protiviti®
Global Business Consulting

監査懇話会セミナー

激変する経営環境において、取締役会は如何に対処するか
～新たな巨大リスクに対処し持続可能な機会を確保する

2023年1月27日
プロティビティLLC
シニアマネージングディレクタ
神林 比洋雄

本日のプレゼンター

プロティビティ LLC　シニアマネージングディレクタ
神林 比洋雄（かんばやし　ひよお）

アーサーアンダーセンに入社し、国内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。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統括パートナー、アンダーセンワールドワイドオーガニゼーション取締役を歴任。
2003年プロティビティLLC創設、CEO就任。攻めと守りを基盤とするERMの高度化による経営戦略実現や、最適なガバナンスと内部統制構築を支援。2017年より現職。

日本内部統制研究学会（現日本ガバナンス研究学会）前会長。株式会社証券保管振替機構リスク管理委員会委員（現任）。一橋大学財務リーダーシップ・プログラム講師（2015～現任）。ERM経営研究所LLC代表社員（17～現任）、双日株式会社社外監査役（17～21）、株式会社村田製作所社外取締役（18～現任）、株式会社東芝コンプライアンス有識者会議委員（20～21）。日本取締役協会内部統制連絡会座長（現任）、会計教育研修機構講師（現任）、公認会計士。

近著：『今さらきけない内部統制とERM』（同文舘2020），『COSO全社的リスクマネジメント』・『COSO内部統制の統合的フレームワーク』・『COSO不正リスク管理ガイド』（共訳）、『内部統制に関する法的責任の研究』・『開示不正』（共著）等

本日のトピック

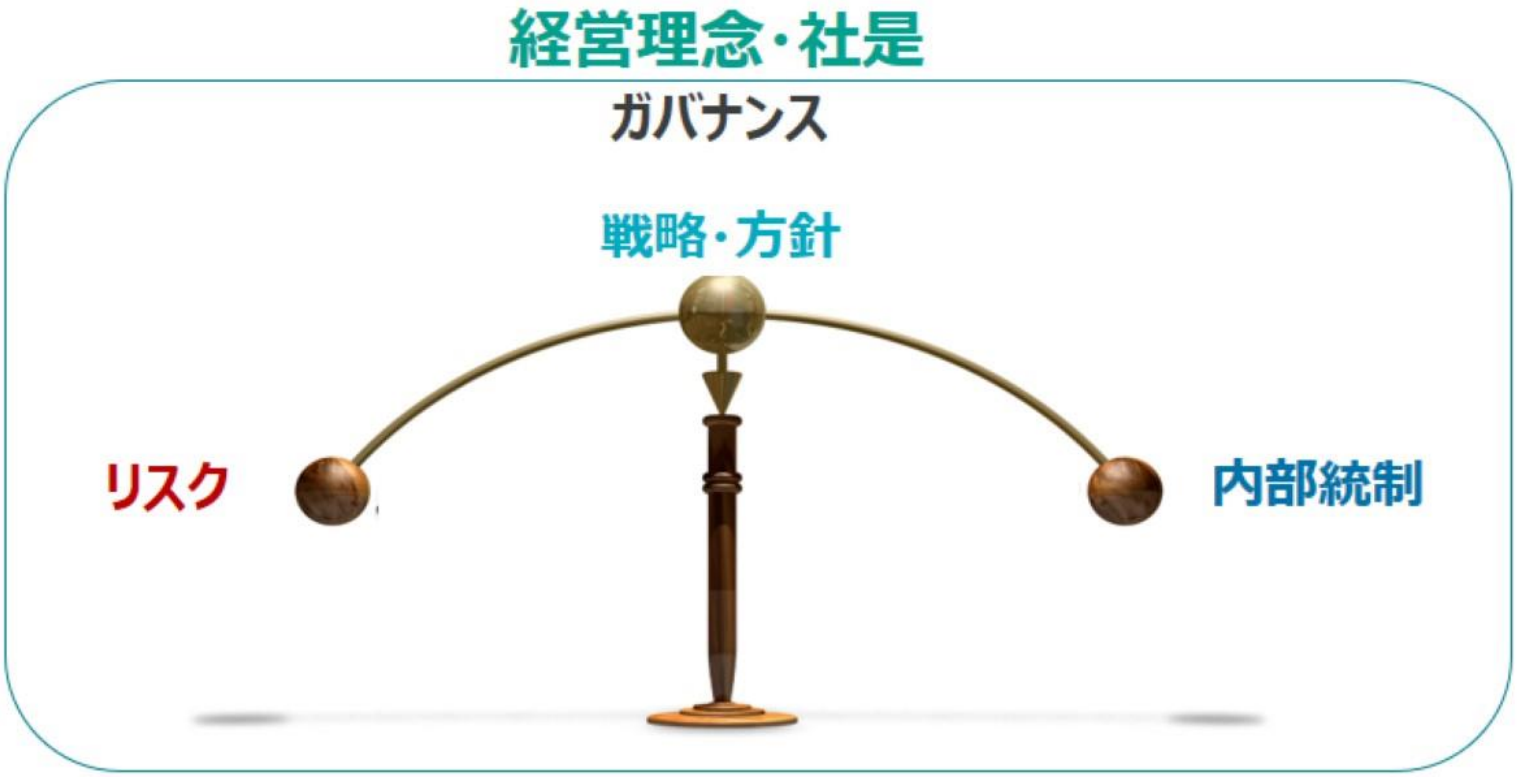
1. **激変する経営環境と新たなリスク**
   ～何が経営戦略に影響を及ぼす事象なのか
2. **攻めと守りの全社的なリスクマネジメントの最新動向**
   ～経営執行およびガバナンス両面の視点から
3. **取締役会が果たすべき全社的なリスクマネジメントにおける役割**
   ～その実効性を高めるには

1. 激変する経営環境と新たなリスク

～何が経営戦略に影響を及ぼす事象なのか

経営理念・社是を基盤とする経営

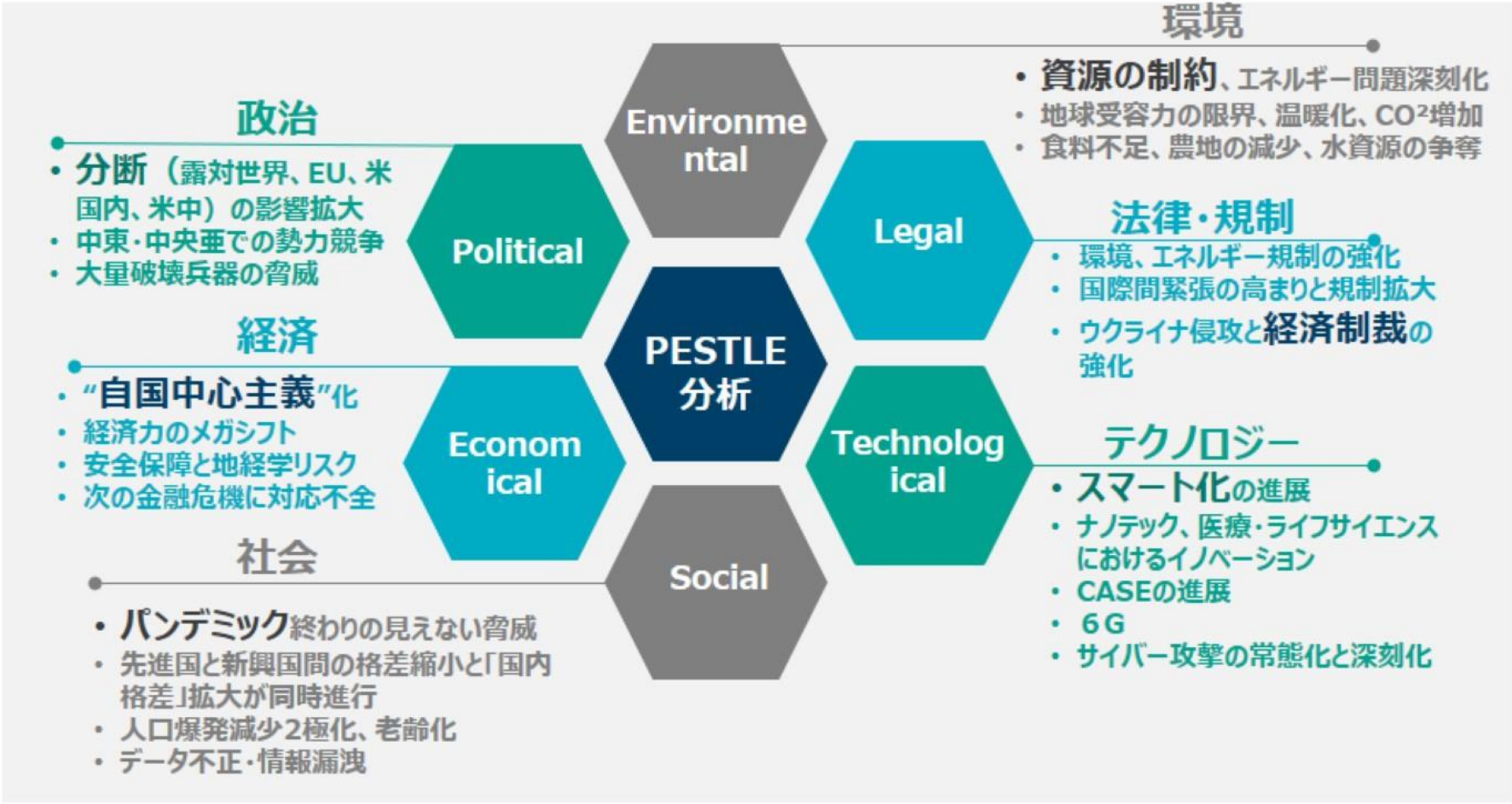
経営理念・社是・ガバナンス・戦略・リスク・内部統制の関係とは



経営理念・社是を実現するとは、適切なガバナンスのもと、外部・内部の環境変化を把握し、企業価値の源泉に影響を与えるリスクを見極め、戦略を策定する中で、選択された戦略の達成に影響を及ぼすリスクを特定し、その影響を経営者の許容範囲に収めるべく、相応の内部統制を構築し、中長期的に、やじろべえのバランスを保つことにより、期待される価値向上を目指すこと。

企業を取り巻く外部環境変化

この数年、世界は激変し、かつての常識が通じなくなっている - パラダイムシフト



protiviti

世界のパラダイムシフトを牽引するステークホルダー

サステナビリティ・ESGに対する意識の高まりから実際の行動へ

公的機関

中長期的なグローバル目標を設定し、
ESGを促進するための規制を制定し、
サステナブルな移行を推進(TCFD等)

投資家

ESG投資プロセスへの統合を強化し、
企業による非財務情報開示を奨励

消費者

サステナブルな行動へのシフト、持続
可能性に対する意識の高まり、「グリーン」な
製品・サービスへの関心の高まり

従業員

持続可能な職場環境を求め、環境
や社会にポジティブな影響を与える企業
を選択

メディア・NGO

持続可能性に関する認識を高め、
サステナブルなビジネス慣行を要求

企業

戦略とサステナビリティを整合させ、
長期的な価値と将来の存続の確保、
パフォーマンスの向上

経営環境の変化：世界の経営者が見る重要な脅威

2023年1月14日ダボス会議が示した今後2年および10年で最も重要な脅威とは

protiviti

「先を見越したリスク」

トップリスク2022および2031に関するエグゼクティブの視点

プロティビティとノースカロライナ州立大学による2022年12月グローバル調査結果～取締役会や経営幹部が議論する重要課題

2023年のリスクトップ10*	YOY change	2032年のリスクトップ10*	YOY change
1. 人材市場が逼迫する中、組織の後継者問題やトップ人材の獲得・維持困難により、事業目標の達成能力が制約される	↑	1. 人材市場が逼迫する中、組織の後継者問題やトップ人材の獲得・維持困難により、事業目標の達成能力が制約される	↑
2. 現在サービスを提供する市場の経済状況により、成長機会が著しく制限される	↑	2. デジタル技術導入にあたり、不足する新たなスキルが求められ、従業員のリスキリングやアップスキリングに多大な労力が必要となる	↑
3. 予想される人件費の増加により、利益目標の達成能力に影響を及ぼす	↑	3. 新たな技術または他の市場原理によりもたらされる、革新的なイノベーションの早いスピードに競争力が追い付かない	↑
4. 変化への抵抗により、組織がビジネスモデルや中核事業に必要な適応・変化が制約される	↑	4. 変化への抵抗により、組織がビジネスモデルや中核事業に必要な必要な適応・変化が制約される	↑
5. 主要なサプライチェーンエコシステム（生態系）を取り巻く不確実性	↑	5. 個人情報保護への要求の高まりにより、プライバシーとコンプライアンスを確保するために多大なリソースが必要となる	↑
6. 職場環境全般の変化により、組織文化や行動規範の維持に課題をもたらす	↑	6. 現行のオペレーションと時代遅れのITインフラでは、パフォーマンスの期待や、「ボーン・デジタル」との競争に応えられない	↑
7. デジタル技術導入にあたり、不足する新たなスキルが求められ、既存従業員のリスキリングやアップスキリングに多大な労力が必要となる	↑	7. 市場情報分析の獲得や生産性・効率性の向上のための、データ解析やビッグデータを使う能力が欠如する	↑
8. 組織の文化が、リスクのタイムリーな特定や上層部への報告を十分に後押ししない	↑	8. 現在サービスを提供する市場の経済状況により、成長機会が著しく制限される	↑
9. 大多数の従業員のリモートワーク環境（ハイブリッドワークの一部としてを含む）で働くことへの要望や期待に対応するアプローチ	↑	9. 規制の変更や規制監督の強化が、製品やサービスの生産方法や提供方法に著しい影響を及ぼす	↑
10. 組織の予期せぬ危機に対処するためのレジリエンス（耐性）やアジャイル（俊敏性）が十分でない	↑	10. 予想される人件費の増加により、利益目標の達成能力に影響を及ぼす	↑

protiviti

「先を見越したリスク」 ～ 調査のハイライト

トップリスク2022および2031に関するエグゼクティブの視点

プロティビティとノースカロライナ州立大学による2022年12月グローバル調査結果～取締役会や経営幹部が議論する重要課題

調査の主なハイライト

不確実性に満ちていることが、経営陣や取締役会のリスクに対する懸念の高まりを引き起こしています。調査回答者は、全体的なリスクの重大さと影響を、この11年間の調査での最も高い水準で評価しています。

リスク環境は変化していますが、変化への抵抗は続いています。新しいリスクが急速に出現する以上、リーダーはリスク環境の変化を無視することはできません。組織の文化は、革新的な変化に適応すべく備え、市場での機会とリスクについて意思決定者への伝達を促進する必要があります。

経済は最重要課題です。世界的にインフレと成長に関する課題が継続する可能性があるという重大な懸念があります。

人材とテクノロジーに関する懸念がトップリスクの大半を占めています。10年後の展望は、革新的イノベーション、進化するテクノロジー、人的資本の課題に関連する機会とリスクが混在していることを反映しています。経営陣や取締役会は、新しいテクノロジーやデジタルイノベーションに関連する顧客価値をフルに実現できる人材を見出す必要性を認識しており、その確保のために既存の従業員への再教育やスキルアップの戦略を優先しています。また、利益目標の達成に影響する人件費の増加や、ハイブリッドやリモートワーク環境下での管理方法のアプローチの模索や働き方の継続的な変化も懸念しています。

経営幹部や取締役会の中でも、多様なリスク観が存在します。どのようなリスクが最も重要であるかについては、様々なリーダーによって顕著な違いがあり、組織において最も重要なリスクについて話し合うことの重要性がハイライトされています。

長期的な視点に立ったリスク管理は、短期的な対処に不可欠です。組織が2023年がもたらす課題に対処する一方で、レガシーITインフラからの効果的な移行、顧客体験価値の重視、将来の成長機会への投資、プライバシーとセキュリティの確保、先進的なデータ分析の導入能力の向上など、今回の調査で指摘された長期的な課題に備えることも必要です。長期的な展望を持つことで、不測の事態への耐性の強化や次の成長段階へ備えるために企業はどこに投資すべきかに焦点を当てることができます。

統制としてのリスクマネジメントが、ビジネス成功のためにさらに重要性を増しており、本調査結果では2023年に経営陣や取締役会がリスクマネジメントの強化に投資する可能性が全体的に高いことを示しています。

protiviti

各種グローバルリスクサーベイから見えてくる

注視すべき5つの重大リスク

① パンデミック
② 地政学リスク
③ ESGリスク
④ サイバー攻撃
⑤ サプライチェーン

（1）パンデミック ～ COVID-19がもたらした5つのメガトレンドへの対応

パンデミックにより、引き起こされた5つのメガトレンドを注視し続ける必要がある

1. 職場環境の変化への対応と活用：

バーチャルワーク体験を通じて、従業員の柔軟性が養われ、生産性向上が期待される。これは競争優位の源泉にもつながり、テクノロジーをバックにした権限移譲の推進や雇用促進への考慮も重要。

2. ビジネスモデル：

顧客・消費者の行動や嗜好の変容により、提供する商品やサービスの見直し、更に、ビジネスモデルそのものの変革の検討を迫られる可能性がある。買い手の行動を注視し危機後に向けて備えを万端に。

3. サプライチェーン：

過去30年のサプライチェーンの複雑化、例えば、シングルソースの戦略的サプライヤー、JITの製造・配送技術、複雑なロジスティクスなどの見直しが喫緊の課題。コストに偏りすぎた品質・時間・コストのトレードオフは見直しが不可欠。重層化するサプライヤーのレジリエンスを見通し、サプライチェーンの長期的な混乱にどの程度、耐えうるか対応能力を常に注視する必要がある。

4. 企業文化を守り、信頼関係を発展：

盤石な企業文化を基盤にして、従業員、顧客、サプライヤーとの間での強力なコミュニケーション能力と、強力なイノベーション能力を培うことが生き残るための重要な要素。

5. デジタル成熟度：

バーチャル・ワークプレイスとデジタルチャネルが定着するにつれ、その基盤であるテクノロジー・プラットフォームを保護し、重要な機密を守るに十分なデジタル成熟度を確保する必要がある。

（2）地政学リスクへの対応　～トップ10地政学リスク

①🇷🇺🇺🇦**ロシア・NATO紛争の激化**
②🇺🇸🇨🇳**グローバルな技術デカップリング**（米中の供給網の再配置）
③🇷🇺🇺🇦**重大なサイバー攻撃（特にロシア発）**
④**湾岸諸国間の緊張**（特にイラン）
⑤🇷🇺🇺🇦**新興国の政治危機**（食料不足・インフレ等）
⑥🇺🇸🇨🇳**米中の戦略的競争**（台湾・南沙諸島を巡る緊張）
⑦**重大なテロ攻撃**
⑧**北朝鮮**（７回目核実験）
⑨🇷🇺🇺🇦**気候変動政策の停滞**
⑩🇷🇺🇺🇦**欧州の分裂**（対露方針：独仏伊 vs ﾎﾟｰﾗﾝﾄﾞ・ﾊﾞﾙﾄ３・英）

出典：BlackRock Investment Institute, Geopolitical risk dashboard, July 2022
https://www.blackrock.com/corporate/insights/blackrock-investment-institute/interactive-charts/geopolitical-risk-dashboard

ウクライナ侵攻前の
グローバル・ビジネスの変調 ①

グローバル化の特徴

- 世界中の企業や政府が基本的な考え方を共有し、商品やサービスを交換
- 外交問題や紛争に取り組む際の影響力を高めるために結ぶ同盟
- 他国の天然資源、技術、能力を利用できることを暗黙の了解

グローバル化の30年間、企業のビジネスモデル形成に多くの進展

- **国境を越えた調達、アウトソーシング、IT、シェアードサービスセンターの増加**
- **設備の統合やプロセスの合理化、非コア活動の集中化・自動化の推奨**
- **サプライヤー・パートナーとの強い関係や緊密な結合による品質維持・コスト削減**

しかし、ここ数年、グローバル化の進化を支えてきた前提を覆すような出来事が起こっている

protiviti

ウクライナ侵攻前の
グローバル・ビジネスの変調 ②

グローバル化の進化を支えてきた前提を覆す流れの例

1

ESGの台頭 -「環境」:

- 製品ライフサイクルにおける脱炭素への期待
- 取締役会や経営者による環境問題への配慮の浸透

2

ESGの台頭 -「社会」:

- **グローバル供給網における人権侵害への注目**
  （児童労働、人権、健康と安全、ジェンダー不平等、等）

3

他国への依存の懸念：

- **国家安全保障の戦略分野（半導体、薬品、鉄鋼など）**
- **パンデミックによるグローバルサプライチェーンの混乱**

4

レジリエンスへの注目：

- **バリューチェーン上の事業活動に対するレジリエンスへの注目、全社的視点の重要性**
- **戦略的サプライヤー、電力供給、主要社員、重要システム、輸送・物流、主要顧客との契約等**

protiviti

ウクライナ侵攻が
グローバル・ビジネスに与える大きな打撃

グローバル化の根底には、**経済的な依存関係**によって、国や地域が国境、領土、貿易、安全保障などに係る**地域紛争を平和的に解決**するという不変の前提

ロシアのウクライナ侵攻は企業が世界をどう見るかという基本的な前提に影響

- **メーカーのサプライヤー・ポートフォリオ、生産拠点、流通経路の多様化など、供給網のレジリエンス強化の必要性**
- **国家の安全保障や日常生活の維持に不可欠な製品に関連する重要な部品や商品の調達が困難に**

これまでの前提や認識は、地政学的な現実を踏まえて改めて見直す必要あり

グローバル戦略の見直しへ向けた地政学リスクにおける考慮点

地政学および規制環境に関する前提事項は戦略設定における重要なインプット

- 適切な手段によるリアルタイムのモニタリングの仕組みが不可欠

前提事項が無効となった場合、戦略とビジネスモデルを調整

- 戦略の基本的前提事項を評価
- 戦略とビジネスモデルへの影響を評価し新たな選択肢を検討

企業投資のROIを維持するためのソブリンリスクの管理

- 事業の国営化あるいは資産の収容など
- 破壊的な事象や状況（暴力、テロリズム、戦争もしくはインフラの不備等）

- ある国において不利な事象が発生した際に事後検証（ポストモーテム）を行う
- カントリーリスクを見直す

protiviti

（3）ESGリスク　～ウクライナ侵攻への制裁がもたらすESG上の主な課題

ロシアへの制裁によってESGにおける地政学がからむ課題はさらに複雑化

「環境課題」

- 石油、ガス、その他化石燃料製品に対する代替エネルギー源の追求
- 短期的に供給不足とエネルギーコストの高騰、エネルギー政策後退の検討
- 原子力エネルギーの検討が進む可能性

「社会課題」

- ウクライナ紛争の甚大な人的被害と国際的な人権基準抵触
- ロシア・ベラルーシでの取引継続、武器の設計・製造に関わる倫理観
- 人身売買や奴隷制度など、難民問題から生じるリスク

「ガバナンスの課題」

- 適切なESG対応への期待、短期的な利益より倫理や長期的な視点
- 多くの企業のロシアでの取引停止発表、投資の保留
- ロシアとの取引継続を選択した組織はの風評被害の勘案が必要

ESGに取り組む企業へ投げかけられる質問

- **制裁がもたらす直接的な課題だけでなく、ESG事項への幅広い影響にも対応が必要**
- **長期的な組織・ESG目標を達成するためには、それらの間のトレードオフがより複雑になる**
- **ESGの基準、フレームワーク、データプロバイダー、ベンチマーク、格付け、ランキングは、ロシア制裁によって生じた課題にまだ適応できていない**

企業や組織に投げかけられる質問：

- ✓ ロシアへの制裁がビジネスに与える広範な**影響や組織のリスク決定に関する議論に、経営幹部が関与**しているか？
- ✓ 紛争状況に対する**ステークホルダーの期待は何か？**
  それを受けての**企業の対応**は何か？
- ✓ 自社の**ESGの定義**は、ロシア制裁によってどのような影響を受けているか？
  ESGのフレームワークに**地政学的リスク**や付随的なリスクを組み込む余地はあるか？
- ✓ **どのESGの成果を優先すべきか**（例：人権、気候・エネルギー、グローバル・ガバナンス、社会）？ これらの優先順位は時間とともにどのように変化するか？

protiviti

（4）サイバー攻撃 ～ “ビジネス化”するその傾向と対策

- 金銭的な利得を狙った攻撃が猛威を振るっているほか、サプライチェーンや生産システムなどへの攻撃、個人情報の搾取などのケースが頻発
- 変異種が急増し、RaaS*として横行しているため更なる対策が不可欠

類型	特徴	最近の事案例
ランサムウェア	標的のデータやシステムを暗号化し、復号化キーと引き換えに「身代金」を要求	コロニアルパイプライン、カプコン、ニップン など
サプライチェーン攻撃	システム管理ツールやソフトウェアライブラリが侵害されており、ユーザー企業が被害を受けるケース	SolarWindsおよびKaseyaのユーザー企業など
海外拠点への攻撃	本社がシステムを把握しきれておらず、比較的統制が効いていない、海外拠点が標的となるケース	自動車企業 など
工場やプラントへの攻撃	工場やプラントなど制御システム(OT)ネットワークへの攻撃	電機企業 など
クラウドシステムの設定 ミスの悪用	クラウドストレージなどに保存されたファイルなどの権限設定や暗号化設定が甘く、大規模漏洩につながるケース	Twillio など

＊ RaaS : Ransomware as a Service

サイバーセキュリティ強化に取組む上で、企業が直面する課題

厳しい リソースの制約	• サイバーセキュリティを深く理解する専門人材供給の要請 • セキュリティ対応や監視へ多くの人手の必要性
一義的ではない 対策アプローチ	• 脅威や情報システム利用の在り方の急速な変化（クラウド/モバイルシフト）に合わせ、セキュリティのアプローチも適時な対応が必要 • 企業ごとに脅威や重要な情報資産が異なり、一律に適用できる対策ポイントは自明ではない
全社的な最適化とガバナンスの必要	• セキュリティと事業の併用確立の困難さ（セキュリティに予算をかけることの正当化） • 「鎖の強さは、一番弱い鎖の輪によって決まる」- 多層的なセキュリティ対策とそのチェックは、委託先を含めた組織・サプライチェーン全体に行きわたる必要がある

（5）サプライチェーンの課題と対応

サプライチェーンの混乱は、今までのSCM原則(効率など)が、在庫が適切な場所で適切な時期で利用可能であることを保証するものではないことを示している。 より強靭で柔軟なモデルに再構築する必要がある。

スエズ運河は2021年3月封鎖され6日間で9.6億ドルの貿易業務が遅れた

ロサンゼルス港は太平洋貿易レーンが記録的に成長し混雑を極めた

顧客と消費者の変化
- 急速に変化する市場の需要と顧客のニーズ
- 顧客ライフサイクルの短縮
- 価格の透明性の向上

競争の激化
- グローバルな競争圧力
- イノベーションスピード
- 段取り替えコストの削減
- 代替製品の容易な移行

労働力格差・不足
- COVIDによる継続的な労働市場混乱
- 限られた供給とスキルと技術
- 人件費の増加

サプライチェーンの混乱
- 環境災害
- 地政学/貿易上の課題
- サイバーセキュリティ
- サプライヤーの破産

輸送の制約
- 配送と港のボトルネック
- 輸送コンテナ不足
- トラック輸送の限界
- 燃料費の増加

コストと希少性増加
- 重要な鉱物の需要増
- 半導体不足
- 梱包および出荷材料

持続可能性と多様性
- 消費者と規制当局からのESG、持続可能性、サプライヤーの多様性への圧力

顧客体験
消費者は高品質でパーソナライズされた製品とサービスを期待

レジリエンス（回復力）の高いサプライチェーンの仕組みとは

事業継続性：
人的資本の変革は、サプライチェーンの混乱と回復に対処するための重要な鍵となる

多様なオペレーション
グローバルサプライチェーンのインフラでの製造と調達の多様化と、ローカル化が必要。

可視性 ：
サプライチェーンの混乱を事前に予測および計画できるようエンドツーエンドの可視性と連携が必要。

弾力性 ：
サプライチェーンのリスク軽減戦略と先行投資を再検討、将来の混乱、セキュリティとコンプライアンスの見直し不可欠

持続可能な成長 ：
破壊的技術は、持続可能な製品、新しいプロセス、サービス開発にイノベーションを推進

リードタイムの短縮
生産スケジューリングと優先順位付けを最適化するために、より優れたデータ主導の統合ビジネスプランニング（IBP）が必要。

製造の柔軟性
計画外の混乱にうまく適応できるようにするには、より適応性の高い生産設備、プロセス、テクノロジーが必要

工場生産量増加
スループットは引き続き最優先事項。
材料と人的資本に関連する制約により、生産を最適化する高度なテクノロジーと自律的な運用を推進

品質の有効性
複雑なバリューチェーン全体で品質を達成すべく、しっかりとしたサプライヤー管理で検査と検証を行うため、新しいAIテクノロジーを活用する。

運用コストの削減
膨大な量の運用データを活用して、コスト削減の機会を特定して実行する。

protiviti

ニューノーマル対応への3つのステップ

ニューノーマルを形作る流れ

需要の変化	サプライヤーと消費者は、デジタルテクノロジーの活用を加速し、需要が変容
人的資本への対応	当面の業務見直しは成功したものの、コラボレーションの推進など長期的な課題は未解決
期待の変化	ビジネスパートナーが回復力を持ち、景気後退への対応能力を如何に確認するか
規制の不確実性	さまざまな景気刺激策などが新たな不確実性を生み出している
ポストコロナへの対応	コロナ禍の収束とポストコロナへの対応

サステナブルなオペレーション
～テーマと活用事例

テーマ	活用事例
エネルギーマネジメント	• 炭素回収と低炭素物流 • デジタルツイン
水資源管理	• リーク・漏水の検出 • リアルタイム測定 • 水利用の最適化
廃棄物管理	• 廃棄物の原材料化 • 在庫の最適化 • ペーパーレスオペレーション
サステナブルな材料と包装	• パッケージのデザインレビュー • 次世代の代替材料 • 製造機器の評価
ESG 調達とサプライヤーのモニタリング	• サプライヤーの持続可能性評価 • サステナブルな調達 • サプライチェーンのトレーサビリティ
ESG の実現状況とバリューチェーン上のコンプライアンス	• IoT モニタリング • ESG報告の最適化 • ERMと情報の統合

protiviti

２．攻めと守りの全社的なリスクマネジメントの最新動向

～ 経営執行およびガバナンス両面の視点から

- リスクとは何か、その定義はどうあるべきか
- リスクと、戦略（経営資源配分）は連携・統合されているか
- リスクの特定において網羅性が確保されているとするなら、なぜそう言えるのか
- ステークホルダーの期待に応え、経営理念を実現するリスクマネジメントの仕組みとは

全社的なリスク管理（ERM）への進化に対するステークホルダーの期待

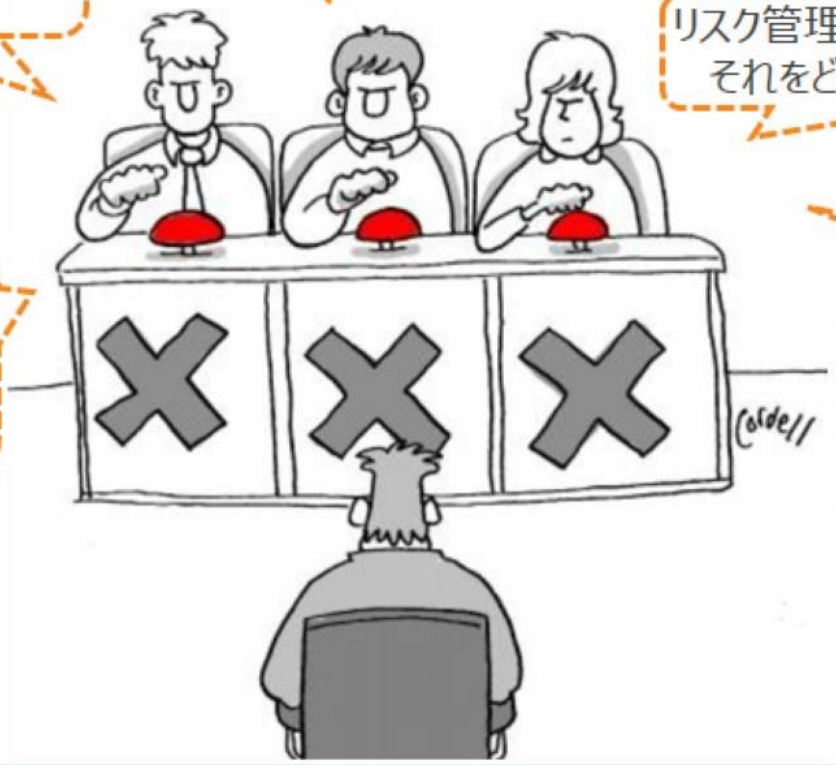
機関投資家、社外取締役、監査役等、格付会社が、経営者に聞きたいリスクマネジメントに関するよくある質問…

経営陣はトップリスクに対し
どのように**対応**しているか？

貴社の**トップリスク**は何か？
どのくらいの頻度でトップリスクを
更新しているか？

リスク管理は**有効**に機能しているか？
それをどのように**測定**しているか？

戦略策定の際に、取締役会や経営陣でリスクマネジメントに関して**どのような議論をしているか**？



業界内での最近の想定外の事態に対し、貴社はどう対応したのか？
想定外の事態が貴社に与えた影響は**他社と比較して**どうだったか？

protiviti

二つの再改定版（コーポレートガバナンス・コードと経産省CGS）が求める全社的リスク管理体制の整備と運用（1）

2021年6月のコーポレートガバナンス・コード再改訂版は、全社的なリスク管理に関する重要な論点追加
2022年7月の経済産業省　CGSガイドラインの改訂は、リスクテイクを推進する環境整備を提唱

CGコード【原則４－３．取締役会の役割・責務(3)】～抜粋
取締役会は、適時かつ正確な情報開示が行われるよう監督を行うとともに、内部統制やリスク管理体制を適切に整備すべきである。

補充原則　４－３④　～一部加工
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（守り）とリスクテイク（攻め）の裏付けとなり得るものであり、取締役会は グループ全体を含めた体制を適切に構築し、内部監査部門を活用し、その運用状況を監督すべきである。

経産省CGS　～抜粋一部加工
『攻めのガバナンス』の実現が掲げられてきたが、リスクの回避・抑制や不祥事の防止を過度に強調するのではなく、むしろ企業家精神の発揮を促し、より良い戦略を立案し、スピードをもってリスクテイクできる環境を整備し、持続的な成長と中長期的な企業価値の向上を図るべきである

二つの再改定版（コーポレートガバナンス･コードと経産省CGS）が求める全社的リスク管理体制の整備と運用（２）

取締役会のリスク管理に関する重要な論点に関する8つの疑問

経営執行の視点

1. なぜ、ガバナンスの話にリスク管理の話が出てくるのか？
2. 全社的リスク管理の対象リスクは、どう捉えるべきか？　守りの回避すべきリスク？攻めのリスクテイクすべきリスク？
3. 今までのリスク管理と全社的リスク管理（ERM）は、何が違うのか？
4. 先を見越した全社的リスク管理（ERM）とは何を意味するのか？

取締役会の視点

5. 取締役会として、リスクやリスク管理に対する実効性の高い監督とは、何が期待されているのか？
6. リスク管理（リスクマネジメント）とリスク監督（リスクオーバーサイト）は何が違うのか？
7. 取締役会として、どのようなテーマを議論すべきなのか？執行のリスク管理にどの位、踏み込むのか？
8. 日本企業の取締役会のリスク管理における役割について、よくある課題とは何か？

経営理念・社是を基盤とする経営

1 なぜ、ガバナンスの話にリスク管理の話が出てくるのか？

経営理念・社是・ガバナンス・戦略・リスク・内部統制の関係とは – 再掲

経営理念・社是を実現するとは、適切なガバナンスのもと、外部・内部の環境変化を把握し、企業価値の源泉に影響を与えるリスクを見極め、戦略を策定する中で、選択された戦略の達成に影響を及ぼすリスクを特定し、その影響を経営者の許容範囲に収めるべく、相応の内部統制を構築し、中長期的に、やじろべえのバランスを保つことにより、期待される価値向上を目指すこと。

コーポレートガバナンスとリスク

① なぜ、ガバナンスの話にリスク管理の話が出てくるのか？

米国COSOは、ガバナンス・リスク・内部統制の関係をどう整理したか

ガバナンス（リスク監視）がERMを包含
ERMは内部統制を包含

ERMは経営そのもの
価値創造において機会と脅威から
リスク（可能性）を特定し、
リスク選好（攻め）と許容度（守り）
を設定し、**戦略を選択する**

内部統制とは、経営者が設定する許容度の範囲内に収まるよう設計されたコントロール

5つのリスク対応：活用*・受容・回避・転嫁・軽減
最初の4つは戦略の課題であり、内部統制の
対象は許容範囲に収めるよう軽減すること

出典：2013及び2017COSO、
一部加工

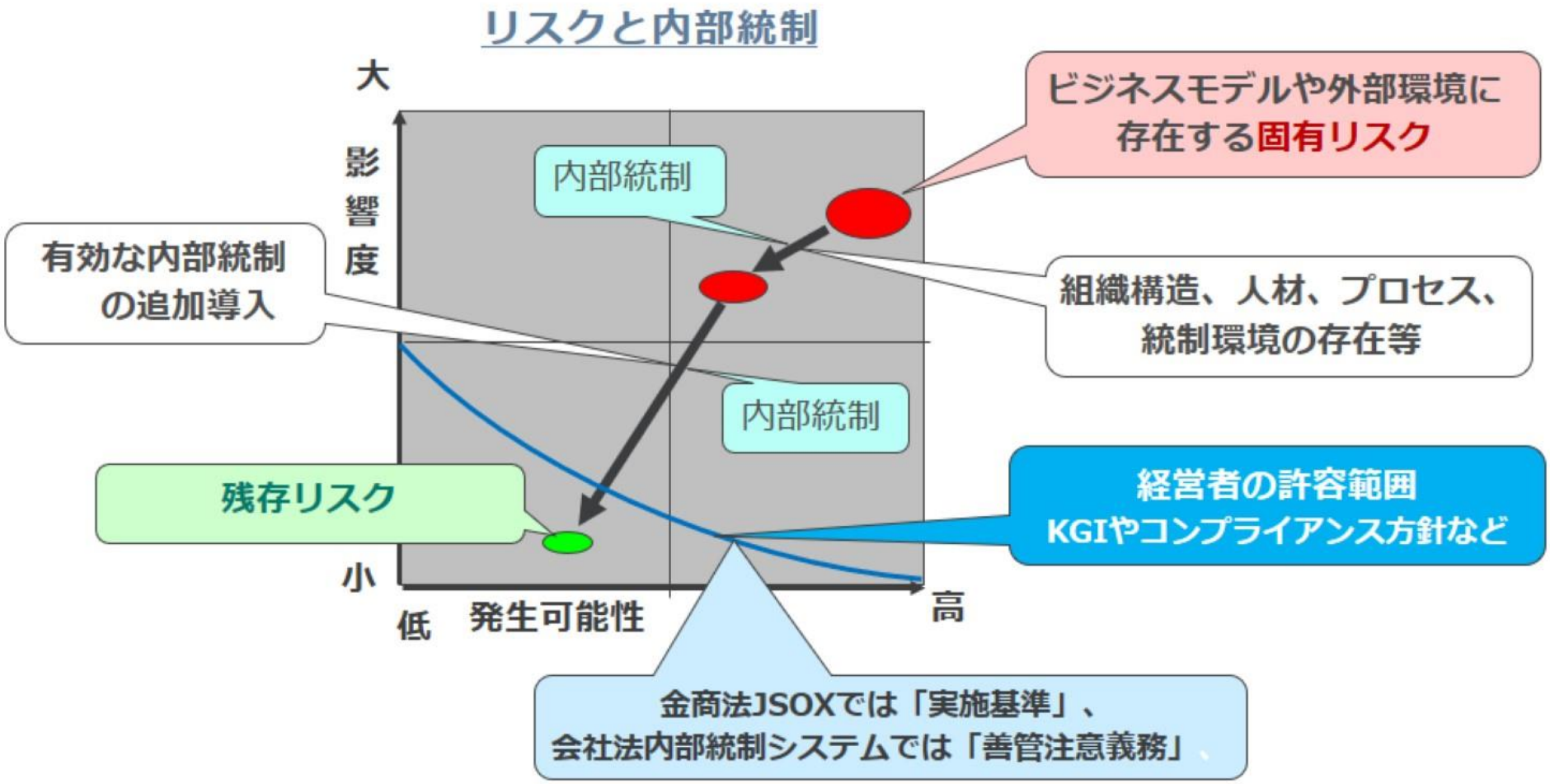
ガバナンスがプロセスである限り、原則主義に則り、経営理念に基づき、あるべき姿を念頭に継続的改善を目指す必要がある。
会社法やJSOXを含め、リスク管理や内部統制が有効であると表明するには、重要な不備がないことを保証することが必要。

＊活用と受容の違いは、リスクプロファイルが受容では変わらないが、活用では変わる、つまり新規事業や大きなM&Aなどが活用の事例

protiviti

リスクと内部統制

必要な打ち手（内部統制）を実施して、なお残る残存リスクが発現したとしても、戦略・方針への影響が経営者の許容範囲に収まっているかどうかを確認する必要がある



protiviti

先を見越したリスクの捉え方（１）

② 全社的リスク管理の対象となるリスクは、どう捉えるべきなのか？守りの回避すべきリスク？攻めのリスクテイクすべきリスク？

「知っていることよりも知らないことの方が重要かもしれない」

- 「VUCA」が一層強まり、事業環境変化の加速化が想定されるなか、どれだけのことを知っているといえるか？
- 最悪のリスクは、知らないことに気づいていないこと
- 留意すべき3つのリスク：**既存リスク、エマージングリスク、未知のリスク**

時代を表すキーワード

- **V**olatility（変動）
- **U**ncertainty（不確実）
- **C**omplexity（複雑）
- **A**mbiguity（曖昧）

- “Known Knowns （既知の知）”
- “Known Unknowns (既知の未知)”
- “Unknown Unknowns (未知の未知)”

protiviti

先を見越したリスクの捉え方（２）
そもそもリスクとは？　～リスクの語源と意味

② 全社的リスク管理の対象となるリスクは、どう捉えるべきなのか？守りの回避すべきリスク？攻めのリスクテイクすべきリスク？

リスク

語源：
ラテン語の
Risicare
「勇気をもって
試みる、挑む」

「報われるリスク」：投下した経営資源より成果が大きくなるもの

「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

- 従来のリスクマネジメントは、「報われないリスク」が中心（保険リスク）
- 価値創造モデルや新たな投資戦略は、「報われるリスク」そのもの

企業価値にプラス・マイナス双方の影響を及ぼす可能性をリスクとして、一つの枠組みで検討することが期待されている。

リスクシナリオを原因と結果で示し、重大性・優先順位は結果がもたらす影響の大きさから判断し、対応は原因・真因に対して、戦略レベルで対処する

COSO*およびISO、IIAのリスクの定義の変遷

～全社的リスク管理の対象となるリスクとは、どう捉えるべきか？守りか、リスクテイクか？

② 全社的リスク管理の対象となるリスクは、どう捉えるべきなのか？守りの回避すべきリスク？攻めのリスクテイクすべきリスク？

枠組み / リスク	COSO 内部統制 1992	COSOERM 2004	新COSO 内部統制 2013	新COSOERM 2017
定義	内部統制の目的達成を**阻害する事象**	ある事象が目的達成とは**反対の影響を与える可能性**	事象が発生し目的達成に**不利な影響を及ぼす可能性**	事象が発生し**戦略と事業目標の達成に影響を及ぼす可能性**
報われないリスク	○	○	○	○
報われるリスク —失敗要因	—	○	○	○
報われるリスク —成功要因	—	(機会として定義)	—	○

IIA 3線モデル 2013▶2020**

ディフェンスから攻めと守りのスリーラインモデルへ改訂

ISO リスク管理

ISO14971 2007年

危害の発生の確率と、それが発生したときの重大性の組み合わせ

▶

ISO31000 2009年

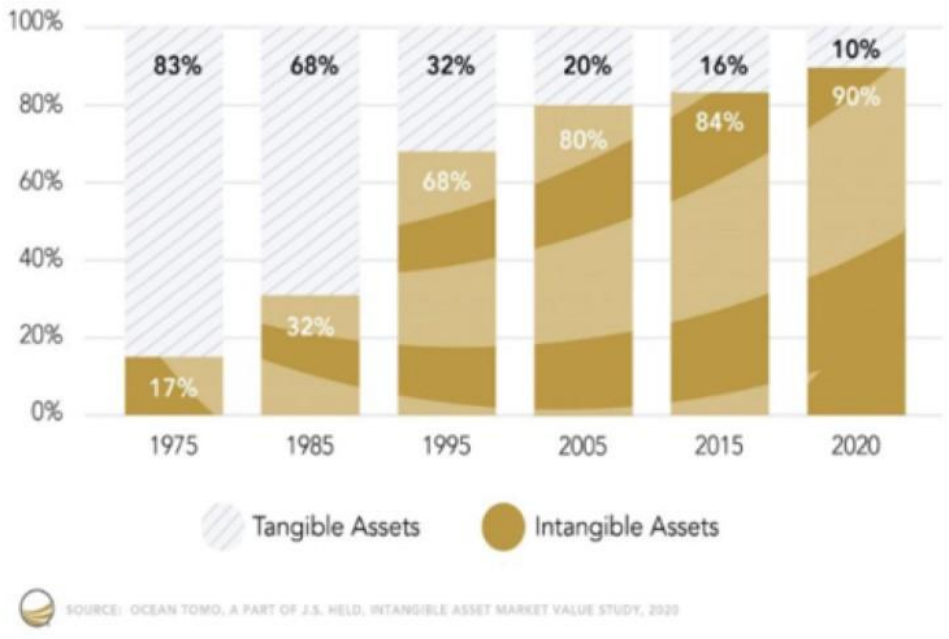
目的に対する不確実性の影響

* COSO:トレッドウェイ委員会支援組織委員会
** IIA：公認内部監査人協会

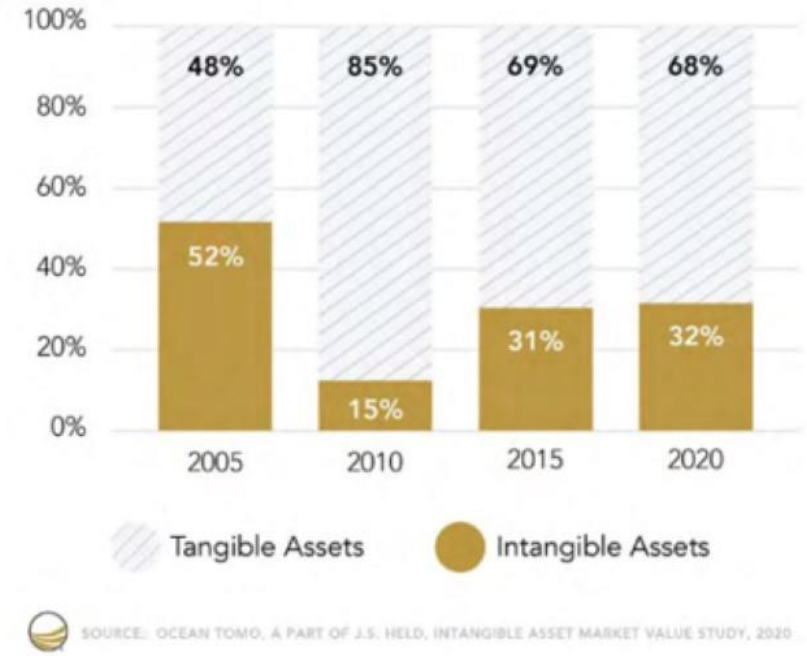
企業（市場）価値の源泉　～　価値の源泉に影響を及ぼす要因がリスク

米国では、マイクロソフトやGAFAの台頭もあり、市場価値に占める無形資産の割合が90年代以降、急激に伸びている。一方、日本では、モノづくりの強みが市場価値の7割近くを占めている。

市場価値に占める無形資産割合（米国　S&P500）



市場価値に占める無形資産割合（日本　日経225）



（出所）Ocean Tomo,　Intangible Asset Market Value Study、2020

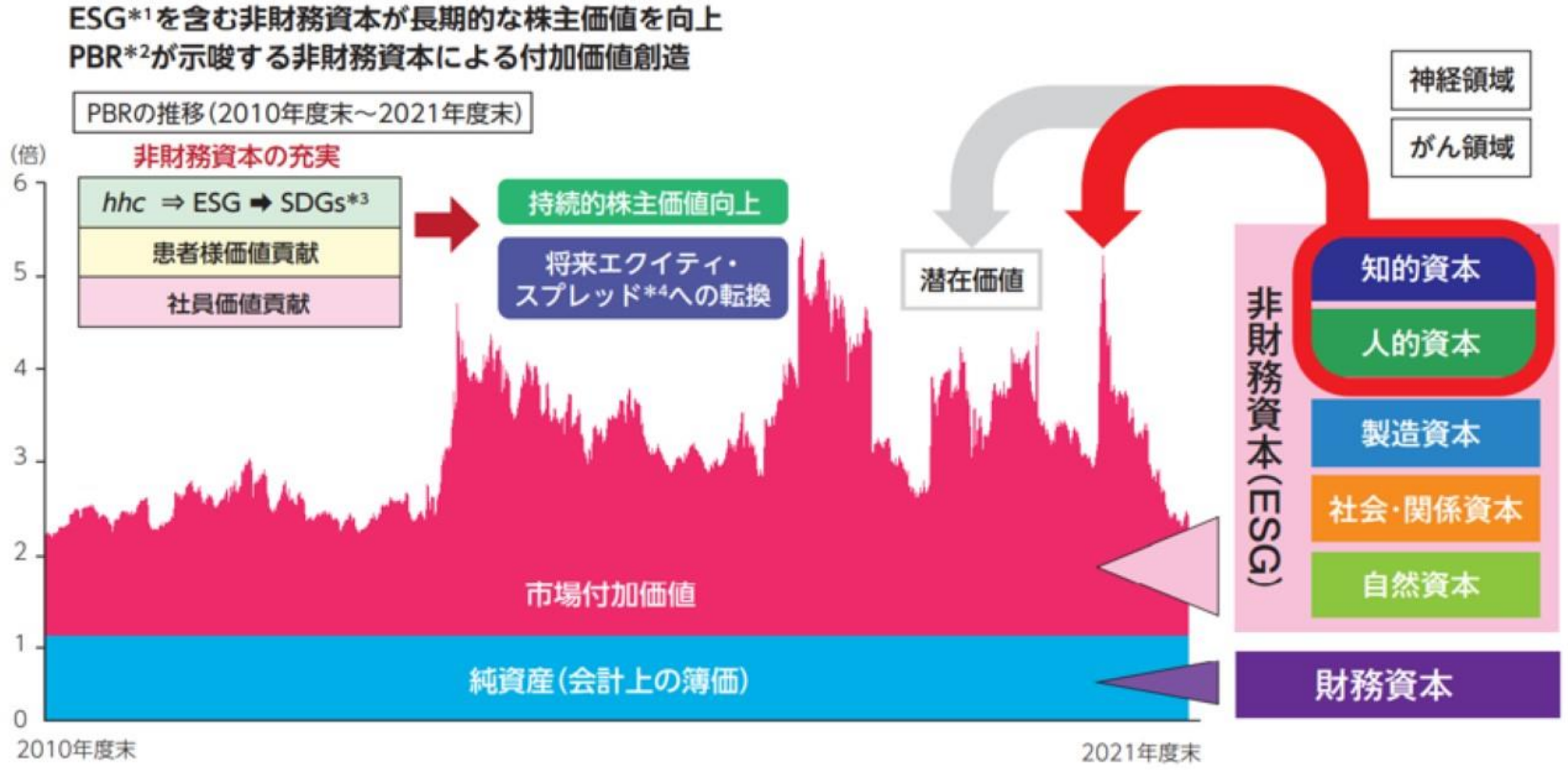
protiviti

エーザイのIIRC-PBRモデル

エーザイ　価値創造レポート2022より

● IIRC-PBR モデル（企業価値を構成する６つの資本の価値関連性）

～純資産（会計上の簿価）は財務資本と、市場付加価値は非財務資本とそれぞれ関係する～



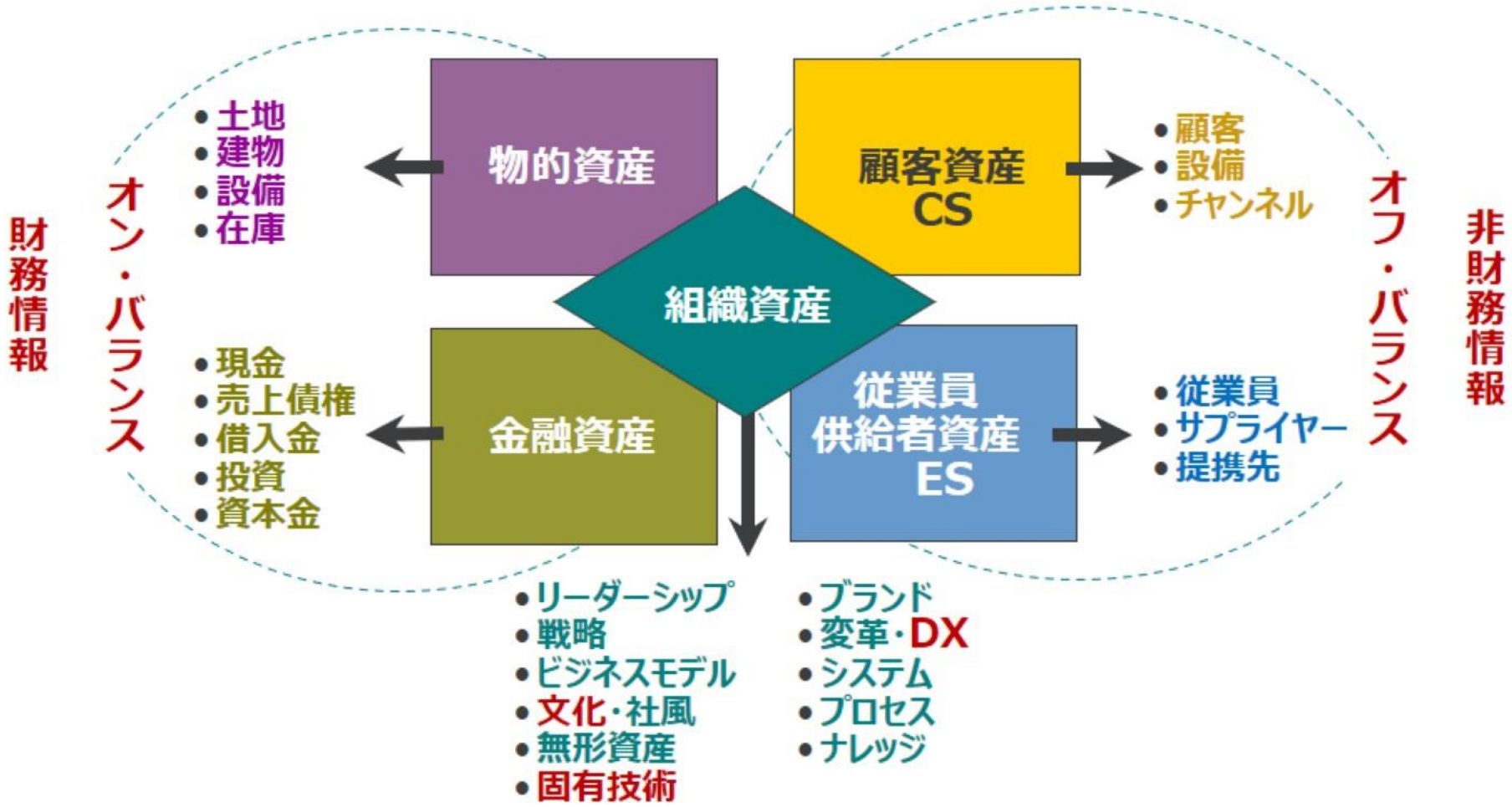
＊1 Environment（環境）、Social（社会）、Governance（企業統治）
＊2 Price Book-Value Ratio（株価純資産倍率）
＊3 Sustainable Development Goals（持続可能な開発目標）
＊4 ROE（親会社所有者帰属持分当期利益率）－株主資本コスト（当社は8%と仮定）

柳良平『CFOポリシー第2版』中央経済社（2021）を一部改編

protiviti

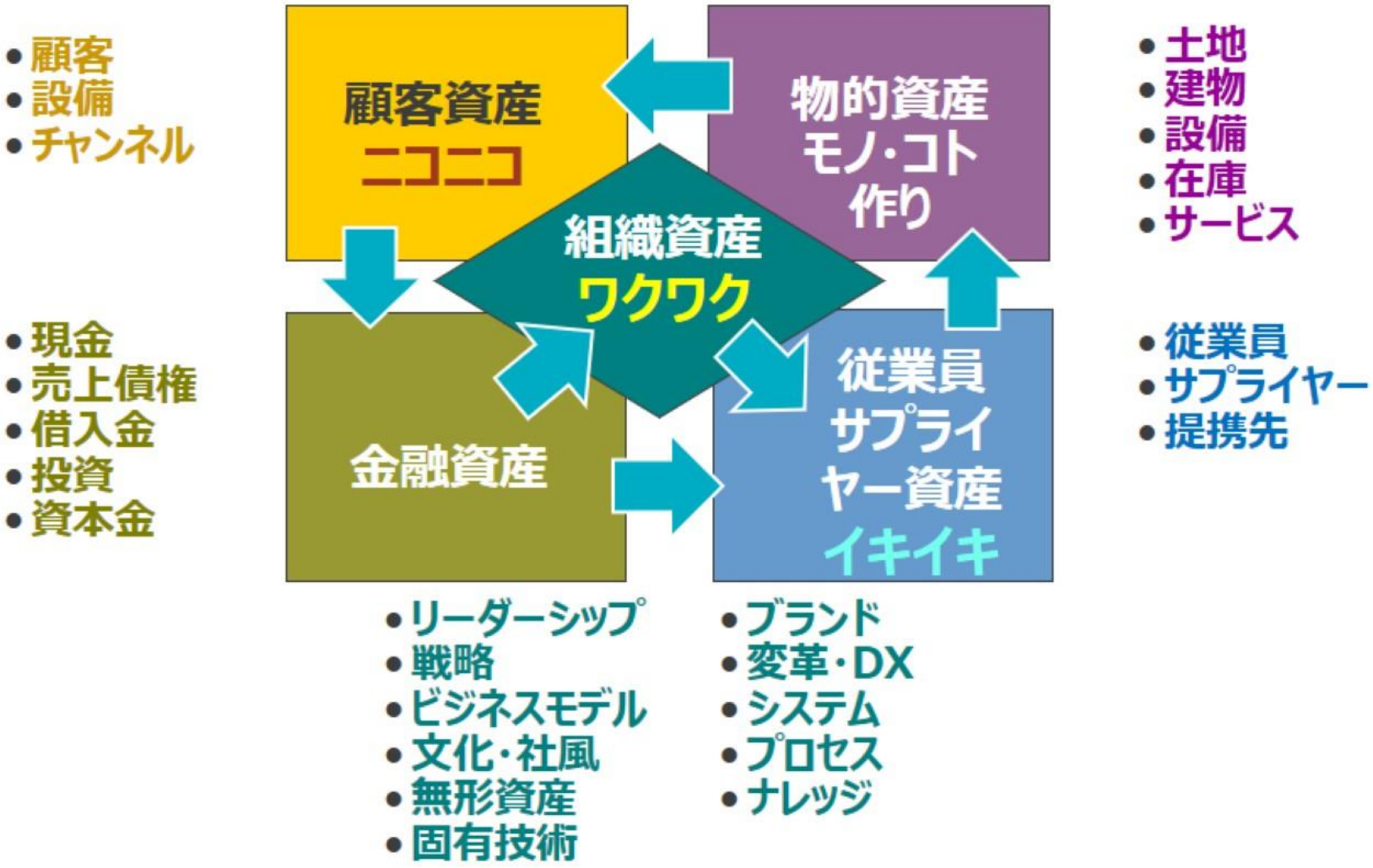
企業価値の源泉　～バリューダイナミクス～

価値を生み出す“資産”は変化している

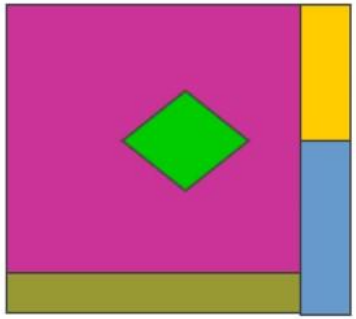


バリューダイナミクスとバリューチェーン

物的資産と顧客資産を、左右入れ替えてみると



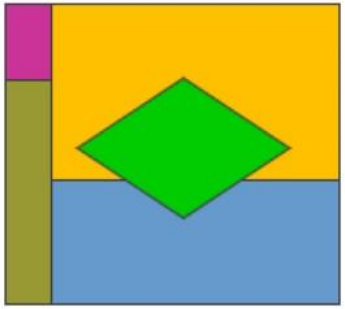
ビジネスモデルにより価値の源泉・リスクは異なる
～価値の源泉に影響を与える可能性がリスク



◆基盤エコノミー

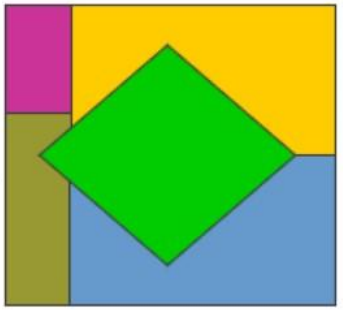
金属・鉄鋼・重工など
重厚長大産業

リスクあるところにチャンスあり
適切なガバナンスの下でリスクをマネージし、
競争力を強化し企業価値を生み出す



◆ニューエコノミー

顧客志向でIT、
知的財産を重視
◇例：デル
ITを活用し、製造、
サプライチェーン、顧
客をかつてない速さ
でつなぐことに成功



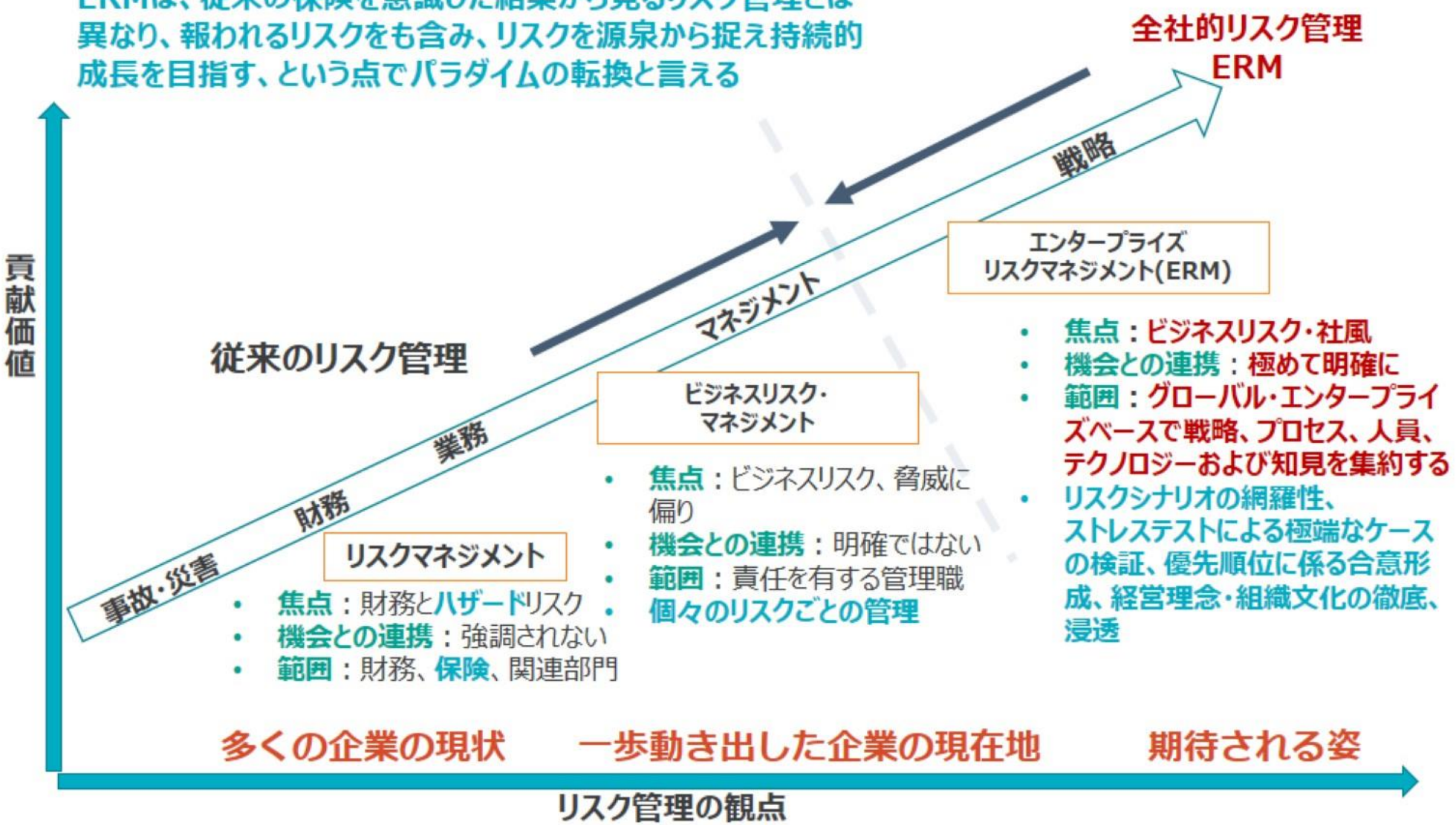
◆リスク新時代

未来指向のバリュー
ダイナミクスは,DX・
AI、サステナビリティ
経営重視や、GAFA
では顧客資産、従業
員/サプライチェーン資
産を支える組織資産
が大きい。

全社的リスク管理（ERM）への進化（1）

3 今までのリスク管理と全社的リスク管理（ERM）は、何が違うのか？

ERMは、従来の保険を意識した結果から見るリスク管理とは異なり、報われるリスクをも含み、リスクを源泉から捉え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る



protiviti

全社的リスク管理（ERM）への進化（2）

4 先を見越した全社的リスク管理（ERM)とは何を意味するのか？

攻めの観点も踏まえた全社的リスク管理：年次･中長期計画策定に戦略達成のためのリスク情報を盛り込むための体制が重要である。

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**	**中長期的な企業価値向上と戦略達成**に影響を与える要因をリスクとして対処
個別最適	**全体最適**	**エコシステム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･モニタリングのプロセスと連動** DXに伴う**データを活用**した継続的評価
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
ボトムアップの対応	**組織的説明責任**	**リスクアプローチ内部監査と継続的モニタリング**を組合わせ、リスク管理の有効性を評価

全社的なリスク管理の導入を検討する製造業企業に よくある課題意識

- **リスクテイク**をもっと進めるには何をすればいいのか、取締役会を説得するにはどうすればいいのか（A社　自動車）
- 全社的なリスク管理を進める上で、**社内の抵抗**にどう対処すればいいのか（B社　化学）
- 選択と集中を進める中で、全社的なリスク管理を**グローバルに展開し、共通言語化する**にはどうすればいいのか（C社　医療機器）
- **競争優位を確保**していくには、全社的なリスク管理をどう活用していけばいいのか（D社　楽器）
- 全社的なリスク管理の導入において、**本社機能や組織体制**はどうあるべきか（E社　タイヤ）
- 全社的なリスク管理の導入において、**社風やリスク感性**をどう高めていけばいいのか（F社　測量機器）

３．取締役会が果たすべきリスクマネジメントにおける役割・責務

～その役割・責務は如何にあるべきか
～ガバナンスコード、経産省CGSガイダンス、米国COSO、全米取締役協会が示す、取締役会に期待されるリスク監督のあり方をどう見るべきか

5 取締役会としての実効性の高い（リスクやリスク管理の）監督とは、何が期待されているのか？

取締役会のリスク管理に対する役割・責務：日本のガイダンス（１）ー再掲

再掲：コーポレートガバナンス・コード再改訂版には、リスク管理に関する重要な論点が、補充原則４－３④に追加されました。

【原則４－３．取締役会の役割・責務(3)】

取締役会は、独立した客観的な立場から、経営陣・取締役に対する実効性の高い監督を行うことを主要な役割・責務の一つと捉え、適切に会社の業績等の評価を行い、その評価を経営陣幹部の人事に適切に反映すべきである。

また、取締役会は、適時かつ正確な情報開示が行われるよう監督を行うとともに、内部統制やリスク管理体制を適切に整備すべきである。

更に、取締役会は、経営陣・支配株主等の関連当事者と会社との間に生じ得る利益相反を適切に管理すべきである。

補充原則 ４－３④

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り、取締役会はグループ全体を含めたこれらの体制を適切に構築し、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。

取締役会のリスク管理に対する役割・責務：日本のガイダンス（2）

経済産業省のCGSガイドライン改訂版（2022年7月19日）

コーポレートガバナンスの改革が会社の持続的な成長と中長期的な企業価値の向上へと寄与する経路（抜粋）

優れた社長・CEO を選ぶことなどにより、経営陣自体の強化を図ることで、中長期的な企業価値の向上を図る優れた社長・CEO ら経営陣を選び、適切なインセンティブを与えることで**適切なリスクテイクを促し**、その成果を評価していく仕組み（例えば、社長・CEO の指名の仕組み、後継者計画や候補人材の育成、インセンティブ報酬の活用など）を作ることは全ての企業において必須である。

そして、**この仕組みの中心は取締役会**である。

2.1取締役会の役割・機能

「取締役会による「監督」とは、単に執行にブレーキをかけたり、不祥事を自ら発見することではない。適切なリスクテイクに対する後押し、社内の経営改革の後押しや、リスクテイクをしないことのリスク（不作為のリスク）を提起することも含まれる。また、取締役会は資本市場からどう見られているかを意識し、自社の企業価値へ の評価を理解しなければならない。社外取締役が監督を行うに当たっては、株主等のステークホルダーの利益に資するかどうかの視点も持つことが重要である。関係者はこれらの点を広く認識する必要がある。」

取締役会のリスク管理に対する役割・責務：グローバルガイダンス（１）

COSOによるERM（2017）フレームワーク

- 内部統制フレームワークで知られるCOSOは、ERMのフレームワークも提唱。
- COSOERMフレームワークは、有効なERMを構築するための5要素・20原則を提示。
- 5要素のひとつ「ガバナンスとカルチャー」第１原則で、「取締役会によるリスク監視（リスクオーバーサイト）」の重要性を強調。

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

取締役会のリスク管理に対する役割・責務：グローバルガイダンス（２）

COSO ERM 原則１.「取締役会によるリスク監視を行う」が具体的に示すこと

取締役会は、適切なリスクテイクが戦略に反映されているか監視し、ガバナンスの責任を果たすことにより、経営者が戦略と事業目標を達成できるよう支援する。

監視責任と執行責任～リスク管理における役割

- **監視責任と執行責任の役割分担**、規定化、
- 取締役会の**諮問委員会としてのリスク委員会**へ監視責任権限委譲

取締役会のメンバー、特に社外取締役の資質

- スキル、経験および業務知識
- 極めて重視される独立性と社外性

全社的リスクマネジメントの活用～監視と執行の両面から

- **リスクマネジメント対応能力の向上～リスクテイクを支える仕組み**
- リスクマネジメントを、攻めと守りの両面から経営に活かす

組織が持つバイアスの管理

- バイアス（先入観、偏見等）を適切に見極める
- **バイアスの有無が問題ではなく如何に管理するかが重要**

取締役会のリスク管理に対する役割・責務：米国の取り組み（１）

リスク監視・監督（リスクオーバーサイト）とリスク管理（リスクマネジメント）の違いとは

リスクマネジメント

マネジメント・経営者の役割

戦略的優先事項の遂行や業績目標の達成にとって影響を与える重要なリスクの特定、優先順位付け、対応、管理および監視・モニタリングが含まれる

リスク・オーバーサイト・監視・監督

取締役会の役割

会社が重要なリスクを管理するプロセスを備え、ビジネス環境の変化に応じて継続的に改善されていることを判断するための取締役会のプロセス

米国SEC規則により、取締役会のリスク監視（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～）
具体的には、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、リスクを理解する上での取締役の資質、および許容しがたい過度のリスクテイクを助長することのないような報酬体系に関する報酬委員会の評価などについて開示する

取締役会のリスク管理に対する役割・責務：米国の取り組み（２）

取締役会のリスク監視10原則（全米取締役協会：NACD 2009）

1	企業の**成功要素**を理解する
2	**戦略の固有リスク**を評価する
3	**リスクオーバーサイト**に係る取締役会、各委員会の役割を定義する
4	リスク管理や内部統制が適切か、**提供される資源**が適切か検討する
5	取締役会に提供される**リスク情報**について、リスクの種類理解すると共に、執行陣と合意する
6	取締役会と執行陣が**建設的なリスクに関する協議**を行う
7	**企業風土とインセンティブ報酬**に係るリスクをモニタリングする
8	戦略、リスク、インセンティブへの準拠状況を**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リスクに関して検討する
10	取締役会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

取締役会のリスク検討テーマの例示

7

取締役会として、どのようなテーマを議論すべきなのか？執行のリスク管理にどの位踏み込むのか？

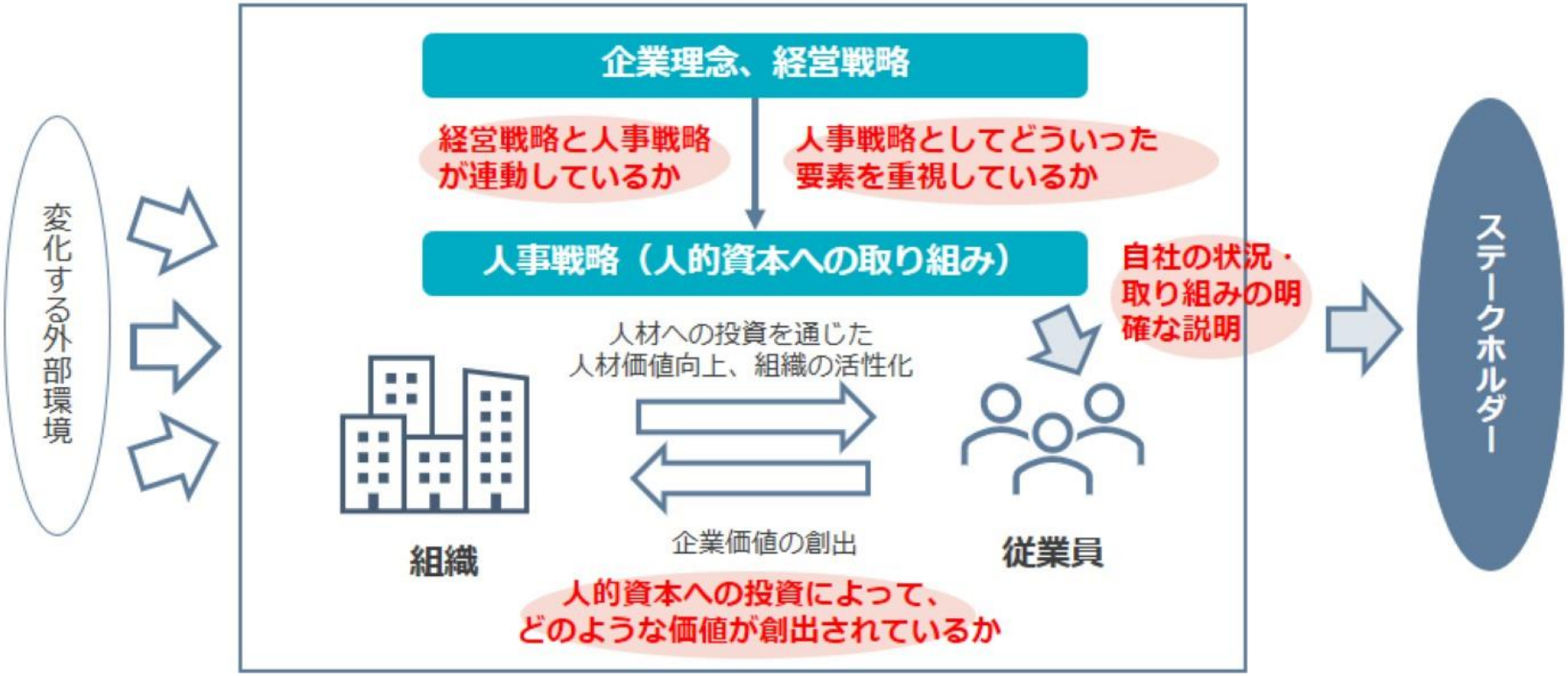
Vol.	Risk Oversight	関連分野
特別	地政学上の不安定さがゴールポストを再び動かす	
150	取締役会のテクノロジー・DXに対する感度を確保する	
149	取締役会におけるデータ・プライバシーに関する議論のフレームワーク	
144	エネルギー革命への参画	
141	ポストパンデミック	
140	職場の未来の再考	
131	オペレーショナル・レジリエンス	
116	将来へ備えるべきこと	
113	サイバーセキュリティ	
93	サプライチェーンリスク	
91	短期志向リスク	
89	リスクの網羅性を確保するには	
86	ブランドリスク	

凡例：ガバナンス・リスクマネジメント(内部監査を含む)、レジリエンス・変革、デジタル、ESG

出典：https://www.protiviti.com/JP-jp/taxonomy/term/3566

人的資本 ～ 企業として求められる対応

人的資本への注目が高まるなか、「人的資本の潜在力をどう可視化し、かつそれを組織としてどのように最大化させるか」、その結果どのような価値が創出されているか適切に把握し、ステークホルダーへの説明責任が求められている。

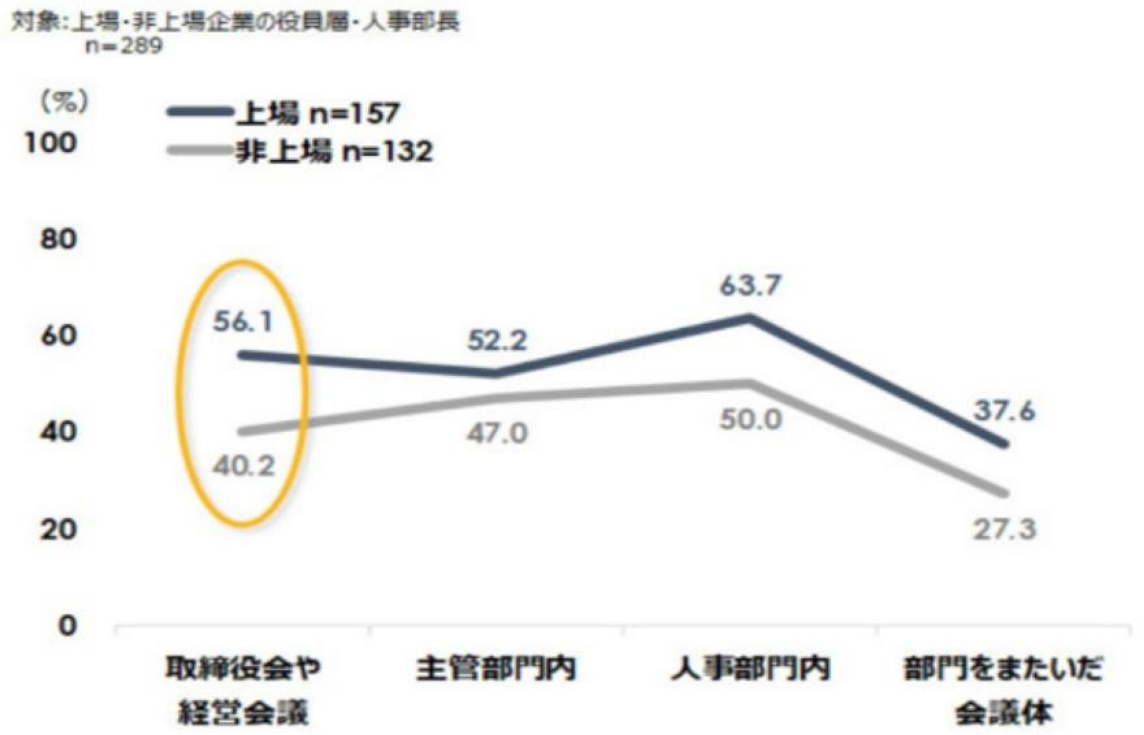


protiviti

取締役会と人的資本

取締役会における人的資本に係る議論は、まだ十分ではない

人的資本情報やその開示に関する社内の議論（上場企業・非上場企業別）



* 数値は下の（ ）内の6つの選択肢のうち、「最優先事項として議論されている」+「優先度高く議論されている」の回答割合
（最優先事項として議論されている ／ 優先度高く議論されている ／ 優先度は高くないが議論はされている／
あまり議論されていない ／ 全く議論されていない ／ 分からない）

（出所）人的資本情報開示に関する実態調査、パーソル総合研究所、2022.5

全社的リスク管理における日本企業の課題

～なぜリスク管理をするのか？リスクに対するマインドセット

8 日本企業のリスクマネジメントにおいてよくある課題とは？

リスクを回避するためだけのリスク管理か、更なるリスクテイクのためのリスク管理も含めるか

リスク分析、リスク対応検討を十分行い・・

リスクテイクする

リスクを回避する

protiviti

全社的リスク管理における日本企業の課題
～ガバナンスの視点から

8 日本企業のリスクマネジメントにおいてよくある課題とは？

COSO ERM 原則１．「取締役会によるリスク監視を行う」 が具体的に示すこと

- **監視責任と執行責任～リスク管理における役割明確化**
  - 監視責任と執行責任の役割分担、規定化、
  - 取締役会から、諮問委員会であるリスク委員会などへ監視責任の権限委譲
- **取締役会のメンバー、社外取締役の資質、スキル**
  - スキル、経験および業務知識
  - 極めて重視される独立性と社外性
- **全社的リスクマネジメントの活用～監視と執行の両面から**
  - リスクマネジメント対応能力の向上～リスクテイクを支える仕組み
  - リスクマネジメントを、攻めと守りの両面から経営に活かす
- **組織が持つバイアスの管理**
  - バイアス（先入観、偏見等）を適切に見極める
  - バイアスの有無が問題ではなく如何に管理するかが重要

protiviti

取締役会がリスクマネジメントにおいて果たすべき役割
～その実効性を高める6つのポイント

① 戦略とリスクは如何に統合・連携すべきか
② リスクテイクに関する建設的な議論は行われているか
③ リスクの定義が拡大するなかで、リスク管理体制は如何にあるべきか
④ リスクの洗出しは、トップダウン・ボトムアップにより網羅性を確保できているか
⑤ 全社的なリスク対応能力は如何に改善を進めるべきか
⑥ 自社のリスク文化は正しい行動を奨励できているか

リスクマネジメントにおける取締役会の実効性を高めるには

①　戦略とリスクの統合・連携

リスク管理が重要な経営プロセスと統合・連携しているか

1

リスク管理が重要な経営プロセスと統合・連携しているかを確認し、目的達成と戦略遂行への確信をさらに高める

主な統合・連携対象：中長期戦略策定、年次計画策定、業績管理、予算策定、人的資本投資、設備投資予算、研究開発投資、DX予算、ESG対応、M＆A、買収後の統合、内部統制システム、BCP、セキュリティ、コンプライアンス対応等

2

統合・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が、統合・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できているかを確認する。

事例：日立製作所：戦略とリスクの連携･統合 ～2022年3月期有報より

「事業等のリスク　リスクマネジメントについて」より

当社では、日々変化する経営環境を把握・分析し、社会的課題や当社の競争優位性、経営資源などを踏まえ、当社として備えるべき様々な「リスク」とさらなる成長「機会」の両面からリスクマネジメントを実施し、リスクをコントロールしながら収益機会の創生に努めています。

かかる多様なリスクに関して、各担当部署がリスクと機会の適切な把握・対応に努め、経営幹部への報告・経営戦略への反映を行っています。

特に、2022年4月から、当社経営における全社的リスクに係る重要事項の議論・決定の場として執行役社長を議長、CRMO（Chief Risk Management Officer）を副議長とする「リスクマネジメント会議」を新設しました。リスクを一元的・横断的に把握することで、成長戦略と連携した盤石な経営基盤の実現をめざしていきます。

「経営環境及び対処すべき課題」よ

注：ハイライトは講師がおこなったもの

protiviti

リスクマネジメントにおける取締役会の実効性を高めるには

② リスクテイクに関する建設的な協議

取締役会と経営者はリスク選好（リスクテイク）について合意しているか

1. 取締役会は、**企業が戦略として取るべきリスク、及び、そもそも回避すべきリスク**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. 取締役会は、ビジネスが**リスク選好指標の範囲内で実施**されているかをどうやって知ることができるかを確認する

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であるKRIが意思決定に重要な影響を与えるものとして示される。

望ましいカルチャーの醸成

経営理念・社是に則り、望ましいカルチャーを増進する行動指針を明示する。

カルチャーのスペクトル

カルチャーのスペクトルと、リスクテイクのパターン例

どちらかと言えば既存技術を最大限に活かす
現状維持型

慎重型 **中立型** **積極型**

今後はM&Aも大いに活用し積極的にリスクテイクを推進する
飛び地戦略型

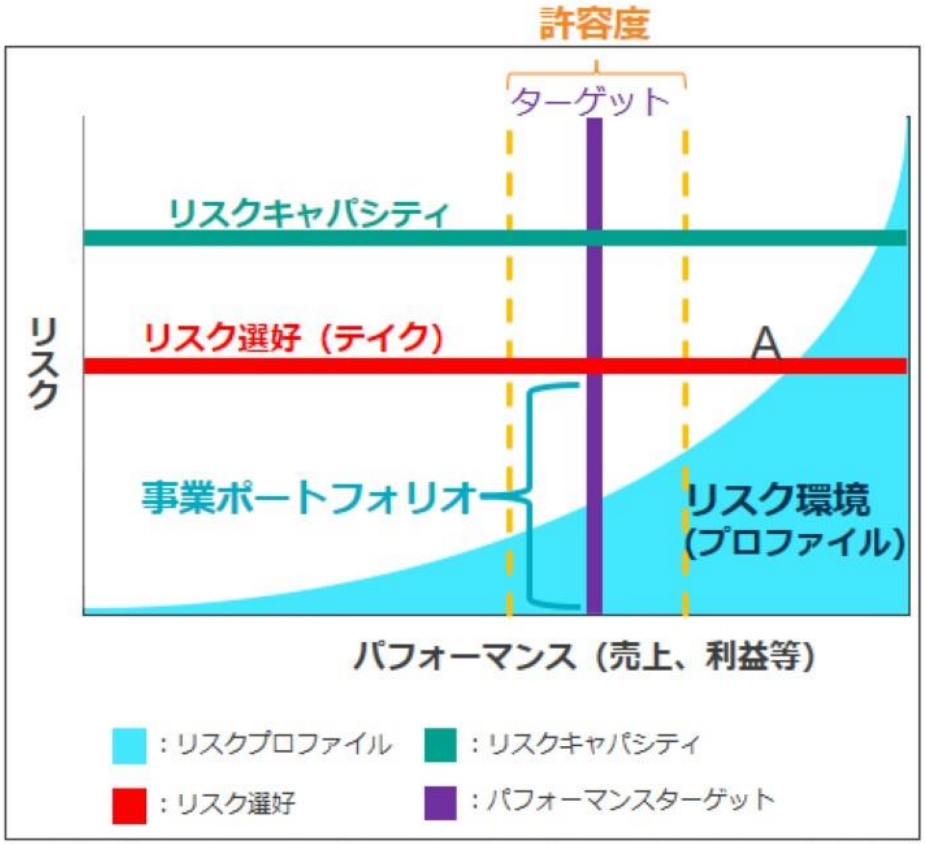
得意分野を中心にM&Aも進めながら新規事業を推進する
滲み出し型

リスク選好（リスクテイク）は適切なレベルか

戦略を策定し代替案を検討する際に、戦略に内在するトレードオフ・二律背反を考慮。
代替戦略にもそれぞれのリスクプロファイルがあり、プランB発動に備え戦略から生じる影響を見極める。

パフォーマンスとリスクの関係

- **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(環境)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
- **限界を超えたリスクテイクが必要なときもある。**
- **リスク選好の緻密さを向上するには、パラメータの設定と仮説指向によるKRIのリアルタイムモニタリングが効果的。**
  - **戦略パラメーター**
    新製品の追及、回避、資本的支出による投資、M&Aの実行
  - **財務パラメーター**
    最大限に許容可能な財務上のパフォーマンスにおける差異、ROAまたはリスク調整後のRAROC、ROIC、格付など
  - **業務パラメーター**
    環境規制要件、安全目標、品質目標、顧客集中度など



※各点のプロットは、定量的アプローチにも定性的アプローチも可能である。 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。

リスク選好とリスク選好指標の事例

経営者および取締役会は企業のリスク選好に関するさまざまな表明について検討する。

リスク選好ステートメントは、許容しうるまたは戦略に沿ったリスク、許容できないまたは戦略に沿わないリスク、そして、戦略・財務・オペレーションリスクのパラメーター3つの要素から構成される。

3要素	リスク選好ステートメントに含まれる表明の例
1. 許容しうるまたは戦略に沿ったリスク	• **市場シェア**：地域戦略を積極的に推進し、市場シェア目標（3パーセント増）を達成し、新興国を中心とした主要市場に投資・進出し、この戦略に内在するリスクを許容する。
2. 許容できないまたは戦略に沿わないリスク	• **レピュテーションおよびブランドイメージ**：自社のレピュテーションおよびプレミアムブランドとしてのイメージを毀損する状況・行動は避け、好ましくない状況が生じた場合、積極的に対応し、レピュテーションおよびブランドイメージを守る。 • **金融デリバティブ**：金融商品については、単純なスワップ・オプションに限定し、カウンターパーティもAA以上の格付けをもった者に限定する。
3. 戦略リスクパラメーター	• **投資の上限**：M&Aや投資については年間5億2500万ドルのフリーキャッシュフローを達成できるレベルに抑える。
財務リスクパラメーター	• **格付け**：負債格付けをA以上に維持する • **自律的成長性**：新規事業について、運転資本比率を1から1.5パーセント内におさめる。 • **財務的体力**：事業を遂行するにあたり、EBIT/利息比率を4から5パーセント内におさめる。
オペレーションリスクパラメーター	• **損失の上限**：税引前営業利益が4000万ドルを下回るような結果を回避するように事業活動を運営する。 • **環境を破壊しないビジネスモデル**：二酸化炭素排出の抑制を目指し、今後5年間にわたり、設備能力の拡張・改造に当たってはエネルギーコスト40パーセント削減を目標とする。 • **顧客依存度**：全売上高の10%以上を単一顧客が占めることのないようにする。

リスクマネジメントにおける取締役会の実効性を高めるには

③　リスク管理の体制の見直し

取締役会はリスクの監視のための体制構築を検討しているか

1. リスクマネジメントとは、**リスクテイク（リスク選好）**の方針の下で策定された戦略の遂行状況を示す業務目標を設定し、**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こと

2. リスク管理プロセスがどのように**整備、運用、評価**されているかを評価する

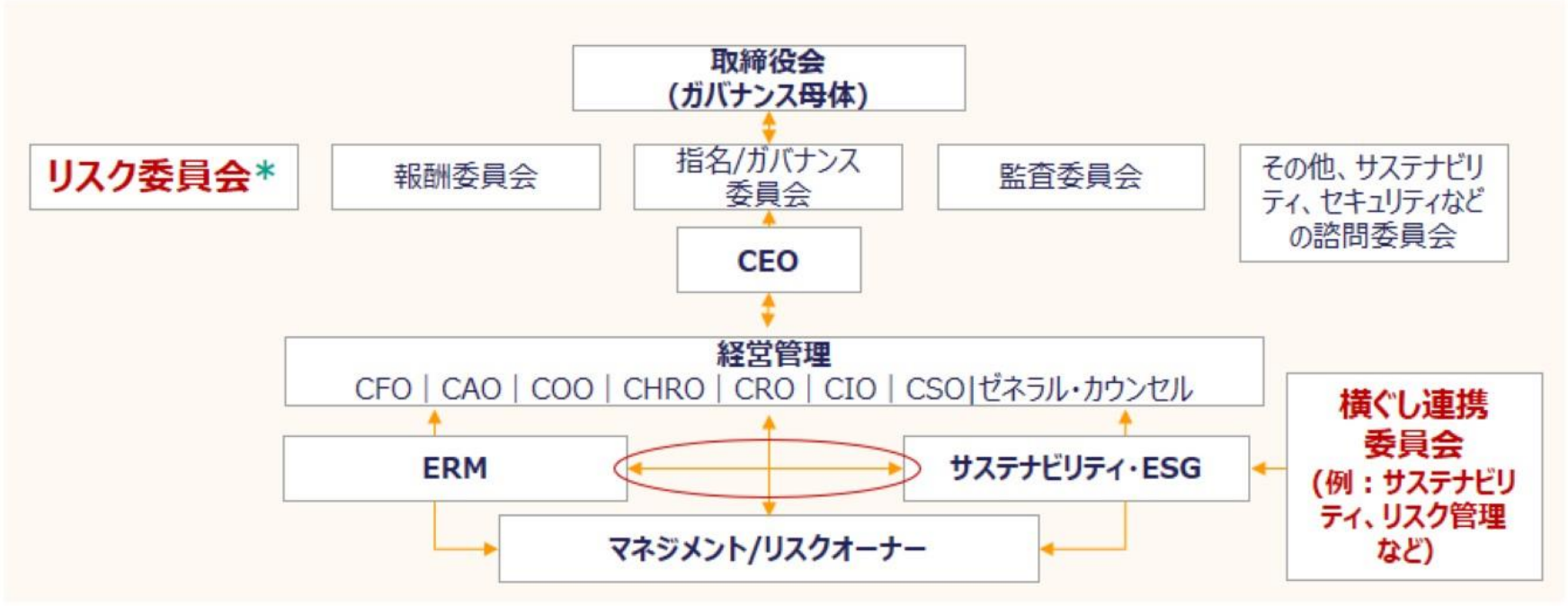
3. リスクの監視体制、運営の在り方は、企業規模、構造、複雑性、社風、重要リスク等の状況を考慮して、リスク管理委員会等を設置するなど、それぞれの企業で**最もふさわしいリスク管理とリスク監視の在り方**を決めることになる

4. **リスクの監視責任は、取締役会の全てのメンバーが負う**ものであり、取締役会がリスクの全容を把握するには、戦略に伴う重要なリスクを建設的に議論する必要がある。

取締役会の監視と責任～組織体制

リスクマネジメント部門や他の関連部門と、サステナビリティ部門の協業体制が確立していない企業は多く見かけるが、ガバナンス体制の中で、協力体制や情報・報告の流れを明確にしていくことが重要。

取締役会の諮問委員会型*に加え、執行陣を支える執行型のリスク委員会やESG委員会のいわゆる"横ぐし連携委員会"形態も有効。



＊OECDが、取締役会の諮問委員会としてのリスク管理委員会の設置を推奨、2023年より実施予定（日経新聞2022年10月10日より）

出典：COSO/WBCSDガイダンス一部加工

protiviti

グローバルガバナンスの方向性

- グローバルガバナンス強化にあたって、グローバル経営モデルを明確にする。
- ライン機能とコーポレート機能の最適なマトリックス型が最も有効。
- 各事業ユニットの成熟度に応じた”遠心力と求心力”のバランスが大切。

事業部門主導型

海外子会社の役割
- 現地の好機を感じ取って対応、成果を上げる自律拠点

イノベーション方式
- 各組織単位内で知識開発を行い、成果を個別に保有

権力と能力配分
- 各事業部門に分散
- 海外子会社は自立している、または各事業部門が管理

本社中央集権型

海外子会社の役割
- 親会社の戦略を実行する出先

イノベーション方式
- 中央で知識を開発して保有

権力と能力配分
- グローバル本社に集中
- グローバル展開
- 規模の経済重視

地域統括設置型

海外子会社の役割
- 事業戦略を実行する上で、地域統括会社の支援有効活用

イノベーション方式
- 中央で知識を開発し、海外の地域組織単位に移転

権力と能力配分
- 能力の中核部はグローバル本社に集中させ、他は地域統括会社に分散

トランスナショナル型

海外子会社の役割
- 海外の組織単位毎に**役割を分担**して世界規模で経営をコーディネート

イノベーション方式
- 全拠点分担の下、共同で知識を開発し、全拠点で分かち合う

権力と能力配分
- 分散
- 相互依存
- 専門化

protiviti

リスクマネジメントにおける取締役会の実効性を高めるには

④ リスクの洗い出し ～ 網羅性の確保とリスクの源泉モデルの活用が重要

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**などを明らかにする

2. **「影響大・発生可能性小」のテールリスク**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することもありうるため、**ストレステスト**なども考慮する

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

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**については、ストレステストなどを行い、レジリエンスの強さを理解し、必要な対応を行う

プロティビティが推奨するリスクモデル　～源泉系リスクモデルによるリスクの棚卸～

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。

A 外部環境リスク		B 業務プロセスリスク						C 意思決定情報リスク	
		(a) 財務		(b) 権限委譲		(d) ガバナンス		(a) 戦略	
1	競合他社	1. 価格		31	リーダーシップ不全	41	組織文化	73	外部環境モニタリング
2	顧客ニーズ	20	金利変動	32	統制不足	42	CSR	74	ビジネスモデルの陳腐化
3	技術革新	21	為替変動	33	アウトソーシング統制	43	取締役会の実効性	75	ビジネスポートフォリオ
4	外部環境への感応度	22	投資持分の価値変動	34	勤務評価基準	44	後継者計画	76	投資判断情報
5	出資者の動向	23	商品相場変動	35	変化への順応性	45	グループガバナンス	77	組織構造の戦略整合性
6	資本調達	24	金融商品変動	36	縦・横の組織内コミュニケーション	(e) 評判		78	KPIの戦略整合性
7	政体の安定性	2. 流動性		(c) 情報処理/IT		46	コーポレートブランド	79	経営資源の最適配分
8	外交関係	25	資金不足	37	データの完全性	47	投資家とのエンゲージメント	80	戦略の外部環境適合性
9	関連法規	26	機会損失	38	情報セキュリティ	(f) 誠実性		81	製品ライフサイクルを考慮した戦略
10	規格変更	3. 与信		39	情報の可用性	48	経営者の不正	(b) 外部報告	
11	業界特性	27	債務不履行	40	情報技術のインフラストラクチャ	49	従業員の不正	82	外部報告の虚偽記載
12	地域特性	28	取引先集中			50	第三者の不正	83	会計基準・見積もり
13	商慣行	29	決済未了			51	過失	84	減損
14	金融市場	30	担保価値損失			52	無権限者による経営資源の使用	85	財務報告の内部統制有効性評価
15	災害・壊滅的損失			(g) 業務/運営				86	開示統制の整備運用
16	気候変動			53	顧客満足	63	流通チャネルの機能不全	87	税務戦略情報
17	少子高齢化			54	人的資源・資質	64	提携先の内部統制	88	年金基金情報
18	サイバー攻撃			55	知的資産の維持活用	65	広義のコンプライアンス	(c) 業務/運営	
19	感染症			56	製品開発力	66	特定の経営資源への依存	89	予算・計画統制
				57	業務効率	67	製品・サービスの欠陥	90	価格設定
				58	生産能力	68	環境への負荷・対応	91	契約履行情報
				59	取引拡大への対応能力	69	労務問題	92	業績評価指標の有効性
				60	期待パフォーマンスとのギャップ	70	人権問題	93	財務業績偏重による経営管理
				61	サイクルタイムにおける業務効率	71	健康・安全管理		
				62	サプライチェーン	72	商品ブランド		

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93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

リスクマネジメントの実効性を高めるには

⑤　リスク対応能力・成熟度の継続的な改善

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. **リスクオーナーや担当部署（第1線）**が**十分なリスク管理能力**を有しているか、その**成熟度**を高めるための**必要な継続的改善**がなされているか取締役会は確かめる
2. **全社的なリスクを管理・監視する強固なプロセス（第2線・第3線）**が確立されているか確かめる
3. **取締役会へのリスク報告が適時かつ信頼性**をもってなされているか確かめる

成熟度の高いERMとは：成熟度モデル

多くの企業は、ERM（全社的リスクマネジメント）のプロセスを有しているが、その成熟度は異なる。
更なる成長を目指し、より多くのリスクをとる企業は、より成熟度の高いERMが期待される。

品質の向上 / リスクの増加

成熟度レベル	能力の特徴	能力の属性
最適化 レベル5	（継続的フィードバック） リスク管理が**競争優位性の要素**として活用される	• 全社的リスク戦略・リスクテイクの推奨 • **企業カルチャーに基づく高いリスク感性とリスク対応** • 知見の蓄積と共有
マネジメント レベル4	（定量化） リスクが数値により測定され、**全社で包括的に管理**される	• 厳密な測定方法/分析 • **リスクとリターンのトレードオフについての討論** • **望ましいリスクカルチャーの醸成**
定義・制度化 レベル3	（質的・数量的） 方針・プロセス・リスク・基準が定義され、制度化される	• **全社的なプロセスとリスクの標準化** • 次段階のインフラ要素 • 厳密な方法論
連続・反復 レベル2	（直感的） 反復可能なプロセスであるが、個人の能力に大きく依存	• 適任者の選任 • 共通言語・定義された作業 • 初期のインフラ要素
初期段階 レベル1	（断片的、混沌） 英雄的要素へ依存、制度的な能力の欠如	• 責任が不明確 • 場当たり的な対応 • 主要な人へ依存

リスクマネジメント能力の成熟度の改善

- リスクマネジメント能力・インフラの現状評価
- リスクマネジメント能力の目標設定とギャップ分析
- アクションプランの策定・導入

能力の成熟度

能力レベル	能力の定義
最適化	全社レベルでの継続的なコントロールの改善
マネジメント	全社的にリスクが数値として管理、“責任能力の連鎖”
定義・制度化	方針・プロセスが定義され制度化される“認証の連鎖”
連続・反復	人的に依存しプロセスが確定して反復して使用される
初期段階	コントロールは優先ではない人の英雄的要素に依存

リスクマネジメントプロセス評価

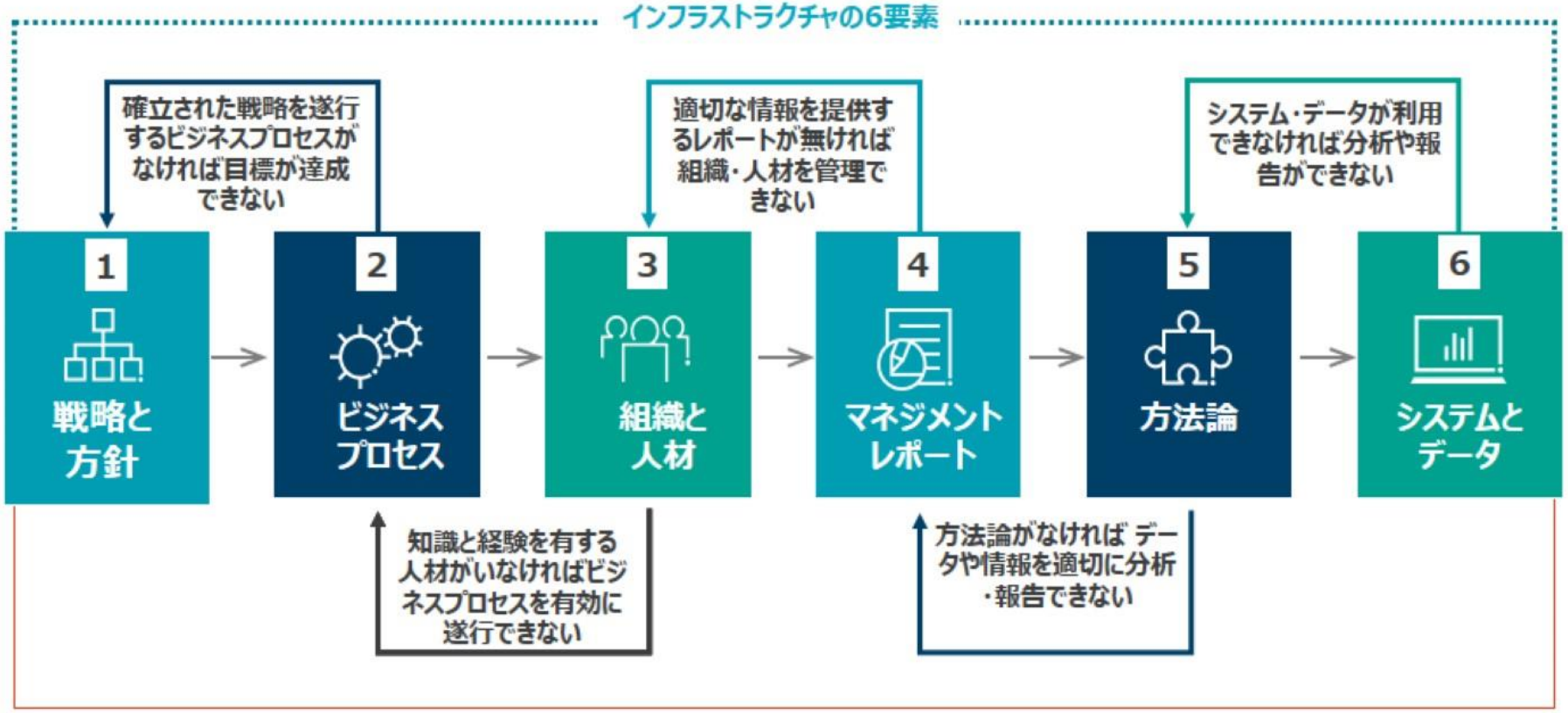
1.コンプライアンス	6.財務報告
2.信用リスク	7.法令改正
3.市場リスク	8.人材
4.テクノロジーリスク	9.アウトソース
5.投資判断	10.キャッシュフロー

protiviti

組織的なリスク対応能力改善のためのフレームワーク

経営インフラストラクチャの6要素

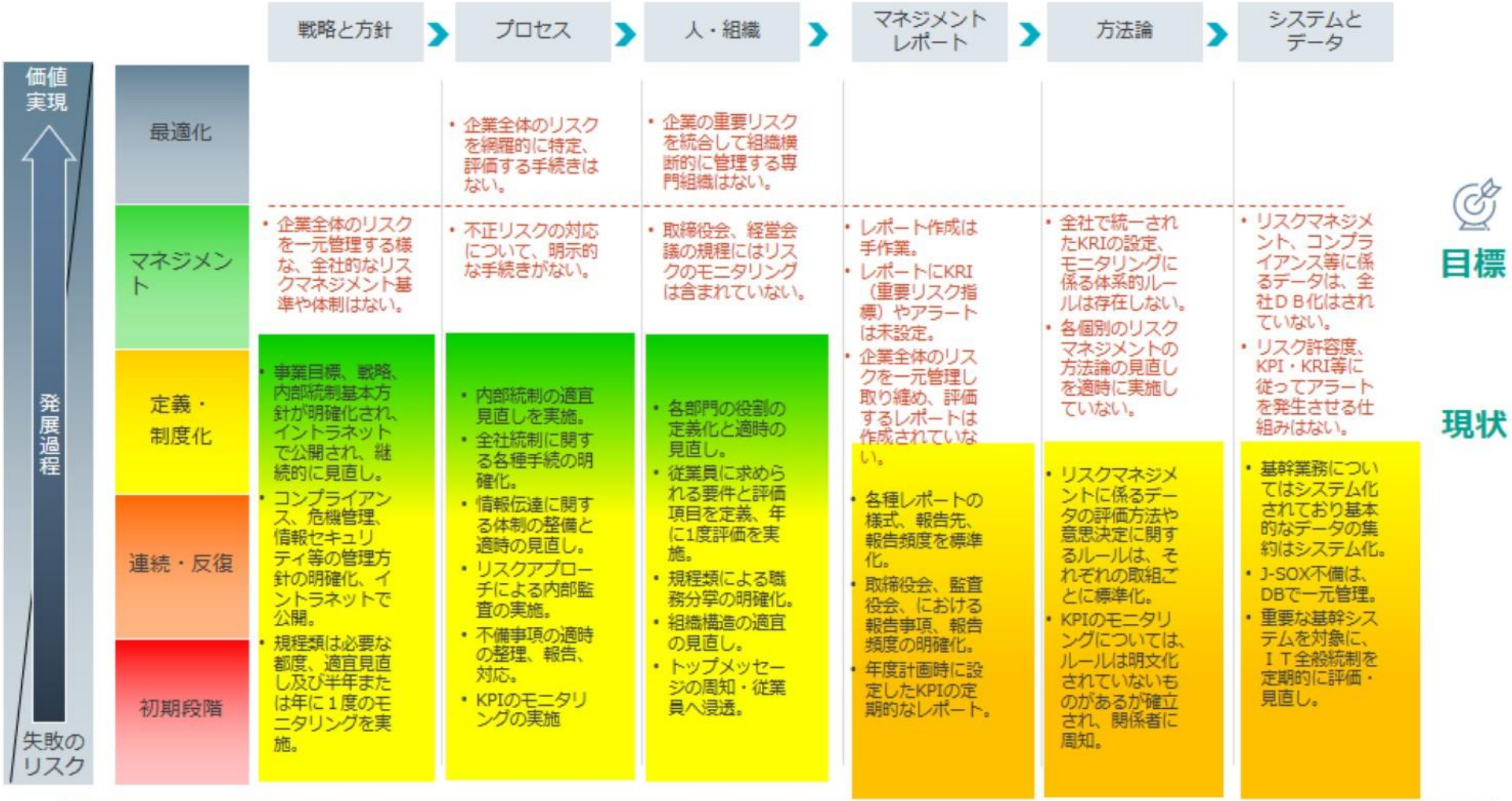
経営インフラストラクチャの6要素は管理態勢を構築するための鍵となる6要素の考え方を活用することで現状の課題の体系的な把握が可能



protiviti

リスク管理能力の成熟度評価例

リスクマネジメントのインフラ6要素は、成熟度を検討する際に現状と目標のギャップを特定するために活用され、リスクの取組み分野ごと、またはプロセスごとに作成することも可能。



protiviti

リスクマネジメントにおける取締役会の実効性を高めるには

⑥　全社リスク管理で最も大切なこととは

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。

protiviti

望ましいリスク文化・カルチャー

望ましいリスク文化・カルチャーを形成する「ドライバー」要素は、**役員や従業員がどのようにリスクを認識し、リスクと機会を判断するか**に影響を与える。

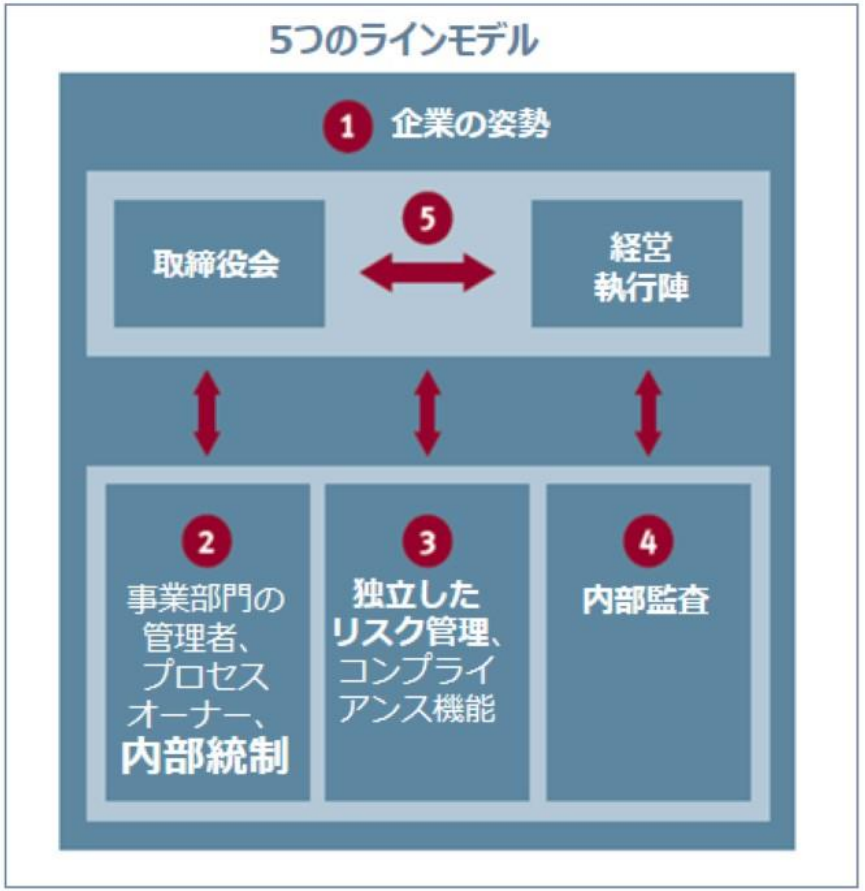
リスクカルチャーのキードライバー

望ましいリスク文化・カルチャーの発揮・実現状態

- **シニア・リーダーシップ**の有効かつ一貫した**ロールモデルの発揮**、日々の行動におけるコア・バリューの実践
- **リスク対応方針が明確・適切かつ十分な伝達**
- **タガに固執することなく、透明性があり複数視点からの意思決定**
- 先入観や、特定意見に対する**建設的なチャレンジ・反対意見の尊重**
- あらゆるレベルでの**高い水準の分析的洞察力と情報共有の**実践
- **脅威や懸念の迅速なエスカレーション**の実行
- **失敗は重要な学習機会**へと活用
- **すべてのメンバーが「正しいことをする」**のを**奨励するインセンティブ**
- リスクに関連する外部のステークホルダー（顧客、市場、社会など）に焦点

5線モデルで考える ～「企業の姿勢」の重視

- ガバナンス、リスク管理、内部統制が有効に機能するには経営理念を基盤とする**「企業の姿勢」**が最重要。
- 「企業の姿勢」とは、取締役会、経営トップ、監査役員、中間層、現場の姿勢の**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**との前提に立たざるを得ない。
- 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**事が大切
- トーンを合せるには、**「共通言語」を構築・浸透させることが必要不可欠。**
- **「共通言語」**とは、**企業の姿勢・バリュー・理念・リスク管理方針・役割分担・リスク定義・許容度・モニタリング・報告等の頑健な仕組み**の総称



持続的成長に向けて：

トップの姿勢、悪い知らせが疎まれない“空気”、タイムリーなコミュニケーション、節度あるプレッシャーとインセンティブ、KPI/KRIによるリアルタイムモニタリングによる牽制と発見、カルチャーの推進、多様な価値観・ベストプラクティスが共有され、風通しのよさや、倫理的行動が徹底される
ー社是を通して以心伝心が実現できるー組織風土づくり

protiviti

ご参考：全社的リスク管理（ERM）導入アプローチ

全社的リスクマネジメント導入へのアプローチは、リスクマネジメントのビジョン設定を含め、大きく４つのフェーズにより構成

1）リスクマネジメントのビジョン
- リスクマネジメントの目的を明確にする

2）全社的リスク評価（ERA)
- 管理すべきリスクの特定・評価・優先順位づけ、対応方針決定を実施する

3）ギャップ分析
- 優先順位の高いリスクにおけるリスク対応管理能力の評価・ギャップ分析を実施し、リスク管理能力を高めるための　アクションプランを策定する

4）導入・実行・モニタリング
- 全社的なリスク監視体制の設計・インフラ構築・モニタリングを実施する

●ERM導入アプローチ

protiviti

Face the Future with Confidence®

protiviti®