

AI標準化・ルールメイクに関する動向と NECの取り組み

田部 尚志 本永 和広 島村 聡也 永沼 美保 ORTOLAN Francois FROST Lindsay

要 旨

NECは、AI技術の開発だけでなく社会実装のため、Institute of Electrical and Electronics Engineers (IEEE) や国際標準化機構/国際電気標準会議 (ISO/IEC)、欧州電気通信標準化機構 (ETSI) などの標準化団体における標準仕様の整備に貢献してきました。生成AIの登場を契機に、各国がAIに関する規制の強化に舵を切りつつあるなか、AIガバナンスに関連する標準が必要とされています。欧州、米国、日本国内の政策や、G7広島AIプロセスなど多国間の枠組みの動向、それに即したガイドライン整備、標準化の動向を解説します。また、関連するNECの取り組みについても紹介します。



生成AI/AIガバナンス/国際標準化/適合性評価/第三者認証/欧州AI規制/EU AI Act/NIST AI RMF

1. はじめに

生成AIの登場により、AIの潜在力と可能性が広く認知されるようになりました。同時に、これまでのプライバシー侵害や差別といったAIリスクに加え、ハルシネーション、知的財産の侵害など、新たなAIリスクへの懸念も高まり、課題が生じています。例えば、生成AIはユーザーのデータをもとに新たなコンテンツを作り出す能力があるため、個人のプライバシーや知的財産の尊重と保護に関する問題が浮上しています。またAIが生成したコンテンツの真偽や適切な利用、透明性も求められています。

これを受けて各国政府は、AIのガバナンスに関する規制の強化に舵を切りつつあります。現在はガバナンス原則やポリシーの実践段階に入っており、さまざまな枠組みでの検討が進んでいます。

社会や国際的なコンセンサスの形成が進むなか、本稿では、AIガバナンスに関するいくつかの枠組みや標準化の動向について紹介し、NECの関連する取り組みについて解説します。

2. AIガバナンスに関する社会ルールの形成

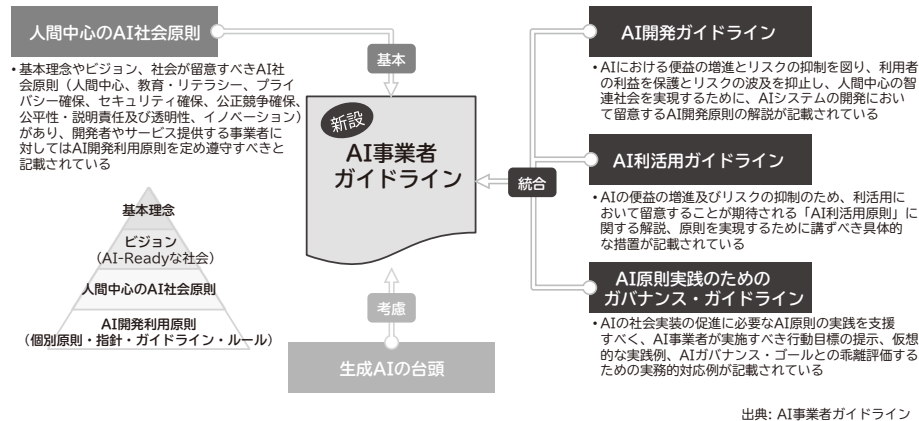
AIは人間のように予測や判断、認識などに利用されるなかで、透明性、公平性、プライバシー侵害、セキュリティ、説明責任などの課題を生じさせる可能性があります。加えて、生成AI・基盤モデルの登場により、著作権など知的財産権侵害、ハルシネーション（誤った情報の生成）やバリューチェーンによる信頼性担保などの課題にも新たに焦点が当たりました。

社会で安全・安心にAIを活用するためには、これらの課題に適切に対処するAIガバナンスが必要になります。各国・地域でこのための社会ルール作りが進んでいますが、先端技術の規制については国・地域によりアプローチが異なります。

2.1 欧州AI規制

2021年4月に公表された欧州AI規制（以下、EU AI Act）案は、世界初のグローバルな包括AI規制であり、ブリュッセル効果と言われる、欧州連合（以下、EU）以外の地域へ与える影響力の大きさからも注目されています。

規制内容は「ハイリスクAIシステム」の提供者に対する要求や義務を中心に構成されており、ハイリスクAIシステ



出典: AI事業者ガイドライン

図1 日本における取り組みの概要

ムには、一部の生体認証システムも含まれます。

EUの立法手続きの過程を経て、基盤モデル提供者の義務や生成AIに対する要求事項なども新たに盛り込むことが2023年12月に合意されました。また、欧州AIオフィスが設置されガバナンスを監督するとともに、AIの性能の評価基準作りにも取り組みます。法律の最終合意は、2024年夏となる見通しです。法律と連携して策定される整合標準については、第3章にて詳述します。

2.2 米国の動向

米国は有数の大手AI企業を有し、かつ伝統的に民間の自主統制を尊重する傾向でありながら、同時に規制の必要性も検討しています。

2023年1月に米国国立標準技術研究所（以下、NIST）がAI技術のリスク管理のための文書として、AIリスクマネジメントフレームワーク（AI RMF）を発表しました。その後、ホワイトハウスは信頼できるAIに関する大統領令（2023年10月）にて、連邦政府調達や国防利用に関する指針を明確化しました。一方、議会では包括的なAI法制や規制強化の議論が進展し、有力AI企業と対話しつつAIに関する連邦法制や規制機関設置の必要性の検討が進んでいます。国防、サイバーセキュリティや労働者保護、選挙制度への影響、高機能AIによる人類絶滅リスクなどに対応することが規制導入の論点となっています。

2.3 日本における取り組み

日本のAI規制の取り組みは、法律による規制、いわゆ

表1 国際・多国間枠組の最新動向: G7広島AIプロセス 11の指針と行動規範

指針	行動規範
1. AI ライフサイクルにわたるリスク低減	ライフサイクルでのリスク緩和とトレーサビリティ。レッドチーム評価などのAI テスト手法。兵器開発、サイバー攻撃、安全リスク、プライバシー、民主主義への脅威、システミックリスク。
2. 導入後の脆弱性・インシデント対策	市場導入後もリスク緩和措置を講じる必要性(バグ報奨金などインセンティブ設計も含む)。
3. 高度 AI システムの情報開示・透明性	生成 AI などの高度 AI システムの十分な情報開示と透明性(リスク評価結果、性能限界、適合性評価結果)。
4. 組織間情報共有とインシデント報告	AI ライフサイクルに携わる組織間での情報共有、インシデント報告、AI 信頼性メカニズムの共創。
5. 組織レベルで AI ガバナンスを実装	組織で個人情報保護などのリスク緩和策を策定、AI ガバナンスプロセスとリスク管理システムを実装。
6. AI のセキュリティを強化する投資	ライフサイクル全体にわたる物理的セキュリティ / サイバーセキュリティ / 内部脅威対策への投資。
7. 電子透かしなどコンテンツ認証や来歴管理メカニズムの開発	AI が生成したコンテンツを識別できるようコンテンツ認証と来歴メカニズムを研究開発、ツールや API を提供導入すべき。来歴にはコンテンツを作成したサービスや機械学習モデルの識別子を含める。
8. AI リスク低減のための研究・投資を優先	組織は、社会的・安全・セキュリティ上のリスクを軽減する研究やリスク緩和策への投資を優先し、社会と共有することが奨励される。
9. グローバル課題(気候変動や教育・医療など)に優先的に AI 技術を適用	SDGs の進歩を支援し、グローバルな利益のための AI 開発を奨励(特に気候危機、世界保健、デジタルリテラシーなど)。
10. 国際技術標準の開発と採用の推進	テスト方法、コンテンツ認証、来歴メカニズム、サイバーセキュリティポリシー、情報公開などの手段を開発する際に国際標準開発組織(SDO)と協力することを奨励。特にコンテンツ認証の国際的な技術標準や枠組を奨励。
11. 訓練データの品質管理と知的財産保護	有害な偏見を軽減するために、訓練データやデータ収集など、データの質を管理するための適切な措置を奨励。またプライバシー保護、情報セキュリティ、著作権コンテンツのための保護の措置を奨励。

るハードローではなく、ガイドラインなどによるソフトローで行われてきました¹⁾。内閣府が「人間中心のAI社会原則」(2019)を発表し、総務省、経済産業省などが複数のAIガイドラインの整備を進めた後、2024年にG7広島AIプロセスによる多国間枠組みとも整合のうえで、「AI事業者ガイドライン」として統合することになりました(図1)。AIをめぐる動向は目まぐるしく変化していることが

ら、定期的な更新が期待されます。NECも、本ガイドラインをベースとした社内ガバナンスを実践しています。

また、適合性評価・認証制度やリスクの高い8分野（政府、金融、エネルギー、運輸、交通、電気通信、放送、医療）における個別ルール作りも検討されています。

2.4 多国間枠組み

AIのもたらす課題への認識は広く共有されており、AIに関するルール of 国際的な整合が求められています。

2023年5月に行われたG7広島サミットでは、相互運用可能なAIガバナンスの重要性に合意しました。特に知的財産や偽情報など生成AIがもたらすリスクに取り組む「G7 広島AIプロセス」において、11の国際指針とAIシステム開発者を対象とする行動規範が定められ（表1）、2023年末に包括的な政策枠組みを合意するなど、日本が国際的議論を主導しています。

3. AIガバナンス関連の標準化動向

AIガバナンスのための相互運用可能なルールが必要とされ、そこには技術的詳細が含まれ得ることから、標準化が重要な役割を果たすことが期待されています。ここでは、欧州標準機関と国際標準による標準化の動向を概観します。

3.1 欧州における整合標準の開発

EU AI ActはNLF (New Legislative Framework) の立法形式で制定される予定であり、整合標準、認証、監査、市場調査を参照する法律により構成されます。主に欧州標準化機関（欧州電気通信標準化機構（以下、ETSI）、欧州標準化委員会（CEN）、欧州電気標準化委員会（CENELEC））によって開発され、欧州規格（EN）及び

表2 横断的なAI規制要求10項目

Reference information	
1	European standard(s) and/or European standardisation deliverable(s) on risk management systems for AI systems
2	European standard(s) and/or European standardisation deliverable(s) on governance and quality of datasets used to build AI systems
3	European standard(s) and/or European standardisation deliverable(s) on record keeping through logging capabilities by AI systems
4	European standard(s) and/or European standardisation deliverable(s) on transparency and information provisions for users of AI systems
5	European standard(s) and/or European standardisation deliverable(s) on human oversight of AI systems
6	European standard(s) and/or European standardisation deliverable(s) on accuracy specification for AI systems
7	European standard(s) and/or European standardisation deliverable(s) on robustness specifications for AI systems
8	European standard(s) and/or European standardisation deliverable(s) on cybersecurity specifications for AI systems
9	European standard(s) and/or European standardisation deliverable(s) on quality management systems for providers for AI systems, including post-market monitoring processes
10	European standard(s) and/or European standardisation deliverable(s) on conformity assessment for AI systems

整合標準（Harmonised Standards）としてEU官報に掲載される技術標準は、製造業者が市販試験の一環として引用することができ、またEU AI Actの要求事項に適合した製品として販売することができます。このように整合標準は、法律と組み合わせることで効力を発揮します（図2）。

欧州委員会（EC）はAI規制に関する標準化要求（M/593）を発行し、横断的なAI規制要求10項目に関する標準の開発を求めました（表2）。これにはAIによるリスクを回避、最小化するためのリスク管理システムの標準仕様、データガバナンスと品質、サイバーセキュリティ、品質マネジメントシステム、適合性評価などが含まれます。

これを受け、CEN/CENELEC JTC21委員会（以下、JTC21）は、まず規制要求10項目に内在する構造を明確化するために標準化アーキテクチャを作成し、既存標準の活用も検討しつつ新たに開発が必要な標準を見極めるためのギャップ分析を実施しました。

JTC21のJoint Work Programmeの計画に従って進められる標準開発には、ETSIも協力します。NECは、ETSI理事会メンバーやOSG（Open Source Group）のAI委員会を主導するなどの取り組みを通じて、通信やサイバーセキュリティ分野でのAI関連標準の必要性について長年取り組んでいます。

現時点では標準策定のデッドラインは、2025年5月22日に設定されています。新たに開発が必要な標準仕様がいくつもあり、標準化のための作業量が多いため、国

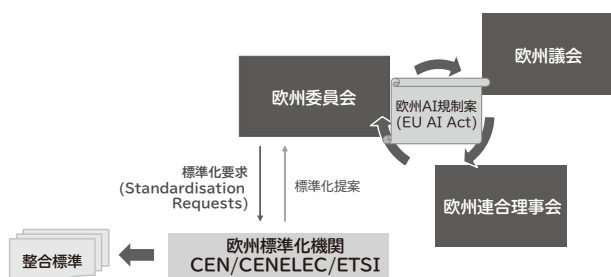


図2 欧州での整合標準

国際標準化機関ISO/IEC JTC1などの国際標準が多く採用されることが予想されます。今後、大規模言語モデル(LLM)や基盤モデルに関する標準化要求が追加される見通しもあります。EU AI Actの施行前にすべての標準を提供することは困難であるため、リスクアセスメント標準を優先するなど、段階的な標準仕様のリリースも検討されています。また、医療分野などの分野別立法との整合性も求められています。

3.2 国際標準化の動向

ISO/IEC JTC1配下に設立された分科委員会SC42(Artificial Intelligence)において活発に国際標準化が行われていますが、なかでもAIガバナンスに関連する標準が先行しています。欧州などの地域標準よりもいち早く始まった取り組みが、注目を集めています。

例えば、作業部会WG2におけるデータ品質の標準、WG3とJWG2によるAIシステムの品質や試験方法の標準(TS29119-11)など、信頼性に関する標準が策定されています。また、JWG4では日本提案のTR5469をベースとしたAI安全性要件に関する標準を、制御機器の機能安全の標準化を行うIEC TC65 SC65A委員会と共同で開発しています。

日本は、SC42(AI)の設立時期から、国立研究開発法人産業技術総合研究所(以下、産総研)を中心に積極的に国際標準化に関与しています。NECもSC42委員会やその国内専門委員会で活動し、WG3やWG5の国内主査、AIの安全性のプロジェクトエディタを務めるなど貢献しました。

米国では、AIのリスクへの効果的な対処のために国際標準の活用や専門家の参加が求められています。EU AI Actでは、前述で示したように国際標準が採用される方向性が示されています。例えば、ISO/IEC 42001はAIシステムを管理するためのAIマネジメントシステムへの要求事項の標準規格(AI MSS)で、さまざまな枠組みで必要性が指摘されている適合性評価のベースとなります。更に、第三者認証制度に関する検討も始まっています。

4. NECの取り組み

NECは、技術開発だけでなく標準化や法制度・ルール作りにも取り組んでいます。

AIガバナンスに関連する取り組みとしては、米国のInstitute of Electrical and Electronics Engineers(IEEE)におけるAI倫理プロジェクト(P7001)を主導し、またNISTのAIリスクマネジメントフレームワークの整備プロセスでは意見を提出しました。

欧州では、ETSIでのポジションを活用し、欧州AI白書やEU AI Actにて参照する標準化に関する提言活動に取り組んでいます。

国内では、各種公的ガイドラインの整備にエキスパートが参画し貢献してきました。国際標準をベースとしたJIS原案作成にも取り組んでいます。また、品質要件に関する系統的・網羅的な枠組みである産総研AIQMの「機械学習品質マネジメントガイドライン」の策定に参画しています。

他にも国連やEUのイベントに参加し、グローバルな啓発活動にも力を入れています。

5. おわりに

NECは、生成AIや生体認証、サイバーセキュリティ対策などの最先端の要素技術を保有しており、これらを組み合わせることで社会課題の解決に取り組んでいます。このため、グローバルな標準化にも積極的に取り組んできました。

AIのリスクを効果的に管理し、グローバル市場の形成を実現するためには、相互運用可能な社会ルールの基盤となる標準化が重要な役割を果たします。社会がAIを安全・安心に活用するには、ガバナンスの仕組みや技術の発展を欠かすことはできません。

参考文献

- 1) 市川 類: 世界の人工知能(AI)ガバナンス制度の進化メカニズム ~技術と制度の共進化の中での地域的多様性による制度イノベーションの進展~, 一橋大学イノベーション研究センター, 2023.3
<https://hermes-ir.lib.hit-u.ac.jp/hermes/ir/re/79802/070iirWP23-01.pdf>

執筆者プロフィール

田部 尚志

グローバルイノベーション戦略統括部
プロフェッショナル

本永 和広

グローバルイノベーション戦略統括部
ディレクター

島村 聡也

デジタルトラスト推進統括部
デジタルトラスト推進統括部長

永沼 美保

デジタルトラスト推進統括部
主席プロフェッショナル

ORTOLAN Francois

NEC Laboratories Europe
Senior Standardisation
Engineer

FROST Lindsay

NEC Laboratories Europe

関連URL

欧州AI規制案（EU AI Act）

<https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence>

EC Standardisation Request M/593 on Artificial Intelligence

[https://ec.europa.eu/transparency/documents-register/detail?ref=C\(2023\)3215&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en)

内閣府 AI 戦略会議

https://www8.cao.go.jp/cstp/ai/ai_senryaku/ai_senryaku.html

NEC 技報のご案内

NEC 技報の論文をご覧くださいありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）

NEC Technical Journal（英語）

Vol.75 No.2 ビジネスの常識を変える生成AI特集 ～社会実装に向けた取り組みと、それを支える生成AI技術～

ビジネスの常識を変える生成AI特集によせて
生成AI技術への取り組み ～基盤から応用、ルール作りまで～

◇ 特集論文

急速に広まる生成AIの市場適用

NECにおける生成AIの取り組みについて
電子カルテと医療文書の作成支援による医師業務効率化
映像×LLMによる報告書作成業務の自動化
映像分析と生成AIによるリアル世界の行動理解
サイバー脅威インテリジェンス生成自動化
生成AIの社内活用を進めるNEC Generative AI Service (NGS)
ソフトウェア・システム開発への生成AIの活用
LLMとMIで革新する素材開発プラットフォーム
LLMと画像分析を活用した被災状況の把握

生成AIの可能性を高める基盤技術

日本語性能に優れたNECの大規模言語モデル (LLM)
NECの生成AIを支える国内企業で最大規模のAIスーパーコンピュータ
より安全な大規模言語モデル (LLM) を目指して
データを秘匿したまま連携できる連合学習技術とLLMへの適用可能性
大規模言語モデル (LLM) によるFew-shotクラスタリングの可能性
オープンドメイン常識推論のための知識拡張型プロンプト学習
AI連携とオーケストレーションのための基盤ビジョンLLM
クエリを考慮した新規手法により関連する企業データを減らしLLM APIの使用コストを最適化

AI技術が社会へ浸透するために

AI標準化・ルールメイクに関する動向とNECの取り組み
人権尊重に向けたNECのAIガバナンスの取り組み
RCModelを用いたAIリスクマネジメントのための人材育成事例

◇ NEC Information

2023年度C&C賞表彰式典開催



Vol.75 No.2
(2024年3月)

特集TOP