「ＣＯＳＯ全社的リスクマネジメント　事例の解説篇」の内部監査での活用方法
～２０の原則の内部監査での８１の視点・着眼点と確認事項～

一般社団法人　日本内部監査協会
ＣＩＡフォーラムNo.ａ３　ＥＲＭ研究会（第１１期）
２０２２年９月１５日

「ＣＩＡフォーラム」は、ＣＩＡ資格保持者の研鑽及び相互交流を目的に活動する、一般社団法人日本内部監査協会の組織上の研究会の一つです。各ＣＩＡフォーラム研究会は、担当の座長が責任をもって自主的に運営し、研究期間、目標成果を設定し、研究成果を発信しています。

本報告書は、本研究会（CIA フォーラムａ３ ＥＲM研究会）が、その活動成果として取りまとめたものです。本報告書に記載された事例は、すべて本研究会メンバーが会合・合宿等で合議して作成したものであり、研究会メンバーが所属する個別企業の事例ではありません。報告書に記載された意見・コメント・その他の記載も同様に、すべて本研究会としての見解であり、メンバー、およびメンバーが属する組織の見解ではありません。また、協会の見解を代表するものではありません。

目　次

１．はじめに

（１）「ＣＯＳＯ全社的リスクマネジメント　事例の解説篇」の特徴

・周知のとおり、ＣＯＳＯ（トレッドウェイ委員会支援組織委員会）は、2004年９月公表の『全社的リスクマネジメント―統合的フレームワーク』を13年ぶりに改訂して、2017年９月（報告書の日付は同年６月）に『全社的リスクマネジメント ― 戦略およびパフォーマンスとの統合』（新フレームワーク）を公表し、戦略およびパフォーマンスに影響を及ぼし得るリスクを管理するための最新のアプローチを提示しました。

・新フレームワークは、事業体の種類、規模、業界、および地域を問わず、あらゆる事業体に適用可能な普遍性を持つものとして作られたため、その性格上抽象度が高いものになっています。そのため、新フレームワークを補完するものとして、その具体的なイメージを把握でき、それをどのように実務に適用すればよいかの理解に役立つ事例集の公表が期待されていました。そこでＣＯＳＯは、フレームワークで提示されている20の原則を組織が日々の実務に適用する方法を説明するための「事例の解説篇」(注) を2018年６月（報告書の日付は同年1月）に公表し、同年12月には日本内部監査協会が邦訳を公表しました。

・本書では、業種も規模も異なる９つの事業体が直面する固有のリスクに対応するため、①新フレームワークの20の原則をどのように適用したかという「原則の適用方法」と、②全社的リスクマネジメントが事業にどのように組み込まれているかという「全社的リスクマネジメントの事業への組み込まれ方」が、個別・具体的な事例に即して詳細に説明されています。

・事例を通して、全社的リスクマネジメントが目指す価値向上を実現するためにそれぞれの原則を、組織の規模、活動範囲、および事業環境に基づいて、具体的な戦略、リスクおよび機会を考慮して適用させる具体的な方法が実に多様な視点から説明されています。個別の組織の全社的リスクマネジメントについての事例ですが、事例の背景にある原則の機能を読み取ることにより、原則が持つ機能を、事例を通して理解できます。また、原則を実務に適用するための具体的なイメージがつかめ、原則を自社にどのように調整して適用すればよいかについての知見を得ることができます。

（注）「ＣＯＳＯ全社的リスクマネジメント　戦略およびパフォーマンスとの統合　事例の解説篇」
（*Enterprise Risk Management Integrating with Strategy and Performance　Compendium of Examples*）

（２）本報告書の目的と特徴

本報告書の目的は、「事例の解説篇」から我が国企業での内部監査で活用できる視点・着眼点と質問事項を読み取り、整理して提示することです。そのため、**20 の原則ごとに、合計 81 の視点・着眼点と確認事項を例示**しました。

事例の解説篇は、前記の通り原則を実務に適用する方法を、個別・具体的な事例に即して実に多様な視点から詳細に説明しているため、内容が大変豊富です。また、米国の様々な組織体（教育機関、政府、非営利団体、および医療機関など）の事例を取り上げており一部、我が国企業での実務とは異なる内容も含まれているため、我が国企業での内部監査の実務に直接活用しにくい面があります。そのため、本報告書では20 の原則を我が国における内部監査の実務で活用するという観点から作成しました。また、監査対象部門が内部統制を含めた全社的リスクマネジメントを評価し、改善提言するという内部監査の実務に活用できるように努めました。

なお、視点・着眼点と確認事項の中には、リスク監視、望ましいカルチャー、およびリスク選好の定義付けなど、取締役会に責任がある事項が含まれていることから、取締役の職務執行を監査する監査役監査にも活用でき、さらに監査役と内部監査部門とのコミュニケーションや連携の推進にも活用できる内容となっています。

（３）使用上の注意

①本報告書は、事例の解説篇で示された９つの事例について、全社的リスクマネジメントの観点から内部監査の実務に資する視点や知見・ノウハウの提供を試みたものであり、事例の解説篇それ自体の解説を目的としたものではありません。

②紹介した視点・着眼点と確認事項はあくまでも一例であり、それ以外にも多くのものがあることにご留意願います。

③**本報告書に記載したものを全て使用する必要はなく、自社で活用できるものから活用し、自社の現在の全社的リスクマネジメントの状況を出発点として、高度化していくことが大切です。**

④本報告書の記載内容に関する責任は、すべて本研究会にあることにご留意願います。

（４）研究会メンバー　（ＣＩＡフォーラムａ３　ＥＲＭ研究会（第 11 期）

（2022 年 8 月 1 日時点）

No.	氏名	会社名等	所属・役職
1	吉野 太郎　（座　長）	前東京ガス（株）	
2	野口 正文　（副座長）	損害保険ジャパン（株）	監査役室・主査
3	新藤　和政 （座長補佐・Web 会議担当）	ファナック（株）	内部監査部長
4	藤枝 繁	個人会員	
5	坂井　香苗	日本電気（株）	経営監査部・監査第二グループ・シニア監査プロフェッショナル
6	紀谷 倫有	個人会員	
7	宮内 隆行	住友化学（株）	内部統制・監査部・主席部員
8	真柳 元	個人会員	
9	丹羽 珠希	（株）三井住友フィナンシャルグループ	監査部・上席考査役
10	有村 祥一	アジア太平洋トレードセンター（株）	監査役
11	伊藤　裕美子	ＮＥＣネッツエスアイ（株）	経営監査部・担当課長
12	宇田　文顕	シナネンホールディングス（株）	ＩＴ戦略部・チーム長
13	大島 誠	（株）アイ・アール・エス	常勤監査役（独立社外）
14	石井 学	Supership ホールディングス（株）	内部統制推進室
15	和田 有弘	出光興産（株）	内部監査室
16	青木 博史	（株）三菱 UFJ フィナンシャルグループ	監査部・上席調査役
17	佐藤 伸吾	のむら産業（株）	内部監査室・室長
18	小林 竹幸	第一生命保険（株）	内部監査部・ラインマネジャー
19	桐山 勝	（株）クレハ	常勤社外監査役
20	村上　裕子	明治安田生命相互会社	監査部・上席内部監査役
21	野々山　一郎	東芝ライフスタイル（株）	経営統括部 監査担当 グループ長
22	板東　理枝	(株)ゆうちょ銀行	地域共創推進部
23	野元　道子	日本郵船（株）	内部監査室 監査企画チーム・課長代理
24	田中　恵太	農林水産省	大臣官房検査・監察部調整・監察課・指導企画係長
25	神山　典子	合同会社オズ	代表社員
26	小関　清久	個人会員	
27	岡田　芳明	三菱地所（株）	内部監査室・理事
28	五十嵐　英知	東京海上ホールディングス（株）	内部監査部・部長兼企画グループリーダー
29	加藤　彰子	(株)ラック	総務・法務部 リスクマネジメント室長

（５）本研究会の活動の経緯

本研究会は 2004 年 4 月から活動を開始し、11 期 18 年にわたり、全社的リスクマネジメント（ＥＲＭ）を内部監査に活用する手法を研究し、内部監査の質的向上に微力ながらも貢献していきたいとの思いで活動を続けてきました。その間の研究成果とその概要は以下のとおりです。

活動期間	研究成果（報告書）	概　　要
第１期 2004 年 4 月 ～2005 年 2 月	**ＥＲＭのよくある質問集（ＦＡＱ）**	ＥＲＭについて理解を促進するためのＦＡＱ。
第２期 2005 年 4 月 ～2006 年 3 月	**使えるＥＲＭ（全社的リスクマネジメント）導入チェックポイント集** ～ 一目でわかるＥＲＭと内部統制の基本的要素の具体例 ～	ＥＲＭの８つの構成要素が有効に機能しているかどうかのチェックポイントと、その具体的な事例。
第３期 2006 年 4 月 ～2007 年 4 月	**ＥＲＭ実施体制を構築するために必要な１０の要件**	ＥＲＭ実施体制構築の要件と、その具体的事例、および中小企業であっても行うべきＥＲＭの最低要件。
第４期 2007 年 5 月 ～2008 年 7 月	**法対応の内部統制から価値創造のＥＲＭ（全社的リスクマネジメント）へ** ～ 会社法と金融商品取引法対応の内部統制を活かしたＥＲＭづくりへの提言 ～	内部統制法制化への対応で得られた成果のＥＲＭ実施体制構築への活用。
第５期Ａ分科会 2008 年 10 月 ～2010 年 1 月	**ＥＲＭ的な視点を取り入れた内部監査の手法** ～ ＥＲＭの視点を活用して、企業目標の達成に寄与し付加価値を提供する内部監査を行うためのノウハウ ～	内部監査にＥＲＭ的な視点を取り入れ、内部監査の質を高め､企業目標の達成に寄与するための手法･ノウハウ。
第５期Ｂ分科会 2008 年 10 月 ～2010 年 1 月	**格付会社のＥＲＭ確認項目を用いた事業会社向けＥＲＭチェックリスト** ～ 事業会社の目線に立った格付会社のＥＲＭ確認項目の読替と解説 ～	格付会社が公表している情報を参考に我が国の一般事業会社を対象としたＥＲＭの取組状況を確認するための項目についての解説。
第６期 2010 年 4 月 ～2012 年 6 月	**「ＣＯＳＯ　内部統制モニタリングガイダンス」に基づいた** **ＥＲＭモニタリング事例集**	「ＣＯＳＯ内部統制モニタリングガイダンス」の手法や考え方を反映させたＥＲＭのモニタリング事例集。
第７期 2012 年 8 月 ～2014 年 10 月	**全社的リスクマネジメント（ＥＲＭ）を活用した内部監査手法の研究** ～「リスク選好・リスク許容度」､「主要リスク指標」､「戦略的優位性を確保するＥＲＭ」についての業種別事例とリスクベース内部監査への活用事例～	「リスク選好・リスク許容度」､「主要リスク指標」､「戦略的優位性を確保するＥＲＭ」に関するＣＯＳＯの３つのレポートから、それらの業種別の具体的事例、および内部監査における確認事項と内部監査の実務で役立つ視点をまとめたもの。
第８期 2015 年 2 月	**改訂版ＣＯＳＯ内部統制フレームワークの内部監査での活用事例** ～改訂版 COSO の 17 の原則の観点から見た内部監査において留意すべ	17 の原則ごとに「具体的視点」を例示し､「内部監査において留意すべき問題事例」と「改善提言のた

～2015 年 11 月	き問題事例と改善提言のための確認事項～	めの確認事項／改善提言」を説明。
第９期 2016 年 2 月 ～2016 年 11 月	**リスク評価手法の内部監査での活用事例** ～内部監査での活用方法・改善提言のための確認事項～	リスク評価の具体的なノウハウ、問題のある事例、および良好な事例について、「具体的事例」を紹介すると共に、「内部監査での活用方法・確認事項・改善提言」を紹介。
第１０期 2017 年 4 月 ～2019 年 11 月	**改訂版ＣＯＳＯ・全社的リスクマネジメントの内部監査での活用方法** ～全社的リスクマネジメントの 20 の原則に沿った内部監査での 73 の「質問・確認事項」と「課題・改善提言」および 61 の「具体例」～	20 の原則ごとに、全社的リスクマネジメントに対する内部監査で質問・確認すべき事項を例示し、課題とその改善提言を紹介。
第１１期（当期） 2020 年 1 月 ～2022 年 9 月	**「ＣＯＳＯ全社的リスクマネジメント　事例の解説篇」の内部監査での活用方法** ～２０の原則の内部監査での 81 の視点・着眼点と確認事項～	事例の解説篇から全社的リスクマネジメントに対する内部監査での視点・着眼点と質問事項を読み取り 20 の原則ごとに紹介。

（注）上記報告書はすべて、一般社団法人日本内部監査協会のホームページ上で公開されています。

・第１期～８期報告書　　:「研究・活動」→「ＣＩＡフォーラム」→「活動実績」（右上）→「過去の活動実績」（最下段）→研究会 No.15（第１期～第８期）
＊https://www.iiajapan.com/leg/kenkyu/forum/report_past.html

・第９期～１０期報告書　　:「研究・活動」→「ＣＩＡフォーラム」→「活動実績」（右上）→ａ３（第９期、第 10 期）
＊https://www.iiajapan.com/leg/kenkyu/forum/report.html

２．本報告書の全体像（「視点・着眼点と確認事項」一覧）

※合計８１項目

構成要素	原　則	当研究会で考察した視点・着眼点と確認事項
構成要素１ ガバナンスとカルチャー	原則１ 取締役会によるリスク監視を行う ＊参考にした事例 ⇒１　高等教育機関におけるガバナンス	①リスク情報の報告体制 ②リスクマネジメントのモニタリングに必要な情報 ③モニタリングの指標やツール ④報告責任と報告経路 ⑤業務の仕組みやシステムが変化した場合の報告経路
	原則２ 業務構造を確立する ＊参考にした事例　⇒同上	①リスクの識別・評価、リスク対応策の評価・見直し ②経営者への報告
	原則３ 望ましいカルチャーを定義づける （15 項目） ＊参考にした事例 ⇒２ 政府機関におけるカルチャー ３ 金融機関におけるカルチャー	（１）ミッション・ビジョン・コアバリュー ①定　義 ②見直し ③社内への浸透 ④浸透状況の確認 ⑤評価・報酬制度
		（２）行動規範 ①望ましい行動の明確な定義 ②見直し ③社内への浸透 ④浸透状況の確認 ⑤評価・報酬制度
		（３）カルチャー ①定　義 ②リスクを認識、指摘・議論できるカルチャー ③互いを認め、尊重し合うカルチャー ④日々の業務処理を過度に重視
		（４）ブランド ①実務の運営方針との整合性

	原則４ コアバリューに対するコミットメントを表明する ＊参考にした事例　⇒同上	①コアバリューの文書化と浸透・定着 ②コアバリューと望ましい行動 ③各階層の役割と責任 ④リスク管理責任者 ⑤個人の業務上の責任
	原則５ 有能な人材を惹きつけ、育成し、保持する ＊参考にした事例　⇒同上	①評価・報酬制度や人材育成制度の設計 ②長期的で持続可能なパフォーマンスを促す評価・報酬体系 ③必要な能力 ④研修 ⑤全社的リスクマネジメントを行うことの意義や役割の理解 ⑥知識・スキルの習得 ⑦スキルの継続的な確保 ⑧人事ローテーション・配置 ⑨採用促進 ⑩退職抑制
構成要素２ 戦略と目標設定	原則６ 事業環境を分析する ＊参考にした事例 ⇒４　エネルギー会社における戦略と目標設定 ⇒５　非営利団体における戦略と目標設定	①事業環境のカテゴリーごとの分析 ②前提や将来予測の根拠の変化に応じた戦略の見直し
	原則７ リスク選好を定義する ＊参考にした事例　⇒同上	①取締役会での承認・文書化・経営者による周知（手続き面） ②ミッション・ビジョン・コアバリューとの整合（内容面）
	原則８ 代替戦略を評価する ＊参考にした事例　⇒同上	①ミッション・ビジョン・コアバリューとの結びつき ②リスクの全体像に及ぼす影響の理解 ③リスクの全体像の継続的モニタリング ④リスクの全体像（リスクプロファイル）の事例

	原則９ 事業目標を組み立てる ＊参考にした事例　⇒同上	①目標とリスクの全社レベルから部門レベルへの落とし込み ②階層に対応した戦略、目標の設定
構成要素３ パフォーマンス	原則１０ リスクを識別する ＊参考にした事例 ⇒６　消費財メーカーにおけるパフォーマンス ７　テクノロジー会社におけるパフォーマンス	①部門別の目標設定とリスクの特定 ②前提条件を明確にする ③環境変化に応じてリスクを識別する ④目的に合った情報を効率的に収集するツールを使用する ⑤適時に情報を収集・伝達する ⑥環境変化のスピードに即した頻度でリスクを識別する ⑦部門内のリスクマネジメント統括者の設置
	原則１１ リスクの重大度を評価する ＊参考にした事例　⇒同上	①リスクの評価基準を設定する ②製品サイクルの節目ごとにリスク評価を実施する ③評価対象の事業と整合した評価基準を用いる ④環境変化のスピードに即したリスク評価の頻度
	原則１２ リスクの優先順位づけをする ＊参考にした事例　⇒同上	①全社目標の達成に与える影響度を基準とする ②優先順位づけの基準・根拠・用いた情報を確認する
	原則１３ リスク対応を実施する ＊参考にした事例　⇒同上	①リスクの優先順位づけ・リスク対応のコスト・パフォーマンスを比較検討する ②パフォーマンス指標に基づいてリスク対応を実施する
	原則１４ ポートフォリオの視点を策定する ＊参考にした事例　⇒同上	①複数部門で関係のあるリスクを全社レベルで集約する ②各部門でのリスクの識別・評価の結果を集約して全社レベルのリスクを把握する
構成要素４ レビューと修正	原則１５ 重大な変化を評価する	①環境変化の影響を把握・分析した上でパフォーマンスを評価する ②今後の変化の兆候とその推移を把握する ③リスクの特性に見合った頻度でのリスクの評価

	＊参考にした事例 ⇒８　工業製品会社におけるレビューと修正	
	原則１６ リスクとパフォーマンスをレビューする ＊参考にした事例　⇒同上	①パフォーマンス変化の分析を通したリスク変化の把握 ②パフォーマンスが許容範囲内に収まっていない場合の対応を検討しておく ③パフォーマンスの許容範囲を明確にしておく ④“Trusted Advisor”として機能する内部監査部門
	原則１７ 全社的リスクマネジメントの改善を追求する ＊参考にした事例　⇒同上	①パフォーマンスとの関係からリスクとその対応状況を把握・評価する ②全社的リスクマネジメント体制全体の課題の把握・改善
構成要素５ 情報、伝達および報告	原則１８ 情報とテクノロジーを有効活用する ＊参考にした事例 ⇒９　医療機関におけるリスク情報	①意思決定に必要なリスク情報の見極め・収集・分析・報告 ②内外の要因の見極め・収集・分析・報告
	原則１９ リスク情報を伝達する ＊参考にした事例　⇒同上	①リスクの原因と影響を適切に分析・評価した調査レポートを提出する ②リスク情報が迅速・正確に報告される体制・組織文化 ③多様な情報伝達経路
	原則２０ リスク､カルチャーおよびパフォーマンスについて報告する ＊参考にした事例　⇒同上	①リスク情報を幅広く収集し多様な視点から分析して報告する ②パフォーマンスを通してリスクをモニタリングする ③望ましいカルチャーの伝達・浸透状況を検証・評価し報告する

（注）構成要素と原則は、トレッドウェイ委員会支援組織委員会（COSO: Committee of Sponsoring Organizations of the Treadway Commission）著　一般社団法人日本内部監査協会、八田進二、橋本尚、堀江正之、神林比洋雄監訳「ＣＯＳＯ全社的リスクマネジメント　－戦略およびパフォーマンスとの統合－」(2018 年 4 月　同文舘出版）74 頁他から引用。

３．本報告書で参考にした事例と原則との関係

注意：「事例の解説篇」（5 頁　「表 1.1　事例で示した原則」）とは一部異なっている。

事　例	事例１	事例２	事例３	事例４	事例５	事例６	事例７	事例８	事例９
業　種	高等教育機関におけるガバナンス	政府機関におけるカルチャー	金融機関におけるカルチャー	エネルギー会社における戦略と目標設定	非営利団体における戦略と目標設定	消費財メーカーにおけるパフォーマンス	テクノロジー会社におけるパフォーマンス	工業製品会社におけるレビューと修正	医療機関におけるリスク情報
規　模	国際規模	全国規模	地方規模	全国規模	国際規模	地方規模	全国規模	国際規模	全国規模
構成要素	ガバナンスとカルチャー			戦略と目標設定		パフォーマンス		レビューと修正	情報、伝達および報告
原則１　取締役会によるリスク監視を行う	●								
原則２　業務構造を確立する	●								
原則３　望ましいカルチャーを定義づける		●	●						
原則４　ｺｱﾊﾞﾘｭｰに対するｺﾐｯﾄﾒﾝﾄを表明する		●	●						
原則５　有能な人材を惹きつけ、育成し、保持する		●	●						
原則６　事業環境を分析する				●	●				
原則７　リスク選好を定義する				●	●				
原則８　代替戦略を評価する				●	●				
原則９　事業目標を組み立てる				●	●				
原則１０　リスクを識別する						●	●		
原則１１　リスクの重大度を評価する						●	●		
原則１２　リスクの優先順位づけをする						●	●		
原則１３　リスク対応を実施する						●	●		
原則１４　ポートフォリオの視点を策定する						●	●		
原則１５　重大な変化を評価する								●	
原則１６　ﾘｽｸとﾊﾟﾌｫｰﾏﾝｽをﾚﾋﾞｭｰする								●	
原則１７　全社的ﾘｽｸﾏﾈｼﾞﾒﾝﾄの改善を追求する								●	
原則１８　情報とテクノロジーを有効活用する									●
原則１９　リスク情報を伝達する									●
原則２０　ﾘｽｸ、ｶﾙﾁｬｰおよびﾊﾟﾌｫｰﾏﾝｽについて報告する									●

参考：ＣＯＳＯ全社的リスクマネジメントの根底にある考え方と本報告書との関係

・企業活動とは、①自社の「ミッション・ビジョン・コアバリュー」に基づいて、②それらを達成・実現するための「**戦略**」を策定し、③戦略を達成するための具体的かつ測定可能な「**事業目標**」を策定した上で、④それら（戦略と事業目標）を達成し、利益や市場優位性などの「**パフォーマンス**」を獲得することを通して、⑤企業の最終目的である「**企業価値の向上**」を実現することである。
・この一連の企業価値向上のサイクルを回すためには、①「**ガバナンスとカルチャー**」、②「**戦略と目標設定**」、③「**パフォーマンス**」、④「**レビューと修正**」、および⑤「**情報、伝達および報告**」**の５つの構成要素を有効に実践**することが必要である。そして**２０の原則**が**構成要素を有効に実践する方法**を説明している。
・本報告書は、この**２０の原則の企業における具体的な活用方法**を８１の「内部監査で活用できる視点・着眼点・質問事項」を通して説明を試みたものである。

用語の定義

当研究会では以下のように定義する。

【リスク】
リスクとは、**企業目的の達成**に**影響**を及ぼす事象が発生する**可能性**である。

【パフォーマンス】
パフォーマンスとは、企業の最終目的である**「企業価値の向上」を実現するために必要な具体的かつ測定可能な個々の成果**。（例：売上、利益、もしくは市場シェアなど）

【リスク選好】
リスク選好とは、企業が**企業価値向上のために受け入れるリスクの種類と量**である。

【リスクの許容範囲】
リスクの許容範囲とは、**「リスク選好の上限」以下**であり、かつ**「パフォーマンスの許容可能な下限」以上**のリスクの範囲である。

【ミッション・ビジョン・コアバリュー】
・当研究会では**コアバリューはミッション、ビジョンを実現するためのもの**と捉えている。
・ミッション・ビジョン・コアバリューは相互に関連しており、当研究会ではこの３つの定義を実務の観点から以下のように整理する。
(a)**ミッション**（経営目的）
㋐**自社の存在意義**、㋑**使命**、㋒**最高の目的**、もしくは、㋓**達成したい事柄**を示すもの。

※特徴：普遍性が高い。

(b) **ビジョン（長期経営目的）**

ミッションに基づき、㋐**長期的な自社の目指す姿**、㋑**願望する将来像**、もしくは、㋒**長期的に達成したい事柄**を示すもの。

※特徴：目指す姿。

(c) **コアバリュー（価値観、信条、信念、理念）**

ミッション、ビジョンの実現に向けて、一人ひとりが**大切にすべき価値観やカルチャー**を示すもの

※特徴：実現するために必要なもの、次の行動に結び付けるトリガー

４．ＣＯＳＯ全社的リスクマネジメントの 20 の原則に沿った内部監査での８１の視点・着眼点と確認事項

構成要素１　ガバナンスとカルチャー

１．原則１：取締役会によるリスク監視を行う

参考にした事例：**事例１　高等教育機関におけるガバナンス**

①リスク情報の報告体制

・取締役会(注１)へのリスク情報(注２)の報告体制（報告経路、報告要件、報告頻度、報告責任者など）は、取締役会がリスクマネジメントをモニタリングするために必要な水準となっているか。

（注１）経営者によるリスクマネジメントのモニタリングを監査対象とする場合には、「取締役会」を「経営者」と読み替えること（以下同じ）。

（注２）㋐リスクの状況、㋑リスクへの対応状況、および、㋒リスク対応上の課題などリスクマネジメントの現状と課題についての情報。

②リスクマネジメントのモニタリングに必要な情報

・取締役会がリスクの状況とリスクへの対応状況や課題を適時に把握し、必要な指示が行えるように、各部門はリスクマネジメントのモニタリングに必要な情報(注)を取締役会に適時に報告しているか。

⇒取締役会資料にリスク監視に必要な情報が記載されているか確認する。

（注）上記①の「リスク情報」と同じ。すなわち、㋐リスクの状況、㋑リスクへの対応状況、および、㋒リスク対応上の課題などリスクマネジメントの現状と課題についての情報。

③モニタリングの指標やツール

・リスク管理部門や経営企画部門は、取締役会が全社のリスクの状況とリスクへの対応状況や課題の全体像を的確に把握できるように、リスクマネジメントをモニタリングするための指標やツールを提供しているか。

＊例：指　標　⇒KPI

ツール　⇒計画対実績の差異についての月次での分析・報告のためのダッシュボード(注)

（注）ダッシュボード

①ダッシュボードとは複数の情報を１つにまとめ、一目でデータを把握できるようにする「データの可視化ツール」。最近では企業の売上やマーケティング関連のデータを集め、表やグラフで分かりやすく表示するツールを意味することが多い。

②ダッシュボードは、あらゆるデータを集め可視化できることから、会社の状況を素早く把握できるようになるメリットがあり、素早い意思決定に役立つ。

④報告責任と報告経路

・リスク管理部門は、各部門から取締役会へのリスク情報の報告責任と報告経路を明確に定めているか。

⑤業務の仕組みやシステム（注）が変化した場合の報告経路

・リスク管理部門は、組織変更などにより業務の仕組みやシステムが変化した場合に、各部門から取締役会へのリスク情報の報告経路に抜け・漏れや脆弱性が発生していないかを確認しているか。また、業務の仕組みやシステムが変化していない場合でも、取締役会へのリスク情報の報告経路に抜け・漏れや脆弱性が発生していないかを定期的に検証しているか。

（注）組織、権限・責任、報告経路、指揮命令・復命系統など

【リスクの定義】

・当研究会では、リスクを以下のように定義する。
リスクとは、企業目的の達成に影響を及ぼす事象が発生する可能性である。

原則２：業務構造を確立する

参考にした事例：**事例１ 高等教育機関におけるガバナンス**

①リスクの識別・評価、リスク対応策の評価・見直し

・（事業環境が変化する中で）戦略と事業目標を達成するために必要な**業務の仕組みやシステム（組織、権限・責任、報告経路、指揮命令・復命系統など）**を確立することを目的に、**以下の視点から**、事業環境の変化に応じて適時に、**リスクの識別・評価**、および**リスク対応策の有効性の評価**と**対応策の見直し**を行っているか。

＊リスクの識別・評価、およびリスク対応策の有効性の評価と対応策の見直しを行うことが、**業務の仕組みやシステムを確立する前提**である。

(a)**中長期**でのリスクの識別・評価とリスク対応策の策定を含めているか。

(b)各部門のリスクだけでなく、**全社的なリスク**（全社横断的・全社共通のリスク）を含めているか。

(c)リスクやリスク対応策の有効性を評価する**指標**や**ツール**を導入しているか。

＊例：指　標　⇒KPI
　　ツール　⇒計画対実績の差異についての月次での分析・報告のためのダッシュボード

(d)KPI を導入する場合には、事前に **KPI の許容可能な変動範囲**を決めているか。また、**許容可能な変動範囲を超えた場合の対応**を決めているか。

【ウイルス付きメールを開封するリスクに対する対応の有効性を示す KPI とその許容範囲（上限と下限）の例】
・当該リスクに対するリスク対応策として、メールに関するオンラインでの情報セキュリティ研修の実施が考えられる。その場合、
　KPI　　⇒オンライン研修の受講率、終了テストの正解率
　許容範囲　⇒受講率は 100%、正解率は 60%（下限）～80%（上限）

②経営者への報告

・各部門は**リスクが変化**し、もしくは**リスク対応策の有効性が低下**した結果、現行の**業務の仕組みやシステムがリスクに適切に対応できていない**と認識した場合には、速やかに**経営者に報告**しているか。

・また、経営者は報告を受けて、業務の仕組みやシステムを見直しているか。

原則３：望ましいカルチャーを定義づける

参考にした事例：**事例２ 政府機関におけるカルチャー**
：**事例３ 金融機関におけるカルチャー**

（１）ミッション・ビジョン・コアバリュー

①定　義

・自社のミッション・ビジョン・コアバリューが、自社のビジネスモデル(注)と整合性を持って定義され、明文化されているか。
（注）㋐自社の存立基盤、㋑重要なステークホルダーとの関係、および、㋒ビジネスを展開するマーケットの環境を含む。
・定義に際しては、オープンで率直な議論(注)を経ているか。
（注）議論には、㋐企業価値向上のために受け入れるリスクの種類と量であるリスク選好、㋑会社が耐えられるリスクの限界であるリスクキャパシティを含む。

【ミッション・ビジョン・コアバリューの定義】
・当研究会ではコアバリューはミッション、ビジョンを実現するためのものと捉えている。
・ミッション・ビジョン・コアバリューは相互に関連しており、当研究会ではこの３つの定義を実務の観点から以下のように整理する。
(a)**ミッション**（経営目的）
㋐自社の存在意義、㋑使命、㋒最高の目的、もしくは、㋓達成したい事柄を示すもの。
※特徴：普遍性が高い。
(b)**ビジョン（長期経営目的）**
ミッションに基づき、㋐長期的な自社の目指す姿、㋑願望する将来像、もしくは、㋒長期的に達成したい事柄を示すもの。
※特徴：目指す姿。
(c)**コアバリュー（価値観、信条、信念、理念）**
ミッション、ビジョンの実現に向けて、一人ひとりが大切にすべき価値観やカルチャーを示すもの
※特徴：実現するために必要なもの、次の行動に結び付けるトリガー

②見直し

・経営会議メンバーなど経営者が現在のミッション・ビジョン・コアバリューを継続的にモニタリングし、必要に応じて見直しを検討する体制となっているか。
・㋐不祥事など望ましい行動からの逸脱の発生、㋑経営環境の変化、もしくは、㋒社会からの期待の変化などに対応して、ビジョンとコアバリューを見直しているか。

③社内への浸透

・ミッション・ビジョン・コアバリューをどのように社内に浸透させているか。
⇒例：㋐研修、㋑トップメッセージの全社員宛メール配信、㋒経営トップとの対話集会、もしくは、㋓職場でのディスカッションを通じた理解の浸透。

④浸透状況の確認

・ミッション・ビジョン・コアバリューの社内への浸透度合や理解度をどのような方法で確認しているか。
⇒例：㋐従業員意識調査（全般的な事項を対象）、㋑従業員へのアンケートやインタビュー（特定分野の事項を対象）。

⑤評価・報酬制度

・社員の評価・報酬制度は、ミッション・ビジョン・コアバリューに沿った望ましい行動を取るインセンティブが働くものとなっているか。
⇒評価・報酬制度は、具体的な目に見える望ましい行動を評価する制度面に限定したものでなくても、望ましい行動を意識するように促す運用面での仕組み(注)でもよい。

（注）例：㋐年度初めの上司・部下間での目標設定の話し合いで望ましい行動を意識した目標設定を行う仕組み、㋑年度末の評価で望ましい行動に反した場合にネガティブ評価がなされる仕組み。

【望ましい行動を取るインセンティブが働く評価・報酬制度の例】
(a)評価・報酬体系が、短期的な営業実績だけでなく、「顧客満足度アンケートの結果、顧客との有効な面談回数、および、顧客からの感謝の声の数など、望ましい行動を促す長期的な顧客との関係性向上」を反映したものになっているか。
(b)また、顧客をお待たせした時間や顧客からの不満の声など、望ましくない行動を減点項目として反映したものになっているか。
(c)利益を出している社員でも望ましくない行動を伴っている場合には、相応のマイナス評価を行い、人事評価が望ましい行動を促すものとなっているか。

（２）行動規範

①望ましい行動の明確な定義

・会社のミッション・ビジョン・コアバリューに沿った具体的な望ましい行動を行動規範の中で明確に定義しているか。

②見直し

(a)上記「（１）ミッション・ビジョン・コアバリュー」の「②見直し」と同じ。
※「ミッション・ビジョン・コアバリュー」を「行動規範」に読み替えること。以下同じ。
(b)顧客満足度調査、従業員意識調査、ストレスチェックなどにより自社のカルチャーを定期的に分析し、把握したカルチャーの特性や変化を行動規範の見直しに反映させているか。
(c)過去に定められた行動規範が長期間見直されておらず陳腐化し、現在の社会から求められている望ましい行動と乖離していることはないか。

③社内への浸透

・上記「（１）ミッション・ビジョン・コアバリュー」の「③社内への浸透」と同じ。
・研修では、法令遵守だけでなく、望ましい行動を取ることの重要性を伝えているか。また、評価・報酬体系で望ましい行動を取ることが評価されることを伝えているか。

④浸透状況の確認
・上記「（1）ミッション・ビジョン・コアバリュー」の「④浸透状況の確認」と同じ。

⑤評価・報酬制度
・上記「（1）ミッション・ビジョン・コアバリュー」の「⑤評価・報酬制度」と同じ。

（3）カルチャー
①定　義
・自社の望ましいカルチャーを**定義**しているか。
・定義に際しては、**オープンで率直な議論**を経た上で取締役会および経営者に承認されているか[注]。
（注）上記「（1）①定義」と同じ。

②リスクを認識、指摘・議論できるカルチャー
・経営者は、㋐**リスクを認識**するカルチャーや、㋑社員が**安心してリスクを指摘し議論**できる**カルチャーの醸成**に**自ら関与**しているか。

③互いを認め、尊重し合うカルチャー
・社員が**互いの良い行動を認め、尊重し合う職場のカルチャー**を醸成する取り組みが行われているか。
⇒㋐顧客からの感謝の声、㋑職場での貢献、もしくは、㋒業務の質向上や効率化などを職場で**共有**し、**顕彰**する制度を構築するなど。
・**挑戦する人が評価**されるようなカルチャーを醸成する仕組みがあるか。

④日々の業務処理を過度に重視
・管理者は、部下が**日々の業務を処理することが重要と考え**、**リスクを指摘し議論することを軽視**する考え方で部下と接していないか。

【考　察】
①カルチャーとミッション・ビジョン・コアバリューとの関係について
・カルチャーがミッション・ビジョン・コアバリューを**生み出して**おり、カルチャーがそれらの**土台**となっていると見ることができる。
・さらに限定して言えば、カルチャーはコアバリューの土台となっており、コアバリューは文書化できるが、カルチャーは文書化しにくいという特徴があるのではないか。
・逆に、**ミッション、ビジョン、コアバリューを踏まえた**社員の**日々の行動から、**「カルチャー」が**形成**されていく場合もある。
②カルチャーの監査手法について
・カルチャーの監査の重要な着眼点のひとつとして、**人事制度との関連**を確認することが挙げられる。例えば、㋐**挑戦**した人が人事上で評価される体系になっているか、㋑実際の**行動に表れていること**が人事上で評価されているかを確認することがあげられる。

・根本原因を解明する中で、カルチャーにたどり着く。
・具体的な行動を評価しないとカルチャーにたどり着けない。

③リスクカルチャーとコーポレートカルチャー

・リスクカルチャーはリスクへの感度高くビジネスを進めていく考え方や行動に焦点を当てており、時には不祥事防止に焦点が絞られている場合もある。
・コーポレートカルチャーは、企業内で共有される組織全体の行動原理や思考様式のことであり、その一部として「リスクカルチャー」がある（包含関係）。例えば、前向きな戦略を進めたい企業にとっては、挑戦による失敗は減点主義ではなく相応に評価することにより、挑戦を促進するコーポレートカルチャーが必要になる。

④カルチャーと風土の違い

・風土は過去からの歴史の中で出来上がってきたもの（雰囲気・空気感）なのに対して、カルチャーは会社に見られる特有の「行動パターン」で新しく作り上げることもできる。

⑤その他

・カルチャーは会社の不文律で、会社全体をカバーしているもの。

（４）ブランド

①実務の運営方針との整合性

・実務の運営方針は、自社の経営方針であるブランドと整合しているか。財務目標の達成や効率性の追求といった実務の運営方針のために、ブランド価値を毀損していることはないか。特に実務の運営方針を変更した時に、ブランドの毀損をうかがわせる兆候(注)が出ていないか。

（注）例：㋐顧客満足度の低下、㋑自社に対するSNSでの否定的な発信の件数増加、㋒退職者の増加、もしくは、㋓内部通報の件数増加。

【実務の運営方針がブランドと整合していない例】

・某自動車メーカーは、ブランドを重視するとの経営方針があるにもかかわらず、実務の運営方針は市場シェアの拡大であるため、販売奨励金を増加させて安売りを進め、ブランドを毀損させた。（この場合、ブランドと実務の運営方針は二律背反の関係にある）

原則４：コアバリューに対するコミットメントを表明する

参考にした事例：**事例２　政府機関におけるカルチャー**
　　：**事例３　金融機関におけるカルチャー**

①コアバリューの文書化と浸透・定着

・経営者は、会社が大切にしているコアバリューや行動規範を文書化し、自らの言動により社内に浸透させているか。また、研修、社内での各種の情報発信(注)、およびトップからの発信と意見交換により定着させているか。
　（注）㋐ｅラーニング、㋑動画配信、㋒イントラネット・社内報への掲載、㋓ポスター、もしくは、㋔業務用パソコンの壁紙。
・コロナ禍で、多人数を集めて訓示するなど直接接触することが難しい状況下でどのような工夫をしているか。
　⇒例：ｅラーニングや動画配信を活用。

②コアバリューと望ましい行動

・社員に会社が大切にしているコアバリューと望ましい行動を理解する機会(注)を提供しているか。
　（注）㋐コアバリューと望ましい行動および行動規範との関係や、㋑望ましい行動の実践に関する好事例についての研修や解説資料の配布など。

③各階層の役割と責任

・リスクマネジメントに関する規則で、各階層のリスクマネジメント上の役割と責任を業務実態に即して明確に定めているか。
・また、定期的に行われる重要リスクの見直しに合わせて、上記の役割と責任を見直しているか。

④リスク管理責任者

・各部門に部門内のリスクマネジメントに責任を持つ階層ごとのリスク管理責任者（例えば、推進責任者（マネージャークラス)、推進担当者（担当者クラス)）を配置しているか。

⑤個人の業務上の責任

・経営者は、社員に対して、担当する業務に関するリスクを管理することは当人の業務上の責任であること明確に伝え理解させているか。また、個々人のリスクの管理状況を人事評価に反映しているか。

原則５：有能な人材を惹きつけ、育成し、保持する

参考にした事例：**事例２ 政府機関におけるカルチャー**
：**事例３ 金融機関におけるカルチャー**

①評価・報酬制度や人材育成制度の設計

・評価・報酬制度や人材育成制度は、**ミッション・ビジョン・コアバリューに沿って設計**されているか。
・また、**望ましい行動**を促すように設計されているか。

②長期的で持続可能なパフォーマンス向上を促す評価・報酬体系

・評価・報酬制度は、**長期的で持続可能なパフォーマンス**を促し、**短期的なリスクテイクによる収益追求**を排除する体系となっているか。

【事例】報酬体系と営業手法の変更による業績向上
・証券Ａ社は、**収益に強くリンクした報酬体系**を採用し、顧客資産の**回転売買に伴う売買手数料を追求した収益獲得を優先した営業手法**で成長したが、顧客資産の目減りに伴い顧客離れが鮮明となり経営不振に陥った。
・経営再建に向け、経営陣のリーダーシップのもと、収益と強くリンクした報酬体系を見直し、回転売買中心の営業スタイルを**資産積み上げ型**へ変更した。その結果、安定した顧客基盤を形成し、経済環境に左右されない強固な経営体質を確立できた。

③必要な能力

・必要とされる能力は、㋐望ましいカルチャー、㋑望ましい行動、㋒自社の業務スタイル、および、㋓組織のニーズに合致しているか。また、必要な能力を**踏まえて**採用と育成を行っているか。
・戦略と事業目標の達成に必要な能力が**明確**になっているか。
・**キャリアビジョン**を示しているか。

④研　修

・入社時、昇格時、ポスト就任時などの**キャリアの節目**で、それぞれの時点・階層で求められる能力・考え方とミッション、ビジョン、コアバリューとのつながりを受講者が理解し、その理解を通して**リスクマネジメント能力の向上につながる研修**が行われているか。
・受講者および上司へのアンケート調査や受講者の実践状況の確認等に基づき、研修の効果を評価し、定期的に**研修の内容をアップデート**しているか。

⑤全社的リスクマネジメントを行うことの意義や役割の理解

・全社的リスクマネジメントは、ビジネスの目的を達成させるための手段であり、ビジネス活動そのものであるという全社的リスクマネジメントの**意義や役割**を理解させているか。

⑥知識・スキルの習得

・社員に全社的リスクマネジメントの知識やスキルを習得する機会(注1)(注2)を提供しているか。また、会社の全社的リスクマネジメントの体制と運用状況について説明しているか。

（注１）㋐社内研修の実施、㋑社外研修の受講、㋒参考文献を提示した自己学習の推奨など。

（注２）社内研修としては、㋐リスクの洗い出し、㋑リスクの評価と優先順位付け、㋒リスク対応策の策定についての解説と社内で過去に発生した重大なリスク事案を題材としたグループ・ディスカッションなど。

⑦スキルの継続的な確保

・全社的リスクマネジメントのスキルが組織として継続的に確保される体制になっているか。

＊全社リスクマネジメントのスキルが、関心の高いトップがいる間だけしか重視されないような継続性のない体制になっていないか。

⑧人事ローテーション・配置

・戦略に合わせた人事ローテーションや配置をしているか。

⑨採用促進

・自社のミッション・ビジョン・コアバリューやカルチャーに適した人材の採用を促進するために、それらに関する情報を積極的に開示しているか。

⇒リクルート用サイトやパンフレットにそれらを掲載すると共に、関連するトップメッセージや社員の声を掲載するなど。

⑩退職抑制

・有能な人材の退職を抑制する観点（リテンション戦略的視点）から、㋐自社で働くことが自身の成長につながることが実感できるように役割を付与しているか。㋑本人の希望キャリアを踏まえた職場ローテーションを行っているか。

・また、働きがいや研修受講の機会を与えているか。いわば、あの手この手で成長の機会を提供しているか。

構成要素２　戦略と目標設定

原則６：事業環境を分析する

参考にした事例：**事例４　エネルギー会社における戦略と目標設定**
　　：**事例５　非営利団体における戦略と目標設定**

①事業環境のカテゴリーごとの分析

・戦略の策定にあたって、将来の**事業環境の変化**を、㋐外部環境なら例えば、政治、経済、社会、技術、法規、および環境などのカテゴリーごとに、また、㋑内部環境なら例えば、資本、人材、および技術などのカテゴリーごとに**分析**しているか。そして、各カテゴリーでの環境変化が、戦略の達成に及ぼす影響を把握し、必要な対応策を検討しているか。

②前提や将来予測の根拠の変化に応じた戦略の見直し

・**事業環境が変化**し、現在遂行している戦略を策定した時に㋐**前提としていた事項**や㋑**将来予測の根拠としていた仮説**が**変化**している場合には、その変化に応じて戦略を**見直す**仕組みがあるか。

　＊当初想定していたシナリオ通りに進まないことが多いが、「いつかはうまくいくはずだ」と思っていることが多い。例えば、戦略の前提としていた技術開発が進んでいないなど当初の**想定**（仮定や前提）**が外れた**のにもかかわらず、前提が変化したことに合わせ**て戦略を見直していない**ことはないか。

原則７：リスク選好を定義する

参考にした事例：**事例４　エネルギー会社における戦略と目標設定**
　　：**事例５　非営利団体における戦略と目標設定**

①取締役会での承認・文書化・経営者による周知（手続き面）

・リスク選好を策定している場合、それは㋐取締役会、もしくは経営会議で**承認**され、㋑**文書化**されたうえで、㋒経営者によって全社に**周知**されているか。

②ミッション・ビジョン・コアバリューとの整合（内容面）

・リスク選好を策定している場合、それは会社の**ミッション・ビジョン・コアバリュー**に**沿った**ものとなっているか。

【リスク選好の定義】
・当研究会では、リスク選好を以下のように定義する。
　リスク選好とは、企業が**企業価値向上のために受け入れるリスクの種類と量**である。

【リスク選好の事例】
(a)**製薬会社**では、**薬事法違反**するリスク選好は非常に低い。
(b)**鉄道会社**では、**鉄道事故に起因する死亡事故**に対するリスク選好は非常に低い。
(c)業界二番手以下の会社のリスク選好は、業界一番手の会社と比較して相対的に高い。

原則８：代替戦略を評価する

参考にした事例：**事例４　エネルギー会社における戦略と目標設定**
　　：**事例５　非営利団体における戦略と目標設定**

①ミッション・ビジョン・コアバリューとの結びつき

・戦略が会社のミッション・ビジョン・コアバリュー（価値観・信念）に結びついているか。

②リスクの全体像に及ぼす影響の理解

・戦略を策定もしくは評価する場合、戦略が**リスクの全体像**（リスクプロファイル）(注1) **に及ぼす影響**を**理解**しているか。そして、戦略が目指すパフォーマンスを追求することでリスクが増加するとき、リスクが**リスク選好** (注2) **の範囲内に止まるよう**に、追求する**パフォーマンスをコントロール**しているか。

⇒戦略がリスクの全体像に及ぼす影響を理解しない場合には、高いパフォーマンスを追求するあまりリスクを過大に取り過ぎたり、逆にリスクを過少にしか取らず、不相応に低いパフォーマンスしか達成できなかったりする可能性が高まる。

（注１）リスクの全体像（リスクプロファイル）とは、**縦軸にリスク、横軸にパフォーマンスをとったリスク曲線とリスク選好との関係**を示したリスクの全体像のこと。**【図原則　８－１】**参照。

（注２）リスク選好とは、会社が企業価値向上のために進んで受け入れてよいと考えるリスクの種類と量のこと。

③リスクの全体像の継続的モニタリング

・高いパフォーマンスを追求する戦略を採用し、経営判断によりあえてリスク選好を上回るリスクを取る場合には、リスクが会社が耐えられるリスクの限界（リスクリミット）を超過しないように、**リスクの全体像**（リスクプロファイル）**を継続的にモニタリング**しているか。

【パフォーマンスの定義】

・当研究会では、パフォーマンスを以下のように定義する。

パフォーマンスとは、企業の最終目的である**「企業価値の向上」を実現するために必要な具体的かつ測定可能な個々の成果**。（例：売上、利益、もしくは市場シェアなど）

【リスクの許容範囲の定義】

・当研究会では、リスクの許容範囲を以下のように定義する。

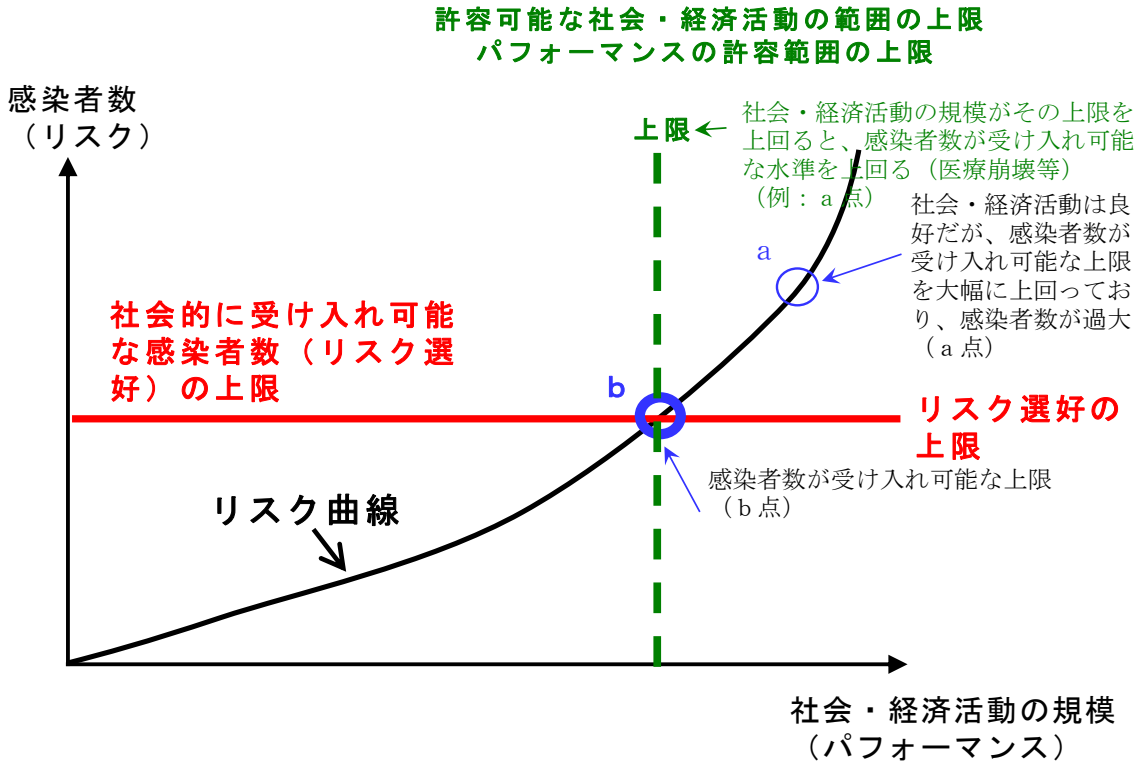
リスクの許容範囲とは、**「リスク選好の上限」以下**であり、かつ**「パフォーマンスの許容可能な下限」以上**のリスクの範囲である。」

④リスクの全体像（リスクプロファイル）の事例

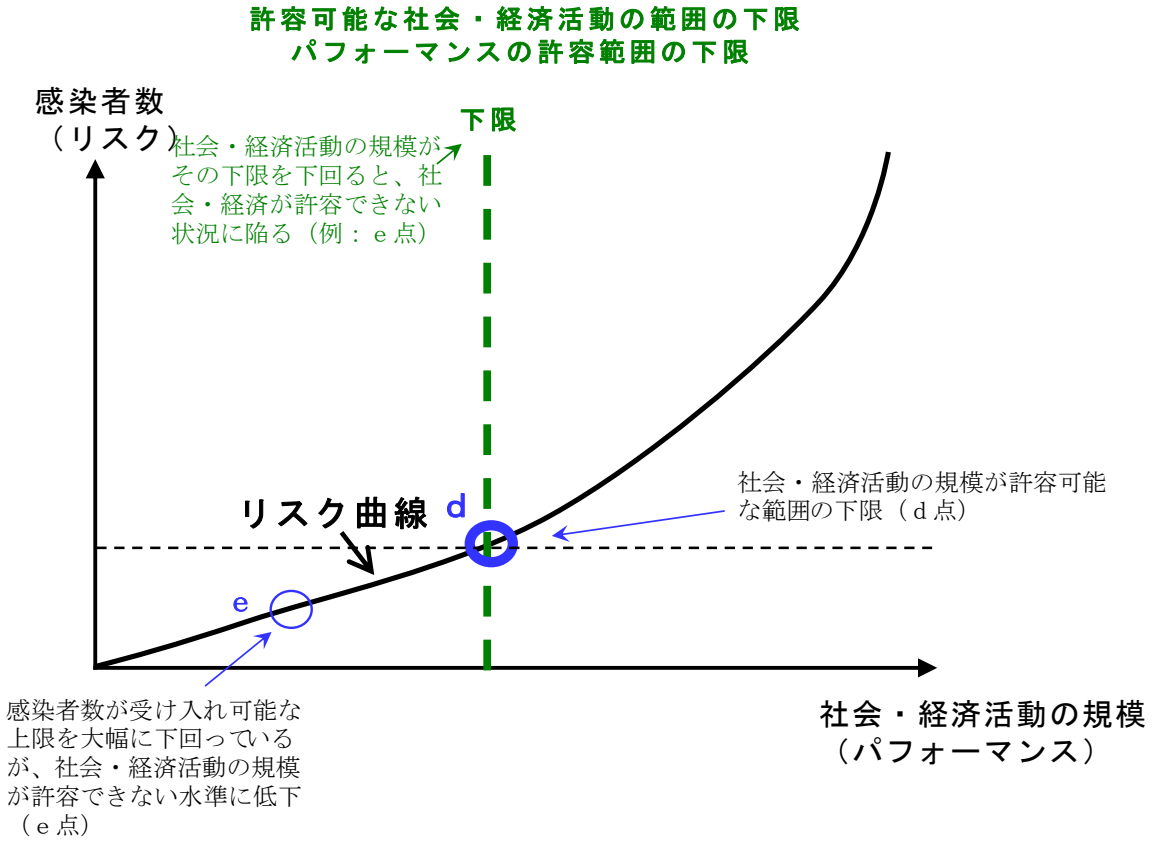
・リスクの全体像（リスクプロファイル）は、リスクとパフォーマンスとの関係を示すリスク曲線で表される。

事例１　リスクの全体像（リスクプロファイル）を用いた「新型コロナウイルス感染者数（リスク）」と「社会経済活動の規模（パフォーマンス）」との関係の整理　【図　原則８－１】

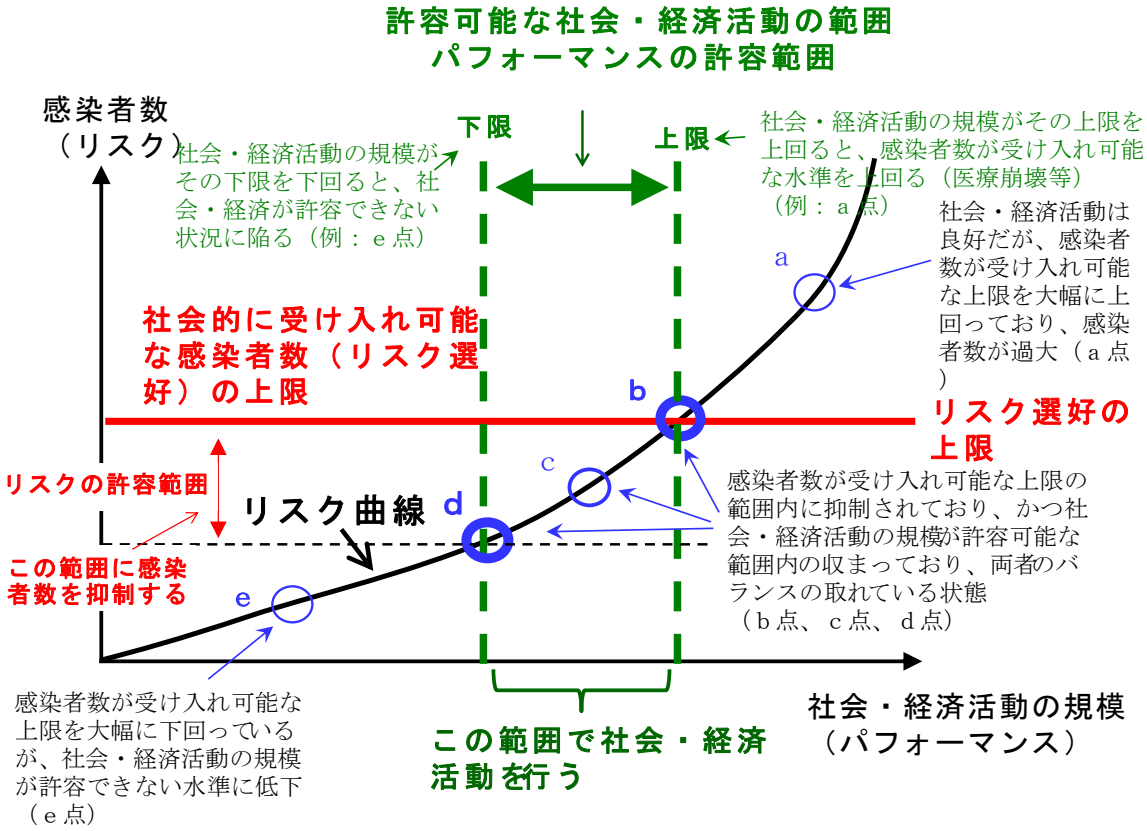
【Step １】　「リスク選好の上限」を起点とした
「リスク曲線」と「許容可能な社会・経済活動の範囲（パフォーマンスの許容範囲）の上限」との交点（ｂ点）の決定



【Step２】　「社会・経済活動の規模」（＝パフォーマンス）を起点とした
「リスク曲線」と「許容可能な社会・経済活動の範囲（パフォーマンスの許容範囲）の下限」との交点（ｄ点）の決定



【Step３】　【Step１】と【Step２】記載の図の合成による「許容可能な社会・経済活動の範囲（パフォーマンスの許容範囲）」である「リスク曲線上のｂ点とｄ点の間」の決定



注：吉野太郎著「全社的リスクマネジメント　会社がやってはいけないこと 80」（中央経済社）57 頁から引用。なお、この表は日本内部監査協会・八田進二・橋本尚・堀江正之・神林比洋雄監訳、日本内部統制研究学会 COSO-ERM 研究会訳「COSO 全社的リスクマネジメント　ー戦略およびパフォーマンスとの統合ー」280 頁「図表 D.6　リスクプロファイルを用いたリスク評価」を参考に作成。

≪解説：リスクの許容範囲とパフォーマンスの許容度との関係≫

・リスクの許容範囲は、リスク曲線がリスク選好と交わるｂ点を上限とし、同曲線がパフォーマンスの許容度の下限と交わるｄ点を下限としたリスクの許容可能な変動範囲である。

・パフォーマンスの許容度は、ｂ点を上限とし、ｄ点を下限としたパフォーマンスの許容可能な変動範囲である。

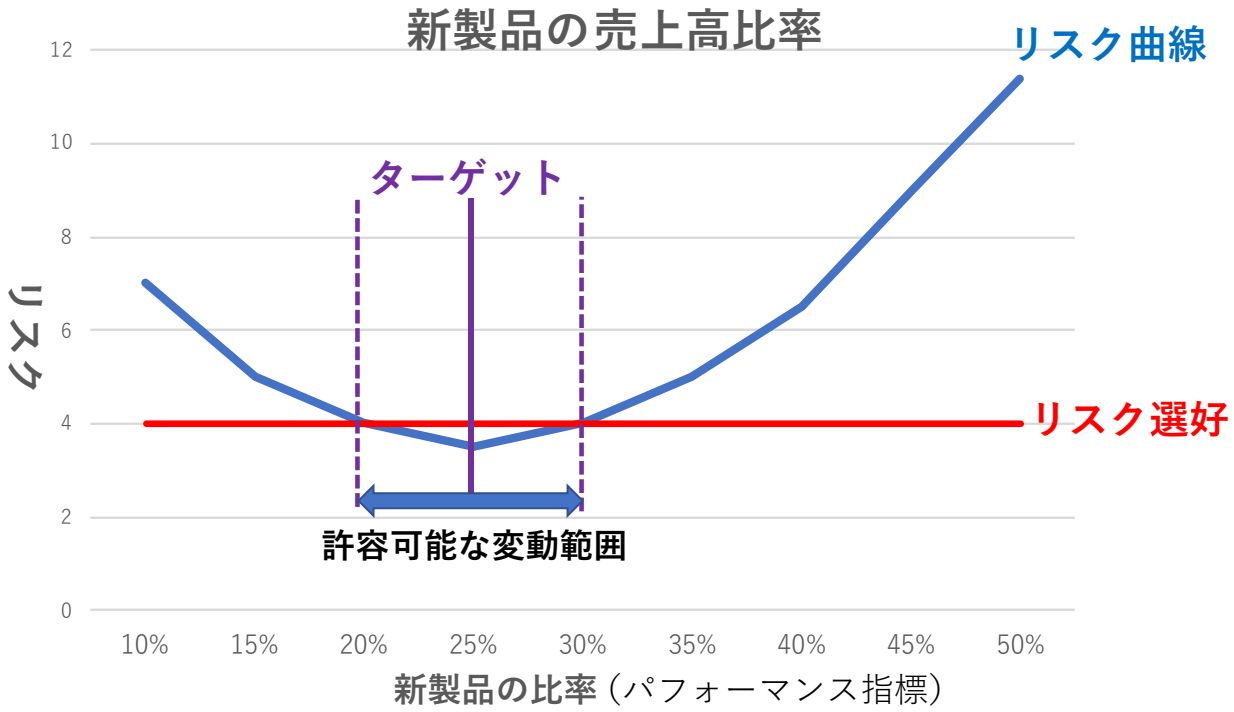
・つまり、リスクの許容範囲はｂ点とｄ点との関係を縦軸（リスク）で見た場合であり、パフォーマンスの許容度はそれを横軸（パフォーマンス）で見た場合に該当する。

・改訂版 COSO-ERM でいう「許容度」はパフォーマンスの許容可能な変動範囲を示すものであり、旧 COSO-ERM の「リスク許容度」とは意味が異なるので注意が必要である。

・パフォーマンスの許容可能な差異や変動の許容度を定義し、パフォーマンスがモニタリングされて許容可能な範囲にあることを確認することが重要である。

事例２　新製品の売上高比率（パフォーマンス）と総売上高の減少（リスク）との関係　【図　原則８－２】

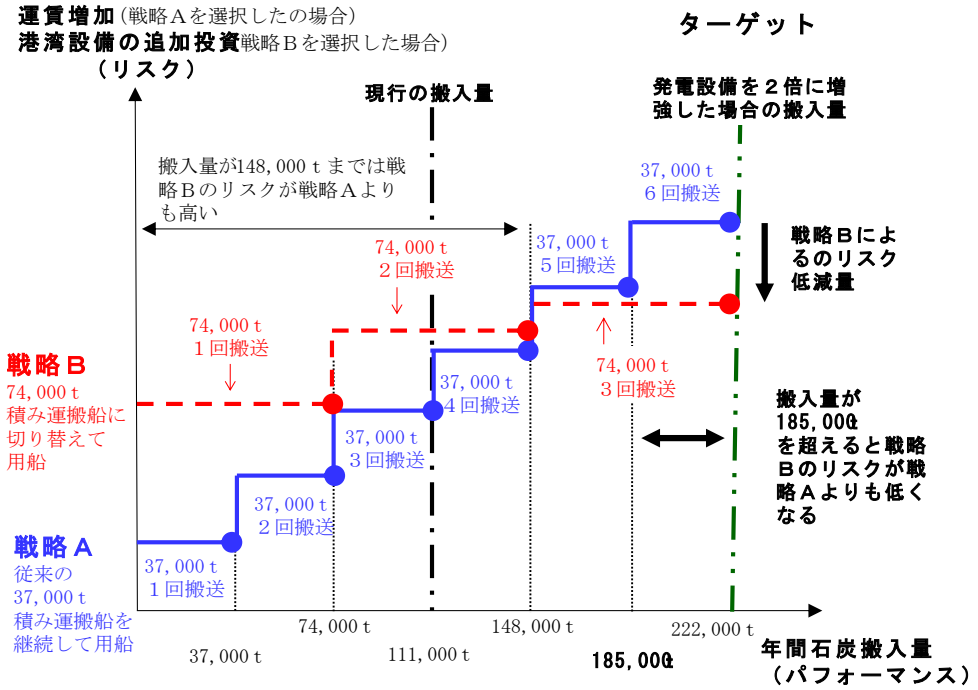
・Ａ社は、積極的な新製品の投入により売上高の拡大を図る戦略を採用している。
・マーケット調査の結果、**全体の売上高に占める新製品の割合（パフォーマンス）が 20%未満**の場合には、競合他社の新製品にシェアを奪われ、**全体の売上高が減少するリスク**があることが分かっている。また、その割合が **30%超**の場合には、既存製品が新製品に置き換えられるが、新製品だけでは既存製品の落ち込みをカバーできず**全体の売上高が減少するリスク**があることが分かっている。
・そのため、**全体の売上高に占める新製品の割合**（パフォーマンス）を 20～30%の水準とする戦略を採用した。この場合、**許容可能なパフォーマンスの変動範囲は 20%から 30%**であり、その範囲であれば全体の売上高が減少するリスクはリスク選好の範囲内に止まる。



事例３　リスクとパフォーマンスの関係から見た戦略の比較・評価　【図　原則８－３】

・ある石炭火力発電所では、石炭を37,000 トン積みの運搬船を用船して年３回（111,000 トン）搬入する前提で岸壁の規模、岸壁の水深、貯炭場の広さ、および荷揚げ設備の能力などの港湾設備を整備しているが、発電設備の２倍増強を検討している。
・発電設備の２倍増強に伴う石炭搬入量の２倍増に対応するために、㋐石炭運搬船を従来の 37,000 トン積みの運搬船を継続して用船し従来の２倍の年６回（222,000 トン）搬入する戦略Ａと、㋑運搬船を 74,000 トン積みに切り換え年３回（222,000 トン）搬入する戦略Ｂの２つの戦略を検討している。
・戦略Ｂ（74,000 トン積みの運搬船を用船）のメリットは船の大型化による１トン当たりの運賃低下であり他方、デメリットは㋐岸壁の拡張、㋑岸壁の水深深掘り、㋒貯炭場の拡張、および、㋓荷揚げ設備の能力増強などの港湾設備港拡充のための追加投資額の増加である。
・つまり、運搬量が少ないうちは小型船を用いる戦略Ａは、大型船を用いる戦略Ｂよりもコスト増加の可能性（リスク）が少ない。しかし、運搬量が増えるにつれて大型船を用いることによるスケールメリットが大きくなり、運搬量が 185,000ｔを超えた時点でコスト増加（リスク）は、大型船を用いる戦略Ｂが小型船を用いる戦略Ａを下回る。

【図　原則８－３】　37,000 トン積み運搬船を用船する戦略Ａと 74,000 トン積み運搬船を用船する戦略Ｂのリスクとパフォーマンスとの関係



原則９：事業目標を組み立てる

参考にした事例：**事例４　エネルギー会社における戦略と目標設定**
　　：**事例５　非営利団体における戦略と目標設定**

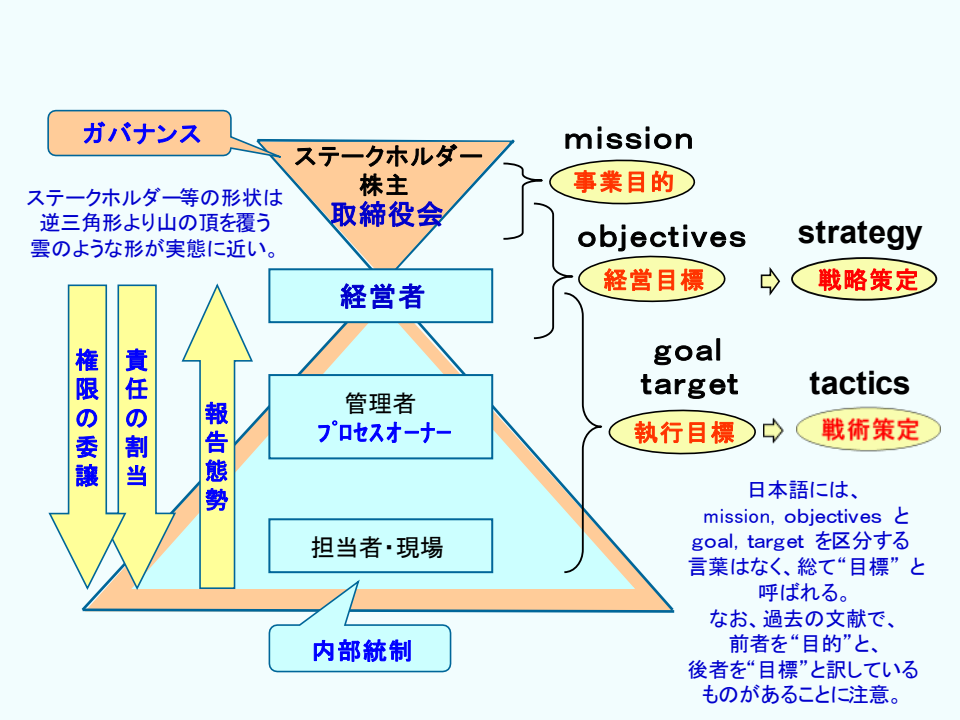
①目標とリスクの全社レベルから部門レベルへの落とし込み

・全社レベルの目標（上位目標）の達成を阻害する全社レベルのリスクを特定しているか。そして、各部門がそれぞれの役割に応じて全社レベルのリスクに対応するために、部門レベルにカスケードダウンした目標に対するリスクを特定しているか。

②階層に対応した戦略、目標の設定

・取締役会、経営者、および各部門といった階層に対応して、戦略、全社レベルの目標、および部門レベルの目標が設定されているか。

【図　原則９－１】　目標設定の概念についての一例



構成要素３　パフォーマンス

原則１０：リスクを識別する

参考にした事例：**事例６　消費財メーカーにおけるパフォーマンス**
　　：**事例７　テクノロジー会社におけるパフォーマンス**

①部門別の目標設定とリスクの特定

・全社目標の達成に繋がる個別・具体的な**各部門の目標が設定**されているか。
・各部門のそれぞれの目標に対し、目標達成に影響を与える**リスクが**洗い出され**特定**されているか。

【事例】

・「利益を対前年 10%増加」というストレッチした高い全社目標に対して、各部門も下記の高い目標を設定している。そして、目標に対し下記のリスクを特定している。

部　門	部門目標	目標に対するリスク
販売部門	新規マーケットへ参入する。	競合他社が多くまた顧客の要求水準が高いため、ニーズに合った商品を提供できない。
購買部門	調達コスト削減のため新規仕入先を開拓する。	新規仕入先の体制が不十分で納期遅れや品質低下が発生する。
製造部門	製品供給量増加のため外部委託を増加する。	外部委託先の技術レベルが不十分で製品の不具合が発生する。

・上記の例は、高い全社目標に対応するために各部門では従来とは異なる新しい取り組みが必要となり、それに伴い新たなリスクが発生していることを示している。つまり、ストレッチした高い全社目標の設定により、各部門に新たなリスクが生じていることを示している。

②前提条件を明確にする

・**戦略と目標を設定する際の前提条件**は、十分な資料に基づく議論を行い明確になっているか。

③環境変化に応じてリスクを識別する

・内外の事業**環境の変化に**関する情報を適時に収集し、環境変化に応じた適切なタイミングで**リスクの識別**を行っているか。

④目的に合った情報を効率的に収集するツールを使用する

・内外の事業環境の変化に関する**情報を収集する**ために使用している**ツール**は、リスクを識別・評価する**目的に合った情報**を効率的に収集するものであるか。

【情報収集ツールの例】
(a)顧客クレームの収集・分析ツール。
(b)顧客満足度調査の分析ツール
(c)修理履歴の収集・分析ツール

⑤適時に情報を収集・伝達する

・情報収集ツールを用いて**適時に**情報を**収集**し、**適時に**リスク識別を行う部門にその情報を**伝達**しているか。

⑥環境変化のスピードに即した頻度でリスクを識別する

・リスクを識別する㋐**頻度**、㋑**手法**、および、㋒識別に**使用する情報**は、経営環境変化のスピードに即しているか。

【経営環境変化のスピードに即したリスク識別の例】
・技術変化の激しいテクノロジー会社では、新しいリスクを早期に識別するため、年1回実施する定例アンケートとインタビューによるリスク識別に加え、**毎月**、㋐データマイニング、㋑自動言語処理、㋒機械学習などのIT技術を利用して、データを収集・分析し、**リアルタイムでのリスクの識別**を行っている。さらに、IOT（Internet of Things＝モノのインターネット）を使用した機械の稼働状況の**常時モニタリング**を行っている。

⑦部門リスクマネジメント統括者の設置

・各部門に、**部門のリスクマネジメント活動をモニタリング、調整、統括する幹部クラスの者**（部長、筆頭マネージャークラスで部門内の各階層のリスク管理責任者を統括する立場にある者）を任命しているか。
＊「部門リスクマネジメント統括者」とは、他部門とリスク対応について調整できる幹部クラスを指し、本書（「COSO全社的リスクマネジメント　戦略およびパフォーマンスとの統合　事例の解説篇」）37頁記載の「リスク大使」に該当する。

原則１１：リスクの重大度を評価する

参考にした事例：**事例６　消費財メーカーにおけるパフォーマンス**
　　：**事例７　テクノロジー会社におけるパフォーマンス**

①リスクの評価基準を設定する

・リスクを評価するための**評価基準**（影響度と発生頻度の目安）が定められているか。
・また、評価基準は**全社で統一**され、**継続的に使用**されているか。
　＊評価基準の統一は、㋐同じ目線でリスクを評価しリスク評価のバラツキを少なくするために、あるいは、㋑同じ尺度でトレンド分析を行い環境変化を把握するために必要。

【評価基準の例】
(a)財務数値
(b)非財務数値・データ　（例：財務情報だけでは分からない案件数、問い合わせ件数、クレーム数など金額換算されていない数値・データ）
(c)定量的基準(モデル化されたデータなど)、定性的基準（レビューやワークショップの結果など）

②製品サイクルの節目ごとにリスク評価を実施する

・設計、開発、検査、発売前、および発売後など製品サイクルの節目でリスク評価を行い、各段階でのリスクが**リスク選好の上限の範囲内**に収まっていることを確認しているか。

③評価対象の事業と整合した評価基準を用いる

・**評価対象の事業**と整合した**リスク評価の基準**を用いているか。

【例】

評価基準 / 事業	市場に関する基準	評判に関する基準	費用に関する基準	業務に関する基準
新製品開発	○	○	○	
設備拡張	○		○	○

④環境変化のスピードに即したリスク評価の頻度

・リスク評価の頻度は、経営環境の変化のスピードに即しているか。

【経営環境の変化のスピードの例】
(a)製品ライフサイクルの変化のスピード
(b)技術革新のスピード
(c)顧客ニーズの変化など需要変化のスピード
(d)競合他社の新製品投入のスピードなど競合激化のスピード

原則１２：リスクの優先順位づけをする

参考にした事例：**事例６ 消費財メーカーにおけるパフォーマンス**
：**事例７ テクノロジー会社におけるパフォーマンス**

①全社目標の達成に与える影響度を基準とする

・各部門の目標に対するリスクは、**全社目標の達成に与える影響度**を基準として対応の優先順位づけをしているか。
・また、**他部門の目標達成に影響を与えるリスク**についても考慮しているか。（こうしたリスクは、全社目標の達成にも大きな影響を与えると考えられる。）

【事例】
・**「購買部門」の納期遅れや品質低下のリスクや「製造部門」の製品の不具合といったリスクは、自**部門の目標達成に影響を及ぼすだけでなく、「販売部門」の新規マーケットへの参入という**他部門の目標達成を困難にし、全社目標の達成にも影響を及ぼす**ため、対応の優先順位が高いと考えられる。

②優先順位づけの基準・根拠・用いた情報を確認する

・㋐リスクを優先順位づけする**基準**と、㋑その基準を選択した**根拠**、および、㋒用いた**情報の内容と入手先・出所**を確認する。

原則１３：リスク対応を実施する

参考にした事例：**事例６　消費財メーカーにおけるパフォーマンス**
　　：**事例７　テクノロジー会社におけるパフォーマンス**

①リスクの優先順位づけ・リスク対応のコスト・パフォーマンスを比較検討する

・リスク対応策の選択は、㋐**リスクの優先順位づけ**の結果、㋑リスク選好の上限の範囲内にリスクを抑制するために要する**コスト**、および、㋒その場合に得られる**パフォーマンス**（リスク選好の範囲内にリスクを抑制した場合のパフォーマンス）を**比較検討**して行っているか。

②パフォーマンス指標に基づいてリスク対応を実施する

・リスクに直接影響を及ぼす**パフォーマンスを追跡する指標**を設定し、指標が閾値に接近した場合にリスク対応をタイムリーに行える体制を整備しているか。

【パフォーマンス指標の例】

㋐製品の売上高・出荷数
⇒増加した時には問い合わせ増加に備えてコールセンター要員を増員し（リスク対応の強化）、低下した時には問い合わせの減少を見込んで減員する（リスク対応コストの適正化）。

㋑製品の操作方法に対する内容別・部位別の顧客からの問い合わせ・クレームの件数
⇒重点的に操作性（ユーザーインタフェース）の改善を要する箇所を特定して、経営資源投入の優先度を高めて、製品競争力の強化につなげる（リスク対応の強化）。

原則１４：ポートフォリオの視点を策定する

参考にした事例：**事例６　消費財メーカーにおけるパフォーマンス**
　　：**事例７　テクノロジー会社におけるパフォーマンス**

①複数部門で関係のあるリスクを全社レベルで集約する

・**複数の部門で関係のある目標に対するリスク**を識別・評価し、その結果を全社レベルで集約して、全社レベルで必要な対応を検討しているか。

⇒メーカーであれば開発・調達・製造・販売というサプライチェーンの中で、担当する各部門がリスクを識別・評価し、その結果をサプライチェーン全体で集約しているか。そして、サプライチェーン全体の観点で、リスクを識別・評価し、対応を検討しているか。

②各部門でのリスクの識別・評価の結果を集約して全社レベルのリスクを把握する

・各**部門でのリスクの識別・評価の結果**を集約し、**複数の部門にまたがる共通のリスク**を**全社レベルで把握**しているか。また、複数の部門に影響を与える共通の重要リスクへの対応を全社レベルで検討しているか。

構成要素４　レビューと修正

※原則１５と原則１６はリスクマネジメントの個別事項を対象としている。原則１７はリスクマネジメント全体を対象としている。

原則１５：重大な変化を評価する

参考にした事例：**事例８　工業製品会社におけるレビューと修正**

①環境変化の影響を把握・分析した上でパフォーマンスを評価する

・パフォーマンス評価のために実績対目標の差異分析を行う時に、**環境変化がパフォーマンスに及ぼす影響**を把握、分析した上で、パフォーマンスを評価しているか。
　　＊本件は**過去**に関する事項を対象としている。

②今後の変化の兆候とその推移を把握する

・環境変化がパフォーマンスに及ぼす影響を把握する時に、変化の結果だけでなく、今後の**変化の兆候と**その**推移**も把握しているか。
　　＊本件は**将来**に関する事項を対象としている
　　＊変化の兆候は主要リスク指標とほぼ同じと考えてよい。

⇒**変化の兆候を示す指標**として、例えば㋐特定地域での市場動向、㋑特定商品の販売動向、もしくは㋒特定商品の需給や価格変動の動向などを設定しておき、それらの指標を継続的にモニタリングすることにより、**今後の変化の兆候**を把握し、**環境変化**を早期に、もしくは事前に把握することが考えられる。

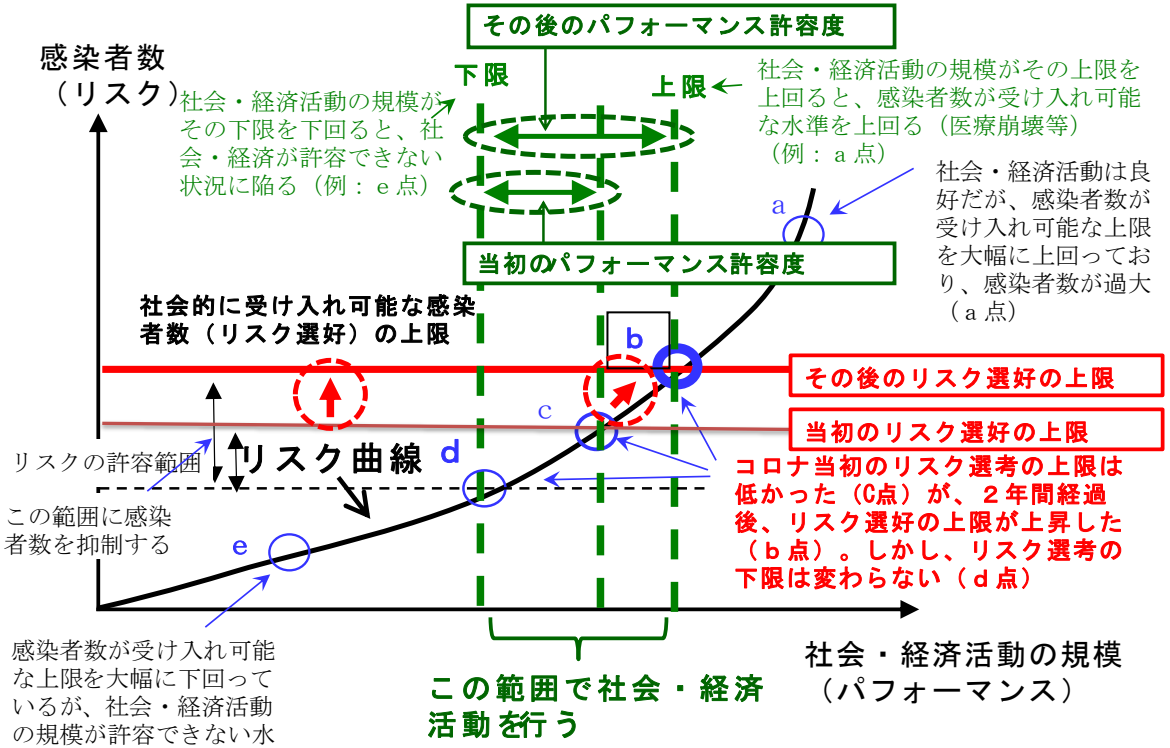
③リスクの特性に見合った頻度でのリスク評価

・リスクの特性に見合った頻度でリスクを評価しているか。

事例　リスクプロファイルの変化：リスク選好上限の上昇とパフォーマンス許容度の拡大　【図　原則１５】

・コロナ禍当初のリスク選好の上限は低く、パフォーマンスの許容度も狭かった（操業停止・自宅待機・イベント自粛）。

・その後２年経過した現在、㋐ワクチン接種が進み重症者数が減少傾向にあること、および、㋑病院病床使用率の逼迫度合いが緩和傾向にあることから、<u>リスク選好の上限は上昇</u>し、<u>パフォーマンスの許容度も拡大</u>している（出勤率回復、イベント再開）。



注：吉野太郎著「全社的リスクマネジメント　会社がやってはいけないこと 80」（中央経済社）57 頁を加工して作成。なお、この表は日本内部監査協会・八田進二・橋本尚・堀江正之・神林比洋雄監訳、日本内部統制研究学会 COSO-ERM 研究会訳「COSO 全社的リスクマネジメント　－戦略およびパフォーマンスとの統合－」280 頁「図表 D.6　リスクプロファイルを用いたリスク評価」を参考に作成。

原則１６：リスクとパフォーマンスをレビューする

参考にした事例：**事例８ 工業製品会社におけるレビューと修正**

①パフォーマンス変化の分析を通したリスク変化の把握

・例えば、「パフォーマンス目標の設定段階（予算の設定時など）で想定されていたリスクの大きさ」と、「パフォーマンス結果のレビュー段階（実績の検討時など）で把握されたリスクの大きさ」を比較、検討することによって、つまり、当初想定したパフォーマンスと実際のパフォーマンスとの対比、検証といったパフォーマンスの変化の分析を通して、リスクの変化を把握しているか。

＊パフォーマンスの変化を把握することを通して、リスクの変化を把握する。つまりパフォーマンスを通してリスクを識別・評価する。

＊全社的プロジェクトとして多額のリソース（予算、人員）を投入してリスク把握と順位付けを行った場合、リスクの識別と評価が長期間に硬直的に維持されることがある。硬直的なリスクの識別と評価はリスク対応の有効性を低下させるため、リスクの変化を把握する仕組みを作っておくことが必要である。

②パフォーマンスが許容範囲内に収まっていない場合の対応を検討しておく

「パフォーマンスが許容の範囲内に収まっていない場合の対応」を確認し、対応策が検討されているか。

③パフォーマンスの許容範囲を明確にしておく

・パフォーマンスの許容範囲が明確にされているか。また、許容範囲の下限・上限に達する手前でのアラートが設定されているか。

④“Trusted Advisor”（信頼されるアドバイザー）として機能する内部監査部門

・内部監査部門は“Trusted Advisor”として機能しているか。

【“Trusted Advisor”として機能する内部監査部門の例】

・社長が懸念しているが公の会議では議論が煮詰まらないことを監査部が社長に代わって議論して、その結果を社長に報告している。10 年以上このやり方を続けている。

・具体的には、社長が懸念していること（気にしていること）に“当たり”をつけて社長に確認して監査の論点を決めている。確認した論点で監査して社長に報告している。

原則１７：全社的リスクマネジメントの改善を追求する

参考にした事例：**事例８　工業製品会社におけるレビューと修正**

①パフォーマンスとの関係からリスクとその対応状況を把握・評価する

・全社的リスクマネジメントをパフォーマンスの向上、つまり企業価値向上に資するものとするために、リスク管理部門は、**パフォーマンスに焦点**を当て、達成された**パフォーマンスのとの関係から、**リスクとその対応状況を把握・評価することにより、**全社的リスクマネジメント全体の改善**を追及しているか。

＊COSO-ERM では、パフォーマンスからリスクを見ている。

＊パフォーマンスとリスクの把握は例えば、経営会議、実績検討会議などのパフォーマンスを検討する会議体に参加すること、または少なくともその情報を入手することにより行う。

＊リスク管理部門のリスク対応状況の把握は例えば、各リスク主管部門との情報交換、内部監査部門との連携により行う。

②全社的リスクマネジメント体制全体の課題の把握・改善

・個別リスクとその対応状況を把握・分析した後に、**全社的リスクマネジメント体制全体の課題**を把握し、改善まで含めた活動を行っているか。

構成要素５　情報、伝達及び報告

原則１８：情報とテクノロジーを有効活用する

参考にした事例：**事例９　医療機関におけるリスク情報**

①意思決定に必要なリスク情報の見極め・収集・分析・報告

・リスク管理部門を含む各部門は、適切なタイミングで（例：四半期、半期、年次）所管業務に関連する取締役会や経営者の**意思決定に必要なリスク情報**を**見極め**、**テクノロジーを活用**して当該情報を**収集**・**分析**し、**報告**しているか。

②内外の要因の見極め・収集・分析・報告

・リスク管理部門を含む各部門は、所管業務に関連する会社の目標達成に影響を及ぼす**外部、内部の要因**を**見極め**、**テクノロジーを活用**して当該要因を**収集**・**分析**し、取締役会や経営者に**報告**しているか。

＊外部要因の収集方法の例：IT 活用によるビックデータの収集・解析。

＊内部要因の収集方法の例：㋐全社レベルでの意識調査・コンプライアンスアンケート・情報セキュリティアンケートなどの調査結果の閲覧、㋑各部門が個別に行うアンケートやインタビュー。

原則１９：リスク情報を伝達する

参考にした事例：**事例９ 医療機関におけるリスク情報**

①リスクの原因と影響を適切に分析・評価した調査レポートを提出する

・経営上のリスクに直面しその対応を検討する時に、取締役会および経営者が最適な意思決定ができるように、社内および社外の関連情報を収集、分析し、リスクの原因と影響を適切に分析、評価した調査レポートを提出しているか。

②リスク情報が迅速・正確に報告される体制・組織文化

・リスク情報（事案だけでなく対応、分析・評価も含む）が迅速・正確に報告される㋐**ルール・規則・報告ルート**などの**体制**（ハード面）や㋑率直に報告できる**健全なコミュニケーション**などの**組織文化**（ソフト面）が構築、醸成されているか。
・特に、現場で経営上重大なリスク事案が発生した時に、現場担当者→現場管理者→本社統括部門→経営者に迅速・正確に報告される体制や組織文化が構築され、実際に機能しているか。

③多様な情報伝達経路

(a)一般社員など下位者から幹部や経営者など**上位者への情報伝達ルート**が整備され、実際に機能しているか。（下から上への伝達ルート）
(b)幹部や経営者など**上位者から**一般社員など**下位者への情報伝達ルート**が整備され、実際に機能しているか。（上から下への伝達ルート）
(c)**異なる職場間・部門間の情報伝達ルート**が整備され、実際に機能しているか。（横の伝達ルート）
(d)職制上の下位者から上位者への情報伝達ルートだけでなく、内部通報制度など**複数の伝達ルート**が整備され、機能しているか。（複数の伝達ルート）
(e)発注元である当社と業務委託先である協力企業、あるいは親会社・子会社間といった**法人を跨いだ情報伝達ルート**が整備され、実際に機能しているか。（法人間の伝達ルート）

原則２０：リスク、カルチャーおよびパフォーマンスについて報告する

参考にした事例：**事例９　医療機関におけるリスク情報**

①リスク情報を幅広く収集し多様な視点から分析して報告する

・リスク情報を特定の分野に偏ることなく幅広く収集し、多様な視点から分析した上で、取締役会および経営者に報告しているか。

＊収集するリスク情報が、㋐内部情報、㋑外部情報、㋒統一の基準や枠組みにより整理された情報、もしくは、㋓整理されていない情報の集積など特定の分野に偏ることがないように留意する。

【事例】

・Ａ病院は、㋐院内の医療従事者へのインタビューなどの**内部情報**、および、㋑当局（厚生労働省、自治体、保健所）からの情報や専門家の見解などの**外部情報**の両方を幅広く収集した。それら内外の情報に基づいて、**専門の医師・看護師も参加した拡大理事会**で新型コロナウイルス対応のための病床数、要員体制、および対応方針を意思決定した。

②パフォーマンスを通してリスクをモニタリングする

・**パフォーマンス**（例：営業実績の拡大、医薬品の売上高）**とリスク**（例：バックオフィス部門のミスの増加、薬価基準の変更）**を別々に議論せず**、一緒に議論し、**パフォーマンスの変化**をモニタリング（把握・分析）することを通して、**リスクの変化**をモニタリング（把握、分析）しているか。つまり、**パフォーマンスを出発点としてリスクを見て**いるか。

【事例】

・Ｂ製薬の収益の大部分を占める医療用医薬品の収益に影響を与える**薬価基準**が、政策の変更により今後大きく**変動**すること（リスク）が想定されている。

・このため、㋐**主力製品の売上**への影響、㋑結果としてのＢ社の**収益**への影響（パフォーマンス）を検討しながら、リスクへの対応策を検討している。

③望ましいカルチャーの伝達・浸透状況を検証・評価し報告する

・取締役会および経営者が求めている**望ましいカルチャー**が適切に定義づけられ、社内に正しく**伝達**され、社員の行動や判断に反映されるなど**浸透**しているかが**検証・評価**され、結果が取締役会および経営者に承認されているか。

【事例】

・Ｃ病院では、近年の採用難により、看護職員の負担が過重になってきている。

・対応策のひとつとして、地域社会・患者への姿勢に関する当病院のミッション・ビジョン・コアバリューを組織内に浸透させ、**望ましいカルチャーを適切に定義し、伝達・浸透**させることにより、看護職員のモラルを維持し、離職を抑制しようとしている。

５．参考資料：全社的リスクマネジメントと内部統制とのおおよその関係

・全社的リスクマネジメントの20の原則と表面上概ね対応していると見える内部統制の17の原則とのおおよその対応関係は下表の通りです。なお、これは両者の関係の理解の一助として記載したものです。

全社的リスクマネジメント（ＣＯＳＯ・全社的リスクマネジメント－戦略およびパフォーマンスとの統合　2017年9月公表）		内　部　統　制（ＣＯＳＯ・内部統制の統合的フレームワーク　2013年5月公表）	
構成要素	**原　　則**	**構成要素**	**原　　則**
構成要素１ **ガバナンスとカルチャー**	**１．取締役会によるリスク監視を行う**	構成要素１ **統制環境**	**監督責任の遂行**　（原則２）
	２．業務構造を確立する		**組織構造、権限・責任の確立**　（原則３）
	３．望ましいカルチャーを定義づける		**誠実性と倫理観に対するコミットメントの表明**（原則１）
	４．コアバリューに対するコミットメントを表明する		**説明責任の履行**　（原則５）
	５．有能な人材を惹きつけ，育成し，保持する		**業務遂行能力に対するコミットメントの表明**　（原則４）
構成要素２ **戦略と目標設定**	**６．事業環境を分析する**		※対応すると思われる内部統制の構成要素はない。
	７．リスク選好を定義する		※対応すると思われる内部統制の構成要素はない。
	８．代替戦略を評価する		※対応すると思われる内部統制の構成要素はない。
	９．事業目標を組み立てる		※対応すると思われる内部統制の構成要素はない。
構成要素３ **パフォーマンス**	**１０．リスクを識別する**	構成要素２ **リスク評価**	**適合性のある目的の特定**　（原則６）
	１１．リスクの重大度を評価する		**リスクの識別と分析**　（原則７）
	１２．リスクの優先順位づけをする		**不正リスクの評価**　（原則８）
	１３．リスク対応を実施する		**重大な変化の識別と分析**　（原則９）
	１４．ポートフォリオの視点を策定する		

構成要素3 **統制活動**	**統制活動の選択と整備**　（原則１０）
	テクノロジーに関する全般的統制活動の選択と整備（原則１１）
	方針と手続を通じた展開　（原則１２）

構成要素４ **レビューと修正**	**１５．重大な変化を評価する**
	１６．リスクとパフォーマンスをレビューする
	１７．全社的リスクマネジメントの改善を追求する

構成要素5 **モニタリング活動**	**日常的評価および／または独立的評価の実施**（原則１６）
	不備の評価と伝達　（原則１７）

構成要素5 **情報，伝達および報告**	**１８．情報とテクノロジーを有効活用する**
	１９．リスク情報を伝達する
	２０．リスク、カルチャーおよびパフォーマンスについて報告する

構成要素４ **情報と伝達**	**関連性のある情報の利用**（原則１３）
	組織内における情報伝達　（原則１４）
	組織外部との情報伝達　（原則１５）

引用文献

・トレッドウェイ委員会支援組織委員会（COSO:Committee of Sponsoring Organizations of the Treadway Commission）著　一般社団法人日本内部監査協会、八田進二、橋本尚、堀江正之、神林比洋雄監訳**「ＣＯＳＯ全社的リスクマネジメント　－戦略およびパフォーマンスとの統合」**（2018年4月同文舘出版）74頁他。

・トレッドウェイ委員会支援組織委員会（COSO:Committee of Sponsoring Organizations of the Treadway Commission）著　八田進二、箱田順哉監訳　日本内部統制研究学会新COSO研究会訳**「内部統制の統合的フレームワーク　フレームワーク篇」**（2014年2月日本公認会計士協会出版局）40～42頁他。

参考文献

・トレッドウェイ委員会支援組織委員会（COSO:Committee of Sponsoring Organizations of the Treadway Commission）著　一般社団法人日本内部監査協会、八田進二、橋本尚、堀江正之、神林比洋雄監訳
「ＣＯＳＯ全社的リスクマネジメント　－戦略およびパフォーマンスとの統合」　（2018年4月　同文舘出版）

・ポール・ソーベル著　八田進二監訳　堺咲子訳
「**不確実な時代のリスクマネジメント　―ＣＯＳＯ新ＥＲＭフレームワークの活用**」　（2018年8月　日本内部監査協会出版）

・トレッドウェイ委員会支援組織委員会（COSO:Committee of Sponsoring Organizations of the Treadway Commission）著　八田進二、箱田順哉監訳　日本内部統制研究学会新COSO研究会訳
「内部統制の統合的フレームワーク　フレームワーク篇」　（2014年2月　日本公認会計士協会出版局）

以　上