一橋大学財務リーダーシップ・プログラム　B

リスクマネジメント（ERM）の最新動向と留意すべき方向性

神林比洋雄
プロティビティLLC　会長
2017年12月23日

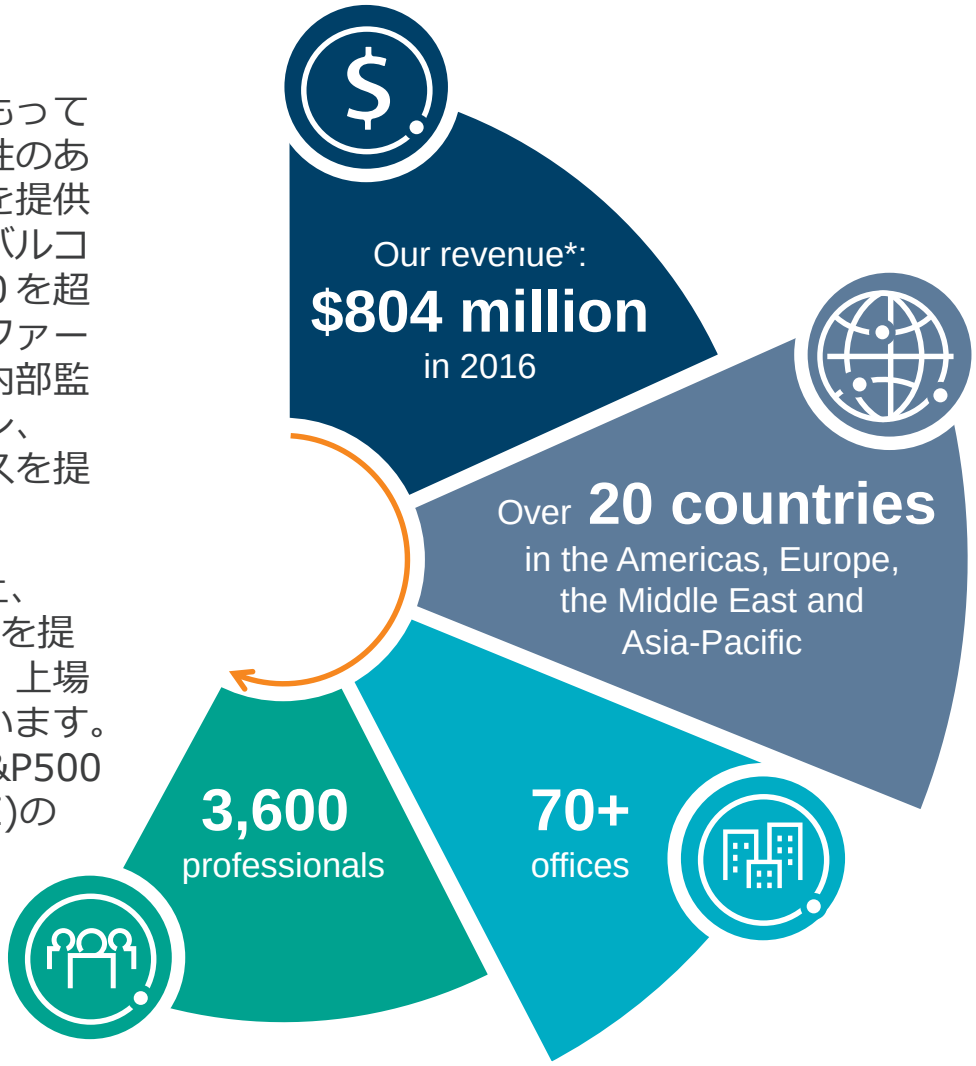
protiviti
Face the Future with Confidence

Internal Audit, Risk, Business & Technology Consulting

プロティビティのご紹介

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*4,600*名。*2015*年度の売上は *865*百万米ドル。

protiviti

今回の講義の目的

■ 講義のテーマ
- 戦略および目標達成を支援するリスクマネジメントとは

■ 講義の目的
- 以下の内容を理解し、自社・自部門の方針・目標達成に活用頂く
  戦略および目標達成とリスクマネジメント
  リスクマネジメントのフレームワーク（COSO ERM）

■ 講義の内容
- リスクマネジメントの基本
- リスクマネジメントのPDCAの検討、協議
- 目標達成を支援するリスクマネジメントの具体的なフレームワーク
- 不正リスク対応

問（1）目標達成に影響する不確実性(リスク)について

皆さんの企業グループを取り巻く不確実性（リスク）は、
ここ10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

protiviti

問（2）　“リスクテイク”について

皆さんの会社では、“取るべきリスク”を取っている、とお考えですか？

1. 大いに取っている
2. まずまず取っている
3. 十分な情報はないが、多分取っていると思う
4. 十分な情報はないが、多分取っていないと思う

アジェンダ

1．リスクとは何か
2．取るべきリスクを取るには
3．リスクへの対応は十分か
4．新COSO ERMフレームワーク
5．不正リスクへの対応
6．まとめ

1. リスクとは何か

リスクとは

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）　自然災害などによる損害をベースにした**結果系分類**、いわゆる怖いもの
ⅱ）　外部・内部要因からみたリスクの源泉に焦点を当てた**源泉系分類**
ⅲ）　「報われるリスク」（投下経営資源より成果が大きくなる）と「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）で、**リスク管理の成果**に焦点を当てるもの＊

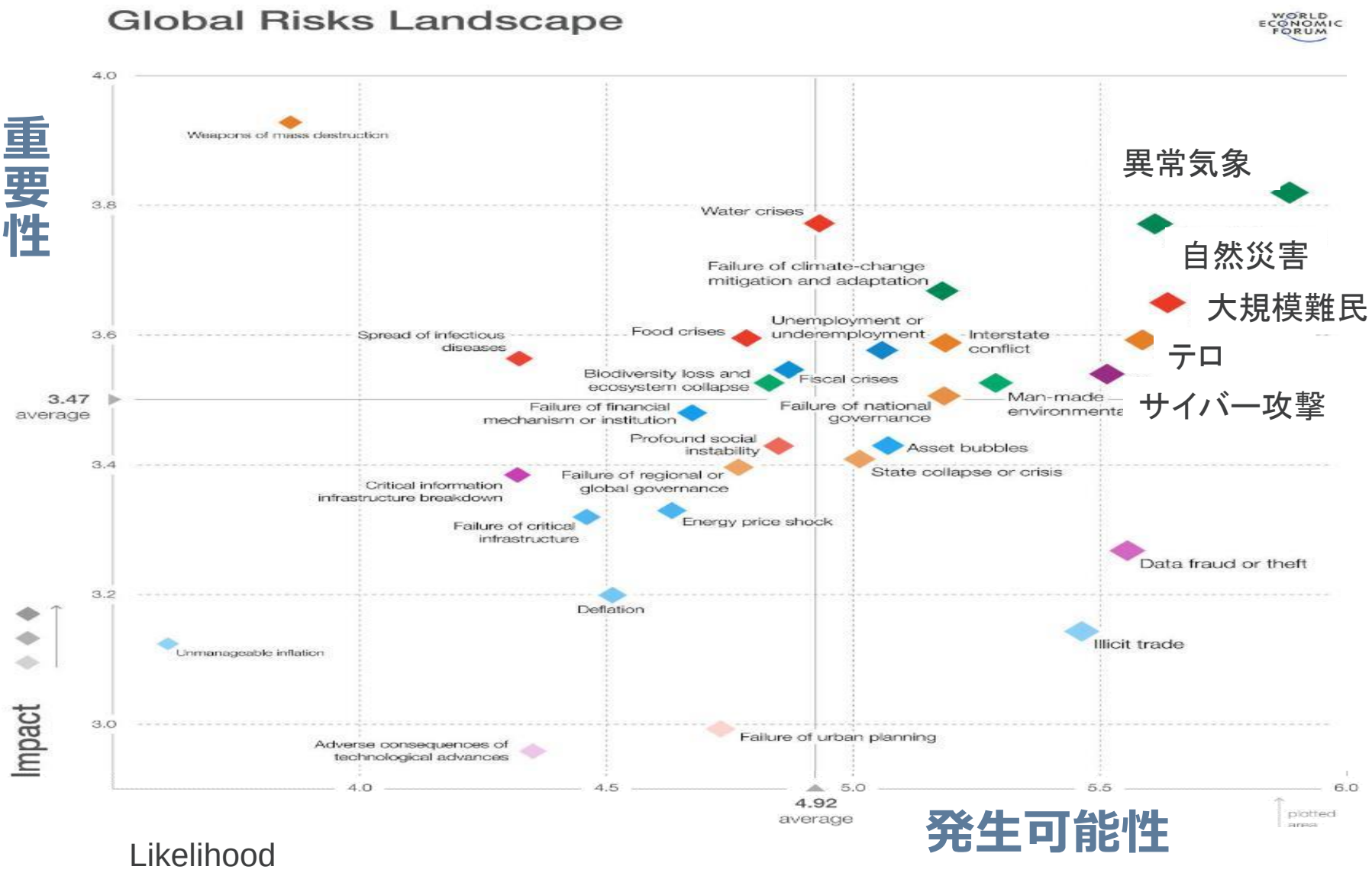
ⅲ）の例：

- 経営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「報われないリスク」との“思い込み”にとらわれない**
- **「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**

＊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

結果系のリスク　～　ダボス会議　2017　リスクレポート



protiviti

源泉系によるリスク調査

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（2016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、下線はリスクの源泉

1. 市場の動向が、成長の機会を著しく妨げる　（2 位　外部環境）
2. 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　（1位　外部環境）
3. 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　（3位　外部環境）
4. 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　（6位　戦略）
5. 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　（5位　業務）
6. 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　（4位　戦略）
7. 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　（8位　外部環境）
8. 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　（9位　ガバナンス）
9. 変化に対する抵抗が、必要な調整の妨げとなる　（7位　ガバナンス）
10. 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　（10位　業務）

このトップ10リスクの源泉を見てみると、

- 外部リスク：4、内部リスク：6（戦略リスク：2、ガバナンスリスク：2、業務リスク：2）
- 「報われるリスク」：7、「報われないリスク」：3

東証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」（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り得るものであるが、取締役会は、これらの体制の適切な構築や、その運用が有効に行われているか否かの監督に重点を置くべきであり、個別の業務執行に係るコンプライアンスの審査に終始すべきではない」（補充原則4－3②）

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ており、まさにリスクオーバーサイトの在り方そのものといえる。**

- **コンプライアンスや財務報告リスクに言及し、「報われないリスク」を対象にしている一方で、「リスクテイクを支える環境整備」、「先を見越したリスク管理体制」で示されるリスクには「報われるリスク」の意味合いが強く感じられる。**

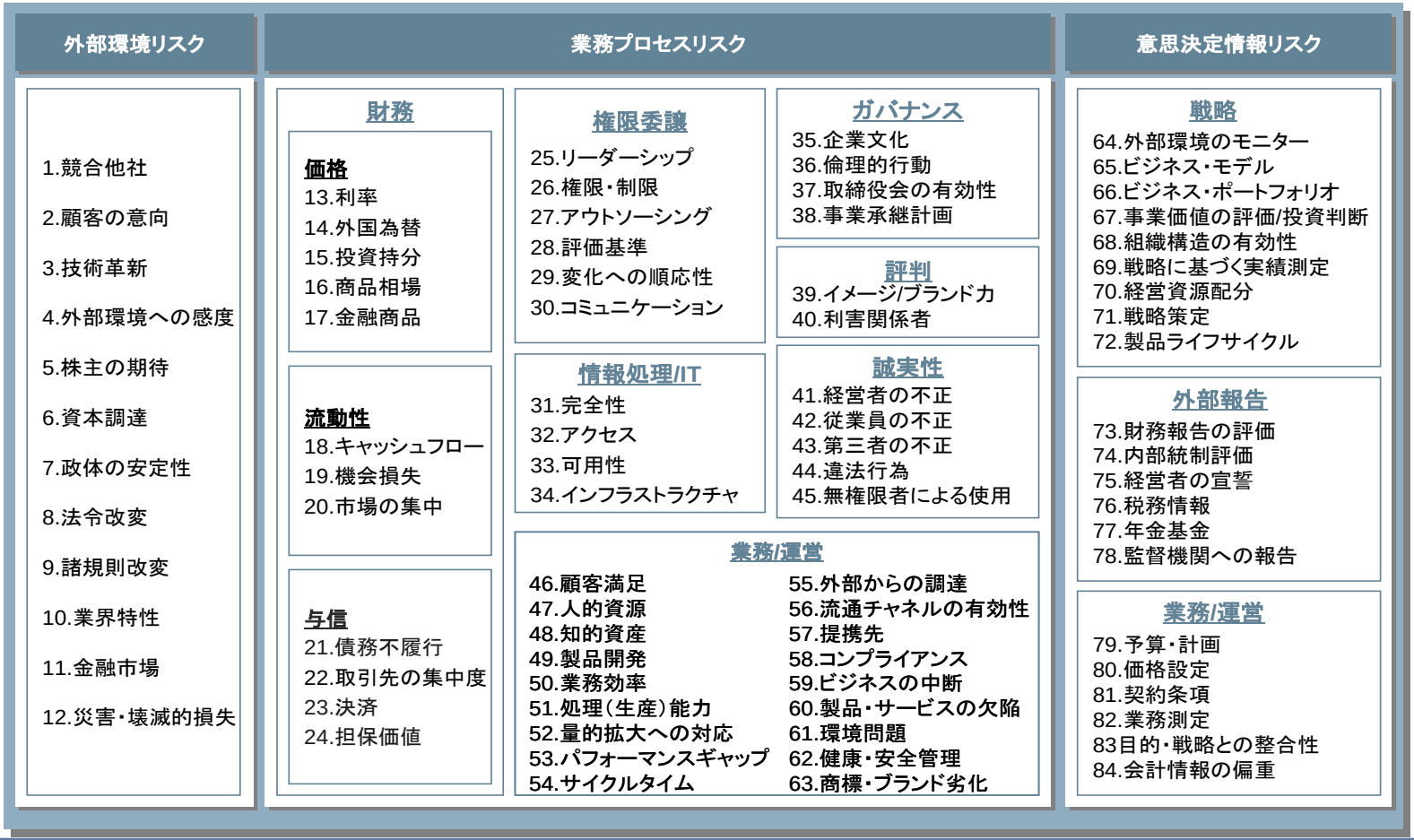
問（3）リスクの定義について

皆さんにとってリスクとは何でしょうか、
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
2. コンプライアンスに反する要因
3. 戦略および事業目標の達成を阻害する要因
4. 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

リスクを体系的に洗出す　(プロティビティビジネスリスクモデル)

- 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



protiviti

BRMのリスク定義書（抜粋）

業務プロセスリスク		
業務／運営リスク	46. 顧客満足	顧客満足に焦点を当てていないために、顧客の期待、または、期待以上に応えることができないリスク。
	47. 人的資源	会社の主要な従業員が、業務上不可欠な知識、技能及び経験を有していないために、想定したビジネスモデルの遂行と重要な事業目的の達成が脅かされるリスク
	48. 知的資産	全社的にナレッジを記録し、制度化するプロセスが存在していない、または、有効でないため、結果として、対応の遅延、高コスト発生、エラーの繰り返し、能力・技術開発遅延、成長の抑制や従業員の士気低下等が発生するリスク
	49. 製品開発	製品開発が効果的でないため、長期に亘り継続的に顧客のニーズを満たすまたは超えることができなくなるリスク
	50. 業務効率	非効率な業務により、競争相手や世界的なレベルの会社が提供するコストレベル以下で製造やサービス提供が出来ないリスク
	51. 処理（生産）能力	生産能力の不足が顧客の需要を満たさない、または過剰な生産能力が高コストを招き競争優位性を維持できないリスク
	52. 量的拡大への対応	より大きな取引量に応じて、又は、より大きな売上高に対する費用の償却において、業務方法を変更しより効率的に業務を遂行することができないリスク。その結果、会社が競争力を持ちつつ利益マージンを生み出すことができないという規模の不経済が生じる。
	53. パフォーマンスギャップ	会社の実際の業務が想定したとおりに遂行されないために、品質、コストあるいはサイクルタイムといった点に関して世的な水準でのパフォーマンスをあげることができず、会社の製品あるいはサービスに対する需要が減少するリスク

源泉系のビジネスリスクモデル～7業種80社の有報・事業等リスク

【統合版／FY2016】

リスク名の右側は登場回数。回数が多いほど緑色になる。

80 社

食料品・化学・医薬品・機械・電気機器・卸売業・銀行業

A 外部環境リスク

1	競合他社	182
2	顧客の意向	141
3	技術革新	27
4	環境感度	29
5	株主の期待	29
6	資本調達	128
7	政体安定	109
8	法令改変	557
9	諸規則改変	281
10	業界特性	10
11	金融市場	365
12	災害・壊滅的損失	708
13	サイバー攻撃	81
14	気候変動	17
15	商慣行	3
16	規格変更	28
17	少子高齢化	23
18	地域特性	92
19	経済環境	100

新たなリスク

B 業務プロセスリスク

(a) 財務

1. 価格

1	利率	140
2	外国為替	299
3	投資持分	102
4	商品相場	58
5	金融商品	31

2. 流動性

1	キャッシュフロー	46
2	機会損失	9
3	市場の集中	0

3. 与信

1	債務不履行	163
2	取引先の集中度	6
3	決済	13
4	担保価値	11

(b) 権限委譲

1	リーダーシップ	2
2	権限・制限	0
3	アウトソーシング	30
4	評価基準	0
5	変化への順応性	3
6	コミュニケーション	0

(c) 情報処理/IT

1	完全性	15
2	アクセス	413
3	可用性	521
4	インフラ	483

(d) ガバナンス

1	企業文化	0
2	倫理的行動	66
3	取締役会の実効性	0
4	事業継続計画	24

(e) 評判

1	ブランド力	165
2	利害関係者	2

(f) 誠実性

1	経営者の不正	0
2	従業員の不正	2
3	第三者の不正	21
4	違法行為	636
5	無権限者による使用	4

(g) 業務/運営

1	顧客満足	3	11	流通チャネルの有効性	78
2	人的資源	121	12	提携先	84
3	知的資産	187	13	コンプライアンス	68
4	製品開発	51	14	ビジネスの中断	5
5	業務効率	18	15	製品サービスの欠陥	164
6	生産能力	97	16	環境問題	435
7	量的拡大対応	1	17	健康・安全管理	94
8	Pギャップ	97	18	商標・ブランド劣化	0
9	Cタイム	11	19	労務問題	95
10	外部からの調達	258	20	過失	20

C 意思決定情報リスク

(a) 戦略

1	外部環境のモニター	2
2	ビジネス・モデル	5
3	ポートフォリオ	23
4	事業投資判断	138
5	組織構造の有効性	0
6	戦略に基づく実績測定	0
7	経営資源配分	25
8	戦略策定	36
9	製品ライフサイクル	3

(b) 外部報告

1	財務報告の評価	0
2	内部統制評価	8
3	経営者の宣誓	2
4	税務情報	125
5	年金基金	0
6	監督機関への報告	0

(c) 業務/運営

1	予算・計画	1
2	価格設定	165
3	契約条項	54
4	業務測定	0
5	目的・戦略との整合性	0
6	会計情報の偏重	0
7	会計基準・見積もり	40
8	減損	33

protiviti

重要なリスクとは～新たなリスクマップと逆説シナリオの特定

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

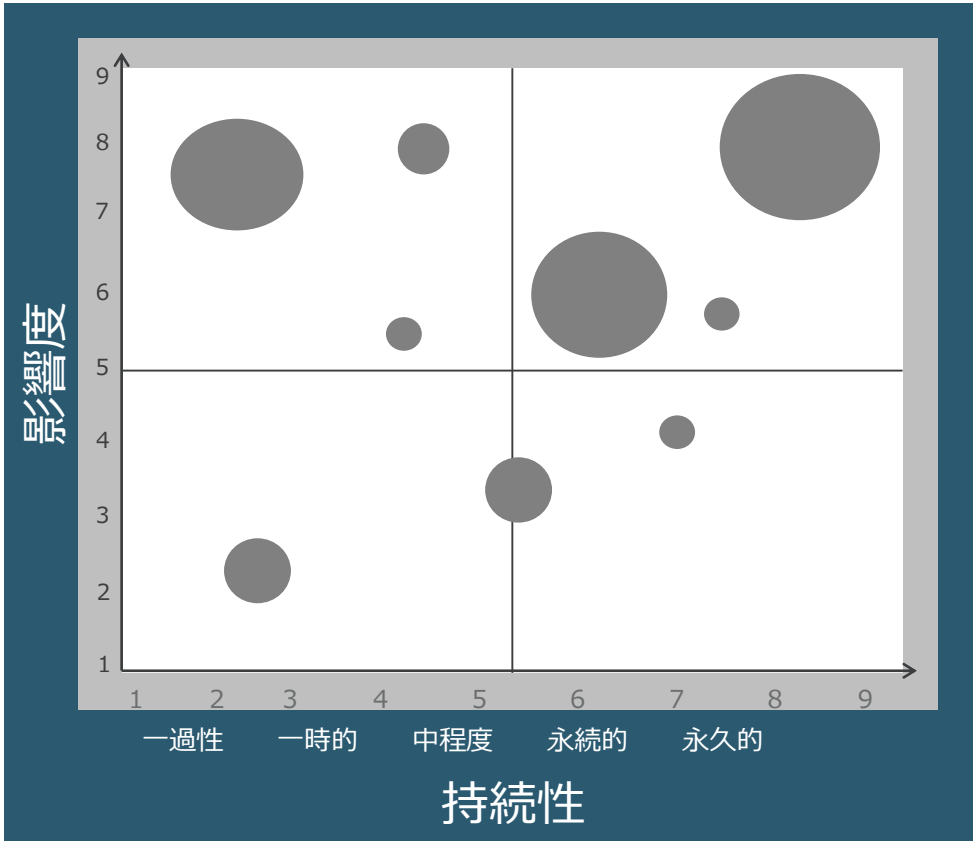
持続性

●特定された期間、全組織あるいは部分的に、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

不確実性、リスク、ERMについて

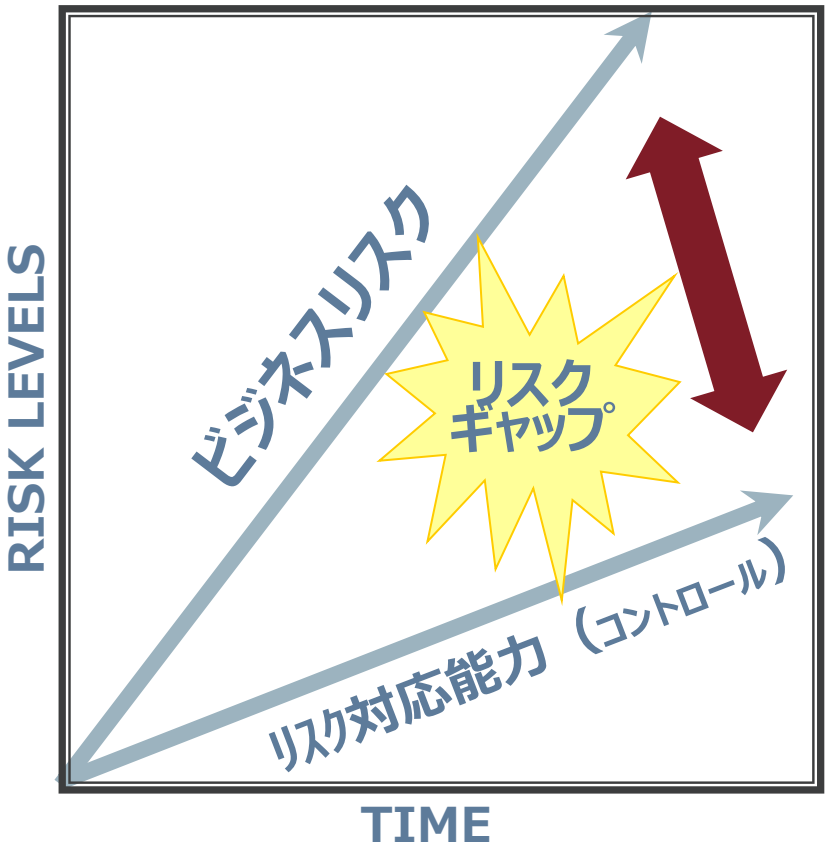
～新COSO･ERMフレームワーク2017より～

- **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」
  「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・企業価値をいかにバランスさせるか、である。経営上最大ともいえるこの問いに応えるのがERMの真髄。
- **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）が大きくなり、許容範囲を超える
- 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？

protiviti

日本企業のリスクマネジメント・内部統制の高度化対策

1．リスクマネジメント・内部統制の目的の明確化とグループ展開

- リスク対応としての内部統制の在り方＝**目的➡戦略➡リスク➡内部統制**

2．リスクの定義の拡大と共通言語の確立

- **リスクの定義**、全組織を通じての**共有と共通認識**
- **リスク選好**と**リスク許容度**

3．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**を強化
- **統合報告におけるリスクテイクと企業価値向上**へのシナリオの説得力
- 長文式監査報告・**KAM**におけるリスク認識の透明性と監査人との合意形成
  （減損、税金、収益認識等、またロールスロイスの監査報告書にはリスクマップが記載されている）

protiviti

2. 取るべきリスクを取るには

問（4）　リスク選好

皆さんの会社のリスク選好は、次のどれが最も近いと思われますか？

1. どちらかと言えば、既存（要素）技術を最大限に活かす現状維持型である
2. 得意な分野を中心に、滲み出し的に、M&Aも進めながら、新規事業を推進している
3. “飛び地的”な分野にも、M&Aも大いに活用しながら、積極的にリスクテイクを推進している

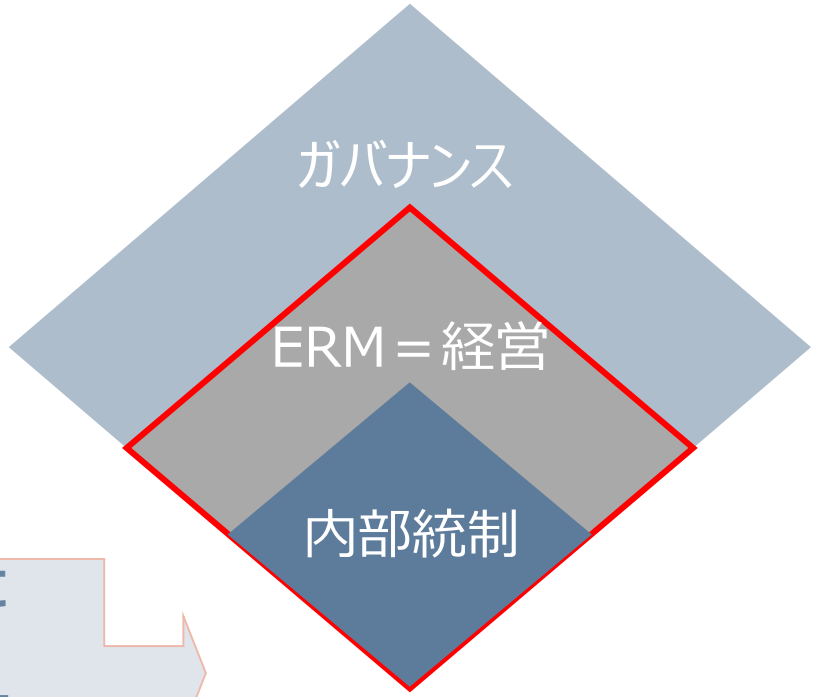
ガバナンス・ERM・内部統制の関係整理

～ 2013年COSO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、**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、4つのリスク対応戦略(受容・転嫁・軽減・回避)の内、**リスクの軽減**に貢献



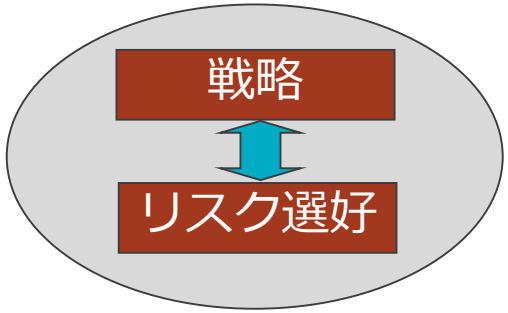
出典：COSO

企業目的 → 戦略 → リスク → 内部統制

protiviti

リスク選好とリスク許容度を設定する

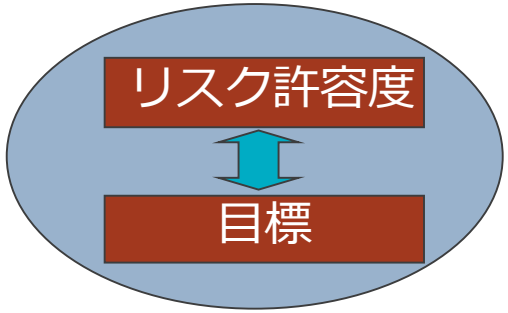
ガバナンスとリーダーシップ：



リスク選好とは:

- 広義には、事業体が企業価値を追求するために受け入れたいと考える**リスクの総量**。
- 事業体のリスクマネジメントの考え方を反映し、一方で**事業体の文化や事業形態に影響**を与える。

戦略の実行：



リスク許容度とは:

- **目標との差異をどの程度許容**できるかというレベル
- リスク許容度は測定されうるものであり、関連目標と同様の事業単位で測定することが望ましい

例:

- 35%の成長目標に対してプラス・マイナス5%の許容限度、など
- 取引限度額、信用度評価など

protiviti

欧米企業のリスク選好方針・リスク許容度の例

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。

リスク選好のための検討事項

- **市場の著しい進化**に対し、今後5年、10年の自社のあるべき姿はどうか。
- 現戦略の方向性、市場動向の予測、シナリオ等の重点項目は**来年も適切か、3年後、5年後**はどうか。

◆ リスク選好は、**経営理念**に合致しているか。

◆ 経営者の**経営哲学**は現状維持（現状のコアビジネスにとどまるか）、新規事業を志向しているか

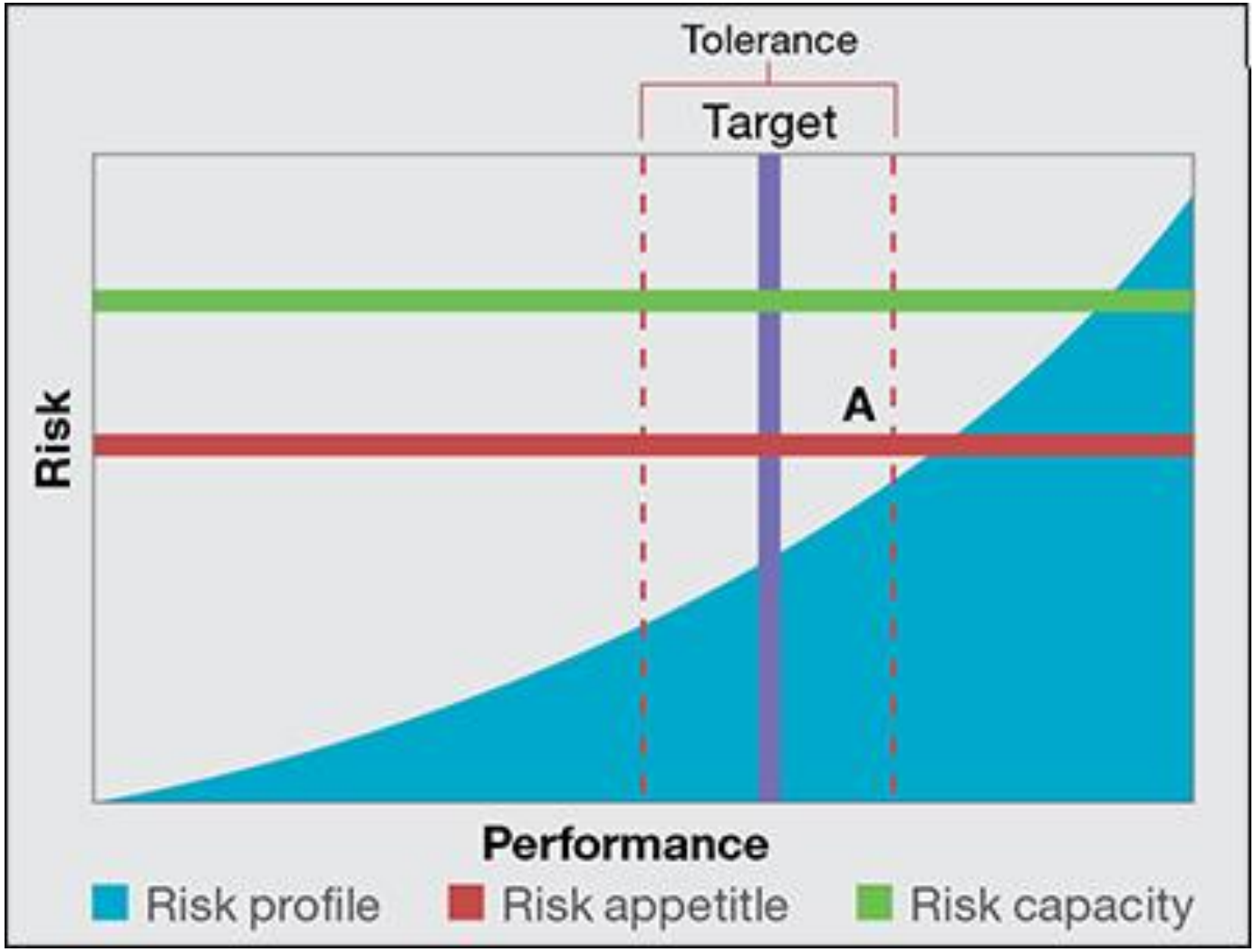
◆ リスク選好は、自社が最も得意とする分野のリスクテイクに焦点を当てているか、**より積極的にリスクをとるか**。

◆ リスク選好は、投資家、主要取引先など**ステイクホルダーの期待**に沿っているか。

■ 自社の**リスク対応能力**は実際にとっているリスクに合致しているか。

■ **競合他社**は自社よりリスクテイクをしているか否か、その理由は？

リスクプロファイル、リスク選好、リスク許容度



protiviti

3. リスクへの対応は十分か

リスクと内部統制

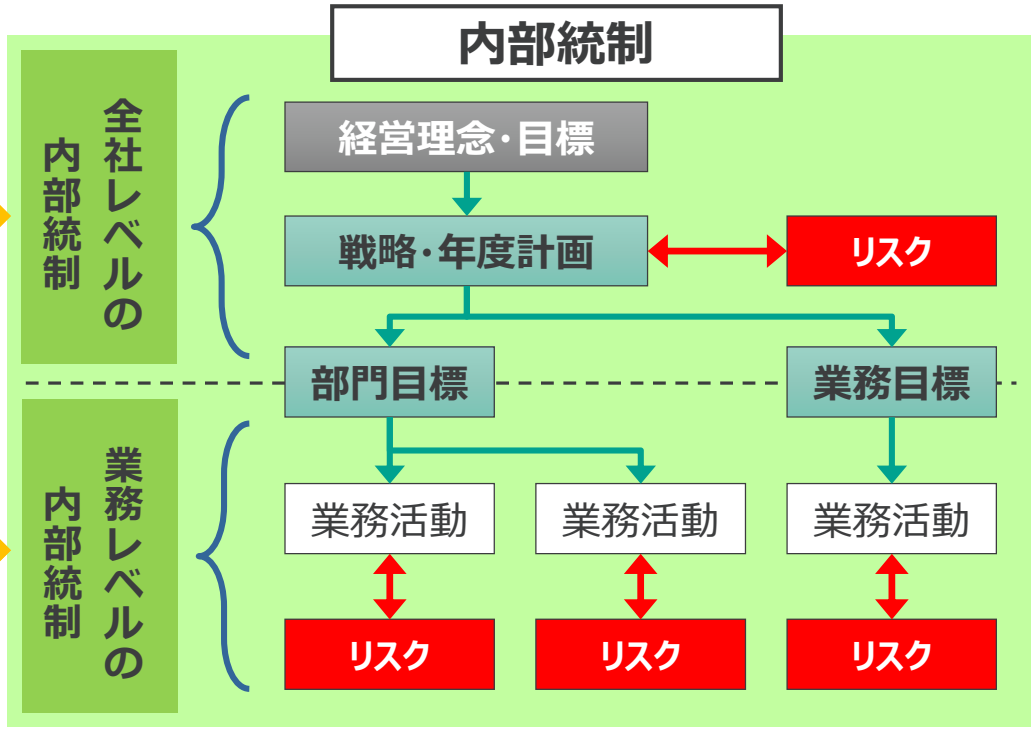
- **内部統制**は、理念・目標達成のため、全ての役職員で整備運用していくプロセス
- **内部統制**は、業務の効率を高め、内外の報告の信頼性を確保し、法令遵守を徹底し、
  目標達成に影響与えるリスクを低減する全社レベルと業務レベルのプロセス
- **リスク**とは、戦略の策定や遂行、目標の達成に影響を与える「不確実性」・「可能性」

「企業の姿勢」が基本

・ビジョン・バリュー
・企業理念
・内部統制体制
・フレームワーク、等

「予防と発見」が基本

・職務分掌
・業務のIT化
・承認手続きの明確化
・有事の対応、等



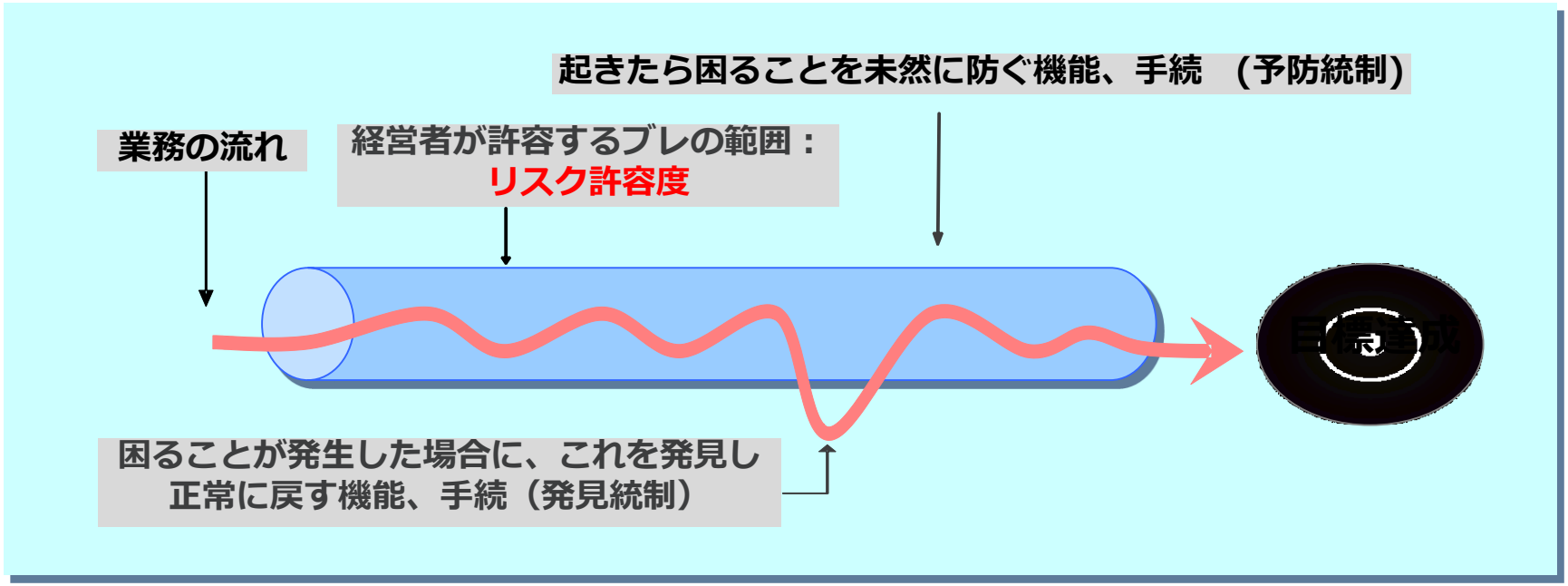
protiviti

内部統制の基本は、“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

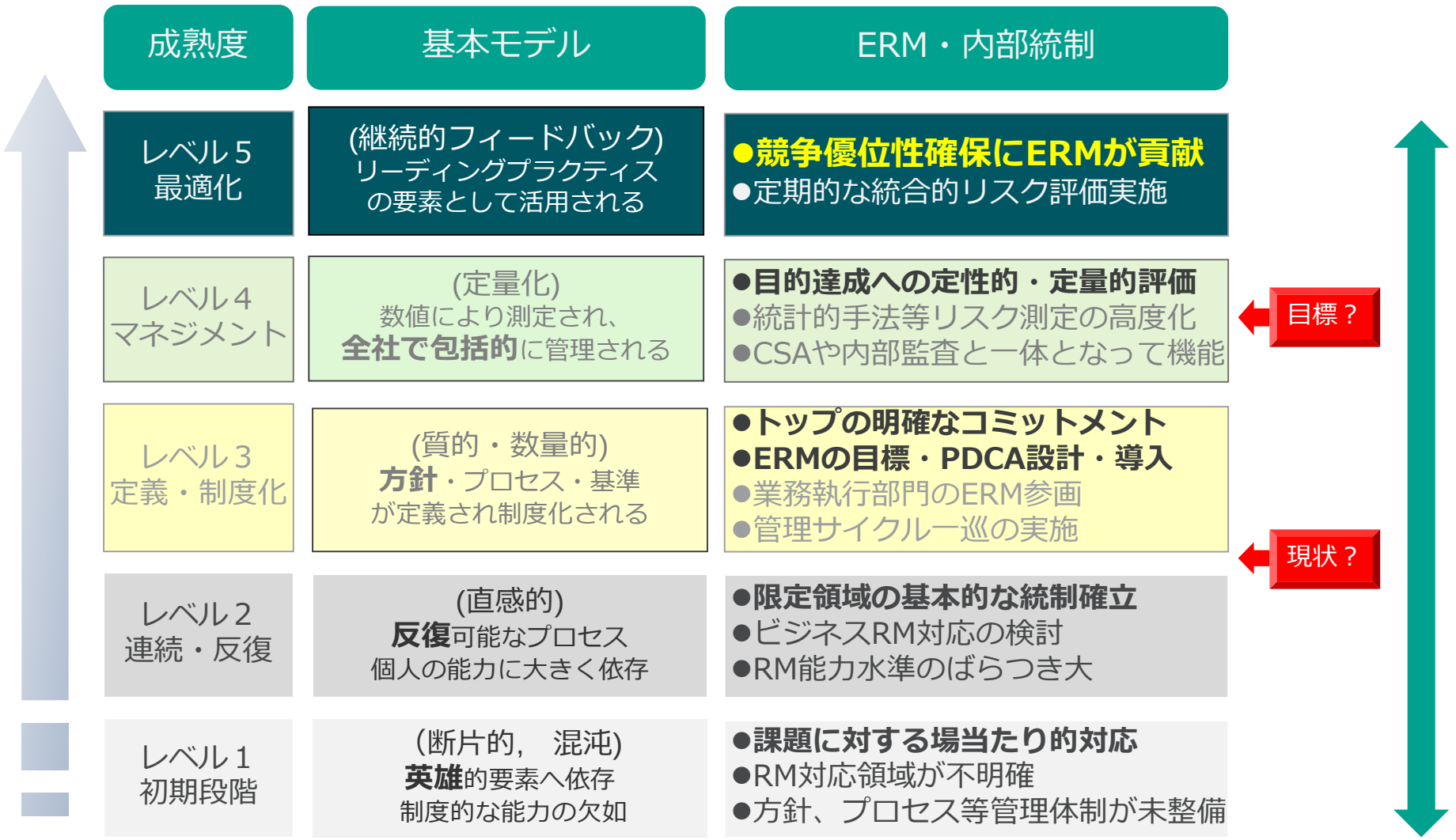
- ◆ 起きたら困ることを起こさないための機能・手続　（予防）
- ◆ 困ることを速やかに発見し正常に戻すための機能・手続　（発見）　（回復）

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

リスク対応能力の成熟度フレームワーク

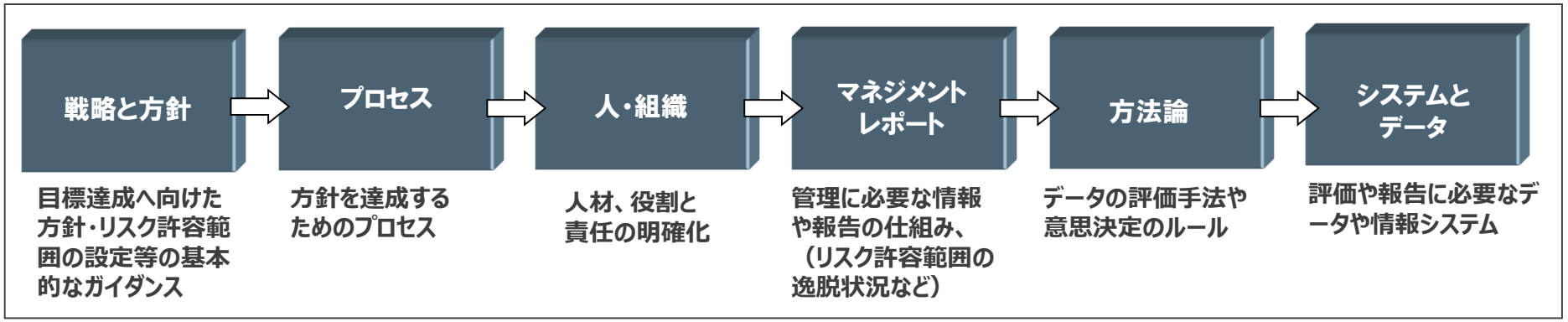


＊J-SOXはレベル3の成熟度

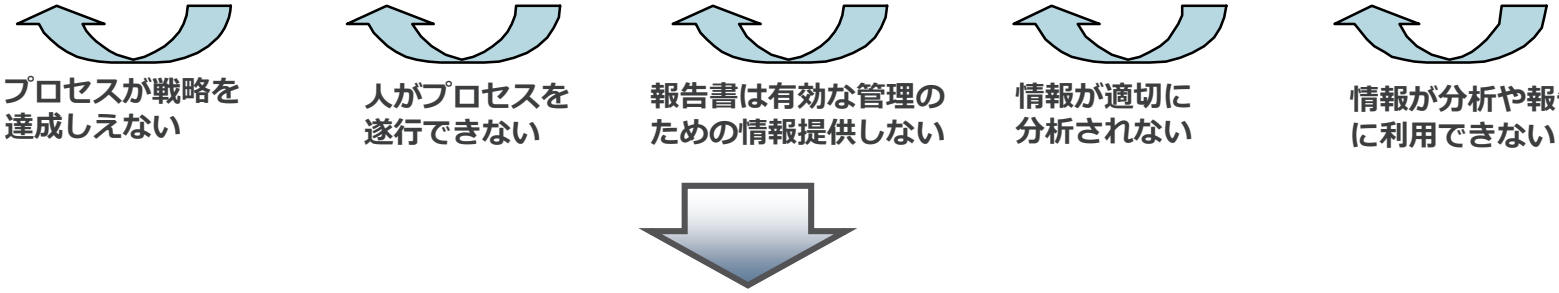
protiviti

成熟度モデルにおける経営インフラの６要素

ProtivitiではCMMに「経営インフラの6要素」を組み合わせて、評価を実施します。



構成要素が不完全な場合



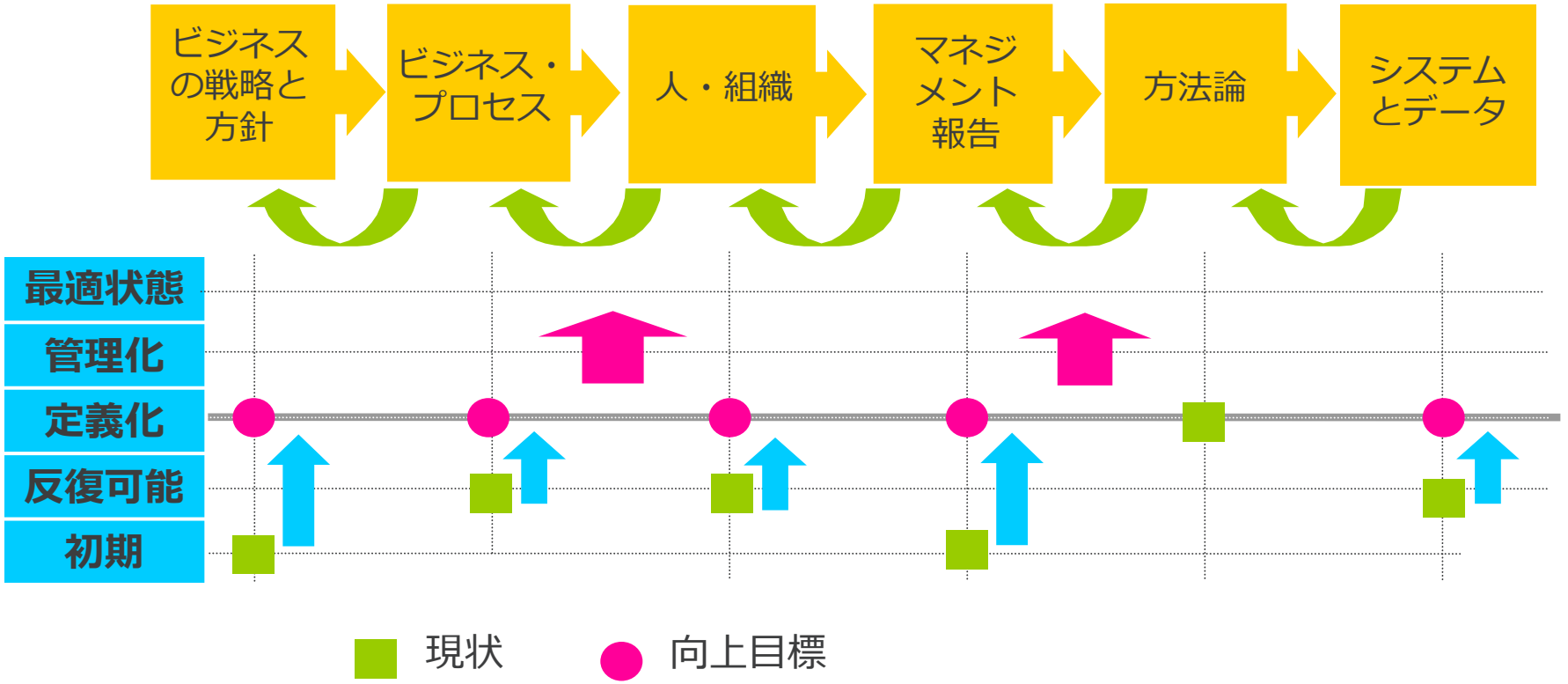
リスク管理・内部統制品質を高めるには、６要素が効果的に連携することが不可欠

6要素の関連性を把握した上で、要素ごとに成熟度を評価することで、具体的な目標設定やアクションプランにつなげる

protiviti

リスクマネジメント能力向上の進め方

全社的リスク或は特定のリスクに対して
リスクマネジメント能力を一定のレベルに合わせる → さらなる向上



protiviti

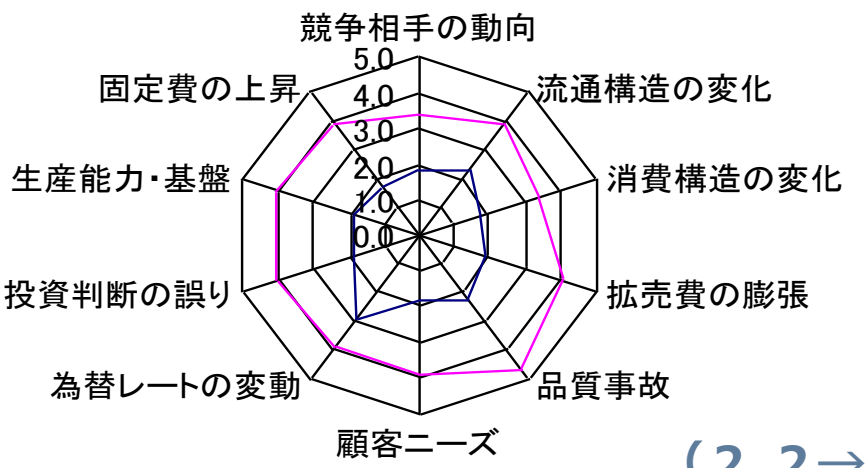
事例：ビジネスリスクマネジメント戦略

- 201X年、第5期中期経営計画で想定されるビジネスリスクについて、重要性および発生可能性を評価し、10の重点ビジネスリスクを特定した。
- 全役員ワークショップ・インタビューにより、各重点ビジネスリスクに対するマネジメント能力レベル（現在と将来）を評価した。

重点ビジネスリスク

1. 拡売費の膨張
2. 品質事故
3. 競争相手の動向
4. 顧客ニーズの適切な把握と顧客への情報発信
5. 流通構造の変化
6. 為替レートの変動
7. 消費構造の変化
8. 投資判断の誤り
9. 生産能力・基盤の過不足
10. 固定費の上昇

現在および将来のマネジメント能力レベル



5．最適化
4．マネジメント
3．定義・制度化
2．連続・反復
1．初期段階

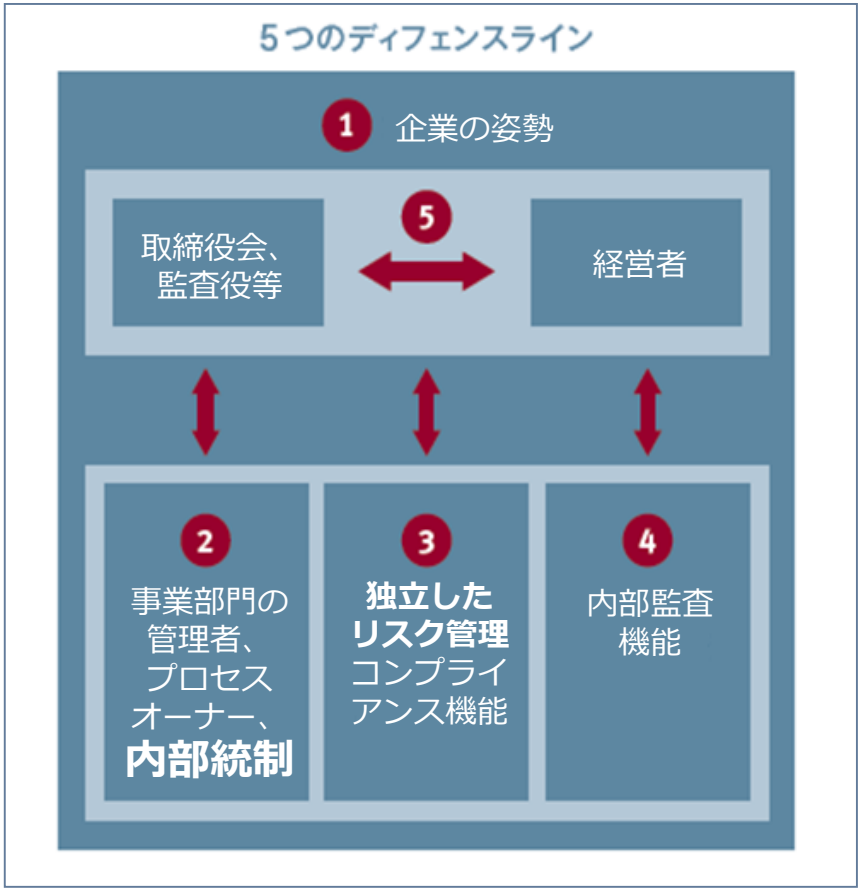
（2.2→4.6）

優先的に検討着手すべき「品質（事故）リスク」を選定し、プロジェクト活動を開始。

protiviti

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**事が大切
- 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

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、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」の原案を作成するなど、**目標達成の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**等に基づいて、不適切な会計処理が同時並行的かつ組織的に実行又は継続された。 • 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。**

4. 新COSO ERMフレームワーク

COSO改訂ERMの背景

- グローバル化の一層の進展と複雑化する新たなリスクの発生
- 取締役会と経営執行陣によるERMの認知とリスクオーバーサイト*が拡大
- 経営陣とステークホルダーの自信を高めるべく、リスクは戦略策定とパフォーマンスの向上の過程で検討することの重要性が高まる
- テクノロジの進化とデータアナリティックスを意思決定に活用

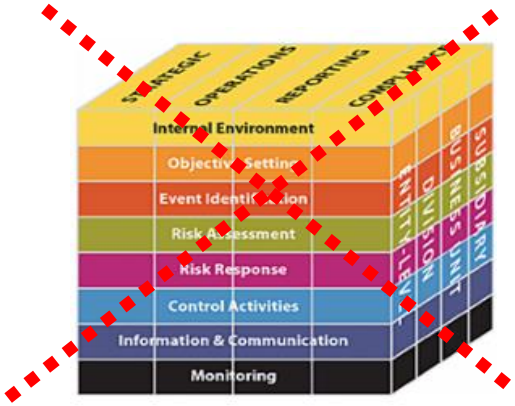
- **2013年　COSOは『内部統制フレームワーク（1992年）』を改訂。**
- **2016年　COSOは『不正リスク管理ガイド』を公表**
- **2016年** ***Enterprise Risk Management – Aligning Risk with Strategy and Performance*** **（ERM－リスクを戦略とパフォーマンスに整合させる）の公開草案を公表。**
- **2017年9月** ***Enterprise Risk Management-Integrating with Strategy and Performance*** **公表　（報告書上は6月の完成）**

***SECのリスクオーバーサイトに関する取締役会の役割開示への要請：**
リスクオーバーサイトにおける取締役会の役割に関する情報開示

主要な変更点

- 「COSOキューブ」ERMは、新しいグラフィックに変更。
- 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。

ERM
統合的フレームワーク
2004年



ERM
戦略・パフォーマンスとの統合
2017年

protiviti

ERMのベネフィット

- 機会の幅を拡げる
- ネガティブなサプライズを軽減しつつ、ポジティブな成果と優位性を増進する
- 全社レベルのリスクを特定・管理する
- パフォーマンスの“ぶれ”を低減する
- 経営資源の活用を改善する
- 組織の持続可能性、しなやかさ、敏捷性を高める

新COSOERM　５つの構成要素と20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。

protiviti

インセンティブとプレッシャーへのCOSOの新たな考察

改訂ERMフレームワークの最初の構成要素“Governance and Culture”、5番目の原則

原則5　組織は、戦略と事業目標にふさわしい人材育成を徹底する。
Principle 5, The organization is committed to building human capital in alignment with the strategy and business objectives.

この原則の要旨：

- 必要な資質、専門性を確立し、評価する。
- 人材を惹きつけ、育成し、保持する。
- 後継者を育成、検討する
- 業績に見合う報酬を提供する
- プレッシャーに対処する

  - インセンティブ（金銭・非金銭）とプレッシャーに留意する
  - 適切なインセンティブは適切な行動を、不適切なインセンティブは不適切な行動を導く。
  - 適切なプレッシャーは目標達成のモチベーションとなるが、不適切なプレッシャーは目標を達成できないという恐れを生み、不適切な行動を導く。

二つの企業倫理　～組織倫理と市場倫理

●**組織倫理で最も重要なこと：**
- 組織の理念・目標を達成すること**（プレッシャー）**
- そのために使命感に燃え一生懸命努力した人に公正に組織成果を分配すること **（インセンティブ）**

●**市場倫理において最も大切なこと：**
- 等価交換(Value for Fee)という絶対的な市場ルールを守ること
- 等価交換の原則を守る中で、コスト管理の徹底による利益の最大化が正当化される

✓**粉飾決算、数々の開示不正**は、組織成果の適切な開示や**“等価交換の原則”を破る重大な違反行為**
✓**ムラ八分**が怖くて或はムラを守るためには、ムラの掟を時には法律よりも優先する
✓**ムラの掟**が時に世間の常識から逸脱することがあるため、「組織のため」に行われる組織ぐるみの行動が、不公正あるいは不適切な事案として世間を騒がせてきたのではないか。
✓個人の利得より**組織の利得**を優先する同質性による思考プロセスは日本の特徴の一つ
✓**ムラへの絶対忠誠**は、一定の規律を維持する反面、個人の良識を遮断し、不正や法令違反を引き起こすという負の面も否定できないことを、ムラのリーダーは肝に銘じるべきである。

“社員は社長が怖い、社長は社員が怖い、世間が怖い。謙虚な気持ちを忘れ、感謝を忘れ、怖さを知らない個人、組織は、必ず自分の力を過信し、挙句の果て暴力を振りかざし、滅びの門に突入する。”（松下幸之助）

protiviti

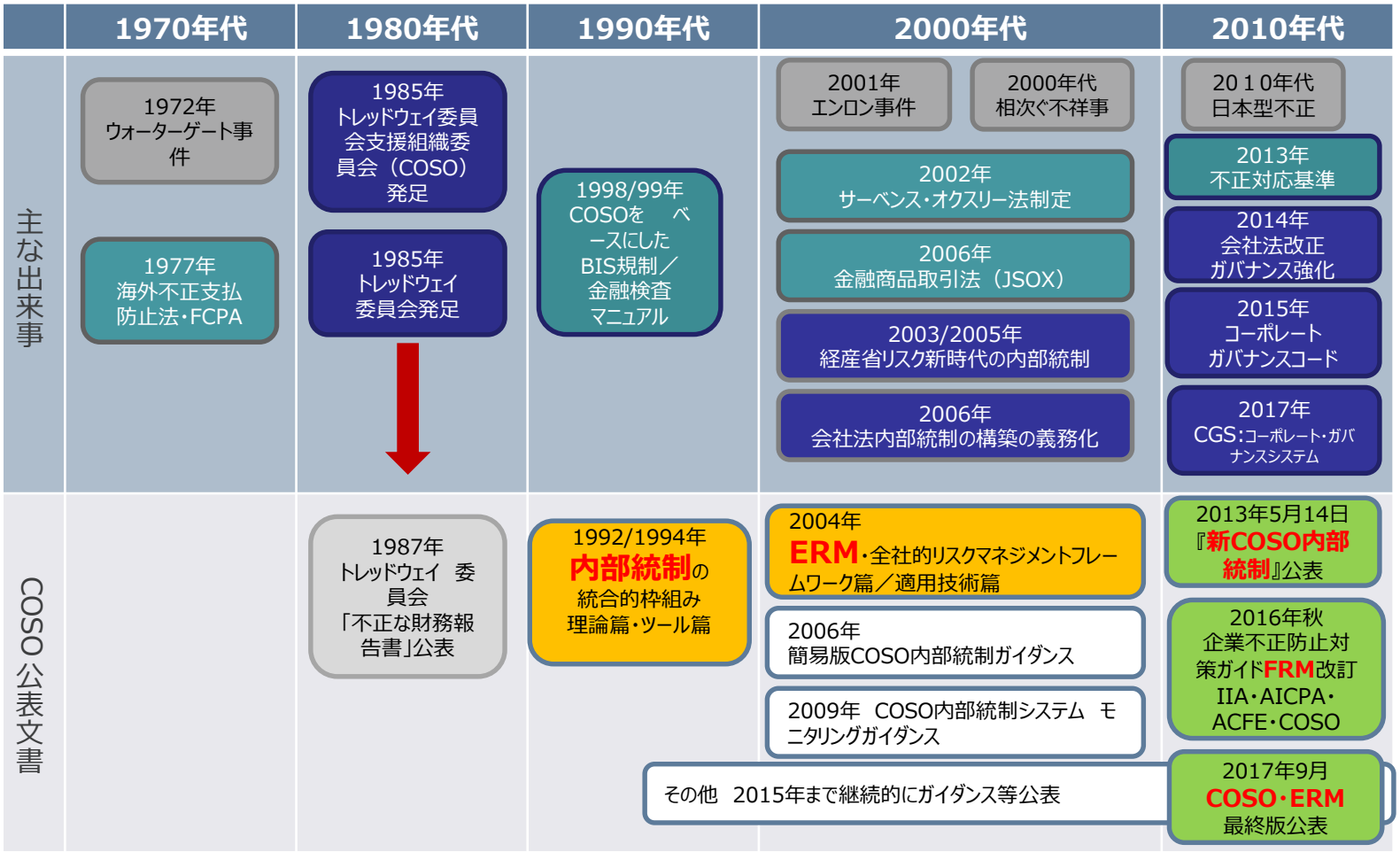
5. 不正リスク対応

問（５）　不正リスクマネジメントについて

皆さんの会社では不正リスクマネジメントを導入していますか？

1. FRMを導入している
2. 導入はしていないが、コンプライアンスの一部として対応している
3. 導入はしていないが、これまで1件も不祥事は生じていない
4. 性善説をモットーとして、従業員の自主性に任せている

不祥事、グローバル規制、COSOフレームワークの動き



protiviti

2013年COSO内部統制は、17原則を明示

統制環境	1. 組織は、誠実性と倫理観に対するコミットメントを表明する **2. 取締役会*は独立性を保持し内部統制の整備運用状況を監視する** 3. 経営者は、組織構造、報告経路および適切な権限と責任を確立する 4. 組織は、有能な人材を惹きつけ、育成、維持にコミットする 5. 組織は、内部統制に対する責任を個々人に持たせる
リスク評価	6. 組織は、リスク評価のための適切な目的を明示する 7. 組織は、リスクの特定と分析を行う **8. 組織は、目的達成のリスク評価に際して不正の可能性を検討する** 9. 組織は、リスクの重要な変化を特定し、分析する
統制活動	10. 組織は、**リスクを許容可能水準まで低減する**統制活動を選択整備する 11. 組織は、**テクノロジ**に係る全般統制活動を選択し整備する 12. 組織は、期待を明記した方針及び手続のもとで統制活動を展開する
情報と伝達	13. 組織は、関連性のある質の高い情報を入手、作成して活用する 14. 組織は、内部統制の目的と責任分担を含む情報を組織内部に伝達する 15. 組織は、構成要素の機能に影響を与える事項を組織外部に伝達する
モニタリング活動	16. 組織は、構成素が存在し機能していることを確かめるため継続的評価及び/又は、独立的評価を、選択、適用、実行する 17. 組織は、適時に不備を評価し、是正措置の責任ある者に伝達する

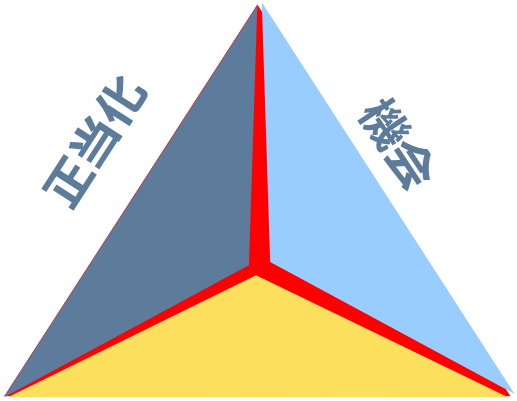
*取締役会：従来、Board of Directorsと示された部分は、今回、Governing Bodyとしてその定義が明確に示され、取締役会と以下を含む。“board of trustees, general partners, owner, or supervisory board。日本では、監査役会、監査委員会も含まれると解釈されることになる。

不正のトライアングル

不正のトライアングルとは、不正が起きる要因のことで、この３つの要因が揃うと不正が発生する確率が高くなる。

・不正に関与しようとする「動機・プレッシャー」
・不正を実行する「機会」
・不正行為に対する「姿勢・正当化」

- 不正を正当化・許容する姿勢（会社のためにやっている等）
- 人格、価値観（自分は不当に評価されている等）



- 適切な内部牽制や職務分掌がなく単独で複数業務を行っている
- 内部統制が整備されていない
- 内部統制を無視できる立場（部門責任者、特定の内部統制不備を認知している者など）にある

- 収入を超えた生活や借金などによる金銭的欲求
- 達成困難な利益目標により、経営者や従業員が企業内外からプレッシャーを受けている

Donald R. Cressey :
「不正のトライアングル」

性善説か、性悪説か、あるいは性弱説か

protiviti

不正リスク管理ガイドの5原則（2016年）

統制環境と関連	1. 組織は、取締役会及び上級経営者の期待と彼らの不正リスク管理に関する誠実性と倫理的価値観に対するコミットメントを表明する**不正リスク管理プログラム**を確立し伝達する。
リスク評価と関連	2. 組織は、具体的な**不正スキームとリスク**を識別し、不正の発生の可能性と重大性を測定し、既存の不正対策活動を評価し、不正の残存リスクを軽減する対策を実施するため統合的な不正リスク評価を実施する。
統制活動と関連	3. 組織は、発生する、または適時に発見されることのない不正リスクを軽減するための**予防的・発見的な不正対策活動**を選定、開発、実施する。
情報と伝達に関連	4. 組織は、潜在的な不正についての情報を入手するための**情報伝達のプロセス**を確立し、調査および不正に適時にかつ適切な方法で対処する是正措置への組織的な取組を採用する。
モニタリング活動に関連	5. 組織は、不正リスク管理の5つの原則の各々が存在し、機能し、運営されているかどうかを確認するための**継続的な評価方法**を選定、開発、実施し、不正リスク管理プログラムの不具合を、上級管理者と取締役会を含む**是正措置**の実施に責任を負う当事者に適時に伝達する。

昨今の不祥事

企業名	時期	概要
日産	• 2017年10月	• 国土交通省の抜き打ちの立ち入り調査で、国内6ヶ所全ての車両組み立て工場で無資格の従業員によって車両製造の最終工程の完成検査が行われていたことが発覚。この問題を受け、同社は再点検のため販売済みの約121万台をリコールすることを発表。
神戸製鋼	• 2017年10月	• 航空機や自動車などに使われるアルミ・銅、鉄粉、銅合金管、銅管、モールド、アルミニウム合金線、合金棒、銅板条、鋼線、特殊鋼、ステンレス鋼線等の製品において、製品仕様に適合していないにもかかわらず、検査証明書のデータを改ざんし出荷していた。出荷先は約200社にも及ぶ。データ改ざんは国内にある全ての製造工場（4ヶ所）やグループ会社で行われていた。問題発生から9日後には、米国司法当局から仕様不適合に関する書類を提出するよう求められた。
SUBARU	• 2017年10月	• 国土交通省の指示により実施された社内調査で、群馬県の製作所で無資格の従業員によって車両製造の最終工程の完成検査が行われていたことが発覚。
三菱マテリアル	• 2017年11月	• 子会社の三菱電線工業株式会社、三菱伸銅株式会社、三菱アルミニウム株式会社において、検査データを改ざんした不適合の素材製品が出荷されたことを発表。
東レ	• 2017年11月	• 子会社の東レハイブリッドコード株式会社において、納入製品の検査データを不正に書き換えていたことを発表。書き換えは2008年4月から行われていた。

出展：https://www.sustaines.com/scandals/

不祥事に関するディスカッション

グループごとに以下のテーマについてディスカッションし、その内容を発表して下さい。

1. 近年、不祥事が増加している原因背景

2. 当該真因への対応策

5. まとめ

日本企業のDNA～何を残し、何を変えるか

◆ 持続的成長

✓日本の長寿企業は 28,972 社（帝国データバンク2016）

長寿の秘訣：変化を恐れず常に新しい可能性を模索し企業活動を継続

✓持続的成長企業4つの共通項

差別化、ポジショニング、事業ポートフォリオ、イノベーション

◆ 日本人のアイデンティティ、企業経営、行動指針

- ✓ 就社意識と就職意識：組織内での立ち回り力と専門性のバランス
- ✓ 終身雇用、家族的経営
- ✓ 自利利他、震災と助け合い精神、お互いさま
- ✓「勤勉、倹約、もったいない」と業務改善、品質改善
- ✓ おもてなし、礼儀作法、品格、GNN
- ✓ グローバルスタンダードという単一価値観と八百万の神・仏：受容と昇華

protiviti

経営者が 価値創造とリスクの統合を推進するための５つの質問

1. 攻めと守りの経営を推進するために、有効なリスクマネジメントを確保すべく、５つのディフェンスラインは強固なものになっていますか？

2. 組織のリスク感性を高め、見えないリスクの把握に努めていますか？

3. 積極的なリスクテイクを進めるため、組織文化やリスクカルチャーのグローバル規模での浸透に十分な取組みを行っていますか？

4. 企業戦略の重要な前提条件に影響を与える兆候を把握分析し、前提条件の変化に対して戦略変更の検討が適時になされていますか？

5. リスク管理指標（KRI)やIT(データベース)を活用したモニタリングや報告が適時になされ、対応策が適切に実施されていますか？

まとめ

- 目的➡戦略➡リスク➡内部統制
- リスクの定義を見直す
- 市場ガバナンスのみならず、組織ガバナンスの強化を
  リスクとコントロールの共有化を通じて推進する
- ERM・内部統制は戦略実現の基盤であり、ボトムアップ
  の情報収集・合意形成から、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

Face the Future with Confidence

protiviti®

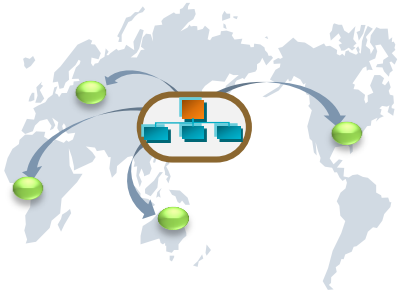
（参考）グローバル事業管理（リスクプロファイル）とERMモデル(1/2)

ビジネスモデルとリスクプロファイルに合わせて最適な運営モデルを選択する

グローバル統合
（グローバル規模で標準化）

ローカル適合

本社中央集権型

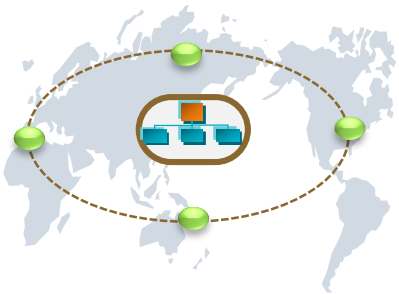


海外子会社の役割
- 親会社の戦略を実行する出先

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

トランスナショナル型

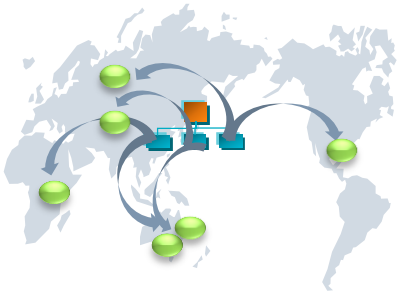


海外子会社の役割
- 海外の組織単位毎に**役割を分担**して世界規模で経営をコーディネート

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

事業部門主導型

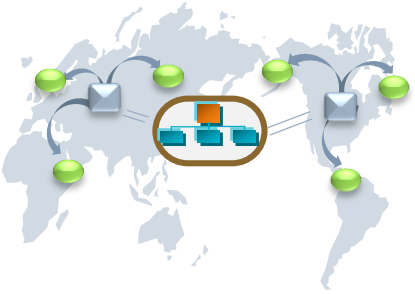


海外子会社の役割
- 現地の好機を感じ取って対応、成果を上げる自律拠点

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、各事業部門が管理

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を有効活用

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

protiviti

（参考）グローバル事業管理（リスクプロファイル）とERMモデル(2/2)

それぞれの強み・弱みを認識し、継続的に成熟度向上を推進する

モデル	強み	弱み（課題）
本社 中央集権型	• 迅速な意思決定が可能 • 本社のオペレーションやルールを統一的に用いて、業務の標準化・効率化が図れる	• 本国で標準化された製品展開・管理方式になるため、必ずしも地域に合ったアプローチがとれない • 地域で蓄積されたナレッジをグループに取り込む仕組みを作るのが困難である • 本社の押し付けと映る場合があり、現地社員にネガティブな印象を与える場合がある
事業部門 主導型	• 事業に特化した効率的な運営ができる • 事業別の利益責任が明確になり、業績向上に向けたインセンティブが働きやすい • 事業部長に経営者としての経験を積ませることができる	• 事業の最適化となるため全社最適化にはならない • 各事業部が経営機能を重複して持つため、経営資源面での無駄が生じる • 組織の壁により、事業部をまたがる新商品、新サービスが生まれにくくなる
地域統括 設置型	• 地域実情・ニーズに合った製品・サービス展開ができる • 地域への権限委譲により、現地でのオペレーション変更に柔軟かつ迅速に対応できる	• 本社・地域統括間で重複が起こりコスト増になる • インフラ（ルール・規程など）が共通化されていないため、グループ全体の管理が非効率である • それぞれ独自のシステムを使用している場合が多いため、地域で蓄積されたナレッジが他の地域あるいは本社で共有されない
トランス ナショナル型	• グローバル共通の経営基盤のもとで、地球規模での経営効率、競争優位性の追求ができる • 現地対応の柔軟性 • 本社、現地の隔てない知の共有と学習	• 理想的な形に見えるが、実現するための情報整備やオペレーション標準化のハードルが高く、リソースやコストの投下に対するリターンを十分検討する必要がある