［機械学習工学］

1 機械学習工学の狙いと展開

基応般

丸山　宏 | （株）Preferred Networks

機械学習工学の生まれた背景

マーク＆スイープ型のガベージコレクションを発明したのは John McCarthy で 1959 年のことであった．彼は「常識」を備えた Advice Taker という自然言語処理システムの開発を企図して，記号処理言語 Lisp を設計したが，そのためにガベージコレクションが必要だったのである．すなわち，今日ほとんどのプログラミングシステムに備わっているガーベージ・コレクションは元々は人工知能技術だったのである．

そのほかにも，自然言語解析のための構文解析アルゴリズム，証明木探索のための探索アルゴリズムなど，人工知能研究を発端とする，情報処理の基礎技術は多い．現在注目を浴びている深層学習も，情報処理の基礎技術の１つとして，日々のプログラミングに使われるようになるだろう．このように，我々は深層学習を（人工知能技術としてではなく）新しいプログラミングツールの１つとして捉える．

プログラミングツールとして見ると，深層学習を代表とする統計的機械学習は，新しいプログラミングモデルと考えることができる．通常の，チューリングマシンをベースにする計算モデルにおいては，プログラミングは演繹的に行われる．すなわち，入力と出力の間の関係を厳密に数学的に定義し（これを仕様と呼ぶ），この仕様を段階的にアルゴリズムに落とし込んでいくことでプログラミングが行われる．これに対して，統計的機械学習によるプログラミングでは，入出力の厳密な関係を仕様として与える代わりに，入出力ペアの例示を与え，それらの例示を模倣するシステムを帰納的に導く．

厳密な仕様がなくてもシステムが作れるので，仕様定義が難しいために今までは解くのが困難だったような問題でも，例示さえあれば解けるようになる．たとえば，「画像に犬が写っているかどうか」という認識問題を考えてみよう．この命題の真偽を各ピクセルの輝度の関係として厳密に規定するのはほとんど不可能であるが，犬の写っている画像，そうでない画像を例示として用意することは簡単である．

このように，統計的機械学習を使った帰納的プログラミングは，仕様から段階的詳細化を行っていく従来のプログラミングと根本的に異なるため，今までのシステム開発のやり方が必ずしもうまく適用できない．特に，深層学習が自動運転や監視など社会の重要な仕組みの中に取り入れられていくようになると，その品質，安全性，保守性などをどのように担保するかはまだ見えていない課題である [1]．

このような背景から，統計的機械学習を使ったシステム（本特集では「機械学習応用システム」と呼ぶ）をどのように効果的に，また安全に開発・運用できるのか，工学的な知識体系の整備が必要と考え，そのための意見交換の場として 2018 年 4 月に日本ソフトウェア科学会に機械学習工学研究会（主査：国立情報学研究所 石川冬樹准教授）を設置し，活動を始めた．統計的機械学習に基づく帰納的なシステムの開発・運用が今までの演繹的システムとどこが違うのか，どこが同じなのか，特に過去 50 年に得られたソフトウェア工学の知見は帰納的システム開発にどのように適用されるのか，などが議論されつつある．本稿では，これらの議論を概括し，今後の展望について述べる．なお，現在では機械学習の主

流は統計的モデリングに基づくものなので，本特集では以降特に断らない限り機械学習とは統計的機械学習を指す．また，機械学習の具体的な手法として深層学習を取り上げることが多いが，ほとんどの議論は一般の統計的機械学習にも適用可能である．

機械学習による帰納的プログラミングとは

機械学習による帰納的プログラミングが，普通のプログラミングとどのように違うかを考えてみよう．たとえば「摂氏を華氏に変換するプログラム」を考える．通常のプログラミングにおいては，「摂氏を華氏に変換する」という要件を，F＝1.8 × C＋32（ただしCは摂氏，Fは華氏を示す）という数理モデルの形の仕様に変換し，それを段階的にアルゴリズムへ変換していくことで開発が行われる．

一方，帰納的プログラミングにおいては，入出力の例を作ることが仕様策定に相当する．1つの方法は，摂氏と華氏の温度計を購入し，同時にその値を読むことで入出力例を作ることである．これを訓練データセットとして機械学習アルゴリズムを適用し訓練済みモデルを得る（図-1）．この場合，F＝1.8 × C＋32という入出力の関係を表す仕様は未知でよいことに注意しよう．また，仕様に合わせて出力を計算するアルゴリズムも構築する必要がない．

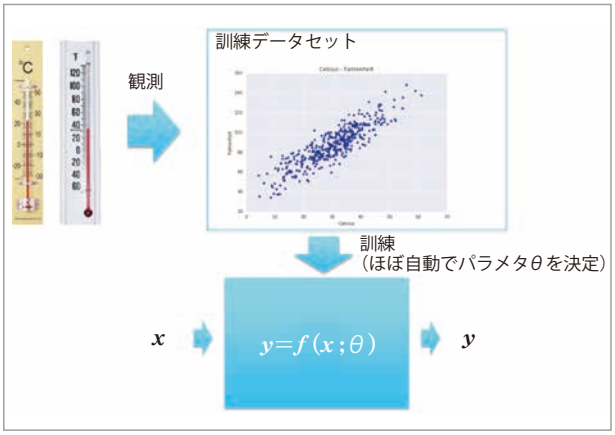
実際の応用システムの中で機械学習が利用されるとき，ほとんどの場合はシステムの一部のモジュールとして機械学習が使われるのにすぎない．システムのほかの部分は通常の演繹的プログラミングで行われる形になる．機械学習で作られるモジュールを本稿では機械学習モジュールと呼ぶことにする．機械学習モジュールは訓練[☆1]パイプラインと推論パイプラインからなる（図-2）．

訓練パイプラインは訓練時（開発時）に使われる．収集された生データは前処理され，正解データと組み合わせて訓練データとなる．この訓練データを訓練アルゴリズムにかけて訓練済みモデルを得る．

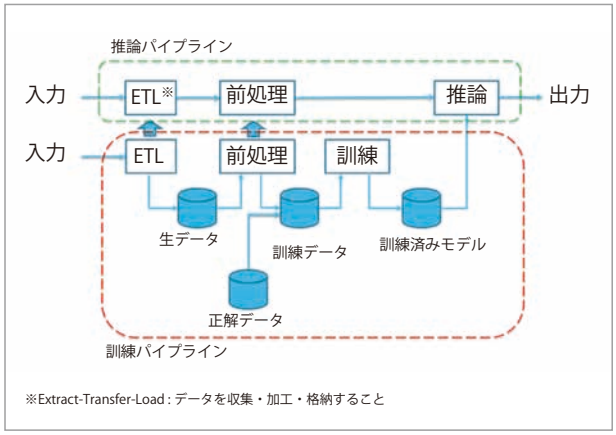
実行時には推論パイプラインを用いる．訓練時とまったく同じデータ収集・前処理をほどこされたデータを入力とし，推論アルゴリズムが訓練済みモデルを用いて出力に変換される．

訓練アルゴリズムにはさまざまなものがある．訓練は，$y=f(x;\theta)$という関数fを求めることで行われる．ここでxは入力，yは出力，θはパラメタである．x, y, θのいずれも一般的には多次元のベクトルである．訓練データに現れる入出力のペア$<x_i, y_i>$（$i=1, 2, ,,,,n$）について，y_iと$f(x_i;\theta)$の誤差ができるだけ小さくなるようなθを求めることが訓練に相当する．関数fの形として最も簡単な

☆1 本特集では，“training”の訳語として「訓練」を用いる．文献によっては「学習」が用いられていることに注意．



■図-1　機械学習による帰納的プログラミング



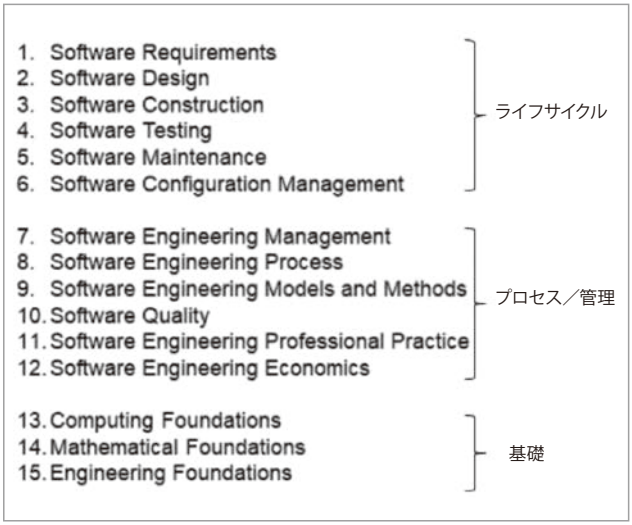
■図-2　機械学習モジュールにおける2つのパイプライン

ものの 1 つが線形関数であり，誤差関数として 2 乗誤差をとれば通常の線形回帰となる．この場合，訓練で得られる関数は常に線形である．

現在注目を浴びている深層学習においては，多くの場合パラメタ θ の次元が数百万，数億などきわめて大きいために，非常に複雑な関数も近似できる．任意の計算可能な多次元関数について，十分に大きな次元のパラメタがあって，その関数を与えられた誤差範囲で近似する深層ニューラルネットを構成することができることが知られている．この意味で，深層ニューラルネットは計算モデルとして擬似的にチューリング完全といえる．

機械学習工学の課題

機械学習工学を，工学的知識体系として構築するには，どのような構成にしたらよいだろうか．ソフトウェア工学知識体系 V3（SWEBOK V3）の章立てを図 -3 に示す．この体系には，15 の知識領域（KA，Knowledge Area）が定義されていて．そのうち 6 つの KA は，要求，設計，構築など 1 つのソフトウェアを開発する際のライフサイクルによる整理であり，次の 6 つの KA は，ソフトウェア開発プロセスや管理など，複数のソフトウェアを開発する際の関心事による切り分けと見ることができる．残りの 3 つは，ソフトウェア開発に必要な基礎知識に関するものである．



■ 図 -3　ソフトウェア工学知識体系（SWEBOK）における知識領域（KA）

機械学習工学の知識体系化においても，このようなフレームワークは有効であろう．本稿では，2017 年後半から 2018 年前半にかけて，機械学習工学のコミュニティが議論したさまざまな課題を，1）ライフサイクルの観点，2）ディペンダビリティの観点，3）マネジメントの観点から整理する．

ライフサイクル各局面における課題

まず機械学習応用システムのライフサイクルについて考えてみよう．機械学習モジュールが，与えられた訓練データセットの下で期待する精度を達成するかどうかはやってみなければ分からない．このため，機械学習応用システムの構築は多分に探索的なものとなる．したがって，開発を始める前にそのことを顧客によく理解してもらうと同時に，そもそも機械学習を使って解くべき問題かどうかをよく吟味しなければならない．これが**アセスメント**の局面である．次に，想定する機械学習モジュールが想定する訓練データセットで必要な精度が出せそうかどうか，を技術的に検証する．これを **Proof-of-Concept**（**PoC**）と呼ぶことが多い．

技術的な可能性が確かめられたならば，機械学習モジュールを含めたシステム全体の**設計・開発**を行う．開発時にも，実際のビジネスデータを用いて継続的に訓練済みモデルの精度向上を行う．開発が終わるとシステムの**実運用**を行う．運用中も，データの統計的な変化（**コンセプト・ドリフト**と呼ぶ）を継続的にモニタリングし，必要に応じて機械学習モジュールの再訓練を行う．ライフサイクルの各局面の課題については，本橋による解説[6] に詳しい．

ディペンダビリティの課題

品質：機械学習モジュールで解くべき問題は，本質

的にモデル化が難しいものが多い．モデル化ができる問題であれば，多くの場合通常のプログラミングによって演繹的に解くことができるからである．モデル化ができない問題とは，個別の入力値に対して，正しい出力値を出す計算のステップが必ずしも分かっていない，あるいはそもそも「正しい出力値」が何かが時として分からない問題であり，そのため，できあがった機械学習モジュールが「正しい」振舞いをしているかを知るのは難しい問題となる．石川による解説[3]は，この品質をどのように測定し，担保するかに関するさまざまな課題とその解決アプローチについて議論する．

セキュリティ・プライバシ：正しい入出力関係を完全にはモデル化できない問題は，できあがった機械学習応用システムのセキュリティにも課題を投げかける．仕様の曖昧な点をついて機械学習モジュールを「だます」ような入力例を作る技術が発達しているからであり，機械学習応用システムの中に，このような騙されやすい機械学習モジュールが１つでもあれば，全体のセキュリティに大きな影響を及ぼしかねない．また，機械学習モジュールの訓練にはきわめて大きな訓練データセットを用いることが多いが，もしこの訓練データセットにプライバシにかかわる情報があれば，プライバシの確保も問題となる．本特集において吉岡[4]は，機械学習応用システムのセキュリティとプライバシに光を当てる．

人間参加：機械学習応用システムにおいては，仕様を定めにくい問題を解くために，しばしば問題解決ループの中に人間を入れること（human-in-the-loop）が行われる．たとえば，画像認識の訓練データセットを作成する際に，正解ラベルを人手で与えることはその一例である．そのほかにも，訓練の状況を可視化したり，人間のオペレータによって推論結果を検証したり修正したりすることもある．このように，問題解決全体の中に人間を参加させることは，しばしば機械学習モジュールにとっての必要な要件となる．本特集では，五十嵐[5]が HCI 専門家の立場から，この点について議論している．

マネジメントに関する課題

開発・実行環境：深層学習のワークロードは通常のプログラムのワークロードとは大きく異なり，PC 等で広く使われるプロセッサでは効率良く実行できない．このため，GPGPU など，深層学習により適した計算機アーキテクチャが用いられる．このため，訓練／推論の両面で深層学習に適した計算環境（ハードウェア・ソフトウェア）が求められる．本特集の今井・太田[2]は，現状の深層学習向け計算環境を概括する．

組織：統計的機械学習は今までの情報システムの作り方と大きく異なる考え方を要求される新技術であるため，これを組織の中で戦略的に活用していく体制を作る必要がある．部門横断的にデータの利用を考え，プロジェクトを優先順位付けし，人材を獲得・育成しなければならない．必要に応じて外部のベンダを利用する場合には，統計的機械学習特有の知財や契約に関する問題についても留意する必要がある．統計的機械学習においては，訓練データセットや訓練済みモデルなど，今までの情報システムにはない新しい形の成果物があり，これらをどのように再利用するかも重要な課題であるからである．本特集において，本橋[6]はこのような組織の能力についても触れている．

その他非機能要件に関する課題

その他の非機能要件に関しても，機械学習応用システムには，従来のシステム開発とは異なる課題がある．たとえば，深層学習における推論では，１回の推論においても大量の訓練済みパラメタを読み込む必要があるため，推論を個別に行うと効率が悪くなる．複数の推論要求を集めてバッチ処理で推論す

ればスループットを上げることができるが，これは応答時間とのトレードオフになる．

システム開発の成果物の再利用についても新たな課題がある．機械学習モジュールはアルゴリズムと訓練済みモデルからなるが，この訓練済みモデルの作成には多くの労力がかかっているので再利用したい．どのように再利用するのか，また再利用における権利と義務の関係がどうなっているのかについては，まだ十分に整理がされていない．

これらの非機能要件に対しても，機械学習工学が取り組んでいくことになるだろう．

今後の展望

橋やダムを安全に設計し建築するための知識を体系化したものは土木工学と呼ばれる．安心して乗れる航空機を設計するための知識体系は航空工学である．工学とは新しい科学の知見や技術を我々の社会に受け入れられる形で利用するために必要十分な知識を体系化したものであり，そのベースには材料力学，構造力学，流体力学などの理論がある．しかし，橋や飛行機がどのように機能するか，すべての原理が完全に解明されているわけではない．たとえば，構造力学が基づくニュートン力学は，我々が日常使う時空間スケールにおいてはきわめて良い近似であるが，あくまでも近似にすぎない．工学においては，理論では把握しきれない細部の誤差を見越して，**安全係数**をかけることによって，橋や航空機の安全性を確保している．安全係数は長い時間をかけて経験的に得られたものであるが，その実績が工学として認められ，さらには社会に受容されている．

深層学習はなぜうまくいくのか原理が分かっていないから使えない，説明可能でないから使えない，などという議論を目にすることがある．しかし問題は，統計的機械学習は新しい技術であり，まだこの技術をどのように使えば安全に，かつ効果的に使えるかの知識が確立されていないことにある．統計的機械学習は本質的に統計であり，訓練データセットはある確率分布から独立・同分布でサンプリングされたものだ，という根源的な仮定がある．このため，訓練データセットにサンプリングバイアスが入ることは避けられない．したがって，機械学習モジュールから得られる結果は常に近似値にすぎない．誤差のある結果をうまく使って安全なシステムを作るには，今までの工学における安全係数に相当する考え方が必要になってくるだろう．これは，技術だけの問題ではなく，社会の期待レベルとのバランスの問題であり，工学的センスが要求されるものとなる．機械学習工学が工学として認知されるようになり，橋や航空機のように，当たり前のように社会に受容される日を願ってやまない．

参考文献

1) 丸山　宏：機械学習工学に向けて，日本ソフトウェア科学会第 34 回大会予稿集 (2017).
2) 今井健男，太田満久：機械学習システムの開発・運用環境，情報処理，Vol.60, No.1, pp.17-24 (Jan. 2019).
3) 石川冬樹，徳本　晋：機械学習システムのテストと検証，情報処理，Vol.60, No.1, pp.25-33 (Jan. 2019).
4) 吉岡信和，機械学習応用システムのセキュリティとプライバシ，情報処理，Vol.60, No.1, pp.34-39 (Jan. 2019).
5) 五十嵐健夫：機械学習システムのためのヒューマンインタフェース，情報処理，Vol.60, No.1, pp.40-47 (Jan. 2019).
6) 本橋洋介：機械学習応用システムのプロジェクト管理と組織，情報処理，Vol.60, No.1, pp.48-55 (Jan. 2019).

(2018 年 9 月 3 日受付)

■**丸山 宏（正会員）** hm2@preferred.jp

1983 年東京工業大学情報科学専攻修士課程修了．日本 IBM 東京基礎研究所にて，自然言語処理，XML，セキュリティなどの研究に従事．2011 ～ 16 年統計数理研究所教授．2016 年より（株）Preferred Networks 勤務，2018 年より同社フェロー．