BCM評価の可能性と課題

～企業の競争力に貢献するBCM～



あらた基礎研究所企業の事業継続性研究会
企業の事業継続マネジメント（BCM）シンポジウム
2010年2月19日

渡辺　研司
WATANABE, Kenji
watanabe@kjs.nagaokaut.ac.jp
長岡技術科学大学大学院技術経営研究科

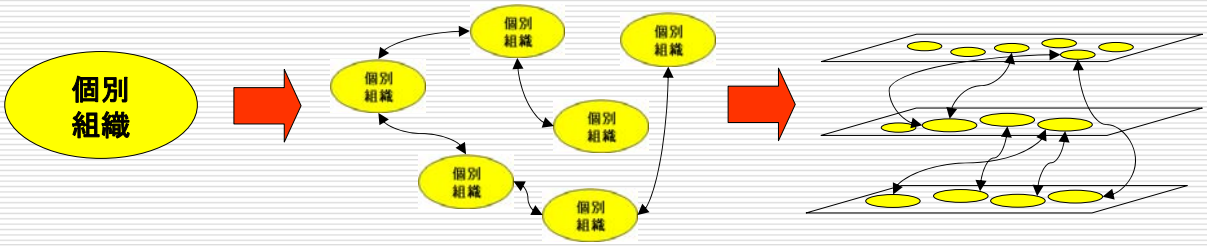
問題意識・研究の背景

事業継続性評価ニーズの高まりと現行の仕組みの限界

- 組織・企業・国家をまたがった事業・業務の水平・垂直分業の拡大
- 社会・経済活動における事業継続マネジメント（BCM）の浸透
- 相互運用性を勘案した事業継続性評価ニーズの台頭
- 発展途上の方法論・仕組みにおける評価軸の整理の必要性

拡大する事業継続マネジメント(BCM)の範囲

ネットワーク型社会における相互依存性の増加:『点』から『線・面』へ、そして『層』へ



個別組織のレジリエンシー	組織間の関係性を考慮したレジリエンシー	社会的な階層を考慮したレジリエンシー
＜視点の例示＞ ■ 企業・企業グループ ■ 中央省庁・地方自治体 ■ 公的機関 ■ NPO・NGO など	＜視点の例示＞ ■ 取引先・サプライチェーン ■ 行政 ■ 業界団体・経済団体 など	＜視点の例示＞ ■ 地域社会 ■ 官民協業 ■ 国家安全保障 ■ 国際間競争 など

＊レジリエンシー(resiliency):しなやかな復元力 / 弾力性のある回復力

事業継続性評価の利害関係者①

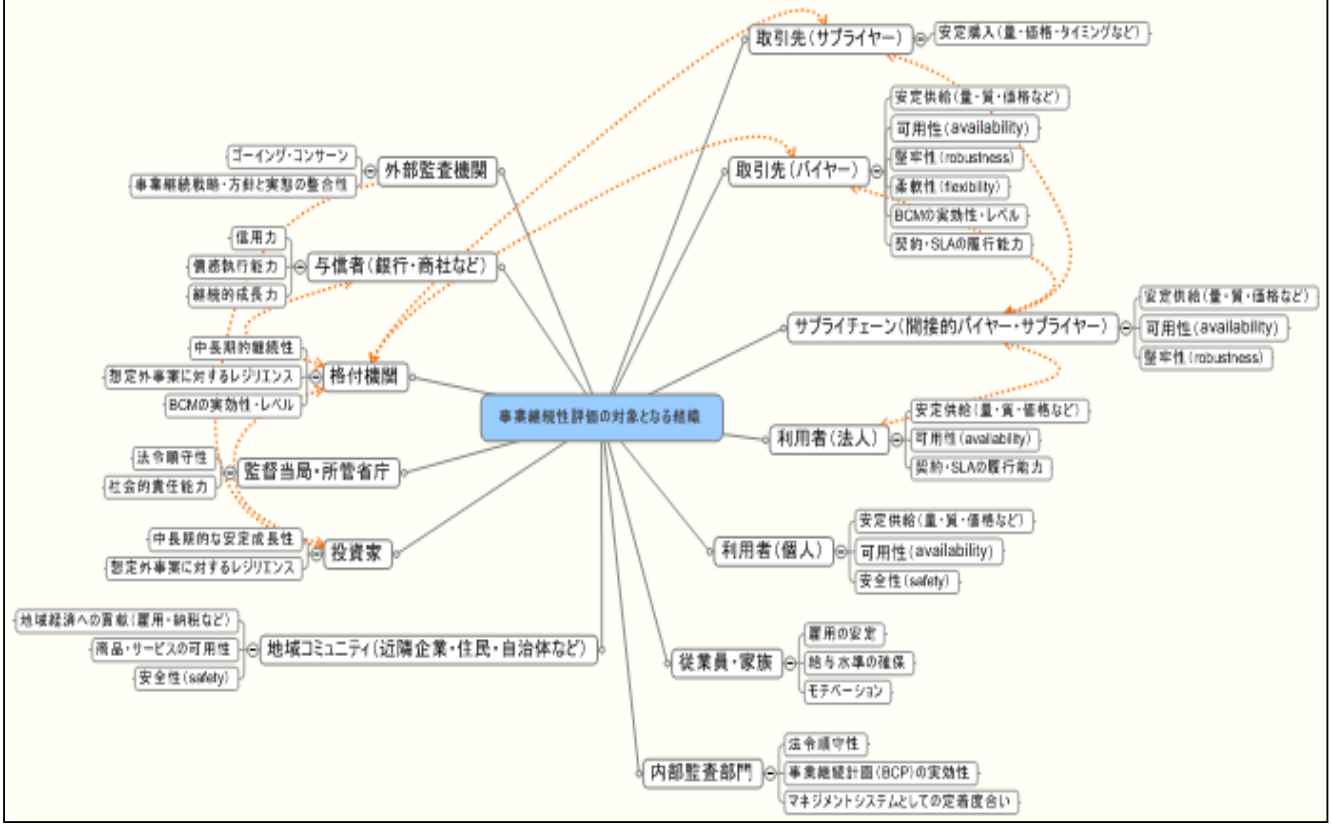
直接・間接的なステークホルダーと被評価組織との関係

ステークホルダー	関係要因
取引先(バイヤー)	商取引契約
取引先(サプライヤー)	商取引契約
サプライチェーン (間接的バイヤー・サプライヤー)	安定供給性
利用者(法人)	購買契約
利用者(個人)	購買契約・消費行為
投資家	出資、株式・債券購入
格付機関	格付評価

ステークホルダー	関係要因
与信者(銀行・商社など)	与信契約
内部監査部門	内部監査義務
外部監査部門	監査契約
従業員・家族	雇用契約
監督当局・所管省庁	許認可
自治体	許認可、登記
地域コミュニティ (近隣企業、住民、自治体など)	地域リソースの共有

事業継続性評価の利害関係者②

直接・間接的なステークホルダーと評価の観点



事業継続性評価への対応アプローチ

SLAと認証制度の特徴と限界

- **SLA（サービス・レベル・アグリメント）への反映**

＞定量的な分野に限られ、また、事業継続性そのものを確保するものではない

- **第一者認証（内部監査による）**

＞あくまで自己評価に基づくもので、事業継続性を客観的に評価するものではない

- **第二者認証（購買者などによる監査）**

＞求められる事業継続性の観点を織り込むことが可能であるが、取引先が多岐に亘る場合はその実施と評価のメンテナンスに限界がある

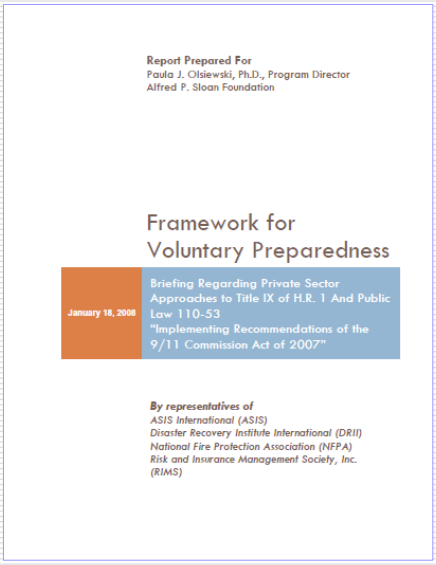
- **第三者認証（標準化された認証規格を用いる）**

＞現在適用可能な認証規格はマネジメントシステム認証規格であるため事業継続性を直接的に評価するものではない

BCM評価を必要とする経済的インセンティブの台頭
資本市場との連携などの効果

- 売上逸失保険などの保険料引下げ
- 金融機関からの借入金利の引下げ
- 中長期投資格付への反映
- BCM関連投資に関する課税減免
- 政府関連機関入札時の優位性付加

企業の自発的な備えに関する枠組み（米国・2008～）
民間企業にも自主的な自助努力を示唆：現実を踏まえた多様な選択肢


Report Prepared For
Paula J. Olsiewski, Ph.D., Program Director
Alfred P. Sloan Foundation

Framework for
Voluntary Preparedness

January 18, 2008

Briefing Regarding Private Sector Approaches to Title IX of H.R. 1 And Public Law 110-53 "Implementing Recommendations of the 9/11 Commission Act of 2007"

By representatives of
ASIS International (ASIS)
Disaster Recovery Institute International (DRII)
National Fire Protection Association (NFPA)
Risk and Insurance Management Society, Inc. (RIMS)

ASIS INTERNATIONAL Advancing Security Worldwide®
セキュリティマネジメント
Security Management

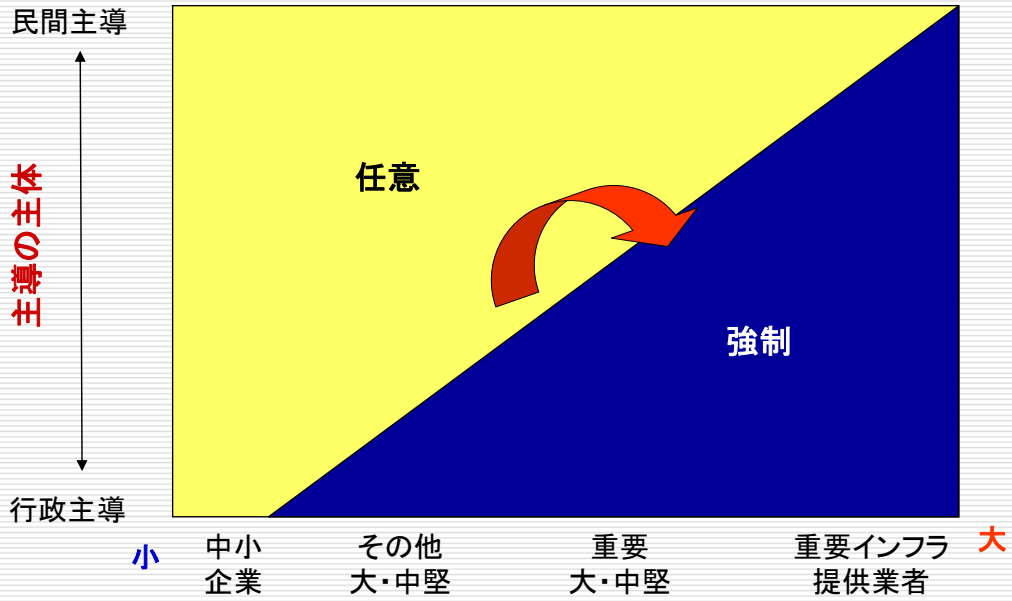
DRI the institute for continuity management
事業継続マネジメント（BCM）
Business Continuity Management

NFPA
緊急時マネジメント
Emergency Management

Risk and Insurance Management Society, Inc.®
リスクマネジメント
Risk Management

企業におけるBCMへの取り組みのインセンティブ領域

市場原理（任意）と法規制によるプレッシャー（強制）のバランス



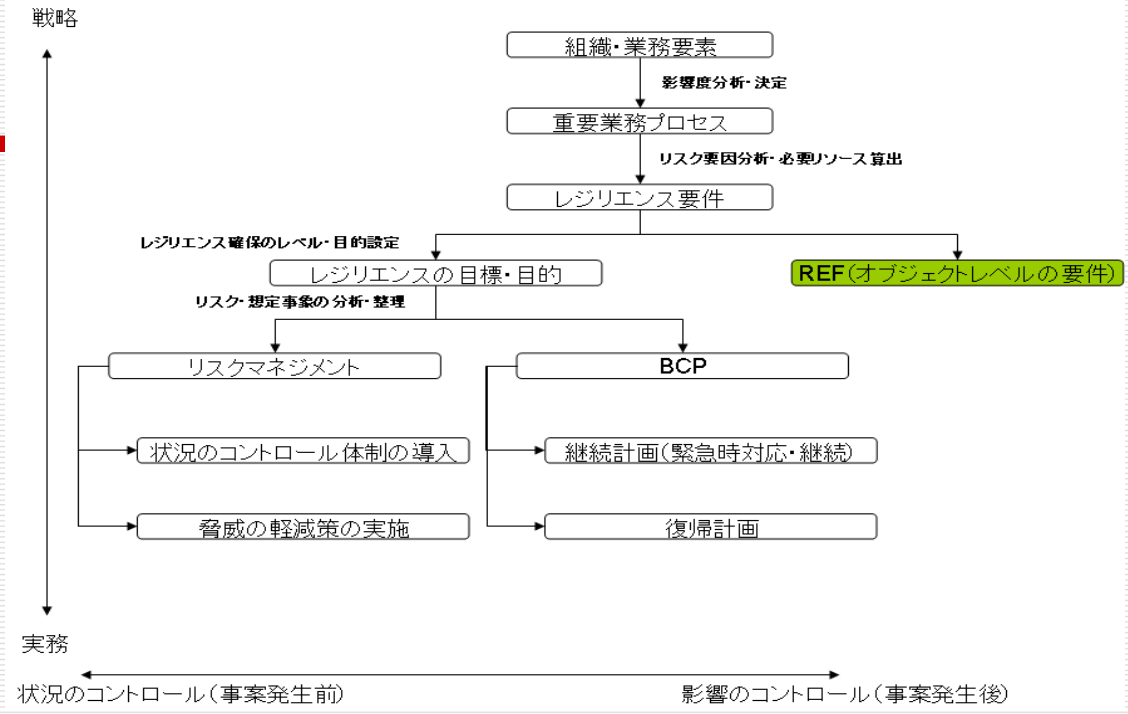
レジリエンシー成熟度モデル（CERT－REF）の概要

REF：Resiliency Engineering Framework

- 米国カーネギーメロン大学SEI（ソフトウェア工学研究所）を中心に開発されたレジリエンシー成熟度モデル。
- 2008年3月にv0.95Rを公開。現在も開発進行中（v1.0）。
- 米国大手金融機関を中心にベンチマークによる評価軸の調整を実施中。米国金融監督当局も協力。
- ソフトウェア開発の分野では常識となっているCMM（Capability Maturity Model：能力成熟度モデル）をベースに作成。

CERT-REFの概要

事業継続性評価のフレームワークとしての有効性と限界の議論



REFにおけるCapability

評価分野の網羅性と要素間排他性の議論

- ADM – Asset Definition & Management
- AM – Access Management
- CM – Controls Management
- COMM – Communications Management
- COMP – Compliance Management
- EC – Environmental Control
- EF – Enterprise Focus
- EXD – External Dependencies
- FRM – Financial Resource Management
- HRM – Human Resources Management
- ID – Identity Management
- IMC – Incident Management & Control
- ISR – Integrated Service Resiliency
- KIM – Knowledge & Information Management
- MA – Measurement and Analysis
- MON – Monitoring
- OTA – Organizational Training & Awareness
- PM – People Management
- PM – Process Management
- RAD – Resilient Asset Acquisition & Deployment
- RISK – Risk Management
- RRD – Resiliency Requirements Development
- RRM – Resiliency Requirements Management
- SC – Service Continuity
- SPM – Security Program Management
- TM – Technology Management
- VAR – Vulnerability Analysis & Resolution

REFと既存の枠組との関係

フレームワーク設計時の考慮点と整合性維持の取組み

- BS25999
- Cobit 4.1
- COSO ERM:2004
- CMMI
- DRII/GAP
- ISO20000-2:2005(E)
- ISO24762: 2008(E)
- ISO27002: 2005(E)
- NFPA1600
- PCI:2005　＋FFIEC（米国金融機関検査マニュアル：BCP編）

CERT-REFにおける成熟度

0－4の5段階評価とその設定アプローチ

CERT-REFの評価

他業界も含めた適用汎用性と実効性が確保できる運用体制の設計が重要

- CMMの実績に裏打ちされた実効性と活用の容易性への期待
- レジリエンシーの要素分解の個別評価の網羅性の高さ
- 経営環境の変化スピードと開発の進捗状況とのギャップ
- システム開発分野と比較してより定性的な分野における評価メッシュの過度な細かさ
- 米国大手金融機関（Citi、JPMC、Master Card、Wakoviaなど）の特殊性と他業界への展開における汎用性確保の困難さ
- 導入後の運用体制の負荷軽減の必要性

今後の課題

引続き研究・開発が必要な分野と期待される動きと課題

- **ベンチマーキングなどによる相対評価の仕組みの開発と導入**

  CERT－REFに見られるような同質のグループ内での相対評価（ベンチマーキングなど）による事業継続性評価の仕組みの開発。
- **標準規格・フレームワークを用いた絶対評価が可能な分野の特定と試行**

  ITサービス継続性といった限られた分野、かつ、組織横断的に汎用性の高い分野における絶対評価を行うための指標の開発。
- **市場に展開中の事業継続性に係わる第三者認証規格の実効性の検証と事業継続性との関係性の整理**

  事業継続マネジメント（BCM）に係わる第三者認証規格（BS25999-2、ISO22301など）によるマネジメントシステム認証と事業継続性評価との関連性の整理。
- **事業継続性の定義・目的・評価の取扱いに関する関係者間コンセンサス**

  事業継続性評価の目的結果の取扱いに関する市場・ステークホルダー間のコンセンサスの醸成。