protiviti®
Face the Future with Confidence

一橋大学財務リーダーシップ・プログラム　B

「攻めと守りのリスクマネジメントの在り方」

～ガバナンス･リスク･内部統制、最近の動向と新COSOERM

神林 比洋雄
プロティビティLLC 会長
2018年12月1日

protiviti®
Face the Future with Confidence

プロティビティのご紹介

Internal Audit, Risk, Business & Technology Consulting

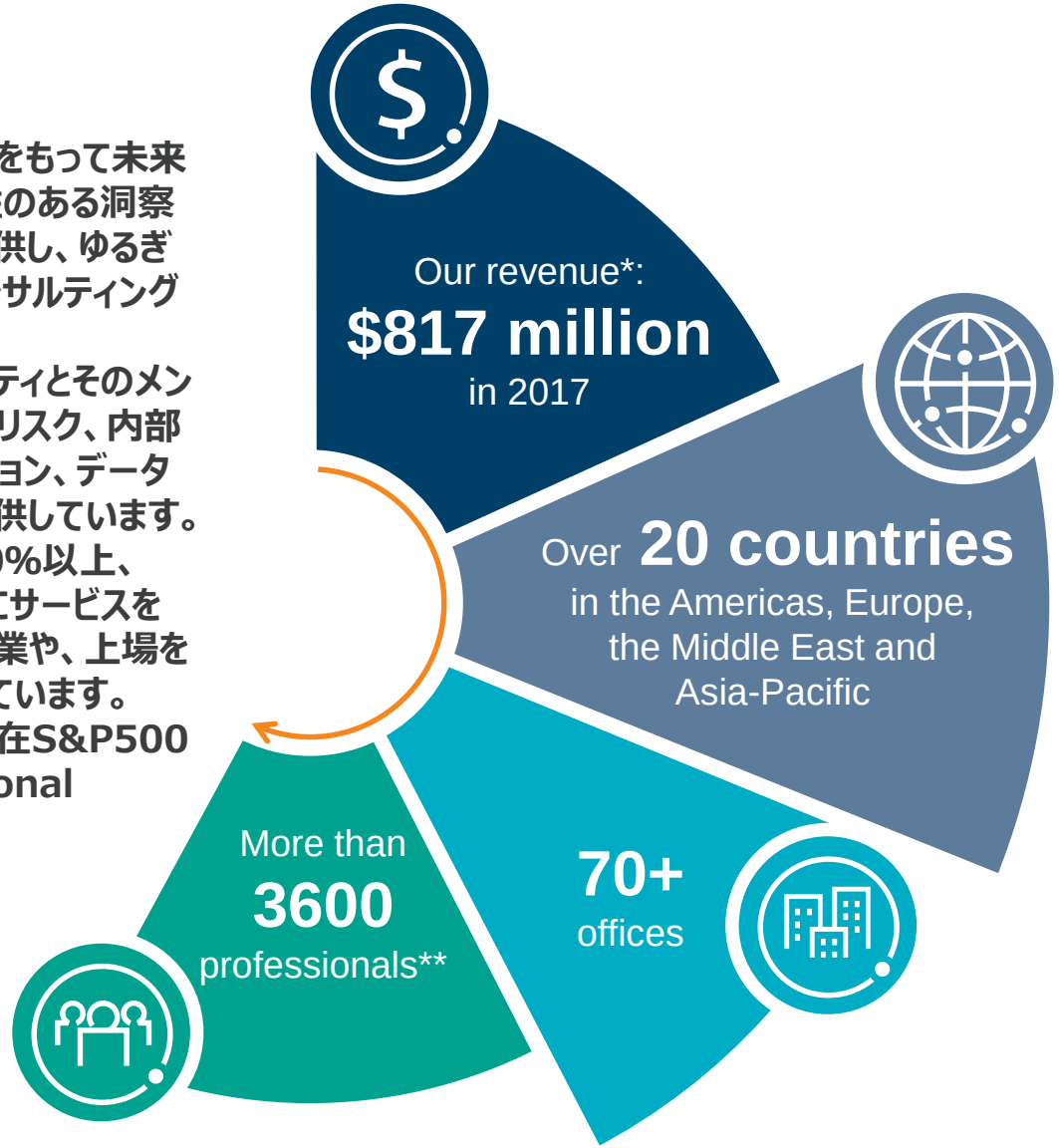
プロティビティとは

プロティビティは、企業のリーダーが自信をもって未来に立ち向かうために、高い専門性と客観性のある洞察力や、お客様ごとに的確なアプローチを提供し、ゆるぎない最善の連携を約束するグローバルコンサルティングファームです。

20ヶ国、70を超える拠点で、プロティビティとそのメンバーファームはクライアントに、ガバナンス、リスク、内部監査、経理財務、テクノロジー、オペレーション、データ分析におけるコンサルティングサービスを提供しています。

プロティビティは、Fortune 1000の60%以上、Fortune Global 500の35%の企業にサービスを提供しています。また、成長著しい中小企業や、上場を目指している企業、政府機関等も支援しています。

プロティビティは、1948年に設立され現在S&P500の一社であるRobert Half International (RHI)の100%子会社です。



*プロティビティのメンバーファームを含めると約*5,000*名。*2017*年度の売上は *888*百万米ドル。

protiviti

海外ネットワーク

The Americas

1. UNITED STATES
Alexandria, VA
Atlanta, GA
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Indianapolis, IN
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

2. ARGENTINA*
Buenos Aires

3. BRAZIL*
Rio de Janeiro
São Paulo

4. CANADA
Kitchener-Waterloo
Toronto

5. CHILE*
Santiago

6. MEXICO*
Mexico City

7. PERU*
Lima

8. VENEZUELA*
Caracas

**Protiviti Member Firm*

Europe/Middle East/Africa

9. FRANCE
Paris

10. GERMANY
Frankfurt
Munich

11. ITALY
Milan
Rome
Turin

12. THE NETHERLANDS
Amsterdam

13. UNITED KINGDOM
London

14. BAHRAIN*
Manama

15. KUWAIT*
Kuwait City

16. OMAN*
Muscat

17. QATAR*
Doha

18. UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

19. SAUDI ARABIA*
Riyadh

20. SOUTH AFRICA*
Johannesburg

Asia-Pacific

21. AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

22. CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

23. INDIA*
Bangalore
Hyderabad
Kolkata
Mumbai
New Delhi

24. JAPAN
Osaka
Tokyo

25. SINGAPORE
Singapore

protiviti

本日のメンバーのご紹介

神林　比洋雄 シニア マネージングディレクタ	アーサーアンダーセン東京事務所入社。海外を含む監査業務およびビジネスコンサルティング業務に従事。サンフランシスコ、香港での勤務を経て、アンダーセンワールドワイドパートナー、朝日監査法人（現あずさ監査法人）代表社員、本部理事、アンダーセンリスクコンサルティング・アジアパシフィック代表、アンダーセンワールドワイド取締役を歴任。 2003年プロティビティ ジャパン社長。統合リスク、内部統制や内部監査に関わるコンサルティングを多数手がけ、SOX、IFRSソリューションなどを指揮・監督。 外務省改革委員会アドバイザー、経済産業省企業行動開示評価委員会事務局、日本監査役協会コーポレート・ガバナンス有識者懇談会委員などの公式職務はじめ、製造・金融・大手建設：運輸・エネルギー・サービス等各種業界企業の発展を攻めと守りのリスクマネジメントを通して支援。 一橋大学CFO教育センター講師（2015～）、日本内部統制研究学会会長(2016～) 株式会社双日社外監査役（2017～）、株式会社村田製作所社外取締役（2018～）
新井　崇之 シニアコンサルタント	大学・大学院にて会計学及びリスクマネジメントを専攻し、大学院卒業後、プロティビティ入社。 プロティビティ入社後はERM推進プロジェクトに従事し、大手メーカーのERM導入や日系企業のPMI支援を経験。 財務報告に係る内部統制の構築・評価プロジェクトにも従事し、新規事業の内部統制構築及び評価を担当。 リスク管理ツールの導入支援プロジェクトでは、内部監査やSOX対応の高度化・効率化に寄与するなど、リスクマネジメント分野で幅広い経験を有している。

protiviti®
Face the Future with Confidence

1. はじめに

本日のセッションの目的と目次

- 経営に寄与するリスク管理のポイントをご理解頂くこと
- 取締役会がリスク管理において果たすべき役割をご理解頂くこと
- 今後のリスク管理の高度化の方向性をご理解頂くこと

	項目	時間
1	はじめに	5分
2	事業環境の変化とリスク	50分
3	経営に寄与するリスク管理	20分
休憩		15分
4．チームディスカッション		40分

	項目	時間
5	取締役会がリスク管理において果たすべき役割	30分
6	まとめとQ&A	20分

protiviti

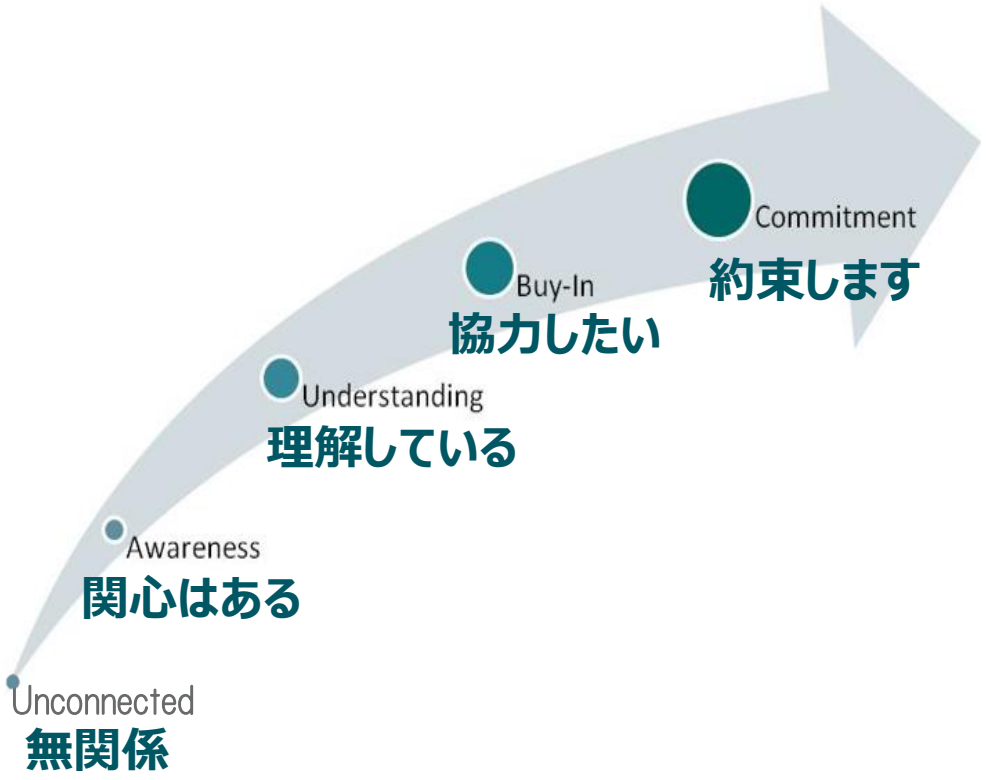
protiviti®
Face the Future with Confidence

2. 事業環境の変化とリスク

質問（1）全社的リスク管理への関心について

現時点の皆さんの全社的リスク管理（ERM）に対する理解や関心度合いはどの程度でしょうか？

1. あまり馴染みがない
2. これから学習してみたい
3. 基本事項は理解している
4. 活用を検討したい
5. 積極的にさらに活用したい

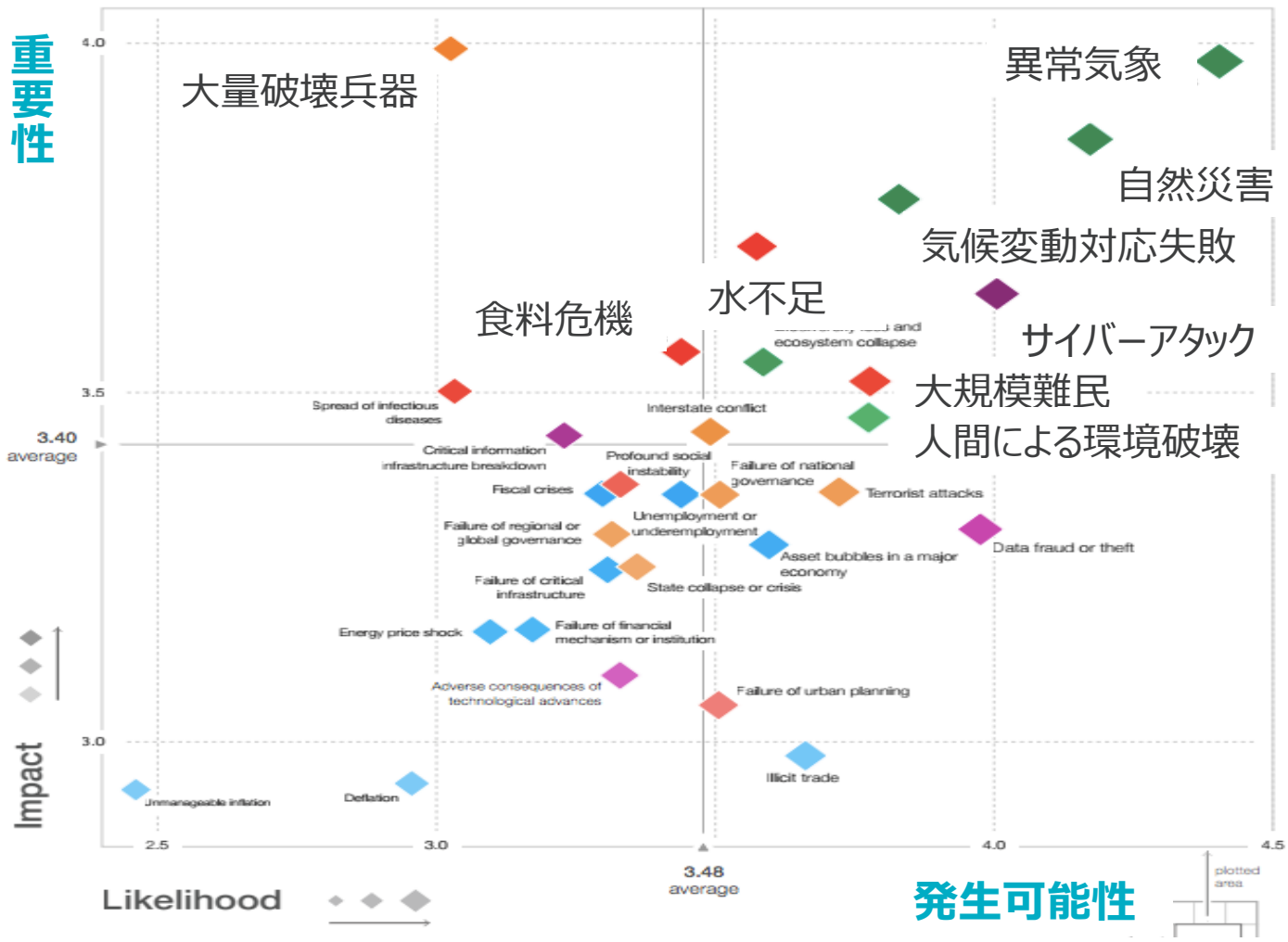


protiviti

ダボス会議　2018　リスクレポート

今後10年の発生可能性と負のインパクトについて、世界経済フォーラム専門家メンバー999名へのアンケート調査

Figure I: The Global Risks Landscape 2018



経済

環境

地政学的

社会

テクノロジー

protiviti

ダボス会議　トップ5リスク　～過去10年推移～

ビジネス環境に重要な影響を及ぼすリスクは大きく変化し続けている

2008年から2018年の10年間のトップ5の重要リスクの変化

出所：World Economics Forum 2018 Global Risks Reports

- ✓ **環境、社会やテクノロジー**のリスクが、さらに重要となる
- ✓ **ESG、SDGsへの関心**が益々高まり、企業の成長と共に**誠実性**が問われる
- ✓ **警告：**AI、ブロックチェーン、バイオなど**新たなテクノロジー**は、**既存のバリューチェーンを破壊**しかねず、この変化に対応できない企業は**現在の競争優位性を著しく失う**と警告している

protiviti

一般的なメガトレンドと想定される巨大リスク

メガトレンド※から、企業経営に与える影響という観点で大型リスクをまとめました

	経済	地政学	環境	社会	テクノロジー
メガトレンド	• 大国による“自国中心主義”化 • 経済力のメガシフト • 中国バブル崩壊リスク • 次の金融危機に対する各国当局の対応不全リスク	• EU分断による影響拡大 • 中東での関係国勢力確保競争 • 国家vs非国家（ISなど）の新対立構造の拡大 • 大量破壊兵器の開発・使用の脅威	• 資源の制約、エネルギー問題の深刻化 • 地球受容力の限界（温暖化、CO2排出増加） • 食料不足、農地の減少、水資源の争奪	• 先進国と新興国の間の格差縮小と各国の「国内格差」拡大が同時進行 • 人口爆発と人口減少の2極化進行 • 先進国での人口老齢化 • データ不正と情報漏洩の頻発	• スマート化の進展 • ナノテクノロジー、医療・ライフサイエンス分野におけるイノベーションの急激な進歩 • サイバー攻撃の常態化と影響の深刻化
巨大リスク	• 世界的不況の到来 • 大国の保護主義政策などにより通商リスクが世界的に拡大 • 資産価値の崩壊リスク • 中国、インドなどの野心的企業の急速なグローバル化、それに伴う市場支配地図の変化	• 新オイルショックの勃発 • 軍事衝突がもたらす世界経済への悪影響	• コスト構造の劇的変化（調達、オペレーション）	• 社会や市場の変化に柔軟に対応できない企業の凋落 • 企業ブランド、レピュテーションの毀損	• 現状破壊的ビジネスモデルの出現 • サイバー攻撃によるオペレーションへの甚大な影響 • 新興国企業による先進国企業からの知的財産の盗用と、それを利用した市場参入

出所：Protiviti、世界経済フォーラムや、国内のシンクタンク等の公表情報をもとにProtiviti作成

protiviti

ESGとSDGs

- ESG：Environmental、Social、Governanceの頭文字を合わせた言葉。投資判断材料として、定量的な財務情報だけでなく非財務情報であるESG要素を考慮する投資を「ESG投資」という。
- SDGs：2030年までに貧困撲滅や格差の是正、気候変動対策など国際社会に共通する17の目標が達成されることを目指した枠組み。

ESGの要素

SDGs(Sustainable Development Goals:持続可能な開発目標)

※年金積立金管理運用独立行政法人（GPIF）HPよりProtiviti加工

protiviti

近年注目されるESGリスクへの対応（1/2）

ESGリスクを管理するにあたり、ESGリスクの特徴を認識し、それらの特徴に応じた管理の仕組みを構築する必要があります。

ESGリスクの特徴

- ESGリスクの評価と優先事項付けは、**定量化が難しい**ことや、ESGリスクに関する知識不足などが原因で、他のリスクの特定よりも難しい傾向にある
- マクロ的で、複雑であるため、より予測が難しく、**長期的**なリスクである
- 過去に顕在化していないリスクであれば、**過去のデータに基づく評価は難しい**
- 低減や排除は難しく、リスクの顕在化への対応として、**レジリエンス**を高める必要がある（危機管理計画・事業継続計画高度化、シナリオ策定の活用、等）

出所：COSO ERM-Executive-Summaryをもとにプロティビティ作成

protiviti

近年注目されるESGリスクへの対応（2/2）

ESGリスク管理活動の概要と、顕在化の早期察知、および顕在化したリスクへの適切な対応を実現させるために重要なポイントを整理しました。

	対応すべき事項
Plan	• 自社に影響を与えかねない**ESGリスクを特定** • ESGリスクに対して**リスクオーナーを割当** • リスクオーナーが、**リスク指標（KRI)**およびリスク顕在化時の**対応計画**を策定
Do	• 指標に基づき**モニタリング**を実施 • リスクの**閾値を超過**した場合には、意思決定者に報告し、必要に応じて見直し
Check	• ESGリスク及びリスク指標が妥当かを**定期的検証**
Act	• 定期的検証に基づき、必要に応じて**見直し**

特に重要なポイント

① 特定したESGリスクに対してリスクオーナー（責任部門）を割り当て、リスクの顕在化状況を示す指標を設定し、リスクの顕在化状況を常にモニタリング

効果：
✓モニタリングデータの蓄積から顕在化の兆候をより高い精度で分析できる

② モニタリングから得られた最新動向をふまえリスク顕在化時の対応計画策定

効果：
✓リスクオーナーがモニタリングと対応計画の策定の双方を担当するため、常に移り変わるリスクの動向が織り込まれた対応計画が用意できる

出所：COSO ERM-Executive-Summaryをもとにプロティビティ作成

protiviti

質問（2）会社の目標達成に影響する不確実性について

皆さんの企業グループの経営戦略に影響を与える外部および内部における不確実性は、この３年で、どの程度変化した、とお考えでしょうか？

1. 激変した
2. かなり大きく変化した
3. これまでと同程度で変化した
4. 多少変化した
5. 変化していない

そもそもリスクとは　～発想の転換～

語源：ラテン語のRisicare「勇気をもって試みる、あるいは挑む」

よくあるリスク分類

ⅰ）　**結果系分類：**自然災害などによる損害をベースにした、いわゆる怖いもの（保険リスク）

ⅱ）　**リスク管理の成果系分類：**

「報われるリスク」：投下経営資源より成果が大きくなる）

「報われないリスク」：いかに努力しても損失のみが発生するもの）＊

ⅲ）　**源泉系分類：**外部・内部要因からみたリスクの源泉に焦点を当てるもの

ⅱ）の例：

- 戦略策定や企業買収などにおける事業上の意思決定に係るリスクはまさに、しっかり対応すればコストを上回る成果が期待できる**「報われるリスク」**
- 会社法の「損失の危険」や、金商法の「財務報告に係る虚偽記載リスク」は、本来自律的に取り組むべき課題だが、法制化されたことから他律的なものと捉えることで、“やらされ感”が強く、できて当たり前という感覚もあり、その意味でも**「報われないリスク」**

- **リスクとは怖いものであり「報われないリスク」との“思い込み”に捉われない**
- **「報われるリスク」にも焦点をあて、リスク管理がコストドライバーではなく、戦略達成に貢献する、強力で頼もしいバリュードライバーであることにも注目**
- **「報われるリスク」への対応は、リスクの結果ではなく、源泉に焦点を当てる**

＊前者を純粋リスクまたはアップサイドリスク、後者を投機リスクまたはダウンサイドリスクとすることもある

源泉系のリスクサーベイ　～各国企業のリスク認識～

企業にとって、中長期的な環境変化とその事業への影響を的確に把握し、事業運営に反映していくことが課題となっています。

今年	前年	分類	リスク
1	4	戦略	**ビジネスモデルを大幅に変更しなければ、破壊的な技術革新や新規テクノロジの急激な進展が競争力やリスク管理能力を上回る**
2	9	ガバナンス	**変化に対する抵抗が、必要な調整の妨げとなる**
3	3	外部環境	サイバー攻撃の脅威を管理する準備が十分にできていない
4	2	外部環境	法規制の変更・規制当局の監視が、事業モデルへの影響を高める
5	8	ガバナンス	組織の文化が、戦略達成に著しく影響を与えかねないリスクについて、適時の識別や報告を促進するものではない可能性がある
6	6	戦略	後継者や有能な人材の確保が事業目的の達成を制限する
7	5	業務	情報セキュリティの保護に、かなりの資源投入を必要とする
8	1	外部環境	市場の動向が、成長の機会を著しく妨げる
9	7	外部環境	グローバルな金融市場のボラティリティが、重大な課題となる
10	10	業務	顧客のロイヤルティの保持が、嗜好変化等により難しくなりつつある

- ノースキャロライナ州立大学とプロティビティによる年次調査（2017年秋）
- マクロ経済、戦略・業務リスクに関して、700名超の経営者（55%：米国、45%：EU・アジア）を対象
- かっこ内は前年順位とリスクの大分類

- 背景色青：**報われるリスク**
- 背景色赤：**報われないリスク**

protiviti

事例：大手メーカー　～リスクの定義の見直し～

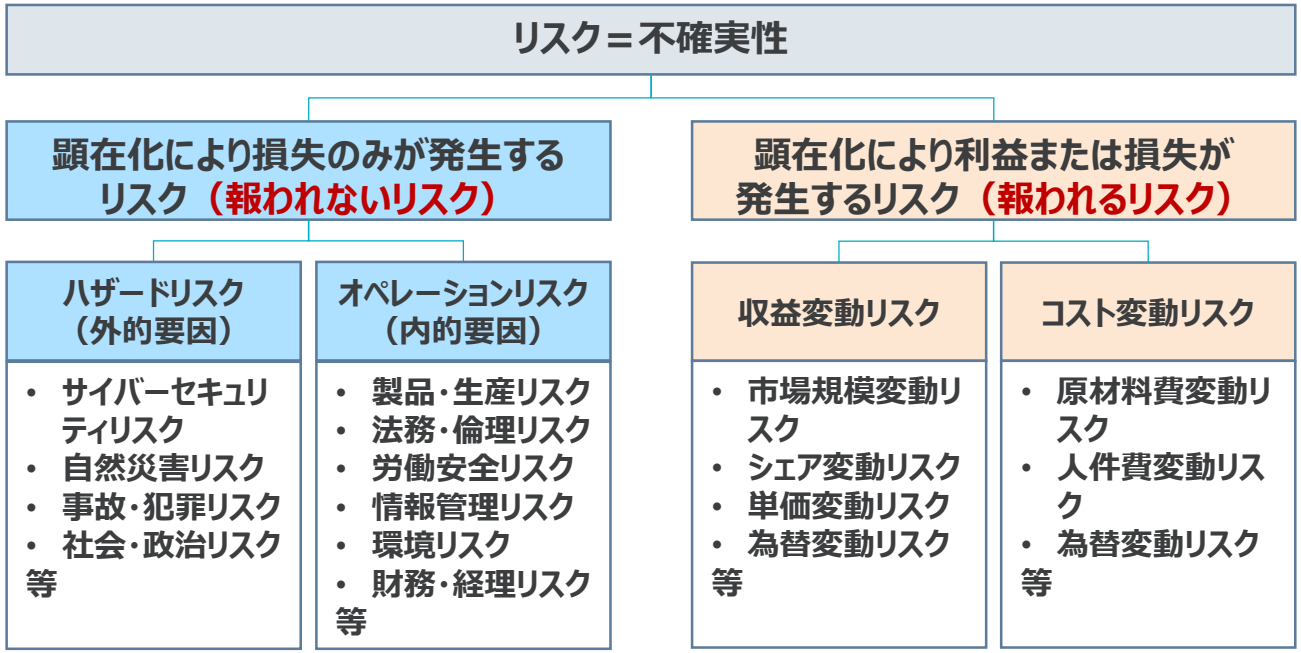
リスクを損失に繋がる可能性として捉えるだけでなく、収益を生む可能性も含めた不確実性として捉え、攻めと守りの両面でのリスク管理を推進しています。

持続的成長を支える仕組み構築
- グループを通して、統一的視点で評価・最適な経営資源配分の実現や経営戦略とリスク管理の整合性確保等を通じた持続的成長を支える仕組みとしてERM構築へ着手した。

持続的成長を支えるERM構築を推進を実施中

【実施状況】

リスクを不確実性と捉え、損失だけでなく、収益を生む可能性のある事象を捉え、持続的成長につながる仕組みを構築しようとしている



【洞察】

市場および法的な価格変動を受けやすく、新規ビジネス領域が台頭してきた業界であるため、マイナスだけでなくプラスの側面のリスクの確実な刈り取りを目指している

protiviti

我が国のコーポレートガバナンスコードにおけるリスク

- 取締役会の役割として、「**経営陣幹部による適切なリスクテイクを支える環境整備**を行うこと、独立客観的立場から経営陣・取締役の実効性の高い監督を行うこと」（基本原則4）

- 「取締役会は、**内部統制やリスク管理体制を適切に整備**すべきである。」（原則4－3(3)）

- 「**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リスク管理体制の整備**は、適切なリスクテイクの裏付けとなるが、取締役会は、これらの体制の…の監督に重点を置くべきであり、個別コンプライアンスの審査に終始すべきではない」（補充原則4－3④）

CGコードのポイント：

- リスクテイクを支える環境整備、独立した立場からの**経営陣・取締役に対する実効性の高い監督、内部統制やリスク管理体制の適切な整備とその運用の有効性の監督、**を取締役会の役割とし、これは2010年から米国でスタートした**リスクオーバーサイト*そのもの**

- コンプライアンスなど、**「報われないリスク」**という**守り**を対象にしている一方で、「先を見越したリスク管理体制」など、**「報われるリスク」**の**攻め**も含められている。

＊．SEC規則により、株主総会招集通知にリスクマネジメントにおける取締役会の役割を記載するというもので、攻めのリスクテイクと守りのリスク管理に関する取締役会の役割が具体的に開示。

質問（3）リスク管理について

皆さんにとってリスク管理とは何でしょうか、
皆さんの印象に最も近いのは次のどれでしょうか？

1. 災害等を含むすべての脅威から組織を守る仕組み
2. 会社法の内部統制システムと同義
3. 戦略実現を後押しするという意味で、コーポレートガバナンスと同義
4. 不正行為を予防する仕組みで、コンプライアンスと同義
5. リスクへの５つの対応（活用・受容・軽減・転嫁・回避）を考慮し、戦略実現の確からしさを高める仕組み

不確実性、リスク、ERMについて

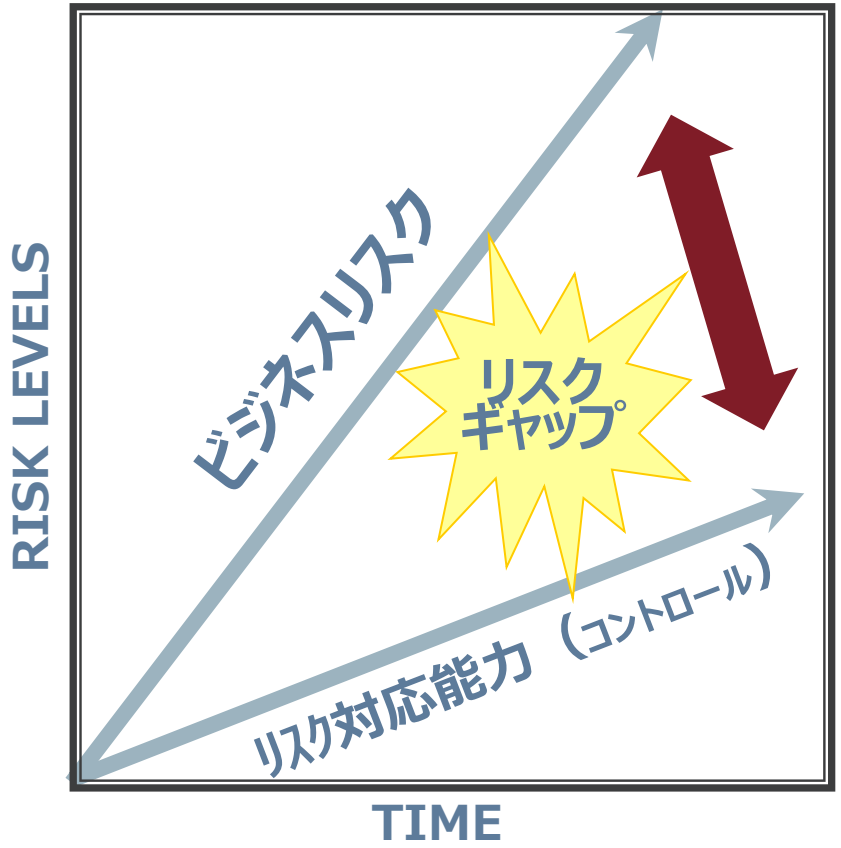
～新COSO･ERMフレームワーク2017より～

- **全ての企業**は、ステークホルダーに価値を提供する過程で**「不確実性」に直面**する
- **「不確実性」**とは、まだ知られていないこと
- **「リスク」**とは、戦略および事業目標の達成に影響を与える「不確実性」「可能性」
  「The possibility that events will occur and *affect the achievement of strategy and business objectives.」（*2004モデルでは、adverselyが入っていた）
- **経営とは**、どの程度の「不確実性」、つまりどの程度の「リスク」を受け入れ、いかに対応するかであり、受け入れるリスクと期待される成果・企業価値をバランスさせること。
- **ERMとは、「組織体が、価値を創造し、維持し、実現する過程において、リスク管理のもとで策定された戦略の遂行と統合された、組織文化と能力と実践である。」**
  「The culture, capabilities, and practices, integrated with strategy-setting and its execution, that organizations rely on to manage risk in creating, preserving and realizing value.」

★　組織が価値を創造し、維持し、実現する過程で、リスクを適切に管理できるか否かは、戦略策定や戦略の実行において組み込まれた、**組織文化とリスク対応能力**にかかっている

リスクギャップと対応能力

- 変化増大するリスクに必要な**経営インフラ（リスク対応能力）**が追いつかないと**リスクギャップ**（残存リスク)が大きくなる
- グループを通して、リスク管理・内部統制の**共通のフレームワーク**を強化し**共通言語を浸透**させる必要がある
- 内部統制とは、受け入れたリスクの発現を**経営者のリスク許容度の範囲内に抑える**ことを目的としたプロセス



では、現在の経営管理システム（リスク管理・内部統制）で、経営者が期待する成果を確実に上げられるという自信はどの程度あり、その根拠は何か、という問いにどう答えるか？

経営インフラの成熟度を高める

（例えば、JSOX、会社法内部統制システムはレベル3）

protiviti

ガバナンス・ERM・内部統制の関係 ～2013年COSO内部統制フレームワークより～

✓**ERMは、ガバナンスに包含**
（鍵は客観性と独立性）
✓**内部統制は、ERMに包含**

ERMフレームワークは、
✓**目的と戦略を設定**
✓**機会と脅威**(不確実性)を特定
✓**リスク選好（攻め）と**
リスク許容度（守り）を設定
✓**リスクポートフォリオ**を考慮

✓ 内部統制は、**経営者のリスク許容度の範囲内に収まるようコントロールを設計**
✓ 内部統制は、5つのリスク対応戦略(活用・受容・転嫁・軽減・回避)の内、**リスクの軽減**に貢献

出典：COSO

企業目的 → 戦略 → リスク → 内部統制

protiviti

リスクマ管理によくある課題

1. リスク管理活動の範囲が限定的

- 情報セキュリティ等の報われないリスクの特定テーマに限定されている
- リスク評価結果が経営者の意思決定に反映されていない
- 事業計画策定とリスク管理活動が連携していない

2. 個別最適の積み上げ

- 事業部門毎や機能毎に活動が行われ、全社横断的な視点が欠如している
- 他部門のリスク対応や経験等が共有されない
- 未検討部分や境界領域のリスク把握の仕組みが不足し、重要リスクが網羅されない

3. モニタリングが必要にして十分なレベルではない

- 全社的な取り組み状況（特に海外拠点）を同じ軸で把握・評価できない
- 活動にダブりがあり、現場が疲弊している
- 内部監査部門が、全社的リスク評価を監査計画に活用していない

日本企業のリスク源泉　～2016年度有報分析より～

【33業界／FY2016】

日本企業も外部環境リスクを中心に
多岐にわたるリスク源泉を意識している

3543 社

v.3

A 外部環境リスク		
★ 1	競合他社	8548
★ 2	顧客ニーズ	2290
★ 3	技術革新	1136
4	外部環境への感応度	4767
5	投資家の信頼	1080
6	出資者の動向	356
7	資本調達	2385
8	政体の安定性	1372
9	外交関係	83
10	関連法規	1444
★ 11	法令改変	21458
12	規格変更	263
13	業界特性	567
14	地域特性	3031
15	商慣行	184
★ 16	金融市場	6462
★ 17	災害・壊滅的損失	12903
★ 18	気候変動	1634
19	少子高齢化	928

B 業務プロセスリスク		
(a) 財務		
1. 価格		
20	金利変動	2738
21	為替変動	6172
22	投資持分の価値変動	577
23	商品相場変動	362
24	金融商品変動	1206
2. 流動性		
25	資金不足	707
26	機会損失	140
27	手元流動性	0
3. 与信		
28	債務不履行	3082
29	取引先集中	130
30	決済未了	400
31	担保価値損失	54
(b) 権限委譲		
32	リーダーシップ不全	19
33	統制不足	214
34	アウトソーシング統制	881
35	勤務評価基準	0
36	変化への順応性	1114
37	縦・横の組織内コミュニケーション	150
(c) 情報処理/IT		
38	データの完全性	327
★ 39	情報セキュリティ	10958
40	サイバー攻撃	2415
41	情報の可用性	2930
42	情報技術のインフラストラクチャ	1573
(d) ガバナンス		
43	組織文化	19
★ 44	企業倫理・社会的責任	546
★ 45	取締役会の実効性	615
46	後継者計画	345
(e) 評判		
47	イメージ／ブランド	5311
48	投資家とのエンゲージメント	17
(f) 誠実性		
★ 49	経営者による統制環境	0
50	従業員による個人的利得不正	30
51	第三者による不正	199
52	役職員による違法行為・訴訟	10525
53	無権限者による経営資源の使用	0
(g) 業務/運営		
★ 54	顧客満足	1255
★ 55	人的資源・資質	3944
56	知的資産の維持活用	2783
★ 57	製品開発力	914
★ 58	業務効率	1038
59	生産能力	3863
60	取引拡大への対応能力	6
61	期待パフォーマンスとのギャップ	1188
62	過失	663
63	サイクルタイムにおける業務効率	345
64	サプライチェーン	8571
65	流通チャネルの機能不全	1500
66	提携先・外部委託先の内部統制	1165
67	広義のコンプライアンス	2275
68	特定の経営資源への依存	386
69	製品・サービスの欠陥	5827
★ 70	環境への負荷・対応	2786
71	健康・安全管理	3066
72	労務問題	1256
73	商標・ブランド劣化	0

C 意思決定情報リスク		
(a) 戦略		
★ 74	外部環境モニタリング	71
★ 75	ビジネスモデルの陳腐化	226
76	ビジネスポートフォリオ	172
77	投資判断情報	2339
78	減損	744
★ 79	組織構造の戦略整合性	0
80	業績評価指標の戦略整合性	0
★ 81	経営資源の最適配分	2094
82	戦略策定の実効性	1402
83	製品ライフサイクルを考慮した戦略	105
(b) 外部報告		
84	財務報告の虚偽記載	121
85	会計基準・見積もり	938
86	財務報告の内部統制有効性評価	255
87	開示統制の整備運用	7
88	税務戦略情報	2203
89	年金基金情報	0
90	監督機関への報告	32
(c) 業務/運営		
91	予算・計画統制	138
92	価格設定	4878
93	契約履行情報	1754
94	業績評価指標の有効性	0
95	事業目標の戦略整合性	0
96	財務業績偏重による経営管理	0

★ ダボス会議とプロティビティ・ノースキャロライナ州立大学調査のトップリスク

protiviti

日本企業のリスク管理・内部統制の課題と対策

1．リスクを取り巻く最近の課題

- **ガバナンス**（取締役会等）における**リスクオーバーサイト**強化要請
- **リスクテイクを支える環境整備と企業価値向上**への関連性の説得力
- **ESG、SDG s** など、サステナビリティ対応へのリスク管理強化要請
- 個別リスク管理では対処しきれない事態、不祥事が多発

2．リスク管理・内部統制の目的の明確化とグループ展開

- グローバル展開におけるグループ一体のリスク管理の成熟度向上
- 戦略実現を支える内部統制　＝　**目的　➡　戦略　➡　リスク　➡　内部統制**

3．リスクの定義の拡大と共通言語・フレームワーク化

- **リスクの定義**、全組織を通じての共有と**共通認識、合意形成**
  - ➢**戦略・事業目標に影響を与える可能性または不確実性**
- **リスク選好**と**リスク許容度の可視化、見える化**
- **それぞれの企業固有の全社的なERMフレームワークを構築**

従来のリスク管理と目指すべきリスク管理

従来のリスク管理

- 自社や他社で発生した事件や事故の再発防止と対処を実施
- 事業計画とリスク管理は独立
- ハザード系リスクに焦点を当てた管理

戦術的／事務的
過去の視点
個別最適

- 個々の担当部門や機能毎に対応

狭い視野

- 既知のリスクや法規制に対応するリスク管理を導入

受動的
年1回の評価

- 組織機能の視点でリスク管理が導入され、機能毎に責任者や管理者を設置

機能重視

- 個別のリスク管理活動の中で年一回の評価を実施

ボトムアップの対応

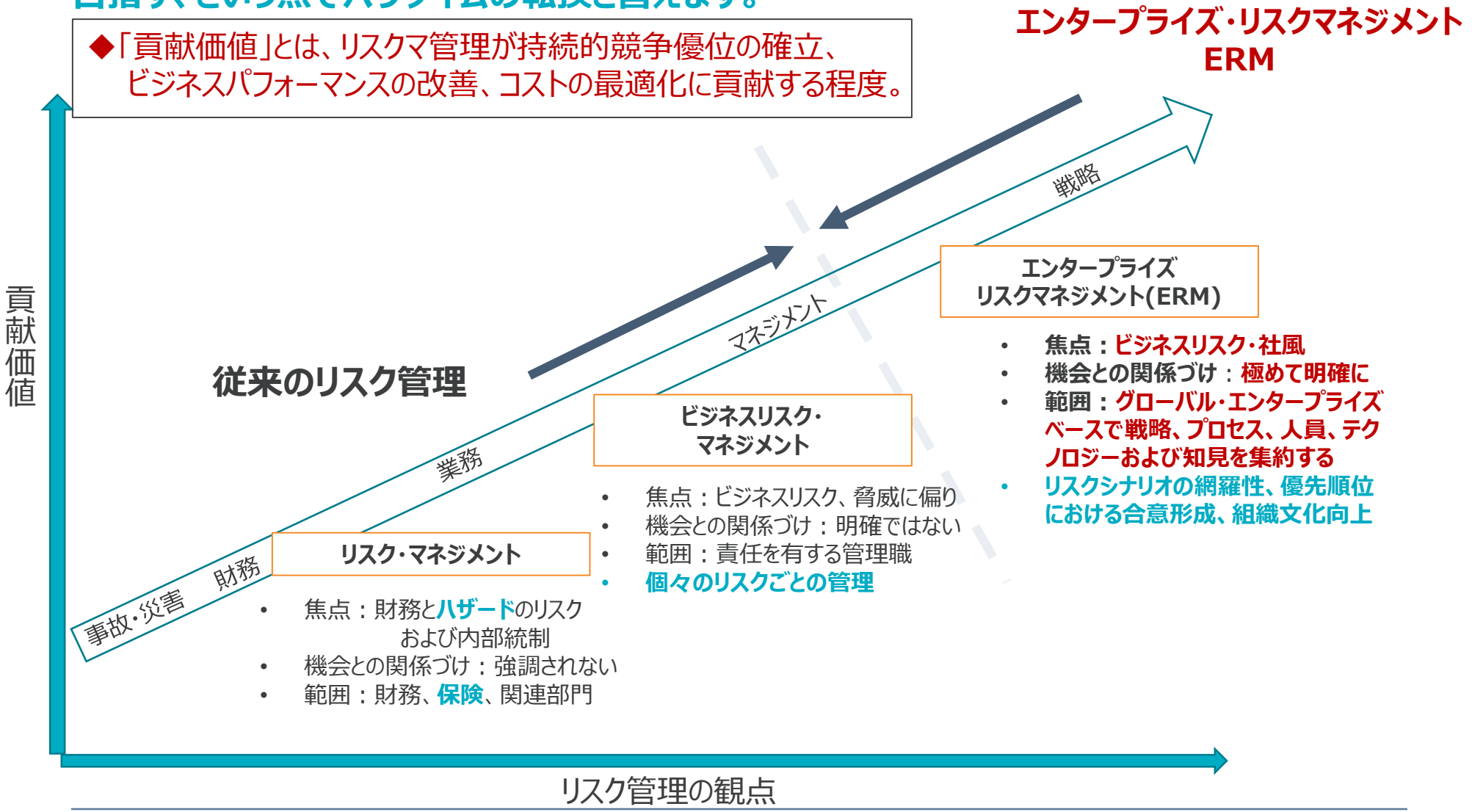
目指すべきリスク管理（全社的リスク管理：ERM）

戦略的	**戦略達成を支援するリスク管理**
将来の視点	**戦略達成を阻害する要因をリスクとして対処**
全体最適	**事業に関わるリスク全般が管理の対象**
広い視野	事業や機能の壁を越え、**グループ経営の視点からリスクを特定・評価し、対処**
能動的	**経営視点で主体的にリスク管理を推進**
継続的な評価と取組	**戦略の策定からモニタリングまでのプロセスと連動**
プロセス重視	**リスク管理プロセスを標準化**し、プロセス単位で対応すること
組織的説明責任	継続的モニタリングと内部監査部門のリスクアプローチ監査を組合わせ、リスク管理の有効性を評価すること

従来のリスク管理とERMは何が違うのか

ERMは、従来の保険を意識したリスク管理とは異なり、報われるリスクをも含み持続的成長を目指す、という点でパラダイムの転換と言えます。

◆「貢献価値」とは、リスクマ管理が持続的競争優位の確立、ビジネスパフォーマンスの改善、コストの最適化に貢献する程度。



protiviti

質問（4）貴社のリスク管理について

**貴社のリスク管理は、従来の伝統的な取組みですか、
それとも新たなERMに近い発想で取り組みを進めていますか？**

1. どちらかと言えば伝統的な取組みである
2. 新たなERM的な発想を取り込みつつある
3. ERM的な発想で推進している

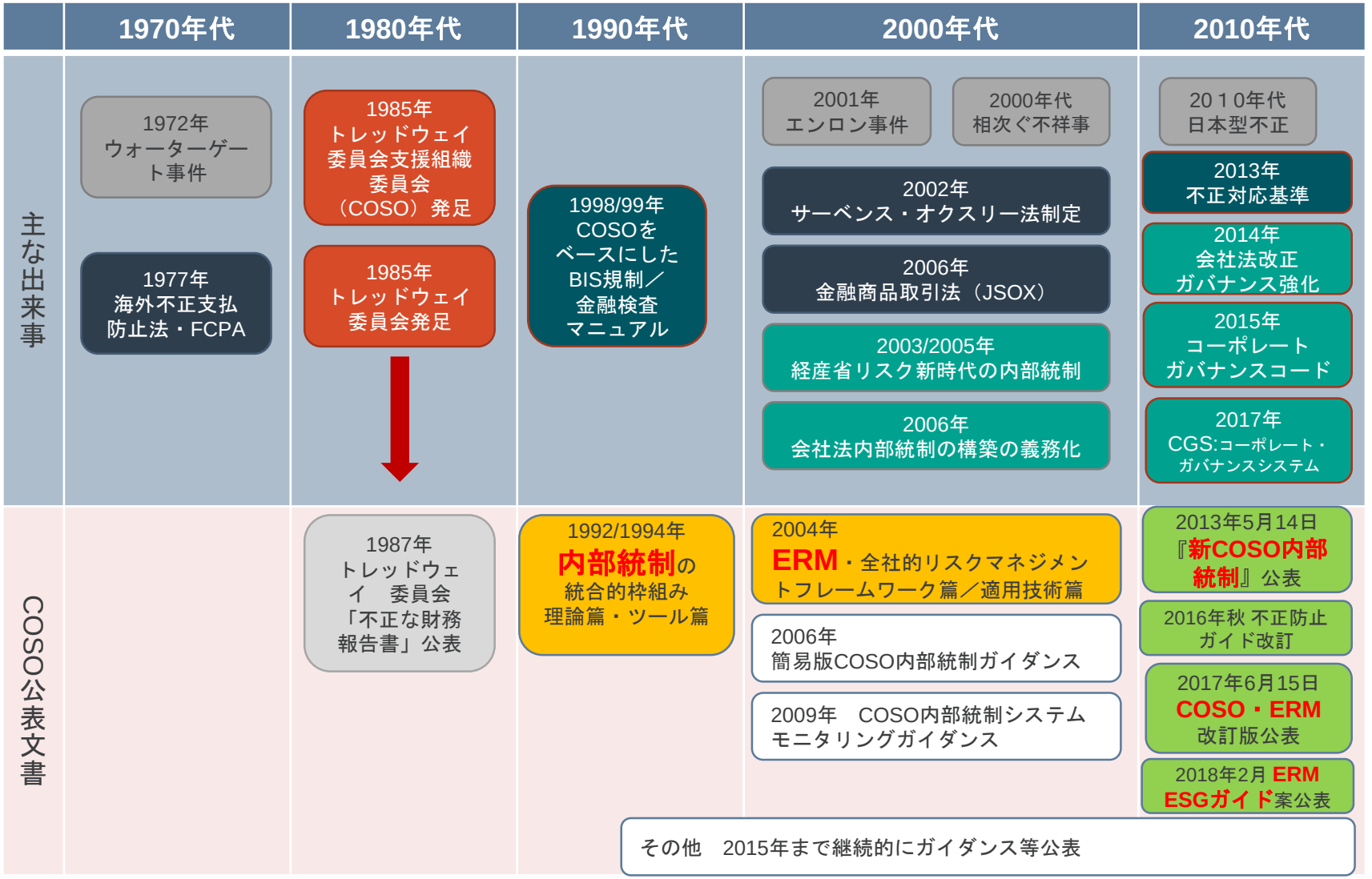
（参考）新COSO ERMの概要

COSOについて…

60万人以上
のプロフェッショナル

- **COSOは、1985年に, 5つの民間団体の共同プロジェクトとして設立され、全社的リスクマネジメント、 内部統制、および不正の抑止に係るフレームワークやガイダンスを開発し、この分野における第一人者として貢献してきている。**
- **COSOの基本的な考え方:**
  すべての組織の長期的な成功には、効果的なリスクマネジメントと内部統制は不可欠である。

不祥事、グローバル規制、COSOフレームワークの動き



protiviti

COSOERMフレームワークを改訂した主な理由

- ERMのコンセプトや**実務が進化**したこと
- **教訓**から学んだこと
- 全社的リスクマネジメントに関する**期待値が上がった**こと
- 主として**テクノロジーの発達**により、グローバルな規模で、ビジネスや業務環境がいっそう**複雑化**したこと
- ステークホルダーが一層関心を持ち、より明確な**透明性と説明責任**を求めている
- **取締役会におけるリスクに関する議論～リスクオーバーサイトの重要性**が高まってきている

2017年　改訂COSOERMの特徴

- リスク、戦略、パフォーマンスの整合性をより明確に説明するため、「COSOキューブ」ERMは、新しい“DNA”グラフィックに変更。5要素・20原則の採用。
- 目的－戦略－リスク－内部統制の関係を明示。ガバナンスとカルチャーの重視。

ERM統合的フレームワーク
（2004年）

戦略目的にフォーカス

代替的なリスク対応を扱う

リスクの回避, 保有, 共有、低減

ERMと戦略・パフォーマンスとの統合
（2017年）

リスクの**活用**、回避, 保有, 共有、低減

protiviti

環境変化に対応するCOSOの動き~5要素・20原則

新COSO-ERMは、ERM実現に必要な要素を提示しています。

2017年の改訂版COSO ERMの5つの構成要素と20の原則	
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。 2. 業務構造を確立する。 3. 望ましいカルチャーを定義づける 4. コアバリューに対するコミットメントを表明する。 5. 有能な人材を惹きつけ、育成し、保持する。
戦略と目標の設定	6. 事業の環境を分析する。 7. リスク選好を定義する。 8. 代替戦略を評価する。 9. 事業目標を体系化する。
パフォーマンス	10. リスクを識別する。 11. リスクの重大度を評価する。 12. リスクの優先順位付けを行う。 13. リスク対応を実行する。 14. ポートフォリオの視点を持つ。
レビューと見直し	15. 持続的な変化を評価する。 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改善を遂行する。
情報、伝達と報告	18. 情報とテクノロジーを活用する。 19. リスク情報に関する伝達を行う。 20. リスク、カルチャーおよびパフォーマンスを報告する。

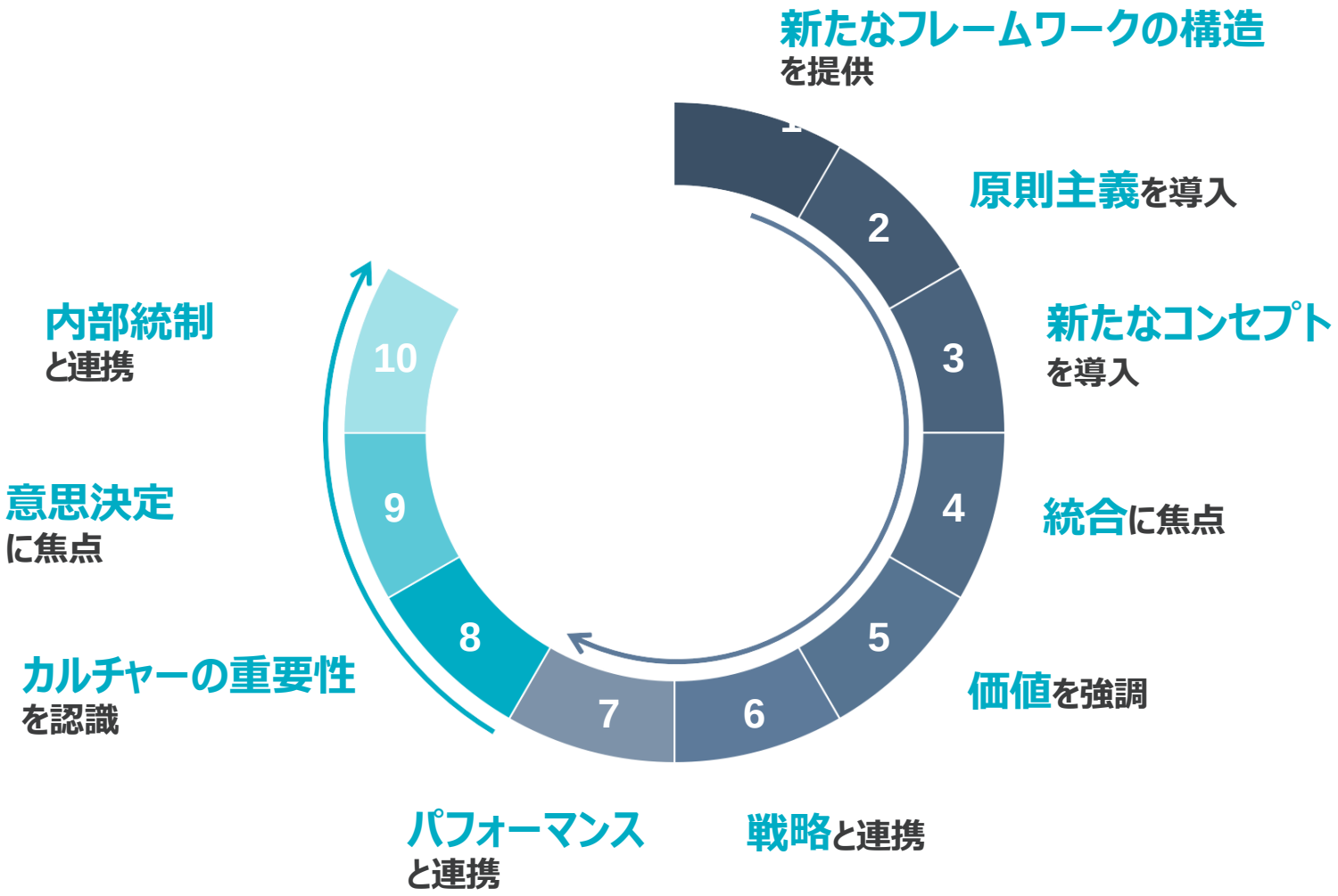
主なポイント

- ✓ リスクと戦略、パフォーマンスの整合性がより重視されている
- ✓ ERMの高度化には、適切なカルチャーの醸成とテクノロジーの活用が不可欠である
- ✓ リスク監視が取締役会の重要な役割として定められている
- ✓ リスク選好とリスクキャパシティの把握によって、代替戦略の評価が可能となる

出所：COSO

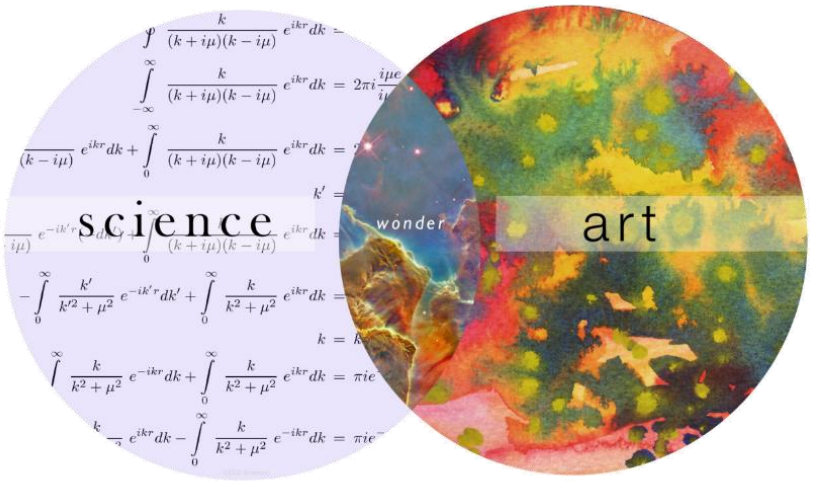
protiviti

改訂COSO ERMフレームワーク…



protiviti

COSO ERMの重要な前置き…



1. リスク（可能性）に関して、COSOの理解としては、

   アート（芸術）＆サイエンス（科学）を基にした選択

   が現代の市場経済の核にあるとしている。

2. 目的の達成に向けての**すべての選択にリスク（可能性）**が存在する。
3. 日々の業務の意思決定から、**取締役会での根本的なトレードオフの判断**に至るまで、これら選択における**不確実性と常に向き合う**ことは組織活動の一部である。
4. 最適の選択を行うには、リスクを特定し、優先順位を付け、**経営力に照らして最終判断を行う。**
5. 判断・意思決定の根拠となる**戦略上のオプション情報が的確**なのかどうか、どの程度信頼できるものなのか、その確信度合いを認識したうえでの、判断・意思決定となる。
6. 意思決定情報の信頼度合いを高め、**戦略の実現の確からしさを高める経営手法がERM**である。
7. 確信度合いが低いとしても、状況によっては最後に、**トップの英断を仰ぐ**ことが必要なこともある。

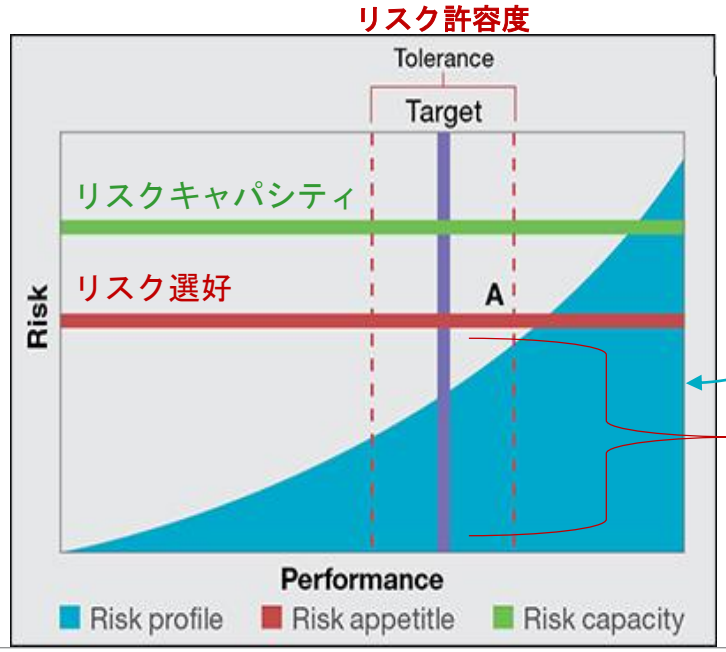
protiviti

パフォーマンス：リスク選好と許容度

戦略を策定し代替案を検討する際に、戦略に内在する二律背反を考慮。
代替戦略にはそれぞれのリスクプロファイルがあり、戦略から生じる影響を見極める。

パフォーマンス（目標）と、リスクプロファイル
の関係は以下のとおりです。

- ✓ **パフォーマンス目標**が変動すると、リスクも変動する。
- ✓ **リスクプロファイル**（青カーブ）は戦略と目標に対するパフォーマンスレベルとリスク想定量から導かれる。
- ✓ 経営者は**リスクプロファイル**を評価して意思決定する
  - リスク量が**リスク選好の範囲内**であることを確認
  - パフォーマンス変動が**許容度の範囲内**であると確認
  - パフォーマンスが**リスクプロファイルと交わるA地点**が許容度の右側の限界点として設定するのが最適
- ✓ 組織は**リスクキャパシティ**を超えてリスクを取ることが求められることがある。



ERMは、戦略選択を強化します。戦略選択は、構造的意思決定を必要とします。
意思決定とは、リスクを分析し、経営資源を組織のミッションとビジョンに整合させることです。

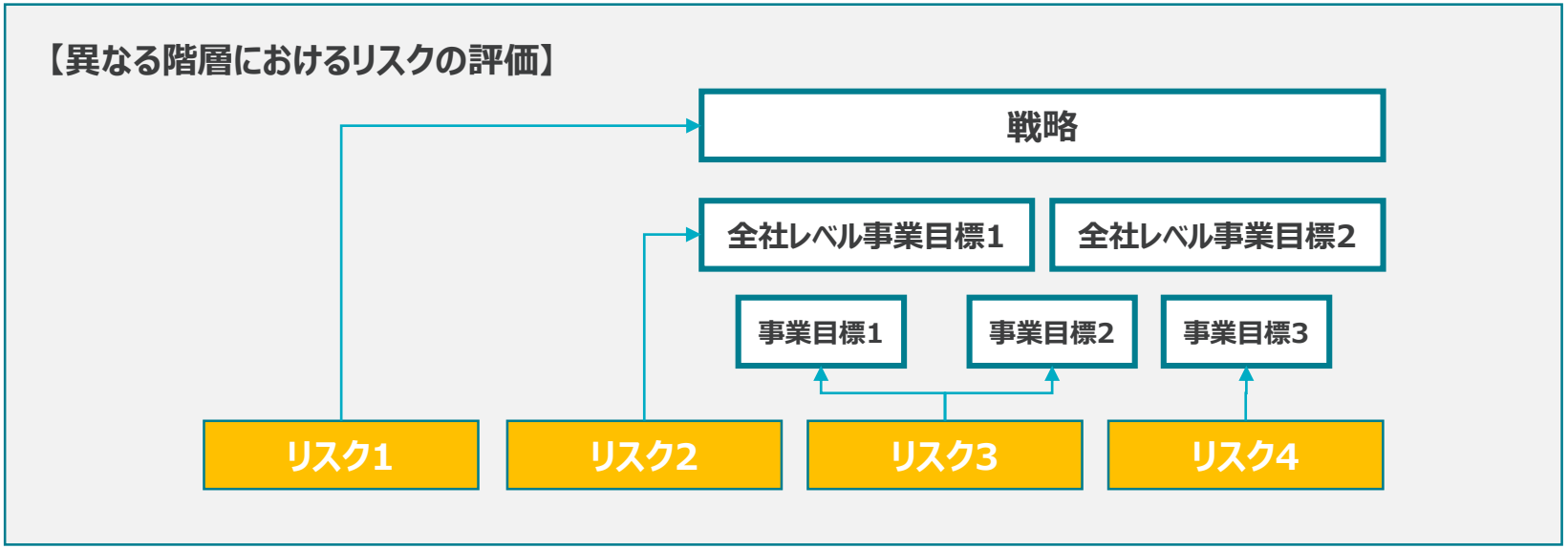
（注）各点のプロットは、定量的アプローチでも定性的アプローチでも可能である。 戦略又は事業目的に関して十分なデータを持っている場合、確率モデル、回帰分析などの定量的なアプローチが可能である。データが十分ではない場合や、事業目的がそれほど重要ではない場合には、インタビュー、ファシリテーション・ワークショップ、ベンチマーキングなどの定性的なアプローチが用いられる。

出所：新COSO-ERM

protiviti

事業体の異なる階層での網羅的なリスクの特定と評価

- ✓ リスクの洗い出しは、組織の異なる階層におけるリスクを対象とし全組織にて把握し整理する（例）
  - ➢ リスク１：戦略に直接影響を及ぼすもの
  - ➢ リスク２：全社レベルの事業目標に影響を及ぼすもの
  - ➢ リスク３：複数の個別事業目標に影響があり、全体として全社レベルの事業目標に影響があるもの
  - ➢ リスク４：一つの個別事業目標には影響ないが、全社レベルの事業目標に影響があるもの
- ✓ リスクの重大度は、事業目標に沿って複数の階層（事業部門、機能および業務ユニット）で評価
- ✓ 標準化されたリスク用語と分類を使用することで、組織のすべての階層でリスクを評価するのに役立ち、業務ユニット・事業部門および機能にわたる共通のリスクをグループ化することができる



例：　「トップダウン」の事業体全体のリスク評価では、リスク4は重大度が低いと評価されるかもしれないが、業務ユニット階層の評価ではリスク4は、より重大度があると考えられるため、重大度は高くなる可能性がある
リスク評価を完了させるために、トップダウン評価はより低い階層で識別・評価されたリスクを考慮する必要がある

protiviti®
Face the Future with Confidence

3. 経営に寄与するリスク管理

企業活動におけるリスク管理の全体像

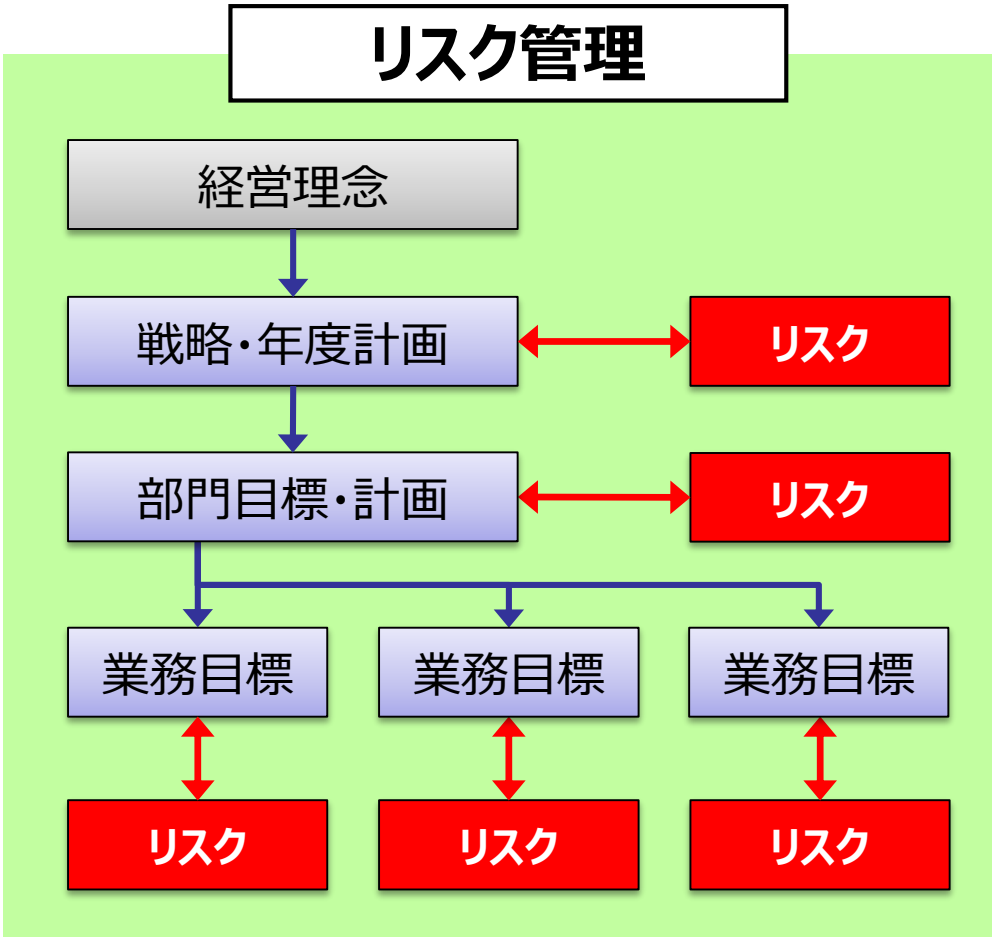
- 各階層における戦略・目標に対してリスクが存在する
- 各階層におけるリスクをいかに管理するかがポイント

「企業の姿勢」が基本

- ビジョン・バリュー
- 企業理念
- リスク管理体制
- リスク管理の枠組み等

「予防と発見」が基本

- 職務分掌
- 手作業のIT化
- 承認手続き
- 有事の対応等



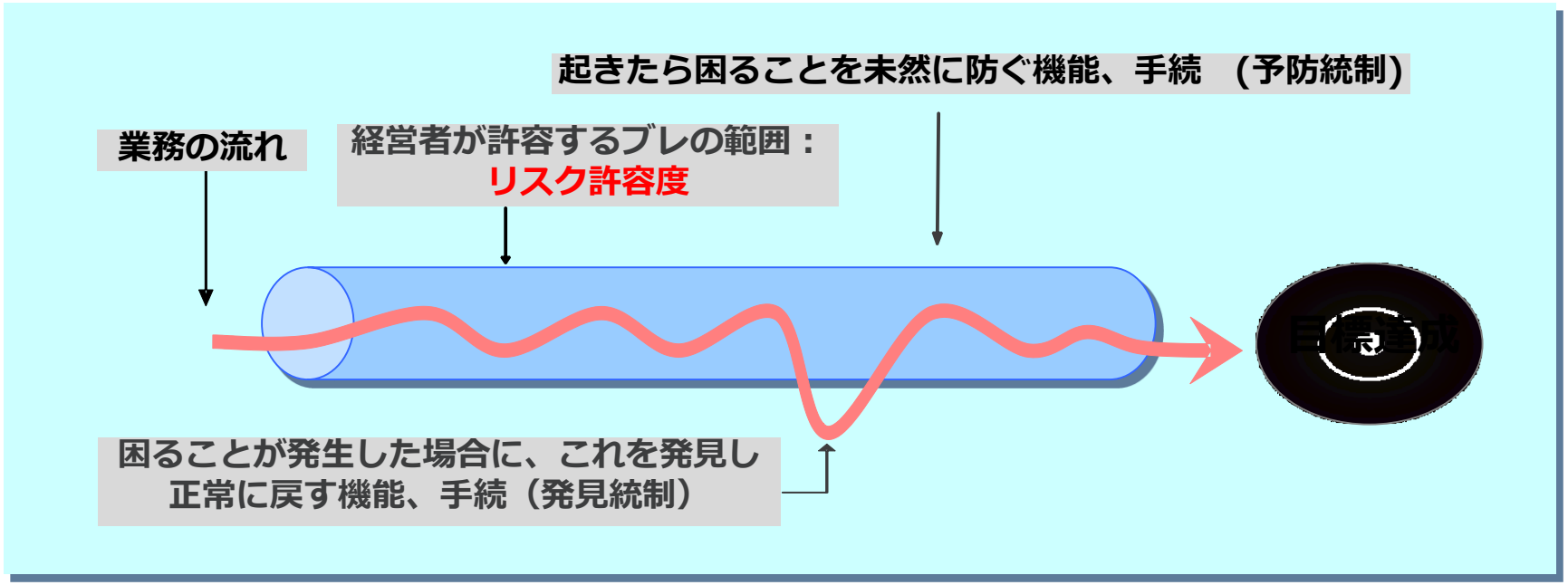
protiviti

リスク対応：内部統制の基本 “予防と発見”

内部統制とは、目標を達成するためのPDCA活動を行う上で

- ◆ 起きたら困ることを起こさないための機能・手続（予防）
- ◆ 困ることを速やかに発見し正常に戻すための機能・手続（発見）（回復）

をビルトインして、継続的に維持・改善する活動の総称です



protiviti

リスク管理の基本は「企業の姿勢」と「共通言語」

- リスク管理を有効に機能させるには**「企業の姿勢」"魂"**が基本
- **「企業の姿勢」**とは、経営層のTone at the Top、取締役会、執行役員、監査役等、管理者、現場の複合的姿勢
- 激変する環境下では、それぞれの姿勢は同じではないという前提に立つ必要がある
- 企業の姿勢を組織の隅々まで反映させるには、先ず経営層と管理者層との間でトーンを合わせることが大切
- トーンを合わせるには、**「リスク管理の共通言語」を構築し、浸透させること**が必要不可欠
- 「リスク管理の共通言語」とは、**経営理念やありたい姿、リスク管理の目的・方針・役割・リスクの評価・リスク対応・コントロール手続、コミュニケーションの仕方、モニタリング方針などの総称**

共通言語を活かした全社横断的なリスク対応　～食品メーカーの事例～　1/4

中期経営計画に対する重要なビジネスリスクとして特定された品質リスクについて、全社の共通言語を設定するなど全社横断的なリスク評価・対応を実施し、リスクを低減しています。

品質リスクマネジメント

- 中期経営計画で想定されるビジネスリスクについて、全役員インタビューにより、品質リスクに対する管理能力レベル（現在と将来）を評価した結果、全社的に優先的に取り組むべき重要リスクとして、品質リスクを特定した。

品質管理活動の強化を実施

主に品質に関して、「共通言語の設計」「評価軸の設計」「業務プロセスの設計」を実施した。

1．共通言語の設計

品質に関するリスクを定義し、品質に関してカバーする範囲を明確化

2．評価軸の設計

品質リスクの評価軸を整備し、全社共通の基準で評価を実施

3．業務プロセスの設計

品質リスクへ対応するための業務プロセスを整備し、リスク対応を標準化

【ポイント】

- ◆ それまで曖昧であった品質リスクに関する共通言語を全社横断的に設定した
  例）品質リスク、品質事故など
- ◆ 品質事故と業務プロセスの関係を体系化
- ◆ 品質リスク管理に関する自社としての評価基準を設計した
- ◆ リスク情報を戦略的意思決定に活用し、成果を上げた
- ◆ 以来、重要な品質事故は皆無

共通言語を活かした全社横断的なリスク対応　～食品メーカーの事例～　2/4

中期経営計画に対する重要なビジネスリスクとして特定された品質リスクについて、全社の共通言語を設定するなど全社横断的なリスク評価・対応を実施し、リスクを低減しています。

1．共通言語の設計

【品質リスク】
「品質事故」による、社会的信用や市場占有率の低下、経営コストロス等を招くリスク

【品質事故】
「社内」次工程の品質管理業務への悪影響、「不適合品」、取引先・消費者苦情等の発生事実

【不適合品】
規格・基準に逸脱した原材料・仕掛品・半製品・製品・商品

【社内外区分】
A社が出荷コントロール可能な配送パートナーまでが社内
（A社資産管理下にある商品を取り扱う関連会社およびこれに準ずる契約配送業者まで）

共通言語を活かした全社横断的なリスク対応～食品メーカーの事例～ 3/4

中期経営計画に対する重要なビジネスリスクとして特定された品質リスクについて、全社の共通言語を設定するなど全社横断的なリスク評価・対応を実施し、リスクを低減しています。

2. 評価軸の設計

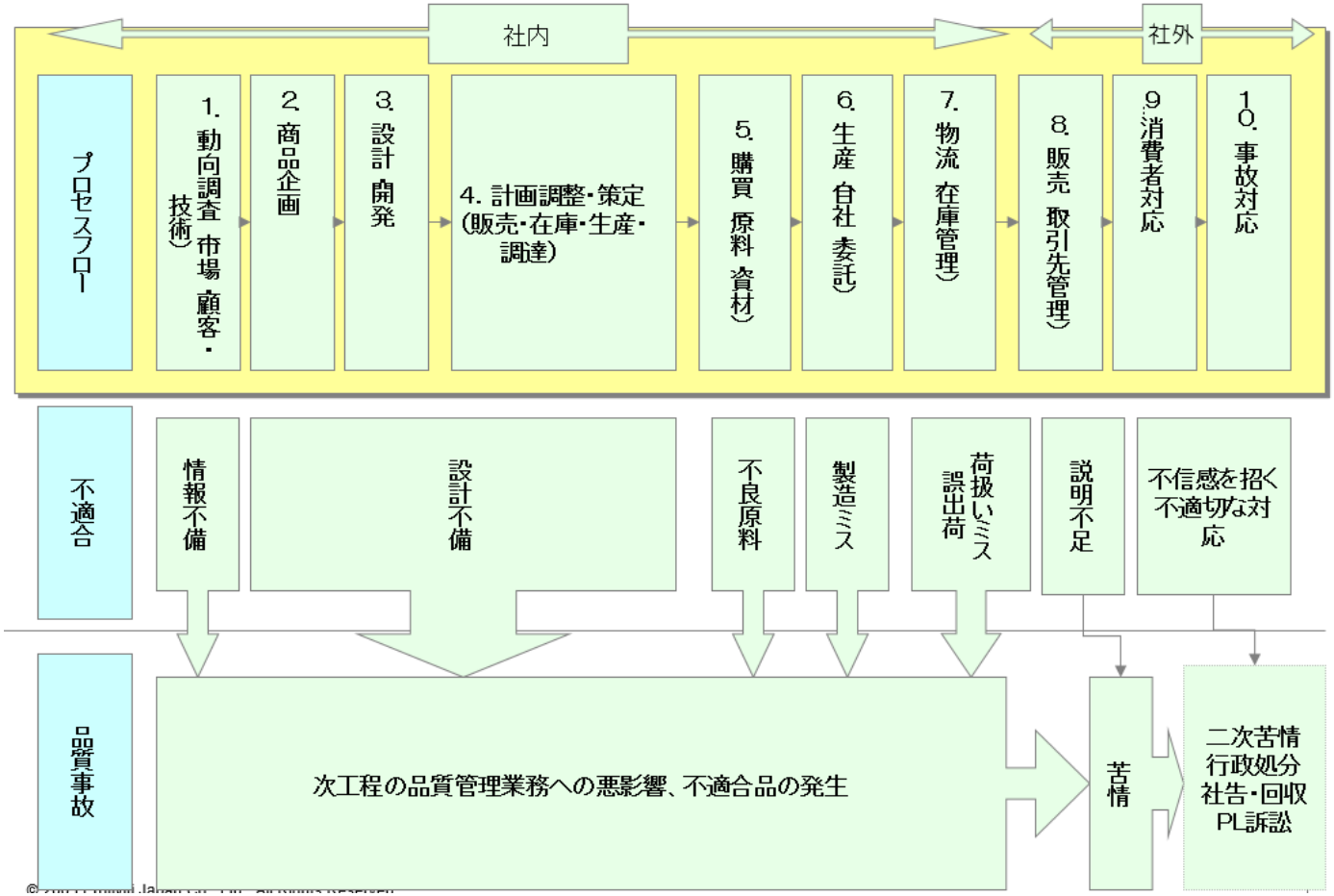
ランク	内　容
5	週に１回以上（日常レベル）
4	月に１回以上
3	毎年１回以上
2	５年に１回以上
1	３０年に１回以上（阪神淡路大震災レベル）

ランク		不具合の程度		
		社会的信用力	マスコミ・取引先	厚生行政
5	全面回収	大きく失墜	ネットマスコミ報道	回収命令行政指導
4	小売・店頭在庫回収			自主回収改善指導
3	卸在庫回収	低下	店頭の商品撤去	立入調査
2	出荷停止(回収せず)			保健所届出のみ
1	個別対応	殆ど影響なし	消費者苦情	

共通言語を活かした全社横断的なリスク対応　～食品メーカーの事例～　4/4

中期経営計画に対する重要なビジネスリスクとして特定された品質リスクについて、全社の共通言語を設定するなど全社横断的なリスク評価・対応を実施し、リスクを低減しています。

3．業務プロセスの設計



protiviti

従来のリスク管理と目指すべきリスク管理

従来のリスク管理

- 戦術的／事務的
  - ・自社や他社で発生した事件や事故の再発防止と対処を実施
  - ・事業計画とリスク管理は独立
  - ・ハザード系リスクに焦点を当てた管理
- 過去の視点
- 個別最適
- 狭い視野
  - ・個々の担当部門や機能毎に対応
- 受動的
  - ・既知のリスクや法規制に対応するリスク管理を導入
- 年1回の評価
- 機能重視
  - ・組織機能の視点でリスク管理が導入され、機能毎に責任者や管理者を設置
- ボトムアップの対応
  - ・個別のリスク管理活動の中で年一回の評価を実施

目指すべきリスク管理（全社的リスク管理：ERM）

戦略的	戦略達成を支援するリスク管理
将来の視点	戦略達成を阻害する要因をリスクとして対処
全体最適	事業に関わるリスク全般が管理の対象
広い視野	事業や機能の壁を越え、**グループ経営の視点からリスクを特定・評価し、対処**
能動的	**経営視点で主体的にリスク管理を推進**
継続的な評価と取組	**戦略の策定からモニタリングまでのプロセスと連動**
プロセス重視	**リスク管理プロセスを標準化**し、プロセス単位で対応すること
組織的説明責任	継続的モニタリングと内部監査部門のリスクアプローチ監査を組合わせ、リスク管理の有効性を評価すること

protiviti

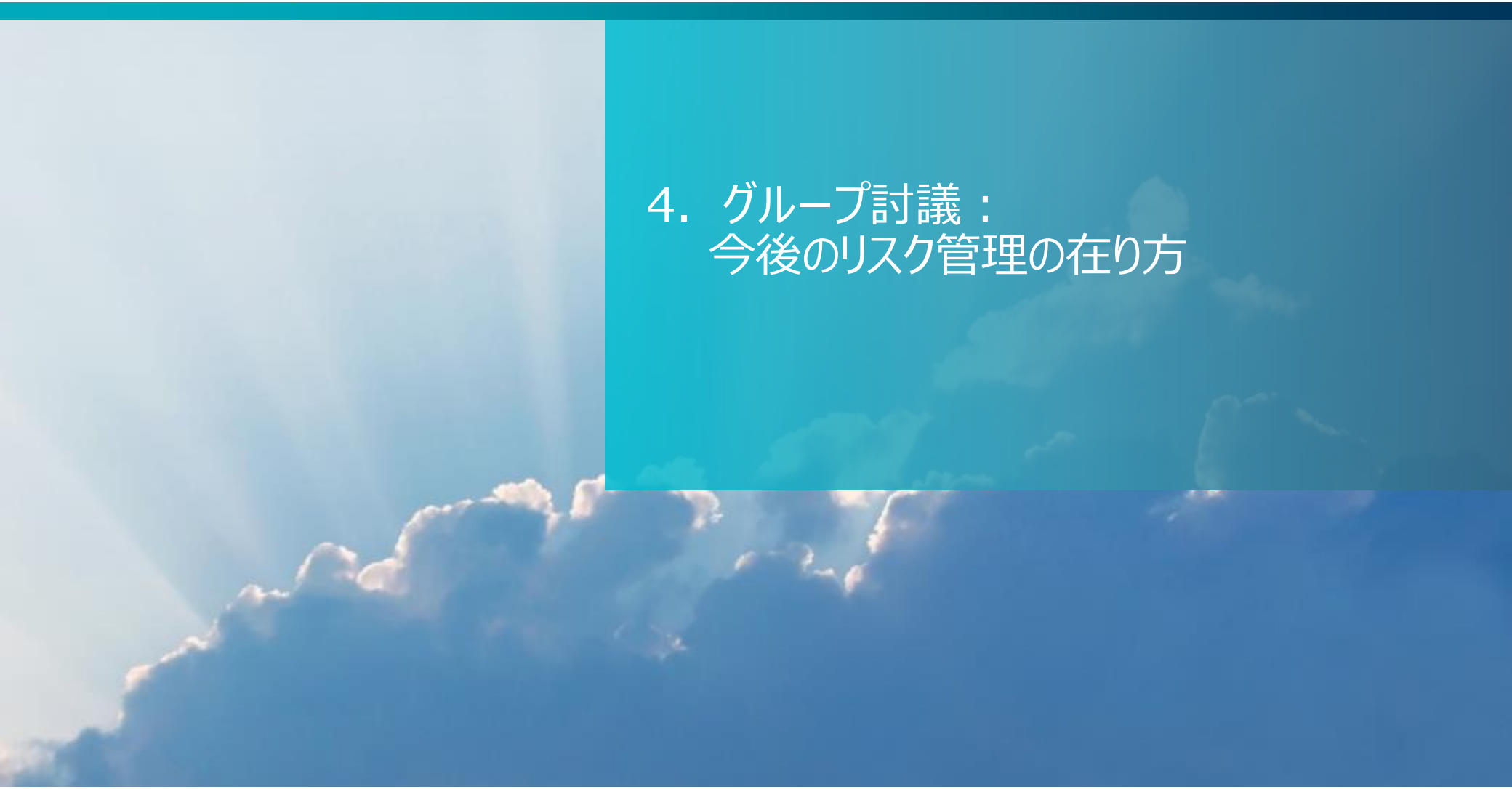
質問（５）10年後のありたい姿の実現に向けて必要な仕組み

皆様の企業の10年後のありたい姿の実現に向けて、リスクに関連して、特に必要と感じられる仕組みは以下のうちどちらでしょうか？

1. 損失回避（脅威）の視点だけでなく、目標達成のための機会も踏まえたリスクを特定するための仕組み
2. 経営の意思決定に必要なリスク情報を経営陣に適時に提供するための仕組み
3. 全社最適・全社横断的なリスク対応を実現するための仕組み
4. リスクに対する対応状況を把握するための仕組み

protiviti

protiviti®
Face the Future with Confidence



4. グループ討議：
今後のリスク管理の在り方

リスク管理高度化に向けた今後の取り組み案

翌期年次計画策定に戦略達成のためのリスク情報を盛り込むことができるよう、以下の取り組みを検討する。

従来のリスク管理	目指すべきリスク管理（全社的リスク管理：ERM）	
戦術的／事務的	戦略的	戦略達成を支援するリスク管理
過去の視点	将来の視点	戦略達成を阻害する要因をリスクとして対処
個別最適	全体最適	事業に関わるリスク全般が管理の対象
狭い視野	広い視野	事業や機能の壁を越え、**グループ経営の視点からリスクを特定・評価し、対処**
受動的	能動的	**経営視点で主体的にリスク管理を推進**
年1回の評価	継続的な評価と取組	**戦略の策定からモニタリングまでのプロセスと連動**
機能重視	プロセス重視	**リスク管理プロセスを標準化**し、プロセス単位で対応すること
ボトムアップの対応	組織的説明責任	継続的モニタリングと内部監査部門のリスクアプローチ監査を組合わせ、リスク管理の有効性を評価すること

今後の取り組み案

① ありたい姿・戦略達成を目的とした事業リスクの定義

② ありたい姿・戦略達成に関する網羅的なリスクを特定のためのリスクモデルの整備

③ リスク管理における役割分担の明確化

protiviti

今後の取り組みイメージ　～①ありたい姿・戦略達成を目的としたリスクの定義～

リスクの定義例

- ●経営リスク：ありたい姿、中期経営計画に影響を与える不確実性
- ●事業リスク：年次計画に影響を与える不確実性
- ●現場リスク：部門実行計画に影響を与える不確実性

protiviti

今後の取り組みイメージ　～②網羅的なリスク特定のためのリスクモデルの整備～

事業に関連する内外の様々なリスクを全社的に、網羅的に特定するためのツール

- リスクの特定をする際、リスクの棚卸表として機能する
- 特定するリスクのレベル感、源泉を意識したリスクの特定に役立つ
- リスク定義を基にコミュニケーションを行うことでリスクに対する共通認識を形成するのに役立つ

外部環境リスク

1.競合他社
2.顧客の意向
3.技術革新
4.外部環境への感度
5.株主の期待
6.資本調達
7.政体の安定性
8.法令改変
9.諸規則改変
10.業界特性
11.金融市場
12.災害・壊滅的損失

業務プロセスリスク

財務

価格
13.利率
14.外国為替
15.投資持分
16.商品相場
17.金融商品

流動性
18.キャッシュフロー
19.機会損失
20.市場の集中

与信
21.債務不履行
22.取引先の集中度
23.決済
24.担保価値

権限委譲

25.リーダーシップ
26.権限・制限
27.アウトソーシング
28.評価基準
29.変化への順応性
30.コミュニケーション

情報処理/IT

31.完全性
32.アクセス
33.可用性
34.インフラストラクチャ

ガバナンス

35.企業文化
36.倫理的行動
37.取締役会の有効性
38.事業承継計画

評判

39.イメージ/ブランド力
40.利害関係者

誠実性

41.経営者の不正
42.従業員の不正
43.第三者の不正
44.違法行為
45.無権限者による使用

業務/運営

46.顧客満足
47.人的資源
48.知的資産
49.製品開発
50.業務効率
51.処理(生産)能力
52.量的拡大への対応
53.パフォーマンスギャップ
54.サイクルタイム
55.外部からの調達
56.流通チャネルの有効性
57.提携先
58.コンプライアンス
59.ビジネスの中断
60.製品・サービスの欠陥
61.環境問題
62.健康・安全管理
63.商標・ブランド劣化

意思決定情報リスク

戦略

64.外部環境のモニター
65.ビジネス・モデル
66.ビジネス・ポートフォリオ
67.事業価値の評価/投資判断
68.組織構造の有効性
69.戦略に基づく実績測定
70.経営資源配分
71.戦略策定
72.製品ライフサイクル

外部報告

73.財務報告の評価
74.内部統制評価
75.経営者の宣誓
76.税務情報
77.年金基金
78.監督機関への報告

業務/運営

79.予算・計画
80.価格設定
81.契約条項
82.業務測定
83目的・戦略との整合性
84.会計情報の偏重

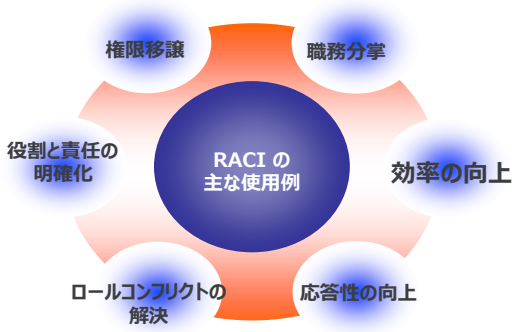
プロティビティのビジネスリスクモデルの特長

- ✓ 特定の業種に依らない**汎用的**モデルとなっており、**網羅的に84のビジネスリスク**を挙げている
- ✓ リスク毎に**リスクのシナリオが定義**されている
- ✓ **結果ではなく源泉を基に整理され**、その後のマネジメント活動に繋げやすい整理となっている
- ✓ 大分類として、**外部環境リスク、業務プロセスリスク**と**戦略と密接に関連する意思決定情報リスク**を持っている

今後の取り組みイメージ　～③リスク管理における役割分担の明確化～

RACIマトリクス

- 組織の責任・役割を整理するフレームワーク
- RACIマトリクスではタスク毎にR（実行責任）、A（説明責任）などを明確にし、役割の偏りや責任者の漏れなどを洗い出すことが可能



R: Responsible（実行責任）　業務の実行責任を担う

A: Accountable（説明責任）　業務について、最終的な説明責任を有する

C: Consult（協業）　業務を実行するにあたり必要な情報や能力を持ち、相談役を担う

I：Inform（報告先）　業務の結果の報告を受ける

		RM委員会	RM委員会事務局	RM各部会スタッフ部門	事業部門子会社	内部監査
リスク分類検討	前年度の結果を受けてリスク分類の見直しを行う	A	R			
リスクアンケート作成	検討されたリスク分類を基にアンケートを作成する	A	R			
リスクアンケート依頼	リスクアンケートの回答を各事業部門子会社に依頼する		R/A			
リスクアンケート回答（子会社向け）	リスクアンケートの設問に回答する		A		R	

protiviti

リスク管理における役割分担事例

<table>
<tr><th colspan="2">対応組織</th><th>事業部門</th><th>所轄部門</th><th>スタッフ部門</th><th>ＲＭ委員会</th><th>内部監査部門</th></tr>
<tr><td colspan="2">役　割
プロセス</td><td>・グループ企業を経営
・自部門の内部統制システムを整備・運用</td><td>・グループ企業を統括
・グループ企業のリスク管理に関する指導助言（リスク担当部門と連携）
・方針等のグループ企業への周知徹底情報提供</td><td>・専門性に基づき担当リスクの基本方針を策定
・担当リスク毎に所轄部門と連携し、グループ企業を支援
・内部統制が有効に機能していることをモニター</td><td>・全社リスクマネジメントに関し、取組み方針を審議
・実施状況をモニタリング</td><td>・グループ企業及び部門に対する監査</td></tr>
<tr><td>P</td><td>・リスク評価
・対応方針</td><td>評価</td><td>評価</td><td>評価</td><td>評価
審議</td><td>監査情報の共有</td></tr>
<tr><td>D</td><td>・対応指示</td><td>リスク対応実行</td><td>連携・共有</td><td>個別リスクのＰＤＣＡ策定</td><td>指示</td><td rowspan="3">監査</td></tr>
<tr><td>C</td><td>・ﾓﾆﾀﾘﾝｸﾞ</td><td>対応状況報告</td><td>ﾓﾆﾀﾘﾝｸﾞ</td><td>ﾓﾆﾀﾘﾝｸﾞ</td><td>ﾓﾆﾀﾘﾝｸﾞ</td></tr>
<tr><td>A</td><td>・改善方針の策定</td><td>改善対応実行</td><td>改善方針の共有</td><td>個別リスク毎に検討</td><td>策定
指示</td></tr>
</table>

チームタスク　：　あるべきリスク管理の在り方

1. ビジネスの変化に的確に対応すべく、変化（或いは無変化）からくる可能性や不確実性をリスクと考えた場合、今後のリスク管理の在り方を検討するとすれば、どのような考え方で、どのようにリスク管理を見直していけばいいか、をチームで議論して下さい（15分）

（検討例）

- リスクの定義を見直す
- 戦略策定時に、攻めと守りのリスクを考慮する
- リスク対応（内部統制）の質を上げてもっと大きなリスクを取る
- リスクの管轄体制とKPIや先行指標のモニタリングを強化する

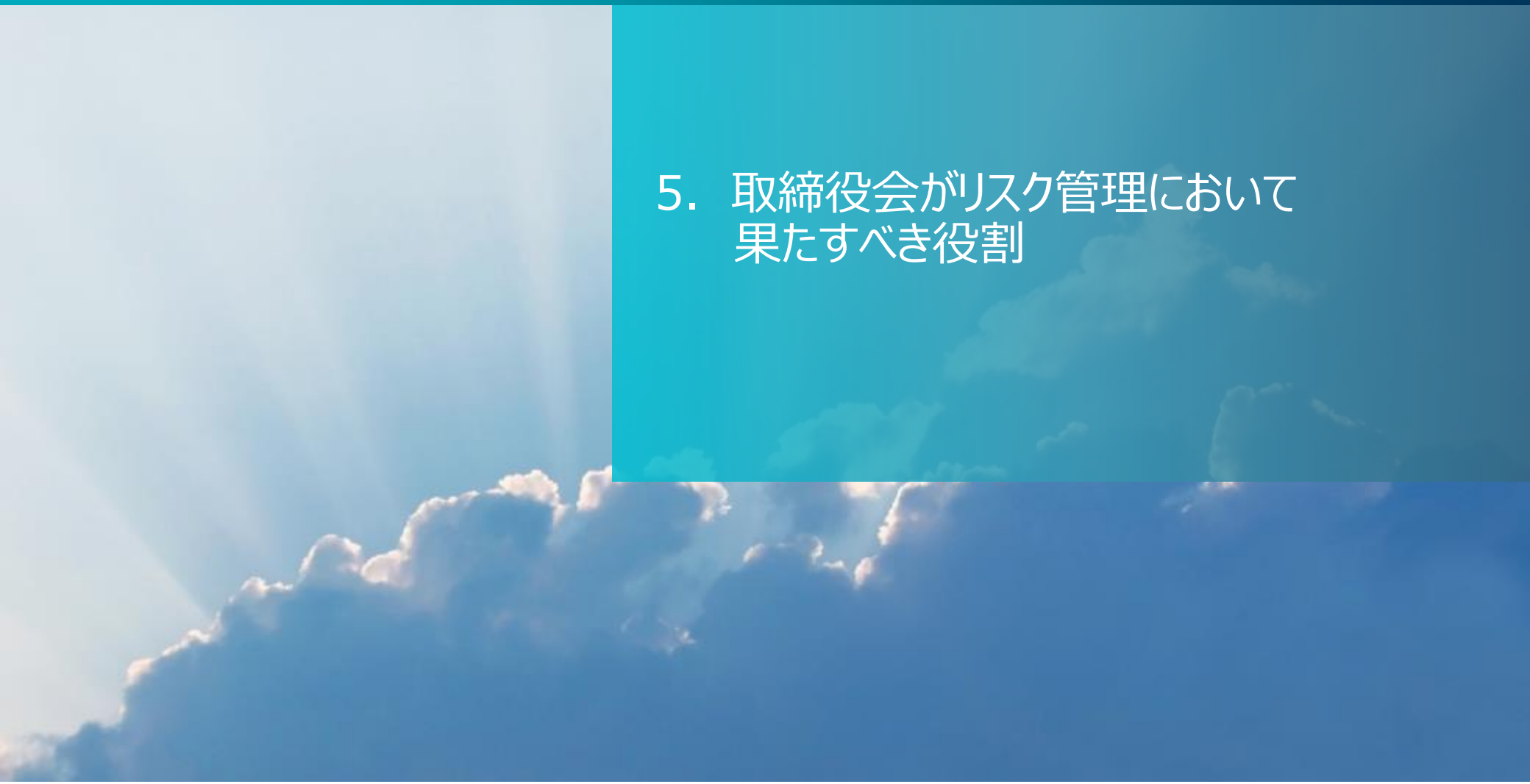
など

2. 協議開始の前に、ファシリテーター、レコーダー、プレゼンターを決めて下さい（1分）

3. チームごとの検討結果を発表して下さい（各チーム２分）

protiviti®
Face the Future with Confidence

5. 取締役会がリスク管理において果たすべき役割



取締役会のリスク監視の10原則

1. 企業の成功要素を理解する
2. 戦略に固有のリスクを評価する
3. リスクオーバーサイトに関する取締役会、監査役、個々の委員会の役割を定義する
4. リスク管理や内部統制システムが適切か、十分に資源が提供されているか、検討する
5. リスク情報に関して、必要なリスクの種類、報告様式について理解するとともに、執行陣と合意する
6. 取締役会、監査役と執行陣で、ダイナミックで建設的なリスクに関する協議を推進する
7. 企業風土とインセンティブ報酬体系におけるリスク要因を注意深くモニタリングしていく
8. 戦略、リスク、インセンティブ報酬への準拠状況の関連をモニタリングする
9. 何が次に来るのか、新たなリスクや派生するリスクに関して検討する
10. 取締役会・監査役のリスク監視の目的が達成されているか、定期的に監視プロセスの実効性評価を行う

米国SEC規則により、取締役会のリスクオーバーサイトに関する役割について、株主総会招集通知に開示が義務付けられている。（2010年より）　会社のリスクマネジメントプロセスの監視に関する取締役会の役割、会社のリスクを理解する上での取締役の資質、および過度の受容しがたいリスクテイクを助長しないようにするための報酬に係る会社の様々な取り決めに関する報酬委員会による評価についての開示を求めています。

取締役会がリスク監視を効果的に推進するには①

取締役会はリスク監視のための体制構築を検討しているか

① リスク管理とは、**リスクテイク（リスク選好）**の方針の下で設定された業務目標や、**リスク許容度**に沿って経営陣が必要なプロセスを遂行する

② リスク監視は、リスク管理プロセスがどのように**整備、運用、評価**されているかを判断する

③ リスク監視の体制、運営の在り方は、企業規模、構造、複雑性、社風、重要リスク等の状況を考慮して、リスク管理委員会等を設置するなど、それぞれの企業で**最もふさわしいリスク監視の在り方**を決めることになる

④ **リスク監視の責任は、取締役会のすべてのメンバーが負う**べきであり、従って取締役会が企業戦略の全体像を把握するには、戦略に伴う重要リスクを把握する必要がある。

取締役会がリスク監視を効果的に推進するには②

識別されたリスクは直面している重要なリスクを反映しているか

① 経営陣が取締役会に提示するリスク情報では、**留意すべき新たなリスク、既存リスク、エマージングリスクのアップデート**などを明らかにすべき

② **「影響大・発生可能性小」リスク**についても、**レピュテーションやブランド**への影響、影響の速度、影響の持続性、企業の対応準備度の観点から優先的に考慮

③ 新規リスクを適時に識別するには、例えば、**戦略の主要な前提**が崩れていないか検討、グローバルトレンドに留意、全く新しい事業を買収するなどの　コアビジネス以外の事業展開による影響を評価、

④ サイバーテロ脅威等、企業の事業戦略を**根底から覆しかねないリスク**を検討

新たなリスクマップ　～重要な逆説シナリオの特定～

リスクシナリオ間の相関性を加味しグルーピングした後で、「影響度」「持続性」「速度」の3軸でシナリオの優先順位を検討します。右上かつ円の大きなシナリオが優先されます。

影響度

●組織の戦略及びビジネスモデルの実行に対して巨大かつ潜在的に破壊的な影響を及ぼす可能性のあるシナリオ

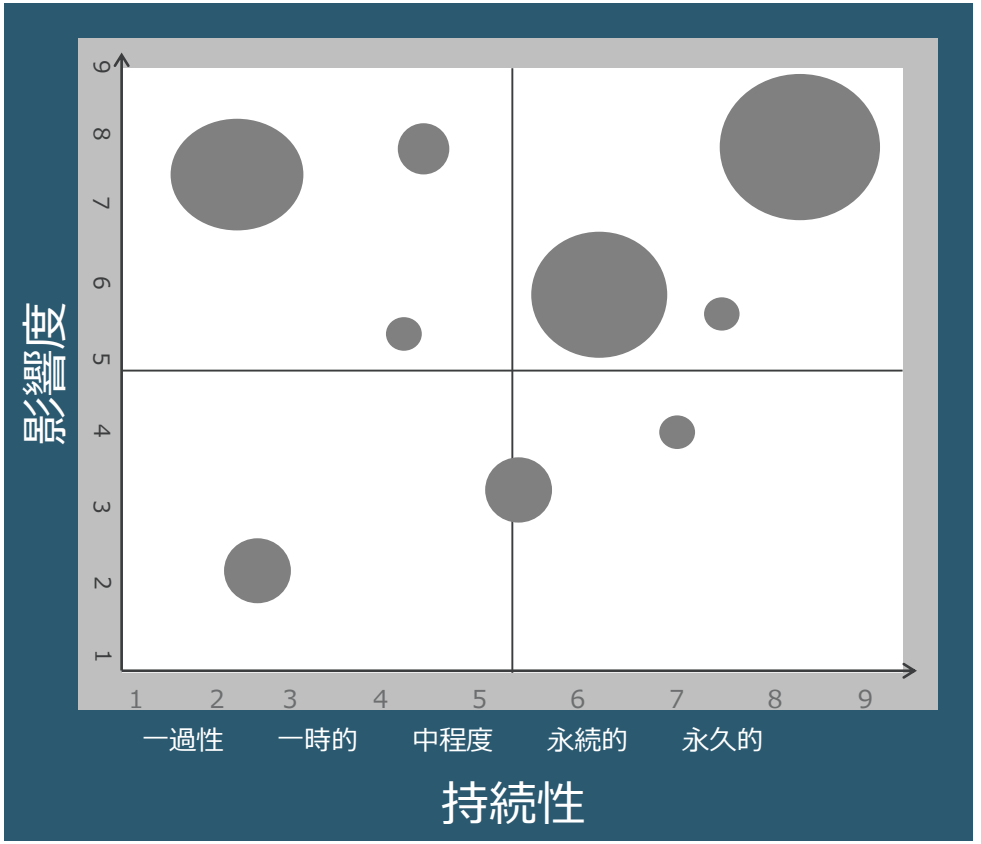
持続性

●指定された期間の間、会社に対して継続的に影響を与えるシナリオ

速度

●組織にとって必要とされる効果的な事業継続計画の迅速な対応案を策定するシナリオ

Illustrative Evaluation of Scenarios



※円の大きさは、シナリオの想定的な速さを表します

protiviti

取締役会がリスク監視を効果的に推進するには③

変容するビジネス環境の中でリスクを効果的に管理できるよう、リスク管理能力を継続的に改善しているか

① 担当部署が**十分なリスク管理能力**を有しているか、**必要な継続的改善**がなされているかを取締役会は確かめる必要がある

② 主要な**全社的リスクを管理・監視する強固なプロセス**が確立されているか、

③ ビジネスの変化速度上昇や複雑化に合わせ**リスク管理能力が改善**されているか

④ **リスク報告が適時かつ信頼性**をもってなされているか

経営インフラの成熟度を高める

（例えば、JSOXはレベル3）

protiviti

取締役会がリスク監視を効果的に推進するには④

取締役会と経営者はリスク選好について同意しているか

① 取締役会は、**企業が取るべきリスク、回避すべきリスク**等に関し、その状況を示す指標について経営者と定期的な協議をもつ

② ビジネスが**リスク選好指標の範囲内で実施**されているかどうやって知ることができるか

③ **リスク選好を個別のリスク許容度に分解**し、事業目的達成に関する業務の変動幅の管理に利用する。

（例えば、リスク許容度は売上変動幅、利率の変動、人材の雇用・育成・維持等に関する指標等で示され、さらに戦略遂行に影響を与え得る兆候を示す先行指標が意思決定に重要な影響を与えるものとして示される）

取締役会・監査役会がリスク監視を効果的に推進するには⑤

自社のリスク文化は正しい行動を奨励できているか

① いかにリスク管理がしっかりできていても、**社会秩序を乱す組織的行動**が存在し、許容されていては意味がない。

② トップがリスク管理部門からの**危険信号を無視**したり、取締役会が戦略の前提やリスクについて厳しい追及をしなかったり、**悪い知らせが疎まれる空気**があると、重要な変化を見誤る可能性が大きい。

③ 不適切なリスクテイクや、誤った戦略から**適時に撤退することができなくなる。**

④ 望ましい文化のもとでは、**多様な価値観、目的、ベストプラクティスが共有**　され、リスクが企業の意思決定に織り込まれ、**風通しのよさや、倫理的行動が徹底**されることになる。

取締役会がリスク監視を効果的に推進するには⑥

リスク管理は適切な経営プロセスと連携しているか

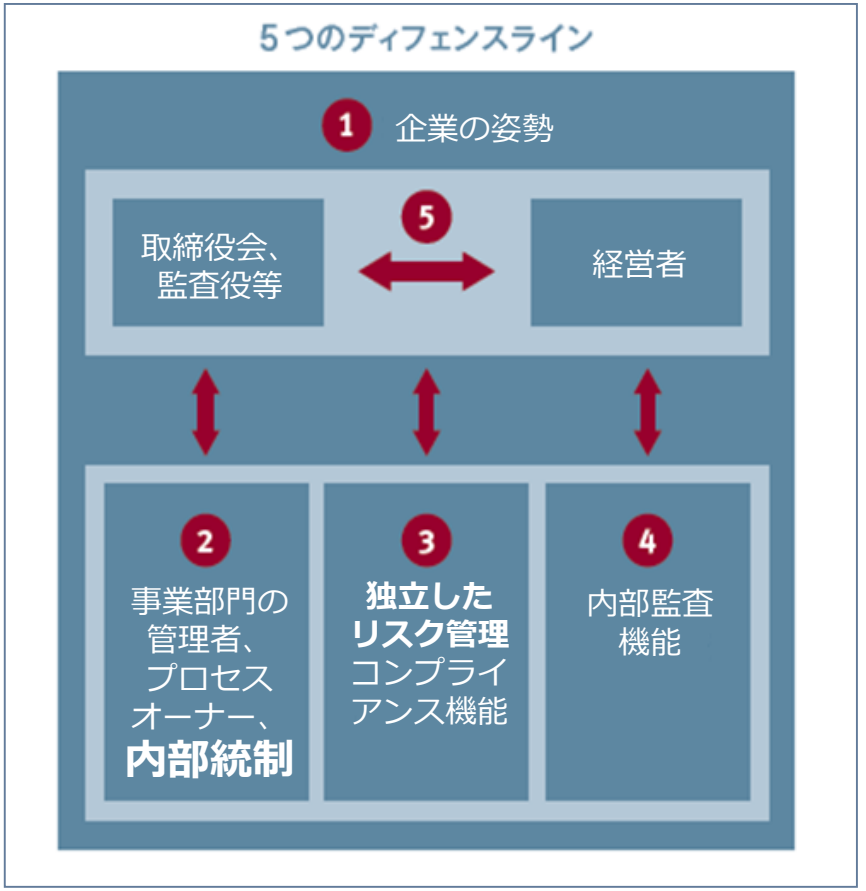
① リスク管理が経営プロセスと連携し、目的達成と戦略遂行への確信を持つ

② **連携の質と程度は業種や企業ごとに異なり**、また経営者の経営スタイルによっても異なる。
中長期戦略策定、年次計画策定、業績管理、予算策定、競争優位性、設備投資予算、
Ｍ＆Ａのターゲット設定、デューデリジェンス、買収後の統合、内部統制全般等

③ 連携を効果的に進め、リスク管理が持続的競争優位性の確立や業績改善に貢献

5つのディフェンスライン　～「企業の姿勢」の重視～

- ガバナンス、リスクマネジメント、内部統制が有効に機能するには**「企業の姿勢」**が最重要
- 「企業の姿勢」とは、経営トップ、中間層、現場それぞれの姿勢の**複合的姿勢**だが、激変する環境のもと、それぞれの姿勢は**同じではない**という前提に立つべきである
- 企業の姿勢を組織の隅々まで反映させるには、先ず**経営層と管理者層の間でトーンを合わせること**が大切
- トーンを合わせるには、**「内部統制の共通言語」を構築し、浸透させることが必要不可欠**
- **「内部統制の共通言語」**とは、**企業の姿勢・理念、内部統制の目的・方針・役割・リスク定義・リスク評価・リスク対応・内部統制の仕組み【統制手続、コミュニケーションの仕方、モニタリング方針】**等の総称
- 5つのラインが有効に機能するには、全社にリスクカルチャー*を醸成・浸透させることが重要



※リスクカルチャーとは、「組織内のリスク管理に対する、許容範囲内での一連の行動、協議、決定や姿勢」である。

protiviti

リスク監視・ディフェンスラインの失敗事例

T社の第三者委員会調査報告書から、リスク監視と5つのディフェンスラインを考える

✓ガバナンス体制整備は進んでいるといわれていたT社の不適切会計に関する報道は、多くの経営者、リスク管理、内部統制や内部監査に関与する人に衝撃を与えた。

＜公表された第三者委員会調査報告書が指摘する原因を、ディフェンスラインにあてはめた結果＞

第三者委員会報告書により指摘された不適切会計の原因	
①企業の姿勢	• **上司の意向に逆らうことができないという企業風土**の下、従業員は上司の意向に沿って目標を達成するために不適切な会計処理を実行していた。
②事業部門	• 当期又は投資半期における利益を最大化するという観点(**当期利益至上主義**)から設定された目標達成値(チャレンジ)を達成するために、**利益の先取りや損失・費用の計上先送りなどの不適切な会計処理**を行わざるを得ない状況に追い込まれていた。
③コンプライアンスや財務部門	• 財務部は各社内カンパニーにおける**会計処理の適切性をチェックする役割**を果たしていなかった。 • また、「チャレンジ」の原案など、**目標達成へ過度なプレッシャーを与える**過程に関与していた。
④内部監査	• 経営監査部は経営トップが所管し、「経営」のコンサルタント業務を主に行い、**会計処理が適切か否かといった会計監査の観点からの監査**はほとんど行われていなかった。
⑤経営者と取締役会	• **経営トップらの関与**等に基づき不適切な会計処理が同時並行的かつ組織的に実行、継続された。 • 受注時または受注後に巨額の損失の発生が見込まれる案件が存在したにもかかわらず、**取締役会で報告されていなかった。** • 監査委員会において、複数の監査委員が不適切な会計処理が行われている事実を認識した場合も、**問題点を指摘するなどの行動はとられなかった。**

protiviti

質問（６）リスクの監視（オーバーサイト）について

皆さんの企業では、攻めと守りの意味で、リスクの監視（オーバーサイト）について、取締役会ではどの程度、実施されていますか？

1. 取締役会にはリスクの監視という機能はほとんどない
2. 重要な投資案件等（攻め）とコンプライアンス等（守り）のリスク対応については議論している
3. 攻めと守り双方の観点から、取るべきリスクと取ってはならないリスクについて、戦略策定時から、全社的視点で積極的に議論している

protiviti®
Face the Future with Confidence

7．まとめ

まとめ①　取締役会における近時のトップ10リスク

1. ガバナンスリスク（取締役構成、選任、役割、インセンティブ）
2. Tone at the Top
3. 戦略リスク（ビジネスモデル、健全性、変化適応力）
4. 取締役会承認リスク（重要な経営判断と根拠情報の品質）
5. ブラックスワンとエマージングリスクへの対応
6. レジリエンス（しなやかさ）
7. ESG/SDGｓリスク
8. 人材戦争
9. イノベーション（デジタル化とモノ作り力）
10. サイバー攻撃（いつ起こるではなく、起こることを前提とした準備）

まとめ②

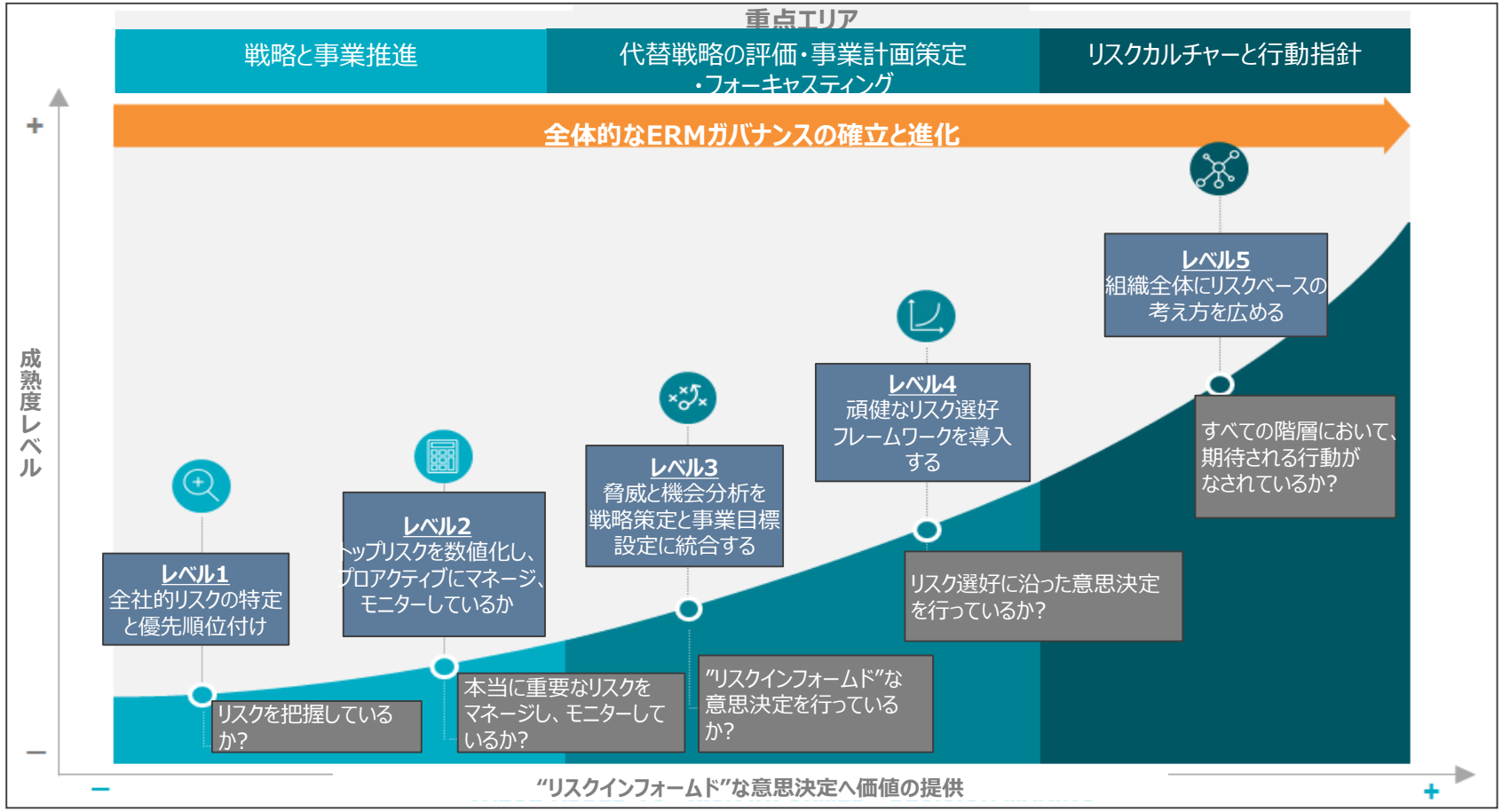
- 目的－ガバナンス－戦略－リスク－内部統制
- 市場ガバナンスのみならず、組織ガバナンスの強化を推進する
- リスクの定義を見直す
- ERM・内部統制は、戦略実現の基盤であり、トップダウンで、グローバル方針を設定し、適切にモニタリングする仕組みを強化
- 取締役会・監査役等＝ガバニングボディとして、的確な質問は、リスク監視の観点から行う

リスクオーバーサイト資料は下記を参照してください
https://www.protiviti.com/JP-jp/Insights

（ご参考）プロティビティ　ERM旅路の枠組み

ProtivitiのERM Journeyフレームワークは、ERM高度化へ向けた道標を提示しています。

凡例：成熟度の目標例



protiviti

Face the Future with Confidence

protiviti®