

ジェンダー視点から捉える航空意思決定インテリジェンス

——AI と人間の判断を組み合わせた次世代の航空安全保障

特別研究官（国際交流・図書担当）付 岩田 英子

はじめに

航空機を安全に飛ばすためには、天気、航空交通、空港の状況、航空機の性能など、多くの情報が必要である。しかし現在、航空を取り巻くリスクはさらに複雑になっている。戦争や紛争、ミサイルやドローン、全球測位衛星システム（Global Navigation Satellite System：GNSS、以下、GNSS）への電波妨害、サイバー攻撃、異常気象、燃料や部品の不足などが、航空機の安全や運航に同時に影響する可能性がある¹。

例えば、ある地域で紛争が起きているという情報だけでは、その上空を飛んでよいかどうかは決められない。どのような兵器が使われているのか、どこまで届くのか、空域は閉鎖されているのか、別の経路を飛べるのか、燃料は足りるのか、代わりの空港を利用できるのか、といった多くの情報を組み合わせる必要がある。国際民間航空機関（International Civil Aviation Organization：ICAO、以下、ICAO）も、紛争地域とその周辺を飛行する民間航空機について、最新情報を共有しながら継続的にリスクを評価することの重要性を示している²。

そこで本稿では、航空意思決定インテリジェンス基盤（Aviation Decision Intelligence Platform：ADIP、以下、ADIP）という分析枠組みを提示する。ADIP とは、航空、気象、地政学・軍事、サイバー、空港などの情報を人工知能（Artificial Intelligence：AI、以下、AI）で分析し、さらに人間の専門知識や経験を組み合わせることによって、航空組織が「どう行動すべきか」を判断するための枠組みである。ADIP は既存の特定の製品や情報システムの名称ではなく、筆者による本稿で提示する考え方である³。

そして、この意思決定をジェンダー視点から考える。それは、多様な立場の人が受ける影響を見落とさないためである。ここでいうジェンダー視点とは、女性だけを見ることではない。性別、年齢、職業、経

験、身体的特性、文化、社会的立場などが異なれば、同じ危機でも見えるものや受ける影響が違うことに注目する考え方である。つまり、「誰の知識を判断に使っているのか」「誰の安全を守ろうとしているのか」を問い直す視点である。

本稿は、こうした問題を検討してきた一連のコメンタリーの第 6 作に当たる。本シリーズは、主として WPS の文脈で制度化されてきたジェンダー視点を、AI をはじめとする防衛先端技術の設計、取得、運用、指揮統制及び組織学習にも応用できるのではないかと、という政策的問いを提示するものである。ジェンダー視点を、防衛先端技術が見落とし得る情報、経験、リスク及び影響を明らかにするための分析視角として用い、複数の事例を通じて、その応用可能性を検討する。

情報を集めるだけでは安全を守れない

AI には、大量の情報を人間より速く処理できるという大きな利点がある。例えば、ある空域で GNSS への電波妨害が起きたとする。AI を使えば、その場所、軍事活動、航空機の飛行経路、天候、利用可能な空港などを短時間で組み合わせて分析できる。

しかし、航空会社や政府が本当に知りたいのは、単に「GNSS への妨害が起きている」という事実ではない。必要なのは、「何が起きているのか」、「それは航空運用にどのような危険をもたらすのか」、そして「では、どう行動するのか」という判断である。ICAO も、安全に関するデータや情報を集めるだけでなく、それを分析し、実際の意思決定に利用できる情報へ変えることを重視している⁴。ADIP で AI に期待するのも、この過程を助けることである。

ただし、AI が示した答えが、そのまま最終的な答えになるわけではない。例えば AI が「この経路なら飛行可能」と判断しても、人間は、乗客の安全、法律、燃料、乗員の勤務時間、代替空港、社会への影響などを考えなければならない。

したがって、航空意思決定インテリジェンス（Aviation Decision Intelligence）とは、AI に判断を任せることではなく、AI の分析を人間が意味のある判断へ変える能力なのである。

AI は速いものの「何を大切にするか」は決められない

AI は、大量の情報から人間が気づきにくいパターンを見つけることができる。

しかし、AI の判断は完全に客観的なものではない。AI が何を危険と判断するかは、どのようなデータを使ったのか、何を重要な指標にしたのか、どのような目的で設計されたのかによって変わる。そのため、責任ある AI（Responsible AI）では、AI の性能だけではなく、人間が AI を監督し、その判断を確認できることが重要になる。

米国防総省（U.S. Department of War: U.S. DoW、以下、U.S. DoW）の責任ある AI に関する方針や、米国立標準技術研究所（National Institute of Standards and Technology : NIST、以下、NIST）の AI リスク管理枠組（AI Risk Management Framework）も、AI のリスクを技術だけの問題ではなく、人間や組織を含めて管理する必要性を示している⁵。

つまり、「AI は分析する。」「人間はその意味を考える。」「組織は最終的な判断に責任を持つ。」という役割分担が必要になる。人間中心の AI（Human-centered AI）とは、単に最後に人間が承認ボタンを押すことではない。AI が「安全」と示した場合でも、人間が「本当にそうなのか」と疑問を持ち、必要であれば異論を述べられなければならない。

さらに、近年では AI が外部の情報システムやツールと接続し、一定の範囲で自律的に行動する AI エージェントの利用も進みつつある。このような AI では、人間による監督は AI の「判断」を確認するだけでは十分ではない。AI にどこまでの権限を与えるのか、どの情報やシステムへのアクセスを認めるのか、行動をどのように監視し、必要な場合に誰が停止させるのかを、あらかじめ決めておく必要がある。責任ある AI には、AI の判断だけでなく、その行動範囲を人間と組織が統制できることも重要になる。

ジェンダー視点は AI の「見落とし」を探す

ここでジェンダー視点が重要になる。

航空の安全に関わる人は、パイロットだけではない。航空管制官、整備担当者、客室乗務員、空港職員、保安担当者、地上支援業務の担当者など、さまざまな人がいる。同じ問題を見ても、立場によって見えるものは違う。

例えば、航空機の遅延について、運航担当者は「次の便をどうするか」と考えるかもしれない。整備担当者は機体の状態を心配するかもしれない。客室乗務員は乗客の安全や疲労に気づくかもしれない。地域の人々は、医療、物流、観光への影響を見るかもしれない。ところが、組織が一部の情報だけを重要と考えていれば、こうした知識は意思決定から抜け落ちる可能性がある。

NATO の 2024 年の WPS 政策も、ジェンダー視点を取り入れることが、作戦環境、リスクや脆弱性の

理解、情報共有、インテリジェンス、意思決定などの改善につながるとしている⁶。ジェンダー視点を取り入れる意味は、単に女性を意思決定の場に増やすことではない。重要なのは、「誰がいるのか」だけでなく、「誰の知識が判断に使われているのか」を見ることである。

AI が高度になるほど、この問いは重要になる。AI の答えが数字や確率で示されると、人間はそれを「客観的な答え」と思い込みやすいからである。異なる経験や専門知識を持つ人が AI の判断を検証することは、AI が見落とした情報や間違った前提を発見することにつながる。

AI 時代に強い組織とは何か

航空安全保障では、AI そのものの性能だけでなく、AI を使う組織の能力も重要になる。

「ジェンダー視点からの防衛先端技術」シリーズで提示する人的・組織的レジリエンス分析（Human & Organizational Resilience Analytics：HORA、以下、HORA）は危機に対応できる人間と組織の力を分析する考え方であり、この問題を考えるための分析枠組みである。HORA とは、カール・E・ワイク（Karl E. Weick）らの高信頼組織研究、エリック・ホルナゲル（Erik Hollnagel）らのレジリエンス・エンジニアリング及び U.S. DoW による責任ある AI に関する知見を統合し、AI 時代の人的・組織的要因を分析する枠組みである⁷。

どれほど高性能な AI を導入しても、組織の中で、「AI の判断は本当に正しいのか」「重要な情報が抜けていないか」「別の可能性はないか」と言える人がいなければ、AI の性能を十分に生かすことはできない。反対に、異なる専門知識を持つ人が情報を共有し、予想外の出来事にも対応し、必要であれば AI の判断にも異論を述べられる組織は、危機への対応力を高めることができる。

ここで重要になるのが、責任ある組織（Responsible Organization）である。本稿でいう責任ある組織とは、既存の固有の政策用語ではない。責任ある AI や人間中心の AI（Human-centered AI）を適切に運用し、AI による分析を信頼される意思決定能力へ変えることのできる組織を意味する。つまり、責任ある組織とは、AI の分析をうのみにせず、確認し、説明し、必要に応じて AI の行動へ介入し、最終判断とその結果に責任を持つ組織である。

AI 時代には、高性能な AI だけでなく、それを正しく疑い、使いこなせる人間と組織が必要なのである。

「航空機を守る」から「社会を守る」へ

航空機が飛べなくなったとき、影響を受けるのは航空会社だけではない。旅行者、仕事で移動する人、医療のために移動する人、空港で働く人、物流会社、観光業、地域住民など、多くの人々に影響が及ぶ。しかも、その影響は全員に同じではない。高齢者、障害のある人、乳幼児を連れた人、緊急に移動する必要がある人などでは、航空機が運航できないことによる負担が違ふ。

そのため、航空のレジリエンスを考えるときには、空港や航空機を早く元に戻すことだけでなく、「誰が影響を受けるのか」「誰に大きな負担がかかるのか」「誰を優先して支援するのか」まで考える必要がある。

NATO の WPS 政策も、危機が人々に異なる影響を与えることを考慮し、性別や年齢などによって細分化されたデータを意思決定に利用することを求めている⁸。この意味でジェンダー視点は、航空安全に後から付け加える「配慮」ではない。危機の全体像をより正確に理解するための方法なのである。

日本に必要なこと

日本でも、航空の安全を気象、サイバー、ドローン、防衛などに分けて考えるだけでは十分ではない。実際の危機では、異常気象が発生しているときにサイバー攻撃が起こったり、利用できる空域が制限されたりする可能性がある。そのため、国土交通省、防衛省・自衛隊、気象庁、警察、海上保安庁、航空会社、空港、自治体などが持つ情報を必要に応じて共有し、全体として判断できる仕組みが重要になる。

また、AI を導入するだけで問題が解決すると考えてはならない。NIST の AI リスク管理枠組が示すように、AI のリスク管理には、技術だけでなく、ガバナンスや継続的なリスク管理が必要になる⁹。

そして AI 時代のリーダーには、AI について詳しいことだけでなく、「AI の能力と限界を理解する」「異なる専門家の意見を聞く」「不完全な情報でも判断する」「AI の判断への異論を認める」「最終的な判断に責任を持つ」という能力が求められる。AI によって情報処理が速くなるからこそ、最後に必要になるのは、人間と組織の判断能力なのである。

おわりに

AI は、人間より速く大量の情報を処理できる。しかし、AI だけで「何が最も重要なリスクなのか」「どこまで危険を受け入れるのか」「誰を守るのか」を決めることはできない。航空意思決定インテリジェンスで重要なのは、AI に人間の判断を置き換えさせることではない。AI が情報を分析し、人間がその意味

を考え、組織が責任を持って判断する。そしてジェンダー視点によって、「誰の経験が入っているのか」「誰の知識が抜けているのか」「誰にどのような影響が及ぶのか」を問いつける。

航空意思決定インテリジェンス基盤の目的も、AI、情報、人間の経験、組織制度、責任構造を組み合わせ、信頼される判断能力をつくることにある。AI 時代の航空安全保障で重要なのは、最も高度な AI を持つことだけではない。AI の能力と限界を理解し、多様な人々の知識を組み合わせ、予想外の事態にも対応できる人間と組織をつくることである。ジェンダー視点は、そのための一つの重要な分析方法になるだろう。

¹ International Civil Aviation Organization (ICAO), Risk Assessment Manual for Civil Aircraft Operations Over or Near Conflict Zones, 3rd ed., Doc 10084; ICAO, Aviation Cybersecurity Strategy; ICAO, Protection of Civil Aviation Infrastructure Against Unmanned Aircraft; ICAO, 2024 ICAO Climate Adaptation Synthesis Report: Understanding Climate Risks and Building Aviation Resilience (Montreal: ICAO, 2024).

² ICAO, Risk Assessment Manual for Civil Aircraft Operations Over or Near Conflict Zones, Doc 10084; ICAO, "Risks Posed to Civil Aviation Operations over or near Conflict Zones."

³ ADIP は本稿が提示する分析枠組みであり、既存の特定企業又は機関による同名の製品・システムを指すものではない。その構成については、ICAO, Risk Assessment Manual for Civil Aircraft Operations Over or Near Conflict Zones, Doc 10084; ICAO, Safety Management Manual, 4th ed., Doc 9859 (Montreal: ICAO, 2018); ICAO, Aviation Cybersecurity Strategy; National Institute of Standards and Technology (NIST), Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (Gaithersburg, MD: NIST, 2023)を参照。

⁴ ICAO, Safety Management Manual, Doc 9859; ICAO, Safety Intelligence Manual, 1st ed., Doc 10159 (Montreal: ICAO, 2025). 同 Manual は、安全データ・情報を収集・分析・共有し、安全上の意思決定に利用できるインテリジェンスへ転換する考え方を示している。

⁵ U.S. Department of Defense, Responsible Artificial Intelligence Strategy and Implementation Pathway (Washington, DC: Department of Defense, 2022); NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1.

⁶ United Nations Security Council, Resolution 1325, "Women and Peace and Security," S/RES/1325 (31 October 2000); NATO, NATO Policy on Women, Peace and Security (Brussels: NATO, 10 July 2024), paras. 16–20, 26–28, 41. NATO 政策は、ジェンダー視点が作戦環境、リスク、脆弱性の理解や情報共有、インテリジェンス、意思決定の改善に寄与するとしている。

⁷ 本稿では、Human & Organizational Resilience Analytics (HORA) という分析枠組みを用いる。HORA は、Weick らの高信頼組織研究、Hollnagel らのレジリエンス・エンジニアリング及び U.S. Department of Defense による Responsible AI に関する知見を統合し、AI 時代における人的・組織的要因を分析する枠組みである。HORA には日本語訳を付さない。

⁸ NATO, NATO Policy on Women, Peace and Security (2024), paras. 4, 13, 19–20, 26–28, 41. 同政策は、社会的レジリエンスや危機対応とともに、性別、年齢その他の文脈上適切な要素によって細分化されたデータを意思決定に利用することを求めている。

⁹ NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1. AI リスク管理を Govern、Map、Measure、Manage の相互に関連する機能として組織全体に組み込むことを示している。

PROFILE

岩田 英子

特別研究官（国際交流・図書担当）付

専門分野：グローバルガバナンスと包摂的レジリエンス、軍事組織でのジェンダー視点のインパクト

本欄における見解は、防衛研究所を代表するものではありません。
NIDS コメンタリーに関する御意見、御質問等は下記へお寄せ下さい。
ただし記事の無断転載・複製はお断りします。

防衛研究所企画部企画調整課

直 通：03-3260-3011

代 表：03-3268-3111（内線 29177）

防衛研究所 Web サイト：www.nids.mod.go.jp