AI Safety & Security の研究・標準化動向：欧州編

櫻井　幸一 [1,]　　溝口誠一郎 [2]

概要：人工知能の安全性とセキュリティに関する欧州の研究と標準化動向を報告する。

キーワード：AI 機械学習 セキュリティ 自動運転 セキュリティ評価・監査

European Trends of Research and standardization of AI Safety and Security

Kouichi SAKURAI [1]　　Seiichiro MIZOGUCHI [2]

Abstract: This note reports on research and standardization trends in Europe on the safety and security of artificial intelligence.

Keywords: AI, Machine learning, Security, Autonomous driving, Security Evaluation/Audit

1. はじめに

欧州委員会(European Commission, EC)は 2021 年 4 月に「欧州 AI 規則案」を発表した[1]。人工知能(AI)はビジネス展開が進み、日常生活への利活用が期待される今日、欧州 AI 規則案は、世界で初めての AI の法的枠組みに関する提案である。AI に関係する規制は、国ごとに対応が検討されている現状で、欧州の AI 規則が、今後及ぼす世界的な影響を勘案し、本稿では、欧州の動向を主体に報告するものである。

情報通信産業団体であるデジタルヨーロッパ[2]は AI 規則案の発表後、懸念を表明した：最新技術の応用など迅速さが要求される AI ソフトウエアが、規則案/規定要件についての適合性評価の対象に含まれたことに関して。また、法案で高リスクと指定された分野へのベンチャー企業参入が減る可能性があるとして、中小企業が規定要件を満たすべく、企業向けガイドラインや財政支援が必要になるとも指摘した。欧州機械・電気・電子・金属加工産業連盟（Orgalim）[3] も「AI システム」の定義をより明確にすることや、産業用 AI が高リスクとみなされないことを保証するため、産業界と協力して、堅固な法的確実性を与えることを求めた。さらに、適合性評価の義務化は、企業の負担を増やし、必ずしも安全性を高めることにはつながらないとも表明した。しかし、両団体とも、欧州委委員会の「欧州 AI 委員会（European AI Board）」創設案には賛同し、官民双方から平等に幅広く参加者を募り、産業界の知見が反映され、規制の削減や規則の円滑な実施につながることには期待している。

この「欧州 AI 規則案」が正式に法律化されれば、世界の先駆けとなる。早ければ 2024 年にも全面施行になる可能性がある。

European Telecommunications Standards Institute, ETSI（欧州電気通信標準化機構)[4] は、情報通信技術に国際的に適用できる標準を作成している欧州における電気通信全般にかかわる標準化組織として、欧州連合が後援している。人工知能の保護に関する ETSI 内業界仕様グループ Industrial Study Group Securing AI（ISG SAI)は、(1) AI を使用してのセキュリティ強化 (2) AI を活用した攻撃の緩和 (3) 攻撃に対する AI 自体の保護 の 3 つの主要分野に焦点を当てている。 ETSI ISG SAI は、AI の成長とともに活動し、人工知能のセキュリティを維持および改善するための標準を作成する。2020 年 12 月には問題声明書（Problem Statements）を発表し、最新では AI セキュリティにおける HW の役割を調査しており、5つの報告書を公開している:

(2022-03) AI のセキュリティにおけるハードウェアの役割
(2022-01) AI 脅威オントロジー
(2021-08) データ サプライ チェーンのセキュリティ
(2021-03) 緩和戦略レポート
(2020-12) 声明文

ENISA (European Network and Information Security Agency：欧州 ネットワーク情報セキュリティ庁)[5]は、2020 から 2021 年にかけて、たて続けに AI セキュリィに関する報告書を発表した。

2021. Feb. 人工知能を使った自律走行におけるサイバーセキュリティの課題
2020 Dec. 人工知能サイバーセキュリティの課題
2020.June 人工知能サイバーセキュリティに関するワーキンググループが始動

1 九州大学　Kyushu University
2 DNV アシュアランス・ジャパン　DNV Assurance JAPAN

ENISA は、もとは欧州ネットワーク情報セキュリティ庁が、2019 年に、欧州サイバーセキュリティ法が施行されて、その名称を変更、組織として格上げされており、「トラストがありサイバー安全な(secure)欧州」という新戦略を公表している。同法は、ENISA を恒久的な機関とするとともに、サイバーセキュリティの認証の仕組みの枠組を準備するものとなっている。

2020 年 3 月、ENISA は人工知能（AI）サイバーセキュリティに関するアドホック専門家グループの募集を開始し、学際的な専門家グループを集めた。(同じレベルでもう一つの WG:新興と将来のサイバーセキュリティの課題予測アドホック ワーキンググループも設置している)。このアドホック ワーキング グループの役割は、人工知能に関連するサイバーセキュリティ関連の話題について ENISA に助言することとしている。このアドホック ワーキング グループは、当初は1年間としているが、作業の範囲が 1 回で完了しない場合、このアドホック ワーキング グループの任務の延長が可能とも述べている。このワーキングの活動の一環として、2021 年 12 月には Securing Machine learning Algorithms と題した報告書を公開している。
後に

2. 産学の研究動向

DNV の研究者 Simen ELDEVIK 博士[5+]は、2018 年に「AI + 安全：人工知能の安全性への影響−因果モデルとデータ駆動モデルを組み合わせる必要がある理由」を DNV のホームページに公開している[5++]: 「最も高度なアルゴリズムがどのように機能するかを実際に、知っている人は誰もいない。コンピュータが重要な決定を下す責任を負うようになるにつれて、これは深刻な問題になる可能性がある。」

3. 最後に

欧州は GDPR（一般データ保護規則）2018 年 2 月の時点で[6]「自動化された個人意思決定とプロファイリングに関する規則 2016/679 のためのガイドライン（Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679）」で、AI 利用規定を示唆していたといえる。自動運転をはじめ、国内企業の海外展開だけではなく、我々の日常生活への影響までも考える時期になってきた。
欧州の自動車一般安全規則(Vehicle General Safety Regulation)の動向も注視すべきである。2022年8月現在、米国のプレス[7]は、EU（欧州連合）が自動運転レベル 4（高度運転自動化）の販売を認める法案を提案する見込みだと報じた。

謝辞

本研究は DNV アシュアランス・ジャパンの支援と人工知能の安全性とセキュリティに関する研究協議会[a-x]の協力を受けています。

参考文献

[1] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS (COM/2021/206 final)
[2] http://www.digitaleurope.org
[3] https://orgalim.eu
[4] https://www.etsi.org
[5] https://www.enisa.europa.eu
[5+] https://scholar.google.com/citations?user=2uuF-AwAAAAJ&hl=en
[5++] https://ai-and-safety.dnvgl.com/#sec-summary
[6] https://gdpr.eu
[7] https://www.politico.eu/article/eu-plans-to-approve-sales-of-fully-self-driving-cars/
[8] The new Vehicle General Safety Regulation https://ec.europa.eu/commission/presscorner/detail/en/IP_22_4312
[9] 丸山：情報セキュリティ日記 http://maruyama-mitsuhiko.cocolog-nifty.com/security/
[10] 松田弁護士 欧州 AI 規則案の概要 https://businessandlaw.jp/articles/a20220101-1/
[11] 江川尚志: AI の倫理とトラストの標準化動向 通信学会論文誌 2021

[a1] MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
[a2] https://www.ai.gov/naiac/
[a2+] https://www.nhtsa.gov
[a-n] https://www8.cao.go.jp/cstp/ai/index.html
[a3] https://www.meti.go.jp/policy/it_policy/ai-governance/index.html
[a4] http://www.keidanren.or.jp/policy/2021/069.html?v=p
[a5]https://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/index.html
[a6] https://www.mhlw.go.jp/stf/shingi/other-kousei_408914_00001.html
[a7] 石村耕治「EU の包括的 AI 規則始動」TC フォーラム研究報告 2021 年 5 号（http://tc-forum.net/）
[a8] https://www.jetro.go.jp/world/reports/
[a-x] Open RDG-AI/SS （https://sites.google.com/view/openrdg-aiss/Home ）

付録

A-US: 米国政府は 2020 年 1 月に、民間部門における AI 技術の開発と利用規定を目的とした 10 項目の規制原則[a1]を公開した。これは過度の規制が AI の発展の妨げにならないようにしたい考えと読める。さらに、米商務省は 2021 年 9 月、AI に関連する問題一般に関して、大統領や連邦機関に助言する全国 AI 諮問委員会(NAIAC)の設置を発表した。この AI 諮問委員

会[a2]は、Google や CMU など産学から次の 27 名の委員を招いて、現在活動をしている:

1. *Miriam Vogel (Chair), Equal AI*
2. *James Manyika (Vice Chair), Google*
3. *Zoë Baird, Markle Foundation*
4. *Yll Bajraktari, Special Competitive Studies Project*
5. *Amanda Ballantyne, AFL-CIO*
6. *Sayan Chakraborty, Workday*
7. *Jack Clark, Anthropic*
8. *David Danks, University of California at San Diego*
9. *Victoria A. Espinel, BSA*
10. *Paula Goldman, Salesforce*
11. *Susan Gonzales, AIandYou*
12. *Janet Haven, Data & Society*
13. *Daniel E. Ho, Stanford University*
14. *Ayanna Howard, Ohio State University*
15. *Jon Kleinberg, Cornell University*
16. *Ramayya Krishnan, Carnegie Mellon University*
17. *Ashley Llorens, Microsoft*
18. *Haniyeh Mahmoudian, DataRobot*
19. *Christina Montgomery, IBM*
20. *Liz O'Sullivan, Parity AI*
21. *Fred Oswald, Rice University*
22. *Frank Pasquale, Brooklyn Law School*
23. *Trooper Sanders, Benefits Data Trust*
24. *Navrina Singh, Credo AI*
25. *Swami Sivasubramanian, Amazon Web Ser*
26. *Keith Strier, NVIDIA*
27. *Reggie Townsend, SAS*

米国は、自動車や運転者の安全を監視する米国運輸省の部局 National Highway Traffic Safety Administration(NHTSA) を 1970 に設置している[a-2+]。自動運転のガイダンスを発表するとともに、最近では自動運転と ADAS の事故レポートも公開している。

A-J. 国内

内閣府では 2021 年より新 AI 戦略会議が開かれている[a-n]
経済産業省は AI 社会原則の実装に向けて、国内産業競争力の強化と、AI の社会受容に関する規制・標準化・ガイドライン・監査等、日本の AI ガバナンスの在り方の検討をはじめている[a3]
経団連も 2022 年 7 月に欧州 AI 規制法案に対する意見を発表している[a4]。
総務省は、平成 28 年 6 月より AI ネットワーク社会推進委員会[a5]を発足させている。
厚生省は、2018 年 7 月より保健医療分野におけるAI開発の方向性に関する検討をはじめ、保健医療分野 AI 開発加速コンソーシアム[a6]として現在に至っている。

欧州の AI 規則案に関して、省庁関係の調査資料も豊富であるが、石村の報告書[a7]は、「EU の顔認証情報利用禁止を含む AI(人工知能)規制案を読む:EU のプライバシー侵害 AI パンデミック対策ワクチン」と題する 60 ページに渡る調査である。

AI 規則に限らず欧州の ICT 動向報告は、JETRO も詳しい[a8]。

【 この位置に改ページを入れ，以降のページを印刷対象外とする 】