ChatGPT

OpenAI DevDay 2026発表と知財・法務実務への影響分析

エグゼクティブサマリ

調査基準日：2026年9月30日（日本時間）。 OpenAI DevDay 2026は米国時間2026年9月29日にサンフランシスコで開催され、基調講演は同日10:00 PT（日本時間9月30日2:00）に開始された。OpenAIは公式リキャップで20件超の発表をまとめている。一方、本調査時点では、**基調講演の公式フル動画は確認できるものの、公式の全文トランスクリプトおよび正式なスライドデッキは確認できなかったため、該当部分は「不明」とする。** 基調講演の公式動画メタデータではSam Altman、Romain Huet、Tejal Patwardhan、Holly Liの出演が示されている。 [1]

- **最大の変化は「生成」から「継続的に行動するエージェント」への移行である。** Dots、Agents API with Computer Use、MCP Events、Team Tasks、Codex Security Cloudは、AIが文書を作るだけでなく、クラウドPC、ブラウザ、GitHub、Slack、Teams、業務アプリを介して継続的・自律的に仕事を実行する方向を明確にした。知財部門にとって、従来の「プロンプトに秘密情報を入れない」という統制だけでは不十分となり、**AI identity、最小権限、承認ゲート、ツール単位の権限、エージェント行動ログ**が新たな統制単位になる。 [2]

- **GPT-6.1 Solは知財実務をかなり深いところまで自動化し得る。** OpenAIは、GPT-6.1 Solについて、コード、複雑なPDF、コンピュータ操作、多段階業務でGPT-6 Solを大きく改善し、GPT-6 Astraに近い性能を低コストで提供するとしている。またPreparedness評価ではCybersecurityを「Critical」と扱っている。特許調査・発明抽出・契約レビュー・OSS解析・ソースコード監査を高速化できる反面、**誤った法的判断、過剰な権限による情報持出し、権利侵害コードの採用、意図しないシステム変更**の影響範囲も拡大する。 [3]

- **データ保護は大幅に強化されたが、「ZDR＝あらゆるデータがどこにも残らない」ではない。** APIデータは原則として明示的なopt-inなしにモデル学習へ使われない。通常の対象APIでは不正利用監視ログが概ね30日保持され、Zero Data Retention（ZDR）では適格コンテンツをそのログから除外できる。他方、Agents、Conversations、Files等には削除まで残るapplication stateがあり、ZDR非適格の機能もある。Private Safety Processing（PSP）では、安全上選択された記録が顧客管理の暗号化ストレージに最長30日保持され得る。したがって**エンドポイント単位でデータフローと保持期間を確認する必要がある。** [4]

- **DevDay 2026に伴う出力所有権・商用利用条件の明示的な変更は、本調査では確認できなかった。** 現行のOpenAI Services Agreementでは、顧客はInputを保持し、法律上許される範囲でOutputを所有し、OpenAIもOutputに関する権利を顧客へ譲渡する。ただしOutputの独自性は保証されず、顧客はInputに必要な権利を有する責任、Outputの適切性を評価する責任を負う。一定のOutput IP補償は存在するが例外が広く、Beta Servicesも原則対象外である。したがって「OpenAIがOutputを契約上譲渡した」ことと、**生成物に法定の著作権が成立すること、第三者権利を侵害しないこと、特許FTOが確保されることは別問題**として扱うべきである。 [5]

- **2026年の規制・判例環境は、企業に「出所・権限・人間関与を証明できるAI利用」を求める方向へ進んでいる。** EUではGPAI規則が2025年8月2日から適用され、新規モデルについて2026年8月2日から執行可能となり、OpenAIはGPAI Code of Practiceの署名者である。日本ではAI法が2025年9月1日に全

面施行され、2026年7月には第 II 期人工知能基本計画が閣議決定された。さらにDevDayと同日の2026年9月29日、米第3巡回区控訴裁判所はThomson Reuters対Ross IntelligenceでAI学習に関するfair use否定の判断を維持したと報じられており、**「AIだから学習・利用が当然に適法」という前提は実務上極めて危険**である。 [6]

調査前提と主要発表

OpenAIの公式イベントページによれば、DevDay 2026は2026年9月29日にFort Mason, San Franciscoで開催され、Opening Keynoteは10:00 PT、Closing Sessionは16:00 PTだった。その他のセッションも録画して後日OpenAIサイトへ掲載すると案内されているため、**2026年9月30日時点の本報告は「発表直後版」であり、今後追加されるセッション動画・技術文書によって補足が必要になる可能性が高い。** [7]

公式基調講演・主要発表の要約

発表名	日時	登壇者	主要技術・ポリシー	潜在的な知財・法務影響
Opening Keynote / DevDay 2026	2026/9/29 10:00 PT、2026/9/30 2:00 JST	Sam Altman、Romain Huet、Tejal Patwardhan、Holly Liが公式動画メタデータに掲載。個々の製品発表担当は**不明**	ChatGPT、Codex、モデル、エージェント、企業向けプライバシーを横断して20件超を発表	AI利用規程を「生成AI」単位ではなく「モデル＋エージェント＋接続ツール＋データストア」単位へ再設計する必要 [8]
GPT-6.1 Sol / Ultrafast	2026/9/29	個別登壇者は**不明**	Agentic coding、computer use、professional workを強化。APIモデルIDは `gpt-6.1-sol`。標準価格は入力$2/M、cached input $0.10/M、出力$10/M。Ultrafastは Codex最大8倍、API最大6倍の生成速度	発明・コード・契約・調査の自動化範囲拡大。高速化により人間レビューを飛ばす誘因も増えるため、レビューを処理速度ではなくリスクで発火させるべき [9]
Private Intelligence	2026/9/29	**不明**	ZDR＋Private Safety Processing。OpenAI personnelに基礎コンテンツを見せず安全レビュー。Private Inferenceは2026年秋preview予定でconfidential computingと検証可能な統制を組み合わせる	特許未公開情報、M&A、ソースコード等への利用可能性を高めるが、対象endpoint・保存場所・例外を案件ごとに確認する必要 [10]

発表名	日時	登壇者	主要技術・ポリシー	潜在的な知財・法務影響
Dots	2026/9/29	**不明**	GPT-6 Astraベースのalways-on agent。自身のcloud computer/browserを持ち、4,000超のappsへの接続、複数案件の継続処理、フィードバック学習	「機密を入力したか」だけでなく「何を閲覧できるか」「誰の権限で何を実行したか」が営業秘密管理・アクセス統制の核心になる [11]
Decisions API	2026/9/29	**不明**	Lunaを有限の事前定義回答に集中させ、text/imageから分類・routing・agent next actionを返す。発表日はlimited preview	自由生成より決定空間を限定でき、法務ワークフロー統制に適する一方、誤分類が自動実行へ直結する場合は高リスク [12]
Agents API with Computer Use	2026/9/29	**不明**	software操作、multi-agent、tool search/calling、context compaction。基盤をOpenAIがホスト	特許・法務AIが調査から実行まで一気通貫になる。資格情報、電子署名、出願、契約送信等には明確なhuman-in-the-loopが必要 [13]
Codex Cloud / Code Review / Codex Security Cloud	2026/9/29	**不明**	reusable cloud environments、GitHub/GitLab review、repository全体の継続scan、fix生成	OSSライセンス、第三者著作権、脆弱性・営業秘密、発明者記録までコードガバナンスと知財ガバナンスの統合が必要 [12]
Plugins / Sites / MCP Events	2026/9/29	**不明**	ChatGPT内native panels、plugin discovery、ユーザーによるアクセス承認、Sites内plugin、app event起点のautomation	OpenAIとの契約だけでなくplugin/MCP先の利用規約・DPA・保存・国外移転・再学習条件をvendor chainとして管理する必要 [14]

発表名	日時	登壇者	主要技術・ポリシー	潜在的な知財・法務影響
Space / Pages / Slides / Teams	2026/9/29	**不明**	人間とagentの共同文書編集、shared knowledge、複数agentのスライド編集、scheduled/event-triggered tasks	「誰が何を創作したか」の境界が曖昧化。著作者性、職務著作、発明者性、承認証跡のためversion/provenance情報の保存が重要 [15]
Slack / Teams / Meetings	2026/9/29	**不明**	@ChatGPTが管理者・ユーザー権限のtoolsを利用。Meetingsは議事メモをSpaceへ保存し、音声はnote完成後削除・再生不能	チャット内の秘密情報への横断アクセスと、会議原音が残らないことによる証拠・record retention上の課題が生じる [16]
OpenAI Marketplace / Sign in with ChatGPT	2026/9/29	**不明**	Enterprise commitmentをHarvey、Legora、Adobe、Salesforce等の承認partner softwareにも適用可能	調達は容易になるが、パートナーごとのデータ処理・知財・補償条件がOpenAI本体と同一になるとの公式説明はなく、別契約としてレビューするのが安全 [16]

トランスクリプト／スライドに関する調査結果。 OpenAI公式の「FULL Keynote」動画および公式リキャップは確認できたが、2026年9月30日時点で、本調査では全文公式トランスクリプト、正式スライドデッキ、各技術breakoutの完全な講演録を確認できなかった。したがって、上表の内容はOpenAIの公式recap、個別製品ページ、Developer documentation、Deployment Safety Hubを優先して復元しており、未確認部分は「不明」とした。 [17]

技術変更点と知財インパクトの詳細分析

モデル能力と出力制御

GPT-6.1 SolについてOpenAIは、実コードベースを対象とするsoftware-engineering、複雑なPDFを読むprofessional work、多段階business workflow、computer useでGPT-6 Solを改善したとしている。とりわけ「文書を読む」だけでなく「GUIやtoolを動かして仕事を完了する」能力の向上は、知財業務でのAIの位置づけを**drafting assistantからsemi-autonomous operatorへ変える**。 [18]

これは、例えば次のような実務を現実的にする。

知財業務	DevDay後に現実味が増す自動化	主なリスク
特許	発明届の整理、先行技術資料収集、クレーム候補生成、競合特許・製品情報監視	発明者認定の混同、未公開発明の漏洩、不正確な先行技術評価、FTOの過信

知財業務	DevDay後に現実味が増す自動化	主なリスク
著作権	ソース・文書の比較、類似表現検出、素材台帳作成、license review	AI output ownershipと法定著作権の混同、類似表現の採用
営業秘密	レポジトリ横断検索、Slack/Teams/Docsから情報収集	agentが「秘密の存在を知る」だけでなく外部サービスへ転送するリスク
契約	契約レビュー、修正案、承認routing、締結準備	権限外の約束、古いプレイブック、誤った自動承認
コンプライアンス	継続monitoring、ticket生成、repository scan	誤検知・見逃し、監視データ自体の個人情報化
訴訟・証拠	e-discovery補助、時系列作成、文書分類	hallucination、原資料とAI要約の混同、chain of custody欠落

この表のリスク評価は、OpenAIがGPT-6.1 Solでcomputer use・professional workflowsを強化し、Agents API/DotsでAIにシステム操作権限を持たせるようになったことから導く**実務上の推論**である。[19]

特に注目すべきなのが**Decisions API**である。自由文章ではなく「ユーザーがあらかじめ設定した有限の回答集合」に判断を制約できるため、「NDA要／不要」「法務承認へ／通常処理へ」「公開可／要確認」などのgatekeeper用途では、通常のgenerative completionより統制可能性が高い。ただし、その結果がAgents APIのtool callを直接起動する構成では、単なる分類誤りが実際の権限行使へ変換される。したがって、**decision confidence → human approval → execution**の三段階に分ける設計が望ましい。[12]

GPT-6.1 SolのDeployment Safety Hubは、同モデルをCybersecurityで「Critical」、Biological/Chemicalで「High」と取り扱い、GPT-6 Astraと同じsafeguard stackを適用すると説明する。また内部Codex traffic simulationでは、misaligned behaviorの評価も行っている。これはモデルが危険という単純な意味ではないが、企業利用側からみれば、**強力なagentにcredential、repository write、production、特許出願システム等を無制限に渡す設計は避けるべき**という強い示唆になる。[20]

データ利用・学習・保持

企業知財実務では、「OpenAIは学習するか」という二択ではなく、少なくとも**学習、abuse monitoring、application state、customer-side storage、plugin/MCP転送**を分けて整理すべきである。

項目	2026年9月時点の確認内容	知財実務上の評価
APIのモデル学習	APIへ送ったデータは、明示的opt-inがない限りモデルのtraining/improvementには使用しない	企業機密用途の基本線としてconsumer利用より有利[21]
Business/API契約	Customer Contentはサービス提供、法令遵守、policy enforcement、abuse防止等のために使用し、明示的同意がなければサービス改善に使用しない	NDA・営業秘密管理では有利だが、保持・tool転送は別途確認必要[22]
個人向けTerms	コンテンツをサービス提供・維持・開発・改善等に利用し得る。training opt-outが用意されている	会社の秘密情報を個人向けaccountへ投入しないことを社内規程化すべき[23]

項目	2026年9月時点の確認内容	知財実務上の評価
通常API abuse monitoring	Chat Completions / Responses等で一般に最大30日程度のabuse-monitoring retention。対象endpointはZDR適格	「APIだから即時消去」と説明してはいけない [24]
Agents / Conversations / Files	trainingには使わないが、機能によってapplication stateが削除まで残り、ZDR非適格のものがある	Agent案件はChat Completionsと同じretention前提で評価してはいけない [24]
ZDR	適格Customer Contentをabuse-monitoring logから除外し、Responses等では `store` をfalseに強制する仕組みがある	高機密案件の標準候補。ただし全機能に自動適用されない [25]
ZDR＋PSP	personnelがunderlying contentを閲覧せずautomated safety review。選択されたinteractionは顧客管理・暗号化されたregional storageでTTL 30日となり得る	「完全にどこにも残らない」と契約・privacy noticeに記載しない [26]
Remote MCP / third-party tool	OpenAIのdata-residency条件とは別に第三者serviceのpolicyが適用され得る	plugin/MCP先をsubprocessor/vendor registryへ入れる必要 [27]
Meetings	note完成後にaudioを削除し、アクセス・再生できない	会議原音の法定・訴訟holdが必要な企業では別記録系統を設ける [16]

最重要ポイントは、「No training」と「No retention」は同義ではないことである。 OpenAIの企業/APIポリシーは原則no-trainingだが、service operation、abuse prevention、application state、customer-controlled PSP storageなど、目的・主体・期間の異なる保存が存在する。営業秘密の合理的秘密管理措置や個人情報保護の説明を作る際は、この区別を明文化する必要がある。 [28]

またGPT-6.1 SolのSystem Card Addendumは、model data/trainingについて「GPT-6 Astraと同じ種類のdataとtraining」としているが、DevDay 2026資料だけから、個々のtraining source、各sourceの権利処理、ライセンス元、opt-out反映状況を特定することはできない。したがって、**GPT-6.1 Solについての完全な学習データ一覧・各データの著作権ライセンス状況は「不明」**とするのが妥当である。 [20]

商用利用、ライセンス、出力所有権

DevDay 2026の公式recapには、Services Agreement、Terms of Use、Output ownershipそのものを変更するとの発表は掲載されていない。本調査で確認した現行Services Agreementは2026年1月1日発効のものであり、**DevDayに伴う新たな出力所有権ルールは確認できない。** [29]

Business/API等のServices Agreement上は、

CustomerはInputの所有権を保持し、Outputについて法律上許される範囲で所有し、OpenAIはOutputに有する権利をCustomerへ譲渡する。 一方で、Outputは他のユーザーへのOutputと同一・類似となる場合があり、CustomerはInputについて必要な権利・許諾を有すること、Outputの正確性・適切性を評価することについて責任を負う。 [22]

ここから重要な実務上の結論が出る。

契約上の「Output ownership」と、著作権法上の「著作物性・著作者性」は別である。

OpenAIとの二者間でOutputの権利をCustomer側へ寄せても、そもそも人間による創作的寄与が足りず法的な著作権が成立しない場合、契約譲渡によって新たな著作権が創設されるわけではない。また第三者著作物と類似するOutputが生成された場合、OpenAIとの所有関係だけで第三者侵害問題は解消しない。日本では文化庁が生成AIと著作権について現行著作権法の適用関係を整理する公式資料群を公表しており、著作権法自体も著作物・著作者の要件を別途定めている。 30

Output IP indemnityは有用だが、**全面的な「非侵害保証」ではない。** OpenAIのService Termsは、一定のAPI OutputやEnterprise向けOutputについて第三者IP claimを補償する一方、顧客が侵害を知っていた／知るべきだった場合、citation・filter・safety featureを無視した場合、Outputを変更したり他製品・サービスと組み合わせた場合、Input/fine-tuning filesへの権利がなかった場合、商標として使用した場合、Third Party Offering由来の場合などに例外を置き、Beta Servicesは原則補償外としている。 31

これはCodex運用で特に重要である。AIが生成したコードを人間が編集し、OSS、社内code、third-party libraryと組み合わせて製品へ入れる行為は通常のsoftware developmentそのものであり、補償例外との関係も確認すべきである。したがって**OpenAI indemnityがあるからSCA、OSS license scan、copyright scan、FTOを省略してよい、とはならない。** 32

法務・知財・規制リスクの評価

著作権・データセットリスク

著作権リスクは「AIへの入力」「モデル学習」「Output生成」「Output利用」の段階を分ける必要がある。特に企業利用者が直接管理しやすいのは、InputとOutput利用である。

Input側では、第三者から受領した設計図、顧客資料、licensed database、出版社コンテンツ、OSS、共同研究資料などに「AIへの入力・機械処理」まで許す権利があるとは限らない。OpenAIのServices AgreementもInputに必要なrights/licenses/permissionsを確保する責任をCustomerへ置いている。 22

Output側では、類似Outputがあり得ることをOpenAI自身が明示しているため、商標、広告コピー、ソースコード、デザイン、長文コンテンツなど重要成果物では「生成した＝自由に使える」とせず、類似性・出典・第三者権利を確認する必要がある。 22

米国判例動向は、training dataの適法性が事案依存であることを強く示す。Bartz v. Anthropicでは2025年、裁判所が一定の書籍trainingをfair useと評価する一方、海賊版書籍libraryの取得・保有について別の著作権問題を残したと報じられた。これに対しThomson Reuters v. Ross Intelligenceでは2025年の地裁判断が、競合AI legal research productのtraining用にWestlaw headnotesを用いた行為についてfair useを否定し、**2026年9月29日には第3巡回区控訴裁判所がThomson Reuters側の勝利を維持したとReutersが報じている。** 控訴審の詳細な理由は当該報道時点でsealedとされ、生成AI一般へどこまで拡張できるかはなお慎重に見る必要がある。 33

したがって企業のfine-tuning、RAG corpus、knowledge base構築については、**「インターネットで取得可能だった」ではなく、「取得・複製・AI利用・保存・再配布の権利根拠は何か」までdata lineageに持たせる**べきである。

特許・発明管理

GPT-6.1 Sol、Codex、DotsによってAIが設計変更、bug fix、アルゴリズム改良、PoC作成を継続的に行うと、「誰が発明にどのように寄与したか」の事実認定が難しくなる。OpenAI自身が、Dotsによるfeature修正、科学分析更新、Codexによるrepository-level変更をユースケースとして挙げている。[34]

したがって、発明届に従来の「発明者名、発明日」だけでなく、

使用モデル、prompt/instruction、AIが提案した構成、人間が着想した構成、人間が選択・修正した理由、実験・検証者、commit ID、日時

を残すことが望ましい。これは特許庁へそのまま提出する情報という意味ではなく、後日のinventorship・ownership争いに備えた社内証跡である。

また「AIが独立に生成した技術だから第三者特許を侵害しない」とは評価できないため、**FTOの対象は生成過程ではなく、最終的に実施する製品・方法**として維持する必要がある。特にCodexやDotsが大量の小規模featureを継続deployする環境では、「リリース前IP review」の静的な方式より、技術的重要度・市場・競合・claim proximityに基づくtrigger方式へ移行する方が現実的である。これはDevDayで示された継続的agentic developmentから導かれる実務上の提案である。[34]

営業秘密・機密情報

DevDay 2026で最も大きい営業秘密リスクは、LLM本体より**接続範囲の拡大**である。Dotsは自分のcloud computer/browserをもち、connected appsを利用し、Slack・Teams間でcontextを持ち越せる。Team TasksやMCP Eventsは新着メールやtaskをtriggerとして自動処理できる。[35]

そのため秘密管理では、従来の「AIへのコピー＆ペースト禁止」だけでは足りない。

必要なのはidentity-centric governanceである。 Agentにも固有identityを与え、人間ユーザーの全権限を継承させず、read/write/export/send/deleteを分離し、案件・repository・data roomごとにscopeを限定する。OpenAI自身もspecialist dotsについて独自identityによるaccess managementを説明している。[36]

さらに、OpenAI側ではno-training/ZDRでも、pluginやremote MCP serverへ情報が渡れば第三者policy・storageが問題となり得るため、**「OpenAIが安全だから社外提供ではない」という一括評価は避けるべき**である。[27]

証拠性・監査可能性

AI Outputは「証拠」そのものではなく、原資料から生成された二次的な推論・要約として取り扱うのが安全である。OpenAI Terms自身もOutputが不正確となり得ること、人によるreviewを含め利用目的への適切性を評価する必要があるとしている。[37]

法務・知財用途では最低限、次を残す必要がある。

```
case_id / user_or_agent_id / timestamp / model+version / system-policy version / input source IDs / tool calls / retrieved documents / output hash / human reviewer / approval decision / subsequent action
```

ここで重要なのは、**OpenAIのabuse logを自社監査ログの代替にしないこと**である。通常のAPI logは保持目的と期間がOpenAI側のabuse monitoring向けであり、ZDRを導入するとむしろOpenAI側に証拠となる

contentが残らなくなる。訴訟hold、発明者立証、契約承認、インシデント調査に必要な記録は、企業側の保存ポリシーに従って別途保全する必要がある。 38

Meetings pluginについてはさらに分かりやすい。OpenAIはnote生成後にaudioを削除し、再アクセス・再生不可と説明している。したがって、取締役会、発明評価会、重要契約交渉など原音そのものをrecords scheduleやlegal holdの対象にしたい会議では、**Meetings pluginだけをsystem of recordにしてはいけない。** 16

国内外の規制・専門家動向

日本。 2025年9月1日にAI法が全面施行され、内閣府のAI戦略ページでは2026年7月14日に第 II 期人工知能基本計画が閣議決定されたこと、AI法、AI基本計画、適正性確保指針が主要政策として整理されている。企業にとって、AI利用を単発IT procurementとしてではなく、リスク管理・説明責任・適正利用を含む継続的governance対象として扱う方向性は明確である。 39

著作権について文化庁は「AIと著作権について」の公式ポータルを設置し、2024年の「AIと著作権に関する考え方」等を公表している。日本企業はOpenAIとの契約上のOutput ownershipだけで判断せず、日本著作権法上の著作物性、第三者著作物との類似・依拠、Inputの利用権限を別に審査すべきである。 30

個人情報保護委員会も生成AI利用に関する注意喚起を行い、OpenAIに対しても注意喚起を行った経緯がある。専門家実務でも、Business & Lawの2026年アップデートは、個人情報を生成AIへ入力する場合に、その利用が特定された利用目的の達成に必要な範囲か確認する必要性等を取り上げている。 40

主要法律事務所の日本語情報として、西村あさひはknowledgeページで「生成AIの適切な利活用等に向けた知的財産の保護」に関する論考を掲載していることが確認できる。ただし、**DevDay 2026固有の日本の大手法律事務所による詳細分析は、発表翌日の本調査では確認できなかった。** 41

EU。 GPAI Code of PracticeはTransparency、Copyright、Safety & Securityの3章から成り、AI Act上のGPAI obligationsへのcompliance手段を提供する。OpenAIも署名者として掲載されている。AI Officeはtraining-data summary templateも整備しており、EUでモデルやAI製品を提供する企業にとって、**training provenance・copyright policy・model documentationを調達時に確認することが規制対応とIP due diligenceの双方を兼ねる**ようになっている。 42

GPAI rulesは2025年8月2日から適用され、新規model providerに関して2026年8月2日からAI Officeによるenforcementが可能となったとEuropean Commissionは説明している。DevDay 2026はまさにこの執行フェーズ入り後の大型発表であり、企業ユーザー側もvendor documentationを保存しておく価値が増している。 43

実務対応策とチェックリスト

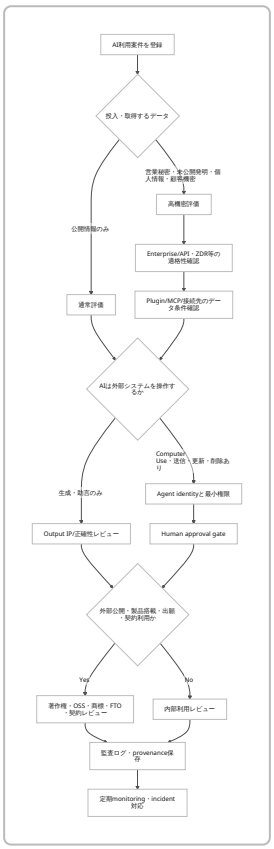
契約条項の見直し

OpenAI本体との契約だけでなく、Marketplace、plugin、MCP、connected apps、クラウド基盤を一つの**AI supply chain**としてレビューする必要がある。OpenAIの現行契約はBusiness/API dataのno-training、Output assignment、security、DPA等を提供するが、third-party servicesには別条件が適用され得る。 44

契約テーマ	推奨する最低条件	DevDay 2026後に特に確認すべき点
入力データ	顧客データの所有権・秘密性維持、目的外利用禁止	agentがtool経由で取得したデータも「Customer Content」に含まれるか
学習利用	default no-training、opt-inは書面承認制	OpenAIだけでなくplugin/MCP/partnerも同等か
保持	endpoint別retention table、削除期限、backup消去	Agents/Conversations/application state、PSP 30日との関係
Subprocessor	list、事前通知、国外移転条件	plugin・Marketplace vendorがsubprocessorか独立controllerか
Output	ownership/assignment、利用範囲	collaborative Pages/Slidesでhuman/agent contributionsをどう扱うか
IP補償	defense、settlement、damages、適用地域	Beta除外、modified output、third-party offering等の除外
Input warranty	権利処理責任を合理的範囲に限定	RAG/fine-tune corpusの権利証跡
Security	encryption、access control、incident notification	agent identity、credential storage、computer use
Audit	logs、export、retention、legal hold	tool call・approval・agent actionを取得できるか
Change control	material changesの事前通知	model、policy、retention、tool permission変更
Exit	data export＋削除証明	Space、Pages、Files、agent memory/state
AI自動行為	authority limits、human approval	契約送信、支払、IP filing、repository merge等

Services Agreementは契約終了後Customer Contentを原則30日以内に削除する規定を置く一方、法令等の例外もあるため、日常利用時のendpoint-level retentionと「契約終了後の削除」を混同しないことも重要である。 22

推奨リスク評価フロー



このフローのポイントは、**「何のAIモデルか」より先に「どのデータに触れ、どの権限で何を実行するか」を問うこと**である。DotsやAgents APIの登場で、model riskとidentity/access riskを分離して評価する必要性が高まった。[34]

知財・法務向け運用チェックリスト

チェック項目	必須確認
利用環境	個人向けChatGPTではなく、承認済みBusiness/Enterprise/API環境か
Model/ version	モデル名・version・reasoning setting等を案件記録に残したか
Input権利	第三者文書、database、code、画像をAI処理する権限があるか
営業秘密	未公開発明、製法、source code、M&A等のclassificationを確認したか
Personal data	利用目的、必要性、越境・第三者提供等をprivacy担当が確認したか
Training	OpenAIおよび接続先のno-training条件を確認したか
Retention	使用endpointのabuse log、application state、PSP、file retentionを確認したか
Plugins/MCP	接続先vendorのTerms、DPA、training、retention、securityを審査したか

チェック項目	必須確認
Agent権限	read/write/send/delete/merge/fileの権限を分離したか
高リスク行為	特許出願、契約締結、外部送信、支払、production deploymentにhuman approvalがあるか
著作権	商用Outputについて類似性・第三者素材・引用・sourceを検証したか
Software	OSS/SCA、license、secret scan、security scanを通常CI/CDに通したか
特許	新規機能が重要ならFTO/競合patent reviewのtriggerを実行したか
発明者証跡	AI提案と人間の技術的寄与を区別して記録したか
契約	OpenAI indemnityの適用条件・除外を確認したか
Evidence	input source、tool action、output、human approvalをaudit trailに保存したか
Legal hold	ZDR/自動削除とlitigation holdが衝突しない設計か
Meeting	AI noteとは別に、必要なofficial minutes/original recordを保持したか
Incident	agent誤送信・誤変更・秘密漏洩時にcredential revoke / tool disableができるか
Insurance	Cyber、Tech E&O、Media/IP liability等についてAI利用、IP claim、contractual liabilityの除外を保険会社・brokerと確認したか

保険の考え方

OpenAIのOutput indemnityを一次的なリスク移転として評価することはできるが、Beta exclusion、Input rights、third-party offering、modified/combined output等の例外がある以上、**vendor indemnity、自己保有、保険の三層で設計すること**が望ましい。[31]

特にrenewal時には、「生成AIを使用しているか」という質問だけでなく、**autonomous agentsがthird-party systemsへ書込みを行うか、顧客データを処理するか、AI-generated codeを製品へ組み込むか、AI-generated mediaを外部公開するか**を保険会社へ正確に説明できるasset inventoryを整備する。保険約款上のAI exclusion、IP infringement exclusion、contractual liability、privacy/cyber incident、territorial limit、defense costの扱いは保険商品・契約ごとに異なるため、個別確認が必要である。

推奨アクションとロードマップ

短期

今後30日以内に優先すべきは、「新機能を全部試す」ことではなく**agentic AIの境界設定**である。

優先度	アクション
最優先	社内AI規程にDots、Agents API、Computer Use、MCP Events、Team Tasksを明示的に追加し、「生成AI」と「自律実行AI」を別リスク区分にする
最優先	API/ChatGPT/connected appsのinventoryを作成し、consumer accountへの会社機密投入を禁止または強く制限

優先度	アクション
最優先	特許未公開情報、source code、M&A、訴訟、顧客秘密について、利用可能environmentを明示
高	OpenAIのcurrent Services Agreement、Service Terms、DPA、Data Controlsのsnapshotを契約台帳へ保存
高	ZDR対象endpointと非対象endpointを棚卸しし、「no training / retention / state / PSP」を別欄で記録
高	plugin/MCPを原則deny-by-defaultにし、承認済みconnector listを作る
高	merge、external send、contract commitment、IP filing、production操作をhuman approval必須にする
高	DevDay 2026の公式session動画・developer docsが追加公開された場合のchange-review担当者を決める

Enterprise/Edu/HealthcareではDots betaがworkspace adminによるopt-inで、default offとされているため、少なくとも高規制部門では、法務・security review前に一括有効化しない運用が適切である。 45

中期

1〜6か月では、社内規程からtechnical enforcementへ移す。

第一に、AI agent用service account/identityを発行し、人間のcredentialを共有させない。Dotsのspecialist-agent構想自体が独自identityによるaccess managementを掲げているため、企業側もこの方向に合わせるべきである。 36

第二に、知財向けAI audit schemaを標準化する。特許・契約・著作権・code reviewで共通して、model/version、source、retrieval、tool action、human approval、最終成果物への採否を残す。

第三に、AI生成codeを既存のsoftware supply-chain controlへ統合し、SCA、OSS license、secret scanning、security scan、SBOM、必要なFTO triggerを**「AIだけの特別プロセス」にせずCI/CDへ組み込む。** Codex Security Cloud自身もrepository-level、scheduled、新commit継続scanの方向へ進んでいる。 12

第四に、標準契約へAI条項を組み込む。特に共同研究、開発委託、広告制作、法律・コンサルティング、データ提供契約では、**生成AI利用の可否、provider、training、retention、Output rights、third-party claim、秘密情報、AI-generated deliverableの表示・保証**を明文化する。

長期

6〜24か月では、AI利用履歴を「情報セキュリティ記録」から**知財資産のprovenance infrastructure**へ発展させることを推奨する。

PagesやSlidesのように人間とagentが同時編集する環境では、最終ファイルだけを保管すると、人間の創作的寄与や発明着想が後から分からなくなる。OpenAIはこうしたhuman-agent collaborative documentsを明確に製品方向として示している。 46

したがって長期的には、

Human contribution ledger → AI interaction/provenance → IP review → publication/release → evidence archive

を一本化し、特許発明者、著作権、営業秘密アクセス、OSS、契約承認、訴訟holdを同じmetadata foundationから追跡できる状態を目標にすべきである。

EUではtraining-data transparencyやcopyright policyがGPAI governanceの一部となり、日本でもAI法・適正性確保指針・AI基本計画が継続的に更新されているため、年次のAI利用規程更新では足りず、**モデル・契約・規制のchange monitoringを常設機能化する**ことが望ましい。 47

参考優先ソース一覧

最優先：OpenAI公式一次資料

優先度	資料	実務上の用途
A	OpenAI「DevDay 2026 Recap」	20件超の公式発表の基準資料。機能名・availability・概要確認 48
A	OpenAI DevDay公式event page	開催日、基調講演時間、session公開方針の確認 49
A	OpenAI「Introducing GPT-6.1 Sol」	能力、価格、availability、benchmark、factualityの確認 18
A	OpenAI Deployment Safety Hub「GPT-6.1 Sol」	model training概要、安全性、cyber/biological capability、agentic risk評価 20
A	OpenAI「Introducing dots」	autonomy、cloud computer、connected apps、identity、working modelの確認 11
A	OpenAI Developer Data Controls	training、30-day monitoring、ZDR eligibility、application state、data residencyの確認 50
A	OpenAI Private Safety Processing documentation	encrypted/customer-controlled retention、human access、TTLの確認 51
A	OpenAI Services Agreement	Business/APIのInput/Output ownership、no-training、security、deletion、indemnity 52
A	OpenAI Service Terms	Output IP indemnityと例外、Beta exclusion 53
A	OpenAI Terms of Use	個人向けChatGPTのownership、content use、accuracy obligations 23

日本の法令・規制・専門資料

文化庁「AIと著作権について」は、生成AIと著作権に関する日本の公式解釈資料へアクセスする起点として最優先である。 54

内閣府のAI戦略・AI法ページは、AI法、人工知能基本計画、適正性確保指針および2026年の政策更新を追う一次資料として重要である。 55

個人情報保護委員会の「生成AIサービスの利用に関する注意喚起等について」は、個人データを生成AIへ投入する際のprivacy reviewの出発点となる。[56]

経済産業省・総務省の「AI事業者ガイドライン第1.1版」はAI開発者・提供者・利用者に必要な取組を整理しており、社内AI governance設計との対応表を作る際に有用である。[57]

専門家資料としては、Business & Lawの2026年版「生成AIへの個人情報・営業秘密・機密情報」の更新解説、西村あさひの生成AI・知財関連knowledge、AIガバナンス協会によるAI事業者ガイドライン改定解説が参考になる。[58]

EU・海外規制

European Commission「General-Purpose AI Code of Practice」はTransparency、Copyright、Safety & Securityの具体化資料であり、OpenAIが署名者であることも確認できる。EU展開企業はvendor due diligence資料として保存すべきである。[59]

European CommissionのGPAI timelineによれば、GPAI rulesは2025年8月2日から適用され、新規モデルについては2026年8月2日から執行段階に入っている。[43]

AI Officeのtraining-data summary templateおよびCode of Practice策定ページは、今後の学習データ透明性・copyright complianceのbenchmarkとして重要である。[60]

判例・訴訟動向

Thomson Reuters v. Ross IntelligenceはAI trainingにおけるfair useの限界を検討する上で最重要の一件である。2025年の地裁判断でRossのfair-use主張が退けられ、2026年9月29日には第3巡回区控訴裁判所がThomson Reuters側の判断を維持したと報じられている。控訴審理由の完全な公開状況には注意が必要であり、事案を生成AI一般へ機械的に拡張すべきではない。[61]

Bartz v. Anthropicは対照的に、一定の書籍trainingをfair useと評価する一方、海賊版libraryの取得・保有を別問題として扱った。この対照は、企業のRAG/fine-tune data governanceにおいて「最終用途」だけでなく**data provenance・取得経路自体**を保存する必要性を示す。[62]

総合評価

DevDay 2026を知財部門の視点で一言に集約すると、**AIガバナンスの対象が「生成された文章」から「代理人として行動するデジタル主体」へ移ったイベント**である。

従来は、プロンプト、Output、training dataを管理すれば一定のリスクを抑えられた。DevDay 2026以後はそれに加え、

Identity → Permission → Context → Tool → Action → Approval → Provenance → Retention

というagent lifecycle全体を管理しなければ、著作権、特許、営業秘密、契約、個人情報、証拠、securityを一貫して統制できない。Dots、Agents API、MCP Events、ChatGPT Space、Codex Security Cloudはいずれもこの変化を裏付ける。[63]

その一方、OpenAIのno-training default、ZDR、Private Safety Processing、今後のPrivate Inferenceは、適切なenterprise architectureを採れば高機密な知財業務への適用余地をむしろ拡大する。重要なのは「AIを禁

止するか許可するか」ではなく、**データ感度・agent autonomy・外部接続・法的効果に応じて利用条件を段階化すること**である。 64

最終的に企業が構築すべきなのは、AI Outputの品質管理制度ではなく、**AIが関与した知的成果物について、人間の寄与、入力権利、取得データの出所、実行権限、第三者サービスへの移転、最終承認を後から説明・立証できる制度**である。2026年のEU規制、日本のAI政策、米国copyright litigationの流れを合わせると、この「provenanceとaccountability」が今後の知財・法務AI governanceの中心になると考えられる。 65

navlistAI学習と著作権をめぐる直近の重要動向turn23news29,turn23news30,turn23news31

---

1 7 49 https://devday.openai.com/
https://devday.openai.com/

2 11 34 35 36 63 https://openai.com/index/introducing-dots/
https://openai.com/index/introducing-dots/

3 9 18 19 https://openai.com/index/introducing-gpt-6-1-sol/
https://openai.com/index/introducing-gpt-6-1-sol/

4 21 24 25 27 38 50 64 https://developers.openai.com/api/docs/guides/your-data
https://developers.openai.com/api/docs/guides/your-data

5 22 28 29 44 52 https://openai.com/policies/services-agreement/
https://openai.com/policies/services-agreement/

6 42 47 59 65 https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai
https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai

8 https://x.com/andrewcurran_/status/2104994885837431192
https://x.com/andrewcurran_/status/2104994885837431192

10 12 13 14 15 16 45 46 48 https://openai.com/index/devday-2026-recap/
https://openai.com/index/devday-2026-recap/

17 https://www.youtube.com/watch?v=Fls_onRviPM
https://www.youtube.com/watch?v=Fls_onRviPM

20 https://deploymentsafety.openai.com/gpt-6-1-sol
https://deploymentsafety.openai.com/gpt-6-1-sol

23 37 https://openai.com/policies/row-terms-of-use/
https://openai.com/policies/row-terms-of-use/

26 51 https://developers.openai.com/api/docs/guides/private-safety-processing
https://developers.openai.com/api/docs/guides/private-safety-processing

30 54 https://www.bunka.go.jp/seisaku/chosakuken/aiandcopyright.html
https://www.bunka.go.jp/seisaku/chosakuken/aiandcopyright.html

31 32 53 https://openai.com/policies/service-terms/
https://openai.com/policies/service-terms/

33 62 https://www.theguardian.com/technology/2025/jun/25/anthropic-did-not-breach-copyright-when-training-ai-on-books-without-permission-court-rules
https://www.theguardian.com/technology/2025/jun/25/anthropic-did-not-breach-copyright-when-training-ai-on-books-without-permission-court-rules

39 55 https://www8.cao.go.jp/cstp/ai/ai_act/ai_act.html
https://www8.cao.go.jp/cstp/ai/ai_act/ai_act.html

40 56 https://www.ppc.go.jp/news/careful_information/230602_AI_utilize_alert/
https://www.ppc.go.jp/news/careful_information/230602_AI_utilize_alert/

41 https://www.nishimura.com/ja/knowledge
https://www.nishimura.com/ja/knowledge

43 https://digital-strategy.ec.europa.eu/en/news/general-purpose-ai-code-practice-now-available
https://digital-strategy.ec.europa.eu/en/news/general-purpose-ai-code-practice-now-available

57 https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20240419_report.html
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20240419_report.html

58 https://businessandlaw.jp/articles/a20260409-1/
https://businessandlaw.jp/articles/a20260409-1/

60 https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice
https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice

61 https://www.reuters.com/legal/thomson-reuters-wins-ai-copyright-fair-use-ruling-against-one-time-competitor-2025-02-11/
https://www.reuters.com/legal/thomson-reuters-wins-ai-copyright-fair-use-ruling-against-one-time-competitor-2025-02-11/