# Defense AI Vision

変わる戦い、変わらぬ使命

令和８年１１月

防　　衛　　省

# 目次

はじめに····· 1

第 1 章　AI 時代に目指す防衛力を描く ·····2

第 2 章　AI 活用の基本原則を定める ····· 4

第 3 章　任務遂行・業務を変革する····· 5

第 4 章　データを戦略的資産として活用する····· 9

第 5 章　AI を使い続け、改善し続ける基盤を構築する ····· 11

第 6 章　人材と組織文化を変革する····· 13

第 7 章　国内基盤を強化し同盟国・同志国等と連携する····· 14

第 8 章　三つの転換を実行し、不断に改善する····· 15

# はじめに

本ビジョンの目的は、AI とデータの活用そのものではなく、AI とデータによって情報をより早く行動に変え、人の知性と部隊の行動を拡張することで、防衛力の発揮の仕方そのものを変えることである。人間が目的を定め、指揮し、責任を負うとともに、我が国が、必要な AI とデータを自ら選び、使い続ける能力を保持する。

令和 6 年 7 月に策定した「防衛省 AI 活用推進基本方針」は、AI の活用自体を目的化せず、人間が課題を特定し、その課題克服のために AI を活用する考え方を示した。本ビジョンは、この考え方、人間の関与、データ、人材、責任ある AI 活用等を発展的に継承しつつ、個別の AI 活用から、防衛力の発揮の仕方を変える段階へ取組を進めるものである。また、政府の人工知能基本計画及び AI に関する関係法令・指針等を踏まえ、防衛分野の特性に応じて取組を進める。

AI の活用は、情報の生成・統合・分析にとどまらず、連続した作業を行う AI エージェントや、情報空間と物理空間をつなぎ、実環境での認識・行動を支えるフィジカル AI へと広がっている。防衛省・自衛隊は、米軍等で転換が進められている Data-Centric Warfare を見据え、AI とデータによって情報を判断と行動につなげる能力を高める。そのため、AI に任せる範囲と人間の役割を見直し、継続的な利用・更新を支える能力を強化する。

また、人口減少・少子高齢化の中で防衛力を持続的に発揮するためには、限られた人員、時間及び予算を、より大きな任務効果に結び付けなければならない。防衛省・自衛隊は、AI とデータによって作戦・人・後方をつなぎ、人間が政策立案、判断、指揮、教育訓練、関係者との調整等、人間の判断力や創造性が求められる、より付加価値の高い仕事に一層集中できる組織への変革を進める。

本ビジョンは、「変わる戦い、変わらぬ使命」との認識に立ち、AI とデータを防衛力の強化に結び付けるための目指す姿、基本原則、重点的な取組及び実行の考え方を明らかにする。

長期に維持すべき目的と原則は本ビジョンに示し、第 8 章に示す統括体制の下で、本ビジョンに基づく実行計画を定める。実行計画には、重点プロジェクトを位置付け、具体的な事業、工程、責任及び資源配分等を明らかにする。本ビジョンの本文の見直しは、第 8 章に示す考え方に基づいて行う。

# 第１章　AI 時代に目指す防衛力を描く

## 1　AI の進展と安全保障環境の変化

AI は、データから特徴や関係を見いだし、分類、異常検知、予測、自然言語処理、行動の最適化等を行うことによって、人間の情報処理と判断を支援する。従来の AI 活用では、特定の課題に対して一定の出力を得る使い方が中心であったが、近年は、複数の情報源や業務システムと接続し、一定の権限の下で連続した作業を行う利用が現実のものとなりつつある。このため、AI を単体のモデルとして捉えるだけではなく、データ、ツール、権限、通信、計算資源及び人間の監督を含むシステムとして捉える必要がある。

また、フィジカル AI の進展により、AI は物理空間における認識、判断支援及び行動へと活用範囲を拡大している。無人アセットやロボティクスとの連携は、人が危険な環境に立ち入る機会を減らし、有人装備と無人アセットのそれぞれの強みを活かした任務遂行につながり得る。防衛省・自衛隊は、情報空間における AI と物理空間における AI を分断せず、任務に必要な能力という観点から活用を検討する。

さらに、AI はサイバー防御を高度化する手段となる一方、脅威を与える側によるサイバー攻撃、偽情報の生成、AI のモデルやデータを標的とする攻撃等にも悪用されている。したがって、AI によって防衛力を強化すると同時に、AI を利用する環境自体の安全性を確保するとともに、機密性、完全性及び可用性を維持する必要がある。

## 2　AI の可能性と限界

AI によって、膨大な情報から重要な変化を抽出し、状況認識を迅速化し、複数の選択肢を整理して人間の意思決定を支援することができる。また、需要予測、整備予測、翻訳、文書処理等を支援し、定型的・反復的な作業に要する負担を軽減することで、限られた人的資源を、より高度な判断や創造的な業務に振り向けることが期待できる。

一方、AI の出力には一定の誤りが含まれ得る。学習データの偏りや運用環境の変化によって性能が低下することがあり、もっともらしいが事実に基づかない内容を生成する場合もある。また、初めて遭遇する状況や、文脈、価値判断、法的評価を伴う複雑な状況では、人間による判断が不可欠である。AI を導入すること自体を目

的としてはならず、防衛省・自衛隊として解決すべき課題を明確にし、その課題にAI が有効か、人間がどのように関与すべきか、必要なデータを確保できるか、利用に伴うリスクを管理できるかを確認することを基本とする。

AI エージェントの利用では、出力の評価に加え、アクセス先、変更可能な情報及び実行可能な行動の管理が必要となる。具体的な権限設定と管理の仕組みは、第5章に示す。

## 3　目指す姿

人間が責任を持って判断・指揮し、AI とデータによって人の知性と部隊の行動を拡張することで、我が国の主権、国民の生命及び財産を守り抜く防衛力を実現する。

この目指す姿の下、第一に、情報の収集、分析、状況認識、判断及び行動に至る一連の過程に AI や自動化技術を最大限適用し、意思決定の質と速度を高める。第二に、無人化・遠隔化に加え、ロボティクス等を活用することにより、隊員が危険な環境に置かれる機会を減らすとともに、一人一人の隊員がより適切に行動できるよう支援する。第三に、補給・整備・輸送等の後方支援を高度化し、厳しい状況における任務の持続性を高める。第四に、行政・管理業務に AI を適用し、人の力を判断、指揮、教育訓練等に振り向ける。

この目指す姿を実現するため、本ビジョンは三つの転換を進める。第一に、「情報を迅速に判断と行動につなぐ」転換である。情報を保有・処理する組織から、AI とデータによって、状況の変化に応じて情報を迅速に判断と行動へつなげる組織へ転換する。第二に、「人間が指揮し、責任を持つ」転換である。人間が最終的に指揮をとり責任を負う原則は維持しつつ、AI の出力を確認する運用から、AI の目的と権限を定め、用途とリスクに応じて監督し、必要に応じて介入できる業務プロセスと体制を備えた組織へ転換する。第三に、「AI を自ら選び、改善し続ける」転換である。優れたAIを導入して終わるのではなく、必要なAIとデータを自ら選択・評価し、必要な改良を行い、運用するとともに、必要に応じて別の技術へ移行できる組織へ転換する。

三つの転換を通じて、情報、指揮統制、有人・無人アセット、後方支援及び行政・管理業務を相互につなぐ。同盟国・同志国等とも、我が国の主体的な意思決定と重要なデータの管理を維持しながら、相互運用性を追求する。

# 第2章　AI活用の基本原則を定める

前章の三つの転換を実現するため、次の原則を貫く。法令適合、安全性及び信頼性等を、責任あるAI活用の不可欠な条件として確保する。

## 1　判断と責任は、人間が持つ

AIは人間の判断を支援するものであり、意思決定は人間が主体的に行う。人間がAIの目的と権限の範囲を定め、適切なタイミングで人間の判断を介在させるとともに、用途、影響及びリスクに応じて作動状況を把握し、監督する。必要に応じて介入できる仕組みを確保し、最終的な指揮及び責任は人間が負う。

自動化されたシステムへの過度な信頼や依存、いわゆる自動化バイアスを防ぐため、利用者及び監督者に対する教育・訓練を行う。AIの提案を鵜呑みにせず、他の情報や専門的知見と照合し、自ら判断する能力を維持・向上させる。

## 2　法とルールに基づく責任ある利用

AIの研究開発、導入及び運用は、国際人道法を始めとする国際法及び国内法に適合する形で行う。AIを活用した装備品等については、関係する規則等に基づき法的適合性及び責任ある利用を確保する。

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。AIの軍事利用に関する国際的な議論に注意を払い、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形成に、積極的かつ建設的に貢献する。

## 3　安全性、信頼性、透明性及びアカウンタビリティ

防衛省・自衛隊におけるAIガバナンスは、リスクを評価及び低減しつつ、AIがもたらす便益を最大化することを目的とする。安全性、信頼性、透明性及びアカウンタビリティ等については、政府の関係指針等を踏まえ、防衛分野の用途及びリスク並びに特性に応じて確保する。

AIの性能は導入時点で固定されるものではない。データの変化、運用環境の変化、モデルの更新等により性能やリスクが変化し得る。このため、導入前の試験だけでなく、運用中の監視、定期的な再評価、更新時の確認、必要な場合の切戻しを含む

継続的な保証を行う。判断に影響するデータ、主要な処理、更新等について、技術的に可能かつ合理的な範囲で追跡・遡及できる状態を確保する。

制度・技術の進展や国内外の知見を取り入れ、AI の性能、利用環境及びリスクの変化並びに評価結果に応じて、評価及び管理の方法を継続的かつ機動的に見直す。その際、法的適合性、安全性及び情報保全を確保しつつ、用途とリスクに応じた管理の下で、迅速な試行、評価及び改善を進める。

### 4　必要な技術とデータを、継続的かつ自律的に利用できる能力を確保する

防衛上重要な AI 及びデータについては、外部の製品・サービスを活用する場合であっても、防衛省・自衛隊が必要な評価を行い、利用条件を把握し、更新、改良、停止及び移行を主体的に判断できる能力を保持する。

特定の技術、製品又は事業者への過度な依存を避け、技術の進展、任務上の要求及び供給環境の変化に応じた更新、改良、停止及び移行が可能となるよう、継続性と選択肢を確保する。そのため、必要なデータ、定義、仕様、利用・改良に関する権利、監査情報等を確保し、必要な時に利用できない、改良できない、他の環境へ移行できない状態を回避する。

### 5　任務を起点に、迅速に導入し改善する

AI の活用は、技術そのものから出発するのではなく、任務上又は業務上の課題から出発する。何を改善するのか、成果を何によって確認するのかを明確にした上で、必要な技術、データ、人材及び運用方法を組み合わせる。

安全性及び情報保全を確保しつつ、迅速に導入する。全ての基盤の完成を待つのではなく、導入と基盤整備を相互にフィードバックさせながら進める。運用部隊、研究開発・装備取得部門及び民間事業者が連携し、短期間で作成した試作品の試用・評価を通じて、得られた知見を継続的な能力の向上に反映する。

人間の指揮・責任、AI による能力の拡張、データとデジタル基盤を一体として構築し、防衛力全体の変革につなげる。

## 第 3 章　任務遂行・業務を変革する

本章の目的は、AI の活用分野を増やすことではない。情報を得てから状況を理解し、人間が判断し、部隊が行動し、その行動を後方が支えるまでの一連の流れを変えることである。AI とデータによって、この流れの分断を減らし、人間がより早く、より確かな判断と行動に集中できる状態をつくる。以下の取組は、それぞれを独立した AI 活用分野として進めるのではなく、情報を人の判断と部隊の行動に活かす一連の流れとして、相互に連接させて導入・運用する。その際、既存の任務・業務の単なる自動化にとどめず、任務遂行要領、業務手順、役割分担及び装備の活用の在り方を一体的に見直す。

## 1　情報の収集・整理から、変化の抽出までを高度化する

レーダー航跡、衛星画像、航空画像、電波情報、公開情報その他の多様な情報について、AI を活用して横断的に整理・分析し、重要性や不確実性に応じた人間の確認を確保しながら、情報処理を効率化する。その際、AI によって大量の情報の中から変化、異常その他の任務上着目すべき情報を即時に抽出し、探知・識別及び今後起こり得る事象の予測を含む状況認識を迅速化することで、刻々と変化する状況に対応する。増大するセンシングデータについては、ネットワークや計算資源の状況に応じ、エッジ AI での処理の活用も図る。

AI に任せるのは、大量の情報の整理・照合と、人間が見るべきものの絞り込みである。その意味を吟味し、相手の意図や情勢を最終的に判断するのは人間である。データの来歴、モデルの特性及び不確実性も踏まえ、人間が限られた時間を情報の探索だけでなく、状況の判断と必要な行動に使えるようにする。

## 2　「情報を示す」から「判断と行動につなげる」へ

警戒監視・情報収集によって得られた情報を、個別のシステムや領域の中にとどめず、統合、分析及び可視化し、指揮官の状況認識と迅速な意思決定につなげる。AI による行動方針の整理やシミュレーション等も活用し、限られた時間の中で、刻々と推移する戦況や各種の目標に対し、対応手順や選択肢を迅速に導き出し、比較・検討できる環境をつくる。

目指すのは、AI に判断させる指揮統制ではない。AI によって重要な情報と選択肢を整理・絞り込み、人間の認知負荷を軽減しながら、より早く自ら判断できる指揮統制である。AI が示した提案について、その前提、使用した情報、確度及び限界を

可能な範囲で把握できるようにし、最終的な判断、指揮及び責任は人間が担う。領域横断の情報連携を進め、防衛力の発揮の仕方を変える。

### 3 「人を危険にさらす」ことを前提としない任務へ

無人アセット、フィジカル AI 及びロボティクスの活用に当たっては、単なる既存装備の無人化・自動化にとどめず、任務の遂行要領を見直し、人と機械のそれぞれの強みを組み合わせる。AI を周囲の認識、経路選択、機体制御、有人装備との連携等に活用し、隊員が危険な環境に立ち入る機会を減らしながら、必要な任務の遂行に寄与する。

その際、AI については、センサー、通信及びデータとの連接並びに人間による指揮・監督を一体として考慮する。通信の制約・途絶時や AI が利用できない場合にも必要な任務を継続できるよう、用途に応じた処理方法と代替手段を検討する。

### 4 AI で守り、AI そのものも守る

サイバー空間では、AI は防御を強化する手段であると同時に、脅威を与える側によって攻撃を高度化・自動化する手段ともなり得る。用途に適した AI の性能及び安全性を評価した上で、振る舞い・異常検知、情報整理等に活用し、関係法令及び所掌に基づき、関係機関とも連携して脅威の把握と対処を支援するとともに、AI を利用した攻撃への対応能力を高める。

同時に、AI を防御側の新たな弱点にしてはならない。AI のモデル、データセット、ハーネス、接続する外部サービス等を一体として防護し、AI が参照する情報を通じた誘導、データの改ざん、モデルの機密性・完全性・可用性を損なう攻撃等を想定して、AI 自体とその利用環境を保護する。また、学習・ビルド環境を含む開発基盤及びソフトウェア・サプライチェーンの安全性・信頼性の確保に努める。

### 5 後方支援の実効性と持続性を高める

補給・整備・輸送等の後方支援は、燃料、弾薬、糧食等の必要な物資を部隊に届け、装備品を任務に使用できる状態に保ち、人員や物資を必要な場所へ移動させることにより、部隊の活動を支え、任務の持続性を左右する重要な要素である。

これらの業務は相互に密接に関連しており、一体として機能することで、厳しい状況においても部隊は活動を継続することができる。後方支援における AI の活用を考えるに当たっては、業務の効率性のみならず、需要予測、整備予測、輸送計画を

含む部隊の活動全体を踏まえた支援の実効性及び任務の持続性の観点を重視する。また、AI への過度な依存を避け、AI や通信等が利用できない場合の影響にも留意する。

## 6　人にしかできない仕事に、人の力を戻す

文書作成、翻訳、情報検索、照会対応、定型的な分析その他の行政・管理業務では、解決すべき課題と期待する効果を明確にし、生成 AI 等の活用の要否及び方法を判断する。AI の導入自体を目的とせず、業務そのものの見直しと併せて、有効性、費用対効果及び利用に伴うリスクを踏まえ、適切な手段を選択する。これにより、隊員・職員の負担を軽減し、その時間と力を、政策立案、判断、指揮、教育訓練、創造及び関係者との調整等、人間が担うべき仕事へ振り向ける。機密性の高い情報についても、情報区分、提供元の条件及び職務上の必要性に応じた利用環境と保全措置を確保した上で、AI の活用を検討する。

安全性及び情報保全を確保した環境で、業務に精通した隊員・職員が生成 AI を用いて簡易なアプリケーションや試作品を作成・検証し、業務改善や要求の具体化に活かす取組を進める。

生成 AI の利用に伴う入力情報、生成物の正確性、著作権その他の権利、ログ、利用環境及び情報保全等のリスクは適切に管理する。同時に、利用を通じて得た知見や課題をルールと教育に戻し、AI を安全に使える範囲そのものを継続的に改善する。

## 7　平素から学び、共に動ける力をつくる

AI は、実際の任務で使用する時だけではなく、その前段階である教育・訓練、研究開発及び能力向上にも活用する。教材作成、シミュレーション、訓練結果の分析・可視化等を通じ、隊員が AI を使う能力だけでなく、AI の結果を評価し、自ら判断する能力を高める。現実世界では十分なデータを得ることが困難な任務については、シミュレーション等も活用し、訓練、研究開発及び AI の評価に必要な知見を蓄積する。

また、国際的な活動では、同じ AI を持つことではなく、AI やデータを活用しながら人間同士が状況を共有し、判断し、共に行動できることを重視する。国連平和協力活動、国際緊急援助活動等における情報整理、意思決定支援、多言語による調整等への活用を検討するとともに、AI 時代に共に任務を遂行するための能力を高める。

# 第 4 章　データを戦略的資産として活用する

情報を判断と行動につなげるためには、必要なデータを、必要な者が、必要な時に、安全かつ適切に利用できなければならない。データとこれを支えるデジタル基盤は、それ自体を整備することが目的ではなく、第 3 章で示した任務能力を実現するための共通基盤である。このため、各組織による部分最適を避け、防衛省・自衛隊全体の最適化、相互運用性及び継続性を確保する。

## 1　「データは任務遂行に不可欠な戦略的資産」との認識

AI の性能と実効性は、利用できるデータの質、量、適時性及び任務との関連性に大きく左右される。このため、「データがなければ戦えない」との危機感を共有し、データを単なる情報システムの付随物ではなく、抑止力・対処力及び任務遂行能力を高める戦略的資産として位置付ける。全ての隊員・職員がこの認識を共有し、日々の業務や訓練で生成されるデータを、将来の利用も見据えて適切に作成・管理する文化を形成する。

紙や閉じたシステムの中に情報を留めることを前提とせず、必要な安全性と権利を確保しながら、組織横断的に活用できるデータを増やす。データをデジタル化し、AI が利用可能な形で整備するとともに、データを使って業務を行うことを前提に、業務とシステムの双方を見直す。任務・業務上の課題から必要なデータを明らかにし、必要なデータの取得・蓄積・利用の仕組みを、業務及びシステムに組み込む。データの保存・廃棄は、関係法令及び文書管理に関する規則等に従い、将来の利用価値と情報保全にも留意して適切に行う。

## 2　データの所在、意味及び責任を明確にし、相互運用性を確保する

必要な者が必要なデータを利用するためには、どこに、どのようなデータが存在し、誰が責任を持ち、どの条件で利用できるのかを把握する必要がある。このため、初期段階で最優先に取り組む事項として、保有するデータの棚卸しとメタデータの整備を進め、データの名称、内容、管理責任、保管先、情報区分、更新頻度、利用条件等を把握できる状態を整える。

組織やシステムを越えてデータを連接・交換し、交換したデータを利用できる相互運用性を確保するため、データの意味・形式及び接続点に関する共通仕様を整備する。既存の国際規格、同盟国の政府標準、広く利用される公開仕様及び省内の標

準化の成果を活用し、全てのシステムの内部構造や機能を統一するのではなく、情報交換に必要な共通項目と接続点を中心に共通化又は相互に変換できる仕組みを整える。適用する規格、版、対象情報及び設定を明らかにし、各システムの特性に応じた連接方法を具体化する。

共通化の実効性を確保するため、仕様への適合性と、異なる実装を組み合わせた際の相互運用性を区別して確認する。既存の試験・評価の仕組みを活用し、必要に応じて実機・実回線による検証を行う。その成果は、関係部署と調整の上、取得・更新及び調達・契約に段階的に反映する。その際、技術的な実現可能性、既存の取得計画、費用及び運用への影響を踏まえ、一律の適用が困難な場合は、代替的な連接方法や適用時期を検討する。

### 3　データのライフサイクルを管理する

データの作成、取得、加工、保管、提供、利用、更新及び廃棄に至るライフサイクルを通じ、一貫したデータマネジメントを行う。提供側、加工側及び利用側の責任を明確化し、来歴、品質及び利用条件を維持する。特に、情報区分や利用条件等をデータと一体で管理し、組織やシステムを越えても取扱条件を維持しながら、安全に流通・活用できる仕組みを追求する。

AI が推論時に参照するデータと、AI 自体の学習・改良に用いるデータは、その影響と取扱いが異なる場合がある。このため、参照・検索と学習への投入を区別し、利用目的、情報区分、提供元条件等に応じて管理する。学習済みモデル、生成物及び処理記録についても、必要な管理を行う。

外部の製品・サービスを利用する場合にも、投入データ及び派生データの定義、来歴、利用条件並びに取り出し・移行に必要な資料及び利用権を確保し、製品や事業者が変わっても必要なデータを継続して利用できるようにする。事業者固有のデータモデル・処理規則と防衛省側の共通定義との対応関係を把握し、データの取り出しと、移行先での任務に必要な中核機能の継続を区別して確認する。事業者の知的財産及び商用製品の利用条件に留意し、権利の全面的な国有化や全機能の相互代替を一律に求めるのではなく、任務の継続等に必要な範囲を明確にする。

### 4　質、アクセス及び保護を両立する

AI に用いるデータについて、正確性、完全性、最新性、代表性等を用途に応じて確保する。偏ったデータによって AI の出力に不適切な偏りが生じないよう、学習データ及び評価用データの品質を確認する。運用中に得られたデータを、評価、再学習及び改善に戻す循環を構築する。

必要なデータへのアクセスを広げることと、情報保全を対立するものとして扱わない。機密性の高い作戦関連データ等にも留意し、情報区分と職務上の必要性に基づくアクセス制御、認証、監査、ログ等により、適切な者が適切なデータを情報区分に応じた環境で利用できるようにする。データの共有に当たっては、情報区分及び取扱条件が共有先でも適切に維持されるようにする。同時に、抗たん性、バックアップ及び継続利用にも配慮する。

### 5　実行計画に基づき、データの整備・管理・活用を具体化する

本章の取組は、第 8 章に示す統括体制の下で策定する実行計画に位置付け、優先分野、整備対象、実施主体、工程及び必要資源を明らかにして進める。データの整備・管理・活用に必要な事項は、同章に示す統括体制の下、関係機関が連携して具体化する。

## 第 5 章　AI を使い続け、改善し続ける基盤を構築する

AI を一度導入して終わるのではなく、任務や技術の変化に応じて選択・評価・改良し、使い続けるための基盤を構築する。前章のデータとデジタル基盤を一体として設計し、特定のモデル、サービス又は事業者が変わっても、重要な任務の遂行とデータの利用を継続できる構成を目指す。

### 1　通信、クラウド、計算資源を一体として整える

AI の利用には、モデルだけでなく、通信、計算資源、クラウド、ストレージ、データ、端末及び開発環境が必要となる。情報区分、用途、必要な性能及び任務の継続性を踏まえ、これらを一体的に整備する。機密性の高い用途では必要な管理権限と保全性を確保しつつ、民間の技術進展を取り込める構成を目指す。

AI の計算需要は、学習、評価、推論等によって異なる。必要な能力を全て単独で保有することを前提とせず、専有・共用、内部・外部等の選択肢を、情報保全、費用、供給継続性及び任務上の要求に応じて組み合わせる。

## 2　開発・学習・評価・配布の循環を確立する

AI は、導入後もデータと環境の変化に応じて評価・改良する必要がある。このため、運用環境及びシミュレーション環境から得たデータを維持管理環境へ移し、データ分析、学習・調整、検証を経て、評価済みのモデルを運用環境へ反映する一連の循環を確立する。

商用サービスの利用、既存モデルの追加学習、共同開発及び独自開発は、それぞれ利点と負担が異なる。任務、データ、機密性、改良の必要性、利用・改変権、計算資源及び人材等を踏まえて選択する。全てを自作するのではなく、必要な選択・評価・改良能力を自ら保持することを重視する。このため、省内の関係機関が、必要な権限及び手続の下で、データ整備、設定変更、再学習、評価、配布、軽微な改修及び不具合対処等を担える能力を段階的に確保する。学習データ、モデル、評価結果、ソースコード、ハーネス等の再利用可能な成果と知見は、情報区分、権利及び利用条件に応じて組織横断で蓄積・共有する。

## 3　AI エージェント及び複数 AI の利用を安全に管理する

AI が複数のツールやシステムを利用して業務を進める場合には、その用途及びリスクに応じ、人間が設定した一定の権限の下で行動するシステムとして管理する。閲覧と変更を区別し、必要最小限の権限を付与し、重要な操作には人間の確認を置き、処理を記録する。人間が入力・出力、権限及び処理状況を把握し、必要に応じて介入又は切戻しを行える仕組みを確保する。

複数の AI モデルやツールを連携させ、又は使い分ける場合、モデルの選択、権限、接続、処理記録等を共通のルールで管理し、異なる AI の出力を安全に組み合わせて利用できるようにするとともに、モデルを変更しても任務の遂行やデータの利用を継続できる構成を目指す。

## 4　通信制約下・途絶時にも任務を継続する

防衛の任務では、クラウドへの接続や通信帯域に制約が生じ、通信が途絶する場合もある。AI の利用に当たっては、こうした通信環境の制約を踏まえ、任務継続の観点に留意する。

具体的には、通信の制約や途絶によりクラウドや外部サービスへの接続が困難となる場合に備え、任務に必要な AI 機能を維持できるよう、エッジ AI やスタンドアロ

ーン環境の活用を図る。あわせて、障害時に損なわれた通信機能等を復旧できるようにし、任務の継続を支える組織のレジリエンスを高める。

# 第 6 章　人材と組織文化を変革する

人材育成の目的は、単に AI の操作方法を教えることではない。全ての隊員・職員が、AI に何を任せるかを考え、その結果を評価し、必要な場合には介入できる力を持つこと、また、必要な AI を選択・評価・改良できる専門人材を育成し、その能力を省内に蓄積することにある。

## 1　全ての隊員・職員の AI リテラシーを高める

AI は一部の専門家だけのものではなく、全ての隊員・職員の任務・業務に関わるものである。このため、全ての隊員・職員が、AI の基本的な特徴と限界を理解する必要がある。各隊員・職員は、講話や公開資料、隊員・職員による創意工夫等を通じ、それぞれの役割に応じて、AI の可能性と限界、誤りや偏りの確認、情報の取扱い及び人間による判断が必要となる場面について理解を深める。

教育は知識の習得だけでなく、実際に AI を利用し、成果を評価し、自らの任務に適用する力につなげる。禁止事項と利用可能な範囲を明確化した上で、認められた環境では積極的に利用し、知見を蓄積する。「使ってよいか分からないから使わない」状態を避け、ルールを理解し、責任を持って使いこなす組織文化を形成する。また、情報過多による認知負荷にも対処し、AI の出力を主体的に吟味する力を養う。安全性及び情報保全を確保した上で、新たな技術の試行と業務の見直しを奨励し、得られた知見を組織として共有して継続的な改善につなげる。

## 2　専門人材とプロジェクトを率いる人材を育てる

AI とデータに関する人材は、利用者、データ人材、AI エンジニア、研究者、プロジェクトを率いる者等、多様な役割から構成される。要求設定、データ整備、モデル評価、学習・調整、改修、試験、運用、調達・契約等の役割に応じ、必要な能力を体系的に育成する。特に、任務上の要求を技術的な要件に具体化し、技術の性能、成熟度、適用可能性、限界及びリスクを評価して、複数の選択肢を比較できる中核的な専門人材を育成する。

専門人材が持つ知識を個人に閉じ込めず、文書化、教育、OJT 及び配置を通じて組織に蓄積する。AI への関心や適性を持つ人材を早期に見いだし、専門教育につなげるとともに、異動後も経験とベストプラクティスを共有できる仕組みを整える。

### 3　民間等の専門性を取り込む

AI の技術革新は民間を中心に急速に進んでおり、防衛省・自衛隊のみで全ての能力を保持することは現実的ではない。国内企業、スタートアップ、国立研究開発法人・大学等との連携を強化し、研究開発、人材育成、評価、政策立案及び取組の具体化に外部の専門性を活用する。また、データの意味や関係をオントロジーとして整理し、現場と技術をつなぐフォワード・デプロイド・エンジニア（FDE）等の専門性を活用する。

一方で、外部に依存するほど、内部に要求設定、技術評価、契約管理及び運用判断の能力が必要となる。委託・共同事業を通じて得られた知見が省内に残るよう、文書化、教育及び知識移転を重視する。

## 第７章　国内基盤を強化し同盟国・同志国等と連携する

我が国が目指す自律性とは、全てを国産化することではない。同盟国・同志国等と連携し、国内外の優れた技術を活用しつつ、我が国の防衛に必要な AI について、我が国が選択権と継続利用の主導権を失わないことである。技術の選択に当たっては、国産・海外製の別のみで判断せず、性能、信頼性、セキュリティ、相互運用性、供給及び運用の継続性、導入後の改良の可能性等を総合的に考慮する。その上で、任務上の要求を定め、AI を評価し、データを管理し、必要な改良を行い、運用を継続するための中核的な技術、知見及び能力を国内に維持・蓄積する。任務の重要性及び情報区分を踏まえ、国内に維持すべき能力と同盟国・同志国等との共通化・連携を適切に組み合わせ、主導権の保持と相互運用性を両立する。

### 1　官側が主導権を持つ開発・調達

AI に係る技術選択は、企業側が提示する製品やサービスに合わせて行うのではなく、防衛省・自衛隊が任務上の要求を明確にし、必要な性能、安全・保全条件、データ条件及び評価基準を主体的に設定した上で行う。仕様、標準及び契約条件を適切に用い、多様な企業が技術を提案し、競争できる環境を整える。官側による試

行・検証の知見を要求及び評価基準に反映するとともに、民間の専門性と継続的な維持管理能力を活用し、内製と民間活用を適切に組み合わせる。

AI 調達では、初期の導入価格だけでなく、運用、更新、再評価、監視、人による確認・修正等を含む総経費を考慮する。また、モデル及びデータの由来、利用条件、利用・改良権、供給継続性、監査、契約終了時のデータ・仕様等の取り出し及び移行可能性を確認する。

研究開発、試行及び調達を通じて民間の創意工夫を取り込み、国内の投資と技術革新を促す。こうした取組を国内企業の競争力の向上と防衛基盤の強化につなげ、防衛と経済の好循環を目指す。

### 2　相互運用性と標準化

同盟国・同志国等との相互運用性は、単に同じシステムや同じ AI を導入・使用することを意味しない。データの意味・形式、接続点、権限、評価及び運用手順を整え、我が国の主体的な意思決定、独立した指揮命令系統及び機微なデータの管理を維持しつつ、異なるシステムや AI が得た情報・分析を相互に理解し、共同の任務に利用できる状態を目指す。

民間分野を含め、国際的に用いられている標準・規格を積極的に活用しつつ、防衛上必要な識別、情報区分、構造、拡張方法等について共通の条件を整える。独自仕様を必要最小限にし、製品や事業者が変わっても、システム間の連接及びデータ交換を継続でき、必要な更新・移行が可能な構成を追求する。

### 3　同盟国・同志国等との協力

日米間では、我が国の主体的な意思決定の軸を堅持しつつ、AI を用いた状況認識、意思決定支援、データ利用等について、相互運用性を高める。異なる AI が異なる分析や提案を示す可能性も踏まえ、何を共有し、どのように人間同士が判断を調整するかという観点から、AI 時代の連携の在り方を深める。

同志国等との間では、活用事例の共有、共同実証、データの意味・形式及び接続点等の標準化、教育・訓練及び人材交流等を進め、AI とデータを安全かつ責任ある形で共に活用できる能力を高める。

## 第 8 章　三つの転換を実行し、不断に改善する

本ビジョンの成否は、AI をいくつ導入したかではなく、「情報を迅速に判断と行動につなぐ」「人間が指揮し、責任を持つ」「AI を自ら選び、改善し続ける」という三つの転換が実際の任務・業務において実現したかによって判断する。

全体の優先順位を定め、重点プロジェクトで具体化し、成果を評価して、次の取組と資源配分につなげる。この循環を通じ、個別の AI 導入を防衛力全体の変革へ結び付ける。技術、脅威及び利用環境の変化を継続的に捉え、試行と評価から得た知見を次の取組に反映することで、組織としての適応速度を高める。

## 1　AI、データ及びデジタルを一体的に統括し、現場が実行する

デジタル統括責任者に、AI 統括責任者及びデータ統括責任者を兼ねさせ、AI、データ及びデジタルを一体的に統括する体制を確立する。デジタル統括責任者は、関係機関と連携し、AI、データ及びデジタルに関する全体方針、優先順位、共通基盤、標準及び運用ルールについて組織横断の調整を行う。

デジタル統括責任者の下に、省全体のデータ管理を担う組織を整備する。同組織は、データの整備・管理・活用に係る共通仕様の策定・更新、データの所在・管理責任の把握、組織横断のデータ連携に係る調整並びに各機関の実施状況の確認を担う。各機関は、所掌するデータの管理責任を明確にし、同組織と連携して取組を実施する。具体的な組織構成、役割分担、権限及び手続は、既存の所掌・体制を踏まえ、別途定める。

デジタル統括責任者の下で、AI、データ、ICT、運用、取得等を所掌する関係機関が連携し、本ビジョンに基づく実行計画を策定する。省全体のデータ管理を担う組織は、データに関する取組の取りまとめを担う。実行計画には、重点プロジェクトを位置付け、各プロジェクトの実施主体、責任者、工程、必要資源、成果指標及び評価・見直しの時期を定める。

各機関は、防衛省・自衛隊全体のアーキテクチャ及び実行計画との整合を図りつつ、任務上の課題を明確にし、所掌に応じて現場の専門性と迅速性を活かして実施する。デジタル統括責任者は、関係機関からの報告等を通じて進捗及び成果を確認し、必要な調整を行う。

共通化する事項と現場の裁量に委ねる事項を明確にし、重複・分断と過度な集中の双方を避ける。安全性、情報保全及び相互運用性等の共通原則を確保した上で、

各機関・部隊の任務、環境及び成熟度に応じた自律的な試行・改善を支える。先行的な取組の成果と知見を組織横断で共有し、方針や基盤の改善に戻すことで、全体最適と現場の柔軟性を両立する。

## 2　重点プロジェクトで具体化する

重点プロジェクトは、三つの転換を具体的な任務・業務で実現する取組及びその実現に必要な共通基盤・ルールを整備する取組として選定し、実行計画に位置付ける。データに関する取組、共通基盤の構築及び人材育成等も対象とする。選定に当たっては、任務への効果と実現可能性を基本に、データ・人材の準備状況、安全・保全、外部依存、総経費及び他組織への展開可能性等を評価する。

各プロジェクトでは、解決する課題、利用部門・運用主体、責任、期限、必要資源及び運用への移行条件を定める。あわせて、三つの転換の何を実現し、実施前と比べて何が変われば成果とするのかを明確にする。既存事業も同じ観点から確認し、本ビジョンとの接続を明らかにする。

## 3　成果で評価し、資源配分に反映する

プロジェクトごとに、判断の質と迅速性、任務への寄与、隊員の安全確保・負担軽減、持続性、安全性・信頼性、総経費及び現場への定着等から、目的に応じた成果指標を設定する。導入数や利用回数だけでなく、実施前後の任務・業務の変化を確認する。指針や共通基盤の整備については、策定・整備の完了だけでなく、各機関での適用状況や任務・業務の改善への寄与も確認する。

一定の節目で成果と課題を評価し、継続、拡大、変更又は終了を判断する。評価結果を、次のプロジェクトの選定、共通基盤の改善及び資源配分に反映する。節目は成功を必須とする期限ではなく、次の判断を行う機会とし、期待した成果が得られなかった取組の知見も活用する。

## 4　取組を見直し、ビジョンの軸を維持する

デジタル統括責任者の下で、技術、脅威、供給環境、法制度及び国際的な規範の変化と評価結果を踏まえ、実行計画及び重点プロジェクトを見直す。

長期に維持すべき目的・原則と、迅速に変更すべき具体的な取組を区分する。三つの転換という軸を維持しつつ、目指す姿や基本原則に影響する重大な変化が生じ

た場合には、本ビジョンの本文も見直す。これらを通じ、任務を起点として、AI とデータによって可能となる新たな任務遂行・業務の在り方を追求し、現場の知見を組織全体に還元しながら、変化に適応して学習・改善し続ける組織への変革を進める。