

18-H007

平成18年度  
セキュリティ技術国際動向調査研究報告書

平成19年3月



財団法人 日本情報処理開発協会

|                                                                                                                                                                                                         |                                                                                      |                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  The Keirin logo features the word "KEIRIN" in a bold, black, sans-serif font above a stylized blue infinity symbol. | <p>この事業は、競輪の補助金を受けて実施したものです。<br/><a href="http://keirin.jp">http://keirin.jp</a></p> |  A standard black and white QR code is located in the bottom right corner of the footer box. |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## はじめに

この報告書は、財団法人日本情報処理開発協会が日本自転車振興会の補助金を受けて実施した平成18年度情報化の進展に関する補助事業「情報セキュリティ基盤の強化に関する調査研究」事業の一環として取りまとめたものである。

情報通信技術の普及は、我々が生活する社会システムを大きく変えた。新たに出現した高度情報通信社会の継続について、多様な視点から見直すべき時期に来ている。

政策においては、国家戦略である「e-Japan 戦略」が2001年から始まり、その端緒となるネットワークインフラの基盤整備により、我が国の「ブロード・バンドは世界で最も低廉・高速」となるに至った。企業内はもとより企業間でも、電子商取引などブロード・バンドを利用したビジネスが盛んに行われている。

ITの利便性追求の中で、確かにシステムは進化し、社会経済活動は激変した。身近なところでは、インターネット検索や電子メールなど多くの人がITの利便性を享受している。ITは、電気、水道、ガスなどと同様にライフラインの一つとして位置付けられるようになったといえるだろう。そのような環境変化の下で、企業が有する電子データは幾何級数的に増加し続けており、その保管に必要な容量は増大の一途を辿っている。

本調査研究では、このようなリスクを単に情報通信システムの問題として捉えるのではなく、より広範な視点からこの高度情報通信社会全体が直面しうる危機に対して、事業を継続するためにどのような備えが必要なのかを考えることに焦点を当て、マネジメントと技術の両方から、近年活発になりつつある国内外の取組みを中心にまとめた。

第1章では、事業継続に取り組むグローバルな活動を概観するとともに、本調査研究で焦点を当てた新たな脅威について触れた。

第2章では、事業継続に関する最近の国内外の動向をまとめた。

第3章では、事業継続に関する欧米を中心とした企業の取組みの実際をヒアリングした結果を中心にまとめた。

第4章では、事業継続に必要なスキルと人材について、海外の団体などの動きから考察した。

第5章では、事業継続への取り組みを支援するソフトウェアツールについて代表的な例を取り上げ概説した。

第6章では、新たな脅威として認識され、取り組みが推進されている「パンデミック・インフルエンザ」対策について、米国ならびに英国における活動を中心にまとめた。

第7章は、事業継続を支援する技術として、リモートバックアップを中心に、関連技術の最新動向について記載した。

最後に、第8章で、全体についてまとめ、課題や見解などを述べた。

本調査研究は、昨年度実施した「セキュリティ技術国際動向調査研究」を更新する形で整理した。したがって、大きな状況変化は見られないが、事業継続に取り組む企業などの組織にとって有用と思われる情報については、昨年度の報告書に記載したものを再掲する形を取った。

なお、本調査研究については、株式会社富士ゼロックスに委託した結果を当協会が取りまとめたことを申し添える。

本調査研究が、事業継続に関する取組みの一助となれば幸いである。

平成 19 年 3 月  
財団法人 日本情報処理開発協会

## 目次

### はじめに

|                                                            |           |
|------------------------------------------------------------|-----------|
| <b>1 事業継続の潮流</b> .....                                     | <b>1</b>  |
| 1.1 事業継続を取り巻く潮流.....                                       | 1         |
| 1.2 新たな脅威への挑戦.....                                         | 2         |
| <b>2 事業継続関連の国内外の動向</b> .....                               | <b>4</b>  |
| 2.1 米国の現況 .....                                            | 4         |
| 2.1.1 事業継続の導入状況 .....                                      | 4         |
| 2.1.2 標準化の動向 .....                                         | 5         |
| 2.1.3 現地の状況.....                                           | 6         |
| 2.2 英国の現況 .....                                            | 9         |
| 2.2.1 事業継続計画の導入状況 .....                                    | 9         |
| 2.2.2 標準化の状況 .....                                         | 9         |
| 2.2.3 現地の状況.....                                           | 14        |
| 2.3 日本の現況 .....                                            | 14        |
| 2.3.1 事業継続計画の導入状況 .....                                    | 14        |
| 2.3.2 標準化の動向 .....                                         | 15        |
| 2.3.3 経済的インセンティブに関する動き.....                                | 15        |
| 2.4 ISO 化の動向.....                                          | 17        |
| 2.4.1 ISO 化の概要とスケジュール .....                                | 17        |
| <b>3 事業継続に関する企業・業界の取組み</b> .....                           | <b>20</b> |
| 3.1 個別企業の取組み .....                                         | 20        |
| 3.1.1 事例：欧州系銀行 A 行.....                                    | 20        |
| 3.1.2 事例：香港系銀行 B 行.....                                    | 21        |
| 3.2 業界としての取組み（欧米） .....                                    | 21        |
| 3.2.1 事例：英国金融サービス機構（FSA） .....                             | 21        |
| 3.2.2 事例：米国証券業協会（SIA：Securities Industry Association） .... | 23        |

|          |                                                                  |           |
|----------|------------------------------------------------------------------|-----------|
| <b>4</b> | <b>事業継続に必要なスキルと人材.....</b>                                       | <b>24</b> |
| 4.1      | 人材・プロフェッショナル育成の重要性 .....                                         | 24        |
| 4.2      | 英国 BCI の資格概要.....                                                | 24        |
| 4.3      | 米国 DRII の資格概要.....                                               | 25        |
| 4.4      | 事業継続管理に必要なスキル・セット分野 .....                                        | 26        |
| 4.5      | 事業継続に係る職種.....                                                   | 28        |
| 4.6      | 事業継続に必要なスキルと人材.....                                              | 29        |
| 4.6.1    | プロフェッショナル人材育成と事業継続管理体制構築.....                                    | 29        |
| 4.6.2    | 今後の事業継続の課題における人材育成.....                                          | 32        |
| <b>5</b> | <b>事業継続管理のためのソフトウェアツール.....</b>                                  | <b>34</b> |
| 5.1      | マネジメント支援ツールの必要性について .....                                        | 34        |
| 5.2      | マネジメント支援ツールの使用状況 .....                                           | 35        |
| 5.3      | マネジメント支援ツールの概要.....                                              | 36        |
| 5.3.1    | <i>Paragon</i> (SUNGARD 社) .....                                 | 36        |
| 5.3.2    | <i>LDRPS</i> (Strohl Systems 社) .....                            | 37        |
| 5.3.3    | <i>BS25999</i> 事業継続評価ツール ( <i>Survive</i> および <i>BSI</i> ) ..... | 38        |
| 5.3.4    | まとめ.....                                                         | 38        |
| <b>6</b> | <b>パンデミック・インフルエンザに対する取組み .....</b>                               | <b>39</b> |
| 6.1      | 英国政府 .....                                                       | 40        |
| 6.1.1    | 英国内閣府のパンデミック計画ガイダンス.....                                         | 40        |
| 6.1.2    | 事業者のためのパンデミック・インフルエンザ チェックリスト .....                              | 48        |
| 6.2      | サーバイブによるパンデミックのガイドライン .....                                      | 50        |
| 6.3      | 米国政府 .....                                                       | 52        |
| 6.3.1    | 米国保健社会福祉省( <i>HHS</i> )の活動.....                                  | 52        |
| 6.3.2    | <i>Homeland Security</i> の活動.....                                | 55        |
| 6.3.3    | その他の一般的情報 .....                                                  | 58        |

## 7 事業継続を支援する技術-リモートバックアップ..... 60

|       |                            |    |
|-------|----------------------------|----|
| 7.1   | バックアップを取り巻く環境変化と現状 .....   | 61 |
| 7.1.1 | バックアップ運用を取り巻く環境変化 .....    | 61 |
| 7.1.2 | バックアップ運用の現状 .....          | 63 |
| 7.1.3 | バックアップ運用のニーズと現状のギャップ ..... | 64 |
| 7.2   | リモートバックアップの技術動向 .....      | 65 |
| 7.2.1 | リモートバックアップ方式 .....         | 66 |
| 7.2.2 | リモートバックアップの要素技術 .....      | 69 |
| 7.2.3 | サーバー層 .....                | 70 |
| 7.2.4 | ストレージ層 .....               | 72 |
| 7.2.5 | ネットワーク層 .....              | 74 |
| 7.3   | リモートバックアップの技術選択 .....      | 77 |
| 7.3.1 | RPO/RTO/RLO .....          | 77 |
| 7.3.2 | サーバー層およびストレージ層の検討項目 .....  | 79 |
| 7.3.3 | ネットワーク層の検討項目 .....         | 80 |
| 7.3.4 | リモートサイトの運営体制 .....         | 81 |
| 7.4   | バックアップ技術を活かすために .....      | 82 |

## 8 まとめ..... 84

|       |                             |    |
|-------|-----------------------------|----|
| 8.1   | 事業継続に関する全体動向 .....          | 84 |
| 8.1.1 | 事業継続の規格やガイドラインについて .....    | 84 |
| 8.1.2 | 欧米における取り組みの現状から .....       | 85 |
| 8.1.3 | 事業継続の専門家について .....          | 85 |
| 8.2   | パンデミック・インフルエンザ対策 .....      | 86 |
| 8.2.1 | 想定されるシナリオ .....             | 86 |
| 8.2.2 | パンデミック・インフルエンザ計画のポイント ..... | 87 |
| 8.2.3 | 国家全体としての取組みの重要性 .....       | 87 |
| 8.3   | 事業継続を支援する技術 .....           | 88 |
| 8.4   | まとめ .....                   | 89 |

## 図表目次

### 図

|      |                                       |    |
|------|---------------------------------------|----|
| 図 1  | BCM プログラム・マネジメント .....                | 11 |
| 図 2  | 英国 BCI が提唱する事業継続のプログラムマネジメント .....    | 13 |
| 図 3  | 日本政策投資銀行の防災格付け制度 .....                | 16 |
| 図 4  | ISO/TC223 の構成 .....                   | 19 |
| 図 5  | FSA による業界横断演習 2006 の報告書 .....         | 22 |
| 図 6  | BCI の会員資格レベル .....                    | 25 |
| 図 7  | DRII の資格概要 .....                      | 26 |
| 図 8  | BCM 体制の構築の段階 .....                    | 30 |
| 図 9  | 事業継続推進機構 .....                        | 32 |
| 図 10 | SUNGARD 社が提供する BCM 統合ツールを用いた方法論 ..... | 37 |
| 図 11 | 民間緊急事態法の対象者分類 .....                   | 41 |
| 図 12 | 統合緊急事態管理全体図 .....                     | 42 |
| 図 13 | 民間緊急事態法における 7 つの市民保護義務の相互関係 .....     | 43 |
| 図 14 | BCM の概念図 .....                        | 44 |
| 図 15 | BCM の 5 ステージ .....                    | 44 |
| 図 16 | 米国保健社会福祉省によるパンデミック・インフルエンザの情報 .....   | 53 |
| 図 17 | 災害対応計画連続体の図 .....                     | 57 |
| 図 18 | バックアップの現状 .....                       | 64 |
| 図 19 | リモートバックアップの概念図 .....                  | 65 |
| 図 20 | 同期式の概念図 .....                         | 67 |
| 図 21 | 非同期式の概念図 .....                        | 68 |
| 図 22 | リモートバックアップの要素技術（3 層分類のイメージ） .....     | 69 |
| 図 23 | ベアメタルリストアの概念図 .....                   | 71 |
| 図 24 | ストレージレプリケーション概念図 .....                | 72 |
| 図 25 | 仮想サーバー概念図 .....                       | 73 |
| 図 26 | WAN 高速化装置の概念図 .....                   | 75 |
| 図 27 | RPO/RPO/RLO の概念図 .....                | 78 |
| 図 28 | バックアップ方式・ツール選定のテンプレート例 .....          | 78 |

## 表

|     |                                       |    |
|-----|---------------------------------------|----|
| 表 1 | NFPA1600 の項目 .....                    | 6  |
| 表 2 | BCI が提供する事業継続管理に関わるシラバス（講義要綱）の雛形..... | 13 |
| 表 3 | 事業継続ソフトウェアの用途別使用者割合 .....             | 35 |
| 表 4 | ガイドラインの全体構成.....                      | 46 |
| 表 5 | パンデミック・インフルエンザ チェックリストの大項目.....       | 48 |
| 表 6 | ガイドラインの項目 .....                       | 51 |
| 表 7 | 米国ビジネス・パンデミック・インフルエンザ計画チェックリストの項目     | 54 |
| 表 8 | 同期式と非同期式の比較.....                      | 68 |
| 表 9 | システム障害おける売上損失額例（1 時間相当） .....         | 82 |

# 1 事業継続の潮流

## 1.1 事業継続を取り巻く潮流

近年、わが国では、事業継続への関心が急速に高まっている。その背景には、2005 年 3 月の経済産業省による「事業継続策定ガイドライン」や同年 8 月の内閣府防災会議による「事業継続計画策定ガイドライン」を皮切りに、翌 2006 年 2 月の中小企業庁の BCP 策定運用指針や金融・建設といった業界別の事業継続にかかわるガイドラインが相次いで公表されたことなどの影響が考えられる。しかしながら、このような動きは、わが国に特化したものではない。米国では、対テロリスト対策を機に発足した米国土安全保障省 (Department of Homeland Security(DHS)) を中心とする取組みの中で、事業継続に関連する情報提供や支援が推進されている。英国やシンガポールなどにおいても、規格やガイドラインの整備が行われている。また、国際標準化機構(International Organization for Standardization(ISO))においても、危機管理体制(Emergency Preparedness)という言葉が使われているが、やはり事業継続に関連する規格策定を検討する委員会が活動を開始した。このような事業継続に関連した活動は、決して新しいものではない。以前からその必要性認識と共に続けられてきた取組みではある。しかし、そのスピードが加速している。これは、世界各国で、次々に発生している大規模災害への脅威や対テロ対策への取組みの中で、事業継続が重要なものとして位置付けられるようになってきたことの現れであろう。

さらに、社会経済的側面から事業継続の取組みに影響する動きとして、リスクマネジメントへの関心の高まりが上げられる。2002 年 7 月に米国で制定された Sarbanes-Oxley (サーベンス・オクスリー) 法 (通称 SOX 法) に続いて、わが国でも企業が開示する文書の虚偽記載や内部統制に関する事項を規定した金融商品取引法が 2008 年 4 月から施行される予定である。金融商品取引法は、財務報告の正確性に主眼が置かれているが、これより先、2005 年 6 月の法改正により成立した会社法 (新会社法とも呼ばれる) では、さらに対象範囲が広いと言われる、業務の適正性を確保するための体制作りが義務付けられた。会社法は、2006 年 5 月から施行されている。金融商品取引法と会社法のそれぞれにおいて規定されている内部統制に関する部分を総称して、一般的に『日本版 SOX 法』と呼ぶ。それぞれ規定の対象や範囲は異なるが、日本版 SOX 法の背景として、社会が要求しているのは、企業等の組織のリスクマネジメントが、適正に行われることである。実際、米国の SOX 法の要求事項に企業等の組織が適合するために参照する

「COSO 内部統制フレームワーク」という 1992 年にトレッドウェイ委員会組織委員会（The Committee of Sponsoring Organizations of the Treadway Commission）が作成したガイドラインがあるが、2004 年にはそれを拡張するかたちで、「COSO-ERM フレームワーク」が公表されている。ERM というのは、エンタープライズ・リスクマネジメントの略で、経営上の戦略策定や意思決定をリスクの視点から行うという考え方である。「COSO-ERM フレームワーク」では、リスクマネジメントを、「事業体の取締役会、経営者やその他構成員によって実施される一連の行為（プロセス）であり、戦略設定において事業体横断的に適用され、事業体に影響を及ぼす可能性のある潜在事象を識別し、リスクをリスク欲求（risk appetite）内に収めて管理し、事業体の目的の達成に合理的な保証を提供するものである」と定義している。ERM が対象とするリスクには、自然災害リスクも含まれており、従来から地震対策を中心として発展してきた危機管理の発展形としての事業継続と、互いに重複する問題を取り扱う。また、事業継続の概念を広く経営の継続性として捉える場合には、リスクマネジメントとの接点はより広くなるであろう。いずれにしても、SOX 法や内部統制というキーワードで高まってきたリスクマネジメントへの関心は、危機管理とは言え、同じように事業にマイナスの影響を与える事象を取り扱うことの重要性を経営層に再認識させ、BCP の取組みについての関心を増大させるであろう。

## 1.2 新たな脅威への挑戦

事業継続は、どのような事件や事故は発生するかを想定せずに、インパクトの分析から入るのが基本的な考え方であるという主張がある。

BSI（英国規格協会）が発行した PAS 56「Guide to Business Continuity Management」<sup>1</sup>などがその一例である。同ガイドによると、BCP や BCM は次のように定義されている。

BCP・・・潜在的損失によるインパクトの認識、実行可能な継続戦略の策定と実施、事故発生時の事業継続を確実にする事業計画

参考 事故発生時の使用に備えて開発、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計画の成果物が事業継続計画（BCP）である。

---

<sup>1</sup> 現在は、英国規格 BS25999 に移行済。

BCM・・・組織を脅かす潜在的なインパクトを認識し、利害関係者の利益、名声、ブランド及び価値創造活動を守るため、復旧力及び対応力を構築するための有効な対応を行うフレームワーク、包括的なマネジメントプロセス<sup>2</sup>

この定義に従うと、“潜在的損失によるインパクト”であるから、「たとえば、震度 xx の地震では」と言うのではなく、「何が起こるか分からないが、何か起こったとして、本社ビルに一人も入ることが許されなかったら」というシナリオからスタートし、事業へのインパクトを考え計画を策定する。このような考え方に基づいて計画を策定しておけば、2001 年 9 月 11 日の同時多発テロのように、ほとんどの人が予測していなかった事象が発生した場合にも、計画が活用できるという。しかしながら、やはり何らかの事象を想定しないと計画を考えるのは難しいという意見もある。本調査研究報告で取り上げた「パンデミック・インフルエンザ」は、まさにその脅威が顕在化した場合に起こりうる状況を想定しなければ、役に立つ計画を策定できない種類に属するものであろう。実際に、英国政府の取組みの中でも、「パンデミック・インフルエンザ」は、“特定のリスク”という範疇に入るものとして、取り扱われている。その特徴は、次の 2 つの指摘が端的に表している<sup>3</sup>。

- 1 ほとんどの BCP は、通常の事業形態に 30 日以内にもどることを想定している。
- 2 一般的な計画では、事業を復旧するために、損害が生じた場所を出て、第二のサイトに移ることを要求している。

「パンデミック・インフルエンザ」の発現を想定して考える事業継続計画は、これまでの事業継続計画と大きく異なる。この 2 つの仮定が、「パンデミック・インフルエンザ」の場合は、成り立たないというのである。2007 年 2 月 6 日時点で、全世界規模で、すでに 272 名の感染者と 166 名の死亡者を出している鳥インフルエンザという、新しい脅威に対して、英国と米国政府を中心に、どのような取組みが推進されているかについては、本報告書の第 6 章で取り上げた。

---

<sup>2</sup> PAS56:2003 日本語版 Guide to Business Continuity Management--事業継続管理のための指針 p1

<sup>3</sup> 「The Greatest Threat of Our Lifetime...or Not?」, Regina Phelps, Disaster Resource Guide 2006-2007, pp. 70.

## 2 事業継続関連の国内外の動向

### 2.1 米国の現況

米国では従来の災害復旧計画（DRP: Disaster Recovery Plan）から、対象範囲を業務プロセスや人的手配にまで広げ、また災害や障害・事故が起こる前の段階も対象とする事業継続管理が官民間問わず浸透・定着しつつある。この背景にはこれまで米国が経験したテロ攻撃、地震・ハリケーンなどの自然災害、大規模停電での教訓が個別企業のみならず、自治体や政府にまで浸透しているということがある。

#### 2.1.1 事業継続の導入状況

個別企業における事業継続計画インセンティブとして、まずは取引先から要求される場合、次に監督当局などから要求されている場合、そして業界として事業継続計画のガイドラインを制定している場合などに分類できるが、半導体製造業や金融業など業界全体で事業継続管理に関するレベルを向上させないと、ビジネス機会が国外に流出してしまうという危機感から取り組んでいるケースも見られる。

事業継続計画に関わる標準・ガイドラインとして NFPA1600<sup>4</sup>が公開されている。この NFPA1600 は、米国連邦・州政府機関を中心に導入が進みつつある。しかしながら、企業などの組織では、実際には上述の、主要取引先が要求してきているガイドラインや、コンサルティング会社が提供する方法論に沿った取り組みを行っており、全般的には NFPA1600 というよりも、米国 DRII<sup>5</sup>や英国 BCI<sup>6</sup>の方法論やガイドラインを参照している。実際の事業継続性についての認証は、監査法人も高リスクと判断しており、現段階では認証を行う制度やシステムは存在していない。

行政・自治体においては、中でも特にニューヨークを始めとする都市型の自治体における事業継続管理は、行政サービスの事業継続性の維持に対する高い意

---

<sup>4</sup> NFPA : National Fire Protection Association（全米防火協会）。  
<http://www.nfpa.org/assets/files/pdf/nfpa1600.pdf> で入手可能

<sup>5</sup> NFPA1600 の現行版に関与、また金融関係当局検査のマニュアルである FFIEC のハンドブックも DRII の手順を参照している。DRII の詳細は <http://www.drii.org/>参照。

<sup>6</sup> 1994 年設立の非営利団体。詳しくは <http://www.thebci.org/>参照。PAS56 の原案を BSI（British Standard Institute: 英国規格協会）と共同で作成。

識と、地元企業との協調という観点から日本の自治体も学ぶべきところは多いと考える。行政として地域のレジリエンスを保持・向上するためには地元企業との連携は不可欠であると位置付け、通常の連絡や訓練・ドリルへの相互参加などを通じて、事業継続計画や事業継続管理の共有化を図ろうとしている。例えばニューヨーク市では、“READY NEW YORK”といった中小企業向けの緊急事態準備計画のハンドブックを公開するといった行政サービスはもちろんのこと、地元産業とも言える金融業と NPO を介して、企業が緊急時に優先的に事業継続に必要な人員や車両を配備できるような仕組み（CEAS: Corporate Emergency Access System<sup>7</sup> 企業緊急時アクセスシステム）<sup>7</sup>を導入したりするなど、積極的に地域レジリエンスの強化を図っている。

一方、広域災害に目を転じると、米国の連邦制度と州、群（カウンティ）、市町村といった行政の階層構造による指揮命令系統の混乱や、組織体制の非効率性などによる不必要な被害の拡大を指摘されるケースも散見され、行政側の事業継続については、その構造的な問題点に関する議論が始まっている。

### 2.1.2 標準化の動向

NFPA1600 を米国規格協会（ANSI : American National Standards Institute）と米国防火協会（NFPA : National Fire Protection Association）が制定。オリジナルは 1995 年の”Recommended Practice for Disaster Management”で、その後 2000 年の改訂を経て、“Standards in Disaster/Emergency Management and Business Continuity Programs”が 2004 年に発行された。同標準は、パブリック・コメントを実施した後、2007 年 2 月に改訂されている。また、この NFPA1600 は、ISO 化のベースとして持ち込まれている。内容は表 1 の通り大きく 5 章に分かれるが、全体の構成として別添資料の方が本体部分よりページ数もかなり多い、即ち本体ではフレームワークだけを示して、別添資料で詳細を参考として提示するというアプローチを採用し、NFPA1600 の導入を検討する組織の形態や業態などによって自己判断の部分を増やし、あらゆる組織が状況に応じて対応できるような柔軟性を持たせる意図が確認できる。

---

<sup>7</sup> BNet : 予め登録された人員・車両は、緊急時に封鎖された地域にも市の判断で優先的に入ることができる仕組みを提供する NPO。毎月のデータ更新と、緊急車両搭載のバーコードリーダーで読み取れるような専用カードを発行する。ボストン、アトランタといった他都市にも展開中。詳細は、<http://www.bnetinc.org/home.html>

表 1 NFPA1600 の項目

|       |                |
|-------|----------------|
| 第 1 章 | 運営             |
| 第 2 章 | 参考文献           |
| 第 3 章 | 定義             |
| 第 4 章 | プログラム・マネジメント   |
| 第 5 章 | プログラム要素（エレメント） |
| 添付資料  | A,B,C,D,E      |

### 2.1.3 現地の状況

#### (1) 事例：SUNGARD 社

米国における事業継続関連の商品・サービスのうちデータ・センターやワーク・スペースの提供の約 60% を SUNGARD<sup>8</sup>、IBM、HP が占めると言われている。その中でも SUNGARD 社は、もともと証券業界向けの情報及びシステム提供ベンダーであったが、コンピュータ関連のリース業からバックアップサイト運営に事業を拡大した COMDISCO 社を買収して現在の業態になっている。その SUNGARD 社は、“information availability services” と自らのサービスを位置付け、顧客企業のビジネスの可用性を上げると同時に、その分野におけるアウトソーシングの投資対効果の向上に努めようとしている。米国と欧州に約 60 のデータ・センターを保有、従業員用ワーク・スペースも 2 万シート以上、ネットワークも総計約 25,000 マイル、また移動式データ・リカバリーセンターも 50 台以上保有するなど、継続的な投資をしながら積極的にビジネスを展開している。

SUNGARD 社はサービス・ラインを

- ① システム・リカバリー
- ② エンド・ユーザー・リカバリー
- ③ モバイル・リカバリー

の 3 分野に分けてサービスを強化しており、特に②については通常の業務や

---

<sup>8</sup> 日本では NEC と業務提携。

コールセンターなど、従来のシステム部門やデータ・センター以外の業務や電子メールシステムといった通常業務の継続には欠かせない機能の可用性強化を主眼としている。

## (2) 事例：ニューヨーク大学/INTERCEP

ニューヨーク大学は米国国土安全保障省（DHS：Department of Homeland Security）からの資金援助を受け、企業の緊急事態準備や事業継続に関する調査・研究及び教育を行う目的で INTERCEP（International Center for Enterprise Preparedness）<sup>9</sup>を設立済。現時点では、全米の主要都市を巡回しながら、2日間で NFPA1600 の解説と組織への導入に関する普及・啓発を行っている<sup>10</sup>が、2007年を目標として修士課程を創設すべく準備を進めている。

現在、INTERCEP が展開しているセミナーの内容は次の通り、NFPA1600の内容を中心に据えている。

第1日目：エグゼクティブ・フォーラム（この日のみの選択も可能）

NFPA1600 の項目を通じた：

- ・ 緊急事態準備と事業継続プログラムの重要要素の認識。
- ・ プログラム導入あるいは更新に必要なマネジメント体制の定義。
- ・ リスクの優先度決定と経営資源の配賦についての議論。

第2日目：監査と評価

NFPA1600 の項目を通じた：

- ・ 効果的な監査の方法についての評価。
- ・ 各要素の正確な解釈と監査の実施。
- ・ 他の監査項目と NFPA1600 に関する項目との統合。
- ・ 事業継続計画改善のための評価結果の経営陣へのコミュニケーション。
- ・ 効果的な NFPA1600 導入評価によるビジネス上の価値認識。

また、2006年4月には事業継続に関わる国際標準（ISO）化にかかわる議論（IWA：International Workshop Agreement）を米国規格協会（ANSI：American National Standard Institution）と共同で主催、ニューヨーク大学のイタリア・

---

<sup>9</sup> 詳細は <http://www.nyu.edu/intercep>

<sup>10</sup> 米国内の各都市で行われているセミナーの詳細は、<http://www.nfpa.org/catalog> 中に掲示。

フィレンツェ校にて事前に ISO 化の原案を提出した主要国（米国・カナダ、英国、オーストラリア、イスラエル、日本）他、各国からの参加者の議論をとりまとめた。

その後も、民間企業の事業継続から重要社会インフラ防護や国家安全保障にまで対象範囲を広げた Round Table 会議を継続する一方、ニューヨークでは保険業界、弁護士業界など業種に特化した議論を主導しつつある。

### (3) 事例：MIT（マサチューセッツ工科大学）

2002 年から 2005 年にかけてマサチューセッツ工科大学（MIT）の輸送・補給センター（CTL: Center for Transportation and Logistics）で、企業のセキュリティやレジリエンシーに関する経営指針、モデル、理論を研究するプロジェクトが展開された。研究では、サプライチェーンを中心とした経済インフラに対するテロ攻撃の可能性とその攻撃による被害についての討議が展開されたが、研究が進むにつれ、テロのみならず多様な災害・事故・事件に調査範囲を広げる必要があることが明白になってきたようである。その背景には、地震、洪水、火災などの多くの偶発的現象はテロ攻撃と同様に大きな被害を企業に与える、と認識されたことがある。この調査研究では次のような論点を中心に検討を進めている<sup>11</sup>。

- ◆ 企業は各種脅威の優先順位付けと定義を如何にすべきか。
- ◆ 大きな被害が出る災害・事故・事件に共通する特徴はなにか。
- ◆ 企業は災害・事故・事件のタイプを知らずに、対策を準備できるか。
- ◆ 企業は脆弱性を増加させずに、業務のスリム化を行えるか。
- ◆ 計画的な攻撃は、事故や偶発的現象と本質的に異なるか。
- ◆ 同時に数多くの出来事が起こる日常業務の中で、災害・事故・事件はどのように察知されるか。
- ◆ しなやか性を持つ企業になるために柔軟性をどのように構築するか。
- ◆ 企業は常に同一材を複数のサプライヤから購入すべきか。
- ◆ 新しいリスクやテロが共同活動にどのような影響を及ぼすか。
- ◆ しなやか性が企業文化に与える役割は何か。
- ◆ セキュリティへの投資と企業のミッションとの関係はなにか。また、コスト面での正当化に必要なものはなにか

本研究を継続している CTL の統括ディレクターの Sheffi 教授によれば、事業継続や

---

<sup>11</sup> Yossi Sheffi 著、The Resilient Enterprise より引用。日本語版は「企業のレジリエンシーと事業継続マネジメント」（日刊工業新聞社）。

レジリエンシーよりも、セキュリティを最優先する政府は、この分野において企業を支援するような活動はほとんど行っていないため、今後は事業継続やレジリエンシーに関わるリスクの計量化やモデルの開発が急がれるとのことであった。

## 2.2 英国の現況

### 2.2.1 事業継続計画の導入状況

米国よりも早い時期から IRA などのテロ攻撃を受けてきた経験のある英国でも、やはり 2001 年の米国同時多発テロを機に、各組織の事業継続計画への取組みは更に促進された。また、これは英国に限ったわけではないものの、英国では特に企業たるものゴーイング・コンサーンとして、成長を続けなければならないという経営者の意識と、企業に投資する投資家や取引を行う取引先や就職する従業員が長期的な継続性をより求めているという背景が強いという観察もある。

事業継続計画の導入状況は官民共に積極的に取り組んでおり、特に民間企業は BS25999 (PAS56 が 2006 年に英国規格化された) や BCI のガイドライン (共に後述)、自治体は Civil Contingency Actなどをベースに事業継続管理体制構築を展開している。

### 2.2.2 標準化の状況

#### (1) BS25999

英国では、BCI (Business Continuity Institute) と英国規格協会 (BSI : British Standards Institution) が 2003 年に公開した事業継続管理に関わるガイドラインである PAS56<sup>12</sup> が標準化の中心となっていたが、パブリック・コメント期間を経て 2006 年 11 月にその一部が英国規格 BS25999 として公開された<sup>13</sup>。

BS25999 は、二つのパートに分かれ、パート 1 が指針、すなわち自己認証用 (code of practice) で、2006 年 11 月に公開された部分である。パート 2 は、第三者認証用の仕様 (specification) となっており、2007 年中に公開される予定である。いずれも、初心者向けガイドラインではなく、事業継続の専門家もしくは担当者が参照する実務化向けの内容となっている。その特徴は、ライフサイクル

---

<sup>12</sup> PAS : Publicly Available Specification、一般仕様書。パブリックコメントの期間を経て、英国標準 (BS : British Standard) となった段階で、PAS は消滅する。

<sup>13</sup> BS: British Standard

を考えたモデルになっている点で、訓練やテストを重視している。

将来的には、3年から4年ごとに、利用者のコメントを反映する更新を行っていく予定になっている。また、CEN規格<sup>14</sup>、ISO規格へと発展させることを目指しており、更新はそのための活動の一環とも言える。規格作成のための委員会は、各国の規格化動向に精通し、国際化を志向した規格作りを行っている。

BS25999の対象は行政・自治体といった公的機関と民間企業であることが明記されており、更に次のような分野と統合的に連関するものであると位置付けられている。

- ① リスク・マネジメント
- ② ディザスター・リカバリー（災害復旧）
- ③ ファシリティ・マネジメント（施設管理）
- ④ サプライ・チェーン・マネジメント（SCM）
- ⑤ 品質マネジメント
- ⑥ 健康と安全
- ⑦ ナレッジ・マネジメント
- ⑧ 緊急時マネジメント
- ⑨ セキュリティ
- ⑩ 緊急時コミュニケーションと広報

また、BS25999-1の内容構成としては次の通り、事業継続管理体制を構築・運営する手順がとりまとめられている。

- 第1章 スコープと適用性
- 第2章 用語の定義
- 第3章 BCMの解説
- 第4章 BCMポリシー
- 第5章 BCMプログラムマネジメント
- 第6章 組織の認識
- 第7章 事業継続戦略の策定
- 第8章 BCM体制の設計と導入

---

<sup>14</sup> CEN: European Committee of Standardization(ヨーロッパ規格)

第9章 BCMに関わる演習、維持、マネジメントレビュー

第10章 BCMの組織文化への定着

事業継続管理（BCM）プログラム・マネジメントは、「組織の理解」、「BCM戦略の定義」、「BCM対応の開発と導入」、「訓練、維持及び見直し」4つプロセスから構成される。その特徴としては、図1に示すように、どこから着手してもよいような仕組みになっている点が挙げられる。

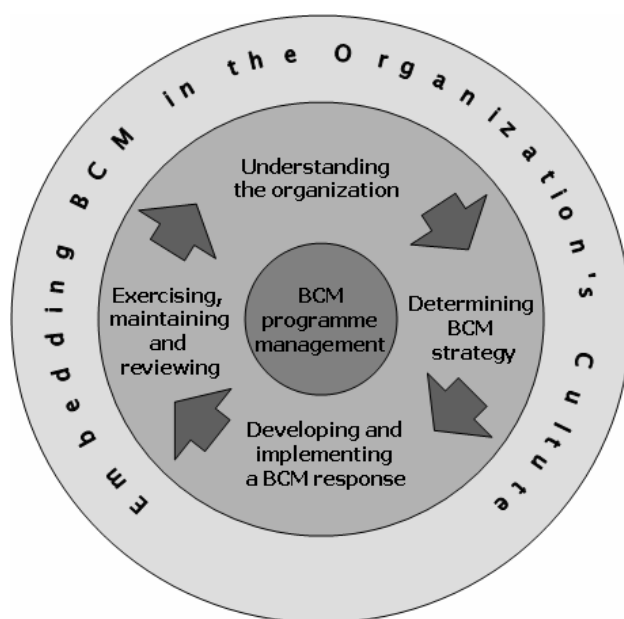


図1 BCMプログラム・マネジメント

(2) PAS77 (IT Service Continuity Management)

2006年8月、ITサービスの事業継続に関するPAS77 (IT Service Continuity

Management Code of Practice(ITSCM))が公開された<sup>15</sup>。事業の継続を脅かすサービスの中断に備えてインシデントの発現前と後の両者について、IT サービスのパフォーマンスを保護するためのシステムである。これを導入することにより、組織は、脅威を最小限に抑え管理するための準備ができるとしている。

次のような目次で構成されている<sup>16</sup>。

- ・ スコープ
- ・ 用語と定義
- ・ 略語
- ・ IT サービス継続管理 (ITSCM)
- ・ IT サービス継続戦略
- ・ 組織のリスクを理解する
- ・ 事業の危険状態の管理／リスク評価
- ・ IT サービス継続計画 (ITSCP)
- ・ ISCP のリハーサル
- ・ ソリューション・アーキテクチャーと設計上の考慮事項
- ・ 継続サービスの購入

PAS77 は、ISO20000<sup>17</sup>や ITIL<sup>18</sup>とも関連している。

### (3) 英国 BCI-Good Practice Guideline

英国 BCI が 2002 年に公開した事業継続計画ガイドラインを 2005 年に改訂したもの。多くの欧米企業が参照している。BCI が提唱するプログラムマネジメントの流れを図 2 に示したが、まず自らの組織の業務やビジネスの可視化から始まり、中長期的にプログラムとして回すことを主張している。

---

<sup>15</sup> PAS77 は、BSI ジャパンで入手できる。(http://asia.bsi-global.com/Japan/index.xalter)

<sup>16</sup> <http://www.standardsdirect.org/pas77.htm> を参照。筆者訳。

<sup>17</sup> 「ISO20000-1: IT サービスマネジメント サービスマネジメントの仕様」および「ISO20000-2: IT サービスマネジメント サービスマネジメントの実施標準」から構成され、ISO20000-1 は、第三者審査登録に使用される。すでにわが国でも JIPDEC パイロット認定などが行われている。

<sup>18</sup> IT Infrastructure Library の略で、IT の運用管理に関して体系的にまとめたガイドライン。

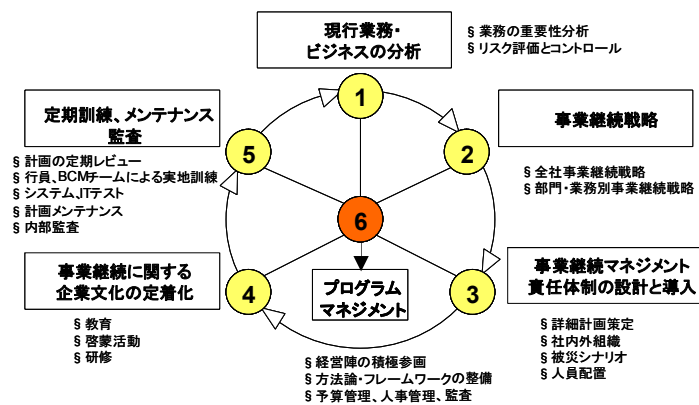


図 2 英国 BCI が提唱する事業継続のプログラムマネジメント

また、BCI の教育部門では、ここに来て急増した大学などの高等教育機関からの要請に応えるべく、事業継続管理に関するシラバス（講義要綱）の雛形を公開している。表 2 はその概要を示しているが、基礎入門レベル（Foundation）、検定レベル（Certificate）と学位レベル（Diploma）の 3 段階で構成され、特に学位レベルでは実際の現場での適用経験が単位として勘案されるなど、実践重視の設計となっている。

表 2 BCI が提供する事業継続管理に関わるシラバス（講義要綱）の雛形

|    | Module title                                                                | Foundation | Certificate | Diploma  |
|----|-----------------------------------------------------------------------------|------------|-------------|----------|
|    | 1 unit = c.6hrs teaching time                                               | 6 Units    | 10 Units    | 20 Units |
|    | Introduction to BCM                                                         | 1          | 1           | 3        |
| 1  | Initiation and Management                                                   | 0.5        | 1           | 2        |
| 2  | Business Impact Analysis                                                    | 0.5        | 1           | 2        |
| 3  | Risk Evaluation and Control                                                 | 0.5        | 1           | 1        |
| 4  | Developing Business Continuity Management Strategies                        | 1          | 2           | 2        |
| 5  | Emergency Response and Operations                                           | 0.5        | 1           | 2        |
| 6  | Developing and Implementing Business Continuity and Crisis Management Plans | 0.5        | 1           | 2        |
| 7  | Awareness and Training Programmes                                           | 0.5        | 1           | 1        |
| 8  | Maintaining and Exercising Business Continuity and Crisis Management Plans  | 1          | 1           | 2        |
| 9  | Crisis Communications                                                       |            | 0.5         | 1        |
| 10 | Coordination with External Agencies                                         |            | 0.5         | 1        |
|    | BCM Activity Logbook                                                        |            |             | 2        |
|    | Assignment                                                                  |            |             | 5        |
|    | UNITS                                                                       | 6          | 10          | 20       |
|    | TEACHING HOURS                                                              | 36         | 60          | 90       |

The Business Continuity institute, Academic Syllabus 2005

### 2.2.3 現地の状況

特に、公的機関では、Civil Contingency Act と連動していることから、BS25999 を基盤とした取り組みが進んでいる。また、金融機関においても当局による規制により、事業継続への関心は高い。事業継続に関心の高い産業分野としては、これらの他に、IT 産業や小売業などがある。IT 産業は、すでに情報セキュリティへの取り組みが進んでおり、その基板上にある事業継続への取り組みが行われているのである。小売業は、サプライチェーンの事業継続の側面で必要性が認識されている。

## 2.3 日本の現況

### 2.3.1 事業継続計画の導入状況

わが国においても、内閣府や経済産業省によるガイドラインの発行、ならびに中小企業庁による「中小企業の BCP 策定運用指針」の公表など、政府機関による推進活動が活発に行われている。

(1) 経済産業省「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」

2005 年 3 月の公開後、約 2 年を経過したことから、内容の見直しを目的とした有識者委員会を設置、2006 年度内の一部改訂を予定している。

(2) 内閣府「事業継続ガイドライン」

2005 年 8 月の公開後、さまざまな企業での導入が進みつつあるが、ガイドライン本体（第 1 版）はそのままとし、解説書を発行すべく企業等の事業継続・防災評価検討委員会を設置、議論を展開している。その中では、解説書に関する議論に加え、「防災に対する企業の取組み」自己評価項目表の第 2 版や、防災報告書の作成に関するガイドラインの公開も併せて検討されている。

(3) 中小企業庁「中小企業 BCP 策定運用指針」

2006 年 2 月の WEB 公開後、中小企業庁と各地の商工会議所による全国展開が開始された。このような動きは各地域独自の取組みに繋がってきたケースも見ら

れ、例えば東京商工会議所では、中小企業の企業防災の観点から業務データを沖縄のデータセンターにまとめてバックアップする実証実験を、100 社近い参加企業で行っている。

さらに、産業界においても様々な取り組みが始まっている。金融機関では、IT に関するコンティンジェンシー・プランを中心とした計画策定が進められてきた。また、建設業界でも災害時における建設会社の事業継続が必要不可欠という認識からガイドライン<sup>19</sup>が作成され、企業等で事業継続計画が作成されているところである。その他、百貨店業界、電子情報業界、情報通信業界、損保業界などでもガイドラインの策定に着手または検討中の状況である。

### 2.3.2 標準化の動向

国際標準化機構（ISO）において、事業継続に関連する危機管理体制（Emergency Preparedness）の国際規格化を議論する会議が始まったのを受け、わが国でも国内の委員会を立ち上げて、わが国のガイドライン等と国際規格との整合を図っている。

2006 年 2 月中旬には、日本原案を作成したが、その主な論点は次のようにまとめられる。

- ① 継続的改善の仕組みは必要であるものの、第三者認証制度にはそぐわない。
- ② 災害発生直後に公的組織が第一義的に行う活動や重要インフラ業務は対象外とする。
- ③ 対象とするリスクは各組織が合理的な基準に基づき自主的に選択するものとする。
- ④ 広域災害においては、被災した地域の復旧計画との連携・調整に留意する。

### 2.3.3 経済的インセンティブに関する動き

2006 年 4 月に、日本政策投資銀行は、防災格付けによる金利優遇制度を開始した。これは、企業などの組織における防災への取り組みに対して、経済的イン

---

<sup>19</sup> 詳細は、[http://www.bousai.go.jp/kigyov-machi/jigyoku-keizoku/2nd/handout\\_5-1.pdf](http://www.bousai.go.jp/kigyov-machi/jigyoku-keizoku/2nd/handout_5-1.pdf)などを参照。

センティブを与える世界初の制度である。

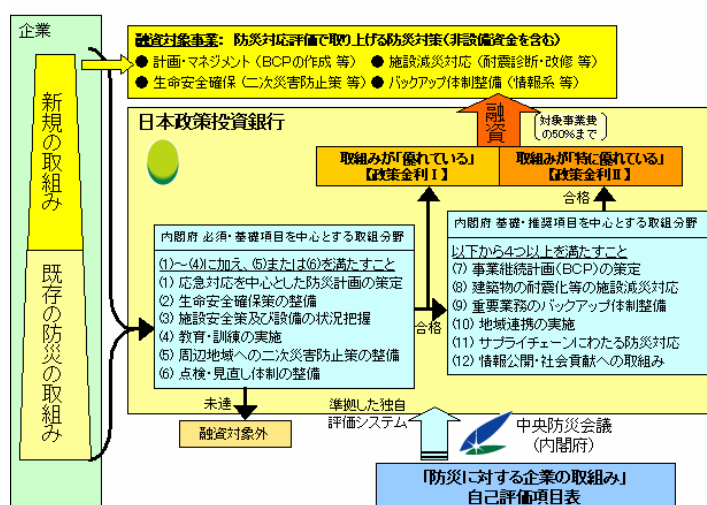


図 3 日本政策投資銀行の防災格付け制度

日本政策投資銀行によるこの制度は、従来の財務・信用状況に加え企業防災への取組みの評価を金利に反映するもので、2006年4月に第1号融資が実施された（安田倉庫）。また、その後も実績は着実に積み上がっており、業種も不動産、ホテル、データセンターなど多岐に亘り、中には資金調達力はあるものの、この融資制度を通じて格付けを取得したいという意向が見られる融資先も出てきている。

この融資制度は中央防災会議「防災に対する企業の取組み」自己評価項目表をベースとして格付けシステムを構築しており、防災への取組みが進めば、より低利の金利が適用される。さらに、保険分野でも損保ジャパン(株)が防災格付による保険料引き下げの商品を導入するなど、BCM では先をゆくと言われてきた欧米に先駆けて、日本でこのような経済的なインセンティブを導入する動きが活発化していることには欧米も注目をしている。

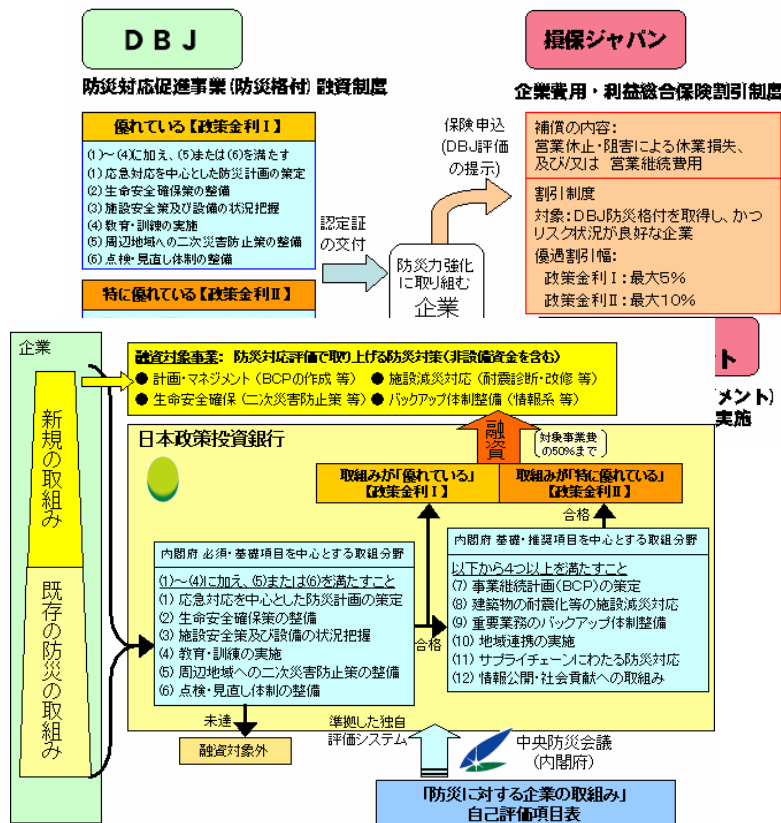


図4 日本政策投資銀行の防災格付を利用した損保ジャパンの保険割引制度

## 2.4 ISO化の動向

### 2.4.1 ISO化の概要とスケジュール

2006年4月、危機管理体制(Emergency Preparedness)に関する国際規格化の会議が開催された。13カ国からの出席者により、さまざまな視点からの意見

が提示された。会議に先立ち、米国・カナダ（NFPA1600）、英国（PAS56→BS25999）、オーストラリア（HB221）、イスラエル、日本から原案が提出された。日本の原案は、既存のガイドライン（経済産業省、内閣府など）と産業界からの意見を統合して作成したものであった。会議では、事業継続の概念の整理、各ステークホルダー間の差異・共通点を中心に議論がなされたが、国、組織により事業継続の認識や国際標準化に対するスタンスは異なり、まとまった合意には至らなかった。

その後、ISO では、2006 年 11 月に、Societal Security(社会セキュリティ)について議論する技術委員会 TC223 が発足し議論を再開した。この TC223 の元に、3 つのワーキンググループ（WG）が設置され、その中の WG1 の傘下に置かれたタスクグループ 1（TG1）において、この事業継続体制マネジメントに関わる国際標準化についての議論が行われてきたが、これまで、5 カ国から提出された原案を統合した最終原案を ISO の PAS として議論を進める方向で準備がなされている。

このような議論の過程において、そもそもの事業継続計画（BCP）や事業継続マネジメント（BCM）といった対象から、IWA<sup>20</sup>のスタート時には EP（緊急時の備え）に置き換わったのは、会議を主催した米国の ANSI（米国規格協会）と NYU(ニューヨーク大学)の INTERCEP(International Center for Enterprise Preparedness)のうち、特に後者は米国国土安全保障省から援助を受けていることで、「有事に向けた事前準備」の色を濃くしていたものと考えられる。

IWA では、これまで先進国の企業が慣れ親しんだ BCP/BCM の方がよろしいのでは、という議論もあったが、公的機関も含めるという議論を通じて、最終的には EP でもなく Operational Continuity という言葉が再定義され、現在の TG1 を引継いだ議論では、IPOCM(Incident Preparedness and Operational Continuity Management)という用語でドラフトがとりまとめられつつある。

---

<sup>20</sup> IWA: International Workshop Agreement の略。NYU（ニューヨーク大学）の動向については、本書の「2.1.3 現地の状況」で説明。

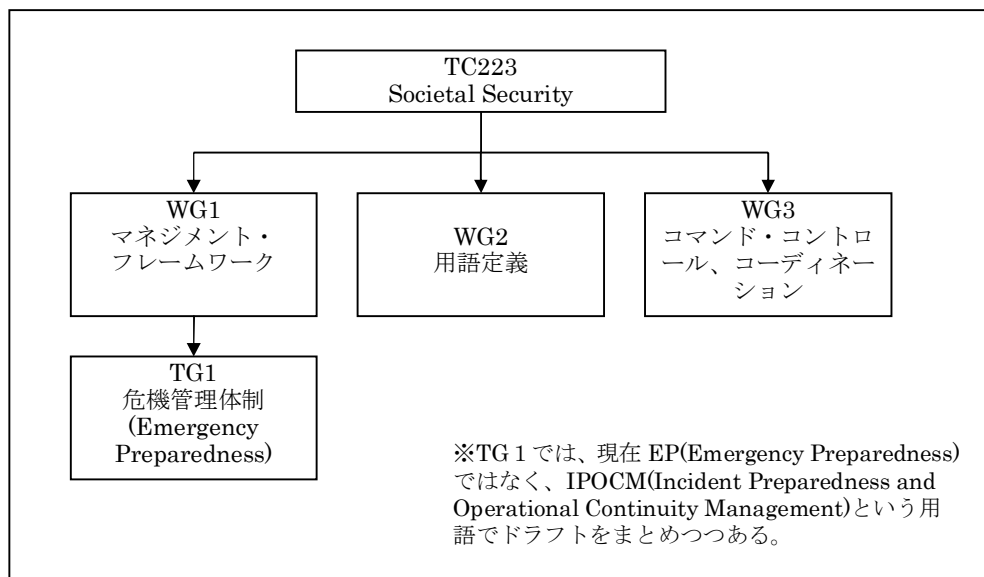


図 4 ISO/TC223 の構成

一方、WG1 ではこの PAS を議論するトラック（TG1 の作業）を切り離れた形で、Societal Security（社会セキュリティ）に関する国際標準化において、何をどこまで、どのように標準化するかといった大きな枠組みの議論を開始している。

### 3 事業継続に関する企業・業界の取組み

本章では、事業継続に関する取組みを個別企業と業界レベルのふたつの観点でまとめる。事業継続マネジメントの導入に積極的な金融業界を中心に事例の分析を試みる。

#### 3.1 個別企業の取組み

今回の調査では、欧州系銀行 A 行のロンドン及び東京での取組み、および香港系銀行 B 行の香港及び東京での取組みについてヒアリングを実施した。

##### 3.1.1 事例：欧州系銀行 A 行

欧州系銀行 A 行のロンドンでの活動は、銀行・証券業務を中心に、シティでも主要金融機関のひとつと位置付けられるが、金融ビジネスを重要な都市機能のひとつと位置付けるロンドン市を中心に、金融業界、交通機関、警察も含めた地域コミュニティ型 BCM の取組みを積極的にリードしてきた。その結果、2005 年 7 月に発生したロンドンにおける同時爆破テロの数週間前に、かなり同事件に類似したシナリオに近い演習を地域で主導するなど、単なる金融機関としての機能だけでなく、都市機能を守る地元先進企業としての役割も果たしている。（このような積極的な取組みは、2001 年に発生した米国同時多発テロの際にも奏功し、NY・マンハッタン地区での被害を最小限にとどめ、いち早い業務復旧を果たした。）

その欧州系銀行 A 行の東京支店の 2006 年の事業継続に関わる演習は、ある政府主要機関の建物の爆破予告のシナリオを用い、刻一刻と変化するインジェクション（新たなシナリオ展開の提示）に対して、コマンド・ルームに集結した役員達が関連部署と連絡を取り合い、判断・指示を出すという机上演習であった。その様子をモニターを通して伺える別室には、本国の BCM 責任者をはじめ、外部専門家や有識者、更には警察も招き入れ、最後にそのフィードバックを聴取して次回の演習に活かすというものであった。この演習は真剣そのもので、よく練られた演習シナリオと、「不具合を発見すること」が演習の目的であるということが明確に定義されていたことが、演習結果を意味あるものにする大前提であることを認識させるものであった。

### 3.1.2 事例：香港系銀行 B 行

香港を中心にアジア展開を積極的に行う香港系銀行 B 行は、香港島に本社機能と主要顧客が訪問するオフィスを構える他、九龍にはバックアップサイトと、相互バックアップ・サイト兼代替ワークスペースとなるオフィスの主要 3 拠点を有する。狭い香港という地域ながらも、オフィスワーク用のオフィスとバックアップサイト、そして両方の機能を兼ね備える相互バックアップオフィス（サイト）を持つことで、事業継続マネジメント体制を柔軟的に展開している。

その東京支店の事業継続マネジメントに関する 2006 年の演習は、鳥インフルエンザをテーマにしたもので、計画発動後直ちに本社機能を司る行員はウィルス感染リスクを分散するために 2 つのグループに別れ、一方は本社に残留し、もう一方は予め定められた手順に従い、業務継続に必要な書類や機器を持ち出し、タクシーで代替サイトへの移動を開始する。その後、移動先では業務システムの立ち上げやログインを行い、その状況を確認した。それまでの災害を対象とした演習とは異なり、形のない障害要因が突然、早いスピードで蔓延する、という潜在リスクに対する演習であり、多くの知見が得られたはずである。

## 3.2 業界としての取組み（欧米）

今回の調査で訪れた英国金融サービス機構（FSA: Financial Services Authority）と米国証券業協会（SIA: Securities Industry Association）による業界レベルでの事業継続体制構築の取組みについてとりまとめる。

### 3.2.1 事例:英国金融サービス機構（FSA）

英国金融サービス機構（以下、FSA）は、英国の金融サービスの品質維持・向上や消費者保護の観点から行政指導する権限を持つが、実際のアプローチは金融業会の自主性に委ねる部分が多く、全般的には協業関係にある。その中でも、2005 年に実施された業界横断演習（対テロシナリオによる机上演習）や、事業継続体制に関するベンチマーク調査に引続き、2006 年には引続き業界横断演習（鳥インフルエンザのシナリオによるバーチャル演習）を行うなど、事業継続マネジメントの分野においては、業界全体の取組みを先導する立場にある。

2006 年の事業継続に関わる業界横断演習は前回の 3 日間の机上演習とは異なり、1 サイクル 1 週間（金曜日に FSA がシナリオを提示、各金融機関は週末をまたいで火曜日までにその対応を演習事務局に回答、それを受けて FSA 側では追加

のやりとりを通じながら新たなシナリオの展開を組み込む）を6サイクル、即ち6週間の演習をWEB 掲示版なども使いながら実施された。この6週間というサイクルでは、鳥インフルエンザの人-人感染の発症から蔓延、その後の収束状況に至るまでの期間の22週間が設定され、参加者は金融機関のその監督当局（FSA、財務省、英国銀行）にとどまらず、シナリオ策定側には組織行動論や行動心理学の研究者が、また、演習参加者にはロンドンの交通当局や製薬会社なども含まれ、総勢約3,500名という大規模なものであった。

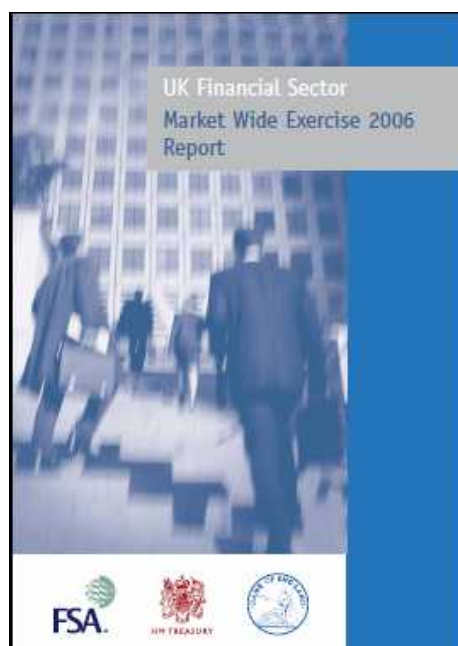


図 5 FSA による業界横断演習 2006 の報告書

FSA の報告書によると、演習中に鳥インフルエンザ感染や隔離などによる欠勤率を15%から49%（部門によっては60%）に上げるようなシナリオを提示するなど、金融ビジネスに関わる業務へのストレスをかけながらその影響を記録していった。その結果、自宅勤務の整備状況や、リテール業務に不可欠な ATM への現金輸送、また監督当局間の連絡体制などに今後の課題が残ったようで、2007 年についても業界内で議論を続けることで業界内レジリエンシーの強化を図りつ

つある。なお、FSA の演習企画責任者によれば、2007 年の業界演習のシナリオも 2006 年と同様の鳥インフルエンザとなる予定である。

### 3.2.2 事例：米国証券業協会（SIA：Securities Industry Association）

ここ数年恒例となった米国証券業協会（以下、SIA）の事業継続に関わる業界横断テストは 2006 年の 10 月 14 日に実施された。参加機関は証券業に関わる、金融機関や市場情報提供会社、決済サービスネットワークや証券取引所である。前述の英国 FSA 主導による業界横断演習とは異なり、SIA の演習は業界が自主的に実施するという位置付けで当局の参加を排除してきたが、2006 年からは SEC（証券取引委員会：Securities and Exchange Commission）も関与し始めた。

演習の目的は、各参加者がそれぞれのバックアップサイトから代替システムを通じてテスト用のダミー取引を実行できるかどうか、というもので大手投資銀行の担当者によれば、「接続テスト」の位置付けであり、極論をすれば証券ビジネスはシステムさえ何とか繋がれば事業継続性が確保できるということのようである。結果分析は前回とほぼ同様の接続上の問題（IP アドレス相違、ファイアウォールの設定ミス、バックアップ用アプリケーションのセットアップミス）や通信業者のサービス上の問題であった。SIA の全体会議に出席した雰囲気では、この接続テストとしての業界横断演習はすでに恒常化しているが故に、参加者が演習を通じて何か新たな発見をしようとする期待感は薄れつつあると見受けられる。

また、これとは別に SIA が実施した BCM に関わる業界内ベンチマーク調査では、次のような結果概要が発表された。

- ◆ SIA 加盟の従業員 500 人以上の証券業 87 社を対象としたベンチマーキング調査
- ◆ BCM 専任は 3 名以下（ただし、大手投資銀行などは 15 名以上）
- ◆ BCM における優先順位は、演習と疫病対策が高順位
- ◆ 米国 SOX 法は最終的には BC 分野の活動には影響なし
- ◆ 危機管理体制として、従業員の自動安否確認システムや、代替要員計画の整備が課題
- ◆ 計画の対象が、重要業務分野から全分野に拡大

## 4 事業継続に必要なスキルと人材

### 4.1 人材・プロフェッショナル育成の重要性

ここでは、事業継続管理体制に必要なプロフェッショナル人材の要件について考えてみたい。まず、現存する事業継続管理関連の資格は主に英国 BCI (Business Continuity Institute<sup>21</sup>) と米国 DRII (Disaster Recovery Institute International<sup>22</sup>) のふたつであるが、これらは個人に与えられるプロフェッショナル資格である。一方、事業継続管理関連のガイドラインや ISO などの標準化の動向に目をやると、こちらは企業や自治体などの組織が遵守・導入するものである。また、個人が取得する BCI、DRII の資格は、フレームワーク (枠組み) を理解・習得しているということよりも、手順・手続きに精通していることを求められ、事業継続管理を実践するコア人材として期待される。

事業継続マネジメント体制の構築には、もちろん組織が何らかのフレームワークを導入し、社内の手順や手続きを制定する必要があるが、それを実行するプロフェッショナル人材が不可欠であることは言うまでもない。このような人材は、社内外の過去の事故・障害事例や各部門や業界団体で記録・分析しているインシデント関連統計データなどを積上げた事業継続計画策定のアプローチ (ボトムアップ) と、重要業務の選定、複数箇所における複合事故・障害の同時・連鎖発生を想定したシナリオに基づくアプローチ (トップダウン) を、確かな知識と経験によって調整することも求められている。

### 4.2 英国 BCI の資格概要

事業継続管理に関する実務経験の専門性と従事期間の長さ、及び後述の 10 のスキル・セット分野の経験範囲により、Fellow・Member・Specialist・Associate・Affiliate・Student・Corporate Partner にランクづけされる。職場での評価や実務経験の査定なども行われ、Fellow については面談も行われる。会員は事業継続管理に関する専門家どうしの情報交換や、研修・トレーニングといった啓発の機会、また会員向けの詳細情報を得る機会を提供される<sup>23</sup> (図 6)。

<sup>21</sup> 1994 年設立の非営利団体。詳しくは <http://www.thebci.org/> 参照。PAS 56 の原案を BSI (British Standard Institute: 英国規格協会) と共同で作成。

<sup>22</sup> NFPA 1600 の現行版に関与、また金融関係当局検査のマニュアルである FFIEC も DRII の手順を参照している。DRII の詳細は <http://www.drii.org/> 参照。

<sup>23</sup> 詳細は <http://www.thebci.org/membershipcriteria.htm> 参照。BCM 関連人材に特化した求人情報も得ることができる。

2006 年の新入会の会員出身国を見ると、特にシンガポールからの入会が目立った。これは、シンガポールが国を挙げて事業継続体制の強化を推し進めており、事業継続マネジメントについては TR19 を、DR・BC のサービスの提供者に対する規格標準 SS507 などを実際に推進する人材の育成に力を入れていることの現れであると考えられる。

| Category          | Summary                                                                                    | Experience                                                                                                   | References                                                    | Competence in BCI Standards                                                                            | Entry Method                                                                    |
|-------------------|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| FELLOW            | Senior / professional working practitioners.                                               | 5 years full time AND currently in a business continuity related profession AND a Member of BCI for 2 years. | 2 required, one of which must be from an appropriate manager. | Thorough knowledge of ALL certification standards.                                                     | By scored assessment & presentation to a structured interview panel of Fellows. |
| MEMBER            | Professional working practitioners.                                                        | 2 years full time & currently in a business continuity related profession.                                   | 2 required, one of which must be from an appropriate manager. | Sound understanding of ALL certification standards.                                                    | By scored assessment based upon evidence supplied by the applicant.             |
| SPECIALIST        | Currently in a business continuity related profession.                                     | 2 years full time & currently in a business continuity related profession.                                   | 2 required, one of which must be from an appropriate manager. | Developing an understanding of 4 of the certification standards and having a specialist qualification. | By scored assessment based upon evidence supplied by the applicant.             |
| ASSOCIATE         | Currently in a business continuity related profession.                                     | Having full or part time experience within the scope of the certification standards.                         | 2 required, one of which must be from an appropriate manager. | Developing an understanding of ALL certification standards.                                            | By scored assessment based upon evidence supplied by the applicant.             |
| AFFILIATE         | An individual expressing an interest in BCM or who is a Member of an associated Institute. | Not applicable but must demonstrate or declare support for BCI aims.                                         | None required.                                                | Not applicable.                                                                                        | Submit an application form.                                                     |
| STUDENT           | Students having an interest in the subject area.                                           | Qualifying course or subject.                                                                                | None required.                                                | Not applicable.                                                                                        | Submit an application form.                                                     |
| CONFESSION        | Directors and senior staff of organisations subscribing to the BCI aims.                   | Professional interest in BCM.                                                                                | None required.                                                | Not relevant.                                                                                          | Nomination to membership secretary is approval by the BCI Board.                |
| CORPORATE PARTNER | Organisations subscribing to the BCI aims.                                                 | Not applicable, but must demonstrate or declare support for BCI aims.                                        | None required.                                                | Not relevant.                                                                                          | Submit an application form.                                                     |

(<http://www.thebci.org> より)

図 6 BCI の会員資格レベル

#### 4.3 米国 DRII の資格概要

BCI の資格と大きく異なるのは、資格試験を課すことである。研修・トレーニングを受講して受験するが、その専門度合いや専門領域によって資格がレベル分けされている。ここでも 10 のスキル・セット分野が基準となるが、これは BCI と共有されているものである（図 7）。

- ① ABCP: Associate Business Continuity Professional  
実務経験 2 年以内の初任者。試験のみ。
- ② CFCP: Certified Functional Continuity Professional  
3 つ以上の専門分野で 2 年以上の事業継続管理実務経験が必要。試験と評価委員会の審査が必要。

- ③ CBCP: Certified Business Continuity Professional  
5 つ以上の専門分野で 2 年以上の事業継続管理実務経験、試験と評価委員会の審査が必要。
- ④ MBCP: Master Business Continuity Professional  
7 つ以上の専門分野で 5 年以上の事業継続管理実務経験。試験と評価委員会の審査が必要。

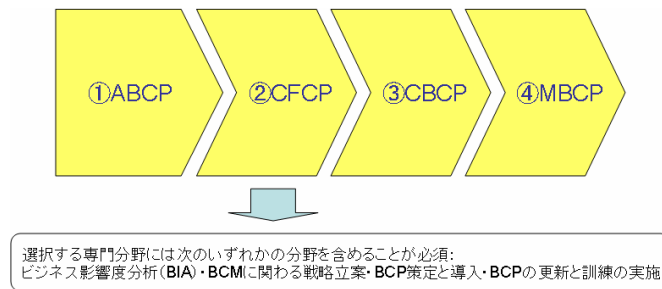


図 7 DRII の資格概要

#### 4.4 事業継続管理に必要なスキル・セット分野

ここでは、英国 BCI と米国 DRII で共有されている、事業継続管理に必要なスキル・セット分野について簡単に解説する。

- ① Initiation and Management (事業継続管理の始動とマネジメント)  
事業継続計画の立案に際し、脆弱性の抽出、及び想定事象に関する対応・リカバリー的能力、継続オペレーションに必要な経営資源配賦にかかわる選択肢の提示などを、重要な機能として提供できること。
- ② Business Impact Analysis (ビジネス影響度分析 : BIA)  
事業継続を脅かす諸要因のビジネス・オペレーション上の影響について定量的・定性的な分析・評価が行えること。またその過程において、強化対策の優先度の高い業務オペレーションの特定、更に RTO (Recovery Time Objective : 復旧目標時間) 設定などが実施できること。

- ③ Risk Evaluation and Control (リスク評価とコントロール)  
事業継続を脅かす諸要因について分析を行うと同時に、リスク対応策や選択肢に係る経済性分析が遂行できること。
- ④ Developing Business Continuity Management Strategies (事業継続マネジメントに係る戦略立案)  
事業継続管理に係る戦略立案において、RTO、RPO (Recovery Point Objective : 復旧時点目標) を設定、重要オペレーションのレジリエンス確保に貢献すること。
- ⑤ Emergency Response and Operations (危機対応と緊急措置の運用)  
障害発生時とその後の復旧プロセスにおける段取りを、危機対応センターを中心とした体制で運用できるよう手配できること。
- ⑥ Developing and Implementing Business Continuity and Crisis Managements Plans (事業継続と危機管理に関する計画の策定と導入)  
事業継続計画及び危機対応計画の立案、導入、定着を支援し、RTOの達成確保を確実にできること。
- ⑦ Awareness and Training Programmes (啓発とトレーニングのプログラム)  
事業継続管理の社内浸透・定着のための研修や諸プログラムについて支援が行えること。
- ⑧ Maintaining and Exercising Business Continuity and Crisis Managements Plans (事業継続と危機管理に関する計画の更新と訓練の実施)  
事業継続計画の実効性を確保するための訓練の計画・実施に際し、必要となる機器・ファシリティの手配を行い、訓練後のフィードバックに対して必要な体制・組織の更改や新規導入の手配ができること。
- ⑨ Crisis Communications (危機広報)  
社内のみならず顧客も含めたステークホルダー(株主、ベンダー、納入業者、地域など)とのコミュニケーションを確実にし、事業継続計画や災害復旧計画(DRP : Disaster Recovery Plan)の発動を確実にすること。
- ⑩ Co-ordination with External Agencies (行政機関との調整)  
監督当局や地方自治体などの行政とのコミュニケーション確保を通じて、事業継続管理を確実にするための側面支援を得たり、コンプ

書式変更: フランス語 (フランス)

書式変更: フランス語 (フランス)

ライアンス上の不必要な瑕疵発生を回避することに貢献できること。

以上、いずれの分野も事業継続マネジメント体制の実効性を高めるには必要な専門分野であり、これに沿って BCI、DRII はそれぞれのアプローチでプロフェッショナル人材育成を推進している。日本からの資格取得者はまだ少ないようだが、外資系金融機関<sup>24</sup>やコンサルティング会社を中心に増加しつつあるようである。

#### 4.5 事業継続に係る職種

参考までに、事業継続管理関連の求人情報から具体的な職種をピックアップし、下記に例示した。

- ① **Business Continuity Relationship Manager**  
事業継続に係るポリシーや戦略立案、事業継続技術マネージャ及び、危機対応マネージャの支援、顧客対応を担当。
- ② **Business Continuity Technology Manager**  
事業継続に必要な情報システムリスクのマネジメント及び、事業継続や危機対応に必要な技術の導入・手配を行う。
- ③ **IT Continuity Analyst**  
情報システム関連資産の統合分析や事業継続のための脆弱性分析を行い、対応策を発案する。
- ④ **Disaster Recovery Coordinator**  
業務機能レベルのリスク分析を行い脆弱性を抽出、災害復旧における選択肢の提示やリスクマネジメントの戦略を立案する。現場のラインマネージャに権限を委譲した上で、コーディネーターがその間をコントロールするという場合に設置される。
- ⑤ **BCM Auditor**  
事業継続管理に係る体制や実務について監査を実施する。

---

<sup>24</sup> 本国を中心にグローバルで BCM 体制を統一しようという意向は、特に 9・11（米国同時多発テロ）以降、強まっている。その一環として在日オフィスにも専門人材を配備、もしくは内製化に着手している。

#### 4.6 事業継続に必要なスキルと人材

以上、事業継続管理の体制構築・運用に必要なスキル・セットの議論を展開したが、最後に事業継続マネジメント全体に係る今後の課題における重要性としてとりまとめを行う。

##### 4.6.1 プロフェッショナル人材育成と事業継続管理体制構築

ここでは実際の企業における人材育成を、企業における BCM（事業継続管理）体制の構築の段階を想定しながら考察する。

###### （１）BCM 体制導入初期

まず、個別企業における BCM 体制の導入初期については、経営者・担当者の認識レベルに合わせて、BCM 導入の必要性や具体的なステップの確認に着手することが出発点として望ましい。これは図 8 で示すような、以後の各段階の大きな骨組みを構築するもので、どの段階にあっても参照する、「原理・原則」として位置付けてもよい。

財団法人 機械振興協会が 2006 年 2 月にとりまとめた『わが国製造業における SCM 及び BCP の実態調査』によると、BCP を策定済という企業のうちの約 4 割が導入のきっかけは取引先からの要請である、と回答している実態を勘案すると、取引先による BCM 体制の要件も考慮する必要も出てくる。しかしながら、事業継続の取り組みは、最終的には自発的なものでなければその実効性は確保されないため、取引先からの要件も考慮しながら、実際の BCM 体制の構築は外部のガイドラインなどをベースに、専門人材の育成も含めて企業自らが愚直に取り組み始めることが肝要である。

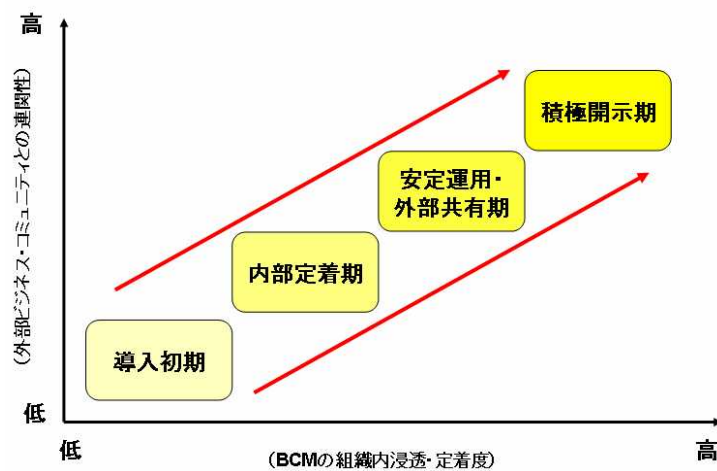


図 8 BCM 体制の構築の段階<sup>25</sup>

## (2) BCM 体制内部定着期

社内への導入が行われた後は、訓練や研修・トレーニングの繰り返しを中心とした内部定着の努力が必要となる。この段階で力尽きると、その後の BCM 体制の構築は危ぶまれ、BCP そのものは、まさに「絵に描いた餅」となってしまう。

この段階で必要なのは、継続的な社内の普及・啓発活動であり、経営陣のコミットメントの継続が不可欠である。BCM 体制構築に必要な BC 計画力は研修・トレーニングにより、また、BC 実行力は訓練を繰り返すことで身をもって覚えてもらう取り組みを定着させることが重要なポイントである。この部分については、普及・啓発活動におけるモチベーションの向上やインセンティブの付与に関してのノウハウ蓄積において先行する欧米の指針・規格を参照することが有用と考える。

また、この段階あたりから、外部のビジネス・コミュニティを意識し始める必要が出てくる。具体的には、ネットワークや SCM（サプライチェーンマネジメント）などを介して外部と情報のやりとりを ICT（情報通信技術）を用いて実施しているよう

<sup>25</sup> 事業継続マネジメント（BCM）構築の実際（小林誠監修、日本規格協会）、第 6 章（渡辺研司執筆）より引用・参照。

な部分についても BCM を強化する必要がある、その際には経済産業省の事業継続策定ガイドラインが参考となる。また、このやりとりには兼業であったとしても、特定の担当者を置くことがその後の展開の礎石となる。

### （３）BCM 体制安定運用・外部共有期

BCM 体制が社内に定着すれば完了ということではなく、PDCA サイクルと同様に、マネジメント・プログラムとして継続的に運用してゆく必要がある。その背景には、企業の経営を取り巻く環境や、ビジネス・業務オペレーションのやり方は常に変化し続けているという現実があることを忘れてはならない。

この段階では経営陣は BCM を日常的な経営のミッションの一部として自らの時間を割り、経常的に予算を配賦し、そして中長期的な人材育成を既にスタートしている必要がある。

また、BCM が個別企業のみでの取り組みだけでは不十分な現実を考えると、企業が属するサプライチェーン内での整合性の確保、同業他社を含めた業界全体としての事業継続の取り組みの中で、自らの BCM 体制の位置付けを調整することが必要不可欠となる。この段階は図 8 で示したように、外部のビジネス・コミュニティとの連関性を強く求められる段階であり、各業界内で策定するガイドラインなどとの整合性を確保することが肝要である。

### （４）BCM 体制積極開示期

BCM 体制が安定運用期に入り、外部との共有体制も構築し、マネジメントプロセスとして回り始めた後は、IR 活動も含め、外部に積極的に開示してゆく段階を迎える。強い問題意識のもとで試行錯誤を経て成熟した BCM 体制を外部に積極的に開示することは、企業のゴーイング・コンサーン（存続し続ける存在）としての継続性を示唆するもので、取引先や投資家からの信頼を向上させ、ひいては企業価値を増強するものである。

また、このような競争優位性を向上させるという効用のほかにも、自らが属するサプライチェーン、業界、また所在する地域コミュニティのレジリエンシー（弾力性のある回復力）を強化に貢献することにもつながり、企業の社会的責任（CSR）の観点からも、今後は経営的にも重要な取り組みと位置付けられるようになるはずである。

この段階まで到達すれば、もはや指針・規格類を活用するというよりも、逆に指針・規格類に影響を及ぼすような先進企業としての位置付けとなる。また、企業内で育成した BCM の専門家についても、外部でもプロフェッショナルとしての活動を開始し、単独の企業では限界のあった、ノウハウや情報の共有や、業界に特化した方法論の開

発など、ひとつの組織から独立した活動ならではの付加価値を生み始めるはずである。

#### 4.6.2 今後の事業継続の課題における人材育成

ビジネス・コミュニティにおける事業継続管理体制の共有化には、共通の方法論導入や標準化が多大な貢献をすることは間違いなく、共通言語として社外とコミュニケーションできるプロフェッショナル人材とその人的ネットワーク<sup>26</sup>が必要となる。

日本でこのような専門家ネットワークもひとつの目的として構築されたのが、特定非営利活動法人の事業継続推進機構（以下、BCAO）であるが、BCAOは2007年2・3月にかけて、事業継続に関わる資格制度を展開することになっており、初級を皮切りに上級、また、緊急時の指揮命令系統に関する資格制度も併せて導入予定である。



図 9 事業継続推進機構

BCAO 全体として、次のような目標を掲げている。

- ① 事業継続の取組みの普及・啓発
- ② 専門家育成
- ③ 標準化

---

<sup>26</sup> 弁護士、医師、研究者といったプロフェッショナルは所属する組織（事務所、病院、大学など）を超えた形態のネットワーク（例えば弁護士会、医師会、学会などに加え個人的な繋がり）を持っている。

- ④ 事業継続を推進している個人・企業・政府などの表彰
- ⑤ 調査・研究
- ⑥ 最新情報の提供

以上、事業継続管理に係るプロフェッショナル人材育成の重要性を確認したが、実際の育成プロセスは企業単体では限界があり、かつ偏りが生ずる可能性も否めないことから、可搬性（**portability**）のある客観的な資格<sup>27</sup>として位置付けることを行政や業界団体が早急に検討すべきタイミングに来ているといえよう。

---

<sup>27</sup> 先の弁護士、医師などと同様。

## 5 事業継続管理のためのソフトウェアツール

事業継続管理に関連する情報通信技術は、大きく2つに分類できる。ひとつは、サーバーのバックアップのように、重要な情報資産を保護する目的で使用されるハードウェアであり、ソフトウェアである。本報告書内では、この種の技術について、「7 事業継続を支援する技術・リモートバックアップ」で触れている。もうひとつは、マネジメントを支援するソフトウェアツール（以下、マネジメント支援ツールと記す）である。本章では、このマネジメント支援ツールについてまとめた。

### 5.1 マネジメント支援ツールの必要性について

事業継続管理は、続けることと更新することが必要不可欠である。たとえば、使用する情報通信システムが変わったにもかかわらず、バックアップや復旧の計画が見直されないままであると、事故や事件が顕在化したときにその古い計画は役に立たない。企業等の組織では、経営方針や事業戦略は当然変更される。これに伴い、特定の業務が中断した場合の経営への影響も変わる。やはり、定常的な見直しと更新が重要なのである。

本章で「マネジメント支援ツール」と呼ぶものは、このように続けることが必要な事業継続管理の作業を支援するツールで、主としてソフトウェアツールのことを意味している。次々に新しい製品やサービスが世に送り出されているため、一概には言えないが、このようなソフトウェアツールは大きく2つに分類できると考える。ひとつは、インパクト分析を支援するツールである。事業継続計画では、緊急時対応から復旧に至るまで、どの作業を優先的に行うかを決めておかなければならない。その目的のために使われるのがインパクト分析を支援するツールである。もうひとつは、対応の実施の中で必要となる情報を整理して取り出しやすくしておくソフトウェアツールである。分かりやすい例で言うと、従業員の緊急連絡先のリストなどがある。組織体制に沿って連絡していくとすると、人事異動の際には必ずリストの見直しが必要になる。また、携帯電話を変更したり引越しをした場合は、連絡先が変わるかもしれない。この情報を常時更新しておく必要がある。組織規模にもよるが、大規模企業になると作業量は少なくない。欧米で、事業継続管理に携わる担当者や所管部門の多くは、このように複雑で更新頻度の高い情報管理に、ソフトウェアツールを使用している。

## 5.2 マネジメント支援ツールの使用状況

2006年2月に発行された「Business Continuity Planning Software Survey (Continuity Insights Magazine)<sup>28</sup>」によると、事業継続計画ソフトウェア・パッケージを利用するか、もしくは計画策定や維持管理のためのホストソリューション(hosted solution)を使っていると回答した割合は、59%に昇る。しかしながら、全般的に使い勝手や拡張性についての改善を要望する声も多い。個々の組織の実状に合わせて使えるツールが求められているようである。

また、Continuity Central が 2004 年に公表した「Business Continuity Software Survey Results」によると、58.75%の回答者が、事業継続ソフトウェアを使用している。その目的は、事業継続計画の管理や更新が、60.62%、クライシス・マネジメントの管理や調整が 37.11%、教育が 25.95%、現在の能力の評価が、31.41%となっている。より詳細に利用目的を調査した結果を表 3 に示す。

表 3 事業継続ソフトウェアの用途別使用者割合

| 内容                               | 回答者の割合(%) |
|----------------------------------|-----------|
| 電話帳                              | 75.4      |
| ビジネスインパクト分析                      | 59.4      |
| テストと演習(exercising)               | 54.7      |
| クライシス・チームの開発                     | 47.2      |
| クライシス・マネジメント                     | 41.5      |
| リスクアセスメント                        | 41.5      |
| プロジェクト・マネジメント                    | 39.6      |
| オンライン・アクセス                       | 39.6      |
| 従属関係モデリング                        | 36.8      |
| 標準のデータベース(ORACLE、SQL サーバなど)とのリンク | 32.1      |
| 訓練(training)                     | 29.2      |
| ギャップ分析                           | 27.4      |
| 自動化クライシス・コミュニケーション               | 16.0      |
| 戦略選択                             | 9.4       |

※ "Business Continuity Software Survey Results" Continuity Central(2004)  
<http://www.continuitycentral.com/feature0142.htm> 筆者訳

<sup>28</sup> <http://www.contingenx.com/IMCD/Continuity%20Insights%20BCPSurvey.pdf>

一方、わが国では、災害時の緊急時対応の側面では、多くの経験や準備を重ねてきているが、事業を継続するという視点での取組みに関しては、まだそれ程取組みが進んでいるとは言いがたい。2006 年 11 月に(株)インターリスク総研が公表した調査結果においても、事業継続計画を策定していると回答した企業は 12.7%に止まっている<sup>29</sup>。本調査研究において実施したヒアリングにおいても、現状では多くの企業で、コンサルタントなどに相談しながら、計画策定に着手したばかりという状況という意見があった。従って、継続的な管理のために、ソフトウェアツール利用の必要性を感じる段階まで至っている企業はまだ少ないのではないかと推測される。ただし、今後、計画策定を通じて体制が整備され、継続的な取組みが行われるようになれば、このようなツールの必要性も認識されるようになるのではないと思われる。

### 5.3 マネジメント支援ツールの概要

マネジメント支援ツールの例として、SUNGARD 社の Paragon と Strohl Systems 社の製品を紹介する。

また、2007 年 2 月 7 日に、Survive と BSI が共同で開発した事業継続評価ツールについても触れる。

#### 5.3.1 Paragon (SUNGARD 社)

Paragon は事業継続のプランニング、統合マネジメントツールである。操作の容易性から顧客が直接購入する場合もあるが、中長期的なメンテナンスの観点から、コンサルティング会社などを通じた販売にも力を入れている（図 10）。

---

<sup>29</sup> [http://www.irric.co.jp/press\\_release/2006/nov/1109.html](http://www.irric.co.jp/press_release/2006/nov/1109.html)

## SunGard's Enterprise Availability Methodology

The "Information Availability (IA) Lifecycle"

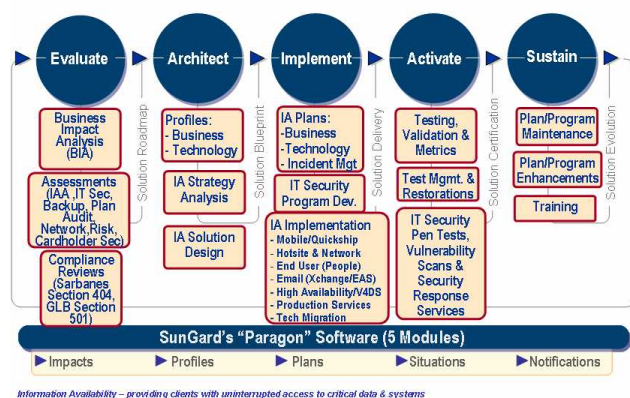


図 10 SUNGARD 社が提供する BCM 統合ツールを用いた方法論

この Paragon がカバーする 5 つの領域の根底に流れる概念は、IA ライフサイクル (IA: Information Availability) と定義され、企業の可用性 (取引先や商品・サービスのユーザーから見た) を確保するためのフレームワークであると位置付けられている。

### 5.3.2 LDRPS (Strohl Systems 社)

Paragon と同じく事業継続計画策定・運用支援ツールとしては、Strohl Systems 社<sup>30</sup>の製品が良く使われているが、今回の調査でヒアリングを行った米国投資銀行では使用しているものの、かなり内容をカスタマイズしている模様。この銀行はユーザー会のリーダーでもあり、また、事業継続管理のレベルは金融機関の中でもかなり高い位置にあるため、ユーザー側に知識と経験があれば使い勝手が良い、との評価であった。また欧州系グローバル銀行では、Paragon と Strohl System 社製品を比較、更に欧州系の専門ベンダーの製品数種類も検討した結果、できるだけユーザーが使いやすく、メンテナンスが簡単である、という事由で欧州系の専門ベンダーの製品<sup>31</sup>を採択している。

<sup>30</sup> <http://www.strohlsystems.com/>

<sup>31</sup> TwelveCubes/IBM による CPro、Office-Shadow による Shadow-Planner など。

Strohl System 社では、データを集積し災害時の復旧ための事業継続計画の構築を支援する LDRPS (Living Disaster Recovery Planning System) やビジネスインパクト分析を助ける BIA Professional などを提供している。LDRPS は、わが国における医療機関の災害訓練などでも利用されている。<sup>32</sup>

### 5.3.3 BS25999 事業継続評価ツール (Survive および BSI)

2007 年 2 月 7 日の発表によると、Survive<sup>33</sup>と BSI は、共同で BS25999 をベースに新しいソフトウェア評価ツール「BS 25999 Business Continuity Assessment Tool」を開発したということである。このソフトウェアを使うことにより、BS25999 に合致した事業継続管理を行うことができる。ベンチマークを提供するウェブ・ベースのソフトウェア・ツールで、個々の評価の後に必要とされるアクションのリストも提供している。

### 5.3.4 まとめ

このような、システム化されたソフトウェアだけではなく、中小企業庁が出しているガイドや各国の政策機関が公表している情報、チェックリストも、ツールのひとつといえる。

重要なのは、まず着手し、訓練などを通して見直しを行うなどの努力を継続的に実施することを通して、所属組織の文化や慣習に合った計画を作っていくことである。

---

<sup>32</sup> 「LDRPS による災害対応マニュアル管理について」第 5 回日本集団災害医学会抄録 一般演題 51 国立病院東京災害医療センター 堀内義仁、他(200 年 2 月)。

<sup>33</sup> 事業継続に関連する事業を行っている企業や担当者、専門家などにより 1989 年に設立されたフォーラム。

## 6 パンデミック・インフルエンザに対する取組み

「パンデミック」は、病気などが世界的に流行するという意味で使われる言葉である。ちなみに、風土病のようなものは、エンデミック、単に流行を表すときはエピソードと使い分けられている。「パンデミック」は、流行のなかでも特に世界的規模で広まる可能性のある病気に対して使われる。

近年、この「パンデミック」という言葉を使うときには、「パンデミック・インフルエンザ」を指していることが多い。わが国では、「新型インフルエンザの世界的流行（パンデミック）」といった形で使われている。この‘新型’というのは、それまでヒトに感染しなかった「インフルエンザ・ウイルス」が変異してヒトからヒトへ感染する‘新型’になったものである<sup>34</sup>。

「パンデミック・インフルエンザ」は大きな被害をもたらす世界的な流行が予想されており、世界保健機関を中心に各国で準備のための取組みが進んでいる。わが国においても、厚生労働省が、新型インフルエンザ対策推進本部を設置し、新型インフルエンザ対策行動計画を策定するなどの対策を実施している<sup>35</sup>。

「パンデミック・インフルエンザ」は、新たな脅威として、事業継続と密接な関係にあると捉えられていることが多い<sup>36</sup>。今回調査を行った英国や米国においても、事業継続やリスクマネジメントの関係者は、「パンデミック・インフルエンザ」対応に高い関心を示していた。

ここでは特に関心の高まっている「パンデミック・インフルエンザ」対策を取り上げ、英国と米国の動きを中心にまとめる。

<sup>34</sup> 詳細な説明は、厚生労働省のホームページを参照。

<http://www.mhlw.go.jp/bunya/kenkou/kekkaku-kansenshou04/index.html>

<sup>35</sup> 「新型インフルエンザ対策ガイドライン(フェーズ4以降)(案)」に関する意見募集が2007年1月31日～3月1日の期間で実施されている

(<http://www.mhlw.go.jp/bunya/kenkou/kekkaku-kansenshou04/09.html>)。

厚生労働省のホームページで公開されている「米国疾病管理センターの推計モデル(FluAid 2.0)」に、わが国の状況を当てはめて推計した。その結果、我が国の場合は、全人口の25%が新型インフルエンザに罹患すると想定した場合に医療機関を受診する患者数は、約1,300万人～約2,500万人(中間値約1,700万人)と推計されている。

(<http://www.mhlw.go.jp/bunya/kenkou/kekkaku-kansenshou04/pdf/03-03-02.pdf>)

<sup>36</sup> ただし、事業継続管理を、脅威を特定しない形で計画を立てるものとして捉えている場合、このように特に「パンデミック・インフルエンザ」に対して、重点的に行動を起こすというアプローチには違和感があるという意見もある。

## 6.1 英国政府

英国では、「パンデミック・インフルエンザ」対策に対する関心が高く、多くの企業が、効果的なアクション・プランを立て、アウェアネス(啓発)や世界的な動向変化の監視を行っている。

以下、英国内閣府の管轄下にある民間緊急事態管理局(Civil Contingency Secretariat)が、事業継続支援のために公開しているさまざまな情報から、特に「パンデミック・インフルエンザ」に関連する情報を取り上げる。

### 6.1.1 英国内閣府のパンデミック計画ガイダンス

「ガイダンス — 起こりうるインフルエンザ・パンデミックのためのコンティンジェンシー・プラン(非常事態対応策)」として、2006年2月に第1版が公表され、同年7月に改訂されている。

このガイダンスの位置付けと使用されている用語を理解するためには、その基盤となっている民間緊急事態法 (Civil Contingency Act) についての基礎的な理解が必要である。

#### 英国内閣府の民間緊急事態法

民間緊急事態法は、英国市民を保護するための枠組みとして作られ、市民保護 (ローカルアレンジメント) を定めたパート1と緊急時の権限 (エマージェンシー・パワー) について定めたパート2から構成される<sup>37</sup>。

民間緊急事態法は、地域の対応者を2つのカテゴリーに分け、個々に義務を課している。カテゴリー1は、緊急事態サービス、地方政府、国民保健サービスなど、緊急時に中心となって対応する組織である。カテゴリー2は、健康安全局 (HSE: Health and Safety Executive)、輸送機関、公益事業者 (ユーティリティ) などの組織で、緊急時にカテゴリー1の組織と協力しながら活動する組織である。

カテゴリー1と2の組織は、共同で、地域レジリエンスフォーラムを作り、

---

<sup>37</sup> パート1の大半は、2005年11月に発効した。ただし、事業者や自主組織が、事業継続管理への取り組みを始めるにあたってのアドバイスを提供したり支援をするという地方政府の義務については、2006年5月の発効となった。

地域レベルの対応者間の調整と協力を支援する（図 11）。

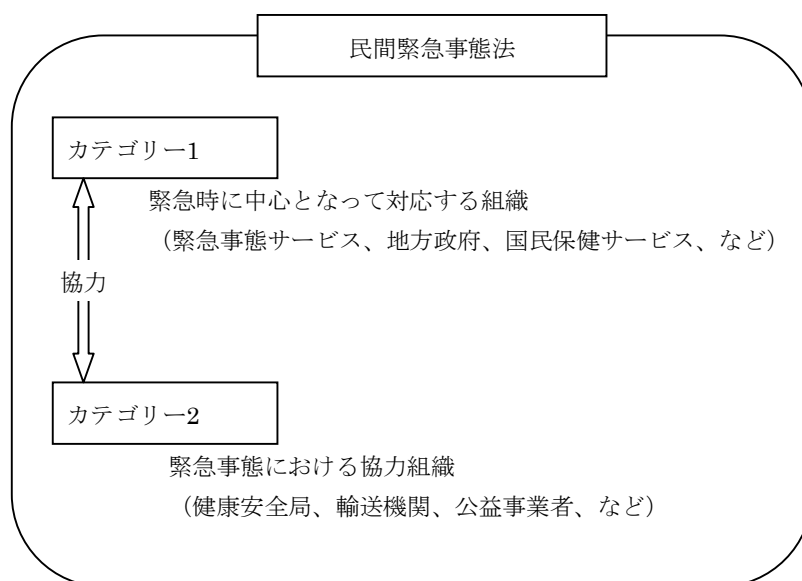


図 11 民間緊急事態法の対象者分類

民間緊急事態法が対象とするマネジメントプロセスは、統合緊急事態管理（Integrated Emergency Management: IEM）の概念をもとに説明されている。IEM は、「予知」、「評価」、「予防」、「準備」、「対応」、「復旧」の 6 つの構成要素からなる。このうち、事前準備に関する要素である「予知」、「評価」、「予防」、「準備」をまとめて、エマージェンシー・プリペアドネス（EP）と呼び、事後対策に関する要素である「対応」、「復旧」をまとめて、エマージェンシー・レスポンスとリカバリー（ERR）と呼ぶ。

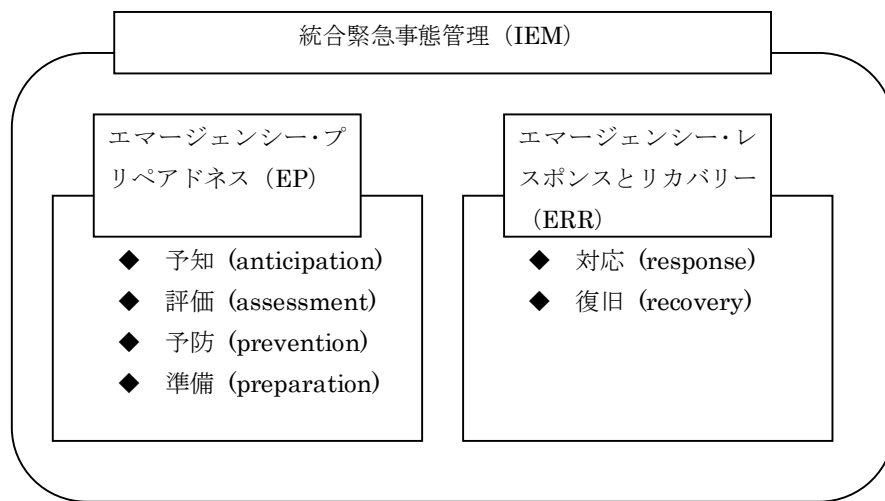
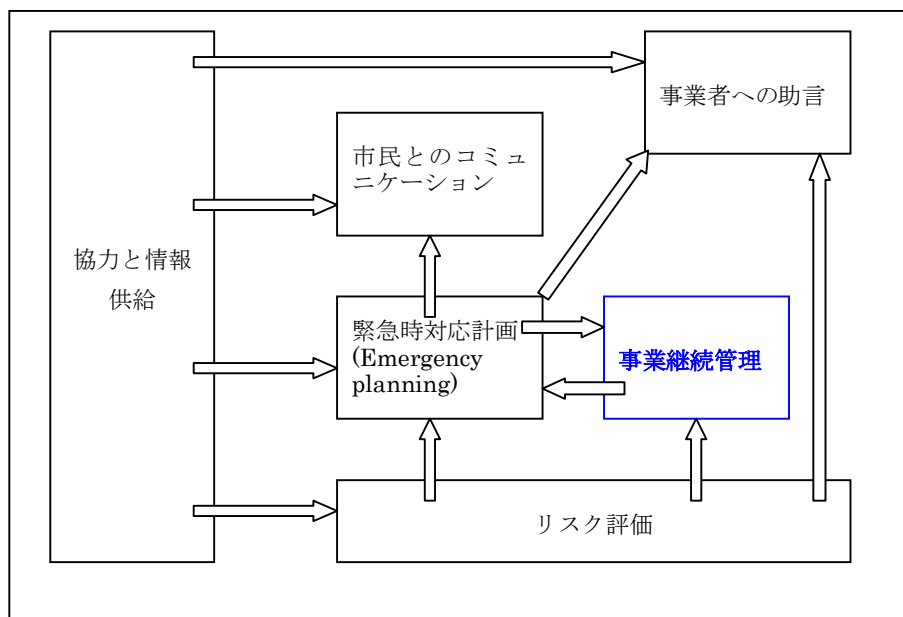


図 12 統合緊急事態管理全体図

EP は、計画策定のためのプロセスであり、民間緊急事態法は、4 つの EP 構成要素の中でも、さらに「評価」と「準備」の 2 つにフォーカスしている。

また、民間緊急事態法の対象領域については、図 13 に示す 7 つの領域となっており BCM は、この中のひとつとして位置付けられている。また、カテゴリー1 に属する機関が負う市民保護義務として、主たる 4 つの領域<sup>38</sup>が提示されているが、BCM は、このうちのひとつでもある。

<sup>38</sup> 4 つの領域は、「リスク評価」、「BCM」、「緊急時対応計画(Emergency planning)」、「市民のウェルネス維持、注意喚起、情報提供、およびアドバイス」である。



※ Emergency Preparedness - Guidance on Part 1 of the Civil Contingencies Act 2004, its associated Regulations and non-statutory arrangements, pp. 6 (筆者訳)

図 13 民間緊急事態法における7つの市民保護義務の相互関係

#### 事業継続について

EPに関するガイダンス（Emergency Preparedness - Guidance on Part 1 of the Civil Contingencies Act 2004, its associated Regulations and non-statutory arrangements）の第6章が、BCMについて説明している箇所である。その中では、事業継続管理は、崩壊事象の発生においても、事業化継続し、その後は、効果的な復旧が図れるようにするためのプロセスと定義されている。

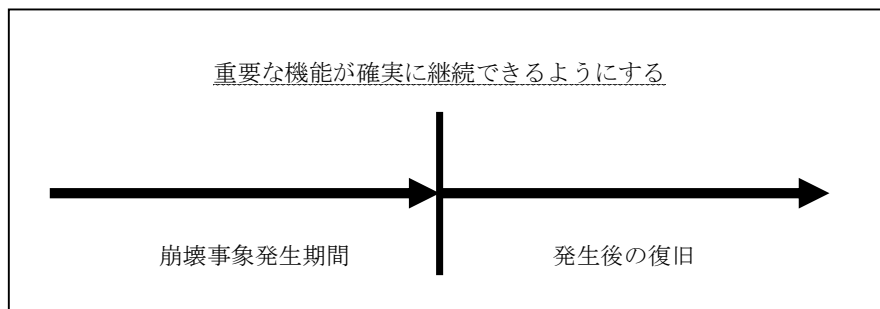


図 14 BCM の概念図

事業継続マネジメントは、公的機関、私的機関、自主機関など、どのような組織にも当てはまる概念となっており、そのプロセスとして、BCI (Business Continuity Institute) が作成した 5 ステージから構成される概念を紹介している (図 15)。

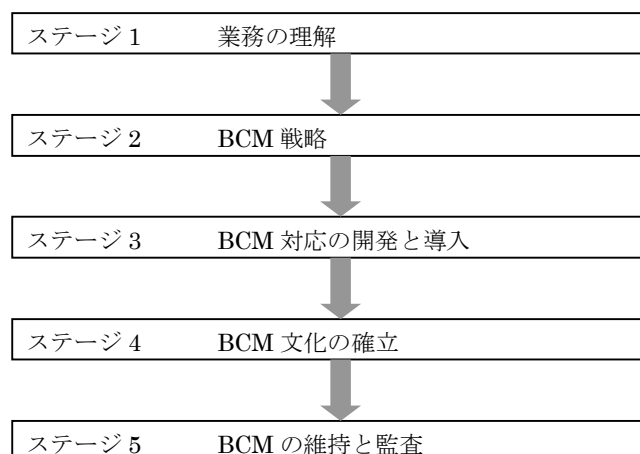


図 15 BCM の 5 ステージ

事業継続計画 (BCP) については、「一般的な計画」と「特定の計画」との組合せで全体を構成するモデルが紹介されている。この場合、「一般的な計画」としては、たとえば発動手順、コマンド&コントロール、財源へのアクセスなどが例として上げられる。「特定の計画」は、特定のリスクやサイト、サービスに関連

して要求されるものである。

その他、事業継続計画の演習やキースタッフの訓練などについて、簡単に触れている。

従って、本章で取り上げる「パンデミック・インフルエンザ」に対する対策などは、特定のリスクに対する「特定の計画」として位置付けられるものであろう。

#### **パンデミック・インフルエンザのためのガイドライン**

このようなフレームワークの中で、取り組まれている「パンデミック・インフルエンザ」対策であるが、その中心的役割を果たすのは、英国健康省である。わが国の厚生労働省と同様に、英国健康省もさまざまな情報を提供している。これらの情報を元に、地域計画を支援する目的で、英国内閣府がまとめたものが、「ガイダンス ― 起こりうるインフルエンザ・パンデミックのためのコンティンジェンシー・プラン(非常事態対応策)」である。

その内容は、英国健康省が発表しているさまざまな「パンデミック・インフルエンザ」に関する情報をサポートするものとなっている。全体は、表 4 に示すような構成で、カテゴリー 1 とカテゴリー 2 は、それぞれ、民間緊急事態法で規定した分類に対応している。「√」が記入されているものが、将来の計画で考慮するものである。

主として、カテゴリー 1 に属する組織を対象としているが、カテゴリー 2 や広範なコミュニティにも関連する内容となっている。

表 4 ガイドラインの全体構成

| 内容                     | 下記の組織により策定される計画との関連性: |                       |                                                   |
|------------------------|-----------------------|-----------------------|---------------------------------------------------|
|                        | カテゴリー 1<br>対応者        | カテゴリー 2<br>対応者        | 広範なコミュニティ<br>(事業者,<br>公共機関,<br>ボランティア組織,<br>慈善団体) |
| 目次と相互関係                | √                     | √                     | √                                                 |
| サマリー                   | √                     | √                     | √                                                 |
| イントロダクション              | √                     | √                     | √                                                 |
| 本書の目的                  | √                     | √                     | √                                                 |
| 本ガイダンスの情報源             | √                     | √                     | √                                                 |
| 地域計画の主たるフォーカス・エリア      | √                     | 注意                    | 注意                                                |
| リスク                    | √                     | √                     | √                                                 |
| 鍵となる計画のための想定           |                       |                       |                                                   |
| 保険衛生関連の影響              | √                     | √                     | √                                                 |
| 職場における従業員の不在           | √                     | √                     | √                                                 |
| 事業継続計画(BCP)において考慮すべき問題 | √                     | √                     | √                                                 |
| パンデミックを管理するためのポリシーの展開  |                       |                       |                                                   |
| 医療対策                   | √                     | √                     | √                                                 |
| 感染リスクの軽減               | √                     | √                     | √                                                 |
| 社会的手段と移動の制限            | √                     | 注意し、必要に応じて計画への事項の盛り込み | 注意し、必要に応じて計画への事項の盛り込み                             |
| ウェブサイト上で見られる追加のアドバイス   | √                     | √                     | √                                                 |

※√は、将来の計画で考慮すべき項目を示す。

※[http://www.ukresilience.info/publications/060710\\_revised\\_pandemic.pdf](http://www.ukresilience.info/publications/060710_revised_pandemic.pdf) より  
(筆者訳)

事業継続計画は、基本的に、“仮定”に基づく計画を立てるものである。その基本の数字として、ガイドラインでは、まず公衆衛生上の影響について、2種類のシナリオを、“Key Planning Assumptions”の項で提示している。基本シナリオでは、累積で全人口の約25%が感染し、それが複数回にわたり発生するとしている。また、最悪の場合を想定すると、約50%が感染し、そのうち2.5%が死亡す

るという想定である。つまり、基本シナリオと同様の事態に至った場合、職場には4分の1の従業員が出てこられなくなり、その状態が3~4ヶ月続くことになる。また、本人は発症していなくとも家族の看病のために出社できない者についても考慮が必要である。このような状況を想定した計画について具体的なアドバイスを行っている。

ガイダンスにおける「事業継続計画で考慮すべき問題」を見ると、組織が考慮すべき事柄として、次のような事項が含まれている。

- パンデミックの影響を減らすための政府の努力を支援する。
- 数週間、高い割合で従業員が出社できなくとも中核となる事業活動を維持継続するための手段を導入しておくこと。
- 不在になった場合、事業継続が特別なリスクにさらされるような必要不可欠の機能や役職や個人を特定しておくこと。
- パンデミックが顕在化した期間もしくはそのピークにおいて、縮小したり中断する可能性のあるサービスを特定すること。
- 従業員に対する健康安全責任が完全に遂行され続けることを確実にすること。
- 組織間の相互依存を明確にし、それがレジリエントであることを確実にすること。たとえば、サプライヤー組織が契約に基づきサービスを確実に継続できるなど。
- 必要に応じ、健康サービスを支援するために必要な事柄を計画に入れること。
- 軍の支援が得られない状況も想定した計画を立てること。
- 医療上の問題解決手段が事業継続上の要求事項を解決しないことを想定して計画を立てること。なぜなら、抗ウイルス性の治療は、疾病の深刻さを少なくするだけで、病気を治したり長期不在を大きく減少させるものではないからである。

また、疾病が広まるのを遅らせるなどの目的で政府が決定した手段によって、さらに多くの従業員が不在になる可能性があることも考慮して計画を立てる必要がある。7月のガイダンス改訂では、この事項に、学校閉鎖などにより、自宅にいる子供の世話をするために、親である従業員が出社できなくなる可能性もあることが付記された。

また、組織が政府の活動を支援する内容として、感染した従業員が出社しないための方針を定めたり、啓発を行ったり、十分な手洗い用品を備えるといった内容も提示している。

### 6.1.2 事業者のためのパンデミック・インフルエンザ チェックリスト

前項のガイダンスの中で、情報源として紹介されている文書のひとつである「事業者のためのパンデミック・インフルエンザ チェックリスト」を取り上げる。

同チェックリストは、主に大・中規模事業者向けに作成され 2006 年 5 月に発行された<sup>39</sup>。

大項目は、次の 6 項目あり、全 30 項目から構成されている。

表 5 パンデミック・インフルエンザ チェックリストの大項目

- |                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>① 事業におけるパンデミックの影響に対する計画</li><li>② 従業員や顧客におけるパンデミックの影響に対する計画</li><li>③ パンデミックの期間中に導入すべき方針の確立</li><li>④ パンデミックの期間中に従業員や顧客を保護するための資源の配置</li><li>⑤ 従業員とのコミュニケーションと教育</li><li>⑥ 外部組織との調整とコミュニティ支援</li></ul> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

個々のチェック項目について、「完了」、「進行中」、「未着手」のいずれかを選択するようになっている。

内容を概略すると、「① 事業におけるパンデミックの影響に対する計画」では、パンデミックの期間中、継続しなければならない重要な活動（critical activities）を特定することやサプライヤーや取引先と事業継続計画について話し

<sup>39</sup> <http://www.ukresilience.info/publications/060516flubcpchecklist.pdf>

合っておくこと、計画に基づき演習を行うことなどが挙げられている。

「② 従業者や顧客におけるパンデミックの影響に対する計画」では、政府のガイドに基づき、従業者不在に備えた予測や計画を立てておくこととしている。考慮すべき事項として、保育園や学校の閉鎖、公共交通機能の低下などが挙げられる。また、会議のために移動できない場合に備え、ビデオ会議や電話会議などを検討することや顧客ニーズに継続的に応えられるようにするためにメールによる注文やインターネット・ショッピングなどの手段を考えておくことなどを例示している。

「③ パンデミックの期間中に導入すべき方針の確立」では、病気から回復した後、職場復帰する際の取り決めや自宅で仕事をするなどの柔軟なワークサイトに関する方針を立てておくことなどが記載されている。また、職場において、呼吸器衛生/咳エチケット<sup>40</sup>、インフルエンザの兆候がある従業者の自宅待機といった指導を行うことを推奨している。わが国の企業でもすでに実施されているようであるが、アウトブレイク（感染の多発）が始まった国への渡航制限などもチェック事項として含まれる。

「④ パンデミックの期間中に従業者や顧客を保護するための資源の配置」では、感染拡大を軽減するための手段を提供することや敷地内をさらに頻繁に清掃すること、自宅で仕事できるように IT インフラを拡張するかどうかを検討することなどが提示されている。

「⑤ 従業者とのコミュニケーションと教育」では、従業者にインフルエンザ感染や、事業における準備・対応計画とその中での各自の役割に関する情報を提供すること、取引先や顧客とパンデミックの状況や活動について情報交換するプラットフォーム（たとえば、ホットラインやウェブサイト）を作成することなどが書かれている。

「⑥ 外部組織との調整とコミュニティ支援」では、地域のパンデミック計画について知ることやコミュニティ内の他の事業者とベストプラクティスについて情報交換することなどを挙げている。

---

<sup>40</sup>インフルエンザに罹患し、咳嗽などの症状のある方は特に、周囲への感染拡大を防止する意味から、咳やくしゃみをする際にはティッシュで口元を覆うか、マスクを着用してもらうということ（国立感染症研究所 感染症情報センター インフルエンザ・パンデミックに関するQ&A 2006.12 改訂版（<http://idsc.nih.gov.jp/disease/influenza/pandemic/pQA2006ver02.pdf>）より）

## 6.2 サバイブによるパンデミックのガイドライン

サバイブ（Survive）は、組織のレジリエンスやサバイバルのために責任を負う事業継続管理の担当者や専門家、管理者などが知識を得たり情報交換を行うために、1989年に設立されたフォーラムである。そのサバイブが、2006年に「事業のための流感パンデミックガイドライン」を作成した。その背景には、パンデミック・インフルエンザの脅威が非常に大きいものとして捉えられていることがある。同フォーラムによると、専門家は、パンデミック・インフルエンザの影響として30%の従業員が不在になり、全ての主要な事業取引が、混乱に陥ると予想している。その際に組織が生き残るために必要な事項をまとめたのがこのガイドラインである。

ガイドラインは、表 6 の各項目で構成されている。

表 6 ガイドラインの項目

|                       |                                             |
|-----------------------|---------------------------------------------|
| ◆ エグゼクティブ・サマリー        | なぜパンデミック・インフルエンザが急を要する優先事項なのかについての説明        |
| ◆ イントロダクション           | ガイドラインの目的、スコープ、構成のアウトライン                    |
| ◆ パンデミック・インフルエンザとは何か？ | インフルエンザ・ウイルスについての情報と我々がどのようなリスクに晒されているかについて |
| ◆ 鍵となる考慮事項            | 心に留めておくべき 10 の極めて重要なメッセージ                   |
| ◆ クイック・ガイド            | 計画プロセスのスナップショット、コアのプロセスは詳細に説明               |
| ◆ 事業インパクト             | 続いて起こる窓外と中断の定量化                             |
| ◆ 計画想定                | 組織に対するパンデミックの影響度合いの特定                       |
| ◆ サバイバルとサクセスのための戦略    | 計画活動のためのフレームワークの提供                          |
| ◆ マネジメントの役割           | 計画活動を支持する上級管理者の役割の分析                        |
| ◆ 計画                  | 詳細な緊急時対応計画（コンティンジェンシー・プラン）の開発方法             |

※<http://www.survive.com/news/viewnews.cfm?newsID=1402>(筆者訳)

### 6.3 米国政府

米国においても、英国と同様に、政府機関が情報提供を通じて、パンデミックに対する準備を推進している。

本項では、米国保健社会福祉省（Ministry of Health and Human Service(HHS)）、米国国土安全保障省（Department of Homeland Security(DHS)）の活動を追いながら、米国におけるパンデミック対策の動向をまとめる。

#### 6.3.1 米国保健社会福祉省(HHS)の活動

日本の厚生労働省にあたる米国の保健社会福祉省（Department of Health and Human Services(HHS)）の下部組織である、米国厚生省疾病管理・予防センター(CDC)では、パンデミック・インフルエンザを、対策を打つべき疾病のひとつとして、位置付けて活動を推進している<sup>41</sup>。

さらに、パンデミック・インフルエンザに関するワンストップ・インフォメーションとして、図 16 に示すサイトをインターネット上に公開している<sup>42</sup>。同サイトも HHS が所管している。

---

<sup>41</sup> <http://www.cdc.gov/>参照

<sup>42</sup> <http://www.pandemicflu.gov/>



図 16 米国保健社会福祉省によるパンデミック・インフルエンザの情報

同サイトは、連邦政府、州および地域政府、個人、ビジネス、教育機関、医療機関、地域などに向けて情報提供をしている<sup>43</sup>。

その中で、ビジネス向けに提供されている、チェックリスト「Business Pandemic Influenza Planning Checklist(December 6, 2005 Version 3.6)」の概要をここで紹介する<sup>44</sup>。

<sup>43</sup> <http://www.pandemicflu.gov/plan/business/index.html>

<sup>44</sup> <http://www.pandemicflu.gov/plan/pdf/businesschecklist.pdf>

チェックリストは、大きく 6 項目あり、すべてのチェック項目数は、35 項目である。それぞれの項目について、「実施済み」、「取組み中」、「未着手」のいずれかを選択するようになっている（表 7）。

表 7 米国ビジネス・パンデミック・インフルエンザ計画チェックリストの項目

|   |                                  |
|---|----------------------------------|
| 1 | 事業におけるパンデミック準備計画。                |
| 2 | 従業員と顧客のためのパンデミックの影響のための準備計画。     |
| 3 | パンデミック期間中に実行されるべき方針を確立する。        |
| 4 | パンデミック期間中に従業員と顧客を保護するための資源を配置する。 |
| 5 | 従業員とコミュニケーションし、教育する。             |
| 6 | 外部組織と調整し、コミュニティを支援する。            |

「1 事業におけるパンデミックの影響のための準備計画」は、計画策定のための組織の設置や、流行中でも必要不可欠な従業員や原材料などの明確化などの項目を含んでいる。また、緊急時のコミュニケーション計画を確立し見直すこととしている。この計画には、サプライヤーや顧客を含むコミュニケーション・チェーンなどが含まれる。

「2 従業員と顧客のためのパンデミック準備計画」は、従業員不在状況の予測や、従業員同士や顧客とのフェイス・トゥ・フェイスの接触の頻度や有様を検討するなどの項目を含む。

「3 パンデミック期間中に実行されるべき方針を確立する」では、流行期間中における休暇の取得や、テレワークなどの柔軟な労働場所の選択に関する基本的な方針を立てておくこととしている。また、アウトブレイクが始まった地域で、従業員が働いている場合に避難する際の方針も必要項目としてあげている。

「4 パンデミック期間中に従業員と顧客を保護するための資源を配置する」では、手洗い用品など感染を予防する備品を十分容易する、従業員がテレワークをしたり、遠隔地の顧客とコミュニケーションするために必要な情報通信技術インフラを強化する、緊急対応のための医療コンサルティングを確保しておくことなどが書かれている。

「5 従業員とコミュニケーションし、教育する」では、従業員がインフルエンザに関する基本的な知識を得るために必要なプログラムを作ったり、対応計画について従業員に周知するといったことが必要としている。また、従業員に加え、ベンダーや取引先、顧客などと、パンデミックの状況や関連する活動について情報交換するためのホットラインやウェブサイトを準備することについても言及している。

「6 外部組織と調整し、コミュニティを支援する」では、保険会社や健康保険組合、地域の健康保健施設とパンデミックに関する計画について協力したり、連邦や州政府、地域の計画に参加し、その対応能力を理解すると共に、コミュニティへの貢献についても、情報交換しておくこととしている。また、商工会議所などを通じて、地域におけるベストプラクティスを作っていくことについても触れている。

### 6.3.2 Homeland Security の活動

米国国家の安全保障を所管する国土安全保障省(Department of Homeland Security)では、事業継続に関連するさまざまな活動を行っている。その活動のひとつとして、2006 年 9 月 19 日に、「国家の重要インフラ及び主要リソースのためのパンデミック・インフルエンザ準備、対応、復旧ガイド (Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources)」を発行している<sup>45</sup>。

同ガイドは、ブッシュ政権が 2003 年 12 月に発表した大統領令である Homeland Security Presidential Directive(HSPD-7)で、定めた安全保障上重要

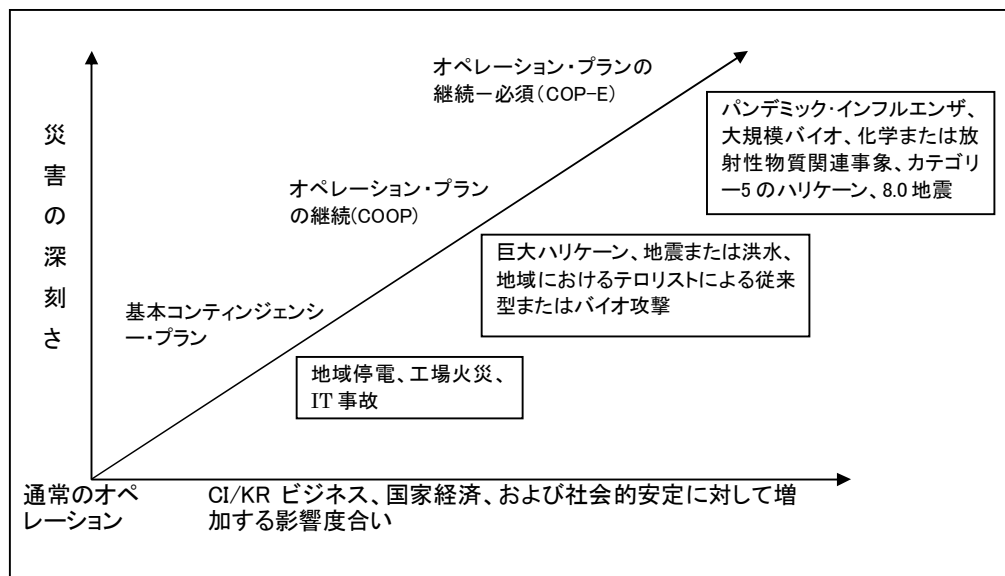
---

<sup>45</sup> [http://www.ready.gov/business/\\_downloads/pandemic\\_influenza.pdf](http://www.ready.gov/business/_downloads/pandemic_influenza.pdf)

なインフラと位置付けられる 17 のセクター（17 CI/KR と呼ぶ）、ならびに一般的な産業界に対して、パンデミック・インフルエンザに関する取組みの重要性和具体策についてまとめている。

ガイドは、パンデミック・インフルエンザに関して、事業者が実施しておくべき基礎的な情報から始まり、その対応計画策定のための、3 つのシナリオを提示する。シナリオ 1 は、最も影響度を低く想定したもので、30～40%の従業員が出社できない状況を想定する。しかしながら、優先順位に基づいて重要な機能を速やかにシフトすることにより、対応が可能なレベルとしている。シナリオ 2 は、40%の労働力が欠け、その中には、要となる上級管理職などがシナリオ 1 よりもさらに多く含まれる状況を想定している。ある事業が継続できなくなった場合に、その他の事業やコミュニティに雪崩のように影響が波及する可能性がある。シナリオ 3 は、数週間に渡り、50%以上の労働者が欠勤する状況を想定している。その理由としては、自身が感染した場合に加え、学校閉鎖、接触への恐れで出社しない者が出るなどの状況を考えている。事業者は、地域などにおいて必要不可欠な物資やサービスの提供を支援し、最低限の機能を維持することに向けられなければならないため、優先順位付けも見直しが迫られる状況である。いずれのシナリオにおいても、交通機関への影響や物流の遅延、金融機関利用への影響などについて、それぞれの影響度合いを示している。

パンデミック・インフルエンザの影響度を、本ガイドは非常に深刻に捉えている。その理由は、状況悪化が急激であることや事業だけでなくコミュニティや国家にまで広がる点にある。そのため、対応計画も最も重要なランクに位置付けしている。図 17 は、ガイド中で示されている災害対応計画の連続体を表す図であるが、パンデミック・インフルエンザは、最も深刻で影響度の大きい分類に属している。



※ Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources, pp.29 (筆者訳)

図 17 災害対応計画連続体の図

パンデミック・インフルエンザが顕在化した時には、必須のオペレーション・プランである COP-E (図 17 の右上) が発動する。COP-E は、計画、準備、対応、復旧の 4 つのフェーズに分かれている。チェックリストとして活用できる形になっており、何をすべきかや考慮事項などが書かれている。「計画」フェーズは、アセスメントや準備のために必要なアクションをまとめており、「準備」フェーズは、まだ初動を起こすまで時間的猶予がある段階において、必要な組織体制を作ったり、維持すべき基本機能を特定するなどの事前準備についてまとめている。「対応」フェーズは、ヒト・ヒト感染のアウトブレイクが始まり、採集の準備と初動の緊急対応を行わなければならない状況で取るべき行動をまとめている。「復旧」フェーズは、スキルを有する従業員の確保や他の工場のシャットダウンの影響など、アウトブレイクが一段落した後の活動についてまとめている。パンデミック・インフルエンザの特徴として、次の流行に備えた準備をすることがこのフェー

ズに含まれている点が特筆される。なお、この中で、「準備」フェーズと「対応」フェーズは、それぞれ、世界保健機関（World Health Organization( WHO)）や米国政府が定めたインフルエンザ流行の警告段階と対応している。

### 6.3.3 その他の一般的情報

新たに認識された大きな脅威として、世界機関や政府が主導し進められているパンデミック・インフルエンザへの準備に対して、産業界でもさまざまな活動や情報提供が行われている。その中で、興味深いいくつかの記事を紹介する。

まず、「Disaster Resource Guide 2006-2007」に掲載されている Regina Phelps 氏の記事「The Greatest Threat of Our Lifetime...or Not?」では、通常の事業継続計画（BCP）とパンデミック・インフルエンザを想定した計画との違いについて、次のように記述している。

- 『1 ほとんどの BCP は、通常の事業形態に 30 日以内にもどることを想定している。
- 2 一般的な計画では、事業を復旧するために、損害が生じた場所を出て、第二のサイトに移ることを要求している。』

これに対して、パンデミック・インフルエンザの場合は、18 ヶ月は続く可能性があり、最初の 90～120 日間は、ほとんど機能しないことが想定される。その影響範囲は、国内外に及び“安全な代替サイト”がない状態である点を指摘し、これまで作成した BCP では上手くいかないことを示唆している。

そのような状況下での問題として、最初に挙げられているのが「恐れ」である。その他、店舗やレストランなどはもとより学校の「閉鎖」も課題としている。そして、パンデミック・インフルエンザの対策としては、手を洗うなどの基本的な予防から始まり、働き方を変えることを提唱している。たとえば、従業員の間の距離を約 1 m～2m 取ること。もし、それができなければ、マスク着用を義務付けること、といった具体的なアドバイスをしている。

パンデミック・インフルエンザに関連した統計調査もいくつか出されている

が、そのうちのひとつであるワトソン・ワイアット・ワールドワイドの調査によると、国際企業 90 社のうち、アジア太平洋地域で操業する企業の 52%が、鳥インフルエンザに関する地域プログラムの導入を考えているということである。アジア太平洋地域で、プログラム導入を考えている企業は 74%に上る。また、同様の調査に対し、米国では 48%、ヨーロッパでは 47%、ラテンアメリカでは 44%、カナダでは 42%の結果を得ている。これに対し、すでに、計画を持っていると思われる企業は、アジア太平洋地域で 32%、米国で 15%、ヨーロッパで 11%、カナダで 10%、ラテンアメリカで 9%であったということである<sup>46</sup>。

経済的インパクトについても、いくつかの調査がある。世界銀行では、世界規模で、3000 億ドルにのぼり、GDP を 2%下げる影響があると試算している<sup>47</sup>。また、2007 年 1 月 23 日の [asahi.com](http://www.asahi.com) の記事では、「世界銀行の試算では、新型インフルエンザが大流行した場合の損失は 2 兆ドルに上るとされ、SARS の 590 億ドルと比べ、額はずっと大きい」としている<sup>48</sup>。

---

<sup>46</sup><http://www.watsonwyatt.com/scripts/printfriendly.asp?ss=News&Region=&printable=yes&ID=15840>

<sup>47</sup> “Bird flu will cost \$800 billion, says World Bank”, Times Online, November 07, 2005

<sup>48</sup> <http://www.asahi.com/business/column/TKY200701230115.html>

## 7 事業継続を支援する技術-リモートバックアップ

IT が組織の重要なビジネスインフラとなるに従い、データ保護の必要性は高まる一方である。IT の黎明期から現在に至るまで磁気テープへのバックアップは当たり前のように行われている。現在のデータセンター内でのデータ保護は、磁気テープに加えて、サーバーのディスク冗長構成などにより更に充実している。そのディスク冗長構成は、基幹系システムから情報系の小規模システムに至るまで採用されることが多くなった<sup>49</sup>。

また、昨今関心が高まっている広域災害への対策として、データセンター<sup>50</sup>自体が利用できない最悪の事態を想定し、データセンターと離れた拠点にバックアップを行うため、リモートサイト<sup>51</sup>を構える事例が出始めている。

そのリモートサイトを運用するために、通常の運用時にはデータセンターからリモートサイトにデータを転送しておき、被災時などに極力早期の復旧を目指す手法が本章のテーマであるリモートバックアップ<sup>52</sup>である。

リモートバックアップはこれから普及期を迎えようとしている技術である。IT やネットワークの進化と価格低下などにより、ハイエンドのバックアップ手法として今後一層の導入促進が予想される。

本章ではそのリモートバックアップに着目し、その技術動向を概観する。次の4項目について記載する。

- バックアップを取り巻く環境変化と現状
- リモートバックアップの技術動向
- リモートバックアップの技術選択
- バックアップ技術を活かすために

まず、バックアップ全体に対する環境変化と現状を捉えて、リモートバックアップが着目されている背景について考察する。次に様々なベンダーからリリースされているリモートバックアップの技術動向について類別し、特にトピックと考えられる技術をピックアップして解説する。そして、現在各種リリースされて

<sup>49</sup> 「情報システムの障害対策の設置（予定）している機能」として RAID(RAID1～5)を選定していると回答した事業体は 82.3%、という調査結果が存在する（出典：『平成 17 年度「情報セキュリティに関する調査」集計結果』2006 年 3 月 財団法人日本情報処理開発協会）。

<sup>50</sup> プライマリサイト、本番サイトなどと表記されることがある。

<sup>51</sup> セカンダリーサイト、バックアップサイトなどと表記されることがある。

<sup>52</sup> 本章では、(遠隔)レプリケーション、遠隔ミラーリング、遠隔バックアップなどと表記される遠隔地へのバックアップ手法を、総称として「リモートバックアップ」と呼称する。

いるリモートバックアップについて、技術選択のポイントを整理する。最後にバックアップを有効にするために行うべき事項について記載する。

## 7.1 バックアップを取り巻く環境変化と現状

ここでは、リモートバックアップの技術動向を論じる前段として、バックアップ全体についての環境変化や現状の運用について整理する。そのうえでバックアップに対する要求と現状のギャップについて考察し、リモートバックアップが本格的に普及しようとしている背景について論を進める。

以下の3点について記載する。

- バックアップ運用を取り巻く環境変化
- バックアップ運用の現状
- バックアップ運用のニーズと現状のギャップ

### 7.1.1 バックアップ運用を取り巻く環境変化

最初に、バックアップ運用を取り巻く環境変化について例示する。

#### 24時間365日フル稼働システムの増加

インターネットの世界的な普及の影響などにより、24時間365日フル稼働のシステムが増加している。いわゆる”止められない”システムが増えている。

#### IT依存性の高まり

業務のIT依存性が高まっている。ITを利用することを前提として業務が回っている。基幹システムなどで行われている大量の処理をIT化以前の手作業に戻すことは極めて難しい。組織の規模が拡大すればするほど、その難易度は高くなる。

#### データ量の飛躍的増大

この点については、次のような要因が考えられる。

### IT化の浸透

インターネットの普及などで IT 化が進み「データ量がおびただしく多くなり、ストレージの発達により蓄えるデータがここ 10 年ほどで 1000 倍<sup>53</sup>」と言われるほどデータ量は短期間の内に増大している。

### 不必要なデータの滞留

データは、数多くのサーバーに散在し、統制されていない。その結果生成・保管・保存・廃棄といった情報ライフサイクルマネジメント(ILM)<sup>54</sup>が十分に機能していない。特に不必要になったデータの廃棄が徹底されていない場合が多い。データは増加する一方である。

### 長期データ保管への対応

法令要求などによりメールや証憑などデータを長期に保存することが必要となりつつある。データの増加に拍車をかけている。

### **マルチメディアコンテンツへの対応**

情報系システム、特に Web システムでは、静止画像、動画、音声などマルチメディアコンテンツへの対応が必要となる。文字データが中心であった時期と比べて、バックアップ対象ファイル単位の容量が大幅に増加している。

### **事業継続への対応**

迅速な災害復旧に対するニーズが日増しに高まり、IT に対して次のような事項が要求されるようになった。

- どのような事態が発生しても重要なシステムを早期に復旧すること
- データ損失を極力防止すること

先述の「IT 依存性の高まり」により、事業継続に重要なシステムの早期復旧の重要性が増している。

組織独自のアプリケーションやデータの損失は代替が効かない。再度購入すれば揃うハードウェアやパッケージソフトウェアとは異なる。特にデータは、一

---

<sup>53</sup> 出典:『実践マニュアル コンピュータシステム災害復旧の対策』2006 年 9 月 谷井成吉著 ダイヤモンド社

<sup>54</sup> ILM: Information Lifecycle Management の略称。ストレージ業界団体の SNIA は ILM を次のように定義している。「情報が生成されてから最終的に廃棄されるまでの間、情報のビジネス価値を最適でコスト効率の高い IT インフラストラクチャに連携させるためのポリシー、プロセス、手法、サービスおよびツール」

且失うと完全には復旧できない可能性も高い。また、再入力など何らかの手段によりデータの復旧が完了するまでシステムは利用できない。最悪の場合、長期間の業務停止に至る場合がある。データの保護と早期復旧は事業継続の重要なファクターであり、重要性は急激に増加している。

### 7.1.2 バックアップ運用の現状

バックアップ運用の現状について、次に一般的な事項を記載する。

- データはディスクのミラーリングや RAID<sup>55</sup>構成による保護とバックアップ専用ソフトウェアによる保護が行われている。耐障害性をさらに向上させるため、サーバーをクラスタリング<sup>56</sup>構成にする場合がある。クラスタリング構成を採っていれば、サーバーがダウンした際には、自動的に別の正常に稼動しているサーバーで処理が継続される。
- バックアップ専用ソフトウェアではテープなどの外部記憶媒体にデータを保管する。週末にフルバックアップ、平日は差分/増分<sup>57</sup>バックアップというバックアップスケジュールの設定が一般的である。また、異なるテープを利用して数日前、数週間前に戻るポイントを複数準備する世代管理が行われることが多い。
- 世代管理された旧世代の媒体を遠隔地にある事業所やアウトソーシング企業の免震倉庫などに保管していることが多い。
- 地震対策としては、サーバーの転倒防止措置などに加えて、データセンターを開設している建物自体の耐震構造化が進んでいる。さらに進んだ企業では免震構造にしている。
- データセンターへの電源供給がストップされた場合に備えて、UPS<sup>58</sup>に留まらず自家発電装置を装備する企業も存在する<sup>59</sup>。

---

<sup>55</sup> RAID: Redundant Array of Independent Disks の略称。複数の HDD にデータを分散して保存する装置のこと。

<sup>56</sup> クラスタリングは「複数のコンピュータを相互に接続し、ユーザや他のコンピュータに対して全体で 1 台のコンピュータであるかのように振舞わせる技術」（出典：『IT 用語辞典 e-Words』）である。

<sup>57</sup> 差分: フルバックアップ後に追加/更新された全てのファイルをバックアップする

増分: フルバックアップ以降、前回のバックアップに対して追加/更新分だけをバックアップする

<sup>58</sup> UPS: Uninterruptible Power Systems の略称。無停電電源装置のこと。

<sup>59</sup> 電源設備の災害対策として自家発電装置を選定した事業体は 45.9%、という調査結果が存在する（出典：『平成 17 年度「情報セキュリティに関する調査」集計結果』平成 18 年 3 月 財団法人日本情報処理開発協会）。

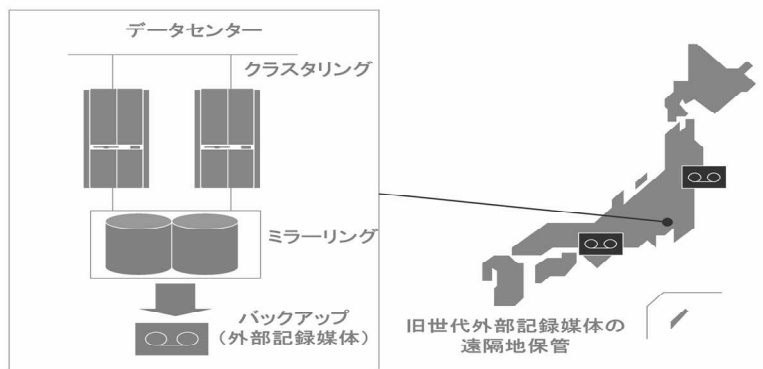


図 18 バックアップの現状

### 7.1.3 バックアップ運用のニーズと現状のギャップ

先述した現状のデータ保護対策はディスククラッシュなど通常のシステム運用で発生する障害時には極めて有効である。また、データセンターの耐震・免震構造化や自家発電装置を装備することは災害対策に効果がある。

しかし、センター内に閉じたデータ保護対策を充実させるだけでは、特に都市型の広域災害発生時にシステムの運用を継続することは難しい。長期間に渡る電力、上下水道、ガス、通信といったインフラの停止や運用要員がセンターにたどり着けない、などの多大なるリスクが存在する。

今回、広域災害に耐えられるデータ保護について調査をする過程で、データセンターと地理的に離れた拠点へのリモートバックアップの導入が本格化しつつあることに着目した。「7.1.2 バックアップ運用の現状」で説明したように、現在、多くの企業では、リモートバックアップは普及していないが、大手金融機関では以前から導入されており、それ以外の企業については、危機管理対策に敏感な企業や業界団体の実験的な試みが、少しずつ始まったという状況である。

リモートバックアップは、広域災害などでサイト運営が不可能となる事態が離れた場所で同時に発生することはない、という前提に立っている。重要なシステムについて、データセンターが利用不可となった場合に、リモートサイトで運用を継続することを目的としている。

これまで、リモートバックアップは高度な技術を利用するため導入の難易度

が高く且つ高価であった。理想的なシステム構成として考えられることはあっても、実際に導入することは難しかった。

しかし、数年前に比べると技術、コスト両面で導入が容易になってきている。実際に信頼性やデータ規模などに応じたソリューションの種類が増えており、雑誌や Web サイトなどでも導入事例が紹介され始めている。

次項ではそういう背景を前提にして、リモートバックアップの技術動向について概観する。

## 7.2 リモートバックアップの技術動向

リモートバックアップは文字通りデータセンターとは別に遠隔地にリモートサイトを開設し、そこに WAN(Wide Area Network)回線を通じてバックアップをオンラインで行う方式である。一例として、東京にデータセンター、大阪にリモートサイトを開設している場合の概念図を記載する。

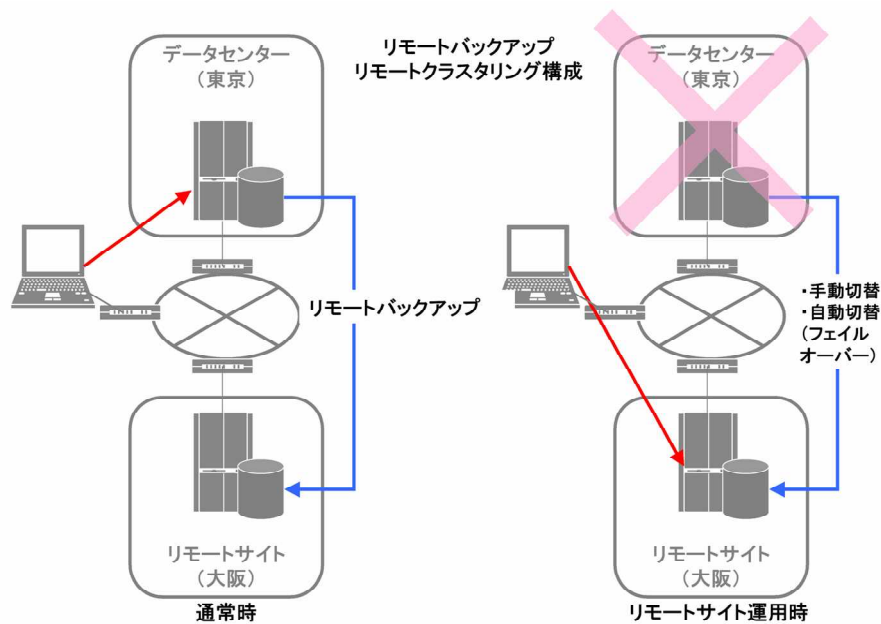


図 19 リモートバックアップの概念図

データセンターでは、通常の運用と並行してリモートバックアップを行う。データセンターが被災するなどサーバーがダウンした際には、リモートサイトのサーバーに自動/手動で処理を引き継ぐ。リモートクラスタリング<sup>60</sup>構成を採っていれば、データセンターサーバーのダウンをリモートサイトのサーバーが検知して自動的にフェイルオーバー<sup>61</sup>を行う。フェイルオーバーには通常少なくとも数秒から数十秒程度必要とするが、ユーザーはほとんど意識することなくサイトが切り替わる。

本項ではリモートバックアップ運用を具現化する様々なツールを、以下のポイントで整理し、各々の動向について概観する。

- リモートバックアップ方式
- リモートバックアップの要素技術

尚、本項では事業継続の観点から最も災害復旧に対する要求が高いと考えられるミッション・クリティカルな基幹系の業務システムを念頭に置き解説する。

### 7.2.1 リモートバックアップ方式

ここでは、リモートバックアップを具現化する実装方式について、その概要とそれぞれを比較した結果を記載する。一般に次の2つに大別される。

- 同期式
- 非同期式

#### 同期式

データセンターとリモートサイトのデータベースが常に一致している方式である。この方式では、データベースへの書込み処理を行う場合、データセンターのデータベースへの書込み処理とともに、リモートサイトのデータベースへの書込みを行う。両サイトでの処理が完了して始めて1つの処理が完結する。あたかも両サイト間を跨ったトランザクションのように処理を行う。

---

<sup>60</sup> クラスタリングを遠隔地にまで拡張した技術である。

<sup>61</sup> 「サーバーに障害が発生した場合に、代替サーバーが処理やデータを引き継ぐ機能」出典:『IT用語辞典 e-Words』

尚、フェイルオーバーを行うために、ツールの提供する機能により、先述のリモートクラスタリング構成を採ることが可能となる。

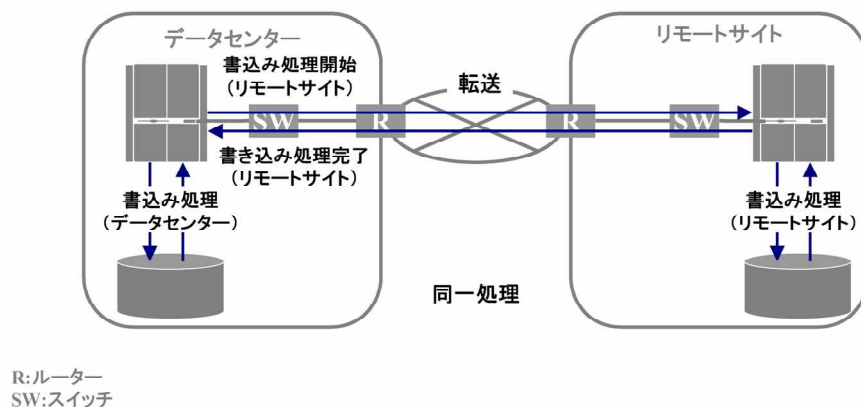


図 20 同期式の概念図

#### 非同期式

データセンターとリモートサイトのデータベースが遅延して一致する方式である。この方式では、データセンターのデータベースに対する書き込み処理はデータセンター内で一旦完結する。リモートサイトへは別途その処理情報を転送する。リモートサイトは処理情報を基にデータセンターとは無関係に処理を行う。この場合、リモートサイトへは設定した時間間隔で定期的に転送を行うが、バッチ処理として一括して夜間などにリモートサイトへ処理情報を転送することもできる。

尚、同期式と同様にリモートクラスタリング構成を採ることが可能である。

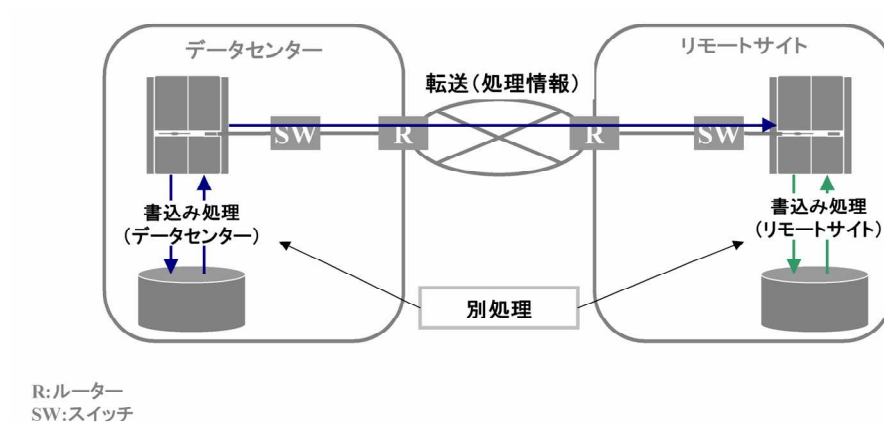


図 21 非同期式の概念図

## 同期式と非同期式の比較

両方式には、相互の方式を比較するとエラー! 参照元が見つかりません。に示すような長所と短所がある。

表 8 同期式と非同期式の比較

|    | 同期式                                                                                                                                 | 非同期式                                                                                    |
|----|-------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 長所 | <ul style="list-style-type: none"> <li>・信頼性が高い</li> </ul>                                                                           | <ul style="list-style-type: none"> <li>・コストがかからない</li> <li>・アプリケーションに負荷をかけない</li> </ul> |
| 短所 | <ul style="list-style-type: none"> <li>・コストがかかる（サイト間で同一ハードウェア構成が前提の場合が多い）</li> <li>・サイト間の距離が長いとアプリケーションのパフォーマンスが落ちる場合がある</li> </ul> | <ul style="list-style-type: none"> <li>・データ損失の可能性がある</li> </ul>                         |

### 7.2.2 リモートバックアップの要素技術

本項では、リモートバックアップの要素技術について以下のように3層に分類して解説する。

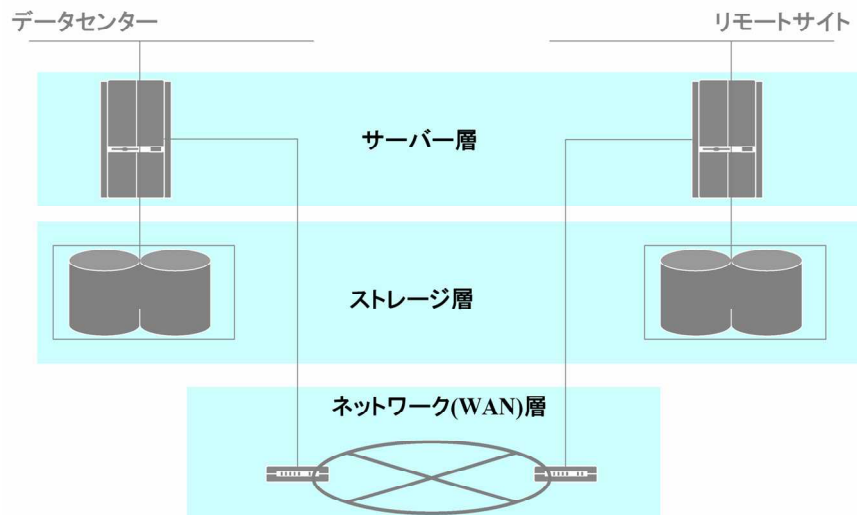


図 22 リモートバックアップの要素技術（3層分類のイメージ）

リモートバックアップにおいて、ネットワーク層は必須であるがサーバー層とストレージ層については、要求仕様に合わせて該当する要素技術を選択することになる。

#### サーバー層

サーバー上でリモートバックアップを行う方式として、次の3つの事項をピックアップして「7.2.3 サーバー層」に記載する。

- ソフトウェアレプリケーション
- データベースツール
- ベアメタルリストア

## ストレージ層

ストレージだけでリモートバックアップを行う方式として、次の 2 つの事項を「7.2.4 ストレージ層」で記載する。

- ストレージレプリケーション
- 仮想サーバー

## ネットワーク層

リモートバックアップで利用されることが多いネットワークサービスについて概観し、最近利用され始めている WAN 高速化装置について、その概要を「7.2.4 ネットワーク層」に記載する。

- 広域イーサネット
- IP-VPN
- インターネット VPN
- WAN 高速化装置

### 7.2.3 サーバー層

#### ソフトウェアレプリケーション

バックアップ専用ソフトウェアでリモートバックアップを行う。この方式では、データセンター側でファイルの追加や変更が発生した場合に、それを検知して一旦ソフトウェア管理下のキャッシュ領域に保存する。変更の場合、両サイトのファイルを比較して、その変更部分だけをデータセンターからリモートサイトに転送する。その変更部分をリモートサイトのファイルに反映することにより、両サイト間のデータ整合性が確保される。

この方式は、ストレージなどのハードウェアに依存しないためサイト間で別のシステム構成を採ることができる。一般にバイト単位でリモートバックアップを行うため、データベースやアプリケーションなどデータ形式を問わない。

このツールでは同期式、非同期式を選択できる。

#### データベースツール

データベースベンダーが提供するオプションソフトウェアなどのツールを利用してリモートバックアップを行う。このツールではログデータを利用してサイ

ト間のデータの同期を図る。この場合もソフトウェアレプリケーション同様、ハードウェアに依存しない。

データベースに特化したバックアップ方式であるため、信頼性が非常に高い。このツールでも、同期式と非同期式が選択できる。同期式ではサイト間のデータベースが密結合のため、データの整合性は保証される。ただし、リモートサイトのデータベースがダウンした際には、データセンターの処理が行えない場合がある。実装方式選定の際には、その点を考慮に入れて検討する必要がある。

### ベアメタルリストア

バックアップ専用ソフトウェアでディスクイメージを DVD などの外部記憶媒体に記録する。従来のテープによるデータのバックアップでは、リストアに至るまでに OS やパッチの適用など数回の再起動を伴う煩雑な作業が発生する。その後、データベースソフトをインストールして、バックアップソフトをインストールする。以上の作業が完了して初めてテープからデータを戻すことができる。

ベアメタルリストアではディスクイメージを取得した媒体をサーバーに戻す操作だけで、取得した状態をそのまま復旧することができる。従来のデータのリストアと比べて大幅な早期復旧が可能である。

ただし、あくまでも取得時点のディスクイメージを復旧するため、当然それ以降に発生した追加・変更などの操作結果は反映されていない。また、基本的に媒体のオフライン搬送が必要となるため、現実的には、通常データセンターサーバーの数日前の状態に戻すことになる。

尚、サーバーの構成は同一であることが基本である。

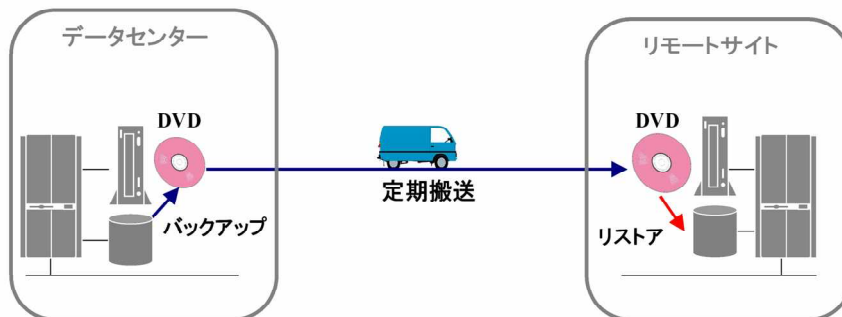


図 23 ベアメタルリストアの概念図

## 7.2.4 ストレージ層

### ストレージレプリケーション

ストレージ装置のデータを物理的にリモートバックアップする。ストレージ装置同士でリモートバックアップを行うため、サーバーの負荷を軽減できる(サーバーフリー)。この場合、SAN<sup>62</sup>構成を採っていることが多い。

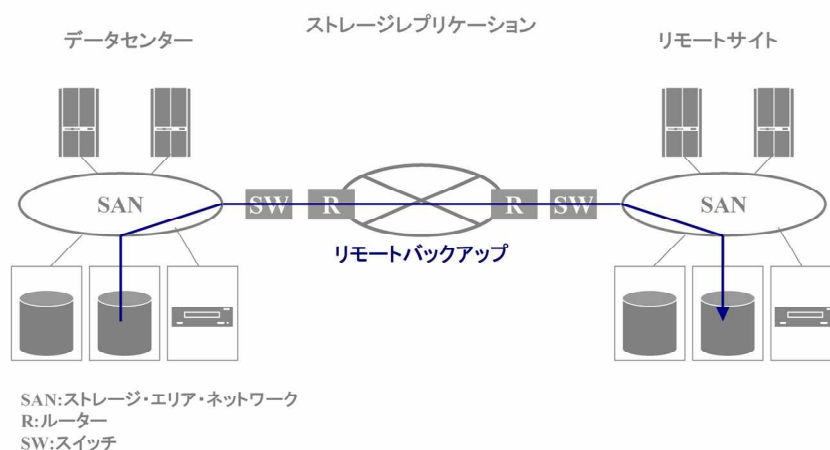


図 24 ストレージレプリケーション概念図

また、ハードウェア構成は、両サイトで同一構成であることが原則である。この方式も同期式と非同期式の構成が可能である。

SAN 構成では、サーバーとストレージ間などを接続する場合、ファイバーチャネル<sup>63</sup>を利用することが基本である。ファイバーチャネルを利用してリモートバックアップを行う場合には、専用の光回線を利用した WAN 構成を採ることが多い。この場合、専用の光回線は高速で品質が良いがその反面コストがかかる。現実的には最大でも両サイト間の距離が 100km 程度で利用されることが多い。

最近では、IP ネットワークを利用して構築する IP-SAN の導入が進んでいる。

<sup>62</sup> Storage Area Network の略称。「SAN とは、複数のサーバとストレージ装置を結び、もっぱらストレージアクセスのために使用されるネットワークである」出典『ストレージネットワーキング技術・SNIA ストレージ技術者認定プログラム準拠』2005 年 7 月 喜連川 優編著 オーム社

<sup>63</sup> ファイバチャネル(Fibre Channel)は主にコンピュータ本体と周辺機器を接続し、ギガビット/秒クラスの高速な通信を行うためのデータ転送方式である。

FCIP<sup>64</sup>、iFCP<sup>65</sup>がそのプロトコルに該当するが、その他 IP ネットワークを利用する方式として iSCSI<sup>66</sup>も挙げられる。

リモートバックアップについても、IP-SAN を利用する場合は、専用の光回線に比べて速度や信頼性が劣る場合が多い。しかし IP-SAN は専用の光回線に比べて圧倒的に低コストであり、サイト間の距離を大幅に延長できる。今後、ストレージでリモートバックアップを行う際には、IP-SAN が普及していくであろう。

また、ストレージ装置そのものは非常に信頼性が高いが、一般に高価である。リモートバックアップ運用を行うためには、同一セットを 2 セット用意する必要があるため、導入に当っては費用対効果について十分検討する必要がある。

### 仮想サーバー

サーバーとストレージの間に仮想化ストレージソフトウェアを実装したサーバーを配置する方式である。

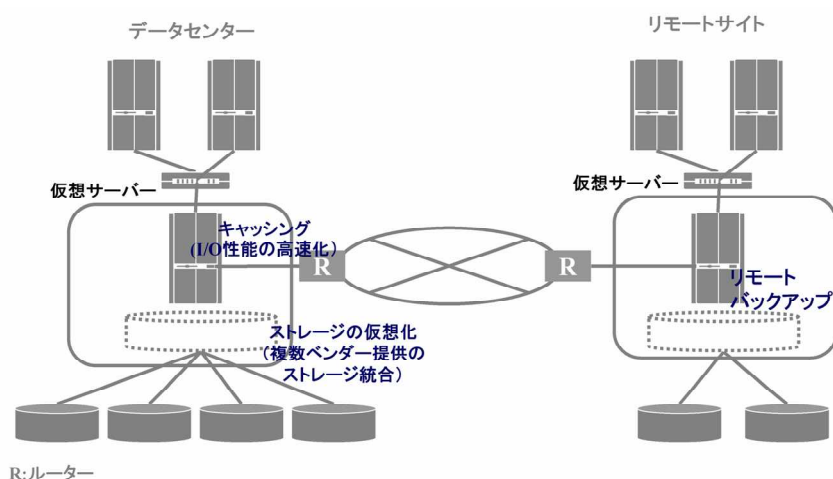


図 25 仮想サーバー概念図

<sup>64</sup> Fibre Channel over IP の略称。ファイバーチャネルのフレーム（基本となるデータの単位）をカプセル化して IP ネットワークで送受信するためのプロトコルの名称。

<sup>65</sup> internet Fibre Channel Protocol の略称。FCIP と同様のプロトコルの名称。iFCP がファイバーチャネルのアドレスを持つのに対して FCIP はアドレスを持たずカプセル化したフレームを透過的に送受信する。

<sup>66</sup> internet Small Computer System Interface の略称。コンピュータと周辺機器を接続する際に利用される SCSI コマンドを、IP パケットでカプセル化して IP ネットワークで送受信するための規格の名称。

仮想サーバーでは、ストレージレプリケーションと同様に、複数のストレージ（異なるベンダーの製品でも可）を束ねてひとつのプール領域として仮想化しサーバーに提供する。また、サーバーに対して大容量のキャッシュ領域を提供することで、サーバーの I/O 性能の高速化を図る。

仮想サーバー構成では、先述のストレージレプリケーションと違い両サイトのシステム構成が異なるものであっても、リモートバックアップを行うことができる。そのため、データセンターと比べてリモートサイトを安価なシステム構成にすることができる。また、必要に応じてストレージを追加できるなど、拡張性の点でも優れている。

リモートバックアップは非同期式ではあるが、大容量のキャッシュ領域を持つことにより、ネットワークがダウンしていても復旧を待って自動的にリモートサイトに送信する。キャッシュ領域のオーバーフローを避けるためにメモリだけではなく、ディスクを利用できる製品も存在する。ただし、被災時などに長期間ネットワークが利用できない場合には、データが損失する場合がある。

尚、この構成では仮想化ソフトウェアがコアとなるが、アプライアンス製品として仮想化ソフトウェアを組み込んでリリースされているものもある。

## 7.2.5 ネットワーク層

### 広域イーサネット

広域イーサネットは LAN で利用しているイーサネット・フレームをそのまま中継できる WAN サービスである。データセンターとリモートサイト同士をあたかも LAN で接続しているかのように利用できる。提供速度については 128kbps<sup>67</sup>～1Gbps など様々なメニューが用意されている。帯域保証や保守などの付加サービスにより料金は異なる。

### IP-VPN

IP-VPN は通信事業者（キャリア）の保有する広域 IP 網を経由して構築される仮想通信網(VPN<sup>68</sup>)である。利用可能なプロトコルは IP に限定されている。通信速度は 10Mbps～1Gbps が中心で、広域イーサネット同様、帯域保証など付加サービスの選択により料金が相違する。また、IP-VPN 網に至るまでの回線を普

<sup>67</sup> bps:bits per second の略称。1bps は 1 秒間に 1bit 転送することを表す。

<sup>68</sup> VPN:Virtual Private Network の略称。公衆回線をあたかも専用線のように利用する技術を指す。

及型の光回線や ADSL 回線を利用する複合型のサービスもリリースされている。

### インターネットVPN

インターネット VPN はインターネットを利用した VPN である。IP-VPN と比べるとインターネット VPN の方が低コストである。ただし、インターネット VPN は帯域制御がされないため、品質は IP-VPN が優れている。

現在、バックアップ専用で利用するネットワークサービスとしてインターネット VPN が脚光を浴びている。一般にバックアップ用のサービスは品質面よりもコスト面での要求が強い。そのためプロバイダーが提供する普及型の光回線や ADSL 回線を採用しているサービスを採用している事例もある。

### WAN 高速化装置

リモートバックアップでは遠隔地にデータを送信する。その場合、近距離に送信する場合と比べて遅延が発生する。遅延防止に対して効果的な WAN 高速化装置が利用され始めている。

WAN 高速化装置は WAN 回線を効果的に利用するための装置である。TCP プロトコルの最適化、データ圧縮、キャッシュなどの機能を実装する。

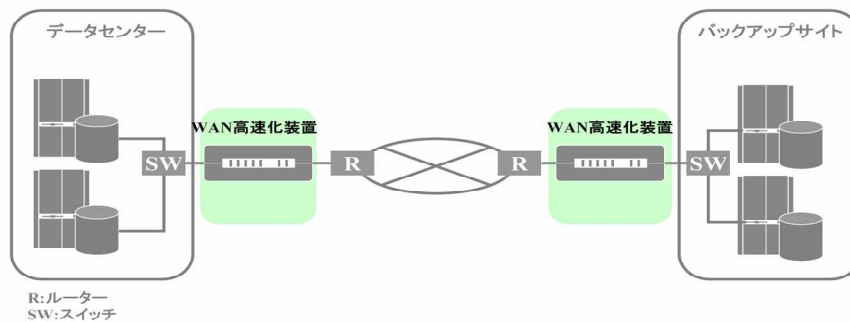


図 26 WAN 高速化装置の概念図

各種ネットワークサービスで利用される WAN 回線の品目速度と実際の速度は異なる。先述のとおり、サイト間の距離に応じて遅延は大きくなる。関東地方に両サイトを配置した場合と東京と大阪に配置した場合とでは倍以上の遅延が発生するという事例がある。受信先からの確認応答を待つ TCP では、その都度遅延

が発生しパフォーマンスが悪化する。

WAN 高速化装置の導入による効果は、リモートバックアップの転送に対する効果というよりもむしろ、Windows のファイル共有プロトコルである CIFS<sup>69</sup>などを利用している既存回線を含めたオーバーヘッド解消に効果がある。

言うまでも無いが、実際のネットワーク環境によりその効果は異なる。そのため、導入前に効果測定などの検証が必要になる。実際にベンダーサイドでも検証を推奨していることが多い。

---

<sup>69</sup> CIFS: Common Internet File System の略称。「CIFS は Microsoft 社によって開発された Windows 上のファイル共有機能を、インターネットプロトコルをサポートするネットワーク上で使えるようにしたものであり、Windows 上のファイルアクセスを、ネットワークを介した環境で実現するように設計されている。」 出典:『IT セキュリティソリューション体系 下巻 IT セキュリティエンジニアリング』2004 年 株式会社フジ・テクノシステム

## 7.3 リモートバックアップの技術選択

前項までにリモートバックアップには、複数の要素技術が存在し、技術採用に当って選択肢があることを記載した。それでは、実際にツール選択の際にどのような事項を検討すればよいのだろうか。次に、少なくとも検討すべきと思われる事項をまとめる。

### 7.3.1 RPO/RTO/RLO

ここで記載する RPO/RTO/RLO は、ビジネス要件から決定すべき事項である。技術選択の前提として定義しておく必要がある。

まず、それぞれの定義について記載する。

- RPO (Required Point Objective) 目標復旧ポイント:  
どの時点までデータを戻せるか
- RTO (Required Time Objective) 目標復旧時間:  
どれだけ事業を早く復旧できるか<sup>70</sup>
- RLO (Recovery Level Objective) 目標回復レベル:  
業務再開するにはどのレベルまで復旧させればよいか

RPO や RTO はこれまでよく使われてきた。RLO は比較的最近よく使われている用語であり、どこまで復旧できれば業務再開するのか、という指標である。

災害時には、業務再開を急ぐあまり、不十分な状態のままで再開してしまう可能性がある。予め RLO を具体的に定義しておけば、比較的問題が少ない状態で業務再開が可能になる。

---

<sup>70</sup> RPO、RTO の定義については次を参照した。2005 年『事業継続計画(BCP)策定ガイドライン』経済産業省商務情報政策局情報セキュリティ政策室編

【目標復旧時間、目標復旧ポイントおよび目標回復レベルの概念】

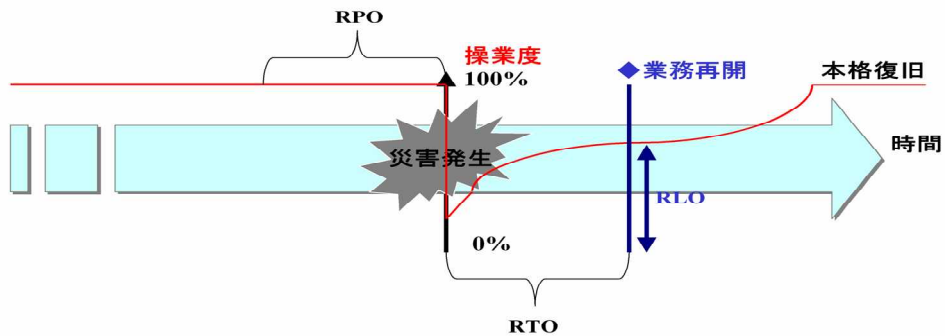


図 27 RPO/RPO/RLO の概念図

次に RPO/RTO からバックアップ方式およびツールを選定するテンプレート例を記載する。

| バックアップ対象システム                 | RPO (レベル) | RTO (レベル) | バックアップ方式          | ツール                  |       |
|------------------------------|-----------|-----------|-------------------|----------------------|-------|
| 生産管理<br>販売管理<br>会計           | 秒         | 秒         | リモートバックアップ(同期方式)  | データベースツール<br>/仮想サーバー | オンライン |
|                              | 分         | 分         | リモートバックアップ(非同期方式) |                      |       |
| メールサーバー                      | 時間        | 時間        | リモートバックアップ(非同期方式) | 仮想サーバー               | オフライン |
| 公開Webサーバー<br>文書管理            | 日         | 日         | ベアメタルリストア         | バックアップ専用ツール          |       |
| スケジュール管理<br>社内情報共有<br>社内名簿管理 | 週         | 週         | データバックアップ         | バックアップ専用ツール          |       |

図 28 バックアップ方式・ツール選定のテンプレート例

まず、①バックアップ対象システム単位に RPO と RTO のレベルを決定する。次に、RPO/RTO に基づいて②バックアップ方式を決定し、③それを具現化するツールを決定する。例えば、生産管理システムは秒単位の復旧ポイントと秒単位の復旧時間が要求されとした場合、信頼性を重視して同期方式のリモートバックアップを選択する。それを具現化するツールとしてデータベースツールを採用

する。以上のようなステップでツールを決定することが必要と考える。

### 7.3.2 サーバー層およびストレージ層の検討項目

大きな投資が必要になる可能性がある層であり、一度設備を導入すると構成変更が難しい。十分に投資対効果などを検討して選択する必要がある。以下に検討項目を例示する。

#### 対象データ範囲の選定

どのデータをリモートバックアップの対象にするのかを選定する必要がある。選定の際には、対象データのデータ関連性を確認する必要がある。どのデータ単位でリモートサイトバックアップを行うかを決めるためには、データ関連性の明確化が必須になる。

例えば、単純に販売管理システムだけを対象に切り出してリモートバックアップを行った場合、関連する在庫管理システムや会計システムなどとのデータの整合性を保持することは難しい。在庫品を販売してその売上を計上するといった場合は在庫、販売、会計システムなどが連動する。より大きな業務システムという枠に対象範囲を拡大せざるを得ない。その場合リモートサイトのシステム規模やデータ転送量が拡大する。

システム単位に先述の RPO/RTO を判定して、最短のシステムに全体を合わせるという方法も有効である。

#### データのライフサイクルの検討

データは増加する一途であり、そのライフサイクルを考慮する必要がある。特にリモートコピーを行うデータは長期保管データまで含めると運用やコスト面で厳しくなる。確定したデータで、かつ参照頻度がほとんどないデータは、データセンター側でより安価なディスクや磁気テープなどの別媒体へ移行する（保管から保存へ工程が移行する）。別媒体への移行が完了したらリモートサイト側ではそのデータを削除する、もしくはリモートサイトと同様に安価な媒体へ移行するなどの仕組みが必要である。

データセンター側で復旧優先度の高い重要なデータを絞り込む運用が実践できれば、リモートサイト側での運用負荷を大幅に軽減できる。そのためには、組織全体で先述の ILM を運用する必要がある。更に複数サーバーへ復旧優先度が高

いデータが散在している場合は、データセンターへの集約も検討すべきである。

#### **優先事項の決定**

信頼性を優先するのか、コストを優先するのか、ステップアップを考慮して柔軟性を優先するのかなどを選定してリモートバックアップ構成を検討する必要がある。

#### **リモートサイトの運用方法の選択**

リモートサイトをバックアップサイト用途専用で運用するのか、ビジネスインテリジェンス<sup>71</sup>や開発・テスト環境など他の用途でも利用するのかなど運用方法を選択する必要がある。

#### **保守運用体制の決定**

シングルベンダー体制であれば保守運用体制も一本化され構築しやすいが、当然調達コストは高くなる。マルチベンダー環境では調達コストは大幅に抑えられるが、障害切り分けなどユーザーサイドで行うべき事項が増える。状況監視や異常時の対応など運用負荷を考えて体制を決定すべきである。

### **7.3.3 ネットワーク層の検討項目**

#### **データ転送量の想定**

これは同期式か非同期式か、どのツールを使うのかによって変動する。システム構成全体の決定が前提となる。データセンターからリモートサイトへのデータ転送量を予測することは、ネットワークサービスを選択するために必要である。さらにピーク時のデータ転送量を考慮しておく必要がある。

#### **ネットワークサービスの提供内容**

先述したとおり、ネットワークサービスが複数存在するため、そのサービス内容やサポートする通信回線などについて検討する。その際には、通信速度や品

---

<sup>71</sup> ビジネスインテリジェンスとは、「業務システムなどから蓄積される企業内の膨大なデータを、蓄積・分析・加工して、企業の意思決定に活用しようとする手法。ERP パッケージや CRM ソフトなどからもたらされるデータの分析を専門家に依存せず、経営者や社員が必要な情報を自在に分析し、経営計画や企業戦略などに活用することを目指している。」出典:『IT 用語辞典 e-Words』

質などの仕様に加えて、ランニングコストも当然重要な検討項目の一つになる。

#### **必要な機器の選定**

必要に応じてルーターやスイッチなどの選定を行う。先述の WAN 最適化装置なども選択肢の一つである。

その他、検討すべき項目としてリモートサイトの運営体制がある。

#### **7.3.4 リモートサイトの運営体制**

リモートサイトを組織内で運営するか、プロバイダーが提供するサービスを利用するかを検討する必要がある。具体的には、プロバイダーが提供しているリモートバックアップサービスの利用を検討することになる。サービスでは、提供メニューにもよるが、基本的に顧客のサーバーやストレージをプロバイダーのサイトに設置し、その顧客専用のリモートサイトを開設する。

その際、リモートサイトの運用監視などはプロバイダーの要員が行う。当然機器に加えて運用コストが加算されるが、自組織内でリモートサイトに適した場所の確保や要員確保が難しい場合には、検討の対象となる。

なお、RPO や RTO が許容できる範囲内にあれば、災害時に共用の設備を利用して遠隔地に保管しているテープなどから復旧するというレベルのサービスを利用することも可能である。この場合、顧客専用リモートサイトと比べて大幅にコストダウンが図れる。

## 7.4 バックアップ技術を活かすために

バックアップは取得することが目的ではない。リストアを RPO/RTO の定義どおり行えることが目的である。当然、事業継続に不可欠なシステムのリストアの失敗は、事業継続に多大なる影響を及ぼす。

表 9 は、システム障害における売上損失額の例である。

表 9 システム障害における売上損失額例 (1 時間相当) <sup>72</sup>

|             |              |
|-------------|--------------|
| 金融仲介        | 6,500,000 ドル |
| クレジットカード    | 2,600,000 ドル |
| 有料ビデオ放送     | 150,000 ドル   |
| TV ショッピング   | 113,000 ドル   |
| カタログショッピング  | 90,000 ドル    |
| チケット予約・販売   | 89,500 ドル    |
| 電話チケット予約    | 69,000 ドル    |
| 宅配便         | 28,000 ドル    |
| キャッシュディスプレイ | 14,500 ドル    |

しかしながら、先述のとおり、バックアップは取得していることが多いが、一般的にそれで安心してしまう傾向が強い。リストアが十分にテストされていない、という運用要員の声もよく聞く。

実際にリストアを行う場合には思いがけないエラーやデータベースの不整合などが発生し、復旧に手間取ることが多々ある。ましてや被災時など通常とは状況が大きく異なる場合にはオペレーションミスなどの不具合も発生しがちである。

また、エラー発生時の対処が不明だった場合に、不明な事項を確認するルートが閉じている、もしくはノウハウを持つ要員にアクセスできない場合などに、パニック状態に陥る危険性がある。

本章のテーマであるリモートバックアップは、ツールを利用してリモートサイトのバックアップを鮮度が高い状態にしておくことで、被災時の対応を大幅に省力化し且つシステムのダウンタイムを極小化することに大いに貢献する。リモ

<sup>72</sup>出典:平成 18 年 3 月独立行政法人科学技術振興機構社会技術研究開発センター「情報と社会」研究開発領域計画型研究開発『社会技術研究開発センター「情報と社会」研究開発領域計画型研究開発「高度情報社会の脆弱性の解明と解決」平成 17 年度成果報告書』P45 表 2-7 資料:Strategic Research group

ートバックアップは事業継続を担保する一つの技術として有効である。

本章の冒頭に述べたとおり、リモートバックアップは一般企業に導入が始まりつつある。今後もツールの更なる機能の向上や価格低下によりその傾向は顕著となろう。更に有効な手法、製品やサービスが続々とリリースされると思われる。

リモートバックアップの手法やツールをよく知り、適切に選択することは極めて重要である。ただしツールはあくまでも道具でしかない。機能が如何に優れていようが適材適所に機能を活かした運用がされることで始めて価値がでる。

また、現状ではリモートバックアップ対象は事業継続に重要なシステム、すなわち基幹系の業務システムでの利用が中心となり、特にコスト面で情報系システムまでカバーできない可能性が高い。この場合、先述のベアメタルリストアやテープからのリストアなど、今後も複数のバックアップ手法を併用する必要がある。そのためにも、適切な要員とそれを支える体制の構築とその継続が非常に重要である。

## 8 まとめ

### 8.1 事業継続に関する全体動向

昨年度の調査に比べ、事業継続に関する活動が活発化している。特に、各国政府ならびに国際機関における新たな取り組みが始まっている。その背景には、各地域で頻発する大規模自然災害やパンデミック・インフルエンザなどの脅威の再認識がある。また、対テロ対策が推進され、推進組織からより具体的なアウトプットとして現れてきたと言う側面もあろう。さらに、米国の SOX 法対応に代表されるコーポレート・ガバナンスへの取り組みが推進され、リスクマネジメントへの関心が高まったことも、事業継続に関する活動の増加を後押ししている。

#### 8.1.1 事業継続の規格やガイドラインについて

規格やガイドラインが、どのようなステップを踏んで計画を策定すればよいかというフレームワークのみを示すに止まっている現状は、昨年度の調査結果と変わらない。これは、あらゆる形態の組織も使えるようにする必要があるという規格やガイドラインが持つ本質的な性格に由来するものである。しかしながら、組織ごとに大きく異なるとはいえ、事業継続の分野において、標準化に対する強いニーズがあることも否定できない事実であり、その結果、自己判断の部分を多くし、柔軟性を持たせる形での規格化が推進されている。

フレームワークのポイントは、次のようにまとめられる。

- 事業継続計画策定と維持継続のための組織体制を構築すること。
- 事業継続計画を策定し、更新すること。
- リスクアセスメントやインパクト分析などを行い、考慮すべき脅威や保護すべきビジネスプロセスなどについて、優先順位付けをし、戦略的な計画策定や取組みを可能にすること。
- 啓発や訓練などを通して、文化や意識の構築と定着を図ること。
- 監査などを実施し、継続すること。

事業継続計画に取り組む組織は、実装や運用について、専門家の助言を仰いだり、組織内で専門知識を有する人員を育成したり、試行錯誤を重ねたりなどし

て、進めていかなければならない。

また、本報告書の第5章でも触れたが、その活動を助けるために、専門家や担当者が活用できるマネジメント支援ツールが開発され進化している。このようなツールとしては、ソフトウェアが提供する選択肢を使うことにより、比較的初心者でも使えるものから、ツールは枠組みだけを提供し個々の利用者がカスタマイズすることにより、組織の事情に合ったマネジメントが行えるようになっているものまで幅広くある。カスタマイズが必要なツールを提供している企業では、ユーザー・コミュニティを支援し、専門家が互いに情報交換してより洗練されたマネジメント手法を開発できるような工夫がなされている。

また、地域特性や業界特性を反映したガイドラインも開発が進み、金融業界はもとより、半導体業界などでも、それぞれの状況にあわせたガイドラインが作成されている。わが国でも、建設業界でガイドラインが作成されたり、中小企業向けの事業継続計画作成支援などが始まっている。

### **8.1.2 欧米における取り組みの現状から**

金融業界での取り組みが、他の業界よりも先行して進んでいることは昨年度の調査と変わりはない。米国や英国では、銀行や証券業界などでは、事業継続計画策定が一巡した状況であり、訓練などを通じた見直しと継続のフェーズに移りつつあるといえよう。

製造業における取組みにおいても、サプライチェーン全体の事業継続の必要性から、取り組みが進んでいる。その動きは、製造プロセスを事業継続の視点から見直すという大きな変革をもたらしつつある。

専門のサービス提供会社の活用は、わが国ではまだあまり進んでいないようであるが、昨年度も紹介した従業員用ワーク・スペースや移動式データ・リカバリーセンターなどは、今後わが国でも、提供され、ユーザー側も活用できるようになることが強く望まれる。

### **8.1.3 事業継続の専門家について**

専門家の育成は、昨年度と比べてそれほど進んでいるとはいいがたい。やはり、大学などの教育機関で、今後いかにして必要な人材を育成するかを検討すべきである。また、企業等の組織レベルでも、内部で人材を育成するか否かとい

った判断に迫られている事情は変わらないが、コーポレート・ガバナンスの重要性が高まっている現在、組織として事業継続に取り組むための体制整備は不可欠であり、そこで役割を果たす人材をどのような形で育成するかは、避けることのできない課題になっているように思われる。そのためにも、教育機関と産業界の連携が重要である。

## 8.2 パンデミック・インフルエンザ対策

わが国でも、宮崎県や岡山県など、相次いで高病原性鳥インフルエンザが発生した。いずれは、ヒト・ヒト感染へと変化するのではないかとされている。欧米の事業継続管理専門家の多くは、発生した特定の地域に封じ込めるのは難しいと考え、アウトブレイクからパンデミック・インフルエンザに発展するのは、時間の問題であるという人もいる。このパンデミック・インフルエンザに対する計画は、従来型の事業継続計画とは異なるため、その準備が急がれているのである。

本調査報告では、世界保健機構（WHO）ならびに各国政府主導の元で行われているさまざまなパンデミック・インフルエンザ対策活動について、事業継続の視点からまとめた。わが国では、まだ政府機関や医療機関の問題として捉えられている側面が強いように感じられるパンデミック・インフルエンザ対策であるが、実は企業などの事業継続管理の取り組みが非常に重要であるということが諸外国の取り組みから伺える。

### 8.2.1 想定されるシナリオ

パンデミック・インフルエンザが発生した場合、約 4 分の 1～3 分の 1 の従業員が不在になるというシナリオを想定する必要がある。最悪の場合は、2 分の 1 以上という状況も考えておかなければならない。全世界での流行であるから、他の地域でのバックアップサイトで業務を続けるというシナリオは成り立たない。また、その期間もこれまで体験してきた地震や洪水といった大規模災害よりも長い。2 ヶ月から 4 ヶ月は続き、それが 1 年半以上にわたり、一定の期間を置いて繰り返される。最初の流行が去った後も、次の流行に備えて計画を見直すなどの柔軟性が要求される。

### 8.2.2 パンデミック・インフルエンザ計画のポイント

計画策定のプロセスは、基本的に従来の事業継続計画と変わらない。業務分析を行い、戦略を立て、具体策を決め、訓練やテストを行い、見直す。これを継続し定着させていくという流れである。

特徴としてあげられる対策のポイントとしては、次のような項目が考えられる。

- 中央政府や自治体の活動についての情報を常に入手し、連動した計画を立てる。
- 中核となる事業を特定する。
- 従業員の保健衛生に必要な設備やアドバイスを行う。
- 従業員が出社できなくとも、自宅などで業務を続けられるようにしておくこと。
- 会議を行ったり、訪問できなくなっても、取引先や顧客とコミュニケーションできる手段を準備しておくこと。

従業員自身が健康であっても、家族の看病や子供の学校閉鎖などにより、出社できなくなる可能性も考慮する必要がある。また、海外でアウトブレイクが始まった際、現地で勤務する従業員を帰国させるためのルールも準備しておかなければならない。

移動手段の発達により、今世紀のパンデミック・インフルエンザは、初期の発生からグローバルな感染拡大までのスピードが非常に速いと予測されており、事前の計画策定は、全ての組織にとって喫緊の課題である。

### 8.2.3 国家全体としての取組みの重要性

本報告書で取り上げた鳥インフルエンザなどのパンデミック系の事案への対応については、面とフローの観点が必要であり、具体的には地域、業界をまたがった速やかな協業が必須である。しかしながら、現在の行政の枠組みにおける地方自治体間の連携や、政府の各事案毎の所管省庁間の連携について、事前の調整ができていくかという点については疑問である。パンデミック系の事案は社会的な動揺や個々人の心理的なパニック状態の集積により、「想定外」の連鎖事案に繋がる可能性が極めて大きいことから、社会・経済の安定性確保のために国家全体としての視点から議論を開始することと、官民挙げての分野横断演習などを通じた取組みに一刻も早く着手することが、喫緊の国家的課題であるとも言える。

### 8.3 事業継続を支援する技術

本報告書では、事業継続を支援する技術として、近年発展が目覚しいリモート・バックアップ技術を取り上げた。急速に増大する情報量とその活用は、単にバックアップを取っておけばよいという考え方から、どの情報が重要で、どの情報が優先的にリストアされる必要があるかというバックアップ戦略という考え方への転換を要請している。

このことは、同時にリストア中などに不測の事態に遭遇した場合に、正確に状況を把握し、的確な判断を下す知識・スキルを保有した要員とその要員をバックアップする体制の重要性を明確にした。

復旧に携わる要員の育成と体制確立に必要なと思われる事項は次のようにまとめられる。

- 要員の役割と責任を明確に定義する
- 複数の要員が復旧作業に対応できるようにする
- 復旧手順を文書化する（文書は簡潔・明確・容易であること）
- 緊急時にはベテランでもミスする可能性があるため、手順の文書化は必須である
- 教育と訓練を定期的実施する
- バックアップツールに精通する
- 基幹システムのコアとなるデータベース技術を理解する
- 訓練目標を明確にする（復旧目標時間の設定など）
- ウォークスルー（机上テスト）、復旧テストを実施する

今後、ITの重要性がますます高まっていく中で、高度な技術がユーザーインタフェースの影に隠れてブラックボックス化の促進が加速するであろう。特に重要であるデータベースについては、不測の事態に備えてオペレーションだけではなく、基本原理を十分に理解しておく必要がある。

## 8.4 まとめ

昨年度の調査と比較すると、事業継続への取り組みは、グローバル・レベルで加速している。わが国は、地震防災を中心として長年取り組んできた歴史がある。また、日本政策投資銀行が他の国々に先駆けてはじめた、防災格付け制度は、防災への取り組みと企業価値をつなぐ画期的な取り組みとして特筆される事柄であろう。

しかしながら、パンデミック・インフルエンザなど新たな脅威に対する備えは、まだ十分とは言いがたく、早急な取り組みが必要である。米国の専門家が集まるコンファレンスでは、すでにパンデミック・インフルエンザに対する何らかの対処を行っている組織についての質問があった際に半数以上が手をあげていた。わが国でも、個々の企業などの組織が、パンデミック・インフルエンザに代表される、地震以外の新たな脅威に対しても、それを政府や医療機関などの特定の機関の問題として認識するのではなく、自らの問題として取り組むことが重要である。

現在、わが国でも多くの組織が取り組んでいる日本版 SOX 法であるが、それを単なるコンプライアンスの問題として終わらせるのではなく、組織のリスクマネジメントである ERM へと発展させ、その枠組みの中で、新たな脅威に備える事業継続管理の取り組みも推進されることが望まれる。ERM への取組みにおいて開発された体制やプロセスと、伝統的な防災から発展したり、情報通信システムにかかわる事故への取組みとして発展してきた事業継続に関する管理のあり方とを、組織への実装段階において、いかに調整するかというテーマを喫緊の課題として捉えなければならない時期にきている。

— 禁 無 断 転 載 —

平成 19 年 3 月発行

編集：富士ゼロックス 株式会社

〒107-0052 東京都港区赤坂九丁目 7 番 3 号（東京ミッドタウン）

TEL:03-6271- 5111 (代表)

発行者：財団法人 日本情報処理開発協会

〒105-0011 東京都港区芝公園 3-5-8 機械振興会館内

TEL:03-3432-9386

E-mail:info@isms.jipdec.jp

印刷所：山 陽 株 式 会 社

東京都千代田区神田神保町 1-18

TEL:03-3293-5411

18-H007