



特集

機械学習工学



編集にあたって

野ヶ山尊秀 | 日本アイ・ビー・エム (株)

丸山 宏 | (株) Preferred Networks

機械学習を含めたシステム（本特集では機械学習応用システムと呼ぶ）を製品として顧客に納品しようとする、さまざまな課題に直面する。たとえば、十分に訓練やテストを実施しているにもかかわらず開発中や運用中に認識精度が下がることがある。ほかに、訓練データとは特徴が異なるデータが入力され始めたとき、当然ながら認識精度が下がる。誤認識した場合だけ別のシステムや人間に処理してもらおうとしても、誤認識したこと自体をどう検出し、どう引き継げばよいだろうか。

約半世紀前、ソフトウェアの利用が民間に拡大する中、人々は同様の課題に直面していた。それはソフトウェア危機として知られ、予算や期間を超過しても完成せず、品質の低いソフトウェアが多数登場した。その後多くの努力によって研究が進み、顧客からの要求を整理する方法、プログラムの書き方、プロジェクトの進め方、品質の検証方法、運用・保守の方法などがソフトウェア工学^{☆1}として整備され、現在ではさまざまな観点でうまくソフトウェア製品を仕上げるができる。

現在、機械学習応用システムの開発・運用は非常に困難を伴う。しかしそれはかつてソフトウェアの技術者が克服したように、機械学習応用システムの技術者にも克服できるはずである。そのための情報交換の場として、機械学習工学研究会は2018年より日本ソフトウェア科学会の研究会として活動を開始した。同研究会では、機械学習応用システムにか

かわるさまざまな手法やツールに関する情報交換、そして知識の体系化が行われている。

本特集は、機械学習応用システムの課題と解決手法について、同研究会の主要なメンバに解説してもらう。まず「機械学習工学の狙いと展開」で、機械学習とソフトウェア工学の境界領域で起きてくる課題について俯瞰し、機械学習に対する工学的な知識体系の必要性を論じる。次に「機械学習応用システムの開発・運用環境」では、提案、開発、運用と進むプロジェクトの各フェーズで必要な手続きとその際に利用するツールやアルゴリズムを紹介する。そして「機械学習応用システムのテストと検証」では、品質保証の難しさについて論じ、現在よく用いられているいくつかのアプローチを紹介する。「機械学習応用システムのセキュリティとプライバシー」では、システムに機械学習を導入したことによって新たに生じる不確かさを利用して、不正な利用が可能となる場合について論じ、その対策について紹介する。「機械学習のためのヒューマンインタフェース」では、データを作成する人、訓練させる人、利用する人、など、システムを取り巻く人間に着目し、より効率的かつ正確にシステムと情報をやりとりするための方法について論じる。最後に「機械学習応用システムのプロジェクト管理と組織」では、安全なプロジェクト進行の観点で特に注意が必要な確認項目や、必要な組織構造について説明する。

本特集の読者に機械学習応用システムに携わる人がいれば、ぜひ担当しているプロジェクトで本稿を活かしてほしい。またぜひ機械学習工学研究会を訪れ、知見を共有し、工学としての成熟に貢献してほしい。

(2018年10月15日)

^{☆1} ソフトウェア工学には立場によってさまざまな定義があるが、本特集では製品を仕上げるために必要な技術という緩い解釈をすることとする。