

事業継続管理（BCM）に関する 利用ガイド

平成 18 年 3 月



財団法人 日本情報処理開発協会



この事業は、競輪の補助金を受けて実施しました。

はじめに

企業などの組織活動において、IT依存度はかつてないほど高くかつ重要になっている。そのような状況下、「情報」の処理・流通・保管の形態については紙の文書やソフトウェアなど様々な形態があり、情報セキュリティへの取組みがますます重要となる。

情報資産の保護という情報セキュリティマネジメントの目的を達成するには、多様化するリスクについて、顕在化させないための予防策と同様に、顕在化した場合にできるだけ損失を小さくする事故対応策を考えておく必要がある。特に事故対応策の中でも事業のサステナビリティへの影響を考慮し、事前に事業の継続計画を策定しておく「BCP（事業継続計画）」及びそれを戦略的に実践するBCM（事業継続管理や事業継続経営と訳される）に焦点を当て、適切な情報資産の保護のあり方について調査研究することは重要であり、情報セキュリティマネジメントの中でBCMの位置付けは非常に大きい。

世界では、様々なBCMのガイドラインが発行されているが、これらを網羅的に取りまとめた資料が無かったため、当協会では専門部会を設置してガイドラインの関連性についてまとめた。

本部会では、国内外のBCMの取組について企業や団体などの活動の調査をするとともに、日本を含めた世界で発行されているBCMのガイドライン・指針などを調査し、本利用ガイドを策定した。本利用ガイドは、我が国の企業など組織におけるBCMの取組を推進させ、今後の日本企業（含む、海外に所在する日本企業）、政府・官公庁を対象に事業継続活動に資する情報を提供するものである。

本利用ガイドの作成にあたり、ご協力頂いた委員の皆様をはじめ関係各位に対し厚く御礼申し上げます。

平成18年3月
(財)日本情報処理開発協会
情報セキュリティ専門部会
委員長 篠原 雅道

目次

はじめに	3
1. 第1章 BCM の必要性	6
1.1 概要	6
1.2 事業継続を脅かした事例	7
1.2.1 日本の事例：新潟中越地震	7
1.2.2 ロンドン連続爆破テロ	8
1.2.3 事業継続不能に陥る悪循環	11
1.2.4 BCM はなぜ必要か	11
1.2.5 欧米では、リスク管理上企業の事業継続に対する関心が最も大きい	12
2. 第2章 BCM の構築と導入動向	13
2.1 BCM の構築について	13
2.1.1 BCM の定義	13
2.1.2 BCM 構築・確立のためのプログラムマネジメント	14
2.1.3 経営トップのコミットメント・推進	15
2.1.4 ビジネスインパクト分析（BIA ; Business Impact Analysis）	15
2.1.5 BCP の展開	16
2.2 日本企業と海外企業の BCM 導入動向結果	18
2.2.1 BCP の展開	18
2.2.2 BCP を策定した理由	20
2.2.3 BCM 責任者の関心あるリスクについて	20
2.2.4 過去に事業継続を妨げた事象について	21
2.2.5 基幹業務が停止した場合に許容できる停止時間	21
3. 第3章 世界の BCM に関するガイド	22
3.1 事業継続ガイドライン 第一版・わが国企業の減災と災害対応の向上のために	22
3.2 事業継続計画(BCP)策定ガイドライン - 高度 IT 社会において企業が存続するために-	25
3.3 中小企業 BCP 策定運用方針	27
3.4 PAS (Publicly Available Specification) 56 Guide to Business Continuity Management	29
3.5 NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs	31
3.6 Business Continuity Management Good Practice Guidelines	34
3.7 TR19 事業継続管理(BCM)のためのテクニカル・レファレンス	36
3.8 金融機関等のコンティンジェンシープラン策定・運用に関する研究会 報告書	45
3.9 The Business Guide to Business Continuity Management	48
3.10 Expecting the unexpected	49
3.11 Civil Contingencies Act 2004	50

3.12 Basel Capital Accord	51
3.13 Business Continuity Management Guidelines	52
3.14 Business Continuity Management HB221:2004	54
3.15 Contingency Planning Guide for Information Technology Systems	55
3.16 The Disaster Process and Disaster Aid Programs	56
3.17 Federal Legislative and Regulatory Business Continuity Requirements for the IRS	57
3.18 FFIEC BCP Handbook	58
3.19 FSA Handbook / Financial Sector Business Continuity Annual Report	59
3.20 NERC Continuity of Business Processes	60
3.21 NFA Rule 2-38	61
3.22 NYSE Rule 446	62
3.23 SS507 Singapore Standard for Business Continuity/Disaster Recovery (BC/DR) for Service Providers	63
3.24 TM-G-2 Business Continuity Planning	64
4. 第4章 ケーススタディ	65
4.1 日本ヒューレット・パッカート社の事例	65
4.1.1 BCM 構築の心構え	65
4.1.2 米国のリスクマネジメント	66
4.1.3 HP 社の BCP (COP)	67
4.1.4 マニュアルはそんなに必要か？	69
4.1.5 想定する被害と対応	70
4.1.6 BCP 以前に平時のリスクマネジメントありき	71
4.1.7 BCM の輪を広げよう	71
4.2 ICT 分野における海外先進事例	72
4.2.1 ビジネスアプリケーションのパフォーマンス低下と停止について	73
4.2.2 事業継続におけるセキュリティの重要性（サイバー脅威から見た BCM/BCP）	79
4.2.3 ディザスター — BCP/DRP 導入とチャレンジ	81
5. 第5章 世界の今後の方向	88
5.1 世界の動き	88
5.2 日本の動き	88
5.3 ISO の動き	89
附録 情報セキュリティ総合的普及啓発シンポジウムにおける講演内容	92
おわりに	101

1. 第 1 章 BCM の必要性

1.1 概要

地震・風水災などの自然災害、火災、大規模なシステム障害などが日本で相次いで発生している。海外では、2005 年 7 月に発生したロンドン中心街シティー近辺を狙ったテロでは 50 名以上の死者を出した。また、8 月に米国ニューオリンズを襲ったハリケーン・カトリーナでは、1,000 名以上の死者を出し、数千人に達する可能性も指摘されている。一方、最近ではサプライチェーンマネジメントの浸透により、自社だけでなく原材料調達企業や納入先企業の事故により思わぬところから企業存続の危機に立たされるケースも見られる。企業の事業継続への関心は確実に高まっており、今や企業の事業継続への取組みは重要な経営課題の一つとなった。

事業継続経営（BCM : Business Continuity Management）は以前から欧米の企業中心に経営管理の一環として行われてきたもので、特に 2000 年問題や 2001 年 9 月 11 日の米国における同時多発テロ以来、企業はその取組みを強化している。欧米では、一般的にリスク意識が非常に高く、「事故発生を前提とした考え方」で、万一大規模な事故・災害・事件が発生した場合に、如何に事業を守っていくかという BCM の推進が図られている。海外では、BCM をリスク管理手法の中心的課題、発展形・進化形と位置付けて取組んでいる。

ガイドライン化の動きも世界的には活発である。先ず BCM に関するガイドラインを世界で初めて作成・発行したのは、BCI（事業継続協会）である。これは、2002 年に「Good Practice Guidelines（実践的な指針）」として発行された。このガイドラインをもとに、英国規格協会が「PAS56（一般仕様書）Guide to Business Continuity Management」として発行したが、これは現在国家規格の前段階にある。BCI は、「実践的な指針」と「一般仕様書」の 2 つを実際に企業や政府・官公庁に活用してもらい、そこからのフィードバックをベースに、2005 年 2 月に「実践的な指針」を全面改訂した。英国規格協会と BCI はその後共同リリースを行い、一般仕様書を併せて改訂し、国際標準に歩み出すと発表した。日本では、日本規格協会が PAS56 をもとにして、2004 年 6 月に日本で初めて BCM に関するガイドライン「事業継続管理のための指針」を発行した。その後、2005 年 3 月に経済産業省から「事業継続計画策定ガイドライン」、そして 2005 年 8 月に内閣府から「事業継続ガイドライン」が各々発行された。一方、アジアに目を向けると、日本よりもいち早く BCM のガイドライン化が始まっている。例えば、シンガポール、香港、マレーシアなどでは、既に PAS56 をベースとして BCM のガイドライン化が進んでいる。特にシンガポールでは国内規格として近々成立する見込みである。今後の世界的な規格化・標準化の動向がますます注目される。

本章では、事業継続を脅かした事例を BCM の観点から解説し、BCM の必要性について概説する。

1.2 事業継続を脅かした事例

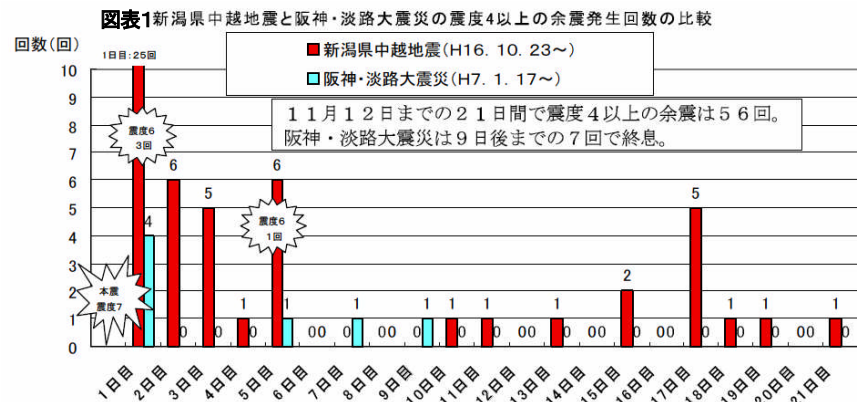
ここでは、BCMに関する日本と海外の事例を挙げる。日本の事例では、新潟県中越大地震（新潟県中越地震）を挙げているが、本地震は多くの日本企業がBCMへの取組みの契機となった。

1.2.1 日本の事例：新潟中越地震

「同じ災害は2度起きない。」これは災害対策を検討する際の鉄則である。しかし、1995年に発生した阪神・淡路大震災で、防災の専門家ですらこの鉄則を忘れてしまった。「阪神・淡路大震災の時には・・・」、「阪神・淡路大震災ではこうだった」というのが組織の地震対策を検討する際の前提条件になってしまっていた感があった。

企業の地震対策検討において、阪神・淡路大震災と新潟中越大震災の最も重要な違いは、人間集中の度合いではなく、余

震の大きさと継続にあると筆者は考えている。図表1は新潟商工会議所がまとめた両震災における余震（震度4以上）の発生回数をグラフにしたものである。阪神・淡路大震災では、本震こそ最大震度7であったが、その後の余震の最大は震度



4であり、9日目までの7回で終息している。これに対し新潟県中越大震災では、本震は同じ震度7であるが、その後震度6以上が4回、17日目に震度5が発生するなど五月雨式に大きな揺れが続き、ゆっくり終息していくという特徴を呈した。

この震災の特徴は企業の事業継続に大きな影響を与えた。阪神・淡路大震災の際も企業のリスク分散という対策の必要性が叫ばれたが、本震が大きく余震がほとんどない震災では被災現場での早期復旧を目指した方が費用対効果の高い対策ができたのである。しかし、五月雨式に大きな地震が続く場合にはそういう訳にはいかない。もちろん早期復旧は必要であるが、復旧に向けた施設や設備の総点検を終えるそばから大きな地震が発生していたのでは、総点検を何回も繰り返さなければならないので、復旧作業に着手する時期はどんどん遅れる。実際、新潟県所在企業ではそうしたことが発生している。早期復旧ができない場合には、被災地外で事業を早期に再開する対策が必要となる。こうした企業の早期再開・早期復旧・全面復旧など事業継続に関する総合戦略を柱としたものが事業継続経営(BCM: Business Continuity Management)と呼ばれる手法である。事業継続経営は、「事業」を1分たりとも休まず何が何でも「継続」する対策ではなく、継続から復旧までを含む広い概念である。

1.2.2 ロンドン連続爆破テロ

2005 年 7 月 7 日（水）8:50 頃（現地時間）でロンドン市内の地下鉄 3 カ所で爆弾によるテロが同時発生し、9 時 47 分には 4 番目の爆発がバス内で起こった。ロンドンの中心街シティー近辺を狙ったテロで 50 名以上の多数の死者が出たにもかかわらず、市民はパニックに陥らず冷静に対処したとされているが、21 日にも同様の爆破事件が発生した。以下に BCM の観点を中心に企業の対応を振り返る。

<事故後の対応>

（1）従業員の安否確認

各企業とも従業員の安否確認を行ったが、通勤時間帯で移動中であったこと、携帯電話、インターネットの通信機能の低下により、確認に手間取った。

（2）公共交通機関停止への対応

公共交通機関が麻痺し長期化すると判明した時点で、従業員の帰宅のための交通手段として、貸し切りバス・タクシーによる代替輸送機関を手配した。また、従業員の宿泊用にロンドン中心部のホテルを押さえる企業が増加し、ホテルの予約が次第に困難となった。

（3）企業の営業状況

7 日（木）1 日目 事件発生後、当初テロの規模がどこまで広がるか不明であったため、事実上営業は停止。ロイズ銀行は警戒のため中心部 25 支店を閉店、HSBC は当局要請により複数の支店を閉店。日系繊維小売りチェーン店も当日休業。

8 日（金）2 日目 マークス&スเปนサーは中央店を除いて開店。現地企業の多くが自宅待機、またはそれに準じた扱いであったが、日系の商社、自動車メーカー、銀行の一部では通常営業としたところもある。

9 日（土）10 日（日）3, 4 日目 小売業は通常通りの営業が多かったが、週末のロンドン中心街への人手は通常より 24%減。

11 日（月）5 日目 大半が通常の営業に戻る。日系企業社員に被害が出なかったのは、イギリスの企業より始業時間が 30 分早く、8 時半としていたため、最初の爆発があった時点では、既に出社済みであったためといわれている。

<金融機関の BCM>

金融街シティーでは、これまで 90 年代のアイルランド共和軍 IRA のテロによって緊急時の対策が整えられ、特に 2001 年の米国 WTC（ワールドトレードセンター）テロでニューヨーク証券取引所が緊急閉鎖されたことを契機に、FSA（金融サービス機構）、財務省、イングランド銀行の 3 者と金融業界の官民共同で事業継続計画（BCP）が作成された。そして、昨年度には当局がテロ攻撃の様な脅威に対してシステムの耐性があるかどうか、市場も巻き込んだテストを実施していた。今回のテロがこの計画やリハーサルが実際に機能するかどうかの最初のケースとなったが、地道に態勢整備に努めてきたことが功を奏して冷静に対応ができたとされている。

今回のテロで BCP を発動させた例としては、スイス系銀行 UBS が爆発地点の駅から近いオフ

イスからトレーディング部門を別のサイトへ退避させたケースが挙げられる。また、債権等の精算業務を行う London Clearing House は午前中に移転して業務を継続しており、その他いくつかの証券会社がロンドン郊外サテライトオフィスへ移転した。

当局では金融業界の事業継続専用のホームページを開設し、事業継続管理の重要性、対策の役割、関連情報をまとめている（www.fsc.gov.uk）。

<事件からの教訓>

（１）想定されるべき事件・事故

今回のテロを機に、これまでに準備された事業継続計画は「IT リスクには効果的であるかもしれないがその他のリスクについては対応が弱かった」という見方も出ている。多くの事業継続計画作成者は IT がダウンすることは想定していたが、「システムが動いていても、従業員がオフィスに到着しない」という状況を想定していなかったのが実状であった。

従業員の中でキーマンを事前に特定し、彼らがオフィスに出向けない時に遠隔地で重要システムにアクセスできる計画を策定することや、自宅から勤務先のシステムへアクセスする方法の検討が今後必要となる。

（２）スタンバイ状況

事故発生後、緊急時の IT 関連バックアップサービス会社は対応に追われた。

その例として SunGard 社では、11 日までに 28 件の発動要請とスタンバイ 84 件の連絡を受けたが、多くは警察による立ち入り制限によりオフィスに入室できないケースであり、そのうち 1 件はシステムを別の復旧サイトへ移して対応したという。

今回、テロの脅威がいつまで続くのか判然としない中で、共同で対応する協定を結んでいる企業間や複数の企業へのサービス提供を行う契約をしているサービスプロバイダーは危機対応サービス提供のスタンバイ状態を長期間強いられるという状況が続いた。サービス提供のためのキャパが限られている中で、客先よりスタンバイ状態の継続を要求される状態が続き、今後の運営方法を再検討するという声もある。

（３）コミュニケーションの問題

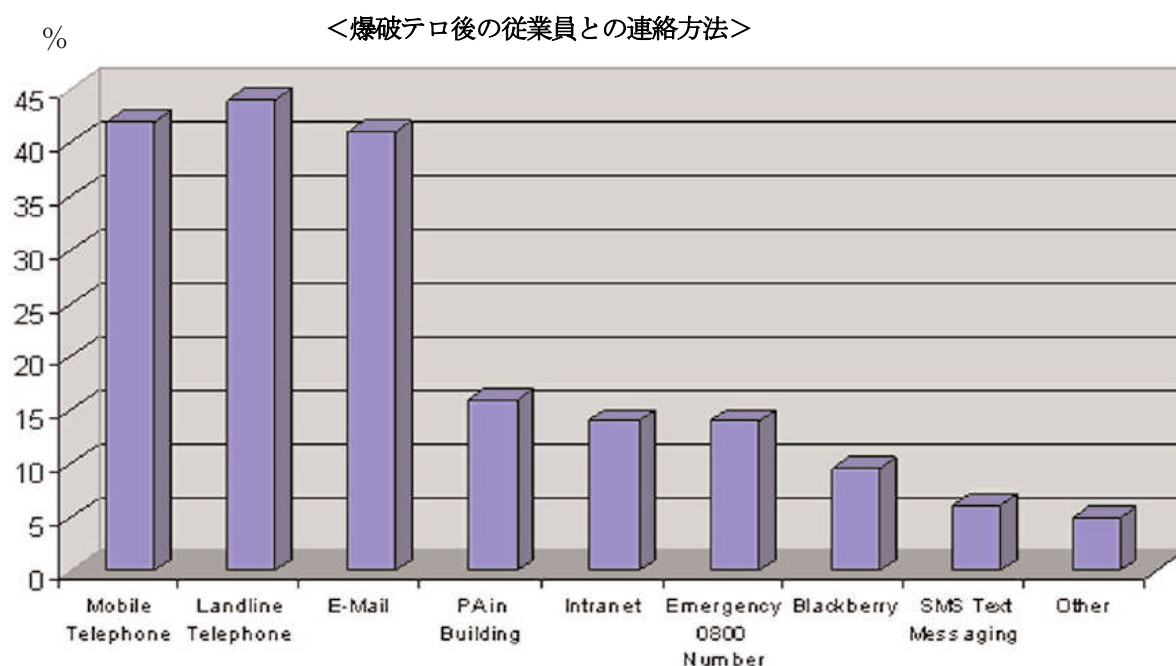
携帯電話が非常時専用として運用されたために通話制限が実施され、通常の電話回線もその影響で混み合った。また、インターネット回線も接続に時間がかかる状態を招いた。

BCP を作成している多くの会社では、電話に代替する設備を供えていないため、初期の段階では電話による連絡を想定していない。この電話回線に代わる通信設備の準備については、ニューヨークでのテロ以降にも必要性が叫ばれたものであるが、今のところ代替策として根本的な解決策がない。

BCI と Link Associates が実施した今回のテロについての「情報コミュニケーションに関する調査レポート」が 8 月 10 日に発表されている（<http://www.thebci.org/7-7Report.pdf>）が、そこでは次の点が指摘されている。

- ・情報提供手段としてはテレビとウェブサイトが最も用いられ、企業内、危機情報提供サービス、地方公共団体による情報よりも役に立った。
- ・従業員の安否把握が予想されたよりも困難であり、設備対策を含め改善が必要。

- ・多くの企業では問い合わせが急増した場合の対応策を準備しておらず、危機対応のリハーサルが現実味のない内容で実施されていたことがわかった。
- ・事業継続計画がどの時点で発動すべきか不明確であったにもかかわらず、リハーサルを実施した企業では対応がスムーズで危機管理チームが機能した。



*PA in Building：ビル内の拡声装置/Emergency 0800：緊急時無料電話

Blackberry：欧米のビジネスマンに普及しているモデムを内蔵した携帯端末で、簡易キーボードを備え、メールの読み書きが可能。

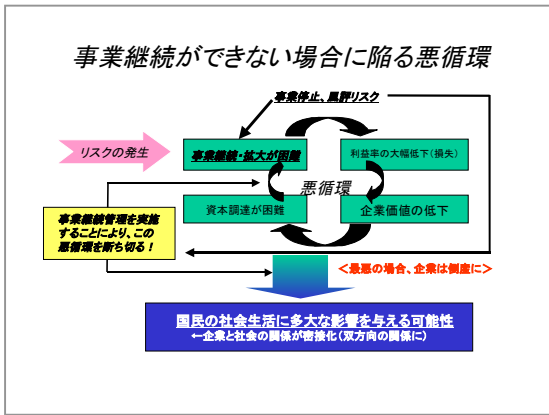
（出典:Information & Communications Survey Report 7th July 2005,BCI&LINK Associates）

＜シティーの企業のBCMは万全か？＞

ロンドン中心部の金融街シティーを管轄する警察本部長ジェームズ・ハート氏が、シティーを標的にしたテロ攻撃は「仮定の話ではなく、いつ起きるかの問題」であると新聞記者に語っている。同氏によると、今回のテロは経済界に緊急事態の対策を準備することを促しはしたが、50%程度の会社しかBCPを準備していないとして、企業の役員を批判している（8月10日付フィナンシャルタイムズ）。これに対して、財界指導者の一部は、対策を準備していないのは中小企業であると反論したという報道があった。

1.2.3 事業継続不能に陥る悪循環

ここで、事業継続ができない状況に陥る悪循環ということを定性的に考えてみる。例えば、企業に火災、地震、自然災害といったリスクが発生し、それが巨大災害であった場合、まず事業の継続、拡大が困難になる。その結果、利益率が低下すると企業価値の低下が起こり、場合によっては金融機関からの資本調達が困難になり、結果として事業継続が困難になっていくという悪循環に陥ってしまう。そして最悪の場合は倒産となる。この悪循環



で追い討ちをかけるのは風評リスク、ブランドの低下であり、この結果企業は倒産、もしくは倒産までいってなくてもかなりの痛手を被る企業が過去にも何社かあった。BCMは、事前に対策を計画化しておき、この悪循環を断ち切るというマネジメント手法である。

1.2.4 BCM はなぜ必要か

BCM を導入する理由は企業によって様々であるが、大きく分けると以下の通りである。

- 企業存続
- 供給責任
- 売上、収益、市場シェアの確保
- 取引先へのアピール など

上記を災害発生時、及び平常時の観点で分類をすると以下の通り整理される。

災害発生時	平常時
1. 災害直後の混乱を少なくする。 ・ 復旧手順や優先順位、判断基準を事前に明確化できる。 ・ 社外への情報開示を適切に行なうことで、取引先などステークホルダーの混乱を減らすことができる。 ・ 供給責任を果たすことができる。	1. BCMを実施していることを社外にアピールすることができる。
2. 目標とする復旧時間内での復旧を目指す。 →取引先からの信頼回復 ・ 災害直後に適切な対処 →被害を最小限に抑える。 ・ 復旧に必要なものが用意されている。	2. BCMへの取組を評価する動き ・ BCMが取引先の選定基準になってきている。 ・ ISO化 ・ BCMの取組状況に応じた融資制度を活

→待ち時間の短縮 ・復旧活動にムダがなくなる。 ・競合他社より先に復旧する。 →利益増	用できる。
3. 社会貢献 ・社会貢献への援助を実施する余裕ができる。	3. BCMが業務改善 ・ビジネスインパクト分析の中で、平常業務の中に潜む問題点、リスク、ムダが見つかる。

1.2.5 欧米では、リスク管理上企業の事業継続に対する関心が最も大きい

現在の欧米における状況として、ロンドンに拠点を置く企業のリスクマネージャーの会員組織である AIRMIC(the Association of Insurance and Risk Managers)は、2003 年 12 月に PAS56 の普及促進をサポートすることを発表した。一方で、2003 年 6 月の AIRMIC の調査では、企業の最も重要なリスクの一つとして「事業継続」が挙げられており、企業の大きな関心が伺える。現在、欧州では、BCI、AIRMIC、BSI など BCM、リスクマネジメント、規格関係団体などが連携を取りながら、BCM の重要性を訴えている。

2. 第2章 BCMの構築と導入動向

2.1 BCMの構築について

本章では、BCMの考え方及びその構築について概説する。

2.1.1 BCMの定義

BCP・BCMには様々な定義が唱えられているが、経済産業省、日本規格協会、英国規格協会、およびBCIの定義は以下の通りである。（由来はPAS56から）

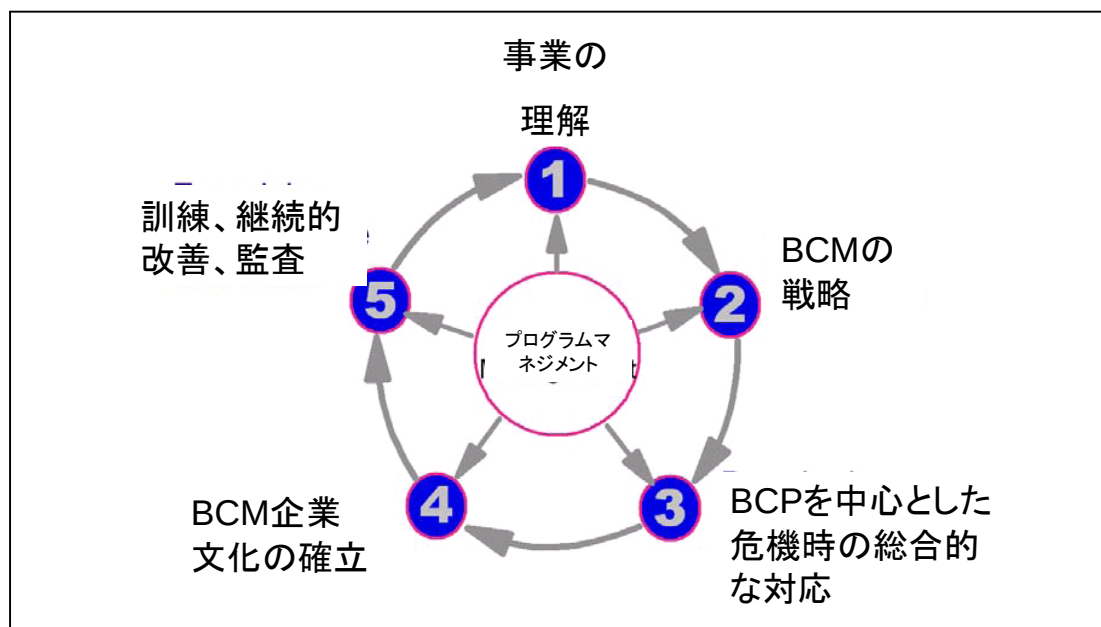
BCP	潜在的損失によるインパクトの認識を行い実行可能な継続戦略の策定と実施、事故発生時の事業継続を確実にする継続計画。事故発生時に備えて開発、編成、維持されている手順及び情報を文書化した事業継続の成果物。
BCM	組織を脅かす潜在的なインパクトを認識し、利害関係者の利益、名声、ブランド及び価値創造活動を守るため、復旧力及び対応力を構築するための有効な対応を行うフレームワーク、包括的なマネジメントプロセス。

つまり、BCMは、事故や災害などが発生した際に、「如何に事業を継続させるか」若しくは「如何に事業を目標として設定した時間内に再開させるか」についてあらゆる観点から対策を講じることである。このためには、マネジメントシステムの構築やビジネスインパクト分析が非常に重要となる。

BCPとBCMの違いを整理したい。BCPはBusiness Continuity Planの略であり、事業継続計画やビジネス継続計画と訳され、「計画」自体を指す。一方、BCMはBusiness Continuity Managementで事業継続経営や事業継続管理などと訳される。従い、BCMは、BCPを活用して、如何にBCMを企業内に浸透させていくか、戦略的に活用していくかというマネジメント自体である。

2.1.2 BCM 構築・確立のためのプログラムマネジメント

BCI では、BCM 構築のためのプログラムとして以下サイクルを提唱している。BCI ガイドラインの詳細は、<http://www.thebci.org/gpg.htm> を参照されたい。



BCM を上記5ステージのプログラムマネジメントで構築していくと、フレキシビリティを保たせながら、BCM の構築ができると考えられる。各フェーズで検討すべき事項は、以下の通りである。

	項 目	内 容
序 論	BCM	■ 会社全体の BCM 戦略と方針 ■ プログラムマネジメント ■ 事態への準備と対応
ステージ 1	事業の理解 (ビジネスインパクト分析を中心に)	■ 戦略 ■ ビジネスインパクト分析 ■ リスク分析とコントロール（予防）
ステージ 2	BCM の戦略	■ 会社レベルの BCM 戦略 ■ プロセスレベルの BCM 戦略 ■ バックアップ戦略
ステージ 3	BCP を中心とした危機時の総合的な対応について	■ 危機管理計画 ■ 事業継続計画（BCP） ■ 事業体（単位）の BCP
ステージ 4	BCM 企業文化の発展・確立	■ BCM に対する意識水準の評価 ■ BCM 文化の発展・浸透 ■ 文化の発展・浸透度合いのモニタリング ■ 訓練

ステージ5	訓練・継続的改善・監査	■ 継続的改善 ■ 監査
-------	-------------	---

BCP を作る際に根底になる考え方は、企業の存続に関わる緊急度が最も高い業務を最優先に再開させるというのが大前提である。この緊急度が高い業務というのは、それを失うと企業の財務状態に直ちに影響を与える業務であり、財務への影響以外にブランドイメージであるとか、シェアの喪失、顧客との関係悪化などの影響を加味して考慮検討していくというものである。

2.1.3 経営トップのコミットメント・推進

BCM を進めるにあたっての前提となることである。BCM の成否は、経営トップの推進が必要であり、これを行うことにより、会社全体の士気が上がり従業員の協力を得やすくなる。また組織全体を通じて「役割」、「責任」の明確化を行わなければならない。

2.1.4 ビジネスインパクト分析（BIA ; Business Impact Analysis）

BIA は BCP 策定の基礎分析であり、性格上「業務プロセス分析」といえる。項目としては、「ビジネスプロセスの分析（脆弱性の分析）、ボトルネック分析」があり、続いて「特定されたボトルネックに対するリスク分析」になる。このボトルネックとは、重要な業務、工程、部門、キーパーソン、システム、データ、物流など、企業に応じて様々である。その結果に応じて、ボトルネックが万一なくなった場合、どのようにボトルネックを機能させていくかという「優先復旧順位の決定」を行う。これら分析のベースには、以下を常に念頭に置く。

- 組織の目的は何か？ 提供する製品・サービスは？
- どのようにその目標は達成できるか？
- 社内外関係者の事業継続上の位置付けは？
- 製品またはサービスの提供に絶対的な必要な時間的条件は何か？

また既存サイトのリスク状況の改善、代替サイトにある設備、資源などの確保に関わる検討も併せ進め、並行的に目標復旧時間（RTO : Recovery Time Objectives）の設定を行う。

なお、BIA は、組織の基幹事業継続の基礎分析であるため、以下のような事業上の重要な変更があった際は、その都度実施することが望まれる。

- 新しい製品・プロセス・技術の導入
- 事業所の移転、または事業の地理的範囲の変更
- 業務、組織、要員に関する重大な変更
- 納入またはアウトソーシングに関する新規契約・変更

ビジネスインパクト分析の進め方の例として、本社機能を対象に行う際の留意点を述べる。

本社には、通常「マネジメント機能」、「管理機能」、「購買・物流機能」、「営業機能」などがある。本社のBIAを行う際には、以下をベースに会社としてのマネジメント、ITシステム、キーパーソン、購買・物流などの観点についてボトルネックを特定していく。

- 災害時などに如何に本社機能を維持・確保するか。
→バックアップ（代替）機能の確保を検討する。
- 本社が機能しなくなった際に、工場・研究所・営業所など他拠点への影響はどうか。

<ビジネスインパクト分析のポイント>

- 各部門の基幹業務
- ボトルネック
- 悪影響を受ける範囲は
- 事業復旧の優先順位付け
- 目標復旧時間
- BCP対策本部との連携
- 取引先など外部基幹との連携—含む、サプライチェーンマネジメント
- 代替復旧場所

2.1.5 BCP の展開

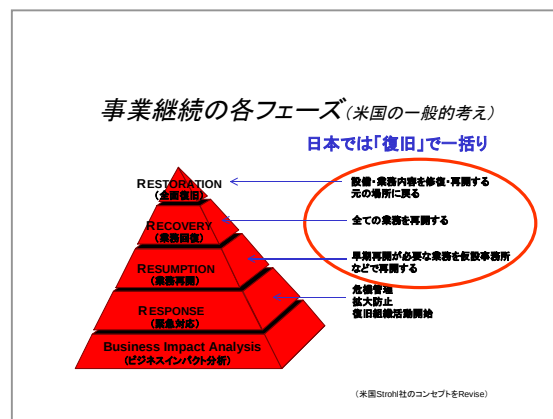
一番の底辺に、ビジネスインパクト分析があり、これが前述したビジネスインパクト分析になる。この結果に基づいて、上にいく「緊急対応」「業務再開」「業務回復」「全面復旧」などの各々の体制を構築していく。本フェーズの構成は、経済産業省の事業継続策定ガイドラインでも同じである。

まず、「緊急対応」は事故、災害が発生した直後の初期対応から構成される。内容は危機管理、損害の拡大防止、復旧組織の活動開始である。そして次の「業務再開」は早期再開が必要な重要業務を仮設事業所などで再開をする。次の「業務回復」は全ての業務を再開する。そして「全面復旧」は設備、業務内容を修復再開し、仮設事務所などから元の場所に戻ってくるというフェーズである。

実はこれは米国の考え方であり、日本の場合は「業務再開」「業務回復」「全面復旧」が「復旧」という言葉で一括りにされているのではないかと考える。

次に、BCP 策定にあたっての考え方をフェーズ毎に見てみたい。

【緊急対応】



このフェーズは危機が発生した直後の対応である。企業としては、従業員そして家族、その生命、安全への配慮が最も重要である。米国の BCP を見ると安否確認を含めた対応策が省かれていて、従業員の安全は確保されているという前提で BCP が作られているケースが結構ある。しかしながら、BCM 上、従業員の生命の配慮は非常に重要である。そして、自然災害の緊急時の対応については日本では避けようがない現象であり、あらかじめ計画化する必要性は大きい。

【業務再開】

企業の存続に関わる最も緊急度が高い業務を最優先に再開させるフェーズである。最も緊急度が高い業務とは、これを失うと企業の財務状態に直ちに影響を与える業務である。ここでは緊急度が高い業務を有する拠点が被災して機能しなくなった場合に、仮設拠点を利用してその業務を復旧する。どういう技術を持った人がいるのか、更にはどういう設備を持ってくるのかといったことを予め管理をしておくことが一つのポイントとなる。

【業務回復】

最も緊急度の高い業務や機能が再開した後に、より緊急性が少ない業務にまで範囲を拡大して業務を再開するフェーズである。この段階ではまだ臨時的な体制によって業務運営を行っている。

【全面復旧】

その後の業務を長期的に継続できる最終的な体制への移行フェーズである。ここでは仮設拠点で行っていた業務を順次復旧拠点に戻していき、人員も全て各々の通常業務に戻っていくフェーズである。なお、企業によってはリストラ、増強、最新鋭設備などによって被災前より優れた拠点構築（事業の再構築）を目指すこともあるだろう。

【予防】

これは事故発生の予防で、平常時における対策フェーズである。ここでは二つの観点がある。まず一つ目はビジネスインパクト分析で、企業や施設の脆弱性分析を基にしたリスクの軽減、リスク状況の改善である。もう一つは事故や災害が発生した場合に備えるフェーズである。例えば、リスクの軽減は建物、設備などの耐震補強、バックアップシステムの導入、代替サイトの構築などが挙げられる。一方で、事故や災害に対し事前に備えるフェーズとしては復旧優先順位の決定、権限委譲の明確化、リスクコミュニケーション、備蓄品などの備えがある。

ここで重要なポイントは、教育シュミレーションの実施である。企業は組織変更や人員の変更が絶えず行われており、定期的に更新しないと何かがあった場合にそれが機能しない。実は本当の緊急事態を除けば、この教育シュミレーションこそが BCP の方針だとか手順、能力の評価を可能とする唯一の方法である。

次に、財務的対応策の検討である。実際に BCP を発動させることになるとう資金が必要になる。この資金をどこから調達するか。代表的な手段は銀行からの借入や損害保険ということになる。例えば損害保険でいうと、企業の喪失利益を補償する利益保険、事業継続のために要した余分な費用を補償する営業継続費用保険などがある。

2.2 日本企業と海外企業の BCM 導入動向結果

インターリスク総研では、2005 年 3 月に「日本国内の上場企業への BCM への取組」についてのアンケート調査を行い、海外企業との比較・分析を行い、そこから得られる知見を整理した。その結果、日本の上場企業の BCM 導入状況は 10%程度であり、2004 年度に BCI（事業継続協会）が海外企業 461 社を対象に実施した調査結果（約 47%）と比較しても大きく遅れている事が判明した。

2.2.1 BCP の展開

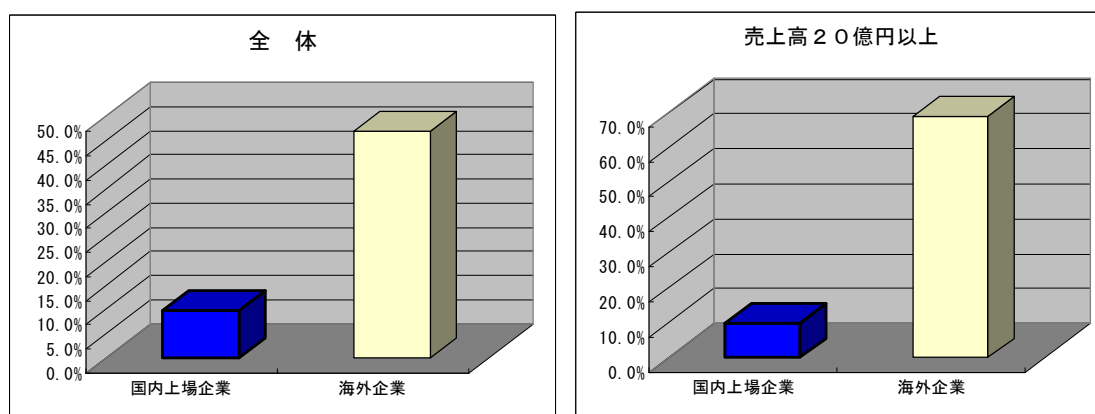
本アンケート調査の大きな特徴は、海外企業と日本企業の比較研究を行なったことである。海外企業の実態は、BCI（世界事業継続協会）が 2004 年に行った海外企業 461 社の調査結果を引用した。海外企業と日本企業の BCM への取組の差異、そして日本企業の取組の特徴を以下に概説する。

調査方法	: 質問紙郵送法
調査対象企業	: 日本国内全上場企業 3,755 社
回答総数	: 547 社
有効回答数	: 533 社
有効回答率	: 14.2%
調査期間	: 2005 年 2 月～3 月

①BCP（Business Continuity Plan:事業継続計画）の策定状況

<全体>

全社ベースで BCP を策定している国内上場企業は 9.8%（売上高 20 億円以上で 9.7%）であり、海外企業（全体で 47%、売上高 20 億円以上で 69%）と比較して BCP の策定割合は低い。



基幹事業など特定部門で策定（8.6%）、情報システム部門で策定（4.3%）している企業を含め

ると合計で 23%に達する。また、検討中・策定していないと回答した企業は、69.8%であった。調査を実施後、経済産業省及び内閣府から BCM のガイドラインが発行されたので、現在多くの企業が BCM の構築に取り組んでいると考えられる。

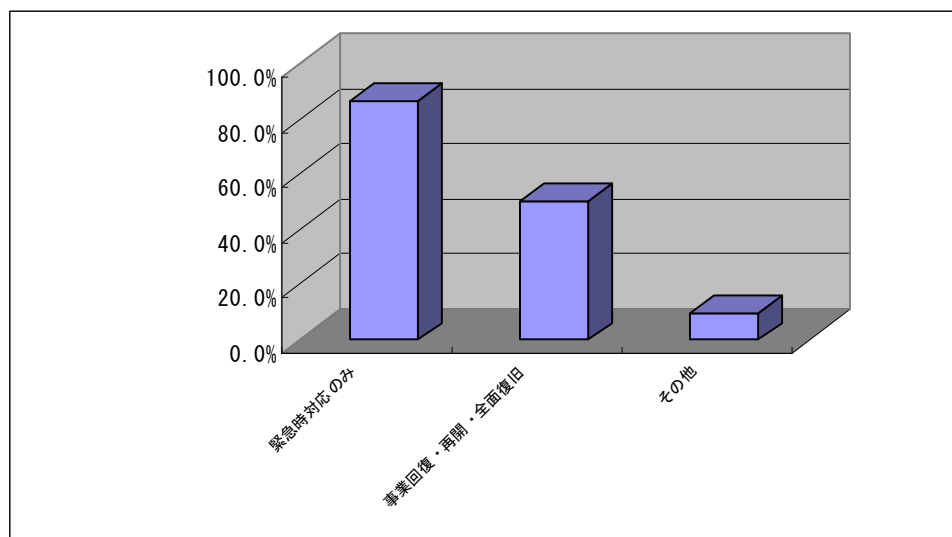
＜国内上場企業の BCP 導入部門の策定状況＞

対象部門	割合
全社ベースで策定	9.8%（＝上記と同じ）
基幹事業部門など特定部門で策定	8.6%
情報システム部門で策定	4.3%
策定中	5.6%
検討中・策定していない	69.8%

なお、製造業は、「基幹事業など特定部門」で BCP を策定している企業が多い（11.5%）が、非製造業は、「全社ベース、若しくは情報システム部門」で策定している割合（各々11.4%、6.1%）が多いのが特徴。

②BCP が対象としているフェーズ

BCP を策定している企業のうち、BCP の対象としているフェーズを「事業回復・再開・全面復旧」と回答した割合は、50.6%に低下する。BCP は緊急時対応のみならず、「事業回復・再開・全面復旧」を対象にするものであり、従って日本企業の再開・復旧時の計画は、前記①の数値の約半分に低下するといえよう。



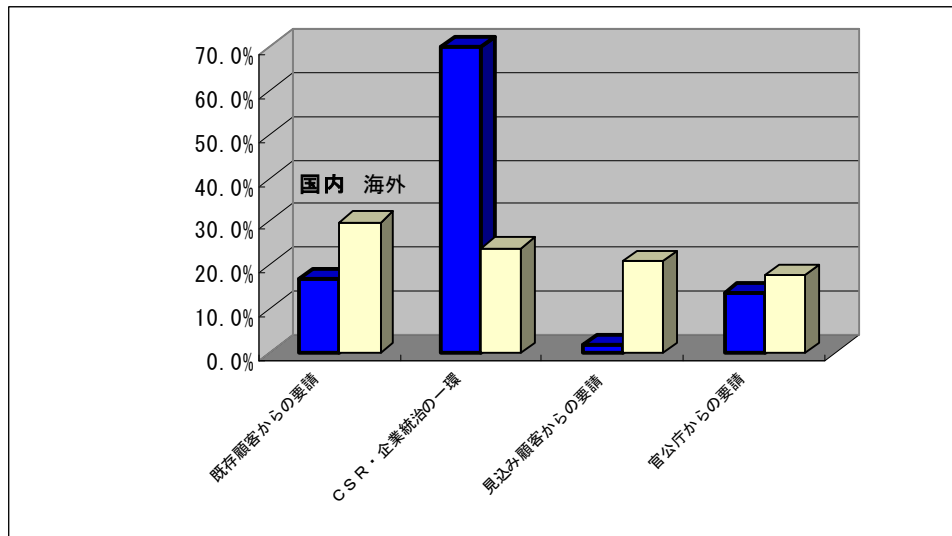
③業種毎の特性

BCP を全社ベースで策定していると回答した数・割合の大きい業種は、銀行(80%)、証券(40%)、鉄鋼・非鉄(33.3%)、倉庫・運輸業(25%)、情報・通信(11.5%)などが挙げられる。金融・ユーティ

リティ企業が代表的なBCP策定企業である。

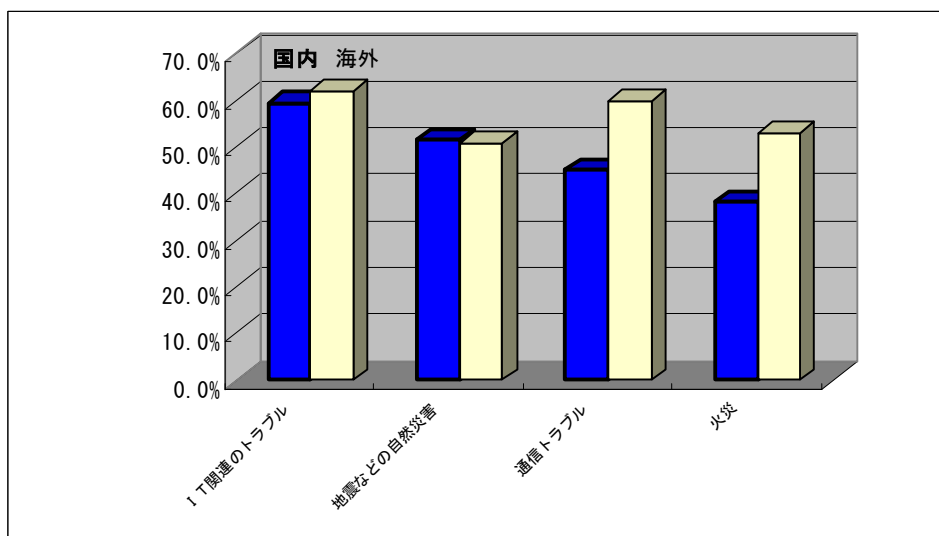
2.2.2 BCP を策定した理由

海外企業では、BCP が「取引先選別基準」／「他社との差別化」など経営戦略に活用されており、日本でも同様な動きが加速している。国内上場企業では、「CSR・企業統治の一環」でBCPを策定している企業が多いのが大きな特徴である。なお、取引先にBCPを策定するよう要請している日本企業は10%にのぼっていることが調査結果で判明した。



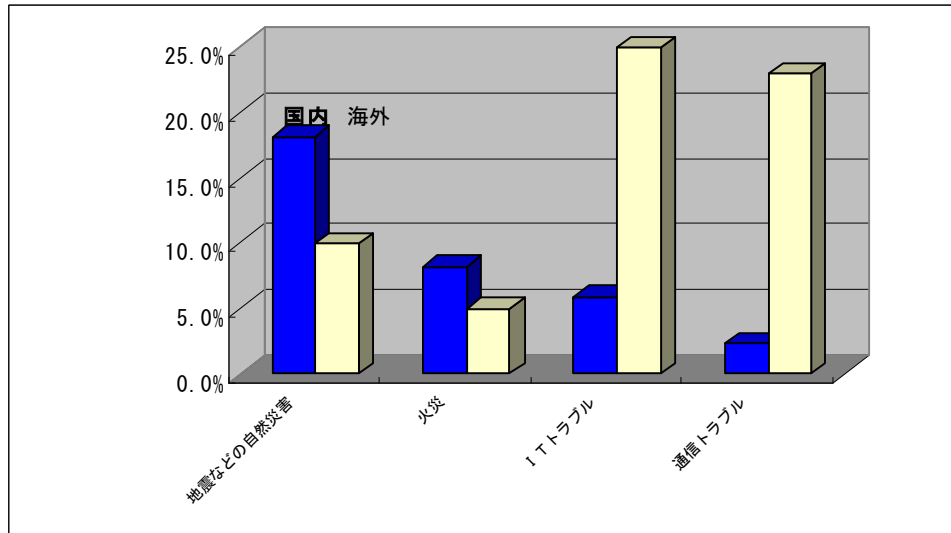
2.2.3 BCM 責任者の関心あるリスクについて

海外・日本企業ともに関心のあるリスクに大きな差は見られない。ともに、IT 関連のトラブルに最も関心があり、事業継続に対する IT 依存度が高まっていることが背景にあると考えられる (IT 依存度が高まっていると回答した企業は84%にのぼる)。



2.2.4 過去に事業継続を妨げた事象について

国内上場企業の約 18%が自然災害で収益減少をきたしたとしている。また火災なども含めると約 26%、約 4 社に 1 社が事業継続に影響があった。日本企業で、IT・通信関係のトラブルが少ないのは、緊急時対応が一定機能しているからと考えられる。



2.2.5 基幹業務が停止した場合に許容できる停止時間

基幹業務とは、「企業存続にとって最も重要な業務」をいう。例えば、その業務がなくなると、直ちに財務上致命的な影響を与えたり、ブランドイメージや顧客／社会との関係悪化を生じさせる業務である。全産業では 50.1%の企業が、許容できる停止時間を「1 日未満」と回答した。非製造業では、「2 時間未満」と回答した企業が、21.7%にのぼる。許容できる停止時間が短い業種は、「情報、通信」、「電力、ガス、水道」、「銀行」、「証券」、「小売業」、「機械・電機製品製造」、「輸送用機器製造」の順である。

3. 第3章 世界の BCM に関するガイド

BCM に関するガイドについて紹介する。

3.1 事業継続ガイドライン 第一版－わが国企業の減災と災害対応の向上のために－

1. ガイドラインの名称	事業継続ガイドライン 第一版 -わが国企業の減災と災害対応の向上のために -
2. 発行時期	2005 年 8 月 1 日
3. 発行者	内閣府 防災担当 中央防災会議 民間と市場の力を活かした防災力向上に関する 専門調査会 企業評価・業務継続ワーキンググループ
4. 対象となる地域	日本
5. 対象リスク	主に自然災害（特に地震）。ただし他のリスクも排除していない。
6. 概要	
(発行の目的)	
日本国企業の減災と災害対応の向上のため	

（章項目）

【ポイント】

1. 事業継続の取組みとは
2. 事業継続の取組みの特徴
3. 本ガイドラインの特徴
4. 取組みを促進する趣旨と論点
5. 本ガイドラインの位置づけ
6. チェックリストの活用

I 事業継続の必要性と基本的考え方

1.1 事業継続の必要性とポイント

- 1.1.1 災害時の事業継続に努力する必要性
- 1.1.2 事業継続の考え方のポイント
- 1.1.3 広域自然災害へ備えるべきわが国の事業継続計画の特徴

1.2 基本的考え方

- 1.2.1 想定する災害リスク
- 1.2.2 事業継続と共ともに求められるもの
- 1.2.3 本ガイドラインにあげた各項目の位置づけ

1.3 継続的改善

II 事業継続計画および取組みの内容

2.1 方針

2.2 計画

- 2.2.1 検討対象とする災害の特定
- 2.2.2 影響度の評価
- 2.2.3 重要業務が受ける被害の想定
- 2.2.4 重要な要素の抽出
- 2.2.5 事業継続計画の策定
- 2.2.6 事業継続と共に求められるもの

2.3 実施および運用

- 2.3.1 事業継続計画に従った対応の実施
- 2.3.2 文書の作成
- 2.3.3 財務手当て
- 2.3.4 計画が本当に機能するかの確認
- 2.3.5 災害時の経営判断の重要性

2.4 教育・訓練の実施

2.5 点検および是正措置

2.6 経営層による見直し

III 経営者および経済社会への提言

23/101

付録 1. 用語の解説

付録 2. 参考文献

付録 3. 国際規格との関連性

III 経営者および経済社会への提言

付録 1. 用語の解説

付録 2. 参考資料

付録 3. 国際規格との関連性

別添 事業継続ガイドライン 第一版 チェックリスト

（概要）

「内閣府 中央防災会議 民間と市場の力を活かした防災力向上に関する専門調査会 企業評価・業務継続ワーキンググループ」によって作成された。

BCM 構築のための「ガイドライン」という範疇にとどまらず、政府・中央防災会議専門調査会から、企業経営者および経済社会への提言を含んでいる。

ガイドラインの基本的考えは、想定するリスクに自然災害リスクである地震リスクを推奨しており、事業継続の取組に加え、生命の安全確保、二次災害の防止、地域貢献・地域との共生について、考慮すべき重要事項としている。

また、ガイドライン本文 26 ページのうちの約一割を、いわゆる防災の観点からの内容、これらの事項（生命の安全確保、二次災害の防止、地域貢献・地域との共生、共助、相互扶助）に割いている。対象とする企業の業種や規模を問わない、自然災害である地震を対象として横断・共通的な内容である。

このガイドラインの項目のうち、英米等の関連規格において重要な要素必須とされている項目が抽出されており、英米等の関連規格との比較がしやすくなっている。

このガイドライン本文の中で、必要であるとされている項目（およびそれに準じた項目）が、チェックリストとして抜き出されており、自社の取り組みがこのガイドラインに準拠しているかどうか、セルフチェックできるようになっている。

7. URL	http://www.bousai.go.jp/MinkanToShijyou/guideline01.pdf
8. 入手方法	ダウンロード可能

3.2 事業継続計画（BCP）策定ガイドライン - 高度 IT 社会において企業が存続するために-

1. ガイドラインの名称	事業継続計画（BCP）策定ガイドライン -高度 IT 社会において企業が存続するために-
2. 発行時期	2005 年 8 月 19 日
3. 発行者	経済産業省商務情報政策局情報セキュリティ政策室
4. 対象となる地域	日本
5. 対象リスク	IT 事故
6. 概要	(概要) 我が国では、e-Japan 戦略に基づく世界最高水準の IT 社会が実現しつつあり、企業は高度な IT 活用によるビジネスの効率化・高付加価値化といった恩恵を享受している。しかし、その一方で、企業一社の IT 事故の影響が社会全体へと波及する事例が出てくるなど、高度に統合された我が国 IT 社会は新次元のリスクに直面している。 こうした状況の中では、企業は IT 社会の一員としての社会的観点も踏まえて、情報セキュリティ対策に取り組む推進力を企業内に構築・運用していくことが重要である。すなわち「情報セキュリティガバナンス」という新たな概念を企業経営に組み込んでいくことが必要となっている。「情報セキュリティに絶対はなく、事故は起こりうるもの」との前提に立ち、突発的な IT 事故が発生した場合であっても事業を中断せず維持するために、各企業において事業継続計画（BCP : Business Continuity Plan）を策定することが重要になってきている。 本書は、経済産業省商務情報政策局長の私的研究会である「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」が平成 16 年 9 月から平成 17 年 3 月にかけて開催される中、同研究会の下に設置された「事業継続計画策定ガイドラインワーキンググループ」が検討した成果を、「事業継続計画（BCP）策定ガイドライン」として取りまとめたものである。本ガイドラインは事業継続計画の基本的な考え方から具体的な計画の構築手順までを解説したものであり、政府が策定したものとしては我が国で初めてのものである。 今回のガイドライン策定にあたっては、IT 事故を想定した事業継続計画の策定手順や検討項目をわかりやすく解説することを念頭におきつつ、IT 事故に限ることなく、広く他の要因も視野に入れた事業継続計画を策定する際にも活用できるよう構成している。幅広いニーズに対応できるガイドラインとなっている。

（目次）

第Ⅰ章 基本的考え方

- 1. 1 BCP（Business Continuity Plan）の必要性
- 1. 2 BCP が求められる背景
- 1. 3 BCP の特性
- 1. 4 世界と日本の動向

第Ⅱ章 総論（フレームワーク）

- 2. 1 BCP 策定に当たっての考慮事項
- 2. 2 組織体制について
- 2. 3 ビジネスインパクト分析から BCP 策定までの流れ
- 2. 4 BCP の導入と教育・訓練
- 2. 5 BCP の維持・管理

第Ⅲ章 BCP 策定に当たっての検討項目

- 3. 1 検討項目の全体像とポイント
- 3. 2 BCP の実施体制
- 3. 3 BCP 発動フェーズにおける対応のポイント
- 3. 4 業務再開フェーズにおける対応のポイント
- 3. 5 業務回復フェーズにおける対応のポイント
- 3. 6 全面復旧フェーズにおける対応のポイント
- 3. 7 リスクコミュニケーションの重要性

第Ⅳ章 個別計画（ケーススタディ）

- 4. 1 大規模なシステム障害への対応
- 4. 2 セキュリティインシデントへの対応
- 4. 3 情報漏えい、データ改ざんへの対応

8. 問合せ先	経済産業省 http://www.meti.go.jp
9. 入手方法	有料 http://books.chosakai.or.jp/books/catalog/27297.html

3.3 中小企業 BCP 策定運用方針

1. ガイドラインの名称	中小企業 BCP 策定運用方針
2. 発行時期	2006 年 2 月
3. 発行者	経済産業省中小企業庁
4. 対象となる地域	問わない（基本的には日本）
5. 対象リスク	リスクを問わない
6. 概要	
（発行の目的） 日本の中小企業が、自ら BCP を策定し運用することができるように策定された。中小企業庁では、BCP を、企業を存続させるための対策であるとして、「事業継続計画」ではなく、「緊急時企業存続計画」と呼ぶ。	
（章項目） 以下 3 コースに分類される。 （1） 基本コース BCP の策定・運用を始めようとする多くの経営者向けのコース。経営者の頭にある考えを BCP サイクルに沿って整理し、BCP 様式類を記入する。 （2） 中級コース BCP の策定・運用について、理論を学びつつ確立したい経営者向けのコース。BCP のサイクルに沿い、体系的に BCP の策定・運用、予習を行なう。 （3） 上級コース 中級コースで BCP を策定・運用済みの経営者が、さらにより広く深く取組むためのコース。指針で紹介する各種資料を参考にし、独自の BCP 構築を目指す。	

（概要）基本コースは以下の通り。

（１） 入門診断

ヒト、モノ、カネ、情報、事業継続に関する 20 の質問に答え、自社の事業継続能力について自己診断する。診断結果に基づき自社の取組み方針を決めることができる。

（２） 基本方針と運用体制の決定

BCP の策定・運用に取り組むにあたり、自社の基本方針を立案し、BCP を策定し、運用を推進していく社内体制を決める。

＜基本方針で定める事項＞

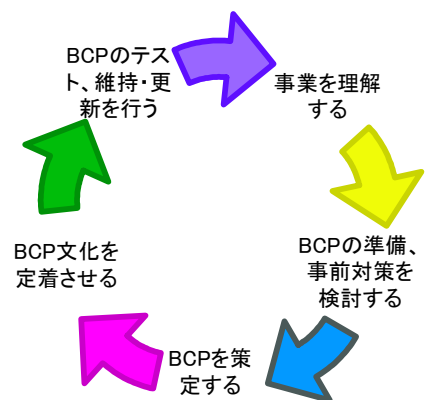
- ・ BCP 策定・運用の目的
- ・ 緊急時に事業継続を図る上での要点
- ・ BCP 及び災害計画の更新時期

＜BCP 策定・運用体制で定める事項＞

- ・ BCP の策定体制
- ・ 緊急時における BCP の発動体制
- ・ 平常時における BCP の運用推進体制

（３） 平常時における BCP の策定

BCP の策定、及び運用のサイクルは、英国 BCI の BCM ガイドラインを参考にして作成されている。



＜ B C P 策定運用サイクル＞

（ベストプラクティス）

具体的な記載はないが、中小企業 BCP 策定運用指針に沿って BCP を策定した企業は、中小企業庁のホームページに公開される。

7. URL	http://www.chusho.meti.go.jp/bcp/index.html
8. 入手方法	ダウンロード可能

3.4 PAS (Publicly Available Specification) 56 Guide to Business Continuity Management

1. ガイドラインの名称	PAS (Publicly Available Specification) 56 Guide to Business Continuity Management
2. 発行時期	2003 年 3 月 24 日
3. 発行者	British Standards Institution（英国規格協会） 日本規格協会とは、日本語版「事業継続管理のための指針」を 2004 年に発行した。
4. 対象となる地域	全世界
5. 対象リスク	リスクを問わない
6. 概要	
(発行の目的) 「It is designed to provide assistance to the BCM manager in understanding and implementing a BCM programme. (BCM プログラムを理解、推進している BCM マネージャーを支援するため)」	
(章項目) 1. Scope（適用範囲） 2. Terms and definitions（用語と定義） 3. Abbreviations（略語） 4. Overview（概要） 5. BCM programme management（BCM プログラム） 6. Understanding your business（事業に対する理解） 7. BCM strategies（BCM 戦略） 8. Developing and implementing BCM plans（BCP の構築） 9. Building and embedding a BCM culture（BCM 文化の構築、及び浸透） 10. BCM exercising, maintenance and audit（BCM のトレーニング、維持、及び監査） Annex A (informative) Participants in the BCM cycle（付属書 A（参考資料）－BCM サイクルの参加者） Annex B (informative) BCM evaluation criteria（同 B－BCM 評価基準） Annex C (informative) Frequency and triggers（同 C－頻度、及び要因） Bibliography	

(概要) BCI のガイドライン(BCI Good Practice Guidelines)をベースとしている。 内容は、BCM を確立する際の包括的なアプローチを記載している。 BCM をリスクマネジメント、災害復旧、ファシリティマネジメント、サプライチェーンマネジメント、品質管理、健康及び安全、ナレッジマネジメント、緊急時対応、セキュリティ、リスクコミュニケーション及び広報との関連付けを行なっている。 ドイツやフランスなどでも翻訳され活用されている。 現在改定中であり、2006 年 7 月に新しい PAS56 が発行・リリースされる予定。	
7. URL	英国規格協会 http://www.bsi-global.com/ 日本規格協会 http://www.jsa.or.jp/
8. 入手方法	有料

3.5 NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs

1. ガイドラインの名称	NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs
2. 発行時期	2004 年 1 月 16 日
3. 発行者	National Fire Protection Association (NFPA)
4. 対象となる地域	記載無し
5. 対象リスク	災害
6. 概要	(発行の目的) 「This standard shall provide those with the responsibility for disaster and emergency management and business continuity programs the criteria to assess current programs or to develop, implement, and maintain a program to mitigate, prepare for, respond to, and recover from disasters and emergencies. (災害及び緊急時の管理および事業の継続プログラムに関わる業務を担当する者に、現行プログラムに対する評価基準や、災害および緊急状態の軽減、準備、対応、復旧のためのプログラムの作成、実施、管理の基準を提供する)」

（章項目）

Chapter 1 Administration（管理）

1.1 Scope（範囲）

1.2 Purpose（目的）

1.3 Application（適用）

Chapter 2 Referenced Publications (Reserved)（参考刊行物（保留））

Chapter 3 Definitions（定義）

3.1 General（概要）

3.2 NFPA Official Definitions（NFPA の公式定義）

3.3 General Definitions（一般定義）

Chapter 4 Program Management（プログラム管理）

4.1 Program Administration（プログラム管理）

4.2 Program Coordinator（プログラムコーディネーター）

4.3 Advisory Committee（諮問委員会）

4.4 Program Evaluation（プログラム評価）

Chapter 5 Program Elements（プログラム項目）

5.1 General（概要）

5.2 Laws and Authorities（法律および当局）

5.3 Hazard Identification, Risk Assessment, and Impact Analysis
（危険の特定、リスクアセスメント、影響分析）

5.4 Hazard Mitigation（危険の緩和）

5.5 Resource Management（資源管理）

5.6 Mutual Aid（相互支援）

5.7 Planning（計画）

5.8 Direction, Control, and Coordination（指揮、監督、調整）

5.9 Communications and Warning（通信および警告）

5.10 Operations and Procedures（業務および手順）

5.11 Logistics and Facilities（物流管理および施設）

5.12 Training（トレーニング）

5.13 Exercises, Evaluations, and Corrective Actions（実施、評価、および修正活動）

5.14 Crisis Communication and Public Information（危機管理および広報）

5.15 Finance and Administration（財源および管理）

Annex A Explanatory Material（説明資料）

Annex B Disaster/Emergency Management and Related Organizations

（災害／緊急時の管理および関連組織）

Annex C Additional Resources（追加資料）

Annex D Disaster/Emergency Management Accreditation and Certification Programs

（災害／緊急時管理の認定と認証プログラム）

32/101

（災害／緊急時管理の認定と認証プログラム）

Annex E Informational References（参照情報）

Index（索引）

Annex E Informational Reference（参照情報）

Index（索引）

（概要）

40 ページ中、規格としての内容は 7 ページしかなく、残りの大部分は参考情報となっている。

3. 6 Business Continuity Management Good Practice Guidelines

1. ガイドラインの名称	Business Continuity Management Good Practice Guidelines
2. 発行時期	2005 年 2 月 6 日
3. 発行者	The Business Continuity Institute (BCI)
4. 対象となる地域	「あらゆる規模、部門、所在地の組織に適用できる」
5. 対象リスク	特定されていない
6. 概要	(発行の目的) 「for the benefit of BCM professionals around the world (世界中の BCM 専門家に貢献する)」 「This document is intended to provide an overview and guidance on good practice covering the whole Business Continuity Management (BCM) Lifecycle from the initial recognition of the need for the development of the programme to the on-going maintenance of a mature Business Continuity capability. (この文書は、事業継続管理（BCM）ライフサイクルを網羅する適正実施の概要と指針を提供するものである。すなわち、BCM プログラム開発の必要性を最初に認識するところから、成熟した事業継続機能の現在進行形の保守に至るまでを取り扱う。)」

（章項目）

OVERVIEW（概観）

Business Continuity Management（事業継続管理）

BCM Policy（BCM 方針）

Managing the Programme（プログラムの管理）

Stage 1: Understanding Your Business（事業の理解）

1.1 Organisation Strategy（組織戦略）

1.1 Business Impact Analysis (BIA)（事業影響度分析）

1.2 Risk Assessment (RA)（リスク評価）

Stage 2: BCM Strategies（BCM 戦略）

2.1 Organisation (Corporate) Strategy（組織（コーポレート）戦略）

2.2 Process Level Strategy（プロセスレベル戦略）

2.3 Resource Recovery Strategy（資源回収戦略）

Stage 3: Developing a BCM Response（BCM 対応の策定）

3.1 Crisis Management Plan（危機管理計画）

3.2 Business Continuity Plans（事業継続計画）

3.3 Business Unit Resumption Plans（事業単位再開計画）

Stage 4: Developing a BCM Culture（BCM 文化の醸成）

4.1 Assessing the level Of BCM Awareness（BCM 意識水準の評価）

4.2 Developing a BCM Culture（BCM 文化の醸成）

4.3 Monitoring Cultural Change（文化的変化の監視）

Stage 5: Exercising, Maintenance and Audit（訓練、保守、監査）

5.1 Exercising（訓練）

5.2 Maintenance（保守）

5.3 Audit（監査）

Appendix – Standard Texts and Further Reading (being updated)

（標準テキストおよび参考文献（改訂中））

3.7 TR19 事業継続管理（BCM）のためのテクニカル・レファレンス

1. ガイドラインの名称	TR19 事業継続管理（BCM）のためのテクニカル・レファレンス
2. 発行時期	2005 年
3. 発行者	SPRING(Standards, Productivity and Innovation Board-規格、生産および変革理事会)Singapore
4. 対象となる地域	シンガポール
5. 対象リスク	特定されていない
6. 概要	
(発行の目的)	
(章項目)	
TR19 は以下 9 項目に附属書と引用文献が付いた構成である。 BCM の構築からレビューまで一連のマネジメントシステムが網羅されている。 各 Sub 項目についてもタイトルを記しておく。 第0項 BCM 枠組みの紹介 0.1 BCM の領域 0.2 BCM の構成要素 第1項 適用範囲 1.1 前提 1.2 他の規格や規則との関係 1.4 条文の解釈 1.4.1 理論的根拠と意図 1.4.2 言語形式 1.4.3 自由裁量の条文 1.4.4 例の利用 1.4.5 リスト上の項目	

第2項 定義

- 2.1 適用範囲
- 2.2 代替場所
- 2.3 認識
- 2.4 BCM 運営委員会
- 2.5 事業継続管理(BCM)
- 2.6 事業継続計画
- 2.7 事業継続の計画立案(BCP)
- 2.8 ビジネス機能
- 2.9 ビジネス・インパクト分析(BIA)
- 2.10 事業単位
- 2.11 事業単位の BCM コーディネーター
- 2.12 事故
- 2.13 重大性
- 2.14 重大な機能・重大なビジネス機能(CBF)
- 2.15 災害
- 2.16 中断
- 2.17 災害からの回復
- 2.18 災害回復計画(DR 計画)
- 2.19 教育
- 2.20 緊急事態
- 2.21 緊急オペレーションセンター
- 2.22 経営幹部
- 2.23 演習
- 2.24 危険状態
- 2.25 インフラストラクチャー
- 2.26 最低限の事業継続目標(MBCO)
- 2.27 組織の BCM コーディネーター
- 2.28 人員
- 2.29 方針
- 2.30 手順
- 2.31 プロセス
- 2.32 回復点目標(RPO)
- 2.33 回復時間目標(RTO)
- 2.34 弾力性
- 2.35 リスク
- 2.36 リスク容認

2.37 リスク回避

2.38 リスク低減

2.39 リスク移転

2.40 リスク処理

2.41 試験

2.42 脅威

2.43 訓練

2.44 バイタルレコード

第3項 リスク分析と検討

3.1 適用範囲

3.2 方針

3.2.1 BCM 運営委員会

3.2.2 リスクの特定と順位付け

3.2.3 リスク処理

3.2.3.1 リスク回避

3.2.3.2 リスク低減

3.2.3.3 リスク移転

3.2.3.4 リスク容認

3.2.4 可能性の高い災害

3.2.5 首尾一貫したリスク分析の手法

3.2.6 専門知識

3.3 プロセス

3.3.1 事業単位

3.3.2 事業運営プロセスの検討

3.4 人員

3.4.1 レビューを行うスタッフ

3.4.2 不可欠なスタッフの役割と技量

3.5 インフラストラクチャー

3.5.1 技術と設備

3.5.2 施設

第4項 ビジネス・インパクト分析

4.1 適用範囲

4.2 方針

4.2.1 最低限の事業継続性目標

4.2.2 BCM 運営委員会

4.2.3 規制上の要求事項

4.2.4 専門知識

4.2.5 インパクト分析の優先順位

4.3 プロセス

4.3.1 事業単位

4.3.1.1 運営上の制約

4.3.1.2 事業単位レベルの MBCO

4.3.2 重要ビジネス機能の特定

4.3.2.1 各重要ビジネス機能を支援する業務

4.3.2.2 代替プロセス

4.3.2.3 文書化

4.3.3 重要ビジネス機能の回復時間に関する要求事項

4.3.4 重要ビジネス機能に優先順位を決定する

4.3.5 バイタルレコード

4.3.6 データ収集

4.4 人員

4.4.1 BIA を実施するスタッフ

4.4.2 主要スタッフ

4.5 インフラストラクチャー

4.5.1 技術および設備

4.5.2 施設

第5項 戦略

5.1 適用範囲

5.2 方針

5.2.1 BCM 運営委員会

5.2.2 戦略の策定

5.2.3 外注

5.3 プロセス

5.3.1 業務回復戦略に関する要求事項

5.3.2 業務回復戦略の評価基準

5.4 人員

5.5 インフラストラクチャー

5.5.1 技術および設備

5.5.2 施設

5.5.2.1 代替処理

5.5.2.2 外注業者の選定基準

第6項 事業継続計画

6.1 適用範囲

6.2 方針

6.2.1 組織の BCM 方針

6.2.2 BCM 運営委員会

6.2.3 緊急事態対応と災害復旧

6.2.4 災害宣言の基準

6.2.5 事業単位

6.2.6 対策の優先順位

6.2.7 緊急事態対応

6.2.8 文書化

6.2.9 情報および情報システムに関する要求事項

6.2.10 情報伝達

6.3 プロセス

6.3.1 事前準備

6.3.2 初期の損害評価

6.3.3 緊急事態対応手順

6.3.4 クライシスコミュニケーション

6.3.5 外部機関との調整

6.3.6 重要品目リスト

6.3.7 有害物質の取り扱い

6.3.8 通信システムの回復

6.3.9 インベントリーリスト

6.3.10 IT 情報サービス

- 6.3.11 セキュリティと管理
 - 6.3.11.1 情報処理と情報セキュリティ
 - 6.3.11.2 物理的アクセスに対するセキュリティと管理
 - 6.3.11.3 論理的アクセスに対するセキュリティと管理
- 6.3.12 災害後の通常業務への復帰
- 6.3.13 BC 計画の配布と管理
- 6.4 人員
 - 6.4.1 BCM 運営委員会
 - 6.4.2 組織 BCM コーディネータ
 - 6.4.3 事業単位 BCM コーディネータ
 - 6.4.4 災害宣言責任者
 - 6.4.5 計画実行チーム
 - 6.4.6 損害評価チーム
 - 6.4.7 医療
 - 6.4.8 集合場所および人的安全
 - 6.4.9 連絡先リスト
- 6.5 インフラストラクチャー
 - 6.5.1 技術と設備
 - 6.5.1.1 一般設備に関する要求事項
 - 6.5.1.2 追加設備に関する要求事項
 - 6.5.1.3 重要設備および補充品のリードタイム
 - 6.5.1.4 計算装置に関する要求事項
 - 6.5.1.5 通信に関する要求事項
 - 6.5.2 施設
 - 6.5.2.1 緊急事態対応センター(EOC)
 - 6.5.2.2 代替場所に関する要求事項
 - 6.5.2.3 施設保護
 - 6.5.2.4 敷地外での保管

第7項 試験および演習

7.1 範囲

7.2 方針

7.2.1 目的

7.2.2 レベルおよび頻度

7.2.3 品質

7.3 プロセス

7.3.1 方法

7.3.2 報告

7.3.3 文書化

7.3.4 勧告および是正措置

7.3.5 保留事項

7.4 人員

7.4.1 評価

7.4.2 是正措置

7.5 インフラストラクチャー

7.5.1 技術および機器類

7.5.1.1 時間設定

7.5.1.2 バイタルレコードおよび資源

7.5.2 設備

7.5.2.1 時間設定

7.5.2.2 代替場所

第8項 プログラムマネジメント

8.1 範囲

8.2 方針

8.2.1 リスクおよび復旧戦略

8.2.2 最低限の事業継続目標

8.2.3 役割および責任

8.2.4 BC 計画

8.2.5 BC 計画の文書化維持

8.2.6 文書化および報告

8.2.7 BCM 監査

8.2.8 業者との契約

8.2.9 訓練および認識

8.2.9.1 訓練および認識プログラムのレベル

8.2.9.2 評価

8.2.10 BCM 計画

8.3 プロセス

8.4 人員

8.4.1 BCM 運営委員会

8.4.2 組織の BCM 統括責任者

8.4.3 組織 BCM 会議

8.4.4 BCM の動向

8.4.4.1 業界の BCM 活動への参加

8.4.4.2 業界の展開を追跡する

8.4.4.3 内部更新および認識

8.4.5 訓練および認識プログラム

8.4.5.1 任務保持者

8.4.5.2 全スタッフ

8.4.5.3 専門スタッフ

8.5 インフラストラクチャー

8.5.1 技術および機器類

8.5.1.1 事業運営および環境の変化

8.5.1.2 訓練・認識の支援

8.5.2 設備

8.5.2.1 事業運営および環境の変化

8.5.2.2 代替場所の準備

附属書

引用文献

SPRING Singapore

www.spring.gov.sg

規格

www.standards.org.sg

（概要）

①TR19 について

TR19 は 2005 年に SPRING Singapore がリリースした事業継続管理（BCM）のためのテクニカル・レファレンス(以下 TR)である。

この TR が焦点をあてているのは、継続管理と重要な業務の回復である。これにはリスク低減（物理的および IT のセキュリティまで含むような）予防手段、災害復興計画、実施の方法論およびプロセス、企業継続計画立案、緊急事態への対応と管理、危機伝達管理、サプライ・チェーンの統制および産業界と公共機関との協力などが含まれる。

内容的には NFPA1600・PAS56・BCI ガイドラインから SOX 法まで幅広く取り込んでいるので BCM を構築しようとしている企業にとっては包括的にマネジメントシステムの必要事項をチェックすることができる。

②SPRING Singapore について

SPRING(Standards, Productivity and Innovation Board・規格、生産および変革理事会)Singapore の使命はシンガポール経済活性化のための企業の競争力を高めることであるが、SPRING Singapore は同時にシンガポールの国内規格団体でもある。SPRING Singapore は国内標準化プログラムの下で、シンガポール規格の発展を図り、会社や企業が国際標準を満たし、要求事項の適合する援助をしている。

SPRING Singapore はシンガポール規格の作成、発表および施行ならびに TR およびその履行について助言する Standard Council を指名する権限を持っている。

③2 年間の暫定適用

TR は参照規格がまだない分野において産業界が直面している製品、工程あるいはサービスについての規格または要求事項の必要性に答えるためにまとめられた一時的なものである。これはシンガポール規格とは異なり、コメントを求めるために 2 年間に限定して発行され、その後シンガポール規格としての適格性について評価されるのである。2 年の経過後、コメントはすべて TR を審査する際に考慮され、これらをシンガポール規格に移行できるか否かが決定される。つまり、TR は 2 年後にシンガポール規格になることも、更なるコメントを求めるために引き続き TR とされることも、または廃止されることもあるわけである。

この TR19 も 2 年間の暫定的適用に供されるものであり、まだシンガポール規格となっているわけではない。TR19 の利用者はその技術的な内容、利用のしやすさ、または不明瞭な点において意見を述べることができる。これらの意見は TR19 の末尾にあるフィードバック用紙を用いて提出することができ、規格発行の再検討時に考慮されることになる。2 年間の最後に TR19 は入手した意見を検討し、シンガポール規格としての妥当性を決めるために専門委員によってレビューされる。シンガポール規格として規格協議会の承認を得るための提出は、レビュー後の合意に基づいて実行されることとなる。

3.8 金融機関等のコンティンジェンシープラン策定・運用に関する研究会 報告書

1. ガイドラインの名称	金融機関等のコンティンジェンシープラン策定・運用に関する研究会 報告書
2. 発行時期	平成 13 年 6 月
3. 発行者	財団法人 金融情報システムセンター
4. 対象となる地域	日本
5. 対象リスク	システムリスク
6. 概要	
（発行の目的） 金融機関等における IT 環境が、クライアント・サーバへと変化し、また、社内ネットワークやインターネットの利用が進展したことに伴い新たなリスクが生じている。これらの問題が、コンティンジェンシープラン策定・運用に与える影響を検討し、必要があれば、新たな内容を追加することを目的とする。	
（章項目） はじめに 第 1 章 状況認識 1 背景 2 研究会活動概要 第 2 章 検討概要 第 3 章 取り上げられた主なテーマ 1 コンティンジェンシープランの定義とその対象とする範囲 2 災害等の予見、予兆がコンティンジェンシープラン策定に与える影響 3 サイバーテロに対するコンティンジェンシープラン 4 リスクの連鎖に対する考え方とコンティンジェンシープラン 5 緊急時における連絡体制のあり方について 第 4 章 まとめ 研究会委員等	

（概要）

コンティンジェンシープランの定義とその対象とする範囲

本書においてコンティンジェンシープランとは、金融機関等のコンピュータシステムが、不慮の災害や事故、あるいは障害等により重大な損害を被り業務の遂行が困難になった場合に、損害の範囲と業務への影響を極小化し、迅速かつ効率的に業務の復旧を行なうために予め策定され、各個別金融機関等においてそれぞれ統一された「緊急時対応計画」である。

災害等の予見、予兆がコンティンジェンシープラン策定に与える影響

有珠山噴火を体験した地元金融機関に取材した結果、災害等の予見、予兆がコンティンジェンシープラン策定そのものに与える影響はないであろうとしている。予見、予兆によって迅速に準備体制がとれ、それによる効果は多大なものがあるが、コンティンジェンシープランそのものに予見や予兆への対応はいまだ難があると思われる。予兆の段階で「連絡本部」を設置することが、考えられるが、このことは、従来のコンティンジェンシープランの範囲で実施可能と考えられるため、現段階では予見、予兆によるコンティンジェンシープラン策定への影響はないと思われる。

サイバーテロに対するコンティンジェンシープラン

本研究会においても、ネットワークセキュリティ専門企業や専門家にヒアリングを実施したが、サイバーテロの危機管理計画については着手した段階であり、広く一般化するところまではいっていないといえる。指摘された点は以下のとおり。

- ① 従来のバックアップ機（代替機）による代替手段は必ずしも有効ではない。

サイバーテロという悪意をもって攻撃を企てるような特殊なケースでは、バックアップ機に切り替えても再び攻撃を加えてくることが予想される。

- ② 侵入検知システム（IDS）の導入は必須である。

高度情報通信社会推進本部ホームページの「情報セキュリティ対策」上にある「セキュリティ対策セルフチェックシート」でIDS導入が指導されている。

- ③ サーバOSの異なるバックアップ機を用意する。

WindowsやUNIXは広くその機能を知られており、サイバーテロの攻撃対象となりやすい。できればそれらのOSを避けるか、メインサーバとバックアップサーバで異なるOSの2システムを用意することが望ましい。

- ④ ネットワークセキュリティ専門企業等によるバックアップ体制を考慮する。

リスクの連鎖に対する考え方とコンティンジェンシープラン

イベントツリーの図を用いながら事象がどのように連鎖的につながって発生していくかを示した例などを用いながら、リスクの連鎖に対する考え方は重要な考え方であることは示すが、今回は改訂への反映を見送る。

緊急時における連絡体制のあり方について

下記等に関する考察は示すが、今回は改訂への反映を見送る

トップダウン型による連絡の断絶や遅延

危機管理マネージャーの設置と位置づけ

広報部の存在と果たすべき機能

危機管理マネージャーの勤務時間外での任務

システム部内の危機管理マネージャーの設置と任務

システム危機管理マネージャーの平時における任務

情報伝達手段について

情報システム部門に関連する危機や事故

7. 問合せ先	(URL or TEL 等) 財団法人 金融情報システムセンター 03-5542-6060（代表）
8. 入手方法	

3.9 The Business Guide to Business Continuity Management

1. ガイドラインの名称	The Business Guide to Business Continuity Management
2. 発行時期	22 Jan 2001
3. 発行者	BCI および BRE/ロス プリベンション委員会とセーフティネット/ガーディアン IT（現在はサンガード社の一部門）のコンソーシアム
4. 対象となる地域	グローバル
5. 対象リスク	
6. 概要	(概要) 下記の3つのドキュメントから構成される。 ・ BCM：ビジネスサバイバルの戦略 企業の取締役を対象に事業継続を戦術レベルから戦略レベルへ高めるリーフレット。 ・ 継続管理のためのビジネスガイド 事業継続カルチャーを企業に導入するための実践ガイドライン。 ・ 事業継続計画の評価基準 企業の各部門がそれぞれの BCM レベルを評価するためのベンチマーク。
7. 問合せ先	(URL or TEL 等)
8. 入手方法	

3.10 Expecting the unexpected

1. ガイドラインの名称	Expecting the unexpected.
2. 発行時期	2003
3. 発行者	英国国家テロ対策セキュリティオフィス (The National Counter Terrorism Security Office.) ロンドン・ファースト (London First) , BCI
4. 対象となる地域	UK
5. 対象リスク	テロ攻撃および火災、洪水等の自然災害
6. 概要	
(発行の目的) BCM に関するチェックリストと有益なアイデアの提供 効果的 BCP 作成の手引き	
(章項目) 1. ビジネス分析 2. リスク評価 3. 戦略策定 4. 計画策定 5. 計画のリハーサル (訓練)	
(概要) BCM プロセスの重要ポイントとマッチしたチェックリストと有益なアイデアを提供することにより効果的 BCP 作成を手引きする。 上記章項目（ビジネス分析、リスク評価、戦略策定、計画策定、計画のリハーサル）を BCM 策定へのステップとして記述している。 (ベストプラクティス) BT Group plc、DTZ Debenham Tie Leung、Ernst & Young、KPMG、Morley Fund Management、Prudential plc、Shell、Tesco plc、など	
7. 問合せ先	http://www.mi5.gov.uk/files/pdf/expecting.pdf#search='expecting%20the%20unexpected%20terrorism%20security'
8. 入手方法	ダウンロード可能

3.11 Civil Contingencies Act 2004

1. ガイドラインの名称	Civil Contingencies Act 2004
2. 発行時期	2004 (2005 年 10 月改定)
3. 発行者	英国内閣府 (Cabinet Office)
4. 対象となる地域	英国
5. 対象リスク	自然災害、重大事故、重大事件、伝染病
6. 概要	(発行の目的) 2004 年 11 月の英国王室より承認を受け、英国市民を様々な自然災害、重大事故、重大事件、伝染病から守るためのフレームワークとして制定された市民緊急事態法。 (章項目) 2つのパートから構成される。 パート1：地域市民保護を地域単位で行うことに重点を置く。 パート2：緊急事態における権限について記載。 (概要) 英国市民を様々な自然災害、事故、伝染病から守ることを目的とし、レスポнда（警察、交通、消防、救急医療、電気、ガス、上下水道、通信）に対する役割と責任範囲について規定している。レスポндаに対する以下の項目が盛り込まれている。 ・ 緊急事態発生時におけるリスク評価とコンティンジェンシープランニング ・ エマージェンシープランとの関連付けと実施 ・ BCM との関連付け ・ 他のレスポндаとの情報共有 ・ 他のレスポндаとの協力体制 ・ ビジネス組織に対する BCM アドバイス
7. 問合せ先	http://www.ukresilience.info/ccact/index.htm
8. 入手方法	ダウンロード可能

3. 12 Basel Capital Accord

1. ガイドラインの名称	Basel Capital Accord
2. 発行時期	2004 年 6 月(2005 年 11 月改定)
3. 発行者	バーゼル銀行監督委員会（Basel Committee on Banking Supervision）
4. 対象となる地域	国際業務を行う銀行
5. 対象リスク	信用リスク、市場リスク、オペレーショナルリスク
6. 概要	（発行の目的） 国際金融市場における取引の安全性強化のために規定された、国際業務を行う銀行の自己資本比率に関する国際統一基準（BIS 規制あるいはバーゼル合意）にオペレーショナルリスクを導入。 （章項目） 4つのパートから構成されている。 1. アプリケーションの適用範囲 2. 資本に関する最低限の要求事項 3. および4. 監督関係当局のレビュープロセスと市場規律 （概要） 新 BIS 規制で拡大されたオペレーショナルリスクについてリスクの定義として内部プロセス、人々、システム、そして外部からのイベントを挙げている。またこのリスクにはリーガル（法的）リスクも含まれていると述べている。 上記リスクに対する測定手法と信用リスクと市場リスクと関連付けされた監督関係当局のレビュープロセスについて記載。
7. 問合せ先	http://www.federalreserve.gov/generalinfo/basel2/default.htm
8. 入手方法	ダウンロード可能

3. 13 Business Continuity Management Guidelines

1. ガイドラインの名称	Business Continuity Management Guidelines
2. 発行時期	2003 年 6 月
3. 発行者	Monetary Authority of Singapore
4. 対象となる地域	シンガポール
5. 対象リスク	リスクを問わない
6. 概要	(発行の目的) The global financial systems is a set of interlinked networks of markets, systems, and participants. While financial institutions acknowledge the need to strengthen their resilience against disruptions, they also recognise that network is only as strong as its weakest link and the potential impacts of a major operational disruption may incapacitate the financial system. The quick recovery of business functions after disruption is therefore crucial on maintaining confidence in institutions. (世界の金融システムは、マーケット・システム・市場関係者で互いに依存・連携している。金融機関は、混乱に対するレジリエンシーの必要性・重要性、及びオペレーションの停止が金融システムを崩壊させ得ることを認識している。ビジネスの早期なる復旧は金融機関の経営にとって極めて重大である。)

(章項目) 1.0 Introduction（序論） 1.1 Readiness is Your Only Protection（BCMは自身を守るもの） 1.2 Application of the Guideline（ガイドラインの適用範囲） 1.3 Glossary（用語解説） 2.0 Business Continuity Management Principle（BCMの基本的考え方） 2.1 Principle 1: Board of Directors and Senior Management should be responsible for their institution's Business Continuity Management (経営者はBCMの責任を負う) 2.2 Principle 2: Institutions should embed Business Continuity Management into their as-usual operations, Incorporating sound practices (金融機関は、BCMを日常の業務に文化として醸成させる必要がある) 2.3 Principle 3: Institutions should test their Business Continuity Plan regularly, completely and meaningfully. (金融機関は、BCPを定期的に、完璧に、意味あるようにテストしなければならない) 2.4 Principle 4: Institutions should develop recovery strategy and set recovery time objectives for critical business functions. (金融機関は、復旧戦略を発展させ、基幹業務の目標復旧時間を設定する) 2.5 Principle 5: Institutions should understand and appropriately mitigate interdependency risk of critical business functions. (金融機関は、基幹業務の相互依存リスクを理解し、低減させる必要がある) 2.6 Principle 6: Institutions should plan for wide-area disruption. (金融機関は、広域災害にもBCPとして対応する必要がある) 2.7 Principle 7: Institutions should practice a separation policy to mitigate Concentration risk of critical business functions. (金融機関は、基幹業務の集積リスクを低減させるためバックアップを 実践すべきである)	
(概要) BCM について、包括的なフレームワークを規定している。金融機関が BCM のフレームワークを構築する際は、DRII 及び BCI の考えを参照することを勧めている。	
7. URL	http://www.mas.gov.sg/
8. 入手方法	ダウンロード可能

3. 14 Business Continuity Management HB221:2004

1. ガイドラインの名称	Business Continuity Management HB221:2004
2. 発行時期	2004 (Second Edition)
3. 発行者	スタンダード オーストラリア、スタンダード ニュージーランド
4. 対象となる地域	オーストラリア、ニュージーランド
5. 対象リスク	ビジネス組織オペレーション
6. 概要	(発行の目的) ビジネス組織の包括的 BCP に含まれる、一般的なフレームワークとコアプロセスを概説。多国籍大企業から小規模企業まで組織のサイズを問わない。 (章項目) 2つのパートから構成される。 パート1：Business Continuity Management とは？ パート2：BCM マニュアル (概要) パート1ではBCMの定義とITをメインに据えたBCMから、戦略的な計画作成を手助けするプランニングツールまでに発展させるための概略について解説。 パート2ではBCMフレームワーク作成方法について解説。ワークブックとしてBCM実践のための各ステップについての補足も提供。このワークブックは様々な組織規模に合った形でプロセスを導入するためのテンプレートから構成されており、次の分野をカバーしている。 ・ IT リカバリープランの作成 ・ リスクマネージメント関連付け ・ 企業ガバナンスと BCM プログラム
7. 問合せ先	http://www.standards.com.au/PDFTemp/Previews/OSH/as/misc/handbook/HB221-2004.PDF
8. 入手方法	ダウンロード可能（要購入）

3. 15 Contingency Planning Guide for Information Technology Systems

1. ガイドラインの名称	Contingency Planning Guide for Information Technology Systems
2. 発行時期	2002 年 6 月
3. 発行者	NIST-National Institute of Standards and Technology（国家標準技術研究所）
4. 対象となる地域	米国
5. 対象リスク	IT システム全般
6. 概要	
（発行の目的） あらゆる IT オペレーションにおける時間、コストを省いた BCP の構築方法を提供する。 （章項目） 1. Introduction 2. Background 3. IT Contingency Planning Process 4. IT Contingency Plan Development 5. Technical Contingency Planning Considerations	
（概要） 行政府関係の一般的な IT システム（パソコン、サーバー、WEB サイト、LAN、分散システム、メインフレームシステム）を対象としており、スーパーコンピュータやワイヤレスネットワークは含んでいない。 とは言うものの、100 ページ以上あるガイドラインは IT システムの BCP について詳細に記載されており、通常の IT システムについては十分な内容である。	
7. 問合せ先	http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf
8. 入手方法	ダウンロード可能

3. 16 The Disaster Process and Disaster Aid Programs

1. ガイドラインの名称	The Disaster Process and Disaster Aid Programs
2. 発行時期	2006 年 4 月 18 日
3. 発行者	FEMA
4. 対象となる地域	米国
5. 対象リスク	自然災害全般
6. 概要	(発行の目的) 災害時における F E M A の活動内容の概要説明 (章項目) 1. Response and Recovery 2. The Major Disaster Process 3. Disaster Aid Programs (概要) FEMA・Federal Emergency Management Agency はワシントン D.C.に本拠地を置き、米国土安全保障省(U.S. Department of Homeland Security)の一部として主に米国内の自然災害に対応する組織である。 本ガイドは行政府として災害の認定、被災者の救援のプロセスなどについて記載したものである。
7. 問合せ先	http://www.fema.gov/library/dproc.shtm
8. 入手方法	ダウンロード可能

3. 17 Federal Legislative and Regulatory Business Continuity Requirements for the IRS

1. ガイドラインの名称	Federal Legislative and Regulatory Business Continuity Requirements for the IRS
2. 発行時期	2003 年 2 月 28 日
3. 発行者	IRS –Internal Revenue Service
4. 対象となる地域	米国
5. 対象リスク	リスク全般
6. 概要	
（発行の目的） IRS（米国国税庁）として行政関係者全員がBCP構築の参考となる情報を提供する。	
（章項目） 1. Introduction 2. Understanding Business Continuity Management 3. Where the Requirements Come From 4. Current Business and Government Business Continuity Best Practices 5. Recommended Approach to Address Business Continuity 6. IRS Business Continuity Requirements	
（概要） 行政府として法的業務が中断しないように作成されたものである。 各行政機関との連携、役割分担、規定類の関係を表にまとめているのが特徴であり、正に行政関係者のためのガイドである。 本ガイドはMITRE(国防省等の委託を受ける非営利機関)がまとめたようである。	
7. 問合せ先	http://www.mitre.org/work/tech_papers/tech_papers_03/talley_irs/fedbuscontreq_irs.pdf

3. 18 FFIEC BCP Handbook

1. ガイドラインの名称	FFIEC BCP Handbook
2. 発行時期	2003 年 3 月
3. 発行者	連邦金融機関検査協議会（FFIEC）
4. 対象となる地域	米国
5. 対象リスク	金融関連業務サービス全般
6. 概要	（発行の目的） 金融機関検査員向け BCP ガイダンスと検査手順および重要金融サービス運用を確実にするためのリスクマネジメントについて記述。 （章項目） ・ 取締役、シニアマネジメントの責任範囲について ・ BCP プロセス ➤ ビジネスインパクトアナリシス ➤ リスクアセスメント ➤ リスクマネジメント ➤ ポリシー、標準化とプロセス ➤ リスクモニター ・ 付録として検査手順、用語説明、内外部の脅威、相互依存関係、BCP コンポーネントを掲載 （概要） 各章の始まりはアクションサマリから始まり BCP のために何を実行しなければならないのかをリストしている。BCP 最終ステップのリスクモニターに関しては BCP テスト戦略、テスト範囲と目的、プラン、レビュー、評価方法を詳細に記述。付録として金融機関検査員のための BCP 検査手順を掲載している。
7. 問合せ先	http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf
8. 入手方法	ダウンロード可能

3. 19 FSA Handbook / Financial Sector Business Continuity Annual Report

1. ガイドラインの名称	FSA Handbook / Financial Sector Business Continuity Annual Report
2. 発行時期	2004 年 10 月
3. 発行者	Financial Services Authority (金融サービス機構)
4. 対象となる地域	英国金融業界
5. 対象リスク	
6. 概要	(発行の目的) FSA Handbook は FSA ルールに関する最も信頼のおける文書として位置づけされる。 Financial Sector Business Continuity Annual Report はイギリス金融業会における事業継続に関する年次報告書。 (章項目) FSA Handbook Block 1 : スタンダード概略 Block 2 : スタンダードの細分化 Block 3 : ビジネススタンダード Block 4 : 規制に関するプロセス Block 5 : 告訴と補償について Block 6 : スペシャリストのソース (原典) Block 7 : 目録、目論見書、開示に関するルール Financial Sector Business Continuity Annual Report 1 : 2005 年 7 月 7 日に発生したロンドン同時爆破事件と金融業界の事業継続、2 : レジリエンス (回復力) のベンチマーク、3 : 事業継続訓練、4 : FSC とのコミュニケーションと協力体制、5 : 事業継続についての政府の取り組み、6 : その他の活動状況について (概要) ハンドブックでは標準、規制、コンプライアンス、インシデント管理のガイドライン等、金融業界が取り組むスタンダードとルールについて広範に渡って記載。また、Financial Sector Business Continuity Annual Report では民間と共同で英国金融業会の事業継続年次報告などを出している。
7. 問合せ先	http://fsahandbook.info/FSA/html/handbook/ http://www.fsc.gov.uk/upload/public/Files/5/64791_1.pdf annual rep.pdf
8. 入手方法	ダウンロード可能

3. 20 NERC Continuity of Business Processes

1. ガイドラインの名称	NERC Continuity of Business Processes
2. 発行時期	2002 年 6 月 14 日
3. 発行者	NERC-North American Electric Reliability Council
4. 対象となる地域	米国
5. 対象リスク	自然災害その他
6. 概要	
(発行の目的) 災害時においてBCPは被害を低減し、速やかな事業回復に役立つ。	
(章項目) 1. Purpose 2. Applicability 3. Guideline Statement 4. Table of Contents(blank) 5. Guideline Detail 6. Exceptions(blank) 7. Certified Products/Tools(blank) 8. Related Documents	
(概要) 電力業界向けのBCPガイドラインである。 電力は公的ライフラインということもあり、代替施設の確保や十分な対応でなくても、電力の供給を最低限止めないための方策を構築するよう指導している。	
7. 問合せ先	http://www.esisac.com/publicdocs/Guides/V1-BusinessContinuity.pdf
8. 入手方法	資料ダウンロード可能

3. 21 NFA Rule 2-38

1. ガイドラインの名称	NFA Rule 2-38
2. 発行時期	2003 年 4 月
3. 発行者	米国先物協会（National Futures Association）
4. 対象となる地域	NFA メンバー
5. 対象リスク	自然災害、重大事故、重大事件、伝染病
6. 概要	
（発行の目的） NFA が NFA 会員（メンバー）向けに規定したコンプライアンスルール。	
（章項目） (a) 事業継続とディザスタリカバリー計画に関する書面を準備、継続的整備を行う義務について。 (b) 緊急時の担当者コンタクト情報提供義務について。	
（概要） NFA メンバー向けに事業継続とディザスタリカバリー計画に関して、書面の準備と継続的整備を行う義務について規定している。 実際に緊急事態が発生した場合における、担当者コンタクト情報提供と復旧状況報告義務を規定している。	
7. 問合せ先	http://www.nfa.futures.org/printerFriendly.asp?tag=ComplianceRules
8. 入手方法	ダウンロード可能

3. 22 NYSE Rule 446

1. ガイドラインの名称	NYSE Rule 446
2. 発行時期	2002 年 8 月
3. 発行者	ニューヨーク証券取引所（NYSE）
4. 対象となる地域	NYSE メンバーおよび関連組織
5. 対象リスク	取引記録、ビジネスシステム、通信、事業所
6. 概要	
（発行の目的） Sep. 11, 2001 テロによる事業停止を踏まえ、証券取引業務継続をより強固なものにするための新ルール。	
（章項目） I. ルール（変更）についての用語と要旨の説明。 II. ルール変更の目的について。 III. ルール適用スケジュールについて。 IV. 意見、コメントの提出方法について。	
（概要） NYSE メンバーおよび関連組織に対する事業継続およびコンティンジェンシープランに関する新ルール。取引記録、ビジネスシステムのバックアップとリカバリープロシージャ作成、メンテナンス、レビューに関するルールと用語の意味、要旨について記述している。	
7. 問合せ先	http://www.sec.gov/rules/sro/34-46443.htm#P13_338
8. 入手方法	ダウンロード可能

3. 23 SS507 Singapore Standard for Business Continuity/Disaster Recovery (BC/DR) for Service Providers

1. ガイドラインの名称	SS507 Singapore Standard for Business Continuity /Disaster Recovery (BC/DR) for Service Providers.
2. 発行時期	2004 8 月
3. 発行者	SPRING シンガポール
4. 対象となる地域	シンガポール
5. 対象リスク	ビジネス組織の情報通信システム
6. 概要	(発行の目的) サービスプロバイダーが顧客に BC/DR を提供する際の品質要求基準についての標準化。 (章項目) 6つのパートから構成される。 1：BC/DR の適用範囲 2：定義事項 3：要求事項 4：DR 施設・設備・環境認定 5：サービスプロバイダー提供能力認定 6：リカバリサイト選択についてのガイドライン (概要) 3つのキーエリアをカバーしている。 一般的な要求事項：設備とその関連サービスプロバイダーが提供すべきサービスの要求事項の定義について。 DR 施設（ファシリティ）認定：BC/DR サービスプロバイダーが顧客に対して提供しなければならない安全な物理的運用環境基本要求的の明確化について。 運用環境基本要求的には通信、電源の安定供給等が含まれる。 サービスプロバイダー提供能力認定：リカバリー時におけるサービスプロバイダーの人材能力、要求事項についての明確化について。
7. 問合せ先	http://eshop.spring.gov.sg/cgi-bin/sgpstd_detail.pl?SgStd_ID_p=1165
8. 入手方法	オンライン購入

3. 24 TM-G-2 Business Continuity Planning

1. ガイドラインの名称	TM-G-2 Business Continuity Planning
2. 発行時期	2002 年 12 月 2 日
3. 発行者	HKMA 香港金融管理局
4. 対象となる地域	香港
5. 対象リスク	建物、人命、金融混乱全般
6. 概要	（発行の目的） HKMA・Hong Kong Monetary Authority（香港金融管理局）として期待される B C P への監督的な取り組みを確立する。 （章項目） 1. Introduction 2. Board and senior management oversight 3. Business impact analysis and recovery strategy 4. Development of Business Continuity Plan 5. Alternate sites for business and technology recovery 6. Implementation of Business Continuity Plan （概要） BCP については Y2K の経験があったものの、9.11（米国同時多発テロ）に十分対応できなかった（前者はソフトウェアの問題で後者は人命や建物の被害）ことを踏まえて双方を対象としている。 有事の対応を端的に記載してある。
7. 問合せ先	http://www.info.gov.hk/hkma/eng/bank/spma/attach/TM-G-2.pdf
8. 入手方法	ダウンロード可能

4. 第4章 ケーススタディ

本章では、具体的にどのようにプロセスを構築をしているかについて2つの事例を紹介する。

4.1 日本ヒューレット・パカード社の事例

4.1.1 BCM 構築の心構え

弊社は米国 Hewlett-Packard 社（以下 HP 社）100%出資の日本法人である。主な事業内容はコンピューターシステムの構築、コンサルティング、PC の製造・販売、プリンターの販売等であり、既に日本市場において 40 年以上ビジネスを展開している。米国系企業ではあるが、ある意味日本企業といってもよい。

国内の社員数は非正社員も含めて約 10,000 人、事業所とよぶ 1,000 人前後のオフィスは東京、大阪に 6 か所、営業・サービス拠点は全国に 47 か所である。

R&D（研究開発）センターおよび大規模な製造ラインは日本国内にはないが、東京の昭島に PC、コンピューターサーバー等の組み立て製造ラインを持っている。これからお話しする BCP は以上のような事業規模の企業における BCP であるのご理解いただきたい。

最近日本でも BCM(Business Continuity Management)の重要性が活発に議論されているが、米国の HP 社では 12 年ほど前から BCP(Business Continuity Plan)の作成が推進されてきた。我々日本人でも 10 年ほど前から BCP の策定に取り組んでいるが、途中会社の分割、合併などがありその都度、組織やビジネス環境の変化を強いられ、思うように BCP の改善が進まない時期もあった。ここ数年は各事業部の意識も高まり、管理部門、サービス事業部、コールセンター、サプライチェーンを中心にプランも整いつつあるが、全社的な取り組みという観点からはまだ道半ばというところだろうか。

何事も初めてのものはスタートに時間がかかるものだが、弊社の場合も各事業部における BCP 担当者は自部署の BCP 作成に苦労した。その原因の一つはまず難しく考えすぎるのである。HP 社が用意した BCP 作成マニュアルも 100 ページ近くあり、これがまた拍車をかけた。確かに自部署だけではプランは完結せず、他部署との連携も口で言うほど簡単ではないのも事実である。優秀で立派なプランを作ろうと思う人ほど苦労している。すでに緊急時や災害時のプランはある程度あるので、BCP というと既存のそれらを大幅に上回るプランを作らなければと気負ってしまうようだ。実際そんなに複雑で立派なプランは実行も難しい。BCP といっても事業の「継続」にフォーカスしているだけで従来の災害時対応プラン等とレベル的にはそう違うものではない。後述するが、最近はHP社の BCP 作成プロセスもシンプルな方向に向かっている。出だしの壁にぶつかっている方は、「BCP なんてコンセプトがなくなつて、自社や顧客の業務が中断したり、設備が壊れたらもとの状態に戻すのは当たりまえのことだ」くらいに考えればいいのではないだろうか。肩の力が抜けるといい考えが浮かぶものである。

ある程度骨子が固まったら、複数の関係する社員の意見を取り入れて練り上げていく。おそら

く関係する人の数にもよるが、ミーティングを重ねるたびにプランは複雑になり詳細な資料が増えていくと思われる。あれもこれもと不安になるのは致し方ないが、とりまとめる者は自社のリソースを考慮して、「できることとできないこと」の見極めが必要になる。役員をはじめ社内関係者に説明する時は詳細な資料も必要かもしれないが、プランはあくまで現場の声を反映した実効性の高いシンプルなものにするべきである。平時の会議室と違い、非常時の現場では限られた条件下でスピーディーな判断、行動が要求されるからである。

4.1.2 米国のリスクマネジメント

HP社は米国西海岸を代表するIT企業であるがHP社のリスクマネジメントを通じて米国におけるリスクマネジメントの特徴を見ることができる。

そのプロセスは日本のそれと大きな違いはないがリスクマネジメントの考え方に大きな違いを感じる。まず日本は昔から「安全と水はただ」という有名なフレーズに代表されるように安全な状態、リスクがない状態をあたりまえとし、リスクを限りなくゼロにすることを当然の目標とする。ある意味完璧主義者と言ってもいい。一方欧米では歴史や国情の違いもあるのだろうが、この世のありとあらゆるものにリスクはつきものであり、それを無くすことは不可能である。ビジネスをしていく上でリスクは避けられないものであり、避けよう、無くそう、保険をかけようの一本やりではなく、時には受け入れようという姿勢がベースにある。いわゆるリスクテイキングである。彼らはよく **Mitigation**（削減・緩和）という言葉を使い、100あるリスクが30に削減できればそれは70安全になったという理解だ。リスクゼロに執着はしない。もちろんどちらがいいとか悪いというものではなく、どちらも正しい。安全と平和を願う気持ちは日本も米国も変わらない。先ほどの例で言えば70安全とみるか30危険とみるか、考え方の違いである。但し、製品の軽微な不具合といった程度のものであれば100%再発防止策も可能であろうが、自然災害、テロといったハイリスクに対して理想を追求するあまり手詰まりになってしまうよりは、不完全ながらもリスクを削減するアクションを少しでも早急にとるほうが賢明である。

またもう一つ違うなと感じるのは「地震」に対する認識である。日本では災害＝地震であり、何はともあれ地震が怖いのだが日本以外の国の人たちはそれほど地震をリスクのトッププライオリティには置いていない。確かに日本は飛びぬけた地震国ではあるが、大地震は米国をはじめ世界のいたるところで起きている。その割には地震がそれほど話題にならない。我々が米国人ほどテロやハリケーンを意識しないのと同様であろうか。彼らにとって地震はもちろん大きなリスクではあるがテロやハリケーン、火災といった様々なリスクの一つという認識である。

このあとBCPの作成プロセスについて説明するが日本のように地震対策といった個別リスク対応ではなく「事業継続」の視点から各リスクに共通する包括的なプロセス、対応組織を構築するのである。

4.1.3 HP 社の BCP（COP）

では以下HP社のBCP作成プロセスを簡単にみていくことにする。日本法人も基本的にはこのプロセスに準ずる。実はHP社では今年に入ってから BCP という呼称をやめて COP(Continuity of Operations Plan)という言い方に変更している。HP社では「従来のBCPは各事業部、各事業所における業務復旧にフォーカスしていたが今日のビジネス環境、業務形態を鑑みると、より包括的、全社的なアプローチの必要がある。」としてCOPの導入を説明しているが、縦横の組織連携を強めようということでBCPと同義とみてよいだろう。また「COPとEPR(Emergency Preparedness & Response 緊急時対応)とCMP(Crisis Management Planning 重大な危機管理プラン)の3つは相互に補完しあい、HPのリスクマネジメントの基盤をなすものである」とも説明している。EPRとCMPの詳細はここでは割愛させていただく。

ではCOP作成プロセスを簡単に紹介していこう。リスクが地震であれ、社員の不正であれCOP作成については以下5つのステップで対応する。

STEP1

Define Critical Business Processes & Activities and Associated Key Risks

このステップの目的は重要な業務とそれに付随するリスクを特定すること。重要な事業とは、それが中断した場合に会社の売上とブランドイメージに深刻な影響を与えるものである。

1) 各事業部及び管理部門において重要な業務を特定する。

影響を受ける重要ファクターとしては会社の評判、ブランドイメージ、顧客の信頼、売上、マーケットシェア、法の遵守などがあげられる。

2) 各事業部単独で行っている業務、管理部門単独で行っている業務、両者が連携している業務を会社全体の業務の流れを考慮して特定する。

3) 重要な業務と特定されたものに深刻なダメージを与えるリスクを特定する。

物理的なリスクとしては火事、洪水、地震、ハリケーン、テロ、爆発、化学薬品漏洩、盗難、機器の故障、社員の不正、伝染病などがあげられる。

4) リスクと特定されたものが業務にあたえる具体的な影響を考察する。

STEP2

Risk Assessment & Prioritization

このステップの目的はSTEP1で抽出されたリスクを分析して、優先付けをすることである。適切なリスク分析によって自社の弱点が把握され、効率的なContinuity of Operationsの作成が可能となる。

- 1) リスクをリストアップしてどの業務にダメージを与えるかを特定する。
- 2) 経済的な影響度を見積もってみる。
- 3) BIA(Business Impact Analysis)をベースにリスクの優先付けを行う。

STEP3

Risk Mitigation

このステップの目的は優先付けされたリスクに対して、既にリスク削減対応がとれているのか、新たに対応策を検討すべきかを特定することである。リスク削減策が適切であれば復旧も効果的に行える。しかも平時に包括的にリスク削減策がとられていれば業務中断のダメージそのものが抑えられるのである。

- 1) 優先付けされたリスクに対して現行のリスク削減策が妥当なものか検討し、文書にまとめる。乖離している部分を特定する。
- 2) 乖離している部分については追加的にリスク削減策を講じ、潜在的なダメージを最低限にする。
- 3) 最も有効で対費用効果の高いリスク削減を検討し、実行責任者を任命する。また会社全体のCOPを包括的にまとめられる担当者も任命する。

STEP4

Incident Response & Recovery

このステップの目的はMALO(minimum acceptable level of operations 業務で最低限要求されるレベル)と短期、長期のリカバリープランを効率的に行うための平時の準備と各プランを実行するためのチームの役割を確定することである。

- 1) MALO を実行するためのリソース（オフィス、ネットワーク、人員、設備等）を決定する。
- 2) 自社と請負業者双方の業務について短期と長期のリカバリープランを作成する。
- 3) 社内および社外のリカバリーチームの役割と責任を決める。

STEP5

Training, Testing & Monitoring

このステップの目的はキーとなる担当者を対象に定期的にテスト、モニタリングを行ってCOPを改善するためのテストプログラムを確定していくことである。COPは変化していくビジネス環境に伴い、あるいは少なくとも1年に1回は見直しを行う必要がある。トレーニングツールを作

成することによって、担当者及びチームは不測の事態に対応することができるようになるのである。

1) キーとなる担当者を対象としたトレーニングプログラムを文書化する。シナリオを伴った机上訓練を実施する。

2) COP が変化するビジネスに対応して業務中断時に機能できるように、テスト、改善、がきちんと行えるプロセスを確立する。

5つのステップを概観してきたわけだが、これをみて何も特別なことはなく皆さんが通常参考に行っているオーソドックスな内容であることがお分かりいただけたかと思う。事業継続マネジメントも基本は ISO のマネジメントシステム同様アセスメント、分析を行って PDCA(Plan-Do-Check-Act)サイクルによる継続的改善である。何もプランのオリジナリティーやユニークさを競う必要がないので、どの企業にも応用できると思う。重要なのは how to よりもすぐに行動をおこせるかどうかである。我々の評価は自社や顧客の現場を速やかに復旧してなんぼである。研究者ではないので、プロセスや分析にあまり時間をかけるのではなく、すぐに使えるリソース（人員、費用、設備等）の確保に注力すべきであろう。HP社も以前は 100 ページ近い BCP 作成マニュアルがあった。これは参考資料として現在も閲覧できるが、COP にリニューアルしてからはエッセンスをまとめた 20 ページ足らずのマニュアルと付随のテンプレートを用いてプランが作成できるようになっている。テンプレートにそって BIA(Business Impact Analysis)や CBA(Cost/Benefit Analysis)を行い、空欄を埋めていくと 5 ステップが完了し、COP ができあがるというわけだ。ビジネスや組織の変化が激しい今日、多忙な各事業部や管理部門の BCP 担当者が 100 ページのマニュアルを読み込んで BCP の作成、改善を行うのは効率が悪いとの声を反映した結果である。BCP の作成そのものにスピードが要求されているのだ。

4.1.4 マニュアルはそんなに必要か？

ところで緊急時のマニュアルの必要性についてだが、地震などの大災害に対して完璧なマニュアルなどないし、阪神淡路大震災や新潟中越地震においても被災時にマニュアルが大変役立ったという話もあり聞かない。実際はその場でリーダーシップを発揮した方々の活躍で復旧が進んだという例が多いという。現実がマニュアルどおりに進まないのであれば、かえってマニュアルが行動を拘束してしまうといったマニュアル弊害説さえある。確かに詳細で複雑なマニュアルは必要ないかもしれない。しかし、必要最低限行うべきことを一覧にしたものは非常時に有効なはずである。非常時になれば誰もパニックとまでいかなくても戸惑うものである。そんな時に自分がとるべき行動が端的にまとめられていれば、何をやっていいのかわからない、あるいは的外れな行動をとってしまうといったリスクは軽減できる。弊社の地震対応マニュアルは HP 社のマニュアルをベースとして、被災現地用と対策本部用の 2 種類を用意している。社員の安否確認、広報対応、IT インフラ復旧、顧客支援など約 12 種類の項目ごとにチェックリスト形式で最低限行うべき事柄が記載してある。また、責任者も平時に任命しているが、その場で適切なリーダー

一をすぐに任命できるようにあえて責任者の欄は空欄にしてあるのが特徴である。阪神淡路大震災では弊社も神戸事業所が被害にあったのだが、そういう時に限って責任者が海外出張などで不在の組織があった。

4.1.5 想定する被害と対応

BCPは何も地震に限らないのだが、日本においては必然性、またどの事業部でも関心が高いということで、地震を想定した BCP の構築をおすすめする。実際大企業であれば各部署に業務中断リスクを洗い出せば重複するものも多いと思うが、20の部署が各50ずつあげると1,000個くらいすぐにあがる。個々のリスクについて対応を考えるよりも地震あるいは他の異なる性質のリスクを2、3種類取り出して、まずは一度 BCP をワンサイクル回してみることである。それを他のリスクに水平展開するほうが効率的である。多分、基本的なプロセスはどのリスクでもそう変わらないはずである。

地震について弊社では震度7クラスの東京直下型地震を想定している。だからといって東京23区をはじめ首都圏が壊滅状態といった最悪のケースを想定しているわけではない。4、5区が深刻な被害で残りの区についてはライフラインは混乱しているものの、かろうじて都市機能を保っているといった状態であろうか。あまり最悪のケースを想定し無理な復旧目標を掲げると一企業の BCP ではお手上げとなり、対策も思考停止してしまう。行政府も東京直下型地震については様々な被害想定を行っているが、正直なところ起こってみないと分からない。これだけ様々な機能と人口が密集し都市部の大震災など世界的に見ても、誰も経験したことがないのだ。その意味では我々には阪神淡路大震災や新潟中越地震といった貴重な経験があるのだが、東京とは規模が違い必ずしも教訓がそのまま生かせるわけではない。例えば弊社の例では、阪神淡路大震災の際は通信手段として専用線（内線）が使える重宝したので、その後内線とボイスメッセージ（留守電）機能を組み合わせて NTT の 171 災害ダイヤルのようなものを社内で構築した。しかしこのシステムは東京が被災して社員が数千人規模で使用するとうまくいかない。地方オフィスが数十人、数百人規模で使用するのにはいいのだが、東京が被災した場合の社員の安否確認には使えない。社員の安否確認については、近々弊社では携帯電話や PC からコンピューターサーバーにアクセスして、自分の安否を登録するといった社外の安否確認サービスを利用する予定である。これについては、社内でも通信インフラがダウンしたら使えないのではといった声も上がったが、通信インフラ復旧後は速やかに社員の安否が集計できるメリットがあると判断し、導入を決めた。

また被災対応のパターンとしては、A)顧客のみが被災した場合、B)弊社のみが被災した場合、C)顧客と弊社が被災した場合の大きく3パターンがある。弊社は IT インフラを社会に供給しているので BCP の対象は顧客の IT インフラ復旧も含む。特に C)の場合は自社と顧客の復旧を平行して行うので、リソースの振り分け判断が必要である。場合によっては、自社のインフラ復旧よりも顧客の IT インフラ復旧の方を優先することも十分考えられる。

4.1.6 BCP 以前に平時のリスクマネジメントありき

事業継続、復旧プランというと事が起きてから速やかにリカバリーするというイメージが強いが、STEP3 の Risk Mitigation で触れたように平時のリスク削減が実は重要である。

そもそも事業中断(Business Interruption)が無ければ BCP も必要ないのである。また、事業中断のダメージが少なければ復旧もそれだけ容易になるのだ。平時のリスクマネジメントで人的オペレーションミスによる火災や工場爆発などはかなりの確率で防げるだろうし、地震の発生そのものは防げないにしてもオフィスの耐震対策によってかなり被害は軽減できるだろう。弊社ではほとんどのオフィスを新耐震基準以降建設されたオフィスとし、それ以外のオフィスは耐震工事を行った。新しいオフィスをプランするときはデュー・デリジェンス(Due Diligence)の内容に地震リスク評価も含まれる。デュー・デリジェンスとは、もともとは証券発行時の基準精査を指す用語であるが、最近では不動産価値の詳細かつ多角的な調査（経済、物理的、法的側面）のことを言う場合が多い。弊社の神戸事業所では阪神淡路大震災の際、机上の CRT モニターがほとんど床に転がっていたことから、CRT モニターの固定を全社的に促進している。但し、全社で 5000 台以上あるので都心部のオフィスから順に固定している。たかが CRT モニターでも被災後にすぐに使えるのと新しいものを調達したり、修理をしているのとでは復旧活動に大きな差がでる。また、阪神淡路大震災は早朝でオフィスに誰もいなかったから良かったが、就業中であつたら CRT モニターが社員を直撃して負傷者が多数でいたかもしれない。もちろん CRT モニターに限らず、液晶モニターやプリンターなども固定するにこしたことはないが、CRT モニターは重量が重く危険性が高いということで対応を優先している。いずれにせよ、平時にできるだけリスク削減対策をしたいものである。

4.1.7 BCM の輪を広げよう

BCP はこれまで述べてきたように、他事業部、管理部門との連携が必要である。当然弊社の BCP も危機管理委員会を中心とする全社的なリスクマネジメントのフレームワークの一部として機能している。各事業部の BCP が単独で存在しているわけではない。弊社ではオンラインストアで PC を販売しているが、この業務の災害時対応を例にとると、まず顧客の注文を受けるコールセンターの BCP が必要である。PC を製造する工場の BCP が必要である。顧客へ PC を届ける物流の BCP が必要である。どの BCP が抜けても顧客へ PC を販売するという「業務継続」はできないのである。交通インフラが遮断されていれば、顧客に商品の配送もできない。こうなると一企業の社内的連携やその関係会社だけではなく、社会全体でインフラの復旧が進まないと BCP は完結しないということになる。

BCP も我々の業務が海外からの様々な情報、原料、部品等に頼っている現状をみると一企業、一国の取り組みではなく、大げさなようだが環境問題のように全世界的な取り組みが必要といえる。

最近では企業の格付や投資ファンドの基準に企業の「防災力」を評価しようという動きもある。今後は BCP が何も特別のことではなく、企業経営、それこそ業務の一つとなって普及していくのかもしれない。BCM の輪が広がることによって各企業の BCP も加速していくのである。

4.2 ICT 分野における海外先進事例

本章では ICT（Information and Communication Technology）から見た事業継続管理について海外における調査結果と事例を交えて説明する。

ICT においてカバーする領域は以下の通りとなり、それぞれ BCP/BCM の観点から見た必要な事柄を一覧で示す。（図表 1－1、1－2 色付き（黄色）の部分）

- ・ アウトソーシング
- ・ コンタクトセンター/CRM（Customer Relationship Management）
- ・ IP インフラストラクチャ
- ・ モバイル通信
- ・ デスクトップ管理
- ・ アプリケーション管理とホスティング
- ・ サーバー/プラットフォーム

図表 1－1

分野	1.アウトソーシング	2.コンタクトセンター/CRM	3.IPインフラストラクチャ	4.モバイル通信
対象	・マネージドサービス ・ネットワークアウトソーシング ・ビジネスプロセスアウトソーシング ・IT アウトソーシング	コンタクトセンター コンタクトセンターのセルフ／アウトソース運用 マネージドプロフェッショナルサービス CRMアプリケーション	WAN IPテレフォニー LAN オプティカル SAN	接続性 複合ソリューション
セキュリティ	・セキュリティギャップ分析（BS7799監査） ・ベンダー選定/評価 ・ポリシー、スタンダード、プロセス策定	コンタクトセンターセキュリティアーキテクチャ ポリシー、スタンダード、プロセス	ポリシー、スタンダード、プロセス策定 セキュリティアーキテクチャ セキュアネットワーキング ファイアウォール BS7799監査	ポリシー、スタンダード、プロセス策定 ワイヤレスLANのセキュリティ モバイルセキュリティポリシー リモート通信のセキュリティ
事業継続計画	BCアウトソーシング戦略策定 ベンダー向けRFQ策定 DRベンダー選定 遵守状況の評価	コールセンターリスク評価 コールセンタービジネスインパクト分析 DRプロセスおよび計画 DRテスト BCP監査 金融業界規制の準拠	復旧を前提としたインフラ技術の選択 高可用性、高回復力システムの構築 電話通信の継続	事業継続における俊敏性 モバイルに対するリスク評価

図表 1－2

分野	5.デスクトップ管理	6.アプリケーション管理 およびホスティング	7.サーバプラットフォーム
対象	パッケージソリューション	メッセージング インターネット Eコマース(ビジネスアプリケーション) ホスティング	システムハードウェア、ソフトウェア(OS、ミドルウェア) サーバシステム設計 サーバ実装 サーバシステムアウトソース
セキュリティ	ポリシー、スタンダード、プロセス策定 デスクトップセキュリティ ウイルス対策アーキテクチャ	ポリシー、スタンダード、プロセス策定 ペネトレーションテスト PKI等認証ソリューション セキュアポータルサイトの構築 セキュリティリスク評価 ウイルス対策	ポリシー、スタンダード、プロセス策定 セキュアOSによる強化 ペネトレーションテスト 脆弱性分析 セキュリティペリメタ検査 ネットワークとサーバー間のセキュリティ
事業継続計画	リカバリー要求度合いの決定 バックアップ・リストアプロセス 構築	バックアップ・リストアプロセス バックアップサイト構築 危機管理チームの構築	バックアップ・リストアプロセス バックアップサイト構築 デザスタリカバリプランの策定

業務・事業の活動低下と停止については様々な ICT 応用分野と起こり得る状況を想定し、対処する手段を準備しておく必要がある。

4.2.1 ビジネスアプリケーションのパフォーマンス低下と停止について

まず始めに挙げられるのがビジネスアプリケーションのパフォーマンス低下と停止である。ビジネスアプリケーションの停止は IT コストの増大と場合によっては顧客満足度の低下や競合他社との競争に敗れるといったことを同時に引き起こす。

欧州トップ 2,000 社の IT 部門に対して行った調査結果 (Coleman Parkes research、January 2004) では

IT コストについて：

- アプリケーションパフォーマンスを低下、停止させている根本原因を突き止めるために年間あたり合計 3 百万時間以上を費やしている。(1 社あたり 1,500 時間)
- これは費用に換算すると約 25 千万ユーロ (約 340 億円) に相当。
- 25% の IT マネージャは自社ネットワーク全体がどの様に使用されているかを説明できないことが判明。

時間とリソースについて：

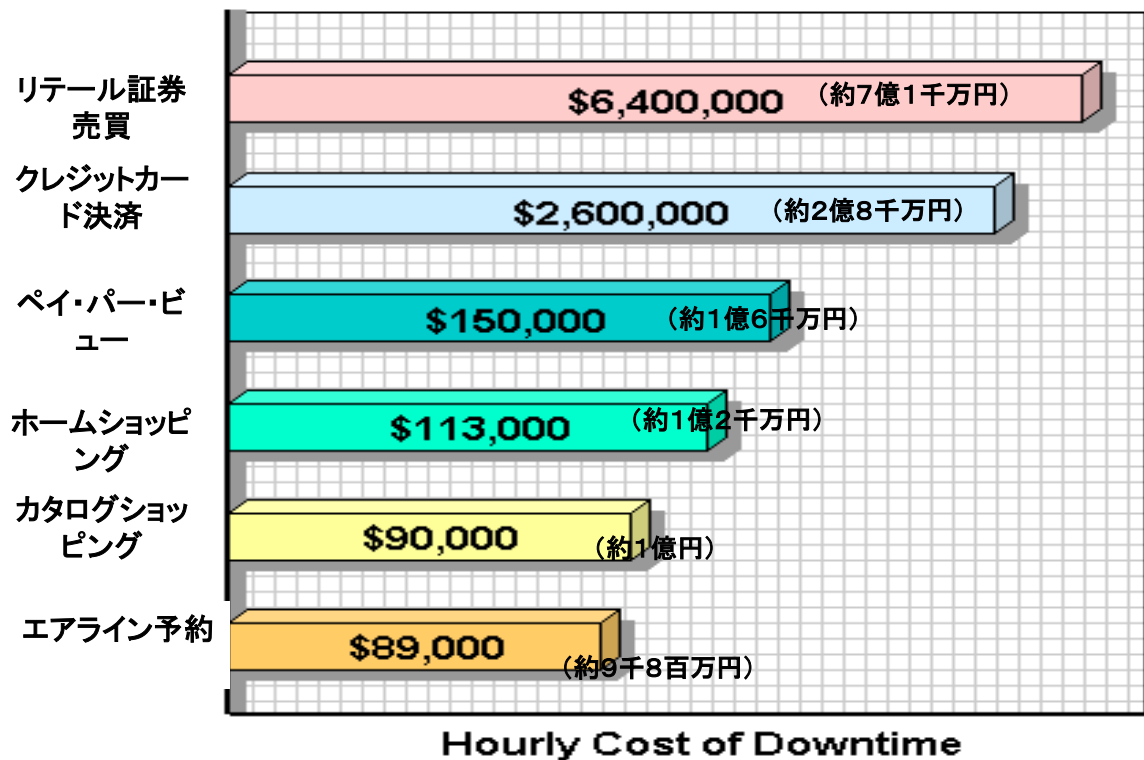
- 50% 以上の IT マネージャが問題の原因究明のためのリソース (お金/人/時間) が不足している。

との回答を得ている。

組織におけるマネージメントと IT 部門が、ミッションクリティカルなビジネスアプリケーションを把握し、継続運用すべきアプリケーションをしっかりと優先順位付けし、問題が発生した場合の原因究明と継続運用手段を準備しておくことがまず始めに必要となってくる。

以下に予想外のダウンタイムが及ぼすコスト（1時間あたり）について参考データを示す。（図表 2）

図表 2



これらのミッションクリティカルビジネスアプリケーションのパフォーマンスを保証し、継続運用するための BT のアプローチについて説明していく。

アプリケーション・アシュアド・インフラストラクチャ（AAI、Applications Assured Infrastructure）

BT のアプリケーション・アシュアド・インフラストラクチャ（AAI）サービスは、クリティカルな判断を行う上で必要な管理情報を生成する。このサービスは、BT の AAI 手法に則した以下の各要素で構成される。

- ・ 顧客のビジネス要求の把握
- ・ アプリケーションの監査
- ・ 主要インフラストラクチャのパフォーマンス監視

- ・ インシデントの調査と管理
- ・ 継続的なパフォーマンスの保証

ビジネスにターゲットを絞ったパフォーマンスの最適化はBTのAAIサービスの根幹をなすものであり、AAIプロセスのどのステージ（図表3）においても効果を発揮することができる。実際のところ、AAIは企業組織に対し、BCM/BCPアプローチはもとより、次のような様々なメリットをもたらす。

- ・ 資産活用の改善
- ・ クリティカルな顧客販売アプリケーションからのROI向上
- ・ 新規IPサービスの確実な展開
- ・ サプライチェーン・マネージメントの改善
- ・ カスタマー・リレーションシップ・マネージメントの強化

AAIから目に見えるメリットを得るための最も重要なステップは、お客様との深いリレーションシップ構築を行うステージです。BTの専門スタッフは、お客様のインフラストラクチャ運営において、アプリケーションのパフォーマンスを改善する上で最も重要となる課題について広範な知識を有しています。BTはお客様のビジネス環境について、さらには現在および将来のニーズを満たすためITがどのように運用されるべきかについて詳細な情報を集めながら、お客様とのバーチャルなチーム関係構築に務める。

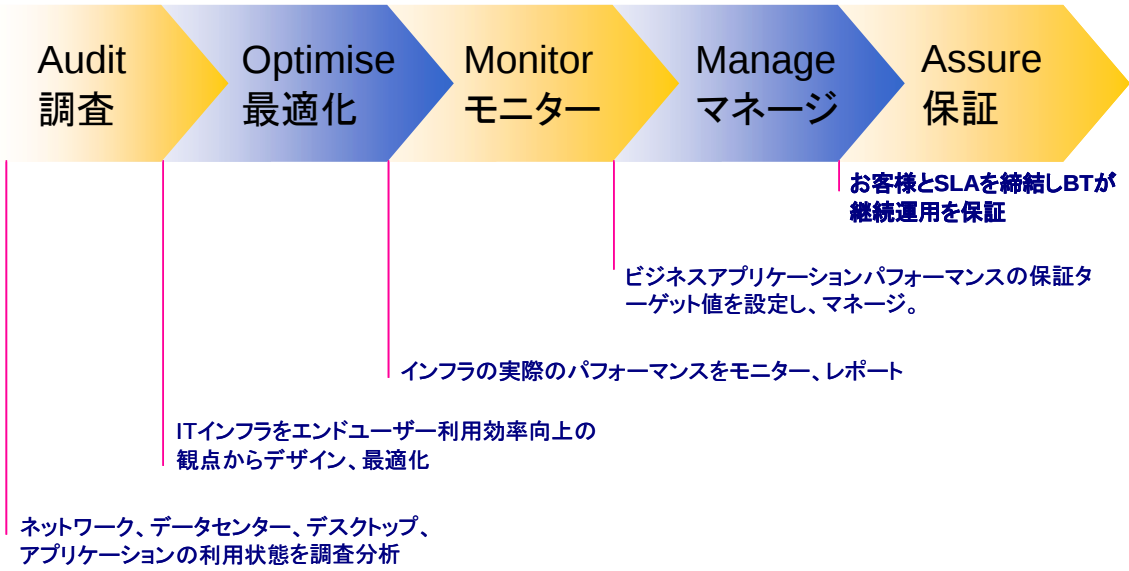
このステージでは、現在のネットワークポロジ、特に興味のあるサイト、IPアドレスの設定スキーム、主要サーバーを調査します。また、ユーザーとホストとの間の主要なリンクがどれであるかを判断し、インフラストラクチャ内にアプリケーションないしネットワーク監視プローブを設置すべき個所についてお客様との協議を行う。

また、迅速かつ効果的なパフォーマンスの改善を実現する上で必要な推奨事項を記載したチェックリストを、サービス提供に先立ってBTが作成する。必要な作業については専任のコンサルタントが担当する。

お客様はここで、AAIサービスのうちどの項目を採用するかを選択できる。AAIは一連の流れとして提供されるのではなく、複数の導入ポイントの何れからでも始めることが可能である。例えばMonitorステージやManageステージから開始されるお客様もいれば、アプリケーションのパフォーマンスに関する具体的な問題に対処するため、Application Troubleshoot 監査から始められるお客様もいる。

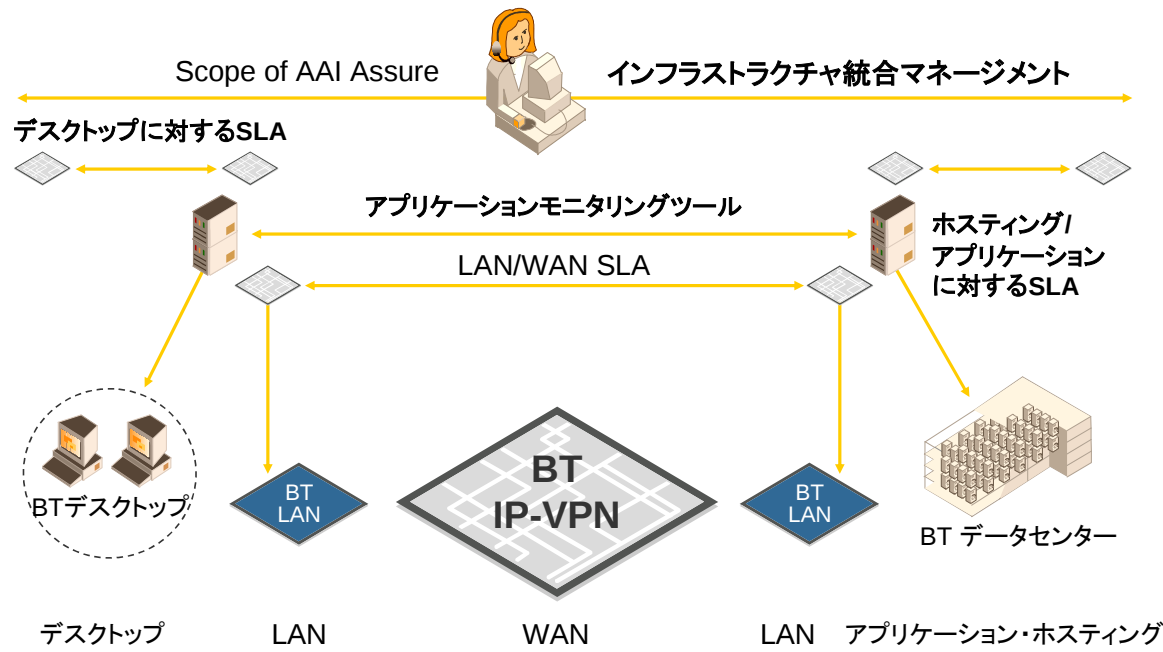
図表 3

アプリケーション・アシュアド・インフラストラクチャ (AAI) AAIポートフォリオ



図表 4

エンド・トゥ・エンドでの運用保証



グローバル大手携帯電話会社事例

このお客様で発生していた問題は、

- イギリス国内 400 店舗のうち最大 60 店舗で POS アプリケーションの停止がランダムに 2 週間以上に渡り発生。
- POS アプリケーションが停止中のビジネスロスを経額で見積ると 1 時間あたり 107,000 ポンド（約 2,140 万円）に相当。

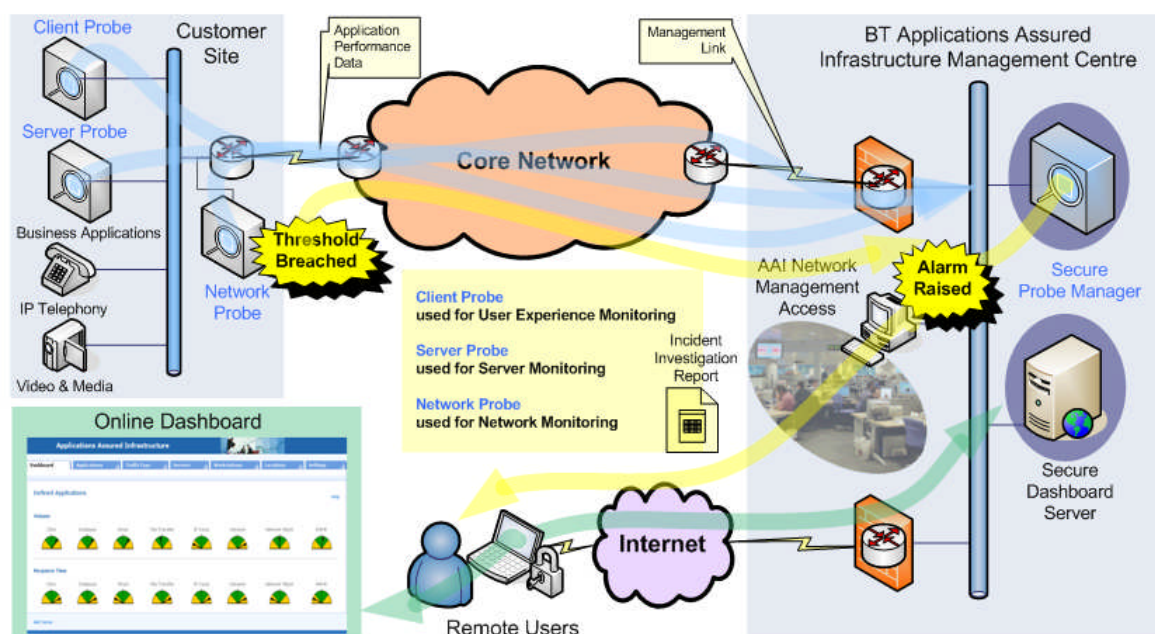
この問題を解決するために BT が提供したソリューションは、

- お客様へ IT インフラ情報収集のためのインタビュー。
- AAI プローブをインフラの主要ポイントに設置。
- お客様 IT インフラの実行パフォーマンスのモニターと分析開始。（図表 5）
- AAI トラブルシュートが 10 分で問題点を発見。
- アンチウイルスソフトウェアアップデートをトレーディングピーク時間外へ設定変更。

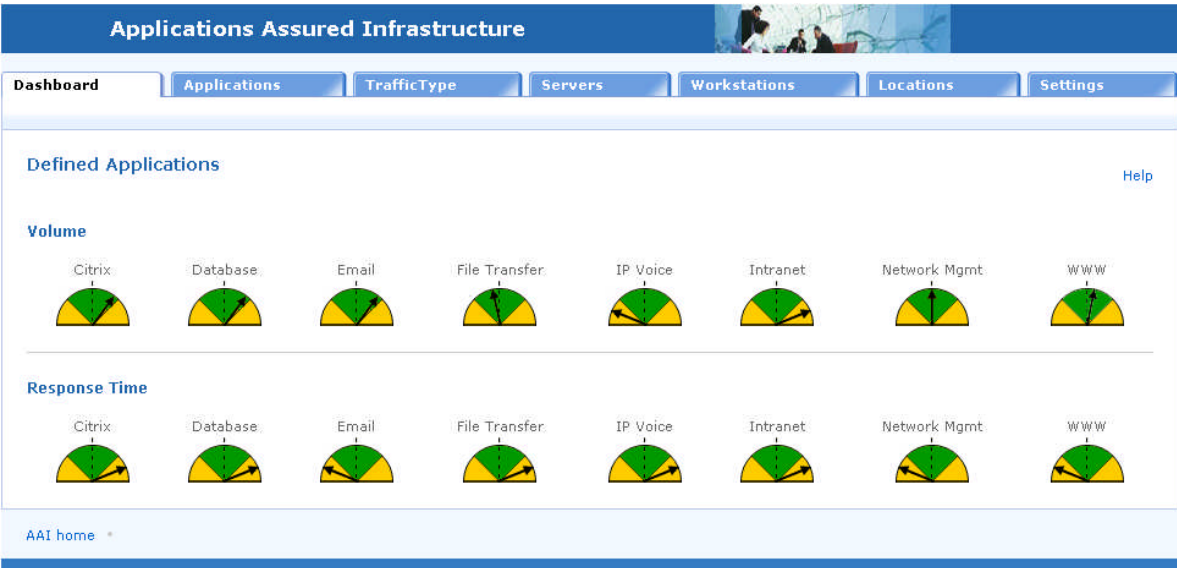
問題の原因はアンチウイルスソフトウェアアップデートによるネットワークトラフィックの増加が、POS アプリケーション応答のタイムアウトを引き起こしていた訳であるが、AAI トラブルシュートサービスの導入後わずか 10 分で原因を突き止め、対処方法としてアンチウイルスソフトウェアアップデートをトレーディングピーク時間外へ設定変更するだけで、重要ビジネスアプリケーションの継続運用が実現できている。

業務・事業の活動低下あるいは停止を防ぐための IT インフラの実態把握、最適化、重要アプリケーションの実行パフォーマンスの確保は、BCM/BCP アプローチの重要ステップであると言える。

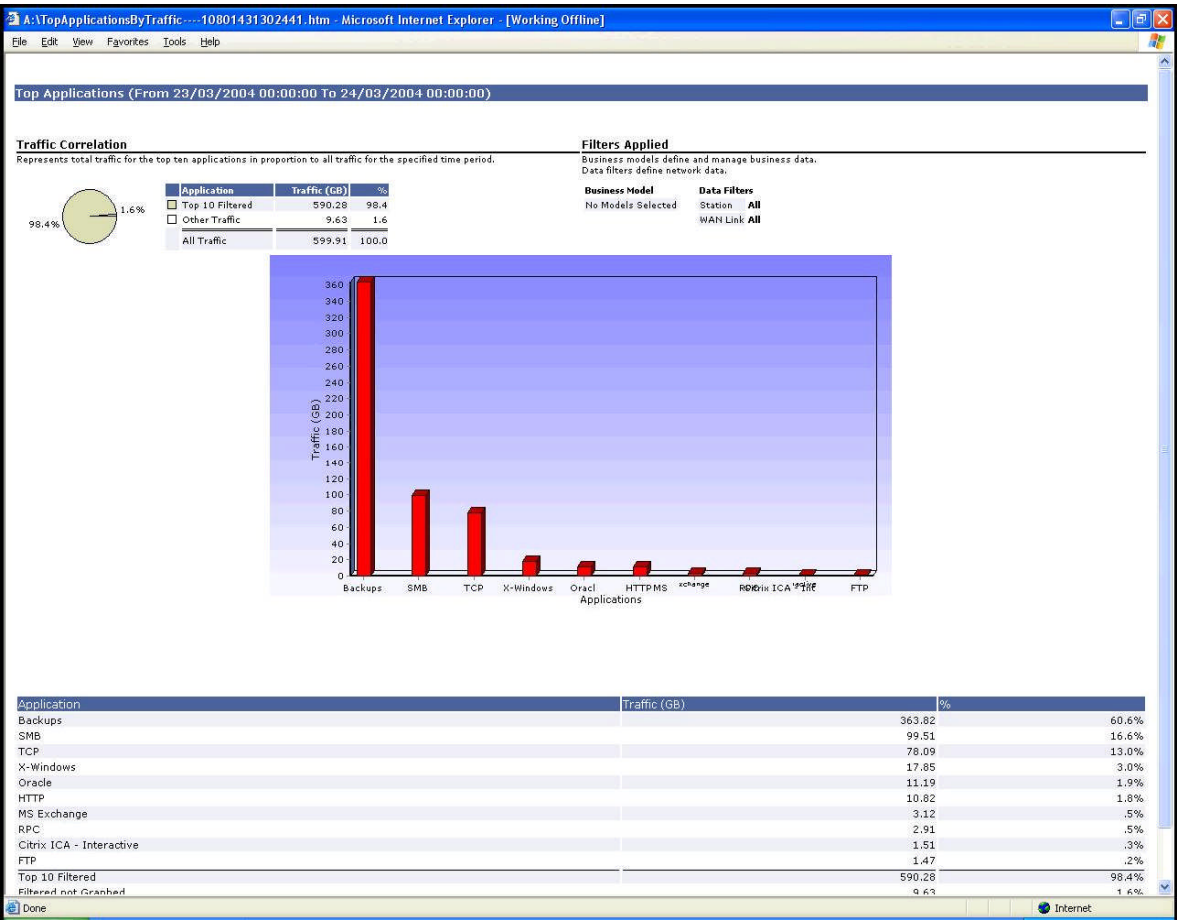
図表 5



図表6：アプリケーションのレスポンスタイムをモニター
ダッシュボード機能



VBC経由でいつでもアクセス可能(<http://vbc.bt.com>)



AAI 導入による以下のような成功例もあわせて記載しておきます。

- ・ **ヨーロッパ大手自動車メーカー – ROI を劇的改善**
クリティカルビジネスアプリケーション ROI を半年間で 40%改善。
- ・ **イギリス大手都市銀行 – IT コストを削減**
IT およびネットワークサービスコストを年間 7M ポンド（約 9 億 8 千万円）削減。
- ・ **大手 IT サービス会社 – IT サービスデリバリ改善**
IT サービスデリバリの改善によって数億円におよぶ顧客への SLA クレジット費用を削減。
- ・ **大手製薬会社 – 次期インフラ構築を最適化**
次期グローバル IP インフラ構築のためのビジョンを明確化。
- ・ **大手携帯電話会社 – カスタマセールスを改善**
時間あたり 10 万 7 千ポンド（約 2 千 140 万円）、月当たり 3 百万ポンド（約 6 億円）失っていたセールスを取り戻す。

4.2.2 事業継続におけるセキュリティの重要性（サイバー脅威から見た BCM/BCP）

事業継続は災害発生時の事業組織および IT オペレーションへの影響を最小限に食い止める対策を講じるのと同時に、プロアクティブに IT 資産を幾つかの特定した脅威から守るためのセキュリティ・ソリューションを導入しておくことにもフォーカスをあてておく必要がある。

以下にセキュリティが影響する幾つかのポイントを挙げる。

- Compliance （準拠）
- Business Continuity （事業継続）
- Reputation （評判）
- Revenue （売り上げ）
- Efficiency （能率、能力）
- Liability （責務、義務）

IT セキュリティ・ソリューションが災害発生時対策と異なることは、故意あるいは計画的に発生する電子的脅威に特化して対策を導入しなければならないところにある。この脅威にはウイルス、Web サイト防御、サービスアタックデニアル（拒絶）などが挙げられる。

セキュリティの実現とは最適なセキュリティポリシーの作成とプロセスの実施、社員全員への意識浸透をファイアウォール、IDS（侵入検知システム）、ID 管理や PKI（公開鍵認証基盤）、アンチウイルス、バイオメトリックス（生体認証）といったベストなセキュリティ製品・サービスと共に実施、配置してプロアクティブな常時警戒を行っていくことである。（図表 8）

図表 8



イギリス大手都市銀行事例ーオンラインバンキングを支えるテクノロジー

オンラインバンキングの登場によって人々の預貯金管理方法が大きく変わろうとしているが、このサービスの普及に鍵を握るのが様々な犯罪に対しての明確な安全性を示すことである。

今回はイギリス大手都市銀行（H 銀行）のケースについて説明する。

H 銀行は預金、貸付においてのイギリスマーケットリーダーで、2002 年の収益はおおよそ 2 ビリオンポンド（日本円で約 4,000 億円）である。

サービスとしてリテールバンキングをはじめファイナンス、インシュランス、コーポレート向けサービス、および株式ディーリングサービスを提供している。

チャレンジ

H 銀行は顧客に対してオンラインバンキングサービスの提供をしたいと考えていたが、セキュアでかつ高信頼 e コマースプラットフォームの構築が必要不可欠と考え、非常に慎重に検討を重ねていた。何故なら 1 度でも犯罪が起きればそれは即、企業ブランドと評判の失墜に繋がるためである。

H 銀行はマーケットに対する新チャネルを開くために、セキュアソリューションのデザインと導入を BCI のメンバーである英国最大のグローバル通信会社 BT に相談した。

ソリューション

マルチサイトに渡る大企業向けサービスを提供する BT グローバルサービスと複数の BT ファイアウォールスペシャリストによるプロジェクトチームを立ち上げた。

提供するファイアウォールサービスは、もっとも厳しいと言われているブリティッシュ品質ス

タンダードの監査を受けたサービスを用意した。

さらに政府、学術、商業の各関係部門との連携により組織される FIRST（Forum of Incident Response and Security Teams）のサイバー犯罪に関する最新情報を常に活用し、よりセキュリティレベルを高めた。

また同時に悪意ある侵入、アタックに対する証拠、根拠およびプロテクション、リカバリー対策を 24 時間 365 日提供した。

このシステムが十分機能することを確認した H 銀行は、顧客へ提供中のその他のサービス用 e コマースプラットフォーム群への応用、幾つかの開発中テストサイトのプロテクト用、そして新しいサービスのトライアル用として、このファイアウォールシステムの導入を中核に据えることを決定した。

オンラインバンキングのみならず、その他のサービス、例えば顧客企業の持ち株サービスと言ったオンラインサービスをセキュア、エンド・トゥ・エンド、暗号化されたパブリックアクセスで提供するのが狙いであるのは言うまでもない。

すべてのアクセスに関するリアルタイムパフォーマンスの統計データ、ログ、タイムスタンプ等のレポートも準備され、アクセスログは十分にセキュリティ管理された場所に保管される。

またこのソリューションは、単体のシステムではなく 2 箇所のデータセンターに導入、完全に二重化され、耐障害性、業務継続性が最大限に強化されている。

4.2.3 ディザスター — BCP/DRP 導入とチャレンジ

火災、水害、地震といったディザスターの状況下では企業の事業所、場合によっては企業全体の事業組織活動および IT オペレーションの低下あるいは停止を引き起こす。

この状態では、企業のマネージメントと直接リンクし、あらかじめ組織された危機管理チーム（CMT）のリードと意思決定フレームワークが準備され、リカバリー計画による影響の最小化と復旧が実行される。

BCP/DRP を推進していく上で次の事柄を事実として認めておく必要がある。

- 従来型ディザスターリカバリでは十分に機能しない。
- 過去発生した業務停止の教訓が十分生かされていない。
- 様々な規定と企業統治の必要性の認識増加。
- ステークホルダーとビジネスパートナーは、より確実な BC（業務継続）とその責任が要求される。
- ビジネスの複雑化
 - B2B、エキストラネット（企業間ネットワーク接続）、新流通構造など

また確実性の低下を引き起こしている BC/DR プロセスを刷新して、ROI の明確性を高めていく必要がある。従来型 BC/DR プロセスが不確実である理由は、

- ビジネスに対する様々なインパクトが評価されていない。
 - 不十分なビジネスインパクト分析と狭い範囲のみでのリスク分析

- リカバリとテストの優先順位付けの理解不足
- ビジネス関連サプライヤ、サービスプロバイダに対するリスクと信頼性評価不足
- 従来型 BC/DR では非常に狭いビジネス範囲でしか対応できない。
 - IT 部門の制限されたオーナーシップとマネージメント
 - 部門を跨ったプロセス/インターフェース/リスク評価の不足
 - 災害/事故発生後のデータとシステムの受動的リカバリ
- 厳密に定義された BC/DR プロセスが反映されていない。
 - 災害時の役割と責任が不明確
 - IT や組織変更に伴ったプロセスの見直し、メンテナンスがなされていない
 - 危機管理チームのシナリオトレーニング不足
 - DR プランのテスト不足が能力改善を妨げる
 - 各拠点におけるアプローチ/方法論の一貫性が保たれていない

BCM・BCP を行うために必要な準備（プロジェクト）を次に示す。（図表 9）

図表 9

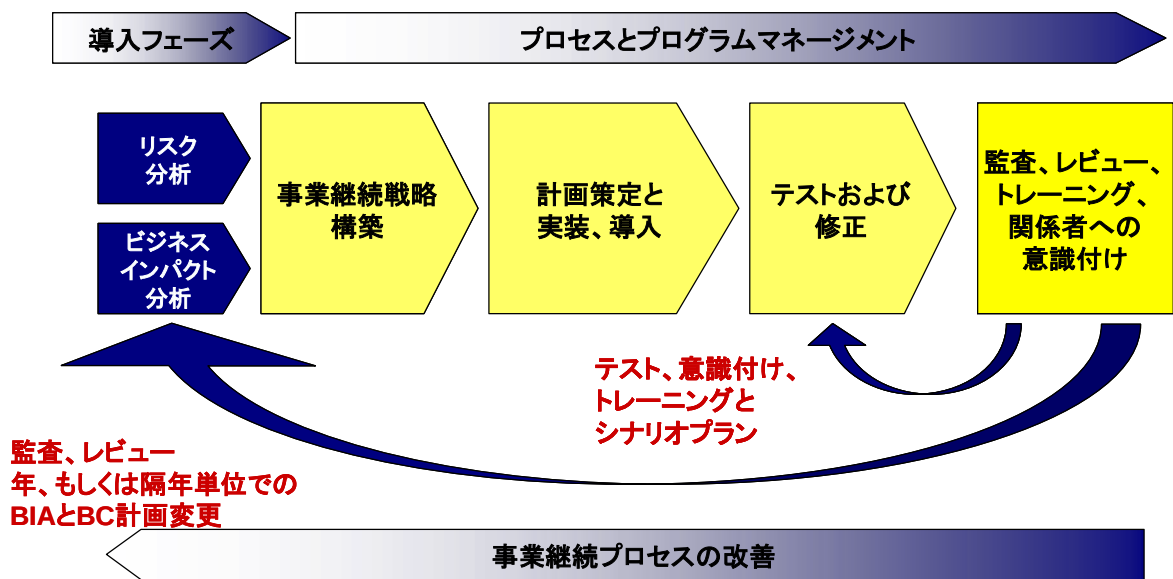


BCM・BCP の策定フローを図に示す。（図表 10、11）

策定プロセスにおける詳述は省くが次の要素を盛り込む。

ビジネスドライバ、障害レッスン、重要顧客、導入実績、企業ガバナンス、規制、ガイドライン（FSA、Basel など）、国際スタンダード（BS7799/BS15000 など）、業界のベストプラクティス（DR Institutes、BCI、BT、Survive など）。

図表 1 0



図表 1 1

BCP/DRP 構築までの流れを一覧で示す。

フェーズ	項目	概要	主な成果物
0	プロジェクトスコープの策定	対象となるビジネス領域とプロジェクト範囲の特定	
1	リスクアセスメント ビジネスインパクト分析	組織のミッションと、ビジネス上の最も重要な機能を特定する － 情報資産の重要性評価/リスク評価 － ビジネスへの影響度評価 － リカバリー計画作成対象の決定	リスク評価報告書 対策優先順位
2	復旧プロセスの構築	障害発生時の対応計画の構築 障害対策組織/連絡体制の構築 復旧許容時間の評価 災害復旧対策案の立案	復旧プロセスチャート 緊急対策体制 災害復旧対策案
3	テスト	テストシナリオの作成 テストの実施	テストシナリオ テスト結果報告書
4	アウェアネスの向上	従業員の認知の向上と復旧プロセスの指導	担当者別対策実施票

ヨーロッパ最大医療サービス会社事例 — BCP/DRP 構築、導入

イギリスの医療サービス会社への導入事例について説明する。このサービス組織は国家レベルで医療、健康に関する様々なアドバイスサポートを提供しており、利用者からの問い合わせに対応するためのコンタクトセンターが 24 時間 365 日運用されている。

いつでも問い合わせに対応し、且つ的確なサービスを継続して提供できることが利用者のために最も重要である。

BCP/DRP 導入にあたっての背景とチャレンジ、BT への要求事項および問題点を以下箇条書きにする。

背景とチャレンジ。

- 電話、Web、E メールといったマルチチャネルコンタクトセンターにおける先端テクノロジーと新データモデル。これに対応するスタッフ強化とナショナルレベルの新プロセスの必要性。
- 業務停止は（潜在的に）生命に危険を及ぼす。
- 限られたリソースと時間の中での手順作成。
- 効果的で且つテストされた DRP – 業務継続のための“Go / No Go”判断の有効性の証明。

導入をサポートした BT への要求事項。

- 業務継続の保証。
 - 非常に限られた範囲内のサービスレベルの低下だけであることを保障して欲しい。
- コンタクトセンター、ナショナル・エグゼクティブ・マネジメントチーム、それとサードパーティにより提供される IT インフラのために安全で受容できるレベルに復帰させる明確なステップシーケンスを提供して欲しい。
 - 障害発生時のリカバリーサイトへの移転方法。
 - インバウンドコールのコールマネジメントプロセスを用いた複数コンタクトセンターへの転送と対応オプション。
- 役割と責任の明確化。
 - コンタクトセンターレベル（ローカル危機管理（CMT）チーム）とナショナルマネジメントレベル（ナショナルレベル危機管理チーム）の両方において必要とされる役割と責任の明確な理解（Understanding）を提供して欲しい。（実際には意思決定、ローカルレベルからナショナルレベルのインシデントマネジメントへのエスカレーション基準と情報のやり取りの責任についてのガイダンスが必要とされました。）
- BC/DR に必要とされるメンバーが内部、外部を問わず常に状況を連絡、把握できるように保証して欲しい。

医療サービス会社側問題点。

- ウェスト（西）コンタクトセンターの稼動までに2ヶ月半しか時間が残されていない。
- 運用開始準備のため、医療サービスとそのコンタクトセンターのキーとなるメンバーの BC/DR プロジェクト参加時間が非常に限定されていた。
- 稼動直前になって関係組織の規模が当初予定の3倍に増大していた。

BT コンサルティングチームは過去実施したノース（北）コンタクトセンター構築およびその DR をテストしていた経験から医療サービス会社の目的を理解し、高い適応能力で目的達成を約束した。

ここで BT のとったアプローチについて説明していく。

まず先に述べた策定のための方法論（策定フロー図表10、11）と独自のテンプレート、テストツールを採用して、戦略的 DR プロセスを作成する。これには関係者に無理のないプロセス

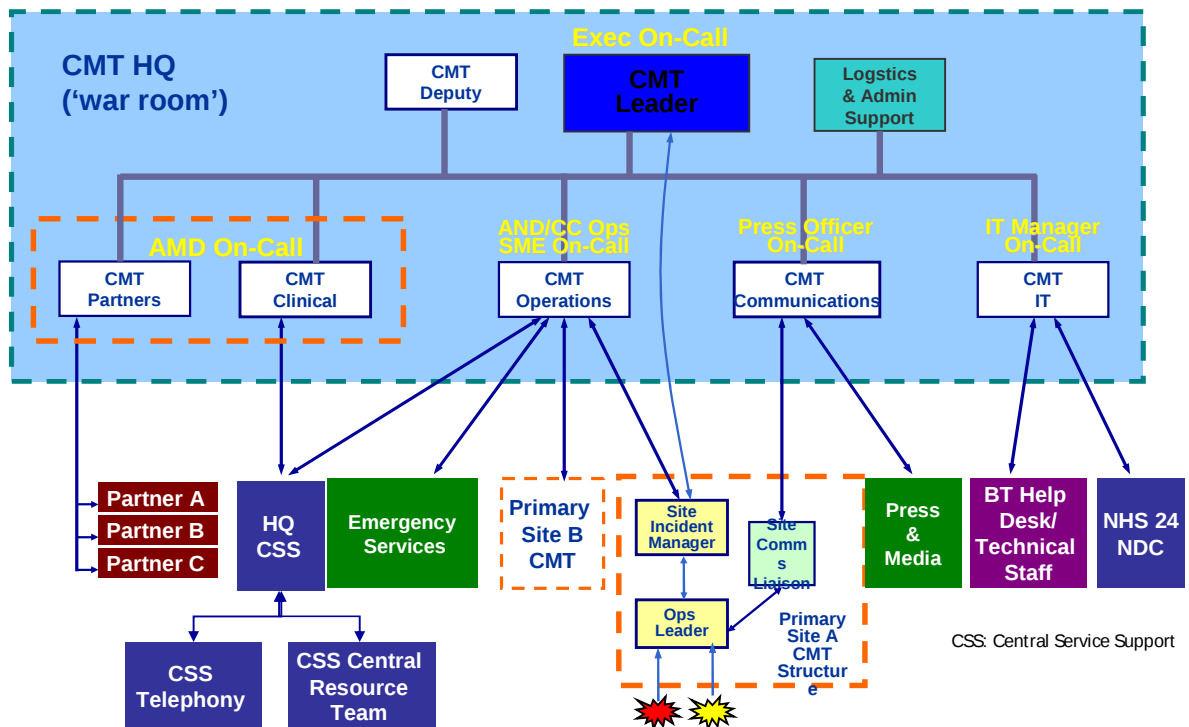
テップ作成と意思決定マネージメントが含まれる。

ワークショップと 1-to-1 ミーティングを開催して

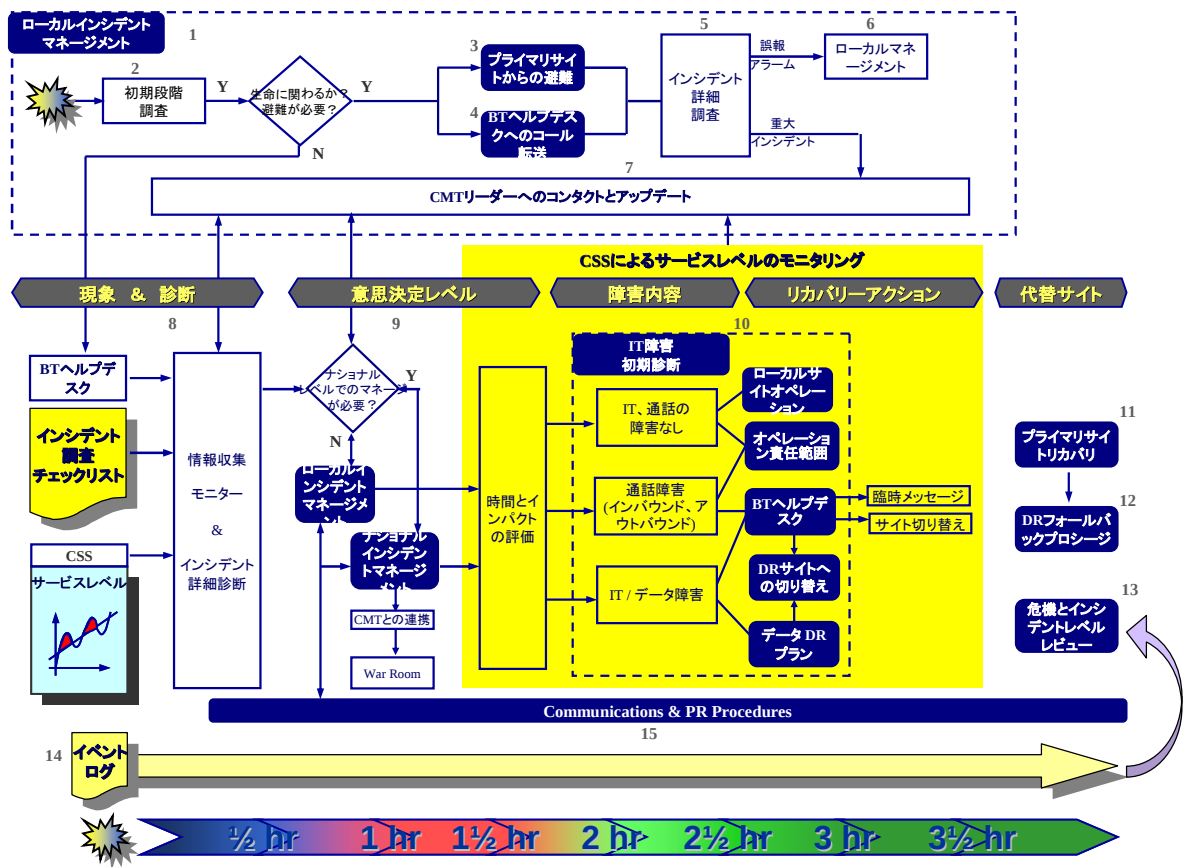
- フローチャートとプロセス全般作成
- キーとなる意思決定ポイントと判断基準の抽出
- 技術、プロセス等に関わるサードパーティベンダーのコーディネーション
- サードパーティのレビューと品質/採用基準（Gate）の作成
- 危機管理チーム（CMT）ストラクチャの作成と立ち上げ（図表 1 2）
- DRP 実行時のポイントを一覧化した Q カードの作成

を行い 3 時間半でリカバリーを実現するための DRP を作成した。（図表 1 3）

図表 1 2



図表 1 3 - ハイレベル DR プラン



各関係者の連絡窓口、予定指示、関係者間のインターフェースのためのプロジェクトオフィスを設置してプロジェクトをプラン通りに進行させた。

導入・運営に先立って、出来上がった DR プロシージャは様々なシナリオの基づくテストが実施され、レビューされる。

- 役割認識訓練（カードエクササイズ）・プロセス確認+指揮、コントロール
- 実訓練（リアルシミュレーテッドエクササイズ）・定義付け、セットアップとコーディネーション
- テスト結果のレビューと報告

まとめとして DRP プロシージャ実行時のポイントを挙げておく。

- CMT（危機管理チーム）リーダーはチームの各メンバーとの連絡に加えてインシデント（事故）発生からの経過時間とプロセス進行・意思決定ポイントのタイムフレーム双方を管理しなければならない。
- すべてのイベント、意思決定が行われた際に、インシデント対応ログを更新すること。また可能な限りの関連情報（意思決定の判断基準、結果を含む）をログに残すこと。また CMT リーダーはステータスボードの更新も行うこと。
- インシデントに関する新たな情報を得た時点でインシデント管理チェックリストを更新すること。これはチームメンバー全員で更新、情報共有が行われること。

- CMT リーダーと広報責任者は常に連絡を取り合い、社内外に対して適切かつタイムリーなコミュニケーションを行うこと。
- 手動的な手順で修復を行う場合は、臨時的に安全が確認されていることの承認をとること。同時に安全に修復可能な時間を報告すること。
- あらかじめ用意された複数の IT リカバリーシナリオ（データ・ディザスタ・リカバリープラン）が常に導入可能となっていること。

最後に BT 社の概要を紹介する。

社 名	British Telecommunications plc.
会 長	Sir Christopher Bland（サー・クリストファー・ブランド）
CEO	Ben Verwaayen
本 社	81 Newgate Street, London, United Kingdom
設 立	1896 年
民営化	1984 年
従業員数	約 99,900 名（2004 年 3 月現在）
売上高	186 億 2,300 万ポンド（2004 年度）
	前年度より 税引前利益 4% 上昇
	一株あたり利益 7% 上昇
事業活動	市内通信、長距離通信、国際通信、移動通信、インターネット・サービス、IT ソリューションなど。 国際直通電話サービスは 230 を超える国々や地域を結び、全世界の 99%を網羅。

5. 第5章 世界の今後の方向

5.1 世界の動き

欧米では多くの企業が BCM の重要性を認識して取組みを進めている。BCI の設立もその延長線上にあり、BCI は BCM の重要性を世界的に強く訴えている。BCI は、以下を目的に設立された BCM を専門とする NPO である。

- BCMの普及・啓発
- BCMの専門化の育成・支援
- BCMに関するガイドラインの作成

BCI は 2002 年に BCM に関する「Good Practice Guidelines（実践的な指針）」を策定した。これをもとに英国規格協会（BSI）は PAS56（一般仕様書）として発行した。これらは、フランスやドイツで翻訳され出版されている。BCI では、上記ガイドライン（実践的な指針）を企業や官公庁にとって使い易いものとするため、企業・官公庁を中心にガイドラインを約 3 年間使ってもらい、その意見をフィードバックさせた。そのフィードバックさせた内容が、2005 年 2 月に発行されたガイドラインとなる。そして、BSI と BCI は共同で 2006 年初頭に新たな PAS56 発行させ、これを国家規格とすることで各種委員会が動き出したことを正式に発表した。また、法規制面では、同じ英国で 2005 年 1 1 月に「Civil Contingencies Act」が施行された。これは、BCM を観点として、中央行政と地方行政との関係、特に地方行政がいかに国民にサービス・業務の提供を図っていくかという内容である。

一方米国では、米国防火協会（NFPA）が、2004 年に BCP に関するガイドラインを発行し、BCM の普及啓発に努めている。

アジアに目を向けてみると、日本よりも BCM の規格化・標準化の動きが活発化している。特にシンガポールでは、2005 年 4 月にウィーンで開催された ISO 会議において、ICT 災害復旧サービス(Information and communications technology disaster recovery services)のガイドラインに関する国際規格の新規業務計画(NWIP)の提案を行った。これは、災害などのリスクにあらかじめ備えて事業継続を図るためのシステムを提供するサービスに関する規格である。また香港、マレーシアでもガイドライン化が進められている。

5.2 日本の動き

これら活発化している海外の動きに対して、日本では、経済産業省が 2005 年 3 月に「事業継続策定ガイドライン」を発表した。また、政府・中央防災会議の「民間と市場の力を活かした防災力向上に関する専門委員会」の中で「企業評価・業務継続ワーキンググループ」を設置し、2005 年 8 月に事業継続ガイドラインを発表した。そして中小企業庁でも、BCP に関する委員会が設置し、2006 年 2 月に中堅・中小企業を対象とした BCM 構築の指針を発表した。日本政府・官公庁では日本の全規産業に BCM に取組んでもらう環境・インフラ作りにつとめている。金融機関においては、日本銀行が 2003 年 7 月に民間金融機関を対象にして「金融機関における業務継続体

制の整備」についての報告書を取りまとめている。これは民間金融機関にも業務継続体制を整えるよう求める内容である。さらに先に述べたように、日本規格協会でも 2004 年 6 月に「事業継続管理のための指針」と題して、PAS56 を翻訳・発行し、日本で初めて BCM に関するガイドラインを発行した。同協会では、日本での普及・啓発活動を推進している。

このように日本では、BCM に関するガイドラインが政府・官公庁を中心に発行されるなど、今後日本で BCM に関する動きがさらに活発化してくると思われる。

<参考：日本の政府・官公庁等におけるBCM関係委員会>

機 関	委員会等
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 事業継続計画策定ガイドライン ワーキンググループ
経済産業省	BCP国際標準化委員会
中小企業庁	BCP有識者会議
内閣府中央防災会議	民間と市場の力を活かした防災力向上に関する専門調査会 企業評価・業務継続ワーキンググループ
内閣府中央防災会議	企業等の事業継続・防災評価検討委員会
(財)情報処理相互運用技術協会	高可用性システム技術委員会（旧ビジネス継続性技術委員会）
(財)日本情報処理開発協会	マネジメントシステム評価検討委員会 情報セキュリティ部会

5.3 ISO の動き

さて、国際標準（ISO）化に目を向ける。

国際標準化機構では、企業や自治体などの緊急時対応（Emergency Preparedness）について、国際標準化されることが決定し、2006 年 4 月に米国で第一回の国際会議が開催される。同会議への参加国は、米国主催で、イスラエル、南アフリカ、フランス、カナダ、オーストリア、オランダ、ドイツ、ノルウェー、日本、そして英国が参加する予定である。

通常の手続きであれば、2008 年夏ごろに規格化されることになるが、実際の制定時期は現段階では未定である。

これに対して、日本では、経済産業省で BCP 国際標準化委員会が設置され、日本案が作成された。日本原案の作成経緯・目的、主な論点は以下の通りである。（以下は日本規格協会の URL から引用）

(1)提案文書の作成経緯

緊急事態対応・事業継続計画の標準化に関する ISO（国際標準化機構）の国際ワークショップが 2006 年 4 月 24 日から 26 日にイタリアで開催されるため、(財)日本規格協会内に設置された事業継続計画（BCP: Business Continuity Planning）作業グループでは、この国際ワークショップへ向けた対応の検討を行って参りました。そこで日本は、各国の事情も踏まえた上で日本のリスクマネジメント、緊急事態対応、災害復旧対応、事業継続管理などに対する考え方

等を尊重しつつ、緊急事態対応・事業継続計画の国際標準化を進めるべきとし、2005年3月に公表された 経済産業省「事業継続計画策定ガイドライン」（PDF形式）や同年8月に公表された 中央防災会議専門調査会（内閣府）「事業継続ガイドライン 第一版」（PDF形式）等をベースとして緊急事態対応・事業継続計画の国際標準化に向けた（1）趣意書（案）及び（2）具体的な標準（規格）の骨子（案）、の日本提案文書（案）を作成いたしました。

（2）提出文書の掲載目的

今後、ISOにおいて緊急事態対応・事業継続計画の標準化に関する議論の活発化に伴い、国内の組織・企業における緊急事態対応・事業継続計画策定への関心が高まることが予想されます。事業継続計画作業グループ事務局では、緊急時対応・事業継続計画に関するISOの動向等の重要性を認識し、情報の掲載を行うことと致しました。

（3）提出文書の概要

①趣意書（案）の提案概要

- 継続的な改善を行う仕組みを取り入れた規格とすること。規格には、第三者による認証制度を採用しない。
- 災害発生直後における、公的組織（警察、消防、自衛隊等）が第一義的に担う災害救助や社会インフラの復旧などの活動の業務の事業継続計画(緊急時対応)を策定することを主眼とした規格としない。
- 対象とするリスクは、各組織が認識したリスクや事業形態を十分に踏まえて、各組織が合理的な基準に基づき自主的に選択できるものとする。
- 広域災害においては、被災した地域の復旧計画との連携・調整に留意し、個別組織が、可能な範囲で地域に貢献することは推奨される。同様に、サプライチェーンを構成する取引先と人的・物的面で相互に支援することも推奨される。このような地域貢献に留意することを明記すること。

②標準（規格）の骨子（案）の目次

- 目的及び適用範囲
- 引用規格
 - 用語定義
 - 事業継続方針
 - 事業継続プログラムの課題
 - リスク分析と影響度分析（BIA）
 - 事業継続計画書の策定
 - 教育、点検及び見直し
 - リスクが顕在化したときの事業継続計画の発動

(4) 今後の動向

2006年4月

イタリア 緊急事態対応・事業継続計画に関するISOの国際ワークショップ

IWA（国際ワークショップ協定）の配付物の作成

2006年5月

スウェーデン TC223（Civil Defense）の第1回総会

TC223の下部委員会において緊急事態対応・事業継続計画に関する検討が行われる予定。（TC：技術委員会）

(5) 参考規格・指針情報

経済産業省の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の報告書で示された「事業継続計画策定ガイドライン」（PDF形式）

中央防災会議専門調査会（内閣府）「事業継続ガイドライン 第一版」（PDF形式）

JIS Q 2001（リスクマネジメントシステム構築のための指針）

PAS 56（Guide to Business Continuity Management）

NFPA 1600（Standard on Disaster/Emergency Management and Business Continuity Programs）

AS/NZS 4360（リスクマネジメント）

上記のように、世界各国で BCM のガイドラインが発行され、そして国際標準化へ議論が世界的に展開されている。一方で、既述の通り、BCM は、企業間取引の条件への変貌を遂げ、そして他社との差別化など能動的な経営戦略としての色彩が強くなってきている。企業は、BCM の専門家を育て、自身を災害・事故・事件などに強い企業に育てていくことが重要である。そのためには、企業はより一層戦略的に BCM を捉え、経営・従業員双方を観点とした BCM 企業文化の構築が求めることが必要であり、それが引いては、企業価値を大きく左右することになる。

附録 情報セキュリティ総合的普及啓発シンポジウムに

おける講演内容

1. 情報セキュリティ専門部会の目的

国内外のBCMのガイドラインに関する調査を行なう。日本では経産省・内閣府・中小企業庁からBCMに関するガイドラインが発行されている。一方、海外では、カナダ、オーストラリア、米国、イギリス、シンガポールなどの調査を行ない、「ガイドの利用ガイド」を策定する。本章では、平成18年2月1日～2日に開催されたシンポジウムにおける、情報セキュリティ専門部会の講演内容を紹介する。

■シンポジウム実施概要

- ① タイトル
ー情報セキュリティ総合的普及啓発シンポジウム
- ② 主催
ー財団法人日本情報処理開発協会
- ③ 後援（順不同）
ーNPO 日本ネットワークセキュリティ協会（JNSA）
ーNPO 日本セキュリティ監査協会（JASA）
ー社団法人電子情報技術産業協会（JEITA）
ー独立行政法人情報処理推進機構（IPA）
ー日本セキュリティ・マネジメント学会（JSSM）
ー財団法人インターネット協会（IA-japan）
ーJapan Security Operation Center(JSOC)
ーBCI 日本支部
ー情報ネットワーク法学会（IN-Law）
- ④ 開催日時
ー1日目：2006年2月1日（水）9時30分～17時00分
ー2日目：2006年2月2日（木）9時30分～17時00分
- ⑤ 会場
ー大手町 JA ホール
東京都千代田区大手町 1-8-3
- ⑥ 申込者数
550 人
- ⑦ 参加者数
479 名

2. BCMに関する事例・リスク

内閣府中央防災会議が首都圏直下地震の被害シミュレーションを行った結果では、倒壊・類焼などの被害想定が発表されている。新宿あたりで地震が発生すると最大で1万2,000人ぐらいの死傷者が発生し、これは阪神淡路大震災の2倍の規模となる。

損害額は、直接損害 67 兆円。これは建物、ライフライン、交通施設などの直接的損害額。一方、間接被害はうべかりし利益であるが、47 兆円となり合計で 112 兆円の規模にのぼる。国家予算の規模が 70 兆円程度と言われているので、これをはるかに上回る災害が東京だけで発生をしてしまうことになる。派生する影響によって、全世界の経済にも大きなインパクトを与える結果に結び付いていくことを容易に想像でき、日本の産業として対応策を検討していかなければならない状況と考える。こういった日本では、地震リスクに加えて、IT への依存が大きく高まっている状況にある。

一方、世界の事例を挙げると、イギリス・アメリカなど欧米ではテロリスクも高い。アメリカではハリケーンが来襲し、自然災害対策自体への対策が見直されているものの、テロについては引き続き関心が高いのは事実である。2005 年の 7 月 7 日には、ロンドン市内で爆発が地下鉄で 3 カ所、そしてバス内で 1 カ所、合計 4 カ所のテロが発生したという事件であるが、50 名以上の死者が不幸にも発生した。

市民は比較的冷静に対応したと言われているが、BCM に関する企業の対応はどうだったか。BCI が調査した結果によると、基礎的な初動という緊急時対応時の情報源としては、テレビとホームページが中心で、中でも BBC だとか、ニュース系のホームページを中心に情報収集ができたことが浮かび上がった。BCM の範疇である、初動、安否確認などは、訓練・シミュレーションをしっかりと行なっていなかったのが、現実的ではなかったと一つの結論が出ている。現実的な迫力あるシナリオに即した訓練の必要性・重要性を改めて認識させられた事件だった。

BCM の観点に絞ると、例えばスイス系の銀行、こちらが爆発地点の駅から近いオフィスでトレーディング業務を行なっていたが、同部門を実際に別サイトに移して業務を継続したという事例があった。また、債券等の精算業務を行うクリアリング・ハウスでは、当日午前中、業務を停止して、別の場所で業務を再開した。その他いくつかの金融機関、証券会社でも、同様にロンドン郊外の場所に移して業務を継続した。

地震、IT リスク、そしてテロなどの実例を説明したが、実際には災害・事件・事故は防げない。海外では当たり前の考え方であるが、日本では過去「安全はただ」と考えられた時代もあったが、状況が大きく変わってきている。昨年の日本経済新聞の調査によると、テロへの関心も非常に高い。そういう意味でも、IT 社会を標榜している事故前提社会がまさに今日本に到来しているのではないかと考えている。そういう環境下で、世界各国では BCM に関するガイドラインが策定されている。

3. BCMについて

BCM に関係する言葉を先ず2つ定義する。BCP（Business Continuity Plan）は、実際に災

害、事件・事故が発生した際に、経営層、会社対策本部、従業員が時系列的にどのような行動を取ればいいのかを示す計画（プラン）そのものである。2つめは、BCM（Business Continuity Management）であるが、「事業継続管理」、若しくは「事業継続経営」と訳される。なぜ、「経営」と言われるかは、「BCM、管理という次元ではなく、経営そのもの、経営マター」考える経営者が増えていることによる。BCM は、経営を巻き込んでマネジメントシステムとして展開していかなければいけないという意味を込めて、事業継続経営と言われる理由の一つである。

現在、BCM は取引先の選別基準に活用されている。例えば同じ製品、サービスを提供している会社が2社あり、BCM を構築している企業と、していない企業の2つあった場合、どちらが選択されるかは明白。供給責任、リスク管理の観点で、取引先が選別されるようになってきている。

サプライチェーンは、全世界で緻密化、発展化している。例えば四国で発生した事故・事故がブラジルの会社の操業にまで影響を与えてしまうと事例も過去あった。海外ではBCM を取引先選別基準として活用されてきているが、日本でも同様な状況になってきた。例えば、企業にも取引先から監査と題して、分厚い資料が送られてきて「BCP 策定しているか」と確認を求められるケースが出てきた。日本であれば「地震に対して事業継続に関する対策を行っていますか」と聞かれることがある。会社によっては他社との差別化という戦略面でBCM を活用していることもある。

一方、今述べたビジネス面の観点に加えて、国際標準化、各国でガイドライン化という状況がある。ビジネス面、規制面、そして自社を守るという危機管理、これらの観点で今 BCM が大きくクローズアップされている。

4. BCM のガイドライン

先ほど述べた通り、世界各国で多くの BCM に関するガイドラインが発行されている。

もう少しまとめてみよう。主要なガイドラインでいうと、BCI のガイドライン、PAS 56、シンガポール、米国、日本などでガイドラインが作成されている。BCI は、「Business Continuity Institute」の略で「事業継続協会」と訳される。BCM 領域では世界最大の NPO 法人である。BCI はイギリスに拠点があり、BCM の普及啓発活動を全世界をベースに展開している。そして、BCM に関するガイドラインの策定、BCM に関する専門家の育成支援を行っている団体である。PAS 56 は英国規格協会から発行され、内容は全て BCI のガイドラインをベースに作成されている。PAS 56 は英国国家規格の前段階を意味する。

BCM 領域で、アジアで BCM が一番進んでいるのはシンガポールである。ここでいうシンガポールには規格が二つあるが、一つは、実際に BCM に関する事業を提供しているサービスプロバイダーに対する規格で、もう一つは BCM を実際に構築しようとする企業に対する規格である。後者は Technical Reference として、シンガポール規格協会によって、2005 年夏にリリースされた。アメリカでは NFPA といって、防災を観点とした BCM のガイドラインが発行されている。

こういったガイドラインに加えて、2005 年後半には、様々なガイドラインも発行された。例えば、最近注目されている鳥インフルエンザに関するガイドラインも、ニュージーランドの経済産業

省からリリースされた。このように、世界の各国、政府、官公庁、そして企業でもかなり関心が高まっている証左と考えている。

日本では、経済産業省、中小企業庁、そして内閣府、金融機関がガイドライン・指針を出している。例えば経済産業省では、2005年3月にBCMに関するガイドライン、事業継続計画策定ガイドラインとして、IT事故を中心にしたガイドラインを発行した。これが日本で初めての政府官公庁が出すガイドラインである。これは情報セキュリティマネジメントの一環としても出されている。

一方、経済産業省では、ISO化に対する国際標準化委員会も設営し、日本の原案を作成した。中小企業庁でもBCP有識者会議を設置している。BCMは大企業だけが構築すればよいものではなく、中小企業庁にもBCMを構築してもらおうという意図がある。例えば、中小企業にBCMを導入しやすいように、BCMに関するガイドラインの作成、さらに言うとBCMを構築している企業には貸出金利を安くする、若しくは災害時には即日に融資することなどについて検討している。

内閣府中央防災会議では、2005年8月に事業継続ガイドラインを公表した。これは、地震を対象にしたガイドラインである。

そして、金融機関では日本銀行が業務継続体制の整備を民間銀行に求めている。金融監督当局では、監査を観点に中小銀行、地域金融に対してBCMを監査基準として明確にうたわれるようになった。日本の流れは、大企業だけではなく、中小企業もBCMで取り組んでいかなければならない状況になっている。これは、国として、災害時にも日本の国力を衰退させてはいけないという意志が明確化されているとも言える。

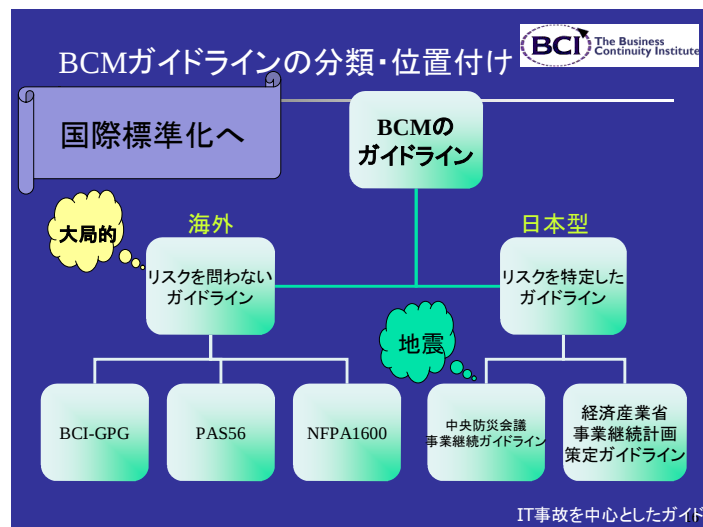
簡単に日本のBCMに関するガイドラインを再整理すると、内閣府のガイドライン、経産省のガイドライン、そして日本規格協会が出した事業継続管理の指針の3つとなる。日本規格協会が出した事業継続管理のための指針は、前述したBCI、そして英国規格協会（BSI）、こちらがつくったPAS 65を日本語訳したものである。

5. BCMガイドラインの分類

まず大きく分けて、リスクを問わないガイドラインと、リスクを特定したガイドラインがあると考えられる。内閣府中央防災会議は地震を中心にしたガイドラインで、経済産業省はIT事故を中心としたガイドラインとなる。具体的なリスクを対象にしているので、日本人には分かりやすい。一方、海外では、リスクを問わないガイドラインが主流になっているわけです。BCI-GPG（Good Practice Guideline）、まさに実践ガイドラインとやそれをベースにして策定したPAS 56（英国規格協会）、そして、米国NFPAはリスクを特定するものではない。

このリスクを問わないガイドラインは、結果事象を基準としていると言える。例えば、本社のケースを考えた場合、「地震が起きました」、「火災が起きました」、「IT事故が起きました」、「テロが起きました」、「疫病が起きました」など、どれを取っても大災害の場合は本社機能は麻痺する。海外の場合はその事象が発生した場合に、どう行動すればよいかが最も重要なポイントなのである。この考え方をベースにすると、新たなリスクが発生した場合でも対応できる形態になっ

ている。



6. BCM の各ガイドラインの動向調査

(1) NFPA 1600

米国規格協会が ISO 化のベースに出しているものである。BCM の ISO 化の主催国はアメリカで 2006 年 4 月に ISO の会合が開かれまして、ISO 化が議論が開始される。NFPA 1600 は、フレームワークのみを記しているだけで、基本的に自治体対象に書かれている。経済産業省の海外調査の結果、現地点では企業はこの NFPA に関心を示しておらず、NFPA で記載されている内容は当然のことと受けとめられている。実際には、DRII、BCI のガイドラインが受け入れられている。

(2) PAS 56

英国規格協会が出したものである。PAS 56 は、BCI がガイドラインを 2002 年に世界で初めて発行したものをベースに、2003 年まとめられたものである。現在英国規格協会では、PAS 56 を改訂中である。新しい PAS 56 は、2006 年 7 月に発行予定で、次に英国国家規格化に展開される予定であり、またその延長線上に ISO 化も見据えている。

(3) TR 19

TR 19 は、2005 年 9 月に ISO の総会がシンガポールで開催されました際にシンガポール規格協会がリリースをした。内容は、NFPA 1600、PAS 56、BCI のガイドラインをバランスよく取り込んでいる。一方、シンガポールには、SS 507 があり、シンガポールにおける BCM に関する事業の提供者（例えば IT 会社やコンサルティング会社など）を規格化するものである。アジアでは、この他にインド、香港、中国などでも BCM の導入を図っている。

7. 各 BCM ガイドラインの内容

(1) BCI のガイドライン及び PAS 56

シンガポールの TR19 も本内容に準じている。まず、BCI ガイドラインの大きな特徴の一つは、世界の企業が BCM を構築する際に最もよく使っているガイドラインということである。同ガイドラインによると、BCM の定義は、英国規格協会、日本では経済産業省、日本規格協会も同様の定義を使っているが、「組織を脅かす潜在的なインパクトを認識して利害関係者、ステークホルダーのインタレストとか名声、ブランド及び価値創造活動を守るため、復旧力及び耐容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」と記載されている。ここでポイントになるのは、復旧力及び耐容力であり、最近ではレジリアンシー（Resiliency）とも言われるが、事故・災害・事件が発生した際でも、いかに復旧力及び耐容力を高めていくか、それを企業として高めていくか、になる。

BCM の運営（マネジメントシステムとしての最終形は、以下の通り 5 つのフェーズから構成される

	項 目	内 容
ステージ 1	自事業の理解	■ 組織戦略 ■ ビジネスインパクト分析 ■ リスク分析とコントロール
ステージ 2	BCM に関する戦略	■ 組織の BCM 戦略 ■ プロセスレベルの BCM 戦略 ■ バックアップの戦略
ステージ 3	BCP を中心とした危機時の総合的な対応	■ 危機管理計画 ■ 事業継続計画（BCP） ■ 事業単位の BCP
ステージ 4	BCM 文化の発展・確立	■ 普及・啓発の現状把握 ■ BCM 文化の構築 ■ BCM 文化の達成度評価
ステージ 5	訓練、継続的改善、監査	■ トレーニング ■ 継続的改善 ■ 監査

上記の 5 つのフェーズを継続的に改善していき、プログラムマネジメントとして、各フェーズに柔軟性を持たせるような形で BCM を構築していこうというのが、BCI ガイドラインの大きな特徴である。

同ガイドラインでは、各フェーズの目的—なぜこの業務、この分析を行う必要があるのか—、プロセス、具体的に何を最終成果物として作成すれば良いのか などについて記載している。また、いつ再検討すべきかについても記載しており、例えば、新規事業を立ち上げた場合、工場など新たな事務所をつくった場合、アウトソーサーを大きく変更した場合などと示している。

BCI のガイドラインのその他主要な特徴を説明する。一つ目は、マネジメントシステムとして経営トップの推進の下、組織全体を通じて、「役割」「責任」の明確化をしていきながら、会社としての方針を作ろうということ。

二つ目は組織戦略との整合を基軸にすること。例えば事業を継続する観点で、もともとの組織の目的は何か。組織の目標はどのように達成できるのか。組織が提供する製品、サービスは何か。組織の目標達成には、社内外を含めてどういう関係者が存在して、どのような位置

付けか。そしてそれらの製品やサービスを提供するのに、絶対的な時間の条件、目標復旧時間はどうか、という大前提を繰り返し聞いていくことになる。これが今までのリスクマネジメントとは異なった大きな観点といえる。

時間的な条件である目標復旧時間は、災害、事件・事故が発生してから復旧までの時間を指す。そしてもう1つの大きな特徴は、事業復旧の優先順位を付けていくことである。時間軸については、MTO、RTO、RPOがあり、MTO（Maximum Tolerable Outage）は、「事業の許容最大停止時間」であり、業務／ファンクションがなくなってしまった場合に許される最大の許容停止時間である。MTOを基本にしながら、目標復旧時間、RTO（Recovery Time Objective）を決めて自社のBCMの取組の目標とする。

RPO（Required Point Objective）は、システム・データを観点として、どの時点までのシステム・データを戻せればよいか、というバックアップ戦略の基本を占めるものである。RPO、目標復旧ポイントが短ければ短いほどバックアップの頻度を高めてしまい、それはコストに跳ね返る。一方、長くすれば長くするほどコストは安くなる。

その他特徴は、事業継続に関する従業員の意識の向上、文化を醸成の必要性・重要性をうたっているのが、BCIのガイドラインの大きなポイントである。そして訓練、継続的改善、監査を進めていく形にある。

なお、本ガイドラインは、元々2002年に作成され2005年に改訂版が発行されたが、その3年間に、企業・官公庁などの組織に使用してもらい、実際の意見をフィードバックさせたところに大きなポイントがある。

(2) NFPA1600

NFPA（National Fire Protection Association；全米防火協会）は、アメリカにおける防火・防爆の団体である。防災の観点では細かな規則を作成している。NFPA1600は元々、地方公共団体向けに防災マニュアルとして、1995年に発行された内容である。それにBCI、DRIIが参画し、同防災マニュアルにBCPの要素を付け加え、2004年に発行された。これはテロの影響を受けてこの改訂を行ったことになる。

NFPAの特徴は、一般的にはBCPを「Business Continued Program」として、BCPのフレームワークのみを記載し、BCPの内容に踏み込んでいない。プログラム、BCPをどのように、策定していけばいいかというフレームワークを記載しているのみである。NFPAでは、災害復旧、BCMの導入、維持管理に関するフレームワークを提供するもので、マネジメントサイクルや監査については言及されていない。想定すべきリスクは、自然災害と人為的災害と2つに大きく分けているのみ。自然災害に括られる、火山の噴火、地震、台風、ハリケーン、SARSだとか疫病も含まれる。人為的災害は、火災、故意による災害などである。

NFPAは、災害復旧に大きく重点を置いている。事業復旧上の優先順位付けなどの記載はない。現状としては、徐々に米国では受け入れられてきている状況である。

この2つ、つまりBCIのガイドライン（PAS 56）とNFPA 1600、これが一つ大きなISO化

の有力候補と言える。

(3) 経済産業省の事業継続計画策定ガイドライン

経済産業省の事業継続計画策定ガイドラインは2005年3月に発行された。内容は、主としてIT事故を中心にした内容になっている。海外の状況や海外のガイドラインをベースにしながらかつて作っているため、整合性・内容ともによくできた内容になっている。例えば、当該ガイドラインの第1章「総論」には、一般的なBCMの構築手法が記載されているが、ビジネスインパクト分析からリスクの分析・評価の手順、教育・訓練維持・管理について網羅的に記載されている。

また、3.3.BCP 発動フェーズー災害・事故などが発生した直後の初動での緊急時対応をどうすればいいですか。次の業務再開フェーズー企業として組織として守るべき業務、ファンクション、これをまずもって継続していきましょう、再開していきましょうというフェーズ。業務回復フェーズー基幹業務を回復した後で、その他のフェーズ、業務についても順次回復していこうというフェーズ。全面復旧、ここは最終の事業体制・組織体制、つまり最終展開までのフェーズとなる。これは米国では一般的な考え方である。

本ガイドラインのさらに特徴的な内容は、最終章の個別計画と一例えば大規模なシステム障害、セキュリティインシデント、情報漏洩、データ改ざん時の対応について述べていることにある。

(4) 内閣府中央防災会議の事業継続ガイドライン

内閣府中央防災会議のガイドラインは、2005年8月に発行された。地震を中心にして検討されたガイドラインである。もともと日本は地震リスクは非常に高い。海外でも日本は地震リスクは高いという認識もある。本ガイドラインは、災害に強い国づくり、防災力を向上させようというのが大きな特徴である。その中で従来の防災対策と異なる特徴は、先ほどから繰り返し説明をしているが、「継続すべき重要業務の絞込み」、「事業継続を妨げる事象の検討」、「重要な要素（ボトルネック）の特定」、「目標復旧時間」である。

まずは地震という自然災害を中心に、取り組みを始めていったらどうかと提言している。

8. まとめ～世界、日本のガイドラインが目指すこと、日本の進むべき方向～

世界のBCMガイドラインの共通する事項は、企業など組織がリスクを問わず大局的な観点に立って、事業継続上、危機的状況に陥った場合に、ステークホルダーの観点にまず立った上で、事業復旧の優先順位付けをまず行う。例えば災害が発生した場合には、人員がすべて駆け付けられることができるわけではなく、全部門一斉に事業復旧できるわけではない。そのような環境下、その組織として何をまず死守すべきか。ファンクションでも結構、業務でも良いのだが、組織として必ず守るべきものを特定しておくこと。

2番目に、事業復旧のタイムスケジュール（時間軸）を示すこと。供給責任など社会的な観点に立って、目標復旧時間を設定して、取引先などのステークホルダーに対する責任を果たしてい

くことが重要である。それを遂行するには、従業員の事業継続に関する意識を高め、企業文化として確立していくことが必要不可欠ということである。

日本にとっては、事業復旧の優先順位付けやタイムスケジュール・時間軸、そして企業文化を醸成していくことについて一定目新しい概念があるかもしれない。ただし日本は他国と比較して防災は先進的と言われている。防災法規も充実しており、例えば地震でも海外と比較して充実した対策が取れていると言われている。充実した防災対策をベースに考えれば、日本企業の BCM、そして国家の BCM は世界一になる可能性があると考えられる。したがって、将来的には日本の BCM、日本の企業は事業継続に優れていると世界から言われる可能性を秘めていると考える。そのためには、世界、そして日本で発行されている BCM の各ガイドラインの特徴を理解しながら、バランスよく取り入れ構築していくことが必要である。そうすれば、ISO 化にも十分対応できる力が付くであろう。

おわりに

本利用ガイドは、世界の主要なガイドラインを調査し取りまとめたものである。対象となるリスクや地域に応じて利用できるのもので、多国籍企業も活用でき国際的にも有用であると思われる。

このガイドで紹介した解説が各団体や企業における BCM 構築の一助になれば幸いである。

情報セキュリティ専門部会メンバー

委員長	篠原 雅道	BCI 日本支部／株式会社インターリスク総研
委員	駒瀬 彰彦	株式会社アズジェント
委員	斎藤 俊治	株式会社KDDI & BT グローバルソリューションズ
委員	原田 薫	日本ヒューレット・パッカード株式会社

以上