自律型兵器による戦争犯罪に対する戦闘員の刑事責任
Criminal Responsibility of Combatants for War Crimes Committed with Autonomous Weapon Systems.

西野　仁人

１．はじめに

1956年、米国ニューハンプシャー州で開催されたダートマス会議において、ジョン・マッカーシー（John McCarthy）、マービン・ミンスキー（Marvin Minsky）らによって初めて人工知能（以下、「AI」（Artificial Intelligence））という言葉が使用された[1]。今日ではこのAIは、第4次産業革命[2]と呼ばれる今後数十年の社会に影響を与える重大な変化の背後にある重要な技術といわれている[3]。近年では、ニューラルネットワークの多層化とインターネットなどがもたらすビッグデータ、そしてそれらを用いたディープラーニングの開発によって特化型AIが成長を遂げている。今やこうした進化はGoogle社やOpenAI社などの企業による汎用型AIの開発へ向かっている。

このようなAIの技術発展の成果は、既に軍隊が使用する兵器に取り込まれ武力紛争において現実に使用されている。2020年、リビアで発生した非国際的武力紛争において、リビア政府は敵対するハリファ・ハフタル側の武装勢力に対してトルコ製の自律型兵器（以下、「AWS」（Autonomous Weapon System））カルグ2を使用し、撤退するハフタル側の輸送車両などを攻撃した[4]。これは人間の意思が介在しないAWSによって初めて人間が殺害された可能性がある事例ではないかといわれている[5]。また、2022年2月より始まったロシアとウクライナとの国際的武力紛争において、両国がAWSを使用して相互に殺傷、破壊しているといわれている[6]。このように、今日の武力紛争ではAIを搭載したAWSと呼ばれる兵器が既に武力紛争において実際に使用され、現実に人や物、施設を殺傷、破壊している。

しかし、AWSが既に武力紛争において使用され、今後も大量に使用されることが予想されているにもかかわらず[7]、このAWSに関する国際法上の規制の進展は順調とはいい難い[8]。AWSの規制に関して、2014年に特定通常兵器使用禁止制限条約（以下、

---

[1] Arlindo L. Oliveira and Mário A. T. Figueiredo, “Artificial Intelligence: Historical Context and State of the Art,” in Henrique Sousa Antunes, Pedro Miguel Freitas, Arlindo L. Oliveira, Clara Martins Pereira, Elsa Vaz de Sequeira, Luís Barreto Xavier (ed.), *Multidisciplinary Perspectives on Artificial Intelligence and the Law* (Springer, 2024), p. 10.

[2] Klaus Schwab, “The Fourth Industrial Revolution: What It Means, How to Respond,” *World Economic Forum*, 16 January 2016, at https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

[3] Oliveira and Figueiredo, *supra* note 1, p. 22.

[4] United Nations, *Letter Dated 8 March 2021 from the Panel of Experts on Libya Established Pursuant to Resolution 1973 (2011) Addressed to the President of the Security Council* (United Nations, 2021), p. 17.

[5] Hitoshi Nasu, “The Kargu-2 Autonomous Attack Drone: Legal & Ethical Dimensions,” *Articles of War*, 10 June 2021, at https://lieber.westpoint.edu/kargu-2-autonomous-attack-drone-legal-ethical/.

[6] David Hambling, “Ukraine’s AI Drones Seek And Attack Russian Forces Without Human Oversight,” *Forbes*, 17 October 2023, at https://www.forbes.com/sites/davidhambling/2023/10/17/ukraines-ai-drones-seek-and-attack-russian-forces-without-human-oversight/?sh=2232100a66da (as of 20 January 2023).ロシア軍のAWSの使用状況は第3節参照

[7] ポール・シャーレ（伏見威蕃訳）『無人の兵団：AI、ロボット、自律型兵器と未来の戦争』（早川書房、2019年）168頁-170頁。

[8] Marco Sassóli, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems*

「CCW」）の締約国会議がAWSを議題に初めて開催され、2016年にかけて年次で非公式専門家会合が行われている。この会合は2017年から政府専門家会合（以下、「GGE」）に昇格して議論が続けられているが、米国、英国、ロシア、イスラエルなどの軍事大国によって議論の進展が遅らされたとされる[9]。

それでも、2019年のCCW締約国会合では今後の議論の指針が採択された。採択された報告書の付属書ⅢにおいてAWSの技術に関する指針が示され、(a)から(k)まで、11項目の指針が明らかにされている[10]。この指針の(b)項では「説明責任を機械に転嫁できないため、兵器の意思決定に対する人間の責任は保持されなければならない。これは、兵器システムのサイクル全体にわたって考慮されるべきである」と示され、また、(d)項では「CCWの枠組みにおけるいかなる新兵器システムの開発、配備、使用についても、適用される国際法に従い、責任ある人間の指揮命令系統の中での運用を含め、説明責任が確保されなければならない」とされ、AWSに関する人間の責任について初めて言及された。しかし、福井康人はこの指針の中で示された責任という文言は飽くまでも説明責任（Accountability）のことであり、法的責任（Responsibility）の意味よりも広い範囲を指す文言が用いられていることに留意しなければならないと述べている[11]。

こうした点について、2017年のGGEにおいてノルウェーはAWSによる国際人道法の違反に対する個人と国家の責任がなければ、誰も責任をとらないという状況が生起することが容易に想像でき、こうした潜在的に存在する「責任のギャップ」は国際法に深刻な結果をもたらすとの声明を発している[12]。また、このAWSの国際人道法の違反に対する人間の法上の責任に関して、ヒューマン・ライツ・ウォッチ（以下、「HRW」（Human Rights Watch））はAWSが引き起こす国際人道法上の違反はそれを使用する軍隊の指揮官に責任を負わせるべきと指摘しており[13]、各国やNGOなどからAWSの使用に対する責任の所在について様々な懸念や意見が出されているのが現状である。

この責任という言葉からは、国際法上、複数の概念が想起され得るが、AWSの使用における責任について、近年、国際刑事法の分野における複数の専門家によってAWSの使用の際に生起し得る戦争犯罪における刑事責任の観点から分析がなされ議論となっている。本稿でも、こうした議論を踏まえ、AWSによる戦争犯罪に対する個人の刑事責任を検討し、AWSの使用によって生じた戦争犯罪に対し、戦闘員たる個人が果たして責任を負うのかという点について検討している。

周知のとおり戦争犯罪はコアクライムの一つであり、国際刑事裁判所に関するロー

Arising in Warfare, Second Edition (Edward Elgar Publisher, 2024), p. 556.

[9] Ibid.

[10] United Nations, *Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects* (United Nations, 2019), p. 10.

[11] 福井康人「自律型致死性兵器システム（LAWS）規制の動向」『国際法法学会エキスパートコメント』No.2020-10、at https://jsil.jp/archives/expert/2020-10。

[12] United Nations, *CCW Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS): General statement by Norway* (United Nations, 2017).

[13] Human Rights Watch, "Losing Humanity: The Case against Killer Robots," *Human Rights Watch*, 19 November 2012, at https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots (as of 20 January 2024).

マ規程（以下、「ICC規程」）第8条においてその構成要件が明らかにされている。そして、同規程第30条では主観的要素の必要性が規定されており、ICC規程では、こうした客観的要素（actus reus）と主観的要素（mens rea）とが立証されてはじめて戦争犯罪が成立するとされている。

だが、AWSは従来の兵器とは異なり、AIによって自律的に戦闘を行う兵器であり、下記で示す先行研究の中には、AWSを使用して戦争犯罪が生起したとしても、戦争犯罪の責任を問うことができないとの主張が存在している。しかし、AWSの開発については未だ技術的な発展の余地があり、AWSによって生起した戦争犯罪に対する刑事責任を如何に扱うのかという点に関しては慎重な検討を要する。その一方で、ロシアとウクライナとの武力紛争などをみても、今後、各国がAWSを大量に導入して使用することが容易に想像でき、この問題に対する関連法規範の解釈を明らかにすることは急務である。こうした状況を踏まえ、本稿では、AWSの使用における戦争犯罪、とりわけICC規程上での戦争犯罪に関し、戦争犯罪に対する刑事責任を実際にAWSを使用する戦闘員に負わせることが果たして妥当なのかについて明らかにする。

最終的に本稿では、各国軍隊の軍事教範等を通じて、このAWSの犯した戦争犯罪に関する刑事責任は、AWSを取り扱う戦闘員に帰責することが上記規程第30条の解釈として導かれるとしている。この結論を導くため、下記において先行研究から問題認識を明らかにしたい。そこで本稿の主張と反対の立場の論者の主張を明らかにし、その反駁を通じて本稿の結論を明らかにする。

２．定義、構造、先行研究、問題認識

（１）AWSの定義、構造

AWSの定義について、専門家、NGO、国家の代表などの間で議論が交わされているが、 AWSの正確な定義に関する共通の合意はまだ得られていない[14]。だが、米国国防総省は、兵器システムにおける自律および半自律機能の開発と使用に関し、省の方針を確立し責任を割り当てるなどを目的として、2012年に国防総省指令3000.09を発出しており[15]、2023年にはこの指令を更新している[16]。この更新された指令において米国のAWSに対する認識が示され、AWSについて「一旦作動させれば、オペレーターによる更なる介入なしに標的を選択し交戦することができる兵器システム」と定義されている[17]。

この他にも、国連が公表しているCCW/GGE.1/2023/CRP.1では、CCWのGGEの中で各締約国が主張しているAWSの定義が列挙されている[18]。それによれば、オーストラリア、カナダ、日本、大韓民国、 英国、米国のグループはAWSについて

[14] Afonso Seixas-Nunes, *The Legality and Accountability of Autonomous Weapon Systems: A Humanitarian Law Perspective* (Cambridge University Press, 2022), p. 4.
[15] U.S. Department of Defense, *Department of Defense Directive 3000.09: Autonomy in Weapon Systems* (U.S. Department of Defense, 2012).
[16] U.S. Department of Defense, *DoD Directive 3000.09: Autonomy in Weapon Systems* (U.S. Department of Defense, 2023).
[17] Ibid., p. 21.
[18] United Nations, *Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects* (United Nations, 2023).

「いったん起動すれば、オペレーターの介入なしに標的を識別し、選択し、殺傷力をもって交戦することができる武器システムを含む、自律機能を備えた斬新でより洗練された武器」であるとの意見を提出している[19]。

また、ロシアはAWSについて「オペレーターによる遠隔操作、自律、またはこれらの組み合わせにより、タスクを実行するように設計された無人技術装備品」との意見を出している。中国はAWSには「5つの基本的特徴を含むべきであるが、これに限定されるものではない。第1は致死性であり…第2は自律性で、任務遂行の全過程において人間の介入や制御がないことを意味する。第3に、終了不可能性…第4に、無差別効果…第5に、進化、つまり、環境との相互作用を通じて、装置が自律的に学習し、人間の予想を超える形でその機能と能力を拡張することができる」ものを指すとの意見を出している[20]。この他にも様々な意見が各国から提出されており一致した定義はないが、各国の主張の基底には、優れたAIが自律的に作動して任務を遂行する兵器を念頭に置いている。こうした各国の定義を考慮し、本稿では、AWSに関する定義について共通認識を持つ必要から、諸国の見解をおおむね含み得る米国の定義に則って検討する。

次に、このAWSの構造に関しても共通認識を持つ必要から、一旦、ここで説明を加える。ティム・マクファーランド（Tim McFarland）によれば、AWSは二つの主要なコンポーネントから成り立っていると述べている。一つは軍事目標と交戦するシステムであり、もう一つは機械の挙動を直接制御するシステムであり、この後者の制御システムはさらに開発者が製作したプログラムに従って兵器やその他の装置を管理するハードウェアとソフトウェアから構成されるとしている。制御システムは、プログラムに従い、AWSに備えられているセンサーからの情報を処理し、兵器をはじめとした搭載機器を制御するための出力信号を生成し、軍事目標と交戦を行う[21]。AIはこの制御システムにプログラミングされており、情報処理を低遅延化させるために端末に情報処理を行わせるエッジAIコンピューティングが用いられているとされる[22]。

この制御システムにおける人間の関与の在り方として、ポール・シャーレ（Paul Scharre）は人間がシステムを制御する種類について分類している。それには、AWSがタスクを実行する際に人間のオペレーターの承認を待ってから実行する「ヒューマン・イン・ザ・ループ」、AWSが起動すると人間の監視下でタスクを実行し、人間のオペレーターが介入して動作を停止しない限りタスクを実行し続ける「ヒューマン・オン・ザ・ループ」、AWSがいったん起動すればタスクを実行し、人間のオペレーターはその活動を監督する能力を持たない「ヒューマン・アウト・オブ・ザ・ループ」の３つが存在している[23]とされる。

---

[19] Ibid., p. 2.
[20] Ibid., p. 7.
[21] Tim McFarland, *Autonomous Weapon Systems and the Law of Armed Conflict : Compatibility with International Humanitarian Law* (Cambridge University Press, 2020), pp. 31-34.
[22] "The Role Of AI Edge Computing In The Moral Dilemmas Of Drone Warfare," *Maris*, 5 March 2023, at https://www.maris-tech.com/blog/the-role-of-ai-edge-computing-in-the-moral-dilemmas-of-drone-warfare/.
[23] Paul Scharre, *Autonomous Weapons and Operational Risk* (Center of a New American Security, 2016), pp. 9-10.

そして、この「ヒューマン・アウト・オブ・ザ・ループ」に分類される既存の兵器には、イスラエルの「ハーピー」が存在する。これを開発したイスラエル・エアロスペース・インダストリー社はハーピーについて、打ち上げ前にプログラムされ、あらかじめ決められた「徘徊エリア」まで自律飛行し、そこで徘徊して標的を捜索し高い命中精度で命中させるものと説明している[24]。本稿では、上記で示した定義とも照らし、この「ヒューマン・アウト・オブ・ザ・ループ」と呼ばれる構造を持つ兵器をAWSとして検討する。

このように、国際社会においてAWSの定義について共通の認識がとれていない状況ではあるが、本稿においてAWSとは「一旦作動させれば、オペレーターによる更なる介入なしに標的を選択し交戦することができる兵器システム」のことであり、制御システムにAIがプログラミングされ、これが搭載機器を制御して交戦する構造を有する、「ヒューマン・アウト・オブ・ザ・ループ」と呼ばれる兵器であるとの認識に立って以下において分析をすすめる。

（２）先行研究、問題認識

上記ではAWSの定義と構造に関して共通認識を定めたが、このAWSを武力紛争で用いる場合、それを扱う軍隊は国際人道法の諸規則に従って使用する必要がある。AWSも人間の戦闘員と同様、国際人道法の条文を理解し、解釈して、実際の戦闘に適用しなければならないが、AWSがそれをどこまで行えるかについては意見が分かれる。

この点について、ロナルド・C・アーキン（Ronald C. Arkin）は、AWSが戦場で完璧に倫理的な行動を取れるとは思っていないが、人間の兵士よりも倫理的な行動を取ることができると述べている[25]。アーキンによれば、後の絶たない人間の戦闘員による戦争犯罪をAWSならば改善でき、戦場の恐怖に直面した人間の戦闘員に対して戦いのルールを守ることを期待するのは非現実的であり、文民が武力紛争で殺害されたりすることも[26]、AWSでは寧ろ考えにくいとしている。

アーキンは倫理的に殺傷力を行使できるAWSの研究をしてきたが、そのための第一の目標はAWSが国際人道法を戦場で遵守できるようにすることであり、その実現には複数の課題があるとしつつも、その開発の先に、文民の犠牲を減らす人道的に重要な成果を実現できるとしている[27]。アーキンは人間の戦闘員よりもAWSの方がより優れた倫理的判断を下すことができると期待しており、AWSの使用について肯定的である。

しかし、ノエル・E・シャーキー（Noel E. Sharkey）は、AWSが武力紛争において国際人道法を遵守して戦闘を行うことについて懐疑的な立場である。シャーキーによれば、優れたセンサーシステム、文民の定義のコード化、戦場における常識的推論などが欠けていることからAWSに区別原則を遵守させることは難しく[28]、ま

[24] IAI, “HARPY: Autonomous Weapon for All Weather,” *IAI*, at https://www.iai.co.il/p/harpy.
[25] Ronald C. Arkin, “The Case for Ethical Autonomy in Unmanned Systems,” *Journal of Military Ethics*, Vol. 9 (2010), p. 334.
[26] Ibid., p. 338.
[27] Ibid., p. 339.
[28] Noel E. Sharkey, “The Evitability of Autonomous Robot Warfare ,” *International Review of the Red Cross*, Vol. 94 (2012), pp. 788-789.

た、AWSは比例性を決定するための状況認識や主体性を持たないため比例原則も適切に判断することが期待できない[29]。さらに、AWSは道徳的であろうとなかろうと主体性を持たないためその行動に対して責任を問われることはなく、誤作動の責任を一体誰が負うのかという点が不明確である。明確な責任の所在なしにAWSを使用することは文民の命が危険にさらされることになるため[30]、AWSの使用を禁止することが倫理的に正しいとしている。

このように、AWSが国際人道法を遵守して武力紛争で戦闘を行うことができるのかについては意見が対立している。また、シャーキーが指摘したように、このAWSによる国際人道法の違反の責任を一体誰が負うのかについて、現代の国際人道法や国際刑事法では明確とはいい難い。

一般的に、軍隊の行為が国際人道法の違反に当たる場合、国際違法行為に対する国家の責任に関する条文第8条に照らし、その軍隊が所属している国家に国家責任が発生すると考えられる。また、国際法上における個人責任の拡大により、国際人道法上の違反行為、特に戦争犯罪に関してはそれを行った戦闘員やそれを指揮する指揮官に責任が帰責されることになると考えられる。だが、AWSの場合には軍事目標を発見して攻撃するまでの行動をすべてAIが判断して実行するため、果たして、個人に責任を帰責し得るのか、そして帰責される名宛人は誰なのかについて不明確となってしまう。

古谷修一は、「国際法に限らず、すべての法における責任制度は、行われた違反行為に対するサンクションという事後的矯正措置としての意味に加えて、違反行為を事前に防止する抑止的効果が期待される。ところが、集団としての国家に責任が問われる場合、実際の違反行為者としての個人への抑止効果はきわめて小さいのが実情である[31]」と述べており、現状におけるAWSの使用によって生じた戦争犯罪に対する個人責任が不明確な状況は、AWSの恣意的な使用を招き、国際人道法の違反行為の発生を助長させるおそれがある。

こうした懸念に関し、ロバート・スパロー（Robert Sparrow）はAWSによる国際人道法の違反の個人の責任の所在について検討をしている。スパローによれば、国際人道法の違反による責任の帰属は正戦論の基本的条件であり、とりわけ文民の死については誰かが責任を負わなければならない[32]としている。武器その他の戦闘の手段の性質上、それが引き起こす死傷者について責任を追及することが一般的に不可能である場合、それは国際人道法の重要な要件に反することになる。AWSの使用は誰も責任を取らないということが暗示され、国際人道法の条件に反することになる[33]との懸念を示している。

その上で、AWSのプログラマー[34]、AWSの配備を命じた軍隊の指揮官[35]、AWS自

[29] Ibid., pp. 789-790.
[30] Ibid., pp. 790-791.
[31] 古谷修一「国際法上の個人責任の拡大とその意義―国家責任法との関係を中心とし―」『世界法年報』第21号（2001年）101頁。
[32] Robert Sparrow, “Killer Robots,” *Journal of Applied Philosophy*, Vol. 24 (2007), p. 67.
[33] Ibid., p. 68.
[34] Ibid., pp. 69-70.
[35] Ibid., pp. 70-71.

体[36]など、いくつかの主体に責任を負わせることができないかを検討しているが、何れも責任の帰属主体として難しいと結論付けている。しかしそれでも責任は何者かが負わなければならないため、AWSをコントロールできなかった行為についてはその使用を命じた軍隊の指揮官などに責任を負わさざるを得ず、当分の間、AWSを導入することは、戦場における犠牲者にとっても、その使用に責任を負うことになる軍隊の指揮官にとっても不公平な状況をもたらすことになるとしている[37]。

他方で、このAWSの使用における個人の責任という点に関し、ヨルダン・グナワン（Yordan Gunawan）らは、ICC規程上の刑事責任の観点から考察している。グナワンらによれば、軍隊を構成する戦闘員や指揮官らに対してICC規程上の刑事責任を発生させるためには、主観的要素（mens rea）と客観的要素（physical elements（actus reus））の二つの要素の立証が含まれるとしている。主観的な要素はICC規程第30条に定められた要件を満たさなければならず、一方、客観的な要素は犯した行為が犯罪の構成要件を満たしていなければならない。そして、個人に両要素が満たされていると証明されれば、その個人に有責性が認められる。武力紛争の当事者である戦闘員は、戦闘の手段および方法を禁止または制限する規定を含む国際人道法の諸規則を遵守しなければならないが、戦闘員がAWSの運用が国際人道法の規定に違反することを認識していた場合、戦闘員はAWSの使用について責任を問われる可能性がある。加えて、AWSの運用が国際人道法の規定に違反する場合、指揮官も責任を問われる可能性がある[38]としている。

上記した通り、ICC規程では戦争犯罪の成立のためには客観的な行為の存在とともに主観的要素が必要である。そして、ICC規程上、戦争犯罪の処罰は故意犯のみを対象としていることから、AWSの行った戦争犯罪に対する個人の刑事責任が生ずることとは、その犯罪における個人の故意が立証されるかどうかである。必要となる個人の主観的な要素について、ICC規程第30条に規定されており以下の通りである。

> 1　いずれの者も、別段の定めがある場合を除くほか、故意に及び認識して客観的な要素を実行する場合にのみ、裁判所の管轄権の範囲内にある犯罪について刑事上の責任を有し、かつ、刑罰を科される。
> 2　この条の規程の適用上、次の場合には、個人に故意があるものとする。
> (a)　行為に関しては、当該個人がその行為を行うことを意図している場合
> (b)　結果に関しては、当該個人がその結果を生じさせることを意図しており、又は通常の成り行きにおいてその結果が生ずることを意識している場合
> 3　この条の規程の適用上、「認識」とは、ある状況が存在し、又は通常の成り行きにおいてある結果が生ずることを意識していることをいう。「知

[36] Ibid., pp. 71-73.
[37] Ibid., pp. 74-75.
[38] Yordan Gunawan, Muhamad Haris Aulawi, Rizaldy Anggriawan and Tri Anggoro Putro, "Command Responsibility of Autonomous Weapons under International Humanitarian Law," *Cogent Social Sciences*, Vol. 8 (2022), p. 8.

っている」及び「知って」は、この意味に従って解釈するものとする。

ICC規程では、故意と認識をもって客観的に戦争犯罪に当たる行為を行った場合に刑事責任が発生すると定められていることから、AWSの使用によって戦闘員たる個人に責任が生じるということとは、AWSを使用する際、戦争犯罪が高い確率で発生することを認識しながらAWSを実際に使用し、その結果、戦争犯罪が発生した場合であり、このような場合にはじめて戦闘員には故意犯が成立し処罰の対象となる。

だが、トーマス・ヴァイゲント（Thomas Weigend）は戦闘員に対しAWSが起こした戦争犯罪の責任を負わせることについて懐疑的立場である。ヴァイゲントによれば、ICC規程の下で個人に対してAWSの使用によって引き起こされた国際人道法の違反による戦争犯罪が認められるためには、ICC規程第30条第2項(b)に規定されている「通常の成り行きにおいてその結果が生じることを意識している」ことが必要とされる。だがそれは、AWSを運用する者が、AWSが通常の過程で誤作動を起こし、被保護者がAWSによって殺害されると考えていた場合にのみ責任を問われることを意味する例外的な場合に限られるとし[39]、戦闘員に個人責任を帰責させることについて難色を示している。

また、ヴァイゲントは指揮官責任に関しても検討しており、ICC規程第28条(a)(i)で規定されている、軍隊が犯罪を行うことを「知っているべきだった」という基準を指揮官に対して適用した場合、指揮官がAWSの誤作動について予見できた場合にその責任を問えるが、しかし、自律的機能ゆえに抽象的な危険を内在するAWSの使用を認めると同時に、一般的に予見可能な危険が現実化した場合に指揮官に刑事責任を問うことは、法として矛盾することになる。この問題を解決するため、法は指揮官の責任を指揮官がAWSに関連する特定の具体的な危険を予見できた場合に限定しなければならないとしている[40]。

そして、AWSがプログラムから逸脱し、保護される人や物に危害を与えた場合、通常、その運用者は、危害を防ぐことができ、実際にそのような事態が起こることを予見していたか、少なくともその発生について無謀であった場合にのみ、刑事責任を問われ、それ以外の場合はいかなる人間による行為も処罰の対象とはならないと結論付けている[41]。

ヴァイゲントは、該当するICC規程の条文に照らし、AWSが引き起こした国際人道法の違反を戦闘員や指揮官個人に帰責させるためには、具体的にAWSが違反行為を引き起こすことを予見していたことが個人の主観には必要であると述べ、もし合理的な予防措置が講じられているにもかかわらず先進的なAWSが暴走しあらゆる安全策を無視するようなことがあれば、それはAIに内在するリスクであり、こうしたAWSの致命的な誤動作という事態が発生した場合、個人に刑事責任を問えないとい

[39] Thomas Weigend, "Convicting Autonomous Weapons?: Criminal Responsibility of and for AWS under International Law," *Journal of International Criminal Justice*, Vol. 21 (2023), p. 1150.
[40] Ibid., pp. 1151-1152.
[41] Ibid., p. 1153.

う事実を受け入れるべきであるとしている[42]。

このようにヴァイゲントは、AWSの使用により客観的に戦争犯罪が生起したとしても、主観的要素の問題からその刑事責任を戦闘員やその指揮官に帰責させるのは難しいとしている。上記したとおり、ICC規程上の戦争犯罪は、客観的な構成要件はもちろんのこと、主観的要素を求めている。しかし、AWSによる軍事目標に対する攻撃の決定は、搭載されたAIの判断に任されており、AIのアルゴリズムに基づく判断に戦闘員が介在していない以上、生起した戦争犯罪に対する主観的要素を戦闘員に対して糾すことは難しいのではないかと考えられる。

しかし、ヴァイゲントは、「AWSを運用する者が、AWSが通常の過程で誤作動を起こし、被保護者がAWSによって殺害されると考えていた場合」には戦闘員に対する刑事責任の発生について認めている。このことは、通常の使用におけるAWSの誤作動の多寡から戦闘員の主観における戦争犯罪の予見可能性を相関的に推測することが可能であり、一般的にAWSの誤作動が多い場合には戦闘員の故意が推定されることになり得るため、AWSの引き起こした戦争犯罪の刑事責任を戦闘員に課すことが可能であると考えることができる。

言葉を換えると、戦闘員の刑事責任の有無は、ヴァイゲントが先進的なAIに伴う内在的なリスクと述べたこのリスクをどう評価するのかということになる。ヴァイゲントは特段の論拠を付さずにAWSに搭載されたAIが「先進的」であるため、AWSによる戦争犯罪に対する責任を戦闘員に課すことに否定的である。しかし果たして、このAWSに内在するリスクはどの程度のものなのか、具体的な分析を踏まえなければ、「先進的」の言葉の意味も不明瞭のままである。高いリスクを有することを知りながらAWSを使用し戦争犯罪が生起した場合、AWSを使用した戦闘員の主観には戦争犯罪の故意が疑われるのではないか。

こうしたことを踏まえ問題認識を明らかにすると、本稿における問題認識とは、ICC規程第30条第2項に規定されているとおり、「その行為を行うことを意図」し「通常の成り行きにおいてその結果が生ずることを意識している場合」にICC規程上の故意が存在すると一般的に解釈されるが、現代において、戦闘員がAWSを使用し戦争犯罪を発生させた場合にも、その戦闘員の主観的要素に故意を認めることが解釈として妥当なのかということになる。この際、戦闘員の故意の存在を推定させる要素は、上記の検討を踏まえると、AWSに搭載されるAIの持つリスクの多寡といえる。そうなると、AWSのリスクとは一体何を指しているのかが不明瞭となることから、AWSの構造に一度着目してみる必要がある。

マクファーランドによれば、AWSに搭載された制御システムは、センサーからの情報を処理し、兵器をはじめとした搭載機器を制御するための出力信号を生成し、軍事目標と交戦を行うと明らかにしていた。AWSが国際人道法に基づき攻撃をするためには、センサーから入手される情報から軍事目標か否かをAIが正確に区別することが必要であるとともに、特定した軍事目標に攻撃する場合、比例原則を適切に適用することが必要であると考えられる。こうしたことができなければ、AWSは無差別攻撃を行う可能性が高く、これを知って使用する戦闘員には、AWSが戦争犯罪

[42] Ibid., p. 1154.

を行う高い可能性があると認識している―それゆえ、故意がある―ことが推定される。このため、ヴァイゲントが述べたリスクとは、AWSが正確に目標を区別することができるのか、適切に比例原則を適用できるのか、という点に具体化される。

AWSの使用における高いリスクを知りながらこれを使用して戦争犯罪が行われれば、AWSを使用した戦闘員はその行為と結果に対して、ICC規程上の戦争犯罪の故意があったと疑われるだろう。このため、AWSが果たしてどの程度のリスクがあるのか次節において分析する。そこでの検討を通じ、AWSにより生起した戦争犯罪の責任を戦闘員に問うことが果たして妥当なのかという点について本稿の結論へと導きたい。本稿では、上記したとおり、ヴァイゲンドが主張する「先進的なAWSが暴走しあらゆる安全策を無視するようなことがあれば、それはAIに内在するリスクであり、こうしたAWSの致命的な誤動作という事態が発生した場合、個人に刑事責任を問えない」との主張に対し、以下の考察を通じて反駁をする。

３．AWSのリスクと戦闘員の認識

マルコ・サッソーリ（Marco Sassóli）は、人間と同等に国際人道法を適用して行動するAWSの開発に関し、敵対行為で起こりうる多種多様な状況に適応するために必要な文脈を理解する知性を備えたマシンを作ることについて懐疑的である[43]。AWSが武力紛争という複雑な状況において国際人道法を適用して行動することができるのかという点に対してこうした懐疑的意見は多い。

シャーレは、「AIシステムは、あるタスクに対しては超人的な性能を示すかもしれないが、タスクの条件や環境が少しでも変われば、AIシステムの性能は劇的に低下する。この汎用性の低さは、今日のAIの大きな限界であり、さまざまなAIシステムで何度も出てくる[44]」と述べ、「各国は、十分に危険性を理解していないAIシステムを実戦配備するおそれがあり、事故が起こりやすいかもしれない」としている。米国の国防高等研究計画局（DARPA）は、複雑な都市環境において人を識別することを目的に、 AIを用いた物体認識アルゴリズムを開発したが、段ボール箱に隠れた人間や、木に変装したりする人間を検知することができず、人間なら簡単に見破れるような単純なトリックが、アルゴリズムを破るには十分であったとされる[45]。

シャーレによれば「あらかじめ学習した以外の状況にAIが直面した場合、突然予期せぬ故障を引き起こす可能性があり、さらに、AIの技術者自身が、AIシステムの動作の限界を前もって知らないことも」あると述べ、「何億ものパラメーターを持つニューラルネットなど、現代のシステムは非常に複雑である。AIシステムが複雑であるということは、時として驚くべき挙動を示すことを意味する…機械学習システムでは、欠陥のある学習データや誤った目標設定など、学習プロセスの複数の段階で障害が発生する可能性がある」とし[46]、AWSに使用されるAIの学習における誤りが人間に予測し得ない障害を引き起こす可能性があることを認めている。

---

[43] Marco Sassóli, “Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified.” *International Law Studies*, Vol. 90 (2014), pp. 312-313.
[44] Paul Scharre, *Four Battle Grounds* (W. W. Notion & Company, 2024), p. 230.
[45] Ibid., p. 231.
[46] Ibid., p. 232.

このような危険性を指摘しているのはシャーレだけでない。国連軍縮研究所も、AWSに入力されるデータ上の問題により予期しないエラーが発生するおそれがあることを指摘している。それによれば、AWSはその活動を収集したデータに依存しているが、不完全なデータ、低品質なデータ、不正確なデータ、虚偽のデータ、不一致のデータ（システムが設計したデータと異なるデータ）によって予期しない問題が発生する可能性が存在しており、すべてのAWSは、その使用期間中、データに対する脆弱性を持つ[47]ことを明らかにしている。

こうした、データに対するすべてのAWSの脆弱性とそれが引き起こす誤作動について人間は不可知ならざるを得ない。しかし、AWSの合法的使用に必要な包括的で文脈に基づいた人間の判断を実現するためには、AWSにとって意図しないデータを予測し、それに対応する能力が必要とされるものの、一体それが何であるかについて現在のテストやリスク評価手段では実現できない。その一方、こうした問題の発生は性質上避けられないもので、AWSを扱う者はこうした問題に対処する必要があり、そうしなかったことに起因する損害について責任を問われる可能性があると同研究所は指摘している[48]。

このように、AWSに搭載されるAIはデータに依存するが、用いられるデータは適不適様々であり、これが時としてAWSに予測不可能な行動を引き起こす。また、AWSは武力紛争において国際人道法に基づき使用されなければならないが、紛争の複雑な状況の中から適切に対処し得る能力や、その能力を構築する技術も現状では難しい。このため、AWSの使用には常に人間にとって予測不可能な誤作動がつきまとい、その誤作動により国際人道法では禁止されている様なことも起こり得ると考えられる。実際に近年の武力紛争では、そこで使用されているAWSによって文民や民用物に対する攻撃がなされている事例が報告されている。

2020年9月にアゼルバイジャンとアルメニアの間でいわゆる第2次ナゴルノ・カラバフ紛争が勃発したが、アルツァフ人権オンブズマン（The Republic of Artsakh Human Rights Ombudsman）によれば、この武力紛争においてアゼルバイジャン軍は無人機を使用して無差別攻撃を行ったとされる[49]。使用された無人機の中には、上記で説明したイスラエルのハーピーが含まれており、こうしたAWSによってアルメニア側の文民や民用物に被害が及んだことが明らかにされている[50]。報告では、人口密度の高い都市の文民の居住地が攻撃を受けている[51]ことが明らかにされ、同オンブズマンはアゼルバイジャン軍によって文民が殺害されるなどの戦争犯罪が引き起こされたと主張している。

こうした状況は、2022年に始まったロシアとウクライナとの武力紛争においても同様である。この武力紛争において、ロシア軍はオルラン-10（Orlan-10）やクブラ

[47] Holland Michel, *Known Unknowns: Data Issues and Military Autonomous Systems* (UNIDIR, 2021), p. 3.
[48] Ibid., p. 12.
[49] The Republic of Artsakh Human Rights Ombudsman, *Second Interim Report on the Azerbaijani Atrocities against Artsakh Population in September-October 2020* (The Republic of Artsakh Human Rights Ombudsman, 2020), p. 3.
[50] Ibid., p. 25.
[51] Ibid.

（KUB-BLA）といったAWSを使用している[52]。また、ロシアはイランからシャヘド-136（Shahed-136）と呼ばれるAWSを輸入し、こうした兵器もまた実戦に投入している[53]。マーク・カーステン（Mark Kersten）は、ウクライナにおけるロシア軍のAWSの使用について調査しており、ロシア軍のAWSの攻撃により、ウクライナ側の病院が攻撃され多くの文民が被害を受けていると主張している[54]。また、こうした状況についてウクライナは国連の安全保障理事会において、ロシアのAWSが文民や民用物を攻撃しており、ウクライナの人口密集地域や重要インフラに対する攻撃手段として使用していることを明らかにしている[55]。

この他にも、2023年10月7日にハマスによる大規模攻撃で始まったイスラエルとハマスとのガザ地区における紛争において、AWSによる文民の被害が欧州地中海人権モニター（Euro-Mediterranean Human Rights Monitor）により報告されている。報告によれば、イスラエル軍はラニウス（LANIUS）と呼ばれるAWSを使用してハマスを攻撃しているとされる[56]。

このラニウスについては、都市環境での短距離作戦用に設計された高い操縦性と汎用性を持つドローン型の徘徊弾薬であるとの説明がウェブ上で明らかにされている。説明では「自律制御のためのカメラおよびフライトコンピュータとインターフェースする内蔵型のコンパニオンコンピュータを搭載し…ユーザーの介入なしに、完全な飛行経路の分析、離陸、航行、偵察を実行することができ」、「自律的に人を識別」し「脅威となる可能性のある武装した者と非武装の文民を区別することができる」とされている[57]。しかし、同モニターが実施した調査によると、イスラエル軍がこうしたAWSを含めたドローンなどを使用して何百人ものパレスチナ文民を殺傷していることが明らかにされており、実際のAWSの使用において、客観的に戦争犯罪に抵触するようなおそれがある事実が生起することがあり得るということが分かる[58]。

こうした3つの武力紛争の事例におけるAWSの使用状況を見ると、何れの事例においても客観的には戦争犯罪と疑われるような事案が発生しており、実際、こうした事例を報告している団体はAWSによる戦争犯罪が発生していると訴えている。しかし、

---

[52] Zachary Kallenborn, “Seven (Initial) Drone Warfare Lessons from Ukrine,” *Modern War Institute at West Point*, 5 December 2022, at https://mwi.westpoint.edu/seven-initial-drone-warfare-lessons-from-ukraine/.
[53] Daniel Boffey, “Revealed: Europe’s role in the making of Russia killer drones,” The Guardian, 27 September 2023, at https://www.theguardian.com/world/2023/sep/27/revealed-europes-role-in-the-making-of-russia-killer-drones.
[54] Mark Kersten, “A War Crime Coalition: Russia’s Iranian and Chinese Drones Target Ukrainian Civilians,” *Justice in Conflict*, 22 February 2023, at https://justiceinconflict.org/2023/02/22/a-war-crime-coalition-russias-iranian-and-chinese-drones-target-ukrainian-civilians/.
[55] Permanent Mission of Ukraine to the United Nations in New York, “Statement by the Permanent Representative of Ukraine, Ambassador Sergiy Kyslytsya at the UN Security Council meeting on “Non-proliferation” (6 July 2023),” *Permanent Mission of Ukraine to the United Nations in New York*, 6 July 2023, at https://ukraineun.org/en/press-center/628-statement-by-the-permanent-representative-.
[56] Euro-Mediterranean Human Rights Monitor, “Gaza: Israel systematically uses quadcopters to kill Palestinians from a close distance,” *Euro-Mediterranean Human Rights Monitor*, 19 February 2024, at https://euromedmonitor.org/en/article/6166/Gaza:-Israel-systematically-uses-quadcopters-to-kill-Palestinians-from-a-close-distance.
[57] Automated Decision Research, “Elbit Systems LANIUS loitering munition,” *Automated Decision Research*, at https://automatedresearch.org/weapon/elbit-systems-lanius-loitering-munition/.
[58] Euro-Mediterranean Human Rights Monitor, *supra* note 56.

こうした文民や民用物を対象とした攻撃が発生したとしても、実際には、AWSに搭載されたAIが区別原則、比例原則、予防原則といった国際人道法の諸原則を遵守した結果であったならば、その攻撃の結果を戦争犯罪と結びつけることは尚早である。ある場合には、敵対行為に直接参加する文民に対して攻撃を実施した可能性があり、ある場合には、比例原則に従った結果、付随的損害として文民を巻き込むかたちで攻撃を実施した可能性がある。

だが、エリオット・ウィンター（Elliot Winter）によれば、AWSが区別原則を遵守することは現時点では難しいとされる。確かにAIにはある特定の物事を観察し認識する点においては、人間と同等の能力があることは疑いないが[59]、しかし、AIによる観察や認識が進んでいるにもかかわらず、AIの判断力は人間に遅れをとっているのが現状とされる。国際人道法では、区別原則の適用をするにあたって、文脈における判断が重要であり、観察と認識だけからでは間違いなく戦闘員に分類される者でも、捕虜、降伏、無力化等になった場合は攻撃対象とならない場合があり、通常、人間が解釈できる文脈上の考慮事項が、AIにとっては難しいと考えられる[60]。また、比例原則の適用に関しては、攻撃によって引き起こされる付随的損害と得られる軍事的利益とを比較する場合、米国で使われている評価方法を使用すれば、AIでも比較可能な値に定量化することが可能であるとしつつも、しかし、これを行うには複雑なプロセスを経る必要があり、高い知能を備えたAIが必要とされる[61]。

ウィンターは、国際人道法の原則である区別、比例、予防原則をAIに遵守させるためにはAIのレベルが高度化されている必要があるが、現状ではそのレベルに至っておらず、現代のAIには状況に応じた判断を下すことができないと述べている。また、技術進歩によっていずれAWSは国際人道法に準拠できるようになるだろうが、それには数十年程度の時間が必要になる可能性を示している[62]。

こうした検討を踏まえると、上記の事例で挙げた、AWSが自律的に攻撃を実施し文民や民用物を殺傷、破壊している場合、現状ではこれらの攻撃は無差別攻撃であった可能性が高い。国連軍縮研究所も、「未知の故障から損害が生じた場合、行為者はそのような故障のリスクを考慮に入れなかった責任を合理的に問われることはない。システムの脆弱性が真に予見できないものであった場合、人間の意思決定者が、そのシステムの脆弱性にもかかわらずシステムを使用することに無謀さや故意の意図があったことを証明することは不可能であろう」[63]としているが、しかし、すべてのAWSは「そのシステムの試験と調査では特定できなかった不具合を使用中に示す。この事実自体が、意図しない危害が回避できるかどうかを疑う合理的な根拠となりうる。…このように定量化はされていないものの、誤作動の疑念が存在しているにもかかわらず、AWSを取得し使用するという決定を下す場合、その結果生じる予期せぬ損害について、当事者に責任を負わせる可能性がある」[64]と述べており、AWSが予期しない不

[59] Elliot Winter, "The Compatibility of Autonomous Weapons with the Principles of International Humanitarian Law," *Journal of Conflict & Security Law,* Vol. 27 (2022). pp. 13-14.
[60] Ibid., p. 14.
[61] Ibid., pp. 16-17.
[62] Ibid., p. 20.
[63] Michel, *supra* note 47, p. 16.
[64] Ibid., p. 17.

具合を示すことを知りながら使用し、戦争犯罪を引き起こした場合、それに対する責任について戦闘員に帰責し得る可能性が生じることを示唆している。

では、戦闘員はどの程度、使用するAWSの不具合について知り得ると考えられるのだろうか。この点について、米陸軍教範の『ADP7-0』には、「部隊は、人員、装備、システムを戦闘中に維持するための訓練を行う。人員を戦闘中に維持するために、指揮官は部下を訓練して部隊の結束と士気を維持し、兵士の健康と福祉を常に監視する。指揮官は、武器、車両、装備などを保守するための要領も訓練に含め、それらが使用可能で常に任務に即応できる状態になるようにする。指揮官は、通信やデジタルシステムなどの複雑なシステムも、高い即応性を維持して使用可能になるように訓練する。指揮官は、部隊があらゆる状況下で保守を行い、長期間にわたり、かなりの距離にわたって最大かつ効果的な戦闘力を維持できるようにする」と述べられている[65]。一般的に、米軍のみならず通常軍隊であればこのような訓練を日頃から戦闘員に対して施していると考えることができる。

また、英陸軍教範の『陸上作戦（Land Operations）』では、「兵士は個々に、または、部隊の一員として、特定の役割に応じた訓練を受ける…一度部隊に配属されると、兵士たちはこの訓練手順を通じて、他兵科や他軍種だけでなく、同盟国との相互運用性も高めていくことになる。この継続的な訓練は、個人訓練と部隊訓練に大別され…戦術・戦闘技術・戦闘方法の新たな導入や新装備の活用といった適応の一環」であるとしている[66]。そして、「陸上部隊の戦闘力の基盤は人にあるため、訓練はまず個人を中心に設計される。教育と密接に関わる個人訓練は、兵士として作戦任務を遂行するための基本技能、専門技能の実地運用、そして部隊の一員として機能する力を提供する。身体錬成、射撃、野外行動の技能は全ての兵士にとっての戦闘技術の基礎であるが、これだけでは現代の作戦には不十分である。現代戦では、情報にアクセスし活用する能力、同盟国やパートナー、その他の作戦地域に関与する主体と効果的に通信・協力する能力など、さらなる技能が求められる。個人訓練は採用後に開始され、その後の軍歴を通じて継続される。この訓練は、兵科・職種ごとの専門技能を積み重ねるものであり、軍事技能の維持と発展には不可欠である。技能は実施しなければすぐに失われるためである。個人訓練は指揮官の最も基本的な責務の一つであり、年次の技能検定の実施などを通じて、基準が維持されていることを確認しなければならない」とされる[67]。このように、戦闘員は軍隊に入隊以降、継続的に訓練を実施し、装備品の取り扱いに習熟することが予想される。

この点について、米陸軍の公式ウェブサイトに掲載された「兵士の能力向上：陸軍訓練における非効率性の改善」では、射撃訓練の非効率性が兵士の装備品操作能力に影響を与えていると指摘している。ここでは、特に兵士の大多数が基本的な射撃評価に合格できない現状が報告されているが、その報告の中で、訓練と装備品の取り扱い習熟度の間に強い相関関係が存在することが述べられている[68]。つまり、軍隊が戦闘

[65] U.S. Army, *ADP7-0* (U.S. Army, 2024), p. 11.
[66] British Ministry of Defence, *Land Operations* (British Ministry of Defence, 2017), pp. 3-13-3-14.
[67] Ibid., p. 3-14.
[68] Alexander Roysden, "Enhancing Soldier Proficiency: Addressing Inefficiencies in Army Training," *U.S. Army*, 22 May 2024, at https://www.army.mil/article/276569/enhancing_soldier_proficiency_addressing_inefficiencies_in_arm

員に訓練を施し、戦闘員がその過程を通じて取り扱う装備品に関する理解を深めると考えることは合理的といえる。同様に、AWSを取り扱う戦闘員もこうした訓練を通じてAWSに関する理解を深めることになるといえる。AWSがどの程度の正確に目標を攻撃するのか、どの程度の誤射、誤爆などが生起するのか、公算誤差はどの程度なのか、破片がどの程度四散するのかなどについて訓練を通じて理解することになる。また、AWSの取り扱いに関する教範なども整備されると考えられる。

こうした事情を踏まえて、旧ユーゴスラビアのための国際刑事裁判所（以下、「ICTY」）において裁判が行われた検察官対ミラン・マルティッチ（Prosecutor v. Milan Martic）について一度想起する必要があると思われる。この裁判では、1991年より始まった旧ユーゴスラビア内戦においてセルビア人勢力が一方的に樹立した「セルビア人クライナ共和国」（Republika Srpska Krajina、RSK）の軍事組織に所属していたミラン・マルティッチ（Milan Martić）が、1995年5月2日と3日に、クロアチアの首都ザグレブに対してM-87オルカン多連装ロケットシステムを使用して攻撃し、文民7人が死亡、200人以上が負傷したザグレブ砲撃事件が訴因の一つとして告発されている[69]。ICTYは、砲撃に使用されたM-87オルカン多連装ロケットシステムの射距離（公算誤差）とクラスター兵器の特性に注目し、当時の状況における砲撃では、特定の目標を攻撃することは不可能であったと結論づけた。裁判所はまた、M-87オルカン多連装ロケットシステムは無差別兵器であり、ザグレブのような人口密集した地域で使用すれば、深刻な死傷者を出すことになると判断している[70]。この判断は第1審のものであるが、マルティッチは控訴審においてもザグレブ砲撃事件について有罪と認められ、禁錮35年の量刑が言い渡されている。軍隊間だけの戦闘ならば、こうした兵器の使用は軍事的には有効であろうが、その手段を誤った方法で用いた場合、使用した戦闘員に戦争犯罪の責任が帰責され得る。

上記までの考察をまとめると、現代のAWSは未だ発展途上と考えられ、区別原則や比例原則について遵守できるのかは難しいと考えられる。こうしたAWSの性能について、戦闘員は訓練を通じて理解すると考えることが合理的である。そして、兵器の使用にあたってその性能上、軍事目標を特定できない攻撃は、無差別攻撃と見なされ戦争犯罪と認められる可能性がある。たとえ戦闘の手段がAWSであったとしても、戦闘の方法次第では戦争犯罪と認められる可能性がある。AWSを取り扱う戦闘員が、人口密集地域や、軍事目標付近に多数の文民や民用物があるにも関わらず、それを知りながらAWSを使用し、文民や民用物に過度な被害を発生させた場合、その無差別攻撃の責任について、AIに内在するリスクとして還元するのはやや飛躍めいてはいないだろうか。

寧ろ、こうした条件が揃えば、AWSを用いて戦争犯罪が生起した場合、その戦争犯罪の責任について戦闘員に帰責される可能性が生じると考える方が合理的である。今日のAIの技術水準の下で製造されたAWSを使用して戦争犯罪が発生した場合、それを使用した戦闘員には戦争犯罪に対する故意が推定されることが―ヴァイゲントは例外としていたが―寧ろ原則的と考えることが妥当と言えるのではないだろうか。

---

y_training.

[69] *Prosecutor v. Milan Martić*, *Trial Judgement*, IT-95-11, 12 June 2007, Paras. 302-323.

[70] Ibid., para. 463.

それでも、戦闘員の主観的要素に関し、どの程度詳細にAWSが不具合を起こしそれによって戦争犯罪が発生するのかについて認識をしていたのかということについては、当然のことながらよくよく吟味する必要がある。相当程度具体的に戦争犯罪が発生することを認識しながらAWSを使用した場合、戦闘員に対して直接的故意を認めることは容易である。他方、こうした犯罪事実の確定的な認識・予見はないが、その蓋然性を認識・予見している場合、未必の故意の問題となる[71]。ICCの予審裁判部はこの未必の故意について、ICC規程の下では犯罪を生じさせないと確認しており、ICC規程第30条は、刑事責任の成立には最低限、犯罪の結果が意識されている必要があることを明確にしている[72]。このため、こうした未必の故意の心理状態で行われた場合には主観的要素を充足し難く、ICC規定上、戦争犯罪について戦闘員に対して責任を問うことは難しい。

このように本節における検討をまとめると、現在のAWSに区別原則や比例原則を遵守させて使用することは難しく、AWSにより戦争犯罪が発生する可能性は現状では未だ高いと考えられる。また、これを扱う戦闘員は普段の訓練を通じてAWSによる戦争犯罪の発生の可能性について理解することになると考えられる。こうした理解の下、AWSを人口密集地域などで使用した場合、AWSによる無差別攻撃が生起する可能性について戦闘員の認識に存在していたと考えることは不合理とはいえない。このことから、ICC規程第30条第2項に規定されている、「その行為を行うことを意図」し「通常の成り行きにおいてその結果が生ずることを意識している場合」にICC規程上の故意が存在するとの規定に関して、現状においてAWSを使用して戦争犯罪が発生した場合、その戦闘の方法如何によっては、戦闘員はAWSによる戦争犯罪が高い可能性で起こり得ることを知っていながらAWSを使用し戦争犯罪を発生させたと考えることが合理的であり、このため、戦闘員の主観的要素に故意があったと解釈することができると思われる。しかしその一方、戦争犯罪の発生について、戦闘員が確定的に認識しておらず、戦争犯罪の発生を単なる可能性とまでしか認識していなかった場合、ICC規程では主観的要素に未必の故意は認められないことから、その責任を戦闘員に帰責させることは難しいと考えられる。

もっとも、ICTYなどのアドホックな国際刑事裁判所では、この未必の故意でも犯罪が成立することを認めている場合があり[73]、また、日本をはじめとした複数の国の国内刑法でも未必の故意を認めている場合がある[74]。ICCがそもそも補完的役割を前提としていることを考えれば[75]、AWSを使用して戦争犯罪が発生した場合、アドホックな国際刑事裁判所や国内刑法の例をみても、戦闘員にその責任を帰責させる可能性は決して少ないものとはいえないだろう。

４．おわりに

AWSを使用して戦争犯罪が発生した場合、その責任を誰が負うべきなのかについ

---

[71] 山口厚『刑法〔第3版〕』（有斐閣、2015年）110頁-111頁。
[72] 佐藤宏美『国際刑事法の複層構造』（有信堂、2024年）51頁。
[73] *Prosecutor v. Dusko Tadic, Appeal Judgement*, IT-94-1-A, 15 July 1999, para. 220.
[74] 佐藤『前掲書』（注70）137頁。
[75] 同上、109頁。

て、先行研究において様々な意見に分かれているのが現状である。こうした中、各国の軍隊はAWSの開発を進めており、将来の武力紛争においてAWSが大量に使用される可能性は高い。しかし、AWSの使用には常に誤作動の危険性が伴い、それによる戦争犯罪の発生があり得る。こうした危険性がありながら、ヴァイゲントのように単にAIに内在するリスクとして受け入れることは、疎放に本来の人間の責任を見過ごすことを許してしまうことになり得る。それは、AWSの恣意的な使用を許し、ひいては国際人道法や国際刑事法の内容を形骸化させることにもつながるおそれがある。本稿では、この点に関し、ヴァイゲントの主張への反駁を通じて、戦闘員個人に刑事責任がなお追及される可能性があることを明らかにした。

ICC規程上、AWSによる戦争犯罪の発生に対する戦闘員の有責性は、戦闘員が戦争犯罪の行為と結果を認識していた場合に限られる。これには未必の故意が含まれず、単なる戦争犯罪の発生の可能性だけでは犯罪成立の要件を充足できない。このため、AWSによる戦争犯罪に対する戦闘員の責任を明らかにするためには、他の戦争犯罪の場合と同様に、刑事手続きに基づき戦闘員の認識を個別具体的に精査し、AWSの性能や戦闘員のAWSの理解の程度、AWS使用時における戦闘員の状況認識などについて一つ一つ該非を明らかにしていく必要がある。このように、現代において、たとえAWSが使用される場合であったとしても、刑事責任は当事者となる戦闘員に問われることになる可能性が存在している。

そしてまた、指揮官責任について本稿では議論に触れなかったが、こうした責任の有無も同時に問われる可能性が生ずることになる。