

2010 年 9 月 2 日

**事業継続マネジメントシステム(BCMS)事始め
～ 第 4 部 ～**

社団法人日本工業技術振興協会
黄野吉博
武田史司

第 4 部では、予防対策、緊急時対策、継続対策、復旧対策を概説します。

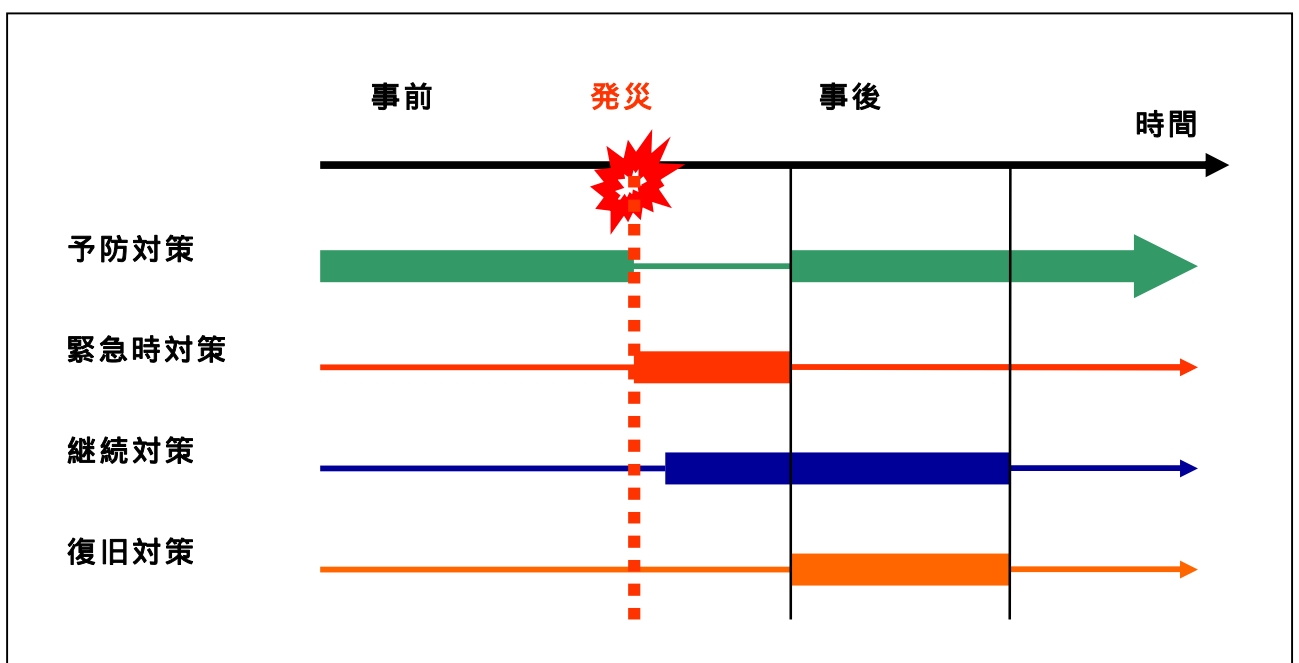
【目次】

第 10 章	予防対策	2
第 11 章	緊急時対策	9
第 12 章	継続対策	14
第 13 章	復旧対策	16

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 4-1 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 4-2 を作成します。この図表 4-2 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 4-2 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	要員	

	復旧費用	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 4-3 を作成します。図表 4-3 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4-3 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 4-3 で検討し、実施した対策を元に図表 4-4 を作成します。図表 4-4 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4-4 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4-5を作成します。図表4-5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4-5 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4-6が参考になります。図表4-6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4-6 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4-7 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 4-8 はその参考です。

図表 4-8 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」としてはいますが、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になります。

- 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ます、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になります。

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となります。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制と、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

ディスラプ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 関係のディスラプションは、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

復旧対策を発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ラプ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