ARIMASS大会自由論題資料

コーポレートガバナンスと リスクマネジメントを考える

2021年10月23日

内田　知男

（目　次）

（はじめに）

前回、「企業事件と内部統制」をテーマに取り上げ、企業事件において、企業が同じような要因で何故失敗を繰り返すか検証した。その上で、企業が不幸な事件を繰り返さないためにはどのような経営を実践していくべきか、3つのディフェンスラインモデルを基にコーポレートガバナンスの視点から考察した。
今回は、最近の動向や議論も踏まえつつ、コーポレートガバナンスの実効性を上げていくうえで、リスクマネジメントが果たすべき役割やあり方について考えてみたい。

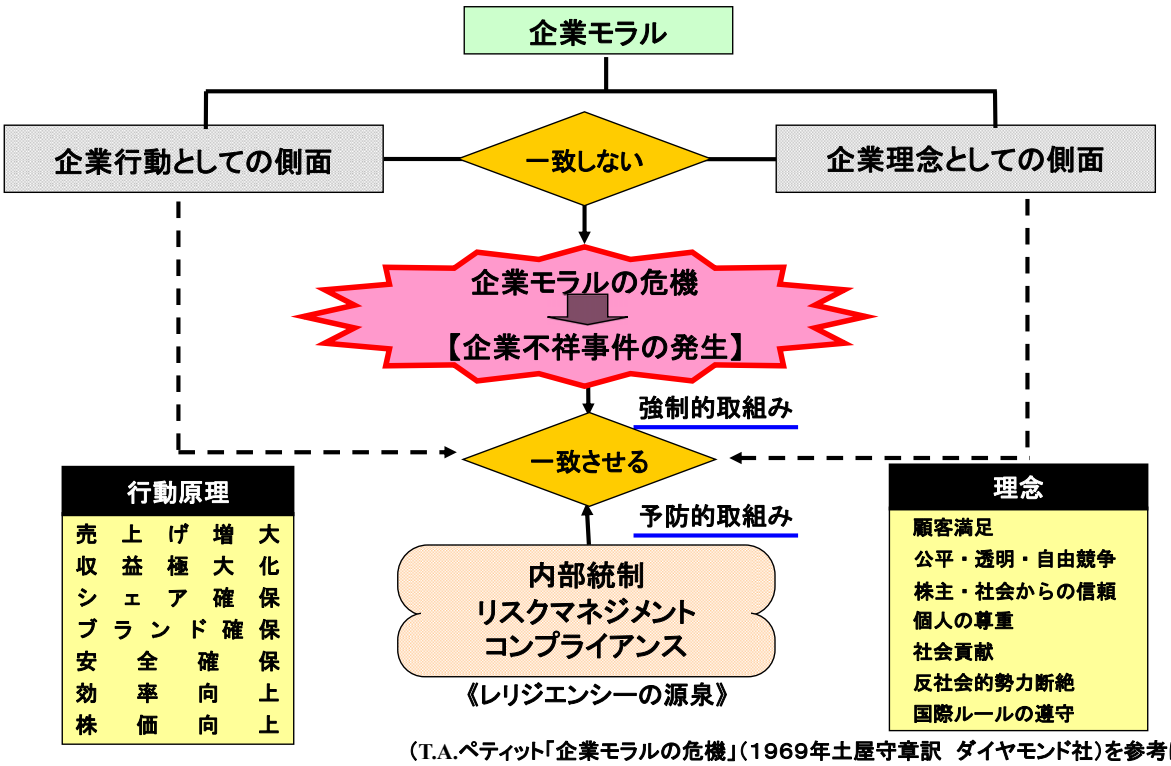
自己紹介
・三井住友銀行（住友銀行）29年
・銀泉リスクソリューション10年　（リスクマネジメント）
・エリーパワー株式会社常勤監査役　10年
・大分大学、慶応SFC、関西学院大学等講師16年（リスクマネジメント論）
・CIA（公認内部監査人）
著書：「リスクマネジメントの実務」2011年中央経済社
＊本論は所属先とは一切関係なく個人の見解である

I. 前回「企業事件と内部統制」のまとめ(1)

1．企業モラル
・企業事件における発生要因は極めて類似，企業は同じような失敗を繰り返す「失敗の本質」について企業モラルの観点から考察。
・企業モラルは「理念としての側面」と「行動としての側面」を備える。「理念」と「行動」との一致が図れないのが「失敗の本質」となるのである。
2．未然防止
・企業事件の未然防止を図る取組みこそが、内部統制、リスクマネジメントの役割となる「理念」と「行動」を一致させる「言行一致」の経営を実現していくことが課題となる。
3．3つのディフェンスライン
・COSOとIIA（内部監査人協会）は，内部統制は3つのディフェンスラインモデルと結び付けて組織全体のガバナンス体制向上に繋げていくべきと提案。
・しかし、企業事件の事例分析からは、こうしたディフェンスラインは易々と打ち破られていたのが現実であった。3つのディフェンスラインを構築するのみでは「言行一致」の経営は実現できない。
4．コーポレートガバナンスへの期待
・さらに必要とされるのはディフェンスラインフレームワークの中で、「理念」の側面からコーポレートガバナンスが有効に機能を発揮することが必須条件となる。
・そのためには、Governing Bodyから内部監査へのルート明確化が課題となる。

Ⅰ．前回まとめ(2)「失敗の本質」企業モラルとコンプライアンス

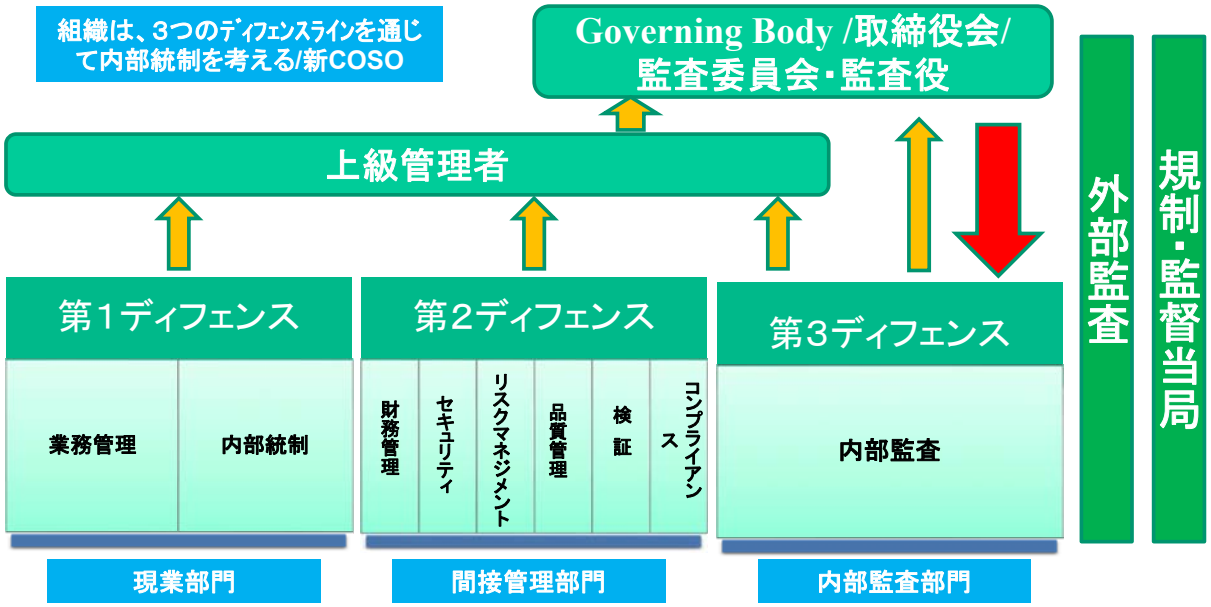
企業モラルの行動的側面、理念的側面は一致するとは限らず、企業モラルの危機が発生する。
行動と理念を一致させるための予防的活動が内部統制、リスクマネジメント、コンプライアンスといえる。



（T.A.ペティット「企業モラルの危機」（1969年土屋守章訳　ダイヤモンド社）を参考に作成）

Ⅰ. 前回まとめ(3)企業リスク/不正対応への3つのディフェンスライン

企業における諸リスクや不正防止のための多層のディフェンスラインが設けられる。
現業マネジメントにとして実践される第1ディフェンス。諸リスクを対象とする管理部門の第2ディフェンス。
内部監査の第3ディフェンス等である。これらのディフェンスライン情報は取締役、監査委員、監査役等「ガバニングボディ」 にエスカレーションされガバナンスの実効性が維持される筋合いとなる



（資料）IIA　Position Paper　第48回内部監査推進大会「監査役会と内部監査部門の理想的な関係」参照

II. その後の動き
コーポレートガバナンスコードと対話ガイドラインの改訂（2021年）

1. コーポレートガバナンスコードと対話ガイドラインの改訂の経緯

（1）2020年7月コーポレートガバナンス改革推進に関する成長戦略フォローアップ閣議決定
「2022年4月の市場構造改革実施に向けて、2021年中に改訂が予定される『コーポレートガバナンスコード』において一段高い水準のガバナンスを求めることとする」とされフォローアップ会議で議論が進められた

（2）2020年12月、フォローアップ会議は意見書「コロナ後の企業の変革に向けた取締役会の機能発揮や企業の中核人材の多様性の確保」を公表

（3）さらに、フォローアップ会議において、本年4月6日「コーポレートガバナンスコードと対話ガイドラインの改訂について」の提言が取りまとめられ、パブリックコメントを経て、2021年6月11日「改訂コード及び改訂対話ガイドライン」が公表された。
（ガイドラインの主要ポイント）
①取締役会の機能発揮：
②企業の中核人材における多様性の確保：
③サステナビリティを巡る課題への取組：
④上記以外の主要課題：
⇒「監査に関する信頼性の確保及び内部統制・リスク管理」グループ全体を含めた適切な内部統制や全社的リスク管理体制の構築と運用状況の監督

II. その後の動き
2. 改訂ガイドライン「監査の信頼性の確保」
（1）実効的な内部統制・リスク管理

フォローアップ会議での議論

・企業を取り巻く環境変化が加速する中で、企業活動のグローバル化に伴うグローバルマネジメントの重要性や、デジタル化等に伴う新たなリスクに対する多様な視点からのマネジメントの必要性が高まっていることを認識していくことが重要
・内部統制やリスクマネジメントを単なる守りとみなして、コストをできるだけかけたくないとする風潮を変えて行く必要がある
・迅速果断な経営判断を可能にするために取るべきリスク、取れる範囲のリスクを、経営において認識することが重要

改訂版コーポレートガバナンスコード

補充原則4－3④ ~~コンプライアンスや財務報告に係る~~内部統制や先を見越した全社的リスク管理体制の整備は、適切なコンプライアンスの確保とリスクテイクの裏付けとなり得るものであるがり、取締役会は、グループ全体を含めたこれらの体制をの 適切にな構築しや、内部監査部門を活用しつつ、その運用状況をが有効に行わ れている~~か否かの~~監督~~に重点を置くべ~~すべきである。~~り、個別の業務執行に係 るコンプライアンスの審査に終始すべきではない~~

（出所）金融庁資料

II. その後の動き

2. 改訂ガイドライン「監査の信頼性の確保」

(2)内部監査部門の活用

フォローアップ会議での議論

・内部監査部門が一定の独立性を持って有効に機能するよう、取締役会や監査役等に対して直接報告が行われる仕組みの確立を促すことが重要であり、こうした内部監査の問題をはじめ、監査の信頼性確保に向けた取り組みについて検討すべき
・内部監査部門によるいわゆるデュアルレポーティングラインは重要である
・監査担当役員が自ら調査を行うことには限界があり、内部監査部門との連携を図る必要性がある。この点は、監査役、監査等委員、監査委員のいずれにも共通する話である

改訂版コーポレートガバナンスコード

補充原則4－13③
上場会社は、*取締役会及び監査役会の機能発揮に向け、内部監査部門がこれらに対しても適切に直接報告を行う仕組みを構築すること等により*、内部監査部門と取締役・監査役との連携を確保すべきである。また、上場会社は、例えば、社外取締役・社外監査役の指示を受けて会社の情報を適確に提供できるよう社 内との連絡・調整にあたる者の選任など、社外取締役や社外監査役に必要な情報を適確に提供するための工夫を行うべきである。

(出所)金融庁資料

II. その後の動き

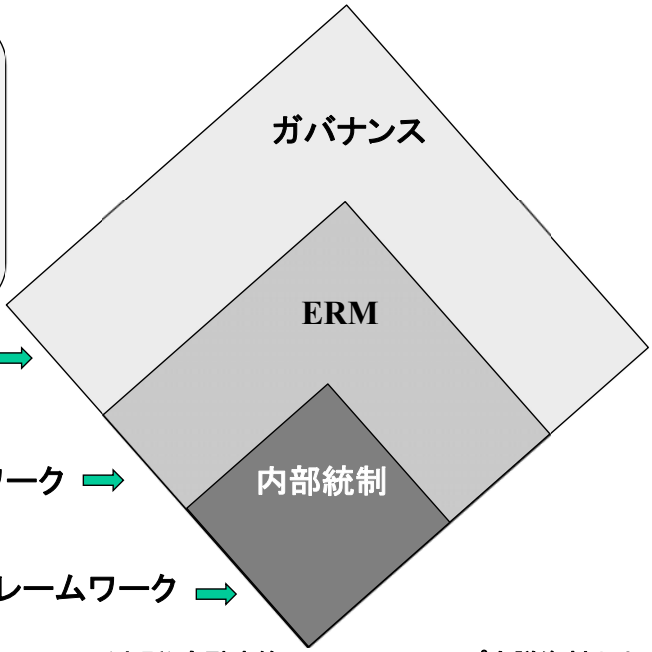
2. 改訂ガイドライン「監査の信頼性の確保」

(3)COSO内部統制とERMについて

フォローアップ会議(第25回)において、米国COSOにおいて、内部統制、リスクマネジメントとガバナンスの関係について以下のように整理されていることが紹介されている

①内部統制は、全社的リスクマネジメントの基盤として、ERMフレームワーク内に位置づけられる。ERMフレームワークは内部統制を超えた領域に焦点を当てている。
②内部統制フレームワークとERMフレームワークは繰り返されず、内部統制フレームワークを参照する形とされる。
③ガバナンスは、これらを含む最上位の概念として位置づけられている。

「内部統制はリスクマネジメントと一体になって機能する」2005年経済産業省リスク管理内部統制研究会報告書



(出所)金融庁第25回フォローアップ会議資料より

Ⅲ. コーポレートガバナンスとリスクマネジメント

1. コーポレートガバナンスとは

（1）ラテン語語源“gubernare”:
舵を取る。「指導する人物は船尾に静かに座して、めったに身動きしない」との引用句が存在

（2）世界銀行コーポレートガバナンス財務的側面委員会定義1999年:
「会社がそれによって指揮され、統制されるシステム」

（3）コーポレートガバナンスコード:
明確な定義はないものの基本原則1が基本的な考え方となる
「上場会社は、株主の権利が実質的に確保されるよう適切な対応を行うとともに、株主がその権利を適切に行使することができる環境の整備を行うべきである。また、上場会社は、株主の実質的な平等性を確保すべきである。少数株主や外国人株主については、株主の権利の実質的な確保、権利行使に係る環境や実質的な平等性の確保に課題や懸念が生じやすい面があることから、十分に配慮を行うべきである」

2. コーポレートガバナンスとリスクマネジメント

株主の目的は株主価値の最大化
⇒株主価値はあらゆるステークホルダーの要請に基づく社会的ルールの下で最大化が図られる
⇒株主目的とステークホルダーの目的が一致する経営の実現を図るのがコーポレートガバナンス
⇒株主やステークホルダーの目的に影響を与える事象が「リスク」
⇒リスクマネジメントはその「リスク」を対象として実施
⇒リスクマネジメントはコーポレートガバナンス実践の基礎的要素となる
⇒ガバニングボディの取締役、監査役などはリスクマネジメントの力量を持つべき

Ⅲ. コーポレートガバナンスとリスクマネジメント

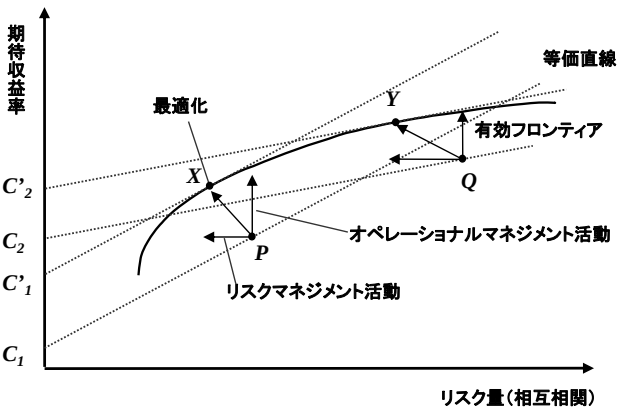
2. 企業価値の創造とリスクマネジメント

リスクマネジメントと企業価値の関係については、以下のように示すことが可能。「企業行動」としてのオペレーショナルマネジメント活動と「企業理念」としてのリスクマネジメント活動の最適化された組み合わせにより企業価値の最大化が図られることになる。

（イ）左図で直線C_1の傾きはリスク量（相互相関）と期待収益率との関係を示している。
同じ傾きをもつC'_1とはリスクと期待収益率について同一の関係をもつ（リスク価格が同じ）

（ロ）今、C_1上に事象Pが展開されているとする。企業は、リスクマネジメント活動によりリスクを低減（図では左方へ）すると同時に期待収益率を努めるため、オペレーショナルマネジメントを展開（図では上方へ）する。その結果、それ以上リスク量を低減することも期待収益率を増大することもできない最適化されたX点に到達する。
同じように等価線C_2上のQの最適化点はYとなる。
こうした最適化点の集合が企業活動ポートフォリオの有効フロンティアとなる。

（ハ）リスクを低減するための左方に向けての「リスクマネジメント活動」と期待収益率の上方に押し上げる「オペレーショナルマネジメント活動」が適切に組み合わされた戦略マネジメントの結果として、期待収益率とリスクとの関係の最適化が図られる。リスクマネジメントが戦略マネジメントにおける、不可欠な役割と機能を果たすことによって、企業価値の最大化を図ることが可能になるのである。



（出所）
Marchel Boyer,Martin Boyer and Rene Garcia[2005]The Value of Risk Mnegement: A Frontier Analysisを参考に作成

（ノーベル経済学賞ハリー・マコービッツのポートフォリオ理論を一般化して考察したもの）

Ⅳ. リスクマネジメントについて

1. COS・ERM

（1）COS・ERM改定の経緯

フォローアップ会議において、実効性のある内部統制・リスク管理の必要性が強調され、COSO・ERMについての紹介がなされた。コーポレートガバナンスにおいてリスクマネジメントが果たすべき役割は重要であるものの、実際のリスクマネジメントが有効に機能しているかは別問題となる。COSO・ERMも2004年公表されてから、2013年、2016年に改定されている。各々の改定のポイントは以下の通りとなるが、とくに2016年の改定は、ERMが十分活用されず経営中枢に届いていないことへの打開がねらいであることが窺われる

㋑2013年5月COSOフレームワーク改定

①原則：内部統制の構成要素に内在する基本的な概念が17の『原則』として明示された。
②報告目的の拡大：内部統制の目的の「財務報告」が「報告」に変更され、非財務報告も対象に含まれることとなった。環境へのアップデートが趣旨とされる。

㋺2016年COSO・ERM改定

COSO・ERM改定の背景として以下が指摘されている。
①組織全体を対象とするERMの必要性
　戦略策定の段階で全社横断的に適用する観点が必要
②ERMのプロセス重視の視点の修正
　ERMが各業務部門のプロセス中心となり、CEO等経営マネジメントとしての関心が薄くなっていた
③ERMが内部監査の保証業務の一環との位置づけになるケースが見られた
④2008年リーマンショック後の大不況の中で、CEO等経営中枢においてもERMの真の意味での課題が認識されるようになった。
⑤CEO等経営中枢は、コーポレートガバナンスの面からも取締役会の議論に専念する必要があり、組織内外のリスク事項に目を向ける対応を進展させる必要性が高まってきた
⑥ビジネス環境の変化が大きくなってきており、様々な説明責任、透明性を果たしていく上で、ERMとステークホルダーとの連繋が不可欠な時代を迎えている

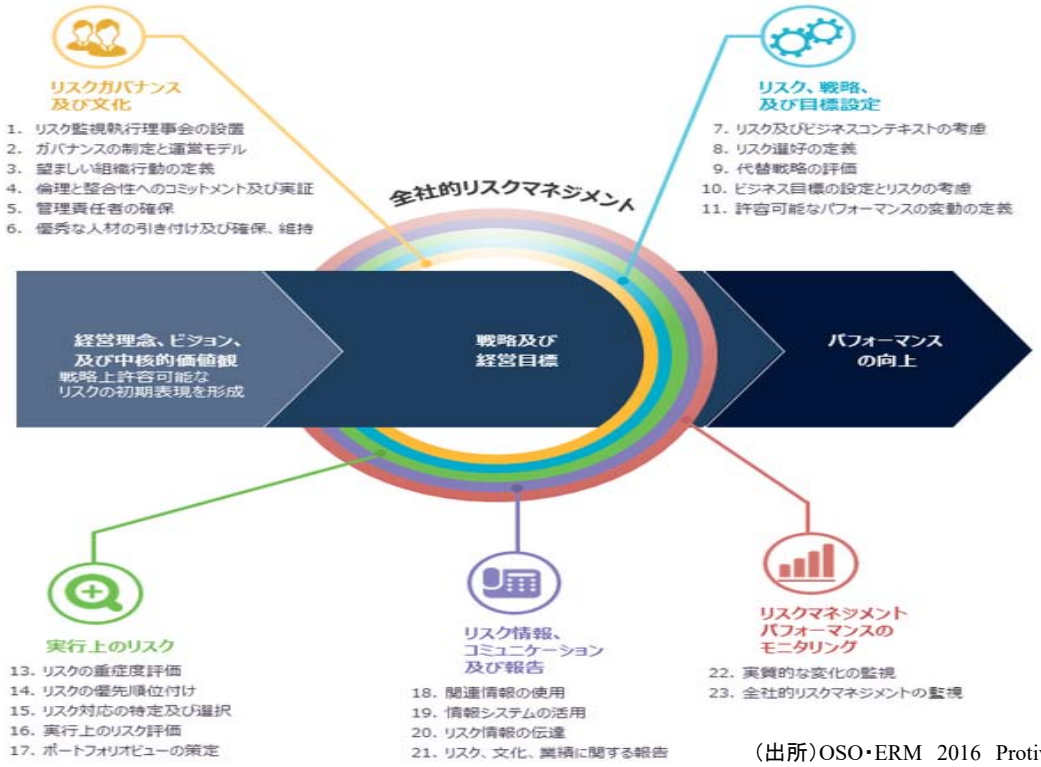
➡ **COSO・ERMが経営中枢に届いていない状況への打開が狙い**

（Protiviti社資料等を参照して作成）

Ⅳ. リスクマネジメントについて

（2）2016年COSO・ERM

2016年COSO・ERM改定後の全社的フレームワークは以下の通りとされる。
経営戦略、経営目標の実現を通じてパフォーマンス向上を図ることがERMの目的とされる。



（出所）OSO・ERM　2016　Protiviti社資料

Ⅳ. リスクマネジメントについて

2. わが国におけるリスクマネジメントの取組み

（1）会社法規定
わが国においては、会社法第362条、同施行規則第100条の下で「損失の危険の管理に関する規定その他の体制」について取締役会決議事項とされる。
このため、大企業ではほぼ例外なく、リスクマネジメントについての取組が講じられている。
一般的には、①リスク管理規定、②リスク管理委員会等の組織対応が図られているものとみられる。

（2）経営者の戸惑い
わが国経営者にとっては、改訂ガバナンスコードにおいてCOSO・ERM全社的リスクマネジメントへの取組要請が出る中で、これまで取り組んできたリスクマネジメントと何が異なるのか戸惑が生じるのは避けられものと思量される。

（3）ERM全社的リスクマネジメントと一般的リスクマネジメントの相違
①ERM全社的リスクマネジメントと一般的リスクマネジメントの相違については、2016年COSO・ERMのフレームワークに示される要請事項は、一般的なリスクマネジメント例えばISO31000等で構築される体制とシステム自体は大きく異なることはないように思われる。
②しかし、対象とされるリスクフィールドが、一般的リスクマネジメントでは各部門が特定する「業務プロセスリスク」が中心となる可能性が大きく、経営者目線からの「経営リスク」（＊）視点に欠ける傾向は否定できない。
（＊）「経営リスク」としては、例えば事業戦略、開発戦略、M&A、投資、組織、人事、報酬等経営パフォーマンスに直接影響を与える諸リスクが考えられる。
これらのリスクは、経営会議、取締役会等で議論されるものの、リスク管理委員会等での議論の対象にはならないケースが多いとみられる。

➡ *リスクフィールドに応じたリスクマネジメント対応が求められる*

Ⅴ. 3つのディフェンスラインとリスクマネジメント

1. 改訂コーポレートガバナンスコード：内部監査と取締役会、監査役会との連携

（1）内部監査の役割
改訂コーポレートガバナンスコードでは、全社的リスクマネジメント体制について、取締役会は内部監査部門を活用しつつその運用状況を監督すべきである。また、取締役会及び監査役会の機能発揮のために、内部監査部門がこれらに対して適切に直接報告を行う仕組みを構築すること等により、内部統制部門と取締役・監査役との連携を確保すべきとされた。

（2）3つのディフェンスラインでの位置づけ
3つのディフェンスラインでの、内部監査部門の位置づけは、社長等上級管理者とガバニングボディ（取締役会/監査委員会/監査役会等）とのデュアルレポーティングラインを構築することになる。

2. コーポレートガバナンスとリスクマネジメントの課題

（1）否定されるリスク
3つのディフェンスラインにおける、リスクマネジメントの課題は、社長等執行上級管理者がリスクを否定する可能性があること。すなわち企業事件事例において、上級管理者の行動によりディフェンスラインが易々と打ち破られていた。リスクマネジメントではリスク発生の可能性などのマイナス情報は組織防衛心理から様々な形で否認される傾向があるとされる。

（2）ガバニングボディの役割
業務執行上級管理者がリスク否認する局面でガバニングボディとしての取締役会（社外）/監査委員会/監査役会等の果たすべき役割は大きい。上級管理者が否認するリスクに対して、リスク発生の可能性を明確に指摘できるか否かの力量が問われることになる。そうした力量を確保していく上では、内部監査部門から単に報告を受けるのみでなく、問題点の把握のために内部監査部門に対して直接指示、命令ができるかが鍵を握ることになる。内部監査が機能しない場合は自ら問題を調査に解明をしていくことができて始めて、リスクマネジメントを踏まえたコーポレートガバナンスが実現できるのである。

Ⅴ．3つのディフェンスラインとリスクマネジメント

3．おわりに：ガバニングボディの力量

（1）改訂コーポレートガバナンスコード：取締役のスキル
改訂コーポレートガバナンスコードでは、取締役会の機能発揮のために取締役会が備えるべきスキル（知識・経験・能力）と各取締役のスキルと対応表の公表が求められることになった。
取締役会並びにその構成員は、リスクマネジメントリテラシーを基本スキルとして備えておく必要がある。

（2）社外取締役、監査役のガバニング力（加護野教授の議論）
加護野教授は、東芝事件を踏まえた上で、社外取締役のガバナンス効果に疑問を呈されている。
すなわち、
「まず、社外取締役は社内の人脈を持たない。そのために、鮮度の高い社内の現場情報を得るのが難しい。今回（東芝）の事件だけに限らず社内の不祥事を防ぐためには、根拠のないうわさ段階の情報を得て手を打つことが重要である。……社外取締役は（内部告発されるような）現場情報を得ることは難しいし、経営執行部が嫌がるような調査をしようとする意欲を社外取締役に持たせることも難しい。社外取締役の多くは経営執行部の知己であることが多い」
⇒内部監査が鮮度の良い情報を提供できるかが課題となる
一方、「社内監査役は社内の人脈を持っているために高鮮度の現場情報を持つことができる。社内の重要会議にも出席しているために、取締役会の議論の前提を知っている。社外監査役にそれを伝えることもできる。社外監査役も、監査役会を通じて鮮度の高い現場情報を得ることができる。…しかも、監査役には調査権も調査予算もある。……振り返ってみれば日本監査役会は…*適正に運営されれば*良い制度だったといえるかもしれない」
⇒内部監査の独立性や調査のあり方等を確立していくための法制整備が課題となる
（出典：加護野忠男神戸大学名誉教授「監査役制度をなくしてよいのか」月刊監査役2016．7.25）

社外取締役であれ監査役であれ*適正に運営*する力量が鍵を握る

ご清聴ありがとう
ございました

（参考1）否定されるリスク

リスク発生の可能性などのマイナス情報は心理的にも否認される傾向にある。

マイナス情報の分析評価は組織の弱み、対応の欠如などを明らかにするプロセスでもあるため、人間の防衛心理と同様、組織防衛メカニズムが作用してリスクは隠ぺいされる傾向がある。

リスクが隠れる組織の防衛メカニズムは下表のように整理されている。ここで示されているような考え方が残る限り、その企業や組織が重大な危機に陥る可能性は大きくなる。
経営執行者が陥りがちなポイントとなる。虚心にリスクに「気付く」ことの重要性を認識しておくことが必要。

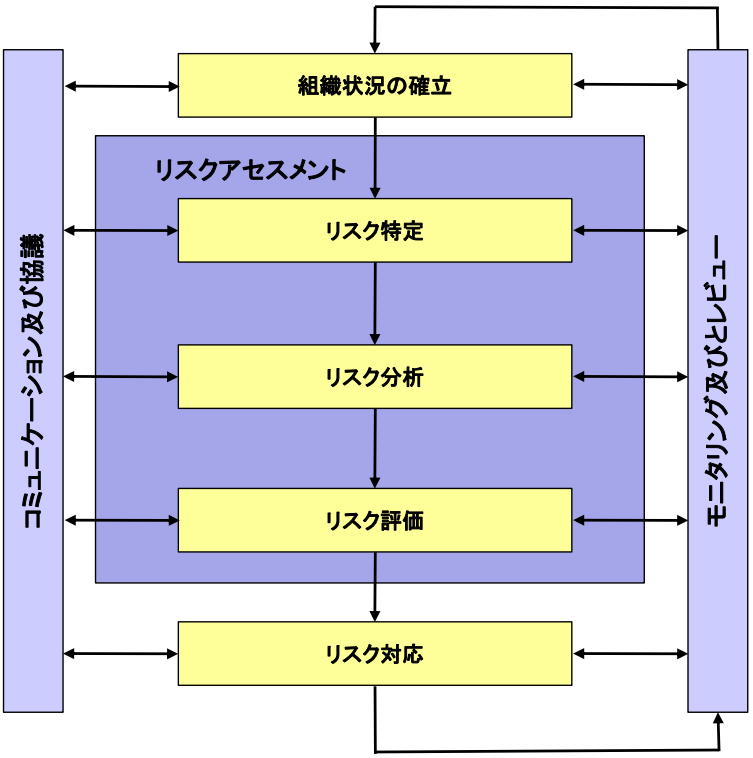
組 織 防 衛 メ カ ニ ズ ム

否定	:危機は他社に起こるが、我が社は大丈夫。
不承認	:危機は起こるが我が社への影響は小さい
理想化	:危機は立派な企業には起こらない。
誇大妄想	:我が社は強大であるから危機を防げる。
転嫁	:もし危機が起こるとしたら、誰が悪いか、もしくは何者かが我が社を陥れようとしている。
理屈	:危機が起こる確率は非常に小さいから、危機を心配する必要はない。 危機を 真剣に考える前に、その発生の確率と帰結を正確に測定するべきである。
仕切り	:危機は我が社全体に影響を与えることはない。なぜなら各部門はそれぞれ独立 している から。

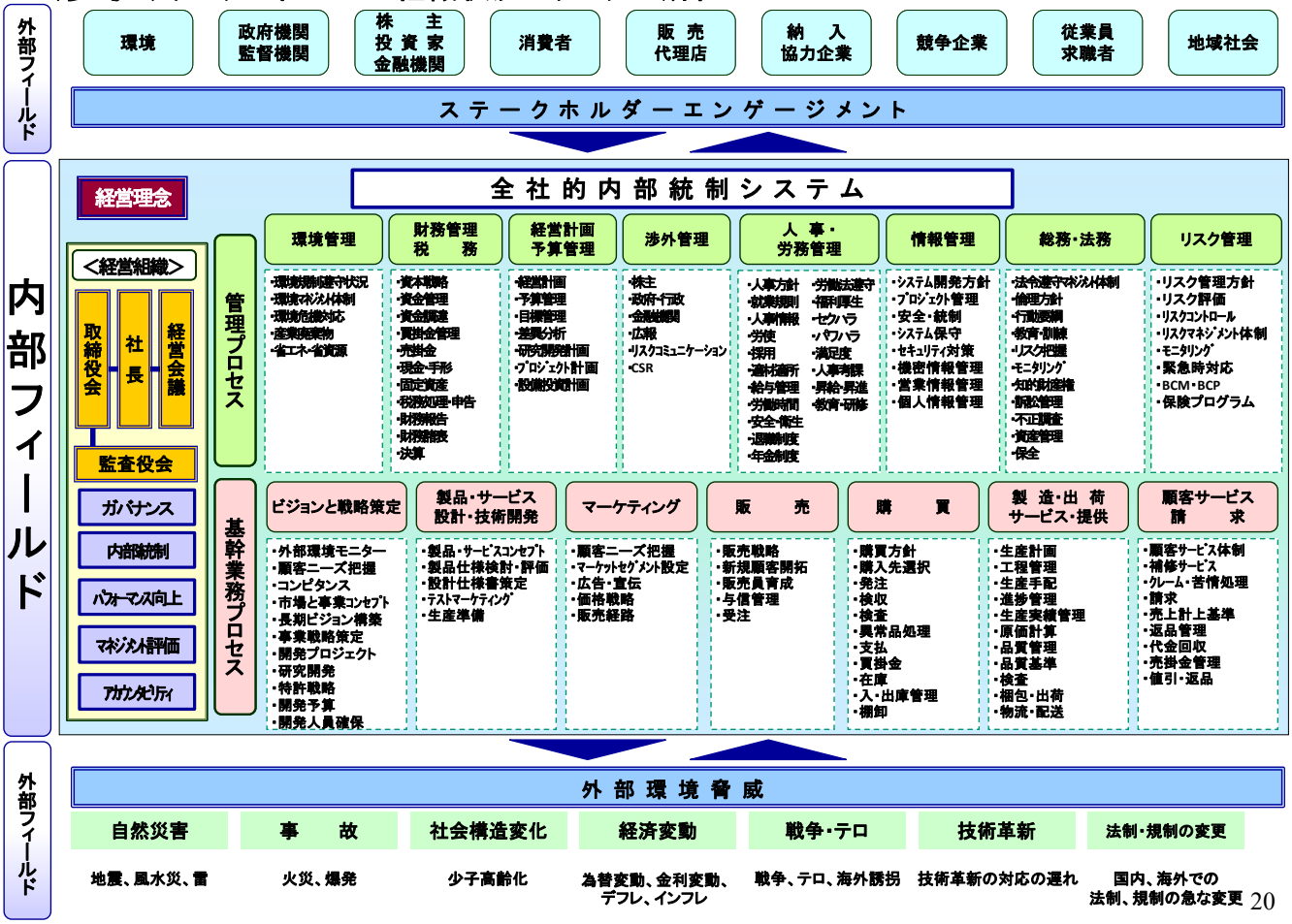
（出典：アイアン・ミトロフ著 上野正安他訳「クライシス・マネジメント」 ダイヤモンド社）

（参考2）一般的なリスクマネジメントプロセスについて

リスクマネジメントプロセス（ ISO31000）

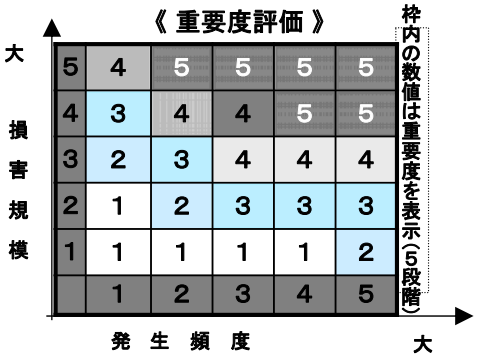


（参考3）リスクフィールド：組織状況とリスクの所在

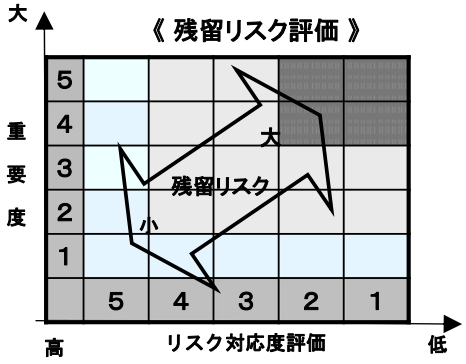


（参考4）リスク評価の考え方（業務プロセスリスク）

1. 頻度、規模と重要度評価の考え方



2. 重要度と対応度による残留リスクの考え方



3. リスク事態把握とリスクマネジメントへの展開（PDCAの考え方）

特定されたリスク事象について、①対策を実施するか監視に止めるかの対応を判定する。②対策を実施するリスクについて、㋑目標、㋺対策の内容、㋩主幹部門、㋥期限等を定め対応を進める。③年度末などに対応結果をレビューして、リスクを再評価し次年度の対応を検討する。⇒PDCAとしての「ISO31000リスクマネジメント国際規格」の考え方。

リスク事象	リスク事態	所属	重要度	頻度	規模	対応度	対応判定	RM目標	RM対策	主管	期限	レビュー（新年度検討）	重要度	頻度	規模	対応度	判定
							① ㋑対策実施 ㋺監視対応		②				③				

（注）RM：リスクマネジメント

以　上