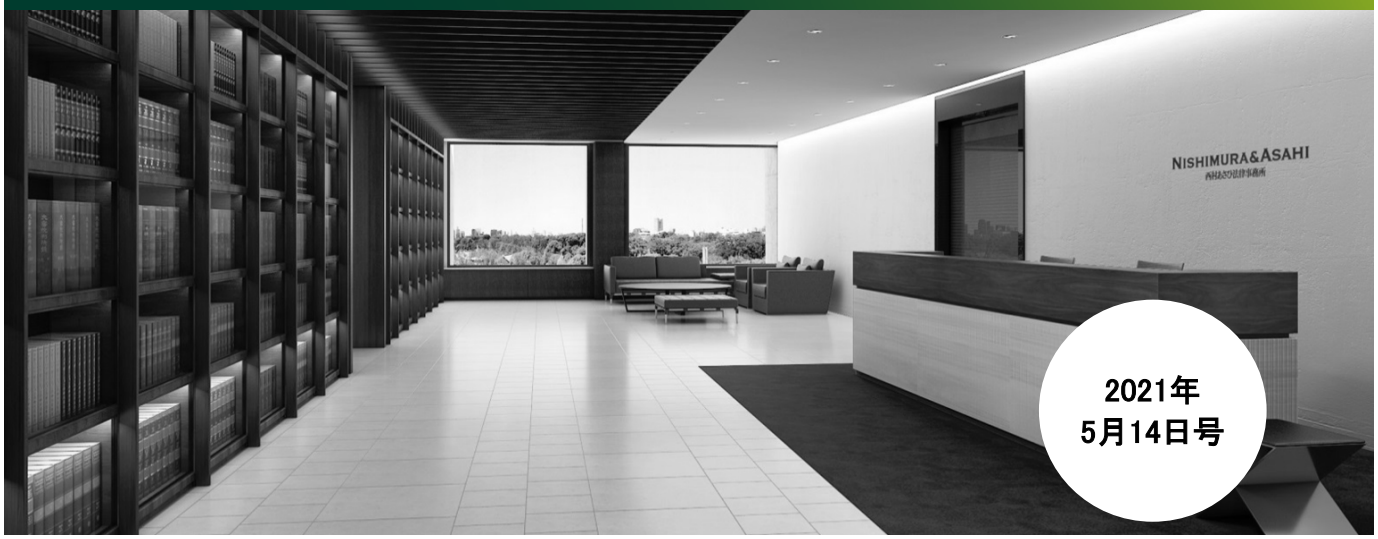
西村あさひ法律事務所
NISHIMURA & ASAHI
ヨーロッパニューズレター



欧州委員会による AI に関する規則案の公表

執筆者:木津 嘉之、角田 龍哉、戸田 相

1. AI に関する規則案の公表

欧州委員会は、2021 年 4 月 21 日、2020 年 2 月 19 日に公表していた「White Paper on Artificial Intelligence: a European approach to excellence and trust」(いわゆる AI 白書)[1]の内容を法規制案(条文)の形に落とし込んだ、「Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)」(以下「本 AI 規則案」という。)[2]を公表した。

本 AI 規則案は、EU 市場に上市され、利用される AI システムが、安全で、基本権及び EU の価値観に関する既存の法令を尊重したものとなることを確保すること等を目的として提案されたもので、欧州委員会は、今後の査読会を経て、2022 年後半に発効することを目指している。同規則案は、今後、AI システム関連の商品役務を提供・利用する日本企業にも適用される可能性があり、また、一般データ保護規則(GDPR)や、プラットフォーム規制等と同様、今後、AI システムに関する規制枠組みを巡る国際的な議論に大きなインパクトを与え、日本の法政策にも影響を及ぼす可能性がある。

そこで、以下では、本 AI 規則案が定める適用範囲、義務内容、及び制裁の概要を解説し、今後の展望や日本への示唆を説明する。

2. 適用範囲

本 AI 規則案は、主に、一定の技術[3]の組み合わせによって開発され、かつ、人間が定義した目的の下で、コンテンツ、予測、推奨又は一定の決定といったアウトプットを生成できるソフトウェアである「AI システム」[4]の提供者又は利用者のうち、以下に該当する者に適用される(前文(11)項、2 条 1 項、3 条(1)・(2)・(4)号、Annex I)。ただし、本 AI 規則案は、軍事用途のためだけに開発又は

1 https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

2 https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=75788、https://ec.europa.eu/newsroom/dae/redirection/document/75789

3 ディープラーニングを含む機械学習アプローチ、論理・知識ベースのアプローチ、統計学的アプローチが列挙されている(Annex I)。

4 AI システムを使った仲介サービスの責任範囲については、別途、電子商取引指令(又は Digital Services Act)が規律する(2 条 5 項)。

利用される AI システムや、国際協定に基づく法執行には適用されない(2 条 3 項・4 項)。

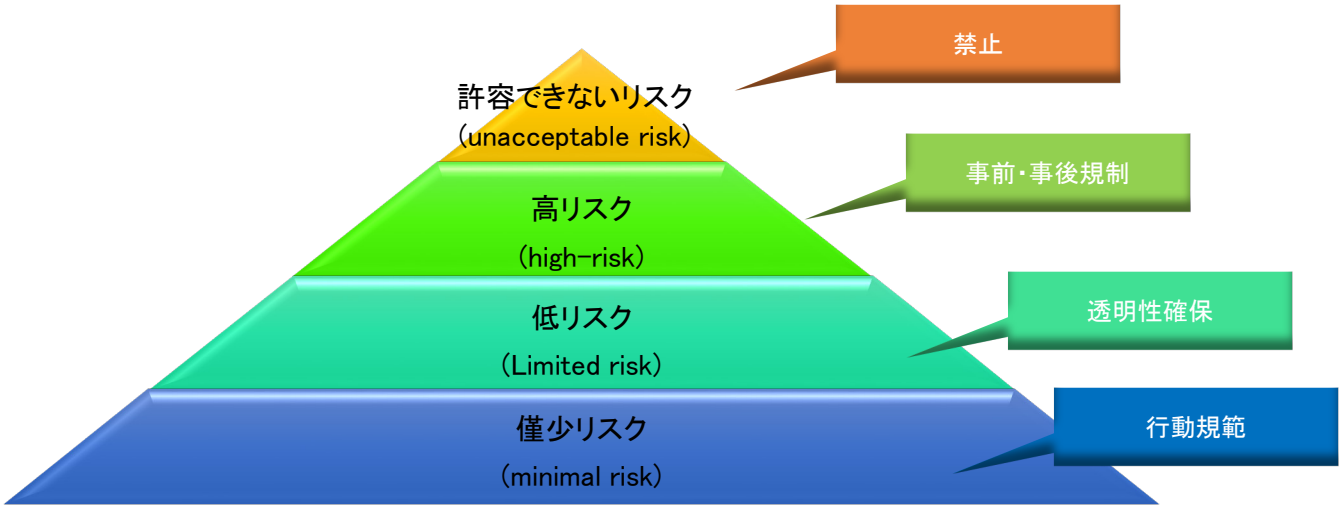
(a)	提供者が EU 域内又は第三国で設立されているか否かを問わず、EU で AI システムを上市又はサービス提供開始している提供者
(b)	AI システムの EU 域内に所在する利用者
(c)	AI システムによって生成されたアウトプットが EU で利用される場合における、第三国に所在する AI システムの提供者及び利用者

このように、日本に所在する事業者であっても、EU で AI システムを提供したり、AI システムによって生成されたアウトプットを EU で利活用するために日本で AI システムを利用したりしている事業者には、本 AI 規則案の地理的適用範囲が及び得る。また、この地理的適用範囲の定め方のうち、(a)号及び(b)号は、EU 域内に所在する者に向けて提供されている AI システムを補足しようとするものである点で、GDPR が定める域外適用の範囲(GDPR 3 条 2 項(a)号)と似た側面がある。もっとも、今のところ EU 域内の主体に向けたサービス提供の意思の明白性が要件として明記されていないことに加え、AI システムそのものではなくアウトプットの利用に関する(c)号も定められていることにより、GDPR に比べても、本 AI 規則案の地理的適用範囲の外延は、条文上は必ずしも明確とは言えない状態にある。

なお、輸入者が特定できない場合には、EU 域外で設立された提供者は、EU 市場で AI システムが利用可能となる前に、書面で EU に設立された権限のある代表者を選任する義務を負う(前文(56)項、25 条 1 項)。

3. 義務内容

本 AI 規則案は、AI システムの利用に関して、以下のとおり、許容できないリスク(unacceptable risk)、高リスク(high-risk)、その他のリスクというように、リスクの程度に応じて、規制の内容を定めている(リスクベースアプローチ)。



(1) 許容できないリスク(unacceptable risk)を伴う AI システム

以下の AI に関する活動は、許容できないリスクをもたらすものとして、いずれも禁止される(5 条 1 項)。

(a)	その者又は他人をして身体的又は精神的な危害を生じさせ又は生じさせるおそれのある形でその者の行動に著しく干渉するため、その者の**意識を超えたサブリミナルな手法**を用いた AI システムの上市、サービス提供開始又は利用
(b)	その者又は他人をして身体的又は精神的な危害を生じさせ又は生じさせるおそれのある形でその者の行動に著しく干渉するため、その者の年齢、身体的又は精神的障害に起因する特定の人間の集合の**脆弱性を利用する** AI システムの上市、サービス提供開始又は利用
(c)	特定の自然人又は集合全体の、データが元々生成又は収集された状況とは無関係の社会的状況において、又は不当若しくは不均衡な社会的行動若しくはその重大さに関して、これを毀損し、又は不利な取扱いにつながる**社会的スコア**

	と、**社会的行動**、又は既知の若しくは予測された人格若しくは**人格的特性**に基づいて、公的機関又はその者の代理によって一定期間にわたり、自然人の信頼性を評価又は分類するための AI システムの上市、サービス提供開始又は利用

なお、法執行を目的とした公的にアクセス可能な空間でのリアルタイム[5]の遠隔生体認証システム(顔認証システム等)[6]の使用も原則[7]として禁止される(5 条 1 項(d)号及び 2 項)。

(2) 高リスク(high risk)を伴う AI システム

高リスクを伴う AI システムとしては、例えば以下の項目の AI システムがリストされている(6 条、Annex Ⅱ、Annex Ⅲ)[8]。

①	既存法令に基づき第三者適合性審査を受ける必要があるもの[9]
②	リアルタイム及び事後における自然人の遠隔生体認証のためのもの
③	重要インフラの管理・運用のためのもの
④	教育及び職業訓練において、学生や希望者の評価や受入れの合否に関わるもの
⑤	雇用、労働者管理、自営業の採用に関する選考に使用されるもの
⑥	重要な民間・公共サービスへのアクセス及び享受(公的支援金の給付、融資、緊急対応措置)に関するもの
⑦	法執行機関の使用するもの
⑧	移民・亡命・国境管理に使用されるもの
⑨	司法又は民主主義プロセスに関するもの

これらの高リスクを伴う AI システムに対しては、以下の 7 項目の要件(以下「高リスク AI システム要件」という。)に従うことが求められる(8 条 1 項)。

9 条	リスクマネジメント体制の設置、実施、書面化及び維持
10 条	一定の品質基準を満たすトレーニング、検証及びテスト用データセットに基づくデータガバナンスの実施[10]
11 条	上市又はサービス提供開始前における技術書の作成及び更新[11]
12 条	AI システム動作期間中におけるログの保存
13 条	利用者がアウトプットを解釈でき、適切に利用できるためにその動作が十分に透明なものとなるような形での AI シス

---

5 敢えて「リアルタイム」のものを要件としている背景としては、影響の即時性、修正やチェックの機会が限定的であるといった点等が指摘されている(前文(18)項等)。

6 遠隔生体認証とは、遠隔地にいる人を、その人の生体データ(人の身体的、生理的または行動的特徴に関する特定の技術処理の結果として得られる個人データ)と参照データに含まれる生体データとを比較又は識別することを目的とした AI システムであり、AI の利用者が、対象者が存在しているか、又は識別できるかを事前に知ることなく利用できるものをいう(3 条(33)号・(36)号)。

7 ①行方不明となった子どもを含む特定の潜在的な犯罪被害者の捜索活動、②自然人の生命若しくは身体的安全に対する具体的、実質的かつ急迫した脅威又はテロ攻撃の防止、又は③一定の犯罪の加害者又は被疑者の探知、所在確認、識別又は訴追のいずれかの目的のために厳密に必要な範囲では、当局による事前の許可を得ることを条件に例外的に法執行を目的とした公的にアクセス可能な空間でのリアルタイムの遠隔生体認証システムは許容されている(5 条 1 項(d)号・2 項・3 項)。もっとも、例えば、このような例外事由のために用いられる AI システムを公的機関に納入している事業者が、例外事由への該当性の判断を厳密に行うことは容易ではなく、詳細なガイドラインの公表等を待つ必要があり得るほか、後記 **4.**のとおり、許容できないリスクに関する義務違反には最も重い制裁金が予定されていることからすると、この例外の利用には慎重になる必要がある可能性がある。

8 欧州委員会は、Annex Ⅲを修正して、高リスクを伴う AI システムの範囲を調整する権限を有する(7 条)。

9 詳しくは Annex ⅡA(https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=75789)参照。例えば、医療機器 AI 等が含まれる。さらに、Annex ⅡA に含まれている機会指令の改正案(2021 年 4 月 21 日公表)<https://ec.europa.eu/info/law/better-regulation/>において、安全機能向けの AI システム、及び AI システムを組み入れた機械は、ハイリスク機械製品として、第三者適合性評価の対象になることが示されている。

10 バイアスの監視、検知又は補正の目的のために厳格に必要な範囲で、一定の条件の下で、GDPR 9 条 1 項が定めるセンシティブデータの処理を行い得るとされている(10 条 5 項)。なお、本 AI 規則案は、個人データ処理の適法性根拠を提供するものと理解されるべきではないと定められてはいる(前文(41)項)。

11 この文書は、AI システムが上市され又はサービス提供開始されてから 10 年間保存するものとされている(50 条(a)号)。

	テムの設計・開発、及び利用者に対する適切な情報提供
14 条	AI システム使用中における自然人による監督 [12]
15 条	意図された利用目的に照らして適切なレベルの精度、頑健性及びサイバーセキュリティを達成するような方法での設計・開発

そのうえで、高リスクを伴う AI システムの提供者は、例えば以下の義務を負う(16 条参照)。

16 条 (a)号	AI システムが高リスク AI システム要件を遵守していることの確保
17 条	品質管理システム [13]を導入すること
18 条	11 条に定める技術書を作成すること
19 条	上市又はサービス提供開始前に 43 条に定める適合性評価手続 [14]を受けることを確保すること
20 条	AI システムにより自動生成される一定のログの保存
21 条	本 AI 規則案に適合しない場合に是正すること
22 条	AI システムが健康、安全又は基本権に対する一定のリスクを生じさせたことを提供者が知った場合に所定の監督機関に直ちに通知すること
23 条	監督官庁に協力すること
49 条	CE マークを貼付すること
51 条	AI システムの上市又はサービス提供開始前に、所定のシステムに登録すること

上記を時間軸に整理して纏めると、本 AI 規則案の適用を受ける、高リスクを伴う AI システムを取り扱う事業者においては、概要、(i)高リスク AI システム要件に従った AI システムのデザインを実施し、(ii)当該 AI システムの第三者又は自己による適合性評価 [15]を実施し、(iii)AI システムの上市及びサービス提供開始後においても事後的なモニタリングを実施し、(iv)何らかの問題が生じた場合は監督官庁に報告を受ける義務があることとなる。

このうち、AI システムの適合性評価については、各 EU 加盟国の既存の組織体や、製品安全性の評価枠組みを活用できる面があるとされており、もしそうであれば、スムーズな実効が図られる可能性がある [16]。なお、特に顔認証等のリアルタイム及び事後における自然人の遠隔生体認証のためのものに関しては、第三者又は自己による適合性評価のいずれかの手続を履行する必要がある旨が定められつつ(43 条 1 項)、前文では第三者適合性評価に依るべき旨が示唆されており(前文(64)・(65)項)、実際にも欧

---

12 GDPR 22 条 3 項は、データ主体とデータの管理者の間の契約の締結若しくはその履行のために必要となる場合、又はデータ主体の明示的な同意に基づく場合に、当該データ主体に関する法的効果を発生させる、又は、当該データ主体に対して同様の重大な影響を及ぼすプロファイリングを含むもっぱら自動化された取扱いに基づいた決定を行うときは、データ主体に対して、データ管理者の側での人間の関与を得る権利を付与している。ただし、GDPR は、個々のデータ処理活動に着目した規制である一方、本 AI 規則案は、AI システムの提供者の体制面に焦点を当てており、法的に必要となる関与の仕方等で差異が生じる可能性がある。

13 ①規制遵守のための考え方、②設計、設計管理、設計検証に使用するための技術、手順及び体系的行動、③開発、品質管理及び品質保証のために用いる技術、手順及び体系的行動、④開発前、開発中、開発後に実施される審査、試験、検証の手順及びそれらの実施頻度、⑤technical specification 及び要求事項に準拠していることを確認するためのもの、⑥データ管理のシステム及び手順、⑦リスク管理システム、⑧市販後の監視システムの設置、実施及び維持、⑨重大な事故及び故障の報告に関する手続き、⑩第三者とのコミュニケーションの取扱い、⑪全ての関連文書及び情報の記録保持のためのシステム及び手順、⑫供給の安全性に関する措置を含むリソース管理、⑬経営陣等の責任を定めた説明責任の枠組みといった、これら①～⑬の要素が含まれた品質管理システムでなければならない(17 条 1 項)。

14 適合性評価は、高リスクを伴う AI システムの種類、(及び統一基準(harmonised standard)[14]又は共通仕様(common specifications)[14]のいずれを適用したか)に応じて、自己の内部基準に基づく適合性評価手続、又は品質管理システムの評価及び技術文書の評価に基づく適合性評価手続(高リスクを伴う AI システムから独立した機関として別途指定された機関(notified body)が関与する)のいずれかに従って行われる(40 条乃至 43 条)。

15 評価機関は、AI システムのソースコードへのアクセスを求める権限を有する場合がある(Annex Ⅶ 4.5)。

16 本 AI 規則案の Explanatory Memorandum 4、5.2.4 等参照。なお、第三者の評価機関による適合性評価は通常有償であるとされている<https://europa.eu/youreurope/business/product-requirements/labels-markings/ce-marking/index_en.htm>。もっとも、機関によって評価に要するコストやスケジュールにはバラつきがあり得るところ、今後、各加盟国で適合性の評価機関が指定されていく中で、この点がどのように定められているかを注視する必要がある。

州委員会からは、評価機関が関与した手続が常に必要となる旨が表明されている[17]。

この他に、AI システムの製造者(24 条)、輸入者(26 条)、流通業者(27 条)、及び利用者(29 条)についても、それぞれの責任が規定されているほか[18]、これらの者が一定の場合には提供者とみなされる旨も定められている(28 条 1 項)[19]。

例えば、AI システムの利用者は、AI システムに対して用いるインプットデータが AI システムの利用目的に照らして関連性のあるものとすることを確保すること、使用に関する説明書に従って AI システムの動作を監視すること、利用者において管理可能な範囲で AI システムから生成されたログを自動的に保持すること、及び GDPR に基づくデータ処理影響評価を行う際、13 条に基づき提供者から提供された情報を利用することが義務付けられている(29 条 3 項乃至 6 項)[20]。

(3) その他のリスクを伴う AI システム

許容できないリスクや高リスクを有さないその他の AI システムについては、以下の一定の AI システム(Limited risk)に関しては、通知及び開示に関する透明性を担保するための規制が定められている(52 条 1 項乃至 3 項)。

一定の自然人に作用する AI	AI システムによって作用されている旨の通知が必要
一定の感情認識システム又は生体分類システム	自然人がそのシステムの動作によって影響されている旨の通知が必要
ディープフェイクを生成又は操作するシステム	コンテンツが人為的に生成または操作されたものであることの開示が必要

また、僅少リスクを伴う AI システム(minimal risk)[21]については、高リスクを伴う AI システムに課された義務を自主的に適用することを推進するための行動規範の作成が奨励されている(69 条 1 項)[22]。さらに、全ての AI システムを対象に、環境サステナビリティや、障がい者のアクセス可能性、AI システム開発の際のステークホルダーの関与、開発チームのダイバーシティ確保等を自主的に適用することを推進するための行動規範の作成も奨励されている(69 条 2 項)。

4. 制裁

本 AI 規則案の違反に対しては、EU 加盟国が定める罰則のほか(71 条 1 項)、以下の金額を上限とする制裁金[23]が定められている(71 条 3 項乃至 5 項)。

前年度における世界売上高の最大 6%又は 3000 万ユーロのいずれか高い金額	①許容できないリスクを伴う AI に関する禁止[24]違反

17 https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683

18 本 AI 規則案 2 条には、製造者、輸入者及び流通業者に関する地理的適用範囲の定めはない。

19 他方で、AI の利用者等が AI システムの利用目的を改変したり、AI システムを実質的に変更したりした場合は、AI システムを最初に上市又はサービス提供開始した提供者は、本 AI 規則案が提議する「提供者」に該当しなくなる(28 条 2 項)。

20 この他に、利用者が、本 AI 規則案に適合しない AI システムを利用した場合に、提供者とともに本 AI 規則案違反に問われ得るのかについては、今のところ明らかでない。

21 ビデオゲームやスパム検知に利用される AI システムが例示されている<https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682>。

22 本 AI 規則案前文(81)項・69 条は、行動規範の対象となる AI システムを、僅少リスクを伴う AI システムに限定しておらず、高リスクを伴う AI システム以外の AI システムを対象とする旨を述べるに留まるものの、欧州委員会の Q&A では、同条は僅少リスクを伴う AI を念頭に置いた定めであるように記載されている<https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683>。

23 ここでいう「制裁金」は、類似の規制を有する EU 競争法及びデータ保護法の議論を参照すると、刑罰ではなく、行政上の制裁としての性質を持つと考えられる(笠原宏『EU 競争法』(信山社、2016 年)241 頁、石井夏生利『EU データ保護法』(勁草書房、2020 年)201 頁参照)。

24 本 AI 規則案 5 条に対する違反を指す。

	②高リスクを伴うAIのデータガバナンスに関する義務[25]違反
前年度における世界売上高の最大4%又は2000万ユーロのいずれか高い金額	前記①・②以外の本AI規則案違反
前年度における世界売上高の最大2%又は1000万ユーロのいずれか高い金額	監督機関への不正確、不完全又は誤解を招く情報の提供

この制裁金の水準は、EU競争法違反に対する制裁金(前年度における世界売上高の最大10%)ほどではない一方で、GDPR違反に対する制裁金と同等又はそれを上回る水準となっている(違反事由に応じて、前年度における世界売上高の最大4%若しくは2000万ユーロのいずれか高い金額、又は前年度における世界売上高の最大2%若しくは1000万ユーロのいずれか高い金額。83条4項・5項)。

5. 今後の展望及び日本への示唆

本AI規則案は、欧州委員会によって欧州議会及び欧州連合理事会に提出され、今後、第一読会から第三読会を経る。欧州委員会としては、2022年後半に発効させ、最速で2024年後半までに適合性評価基準を準備することを目指している[26]。さらに、欧州委員会は、AI等に関連する賠償責任のルール整備も進める予定である[27]。米国においても、公的機関による顔認証技術を規制する州法が複数制定されたり、国家安全保障の観点に基づくものではあるが、AIの研究開発・利用に関する活発な動向[28]が見られたりしている。また、中国を含め、AIや機械学習を巡るデータや技術は、重点領域として、厳格な輸出入規制や投資規制に服するトレンドも見られつつあり、今後もAIを巡る実効的で予見可能性のある規制枠組みの議論は更に活発になることが予想される。

その中で日本企業としては、前記**2.**のとおり、本AI規則案は、日本企業にも適用され得る地理的適用範囲を定めているため、自社が研究開発又は販売しているAIシステムの中に、この適用範囲に含まれ得るものがあるかの洗い出しが求められる。

また、本AI規則案が域外適用されるか否か、また、その場合の判断基準の詳細はまだ不明であるところ、その判断が微妙なケースにおいて、域外適用されないことを完全に担保することは容易ではないケースに直面する可能性もある。その場合には、実務的には、その適用は否定できないことを前提に、GDPRと同等又はそれを上回る制裁金を定めていることを踏まえ、今後どのような修正が加えられるかの動向を注視するとともに、AIシステムの用途や想定されるリスクの内容・程度に応じて、いくつかの企業で既に設置されているAI倫理委員会のような組織体でリスクマネジメント体制の整備義務等を履行できるかといった検証等を開始しておくことも有益であると考えられる。

以 上

---

25 本AI規則案10条に対する違反を指す。高リスクAIシステム要件の中でも、特にデータガバナンスに関する違反に対してのみ、相対的に高額な制裁金の上限が予定されている点については、データに関する規制は、AIシステムの利用目的に照らして適用可能な、健康、安全、基本的権利に対するリスクを効果的に軽減するために必要であり(前文(43)項)、また、AI学習に使われるデータの品質を確保することで、AIシステムが差別の原因となることを防止し、安全性を発揮できる(前文(44)項)が影響している可能性がある。

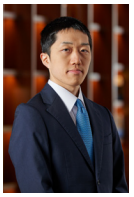
26 https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

27 欧州委員会は、2020年2月19日、「AI・IoT・ロボットに関する安全・賠償責任レポート」を公表していた<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0064&from=en>。

28 ホワイトハウスにおける国家AIイニシアチブオフィスの設置<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/14/executive-order-on-the-establishment-of-the-white-house-office-of-faith-based-and-neighborhood-partnerships/>、AIに関する国家セキュリティ委員会の報告書<https://www.nscai.gov/2021-final-report/>等。

木津　嘉之（きず　よしゆき）
西村あさひ法律事務所　パートナー弁護士
y.kizu@nishimura.com

2007年弁護士登録。2015年ユニバーシティ・カレッジ・ロンドン(ロンドン大学)ロースクール卒業(LL.M.)。欧州のM&A案件を中心に、欧州の企業法務全般に従事。ロンドン留学の後、欧州各主要国(ドイツ、フランスおよびイタリア)の法律事務所および日本企業の戦略チームにて約3年に亘り出向する中、日本企業およびプライベートエクイティファンドをクライアントとする欧州案件に、数多く関与。日本に帰国後、西村あさひ法律事務所の欧州プラクティスの中心メンバーとして、欧州案件を担当。



角田　龍哉（つのだ　たつや）
西村あさひ法律事務所　弁護士
t.tsunoda@nishimura.com

2014年弁護士登録。日本内外の独占禁止法/競争法全般のほか、IT/デジタル、プラットフォーム規制や、通商法、データ保護法、会社法等を幅広く担当。近時の著作として、「プラットフォーム事業者側の視点（特集: プラットフォーム規制の現在地）」(ジュリスト1545号)、「ビッグデータと単独行為（特集: プラットフォームと競争法）」(ジュリスト1508号)等がある。情報法制学会会員、Certified Information Privacy Professional/Europe(CIPP/E)。

戸田　相（と だ　しょう）
西村あさひ法律事務所　弁護士
s.toda@nishimura.com

2020年弁護士登録。2017年中央大学法学部法律学科卒業、2019年慶應義塾大学法科大学院修了。知的財産権や技術関連の国内外案件、コーポレート案件、その他ベンチャー支援を含む一般企業法務を幅広く取り扱う。