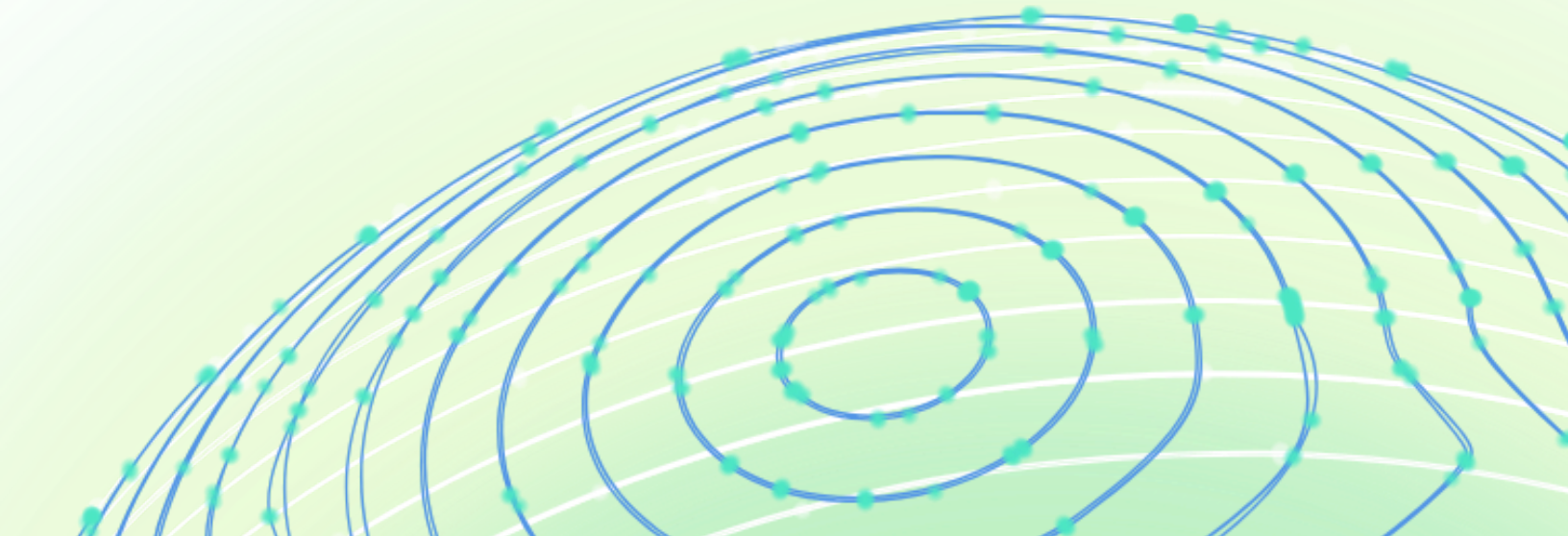
「いつの間にか」AIの
リスク実態調査

～シャドーAI等の管理と捕捉
課題とプラクティス～

一般社団法人AIガバナンス協会
2026年01月29日



はじめに

AI技術の急速な普及と進化は、企業・組織にとって、シャドーAI（シャドーIT）という管理部門が関知しないところで導入・利用されるAIという新たな火種をもたらした。自社やグループ内に潜むAIをいかに捕捉し、「リスクの芽」を摘むか。昨今のAIガバナンスにおける最も切実な課題の一つといえる。

本稿は、こうした問題意識のもと、一般社団法人AIガバナンス協会（以下「AIGA」）の会員企業を対象に実施した調査（以下「本調査」）に基づくものだ。各社・グループのAI利用状況や管理手法について、定量・定性の両面から分析を試みた。

本調査を通じて浮き彫りになったのは、企業が意図して導入したAIではなく、ガバナンスの網の目をすり抜けて「いつの間にか」流入してくるAIの存在だ。既存システムへのAI機能の追加、従業員の個人利用、そして外部パートナーをはじめとするサプライチェーン経由での侵入。さらに、企業がガバナンスを追求すればするほど、AIを管理しきれない「網の目」が可視化されるという「逆説的」状況も明らかになった。

本稿は、企業内に「いつの間にか」AIが入り込んでいる実態を可視化し、そこにある課題と実践的な解決策を提示したい。多くの悩める企業にとって、AIの活用の促進とガバナンスの高度化の両立に向けた手がかりとなるはずだ。

本調査結果は、日本企業全体の平均値を示すものではない。むしろ、国内で最もAI利活用とリスク管理に真剣に取り組む「先行企業群」が直面している「未来の課題」として捉えるべきである。統計的な有意差以上に、本調査が浮き彫りにした「AIガバナンスのパラドックス」や「現場の創意工夫」といったインサイトこそが、今後の政策や実務において重要な示唆を与えるものと考える。

第1. 本調査について

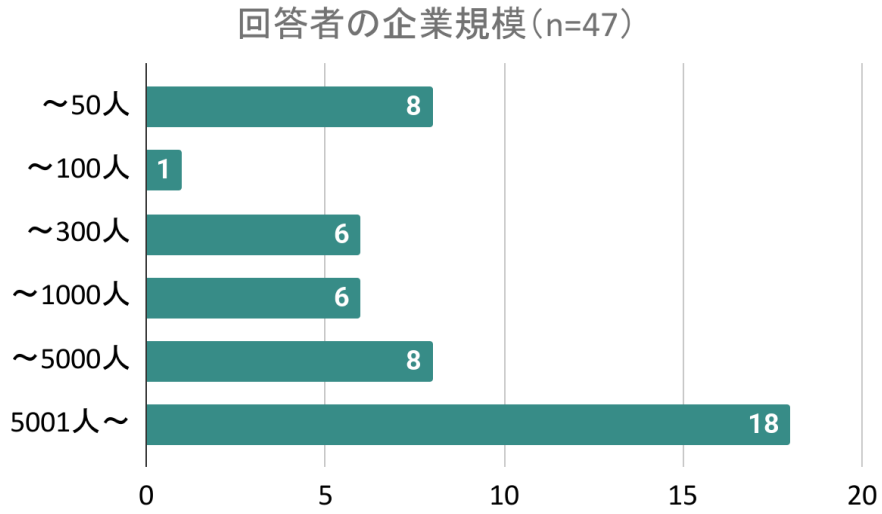
1. 本調査の概要[1]

- 調査期間：2025年8月12日 ～ 同9月10日
- 調査対象：AIGA会員企業 115社
- 有効回答数：47社
- 調査方法：オンラインアンケート形式
- 設問構成：全27問（選択式および自由記述）

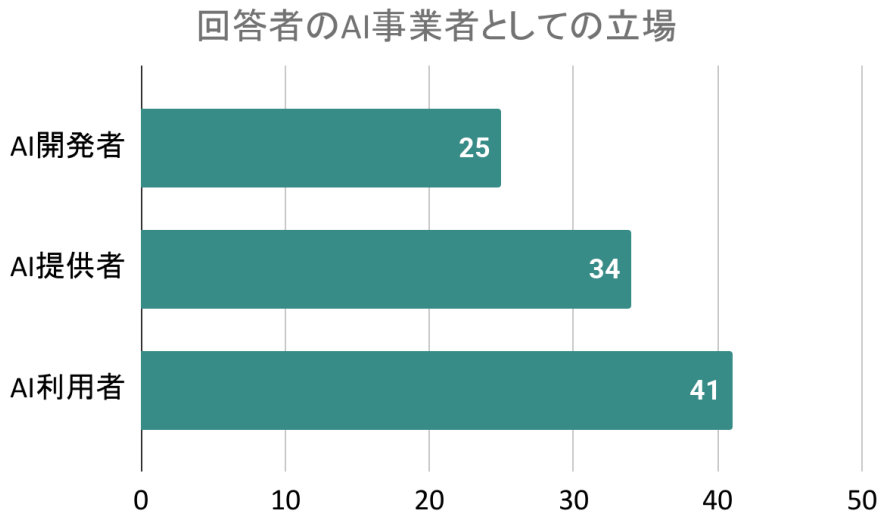
2. 回答企業の属性：多様な規模と立場

スタートアップから従業員5000人超の大企業まで幅広い層が回答した。特に、「AI利用者」に留まらず、開発・提供も行う複合的な立場の回答企業が多い点が特徴である。

- 企業規模：従業員数**5001**人以上の大企業が約**38%**（**18**社）と最多。次いで50人以下（8社）、100人以下（1社）、300人以下（6社）、1000人以下（6社）、5000人以下（8社）。
- 業種：IT・通信、保険・証券・銀行などの金融、製造など
- **AI**事業者としての立場（複数選択可）[2]：AI利用者87%（41社）、AI提供者72%（34社）、AI開発者53%（25社）



[1] 本調査で示される数値の差異や特徴は、実務上の傾向や課題を推察するためのインサイトを得ることを目的とし、統計的に有意な相関関係や、項目間の因果関係を証明するものではない。
[2] 「AI事業者ガイドライン」区分に準拠。



3. 本調査結果の解釈における留意点

- 回答企業は、AIGA会員の中でも「AIガバナンスナビ[3]」等を活用し、ガバナンス成熟度が比較的高い層が含まれている可能性がある。したがって、本調査結果は日本企業全体の平均的な実態というよりは、ガバナンスへの意識が高い企業においてさえ直面している課題として捉えるべきである。

- 本稿におけるインサイトは、アンケートの集計結果および回答企業への個別インタビューのエッセンスに基づいている。示される数値の差異や特徴は、実務上の傾向や課題を推察することを目的としたものであり、統計的に有意な相関関係や、項目間の厳密な因果関係を証明するものではない[4]。

[3] AIガバナンスナビver1.0については、AIGAのHPにおいて詳細が公開されている。
https://www.ai-governance.jp/blog-articles/aigovernance-navi-1-0
[4] なお、回答の一部には、企業側が現場の裁量を重視し、把握の対象外とする運用事例が含まれるが、その割合は限定的であり、調査全体の主要な傾向を左右するものではない。したがって、全体の把握状況を概観する目的から、これらも「把握に課題」（把握漏れ・未着手）の範疇に含めて整理を行った。

第2. 調査結果の詳細

本章では、AIが自社に流入する**6**つの経路を想定し、企業が、社内で利用されているAIツール・サービスについての把握・管理の認識状況を報告する。

全体傾向として、自社が主導する領域は管理が機能している一方、外部要因・個人裁量の領域に死角があることが浮き彫りとなった。

【共通設問】

貴社単体において、現在利用されているAIツール・サービス（生成AI含む）の「導入経路」をどの程度把握できていると考えますか？それぞれの導入経路について、最も近い状況をお選びください。

【選択肢】

- 全て把握できている（一切利用していないことを確認している場合も含む）
- 一部把握できていないものがある
- 把握の努力はしているが、ほとんど把握できていない
- 把握自体行っていない

【6つの導入経路】

- 独自開発・内製AI
- 外部からの調達AI
- オープンソースAI
- 既存システムへの組み込み・アップデートAI
- 外部パートナーにおけるAI利用
- 従業員の個人利用AI

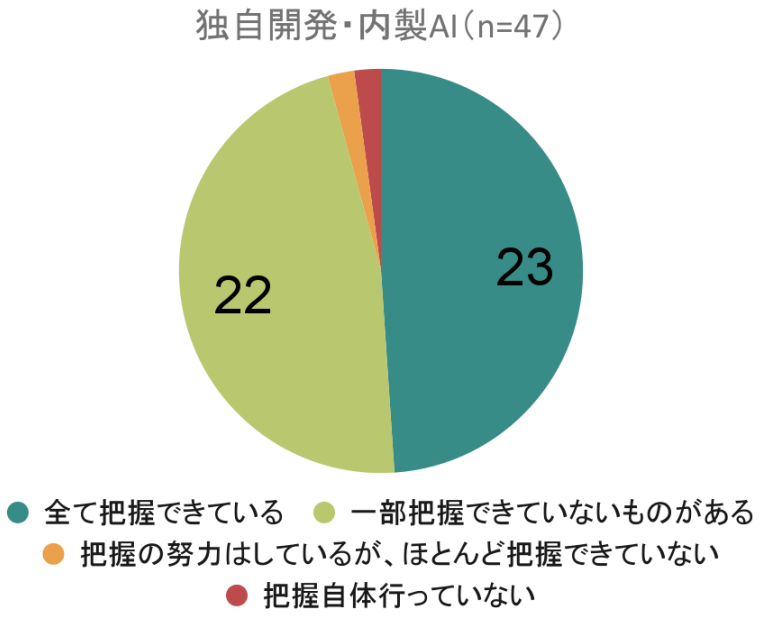
1. 管理の目が比較的行き届いている領域（自社主導型）

（1）独自開発・内製AI：約半数が「完全に把握」、予算管理が奏功

【設問スコープ】
　独自開発・内製AI（貴社内で企画・開発・導入し、利用しているAI。ゼロベースの開発だけでなく、モデル・サービスを、自社でカスタマイズやファインチューニングを行なって利用している場合も明示的に含む）

【結果】
- 「全て把握できている」**49%（23社）**
- 「一部把握できていない」**47%（22社）**
- 「ほとんど把握できていない」2%（1社）
- 「把握自体行っていない」2%（1社）

【インサイト】
　開発プロジェクトとして予算やリソースが紐づくことが背景にあると考えられ、管理部門の目が比較的行き届きやすい領域であることが伺えた。
　一方、一部の把握に課題認識（把握漏れ・未着手）のある企業からは「ある程度開発者の裁量に任せている」「部門によって体制の理解度・浸透に差異がある」といった要因が挙げられた。

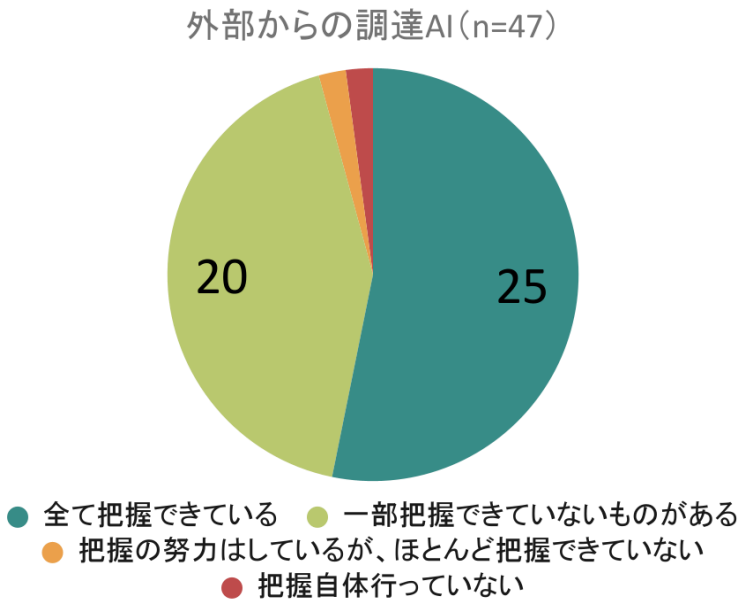


（2）外部からの調達AI：契約を通じて過半数を捕捉

【設問スコープ】
　外部からの調達AI（貴社が外部ベンダーから購入・契約し、直接利用しているAIツールやサービス）例：ChatGPT EnterpriseのようなSaaS型AIサービス、特定のAI機能を持つパッケージソフトウェア、AI連携APIサービスなど

【結果】
- 「全て把握できている」**53%（25社）**
- 「一部把握できていない」**43%（20社）**
- 「ほとんど把握できていない」2%（1社）
- 「把握自体行っていない」2%（1社）

【インサイト】
　外部からの調達時に契約行為を伴うため、比較的、捕捉しやすいことがうかがえるが、全体の4割強が把握の課題（把握漏れ・未着手）を認識している。「各部門での個別契約」や翻訳ツールなどの「生成AIの隆盛以前から使用しているAIシステムは管理対象外」となっていることが要因として示唆された。

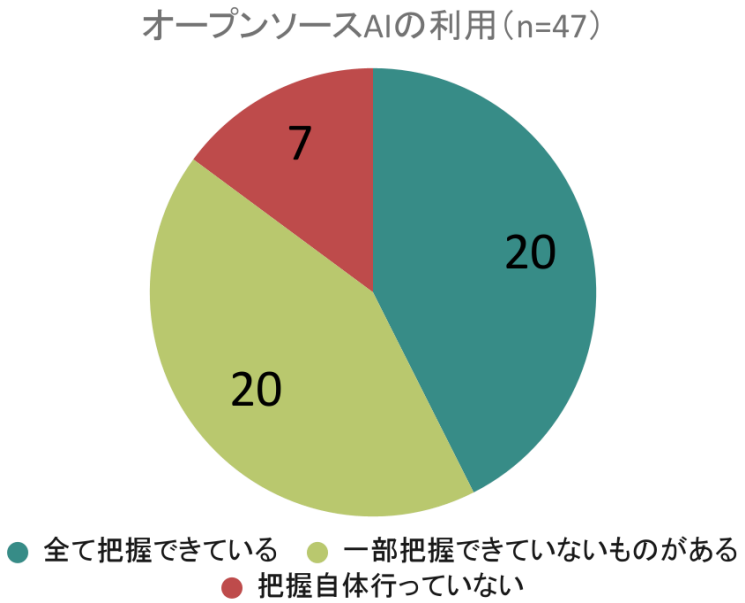


（3）オープンソースAI：6割で把握に課題、現場裁量に要因

【設問スコープ】
　オープンソースAIの利用（社内の開発者や研究者が公開されているAIモデルやライブラリを直接利用している場合）

【結果】
- 「全て把握できている」**43%（20社）**
- 「一部把握できていない」**43%（20社）**
- 「ほとんど把握できていない」0%（0社）
- 「把握自体行っていない」15%（7社）

【インサイト】
　一定の管理下にあることが伺えたが、独自開発・内製AI、外部からの調達AIの導入経路と比較して把握の程度はやや低下した。その要因として「明確なルールやガイドラインがない」「サンドボックス内での活用に限定させているためあえて把握していない」といった点が挙げられた。意図的に、あるいは結果的に、現場の裁量に委ねられている実態が見て取れた。



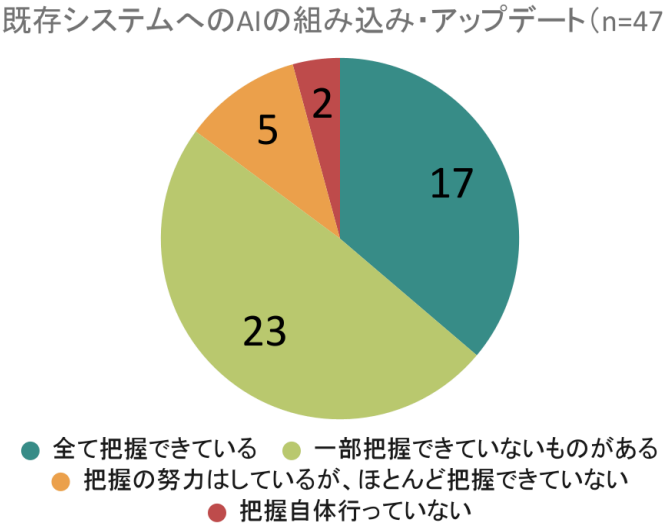
2.「いつの間にか」AIが流入し、課題となっている領域

（1）既存システムへの組み込み・アップデートAI：「いつの間にか」流入の典型

【設問スコープ】
既存システムへの組み込み・アップデート（貴社が利用する既存の業務システムやソフトウェアのアップデートで、AI機能が追加・利用可能になった場合）例：Microsoft 365のCopilot機能、Google WorkspaceのAI機能など

【結果】
- 「全て把握できている」**36%（17社）**
- 「一部把握できていない」**49%（23社）**
- 「ほとんど把握できていない」11%（5社）
- 「把握自体行っていない」4%（2社）

【インサイト】
既存システムへの組み込み・アップデートAIは、全体の64%が把握の課題（把握漏れ・未着手）を認識しており、最も社内に「いつの間にか」AIが流入している経路であるといえそうである。その背景として「（ベンダー側の）アップデート情報や利用規約変更の把握が追い付いていない」「特定の部門で使っているツールのAI機能追加までは追いきれていない」といった点が挙げられた。日常業務で利用しているシステムやグループウェアへのAI機能の追加（サイレントアップデート）は、既存の契約の延長線上にあるため、管理部門が気づかぬうちに全社的なAI利用が開始される恐れがあるといえる。情報漏洩などの予期せぬトラブルに発展するリスクが潜んでいる。



（**2**）外部パートナーにおける**AI**利用：約**9**割が管理不能、最も無防備な領域

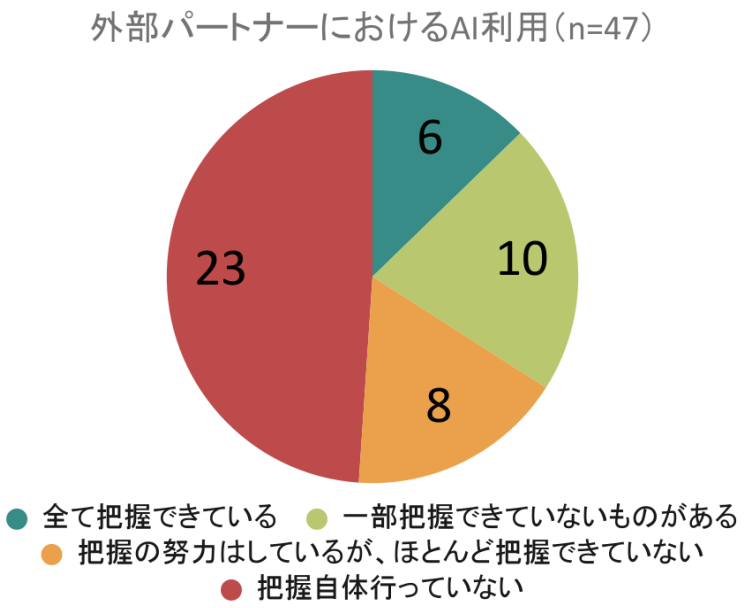
【設問スコープ】
外部パートナーにおけるAI利用（貴社が業務を委託・依頼している外部パートナー（業務委託先、代理店、販売パートナーなど）が、その業務遂行のためにAIを利用している場合）

【結果】
- 「全て把握できている」**13%**（**6**社）
- 「一部把握できていない」21%（10社）
- 「ほとんど把握できていない」17%（8社）
- 「把握自体行っていない」**49%**（**23**社）

【インサイト】
6つの導入経路において、最も課題が浮き彫りになった。実に9割近くの企業において、業務委託先などのサプライチェーン上におけるAI利用は、把握の課題（把握漏れ・未着手）が認識されている。その理由として、次のような声が寄せられた。

➔「（外部パートナーとの）契約にAI利用に関する記載がないため」
➔「成果物での評価をしており、外部パートナーへのAIガバナンスの定義が確立できていない」
➔「外部パートナーのAI利用状況を監視する体制がない」
➔「委託先の業務にまで口は出せない、縛れない」
➔「AI利用は申告ベースであり、外部パートナーが利用しているサービスについて『AIを利用している』と認識できるとは限らないため」

契約における縛りや監督体制などの未整備に苦悩している状況が伺われた。委託先経由でのデータ漏洩や権利侵害リスクに対して、無防備な状態といえる。



一方、一部の企業では以下のような「泥臭い」運用でカバーしようとする動きも見られた。

- ➔ 契約時のヒアリング：「外部パートナーとの契約時にどのようなAIを業務で利用しているか聞き取りを行っている」「定期的な報告会やヒアリングを通じて、AIの利用状況を確認している」
- ➔ ガイドラインの義務化：「AI利用に関するガイドラインを策定し、パートナーに遵守を義務付けている」
- ➔ **AI**ツールの指定：「当社が契約するシステム上のAIの利用をお願いしている」

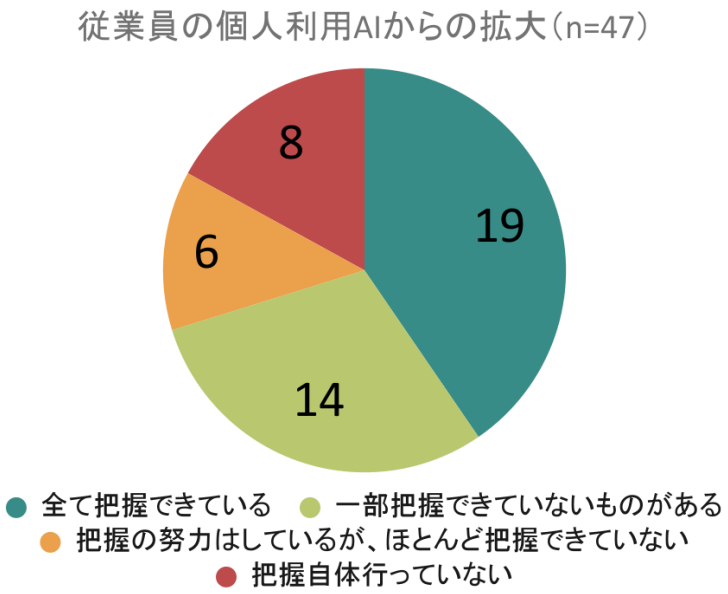
ガイドライン遵守への誓約や自己申告といった外部パートナーのリテラシーに頼らざるを得ないが、AIリスクの顕在化を防止するうえで一定の有効性があるといえそうである。

（3）従業員の個人利用AI：シャドーAIの検知困難、6割が把握に苦慮

【設問スコープ】
　従業員の個人利用からの拡大（従業員が個人の裁量で外部AIツールを試用し、それが業務利用に広まっている場合）

【結果】
- 「全て把握できている」**40%（19社）**
- 「一部把握できていない」**30%（14社）**
- 「ほとんど把握できていない」13%（6社）
- 「把握自体行っていない」17%（8社）

【インサイト】
　シャドーITの典型であるため、一定の目配りがされていることが伺えたが、約6割（28社）が把握の課題（把握漏れ・未着手）を認識している。
　その要因として「技術的に検知・ブロックする仕組みがない」「個人のメールアドレスでログインしているサービスなどは検知ができていない」「私有AIの利用制限ルールは設けているが、ルール不履行状況を確認・モニタリングする体制がない」「無料で使用可能なサービスは、申請されない可能性がある」「会社支給・管理のアセット以外の個人パソコン、スマホに関しては管理はできない」といった点があげられた。
「禁止」ルールを設けても、物理的な遮断が難しく、私用デバイス経由での利用などは「検知不能」である。個人のモラル・性善説に依存せざるを得ず、セキュリティ上の脅威となっていることが伺える。



3. AIツール・サービス管理体制の実態と課題感

本調査では、導入経路別の把握の認識に加え、企業が実際にどのような管理体制（プラクティス）を構築し、運用上の課題を感じているのかについても尋ねた。調査結果からは、制度の整備は進んでいるものの、実効的な運用に苦慮する企業の姿が浮き彫りになった。

（1）社内利用のAIの管理・捕捉の状況：約半数が「専用レジストリ」で管理

【設問スコープ】
貴社単体において、社内で利用されているAIツール・サービス（生成AI含む）の管理・捕捉について、最も近い状況をお選びください[5]。

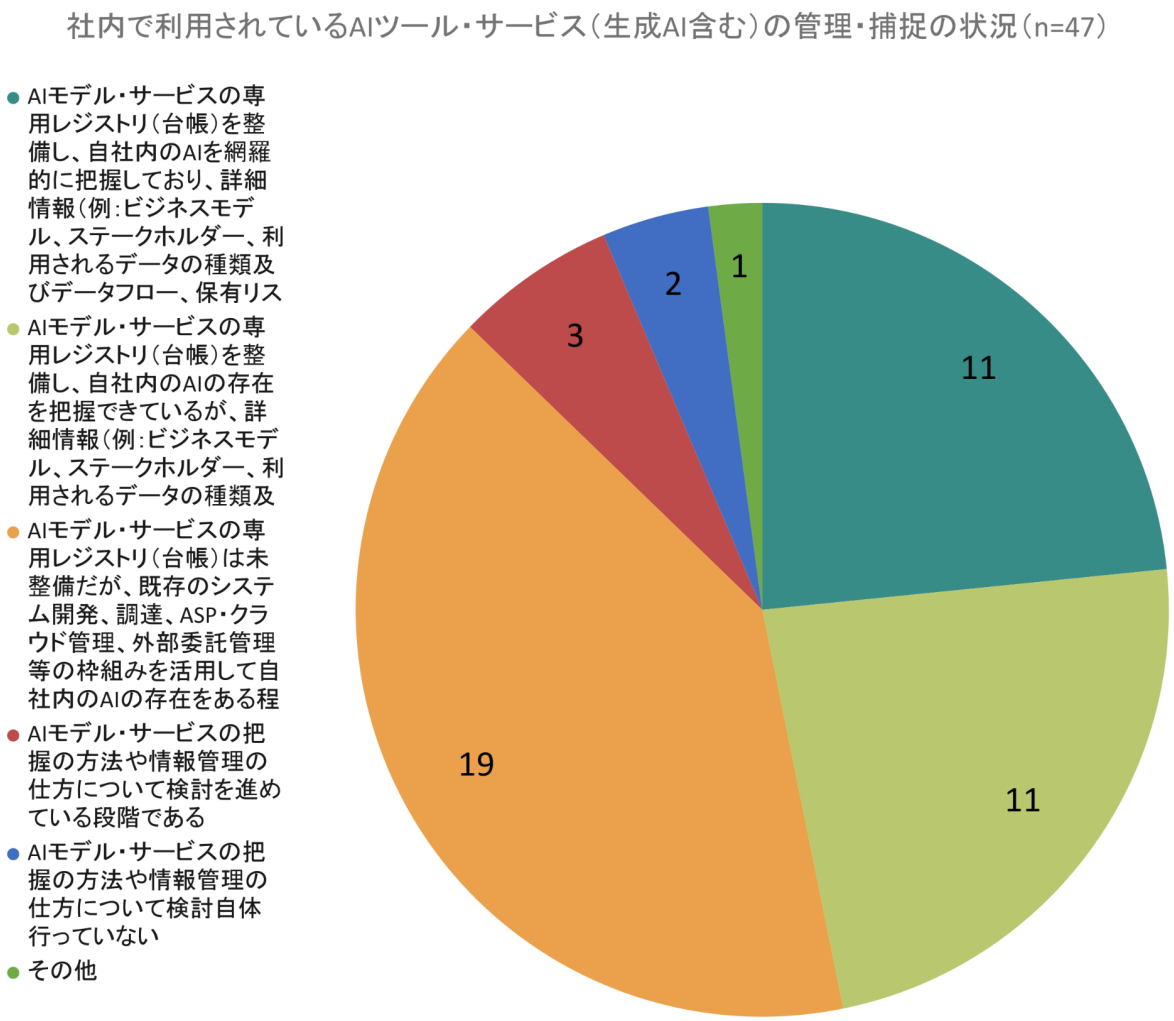
【結果】

- AIモデル・サービスの専用レジストリ（台帳）を整備し、自社内のAIを網羅的に把握しており、詳細情報（例：ビジネスモデル、ステークホルダー、利用されるデータの種類及びデータフロー、保有リスク及びその対策、リリース時点のアルゴリズム・学習済モデルのバージョンなど）まで統一的なフォーマットで管理している **23.4%（11社）**
- AIモデル・サービスの専用レジストリ（台帳）を整備し、自社内のAIの存在を把握できているが、詳細情報（例：ビジネスモデル、ステークホルダー、利用されるデータの種類及びデータフロー、保有リスク及びその対策、リリース時点のアルゴリズム・学習済モデルのバージョンなど）は部門・部署が個別フォーマットで管理している **23.4%（11社）**
- **AI**モデル・サービスの専用レジストリ（台帳）は未整備だが、既存のシステム開発、調達、**ASP**・クラウド管理、外部委託管理等の枠組みを活用して自社内の**AI**の存在をある程度は把握できている **40.4%（19社）**
- AIモデル・サービスの把握の方法や情報管理の仕方について検討を進めている段階である **6.4%（3社）**
- AIモデル・サービスの把握の方法や情報管理の仕方について検討自体行っていない **4.3%（2社）**
- その他（自由記述） **2.1%（1社）**

【インサイト】
全体の約半数（47%）がAI専用の管理台帳を有しているほか、既存の管理の延長線上でAIを捕捉しようと試みている企業も多いことがわかった。AIGA会員企業という回答者の特性上、AIガバナンスへの意識は高く、基盤が整備が進んでいるといえる。ただし、詳細情報まで統一

[5] 本設問の設計にあたっては、AIGAが提供するAIガバナンスの自己診断「AIガバナンスナビver1.0」における成熟度評価を参考にした。

フォーマットで管理できている企業と、部門任せの企業で濃淡があることもうかがえた。



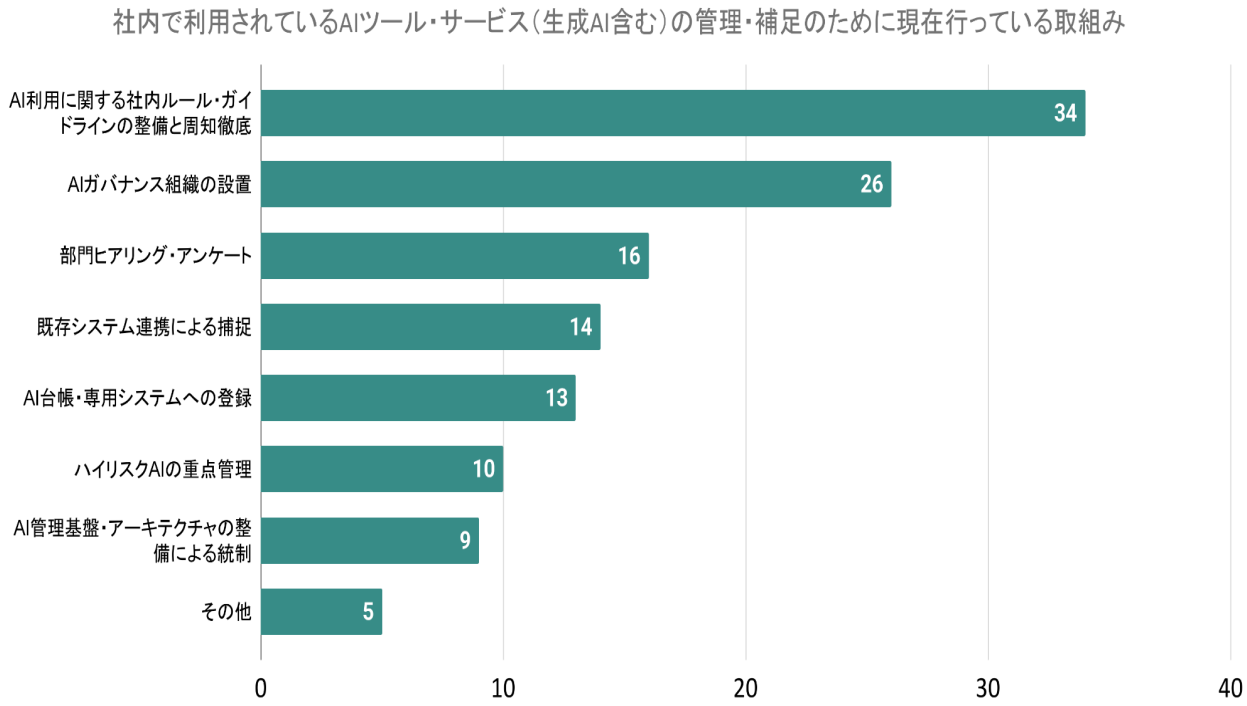
（**2**）現在の具体的な取り組み：ルール作りは先行、監視体制は道半ば

【設問スコープ】
　貴社単体において、社内で利用されているAIツール・サービス（生成AI含む）の管理・捕捉のために、現在どのような取り組みを行っていますか？当てはまるものを全てお選びください（複数選択可）

【結果】

- **AI**利用に関する社内ルール・ガイドラインの整備と周知徹底 **72.3%**（**34**社）：AI導入時の把握・管理をプロセスとして含む社内ルール・ガイドラインを既に整備し、従業員に周知徹底している
- **AI**ガバナンス組織の設置 **55.3%**（**26**社）：AIガバナンスを主管する部門（AIガバナンス組織、CoEなど）を設置し、AI利用の申請・審議プロセスや相談窓口を設けている
- 部門ヒアリング・アンケート **34%**（**16**社）：定期的に各部門へのヒアリングやアンケートを実施し、利用状況を把握している
- 既存システム連携による捕捉 **29.8%**（**14**社）：既存のIT資産管理・システム開発・調達管理ツール等（プロジェクト管理ツールなど）を活用し、AIツール・サービスも網羅的に捕捉できている
- **AI**台帳・専用システムへの登録 **27.7%**（**13**社）：AI台帳や専用のシステムを整備し、網羅的な登録・管理を行っている
- ハイリスク**AI**の重点管理 **21.3%**（**10**社）：ハイリスクなAI活用と判断されたAIのみを重点的な把握・管理の対象としている（例：モデルカードの作成・保存、詳細なリスク評価）
- **AI**管理基盤・アーキテクチャの整備による統制 **19.1%**（**9**社）：社内のAIは全て共通の基盤となるシステム上で開発・運用することを必須としている（注：共通の基盤とは、AIの開発から運用までを統一的に管理・統制するためのインフラやプラットフォームを指します）
- その他（自由記述）**10.6%**（**5**社）

【インサイト】
「AI利用に関する社内ルール・ガイドラインの整備と周知徹底」で72%（34社）、「AIガバナンス組織の設置」が55%（26社）と、制度設計や組織作りは進んでいることが伺えた。一方で、現場の実態を継続的にモニタリングする実効的なアクション（例えば部門ヒアリング等）は多くの企業が未だ試行錯誤の段階にあることを示唆している。



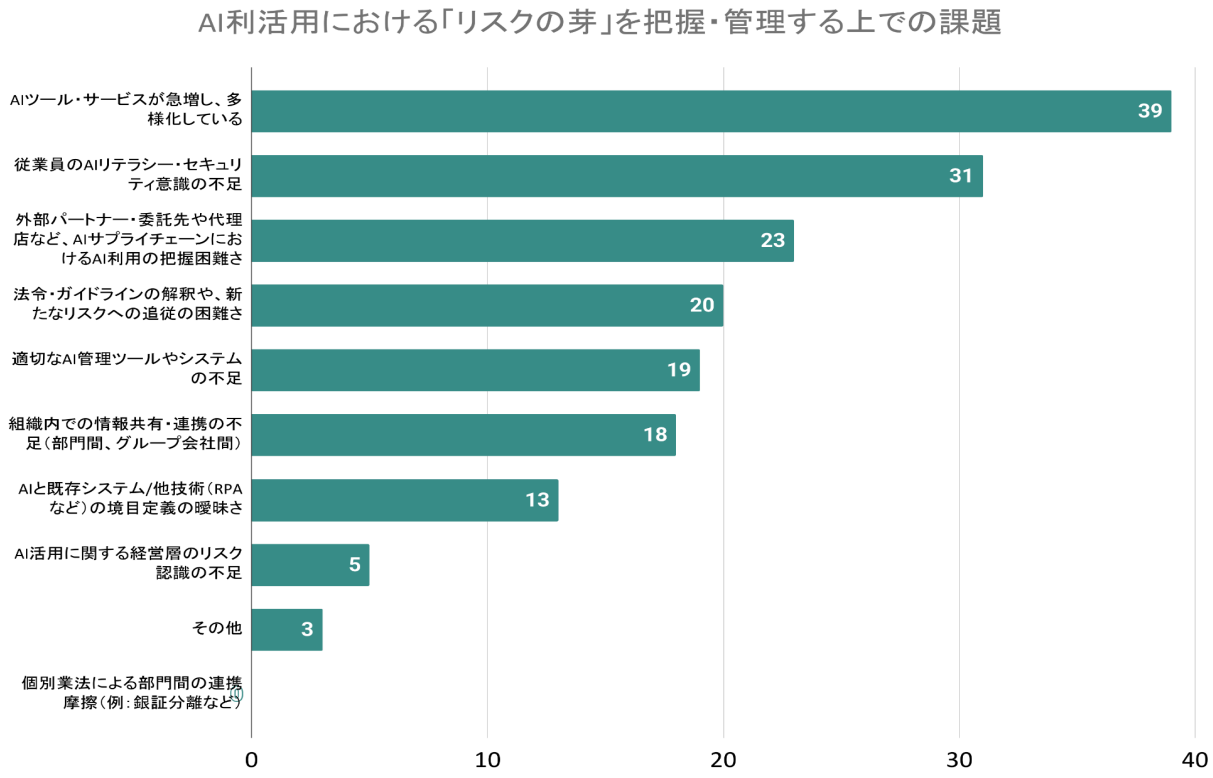
（3）「リスクの芽」を捉える上での課題：**AI**の爆発的増加とリテラシー不足

【設問スコープ】
AI利活用における「リスクの芽」を把握・管理する上で、貴社（貴社グループ）が特に課題と感じる点は何ですか？（複数選択可）

【結果】

- **AI**ツール・サービスが急増し、多様化している **83%**（**39**社）
- 従業員の**AI**リテラシー・セキュリティ意識の不足 **66%**（**31**社）
- 外部パートナー・委託先や代理店など、**AI**サプライチェーンにおける**AI**利用の把握困難さ **48.9%**（**23**社）
- 法令・ガイドラインの解釈や、新たなリスクへの追従の困難さ 42.6%（20社）
- 適切なAI管理ツールやシステムの不足 40.4%（19社）
- 組織内での情報共有・連携の不足（部門間、グループ会社間） 38.3%（18社）
- AIと既存システム/他技術（RPAなど）の境目定義の曖昧さ 27.7%（13社）
- AI活用に関する経営層のリスク認識の不足 10.6%（5社）
- 個別業法による部門間の連携摩擦（例：銀証分離など） 0%（0社）
- その他（自由記述） 6.4%（3社）

【インサイト】
　現在のAIの管理の本質的な困難さは、「技術的な進化スピード（ツールの急増・多様化）」と「人的・組織的な統制の難しさ（リテラシー不足）」という二つの要因が掛け合わさる点にあることが伺える。制度や組織といった静的ガバナンス基盤は整備されつつあるが、日々爆発的に増殖するAIツールや、従業員の利用実態という「動的」な要因に対し、従来のトップダウン型の管理アプローチでは追いつかないことへの危機感が浮き彫りになった。



4. グループ全体におけるガバナンスの実態

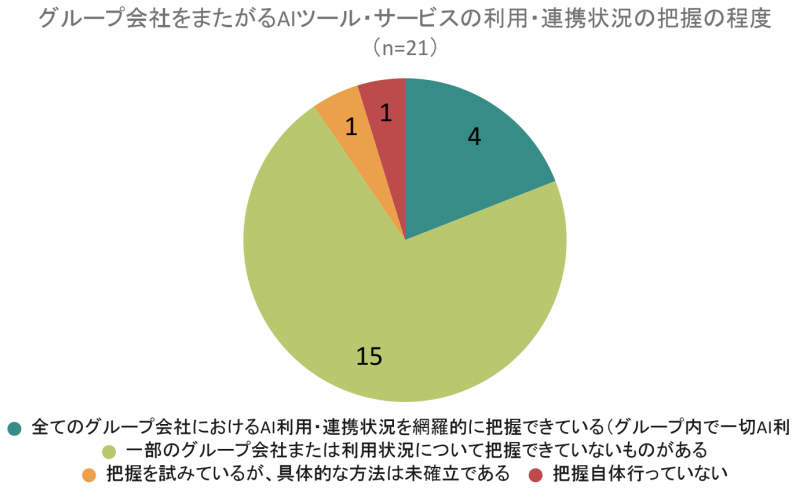
自社が持株会社（ホールディングス）およびグループ本社機能を持つ企業であると回答した企業（21社）を対象に、グループ会社をまたがるAI利用の把握状況と管理体制について調査したところ、企業単体以上に、AIの管理・捕捉の難易度が跳ね上がることが確認された。

（1）把握状況：グループ統制、8割が課題感　単体以上に高い壁

【設問スコープ】
貴社グループ全体において、グループ会社をまたがるAIツール・サービスの利用・連携状況をどの程度把握していますか？

【結果】
- 全てのグループ会社におけるAI利用・連携状況を網羅的に把握できている（グループ内で一切AI利用がないことを確認している場合を含む）19%（4社）
- 一部のグループ会社または利用状況について把握できていないものがある **71%（15社）**
- 把握を試みているが、具体的な方法は未確立である 5%（1社）
- 把握自体行っていない 5%（1社）

【インサイト】
「全てのグループ会社におけるAI利用・連携状況を網羅的に把握できている」と回答した企業はわずか19%（4社）に留まった。多くの企業において、子会社や関連会社のAI利用実態までは目が届いていない状態にある可能性が伺える。

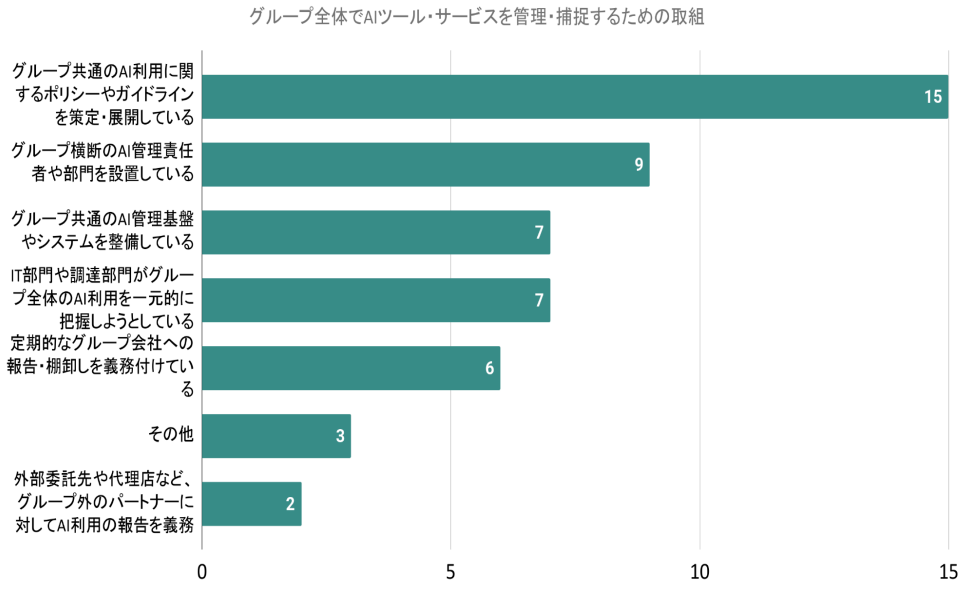


（2）グループ統制の具体的なアプローチ：ポリシー策定にとどまる

【設問スコープ】
　貴社グループ全体でAIツール・サービスを管理・捕捉するために、どのような取り組みを行っていますか？（複数選択可）

【結果】
- グループ共通の**AI**利用に関するポリシーやガイドラインを策定・展開している **71%（15社）**
- グループ横断の**AI**管理責任者や部門を設置している **43%（9社）**
- グループ共通のAI管理基盤やシステムを整備している　33%（7社）
- IT部門や調達部門がグループ全体のAI利用を一元的に把握しようとしている 33%（7社）
- 定期的なグループ会社への報告・棚卸しを義務付けている 29%（6社）
- 外部委託先や代理店など、グループ外のパートナーに対してAI利用の報告を義務付けている 10%（2社）
- その他（自由記述） 14%（3社）

【インサイト】
　単体同様、ルールの制定は先行しているが、それを実効あらしめるための「組織体制」や「技術的基盤」の整備は道半ばであることが伺える。グループガバナンスにおいては、各社の独立性や事業特性の違いも相まって、単体以上にガバナンスを効かせていく難易度の高さが浮き彫りになった。



第3. AIガバナンスのパラドックス

前章までのデータは、多くの企業が自社やグループ内に流入するAIツール・サービスを把握できていないという現実を明らかにした。一見すると、これはガバナンス不全を示すネガティブな結果のように映るかもしれない。しかし、データを深く読み解くと、そこには「ガバナンスを真剣に実践すればするほど、自分たちの死角に気づかされる」という逆説的な実態が浮かび上がってきた。

本章では、データが語る「パラドックス」の正体に迫る。

1. 大企業ほど流入するAIが「見えていない」？

一般的に、大企業ほど管理体制が整備され、AIの管理・捕捉にあてられる予算や人的リソースも潤沢であると考えられる。しかし、企業規模別に把握の認識を集計した結果は、その予想を覆すものであった。

【企業規模（従業員数）別にみる「全て把握できている」と回答した割合】

- 「独自開発・内製AI」
    - **50**人以下：**87.5%**（**7**社／**8**社）
    - 300人以下：60%（3社／5社）
    - **5001**人以上：**44.4%**（**8**社／**18**社）
- 「オープンソースAI（OSS）
    - **50**人以下：**75.0%**（**6**社／**8**社）
    - 300人以下：66.7%（4社／6社）
    - **5001**人以上：**27.8%**（**5**社／**18**社）

上記の通り、企業規模が大きくなると「全て把握できている」の回答割合が低下する傾向が認められたが、これは「大企業のガバナンス力の不足」を示しているわけではないと考えられる。小規模組織では、開発者と管理者の距離が近く、「誰が何を使っているか」が自然と可視化されやすいが、大企業では、組織の複雑化に伴い、OSSのような導入ハードルの低い技術ほど、部門の自律性や縦割り構造の中で、管理の死角に入りやすいことが伺える。

大企業群にみられた回答傾向は、AIの急速な流入と広がりに対し、自社のガバナンスの限界という事実を、より正確かつ誠実に認識している結果であるといえよう。

2. ガバナンスを実践するほど「AI捕捉」が下がるメカニズム

さらに興味深いのは、「ガバナンスの優等生ほど、自信を失っている」とでもいえる現象である。本来であれば「ルールを整備」し、「専門組織」を作り、「ヒアリングを行っている」企業群ほど、AIについて「把握できている」と回答する傾向にあるはずである。しかし、ここでも「逆転現象」が映し出された。

【行動する企業ほど「課題」が見えている】

- 「部門ヒアリング・アンケート」実施率は把握に課題感のある企業群の方が高い
    - 外部からの調達AI
        - 「全て把握できている」群の実施率　28%（7社／25社）
        - 「一部把握できていない」群の実施率　45%（9社／20社）

- 「ルール・ガイドライン整備」の実施率は把握に課題感のある企業群の方が高い
    - 既存システムへの組み込み・アップデートAI
        - 「全て把握できている」群の実施率　23.5%（4社／17社）
        - 「一部把握できていない」群の実施率　47.8%（11社／23社）
    - 独自開発・内製AI
        - 「全て把握できている」群の実施率　69.6%（16社／23社）
        - 「一部把握できていない」群の実施率　77.3%（17社／22社）

- 「ガバナンス組織の設置」の実施率は把握に課題感のある企業群の方が高い
    - 独自開発・内製AI
        - 「全て把握できている」群の実施率　47.8%（11社／23社）
        - 「一部把握できていない」群の実施率　63.6%（14社／22社）

AIガバナンスの実践を努力している企業ほど、AIの把握に課題を感じている「AIガバナンスのパラドックス」ともいえる状況がなぜ生まれるのか。

それはガバナンス部門がヒアリングや台帳整備など地道なアクションを重ねることで、日々、想定外の利用実態やルールの隙間を突く現場の「工夫」を目の当たりにしているからではないだろうか。

ガバナンス部門の不断の努力が、結果的に「真実」を掘り起こしているのである。

3.「無知の知」が示すAIガバナンスの成熟

そして、把握に課題意識（把握漏れ・未着手）を抱えている企業群の中には、自社やグループ内に流入しているAIリスクを正しく認識できていない可能性がある。

【「全て把握」企業ほど、従業員のリテラシーに不安】

例えば「従業員の個人利用AI」において「全て把握できている」群（19社）は、課題として「従業員のAIリテラシー不足」をあげた割合が84.2%（16社／19社）に上るが、「一部把握できていない」群（14社）は50%（7社／14社）、「把握自体行っていない」群（8社）は37.5%（3社／8社）にとどまる。

「外部からの調達AI」においても「全て把握できている」群（25社）は「従業員のAIリテラシー不足」を課題として挙げた割合が68%（17社／25社）、「AIツール・サービスが急増し、多様化している」を課題として挙げた割合が88%（22社／25社）にのぼったが、「一部把握できていない」群は、それぞれ65%（13社／20社）と、75%（15社／20社）と「全て把握できている」群より

減少する傾向がみられた。

ガバナンス実践企業は、AIリスクを捕捉しようとする過程で「従業員のリテラシー不足」や「AIツールの急増・多様化」という事態を痛感し、「管理しようとすればするほど、管理できない領域の広さを思い知らされる」と現実に直面しているようだ。

したがって、本調査において示された把握の課題認識（把握漏れ・未着手）は、ただちに管理能力の欠如を示すものではなく、むしろ、ガバナンスが「形式」から「実効」へと進む過程で、自社のコントロールの限界を正しく認識できているという成熟の証左と捉えるべきである。逆に言えば「全て把握できている」と断言できる場合、その捕捉スコープが狭すぎる、あるいは楽観的すぎる可能性すら疑う必要がある。

4. 「完全管理」という幻想を捨てる時

この「AIガバナンスのパラドックス」が示す教訓は明確である。それは「全て把握し、管理する」というアプローチの危うさである。AI技術の進化と普及スピードは、既存の管理プロセスのキャパシティを超えているといえる。社会のあらゆる場所にAIが実装されていく中で、企業側が全てのAI利用を網羅的に把握しようとすれば、ガバナンス部門は疲弊し、ビジネススピードは失われ、結果として「把握できているつもり」という状態になり、形骸化に陥りかねない。

私たちは今、「捕捉しきれないAIがある」という事実を受け入れた上で、AIごとのリスクのグラデーションを見極めてリソースを配分する、新たなガバナンスのフェーズへと足を踏み出す時が来ているといえる。

次章以降は、本調査に寄せられた声や先行企業のケーススタディから、その具体的な解法を探る。

Column：AIヒヤリハット「リスクの芽」

本調査に寄せられたAI利活用において「リスクの芽を見過ごしかねない」と感じた「ヒヤリハット」の具体的な経験を、三つの典型的なシチュエーションに分類して提示する。

【設問スコープ】貴社（貴社グループ）で、AI（生成AI含む）の利活用において、「いつの間にかAIが導入・利用されており、リスクの芽を見過ごしかねない」と感じた具体的な状況や経験があれば、ご記載ください。 例：ある部門が、知らない間にSaaS利用規約のAI関連条項に同意していた／従業員が、禁止されているにもかかわらず、機密情報を外部AIに入力しているのを見かけた／システムアップデートで導入されたAI機能が、どのようなデータを利用しているか不明だった／業務委託先がAIを導入したが、契約上の確認が不十分だった／利用している既存のSaaSツール（例：Microsoft365, Google Workspaceなど）のアップデートでAI機能が追加されたが、その利用規約の変更点やリスクを十分に把握できていないまま利用が始まっている／AIと他のシステムの境目、AIとRPAなどの他技術の境目の定義が曖昧で、管理が難しい／銀証分離など個別業法による部門間の連携がAI利用で摩擦を生んでいる、など

Category 1：気づいた時には…

☛ 暴走した議事録ボット

「個人で試験的にPCにインストールしていたAIによる議事録作成アプリについて、取引先企業とのオンラインミーティングで使用する予定はなかったにもかかわらず、一度アプリをmeetやzoomに連携すると、全てのミーティングで使用され、かつ全ての出席者に通知がいく設定がデフォルトとなっていた。（中略）使用の承諾がない状況で、当該アプリによって議事録が作成され、その通知が全出席者になされていた。……取引先への説明に追われた」
【解説】悪意なき個人の「お試し」が、一瞬で全社の信用に火をつける。アプリのデフォルト設定という「地雷」は、足元に埋まっている。

☛ アップデートという名の**AI**強制実装

「利用している既存のSaaSツールのアップデートでAI機能が追加されたが、その利用等への重要なリスクを十分に把握できないまま利用が始まってしまった」「システムアップデートで導入されたAI機能が、どのようなデータを利用しているか不明だった」
【解説】昨日までの安全なツールが、今日から「企業の情報の吸い上げ口」に変わる。プラットフォーマーの仕様変更に対し、利用者側は無力である。

☛ 「議事録を見たいなら同意せよ」ボタン

「ある部門が導入した議事録作成SaaS AIが、Web会議参加者への議事録閲覧の権限付与＝SaaS利用同意という形態で提供されており、利用規約内容不明、アクセス可能者不明のまま利用が拡大していた」
【解説】「見たいなら同意せよ」－業務遂行を人質に取ったパターンに対し、現場は規約を読む暇もなく「Yes」を押してしまう。

Category 2：信じて任せた先で、何かが起きている…

☛ **SNS**で知った**AI**の無断使用

「業務委託先による生成AIの無断使用が、SNSなどを通じて発覚した。委託先は委託元に連絡なく生成AIを利用しており、委託元は外部からの指摘で初めてこの事態を認知した」
【解説】契約書にハンコをついても、外部パートナーのAI利用を制御することは難しい。会社の機密情報は、今この瞬間もどこからか流出しているかもしれない…。

☛ **PoC**という名の落とし穴

「あるSaaSサービスベンダーから提供されるコンサルティングサービスをPoCとして発注して試す際に、サービス利用契約も込みでPoC契約されることとなっていた。当該サービスには AI 機能が盛り込まれていた。（中略）成果物の検収をどのように行うかは大きな課題である」
【解説】試しに使うつもりが、いつの間にか本契約のような拘束を受ける。「とりあえずPoC」という判断が、ガバナンスの落とし穴となる。

Category 3：ルールを作ったけれども…

☛ プレスリリースで知った自社の「高リスク**AI**」販売

「高リスクと定義したAIシステムを捕捉する仕組みを開始する前に、本社リスク管理部門において当該定義に該当するAIシステムの販売開始を自社のプレスリリースで知ったことがあった」
【解説】管理部門がリスク評価シートを作っている間に、ビジネスサイドは商品を世に出してしまう。ガバナンスのスピードが、イノベーションに遅れをとった瞬間。

☛ 私用端末で作った業務利用ロゴ

「社員の私用端末上のChatGPTで作成した画像（ロゴ）を業務利用したいと相談が入った事例がある。本件については、社内に閉じた用途であっても私用端末の業務利用を認めていないことから利用を見送っていただいた」
【解説】「会社のために良いロゴを作りたい」という意欲が、権利関係不明の生成物を業務に混入させる。悪意がない分、防ぐのは難しい…。

☛ オプトアウトって何ですか？

「ChatGPTやGeminiなどをオプトアウトせずに利用しているのを発見した。Azure経由のcopilotなどを社内整備はしているが、そのような現状を完全把握や誘導、禁止遵守させることの難しさは感じている」
【解説】ルールはあっても、遵守の徹底は従業員のリテラシー次第。物理的な遮断までは難しい。

第4. 現場の「実践知」に学ぶAIの管理・捕捉手法

「第3. AIガバナンスのパラドックス」で見た通り、AIの管理・捕捉の実践は「自分たちの死角に気づかされる」ことと表裏である。では、現場の担当者はどう戦っているのか。本調査から浮かび上がってきたのは、リソースの限られた現場が試行錯誤しながら編み出した「工夫」の数々である。四つの類型に整理し、紹介する。

【設問スコープ】貴社単体におけるAIの利用状況把握やリスク管理に関して、最も効果的だった取り組みは何ですか？その理由もあわせてご記入ください。

1. 既存フレームワークを活用した「相乗り型」

新たなAI専用の管理フローをゼロから構築するのではなく、既存の業務プロセスやIT資産管理の仕組みにAIの要素を「相乗り」させるアプローチである。

現場は新しい管理ツールの導入や申請フローの追加を嫌う傾向にある。そこで、既存のプロジェクト管理の規定や情報資産管理プロセスの中に、AIに関するチェック項目やフラグ等を組み込み、予算執行やセキュリティ審査といった、業務上回避できない「関所」を設けることで、AI利用を捕捉する。これにより「AIガバナンスのためだけの申請」という心理的負担を解消しつつ、強制的かつ自然に、法務、セキュリティ部門を巻き込むことが可能になる。

【現場の声】

- 「生成AI関連のユースケースは弊部の承認を得ているかを他のガバナンス部門（PIA、法務、セキュリティ等）にも確認してもらい、未相談の場合は斡旋してもらっている。既存プロセスでは（上記部門に）相談なしにプロジェクトが進むことは考えにくい」
- 「既存のフレームワークにAI要素を組み込むことで、社内での管理の浸透を図れた」

2.「対話」と「審査」による担当者のリスク感度の向上

対象となるAIの仕様について、書面上のチェックリストだけで終わらせず、会議体や窓口を通じた「対話」を重視し、担当者のリテラシーまで含めて評価するアプローチである。

AIのリスクは、ツールそのものより、それを使う「人のリテラシー」に依存する。そこで、部門横断的な専門家が出席する「レビュー会」を設置し、単にツールの安全性を審査するだけでなく、対話を通じて担当者がどの程度リスクを理解しているか（リスク感度）を評価する。ツール評価のみならず、担当者の教育機会としても機能させることが可能になる。

【現場の声】

- 「一部プロダクトについては、開発の途中でモデルレビュー会という会議を通すこととしており、そこに部門横断の専門家がそれぞれの観点で評価。このプロセスが効果的であると感じている理由は、会議体であることで、担当者も事前に評価される項目に合わせて準備を実施するある種のハードルと、また会話を通じて、担当者のリスク感度のレ

ベルを把握しやすいことにある」

3. ホワイトリストの提示と技術による「リスクの早期遮断」

AIの利用が拡大してから対処するのではなく、入り口でリスクをコントロールする予防的なアプローチである。

自社やグループ内に「いつの間にか」AIが広がる最大の要因は、ルール不在の空白期間にある。そこで、利用拡大前にルールを整備し、「使ってよい認定AI」のホワイトリストを明示する。併せて、アクセスログを監視し、リスクの高いサービスへの接続を技術的に遮断（ブロック）する。推奨と強制力を組み合わせることで、AIを利用したい従業員の迷いを消し、シャドーAIへの流入を防ぐ最もシンプルな防波堤となりうる。

【現場の声】

- ➢「AI利用に関する社内ルール・ガイドラインを早期に整備し、社内利用が拡大する前に周知徹底を図った」
- ➢「外部へのアクセスログから、どのような生成AIが利用されているか確認し、リスクが高いと判断したAIサービスへの接続を制限した」
- ➢「会社管理パソコン、スマホ経由で社内標準（随時アップデート）と推奨AI利用に限定している」
- ➢「利用可能なAIサービスを決めており、その範囲内での利用が原則。その他の利用は、管理者の承認が必要としており、また費用支出でもモニターしている」
- ➢「認定AIについては明示的に許可されているので使ってよいものがわかりやすくまとまっている」

4. 従業員の「関心」を入り口にした実態把握

従業員の学習意欲や関心を入口に、AI利用の実態を引き出すアプローチである。

いきなり「管理のため」のアンケート調査は、従業員から率直な回答が得られにくい可能性がある。そこで、AI活用のための「勉強会」を実施し、AIへの興味関心を高めた上で、アンケートを実施することで、ポジティブな文脈での実態把握を行うことが可能になる。従業員の心理的ハードルを下げ、AIについて「隠すべき利用」から「共有すべき知見」へと意識を転換するものである。

【現場の声】

- ➢「AI活用勉強会の実施でAI活用そのものに興味を持っていただき、その上で使っている・使ってみたいサービスについてアンケートを実施している」

AIの管理・捕捉の
課題とプラクティス
（個社インタビュー調査）

第5. 先行企業のケーススタディ（インタビュー）

本章では、AIガバナンスにおいて先行的な取り組みを進める6社の実態に迫った。各社へのインタビューから見えてきたのは、シャドーAIやAIツール・サービスの爆発的な増加に対し、完璧な統制は不可能という現状認識をもち、限られたリソースを「守るべき領域」に集中させる「選択と集中」の決断である。

A社：完璧な統制は不可能ー「人力の限界」を認め、自動化へと舵

（1）企業プロフィール

- 業種：サービス
- 立場：AI開発者・AI提供者・AI利用者
- 規模：5000人以上

（2）特徴的な工夫：利用申請（入口）と購買（出口）の突き合わせによる捕捉

A社は、AIの急速な進化と普及に対し、完璧な統制は不可能であるという現実的な認識に立つ。

その上で構築したのが、AIツールの利用申請窓口（入口）と、購買部門が管理する購買データ（出口）を一元的に突合させることで、申請漏れのAIを発見する仕組みである。

まず、利用申請時には、会社が許可したツールであるかの確認に加え、機密情報の入力禁止や会社アカウントの利用といった、利用リスクに応じた具体的な条件を付与して許可する。そして、購買部門が保有するツール・サービスの購買（契約）リストと申請リストを共有・突合させる。これにより、申請なく契約・利用されているシャドーAIなどのAIツールを検知できるほか、既存契約の有無の確認や、社内クロスチャージの判断が容易になり、AI利用の申請・レビュープロセス全体の効率化とリスク低減を実現した。担当者は、「申請窓口（入口）と購買リスト（出口）の両方を押さえることで、未申請利用の発見や管理体制強化が可能になる」と述べる。

（3）直面する課題：「見えない」ローカルLLMとサプライチェーン

A社が今、最も警戒するのが、PCに直接インストールされるローカルLLMの存在である。外部通信の有無やセキュリティリスクの把握が難しく、従来のネットワーク監視では検知できない。また、従業員には社内標準AIの利用を教育し、ビジネスユーザー向けには推奨AIツールを整備するが、現場からは常に最新機能を持つ新しいAIツールの利用要望が挙がってくるため「対応が追いつかない」（担当者）。なお、個人利用については、アカウント不要で利用できるAIサービスについては禁止しておらず、モニタリングはしているが厳格な制限は設けていないという。

また、業務委託先や外部パートナーの管理も課題として挙げた。担当者は「業務委託先・再委託先がどのAIサービスを利用しているかまで追跡するのは難しい」として、A社が提供したAIツール以外を使う場合はコントロールが困難であると頭を悩ませる。今後は、業務委託契約にAI利用に関する情報や条件を組み込むことを検討しており、法務や知財部門と連携しながら適切な文面やガイドラインの策定が必要であるとの認識を示した。また、業務委託の形態が多様であるため、AI利用規定の網羅的な適用や個別対応の必要が課題となっていることも述べた。

（**4**）次なる「一手」：ガバナンス・オートメーションの実装

A社は、現在「AIガバナンスの問い合わせ対応が、人力では限界に達しており、ルールや優秀な人材だけでは対応しきれない」として、ガバナンスオートメーションツールやプラットフォームの構築を最大のチャレンジと位置づける。そして、AIツールやモデルのライフサイクルが非常に短い点を踏まえ、スピード感を持ちながら統制を効かせるためには「アジャイル・ガバナンス」の実現とそのための仕組化・自動化が不可欠であると強調する。既存ツールの組み合わせを基本線としつつ、必要に応じて独自開発も視野に入れているという。

B社：従業員を信頼ーリテラシー向上と裁量拡大で自律を促す

（1）企業プロフィール

- 業種：情報・通信
- 立場： AI提供者・AI利用者
- 規模：5000人以上

（2）特徴的な工夫：既存システムへの「相乗り」と利用者層に応じた裁量拡大

B社は、AIガバナンス体制をゼロから構築せず、AIガバナンスに関する検討事項が発生した場合、既存のプライバシー影響評価（PIA）や法務、セキュリティ部門のガバナンスプロセスにAIチェックを「相乗り」させるアプローチを採る。これにより、プライバシー、セキュリティ等のAI特有のリスクを、既存の専門組織の知見を活用しながら効率的に評価・管理している。

また、従業員への「信頼」をベースとした性善説に基づき、ガバナンス部門が、現場の利用状況や雰囲気を見ながら、裁量範囲を調節する運用を採用している。例えば、従来型AI（レガシーAI）は、各分野の専門家が独自の基準で運用することを認めるが、生成AIは、これまでAIを使ってこなかった層も利用するようになったため、ガバナンス部門が新たな管理範囲を設定するといった対応を採っている。

（3）直面する課題：後追い対応と想定外利用の発生

課題は、次々と登場する技術やサービスへのスピーディーな対処である。担当者によると、MCPやAIによるコンピュータ操作などの新技術・新サービスが現場で利用され始め、問題が顕在化してから、ガバナンス部門が初動対応としてルールやガイドラインを後追いで整備するケースが多いと頭を悩ませる。

また、担当者は、従業員のルール誤解や想定外の利用事例は「一定数は存在している」と打ち明ける。情報漏洩リスクはセキュリティ部門が厳格にモニタリングしているが、それ以外の軽微な事例については、従業員から自己申告ベースで相談窓口に報告されてから発覚するため、注意喚起やルール改定とのタイムラグに苦心しているという。

（4）次なる「一手」：AIの品質管理と人の責任所在の明確化

B社は、ビジネススピードを阻害しないガバナンスと、従業員の自律的な成長のバランスを重視する。ガバナンスがビジネスの足枷になることを避けるため、事業部に対しては、セキュリティやプライバシーのリスクが低い範囲を明確化し、「一括で許可する」といった提案も行う。また、AIを利用する従業員に対しては、Eラーニング教材などを通じて、不安な点があれば気軽に相談できる環境を整え、ケースバイケースでの相談を促しながら、徐々にルールの輪郭を明確化するという手法を採っている。

B社の「次の一手」として見通すのが、AIエージェントやAIがAIを作る時代において、従来の

リテラシー教育から品質管理へのシフトが必要であるという点である。AIについて定量的な品質基準の策定や人の責任範囲の明確化が今後の大きな課題になると指摘した。

C社：ガバナンスは「人」ー緩やかな統制と全社的なAI教育

（1）企業プロフィール

- 業種：金融
- 立場：AI提供者、AI利用者
- 規模：1000人以下

（2）特徴的な工夫：既存の「重要ECU」区分を転用した段階的AIリスク評価

C社は、AIを使わないことの方がリスクだと考え、あえて緩やかなルール運用を行い、現実的かつ効率的なリスク管理体制を構築している。

最大の特徴は、既存のEUC（エンドユーザーコンピューティング）管理の枠組みにおいて、重要か否かという線引きを転用して、AIリスク評価に濃淡をつけた段階的審査にしている点である。

C社では従来、業務上の重要度（例えば個人情報、対外決済、取引など業務上重要なシステムを指す）に基づき、IT部門が管理する「重要EUC」と、それ以外の「一般EUC」を区分してきた。この「重要EUC」に関して、AIを利用しているかを洗い出し、一元管理する体制をとっている。

管理対象となったAIは、C社が定めるセルフチェックシートを用いて、AIリスク評価を行う。チェックシートは、EU AI法に準拠した4段階のリスク区分（許容できない・高・低・最小）を採用し、高リスク・低リスクの場合は、セルフチェックを必須とし、最小リスクの場合は、ユーザー判断に委ねる運用となっている。高リスクは全項目、低リスクは特定の項目のみのチェックとするなど、リスクに応じた評価の濃淡付けも徹底する。これにより最もリスクの高い領域にリソースを集中させることを実現している。

（3）直面する課題：少数精鋭ゆえのリソース不足

C社は、AIガバナンス担当が少数精鋭体制のため、リソース不足という根本的な課題を抱えている。現状は、AI活用推進のために「あえて緩やかなルール」で運用しているが、今後、AI利用が全社的に拡大する中で、「人手不足や知識レベル向上が課題となる」ことが見通されている。

また、現状は、グループ本社のC社のガバナンス体制が中心である。グループ会社や海外拠点に対しても生成AIツールやAIエージェントを展開し、同時に学習コンテンツを展開しているもののAIの活用状況について十分に把握できているとは言えないと打ち明けた。

（4）次なる一手：活用推進体制の強化と、ガバナンス体制の継続的な見直し

C社はグループ全体でのベストプラクティスを共有する等、活用推進体制を強化しつつ、外部環境を見ながら随時ガバナンス体制の見直しを進めている。

今後は各国の状況に合わせて、必要に応じて各国の規制やガイドラインを反映したフレーム作りを計画している。

また、海外拠点も含めたグループ全体でリテラシー向上が不可欠であると考えており、従業員向けにAI利活用やガバナンスを必須項目として研修を実施するほか、AI活用セミナーの開催や、AIガバナンス研修動画の英語翻訳による海外拠点への展開など、教育施策を積極的に進める意向だ。

D社：自社の重大リスクを定義、「選択と集中」の徹底

（1）企業プロフィール

- 業種：メーカー
- 立場：AI開発者、AI提供者、AI利用者
- 規模：5000人以上

（2）特徴的な工夫：「高リスク8類型」の明文化と報告義務

D社はAIの「開発者」「提供者」「利用者」という複数の立場を持つため、全てのAI活用を網羅的に管理・棚卸しすることは現実的ではないと割り切り、徹底した「選択と集中」を行っている。
D社は、管理すべき高リスクAIや社外提供AIと管理しない社内利用AIや低リスクAIを明確に切り分けている。
D社は、EU AI法などを参考に、自社ビジネスにおいて提供する製品・サービスを踏まえ、特にリスクが高いと考えられるAIについて「高リスク8類型」として独自に定義し、明文化した。事業部門が8類型に該当するAIを開発・市場投入する際は、リスク管理部門への連絡を義務付けている。これにより、リスクの高いAI開発・提供の動きを、早期に確実に捕捉する体制を構築している。
この仕組みは、過去の失敗経験により作成された。過去、リスク管理部門が「自社のプレスリリースで高リスクAIの販売開始を知った」という事例が発生。これを契機にプロセスを見直し、定義の周知徹底と報告義務化を再構築した。現在も、社外提供する高リスクAIの実態に合わせたプロセス改善を検討中だ。

（3）直面する課題：定義の精緻化とリスク定量化、リテラシー格差

D社は、「高リスク8類型」の中でも、より高リスクと考えられる条件を緻密化する必要性を感じている。背景として、現状の8類型は事業部門によって広く解釈できるため、実運用上は社内での調整が多く発生しているからだ。
また、AIの利用が全社的に拡大する中で、従業員間のリテラシー格差も課題であると考えている。特に、日常業務でAIの活用が身近でない層はリテラシーが低い傾向にあり、「高リスク8類型」の定義の浸透や、適切なAI利用文化の醸成に向けた障壁となっていると指摘する。

（4）次なる一手：ガバナンスのグローバル展開と高度化

D社の次なる一手は、AIリスクの定量化基準の設定と自動評価への試みだ。リスクの度合いを、誰もが客観的に判断できるようにAIリスク評価を定量化することで、属人的な判断要素を極力減らし、仕組みを全事業部門で定着させることを目指す。
D社は定義の精緻化やリスクの定量化に取り組みつつ、将来的には、これらの評価プロセスを自動化することも視野に入れている。

E社：AI利用ルールの「伝え方」を工夫－丁寧さと形骸化のジレンマ

（1）企業プロフィール

- 業種：情報・通信
- 立場：AI提供者、AI利用者
- 規模：1000人以下

（2）特徴的な工夫：2段階チェックとAI機能追加時の再許可フロー

E社は、リスクゼロは不可能と割り切り、リターンが見込める許容可能なリスクであれば試用を認めるというバランス重視の方針を採る。

E社は、AIサービス利用の安全性を担保するため、台帳による一元管理をベースとした二段階の承認プロセスを実践している。まず、セキュリティ等の技術的なチェックが行われ、次に法務部門によるリーガルチェックが入り、この二段階をクリアしたサービスのみが、社内の利用可能リストに追加される。

E社の運用の丁寧さを示しているのが、既存サービスへのAI機能追加時の対応である。担当者は、チャットツールに要約機能が追加されるなど、既存の認可済みサービスにAI機能が追加された場合、そのサービスを「新規」と同様とみなし、再度AI許可フローにかける運用を徹底している。

（3）直面する課題：「全件を人の目で」のボトルネック、ガイドライン形骸化

E社は、運用負荷とルールの実効性という二つの大きな課題に直面している。

現状、最大のボトルネックは、法務部門のリーガルチェックにある。担当者曰く、利用規約やデータ取り扱いの確認を「全件人の目で行っている」ため、法務部門の負担が極めて高く、依頼から許可まで時間がかかる状態が常態化していると打ち明ける。承認プロセスの遅延は、プロセス外での利用を誘発しかねない。実際に、AIによる議事録自動要約サービスなど、プロセス外でAIサービスを試用した後に、許可申請されるケースがあったことを挙げた。

さらに、DeepLなどの翻訳ツールはAI元年（2023年）以前から使われており、従業員が「AI機能として認識していない」ケースも多く、管理が難しいと頭を悩ませる。

E社が深刻な課題として挙げたのは、ルールの形骸化である。社内アンケートの結果、AI利用者のうち8.8%がガイドラインを読んでいないことが判明し、未認可AI利用のリスクが高いことに懸念を示した。

（4）次なる一手：ショート動画でリテラシーの向上

E社は、管理プロセスの厳格化ではなく、従業員のリテラシーを変える方向へと舵を切っている。

ガイドライン未読という課題に対し、従来型の長い動画の視聴率が低いことを問題視し、AI

のルールやリスクに関する勉強会を増やしつつ、AI教育コンテンツは1～2分程度のショート動画をスマホで見られる形で量産する計画を進めている。
　また、担当者は、社内のガイドラインの更新ペースを上げ、実態に合わせる必要性を述べた。今後は社外向けサービスのリリースに合わせ、社外向けのAI倫理・規定を策定し、自社のAIが安心であることを外部に発信していく計画も進めている。

F社：AI利用者にとってガバナンスはコスト―全件管理からの脱却

（1）企業プロフィール

- 業種：金融
- 立場：AI利用者
- 規模：5000人以上

（2）特徴的な工夫：現場を伴走支援、ヒアリング内容を「組織知」に

F社は純粋な「AI利用者」の立場であり、ガバナンスは「純粋なコスト」であると考えている。そこで、リスクとコストのバランスを常に意識した、地に足のついたAIガバナンスを模索している。

F社のガバナンスは、現場に寄り添う伴走型支援と、それを組織知に変える仕組みによって特徴づけられる。まず、AI活用を申請した部門に対し、データ管理部門が直接ヒアリングを実施し、ファクトシートに基づきリスクの有無を確認する。その際、単に評価を下すのではなく「利用者が気づいていないリスクもその場でアドバイスしている」という（担当者）。

さらに、ヒアリング内容やリスク評価を「評価結果シート」として記録、トラッキングや事例集積、振り返りに活用する「組織知」としてのデータベース化も予定している。また、過去の事例をもとにリスク対応策のサンプルも用意。利用申請部門からのフィードバックを受けて運用を改善する仕組みになっており、体系的な管理を目指している。

（3） 直面する課題：「AI利用者」特有のコスト構造

F社の担当者は、AIガバナンスにおいて「AI開発者側がガバナンスコストを商品コストに転嫁できる（投資対効果が説明しやすい）」のに対し、「AI利用者側は会社全体の間接コストとなる」ため、リソース確保や組織体制の構築において大きな制約がある」ことを課題として挙げる。

さらに、既存SaaSがサイレントアップデートされ、「主管部門が気付かないうちにAI機能が追加されていた」事例が実際に発生した。担当者は「主要サービスは監視しているものの、一般的なサードパーティ製品では気付きにくい」と打ち明ける。

ガバナンス部門のリソース不足に加え、技術進化や社会的受容性（リスクの認識）の変化も速すぎるため、「蓄積したノウハウがすぐに陳腐化し、対応策のバリエーションも増え続け、継続的なアップデートが求められる」ことにも頭を悩ませる。

（4） 次なる「一手」：スクリーニング基準による「足切り」

F社は「全件管理」からの脱却を次の一手と位置づける。

現状、AIの定義（AI技術と他技術の境界）が曖昧で、現場での判断が難しいため、「全ての案件をガバナンス側で確認・管理している」状態であり、リソース的に限界を迎えている。そこで、リスクが低いAI利用についてはガバナンス側への報告を省略できるよう、「スクリーニング基準」や「閾値の策定」を目指していると述べた。

また、F社は、AI利用者ゆえのコスト構造という課題意識に基づき「利用者側だけで課題を共有・議論できる場」の必要性を指摘する。個社での対応には限界があり、業界全体での情報共有や外部団体の支援に期待を寄せている。

まとめ

6社のインタビューから、AIガバナンスにおいて「完璧な統制は不可能」であるという現実的な認識が明らかになった。背景には、AIの急速な技術進化やツールの多様化にルールや組織整備が追いつかないという課題がある。

このため、AIの管理・捕捉においては、全件を網羅的に確認するのではなく、「高リスク8類型」や「重要EUC」概念による切り分けのように、自社にとっての「重大なAIリスク」を定義し、そこに限られたリソースを集中させる「選択と集中」のリスクベースアプローチが共通点としてあげられよう。

厳格な管理プロセスや「人の目」に頼った管理・捕捉では、リソースの限界があることも共通して課題として挙げられた。ガバナンスがビジネスにおけるAI活用やスピードを阻害しかねない点には注意が必要であろう。また、従業員のリテラシー教育や、現場の裁量に委ね、自律を促す文化の醸成に力を入れている傾向も見られた。

今後は、ガバナンスの自動化や、AIリスクを振り分ける基準づくり、さらにAIの生成物に対する「品質」や「責任」の明確化が、焦点となってくると考えられる。

第6. AIガバナンスの高度化に向けた課題

本調査から見えてきたのは、AIツール・サービスの急速な増加・進化・多様化を前にして、企業の従来型ガバナンスが構造的な限界を迎えつつある点である。自社／自社グループ内のAI利活用について「全件把握」や「厳格な事前統制」は最早、現実的とはいえない。企業・組織には、一定の不確実性が残存することを前提とした「アジャイル・ガバナンス」の実践への転換が求められる。ここまでの調査や事例をもとに、AI時代の企業における代表的な取組課題の試案として以下の3点を示す。

- リスクベースのガバナンスへの転換：まず根本的な考え方として、「全てのAI利用を管理する」ことを目指す完璧主義からの脱却が必要である。そのためには、リスクベースアプローチを徹底するため、各企業がユースケースごとのリスク評価基準を策定することや、それをもとにしたハイリスク領域への管理リソースの集中的な配分が必要である。

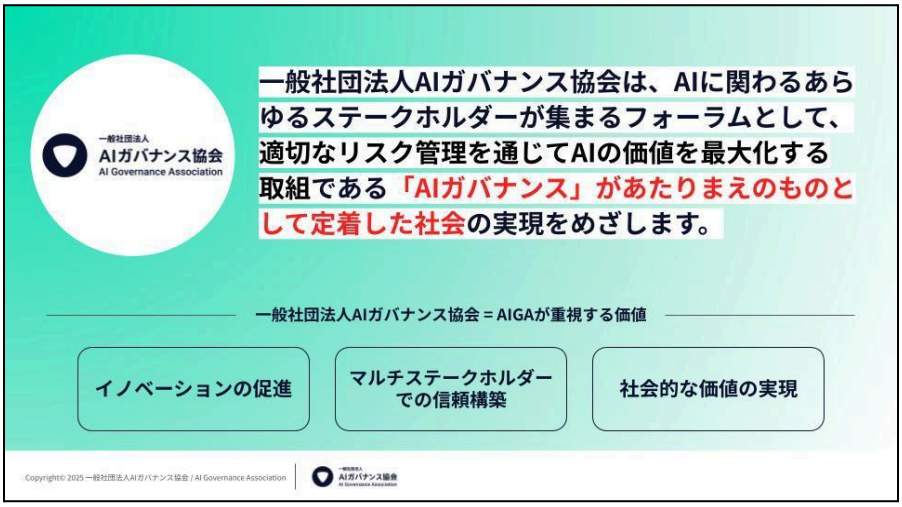
- サプライチェーン管理の規格化：SaaSへの組み込みやベンダーのAI利用も含め、サプライチェーン上に多岐に渡る「いつの間にかAI」のリスク要因が存在することを踏まえ、個別判断に頼らず、可能な限り規格化・標準化した方法でそれらを管理することが重要である。そのためには、調達要件や契約におけるAI利用の位置付けの整理や、ベンダーへの情報開示要求の標準化などを行い、AIの利用状況の透明性を確保することで、個別のデューデリジェンス等の負担を可能な限り減らしていくことが求められる。

- テクノロジーと人材育成による多層的ガバナンス：最後に、あらゆる手段に「完璧」がない中でAIリスクを低減していくためには、テクノロジーと社員リテラシーの双方の洗練を通じたガバナンスの高度化が必要である。ガードレールツールをはじめとするテクノロジーによる自動化されたガバナンス手法の導入や、実際にAIを利用する職員が「リスクに気づく」ための教育とマインドセットの醸成が求められる。

これらの課題は、先進企業が今まさに、それぞれの試行錯誤の中で取り組んでいるものである。そして、リスク評価基準をはじめとして、個別企業の内部だけに閉じた検討ではなく、集合知を活用することで効率的かつ効果的にアプローチできる課題も多い。AIGAでは引き続き、マルチステークホルダーでの情報交換と議論を通じ、こうした課題に立ち向かう企業・組織を支援するとともに、共通して活用できる標準策定等にも取り組んでいく。

一般社団法人AIガバナンス協会について

AIのビジネス活用の可能性は生成AIの流行を背景に急拡大しており、今やほとんどの業界・業種がAIと無関係ではなくなっています。一方、そうした活用の広がりの裏で、そこに潜むリスクも広く認識されるようになり、国内外の政府が新たな政策を検討するなど、AI活用を進めようとするプレイヤーへ「AIガバナンス」を求める動きも加速しています。 一般社団法人AIガバナンス協会（AIGA）はこうした背景のもと、社会が安心してAIを活用し、持続可能な成長を遂げるために、多様なプレイヤーがAIガバナンスのあり方を議論できる場を創るべく立ち上げられました。AIGAでは以下のミッションステートメントのもと、AIのビジネス活用を進める企業を中心とするメンバーが産業横断で議論を行い、企業のあるべきAIガバナンスに関する共通理解の醸成や政策提言等の活動を実施します。



AIGAの活動の特徴は、大きく以下に示す3点です。具体的な活動内容については、[AIGAのウェブサイト](#)をご覧ください。

レポートの策定経緯・メンバー

本レポートは、以下に掲げる政策提言ワーキンググループメンバーの皆様のご助言とAIGA会員企業のご協力のもと、AIGA事務局によって取りまとめられました。
本レポートの策定にあたり、ご協力いただいた皆様に厚く御礼申し上げます。

政策提言**WG**メンバー

- 佐藤竜介（WGヘッド、東京海上ホールディングス株式会社）
- 財津健次（楽天グループ株式会社）
- 佐久間弘明（一般社団法人AIガバナンス協会）
- 田中孝昌（株式会社リクルート）
- 藤井達人（株式会社みずほフィナンシャルグループ）

AIGA事務局

- 事務局員　宮原瑞穂（主筆）
- 事務局員　田中励雄
- 事務局員　廣田早希

問い合わせ

本レポートについてのお問い合わせ等は、下記のAIガバナンス協会ホームページ上のお問い合わせフォームよりお寄せください。
https://www.ai-governance.jp/