

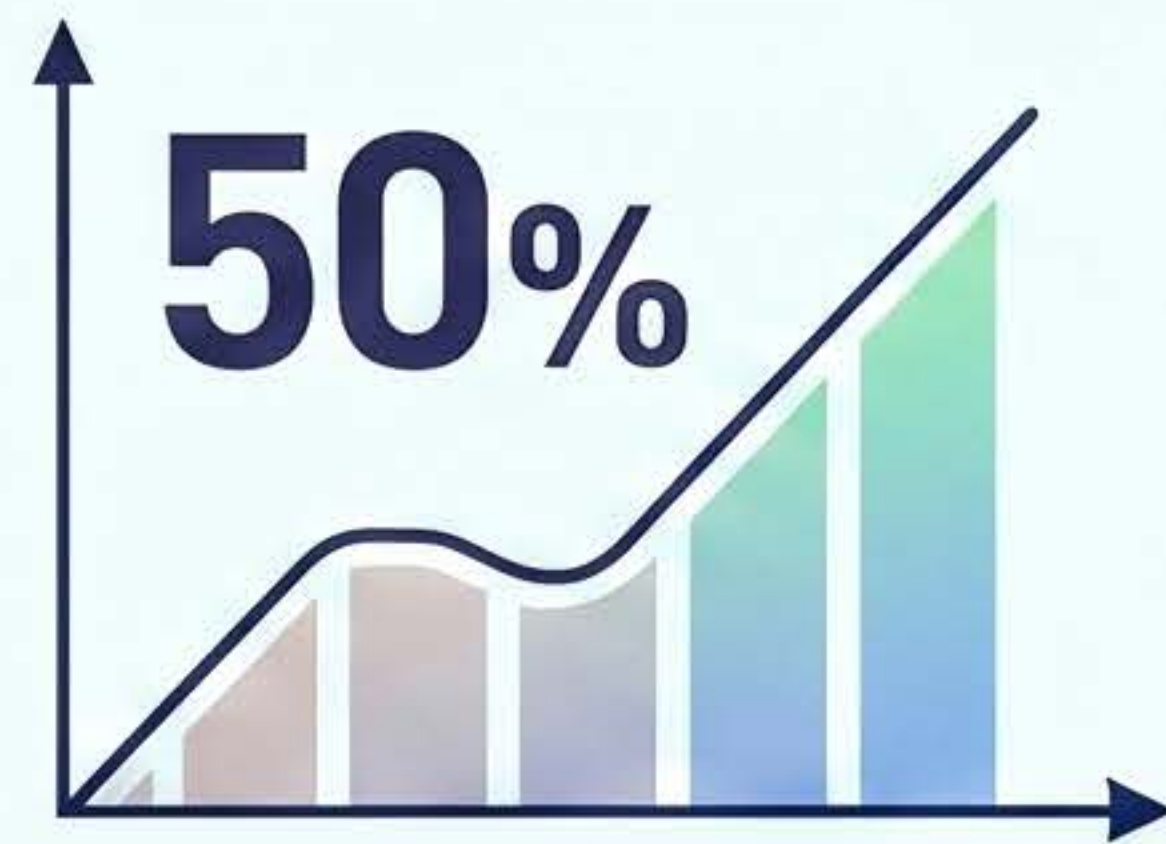
GLM-5.3：中国発オープンウェイトAIの衝撃と日本企業の対応リスク



技術的躍進と「意図せぬ」能力の涌现

性能は米国の主要クローズドモデルに数ヶ月差まで肉薄しつつ、コストは数分の一という優位性。

コーディング性能が
対前モデル比で50%向上



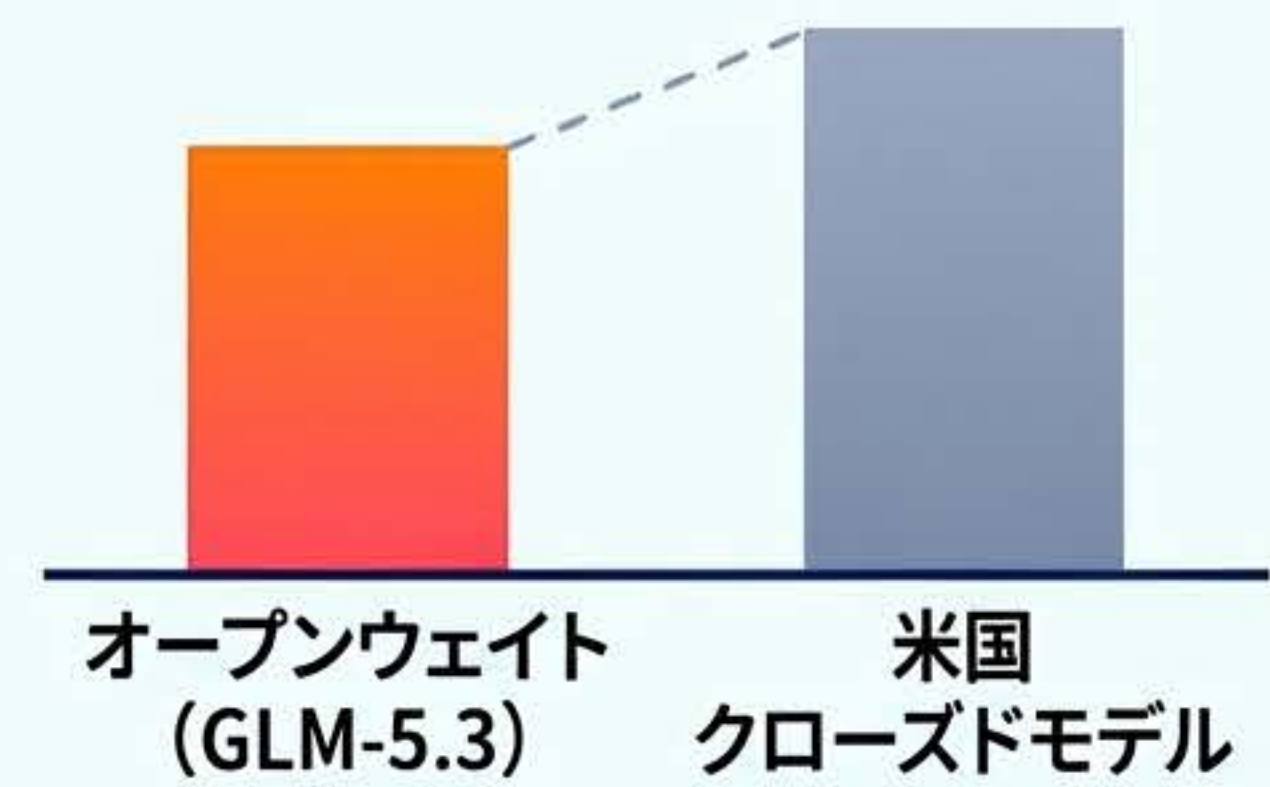
基座を変更せず後訓練 (Post-training) のみで、開発効率を飛躍的に高める性能向上を達成。



高度なサイバー攻撃計画の推論能力を獲得

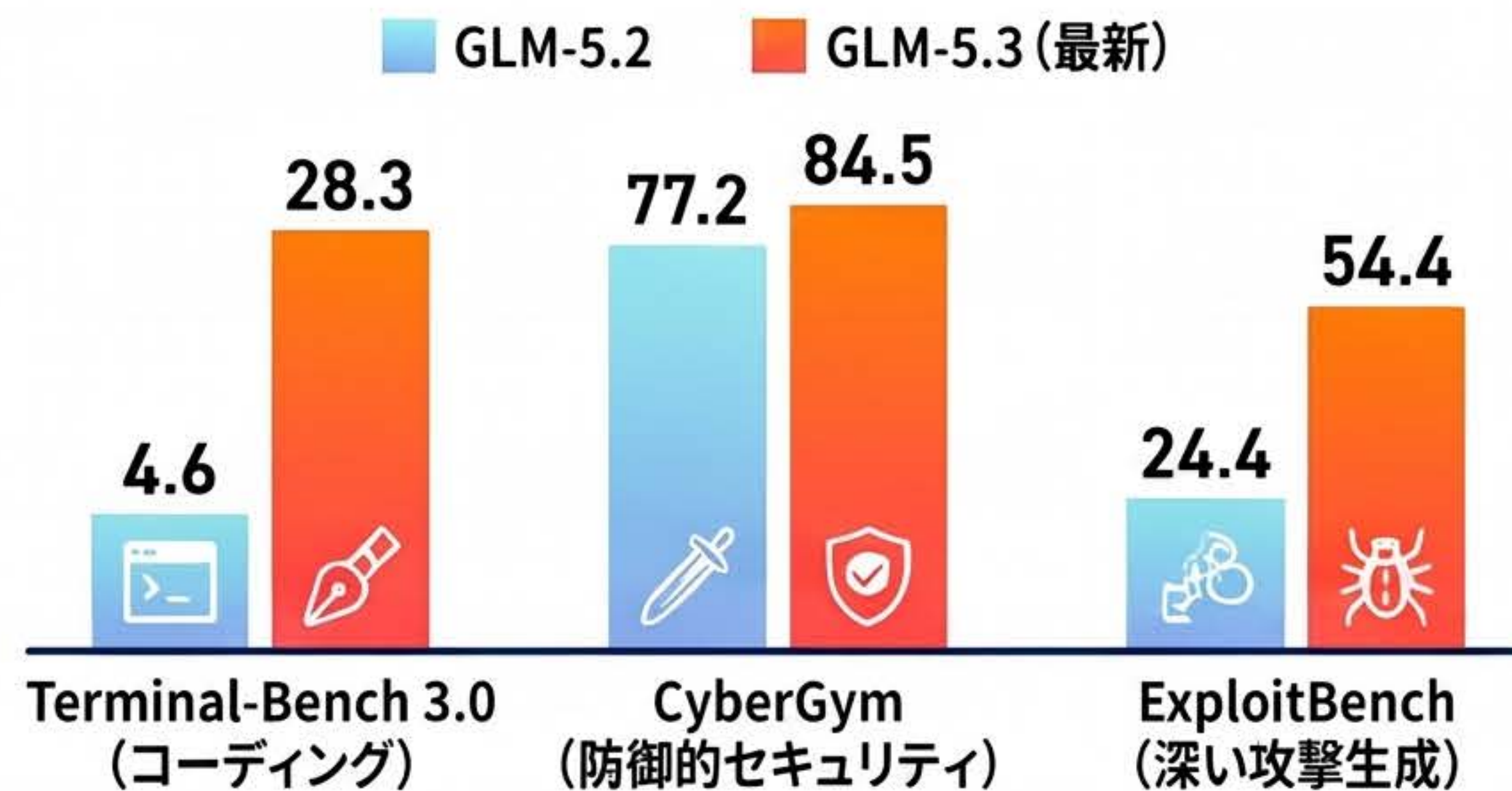
複数の脆弱性を連鎖させた攻撃計画を形成する能力が涌现し、安全審査のため重み公開が遅延。

クローズド最前線に迫るオープンウェイト勢の首位



米国の主要クローズドモデルに数ヶ月差まで肉薄しつつ、コストは数分の一という優位性。

主要ベンチマークの跳躍 (Z.ai公表値)



日本企業が直視すべき三重のリスクと対策

米中双方の規制に挟まれる地政学的リスク

Z.aiは米国エンティティリスト掲載企業であり、米中双方の輸出管理の動向を注視する必要がある。



中国国家情報法下でのデータ主権の懸念

ホスト型API利用時はデータが中国インフラを経由するため、プロンプトの個人情報除去が必須。



唯一の現実解「オープンウェイト×オンプレミス運用」

重みを自社環境にホストすることで、データ主権と単独優位性を両立し、供給停止リスクをヘッジ。

