令和 7 年度 厚生労働科学研究費
（医薬品・医療機器等レギュラトリーサイエンス政策研究事業）

AI を用いた医療情報の医薬品安全への活用に向けた諸要件の調査研究
分担 研究報告書

－医薬品安全性監視活動（PV）への人工知能（AI）技術導入に関する倫理的・法的・社会的課題に関する調査：PV 業務における個人情報・個人データ保護の観点から－

研究分担者　鈴木晶子
国際高等研究所 主席研究員・京都大学名誉教授

研究要旨

本研究は、医薬品安全性監視（Pharmacovigilance, PV）分野における人工知能（AI）の導入をめぐる動向について、制度・データ・技術の三層を横断的に整理し、その構造的理解を提示することを目的とする。近年、医療 DX の推進に伴い、医療・介護データの利活用が制度的に整備されるとともに、リアルワールドデータ（RWD）を活用した市販後安全対策の高度化が進展している。他方で、AI 技術の導入は、従来の人間中心の判断構造に対し、学習と推論の分離、モデルの残存性、判断過程の不可視性、責任主体の分散といった新たな構造的課題をもたらす。

本研究では、まず日本における医療データ利活用の制度環境および欧州 EHDS の動向を整理し、次に PV 分野における RWD 活用の実務構造を明らかにした。その上で、RAG（Retrieval-Augmented Generation）およびログ管理に着目し、AI 利用における知識の所在と判断過程の可視性に関する論点を概念的に分析した。さらに、これらの検討を踏まえ、目的明確性、人間責任、監査可能性等の基本原則を整理するとともに、「閉域運用×非学習・非保持×人の判断記録」を中核とする最小安全構成という視点を提示した。

本研究は、特定の制度設計や技術導入の是非を示すものではなく、今後の国内外における PV×AI の議論に対し、制度・技術・実務の交差における構造的理解に基づく参照枠を提供するものである。

A. 研究目的

近年、医療分野においては、医療 DX の推進を背景として、医療・介護データの利活用が急速に進展している。とりわけ、全国医療情報プラットフォームの構築、公的データベースの整備、さらには仮名化情報の利活用を可能とする制度改正などを通じて、医療データの二次利用は政策的に強く位置づけられるに至っている。

これと並行し、人工知能技術の医療分野

への導入も進展している。なかでも医薬品安全性監視活動（Pharmacovigilance, PV）では、リアルワールドデータ（RWD）の活用と AI の組み合わせにより、安全対策の高度化および効率化が期待されている。

しかしながら、これらの動向は単なる技術革新にとどまるものではない。医療データの利活用と AI の導入は、判断主体、責任構造、データの取扱い、さらには公共性の位置づけといった、制度および実務の前提そのものに変化をもたらしつつある。

従来の PV 業務は、人間の専門的判断を前提とする構造のもとで運用されてきた。すなわち、データの収集、評価、因果関係の判断といった各プロセスは、人間の判断を中核として構成されている。

これに対し、AI の導入は、学習と推論の分離、モデルの継続的利用、判断過程の不可視性、さらには責任主体の分散といった新たな構造的特徴をもたらす。また、RAG（Retrieval-Augmented Generation）のような外部参照型 AI の登場は、知識の所在をモデル内部から外部データへと拡張し、判断過程の構造そのものを変容させる可能性を有する。

このような変化に対し、現行の制度やガイドラインは、主として個別の論点や原則の提示にとどまり、全体としての構造的理解は必ずしも十分に整理されているとはいえない。したがって、PV×AI をめぐる課題は、個別技術の是非としてではなく、制度・技術・実務が交差する構造の再編として捉える必要がある。

以上のような問題意識に基づき、本研究では、PV 分野における AI 導入をめぐる議論を、制度・技術・実務の交差する構造として捉え直し、その全体像を明らかにすることを試みる。

本研究の目的は、PV 分野における AI 導入をめぐる議論について、制度的前提、実務構造および技術的特性を横断的に整理し、その構造的理解を提示することにある。

具体的には、①医療データ利活用をめぐる制度環境の整理、②PV 分野における RWD 活用の構造把握、③AI 導入による構造的変化の概念整理、④RAG およびログ管理を含む AI 利用形態の分析、⑤基本原則および今後の方向性の提示を行う。

なお、本研究は、特定の技術導入や制度設計の是非を判断することを目的とするものではない。

B. 研究方法

本研究は、以下の二層構造を採用する。

第一に、医療データ利活用および PV 分野に関する制度・法的枠組みについて、既存の調査報告を基礎資料として整理し、議論の前提となる制度環境を明確化する。

第二に、これらの制度的前提を踏まえ、AI 導入に伴う構造的変化を概念的に分析し、その特徴を抽出する。その際、本研究は実装論には踏み込まず、また特定のガイドライン策定や規範の確定を目的とするものではなく、方向性の提示をするものである。つまり、本研究は政策提言や実務指針の提示を直接の目的とはせず、今後の議論における参照枠（フレームワーク）を提供することを目指す。

なお、医療データ利活用および関連法制度の整理にあたっては、外部専門家の協力により作成された調査報告書を基礎資料として用いている。同報告書は、本研究におけ

る制度的前提を構成する重要な資料として位置づけられる。

本報告書の構成は以下のとおりである。第Ⅰ部では、医療 DX および医療データ利活用の制度環境を整理するとともに、EHDS を中心とした国際的動向を概観する。第Ⅱ部では、PV 分野における RWD 活用の現状を整理し、その制度的・実務的構造を明らかにする。第Ⅲ部では、AI 導入による構造的変化を分析し、RAG およびログ管理に関する論点を整理した上で、基本原則および今後の方向性を提示する。

本研究は、PV 分野での AI 利活用について、個別の技術評価や制度設計に先立つ段階において、全体構造を俯瞰的に整理する試みである。特に、制度（医療 DX・法規制）、データ（RWD）、技術（AI・RAG）の三要素が交差する領域において、それらを統合的に捉える視座を提示する点に特徴がある。その意味で、本研究は直接的な結論を提示するものではないが、今後日本を含め国際的に展開されていくであろう PV×AI に関する議論の前提となる枠組みを提供するものである。

C 結果および考察

本報告書は、PV 分野における AI 導入をめぐる構造的課題を多面的に整理するため、以下の構成で検討を行った。

まず、第Ⅰ部では、制度環境の整理として、PV 業務に関連する個人情報保護および個人データ利活用に関する国内外の検討体制と主要論点を概観する。第 1 章では医療 DX および医療データ利活用の動向を整理し、第 2 章では EHDS 等の国際的動向を含めた制度的枠組みを検討する。

次に、第Ⅱ部では、PV 分野における RWD 利活用の構造に焦点を当てる。第 3 章では、PV 業務における RWD 活用の現状を整理し、その制度的・実務的特徴を明らかにする。第Ⅲ部では、PV 領域への AI 導入に伴う構造転換を扱う。第 4 章では AI 導入により生じる構造的課題を分析し、第 5 章では RAG およびログ管理を中心に、AI 利用形態に関する論点を概念的に整理する。

さらに、第Ⅳ部では、これらの検討を踏まえたガバナンス枠組みを整理する。第 6 章では PV×AI に関する基本原則を提示し、第 7 章では今後の国内向けガイダンス作成に向けた要点を整理する。

第Ⅰ部 制度環境の整理：PV 業務における個人情報保護・個人データ保護についての国内外の検討体制および主要な論点

第 1 章 医療 DX[1)]と医療等データ利活用の動向

第 1 章は、本報告書において PV×AI の議論を展開する前提として、日本における医療データ利活用をめぐる制度環境を整理するものである。

近年、医療 DX の推進を背景として、医療・介護分野におけるデータの収集、連携および二次利用が政策的に強く位置づけられており、その制度的枠組みは大きく変容しつつある。特に、医療 DX 工程表、改正医療法、次世代医療基盤法、個人情報保護法の見直しといった一連の制度動向は、医療データの利活用を「公益性」「安全管理」「ガバナンス」の枠組みの下で推進する構造を形成している。以下では、これらの制度的前提について、政策動向および法的枠組みの観点

から整理する。

第 1 章第 1 節 政府が推進する医療 DX と医療等データの利活用

現在、政府は「医療 DX の推進に関する工程表」（令和 5 年 6 月 2 日 医療 DX 推進本部決定）に基づき医療 DX を推進しており、その取組の一環として全国医療情報プラットフォームの構築を進めている。

全国医療情報プラットフォームとは、オンライン資格確認等システムのネットワークを拡充し、レセプト・特定健診等情報に加え、予防接種、電子処方箋情報、自治体検診情報、電子カルテ等、医療（介護を含む。）全般にわたる情報の共有・交換を可能とする全国的な基盤と位置づけられている。

公表されている構想によれば、この基盤は、医療機関間における患者情報の共有にとどまらず、介護情報基盤や行政・自治体情報基盤との連携も想定されており、当該基盤上で共有される情報の二次利用も視野に入れられている。

また、医療等データの利活用については、厚生労働大臣等が保有する医療・介護関係データベース（公的 DB）の活用が進められている。具体的には、NDB（National Database of Health Insurance Claims）のリモートアクセスによる解析環境の整備や、当該環境で利用可能なデータ範囲の拡大に加え、データ提供に係る審査期間の短縮、不適切利用に対する監視機能の強化等が進められており、匿名化情報の第三者提供による利活用が促進されている。

さらに、「デジタル社会の実現に向けた重点計画」（令和 7 年 6 月 13 日閣議決定）においては、医療データの二次利用を制度的に一層円滑化する観点から、令和 7 年末を目途に中間整理を行い、令和 8 年夏を目途に制度全体の整理を進めることとされている。具体的な検討事項として、以下の点が示されている。

・EHDS（European Health Data Space）規則を参考としつつ、我が国における医療データ利活用（一次利用・二次利用）に関する基本理念および包括的・体系的な制度枠組みと、それと整合的な情報連携基盤の在り方を含む全体像（グランドデザイン）の検討

・対象とする医療データの範囲、収集方法、内容・形式の標準化、ならびに各種データを横断的に解析可能とする患者識別子の整備

・多様な主体が保有する医療データを、一定の強制力またはインセンティブの下で収集・利活用する仕組みおよび研究者や企業等が円滑に利用可能な公的情報連携基盤の在り方（学会データベース等との連結解析を含む）の検討

・仮名化情報の利活用に関する適切な監督およびガバナンスを前提とした患者関与の在り方（同意に依存しない仕組みを含む）の検討

・個人の権利・利益の保護と医療データ利活用の両立に向けた実効的措置（特別法の制定を含む）の検討、

などである。

また、「規制改革実施計画」（令和 7 年 6 月 13 日閣議決定）においても、「医療等データの包括的かつ横断的な利活用法制の整備」が掲げられており、上記重点計画と整合的な内容が示されている。特に、医療等データの二次利用の目的に関しては、公益性が認められる場合の具体例として、「医療機器、

AI システム、デジタルヘルスアプリを含むアルゴリズムのトレーニング、テストおよび評価」が明示されている。

さらに、医療等データの情報連携基盤の構築に関しては、データ利用・提供に際し、氏名等の直接識別子の削除を含む加工基準を定めたガイドライン整備の必要性が指摘されている。また、データベース間連携における突合手段として、被保険者番号やマイナンバーの活用を含む識別子の整備が検討課題とされているが、その際には、再識別リスクの増大を踏まえ、個人の権利利益保護の観点から必要な措置を講じる必要がある点が留意事項として示されている。

第 1 章第 2 節 医療等データの利活用に関する国内法の動向

1 医療法等改正（公的 DB における仮名化情報の利活用）

第 217 回国会（令和 7 年）に提出された「医療法等の一部を改正する法律案」は、同年 12 月 12 日、「医療法等の一部を改正する法律」（令和 7 年法律第 87 号。以下「改正法」という。）として公布された[2)]。

本改正は多岐にわたる内容を含むが、本研究との関係では、医療情報の二次利用の推進を目的として、厚生労働大臣が保有する医療・介護関係データベース（公的 DB）における仮名化情報の利用および提供を可能とした点が特に重要である。以下では、この点に限定して、改正の背景および制度内容を整理する。

まず、改正の背景として、我が国では欧米諸国と比較して、RWD（リアル・ワールド・データ）[3)]等の研究利用が困難であることが従来から指摘されてきた。匿名化情報（本人を識別することおよび復元ができないように加工された情報。以下同じ。）の活用は進展してきたものの、医療分野の研究開発においては、匿名化情報では精緻な分析や長期追跡が困難であるという限界がある。

一方で、氏名等を削除して作成される仮名化情報（以下「仮名化情報」という。）は研究利用への期待が高いにもかかわらず、公的 DB においては十分に利用可能な状況に至っていなかった。さらに、民間企業や学会等が保有する複数のデータベースが分散的に存在しており、利用者は個別に申請・審査を受ける必要があるほか、データの利用環境についても厳格な要件が課されていることから、利活用に係る負担が大きいという課題があった。

これらの課題を踏まえ、改正法は、公的 DB における仮名化情報の利活用を可能とするとともに、他の公的 DB や「医療分野の研究開発に資するための匿名加工医療情報及び仮名加工医療情報に関する法律」（平成 29 年法律第 28 号。以下「次世代医療基盤法」という。）[4)]に基づくデータベース（認定 DB）との連結解析を可能とする制度を整備した。

具体的には、各公的 DB の根拠法の改正により、仮名化情報の利用・提供の根拠規定が整備されるとともに、利用目的の制限、適切な管理義務、厚生労働大臣による是正命令等の規律が導入されている。また、次世代医療基盤法の改正により、民間の認定事業者による連結可能な仮名加工医療情報の提供や、基盤機構を経由したデータ連携の枠組みも整備された。

さらに、個人情報保護との両立を図る観

点から、仮名化情報の利用に際しては、以下のような管理・運用が求められている。

・利用は「相当の公益性」が認められる場合に限定され、目的および内容に応じた必要性・リスクの審査が行われること

・公的 DB には、個人情報保護法[5] 上の保有主体に準じた安全管理措置および不適正利用防止措置が求められること

・データは原則としてクラウド上の情報連携基盤において解析され、データ自体の外部提供は行わないこと

・照合禁止、データ消去、安全管理措置および不正利用時の罰則等について、匿名化情報と同様の規律を適用しつつ、より厳格な管理を確保するための措置（利用目的・方法の制限等）が設けられていること

以上のように、本改正は、医療データ利活用の促進と個人情報保護の両立を図りつつ、仮名化情報を中核とした新たなデータ利用基盤の構築を志向するものであり、今後の PV 分野における RWD 活用および AI 導入の前提となる制度的基盤を形成するものと位置づけられる。

2 次世代医療基盤法

次世代医療基盤法（医療分野の研究開発に資するための匿名加工医療情報及び仮名加工医療情報に関する法律）は、健診結果や電子カルテ等の医療情報を匿名加工医療情報として加工し、医療分野の研究開発における利活用を促進することを目的として制定された法律であり、個人情報保護法の特例法として位置づけられる。

同法は令和元年 5 月に施行され、その後、令和 6 年 4 月の改正により、医療情報を仮名加工医療情報として加工・利用する仕組みが新たに導入された。これにより、匿名加工医療情報に加え、より分析可能性の高いデータの利活用が制度的に可能となった。

同法に基づく医療情報の利活用の仕組みは、概ね以下のように整理される。すなわち、国の認定を受けた認定作成事業者が、医療機関や自治体から提供を受けた医療情報について匿名加工または仮名加工を行い、企業や研究機関等の利用事業者がこれらの情報の提供を受けて研究開発等に利用するという構造である[6]。

もっとも、仮名加工医療情報については、利用主体が認定事業者に限定されるとともに、再識別の禁止、第三者提供の制限（医薬品医療機器総合機構（PMDA）への提供等の例外を除く）など、厳格な利用規律が課されている。

このような制度の下で、次世代医療基盤法に基づくデータベース（以下「次世代 DB」という。）の活用は着実に進展している。令和 7 年 7 月末時点において、収集された医療情報は約 512 万人規模に達し、医療情報取扱事業者は 158 機関にのぼる。具体的な利活用事例としては、電子カルテの非構造化データを自然言語処理により解析し、薬物治療効果の抽出や治療抵抗性の判定に関する AI モデルの構築が行われているほか、医療データと介護データ、購買データ等を統合的に解析することにより、生活習慣病の予防に資する知見の創出が試みられている。

他方で、同制度の運用に関しては、いくつかの課題も指摘されている。すなわち、医療機関からの情報提供が任意であることに伴うインセンティブ不足、オプトアウト手続に係る医療現場の負担、認定作成事業者と

医療機関との個別契約に依存した非効率性、オプトアウト通知前に死亡した患者の情報が利活用できない点、ゲノム情報の取扱い制約、さらに仮名加工医療情報の利用に係る認定手続の負担の大きさ等が挙げられる。

以上のように、次世代医療基盤法は、医療データの利活用を制度的に推進する重要な枠組みを提供する一方で、その運用においてはなお改善の余地を残している。特に、データ利活用の促進と個人情報保護との均衡、ならびに制度の実効性確保という観点は、今後の制度設計における重要な論点となる。

3 個人情報保護法のいわゆる「3 年ごとの見直し」（同意規制の在り方）

個人情報保護法については、いわゆる「3年ごとの見直し」に基づき、同意規制の在り方を含む制度見直しが進められている。本見直しは、令和 2 年改正法附則第 10 条の規定[7)] を踏まえ、個人情報保護委員会において令和 5 年 11 月より検討が開始されたものである。

また、政府全体の政策動向として、「規制改革実施計画」（令和 7 年 6 月 13 日閣議決定）においても、医療等データの包括的かつ横断的な利活用法制の整備の一環として、本人同意規制の在り方およびこれに対応するガバナンスの在り方について検討を行い、結論を得次第、速やかに法案提出を行う方針が示されている[8)]。

同計画では、特に以下の観点が検討課題として示されている。すなわち、統計作成等のように特定個人との対応関係が排除された分析結果の取得・利用を目的とする場合の同意の在り方、公衆衛生の向上等のための取扱いにおける同意取得困難性要件の在り方、ならびに病院等による学術研究目的での個人情報の取扱いに関する規律の整理である。

こうした検討を踏まえ、令和 8 年 1 月 9 日には「個人情報保護法 いわゆる 3 年ごとの見直しの制度改正方針」が公表された。本改正方針は、「適正なデータ利活用の推進」「リスクに応じた規律」「不適正利用の防止」「規律遵守の実効性確保」等を柱として構成されている。

このうち、医療等データの利活用と特に関係する「適正なデータ利活用の推進」に関しては、本人の権利利益への影響の程度に応じて本人関与の在り方を再整理することにより、個人の信頼を確保しつつデータ利活用を促進するという方向性が示されている。

具体的には、統計情報等の作成にのみ利用されることが担保されている場合には、個人データの第三者提供や公開されている要配慮個人情報の取得について、本人同意を不要とすることが検討されている。この「統計情報等の作成」には、統計的処理として位置づけられる AI 開発等も含まれると整理されている。もっとも、このような取扱いは、個人の権利利益を害するおそれが小さいものとして個人情報保護委員会規則により限定されることが想定されている。

さらに、同意規制の見直しに関連して、取得の状況からみて本人の意思に反しないと認められる場合には同意を不要とする取扱い、公衆衛生の向上等を目的とする場合における同意取得困難性要件の緩和、ならびに学術研究例外の対象に医療機関等を明示的に含めることなどが検討されている。

以上のように、個人情報保護法の見直し

は、従来の同意中心の規律から、リスクおよび利用目的に応じた柔軟な規律への転換を志向するものであり、医療データの利活用、とりわけ PV 分野における RWD および AI 活用の制度的基盤に重要な影響を及ぼすものと位置づけられる。

第 2 章 EHDS 等の国内外の動向

前章では、日本における医療 DX および医療データ利活用の制度的枠組みを整理した。本章では、これを相対化する視座として、欧州を中心とした国際的動向、とりわけ European Health Data Space（EHDS）に焦点を当てる[9]。EHDS は、医療データの一次利用および二次利用を統合的に制度設計する試みであり、データアクセスの仕組み、公益概念、同意・オプトアウトの位置づけ、さらにはガバナンス機構の設計において、体系的かつ包括的な特徴を有する。

以下では、その調査報告書に基づき、EHDS における医療データ二次利用の制度構造を中心に整理し、日本の制度との比較可能性を検討するための基礎的視座を提示する。すなわち、本章は、日本の制度を単に紹介する前章に対し、制度設計の選択肢を比較可能な形で再配置することを目的とする。

第 2 章第 1 節 EHDS に基づく健康データの二次利用の概要

前章第 1 節で言及した「デジタル社会の実現に向けた重点計画」において、医療等データの利活用の仕組みを構築する上で参照すべきものとされている EHDS 規則（以下「EHDS」という。）について、本節では、医療データの二次利用の観点からその制度的枠組みを概観する。

EHDS の主要な目的は、GDPR に整合的な形で、①医療の文脈における個人の電子健康データへのアクセスおよび管理を容易にすること、ならびに②電子健康データの利用を通じて、研究、イノベーション、政策立案等の社会的利益をより効果的に実現することにある（EHDS 前文 1)。とりわけ後者の観点から、EHDS は健康データの二次利用を制度的に位置づけ、その促進を図る枠組みを構築している（EHDS 第 53 条)。

この枠組みにおいて特徴的なのは、一定の条件の下で、データ保有者に対して電子健康データの共有を義務付ける点にある。すなわち、データ利用者（個人または組織）は、第 IV 章に定める要件を満たす場合、医療・介護分野の事業体や研究機関等のデータ保有者に対し、データ要請を通じてデータアクセスを請求することができる。他方で、当該データの審査、準備および提供に要する費用については、データ利用者に負担が課され得る（EHDS 第 62 条)。

対象となるデータは、臨床ケアや研究を通じて収集された電子健康記録に加え、社会経済的・環境的・行動データ、医療関連行政データ、遺伝子情報等を含む広範なものである（EHDS 第 51 条)。これらのデータは、健康データアクセス機関（Health Data Access Bodies, HDAB）を介して提供され、科学研究、アルゴリズムの訓練、個別化医療等の二次利用目的に供される（EHDS 第 53 条(1)、第 55 条)。

また、EHDS におけるデータ二次利用は、原則として匿名化されたデータセットに基づいて行われる[10]。これにより、プライバ

シー保護とデータ利活用の両立が制度的に図られている。

このようなデータ利用のプロセスは、概ね以下の段階から構成される。まず、データ利用者は公的メタデータカタログを通じて利用可能なデータを探索する。次に、HDABが利用目的および申請内容を審査し、許可された場合にはデータ保有者に対してデータ提供が要請される。その後、データは利用目的に応じた形式およびプライバシー保護措置を施した上で準備され、利用者はリモート環境を通じて解析を行う。データ自体は外部に提供されず、利用者は解析結果のみを取得する仕組みとなっている。最後に、利用者は研究成果等を HDAB に報告することが求められる。

以上のように、EHDS は、データアクセス権の制度化、データ提供義務の導入、およびアクセス手続の標準化を通じて、医療データの二次利用を体系的に設計する枠組みである。この点において、同意を基軸とする従来の枠組みとは異なる制度的特徴を有しており、日本の制度との比較において重要な参照点を提供する。

第 2 章第 2 節 EHDS 下の医療データ二次利用に関する論点と示唆

2025 年 6 月に「Frontiers in Digital Health」誌に掲載された論文 “Secondary use under the European Health Data Space: setting the scene and towards a research agenda on privacy-enhancing technologies”[11]は、EHDS に基づく健康データの二次利用に関して、懸念事項およびそれに対する解決策を、プライバシー強化技術（PETs）の観点から体系的に整理したものである。

同論文は、EHDS に関与する医療分野の専門家 16 名への半構造化インタビューに基づき、制度運用において顕在化し得る課題を抽出するとともに、それらに対応するガバナンスおよび技術的アプローチを提示している。本節では、そのうち本報告書の後続の議論と関連性の高い論点を整理し、日本における制度検討への示唆を導出する。

まず、懸念事項として提示される主要な論点の一つは、「公益と商業的利益の関係」である。すなわち、健康データが公共的利益のためではなく、特定の商業主体に偏って利用されることへの懸念である。この点については、データの経済的価値が社会に還元されない可能性、医療機関や企業によるデータの収益化、さらには保険会社等による不適切利用のリスクが指摘されている。また、データアクセスに必要な資源や専門性の差異により、大企業が優位に立ち、小規模主体が排除される構造的不均衡も問題とされている。

第二に、「同意と管理」に関する論点として、現行のオプトアウト制度の粗さが指摘される。すなわち、データ利用目的ごとの選択が困難であるため、患者が包括的に利用を拒否せざるを得ない状況が生じ得る点である。加えて、データ利用に関する透明性の不足は、制度への信頼低下を招き、結果として大規模なオプトアウトの発生につながる可能性がある。また、インフォームド・コンセントの取得に関しても、その複雑性および医療現場の負担が課題として指摘されている。

これらの懸念に対し、同論文は、主としてガバナンスおよび政策に関する解決策を提

示している。まず、データガバナンスの観点からは、責任主体およびオーナーシップの明確化とともに、「公益」の概念を具体的に定義する必要性が指摘される。また、データを可能な限り提供元に保持させることにより、管理責任の所在を明確化する方策も提案されている。

なお、同論文の Appendix には、プライバシー強化技術の具体的な適用を示すユースケースが提示されている。同論文の Appendix 3 において提示されるユースケース（特に Case E 等）は、プライバシー強化技術の適用およびデータアクセスの具体的運用形態を示すものであり、本報告書で整理した判断枠組みと整合的な構造を有している。これらの事例は、制度設計上の論点を実務的文脈において具体化するものとして参考となる[12)]。

さらに、制度運用の観点からは、標準化された手続および定期的なコンプライアンス監査の導入が重要であるとされる。これにより、制度の透明性および説明責任を担保することが可能となる。また、市民参画および意識向上の重要性も強調されており、データ主体に対する継続的な情報提供とフィードバックを通じて、制度への信頼を構築する必要があるとされている。

加えて、同意およびオプトアウトの仕組みについては、情報提供の階層化や、利用目的に応じた柔軟な選択を可能とする仕組み（オプトインとオプトアウトの組合せ）の導入が提案されている。さらに、これらの意思表示を一元的に管理する中央的な仕組みを設けることにより、利用者の負担軽減と透明性向上を図ることが可能であるとされる。

以上の整理を踏まえると、EHDS に関する議論は、日本における医療データ利活用の制度検討に対して複数の示唆を与える。すなわち、公益概念の明確化、データアクセスの公平性確保、同意に依存しないガバナンスの構築、ならびに透明性と信頼を基盤とした制度設計の必要性である。

他方で、商業的利用に対する倫理的統制やデータアクセス格差への対応、細分化された同意管理の仕組み等については、日本の現行制度において必ずしも十分に明示されていない論点である。これらの点を含めて検討することにより、医療データ二次利用に関する制度設計を一層深化させることが可能となる。

以上のように、EHDS は、医療データの二次利用を前提とした制度設計を体系的に構築している点に特徴があり、その構造は、日本における制度設計を検討する上で重要な参照枠を提供するものである。特に、データアクセス機関を中核とする許可モデル、リモートアクセスを前提としたデータ利用形態、および公益性を基軸とした利用目的の整理は、後続章における PV 分野および AI 導入の議論においても基礎的前提として位置づけられる。

上記の検討から明らかなように、EHDS における医療データ二次利用の制度設計は、単にデータアクセスの仕組みを整備するものにとどまらず、公益概念の定義、データ利用主体間の関係性の再編、ならびに同意に依拠しないガバナンスの構築といった、制度の基底に関わる問題を包含している。

これらの論点は、前章において整理した日本の制度枠組みと対比することで、医療データ利活用における制度設計の選択肢を

相対化する視座を提供するものである。特に、データの二次利用を前提とした制度構造、リスクに応じた規律の在り方、ならびに透明性と信頼の確保をめぐる議論は、日本における制度的検討においても中核的な課題として位置づけられる。

こうした制度的前提の変容は、医薬品安全性監視（PV）分野において顕著に現れる。すなわち、RWD の利活用および AI の導入は、従来の人間中心の判断構造を前提とした業務プロセスに対し、データ駆動型の意思決定やアルゴリズムによる分析を組み込むことにより、その構造自体の再編を促すものである。

したがって、次章では、これまでに整理した制度的枠組みおよび国際的動向を踏まえ、PV 分野における RWD 活用の実態とその構造を明らかにするとともに、AI 導入がもたらす構造的変化について検討を行う。これにより、制度・データ・技術が交差する領域における課題を、具体的かつ統合的に把握することを目的とする。

第 II 部 PV 分野における RWD 利活用の構造

第 3 章 PV 分野における RWD 利活用の現状

前章まで整理した制度環境および国際的動向を踏まえ、本章では PV 分野におけるリアルワールドデータ（RWD）の利活用状況を整理する。

近年、医薬品医療機器法の改正や医療情報データベースの整備により、RWD は市販後安全対策において重要な役割を担うようになっている。他方で、その利活用は多様なデータ基盤、制度的制約、責任構造のもとで成立しており、単純な技術導入としては捉えられない複雑な構造を有している。

以下では、専門家による調査報告書に基づき、PV 分野における RWD 活用の制度の位置づけ、データ基盤および具体的ユースケースを中心に、その構造を整理する。

第 3 章第 1 節 PV 分野における RWD の利活用の現状

1 2025 年医薬品医療機器等法改正

2025 年 5 月、医薬品医療機器等法の改正法[13]が公布され、リアル・ワールド・データ（RWD）[14]の薬事申請および安全対策への利活用が制度上明確化された。

2025 年 1 月に公表された「薬機法等制度改正に関するとりまとめ」（厚生科学審議会医薬品医療機器制度部会）によれば、RWD の安全対策への利活用は、「医薬品等の品質確保及び安全対策の強化」に向けた施策の一つとして位置付けられている。同とりまとめでは、RWD の活用により、より長期間にわたる調査の実施や、当該製品の使用患者と非使用患者との比較研究等が可能となり、有用であると指摘されている。

これを踏まえ、RWD のみに基づく再審査または使用成績評価の申請が可能であることを明確化するため、当該申請時の添付資料に関する規定が見直された。

もっとも、RWD を用いた承認申請や再審査申請自体は従来から一定程度行われてきたものである。以下では、PV 分野における RWD の具体的な活用事例について概説する。

2 医療情報データベース（MID-NET、JADER、NDB）

MID-NET は、医療機関及び製薬企業からの副作用報告の限界を補完し、薬剤疫学的手法に基づく医薬品安全対策を推進することを目的として構築された医療情報データベースであり、全国 9 拠点 31 の協力医療機関が保有する電子カルテ（オーダリング情報、検査結果等を含む）、レセプト及び DPC データを統合的に利用可能とするものである。PMDA が安全対策業務の一環として管理・運営している。

MID-NET は、830 万人超（2024 年 12 月時点）のデータを解析可能な大規模データベースであり、主な特徴として以下が挙げられる。

・電子カルテ、レセプト、DPC データを統合しているため、患者背景や臨床検査値の変動など、多面的な情報把握が可能である。
・データは定期的に更新されるため、準リアルタイムでの利活用が可能である。
・データの信頼性は、医療機関の原データとの照合や抽出過程の検証により担保されている。
・大学病院を中心とした協力医療機関により、急性期医療に関するデータの把握が可能である。

JADER（Japanese Adverse Drug Event Report database）は、2004 年以降に医療機関や製薬企業等から報告された国内の副作用疑い症例を PMDA がデータベース化し公開しているものである。症例は重篤例に限定され、症例情報、医薬品情報、副作用情報及び原疾患情報の 4 テーブルから構成される。主として安全性シグナルの検出に利用されるが、自発報告データであることに由来する過少報告、分母情報の欠如、報告バイアス等の限界が指摘されている。

また、レセプト情報・特定健診等情報データベース（NDB）を用いた薬剤疫学研究に基づく安全性評価も実施されている。NDB は匿名化レセプト情報及び特定健診データから構成され、悉皆性及び症例数の点で MID-NET に優れる一方、臨床検査値等の詳細情報を含まないという制約がある。

3 RWD を用いた市販後安全対策のユースケース

RWD を用いた市販後安全対策の主なユースケースとして、以下が挙げられる [15]。

① 新たな注意喚起
ペグフィルグラスチムによる血小板減少の事例では、G-CSF 製剤 [16]投与に関する副作用報告の集積を契機として、MID-NET を用いたネステッドケースコントロール研究が実施された。その結果、投与前 2〜7 日の期間に当該薬剤の処方を受けた患者において、非処方患者と比較して血小板減少リスクの有意な増加が認められ、添付文書改訂による注意喚起につながった [17]。
② 現在の安全対策の適切性確認
C 型肝炎治療薬（DAA）に関する腎機能障害リスクについて、添付文書上の記載に差異が認められていたところ、MID-NET を用いた解析により製剤間のリスク比較が行われた。その結果、リスク上昇が認められた製剤については既に適切な注意喚起がなされており、安全対策措置が妥当であることが確認された [18]。
③ 安全対策措置の効果評価
メトホルミン製剤については、2019 年 6 月の注意事項改訂により中等度腎機能障害患

者への投与が可能となったことを受け、MID-NET を用いて改訂前後の処方実態及び乳酸アシドーシス発現状況が評価された。その結果、新たな安全性上の懸念は認められず、追加的リスク最小化活動は不要と判断された事例が報告されている[19]。

④ 新たな安全性シグナルの検出・強化

曝露医薬品と対照医薬品における臨床検査値異常（肝機能、腎機能、血球等）の発現率を比較する「早期安全性シグナルモニタリング」が実施されている。この取組は、条件付き承認制度、緊急承認制度及び特例承認制度の対象医薬品等におけるシグナル検出、並びに既存シグナルの検証・強化を目的とするものである[20]。

4 MID-NET の利活用に関するガイドライン（以下「MID-NET ガイドライン」という。[21]）

（1）利活用目的の範囲

MID-NET ガイドラインは、利活用の主目的を「医薬品等の市販後安全監視及びリスク・ベネフィット評価を含む安全対策」としつつ、一定の公益性を有する調査・研究についても利用を認めている。

（2）利活用可能な電子診療情報の特性

利活用の対象となるデータは、協力医療機関の統合データソース及び国立病院機構診療情報集積基盤（NCDA）から抽出・加工された分析用データセットに限られる。これらのデータは元データとの対応表を持たない形で構成され、個票単位での再識別が困難な構造となっている。また、分析用データには年齢及び性別等は含まれるが、氏名、住所、患者番号等の直接識別子は含まれず、生年月日は年月単位に変換される等の措置が講じられている[22]。

（3）個人情報保護に関する考え方

利活用に供されるデータには識別性を低減する処理が施されており、原則として個人情報には該当しないと整理されている。仮に個人情報に該当する場合であっても、MID-NET は独立行政法人医薬品医療機器総合機構法に基づく事業として運営されているため、個人情報保護法上、本人同意の取得は必須とはされていない。

もっとも、協力医療機関による利用目的の公表や、PMDA による情報公開を通じて、本人に対する周知およびオプトアウトの機会が確保されている。

第 3 章第 2 節 医療等データの利活用において検討すべき論点―個人情報保護の観点から― [23]

1 医療等情報の利活用の推進に関する検討会の論点整理

本報告書第 1 章で言及した「デジタル社会の実現に向けた重点計画」及び「規制改革実施計画」を踏まえ、医療等情報の利活用に関する基本理念及び制度枠組みを含む全体像（いわゆるグランドデザイン）を検討するため、令和 7 年 9 月より「医療等情報の利活用の推進に関する検討会」（以下「検討会」という。）が開催された（令和 7 年 9 月 3 日内閣府特命担当大臣決定）。

検討会では、第 1 回会合において内閣府健康・医療戦略推進事務局から提示された以下の論点を基礎として、有識者ヒアリング及び意見交換が行われた。

論点(1) 対象となる医療等情報の範囲及び優先順位（例：公的データベース、次世代医療基盤法に基づくデータベース、電子カルテ情報、画像情報、疾患レジストリ、バイオバンク、PHR 等)。また、どの主体（行政、医療機関、学会、企業等）からどのような情報提供を求めるかも含まれる。

論点(2) 医療等情報の収集方法等

① 医療等情報の収集方法

利活用ニーズ、費用、医療現場の負担、知的財産権保護等を踏まえつつ、データ提供に関する一定の強制力又はインセンティブ付与の必要性及び内容を検討する。

② 患者識別子

データ連結を可能とする識別子（例：被保険者番号、マイナンバー等）の在り方。

③ 医療等情報の標準化

非構造データ（テキスト、画像等）についても、AI 等の活用により構造化し得る点を踏まえる必要がある。

論点(3) 患者の権利利益及び情報の保護

① 本人関与の在り方（同意の要否、同意に依拠しない枠組みを含む）

② 不適切利用の防止及び情報セキュリティ

③ 国民・患者の理解の確保

論点(4) 情報連携基盤及びガバナンス

① 情報連携基盤の在り方

② 審査・監督・ガバナンス体制の確保

論点(5) 費用負担

2 中間とりまとめ（案）に示された論点と主な意見

令和 7 年 12 月、検討会の議論状況を整理するため、中間とりまとめ（案）が作成された。同案は本書作成時点ではドラフト段階にあり、各論点に対する最終的な方向性は示されていないものの、有識者の主要な意見が整理されており、今後の制度設計に対して一定の示唆を与えるものと評価できる。

検討会では、令和 8 年度夏を目途に最終的な議論の整理が行われる予定である。以下では、個人情報保護との関係が特に深い「5. 患者の権利利益及び情報の保護等」に関する論点について整理する。

(1) 患者本人の適切な関与の在り方

医療情報の二次利用については、その高度な専門性ゆえに、本人が内容を十分理解した上で同意することは実務上困難であるとの指摘がある。また、オプトアウト対応が医療現場の負担となっているとの問題も指摘されている。

これを踏まえ、従来の、同意を中心とした「入口規制」から、利用段階での審査・監督を重視する「出口規制」への転換を提案する意見が示された。これに対し、本人関与の水準を緩和すべきではなく、少なくとも拒否権の保障及び通知の仕組みは維持すべきであるとする意見もある。

また、同意に代え得る要件として、以下のような要素を組み合わせるべきとする見解が示された。

・相応の非識別化（コード化等）
・法令又は制度に基づく承認
　（例：薬機法、GCP）
・第三者による審査（例：IRB）
・情報公開等による社会的承認
・オプトアウト機会及び利用状況の可視化

さらに、利用停止については、本人が一元

的に申請できる仕組みの必要性が指摘されている。

加えて、医療機関ごとの対応負担を軽減する観点から、マイナポータル等を活用したデジタルオプトアウトや、政府による一元管理の導入を求める意見も示された。

(2) 不適切利用防止及び情報セキュリティ

二次利用における事故が一次利用や他の利用に波及しないよう、影響を限定する仕組みの必要性が指摘されている。また、国家安全保障の観点から、医療情報の国内管理の重要性も論じられている。さらに、利用目的及び禁止事項の明確化に関し、EU の欧州保健データスペース（EHDS）における規律（第 53 条及び第 54 条）[24]に類似した制度設計が参考になるとの意見がある。

加えて、

・不適切な利用事例の明確化

・差別的取扱いの禁止（法令による補完）

といった点の必要性も指摘されている。

(3) 国民・患者の理解と信頼

医療等情報の利活用の推進には、国民・患者の理解と信頼（コンセンサス及びトラスト）の確保が不可欠であるとの認識は共有されている。

制度説明に加え、ユースケースや研究成果を含めた分かりやすい情報提供の重要性が指摘されている。

また、個人情報保護法改正の方向性として示されている「統計利用等に限定される場合の同意不要」という考え方については、支持する意見がある一方で、実務との乖離を指摘する意見もみられた。

以上から、PV 分野における RWD の利活用は、単一のデータ基盤に依拠するものではなく、MID-NET、JADER、NDB 等の複数のデータベースの特性を踏まえた多層的構造の下で展開されていることが確認できる。

また、制度整備は進展しつつあるものの、データの性質、利用主体、責任分配の在り方についてはなお整理途上にある。とりわけ、

・公益性と個人情報保護の調整

・患者関与の在り方

・データ利活用におけるガバナンス確保

は、今後の制度設計における中核的論点である。

本章で整理した枠組みは、次章以降において検討する AI 導入による構造的変化を理解する前提となる。

さらに、以上の論点は、単なる医療データの利活用や個人情報保護の問題にとどまらず、AI の社会実装を前提としたデータガバナンスの在り方そのものに関わる問題として位置づける必要がある。

すなわち、医療等情報の利活用に関する議論において提示された「入口規制から出口規制への転換」、「本人同意に依拠しない利用の正当化」、「第三者による審査・監督」、「データの非識別化及び標準化」、「情報連携基盤の整備」といった諸要素は、いずれも AI の学習・推論に不可欠なデータ利用を前提とした統治枠組みの構成要素にほかならない。

とりわけ、AI の高度化に伴い、データ利用の目的は事前に限定し難たくなり、また、個別具体的な同意に基づく管理には制度的限界が生じる。このため、従来の個人情報保護法制における「同意中心モデル」から、「適

正利用を事後的に統制するモデル」への移行が不可避となりつつある。

このような変化は、単に法技術的な問題ではなく、

・誰がデータ利用の正当性を判断するのか

・どのような手続によって社会的信頼を確保するのか

・アルゴリズムによる意思決定の透明性・説明可能性をいかに担保するのか

といった、より広範な AI ガバナンスの問題へと繋がる。

したがって、PV 分野における RWD の利活用に関する制度設計は、AI 時代におけるデータ統治の先行事例として位置づけることができる。すなわち、本節で整理した「患者関与」「出口規制」「第三者審査」「情報連携基盤」といった論点は、今後の AI ガバナンスの基本構造を先取りするものと評価できる。

この点を踏まえれば、次章において検討する AI 導入は、単なる技術導入ではなく、既存の法制度・倫理・社会的合意の枠組みを再編成する契機として理解されるべきである。

第Ⅲ部 PV 領域への AI 導入における構造転換

第 4 章 AI 導入による構造的課題

前章までに整理した制度及び実務構造は、人間による判断を前提として成立している。本章では、AI の導入がもたらす構造的変化を明らかにすることで、従来の構造との連続性および断絶の双方を位置づける。

前章でみたとおり、PV 分野における RWD の利活用は、制度的・実務的基盤の整備の下で段階的に進展してきた。これに対し、AI 技術の導入は、既存のデータ利活用構造に対して、より根源的な変化をもたらす可能性を有する。

とりわけ重要なのは、AI の導入が単なる業務効率化にとどまらず、「判断主体」「責任構造」「データ利用の時間軸」といった前提そのものを変容させる点にある。すなわち、AI の導入は、PV 業務を支える認識論的及び制度的基盤に対して再編を迫るものである。

本章では、こうした構造変化を、AI 関連ガイドライン及び規制動向の整理を踏まえつつ、「学習段階と推論段階の区別」「モデルの残存性」「ブラックボックス性」「責任の所在」といった観点から概念的に整理する。

第 4 章第 1 節 人間判断構造との対比

AI 導入に伴う構造変化を理解するためには、従来の PV 業務が前提としてきた「人による判断構造」との対比が不可欠である。

従来の PV 業務においては、データ収集、医学的評価、因果関係判断といった各プロセスは、いずれも人間の専門的判断を中核として構成されてきた。この構造において、判断は個別事例ごとに完結し、その都度、判断主体と責任主体が一致する点に特徴がある。

また、判断の根拠は医学的知見や臨床経験に基づき言語化可能であり、事後的な検証および説明も一定程度可能であった。ここでは、判断は「理由付け可能な行為」として制度的に位置づけられている。

これに対し、AI の導入は、「都度判断」「主

体の一致」「理由付け可能性」といった従来構造の前提を動揺させる。すなわち、判断は個別事例に閉じた行為ではなくなり、学習段階と推論段階に分離されたプロセスとして再構成される。

その結果、判断は時間的に分散し、主体の所在も一義的に定まらなくなる。したがって、AI の導入は単なる業務効率化にとどまらず、「判断とは何か」という制度的・概念的枠組みそのものの再定義を要請するものである。

第 4 章第 2 節 AI に固有の構造特性

前節で示した人間判断構造との対比を踏まえ、AI の導入がもたらす構造的特性を整理する。以下に示す各要素は相互に独立するものではなく、時間構造、認識構造及び責任構造の再編として相互に連関している点に留意する必要がある。

1 学習段階と推論段階の分離

AI は、学習（training）と推論（inference）という、２つの異なるフェーズから構成される。この構造は、従来の「都度判断」とは異なり、過去のデータに基づいて構築されたモデルが将来の判断に継続的に影響を及ぼすという時間的非対称性をもたらす。

この時間的非対称性の下では、個々の判断は単一の時点に帰属するものではなく、学習過程におけるデータ選択、前処理、モデル設計等の複数の要素に依存する。その結果、特定の判断結果について、どの要因がどの程度寄与したかを遡及的に特定することは困難となる。

したがって、判断責任を特定の時点や主体に一元的に帰属させる従来の枠組みは、そのままでは適用し難くなる。

2 モデルの残存性

AI モデルは、一度構築されると、その内部構造が継続的に利用される。この「残存性」は、判断が一回限りの行為として完結するのではなく、過去のデータ処理の結果が将来の判断に持続的に影響を与え続けることを意味する。

この点において、判断の履歴は「人間の記憶」として可変的に保持されるのではなく、「モデル構造」として半固定的に保持される。その結果、判断の再現性が高まる一方で、過去のバイアスや誤りが構造的に温存され、継続的に影響を及ぼす可能性が生じる。

3 ブラックボックス性

AI モデルの内部処理は必ずしも可視化されず、判断過程の完全な説明可能性は制約される。この点は、従来の医学的判断において前提とされてきた「理由付け可能性」とは質的に異なる。

ここで問題となるのは、単に説明が困難であるという点にとどまらない。すなわち、説明の対象及び水準そのものが変容する点に本質がある。完全な内部説明が困難である場合には、外部的な証跡、結果の一貫性、統計的妥当性等を基礎として、説明責任を代替的に構成する必要が生じる。

4 責任所在の分散

AI の利用においては、開発者、提供者、利用者等の複数の主体が関与するため、責任の所在は単一主体に帰属せず、構造的に分散する。この分散は責任の空白を意味す

るものではなく、むしろ責任の再配分を要請するものである。すなわち、

・モデル設計に関する設計責任
・学習データに関するデータ管理責任
・運用に関する運用責任
・最終的な意思決定に関する判断責任

複数の責任層を区別し、それぞれを制度的に位置づける必要がある。

第 4 章第 3 節 出口規制モデルとしての AI ガバナンス

前節までにみたとおり、AI の導入は、判断の生成過程を学習段階と推論段階に分離し、判断の時間的・構造的分散をもたらす。このような構造の下では、従来のように個別の判断行為に着目し、その適法性や妥当性を評価する枠組みには限界が生じる。

従来の個人情報保護法制及び医療データ利活用の枠組みは、主として「入口規制」を中心として構成されてきた。すなわち、データ取得時点における本人同意や利用目的の特定を通じて、データ利用の適法性を事前に担保する構造である。しかしながら、AI においては、データの利用目的が学習過程において動的に変容し得ること、また、将来の利用形態を完全に予見することが困難であることから、このような入口規制モデルのみでは十分な統制を確保することが難しい。

この点に鑑みると、AI 時代のデータ利活用においては、利用の適法性を事前に固定するのではなく、利用過程及び利用結果に対する統制を重視する「出口規制モデル」への転換が要請される。すなわち、データの取得・入力段階における同意や形式的要件に過度に依拠するのではなく、実際の利用行為及びその帰結に着目し、その適正性を継続的に監視・評価する枠組みが必要となる。

この出口規制モデルは、以下のような要素から構成される。

第一に、第三者による審査・監督の制度化である。AI の利用においては、個々の判断の妥当性を事前に担保することが困難であるため、独立した主体による継続的な評価及び監査が不可欠となる。これは、従来の IRB 審査や倫理審査の枠組みを拡張し、アルゴリズム及びデータ利用全体に対するガバナンスとして再構成することを意味する。

第二に、説明責任の再構成である。前節でみたとおり、AI においては完全な内部説明が困難である場合が多い。このため、説明責任は、個別の判断過程の完全な可視化ではなく、結果の一貫性、統計的妥当性、外部監査可能性といった要素を基礎として構成される必要がある。

第三に、責任構造の多層化への対応である。AI の利用に伴い、責任は設計、データ、運用、意思決定といった複数の層に分散する。このため、各層に応じた責任の所在を明確化し、それぞれに適合的な規律を設計することが求められる。

第四に、継続的なモニタリング及びフィードバックの仕組みである。AI モデルは運用後も環境やデータの変化に応じて性能が変動し得るため、導入後の継続的な監視と改善が不可欠となる。これは、従来の一回的な審査・承認とは異なり、動的なガバナンスの必要性を示すものである。

以上のように、出口規制モデルとしての AI ガバナンスは、「事前の同意による統制」から「事後的・継続的な統制」への重心移動を特徴とする。この転換は、単なる規制手法の変更にとどまらず、データ利用の正当性

を支える原理そのものの再編を意味する。

すなわち、従来は本人同意が正当化の中心に位置付けられていたのに対し、AI 時代においては、適正な利用プロセス、透明性の確保、監査可能性、社会的受容といった複合的要素によって正当性が構成されることになる。

このような観点からすれば、PV 分野における RWD 利活用に関する制度的検討は、AI ガバナンスの先行的実装と位置づけることができる。すなわち、医療分野において蓄積されつつある出口規制的要素（第三者審査、オプトアウト、継続的監視等）は、AI 時代の一般的なデータガバナンスのモデルを先取りするものと評価できる。

したがって、今後の制度設計においては、個人情報保護法制、医薬品規制、AI 規制といった分野横断的な視点から、出口規制モデルを基軸とした統合的ガバナンスの構築が求められる。

第 4 章第 4 節 AI 時代における主体・責任・関係性の再構成

前節までにおいて、AI の導入が判断構造及びガバナンス構造に対してもたらす変容を整理した。これらの変化は、単に制度設計や運用の問題にとどまらず、「主体」「責任」「関係性」といった法制度の基底概念そのものの再構成を要請するものである。

1 主体の再構成

従来の法制度においては、「主体」とは意思能力を有し、自律的に判断し、その結果に責任を負う存在として想定されてきた。この前提の下では、判断主体と責任主体は基本的に一致し、主体は意思決定の中心に位置づけられている。

しかしながら、AI の導入により、判断の生成過程は人間の内部から外部のシステムへと部分的に移行する。すなわち、判断は人間単独の行為として完結するのではなく、データ、アルゴリズム、モデルといった非人格的要素との相互作用の中で生成されるものとなる。

この結果、主体はもはや単一の意思決定者としてではなく、複数の要素が関与する「分散的構成体」として捉えられる必要がある。ここにおいて、主体とは固定的な存在ではなく、関係の中で生成される機能的概念へと転換する。

2 責任の再構成

主体の分散化に伴い、責任の在り方も再構成を迫られる。従来は、特定の主体に対して結果責任又は過失責任を帰属させることにより、法的評価が行われてきた。

しかし、AI の関与する判断においては、結果が複数の要因（データ、モデル設計、運用環境等）の複合的作用として生じるため、責任を単一主体に帰属させることは困難となる。

このため、責任は単一の帰属対象ではなく、

・設計段階における設計責任
・データに関する管理責任
・運用段階における監督責任
・最終判断における意思決定責任

といった形で、多層的に配分する必要がある。

ここにおいて重要なのは、責任の所在を曖昧にすることではなく、むしろ責任を可視化し、適切に分節化することである。すな

わち、責任の再構成とは、責任の希薄化ではなく、責任構造の再設計を意味する。

3 関係性の再構成

主体及び責任の再編は、同時に関係性の再構成を伴う。従来の法制度は、主体間の関係を契約や権利義務関係として明確に定式化することを前提としてきた。

これに対し、AI を介在させたデータ利用の構造においては、関係は固定的なものではなく、動的かつ多層的に形成される。すなわち、データ提供者、医療機関、開発者、規制当局、患者等が相互に関係しながら、判断及び価値が生成される構造となる。

このような関係性においては、個別の同意や契約のみならず、透明性、説明可能性、監査可能性といった制度的装置を通じて、関係全体の信頼性を確保する必要がある。

ここで重要となるのは、関係性の基盤としての「信頼（トラスト）」である。AI 時代のガバナンスにおいては、個別の主体の意思に依拠するのではなく、制度及びプロセスを通じて信頼を構築することが求められる。

以上の検討から明らかなとおり、AI の導入は、①主体を固定的存在から関係的存在へと変容させ、②責任を単一帰属から多層配分へと再編し、③関係性を静的構造から動的ネットワークへと転換させるものである。

この変化は、従来の「主体中心モデル」に基づく法制度から、「関係性中心モデル」への移行を示唆する。すなわち、法的正当性は個別主体の同意や意思にのみ基礎づけられるのではなく、制度的手続、透明性、監査及び社会的受容といった複合的要素によって支えられることとなる。

このような観点からすれば、PV 分野における AI 導入は、単なる技術革新ではなく、人間・技術・制度の関係を再編成する契機として位置づけられるべきである。

第 4 章第 5 節 PV における AI 利用に関連する内外のガイドライン等

1 国内のガイドライン

（1）人工知能関連技術の研究開発及び活用の適正性確保に関する指針 [25)]

本指針は、PV 分野に特化したものではないが、AI 法第 13 条を根拠として策定され、2025 年 12 月 19 日に内閣府より公表されたものである。本指針は、人間中心（人間尊重、法令遵守、多様性・包摂性、人間による最終判断）、公平性、安全性、透明性といった基本原則に基づき、AI の研究開発及び活用における適正性の確保を求めるものである。

PV 分野における AI 利用においても、これらの原則は、判断の最終責任の所在や説明責任の在り方を検討する上で重要な指針となる。

（2）人を対象とする生命科学・医学系研究に関する倫理指針及び同ガイダンス [26)]

本指針は、厚生労働省、文部科学省及び経済産業省の 3 省により策定された統一的ガイドラインであり、AI 研究に特化したものではないものの、臨床データを用いた研究全般に適用される。特に、研究参加者からの同意取得に関する規律については、個人情報保護法における学術研究例外を補完する

機能を有している。他方で、同法の学術例外が主として学術研究機関を対象としているのに対し、本指針は非学術機関を含む広範な研究主体を対象としているため、両者の適用関係には留意が必要である。

なお、2025 年 12 月 24 日には、厚生科学審議会の合同会議により、個人情報の取扱い等に関する見直しの方向性が取りまとめられており[27]、今後、個人情報保護法の見直し動向を踏まえた改訂が予定されている。

（3）AI 事業者ガイドライン（Ver.1.1 及び 1.2）[28]

本ガイドラインは、総務省及び経済産業省により策定されたものであり、AI の開発、提供及び利用に関わる事業者に対して横断的に適用される包括的指針である。

PV 分野に特化したものではないが、AI の利用主体全般を対象とするため、PV 目的での AI 活用においても直接的な影響を有する。

近時の改訂（2025 年 3 月 28 日 Ver.1.1、2026 年 3 月 31 日 Ver.1.2）では、生成 AI に特有のリスク（誤情報、バイアス等）への対応が強化されるとともに、高度 AI に関する追加的要請として、レッドチーミング、文書化、透明性の確保、人間による最終判断の確保等が明示された。

これらの要請は、PV 業務における症例要約や文献スクリーニング等への AI 活用において、監査体制及びガバナンス要件の強化をもたらすものと考えられる。

（4）医療・ヘルスケア分野における生成 AI 利用ガイドライン（第 2 版）[29]

本ガイドラインは、医療 AI プラットフォーム技術研究組合が、厚生労働科学研究の成果として取りまとめたものであり、主として医療従事者による診療場面での生成 AI 利用を対象としている。そのため、直接的には PV 業務への適用を想定したものではない。しかしながら、PV において利用されるデータの多くが医療現場において生成されること、また、当該データの作成過程における AI 利用がデータ品質に影響を及ぼし得ることを踏まえれば、本ガイドラインは PV 分野に対しても間接的な影響を有する。

したがって、AI 開発及び運用の前提となるデータ生成過程の観点からも、本ガイドラインの内容は参照に値する。

2 FDA（U.S. Food and Drug Administration）と EMA（European Medicines Agency）の動向

（1）FDA と EMA の共同原則（Good AI Practice）

FDA の AI 関連ドラフトガイダンス（Considerations for the Use of Artificial Intelligence to Support Regulatory Decision-Making for Drug and Biological Products）[30] および、EMA の Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle[31] と整合する形で、FDA と EMA は、2024 年 4 月の FDA-EU 二国間会議後の共同作業を踏まえ、2026 年 1 月 14 日に Guiding Principles of Good AI Practice in Drug Development を公表した[32]。

本原則は、医薬品開発および医薬品ライフサイクル全体における AI 活用に関する基本的枠組みを提示するものであり、今後の各国規制および国際的ガイダンス形成にお

いて中核的な参照基準となることが想定される。

同文書では、以下の 10 項目の原則が提示されている。

①人間中心の設計（Human-centered design）

AI は倫理的かつ人間中心の価値観に基づいて設計されるべきであり、人間の意思決定を補完しつつ、患者の利益を最優先とする。

②リスクベースのアプローチ（Risk-based approach）

AI の利用目的（コンテキスト・オブ・ユース）に応じてリスクを特定・評価し、そのリスクに見合った検証、監視および管理措置を講じる。

③関連標準および規制への適合（Compliance with applicable standards）

法規制、倫理指針、科学的基準、技術標準、サイバーセキュリティ、および GxP（GCP、GMP 等）を含む関連要件への適合を確保する。

④明確な使用文脈の定義（Clear context of use）

AI の目的、機能、出力の用途および適用範囲を明確に定義し、透明性を担保する。

⑤学際的専門性の統合（Multi-disciplinary expertise）

データサイエンス、ソフトウェア工学、医学・薬学領域、品質保証、セキュリティ等の専門知を統合した開発・運用体制を構築する。

⑥データガバナンスと文書化（Data governance and documentation）

データの出所、前処理、品質管理、分析手法および意思決定プロセスを追跡可能かつ検証可能な形で文書化し、個人情報保護およびデータ完全性を確保する。

⑦モデル設計・開発の妥当性（Model development and appropriateness）

AI モデルは、目的適合性、説明可能性・解釈性および予測性能のバランスを考慮し、適切な技術基盤のもとで設計・構築されるべきである。

⑧リスクに応じた性能評価（Performance evaluation）

AI モデルの性能はリスクに応じて評価され、妥当性確認（validation）、堅牢性、一般化可能性を確保するとともに、継続的なモニタリングを行う。

⑨ライフサイクル管理（Lifecycle management）

AI は開発、検証、導入、運用、モニタリング、改良に至る全ライフサイクルを通じて管理され、データドリフトやモデル劣化への対応を含めた継続的改善が求められる。

⑩透明性と適切な情報提供（Transparency and communication）

AI システムの構造、限界、前提条件および利用方法について、利用者が理解しやすい形で本質的な情報を提供する。

以上の原則は、従来の GxP や品質保証の枠組みを拡張し、AI 特有の不確実性および動的特性を統合的に扱うための指針として位置づけられる。特に、リスクベースアプローチとライフサイクル管理の強調は、AI を静的なツールではなく、継続的に更新・監視される「進化的システム」として捉える規制思想の転換を示している。

また、本原則は拘束力を持つ規制ではないものの、FDA および EMA という主要規制当局による共同提示であることから、今

後の各国規制や ICH 等の国際調和プロセスにおいて、事実上のグローバル標準として機能する可能性が高い。

（2）The Council for International Organizations of Medical Sciences (CIOMS), Artificial Intelligence in Pharmacovigilance [33)]

本報告書は、CIOMS の Working Group XIV により取りまとめられた、ファーマコビジランス（PV）領域における AI 活用に特化した国際的指針であり、2025 年に公表された成果物である。とりわけ Chapter 7 においては、データプライバシーの観点から、個人情報保護およびデータガバナンスの確保に関する論点が体系的に整理されており、AI を用いた安全性監視における倫理的・法的配慮の重要性が示されている。

3 その他 （関連する補足的文書）

（1）Guiding principles on the use of large language models in regulatory science and for medicines regulatory activities [34)]

本原則は、欧州医薬品庁（EMA）および欧州医薬品規制当局長官会議（HMA）により策定されたものであり、欧州医薬品規制ネットワーク（EMRN）の全職員を対象として、大規模言語モデル（LLM）の業務利用に関するハイレベルの原則および推奨事項を提示するものである。2024 年 8 月 29 日付で公表されている。本原則は、規制科学および規制業務における LLM の適切な利用に向けた初期的枠組みを示すものであり、今後の実務指針や内部ガバナンス整備の基盤として位置づけられる。

（2）医療デジタルデータの AI 研究開発等への利活用に係るガイドライン [35)]

本ガイドラインは、厚生労働省科学研究費補助金による研究班により策定されたものであり、医療機関、学術研究機関および民間企業等が共同研究を起点として、医療機関が保有する医療情報を活用した製品開発を行う場合を想定した実務的指針である。2024 年 3 月 31 日付で公表されている。医療データの利活用に関する具体的な手続や留意点を提示する点に特徴があり、日本における医療 AI 開発の実務基盤を支える文書として一定の意義を有する。

以上のとおり、日本における AI 関連ガイドラインは、主として原則および実務指針を中心とするソフトローとして整備が進展している。他方で、これらの多くは法的拘束力を伴うものではなく、統一的かつ強制力を有する規制枠組みとしては、なお発展途上の段階にあると評価される。

この点は、次節において検討する EU の包括的規制枠組みとの対比において、重要な分析視角を提供するものである。

第 4 章第 6 節 海外規制動向
—EU AI Act 及び EHDS を中心に—

PV 分野における AI 利用を検討するに当たっては、国内ガイドラインのみならず、海外における規制動向も参照する必要がある。とりわけ EU では、AI そのものを横断的に規律する AI Act [36)] と、医療データの一次利用・二次利用の基盤整備を目的とする European Health Data Space（EHDS）[37)] が整備されつつあり、両者

は、医療分野における AI ガバナンスを考える上で重要な参照枠組みを提供している。AI Act は AI システムのリスク管理、透明性及び人間による監督を中心に規律するのに対し、EHDS は電子的医療データのアクセス、共有及び再利用の制度的基盤を構築するものであり、両者はそれぞれ異なる角度から AI 時代の医療データ利活用を支える。EU の制度設計は、日本における PV 分野の AI 利用に直接適用されるものではないが、今後の制度構築及び実務運用を検討する上で示唆に富む。また、EHDS については、欧州委員会により FAQ が公表されており、制度の適用範囲やデータ利用の在り方に関する実務的解釈が補足されている。

1 EU AI Act

EU AI Act は、EU における包括的な AI 規制として 2024 年 8 月 1 日に発効し、原則として 2026 年 8 月 2 日から全面適用されるが、一部の規定はこれに先立って段階的に適用されている。たとえば、禁止される AI 慣行及び AI リテラシーに関する義務は 2025 年 2 月 2 日から適用されており、汎用 AI モデル（general-purpose AI models）に関する義務は 2025 年 8 月 2 日から適用されている。もっとも、高リスク AI システムに関する主要な規律の多くは、2026 年 8 月 2 日又は 2027 年 8 月 2 日に適用開始とされており、現在は移行期間にあると理解すべきである。

AI Act は、AI システムをリスクに応じて区分し、一定の AI 慣行を禁止し、高リスク AI システムについては、リスク管理、技術文書、ログ記録、透明性、人間による監督、精度・堅牢性・サイバーセキュリティ等の要件を課す構造を採用している。また、汎用 AI モデルについても、技術文書の整備、著作権ポリシー、学習データの要約公表等の義務が課され、さらにシステミックリスクを有する汎用 AI モデルについては、リスク評価・低減、インシデント報告、サイバーセキュリティ対策等の追加義務が課される。

PV 分野との関係では、症例要約、文献スクリーニング、シグナル検出補助、問い合わせ対応等に AI を利用する場合、当該 AI が直ちに AI Act 上の「高リスク AI システム」に該当するか否かは個別評価を要するものの、少なくとも、透明性、人間による監督、文書化、監査可能性 といった規律は、PV における AI 利用の実務設計に直接的な示唆を与える。とりわけ、最終判断を人間が担保すること、利用目的や性能限界を明確化すること、導入後も継続的に監視・改善することは、前節までに述べた「出口規制モデルとしての AI ガバナンス」と整合的である。これは、AI 利用の適法性を事前の同意や形式的要件のみによって担保するのではなく、実際の運用過程とその帰結を継続的に統制するという方向性を強化するものといえる。

2 European Health Data Space（EHDS）

これに対し、既出の EHDS は、医療データの流通及び再利用に関する制度的基盤を整備するものであり、Regulation (EU) 2025/327 として 2025 年 3 月 5 日に EU 官報に掲載され、同年 3 月 26 日に発効した。EHDS の目的は、個人が自己の電子的

医療データへのアクセス及び統制を強化できるようにするとともに、研究、イノベーション、政策立案、患者安全、規制活動等の公益的目的のために電子的医療データの二次利用を可能にする点にある。

EHDS の特徴は、医療データの一次利用（診療等における利用）と二次利用（研究、規制、政策立案等のための再利用）を制度上区別しつつ、後者について一定の手続的・組織的統制の下で利用を認める点にある。前章第 2 節で取り上げた「入口規制から出口規制への転換」という視点との関係では、EHDS は、個別同意のみに依拠せず、許可手続、利用目的の限定、アクセス主体の要件、禁止される利用の明確化等を通じて、医療データの公益的利活用を制度的に正当化しようとする試みとして理解することができる。とりわけ、研究、イノベーション、政策形成、患者安全及び規制活動が二次利用の対象目的として明示されている点は、PV 分野における RWD 利活用との親和性が高い。

PV との関係では、EHDS は、将来的に、安全性評価、シグナル検出、規制当局による検証等に利用し得る広域的データ基盤の形成を志向している点で注目される。他方で、その利活用は無制限に許容されるものではなく、アクセス及び再利用は、制度上定められた目的、手続及びガバナンスの枠内で行われることが予定されている。この点は、AI による分析・推論の高度化が進むほど、データそのものの可用性だけでなく、誰が、どの目的で、どの条件の下で利用できるのか という統治構造が決定的に重要になることを示している。EHDS は、この意味において、AI 時代の医療データガバナンスを具体化する制度的試みと位置づけることができる。

以上のとおり、EU AI Act と EHDS は、それぞれ AI システムの規律 と 医療データ流通の規律 という異なる領域を対象としつつ、AI 時代の医療データ利活用における統合的ガバナンスの基礎を形成している。前者は透明性、人間による監督、文書化、リスク管理等を通じて AI 利用の適正性を担保し、後者はデータアクセス及び再利用の条件、目的制限及び制度的統制を通じて医療データ利活用の正当性を支える。

したがって、PV 分野における AI 利用を検討するに当たっては、AI の性能や有用性のみならず、①どのようなデータ基盤の上で、②いかなる主体が、③どのような手続と監督の下で AI を利用するのか、という観点から制度を構想する必要がある。日本においても、今後、個人情報保護法制、医療情報利活用制度及び AI 規律を相互に連関させながら、入口規制と出口規制を適切に組み合わせたガバナンスの構築が求められる。

第 5 章 RAG およびログ管理の論点（概念整理）

前章では、AI 導入により PV 業務における判断構造が変容することを概念的に整理した。本章では、その具体的な技術形態の一つとして近年注目されている RAG（Retrieval-Augmented Generation）及びログ管理に着目し、その構造的特性とガバナンス上の論点を整理する。本章の目的は、特定の技術実装の優劣を評価すること

ではなく、AI の利用形態の差異がもたらす「知識の所在」「判断過程の記録」「監査可能性」の構造的相違を明らかにする点にある。なお、本章では技術的要素を扱うが、実装の詳細には立ち入らず、あくまで制度設計及びガバナンスとの関係における構造的特性に焦点を当てる。

第 5 章第 1 節 知識構造としての RAG

1 RAG の基本構造

RAG とは、大規模言語モデル（LLM）が内部に保持する知識に加え、外部データベースや文書群を検索し、その結果を参照しながら応答を生成するアーキテクチャをいう [38)]。

この構造において重要なのは、AI の知識が「モデル内部の知識」と「外部参照知識」という二層に分離される点にある。この二層構造は、従来の AI における「学習＝知識保持」という前提を相対化し、知識を「保持されるもの」から「参照されるもの」へと転換する契機を与える。

近年、医薬品安全性監視（PV）分野においても、AI の活用は症例処理、文献レビュー、シグナル検出等に広がりつつあり、外部知識を参照する構造は実務上の重要性を増していると指摘されている [39)]。

2 モデル内部知識と外部参照知識の分離

従来の AI モデルは、学習時に取り込まれたデータを内部に保持し、その範囲内で推論を行う構造を有していた。

これに対し、RAG では、あらかじめ設定された外部の知識源（データベース、文書群等）を参照・抽出し、その結果を踏まえて応答が生成される。すなわち、参照対象となるデータは、利用者又はシステム設計者によって選定・管理されるものであり、無制限に外部情報を自律的に探索するものではない。

この構造は、以下の特徴を有する。

・知識の更新可能性が高い（外部データの更新に依存）
・モデル内部に情報を保持しない設計が可能
・応答の根拠が外部文書に依拠する

このように、RAG は従来の「学習データ依存型 AI」とは異なり、「参照型 AI」として位置づけることができる。

さらに重要なのは、この構造が「知識に関する責任主体」を変化させる点である。すなわち、モデル開発者のみならず、参照対象となるデータの選定及び管理主体が、判断の質及び妥当性に直接的な影響を及ぼすことになる。

3 非保持性（non-retention）との関係

RAG の構造は、入力データや出力結果をモデル内部に保持しない設計（非保持）と高い親和性を有する。すなわち、推論時に利用される情報は外部参照に依拠するため、モデル自体が新たな個人データを学習・蓄積する必要がない。

この点は、個人情報保護及びデータ最小化の観点から重要な意義を有する。特に、医療データのような高機微情報を取り扱う場面においては、データをモデル内部に取り込まないという設計は、リスク低減の手段として機能し得る。

さらに、この非保持性は、AI の利用形態を「データ蓄積型」から「データ参照型」

へと転換する可能性を有している。この転換は、単なる技術的差異にとどまらず、データの管理責任、利用範囲、監査可能性といったガバナンス構造全体に影響を及ぼすものである。

第 5 章第 2 節 記録構造としてのログ管理

1 ログ管理の位置づけ

AI の利用においては、判断過程の記録としてのログ管理が重要な役割を果たす。特に RAG 型 AI においては、検索クエリ、参照された文書、生成された応答、さらにはユーザーによる最終判断といった一連のプロセスがログとして記録され得る。

ここで重要なのは、ログが単なる事後的記録にとどまらず、「判断過程を再構成可能にする構造」を提供する点にある。すなわち、ログは、AI による判断生成プロセスを時間的に遡及し、再現するための制度的基盤として機能する。

2 証跡性（traceability）

ログは、AI の出力がどのような情報に基づいて生成されたかを追跡するための証跡を提供する。この機能は、前章で指摘した AI のブラックボックス性に対する重要な補完手段となる。

特に、外部参照型である RAG においては、「どの文書が参照されたか」という情報が記録されることで、判断の根拠を外部から追跡することが可能となる。

この点において、説明可能性の重心は、「内部構造の理解」から「外部証跡の追跡」へと移行する。すなわち、完全な内部説明が困難である場合であっても、どの情報に依拠して判断が形成されたかを検証可能とすることにより、説明責任を代替的に構成することが可能となる。

3 監査可能性（auditability）

ログは、第三者による事後的検証を可能とする基盤を提供する。すなわち、

・適切なデータが参照されていたか
・不適切又は誤導的な出力がなされていないか
・人による最終判断が適切に介在しているか

といった点について、客観的に検証することが可能となる。

この監査可能性は、前章で整理した説明可能性および AI ガバナンスと密接に関連している。とりわけ、AI において完全な内部説明が困難な場合には、ログに基づく外部的検証が、適正性担保の中核的手段となる。

また、監査可能性は単なる事後的検証にとどまらず、運用段階における抑止効果（deterrence）をも有する。すなわち、記録され、検証され得るという前提が、AI 利用における適切な行動を促す制度的機能を果たす。

近年、AI の説明可能性には技術的限界が存在することが指摘されており、完全な内部理解に代えて、出力結果の検証可能性及び監査可能性を重視するアプローチが提唱されている [40)]。

4 人間判断との接続

ログ管理は、AI の出力と人間の最終判断との関係を明示する役割も有する。すなわち、AI が提示した情報に対して、人間がど

のように評価し、どのような判断を行ったかを記録することにより、判断プロセス全体の可視化が可能となる。このことは、責任の所在を明確化する上でも重要な意味を持つ。

ここで重要なのは、単に人間が関与したという事実ではなく、「人間の判断がいかなる過程を経て形成されたか」が記録される点にある。これにより、AI と人間の協働関係は、抽象的な原則ではなく、検証可能な形で制度的に把握されることとなる。

このように、ログは、AI と人間の関係を媒介し、責任構造を接続する装置として機能する。

第 5 章第 3 節 ガバナンス上の論点

以上に整理した知識構造（RAG）及び記録構造（ログ管理）を踏まえると、AI の利用は、従来の枠組みとは異なるガバナンス上の論点を提起する。以下では、その主要な点を整理する。

1 知識の所在の分散

RAG においては、知識がモデル内部ではなく外部データに分散して存在する。このため、データの選定、更新管理、信頼性評価といった問題が新たに生じる。

この構造は、判断の質が単にモデルの性能に依拠するのではなく、参照されるデータの質及び管理体制に大きく依存することを意味する。すなわち、AI の適正性は「モデル中心」から「データガバナンス中心」へと重心を移す。

この点において、RAG の導入は、AI ガバナンスの焦点をアルゴリズムそのものから、データの選定および管理という外部要素へと拡張する契機となる。

2 責任構造の再編

RAG 型 AI では、モデル提供者、データ提供者、利用者等の複数の主体が関与するため、責任は単一主体に帰属するのではなく、構造的に分散する。

この場合、責任が消失するのではなく、むしろ機能ごとに分解し、再配置する必要がある。すなわち、

・モデル設計に関する設計責任
・データ選定及び管理に関するデータ責任
・運用に関する運用責任
・最終判断に関する判断責任

といった多層的な責任構造を前提とする必要がある。

このような責任の分解は、責任の所在を曖昧にするものではなく、各機能に対応した責任の明確化を可能とするものである。すなわち、責任構造の再編とは、責任の希薄化ではなく、責任の可視化及び制度的再設計を意味する。

この点については、AI の実装において責任主体が多層化することを前提としたガバナンス設計の必要性が、医療分野を含む複数の研究において指摘されている[41)]。

3 記録とプライバシーの関係

ログの記録は監査可能性を高める一方で、個人情報や機微情報の保存につながる可能性もある。このため、

・どの範囲のログを保存するか
・保存期間をどのように設定するか
・匿名化又は仮名化をどの程度適用するか

といった点が重要な論点となる。

ここでは、記録の充実による監査可能性

の確保と、プライバシー保護との間での調整が不可避となる。すなわち、「完全な記録」と「完全な非保持」という二項対立ではなく、リスクに応じた中間的設計が現実的な選択肢となる。

このような設計は、データ最小化原則や目的限定原則と整合させつつ、AI の利用実態に即した柔軟なガバナンスを構築する観点から重要である。

第 5 章第 4 節 構造的意義と生成 AI に関する追加的論点

本章で整理した RAG 及びログ管理の特性は、単なる技術的差異にとどまらず、AI 利用における基本構造そのものの再定義をもたらすものである。すなわち、

・知識は「保持」から「参照」へ
・説明は「内部理解」から「外部証跡」へ
・責任は「単一主体」から「多層構造」へ

と転換する。

このような構造的転換は、AI の個別的な実装を超えて、データ、判断及び責任の関係を再編成するものであり、AI ガバナンスを理解する上での基盤を構成する。すなわち、AI の適正性は、モデル単体の性能ではなく、データの管理、記録の確保及び監査可能性を含む総体的な構造によって担保されることとなる。

さらに、これらの構造的特性は、近年急速に普及している生成 AI の利用において、より顕著に現れる。生成 AI は、従来の AI とは異なる特性を有し、以下のような追加的論点を提起する。

第一に、生成 AI は確率的に出力を生成する特性を有し、同一入力に対しても結果が変動し得る非決定性を有する。このため、誤情報（いわゆるハルシネーション）の発生可能性があり、特に医薬品安全性評価のような高リスク領域においては、出力結果の検証及び人間による確認が不可欠となる。

第二に、生成 AI の利用においては、入力情報が外部環境に送信・保存され、学習に利用される可能性がある。このため、医療情報等の機微情報を取り扱う場合には、閉域環境での運用、学習・保持の制御、契約上の制限等を通じて、情報流出及び不適切利用のリスクを低減する必要がある。

第三に、生成 AI はその内部構造の特性上、出力過程の完全な説明が困難である場合が多い。このため、説明可能性は内部処理の理解に依拠するのではなく、入力・出力の記録及び参照情報の管理を通じた事後的検証可能性（監査可能性）によって担保される必要がある。

第四に、AI の利用はあくまで人間の意思決定を支援する補助的手段として位置付けられるべきであり、最終的な判断及び責任は人間に帰属する。この点は、生成 AI の出力が高度に自然な形で提示されることにより、過度な依存が生じ得ることを踏まえると、特に重要である。

以上の点は、総務省「AI 事業者ガイドライン」において示されている人間中心性、リスクベースアプローチ、データガバナンス等の原則とも整合するものであり、PV 分野における生成 AI の適切な利用において重要な視点となる。

以上を踏まえると、PV 分野における AI 利用は、従来の枠組みでは十分に捉えきれない新たなガバナンス原則を要請するものである。すなわち、AI の利用形態に応じ

て、知識の所在、判断過程の可視性及び責任構造が変化することを前提とし、それに対応した制度設計が必要となる。

本章で整理した構造的理解は、次章で提示する基本原則の理論的基盤を構成するものである。

第Ⅳ部 ガバナンス枠組みの整理

第 6 章 PV×AI の基本原則

前章までにおいて、PV 分野における RWD 活用の構造及び AI 導入による構造的変化を整理するとともに、RAG 及びログ管理に関する検討を通じて、AI 利用における知識構造及び判断過程の可視性に関する論点を明らかにした。これらの検討から明らかとなったのは、AI の利用が、知識の所在、判断の形成過程及び責任の帰属といった基盤的要素に対して構造的な変容をもたらすという点である。

本章では、これらの構造的変化を踏まえ、PV 領域における AI 利用に関する基本的な原則を、将来的なガイダンス策定に向けた参照枠として抽象的に整理する。

なお、本章で提示する原則は、前章までに整理した構造的特性、すなわち「知識の参照化」「判断過程の記録化」「責任の多層化」といった変化に対応するものとして位置づけられる。

第 6 章第 1 節 原則の位置づけ

本章で提示する原則は、個別の技術や制度を直接規律するものではなく、AI 利用に関する多様な実装形態を横断的に評価するための参照枠としての性格を有する。すなわち、これらの原則は、①技術的実装の適否を判断する基準、②制度設計における選択肢を整理する枠組み、③リスク評価の前提となる観点として機能することが想定される。

また、これらの原則は固定的な規範として一律に適用されるものではなく、利用文脈（context of use）に応じて相対的に適用されるべきものである。特に PV 分野においては、対象業務の性質、データの特性、患者安全への影響の程度等に応じて、その適用の態様を調整する必要がある。

さらに、本章で整理する原則は、前章までに検討した構造的特性、すなわち「知識の参照化」「判断過程の記録化」「責任の多層化」といった変化を踏まえて導出されるものであり、技術中立的かつ実装横断的に適用される枠組みとして位置づけられる。

したがって、これらの原則は特定の技術類型に限定されるものではなく、RAG や生成 AI を含む多様な AI 利用形態に適用可能な基盤的視座を提供する。

また、本章で提示する原則は、後続章において具体的な運用構造として再構成されることを前提とするものであり、ここではその方向性を示す抽象的枠組みとして整理する。

第 6 章第 2 節 各基本原則

1 目的明確性の原則

AI の利用にあたっては、その目的および利用範囲が明確に定義される必要がある。これは、AI の出力がどのような意思決定に用いられ、その影響がどこまで及ぶのかを事前に特定することである。

特に PV 分野においては、安全対策という公共性の高い目的に関わるため、利用文脈（context of use）の明確化が不可欠である。目的が不明確な場合、リスク評価および責任の所在も不明確となる。

さらに、目的の明確化は、AI が関与する判断の範囲を限定する機能を有する。すなわち、どの段階で AI を用い、どの段階を人間の判断に委ねるのかを明示することが、適切なガバナンスの前提となる。

また、AI の利用可否や管理の強度は一律に定めるべきものではなく、対象業務の性質、利用文脈、データ品質、患者安全への影響の程度等に応じて判断される必要がある。このようなリスクベースアプローチは、近時の国際的整理とも整合する[42)]。

2 影響最小化の原則

AI の利用にあたっては、個人の権利利益および社会的影響を最小限に抑えることが求められる。これは、データの収集・利用・保存の各段階において、必要最小限の範囲に限定するという考え方であり、個人情報保護におけるデータ最小化原則とも整合する。

特に、AI の学習や推論において過剰なデータ利用が行われる場合、再識別リスクや不適切利用の可能性が高まるため、利用の必要性とリスクとの均衡を検討することが不可欠である。

また、前章で整理した RAG のような構造は、データを「保持」ではなく「参照」することにより、この原則を技術的に補完し得る可能性を有する。この意味において、影響最小化は制約にとどまらず、技術設計の方向性とも結びつく原則である。

3 人間責任の原則

AI が意思決定を補助する場合であっても、最終的な判断および責任は人間に帰属する。この原則は、AI の導入によって判断主体が曖昧化することを防ぐとともに、特に PV 分野においては、医学的評価および安全対策に関する責任の所在を明確にする観点から重要である。

また、人間責任は単なる形式的な最終承認を意味するものではなく、AI の出力内容を理解し、必要に応じて修正または否定する能力と体制を含むものである。

さらに、この原則は、AI の出力を無批判に受容することを防ぎ、人間による批判的検討を前提とする利用形態を確保するという意味も有する。ログ管理による判断過程の記録は、この原則の実効性を支える重要な要素となる。

近時の国際的整理においても、人間による監督は AI 利用の例外的付加要件ではなく、信頼性と説明責任を成立させるための基本条件として位置づけられており、本原則と整合する[43)]。

4 説明可能性および監査可能性の原則

AI の利用においては、その判断過程および出力の根拠が、一定程度説明可能であることが求められる。

もっとも、すべての AI モデルにおいて完全な説明可能性を確保することは技術的に困難であるため、ログ管理や外部参照構造等を通じて、事後的な検証が可能な状態（監査可能性）を確保することが重要となる。

この点において、説明可能性は「内部構

造の完全な理解」から「外部的な検証可能性」へと再定義される。これにより、説明責任は技術的問題にとどまらず、記録および運用の問題として把握されることとなる。

また、監査可能性は、出力結果の点検にとどまらず、入力データの出所、処理過程、モデルの管理、運用履歴等が合理的範囲で追跡可能であることを含む。これは、AI の適正利用を担保するための基盤的要件である[44)]。

5 ガバナンス確保の原則

AI の利用は、開発者、提供者、利用者等の複数の主体が関与することを前提とする。このため、各主体の役割および責任を明確化し、適切なガバナンス体制を構築することが必要である。特に、データの取得、モデルの開発、運用、監視といったライフサイクル全体を通じた統合的管理が求められる。

また、前章で整理した責任の分散構造を前提とすれば、ガバナンスは単なる統制ではなく、多主体間の調整メカニズムとして理解される必要がある。この意味において、ガバナンスは各原則を統合する上位概念として位置づけられる。

第 6 章第 3 節 原則間の関係

以上の各原則は、それぞれ独立したものではなく、相互に関連し合う構造を有している。例えば、目的明確性は影響最小化の前提となり、説明可能性および監査可能性は人間責任の実効性を支える。また、これらの原則を統合的に担保する枠組みとしてガバナンスが位置づけられる。

したがって、PV×AI における原則は、単一の規範としてではなく、相互補完的な関係を有する体系として理解される必要がある。

さらに、これらの原則は相互にトレードオフ関係に立つ場合もある。例えば、詳細なログ記録は監査可能性を高める一方で、プライバシーへの影響を増大させる可能性がある。このため各原則は相互に調整されるべきものであり、単独で絶対化されるべきではない。

本章では、PV 領域における AI 利用に関する基本原則を、抽象的なレベルで整理した。これらの原則は、具体的な制度設計や実装に先立つ「方向性」としての性格を有し、今後のガイダンス策定において参照されることを想定している。また、本章で提示した原則は、前章までに整理した構造的特性に対応する形で導出されたものである。すなわち、知識の参照化、判断過程の記録化および責任の多層化といった変化に対して、それぞれ対応関係を有する。

次章において提示する「最小安全構成」は、これらの原則を具体的な運用の枠組みとして再構成する試みとして位置づけられる。

第 7 章 今後の国内向けガイダンス作成に向けた要点―「閉域運用×非学習・非保持×人の判断記録」を前提とする最小安全構成―

これまでの章において、PV 領域における AI 導入に伴う構造的変化および基本原則を整理した。本章では、これらの検討を踏まえ、今後、日本においてガイダンス等が検

討される際に参照し得る視点として、「最小安全構成」という考え方を概念的に提示する。ここでいう「最小安全構成」とは、AI 利用の多様な形態の中で、比較的リスクを限定し得る要素を組み合わせた運用モデルを抽象化したものである。例えば、閉域環境において入力データが外部に送信されず、かつモデル学習にも利用されない設定とし、さらに AI 出力に対する人間の判断内容をログとして記録する構成が、その典型例として挙げられる。

本章の目的は、このような構成を一つの基準として提示することにより、今後の制度設計や実務運用における議論の参照軸を提供する点にある。

さらに、本章は、前章までに提示した原則を具体的運用へと接続する試みとして位置づけられる。すなわち、「どのような構成が現実的な出発点となり得るか」を示すことを通じて、抽象的原則を実装可能な形へと翻訳することを意図するものである。

したがって、本章で提示する内容は特定の実装を固定的に推奨するものではなく、構造理解のためのモデルとして提示されるものであり、その意味において「構造の可視化」として理解される必要がある。

第 7 章第 1 節 最小安全構成という視点

AI の利用は多様な形態を取り得るが、そのすべてを一律に規律することは現実的ではない。このため、まずはリスクを相対的に限定し得る構成を抽出し、それを基準として他の形態との比較を可能にする視点が有用である。

本章では、このような観点から、「閉域運用」「非学習・非保持」「人の判断記録」という三つの要素から構成される「最小安全構成」を提示する。この「最小安全構成」は理想形を示すものではなく、「どの程度までリスクを抑制した状態で AI 利用が可能か」という観点から設定された基準点である。この基準点を設定することにより、より高度な AI 利用との間で段階的な比較が可能となる。

また、AI の導入は PV 業務の効率化および高度化を促進する一方で、その完全な自動化には依然としてリスクが伴い、特に最終的な安全性判断における人間の関与が不可欠であるとされている[45]。この点は、本研究において提示した最小安全構成の考え方と整合する。すなわち、AI の活用はあくまで判断支援として位置づけられ、その運用は人間による統制および記録を前提として構成される必要がある。

第 7 章第 2 節 3 つの構成要素

1 閉域運用（closed environment）

閉域運用とは、AI システムが外部ネットワークから隔離された環境、または限定されたアクセス制御の下で運用される構成を指す。この構成は、以下の点においてリスクの限定に寄与する。

・外部へのデータ流出リスクの低減
・利用主体の限定による統制の容易性
・データ利用範囲の明確化

特に、医療データのような機微性の高い情報を扱う場合、データの所在およびアクセス経路が制御可能であることは、ガバナンスの基盤となる。この点は、リモートアクセス環境での解析やデータ持ち出し制限を伴う運用とも整合する。

さらに、閉域運用は単なる技術的隔離にとどまらず、「データの流通経路を限定することによる責任の明確化」という機能を有する。すなわち、どの主体がどのデータにアクセス可能であるかが明確になることで、ガバナンスの実効性が高まる。

2 非学習・非保持（non-training / non-retention）

非学習とは、AI モデルが利用時に新たなデータを学習しない構成を指し、非保持とは、入力データや出力結果を継続的に蓄積しない構成を指す。

この構成は、以下の点において重要である。

・個人データの蓄積によるリスクの抑制
・モデル内部への情報混入の回避
・データ管理範囲の限定

前章で整理した RAG 構造との関係では、外部参照型の設計により、モデルに情報を保持させない運用との親和性が高い。また、非保持の考え方は、データ最小化および保存期間制限といった個人情報保護の原則とも整合する。

さらに、この構成は、AI 利用を「データ蓄積型」から「データ非蓄積型」へと転換する可能性を有しており、制度的リスクの低減と技術設計が結びつく典型例と位置づけることができる。

特に PV 業務は高い規制影響を伴い得る領域であるため、AI 利用の初期段階又は高感度な業務においては、閉域かつ非保持的な利用形態を基準とすることに合理性がある。この点は、リスクベースアプローチを採る国際的ガイドラインとも整合する。

3 人の判断記録（human-in-the-loop with record）

AI の利用においては、人間が最終判断を行うことに加え、その判断過程が記録されることが重要である。

ここで重要なのは、「人間が関与すること」自体ではなく、AI の出力、人間の評価、最終判断の関係が記録として残る点にある。

この構成は、以下の機能を備えている。

・責任所在の明確化
・判断過程の事後検証可能性
・AI 出力の適切性の評価基盤

特にログ管理との関係においては、AI の出力と人間の判断の接続が可視化されることで、監査可能性が担保される。

また、この構造は、第 6 章で示した「人間責任の原則」および「監査可能性の原則」を具体的に運用するのに結びつくものである。

ここでいう「人の判断記録」とは、単なる最終確認の事実ではなく、誰が、いつ、どの入力・参照情報・出力に基づいて判断又は修正を行ったかを、追跡可能な形で残すことを含む。このような記録化は、国際的に求められるトレーサビリティおよび文書化の要請とも整合する。

第 7 章第 3 節 三要素の相互関係

以上の三構成要素は、相互に補完し合う構造を有する。

・閉域運用は外部リスクを制御する
・非学習・非保持は内部蓄積のリスクを制御する
・人の判断記録は判断過程の責任および検証可能性を担保する

したがって、これらを組み合わせることにより、AI 利用に伴う主要なリスクを相対的に限定する構成が形成される。

ここで重要なのは、これらの要素が単独で機能するのではなく、「外部リスク」「内部リスク」「判断リスク」という異なるリスク領域を分担して制御している点である。この意味において、最小安全構成は「リスク分解に基づく統合構造」として理解される。

本章で提示した最小安全構成は、国際的および国内のガイドラインが共有する要求を、PV 実務における運用要件として整理したものと位置づけることができる。すなわち、リスクベースアプローチ、人間による監督、トレーサビリティおよびガバナンスといった要請は、いずれも統制された環境の下で AI 利用を行い、人間責任と検証可能性を確保することを求める点で共通している。

第 7 章第 6 節 位置づけ

ここで提示した「最小安全構成」は、最適な構成、唯一の構成、あるいは規範的に要求される構成を意味するものではない。むしろ、AI 利用の多様な形態の中で、「比較的リスクが限定された基準点」として位置づけられるものである。このような基準点を設定することにより、

・より高度な AI 利用との比較
・リスク評価の段階的整理
・制度設計における選択肢の明確化

が可能となる。

また、この構成は固定的なものではなく、技術の進展や制度環境の変化に応じて見直され得る、動的な参照枠として理解されるべきである。

さらに、本章で提示した最小安全構成は、第 6 章において整理した基本原則、すなわち目的明確性、人間責任、説明可能性および監査可能性、ガバナンス確保といった観点を、具体的な運用構造として翻訳したものである。すなわち、これらの原則は抽象的な規範にとどまるのではなく、閉域運用、非学習・非保持、人の判断記録といった構成要素として具体化されることにより、初めて実務における実効性を持つこととなる。

もっとも、これらの構成要素の実効性は、技術的設定のみによって担保されるものではない。AI サービスの利用に関わる契約条件および運用要件の中で制度的に位置づけられることにより、持続的かつ検証可能な形で確保される必要がある。とりわけ、データの取扱い、学習の有無、ログの管理、責任分担といった事項は、契約上の義務として明確化されることが重要である。

この観点から、本研究では、第 6 章において提示した原則および本章の最小安全構成を実務的に接続する試みとして、契約実務の観点からこれらの要素をどのように担保し得るかについて、具体的なチェックポイントとして整理した別添資料を付す。当該資料は、本研究における構造的理解を、制度・技術・実務の接点において具体化するための補助的参照資料として位置づけられる。

以上のように、本章で提示した最小安全構成は、「閉域運用×非学習・非保持×人

の判断記録」という三要素からなる運用モデルとして整理されるものであり、将来的には、より高度な AI 利用形態との比較基準として機能し得るとともに、段階的なガバナンス設計を検討する際の出発点となり得る。

この意味において、本章は、原則（第 6 章）と実務（別添資料）の中間に位置するものであり、両者を接続する概念的枠組みとして理解される必要がある。

D. 結論

本研究は、医薬品安全性監視（PV）分野における人工知能（AI）導入をめぐる議論について、制度・データ・技術の三層が交差する構造として捉え直し、その全体像を整理することを目的として検討を行った。

本研究により明らかとなったのは、AI の導入が単なる業務効率化にとどまるものではなく、判断主体、責任構造、データ利用の時間性および知識の所在といった、PV 業務の基盤的前提そのものを変容させる構造的契機であるという点である。とりわけ、学習段階と推論段階の分離、モデルの残存性、判断過程の不可視性および責任の分散といった特性は、従来の人間中心的判断構造に対して連続性と断絶の双方をもたらす。

こうした構造的変化に対応するためには、従来の同意を中心とした「入口規制モデル」のみでは十分ではなく、利用過程および利用結果に対する継続的統制を重視する「出口規制モデル」を基軸としたガバナンスの再構成が不可欠である。本研究において整理した、第三者による監督、説明責任の再構成、責任の多層的配分および継続的モニタリングは、このような転換を支える基本的要素として位置づけられる。

また、RAG（Retrieval-Augmented Generation）およびログ管理に関する分析を通じて、AI 利用における知識構造および記録構造の変化が、説明可能性および監査可能性の在り方を再定義することが示された。すなわち、説明可能性は内部処理の完全な理解に依拠するものから、外部証跡に基づく検証可能性へと重心を移し、ガバナンスはアルゴリズム中心からデータおよび記録の管理を含む総体的構造へと拡張される。

これらの検討を踏まえ、本研究は、PV 領域における AI 利用に関する基本原則として、目的明確性、影響最小化、人間責任、説明可能性および監査可能性、ならびにガバナンス確保の各原則を整理した。さらに、これらの原則を具体的運用へと接続する視点として、「閉域運用×非学習・非保持×人の判断記録」から構成される「最小安全構成」を提示した。この構成は、AI 利用の多様な形態の中でリスクを相対的に限定し得る基準点として機能し、今後の制度設計および実務運用における比較および段階的評価を可能とするものである。

以上の知見を踏まえると、今後の PV 分野における AI 導入においては、

①利用目的および文脈の明確化、
②人間による最終判断およびその記録の制度的確保、
③ログ等を通じた監査可能性の担保、
④データおよびモデルのライフサイクルを通じたガバナンス体制の構築

などの諸点が、実務上の重要な検討課題となる。

本研究は、特定の制度設計や技術導入の是非を直接的に提示するものではないが、PV×AI をめぐる議論を、制度・技術・実務の交差における構造的問題として再定位し、その理解のための参照枠を提示した点に意義を有する。今後は、本研究で提示した枠組みを基礎として、具体的なガイダンス策定、実務運用への適用および国際的制度調和に向けた検討が深化することが期待される。

E. 研究発表

1. 論文発表

1)Suzuki、S. (2025): Delegating tasks to AI encourages cheating, *Nature*, Vol. 646, 2—October, News and views, p.46. People are more likely to cheat when they delegate tasks to AI | Nature

2)Suzuki, S. (2025): Human Transformation and Generative Universality: Rethinking Citizenship in the Posthuman Age, *Paragrana*, Vol. 34 (2), pp. 280-291. https://doi.org/10.1515/para-2025-0034

2. 提言・報告書

1）鈴木晶子: 総務省 AI ネットワーク推進会議報告書 「AI 事業者ガイドラインの更新版（第 1.2 版）2026 年 3 月 31 日公表」（同 会議幹事として作成に参加)。https://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/02ryutsu20_04000019.html

註

1）厚生労働省の「医療 DX について」のサイトの説明によると、「医療 DX」とは、保健・医療・介護の各段階（疾病の発症予防、受診、診察・治療・薬剤処方、診断書等の作成、診療報酬の請求、医療介護の連携によるケア、地域医療連携、研究開発など）において発生する情報やデータを、全体最適された基盤（クラウドなど）を通して、保健・医療や介護関係者の業務やシステム、データ保存の外部化・共通化・標準化を図り、国民自身の予防を促進し、より良質な医療やケアを受けられるように、社会や生活の形を変えることをいう。

2）医療法等の一部を改正する法律（令和 7 年法律第 87 号）〔令和 7 年 12 月 12 日公布〕。なお、立法過程に関する資料として、厚生労働省ウェブサイトに「医療法等の一部を改正する法律案」（令和 7 年 2 月 14 日提出）および衆議院における修正案が掲載されている。厚生労働省のサイト

3) RWD（Real World Data）とは、日常診療において生成される医療情報（電子カルテ、レセプト、レジストリ等）を指し、医薬品の安全性評価や有効性評価に活用されるデータをいう。例えば、FDA は、RWD を「日常的な医療提供の過程で収集される健康関連データ」と定義している。

４） 医療分野の研究開発に資するための匿名加工医療情報及び仮名加工医療情報に関する法律（平成 29 年法律第 28 号)。医療データの利活用を促進するため、認定事業者による匿名加工医療情報および仮名加工医療情報の作成・提供等の枠組みを定め

るものであり、複数データベース間の連結解析を可能とする制度的基盤を構成する。

5）個人情報の保護に関する法律（平成 15 年法律第 57 号）。個人情報の適正な取扱いを確保するため、利用目的の特定、安全管理措置、不適正利用の禁止等の基本的規律を定めるものであり、医療データの利活用においても基盤となる法制度である。

６） 次世代医療基盤法に基づく医療情報の利活用の仕組みについては、認定作成事業者による匿名加工医療情報および仮名加工医療情報の作成・提供と、利用事業者による研究開発等への利用から構成される制度として整理される。

７） 個人情報の保護に関する法律の一部を改正する法律（令和 2 年法律第 44 号）附則第 10 条。施行後 3 年ごとに制度の見直しを行う旨を定める。

８） 規制改革実施計画（令和 7 年 6 月 13 日閣議決定）。医療等データの包括的かつ横断的な利活用法制の整備の一環として、本人同意規制の見直しが位置づけられている。

9) Regulation (EU) 2025/327 of the European Parliament and of the Council of 5 March 2025 on the European Health Data Space.

10） EHDS における匿名化データとは、個人を識別できないよう不可逆的に加工されたデータを指し、GDPR 上の個人データには該当しないものとして取り扱われる。EHDS における二次利用は、このような匿名化データを前提として設計されている。

１1） Secondary use under the European Health Data Space: setting the scene and towards a research agenda on privacy-enhancing technologies, Frontiers in Digital Health, 2025.

１２） Appendix 3 では、健康データの二次利用に関する複数のユースケース（Case A～E）が提示されており、特に Case E は、データアクセスの管理、利用目的の制御、およびプライバシー強化技術の適用を組み合わせた実務的な運用モデルを示している。本報告書における判断枠組みとも整合的な構造を有しており、制度設計の具体化に資する事例として参考となる。

１3） 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等の一部を改正する法律（令和 7 年法律第 37 号）。RWD の薬事申請の利活用は、第 14 条第 3 項、第 23 条の 2 の 5 第 3 項及び第 23 条の 25 第 3 項に、RWD の安全対策への利活用は、第 14 条の 4 第 5 項、第 23 条の 2 の 9 第 4 項及び第 23 条の 29 第 4 項にそれぞれ関係する。

14）「薬機法等制度改正に関するとりまとめ」において、RWD は、「実臨床の環境において収集された、患者の実際の健康状態や医療情報、治療経過等の安全性・有効性の評価に活用できる電子的データ」と説明されている。

15）独立行政法人医薬品医療機器総合機構（PMDA）「MID-NET の利活用事例」及び関連資料を参照。「『医薬品安全性監視における医療情報データベースの活用とその事例』について」（令和 5 年 6 月 9 日付事務連絡、厚生労働省医薬・生活衛生局審査管理課・医薬安全対策課）は、医薬品安全性監視における医療情報 DB の活用促進を目的に、医療情報 DB の活用事例を踏まえ

て、その活用目的及び一般的な留意事項を取りまとめたもので、別添に具体的な活用事例が整理されている。

16) G-CSF（Granulocyte Colony-Stimulating Factor）顆粒球コロニー形成刺激因子製剤とは、好中球の増殖・分化を促進する造血因子製剤であり、骨髄中の顆粒球系（特に好中球）の分化・増殖の促進作用を示し、主として抗がん剤治療に伴う好中球減少症の予防又は治療に用いられる。17) PMDA「MID-NET を用いた安全性評価事例（ペグフィルグラスチムと血小板減少）」に基づく。宇山佳明氏（独）医薬品医療機器総合機構(PMDA)資料の 8 頁を参照。また、次段落に記載する②の事例は同 9 頁を参照。

「医薬品安全性評価への RWD 活用に関する取組み」

18） クラスエフェクト（class effect）とは、同一又は類似の作用機序を有する医薬品群において、共通して現れる薬理作用又は副作用をいう。同じ薬のカテゴリー（クラス）に属する薬剤全般に共通して見られる効果や副作用を指す。

19) PMDA「MID-NET を用いた安全性評価事例（メトホルミンと乳酸アシドーシス）」に基づく。PMDA 資料の 7 頁を参照。

「医療情報データベースの活用促進のための規制当局としての取り組み」

20) PMDA「早期安全性シグナルモニタリング」に関する資料（条件付き承認制度等対象品目に関する安全性評価の枠組み）を参照。詳細は PMDA の以下の内容を参照していただきたい。

「早期安全性シグナルモニタリング」のサイト

21）独立行政法人医薬品医療機器総合機構「MID-NET の利活用に関するガイドライン」（最新版）。PMDA の以下のサイトに掲載されている「(1)利活用に関するガイドライン」。

MID-NET の関連通知等

利活用に関するガイドライン

22) PMDA が運営・管理を行い、データの抽出等の処理を依頼するためのスクリプト作成システム及び分析用データセット又は統計情報を解析するための複数施設統合処理システム、並びに MID-NET 接続環境又はオンサイトセンターからリモートアクセスする作業領域が設置されているところをいう。また、分析用データセット及び統計情報を保存する。

23）内閣府「医療等情報の利活用の推進に関する検討会」の設置及び議論状況に基づく整理。

医療等情報の利活用の推進に関する検討会のサイト

24) Proposal for a Regulation on the European Health Data Space（EHDS）, Articles 53 and 54.

25）内閣府「人工知能関連技術の研究開発及び活用の適正性確保に関する指針」（2025 年 12 月 19 日公表）。

https://www8.cao.go.jp/cstp/ai/ai_guideline/ai_gl_2025.pdf

26）厚生労働省・文部科学省・経済産業省「人を対象とする生命科学・医学系研究に関する倫理指針」及び同ガイダンス。本文 https://www.mhlw.go.jp/content/001077424.pdf ガイダンス

https://www.mhlw.go.jp/content/001237478.pdf
27）厚生科学審議会「生命科学・医学系研究等における個人情報の取扱い等に関する合同会議とりまとめ」（2025 年 12 月 24 日）。
https://www.mhlw.go.jp/content/10601000/001619373.pdf
28）総務省・経済産業省「AI 事業者ガイドライン」Ver.1.1（2025 年 3 月 28 日）、Ver.1.2（2026 年 3 月 31 日）。
総務省｜AI ネットワーク社会推進会議｜「AI 事業者ガイドライン」掲載ページ
29）医療 AI プラットフォーム技術研究組合「医療・ヘルスケア分野における生成 AI 利用ガイドライン（第 2 版）」。
https://haip-cip.org/assets/documents/nr_20241002_02.pdf
30) FDA, Considerations for the Use of Artificial Intelligence to Support Regulatory Decision-Making for Drug and Biological Products, Draft Guidance, Jan 2025.
Considerations for the Use of Artificial Intelligence To Support Regulatory Decision-Making for Drug and Biological Products｜FDA
31) EMA, Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle, 30 Sep 2024.
Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle_240903
32) FDA / EMA, Guiding Principles of Good AI Practice in Drug Development, 14 Jan 2026.
Guiding Principles of Good AI Practice in Drug Development｜FDA
33) Artificial intelligence in pharmacovigilance. CIOMS Working Group report. Geneva, Switzerland: Council for International Organizations of Medical Sciences (CIOMS), 2026.
Artificial Intelligence in Pharmacovigilance - CIOMS
34) EMA / HMA, Guiding principles on the use of large language models in regulatory science and for medicines regulatory activities, 29 Aug 2024.
35）厚生労働科学研究費補助金研究班「医療デジタルデータの AI 研究開発等への利活用に係るガイドライン」2024 年 3 月 31 日。
https://www.mhlw.go.jp/content/001310044.pdf
36) European Commission, AI Act – Shaping Europe’s digital future.
EU における包括的 AI 規制であり、2024 年 8 月 1 日に発効し、段階的に適用されている。禁止される AI 慣行及び AI リテラシー義務は 2025 年 2 月 2 日から、汎用 AI モデルに関する義務は 2025 年 8 月 2 日から適用されるなど、段階的施行が採用されている。
AI Act（欧州委員会ページ）
https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

（補足：汎用 AI 義務の詳細）
https://digital-strategy.ec.europa.eu/en/factpages/general-purpose-ai-obligations-under-ai-act
37) Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space (EHDS). 医療データの一次利用及び二次利用の枠組みを定める EU 規則であり、2025 年 3 月 5 日に公表され、同年 3 月 26 日に発効した。電子的医療データへのアクセス強化と公益目的での二次利用の制度化を目的とする。なお、欧州委員会は 2025 年 3 月 26 日付で本規則に関する FAQ を公表しており、制度運用に関する実務的解釈が提示されている。
EHDS（公式法令 EUR-Lex）
https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng
（補足：欧州委員会解説ページ）
https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en
EHDS（公式法令 EUR-Lex）
https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng
Artificial intelligence in pharmacovigilance. CIOMS Working Group report. Geneva, Switzerland: Council for International Organizations of Medical Sciences (CIOMS), 2026.
Artificial Intelligence in Pharmacovigilance – CIOMS.
なお、EHDS については、我が国においても、厚生労働省の審議会（2024 年）及び内閣府の検討会等において議論の対象とされており、医療データ利活用に関する制度設計の参照枠として言及されている。
001327545.pdf
s-2.pdf
38) European Data Protection Board (EDPB), “Guidelines on Data Minimisation,” 2023.
39) Choi, J., Palumbo, N., Chalasani, P.R., Engelhard, M.M., Jha, S., Kumar, A., & Page, D. (2024). MALADE: Orchestration of LLM-powered Agents with Retrieval Augmented Generation for Pharmacovigilance. ArXiv, abs/2408.01869.
40) AI の説明可能性（explainability）については、特に深層学習モデル等において、その内部処理を完全に解釈することが困難であることが指摘されている。このため、近年では、モデル内部の説明可能性に依拠するのではなく、出力結果の検証可能性や外部証跡に基づく監査可能性（auditability）を重視するアプローチが提唱されている。例えば、欧州委員会の AI 規制に関する議論においても、透明性及び監査可能性の確保が重要な要素とされている。Ohana, B., Sullivan, J.D., & Baker, N. (2021). Validation and Transparency in AI systems for pharmacovigilance: a case study applied to the medical literature monitoring of adverse events. ArXiv, abs/2201.00692.
41) Jain, A., Salas, M., Aimer, O. et al. Safeguarding Patients in the AI Era: Ethics at the Forefront of Pharmacovigilance. Drug Saf 48, 119–127

(2025). https://doi.org/10.1007/s40264-024-01483-9

42) CIOMS, CIOMS Working Group Report on Artificial Intelligence in Pharmacovigilance;
European Medicines Agency (EMA), Reflection paper on the use of artificial intelligence in the lifecycle of medicines;
総務省・経済産業省「AI 事業者ガイドライン」。これらはいずれも、AI の利用においてリスクベースアプローチを中核的原則として位置づけており、利用目的、影響範囲及びリスクの程度に応じた段階的評価の必要性を指摘している。
CIOMS-WG-XIV_Draft-report-for-Public-Consultation_1May2025.pdf
Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle_240903
日本病院薬剤師会 生成 AI 利活用ガイダンス（2026 年 2 月 18 日版）
病院薬剤師のための生成 AI 利活用ガイダンス

43) CIOMS, CIOMS Working Group Report on Artificial Intelligence in Pharmacovigilance;
European Medicines Agency (EMA), Reflection paper on the use of artificial intelligence in the lifecycle of medicines;
医療 AI プラットフォーム技術研究組合「医療・ヘルスケア分野における生成 AI 利用ガイドライン（第 2 版）」。これらは、AI の利用において人間による監督（human oversight）が不可欠であることを共通して指摘し、最終判断および責任が人間に帰属することを前提としている。
日本病院薬剤師会 生成 AI 利活用ガイダンス（2026 年 2 月 18 日版）

44) European Medicines Agency (EMA), Reflection paper on the use of artificial intelligence in the lifecycle of medicines;
CIOMS, CIOMS Working Group Report on Artificial Intelligence in Pharmacovigilance;
総務省・経済産業省「AI 事業者ガイドライン」。これらは、AI 利用における透明性（transparency）、説明可能性（explainability）及びトレーサビリティ（traceability）の確保の重要性を指摘しており、特にログ管理や文書化を通じた監査可能性の確保が、説明責任を担保する手段として位置づけられている。
Nagar A, Gobburu J, Chakravarty A. Artificial intelligence in pharmacovigilance: advancing drug safety monitoring and regulatory integration. Ther Adv Drug Saf. 2025 Jul 31;16:20420986251361435.

45) CIOMS, CIOMS Working Group Report on Artificial Intelligence in Pharmacovigilance;
European Medicines Agency.
https://cioms.ch/artificial-intelligence-inpv/?utm_source=chatgpt.com
(EMA), Reflection paper on the use of artificial intelligence in the lifecycle of medicines.
https://www.ema.europa.eu/system/files/documents/scientific-guideline/reflection-paper-use-artificial-intelligence-ai-medicinal-product-

lifecycle-en.pdf?utm_source=chatgpt.com

これらは、PV 領域における AI 利用に関し、完全な自動化には限界があり、特に安全性評価や規制判断においては人間による関与（human oversight）が不可欠であることを指摘している。また、AI は意思決定を代替するものではなく、補助的手段として位置づけられるべきであるとされている。

表 1

令和５年	
11月15日	「個人情報保護法 いわゆる３年ごと見直し規定に基づく検討」公表
11月下旬～	関係団体等ヒアリングを順次実施
令和６年	
２月21日	「個人情報保護法 いわゆる３年ごと見直し規定に基づく検討項目」公表
４月上旬～	有識者ヒアリングを順次実施（医療等関係は４月３日実施）
6月27日	「中間整理」公表（～7月29日まで意見募集実施）
9月 4日	「中間整理」に関する意見募集の結果 公表
10月16日	「個人情報保護法のいわゆる３年ごと見直しの検討の充実に向けた視点」公表
12月17日	事務局ヒアリング（有識者、経済団体・消費者団体等）の状況報告
12月25日	「個人情報保護法のいわゆる３年ごと見直しに関する検討会 報告書」公表
令和７年	
１月22日	「「個人情報保護法 いわゆる３年ごと見直しに係る検討」の今後の検討の進め方について」 「個人情報保護法の制度的課題の再整理」公表
２月 5日	「個人情報保護法の制度的課題に対する考え方について（個人データ等の取扱いにおける本人関与に係る規律の在り方）」公表
２月19日	「個人情報保護法の制度的課題に対する考え方について（個人データ等の取扱いの態様の多様化等に伴うリスクに適切に対応した規律の在り方）」公表
３月 5日	「個人情報保護法の制度的課題に対する考え方について」公表
６月13日	「経済財政運営と改革の基本方針2025」、「規制改革実施計画」等閣議決定

出典：医療等情報の利活用の推進に関する検討会（第 1 回）資料 5（個人情報保護委員会）

図 1

出典：医療等情報の利活用の推進に関する検討会（第 4 回）資料 6 の 7 頁より抜粋

資料１　AI 利活用に関する契約チェックポイント（PV 領域）

本資料は、本報告書第 7 章において提示した「最小安全構成」を前提として、PV 領域における AI 利用に関する契約実務上の論点を整理したものである。特に、ベンダ管理の観点から、AI サービスの導入および利用に際して契約上検討すべき主要な事項を、実務的なチェックポイントとして整理することを目的とする。

契約に基づくベンダ管理のための契約時にチェックすべきポイント

1. はじめに

AI 技術の利活用に関する契約に伴う法的リスクが十分に検討されていないとの懸念を踏まえ、令和 7 年 2 月に経済産業省から「AI の利用・開発に関する契約チェックリスト」（以下「チェックリスト」という。）が公表された。

本文書では、本報告書第 7 章「今後の国内向けガイダンス作成に向けた要点」において提示した最小安全構成を前提として、PV 領域において AI を利用したサービスを活用する場合に、ベンダ管理の観点から契約時に確認すべきポイントを、チェックリスト等に基づき整理するものである。

なお、契約内容は、個々の目的や当事者間に固有の制約等に応じて相対的に変化し得るものであり、本書において必要かつ十分な条項を網羅的に提示するものではない。そのため、チェックリスト記載の「チェックリストを活用する上での留意点[1]」は本文書にも妥当するものであり、契約実務において極めて重要である。実際の契約書確認に際しては、当該留意点をあらかじめ参照した上で、本文書を利用することが望ましい。

２．　チェックリストを参照する際の PV 領域における AI 関連サービス契約の整理

チェックリストは、AI 関連サービスの利用に際して、ユーザがベンダに対し「インプット」（例：分析対象データ）を提供し、ベンダがサービス内容に応じた「アウトプット」（例：分析結果）を提供すること、また、ベンダがインプットを用いてアウトプット以外の処理成果（「インプット処理成果」）を創出することや、ユーザがアウトプットを処理して「アウトプット処理成果」を得ることを想定し、これらの適切な利用とリスク分配の観点からチェックポイントを整理している。PV 領域における AI 関連サービスの利用も、基本的にこれと同様の構造であると理解される。

本文書は、(1) 製薬企業が汎用的 AI サービス（生成 AI を含む）を直接利用する場合に加え、(2) PV 業務委託先（CRO 等）が業務遂行の手段として汎用的 AI サービスを利用し、その成果（アウトプット）を製薬企業に提供する場合（委託＋ツール利用）を含め、委託先管理の観点から契約時に確認すべき事項を整理するものである。

後者の場合、委託先が利用する第三者 AI サービスの利用規約・運用条件（学習利用、保持、越境移転、再委託等）がリスクに直結するため、可能な範囲で情報開示を求め、契約および SOP により統制することが重要となる。

・本文書における「ベンダ」とは、製薬企業が行う AI を利用した PV 業務に関連して、製薬企業に対しサービスを提供する事業者（汎用的 AI サービス提供者又は PV 業務委託先（CRO 等））をいう。チェックリストの用語に照らすと、(1) 製薬企業が汎用的 AI サービスを直接利用する場合には、当該ベンダが「AI 提供者[2]」」および「ベンダ」に相当する。(2) 委託＋ツール利用の場合には、PV 業務委託先（CRO 等）が本書の「ベンダ」に相当し、当該委託先が利用する汎用的 AI サービス提供者（第三者 AI サービス提供者）の利用規約・運用条件がリスクに直結するため、可能な範囲で当該条件の情報開示を求め、契約および SOP により統制する。利用する側の製薬企業は、「AI 利用者[3]」および「ユーザ」に相当する。

・チェックリストでは、AI 利活用の場面で取り扱われる契約を、生成 AI サービスに代表される幅広い利用者への汎用的 AI サービスの提供に関する①利用型契約と、新たなソフトウェアやデータベース、モジュールやシステム等の開発要素が加わる②開発型契約の二類型に整理している。

・また、チェックリストにおいては、類型 1：汎用的 AI サービス利用型、類型 2：カスタマイズ型、類型 3：新規開発型の三類型のユースケースを想定し、各契約類型が提案されている。類型 1 は前記①利用型契約に、類型 2 および類型 3 は②開発型契約に対応する。

・PV に AI を利用するにあたっては、「特定のユーザが内部文書や取引情報をベンダに提供し、これらの情報を用いて AI システムを改良・調整することで、当該ユーザの個別ニーズに特化したアウトプットを出力する」ことにより、効率化および精度向上が期待される。チェックリストにおいて、このような利用は類型 2（カスタマイズ型）として定義され、②開発型契約に分類されている。

もっとも、この形態で開発に立ち入る場合、第三者による AI サービス提供が関与するなど、技術的および権利関係の双方において複雑性が増す。また、研究班報告書が想定する「閉域運用×非学習・非保持」の要件との関係で、当該構成に抵触する可能性を完全に排除できない。

このため、本文書では、①利用型契約、すなわち類型 1（汎用的 AI サービス利用型）に限定して整理する。なお、(2)の委託＋ツール利用の場合についても、委託先が利用する AI が汎用的 AI サービスの範囲にとどまる限り、チェックリスト上の類型 1 に関する論点整理を準用して検討する。

3．チェックリストに基づくベンダ管理の観点からのチェックポイント

本項目では、チェックリストに挙げられているチェックポイントのうち、インプットを提供し、アウトプットを受け取るユーザの立場で、専らベンダ管理の観点から、特に留意すべきものをピックアップし、適宜、編集等して記載する。なお、チェックリストにおいて各チェック

ポイントに付されている記号に対応しており、適宜、チェックリストの対応箇所を参照することを前提としている。なお、３．２アウトプット関連では、３．１インプット関連と重複する項目については、該当項目の指摘にとどめ、説明は割愛する。

3.1 インプット関連

（A-１-1） **定義｜インプットの定義を定める条項**

- 提供情報がインプットの定義に合致するか
- ユーザのサービス利用目的に照らして、上記内容は許容できるか
- インプットに個人データが含まれる場合の考慮要素は、脚注に記載[4)]

（A-2-1）**提供義務・条件｜ユーザがベンダに対してインプットを提供する義務の有無、及びその内容を定める条項**

（A-2-2）保証・情報提供｜ユーザがベンダに対し、インプットに関する一定の保証又は情報提供を行うことを定める条項

- インプット（提供情報）の取得・利用が適法であること（個人情報保護法、秘密保持義務、第三者の権利等）について、ユーザとして確認・整理できているか
- ベンダが適切にインプットを取り扱うために必要な情報（データの機微性、取扱い制約、保存・削除要件等）を、提供すべき範囲が明確か
- 保証・情報提供の範囲が過度に広く（包括保証、無過失責任等）なっていないか、また違反時の効果（是正、損害賠償等）が釣り合っているか

（A-3-1） **利用目的｜ベンダによるインプットの利用目的を定める条項**

- ベンダによるインプットの利用目的がサービス提供目的に限定されているか
- 目的外利用禁止が明確化されているか
- その他、**非学習に抵触する**目的が含まれないか

(A-3-2) **利用条件｜ベンダによるインプットの利用条件を定める条項**

- 自社技術開発や学習目的等、サービス提供目的外利用に該当する条件が含まれていないか

（A-3-3） **管理・セキュリティ｜ベンダによるインプットの管理・セキュリティ体制（セキュリティ水準を含む）を定める条項**

- インプットの管理義務、要求すべきセキュリティ水準が、**閉域利用**に抵触しないか
- ユーザによる監査権、ベンダーによる管理体制に係る情報提供義務、ログ保存義務が許容範囲内か。汎用的 AI サービスを利用する場合、利用規約型契約が多いため、問題となる[5)]。

（A-3-4） **保持期間・消去｜ベンダによるインプットの保持期間及び消去義務の有無を定める条項**

- ユーザが求める場合や契約終了時のインプットの削除義務（必要に応じて削除の履践を証明する書類等の発行義務）を定めているか
- その他、**非保持の原則**に抵触しないか

（A-4-1） **ユーザへの提供｜ベンダがインプットをユーザに対して提供する義務を定める条項**

本条項は、契約終了時やサービス切り替え時等にベンダからインプットの提供を受ける場合が想定されるが、含まれている場合、**非保持の原則**に抵触する可能性が高い条項であることに留意し、慎重に要否を検討する必要がある。

(A-4-2) **第三者提供[6]｜ベンダがインプットを第三者に提供することができるか、できる場合にその条件を定める条項**

- 外部流通を適切に制御し、**閉域利用の原則が担保される**構成になっているか
- インプットの第三者提供を禁止しているか（あるいはインプットをユーザの秘密情報として秘密保持義務の対象としているか）
- **閉域運用×非学習・非保持の要件**との整合（外部アクセス、ログ、保持期間等）を含めて、受容可能なリスク水準か評価する
- 越境移転・海外ベンダに関する事項[7]が、法令に抵触しないように規定されているか

（A-５ - １）**権利帰属｜インプットの権利がベンダに移転するか否かを定める条項**

ベンダへの権利移転は、**閉域運用・非学習・非保持**のいずれにも抵触し得るもので、回避すべきであるが、利用規約型契約で当該条項を排除できず、他に代替手段がない場合には、不必要な情報を提供しない等、運用面での対応もあり得る。

（A-6 - １） **特定｜インプットの処理成果のうち、アウトプット以外のもので契約上規律の対象とするものの定義を定める条項**

- 発生が想定される場合、契約上保護すべきインプット処理成果を疑義なく定義しているか。必要に応じて、インプットと同様の規律の対象になっているか

3.2 アウトプット関連

（B-１-１） **定義｜アウトプットの定義を定める条項**

(B-2-2) **提供義務・条件｜ベンダがユーザに対し、アウトプットを提供する義務の有無及びその内容を定める条項[8]**

- アウトプットを自動的な結論（規制当局への提出内容、医学的判断、安全対策判断等）に直結させず、専門家によるレビューを必須とする、**人の判断記録の原則**
- どのインプットに対してどのアウトプットを採用したか（採否・修正の理由を含む）を記録できる運用とする
- アウトプット生成条件（入力、モデル/バージョン、設定、参照情報の有無等）を追跡可能な形で保存し、必要に応じて再現できるようにする

（B-2-3） **保証・情報提供｜ユーザがベンダに対し、アウトプットに関する一定の保証を求める条項**

- ベンダによる保証が必要か
- 何についてどのような条件下で保証させるか（例えば第三者の権利非侵害等）
- アウトプット生成に関する情報について提供・説明義務を負わせる条件
- これらの義務違反があった場合、どのような効果を生じさせるか

（B-3） **利用目的、利用条件、管理・セキュリティ・消去｜各項目が、ユーザに課される条件として、利用目的に照らして、許容できる内容か**

（B-4-1） **第三者提供｜ユーザがアウトプットを第三者に提供することができるか、できる場合にその条件を定める条項**

（B-5 - 1） **権利帰属｜ベンダがユーザに対し、アウトプットを提供する場合、アウトプットの権利がユーザに移転するかどうかを定める条項**

- ユーザのサービス利用目的に照らして、必要な権利が備わっているか
- アウトプットに関する権利がユーザに移転しない場合、アウトプットの利用方法が限定されることを理解した上でサービスを利用する

（B-6 - 1） **特定｜アウトプットの処理成果のうち、契約上規律の対象とするものの定義を定める条項**

4. ベンダに提供を求めるべき情報の内容について

AI 事業者ガイドラインには、「関連するステークホルダーへの情報提供」は、提供する AI システム・サービス（「AI サービス等」）について、平易かつアクセスしやすい形で、適時かつ適切に提供すべき情報として次のものを例示しており[9)]、上記 3.1 で言及した情報提供義務に関して、具体的にいかなる情報の提供を求めるかを検討する際に参考になる。

- AI を利用しているという事実、活用している範囲、適切/不適切な使用方法等
- 委託先が利用する第三者 AI サービス/サブプロセッサの有無（名称、役割、契約形態）及び主要な取扱条件（学習利用、保持、越境移転、再委託等）
- 提供する AI サービス等の技術的特性、利用によりもたらす結果より生じる可能性のある予見可能なリスク及びその緩和策等の安全性に関する情報
- AI サービス等の学習等による出力又はプログラムの変化の可能性
- AI サービス等の動作状況に関する情報、不具合の原因及び対応状況、インシデント事例等
- AI システムの更新を行った場合の更新内容及びその理由の情報
- AI モデルにて学習するデータの収集ポリシー、学習方法、実施体制等

5. ガバナンスと説明責任に関する事項

5.1 SOP の策定と遵守

本報告書第 7 章「今後の国内向けガイダンス作成に向けた要点」において示した閉域運用および非学習・非保持の原則との関係は、上記のとおりである。

契約に定められた項目のうち、特にユーザが義務を負う事項については、PV 業務に AI を利用する CRO 等の受託事業者にも遵守させる必要がある。

このため、ユーザは、委託する PV 業務に関する SOP を策定し、これを受託事業者に提示する（又は受託事業者と協議の上で共同策定する）とともに、当該 SOP の遵守義務を委託契約において明確に定めることが考えられる。

5.2 トレーサビリティおよびバージョン管理（文書化）

トレーサビリティおよび透明性の向上の観点から、意思決定に影響を与える AI システム・サービスについて、そのシステムアーキテクチャやデータ処理プロセス等を文書化することを契約上義務付けることが考えられる [10)]。

CIOMS WG XIV の報告書 [11)]においても、AI モデルの文書化はライフサイクル全体を通じて行われるべきであり、事前計画からの逸脱の根拠や推論を含め、重要な手順および意思決定について検索可能性および再現性を確保する必要があるとされている。

また、同報告書は、厳格なトレーサビリティおよびバージョン管理の必要性に言及し、各バージョンのソースコード、基盤となるモデルアーキテクチャ、トレーニングデータセットおよびテストデータセット、性能評価結果、並びに AI モデルの展開後における継続的改善および適応に関する事項について文書化すべきであるとしている。

5.3 規約改定

汎用的 AI サービスの利用を前提とする場合、利用規約に基づいて契約が成立することが少なくない。

当該利用規約が民法上の定型約款（民法 548 条の 2）に該当する場合、インターネットの利用その他の適切な方法により周知されるときには、その変更が合理的なものである限り、ユーザの個別の同意を要することなく契約内容を変更することができる（民法 548 条の 4）。

このため、ユーザが変更内容を十分に把握しないまま契約に違反する事態が生じる可能性がある。

したがって、ユーザは利用規約の内容および変更状況を継続的に確認する必要があり、その確認手続を SOP に組み込むなど、漏れのない運用体制を整備することが望ましい。

註

1）チェックリストの「4.1 チェックリストを踏まえた対応」（同 2 4 頁）では、チェックリス

トは、AI 利活用契約で検討すべき論点例を示すもので、指摘されたリスクがあっても直ちに是正交渉や締結拒否を推奨する趣旨ではない。AI に内在するリスクは契約文言だけで完全に制御できないため、サービス内容、契約形態（規約/個別契約）、受容リスク、履行可能性、代替手段、交渉コスト、運用等による低減可能性を総合して判断することが必要である旨記載されているので参照されたい。

2) AI システムをアプリケーション、製品、既存のシステム、ビジネスプロセス等に組み込んだサービスとして AI 利用者（AI Business User）、場合によっては業務外利用者に提供する事業者（AI 事業者ガイドライン（第 1.1 版）5 頁参照）。

3) 事業活動において、AI システム又は AI サービスを利用する事業者（同 5 頁参照）。

4) インプットに個人データ（個人情報保護法上の「個人データ」）が含まれる場合、当該提供が「委託」か「第三者提供」かの整理により、本人同意の要否等が左右され得る。ベンダによる取扱いがサービス提供目的に限定され、自己目的利用（学習、統計、モデル改善等）や突合・再利用が認められないことを、契約上明確化する。

「委託」と整理する前提（例）：利用目的の限定、秘密保持、再委託管理、返却・削除、アクセス制御等が担保されるか、「第三者提供」に該当し得る要素（例）：ベンダの自己目的利用（学習・モデル改善等）、別サービスへの転用、データの突合・共同利用等が許容されていないか、個人データの種類（要配慮個人情報を含むか）、国外移転の有無、サブプロセッサの関与を把握し、必要な対応（本人同意、相当措置の確保等）を検討する。

個人情報保護法の観点から検討すべき事項は、チェックリストの「4.4　個人情報保護法に関する留意点」（同 33～38 頁）に記載されているので、参照されたい。

5) ユーザ側契約担当者がセキュリティ関連条項を検討する際に有益と考えられる着眼点が、チェックリストの「4.5　セキュリティに関する留意点」（同 39～41 頁）に記載されているので参照されたい。

6) 特に個人データのインプットについては、委託と第三者提供の区別が、個人情報保護法の規律である本人同意の有無と関連して問題になり得る。既出のチェックリストの「4.4　個人情報保護法に関する留意点」（同 33～38 頁）に記載されているので、参照されたい。

7) ベンダ又は再委託先が国外に所在する場合や、国外からインプット（個人データ）にアクセス可能な体制がある場合には、個人情報保護法上の越境移転（28 条）に係る対応が問題となり得る。サーバ所在地のみでは判断できないため、提供先・再委託先の所在国、アクセス権限、相当措置の内容等について情報提供を求め、必要な同意取得又は相当措置の確保を検討する。

8) アウトプットは不正確・不完全（いわゆるハルシネーション）、偏り、第三者の権利侵害等を含み得る。PV 判断に直接用いる場合は、最終判断を人が行い、必要に応じて根拠及び判断過程を記録する運用（SOP）を前提とする。

9) AI 事業者ガイドライン　第 1.1 版　第 4 部 AI 提供者に関する事項　P-6）ii. 関連するステークホルダーへの情報提供(同 36～37 頁)

10) AI 事業者ガイドライン第 4 部　（同 35～37 頁参照）

11) Report of the CIOMS Working Group XIV “Artificial intelligence in pharmacovigilance” “Chapter 9. Governance & Accountability” 9.3 Traceability and version control”

謝辞
本研究の実施にあたり、医薬品規制および医療データ利活用・AI に関する法的整理に関する調査・資料提供について、渥美坂井法律事務所・外国法共同事業の弁護士 越後純子氏、佐々木郁氏、三部裕幸氏に多大なるご協力を賜った。ここに記して深甚なる謝意を表する。