



055 JAPAN



寄稿：(株)インターリスク総研  
小林 誠氏

## ASIS インターナショナル日本支部便り

### 「リスクマネジメントの国際標準化～未来の不確かさにどう対応するか～」

5月の月次セキュリティミーティングでは、株式会社インターリスク総研研究開発部部長 小林誠氏に、リスクマネジメントの国際標準化と題して、講演をいただきました。小林氏は、リスクマネジメントの国際標準化にかかるリスクマネジメント規格国内委員会のワーキンググループ委員として、国際標準化の当初より関わってこられた方です。

小林氏には、講演内容の概要について寄稿していただきました。以下はその内容です。(以下、寄稿文)



#### ■ ISO31000 の公表

2009年11月中旬に ISO31000:Risk management – Principles and guidelines とリスクマネジメントの用語の定義集である ISO Guide73 が ISO(国際標準化機構)より正式に公

表された。開発の決定から約4年かかったプロジェクトであった。この規格開発に関しては国内でも委員会が組成され、継続的に審議が行われてきた。

このリスクマネジメント規格の特徴は、企業等組織のリスクに焦点を絞り、組織経営のための取り組みプロセスを明確化したことであり、今後企業等が組織全体のリスクマネジメントを推進していく際の有用な指針となることが期待されている。

国内では、この規格をベースに JISQ31000 の審議が行われ、今年の12月に国内規格の整備も完了する予定である。

#### ■ ISO31000 におけるリスクとは

リスクに関して、ISO31000の序文は次のように述べている。

あらゆる業態及び規模の組織は、自らの目的達成の成否及び時期を不確かにする内部及び外部の要素及び影響力に直面している。この不確かさが組織の目的に与える影響を“リスク”という。

この規格の書き出しは次の点でリスクについての新しい視点を含んでいる。

- 1) この規格が目しているのは企業等の組織にかかるリスクであること
- 2) 組織が組織として社会において存在するため

の十分条件である「組織の目的の達成」を重要視し、ISO としてはその目的の達成に影響を与える可能性のある不確実性に関するマネジメントの方法論の標準化を目論んだこと

つまり、ISO リスクマネジメントは企業等の組織経営のための手法という認識が標準化の根底にある。こうした経営のためのリスクマネジメントという理念を達成するために、ISO31000 の制定に伴い、2002年に策定されたリスクマネジメントに関する用語の定義集、ISO/IEC Guide 73 を改定し(ISO Guide 73 として公表)、リスクの定義を大きく変えたのである。

### ■リスクマネジメントの11の原則

ISO31000 は、リスクマネジメントに関する原則及び一般的な指針を提供する規格である。この規格ではリスクマネジメントを「リスクに関して組織を管理・統制するための協調的な活動」と定義しているが、その構造は①リスクを運用管理<sup>1</sup>するための原則、②それを取り巻く枠組み、及び③リスクマネジメントプロセスの三つの要素から構成され、それらを順守することによって、リスクを効果的に運用管理することができるとしている。

この三要素の中で基本として重要なものが「リスクマネジメントの原則」である。

リスクマネジメントは...

原則1: 価値を創造し、保護するもの

原則2: 組織のすべてのプロセスにおいて不可欠な部分である

原則3: 意思決定の一部である

原則4: 不確かさに明確に対処するもの

原則5: 体系的かつ組織的で、時宜を得たもの

原則6: 最も利用可能な情報に基づくもの

原則7: 組織に合わせて作るもの

原則8: 人的及び文化的要素を考慮に入れるもの

原則9: 透明性があり、かつ、包含的なもの

原則10: 動的で、繰り返し行われ、変化に対応するもの

原則11: 組織の継続的改善を促進するもの

どのような組織でも程度の差こそあれ、リスクマネジメントを行っているが、ISO では、リスクマネジメントを効果的なものにするために組織のマネジメントがはじめに指令及びコミットすべき11の原則を確定した。

これはリスクマネジメントの目的ではなく、リスクマネジメントにおける行動の基礎・基盤である。組織はこの原則を念頭に入れ、リスクマネジメントを効果的なものにするために組織に展開していくことを求めている。

この11の原則は玉石混淆である。ISO リスクマネジメント特有のものも、そうでない当たり前のことも混じっている。従来のリスクマネジメントの原則と異なり、かつ私たち日本人にとって新鮮なものは、原則1、2、3、5及び11ではないだろうか。そのなかでも特に、原則1の「好ましい影響」も対象としたリスクマネジメントのあり方と原則11の「成熟度」に基づく継続的改善に注目してほしい。

ISO31000 では、リスクを不確かさの組織の目的に対する影響と定義したが、その影響には「好ましい影響」も含まれる。このため、組織はリスクマネジメントの実践における不確かさへの十分な対応

等により事業の成功をもたらすことができる。この事業の成功により企業等組織の価値は増大、創造しうる。これがリスクマネジメントの「好ましい」影響であり、「リスクマネジメントは、組織の目的の明確な達成に寄与するもの」と規定した所以である。

一方、「好ましくない」影響への対応を誤ると企業等組織の価値は減少し、保護することが難しくなる。従来の危機管理やリスクマネジメントで行われてきたことである。原則1はリスクマネジメントには「価値創造」と「価値保護」の二つの側面があることを規定したものである。

また、めったに顕在化しないリスクに関するフレームワークの有効性を見直すためには従来のPDCAサイクルだけでは十分ではない。このため原則11では、「成熟度」という考え方を導入して継続的改善を図ることを求めている点も新しい。

### ■リスクマネジメントの枠組みとは

ISO31000は、本来、リスクマネジメントのプロセスを規定する規格として策定される予定であった。いわゆる「プロセス規格」である。しかしながら、2005年から始まったISOにおける審議の過程において、そのリスクマネジメント・プロセスを効果的に運営するための「仕組み」が組織内に必要であるとの認識が提案され、了承された。これが「リスクマネジメントの枠組み(フレームワーク)」である。

「枠組み」とは、リスクマネジメントを組織のすべての階層に定着させるための基盤や組織体制の整備をいい、リスクマネジメントがうまくいくか否かは、その有効性にかかっている。いいかえれば、枠組みが機能することによって、リスクマネジメント・プロセスの適用にもとづくリスクの運用管理が効果的に行えるのである。

また、枠組みがあることによって、リスクマネジメント・プロセスから出てくるリスク情報は組織内で共有され、意思決定とアカウンタビリティ確保のための基礎情報として活用可能となるのである。

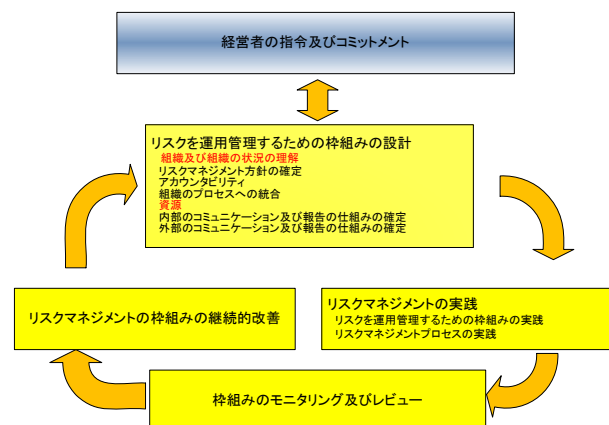


図 リスクマネジメントの枠組み

「リスクマネジメントの枠組み」の内容は、JISQ2001で「リスクマネジメントシステム」と呼ばれた仕組みに大変似ているが、ISO31000の利用者に認証を意識させないことや組織の負荷をなるべく少なくするという観点から限定的なものにとどめている。

そのため、ISO31000を用いて、リスクマネジメントシステムを構築しようとする場合には、上記に示したリスクマネジメントの枠組みの構成要素に次の項目を加えて、適用することによりその整合性を取らなければならない。

- 教育・訓練
- 文書管理
- リスクマネジメントシステム監査
- 組織の最高経営者によるレビュー

なお、これらの追加の要素に変えて、JIS Q 9001、JIS Q 14001 や JIS Q 27001 などの構成要素を参考にしても効果は同じである。自社のマネジメントシステムの導入状況に応じて対応することが望ましい。

### ■リスクマネジメント・プロセス

リスクマネジメントのプロセスについては、さまざまな分野で独自の分類方法が提案されてきた。

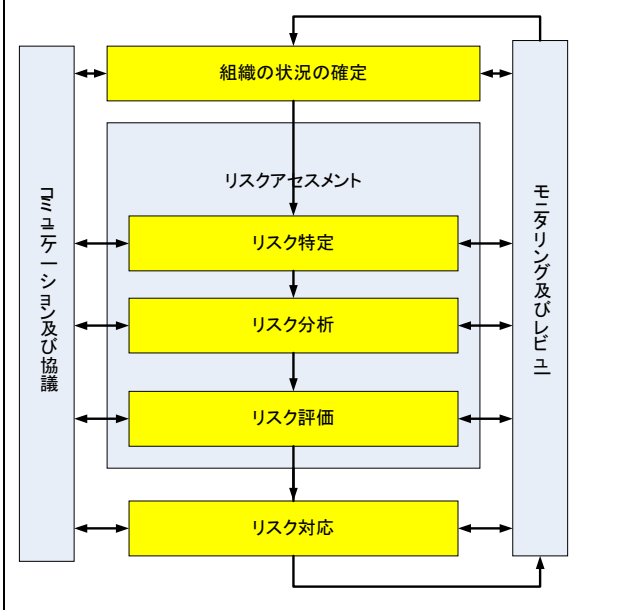
どのリスクマネジメント・プロセスの考え方も似たり寄ったりで、それを最も単純化すると、①リスク特定(発見)、②リスク評価、③リスク対応の3つに集

約できる。

しかしながら、ISO31000 では、分野を問わずに適用可能なプロセスを検討し、その定義と構成要素を次のように規定した。

定義:コミュニケーション、協議及び組織の状況の確定の活動、並びにリスクの特定、分析、評価、対応、モニタリング及びレビューの活動に対する、マネジメント方針、手順及び実務の体系的な適用。

構成要素:



リスクマネジメント・プロセスのなかで、わが国では初めての概念が「組織の状況の確定」である。このプロセスは、組織の目的を明確に表現し、考慮すべき内部及び外部の要因を把握し、以降のプロセスに関する適用範囲及びリスク基準を設定することを目的として行うものである。

この活動は、リスクマネジメント・プロセスの2番目の活動であり、リスクマネジメントの枠組みにおける「組織の状況の確定」と内容もほぼ同じであり、規格制定に当たっても重複しているとの批判があった。

状況(context)とは、環境(environment)のことである。自然環境の環境ではなく、組織を取り巻く環境や組織内の業務遂行等の環境のことである。

ISO 31000 でも非英語圏に配慮して、contextの代わりに environment を使おうという意見が出されたが、時間切れでそのままになっている。

この「環境」を把握するするためには次のようなことを実施しなければならない。

- ・ステークホルダの特定及び分析(前工程)
- ・SWOT 分析
- ・リスク基準の決定

### ■終わりに

標準化とは直接関係ないが、リスクとは未来のことである。まだ問題として顕在化していないことである。したがって、リスクマネジメントとは組織の未来を運用管理することであり、現在すでに起きている問題解決とは少し違うものである。わが国ではすでに起きている「問題」とまだ起きていない「リスク」が混同されることが多いので注意が必要である。

また、ISO31000 という規格は、組織のリスクを対象にしており、個人のリスクという発想はない。このため、ISO リスクマネジメントは経営のためのものといってよい。

そのため、経営者はリスクマネジメントの実践に人と予算を投入する責務があり、また、経営者はリスク対応に失敗したら、責任を取ること (Accountability) を自覚して取り組むべきである。

マネジメントの原義は「難しいことをうまくやる」ということであり、マネジャーはそうできる人のことである。単なる管理者ではない。マネジャーはリスクを察知できるようリスク感性を磨く必要がある。

ISO31000 によって、外形標準はできた。今後、各組織が中身を組織に合わせて作ることを期待する。(小林氏投稿 終わり)

### ■ ASIS インターナショナル日本支部の月次セミナーへのお誘い

一般社団法人 ASIS インターナショナル日本支部は、月次セミナーを開いています。産業セキュリティに興味がある方ならどなたでも参加できます。お申し込みはホームページから！

■ 開催日

毎月第三火曜日 午後 6 時半より

■ 場所

国際文化会館(六本木)

東京都港区六本木 5-11-16

TEL: 03-3470-4611

<http://www.i-house.or.jp/jp/ihj/access.html>

■ 参加費

2,000 円 (ASIS 会員・非会員同一料金)

このコーナーへのお問い合わせや入会お申込みは  
一般社団法人 ASIS インターナショナル日本支部  
事務局まで

〒101-0021 東京都千代田区外神田 2-2-17  
日本保安人事株式会社内  
TEL 03-3255-3468 FAX 03-3258-7630  
E-Mail [info@asis-japan.org](mailto:info@asis-japan.org)  
[www.asis-japan.org](http://www.asis-japan.org)

---

<sup>i</sup> ISO31000 では組織への好ましい影響も好ましくない影響も対象としているので“manage”は「運用管理」と訳されている。