

実効力のある事業継続マネジメントの実現に向けて — 東日本大震災から学ぶ —

To realize the effective Business Continuity Management
— Learning from the 2011 Great East Japan Disaster —

小 川 裕 克

Hirokatsu OGAWA

1. はじめに

2011年3月11日に発生した東日本大震災は、M9.0と過去最大級の地震となった。大津波が発生したこともあり、被害は広域にわたり、多くの人命や家屋が奪われ、道路も寸断された。ガソリンや日常生活用品の調達等に大きな影響を与え、日本経済も大きな打撃を受けることとなった。さらには原発事故が追い打ちをかけ、電力の供給と放射能による影響が全国、さらには海外にまで及ぶこととなった。

地震大国日本においては、このような災害に遭遇したのは初めてではない。近年においても、これに準じるような阪神・淡路大震災や中越地震などが発生している。しかも今後30年以内にかなり高い確率で東海・東南海・南海地震や首都直下型地震¹⁾が起こるものと推定されている。

企業がこのような災害発生に備えて、関係者の身の安全を確保し、重要事業を継続することは、企業の社会的責任の観点からも重要である。中央政府や地方自治体等も、これまで事業継続計画策定の必要性を指摘している。しかしながら、実際に策定していた企業はほんの一部であったようである。しかも今回の東日本大震災に関しては、事業継続計画を策定していた企業においても、「想定外」の事象が多く発生し、これが十分に機能しなかった（もしくは役にたたなかった）ところも多いようだ。

そこで本稿では、まず事業継続計画（BCP）、事業継続マネジメント（BCM）とはどういうものか、特にリスク管理の観点中心に解説し、東日本大震災を踏まえたBCP、BCMのあり方を考察してみたい。

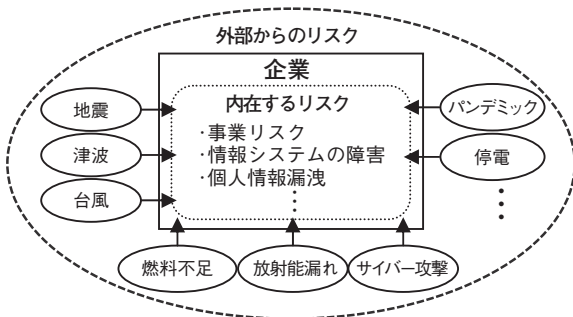
2. BCPとBCM

(1) 企業を取り巻く様々なリスク

私たちは日常様々なリスク（脅威）に取り巻かれている。その代表的なものが台風や地震、火災等により被害を受けるリスクである。特に企業を取り巻くリスクには、企業外部からのリスクと企業自身に内在するリスクがある（図表1）。

外部からのリスクには自然災害等の災害リスクや法律改正・内乱などの政治リスク、景気変動や為替変動・金融危機等の経済リスク、パンデミック（感染症の世界的な流行）などがある。一方、企業に内在するリスクには、事業戦略リスクやオペレーショナル・リスクがある。ここで、オペレーショナル・リスクとは、「内部プロセス・人・システムが不適切であること

図表1. 企業をとりまく様々なリスク



（出所）筆者作成

若しくは機能しないこと、または外生的事象に起因する損失に係わるリスク」を指す²⁾。具体的には、事務処理の誤りや情報システムの障害等により損失を被るリスク、従業員の不正、コンプライアンス体制の不備、自然災害やテロ等により事業活動が中断して被る損失、さらにそれらに伴う企業イメージの低下、訴訟を受けるリスクなどである。

内在するリスクの中には、外部で発生した災害等の影響で二次的に発生し得るリスクもある。たとえば原発事故による停電は工場の稼働やコンピュータシステムの停止等の原因となる可能性がある。

もちろん一般的にリスクといった場合、すべてが企業にとってマイナスであるわけではない。事業戦略リスクや資産運用のリスクは、企業利益の源泉である。

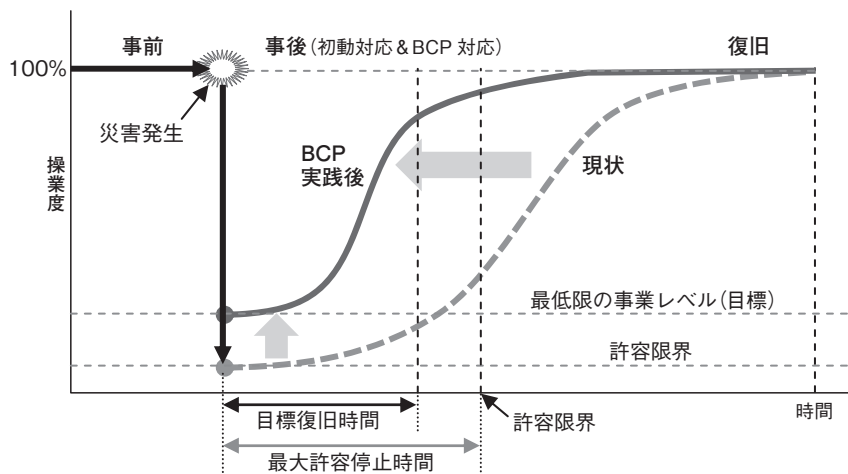
(2) BCPとは

企業にとって、そのリスクが現実のものとなった場合、企業に甚大な損害を及ぼす可能性のあるものも多い。事業継続計画（BCP：Business Continuity Plan）は、企業が災害等の緊急事態に見舞われたとき、これに素早く対応し、重要事業の継続もしくは早期復旧を可能にするための計画書である。BCPは経営戦略の一環としての基本方針と長期的計画（継続戦略）、緊急時における事業継続のための行動計画（継続計画）、そして危機事象発生時に備えて開発、編成、維持されている手順及び情報を文書化した事業継続の成果物から成る³⁾。

図表2はBCP（行動計画）の概念を表したものである。災害発生時にはまず最低限の事業レベルを確保できること、そしてそのレベルをなるべく高くすることが重要である。停止してしまった事業は、BCPを発動することにより、目標復旧時間までに復旧させることを目的とする。実際に災害が発生した場合、①まず事態を把握し、関係者の安全確保と安否確認を行う、②BCPを発動する、③機能停止した重要事業の再開のための対応を行う（再開に時間を要するものは代替手段を使う）、④その後順次平時の業務運用へ切り替える、という順序で実施する。

なおコンティンジェンシープランは災害等の緊急事態発生による被害や損失を最小限にとどめるための対応策や行動手順をいうが、BCPはこれらも含めた事業の継続と復旧に重点が置かれている点に違いがある。

図表2. 事業継続計画（BCP）の概念



（出所）内閣府（一部筆者加筆）

(3) BCP と BCM

BCPは、単に策定しただけでは、危機発生時に必ずしもうまく機能しない。BCPをビジネス環境の変化に適応させていくと共に、様々な準備と訓練を行い、危機発生時に確実に機能するようにマネジメントしていくことが必要である。これをBCM（Business Continuity Management：事業継続管理）という。平時から備えておくことにより、重要事業の継続、もしくは短期間での再開が可能となり、自社の顧客の減少やマーケットシェアの低下、レピュテーションの低下などを防ぐことができる。

ところでBCP、BCMの重要性が世界的に注目されるようになったのは、2001年9月11日の米国で発生した同時多発テロである。この同時多発テロによりウォール街近辺の企業、特に多くの金融機関は大打撃を受けた。そういう中で、BCP、BCMへの

対応を行っていた金融機関はニュージャージー州等の代替オフィスに拠点を移し、素早くビジネスを立ち上げることができた。そして、オフィスは近隣に集中させないことや、代替オフィスを確保しても、従業員がそこに出勤できなければ業務が機能しないこと、複数の通信キャリアを使うこと、コンピュータシステムを駆使することにより、できるだけ業務のSTP⁴⁾化を推進することなどが重要であると認識するに至った。

なおBCMについては、国内においても、第三者認証制度として、日本情報処理開発協会(JIPDEC)によるBCMS適合性評価制度⁵⁾が2010年3月よりスタートしている。また英国規格BS25999が2012年中頃に国際規格ISO22301として採用される予定となっている⁶⁾。

(4) BCP, BCMと内部統制

企業を取り巻くリスク(脅威)に対応できるようBCMを効果的に進めるためには、経営者自ら率先して社内態勢の整備を行っていく必要がある。一方、リスクへの対応という点では、企業の内部統制の構築・整備も重要である。そして内部統制においてもリスクの洗い出しやその評価、そしてリスクへの対応の一環で社内態勢の整備を行う。それではBCP, BCMと内部統制等とはどういう関係にあるのだろうか。

内部統制に関しては、1992年に米国のトレッドウェイ委員会組織委員会(COSO: the Committee of Sponsoring Organization of the Treadway Commission)が公表した内部統制のフレームワーク(COSOモデル)が有名である。COSOは内部統制を「業務の有効性・効率性、財務諸表の信頼性、関連法規の遵守の3つの目的を達成するために、合理的な保証を提供することを意図した、取締役会、経営者およびそのほかの職員によって遂行される1つのプロセスである」と定義している。ここでいう業務の有効性とは事業活動や業務の目的が達成された程度をいい、業務の効率性とは、「組織が目的を達成しようとする際に、時間、人員、コスト等の組織内外の資源が合理的に使用される程度」をいう。2002年7月に施行された米国企業改革法(SOX法: サーベンス・オクスリー法)における内部統制の構築・整備においては、実質的にCOSOモデルがベースとなっている。同様に日本でも2007年9月に金融商品取引法が施行され、上場会社等は内部統制の構築・整備が必要となった(いわゆるJ-SOX法)。J-SOX法への対応においても、企業会計審議会はCOSOモデルをベースにしたフレームワーク採用している⁷⁾。ただしSOX法、J-SOX法共に、企業の粉飾決算等への対応を主目的にしたもので、「財務報告の信頼性確保」に焦点を当てている。

これに対して、BCP, BCMは災害等の脅威が現実のものとなった場合への対応を目的としている。BCP, BCMは内部統制の目的の一つである「業務の有効性確保」と関係していると考えられるが、基本的に重要事業が継続できなくなるような緊急時の対応である。内部統制の構築においても、システム障害等、緊急時の対応も含まれるが、主に企業の平時の業務の適正性を確保するための統制を主眼にしたものであると

いえよう。またBCP、BCMにおける脅威の多くは外部にある場合も多い。たとえ自社の業務プロセスに問題がなくても、部品の仕入れ先が被害にあったために、自社の生産ラインを停止せざるを得ない場合への対応等も含まれる。自社への送電が停止してしまった場合も同様である。

なお「企業内容等の開示に関する内閣府令」⁸⁾は、有価証券報告書に「事業等のリスク」を記載することを要求している。「事業等のリスク」とは「企業が将来にわたって事業活動を継続するとの前提に重要な疑義を生じさせるような事象又は状況その他、企業経営に重要な影響を及ぼす事象」を指す。BCP、BCMはこの内閣府令と強く関連しているといえよう。

COSOは2004年9月に、企業の各種リスクへ対応すべきフレームワークとして、ERM (Enterprise Risk Management) を公表した。ERMは、COSOモデルを発展させたものである。リスクを業務遂行上のリスクのみならず、事業活動を取り巻く不確実な要素(外的要因)や事業戦略といったものを含めた広い意味で捉えて、全社的なリスクを管理する枠組みである。

具体的には、目的(目標)に、戦略を追加すると共に、財務報告に非財務報告も加えて報告とした。そしてERMを「事業目的の達成に関する合理的な保証を与えるために事業体に影響を及ぼす発生可能な事象を識別し、事業体のリスク選好に応じてリスクの管理が実施できるよう設計された、一つのプロセス」と定義している。ERMから見ると、BCMはその一部と理解することができよう。

会社法も、会社全体の内部統制(会社の業務の適正を確保する体制)⁹⁾の整備を要求している。そして業務の適正性確保のためには、「損失の危険の管理に関する規程その他の体制」を整備する必要がある¹⁰⁾。会社法は整備すべき内部統制の内容を明確かつ具体的に示しているわけではないが、BCMは「損失の危険の管理」のための対策の一環と理解できる。さらに会社法は取締役(執行役)に対して、「善良なる管理者の注意をもって業務執行を行う義務(善管注意義務)」¹¹⁾と、「会社のために忠実に職務を遂行する義務(忠実義務)」¹²⁾を要求している。特に善管注意義務に関しては、結果予見義務と結果回避義務が考えられるが、東海地震等が高い確率で発生すると予想されている以上、脅威が実際に起こってしまった結果、どういう事態が生じるかを予見し、どう回避策をとるべきか、BCP、BCMが必要であると解釈できよう。

(5) BCP策定のこれまでの現状

日本は自然災害に見舞われるケースが多いにも関わらず、BCPを策定している企業は少ないという現状がある。KPMG ビジネスアシュアランスが2006年4、5月に実施した調査結果¹³⁾によると、米国ではBCP策定済み企業が62%であるのに対し、日本では15%に留まっている。また「策定していない」は米国が4%に対して日本は51%、「策定中」は米国、日本共に34%となっている。日本のBCPに対する対応の遅れ、

認識の低さがわかる。

一方帝国データバンクが2011年4月に行った「BCP（事業継続計画）についての企業の意識調査」¹⁴⁾によると、東日本大震災の前までに「BCPを策定していた」企業は7.8%（大企業21.5%，中小企業6.5%），「BCPを知っていたが策定していなかった」企業は29.2%（大企業31.4%，中小企業29.1%）となっている。また「BCPを知らなかった」企業は47.7%（大企業25.9%，中小企業49.7%）と、半数近くに達している。

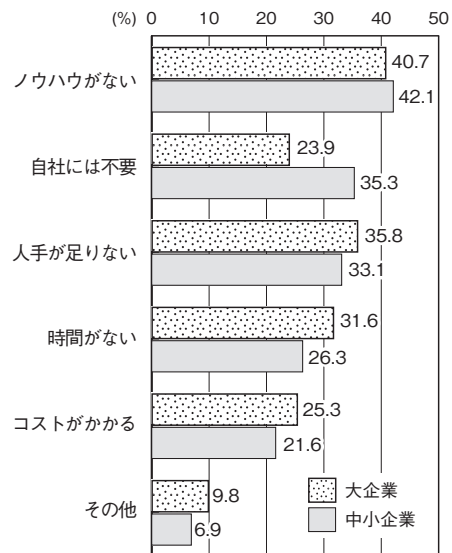
図表3は「BCPを知っていたが、策定していなかった」理由をグラフ化したものである。「ノウハウがない」が一番多く、大企業40.7%，中小企業42.1%となっている。

また「自社には不要」は大企業23.9%，中小企業35.3%と中小企業の方が10ポイント以上高くなっている。これまでも政府をはじめ関係機関がBCP策定に関する啓蒙を積極的に行っている。例えば中小企業庁は「中小企業BCP策定運用指針」においてBCPの策定の方法をアドバイスしており、東日本大震災以降は、自治体やコンサルティング企業等がBCPセミナーを多数開催している。東京都のように中小企業等を対象に、無料のBCP策定支援コンサルティングを行っている自治体もある。今後は「ノウハウがない」をBCP未策定の理由とするわけにはいなくなるだろう。

「自社には不要」も同様である。今回の大震災で発生した「想定外」のできごとへの対応も必要であろうし、中小企業といえども、大半はサプライチェーンという鎖に組み込まれているという現実を考える必要がある。

ビジネスが仕入れ先や顧客等との強い鎖で結ばれている以上、自社だけではなく、仕入れ先や顧客もBCPを策定することが重要である。東京都が2009年度に都内企業を対象に実施したアンケート¹⁵⁾によると、「取引先からBCP策定の要請を受けた」企業は15.6%にとどまっているが、「今後はこの要請を受けると予想している」企業は52.1%と半数以上に達している。東日本大震災の発生、および東海地震等の発生確率が高いこともあり、親会社や取引先、金融機関からのBCP策定要請は確実に増加するものと思われる。

図表3. 「BCPを知っていたが、策定していなかった」理由



(出所) 帝国データバンク

3. 東日本大震災から学ぶべきもの

東日本大震災において、「想定外」の事象が数多く発生してしまったためもあり、BCPが必ずしもうまく機能しなかった企業も多いようだ。震災発生時の初期対応や危機事象の見直しなど、BCP、BCMの抜本的な見直しが急務である¹⁶⁾。

(1) 自社の社会的な役割と存在意義を認識すること

大震災のような未曾有の危機的状況発生に備えて、各企業はBCMに真剣に取り組む必要がある。BCMを組織に浸透させるためには、まず経営トップがその重要性を認識し、リーダーシップを持って推進することが大切である。災害はいつどのような形で発生するかわからない。発生時の迅速な行動と、事業継続に向けた対応をとる必要がある。そのために重要なことは、経営者はもちろん、全社員が自社の社会的な役割と存在意義を認識し、日頃から災害等への対応・訓練に真剣に取り組む必要がある。

(2) 危機発生時の初期対応の見直し

誰がBCPを発動するのが曖昧で、BCPが効果的に発動できなかった企業が多かったという。また震災発生時に社員や家族の安否確認でさえうまく取れなかった企業も多いという。

改めてBCP発動のルールや手順を見直し、整備する必要がある。職場の安全確認や連絡体制、安否確認等の連絡手段を見直し、BCP発動の責任者を明確にする。また、情報の伝達収集は迅速かつ漏れないような体制を構築すること、また各職場の責任者が不在の場合でも柔軟かつ迅速に行動できるようにしておく。

BCPの発動およびその後の行動は、基本的にBCPマニュアルに沿って行うことになる。しかし危機事象はいつどのような形で起こるかわからないし、私たちも職場にいて被災するとは限らない。マニュアルがなくとも迅速かつ臨機応変に動けるように、その内容を全役職員に徹底しておく必要がある。BCPマニュアルはコンパクトにし、現場の情報や判断を優先しながら、臨機応変に対応することが重要であろう¹⁷⁾。

(3) 「想定外」の危機事象をなくすために

① 危機事象を「想定内」に閉じ込めない

東日本大震災では多くの想定外の出来事が発生した。地震の大きさは、これまでの予想値M7.5～8.6に比べてM9.0と、はるかに大きいものとなり、津波も15m程度と、10m規模の堤防や防波堤を軽々越え、ハザードマップの津波浸水地域をはるかに越えてしまった。携帯電話の輻輳や利用制限も想定外だったが、想定外の原子力発電所の事故が起こり、関東地方等も含めた広範囲な電力不足が長時間にわたるという想定外の事態が発生してしまった。

ところがこれまでのBCPの多くは、「想定内」の危機事象のみを対象とし、特に計画が立てやすいように、数々の制約条件をつけて、楽観的なシナリオに基づくものが多かったようだ。これでは今回のような大震災が発生したとき、せっかく策定したBCPも役にたつわけがない。「想定内」の対策は、それ以上の危機事象、いわゆる「想定外」に対する思考を停止してしまうという意見も多い。BCP策定にあたっては、危機事象を「想定内」に閉じ込めないことが肝要である。

② 危機事象は結果事象を中心に分析する

通常BCP策定にあたっては、BCPの適用範囲や事業計画の目的の明確化、事業インパクト分析（BIA：Business Impact Analysis）の実施、リスク評価、事業継続戦略の決定という手順を踏む。この中で、BIAではまず発生しうる危機事象を洗い出し、これに対する、事業遂行上の脆弱性やお互いの依存関係を分析する。次に事業継続にとって重要な要素（製品やサービスをサポートする業務プロセス）を特定する。そして危機が現実のものとなった場合、主要な製品製造工程やサービス、ステークホルダーに与える影響度が時間と共にどう変化するか、最大許容停止時間や損失額などを算出し、目標復旧時間を決める。

これまで、BCPの多くは危機事象として「災害の原因」、つまり原因事象（災害シナリオ）をもとに作成されていたようだ。東日本大震災においては、まず想定外の巨大地震（一次危機事象）が発生し、この地震に伴って想定外の巨大津波（二次危機事象）が発生、さらには想定外の道路やサプライチェーンの寸断（三次危機事象）が続いた。また巨大地震と巨大津波の両者により福島第一原発事故が発生し、この原発事故が放射能汚染、計画停電などを引き起こすこととなった。

このように原因事象を基本とすると、個別災害ごとに対策を考えることになり、複合的な原因に対処できないばかりか、想定外の事象への対策は難しくなる。それよりも災害の結果、つまり結果事象（被災シナリオ）を中心に分析する方が対策を立てやすい。結果事象とは、例えば社員の帰宅・出社困難、自社オフィス使用不可能、情報システム使用不可、電力不足、重要部品の調達困難、物資の輸送困難などである。

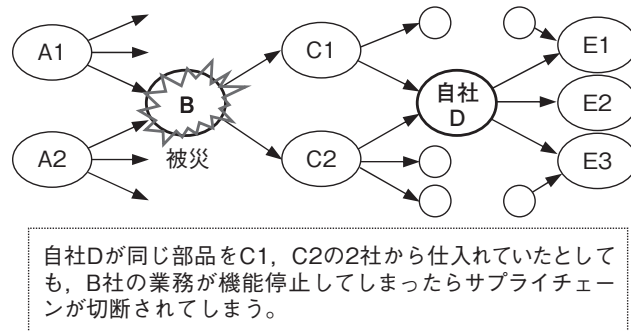
（4）事業継続のための対策の見直し

① 取引先等とのBCPの整合性確保、サプライチェーンの確保

BCP策定にあたっては、想定シナリオと共に重要事業（優先業務）の特定と目標復旧時間の設定が重要であるが、取引先のBCPと自社のBCPとが、互いに整合性が取れていない可能性もある。お互いに整合性がとれていないと、取引先が供給する部品やサービスが自社にとって優先度が高くても、取引先にとっては低い可能性がある。確認の上、整合性をとっておく必要がある。もちろん重要な事業に関連した業務の一部を外部委託先にアウトソースしている場合も同様である。

2007年7月に発生した中越沖地震(M6.8, 震度6強)では自動車部品メーカーR社が被災し、サプライチェーンが途中で切れてしまった。幸い取引先の支援等により、半月ほどで全ラインの生産が復旧したが、メーカー各社はサプライチェーン確保の重要性を認識したという。ところが

図表4. サプライチェーン上の問題点



(出所) 筆者作成

今回の大震災においてもサプライチェーンが切れてしまい、多くのメーカーが生産を一時停止するはめに陥ってしまった。その原因として挙げられているのが図表4のようなケースである。サプライチェーンは自社の直前・直後のみならず、サプライチェーン全体の構成がどうなっているか、脆弱性はどこにあるのかをグローバルレベルで分析し対策をとる必要性がある。

② 自社設備・情報システム等の確認と補強

停電による重要な業務が停止しないように自家用発電機を備えている企業も多い。しかしながら、非常用電源や自家用発電機がうまく機能しない問題も発生したという。しかも今後は長時間にわたって電力供給がストップする可能性もある。数日間対応できる発電機の準備も含めた自社の施設や機器の確認と補強が必要となろう。そしてこれらが危機発生時に必ず機能するよう定期的に稼働テストを行うことも必要である。津波の被害を受ける恐れがある場合、地下設備が浸水する可能性もあるのでその点も確認する必要がある。

一方都内においては、社員が帰宅できないような状況が生じてしまった。このような状況が生じた場合のための安全なスペースや会議室等も確保しておく必要がある。

金融機関中心に、業務継続のための代替オフィスを用意しているところも多い。しかしながらこれまでのBCPは、主としてテロや停電等を想定していたケースが多かったようだ。そのため、代替オフィスも、現在使用しているオフィスビルのみが使えなくなるケースを想定して選定されたものも多いものと推測される。

今回の大震災を機に、改めて代替オフィスの立地条件を検証しておく必要がある。まず代替オフィスは広域災害に対応できるよう遠隔地に設置し、液状化リスクや津波、河川の氾濫、停電・通信障害などのリスクを考慮する。オフィスビルは耐震性などが考慮され、交通機関が機能していない場合でも社員がオフィスへ出勤できる環境にあることが条件となる。そして一番良いのは、代替オフィスが日常業務で使われて

いることである。

③ 書類等のペーパーレス化とバックアップ化の推進、インターネット等の活用

東日本大震災では、津波により重要な書類が流されてしまったケースも多く発生した。また原発事故による放射能漏れにより、強制的な避難区域が設定され、その区域内に入れなくなり、重要なデータや書類、さらには自社の情報システムを利用することもできない状態が発生してしまった。

対策としては、まず紙による書類の保存は極力少なくし、電子化することである。電子化されたデータは二重化し、一つは遠隔地に格納するなどの手立てを講じることにより、万が一の場合、インターネット等を使ってデータにアクセスすることを可能にする。

今回の大震災では、携帯電話や固定電話等の通信インフラも大きな被害を受けた。一部エリアを除き、4月末までにはほぼ復旧したものの、その間、通信輻輳が発生したり、通信規制が行われたりした。

そういう中で、電子メールやTwitter, Facebookなどが有効に利用されたという。またAmazon.co.jpの「ほしい物リスト」などのように、被災者の立場から必要な物を適切に届けられる仕組みも多く使われた。寸断されてしまっている道路については、「Honda インターナビ」(自動車通行実績情報マップ)を利用することにより、前日時点での通行可能な道路をインターネットで確認でき、大きな反響を呼んだという。

しかしながらインターネットは被災しなかった地域では有用であったものの、被災者は必ずしも恩恵を受けることができなかったようである。手動のラジオは例外として、携帯電話等の充電の問題など、テレビを含めた情報機器は、停電により利用できない状況が多く発生した。またインターネット上の情報には問題があるものもあり、情報の品質管理がクローズアップされた¹⁸⁾。さらには情報機器を使いこなせない等のデジタルデバイドの問題も指摘されている。

このように色々な課題や問題があるものの、今回の大震災では、インターネット上で支援・復旧のための様々な新機能が提供されてきているのも事実である。しかも今後はテレビ放送などのマスメディアとインターネットとの融合が進むと予測されている。冗長性を持たせた通信ラインの確保も含めて、BCPにおいてインターネット等をどう活用するかが重要な鍵となると考えられる。

④ 事業継続のための訓練の実施

危機事象が発生した場合、そのときの状況に応じて的確な対応をとるためには、単にBCPやマニュアルを作成するのみならず、BCMの一環で訓練を繰り返すことが必要である。たとえ安否確認といえども訓練をしていないといざという時にスムーズに進めることができない。

訓練は、通常業務の合間をぬって行うことが多いためか、想定シナリオも甘くなりやすい。訓練参加者の多くは、「想定シナリオが実際に発生し得る」という危機意識が少ないように思える。今回の大震災を踏まえて、想定シナリオの見直しと共に危機意識の徹底も必要であろう。

⑤ 情報の迅速な開示

企業で不祥事等が発生した場合、不十分な情報開示が問題になることが多い。企業が災害等の危機的事象に合ったときも同様である。自社が被災してから現在までの状況、今後どう対応しようとしているかを顧客や取引先、従業員等のステークホルダーに迅速に開示していく必要がある。情報開示を的確かつ迅速に行わない、ステークホルダーから多くの不信感を買うことになり、多くの取引を失う可能性がある。

⑥ 企業グループを越えた協力関係の構築、標準化の推進

今回、自社の業務プロセスが震災により停止してしまったが、同業他社にその機能を代替してもらうことにより危機を乗り越え、自社の業務プロセスが回復した時点で元に戻してもらったケースも報告されている。普段は競合している同業者でも危機発生時は互いに協力できる体制作りも必要である。

またペットボトルのキャップのように、ある部品の代替品を普段取引のない別の企業から調達しようとしたが、形状が若干異なっていたため、これを使うことができなかった例もある。自社の強みや独自性とのバランスを取る必要もあるが、部品やサービス等は、できるだけ共通化および標準化する努力も必要である。

広範囲かつ大きな災害に見舞われたときは、道路や電力等のインフラが麻痺してしまう可能性が高い。今回の大震災では、インフラが麻痺した状況で、各企業等がバラバラに支援活動を行ったため、食糧や燃料等の支援物資を被災地に効率的に輸送できなかったという指摘が出ている。企業グループを越えた、場合によっては業界横断的な支援活動を積極的に行う必要があるものと考えられる。そのためには、各企業は政府や自治体と連携した対応が必要であろう。もちろん業界横断的な活動を目指したがために、緊急を要する支援活動に遅れが出てしまっただけでは意味がない。

4. IT-BCP への対応

(1) IT-BCP とは何か

今や情報技術 (IT) は、多くの企業にとって、事業遂行のためにはなくてはならない存在となっている。BCPの策定にあたっては、業務とITとの整合性を図りながら進める必要がある。このITに関する事業継続計画を通常IT-BCPと呼ぶ。

IT-BCPの策定にあたっては、重要事業と情報システム等の対応づけ、データベ-

ス等の配置状況の確認、システムの想定復旧時間の設定、IT部門の緊急時の行動計画書やバックアップシステムの立ち上げ手順書等の整備などを行う。ユーザ部署との情報連携も重要である。また重要事業で利用する情報システムは、その業務の目標復旧時間（RTO：Recovery Time Objective）までに利用できる状態になるようにしなければならない。そのためにも、情報システムの運用に関する各種契約内容、特にSLA¹⁹⁾の確認が必要となる。

IT-BCPをJ-SOX法対応におけるIT統制との対比で分類してみたのが図表5である。IT-BCPにおいては、緊急時の行動計画が重要であるが、J-SOX法におけるIT統制においては、システム障害等の緊急時の対応は通常IT全般統制に含まれる。IT全社BCPは、企業としてのBCPの基本方針等や全体計画のうち、特にITに関するものである。IT全般BCPは、BCP策定の一環で洗い出された重要な事業やサプライチェーンに関して、これらを支えるIT基盤に関するBCPである。つまりサーバーや通信ネットワーク等のIT基盤の運用継続性確保、もしくは早期復旧により、重要事業の継続性を確保しようとするものである。IT業務BCPは業務プロセスと密接に関係し、アプリケーションシステムの運用継続性確保、重要データの二重化、他のサーバーでの業務処理継続などがこれにあたる。

図表5. IT-BCPの分類（J-SOX法におけるIT統制との対比）

	IT-BCP	J-SOX法におけるIT統制
緊 急 時	緊急時のITに関する行動計画	（通常IT全般統制に含まれる）
全社レベル	IT全社BCP 全社的なBCPに関する基本方針や全体計画のうちITに関するBCP	IT全社統制 主に全社的なITに関する計画と組織に関する統制
IT 全 般	IT全般BCP サーバーやネットワーク等のIT基盤に関するBCP	IT全般統制 プログラム開発やIT基盤に関する統制
業務レベル	IT業務BCP 個別の業務プロセスの継続のためのアプリケーションシステムに関するBCP	IT業務処理統制 ITを利用して業務プロセスに組込まれた統制

（出所）筆者作成

（2）IT全社BCP

IT全社BCPは、IT-BCPに関する全社レベルの基本方針や投資計画を策定することである。危機的事象は明日にでも発生するかも知れない。すぐ手を打つべき短期的な方針と長期的な方針に分けて考える。短期的な方針は安否確認や社員・家族の安全

確保等におけるIT利用に関するもの、現在利用している全社IT利用環境等に関する短期的な見直しなどが考えられる。長期的な方針は自社の戦略そのものに組み込まれる。たとえば、データセンター利用に関する方針や、クラウドコンピューティングなども含めたIT関連のアウトソースの方針等、長期投資計画などがこれにあたる。

(3) IT全般BCP

IT全般BCPとは、サーバーやネットワーク等のIT基盤の全体構成を見直すことにより、事業の継続性を確保することである。

① サーバルーム等の強化

既に多くの企業は、情報システムのダウンに備えてバックアップサーバーの準備等、サーバーの二重化（レプリケーション化）やネットワーク等の二重化を実施しているものと考えられる。しかしサーバルームがオフィスと同じサイト内に存在するときは多くのリスクがつきまとう。電力供給がストップすればサーバーも停止・故障してしまう可能性があり、業務継続不可能となる。通常のUPS（Uninterruptible Power Supply：無停電電源装置）のみならず、数日間稼働可能な非常用電源の導入の検討等が必要である。

② 重要サーバーのデータセンターでの運用

サーバルームがオフィスもしくは工場と同じ施設内で運用されている場合、その施設が被災してしまった場合には情報システムも被害を受ける可能性が極めて高い。このようなリスクを避けるためには、停電対策や耐震・免震対策が施され、かつセキュリティ管理レベルの高いデータセンターで運用管理されるべきである。データセンターは自社所有の必要はない。ハウジングサービス²⁰⁾やIT運用の外部委託サービスを提供しているITベンダーを利用するとコストセーブが可能となる。

しかしながら、東日本大震災においては、最も堅牢な設備の一つであると思いついていた原子力発電所が破壊されてしまった。データセンターといえども安全とはいえない。データセンター選択の要件としては正副データセンターでの運用、台風や地震・津波による被害が少ない等の立地条件、電源や空調、免震構造かつセキュリティ対策等のとれたセンター内の設備が挙げられよう。また正と副のデータセンターは計画停電等のリスク分散の意味で互いに別の地域に設置されていることが望ましい。

大手金融機関の場合、正副データセンターを利用しているケースが多いと思われるが、他の業種等では、データセンターは一つだけというところが多いという。コストベネフィットも考慮しながら、自社に最適な利用形態、バックアップ対策を講じる必要があるだろう。

③ PC等、オフィス内IT環境の整備

オフィス内IT環境の整備も重要である。PCやLAN等については、停電等に対応するために、非常用電源の確保を考える。またオフィスが被災等により使用不可となった時のための対応として、データ等はサーバー側で集中管理し、代替オフィスからの利用も可能にする。またインターネットを活用できれば、安否確認のみならず、業務の継続性確保も容易になる。例えば、自宅等のオフィス外からのリモートアクセス環境を充実させることにより、情報システムの可用性が高まる。さらに災害時の備えとして無線通信技術の活用も有効である²¹⁾。

④ 仮想化技術やクラウドコンピューティング等の活用

仮想化技術の利用は、情報システム構築において、今や必須条件といっても過言ではない。仮想化技術を使えば、サーバーの統合や動的変更を柔軟に行うことができる。これによりハードウェアとしてのサーバー台数の削減やアプリケーションの再配置が容易になり、サーバー障害が発生しても短時間で復旧可能になる。クライアントPCも仮想化技術を利用するか、シンクライアント (Thin Client) 化²²⁾できれば、IT環境の設定・変更が比較的容易になる。

一方インターネットを利用したクラウドコンピューティング (パブリッククラウド。以降、クラウドと省略する) の活用も徐々に加速してきている。クラウドを全面活用できれば自社でデータセンターを所有することもなく、またオフィスの設置場所としての物理的制約も緩和され、オフィス外からの業務を継続することも可能になる。

ただしクラウドも制約や課題がある。クラウドを提供するITベンダーのデータセンターが海外にある場合、その国の法制面での制約を受ける。データセンター自身の立地状況や、サービス停止時の損害賠償責任、データのバックアップや、システム障害時における障害箇所の特定や復旧など、SLAの確認も必要である。

またクラウドは必ずしもミッションクリティカルなシステムに適さないケースも多いようだ。セキュリティ上の不安や性能面、運用の柔軟性の確保上等の課題が考えられるからである。オンプレミス²³⁾にするかクラウドにするか、または両者の組み合わせにするか、どういう仕組みが自社にとって最適かを検討する必要がある²⁴⁾。もっとも最近ではデータセンターを日本国内に設置し、インターネットではなく専用線を使ってハードウェア環境を提供するサービス (プライベートクラウドの一種) も出てきている。クラウドの可用性は徐々に高まってきているといえる。

(4) IT業務BCP

重要事業を支える情報システムが複雑化してしまっているケースも多いように思われる。例えば同一機能を提供しているシステムが複数存在したり、同じデータが複数のシステムに散在、もしくはどこでどのデータが使われているのか不明瞭の状態と

なっている場合である。このような状況では、ITコストの増加を招くと共に、効率的なIT運用ができず、いざというときにIT-BCPが機能しない可能性もある。まず情報システムのシステム相互間の関係や機能を整理すると共に、重要事業を遂行する上で必要なデータの流れを分析し、無駄を排除していく必要がある。その上で、災害等に備えたシステムの冗長性を高めていく。

また業務フローの中に、手作業や人による判断が複雑に入り込んでしまっていると、事務ミスも発生し易くなると共に、担当外の者が当該業務を代替できない場合もあり得る。ITを活用して、できるだけ業務のSTP (Straight Through Processing) 化を図るべきである²⁵⁾。

5. 経営革新のための戦略的BCP, BCMの推進

企業経営者がBCP, BCMをどう捉えるかにより、その対応は大きく異なってくる。売上・利益に貢献しないが、やむを得ないコストだと認識すると、後ろ向きのBCP, BCMとなり、中途半端なものとなってしまいうだろう。逆にBCP, BCMを経営革新のチャンスだと戦略的に捉えることにより企業競争力の強化につなげることができる。

たとえば社内の業務プロセスや商品群を見た場合、重複や無駄が多い場合が見受けられる。BPR (ビジネスプロセス・リエンジニアリング) により改革しようとしても、コストがかかる上に、直接影響を受ける現場は、必ずしも積極的に推進しようとはしない。しかしながら企業の社会的責任、顧客からの信頼性獲得、競争力強化を目的にBCP・BCMとBPRを併せて推進することにより、経営革新につなげることも可能となる。またトヨタのように、東日本大震災や円高、欧州債務危機などに対応するため、主力車ごとに部品の設計を世界統一し、コストセーブと先進デザインの両者を追求する動きも出ている。スマートフォンやタブレット端末も日々進化している。安否確認での利用はもちろん企業として様々な用途に活用できる可能性がある。

一方で、今や中小企業といえどもグローバルなレベルでの戦いを強いられている。BCPはグローバルレベルでの工場・オフィスの配置、さらには商流の見直しのチャンスにもなる。そして中小企業同士が力を併せてBCPに対応すると共に、競争力強化のための合従連衡のチャンスでもある。野村総合研究所の藤野氏らは、SCM (サプライチェーンマネジメント) において、「バーチャル・デュアル・ソーシング」を提案している。災害対応の「デュアル・ソーシング」だと、生産や調達の仕組みを二重化しておくことになるため、コスト増につながる。バーチャル・デュアル・ソーシングは仮想的な資源調達の二重化により、あらかじめ定められた許容期間以内で機能を復旧できる仕組みであり、少ない費用で被害を最小限に食い止めようという考え方である。

このように、BCPを経営革新のチャンスとして捉え、戦略的BCPを推進することが、今後の企業の存亡を左右することになるかも知れない。

6. おわりに

BCP, BCMは今回の東日本大震災により、その重要性が強く認識されたことと思える。しかしながら、BCP, BCMは国内の地震等の自然災害だけへの対応ではない。企業活動が益々グローバル化している中、タイにおける水害や中東における紛争、世界各地で発生しているテロなど、脅威もグローバル化してきている。BCP, BCMはこれらの脅威に対する備えである。しかも欧州危機のように、単なる景気変動ではない経済危機も企業にとって大きな脅威となってきた。これらの脅威が現実化したとすのために、企業はどう備え、事業を継続させていくか、大企業はもちろん中小企業もグローバルな視野での経営、そして経営者と社員が一丸となった「革新へのチャレンジ」が必要とされているといえよう。

注

- 1) 政府地震調査委員会によると、2012年1月1日での算定では、今後30年以内の発生確率は東海地震(M8程度)が88%、東南海地震(M8.1前後)が70%程度、南海地震(M8.4前後)が60%となっている。また東京大学地震研究所が2012年1月に発表した予測によると、首都直下型地震の発生確率は、4年以内で50%以下、30年以内では83%以下という。
- 2) パーゼル銀行監督委員会の定義による。
- 3) BSI(英国規格協会)が策定した「PAS 56」(Guide to Business Continuity Management)の定義による。
- 4) STP(Straight Through Processing)とは、社内外の一連の業務の流れが、人手を介さず、全て電子的なネットワークを通じて行われることをいう。
- 5) BCMSはBusiness Continuity Management System(事業継続マネジメントシステム)の略。
- 6) ITに関する事業継続(IT-BCP)に関するガイドラインとして、ISO27031がある。これはITの観点から事業継続を深く掘り下げたものであり、BCPガイドラインを補完するものである。
- 7) 「財務報告に係る内部統制の評価及び監査の基準のあり方について」(企業会計審議会内部統制部会)から抜粋した。この定義は米国COSOの定義にはほぼ準じている。企業会計審議会は、内部統制を、「基本的に、業務の有効性及び効率性、財務報告の信頼性、事業活動に関わる法令等の遵守並びに資産の保全の4つの目的が達成されているとの合理的な保証を得るために、業務に組み込まれ、組織内のすべての者によって遂行されるプロセス」と定義している。
- 8) 根拠法は金融商品取引法24条(有価証券報告書の提出)。
- 9) 会社法348条3項4号、362条4項6号、416条1項1号。

- 10) 会社法施行規則100条1項2号。
- 11) 会社法330条(402条)によると、会社と取締役(執行役)の間には委任契約が存在し、会社が委任者、取締役(執行役)が受任者という関係になる。そして受任者には善管注意義務がある(民法644条)。
- 12) 会社法355条(419条)。
- 13) 調査は2006年4月12日～5月8日、上場企業、店頭公開企業など4,452社を対象に調査、解答数は274社(有効回答率6.2%)。
- 14) 2011年4月18日～30日、TDB景気動向調査登録企業2万2,240社に対してインターネットにより調査を実施。有効回答企業数1万769社(中小企業基本法上の区分に基づく大企業908社、中小企業9,861社、回答率48.4%)。
- 15) 回答社数は約2,000社。
- 16) 参考までに前述の帝国データバンクによる調査結果によると、全企業10,769社のうち「新たに策定する(した)見直す(した)」が25.9%、「策定する・見直す予定はない」が18.3%となっている。BCPを策定していた企業では、「新たに策定する(した)見直す(した)」が68.2%と7割近くに達している。
- 17) 単純に「現場の判断で」とはいえない面もある。N銀行のケースでは、ある支店の地域の指定避難場所が、徒歩5分ほどにある高台だったにもかかわらず、支店長の指示により、高さ約10メートルの2階建ての支店屋上に避難したことにより、死亡者や行方不明者を多く出してしまった。また本店から避難に関する指示もなかったという。
- 18) 例えばTwitterのケースでは、誤った情報が大量のリツイートでチェーンメール化したケースも多く見られたという。
- 19) SLA (Service Level Agreement) とは、サービスの提供者と利用者との間で決められたサービスの内容と範囲、保証すべき品質のこと。
- 20) データセンター等の設備の整った場所や回線、電源を提供するサービスで、ネットワーク機器やサーバーなどは顧客が用意する。
- 21) インターネットの一経路としてWiMAX (Worldwide Interoperability for Microwave Access) の活用も有効である。またコンビニエンスストアの中には業務通信システムとして、MCA (Multi-Channel Access radio system) 無線を採用している企業もある。
- 22) シンクライアントとはクライアント側に最低限の機能しか持たせず、サーバー側でPC側のソフトやファイル等を管理するシステムのことをいう。
- 23) オンプレミスとは企業が自社でハードウェア等の設備を用意し、情報システムを導入・運用すること。
- 24) ここではクラウドとしてパブリッククラウドを前提としているが、大企業の場合、プライベートクラウドを利用することも考えられる。
- 25) M銀行のように、東日本大震災の関連でATMが停止してしまい、手作業でこれを代替しようとして混乱してしまったケースもある。STP化においては、このようなリスクへの対応も

検討しておく必要があろう。

参考文献

戸村智憲「中小企業のための危機管理・事業継続・防災対応へのクラウド活用」同友館, 2011年10月31日

野村総合研究所「連載 BCP 総点検の勘所」日経 BP, 日経コンピュータ 2011 年 7 月 7 日号～2011 年 9 月 15 日号

新建新聞社「東日本大震災を生き抜いた 16 社の証言 総検証 BCP」リスク対策 .com, Vol28, November 2011

藤野直明, 他「災害で見直されるグローバル SCM のあり方」野村総合研究所, 知的資産創造 2012 年 2 月号

帝国データバンク「特別企画: BCP (事業継続計画) についての企業の意識調査」2011 年 6 月 27 日

KPMG ビジネスアシュアランス喜入博「事業継続をどのように考えればいいか」@IT 情報マネジメント, 2006 年 9 月 27 日, <http://www.atmarkit.co.jp/im/cop/serial/bcp/01/02.html#profile>

インプレスジャパン「インターネット白書 2011」2011 年 8 月 1 日

内閣府「事業継続ガイドライン 第二版」2009 年 11 月

中小企業庁「中小企業 BCP 策定運用指針」2006 年 2 月, <http://www.chusho.meti.go.jp/bcp/index.html>

事業継続推進機構「中小企業 BCP ステップアップ・ガイド (4.0 版)」2008 年 11 月 8 日, <http://www.bcao.org/data/01.html>

小川裕克「金融商品取引法施行に伴う内部統制の整備」野村アセットマネジメント, ファンドマネジメント 2008 年新春号

春口景助「テロ事件からの復興に向けて頑張るニューヨーク」野村アセットマネジメント, ファンドマネジメント 2002 年新春号

企業会計審議会内部統制部会「財務報告に係る内部統制の評価及び監査に関する実施基準—公開草案—」2006 年 11 月 21 日