

事業継続性を支援する I T 技術に関する一考察

鶴 薫

三菱電機株式会社 情報技術総合研究所

要旨：

社会インフラにおける情報システムの重要性が増すに従い、IT 災害発生時にも早期に復旧することが求められており、その手法として事業継続性という考え方が登場した。しかし、現実世界は情報システムだけに閉じてはいないため、個別の業種、業態、企業による試行錯誤が行なわれている。本研究では、情報システムの視点から事業継続管理に適用可能な情報技術の体系化を進めると共に有用な情報システム、情報ツールのアイデアを抽出することを目的としている。本稿では、事業継続性と情報技術の関わりを明確化しようと試みると共に、研究を進めるに当たっての課題の抽出を行なった。

A Preliminary Study of the Information Technology that Support the Business Continuity

Kaoru TSURU

IT R&D Center, Mitsubishi Electric Corporation

Abstract:

The request to restore the IT system early when the IT disaster occurred is growing stronger with the importance of the IT systems is increasing as a social infrastructure. Then the idea of BCM (Business Continuity Management) appeared as one of the management methodologies. In this research, our objective is to systematize the information technology that can support the business continuity from the aspect of the information systems. In this paper, we considered the relations of the business continuity and the information technology, and clarified problems and tasks of our research in next steps.

1. はじめに

1.1 背景

世界的には、2001年の米国同時多発テロ、日本国内においては、ここ2~3年の自然災害に代表される予測困難なリスクの頻発により、社会インフラとしての重要度が増している情報システムに対する事業継続(BC¹)/事業継続計画(BCP²)/事業継続性管理(BCM³)というキーワードが注目されるようになってきている。

しかし、多くのITベンダから提示されるのは、情報システムの復旧手段や、安全確認の手段と言った個別の技術やノウハウの提示の枠を出ておら

ず、BCコンサルティングから運営までのノウハウを持つ個別の企業はあるものの、情報技術という視点から体系的にユーザに提示されているものはないと思われる。BCコンサルティングを行なっている主な企業は、業務分析、BCP立案の指導などには強いが、情報システムの活用まで含めてユーザに提示出来ている企業は少ない。

また、相互依存性の高まった社会における情報システムに限定されない組織存続の為の方法論、及び、存続対象ではなく、支援技術としての情報システム、情報ツールが求められているが、部分的にはあるものの、体系的な研究は見当たらない状況である。

¹ BC: Business Continuity

² BCP: Business Continuity Plan

³ BCM: Business Continuity Management

1.2 目的

本研究では、BCP/BCM の普及を支援するべく、以下の2点を目的としている。

- ① BCP を策定・運用管理するマネジメントサイクルと BCP の実行に対する支援技術としての情報技術の体系化

BCP とは、情報システムの復旧が目的ではなく、業務復旧が目的であり、ほとんどの業務は情報システムだけで成り立っている訳ではない。従って、業務復旧を支援する為の情報技術が必要であるし、BCM を運営するにあたっては様々な情報技術が必要となる。こうした情報技術を体系化してユーザーに提示できる形を目指す。

- ② BCM を支える情報技術と物理世界の接点の具体化

BCM の個々の作業を支援する為の具体的な手段や情報システム、情報ツールのアイデアを抽出する。

2. BC とは

2.1 BC の定義

BCI⁴による定義では、BCP は「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」であり、BCM は「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」とされている[1]。

この定義にあるように、BC とは、テロや災害だけではなく、セキュリティ事故、企業不祥事といった事業に損害を与えるような事故も対象としている。従って、ISMS⁵適合性評価といったセキュリティ標準や、日本版 SOX 法といった企業の内部

統制などとも密接に関連している。

また、BC は企業や自治体のみならず、あらゆる組織に対して適用可能な考え方であるし、組織の大小も問わない。

BCM を従来からある企業統治の一手法である RM⁶との違いで見ると表 1 のようになる。

表 1：RM と BCM の違い

	RM	BCM
分析の切り口・視点	特定のリスク(地震・火災・IT事故など)	事業継続に必要な事象(業務、物流、人、データ、資金など)の脆弱性
分析パラメータ	確率(可能性)と損害額	時間と損害額
想定するリスク	基本的には全てのリスク	事業/企業の存続を妨げるリスク

次に、日本で比較的進んでいる一般的な防災対策との違いを表 2 に示す。

表 2：防災対策と BCM の違い

	防災対策	BCM
リスク分析、損失分析などの視点	リスクとして、地震・火災などの災害のみを考慮し、人命安全の視点で画位立案	事業上の損失が発生しうる全ての脆弱性が対象で、経済的な分析に基づいて計画立案
予防・予知の視点	災害発生時に被害を最小にする為の対策	災害に対する予防処置など、BCP 策定過程で盛り込む
経営資源(人物金)の視点	リソースの管理(社員の扱、機材の手順など)は通常考慮されていない	事業継続・復旧のコストを考慮
RTO/ RPO の視点	未設定、又は限定的/部分的	具体的な目標値を設定
企業内周知と訓練・見直しの視点	避難訓練は行なわれるが、それ以外に対して限定的	計画の検証の為の定期的な訓練と計画の見直し

以上のように BCM は、従来の RM、防災対策とは異なる視点で取り組む必要がある。最も異なるのは、RM や防災対策が、特定災害(リスク)の被害抑止、被害軽減に力点を置いているのに対し、BCM は起きてしまった事にどう対処するかに焦点があ

⁴ BCI: the Business Continuity Institute

⁵ ISMS: Information Security Management System

⁶ RM: Risk Management

てられている点である。

なお、災害発生時における BCM の実現手段レベルでは、初動対策に防災対策の内容を流用したり、情報システム対策に同じような情報技術を適用したりすることは可能である。

2.2 BC のマネジメントサイクル

他の多くの管理手法と同様に BCM も図 1 に示すようなマネジメントサイクルによる BCP の検証・評価・更新が必須である。このサイクルを怠ると BCP が陳腐化し、災害時に適用できなくなる。

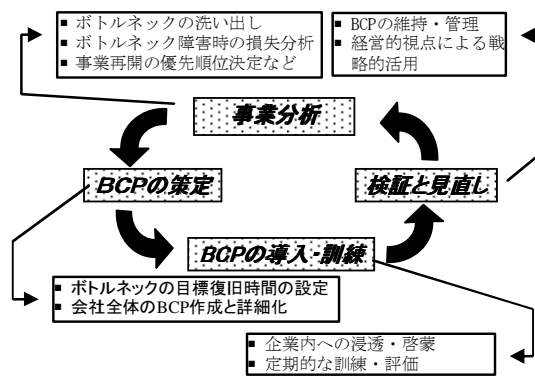


図 1: BC のマネジメントサイクル

2.3 普及状況と標準化

各種調査[3][4]によると欧米企業における普及率が 50~70%に対して、日本国内の普及率は 10~20%程度となっている。これに対して、行政(経産省、内閣府)が BCP 策定ガイドラインを公開するなどの普及活動を行なっている[5][6]。

最も導入が進んでいるのは、金融業界である。これは、社会インフラとして規制業種であった為と金融事業が守るべきものが取引データに集約される為、情報システムの災害対策として取り組み易かった為と考えられる。

欧米では、英国の BCI、北米の DRII⁷を中心とした普及活動と標準化推進がなされている。現在、ISO 化の議論が開始されており(担当委員会は TC233)、3~5 年で ISO 標準となる見込みである。なお、ISO 標準では、BCM ではなく、EP (Emergency

⁷ DRII: Disaster Recovery Institute International

Preparedness) と呼称される予定である。

既に欧米企業と取引のある国内企業では BCP 策定を求められている例もあるようであり、ISO 化されると契約の前提条件となる可能性が高く、標準化動向を注視する必要がある。

2.4 日本固有の状況

欧米の企業などで策定が普及している BCP は、主にテロや火災などのピンポイントでの災害への対応であるが、日本の場合、地震に代表される広域災害への対応が必須と考えられる。広域災害の場合、長期に渡り拠点周辺のライフラインの停滞することなどが想定され、一企業のみではなく、自治体、地域と協力した復旧も考慮する必要があると言われている。

なお、広域災害である大地震への対策を考えておけば、他の多くの災害への応用が利くと考えられる。それは、地震による広範囲な社会機能の麻痺、設備の破壊という点で、洪水や津波などの他の広域災害への対策に応用可能であるし、また、業務遂行に必要な社内外の人や機材の手当てができなくなるという点で、伝染病流行や、テロ、火災などへの対策にも応用可能であろう。

3. BC に必要とされる情報技術

3.1 概要

BC に必要とされる情報技術としては、図 2 に示すように、実際の災害発生時に BCP を実行支援する為の技術分野と図 1 に示した BC のマネジメントサイクルを支援する平常時の各フェーズ対応の技術分野に分けられる。なお、防災・減災への

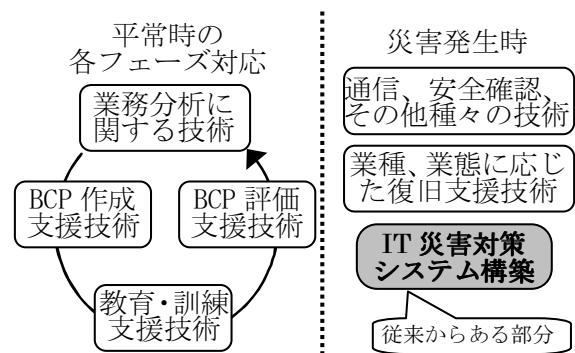


図 2: BC を支える情報技術の概要

対応も災害発生時の技術分野を含む。

多くの企業は、情報システムのみで業務がなりたっている訳ではなく、物理的な資源(人、装置など)と物流(Logistics)、他の企業との連携(Supply Chain など)で、その事業が成り立っており、従来の IT 災害対策システムは、一部分に過ぎない。

次節以降で、BCM の各フェーズに対応する情報技術の整理を試みた内容を示す。

3.2 BC 運営の各フェーズ

BC 運営の各フェーズで行なうべき内容とそれを支援する情報技術を以下に示す。

(1) 事業分析フェーズ

- ビジネス影響分析(BIA⁸)
 - 事業継続、復旧の優先順位付け
 - ⇒ 経営情報の提示による経営判断なので、事業の重み付けを支援する情報システム/ツールがあれば有用。
 - ボトルネックの特定
 - ⇒ 業務プロセスの可視化支援を行なう情報システム/ツールが有用。
- 事業中断リスクの評価
 - ⇒ 各業務が中断することにより被る損害の算出支援する情報システム/ツールが有用。
- 発動基準の明確化

事業、業務分析主体の本フェーズでは、業務分析を行なう BPR⁹、BPM¹⁰を目的とした既存技術、情報システム/ツールの応用が可能であると認識している。

(2) BCP の策定フェーズ

- ボトルネックの RTO の設定
 - ⇒ 許容可能な損害限界点を RTO に設定する。実現可能性から設定するものではない。
- 対策手法の立案

⇒ 前項の RTO を実現する個別の業務対応となるので、様々な業態に向けた技術開発と技術のカタログ化が必要。必ずしも実現可能となるとは限らない。

■ 投資額の算定と予算化

⇒ RTO を満たす為の投資が出来ないことがほとんどなので、予算額で可能な対策を立案。予算に応じた技術を選択する為のガイドラインが必要。

■ 全社レベル、部署毎の対応計画立案

⇒ マニュアル作成支援を行なう情報システム/ツールが有用。

実際に BCP を策定する本フェーズでは、業態、業種毎の技術、ノウハウの蓄積が欠かせず、一律な体系化は困難だと認識している。また、マニュアル化ができる範囲は、標準的な作業や事前に予想できる事態への対応に限られる為、マニュアルを作成すること自体を目的としてもあまり意味がなく、考えられるさまざまなケースについて問題を整理し、関係者で関連事項を考え、対策や復旧手順を議論することに意味がある。従って、マニュアル作成のための検討作業を記録し、支援できるような情報システム/ツールが有用となる。これを元に次項の教育・訓練に利用可能な状況把握や対応力の学習、問題把握の為の教材を作成出来るような情報システム/ツールが有用となるが、ほとんど存在していない。

(3) BCP の導入・訓練フェーズ

■ 教育と訓練

⇒ BCP 策定で検討された内容を元にシミュレーションやロールプレイによる教育・訓練を支援する情報システム/ツールが有用。

■ テスト(BCP の有効性の検証)

■ 結果の記録、評価

⇒ 机上、実地テストを実施した結果を記録し、評価を支援する情報システム/ツールが有用。また、結果を次項の

⁸ BIA: Business Impact Analysis

⁹ BPR: Business Process Re-engineering

¹⁰ BPM: Business Process Management

BCP の見直しにフィードバックできればなお良い。

いかに良いBCPが策定できたとしても、実行出来なければ意味がなく、本フェーズはその点で重要な意味を持つ。従って、教育と訓練を効率良く実現可能とする支援技術が極めて有用となるが、ほとんど存在しない。

(4) 検証と見直しフェーズ

■ BCP の見直し・変更

⇒ テスト結果、評価を受けて、対策とマニュアル作成のフェーズにフィードバックする情報システム/ツールなどが有用。

■ BCP の監査

⇒ ISO などの標準化対応で監査を支援する情報システム/ツールなどが有用。

BCP が有効に機能するかどうかの評価、監査を支援する技術は有用であるが、極めて困難であると認識している。

3.3 災害発生時

実際に災害が発生した際の対処だが、IT 災害発生時の災害対策計画としては、図3に示すようなRPO¹¹とRTO¹²を考慮したバックアップからの復旧を計画することが従来言われている。

しかし、実際のBCPを検討する際には、情報シ

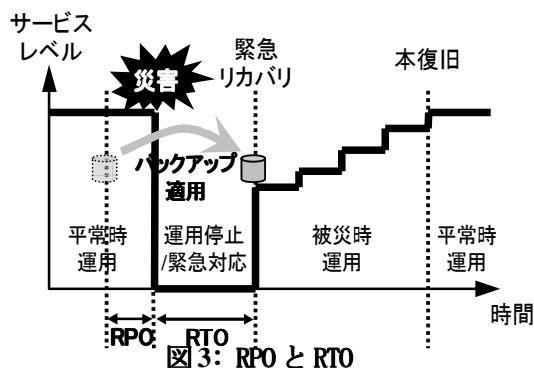


図3: RPO と RTO

¹¹ RPO: Recovery Point Objective

ステムだけではなく、業務、資源なども考慮する必要がある。これを考えるには図4に示す4つのフェーズに沿って検討する必要がある。

各々のフェーズで必要とされる情報技術としては、従来の災害対策技術に加えて様々な技術、システムが登場してきている。以下、各フェーズの内容と対応する情報技術を示す。

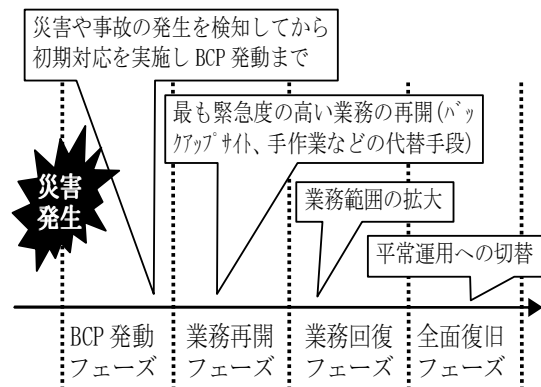


図4: 災害発生から復旧までのフェーズ

(1) BCP 発動フェーズ

■ 発生事象の確認・情報収集

⇒ 様々なセンサー、通信路を利用した遠隔での監視に関する情報システム/ツールが有用。

■ 安否確認、安全確保

⇒ 組織に所属する構成員の安否確認を支援する情報システム/ツールが有用。

■ 対策本部設置

■ 被害状況の確認

■ 業務影響の確認

■ 基本方針の決定

本フェーズにおいては、特に広域災害の場合、社会インフラ(通信、電力など)も被害を受けている可能性が高く、情報システムの利用が難しいケースが多い。しかし、対策本部と構成員を結ぶ情報伝達路の確保は、状況確認、安否確認などの基本的な前提条件の確保の為に重要であり、現在、様々な技術、システムが開発され

¹² RTO: Recovery Time Objective

つつある。また、遠隔地に設置されるだろう対策本部において、状況の整理、現場に対する指示を支援する情報システム/ツールなども有用である。

(2) 業務再開フェーズ

- 資源(人、機材、場所)の確保
- 代替手段への切り替え、人員の配置
 - ⇒ 代替オフィスを提供するサービスなどはある。
- 復旧作業の実施
 - ⇒ 従来の災害対策技術の適用可能な領域と新たな技術開発が必要な非情報システム業務に対する領域とがある。
- 業務再開とモニタリング

情報システムに対しては、従来の災害対策技術を適用するフェーズであるが、業態、業種により復旧の対象は異なり、個別の技術開発が必要となる。

(3) 業務回復フェーズ

- 業務拡大範囲の見極め
- 復旧状況の確認
- 追加資源投入の検討・実施
- 継続業務拡大の検討・実施
- 全面復旧のタイミング決定

本フェーズは、ある程度の資源が利用可能になりつつある段階である為、復旧支援の為の情報システムなどがあると有用である。加えて、状況判断を支援する為のなんらかの技術があると有用である。

(4) 全面復旧フェーズ

- 切り替え判断
- 全面復旧手順の確認と実施
- 資源の再配置
- 業務制限への対応
- 総括

本フェーズも情報システムに対しては、従来の災害対策技術を適用するフェーズであるが、

業態、業種により復旧の対象は異なり、個別の技術開発が必要となる。同様に状況判断を支援する為のなんらかの技術があると有用である。

4. BC 支援技術の普及に向けた課題

4.1 体系化の課題

表3に前章で述べた各フェーズに対応した情報技術を大まかに分類した一覧を示す。

表 3：各フェーズ対応情報技術分類

フェーズ	分類	既存システム/ツール
防災/減災	セキュリティ	認証、アクセス管理など
	高可用性システム	冗長構成、HA/クラスタなど
	予知・予防	地震予知、アクセス監視など
災害発生時	監視・情報収集	有線・無線による遠隔監視、センサ技術など
	システム復旧	復旧支援ツール生成システムなど
	バックアップ	テープバックアップなど
	代替システム	遠隔バックアップなど
	業務復旧支援	緊急時指揮支援システムなど
	安全確認	携帯メールを用いた安全確認システムなど
BC運営	安全確保支援	緊急時の情報提供用掲示板システムなど
	業務分析	業務プロセスの可視化ツールなど
	BCP策定	災害対策作成支援システムなど
	教育・訓練	
	評価・監査	

体系化を進めるにあたっては、ユーザに対して、BCP/BCMの全体像を示しながら対応する技術を提示すると共に、その技術で対応可能な支援レベルも提示する必要がある。また、概算のコスト計算の手法を提示することにより、ユーザが個別の技術を選択し易くする必要もあるだろう。

4.2 コストの問題

情報システム向けの災害対策で通常システムの2~3倍のコストがかかることや、費用対効果が見え難いことから考えても、BCP/BCMを行なうのは、経営的には単なるコスト増大にしか見えない。この為、経営面から、このようなシステムには投資し辛く、既に導入している企業においても、規制対応や、保険的な扱いと言った後ろ向きの理由で導入がなされていることが多いようである。

従って、今後BCP/BCMの普及を促進させるには、対策システム導入が利益を生む投資として認識さ

れる必要がある。即ち、平常時の事業活動に寄与しないような支援システムでは受け入れ難く、平常時においても事業活動に寄与するシステムを構築する必要がある。

例えば、運送業で、安否確認システムを兼ねて、作業車(及び、作業者)の配置管理システムを構築するなどの工夫が必要である。

4.3 情報システムがない組織に対する課題

情報システムがそもそもないような中小の組織に対して、BCP/BCM を導入させるには、パソコン減税に見られるような税制による優遇処置や、融資条件での優遇のような何らかのインセンティブが必要である。その上で、導入のハードルを低くする情報ツール類の提供が必要となる。

例えば、事業のボトルネックとして地震などの広域災害を想定せずに仕入れ事故、機材の故障などといった対処しやすい事故を前提として、BCP を考慮する為のチュートリアル的なパソコン用情報システム/ツールなどが考えられる。

4.4 取組み強化が必要な分野

既存のシステムがほとんどなく、情報システムでの支援が必要な分野としては、教育・訓練と評価・監査の2つがある。評価・監査に関しては、そもそも評価尺度や、監査対象の議論が始まったばかりの状況であるので、まずは、教育・訓練分野への取組みが期待される。

例としては、図5に示すような災害状況のシミ

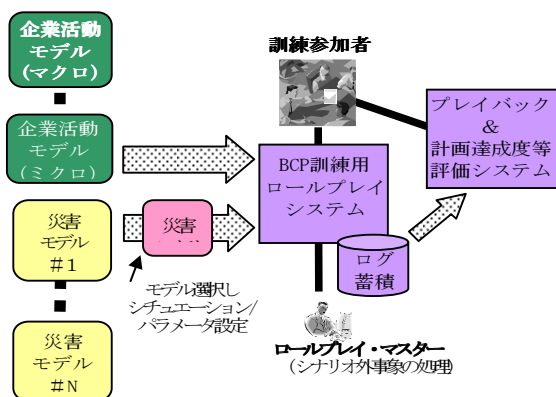


図5: 訓練システム例

ュレータとロールプレイのゲームシステムを組み合わせたような訓練システムがアイデアとしてある。

5. おわりに

以上のように BC を支援する情報技術を簡単に洗い出し、大まかな分類を行なった。また、BCP/BCM の普及を推進するにあたっての以下の課題抽出を行なった。

- ・ 技術の詳細な体系化とユーザへの提示
- ・ 投資効果が明確なシステムの構築
- ・ BC 導入を誘導するような情報ツール類
- ・ 教育・訓練を支援する情報システム

今後は、これらの課題に優先度を付けて取り組んで行く予定である。

参考文献

- [1] “PAS56: Guide to Business Continuity Management” The British Standards Institution, 2003
- [2] 「平成 16 年度 ビジネス継続性技術調査報告書」 財団法人情報処理相互運用協会, 2005 年 3 月
- [3] 「国内上場企業の BCM(事業継続経営) 導入調査を実施」 (http://www.irric.co.jp/press_release/2005/may/0509_2_1.html) インターリスク総研, 2005 年 5 月
- [4] 「災害時に有効な事業継続計画を持つ企業は約 2 割」 (http://www.mri.co.jp/PRESS/2005/pr050801_spd01.html) 三菱総合研究所, 2005 年 8 月
- [5] 「企業における情報セキュリティガバナンスのあり方に関する研究会報告書, 参考資料: 事業継続計画策定ガイドライン」 経済産業省, 2005 年 3 月
- [6] 「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 —」 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 防災担当, 2005 年 8 月