

ITサービス継続マネジメントの外部環境に係わる考察

Discussions on external environment of the IT service continuity management

渡辺研司

Kenji Watanabe

長岡技術科学大学大学院技術経営研究科

Management of Technology, Graduate School, Nagaoka Univ. of Technology

要旨

企業の事業継続の重要な部分を担う、ITサービス継続マネジメントについては、先日、経済産業省からもガイドラインが公開されたばかりであるが、実際には「どこまで、何をすべきか」というインセンティブを個別企業が持つまでには至っていない。本発表では、そのインセンティブとなる可能性のある、英国における第三者認証制度の開発状況や、米国金融業界で開発中の成熟度モデルを俯瞰しながら、ITサービス継続マネジメントの外部環境における論点の整理を試みる。

1. はじめに

現代のビジネスの手法は、ICT（Information & Communication Technology：情報・コミュニケーション技術）を積極的に経営・管理・オペレーションの分野に取り入れることで、地域や組織をまたがった形で分業体制が進み、効率性と即時性の向上を通じた全体最適を目指している。その結果は、100兆円を超えた電子商取引の急速な浸透や、SCM（Supply Chain Management：サプライ・チェーン・マネジメント）に代表されるような複数の企業間での効率性の追求が可能となったことに現れている。

このような「ネットワーク型」ビジネスの発展は、個別企業の経営においても効率化や拡張性の向上に大きく貢献しているが、一方で、ネットワーク内の連鎖障害に係わる対策が遅延していることで脆弱性も増加していることも認識する必要が出てきた。例えば、ここ数年で発生した地震、風水害などの広域災害によるサプライ・チェーンを通じた非被災地での操業停止や、システム障害の事例に目をやると、障害を起こしたシステムのみならず、インターフェースを持つ社内他システム、更にはネットワークを介して他社のシステムにまで影響を及ぼしたようなケースである。その結果は組織全体の機能不全やサプライ・チェーン全体の稼働停止にまでつながるケースも出てきている。利便性の裏側にある脆弱性が可視化され、実際の対応策が取られ始めない限りは、このような傾向は継続し、ネットワークやサプライ・チェーンを介した複合障害は増加してゆくものと考えられる。

このような状況下、日本でも事業継続マネジメント（BCM: Business Continuity Management）を多くの企業が導入しつつあり、具体的には2005年以降、経済産業省、内閣府、中小企業庁や業界団体などが相次いでガイドラインを公開したことや、ISO化の動きが出てきたことで、その取組みは加速されつつある。その中でも特に企業活動のIT依存度が急伸することを勘案すると、ITサービス継続性のマネジメント体制について規格化や評価モデルをベースに構築する必要が出てきている。

2. ICTサービス継続とそのマネジメント体制

企業が事業活動のICT依存性が急伸することを勘案、事業継続の観点から必要なICT機能を如何に確保するか、という観点で英国をはじめとしてITサービス継続マネジメントというマネジメント手法が浸透し始めている。そのアプローチは事業継続マネジメントにおいて、BIA（Business Impact Analysis：ビジネス影響度分析）を経て抽出された重要業務プロセスに係わるICT機能やICTインフラ、更には企業内外の要員にいたるまでの確保の段取りを計画するというものが今のところ主流である。このようなアプローチに具体的な業務プロセスと使用されるICTリソースのマッピングを行うような従来手法 [1] などを組み合わせて運用されている企業もある。

2.1. 英国規格（案）BS25777

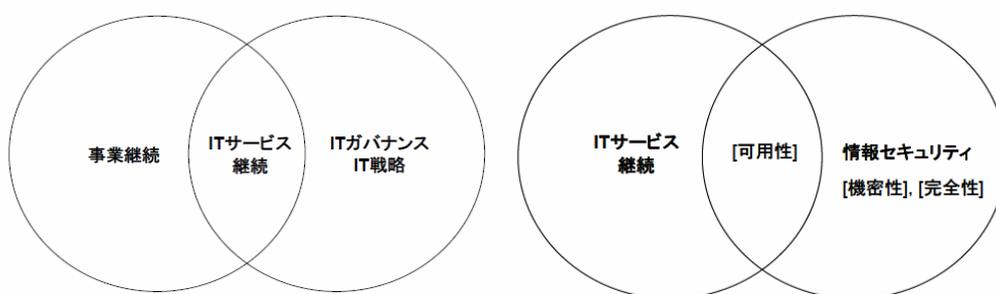
第三者認証を想定して策定された規格として英国で2006年に公開されたPAS77 [2] をベースに、2008年8月にBS25777がパブリックコメントを求めるための草案として公開された。その内容は下記の通り。

- 第1章：適用範囲
- 第2章：用語の定義
- 第3章：ICT 継続のプログラムマネジメント
- 第4章：事業継続のために I C Tに求められる要件
- 第5章：I C T継続戦略立案
- 第6章：I C T継続活動の開発と導入
- 第7章：演習と技術テスト
- 第8章：維持・レビュー・改善

2.2. 経済産業省『ITサービス継続ガイドライン』

我が国でも 2005 年に経済産業省から公開された「事業継続ガイドライン」からより I Tの観点を強くした形で、「ITサービス継続ライン」が 2008 年 8 月に公開された。[3] この議論の過程においては、上述の P A S 7 7 も意識しながら、更に経済産業省が公開している、信頼性確保や I Tガバナンスに係わるガイドラインとの位置関係や役割分担も議論された。

図 1 IT サービス継続と事業継続/ITガバナンス、及び情報セキュリティとのバウンダリーの議論



3. ITサービス継続性の評価と成熟度モデル

3.1. ITサービス継続性評価の必要性

I Tサービス継続性の評価は単体では企業の意味決定にはそれほど付加価値を与えることがないが、事業継続マネジメントへのフィードバックとしては欠かせないものである、という位置づけと考えられる。この継続性は別途「レジリエンシー (resiliency)」という言葉で置き換えることができるか、このレジリエンシーについては、例えば I B Mインド基礎研究所で開発中の R M I (Resiliency Maturity Index、情報システムが中心) や、米国の金融機関が集まって活動する米 F S T C (Financial Services Technology Consortium) と C E R Tが開発中の R M M (Resiliency Maturity Model) がある。

3.2. 米国 F S T C・C E R T『レジリエンシー成熟度モデル』

2005 年前後よりカーネギーメロン大学ソフトウェア研究所、金融業界、主要ベンダーがコンソーシアムを作成し、テロ・災害・サイバー攻撃対応、制度対応、重要インフラ障害対応、サプライチェーン途絶対応などの能力に関する成熟度モデルを開発している。[4] 現在、参加企業の評価データを出し合ってベンチマーキング中。

表 1 CERT-REF における成熟度①

成熟度	評価基準
4	Continuously Improved
3	Directed
2	Managed
1	Performed
0	Incomplete

表2 CERT-REFにおける成熟度②

成熟度	評価基準
1 : Performed	Fully Implemented
↑	Largely Implemented
↑	Partially Implemented
↑	Not Yet Implemented
0 : Incomplete	Not Implemented

4. まとめ:今後の課題

事業継続マネジメントの観点からもその開発と普及が望まれるITサービス継続マネジメントの考え方は、ITサービス継続性をどう定義し、どのような評価軸を構築できるかが実効性を確保する鍵となる。

しかし、現状では方法論や評価軸も発展途上、もしくは、ある特定の産業やグループに限定的なフォーカスで推進されていることから、今後は汎用的な考え方と、産業あるいは業種特有の部分を担当個別の考え方の整理と統合が不可欠である。個別企業においてもITガバナンスやITリスクマネジメントといった一連のICT関連の諸活動との関連や、全体的な経営資源の配賦について本発表で概説する外部環境も考慮に入れながら取り組む必要がある。

参考文献

- [1] Suh, B. and Han, I. “The IS risk analysis based on a business model, *Information & Management* “, 41, pp.149-158, 2003
- [2] British Standards Institute, IT Service Continuity Management (Code of Practice, PAS77:2006), 2006.
- [3] 経済産業省, ITサービス継続ガイドライン, 2008.
- [4] Carnegie Mellon Software Engineering Institute, CERT Resiliency Engineering Framework(Review version, v0.95R), 2008