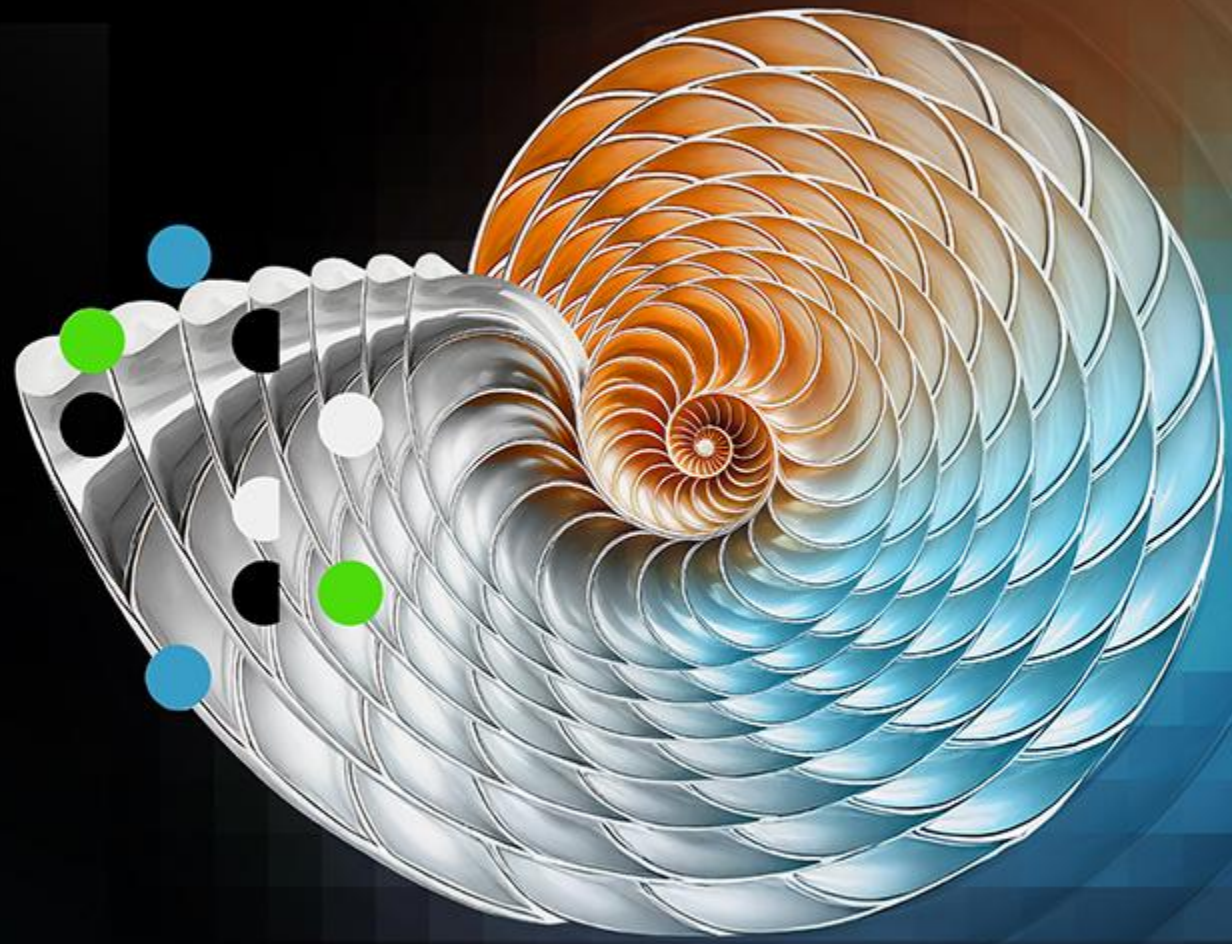
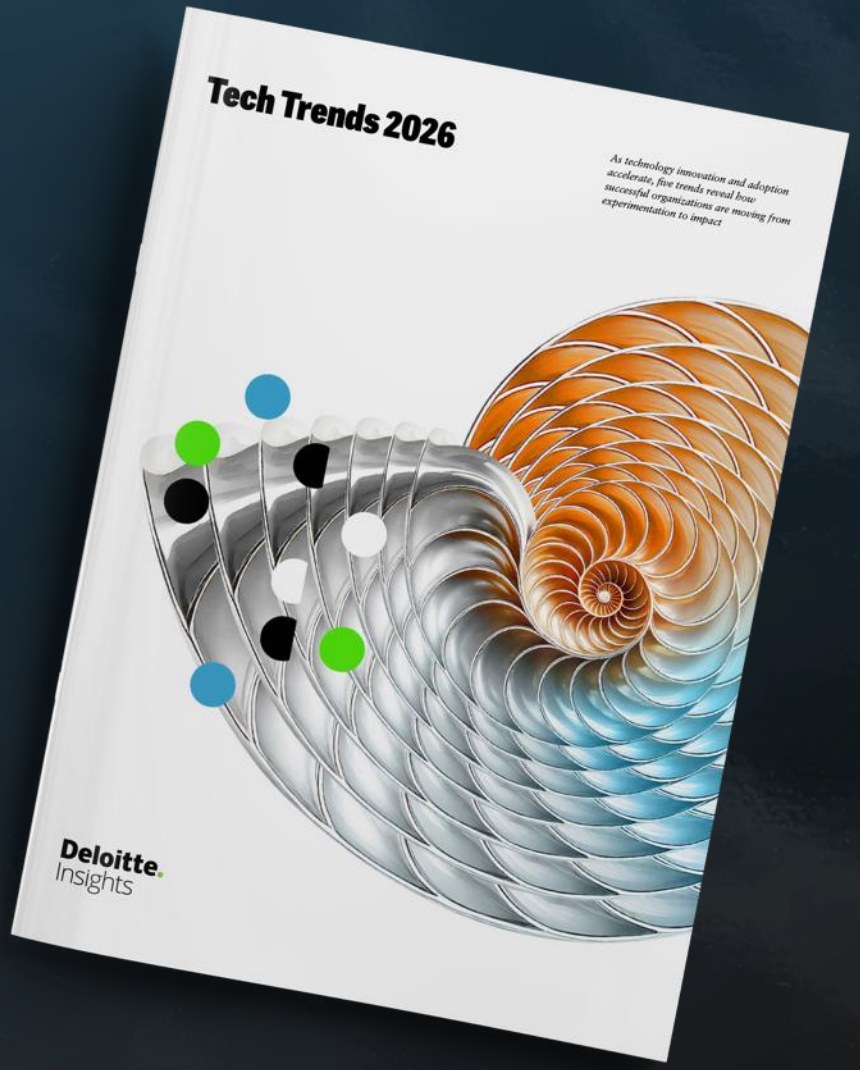
Deloitte.
デロイト トーマツ
Together makes progress

Tech Trends 2026



日本版 Perspective（抜粋版）



Deloitte's 17th annual
Tech Trends report

Tech Trendsは、今後1年半から2年の間に顕著になると予測されるテーマを取り上げ、技術傾向や流行に加えてビジネスへの影響を解説しています

テクノロジーの最前線にいる先進的な組織（Trend Linesより）、クライアントの経営幹部、学術界・産業界の第一人者、主要なスタートアップ、ベンチャーキャピタル、テクノロジーベンダーなどから得た**示唆に富んだ情報を結集**

グローバル・日本それぞれの視点を含む下記で構成

- グローバルトレンドを解説した**本編**
- 日本のコンサルタントの見解を収載した**日本版Perspective**

Free for download at
日本版：https://www.deloitte.com/jp/ja/Industries/technology/about/tech-trends.html
グローバル版：https://www.deloitte.com/us/en/insights/topics/technology-management/tech-trends.html

Tech Trendsが定義する5つのマクロフォースのフレームワークに沿って、大きく2つの方向性でトレンドをピックアップしている

Tech Trendsが定義するマクロフォースのフレームワーク

発展する力：
進化するテクノロジーを活用し
成長につなげていく

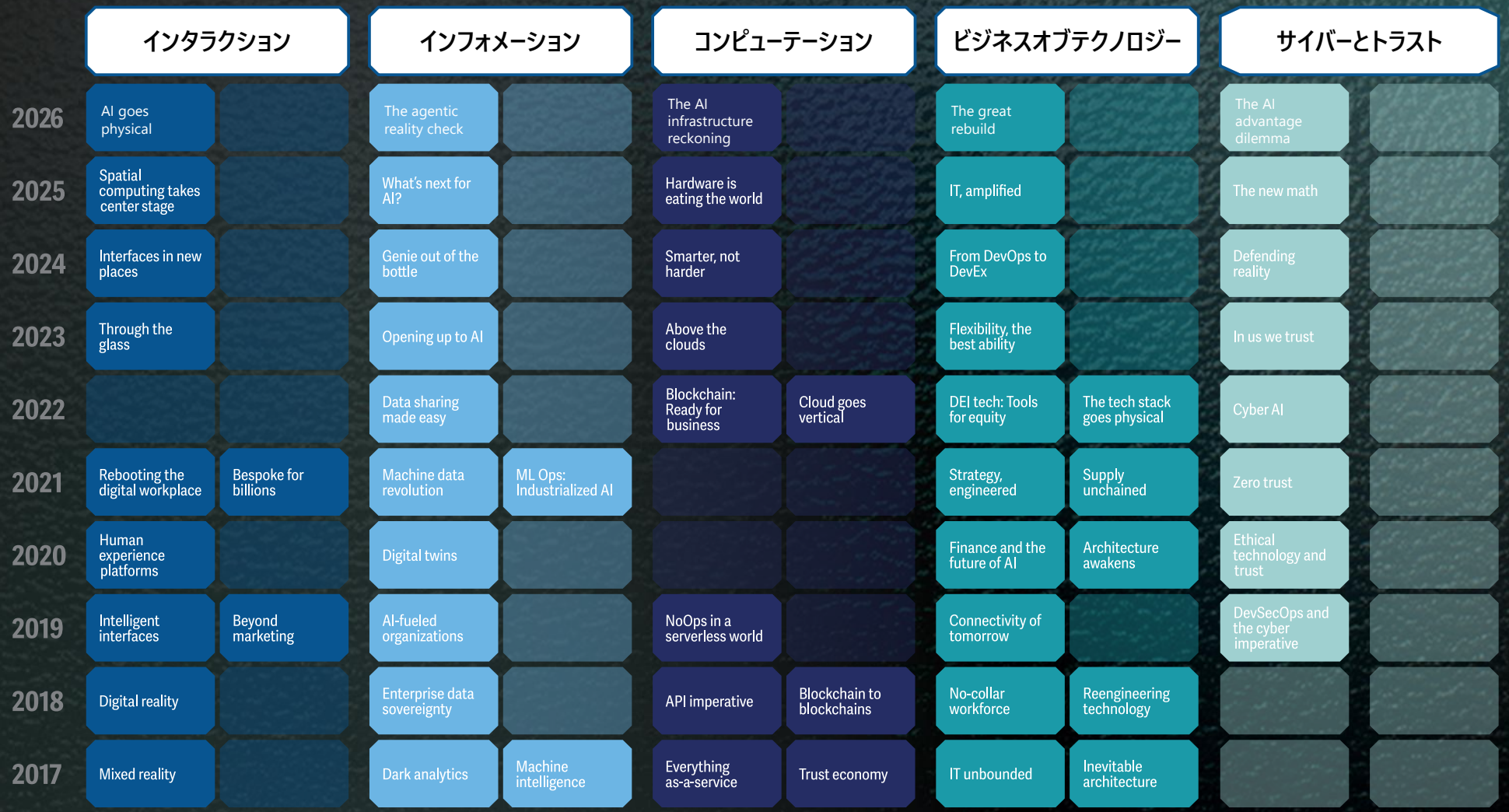
ELEVATING FORCES

GROUNDING FORCES

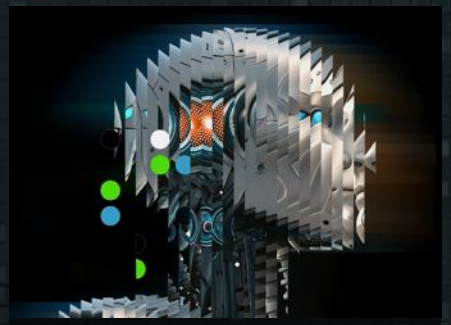
基礎となる力：
地に足を着け、既存の仕組みを
適切に管理していく

Tech Trendsは10年以上にわたり、各領域のトレンドを経年で考察している

Trending the trends: 過去10年間のトレンド



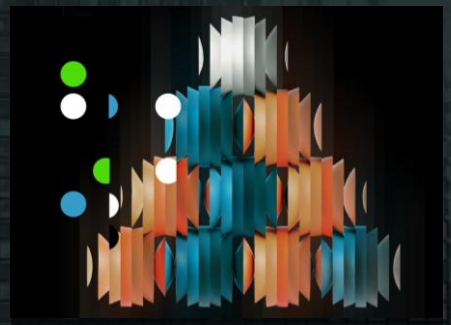
Tech Trends 2026



AIは物理世界へ

AIとロボティクスの融合がもたらす新たな可能性

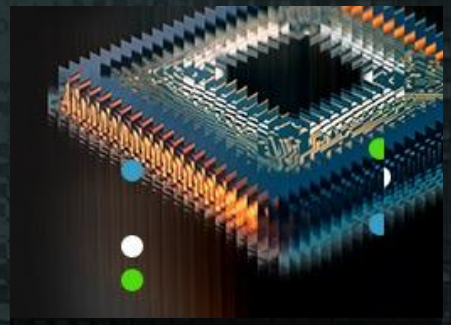
AIを搭載したロボットはスマート製造や物流の分野で急速に拡大しており、中期的にはニッチな存在から主流の採用へと移行する見込みだ。次のフロンティアは、人型（ヒューマノイド）の形態となる。



エージェント化のリアリティチェック

シリコンベースの労働力に備える

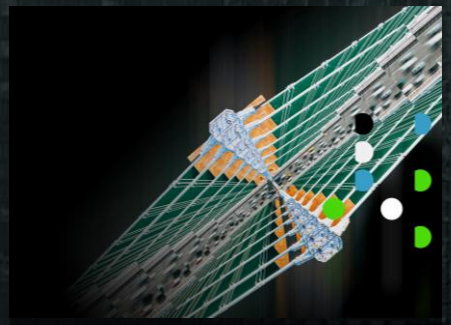
企業は、過剰な期待を超えて、エージェントファーストのアーキテクチャ構築へと移行している。成功を収める組織は、オーケストレーションのフレームワークを使いこなし、自律的なAIの能力を最大限に引き出すためにプロセスを再構築するだろう。



AIインフラの転換点

推論エコノミクス時代におけるコンピューティング戦略の最適化

既存のインフラ戦略は、AIの要求と整合していない可能性がある。企業は、各ワークロードに応じて最適なコンピューティングプラットフォームを活用するハイブリッドなAIインフラのエコシステムを設計・構築している。



テクノロジー組織の再構築

AIネイティブなテクノロジー組織の設計

AIは、テクノロジー組織の構造、ガバナンス、そしてリーダーシップのあり方を再設計している。未来への道筋に唯一の青写真はないものの、組織はAIが駆動する未来に備え、積極的に行動を起こしている。

AIのジレンマ

サイバー防御のためのAIの確保と活用

AIは企業のサイバーセキュリティを再構築し、利点とリスクの両方を生み出している。組織は、差し迫ったリスクに対処するとともに、将来の情勢を左右する脅威に備えて高度な防御戦略を展開する必要がある。

AIは物理世界へ

AIとロボティクスの融合がもたらす

新たな可能性

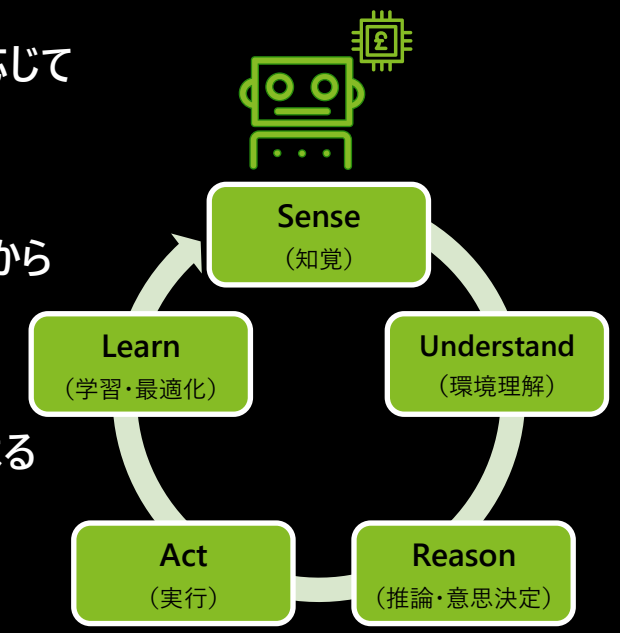
AIによりロボットは「決められた動き」から「知覚・推論・行動・学習による適応」へ進化し、工場を超えて手術支援や都市走行、倉庫など多様な現場で実運用が広がっている

フィジカルAIにおけるトレンドサマリー

技術エネイブラー

機械学習・強化学習 / GPU / 大規模データ / センサー進化など

	従来（従来ロボティクス）	現在（フィジカルAI）
制御・行動	ルールベース制御による事前定義された動作	AIによる自律制御、環境に応じて動作を生成
学習	手動チューニング・オフライン調整	機械学習・強化学習データから行動を学習
計算処理	組込みCPU中心の限定的処理能力	GPU・クラウド・エッジAIによるリアルタイム推論
適用範囲	工場ラインなどの固定環境	倉庫・配送・家庭・医療などへの適用



反復性が高く、危険性や精密性が求められる領域ほどROIが成立しやすく、海外ではすでに多数の導入事例が蓄積されている

海外事例

企業	領域	事例	インパクト・ユーザー価値
Amazon	 物流・倉庫	**100万台のロボットを** 搬送システムの一部として導入	✓ 入出庫・仕分け・搬送の**タクトタイム短縮、ピーク耐性力を強化** ✓ 重作業に伴う**人的負担の軽減**、および**ヒューマンエラーの低減**
BMW	 製造	**工程間搬送を無人化** 組立後は自律走行で次工程へ	✓ 搬送待ちを削減し、**タクトタイム短縮・スループット向上** ✓ 人とロボットの動線分離、搬送の一貫性で**ばらつき低減**
Waymo	 モビリティ・公共	**1,000万回以上** 自動運転による無人タクシーサービスを提供	✓ ドライバー不足の補完による**モビリティ供給力の確保・拡張** ✓ ドライバー都合による**サービス品質のばらつき低下**

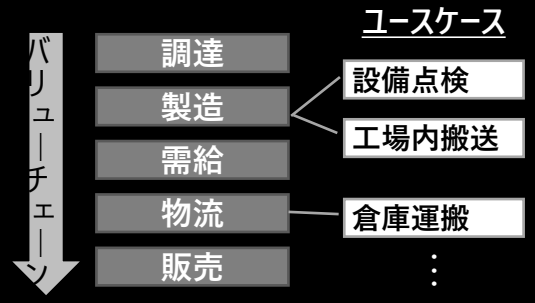
出典：Deloitte Insight, " Physical AI and humanoid robots | Deloitte Insights", （参照2026年3月）

「安全」を起点にSmall Startで本番運用を開始し、業務の再設計と並行して運用・モデルを改善しながら、再現性・安全性の高い領域から段階的に展開していく

日本のフィジカルAI活用に向けたアプローチ

ユースケース選定

- ✓ バリューチェーン全体のユースケースを洗い出し、再現性・安全性・業務特性・ROIなどの観点から優先順位を付けて選定する
- ✓ 安全性を重視し、初期段階での事故やトラブルを未然に防ぐことで社会的信頼の向上に繋げる
- ✓ 屋内でレイアウトが安定し、人的交錯リスクが低い反復作業領域を優先的に選び、横展開しやすいユースケースからSmall Startで運用を開始する

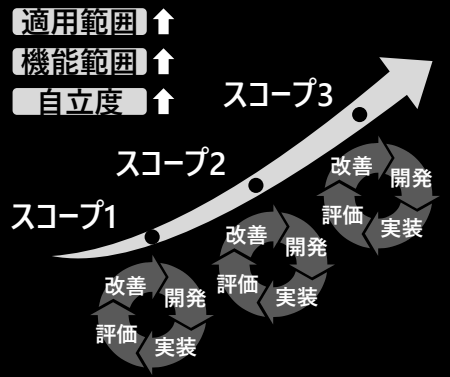


実装準備

- ✓ 最終的なフィジカルAIの活用イメージから、最小実装範囲と実装後の効果の検証方法を明確にする
- ✓ 業務設計・技術開発・組織体制・制度整備を同時並行で進める

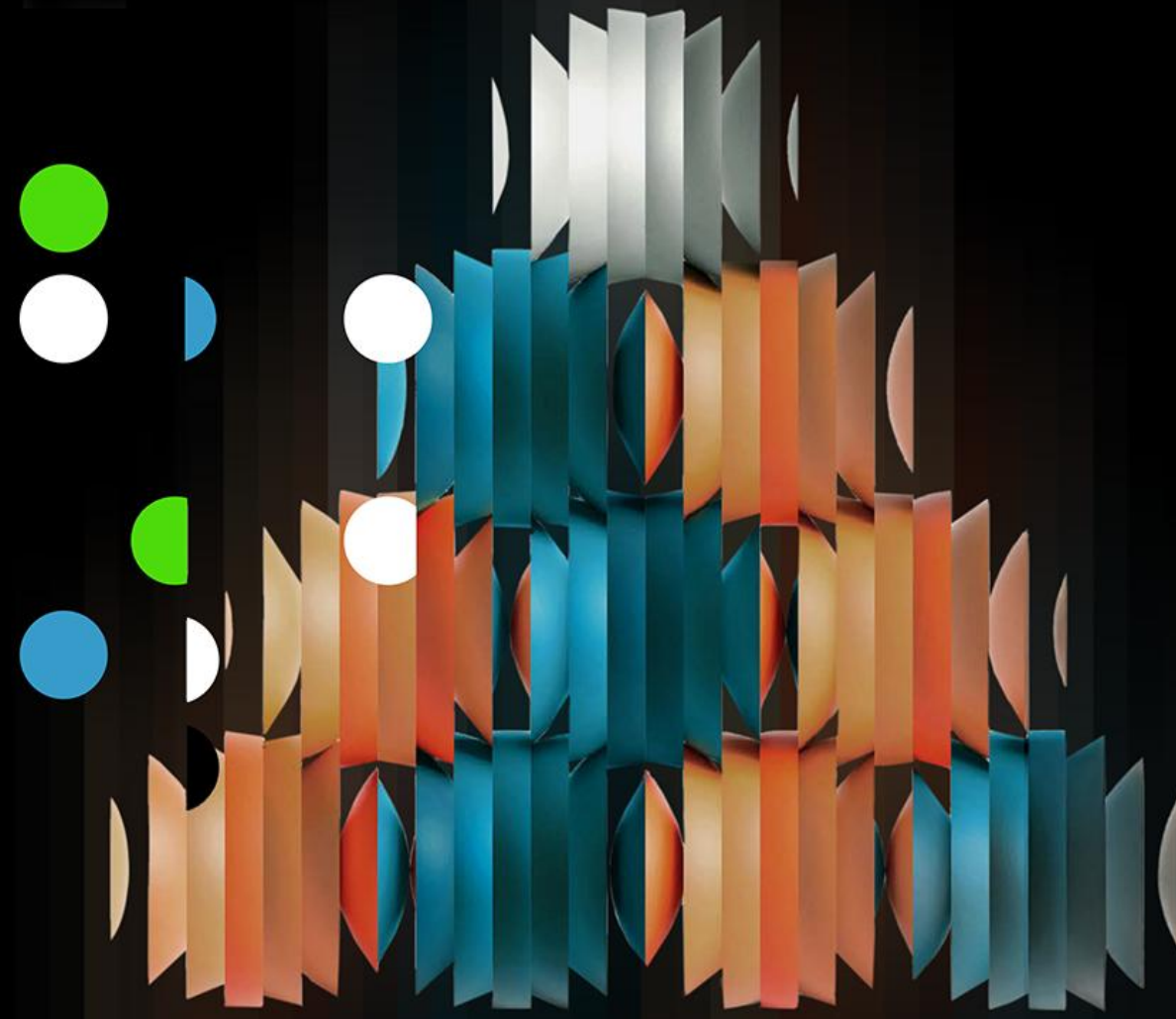
技術実装

- ✓ 限定スコープで本番に近い運用を開始する
- ✓ 取得データや現場知見からの検証、評価・改善を短サイクルで繰り返し、データの学習・モデルの改善を実施する
- ✓ 適用範囲・機能・自立度を段階的に拡大させる



エージェント化のリアリティチェック

シリコンベースの労働力に備える



多くの企業でAgentic AI導入が進まない背景には、レガシーシステム・データ構造・AIガバナンスの構造的制約が存在する

Agentic AIの現実とギャップ

予測されるAgentic AIの導入率 (2028年まで)

15%

日常業務における意思決定を自律化

2024年の0%からの増加予測

33%

エンタープライズアプリケーションに搭載

2024年の1%未満からの増加予想

導入を阻む3つの根本的障壁

レガシーシステム統合の欠如	従来システムはAgenticインタラクション向けに設計されていない。 欠如要素：リアルタイム実行能力、モダンAPI、モジュラーアーキテクチャー
データアーキテクチャーの制約	ETLプロセス中心の構造がAgent展開の摩擦を生む。コンテキスト理解に必要なデータ構造になっていない。 課題：データの検索性、再利用性が低い
ガバナンスとコントロールの未確立	自律的に意思決定し行動するシステムに対する監視メカニズムが不足。 リスク：予測不能な挙動、責任分界点の曖昧さ

単にエージェントを導入するのではなく、エージェントが活躍できる「土壌（プロセス・データ・基盤）」を作り直すことが先決

出典：Gartner® プレスリリース（2025年6月25日）"Gartner Predicts Over 40% of Agentic AI Projects Will Be Canceled by End of 2027"

先進企業は、AIエージェントを定型業務の自動化と人との役割分担を前提に業務や組織を再設計し、効率化と変革を実現している

先行企業の取り組み

事例	マフレ：スペインの大手保険会社	モデルナ：アメリカのバイオテクノロジー企業	HPE：アメリカのIT企業
プロダクト	保険請求処理を自動化する 保険業務AIエージェント	人間とAIを統合した AI Workforceモデル	財務分析を自動化する マルチエージェント分析システム
背景・目的	■ 保険金請求や損害査定などの管理業務は定型処理が多く、業務負荷が高い ■ 一方で顧客対応など判断を伴う業務は自動化が難しく、効率化に限界があった ■ 人とAIが協働する形で業務効率を向上させる新しい業務モデルの構築が求められていた	■ AI導入を進める中で、人材計画と技術計画が分断されていた ■ AIエージェントを単なるツールではなく労働力として活用するため、組織設計の見直しが必要となった	■ 業績レビューなどの財務分析業務は大量のデータ処理が必要 ■ データ分析・レポート作成に多くの時間がかかっていた
ソリューション概要	■ 保険金請求管理プロセスにAIエージェントを導入 ■ 損害査定などの定型業務をエージェントが処理 ■ 顧客対応など判断を伴う業務はHuman-in-the-loopで人間が対応	■ 最高人事・デジタル技術責任者を設置し、人事部門とIT部門を統合 ■ 人間とAIを同じ労働力として設計する運用モデルを構築 ■ 業務計画を「人かAIか」ではなくプロセス単位で設計	■ 業績レビュー支援AIエージェント「AIfred」を開発 ■ クエリ分解／データ分析／可視化／レポート生成を行う複数エージェントを構成 ■ ERP・CRMのデータウェアハウスから情報を取得
導入効果	■ 定型業務の自動化による業務効率化 ■ 人間は顧客対応など付加価値の高い業務に集中 ■ 人間とAIのハイブリッド運用モデルを確立 人間とAIのハイブリッド運用	■ AIエージェントを前提とした新しい業務モデルを確立 ■ 人材戦略とAI活用を統合した組織運営を実現 人とエージェントを 対等な労働力として設計	■ 財務分析プロセスの自動化 ■ レポート作成の効率化 ■ end-to-endでの業務プロセス変革を実現 単一課題ではなく end-to-endで変革を実施

経営設計は、AIエージェント導入によるROIは短期的な定量効果だけでは測れないため、業務品質向上やリスク低減なども含め、将来価値まで踏まえたROI改善の仕組みが必要である

Agentic AI時代の経営変革

AS-IS（現状）

部分的なAIエージェント導入
42％の組織がエージェント戦略のロードマップを策定中、35％は正式な戦略を持っていない。より単純なツールで十分な場面でもエージェントを適用し、結果としてROIが低くなる

TO-BE（あるべき姿）

現実的なROI/KPI設計へ
初期段階で財務部門と事業責任者が署名した現実的なROIが必要。導入可否はROIを起点に判断し、業務効果を継続的に測定・管理する

AIエージェント導入におけるマネジメント設計

	AI投資の判断プロセス	KPI設計
定量的効果 (Hard ROI)	**直接財務効果** 工数削減・外注費削減・売上増加を金額換算し、投資回収期間で資本効率を判断する	✓ コスト削減総額 ✓ 売上貢献額 ✓ 投資回収期間
定性的効果 (Soft ROI)	**リスク調整効果** エラーやコンプライアンス逸脱を抑制し、将来の損失や法的リスクを未然に防ぐ価値を評価する	✓ エラー削減率 ✓ ガイドライン準拠性スコア ✓ ハルシネーション発生率
戦略的価値 (Strategic Value)	**将来価値創出** データ資産化と再利用を通じて組織能力を高め、持続的な競争優位と新規事業機会を創出する	✓ データ資産蓄積量 ✓ モデル再利用率 ✓ 新領域への適用可能性

段階的な実現ステップ

① 3つの効果指標について経営と合意

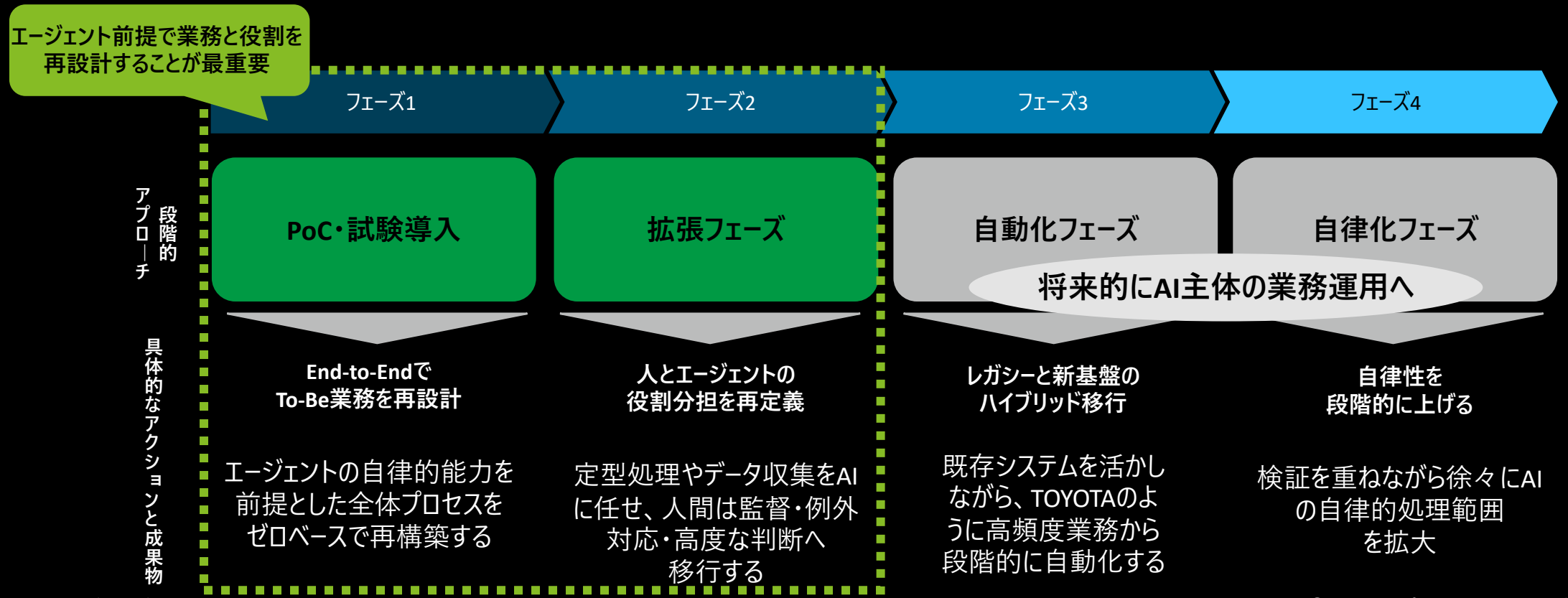
② KPIモニタリングとリソースアロケーション実行

③ 定期レビューに基づく投資判断とリソース集中

Agentic AI導入では、現在の業務をそのままAI化するのではなく、業務プロセス全体を再設計したうえで段階的に移行することで、エージェント主体の業務運用を実現する

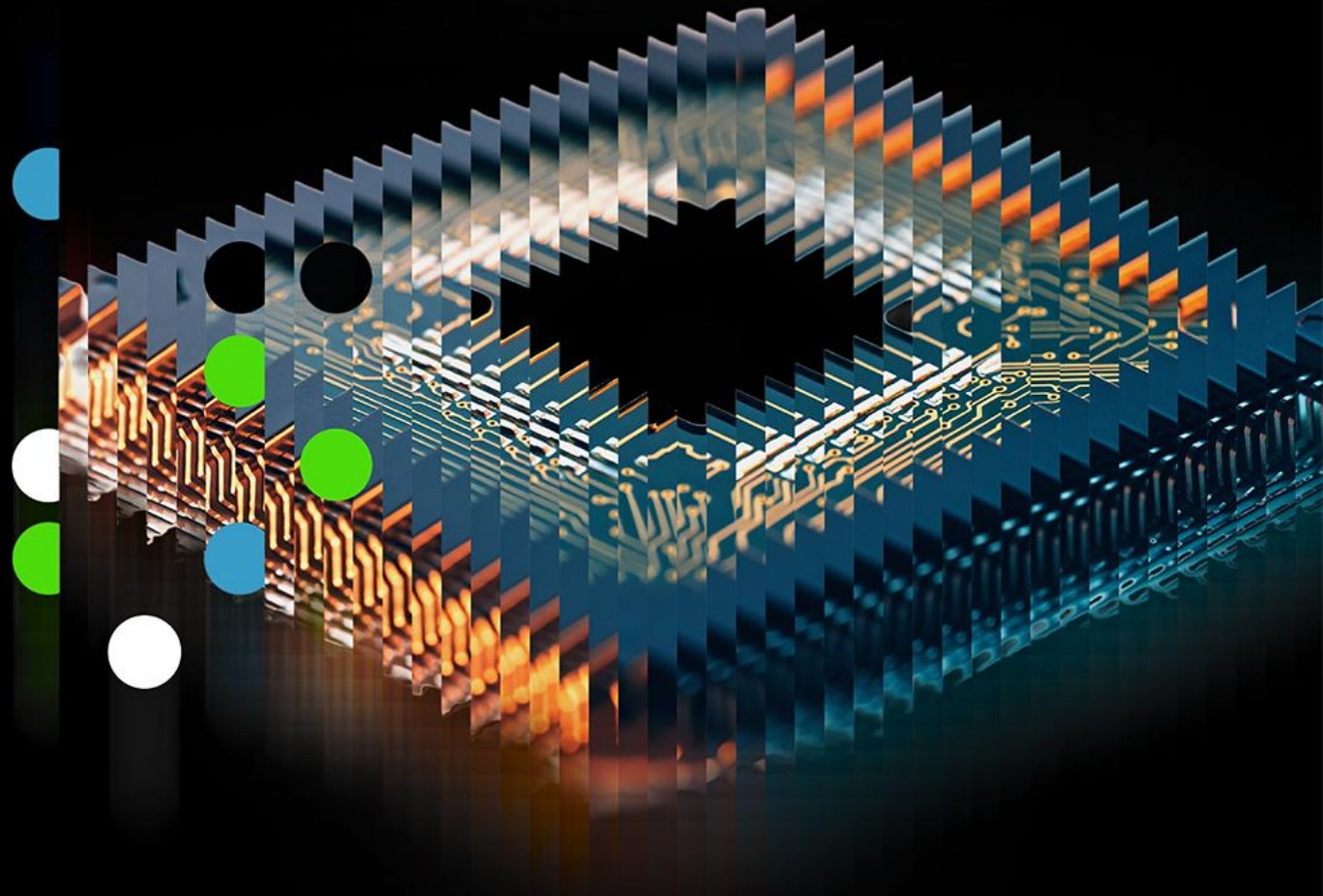
現状把握とあるべき姿を策定し、移行戦略を設計する

■ エージェントを前提に業務・組織・基盤を再設計し、Human in the LoopとROI/KPIで段階的に実装・運用することが肝要である
■ 導入停滞の原因はレガシー統合、データ構造、ガバナンスの欠如にあり、「プロセス・データ・基盤」という土壌の作り直しが出発点となる
■ 成功事例が示す通り、エンドツーエンドの再構築と人×AIの役割分担・ガバナンス整備により、効率化と変革を同時達成できる



AIインフラの転換点

推論エコノミクス時代における
コンピューティング戦略の最適化



グローバルでは、AI活用が本番段階へ進むなかで推論処理は持続的な需要へと変化し、コンピュート資源をどこでどのように確保するかが企業競争力を左右する経営課題になりつつある

グローバル版Tech Trends 2026が示したAIインフラの転換点

AI活用の本番展開

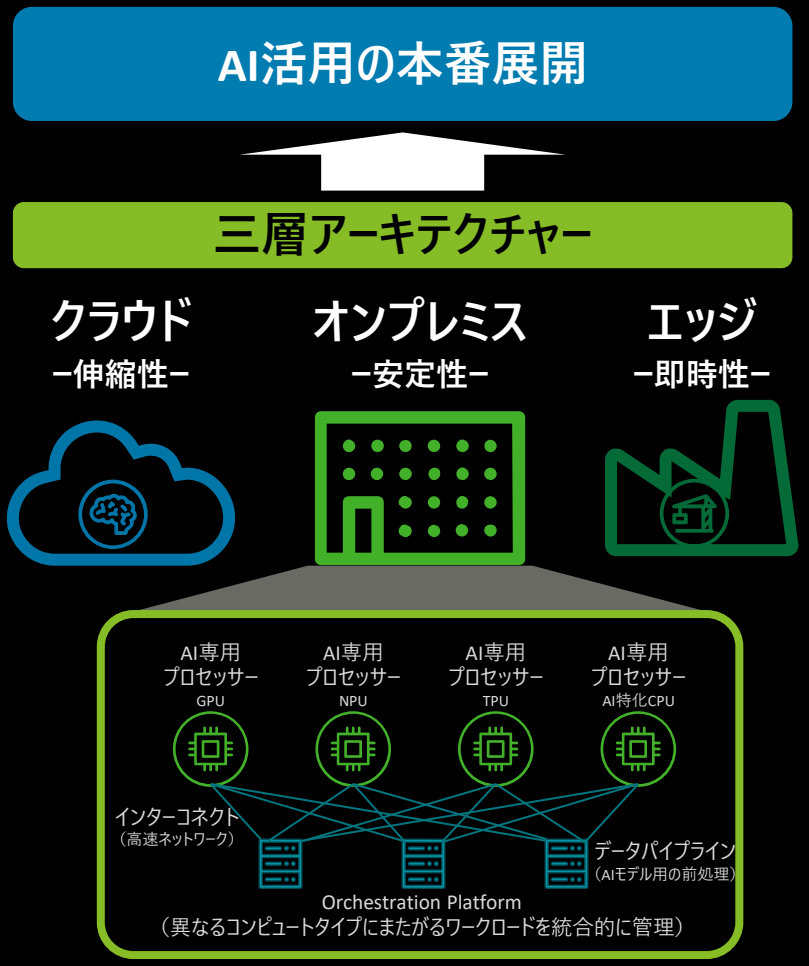
- AI活用はPoC中心の段階から本番展開へ移行
- 推論は断続的な処理ではなく、業務に組込まれた持続的な需要へ変化
- 推論コストそのものは低減しているが、利用量の急増によりAIコストは拡大

➡コンピュート資源をどこでどのように確保するかは、IT運用上の論点ではなく経営資源配分と直結する課題になっている

グローバルの最先端トレンド

- クラウド・オンプレミス・エッジを組み合わせる三層アーキテクチャー

➡クラウドからオンプレミスへの単純な回帰ではなく、ワークロード特性に応じてAIに最適なプロセッサーを組み合わせる



AIインフラは裏方の技術基盤ではなく、
もはや競争力を左右する経営アジェンダ

推論エコノミクスや三層アーキテクチャーは、AIを業務の中核に組み込み、クラウドを全社基盤としている企業のアジェンダである一方、多くの日本企業はその段階に到達していない

AIインフラ戦略をめぐる前提条件の差異

AI活用の条件

- 弾力的なコンピュート確保、データ基盤との統合、迅速な実験と展開を可能にするアーキテクチャー設計が不可欠

グローバルの最先端組織

- AIがすでに業務の中核に組み込まれ、推論が継続的かつ大量に発生
- クラウドが単なる選択肢ではなく、全社基盤として一定の統合度と成熟度を備えている

➡推論エコノミクスや三層アーキテクチャーがアジェンダとなる

日本企業の状況

- 多くは、既存システムのリプレースや部門最適を目的としたクラウド導入
- 業務構造やガバナンスの設計思想は従来の延長線上に残り、AIを前提としたコンピュートポートフォリオを戦略的に設計する段階に至らない

➡ AI活用は局所的な取り組みにとどまり、グローバル版が前提とする議論にはつながらない

現行プロセス改善や現行システム更改を優先するのではなく、AIを業務プロセスに組み込み、システム構造とケイパビリティー変革を同時に進めることが、企業競争力の拡大につながる

AI前提の企業へ転換する三つの変革

業務プロセス変革

AIを付加機能ではなく業務プロセス変革の前提として位置づける。
AIを既存業務に後付けする発想のままでは、PoCや個別業務の効率化にとどまり、持続的なワークロードにはつながらない。どの意思決定をAIが担い、どの業務を再定義するのかを明確にし、AIを業務アーキテクチャーの構成要素として扱う視点が求められる。

システム構造変革

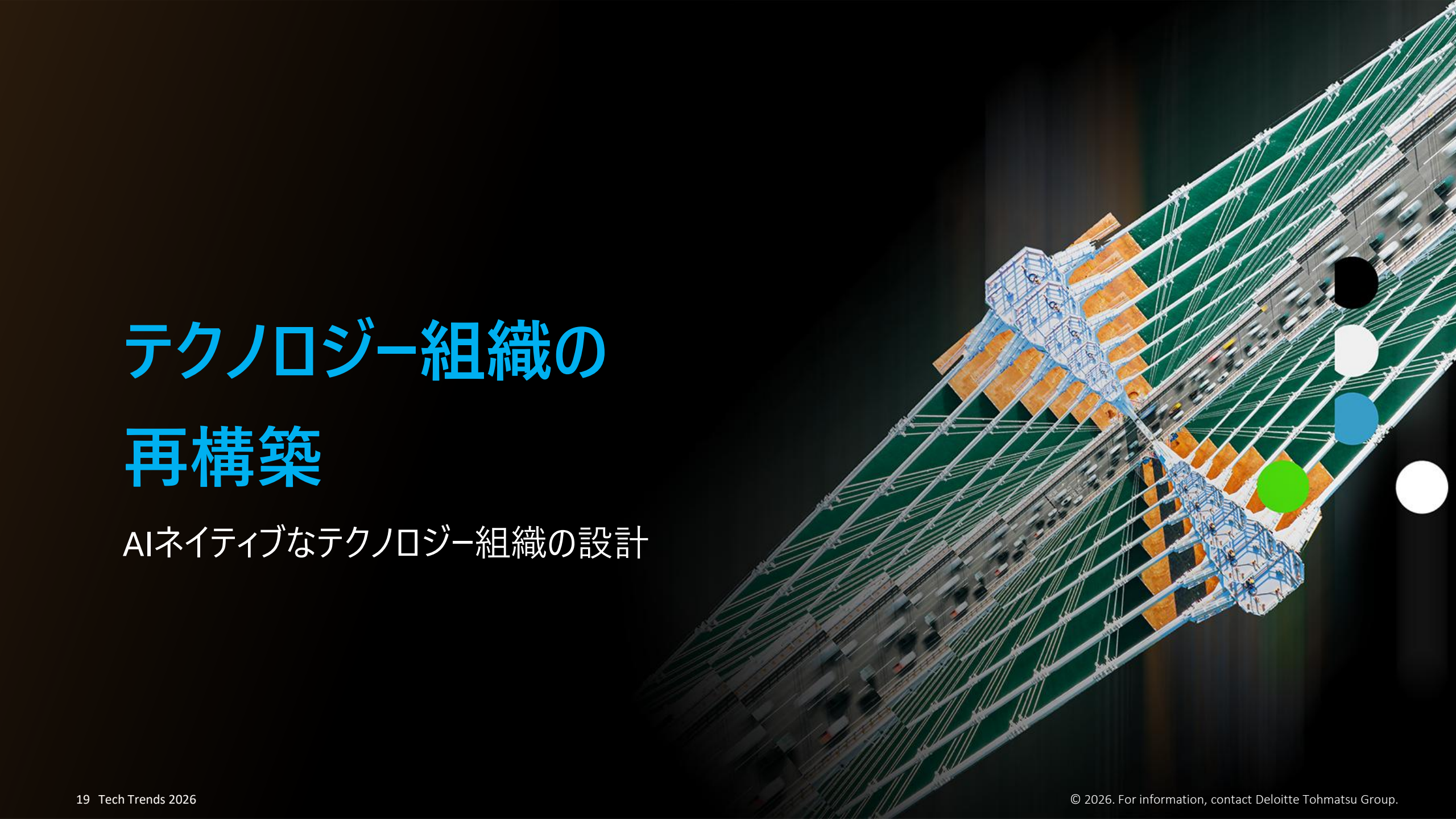
既存資産を抱えたままシステム構造変革を進める。
既存システムを整理してからAIに取り組むという段階論では、変革は常に後回しになる。全社アーキテクチャーの将来像を描き、優先度の高い領域から段階的に再設計しながら、新しい基盤とAI活用の範囲を広げていく必要がある。

ケイパビリティー変革

クラウドとAIを前提に業務やシステムを設計できる組織能力を高める。
求められるのは技術スキルの拡充だけではなく、意思決定プロセス、ガバナンス、評価制度、組織文化まで含めたケイパビリティー変革である。

テクノロジー組織の再構築

AIネイティブなテクノロジー組織の設計



テクノロジー組織は、AI導入収益成長を牽引する戦略的リーダーへ転換し、ビジネスモデル変革と学習文化を加速させる

グローバル版で紹介されたトレンドのサマリー（テクノロジー組織の役割変化）

テクノロジー組織は”サービスセンター”から、ビジネス成長を実現する”戦略的リーダー”に変化

66%

テクノロジー組織を**サービスセンターではなく収益創出源**と見なしている企業

出所：Deloitte‘s Tech Exec Survey 2025

71%

AI導入をサポートするためにコアインフラをモダナイズしている組織

出所：Tech Spending Outlook 2025

70%

生成AIの専門チームを増強する計画を立てている企業

出所：Deloitte‘s Tech Exec Survey 2025

「人間×AIエージェント」の新しい働き方の先駆者となる

- 人間とAIエージェントが効率良く協働するための、橋渡し役（オーケストレーター）としてのケイパビリティーをいち早く獲得する
- AI/ロボティクスにより、プロダクトロードマップの達成を加速し、フィードバックループを自動化し、リアルタイムでタスクの優先順位を見直す
- 社外パートナーを含むオーケストレーションで戦線を広げ、「早く失敗し、より早く学ぶ」文化を定着させる

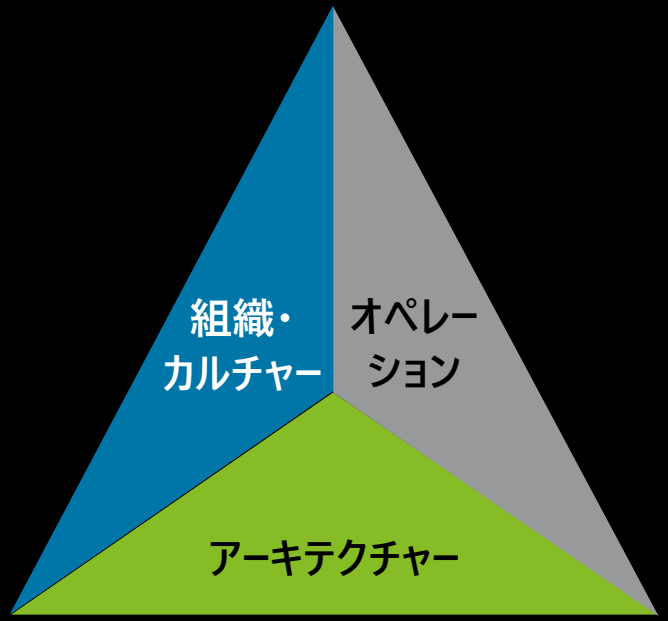
ビジネス成長に求められる新たなロールを提供する

- AIがコード生成等のエンジニアリングを担うことで、テクノロジー組織に属する人間の役割は上位レイヤーに変化し、テクノロジー活用によるビジョン策定・トップライン成長・ビジネスモデルの転換を担う
- AIOpsリードやプロンプトエンジニア等の新しい役割を提供する

AI主導の世界で成功しているテクノロジー組織では、AI活用を前提としたアーキテクチャー・オペレーション・組織／カルチャーに変革し、テクノロジーの変化とともに進化し続けている

AI Transformationに成功している米国企業の共通項

- **柔軟に変化・進化し続ける組織とカルチャーの醸成**
  AI変革を中核ケイパビリティーとして組織構造・文化に組み込み、技術進化に同調して学習し続ける柔軟な組織への転換
- **継続的なイノベーションを実現するエコシステムを構築**
  スタートアップ、ハイパースケーラー、規制当局、学界との連携による流動的ネットワークを基盤とした「早く失敗し、より速く学ぶ」文化の醸成



- **スピード重視のオペレーティングモデルとプロダクト型チームの構築**
  プロジェクト型からプロダクト型の横断チームへの移行による、連続的な計画・開発・改善と価値創出までのリードタイム短縮
- **人x AIエージェントの協働**
  人は創造性・監督・倫理判断、AIはスピード・精度・パターン認識を担う協働体制による、継続的実験とスケーラブルなイノベーションの推進

- **クラウドネイティブなプラットフォームと、柔軟性・可視性を重視したアーキテクチャーへの移行**
  AIをアドオンではなく、意思決定・オペレーション・プロダクト開発など、全ての領域に組み込む前提で、インフラを再構築
  システム全体管理自動化のために、オブザーバビリティアーキテクチャー（各種メトリクス、ログ、トレース、イベント等収集と可視化の仕組み）を構築

トップダウンでのAI Transformationを後押しするために、テクノロジー組織は、レガシー業務・システムのモダナイズに着手し、スピードや柔軟性といったケイパビリティを獲得する必要がある

日本のテクノロジー組織の障壁と打ち手

AI Transformationに向けた日本企業の障壁

- **「守り」に重きを置いたレガシーの業務・システム**
  稟議制・階層型の意思決定プロセスや属人的な業務が残り、デリバリースピードが出ない
  オンプレ含む複雑なレガシーアーキテクチャーが残存、データも散在しており、AIによる開発・データ活用の足枷となる
- **ITの投資・施策目的がコスト削減に偏重**
  グローバルと比べCIO/IT部門に対する期待・権限が限定的
  目先の外注費削減施策から着手するケースも多く、イノベーションや多様なサービス・サプライヤーのコラボレーションを実現するための戦略や仕組みの整備が遅れている
- **専門人材の不足**
  ジェネラリスト型のキャリア形成や終身雇用が主流であり、専門人材向けの人事制度変革が遅れ、テクノロジーの変化ペースに合わせた柔軟な採用・育成戦略の見直しも課題となっている

必要となる打ち手の方向性

CxOレイヤー
- CIOのケイパビリティーの拡大／細分化とテックリード間での役割分担
- CIO(CAIO)・CFO・CSOのワンチームの組成、AI×事業戦略の策定

デリバリーモデルとアーキテクチャー
- AIと人間のワンチームを前提とした組織/機能横断のプロダクトチーム組成
- クラウドネイティブ・モジュール型のアーキテクチャーへの移行
  AIによる活用を前提としたデータアーキテクチャーの設計

ソーシング戦略・サプライヤー管理
- AI／ビジネス戦略に適合した全社的なソーシング／パートナー戦略の策定
- AI特有のリスクを考慮した契約・サプライヤー管理の構築

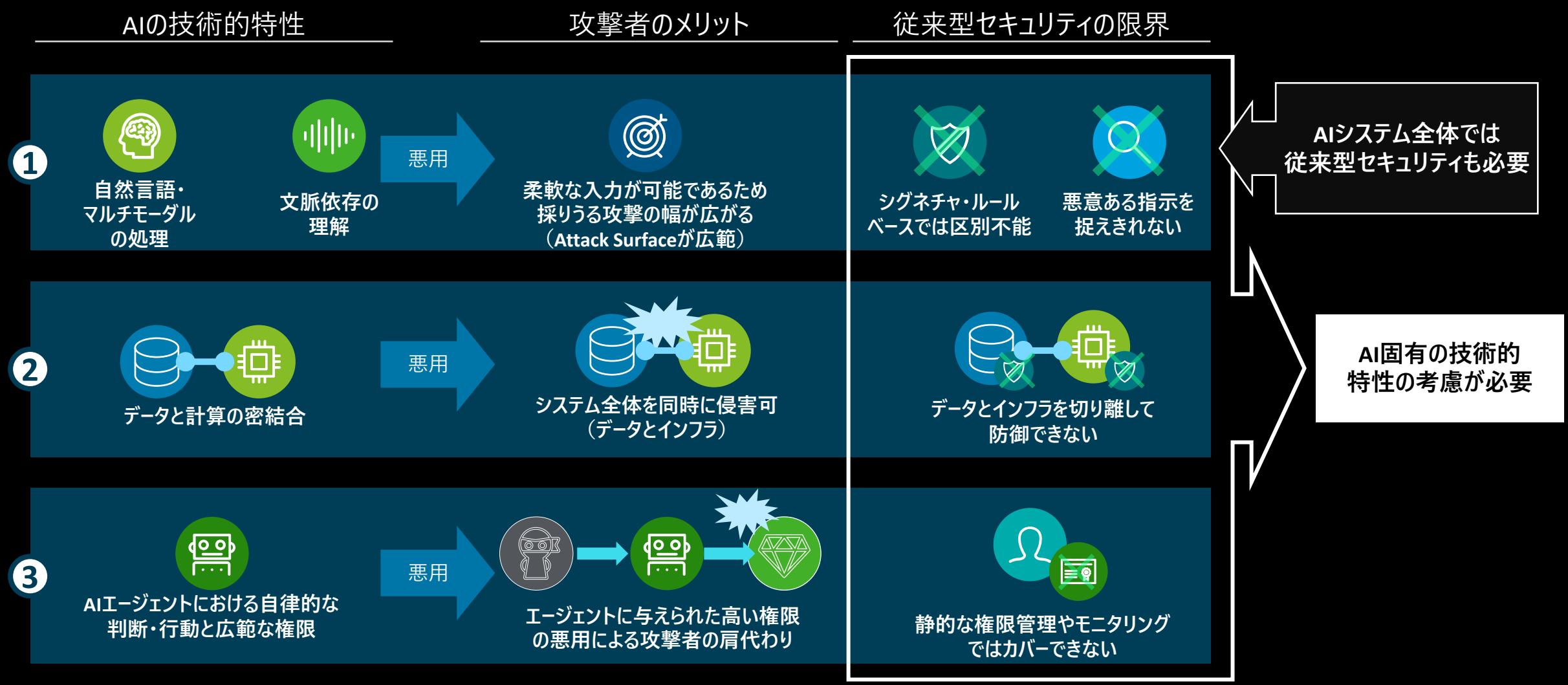
タレントマネジメント
- 社内ナレッジマネジメント高度化、AI基礎教育の提供
- 専門人材の確保・定着に向けた、評価制度・キャリアパスの整備

AIのジレンマ

サイバー防御のためのAIの
確保と活用

AIセキュリティにおいては、従来型セキュリティのコントロールを適用するとともに、AI固有の技術的特性を踏まえた適応や更新が必要

AIの技術的特性を踏まえ従来型セキュリティを包含した対応が必要



AIセキュリティをコストではなくイネーブラーとして扱い、多層防御を構築する

AIセキュリティについて組織が取るべきアクション

01
管理・統制

GRC（ガバナンス・リスク・コンプライアンス）の強化
- ✓ AIデプロイメントに係るリスクコントロールを実現するための継続的な監督・評価体制の整備
- ✓ 国境を越えたAI実装に係る規制遵守
- ✓ シャドーAIを発見するためのネットワーク監視

02
計画・設計

AIブループリントと設計段階からのセキュリティ
- ✓ 人材・運用・ガバナンス・技術アーキテクチャーを一体として再設計する「AIブループリント」の策定
- ✓ AIエージェントの活用を見据えた設計段階からのセキュリティの組み込み（Security By Design）

03
開発・運用

AI開発・運用セキュリティ
- ✓ 強固な開発プロセス（SDLC）の遵守
- ✓ 敵対的トレーニングによるデータポイズニング等への攻撃耐性・ロバスト性の向上
- ✓ AIレッドチーミング（疑似攻撃）の実施による、AIシステムの脆弱性・弱点の特定

04
高度化

エージェントセキュリティ
- ✓ エージェントの意思決定パターンやエージェント間通信のリアルタイム監視・分析による、異常行動の自動検出
- ✓ エージェントの作成・変更・無効化・継承を制御するライフサイクル管理ポリシーの策定（孤立エージェント発生・残置の阻止）

05
高信頼化

フィジカルAIセキュリティ
- ✓ 重要な物理システムにおいて、人間のオペレーターが自動化された意思決定を上書きできる手動バックアップ制御の整備
- ✓ 接続されたシステム全体に問題が広がることを防ぐ分離境界（カスケード防止アーキテクチャー）の実装

06
効率化

セキュリティ機能へのAI活用（AI for Security）
- ✓ サイバー攻撃へのマシンスピードでの対応・防御
- ✓ AIによる業務効率化（リスクスコアリング・TPRM・ポリシーのレビュー・成熟度評価・コンプライアンス対応等）
- ✓ AIエージェントの活用による自律型の脆弱性診断や敵対的トレーニングの実行

「AIシステムの4レイヤー」×「実用化への3局面」ごとにセキュリティ課題・リスクが存在し、それぞれの領域で対応が求められる

AIセキュリティの課題・リスク領域

	設計・開発／学習フェーズ	展開フェーズ	利用／運用フェーズ
アプリケーション セキュリティ	• サプライチェーン（LLM03:2025） • 不適切な出力ハンドリング（LLM05:2025） • 安全でないコーディング手法 • 設計上の欠陥	• サプライチェーン（LLM03:2025） • 過剰なエージェンシー（LLM06:2025） • システムプロンプト漏洩（LLM07:2025） • 展開環境における資格情報の不適切な使用 • ベクターデータベースへの不正アクセス	• プロンプトインジェクション（LLM01:2025） • システムプロンプト漏洩（LLM07:2025） • 無制限のリソース消費（LLM10:2025） • 不適切な権限管理 • APIの不正使用 • Webの脆弱性
モデルセキュリティ	• サプライチェーン（LLM03:2025） • モデル・データポイズニング（LLM04:2025） • 誤情報（LLM09:2025） • モデルのバックドア	• サプライチェーン（LLM03:2025） • 誤情報（LLM09:2025） • モデルパラメータの改ざん	• 誤情報（LLM09:2025） • 非準拠コンテンツ生成 • モデル機能の悪用
データセキュリティ (RAG含む)	• 機密データ漏洩（LLM02:2025） • モデル・データポイズニング（LLM04:2025）	• ベクトル・埋め込みの不備（LLM03:2025） • バックアップデータの盗難	• モデル反転 • 学習データの推論
インフラセキュリティ	• サプライチェーン（LLM03:2025） • トレーニング環境の不十分な分離	• サプライチェーン（LLM03:2025） • 安全でないシステム構成 • モデル展開サービスにおける脆弱性	• 無制限のリソース消費（LLM10:2025） • ホストの脆弱性 • コンテナからの脱出攻撃

白色太字は「OWASP Top 10 for LLM Applications 2025」に記載の項目

参考：OWASP（Open Worldwide Application Security Project）「OWASP Top 10 for LLM Applications 2025」

各章の担当者および日本版発行責任者

■AIは物理世界へ
DT LLC Supply Chain & Network Operations

高橋 直之　　戸辺 諒太
大地 宏明　　西村 咲映
川上 秀之

■エージェント化のリアリティチェック
DT LLC AI & Data

宍倉 剛　　ウェイレン 由子
河原 弘宜
米島 慎二

■AIインフラの転換点
DT LLC Technology Strategy & Transformation

南野 香澄

■テクノロジー組織の再構築
DT LLC Technology Strategy & Transformation

斉藤 宏樹　　近藤 正尭
植木 成実　　吉田 晃大
篠塚 竣　　塩見 遥

■AIのジレンマ
DT Cyber LLC Cyber Competency

大場 正士
坂井 星児

イントロダクション

DT LLC Technology Strategy & Transformation
武野 淳　　李 作鵬

日本版発行責任者 / 国内のお問い合わせ先

DT LLC Technology Strategy & Transformation
中川 貴雄 / taknakagawa@tohmatsu.co.jp

デロイト トーマツ グループの最新情報

Please follow and subscribe

Facebook

X

LinkedIn

YouTube

Instagram

各種メールマガジン

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーである合同会社デロイト トーマツ グループならびにそのグループ法人（有限責任監査法人トーマツ、合同会社デロイト トーマツ、デロイト トーマツ税理士法人およびDT弁護士法人を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従いプロフェッショナルサービスを提供しています。また、国内30都市以上に2万人超の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト、www.deloitte.com/jpをご覧ください。

Deloitte（デロイト）とは、Deloitte Touche Tohmatsu Limited（"Deloitte Global"）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して"デロイトネットワーク"）のひとつまたは複数を指します。Deloitte Globalならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。Deloitte Globalおよびその各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。Deloitte Globalはクライアントへのサービス提供を行いません。詳細はwww.deloitte.com/jp/aboutをご覧ください。
デロイト アジア パシフィック リミテッドは保証有限責任会社であり、Deloitte Globalのメンバーファームです。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、最先端のプロフェッショナルサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促進することで、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来180年の歴史を有し、150を超える国・地域にわたって活動を展開しています。"Making an impact that matters"をパーパス（存在理由）として標榜するデロイトの約46万人の人材の活動の詳細については、www.deloitte.comをご覧ください。

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

IS/BCMSそれぞれの認証範囲はこちらをご覧ください
https://www.bsigroup.com/clientDirectory

Member of
Deloitte Touche Tohmatsu Limited