防衛省ＡＩ活用推進基本方針

令和６年７月

防　　衛　　省

要　約

１．本文書策定の背景と目的

人工知能（以下「ＡＩ」という。）がデジタル社会を形成する上で不可欠のものとなる中、防衛分野でもＡＩを活用する試みが広がっている。米国は多様なシステムと大量のデータを統合し状況認識や意思決定等を行うため、指揮統制システムにＡＩを適用することを検討し、軍の「智能化」を掲げる中国はＡＩを活用した無人アセットの強化に取り組んでいるとの指摘がある。我が国も、令和４年１２月に閣議決定した国家防衛戦略や防衛力整備計画で、無人アセット、指揮統制・情報関連機能、意思決定を支援する技術にＡＩの活用を進めることを明記している。

国家防衛戦略は、従来の戦闘様相が大きく変化する中、新しい戦い方に対応できるかどうかが今後の防衛力を構築する上で大きな課題となること、また、人口減少と少子高齢化が急速に進展する中、人員をこれまで以上に効率的に活用することが不可欠である旨を指摘している。ＡＩは、これらの課題を克服する技術の一つとなる可能性がある。

このような背景の下、防衛省・自衛隊のＡＩ活用に関する考え方を部内・部外に示すことにより、次のような効果の創出を目的として、防衛省ＡＩ活用推進基本方針（以下「本方針」という。）を策定することとした。

○　個別の取組の戦略性や一貫性を担保するとともに、データや人材という貴重な資源について、組織の垣根を越えて共通化を図ること

○　国民の理解を背景とする行政や、ＡＩ活用に関する他国との協力・連携を推進すること

○　防衛省・自衛隊の取組に対する予見可能性を高め、部外の企業や研究機関等との円滑な協力関係を構築すること

２．ＡＩの活用分野と方向性

ＡＩは、データから法則を見つけ出し、与えられた課題をその法則に当てはめて推論することにより、正解（と思われる）回答を出力するものである。ただし、現在のＡＩには、人間の周囲の状況を全て把握し何が課題となっているかを見出す能力はない。そのため、ＡＩの活用に当たっては、その活用自体を目的化するのではなく、まずは人間が具体的な課題を特定し、その課題克服のためにＡＩを役立てることができるか検討するというプロセスが重要となる。ＡＩの機能（本方針では、便宜上、分類、異常検知、回帰、自然言語処理、強化学習による行動の最適化に大別）と上記のような限界を考慮すると、ＡＩの活用に適した業務は、

○　克服すべき課題を人間が特定できていること
○　正解（と思われるもの）が存在すること
○　ＡＩの機能を用いることにより課題を克服できること
○　学習に必要なデータの質と量を確保できること
といった要素を備えるものになると考えられる(1)。このような要素や、他国での活用事例、防衛省・自衛隊で実際に進んでいる取組等を踏まえつつ、防衛省の所掌事務や自衛隊の任務に照らして活用分野を整理すると、①目標の探知・識別、②情報の収集・分析、③指揮統制、④後方支援業務、⑤無人アセット、⑥サイバーセキュリティ、⑦事務処理作業の効率化の７つの分野で重点的にＡＩの活用を図ることとする。これにより、意思決定の迅速化と情報収集・分析能力の優位性の確保や、隊員の負担軽減と省人化・省力化に取り組む。ただし、ＡＩの活用を上記７分野に限定する趣旨ではなく、課題克服のためにＡＩを活用できるものがあれば、まずは試行してみることも重要である。また、ＡＩが行うのは人間の判断のサポートであって、その活用に当たっては人間の関与を確保する必要があることに留意すべきである。

ＡＩには、一定の誤りが含まれることによる信頼性の懸念のほか、学習データの偏りなどに起因するバイアスや、誤用・悪用等の課題やリスクが伴うと指摘されている。そこで、総務省と経済産業省が策定した「ＡＩ事業者ガイドライン」で示されている、①人間中心、②安全性、③公平性、④プライバシー保護、⑤セキュリティ確保、⑥透明性、⑦アカウンタビリティ等の考え方を参考としつつ、国際社会や他国の防衛当局等との議論にも注意を払い、ＡＩがもたらすリスクの低減に取り組むこととする。さらに、防衛省・自衛隊が得た知見を共有するなどして、国際的な議論やルール作りにも積極的かつ建設的に参加していく。

３．ＡＩ活用推進に向けた取組

国家防衛戦略は、我が国の防衛上必要な７つの機能・能力を示しているが(2)、ＡＩはそのいずれの文脈においても、具体的な課題の解決やそれぞれの機能・能力の強化に貢献できると考えられる。７つの機能・能力のうち、陸・海・空自衛隊の様々な装備品を情報通信ネットワークで連接し、部隊や個々の装備品が、同ネットワークを介して、探知・識別等で得られた情報をデジタル化されたデータの形で処理し、統合された指揮統制の下で行動することが肝となる領域横断作

(1) ＡＩの学習方法として強化学習を採用する場合、学習データを確保することは必ずしも求められない。
(2) ①スタンド・オフ防衛能力、②統合防空ミサイル能力、③無人アセット防衛能力、④領域横断作戦能力、⑤指揮統制・情報関連機能、⑥機動展開能力・国民保護、⑦持続性・強靭性の７つ。

戦能力を例にすると、目標の探知・識別の精度向上や指揮官への行動方針案の提示等のためにＡＩを活用し、探知・識別から意思決定に至る過程の優位性や迅速性を確保することが考えられる。ＡＩは、このような形で新しい戦い方に対応できる防衛力の一部を構成することとなろう。また、防衛力の抜本的強化に向けてＡＩ活用を進める上で、好事例や教訓を組織横断的に横展開し、今後の取組にフィードバックするプロセスを確立することとする。

領域横断作戦の実効性を上げるためには、ＡＩの活用のほかにも、陸・海・空自衛隊の組織の壁や個々の情報システムの仕様を越えて、必要な者が必要なデータにアクセスできる状態を実現することが欠かせない。そこで、全ての隊員を対象に「データは任務遂行に不可欠な戦略アセットである」との意識を涵養しつつ、データの設計・作成から利用に至るまでの連続的な管理を行うデータマネジメントの取組を進めることとする。

ＡＩの性能を維持・向上させるためには、データマネジメントに加え、人材の確保・育成も必要である。防衛省・自衛隊では、業務でＡＩを利用することによる知識やスキルの習得に加え、ＡＩ講座等を開講するなどして、隊員のＡＩリテラシーの向上を図るとともに、ＡＩの研究開発や維持管理に携わる者とそれぞれの部署でＡＩの活用に取り組む上でそれをリードするプロジェクトリーダーの育成を進め、部署ごとの状況に即した具体的な課題の克服に取り組む。同時に、ＡＩの技術革新は民間を中心に進んでいること、ＡＩ関連の全ての業務を隊員のみで処理するのは現実的ではないことから、民間のＡＩ・データ人材への積極的なアプローチを行う。

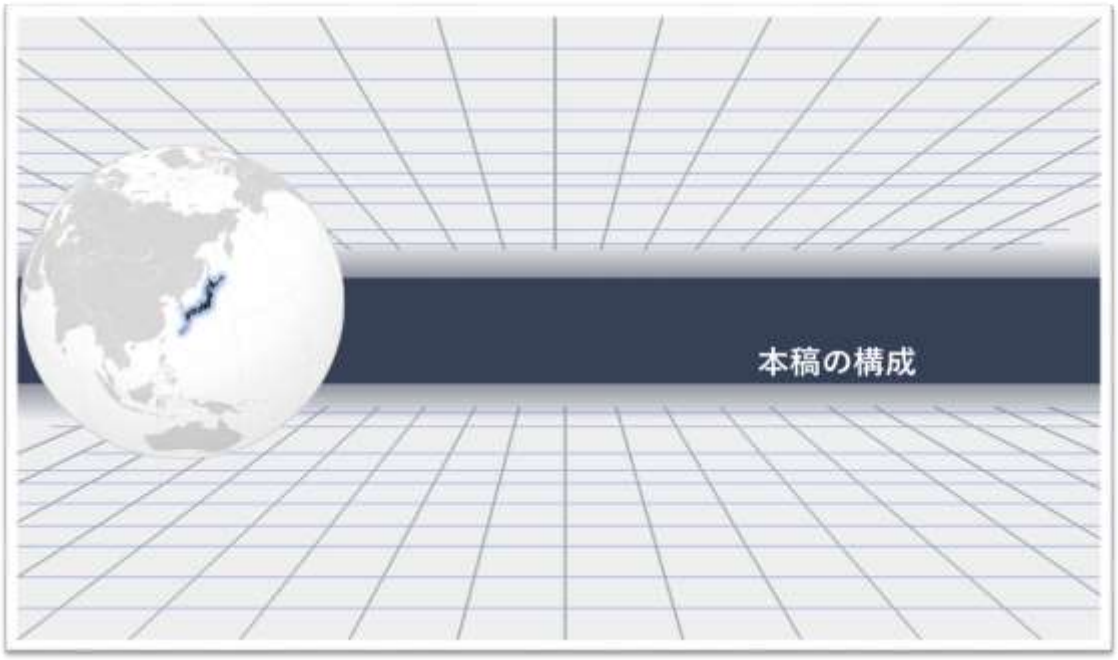
ＡＩを使った装備品の研究開発については、国際的な議論の文脈で我が国が表明している一連のコミットメントをどのように具体化するかについて、「ＡＩ事業者ガイドライン」を参考としつつ、他国の政府機関等との議論を通じて検討を深め、防衛省・自衛隊独自のガイドラインを策定する。

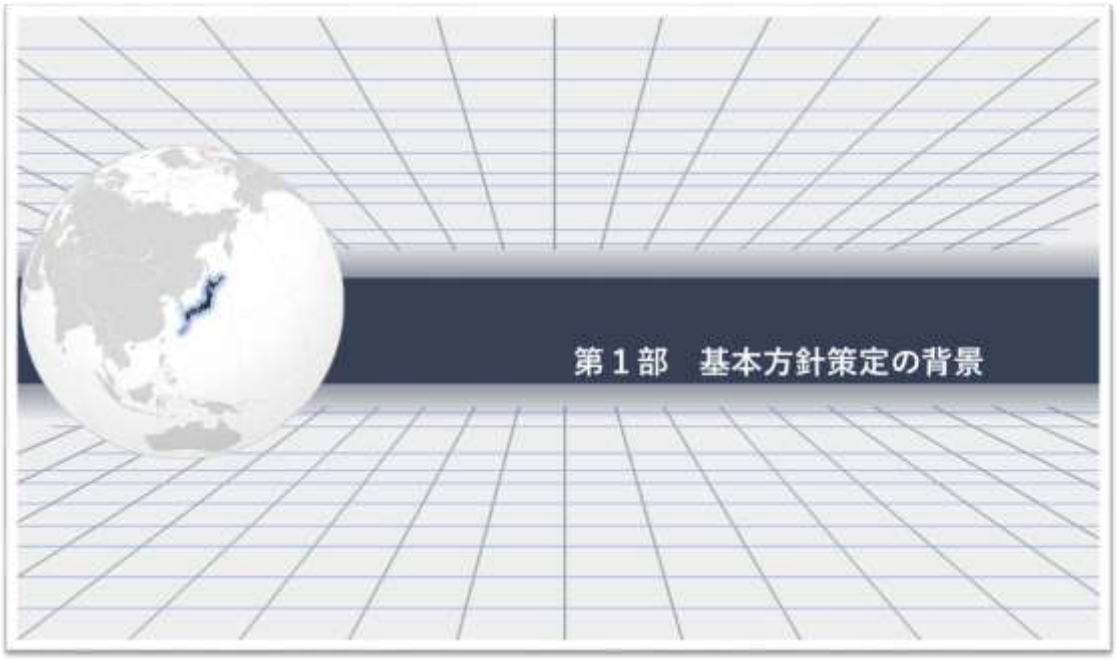
このほか、外部の教育・研究機関との協力関係の拡大・深化、国際的な協力・連携の拡充、防衛分野におけるＡＩの利用に関する国際的な議論やルール作りへの積極的かつ建設的な参加、ＡＩ以外の先端技術の活用等にも取り組む。

生成ＡＩについては、政府における検討状況を踏まえながら、できる限りリスクを低減することを重視して導入に取り組む。実際に業務で生成ＡＩを使用することを通じて隊員のリテラシー向上を図るとともに、必要に応じ課題を抽出し対策を講じることで、リスクを受容可能な水準で管理しつつ、便益を最大化することを追求する。

日本社会全体とともに自衛隊が人口減少に直面する中、ＡＩは課題解決の重要なツールであるとともに、これらの取組は将来的な組織の構成や文化の改革の基盤となるものである。国家安全保障戦略には、「我々は今、希望の世界か、

困難と不信の世界のいずれかに進む分岐点にあり、そのどちらを選び取るかは、今後の我が国を含む国際社会の行動にかかっている」と記されている。その言葉を防衛省・自衛隊におけるＡＩの活用に当てはめれば、「我々は今、ＡＩの活用により効率的で将来を自ら創り出す組織となるか、後れをとって非効率で旧態依然の組織となるのかの分岐点にあり、そのどちらを選び取るかは、今後の我々の努力にかかっている」と言えるだろう。


本稿の構成


第１部　基本方針策定の背景

第１部　基本方針策定の背景

１．基本方針策定の背景と目的

（１）基本方針策定の背景

ＡＩは、ものづくり、物流、医療、金融などの様々な分野で急速に活用が進み、今やデジタル社会を形成していく上で不可欠の要素となっている。特に２０２２年１１月に米国 OpenAI 社が発表した ChatGPT は大きな話題となり、生成ＡＩによって仕事や生活の在り方が大きく変わる可能性も指摘されている。２０１９年には、統合イノベーション戦略推進会議が「ＡＩ戦略２０１９」を発表し、今後のＡＩ利活用のための方針が示された。２０２２年には、同会議から「ＡＩ戦略２０２２」が発表され、ＡＩの社会実装を推進しているところである。

防衛分野においても、令和４年１２月に閣議決定した国家防衛戦略や防衛力整備計画では、例えば無人アセット、指揮統制・情報関連機能、指揮官の意思決定を支援する技術にＡＩの活用を進めることが記されている。他国でも軍事分野でＡＩを活用する試みが行われており、例えば、米国では、「ＡＳＴＡＲＴＥ計画」(ASTARTE: Air Space Total Awareness for Rapid Tactical Execution)の下、多様なシステム・大量のデータを統合し、状況認識や意思決定などを行うため、指揮統制システムにＡＩを適用することを検討している。先端技術を応用した軍の「智能化」を掲げる中国は、ＡＩを活用した無人アセットの強化に取り組んでいるとされる。

国家防衛戦略は、我が国の防衛目標として、

- 力による一方的な現状変更を許容しない安全保障環境を創出すること、
- 我が国の平和と安全に関わる力による一方的な現状変更やその試みについて、我が国として、同盟国・同志国等と協力・連携して抑止し、これが生起した場合でも早期に事態を収拾すること、
- 万が一、抑止が破れ、我が国への侵攻が生起した場合には、その態様に応じてシームレスに即応し、我が国が主たる責任をもって対処し、同盟国等の支援を受けつつ、これを阻止・排除すること、

を掲げている。同戦略は、このような防衛目標を実現するためのアプローチの一つとして、「我が国自身の防衛体制の強化として、我が国の防衛の中核となる防衛力を抜本的に強化するとともに、国全体の防衛体制を強化すること」を示している[(3)]。防衛力の抜本的強化を進める上で、ＡＩのような先端技術に関しては、「科学技術の急速な進展が安全保障の在り方を根本的に変化させ、各国は将来

(3) このほかのアプローチとして、「同盟国である米国との協力を一層強化することにより、日米同盟の抑止力と対処力を更に強化すること」、「自由で開かれた国際秩序の維持・強化のために協力する同志国等との連携を強化すること」も示している。

の戦闘様相を一変させる、いわゆるゲーム・チェンジャーとなり得る先端技術の開発を行っている」との認識を示しつつ、従来の戦い方の様相が大きく変化しており、新しい戦い方に対応できるかどうかが今後の防衛力を構築する上で大きな課題であると指摘している。さらに、人口減少と少子高齢化が急速に進展している我が国では、人員をこれまで以上に効率的に活用することが必要不可欠であるとも強調している。ＡＩという言葉に必ずしも明確な定義があるわけではないが、大量のデータに対して、高度な推論を的確に行うことを目指したものと大まかに捉えた場合、ＡＩがこれらの課題を克服する技術の一つとなる可能性がある。

実際、防衛省では、翻訳などの事務処理作業に加え、サイバーセキュリティ、意思決定支援、目標の探知・識別、情報戦への対応、整備・補給等の後方支援業務、無人アセットといった分野でＡＩの活用を進めている。

一方で、深層学習(4)に代表されるＡＩは、ドメインシフト(5)の問題が指摘されているように、課題解決に即したターゲット集団のデータを用いて学習を行わなければ精度が低下することが知られており、防衛省でＡＩの活用を進める中でも、データを蓄積するための基盤の整備や、ＡＩに学習を行わせる要員の確保・育成が課題となっている。その意味において、防衛装備品にＡＩを活用するに当たっては、単純にシステムのハードウェアやソフトウェアをアップグレードするだけでは十分でなく、ＡＩの性能を維持管理するデータ基盤や人材が備わっているのかという点も考えなければならない。さらに、「責任あるＡＩ」（Responsible AI）を始めとする考え方に沿った運用が求められている。

（２）基本方針策定の目的

他国で軍事分野へのＡＩの導入が試みられる中、我が国でも国家防衛戦略等でＡＩの活用が明記され、防衛省では既にいくつかの事業が行われている。今後もＡＩを活用する事業を進める上で、個別の取組を貫く基本的な方向性や、ＡＩを扱う上で不可欠となるデータ基盤の整備や人材の確保・育成に関する防衛省の方針を体系的に示すことにより、個々の取組の戦略性や一貫性を担保するとともに、データや人材という貴重な資源について陸・海・空自衛隊の垣根を越えて共通化を図ることが容易になる。また、防衛省がいかなる考え方に基づきＡＩの活用を進めるのかを示すことにより、防衛省の取組に関する国民や諸外国の理解を促し、ひいては国民の理解を背景とする行政の推進や他国の防衛当局との協力を容易にすることに寄与すると期待される。さらに、ＡＩ活用を進める上

(4) 多数の層から成るニューラルネットワークを用いて行う機械学習のこと。近年、急速に発展した生成ＡＩについても深層学習を用いている。
(5) 学習データと運用時（推論時）のデータの分布が一致せず、出力した回答の精度に影響が生じる現象。

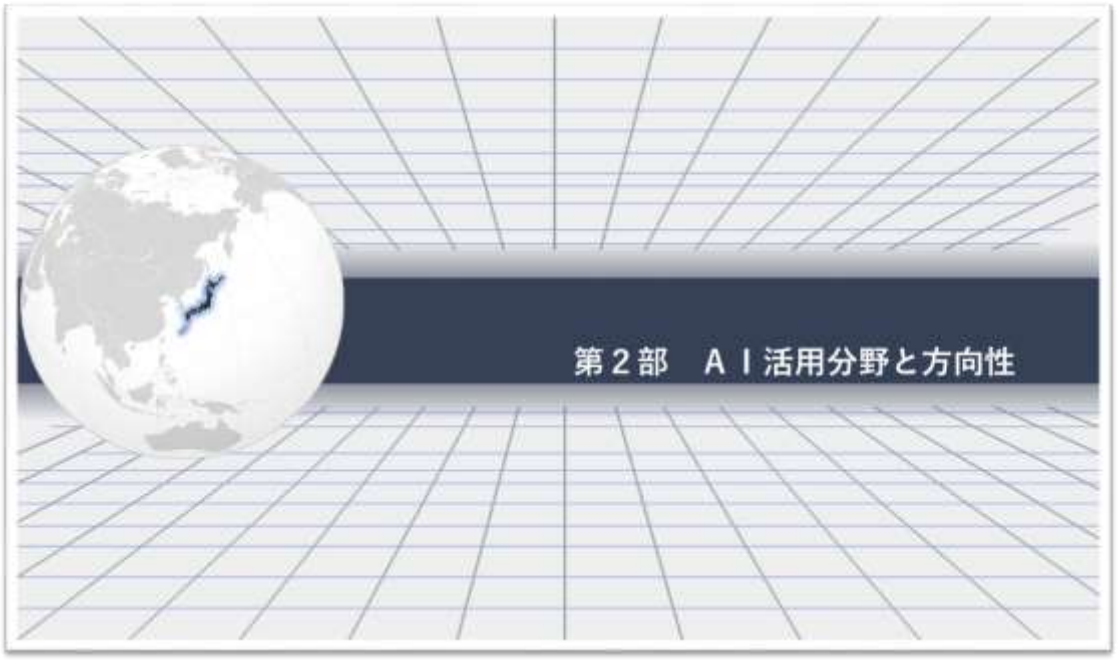
で、国内外の企業や研究機関との協力も重要である。そこで、防衛省がＡＩをどのように活用するのか示すことができれば、防衛省の取組に対する予見可能性が高まり、ひいては企業や研究機関との円滑な協力関係の構築に資すると考えられる。

今般、上記のような効果の創出を目的として、本方針を策定することとした。本方針では、ＡＩの活用分野と方向性を示すとともに、ＡＩ活用推進に向けた今後の取組を示すこととする。

２．本方針で扱うＡＩの定義

ＡＩという言葉に明確な定義はなく、機械学習(6)を使用するもの以外にも、ルールベース(7)などの他の技術を使用するものが含まれ得る。しかしながら、機械学習を使用したＡＩは、旧来のルールベースを使用するものに比べ複雑な処理が行えるようになり、その恩恵が増した一方、学習データの偏りなどに起因するバイアスが生じる可能性やデータ管理を強化する必要があることなど、機械学習登場以前のＡＩでは考慮を必要としなかったような対策を講じることが求められる。本方針はそれらに関する基本的な方向性を示すことも目的の一つとしているところ、本方針におけるＡＩとは、近年急速に発展している生成ＡＩを含め、機械学習を使用するものを念頭に置くこととする。

(6) コンピュータが数値やテキスト、画像、音声などの様々かつ大量のデータからルールや知識を自ら学習（見つけ出す）技術。
(7) 人間が定めた明確なルールや条件に基づいて動作するもの。


第２部　ＡＩ活用分野と方向性

第２部　ＡＩの活用分野と方向性

１．ＡＩの機能と限界

民間分野においてＡＩに係る技術革新が急速に進展し、諸外国の防衛当局がＡＩの活用に取り組む中、近い将来、ＡＩの活用が戦闘様相を決する可能性が指摘されている。ＡＩは、その活用により戦闘のスピード・精度・効率の向上、ヒューマンエラーの削減、省人化・省力化につながることが期待されており、多くの領域に変革をもたらし得るゲーム・チェンジャー技術とも指摘される。

ＡＩは、データから法則を見つけ出し、入力された課題をその法則に当てはめて推論することにより、正解（と思われる）回答を出力する。ＡＩに正解（と思われる）回答を出力させるためには、学習に必要なデータの質と量を確保することが重要となる。民間分野では、データを活用した学習を繰り返すことにより精度が向上するというＡＩの特性から、反復・継続的で、膨大なデータをもとに迅速な情報処理を行う能力が求められる業務にＡＩを導入する傾向がある。そのような業務で使われるＡＩの機能はいくつかに分類できるが、本方針では、便宜上、①分類、②異常検知、③回帰（入力データから連続値を予想して出力。例えば、季節、気温、天候等をもとに特定の商品の売行きを推測。）、④自然言語処理、⑤行動の最適化（強化学習(8)により、累積報酬が最大となる行動を提示）の５つに大別する。

一方で、ＡＩはデータによる学習を前提とするため、前例のない状況では出力する回答に限界がある。また、ＡＩ自体には人間の周囲で起きている複合的な状況を全て把握し何が課題となっているのかを見出す能力はないため、人間が課題を特定し、その課題の克服のためにＡＩをどのように使うのか決めなければならない。その意味において、ＡＩの活用に当たっては、ＡＩの機能と限界を念頭に置きつつ、人間が特定した課題を克服する上でＡＩを活用することが有効かを考える必要がある。ＡＩの活用自体を目的としてしまい、ＡＩの機能や限界を考慮することなくＡＩの活用を検討することは避けるべきである。

ＡＩの機能と限界を考慮すると、防衛省・自衛隊がＡＩを活用する場合も、民間分野での活用例と同様、分類、異常検知、回帰、自然言語処理、行動の最適化といった機能を活かすことのできる業務が基本となろう。さらに、学習データの質と量を確保しなければならないことを勘案すると、行政組織としての防衛省が行う反復・継続的な事務処理作業での活用はもちろんのこと、日々の警戒監視活動や情報収集活動、後方支援活動、サイバー攻撃対処を通じて蓄積したデータ

---

(8) 機械学習の一つ。コンピュータが一定の環境の中で試行錯誤を行うことが学習用データとなり、行動に報酬を与えるというプロセスを繰り返すことで、何が長期的に良い行動なのかを学習する方法。

を活用することで、ＡＩの効果的な活用が可能になると考えられる。また、幾何級数的に増大するセンシングデータを、ＡＩを搭載したエッジコンピューティング(9)で処理し必要な対応を講じるプロセスや、ミッション・エンジニアリングの概念の下で行うシミュレーションにＡＩを活用することも有益であろう。

米国、中国、ロシアでは、取り得る選択肢を指揮官に示し意思決定を支援する技術、無人機を使った戦闘、多様なセンサーなどから得られるデータを分かりやすく表示することにより情勢判断を支援する技術（例えば、目標の探知・識別と対処目標の優先順位の提示）などにＡＩの活用が検討されているとの指摘がある。さらに、主に米国では、技術革新により複雑化する戦闘様相に対応するため、達成すべき任務をタスクに分解し具体的なシステムを検討するための手法であるミッション・エンジニアリングが注目されている。

我が国も、令和４年１２月に策定した国家防衛戦略や防衛力整備計画において、無人アセット防衛能力、指揮統制・情報関連機能、指揮官の意思決定を支援する技術の研究に関する文脈でＡＩの活用にそれぞれ言及している。

２．ＡＩの活用分野と方向性

ＡＩの機能と技術的限界を考慮すると、ＡＩの活用に適した業務は、

① 克服すべき課題を人間が特定できていること、

② 正解（と思われるもの）が存在すること、

③ ＡＩの機能（分類、異常検知、回帰、自然言語処理、行動の最適化）を用いることにより課題を解決できること、

④ 学習に必要なデータの質と量を確保できること、

といった要素を備えるものになると考えられる(10)。ＡＩの機能と限界から導かれるこのような要素と防衛省で既に進行しているＡＩを使った取組、他国でのＡＩ活用事例、国家防衛戦略や防衛力整備計画で示されている具体例を踏まえつつ、防衛省の所掌事務や自衛隊の任務に照らして活用分野を整理すると、以下の７つの分野に大別できる。そこで、防衛省としては、以下の７つの分野で重点的にＡＩの活用を図ることにより、意思決定の迅速化や情報収集・分析能力の優位性の確保に取り組むこととする。７つの分野の中には、勤続年数を重ねたベテラン隊員の知見・経験に裏打ちされた「匠の技」を要する業務もあるが、そのような業務にＡＩを導入することで、ＡＩが隊員の判断をサポートすることが可能となり、隊員の負担の軽減や省力化・省人化にも寄与すると期待される。

ただし、平成３１年３月に統合イノベーション戦略推進会議が策定した「人間

(9) ネットワークの末端側で中心的な情報処理を行うこと。

(10) ただし、ＡＩの学習方法として強化学習を採用する場合、学習データを確保することは必ずしも求められない。

中心のＡＩ社会原則」で示されているように、ＡＩは、「高度な道具として人間を補助する」ものであり、「ＡＩの利用にあたっては、人が自らどのように利用するのかの判断と決定を行うこと」が求められる。この点に関しては、後述の「ＡＩ事業者ガイドライン」においても、「ＡＩに単独で判断させるだけでなく人間の判断を介在させる利用を検討する」との考え方が示されているところである。ＡＩが行うのは人間の判断のサポートであって、その活用に当たっては、人間による関与を確保する必要があることに留意すべきである。

なお、今後のＡＩ活用分野を以下の７つに限定する趣旨ではなく、課題を克服するためにＡＩを活用できるものがあれば、以下の分野にとらわれることなくまずは試行してみることも重要である。

①目標の探知・識別

レーダー航跡、衛星画像、航空画像などの多岐にわたるセンシング情報の増加や高性能化に伴う目標情報の幾何級数的な増大に対応するため、人力で実施していた目標の探知・識別作業に、ＡＩやＡＩを搭載したエッジコンピューティング技術等を活用し、探知・識別能力の向上及び迅速化を図る。

②情報の収集・分析

各種情報の自動収集や分析・評価にＡＩを活用し、インターネットやＳＮＳ上の膨大な情報、センサーなどの多種多様な電波情報や画像情報の収集・分析に対応する。

③指揮統制

複雑かつ高速に推移する戦闘様相に対応するため、警戒監視・情報収集により得られた情報の分析・見積・評価を踏まえた行動方針の導出にＡＩを活用し、ターゲティングの高度化や、指揮官に行動方針案を適時適切に提示することによる迅速な意思決定を支援する。

④後方支援業務

装備品の可働率向上や効率的な装備品の維持管理に対応するため、補給データや故障品データを基にした需要予測や整備予測、輸送計画の策定にＡＩを活用し、整備・補給等の後方支援業務の効率化を図る。

⑤無人アセット

無人アセットの機体制御や行動判断にＡＩを適用し、無人アセットの自律運用能力の向上や、有人装備と無人アセットの連携を図る。

⑥サイバーセキュリティ

ＡＩを活用した振る舞い解析の導入などによるサイバーセキュリティ能力の向上や、ＡＩのモデル・データセットを標的としたＡＩそのものに対するサイバー攻撃への対処能力の向上を図る。

⑦事務処理業務の効率化

行政組織としての防衛省の中で行われている様々な事務処理業務にＡＩを導入し効率化を図ることにより、例えば、新たなものを創造する業務、人間の気持ちを汲み取ることが強く求められる業務といったＡＩが不得手とされる業務や、人間が重要な役割を果たす、高度な論理展開と判断を要する業務に、人的リソースを割くことができると期待される。

３．ＡＩの利用に伴うリスクへの理解と対応

ＡＩについては、一定の誤りが含まれることによる信頼性の懸念のほか、学習データの偏りなどに起因するバイアスや、誤用・悪用などの課題やリスクが伴うと指摘されている。そこで、その活用に当たっては、リスクを正しく認識し、必要となる対策を講じることが重要となる。このような背景の中、令和６年４月、総務省と経済産業省は、「様々な事業活動においてＡＩを活用する全ての者（政府・自治体等の公的機関を含む)」を対象とする「ＡＩ事業者ガイドライン」を策定した。同ガイドラインは、「ＡＩ開発・提供・利用にあたって必要な取組についての基本的な考え方を示すもの」であり、「実際のＡＩ開発・提供・利用において、本ガイドラインを参考の一つとしながら、ＡＩ活用に取り組む全ての事業者が自主的に具体的な取組を推進することが重要」とされている。同ガイドラインは拘束力を有するものではなく、「関係事業者による自主的な取組を促し、非拘束的なソフトローによって目的達成に導くゴールベースの考え方」で作成されたものである。同ガイドラインは、国際場裡における議論との整合性も意識したものとなっており、２０２３年５月のＧ７広島サミットの結果を受けて生成ＡＩに関する国際的なルールの検討を行うために立ち上げた「広島ＡＩプロセス」への貢献を意図するとともに、「同プロセスを含む国際的な議論を踏まえながら検討されたもの」とされる。

ＡＩ事業者ガイドラインは、民間事業者を含め、様々な事業活動においてＡＩを活用する全ての者を対象としているため、必ずしも防衛分野の動向に即したものではなく、記載内容の全てを防衛省・自衛隊に当てはめることは妥当ではないが(11)、同ガイドラインが示す以下のような考え方は、防衛省・自衛隊がＡＩの活用を進める上でも重要と考えられる。そこで、防衛省・自衛隊としては、同ガイドラインを参考の一つとしつつ、ＡＩをめぐる国際社会や他国の防衛当局等との議論にも注意を払い、ＡＩの活用推進とＡＩがもたらすリスクの低減に取り組むこととする。さらに、防衛省・自衛隊が進める取組から得られた知見を共有するなどして、国際的な議論やルール作りにも積極的かつ建設的に参加して

(11) ＡＩ事業者ガイドラインは、「ＡＩ提供者やＡＩ利用者が政府・自治体等、公的機関になる場合は、民間事業者の場合とは別の考えが必要になる可能性がある」と記述。

いく。

【ＡＩ事業者ガイドラインが示す考え方】

（注：以下の記述は、防衛省・自衛隊がＡＩの活用を進める上で重要と考えられるＡＩ事業者ガイドラインの記述を引用・編集したもの）

（１）関連する用語

- ＡＩシステム
  活用の過程を通じて様々なレベルの自律性をもって動作し学習する機能を有するソフトウェアを要素として含むシステムとする（機械、ロボット、クラウドシステム等）。
- ＡＩモデル（ＭＬモデル）
  ＡＩシステムに含まれ、学習データを用いた機械学習によって得られるモデルで、入力データに応じた予測結果を生成する。
- ＡＩサービス
  「ＡＩシステム」を用いた役務を指す。
- ＡＩガバナンス
  ＡＩの利活用によって生じるリスクをステークホルダーにとって受容可能な水準で管理しつつ、そこからもたらされる正のインパクト（便益）を最大化することを目的とする、ステークホルダーによる技術的、組織的、及び社会的システムの設計及び運用。

（２）原則

各主体は、基本理念（注：①人間の尊厳が尊重される社会、②多様な背景を持つ人々が多様な幸せを追求できる社会、③持続可能な社会）により導き出される人間中心の考え方を基に、ＡＩシステム・サービスの開発・提供・利用を促進し、人間の尊厳を守りながら、事業における価値の創出、社会課題の解決等、ＡＩの目的を実現していくことが重要である。このため、各主体は、ＡＩ活用に伴う社会的リスクの低減を図るべく、安全性・公平性といった価値を確保することが重要である。また、個人情報の不適正な利用等の防止を始めとするプライバシー保護並びにＡＩシステムの脆弱性等による可用性の低下や外部からの攻撃等のリスクに対応するセキュリティ確保を行うことが重要である。上記を実現するために、各主体は、システムの検証可能性を確保しながらステークホルダーに対する適切な情報を提供することにより、透明性を向上させ、アカウンタビリティを果たすことが重要となる。

（注：下線部はＡＩ事業者ガイドライン本文のまま）

（３）共通の指針（注：各主体が取り組むべきことを整理したもの）

取組に当たり、各主体は、以下に述べる「人間中心」に照らし、法の支配、人権、民主主義、多様性及び公平公正な社会を尊重するようＡＩシステム・サービスを開発・提供・利用すべきである。また、憲法、知的財産関連法令及び個人情報保護法をはじめとする関連法令、ＡＩに係る個別分野の既存法令等を遵守すべきであり、国際的な指針等の検討状況についても留意することが重要である。

なお、これらの取組は、各主体が開発・提供・利用するＡＩシステム・サービスの特性、用途、目的及び社会的文脈を踏まえ、各主体の資源制約を考慮しながら自主的に進めることが重要である。

①　人間中心

■　ＡＩシステム・サービスの開発・利用・提供において、自動化バイアス(12)等のＡＩに過度に依存するリスクに対して、必要な対策を講じる

■　フィルターバブル(13)に代表されるような情報や価値観の傾斜を助長し、ＡＩ利用者を含む人間が本来得られるべき選択肢が不本意に制限されるようなＡＩの活用にも注意を払う

■　ＡＩが生成した偽情報・誤情報・偏向情報が社会を不安定化・混乱させるリスクが高まっていることを認識した上で、必要な対策を講じる

■　合理的な範囲で、ＡＩシステム・サービスの機能及びその周辺技術に関する情報を提供する

②　安全性

■　ＡＩシステム・サービスの出力の正確性を含め、要求に対して十分に動作している（信頼性）

■　様々な状況下でパフォーマンスレベルを維持し、無関係な事象に対して著しく誤った判断を発生させないようにする（堅牢性（robustness））

■　ＡＩの性質・用途等に照らし、必要に応じて客観的なモニタリングや対処も含めて人間がコントロールできる制御可能性を確保する

■　ＡＩシステム・サービスの安全性を損なう事態が生じた場合の対処方法を検討し、当該事態が生じた場合に速やかに対処できるよう整える

■　主体のコントロールが及ぶ範囲で本来の目的を逸脱した提供・利用により

---

(12) 自動化バイアスについて、ＡＩ事業者ガイドラインは、「人間の判断や意思決定において、自動化されたシステムや技術への過度の信頼や依存が生じる現象」としている。

(13) フィルターバブルについて、ＡＩ事業者ガイドラインは、「アルゴリズムがネット利用者個人の検索履歴やクリック履歴を分析し学習することで、個々にとって望むと望まざるとにかかわらず見たい情報が優先的に表示され、利用者の観点に合わない情報からは隔離され、自身の考え方や価値観のバブル（泡）の中に孤立するという情報環境」としている。

危害が発生することを避けるべく、ＡＩシステム・サービスの開発・提供・利用を行う

■　ＡＩシステム・サービスの特性や用途を踏まえ、学習等に用いるデータの正確性・必要な場合には最新性（データが適切であること）等を確保する

③　公平性

■　不適切なバイアスを生み出す要因は多岐に渡るため、各技術要素（学習データ、モデルの学習過程、ＡＩ利用者が入力するプロンプト、ＡＩモデルの推論時に参照する情報や連携する外部サービス等）及びＡＩ利用者の振る舞いを含めて、公平性の問題となり得るバイアスの要因となるポイントを特定する

■　ＡＩの出力結果が公平性を欠くことのないよう、ＡＩに単独で判断させるだけでなく、適切なタイミングで人間の判断を介在させる利用を検討する

④　プライバシー保護

■　プライバシーが尊重され、保護されるよう、その重要性に応じた対応を取る

⑤　セキュリティ確保

■　ＡＩシステム・サービスの機密性・完全性・可用性を維持し、常時、ＡＩの安全な活用を確保するため、その時点での技術水準に照らして合理的な対策を講じる

■　ＡＩシステム・サービスに対する外部からの攻撃は日々新たな手法が生まれており、これらのリスクに対応するための留意事項を確認する

⑥　透明性[14]

■　ＡＩの判断にかかわる検証可能性を確保するため、データ量やデータ内容に照らし合理的な範囲で、ＡＩシステム・サービスの開発過程及び利用時の入出力等、ＡＩの学習プロセス、推論過程、判断根拠等のログを記録・保存する

■　ログの記録・保存に当たっては、利用する技術の特性や用途に照らして、その記録方法、頻度、保存期間等について検討する

(14) 透明性については諸外国でも様々な定義があるが、ＡＩ事業者ガイドラインでは、情報開示に関する事項を広く「透明性」としている。

⑦　アカウンタビリティ[15]

■　データの出所、ＡＩシステム・サービスの開発・提供・利用中に行われた意思決定等について、技術的に可能かつ合理的な範囲で追跡・遡及が可能な状態を確保する

⑧　教育・リテラシー

■　ＡＩに関わる者が、その関わりにおいて十分なレベルのＡＩリテラシーを確保するために必要な措置を講じる

■　生成ＡＩの活用によって、ＡＩと人間の作業の棲み分けが変わっていくと想定されるため、新たな働き方ができるよう教育・リスキリング等を検討する

⑨　イノベーション

■　国際化・多様化、産学官連携及びオープンイノベーションを推進する

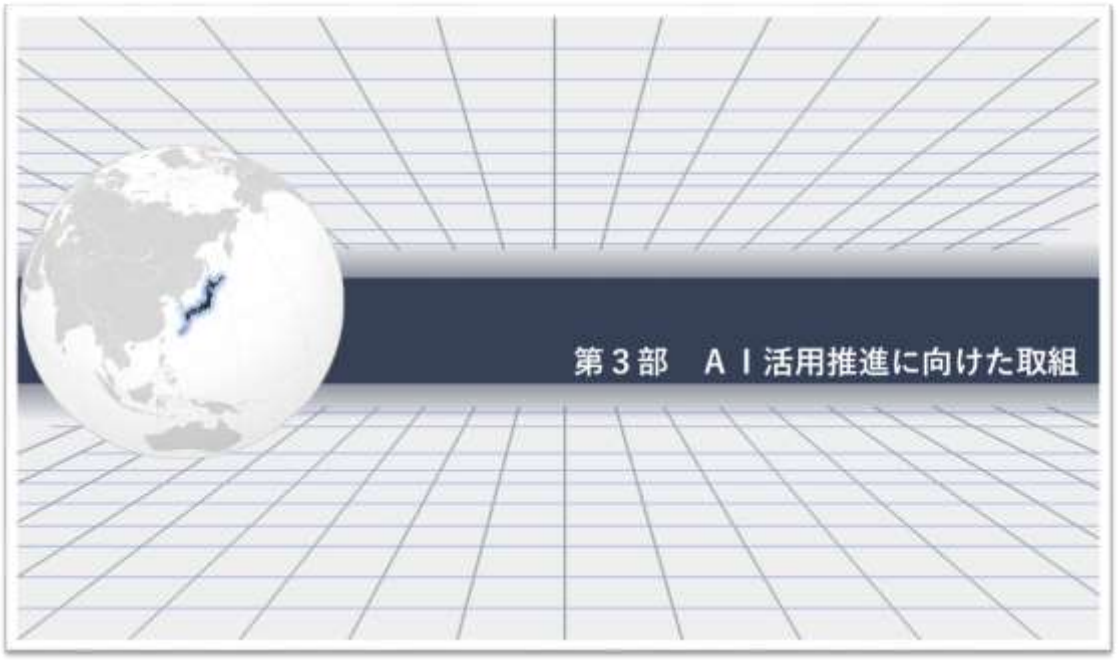
■　自らのＡＩシステム・サービスと他のＡＩシステム・サービスとの相互接続性と相互運用性を確保する

（４）ＡＩガバナンスの構築

各主体間で連携しバリューチェーン全体で「共通の指針」を実践しＡＩを安全安心に活用していくためには、ＡＩに関するリスクをステークホルダーにとって受容可能な水準で管理しつつ、そこからもたらされる便益を最大化するための、ＡＩガバナンスの構築が重要となる。…（中略）…事前にルールや手続が固定されたＡＩガバナンスではなく、企業・法規制・インフラ・市場・社会規範といった様々なガバナンスシステムにおいて、「環境・リスク分析」「ゴール設定」「システムデザイン」「運用」「評価」といったサイクルを、マルチステークホルダーで継続的かつ高速に回転させていく、「アジャイル・ガバナンス」の実践が重要となる。

なお、具体的な検討にあたっては開発・提供・利用予定のＡＩのもたらすリスクの程度及び蓋然性や、各主体の資源制約に配慮することが重要である。

(15) アカウンタビリティを説明可能性と定義することもあるが、ＡＩ事業者ガイドラインでは情報開示は透明性で対応することとしており、アカウンタビリティとはＡＩに関する事実上・法律上の責任を負うこと及びその責任を負うための前提条件の整備に関する概念としている。


第３部　ＡＩ活用推進に向けた取組

第３部　ＡＩ活用推進に向けた取組

１．防衛力の抜本的強化に向けたＡＩの活用

ＡＩの活用に当たっては、その活用自体を目的化するのではなく、まずは人間が具体的な課題を特定し、その課題克服のためにＡＩを役立てることができるか検討するというプロセスで進めることが重要である。国家防衛戦略で示されている領域横断作戦能力を例に、ＡＩを大きな文脈の中でどのように活用できるか提示すると、以下のようなものとなろう。

宇宙・サイバー・電磁波の領域と陸・海・空の領域の能力を有機的に融合し、相乗効果によって全体の能力を増幅させる領域横断作戦では、宇宙空間を含む広大な戦域に点在する陸・海・空自衛隊の様々な装備品を情報通信ネットワークで連接し、部隊や個々の装備品が、同ネットワークを介して、探知・識別等で得られた情報をデジタル化されたデータの形で処理し、統合された指揮統制の下で行動することが考えられる。そのような一連のプロセスにおいて、例えば探知・識別の精度を上げたいという課題があるのであれば、画像や音声の処理と分類を機能とするＡＩを活用することが考えられる。また、領域横断作戦の指揮官の意思決定を支援すべく、行動方針案を提示するツールとしてＡＩを活用することも考えられよう。

領域横断作戦能力を始めとして、国家防衛戦略は、我が国の防衛上必要な７つの機能・能力(16)を示している。第２部で示した７つの分野は国家防衛戦略が示す７つの機能・能力の全てに関連しており(17)、ＡＩは、これら７つの機能・能力のいずれの文脈においても、人間が特定した具体的な課題の解決やそれぞれの機能・能力の強化に貢献できると考えられる。

こうした防衛力の抜本的強化に向けてＡＩを活用するにあたっては、ＡＩ活用推進検討委員会のような組織横断的な枠組みを活用し、各機関等がそれぞれ進めている事業から得られた好事例や教訓を共有した上で今後のそれぞれの取組にフィードバックするという一連のプロセスを確立させることとする。

なお、ＡＩの活用を含む新しい戦い方への対応については、次世代情報通信技術導入推進委員会において検討が進んでいる。ＡＩ活用推進委員会としても、同委員会での検討に沿う形で関連の取組を推進することとする。

---

(16) ①スタンド・オフ防衛能力、②統合防空ミサイル防衛能力、③無人アセット防衛能力、④領域横断作戦能力、⑤指揮統制・情報関連機能、⑥機動展開能力・国民保護、⑦持続性・強靭性の７つ。

(17) 例えば、後方支援業務が機動展開能力や持続性・強靭性に関連すると考えられるように、第２部で示した７つの分野と国家防衛戦略の７つの機能・能力は、必ずしも一対一の対応関係にあるわけではない。

２．防衛省におけるデータ・情報基盤の構築

領域横断作戦の実効性を上げるためには、ＡＩの活用のほかにも、陸・海・空自衛隊の組織の壁や個々の情報システムの仕様を越えて、必要な者が必要なデータにアクセスできる状態を実現することが期待される。そのためには、組織横断的なデータフォーマットの整備などの新たな取組が必要となる。

ＡＩは意思決定や情報収集・分析能力の優位性確保に寄与するツールの一つであるが、その精度を維持・向上させるためには、質の高いデータを学習させることが欠かせない。その意味において、データは単なるＩＴ資産ではなく、任務遂行に不可欠な戦略アセットとなっている。意思決定者、政策立案者、指揮官、幕僚、現場の隊員が、必要な時に必要なデータを利用可能な状況を実現するためには、データの組織的・集合的な管理が必要となる。そうでなければ、データに基づく意思決定や、迅速かつ適切な任務の遂行は困難となろう。このような状況の下、データの設計・作成から運用、利用に至るまでの連続的な管理を行うデータマネジメントの重要性が増している。データが利活用しやすい形で蓄積されるよう、業務の見直しやシステムの構築を行うことで、ＡＩの活用を推進する。防衛省・自衛隊では、ＡＩの学習に必要となるデータ基盤の構築に取り組み始めたところであるが、今後、以下の考え方に基づきデータマネジメントを進めることとする。

（１）「データは任務遂行に不可欠な戦略アセット」という意識の涵養

令和３年６月にデジタル庁が策定した「包括的データ戦略」には、「日本社会全体でのデータに係るリテラシーの低さ、プライバシーに関する強い懸念等から、データの整備、データの利活用環境の整備、実際のデータの利活用は十分に進んでこなかった」、「今般のコロナ禍においては、…（中略）…我が国のデジタル化への対応の遅れが露呈した」、「今の政府においては、そもそも行政を行うにあたって、『データを重視する姿勢・文化』が十分でなく、『データを活用する環境』も整備されておらず、その結果、諸外国との比較において『実際の利活用』も進んでいない」などの厳しい表現が並んでいる。この点は防衛省も例外ではなく、「データを活用する環境」の整備として、令和５年度からＡＩの学習に必要となるデータ基盤の構築に取り組み始めたところであり、これまでデータの活用に必要な態勢を十分に組めていたわけではない。防衛省がまず取り組むべきは、全ての隊員に、「データが任務遂行に不可欠な戦略アセットである」との意識を涵養することである。そのような意識に基づく具体的な行動として、これまで紙で行われていた業務を、データを使って行うよう見直すことも必要になろう。

（２）防衛省におけるメタデータの把握とデータフォーマットの整備

必要な時に必要なデータを利用できる状況をつくるためには、データの棚卸をして、どこにどのようなデータが存在するのか整理し、メタデータ(18)の一覧を作成することが必要となる。メタデータ把握のためには、データ作成時にタグ付けを行い、カタログ化することが有効である。

また、防衛省は、陸・海・空自衛隊や防衛装備庁など多くの機関から成る巨大な組織であり、それぞれの機関が独自の情報システムを構築している。今後、統合運用や領域横断作戦の深化を図る上で、データを組織横断的に共有することがますます重要となるところ、共有することが必要なデータを特定した上で、それを可能とするデータフォーマットの整備も必要である。

さらに、学習データの質と量の向上の観点から、他の政府機関等とのデータの共有が有効である場合、必要に応じ、個別の事例に即した取組を検討する。

（３）クラウドを活用したデータの収集・蓄積・管理

防衛省・自衛隊では、統合幕僚監部と陸・海・空自衛隊がこれまでそれぞれ整備してきた任務遂行の基盤となる情報システムを、クラウドに統合することとしている。実際の統合は、個々の情報システムの換装のタイミングで順次行われる予定であるが、各機関の個々の情報システムのクラウドへの統合は、データの収集・蓄積・管理を進める上で良い機会となる。この機会を捉え、標準化されたデータの蓄積・管理とメタデータの把握を軌道にのせることを目指す。同時に、情報の保全区分も考慮しつつ、誰がどのデータにアクセスできるのかというデータアクセスに関するルールを明確化することも必要である。さらに、データが外部等から不正にアクセスされ、改ざんされることがないよう、セキュリティを確保する必要がある。

また、ＡＩのためのデータの蓄積・管理という点では、取得したデータを蓄積するデータレイク(19)、ＡＩが学習しているデータの分析やＡＩの学習に適した形にデータを加工・保存するためのデータウェアハウス(20)、ＡＩの学習を行うためのサーバ及び操作用端末などから構成されるＡＩの性能の維持管理のための環境を整備することが重要である。そこで、防衛省では、ＡＩ運用環境での新しいデータの蓄積、維持管理環境でのデータ分析、ＡＩの再学習、ＡＩ運用環境への学習済モデルの配布といった一連のサイクルを実現できる態勢を構築することとしている。

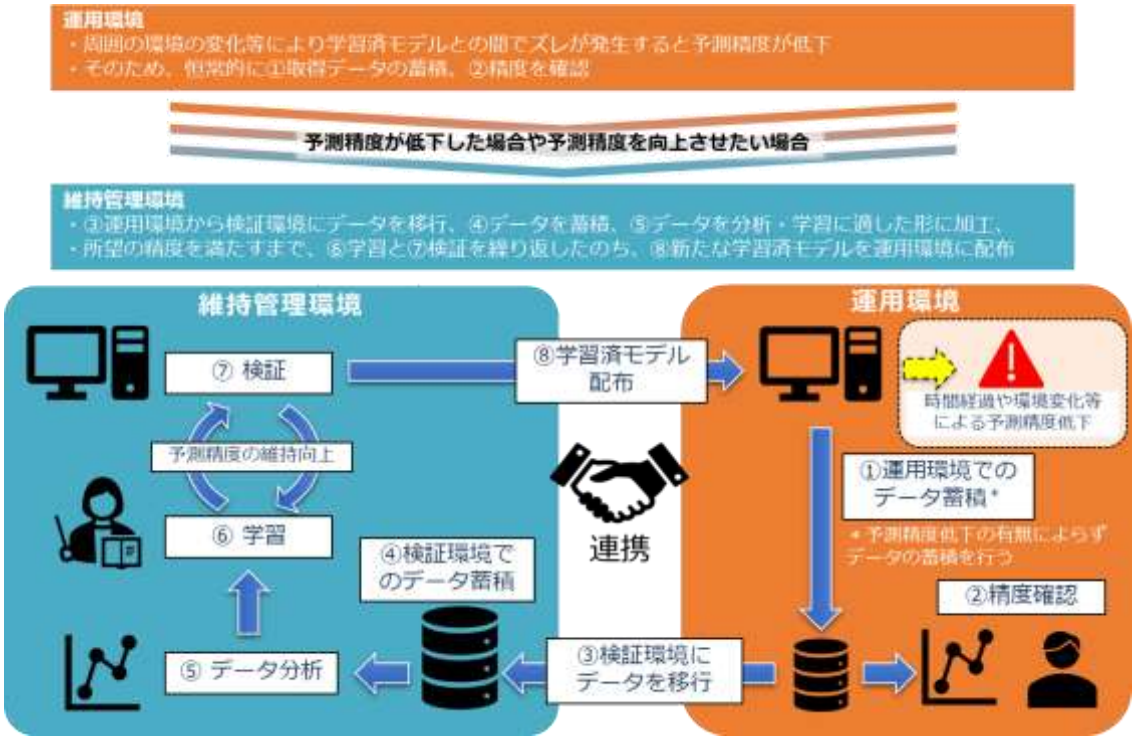
その上で、収集したデータの信頼性を確保し、その品質を維持するとともに、

---

(18) データを説明するための情報から構成されるデータ。
(19) データをそのまま貯めておく場所。
(20) データを使いやすく加工、整理した上で貯めておく場所。

収集したデータを基にした学習用データの作成（タグ付け）等のために継続的な取組が必要である。この際、ＡＩに学習させるデータが偏りを持たないように着意することが重要である。また、学習用データや学習後のデータに対する攻撃等への対処についても検討する必要がある。

【ＡＩの精度の維持・向上とデータ蓄積】



（４）防衛省のデータマネジメント推進体制

「データは任務遂行に不可欠な戦略アセット」という意識の涵養に始まり、メタデータの把握やデータフォーマットの整備に至るまで、本方針に記載すれば個々の隊員の自発的な努力のみで実現できるというわけではなく、防衛省内でこれを組織横断的に推し進めるエンジンが必要となる。この点、防衛省には、「防衛省行政情報化推進体制整備要綱について（通達）」（防運情第８１８５号。２３．７．１）に基づき、デジタル統括責任者（整備計画局長）の統括の下、行政情報化を推進する体制が整備されている。データマネジメントは行政情報化推進の取組の一つであることから、この体制の下、上述の施策を進めることとする。これにより、デジタル統括責任者（整備計画局長）は、防衛省におけるデータマネジメント責任者（ＣＤＯ：Chief Data Officer）に当たる役割を事実上務めることとなる。省内の組織横断的なデータマネジメント施策の企画立案はデータガバナンスを行う防衛省全体管理組織（ＰＭＯ：Portfolio Management Office）

[21]が担い、個々の情報システムごとに必要なデータ関連の措置やデータマネジメントはＰＪＭＯ（Project Management Office）が講ずることとする。

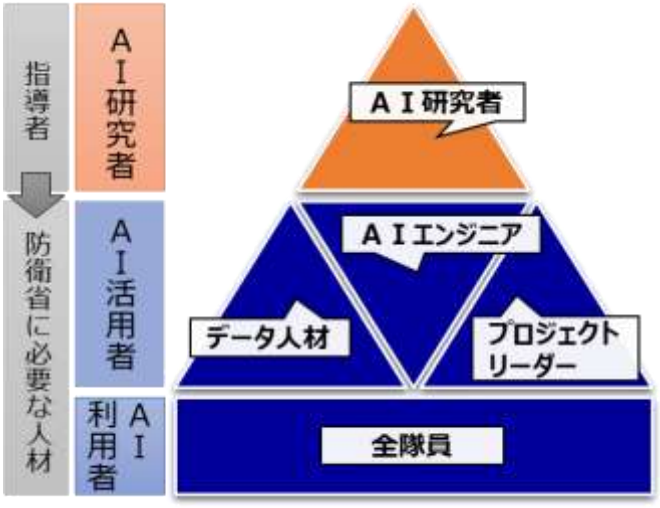
３．ＡＩやデータに関する知見を有する人材とその確保・育成

（１）防衛省に求められるＡＩ・データ人材

データを用いた学習を繰り返すことによりＡＩの性能を維持・向上させるためには、ＡＩやデータに関する知見を有する人材が欠かせない。

ＡＩ人材は、研究者と、個別の業務目的に応じてＡＩモデルの組込み、アルゴリズムの適用、これらの維持管理を担う活用者に大別することができる。防衛省では、個々の業務にＡＩを活用するために必要なデータの準備を行うデータ人材、用途に応じてＡＩモデルを評価し、学習やパラメータの最適化等を通じてカスタマイズするＡＩエンジニア、ＡＩを活用するプロジェクトの企画から評価までを総括するプロジェクトリーダーが必要となることから、これまで隊員を対象とするＡＩ講座等を開講し、必要な知識の取得を促してきた。同時に、民間の研究者を「ＡＩ・データ分析官」として採用し、高度な専門性に裏付けられた助言や隊員への教育の機会を得てきたところである。

また、ＡＩに関する研究開発や維持管理に携わらない、ＡＩを利用するだけの隊員についても、ＡＩを利用するに当たって最低限知っておくべき知識[22]を有していることが求められる。



(21) ＰMOは、各府省のＩＴガバナンスの機能強化を目的に、デジタル庁が定める「デジタル・ガバメント推進標準ガイドライン」により設置することとされている組織。防衛省では、整備計画局サイバー整備課に置かれている。
(22) 例えば、「ＡＩは事実に基づかない情報を出力する（いわゆるハルシネーション）ことがあり、最終的な判断は人が行う必要がある」ということ。

（２）ＡＩ・データ人材の育成

ＡＩ・データ人材にはその業務目的に応じた能力が求められる。各機関は、具体的なニーズに適した講座を見極めて取り入れることが重要である。整備計画局サイバー整備課は、これまで隊員を対象とする初級・中級のＡＩ講座を開講し受講者を募集してきたが、他の政府機関もＡＩに関連する講座を提供している。以下では、上述の考え方に倣いＡＩへの業務上の関わり方の観点から人材像を類型化するとともに、それぞれの類型ごとに受講することが効果的と考えられる講座の例を示すこととする。

①ＡＩを利用する者

今後、ＡＩの普及が更に進み日常生活で広く使われるようになると、翻訳作業のような一般的な行政事務の遂行に当たってもＡＩを活用する場面が増えると想定される。そこで、例えば隊員が日常的に使用する業務処理システムにＡＩを活用したソフトウェアを導入するなどして、隊員が業務の遂行を通じて恒常的にＡＩの利活用に関する知識とスキルを習得することを促進する。

実際の業務を通じた知識とスキルの習得に加え、ＡＩ講座の受講も有効な手段である。ＡＩは、一般的な行政事務のほか、指揮統制における意思決定支援から整備・補給における補用品取得の最適化に至るまで、多くの場面で活用が進むと考えられる。そのため、作戦の立案者・意思決定者から整備・補給要員に至るまで、実際にＡＩを利用し得る隊員が、ＡＩ、数理、データサイエンスに関する基礎的な素養を身に付けることは重要である。

政府全体でＡＩの利用が進む中、隊員のＡＩリテラシーの向上は、防衛省・自衛隊のみならず他の政府機関等においても重要な課題となっている。ＡＩ事業者ガイドラインにおいても、「各主体内のＡＩに関わる者が、その関わりにおいて十分なレベルのＡＩリテラシーを確保するために必要な措置を講じる」ことが記述されているところ、政府全体の取組も活用しつつ、隊員のＡＩリテラシー向上に取り組む。

講座の例：

整備計画局サイバー整備課「ＡＩ基礎講習」

総務省統計局「社会人のためのデータサイエンス入門」「社会人のためのデータサイエンス演習」

②ＡＩの研究開発や維持管理に携わる者（データ人材、ＡＩエンジニア）

さらに、ＡＩの研究・開発や維持管理に携わる隊員は、ＡＩ・データを専門にする企業や研究機関の関係者と専門知識を交えてやり取りすることが期待される。その際、例えばPython(23)のようなＡＩ開発及び活用との親和性の高いプロ

(23) 人工知能や機械学習などＡＩ分野で利用されている汎用的なプログラミング言語。

グラミング言語に触れた経験を有することが専門的なやり取りを行う上での資となることから、Python 等を用いたプログラミングなどの講習の受講と能力の取得を推進する。その上で、各々の職務に応じて、ＡＩエンジニアリング、データサイエンス、ＡＩプロジェクトマネジメントのうち必要となる能力を伸ばすことが重要である。

講座の例：

整備計画局サイバー整備課「ＡＩ中級講座」「ＡＩ実践講座」

③ＡＩの活用をリードする者（プロジェクトリーダー）

中級のＡＩ講座を履修し、プログラミングやデータサイエンスの素養を身に付けた隊員は、自身の部隊等のＡＩ適用システムについて理解を深めることで、所属部隊でＡＩの活用をリードし、後進の育成に携わる人材を目指すべきである。その際、部隊等の現場で利用されているＡＩはシステムにより様々であることから、実務を通じてスキルを引き継ぐことが重要である。

このような人材が新たな部隊に赴任した際は、着任先の部隊等で使用されているＡＩ適用システムについて理解を深めるとともに、前職の経験に基づくベストプラクティスの共有を行うことで、防衛省全体のＡＩ・データ人材の成熟度が増し、ＡＩの活用がより一層推進される好循環が生まれることとなる。このような人材育成のエコサイクルを確立することが重要となる。

講座の例：

整備計画局サイバー整備課「ＡＩ実践講座」

ＡＩ適用システムの維持管理によるＯＪＴ

（３）民間のＡＩ・データ人材の活用

ＡＩの技術革新は民間を中心に進んでいるところ、民間知見を取り込むことは非常に重要である。加えて、国家防衛戦略や防衛力整備計画がＡＩの活用に言及し、実際に防衛省においてＡＩを使った取組が進む中、ＡＩに関連する全ての業務を隊員だけで処理するのは現実的ではない。そこで、この分野に知見やノウハウを有する民間の企業や研究機関の活用を通じ、そこで働くＡＩ・データ人材の方々と協力することが重要となる。この点、整備計画局サイバー整備課では、令和２年度から、ＡＩ導入推進アドバイザー役務を調達しており、安全保障分野における諸外国のＡＩ導入に関する調査、防衛省・自衛隊へのＡＩ導入に関する政策の企画立案の支援、ＡＩを活用する事業への助言など、幅広い支援を得ている。ＡＩを活用する事業の担当者など、業務上ＡＩと深く関わる隊員は、このような民間の専門的知見を得ることが業務を遂行する上での助力となろう。

このほか、ＡＩやデータに関する専門的な知見・経験を有する民間の人材を個別に採用することも重要である。防衛省では、令和３年度から、ＡＩやデータ分

析に関する高度な知識と豊富な経験を有する民間の人材を「ＡＩ・データ分析官」として採用する取組を行ってきた。今後もこのような取組を継続・拡充し、民間人材への積極的なアプローチを進める。

４．ＡＩを使った装備品の研究開発

ＡＩシステムの開発は単純に言えばソフトウェア開発の一種ではあるが、従来のソフトウェア開発の考え方をそのまま適用するには技術的に不足する点がある。そのため民生分野においてＡＩシステム開発のための様々な方法論が用いられている。例えば、Proof of Concept（PoC）と呼ばれる予備的実験段階の導入や同段階における運用者の参画、アジャイル開発など、いわゆる従来のウォーターフォール型の開発のみではない、より柔軟で効率的な開発プロセスの適用が広く行われている。また、運用段階で得られる実際のデータをもとにして、より高い精度の実現や環境変化への適応を運用中に行うための継続的な評価・改善も必要となる。ＡＩを使った装備品の研究開発においてもこのような民生の知見を必要に応じて適切に取り込み、効率的な事業実施に努める必要がある。

さらに、ＡＩの学習に必要となる防衛省・自衛隊特有のデータは、一般社会におけるデータ量と比較すると圧倒的に不足する面があるため、少ないデータ量でも学習が可能、または与えられたルール下でＡＩ自身が学習データの生成が可能となる技術の基礎研究に投資するとともに、研究開発段階から組織横断的にデータや研究開発案件を共有することも重要である。この点について、防衛省・自衛隊特有のデータを収集する方法として、データの収集を目的とした演習等を行うことも考えられる。

リスクへの理解と対応の観点からは、ＡＩを使った装備品の研究開発段階で、ＡＩのリスクを正しく認識し、必要となる対策を講じることが重要である。この点について、前述のＡＩ事業者ガイドラインは、第２部に記したＡＩ開発・提供・利用の全ての段階に共通する基本的な考え方に加え、特にＡＩ開発者にとって重要な事項として、例えば以下のような点を指摘している。ＡＩの開発者は、「ＡＩモデルを直接的に設計し変更を加えることができるため、ＡＩシステム・サービス全体においてもＡＩの出力に与える影響が高い」（ＡＩ事業者ガイドライン）とされるところ、以下の事項は防衛省・自衛隊がＡＩを使った装備品の研究開発を進める上でも重要な観点であると考えられる。

【ＡＩ事業者ガイドラインがＡＩ開発者にとって重要として示す事項】

（注：以下の記述は、ＡＩ事業者ガイドラインの記述を引用・編集したもの）

■　学習データ、モデルの学習過程によってバイアス（学習データには現れない

潜在的なバイアスを含む）が含まれうることに留意し、データの質を管理するための相当の措置を講じる

■　学習データ、モデルの学習過程からバイアスを完全に排除できないことを踏まえ、必要に応じて、単一手法ではなく多様な手法に基づく開発を並行して行う

■　予想される利用条件下でのパフォーマンスだけでなく、予期しない環境での利用にも耐えうる性能を検討する

■　リスク（連動するロボットの制御不能や不適切な出力等）を最小限に抑える方法（ガードレール技術等）を検討する

■　開発時に想定していないＡＩの提供・利用により危害が発生することを避けるため、安全に利用可能なＡＩの使い方について明確な方針・ガイダンスを設定する

■　ＡＩシステムの開発の過程を通じて、採用する技術の特定に照らし適切にセキュリティ対策を講ずる

■　ＡＩの予測性能や出力の品質が、活用開始後に大きく変動する可能性や想定する精度に達しないこともある特性を踏まえ、事後検証のための作業記録を保存しつつ、その品質の維持・向上を行う

■　トレーサビリティ及び透明性の向上のため、ＡＩシステムの開発過程、意思決定に影響を与えるデータ収集やラベリング、使用されたアルゴリズム等について、可能な限り第三者が検証できるような形で文書化する

また、令和６年２月、ＡＩの安全性に対する国際的な関心の高まりを踏まえ、ＡＩの安全性の評価手法の検討等を行う機関として、米国や英国と同様に、我が国においても、ＡＩセーフティ・インスティテュートが設立された。同機関は、今後ＡＩの安全性評価に関する基準や手法の検討などを進めることとしているところ、防衛省・自衛隊としても必要な協力を行い、必要に応じ自らが行う研究開発にも活かしていく。

ＡＩを使った装備品の研究開発は、ＡＩの軍事的な利用をめぐる国際場裡での議論とも関連している。我が国は、人間の関与が及ばない完全自律型の致死性兵器の開発を行う意図がない旨を表明しているほか、令和５年１１月には、米国主導でまとめられた「ＡＩと自律性の責任ある軍事利用に関する政治宣言」への支持と参加を表明した。同宣言は、モニタリング等のプロセスを通じて重要な安全機能が低下していないことを保証すること等、軍事分野でのＡＩの責任ある開発、配備及び使用を確保するという観点から各国が実施すべき措置のあり方を示すものとされている。今後、研究開発の文脈で、このような我が国の一連のコミットメントをどのように具体化するかについて、ＡＩ事業者ガイドライン

を参考の一つとしつつ、他国の政府機関等との議論を通じて検討を深め、防衛省・自衛隊のガイドラインを策定する。このような取組を通じ、信頼性や堅牢性を有するとともに、人間がコントロールできる制御可能性を備えたＡＩの研究開発を進めていく。

５．大学等の教育・研究機関との協力関係

ＡＩの研究開発や活用を進める上で、大学等の教育・研究機関との協力は重要である。大学等の教育・研究機関は、ＡＩ技術の研究開発、ＡＩの普及に必要な社会環境や条件の研究、ＡＩ倫理や規制の研究など様々な観点でＡＩにアプローチしている。ＡＩの学習に必要となるデータ基盤の構築を開始し、これからＡＩを本格的に活用する防衛省にとって、大学等の教育・研究機関は、研究開発の頼れるパートナー、ＡＩ人材育成に欠かせない教育プログラムのプロバイダー、活用推進に当たっての心強いアドバイザーとなる。このような観点から、引き続き大学等の教育・研究機関とのネットワークを広げ、協力関係を拡大・深化させる。

６．各国との協力・連携

ＡＩに係る技術革新が急速に進展する中、各国の防衛当局においてもそれぞれの軍事的必要性や能力に応じて、様々な軍事領域へのＡＩの導入を進めているところである。各国の動向に立ち遅れることなく我が国もＡＩの活用を推進するためには、我が国独自の努力のみならず、各国との連携を進めることが重要である。

そのため、まずは各国防衛当局との協議や会談等の機会を活用し、軍事分野へのＡＩの活用事例に関する情報交換を積極的に行っていく。同盟国・同志国を始めとする各国の防衛当局との間でＡＩの活用事例について知見の共有を行うことで、我が国のＡＩ活用に資する情報の獲得を目指す。それに加えて、我が国からの情報提供を通してＡＩ活用の透明性を高めることで、各国からの信頼の確保を図るとともに、我が国としてＡＩ活用において注力する分野を示し、双方のニーズを踏まえたより効果的な連携及び協力につなげる。

さらに、我が国のＡＩ活用と親和性のある取組を進めている同盟国・同志国との間では、互いの効果的なＡＩ活用を促進するため、ＡＩの活用や関連する研究開発における連携を進めることを目指す。

７．ＡＩ軍備管理・ＡＩ倫理をめぐる国際社会の動きと防衛省の対応

急速な技術の発展を背景に、近年、ＡＩの軍事的な利用に係る規範や、どのように責任のある形でＡＩの軍事利用を図るかにつき国際的な議論が活発化して

いる。自律型致死兵器システム（ＬＡＷＳ）については、２０１７年から特定通常兵器使用禁止制限条約の政府専門家会合において、その定義・特徴、国際人道法上の課題、規制の在り方等、国際的なルール作りの議論が継続しているところである。また、２０２３年２月にはオランダで「軍事領域における責任あるＡＩ利用（ＲＥＡＩＭ）サミット」が開催され、我が国を含む６０ヶ国以上の支持により採択された「ＲＥＡＩＭ」宣言において、軍事領域でのＡＩの導入に当たっては国際法を遵守する形で責任ある利用を行うことが重要であることが確認された。さらに、軍事分野でのＡＩの責任ある開発、配備及び使用を確保するという観点から、各国が実施すべき措置の在り方を示した「ＡＩと自律性の責任ある軍事利用に関する政治宣言」が米国主導でまとめられ、２０２３年１１月、我が国を含む４６の国の支持・参加が表明された。

このようにＡＩの軍事的な利用に関する国際的な議論が活発化し、各国が実施すべきとされる措置が具体化されつつある中、防衛省・自衛隊におけるＡＩの積極的な活用に際しては、そうした議論の内容に十分留意しつつ、進める必要がある。

まず、「ＲＥＡＩＭ」宣言や「ＡＩと自律性の責任ある軍事利用に関する政治宣言」を始めとするＡＩの軍事利用に関する議論においては、ＡＩの使用が国際法、とりわけ国際人道法上の国家の義務に合致した上で行われることを重視している。防衛省・自衛隊としては、国際人道法の原則は、新興技術を活用するものを含め、あらゆる兵器に適用されるという考えであり、当然のことながら国際法や国内法により使用が認められない装備品の研究開発及び導入を行うことはない。ＡＩ技術が急速に進展し、防衛装備品への活用が更に進むことが見込まれる中、ＡＩを活用する装備品の研究開発及び導入において、国際人道法を始めとして法的適合性をしっかりと確認した上でこれを進める必要がある。

また、国際的な議論でも指摘されているとおり、ＡＩの活用に当たっては、責任のある形でこれを進める必要がある。国際的な議論や技術開発の動向を踏まえつつ、ＡＩを活用する装備品の研究開発、導入及び運用といったライフサイクルを通じ、「責任のある利用」を確保するための施策について引き続き検討していく。

その上で、ＡＩの軍事利用に係る国際的なルール作りに関する議論については、人道上の視点と安全保障上の必要性を踏まえたバランスの取れた原則及び規範の策定を目指し、国際的な議論に積極的かつ建設的に貢献していく。

上記の国際人道法を始めとする法的適合性の確認や「責任のある利用」の確保については、「ＡＩと自律性の責任ある軍事利用に関する政治宣言」や米国防省が主導する防衛ＡＩパートナーシップの枠組みを含む各国との意見交換の機会を活用し、他国の効果的な取組事例についての情報収集も同時に進めていく。

８．他の先端技術の活用可能性と生成ＡＩの活用

（１）次世代情報通信技術や量子コンピューティング技術等の情報処理能力等の向上に資する技術の活用可能性

ＡＩの活用に当たっては、質・量ともに十分なデータを収集・蓄積し、そこへのアクセスを提供する超高速通信網が重要となる。防衛省がＡＩに学習させる必要があるデータの中には、例えば大規模な部隊の運用のように、現実世界でのデータ取得が困難なものがあると想定される。そのようなデータの生成・収集・蓄積のため、将来的には、現実空間とサイバー空間（仮想空間）を高度に融合させたシステム（デジタルツイン）をベースとするシミュレーションの活用が考えられる。この点、大容量・低遅延・低消費電力を特徴とし、デジタルツイン技術に強みを持つ次世代情報通信技術は、ＡＩを支えるインフラの一つとなる可能性がある。

また、ＡＩの発展と共に、大量のデータを効率的に学習することが求められることになる。その点、高速の情報処理を可能とする量子コンピューティング技術等の次世代コンピューティング技術は、ＡＩへの適用の可能性を秘めた重要な技術であると言える。既に、機械学習や深層学習を量子コンピュータで行うためのアルゴリズムの研究が世界中で開始されており、今後の発展が期待されるところである。これらの先端技術については、今後の発展・進化を踏まえつつ、必要に応じ導入を検討する。

（２）生成ＡＩの活用

生成ＡＩについては、様々な事務作業の効率化が期待される一方で、単語による検索のみでなく、多様な文章形式の質問や応答が行われる、入力したデータがＡＩの学習に使われるなどの特徴があり、従来の検索サービスと異なるリスクが存在すると想定されている。政府としても、「ChatGPT 等の生成ＡＩを巡る技術革新は、さまざまな利点をもたらす一方、プライバシーや著作権の侵害などの新たな課題が生じるとの見方もある。生成ＡＩを巡る様々な課題や規制の在り方に関しては、国際的にも議論が行われているところ、政府としては、そうした議論の動向を見極めつつ、関係省庁が連携して生成ＡＩに関する実態の把握に努め、適切な措置を講じていく必要がある」（デジタル社会推進会議幹事会申合せ。令和５年９月１５日）との考えの下、ＡＩ戦略会議などで議論が行われている。

防衛省においては、生成ＡＩ利用のメリットとリスクを勘案し、政府における検討状況を踏まえながら、できる限りリスクを低減することを重視しつつ、生成ＡＩの導入に取り組む。実際に生成ＡＩを使用することを通じて隊員のリテラ

シーの底上げを図るとともに、必要に応じ課題を抽出し、対策を講じることで、リスクを受容可能な水準で管理しつつ、便益を最大化することを追求する。

おわりに

１８世紀の水力や蒸気機関による工場の機械化による第１次産業革命、２０世紀初頭の分業に基づく電力を用いた大量生産による第２次産業革命、１９７０年代初頭の電子工学を用いたオートメーション化による第３次産業革命に続き、ＡＩは、ＩｏＴ・ビッグデータ・ロボットなどと並び第４次産業革命の一つの要素に挙げられるなど、社会と時代に大きな変革をもたらす技術とされる。

日本社会全体とともに自衛隊が人口減少に直面する中、ＡＩは課題解決の重要なツールであるとともに、これらの取組は将来的な組織の構成や文化の改革の基盤となるものである。国家安全保障戦略には、「我々は今、希望の世界か、困難と不信の世界のいずれかに進む分岐点にあり、そのどちらを選び取るかは、今後の我が国を含む国際社会の行動にかかっている」と記されている。その言葉を防衛省・自衛隊におけるＡＩの活用に当てはめれば、「我々は今、ＡＩの活用により効率的で将来を自ら創り出す組織となるか、後れをとって非効率で旧態依然の組織となるのかの分岐点にあり、そのどちらを選び取るかは、今後の我々の努力にかかっている」と言えるだろう。ただし、ＡＩの活用に当たっては、それに伴うリスクを正しく認識し、必要となる対策を講じることで、リスクを低減しつつ便益を最大化することが求められる。本指針を、今後の防衛省・自衛隊におけるＡＩ活用推進の羅針盤としたい。