TRS におけるリスクマネジメント
の観点からのコンプライアンス

ツクバリカセイキ株式会社

筑波大学

第三学群社会工学類

金井　智史

１．序論

近年の企業の不祥事による信用失墜は企業の存続すら危うくする大きなリスクであるという考えが広まってきている。そのためリスクマネジメントとしてコンプライアンスが重要視されるようになってきた。しかし中小企業の多くは生き残るために社会正義よりも利益を優先せざるを得ず、コンプライアンスを考える余裕がないというのが現状である。

そのような中でＴＲＳがコンプライアンス重視の企業経営を目指す背景には社会貢献をすることが経営理念としてあり、それができないならば企業として存続していく価値がないと考えているからである。

しかし今後企業規模の拡大を目指す中で情報公開によるコンプライアンス確保と情報セキュリティの強化が矛盾することから主にその点に着目し、検討する。

２．コンプライアンス

コンプライアンス

企業が経営・活動を行う上で、法令や各種規則などのルール、さらには社会的規範などを守ること。

CSR（corporate social responsibility）

企業は社会的存在として、最低限の法令遵守や利益貢献といった責任を果たすだけではなく、市民や地域、社会の顕在的・潜在的な要請に応え、より高次の社会貢献や配慮、情報公開や対話を自主的に行うべきであるという考えのこと。

企業がこうした社会的要請に応えることは、社会的行動の不足や欠落が招くリスクを回避するとともに、社会的評価や信頼性の向上を通じて経済的価値を高めることができると認識されるようになってきている。

TRS の中では法令遵守より一歩進んだ CSR の意味でコンプライアンスが理解されている。

３．リスクマネジメント

３－１

リスクマネジメントとクライシスマネジメント（危機管理）

リスクマネジメント

企業経営の存続及び人的・物的資産に悪影響を及ぼす重要なリスクを合理的にコントロールするための経営手段であり、事故、事件、災害リスクの目を未然に摘み取る目的で行われる。

クライシスマネジメント（危機管理）

想定される危機への迅速、的確な対応を前もって決めておくことで、現実に発生した緊急事態の企業経営の存続への影響度をいかに小さくするかを考える目的で行われる。

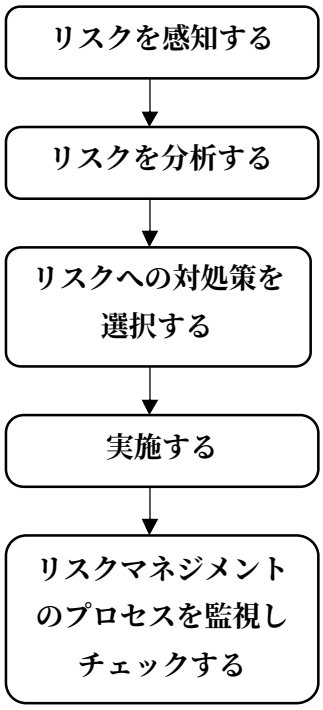
３－２

TRS **において想定される主なリスク**

分類	想定されるリスク
事件	盗難及び従業員の不正持ち出し
製品、サービス	顧客対応の失敗 納期遅延 在庫管理の不備 欠陥製品
法務	反社会的取引、不正取引 商法違反 税法違反 経営、技術、顧客、役職員情報等漏洩
労務	差別、セクハラ、プライバシー侵害等人権問題 労働基準法違反 就業規則違反 内部告発
財務	決算粉飾 保険未加入
環境	廃棄物処理、管理リスク 大気、水質、土壌汚染、騒音、振動、悪臭等環境汚染 環境負荷の多い製品、工程への対応 リサイクル対応 省エネ対応

３－３

リスクマネジメントの流れ



①リスク感知

・何がリスクなのか

見極めのポイントとして重要性の高い価値あるもの、大切なものの価値を減らすもしくは滅失させる可能性があるかどうかで判断する。

・　誰のリスクなのか

誰のリスクなのか＝誰の為のリスクマネジメントかを考える。基本的にリスクマネジメントは組織全体の目標や目的のために行われるが、会社は誰のもので誰をリスクから守るのかを考える。

②リスクを分析する

どういう類のリスクなのか考える。

・リスクの測定

一定期間内にそのリスクがどのくらい起こるのか（＝発生件数・発生頻度)、どの程度の価値の減少、滅失が発生するのか（＝損失の大きさ）を考え、

発生件数（頻度）×損失の大きさ＝リスクの大きさ
として測定されたリスクの大きさからそのリスクは会社にどのようなマイナスの影響をおよぼすのかを考える。

・リスクの評価
リスクの影響度、深刻度合いを見極める。リスクは影響が大きいのか、小さいのか、無視していいレベルかを検証することで適切な対策をたてることができる。

リスクを適切に測定・評価して数あるリスクのなかからマネジメントしたほうがいいリスクとしなくても問題ないリスクの見極めが大切で何もしない方がいいリスクを取り上げてマネジメントまで行うことは本当に必要なリスクマネジメントの効率を低下させることになる。また人や組織によって捉え方や度合いが違うため主観と客観ではリスク評価が随分と変ってくる。よってリスクマネジメントでは主観的でないできる限り客観的なリスク評価の視点がもとめられる。

・リスクを分析する　急務か長期スパンか
短期間のリスクとは急いで対策を打つべきリスクである。
長期的なリスクは先の話なのでなかなか注意を払わない傾向があり、長期的経営戦略をもって対処しないと事業継続、事業継承に直結するようなリスクである。
コンプライアンスは長期的なリスクを回避するために有効である。

③リスクへの対処策を選択する
誰がその対策を行うのか、リスク処理の主役は誰なのかを考える。自分たちだけで解決できるリスクか、利害関係者や専門家と協力して対処すべきか検討する。

・　リスクコントロール
いかにしてリスクによる損失を除去、軽減するかを考える。

a.リスクの回避
リスクそのものに初めから関係を持たないか、関係を持ったとしても途中で引き上げる。
例えば、社内の情報を完全にプロテクトして社員に情報を開示しないなどが挙げられる。

b.ロスコントロール
損失の大きさや発生確率を小さくする方法。

c.リスクの分離、分散

大きなリスクを細かくして切り離すことでリスクを分散する。例として現在一つしかない TRS のファイルサーバをセクションごとに分けるなどする。

d.リスクの結合
バラバラのリスクをひとまとめにして損失を小さくする。

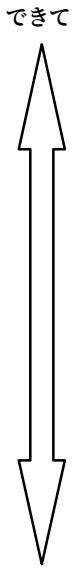
e.リスクの移転
保険を除く契約などによってリスクの移転をはかり、損失を低減する。
リピートオーダー可能そうな物件は共同開発時点で相手の技術を契約によって買い取ってしまうなど。

④実施する
実際にリスクマネジメントを行う。

⑤リスクマネジメントのプロセスを監視しチェックする
リスクとは解釈の幅が広く時代や環境によって大きく変わるので、前回は正しいと思われた対処策が今回も同じように正しく機能するとは限らない。よってリスクマネジメントの見直しと改善が必要であり、それを適切に行うには PDCA サイクルまたはリスクマネジメントのプロセスチェックを怠らないで常に監視していかねばならない。

※PDCA サイクル
管理業務を円滑に進めるためのマネジメントサイクル
Plan（計画） Do（実施） Check（見直し） Action（改善）

４．成熟度の構成



経営者にそのような意識がないか、意識はあっても方針やルールを定めていない

経営層にそのような意識はあり方針やルールの整備周知を図りつつあるが、一部しか実現していない

経営層の承認の元に方針やルールを定め、全社的に周知、実施しており、かつ責任者による状況の定期的確認も行っている

加えて周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社への模範となるべきレベルに達している

経済産業省　企業における情報セキュリティガバナンスのあり方に関する研究会　報告書（案）　参考資料　より

５．考察

TRS の現状の問題点

TRS では今まで個の営業を重視してきたため、個人のスキルを発揮させる為になるべく縛りを少なくする方向でやってきた。しかし個人の主観的判断によって失敗するケースが見られ、また社員もそのリスクを自覚している。例としてリピートオーダー可能な物件について取引先により多くの情報を提供し、営業成績を伸ばすことで社会貢献に繋がりコンプライアンスを満たすことができる反面、あいまいな自己判断での情報流出のリスクを併せ持つということが挙げられる。それに対して現在は上司の判断を仰ぐなどして対処しているが、より多角的な視点からの客観的なリスク評価のためには役職の上下を排除したフラットな場での意見交換が必要である。取引先への情報提供の際は、現在でも営業個人レベルでは共同開発者に対し細部までの確認と承認を逐一行う努力がなされているが、共同したリスクマネジメントを構築するためよりはっきりとした相手方との取り決めを持ったほうがいいのではないかと思われる。一方、技術での設計レビューでは普段各人が担当を任されているが技術的な問題がないか確認の機会を持っているので顧客対応の失敗をなくすためには営業でも同じしくみは必要である。

同じく技術では社内標準品の検査成績書の作成手順や検査手順書も文章化が行われているように、個人、顧客情報などの重要なものに関しては取得、利用、保管、開示、消去などの一連の業務工程ごとにきめ細かく、手順の明確化、処理の記録、確認をする必要がある。社員への情報開示は組織の透明化を図り、不正をなくしていくことに対し重要であるため継続するべきだが、開かれていることとルールがないことは同じではないことを意識するべきである。このように TRS では現在不文律によってリスク対処している面が多いことについて、きちんと明文化して共通理解することが重要である。企業秘密、顧客情報を扱う際の取り決め、明確なルールの欠如は顧客の為のリスクマネジメントの軽視と考えるべきである。情報開示もコンプライアンスであるが、同時にその情報を厳しく管理することもコンプライアンスとなりうるからである。

今後の課題

現在技術分野でのリスクマネジメントがよくなされているのは研究開発型企業として製品の欠陥は影響が大きいとリスク評価されているためである。逆に情報セキュリティに関してはリスクの評価が甘くコンプライアンス要件も満たさないと判断した。こういった分析をあらゆる方面のリスクに対して検討していくことがもとめられる。

しかしゼロからリスクマネジメントのルール作りを始めるのは難しい。そこで業務会議などで日常業務での疑問点、問題点をあげていきリスクの洗い出しを行うことでリスクへの対応策が立てやすくなる。今回実施したアンケートからも有用な情報が出てきたのでこれを定期的に行うことは大変効果的である。また他社の具体的な不祥事例が TRS でも起こりうるか会議で検討することはさほど手間がかからないので実施するべきである。

加えて経営理念、事業目的の周知を徹底し、TRS は何にリスクの重点を置くのかはっきりさせ優先順位を決めて、みんなで共有できる価値観を軸にしてまとめ定期的に見直しを行う。現時点での課題としては社員教育で客観的なリスク評価をする訓練を受けていない、そのための知識も持ち合わせていないことが挙げられるが、社員のリスクマネジメントの意識は高いと感じられるので具体的な方法は専門家を招くなどして学んでいくことは難しくないと思われる。

参考文献

不祥事はなぜ繰り返されるのか　~日本人のためのリスク・マネジメント～
武井勲　　扶桑社

危機管理学総論　理論から実践的対応へ
大泉光一　ミネルヴァ書房

経済産業省
「コーポレートガバナンス及びリスク管理・内部統制に関する開示・評価の枠組について－構築及び開示のための指－」
http://www.meti.go.jp/press/20050713001/050713kigyokodo.pdf