

2011.3.29

BCMニュース <2010 No.12>

BCMを支えるIT即応能力の最適化

今年の3月1日付けで、ISOから新しい規格「ISO/IEC 27031」が発行された⁽¹⁾。これは情報セキュリティの範疇で策定された規格ではあるが、事業継続に求められるITシステムの対応能力を取り扱うもので、BCMとの関連が非常に高いガイドラインとなっている。

本稿ではこの規格の概要を紹介した上で、BCMとともにITシステムの対応能力の最適化に取り組む意義について、あらためて問題提起したい。

ISO/IEC 27031 の概要

この規格の正式な名称は「ISO/IEC 27031 Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity」（事業継続のための情報通信技術の即応能力に関するガイドライン）である。タイトルから分かるように、この規格はあくまでもガイドラインであり、外部機関による審査に用いられるものではない。

規格本文の中では、タイトルにある「information and communication technology readiness for business continuity」を略して「IRBC」と表記している。これは従来あまり使われていなかった用語であり、この規格の開発によって生まれた用語だと思われる。つまり事業の一部（もしくは大部分）がITに依存しているという状況において、ITシステムがその組織の事業継続のために求められるレベルの対応能力を備えているかどうか、という観点である。ここでいう「対応能力」とは、事故や災害に見舞われてもITシステムがその機能を維持するか、もしくは短期間のうちに再開・復旧する能力を指す。これ以降、本文中ではこれを「IT即応能力」と呼ぶ。また「ITシステム」には単にハードウェアやソフトウェア、通信ネットワークだけでなく、これらを運用するために必要な人員および運用業務等が含まれる。

規格の構成は図1のようになっており、IRBCを組織にとって適切な状態に保つために、どのような取り組みをすべきかが記述されている。

ところで、この規格が取り扱っている範囲は、従来から「ITサービス継続マネジメント」と呼ばれてきたものと同じであると考えてよい。情報セキュリティの範疇では、ISO/IEC 27001において「事業継続管理」というセクションで取り扱われている。またITサービスマネジメントの範疇でも、ISO/IEC 20000およびITIL⁽²⁾において「ITサービス継続性管理」としてガイドラインが示されている。このように従来のISO規格等でフレームワークの一部として扱われてきたものが、独立した規格となった⁽³⁾のは、ITサービス継続マネジメントに対する注目度がより高くなってきた結果であると考えられる。

BCMにおけるIT即応能力が注目される背景

では、BCMにおけるIT即応能力が以前にも増して注目されるようになったのは何故であろうか。もちろんITに対する業務の依存度が高くなった、という点は言うまでもない。今や多くの組織において、業務にITは不可欠であり、ITシステムが停止したら手作業でしのぐという代替手段は、現実的に困難な状況になりつつある。

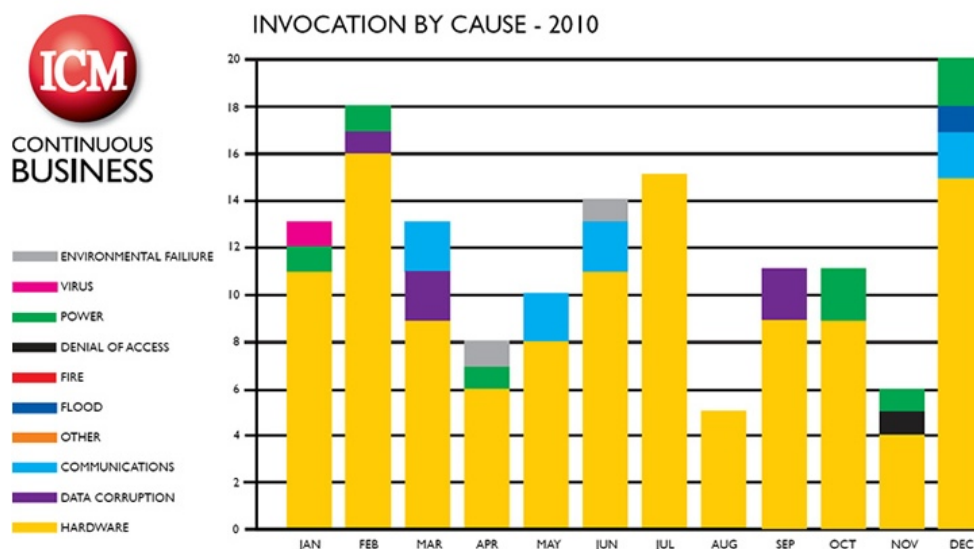
これに加えて、ITシステムの障害によって、実際に事業中断が多数発生しているという現実がある。英国のBCM関連サービス業であるICM Continuity Services社によると、図2で示されているように、2,000社におよぶ同社の顧客において、BCPが発動されたケースの80%以上が、ITのハードウェア障害によるものであった⁽⁴⁾。また英国のChartered Management Instituteが英国内の企業を対象に行った調査⁽⁵⁾によると、実際に発生した業務の途絶⁽⁶⁾の原因として最も多かったものは、2003年から2008年までの間、

「ITの喪失」であった（2009年、2010年は「異常気象」が1位になっているが、これに次いで2位である）。

1. スコープ 2. 引用規格 3. 用語と定義 4. 略語	
5. 概要	5.1 BCMIにおけるIRBCの役割 5.2 IRBCの方法論 5.3 IRBCの要素 5.4 IRBCの成果と利益 5.5 IRBCの構築 5.6 IRBCの構築におけるPDCAアプローチの活用 5.7 経営層の責任
6. IRBCの計画	6.1 概要 6.2 資源 6.3 要件の定義 6.4 IRBC戦略オプションの決定 6.5 承認 6.6 IRBCの対応力の拡張 6.7 ICT即応能力のパフォーマンス基準
7. 実施と運用	7.1 概要 7.2 IRBC戦略の要素の導入 7.3 インシデント対応 7.4 IRBC計画文書 7.5 意識・能力向上、および訓練プログラム 7.6 文書管理
8. 監視とレビュー	8.1 IRBCの保守 8.2 IRBCの内部監査 8.3 マネジメントレビュー 8.4 ICT即応能力のパフォーマンスの測定
9. IRBCの改善	9.1 継続的改善 9.2 是正措置 9.3 予防措置
付属文書A	IRBCと障害発生時におけるマイルストーン
付属文書B	高可用性を備えたシステム
付属文書C	障害シナリオの評価
付属文書D	パフォーマンス基準の開発

（項目名称は筆者による参考訳）

図1 ISO/IEC 27031の項目構成



（出典：Continuity Central - <http://www.continuitycentral.com/news05634.html>）
（図中、黄色で示されている部分がハードウェア障害によるもの）

図2 英国内におけるBCP発動事由の月別推移

日本国内においても、IT システムの障害による事業中断がいくつも発生している。ここ数年の間に、マスコミで報道された大規模なものだけでも、IT システムのトラブルに起因する飛行機や鉄道の運行停止、証券取引所での取引停止、金融機関の業務停止等が発生している。このように日本においても、IT システムの障害による事業中断は、現実に見ても過剰でない頻度で発生しているのである。

ところで、IRBCが「事業継続のためのIT即応能力」であり、かつ日本企業の多くが大規模地震を対象としてBCMに取り組んでいることから、日本企業におけるIRBCは地震に対するITシステムの耐障害性であると考えられる方が多いかも知れない。つまり地震に被災した後の事業継続・再開のプロセスにおいて、ITシステムの故障やトラブルが足を引っ張らないようにすべき、という観点である。もちろんそのような取り組みも必要であるが、必ずしもこれが中心ではないという点を確認しておきたい。なぜなら、上であげた日本における事業中断の事例は全て、地震などの災害とは無関係に発生しているからである。即ち上の事例はいずれも、プログラムの不具合、システムの能力不足、運用業務におけるミス、オペレーションミスなど、ITシステムそのものや管理運用等が原因となっている。つまりITシステムに関する問題によって事業中断が発生しているのである。

したがって日本企業においても、BCMに取り組む際に地震だけに注目し過ぎず、想定すべきリスクを広く捉えるべきであり、特にITシステムとその運用に起因する事業中断リスクについて、あらためて評価すべきである。

IRBC の最適化に取り組む意義と効果

IRBC の最適化とは、組織の事業継続に求められる水準に対して、必要かつ十分な IT 即応能力を備えることである。したがって、組織にとって重要な業務に求められる IT 即応能力を、次のような指標によって明らかにした上で、これらに対して必要十分な準備や対策が行われているか、不足している場合はどのような対策が必要かを検討していくことになる。

RTO : Recovery Time Objective (目標復旧時間)

RPO : Recovery Point Objective (目標復旧ポイント)

MBCO : Minimum Business Continuity Objective (最小事業継続目標)

RTO と RPO については、BCM 関係者にとっては既におなじみの指標であろう。MBCO については ISO/IEC 27031 で、事故や災害等が発生した場合でも、組織が最低限維持したい事業活動のレベルを示すものとして定義されている。これらのうちのどの指標を用いるべきかは組織によって異なるが、このような指標を用いて IT 即応能力に対する要件を明らかにする方法論が、ISO/IEC 27031 では「6. IRBC の計画」で記述されている。

ところで、上のような取り組みの中で、IT 即応能力に対する要件を明らかにするためには、前提としてまず組織において BCM への取り組みが行われ、BIA (Business Impact Analysis : 事業インパクト分析) 等によってビジネスに対する事業継続上の要件が明らかになっていることが必要である。このような BCM への取り組みには、経営層のリーダーシップの元で、部門横断的な取り組みが求められる。したがって IRBC の最適化への取り組みは、IT 部門だけの努力で推進できるものではない。

しかしながら多くの企業では、BCM に取り組む以前から、IT 部門を中心に災害対策・障害対策として、データのバックアップ、ネットワークやサーバの冗長化、耐障害性に優れたデータセンターの活用などが行われ、経営資源が投下されてきた。もちろんこれらの対策の導入にあたっては、必要性や費用対効果について検討が行われてきた筈であるが、ここであらためて BCM および IRBC で提供される方法論を用いて、再評価することをお勧めしたい。

IRBC の最適化が目指すのは、闇雲に IT 即応能力を向上させることではない。もし現状の IT 即応能力が、組織の事業継続に求められる水準を大幅に上回っている場合は、IT 即応能力を下げるという選択肢もある。特に、まだ BCM が一般的でなかった時代から IT の災害対策に取り組んできた企業や、IT 部門が先行・主導して災害対策を進めてきた企業においては、もし現状の IT 即応能力がオーバースペックになっていることが分かれば、コストダウンに繋がる可能性もある。また結果としてコストダウンに繋がらなかった場合でも、現状の IT 即応能力が必要十分であることや、これに投下しているコストが妥当であることについて、より確信を持てるようになるであろう。

これは自社の対策状況や費用対効果の妥当性について、社内外に説明しやすくなることでもある。日本ではまだ、BCM や情報セキュリティに対する投資家や監査役の関心が比較的低いようであるが、欧米の状況から推測すると、近い将来には日本の投資家や監査役も、BCM への取り組み状況や、これが収益に与える影響について関心を持つようになると考えられる。そのような状況に備えて、BCM や IT 即応能力に関する説明責任を果たせるよう、今のうちから少しずつでも準備を進めておきたいものである。

以上

株式会社インターリスク総研
コンサルティング第二部 主任研究員 田代 邦幸
kuniyuki.tashiro@ms-ad-hd.com

[注釈]

- (1) 本稿執筆の時点では ISO または (財) 日本規格協会の Web サイトから購入可能だが、日本語訳はされていない。
- (2) IT Infrastructure Libraryの略で、ITサービスマネジメントに関するガイドラインである。ITIL[®]は英国商務局が所有しており、商標登録されている。ITIL[®] is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom and other countries.
- (3) 英国規格においては、IT サービス継続マネジメントに関する規格として「BS25777」が2008年12月に発行されている。BS25777については以前に『InterRisk Report BCM ニュース<2008 No.4>』(http://www.irric.co.jp/risk_info/bcm/pdf/bcm_news0804.pdf)で紹介しているので、そちらを参照されたい。なお ISO/IEC 27031 の記述内容の多くに BS25777 を踏襲した部分があり、この規格の開発における BS25777 の影響の大きさがわかる。
- (4) Continuity Central の Web サイト (<http://www.continuitycentral.com/news05634.html>) による。
- (5) 『Managing Threats in a Dangerous World - The 2011 Business Continuity Management Survey』Chartered Management Institute、2011年3月
(http://www.continuitycentral.com/Managing_threats_BCM_2011.pdf)
- (6) 「disruption」という表現が使われているので、事業中断に至らないようなトラブルも含まれている可能性がある。

株式会社インターリスク総研は、MS&AD インシュアランスグループに属する、リスクマネジメントについての調査研究およびコンサルティングに関する専門会社です。
事業継続マネジメント (BCM) に関するコンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問い合わせ先、または、あいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合わせ先

㈱インターリスク総研 コンサルティング第二部 BCM第一グループ
TEL.03-5296-8918 <http://www.irric.co.jp/>

本誌は、読者の方々が企業の BCM 取り組みを推進する際に、役立てていただくことを目的としたものであり、事案そのものに対する批評その他を意図しているものではありません。

不許複製/Copyright 株式会社インターリスク総研 2011