【特集：安全保障関連技術】

人工知能の防衛装備品への適用における課題
―特に機械学習について―

航空研究センター運用理論研究室
2等空佐　上髙原　賢志

本稿は、人工知能学会倫理委員会主催『セミナーシリーズ「AIと安全保障」』第3回「AIと安全保障技術と政策」（2019年6月2日実施）において発表した内容を大幅に加筆修正したものである。

はじめに

昨今、「人工知能」という言葉を耳にしない日はほとんど無い。人工知能はその言葉そのものがすでに一般化している。様々な製品やその機能が「人工知能を採用することで能力が向上した。」とか、「人工知能によって実現した。」といった表現を頻繁に目にする。しかし、人工知能は決して新しい技術ではない。コンピュータが出現してから、言語理解や推論、問題解決といった人間の脳活動をコンピュータで実現しようと、これまで多くの科学者及び技術者が取り組んできた。人工知能研究は1950年代から始まった。研究目標が非常に華々しかったことから、多くの研究者が取り組みブームとなったが、研究目標と当時の技術レベルがあまりにも乖離していたことから、ブームは徐々に衰え、いわゆる冬の時代に突入した。人工知能はこれまで2回のブームと冬の時代を経験し、現在は第3次ブームと言われている[1]。

2000年代から始まった第3次ブームでは、ビッグデータと呼ばれる大量のデータを用いて、人工知能が自ら学習する「機械学習」が実用化された。また、ニューラルネットワークを深化させた「ディープラーニング（深層学習）」の登場により、データの特徴量を人工知能が自ら見つけることが可能となり、飛躍的に能力が向上した。

防衛省・自衛隊においても2018年度末にまとめられた防衛大綱において、「人

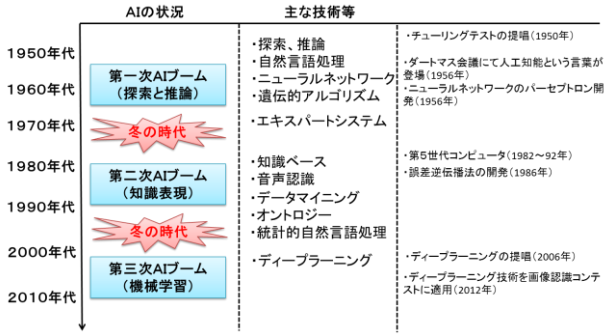
工知能（AI）等のゲーム・チェンジャーとなり得る重要技術に重点的に投資する」と打ち出した[2]。具体的な活用例として、「サイバー防衛の自動化」、「軍事・防衛関係のデータ翻訳」、「装備品の補修等管理」があげられている[3]。一方で、人工知能は、大まかには「知的な機械、特に、知的なコンピュータプログラムを作る科学と技術」と説明されているものの、その定義は研究者によって異なっている[4]。しかしながら、多くの人は人工知能と聞くと、将棋や囲碁のプロ棋士にコンピュータが勝利したように、人間の思考をはるかに超え、自律的に行動できるようなものを想像する人が多いと考えられる。将棋や囲碁のプロ棋士に勝利したコンピュータは、ディープラーニングに代表される機械学習や強化学習といった技術により実現できた。防衛大綱に記載されている人工知能技術の活用例や、複雑な状況判断、指揮統制あるいは、無人機のようなプラットフォームの自律化等、人間の高度な思考過程をサポートあるいは代替することを想定していると考えられ、それらの実現には機械学習は必要不可欠である。一方で、一般的に防衛装備品は民生品と比較して、運用数量が圧倒的に少なく、新旧技術（アナログとデジタル）が混在して運用されている。したがって、当該技術を防衛装備品へ適用する場合、民生品への適用とは異なった課題が存在する。

本稿では、人工知能技術、特に深層学習に代表される機械学習の特徴を考察しながら、機械学習の防衛装備品への適用における様々な課題とその解決策について述べていきたい。

１　機械学習と人工知能

(1)　機械学習出現前の人工知能

人工知能が研究分野として確立したのは、1956 年のダートマス会議[5]である。この会議の提案書において、人工知能という言葉がジョン・マッカーシーによって初めて使われた[6]。これ以降、2 回のブームと冬の時代があり、今回が 3 回目のブームである。これまでの 2 回のブームで様々な技術が提唱され、それぞれ発展してきた（図 1）。第 2 次ブームまでの技術は、既に自衛隊の装備品に何らかの形で導入されている。特にエキスパートシステム[7]は、航空機や艦船、車両といった装備品の訓練用シミュレーターに採用されてきた。しかし、専門的な知識をデータ化すること自体が難しく、例えば対戦型シミュレーターでは、敵の動きが単純なものに留まる等、技術的な限界が見え始めた。そのため、人工知能の装備品への適用は限定的になっていった。



（出典）総務省「ICTの進化が雇用と働き方に及ぼす影響に関する調査研究」（2017年）

図１　年代ごとの人工知能のトレンド技術

(2)　機械学習出現後の人工知能

第 2 次ブームが 1990 年代に終わると、2000 年代にかけて、人工知能は再び冬の時代に突入したが、機械学習の研究はこの頃から発展してきた。機械学習とは、研究者により若干定義が異なるが、観測センサーやその他の手段で収集されたデータの中から一貫性のある規則を見出そうとする技術で、統計学と強い関連がある[8]。人工知能の応用分野は非常に広範囲であるが、現在、ほとんどの分野で利用されている技術である。

機械学習は大きく 3 種類に分類され、それぞれ活用先が異なる（表 1）。教師あり学習[9]と教師なし学習[10]はどちらも大量のデータを用いた統計的手法である。一方、強化学習[11]は、大量のデータを用意できない場合に有効となる技術である。

表１　利用可能なデータに基づく機械学習の分類

	入力に関するデータ［質問］	出力に関するデータ（教師データ）［正しい答え］		主な活用事例
教師あり学習	与えられる	○	与えられる	出力に関する予測、分類
教師なし学習	与えられる	×	与えられない	入力に関するグループ分け、情報の要約
強化学習	与えられる（試行する）	△（間接的）	正しい答え自体は与えられないが、報酬（評価）が与えられる	将棋、囲碁、ロボットの歩行学習

（出典）総務省ICTスキル総合取得教材eラーニング用「コース3」3-5人工知能と強化学習

この機械学習をさらに発展させ、人工知能の技術的障壁のブレークスルーとなったのが、深層学習である。深層学習は、長年研究されてきたニューラルネ

ットワークの最近の呼称であり、特に 4 層以上の深いニューラルネットワークを作る技術を示す[12]。深層学習の出現により、人工知能が広く一般に知れ渡るきっかけとなった。特に将棋や囲碁で国内の有名なプロ棋士がコンピュータに負ける光景は、多くの人に人工知能の限りない可能性を印象付けた。

２　年代ごとの人工知能の変化　―　演繹と帰納

1945 年に米国で開発された ENIAC(Electronic Numerical Integrator and Computer)は、最も初期に開発された電子式の自動計算機の1つで現代のコンピュータの祖先として有名である。この自動計算機は第2次世界大戦中に米陸軍の弾道研究所とペンシルヴァニア大学が中心となって大砲の弾道計算に用いる計算機として開発された。この計算機は、熟練した技術者が20時間かかる計算を約30秒で計算するという、当時としては驚異的な演算速度であった[13]。コンピュータはその名のとおり、原点は計算機である。即ち、計算を人間より速く、正確に行う機械である。この「正確」という特徴が重要である。

第1次から現在の第3次ブームまでの人工知能を年代ごとに分類すると、第1次と第2次ブームは、論理とそれを補強する知識である（表2）。

表２　人工知能ブームの歴史

年代（ブーム）	キーワード	応用範囲	正確性
第 1 次 **（1950～60 年代）**	論理	小 （パズル、ゲーム等）	◎
第 2 次 **（1980 年代）**	知識	中 （エキスパートシステム等）	○
第 3 次 **（2010 年代～）**	統計 （学習）	大 （パターン認識、機械翻訳等）	△

出典：西垣通『ビッグデータと人工知能』中公新書、2016 年、172 頁。

表 2 のとおり、正確性が時代の進化に伴って、減少している。これは、第 2 次ブームまでと第 3 次ブームでの「推論と探索」が大きく変化しているからである。第 2 次ブームまでは、3 段論法に代表される単純な論理による推論と探索であった。第 2 次ブームまでは、入力（問い）に対して論理条件で出力（解答）を算出していた。基本的には、何度入力しても論理条件が変わらなければ出力は変化しない。

一方、第 3 次ブームに代表される機械学習は、入力に対して統計処理により出力（解答）を探し出す。よって、統計処理のベースとなるデータが異なれば、出力は異なる。もし入力が同じでも、統計処理するデータが毎回異なれば、出力は毎回異なる。このように、人工知能の開発が進むとともに、入力（問い）と出力（結果）の関係は「必然的」[14]から、「蓋然的」[15]に変化した（図 2）。

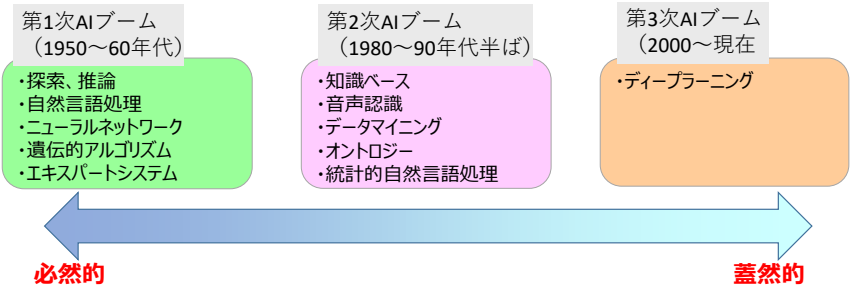


図２　人工知能技術と入出力の変化

図 2 では、人工知能の開発が進むにしたがって、開発された技術がよりデータ依存型になっていることを示している。しかしながら、第 1 次ブームの「必然的」出力を生成する技術が劣り、第 3 次ブームの「蓋然的」出力を生成する技術が優れているわけではない。丸山宏は、機械学習はプログラミングの方法論という観点から、「蓋然的」出力を生成するシステム開発を帰納的システム開発とした。これに対し、従来の人工知能技術の開発を演繹的システム開発とした[16]（表 3）。即ち、演繹的システムは入出力関係が必然的であり、帰納的システムは蓋然的となる。

表３　演繹的システムと帰納的システム

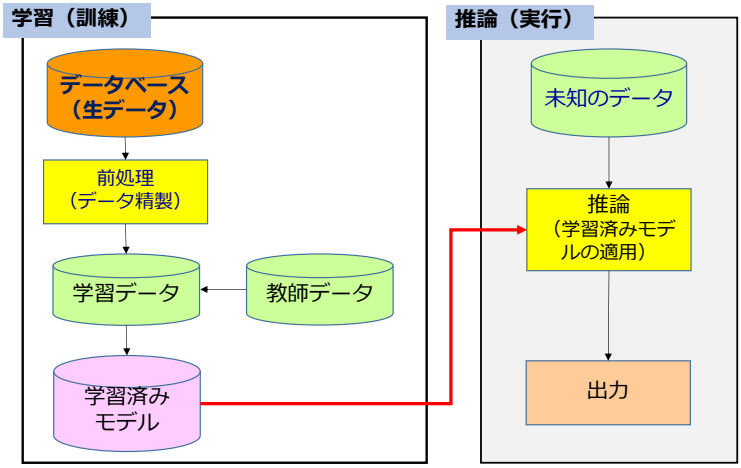
名称	定義	入出力関係
演繹的 システム開発	システムの仕様を定義し、先験的な知識に基づいて それをモデル化し、段階的に詳細化していく方法	必然的
帰納的 システム開発	仕様を訓練データの形で表現し、実装は訓練によって行う。すなわち、計算や判断を行うための知識 （モデル）を訓練データから獲得し生成する方法	蓋然的

出典：丸山宏、城戸隆「機械学習工学へのいざない」『人工知能』Vol. 33、No. 2、2018 年、124 頁を基に筆者作成。

３　機械学習の仕組みと課題

(1)　機械学習出現後の人工知能

機械学習によるシステムの構成例を図 3 に示す。一般的にコンピュータは、ある入力に対して、処理（推論）を施してその結果を出力する。機械学習では、入力（未知のデータ）の処理を実施する「推論」で使用するモデルを、データベースを活用して構築する。このプロセスは、推論モデルを構築するための学習（訓練）系統と、その系統により学習された推論を使った推論（実行）系統の 2 つから構成される。



（出典：丸山宏、城戸隆「機械学習工学へのいざない」『人工知能』Vol. 33、No. 2、2018 年、125 頁を基に筆者作成）

図３　機械学習システムの構成例

学習（訓練）系統では、まず様々な形で収集した生データを、この系統で処理できるようにデータ精製（前処理）を行う。そして前処理された学習データを用いて、推論を実行するための学習済みモデルを作成する。学習の過程で、教師データ（正解データ）を使用することで、より学習済みモデルの精度を向上させることもある。この学習済みモデルが推論モデルとなり、推論（実行）系統で、未知のデータ入力に対する何らかの解を出力する。

(2)　機械学習の課題　―　データベースの構築

機械学習システムの出力精度は、学習（訓練）系統におけるデータベース（生データ）の多寡が鍵となると考えられがちであるが、決してそれだけではない。非常に重要なのはデータ品質である。データ品質の要件は、様々な定義や尺度

があるが、一般的には、完全性（データが全て揃っていて欠損や不整合がないこと）、正確性（データが正確であること）、妥当性（データが正しい前提から導き出されていること）、一貫性（データに矛盾がないこと）、適時性（データ収集や使用するタイミング等が適正であること）が挙げられている。つまり、学習データは、データに偏りがなく、正確であり新しいデータで構成されていることが理想である。したがって、データ品質を向上させるプロセスである生データの前処理（データ精製）が重要である。データベース構築作業の大部分は、この前処理である。特に、データの収集源が多くなると、自動化がより難しくなり、多くの人手が必要になる。

更に、精製した学習データに正解を付与するための教師データの作成は、さらに人手が必要である。データ品質要件を満たしたデータの選別、そして人手で教師信号（アノテーション[17]という。）を付与しなければならない。大きい教師データを構築する場合、正に人海戦術で実施することになる。

(3) 防衛装備品用データベース構築の課題

防衛装備品に機械学習システムを適用する上で、前項のとおりデータベースの構築が必要不可欠である。しかしながら、適用する装備品や機能にもよるが、一般的にベースとなるデータが非常に少ないことが課題となる。例えば、航空機の整備データを構築しようとしても、民間機と自衛隊の航空機では、運用機数が桁違いである[18]。1 機あたりの航空機から収集できる整備データは限られているので、運用機数が少なければ収集できる整備データも少なくなる。また、航空機だけでなく、運用目的が同一の装備品である警戒管制レーダは、新旧の機種差が激しく、設置されてから 30 年以上の装備品も運用されている。当然ながら、古い機種はアナログ回路、新しい機種はデジタル回路で構成されている。アナログデータとデジタルデータというフォーマットが異なるデータを整える必要がある。よって、データ収集と前処理で非常に煩雑な作業が必要となり、人手を多く要するのである。

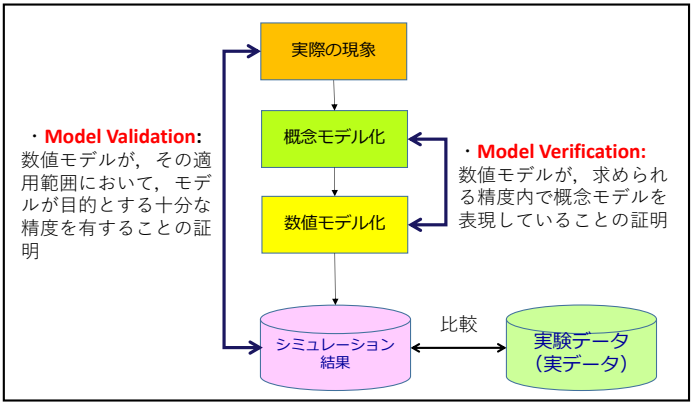
(4) 学習（訓練）系統から推論（実行）系統移行時の課題

学習（訓練）系統では、推論（実行）系統で使用する学習済みモデルを作成する。このため、データベース（生データ）と通常、オンライン状態になっている。学習済みモデルは、学習する度に変化する。よって、常に学習している状態と言える。

一方、推論（実行）系統では、学習系統で生成された学習済みモデルを推論モデルとして使用するが、このモデルがシステムの目的に合致しているか検証

と妥当性確認（V&V, Verification & Validation）が必要である。検証と妥当性確認を実施することで、初めて推論（実行）系統で出力される結果の品質が保証される。この品質保証の重要性は、工学シミュレーション分野等、モデリング&シミュレーション（M&S）では広く認識されている[19]。

M&S におけるモデルの V&V は、実際の現象から概念モデルを作成、それを基に数値モデルを作成し、シミュレーションを行う。シミュレーションの結果は、実験データ（実データ）と比較し、結果の評価を行う。シミュレーション結果が実データと相違ない、または差異が許容する範囲内であればこのシミュレーションモデルは妥当であると言える。しかし、実データと異なる場合、概念モデルと数値モデルそれぞれを検証し、シミュレーション結果と実際の現象との妥当性確認を行う（図 4）。



（出典　部会トピックス「シミュレーションの信頼性確保に関する取り組みの現状と課題」『日本原子力学会誌』Vol. 60、No. 3、2018 年、48-49 頁を基に筆者作成）

図４　M&S における V&V（モデルの検証と妥当性確認）

V&V の重要性及び必要性は、様々な分野で広く認識されており、シミュレーションの信頼性の確保に関するガイドラインや標準を作成する動きが活発になっている。日本原子力学会は、2016 年 7 月に「シミュレーションの信頼性確保に関するガイドライン：2015」を発行している[20]。

この方法は、M&S が演繹的推論システムであるため実施できる。一方で、帰納的推論システムである機械学習システムでは、データの品質向上が推論モデルの品質向上に資する。したがって、これまでの機械学習システムで作成されたモデルは V&V を経て、推論（実行）系統に移行されるべきである。また、再度学習系統にて成長させる場合は、V&V を経て、推論（実行）系統に移行すべきである（図 5）。ここで、モデルの V&V を実施するためには、図 3 における学習データや教師データとは別に、評価用のデータセットが必要となる。しかし、防衛装備品では、データが少ない中で、学習データと別のデータセットを準備することは非常に難しいと考える。

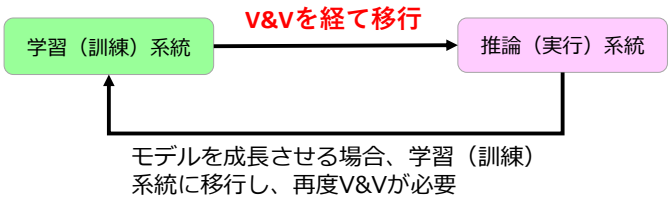


図５　学習（訓練）系統と推論（実行）系統間のＶ＆Ｖプロセス

４　機械学習システム導入における課題

機械学習システムの社会実装が進むにしたがって、様々な技術課題が浮き彫りになっている。代表的な課題として、ブラックボックス問題、バイアス問題、品質保証が挙げられている[21]。

ブラックボックス問題はいわゆる説明責任の問題であり、「何故この結果になるのか人間が理解できる説明を出力しない」、「出力がどのような振る舞いをするのか動作保証ができない」というものである。

バイアス問題は、学習データに偏見が含まれていると、推論モデルにもその偏見が反映されるというものである。2018 年に、Amazon は人工知能を活用した人材採用システムの開発中止を発表した。Amazon は、2014 年からこのシステムの開発に取り組んでいたが、データの偏見性により差別的な採用が散見されたため、運用を取りやめた[22]。

品質保証で問題なのは、人工知能の振る舞いが仕様で定義できないため、そもそも出力結果の成否を判断することが難しいことである。

これらの課題を解決するために、現在、科学技術振興機構によって、従来のソフトウェア工学ではなく、新しいアプローチによる「AI ソフトウェア工学」

の必要性が提唱されている[23]。同機構は、機械学習システムに、演繹的推論システムの手法と帰納的推論システムの手法の双方を適用することを提唱している。これは、学習データの収集、管理、精製だけでなく、動作保証、品質保証の考え方を採用することである。安全保障分野で使用される防衛装備品は、機能発揮に必要となる品質保証の要求レベルが高い。よって、防衛装備品に機械学習システムを導入する場合、データの品質向上だけでなく、作成された推論モデルの品質保証が必要である。

５　防衛装備品への機械学習システム適用への課題

防衛装備品に機械学習システムを適用する上での最大の課題は、データが少ないことである。データは学習用だけでなく、教師用、さらには V&V 用のデータも必要である。データの多寡はデータ品質が高ければ本来大きな問題ではないが、防衛分野では、新旧装備品の混在により品質の高いデータそのものが少ない。従って、今後少ないデータから効果的にモデルを作成する技術が必要となる。また、データをできるだけ多く収集し、その中から質の高いデータを抽出することも重要である。

次に、V&V（検証と妥当性確認）の実施が必要である。機械学習システムはバイアス問題等、データに起因する問題を抱えている。データそのものの検証だけでなく、出力の確からしさの証明が必要である。特に、意思決定に係るシステムに機械学習を採用する場合は、必要不可欠と考える。

これらの課題を解決するためには、防衛装備品を製造する会社だけでは解決は不可能である。装備品のユーザーである自衛隊自身が保有するデータの提供、データ処理（精製）、そして、学習系統によって生成された推論モデルの V&V を実施することが必要不可欠である。特に専門性が高い分野に機械学習を適用する場合は、出力結果が妥当であるか否かの判断は、高いスキルレベルを有したユーザーしかできない。よって、機械学習システムを導入する際には、自衛隊自身がシステムをハードウェア面の整備だけでなく、データ管理、モデル検証等のソフトウェア面の整備を実施できる態勢を準備する必要がある。だが、ユーザーが推論モデルの検証を実施しなければならないため、ユーザーの能力を大幅に超越した能力を有する人工知能の導入は、実際上、評価が困難である。従って、現時点での導入は難しい。機械学習の防衛装備品への適用は、あくまでユーザーの行動を支援するサポートシステムとしての導入となると考える。

結論

機械学習の登場以降、人工知能は第3次ブームと呼ばれる発展を遂げてきた。多くの人が人工知能に対して、大きな期待を抱き、人工知能により省力化・省人化が達成できる他、あらゆる思考的問題を解決できると信じている。自衛隊においても適用可能な分野の検討が進んでいるところである。

しかしながら、機械学習は、統計処理に基づいているためデータセットがどんなにビッグであろうと、所詮、有限であるデータ集合からの推論であることには変わりない。従って、工夫なしにはその根源的弱点を回避できない[24]。防衛装備品への適用は、データセットの準備と処理が必要不可欠である。そして、重要なシステムであるほど、出力結果の検証が必要であり、その作業には高いスキルレベルを有したユーザーが必要不可欠である。

人工知能は日々発展しており、今後様々な分野に導入されるのは間違いない。しかし、現時点では万能ではなく、今後もその状況は続くと考えられる。人工知能を有した装備品を自衛隊に円滑に導入するためには、まずユーザーが機械学習の実情を正しく認識することが重要である。機械学習は統計的処理を行っている以上、出力精度が100%にはならないことを認識する必要がある。そして、機械学習は学習データには無い稀な事象に対しては基本的に無力である。また、防衛装備品のデータは、製造会社へ提供する際にセキュリティー上の課題が発生する可能性もある。これらを認識したうえで、ユーザーと製造会社が協力してデータ管理（収集、処理、保全）と推論モデルのV&Vを実施することで、ユーザーを強力に支援する機械学習システムが構築できると考える。機械学習の防衛装備品への適用は、現時点ではあくまでユーザーを支援するシステムとして導入すべきである。

（2021年3月11日受付）

---

1 松尾豊『人工知能は人間を超えるか』角川 EPUB 選書、2015 年、60 頁。

2 「平成 31 年度以降に係る防衛計画の大綱について」2018 年 12 月 18 日。

3 「防衛省、AI 導入拡大　サイバー対策や装備補修」『日本経済新聞』2018 年 6 月 17 日。

4 「総務省平成 28 年度版情報通信白書」、2018 年 7 月。

5 日本では会議と訳されているが、正式には、”The Dartmouth Summer Research Project on Artificial Intelligence”で、互いの研究成果を発表し合う、研究会である。1956 年 7 月から 8 月にかけて米国ニューハンプシャー州ハノーバ市のダートマス大学に在籍していたジョン・マッカーシーが主催した。

6 「人工知能の話題　ダートマス会議」、“What’s AI”、人工知能学会、https://www.ai-

gakkai.or.jp/whatsai/AItopics5.html（2021 年 4 月 2 日アクセス）。
[7] ある分野の専門家が保有している知識をデータ化し、専門家のように推論や判断ができるようにするコンピュータシステムのこと。
[8] 「人工知能研究　機械学習」、“What’s AI”、人工知能学会、https://www.ai-gakkai.or.jp/whatsai/AIresearch.html（2020 年 4 月 2 日アクセス）。
[9] コンピュータに「入力」と「正しい出力」が紐づいた学習データを与え、ある入力を受けた時に正しい出力を応答するアルゴリズムを構築する学習法。
[10] コンピュータに「入力」データのみ与え、データに内在する特徴量等のパターンをコンピュータ独自で抽出する学習法。
[11] コンピュータにある「環境」の中で、目的として設定された「報酬（スコア）」を最大化するための行動を学習する方法。
[12] 松尾豊「人工知能関連技術の歴史と技術動向」『電子情報通信学会誌』Vol. 103、No. 5、2020 年、451 頁。
[13] 「ENIAC」、コトバンク、https://kotobank.jp/word/ENIAC-1573（2021 年 4 月 2 日アクセス）。
[14] 特定の入力（原因）に対して常に特定の出力（結果）となるものと定義。
[15] 特定の入力（原因）に対して、（統計的処理により）一義的に出力が決定しないがある程度確実であるものと定義。
[16] 丸山宏、城戸隆「機械学習工学へのいざない」『人工知能』Vol. 33、No. 2、2018 年、124 頁。
[17] Annotation：あるデータに対して関連する情報（メタデータ）を注釈として付与すること。
[18] 例えば、ボーイング社の B-767 や B-777 は、それぞれ 1000 機以上生産されている。一方、航空自衛隊の航空機は、F-15 戦闘機と T-4 練習機はそれぞれ約 200 機、それ以外の航空機は各機種 100 機以下しか生産されていない。
[19] 中村均「第 3 回 V&V にかかわる技術標準の動向」『日本原子力学会誌』Vol. l57、No. 2、2015 年、33 頁。
[20] 部会トピックス「シミュレーションの信頼性確保に関する取り組みの現状と課題」『日本原子力学会誌』Vol. 60、No. 3、2018 年、47 頁。
[21] 村尾麻悠子「AI は品質・信頼性確保が急務、「日本が先行している」」『EE Times Japan』2019 年 9 月 2 日、https://eetimes.jp/ee/articles/1909/02/news029.html。
[22] Jeffrey Dastin「アマゾンがＡＩ採用打ち切り」REUTERS、2018 年 10 月、https://jp.reuters.com/article/amazon-jobs-ai-analysis-idJPKCN1ML0DN。
[23] 研究開発戦略センター「戦略プロポーザル AI 応用システムの安全性・信頼性を確保する新世代ソフトウェア工学の確立」科学技術振興機構、CRDS-FY2018-SP03、2018 年 12 月。
[24] 樋口智之「データ関連の数理技術の変遷」『人工知能』Vol. 33、No. 2、2018 年、116 頁。