

GLM-5.3(Z.ai／智譜 AI)調査レポート

— 事実確認・仕様・ベンチマーク・影響分析 —

想定読者:知財戦略実務家／2026 年 8 月 15 日時点

Claude Opus 5

1. 要旨

- 前提は事実。「Z.ai が 2026 年 8 月 14 日に大規模言語モデル GLM-5.3 を発表した」という前提は、公式技術ブログ¹、公式 X 投稿²、公式開発者ドキュメント³という一次情報で確認できた。モデル名は正確に「GLM-5.3」であり、発表前に流れた「GLM-5.5」「一兆パラメータ級」への改称・拡大の噂は否定されている⁵。ただし発表日は GLM Coding Plan および ZCode での提供開始日であって、オープンウェイト(重み)と API は発表時点では未提供である^{2,3}。重みは安全性審査を経て 2026 年 8 月 28 日に Hugging Face で公開予定と報じられ、GLM シリーズ初の意図的な公開遅延となった^{10,23}。
- 技術的核心は「基座を変えず後訓練だけで伸ばした」点にある。GLM-5.3 は GLM-5.2 と同一の基座モデル(総パラメータ約 7,430 億の MoE、アクティブ約 400 億、コンテキスト 100 万トークン)を用い、性能向上はすべて後訓練(post-training)のスケーリングによるとされる^{1,3}。自社内部評価ではコーディング体感が対 GLM-5.2 で約 50%向上し^{6,7}、Terminal-Bench 3.0 は 4.6 から 28.3 へ跳躍したと公表されている^{16,17}。ただし数値は原則すべて Z.ai 自社公表値であり、独立第三者による再現検証は重み公開後に始まる¹⁵。
- 影響の要点は三層に整理できる。第一に、中国製オープンウェイトモデルがクローズド最前線に数か月差まで肉薄しつつ価格は数分の一という構図を再確認させたこと。第二に、GLM-5.3 が意図せず高度なサイバー攻撃連鎖の推論能力を獲得したとして初めて重み公開を遅延させ、デュアルユースと輸出管理の論点を先鋭化させたこと^{4,26}。第三に、日本企業にとっては「MIT オープンウェイト×オンプレミス運用」がデータ主権と単価優位を両立する現実解となる一方、Z.ai が米国エンティティリスト掲載企業である点³⁵、学習データの由来が非開示である点、中国国家情報法下のデータ経路という三重のリスク評価が不可欠であることである。

2. 主要な調査結果

2.1 発表の事実確認

2026 年 8 月 14 日正午(中国時間)、智譜(Z.ai、香港証券取引所 02513.HK)が GLM-5.3 を正式発表した^{6,7}。一次情報として公式技術ブログ¹、公式 X(@Zai_org)²、公式開発者ドキュメント³を確認し、準一次情報として中国主要メディア(IT 之家⁶、新浪科技⁷、掘金⁸、CSDN⁹、百度百科⁵)を照合した。同日 13 時に GLM Coding Plan 全ユーザーの利用枠がリセットされている⁶。

モデル名は正確に「GLM-5.3」である。発表前は「GLM-5.5」への改称や一兆パラメータ超への拡大が噂されたが、基座は 7,400 億級に据え置かれ、GLM-5 系列の番号ロジックが継承された⁵。

GLM-5(2026 年 2 月)→5.1(4 月)→5.2(6 月)→5.3(8 月 14 日)という約 2 か月ごとの高速リリースの最新版にあたる^{5,21}。

発表日と提供形態は峻別が必要である。8 月 14 日は GLM Coding Plan 全量ユーザー、ZCode(公式エージェント開発環境)、AutoClaw(効率化ツール)での提供開始日であり^{6,8}、API は「近日提供」と表示され³、オープンウェイトは未公開であった²。

2.2 仕様(Z.ai 公表)

基座は GLM-5.2 と同一で、総パラメータ約 7,430 億の MoE アーキテクチャ、アクティブパラメータは 1 トークンあたり約 400 億とされる^{1,3}。コンテキスト長は 100 万トークン、最大出力は 128K トークン³。入出力はテキストのみで、マルチモーダル(視覚)には非対応である³。コミュニティ投票では視覚機能が最多要望であったが今回は搭載されなかった⁵。Thinking Mode(複数の思考レベル)、Function Calling、MCP、構造化出力、コンテキストキャッシュに対応し、長時間稼働するエージェント能力を主眼に置く³。

2.3 ライセンス・価格

前世代 GLM-5.2 は MIT ライセンスで Hugging Face(zai-org)に公開されている²²。GLM-5.3 も MIT 継承が有力視されるが、発表時点で重み未公開のため未確認である。サイバー能力を理由としたゲート化の文脈上、公開時に利用制限付きライセンスへ変更される可能性は理論上残る(投機的、要確認)。

GLM Coding Plan(サブスクリプション)は月額 18 ドル(Lite)、80 ドル(Pro)、168 ドル(Max)で、年額契約では実質 12.6 ドルからとなる^{18,19}。ポイント制でオフピークは 50%レート、ZCode は 8 月 31 日まで 1.5 倍の枠ブーストが適用された⁸。GLM-5.3 の API 単価は発表時点で未公表であり、参考として GLM-5.2 は入力 1.40 ドル・出力 4.40 ドル(百万トークンあたり)であった¹⁸。なお

Coding Plan は公式サポートツール限定であり、自作エージェントからの汎用 API 利用は別契約となる¹⁹。

3. ベンチマークと検証状況

以下はすべて Z.ai 自社公表値である。Z.ai は評価ハートネス設定を開示しており(例: CyberGym は Claude Code 2.1.207、最大推論、temperature=1.0、1,507 タスクの単一実行 Pass@1)¹⁵、GDPval-AA v2 は Artificial Analysis による評価とされる¹⁶。ただし独立第三者による GLM-5.3 自体の再現実行は重み公開後(8月28日目処)まで始まらず、発表時点で独立 DeepSWE リーダーボードに GLM-5.3 は未収録である^{15,16}。Z.ai Code Bench は非公開ベンチマークであり外部監査不能である¹⁵。

ベンチマーク	GLM-5.2	GLM-5.3	備考
Terminal-Bench 3.0	4.6	28.3	オープンウェイト勢首位を主張
DeepSWE v1.1	46.2	66.9	独立リーダーボードには未収録
Agents' Last Exam(CLI)	23.8	28.5	—
GDPval-AA v2(44 職種)	—	1,769	Z.ai 評価中の全モデルで最高値と主張
Terminal-Bench 2.1	—	88.2	クローズド最前線と同水準
CyberGym	77.2	84.5	クローズド最前線を僅差で上回ると主張
ExploitBench	24.4	54.4	深い攻撃生成では最前線に依然劣後
Z.ai Code Bench(High)	—	31.4%	非公開ベンチ。外部監査不能

数値の出典は公式ブログおよび公式 X 記事^{1,4}、ならびにこれを引用した第三者記事^{14,15,16,17,18}による。

評価(分析): GLM-5.3 は全方位でトップというわけではない。深い攻撃生成(ExploitBench 等)やハードなエージェントコーディングではクローズド最前線に劣後しており^{15,17}、真の差別化は GDPval-AA v2 と CyberGym という「業務自動化と防御的セキュリティ」のクラスタに集中している。適切な要約は「重みが実際に公開されれば、オープンウェイト勢で最良の価格対能力比」である。

4. サイバー能力と重み公開遅延

Z.ai は後訓練に脆弱性発見データと認可されたセキュリティ環境を投入した。当初は単一バグ発見の改善を期待していたが、実際には複数段階の攻撃連鎖を横断的に推論し完全な攻撃計画を形成し始めたとされ、この「意図せぬ涌现」を理由に重み公開を 8 月 28 日まで遅延させた^{4,10,26}。

具体的成果として、中国のセキュリティチーム(NSFOCUS、CyberKunlun、DARKNAVY 等)および清華大学・南開大学の研究者と協働し、GLM-5.2 以降で 269 プロジェクトから 2,436 件の脆弱性を発見したと報じられている(うち重大・高危 1,097 件)²⁶。影響ソフトウェアには Linux カーネル、WinRAR、Redis、FFmpeg 等が含まれる¹⁰。最古の脆弱性は概ね 1981 年に混入したもので、発見までの平均経過年数は 26.6 年とされる²⁷。公開台帳には 53 件が CVE 付きで公開され、2,383 件は修正作業中で非公開とされる^{10,24}。発表当日には、AI コードエディタ Cursor の重大な脆弱性を GLM-5.3 が特定した事例も報じられた¹⁴。

デュアルユースの緊張(分析):これは「防御側の恩恵(攻撃者より先にバグを発見・修正)」と「攻撃側リスク(同能力の悪用による攻撃者の底上げ)」が表裏一体という古典的問題を先鋭化させる。

Z.ai は、オープンソースプロジェクトの監査、防御目的でのモデルアクセス提供、ZCode へのコード監査機能追加からなる「Open Source Shield」構想を打ち出し、開かれた世界も自らの盾を持つ必要があると主張した⁴。段階的公開(選定パートナーによる制御環境での評価→広域アクセス→重み公開)、リクエスト分類器と思考連鎖の監視も実施するとされる⁴。

もっとも、真のオープンウェイトが公開される以上この種の安全策の効果は限定的であり、GLM-5.3 でなくとも別のモデルが同じ能力を持つため、政府主導・業界連合による産業規模の対応が急務だとする指摘もある¹³。業界では 2026 年 7 月 24 日に Nvidia、Microsoft、Meta、IBM、Palantir から 25 社が「防御側は攻撃者が入手可能なものと同等能力のモデルへのアクセスを要する」とする公開書簡を発表した一方¹⁷、Anthropic は公開重みの最前線サイバーモデルが悪意ある行為者の敷居を下げ公開後は不可逆であるとして反対しており²⁴、GLM-5.3 はこの対立を先鋭化させた。

5. 企業・資本市場動向

上場:Z.ai(智譜)は 2026 年 1 月 8 日に香港取引所主板へ上場した(銘柄コード 02513.HK)。公募価は 1 株 116.20 香港ドル、初値 120.00 香港ドルで時価総額は約 528.3 億香港ドルであった²⁹。初日終値は 131.5 香港ドル(+13.2%)³⁰。上場前には 8 ラウンド超・累計 83 億元超を調達し、美团・アリババ・テンセント・小米・金山等の産業資本に加え紅杉・高瓴等が出資していた²⁸。

株価・時価総額:上場来の上昇率は約 1,600%に達し、時価総額は 1,100 億ドルを超えたと報じられている³¹。一方でピーク時からの変動幅も大きく、極めて高いボラティリティを伴う²⁸。

収益:2025 年通期売上は 7.24 億元(前年比+132%)²⁸。2026 年 7 月時点で ARR(年換算収益)が 10 億ドルに到達したと複数媒体が報じている^{23,32,33}。36Kr 系媒体は、Anthropic が 1 億ドルから 10 億ドルへ 15 か月を要したのに対し智譜は 5 か月であり、2026 年 1 月から 7 月で ARR が 15 倍になったと算定する³⁴。他方 Macquarie は過去 12 か月で約 10 倍として 7 月に 10 億ドルを突破したと別算定しており³¹、算定基準の差に留意が必要である。赤字は継続しており、2025 年の調整後純損失は 32 億元²⁸。API 利用者は約 700 万人に接近し、5 万超の国産 AI チップが稼働しているとの報道もある²⁵。

6. 開発者・企業ユーザーへの影響

エコシステム:GLM-5.3 は ZCode、Claude Code、OpenCode に加え、Trae／扣子(Coze)、WorkBuddy／CodeBuddy、Qoder／QwenWork、CatPaw、JoyCode 等の多数のサードパーティ環境で先行体験可能とされた^{6,8}。Z.ai は Anthropic プロトコル互換の専用 API エンドポイントを提供しており、環境変数の変更のみで Claude Code 等から GLM へ切り替えられる。既存の CLAUDE.md、スラッシュコマンド、MCP 設定がそのまま流用できる点が移行障壁を大きく下げている^{19,20}。

採用実態:OpenRouter の月間上位 10 エンドポイントのトークン処理量の約 8 割を中国系モデル(DeepSeek、Qwen、GLM、Kimi)が占めるとの集計がある³⁸。GLM-4.6 から 5.2 にかけて Claude Code 代替として実務水準に到達したことが、Z.ai の ARR 急成長の主因とされる^{32,33}。

実務評価:GLM Coding Plan 既加入者にとっては実質無償の性能アップグレードにあたる¹⁸。一方で、全エージェントベンチで無条件にリードするモデルが必要な用途ではクローズド最前線が依然優位であり、自己ホストで重みが必要な用途は公開(8 月 28 日目処)まで待つべきというのが一般的な助言である^{15,18}。

競合構図:同週に DeepSeek が上位モデルの正式版移行に伴う大幅値上げを予告しており(出力単価が百万トークンあたり 0.87 ドルから 3.96 ドルへ)¹⁰、GLM-5.3 はこの値上げ局面でオープン戦略を維持することで差別化を図った。オープンウェイト勢に対してはコーディングとサイバーで多くの領域をリードするが、Kimi K3 が DeepSWE 等で上回る領域も残る^{15,17}。

7. 知的財産・法務・ガバナンス上の論点

7.1 オープンウェイト利用のライセンス上の留意点

MIT ライセンス(GLM-5.2 で確認、5.3 は予想)は極めて寛容で、商用利用・改変・自己ホストが自由である²²。しかし「現状有姿・無保証」であり、知的財産に関する免責(indemnification)は一切付されない。米国の一部クローズド商用モデルが提供する著作権侵害免責プログラムのような後ろ盾がなく、学習データに由来する第三者著作権侵害リスクは利用企業自身が負う。MIT は「重みのライセンス問題」を解決するが「学習データの由来(プロベナンス)」を保証しないという峻別が、実務上決定的に重要である。

7.2 学習データを巡る懸念

GLM 系の学習データ構成・由来は非開示である。中国勢の性能追従をめぐっては、米国最前線モデルの推論トレースを抽出する蒸留の疑義が繰り返し提起されるが、後訓練スケーリングという今回の説明は蒸留主導ではなく強化学習主導の訓練体制と整合的だとする評価もある¹³。実務上は、学習データの適法性・出所を外部から検証できないことを前提にリスク評価を組むほかない。

7.3 輸出管理・安全保障

Z.ai は米国エンティティリスト掲載企業である。2025 年 1 月 15 日、先端 AI 研究の開発・統合を通じて中国の軍事近代化を推進しているとの理由で、Beijing Zhipu Huazhang Technology Co., Ltd. を含む複数法人が追加され、EAR 対象品目の全てにライセンスを要し審査方針は原則不許可とされた。域外直接製品規則を拡張適用する脚注 4 指定も付されている³⁵。Z.ai はこれを事実根拠を欠くとして強く反対している²⁸。

米国の規制動向としては、2026 年 7 月に米政権が国内での中国製先端 AI モデルへのアクセス制限を検討中と報じられた(政策アイデア段階であり、正式提案・執行機構は未定)³⁶。オープンウェイトは半導体のような物理的チョークポイントを持たないため、規制の実効性には構造的困難がある。連邦調達禁止(政府機関・請負業者による利用制限)が有力な手段として言及されている³⁶。

中国側からの逆方向の規制も進行している。2026 年 7 月、中国商務部がアリババ、字節跳動、Z.ai と海外向けの最先端モデル(オープンウェイトを含む)アクセス制限を協議していると報じられた³⁷。米中双方から「オープンソース裁定」チャンネルが挟撃され、エコシステムの分岐が加速している。

7.4 企業利用時のリスク評価

データ経路:Z.ai のホスト型アプリケーションおよび API への直接呼び出しは、プロンプトとコンテキストが中国のインフラを経由する。中国は個人情報保護法、データセキュリティ法、サイバーセ

セキュリティ法の三層体制を有し、国家情報法の下で当局のデータ提供要請に事業者が応じる義務が想定される点が、日本企業のリスク評価上の中核論点となる。

緩和策:(1)機密度分類により個人情報・機密設計情報・未公表財務情報を直接 API 利用から除外する、(2)送信前のプロンプトフィルタリングと個人情報除去を行う、(3)オープンウェイトを自社 GPU 環境または自社クラウドアカウント内で完結させ、そもそも中国事業者のサーバーにデータが送られない構成とする。とりわけ(3)の「オープンウェイト×オンプレミス運用」は、機密性の高い業務に中国製モデルの単価・性能メリットを引き込む唯一の現実解であり、米国クロード最前線にはこの選択肢が存在しない点が構造的な差異である。

8. 日本企業・日本の知財実務への含意

知的財産推進計画 2026(2026 年 6 月 12 日、知的財産戦略本部決定)は、生成 AI の社会実装をあらゆるものに大きな変革をもたらすインパクトと位置づけ、経済安全保障の観点からも知財戦略が不可欠と明記している⁴⁰。学習データの取扱いおよび生成物と著作権の関係を新たな課題とし、権利者の懸念に応える枠組みとして「生成 AI の適切な利活用等に向けた知的財産の保護及び透明性に関するプリンシプル・コード(仮称)」の策定を打ち出した⁴⁰。ただし同計画は著作権法第 30 条の 4 を詳細に再定式化するものではなく、所管は文化庁である⁴³。

著作権法第 30 条の 4 により、AI 学習は原則として情報解析として権利者の許諾なく適法とされるが、著作権者の利益を不当に害する場合等の但し書による例外がある⁴³。2026 年時点で条文改正はなく、日本の方針は解釈の明確化と周辺法・運用整備に置かれている。関連して AI 推進法(2025 年 5 月 28 日成立、9 月 1 日全面施行)および AI 基本計画(2025 年 12 月 23 日閣議決定)が枠組みを提供している⁴⁴。

政府調達については、デジタル庁「行政の進化と革新のための生成 AI の調達・利活用に係るガイドライン」(DS-920)がある。v1.0 は 2025 年 5 月 27 日制定で遵守が義務、v2.0 は 2026 年 6 月 12 日改定(内容は 9 月 1 日、ガバナンス部分は 7 月 1 日施行)である^{41,42}。適用対象は国の府省庁であり、地方公共団体は必要に応じ参考とすることが期待される努力目標にとどまる⁴²。高リスク AI 判定シート、調達・契約チェックシート、CAIO(AI 統括責任者)設置を規定する⁴¹。なお、中国製モデルを名指しで制限する条文は確認されておらず、リスクは能力とデータフローの基準で判定される。「中国製ゆえに一律禁止」という規定が同ガイドラインに存在するという理解は誤りであり、事実と推論の峻別が必要である。

国内の反応としては、複数の実務系媒体が中国製 LLM(GLM、Qwen、DeepSeek、Kimi、

MiniMax)を実務比較の対象として本格的に扱う段階に入っている。論調としては「国名だけでなく、どこで動作し誰がデータを処理するかで判断せよ」というものが主流であり、日本語処理・多言語対応・オンプレミス運用適性を評価しつつ、米国側の規制と中国側の提供停止という双方向の地政学的継続性リスクを明記するものが多い。

8.1 知財実務家への実践的含意

- 法務・知財関連の機密文書を扱う場合は、オンプレミスまたは自社クラウドでの自己ホストを基本とする。
- MIT ライセンスの無保証・無免責を前提に、学習データ由来の侵害リスクは自社負担であると認識する。
- モデル層を抽象化したマルチベンダー戦略により、供給継続性リスクをヘッジする。
- 米国子会社や米国政府調達との関係では、Z.ai がエンティティリスト掲載企業である事実を継続監視する³⁵。
- 重み公開後は、実際のライセンス条項とモデルカードを必ず一次情報で確認する。

9. 推奨アクション

9.1 段階 1:即時(情報収集)

- GLM-5.3 を評価対象に加える。ただし現時点では重みのダウンロードが不可であるため、まず GLM Coding Plan(月額 18 ドルから)または API 提供開始後に実証実験を行う^{18,19}。対象はコーディングエージェント、業務自動化、防御的セキュリティ用途に絞る。
- 2026 年 8 月 28 日目処の Hugging Face(zai-org)における重み公開を監視し、公開されたライセンス条項とモデルカードを必ず確認する^{10,22}。これが確認できるまで本番採用の意思決定は保留する。

9.2 段階 2:条件付き採用

- 機密性の高い業務(法務・知財文書、顧客データ、未公表情報)ではオンプレミスまたは自社クラウド内の自己ホストを一択とする。ホスト型 API の直接呼び出しは非機密・公開情報タスクに限定し、送信前の個人情報除去を必須化する。

- MIT の無保証・無免責を前提に、学習データ由来の第三者著作権侵害リスクを社内ガイドライン(生成物の出力審査プロセス)でカバーする。デジタル庁 DS-920 の調達・契約チェックシートは、民間契約のひな型としても援用可能である⁴¹。

9.3 段階 3:ガバナンス整備

- GLM、Qwen、DeepSeek、米国モデルを切替可能なモデル層で抽象化したマルチベンダー戦略を構築し、米中双方の規制リスクと供給停止リスクをヘッジする^{36,37}。
- 米国子会社を保有し、または米国政府調達に関与する企業は、Z.ai のエンティティリスト掲載を踏まえて法務と連携し利用範囲を精査する³⁵。

9.4 判断を変える閾値

採用を前進させる条件:重みが MIT ライセンスで公開され、独立検証(Artificial Analysis、DeepSWE リーダーボード等)が公表値を概ね再現し、日本語タスクで実務水準を確認できた場合。

採用を見送り、または再評価すべき条件:公開ライセンスに商用制限・地域制限が付いた場合、独立検証で公表値と大きな乖離が生じた場合、米国が中国製モデルの国内利用を正式に規制した場合、または自社が米国政府調達要件に抵触する場合³⁶。

10. 留意事項(認識論的ヘッジ)

- ほぼ全てのベンチマーク数値は Z.ai 自社公表値であり、独立第三者による GLM-5.3 の再現検証は重み公開(8月28日目処)後に始まる。とりわけ非公開の Z.ai Code Bench と自社ハーネスで実行したサイバースコアは外部監査が不能である¹⁵。なお「公開ベンチマーク」とはタスクセットが公開されている意味であって、実行自体が独立検証済みという意味ではない。
- 重み、API、ライセンスは発表時点で未確定である。GLM-5.3 のライセンスが MIT となるかは予想であって未確認であり、API 価格も未公表である。これらは公開後に必ず一次情報で再確認すべきである^{3,22}。
- サイバー能力の「意図せぬ湧現」というナラティブは Z.ai 自身の説明であり、「防御のための開放」というマーケティング的側面を含む可能性に留意すべきである。ExploitBench 等で攻撃能力がクローズド最前線に劣後する点は能力の偏り(防御寄り)という Z.ai の主張と整合的である一方、公開遅延の真因が純粋な安全性配慮か規制対応・広報戦略かは外部から断定できない^{4,15}。

- 公式技術ブログは本調査時にツール制約により直接取得できず、これを直接引用した第三者記事に依拠した部分がある^{11,12,13}。公式開発者ドキュメントおよび公式 X 投稿は取得・確認済みである^{2,3}。
- 競合モデル名(GPT-5.6 系、Claude Fable 5/Mythos 5/Opus 4.8、Gemini 3.x、Kimi K3、DeepSeek V4 Pro、Qwen3.8-Max 等)は各社の 2026 年時点のラインアップとして報道および Z.ai の比較表に登場するものであり、本レポートはそれらの詳細仕様を独立検証していない。特に Anthropic の呼称については Z.ai 公表資料内で同一数値に二つの名称が併記される不整合が第三者に指摘されており、命名の権威的解決は文書上不能である³⁹。
- ARR および時価総額の数値は、算定基準の差異(ARR は実収益ではなくラン・レート、時価総額は変動が極めて大きい)により出典間で差がある。確定財務値ではない点に留意されたい^{31,34}。
- 日本法・政策の解釈は 2026 年時点の状況に基づく。DS-920 が中国製モデルを名指しで制限する条文は確認されておらず、知的財産推進計画 2026 の「プリンシプル・コード(仮称)」は策定予定段階である。法および事実が未確定な部分については断定を避けた^{40,41}。
- 参考文献のうち、URL 末尾に「※URL 未検証」と付したものは、本調査の過程で記述内容は確認したが URL 自体を直接取得できなかったものである。引用にあたっては原典の再確認を推奨する。

参考文献

文中の上付き番号は下記の番号に対応する。アクセス日はいずれも 2026 年 8 月 15 日。

- [1] Z.ai 公式技術ブログ「GLM-5.3」<https://z.ai/blog/glm-5.3>(※直接取得できず、第三者記事による引用内容から確認。URL 未検証)
- [2] Z.ai 公式 X(@Zai_org)投稿、2026 年 8 月 14 日 https://x.com/Zai_org/status/2088132965922476159(※URL 未検証)
- [3] Z.ai 公式開発者ドキュメント「GLM-5.3」<https://docs.z.ai/guides/llm/glm-5.3>
- [4] Z.ai 公式 X(@Zai_org)記事「Preparing GLM-5.3 for Open Release: A Responsible Path to Cyber Defense」https://x.com/Zai_org/article/2088280509474320693
- [5] 百度百科「GLM-5.3」<https://baike.baidu.com/item/GLM-5.3/68244961>
- [6] IT 之家「智譜正式發布 GLM-5.3:編程能力最強開源模型、較 GLM-5.2 提升 50%」<https://www.ithome.com/0/989/689.htm>
- [7] 新浪科技「智譜正式發布 GLM-5.3」2026 年 8 月 14 日 <https://finance.sina.com.cn/tech/digi/2026-08-14/doc->

ininhhrs2630952.shtml

- [8] 掘金「GLM-5.3 技術測評:後訓練 Scaling 極限、編程能力提升 50%」
<https://juejin.cn/post/7673522589588783158>
- [9] CSDN「GLM-5.3 發布:基座不換只煉後訓、開源編程能力超越 Claude Opus 4.8」
<https://blog.csdn.net/aidoudoulong/article/details/163755988>
- [10] COINOTAG(重み公開日程および脆弱性発見件数に関する報道)※URL 未検証
- [11] The Decoder(Z.ai 公式ブログを引用した GLM-5.3 報道)※URL 未検証
- [12] MarkTechPost(GLM-5.3 の技術解説記事)※URL 未検証
- [13] Nathan Lambert, Interconnects(GLM-5.3 および中国勢の追従要因に関する分析)※URL 未検証
- [14] Decrypt「China's Z.AI Ships GLM-5.3, Calling It the Top Open-Weight Coding Model」
<https://decrypt.co/375684/china-z-ai-glm-5-3-top-open-weight-coding-model>
- [15] Unite.AI「Z.ai Launches GLM-5.3 With Frontier Coding and a Cyber Capability That Outgrew Its Training」
<https://www.unite.ai/z-ai-launches-glm-5-3-with-frontier-coding-and-a-cyber-capability-that-outgrew-its-training/>
- [16] The Agent Report「GLM-5.3: Z.ai Tops the Open Coding Leaderboard on Post-Training Alone」
<https://the-agent-report.com/2026/08/glm-5-3-zai-post-training-coding-cyber/>
- [17] byteiota「GLM-5.3: Open-Weight Coding SOTA and Emergent Cyber Risk」
<https://byteiota.com/glm-53-open-weight-coding-emergent-cyber/>
- [18] Fello AI「GLM 5.3: Benchmarks, Pricing and the Held-Back Weights」
<https://felloai.com/glm-5-3/>
- [19] AIToolsReview「GLM 5.3 Review: Benchmarks, Cyber Risk & Pricing (August 2026)」
<https://aitoolsreview.co.uk/insights/glm-5-3>
- [20] Kie「What Is GLM-5.3? Z.ai's Next Open-Weight Model」
<https://kie.ai/blog/what-is-glm-5-3>
- [21] GLM 5 情報サイト「GLM 5: Zhipu AI 745B LLM」
<https://glm-5.org/>
- [22] Hugging Face, zai-org(GLM-5.2 モデルカードおよび MIT ライセンス表示)※URL 未検証
- [23] BigGo Finance「Zhipu AI Releases GLM-5.3: Coding Capability Jumps 50%, Open-Source Weights Coming in Two Weeks」
<https://finance.biggo.com/news/0b571a42-9531-433c-b81b-c8468d173989>
- [24] BigGo Finance「China's Zhipu Says Open-Source GLM-5.3 Outperforms Anthropic's Restricted Model in Vulnerability Detection」
<https://finance.biggo.com/news/b569502f-66a8-4fbc-94f1-8ffd61046cee>
- [25] BigGo Finance「Zhipu AI ARR Rumored to Hit \$2 Billion, Denied by Company; API Users Near 7 Million」
<https://finance.biggo.com/news/e3302133-fac2-4e66-a927-847a6174f1fe>
- [26] Tech Times「GLM-5.3: Post-Training Produced Exploit Chains Z.ai Never Planned, Finds 1,097 Critical Bugs」
<https://www.techtimes.com/articles/324426/20260814/glm-53-post-training-produced-exploit-chains-zai-never-planned-finds-1097-critical-bugs.htm>
- [27] SaaSCity(発見された脆弱性の平均未発見年数に関する報道)※URL 未検証
- [28] Caixin Global「China AI Developer Zhipu Hits Record \$112 Billion Valuation」
<https://www.caixinglobal.com/2026-05-29/china-ai-developer-zhipu-hits-record-112-billion-valuation->

102449295.html

- [29] PR Newswire(智譜 香港取引所上場に関するリリース、2026 年 1 月 8 日)※URL 未検証
- [30] Bloomberg(智譜 上場初日終値に関する報道、2026 年 1 月 8 日)※URL 未検証
- [31] YourStory「China's Z.ai is closing in on \$1 billion in annual AI revenue」(Macquarie 分析を引用)<https://yourstory.com/ai-story/z-ai-1-billion-arr-coding-ai-growth>
- [32] The Next Web「Z.ai nears \$1bn in sales, and gives its models away」<https://thenextweb.com/news/a-chinese-ai-startup-is-about-to-hit-1bn-in-sales-while-giving-its-best-models-away-for-free>
- [33] Dealroom.co「China's Zhipu hits \$1B ARR in five months with coding model push」
<https://app.dealroom.co/news/feed/china-s-zhipu-hits-1b-arr-in-five-months-with-coding-model-push>
- [34] 36Kr / Intelligent Emergence(智譜 ARR 成長に関する独占報道)※URL 未検証
- [35] 米国商務省産業安全保障局、エンティティリスト追加に関する連邦官報告示(Federal Register 文書番号 2025-00704、2025 年 1 月 15 日、15 CFR Part 744)※URL 未検証
- [36] Axios(米政権による中国製先端 AI モデルのアクセス制限検討に関する報道、2026 年 7 月)※URL 未検証
- [37] Reuters(中国商務部とアリババ・字節跳動・Z.ai による海外向けモデル提供制限の協議に関する報道、2026 年 7 月 7 日)※URL 未検証
- [38] OpenRouter 月間トークン処理量統計(中国系モデルのシェアに関する集計)※URL 未検証
- [39] Digital Applied(Z.ai 公表資料における Anthropic モデル呼称の不整合に関する指摘)※URL 未検証
- [40] 知的財産戦略本部「知的財産推進計画 2026」2026 年 6 月 12 日決定 ※URL 未検証
- [41] デジタル庁「行政の進化と革新のための生成 AI の調達・利活用に係るガイドライン」(DS-920)v2.0、2026 年 6 月 12 日改定 ※URL 未検証
- [42] Manabia「政府の生成 AI ガイドラインが公開|令和 8 年からの適用内容と注意点まとめ」
<https://manabia.jp/column/ai-guidelines/>
- [43] 著作権法第 30 条の 4(情報解析等のための利用)および文化庁「AI と著作権に関する考え方について」※URL 未検証
- [44] 「人工知能関連技術の研究開発及び活用の推進に関する法律」(AI 推進法、2025 年 5 月 28 日成立)および AI 基本計画(2025 年 12 月 23 日閣議決定)※URL 未検証