【解説】

ビジネスレジリエンスを実現するオンデマンドソリューションの展望

大塚 純一

Perspective of On Demand Solutions to Business Resilience

Junichi Ohtsuka

オンデマンドビジネス環境では従来の経験に基づくリスクへの対策立案（ソリューション）ではなく，未知のリスクをも含めたあらゆるリスクに対して予期し迅速にかつ柔軟に対応できる能力が求められる．
この論文は，オンデマンドを実現する要件であるビジネスレジリエンス（Business Resilience），つまりリスクに対する弾力性や情報システムの回復力を高めるために，オンデマンドテクノロジーが有効であり，従来の事前予防策中心のパラダイムから新しい事故後の回復力向上策のパラダイムへ大きく転換させる技術であることを展望する．

The on demand business environment requires capabilities to predict all kinds of risks including the unknown, and to make rapid and flexible responses to them, not the risk solutions based on the past experiences. This paper presents a view that the on demand technologies are effective for business resilience essential for the on demand world, namely for increasing elasticity to risks and recovery capability of information systems, and that they are causing a radical paradigm shift from the conventional prevention-centric approaches to the improvement of capabilities to recover from disasters.

Key Words & Phrases：統合リスクマネジメント，ビジネスレジリエンス，高可用性，
ビジネス・コンティニュイティー，災害対策
integrated risk management, business resilience, availability,
business continuity, disaster recovery

1．はじめに

ビジネスレジリエンス（Business Resilience,以下BRと記す）とは，ITサービスを中断させるリスク，つまり情報システムの障害や災害，または予期しない急激な需要の増加等に対し，迅速にITサービスを回復しビジネス継続を実現させる能力を言う．［1］

これを実現させるためにBRでは6レイヤーに分けて定義している．（**図1**）

BRを高めるためには6レイヤーそれぞれにリスクを洗い出しリスクの大きさを判定し，対策を立案することが必要である．レジリエントビジネス・インフラストラクチャー分析手法（Resilient business infrastructure analysis 以下 RBIAと記す）［3］は網羅的な調査シートによって各レイヤーのすべてのリスクを把握し，過去累積された他社との比較を行い成熟度の評価を行い提言してくれる．

提出日：2004年08月31日　再提出日：2005年1月17日

一方，BRを実現するソリューションとはITサービスを中断させるさまざまなリスクへの対応策である．

これには従来の高可用性システム（High Availability Systems, 以下HAと記す），災害対策（Disaster Recovery, 以下DRと記す）またはセキュリティなどが含まれる．

すべてのソリューションが全体としてどの程度の効果があるのかを説明するためにはリスクを共通の評価軸で測定し個々のソリューションを対応させて評価する，統合リスクマネジメントの考え方が必要となる．

たとえばデータセンターの脆弱（ぜいじゃく）性に着目し，データセンターの移転をし，かつ災害時のバックアップセンターを同時に持つとする．この場合，二つのソリューションの効果を評価すると次のように言える．

移転することにより，固い地盤に立地し最新の耐震施設に入るなどリスクの発生頻度を下げる予防効果がある．またバックアップセンターは万が一の被災に迅速に業務を回復し被害を最小限に抑える軽減効果がある．

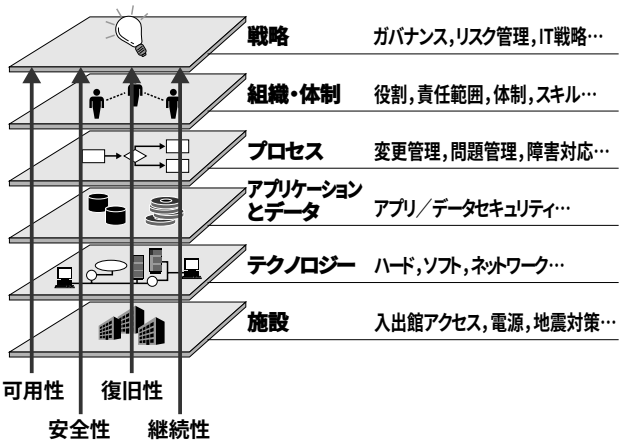

図1. BRの6レイヤー [2]

オンデマンドテクノロジーによって提供される仮想化・統合化・オープン化の機能により, すべてのITサービスを短時間で距離を置いた場所に設置されたITインフラストラクチャーで切り替え継続させることができる.

これらを応用したオンデマンドソリューションはリスク軽減策としてHAだけでなくDRにも利用できる技術である.

本論文では, オンデマンドテクノロジーの実現によるオンデマンドソリューションの登場が従来の事前予防策中心のパラダイムから新しい事故後の回復力向上策のパラダイムへ大きく転換する技術であることを展望する.

本論文では, 第二章で一般的なリスクマネジメントの手法であるリスクポートフォリオ分析を情報システムに応用してリスクとそれに対応するソリューションの関係を解説する.

第三章では第二章を踏まえてオンデマンドソリューションの効果, 価値を理解するための前提となる統合リスクマネジメントの考え方を解説する. 第四章ではオンデマンドソリューションの実現が第三章でとらえた統合リスクマネジメントの視点(パラダイム)を大きく変化させる可能性があることを提起し, 新パラダイムに移行する効果は何かを考察する.

第五章では新パラダイムの実現を阻害する現状の情報システム環境の課題に触れ, 課題を解決しスムーズに移行させるためにはどのような方策があるかを展望する.

2. リスクとソリューションの相関

2.1 リスク損失を定量的に計るには

一般的なリスク分析手法ではリスクの大きさは次のように定義される. [4]

リスク損失額＝発生頻度×1回あたり損失額
(サービス中断時間)　(1)

ここで,

(1)「リスク発生頻度」とは, 単位期間あたり(1日あたり, 1ヶ月あたり, 1年あたり, 10年あたり, など)の発生期待値である.

(2)「1回あたり損失額」とは, リスクが発現した場合の直接および間接的な損失額であり, 金額に換算されるものである. BRではITサービスの中断時間に応じて損失額の大小が決まるので, ITサービス中断時間を損失額の代替属性とみなすことができる.

実際, 発生頻度, 1回あたり損失額を決めるためには定性的な要因をできる限り定量化することが必要である.

発生頻度, 1回あたり損失額とも定量的に測定する方法として, ハインリッヒの法則を使った分析, 確率論的安全評価法(PSA), モンテカルロ法によるシミュレーション技術などのいくつかの方法が試みられている. [5] [6]

リスクの発生頻度を縦軸(y軸)に, 1回あたりの損失額(サービス中断時間)を横軸(x軸)に置くと, 識別されたリスクは, R(x, y)で表され, リスク損害額はR(x, y)で囲まれた面積となる. (**図2**)

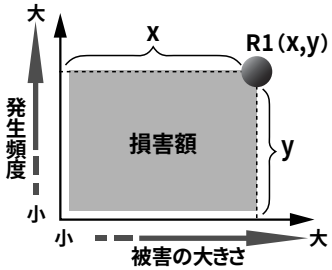

図2. リスクの評価

リスク損失を定量的に把握するには次の手順で行う.

(1) できる限り多くのリスクを認識し特定する.
(2) それぞれのリスクの発生頻度をつかむ.
(3) 1回あたりの損失額をつかむ.
　(損失額はサービス中断時間に置き換えて評価することも可)
(4) おのおののリスクについて, リスク損失額を式(1)で求める.
(5) 識別されたすべてリスク損失額の合計を求める.

2.2 ソリューションの価値

ある特定のリスクの損害額を下げるためのソリューションには二つの方法がある. 一つはリスク発生頻度を下げることでありリスク予防策である. リスク予防策は識別されたリスクを上から下へ移動させるソリューションである. 二つ目は1回あたり損失額を小さくすることであり(サービス中断時間を短縮することと言える)リスク軽減策である. リスク軽減策は識別され

たリスクを右から左へ移動させるソリューションである.（**図3**）

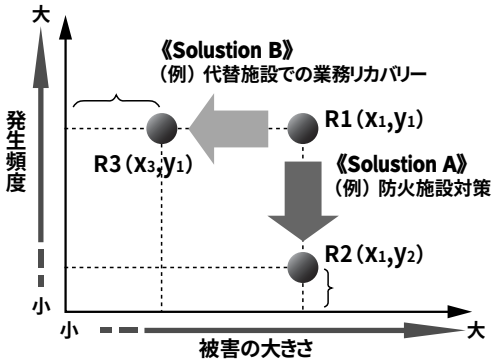

図3. ソリューションの価値

ソリューションの価値はリスク予防効果またはリスク軽減効果（リスクを下または右に移動させる距離）に比例して高まり, リスク予防策または軽減策構築費用またはその維持費用に反比例するものと考えられる.

2.3 リスクの識別と分類

リスクポートフォリオ分析はリスクを特性によって分類し把握する手法である. [7]

これを情報システムのITサービスを中断させるリスクに応用しソリューションとの対応で考察する.

発生頻度（縦軸, y軸）と1回あたりの損失額（横軸, x軸）にマッピングされたリスクを4つの象限に分割する.（**図4**）

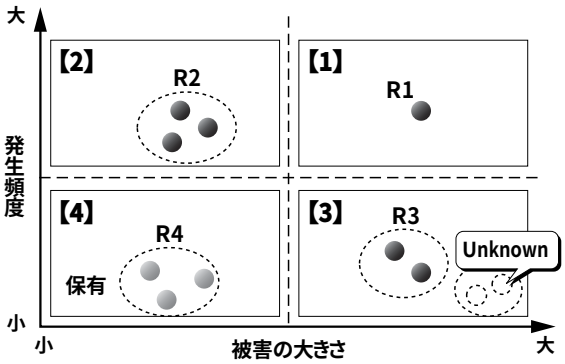

図4. リスクポートフォリオ

それぞれの象限のリスクに対するソリューション戦略の基本方針は次のように考えられる.

（1）第一象限【1】 発生頻度が高く, 被害の大きさが大きいリスクであり, 最も対応すべき優先順位の高いリスク領域である. 対策としてリスク予防を十分行った上でリスク軽減をとる.

（2）第二象限【2】 発生頻度は高いが被害は大きくないリスクであり, 通常の情報システムの運用で遭遇するシステム障害である. 対応策としてリスク予防をとる

（3）第三象限【3】 発生頻度は低いが1回あたりの被害が大きいリスクである. いわゆる災害事象がこの領域に含まれる. 対応策としてリスク軽減をとる.

（4）第四象限【4】 発生頻度, 被害とも小さく容認できるリスクである. 対応策としてリスク保有し, 一時的な経費で処理する.

2.4 リスク予防策

リスク予防策とはリスクの発生を事前に予防し発生頻度を下げることによってリスク損失額を削減することを目的とした対策である. 実際には日々の運用で発生し直面する機器障害, 人的運用ミス, ネットワーク障害など障害対策の領域と考えられる. これらは部分的な障害による局所的なITサービスの停止であり, 障害を取り除くことによって比較的に早くITサービスが回復する.

この領域のリスクは発生頻度が高い, すなわち繰り返しリスクの発生を経験することから日々の運用管理のなかで障害管理, 問題管理として扱われ対応されている. 対策立案にはリスクが発生した真の原因をなぜなぜ, を繰り返しながら分析し追究し最終的に根本的な原因を取り除く. 真の原因はそれぞれ異なるためこれをすべてのリスクについて検討し対応する.

リスク予防のソリューションは発生頻度を十分に下げ, 第二象限のそれぞれのリスクを第四象限に移動させる.（**図5**）

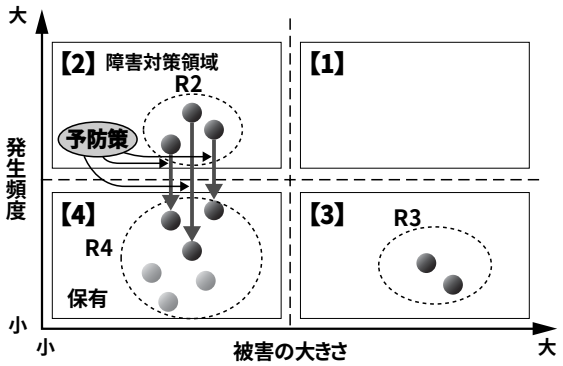

図5. 事前予防策

2.5 リスク軽減策

リスク軽減策とは, リスクの発生後に被害の拡大を防ぎできる限り早くITサービスを回復させることを目的とした対策で, 広域災害対策であるコンティンジェンシープランなどが相当する.

発生頻度が低く1回あたりの被害が大きい（ITサー

ビスの停止時間が大きい）リスクは，リスクの発生を事前に予測し予防することが難しい．

リスク軽減策は，リスクの種類を問わず，リスクの発生とITサービスの停止を前提に代替設備や代替センターなどに切り替えすばやくビジネスを継続させ，被害の大きさを低減する対策である．すなわちビジネス継続のために必要なITサービス機能の分散，すなわちITコンポーネントの冗長化，二重化などの対策である．

リスク軽減のソリューションによって第三象限のリスクを第四象限へ移動させることができる．（**図6**）

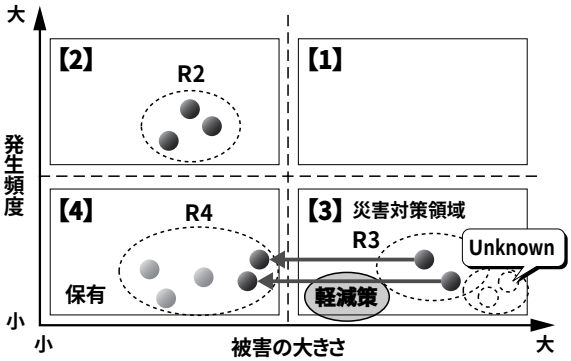

図6．事後軽減策

3．統合リスクマネジメント

統合リスクマネジメントとはリスクポートフォリオ分析でマッピングされ分類されたリスクに対しリスク予防策とリスク軽減策を適切に組み合わせて，最も効果的にBRを達成するための全体的包括的なリスク戦略である．つまり，発生頻度と被害の大きさでマッピングされ分類された第一，第二，第三象限のリスクに対し第四象限（リスク保有）に落とし込む戦略立案である．（**図7**）

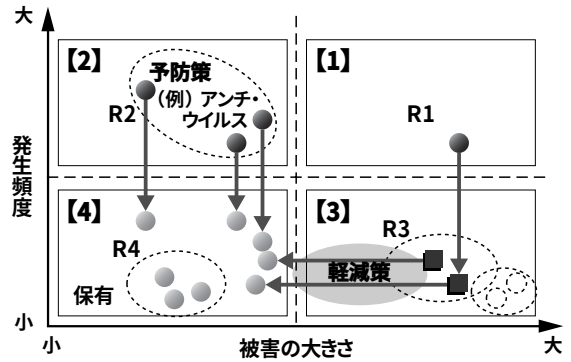

図7．統合リスクマネジメント戦略

いままで経験したことのない未知のリスク（Unknown Risk）は発生頻度が非常に少なくまたリスク損失額が非常に大きいと考えられるので第三象限に入る．

リスク戦略立案において，特に未知のリスクを含む第三象限に対する対応を忘れてはならない．

実施のステップは以下のように行う．

（1）全体のリスクの内容を理解し俯瞰（ふかん）する．
（2）第一象限から第四象限に含まれるリスクの配置の妥当性を確認する．
（3）第一，第二，第三象限に予防策，軽減策のソリューションの効果を当てはめながらすべてのリスクが第四象限に移動できることを確認する．
（4）全体的な対策費用を確認する．
（5）実行優先順位を設定する．

個々のリスクに対するソリューション構築を行う前に，統合リスクマネジメントによるリスク戦略の検討が必要な背景は次のように考えられる．

（1）24時間ITサービス提供やネットワークを使ったサービスの拡大により情報システムに対する安定性，完全性，機密性の要求が高まっていること．
（2）自然災害，特に地震など単一のリスクだけではなく，事故，故障，障害または人的過失，犯罪，不正行為，テロなど，リスクが多様化していること．
（3）SARS，鳥インフルエンザなどかつて経験していない未知のリスクが存在しこれらを含めた対策が必要なこと．

4．オンデマンドテクノロジー

最新の研究・調査報告［8］によるとオンデマンドオペレーティング環境（On demand operating environments）のコアの構成要素に実装されるオンデマンドテクノロジーによるBRを達成するための以下の機能の実現が期待されている．

4.1　実現のための主要な目標と要件

（1）ITインフラストラクチャーに対しBRを実現する機能を実装すること．
（2）ITインフラストラクチャーとアプリケーション・データ配置，およびビジネスプロセスの関連を理解した上で，重要ビジネスプロセスの継続性を主眼に置きBRを実現させること．
（3）ITサービス中断による業務および財務的な影響を最小化させることを最終的な目標に置くこと．
（4）継続的なBR機能の検証を可能にすること．
（5）マルチベンダー，マルチプラットフォームで統一した回復機能を提供すること．
（6）通常のIT運用管理にBR管理を組み込むこと．

4.2 実現への展望

(1) 仮想化技術によってITインフラストラクチャーの各コンポーネントの分散化, 冗長化をはかる.
(2) ストレージ環境における対等遠隔コピー(Peer to Peer Remote Copy以下PPRCと記す)とネットワークソリューションの利用により短時間でデータロスなしでシステムを回復させる.
(3) オートノミック技術によるBRポリシーに従ったリカバリー資源の管理, リカバリーアクションの決定および実行.
(4) マルチベンダー, マルチプラットフォームに共通な機能を定義する.
(5) 低価格化を実現する.

4.3 新しいパラダイムへ

革新的なオンデマンドテクノロジー, つまり高速のリモートデータミラーリング技術および急激な低価格化は, 情報システムのITサービス中断から, リカバリー目標時間(Recovery Time Objectives, 以下RTOと記す)の驚異的な短縮とバックアップデータの鮮度を示す指標であるリカバリーポイント目標(Recovery Point Objectives, 以下RPOと記す)を急激に縮め, ほとんどデータロスなしでITサービスが回復することを可能にする.

その結果, リスク予防策で対応していた第二象限のあるリスク領域に対してもリスク軽減策で対応できる戦略の転換を生むことになる.

これをリスクポートフォリオ分析を使って説明する. 第二象限の領域(リスク予防策)が縮小され, 第三象限の領域(リスク軽減, 事後対応策)が拡大されると示される. (**図8**)

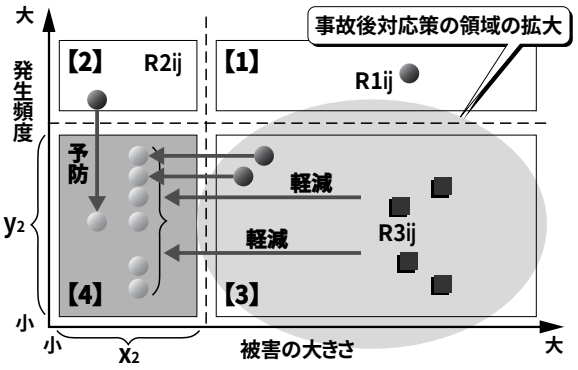

図8. パラダイムチェンジ

第三章, 統合リスクマネジメントで述べた図8に比べると, 各象限の境界線の交点が左上へ移動している. しかしリスクを許容し保有できる損害額の要件(リスク保有)は変わりない. なぜなら発生頻度の大きさ(y2)は大きくなったものの1回あたり損失額(x2)は小さくなったため第四象限(リスク保有)領域の面積(x2 x y2)に変化はないからである.

つまりオンデマンドテクノロジーを採用することによって従来のソリューションに比べ飛躍的に短時間でサービスを再開することができるため, 多くのリスクに対してリスク予防策でなく, リスク軽減策で対応するパラダイムチェンジを引き起こすことを意味している.

4.4 新しいパラダイムの価値

オンデマンドテクノロジーを採用することによって, 新パラダイムモデルに転換することの価値を整理すると次のようになる.

(1) リスク予防策は事前にリスクを識別しそのリスクが発生する真の原因を追究し対策を立案するが, 今日の複雑化したマルチベンダー・オープンシステム環境においては経験や専門的なスキルが不足しており大変難しい問題になっている.
(2) リスクは変化しているため, 常にリスクを識別し評価する必要がある. また, 未知のリスクに対しはリスク予防策が不可能であり意味がない.
(3) オンデマンドテクノロジーの発展によってマルチベンダー, マルチプラットフォームへの拡張やITインフラストラクチャーの低価格化が期待できる.

5. 実現への課題と展望

今日のITシステム環境を, BRを実現させるオンデマンドテクノロジーの環境へスムーズに短時間で移行させ実装するには大きな困難さが存在する.

新パラダイムモデルへ移行するために解決すべき課題を整理する.

(1) 現在のITシステムはレガシーシステムと最新のWebソリューションが混在しておりさまざまなマルチベンダー環境で構成されている. 新旧のITインフラストラクチャーや複雑なシステム環境のため簡単にオンデマンドテクノロジーを採用することができない.
(2) また, これらのインフラストラクチャーの導入にあたって, あらかじめ明確なBRの目標が設定されていない.

これらの問題に対して, アイ・ビー・エム グローバルサービスで提供するさまざまなBR関連のサービスがその課題を解決する糸口を提供してくれるだろう. [9]

HA, DRの多くの稼動実績に基づいた知的情報アセットやBRビジネス要件またはリスク調査, ビジネス影響度分析(Business Impact Analysis)などのメソドロジー, あるいはHA, DR設計構築サービス, または運用サービスがある. 上流工程から実施運用に至る下流工程まで一貫した支援サービスが提供されている.

6. おわりに

本論文では, 新しいオンデマンドテクノロジーによって, いかなるリスクでも情報システムのサービスが中断した場合に, 自動的にその影響を分析しバックアップシステムを使って速やかに切り替えビジネスを継続させる機能が提供され, 統合リスクマネジメントの戦略立案のパラダイムを従来の事前予防策中心から事後軽減策へ転換させることができることを展望した.

オンデマンドテクノロジーによるBRの実現はBRのテクノロジーレイヤーに相当するが, (図1)他の5レイヤーの統合リスクマネジメント戦略にも大きく影響する.

戦略, 組織・体制, プロセス, アプリケーションとデータ, 施設の各レイヤーにわたって従来の事前予防策中心の考え方から事後軽減策へのシフトを行うことによってより柔軟な回復力のある情報システムの機能が実現されると期待する.

参考文献

[1] IBM BRCS編集, Finding the Return on Resilience, IBM ITS University 2003
[2] 日本アイ・ビー・エム主催, 情報セキュリティ強化セミナー, ITインフラにおけるレジリエント(回復力)の向上, 発表資料, 2004.09.03
[3] IBM, IBM Global Services - Resilient business and infrastructure assessment Internet site, http://www-1.ibm.com/services/us/index.wss/so/its/a1000230
[4] 日本情報処理開発協会編, リスク分析(JRAMによるアプローチ), 日本情報処理開発協会, 1992
[5] 危機マネジメント研究会編集, 実践危機マネジメント, ぎょうせい, ISBN4-324-06718-X, 2002
[6] 経産省工業技術院, JISQ2001 リスクマネジメントシステム構築のための指針, 2003.3.20制定
[7] JIPDEC, JRM解説書, 財団法人日本情報処理開発協会, ISBN4-89078-012-2, 2004
[8] 日本セキュリティ・マネジメント学会編, セキュリティハンドブック, 日科技連, ISBN4-8171-6059～ISBN4-8171-6061, 1998
[9] Donna Scott, *Trends & Best Practices in Business Continuity & Availability Management*, Gartner Research, 2003
[10] IBM, Business Resilient Internet site, http://www.ibm.com/services/its/resilience

日本アイ・ビー・エム株式会社
ICP コンサルティングITスペシャリスト
大塚 純一 Junichi Ohtsuka

[プロフィール]
1979年, 日本IBM入社. 1999年から数多くの大規模, マルチベンダー環境の災害対策構築プロジェクトを経験する. その後災害対策ソリューションのコンサルティング, 構築・運用サービスであるBCRS(ビジネス・コンティニュイティ アンドリカバリーサービス)に異動し, 現在ビジネスレジリエンスのプロジェクトをリードする一方でお客様にソリューションのご提案、展開を担当。

E17017@jp.ibm.com