2026年Microsoft Buildが示唆する「エージェントAI元年」と知財業務のパラダイムシフト

Gemini 3.1 pro

1. 序論：AIとの対話から「業務の完全委任」へのパラダイムシフト

2026年6月2日から3日にかけて、米国カリフォルニア州サンフランシスコのフォートメイソンセンターにおいて開催された「Microsoft Build 2026」は、コンピューティングとエンタープライズ・ソフトウェアの歴史において、極めて重要な分岐点となるカンファレンスであった[1]。従来のシアトルからAIの聖地とも言えるサンフランシスコへと会場を移して開催された本イベントにおける最大のハイライトは、人工知能の役割が従来の「人間の問いに答えるチャットボット」から、「長期的なタスクを自律的に実行する非同期の同僚（Async Coworkers）」へと根本的に進化したことを、サティア・ナデラCEOが正面から宣言した点にある[1]。同氏は基調講演において、この新たなエージェント群を「エンタープライズグレードの爪（enterprise-grade claws）」と表現し、単純作業を削減して人間が真に価値のある業務に回帰するための全く新しい手段であると位置付けた[1]。

この「エージェントAI元年」の到来は、知的財産（IP）という高度な専門性、厳密な期限管理、そして最高レベルの機密性が要求される領域において、不可逆的なパラダイムシフトを引き起こす。知財業務は伝統的に、先行技術調査、侵害予防調査（FTO）、特許明細書の作成、各国の特許庁からのオフィスアクション（拒絶理由通知）への対応、競合他社の特許ポートフォリオ分析など、膨大なデータ処理と高度な推論を必要とする労働集約的なプロセスから成り立っている。これまでの生成AIは、特定の技術文書の要約やクレームの草案作成といった「点」の業務を支援するに留まっていた。しかし、Microsoft Build 2026で発表された自律型エージェント（Autopilots）や、それを支えるプラットフォーム（Microsoft Agent Platform、Windows 365 for Agentsなど）は、知財業務の「線」あるいは「面」全体を自律的にオーケストレーションする能力を備えている[4]。本稿では、同カンファレンスで発表された一連の最先端テクノロジーが、知財業務の生産性、セキュリティ、研究開発（R&D）との連携、そしてシステムインフラにおいてどのような変革をもたらすのかを、技術的および実務的観点から網羅的かつ詳細に分析する。

2. 自律型エージェント「Autopilots」と次世代知財業務基盤

2.1. Microsoft Scoutによる「常時稼働型」知財パラリーガルの実現

Microsoft Build 2026では、エンタープライズ向け自律型エージェントの新カテゴリとして「Autopilots」が発表され、その第一弾として「Microsoft Scout」が「Frontier Program」のユーザーおよび一部のプレビュー顧客向けに提供開始された[6]。Scoutは、ユーザーが都度プロンプトを与えなくても、独自のアイデンティティを持ち、バックグラウンドで常時稼働しながら複数のアプリケーションやシステムを横断して自律的にタスクを実行する[6]。

この技術基盤は、知財管理システム（IPMS）の運用や、複雑な期限管理プロセスにおいて革命的な影響を及ぼす。知財部門では、各国の特許庁から送達される通知書の期限管理、社内発明者との面談調整、外部の特許事務所や現地代理人との時差を伴うやり取りなど、煩雑な調整業務が日常

的に発生している。Scoutは、Microsoft 365に統合され、Teams、Outlook、OneDrive、SharePointなどのアプリと、チャット、メール、カレンダー、連絡先などのデータを常時監視する[6]。例えば、海外代理人から届いた重要通知の期限が迫っている手続きや、社内の発明提案に対する審査請求の可否判断など、停滞している意思決定を早期に検出する機能を有する[6]。さらに、タイムゾーンを横断した会議のプロアクティブなスケジュール調整、重要会議のフラグ付け、事前準備資料の自動生成などを自律的に行うため、事実上の「デジタル・知財パラリーガル」として機能する[6]。

2.2. OpenClawの統合とエンタープライズ・ガバナンスの確立

エージェントAIを知財業務に導入する際の最大の障壁は、権限管理と情報漏洩リスクであった。知財情報は企業にとって究極の機密情報（営業秘密、未公開特許など）であるため、匿名のサービスアカウントが社内データを横断的にクロールすることは許容されない。注目すべきは、Scoutの技術基盤として、オープンソースのパーソナルエージェント基盤である「OpenClaw」（開発初期はClawPilotとも呼称されていた）が採用されている点である[6]。OpenClawは自律的なタスク実行能力に優れる一方で、サイバーセキュリティ上の脆弱性やコンプライアンス上の課題が指摘されてきた[8]。この課題に対し、MicrosoftはAutopilotsに対して個別の管理対象である「Entra ID」を付与するアーキテクチャを採用し、OpenClaw本体のポリシー準拠機能を上流から貢献（アップストリームへのコントリビュート）することで解決を図っている[6]。これにより、各エージェントは「組織内の一人の従業員」として振る舞い、厳格なロールベースのアクセス制御（RBAC）とMicrosoft Purviewによるコンプライアンスポリシー（データ損失防止や秘密度ラベルなど）の枠内で動作する[6]。例えば、「未公開の発明届出書を分析するエージェント」と、「公開済みの競合特許を分析するエージェント」に対して異なるEntra IDを付与することで、エージェント間でのチャイニーズウォールをシステムレベルで構築できる。また、特許庁への書類提出や高額な外部費用の承認など、極めてセンシティブなアクションに対しては、人間の承認（ヒューマン・イン・ザ・ループ）を必須とする設定も組み込まれており、知財業務におけるガバナンスと自動化を完全に両立させている[6]。

エージェントの種別	主な機能と特徴	知財業務における具体的な適用シナリオ	動作・ガバナンス環境
Autopilots (Microsoft Scout)	常時稼働型、独自のEntra IDを保持、マルチアプリ横断の自律調整。	期限管理、発明者面談の調整、外部事務所とのやり取りの自動化、停滞している意思決定の検知。	Microsoft 365統合、Purviewポリシー準拠、ヒューマン・イン・ザ・ループ承認。
カスタムエージェント **(Copilot Studio)**	ユーザー固有のプロンプトとナレッジベースに基づく特定タスクの自動化。	自社特有の評価基準に基づく特許性評価、特定の技術分野に特化した社内ヘルプデスク。	Microsoft Agent Platform、Copilot Studio内での展開と管理。
R&D特化型エージェ	科学的ワークフロー	新素材探索、創薬プ	Azure基盤、エンター

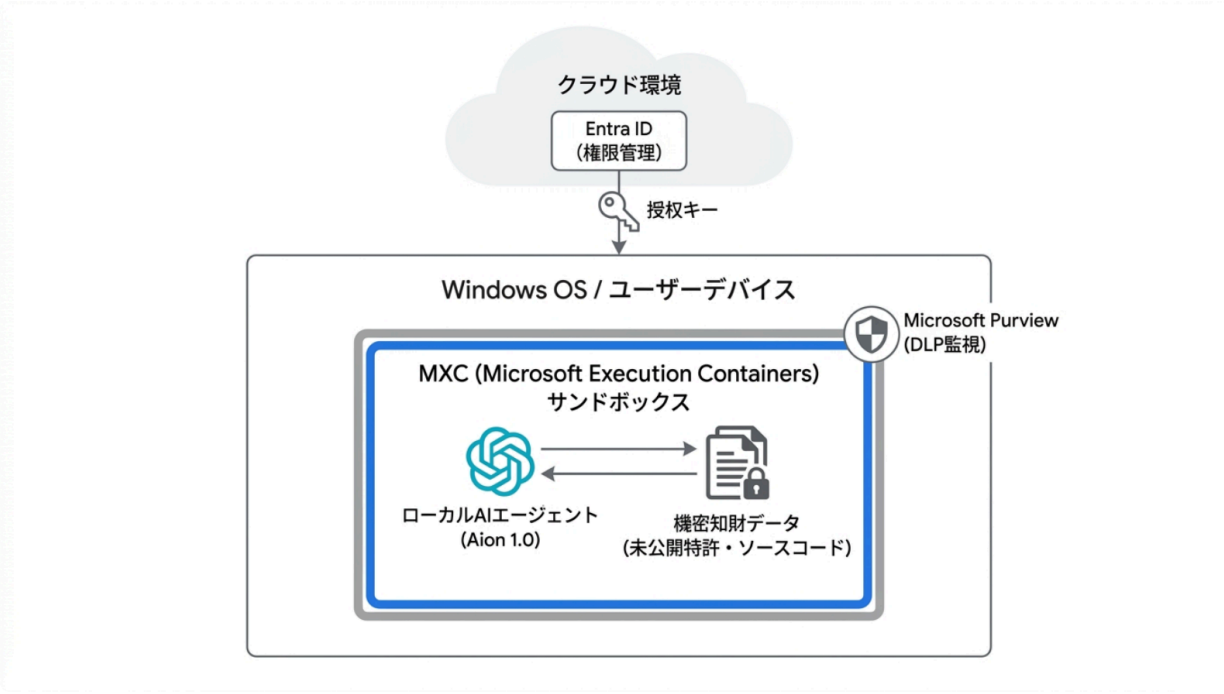
ント **(Microsoft Discovery)**	のオーケストレーション、実験データの反復分析。	ロセスの反復、R&D部門から知財部門へのシームレスな発明情報の受け渡し。	プライズグレードの科学プラットフォーム。

3. エッジとクラウドを横断する機密情報保護と実行環境

3.1. Windowsの「エージェントAIプラットフォーム」化とMXCによるサンドボックス化

特許明細書のドラフティングや発明発掘において、外部のAIモデルにデータを送信することは、特許法上の新規性喪失リスクや営業秘密の漏洩リスクに直結する。このため、多くの企業はAIの利用を公開情報に限定するか、厳格に隔離されたオンプレミス環境に限定してきた。Build 2026では、この課題に対する技術的ブレイクスルーとして、Windows自体を「AIエージェントの構築と実行に最適なOSプラットフォーム」へと進化させる方針が打ち出された[4]。
その中核となるのが、早期プレビュー版のSDKとして発表された「Microsoft Execution Containers (MXC)」である。MXCは、WindowsおよびWindows Subsystem for Linux (WSL) 上で稼働する、ポリシー駆動型の実行レイヤーである[4]。AIモデルが生成した未信頼のコードやツール出力、プラグインなどを、プロセス分離やセッション分離といった分離技術を用いて、安全なサンドボックス環境で実行することを可能にする[4]。知財業務においては、例えばエージェントに自社のソースコード（営業秘密）と競合他社の特許クレームを比較させ、特許侵害のリスクを検証させるといったタスクが想定される。MXCを利用することで、エージェントは指定されたファイルパスのみにアクセスし、ネットワーク通信を完全に遮断された状態でローカル推論を行うことができる[4]。これにより、分析対象の機密データがクラウド上のモデル学習に利用されたり、外部のネットワークに流出したりする物理的・システム的リスクを根本から排除することが可能になる。MXCの設計思想は、オペレーティングシステムによって強制される境界内部でエージェントを走らせることで、デバイス上のファイルアクセスやネットワークインタラクションに伴うリスクを劇的に低減することにある[8]。

機密知財情報を保護する次世代エージェントAI実行アーキテクチャ



Windows OSレベルでの分離技術（MXC）とEntra IDによるアイデンティティ管理により、エージェントAIは未公開の発明データや営業秘密にアクセスする際、厳密なサンドボックス内でタスクを実行する。これによりクラウドへの意図せぬデータ流出を防ぐ。

3.2. Aion 1.0とProject Solaraが描くローカル推論とエージェントOSの未来

ローカル環境におけるエージェントAIの実行をさらに強力に後押しするのが、新たに発表された140億パラメータの推論・ツール呼び出しモデル「Aion 1.0 Plan」である。32Kのコンテキスト長を持つこのモデルは、対応デバイスのWindowsに標準搭載され、デバイス上で直接エージェント的ワークフローを完結させることができる[4]。これにより、知財担当者はネットワークから切断された機密環境下でも、膨大な特許公報のローカル推論や、自社発明のクレーム分析、サブエージェントのオーケストレーションを遅延なく、かつ完全にセキュアに行うことが可能となる。
さらに長期的なプラットフォームの進化として、Build Liveで初公開された「Project Solara」は極めて重要である[4]。これはAndroidベースのソフトウェアプラットフォームであり、Microsoftはこれを「オープンでマルチエージェントな世界のために設計されたチップ・トゥ・クラウドのプラットフォーム」と呼称している[4]。将来的に、スマートフォンやタブレットなどのモバイルデバイス上でも、複数の特化型エージェント（例えば、発明者の音声を記録・構造化するエージェントと、関連する先行技術をリアルタイムで検索するエージェント）がセキュアに連携し、場所を選ばずに知財業務を遂行できる環境が構築されることを示唆している。

3.3. Windows 365 for Agentsを用いたレガシーシステムとの統合

知財業務においては、各国の特許庁が提供するレガシーなデータベースや、電子出願ポータルなど、最新のAPIが提供されていないWebシステムとの連携が不可避である。このような人間の介入や複雑なUI操作を必要とするタスクに対して、「Windows 365 for Agents」が解決策を提供する。これはMXCのクラウド側対応機能であり、エージェント専用の完全に隔離されたCloud PC（仮想Windowsデスクトップ）をプロビジョニングし、Windowsセッション内でエージェントに直接UI操作を実行させるものである[4]。
エージェントがタスクを実行する際のみCloud PCをチェックアウトし、完了後にチェックインするモデルを採用することで、リソース効率を最大化している[10]。知財部門はMicrosoft Intuneのプロビジョニングポリシーを通じてこれらのCloud PCを管理できるため、エージェントが海外の特許データベースを自動巡回してステータスを取得する際にも、組織のセキュリティポリシー（Entra IDによる条件付きアクセスやネットワーク制限など）を完全に適用・監視することができる[4]。また、「Project Opal」を通じたMicrosoft 365 Copilot内での動的エージェントワークフローのオーケストレーションや、Copilot Studioからの直接操作もサポートされており、レガシーシステムと最新のAIを安全に橋渡しする重要なインフラとなる[10]。

実行環境レイヤー	コアテクノロジー	知財システムにおける主要な利点とユースケース
オンデバイス分離 (ローカル)	Microsoft Execution Containers (MXC)	未公開ソースコードと特許クレームのローカル比較分析。ネットワーク遮断環境下での安全なコード検証。
オンデバイス推論 (ローカル)	Aion 1.0 Plan	14Bパラメータによる高精度のローカルテキスト推論。機密文書の要約やドラフト作成のオフライン処理。
クラウド分離 (仮想デスクトップ)	Windows 365 for Agents	API非対応の各国の特許庁データベースの自動巡回、電子出願ポータルにおけるUI自動操作。
次世代OSアーキテクチャ	Project Solara	モバイル環境におけるマルチエージェントの安全な連携（発明者インタビュー中のリアルタイム先行技術検索など）。

4. 知財情報の統合と「Microsoft IQ」によるコンテキストの変革

エージェントが真に有用なタスクを実行するためには、企業の過去の開発履歴、蓄積された知財ポートフォリオ、さらには競合他社の動向といった「文脈（Context）」を深く理解している必要がある。Build 2026では、この文脈基盤として、GitHub Copilot、Microsoft Foundry、およびCopilot Studioを横断して利用可能な「Microsoft IQ」プラットフォームが一般提供された[5]。

4.1. Work IQとFabric IQによる社内知財資産の構造化

知財業務の起点は、常に社内の研究開発活動にある。「Work IQ」は、Microsoft 365や組織システム内の人々、メール、ドキュメント、会議、そしてそれらがどのように繋がっているかを意味的に理解する職場インテリジェンスレイヤーである[5]。知財担当者は、新たに一般提供されるWork IQ APIsを利用することで、「どの研究チームが現在どの技術領域で最も活発に議論しているか」「特定の発明に関連する過去の会議録や設計書はどこにあるか」をエージェントに自律的に分析させ、発明の萌芽を従来よりも遥かに早期に特定することが可能になる[5]。

一方、「Fabric IQ」は、企業の構造化されたビジネスデータに対する共通のセマンティック（意味論的）基盤を提供する[5]。自社の特許管理データベース（IPMS）に蓄積された書誌事項、維持年金データ、ライセンス契約のメタデータなどをFabric IQを通じて統合することで、エージェントは「過去5年間で最も収益を生み出している特許ファミリーの傾向」といった高度な経営的問いに対して、データに基づいた推論を行うことができる。

4.2. Foundry IQとWeb IQを用いた動的IPランドスケープ

社内データの理解に加えて、広大な外部データのリアルタイムな把握が不可欠である。「Foundry IQ」は、エンタープライズナレッジとライブWeb全体にわたる検索計画（リトリーバル・プランニング）を可能にし、これらを統合する役割を果たす[5]。そして、今回新たに発表された「Web IQ」は、AIファーストのWeb検索スタックであり、モデルに依存せず、MCP（Model Context Protocol）ネイティブに構築された最速の現実世界のグラウンディングを提供する[5]。

これらのIQレイヤーを統合することで、知財部門のAutopilotsは、「自社の非公開の研究データ（Work/Fabric IQ）」と「世界中の特許データベース、学術論文、技術ニュース（Web IQ）」を常時照合し、動的なIPランドスケープ（特許網の俯瞰図）やFTO（侵害予防調査）分析を継続的に更新し続けることが可能となる。知財担当者は、AIに都度「調査を指示する」のではなく、AIが構築・更新し続ける「最新の知財リスク・機会ダッシュボードを監視・評価する」オーケストレーターへと役割を変えることになる。

5. Agentic R&Dの加速に伴う知財戦略の根本的再考

5.1. Microsoft Discoveryがもたらす発明創出の指数関数的増加

Build 2026における最も注目すべき発表の一つが、科学ワークフローのためのエンタープライズグレードのエージェントAIプラットフォーム「Microsoft Discovery」の一般提供開始である[1]。Azure上に構築されたこのプラットフォームは、BHP社が数年かかっていた銅リーチング（浸出）ソリューションの

発見を数ヶ月に短縮し、Syensqo社が半導体R&Dを加速し、GSK社が創薬プロセスを劇的に反復しているという圧倒的な実績を示した[5]。
この研究開発の「エージェント化（Agentic R&D）」は、知財部門に対してパラダイムシフトを強制する。研究開発のサイクルが数年から数ヶ月へと短縮されることは、発明の創出ペースが爆発的かつ指数関数的に増加することを意味する。従来の、研究者からの「発明届出書の提出」を待ってから人間がインタビューを行い、特許性を評価するというリアクティブな知財実務のペースでは、Agentic R&Dのスピードに追従することは物理的に不可能である。知財部門は、自らもAgent 365 SDKなどを活用してカスタマイズしたエージェントAIを導入し、R&D部門のDiscoveryプラットフォームとAPIレベルで連携する「リアルタイム発明発掘・監視エージェント」を稼働させる必要がある。

5.2. 量子コンピューティング（Majorana 2）を見据えた特許ポートフォリオ戦略

さらに、カンファレンスの基調講演では、次世代量子コンピューティングチップ「Majorana 2」が発表され、平均量子ビット寿命が20秒、インスタンスが最大1分と、前世代の1000倍の信頼性を達成したことが報告された[5]。Microsoftは、エージェントAIの支援により「2029年までに手のひらサイズのチップ上で100万量子ビットのスケーラブルな量子マシンを実現する」という明確なタイムラインを提示している[5]。
知財の観点から見れば、これは「耐量子暗号アルゴリズム」「量子化学シミュレーションによって発見された新素材」や「量子機械学習」に関する特許出願競争が、今後数年で劇的に激化することを示唆している。知財部門は、エージェントAIを活用して現在の技術動向を監視するだけでなく、2029年のスケーラブル量子時代を見据え、自社のコア技術が量子コンピューティング環境下でどのように拡張されるかを予測し、先回りして上位概念化された特許網を構築する戦略的思考（フォアキャスティング）が強く求められる。

エージェントAI基盤テクノロジーの飛躍的パフォーマンス指標

Build 2026で発表された各インフラ層のパフォーマンス指標。データウェアハウスのクエリ速度から量子ビットの信頼性、そして自律型セキュリティエージェントの驚異的な精度に至るまで、全方位でインフラストラクチャの性能が底上げされている。

データソース: Microsoft Blog, Microsoft News, Microsoft Security Blog

6. 開発者ツールとインフラの進化：知財システムの自製と運用

知財部門がAI時代に適応するためには、市販のツールを利用するだけでなく、自社の特殊な業務フローや独自の評価基準に合わせた知財特化型エージェントを自製（内製化）する能力が問われる。Build 2026では、これを強力に支援する開発者ツールとバックエンドインフラの進化が多数発表された。

6.1. Copilot StudioとAgent 365 SDKによる知財特化型エージェントの開発

企業内でのエージェント開発において、ローコードからプロコードまでをカバーする階層的なアプローチが提供されている。Microsoft Copilot Studioは、新しいナレッジタイプや洗練されたツールのサポート、評価機能のサポートを追加し、Agent Builderで構築されたエージェントの拡張をさらに容易にした[12]。これにより、プログラミング経験の少ない知財担当者でも、社内の過去の特許明細書データや審査基準のガイドラインを読み込ませたカスタムエージェントを迅速に構築できる。
より高度な制御が必要な場合、一般提供が開始された「Agent 365 SDK」が利用可能である[10]。このSDKは、C#、JavaScript、Pythonをサポートし、メッセージの受信、正規化、ルーティングを行うための通信レイヤーを提供する[10]。AIアグノスティックな設計であるため、Azure AI FoundryやSemantic Kernelなど、基盤となるAIモデルを柔軟に差し替えることが可能である[10]。これにより、開発者はマルチチャネル（Teamsや社内ポータル等）でのインタラクションや状態管理といった煩雑な実装から解放され、エージェントのコアロジック（例えば、知財価値評価アルゴリズムの実装など）にのみ集中することができる。

6.2. Intelligent TerminalとWindows Development Skills

知財部門を支援する社内ITエンジニアにとって、開発環境（インナーループ）の劇的な改善は見逃せない。新たに一般提供された「Windows Development Skills」は、エージェントにWindowsネイティブアプリ開発の構造化された知識（WinUI 3スキルなど）を提供し、設計からビルド、テスト、パッケージングまでのワークフローを支援する[4]。
さらに、実験的オープンソースとして公開された「Intelligent Terminal 0.1」は、Windows Terminalにネイティブなエージェント統合（GitHub Copilot CLI等）をもたらす[4]。ビルドエラーやGitのステータスといったシェルのコンテキストを直接読み取り、エラー原因の特定から修正の実行までをエージェントがペアプログラマーとして支援する[4]。また、GitHubにチューニングされた新たなAIコーディングモデル「MAI-Code-1」がCopilotおよびVS Codeに導入されており、独自システムの開発速度を飛躍的に高める[1]。

6.3. RayfinとAzure HorizonDBによるスケーラビリティの確保

プロトタイプとして開発した知財エージェントを、全社規模の本番環境（プロダクション）へ展開する際のスケーラビリティとインフラ管理も重要な課題である。Microsoftは、Fabricを本番対応のアプリケーションバックエンドにするための新しいSDKおよびCLIである「Rayfin」を発表した[13]。これにより、インフラストラクチャを管理することなく、GitHubベースのワークフローを通じてプロトタイプから本番環境へシームレスに移行できる[5]。
さらに、膨大な特許データや非構造化データを処理するためのAIアプリケーション向けに設計された新しいPostgreSQLデータベース「Azure HorizonDB」がパブリックプレビューとして公開された[13]。内部テストにおいて、類似の自己管理型セットアップと比較して3倍以上のスループットを達成しており、最も要求の厳しいデータベース要件を満たす[5]。また、GPUアクセラレーションを活用したFabric Data Warehouseは、共通のレポート作成やAI主導の分析シナリオにおいて最大7倍高速に実行され、UNC Healthの事例では既存ワークロードで最大5倍のクエリ速度向上が確認されている[11]。これらのバックエンドインフラの進化により、数百万件の特許データをリアルタイムで分析する高度なIPランドスケープシステムの構築が現実のものとなる。

7. Agentic DevSecOpsとシャドーAIのリスク管理体制

エージェントが自律的にコードを書き、データを検索し、ツールを実行する世界において、「AIが意図

せず他社の特許を侵害するコードを生成するリスク」や、「AIが未公開の知財データを外部のAPIに送信してしまうリスク」は、企業の存続に関わる致命的な脅威となる。Microsoft Build 2026では、こうしたAgentic AI特有のリスクに対処するための包括的な「DevSecOps」の枠組みが発表された。

7.1. MDASHとDefender AI Model Scanningによるコード生成とモデルの監査

ソフトウェア特許の分野において、生成AIが既存のオープンソースライセンスを侵害するコードや、他社の特許技術を模倣したコードを生成してしまうリスクは、知財部門にとって頭痛の種である。このコード生成エージェントのリスク管理として、「Microsoft Security multi-model agentic scanning harness（開発コード名：MDASH）」が極めて重要な役割を果たす[5]。

MDASHは、単一のAIモデルに依存するのではなく、100以上の専門化されたAIエージェント（監査役、討論役、証明役など）を統合したアンサンブル・モデル・パイプラインである[10]。このシステムは、生成されたコードやソフトウェアインフラに対して、データの流れ、ビジネスロジック、エクスプロイト（脆弱性の悪用）チェーンを推論し、コンテキストを考慮した修正案をDefenderポータルに直接提供する[5]。特筆すべきは、ストレージドライバに意図的に注入された21の脆弱性に対するテストにおいて、MDASHが「誤検知ゼロ（Zero False Positive）」で全ての脆弱性を特定したという実績である[10]。

また、「Microsoft DefenderとGitHub Code Securityの統合」により、ランタイムのコンテキストが開発およびセキュリティのワークフローに持ち込まれる[10]。これにより、本番環境でのエクスポージャーやデータ感度などのシグナルが自動的に付与され、修復作業の優先順位付けが可能となる[10]。さらにプレビュー版として発表された「Defender AI Model Scanning」は、プラットフォームネイティブか持ち込み（BYOM）かを問わず、デプロイされる前にモデル成果物を検査し、脆弱または侵害されたモデルを検出・ブロックする[10]。これにより、悪意のあるバックドアが仕込まれたモデルを通じて知財データが窃取されるサプライチェーンリスクを低減できる。

7.2. Microsoft Purviewによるランタイム DLPと情報漏洩防止

知財業務においてエージェントAIを利用する際の最大の懸念の一つが、ユーザー（発明者や知財担当者）が不用意にプロンプト内に未公開の発明内容やソースコードを入力してしまう「プロンプト・インジェクション型のリスク」である。

この課題に対し、Build 2026では「Microsoft Purview for Agents」を通じたデータ損失防止（DLP）機能の強化が発表された[10]。Purviewは、GitHub Copilot、Claude Code、OpenAI Codex、そしてOpenClawといったローカルおよびエンドポイントのエージェントに対しても、データの可視性と保護機能を提供する[10]。具体的には、ランタイムDLPコントロールにより、エージェントの実行フロー内でプロンプトやツール呼び出しをリアルタイムに検査し、機密情報（Sensitive Information Types: SITs）が含まれている場合は、モデルによって処理される前に自動的にブロック・監査する[10]。

新たにパブリックプレビューとなる「Microsoft Purview SDK for.NET」を利用すれば、開発者は数行のコードを追加するだけで、非Microsoftプラットフォーム上に構築されたAIアプリに対してもこの強力なコンテンツスキャンとDLPチェックを実装できる[10]。これにより、企業は「未公開特許情報の外部流出」という最悪の事態をシステムレベルで防止することが可能になる。

7.3. Agent 365 Agent Registryによるガバナンスの徹底

各事業部門や研究チームが独自のローカルエージェント（シャドーAI）を無秩序に運用する「エージェ

ント・スプロール現象」は、知財情報の管理において重大な盲点となる。これを統制するため、「Agent 365 Agent Registry」が提供される[10]。これはMicrosoft Defender、Entra、Intuneの連携により、ネットワーク上で発見された未管理のローカルエージェント（コーディングエージェントやMCPサーバーを含む20種類以上）を表面化し、その活動を監査・統制する機能である[10]。知財部門は情報システム部門と連携し、このRegistryとASSERT（Adaptive Spec-driven Scoring for Evaluation and Regression Testing）を利用したポリシー駆動型の安全性評価フレームワークを活用して、知財ポリシーに準拠したエージェントのみが稼働する環境を維持しなければならない[5]。

7.4. 音声・画像生成AIモデルにおける革新と保護機能

テキストベースの推論モデルだけでなく、Build 2026では7つの新しいAIモデルが発表され、その中にはクリエイティブな側面を引き出す画像生成モデル「MAI-Image-2.5」が含まれる[1]。このモデルは、GoogleのNano Bananaを凌駕する性能を持つと報告されている[3]。知財実務において、特許図面の自動生成や、商標出願のためのロゴデザインのバリエーション作成などへの応用が期待される。

さらに、競合モデルの5倍の速度を持つ新しい文字起こし（トランスクリプション）モデルや、クローニングに対する保護機能を備えた高速でインタラクティブなAI音声モデルも発表された[1]。発明者とのヒアリングにおいて、これらのモデルを活用することで、インタビュー内容をリアルタイムで極めて正確にテキスト化し、直ちにエージェントが特許クレームのドラフトを作成するプロセスが実現する。同時に、音声クローニング保護機能により、ディープフェイク技術を用いた社内でのなりすましや、発明者の発言の改ざんといった証拠保全上のリスクを軽減できる点は、法務的観点からも高く評価できる。

セキュリティ・ガバナンス機能	保護対象・監視対象	知財業務における具体的な保護効果
MDASH (Agentic Security)	ソフトウェアインフラ、生成コードの脆弱性	オープンソースライセンス違反のコード生成や、特許侵害コードの混入の自律的な検出と修正。
Defender AI Model Scanning	プラットフォームモデル、BYOM（持ち込みモデル）	悪意のあるバックドアが仕込まれたモデルによる、知財データの外部への不正送信の防止。
Microsoft Purview (ランタイムDLP)	プロンプト、エージェントのツール呼び出し	未公開の発明アイデアや営業秘密を含むプロンプトが、意図せず外部モデルで処理されることの遮断。
Agent 365 Agent Registry	シャドーAI、ローカルエージェント (OpenClaw等)	企業ポリシーに準拠しない野良エージェントの発見と、

		Intuneを通じた実行のブロック。
音声クローニング保護機能	音声モデル、トランスクリプションデータ	発明者インタビューの記録に対するなりすましの防止、証拠保全能力の向上。

8. 結論：オーケストレーターとしての知財専門家の進化

Microsoft Build 2026が提示した「エージェントAI元年」のビジョンは、AIが単なる「作業効率化のツール」から、「自律的に思考し、行動し、ワークフローを完遂するデジタル従業員（Autopilots）」へと進化したことを意味している。Rayfin SDKを用いたバックエンドインフラの管理から、FabricやHorizonDBを通じたデータの統合化まで、開発者がプロトタイプからプロダクションへと移行するための障壁は極限まで引き下げられた[5]。

このパラダイムシフトは、知財業務のあり方を根本から覆す。先行技術の検索、クレーム案の作成、データ入力といった個別最適化されたタスクは、安全なサンドボックス（MXC）内で稼働し、組織の文脈（Microsoft IQ）を深く理解した複数のエージェント群へと完全に委譲されることになる。R&DのスピードがAgentic AIによって劇的に加速する中、知財部門が旧来の労働集約的なアプローチを維持することは、企業のイノベーションサイクルにおける致命的なボトルネックとなる。

今後、知財専門家（弁理士、知財部員）に求められる役割は、個々の明細書を執筆する「作業者」から、高度な専門知を用いて複数のエージェントを統括・指揮し、知的財産の創出から権利化、活用までのエコシステム全体を設計する「オーケストレーター」へと移行する。エージェントが動的に提示する複雑なIPランドスケープやリスク分析を解釈し、経営戦略やR&D戦略とアラインメントを取るための高度な戦略的判断こそが、人間の知財専門家に残される最大の付加価値となる。

企業は直ちに、エージェントAIを知財業務に統合するためのロードマップを策定すべきである。その際、単に新しいAIモデルを導入するだけでなく、Entra IDによるアイデンティティ管理、MXCによるサンドボックス化、そしてPurviewによるDLPといったガバナンスとセキュリティの基盤を同時に整備することが、機密性を命綱とする知財業務においては不可欠である。Agentic AIの自律的な処理能力と、エンタープライズグレードの堅牢なセキュリティ基盤を融合させることで、知財部門は従来のコストセンターから、イノベーションを先導し企業の競争優位性を担保する、真のプロフィットセンターへと進化を遂げることができるだろう。

引用文献

1. Microsoft Build 2026 Kicks Off Today: Live Updates on Copilot AI and Dev Tools - CNET, 6月 3, 2026にアクセス、https://www.cnet.com/news-live/microsoft-build-2026-news-ai-copilot/
2. Microsoft Build 2026、今年はサンフランシスコで2日間の開催に - ITmedia NEWS, 6月 3, 2026にアクセス、https://www.itmedia.co.jp/news/articles/2603/04/news086.html
3. Microsoft Build 2026: Everything Microsoft is Unveiling Today Live | PCMag, 6月 3, 2026にアクセス、

https://www.pcmag.com/news/microsoft-build-2026-live-san-francisco-everything-microsoft-is-unveiling
4. At Build 2026, Microsoft Sets Up Windows as an OS for AI Agents ..., 6月 3, 2026にアクセス、https://visualstudiomagazine.com/articles/2026/06/02/at-build-2026-microsoft-sets-up-windows-as-an-os-for-ai-agents.aspx
5. Microsoft Build 2026: Be yourself at work, 6月 3, 2026にアクセス、https://blogs.microsoft.com/blog/2026/06/02/microsoft-build-2026-be-yourself-at-work/
6. Introducing Microsoft Scout: Your always-on personal agent ..., 6月 3, 2026にアクセス、https://www.microsoft.com/en-us/microsoft-365/blog/2026/06/02/introducing-microsoft-scout-your-always-on-personal-agent/
7. Microsoft、自律エージェント「Scout」発表 OpenClawベースでMCP対応 - ITmedia AI＋, 6月 3, 2026にアクセス、https://www.itmedia.co.jp/aiplus/article/2606/03/2000000049/
8. Everything we learned from the Microsoft Build 2026 keynote | Mashable, 6月 3, 2026にアクセス、https://mashable.com/tech/microsoft-build-2026-keynote-everything-we-learned
9. Microsoft introduces Scout, an OpenClaw-based “always-on” personal AI agent, 6月 3, 2026にアクセス、https://msdynamicsworld.com/story/microsoft-introduces-scout-openclaw-based-always-personal-ai-agent
10. Microsoft Build 2026: Securing code, agents, and models across the development lifecycle, 6月 3, 2026にアクセス、https://www.microsoft.com/en-us/security/blog/2026/06/02/microsoft-build-2026-securing-code-agents-and-models-across-the-development-lifecycle/
11. Microsoft Build Live, 6月 3, 2026にアクセス、https://news.microsoft.com/build-2026-live-blog/microsoft-build-2026-live/
12. Overview of Microsoft Copilot Studio 2026 release wave 1, 6月 3, 2026にアクセス、https://learn.microsoft.com/en-us/power-platform/release-plan/2026wave1/microsoft-copilot-studio/
13. Microsoft Build 2026: Building agentic apps with Microsoft Fabric and Microsoft Databases, 6月 3, 2026にアクセス、https://azure.microsoft.com/en-us/blog/microsoft-build-2026-building-agentic-apps-with-microsoft-fabric-and-microsoft-databases/