リスクマネジメントのベストプラクティス

２０１８年６月吉日

一般社団法人ディレクトフォース
企業ガバナンス部会
小研究会第２グループ

目次

１．はじめに
２．リスクの定義
３．リスクマネジメントと法制度
４．ウェブリスクに関する報告
５．対人関係教育
６．事例研究
７．2017 年版 COSO
8. ガバナンス・リスク・コンプライアンス紹介
９．おわりに

企業ガバナンス部会　小研究会第２グループ

研究会メンバー	会員番号	
藤村峯一	499	リーダー
喜藤憲一	768	
高橋宜治	858	
森野稔晴	1222	
木村盛計	1224	

メンター	会員番号
三神明	842
橋本健	1038

はじめに

日大のアメフト部の問題、日産と富士重工の完成車検査の手抜き、神戸製鋼のデータ改ざんなど不祥事が後を絶たない。多くの不祥事は企業内のガバナンスが正常に機能していれば防げるし、防止のためのコストは不祥事の収拾コストより遙かに少ないことはほぼ常識であるにもかかわらず、次々に不祥事が続くのはどうしたことなのか。
不祥事発生防止のガバナンスが不祥事発生に追いつかない理由の１つがグローバル化である。例えば米国で車両部品メーカー間の価格カルテルが摘発されると同じ自動車が輸出されている他の国で同種訴訟が発生する。また欧州での個人情報保護の立法が成立するとその影響は日本企業のビジネスのやり方の変更を迫る。
もう一つの大きな要因が IT 関連の変化である。AI, IOT などあらゆる企業へ急激な環境変化を迫ってくる。
もう１つの変化は企業内部の変化である。環境対応による企業体制の変化もあるので環境と内部を厳密に分けることはできないが企業成長のための M&A,新技術、新マーケットへの進出のために企業の組織体制を積極的に変更する。
しかしながら変えてはいけないものがある。それは組織の個々人の倫理意識である。多くの企業では創業の精神、企業文化として引き継がれ経営理念として表され、洗練されて継続する努力がなされている。
この継続すべき企業理念を元に企業内外部の両者の変化に対応可能な「リスクマネージメントのベストプラクティス」について検討、研究した。

具体的にはリスクをどのような観点から捉えるか、即ち「リスクの定義と分類」から「不祥事防止への法的な対応」、ここ数年で大きく注目される「ウエブ関連のリスク」、企業活動の根幹である「人の育成」へと章を進め実際に企業ではどの様ようにリスクマネジメントが展開されているかの事例研究と 2017 年版 COSO がリスクマネジメントをどのようにとらえているか、さらにはコンサルタントがガバナンス・リスク・コンプライアンス（GRC）と言う概念と IT システムを推奨している。これらがリスクマネジメントのベストプラクティスの方向性の１つであると思い紹介した。

リスクの定義

リスクとは一般的に日本語では「危険」と訳されるが、リスクマネジメントの立場からすると、リスクとは「組織の目標達成に影響を持ちうる不確実性」と整理できる。
その中で、損失を発生させるマイナスの結果をもたらす事象のみを対象とするのか、事業機会に関連するプラス・マイナス両面のリスクを対象とするのかは、リスクマネジメントのあり方と関係付けて把握する必要がある。

リスクの分類

リスクの分類には分類の目的によって様々な方法があり、その主要なものを示すと以下のようになる。

（1）純粋リスク、投機的リスク

純粋リスクは顕在化した場合に損害のみを発生させるリスクであり、静態的リスクとも言われる。例えば、自然災害や偶発事故がこれに当たる。一方、投機的リスクは損害か利益のいずれかを発生させるリスクであり、動態的リスクとも言われる。企業活動や社会的・経済的（為替リスク、金利リスクなど）がこれに当たる。純粋リスクは一般に前兆なく偶発的に発生し、損害の範囲を特定できないが、投機的リスクは突発的、偶然の出来事ではなく、損害の範囲も推測可能である。

（2）人的リスク、物的リスク、賠償責任リスク

損害を受ける対象による分類であり、自動車事故で考えると人的リスクは対人事故、物的リスクは車両事故、賠償責任リスクは他人に損害を与えた場合の損害賠償リスクということになる。

（3）事業機会に関連するリスク、事業活動の遂行に関するリスク

前者は経営上の戦略的意思決定に関わるリスクであり、後者は適正かつ効率的な業務の遂行に関するリスクである。さらに事業活動の遂行に関するリスクは、①オペレーションリスクと②経営環境リスクに分類することができる。

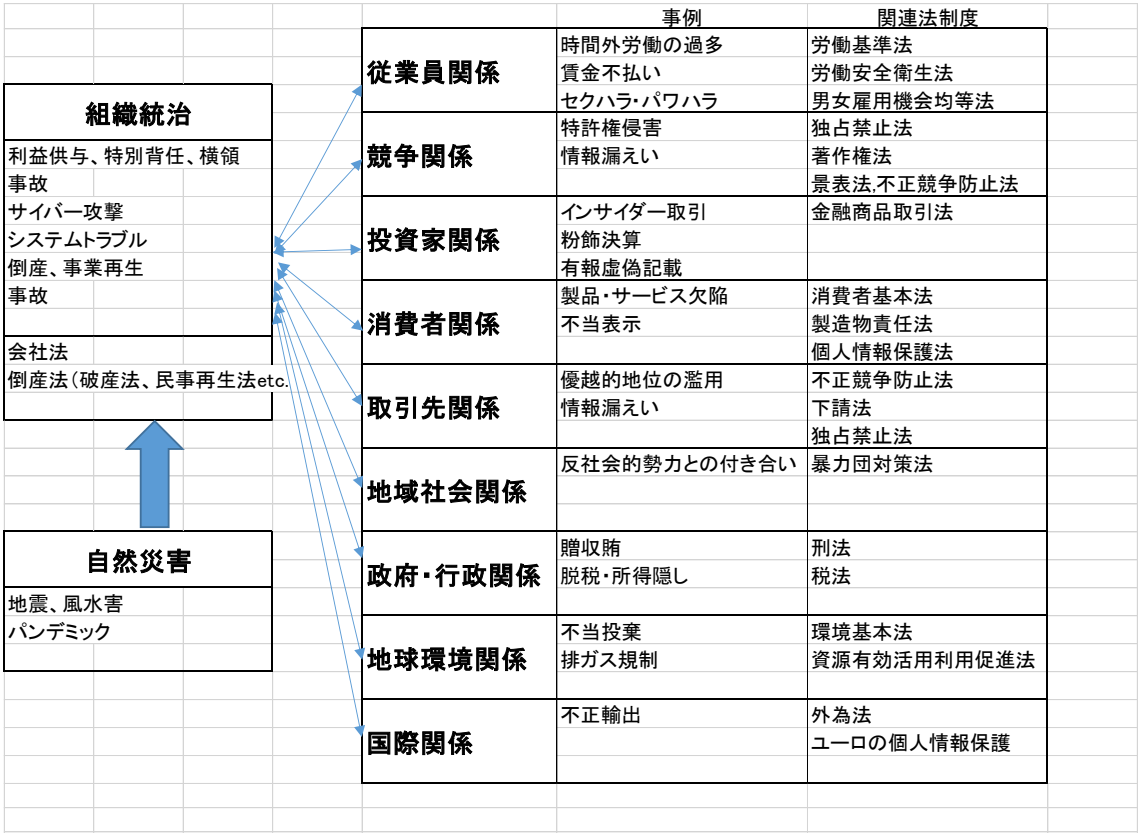
（4）その他のリスク分類

その他にもリスク分類は対象の置き方によって様々な分類がある。①受動リスク/能動リスク、②自然的リスク/人為的リスク、③一般的リスク/特殊リスク、④保険可能リスク/保険不能リスク等、多様な分類がされるが、自らの組織に相応しい分類を検討すべきである。

ここでは危機管理型に限ったリスクマネジメントを議論するのではなく、経営戦略としてのリスクマネジメントを議論する予定なので、純粋リスクであれ、投機的リスクであれ、企業経営に脅威を与えたり、企業環境に影響するリスクはすべてマネジメントの対象とすべきと考えており、事業機会に関連するプラス・マイナス両面のリスクを対象とすることとしたい。

リスクマネジメントと法制度

リスクマネジメントは、組織内部の円滑な運営と会社を取り巻く幅広いステークホルダーから、一層の信頼を確保する観点から取り組む必要がある。
そのステークホルダーとの関係は、各種の法制度に守られており、これを侵すことの無いよう十分な注意が必要である。
ステークホルダーと、具体的な不祥事の例及びそれに関与する主な法律制度について下記の一覧にする。
法制度は、時代の要請にこたえて随時改正されており、これらの変更に組織統治する会社は、その改正の趣旨を十分理解し対応していく必要がある。



	事例	関連法制度
従業員関係	時間外労働の過多 賃金不払い セクハラ・パワハラ	労働基準法 労働安全衛生法 男女雇用機会均等法
競争関係	特許権侵害 情報漏えい	独占禁止法 著作権法 景表法,不正競争防止法
投資家関係	インサイダー取引 粉飾決算 有報虚偽記載	金融商品取引法
消費者関係	製品・サービス欠陥 不当表示	消費者基本法 製造物責任法 個人情報保護法
取引先関係	優越的地位の濫用 情報漏えい	不正競争防止法 下請法 独占禁止法
地域社会関係	反社会的勢力との付き合い	暴力団対策法
政府・行政関係	贈収賄 脱税・所得隠し	刑法 税法
地球環境関係	不当投棄 排ガス規制	環境基本法 資源有効活用利用促進法
国際関係	不正輸出	外為法 ユーロの個人情報保護

その他、法制度として業界あるいは事業に特有の法律もあり、それらをも製品、サービスの基本的な遵守事項である。例えば建築基準法、食品衛生法、保険業法、薬事法等々である。

上記のステークホルダーとの関係を壊す原因としていくつかに類型化される。

１．新しく法制度が制定されても、その趣旨が十分理解できず、あるいはその定義が曖昧なため不祥事につながるケース

例としては、1985 年の男女雇用機会均等法の施行に伴い、男女の差別的扱いが是正されてきたが、セクハラについては,その理解が十分ではなく、またセクハラを訴える方の受け取り方によって事例が異なるために、不祥事と捉えられてしまうケースである。
もう一つの例として、みずほ銀行の 2013 年のみずほ銀行反社会的勢力融資事件があげられる。1992 年に「暴力団対策法」が施行されその後 2007 年に「企業の反社会的勢力による被害を防止するための指針」が発表されている。しかしみずほ銀行の反社会的勢力の定義が曖昧なため、混乱が生じ、またその対応も不十分であったために起こった事件である。

２．今まで法律では制定されていたが、慣習として行われていたことが、厳格な指導で認められなくなったケース

労働基準法にでは、その制定の時から時間外労働の扱いについては定められていたが、現場ベースではそれが守られずに常態化していた。
1993 年には労働時間法制に関する改正、1998 年には労働時間及び労働契約法等法制整備が行われ、労働時間の扱いについては柔軟な対応ができるようになった。
一方時間外労働は賃金支払いに関しては厳格な指導のもと、過重労働問題や賃金未払い・不払い問題が多数発生している。同時に 36 協定違反についても厳しく問われるようになってきた。
その例として 2017 年 7 月に、宅配便大手のヤマトホールディングでは、セールスドライバーの残業代未払い問題が発生し、結果的に 230 億円を支払うことになった。
また扱い数量の統制や宅配料金の値上げなど事業の構造の変革をもたらすことになっている

３．新しい技術の進歩や社会の変革、特にＩＴ化の進展にともなう不祥事のケース

1990 年代終わりからのＩＴ化の進展は急速に社会に変革ももたらすことになった。そのため情報の価値が重要視されるようになってきた。
2003 年に「個人情報の保護に関する法律」が施行され、企業も対策を講じてきたが、ＩＴ化の進展は個人情報の価値を高めたこともあり、

管理の目をすり抜けて不祥事が発生している。2014 年にはベネッセで個人情報が流出し、その数は 2,070 万件にも及び会社の補償を含めて大きく屋台骨を揺るがす事件となった。

４．自社の技術力不足が、偽装につながり不正競争防止法、偽装罪や製造物責任を問われるケース

1995 年に製造物責任法が施行され、製品の安全確保に対する責任が重くなった。しかし現場では「技術力＜製造」のアンバランスのため、また人材の不足のため、あるいは社内での教育不足のため幾つかの不祥事が起きている。2016 年に発覚した三菱自動車の燃費偽装の問題、2017 年の神戸製鋼所の強度偽装など、直近でも沢山の事例がある

５．内部統制が効かなくなり、金融商品取引法違反あるいは会社法違反を起こすケース

2007 年に従来の証券取引法を大幅に改正し、適用範囲を拡大して投資家の保護等を目的に「金融商品取引法」が施行された。
それによってディスクロージャーや不公正取引の禁止などのルールが定められ、その後も改正を繰り返しているが、それでもインサイダー取引が発生するなど法を順守しない形で不祥事が発生している。
会社の基本法である商法は、2006 年に大幅改編、そして「会社法」として施行され会社類型の見直しや組織再編の機動性・柔軟性の向上などの規制緩和をする一方、内部統制システムの義務化や会計監査人制度の創設などガバナンスについては大幅に強化する内容であった。
さらに、2015 年施行の会社法改正では、企業統治に関する改正が主要なテーマとなり、監査等委員会設置会社制度の創設や、社外取締役を置いてない場合の理由の開示など、機関設計を基にガバナンスの強化を図った。監査役の権限強化も同時に行われ、会計監査人の選任等議案の内容の決定に関する改正も行われた。
しかしこのような監視強化にもかかわらず、いくつかの不祥事が発生している事実もある。2011 年に起きた大王製紙巨額借り入れ事件は、経営者による公私混同の不祥事で、強大な権限を持つオーナー経営者一族が、代表取締役の地位を利用して 106 億円を超える会社資

金を個人的に流用、それも個人のカジノ利用の資金であった。全く内部統制が働かなかった例である。
2011 年に起きたオリンパス粉飾決算事件は、3 代にわたる経営トップが、資産運用の失敗を隠すため粉飾決算を行ったものであり、外国人が社長になって初めて発覚したものである。つまり内部統制が全く働かなかった例と言える。
2015 年に発生した東芝の粉飾決算事件は、利益をかさ上げするために費用の計上を先送りするなど会計上の操作を行っていたもので、金融商品取引法違反で 73 億円強の課徴金納付が命じられている。これらの行為はトップによる利益へのプレッシャーから生じたものと言われているが、発覚したのは内部通報による社内からの告発であり、ガバナンスが働いていたとは言えないものである。
さらに東芝は、2006 年に買収した原子力関連企業のウェスティングハウスも 2017 年に 90 億ドルの損失を理由に破産法申請を行っている。ウェスティングハウスは東芝の子会社であるにもかかわらず、ほとんど独立した会社のごとく東芝の統治がされてなかったと言われている。
このように法制度またにコーポレートガバナンスコードなど、ガバナンスの制度はできても、その実態が伴わず数々の不祥事が生じていることも事実としてある。

ウェブリスクに関する報告

1.　SNS の登場と企業リスク

インターネットの存在は、現代を生活する者にとっては欠く事の出来ないものである。

1990 年代、ネットサーフィンが主流であった頃は、ユーザーは情報の受け手としての役割が主流だった。しかし、掲示板のような投稿機能が一般ユーザーをして情報発信者に変えた頃からウェブ上のリスクという認識が成され始めた。

そして､所謂 SNS（ソーシャル･ネトワーキング･サービス）が登場した｡2004 年に Facebook が米国で、グリーが日本で登場。

米国で Twitter が 2006 年に登場すると、日本でも mixi が登場した。

そして、ウェブ上の炎上が、この 2004 年頃から発生する様になる。

個人がブログに発信するコメントを荒らしたり、掲示板で晒したり、誰かを批判したりなどである。

そして、2007 年に iPhone、2008 年に Facebook と Twitter が日本に上陸するとウェブ上の炎上は一気に加速した。

iPhone の上陸は、PC に頼らなくてもウェブにアクセスでき、キーボードを打つことなく情報を発信できるような環境が個人に与えた。

その後 2012 年には LINE がプラットホーム化し、2014 年にはインスタグラムの日本語アカウントが開設された。

各メディアが発表する月間アクティブユーザー数は、2018 年 1 月時点で、LINE が 7100 万人、Twitter が 4500 万人、Facebook が 2800 万人、インスタグラムが 2000 万人となっているが、日日進化している SNS のユーザー数は日々増加している。

一つの要因として、自治体や警察等の利用浸透、企業の公式アカウントの増大などによるものである。

平成 29 年度版総務省の情報通信白書によるとスマートフォンの SNS 利用率は、2012 年に 41.4%だったものが、2016 年には 71.2%にまで拡大している。代表的な 6 つの SNS 別にみると、LINE が 20.3%（2012 年）から 67.0%（2016 年）、Facebook が 16.6%（同）から 32.3%（同）、Twitter が 15.7%（同）から 27.5%（同）、mixi が 16.8%（同）から 6.8%（同）、Mobage が 12.9%（同）から 5.6%（同）、GREE が 11.8%（同）から 3.5%（同）となっている。

SNS 利用者数が増大する一方で、その種類は寡占化が進んでいる。

そして、これら SNS が炎上する一つの理由として、その匿名利用がある。

総務省の調査によると、実名性を謳っている Facebook でさえ 15.2%が匿名利用である。

次いで LINE が 37.2%、インスタグラムが 68.1%、mixi78.4%、Twitter76.5%がそれぞれ匿名利用となっている。

この様な匿名性が炎上リスクを考えずに投稿させる一因になっていると思われる。

一方で SNS は、企業によって、販路開拓、ブランディング、更にはそこから得られる消費者ニーズを商品企画に生かすといった取り組みといったことに活用されている。
「企業のソーシャルメデイア活用に関する調査報告書」（経産省参加者 170 名）によると、63%の企業が活用しており、35%の企業が今後活用を検討するとしており、実に 98%の企業が SNS を重要なツールと認知している。その活用用途は、88 社が認知向上、35 社が販売促進、3 社が製品開発、11 社がサポートに活用をするか、検討している。
このような活用の範囲が広がってくると、益々炎上リスクの影響の大きさが問題になってくる。

2.　WEB リスク・炎上事例及びその影響

ウィキペディアでは、炎上（flaming）とは、『サイト管理者の想定を大幅に超え、避難・批判・誹謗・中傷などのコメントやトラックバックが殺到することである。つまり、特定の事象に対して、不特定多数のユーザーの（批判的な）記事が殺到すること』となっている。
ソーシャルリスク等のデジタルを通じて発生するコーポレートリスクを包括的に支援するベンチャーエルテス社の定義では、『炎上とは Twitter で 50 回以上のリツイートがされ、特定のまとめサイトにまとめられたものから同社が” 炎上 “と判断したものとなっている。
ネット炎上は第 3 者が炎上の元となる投稿を発見し、拡散していくことで発生をする。
文化庁が平成 28 年度に行った調査（全国 16 歳以上の男女 3,566 名の面接）では、『炎上を目撃した際に書き込みや拡散をするか』という質問に『大体する』0.5%強『たまにすると思う』2.2%と、3%に近い人が炎上に加担するとの結果になっている。
一般に、炎上の流れは、①火種の投稿⇒②第 3 者が投稿を発見⇒③フォロワー外からも拡散⇒④爆発的な拡散（新聞・TV 等のメディアに転載され広く拡散）⇒⑤半永久的に残り続ける。といった流れになる。
代表的な炎上例をクラシックなものも含めて幾つか紹介したい。

①　患者情報漏洩

〇〇記念病院の診療情報管理士の△△が、「今日ものすごい事実発覚！■■（サッカーチーム）のカルテ発見！住所も電話番号もわかる。これが散々言われた個人情報保護法か！」「今日見つけたのは××君でも検索すれば他にも絶対いるー！笑」「なんか誰かが〇×選手を見かけたらしいから明日探す―！爆笑」とツイート。
カルテを適切に管理する専門職である診療情報管理士であるにも関わらず、患者の情報を外部に漏洩したこと、同僚も私的興味でデータを見ている上に仲間内で話し合っていると公開したことにより△△の twitter は炎上した。
後日、本事案についての謝罪文が掲載された。文中発言者の処分については同病院運営会議にて決定すると記載されていた。

②　プレスリリースで炎上

〇〇製菓が辛ラーメンで知られる韓国の大手食品メーカー「△△」と提携して商品の共同開発や生産技術の提供に乗り出すことが報道された。〇〇製菓の公式ブログの某月某日付の記事に対し、韓国の同社が日本製の菓子に類似した商品の製造や異物混入の為、英独で輸入禁止になったりした実績のあることの懸念などから提携に反対するコメントが 2 日後に 6500 件以上も寄せられた。

③ 失言で炎上、そして退社

早稲田大学を卒業し大手スポーツメーカーに勤めていた社員△△が同社と契約している某スポーツ選手が来店したことをツイートした。ツイートの内容は同選手を中傷したものだった為に炎上した。翌々日、同社は謝罪文を掲載、当該社員は退社することとなった。また、この炎上により、後々でもネット検索結果の上位に、この炎上関連の記事が表示され続け、企業のイメージダウンはぬぐい切れない。

④ その他過去にあった炎上事例

i. マスメディアの情報がネット上で話題になり、それが炎上した事例
ii. 某地方都市の FB で終戦記念日に､戦争責任というデリケートな問題に触れた。そのことが Twitter で拡散し、炎上した事例
iii. 某洋酒メーカーが HP 上での販促文にデリケートな表現（日本海→東海）を間違ったために炎上した事例
iv. 社内のスタッフが個人情報に当たることをツイートしたために炎上した事例
v. 某家庭用品メーカーがスポンサーとなった韓流番組に対するツイートが拡散し、そのメーカーの不買運動までになった事例。確証はないがその時期に急激に株価が下降した。

このように拡散した炎上は企業に対して様々なリスクを発生させることになる。そのリスクを纏めると以下のようになる。

(ア) ブランドの毀損
(イ) 株価の暴落
(ウ) 採用時の応募者の低下
(エ) 新規取引数の減少
(オ) 売上の低下
(カ) 退職者の増加

誰でもインターネットに繋がる時代にその影響力は多大なものになっている。例えば、『何かを検討する際にインターネット検索しますか』という問に対しては 87.5%が『YES』と答え、『検索した結果、悪評等のネガティブな記載は気になりますか』という問に対しては 91.5%が『YES』と答えている。

このような状況で、ウェブ上の口コミによる影響度が高まっていることは SNS の企業リスクを増大させる傾向にある。

ここにちょっと面白い調査（AMEX）がある。

自らの経験を他者に伝える場合、良い経験は平均 8 名の他者に話すが、悪い経験は平均 21 名の他者に話すというものである。
つまり、ウェブ上においても、悪いツイートの方が良いツイートよりも拡散する確率が高いということである。

3. Web メディアリスクマネジメント：企業の対策と実態

Web メディアを通じたリスクは発生原因によって以下の 3 つに分類できる。

① 役員・従業員、関連会社の役職員等、企業内部の人物の失態（失言等）悪意（情報漏洩等）や企業の不適切な事業活動によって、Web メディア事件が発生するリスク。情報漏洩・失言・クレーム等
② 外部の第三者の発言や行動が原因となって Web メディア事件が発生するリスク。誹謗中傷・風評流布、なりすまし、苦情クレーム等
③ 発生したトラブルに関する情報が、誰もが閲覧できるデータとして WEB 上に長期間（場合によっては半永久的）残存し、検索等によって過去の情報が露出し、企業や従業員が被害を受けるリスク。

このようなリスクに対応する時の重要ポイントは、①経営トップの理解と対策に対する姿勢②社内の Web メディアリスクに関する正しい理解③Web メディアリスクマネジメント専門人材の確保と配置④外部機関・外部専門家の活用⑤Web メディアリスクに関する最新情報の入手と活用⑥自社の Web メディアリスクの実態把握と実態に即した対策の重要性⑦即時対応可能な組織と体制⑧自社の実態に最も合った方法の構築といったことがあげられる。
また、Web メディアリスクマネジメント推進の具体的な手順としては、

i. 自社の Web メディアリスク管理体制に関する現状認識（実態調査の実施）とそれに基づくトップの経営判断。
   (ア) 実態調査（アンケート調査、ヒヤリング）の実施をする。
   (イ) Web メディアリスクマネジメントの実施・是非についての基本的な方向性の確認をする。
ii. Web メディアリスクマネジメント推進体制（組織）を整備する。
iii. 「ソーシャルメディアに関する基本方針」等、Web メディアリスクの管理に関する諸規定を整備する。
iv. Web メディアリスクマネジメントに関する具体的な実施計画を立てる。
v. Web メディアリスクの洗い出し（Web メディアリスクの見える化）を行い、対策の優先順位を決定する。
vi. Web メディアリスクの防止・軽減対策の実行
   (ア) 企業が利用している Web メディアの公式アカウントについて厳正な管理を行う。
   (イ) Web メディア事故発生を想定して事前に事故対応訓練を実施する。

(ウ) Web メディアリスクの監視（モニタリング）を行い、Web メディアリスクの発生状況や予兆を常時把握すると共に、顕在化したリスクについては早期発見・早期対応ができる体制を構築する。

vii. Web メディアリスクに関するデータベースを構築し、Web メディアリスクに関する情報を記録・一元管理すると共に、全社内で情報を共有する。

viii. 重大な Web メディア事件が発生した場合の対応について事前に準備する。

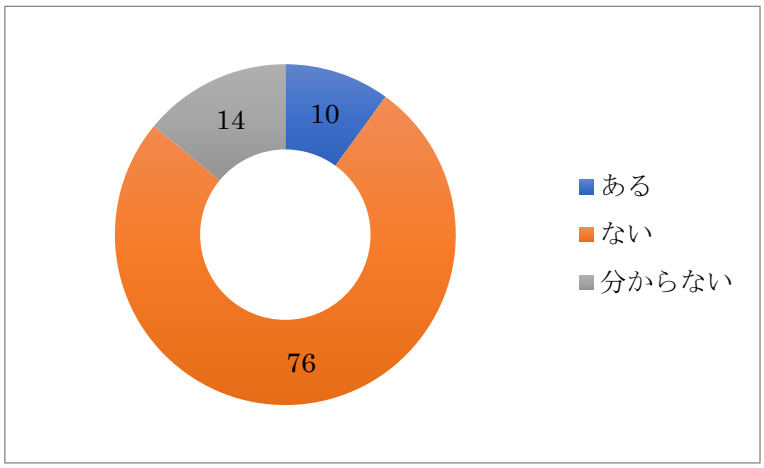
ix. Web メディアリスク管理に関する制度や実施状況の形骸化を防止する為、社内の各部門･部署での Web メディアに関するリスク管理の進捗状況をフォローし続け、必要に応じて制度や実施方法の見直しを行う。

4. Web リスクの関する調査

このような WEB リスクに関する企業への調査の結果を見てみると以下のようになる。

① 勤務先において炎上を未然に防いだものを含めて、SNS によるトラブルが発生したことがありますか？

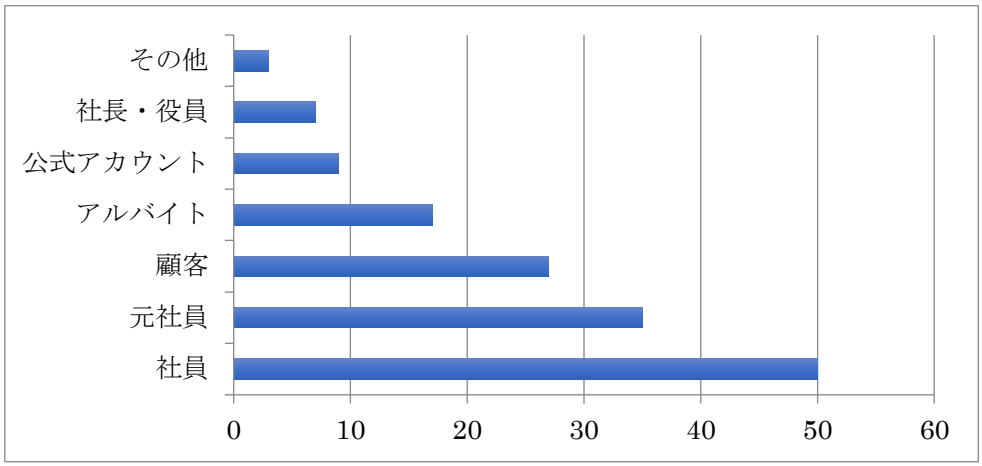
トラブルの内容として、CM に対する苦情や第三者による不実なネガティブな投稿、また、



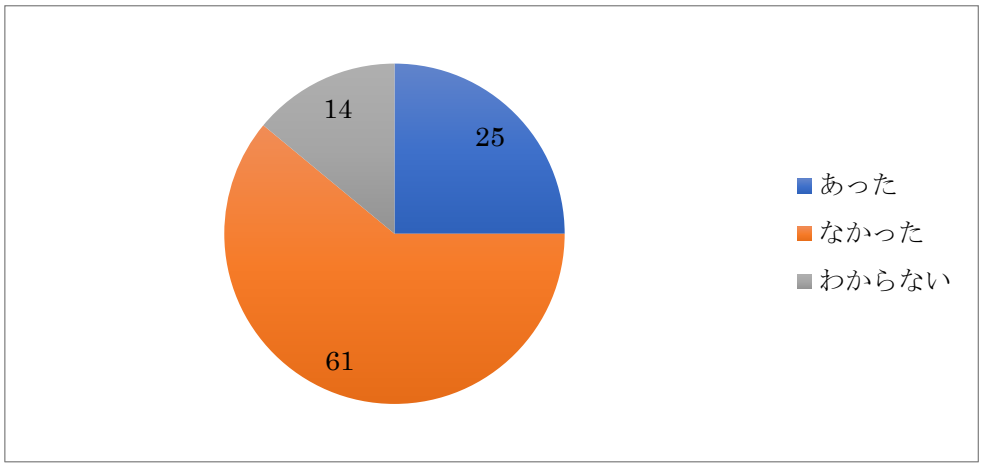
Twitter 公式アカウントで運用担当者が呟いた一言を『失言』と捉えられて炎上したケースもある。他者によるもの、捉え方の違いなどにより社内教育や体制を徹底していたとしても防げないタイプのものがある。

② 貴方の勤め先で SNS 炎上トラブルが仮に発生するとしたら、誰の投稿が原因になると思いますか？

最も多かったのは社員、元社員である。その他に協力会社社員、競合他社社員、契約社員となっている。



③　入社時に SNS に関する研修や指導があったか？というと、実に 61%の会社がなかった。と答えている。



④　あなたの勤め先や部署では SNS トラブル対策をしていますか？

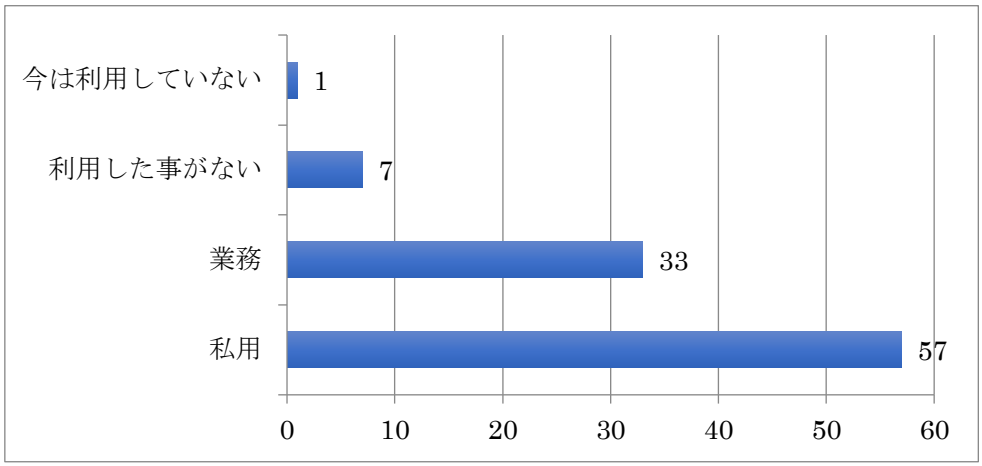
という質問には、34%がしている。24%が検討中と何らかの対策を考えている企業は過半数に上り、その必要性を各社が感じていることが伺える。

具体的なトラブル対策は

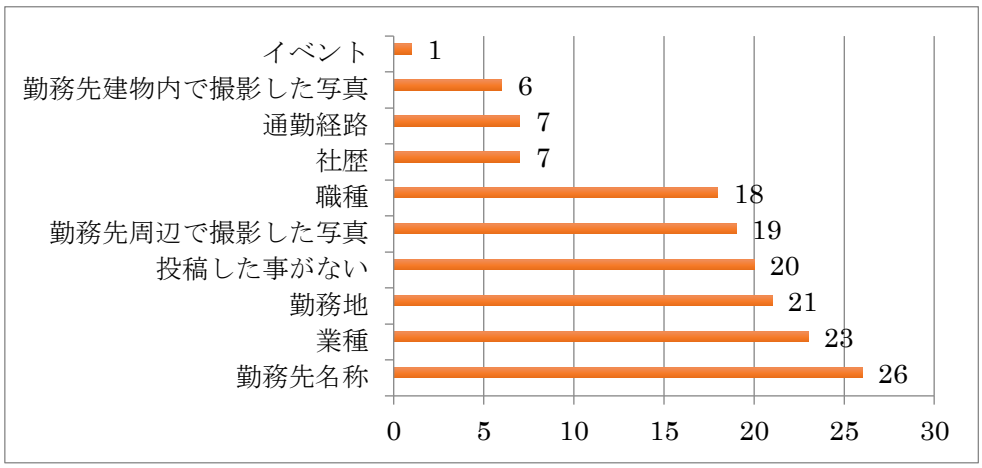
i. セミナー、研修、勉強会
ii. モニタリングサービスの導入
iii. 担当者による投稿モニタリング
iv. ガイドラインの策定と周知
v. 断続的なメール等による注意喚起
vi. 入社時のオリエンテーション

となっている。

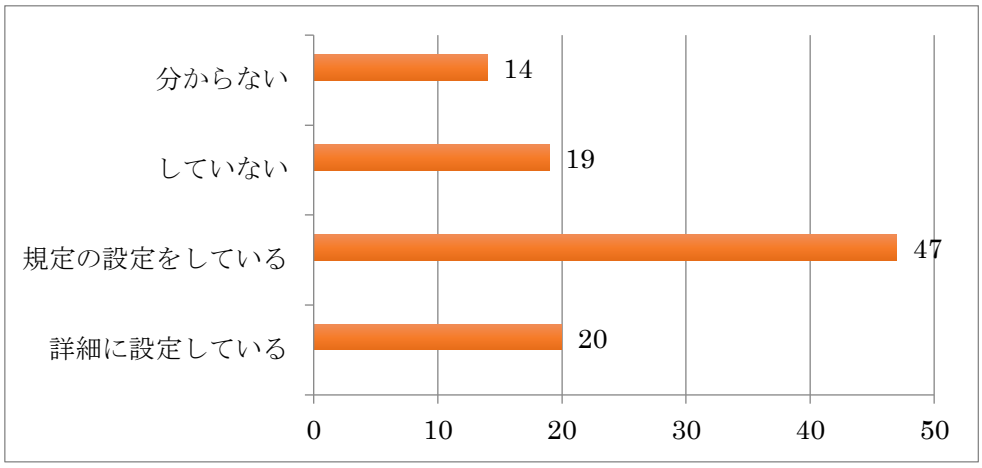
⑤　どのようなシーンで SNS を活用しているかの質問に対しては、57%が私用であるが、33%が業務ということで、公式アカウントが増加していることが伺える。



⑥　勤務先に繋がる情報を SNS に投稿したことがあるかどうか？では何らかの情報を投稿しているようで、適切な管理が望まれる。



⑦　最後に SNS の公開範囲を設定しているかの質問に対しては規定の設定をしている人が 6 割以上おり、リスクがあるとの認識はできているようである。



最後に炎上のトレンド変化を見て纏めたい。
ネット炎上は、社会情勢を強く反映する傾向にあり、その原因となる話題（火種）は年々増えている。
これまでのトレンドを振り返ってみると

A） 2011 年は『反・韓流』『反・原発』
B） 2012 年は不況、景気の谷間でバイトテロなるものが発生。現在に及んでいる
C） 2013 年情報漏洩、労務問題（ブラック企業大賞など）～現在
D） 2014 年内部告発　～現在
E） 2015 年異物混入、広告表現　～現在
F） 2016 年ジェンダー論　～現在

このように、企業がリスクとして対応しなければならない対象は増え続けていくことが予想される。

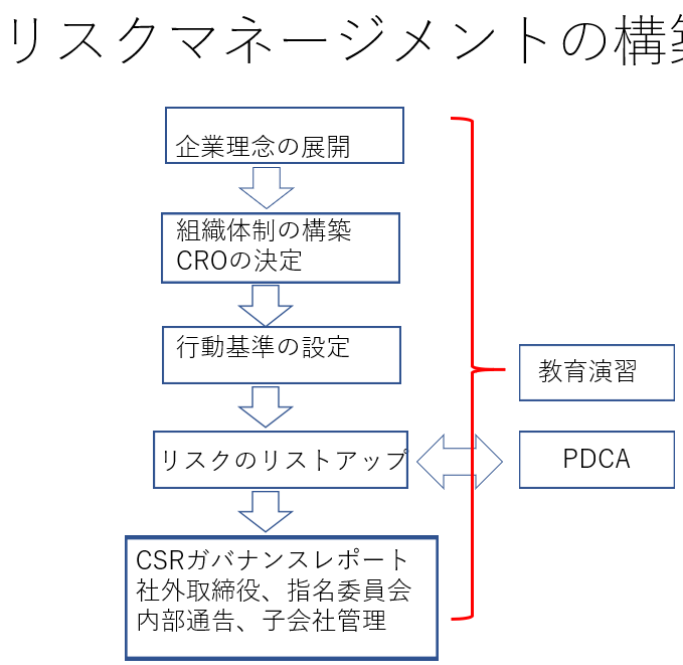
「対人関係教育」：企業の危機管理・リスク管理の原点

＜様々なリスク管理体制がとられる中で最も基本とすべきことは何だろう＞
企業のリスクマネジメントでは、製品の不良、製品情報、顧客情報等の様々な点、また材料、装置、製品、保管体制、資金管理、顧客情報管理等々、リスクは様々なところに潜在している。
そして、一旦発生してしまった際に、それを最小限の被害で納めることが出来る体制があるかどうかも大切なポイントである。
　そこで、これらの全てに関わる共通点は何かと考えてみると、、、
一旦会社を離れて、外へ出た製品や情報から生じる問題は別として、少なくとも社内の原材料受入から製品出荷までの一連の流れや、それに伴う資金の流れ、情報の流れ、顧客・仕入先等との対応、社内部門間の衝突、上司・部下の対立、これらの何れも全て「人」が関わっていることは共通している。
そしてそれらの「人」はアルバイト、パート、嘱託から役員、社長、会長まで、また国内の日本人社員から、現地採用の外国人社員まで、立場は様々である。
この１人１人の立場や考えや気持ちを持つ社員全員が、昔の戦時中の「お国のためなら！」というような、自分はどうなろうと会社を守る！というような気持ちを持っていると信じることはできない。
素晴らしく会社に貢献している有能な社員が、数日前の上司とのいざこざが元で、ある日突然大切な企業情報を競合相手に漏らしてしまった。本人はその直後既にやったことを後悔していても、情報は独り歩きしてしまう。つまり企業の抱えるリスクは社員一人一人の上にのって、日々が流れていると言える。
では、このどうしようもなく、何時何処でも突然発生してしまう可能性のある「人的リスク」を根絶する、或いは最小限に留めるにはどうすればよいか？・・・完璧に効く薬は無い。
それならば、社内規則、製品管理規定、管理規定、営業規則、運営規定等々、、、を非常に厳しく漏れなくし、厳罰主義を徹底すればよいのではないか？・・・無理である。
採るべき道は、「社員を信頼する」「社員同士の相互信頼感を醸成する」「上下や部門間のコミュニケーションを良くする」ことにつきる。このための必要な対応は、地道だが「社員教育」につきる。但し、会社への忠誠心を訴えかける、いやいや出席している社員へお仕着せの「会社のルール」「社是の教育」等をするというような、一般的によく行われている社員教育・研修ではなく、「人間関係」「相互尊重」「自己理解と他者理解」「コミュニケーション力の醸成」という「対人関係教育」である。
幼い子供でも幼稚園や学校で、良い先生にあたれば、自分の本心で素直に、悪いことはしない、友達をいたわる、家族と仲良くできるのというのと原点は同じである。

この社員教育・研修がきちっとなされている企業では、業績の伸びだけではなく、リスクの面でも安心できる状態を維持・継続して行くことができる。

リスクマネジメント事例研究

以下にパナソニック株式会社と株式会社神戸製鋼を事例としてリスクマネジメントの実態を推察してみたい。
リスクマネジメント構築手法



・企業理念の展開：企業の存在意義 Mission, Vision and Core value
・リスクマネージメントを支援する組織体制。特に CRO(chief risk management officer)の任命と支援体制
・倫理規範・行動基準の明文化とその浸透
・リスクアセスメントと PDCA による更新とフォロー
・最終的には CSR 報告書やガバナンスレポートに記載される内容の実施

パナソニック株式会社のリスクマネジメントを参考としてリスクマネジメントの意義と方策を見て行こう。https://www.panasonic.com/jp/corporate/sustainability/management/riskmanagement.html

以下引用

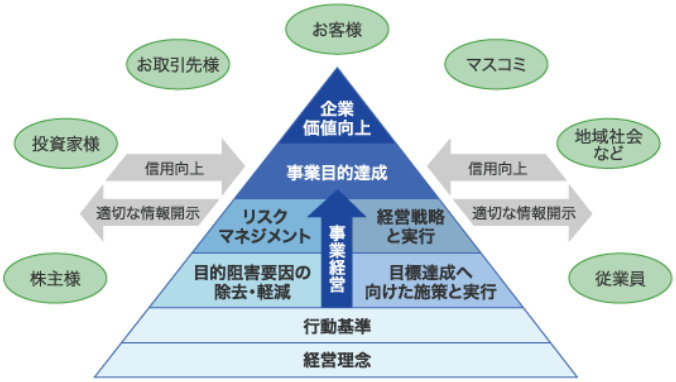
基本的な考え方

当社では、創業者 松下幸之助の「先憂後楽の発想」「失敗の原因は我にあり」「すべての事には萌しがある」「小さい事が大事に至る。萌しを敏感にとらえて憂慮しなければならない」などの考え方を基軸とし、"失敗の原因"すなわち事業目的の達成を阻害する要因を事前になくしていく活動として、全社的リスクマネジメント活動をグローバルに展開しています。また、リスクマネジメント活動は、経営戦略の策定・実行とともに事業経営を推進するための「車の両輪」であり、これら両者が機能することで事業目的の達成をより確実にし、企業価値の向上につながるものと考えています。さらに、リスク情報を適切に社会に開示し、事業経営の透明度を高めるとともに、リスクに対して事前に対策を打ちリスクを低減することによって、お客様をはじめとするステークホルダーの皆様や地域・社会にご安心いただくことができるものと考えています。

創業者の経営理念を行動基準リスクマネジメントの基本として展開している

推進体制

当社では 2005 年 4 月から、パナソニックグループ全体のリスクマネジメントを推進する「グローバル&グループ リスクマネジメント委員会」（以下「G&G リスクマネジメント委員会」）を設置しています。グループの経営幹部の中から任命されるチーフ・リスクマネジメント・オフィサー（CRO）を委員長とし、メンバーはカンパニーCRO（Chief Risk Officer）、地域統括会社、戦略本社・職能の責任者



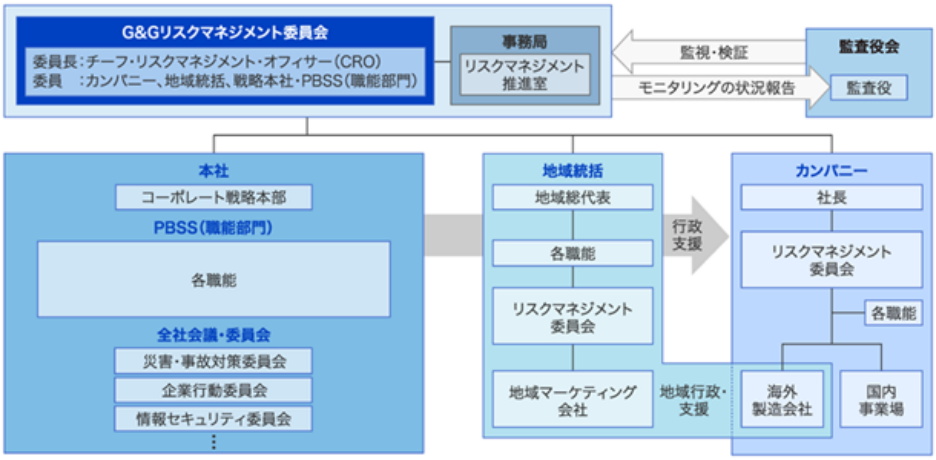
から構成され、事務局はリスクマネジメント推進室が担当しています。

G&G リスクマネジメント委員会は、カンパニー・関係会社・本部および地域統括が実施したリスクアセスメントの結果をもとに全社重要リスクを決定します。これは、コーポレートとしての法的要請への対応の一環です。また、カンパニー・関係会社・本部および地域統括が策定した重要リスクの対策計画をもとに、対策進捗のモニタリングを実施し、必要に応じ職能・各種委員会への指示やカンパニー・関係会社・本部および地域統括への支援を行い、継続的改善を推進します。モニタリングの状況については G&G リスクマネジメン

ト委員会から監査役に報告され、監査役会がその監視と検証を行っています。

基本的枠組み

当社では、G&G リスクマネジメント委員会、カンパニーおよび事業部の 3 つのレベルでリスクマネジメントを推進しています。毎年、カンパニーおよび傘下の事業部等にて事業経営に影響を与えるリスクについてグローバル共通の基準（経営への影響度と発生可能性他）でリスクアセスメントを行い、カンパニー重要リスクを選定し対策を実施します。さらに、このカンパニー重要リスクを踏まえ、全社的見地から全社重要リスクとして取り上げるべきリスクを G&G リスクマネジメント委員会で検討、選定し、対策進捗のモニタリング、改善を行い、全社的なリスク対策の強化を図っています。



- 2

016 年度全社重要リスク

自然災害

（地震、津波、気象災害など）

品質問題

カルテル

サイバー攻撃

- 2017 年度全社重要リスク
  自然災害
  （地震、津波、気象災害など）
  品質問題
  カルテル
  サイバー攻撃
  労働災害

リスク感性の向上

G&G リスクマネジメント委員会では、リスクマネジメントの基本的な考え方を周知徹底し実践するため、パナソニックグループの従業員を対象として、リスクマネジメントに関する教育・啓発活動を計画的に推進しています。全従業員に社内広報を通じて G&G リスクマネジメント委員会の内容（選定された全社重要リスクやその対策進捗）を周知するとともに、リスクマネジメント推進担当者に対しては毎年リスクアセスメントの説明会を実施。当社のリスクマネジメントの基本的な考え方である「リスクマネジメント実施要綱」を解説することで、リスクアセスメントの効果的な推進を行うためのスキルアップを図っています。
また、リスク発現時の対応不全によるリスク拡大を防止することを目的に、事業場長を対象とした「リスク発現時の対応指針」を発行し、徹底しています。新任の海外会社社長、海外赴任前の従業員に対しては、リスクマネジメントの基礎、リスク発現時の対応等についての研修を実施し、海外における現場でのリスク対応力を向上させています。
従業員が潜在的なリスクを報告できる仕組みとしては、コンプライアンス違反や各種ハラスメント、調達活動などに関するホットラインを整備しています。従業員およびお取引先様は、問題と感じた事象をいつでも自主的に通報することができます。また、毎年実施される全従業員対象のコンプライアンス意識実態調査でも職場に潜在的にあるコンプライアンス関連リスクを自主的に報告できる仕組みを設けています。収集されたリスクは各職場にフィードバックされ、リスク対応を行っています。
以下 BCM へとつづく
引用終了

ネット上の公開情報から見る限り、パナソニック株式会社は模範的なリスクマネジメントを展開しており、コーポレート・ガバナンスと内部統制報告書も含めると社外取締役、監査役、内部通告制度についても十分な体制と判断される。

一方、下記記事に見られる不祥事が発生した神戸製鋼所のリスクマネジメントを見ると

データ改ざん　虚偽表示容疑で捜査　東京地検・警視庁

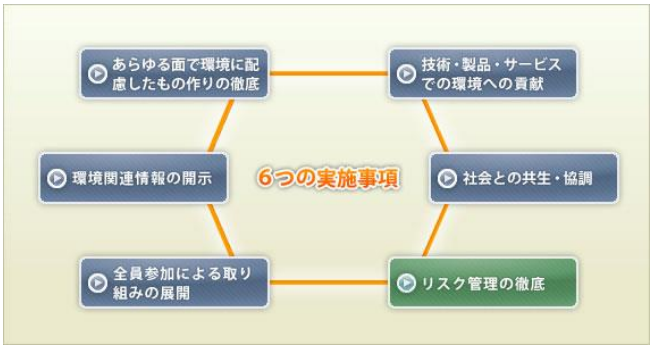
毎日新聞 2018 年 4 月 25 日　神戸製鋼所による品質検査データ改ざん問題で、東京地検特捜部と警視庁捜査２課が不正の実態解明に向け、捜査を始めたことが、捜査関係者への取材で明らかになった。不正競争防止法違反（虚偽表示）容疑を視野に、関係者から事情を聴くとみられる。米司法当局も調査に乗り出していた問題は、刑事事件に発展する可能性が高まった。

http://www.kobelco.co.jp/about_kobelco/csr/kaiji/files/2017riskmanagement.pdf

リスクマネジメントを探すと環境リスクについてしか出てこない

リスク管理の徹底

神戸製鋼グループは、事業活動に伴う環境リスクを把握し、リスク低減活動を実施すると共に、日常の管理手順を定め、適切な管理を実施しています。



次にコンプライアンスに関する記述は

神戸製鋼所企業倫理綱領

http://www.kobelco.co.jp/about_kobelco/kobesteel/cce/cce_jp201506.pdf

２０００年６月制定

２０１５年６月改定

『企業倫理規範』

１．法令その他の社会的規範を遵守し、公正で健全な企業活動を行う。

２．安全性や個人情報･顧客情報の保護に十分配慮し、優れた製品･サービスの提供を通じて社会に貢献する。　・・・・以下省略　７項まで

『企業行動基準』

第 1 事業活動について

1．優れた製品･サービスの提供と安全性に関すること

(1)顧客ニーズの的確な把握

(2)アフターサービス、ユーザーサポート体制の充実とマニュアル化

(3)安全性に関する法令、ガイドラインの遵守

法令や 公的なガイドラインが設けられている場合には、

厳密にそれら を遵守しなければなりません。

(4)安全性に関する自主基準の制定と遵守

(5)わかりやすい取扱説明書の作成

・・・以下省略

8．企業倫理の徹底に関すること

(1)全社的な取組体制の整備

●全社的なコンプライアンス活動を推進する常設のコンプライアンス委員会を設置する。

コンプライアンス委員会は独立した取締役会の諮問機関であり、コンプライアンスに関する方針、監 査、コンプライアンス違反事例についての対応策・再発防止策 を審議・策定した上、これらを取締役会に上程し、更に、重大な法令違反について、違法行為是正のため取締役会に対して勧告する権限を有する。

また、特に必要と認める場合には、第三者委員会の設置を取締役会に勧告する権限を有する。

●コンプライアンスに関連するコードの策定、体制の整備、教育 の実施等全社コンプライアンス活動の取りまとめを行うコンプ ライアンス統括室を設置する。

(2)内部通報制度の整備

●コンプライアンス違反についての内部通報制度として、社外の弁護士を受付窓口とする「内部通報システム」を設置する。

9．経営トップによる取組に関すること

具体的には、経営トップ 自ら指揮をして、速やかに事実調査、原因究明、再発防止策の策定 等を行い、企業としての責任ある適切な対応を打ち出します。また、 人の健康または安全が危険にさらされる場合には、社会に対して明 確な説明を迅速かつ的確に行います。更に、責任の所在を速やかに 明らかにし、社会的に十分理解される形で厳正な処分を行うことと します。事案によっては、経営トップとしての責任を十分認識した 上で、自らに対し厳しい処分を課すこととします。

(注)この『企業行動基準』の制定、廃止および変更は取締役会の決議による。

企業理念関係

昨年、創業 100 周年を迎えた神戸製鋼グループにとって、2006 年度は新たな世紀の始まりであり企業理念を下記の通り策定する。

「神戸製鋼グループ　企業理念」

１．信頼される技術、製品、サービスを提供します

２．社員一人ひとりを活かし、グループの和を尊びます

３．たゆまぬ変革により、新たな価値を創造します

「KOBELCO の約束　Next100 プロジェクト」について

2017 年 5 月 31 日

株式会社神戸製鋼所

当社グループは、全社員が一つになって、より良い企業集団、すなわち「誇り」「自信」「愛着」「希望」溢れる企業集団を作り、当社グループが持続的に発展していくことを目指した活動として、「KOBELCO の約束　Next100 プロジェクト（次の 100 年に向

品質憲章

KOBELCO グループは、製品、サービスにおいて「信頼される品質」を提供するために法令、公的規格ならびにお客様と取り決めた仕様を遵守し、品質向上に向けてたゆまぬ努力を続けてまいります。

神戸製鋼の不正問題が起きたと言う結果を知ってからのためもあるが上記に引用したリスクマネジメント体制を見ると次の点でパナソニックに比べ見劣りする。

・経営理念がパナソニックでは創業者の言葉から、神戸製鋼は新たに見直しで授業員への浸透の歴史が違うと思われる。

・神戸製鋼にも企業倫理、企業行動基準が設定されているが今回の不正ではこれの基準に明らかに反している。

・パナソニックのウエブサイトには組織体制とその運用、教育の記述があるが、神戸製鋼では見つけられなかった。トップのリスクマネジメントへの関与、従業員のコミットメントが低いように推察される。

また、今回の不祥事に関する報告書が下記の通り発表された

2018 年 3 月 6 日 株式会社神戸製鋼所
当社グループにおける不適切行為に関するご報告
当社及び当社グループ会社（当社グループ）における不適切行為に関しまして、お客様、お取引先様、 株主様そのほか多数の皆様に多大なるご迷惑をお掛けしておりますこと、改めて深くお詫び申し上げます。

当社は、当社グループの過去 1 年間（2016 年 9 月～2017 年 8 月）の出荷実績に対する品質自主点検に より発覚した不適切行為（公的規格又は顧客仕様を満たさない製品等につき、検査結果の改ざん又はねつ造等を行うことにより、これらを満たすものとして顧客に出荷又は提供する行為。以下「本件不適切行為」 といいます。）について、2017 年 10 月 26 日、松井巖氏（元福岡高検検事長、弁護士）を委員長とする外 部調査委員会を設置して調査を引き継ぎ、その後、同委員会による調査に全面的に協力してまいりました。 今般、外部調査委員会の調査結果を受け、当社の品質ガバナンス再構築検討委員会や品質問題調査委員 会における検討結果と併せて、当社として、外部調査委員会の調査によって明らかになった事実関係をご説明するとともに、その原因分析及び再発防止策を報告するため、当社取締役会において、本日付「当社 グループにおける不適切行為に関する報告書」（以下「本報告書」といいます。）の公表を決議いたしまし た。本報告書の概要は、以下のとおりです。

途中省略

２．本件不適切行為の原因分析
外部調査委員会による調査結果と当社における検討から、本件不適切行為を引き起こした原因は、（1） 収益偏重の経営と不十分な組織体制、（2）バランスを欠いた工場運営と社員の品質コンプライアンス意識 の低下、（3）本件不適切行為を容易にする不十分な品質管理手続、の三つに集約されると考えています

省略

３．本件不適切行為に対する再発防止策
上記の原因分析に基づき、外部調査委員会からの提言も踏まえて当社がとりまとめた、本件不適切行為 に対する再発防止策は、以下のとおりです。
（1） ガバナンス面－品質ガバナンス体制を再構築すべく、以下を実施いたします。
ア．グループ企業理念の浸透
イ．取締役会のあり方
ウ．リスク管理体制の見直し
エ．組織の閉鎖性の改善
オ．品質保証体制の見直し

以下省略

途中経過の公表など大きく改善に向けて舵を切った様子は見て取れるが、本格的なリスク

マネジメントの浸透には全社をあげた更なる努力と学習が必要であると思われる。
具体的には品質確保のための作り直しのコストアップ、納期遅れなどによる契約の喪失など売上、利益の減少とのバランスを具体的に管理職はどのように指示するのか。
各子会社間での人事ローテーションが少ないためのガバナンスの浸透不足が指摘されているが、固有技術を無視した人事異動は競争力を落とす可能性が大きく具体化には困難が伴う。
リスクマネジメントのレベルから、企業を分類すれば、神戸製鋼以下の企業は多数存在すると推定される。またパナソニックは最高位に近いと視察する。

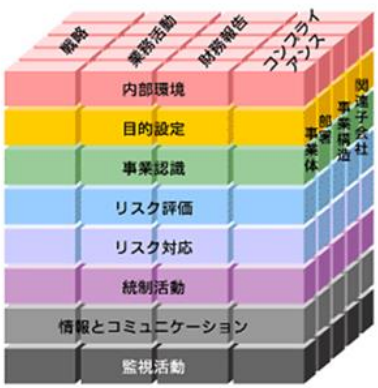
リスクマネジメントの実施のレベル測定指標として下記を提案したい

項目	レベルの評価内容
企業理念	社会性の強調程度、浸透程度、歴史の長さ
組織体制	CRO の指定、位置づけ、トップの意識、活躍度
社外取締役	社外取締役比率、監査指名委員会等設置会社
子会社、グローバル対応	海外子会社を含むリスクマネジメントの体制と浸透
内部通報制度	制度の設置、通報者保護、頻度内容
社内教育	内容、頻度、範囲
ICT 活用	ERM の活用度合い

2017 年版 COSO－ERM

http://www.itmedia.co.jp/im/articles/0505/10/news111.html
https://www.newton-consulting.co.jp/bcmnavi/column/20170421_cosoerm2017.html

2002 年に制定されたサーベンス・オクスリー法が求める内部統制に関して、具体的な実施に際しては COSO フレームワークに基づいて行うよう SEC（米国証券取引委員）が定めている。2006 年の J-SOX 法（日本）対応にあたっての根幹を支えるものとなった。



COSO では内部統制フレームワークを拡張する形で、2004 年に「エンタープライズリスクマネジメント・フレームワーク」（ERM フレームワーク）を公表した。しかし 10 年以上経過し、環境変化もあるために 2017 年版として改訂を行った。

この間に新しいリスクが生まれ、対応も複雑になった。テロ、地震、爆発、サイバー攻撃、偽装、リコール、過重労働、風評、知財違反・・・等など、組織をとりまくリスクは増える一方である。企業経営者もリスクマネジメントを軽視できなくなってきた。組織の戦略遂行に合わせて、効果的・効率的なリスクマネジメントの実践がこれまで以上に必要になった。

また同時に 2004 年版の反省として次の誤解を解消するように努力した。

誤解

①ERM は機能や 部門である、

②ERM とはリスクを一覧化することである、

③ERM とは内部統制を対象とすることである、

④ERM はチェッ クリストである、

⑤ERM は中小規模の組織には適用できないなど

２０１７年版

COSO-ERM（2017）の目的

リスクマネジメントはコストサイドだけではなく、適切に運用することにより企業の業績を高めるものであり、組織の経営目的達成を促進するために、組織に取り込むべきリスクマネジメントのフレームワークなので経営者自らがトップダウンで実施する必要がある。上図に示したように左側に位置付けられた企業理念（Mission, Vision and Core value）を達成し、一番右側のより強化された業績を達成するために中央に表示されている戦略および経営目標を５色で表されている下記の５つのカテゴリーを間断なく回すことが推奨されている。

COSO-ERM は、自らの意義を次のように説明している。

・戦略策定や実行の際の ERM の役割に大きなヒントを提供すること
・パフォーマンスとリスクマネジメントの間の連携を強めること
・ガバナンスと監査の期待値を取り込むこと
・市場とオペレーションのグローバリゼーション、共通（ただし）地理的な特性に合わせてカスタマイズされたアプローチの必要性を知ること
・より複雑化するビジネスコンテキストの中で、目標設定やその達成のためにどのようにリスクの捉え方を提供すること
・よりステークホルダーへの透過性を強めるため期待値を特定するための報告を拡張すること
・進化する技術と意思決定を支援するためのデータ分析の成長を取り込むこと

5 つのカテゴリーと 23 の原則

1 つ目の「リスクガバナンス及び文化」では、Mission, Vision and Core value に基づき取締役会など組織の機関設計やトップの倫理感のあるべき姿について述べている。

2 つ目の「リスク、戦略、及び目標設定」では、組織の戦略策定におけるリスクマネジメントについて述べている。いわゆる戦略リスクマネジメントです。そもそも組織が採用する戦略が、経営理念やビジョンからかけ離れてしまわないか、組織がとれるリスクの大きさの範囲内におさまる戦略かなどをどのように考えるべきかを解説している。

3 つ目の「実行上のリスク」では、組織が選択した戦略を遂行する上で、その目標達成に影響を与えるリスクマネジメントについて言及している。ここで、リスクマネジメントを支える代表的なプロセスである「リスク特定」「リスク分析」「リスク評価」「リスク対応」が登場する。COSO-ERM（2017）では、リスク対応に加え、どのように対応の現状を「見える化」するかについても解説している。

4 つ目の「リスク情報、コミュニケーションと報告」では、組織が認識したリスクに関する情報を、いつ誰にどうやってどれくらいのスピード感で報告・共有するのかを考えるポイントについて解説している。

5 つ目の「リスクマネジメントパフォーマンスのモニタリング」では、上記 1～4 つまでの

活動が適切に行われているかどうか、期待通りの効果を発揮しているかどうかのモニタリングについて言及している。具体的にはたとえば、ERM に関わる内部監査や現場でのセルフモニタリングなどに関する話で、組織のリスクマネジメントの仕組みを継続的改善するための鍵となる活動である。
考えて見れば
企業経営そのものがリスクマネジメントそのものであるとも言える。例えば今話題の武田製薬の巨額買収は社運を左右する最大経営判断であり、チャンス且つリスクである。

武田薬品
製薬大手シャイアー７兆円買収、最終調整
毎日新聞 2018 年 4 月 25 日　20 時 29 分
武田薬品工業は２５日、アイルランドの製薬大手シャイアーを買収する方向で最終調整に入った。武田は約４６０億ポンド（約７兆円）でシャイアーの全株式を取得すると提案し、シャイアーの取締役会は提案を自社の株主に推奨する方針を決めた。武田は最終合意の期限を当初の英国時間２５日午後５時（日本時間２６日午前１時）から５月８日まで延長し、詰めの交渉を急ぐ。

「ビジョナリーカンパニー」に記述されているように社内全員が良い企業文化 Mission, Vision, and Core Values を共用、実行し続けることが効果的な企業運営の基礎であり、それが COSO2017 版上記図の左側に一致している。
上記武田薬品の例を COSO 提言に当てはめれば大型企業買収の与えるリスクの大きさが企業の存続に必要な資金、人材、技術などの供給サイドの限界内にあるか、また買収後の PMI 実行計画がどの程度順調に行くかなどを上記に示された５つの項目で適宜、関連部門が効率的、有機的に PDCA を回してゆくことを推奨していると思われる。つまりリスクマネジメントを経営の根幹に位置付けたことになろう。

ガバナンス・リスク・コンプライアンス

更に下記のダイヤモンド誌を引用したい
http://diamond.jp/articles/-/150942
以下引用
「攻めの IT」と「守りの IT」は表裏一体
上原 聖 【第 1 回】 2017 年 12 月 13 日より

「The 2017 CEO Survey: CIOs Must Scale Up Digital Business」によると、CEO のトッププライオリティとして“ビジネスの成長”があげられている。興味深いことは、テクノロジーの活用、最近のバズワードで言うところの“デジタルトランスフォーメーション”がセカンドプライオリティにあげられていることである。

このことは、ビジネスの成長とテクノロジーの活用は、今や切っても切れない関係にあるということを示している。途中省略
ビジネスの成長はトッププライオリティとして、企業は絶えず新しい事業機会を模索している。しかしながら、この事業機会の裏の側面であるリスクマネジメントを過小評価してはいけない。つまりは、ビジネスの成長を取り込むためには、その不確実性に対処するための「ビジネスリスクマネジメント」が必要不可欠となる。
途中省略
他にも、M&A（Merger and Acquisition）による合併や買収という手段をとるにしても、事業継続や合併・買収後の統合（PMI: Post Merger Integration）に関するリスクマネジメントが、新市場参入や新事業開発に伴う他社との業務提携や技術供与などのアライアンスを組むにしても、「サードパーティ」に関するリスクマネジメントが必要になる。
このように、ビジネスの成長の裏の側面としてのリスクマネジメントは、広範囲かつ多岐にわたるため、リスクマネジメントと一言で言っても、そう簡単にマネジメントできる時代ではなくなっていることも事実である。途中省略

思い出されるのは東芝によるウエスティングハウスの買収である

2017年3月に公表された米国公認会計士協会の調査「8th Annual AICPA & NC State Poole College of Management Survey」によると、約7割の組織（企業および非営利組織）は、過去5年間にリスクの量と複雑さが大幅に増加したと回答している。
従って、ビジネス戦略を準備する上では、法令や基準に従うだけの“既成”のリスクマネジメントではなく、ビジネス戦略の目的や方針を十分に反映した“特注”のリスクマネジメントが必要となる。つまりは、既成の枠組みでは捉えきれない、ガバナンス・リスク・コンプライアンス（以下、GRC）全ての領域にまたがる、全社横断的なリスクマネジメントプログラムを構築し、ビジネス展開をする上での不確定要素をできるだけ炙り出し、対処していく活動が必要となる。
一方で、この特注のリスクマネジメントに関するプログラムを実際に運用することで、ビジネスパフォーマンスが向上したとする調査結果もある。
具体的には、2017年2月に公表されたIDC社の調査「Quantitatively analyzed return across 6 FIs and 1 HC provider」によると、GRCに関するプログラムを積極的に活用する企業は、リスク評価の効率が33%高まったこと、加えて、63%の企業がより迅速にセキュリティインシデントを解決できたこと、そして、成熟したリスクマネジメントプログラムを活用することで収益性が10%高まった、という結果をもたらしている。
では、ビジネスの成長に直結する「リスクマネジメントプログラムを実践する」とはどの

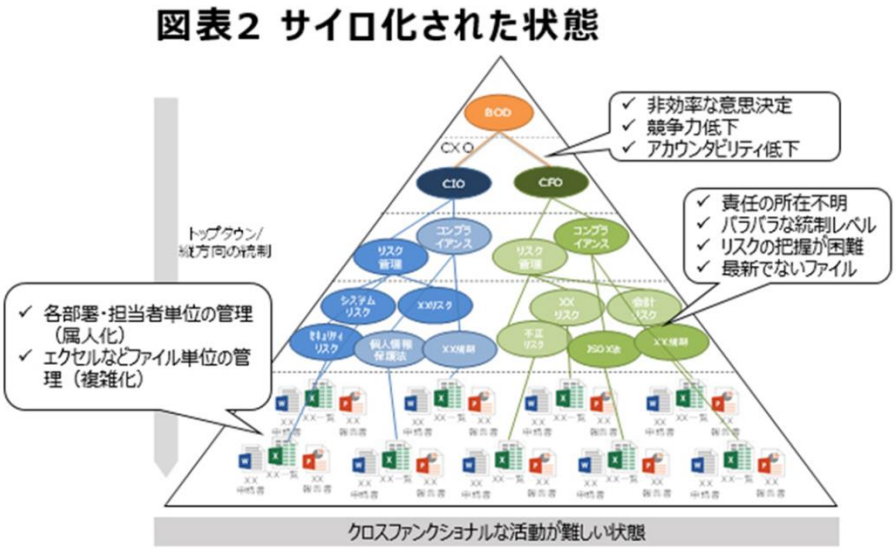
ようことであろうか。それは、ビジネス戦略の目的や方針を十分に反映し、GRC 全ての領域にまたがる、全社横断的なリスクマネジメントプログラムを準備、計画、実行することである。具体的には、ビジネス戦略を実行する上での不確定要素を特定するとともに、その対処策であるコントロールを含めたアカウンタビリティ（説明責任）を明確化する。さらに、リスクとコントロールに関連するビジネス資産（組織、ビジネスプロセス、機器、施設、情報など）を特定し関連づけることで、持続・反復・監査が可能な情報基盤を確立することである。

リスクの考え方
現場と経営とのギャップを越える
上原 聖 【第 2 回】 2017 年 12 月 28 日

リスクマネジメント活動について語るとき、経営陣とリスク管理者の間には、認識の大きなギャップが存在することが多いのではなかろうか。

つまりは、リスクマネジメントについて経営陣が語るとき、その興味は、いかにしてビジネスリスクへ対応していくべきか、具体的には、売上や利益、コストや株主への期待に対する不確実性をマネジメントし、事業を永続的に成長させていく“ゴーイングコンサーン”であったり、ビジネスを遂行する上での法的な影響や株価への影響などの“ビジネスインパクト”を最低限に抑えることであったりする。一方で、リスクマネジメントについてリスク管理者が語るとき、その興味は、各々の責任範囲に限定されてしまう。例えばコンプライアンスリスクのオーナー（責任者）であれば、J-SOX 法や個人情報保護法などの法令対応は適切か、オペレーショナルリスクのオーナーであれば、事故件数、人による過誤やオペレーションプロセスの欠陥が適切にマネジメントされているか、そして、セキュリティリスクのオーナーであれば、バッファオーバーフロー、SQL インジェクション、サ

ービス拒否攻撃などへの対策は十分かなど、限定された範囲における個別最適化された活動に終始してしまう。



途中省略

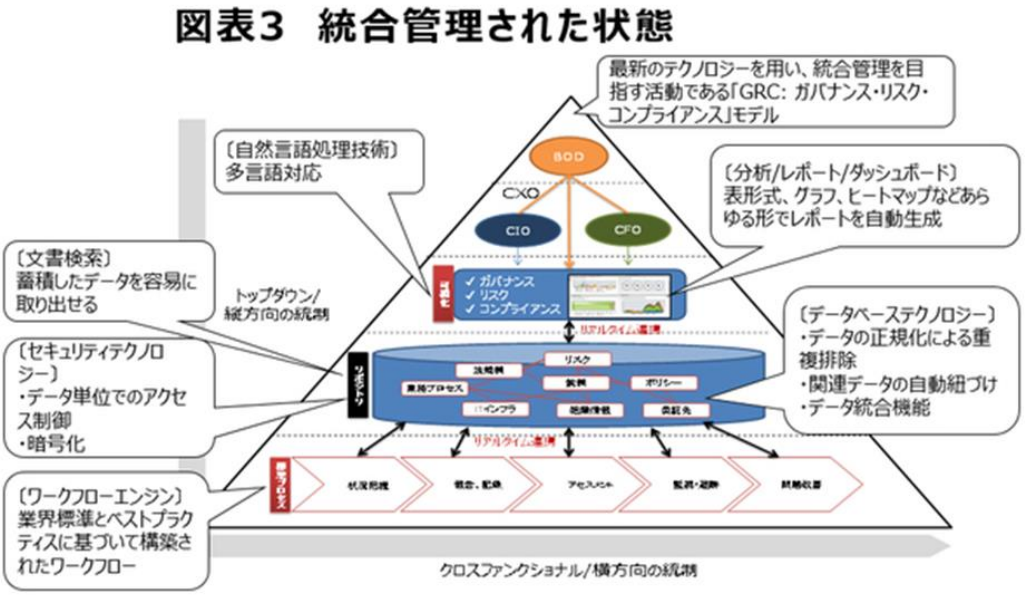
多くの企業では組織が縦割りでありガバナンス・リスク・コンプライアンス（以下、GRC）が実施できない

インターネットが爆発的に普及する以前、別の言い方をすると、IT については情報システム部門の範囲内で管理可能な時代であれば、このような組織構造でも大きな問題は発生しなかったであろう。しかしながら、インターネットの業務利用が急速に進むことで、ユーザ部門でも容易に Web ベースのシステム導入が可能になり、また、多くのクラウドサービス事業者の存在やネットワーク網の高度化により、データのやり取りも容易になった。

この時代背景に呼応する形で、多くの規制が設けられたことで、今では情報システム部門だけでなく、コンプライアンス部門、リスク管理部門、内部監査部門などが横連携しないとリスクマネジメント活動が追い付かない時代になっている。

自社の「トップ 10 リスク」は何か？
――ビジネスリスクを測定し、管理する
上原 聖
【第 3 回】 2018 年 1 月 31 日
グローバル先進企業の統合管理事例

では、グローバル先進企業はこのような時代背景に対して、どのような対応をしているのであろうか。具体的には、どのような形で横連携し、統合管理を実現しているのであろうか。

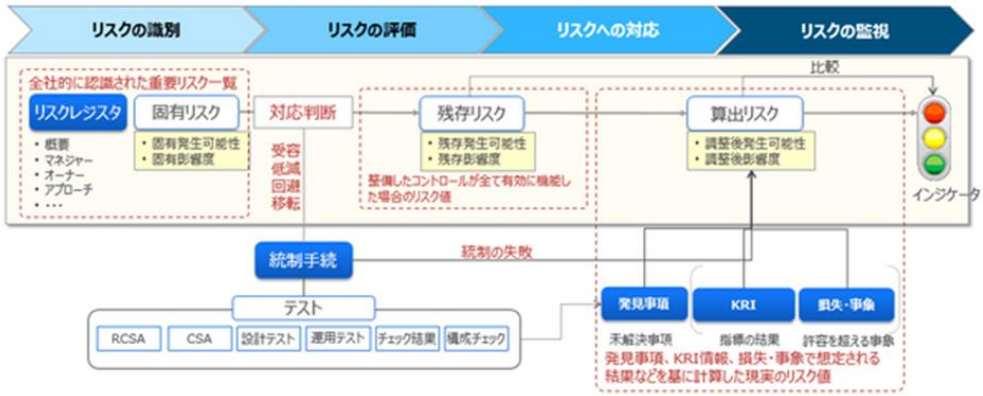


弊社がこれまで多くのグローバル企業を支援してきた経

験からまとめると、次の 6 つのテクノロジーを活用することで、統合管理を実現している。
1.データベーステクノロジー
2.ワークフローエンジン
3.分析／レポート／ダッシュボード
4.文書検索テクノロジー
5.セキュリティテクノロジー
6.自然言語処理技術
途中略
統合的なリスクマネジメントの実践事例

図表4．従来型のリスク監視のアプローチ

図表5．先端企業が採用しているリスク監視のアプローチ

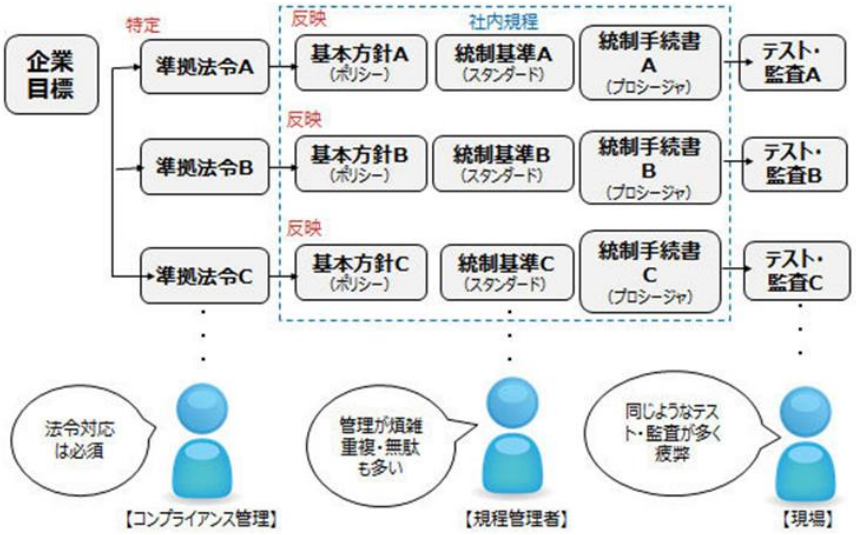


途中省略
企業の内部監査はビジネス成長の原動力になる理由
上原 聖
【第 4 回】

2018 年 3 月 7 日
この回のほぼ全部を省略するが、効果につき下記のように述べている。
例えば CFO を対象とした「FM グローバルホワイトペーパー（2017 年発行）」によると、CFO の 86%が「オペレーショナルリスクに厳格かつ効果的に取り組むことで、収益変動を減らすのに役立つ」と回答している。また共通するメッセージとして、「リスクマネジメントの改善は、経営陣と株主が望むビジネスの成長を促進する」と示唆している。

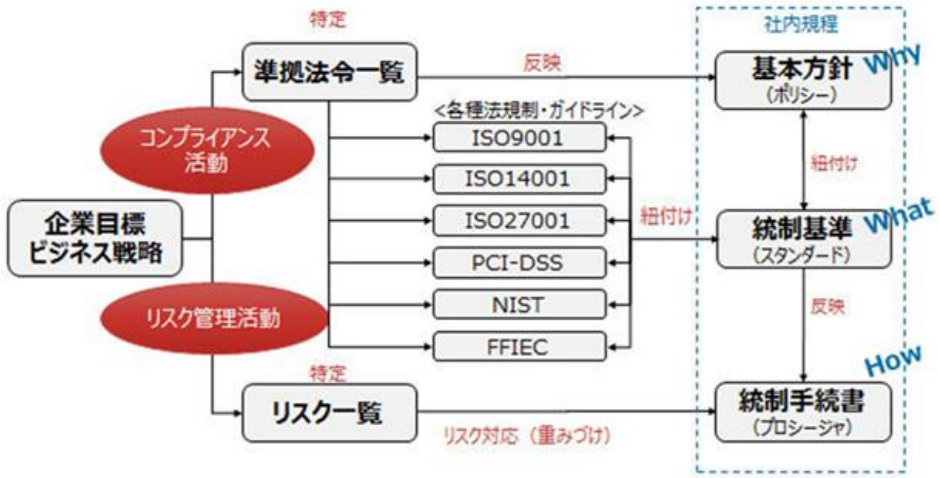
またこの記事で共感できるのは、事業部門で負担である。 リスクマネジメントが嫌わせるのは経営トップの軽視ばかりではなく、現場レベルでは生産性を阻害する作業や事務作業が増えるばかりという点ではなかろうか。

図表2．事業部門の負荷増加を招くケース



ここで登場するのが、統合管理モデルである。このモデルで重要なのが、企業目標・ビジネス戦略で、これらを実現するために必要な、市場のルールへの対応を“コンプライアンス活動”、不確実性への対応を“リスクマネジメント活動”として位置付ける。例えば、「米国でインターネットを介した金融事業を立ち上げる」という企業目標の場合、金融サービスを実施する上で準拠しなければならない法規制への対応が“コンプライアンス活動”となり、インターネットに関連するサイバー攻撃などへの対応が“リスクマネジメント活動”となるイメージだ。

図表3．リスクマネジメント活動の統合管理モデル



まず初めに、自社に関連する法規制およびリスクを洗い出して一覧化し、各法規制およびリスクを鑑みて、漏れなく重複のない形でコントロールをデザインする。ここでポイントとなるのが、統制基準をキーとして、コントロールをデザインすることである。統制基準とは、多くの法規制を横串で通せる形に標準化したもので、例えば、「システムログの管理」という形に標準化すると、多くの法規制と紐づけることが可能になる。

次に、統制基準と自社のポリシーを紐づけることで、統制基準に紐づく法規制が変更になった場合、どのポシリーを変更すべきかを容易に特定することが可能になる。

途中省略

統合管理モデルの真の効果

このように、統合管理モデルを採用することで、統制活動の効率化により事業部門の負荷が軽減され、結果として三線防衛モデルが効果的に機能する可能性が高まる。そして最も重要な点は、これまでの第二線の閉じられた活動としてのリスクマネジメントから、事業部門や監査部門を巻き込んだ活動につながり、更にはビジネスの成長を後押しする活動へと昇華できることであろう。

引用終了

上記記事のように実行できれば、リスク管理が強力な経営革新手段へと変革できる。しかしこのシステム導入にかかる費用、労力、運営コストに対して効果はどのようになるのであろうか。

おわりに

引用が多い研究報告書となった。その理由は研究会のスタートがリスクは時代や状況により変化するので「リスクマネジメントにベストプラクティス」は無いのではないかと言う議論からスタートしたからである。
また、この研究に着手するまでリスクマネジメントの担当部門は戦略企画部門や営業や開発の第 1 線に比べ地味な守り主体でトップマネージメントとは遠い存在と言うイメージをいだいていた。
しかしながら議論と調査を続けるうちに COSO の 2017 年改訂に見られるようにリスクマネジメントを経営の根幹として位置付けるようになって来ていることに気付かされた。
それは従来、リスクを危険性主体で捉え、損失の最小化を中心に着目して来たことに由来している。最近のリスクマネジメントは新規事業への進出や M&A などの戦略的活動もしっかりと範疇に取り入れることにより企業経営の根幹として位置付けられるようになって来た。広くとらえれば人類の活動そのもの（生きて行くこと）がリスクマネジメントとも言え、企業経営においても日々新しい活動を展開するほど新たなリスクが発生するので先行的にリスクを管理することには論理的にも合理性がある。
このようなリスクマネジメントそのものへの視点の転換により、世の中と自身の企業の変化を積極的に取り入れ対応する思想、組織、IT 技術を中心とするサポート体制を理想的に整えることが「リスクマネジメントのベストプラクティス」と言えるのではないかと言う結論である。
理想とする方向性は判った。しかしながらプラクティスと呼べる実行性まで理解と手法の開発が実行可能なレベルに至っているかと言う点では現状では大きな疑問点がある。

- 2017 年版の COSO に示されるようにリスクマネジメントの解釈の浸透
  企業内部でのリスクマネジメントへの理解が従来の損失の最小化レベルに止まっているのが現状ではないか
- 上記に引用した上原聖の先端企業の IT 活用例は理想的には見えるが実効性、投資などの面から普及には時間が掛かるように思える。

これらの考えは未だ一般的ではないと思われ、多くを引用した次第である。
今後もリスクマネジメントこの理想の方向に向かいどのように進歩して行くかを見守って行きたい。
最後となるがメンターをはじめとする DF 企業ガバナンス部会の方々に大変お世話になったことに感謝申し上げます。