…› 石井一夫（公立諏訪東京理科大学）

機械学習工学

石川冬樹，丸山　宏 編著
柿沼太一，竹内広宜，土橋　昌，中川裕志，原　　聡，堀内新吾，鷲崎弘宜 著
講談社（2022），3,300 円（税 10%込），336p., ISBN：978-4-06-528586-2

本書籍の概要と AI の品質に関するガイドライン

本書籍は，編者である石川冬樹，丸山宏らが運営している日本ソフトウェア科学会機械学習工学研究会での研究活動成果をまとめたものである．機械学習に関するシステム開発，システム運用，機械学習システムの品質保証，説明可能な AI，AI の倫理，知財側面に焦点が当たっている．本書籍に関連して，本誌でも，私自身が「ビブリオ・トーク―書評―：ソフトウェア工学から学ぶ機械学習の品質問題」[1] や，「5 分で分かる !? 有名論文ナナメ読み：Marco T. Ribeiro et al.：“Why Should I Trust You?”：Explaining the Predictions of Any Classifier」[2] などの記事を取り上げてきた．また，本書籍編者の丸山宏らにより本誌 2019 年 1 月号に「機械学習工学」[3] の特集が組まれ，最近でも本誌 2022 年 11 月号に「AI の品質保証」[4] という関連する特集が組まれた．

今回，AI プロダクト品質保証ガイドライン（以後 QA4AI ガイドライン）[5] や，機械学習品質マネジメントガイドライン（以後 AIQM ガイドライン）[6] について解説してほしいというリクエストがあり，そのまとめとした背景を知るために本書籍を紐解いた．

第 3 次 AI ブームと言われるようになって久しいが，AI の活用が進むにつれ，AI の社会的インパクトや倫理的側面，世間の関心などもあり，AI に関する多くのガイドラインが作られている．国内では機械学習の品質に関して，QA4AI ガイドラインと AIQM ガイドラインが，公開されている．

QA4AI ガイドラインは，AI の品質管理として Data Integrity（データの完全性），Model Robustness（モデルの頑健性），System Quality（システムの質），Process Agility（プロセスの迅速性），Customer Expectation（顧客満足）という 5 つの軸を取り上げている．それぞれ，成果物（データ，モデル，システム）と開発工程（プロセス），ユーザ評価（顧客）についてチェック項目を設けて評価し，チャート化するという方法をとっている．具体例として，自動運転，産業プロセス（プラントでの適用），音声インタフェース（スマートスピーカなど），画像や動画などのコンテンツ生成，文字自動読み取り（OCR）が紹介されている．

AIQM ガイドラインは，機械学習技術モデルに関する固有の品質特性を挙げ，これについて内部特性と外部特性に分けて明確化し整理する．その後，各特性のレベルを定義するという形をとる．特に，プライバシーとセキュリティの問題を取り上げているところは，QA4AI ガイドラインにないところである．執筆時点で，QA4AI ガイドラインは 2022.07 版が，AIQM ガイドラインは第 3 版（Revision 3.1.0）2022 年 8 月 2 日が最新版である．1 年ごとぐらいの短期間でアップデートされており，アップデートのたびに内容充実と新技術が盛り込まれているので，AI についての最新の問題点を確認するのにちょうどいい感じである．

本書籍の内容

本書籍は，第 I 部「機械学習工学とは」，第 II 部「機械学習システムの開発・運用マネジメント」，第 III 部「機械学習システムの開発技術と倫理」，第 IV 部「機械学習と知財・契約」，第 V 部「機械学習工学の今後」の 5 部構成からなり，2 つのガイドラインを併せて圧縮したような感じになっている．

第 I 部の第 1 章「機械学習工学」は機械学習全体のまとめである．第 II 部の第 2 章「機械学習システムの開発とその検証プロジェクト」，第 3 章「機械学習システムの運用」は，機械学習システムの開発と運用についてのまとめである．

第 III 部は，本書籍の最も中心的な部分であるが，第 4 章「機械学習デザインパターン」，第 5 章「品質のとらえ方と管理」，第 6 章「機械学習モデルの説明法」，第 7 章「AI 倫理」と機械学習工学に関するトピックが続いている．第 4 章は機械学習をデザインパターンの考え方で分類を試みている．第 5 章は機械学習の品質に関することがコンパクトにまとまっている．第 6 章は説明可能な AI（Explainable AI）のまとめである．第 7 章は，AI 倫理についてであるが，AI の説明可能性，透明性，アカウンタビリティ，公平性，バイアスなど，AI 特有な倫理課題がまとまっている．

第 IV 部は，第 8 章「機械学習と知財・契約」で AI 特有の知財や契約に関する項目がまとまっている．

第 V 部は，第 9 章「今後に向けて」で本書籍のこれより前の章で取り上げられなかったトピックの補足，将来展望である．プライバシーやセキュリティの問題はここで取り上げている．

本書籍は，新用語が多いが，内容は平易で一気に読み通せる．したがって，先に紹介した AI に関するガイドラインのような詳細ドキュメントに目を通す前にざっと最新事情を知るのにちょうどいい．しかし，先に紹介したガイドラインと同様，進歩が早く，アップデートが頻繁な領域なので，この書籍を踏み台に，色々なドキュメントやガイドラインを追いかけていく起点とするのがいいと考える．

本書籍をだれに薦めるか

本書は，AI の品質管理や，説明可能性，倫理やコンプライアンスに関する総まとめのような本である．実際の AI や機械学習の導入や運用を担当するようになった現場に近い技術者に，お薦めできる．また，新規事項を広く浅くまとめているので，関連事項をざっとおさらいしたい，研究者や大学院生，学生にも適すると思われる．

参考文献

1）石井一夫：ビブリオ・トーク —書評—：ソフトウェア工学から学ぶ機械学習の品質問題，情報処理，Vol. 62, No.11, pp.626-627（Nov. 2021）．
2）石井一夫：5 分で分かる !? 有名論文ナナメ読み：Marco T. Ribeiro et al. “Why Should I Trust You?”：Explaining the Predictions of Any Classifier, 情報処理，Vol.62, No.10, pp.568-570（Oct. 2021）．
3）野ヶ山尊秀，丸山　宏：機械学習工学：編集にあたって，情報処理，Vol.60, No.1, pp.10-11（Jan. 2018）．
4）中島　震，中谷多哉子，滝澤真一朗：AI の品質保証：編集にあたって，情報処理，Vol.63, No.11, pp.602-605（Nov. 2022）．
5）AI プロダクト品質保証ガイドライン，https://www.qa4ai.jp/download/（2022 年 9 月 1 日閲覧）
6）機械学習品質マネジメントガイドライン 第 3 版を公開 https://www.ai-japan.go.jp/ai-and-society/privacy-and-security/post-149/（2022 年 9 月 1 日閲覧）

（2022 年 9 月 1 日受付）

石井一夫（正会員） kishii@rs.sus.ac.jp

公立諏訪東京理科大学工学部情報応用工学科教授，久留米大学医学部内科学講座心臓・血管内科部門客員准教授．専門分野：ビッグデータ分析，計算機統計学，データサイエンス．医療ビッグデータ，気象ビッグデータ，金融ビッグデータ研究に従事．2015 年度情報処理学会優秀教育賞受賞．研修認定薬剤師，日本技術士会フェロー，APEC エンジニア，IPEA 国際エンジニア．