第 2 回　医療 AI に関連する個人情報保護法、著作権法、薬機法、AI 規制等に関する論点
(弁護士　児玉　安司)

1. 「入口」「出口」の再確認

第 2 回「医療 AI に関連する個人情報保護法、著作権法、薬機法、AI 規制等に関する論点」ということで、進めさせていただきます。まず情報科学研究者や医学研究者の人たちに、「入口」「出口」の再確認したく、昨日の法律相談でも最初に強調させていただきました。それから、著作権、情報保護、薬機法規制・AI 規制と Sandbox という順番で話します。

研究開発にあたっての入口は著作権の権利制限、裏返して言うと規制緩和が行われています。これまでの著作権法の枠組みが、大きく修正されつつあり、文化庁の 3 月 15 日報告書を踏まえると、一層大きなインパクトがあるとされています。また、医療生成 AI と個人情報保護ですが、研究開発の「入口」のほうは、「緩和方向へ？」と書いてあります。これは、研究開発で情報を使えるようにしないと、ポリティカルにはもう一歩も進めないということで、個人情報保護委員会に対しては、いろいろと政治的な動きもあるようです。それから前回紹介したような、例えばハーバードでは、患者さんの電子カルテに研究者がログインし、患者さんの名前が付いたままの電子カルテ空間の中を走り回って、AI を作成する。つまり解析のためのプログラムを電子カルテ空間に持ち込んで、そこで AI を開発していくようなことも視野に入れた、二次利用の議論が行われています。いままでの個人情報保護法のカルテの取り扱いからすると、かなり驚くような内容も含まれており、相変わらずコンサーバティブな議論もなされています。

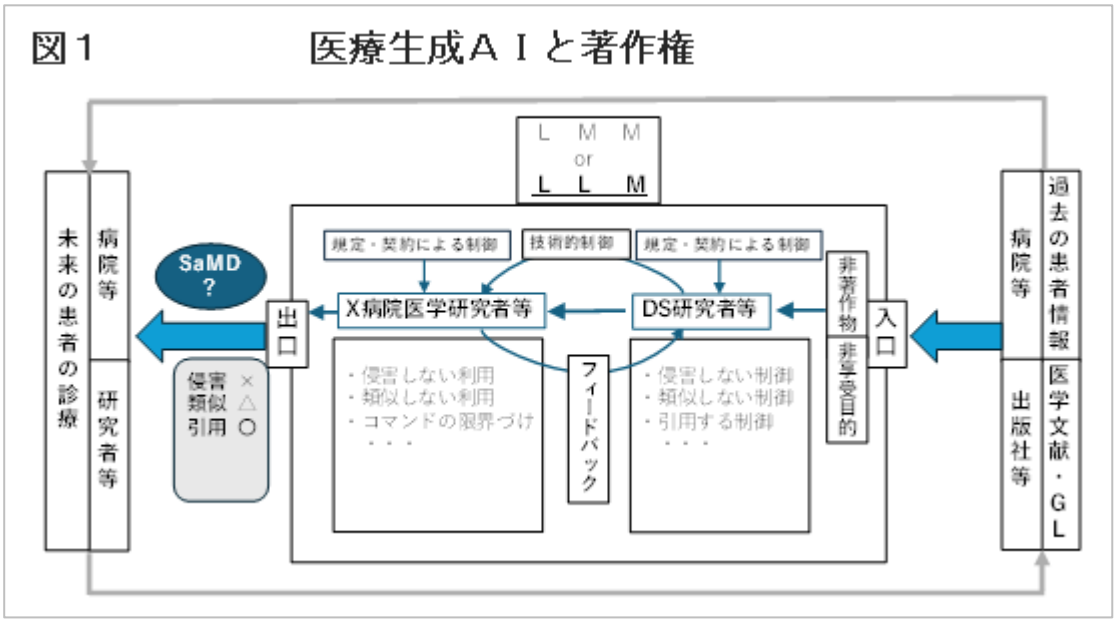
医療生成 AI と製造物責任、薬機法承認に関しては、SaMD（Software as a Medical Device）が出口になるときについては、承認の手続きも日本でもだいぶ安定してきております。しかし、LLM、LMM がオープン化されたり、商用化されたりする状況については、実際に医療現場で使われるとなると、AI as Medical Device という捉え方も十分あり得ます。何しろ日本では医療 AI そのものをいまここで作っている最中なので、規制についての議論はまだこれからで、課題が多いということになります。

テーマ	論点	
医療生成AIと著作権	• 研究開発の「入口」は規制緩和 →著作権法30条の4、47条の5 →文化庁文化審議会著作権分科会法制度小委員会令和6年3月15日 「AIと著作権に関する考え方について」 • 課題は「出口」の制御	図1参照
医療生成AIと個人情報保護	• 研究開発の「入口」は緩和方向へ？「2次利用」の拡大への期待 • 社会実装の「出口」についても規制あり →Cf.個人情報保護委員会　令和5年6月2日 行政指導 「生成AIサービスの利用に関する注意喚起等について」	図2参照
医療生成AIと製造物責任（薬機法の承認）	• SaMDを「出口」とするときには、手続が安定し始めた →厚生労働省医薬生活衛生局　令和5年3月31日 「プログラムの医療機器該当性に関するガイドラインの一部改正について」 • LLM, LMMを「出口」とするときは、これからの課題が多い	図3参照

1-1.　医療生成 AI と著作権

AI と著作権に関しては、非著作物としての病院の患者情報、そして医学文献やガイドラインについては、非享受目的のため、機械学習の対象として問題ないということです。法律相談の議論でも随分ありましたが、クローリングの結果も含めて、入ってきたものが出口から同じ形で出ていってしまうことが起こると、複製権の侵害にもなり得ることがあります。そのため、入口の非享受目的というのは、それをどう使い、何を出口とするのか、LLM/LMM の設計段階で何を目的としどのような出力の制御をするのか、具体的に話を伺わないと答えが出にくいのです。

一方でSaMDですと、ソフトウェアとして、「あなたはいま血糖値が高いので、こんなふうにしたほうがいいですよ」などのリアクションが返ってくるようなアルゴリズムを組むという話なので、いま既に売られている医療機器 SaMD については、そのまま文献の表現出てくるような懸念は、あまりないようなかたちで製造販売されています。医療生成 AI と著作権については、文化庁文化審議会著作権分科会法制度小委員会の令和6年 3 月 15 日「AI と著作権に関する考え方について」が最新の整理となっています。法律的にどのように要件論が議論されているか、ただし書きの射程がどのようになるのか、それが実際に非享受利用をするときの契約書にどう響いてくるのかというようなことも、検討課題になります。

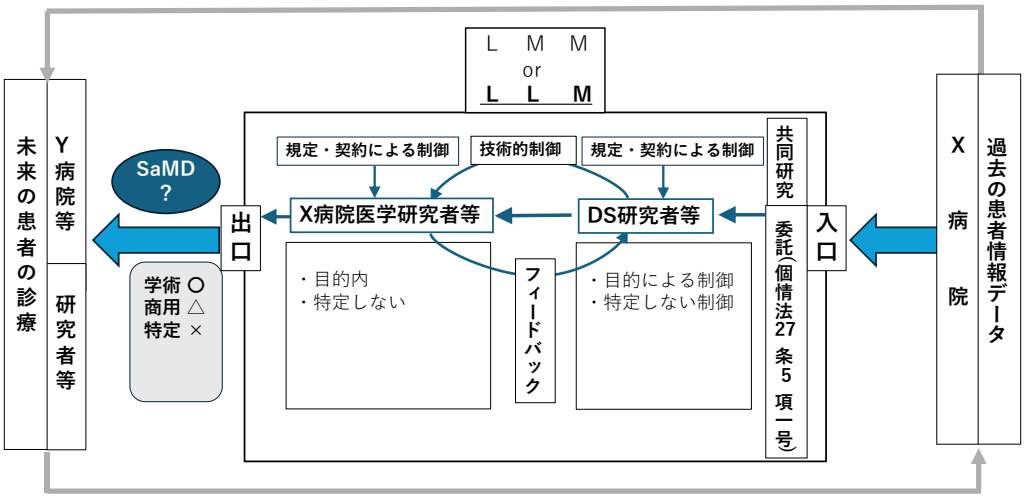


1-2.　生成 AI と個人情報保護

個人情報保護法 27 条 2 項五号六号七号に基づき学術研究例外として共同研究を行うこともあります、過去の患者情報データを「委託」形式で情報解析したり、「共同利用」を行うこともありえます。研究グループは、症例報告をデータベース化し、AI 開発に活用しています。特に、診断支援 AI や画像診断支援 AI の研究が進行中です。かかり

つけ医の支援や、放射線学会との連携も進められています。個人情報保護法の厳しい規制下で、倫理委員会の承認を得た枠組みでプロジェクトが進行しています。

図２　　生成ＡＩと個人情報保護



1-3.　生成 AI と製造物責任

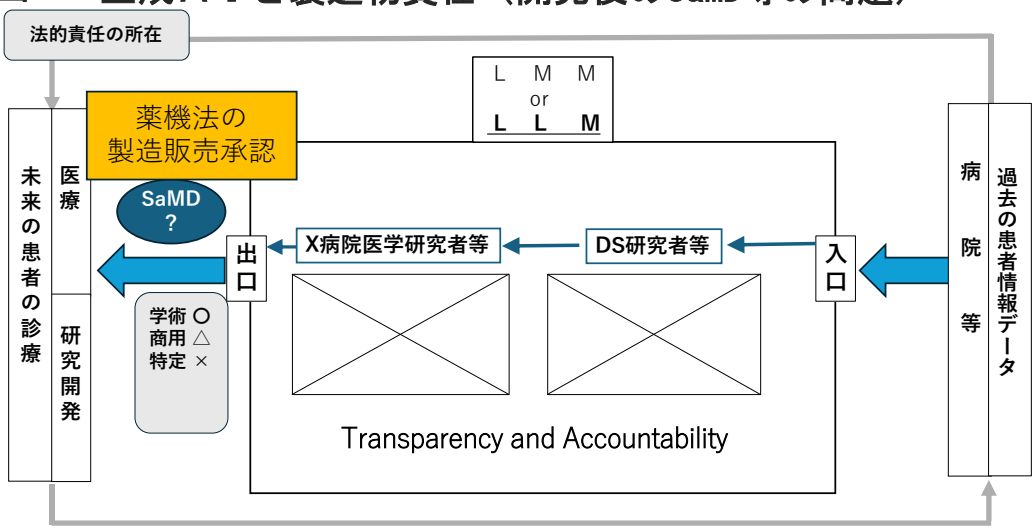
薬機法の製造販売承認については、令和 5 年 3 月 31 日の「プログラム医療機器該当性に関するガイドラインの一部改正について」において、規制当局が、SaMD について、どのような範囲で規制しようとしているかが記載されています。

もともと「文化的所産の公正な利用（著作権法 1 条に掲げた著作権法の理念の一つ）に配慮して、一定の場合に著作権者の許諾なく著作物を利用できることとする規定」が、著作権法の権利制限規定として並んでいて、「私的利用のための複製」、「引用」、「試験問題としての複製」、「裁判手続き等における複製」などが知られています。著作権法 30 条の 4、第 47 条の 4 及び 5 が作られたあと、令和元年 10 月 24 日、文化庁著作権課が、「現在我が国では、IoT・ビッグデータ・人工知能等の『第 4 次産業革命』に関する技術を活用したイノベーションの創出が期待されているところ、改正前の著作権法の権利制限規定には、法律上の要件が一定程度具体的に定められているものが多く、その要件から外れるような新たな利用方法が生まれた場合には、実質的には権

利者の利益を害しないような利用であっても、その権利制限規定の適用を受けられずに著作権侵害となるおそれが指摘されてきた」と。旧来の著作権による制限の緩和が必要だということで、非享受目的でコンピューターに読ませる、機械学習をさせる、あるいはGoogleで検索するというのは全部を享受しているのではなく、軽微利用だというような新たな条文ができたわけです。

今回（「令和6年3月15日文化庁『AIと著作権に関する考え方について』」）の考え方では、「技術革新により大量の情報を収集し、利用することが可能となる中で、イノベーション創出等の促進に資するものとして、社会の変化に対応できるようにするため、著作物の市場に大きな影響を与えないものについて個々の許諾を不要とする規定が新設された」とありますが、ここに「市場」という言葉が出てきています。例えばX書店が内科学の本を出していて、その中に敗血症についての記載があるとします。X書店の内科学の本を買わなくても、それをAIが学習したAIができてしまうと、マーケットは交錯するかもしれないし、書籍の売上も減るかもしれません。独禁法の議論で出てくるいわゆるcontestable market、マーケットで本当に競争関係になるのか、書籍とＡＩが本当に市場で競争相手になるのかというような発想は、「法と経済学 law and economics」を研究分野とする人にとっては非常に聞き慣れた発想です。「著作物の市場に大きな影響を当てないものについて個々の許諾を不要とする規定が新設された」、「AI の学習用データの収集・加工等の場面において、既存の著作物の利用が生じ得ることから、AI 開発の学習、情報解析の用に供するための著作権の利用に関して、著作権の制限を規定する」という発想が生まれます。

図３　生成ＡＩと製造物責任（開発後のSaMD等の問題）



2. 医療生成 AI と著作権

2-1. フェア・ユースと AI 開発の関係

US には「フェア・ユース」という法的概念があります。概括的なフェア・ユースがあることで、アメリカのほうが、AI 開発に関してはより容易なのではないかとも思えますが、実際には、日本の著作権法 30 条の 4 よりも実体的な制約があり、New York Times, Microsoft, Open AI のような訴訟が多数起こっています。EU の側は、EU デジタル単一市場における著作権指令の第 3 条に「学術研究目的」の規定があり、EU の法律でも学術研究目的の枠の中にいるあいだは大丈夫だととりあえず申し上げられると思います。

もう一つ、第 4 条「テキスト及びデータマイニングのための例外または制限」では、「第 1 項に従って行われた複製および抽出は、テキストおよびデータマイニングの目的に必要な期間、保持することができる」などの規定があります。データマイニングは、もう学術研究にとって必須です。学術研究の外側で、商用といわれるビジネスの

分野でも、データマイングをやらなければもう仕事はできないというような時代の中で、EU もが著作権に関してこのような規定を置いています。

US フェアユース （一般的著作権制限規定）	第107条（一部省略） ➢ **批評、解説、ニュース報道、教授、研究または調査等を目的**とする著作権のある著作物のフェア・ユースは、著作権の侵害とならない。著作物の使用がフェア・ユースとなるか否かを判断する場合に考慮すべき要素は、以下のものを含む (1) 使用の目的および性質（使用が**商業性**を有するかまたは**非営利的教育目的**かを含む） (2) 著作権のある**著作物の性質** (3) 著作権のある**著作物全体との関連**における使用された部分の**量**および**実質性** (4) 著作権のある著作物の潜在的市場または**価値に対する使用の影響**

2-2. 日本の個人情報保護法

旧法	平成２７年改正法	令和３年改正法
第一条 この法律は、**高度情報通信社会の進展**に伴い**個人情報の利用が著しく拡大**していることにかんがみ、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共 団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等 を定めることにより、**個人情報の有用性に配慮しつつ、個人の権利利益を保護**すること を目的とする。	第一条 この法律は、高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、**個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであること**その他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。	第一条 この法律は、**デジタル社会の進展**に伴い個人情報の利用が著しく拡大していることに鑑み、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにし、**個人情報を取り扱う事業者及び行政機関等についてこれらの特性に応じて遵守すべき義務等を定めるとともに、個人情報保護委員会を設置することにより、行政機関等の事務及び事業の適正かつ円滑な運営を図り、並びに個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮**しつつ、個人の権利利益を保護することを目的とする

最初に 2004 年に施行された時は、「個人情報の有用性に配慮しつつ、個人の権威利益を保護する」という表現でした。医療現場などでは同意を得なければ個人の情報を絶対に外に出さないということについて過剰反応が起こり、警察が捜査として任意で患者の情報を求めたら、令状を持ってこなければ何も教えないというような事象が起こりました。厚生労働省が、そういう過剰反応を戒める通知を出すような状況になりました。

平成 27 年改正法では、同意を取らない限り個人情報を利活用できないということを強調し過ぎないように、「個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性」という文言が追加され、利活用の促進を強調しました。

さらに、令和 3 年改正法では、最初に「デジタル社会の進展に伴い」という言葉が追加されました。それから、行政個情法との統合がおこなわれたので、この青字の部分が増えました。あとの「個人情報の適正かつ効果的な活用が…」と続く部分は、平成 27 年改正法と同じです。個人情報保護に関する法律では、第 4 章「個人情報取扱事業者の義務等」で、個人情報を取り扱う事業者は、病院からさまざまなところが規制されていました。

個人情報保護法 20 条は、医療情報を含む要配慮個人情報の取得の段階、まさに入口規制で、「あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない」という、いわゆる事前の同意原則の入口規制がかかっています。しかし、20 条 2 項五号、六号で、「当該個人情報取扱事業者が学術研究機関等である場合」、主体が学術研究機関であり個人情報の利用目的が「学術研究目的」（一部でもよい）の場合は、「個人の権利利益を不当に侵害するおそれがある場合」を除いて、要配慮個人情報の取扱いについては同意不要とする規定が令和 3 年改正法で置かれました。

27 条 1 項の「第三者提供」についても、同じく、学術研究機関が個人情報を受け取る場合、学術研究機関が出す場合、成果を公表する場合などについては、第三者提供における同意原則が除外されています。学術研究機関とは何かという定義を個人情報保

護委員会のＱ＆Ａで公表するに当たり、議論がありました。医学研究というのは大学だけでやっているものではなく、市中の病院であっても病院は、個人情報取扱事業者としての医療機関であると同時に、日本最大級の医学研究機関でもある事例が多々あります。ところが、個人情報保護委員会は、ここで言う学術研究機関に該当するのは、国立がんセンター、国立国際医療センター、国立循環器センター、国立長寿医療センターなどのいわゆるナショナルセンターと大学だけで、一般病院には学術研究機関のこの例外規定が適用されないという解釈をQ&Aで当初出しました。その結果、著名な大病院が要配慮個人情報の取得、共同研究、研究発表をするに当たって、同意原則の法規制が外れなくなってしまいました。

一方、個人情報保護法の20条2項三号、公衆衛生例外というものがありまして、公衆衛生の向上や児童健全育成の目的で、同意取得が著しく困難な場合は、同意がなくてもよいという「公衆衛生例外」で学術研究をやるのであれば、同意原則の例外とするということに、当初はなりました。

個人情報保護法27条5項では、「委託」「共同利用」という二つの第三者提供の例外を定めています。例えば、病院が個人情報に関連してデータサイエンスの学術研究をする人や機関に委託をする場合は、第三者提供にはならないので事前の同意原則がはずれます。

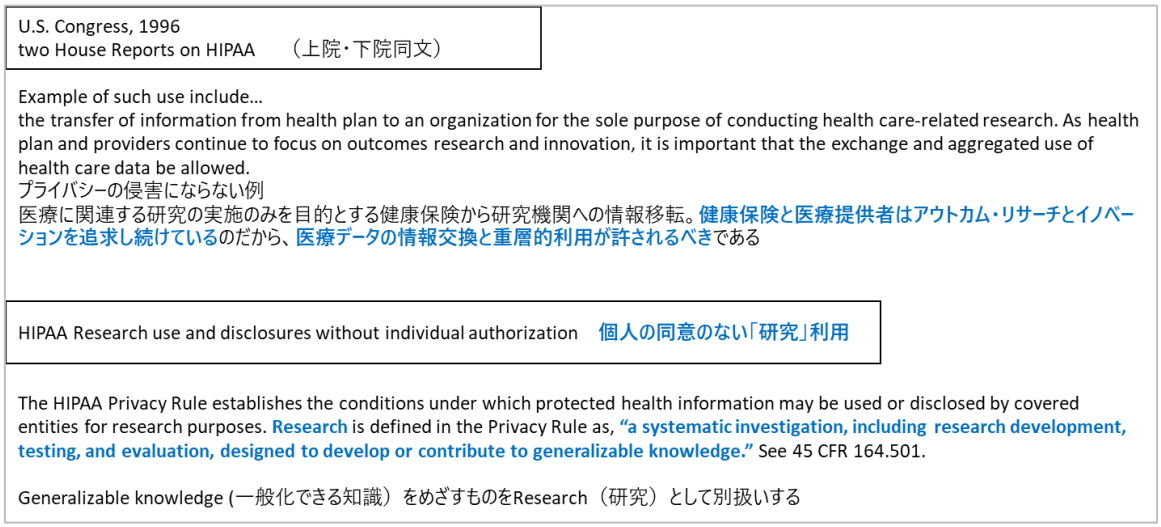
「共同利用」については、また機会があったらお話ししますが、例えば有力な医師のところに製薬企業から医薬品の情報をお届けしたいというMR活動のニーズがあります。大規模な医療機関の幹部となる医師の出身大学情報や所属機関情報などを一手に集めているデータベースがあります。二百社をこえる医薬品・医療機器企業等の共同利用ということで、代表者、会員、使用目的などをインターネット上に掲載して、27条5項三号の用件を満たすようにしています。これによって、会員企業間の個人情報の共有は第三者提供ではなく「共同利用」となります。

2-3. US HIPAA との比較

アメリカの HIPAA では、プライバシー侵害にならない例として、research が広く認められています。例えば心臓病の研究をしているので、心臓病が心電図からどのように診断にできるかというような generalizable knowledge（一般化できる知識）を目指すものはリサーチであって、別扱いにするという「リサーチ例外」が認められているのです。

アメリカでは、病院の IRB（研究審査委員会）または Privacy Board が、approve a waiver of authorization、つまり患者の同意を免除するという approval を与えたときには、患者の同意が不要になるというやり方をしています。各国でいろいろな工夫があり、健康保険証を提示して健康保険で診療を受けている以上、医療情報は全部研究目的で使ってよいとする国もあります。薬の副作用調査などについても活用されています。薬を処方されて飲んでいる人のそのあとの健康保険の履歴を見ていけば、どんな副作用が出てくるかというのはビッグデータ（RWD: Real World Data）で速やかに検出でき仮説がたてられる、というようなやり方が、例えばフランスなどでもおこなわれています。今、日本で、医薬品の副作用やファーマコビジランスについて論文ベース、治験ベースでいろいろ検討されているものを、健康保険を軸にした公的データベースで、少なくとも仮説をたてるところまでは、やってしまおうというような国は、ヨーロッパにも多々あります。アメはもともと、各病院の IRB や Privacy Board が認めれば患者の同意は不要で、その代わり identifiers の protect とか destroy とか、患者保護のための手続きは必要であることが記載されています。欧米で COVID-19 の治療薬やワクチンの研究などが爆発的な速度で進むときには、このリサーチに関する同意原則の例外が大変大きな力を発揮しました。日本では、公衆衛生例外の条文で、「特に必要」「同意を得るのが困難」というような要件の議論をしているうちに、世界の主要

な雑誌に掲載された論文ゼロ、ワクチンゼロ、というような国際競争の中での立ち遅れの原因になっています。



2-4. EU GDPR との比較

EU の GDPR について、日本では令和 3 年改正法で、個人情報保護法の適用除外から学問の自由は除かれてしまいました。個人情報保護委員会は、学問の自由における個人情報保護の緻密化と説明しています。GDPR85 条は、情報伝達の自由とデータ保護の調和を各国法で保つため「報道、学術、芸術、文学の目的のために行われる取り扱いに関し、GDPR のさまざまな規制について各国法で「例外や特例を定めなければならない」という義務規定を置いています。同意なく個人情報が取り扱われる場合の典型が GDPR の Article 9 Processing of special categories of personal data の 2（h）項で、「EU 法又は加盟国の国内法に基づき、又は、医療専門家との契約により、かつ、第 3 項に定める条件及び保護措置に従い、予防医学若しくは産業医学の目的のために、労働者の業務遂行能力の評価、医療上の診断、医療若しくは社会福祉又は治療の提供、又は、医療制度若しくは社会福祉制度及びそのサービス提供の管理のために取扱いが必要となる場合」としています。日本法は、同意がまず原則としてあって、同意を得るのが困難な場合の例外を定めるという立て付けになっています。これに対して

GDPR では、9 条の 2（a）項が同意原則、これと並列で（h）項に要は医療に必要だということであれば同意不要という例外規定が置かれています。

（h）項は医療専門家（i）項には「医療及び医薬品若しくは医療機器の高い水準の品質及び安全性を確保することのような」、これを「公衆衛生」と言っているのですが、「公衆衛生の分野において、公共の利益を理由とする取扱いが必要となる場合」とあります。日本では、学術というのは大学であると。医薬品メーカーが研究をしているのは、商用である。医薬品や医療機器の向上というのは学術例外には当たらず、公衆衛生でもないという扱いをされています。しかし、GDPR は、医薬品・医療機器の水準、品質や安全性の確保のために研究開発を行うこと自体が公衆衛生であり、公共の利益だということを規定に明文化し、同意と並ぶ個人情報取り扱いの原則として定めています。医師が取得した「私」の情報を研究に使うかどうかは「私」の同意にかかっているのだという考え方ではなく、「私」の情報が、例えば診断技術や治療法の改善、医薬品の効果・副作用などの「公共の目的」のための調査に使われるということは国民全体の reasonable expectations（合理的な期待）なので、その法的根拠を提供しなければならないということが前文（47）に記載されています。

そして、科学的研究、公共の利益における保管の目的、統計、歴史的研究などについて当初の目的を超える「追加的取扱い」。例えば、病院に自分の病気を治してもらうために行き、「追加的取扱い」としてそれを統計的なエヴィデンスを構成する研究に使うということは、問題ないというのが GDPR の立場です。Without consent で使えるものの代表が public health（公衆衛生）です。二次利用について、「公益」という言葉でなんとなく商業利用を排除する空気感があるのですが、GDPR は、公衆衛生とは「健康に関する全ての要素、換言すると、健康状態のこととして解釈されなければならない」と、普通考える public health よりかなり広い定義の仕方をしているので、後ろの条文の公衆衛生例外も、かなり広い意味と解釈されるべきと思われます。

該当箇所	内容
GDPR （27 April 2016） 前文（47）	The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. 個人データの開示を受けうる管理者の正当な利益を含め、管理者又は第三者の正当な利益は、データ主体と管理者との関係に基づくデータ主体の合理的な期待を考慮に入れた上で、データ主体の利益又は基本的な権利及び自由を覆すものとならない場合に、取扱いのための法的根拠を提供しうる
GDPR （27 April 2016） 前文（54）	The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC)No 1338/2008 of the European Parliament and of the Council, namely all elements related to health, namely health status,including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. 特別な種類の個人データの取扱いは、データ主体の同意なしに、公衆衛生の分野における公共の利益を理由として、必要となることがある。そのような取扱いは、自然人の権利及び自由を保護するための適切かつ具体的な措置に服するものでなければならない。この文脈において、「公衆衛生」とは、欧州議会及び理事会の規則 No 1338/2008に定義されているように、すなわち、健康に関する全ての要素、換言すると、健康状態のこととして解釈されなければならない。それは、疾病率及び障害、健康状態に影響を与える素因、医療の必要性、医療に割り当てられる資源、医療の提供及び医療へのユニバーサルアクセス、並びに、医療の支出及び資金手当、そして、死亡原因を含む

3. 医療生成 AI と個人情報保護

生成 AI についての注意喚起としては、令和 5 年 6 月 2 日、ChatGPT の流行に伴って、クエリーの入力によって個人データが出てこないように、きちんと防止措置をせよという個人情報保護委員会の行政指導が行われ、これはマスコミ等でも大々的に報じられました。

米国の AI 規制では、やはり AI は野放しというわけにもいかないということで、大統領令で何かやろうとしているのですが、やはり産業発展その他を考えると厳しい規制がなかなかやりにくいということです。ただ、カリフォルニア州の消費者プライバシー保護法制の中では、AI 関連法案が、つい直近で、次々に通り始めている状況のようです。

日本の生成AIサービスの利用に関する注意喚起について
令和5年6月2日　個人情報保護委員会

（１） 個人情報取扱事業者における注意点
① 個人情報取扱事業者が生成 AI サービスに個人情報を含むプロンプトを入力する場合には、特定された当該個人情報の利用目的を達成するために必要な範囲内であることを十分に確認すること
② 個人情報取扱事業者が、あらかじめ本人の同意を得ることなく生成 AI サービスに個人データを含むプロンプトを入力し、当該個人データが当該プロンプトに対する応答結果の出力以外の目的で取り扱われる場合、当該個人情報取扱事業者は個人情報保護法の規定に違反することとなる可能性がある。そのため、このようなプロンプトの入力を行う場合には、当該生成 AI サービスを提供する事業者が、当該個人データを機械学習に利用しないこと等を十分に確認すること

米国のAI規制（2024年5月時点）①連邦政府

JETRO2024年5月1日付地域・分析レポート＊
「**AI規制に大統領令で先手（米国）**」、
「議会は法整備に動くも**一致点を見いだせず**」

大統領令 ＝連邦政府機関への命令（Executive order）
2023.10　Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

米国のAI規制（2024年5月時点）②州政府

例　カリフォルニア州
１)消費者プライバシー保護法制
- CCPA：California Consumer Privacy Act（2021年成立）

２)さらなるAI関連法案が上院を通過(2024.5)
- California Artificial Intelligence Transparency Act (SB 942)
- Artificial Intelligence Accountability Act(SB 896)
- Safe and Secure Innovation for Frontier Artificial Intelligence Models Act(SB 1047)

EU の AI 規制は、リスクベースアプローチで、リスクの大きさごとに 4 段階で規制をする EU AI Act が 2024 年 5 月 22 日に成立しています。Chapter VI「イノベーション支援」に各国政府の規制サンドボックス開発・提供義務等というところがあり、原則リスクベースアプローチではありますが、規制サンドボックスという大きな例外を設けています。例えば、フランスの CNIL などでは、既に 2021 年から規制サンドボックスを実際に運用して、優良な医療 AI 開発を促進・支援しています。

EUのAI規制（2024年5月時点）

2024年5月　**EU AI Act**が成立
- AIシステム,汎用型AIモデル, 提供者(Providers), 利用者(Deployers)等を定義

- リスクベースアプローチ（4段階のリスク分類と規制方法）
  - ①Unacceptable Risk　→禁止
  - ②High Risk　→事前/事後の厳格規制
  - ③Limited Risk　→Transparency Requirements（透明性）
  - ④Minimal Risk　→特に規制なし

- 域外適用（EU圏外の者であっても、EU内で利用されるアウトプットの生成に係る提供者や利用者には適用される）
- **イノベーション支援(ChapterVI)**…各国政府の規制サンドボックスの開発・提供義務等

併せてThe European AI Officeを欧州委員会内に設置(2024)
…加盟各国政府を支援し、AIガバナンスシステムの一体性を確保

4. 医療生成 AI と薬機法規制・AI 規制と Sandbox

SaMD（Software as a Medical Device、ソフトウェア医療機器）とは、医療機器として単独で機能するソフトウェアを指します。ハードウェアを伴わない純粋なソフトウェアでありながら、診断や治療、モニタリングに用いられるため、医療分野での AI 技術の発展とともに注目されています。特に AI を用いた SaMD は、診断補助や治療計画の作成、病状予測など、医療従事者を支援する多岐にわたる役割を果たすことが期待されています。しかし、こうしたソフトウェアが医療機器として承認され、実際に医療現場で使用されるためには、規制上の枠組みに基づく厳密な審査が必要です。

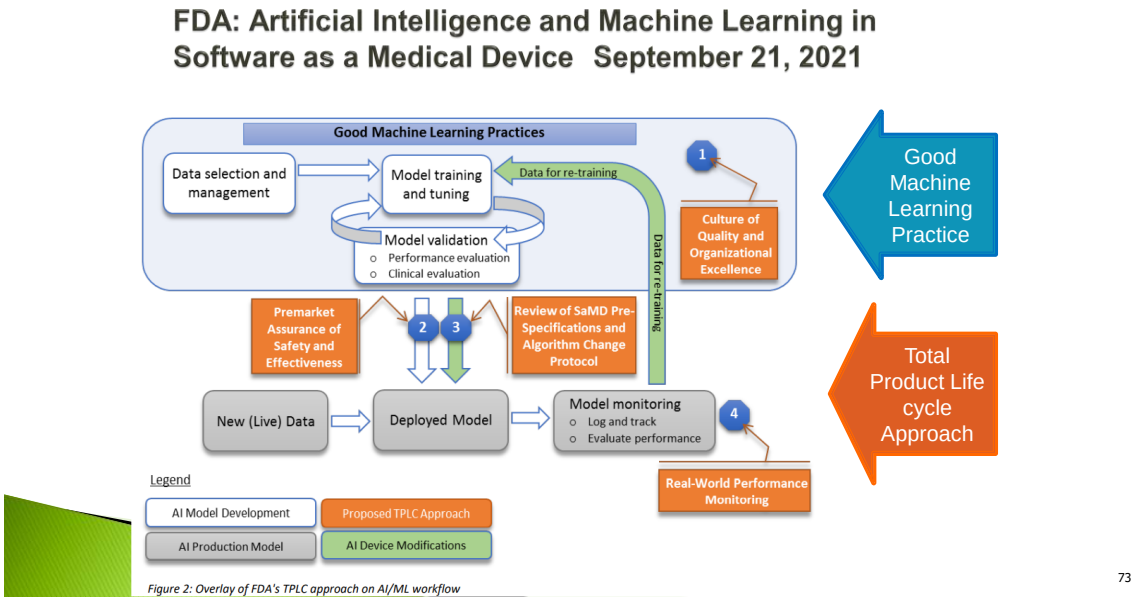
まず、SaMD の規制に関して、国際的には IMDRF（International Medical Device Regulators Forum）が基準の策定に重要な役割を果たしています。IMDRF は、SaMD の定義やリスク分類を行い、各国の規制当局がこの基準を参考にしています。IMDRF では、SaMD がその機能に基づいてリスクを評価され、診断や治療に直接関与するかどうか、患者に与える影響の大きさなどに基づき、低リスクから高リスクまでのクラス分けが行われます。リスクが高いと判断されたソフトウェアは、より厳しい審査を受け、臨床試験が要求される場合もあります。

日本においても、SaMD は薬機法（薬事法）に基づいて規制されており、厚生労働省が承認手続を行っています。薬機法では、医療機器としての SaMD の機能やリスクに基づき、各製品が適切に分類され、承認プロセスが定められています。特に AI を用いた SaMD は、リアルワールドのデータを解析し、診断結果や治療法を提案するため、そのアルゴリズムの透明性や安全性が重要視されます。AI の判断が誤った場合、患者の治療に悪影響を与える可能性があるため、開発者はソフトウェアの検証を徹底し、信頼性の高いデータを用いることが求められます。

さらに、SaMD の特性として、ソフトウェアがアップデートを繰り返すことによるリスクも考慮しなければなりません。AI 技術を用いる SaMD では、学習データが追加されることでアルゴリズムが進化し、診断精度が向上することが期待されますが、同時に新たなバグや不具合が生じるリスクもあります。そのため、アップデート後のソフトウェアが再び医療機器として承認されるべきか、あるいはどの程度の変更なら承認を必要としないかについても、明確な基準が必要です。日本の薬機法では、重大な変更が行われた場合は再承認が必要ですが、軽微な変更の場合は届出だけで済むことがあります。AI 技術を用いた SaMD は、常に進化する技術であるため、この区分がますます重要になります。

また、SaMD の規制においては、データのセキュリティも大きな問題となります。SaMD は患者の診療データや医療情報を扱うため、これらの情報が不正にアクセスされたり、漏洩したりするリスクが常に伴います。特に、AI を用いた SaMD では、クラウド上でのデータ処理が行われることが多く、遠隔操作やデータ共有が必要となるため、サイバーセキュリティ対策が不可欠です。開発者は、セキュリティに配慮したソフトウェア設計を行い、外部からの攻撃を防ぐための防御策を講じる必要があります。GDPR などのデータ保護規制が厳しくなる中で、SaMD がどのように個人情報を保護するかも、重要な規制ポイントとなっています。

加えて、SaMD の利用には倫理的な課題も伴います。AI 技術が診断や治療に関与する場合、その結果に対する責任の所在が曖昧になることがあります。例えば、AI が誤った診断を下した場合、その責任がソフトウェアの開発者にあるのか、医療従事者にあるのか、あるいはその両方なのかが不明確になることがあります。このため、SaMD の運用には、開発者と医療従事者の間での責任の分担や、AI による診断の補助的な位置づけを明確にするためのガイドラインが求められます。



前回、少しお見せしましたが、SaMD を作る時の Good Machine Learning Practice と、AI が外に出て育ち続ける Total Product Life cycle Approach を組み合わせようというのが、アメリカの FDA の考え方です。

EU の AI Act には、59 条 1 項（a）（i）Regulatory Sandbox for Public Health という条項があります。これは“public safety and public health, including disease detection, diagnosis, prevention, control and treatment and improvement of health care systems”、要するに医療システムの開発や治療法、診断法等々については、いわゆる規制サンドボックスで規制を外してやらせてみるということが認められています。

●§59　1．(a)（ｉ）Regulatory Sandbox　for Public Health

Further processing of personal data for developing certain AI systems
in the public interest in the AI regulatory sandbox
1.Personal data lawfully collected for other purposes may be processed in an AI regulatory sandbox solely for the purpose of developing, training and testing certain AI systems in the sandbox when all of the following conditions are met:
(a)　AI systems shall be developed for safeguarding substantial public interest by a public authority or another natural or legal person and in one or more of the following areas:
(i) **public safety and public health, including disease detection, diagnosis prevention, control and treatment and improvement of health care systems;**
(ii)　・・・

●§５７　Regulatory Sandbox

Member States shall ensure that their competent authorities establish at least one AI regulatory sandbox at national level, which shall be operational by … [24 months from the date of entry into force of this Regulation]. That sandbox may also be established jointly with the competent authorities of one or more other Member States. The Commission may provide technical support, advice and tools for the establishment and operation of AI regulatory sandboxes.
The obligation under the first subparagraph may also be fulfilled by participating in an existing sandbox in so far as that participation provides an equivalent level of national coverage for the participating Member States.

次に Regulatory Sandbox については、AI Act79 条にご覧のような定義があります。日本語で簡単に言うと、内閣官房は「規制のサンドボックス制度とは」「新たな技術の実用化や、プラットフォーマー型ビジネスシェアリングエコノミーなどの新たなビジネスモデルの実施が現行規制との関係で困難である場合に、新しい技術やビジネスモデルの社会実装に向け、事業者の申請に基づき、規制官庁の認定を受けた実証を行い、実証により得られた情報やデータを用いて規制の見直しに繋げていく制度です」としています。サンドボックスというのはご存じのとおり砂場です。爆発物を処理するときに砂場でボンと爆発させます。医療に関連する AI の研究・利活用は、何かあっても大丈夫なように砂場に置くという administrative sandbox の典型的な対象となるように思われます。

●**規制のサンドボックス制度　（内閣官房）**

規制のサンドボックス制度とは、IoT、ブロックチェーン、ロボット等の新たな技術の実用化や、プラットフォーマー型ビジネス、シェアリングエコノミーなどの新たなビジネスモデルの実施が、現行規制との関係で困難である場合に、新しい技術やビジネスモデルの社会実装に向け、事業者の申請に基づき、規制官庁の認定を受けた実証を行い、実証により得られた情報やデータを用いて規制の見直しに繋げていく制度です

●**EU AI Act　Recital (64)**

・・・For example, machinery or medical devices products incorporating an AI system might present risks not addressed by the essential health and safety requirements set out in the relevant Union harmonised legislation, as that sectoral law does not deal with risks specific to AI systems. This calls for a simultaneous and complementary application of the various legislative acts. To ensure consistency and to avoid an unnecessary administrative burden and unnecessary costs, providers of a product that contains one or more high-risk AI system, to which the requirements of this Regulation and of the Union harmonisation legislation based on the New Legislative Framework and listed in an annex to this Regulation apply, should have flexibility with regard to operational decisions on how to ensure compliance of a product that contains one or more AI systems with all the applicable requirements of that Union harmonised legislation in an optimal manner.

日本のAI事業者ガイドライン（第1.0版）
⇒医療に特化した規定はみあたらない

最後に日本の AI 事業者ガイドライン（第 1.0 版）は、諸外国の原則的なところだけ翻訳して、そこで皆さん力尽きてしまうので、医療の例外のところまでなかなか紹介してくれません。アメリカやヨーロッパでは、GDPR ではこうと繰り返されることが日本の医療の規制を強めるほうにばかり働いているのは、医療のところまで検討が及んでいないことが理由ではないかと、私は常々思っています。

以上のような話を共有しつつ、次回、AI と著作権のお話をもう少し深掘りしていただき、次々回、EU の AI Act と Europe Health Data Space（EHDS）などの状況を紹介していただくと、日本の規制が過剰規制になっていて、実際に国際競争力を落とし続けてきた経過が少し見えてくるかもしれません。SIP そのものもなかなか微妙な立ち位置で、これは学術である上、社会実装につなげていくという、国のプロジェクトなのです。立法への提言もこの ELSI チームの役割でありますので、きちんと各国の法規制の実際の条文を見ながら進めていきたいと思っています。