

監査懇話会 監査セミナー

新たなリスクへの挑戦と対応

～アジャイルガバナンス・ERMのススメ

神林比洋雄

プロティビティ LLC

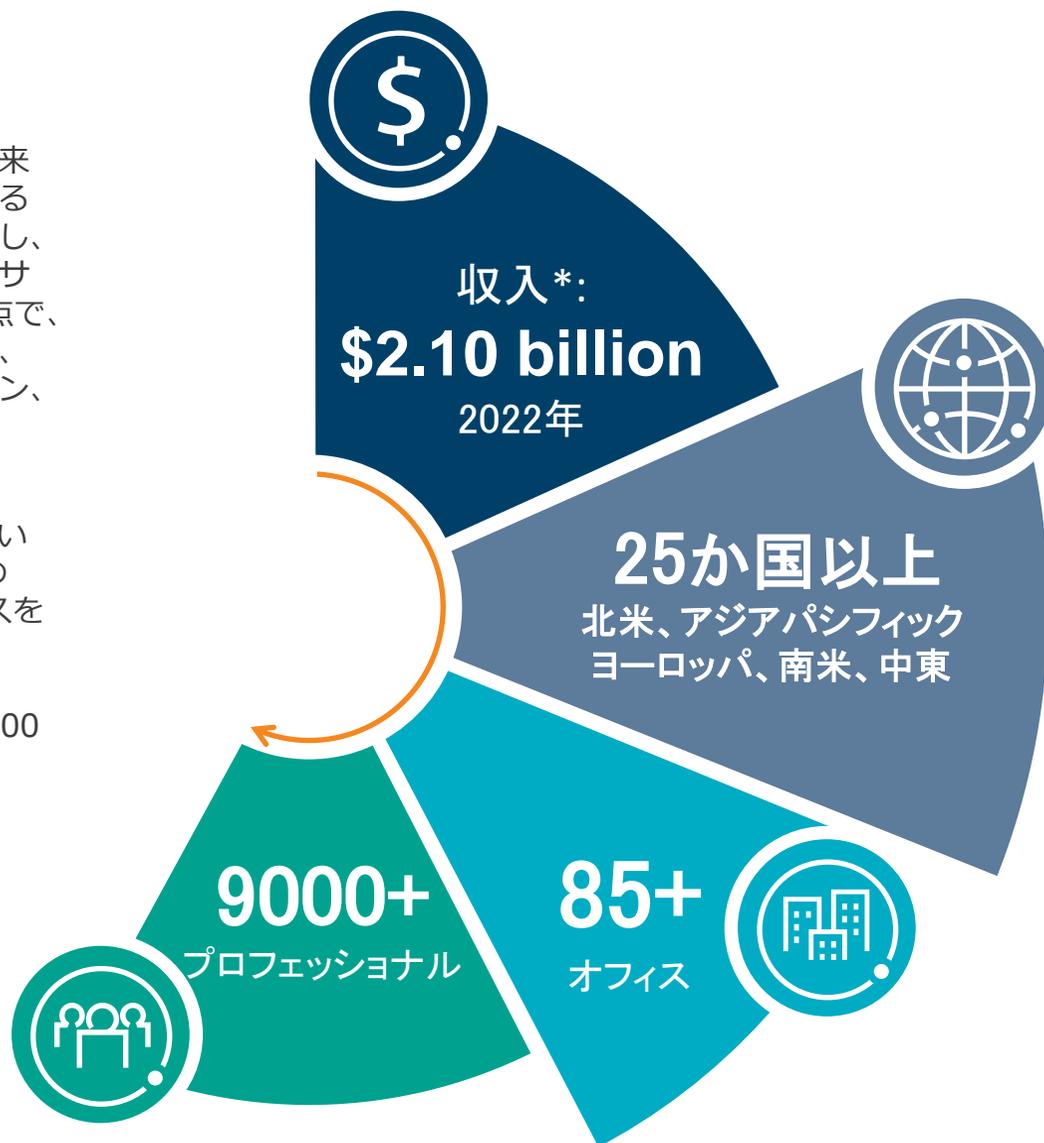
シニアマネージングディレクタ

2024年1月23日

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われますよう、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ご提供し、ゆるぎない最善の連携をお約束するグローバルコンサルティングファームです。25か国、85を超える拠点で、プロティビティは、ガバナンス、リスク、内部監査、経理財務、テクノロジー、デジタル、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とマネージドソリューションを提供しています。

プロティビティは、2022年フォーチュン誌“働きがいのある会社ベスト100”に選出され、Fortune 100の80%以上、Fortune 500の約80%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、上場を目指す企業や、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む。

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ー 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、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）元会長。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（現任）。ERM経営研究所LLC代表社員（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）。日本取締役協会リスク・ガバナンス委員会委員長（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』（同文館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

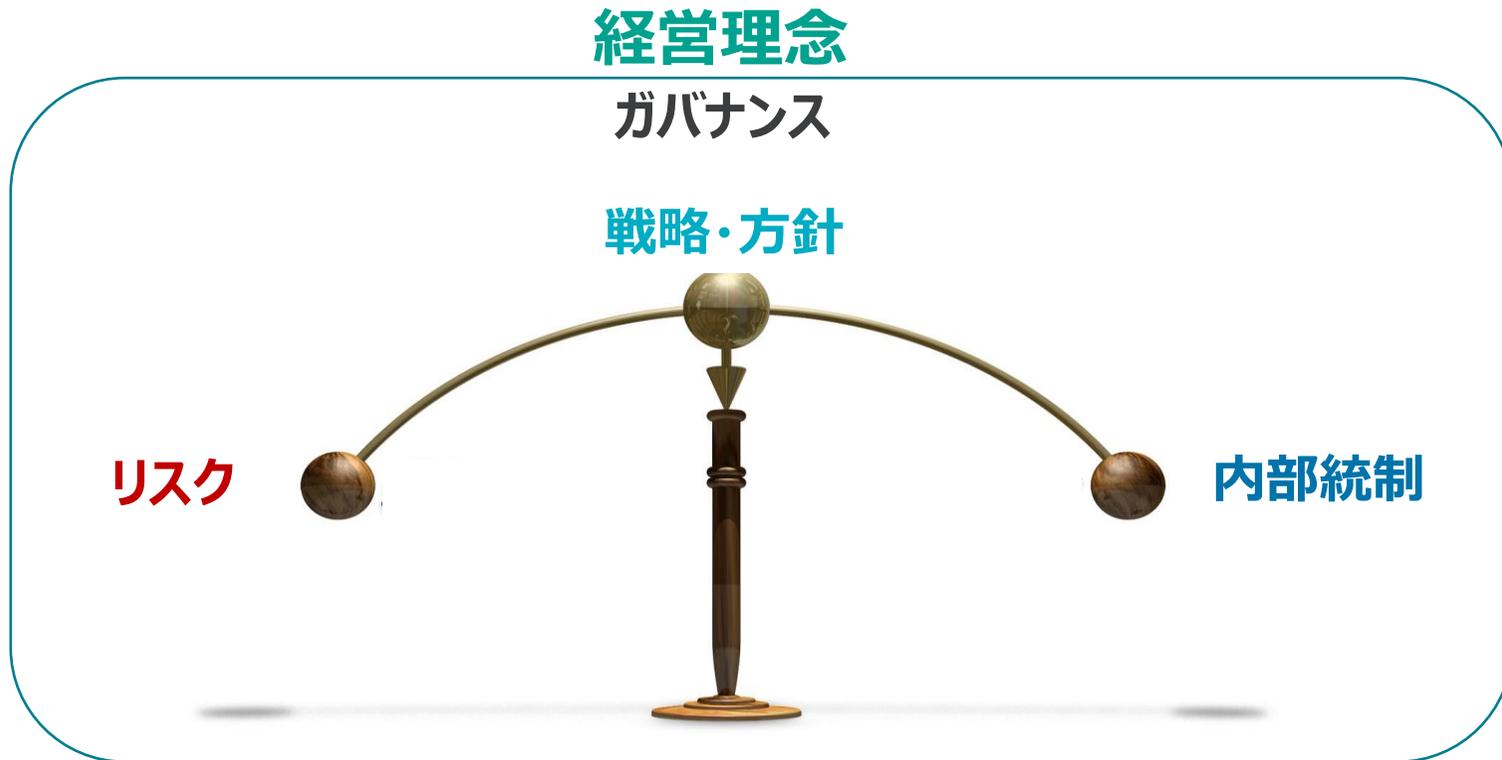
本日のトピック

- 1 最新のトップリスクサーベイから
- 2 Society5.0とアジャイル・ガバナンス
- 3 アジャイル・ガバナンスの取組みとERM
- 4 ビジネスと人権
- 5 テクノロジーリスク



はじめに

経営理念・ガバナンス・戦略・リスク・内部統制の関係とは

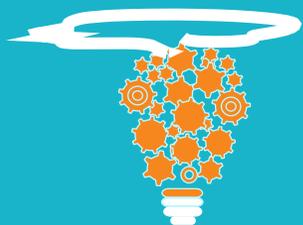


経営理念を実現するとは、適切なガバナンスのもと、外部・内部の環境変化を把握し、企業価値の源泉（資本又は資産）に影響を与える可能性（リスク）を見極め、戦略を策定し、選択された戦略の達成に影響を及ぼすリスクを特定し、その影響を経営者の許容範囲に収めるべく、相応の内部統制を構築し、中長期的に、やじろべえのバランスを保ち、期待される価値向上を目指すこと。

1. 最新のトップリスク調査から

企業のトップリスクをなぜ調査するのか？

機関投資家や、社外取締役、格付会社等が、企業経営者に問う
リスクマネジメントに関する質問



戦略策定の際に、取締役会や経営陣において、リスクマネジメントに関してどのような議論をしていますか？

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ますか？

経営陣はトップリスクに対しどのように対応していますか？

リスクマネジメントは有効に機能していますか？

それをどのように測定、評価していますか？

業界における最近の想定外の事象に対し、貴社はどう対応しましたか？

その想定外の事態による影響は他社と比べどうでしたか？

トップリスク調査の概要

プロティビティとノースカロライナ州立大学のERMイニシアチブは、今後1年間および今後10年間に組織に影響を及ぼす可能性のあるリスクについて、グローバルレベルで取締役・経営陣1,143人を対象に2023年後半に調査を実施。



この調査は、下記の3分野に関連する38のリスクの潜在的な影響に関する見通しを提供

マクロ経済リスク

組織の成長機会に影響を与える可能性



オペレーショナルリスク

組織の戦略を実行する際、組織の主要な業務に影響を与える可能性

戦略リスク

成長機会を追求するための組織の戦略の妥当性に影響を与える可能性

トップリスクの調査方法

回答者は、10ポイントスケールを使用して38の個々のリスクを評価

スコア1は、
この1年を通して
(さらに2034年の)
影響なしを反映

スコア10は、
この1年を通して
(さらに2034年
の) 組織への**広範**
な影響を反映



平均スコアに基づいて、個々のリスクを、
それほど重要ではない影響・**潜在的な影響**・**重要な影響** のいずれかに分類

Executive summary: [nc-state-protiviti-survey-top-risks-executive-summary-2024-2034.pdf](#)

Full report: [nc-state-protiviti-survey-top-risks-2024-2034.pdf](#)

短期的な全業界グローバル優先順位の変化～正負のインパクト



2024年グローバルリスクトップ10

1

現在サービスを提供する**市場の経済状況・インフレ**により、**成長機会が著しく制限**される

2

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

3

サイバー攻撃の脅威への対応不足

4

第3者からの供給が**安定的アウトソース**や**調達戦略**と**不適合**

5

規制変更や規制監督の強化が**製品やサービスの生産や提供**に**著しい影響**を及ぼす

6

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ングやアップスキング**に**多大な労力**が必要

7

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**に対応できない

8

金利の上昇の**資本コスト**や**オペレーションへの影響**

9

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

10

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

長期的な全業界グローバル優先順位の変化



2034年グローバルリスクトップ10

- 1 サイバー攻撃の脅威への対応不足
- 2 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
- 3 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
- 4 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
- 5 規制変更や規制監督の強化が製品やサービスの生産や提供に著しい影響を及ぼす
- 6 第3者からの供給が安定的アウトソースや調達戦略と不適合
- 7 現在サービスを提供する市場の経済状況・インフレにより、成長機会が著しく制限される
- 8 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」との競争に対応できない
- 9 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
- 10 市場情報分析の獲得や生産性・効率性の向上に必要なデータ解析やビッグデータを使う能力が欠如する

2024年のトップリスク調査から得られる重要なポイント

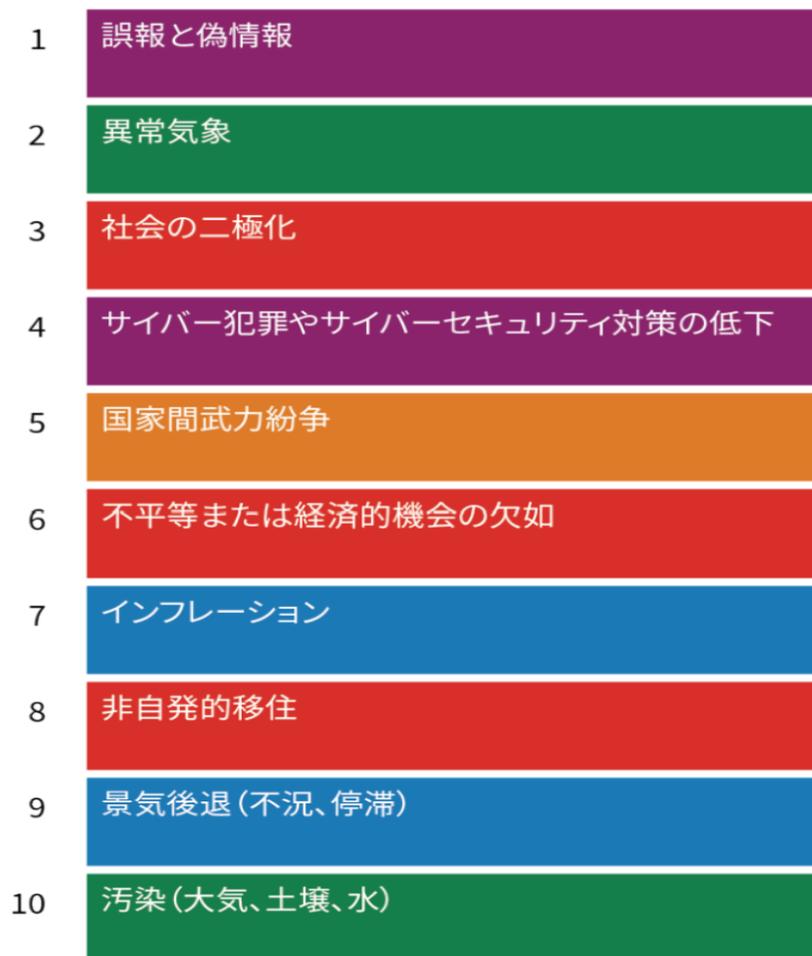
重要な ポイント



- 1 多元的なリスク要因が、直近の不確実性を高めている
- 2 直近の地政学的リスクによる影響が複雑化している
- 3 インフレなどの経済要因によるリスクが高まりを見せている
- 4 テクノロジー関連リスクとして、データプライバシーに加えて、サイバー攻撃の脅威が急浮上している
- 5 人材関連のリスクが、引き続き、短期的、長期的にも重大なリスクとなっている
- 6 イノベーションへの機会とリスクは益々重要になっており、リスクリングやアップスキリングへの適時適切な対応が不可欠である

ダボス会議・グローバルリスクレポート2024～負のインパクト

今後2年間



今後10年間



リスク分類

■ 経済

■ 環境

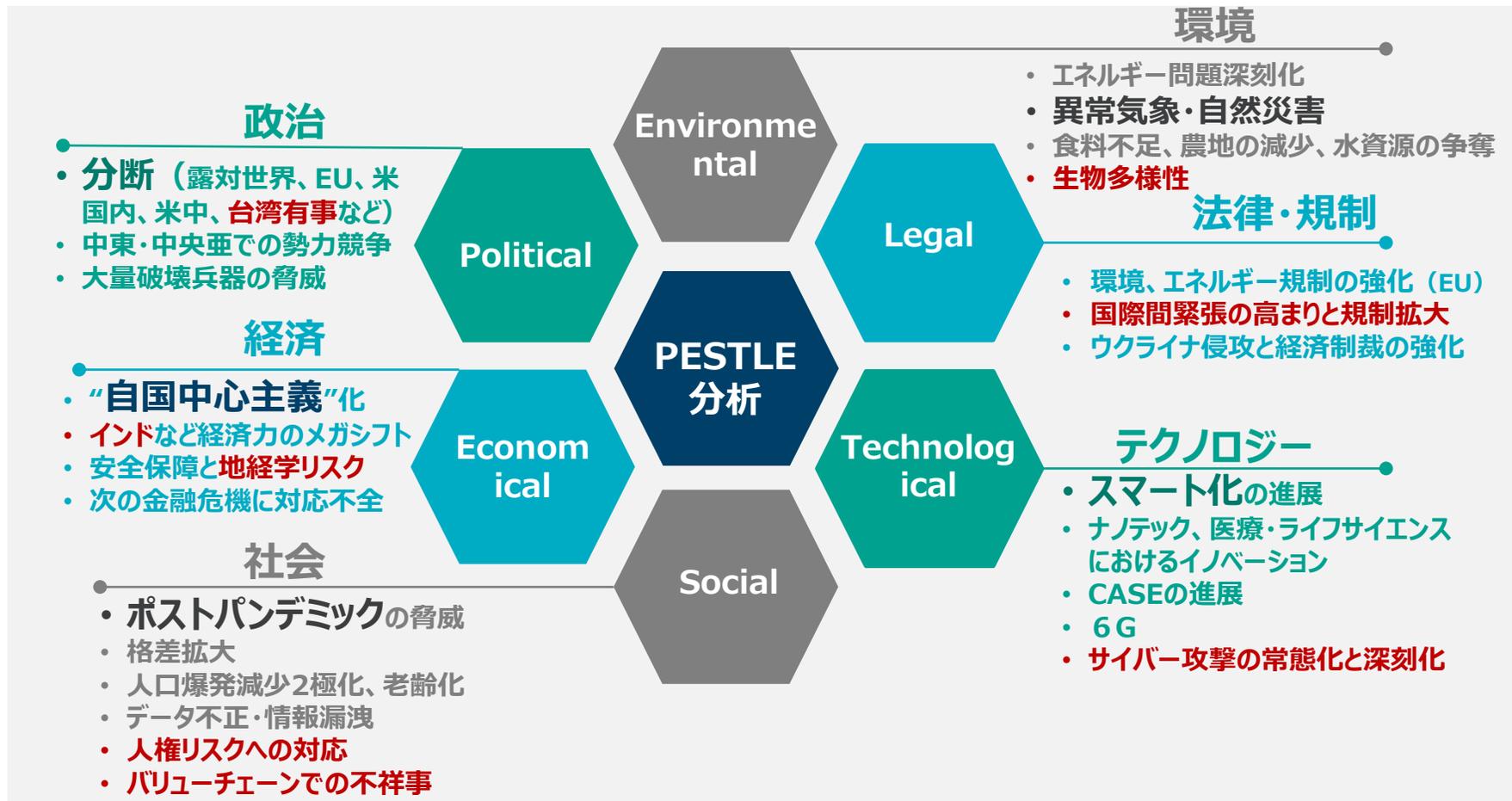
■ 地政学

■ 社会

■ テクノロジー

以上を要約した 企業を取り巻く外部環境変化 ～リスクの外的要因

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



この変化が自社のビジネスの成否に影響を及ぼすシナリオを描き切れるか

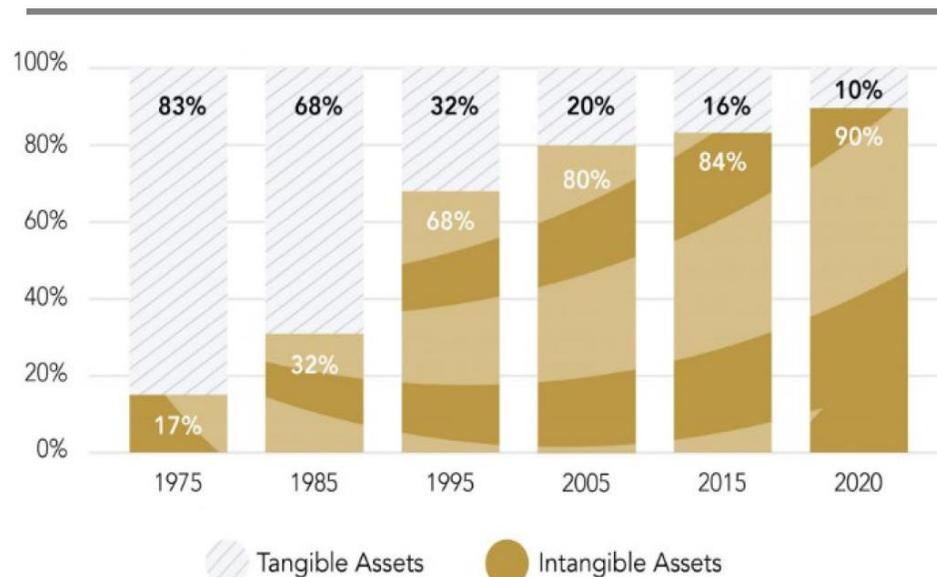
企業価値の源泉 ～リスクの内的要因

企業（市場）価値の源泉 ～ リスクの内的要因

価値を産み出す源泉に影響を及ぼす要因がリスク

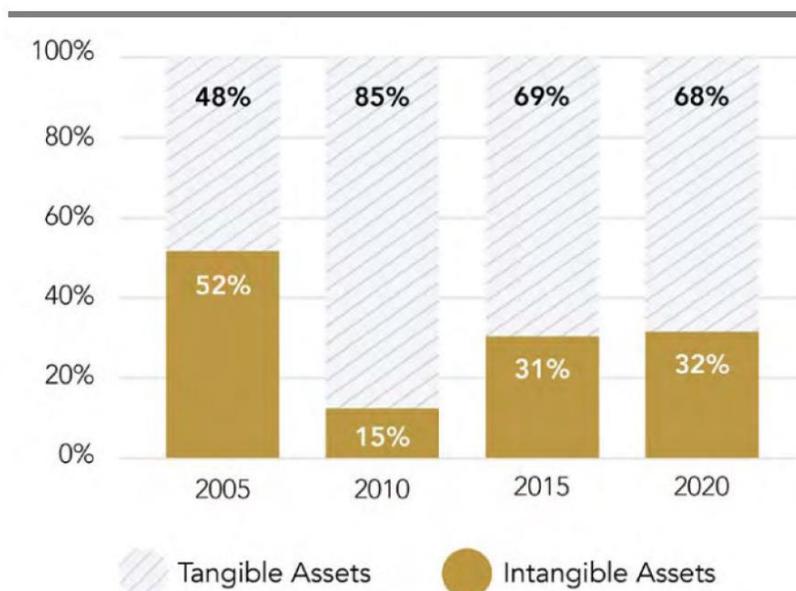
米国では、GAFAMの台頭もあり、市場価値に占める無形資産の割合が90年代以降、急拡大。日本では、モノづくりの強みが市場価値の7割近くを占めている。

市場価値に占める無形資産割合 (米国 S&P500)



SOURCE: OCEAN TOMO, A PART OF J.S. HELD, INTANGIBLE ASSET MARKET VALUE STUDY, 2020

市場価値に占める無形資産割合 (日本 日経225)



SOURCE: OCEAN TOMO, A PART OF J.S. HELD, INTANGIBLE ASSET MARKET VALUE STUDY, 2020

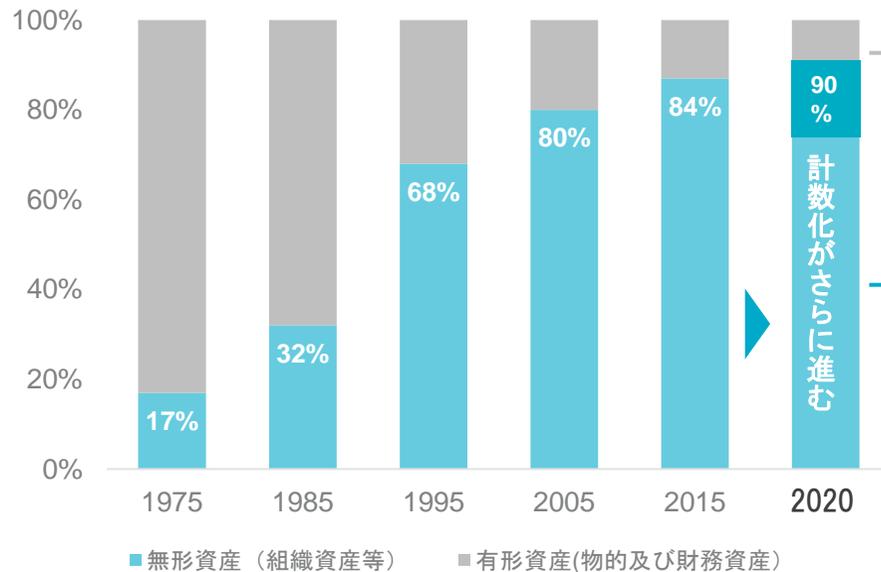
(出所) Ocean Tomo, Intangible Asset Market Value Study, 2020

「企業価値」を生み出す源泉の変化(リスク)を考慮する

S&P 500企業の市場価値に占める無形資産の割合は急増。

無形資産の相当部分は、今後、可視化・測定され、投資家の注目がさらに高まる。

S&P 500市場価値の構成比の推移



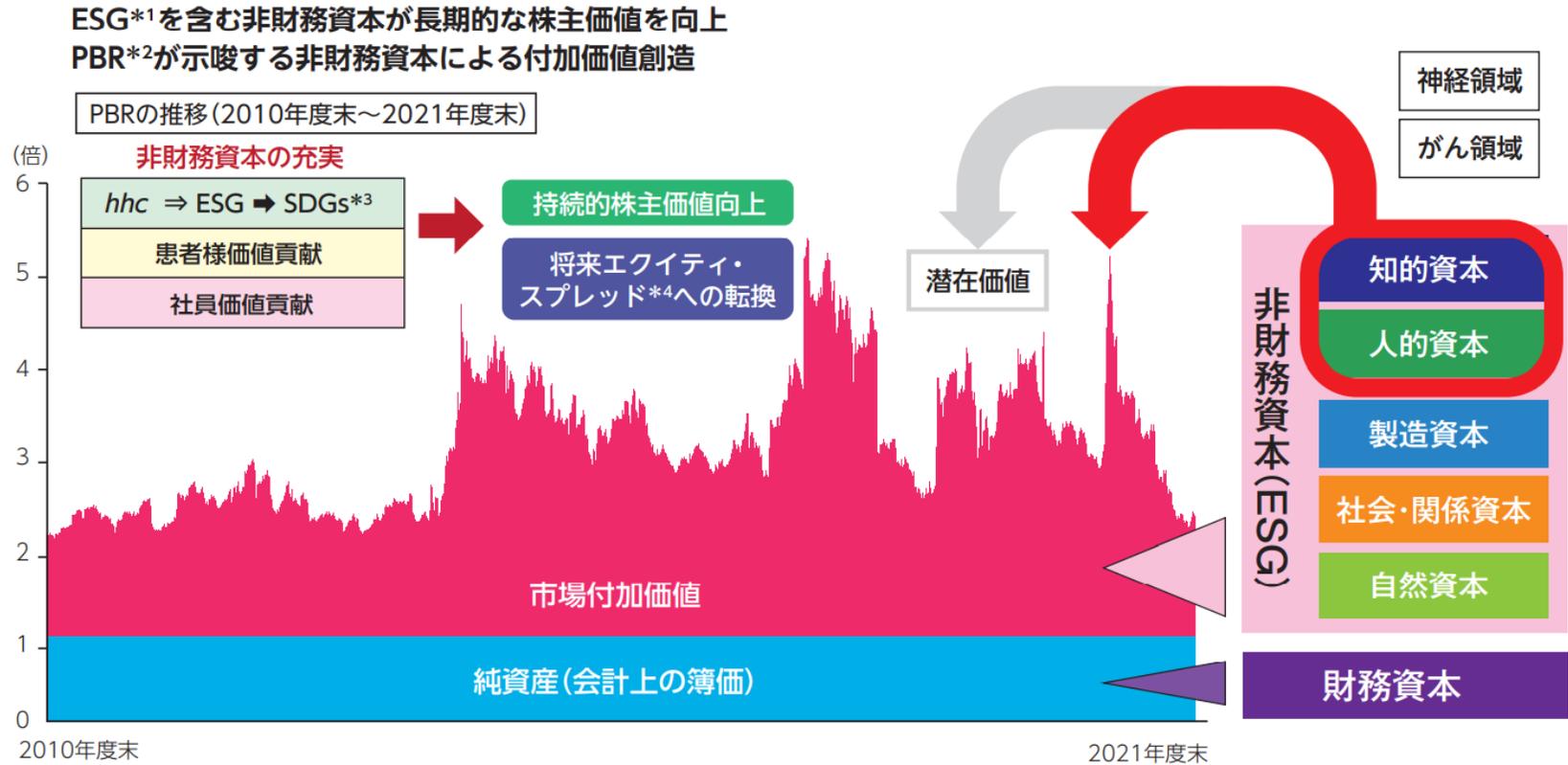
新しい有形・無形資産

財務物的	旧型の貸借対照表、クレジット
社会	規範、コミュニティ、支持・提言
自然	資源、上・下流のフットプリント
ブランド	アイデンティティ、デザイン、経験
知財	発明・イノベーション・アイデア
人的	人材、労働力、顧客ネットワーク

出典: WBCSDの資料、IIRC「統合報告に関するディスカッション・ペーパー」および、OCEAN TOMO, LLC、The 2018 EPIC Report, Embankment Project for Inclusive Capitalismを基に加工

● 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～

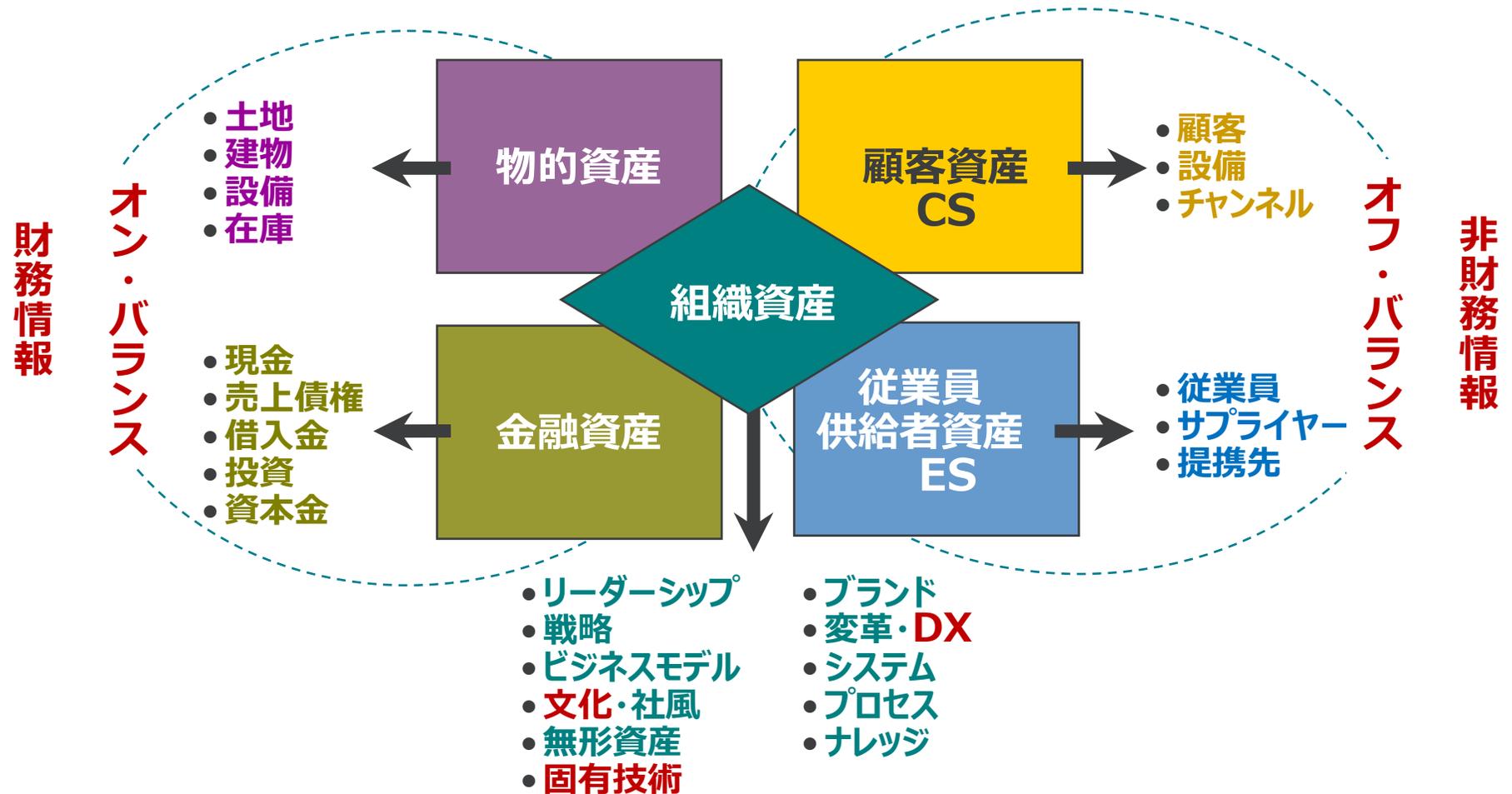


- *1 Environment (環境)、Social (社会)、Governance (企業統治)
- *2 Price Book-Value Ratio (株価純資産倍率)
- *3 Sustainable Development Goals (持続可能な開発目標)
- *4 ROE (親会社所有者帰属持分当期利益率) - 株主資本コスト (当社は8%と仮定)

柳良平『CFOポリシー第2版』中央経済社(2021)を一部改編

企業価値の源泉 ～バリューダイナミクス～

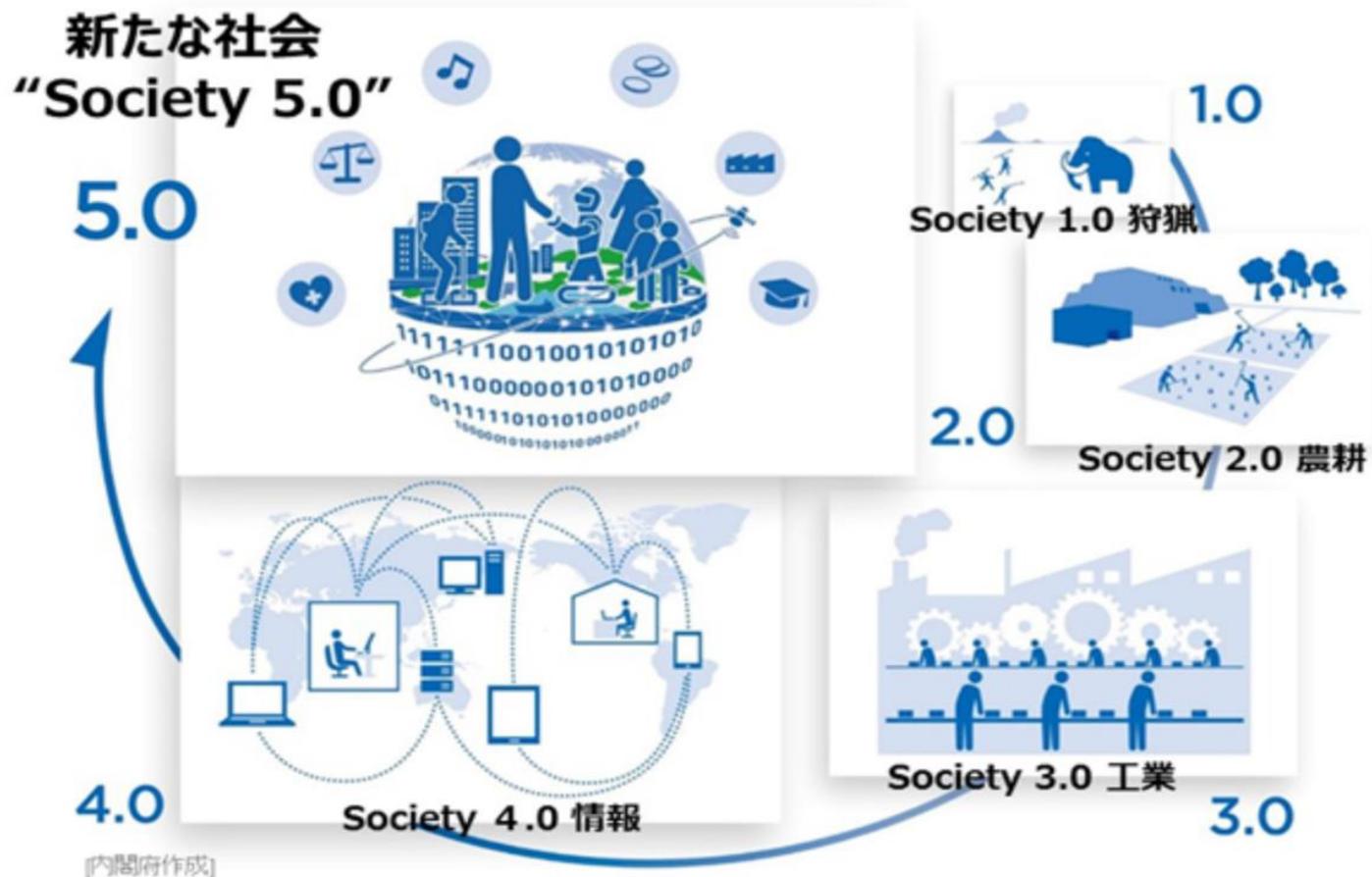
価値を生み出す“資産”は変化している～この資産に影響を与えるものがリスク



2. Society5.0とアジャイル・ガバナンス

Society 5.0とは

サイバー空間とフィジカル空間の融合したシステム、**CPS** (Cyber-Physical System)により社会課題の解決と経済成長の双方を実現する人間中心の社会



新たな価値で経済発展と社会的課題の解決を両立

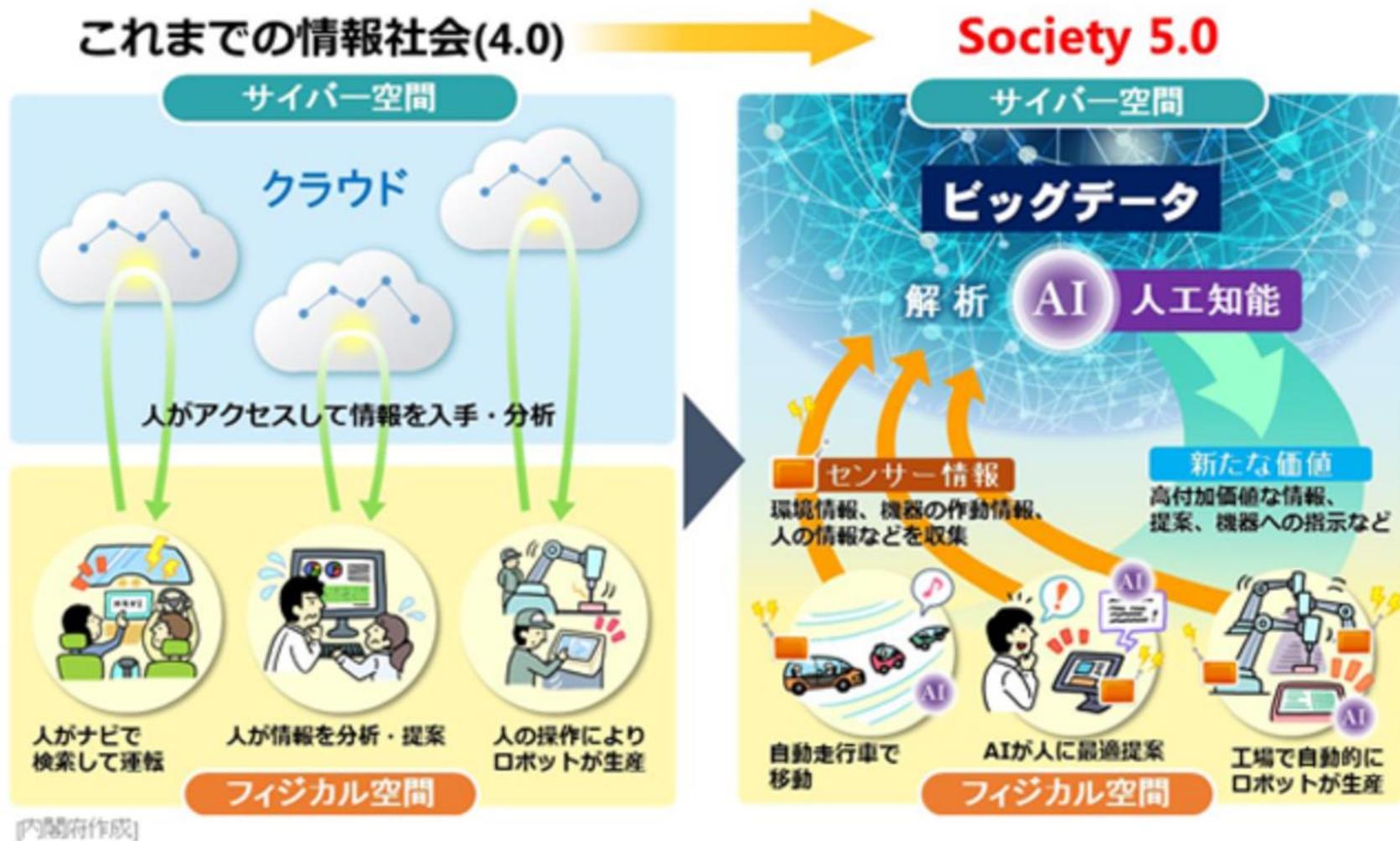


[内閣府作成]

新たなガバナンス・システムが不可欠

ガバナンスのプロセス（ルール形成、モニタリング、エンフォースメント）

ガバナンスの主体（国家、企業、コミュニティ・個人）に着目した新たなガバナンスシステムの構築



伝統的ガバナンス・モデルの限界

- 従来の**社会統治の意味でのガバナンス**は規制当局が中心的役割
- 企業活動・社会活動の変化の加速度化・デジタル化・複雑化・グローバル化等により規制当局を中心とした伝統的な**「垂直型」ガバナンスモデル**:
 - ①ルール形成、
 - ②ルールの遵守状況をモニタリング、
 - ③違反に対するエンフォースメントを実施

は、**機能不全**を起こしつつある

① ルール形成における課題

- サイバー空間 + フィジカル空間が融合したCPSでは変化が早く、AI等の自律的に駆動されるシステムが他システムと複雑に相互作用
- 事前にリスクを特定し、最適制御を明示し、ステークホルダーが遵守すべきルールの明示が困難
- むしろ、事前の詳細なルール設定は、すぐに陳腐化し、かえってリスクやコストの高い制御方法を強制することに。
- さらに、イノベーティブな制御方法のタイムリーな社会実装を妨げる要因となる可能性も。またルール形成に必要な情報が、民間側に偏在し、規制当局のアクセスが困難に

② モニタリングにおける課題

- 従来は、**規制当局**が法令違反等を含むオペレーション状況を定期的に検査し監督
- 一方で、企業活動の複雑化とともに、サイバー空間の特徴として、その活動や製品を規制当局などの第三者が正確に観察し適時に、**不正や欠陥を発見・摘発することが困難に**
- また規制当局による定期検査や定期報告では、**画一的に実施される非効率性**、および直ちに改善を要する問題があっても、定期検査までは発覚しないという遅延性を生む

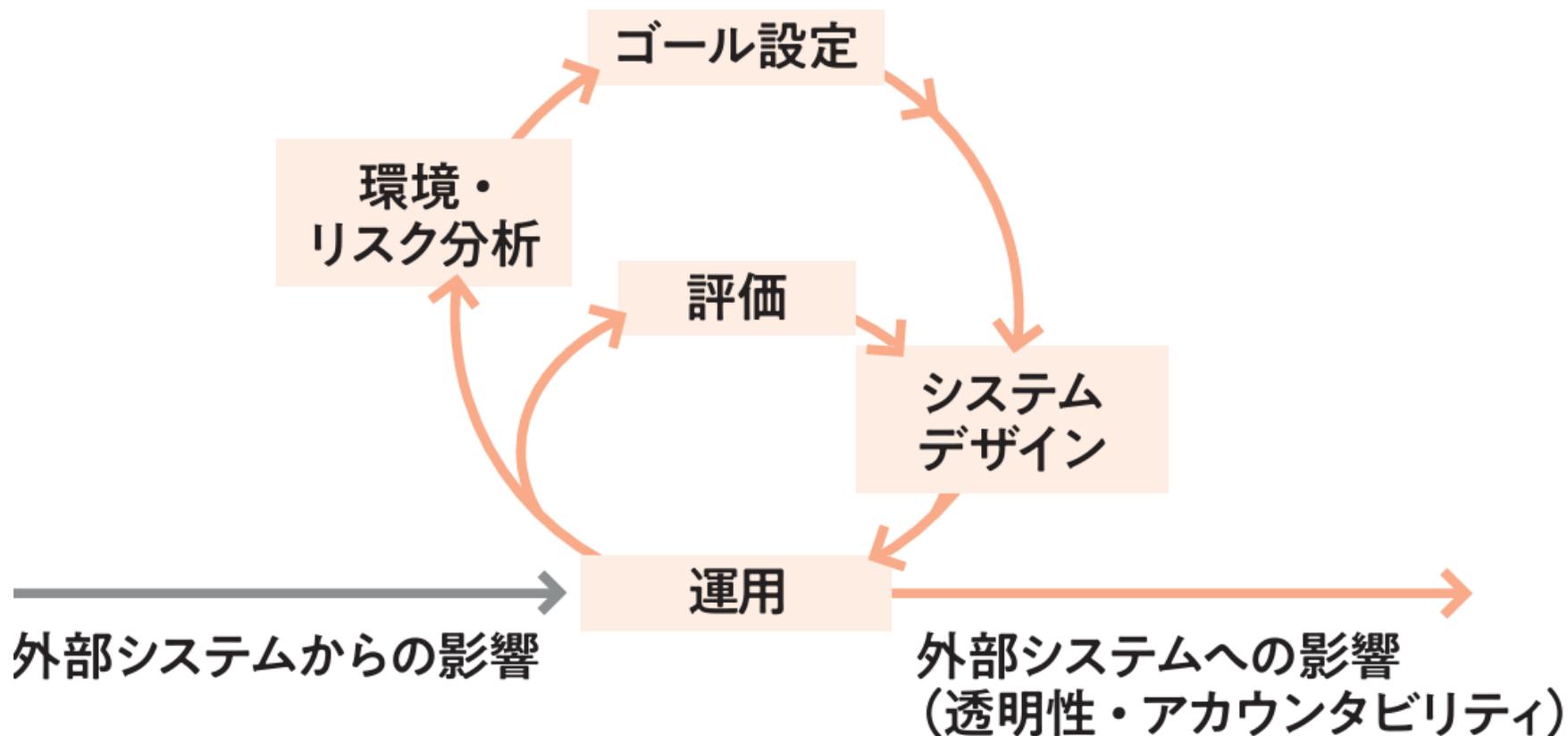
③ エンフォースメントにおける課題

- 従来の変化のスピードが遅く安定した社会では、行為者の行為は**相対的に予見可能**であり、**故意過失など帰責事由の有無を判断し**、法的制裁を個人や法人に課すエンフォースメントが主流
- 一方で、フィジカル空間とサイバー空間の融合が進行して、**AI等が自律的な判断によって予見困難な事故を招来させた場合、その法的責任の所在の特定は困難**。また特定の主体に制裁を加えることが、今後の法益侵害の予防効果を発揮しえない場合も増加
- さらに、サイバー空間の拡大、匿名性の特徴、企業活動のグローバル化によって、**自国だけの法執行確保がより困難に**

アジャイル・ガバナンスとは

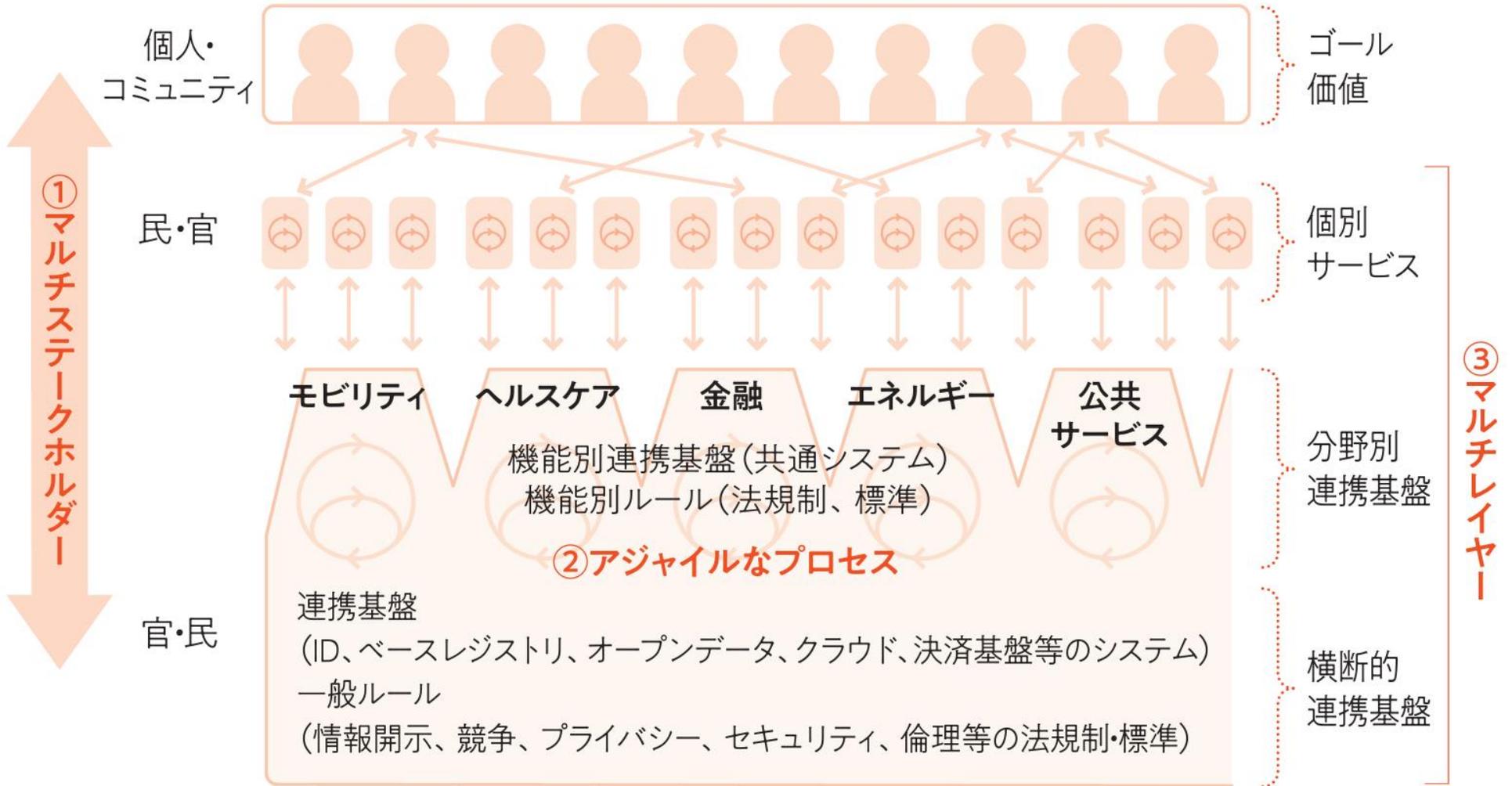
- 定義：CPSによって生じうるリスクを受容可能な程度に管理しつつ、**CPSがもたらす正のインパクトを最大化する仕組み**
- 政府だけでなく企業、ユーザー、市場参加者等の**マルチステークホルダー**がガバナンスの各プロセスに主体として参加
- CPSを構成する多様なサブシステムにおいて、「**ゴール設定**」、「**システムデザイン**」、「**運用**」、「**評価**」、「**環境リスク分析**」といったガバナンスサイクルをアジャイルに回転
- 各ステークホルダーが、そのガバナンス過程で協調する仕組みであり、階層化、分散化されたガバナンスシステムが相互影響し、CPS全体のガバナンスを創発（Governance of Governance）

アジャイルガバナンスのサイクル



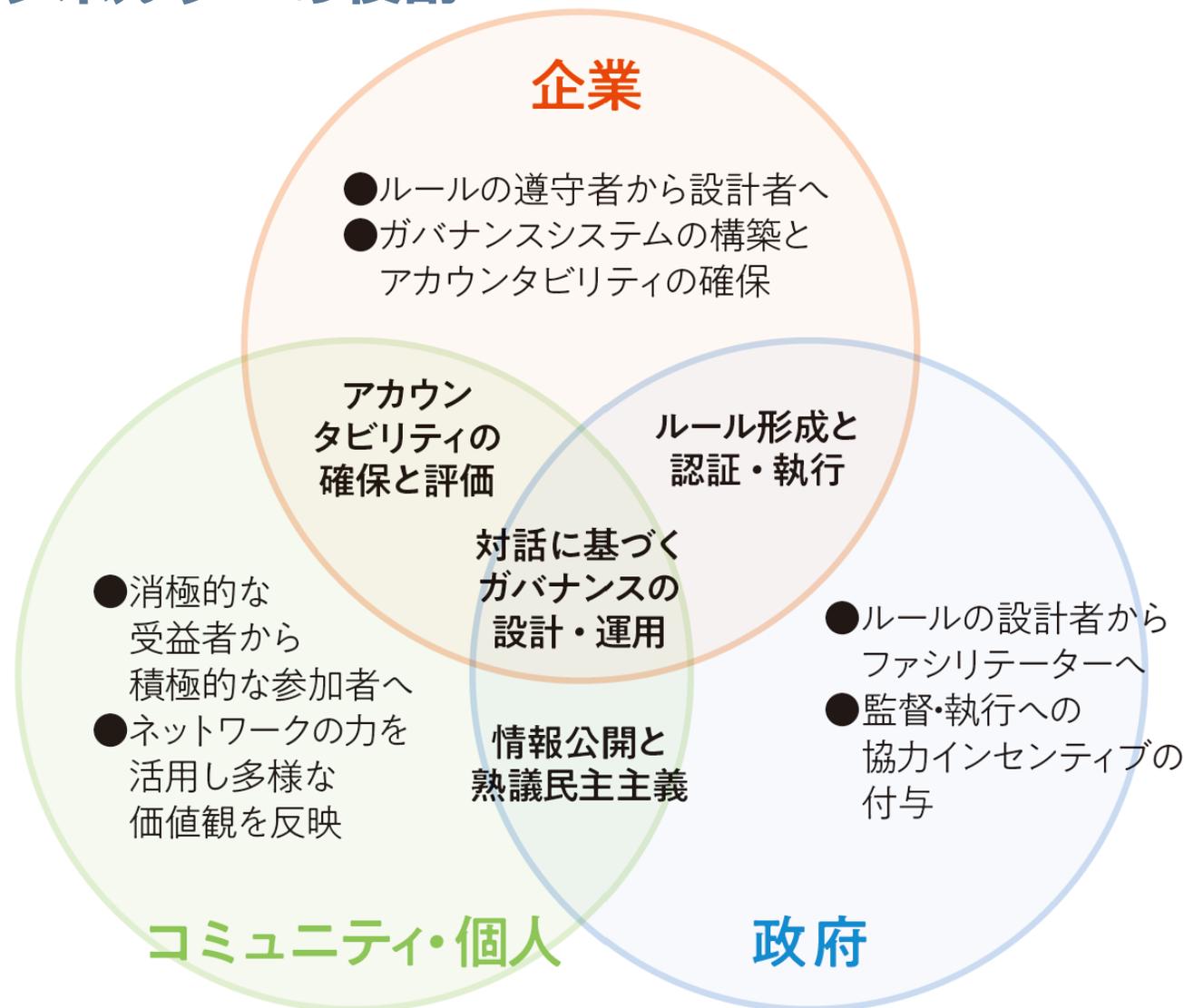
出典：2022年8月8日経済産業省「アジャイル・ガバナンスの概要と現状」報告書

アジャイル・ガバナンス・モデルの全体像のイメージ



出典：2022年8月8日経済産業省「アジャイル・ガバナンスの概要と現状」報告書

各ステークホルダーの役割

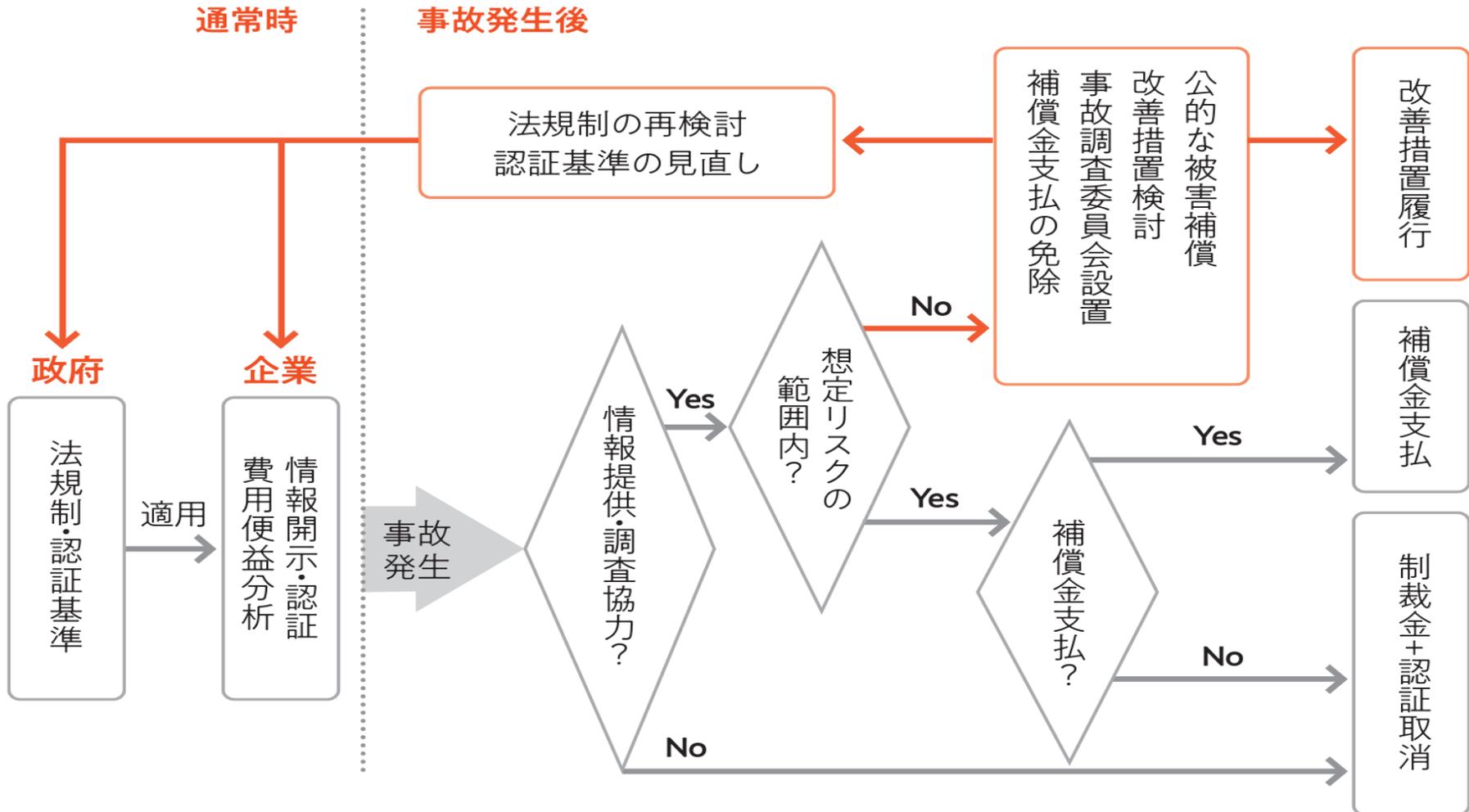


出典：2022年8月8日経済産業省「アジャイル・ガバナンスの概要と現状」報告書

政府の役割の変化

- 独占的な垂直的統治者から各ステークホルダーの協調行動のファシリテーターに（主たる役割は、各ステークホルダーの協調行動を引き出すインセンティブ設計・インフラ整備）
- 各ステークホルダーが示した実現すべきゴールの達成に向けて積極的にガバナンスを行うことを促進、インセンティブの付与
EX. 重要事項の情報開示、認証制度、望ましいガバナンスのガイドライン策定を後押し
- CPSにおいて事故などのネガティブな結果に対する対処→事実関係の解明、ガバナンスシステムの改善への協力を求める仕組みも重要

イノベーションとリスクをバランスし続けるインセンティブを与える制裁制度



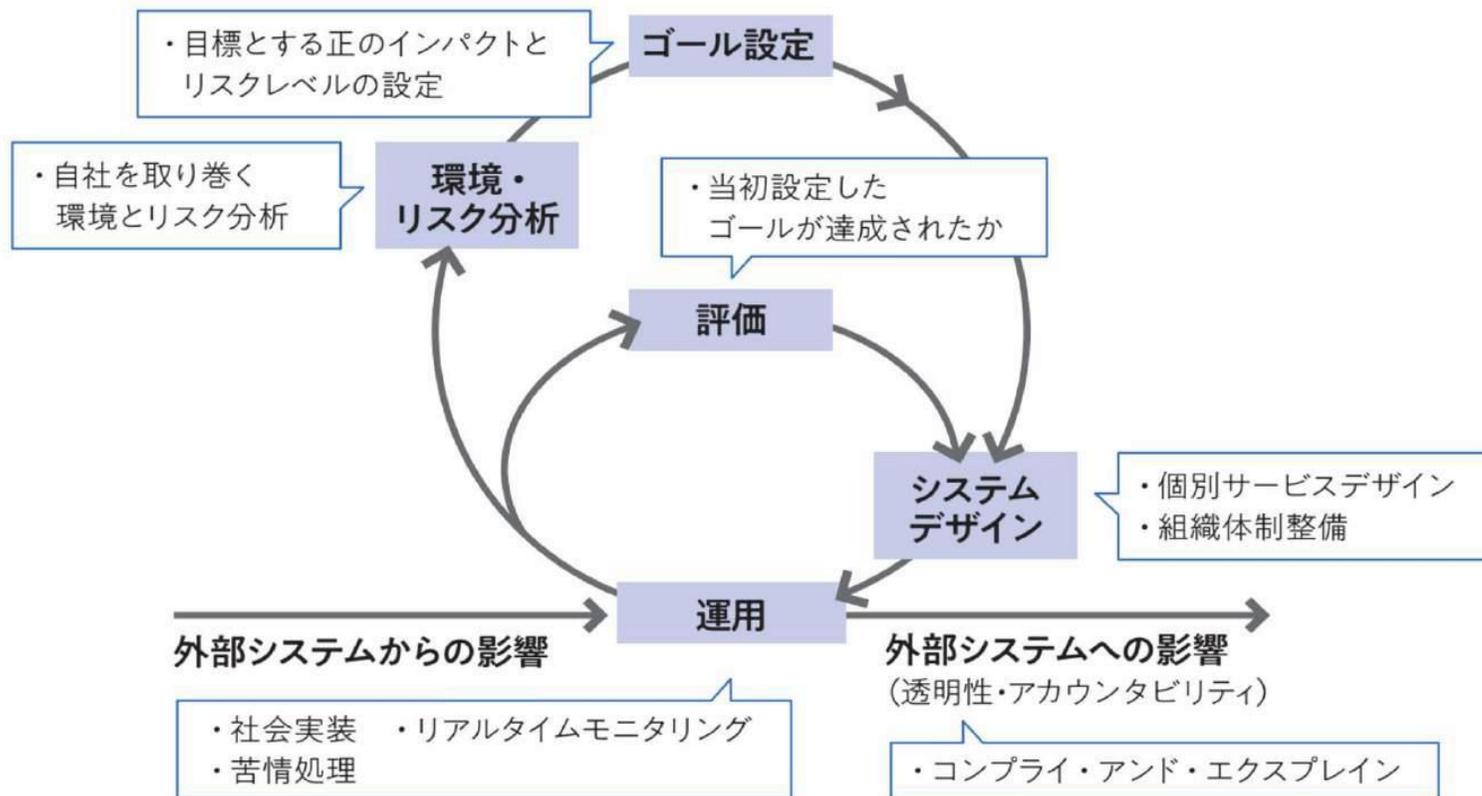
※不確実性をリスクに転換するサイクルを**橙枠**で示す

出典：2022年8月8日経済産業省「アジャイル・ガバナンスの概要と現状」報告書

企業の役割の変化

- 受動的なルールの遵守者 から、 **ルールおよび社会システムの共同設計者・共同運用者**に（情報提供、課題の共有、自主規制の設計・運用という形でルール形成プロセスに参加）
- ステークホルダー間で共有されたゴールの実現のため主体的役割を担い、その方法の選択には裁量の余地はあるも、判断や活動についてのアカウントビリティ（**Comply and explain**）が求められる
- **企業に関わるCPSでの事故や不正**が発覚した場合、率先して事実関係・原因究明し、改善措置と結果を当局と共有し、これを可能とするガバナンスの設計・運用・エンフォースメントを担う

アジャイル・ガバナンスにおける企業の役割

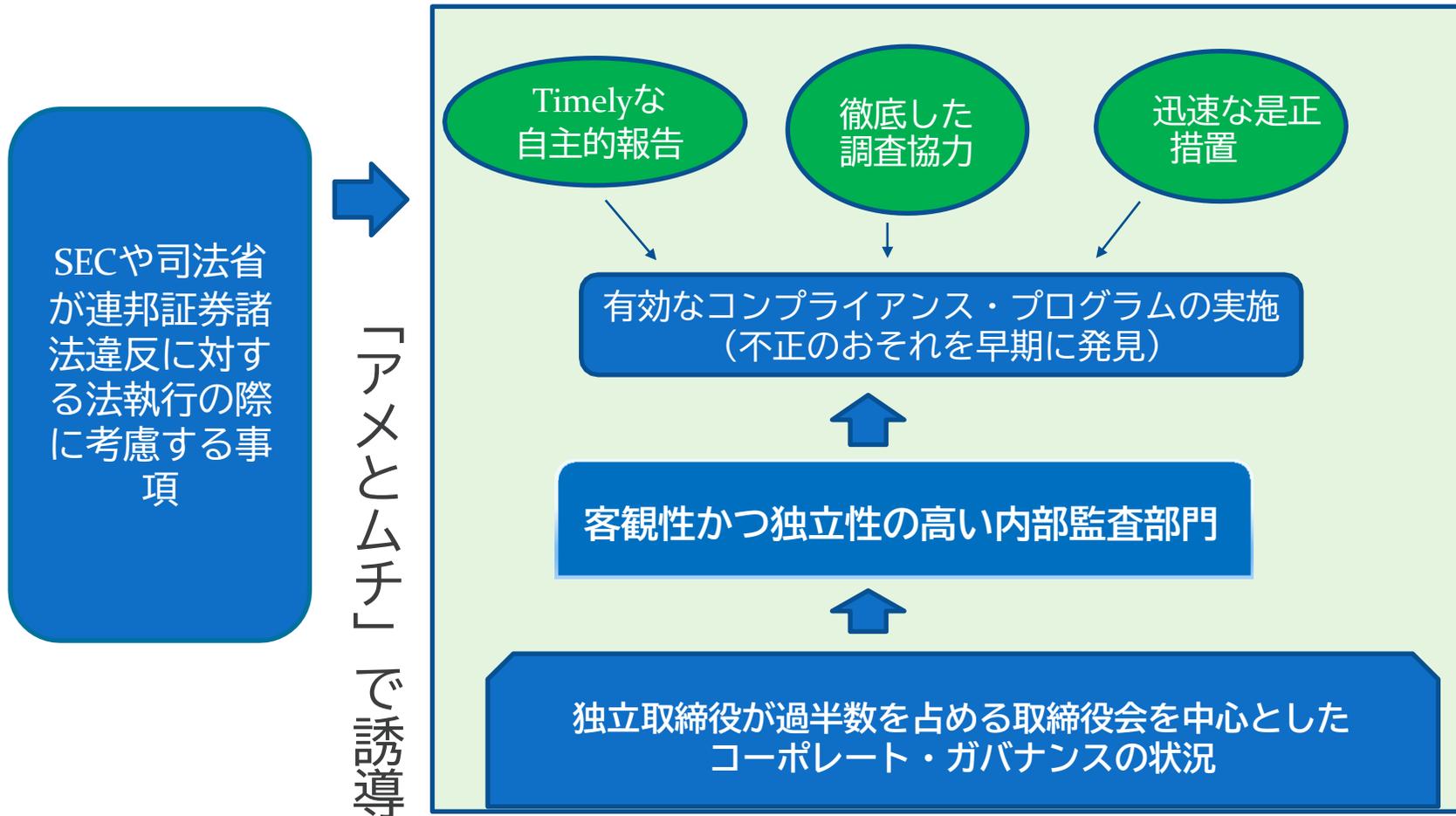


出典2021年「GOVERNANCE INNOVATION Ver.2 – アジャイル・ガバナンスのデザインと実装に向けて」

米国・英国の動き

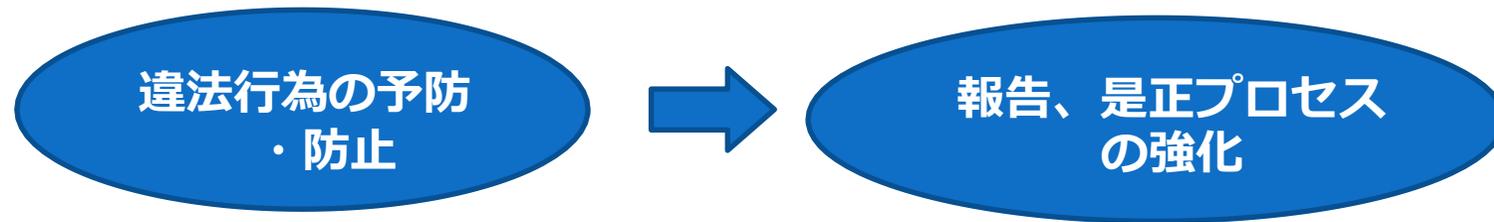
米国のコンプライアンスプログラムの有用性

～訴追延期合意：DPA・訴追免除合意：NPAの背景



米国2010年連邦量刑ガイドライン改定以降の方向性

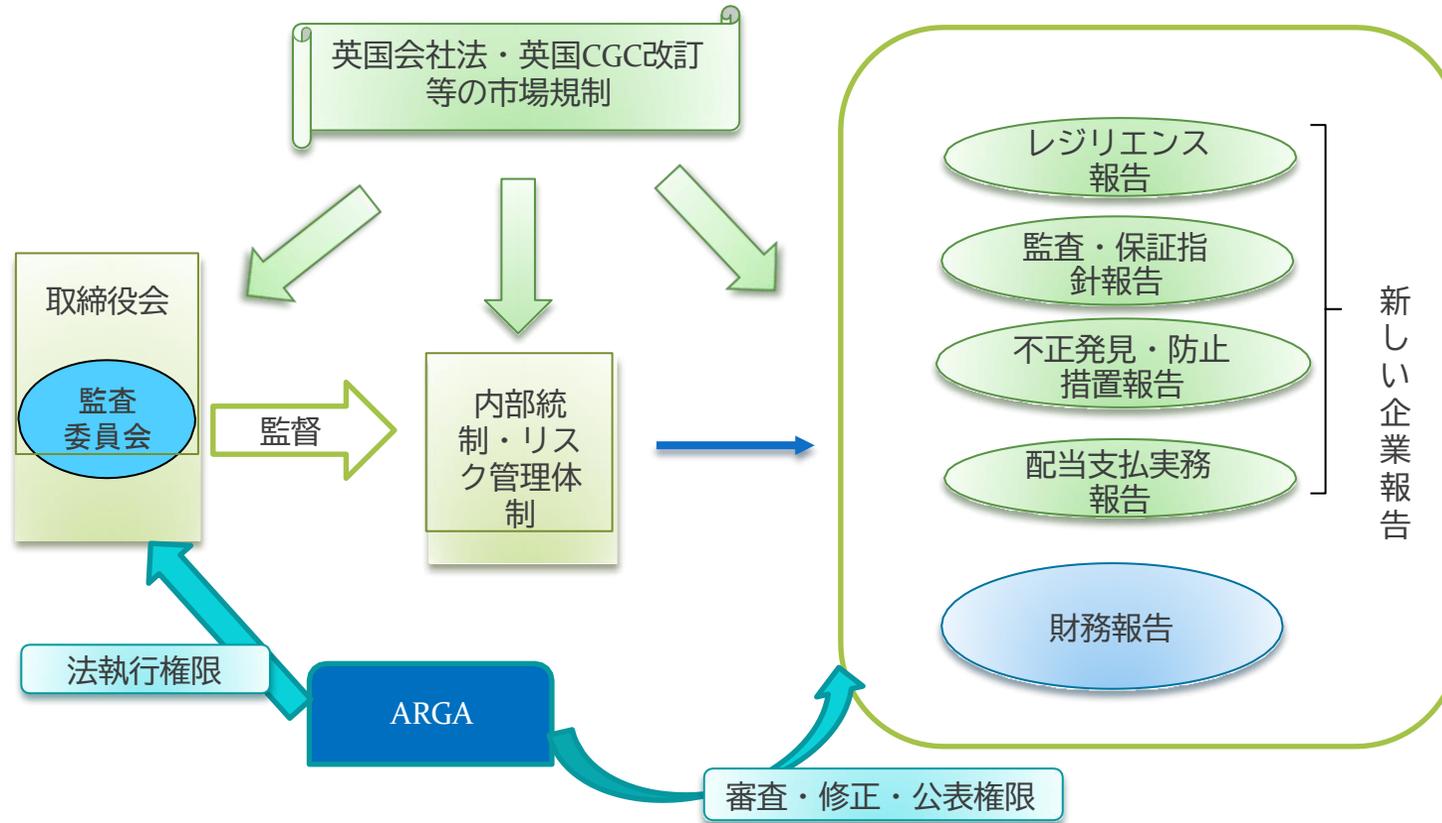
～違反企業の量刑判断に考慮される企業内コンプライアンス体制の焦点の変化



自主的な調査に基づき企業が自ら不正を発見し、これを最初に規制当局に報告した場合には、量刑減輕の考慮事由となり、企業内の情報ラインの透明化、不正発見時の企業の迅速な対応と改善を可能とするCPを要求

もっとも、量刑ガイドラインは、有罪判決の際に適用されるため、その影響力は相対的に小さく、むしろ、**訴追前の検察によるDPA・NPAが企業にとってのインセンティブ規制として重要。**

英国で進行するガバナンス改革（1）



ARGA: Audit, Reporting and Governance Authority: 監査・報告・ガバナンス庁

英国で進行するガバナンス改革（2）

- 年次報告書に含まれる新しい企業報告書については**ハードロー**で法定し、その内容の信頼性を確保すべく法執行権限を強化した新しい規制主体（**ARGA**）を創設
- 企業に対しては、**ソフトロー**である**CGC改訂**により、年次報告書の記載事項としてガバナンスの充実を含む非財務情報の開示と、**新しい企業報告の信頼性を確保するための「リスク管理と内部統制」の構築・維持**および内部統制に対する外部監査の導入の見直しを監査委員会に要請
- 現在進行形で変化し続ける**非財務報告の要請に柔軟に対応できるコーポレートガバナンスの発展に貢献するアプローチ**を採用。
- **ソフトローとハードローの連携**として、長期かつ持続可能性を重視する経営戦略的視点から、足元のリスク管理と内部統制を日々実践することで、**変化の時代のガバナンス改革を推進**

3. アジャイルガバナンスへ取り組むには ～COSO ERMアジャイル版の活用

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・ERM・内部統制の三者の共通点はプロセスであり、プロセスの継続的改善が大切です

ガバナンスがERMを包含（リスク監視）
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・実行する

内部統制とは、経営者が設定する許容度の範囲内
に、プロセスが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
プロセスが許容範囲に収まるようリスクを軽減すること

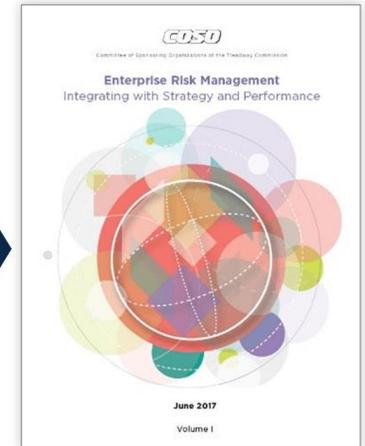


出典：2013及び2017COSO、
一部加工

プロセスである限り、原則主義に則り、経営理念や方針に基づき、自らあるべき姿を念頭に構築すべきです。
JSOXを含め、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です。

* 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

2017COSO ERMの5要素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

戦略と目標設定

6. 事業環境を分析する
7. リスク選好を定義する
8. 代替戦略を評価する
9. 事業目標を組み立てる

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する
13. リスク対応を実施する*
14. ポートフォリオの視点を策定する

レビューと修正

15. 重大な変化を評価する
16. リスクとパフォーマンスをレビューする
17. ERMの改善を追求する

情報、伝達および報告

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

* 原則13の受け口として、2013年COSO内部統制フレームワークがあり、合わせて参考にする必要があります。

TCFD提言とCOSO ERMの親和性

- ✓ 自社の気候変動のリスクと機会について把握し、4項目（ガバナンス、戦略、リスクマネジメント、指標と目標）について開示することを推奨している。
- ✓ 気候変動のリスクを特定し、評価し、マネジメントするプロセスが、全社的リスクマネジメントにどのように統合されているかを開示することを推奨している。

推奨される気候関連財務開示の中核要素



ガバナンス

気候関連のリスクと機会に関する組織のガバナンス

戦略

気候関連のリスクと機会が組織の事業、戦略、財務計画に及ぼす実際の影響と潜在的な影響

リスクマネジメント

気候関連リスクを特定し、評価し、マネジメントするために組織が使用するプロセス

指標と目標

関連する気候関連のリスクと機会の評価とマネジメントに使用される指標と目標

リスクマネジメント: 組織がどのように気候関連リスクを特定し、評価し、マネジメントするのを開示する。

推奨開示 a)

気候関連リスクを特定し、評価するための組織のプロセスを記述する。

推奨開示 b)

気候関連リスクをマネジメントするための組織のプロセスを記述する。

推奨開示 c)

気候関連リスクを特定し、評価し、マネジメントするプロセスが、組織の全体的なリスクマネジメントにどのように統合されているかを記述する。

アジャイルガバナンスへCOSOガイダンスの活用



内部統制の統合的
フレームワーク

全社リスクマネジメント
統合的フレームワーク

全社リスクマネジメント
ESG関連リスクへの適用

全社リスクマネジメント
スピードとディスラプション
の時代における組織の
アジリティ・俊敏性を実現

サステナビリティ報告の効果的な内部統制
～COSO内部統制フレームワークの適用～
“ICSR”

改定版 2013年

改定版 2017年

2018年

2022年

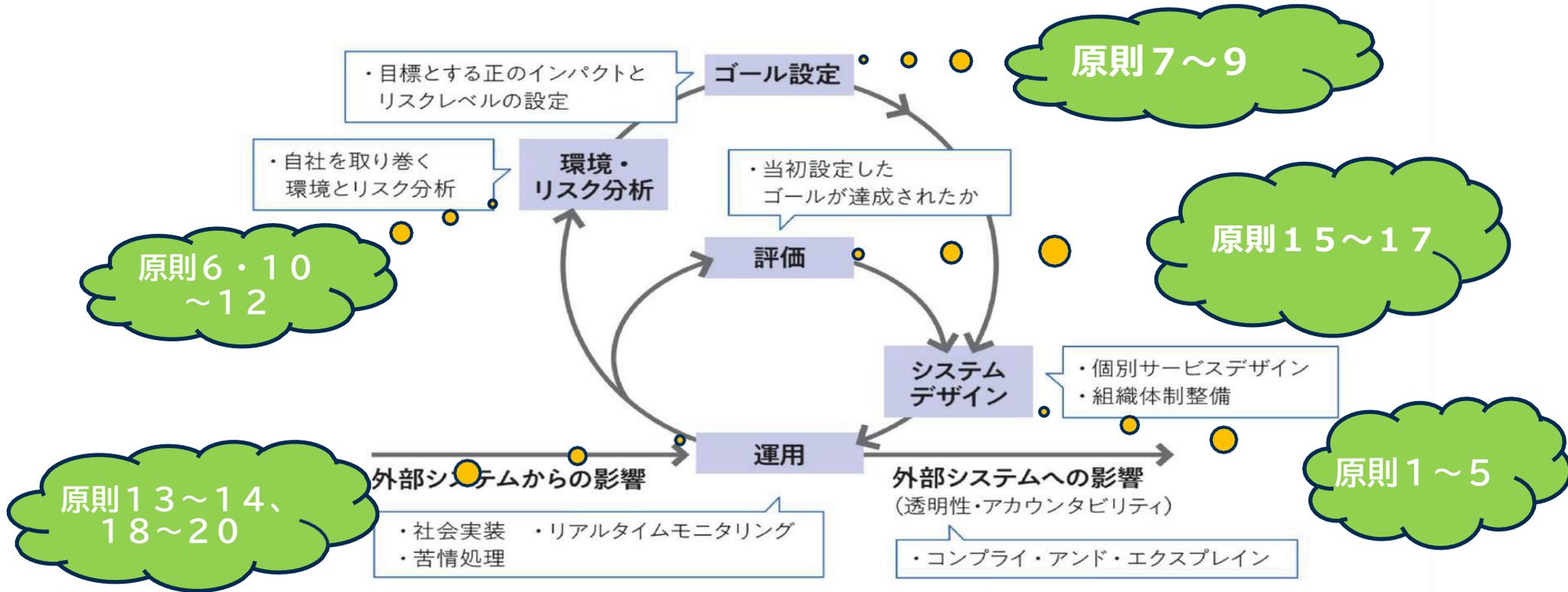
2023年

全社的リスクマネジメント

～スピードとディスラプションにおける組織のアジリティを実現～10の要点

1. 変化のスピード、リスク、ディスラプションにより、企業は**ビジョンと戦略を適宜見直す**。
2. **アジャイルとは戦略の延長**であり、アジャイルでないことは戦略的な誤りとなりうる。
3. リーダーは戦略的アプローチが経営環境において成功するか**定期的に評価**すべきである。
4. **リスクを取ることは素晴らしいことだが、決して無謀であってはならない**。
5. ニューノーマルや新しいビジネスモデルでは変化の**スピード、リスク、ディスラプション**を考慮に入れる必要がある。
6. アジャイルにより、あるリスクに対処する際に**他のリスクに波及**しうることに注意が必要。
7. **ノイズ、環境、戦略、ビジネスモデル**を評価し、ノイズをビジネスモデルにリンクさせるための新しいツールと方法が利用可能となる。
8. **優れたERMアプローチ**は、正しい戦略とリスクに焦点を当てることで、組織がより成功する上で大きな要因となる。
9. **市場のノイズを収集し理解**し、それがビジネスやオペレーションモデルにどのように影響するかを把握し、**早期警告システム**を構築することが重要となる。
10. 組織は定期的にERMを評価し、その仕組みが現在の環境、戦略的アプローチ、および事業部門との目的、ミッション、との**適合状況を見直す**べきである。

COSOERMとアジャイルガバナンス・サイクルとの親和性



出典2021年「GOVERNANCE INNOVATION Ver.2 - アジャイル・ガバナンスのデザインと実装に向けて」

ERMを活用したアジャイルガバナンスからの 取締役会へのインプリケーション

- **ゴールベースで企業の事業戦略を常に見直す**ことが可能となるアジャイルな体制づくりの重要性
- **リアルタイムに内外の経営環境を把握し**、システムの変更修正を促すための、**3ラインモデルの活用**（2024年1月グローバル内部監査基準公表）
- 取締役会として、さらなる透明性、アカウンタビリティの確保に向けて、最終的には**リアルタイムディスクロージャーに対応可能な適時開示体制**の構築・整備が企業価値向上に繋がる
- **市場圧力によるリスクテイクの促進に加え、事前開示の内容の深さが事故や不正に対する責任減免に考慮される可能性**があるため、マルチステークホルダーによる企業規律、ハードローとソフトローの有機的連携の重要性。**伝統的な民事責任、刑事責任のみに注視するのでは不十分。**

4. 重大化するビジネスにおける人権リスク

多岐にわたる人権問題

企業に関わる人権課題は多岐にわたり、企業のビジネスモデル（操業・サプライチェーンの国・地域等を含む）社会的状況、認識とともに重点となる分野は異なる

1 賃金の不足・未払	賃金の不足・未払、生活賃金	9 強制的な労働	強制的な労働	17 差別的対応・表現	差別
2 労働時間	過剰・不当な労働時間	10 居住移転の自由	居住移転の自由	18 ジェンダー	ジェンダー（性的マイノリティを含む）に関する人権問題
3 労働安全衛生	労働安全衛生	11 結社の自由	結社の自由	19 表現の自由	表現の自由
4 社会保障	社会保障を受ける権利	12 外国人労働者	外国人労働者の権利	20 先住民族・地域住民の権利	先住民族・地域住民の権利
5 パワハラ	パワーハラスメント（パワハラ）	13 児童労働	児童労働	21 環境・気候変動	環境・気候変動に関する人権問題
6 セクハラ	セクシュアルハラスメント（セクハラ）	14 テクノロジー・AIに関する人権問題	テクノロジー・AIに関する人権問題	22 知的財産権	知的財産権
7 マタハラ パタハラ	マタニティハラスメント/ パタニティハラスメント	15 プライバシーの権利	プライバシーの権利	23 賄賂・腐敗	賄賂・腐敗
8 ケアハラ	介護ハラスメント（ケアハラスメント）	16 消費者の安全と知る権利	消費者の安全と知る権利	24 サプライチェーン管理の不徹底	サプライチェーン上の人権問題
				25 経済へのアクセス	救済へアクセスする権利

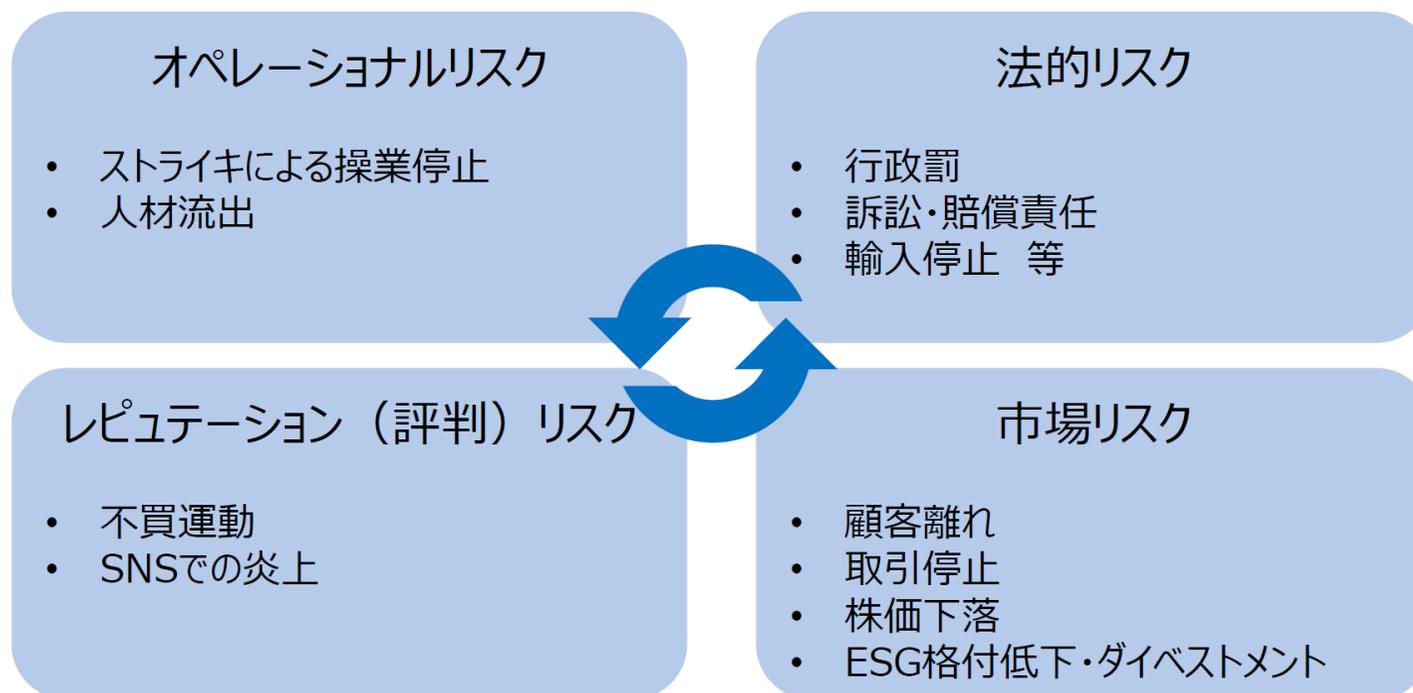
未成年者への性加害

（出所）法務省 今企業に求められる「ビジネスと人権」への対応 詳細版 「ビジネスと人権に関する調査研究」報告書 2021.3

経営における人権問題の重大化

人権意識の高まりとともに、人権課題による経営リスクが増大する。企業の財務的側面や持続的な企業価値創出能力へ影響を及ぼす可能性が高い

人権にかかる経営リスク



(出所) 法務省今企業に求められる「ビジネスと人権」への対応詳細版「ビジネスと人権に関する調査研究」報告書
2021.3を参考に一部加工

人権尊重における主なガイダンス

2011年 国連が公表した
ビジネスと人権に関する
デファクトスタンダード

人権と多国籍企業及びその他の企業の問題に関する
事務総長特別代表、ジョン・ラギーの報告書

ビジネスと人権に関する指導原則：
国際連合「保護、尊重及び救済」枠組実施のために

2018年 OECDが公表した
人権デュー・ディリジェンス
に関する詳細規定



2021年 国連が公表した、10年経過
時の課題と今後の10年に
向けた行動指針

UNGPs 10+ビジネスと人権の
次の10年に向けたロードマップ

2022年 経産省が公表した、国内初の
人権に関するガイドライン

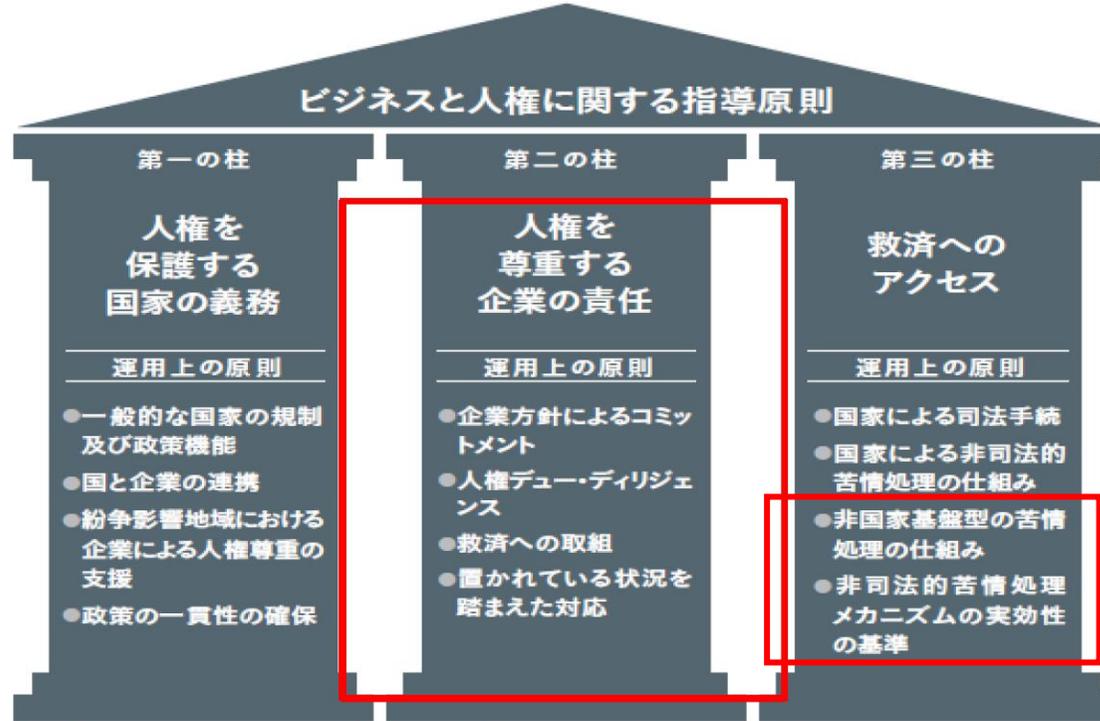
「責任あるサプライチェーン等における人権尊重
のためのガイドライン」

国連のビジネスと人権に係る指導原則

国のみならず、企業も人権への責任を果たすことを求める基本原則が制定された

- 悪影響を引き起こすことの予防、回避、軽減措置と影響が生じた場合は対処することが重要
- サプライチェーンを含むすべての企業の活動における悪影響の予防または軽減に努める責任を負う
- 企業規模、業種等に関係なくすべての企業が人権尊重の責任をはたすことが期待される
- グローバルに統一された人権を尊重（国際人権章典、ILO宣言等に規定）

ビジネスと人権に関する指導原則 3つの柱



(出所) 「ビジネスと人権に関する指導原則」パンフレット、外務省

日本国政府：「ビジネスと人権」に係る行動計画2020～25

欧米諸外国に比べて、日本の法規制・指針は遅れていたが、国連の「ビジネスと人権に関する指導原則」を踏まえて、外務省、経産省を中心に「ビジネスと人権」に関する行動計画を策定

「ビジネスと人権に関する行動計画」における政府から企業への期待

人権方針の策定
(指導原則16)

人権デューデリジェンス・
プロセスの実施
(指導原則17-21)

救済メカニズムの構築
(指導原則22)

サプライチェーンを含む
ステークホルダーとの対話の実施

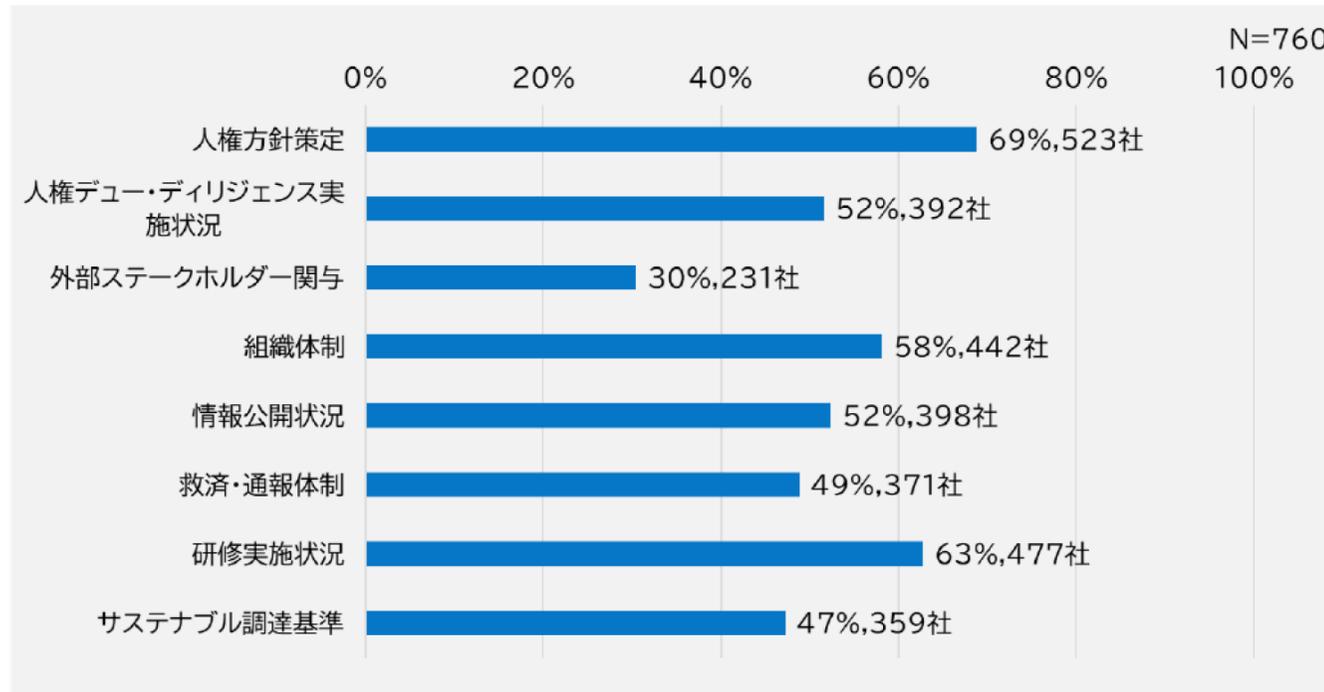
(出所) 「ビジネスと人権」に関する行動計画 (2020-2025)、
ビジネスと人権に関する行動計画に係る関係府省庁連絡会議、2020.10より一部加工

人権リスクに対する日本企業の取組み

日本企業 サプライチェーンにおける人権に関する取組み状況 (回答企業760社)

- 人権方針を策定：7割
- 人権デューデリジェンスの実施：5割
- 情報開示：5割
- 外部ステークホルダーの関与の特定がまだ道半ば

* 人権DD実施企業の内、
間接仕入先まで実施が25%。
販売先・顧客まで実施が10~15%



(出所)「日本企業のサプライチェーンにおける人権に関する取組状況のアンケート調査」 経済産業省、外務省 2021.11

コーポレートガバナンスコード改訂（2021）と人権

改訂コーポレートガバナンス・コードにおいて、人権等のサステナビリティ課題、ダイバーシティ、人的資本、人材戦略に関する対応・開示と取締役会による監督等が記載された

コーポレートガバナンス・コード 人権・人的資本に係る箇所（抜粋）

取締役会	原則2-3. 社会・環境 問題をはじめ とするサステ ナビリティをめ ぐる課題	<p>(補充原則 2 – 3 ①) 取締役会は、気候変動などの地球環境問題への配慮、人権の尊重、従業員の健康・労働環境への配慮や公正・適切な処遇、取引先との公正・適正な取引、自然災害等への危機管理など、サステナビリティを巡る課題への対応は、リスクの減少のみならず収益機会にもつながら重要な経営課題であると認識し、中長期的な企業価値の向上の観点から、これらの課題に積極的・能動的に取り組むよう検討を深めるべき。</p>
	原則4-2. 取締役会の 役割・責務 (2)	<p>(補充原則 4 – 2 ②) 取締役会は、中長期的な企業価値の向上の観点から、自社のサステナビリティを巡る取組みについて基本的な方針を策定すべきである。 また、人的資本・知的財産への投資等の重要性に鑑み、これらをはじめとする経営資源の配分や、事業ポートフォリオに関する戦略の実行が、企業の持続的な成長に資するよう、実効的に監督を行うべきである。</p>
執行	原則2-4. 女性の活躍 促進を含む 社内の多様 性の確保	<p>(補充原則 2 – 4 ①) 上場会社は、女性・外国人・中途採用者の管理職への登用等、中核人材の登用等における多様性の確保についての考え方と自主的かつ測定可能な目標を示すとともに、その状況を開示すべきである。 また、中長期的な企業価値の向上に向けた人材戦略の重要性に鑑み、多様性の確保に向けた人材育成方針と社内環境整備方針をその実施状況と併せて開示すべきである。</p>

7. (補足) 「未成年者に対する性加害に関する標準ガバナンスコード」 における重要な論点

日本取締役協会の未成年者に対する性加害に関する 人権侵害への取組み（1）

2023年9月21日 日本取締役協会富山和彦会長による「未成年者に対する性加害問題と企業のコンプライアンス姿勢に関する緊急声明」より抜粋

- 今回の問題は、経済人に対して、**未成年者を性加害から守るためのコンプライアンスとガバナンス体制**についてより普遍的かつ重い課題を突き付けられた
- 未成年者に対する性加害行為（不同意性交、強制わいせつや性的虐待等）に対する**重大性の認識が弱かったことに根本原因**がある
- 広告主としての取引企業、テレビ番組等で取り扱ってきたメディアには問題意識はあったはずで、関連する書籍や週刊誌報道もあり、2004年には未成年に対する性加害行為が最高裁で確定。この重大犯罪性に鑑みると、**合理的な疑いを示す証拠を見逃したこと自体、ガバナンスの脆弱性**を指摘されてもやむを得ない
- 企業及びメディアは、スポンサーシップの打切りや所属タレントの起用見送りといった**受け身の対応に留まることなく**、我が身を省みる姿勢、そして未来に向けて**未成年者に対する性加害について決して加担しない姿勢**を示すべきである
- 今後、当協会では、リスク・ガバナンス委員会で「未成年者に対する性加害問題に関わる標準ガバナンスコード」策定した上で公表する予定

日本取締役協会の未成年者に対する性加害に関する 人権侵害への取組み（2）

2023年10月12日 日本取締役協会リスク・ガバナンス委員会から公表された
「未成年者に対する性加害問題に係る標準ガバナンスコードについて」前文より抜粋

- 企業による人権尊重に国際的な関心が高まる中、国連人権理事会では「**ビジネスと人権に関する指導原則**」が支持され、各国に**国別行動計画の策定**を促し、持続可能な開発目標（SDGs）達成には、**人権の保護・促進が重要な要素**と位置付け
- 芸能事務所元代表者による未成年者に対する性加害問題に関して、相次いで同事務所とのスポンサーシップ契約を解除し、メディアが同事務所のタレントの起用を見送るといった対応が行われているが、**未成年者に対する性加害に直接的あるいは間接的に関わってきた企業はいかなる行動を取るべきかが、今、問われている**
- そうした中で、「未成年者に対する性加害問題に関わる標準ガバナンスコード」は、国連の「**ビジネスと人権に関する指導原則**」（2011年）、および「**ビジネスと人権の次の10年に向けたロードマップ**」（2021年）を踏まえて策定
- 本コードは、**企業が未成年者の人権を尊重する責任を如何に果たすかに焦点を当てたものであるが、それにとどまらず、企業は時とともに変化する人権尊重に対する企業責任を継続的に果たすことが期待される**

日本取締役協会リスク・ガバナンス委員会2023年10月12日公表 未成年者に対する性加害問題に関わる標準ガバナンスコード

標準ガバナンスコードの構成：5つの基本原則と10の補充原則

基本原則 1. 未成年者の人権の尊重（補充原則1-1）

基本原則 2. 未成年者の人権を尊重する企業の責任（補充原則2-1）

**基本原則 3. 未成年者の人権を尊重する企業が確立すべき方針およびプロセス
（補充原則3-1、3-2、3-3、3-4、3-5、3-6）**

基本原則 4. 負の影響の是正

基本原則 5. 救済（補充原則5-1、5-2）

未成年者に対する性加害問題に関わる標準ガバナンスコード 基本原則 3 (抜粋)

補充原則 3-2 人権デュー・ディリジェンス

未成年者の人権デュー・ディリジェンス：企業は、未成年者の人権への影響を特定し、防止し、軽減し、そしてどのように対処するかについて責任を果たすために、未成年者の人権デュー・ディリジェンス・プロセスを継続的に実施すべきである。

- ① 対象
- ② 未成年者の人権リスクと全社的リスクマネジメント と権利保持者のリスク
- ③ 未成年者の人権リスクへの加担と責任

「刑事責任との関係では、刑法上の「加担」である教唆または幫助のいずれについてもそれぞれについての故意が必要とされているが、民事責任との関係では、過失により責任が基礎づけられ、未成年者の人権侵害、なかんずく、性加害といった極めて深刻な人権侵害に対しては、積極的な調査を怠るという不作為が過失を基礎づけることもあり得ることを認識しなければならない。」

補充原則 3-3 未成年者の人権リスクの評価

企業が引き起こし、または助長する人権に対する負の影響からの是正を可能とする以下のプロセスを構築すべきである。なお、未成年者の人権への影響を評価するためのプロセスは、リスク評価や環境・社会に対する影響の評価などの他のプロセスのなかに組み込むことができる。

未成年者に対する性加害問題に関わる標準ガバナンスコード 基本原則 3 (抜粋)

補充原則 3-4 未成年者の人権リスクへの対応

未成年者の人権に対する負の影響を防止し、または軽減するために、企業はその影響の評価結論を、関連するすべての社内組織およびプロセスに組み入れ、適切な措置をとるべきである。取るべき適切な措置は以下の要因によって様々である。

- i 企業が負の影響を生じさせ、もしくは助長するかどうか、またはその影響への関与が、取引関係によって、その事業、サービスもしくは商品との直接的な結びつきのみを理由として関与してきたものかどうか。
- ii 負の影響に対処する際の企業の影響力の大きさ。

① 負の影響の助長

② 負の影響に取引関係を通じて関与する場合

③ 負の影響を防止または軽減する影響力

④ 取引関係の終了

キーマッセージ：

1. 人権を尊重するとは：

尊重から行動へ

2. 人権に係る企業の責任：

- 惹起型
- 助長型
- 直接リンク型（事業上の関係）影響力の行使

例えば、

芸能事務所
広告代理店、メディア
広告スポンサー等

3. 人権DD（人権リスクマネジメントシステム）：

- 方針の表明、人権リスクの特定、評価、優先順位付け、対応、報告
- 人権リスクは、バリューチェーンで検討する
- リスク管理は、事業リスクに加え、被害者の人権リスクも含めて考慮

4. 是正：影響力の大きさ、取引の停止は是正や被害者救済を考慮して決定

5. 救済：通報対応システムの確立、救済状況の適切な開示

5. テクノロジーリスク ～AIとサイバー攻撃

監査人の見るデジタル活用のリスク

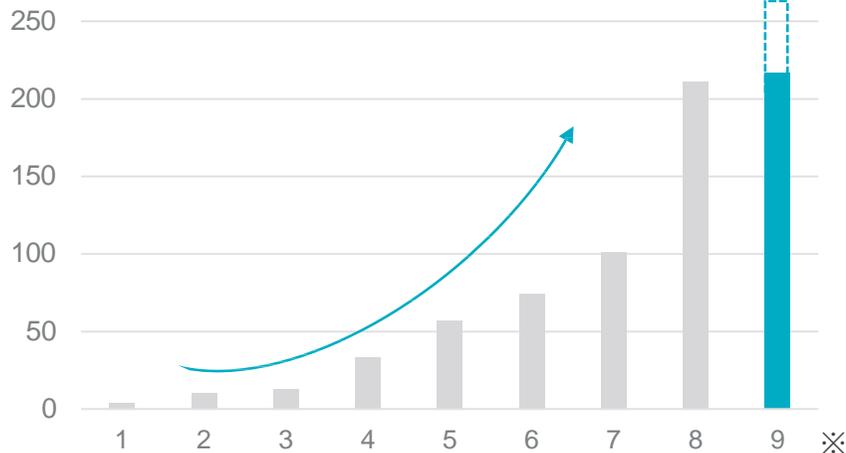
Protiviti: 2023 Global Technology Audit Risk Survey

今後12か月で大きな脅威となる技術的リスク	
サイバーセキュリティ	74%
外部委託先／サードパーティ	60%
データプライバシーとコンプライアンス	58%
データガバナンスと完全性	55%
システム導入とトランスフォーメーション	55%
IT人材の管理	52%
クラウド・コンピューティング	50%
IT BCP（テクノロジー・レジリエンス）	44%
技術的負債と老朽化したインフラ	43%
規制遵守	41%
新しいソフトウェア開発手法	36%
IoT	29%
AIとML（生成AIを含む）	28%

AI関連のインシデント

人工知能を搭載した技術が日々増えている一方、AI関連のインシデント数も年々増加しています

AI 関連のインシデント推移



※データ未反映のため、2021年は暫定値

出典: 『AIAAIC Repository』 <https://www.aiaaic.org/aiaaic-repository> をもとにプロテビティが作成

AIインシデントの例

採用アルゴリズムが男性候補者を優先

- 候補者の履歴書から点数をつけるAIシステムが女性候補者の点数を極端に下げていた
- 過去の男性候補者を学習データとして使用していたため、偏った結果を出力してしまっていた
- 企業はこのシステムは研究目的であり、実用されたことはないと公表した

アクセス権限の誤設定による情報漏洩

- アメリカ大手AI研究チームが秘密鍵、パスワード、個人メッセージなど含む38テラバイト分のデータが漏洩されたと発表した
- クラウドの共有設定に誤りがあり、特定の人物への共有ではなくストレージの権限を持っている全員に共有されてしまった
- 今後は最小権限の徹底を行うと公表した

AIアートによるレピュテーションリスク

- ドラマのオープニングにAIが生成したアートを起用したことにより、アメリカの制作会社に批判が殺到
- 人間の仕事を奪われることに反対し今回に至った
- 制作会社はこれによる職を失ったアーティストはいないとの主張

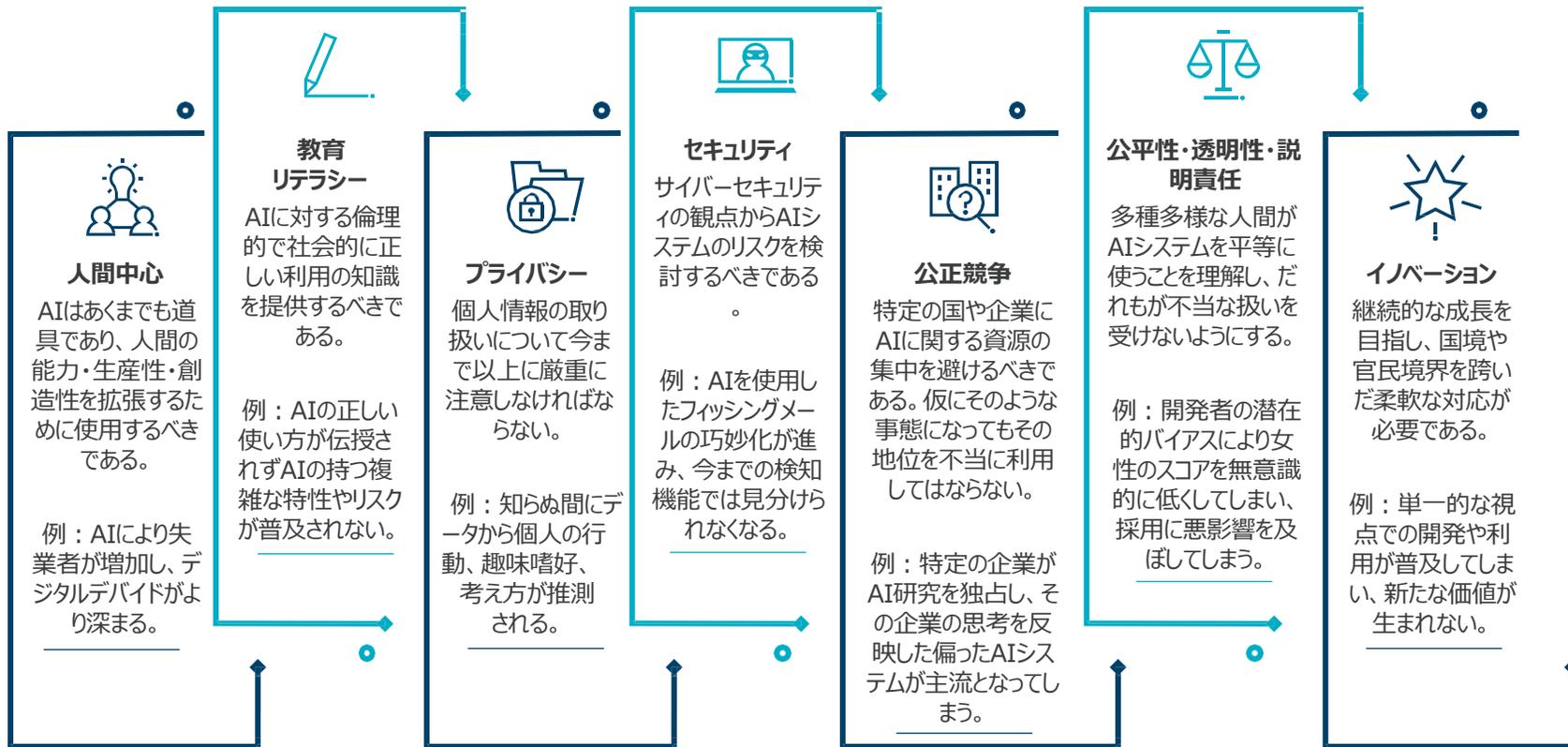
AI関連の各国の法規制等

EUや中国でサービスを展開する際にはデータ越境リスクを鑑み、現段階から規制に遵守した開発を行う必要があります

	タイトル	概要	発行機関・団体	強制力
EU	<ul style="list-style-type: none"> AI法 (AI Act) 	<ul style="list-style-type: none"> リスクベースで「許容できないリスク」「ハイリスク」「限定的なリスク」「低・最小リスク」に分別され、要求事項が異なる 	<ul style="list-style-type: none"> 欧州委員会 	強
中国	<ul style="list-style-type: none"> 生成式人工知能服務管理暫定弁法 	<ul style="list-style-type: none"> 生成AIのサービス提供には事前の登録および中国国家インターネット情報弁公室の許可が必要 	<ul style="list-style-type: none"> 中央7省庁 	強
アメリカ	<ul style="list-style-type: none"> AI Bill of Rights AI Voluntary Commitments 	<ul style="list-style-type: none"> AIに対する5原則 AI開発大手7社による自社規制 	<ul style="list-style-type: none"> ホワイトハウス Amazon, Microsoft, OpenAI他 	中
日本	<ul style="list-style-type: none"> AI原則実践のためのガバナンス・ガイドライン Ver. 1.1 著作権法第30の4 	<ul style="list-style-type: none"> AI開発・利用の際実施すべき行動目標 著作権者の利益を不当に害さない限り、AIは学習してもよいのでは。 	<ul style="list-style-type: none"> 経産省 文化庁 	弱

AIの基本原則

社会および企業は安全で倫理観を有する「責任あるAI」を、AI基本原則に沿って開発する必要があります



出典：内閣府『人間中心のAI社会原則』（2019.3.29 統合イノベーション戦略推進会議決定）

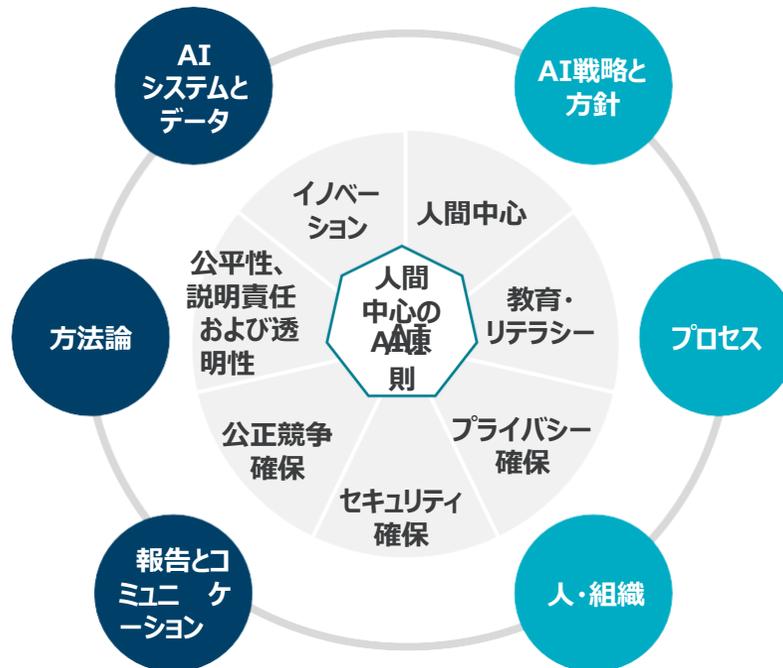
AIガバナンスの必要性

AIガバナンスはAIの進歩と普及に伴うリスクを受容可能な水準まで低減し、技術の発展とリスクのバランスを取るために不可欠です

人間中心のAI原則

What: 最終的に保護されるべきゴール

AI固有のリスクが顕在化する中で、AIの利用は、基本的な人権を侵してはいけないという理念のもと、定められた7つの基本原則



AIガバナンス

How: AI原則をどのように実現するか

AIの利活用によって生じるリスクをステークホルダーにとって受容可能な水準で管理しつつ、そこからもたらされる正のインパクトを最大化することを目的とした、ステークホルダーによる技術的、組織的および社会的システムの設計および運用

出典: 経済産業省『AI原則実践のためのガバナンス・ガイドライン Ver. 1.1』を元にプロティビティが加工

生成AIのリスクとガバナンス

生成AIには課題と不確実性はあるものの、経営者は提供される機会を積極的に捉えるべきです。そのためには、生成AIのリスクとリターンの適切なバランスを見つけることが重要です

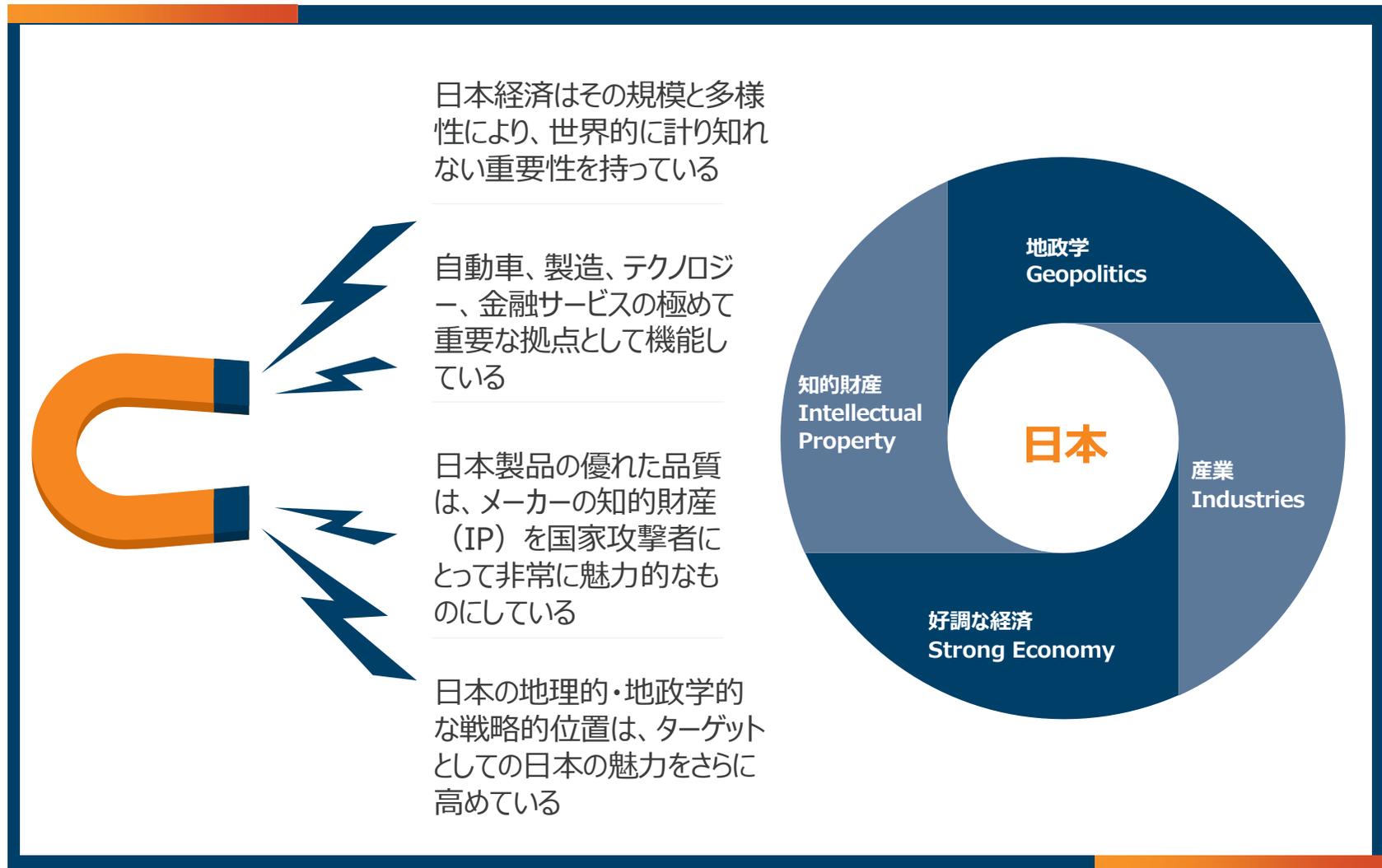
生成AIの5大リスク



生成AIアプリケーション作成に必要なポリシー



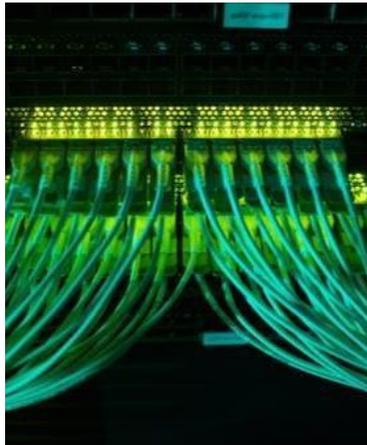
狙われる日本の現状



サイバー攻撃が急速に拡大する理由

01

- 技術的負債と**レガシー・インフラストラクチャ**
- 時代遅れのソフトウェアとハードウェア



03

- **サプライチェーンのサードパーティ**が引き続き標的となる



02

- **デジタルトランスフォーメーション**のスピード
- 急速に拡大する攻撃対象や、安全でないIoTデバイスの利用、サイバー意識の低さ

04

- **物理的な領域への影響**
- キネティック攻撃の進化

日本が直面する新しい脅威

1. 業界横断的なサイバー活動の活発化

サイバー犯罪者は、金融サービス（BFSI）だけでなく、製造業、自動車、航空、小売業など様々な分野で顕著な活動を行っている

2. 焦点を絞った知的財産の抜き取り

知的財産の不正流出、特に重要な分野からの流出には、脅威行為者の間に明確な動機がある

3. 海外子会社および関連会社をターゲット化

最近の日本企業に対する大規模な攻撃の多くでは、攻撃者は、日本の標的のネットワークへの侵入口として、これらの海外子会社または他国の関連事業体の脆弱性を戦略的に悪用している

4. マネージド・サービス・プロバイダーの継続的なターゲット化

マネージド・サービス・プロバイダーは依然としてサイバー犯罪者の標的とされており、彼らに対する攻撃が急増している

05 偽のキャンペーン情報の拡散

詐欺師は、個人を特定できる情報（PII）や行動データを無防備な個人から採取するために、積極的に偽の情報を広めている

06 サプライチェーンにおける脆弱性

主要産業のサプライチェーンは、重大なサイバーセキュリティ・リスクにさらされており、このような脆弱性には、一層の注意と保護対策が必要である

06 次世代のサイバー脅威（Next Gen Cyber Threats）

新しいテクノロジーを使ったサイバー攻撃が誕生しており、その脅威は従来の脅威を凌ぐ可能性がある

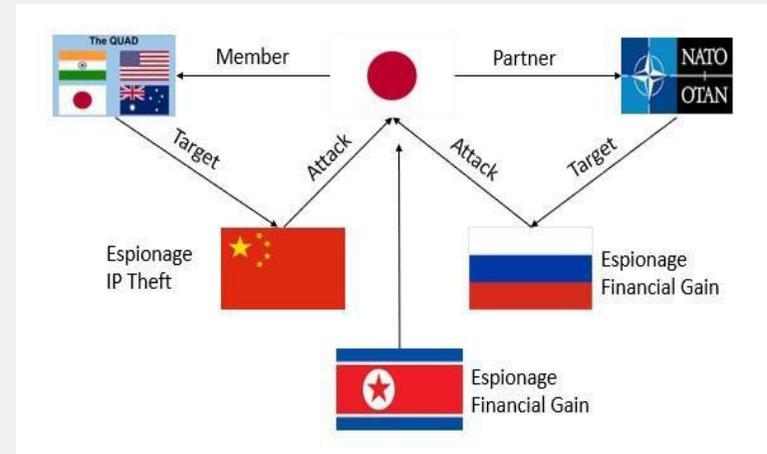
- AIを使った攻撃：攻撃パターンの自動化、ゼロディ攻撃やランサム攻撃の高度化、高度なフィッシング、ソーシャルエンジニアリングの成熟
- 量子コンピューティングの脅威：暗号解読

地政学リスクが引き起こすサイバー脅威



地政学的な見地から、日本は中国、ロシア、北朝鮮に起因する大きな課題に直面している。

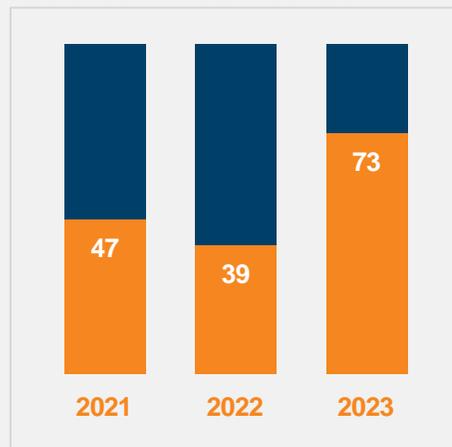
これらの課題は、地域支配、QUADやNATOとの戦略的同盟関係、そして現在進行中の領土紛争に大きく関連している。



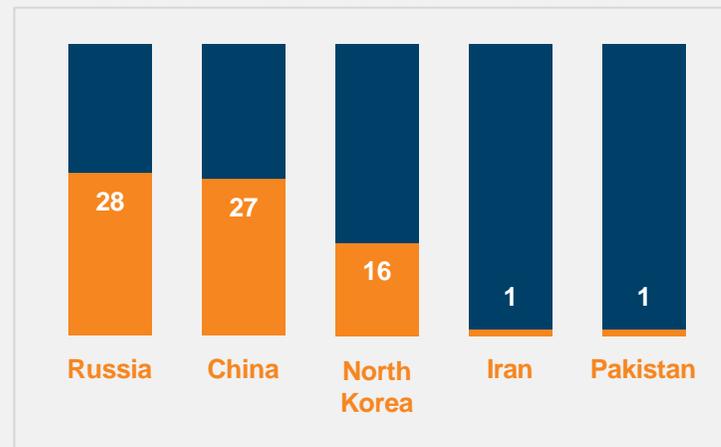
(ご参考) 攻撃キャンペーンの状況①

- 2023年中に日本の様々な産業を標的とした73のキャンペーンが識別された。これらのキャンペーンの背後には、中国、ロシア、北朝鮮の国家に支援された脅威アクターが関与している。
- 過去2年間に比べ、観測されたキャンペーンの数は大幅に増加しており、脅威行為者が経済的・知的大国の日本に関心を寄せていることを示している。
- 2023年、ロシアと中国の脅威者はともに日本を積極的に標的とした。また、北朝鮮の脅威勢力は2022年と比較してキャンペーンを倍増させた。

日本をターゲットにしたキャンペーン



日本をターゲットにしたキャンペーンの実施元

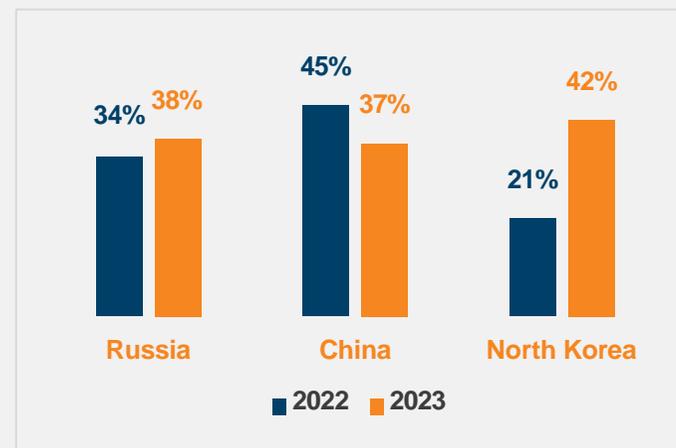


(ご参考) 攻撃キャンペーンの状況②



- 特に、ロシア・ウクライナ戦争に対する日本の立場や、QUADやアジア太平洋問題のようなグローバルフォーラムへの日本の積極的な関与が、日本へのサイバー攻撃に大きく影響しており、地政学的緊張を強調している。
- ダークウェブのトレンドの領域では、中国のサイバースパイ集団が、日本の製造業やテクノロジー企業が保有する知的財産（IP）に対して顕著な脅威を呈していることは明らかである。
- ロシアの脅威行為者の行動には顕著な変化が見られる。彼らは、日本、アジア太平洋地域、EMEAを含む新たな地理的地域を包含するように攻撃範囲を拡大している。
- 北朝鮮のサイバー犯罪グループは、日本の暗号通貨を窃取することに明確な嗜好性を示している。このような嗜好性は、このようなデジタル資産が従来の金融機関の範囲を超えた非伝統的な資金供給源として機能しているという事実から生じている。

実施元別のキャンペーン前年比



サイバー攻撃に対する新しいリスク対策

Cyber Threat Intelligence は、サイバー攻撃に関する脅威アクターの動機、標的、攻撃の振舞いを理解するために、膨大な情報を収集、蓄積、分析し、セキュリティ対策を強化する取り組み



組織外部の攻撃対象

サイバー 脅威インテリジェンス:

- デジタル資産、システム、ネットワークに対する潜在的または実際の**サイバー脅威に関する情報と洞察**
- **サイバー犯罪者が使用する戦術、技術、手順を理解するための、データ収集、分析、解釈**
- 潜在的な脅威や脆弱性に関する実用的な知識の提供
- **サイバー攻撃の積極的な特定、防止、検出、対応を支援**
- **進化する脅威を先取りし、機密データ、知的財産、顧客情報、インフラストラクチャーの保護を強化**

情報の例：オープンソース情報、脆弱性情報、マルウェアの解析結果、不正なIPやドメインの情報

デジタル活用において、取締役会が考慮すべきポイント



- 取締役会は、デジタル活用の議論のために**十分な時間**を割り当てていますか
- 取締役会は、**デジタル活用による投資回収の結果**について議論していますか？
- 取締役会は、**組織のデジタル活用戦略、イノベーション文化、実行プロセス**に満足していますか？



- 取締役会と経営陣は、**組織の技術的債務の程度と性質**を可視化しているか
- TDのリスクとコストの軽減への**実行可能なロードマップ**はありますか？
- TDについて**継続的かつ能動的に管理**していますか
- 効果的なリスク受容の意思決定が行われるように、**TDに対して適切なガバナンス**が行われていますか？



- 企業は、**顕在化しつつあるリスク**を時系列的に認識し、**戦略やそれを支える技術インフラ**を適時に調整していますか？
- デジタル活用に対して、**リスクを十分に低減できるアジリティとレジリエンス**を備えていますか？

Q&A



Face the Future with Confidence[®]

© 2024 Protiviti – Confidential. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.

protiviti[®]