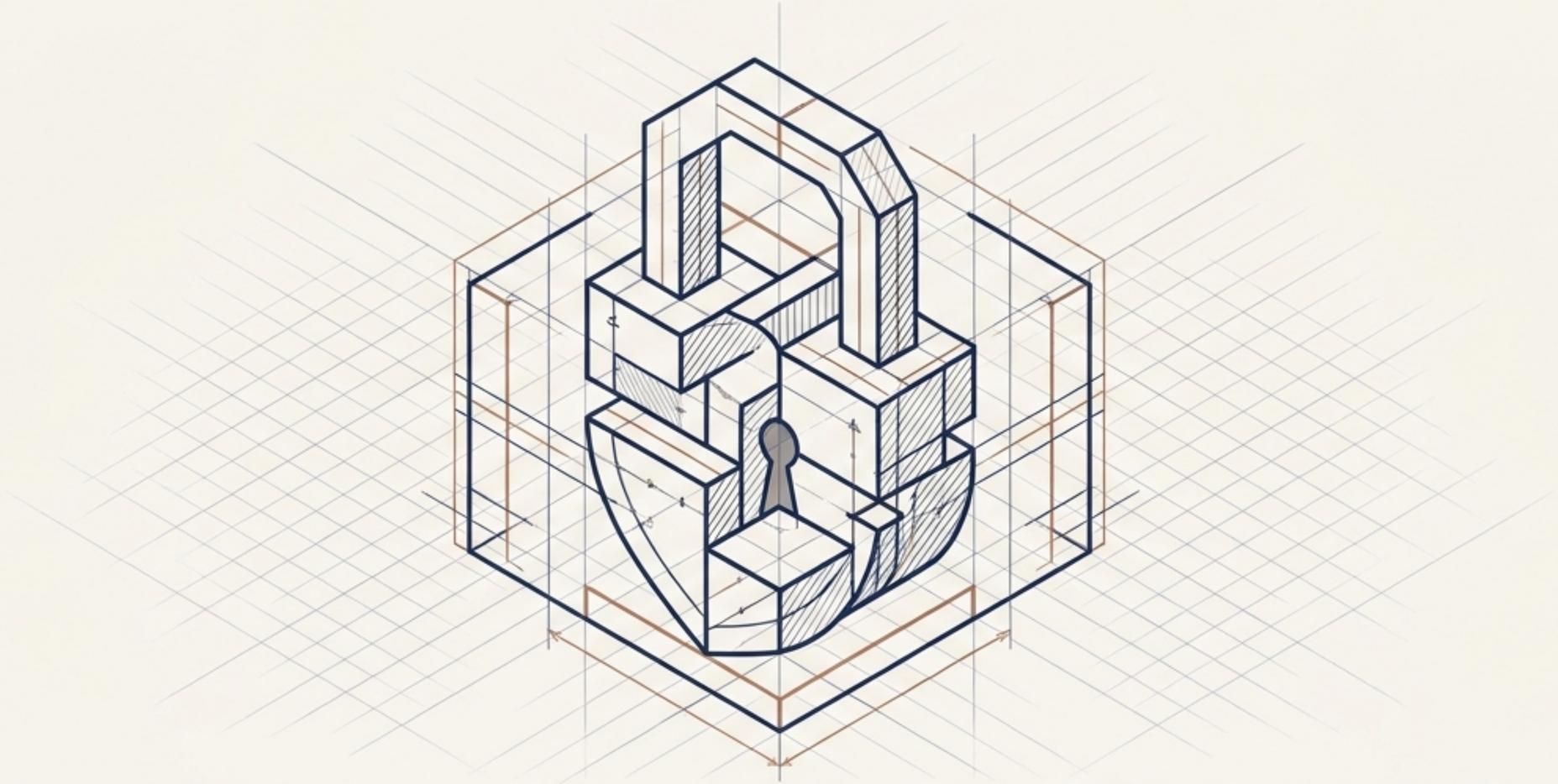
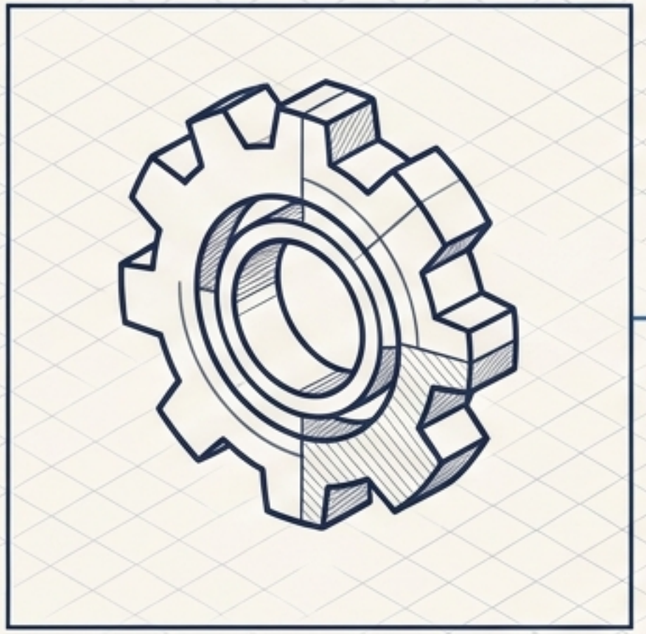


Microsoft Build 2026 と知財業務の転換点

エージェントAI時代のハイブリッド・ガバナンスと組織再編

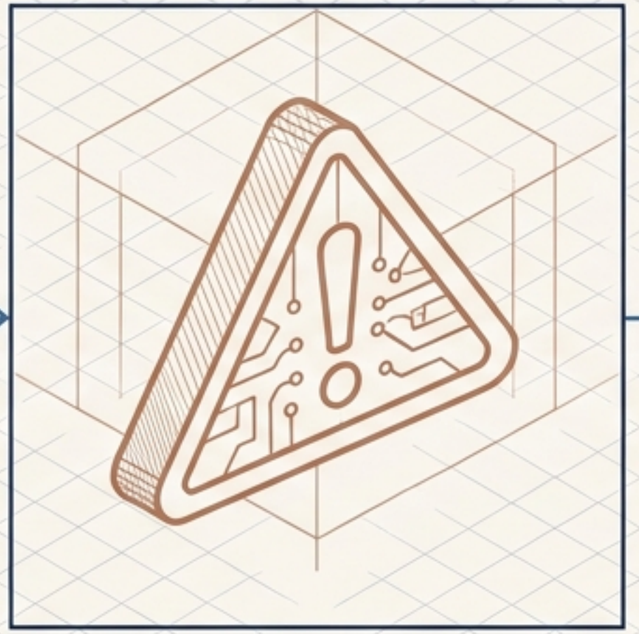
CIPO・知財部門長・リーガルテック戦略担当者向けガイド

エグゼクティブ・サマリー：AIへの「指示」から「委任」へ



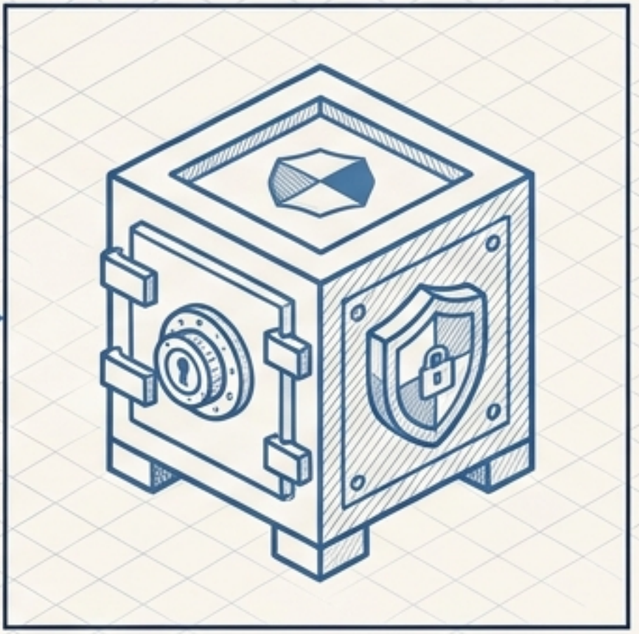
1. パラダイムシフト

自律エージェント「Microsoft Scout」やAgent Framework 1.0の登場により、AIは知財業務の「アシスタント」から「自律的実行者」へと進化。



2. 最大の脅威

エージェントの自律化は、未公開発明の外部漏洩による「新規性喪失」と「守秘義務違反」という致命的リスク（Shadow AI）を伴う。



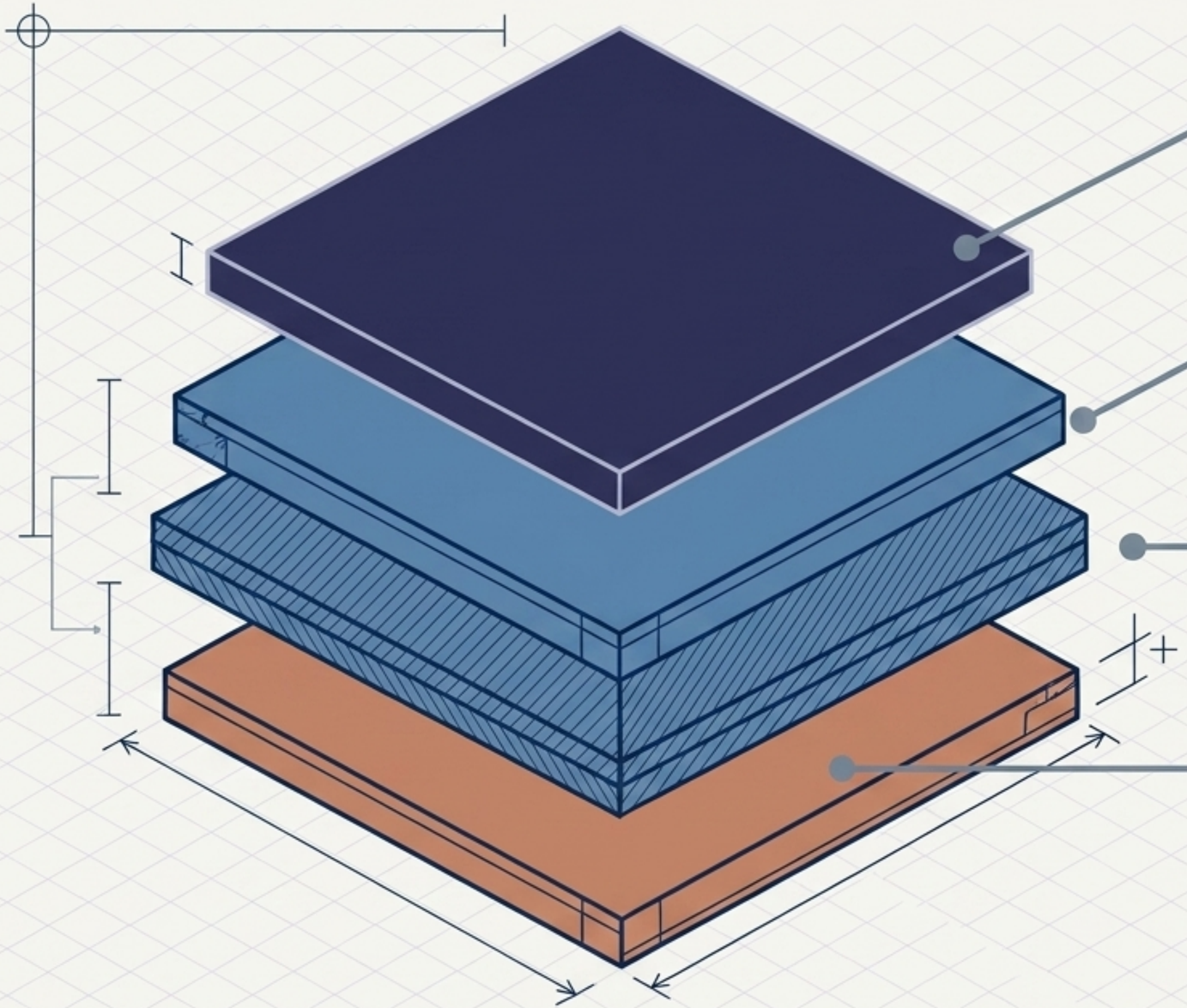
3. ガバナンスの要塞

Microsoftエコシステムの真の価値はAIの精度ではなく、専用IPツールを安全に包み込む「Entra Agent ID」と「Purview」による統制基盤にある。

AIアシスタントから「自律型エージェント」への移行

従来モデル: Copilot / Assistant	新モデル: Microsoft Scout / Agent Framework
起点: 人間によるプロンプト入力	起点: システムのイベントや常時監視による自律的トリガー
動作: 単発のタスク実行（例: 翻訳、要約）	動作: 複数エージェント間での連携と長期ワークフローの進行 (A2A)
監督: 毎回人間が結果をレビュー	監督: 監査証跡（ポリシー適合チェック）とHuman-in-the-loop承認
アイデンティティ: ユーザーの権限を借用	アイデンティティ: 第一級アイデンティティ（固有のEntra Agent ID）を保持

Microsoftエージェント・アーキテクチャの解剖



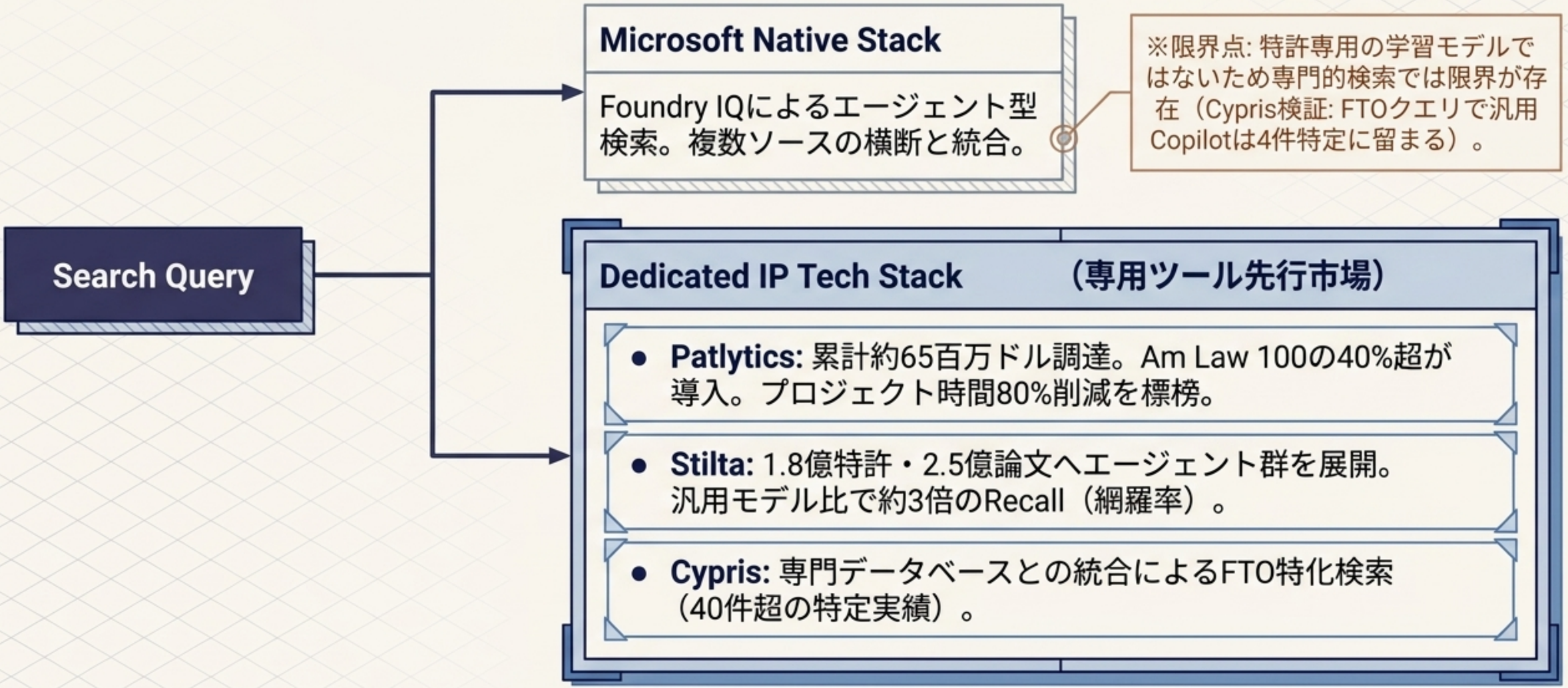
Layer 4: 自律エージェント層
Microsoft Scout - OpenClaw基盤の常時稼働エージェント

Layer 3: コンテキストと意味論基盤
Microsoft IQ層 (Work IQ, Fabric IQ, Foundry IQ, Web IQ)

Layer 2: 制御・ガバナンス層
Agent Framework 1.0, Agent 365, Entra Agent ID - エージェント統制とオーケストレーション

Layer 1: 多様性モデル層
MAI-Thinking-1, GPT-4, Anthropic Claude - Model-diverse by design

知財ワークフローへの影響：先行技術・無効資料調査

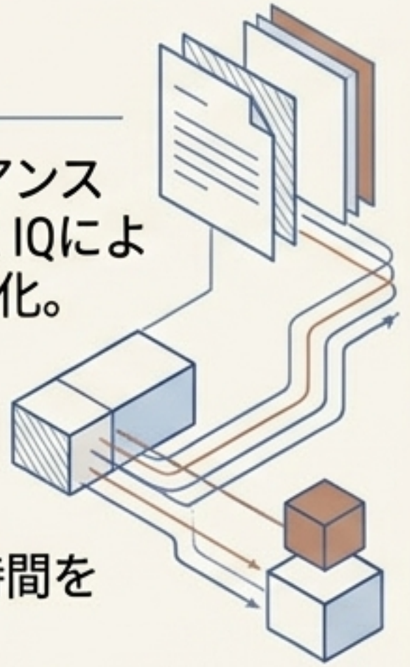


知財ワークフローへの影響：明細書作成とポートフォリオ管理

明細書ドラフティング

MS基盤:

Frontier Tuning（コンプライアンス境界内での強化学習）とWork IQによる過去明細書スタイルの個別化。



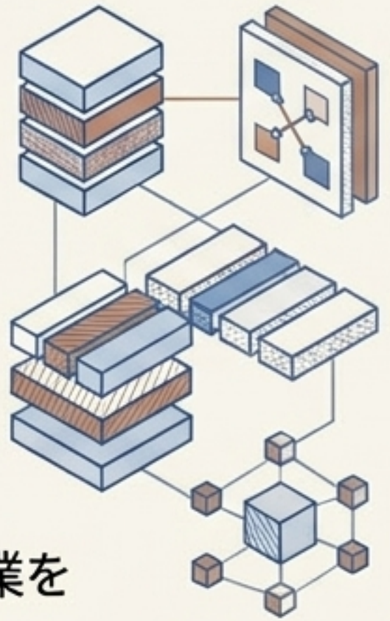
専用ツール:

- **DeepIP**（ドラフティング時間を20〜50%削減）
- **Solve Intelligence**（400超のIPチームが利用、50%以上の生産性向上）

ポートフォリオ分析・IPランドスケープ

MS基盤:

Fabric IQとFoundry IQの組み合わせによる自社データと市場データの構造化。



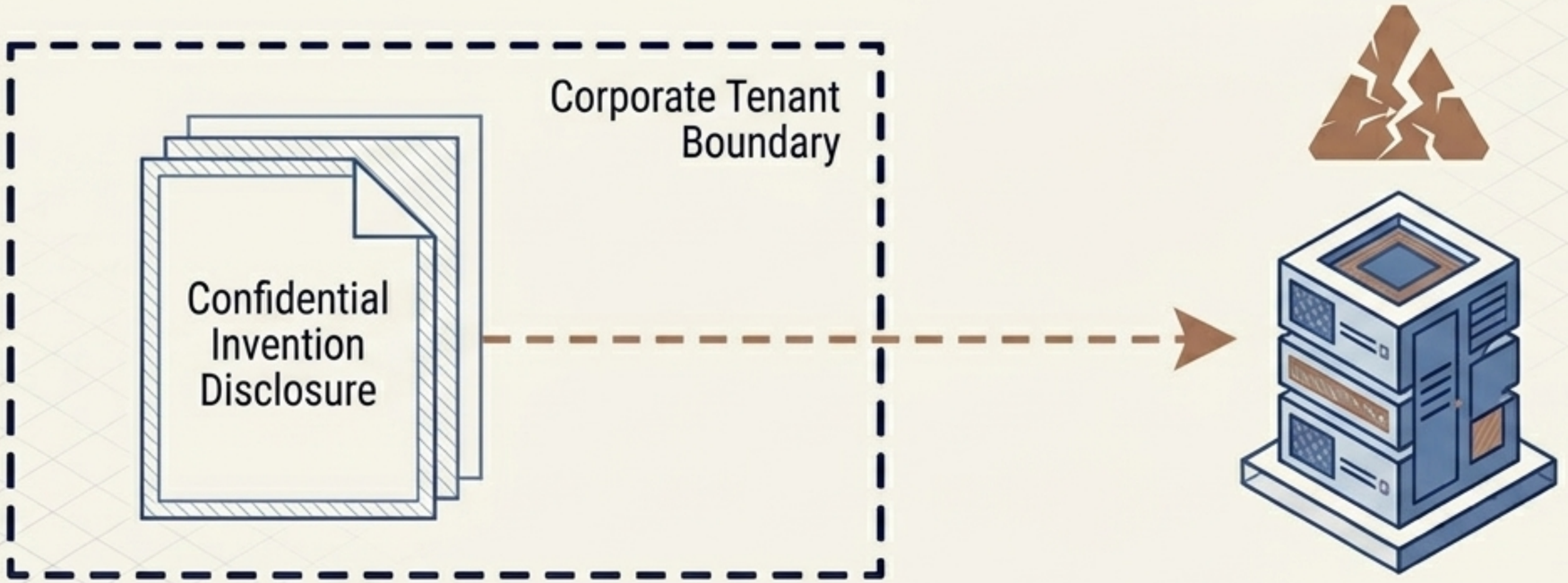
専用ツール:

- **Patentfield**（検索・分析作業を最大80%削減）
- **IP Copilot**（Jira/Confluence連携による発明開示プロセスの効率化）

比較マトリクス：Microsoft Native vs. 知財専用プラットフォーム

評価軸	Microsoft Native Stack	Dedicated IP Platforms (専用ツール)
導入直後の知財精度	**中** - 汎用モデルの限界	**高** - 特許語彙・クレーム解釈に特特化学習
実装・展開スピード	**中** - カスタム構築が必要	**高** - プラグアンドプレイ
ガバナンスとテナント統制	**最高** - 自社テナント内で完全完結	**中〜高** - ベンダーのセキュリティ依存
最適なユースケース	社内文書検索、非特許データ分析、厳格な機密環境	高度なクレーム生成、無効資料調査、FTO分析

致命的リスク：「新規性喪失」と「守秘義務違反」



メカニズム

未公開の発明情報や先行技術調査のプロンプトが外部AIサーバーに送信・保持されることで、法的な「公知」状態を招くリスク。

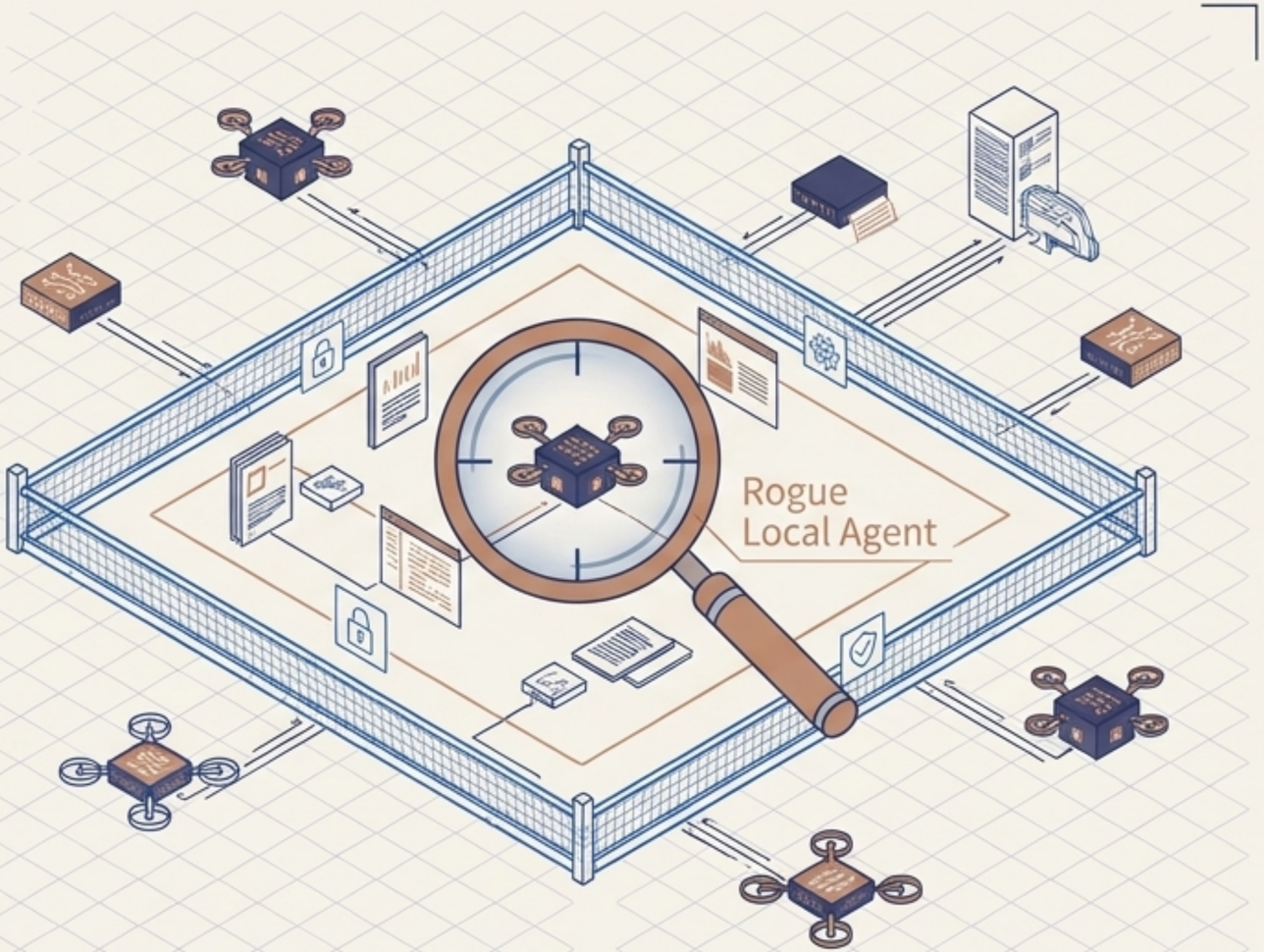
USPTO警告 (2024年4月施行)

AIへの発明側面の入力は、AIがデータを保持・訓練利用・第三者提供し得る場合、守秘義務違反を構成する。

日本弁理士会ガイドライン

外部生成AIへの秘密情報入力は第三者開示にあたり、弁理士法違反のおそれ。新規性喪失の観点から厳重な注意が必要。

目に見えない脅威：「Shadow AI（野良AIエージェント）」



The Threat（脅威）

従業員が独自に導入したローカルAIエージェントや未登録の調査ツールが、IT部門の検知をすり抜けて機密の発明データにアクセスする事態。

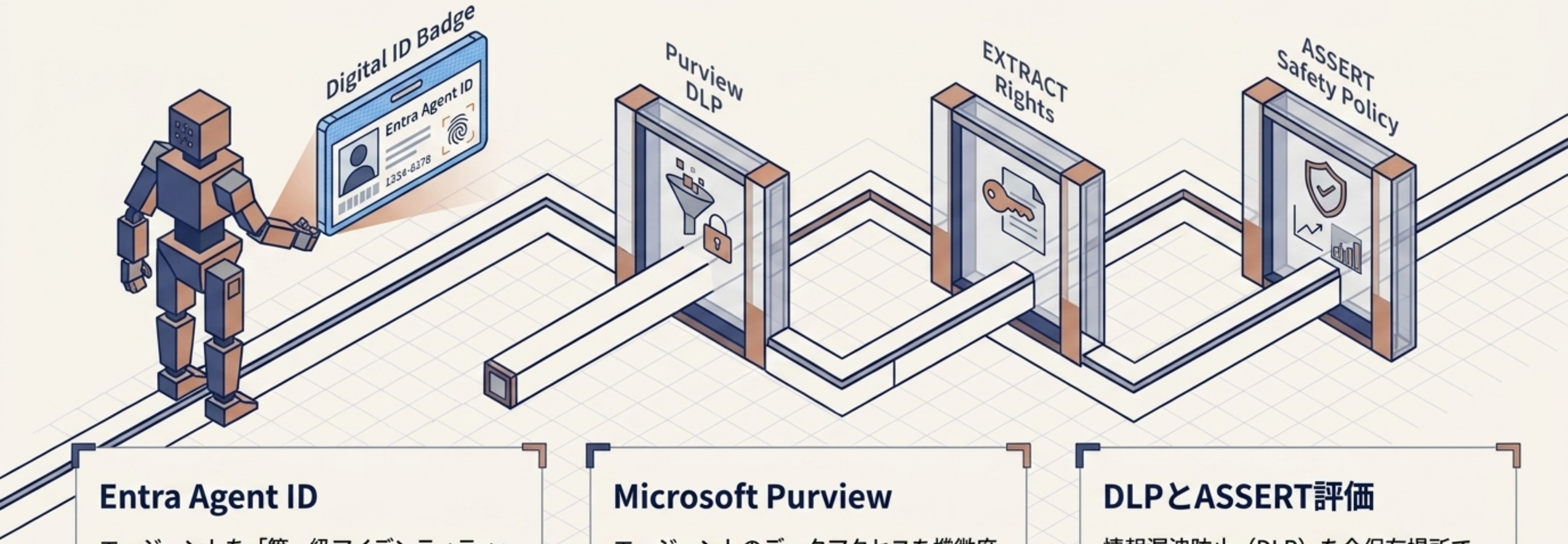
The Challenge（課題）

従来のユーザーベースのアクセス権限では、自律的に動く「エージェント自体」の挙動を追跡・監査できない。

The Solution（解決策）

Build 2026で発表された「Agent 365」によるローカルエージェントの検出と、Defender/Intuneに新設された「Shadow AI」統制ページが必須の防衛線となる。

ガバナンス・シールド：エージェントの身元保証とデータ保護



Entra Agent ID

エージェントを「第一級アイデンティティ」として扱い、固有のID、条件付きアクセス、人間のスポンサー、ライフサイクル管理を適用。誰の指示で動いているかを完全追跡。

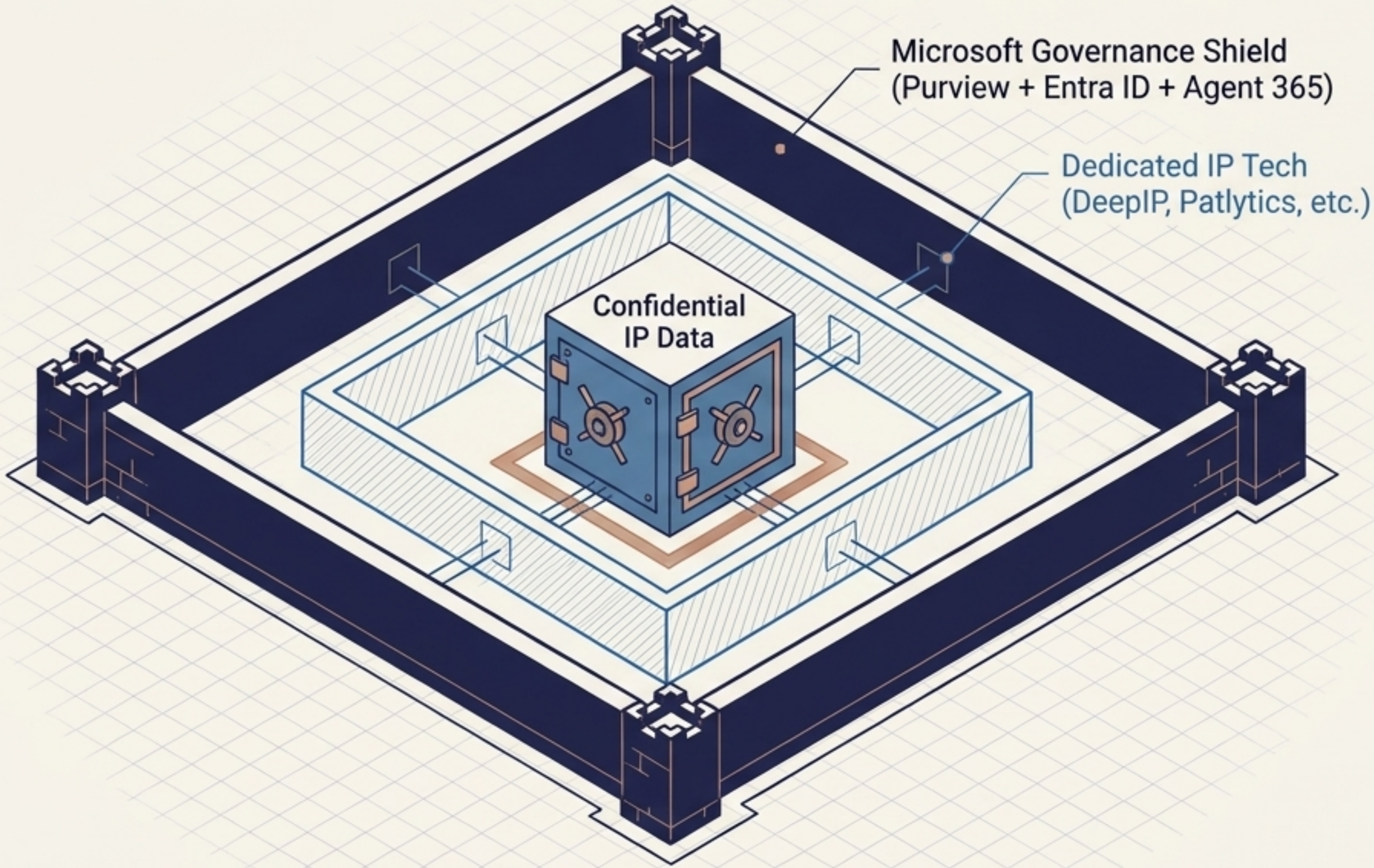
Microsoft Purview

エージェントのデータアクセスを機微度ラベル単位で厳格に制御。
「EXTRACT権限」を持たないエージェントは機密情報への接触を遮断される。

DLPとASSERT評価

情報漏洩防止（DLP）を全保存場所で有効化し、ポリシー駆動の安全性評価（ASSERT）で自律エージェントの挙動を常時監視。

ハイブリッド知財アーキテクチャの完成



Synthesis Insight

Build 2026の真のインパクトは、最先端の知財専用AIツールを、機密漏洩リスク (新規性喪失) なしに企業テナント内で安全に運用可能にしたことにある。

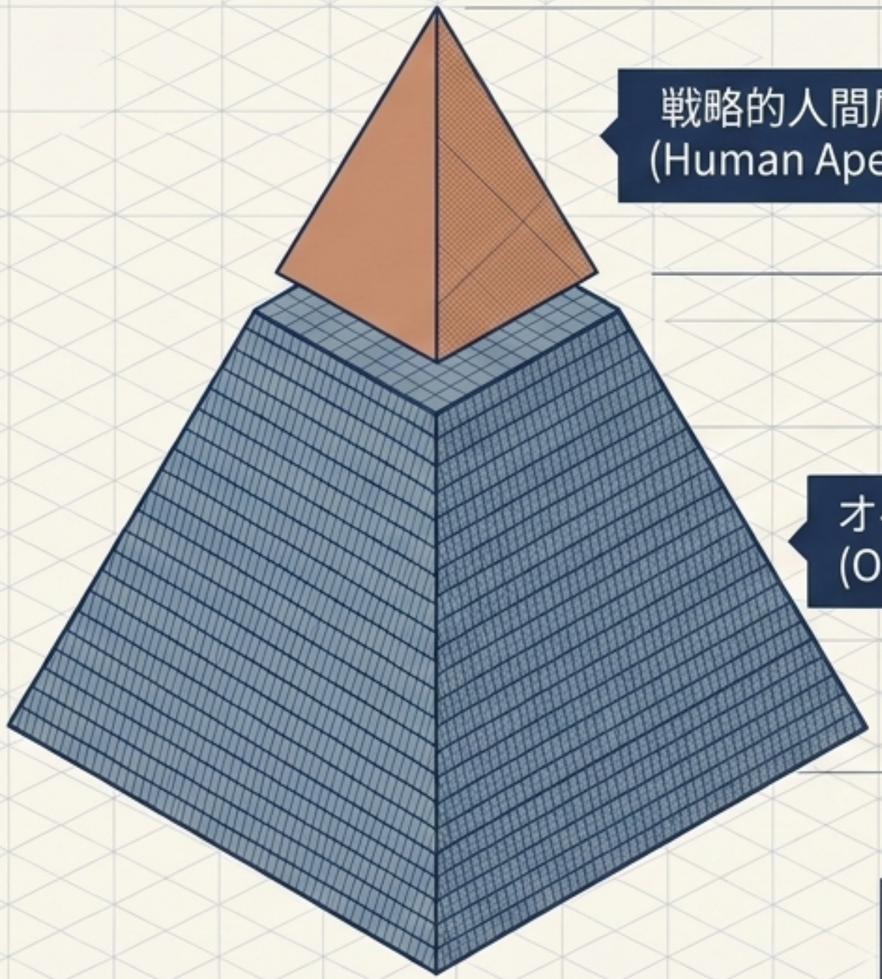
Role of Microsoft

専用ツールを包み込む「ガバナンス・インフラ」と「アイデンティティ基盤」。

Role of Dedicated IP Tech

高精度な検索、高度なドラフティング、特許特有の推論モデルの提供。

組織再編：「二層型」知財デパートメントの構築



役割: 方向付け、標準設定、クレーム解釈、出願戦略、侵害の最終判断。

マインドセット: 実行者から「オーケストレーター」へ。AI出力を出発点とし、品質管理と批判的思考に集中。

役割: 先行技術の一次スクリーニング、明細書初稿作成、クレームチャート素案、ポートフォリオ可視化。

Data Point: 2026 Work Trend Index — 86%のユーザーがAI出力を「最終回答ではなく出発点」として扱っている。

導入プレイブック [Stage 1]：即時実行すべきガードレール

1

ポリシーの再定義: 知財部門のAI利用方針をUSPTOおよび日本弁理士会ガイドラインに整合。「未公開情報入力時のデータ保持・訓練利用なしの契約条件」を明文化。

2

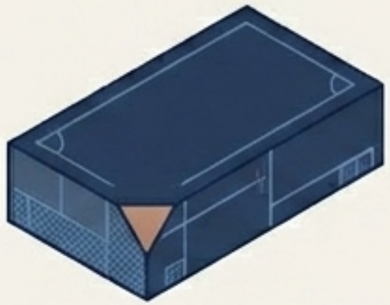
Purviewによるデータ防壁構築: 未公開明細書や発明提案書に最高機密ラベルと「EXTRACT権限」を付与。全保存場所でDLP (情報漏洩防止) を有効化し、AIによる背景索引をブロック。

3

Shadow AIの棚卸し: DefenderとAgent 365を連携させ、組織内で稼働している未登録の野良エージェントを検出・統制下に置く。

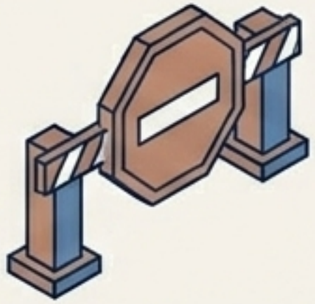
導入プレイブック [Stage 2 & 3]：パイロットからオーケストレーションへ

検索エージェント



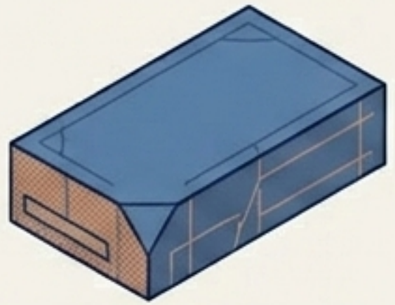
検索エージェント

Human Tollgate



Human Tollgate

ドラフティング・エージェント



ドラフティング・エージェント

Stage 2 (低リスク領域からの委任)

新規性喪失リスクのない「公開済み特許」の一次スクリーニングやIPランドスケープ分析からエージェント化を開始。Microsoftスタックと専用ツールをハイブリッド環境でテスト。

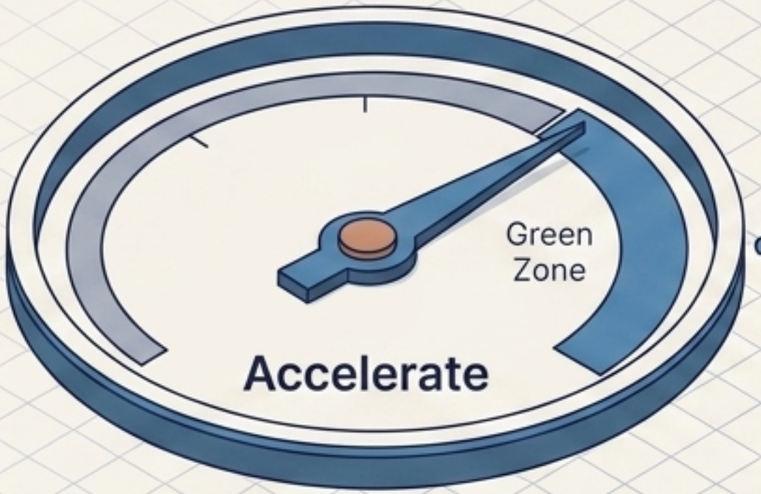
Stage 3 (マルチエージェント連携)

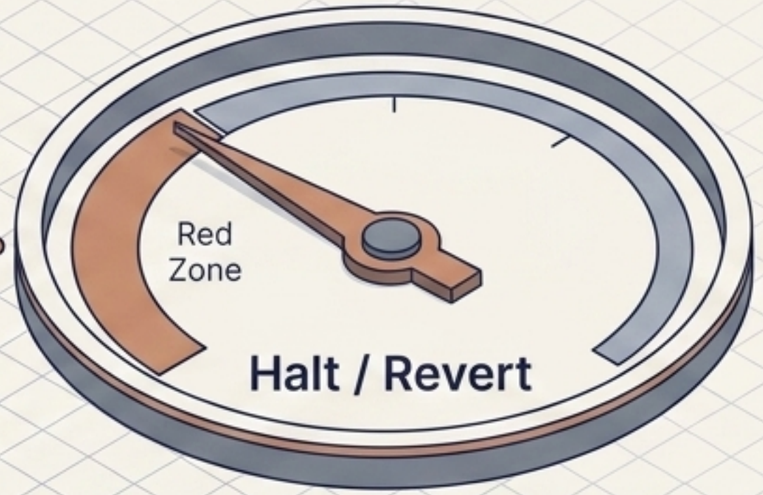
Agent Framework 1.0を活用し、先行技術調査からドラフティング支援へのデータ受け渡しを自動化。

必須要件 (Human-in-the-loop)

エージェント間の連携プロセスには、必ず人間による承認ノードを組み込み、暴走を防止する。

監査トリガー：アクセルとブレーキの判断基準





全面移行への閾値

パイロット運用において、専用ツールによる「弁理士レビュー後の手戻り率」が許容水準を満たし、従来比で、品質同等以上かつ20%以上の時間短縮が証明された場合。

拡張凍結・即時停止の閾値

Purview監査において、ラベル未付与データへの不正アクセスや権限逸脱が検知された場合。または、機密プロンプトの漏洩懸念が払拭できない場合。拡張を停止し、直ちにStage 1の統制基盤に差し戻す。

革新は自律的エージェントによってもたらされるが、その安全を担保するのは人間による冷徹なアーキテクチャ設計である。