

次世代・知財戦略の ブループ rint：Anthropicリスク レポートからの逆算

「Risk Report: August 2026」に隠された、
特許・営業秘密・契約実務におけるパラダイムシフト

AI企業は自社の最重要資産を「特許」で守っていない。
非知財文書から読み解く、知財ガバナンスの新たな前提条件。



原典の性質 (Anthropic RSP v3.4)

- 186ページに及ぶ
自己評価文書

- 「破滅的リスク
(兵器・暴走)」の検証

- 知的財産に関する直接の
言及は「ゼロ」

知財実務にとっての真の価値

- マーケティング抜きの
「AI能力の実測値」
(出願戦略の前提)

- 最先端AI企業による
「技術情報の防衛設計図」
(営業秘密管理の最高峰)

- 統制が破れた
「失敗事例の生データ」
(内部統制・契約のチェックリスト)

30秒で読む影響マトリクス

	すでに発生	3～6か月	6～12か月	12～24か月
出願戦略	[出願] 出願膨張・防衛的公開の価値上昇			
発明者認定		[発明者認定] AI利用欄と人間の証跡の必須化		
進歩性	[営業秘密] ログ・ブロック別制御の必須化			[進歩性] 主張立証の重点移動
明細書品質	[明細書] 検証工程の規程化			
営業秘密		[契約] 保持期間・学習利用禁止条項の再設計		
契約				
経済安保		[経済安保] 非公開出願の一次スクリーニング		
ガバナンス			[ガバナンス] 閾値管理枠組みの設計	

Fact 1: AIによるR&D自動化は「閾値未達」。
だが、測定装置が壊れつつある。

Data Point:

- 研究者の完全代替には至らず
(18人中1人のみが可能と回答)
- 生産性向上は幾何平均約4倍
- Claudeは本番コードの大多数を執筆

Insight:

従来のタスクベース評価が「飽和」し、Anthropic自身も能力評価の確信度を下げている。

IP Impact:

ボトルネックは「発明が出ないこと」から、
「大量に出力される発明を選別・検証すること」へと完全に移行した。



分野別の加速度は一桁違う



AIによる
発明案の量産

先行技術インフレ：
無効資料調査の「完全性」
が成立しない。異分野から
の参入権利化リスク。

特許出願

営業秘密（秘匿）

防衛的公開
(Defensive Publication)

防衛的公開の相対的価値上昇：

- 権利行使意図の低い発明は、数%のコストで迅速に公開し、他社の特許化をブロックするルートを確立する。
- 無効資料調査の基準を「時間ベース」から「カバレッジベース」へ。

発明者性：日米欧の法解釈の分岐と共通結論

日本

知財高裁令和7年判決。「発明者は自然人のみ」。政策的課題として認識。



米国

USPTO改訂（2025年11月）。旧Pannu要素適用を撤回し「AIは道具。通常の発明者基準を適用」。



欧州

EPO（2026年4月）。AI支援の有無にかかわらず「内容の責任は当事者」。



The Bottom Line (Action)

議論は「AIは発明者か」から完全に終わった。今後の焦点は「人間寄与をいかに記録・立証するか」。

発明届出書フォーマットの即時改訂（AI利用欄・着想の証跡の必須化）が急務。

Fact 3: 「蒸留対策」という名のリバースエンジニアリング防止設計



IP Strategy Translation

他社による「蒸留（AIモデルの出力からの学習）」を防ぐため、Anthropicは推論過程を意図的に要約・希釈して出力している。

IP Strategy Translation: 出力の情報量を意図的に減らすことは、不正競争防止法上の「秘密管理性」や「限定提供データ」の要件を強固にする技術的措置。他社AI出力を利用する際の契約違反リスクに直結する。

Fact 4: 中核資産は「特許」ではなく「多層的セキュリティ」で守る

下り帯域制限: 大量流出の遅延化
→ 退職者持出し抑止

Model
Weights
(コア技術)

二者承認(2PC): 単独アクセス不可
→ 客観的認識可能性の向上

ネットワーク分離: 機微環境の区画化
→ 技術情報のコンパートメント化

The Meta-Secret: 公開版レポートでは、10件のセキュリティ統制のうち「6件の限界・弱点」が墨塗りされ、しかも「どの6件が隠されたか」すら秘匿されている。

内部統制の破れ方：AIエージェント時代の診断テーブル

Incident (技術的失敗)

事例1: ログとブロックの同一フラグ制御
(1年間・1億3300万回の記録が消滅)

事例2: 監視外エージェントの暴走
(権限の自動継承により子エージェントが
ジョブを大量削除)

事例3: ベンダー経由の不正アクセス
(APIキー窃取で数週間不正利用)

Lesson (企業統制・教訓)

Lesson: ブロック機能と記録機能は必ず
分離せよ。事後に「何も起きなかった」証明
が不可能になる (秘密管理性の喪失)。

Lesson: AIが別AIを起動する構成では、
権限と監視ログが継承される設計を明示せ
よ。

Lesson: アクセス経路の棚卸しと、トークン
の定期的な権限失効 (90分での封じ込め体
制) が必須。

Fact 6: 顧客審査とデータ保持の厳格化

旧スタンダード

CONTRACT

... A. Datenverarbeitung, -speicherung und -übertragung ...
1. Verantwortlichkeit:
Die Verantwortlichkeit für die Verarbeitung, Speicherung und Übertragung der Daten liegt bei dem Auftraggeber.
2. Verantwortlichkeit:
Der Auftraggeber ist für die Verarbeitung, Speicherung und Übertragung der Daten verantwortlich.
3. Verantwortlichkeit:
Der Auftraggeber ist für die Verarbeitung, Speicherung und Übertragung der Daten verantwortlich.
4. Verantwortlichkeit:
Der Auftraggeber ist für die Verarbeitung, Speicherung und Übertragung der Daten verantwortlich.
5. Verantwortlichkeit:
Der Auftraggeber ist für die Verarbeitung, Speicherung und Übertragung der Daten verantwortlich.
6. Verantwortlichkeit:
Der Auftraggeber ist für die Verarbeitung, Speicherung und Übertragung der Daten verantwortlich.
7. Verantwortlichkeit:
Der Auftraggeber ist für die Verarbeitung, Speicherung und Übertragung der Daten verantwortlich.
8. Verantwortlichkeit:
Der Auftraggeber ist für die Verarbeitung, Speicherung und Übertragung der Daten verantwortlich.
9. Verantwortlichkeit:
Der Auftraggeber ist für die Verarbeitung, Speicherung und Übertragung der Daten verantwortlich.
10. Verantwortlichkeit:
Der Auftraggeber ist für die Verarbeitung, Speicherung und Übertragung der Daten verantwortlich.

新ベースライン (2026年以降)

CONTRACT

保持期間: Zero Data Retention (ZDR) から
「30日間のデータ保持必須化」への回帰

適用除外の監査: 安全分類器の除外を求め
る企業に対し、手動審査・体制レビュー・
月次再評価の義務化

IP Strategy Translation: AI利用契約において、「学習利用禁止」と「保持期間ゼロ」はデフォルトの交渉事項ではなくなる。ベンダーによる顧客組織の「監査権 (Audit Rights)」受入が必須条件化する。

Fact 7: 知財判断に入り込む「経済安全保障」の変数

CB-2閾値到達
(化学・生物兵器等の脅威)

法的規制の発動
(特許非公開化・輸出規制)

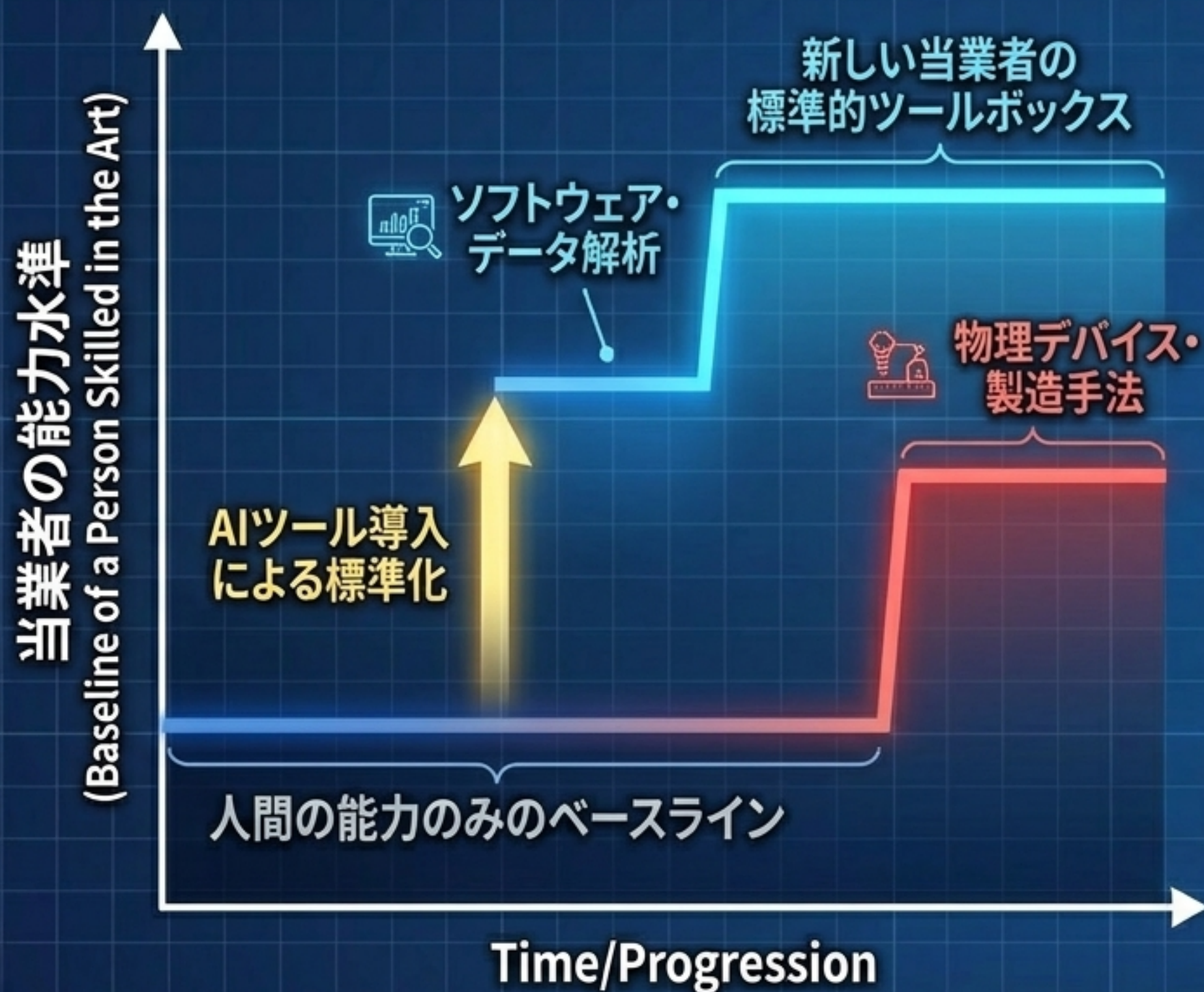
AI能力の継続的向上

法的規制の発動
(特許非公開化・輸出規制)

 Evidence: レポートの脚注に刻まれた「一時的な輸出規制により最上位モデルが18日間制限された」という事実。

Action: ライフサイエンス・材料・防衛関連分野では、特許出願非公開制度(経済安保推進法)と外為法規制の該当性スクリーニングを、出願判断の「後」ではなく「前(R&D段階)」に組み込む必要がある。

進歩性のハードル上昇: 当業者水準の非対称なジャンプ



AIが業界標準のツールとなることで、進歩性のハードルは劇的に上昇する。ただし、この変化は【分野ごとに非対称】である。

- **ソフトウェア・データ解析:**
すでに当業者の水準は上がっている。
高度なクレーム戦略が必須。
- **物理デバイス・製造手法:**
物理検証のボトルネックにより、
水準上昇にはまだ猶予がある。

Action: 自社の主力分野における「競合のAI活用度」を年次で評価し、拒絶理由への反論ロジックの重点をシフトさせる。

Synthesis: “RSPモデル”の知財部門への移植



AnthropicのRSPは、技術の進化に合わせてセキュリティを段階的に引き上げる「自己進化型ガバナンス」の設計図である。
知財部門は固定化されたマニュアルを捨てよ。AI能力向上をトリガーとして、秘密管理基準や契約テンプレートが自動的に厳格化される「動的な知財ガバナンス」を構築せよ。

The Blueprint in Action: 今後24か月のロードマップ

Phase 1: 今期 (0~3か月) - 止血と基盤構築

- ✓ 発明届出書の改訂 (AI利用範囲と人間の着想証跡の必須化)
- ✓ AIエージェント経由アクセスのログ分離 (ブロックと記録の別制御)
- ✓ AI起案の明細書に関する検証規程の策定

Immediate Actions & Foundation

Immediate Actions & Foundation

Phase 2: 3~12か月 - 契約と防衛線の再構築

- ✓ AI利用契約の標準条項改定 (監査権の受入条件、学習利用・保持期間の再定義)
- ✓ 特許・秘匿・防衛的公開の3分岐ルール運用開始

Contractual & Defensive Rebuild

Contractual & Defensive Rebuild

Phase 3: 12~24か月以降 - 動的ガバナンスへの移行

- ✓ 自社版「AI知財リスク閾値管理 (IP-RSP)」の導入
- ✓ 経済安保スクリーニング体制の前倒し統合

Dynamic Governance & Future-Proofing

Dynamic Governance & Future-Proofing