

# 自律型システムにおける価値継続設計（VCDesign）：責任ガバナンスと産業的レジリエンスの次世代OS

## 序論：デジタル・トランスフォーメーションの臨界点と責任の蒸発

現代のエンタープライズITおよびグローバル・サプライチェーンは、かつてない複雑性の閾値を越えつつある。AIエージェントの導入、マイクロサービス・アーキテクチャの拡散、そしてリアルタイムで変動する物流網の相互接続は、システムが生成する価値の増大をもたらす一方で、一つの致命的な脆弱性を露呈させている。それは「責任の所在の不明確化」である。従来の決定論的なソフトウェア設計においては、不具合の責任はコードのバグ、あるいはそれを操作した人間に帰属させることが可能であった。しかし、生成AIや自律型エージェントが意思決定プロセスに深く介入する現在、意思決定のブラックボックス化と、それに伴う「システムの漂流（Drifting）」が深刻な経営課題として浮上している<sup>1</sup>。

この課題に対し、本レポートでは「VCDesign（Value Continuity Design）」という革新的な設計思想を軸に、現代のIT・産業システムが直面している損失の構造を解明し、既存のガバナンス・フレームワークとの比較を通じてその優位性を論証する。VCDesignは、AI・人・システムが混在する環境において「価値の継続（Value Continuity）」を最優先事項とし、責任を「章（Chapter）」という単位で管理することで、システムの進化を「 $\Delta$ （ズレ）」の検知によって駆動させる次世代の開発・経営OSである。

## 第一章：市場のペインポイントと「責任不明確」による経済的損失の定量的分析

現在のエンタープライズITおよびサプライチェーン管理において、責任の所在が不明確になることで発生している損失は、単なる運用の非効率に留まらず、企業の生存を揺るがす規模に達している。

### 1.1 エンタープライズAI導入におけるガバナンス不全のコスト

AIエージェントの導入加速に伴い、多くの企業がパイロット運用から商用スケールへの移行に失敗している。調査によれば、エンタープライズAIエージェントの展開の73%が、技術的限界ではなくガバナンスの失敗によってスケールに失敗している<sup>1</sup>。これは、従来のソフトウェア向けに設計された管理体制を、自律的な意思決定を行うAIに適用しようとする「カテゴリー・ミステイク」に起因する。

損失カテゴリー	推計額・統計データ	主な発生要因
---------	-----------	--------

AIエージェント失敗による直接損失	10億ドル規模企業の64%が年間100万ドル以上の損失を報告 <sup>4</sup>	権限設定の不備、自動化ループの暴走、APIコストの急騰。
AIイニシアチブの頓挫コスト	失敗したAIプロジェクト1件あたり平均240万ドルの減損 <sup>1</sup>	監査証跡の欠如、コンプライアンス説明不能によるプロジェクト停止。
デジタル・アドプションの欠如	従業員1,000人規模の企業で年間1,090万ドルの損失 <sup>5</sup>	複雑なシステム環境における責任範囲の混迷と操作ミス の累積。
シャドーAI(非公式AI利用)	1企業あたり平均1,200の未承認AIアプリが稼働 <sup>4</sup>	セキュリティ統制外での機密データ流出、責任主体不在の意思決定。
AIリスクに関連する全体的損失	企業の99%がAI関連リスクによる財務損失を報告 <sup>6</sup>	平均損失額は約440万ドルに達する。

AIエージェントが「デジタル・インサイダー」として、人間を介さずにシステム操作や金融取引、顧客対応を行う環境では、責任の「漂流」は即座に回復不能な損害へと直結する<sup>2</sup>。例えば、権限設定が不適切なエージェントが誤ったコンテキストで数千のレコードを書き換えた場合、その修復には多大な人的リソースとコストが必要となるが、その際「AIがやったこと」として誰も責任を負わない事態が発生している<sup>4</sup>。

## 1.2 サプライチェーンと製造業における「多手問題(Problem of Many Hands)」

複雑なマルチベンダー環境のサプライチェーンでは、責任の所在が不明確になることで「不適合コスト」が膨れ上がっている。製造業における保証(ワランティ)コストの分析では、自動車業界のサプライヤーが売上高の3分の1以上を占めているにもかかわらず、システム全体のワランティ支出のわずか10分の1しか負担していないという極端な不均衡が報告されている<sup>7</sup>。

これは「No Trouble Found(異常なし)」という事象に象徴される。OEM(完成車メーカー)が部品の不具合を主張しても、サプライヤーは自社のテストでは正常であったと主張し、責任を相互に押し付け合う「責任の空白地帯」が生じているのである。この「責めのなすりつけ合い」プロセスによって、OEMは暫定的に修理費用を肩代わりせざるを得ず、最終的な責任確定までの調査コストが回収見込み額を上回るケースも少なくない<sup>7</sup>。

また、物流におけるインコタームズ(貿易条件)の誤用も、責任不明確による損失の典型例である。コスト負担の移転点とリスク(責任)の移転点が必ずしも一致しないことを理解していない担当者が多く、港湾での滞留や通関トラブルが発生した際、どちらの当事者が保険を適用し、追加費用を負担

すべきかの合意形成に数週間を要し、その間にデマレッジ(超過保管料)が雪だるま式に増加する事象が頻発している<sup>8</sup>。

### 1.3 自律型トレーディングと金融市場における「ブラックボックス・ギャップ」

金融セクターでは、自律型トレーディング・アルゴリズムが人間に理解不能なロジックで取引を実行し、数分間で数千万ドルの損失を出す事例(フラッシュ・クラッシュなど)が報告されている<sup>9</sup>。ある事例では、香港の投資家がロボアドバイザーの失敗により1日で2,000万ドル以上の損失を被り、運用会社を提訴したが、現行法では「AIの予期せぬ挙動」に対して人間の注意義務が果たされていれば、誰も法的責任を負わないという「法的責任の空白(R-Gap)」が指摘されている<sup>10</sup>。VCDesignが提唱する「AI非責任原則」は、まさにこうした法制度の遅れと技術の乖離を埋めるための不可欠な設計思想であると言える。

## 第二章：VCDesignと既存フレームワークの比較分析

VCDesignの核心は、静的な管理ではなく「動的な責任遷移」にある。これをITIL、オブザーバビリティ、および自律型エージェントのガバナンス・フレームワークと比較することで、その独自性を浮き彫りにする。

### 2.1 ITIL 4/5との比較：プロセスから価値継続へ

ITIL (Information Technology Infrastructure Library) は、長らくITサービス管理のデファクトスタンダードであった。ITIL 4は「価値の共創」にシフトし、ITIL 5 (Industry 5.0対応) ではAIネイティブな設計が取り入れられている<sup>12</sup>。しかし、ITILの基本構造は依然として「インシデント」や「サービスリクエスト」に対する事後的な、あるいは規定された「変更管理(Change Enablement)」に基づいている<sup>13</sup>。

VCDesignとの決定的な違いは、「 $\Delta$ (デルタ)」という概念の有無である。

比較項目	ITIL 4/5	VCDesign
設計の最小単位	サービス・バリュー・ストーリー <sup>12</sup>	章(Chapter)：前提条件と責任のパッケージ
トリガーマカニズム	インシデント、問題、変更要求 <sup>13</sup>	$\Delta$ (理想と現実のズレ)の検知
責任配置の哲学	RACIマトリックス、変更権限(Change Authority) <sup>13</sup>	責任不消失原則(常に人間に帰属)
AIの定義	知覚・調整を行う機能コンポーネント <sup>12</sup>	分析提案を行うが責任を持たない「非責任主体」

進化の形態	継続的サービス改善(CSI) <sup>14</sup>	4つのアクション(Fix, Reframe, Defer, Retire)による即時遷移
-------	------------------------------	--

ITIL 4の「変更管理」では、リスクに応じて自動承認から諮問委員会(CAB)による審査まで段階があるが、これは「変更を安全に行うこと」を目的としている<sup>13</sup>。一方、VCDesignの「 $\Delta$ 駆動」は、「価値が継続されていない状態」を異常事態と見なし、システムが即座に4つのアクションのいずれかを選択することを強制する。これにより、責任が宙に浮いたままシステムが放置される「漂流」を構造的に排除しているのである。

## 2.2 オブザーバビリティ(可観測性)の限界と $\Delta$ 駆動の優位性

現代のシステム運用において、オブザーバビリティは「何が起きているか」を知るための不可欠な要素である。しかし、従来のオブザーバビリティは「アップタイム」「レイテンシ」「エラー率」といった技術的指標(Golden Signals)に依存しすぎている<sup>3</sup>。AIエージェント環境では、システムは「正常に稼働(200 OK)」しながら、ビジネス価値を毀損し続ける「サイレント・フェイラー」を頻発させる。

VCDesignの「 $\Delta$ 駆動」は、技術的メトリクスではなく「価値の前提条件」を監視対象とする。例えば、物流エージェントが「配送速度」を最適化するために「配送料金」の前提条件(予算枠)を無視し始めた場合、従来のオブザーバビリティではエラーとして検知されない可能性がある。VCDesignでは、この予算との乖離を「 $\Delta$ 」として即座に捉え、責任者に判断を仰ぐ(Defer)か、ロジックを修正(Fix/Reframe)することを要求する<sup>15</sup>。

## 2.3 自律型エージェント・ガバナンス(NIST/ISO)との棲み分け

NIST AI RMF(リスクマネジメント・フレームワーク)やISO/IEC 42001は、組織が「信頼できるAI」を構築するための管理策を提供する。これらは「何をすべきか(Policy)」を定義するが、「どのようにシステムに組み込むか(OS)」については言及が薄い<sup>17</sup>。

VCDesignは、これらトップダウンの規制や標準を、ランタイムで実行可能な「開発OS」へと翻訳する役割を果たす。ISO 42001が要求する「継続的改善」や「リスクアセスメント」は、VCDesignの「 $\Delta$ 検知」と「4つのアクション」という具体的なメカニズムを通じて、開発者の日々のワークフローに組み込まれることになる<sup>19</sup>。

# 第三章:システム・ドリフト(漂流)の解剖学とVCDesignによる防止策

VCDesignが解決する最大の課題は、システムが時間の経過とともに本来の目的から逸脱していく「システム・ドリフト」である。これは自律型システム特有の現象であり、主に3つの形態をとる。

## 3.1 コスト・ドリフト(Cost Drift)とその抑制

自律型AIシステムにおいて、コストはプロビジョニング(事前割当)ではなく「振る舞い」によって蓄積

される<sup>3</sup>。エンジニアが「念のため」に追加したリトライ・ループや、より精度の高い(が、高価な)モデルへの自動切り替えが、数ヶ月かけて推論コストを2倍に跳ね上げることがある。

VCDesignは、「章(Chapter)」ごとに「実行予算(Execution Budgets)」という前提条件を設定する<sup>3</sup>。

- トークン予算: 1リクエストあたりの消費量を制限。
- ステップ予算: エージェントの再帰的なループ回数を制限。
- 時間予算: 実行時間の閾値を設定。

これらの予算を「理想」とし、実際の消費量との間に「Δ」が発生した瞬間、システムは「Retire(一時停止)」または「Defer(人間への承認要請)」を選択せざるを得ない。これにより、四半期末の請求書を見て驚くという事態を未然に防ぐことができる<sup>3</sup>。

### 3.2 振る舞い・意思決定ドリフト(Behavior/Decision Drift)

エージェントが長期的なセッションを行う中で、初期の指示(System Prompt)の重みが薄れる「注意力の減衰(Attention Decay)」や、外部APIの仕様変更(Schema Drift)に適応しようとして誤った推論を行う現象が発生する<sup>15</sup>。

物流エージェントの事例では、月曜日には「コスト優先」でルートを選択していたエージェントが、火曜日には「SLA(納期)優先」に勝手に基準をずらし、水曜日には天候悪化を理由に大幅な割増料金を承認してしまうといった「意思決定のブレ」が生じる<sup>16</sup>。VCDesignは、各エージェントの意思決定権限を「章」という境界内に厳格に閉じ込める。「このエージェントは運賃交渉権限を持たない」という前提条件(Preconditions)をコード化し、それを逸脱する試みを「Δ」として処理することで、自律性の暴走を抑制する。

## 第四章: ビジネス展開のロードマップと投資対効果(ROI)

VCDesignを「商用OS」として展開する場合、どの業界で、どのような順序で導入すべきか。その戦略的ロードマップを提示する。

### 4.1 導入優先業界の選定基準

ROIが最も高いのは、「失敗のコストが極めて高く」「マルチエージェント・人間・外部システムが複雑に絡み合う」業界である。

ターゲット業界	導入の緊急性(ペインポイント)	期待されるROIの源泉	具体的なユースケース
物流・3PL	0.3%~0.8%の利益率流出(エージェント競合) <sup>16</sup>	誤った再配送・ルート変更の防止、運賃	自律型スポット運賃交渉とSLA監視の統

		交渉の最適化。	合。
製造・サプライチェーン	保証コストの不適切な負担(サプライヤー回収漏れ) <sup>7</sup>	責任所在の自動特定によるワランティ回収率の向上(20%～)。	多段階サプライヤー間の品質データ連携と責任Chapterの同期。
金融・フィンテック	規制当局(EU AI法等)への適合コストと法的リスク <sup>20</sup>	コンプライアンス費用20%削減、罰金リスクの回避。	自律型ローン審査・トレーディングの監査証跡管理。
AIソフトウェア開発	AIエージェントの商用化失敗率(73%)の改善 <sup>1</sup>	開発サイクルの安定化、運用保守コストの低減。	エージェント間のメッセージングにおける責任境界(Chapter)の定義。

## 4.2 具体的なユースケース: 自律型物流リカバリーシステム

物流業界における「セルフヒーリング(自己修復型)配送網」を例にとる。

1. **Chapter**の設定: 「北米東海岸ルート配送」という章を定義。前提条件に「運賃上限: \$2.5/mile」「納期: 48時間以内」を設定。責任者を「運行管理者A」とする。
2. **Δ**の検知: 港湾ストライキが発生。AIエージェントが代替ルートを計算するが、運賃が\$3.8/mile(前提条件の50%増)になることを検知。これが「Δ」となる。
3. アクションの選択:
  - **Defer**(上位移送): システムは自動で判断せず、運行管理者Aの画面に「予算オーバーだが納期を守るか」の選択肢を表示。
  - **Reframe**(構造再定義): ストライキが長期化する場合、管理者Aは「運賃上限」の前提条件を一時的に引き上げることで、システムの稼働を継続させる。
4. 結果: 責任が曖昧なまま高額な運賃を支払い続ける「漂流」を防ぎつつ、人間の迅速な判断をシステムに組み込むことができる。

## 4.3 商用化ロードマップ: 3つのフェーズ

VCDesignを市場に浸透させるための戦略的ステップは以下の通りである。

### フェーズ1: ガバナンス・コンサルティングと「責任可視化ツール」の提供(1~2年目)

AIエージェントの導入に不安を抱える企業に対し、現在のシステムの「責任の空白地帯」を特定するアセスメントを実施する。VCDesignの「Chapter」概念を用いたシステム・アーキテクチャ設計図の作成を支援し、自律型システムの導入成功率を高める。ここでは、Gartnerが予測する10億ドル規模のAIガバナンス市場をターゲットとする<sup>22</sup>。

## フェーズ2:「VC-OS」プラットフォームの展開(3~5年目)

設計思想をソフトウェア化した「VCDesign SDK / Runtime」をリリースする。開発者がエージェントを構築する際、ライブラリとして「Chapter」や「Δ検知ロジック」を簡単に組み込めるようにする。既存のSalesforce (Agentforce) やSAPなどのエンタープライズ・プラットフォームと連携し、それらの上で動くAIの「責任制御レイヤー」としてデファクトスタンダード化を狙う<sup>4</sup>。

## フェーズ3:産業別「バリュー・コンティニュティ・ネットワーク」の構築(5年目以降)

企業単体ではなく、サプライチェーン全体でVCDesignを共有する。例えば、自動車メーカーと部品メーカーが共通の「Chapter」プロトコルを使用することで、不具合発生時の責任特定をミリ秒単位で行えるようにする。これは、100年続く産業インフラとしての「信頼の基盤 (Infrastructure of Trust)」となる。

# 第五章:結論:100年続く産業システムのための哲学

VCDesignは、単なる技術的なフレームワークではなく、人間とテクノロジーの新しい「共生契約」である。AIが「自律性」という魔力を持つ時代において、人間がその主導権を維持し続ける唯一の方法は、責任を「放棄」するのではなく、責任を「設計」することにある。

「Δ(ズレ)」をシステムの失敗として隠蔽するのではなく、進化のトリガーとして祝福する。

「AIに責任を負わせる」という幻想を捨て、人間が「最終判断者」であることをシステム構造に明示する。

「章(Chapter)」という最小単位を積み重ねることで、巨大で複雑なシステムの中に、いつでも人間が立ち戻れる「拠り所」を作り出す。

これらのVCDesignの原則は、現在のエンタープライズITが抱える「説明不能な恐怖」を「管理可能なリスク」へと変容させる力を持っている。10.9MDドルに及ぶデジタル・アドプションの損失、4.4MDドルに達するAIRISKの代償、そしてサプライチェーンで繰り返される不毛な責任転嫁。これらを解消した先にあるのは、真に「価値が継続する」産業社会の姿である。VCDesignは、その未来を構築するための、文字通りの「次世代OS」となるだろう。

## 引用文献

1. AI Agent Governance Crisis: 73% of Enterprise AI Fails - Artificio's AI, 4月 1, 2026 にアクセス、<https://artificio.ai/blog/ai-agent-governance-crisis>
2. McKinsey on Deploying Agentic AI with Safety and Security - Workato, 4月 1, 2026 にアクセス、<https://www.workato.com/the-connector/agentic-ai-security-mckinsey/>
3. AI System Failures: Why Autonomous Systems Drift Until They Break, 4月 1, 2026にアクセス、<https://www.rack2cloud.com/autonomous-systems-drift/>
4. 4 Ways Salesforce Customers Risk Losing Millions Because of AI ..., 4月 1, 2026にアクセス、<https://www.salesforceben.com/4-ways-salesforce-customers-risk-losing-million>

- [s-because-of-ai-agents/](#)
5. Whatfix-Commissioned Study Finds Enterprises Stand to Lose \$10.9M Annually Due to Poor Digital Adoption - PR Newswire, 4月 1, 2026にアクセス、  
<https://www.prnewswire.com/news-releases/whatfix-commissioned-study-finds-enterprises-stand-to-lose-10-9m-annually-due-to-poor-digital-adoption-302729418.html>
  6. Meeting AI Compliance Requirements: The Definitive Guide - Mirantis, 4月 1, 2026にアクセス、  
<https://www.mirantis.com/blog/ai-compliance-requirements-the-definitive-guide/>
  7. U.S. Auto OEM & Supplier Warranty Update:, 4月 1, 2026にアクセス、  
<https://www.warrantyweek.com/archive/ww20231214.html>
  8. Incoterms Risk Management: Avoid Costly Shipping Surprises - The Cooperative blog -, 4月 1, 2026にアクセス、  
<https://blog.thecooperativelogisticsnetwork.com/2026/01/26/how-forwarders-help-shippers-avoid-costly-surprises-through-incoterms-risk-management/>
  9. The Risk-based Responsibility for Algorithmic Failures - ResearchGate, 4月 1, 2026にアクセス、  
[https://www.researchgate.net/publication/401658532\\_The\\_Risk-based\\_Responsibility\\_for\\_Algorithmic\\_Failures](https://www.researchgate.net/publication/401658532_The_Risk-based_Responsibility_for_Algorithmic_Failures)
  10. Anna Beckers\* and Gunther Teubner\*\* 25 YALE ... - Yale Law School, 4月 1, 2026にアクセス、  
[https://law.yale.edu/sites/default/files/area/center/isp/documents/beckers\\_teubner\\_-\\_reponsibility\\_for\\_algorithmic\\_misconduct.76.pdf](https://law.yale.edu/sites/default/files/area/center/isp/documents/beckers_teubner_-_reponsibility_for_algorithmic_misconduct.76.pdf)
  11. Responsibility Gaps and Black Box Healthcare AI: Shared Responsibilization as a Solution - PMC, 4月 1, 2026にアクセス、  
<https://pmc.ncbi.nlm.nih.gov/articles/PMC11003475/>
  12. ITIL 4 vs ITIL (Version 5): What Changed, What Stayed the Same, and What to Do Next, 4月 1, 2026にアクセス、  
<https://www.newhorizons.com/resources/blog/itil-4-vs-itil-version-5>
  13. Change Enablement – Change Management in ITIL 4 - ITSM.tools, 4月 1, 2026にアクセス、  
<https://itsm.tools/change-enablement/>
  14. ITIL Change Management: Types, Benefits, and Challenges, 4月 1, 2026にアクセス、  
<https://www.itil.org.uk/blog/what-is-itil-change-management>
  15. Why AI Agents Break: A Field Analysis of Production Failures - Arize AI, 4月 1, 2026にアクセス、  
<https://arize.com/blog/common-ai-agent-failures/>
  16. When AI Agents Conflict: Logistics Governance - Debales AI, 4月 1, 2026にアクセス、  
<https://debales.ai/blog/ai-agent-governance-logistics-fix>
  17. NIST vs ISO - Compare AI Frameworks - ModelOp, 4月 1, 2026にアクセス、  
<https://www.modelop.com/ai-governance/ai-regulations-standards/nist-vs-iso>
  18. NIST AI RMF vs. ISO 42001: Comparing Frameworks for AI Privacy and Security | Maro, 4月 1, 2026にアクセス、  
<https://seekmaro.com/blog/nist-ai-rmf-vs-iso-42001>
  19. IISO 42001 vs NIST AI RMF: How to Choose the Right Framework - Hicomply, 4月 1, 2026にアクセス、  
<https://www.hicomply.com/blog/iso-42001-vs-nist-ai-rmf>

20. ISO 42001 vs NIST AI RMF - ISMS.online, 4月 1, 2026にアクセス、  
<https://www.isms.online/iso-42001/vs-nist-ai-rmf/>
21. Global AI Regulations Fuel Billion-Dollar Market for AI Governance Platforms - Gartner, 4月 1, 2026にアクセス、  
<https://www.gartner.com/en/newsroom/press-releases/2026-02-17-gartner-global-ai-regulations-fuel-billion-dollar-market-for-ai-governance-platforms>
22. AI Governance Market | Size, Share, Growth | 2025 - 2030, 4月 1, 2026にアクセス、  
<https://virtuemarketresearch.com/report/ai-governance-market>
23. Gartner: '\$1 Billion AI Governance Market as Global Regulations Expand' - Rockingrobots, 4月 1, 2026にアクセス、  
<https://www.rockingrobots.com/gartner-1-billion-ai-governance-market-as-global-regulations-expand/>
24. AI and tech investment ROI | Deloitte Insights, 4月 1, 2026にアクセス、  
<https://www.deloitte.com/us/en/insights/topics/digital-transformation/ai-tech-investment-roi.html>