Microsoft Build 2026と知財実務

エンタープライズAIガバナンスと「エージェント実装」のパラダイムシフト

CONFIDENTIAL // STRATEGIC ADVISORY FOR IP & LEGAL ARCHITECTS

「生成」の時代

- Copilotの機能追加、テキスト生成、人間のプロンプト依存

⚠ リスク: 個人の操作ミス

「運用と統制」の時代（Build 2026）

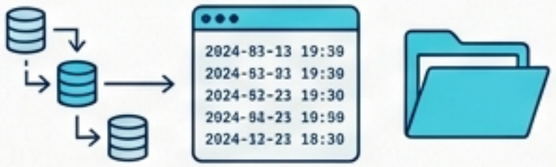
- エージェント実装のフルスタック
  (GitHub → Foundry → Teams → Purview)
- 本質は作成から運用と統制への重心移動

知財業務への導入は、便利な新機能の追加ではなく、証拠化・統制・契約更新を急ぐべき転換点である。

3つの急務

1. 用途別ポリシーとリスク区分の策定

2. Matter単位のログと証拠化の制度化



3. AI特化型の契約・ベンダー審査の更新

統合的IP AIアーキテクチャ：5つの階層

1. 統制層（Control Plane）
Purview DLP, Agent Registry, Entra
— 証拠保全, 権限管理, 監査

2. 配布層（Distribution Layer）
Teams, M365 Copilot, Power Apps
— 事業部連携,
発明届出インターフェース

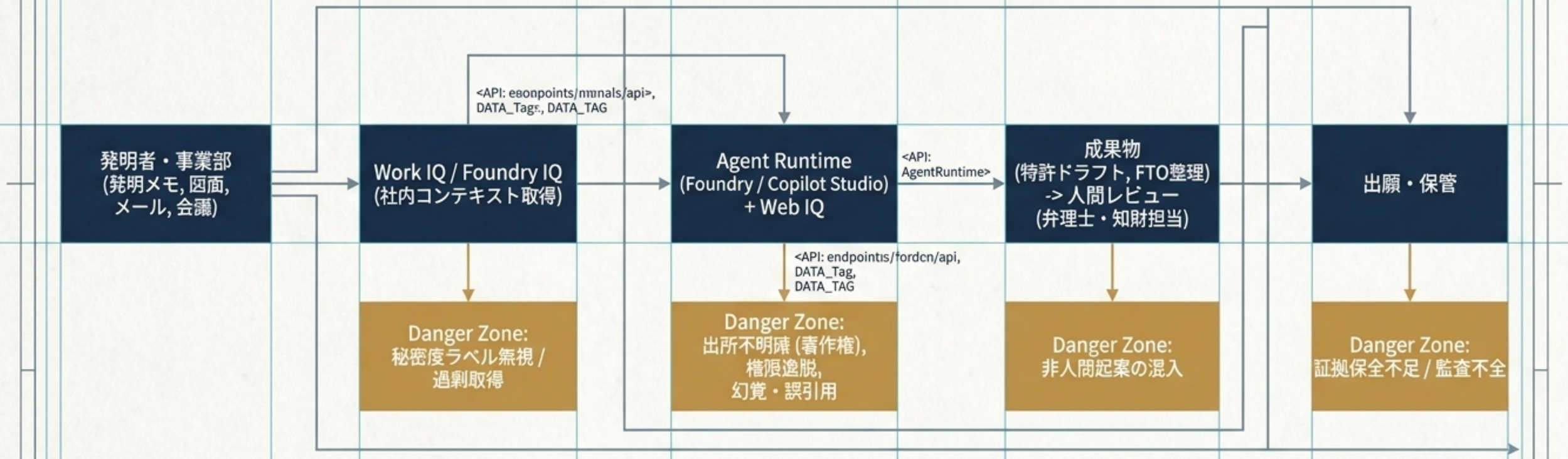
3. 実行層（Execution Layer）
Foundry, Copilot Studio, GitHub Copilot
— 特許起案, 契約レビュー自律実行

4. 外部情報層（External Layer）
Web IQ, External APIs
— 先行技術ニュース, 競合他社動向

5. 社内知識層（Knowledge Layer）
Work IQ workspaces, Foundry IQ
— 発明メモ, 過去契約,
社内コンテキスト

この5層を単一のシステムとして統治しなければ、リスクの伝播速度が制御不能になる。

IPワークフローにおけるAIリスクの伝播



特許起案フローの再設計：3層アプローチ

米国特許法（Thaler v. Vidal）および日本国特許庁（JPO）の建付け上、発明者は「自然人」に限定される。AIによる支援は有効だが、人間の着想と差異化判断の記録が必須。

Step 1: 情報整理 (AI領域)

Work IQ, Foundry IQを使用

エージェントによる発明届・実験結果・先行資料の抽出と要約。

Step 2: 案出 (AI+人間領域)

Foundry (Procedural Memory)を使用

請求項候補・実施形態の叩き台生成。

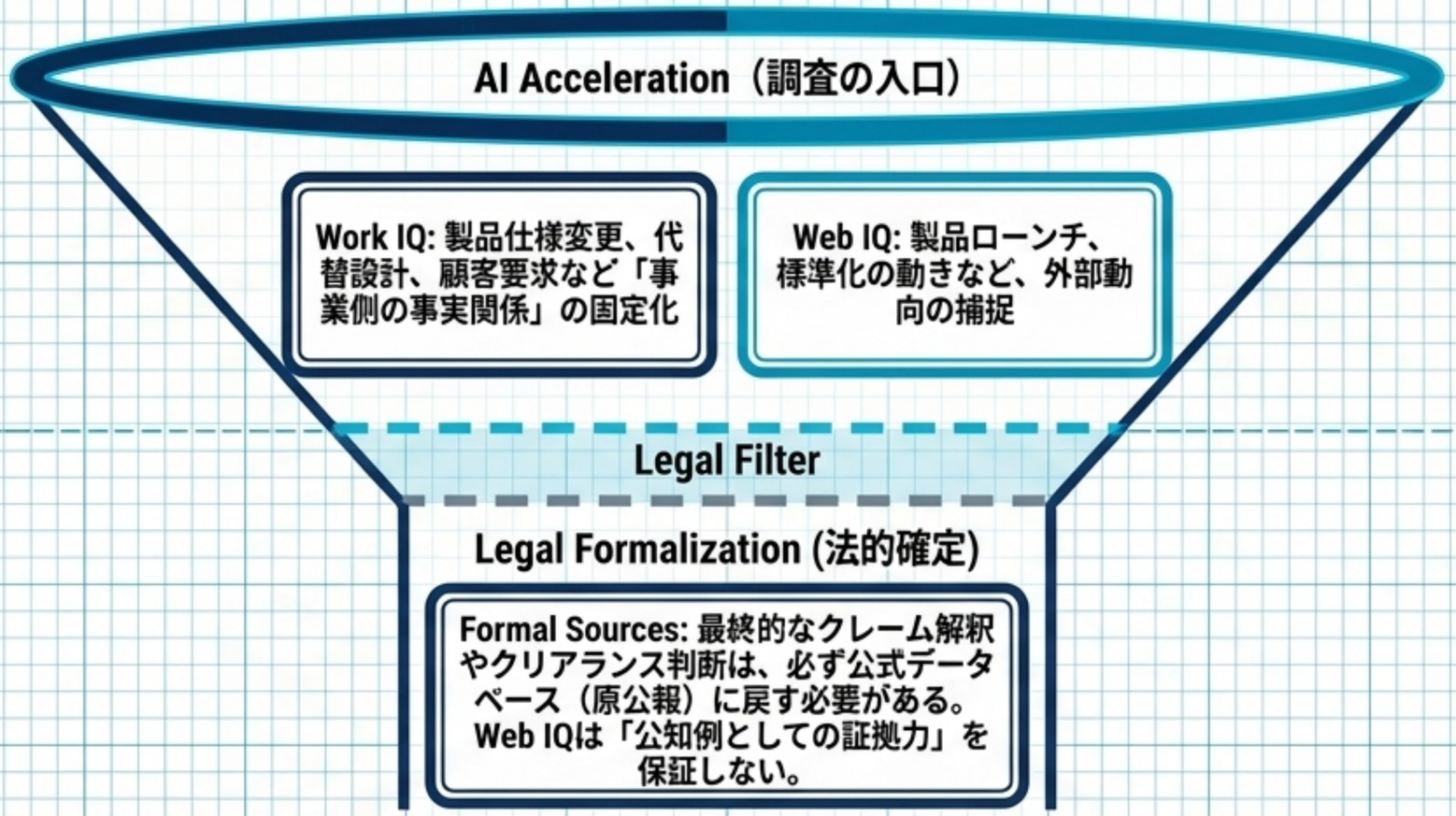
⚠ 必須要件: Source-backed（引用元の紐付け）な出力に限定。

Step 3: 法的仕上げ (人間絶対領域)

Human Legal Review

発明者性、サポート要件、実施可能要件、クレーム・分割戦略の最終確定。

先行技術調査とFTO：コンテキストと証拠能力の境界



Build 2026の新機能は「調査の入口と整理の高速化」に留め、最終意見書の根拠には直結させない。

営業秘密と契約：コンテキストの諸刃の剣

Deep Collaboration（恩恵）

Work IQ / Power Appsにより、既存契約、社内ポリシー、過去交渉経緯を横断した条項比較や論点抽出が劇的に向上。

Amplified Risk（脅威）

エージェントがより長く状態を持ち、より広く配布されるほど、秘密情報が一度漏れた際の「広範な派生リスク」が増大する。

Purview Containment Shield

Purview Runtime DLP & Control Plane Insights

- 生成AI用のDLPルールを既存メールDLPと分離。
- 「入力」「取得」「出力」「ツール呼び出し」の各フェーズで禁止パターン（未公開出願の外部送信など）を定義。

法的リアリティ：完璧さよりも「来歴（Provenance）」

米国（US）

U.S. Copyright Officeレポート & Thaler v. Vidal。生成AI出力の著作物性には「人間の寄与」が中心。発明者は自然人に限定。

日本（Japan）

文化庁2024年整理。現時点では包括的整理に留まり、法的拘束力は持たず具体的事案の蓄積待ち。JPOも自然人限定。

欧州（EU）

AI Act & GDPR。AIシステムの統一ルールと厳格な越境移転（Chapter V）規制。

Strategic Synthesis

法学的な最終解が存在しない現在、IP実務における最大の防御策は「AIを使わなかった証明」ではなく、「誰が、どのデータに依拠し、どこを人間が編集したか」を完全にトレースできる状態（Provenance）を確保することである。

IPタスク別 リスク・ツール選定マトリクス

リスク区分 (Risk)	対象タスク (Tasks)	ツールとガバナンス (Tools & Guardrails)
低リスク (Low Risk)	FAQ対応、期限照会、社内台帳検索	Agent Builder / Work IQ API。 Read-onlyシナリオ。 既存権限への依存で運用可能。
中リスク (Medium Risk)	発明届の整理、先行資料の補助収集、 契約条項比較	Copilot Studio / Power Apps。 秘密度ラベルの同期。 案件ごとのSecurity Role再点検。
高リスク (High Risk)	特許請求項起案、FTO結論、外部送付 文書、訴訟関連メモ	Foundry使用。 Tenant-boundary内での処理、 Runtime DLP、Human Approval （人間承認）の必須化。

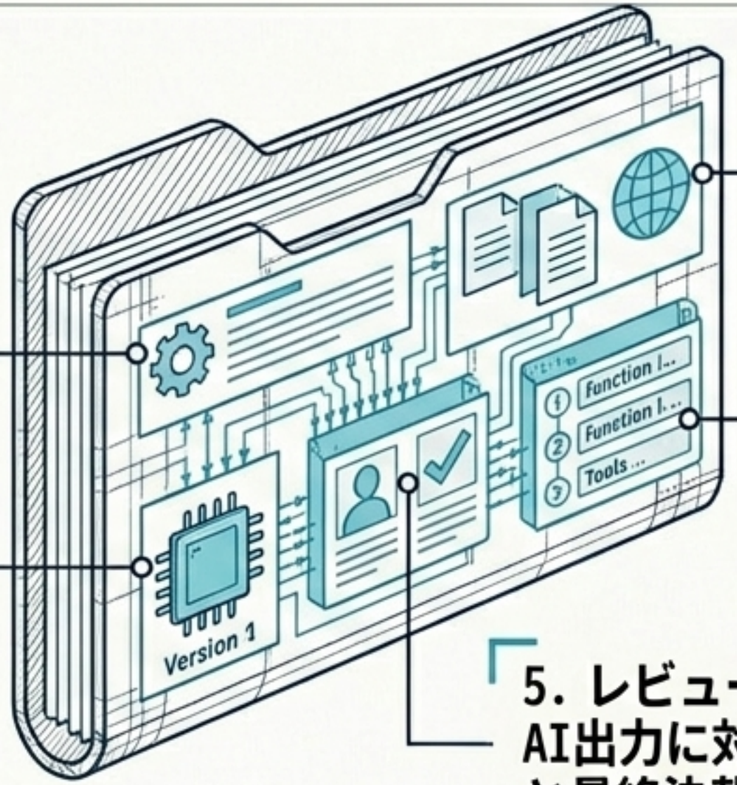
究極の防御構築：「Matter File for AI」の解剖図

Blueprint of Trust

⚠ M365 Copilotの履歴機能はユーザー側で削除可能。知財案件の正式な証拠保全としては不十分であり、案件管理側へのエクスポート固定が必須。

1. プロンプト & 温度設定:
詳細な指示内容と
Temperature等の主要設定値。

2. 取得ソース一覧:
AIが参照した社内文書・
Web IQの外部URL履歴。



3. モデル版指定:
使用した基盤モデル
（例:MAI-Thinking-1）。

4. ツール呼出し履歴:
どのAPI/Toolboxが実行
されたかのトレース。

5. レビュー差分 & 最終承認者:
AI出力に対する人間の編集箇所（Diff）
と最終決裁した自然人。

Blueprint of Trust

調達とベンダー統制：エコシステムの落とし穴

Microsoft 1st-Party Models

MAI-Thinking-1等は商業ライセンス済みのクリーンなデータで学習。AI生成物のPre-training除外。

EDP（Enterprise Data Protection）適用。プロンプトの汎用学習利用なし。デューデリジェンスで極めて有利。

Marketplace & 3rd-Party Agents

事業部が手軽に導入する「野良エージェント」リスク。MicrosoftのEDPだけでは未公開出願の流出は防げない。

Mandatory Audit Checklist

- [ ] 汎用学習・二次利用の禁止条項
- [ ] データ処理主体（Processor）とSubprocessorの明記
- [ ] 越境移転先の地域（Data Location）確認
- [ ] セキュリティ事故通知と是正義務のSLA

エージェント実装へのロードマップ（Timeline）

短期: 境界の確定とガードレール

- 用途別ポリシー（禁止データ、承認フロー）の策定。
- Agent Registry有効化とPurview Runtime DLPの構成。
- Matter Fileに基づく証拠化の部分施行。

中期: 業務組み込みとコスト統制

- 発明届・期限管理をWork IQ / Power Appsと接続。
- 外部Agent導入時の「法務・知財・セキュリティ三者レビュー」義務化。
- 従量課金コストの業務別可視化とROI測定。

長期: オペレーティングモデル再設計

- 個人の工夫から、部門の標準プロセスへの定着。
- 低リスク監視業務における自律エージェントの限定導入。

最終監査チェックリスト：7つの問い

1. 未公開出願・秘密ノウハウを含む入力データの扱いを明確に定義したか？ [Y] [N]
2. 第三者エージェント / Marketplace App の個別利用規約を審査したか？ [Y] [N]
3. M365履歴に頼らず、案件ごとのPrompt/Source/Reviewを別保存しているか？ [Y] [N]
4. 公報調査において、Web IQ等の外部Groundingを「最終証拠」と誤認していないか？ [Y] [N]
5. 発明者性を担保するため、AI出力に対する「人間の関与」の記録を残しているか？ [Y] [N]
6. Agentに流入するデータの越境移転とデータ所在地を契約上確認したか？ [Y] [N]
7. 実効量ベースの課金（Usage Cost）を予算承認プロセスに組み込んでいるか？ [Y] [N]

これらのどれかが欠けるなら、Build 2026の機能は「使える」状態であっても、知財実務に「耐える」状態とは言えない。