

リスクマネジメント最前線

2012-3

東京海上日動火災保険株式会社

企業営業開発部

〒100-8050

東京都千代田区丸の内 1-2-1

TEL 03-5288-6589

FAX 03-5288-6590

<http://www.tokiomarine-nichido.co.jp/>

東京海上日動リスクコンサルティング株式会社

<http://www.tokiorisk.co.jp/>

事業継続マネジメント 国際標準規格 ISO 22301:2012 発行

事業継続マネジメント（以下、BCM）とは、製品の供給やサービスの提供を中断するリスクを管理し、中断事象の発生による影響の軽減や未然防止に取り組むとともに、万が一中断事象が発生した場合の対応計画・復旧計画（事業継続計画（以下、BCP））を策定し、実効性の向上と継続的な改善を進めるための仕組みである。

2012年5月15日に発行された、BCMに関する国際標準規格である「ISO22301:2012 社会セキュリティ-事業継続マネジメントシステム-要求事項」について概要を説明する。

1. 事業継続に関する ISO 化の背景について

大規模な事故・災害等により事業が中断すると、企業の存続を揺るがしかねない大きな問題になることは、阪神淡路大震災で見られた幾多の事例から明らかである。

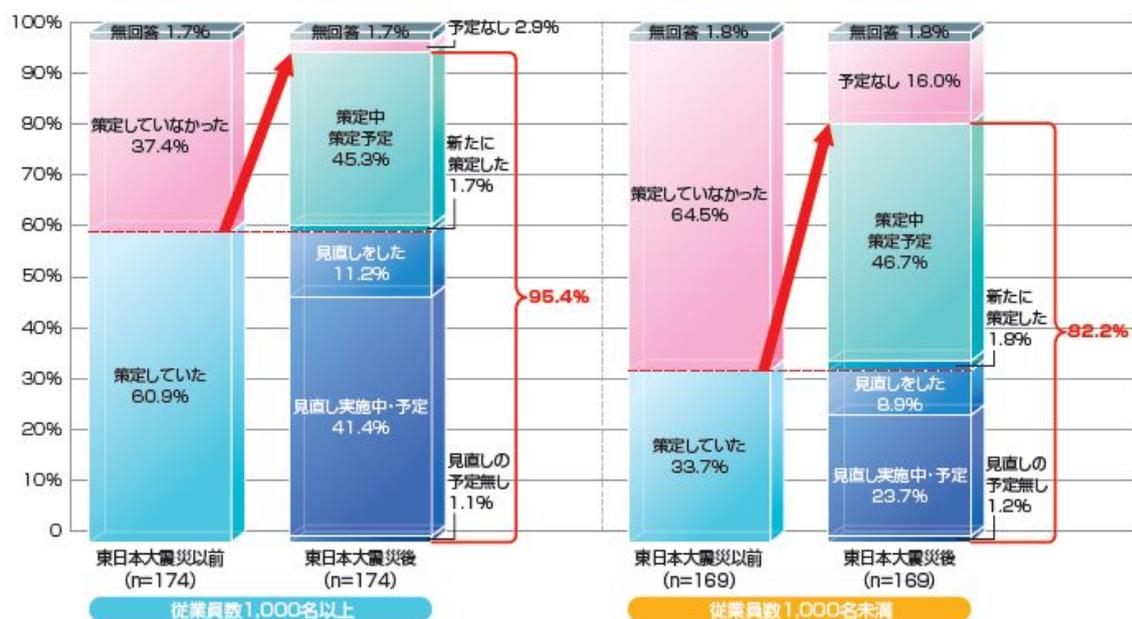
ここで BCM に関する経緯を振り返ると、例えば 1980 年代から金融機関のバックアップシステム構築の動き等がみられることからわかるように、古くから取り組みがなされてきた。また 1990 年代には、工場火災や台湾の地震において事業全体に影響が出る事例が見られたが、当時は社会全体として、すべての企業が BCM の構築に取り組むべきであるとは認識されていなかった。

その後、2001 年に発生した米国同時多発テロでは、ニューヨーク証券取引所が一週間にわたり取引を停止する事態が生じた。これに伴い、欧米においても国家として企業の事業継続の問題に取り組むべきであるという認識がされ、米国からの提案で事業継続に関する国際的な議論が始まるに至った。その後も、2003 年に北アメリカ大停電、2004 年に新潟中越地震における半導体工場の被災、2005 年にカトリナ水害による中断事故等が起こり、BCM の必要性は次第に強く認識されるようになった。

この様な情勢の中で 2006 年に ISO 化の検討がスタートし、2012 年 5 月 15 日、ISO22301 が発行されるに至った。

なお、東京海上日動リスクコンサルティングではこの間、BCMS を始めとする社会セキュリティに関する ISO の検討委員会である TC223 に ISO22301 の日本代表委員を派遣し、ISO22301 の制定に大きく関わった。

現在においては、多くの企業においてBCPの必要性が認識されており、2011年11月の当社調査では、従業員1,000名以上の企業で実に95.4%がBCP策定に向けての取り組みを行っている、あるいは、BCPをすでに策定していることが明らかになった。



出典：東京海上日動火災保険株式会社 「リスクマネジメント動向調査 2011」

2. ISO22301 の特徴

ISO22301は従来のオーソドックスな事業継続（BCP・BCM）の考え方に基づくものになっている。今日までに、内閣府や経済産業省などのガイドラインや英国規格BS25999-2等に準拠して事業継続を構築している企業であれば、これまでの取り組みを生かした上でISO22301の枠組みに合わせていくことが十分に可能である。

一方、ISO22301に特有の事柄として、以下の特徴が挙げられる。

(1) 要求事項を規定している

内閣府や経済産業省および国内の業界向けの事業継続に関する指針類は、ガイドラインであった。ガイドラインとは、読者が事業継続の概要をつかむことが目的であり、例示など参考となる情報を交えつつ出来上りの姿を示すいわば参考書としての位置づけであった。

これに対して、ISO22301は要求事項を規定しているⁱⁱ。

第三者認証制度に活用できることを前提としており、ISO22301では基本を定めることを重視し、各項目も最低限の内容に絞られ、概念統一に基づく簡潔な表現となっている点が大きな

違いである。

そして、品質マネジメント ISO9000 や環境マネジメント ISO14000 などと同様に ISO に基づく第三者認証制度が今後行われていくことが大きなポイントである。

(2) マネジメントシステムである

事業継続の分野に本格的にマネジメントシステムの導入を求めている点も大きな特徴である。

従来の事業継続のガイドラインでも、PDCA の考え方による改善の視点は示されているが、どちらかといえば、BCP の普及に重点が置かれ、BCP の策定までを中心とした記述となっていることが多かった。これに対して ISO22301 では、平時の改善を確実に進めていくことを重視する “マネジメントシステム” の導入を求めている。

ISO22301 では、演習・試験、対応策の運営、パフォーマンス評価・マネジメントレビュー、是正処置など、策定後の維持改善のための基本設計をより具体的に示している。

これにより、計画が策定されていれば良いという時代が終わり、組織に定着させていくことが求められる新しい時代に差し掛かったことになる。

(3) リーダーシップの重要性

事業継続を成功させるために重要なポイントは、有事（インシデント発生時）においても、平時の改善においても経営の意思に基づいているか否かにある。ISO22301 では、5 章に “リーダーシップ” という題で、トップマネジメントの事業継続マネジメントシステム（以下、BCMS）における責任と役割を明示している。事業継続を検討するために経営の方針や組織の置かれている状況を十分踏まえた上で、経営トップの強いリーダーシップの下に取り組みを推進していくことが明確に求められている。

ISO 22301 の構成

| | |
|------------------------|------------------------|
| 1 適用範囲 | 7 支援 |
| 2 引用規格 | 7.1 資源 |
| 3 用語及び定義 | 7.2 力量 |
| 4 組織の状況 | 7.3 認識 |
| 4.1 組織とその状況の理解 | 7.4 コミュニケーション |
| 4.2 利害関係者のニーズ及び期待の理解 | 7.5 文書化した情報 |
| 4.3 マネジメントシステムの適用範囲の決定 | 8 運用 |
| 4.4 事業継続マネジメントシステム | 8.1 運用の計画及び管理 |
| 5 リーダーシップ | 8.2 事業影響度分析及びリスクアセスメント |
| 5.1 一般 | 8.3 事業継続戦略 |
| 5.2 経営者のコミットメント | 8.4 事業継続手順の確立及び導入 |
| 5.3 方針 | 8.5 演習及び試験の実施 |
| 5.4 組織の役割、責任及び権限 | 9 パフォーマンス評価 |
| 6 計画 | 9.1 監視、測定、分析及び評価 |
| 6.1 リスク及び機会に対応するための処置 | 9.2 内部監査 |
| 6.2 事業継続目的及び達成計画 | 9.3 マネジメントレビュー |
| | 10 改善 |
| | 10.1 不適合及び是正処置 |
| | 10.2 継続的改善 |

(4) パフォーマンスに関する評価が充実

ISO22301 では実効性の確認と維持を重要視しており、事実上三つのパフォーマンスに関する評価が求められている。

① 事業継続手順の評価 Evaluation of continuity procedures

この項目では文書の定期的な見直しによる取り組みの見直し、事故・災害が発生した場合の災害対応に関する目標の達成状況の評価を求めている。

② 演習 (exercising) と試験 (testing)

事業継続手順が実際に機能する手順となっているかを確認する試験と、基本的な手順の習得と応用力を確認するための演習を行う。品質マネジメントや環境マネジメントなどと異なり、事業継続はインシデント発生時の対応水準を向上させるための取り組みである。インシデントは普段は発生しないため、日常の取り組みで実際に BCP が機能するか、否かの判断や評価が難しい。そのため ISO22301 では演習と試験に着目し、その結果の評価と、対応水準を確認することを求めている。

③ PDCA プロセスに関するパフォーマンス評価

マネジメントシステムつまり、PDCA を構成するそれぞれのプロセス（定期的な計画の見直し、演習・試験、内部監査、マネジメントレビュー、是正処置等）がそれぞれ当初の意図通りの成果を出しているかをモニタリングするものである。

例えば、年初に取り組みを予定した際の意図通りに、取り組みが進んでいるかを都度評価することが求められていると考えるとわかりやすい。

(5) 二つのキーコンセプト 優先順位と時間

ISO22301 で用いられている事業継続に関する言葉の定義のうち、ISO22301 のコンセプトを象徴する二つのキーワードを紹介する。

① 優先順位付けされた活動 Prioritized Activity

これは従来よく知られた用語でいうと、“重要業務”に相当する。ISO22301 は、業務を再開していく際にどのような順番で業務を再開するべきなのかという点に注目して議論を整理している。このコンセプトに基づき、Prioritized Activity という表現がされている。

② 時間枠 Time Frame

従来良く知られた用語でいうと、“目標復旧時間”などにあたる。世界の先行した規格やガイドラインでは事業継続の取り組みのポイントは中断事象が発生した場合のスピードの改善にあると考えられている。事業継続に関する様々な業務は必ずいつまでに実施するかという時間枠の管理に基づいて行う必要がある。そこで、ISO22301 では時間に関する概念が複数提示されている。その代表的な表現が、時間枠 (Time Frame) である。

3. 企業への影響・効果

(1) 利害関係者からの認証取得要請

本規格は、第三者認証規格であるため、従来の品質マネジメントや環境マネジメント、情報セキュリティマネジメントなどの第三者認証制度を持つ ISO と同様、各企業がその取引先の選定条件、評価条件に ISO22301 の認証取得の有無を加えることは十分に考えられる。

また、取引先と相対で個別に取引先評価・事業監査などを行う場合に当事者間の評価基準の考え方として ISO22301 が取り入れられていくことも十分考えられる。また、第三者認証を取得せずとも、自己適合宣言を行って取引先にアピールする企業も現れるであろう。

一方、事業継続に関する第三者認証制度の評価には、留意点も存在する。

例えば、事業継続の場合、第三者認証制度は、直接的に事業継続の達成を担保しているわけではない。マネジメントシステムの第三者認証は企業が事業継続のために自ら定めたルールを達成するために誠実に努力をつづけている企業であるか否かを評価するものである。つまり、認証の取得が、災害時に事業継続が確実に履行されることを担保するものではない点である。

さらに、ISO22301 の認証審査は、それぞれの取り組み主体が優先業務であると考えた業務を自ら定めた時間枠で再開させるための取り組みがなされているかを評価するものである点もある。このことは、裏を返せば、認証取得にあたっては、優先業務以外について早期再開させるための取り組みを定める必要はないことになる。

そのため、取引先の評価等に ISO22301 の取得の有無を入れる場合、自社が求めている製品・サービスが相手先の優先業務に含まれているのか否かという点は忘れずに確認する必要がある。

(2) 維持管理に重点を置くマネジメントシステム導入の効果

第三者認証を取得するか否かは別として、ISO22301 を参考にし、BCMS を導入する効果は大きい。従来の日本企業では計画を作るところまでは熱心であっても、その後の改善の推進、計画の改訂等に弱点があることが多かった。

例えば、経済環境の変化の中で主力製品の変化や、事業ポートフォリオの変化があっても、なかなか計画の修正がされない、BCP を作ってはみたもののその後の定期的な教育がされていないなどはその典型例である。

当然ながら、これらの変化に合わせて BCP を更新しておかなければ、万が一のときに機能しない。このような事態を防ぐために、定期的な取り組みのモニタリングと見直しを会社の運営の仕組みとして組み込むマネジメントシステムは有効である。

4. 最後に

東日本大震災やタイの水害などの経験により、自社のみならずサプライチェーンも含めた事業継続に取り組む必要性を認識した企業も多い。

サプライチェーンに依存して製品・サービスの提供を行う企業において、事業継続を図る場合、それぞれの企業が事業継続を達成しそれが連鎖する必要がある。そのためには、自社のサプライチェーンを構成する各企業の個々の BCP で優先業務とされる製品やサービスの内容と時間枠について把握し管理することが必要である。今回の標準化はこの事業継続水準の摺合せを実現する物差しを提供している。特に、グローバルに活動する企業にとっては、地域ごとに事業継続に関する異なる考え方を一本化していくことは大きな課題であった。

サプライチェーン全体の事業継続を強化させることにより、はじめて企業の供給責任を果たすことが確実になる。おりしも、日本企業の東日本大震災からの復旧の早さには称賛の声が世界の経済界から挙がっている。今後は事業継続を実践することにより被災後の早期復旧という現場力の強さに加えて、あざやかに製品・サービスの供給を再開ができれば、さらなる付加価値の向上につながる。そのための取り組みをより確かに進めていく方法を示す ISO22301 は、検討する価値がある規格といえるであろう。

(2012年5月25日発行)

ⁱ 規格は、ISO の出版物として位置づけられるため、「発行」と表現される。

ⁱⁱ BCM に関する認証規格としては、これまで英国規格である BS25999-2 で、第三者認証制度が運営されてきている。既に日本でも英国に習って JIPDEC (一般財団法人日本情報経済社会推進協会) が BS25999-2 の第三者認証を行っている。今後、全世界で ISO22301 の第三者認証制度の本格運用に伴い、BS25999-2 の認証は ISO22301 の認証に移行する予定となっている。