確認、報告、対処方法
- 従業員、顧客、協力会社への連絡方法と連絡内容
- 地域の住民、隣接会社、メディアへの連絡方法と連絡内容
- 食料供給サービスの確保
- 資金調達方法の確認

14.3 訓練計画のチェックリスト

訓練計画の立案が出来たら、次の項目のチェックをします。脱落点、重複点があれば計画を修正します。また、施設の外から実地訓練が見える場合は、事前に地域住民、隣接会社、協力会社、顧客などに訓練の日時、目的、内容を周知します。

- 関係者に、机上または実地訓練の目的、日程、影響を伝える準備が出来ているか
- 訓練参加者の経験や知識に基づき計画が作成されているか
- 訓練のシナリオは十分現実的か
- 訓練で使う連絡網は最新のものか
- 社内ロジスティック(会議室、パソコン、白板、固定電話など)の手配が出来ているか
- 訓練参加者の役割と責任が明確に規定されているか
- 複数の施設が参加する場合には、施設間に複数の連絡手段が確保されているか
- 訓練の成功判定基準は明確か
- 訓練を行うチームごとに、少なくとも1名のオブザーバーを手配したか
- 訓練参加者に、訓練の目的が「訓練シナリオを正確に理解する」ことではなく、「緊急事態にいかに対処するか」である点を明確に伝えてあるか

14.4 訓練で使用するメッセージ

訓練に使う様々なメッセージを作成します。重要な点は、メッセージがもたらす反応を理解することです。図表46は、訓練計画の立案チームが作成します。メッセージはEメール、電話で受信者に伝えます。メッセージは当初の予想より、大変多い数になります。実地訓練をする前に、メッセージの確認のみを机上訓練の方が実際的です。

図表46 訓練時のメッセージリスト

メッセージ		送信時刻		送信者	受信者	予想される 反応と行動
番号	内容	予定	実際			

メッセージが滞留した時の処理方法						
メッセージが混乱した時の処理方法						

14.4 訓練の実行

(1) 訓練前のステップ

図表47を作成し、訓練の参加者全員に周知します。また、訓練のいずれかの段階で本当の緊急事態が発生した場合には、訓練が中止になることを参加者全員に伝えます。

訓練の参加者は、パニックや流言飛語を避けるため、同僚、顧客、協力会社、家族などに必要に応じ訓練のことを伝えます。

図表47 訓練計画の概要書

項目	説明	
訓練の実施場所		
訓練の日時		
想定リスク		
訓練の目的		
訓練の適応範囲		
訓練の適応除外		
訓練の内容	ステップ1	
	ステップ2	
	ステップ3	
	ステップ4	
	ステップ5	
事前の説明会	日時	
	会場	
	参加者	

(2) 訓練の開始

第一発見者、発災確認者、準備室長を経由する発災の確認プロセスを実施し、対策本部の訓練を開始します。

(3) 訓練後の評価

訓練を効果的に終了させるため訓練終了直後に出来れば参加者全員と話し合い、学んだ教訓や提案事項を把握します。その際は図表48のような評価表を活用します。

- 把握した内容は文書化し、緊急時対策書に反映させる
- 訓練時のオブザーバーと面談し、訓練についてのコメントや評価内容を聞き取る

図表48 訓練の評価表

訓練の実施場所	
訓練の日時	
想定リスク	
訓練の目的	
訓練の概要	
良かった点	行動の内容
改善すべき点	行動の内容（緊急時対策書を修正します）
主要な習得事項	<ul style="list-style-type: none"> ●（訓練から学んだ内容をリストアップします。） ● ●

第 15 章 BCMS 構築のための組織

ここでは、全社を対象として BCMS を構築するための社内組織を概説します。施設が対象の場合は、役職名(社長→施設長)や部門名(事業部→部)などを読み替えてください。

15.1 BCMS の責任者

BCMS の責任者は社長または CEO が就任するのが一般的ですが、社長が指名した役員が就任することもあります。なお、BCMS は会社の経営に基づく判断と対策が必要になるため役員以外が就任することはできません。

15.2 BCMS 担当者

BCMS 担当者は BCMS 責任者を補佐する人で、BCMS に関する社内組織を取りまとめ、社内の全業務とインフラ経由、サプライチェーン経由のディスラプションを把握し、ディスラプションによる被害額とそれが経営に及ぼす影響について習熟し、適切な提案を最高経営者に進言できる人になります。

日本の場合は BCMS 責任者に、副社長または専務が指名され、BCMS 責任者の下にリスク室長または BCMS 事務局長が指名されることがあります。

米国では CRO(Chief Risk Officer)が BCMS 責任者兼 BCMS 担当者に就任するのが一般的です。この CRO の権限は大変大きく、保険契約はもちろんのこと、ディスラプション発生時の資金調達先の金融機関との契約にまで及びます。また、IT システムを含めたサプライヤーとの新規または更新契約の際は、安定供給の観点から契約内容をチェックし、サインをします。これは CRO のサインがないとサプライヤーとの新規または更新契約が出来ないことを意味します。また、災害・事故・事件(以下「災害など」)が発生した場合は、CRO が全ての権限を持ちます。さらに、警察・消防・行政・近隣住民との連絡・説明・調整も CRO の責任の下に行われます。

15.3 BCMS 担当者の業務

BCMS 担当者は、平時は BCP(事業継続計画書)の作成・維持・管理、社内外の関係者への教育・訓練・周知・連絡などを掌握し、サプライヤーからの部品・材料・サービスの安定供給と、インフラの脆弱度と影響度をチェックします。緊急時には、本社対策本部の事務局長に就任し、対策

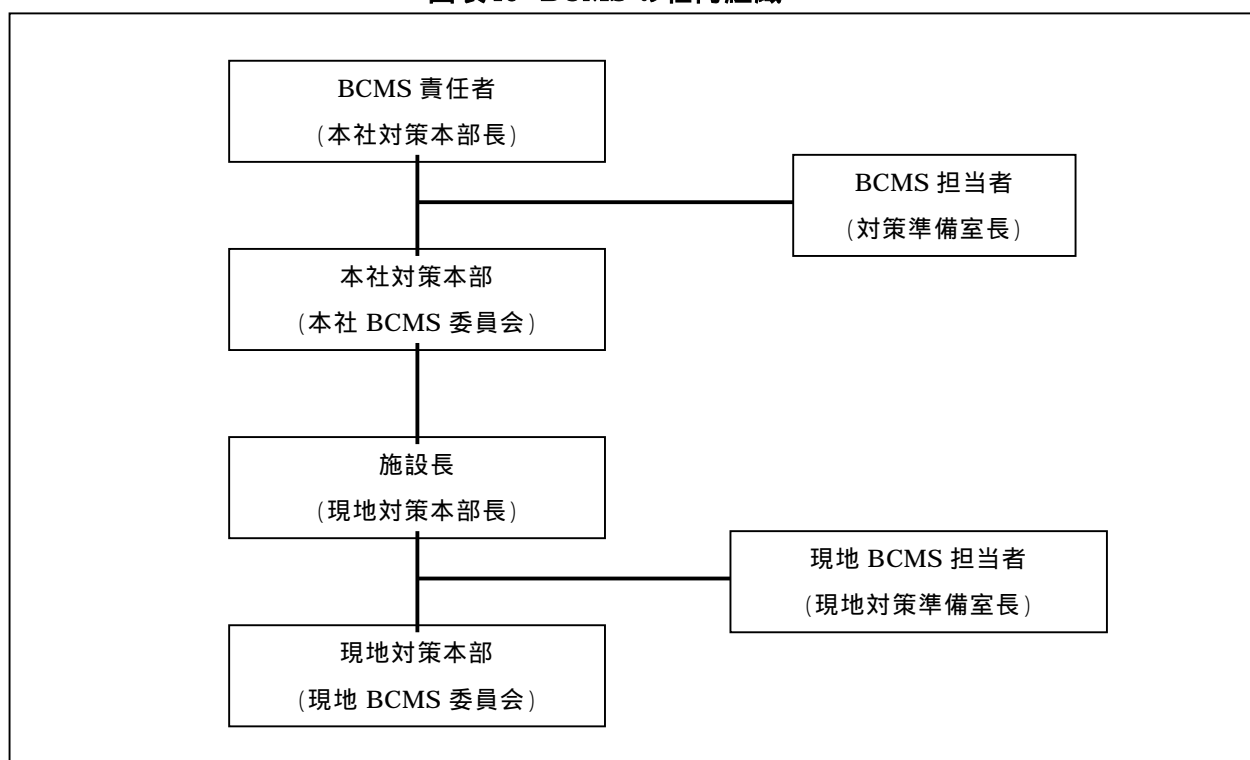
本部長の活動を支援します。

15.4 BCMS の社内組織

BCMS の社内組織は、会社毎に異なりますが、役員会または執行役員を中心に BCMS 委員会を設置する事例が多いようです。この BCMS 委員会の委員は緊急時の本社対策本部の主要メンバーになります。対策本部のその他メンバーは、対策本部長が必要に応じ委嘱します。

各施設の現地対策本部長は施設長が就任し、現地対策本部のメンバーは施設長が決めることとなります。その中には、現地対策本部の事務局長役の現地 BCMS 担当者を含みます。

図表49 BCMS の社内組織



15.4 BCMS 委員会の業務

本資料の各章で行った各種調査は、本社 BCMS 委員会と現地 BCMS 委員会にそれぞれ報告します。各委員会は、調査結果を検討し、判断します。

- 施設毎の災害などの発生頻度
- 施設毎の周辺環境の脆弱度
- 周辺環境を含めた施設毎の脆弱度

- 各建物外部の脆弱度
- 各建物内部の脆弱度
- 施設毎の内部の事故・事件発生頻度
- 施設毎の防災・防火・防犯・セキュリティ力評価
- 施設毎のマネジメントシステムの成熟度
- 施設毎の BCMS の目標
- 施設毎の間接被害を含めた BIA 評価
- 施設毎のインフラの脆弱度と影響度
- 施設毎のサプライチェーンの脆弱度と影響度

本資料では解説していませんが、次の事項についても、各 BCMS 委員会は把握する必要があります。

- 同業他社のディスラプションの発生状況・原因・被害の調査
- 保険契約の確認と評価
- 今までに作成した防火・安全・防災などのマニュアル書の確認と評価
- その他必要な事項

15.5 各対策本部の拡大メンバー

本社および現地の対策本部は必要に応じ次の専門家を拡大メンバーにします。このためには、平時に各専門家と契約を結ぶ必要があります。またこの契約は、毎年見直す必要もあります。なお、専門家は社内にもいます。

- 労働衛生の専門家
- IT システムの専門家
- 各種技術の専門家
- 医師・看護師
- 弁護士・弁理士
- 建築の専門家
- 土木の専門家
- その他(防火の専門家、防災の専門家など)

参考文献

1. 「ISO/PAS22399: Societal security - Guidelines for incident preparedness and operational continuity management」 ISO 2007
2. 「ISO/PAS22399: 緊急事態準備及び業務継続マネジメント」 日本規格協会 2008
3. 「BS25999-1: Business continuity management Part1: Code of practice」 BSI 2006
4. 「BS25999-2: A specification for Business continuity management」 BSI 2007
5. 「BS25777: Information Communications Technology Continuity Management」
6. 「事業継続ガイドライン第1版」 内閣府防災担当 2005
7. 「事業継続計画(BCP)策定ガイドライン」
経済産業省情報政策局情報セキュリティ政策室編、経済産業調査会 2005
8. 「事業継続マネジメントシステムの構築と実務」 黄野吉博編著、共立出版 2008
9. 「BCM(事業継続マネジメント)入門」 小林誠・渡辺研司著、日本規格協会 2008
10. 「事業継続マネジメント 訓練デザインマニュアル」 Tracy K. Gillis 著、林春男監修
NTT 出版 2007
11. 「企業のレジリエンシーと事業継続マネジメント」 Yossi Sheffi 著
渡辺研司・黄野吉博監訳、日刊工業新聞社 2007
12. 「サプライチェーン リスクマネジメント入門」 R. Handfield、K. McCormack 著
東京海上日動リスクコンサルティング訳、日科技連 2010

筆者（役職は、2010年9月15日現在）

黄野吉博	社団法人日本工業技術振興協会 理事
武田吏司	社団法人日本工業技術振興協会 主任研究員
高橋義久	社団法人日本工業技術振興協会 主任研究員
須藤直俊	社団法人日本工業技術振興協会 研究員

事業継続マネジメントシステム(BCMS) 事始め

Version 2.1

2010年9月15日 発表

Copyright 2010

Yoshihiro Kohno, Satoshi Takeda, Yoshihisa Takahashi, Naotoshi Sudo

All rights reserved.

事業継続マネジメントシステム(BCMS)研究会
ykohno@arm.jp

発行者：社団法人日本工業技術振興協会
〒105-0003 東京都港区西新橋 1-5-5
電話：03-3597-7888