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

TRC EYE Vol. 284

東京海上日動リスクコンサルティング（株）
ビジネスリスク事業部　グローバルグループ
研究員　高村早織

先手を打つリスクマネジメント　～リスク先行指標の活用～

2011 年 3 月の東日本大震災、同年秋のタイにおける大洪水など大規模自然災害の頻発、技術革新に伴う新たなリスクの出現、各種規制環境の変化など、企業経営を取り巻くリスクは益々増大している。このような状況に対応するためには、企業におけるリスクマネジメントも、その方法論の高度化を図っていく必要がある。

リスクマネジメント高度化の一つの方向性として、「リスク顕在化の予兆を把握する」アプローチが存在する。「リスク顕在化の予兆を把握する」ことが可能になれば、事前に対策を講じることによって、その顕在化を防止する、あるいは顕在化した場合においてもその被害を軽減することが可能になる。

例えば、タイにおける洪水被害を振り返ってみると、2011 年 10 月のバンコク近郊の工業団地等での浸水被害の発生に至る以前に、「5 月の降雨量が過去 30 年間でトップクラスとなった」、「8 月には流域のダムの貯水量が計画値を上回り始めた」など、いくつかの予兆となる事象を見出すことができる。結果論にはなるが、これらの予兆が把握された時点で、代替生産体制の立案や重要設備の退避等の策を講じていれば、企業経営への影響を軽減することができた可能性がある。

このような「リスク顕在化の予兆を把握することで、その顕在化を防ぐ」＝「先手を打つ」リスクマネジメントを実践するための手法の一つとして、リスク発生に先行して起こる事象を特定し、その変化を指標として把握することで、リスク顕在化の予兆を発見するという方法が挙げられる。本稿では、リスク発生の先行事象の変化を示す指標を「リスク先行指標（RPI: Risk Precursory Indicator）」[1]と定義し、その活用法について概説する。

1. リスク先行指標の定義

本稿ではリスク先行指標（RPI）を以下の通り定義する。

- 組織に影響を及ぼす純粋リスク（損失のみを発生するリスク）の、
- 将来における顕在化の予兆を示す、
- 定量的、準定量的な指標

上述したタイ洪水被害の例で概説しよう。タイ洪水では浸水被害に至る前に「降雨量の増加」、「ダム貯水率の増加」、「河川水位の上昇」などのいくつかの先行する事象（予兆）が存在していた（図 1 参照）。

図 1　洪水被害の発生とリスク先行指標（RPI）

[1]本稿の「リスク先行指標」とは、米国 COSO（Committee of Sponsoring Organizations of the Treadway Commission）のディスカッションペーパー「DEVELOPING KEY RISK INDICATORS TO STRENGTHEN ENTERPRISE RISK MANAGEMENT」に提示された KRI（Key Risk Indicator）という概念を参考に、それを自然災害等の損失のみを発生させるリスク（純粋リスク）に適用する際の方法論に着目したものである。ただし、リスクについては頻度や影響度など様々な評価指標があるため、その中でも「リスク顕在化の予兆を把握する」という特性を強調すべく、「リスク先行指標」（RPI）という名称を提起している。

この例で言えば、これら「降雨量」「ダム貯水率」「河川水位」が「浸水被害の発生」というリスク顕在化の予兆を示す RPI の候補として挙げられる。すなわち、これらの変化を事前に把握しておけば、洪水による浸水被害の発生を予測し、その影響をコントロールするための対策を講じられる可能性があったと考えられる。

リスク発生の予兆を察知しようとする取組み自体は決して新しいものではない。しかしながら、これまでの取組みは熟練の担当者の勘や経験に基づくものが多かったように考えられる。RPI の活用は、このような取組みを明確化・体系化して、組織全体で予兆を拾い上げ、組織を取り巻くリスクの将来動向をより網羅的・効率的につかむことを可能にするものである。

なお、多くの組織で活用される指標の 1 つに重要業績評価指標（KPI：Key Performance Indicator）がある。KPI と RPI は対照的な関係にある。RPI が「組織の将来の目標達成状況を事前に評価する指標」であるのに対し、KPI は「組織の現時点までの状況を事後的に評価する指標」であり（表 1）、図 1 の事例で言えば、「物的損害」「事業中断による損害」がそれに相当する。

表 1　リスク先行指標（RPI）と KPI の比較

リスク先行指標（RPI）	重要業績評価指標（KPI）
・将来、組織の目標達成状況がどのように変化しうるのかを事前に評価する指標 ・組織の**将来の状況**（純粋リスクの発生状況）を推測する	・組織の現時点までの目標達成状況を事後的に評価する指標 ・組織が**現在おかれている状況**（純粋リスクの発生状況も含む）を把握する

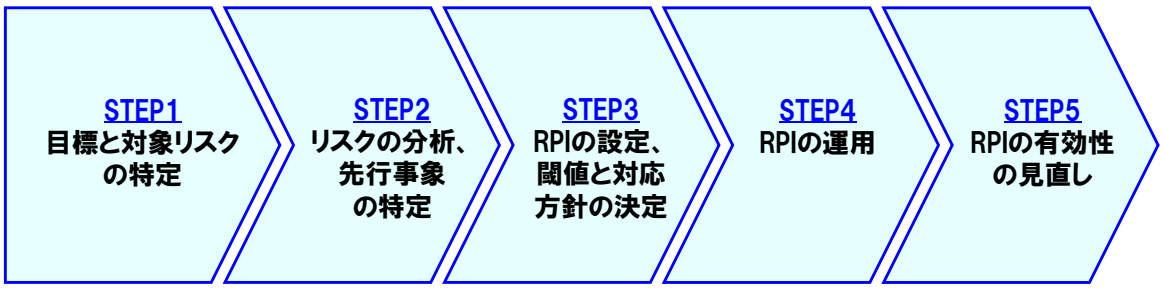
KPI は、現在の目標達成状況を確認し経営を改善していく上で重要な評価指標であるが、事後的な評価であるためにリスク発生に先駆けて対策を講じることは難しい。

RPI には KPI のこのような欠点を補完する効果が期待される。事前にリスク発生の兆しを把握し、迅速な予防的対策を講じることで、リスク顕在化の防止や顕在化した際の被害軽減につなげること、すなわち「先手を打つ」リスクマネジメントの実践が可能になるからである。

2. リスク先行指標（RPI）の導入と活用

それでは、実際に RPI を導入して有効に活用するためにはどうしたらよいのだろうか。本節では、RPI を導入し、有効に活用するための方法論と留意事項を説明する。

図 2　リスク先行指標（RPI）導入のステップ



【STEP1】目標と対象リスクの特定

RPI の役割は、組織の目標達成に影響する純粋リスクについて、その発生の予兆をつかむことである。そのため、最初に組織の目標と、その達成に影響するリスクを明らかにする必要がある。リスクマネジメント活動の中で既にリスクの洗い出し、頻度・影響度の評価が実施されている場合には、この結果がリスクを特定する際に有用となる。

また、STEP2 以降においては、リスク管理部門だけでなく、実際の業務について深く理解している事業部門の協力が必要不可欠である。従って、取組みを始める際には、経営トップから RPI 導入の重要性について強いメッセージが発信されることが望ましい。

【STEP2】リスクの分析、先行事象の特定

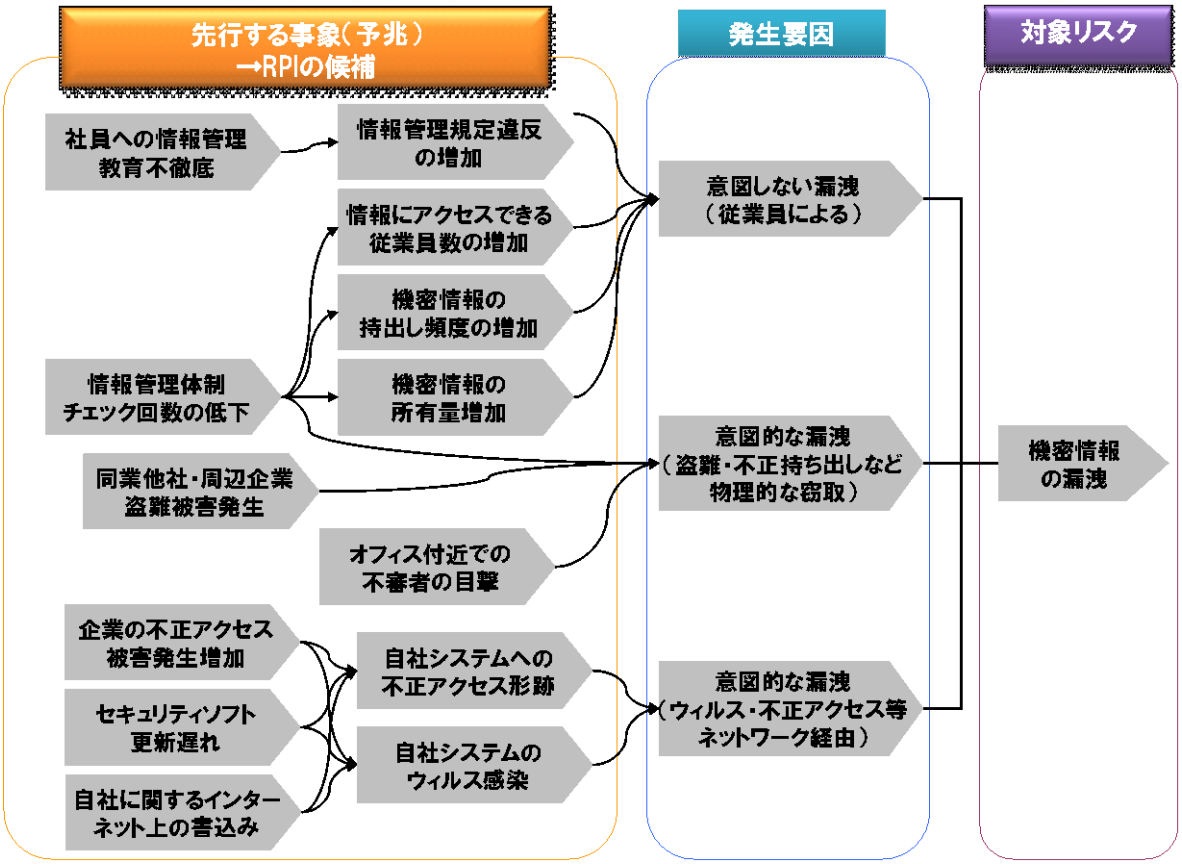
次に、対象とするリスクについて、発生要因や発生前の状況を遡って分析し、リスク顕在化へとつながる先行事象（予兆）を特定する。

本プロセスを、ここでは「機密情報の漏洩」のリスクを例に概説したい。新技術や新製品に関わる重要情報、付加価値の高いサービスの開発や顧客管理等のために所有する個人情報等の漏洩は、多くの組織にとって利益やシェアの拡大、持続的な成長といった重要な目標を妨げうる重大なリスクである。

まず、漏洩の発生要因は、意図しない漏洩と意図的な漏洩（重要書類の盗難や不正持ち出し、不正アクセス等のインターネットを介した漏洩）とに分類される。さらに、これらの発生要因について、組織内で過去に発生したヒヤリハット事例や他社の事故事例等を分析することで、先行事象（予兆）が明らかになる。

以下の図は、「機密情報の漏洩」の発生要因、先行事象（予兆）についての分析例である。漏洩が発生する前には、「機密情報にアクセスできる従業員が不必要に多かった」、「情報管理についての社員教育が徹底されていなかった」、「企業における不正アクセス被害が増加していた」、「インターネット上での（サイバー攻撃を暗示するような）書き込みが複数件見つかっていた」などの事象が発生している可能性がある。このようにして浮かび上がった様々な事象を「機密情報の漏洩」の先行事象として特定するのである。

図３　「機密情報の漏洩」の発生要因・先行事象（予兆）



【STEP3】RPI の設定、閾値[2]と対応方針の決定

STEP2 の先行事象（予兆）のうち、指標化やデータの観測が可能で、リスク発生を予測する上で有効と考えられるものを RPI として設定する。設定した指標についてデータの推移を観測し、継続的に状況を把握することにより、リスクが顕在化する前に予兆をつかむことが可能となる。

ここで重要なのは、各指標に対し、これ以上（または以下）になると組織の目標達成への影響が

[2] 「閾値（しきいち、いきち）」とは、その値の上下で判定や対応が異なるような境界の値を意味する。

無視できなくなると考える閾値と、閾値に達した場合の対応方針を事前に決めておくことである。というのは、これらを事前に決定していなければ、データを観測する中で予兆を見つけたとしても、どの程度の値となったらリスク顕在化の可能性が高まっているのか、あるいは、どのような予防的対策をしたらよいのかを決断することができず、対策が後手に回ってしまう恐れがあるからである。

閾値と対応方針を決定して初めて、RPI が本来の役割を果たし、発見した予兆をリスク発生の影響をコントロールするための活動へとつなげていくことが可能となる。閾値の決定にあたっては、過去のリスク顕在化事例等を分析し、リスクが発生する前に RPI のデータがどのように推移していたのか、どのような値だったのかを参照または推測することが有用だと考えられる。

以下の表は、「機密情報の漏洩」についての RPI・閾値・対応方針の例である。

表 2　リスク先行指標（RPI）・閾値・対応方針の例

先行事象（予兆）	RPI	閾値	対応方針
情報にアクセスできる従業員数の増加	アクセス権限を持つ従業員数	○○人	・当該情報の管理体制強化 ・アクセス権の見直し
情報管理規定違反の増加	違反発生件数（月間）	××件	・メール等での注意喚起 ・臨時の社員教育の実施
企業の不正アクセス被害発生増加	被害発生件数増加率（月間）	△△%	・新たなセキュリティ対策の導入

【STEP4】RPI の運用

STEP3 で RPI・閾値・対応方針を決定したら、実際に RPI の運用を開始する。

表 2 で示した RPI の例では、アクセス権限を持つ従業員数と情報管理規定の違反発生件数については社内情報、企業の不正アクセス被害については警察機関が発表する統計等の外部情報を活用してデータの観測を行うことができる。データの観測は、リスク管理部門、対象とするリスクとの関連が深い事業部門などの担当者が行うことが想定される。

RPI のデータの観測を続ける中で閾値に達していることが判明した場合には、事前に決定した方針に基づく対応を実施することになるが、そのためには適切なタイミングで適切な関係者に情報を伝えることも重要である。現場マネージャーや経営層などの職位に応じて、定期的な報告と、データに急激な変化が見られた場合等の臨時の報告の両方が円滑に行われるよう、体制を構築しておくことが望ましい。

なお、RPI 以外の評価指標についても言えることであるが、有効活用のためにはデータの信頼性の確保と、取扱いに対する関係者の正確な理解が必要不可欠である。というのは、不確かな情報源の使用や、取扱いへの理解不足からデータ間の無意味な比較をしてしまうことは、貴重な時間と労力の無駄となるだけでなく、重要な意思決定を攪乱してしまう恐れさえあるからである。

【STEP5】RPI の有効性の見直し

RPI の有効性を確保するためには、リスクマップ更新に合わせて一年に一度見直すなど、定期的な見直しの機会を確保する必要がある。それ以外にも、RPI のデータが閾値に達し、対応した場合など必要に応じて見直しを行う。

具体的には、蓄積された RPI のデータとリスク顕在化状況の関連性を分析し、RPI・閾値・対応方針が妥当なものであるかを検討する。分析の結果、ある RPI がリスク発生を予測する上で他の指標に比べて有効性が高いと評価される場合には、当該指標に重み付けをするという選択肢もある。検討の結果、必要な改善点を反映し、再度 RPI の運用を続ける。

例えば、「情報管理規定の違反発生件数（月間）」という RPI について考えてみる。発生件数が閾値を超えたことを受けて注意喚起や社員教育を行ったが、実はこれらの対応を実施する前に、あと一歩で機密情報が漏洩してしまうという重大なインシデントが発生していたとする。違反発生件数という指標はリスクの顕在化を予測する上で有効な指標であると言えるが、閾値についてはもう少し低く設定し、重大インシデントが発生する前に対応できるように改善する必要性があるかもしれない。

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

3. おわりに

リスク先行指標（RPI）は、組織の目標達成に影響する純粋リスクについて、その発生や変化を予測するためのツールである。RPI を上手く活用し、「先手を打つ」リスクマネジメントを実践することができれば、組織はリスクの変化に対して迅速に反応し、不測の事態を回避することが可能になる。

また、2009 年に発行されたリスクマネジメントの国際規格である ISO31000 がリスクを「諸目的に対する不確かさの影響」と定義しているように、リスクとはその影響の良し悪しを問わず、目的の達成に影響する全ての不確実性であると捉えることができる。本稿では、純粋リスクを対象に RPI の活用について概説したが、事業リスク等の利益と損失の両方を発生しうる投機的リスクについても、リスク顕在化の予兆を把握することで、損失の軽減だけでなく、新たな戦略を展開するための好機の発見が可能になると考えられる。

さらに、RPI の導入には副次的な効果も期待される。対応を開始するための閾値は、同時に組織が許容できるリスクを示すものである。そのため、閾値の決定はリスクマネジメントを行う上で重要となる組織のリスク選好度を改めて見直す機会にもなる。さらに、RPI のデータを蓄積・更新していくことで、リスクについて担当者・管理者・経営層の円滑なコミュニケーションが促進されることも考えられる。

組織に様々な効果をもたらす RPI であるが、最大限に活用していくためには、経営層がその必要性を強く発信し、全関係者の協力のもとに設定・運用されること、確かな情報源を確保し、関係者が内容を正しく理解すること、予測ツールとしての有効性を継続的に見直していくことが必要不可欠である。

■参考文献

1.「DEVELOPING KEY RISK INDICATORS TO STRENGTHEN ENTERPRISE RISK MANAGEMENT　How Key Risk Indicators can Sharpen Focus on Emerging Risks」Mark S. Beasley, Bruce C. Branson, Bonnie V. Hancock
2.「標的型サイバー攻撃の事例分析と対策レポート」独立行政法人情報処理推進機構
3.「ISOGuide73:2009 Risk management-Vocabulary リスクマネジメント－用語」日本規格協会