第407回 NRIメディアフォーラム

エージェント型AI（Agentic AI）
～その現状と実装論点

幸田　敏宏

NRI IT Solutions America, Inc. Pacific Branch
Branch Manager

2026年3月24日

Envision the value,
Empower the change

エージェント型AIとは

背景

AIは情報の生成から、システムを自律操作して実業務を遂行する主体へと変わった

- AIの役割は、情報を読む、作る段階から、外部ツールを使って処理を進める段階へ広がっている。この進化は、AIの役割が情報処理やコンテンツ生成のツールから、**ビジネスプロセスを直接駆動する主体への変化**を意味する。
- 重要なのは、人を不要にすることではなく、業務の一部を委任可能にすることである。そのため、評価の軸も回答品質だけでなく、完遂率、例外処理、監査可能性へ広がる。

AIの役割は認識から、生成を経て、実行を伴う「主体」へ

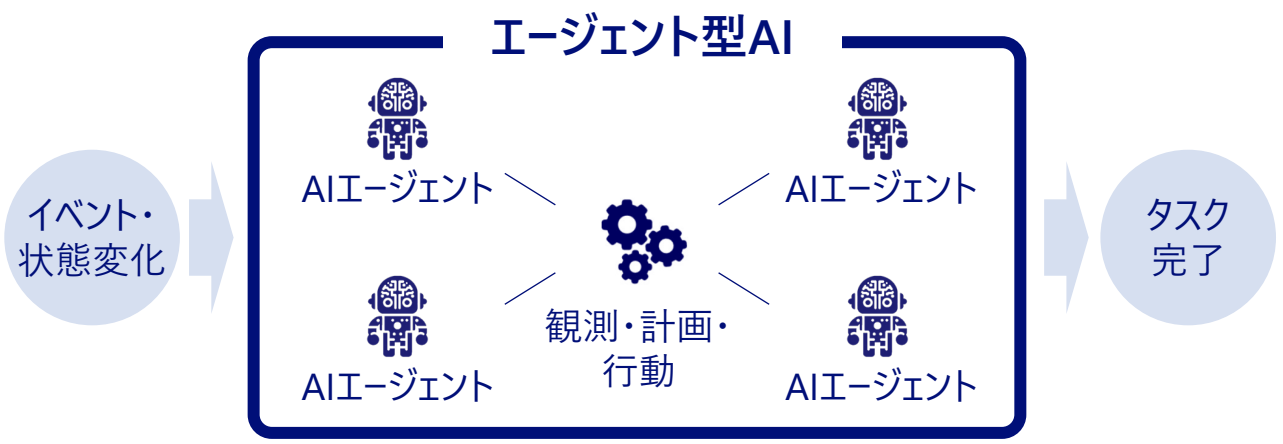
	Perception AI（認識AI）	Generative AI（生成AI）	**Agentic AI（エージェント型AI）**
主機能	画像、音声、文書などを識別、分類、抽出する	文書、コード、画像などを生成、要約、変換する	目標に沿って計画し、ツールやデータを使って業務を**実行**する
出力	ラベル、判定結果、異常検知、構造化データ	文章草案、回答、要約、コード、画像	回答に加え、**状態更新**、申請、通知、実行結果、次アクション
外部連携	限定的。判定結果を人や業務システムへ渡す	対話中心であり、必要に応じて検索や単一ツールと連携する	複数ツール、**複数システム**、場合によっては**複数エージェントと連携**
主要技術	画像認識、音声認識 (AlexNet、ResNet)	LLM、拡散モデル (GPT、Claude、Gemini)	LLM、エージェント実行基盤、運用・統制、データ/知識基盤

エージェント型AIとは

LLMを中核とし、自律的ループとガバナンスを統合した「自律型システム」である

- エージェント型AIとは、ユーザの単発プロンプトへの応答ではなく、**イベントや状態変化を起点に判断から実行まで、一貫して遂行する自律的なAIシステム**を指す。
- 目的に沿って計画を立て、必要なツール（API、業務システム、ブラウザ操作等）を呼び出して実行し、結果を評価して次の行動を選択する。人間は方針・制約・承認・例外判断を担い、AIは反復作業と実行を担う。
- AIエージェントは「役割を持つ実行主体」、エージェント型AIは「複数主体と統制を含む実行システム」である。

実行を伴う自律型システム



期待される効果

プロセス全体の滞留解消
（リードタイム短縮）

変化・例外からの自律的な回復
（回復力）

複雑な条件変化への適応
（適応性・個別最適）

処理能力の動的な拡張
（弾力性）

出所）https://www.anthropic.com/news/model-context-protocol
出所）https://developers.googleblog.com/en/a2a-a-new-era-of-agent-interoperability/
出所）https://openai.com/index/bny/

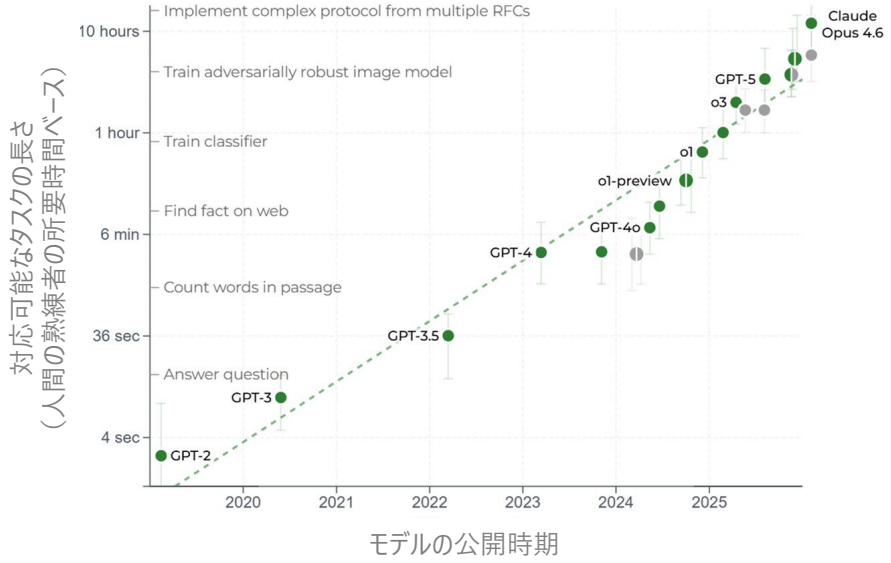
なぜ今なのか

推論力向上と「エージェント型ワークフロー」確立により、委任可能なタスクの時間が伸びている

- 米国の評価機関METRのデータは、AIが人間の介入なしに完遂できるタスクの規模が、**モデルの性能向上に伴い、指数関数的に伸びている**ことを示している。長期トレンドとしては約7か月で倍増するペースで推移している。
- この能力向上の背景には、LLM自体の推論力向上に加え、「エージェント型ワークフロー（自己内省・ツール利用・計画・複数AIの協調）」の確立がある。
- これらの要素により、数時間規模の業務プロセスをAIへ委任できる段階に入りつつある。

AIが対応可能なタスクの長さは、指数関数的に伸びている

LLMが対応可能な、タスクの長さの推移（成功率50%）



- 本図は、AIが自律的に完了できるタスクの長さを、人間の熟練者の所要時間で示した指標である。
  例えば「2時間」の長さとは、人間なら約2時間を要する課題を、AIが一定確率で完了できる能力水準を意味する。
- 近年のモデルでは、短時間の単発作業だけでなく、数十分～数時間規模の連続タスクが可能になっている。

※注意
本図が示す時間は、AIの独立稼働時間ではなく、人間の作業時間換算で、AIが50%の確率で完遂できるタスクの規模（長さ）を示す。本指標は特定条件下での能力推定であり、実運用の安定性を保証するものではない。また、実導入時には信頼性評価と、失敗を前提とした制御設計が必要である。

出所）METR「Task-Completion Time Horizons of Frontier AI Models」https://metr.org/time-horizons/
（2026年3月17日参照）

なぜ今なのか

相互運用の標準化により、孤立したエージェントが連携可能になりつつある

- MCP※1を始めとした標準プロトコルの登場により、エージェント同士が協調動作する環境が整いつつある。
- 実際に、人間を介さずAI同士がAPI経由で自律的に相互作用する事象も既に確認されている。
- 企業は単体利用だけでなく、**複数エージェントの連携を前提**にシステムの設計を考える必要がある。

標準プロトコルによる「相互運用性」の獲得

出所）https://www.linuxfoundation.org/press/linux-foundation-announces-the-formation-of-the-agentic-ai-foundation

- 2025年にはGoogleがA2A※2を公開し、2025年末にはLinux Foundation配下でAAIF※3が発足するなど、エージェント連携の標準化議論が進み始めている。
- 特定のベンダーに依存せず、異なる専門性のエージェント群がシステムを跨いで協調する技術的な土台が整ってきた。

エージェント同士の相互作用が顕在化

出所）https://www.bloomberg.com/news/articles/2026-02-10/what-is-moltbook-the-ai-only-social-network

- 2026年1月に公開されたエージェント専用SNS「Moltbook」では、人間が介在せず、AIエージェント同士がAPI経由で自律的に投稿や返信、投票を行っている。
- エージェント間の自律的なコミュニティ形成が見られている。

※2026年3月 MoltbookはMetaにより買収された。

※1 **MCP** (Model Context Protocol)：AIモデルと外部のデータソースやツールを、安全かつ標準化された手順で連携させるためのオープンな接続規格
※2 **A2A** (Agent-to-Agent Protocol)：異なるAIエージェント同士が自律的に通信し、タスクの委譲や複雑な情報交換を協調して行うための標準的な通信プロトコル
※3 **AAIF** (Agentic AI Foundation)：エージェント型AIの相互運用性やオープンな技術標準の策定を推進する国際的なコンソーシアム

エージェント型AIの萌芽事例

事例の俯瞰

業務特性やデータ整備状況に応じ、萌芽事例は4つの価値創出パターンに大別される

- 完全な自律稼働を果たすエージェント型AIは未だ登場していない。一方、自動化の領域を拡張し、**段階的な自律化を模索する萌芽事例**は現れ始めている。
- 価値を創出する仕組みの違いにより、現時点の先行事例は 4 つの類型に分けられる。各類型には固有の前提が存在する。どの類型が適するかは、業務特性と既存データ、権限設計の状況で変わる。

	① トレンド即応型	② 例外復旧型	③ 仮想検証型	④ 統制組込み型
概要	外部トレンドを起点に、企画、初期設計、商品仕様書作成を連動させ、**商品化準備を早める**。 最終判断は人が担う。	遅延や未処理などの例外を検知し、状況確認、判断、再手配、通知までを連続して進める。**復旧速度が向上**する。	実機投入前に、試行がしやすい仮想空間にて、自律的に**検証を繰り返す**。 条件変更、異常時対応、最適化を行う。	権限、監督、証跡を先に設計し、その枠内で定型業務を任せる。 「自由な自律化」より「**安全な実行**」を優先する。
価値の源泉	需要変化を早く捉え、商品化の初動を前倒しできる。	例外対応の滞留を減らし、業務を早く正常化できる。	手戻りや停止リスクを抑え、立ち上げを安定化できる。	統制を守りながら、処理能力と再現性を高められる。
前提	• 外部トレンドのデータ化 • 設計情報との接続 • 人の承認	• 状態のデータ化 • 対応ポリシーの明文化 • 通信経路の整備	• 仮想環境の整備 • 現場データとの連携 • 検証条件のモデル化	• IDと権限の設計 • 監督者の設定 • 監査と承認ルールの整備
萌芽事例	米Walmart （小売）	米C.H. Robinson （物流）	独Siemens （製造）	米BNY Mellon （金融）

※各情報の出所は以降の事例の紹介ページに記載

萌芽事例｜① トレンド即応型｜米Walmart（小売）

商品企画から製造までのプロセスをAIで連動させ、商品化のリードタイムを短縮する

- Walmartは2025年、AIを活用してSNSのトレンド分析から商品デザイン・製造・物流・棚出しまでの、商品開発工程全体をAIで効率化する取り組みを発表した。
- トレンド調査と初期設計の**作業をAIで圧縮**。6ヶ月を要していた商品の企画から発売までを、最大18週間短縮した。
- AIの生成案を人が判断して品質とブランド価値を担保する、「定型生成＋判断集中」の役割分担を採用している。

AIで流行や変化への対応速度と開発リードタイムを短縮する「Trend-to-Product」

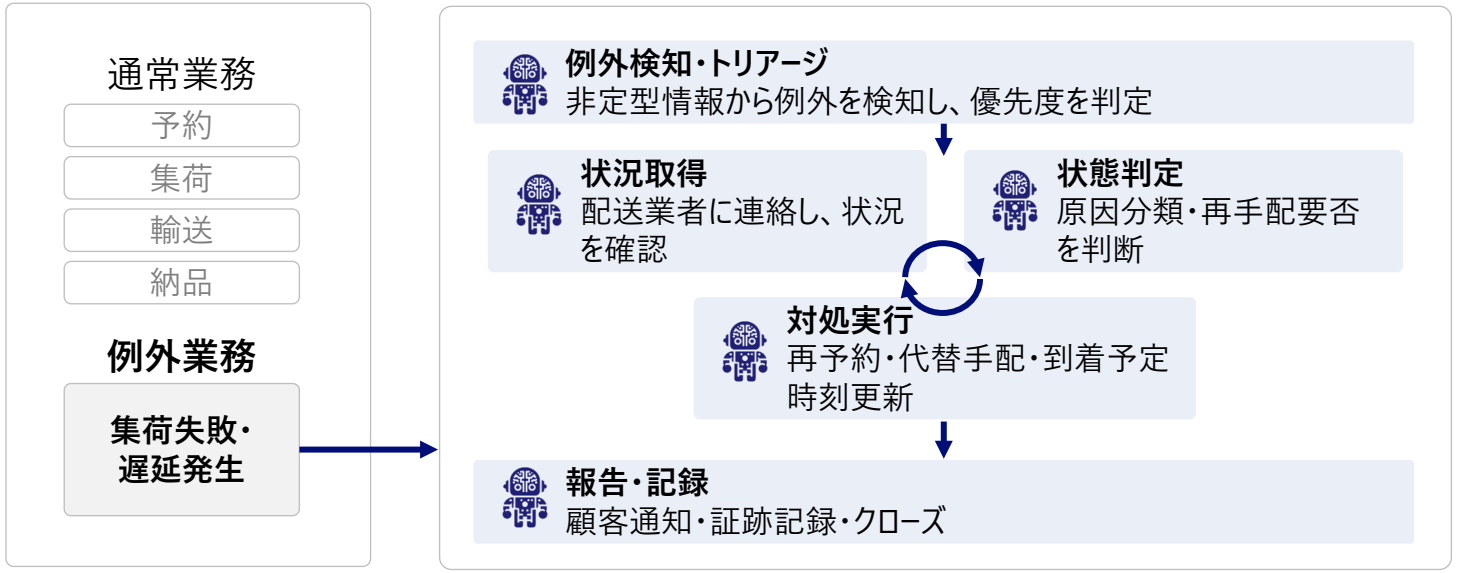
	トレンド収集/分析	初期デザイン案作成	デザイナー決定	デザインパック作成	サプライヤー連携
従来	デザイナー/商品責任者 SNSやランウェイ情報を調べ、トレンドを解釈、要約して企画の起点を作る。	デザイナー ムードボード、商品コンセプト案、名称、素材案などを人手で作成する。	デザイナー/商品責任者 売れ筋などを踏まえ、採用案を絞り込み、最終案を決める。	商品開発/生産技術担当、商品責任者 仕様を整理し、デザインパックを作成し、整合性を確認する。	調達担当/サプライヤー デザインパックを共有し、質疑や試作調整の往復が発生する。
AIによる短縮	AIエージェント/デザイナー/商品責任者 **探索・整理の工数圧縮** 外部トレンドを収集、統合、分析し、示唆を提示する。人が確認する。	AIエージェント/デザイナー **叩き台作成、反復短縮** ムードボード等を短時間で生成し、人が精緻化と選別を行う。	デザイナー/商品責任者 **判断材料準備を高速化** 生成案を基に案を具体化し、売上情報なども踏まえて人が最終決定する。	AIエージェント/商品開発 **仕様書作成を自動化** AIがデザインパックを生成し、人がレビューして確定する。	AIエージェント/商品開発 **解釈ブレと手戻りを削減** デザインパックを起点に連携し、試作と量産へ接続する。

出所）https://corporate.walmart.com/news/2025/04/09/in-an-ever-changing-environment-walmart-uses-genai-to-create-cool-for-customers　を元に一般的な小売・アパレル業務分掌からの推定を加え作成。

非定型情報から状況をデータ化し、例外対応の自律化によって復旧速度を早める

- 米物流大手の C.H. Robinsonは、30以上のAIエージェントが連携する自律システムを構築した。AIで非定型情報をデータ化し、**例外対応の自律化**を進めている。
- 物流業務においては、遅延、欠品、変更などの例外が日常的に発生し、「例外の早期検知→復旧→顧客への説明」という一連の対応速度が重要となる。一方、従来は電話やメールを起点として、担当者の経験と手作業に大きく依存してきた。
- 同社は、複数の専門エージェントが連携する仕組みにより、属人的な調整業務の自動化を進めている。

エージェントが連携して、人手による例外対応を自動化する「Agentic Supply Chain」



導入成果

- 集荷失敗チェックの**95%を自動化**
- **1日350時間超**の手作業を削減
- 無駄な再集荷手配を**42%削減**
- 輸送リードタイムが**最大1日短縮**

出所）https://www.chrobinson.com/en-us/about-us/newsroom/press-releases/2025/ch-robinson-agentic-supply-chain-advance-2025/ 、https://www.chrobinson.com/en-us/about-us/newsroom/press-releases/2026/chrobinson-lean-ai-agents-for-ltl-pickup-efficiency/ を元に作成

エージェント主導の仮想空間検証により、実世界における実行コストの削減を目指す

- Siemensは、設計、製造、運用をつなぐ産業AI基盤の拡充を進めている。実機での検証は手戻りや品質問題を招きやすいため、同社はデジタルツイン、シミュレーション、実データを組み合わせ、仮想空間での検証結果を実運用へ反映するコンセプトを模索している。
- 仮想環境は条件を固定、変更しやすく、安全に大量試行できるため、AIによる**自律的な比較や、異常検証の反復**に適している。エージェント型AIは、実世界より先に、検証可能な仮想環境で価値を出しやすい。

仮想空間での反復検証を含む「Industrial Copilot」

出所）https://press.siemens.com/global/en/pressrelease/siemens-expands-industrial-copilot-new-generative-ai-powered-maintenance-offering
出所）https://news.siemens.com/en-us/digital-twin-composer-ces-2026

萌芽事例｜④ 統制組込み型｜米BNY Mellon（金融）

統制を最優先とし、デジタル従業員を本番展開

- 2025年10月、BNY Mellonは100体超の「デジタル従業員」を配備し、定型業務の自動化を進めていると公表した。
- 金融機関におけるAI導入では、既存の法令、リスク管理、監査、ガバナンスの枠組みに適合させつつ、業務効率化や自動化の効果を追求することが求められる。実際、支払検証のように統制と正確性が求められる業務に加え、コード修正のような専門性を要する業務も、従来は人手に大きく依存していた。
- 同行は、デジタル従業員に対して人間の社員と同様のシステムID、アクセス権限、マネージャーを付与し、**既存の組織構造と権限管理体制に組み込む**ことで、統制を実現している。

デジタル従業員の展開方法

ペルソナ設計

AI Hub※がコード修正用と支払検証用の2種類のペルソナを約3か月で設計。インスタンスとして展開。

権限・アクセス設計

各インスタンスは導入チームの一員として割り当てられ、そのチームの業務データとツールにのみアクセス可能な個別の権限設計。

ツール利用・業務フローを設計

- **人間社員と同様のシステムID**が与えられ、社内アプリケーション群にアクセスして作業する。
- **既存の承認ワークフローと監査の仕組みと連携**させ、安定運用を図る。
- メールやMS Teamsの権限を与え、解決できない案件を自らエスカレーション可能にする（計画）

既存体制へ組み込み

- 所属チーム・人間のマネージャーを持ち、**評価・管理も組織のライン上**で行う。
- ボットではなく、特定チームの一員として働き、マネジャーへ直接レポートするAIスタッフとして位置づける。
- 自律実行を許容しつつ、コードマージや支払決定など最終判断は人間の承認を必須とするHuman-in-the-loop運用とする。

※**AI Hub**：2023年にピッツバークに設立。社内のデータサイエンティストやAI専門家を束ねる組織として機能。社内のAIユースケースの探索・優先順位付け・展開をリードする。

出所）https://www.wsj.com/articles/digital-workers-have-arrived-in-banking-bf62be49

萌芽事例から見える示唆

前提条件は「検証の土台」「データ整備」「境界の標準化」「現場協働」に集約される

- 萌芽事例は業種が違っても、実行の前提となる条件は大きく変わらない。
- なお、権限、承認、証跡といった統制は、これら全体を支える共通の前提として、組み込む必要がある。

萌芽事例から見える、実施の前提

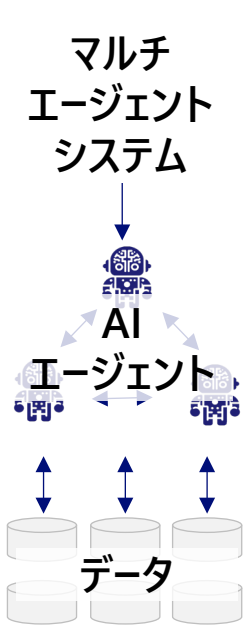
改善を回し続ける **「検証土台」**	自律性発揮の前提として、動かして逸脱を見つけ、戻し、改善できる運用を先に整える。
判断根拠となる **「データ整備」**	稼働の前提として、判断に使うデータの鮮度、網羅性、権限を揃え、非構造データも扱える状態にする。
成果物を固定した **「境界の標準化」**	横断実装のポイントとして、工程間で受け渡す成果物と品質基準を定め、差し戻しを減らす。
定着に向けた **「現場協働」**	共通の雛形を用意しつつ、現場と一緒に対象選定から定着まで進める。

エージェント型AIを支える技術とベンダー

全体最適と安全な実行を担保する、「データ・実行・統制」の3層アーキテクチャが必要

- エージェント型AIを支える技術は、信頼できる情報源を提供する「データ基盤層」、連携のオーケストレーションを担う「エージェント実行層」、ガバナンスを確保する「運用・統制層」の3層で構成される。
- 個々のエージェント性能が高くても、データの不整合や統制不在があれば本番運用は難しい。自律型AIの構築においては、これら3層のうち**自社環境で何が弱いかの確認が、検討の最初の着手点**となる。

全体最適と安全な自律実行を担保する3層構造



運用・統制層

- システム全体を監視・評価し、安全性とコンプライアンスを担保する。
- 自律的に動作するエージェントのリスクを管理し、信頼性を確保する。

エージェント実行層

- 複数の専門エージェントを実行し、計画、協調、記憶を管理する。
- タスクの動的な分割と依存関係の解決を行い、外部ツールの呼び出しと状態遷移をオーケストレーションする。

データ基盤層

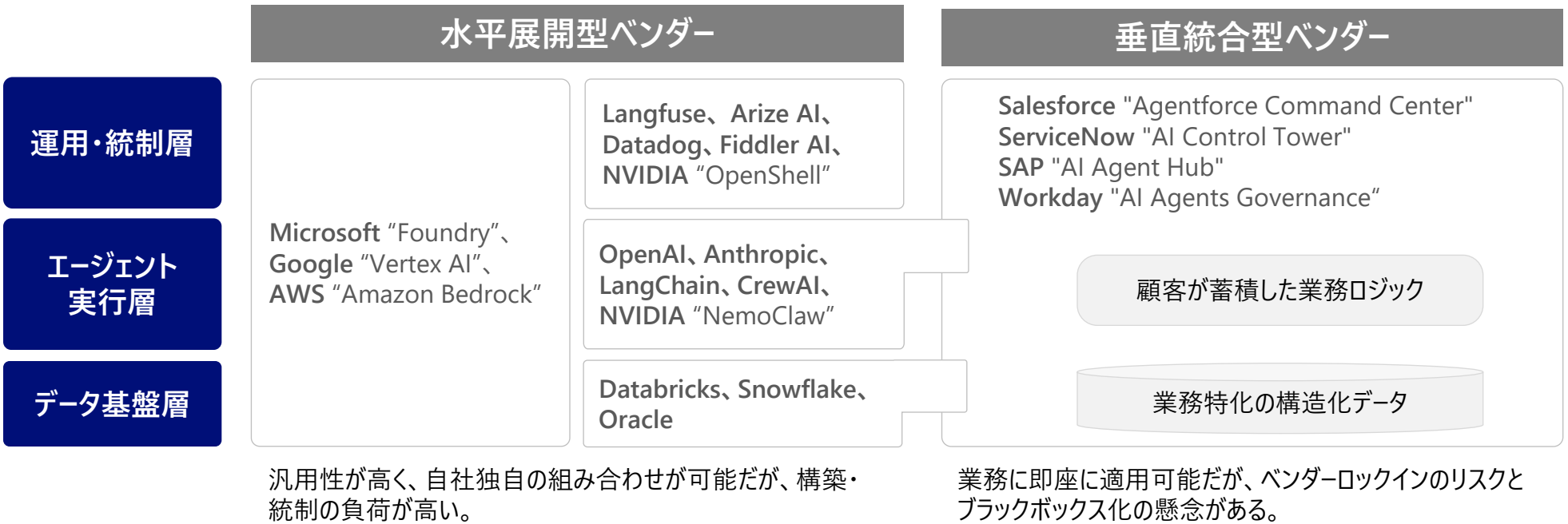
- 信頼できる唯一の情報源をリアルタイムに提供する。
- データのサイロ化や不整合を防ぎ、マルチエージェントの前提を整える。

エージェント型AIの関連ベンダー

AIエージェントの「工場」を提供する水平型と、「デジタルワーカー」を提供する垂直型が存在する

- ベンダーは、企業が独自のデジタルワーカーを構築するための汎用的な開発基盤（工場）を提供する「**水平展開型**」と、特定業務に特化し、即時稼働可能なデジタルワーカーを提供する「**垂直統合型**」に分けられる。
- 現時点では、垂直統合型の製品であっても、内部の推論エンジンには水平展開型の基盤モデルを利用するケースが多い。市場は「**協調と競争**」**が併存**する黎明期特有の段階にある。

エージェント型AIの関連ベンダー俯瞰と代表例



汎用性が高く、自社独自の組み合わせが可能だが、構築・統制の負荷が高い。

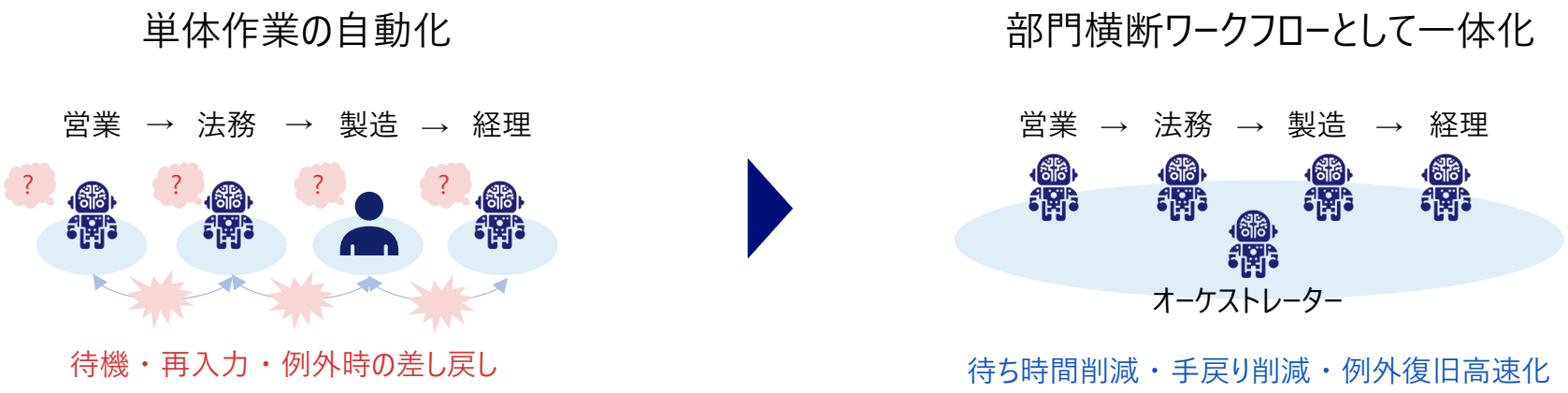
業務に即座に適用可能だが、ベンダーロックインのリスクとブラックボックス化の懸念がある。

※ベンダー名は推奨ではなく、市場構造を説明するための例

エージェント型AIの特徴は単体作業の自動化ではなく、業務の流れをつなぐ点にある

- 単体作業の自動化は個別タスクの効率化に有効な反面、前後工程や全体進捗の俯瞰が困難である。結果として意思決定が分断され、処理精度の頭打ちや、工程間の待機・受け渡し・手戻りといった非効率を招きやすい。
- そのため業務の自律化には、AIを単独ツールとしてではなく、計画・協調機能を備えた**「ワークフロー」としての実装**が有効であり、これはAI有識者の提唱方針※とも合致する。
- エージェント型AIは、複数エージェントが状況を共有・協調し、条件分岐を含む処理を自律実行する。これにより、部門横断プロセスが統合され、待機・手戻りの削減、迅速な例外復旧、全体的な判断精度の向上が実現する。

工程間の待ち時間や差し戻しを減らし、価値を高める



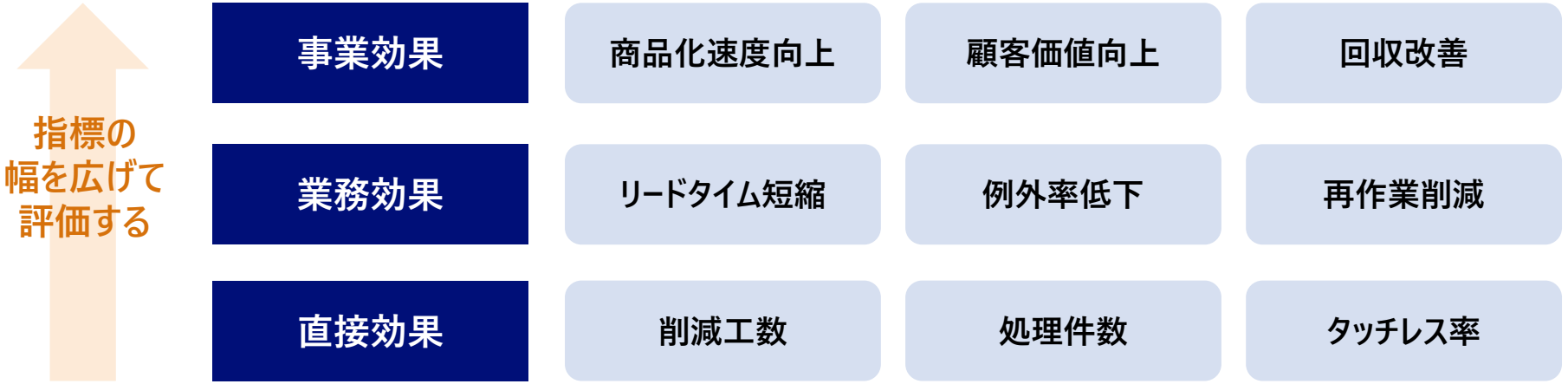
※ スタンフォード大学客員教授であり、著名なAI研究者である Andrew Ng氏は、「企業はAGIのような壮大な目標を追うよりも、既存技術を賢く組み合わせ、具体的なビジネス価値を生む『エージェント型ワークフロー』構築に集中すべきである」と提唱している。

エージェント型AIの実装方法

単体の工数削減ではなく、部門横断の滞留解消と品質向上によってROIを高める

- 個別作業の自動化にとどまる場合、工程間の待ち時間や手戻りが解消されず、十分な投資対効果（ROI）を示しにくい※。エージェント型AIは、複数エージェントの協調により部門横断プロセスを統合することで、滞留を解消し、例外復旧を迅速化する。
- そのため、導入効果は局所的な工数削減で測るのではなく、リードタイムの短縮や例外率の低下など、事業成果に直結する**業務フロー全体の指標でROIを評価**することが不可欠である。

導入効果の測定指標の例



※ MIT NANDA「STATE OF AI IN BUSINESS 2025」 https://mlq.ai/media/quarterly_decks/v0.1_State_of_AI_in_Business_2025_Report.pdf

普及に向けた課題

普及に向けた課題

エージェント型AIによる部門横断ワークフロー自律化の導入に向けた、事業会社の課題と論点

	課題と対策	対応の論点
技術： **自律性の向上**	**エージェントの動作品質が業務要件に達していない** • 逸脱の検知、復旧、再発防止の標準が未整備 • 長時間実行により、品質、意図、安全性が劣化する	✓**信頼性エンジニアリング**の確立 （計測・改善サイクルとフェイルセーフ設計）
ガバナンス： **動作の統制**	**エージェントの判断や動作を統制する共通基盤が不在** • 確率的な判断を本番業務へ直接適用できない • 権限管理が共通化されていない	✓プロセスオーケストレーション層による**決定的制御** ✓ID・権限・監査証跡の**共通基盤構築**
組織： **全体最適の実現**	**部門横断で自動化の効果を評価する機能が不在** • 独立した支援機能により、フローが途中で止まりやすい • 部門別KPIのため効果が全体で測りにくい	✓法務、経理、人事などの**支援機能を業務へ埋め込む** ✓共通データとKPIを軸に**Ops基盤**を構築

普及に向けた課題｜技術に関する対応の論点

信頼性は従来の稼働・停止に加え、逸脱をどう検知し復旧するかで測定する

- エージェント型AIの運用では、従来のSRE※ における監視の観点を、**AI特有の「品質・意図・安全の逸脱」を扱える**形に再定義する必要がある。
- その中では、障害を停止条件ではなく「出力品質や目標達成の劣化イベント」として捉え、観測・復旧・再発防止を仕組みとして確立することが普及の前提となる。

「観測・復旧・再発防止」を確立する、信頼性測定指標

システムの信頼性を測定する指標

逸脱の早期検知

品質・意図・安全の逸脱を「**障害**」**の兆し**として早期に検知

幻覚兆候、根拠不整合、目標ドリフト

安全停止・迅速復旧

失敗時に**自動回復と人手介入**で安全に処理を再開

ツール失敗、ループ、権限逸脱、委任の期限

再発防止

仮想環境（デジタルツイン）などを活用した**反復テスト**により、精度・性能の劣化を防止

逸脱率、完遂率、品質閾値違反

長時間運転時の破綻を検知する指標

ハルシネーションの蓄積	**文脈の欠落**
目標の逸脱	**エージェント間の連携不備**

※ **SRE** (Site Reliability Engineering)：Googleが提唱したソフトウェアエンジニアリングの手法を用いて、システムの信頼性（安定稼働）を維持・向上させる運用アプローチ。

確率的に動作するAIを実業務に適用するには「プロセス・オーケストレーション層」が必須となる

- 確率的に動作する生成AIを、高精度な実業務へ直接組み込むことはリスクを伴う。一方で、柔軟さや非定型対応力は生成AIの強みであり、制約をかけすぎると従来システムやRPAと変わらなくなる。
- このジレンマを解決するのが「プロセス・オーケストレーション層」である。AIによる「確率的な判断」を、処理の順序や分岐、期限、失敗時の取り消し、人的承認といった**「決定論的なルール」で統制**し、タスクの依存関係や例外復旧を一元管理する。
- これにより、AIの非定型対応力を活かしつつ、業務フローの確実性と監査性を両立させることが可能になる。

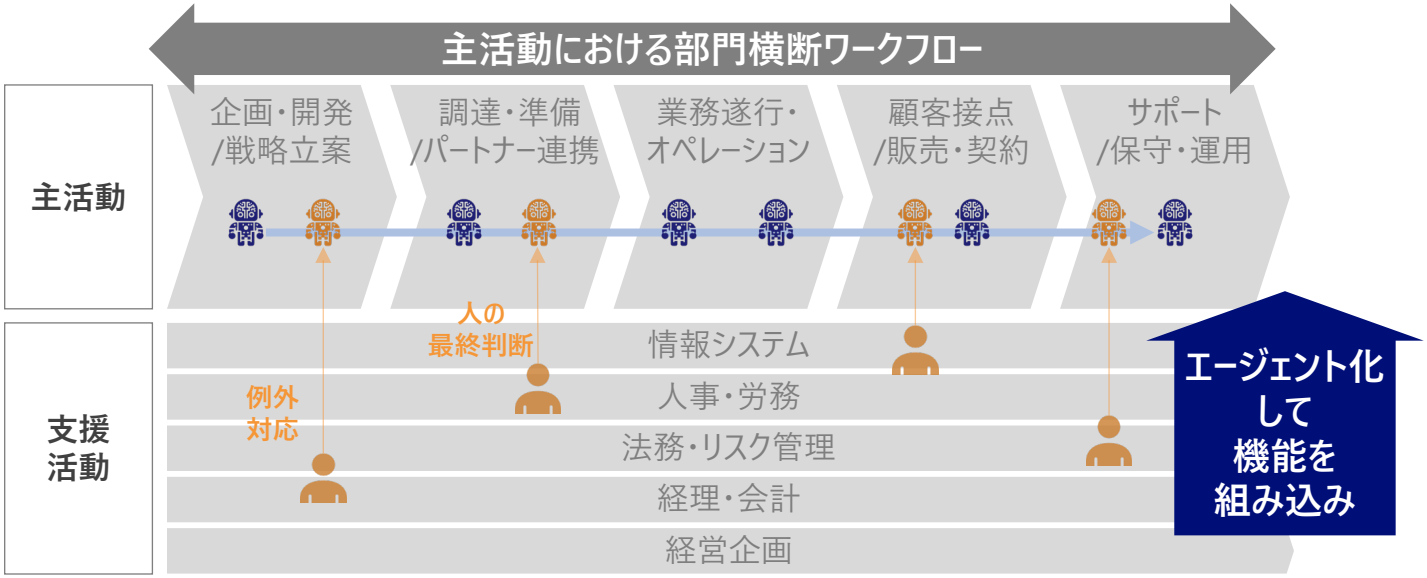
多層オーケストレーション構造

	機能概要
意思決定層（AI層）	• 生成AI・ルール・スコアリングで判断トリガーを生成。 • 承認、分岐、優先度、例外処理の提案を行い、下位フローへ指示を出す。
判断トリガー ↑ ↓ 判断結果	
プロセス・オーケストレーション層	• 業務フロー全体の統合的な制御を担う。 • 処理の順序や分岐、期限、リトライ、失敗時の取り消し（補償）などを一元管理し、AIの意思決定層とシステムの実行層を橋渡しする。
実行計画 ↑ ↓ 実行指示	
実行管理層	• 個別タスクの実行・再実行・リソース割当・キュー管理。 • RPAやジョブ、関数、API呼び出しを確実に動かす。
イベント通知 ↑	
イベント連携層	• 複数システムをリアルタイムに接続し、状態の変化を上位層へ即座に通知する。 • イベントの検知、継続的な通信、外部サービス連携、データ形式の統一を担う。

支援活動の組み込みにより、部門横断のプロセスを実現する

- 企業のバリューチェーンと同様に、AIへの業務委託においても、プロセスを前へ進める「主活動」と、品質管理や法務確認などを担う「支援活動」に分離して設計することが重要である。
- 主活動におけるエージェントの整備とともに、専門化した支援活動のエージェントをプロセス内に**「エンベデッド（組み込み）」**することで、業務の実行速度を落とさずにガバナンスを効かせることが可能になる。
- ただし、規程解釈や高リスク判断では、人の最終判断を残す前提が現実的である。

支援機能を後工程で回すのではなく、必要な場面で業務フローに埋め込む



エンベデッド法務：
契約書作成のリアルタイム化

契約書作成時に、法務が条項を確認し、会計ルールとの整合も同時に確認する。別部門へ回す往復を減らし、起案から締結までの待機を短くする。

その他の例

エンベデッドHR
エンベデッド監査・コンプライアンス
エンベデッドファイナンス

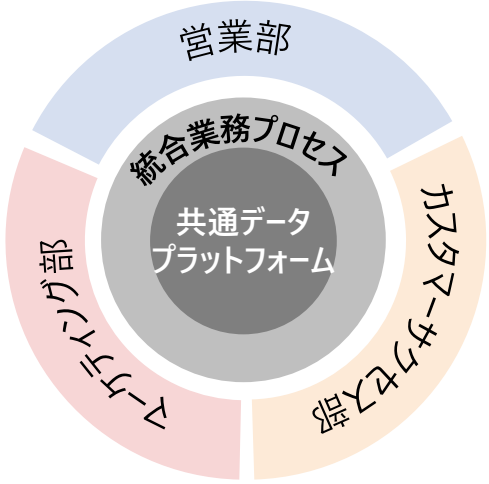
普及に向けた課題｜組織に関する対応の論点

ミッションが異なる部門のエージェント群を全体最適化する「Ops基盤」の整備が不可欠である

- Ops基盤とは、共通データ、共通KPI、責任分界、改善サイクルを束ね、部門別の局所最適を全体最適へ変える運営基盤である。
- AIエージェントが営業、マーケ、CS、調達、生産などを横断して動くほど、どのKPIを優先するか、例外時に誰が判断するか、改善責任を誰が持つかを明確にする必要がある。
- これは単なるITの導入ではなく、目標設定、権限配分、評価制度まで含む**業務運営の設計変更**である。

エージェント型AIの実運用で求められる、「Opsモデル」の例

「RevOps」（収益横断最適）



- 営業・マーケティング・CS間で分断されていた業務プロセスとKPIを統合し、共通の顧客データに基づく横断的な意思決定を仕組み化する。
- 顧客獲得の精度向上やリードタイムの短縮、解約抑制といった各部門の活動を連動させ、最終的な目的である全社の収益成長を最大化する。

ProfitOps（利益横断最適）

営業、購買、生産を横断し、売上、原価、経費を合わせて利益を最適化する。

RiskOps（リスク横断最適）

分散したリスク管理を統合し、監視と未然防止を強化する。

出所）https://www.gartner.com/en/sales/topics/revenue-operations　の整理も踏まえ、本資料で整理

今後の見込み

今後の見込み

企業内自律化は、やがて企業間の自律連携へ広がる

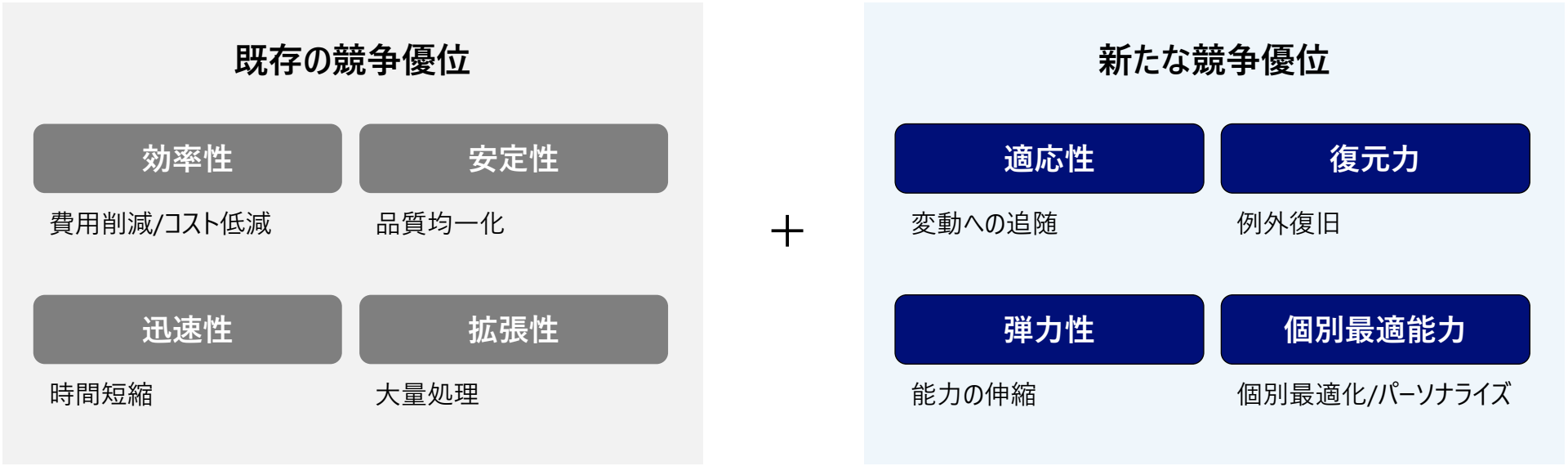
- 企業内では、既存システム、人、統制の上にエージェント型AIが重なり、判断と実行の一部を担う「**自律型企業（エージェンティック・エンタープライズ）**」が立ち上がる。次の段階では、こうした企業を中心に、部分的に自律化した企業、従来型企業、個人のエージェントが接続され、発見、交渉、契約、履行が機械可読な条件の下で連鎖する「**自律型経済圏（エージェンティック・エコノミー）**」が形成される。
- この変化は、企業に対して、待ち時間や例外復旧の削減による生産性向上、取りこぼし需要の回収、遊休資産や余力の流動化、市場接続コストの低下をもたらす。
- また、社会全体に対しては、需給調整や障害時復旧の柔軟化を通じたレジリエンス向上をもたらす。加えて、Agent ID、委任管理、決済、監査、紛争処理、能力流通といった基盤そのものが、新たな認証、保証、仲介サービスの市場を形成していく可能性がある。

自律型企業と自律型経済圏

事業会社の競争優位は、効率だけでなく、適応と回復へ広がる

- 実行を担えるエージェント型AIの活用により、企業の競争優位性は、従来の「効率性・安定性・迅速性・拡張性」といった静的な指標を超え、新たな能力を獲得できるようになる。不測の需要変動に対する「**適応性**」、例外事象からの「**復元力**」、処理能力の「**弾力性**」、そして状況や顧客に応じた「**個別最適化能力**」が、今後の市場における必須要件となる。
- これを受け、企業間競争の主軸は「**不確実性下における持続的な成長力**」へと拡張する。事業会社には、自社が培ってきた既存の強みと、AI技術がもたらす新たな共創優位の統合が求められる。

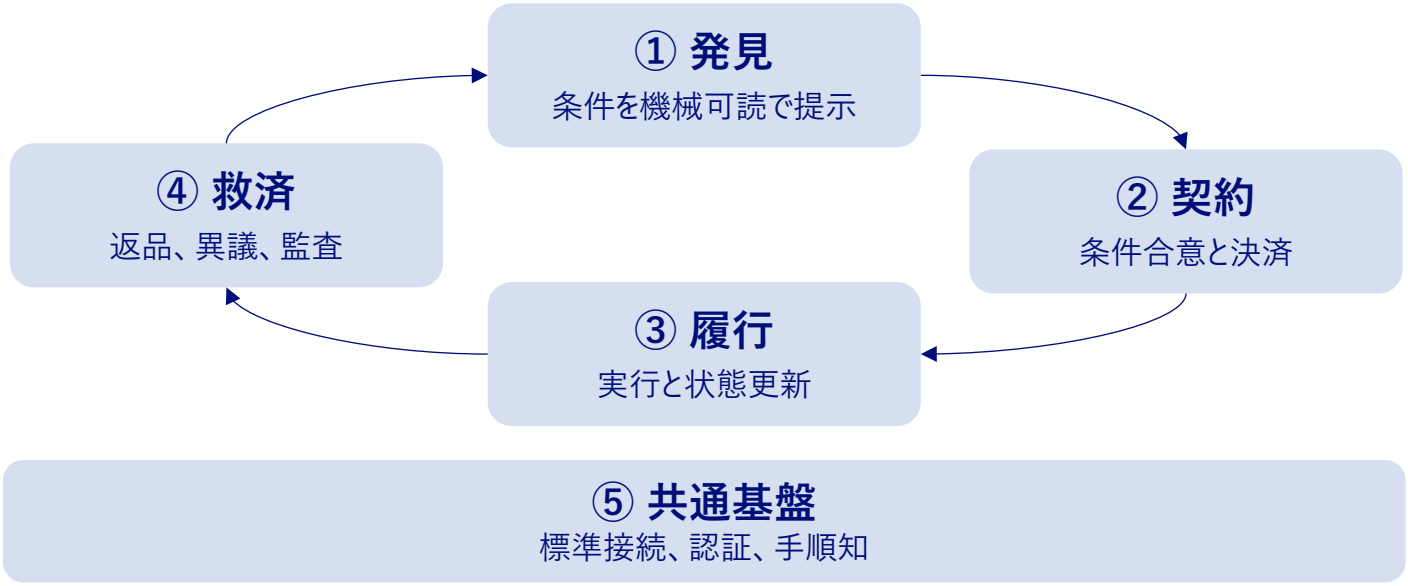
エージェント型AIにより、事業会社が獲得できる新たな競争優位



エージェントの企業間連携により、新たな「経済圏」が形成される

- エージェンティック・エコノミーとは、複数企業が提供する自律型AIエージェントが、意思決定・交渉・取引・実行を担い、相互に連携しつつ競争しながら形成される経済活動を指す。
- 単なる自動化ではなく、企業をまたぐプロセスがエージェント間の相互作用で進行し、成果と責任がエージェント単位で可視化される世界観である。
- 必要な機能は、**①発見**→**②契約**→**③履行**→**④救済**と、下支えする**⑤共通基盤**で構成される。

エージェンティック・エコノミーを形成する機能



※ スケールの条件
- 条件の機械可読化
- 任せる範囲の明確化
- 実行と監視の閉ループ化
- 救済と説明責任の設計
- 相互運用標準の整合

自律型コマースの分野が先行し、経済圏の構成要素が実装され始めている

■ 商取引は、商品探索、支払い、配送、返品という流れが比較的明確で、決済と救済の仕組みも整っている。
■ エージェント連携を実装に落とし込みやすいため、自律型経済圏の構成要素の実装が先行して始まっている。

自律型コマースの環境整備と、関連技術・ベンダー

① 発見

ユーザー要求に基づき、商品や配送等の情報を評価・順位付けする。

- OpenAI
- Google

② 契約

代理決済により取引条件を共有し、加盟店が承認・拒否を判断する。

- Visa

③ 履行

既存システムで提供・返品等を処理し、例外事象は上位へ通知する。

- Mastercard

④ 救済

正規性確認や脅威対応を組み込み、迅速なトラブル解決で信頼を担保する。

- Cloudflare

⑤ 共通基盤

相互接続を標準化し、タスク実行手順やルールの再利用を促進する。

- **接続標準** (ACP/UCP※)
- **手順知** (Agent Skills/AGENTS.md※)
- **監査・認証** (Auth/Audit)
- AAIF (Linux Foundation)

※ **ACP/UCP**：エージェント間通信および商取引を自動化するための標準プロトコル（Agent Communication Protocol / Universal Commerce Protocol）
※ **AGENTS.md / Agent Skills**：サイト側がAIエージェントに対して「実行可能なタスク」や「ルール」を提示するための機械可読ファイル

今後の見込み

エージェント型AIの普及は、個別業務から企業内横断、企業間連携へと段階的に進む

- 普及は、個別業務での即応から、企業内の横断実行、限定的な企業間連携へと段階的に進む可能性が高い。
- 短期は信頼できる運用の確立、中期はデータと権限をまたぐ実行、長期は標準と救済が整った領域での連携が焦点になる。

	短期（～2026年）	中期（2027～29年）	長期（2030年～）
	個別業務	**企業内横断**	**企業間連携**
	特定業務で即応力を磨き、評価とガードレールで運用品質を固める。	部門横断で実行をつなぎ、共通データと権限の上で全体最適を進める。	標準、認証、決済、救済が整う領域から、企業間の自律連携が立ち上がる。
企業の競争優位性	• 即応性 • 品質安定	• 待ち時間削減 • 例外復旧 • 並行実行力	• 新市場 • 連携コスト低下
主要技術	• 専門エージェント • RAG • 評価とガードレール	• オーケストレーション • マルチエージェント • 統合データ • 共通KPI	• 相互運用標準 • Agent ID • 決済と救済
活用領域	自律型企業 企業内（個別業務・タスク）	企業内（部門横断の業務フロー）	自律型経済圏 企業間連携、自律型市場

まとめ

まとめ

エージェント型AIの本質は、対話の高度化から「プロセスの自律実行」への進化にある

■単なるモデル導入から、統制を伴う「システム基盤」の構築へ

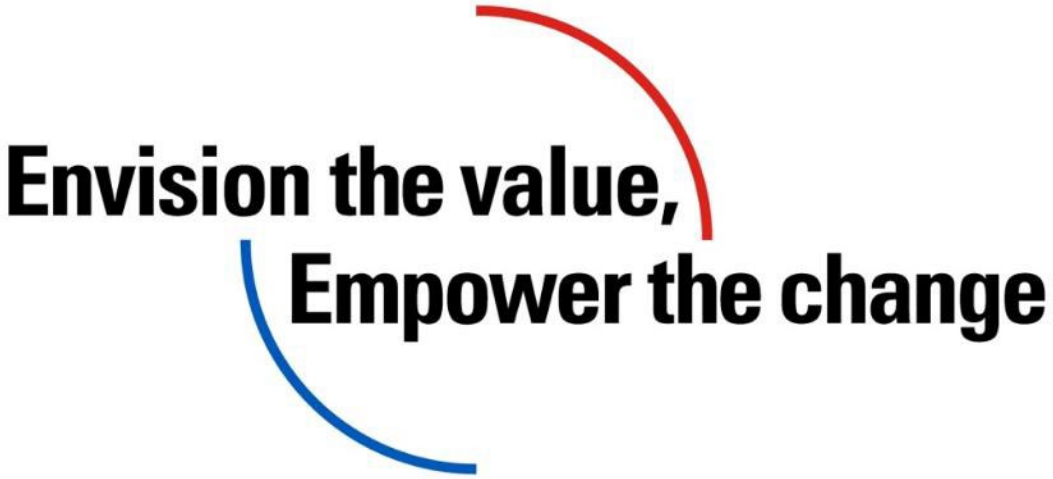
- エージェント型AIは、人間のプロンプトを待つ受動的なツールではなく、イベントや状態変化を起点にプロセスを自律的に完遂する**「主体」**である。
- その実装には、AI単体の性能向上に依存するのではなく、データ基盤、オーケストレーション層、運用統制（ガバナンス）を統合した**「システムアーキテクチャ」の構築**が不可欠となる。

■局所的な工数削減から、「部門横断の滞留解消とフロー全体の最適化」へ

- 価値の源泉は、局所的な工数削減ではなく、工程間の待ち時間、手戻り、例外対応を仕組みとして解消し、**業務の流れを統合する点**にある。
- したがって、導入効果はリードタイムの短縮や例外率の低下など、事業成果に直結する指標を用いて、**ワークフロー全体で評価・測定**する必要がある。

■企業の競争優位は、「不確実性下における持続的な成長力」へ

- エージェント型AIの適用範囲は、**企業内の個別業務**から**部署横断**、そして相互運用を基盤とした**企業間連**携へと段階的に拡大する。
- この移行に伴い、企業に求められる競争力は静的な効率性だけでなく、環境変化への適応や例外からの復元力を備えた、**動的かつ自律的な事業基盤**の確立へとシフトする。


Envision the value,
Empower the change