

AI システムの認証制度に関する比較法的検討

～各国の現状と今後の検討課題～

京都大学 大学院法学研究科 法政策共同研究センター

羽深宏樹(京都大学 大学院法学研究科 法政策共同研究センター 特任教授)

高橋圭(京都大学大学院法学研究科・法政理論専攻・博士後期課程/弁護士)

Socol de la Osa David Uriel(一橋大学 社会科学高等研究院 准教授)

インデックス

はじめに	3
本報告書の目的	3
本調査の経緯及び本報告書の対象	4
本報告書の構成	4
1. 認証の構造	6
(1) 既存の認証制度の枠組み	6
(i) プロダクト認証	6
(ii) マネジメントシステム認証	6
(iii) オペレーター認証	6
(2) AI を認証する際の課題	7
2. 各国の比較分析	8
(1) 自動運転車	8
(i) 日本	8
(ii) アメリカ	10
(iii) EU	11
(iv) 英国	14
(2) 医療機器	17
(i) 日本	17
(ii) アメリカ	19
(iii) EU	21
(iv) 英国	23
3. AI 認証における主な発見と今後の課題	26

(1) 比較分析の主な結果	26
(i) 自動運転車.....	26
(ii) 医療機器.....	26
(2) 今後の検討課題.....	27
(i) AI に対する認証の制度的枠組み.....	27
(ii) 認証の方法.....	28
(iii) 認証機関の在り方	29
(iv) 認証と責任制度の関係	29
別紙 1 各国の法的認証制度に関する初期調査	30
1. 結果の概要.....	30
2. 調査結果.....	31
別紙 2 EU:ハイリスク AI システムに関する AI 法の要件の概要.....	44

はじめに

本報告書の目的

近年、AI システム¹が多くのタスクについて人間と同等の(あるいはそれ以上の)高度な性能を有するに至っており、その結果として AI による人間の業務への代替があらゆる分野で進んでいる。これに伴い、AI システムに対する信頼確保の一つの方法として、認証(Certification)への期待が高まっている。認証とは、製品、プロセス、サービス、又はシステムが、指定された要求事項又は規格に適合していることを、独立した組織が評価し、検証する正式なプロセスをいう²。AI システムは、高度な自律性、人間の判断への影響の大きさ、そして複雑な機械学習がもたらす予測不可能性や説明不可性といった特徴を有するため、一般に第三者が AI システムの安全性や信頼性を判断することは難しい。そのため、独立の専門家が AI システムに認証を付与し、客観的に信頼性を担保することに対するニーズは、従来型のシステムに比較しても大きいといえる。しかし、まさにそのような AI システムの特徴ゆえに、AI システムの認証には、従来型のシステムにはない困難な課題が伴う。

従来の認証は、一般的に明確に定義されており、予測可能なパラメータと確立されたフレームワークの中で動作する製品、プロセス、又はシステム(ウォータールシステム)を対象としていた。それは、安全性、品質、信頼性を保証する正確で測定可能な基準に依存しており、関連するリスクが明確に理解された上で適用される。例えば、伝統的な自動車や医療機器については、その性能や安全性、すなわち自動車の衝突抵抗や医療機器の効果について一定の閾値が規定されており、これによって直接的なリスク評価と軽減策の評価が可能となっている。

他方で、AI システムは、従来の技術とは異なり、機械が学習データに基づき極めて複雑なアルゴリズムを自律的に構築する。そのため、挙動の予測や説明が事実上不可能であり、信頼性判断の基準を一律に固定することが困難である。また、自動運転車が直面する無限の交通状況や、AI 支援医療機器による予期せぬ医療合併症など、対処しなければならないリスクのシナリオや不確実性も各段に多い。さらには、AI はデータ、ソフトウェア、ハードウェア、そして人間との相互作用といった多様な要素を統合して機能するものであり、これらの複数の構成要素の相互作用は、各システム単独の機能だけでは予測できないリスクをもたらす。

本報告書は、このような多くの課題を伴う AI システムの認証について、主要国における法制度を横断的に比較することで、異なる分野や国に共通する制度の枠組み及び今後議論されるべき事項を抽出し、もって我が国としてあるべき AI ライセンスの姿、及び異なる国家間協力の可否について検討する際の示唆を得ることを目的とするものである。

¹ AI の定義については、OECD が提示する以下の定義に従う。「明示的又は暗黙的な目的のために、受け取った入力から予測、コンテンツ、レコメンド、物理的又は仮想環境に影響を与え得る決定の出力を生成する方法を推測する機械ベースのシステム。実装後の自律性と適応性のレベルは、個別の AI システムによって異なる。」

² <https://www.iso.org/certification.html>

本調査の経緯及び本報告書の対象

本報告書の作成にあたっては、まず、モビリティ(自動運転車)・医療・金融・法務・生成 AI・労務の分野において、日本、EU、米国、英国、カナダ、シンガポール、及び中国について認証に関する法制度の初期的な調査を実施した(別紙 1)。認証は、自主的な取組として(法的義務としてではなく)取得されるものが多いが、本調査では、法令上要求される認証を対象とすることで、立法プロセスを経て確立された認証プロセスの比較検討を行うことができると考えた。

初期調査の結果、これら全ての国・地域において、自動運転車及び医療機器に関する AI システムの認証制度が存在することが確認された。他方で、金融・法務・労働分野の AI システムについては、AI システム自体に対する認証制度を導入する国・地域は少数にとどまった。また、生成 AI についても、EU 及び中国を除いては、具体的な立法に踏み切った国が見られなかった。

自動運転車及び医療機器において特に認証制度の発展がみられた背景には、(i)両分野において AI 技術の導入が急速に進んでいること、(ii)これらの分野は、AI の誤った判断が人命や安全に深刻な影響を及ぼしかねないハイリスクな性質を有していること、(iii)AI の登場以前から、これらの分野の製品について、厳格な規制の下で認証制度が存在していること、といった事情が考えられる。そのため、本報告書では、自動運転車 (Auto-nomous Vehicle: 以下、AV と表記することがある。) 及び医療機器 (Medical Devices: 以下、MD と表記することがある。) の分野を対象として各国制度の比較検討を行うこととした。

検討対象の法域としては、日本・米国・EU・英国という 4 つの国・地域を選定した。これらの国は、いずれも G7 のメンバーであり、民主的かつ技術的にも先進的であるために、日本にとって有益な制度比較を行うことができると考えられる。なお、EU については、AI 法によって、AV や MD のような伝統的な認証対象分野にとどまらず、「ハイリスク AI システム」として広い範囲で認証(適合性評価)が求められており、同法の一般的な認証制度のほか、AV と MD への同法の適用可能性等に関する解説を別紙 2 にまとめた。また、中国についてあては、制度整備が別途進んでいるものの、政治体制が上記 4 つの国・地域と大きく異なることから、横断的な制度比較の対象とはしなかった。

以上をまとめると、本報告書(本体)の検討対象は、以下のようになる。

- 目的: AI システムに関して法的に義務付けられた認証制度の比較
- 対象分野: AI を主たる機能として搭載した自動運転車及び医療機器
- 対象地域: 日本・米国・EU・英国

本報告書の構成

本報告書は、以下の 3 つのセクションから構成されている。

1. 認証の構造

製品、マネジメントシステム、オペレーターという 3 つの異なる対象に対する認証メカニズムの概要を説明する。

2. 各国の比較分析

AV 及び MD について、型式認証プロセスやリスクベースの試験プロセスなどの項目に焦点を当て、各国の認証制度の概要及びその共通点と相違点を分析する。

3. AI 認証における主な発見と今後の課題

2.での分析を踏まえ、AI システムの認証制度について現時点で共通する事項と今後検討されるべき課題を明らかにする。

1. 認証の構造

(1) 既存の認証制度の枠組み

ある製品やシステムを認証する場合、その対象としては、(i)製品(プロダクト)、(ii)マネジメントシステム、(iii)オペレーターという3つの階層に分類できる。

(i) プロダクト認証

プロダクト認証とは、製品そのものを評価し、規制機関が定めた技術仕様や性能基準に適合しているかどうかを審査するものである。

- **例:**(従来型の)自動車については、衝突試験、排ガス規制、ブレーキ性能などの安全基準を満たしていることが認証の対象となる。医療機器については、たとえば体温計や輸液ポンプについて、それぞれ体温を正確に測定すること、薬剤を正しい投与量で送達すること、及び米国におけるFDAの510(k)が要求する安全規制に準拠していること等が認証の対象となる。

(ii) マネジメントシステム認証

マネジメントシステム認証とは、リスクマネジメント、品質保証、継続的改善プロセスなどの組織のマネジメントプロセスと構造を評価するものである。

- **例:**自動車業界では、自動車メーカーがISO9001やIATF16949などの品質マネジメント規格に準拠していることについて認証を受けることで、同社が安全で信頼できる自動車の設計、試験、製造のための効果的なプロセスを維持していることが担保される。医療分野では、医療機器の品質マネジメントに関するISO13485が同様の機能を果たしている。

(iii) オペレーター認証

オペレーターに対する認証は、システムを操作・運用する個人が、技術を安全かつ効果的に使用するために必要な資格と技能を有していることを保証するものである。いわゆる「免許」である。

- **例:**従来型の自動車では、自動車のオペレーターである人間が、自動車を安全に運転する技能と知識を有することを証明する運転免許を取得しなければならないことがオペレーター認証にあたる。同様に、医療分野では、医師免許や診療放射線技師などの資格が、人工呼吸器やX線装置などの医療機器を操作するために必要となる。

(2) AI を認証する際の課題

以上のような既存の認証制度の枠組みを AI システムに適用する場合には、以下のような課題が生じる。

- プロダクト認証及びマネジメントシステム認証の限界

アルゴリズムの予測不可能性、外部環境との相互作用、システムの構成要素の複雑さといった AI の特徴は、従来のようなプロダクト認証のアプローチを極めて困難にする。従来、製品安全基準は、具体的で詳細な技術仕様に依存していた。しかし、AI システムの上述のような性質は、一律に固定された検証可能な技術的ベンチマークを確立することを困難にしている。その結果、継続的な安全性と信頼性を確保するためにメーカーが使用するプロセスとシステムの評価に重点を置くマネジメントシステム認証へのシフトが進んでいる。しかし、マネジメント認証にも限界がある。メーカーが強固な安全・品質プロセスを維持していることを保証することは、運用中の AI システムのリアルタイムの安全性や信頼性を直ちに保証するものではない。このようなリアルタイムの信頼保証は、データ入力に基づいて継続的に進化・適応する AI システムにとって特に重要であり、従来型のマネジメント認証では、実装後に発生する予期せぬリスクや突発的な挙動に対処できない可能性がある。

- オペレーターの自動化

さらに、AI は従来人間が担ってきたオペレーターの役割を代替するため、その機能についてどのような認証制度を導入するかも課題となる。従来のシステムでは、操作・運用の安全性や信頼性は運転手や医師のようなユーザー（人間）に依存していたが、AI による自動化によって、その機能の一部又は全部がシステムに置き換わる。この文脈では、「オペレーター」はエンドユーザーではなく、自動化システムをマネジメントする組織（自動車の製造者や医療機器のメーカー等）となる。こうした変化に伴って、新たなオペレーターがどこまでシステムのモニタリングに責任を負うのか、また、どのような方法によってそれを達成できるのかが問題となる。

以上のような課題を念頭に、次節では、各国の法整備の状況を概観する。

2. 各国の比較分析

以下では、自動運転車と医療機器に関する日本、アメリカ、EU、及び英国の規制における、AI認証の仕組みについて比較分析を行う。この比較分析に際しては、AIを用いた製品の市場への導入、製品の販売後の監督、及びコンプライアンスに関する各種の要件について定める規制枠組みに関する調査を行った。そして、かかる調査結果を、製品レベル、マネジメントシステムレベル、オペレーターレベル³という3つのレベルに区分の上で整理をして、各国の制度を比較することにより、規制枠組みに関する共通点と相違点を特定している。

(1) 自動運転車

(i) 日本

a. 製品レベル

日本においては、同一の規格で大量に生産される車両に関する国の新規検査の合理化を図り、かつ、新たに運行の用に供される車両1台毎の「保安基準」への適合性を確実に確保するための制度として、道路運送車両法により型式指定制度が採用されている⁴。具体的には、車両の製作者等は、販売しようとする車両について国土交通大臣による型式の指定を受けた場合には、当該指定を受けた車両を製作し、これの販売等をする場合には当該車両が保安基準に適合しているかどうかを1台ごとに検査（完成検査）し、保安基準に適合すると認める場合には完成検査終了証を発行することとされている。

こうした保安基準への適合が必要な車両の装置の1つとして、「自動運行装置」が定められている。この自動運行装置とは、国土交通大臣が付する条件（走行環境条件[ODD]）で使用される場合において、自動車を運行する者の操縦に係る認知、予測、判断及び操作に係る能力の全部を代替する機能を有するものとされている⁵。この保安基準の詳細は「道路運送車両の保安基準の細目を定める告示」（「細目告示」）において定められている。もっとも、その内容としては、「自動運行装置の作動中、他の交通の安全を妨げるおそれがないものであり、かつ、乗車人員の安全を確保できるものであること」、「自動運行装置が正常に作動しないおそれがある状態となった場合にあっては、車両を停止させることができるものであること」、「自動運行装置の機能について冗長性をもって設計されていること」といった抽象的なレベルの規律に留まっている⁶。

³ 本報告書においては「オペレーター」とは、広く自動運転車や医療機器を用いる者を意味するものとして用いており、例えば、自動運転車に関しては、レベル3までの自動運転車であれば「運転手」が、レベル4以上の自動運転車であれば、当該自動運転車を用いて事業を行う「運用事業者」が含まれる。

⁴ 道路運送車両法第75条。

⁵ 道路運送車両法第41条第2項。

⁶ 細目告示第72条の2参照。

なお、公道走行試験に当たっては、道路交通法上の道路使用許可⁷を取得する必要があるが、型式認証の場面に比して緩和された基準による運用がされている⁸。

b. マネジメントレベル

型式指定に当たっては、車両(装置)が保安基準に適合するかの上記の審査のほか、品質管理システム、完成検査、そして、自動運行装置を含む車両の装置の検査に関する業務組織・実施要領に係る書面を申請書に添付して、その審査を受けることとされており、型式指定を受けるためには、マネジメントレベルでの体制整備が必要となる⁹。ただし、法令で求められている内容は非常に抽象的な内容にとどまっており、具体的にどのような組織体制が求められるのかなどは明確には規定されていない¹⁰。

c. オペレーターレベル

レベル 3 までの自動運転車については、その運転について、運転免許が必要となる。免許を受ける主体は、ユーザーである運転手である。これに対して、ユーザーである運転者の存在を前提としないレベル 4 に相当する自動運転のうち一定の基準を満たすものの運行を可能とする制度が令和 4 年(2022 年)の法改正により創設された。この制度は、自動運転車を運行の用に供するユーザー以外の主体をオペレーターとしてその者に認証を与えるものであるが、その趣旨は、自動運転システムによる対応が困難な既存のルールについて、監視を行う責任者を置くなどして人間による遵守を義務付けることで、自動運転下においても従前のルールが遵守されることを確保するというものである。

令和 4 年(2022 年)の法改正の内容としては、まず、道路交通法の改正により「特定自動運行」の許可制度が創設された¹¹。具体的には、①特定自動運行を行おうとする者は、特定自動運行を行おうとする場所を管轄する都道府県公安委員会の許可を受けなければならないこととされ、また、②許可を受けた者(「特定自動運行実施者」)は、作動状態の監視を行うために「特定自動運行主任者」を配置した上で、特定自動運行計画に従って特定自動運行を行う義務を負うとともに、③特定自動運行主任者は、作動状態の監視のほか、交通事故があった場合必要な措置等を講じなければならないこととされた。また、道路運送法・貨物自動車運送事業法の改正により、特定自動運行を用いて旅客自動車運送事業又は貨物自動車運送事業を行う場合には、運転以外の業務を行う「特定自動運行保安員」を設置する必要があるとされた¹²。

⁷ 道路交通法 77 条。

⁸ 詳しくは、警察庁「自動運転の公道実証実験に係る道路使用許可基準」(令和 6 年 9 月)、国土交通省「遠隔型自動運転システム等を搭載した自動車の基準緩和認定要領」を参照。

⁹ 自動車型式指定規則第 3 条第 2 項第 4 号～第 6 号。

¹⁰ 通達(平成 10 年 11 月 12 日付け自審第 1252 号「自動車型式認証実施要領(依命通達)」)においても、完成検査の実施要領に関して、検査項目や検査ラインの工程図の記載が必要となるなど一定の具体化は図られているが、組織体制については「業務の担当部門等が明確となるよう記載すること。」といったレベルでの具体化が図られているにすぎない。

¹¹ 道路交通法第 75 条の 12 以下。

¹² 道路運送法施行規則第 51 条の 16 の 2 第 1 項、貨物自動車運送事業輸送安全規則第 3 条第 1 項など。

(ii) アメリカ

a. 製品レベル

アメリカでは、自己認証制度が採られており、自動車車両や自動車関連用品の安全基準については、国家道路交通・自動車安全法 (National Traffic and Vehicle Safety Act of 1966) に基づき、国家道路交通安全局 (National Highway Traffic Safety Administration :NHTSA) が、連邦自動車安全基準 (Federal Motor Vehicle Safety Standards: FMVSS) を制定している¹³。もっとも、連邦自動車安全基準 (FMVSS) は、2022 年 3 月に、レベル 4・5 の自動運転車を想定した若干の修正が加えられたものの¹⁴、現時点では、日本における自動運行装置に相当するような自動運転に関連する装置についての定めはない¹⁵。

このように連邦レベルにおいて自動運転車に関する定めが無いことから、自動運転に関するルールを各州が定めている。例えば、カリフォルニア州においては、その自動車法 (Vehicle Code (“VEH”)) において、自動運転車に関する章 (Division 16.6 Autonomous Vehicles) が設けられている。ここでは、公道で自動運転車を走行させるための許可要件の中で、自動運転技術が備えるべき性能等に関する定めが置かれているが、その内容としては、日本と同様、「自動運転車に、オペレーター (operator)¹⁶ が簡単にアクセスできる、自動運転技術の起動及び解除を行うための機構が備わっていること」¹⁷といった抽象的なレベルに留まっている¹⁸。

b. マネジメントレベル

日本では、前記 (i) b. のとおり、型式指定の際に、所定の品質管理体制等を整備することが要件とされているが、連邦自動車安全基準 (FMVSS) やカリフォルニア州・自動車法においては、こうした品質管理体制等は、要件としては挙げられていない。もっとも、自動車業界としては、品質マネジメントシステムに関する国際規格である ISO9001 や自動車産業に特化した品質マネジメントシステムに関する国際規格である IATF16949 の認証が取得されることが一般的であるようである。

¹³ 49 CFR Part 571.

¹⁴ Federal Register Volume 87, Issue 61 (March 30, 2022).

¹⁵ なお、連邦運輸省により自動運転技術の開発者や各州に対する法的拘束力のないガイダンス形式の Federal Automated Vehicles Policy (2016 年 9 月制定。2017 年 9 月改訂) が示されており、そこでは日本の自動走行装置の保安基準で挙げられている事項と同様の事項が、安全要素 (Safety Element) として挙げられている (https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf)。

¹⁶ 同法において、オペレーター (operator) とは、運転席に座っている者又は運転席に人がいない場合には自動運転技術を作動させる者のことを指すとされている (VEH §38750 (a)(4))。

¹⁷ VEH §38750 (c)(1)(a).

¹⁸ なお、2020 年に、産業界より、レベル 4 以上の自動運転車向けの UL4600 が発行されている (国家規格 ANSI として発行され、ANSI/UL4600 となっている。)

c. オペレーターレベル

カリフォルニア州においては、①試験目的での公道走行の許可制度のほか、②自動運転車の公道における製造者の従業員等以外の一般市民の利用又は商業利用目的での利用に関して、配備許可 (Deployment) の制度が定められている¹⁹。日本とは異なり、責任保険への加入等による一定額以上の賠償資力の確保が求められているほか、遠隔監視が必須とはされていない点が特徴的である²⁰。

(iii) EU

a. 製品レベル

EU における製品レベルに関する規制枠組みとマネジメントレベルに関する規制枠組みのいずれも、二重構造となっている。すなわち、まず、EU AI 法が、AI に固有の項目を包括的に規定しているため、これによる規制を受けることになる。加えて、ある分野に固有の項目は、当該分野に関する規制法による更なる規制を受けることになる(なお、この規制法も、EU AI 法に適応するのみならず、それ自体として AI の課題に対応するために変化している)。自動運転車に関する規制についての主な特徴としては、以下のものが挙げられる。

1. 2つの主要な規制構造:

EU においては、自動運転車に関して **2つの主要な規制構造** — 型式認証枠組み規則 (Type-Approval Framework Regulation: TAFR) と一般安全規則 (General Safety Regulation : GSR) — が存在している。これらの規則によれば、自動運転車及びその部品は、その販売又は使用の前に、必要な安全基準と技術基準の全てを満たして型式認証を取得しなければならない。

2. インテリジェントシステムの導入の義務付け²¹:

EU では、安全性を高めるために、自動運転システムにスマートテクノロジーを導入することが義務付けられている。これには、次のものが含まれる。

- a. 全ての道路運行車両(自動車、小型貨物自動車(vans)、トラック、バス): インテリジェント速度制御機能、カメラ又はセンサーによる後退検知、注意警告。
- b. 乗用車及び小型貨物自動車: 車線維持システムや自動ブレーキなどの追加機能。

¹⁹ CCR Title 13, Division 1, Chapter 1, Article 3.7 & 3.8.

²⁰ ただし、今後の改正に向けた非公式の改正草案では、遠隔監視を要求する条項が設けられている (Potential Draft Regulatory Language, §228.06. Requirements for Remote Drivers and Remote Assistants) (<https://www.dmv.ca.gov/portal/file/article-3-8-express-terms-pdf/> [最終閲覧:2024年12月23日])。

²¹ https://ec.europa.eu/commission/presscorner/detail/en/ip_22_4312

- c. バス及びトラック: 死角の認識を向上させる技術、歩行者や自転車との衝突を防止する警告装置、タイヤ空気圧モニタリングシステム。

3. レベル 3 自動運転車に関する規制:

高速道路上での運転手による運転を代替する自動運転(レベル 3 自動運転車)について、EU 法は、国連のレベル 3 自動運転車に関する新たな規則²²を参照する形で、国連の規則に準拠している。この規則による要件は主として技術的なものである。

4. レベル 4 自動運転車の規制:

欧州委員会は、完全自動運転車(レベル 4 自動運転車。例えば、都市内での自動運転)のための技術的な型式認証に関する法律を採択した。技術規則は、委任規則(delegated act)²³及び実施規則(implementing act)²⁴を通じて定められているが、これは、完全自動運転車が EU 市場に導入される前に、その安全性と市場への導入の可能性に関して包括的な評価を行うものである。この規則は、テスト手順(衝突テスト、燃料システムの完全性、ブレーキ)、サイバーセキュリティに関する要件、データの記録に関するルール、そして、完全自動運転車の製造者に対する安全性能の監視と事故報告に関する要件などをカバーしている。

なお、EU AI 法が定める標準的なハイリスク AI に関する要件は、自動運転車には直接には適用されず²⁵、自動運転車に関する従来の規制が引き続き妥当することとなるが、EU AI 法は、自動運転車に関する従来の法律がハイリスク AI システムに関する要件を盛り込むことを要求している点には留意する必要がある(なお、重要なインフラ(道路交通)に関連する項目は、EU AI 法の Annex III Point 2 に含まれている。)

さらに、EU は、技術の発展が制約されないような形で、製品及びその管理に焦点を当てた自動運転車に関する法的枠組みを策定している。主要な規則としては、次のものがある。

- EU 規則 2019/2144: この規則は、自動化された項目を含む自動車の型式認証に関する要件を定めるものであり、安全性及び排出に関する基準を設定している。

- EU 規則 2022/1426: この規則は、完全自動運転車の自律走行システム(automated driving systems: ADS)の型式認証について具体的に規定して

²² <https://unece.org/media/press/368227>

²³ https://eur-lex.europa.eu/legal-content/EN/PIN/?uri=PI_COM:Ares%282022%292077610

²⁴ https://eur-lex.europa.eu/legal-content/EN/PIN/?uri=PI_COM:Ares%282022%292667391

²⁵ Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users.

いる。この規則は、技術的要件と試験手順について定めており、また、技術を特定の形に限定しないようにするという観点から規律を行っている。

- EU 規則 2022/2236**:この規則は、生産台数が限られた完全自動運転車を含む様々な種類の車両に関する技術的要件を定めている。

b. マネジメントレベル

自動車メーカーは、型式認証を取得するために安全規制への適合性を証明する書類とともに、以下に関する補足書類を提出する必要がある。

- (i) 構造化されたリスクアセスメントおよびコンプライアンスフレームワークを含む安全および品質マネジメントシステム
- (ii) 特に自動運転システム(ADS)を備えた車両が規制上の安全基準および運用基準を満たしていることを示す承認および検証手続
- (iii) 車両の開発および生産全体にわたり、安全上重要なプロセスを監視、記録、継続的に改善する方法を詳述するコーポレート・ガバナンスおよび監督メカニズム

自動車の型式承認に関する規則((EU) 2019/2144)、自動運転システムに関する規則((EU) 2022/1426)、および委任規則(EU) 2022/2236 の下では、品質マネジメント、安全性ガバナンス、およびコンプライアンス報告に関するマネジメントレベルでの義務が規定されている。しかし、これらの要件は主に (i) 製品レベルの安全要件に関する技術的要素、および (ii) 手続的要素であり、特定の手法を規定するものではなく、メーカーが内部の安全およびリスクマネジメントフレームワークをどのように構築するかについて一定の柔軟性を持たせている。その結果、各組織は、自社の業務構造に基づいて適合措置を解釈・実施しつつ、EU の型式認証プロセスと整合させなければならない。

c. オペレーターレベル

EU においても、従来は、車両のオペレーターは運転手だけであったが、完全自動運転車の出現によって、この「オペレーター」の概念は拡大し、自律走行システム(ADS)の運用に責任を負う製造者や事業体も含まれることとなった。

従来の EU における完全自動運転車に対する規制は、主として、**予防的な安全対策**を主眼としたものであり、法的責任の構造を明確に再定義することには重点は置かれていなかった。例えば、製造者を含むオペレーターには、リスクマネジメントシステムを導入することや、潜在的な欠陥箇所(“fault items”)を特定することにおける透明性を確保することが要求されており²⁶、また、オペレーターは、そのような欠陥に関連するリ

²⁶ Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles at Art. 2(7) among others.

スクを軽減するための適切な体制と対応策を確立して、型式認証の期間を通じてこれらについての開示を行わなければならないとされている。

(iv) 英国

a. 製品レベル

英国においては、自動運転車を規制する自動運転車両法 (Automated Vehicles Act: AVA) が制定され、2024 年 5 月 20 日に施行された²⁷。この法律は、自動車分野に固有の法律と併せて二重の認証制度を確立し、従来の型式認証の枠組みを補完するものである。

同法によれば、製品、マネジメント、及びオペレーターの各レベルの認証に関する要件を定める権限は運輸大臣に委任されているが、同法において、既に、認証に関する一般的な指針となるような規定が見られる。すなわち、運輸大臣は、それが自動運転に関する試験を含む所定の要件を満たす場合には、道路走行車両について (i) 個別に、又は (ii) 一般的に許可 (authorization) をすることができるが²⁸、その許可に当たって、次の事項を含めた形で自動運転に関する試験を満たしていると判断する機能を特定して明らかにしなければならない²⁹。

- 当該機能の動作の種類が、「運行管理者同乗型 (user-in-charge)」と「運行管理者非同乗型 (no-user-in-charge)」のいずれであるか。
- 当該機能の起動方法及び停止方法。
- 当該機能によって当該車両が自動運転に関する試験を満たしていると運輸大臣が判断する際に参照した場所や状況。

なお、自動運転車両法上、運輸大臣には、以上の認可の要件に関する規則を策定する権限のほか³⁰、型式認証に関する法令を自動運転車に適合するように更新する権限³¹が認められており、今後、規則等の策定や更新がされることが見込まれる。

b. マネジメントレベル

自動運転車両法では、マネジメントレベルに関わるものとして、次のような規律が置かれている。

²⁷ <https://www.gov.uk/government/news/self-driving-vehicles-set-to-be-on-roads-by-2026-as-automated-vehicles-act-becomes-law>.

²⁸ Automated Vehicles Act 2024 (“AVA”), Art. 3.

²⁹ AVA Art. 4.

³⁰ AVA Art. 5.

³¹ Art. 91.

認可自動運転事業主体 (authorised self-driving entity)³²

自動運転車両法によれば、運輸大臣は、自動運転車両の許可に当たり、当該車両の「認可自動運転事業主体」として指定される個人又は事業体が存在するように許可要件を課さなければならないとされている。

そして、この許可要件を課すに当たっては、①許可自動運転事業主体が、認可された自動運転車両が自動運転に関する試験を継続的に満たすことを確保する全般的な責任を負い、かつ、②(i) 評判が良く、(ii) 財務状態が良好で、(iii) ①の責任を適切に果たすことができるという目的が達成されるようにしなければならないとされている。

c. オペレーターレベル

運行管理者非同乗型運行者 (no-user-in-charge operator)³³

自動運転車両法によれば、運輸大臣は、運行管理者非同乗型運行者の免許に関する規定のほか、運行管理者非同乗型走行 (no-user-in-charge journey) 又はそれを行う車両に関する要件についての規定を定めることができるとされている。

そして、この運行管理者非同乗型運行者の免許に関する規則を定める場合には、前記 [b](#) と同様、①免許を受けた運行管理者非同乗型運行者が、その監督の下での運行管理者非同乗型走行中に生じた問題の検知及び対応について、全般的な責任を負い、かつ、②(i) 評判が良く、(ii) 財務状態が良好で、(iii) ①の責任を適切に果たすことができるという目的が達成されるようにしなければならないとされている。

また、この運行管理者非同乗型運行者については、運行管理者非同乗型走行について「監督 (overseen)」するものとされており、自動運転車両法上も、明示的に監督義務が認められているが、現時点において、かかる監督の内容について定める運輸大臣による規則は策定されておらず、具体的にどのような内容の監督が必要となるかについては明らかではない。

運行管理者 (user-in-charge)

自動運転車両法によれば、運行管理者とは、①当該車両が、許可された運行管理者同乗型機能 (authorised user-in-charge feature) を備えた許可された自動運転車であり、②当該機能が作動しており、かつ、③当該車両内におり、これを制御できる状態にあるが、制御をしていない個人をいう³⁴。そして、ここでいう運行管

³² AVA Art. 6.

³³ AVA Art. 12.

³⁴ AVA Art. 46.

理者同乗型機能とは、行程の一部のみ自動運転をし、残りの区間は運転手が運転を行うこととなる機能を意味している³⁵。

なお、自動運転車両法は、運行管理者の刑事責任に関し、(i) 運行管理者同乗型機能が作動している際に生じた違反や、(ii) 自動運転車が運転を運転手に引き継ぐ際に、当該状況下における運転手に合理的に期待される注意を果たしても回避することができなかったような違反について、刑事責任を負わないものとしている³⁶。

自動旅客サービス(Automated passenger services)³⁷

自動運転車両法によれば、適切な国家機関 (appropriate national authority³⁸) が、自動運転車両を用いた自動旅客サービス又はその試験に関する許可 (permit) を与えることができる。そして、この許可は、タクシー、個人用ハイヤー及びバスに関する法律の適用除外³⁹を確保するため、又は、運行管理者非同乗型運行者の免許 (licensing of no-user-in-charge operation) に関する要件⁴⁰を満たすために与えることができるとされている。

そして、この許可に当たっては、次の項目が明示されなければならない。

- 当該許可に基づきサービスが提供することができる区域
- 当該許可に基づきサービスが提供することができる車両（又は車両に関する説明）
- 当該許可の有効期間
- 当該許可が付与されるための条件（「許可条件」）

以上の許可の付与の手続に際しては、関係する国家機関のみならず、サービスを行うことが許可される区域を所管するタクシー等の免許を交付する機関のほか⁴¹、バスに関しては、関連するフランチャイズ機関も関与する⁴²。また、許可にあたっては、交通当局やエマージェンシー・サービスとの協議をしなければならない⁴³。

また、許可に当たっては、障害者や高齢者の乗客のニーズへの対応するために自動乗客サービスがどのように設計されるべきかといったことが考慮されなければ

³⁵ Department for Transport, “Explanatory Notes: Automated Vehicles Act 2024 Chapter 10”, p.15.

³⁶ AVA Art. 47; *ibid.* p.30.

³⁷ AVA Art. 82.

³⁸ これは、ウェールズとスコットランド政府の各大臣が自動旅客サービスに関する許可を与えることを認めるための文言である。参照、Department for Transport, “Explanatory Notes: Automated Vehicles Act 2024 Chapter 10”, p.45, https://www.legislation.gov.uk/ukpga/2024/10/pdfs/ukpgaen_20240010_en.pdf

³⁹ AVA Art. 83

⁴⁰ AVA Art. 12

⁴¹ AVA Art. 85, 86.

⁴² AVA Art. 86.

⁴³ AVA Art. 87.

ならないとされ⁴⁴、また、適切なデータプライバシー管理などの項目を許可要件に含むことができるとされている⁴⁵。

(2) 医療機器

(i) 日本

a. 製品レベル

日本における医療機器の許認可に関しては、製造販売⁴⁶の承認制度が採用されており、この承認制度の中で、医療機器それ自体の有効性・安全性等についての審査がなされるほか、製造販売を行う主体の製造マネジメント・品質マネジメントの基準やその組織体制等について審査が行われる仕組みとなっている。医療機器については、医療機器に関するクラス分け（一般医療機器、管理医療機器、高度管理医療機器⁴⁷）に応じた審査が行われ、リスクが最も低いクラス一般医療機器については届出、管理医療機器及び高度管理医療機器のうち、比較的风险が小さく、基準を定めることで有効性・安全性が確保できるものとして基準が定められているものについては、登録認証機関による認証、リスクが高いその他のものについては厚生労働大臣による承認（審査は医薬品医療機器総合機構（PMDA）が行う）によるものとされている⁴⁸。

医療機器に関しては、プログラム医療機器に限らず全ての医療機器が備えるべき基本的な要件について「基本要件基準」が定められている⁴⁹。基本要件基準において、プログラム医療機器に関しては、特に、①そのシステムの再現性・信頼性・性能の確保、②最新の技術に基づく開発のライフサイクル、リスクマネジメント並びに当該医療機器を適切に動作させるための確認及び検証の方法を考慮した上での品質及び性能についての検証の実施、③サイバーセキュリティへの配慮が要請されているが、基本要件基準自体は、全ての医療機器が備え

⁴⁴ AVA Art. 87.

⁴⁵ AVA Art. 88.

⁴⁶ 「製造販売」とは、「その製造（他に委託して製造をする場合を含み、他から委託を受けて製造をする場合を除く。以下「製造等」という。）をし、又は輸入をした(...)医療機器(...)を、それぞれ販売し、貸与し、若しくは授与し、又は医療機器プログラム（医療機器のうちプログラムであるものをいう。以下同じ。）を電気通信回線を通じて提供することをいう。」とされている（薬機法第2条第13号）。

⁴⁷ 一般医療機器がクラスⅠ、管理医療機器がクラスⅡ、高度管理医療機器がクラスⅢ・Ⅳにそれぞれ対応する。

⁴⁸ 薬機法第23条の2の5第1項（承認）、第23条の2の23第1項（認証）、第23条の2の12第1項（届出）

⁴⁹ 薬機法第41条第3項、平成17年3月29日付け厚生労働省告示第122号「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律第四十一条第三項の規定により厚生労働大臣が定める医療機器の基準」（「基本要件基準」）。これは、医療機器規制国際整合化会議（Global Harmonization Task Force: GHTF）（現在は、国際医療機器規制当局フォーラム（International Medical Device Regulators Forum: IMDRF）に発展的に解消）が2005年に示した医療機器及び対外診断用医薬品の基本要件（GHFT/SG/N41R9:2005／改訂後はIMDRF/GRRP WG/N47 Final: 2018）を薬機法において位置づけたものであるとされる。

るべき基本的な要件に関するものであり、AI の特性等を踏まえた規律がなされているわけではない⁵⁰。

ただし、薬機法の令和元年改正により、AI のように恒常的に性能等が向上し続けるプログラムが登場してきたことを踏まえ、変更計画の事前確認制度（IDATEN 制度）が制定された⁵¹。これは、市販後に恒常的に性能等が変化する医療機器について、医療機器の改良プロセスを評価することで、市販後の性能変化に合わせて柔軟に承認内容の変更を可能とするためのものであり、医療機器の製造販売の承認制度全体としては、AI の特性等を踏まえた改正がされている。

b. マネジメントレベル

医療機器の製造販売の承認を得るには、QMS 省令（「医療機器及び体外診断用医薬品の製造管理及び品質管理の基準に関する省令」）⁵²、QMS 体制省令（「医療機器又は体外診断用医薬品の製造管理又は品質管理に係る業務を行う体制の基準に関する省令」）⁵³、そして、GVP 省令（「医薬品、医薬部外品、化粧品、医療機器及び再生医療等製品の製造販売後安全管理の基準に関する省令」）⁵⁴に定める基準に適合した製造管理・品質管理やその組織体制を整備する必要がある。

QMS 省令は、医療機器の製造管理又は品質管理の実施方法等について定める厚生労働省令であり、国際的な整合性を確保する観点から、医療機器産業に特化した品質マネジメントシステムに関する国際規格である ISO13485 と整合するものと位置づけられている。

QMS 体制省令は、製造販売業者が、QMS 省令を遵守するための必要な体制に関する基準を定めるものであり、QMS 省令に定める品質管理監督システムの確立及び実効的な運用や、文書・記録の適切な管理・保管など QMS 省令の規定を遵守するために必要な組織の体制を整備することや、総括製造販売責任者・管理監督者をその業務を適正に行うことができるように適正に配備すると共に、QMS 省令の遵守のために必要な人員を配置することが求められている。

GVP 省令は、製造販売した医療機器が適正に使用するための安全管理を行う上で従うべき基準を定めるものであり、製造販売業者が、医療機器の品質、有効

⁵⁰ なお、一部の医療機器については、通達により承認基準が示されているが、AI を用いた医療機器に関する承認基準は現時点では存在しないようである。ただし、平成 17 年から厚労省に設置されている「次世代医療機器評価指標検討会」より、「人工知能技術を利用した医用画像診断支援システムに関する評価指標」（令和元年 5 月 23 日付け薬生機審発 0523 第 2 号）が示されている。

⁵¹ 薬機法第 23 条の 2 の 10 の 2。

⁵² 薬機法第 23 条の 2 の 15 第 1 項。

⁵³ 薬機法第 23 条の 2 の 2 第 1 項第 1 号。

⁵⁴ 薬機法第 23 条の 2 の 2 第 1 項第 2 号。

性及び安全性に関する事項その他医薬品等の適正な使用のために必要な情報（安全管理情報）を収集、検討し、その結果に基づいて医療関係者に対する情報提供などの安全確保のために必要な措置を行うこと（安全確保業務）などが求められている。

もっとも、いずれの省令についても、あくまで医療機器一般に関して、製造管理・品質管理の基準やその組織体制等に関して概略的な要求事項を定めるものであり、AIを利用した医療機器に焦点を合わせたものではない。

c. オペレーターレベル

自動運転車とは異なり、現在の AI を用いた医療機器（医用画像診断支援システムなど）は、あくまで医師による診断を補助するツールとして位置づけられている。そのため、かかる医療機器を「医業」において用いる場合、そのユーザーは医師免許を取得していることが必要となる⁵⁵。他方で、AIを用いた医療機器の利用に焦点を当てたオペレーターレベルでの規制等に関する特段の議論の存在については確認することができなかった⁵⁶。

(ii) アメリカ

a. 製品レベル

アメリカにおいても、日本と同様、医療機器のクラス分けがされており（クラス I（リスク低）～クラス III（リスク高））、クラス II（例：輸液ポンプなど）とクラス III（例：ペースメーカーなど）については、FDA の承認が必要となる。主としてクラス II の医療機器を対象とする 510(k)と呼ばれる承認手続では、先行機器と「実質的に同等（substantially equivalent）」と言えるかが審査される⁵⁷。ただし、先行機器が存在しない場合でも、リスクの程度が高くない医療機器については、使用目的との関係での安全性・有効性を根拠づけることにより販売を承認する De Novo 制度も用意されている⁵⁸。これに対して、クラス III 医療機器を対象とするのが市販前承認（Premarket Approval: PMA）であり⁵⁹、使用目的との関係での安全性・有効性を根拠づけるために提出される証拠の条件等が 510(k)よりも厳格となっている⁶⁰。

⁵⁵ 医師法 17 条。

⁵⁶ なお、AIを用いた診断・治療支援を行うプログラム用いて診断を行う場合にも、診断・治療等を行う主体は医師であり、医師法 17 条の「医業」として行われるものとの理解が厚労省の通達より示されている（平成 30 年 12 月 19 日付け医政医発 1219 第 1 号）。

⁵⁷ FDCA510(k)(21USC360(k)), 21CFR807.81(a), 21CFR807.100

⁵⁸ FDCA513(f)(2)(21USC360c(f)(2))

⁵⁹ FDCA515(21USC360e)

⁶⁰ FDCA515(c)(1)(21USC360e(c)(1)), 21CFR814.20

プログラム医療機器に関しては、2016 年の the 21st Century Cures Act により、一定のソフトウェアについて、食品医薬品局（Food and Drug Administration: FDA）の判断で規制対象とすることができることとされ、AI が利用されることが多い医用画像等処理するソフトウェアなどは、医療機器に該当するものとして扱われている⁶¹。

そして、医療機器の性能に関して、医療機器の種類に応じて、FDA が認定をしたコンセンサスのある基準（recognized consensus standards）が定められているが⁶²、AI を利用した医療機器に焦点を当てた基準の存在については確認することができなかった。

なお、AI を利用した医療機器については、市販後の性能変化が見込まれることから、（日本の IDATEN 制度に類似する）予め改良計画を立てておき、承認後に機能変化があった場合でも追加の承認を不要とする Predetermined Change Control Plan（PCCP）制度が 2022 年に新設されている⁶³。

b. マネジメントレベル

前記 a. のいずれの承認手続においても、承認を受けるためには、日本と同様、品質管理規則（Quality System Regulation）の充足が求められている。この品質管理規則は、医療機器に特化した品質管理規格である ISO13485:2016 と異なる内容であったが、2024 年に改正がなされ、ISO13485:2016 の要件が組み込まれることとなった（2026 年 2 月施行予定）⁶⁴。

c. オペレーターレベル

アメリカでも、現在の AI を用いた医療機器は、医師による医療行為を補助するツールとしての位置づけであり、医療行為を行う場合には、医師免許（専門医療行為を行う場合には、専門医師免許）が必要である（所管は各州）。他方で、日本と同様、AI を用いた医療機器の利用に関するオペレーターレベルでの規制等に関する特段の議論の存在については確認することができなかった。

⁶¹ FDCA520(o)(1)(A)-(E)(21USC360j(o)(1)(A)-(E)), FDCA201(h)(1)(21USC321(h)(1))

⁶² FDCA514(c)(21USC360d(c))

⁶³ FDCA515C(21USC360-e). なお、2023 年に、AI に関する PCCP についてのガイダンス草案（Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence/Machine Learning (AI/ML)-Enabled Device Software Functions）が公表された。そこでは、計画に記すことが推奨される事項（訓練・学習データ等のデータ管理、再学習の方法、性能評価方法、アップデートの手続）等が示されている。
<https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendations-predetermined-change-control-plan-artificial-intelligence>

⁶⁴ <https://www.fda.gov/medical-devices/quality-system-qs-regulation/medical-device-current-good-manufacturing-practices-cgmp/quality-management-system-regulation-final-rule-amending-quality-system-regulation-frequently-asked>

(iii) EU

a. 製品レベル

EU は、製品レベル及びマネジメントレベルにおいて、自動運転車の場合と同様に、多層的な規制アプローチを採用している。すなわち、(i) 医療機器に特化した規制と、(ii) AI に関する項目について全般的に規定する EU AI 法による規制が行われている。

まず、(i)について、EU においても日本やアメリカと同様、医療機器に関しては、EU 医療機器規則(Medical Device Regulation(“MDR”))によって、リスク分類に応じた規制が行われている⁶⁵。具体的には、EU 医療機器規則(MDR)が定めるリスク等級ごとに、具体的なコンプライアンス要件が定められており、Class IIa 以上の医療機器は、第三者機関である適合性評価機関による市販前の適合性評価を受けなければならないとされている。

製造者には、市場への導入後も、製品の安全性に関して相応の責任が課されている⁶⁶。具体的には、製造者は、その市場への導入後も、品質管理システムの一部として、予防措置又は是正措置を実施するための市販後臨床追跡(post-market clinical follow-up : PMCF)を行うほか、医療機器の性能を監視したり、技術文書を更新するなどして市販後調査システムを維持しなければならないとされ、そこでは、適切な者の監視の下で、臨床評価に適合したリスクマネジメントシステムを通じてリスクを管理して規制が遵守される状態を確保することが求められている。また、このシステムは、医療機器のリスク等級と種類に適合した形で継続的な安全性と規則への適合性を確保するものでなければならず、臨床データの収集も求められている。その他、リスクの高い医療機器の製造者については、各機器について、市販後調査により得られたデータの分析結果等を内容とする定期的安全性最新報告(periodic safety update report: PSUR)を作成することも求められている⁶⁷。

その上で、(ii)EU AI 法においては、医療に関する項目として、Annex III の「不可欠な民間サービス・給付及び不可欠な公共サービス・給付へのアクセスと享受」の中に次のものが含まれている。

- a. 公的機関による支援: 医療サービスを含む重要な公的給付・サービスの受給資格を決定し、この給付を管理(付与、削減、取消)するために、公的機関により又は当該機関に代わって使用される AI システム
- b. 保険のリスク評価: 個人の生命保険及び医療保険に関するリスク評価と価格設定のために使用される AI システム

⁶⁵Regulation (EU) 2017/745; MDCG 2021-24 Guidance on classification of medical devices (https://health.ec.europa.eu/system/files/2021-10/mdcg_2021-24_en_0.pdf)

⁶⁶ MDR at Preamble, at 20, 32-34, 48. Art. 10 (9)(i); (10); Art. 83; Art. 92.

⁶⁷ MDR at Art. 86.

- c. 緊急対応管理: 緊急通報の評価と優先順位付け、エマージェンシー・サービス(警察、消防、医療支援を含む)の派遣、及び、緊急医療患者のトリアージを行うための AI システム

医療機器が上記のいずれかのカテゴリーに該当する場合には、EU AI 法のハイリスク AI に関する義務が上乗せされることとなる。もっとも、EU AI 法は既存の医療機器に関する規制枠組みを置き換えたり、それを無効にしたりするものではなく、それを補完するものである。

b. マネジメントレベル

EU における医療機器に関する AI システムのガバナンスは、医療機器規則(MDR)および EU AI 法の特定の規定を通じてマネジメントレベルで構築されている。これらの規則は、適合性の確保および安全性・有効性基準の維持を目的とした責任および義務を定めている。MDR および体外診断用医療機器規則(IVDR)では、規制適合を担当する部門の設置を通じた組織能力の構築が求められており、加えて EU AI 法のハイリスクシステムに関する一般要件が適用される。

1. 医療機器規則(MDR)

MDR は、製造業者および認定代理人に対し、「規制適合責任者 (PRRC: Person Responsible for Regulatory Compliance)」の任命を義務付けている。PRRC は、以下を含む品質管理要件の機能性を確保する責任を負う。⁶⁸

- 該当する医療機器が規制基準を満たしていることの確認
- 技術文書および EU 適合宣言の維持
- 市販後監視 (PMS: Post-Market Surveillance) 義務の遵守
- 重大事象の報告義務の履行

2. AI 法

AI 法では、AI システムのリスクに基づく分類を導入し、医療機器に使用される AI システムなどのハイリスク AI システムに対し、マネジメントレベルでの適合要件を定めている。ハイリスク AI 医療機器の提供者は、以下の義務を負う。⁶⁹

- 品質管理システムの導入
- 技術文書の維持
- 市場投入前の適合性評価の実施

⁶⁸ Regulation (EU) 2017/745; Regulation (EU) 2017/746, (“MDR” & “IVDR”) Art. 15.

⁶⁹ EU AI Act Arts. 16-19, 43, 49; Chapter IX, Sections 1, 2.

- ・ 市販後監視の確立（継続的な適合性及び安全性の確保）

これらの規則により、AIを活用した医療機器の管理・適合性確保の枠組みが構築されている。

c. オペレーターレベル

EUにおいても、オペレーターは医師等であり、責任についても医師等と製造者の間で分担されることになる。

(iv) 英国

英国における医療機器に関する規制枠組みは、現在、従来依拠してきた EU の規制枠組みからの移行段階にある。従来、英国は、EU 指令による 2002 年の医療機器規則（Medical Devices Regulations 2002）に基づいて運営されており、これには製品認証のための CE マーキング制度も含まれていた。もともと、2023 年に独自の医療機器規則（UK Medical Device Regulations 2023）が制定され、AI を用いた医療機器を含む医療機器のための独自の枠組みが構築されることとなった。なお、この移行は段階的に行われ、現在の EU の規制に基づく認証制度は 2030 年までに徐々に廃止されるものとされている。

英国の現行の規制枠組みの主な特徴としては、次のものが挙げられる。

1. EU の規制からの移行

従来の CE マーキングは 2030 年まで認められるが⁷⁰、その後は、UKCA マーキング（UK Conformity Assessed marking）（英国独自の適合性及びコンプライアンス評価の枠組み）に移行することになるとされている。

また、将来の政策及び規制の中核は「英国の市場に導入される医療機器の必要条件を EU のそれとより整合させる」ように更新され、「これには、AI を含む医療機器としてのソフトウェアのサイバーセキュリティに関する要件も含まれる」とされている⁷¹。

2. リスクに基づいた認証制度：

⁷⁰ Medicines & Healthcare products Regulatory Agency, Standard: Implementation of the future regulations (<https://www.gov.uk/government/publications/implementation-of-the-future-regulation-of-medical-devices/implementation-of-the-future-regulations>); Medicines & Healthcare products Regulatory Agency, Guidance: Regulating medical devices in the UK (<https://www.gov.uk/guidance/regulating-medical-devices-in-the-uk>)

⁷¹ Medicines & Healthcare products Regulatory Agency, Standard: Implementation of the future regulations (<https://www.gov.uk/government/publications/implementation-of-the-future-regulation-of-medical-devices/implementation-of-the-future-regulations>)

英国の医療機器の認証制度は、EU における分類に基本的に対応している。「グループ A 医療機器 (Group A device)」とは、EU の Class I の医療機器、Class IIa の医療機器、又は埋込み型医療機器でも長期侵襲性医療機器でもない Class IIb の医療機器に相当する。また、「グループ B 医療機器 (Group B device)」とは、埋込み型医療機器又は長期侵襲性医療機器である Class IIb 医療機器、又は Class III 医療機器に相当する。

3. 制度構造とソフトウェアグループ：

英国は、医療機器に用いられる AI に関する規制の策定に向けた専門的なタスクフォースグループの枠組みを構築し、制度の構築に向けた取り組みを行っている⁷²。

4. アメリカ及びカナダとの国際的な連携：

英国は、(a)アメリカ及びカナダと共に複数の計画を作成し、(b)AI に対応できるように従来の法律の調整を行うと発表した。

(a) 米国及びカナダと共に作成した計画：

- i. ライフサイクル、透明性などを含む 10 原則の策定⁷³（これはアメリカ食品医薬品局 (FDA) 及びカナダ保健省 (Health Canada: HC) と並行して行われている。
- ii. アメリカ食品医薬品局及びカナダ保健省と共同で、大規模言語モデルに対応した医療機器に関する Predetermined Change Control Plan も発表している⁷⁴。
- iii. これらの計画により、アプリケーションを含む医療機器スタンドアロン型ソフトウェアのガイドラインが作成された。アプリケーションは次の 4 つのカテゴリーに分類されている。
 - (i) 症状チェッカー (symptom checkers)
 - (ii) 臨床計算ツール (clinical calculators)
 - (iii) 「機器の使用を促進又は影響する」

⁷² Medicines & Healthcare products Regulatory Agency, Guidance: Software and artificial intelligence (AI) as a medical device (<https://www.gov.uk/government/publications/software-and-artificial-intelligence-ai-as-a-medical-device/software-and-artificial-intelligence-ai-as-a-medical-device>)

⁷³ Medicines & Healthcare products Regulatory Agency, Guidance: Good Machine Learning Practice for Medical Device Development: Guiding Principles (<https://www.gov.uk/government/publications/good-machine-learning-practice-for-medical-device-development-guiding-principles/good-machine-learning-practice-for-medical-device-development-guiding-principles>)

⁷⁴ https://assets.publishing.service.gov.uk/media/6537be725e47a500149898dc/Predetermined_Change_Control_Plans_-_Guiding_Principles.pdf

(iv) 現場での安全警告及び製品寿命終了通知 (field safety warnings and end of life notifications) ⁷⁵

(b) AI に対応するように市場への導入に関する要件が更新される予定である ⁷⁶。この更新は、市場に導入される前の安全性、有効性、品質に重点を置き、要件が医療機器がもたらすリスクに見合ったものであることを保証することを目的としたものであり、ISO 規格 (IEC 62304:2006) にも言及されている ⁷⁷。

5. 構築段階

今後の主要な規制については、2025 年頃に発表予定であるとされている ⁷⁸。

⁷⁵ Medicines & Healthcare products Regulatory Agency, Guidance: Medical device stand-alone software including apps (including IVDMDs)(https://assets.publishing.service.gov.uk/media/64a7d22d7a4c230013bba33c/Medical_device_stand-alone_software_including_apps_including_IVDMDs.pdf)

⁷⁶ Medicines & Healthcare products Regulatory Agency, Guidance: Software and AI as a Medical Device Change Programme – Roadmap, WP3 Premarket requirements (<https://www.gov.uk/government/publications/software-and-ai-as-a-medical-device-change-programme/software-and-ai-as-a-medical-device-change-programme-roadmap#wp-3-premarket-requirements>)

⁷⁷ <https://www.iso.org/standard/38421.html>

⁷⁸ Medicines & Healthcare products Regulatory Agency, Roadmap towards the future regulatory framework for medical devices(9th January 2024) (https://web.archive.org/web/20240221112716/https://assets.publishing.service.gov.uk/media/659d3539aaae22001356dc3c/Roadmap_towards_the_future_regulatory_framework_for_medical_devices_Jan_24.pdf)

3. AI 認証における主な発見と今後の課題

(1) 比較分析の主な結果

2.における分析結果を踏まえた自動運転車及び医療機器に関する規制の共通点と相違点は次のとおりである。

(i) 自動運転車

- 共通点:
 - 必要な許認可の取得: 自動運転車の走行試験及び市場へ導入するの双方に関して、許認可の取得が必要である。
 - 走行試験に関する要件の緩和: 自動運転車の走行試験段階における規制基準は緩和されている。
- 相違点:
 - 型式認証の要否: 日本、EU、英国では公的機関による型式認証が必要とされているが、アメリカでは自己認証が認められている。
 - 型式認証の対象範囲: アメリカでは車両のハードウェアとソフトウェアに重点が置かれているが、日本、EU、英国ではマネジメントシステムも認証の対象範囲に含まれている。
 - オペレーターの役割: 日本、EU、英国では、法令上、人間による監視が求められているが、アメリカ(カリフォルニア州)ではこうした監視は現時点では求められていない。

(ii) 医療機器

- 共通点:
 - リスクレベルの区別に応じた認証: 医療機器のリスクのレベルに応じた認証制度が採用されている。
 - AIを用いた医療機器の位置づけ: 現行のAIを用いた医療機器は医師や医療従事者による医療行為の支援等を行うものとして位置づけられている。
- 相違点:
 - EUでは、既存の規制に加えて、AI法によりAIについて包括的な規律がなされており、AIを用いた医療機器についても、同法に基づく各種義務の履行が必要となるが、その他の国ではそうした規制はない。
 - 日本やアメリカでは、AIが作用する医療機器のように市販後に恒常的に性能等が変化する医療機器について、市販後の性能

変化に併せて柔軟に承認内容の変更を可能としたり、追加の承認を不要とするための制度が制定されている。

(2) 今後の検討課題

本報告書の対象となった AV, MD の領域のほかにも、従来人間が行ってきた一定のハイリスク行為を AI システムで代替する領域は急速に拡張すると考えられる。そのため、そのような AI システムを認証するニーズは今後増加すると思われる。その際には、以下のような論点について検討することが必要と考えられる。

(i) AI に対する認証の制度的枠組み

a. 認証制度を設定する領域

<Q1> 包括・分野別の認証システムをどのように組み合わせることが、AI システムに対する信頼を確保するために効果的か?

- AI 全般に関するマネジメントシステムに関する国際標準としては、ISO/IEC 42001 が存在。もっとも、その内容は、マネジメントシステムを対象としたものであり、具体的なAI製品やサービスを認証するものではない。
- 自動車及び医療機器など、既に分野別に認証の仕組みが発達している分野のほかに、AI の浸透によって新たに認証制度のニーズが高まる産業分野やサービス分野はあるか。

b. ハードローによる認証取得義務付けが必要となる領域

<Q2> ハードローによる認証取得を義務付ける必要があるのはどの範囲か

- 既存法で認証取得が義務付けられている分野(自動車・医療機器等)においては、AI 製品についても認証取得が求められるのが原則(但し、認証の対象や方法については検討の必要あり。下記(ii)参照。)
- 上記の他に、新たに認証取得を義務付ける必要がある場合はあるか
 - EU AI 法では、Annex III において、AI 独自のハイリスク領域を指定しており、適合性評価の実施を求めている。

c. 国際規格による相互運用確保が可能な範囲

<Q3> 認証の仕組みを国際間で相互運用可能なものとする際の限界は何か。

- とりわけ、人間の監視の必要性など、国家間で立場が異なる内容についてはどうか。

(ii) 認証の方法

a. 認証の対象

<Q4> AI 製品やサービスについて、何を認証の対象とすべきか。

- AI のブラックボックス性や説明不可能性などから、伝統的なプロダクト認証の手法に限界がある。
- 他方で、マネジメントやオペレーターの認証は、必ずしも製品・サービス自体のリスクを直接判断するものではないので、その実効性には限界がある。
- 上記を組み合わせたジョイント認証（Joint-Certification）⁷⁹を採用する場合、どのような設計とすべきか。

b. 認証基準

<Q5> AI 製品やサービスの認証の基準をどのように設定すべきか。

- AI アルゴリズムの複雑さから、その内容について直接信頼の可否を判断することは困難（従来型のウォーターフォールシステムとの違い）
- パフォーマンスベース（走行距離あたりの事故件数、診断数あたりの誤判断数等）の認証を行う場合、テスト方法について合意することは可能か？
- 上記 a. に掲げた各要素について個別に判断する場合、それぞれをどのような基準で判断できるか。
- データガバナンス、サイバーセキュリティ、アルゴリズムパフォーマンス、モニタリング体制等、認証対象を要素分解して個別に判断することは可能／妥当か？
- a. に記載の Joint-Certification を採用する場合、最終的に何を基準に判断するのか。

c. 認証のタイミング

<Q6> AI 製品やサービスの認証は、どの時点で付与されるべきか。

⁷⁹ Joint-Certification モデルとは、組織における特定の領域（例：プライバシー）のマネジメントやガバナンスに関するプロセスと、その領域が適用される製品（例：クラウドコンピューティングサービス）を階層的に統合するモデルである。このモデルは、マネジメントシステム（ガバナンスおよび監督）に関する ISO/IEC 規格と、製品・サービスに適用される規格を組み合わせることで、必要な柔軟性を提供することを前提としている。詳細については、EY and Microsoft, “A Joint Certification Approach for Digital Services and Regulatory Compliance” (2022)を参照。

- 上市後も継続的に環境やアルゴリズムが変更されること、技術進歩のスピードが著しいこと等に鑑み、上市前にどこまで厳格な認証を要求するか。
- 上市後も継続的に安全性を確認する必要があるが、誰がどのようにして継続的なモニタリングを行うのか。

(iii) 認証機関の在り方

a. 認証機関に求められる要件 (minimum requirements)

<Q7> 認証機関には高度な専門性が要求されるが、具体的に求められる最低限の要求は何か。

b. 認証プロセスへの専門家の関与

<Q8> 認証プロセスにおいてどのような専門家が関与すべきか。

(iv) 認証と責任制度の関係

<Q9> 認証制度の下で事故が発生した場合、民事・刑事・行政上、どのような責任が生じるように設計すべきか

- ① 事業者が認証を取得しており、取得後も認証の内容に沿ったオペレーションが実施されていた場合
- ② 事業者が認証を取得していたが、取得後に認証の内容に沿ったオペレーションが実施されていなかった場合
- ③ 事業者が認証を取得していなかった場合

折しも、日本では2025年2月4日に政府のAI制度研究会による中間とりまとめが公表され、また、同28日には「AI関連技術の研究開発・活用推進法案」が閣議決定された。これらの政策に共通しているのは、民間事業者によるAIの実装を強く後押ししつつ、その信頼性の確保については事業者の自主的な取組に委ねるということである。これは、民間主導によるAIに対する認証メカニズムの構築が一層重要になってきていることを意味する。本報告書はその現時点での国内外の制度の状況を取りまとめたものであるが、そこから見えてきたのは、現時点において、AIに対する認証のメカニズムはいずれの分野においても発展途上であるという現実である。本報告書の調査及び論点整理が、今後の国内外における認証制度の議論の進展に少しばかりでも寄与することを願う。

別紙 1 各国の法的認証制度に関する初期調査

注:本初期調査は、2024年8月時点での各国の立法動向をデスクトップ調査に基づいて概略として記載したものである。あくまで法規制の存否という観点からの調査であり、具体的な法令の内容及びその最新性について担保するものではない。

1. 結果の概要

- 全ての国において、医療機器及び自動車について、AIシステムの認証制度が存在。
 - 但し、これは、もともと自動車(車両)や医療機器について認証制度が存在していたために、それが AI システムにも適用されることから生じたものといえる。その上で、各国で AI システムの導入にあわせたアップデートが行われている。
 - EU AI 法では、製品安全の構成要素であって、現行 EU 法上第三者認証が求められているものに AI を使用する場合、ハイリスク AI システムに分類され、(現行法の義務に加えて)同法の定める義務が追加される¹。
- 他方、金融・法務・労働分野で使われる AI システムについては、多くの国で AI システム自体に対する認証制度は導入されていない。
 - これらの分野については、従来は基本的に事業者(エンティティ)自体への免許が行われており、システムはそのような事業者が責任をもって用いることが前提とされていた。
 - これに対し、EU AI 法では、事業者への免許に加えて、ハイリスク AI システムへの認証を義務づけることとしている。
- 高度な AI モデル(汎用目的 AI、フロンティア AI 等)について特別な規制の導入を検討している国・地域が複数存在。

¹ AI 法 Annex I。具体的には、(1)機械指令、(2)玩具安全指令、(3)レクリエーション用舟艇指令、(4)リフト指令、(5)防爆指令、(6)無線機器指令、(7)圧力機器指令、(8)ケーブルウェイ規則、(9)個人用保護具規則、(10)ガス機器規則、(11)医療機器規則、(12)体外診断用医療機器規則、(13)民間航空安全規則、(14)二輪・三輪・四輪車両に関する規則、(15)農業・森林業用車両規則、(16)船舶機器指令、(17)鉄道システム相互運用性指令、(18)自動車及び部品等に関する規則、(19)自動車の型式承認に関する規則、(20)民間航空の安全に関する共通ルールに関する規則、が含まれる。

- EU、中国では既に法規制が成立。
- 日本及び英国でも法規制の導入が検討されたが、具体的な立法には至っていない。米国カリフォルニア州では、学習データの透明性に関する法律は可決されたものの、大規模基盤モデルを対象とする「最先端人工知能(AI)システムのための安全でセキュアな技術革新法(SB1047)」(カリフォルニア AI 安全法)については、州知事が拒否権を行使したために廃案となった。

2. 調査結果

<凡例>

PL: Public licensing is required

TC: Third-party certification is required

SC: self-certification

PR: Public registration is required

UD: Under Official discussion

NA: None (該当事項なし)

<Categories and possible use cases²>

Healthcare: Diagnosis, Symptom prediction, Surgery assistance, Personalized treatment plans

Mobility: Autonomous vehicles, Traffic management, Predictive maintenance, Route optimization

Finance: Fraud detection, Algorithmic trading, Credit scoring, Customer service chatbots

² The following examples are not necessarily covered by regulations in each jurisdiction.

Legal: Document review, Predictive analytics for case outcomes, Contract analysis, Legal research

Generative AI: Content creation, Language translation, Personalized marketing, Code generation

Labor: Workforce management, Skill matching, Employee performance analytics, Predictive hiring

	Healthcare	Mobility	Finance	Legal	GenAI	Labor	Other Comments
Japan	PL Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices (薬機法)	PL the Act on Vehicles for Road Transportation (道路運送車両法), Road Traffic Act(道路交通安全法)	PL Installment Sales Act(割賦販売法) to become the “Certified Comprehensive Credit Purchase Intermediary” (※J1)	NA (※J2)	UD (※J3)	NA	
EU	PL Medical Devices Regulation (MDR), and the In Vitro	PL Type-Approval Framework Regulation (TAFR) and	TC/SC High risk AIs include: Credit-worthiness.	TC/SC High risk AIs include: (i) Judicial and	TC/SC Systemic Risk: Notification to Commiss	TC/SC High risk AIs include: (i) Recruitment and selection,	Under the AI Act, High-risk AIs will have to (a) register in a EU database, and (b) perform pre-

	Healthcare	Mobility	Finance	Legal	GenAI	Labor	Other Comments
	Diagnostic Medical Devices Regulation (IVDR) TC/SC AI Act (High risk AIs include: (i) Public authority assistance, (ii) insurance risk assessment, (iii) Emergency response management)	(2) the General Safety Regulation (GSR) UD Autonomous Vehicles (sectorial regulation)		dispute resolution assistance, (ii) Election/public opinion influence	ion, and publicly listed	(ii) Workplace decisions	market Conformity Assessments (CAs). Generally, for AIs classified as high-risk systems: (i) When there's no harmonized standards, then Mandatory TC CA; (ii) where there are harmonized standards, then Mandatory SC CA. General Purpose AIs have their own assessment.
US (Federal/other)	Federal: PL Federal Food, Drug, and Cosmetic Act (all medical devices are	Federal: PL (※US1) Safely Ensuring Lives Future Deployment and Research	Federal: NA (※US2)	Federal: NA	Federal: NA California a UD Safe and Secure	Federal: NA New York City: TC for hiring algorithms	Colorado: NA? “Consumer Protections in Interactions with Artificial Intelligence Systems” (the

	Healthcare	Mobility	Finance	Legal	GenAI	Labor	Other Comments
	subject to the Federal permission)	In Vehicle Evolution Act (2017) States: PL/UD Many states including California, Florida, Arizona etc. introduced State acts.			Innovation for Frontier Artificial Intelligence Models Act (SB1047) (※ US3)		Colorado AI Act) (※ US4)
UK	PL/UD UK Medical Devices Regulations 2002 (Detailed guidance specifically for AIaMD products to be provided in Spring 2025)	PL Automated Vehicles Act 2024 (Authorisation of road vehicles for automated use/ Licensing of operators for vehicle use without user-in-charge/	NA The FCA (Financial Conduct Authority) addresses a tech-neutral approach (AI Update , 3.2)	NA	NA (UD?) On July 17, 2024, it was reported that the new government aims to regulate most powerful	NA	The UK Government's March 2023 white paper 'A pro-innovation approach to AI regulation' laid out the framework for current plans to regulate of AI. This would take a non-statutory approach, relying on existing regulators to oversee

	Healthcare	Mobility	Finance	Legal	GenAI	Labor	Other Comments
		Permits for automated passenger services)			AI models		the use of AI in their areas while following five broad principles: safety, transparency, fairness, accountability, and contestability.
Canada	PL Canada's federal Medical Device Regulations (SOR/98-282) under the Food and Drugs Act require pre-market approval (licensing) for software as a medical device (including AI).	PL In 2018 the Motor Vehicle Safety Act was amended to add limited exemptions for AVs meeting certain standards. Provincial pilot programs govern autonomous vehicle testing; no finalized nationwide AV regulation yet.	UD Bill C-27 may be applicable	UD Bill C-27 may be applicable	UD Bill C-27 may be applicable	UD Bill C-27 may be applicable	Bill C-27 (the proposed "AI and Data Act") is under parliamentary discussion and would impose obligations (e.g. risk management, assessment) on "high-impact" AI systems. The definition of high-impact AI systems is not clear but it may cover AI systems impacting access to services or employment, biometric identification and inference, large-scale

	Healthcare	Mobility	Finance	Legal	GenAI	Labor	Other Comments
							behavior influence, and critical health and safety.
Singapore	PL (※S1) Health Products Act 2007 (as detailed guidelines and guidance, “Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach Revision 2.0” and “Medical Devices Guidances”)	PL (※S2) Road Traffic (Autonomous Motor Vehicles) Rules 2017(as detailed standards, “Technical Reference 68 (2019), which was revised in 2021)	NA (※S3)	NA (※S4)	NA (※S5)	NA (※S6)	
China	PL	PL (Public Trans.)	PR (Must (i) have “investment	NA (encourag ement for	PR	NA	

	Healthcare	Mobility	Finance	Legal	GenAI	Labor	Other Comments
General registration requirements, and security assessments, for algorithms with (a) public opinion properties or (b) the capacity for social mobilization	(1) Devices: Depending on risk Classification; (2) Practice: Local laws (i.e. Beijing prohibits use of AI in diagnosis and treatment services w/o supervision)	TC/SC (Private Trans.: Safety guidelines)	advisory qualifications”, and (ii) “file the main parameters of its artificial intelligence model and the main logic of asset allocation with the financial regulatory authority.	development in judicial decision-making)	Registration requirements, and security assessments, for algorithms with (a) public opinion properties or (b) the capacity for social mobilization	(specific protection in Algorithm Law)	

※注釈

Japan

※J1 (Finance)

金融関係は「割賦販売法」で「AI による貸付可能額の算定」に関連した規制(認定制度)が存在している(利用が認められる(AI を利用した]システムについての概括的な要件は同法施行規則で定められている)が、金融関係における一般的な AI の利用等に関する法規制(認証・認定・登録制度等)は現時点では確認できなかった。

「金融データ活用推進協会(FDUA)」(銀行や生命保険・損害保険会社が参加する業界団体)が、「生成 AI」に関連した「金融生成 AI 実務ハンドブック」(2024 年 5 月)及び「金融機関における生成 AI の開発・利用に関するガイドライン」(2024 年 8 月)に公表したが、いずれも認証等が視野に入れられたものではない。

※J2 (Legal Advice)

・リーガルアドバイス全般ではなく、いわゆるリーガルテック(Legal Tech)のうち、「契約書レビュー」と弁護士法 72 条との関係について、2023 年 8 月に法務省よりガイドラインが示された(法務省大臣官房司法法制部「AI 等を用いた契約書等関連業務支援サービスの提供と弁護士法第 72 条との関係について」)が、リーガルアドバイスにまつわる AI に関する規制等については現時点で確認することができたのは、このガイドラインのみである(現時点では、規制の導入等に関する議論も特段なされていない模様)。

※J3 (GenAI)

内閣府の AI 戦略会議で現在議論中。

United States

※US1 (Mobility)

連邦レベルでの自動運転車を規制する主要な法律は、2017 年 6 月 9 日に成立した the Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution Act である。この法律は、それが連邦基準と同一である場合には、各州が自動運転車に関する法律を制定することができることを規定するものであり、州レベルの法制化への道を開いている。また、この法律は、運輸省に対して安全性評価の実施や Highly Automated Advisory Council の設置を義務付けている。

(参考: <https://www.holisticaai.com/blog/ai-regulations-for-autonomous-vehicles>, また、次の JETRO のウェブサイトも参照:
<https://www.jetro.go.jp/biz/areareports/2023/bcdf631c4ffdb352.html>,
<https://www.jetro.go.jp/biznews/2024/04/65d431a83da79f72.html>)

※US2 (Finance)

この大統領令は、消費者金融保護局 (Consumer Financial Protection Bureau : CFPB) 及び連邦住宅金融局 (Federal Housing Finance Agency: FHFA) に対して、これらの当局が、AI ツールを使用して連邦法への遵守を確保し、保護対象グループに対するバイアスの有無を評価するためのアンダーライティングモデルを評価し、バイアスを最小化するために自動化された担保評価や査定プロセスを評価するよう指示をするものである。

この大統領令では、規制当局が権限を行使して、詐欺、差別、プライバシーへの脅威からアメリカの消費者を保護し、金融の安定性へのリスクに対処することが期待されている。各機関には、既存の規制やガイダンスが AI にどのように適用されるかを明確にすることが求められている。

大統領令では、特にベンダーのデューデリジェンス(例として、2023 年 6 月に連邦準備制度理事会 (Federal Reserve Board : FRB)、連邦預金保険公社 (Federal Deposit Insurance Corporate: FDIC)、通貨監督庁 (Office of the Comptroller of the Currency: OCC) によって発行されたガイダンスである Interagency Guidance on Third-Party Relationships: Risk Management) や、AI モデルの透明性及び説明可能性に関する要件や期待(例として、OCC のハンドブックである Model Risk Management (このハンドブックでは、銀行がリスク評価の方法論で AI モデルを使用する場合に説明可能性を評価するよう監査官に求めている))が引用されている。

(参考: <https://www.skadden.com/insights/publications/2023/12/how-regulators-worldwide-are-addressing-the-adoption-of-ai-in-financial-services>)

※US3 (GenAI)

学習開始前に、対象モデルに取り組む従業員及び契約委託先による順守の確保、実施状況の監視及び報告、並びに第三者監査人による監査を含む監査の実施に責任を負う上級役員を選任することを含め、安全性とセキュリティのプロトコルが文書通りに実施されることを確保することが求められる。

(参考: <https://www.nikkei.com/prime/digital-governance/article/DGXZQOUC241HT0U4A620C2000000>)

※US4

同法案は、AI システムの開発者及び配備者に対して、教育機会や雇用機会、金融サービス、行政サービス、医療サービスなどの分野において、アルゴリズムに基づく決定によって消費者が差別的な取り扱いを受けることを避けるために合理的な注意を払うことを要求するもの。具体的には、開発者は、システムの種類・管理方法に関するステートメントを作成するとともに、配備者が影響評価を行うために必要な情報を入手可能とすることなどが求められる。配備者は、システムのリスク管理方針・プログラムの実施や、影響評価を完了させることのほか、システムが消費者に関する決定を行った場合、特定事項を消費者に通知することや、システムに起因する消費者に関する不利な決定について、技術的に可能であれば、人的な審査を通じて不服を申し立てる機会を消費者に提供することが求められる。

また、開発者・配備者ともに、システムが差別を引き起こしたことが判明したなどの場合には、90 日以内に司法長官に当該リスクを開示することとされている。なお、同法案には私的訴権に関する内容は含まれておらず、司法長官室によってのみ執行が可能とされているが、要求事項を順守していれば、開発者及び配備者は合理的な注意を払ったという推定がなされることとなる。

(参考: <https://www.jetro.go.jp/biznews/2024/05/f8314d21a2862c13.html>, <https://www.perkinscoie.com/en/news-insights/states-begin-to-regulate-ai-in-absence-of-federal-legislation.html>)

Singapore

※S1 (Health Care)

健康機器法 (Health Products Act 2007) により AI を用いた医療機器についてもライセンス制度が採用されているが、要件等についてはガイドライン (Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach Revision 2.0 (April 2022)) やガイダンス (Medical Devices Guidance) で対応されている。

※S2 (Mobility)

自動運転車両の審査・認証制度については、道路交通法 (Road Traffic Act) (及び直接的には、2017 年の道路交通 (自動運転) 規則 (Road Traffic (Autonomous Motor Vehicles) Rules 2017: RTA 2017)) に基づき、陸上交通庁から委託を受けた CETRAN (Centre of Excellence for Testing & Research of Autonomous Vehicles) が行っている (書類審査のほか、テストベクトでの実走審査が行われる)。

規格そのものについては、2019 年にシンガポール規格評議会 (Singapore Standards Council: SSC) の製造規格委員会 (The Manufacturing Standards Committee :MSC) (シンガポールの貿易産業省 (MTI) 傘下のシンガポール企業庁 (Enterprise Singapore) により設立されたシンガポールの SSC の機関の 1 つ) によって任命された自動車技術委員会 (Technical Committee on Automotive) によって監督され、AV 業界、研究機関、高等教育機関、政府機関の代表者で構成される 4 つのワーキング・グループにより「TR68 (Technical Reference for Autonomous Vehicles (Avs))」という暫定規格が示されている (2021 年に更新があった模様)。今後、業界からのフィードバックを受けながら都度更新されることが予定されている。

※S3 (Finance)

認証制度等は設けられていない模様。

シンガポール金融管理局 (Monetary Authority of Singapore: MAS) が 2018 年 11 月に FEAT 原則 (Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT)) を示したほか、2022 年 2 月にその評価手法を詳述したホワイトペーパーを開示するなど、ソフトローを用いた規制が行われている (また、2023 年 6 月に各金融機関が当該評価手法を実

施する際に利用可能な Veritas コンソーシアム(MAS 主導の業界 31 社によるコンソーシアム)が発行するツールキットも公表された)。

※S4 (Legal Advice)

認証制度等のほか、法規制も設けられていない模様。

なお、2024 年 5 月末、情報通信メディア開発庁 (Infocomm Media Development Authority: IMDA) とシンガポール法曹協会 (Singapore Academy of Law) が新しい大規模言語モデル (PLM) を共同開発し、Legal Research において活用していく予定であることが報道されており、今後、Legal Advice 分野への技術展開の可能性もあるものと予想される。

(参考: <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/factsheets/2024/gpt-legal>)

※S5 (GenAI)

認証制度等は設けられていない模様(後述の 2024 年 5 月末公表のモデル AI ガバナンスフレームでは、third-party testing の必要性等について言及されているが、一般的な言及に留まっている)。

2023 年 6 月に情報通信メディア開発庁 (Infocomm Media Development Authority: IMDA) と Aicadium (シンガポール政府系投資会社 Temasek Holdings 傘下の AI ソリューション会社) が「Generative AI: Implications for Trust and Governance」を公表するとともに、同月、IMDA は、AI の信頼性を検証するための AI ガバナンス・テスト・フレームワークとソフトウェアツールキットである AI Verify の開発とともに、AI の責任ある利用を推進し、世界中の企業や規制当局のニーズを満たすための団体として、AI Verify Foundation の設立を公表。

また、2024 年 5 月末に、AI Verify Foundation と情報通信メディア庁より、生成 AI 向けのモデル AI ガバナンスフレーム (Model AI Governance Framework for Generative AI) が公表された (2019 年に情報通信メディア開発庁 (IMDA) と個人情報保護委員会 (Personal Data Protection Commission: PDPC) により従来型の AI に関して作成されていた (2020 年に Ver.2.0) が、生成 AI 向けに新たにフレームワークが策定された)。

※S6 (Workforce & Labor)

労務関連の AI の利用に関する法規制等はなく(議論も特になされていない模様)、一般的な倫理原則(例えば、Model AI Governance Framework 2nd Edition (Jan 2020))の Fairness の項目中で AI による決定において差別的影響が生じることへの配慮の必要性が言及されているにとどまる。

別紙 2 EU:ハイリスク AI システムに関する AI 法の要件の概要

EU AI 法における市場導入のための要件： 自動運転車と医療機器に関するハイリスクの分類

Socol de la Osa David Uriel

本別紙では、(i) (医療機器に焦点を当てて)医療、及び(ii) (自動運転車に焦点を当てて)モビリティという重要な分野に影響を与える可能性がある AI システムを市場に導入するために必要となる特定のプロセスに焦点を当てながら、EU AI 法における一般的要件の概要について説明することとする。

特定のカテゴリーの AI システムを市場に導入する場合の AI の規制は、次のとおり、二重構造の規制枠組みの下で行われている¹。

1. EU AI 法における AI の一般的ガバナンス(同法は、リスク分類に基づいた AI システムに関する要件を定めている。)
2. 分野別の規制(例えば、医療機器に関する医療機器規則(MDR)²や、自動運転車に関する型式認証枠組み規則(TAFR)³など。)

本別紙の対象

本別紙は、分野別の規制ではなく、ハイリスク AI システムとしての自動運転車と医療機器に関する EU AI 法の一般的要件に焦点を当てている。モビリティ分野や医療分野における AI は、業界固有の規制枠組みにも含まれる可能性があるが、本別紙では、EU AI 法に基づく包括的な遵守すべき義務と、それらがハイリスク AI に分類された自動運転車や医療機器の構成要素にどのように適用されるかを取り上げる。これらの要件を詳述することで、本別紙は、ハイリスクとされる AI システムに対して規制上期待されている基本的事項を明らかにし、報告書を補完するものである。

主な対象分野は次のとおりである。

- EU AI 法における AI システムの分類、及びこれと自動運転車・医療機器との交差。

¹ 報告書本文の [2\(1\)\(iii\)](#) 及び [2\(2\)\(iii\)](#) を参照。

² これには、Regulation (EU) 2017/745, OJ L 117, 5.5.2017, p.1-175 及び Regulation (EU) 2017/746, OJ L 117, 5.5.2017 が含まれる(これらは医療機器及び体外診断用医療機器を一般的に規制している。)

³ これには、Regulation (EU) 2018/858, OJ L 151, 14.6.2018, p.1-218, Regulation (EU) 2019/2144, OJ L 325, 16.12.2019, p.1-40 及び Commission Implementing Regulation (EU) 2022/1426, OJ L 221, 26.8.2022, p.1-64 が含まれる(これらは型式認証を一般的に規制すると共に、自動運転車の各項目に具体的に言及している。)

- 市販前のハイリスク AI システムに関する登録義務。
- 適合性評価手続(自己評価が認められる場合と第三者評価が必要な場合の概要)。
- 要遵守事項(リスクマネジメント、人間による監視、技術文書を含む)。

EU AI 法における一般的要件とその遵守のプロセス

ハイリスク AI システム: AI システムが、個人の健康、安全、又は基本的権利に重大な危害を及ぼすリスクがある場合には、一般的にそれはハイリスク AI とみなされる⁴。本報告書で取り上げる分野(自動運転車と医療機器)は、特に医療分野やモビリティ分野における重要な機能と交差する部分において、ハイリスク AI システムに該当する可能性がある構成要素を含んでいる。Annex III では、特定の用途(道路交通管理や保険リスク評価など)がハイリスク AI として明示的に指定されている。

登録義務: ハイリスク AI の提供者(provider)は、ハイリスク AI システムを市場に導入し又はサービスに供する前に、欧州委員会の監督下にある EU データベースにそのシステムを登録しなければならない(第 49 条、第 71 条)。

事前の適合性評価: EU AI 法では、ハイリスク AI の提供者は、登録に加えて、事前の適合性評価を行わなければならない——これは、市場に導入する前に行わなければならない重要な要遵守事項である(Chapter III, Section 5)。

- 遵守方法: 事前の適合性評価は、EU AI 法に定められた要件への適合性を証明する手段である。ハイリスク AI システムの開発者は、システムを EU の市場に導入する前に事前の適合性評価を行わなければならない(第 43 条)。
- 適合性評価を行う主体: 事前の適合性評価は、AI システムの分野や整合規格(harmonised standards)の有無・使用状況に応じて、提供者が自ら行うか、又は第三者機関(Annex VII の評価を実施する機関である「適合性評価機関」)によって行われることとなる(第 40 条～第 43 条; 前文(78), (123)-(128), (147))。
 - 自己評価: ハイリスク AI システムの提供者は、一般的に、適合性評価機関の関与なしに自己適合性評価(Annex VI)を行うことができる。これは、Annex III, Point 2～8 に列挙されている全てのハイリスク AI システム(これには医療分野や重要なインフラとしての交通分野におけるモビリティ分野における利用が含まれる。)に適用される。ただし、Annex III, point 1 (EU 法又は加盟国の国内法で許可されている生体認証に関する AI システム)については、整合規格(第 40 条)又は共通仕様(common specifications)(第 41 条)が存在し、かつ、それが完全に適用される場合に限り、自己評価を行うことができる。

⁴ ハイリスク AI システムに該当する可能性があるものに関するより詳細な説明は、後記 1.2 を参照。また、Regulation 2024/1689, of the European Parliament and of the Council of 13 June 2024, laying down harmonised rules on artificial intelligence, 2024 O.J. (L 210) 1 (「EU AI 法」)の第 6 条、前文(46)～(63)、Annex I 及び Annex III も参照。なお、本別紙において引用されている条項等は、特にその旨を明示しない限り、EU AI 法に関するものである。

- 第三者機関(「適合性評価機関」)による評価: 整合規格が存在しない場合、これが完全には適用できない場合、又は共通仕様が利用できない場合には、第三者による適合性評価(Annex VII)が必要となる。生体認証に関する AI システム(Annex III, point 1)については、整合規格又は共通仕様を使用できない場合、又は完全には適用できない場合には、常にこのことが妥当する。ただし、その他の全てのハイリスク AI システム(Annex III, Point 2~8)については、自己評価のみが求められ、適合性評価機関を関与させる義務はない。
 - プロセスの項目:
 - 適合性評価機関: 適合性評価機関は EU 加盟国によって指定される(Chapter III, Section 4, 第 28 条)
 - 整合規格・共通仕様: 整合規格に準拠する AI システムは、EU AI 法の法的要件及び技術的要件に適合しているものと推定される。整合規格の策定は、複数の関係者が関与するプロセスである。:すなわち、整合規格は、欧州委員会が標準化要求を発出し、欧州標準化機関、専門委員会、各国当局、その他の利害関係者と協力の下で策定される。整合規格は、最終化された後、EU 官報に掲載されることによって正式に承認されることとなる。整合規格が利用できない場合、策定が遅れている場合、又は基本的権利に関する懸念に適切に対処できていない場合には、欧州委員会は実施規則を通じて共通仕様を採択し、正式な整合規格が存在しない場合でも規制の明確性を確保することができる(第 40 条、第 41 条; 前文(121))。
- 適合性評価の対象者: 原則として、ハイリスク AI の提供者が、AI システムを市場に導入する前に適合性評価を行う責任を負う(第 16 条、第 25 条)。ただし、例外的に、この責任が他の事業体に移る、あるいは、他の事業体が EU AI 法の提供者とみなされる場合がある。例えば、AI システムが EU 整合法令(harmonisation legislation) (Annex I)の対象となる製品の安全性に関する構成要素であり、それが当該製品と共に製造者(manufacturer)の名若しくは商標で市場に導入される場合、又は、市場に導入された後に製造者の名若しくは商標でサービスに供される場合には、製造者は提供者としての義務を負う可能性がある(第 25 条第 3 項)。さらに、輸入業者(importer)、販売業者(distributor)又はディプロイヤー(deployer)は、自らの名又は商標でハイリスク AI を市場に導入する場合、提供者が定めた目的を変更する場合、又は要遵守事項の遵守に影響を与えるような重大な変更を加える場合には、提供者とみなされ、適合性評価を行う義務を負う可能性があり、これらの義務は、これらの者が AI のバリューチェーンにおいて果たす役割や、AI システムのリスクの程度に応じて異なっている(第 23 条~第 27 条; 前文(83)~(90))。
- 適合性評価の範囲・主な事項: 適合性評価は、Chapter III, Section 2 に定められた義務を遵守していることを証明するために必要なものである。適合性評価は、ハイリスク AI システムが、市場への導入及び継続的な運用のために必要な法的要

件、技術的要件及び手続的要件を満たしているかどうかを評価するものである(第 43 条)。

評価の対象となる主な事項は、次のとおりである。

- リスクマネジメントシステム — AI のライフサイクル全体にわたるリスク緩和措置の実施(第 9 条)。
 - データ及びデータガバナンス — 高品質なデータセット、バイアスの緩和、トレーサビリティの確保(第 10 条)。
 - 技術文書 — システム設計、学習プロセス、機能性に関する詳細な記録の保管(第 11 条)。
 - 記録の保存 — 説明責任のためのシステムパフォーマンス、決定、データ処理の記録(第 12 条)。
 - 透明性及びユーザーへの情報提供 — システムの性能、リスク及び限界の明確な伝達(第 13 条)。
 - ヒューマン・オーバーサイト — 自動化のリスクを防止するための必要に応じた人間による介入の仕組みの確立(第 14 条)。
 - 正確性、頑健性及びサイバーセキュリティ — システムの信頼性、敵対的な攻撃に対する耐性、及びエラーに対するレジリエンスの確保(第 15 条)。
 - 追加的要件: 基本的権利影響評価 — ハイリスク AI システムは、基本的権利に対する潜在的な影響を評価するための基本的権利影響評価を受けなければならない(第 27 条)。
- 有効期間: 適合性評価機関は、AI システムのカテゴリーに応じて、認証を、最長 4 ～5 年延長することができる。AI システムが要遵守事項を満たさなくなった場合には、認証は一時停止又は取り消される(第 44 条)。

重要な点:

- 適合性評価: EU AI 法においては、ハイリスク AI システムの開発及び展開におけるアカウントビリティを確保するために、適合性評価が義務付けられている。
- 適合性評価の目的: 適合性評価は EU AI 法に定められた AI システムに関する特定の要件(特に Chapter III, Section 2 に列挙されたもの)への適合を証明するために用いられる。
- 適合性評価のタイミング: 開発者は、ハイリスク AI システムを市場に導入する前、又は EU 内で初めて使用する前に適合性評価を完了させなければならない。
- 適合性評価の実施: 整合規格又は共通仕様が存在し、かつそれを使用しているか否かに応じて、適合性評価は、(i) 原則として提供者による自己評価、又は (ii) 外部の第三者機関(加盟国が指定)の評価のいずれかによって行われる。

1.2 分野別の分析:

EU AI 法においては、AI システムは、前文(46)～(63)に示された考慮事項のみならず同法第 6 条に概説された基準を満たした場合のほか、特定の AI システムが Annex I に列挙された EU 整合法令の対象であるかどうかに応じて、ハイリスクに分類される。大まかに言えば、個人の健康、安全、又は基本的権利に重大な危害を及ぼすリスクがある場合には、そのシステムはハイリスクとみなされる。これには、個人に悪影響を及ぼし得る形で意思決定プロセスに重大な影響を与える AI も含まれる。また、潜在的な危害の重大性や規模、システムの意図された用途、運用におけるヒューマン・オーバーサイトの程度も考慮される。

これらの基準を踏まえた場合、自律的なモビリティ分野や医療分野における多くの AI の利用は、ハイリスク AI の範囲に含まれる可能性がある。自動運転車で使用される AI——特にナビゲーション、衝突回避、リアルタイムの意思決定などの安全上重要なアプリケーションで使用される AI——は、生命や公共安全に直接的な影響を与える可能性がある。同様に、診断、治療の推奨、リスク評価のために AI を組み込んだ医療機器は、患者の健康や予後に重大な影響を与える可能性がある。

これらの一般的な基準に加えて、EU AI 法の Annex III は、特定の AI システムを明示的にハイリスクとして挙げており、これにより、自動運転車と医療機器の特定の用途を、規制監督を強化すべき対象として指定している。EU AI 法は、特定の分野を対象とする規制に取って代わるものではないが、(i)医療や(ii)モビリティを含むハイリスク領域における特定の AI システムに対して、追加の義務を課している。

i. 医療

Annex III, Point 5(a), (c), (d) は、医療分野における AI システムを「不可欠な民間サービス・給付及び不可欠な公共サービス・給付へのアクセスと享受」に該当するものとしてハイリスクに分類している。このカテゴリーに含まれる AI の用途には次のものが含まれる。

- 公的機関による支援：医療サービスを含む重要な公的給付・サービスの受給資格を決定し、この給付を管理（付与、削減、取消）するために、公的機関により又は当該機関に代わって使用される AI システム。
- 保険リスクの評価：個人の生命保険及び医療保険に関するリスク評価と価格設定のために使用される AI システム。
- 緊急対応管理：緊急通報の評価と優先順位付け、エマージェンシー・サービス（警察、消防、医療支援を含む）の派遣、及び、緊急医療患者のトリアージを行うための AI システム。

以上の明示的に挙げられた用途以外にも、AI による診断、ロボット支援手術、疾病予防における予測分析も、特に患者の予後に重大な影響を与える可能性がある重要な意思決定に使用される場合には、厳格に精査されることになる。

ii. モビリティ

EU AI 法は自動運転車を直接的に規制するものではないが、モビリティ分野における AI の特定の用途——特に道路交通管理及び公共の安全に関連するもの——は、ハイリスクに分類される。Annex III, Point 2 は、重要なインフラ(道路交通)における AI をハイリスクと特定しており、これには次のような用途が含まれる。

- 交通管理及び交通安全システム、重要インフラ：重要なインフラネットワークに影響を与える AI システムは、EU AI 法の下ではハイリスクに分類されることとなる。これには、事故防止、交通の流れの最適化、公共の安全の確保において重要な役割を果たすような AI を用いた技術が含まれる可能性がある。特に、道路の渋滞、横断歩道、交通規制を管理する AI を用いたシステムは、重要インフラの運用に与える影響如何では、このハイリスクのカテゴリーに該当する可能性がある。

さらに、モビリティ分野における AI のその他の用途も EU AI 法のハイリスクに分類される可能性があるが、この点について明確には定義されていない。

- AI による運転支援及び衝突回避：完全自動運転車は、主に分野別規制(例えば、TAFR)が適用されるが、リアルタイムの安全上重要な意思決定に使用される AI サブシステム——例えば、車線維持支援、自動ブレーキ、危険検知など——は、その機能が公共の安全やインフラの完全性に重大な影響を与える場合には、EU AI 法の下でハイリスクと解釈される可能性がある。もっとも、これらのシステムが EU AI 法の適用範囲にどの程度含まれるかについては、規制当局の解釈、今後の執行実務、EU AI 法と特定の分野別規制との相互作用のあり方に左右される面が残されている。
- 公共交通機関の AI システム：乗客の安全、スケジュール管理、予知保全、インシデント対応のために公共交通機関のネットワークに導入される AI システムも、EU AI 法のハイリスク枠組みの対象となる可能性がある。公共交通機関は不可欠の移動インフラであることを踏まえると、この分野における AI の特定の用途——特に、その故障や不適切な管理がサービスの中断や公共の安全への懸念に繋がりが得るような場合——について EU AI 法の規定を遵守することが必要となる可能性がある。ただし、このようなシステムの規制上の取扱いは依然として

明確ではなく、規制当局が重要インフラの分類の中でその役割をどのように解釈するかによって決まることになると考えられる。

自動運転技術は主に分野別規制の対象にあるが、EU AI法は、重要インフラという分類を通じて、道路の安全性や交通管理に影響を与える安全上重要な AI の用途に関する基本的な義務を定めている。モビリティに特化した法律と AI に関する規制との交差は、整合規格の策定が進み、AI を用いた自動運転車の特定の構成要素が輸送と AI ガバナンスの枠組みの双方において更に精査されるにつれて、発展していくことが見込まれる。