東日本大震災に学ぶ事業継続計画とITの在り方
組織におけるITリスク管理

原田要之助[1]

概要

東日本大震災を受けて，多くの企業や組織では事業継続計画が役立たなかったり，十分に機能しなかった．この「事業継続」は，比較的新しい概念であり，多くの場合，緊急時対策計画や災害対策で用いられてきた．用語が最初に用いられたのは，BS7799であり，国際基準（現在のJIS Q 27002[1]）になることから注目されるようになった．このような経緯から，「事業継続」は情報セキュリティマネージメントの対策と理解されてきた．今回の大震災で，多くの企業では，経営資源の破壊，電力などのインフラサービスの中断，材料・原料のサプライチェーンの寸断などで事業が正常に継続できないという場面に遭遇して，「事業継続」が企業の経営上の重要課題であることを理解したと言えよう．

現在の企業は，殆どの場合ITを利活用しており，ITが停止するとこれを利用している事業が停止する．そのため，「事業継続」にはITサービスの継続性が重要となる．情報セキュリティ大学院大学では，新聞，Web調査及びヒアリングから，東日本大震災でのさまざまな課題を調査している[3]．本稿では，この調査をベースにして，企業がBCP/BCMやITサービス継続を実践するうえで必要となる対策について考察して，2つのモデルを使い分けること，経営の観点からのITリスク管理のアプローチが重要であることを述べる．

1 はじめに

日本では，大規模な自然災害に対する備えと被災後の早期復旧を中心に様々な対策が考えられてきた．これらの対策は，災害などに緊急に対応できる観点から，緊急時対応計画として捉えられてきた．ちなみに，2000年7月，政府（情報セキュリティ対策推進会議）が発表した情報セキュリティポリシーに関するガイドラインでは，緊急時対応計画が述べられている．しかし，2000年から始まったISMSが国際基準ISO/IEC27002（JIS Q27002[1]）及びISO/IEC27001（JIS Q27001[2]）をベースとするものとなり，この中で，事業継続計画（以下，BCPという:Business Continuity Planning）が概念として導入され，緊急時対応計画を包含するものと位置づけられた．これを契機としてBCPが用いられるようになった．また，BCPを効率よく管理・運用する概念として事業継続マネジメ

1 情報セキュリティ研究科　教授

ント（以下，BCMという:Business Continuity Management）が使われるようになった．本稿では，「事業継続」をBCPとBCMの両方を併せたものとして，BCP/BCMと表記する．

さて，2003 年10 月の経済産業省による情報セキュリティ総合戦略［4］では，「高信頼性社会」の構築として“事故前提社会システム”をめざすことになり，「サービス継続・復旧計画の策定ガイドラインの整備」が用いられた．この時点では，事業継続ではなくサービス継続という用語が用いられた．これは，情報サービスの提供側の事業継続の観点からのアプローチであったためである．その後，2005年に経済産業省では，企業における情報セキュリティガバナンスのあり方に関する研究会で，経営的な観点から，事業継続計画策定ガイドライン［9]を提唱した．その後，内閣府から，2005年に事業継続ガイドライン 第1版が策定され，2009年に改定され第2版となった[10]．一方，経済産業省では，BCP/BCMのITの位置づけを明確にするため，2007年にITサービス継続ガイドラインを策定している．

2 東日本大震災でのBCM/BCPについて

2.1 東日本大審査でのBCM/BCPの状況

野村総研では，被災地区の企業を除く全国3,000社を対象に調査を実施している[5]．この調査では，26%の企業が「重要な業務が停止した」と答えており，「一部（重要でない）業務が停止した」（29%）を含めると，55%の企業で何らかの業務停止を経験したとまとめている．また，「重要な業務が停止した」企業のうち21%では，「停止期間が1カ月以上に及ぶ重要な業務が停止した」と述べている．その理由としては，計画停電およびサプライチェーンの機能不全が原因であると述べている．

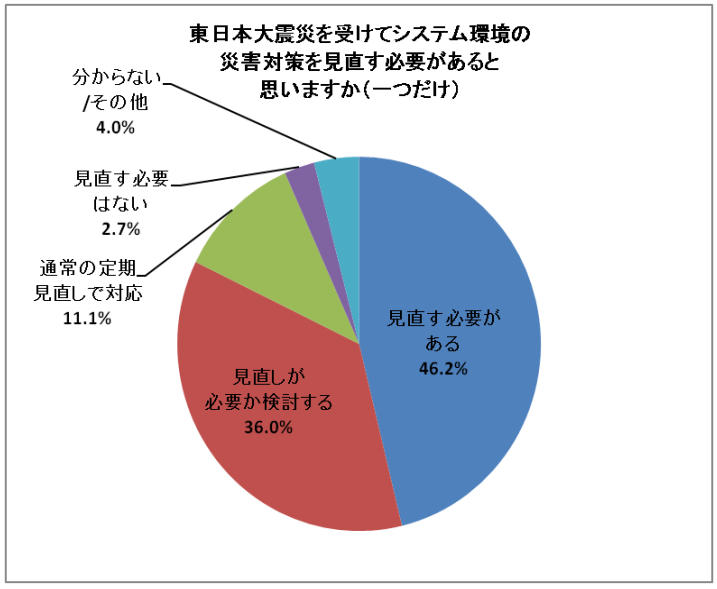
一方，JUAS（財団法人日本情報システム・ユーザ協会）の調査[6]では，野村総研の調査のように重要業務と限ってはいないが，大震災による直接・間接被害があった企業は「全体」の3/4，「製造業」では9割弱と述べている．また，被害の原因は「施設や設備が稼働できなかった」が3/4，「電力や燃料の調達」や「仕入れや材料・部品調達」ができなかったのは４割強と述べている．

どちらの調査結果からも，計画停電やサプライチェーンの機能不全の二点が大きな問題であったことが分かる．BCPでは，ビジネス・インパクト分析（BIA）が用いられる．BIAでは，まず，あらゆる事件や事故を想定して，重大な事業を明確にする．次に，重要な事業の停止に至る事件や事故を一般化して，事業の目標標復旧時間や目標復旧レベルを決めて，BCP/BCM対策を考える．今回の大震災で計画停電がITに与えた影響については想定できなかったとの意見が多い．BIA分析で想定した停電によるITの停止と実際に起きた事象とのギャップが大きすぎたのかもしれない．

また，日経BP社では，東日本大震災を受けてシステム環境の災害対策の見直しについて調査している[7]．この調査では，BCP/BCMを「見直す必要がある」が46.2%，「見直

す必要か検討する」が36.0%としており，約82%の企業がITの災害対策について見直しを始めていると述べている．すなわち，これは，BCP/BCMの観点からITについて，事業継続上の問題があったことが分かる．

図1　震災を受けてのシステムの見直し[7]より



情報セキュリティ大学院大学では，東日本大震災におけるBCP/BCMの問題点を新聞，ヒアリング，Webなどを通じて調査して，課題を整理して表１にまとめた[3]． 表１からは，様々な問題が顕在化したことが分かる．この中で，例えば，5の通信の問題が1のBCPの発動遅れの主な原因となっている．同様に，ITの課題は，BCPの問題点の多くの部分を占めている（7，9，10，11，12，13）．したがって，3章では，BCP/BCMをITの問題に焦点をあてて分析する．

表1　東日本大震災における BCP の問題点([3]より)

No	問題点	No	問題点
1	BCP の発動	8	要員の問題
2	BCP の不備	9	計画停電の影響
3	DRP（復旧計画）の問題	10	外部電源
4	インフラの問題	11	個人情報の取扱い
5	通信インフラの問題	12	情報漏えい
6	サプライチェーンの問題	13	バックアップ
7	自社のセキュリティ環境の問題		

3 東日本大震災でのBCP/BCMとITリスク

3.1 通信の輻輳がBCPの発動を遅らせた

東日本大震災での震度は首都圏では，震度５強であり，多くの企業がBCP/BCMの発動条件とする震度６以下であった．そのため，多くの企業の本社では，企業としてBCPを発動する判断のためには，東北地方の事業所の被害状況を調査する必要があった．また，多くの企業では，社外にいる社員の安否確認や幹部との連絡などで，電話や電子メールが多用された．また，社員も自分の家族の安否確認に携帯電話やメールを用いた．

そのため，東日本大震災では地震直後から，問い合わせの電話や電子メールがネットワークを飛び交って，通信の輻輳が震源地のみならず，全国的に発生した．この輻輳のために，企業や行政機関などでは，安否確認や地震に関する連絡が遅れ，BCPの発動・指示命令や，及び要員確保がタイムリーに実施できなかった．

事業継続ガイドライン[9]などが推奨するBCP/BCMでは，幹部や従業員の安否確認，BCPの発動，関連する企業や取引先などへの連絡などが最初のステップとして挙げられている．安否確認や連絡には，電話やメールなどが想定されている．しかし，通信が長期間輻輳すると，タイムリーに連絡できないため，次のステップに移れない．BCP/BCMでは，初動の3時間の対応が重要と言われているが，今回の東日本大震災では，通信の広域輻輳のためBCPの対応が遅れた．

通常，このような輻輳の現象は，震源地の近郊で発生するが，東日本大震災では，震源に近い東北３県で震度６を超えた．また，関東地方の多くが震度５であったため，家族や企業の安否確認の電話や電子メールが飛び交うこととなった．その結果，通信ネットワークが輻輳状態に陥ることとなった．

表2 安否確認に要した時間の調査結果[8]より

	全国	被災地
全メディア平均	3 時間 15 分	4 時間 9 分
公衆電話	3 時間 49 分	5 時間 46 分
固定電話	3 時間 29 分	4 時間 35 分
携帯電話	3 時間 40 分	3 時間 35 分
携帯メール	3 時間 4 分	3 時間 11 分
インターネットメール	3 時間 5 分	4 時間 35 分
災害用伝言板	3 時間 38 分	4 時間 24 分
Twitter やmixi, Facebook 等のサイト	1 時間 59 分	2 時間 56 分

表２は，ウェザーニュース社が会員対象に，東日本大震災のときに安否が確認できるま

でに要した時間を調査したものである[8]．この結果からは，東北3県では，安否確認できるまでにメディア平均で4時間，それ以外の地域でも，平均で3時間以上かかったことが分かる．さらに，固定電話，携帯電話，携帯メール，インターネットメール，災害用伝言版のすべてで3時間以上かかっていることである．これから分かることは，情報通信メディアのほとんどが，利用者が殺到することによる輻輳が起きて，十分に性能を発揮できていないことである．

表3　過去の震災における情報通信メディアの状況比較

震災	阪神･淡路大震災	新潟県中越地震	東日本大震災
発生	1995	2004	2011
種類	直下型	直下型	広域，津波を伴う
通信の状況	･固定電話が輻輳 ･携帯電話やポケベルで連絡 ･インターネット伝言板での情報提供	･固定電話が輻輳 ･携帯電話が輻輳 ･携帯メールが有効 ･伝言板サービス提供	･全国的に通信が輻輳 ･携帯電話が輻輳 ･携帯メール，インターネットメールが遅延 ･伝言板サービスが輻輳 ･Twitter や衛星携帯電話が有効

表３に最近の3つの震災級の地震のときの情報通信メディアの比較を示す．表３からは，メディアの進歩とともに輻輳がおきるメディアが変遷していることが分かる．例えば，阪神・淡路大震災では固定電話が輻輳したものの，携帯電話やポケベルが連絡に有効であった．2004年の新潟県中越地震では，携帯電話が普及し輻輳した．一方，携帯メールは利用者が少なく有効に使えた．また，伝言板サービスも有効であった．東日本大震災では，携帯メールやインターネットメールが普及していたため遅延が起きている．一方，Twitterや衛星携帯電話が有効であったと報道され，Twitterは素早く連絡がとれるツールとして，多くの自治体などで認知され始めている[7]．しかし，表２ではTwitterなどのメディアも，安否確認がとれるまでに平均として約２時間かかっている．この数値は，安否を確認したい相手がTwitterを見ていないことやインターネットへの接続が制限されていたなどによるものと思われる．

通信は同時に利用する人が少ないという原理に基づいて設計されているので，利用者が集中すると輻輳や遅延が起きる．TwitterなどのSNSでも，利用者認証など利用者が共通に利用するサーバやインターネットに接続する回線は利用者が共通に利用するので，輻輳や遅延が起きることがある．

以上からは，次の震災までに，利用者が通話せずに相手の安否を知ることのできるサービスを開発する必要があると考える．携帯電話システムでは，端末の位置情報を常に

データベースに記録しており，これを安否確認に利用するなどが候補となりうる．通話の場合も，例えば，接続時間を予約制にして繋げるサービスなども考えてみてはどうであろうか．

3.2 企業のセキュリティ環境の問題

多くの企業では，JIS Q27002[1]が国際基準となった 2000 年以降，情報セキュリティ対策を強化してきている．例えば，情報流出を防ぐために，個人 PC や記録媒体などの持ち込みを制限したり，入退室管理を厳格に実施している．しかし，今回の震災では，以下のような企業の情報セキュリティ対策と矛盾するような問題が発生している[3]．

① 企業のサーバ室が地震や津波で壊れ，サーバとともに重要な企業の個人情報や機密情報が流出した．これらについて，セキュリティインシデントとして報告されたケースは少ない．大震災ということで，企業側も非常事態と捉えていると考えられる．
② 多くのサーバ室などでは，電子的な施錠システムが導入され，IC カードによって入退室管理をしているケースが多い．これらのシステムでは，商用電源を利用しているため，計画停電時にセキュリティを保持できない．人手でカバーするしかない．
③ サーバ室など高度なセキュリティエリアへの入室ドアには，監視カメラが導入され記録されているケースが多い．しかし，監視カメラが記録機器が地震で壊れたり，停電で使えない場合には，監視ができていないため，誰が入室したか分からない．
④ 計画停電の際，企業の重要な情報資産や個人情報を持ち出して自宅で作業するケースがある．

以上の問題点の解決には，非常時にも，セキュリティ関連システムに電源を供給することが求められる．すなわち，商用電源が提供されないときのバックアップ電源については，BCP 策定の際にセキュリティ関連機器への電源供給を含めた検討が必要となる．
とくに，重要な情報資産については，例えば，サーバ室の入退室管理システムが停電で機能しないような非常時でも機密保持ができるように，全てのデータを常時暗号化して利用するなどの対策[2]が必要であろう．また，BCP には，被災時の情報セキュリティの管理レベルを下げたり，制限を緩和（自宅作業を容認）することも記載しておいて，柔軟な対応がとれるようにすることも大切であろう．また，情報処理環境に自宅作業を含める場合には，自宅 PC を含む拡張した環境全体での情報セキュリティ対策が必要となる．ISMS やプライバシーマークの認証を取得している場合には，新しい環境での認証が必要になるケースもあるので注意が必要であろう．

3.3 計画停電の影響

計画停電は，今回の大震災で初めて認知された問題であり，多くの企業に影響を与え

2 サーバが流出しても内部のデータが第三者に解読されないようにする

た．エリアで停電が画一的に決められており，また，エリアが行政区画と異なっていたことや停電が実際には実際されないこともあったりして，混乱を生じた．とくに，首都圏に多数の事業所展開している企業の IT 関係者は以下のような問題で苦しんだ[3]．

① 企業の IT 機器は，商用電源の供給を前提としているため，停電時に，バックアップ電源は，一部の重要な機器しか供給されないことが多い．
② サーバのある地域と事業所が計画停電の異なるエリアの場合，いずれかのエリアが停電中は企業としてシームレスな運用ができない．
③ 計画停電の際，サーバを安全に停止し，停電が終わった後，スムーズに再稼働するためには，保守者がスタンバイする必要があり，保守者の稼働がひっ迫した．

計画停電については，今まで経験したことのない問題であり，多くの企業が手探りで対策を検討し，実施しており，企業から以下のような対策がヒアリングで得られた．

・計画停電による自社の影響（複数の事業所に渡って，どこが停電するとどこに影響するかなど）を事前に分析しておく
・事業所内に商用電源と無停電電源の配線を分けて実施しておき，事業の継続に必要な機器を選別して，動作できるようにする（無停電電源と発電機の発電容量とをあらかじめ合わせておく）
・小規模な事業所などでは，例えば，EV 車の電源を利用して，最低限の機器に給電できるようにする[3]．

3.4 個人情報の取扱いの混乱

個人情報の取扱いについては，以下のような問題が指摘されている[3]．

① けがを負った方の救助や死者の身元調査で，本人同意を得ていないとの観点から PC に保存されている個人情報を提供しなかったなど，個人情報の利用の誤解からせっかくの個人情報が利用されないケースが多かった
② 医療機関で被災者の医療記録（カルテ）を本人の同意がない場合に，他の医療機関に個人データを送信できなかった[4]
③ 不明者に関する個人情報の開示の明確な基準がないため，ホームページなどで不明者の情報を公開するまでに時間を要した

今回の震災のような場合には，個人情報保護法や JIS Q15000 に述べられているように，例外事項に該当すると考えられ，個人情報を同意なしに提供や利用できる．役場が地震で崩壊したり，津波に流されたりした市町村では，避難場所などで，PC を用いて

3 この実現には，現在，実証実験されているスマートグリッドの技術が適用できるであろう．ただし，直流から交流に変換する機器などが新たに必要となる

4 被災者に紙に書いたカルテを先方の医療機関に持たせた医療機関もあった

臨時の役所サービスが提供された．このような極限の状態では，法律の専門家が身近にいることは少なく，法的に例外事項となるかの判断は現場要員には難しい．どうしても，安全側に判断して，個人情報の利用を制限することが多い．そこで，行政機関などでは，非常時のマニュアルなどを作成して，個人情報や医療情報を適切に利用できるようにすることも必要である．また，役場のサービスを避難所などで PC を用いて臨時提供する際には，個人情報や医療情報などが（操作者の判断なしに）自動的に取り扱えるようなシステムの開発も必要であろう．さらに，不明者を探すため，氏名，年齢，性別，体の特徴などの個人情報をホームページで開示しているケースがあるが，本人同意がないという点と何時まで掲示できるか（何時まで例外事項として掲示できるのか）の問題があり，法曹関係者でも見解が分かれている．少なくとも，次の震災までに，同じような誤解を減らすためにも，何らかの判断基準を示すことが求められている．

3.5 データのバックアップ

多くの企業は，サーバのデータのバックアップの重要性を理解している．しかし，今回の大震災では，バックアップで想定していなかった以下の問題が発生している[3]．

① 50 キロ程度離れたバックアップサイトにバックアップメディアを保管していたが，メインサイトとバックアップサイトの両方が津波によって喪失した
② バックアップサイトが停電のため，バックアップとして機能しなかった
③ 宮城県南三陸町や岩手県陸前高田市などの戸籍が流出し，バックアップから回復したものの，バックアップ時点から震災時点までの届け出関連のデータが喪失した[5]
④ バックアップから正常運転に切り戻すことができない企業があった
⑤ システムが動作しない間の取引は紙ベースで行い，後日，入力したが，データを整合させるのに時間を要した

多くの企業は，阪神大震災以降，同一の地震で被災しないよう離れたバックアップサイトにバックアップメディアを保管する対策を採っている．津波による同時被災を考えていなかったため，バックアップをも含めて被災した企業がある．広域震災の場合には，バックアップサイトの喪失や停電なども考慮にいれたバックアップサイトの選択が必要であることが分かった．これについては，クラウドも選択肢となる．

重要なデータベースの場合には，定期的なバックアップでは，その間のデータが喪失するリスクがあり，リアルタイムバックアップが必要となると考える．また，バックアップサイトで運用する場合には，どのタイミングで，どう切り戻すかの手順やテストするかを検討する必要がある．また，これらの手順について，専門家でなくても簡単に扱えるような手順の開発やマニュアルの整備が重要となっている[11]．

5 法務省，東日本大震災により滅失した戸籍の再製データの作成完了について
http://www．moj．go．jp/MINJI/minji04_00024．html

4 BCP/BCMとITサービスの継続のモデルの考察

4.1 BCP/BCMのモデルの前提条件

企業や政府機関などが，ITの災害対策に積極的に取り組み始めたのは，阪神・淡路大震災で神戸市役所が崩壊し，水道事業を管理する情報システムが使えなくなり，復旧するまでに長時間を要したことがきっかけであった．そのため多くのBCPは，地震対策，それも直接被害の大きな直下型地震のみを想定することとなっている．今回の東日本大震災では，震源地に近い東北3県に事業所や工場などを持つ企業は，震度６から７の地震や10メートルを超える津波による被害の状況に合せてBCP/BCMを発動している．

一方，首都圏では，東日本大震災での震度は５強であり，多くの企業がBCP発動の条件として設定する震度６に至らなかった．さらに，多くの企業において地震による直接的な被害は少なかった（千葉県と栃木県の一部を除く）．そのため，地震直後にBCPを発動した企業は少なかった．しかし，情報システムが地震で破壊されなくても，停止することに対する配慮が不十分であった．すなわち，福島第一原子力発電所の事故や，長期にわたる発電量の制限や計画停電のためにITを中断させることになり，そのため事業が中断することになった．これについては，多くの企業のBCP/BCM担当者が，ほとんど検討すらしていなかった．今まで，電力供給が安定し，停電もほとんどない状況に慣れてしまっていたためである．米国を含む多くの国ではUPSが一般的に用いられている．一方，日本では普及していない．今後，UPSなどの採用も検討すべきである．

なお，3月11日の地震の揺れが収まった時点では，首都圏では停電がおきなかった．そのため，この時点で情報システムに対する電源への対応をとった企業は数少ない．この時点で対策した企業は，簡単に発電機用の重油を入手でき，その後の計画停電で柔軟な対応ができている．計画電源の問題がクローズアップされた3月13日に，多くの企業が電源供給の問題に気づいた．あわてて，重油の手配を始めた時点では，ほとんど入手できない状況であった[7]．

また，さらに，地震による二次的，三次的な影響で，計画停電，銀行のサービス中断，部品のサプライチェーンの寸断など，思いがけぬところで企業の事業が脅かされることになった．ここで，大切なのは，BCP/BCMについて，災害直後の機能停止だけでなく，災害後の複合的な要因によって発生する二次被害，三次被害を広義に捉えた対策が必要となったことである．

4.２ ２つのBCP/BCMのモデル

BCP/BCMのモデルとしては以下の二つを考える必要がある．とくに，地震などの事件直後に，被害状況が表面化する場合，例えば，設備の動作や稼働が停止する場合（図２に例示する）と事件直後には直接の影響が表面化しない場合（図3に例示する）がある．

図2　事件の影響がすぐに現れる場合（文献[10]より）

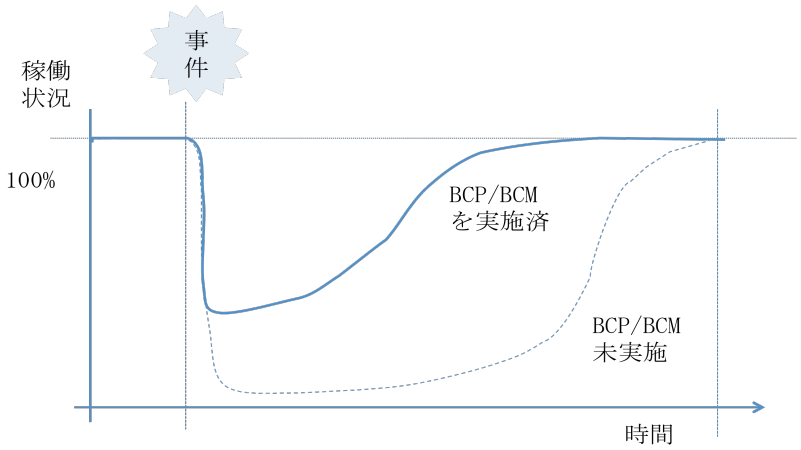


図２に示す場合は，事件が起きるとすぐに，事件の影響から性能低下を起こす．もし，BCP/BCMの対策がなされていない場合には，殆ど事業が停止状態となる．しかし，BCP/BCMの対策がなされている場合には，稼働もある目標までのレベルでとどめ，その後，回復過程を進めることができる．

図3　事件の影響がすぐに現れない場合（文献[12]より）

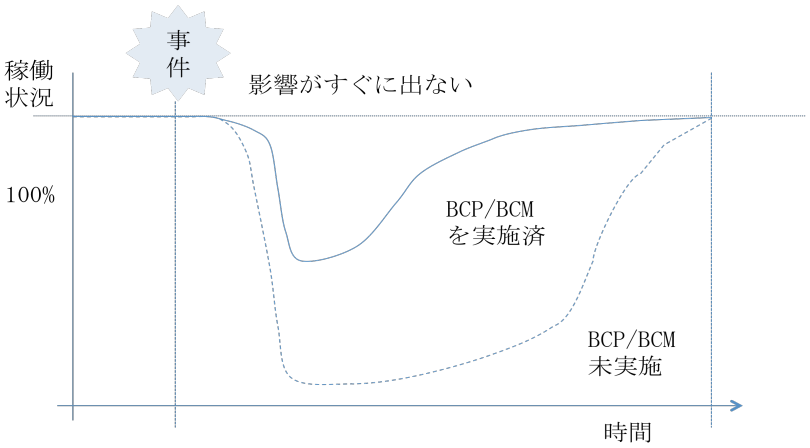


図３に示す場合には，事件が起きてもすぐに，事件の影響がないため，被害として認知されない可能性がある．このような場合に被害に気付くのが遅れると致命的な状況に繋がることがある．東日本大震災の場合には，福島第一原子力発電所の停止により関東地区の電気が不足して，計画停電という二次被害で発露した．企業は強制的に電気が止められ，製造装置やIT機器が使えない状況に陥った．BCP/BCM対策として，電気の停止に対して，発電機などを用意している企業の場合は，必要な製造装置やIT機器を動作させることができたため，一定の稼働状況を担保できた．

一方，BCP/BCMの対策がなされていない場合には，図２の場合と同様に殆ど事業が停止状態となる．東日本大震災では，道路が損傷して（一次災害），ガソリンなどの燃料

を輸送できず（二次災害），車などによる輸送手段が止められてしまった．その結果，機会部品などが輸送されずサプライチェーンが崩壊してしまった．通常の場合，部品などは一定の在庫があるため，すぐには生産が止まることはないが，在庫が切れてしまうと製造ができなくなり，最終的には生産を止めることになる．東北地方の工場で生産されている部品が製造や輸送できなくなり，その影響は世界中の車の工場の生産をとめることになった．すなわち，多くの企業の事業所や工場が図３の状況に陥った．このモデルでは，事件が起こってもすぐに影響がでないため，問題を看過することである．大切なのは，稼働状況をモニタして早期に問題を発見するとともに，次におきる二次災害や三次災害の発生を予期して，対応することである．

5 企業のBCM/BCPに重要なガバナンスの視点

5.1 企業経営の視点からのBCP/BCM

BCP/BCMは，金融機関においては，早くから整備されている．しかし，一般企業は，受動的なものが多く，経済産業省のガイドライン[9]や内閣府などのガイドライン［10］が発表されるまでに対応した企業は少ない．内閣府による調査[13]を図４に示す．

図4．事業継続計画（BCP）の策定理由（内閣府調査[13]より，一部修正）

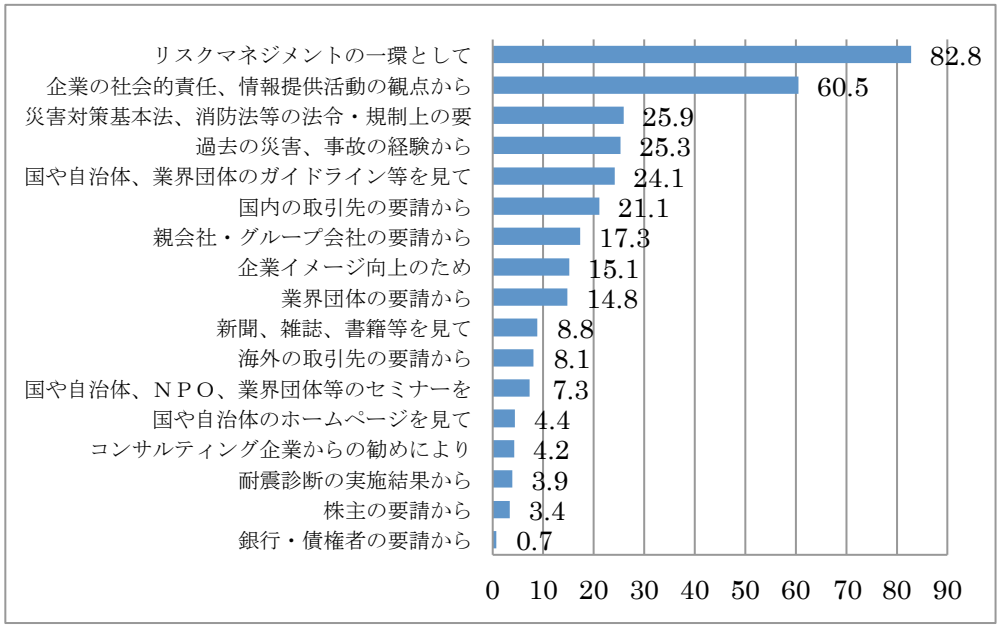


図４からは，企業のリスクマネジメントの一環として」が82.8%，「企業の社会的責任，情報提供活動の観点から」が60.5%，と他の項目を大きく引き離している．これに引き続くのは，「過去の災害・事故の経験から」，「災害対策基本法，消防法等の法廷・規制上の要求から」，「国や自治体，業界団体のガイドラインを見て」の３項目がほぼ

25%となっている．すなわち，企業は，リスクを管理して，経営を維持継続していくことが，ステークホルダや顧客への責任として求められると考えて，BCP/BCMを導入しているケースが多い．これは，企業にとってBCP/BCM対策は費用であり，収益を伴わない．その投資額についても明確な基準があるわけではない．企業が多額のBCP/BCM対策を行った場合，ステークホルダへの説明責任が難しい．そのため，経営者はリスク対策やCSRを理由に選んでいると考えられる．また，CSR報告書を公開している企業の多くがBCP/BCMを実施していることから，企業のサステナビリティのための対策と言えるからである．しかし，このような対策では，本来の事業継続に必要な対策を実施することはできない．それが，今回の問題の背景にあると考えられる．

内閣府のBCP/BCMガイドラインなどは，具体的にBCP/BCMの策定，維持管理について詳細に展開されており，BCP/BCMをオペレーショナルな観点から捉えている．そのため，BCP/BCMは企業の運用面，すなわち，林のいう「係長セキュリティ」[14]の観点が色濃くでている．しかし，一方，BCP/BCMは事業をどのように継続するのか中断するのかを判断する必要があるため，経営判断そのものである．すなわち，「社長セキュリティ」[14]の観点から取り組む必要がある．ガイドラインでは，現場で使えるよう工夫するあまり，「社長セキュリティ」と「係長セキュリティ」との関係が明確になっていないのが問題であろう．今後は，社長が実施するものと係長などマネジメント層が実施するものを明確に分けることが必要と考えられる．

5.2 社会的な視点の必要性

事業継続を企業経営から考える場合，どうしても自社・自組織を中心に考えてしまう．そのため，自社を中止にして，ステークホルダとの関係を考えてしまう．すなわち，取引先はいつでも，自社に対して必要な経営資源を提供してくれることを前提として，BCPが策定される．東日本大震災のような広域災害では，取引先も被災していて，被害がでているかもしれない．また，サプライ品や支援をしてもらうためのインフラが被災しているかもしれない．道路が寸断されていれば，例え，サプライ品があっても届けられない．

内閣府の事業継続ガイドラインでは，BCPを策定するときの前提として，他の取引先や関係会社の協力が得られることを前提としている[10]ため，協力を得られない場合を想定していない．すなわち，自社の視点からのみ事業をどう継続するかのみを考える対策を述べている．阪神大震災や中越新潟地震は直下型であり，企業が復旧に必要な資材やサプライを提供する取引先などの企業が同時に被災するケースは少なかった．しかし，東日本大震災のような広域災害の場合には，インフラが被災したり，サプライチェーンそのものが機能しなかったりして，自社の視点だけでは行き詰ってしまう．このように見てくると，BCP/BCMモデルは自社のことだけを考えた利己的なプログラムとなっていることが分かる．

自己中心的でない広域災害に適したBCP/BCMモデルを考えるには，何が必要か？．これには，地域や社会という視点で考える必要があろう．地域をどう復旧するのがよいのか，地域全体からの視点で，どう全体を復旧・復興していくのがよいか，その中で，自社は何をできて，何をしてもらえるかを明らかにして，自助努力をどうするかという視点でBCP/BCMを再構築すること必要であると考える．すなわち，広域企業の連合したBCP/BCMモデルを構築することになる．

野中[15]は，今までの企業の収益モデルが成り立たないのではないかと疑問を持ち，「企業は収益を上げるモデルを磨きながらも，より良い社会を志向する価値観を併せ持たねばならない」，そこで，「企業は，二律背反とされてきた収益性と社会性に関する暗黙の了解を覆し，両者の二律創生を共通感覚として組み込んだ新しい次元の競争で世界の発展，未来の創造を目指すべき」と述べている[15]．今回の東日本大震災では，早期に復旧できた企業の多くは，まず，従業員の食糧確保などから始め，道路，電気のインフラを先に修復し，関連会社，ボランティア及び地域の協力を得て，自社のBCP/BCMに取り組んで復興を果たしている．自社が事業を継続するのは社会のためと定義して，社会的な視点からBCP/BCMを扱う方法論を確立する必要があると考える．そのためには，ITリスクについても社会的な観点で分析すると，共同でバックアップサーバを準備したり，広域なEV車によるスマートグリッドを構築して，EV社を中心にバックアップ電源を供給するような発想が有効となるのではないであろうか．

まとめ

東日本大震災では，BCP/BCM について，IT のリスクについてさまざまな問題点が明らかになった．例えば，BCP/BCM を策定する際には，事業を想定して考えていく必要がある．しかし，事業に IT が用いられるようになったのはこの 10 年ほどであり，過去の事件・事故，災害と IT との関係の蓄積は少ない．また，阪神大震災と現在とでは，携帯電話やインターネットの利用状況，さらには，個人情報保護法の有無が異なるため，そのままを適用して考えることができない．そのため，悪いケースや遭遇したことがないケースが見落とされがちである．また，今回の大震災で明らかになった計画停電やサプライチェーンの崩壊による事業の中断が震災直後ではなく，後になって表出することである．これをカバーするにはモデルを立てて対策を考えることが重要である．重要な事業に対する目標復旧時間，目標復旧レベル，目標復旧時点を設定して，すぐに事業に影響する事件・事故，災害とある程度の時間が経過した後に影響があるものを分けて考えるとよいであろう．また BCP/BCM を考える際には，個々の事業を継続するための対策と経営的な大局的な視点から全体像を考える両方からのアプローチが重要である．さらに，BCP/BCM を策定，運用するにあたって自社中心の視点だけでなく地域や社会との協調の中で考えていかないと東日本大震災のような広域な災害からの早期の復旧は難しい．今

後は，社会的な観点からの BCP/BCM や IT のリスクを捉えていくことが必要となる．

謝辞

本稿をまとめるにあたって，情報セキュリティ大学院大学の教員，研究室の学生や研究生から得られた温かい助言や調査への協力に感謝する．

参考文献

［１］日本規格協会，JIS Q27002:2006（情報技術―情報セキュリティマネジメントの実践のための規範），2006 年
［２］日本規格協会，JIS Q27001:2006（情報技術―情報セキュリティマネジメントシステム―要求事項），2006 年
［３］情報セキュリティ大学院大学 原田研究室，「東日本大震災における BCP の問題点について」，2011 年 5 月，http://lab.iisec.ac.jp/~harada_lab/BCP_20110518.pdf
［４］経済産業省，情報セキュリティ総合戦略，2003 年 10 月
［５］野村総研，大手企業の 26%で重要業務の停止が発生，大手企業 3,000 社を対象調査，2011 年 6 月 30 日発表，http://www.nri.co.jp/news/2011/110630_1.html
［６］社団法人日本情報システム・ユーザー協会，第 17 回企業 IT 動向調査 2011 調査追加調査，2011 年 5 月 30 日発表，http://www.juas.or.jp/servey/it11/it11add_press_pp.pdf
［７］日経ＢＰ，「IT で実現する 震災・省電力 BCP 完全ガイド」，2011 年 7 月
［８］ウェザーニューズ社，「東日本大震災」調査結果-全国 8 万 8 千人の津波・地震発生時の行動・意識を分析-，2011 年 6 月
［９］経済産業省，事業継続計画策定ガイドライン（企業における情報セキュリティガバナンスのあり方に関する研究会報告書・参考資料），2005 年 3 月
［10］内閣府，事業継続ガイドライン 第二版― わが国企業の減災と災害対応の向上のために ―，2009 年 11 月
［11］岩崎正治，東日本大震災を踏まえた災害時情報システムの復旧手順の見直しありかたについて，防衛調達基盤整備協会懸賞論文，2011 年 11 月
［12］ISO/IEC，ISO/IEC27031，Information technology -- Security techniques -- Guidelines for ICT readiness for business continuity，2011 年 3 月
［13］内閣府，企業の事業継続及び防災の取組に関する実態調査，平成 21 年度
［14］林 紘一郎，係長セキュリティから社長セキュリティへ：日本的経営と情報セキュリティ，情報セキュリティ総合科学 第２号，2010 年11 月
［15］野中郁次郎，「知」を価値に変える経営を，日経2011年10月14日朝刊，2011年10月