

はじめに

近年の AI の発達には目覚ましいものがあり、各分野でその利用が進められている。防衛分野においてもその利用を図ることは当然であろう。効果的に利用できれば、いわゆるゲームチェンジャーとなる可能性もあると考えられる。本稿は、一般的に指摘されている AI の基本的な特徴を挙げ、それを踏まえた我が国の防衛における利用について戦略的な考察を試みるものである。

AI の基本的な特徴

一般的に指摘されている AI の基本的な特徴を筆者なりに整理すれば、次のとおりである。(なお、筆者は、AI については素人であり、本稿では、以下に引用する著作を始め、一般に公開されている生成 AI や AI 関連企業のインターネット上のサイト等から得た情報・知識に基づいて記述しているが、仮に誤りがあるとすれば責めを負うべきはもっぱら筆者であることを念のため付言しておく。)

第一は、動作の高速性である。これは、コンピューターの計算能力に由来するものであり、コンピューターを基盤とする AI の動作が高速であることは当然である。しかしながら、生成 AI が広く利用されるようになった結果、その回答の速さや的確さに多くの人が改めて驚かされているというのが実情であろう。

第二は、創造性である。これは必ずしもすべての AI の特徴ではないが、生成 AI は学習したデータからその背後にある「本質的な構造や表現をとらえ、新しいものを生み出すことができる」(今井翔太「生成 AI で世界はこう変わる」SB 新書)る。この特徴こそが AI 利用を飛躍的に拡大したと言えよう。実際、代表的な生成 AI であるチャット GPT は、「登場から 2 か月で月間 1 億人が利用するサービスに」(岡野原大輔「大規模言語モデルは新たな知能か」岩波科学ライブラリー 319) なったとされる。

第三は、博識性である。これは、AI モデルの種類、サイズ、データの学習度合によるが、例えば、一般に公開されているチャット GPT は、主としてインターネット上の公開情報を学習しているとされる。そうだとすれば、そのデータ量はすでに天文学的ということになる。しかも、生成 AI の性能は、「モデルサイズ、学習に使用するデータセットの量、学習に使う計算量で決まる」(今井前掲)とされていることから、生成 AI の性能を上げようとするれば、より多くのデータを学習させることが必要となる。したがって、AI、特に生成 AI は、途方もなく博識な存在と言える。

第四は、発達途上性である。第三の点と関連するが、AI は、学習によって日々性能を向上させ続けており、少なくとも現時点ではその限界は知られていない。したがって、今日、

AI 関連企業が競って巨大なデータセンターの建設を進めているのは当然と言える。

第五は、適確性と不完全性である。膨大な情報・知識を背景に持つ生成 AI は、統計と確率に基づき、幅広い問題に適確な答えを提供できる一方、少なくとも現時点では、完全無欠ではない。例えば、存在しない情報を作り出してしまう「幻覚（ハルシネーション）」と呼ばれる現象が生じることが知られている。また、「破滅的忘却」と呼ばれる回答精度の急激かつ大規模な低下が知られている。これらの問題点については、解決の努力が続けられているが、まだ完全解決には至っていない模様である。

第六は、膨大なコストの可能性である。大規模な AI モデルではデータを学習させる過程で膨大な電力が必要になることが知られており、AI の発達とともに、AI のコストが急速に増大していく傾向がある。今日では、「一つのモデルの学習には、数百人から数千人が関与し AI 向け半導体が数千個から数十万個規模で用いられ、消費電力は数百メガワットに達する（数百メガワットは、数十万世帯分を支える電力）。学習期間も数か月から一年程度に及ぶことが珍しくなくなっている」（岡野原大輔「ヒトと AI」岩波新書）とされる。

我が国防衛の戦略的課題

今日の AI は、防衛関連のほとんどすべての業務に利用可能だと考えられるが、当然のことながら、我が国防衛の戦略的な課題の解決に優先的に用いられるべきであろう。特に、AI の導入にかかる時間やコストを考慮すれば、少なくとも見通し得る将来にわたって継続することが見込まれる重要課題がこれに当たることになる。

そのような課題としては、第一に、防衛力整備の迅速化・効率化が挙げられる。ますます厳しさを増す安全保障環境に鑑みれば、防衛力の抜本的な強化に当たって防衛省・自衛隊が重視する 7 つの機能・能力を始め、所要の機能・能力を可能な限り早期に整備する必要があることは明らかである。そのためには、それらの整備に要する予算を確保し、それを着実に執行していくことが何よりも必要である。

第二に、省力化・省人化である。我が国の就労適齢人口は、見通し得る将来にわたって確実に減少する。したがって、自衛隊が確保し得る隊員の数も今後確実に減少していくと見るべきである。十分な予算を確保して募集の強化や処遇の改善等の措置を最大限講じることが当然としても、それでもって所要の人員を将来にわたって確保できると期待すべきではないであろう。そうなれば、予算を確保しても、防衛力整備が計画通りには進まなくなる可能性が出てくることになる。

第三は、情報・部隊運用能力の向上である。現代戦においては、宇宙、ミサイル、ドローン、電子戦等の先進技術の発達により戦域・戦場の広域化・複雑化が進んでおり、これに対応して戦況をリアルタイムに把握し、迅速に判断・攻撃し得る能力が必要となっている。この点において後れを取れば、敵に主導権を委ねたままで戦うことを余儀なくされ、不利を免れないこととなる。

AI の用途

AI は、防衛力整備の迅速化・効率化には寄与し得るであろうか。防衛分野における AI の利用は、今日の生成 AI が文書作成全般を人並み以上に行えることから、おそらくほとんどすべての業務に及び得る。防衛力整備のプロセスにおいても、整備計画の立案、予算の計上、予算の執行等の各業務に利用可能であり、有用であると考えられる。例えば、防衛力整備計画関連のデータを学習した生成 AI であれば、新たな整備計画の原案を極めて短時間で作成することが可能であろう。従来人が一週間かけて作っていた原案が一日足らずでできるかもしれない。そうであれば、原案作成が著しく容易になることは明らかである。それどころか、将来、防衛省のみならず財務省等関係省庁が AI エージェントⁱⁱに予算関連業務を委ね、AI エージェント間のネットワークが構築されれば、概算要求から予算編成までの時間が劇的に短縮される可能性も十分に考えられる。また、予算額が飛躍的に伸びる一方で予算に携わる要員数が増えない現状にあつて、予算執行は、防衛省・自衛隊にとって最も効率化が求められる業務であり、実際に施設整備における ECI のような新たな発注制度の導入等による効率化が図られているところである。こうした業務についても、既存の執行制度の枠内でのより効率的な業務遂行、あるいは、より効率的な執行制度の追求手段として、AI の導入・利用を図る余地はあり得るであろう。

しかしながら、各業務の迅速化・効率化が実際にどの程度実現できるかは、AI が発達途上にあることや関連業務の迅速化・効率化の進捗度合等により、少なくとも現時点においては明確とは言い難い。防衛力整備計画の例で言えば、原案作成が早まっても、その内容のチェックを始め、関係者間で議論や調整が重ねられることとなれば、結論を得るまでに要する時間は従前と大差ないということも起こり得る。また、予算は基本的に年度単位で進められるプロセスであり、これを短縮することは困難であることから、防衛力整備の迅速化には現行制度上の限界がある。さらに、専用の AI モデルの開発・運用には膨大なコストが必要となり得ることも考慮する必要がある。これらの点を勘案すれば、防衛力整備関連業務については、チャット GPT のような一般の利用に供されている AI モデルや簡易なカスタマイズを施された AI モデルの利用をまず検討することとし、高度にカスタマイズされた AI モデルの開発は、民間での成功例の検証等を通じてその効果が相当程度見通せた場合に着手することとすべきであろう。

省力化・省人化については、予算関連業務の迅速化と同様、事務的な業務については AI がどの程度寄与するのかは必ずしも明らかでない。生成 AI が文書や画像を迅速に作成しても、前述のように、少なくとも現時点ではこれをノーチェックで利用できるわけではないからである。AI が作成した文書等を人間がチェックする必要や議論する必要があるとすれば、必ずしも相当な省力化・省人化にはつながらないであろう。実際、AI 利用の先進国である米国においては、コンピュータープログラミングについては、生成 AI の成果物をチェックするため、プログラマーが引き続き必要とされている旨の報告がある。もっとも見方によっては、これまでの人間の作業にも誤りはあり得るわけであり、どこまで適確性を求めるかは、

程度の問題に過ぎないとも言えよう。ただし、適確性の問題がクリアされたとしても、AIの成果物に対して責任を負う人は必ず必要であり、そこにAIによる省力化・省人化の限界がある。

おそらくAIの活用による省力化・省人化が最も有望と考えられる領域は、装備品の自律化であろう。自衛隊の職階性において最も充足に困難をきたしているのは曹士、すなわち装備品取り扱いの中心となる階級である。車両、艦艇、航空機等の自律化やそれらの維持・整備の自動化はAIなしでは考えられない。実際、ウクライナ軍は、AIを利用した自律装備品をすでに実戦に投入していると伝えられている。ウクライナ軍自身はこれを先進的な取り組みとしてプレイアップしているようだが、実態としては深刻な兵員不足を補うためであることは明らかである。換言すれば、省力化・省人化にAIを利用した自律装備品の導入が有効であることが戦場で実証されつつあるということである。そうであれば、防衛省・自衛隊も、各種装備品について、自律化に向けたAIモデルの開発に早々に着手すべきであろう。念のために付け加えれば、装備品の自律化は、無人装備品の導入とは似て非なることには注意が必要である。無人装備品の多くは、遠隔操縦者を必要としており、省力化・省人化の効果は自律装備品ほど大きくないからである。なお、装備品の自律化は、新たな倫理的、法的な問題を提起する。本稿ではこの問題に深く立ち入らないが、そのような問題も並行して検討を進めるべきであろう。

情報・部隊運用は、AIの活用が潜在的に最も期待し得る領域であるとも言えよう。具体的には、まず情報分析、特に動態分析である。今日、情報業務においては、ヒューミント、シギント、イミント等多種多様な収集手段から得られた情報を迅速に総合分析し、対象地域・地点における対象物の動態を時々刻々と把握することが求められるようになっていく。得られる情報はしばしば膨大でもあり、個々の担当分析官がかかる要求に適時・適確に応えることはますます困難となっている。少なくとも識別AIⁱⁱⁱが分析を支援できる余地は大いにありと考えられる。例えば、学習されたデータに基づいて不明瞭な画像や音声を瞬時に解析することは、識別AIの得意技であろう。生成AIならば更なる寄与も期待し得る。例えば、断片的な情報から敵の戦略的・戦術的意図を「生成」してみせることも可能と考えられる。

また、こうした情報分析に基づく作戦計画の立案もまたAIの有力な活用先であろう。詳細は明らかにされていないが、米軍の指揮統制システムとして実用化されているMavenは、情報分析と作戦計画を一体的に支援する生成AIが使用されているものとみられる。この例からしても、作戦計画の立案へのAI利用が有望であることは明らかであろう。

もっとも、これらの業務向けのAIモデルの開発に直ちに本格的に着手すべきかという点、必ずしもそうではない。なぜならば、第一に、AIモデルの性能をどこまで求めるべきかという問題が未解決のままだからである。前述のように、AIモデルは、大規模化し、大量の学習データを投入すればするほど高性能化することが知られている。AIを活用する側が所要性能に限界を画さなければ、「多々益々弁ず」に陥ることになりかねない。また、経費面でも、際限のない状況に陥りかねない。第二に、どこまで実戦に役立つかも完全に証明され

ているわけではないということである。今次の米イスラエル・イラン戦争の初期にハメネイ最高指導者等イランの指導者多数を一举に排除するのに **Maven** が決定的に貢献したとの見方がある一方、その後の戦闘においては **Maven** ゆえに米軍がイラン軍を圧倒したという事例は聞かれない。また、これまでのところ戦闘全般において米軍が圧倒的に優勢であるとの評価も聞かれない。これまでのところ、印象論はともかく、AI が作戦計画の立案を始めとする軍隊の指揮統制にどこまで有用なのかについては、未だ定説はないと言ふべきであろう。

このような未解決又は未解明の点を勘案すれば、これらの業務においては、AI モデルの開発を進めながら、実際に利用を重ね、その有用性を検証していくという手順を踏むべきであろう。加えて、生成 AI に関しては、使用者側の指示（プロンプト）の巧拙によっても結果が異なるとされることから、かかる手順を通じて使用者側の要員養成・技量の向上も図っていくべきであろう。いわば AI と人間がともに学び、ともに成長することが期待される手順とすることが理想と考えられる。その中で、先の第一の問題の答えも見いだせるであろう。

AI の国産化

AI を国産化すべきか否かという問題は、防衛分野における AI 利用については特に重要である。なぜならば、防衛においては、セキュリティの問題が極めて重要だからである。この観点からすれば、国産 AI が最善であることは言うまでもない。しかしながら、一方で、国産 AI が米中のような先進国の AI の後塵を大きく拝していることは厳然たる事実である。これに追いつくことは、経済的にも時間的にも容易でない。米中の AI が日進月歩の勢いで高性能化していることを考慮すれば、国産 AI がこれに追いつくのを悠長に待っているわけにはいかないであろう。 そうだとすれば、短期的にはセキュリティに十分に配慮しつつ外国の先進的な AI を利用するとともに、長期的に国産 AI の開発に注力するしかないということになる。ちなみに、国産 AI 開発を標榜する **Sakana AI** の取り組みは実質的には前者に当たり、正確には準国産開発だが、スタートアップとしては現実的なアプローチと言ふべきであろう。

短期的なセキュリティの確保は難問である。外国製 AI を導入する場合、AI モデルの詳細（モデルサイズ、アルゴリズム、学習履歴等）はブラックボックス状態で提供されることが通常と考えられるからである。AI モデルの開発企業が巨額を投じて開発した AI モデルの詳細の開示を行うことはおよそ考えられない。もちろん契約上はセキュリティ保証条項を盛り込むことになろうが、顧客が知らない間に AI モデルに学習させたデータが外部に流出する危険を顧客側で確実に回避することは極めて困難である。技術的には、おそらく AI の通信状況を常時監視して異常を感知するシステムを AI と同時に導入するぐらいが関の山であろう。また、AI の運用要領としては、当初は機密度の低いデータを学習させて様子を見つつ、機密度の高いデータの学習に移るという段階的なアプローチが考えられる。

長期的な国産 AI 開発については、オープン AI やアンソロピックのような米国の先進企

業が開発に取り組んでいるような汎用 AI の後追いは見込み薄であり、防衛省・自衛隊としては、いわゆるフィジカル AI に相当する自律装備品向けの AI の独自開発を目指すことが有用かつ現実的であろう。

AI 利用に向けたアプローチ

以上の議論を踏まえ、我が国の防衛における優先順位の高い AI 利用に関して具体的なアプローチを整理すれば、次のとおりである。

第一に、予算関連業務については、無料又は安価に提供されている AI モデルをベースとして、各業務固有のデータを学習させてカスタマイズすることを検討する。かかる業務であれば、セキュリティにさほど注意を払う必要はないであろう。

第二に、装備品の開発業務については、AI による装備品の自律化に向けた取り組みを本格化させるべきである。隊員が乗組み又は操作するあらゆる装備品が対象となり得る。取り組みに当たっては、総合的、効率的な開発の推進のために、防衛装備庁に「装備品自律化推進本部（仮称）」のような開発業務の統括組織を設けるべきであろう。併せて、内局に LAWS の規制に関する検討組織を設置して自律化関連 AI モデルの開発にその検討成果を反映させていくことも必要であろう。

第三に、情報・部隊運用業務については、まず、多様な手段によって収集される情報の総合的な分析・評価のための AI モデルの開発に着手すべきである。要求されるセキュリティが最高レベルの業務であることから、準国産開発が望ましい。次に、Maven のような指揮統制のための AI モデルの開発である。これも、同様な理由から準国産開発が望ましい。なお、動態情報は部隊運用と密接に関連しているので、動態情報の分析・評価と部隊運用を一体的に支援する AI モデルの開発も一考に値するであろう。これらの AI モデルの早期開発のためには、外国製の先進的な AI モデルをベースとする準国産開発とすることはやむを得ない。その場合、さすがに中国製を利用するわけにはいかないことから、セキュリティに関し前述のような措置を講じつつ、米国製を利用するしかないであろう。装備品については、我が国は長くブラックボックス状態で多くの米国製品を導入・調達してきたところであり、AI モデルについても同様の状況が生じることも少なくとも短期的にはやむを得ないと割り切るべきであろう。

AI に係る権限と責任

AI に係る権限と責任の問題は、AI の導入・利用に当たって整理しておかなければならない基本的な課題である。

一般に、組織において業務を処理するために権限と責任が構成員に対して配分されていることは周知の事実であろう。この二つは表裏一体・不即不離の関係にあることは言うまでもない。これに対して、AI、特に AI エージェントの導入・利用は、そのような体系に変更を迫る可能性が考えられる。AI エージェントは、適切に指示を与えれば、幅広い業務を迅

速かつ確実に処理してくれる。十分な学習を了した AI エージェントになれば、おそらく組織経営をすべて任せることすらも可能であろう。その場合には、権限と責任の配分も不要になるとも考えられる。

しかしながら、人間は、少なくとも二つの責任から逃れることはできないであろう。それは、監督責任と結果責任である。特に後者は回避不能と言ってよい。AI は完全に正しい存在ではないので、例えば、AI に化学会社の経営を任せた結果として環境問題が発生し得る。その場合、AI にその責任（刑事責任/民事責任）を取らせるわけにはいかないことは明白である。誰であれ人間が責任を負わざるを得ない。そうだとすれば、AI に対する監督責任もほぼ必然的に避けられないと言うべきであろう。結果にだけ責任を持つ気にはなれないのが人情だからである。したがって、権限と責任の配分の体系は、基本的には維持される必要がある。ただし、AI の能力と信頼性次第では、監督者の数を相当に減らすことは可能と考えられる。

以上は組織に関する一般論だが、防衛省・自衛隊もその例外とは考えられない。むしろ、権限・責任配分の明確性が強く求められる自衛隊組織においてはより先鋭な課題と言うべきであろう。したがって、防衛省・自衛隊においても、今後 AI、特に AI エージェントを導入・利用するに当たっては、権限・責任配分の問題を予め又は少なくとも並行して検討する必要がある。

おわりに

AI は、大仰に言えば、時々刻々と進歩している一方、これを導入・利用するには一定の時間がかかる。このため、AI 利用をどのように進めればよいか、何が最善の利用方法なのかは、非常に悩ましい問題である。とはいえ、これらの問いに明確な答えが出るまで待っているのは、時代に取り残されて取り返しがつかなくなるおそれがある。そうだとすれば、暫定的であっても一定の戦略（らしきもの）を立て、それに基づいてある程度体系的に導入・利用を進めるべきであろう。本稿はそのような問題認識に立ったいわば試論であるが、我が国の防衛における AI の導入・利用の実務に何らかの参考となれば幸いである。

i 大量のデータからパターンや構造を学習し、テキスト、画像、音声、動画、プログラムコードなどの新しいコンテンツをゼロから自動生成する AI（人工知能）（Google の Gemini による定義）

ii 人間から与えられた目標を達成するために、必要なツールや外部システム（Web 検索、API、コード実行など）を自動で使いこなし、結果を評価しながら自律的にタスクを遂行するソフトウェア（同上）

iii 入力されたデータが「何であるか」を判別・分類・認識する人工知能（同上）