グローバルでのAI規制の潮流・最新動向とAIガバナンスの体制構築

2024年12月19日

西村あさひ法律事務所・外国法共同事業　パートナー弁護士

石川　智也

講師紹介

石川 智也

Noriya Ishikawa

パートナー｜フランクフルト / デュッセルドルフ
フランクフルト＆デュッセルドルフ事務所共同代表

n.ishikawa@nishimura.com

2020年秋よりドイツ在住。EUのデジタル分野における法令・政策（GDPR、デジタルサービス法、デジタル市場法、データ法、AI法、サイバーレジリエンス法、NIS2指令等）に明るく、また、グローバルでのプライバシーガバナンス・AIガバナンスの体制構築や、各国のデータ保護監督当局への報告が必要となる大規模なサイバーアタック事案への対応等を数多く手がけている。日系企業のData Protection Officerやデジタル分野のアドバイザーにも多く就任している。

学歴

- 2005年　東京大学法学部第一類 (LL.B.)
- 2015年　University of Virginia School of Law (LL.M.)
- 2016年　Munich Intellectual Property Law Center (LL.M.)

書籍/論文

- 2024年「〔鼎談〕EUデータ法が目指す世界」ジュリスト1599号
- 2024年「資本業務提携の実務」中央経済社、共編著
- 2024年「EU Data Actの解説（B2C/B2B共有を中心に）」Les Japan News 65号2巻
- 2023年「EUサイバーレジリエンス法案の概要」NBL1234号
- 2020年「個人情報保護法制大全」商事法務、共編著
- 2020年「いますぐわかるCCPAの実務対応」中央経済社、共著
- 2019年「秘密保持契約の実務〔第2版〕」中央経済社、共著

受賞

- 2024年　日本経済社「2024年に活躍した弁護士ランキング」<AI・テック・データ>第2位（企業票、企業票＋弁護士票）
- 2024年　Thomson Reuters Stand-out Lawyers 2024

ヨーロッパ

欧州全土におよぶ幅広いカバレッジ

欧州4拠点が有機的に連携し、欧州でのM&A、GDPRを含むデジタル法規制全般、競争法、その他各種業規制等の法対応全般について、欧州に進出する日系企業を包括的にサポート：欧州の取引・規制法については一通りカバー

ヨーロッパプラクティスの強み

- 欧州各国の法規制の違いにより複雑化する傾向のある法律問題において、欧州と日本の両面からサポート。多様なビジネス、文化、言語を深く理解する現地法カウンセル、日本法カウンセルが協働して、クライアントが直面する各種の問題へ的確かつ効果的なソリューションを提供

- 2020年よりフランクフルト、デュッセルドルフで培ってきた欧州での実務経験に加え、法規制の発信地であるブリュッセルに2025年1月に事務所を開設。ロンドン含む欧州４拠点から欧州の規制動向を注視。ルール形成支援等の法政策業務も強化

- デジタル分野について豊富な知識・経験。データ保護/プライバシーに加え、競争法、プラットフォーム規制、データの越境移転とDFFT、経済安全保障、AI規制、ヘルスケア、サイバーセキュリティ等を横断的に俯瞰する「Digital Policy & Regulation」という枠組みで対応

1966	2007	2020	2025
西村法律事務所設立 (西村総合法律事務所の前身)	統合を経て 西村あさひ法律事務所 設立	フランクフルト・ デュッセルドルフ 事務所開設	ブリュッセル・ ロンドン事務所 開設

1 EU AI Act

AI Actの全体像

- 2021年4月、AIによる健康、安全、民主主義、法の支配、環境その他の欧州連合基本権憲章で保障される基本権へのリスクを適切にコントロールする目的で提案
- 2022年以降の生成AIの隆盛に伴い、基盤モデルに対する規制も追加
- 製品安全性の枠組みを採用
  - ハイリスクAIシステム：適合性認証(適合性評価機関による適合性評価又は自己認証スキーム)、EU適合性宣言書、CEマーク等
  - 今後は、法律適合性を確保するための規格の内容が争点に
- バリューチェーンを通じたAIシステムの確保が目指される
  - 提供者(Provider)、輸入者(Importer)、流通者(Distributor)と立場に応じた義務

AI Actの全体像

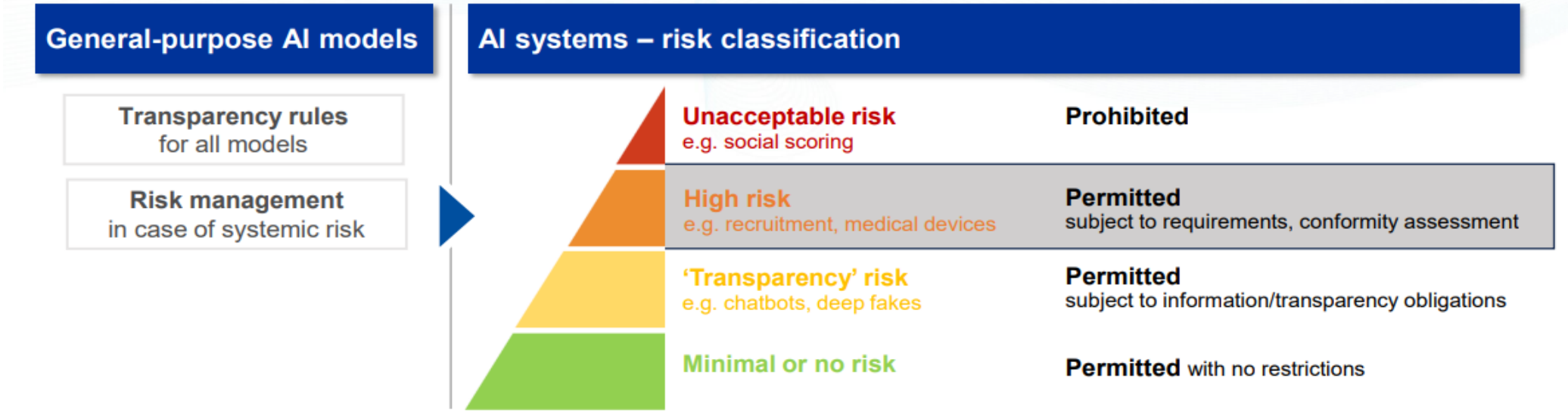
- 欧州委員会のサイト。法令のリンク
- European AI Officeのサイト。第1回ウェビナーも同ページに掲載。その後もウェビナー開催
- 規則(Regulation)であるため、加盟国法の制定を要さずに直接適用される
- 原則として2026年8月2日から適用開始だが、一部の規定は適用開始時期が異なる
  - 禁止されたAIシステム：2025年2月2日
    - AIシステムと禁止されたAIの定義に関するパブコメ開始(11/13)
  - 汎用AIモデル：2025年8月2日。但し、提供者への罰金は2026年8月2日から
    - 汎用AIモデルに関するQ&A公表(11/14)、Code of Practiceドラフト公表(11/14)
  - 6条1項に基づくハイリスクAIシステム(Annex 1に規定された法令が適用される場合)：2027年8月2日
- 高額な制裁金が規定されている

概要

▶リスクベースアプローチを採用

▷ AIシステムの持つリスクを①許容できないリスク、②ハイリスク、③透明性に関するリスク、④最小限のリスクに分け、リスクに応じた規制

▷ 基盤モデルは、①汎用AIモデル、②システミックリスクを有する汎用AIモデルに分けて、②の規制を加重



EU AI Office "Risk management logic of the AI Act and related standards 30 May 2024" 8頁

定義

- AIシステム(3条(1))
  - AIシステム：自律的に作動するよう設計され、導入後に適応性を示す可能性があり、入力から出力を生成する方法を推論する機械ベースのシステム
    - 主たる特徴は推論能力(出力を得るプロセス、入力・データからモデル/アルゴリズムを導出する能力)、人が定義したルールのみに基づき自動的に動作するシステムは含まない
  - 汎用AIモデル：顕著な汎用性を示し、広範なタスクを適切に実行でき、様々な下流のシステム/アプリに組み込むことができるAIモデル(いわゆる基盤モデル)
- 提供者(Provider)と導入者(Deployer)(3条(3)、(4))
  - 提供者：AIシステム/汎用AIモデルを開発し又は開発させ、自己の名義/商標の下で上市/サービス供給する者
  - 導入者： AIシステムを権限の下で利用する者(個人的な非専門的活動の過程で使う場合を除く)

適用範囲(2条)

▶適用範囲一般(1項)

- ▷ AIシステムのEU域内への上市・サービス提供、又は汎用AIモデルのEU域内への上市を行う提供者(EU域内と第三国の何れにて設立され、又は所在するかは問わない)
- ▷ EU域内に拠点を有し、又は所在するAIシステムの導入者
- ▷ 第三国に拠点を有し、又は所在するAIシステムの提供者及び導入者であって、AIシステムによって生成された出力がEU域内で使用されるもの
- ▷ AIシステムの輸入者及び流通者
- ▷ 自身の名称又は商標の下で、自身の製品と一緒にAIシステムをEU域内に上市し、又はサービス提供を行う製造業者
- ▷ EU域内で設立されていない提供者の、正式代理人
- ▷ EU域内に所在し、影響を受ける者

※「上市(placing on the market)」と「サービス提供(putting into service)」は定義語で、EU域内への製品の投入・サービス提供を指すことに注意(3条(9)(11))

禁止されたAI(5条)

- サブリミナル技術、操作的又は欺瞞的な技術を用いたAIシステム(十分な情報に基づく意思決定能力を著しく損ない、行動を大きく歪めるもの)
- 脆弱性(年齢、障害又は社会的若しくは経済的状況(極度な貧困、民族的/宗教的マイノリティ等)によるもの)を悪用するAIシステム(行動を大きく歪め、重大な危害をもたらす合理的な可能性があるもの)
- ソーシャルスコアリングにより社会的行動又は人格的特徴に基づき人を評価又は分類するためのAIシステム(データ収集時と異なる文脈での不利益又は人の社会的行動への不当な不利益をもたらすもの)
- インターネット、監視カメラから顔画像をスクレイピングして顔認識データベースを作成するAIシステム
- 職場及び教育機関における個人の感情を推測するAIシステム(医療又は安全上の理由による場合を除く)
- 人種、政治的意見、労働組合への加入、宗教的/哲学的信条、性生活又は性的志向を推測/推論するために、生体データに基づき個人を分類する生体分類システム(適法に取得した生体データセットのラベリング・フィルタリングは含まれない)
- (一定の場合を除く)法執行目的で公にアクセス可能な空間で使用するリアルタイム遠隔生体識別システム

ハイリスクAIシステム – 概要

- Annex IとIIIの区別が重要
  - I：整合法令適用対象製品であるAIシステム及びその安全性コンポーネントとして使用されるAIシステムが、整合法令に従って第三者機関による適合性評価を受ける必要がある場合
  - III：バイオメトリクス、職場、教育・職業訓練機関、重要インフラ等において利用されるAIシステム等
- 製品安全性の枠組みで規制される
  - 将来的にシステム要件は標準規格又は共通仕様への準拠を検討する必要がある
  - 例：適合性評価(43条)、適合性宣言書(47条)、CEマーク(48条)
- 欧州委員会は、1年に1回、Annex IIIのリストの修正の必要性を評価し、欧州議会・閣僚理事会に修正の必要性を報告する
- ハイリスクAIシステムの提供者と導入者とで義務が異なる。分けて整理する

ハイリスクAIシステム – 類型(6条2項)

- EU法又は加盟国法に基づき許容されるバイオメトリクスの使用
  - 遠隔生体識別システム(本人確認のみの目的で生体認証に使用されるAIシステムを除く)
  - 推測に基づくセンシティブ若しくは保護された属性又は特徴により、生体分類への使用を意図するAIシステム
  - 感情認識への使用を意図するAIシステム
- 不可欠なデジタルインフラ、道路交通の管理・運営又は水、ガス、熱若しくは電気供給における安全性コンポーネントとしての使用を目的としたAIシステム
- 教育及び職業訓練
  - 教育及び職業訓練機関への入学許可/レベル分け、学習成果の評価、受講する教育レベルの評価、試験中の生徒の禁止行為の監視及び検知を目的としたAIシステム

ハイリスクAIシステム – 類型(6条2項)(続き)

▶雇用、労働者管理、自営業へのアクセス

▷ 採用又は選考への使用、仕事に関連する条件、契約関係の促進/終了に影響する決定、個人の行動/特性に基づく業務の割当て、パフォーマンス・行動の監視・評価のために使用することを目的としたAIシステム

▶不可欠なサービスへのアクセス及び享受

▷ 不可欠な公的扶助・サービスの受給資格の評価、人の信用評価又はクレジットスコアの構築、生命・健康保険におけるリスク評価・価格設定、緊急通報の評価・分類、緊急初動サービス(警察、消防、医療救護等)の派遣のために使用することを目的としたAIシステム

▶法執行、移民、亡命/国境管理、司法・民主的プロセスで所定の用途で使用されるAIシステム

ハイリスクAIシステム – 提供者の義務(一覧)

類型	項目	条文
システム要件	リスクマネジメントシステムの実施	9条
	データガバナンス	10条
	技術文書の作成	11条
	ログの自動記録	12条
	透明性の確保(導入者への情報提供)	13条
	人間による監視	14条
	正確性、堅牢性、サイバーセキュリティ	15条
市販後モニタリング	市販後のシステム要件遵守に係る継続的なモニタリングの実施	72条
品質管理	品質マネジメントシステム(ポリシー、手順書及び指示書の形で文書化)	17条
文書・記録保管	技術文書・品質マネジメントシステムに係る文書等、自動生成ログの保管	43、47条
	監督当局の求めに応じたシステム要件適合性の証明文書、自動生成ログの提出	21条
不適合時の対応	是正措置(リコール、廃棄等)・導入者への通知	20条
製品表示	AIシステム又はパッケージ/附属文書上に名称、商標、連絡先住所の記載	16条(b)
製品安全性	域外適用時の認定代理人の指名	22条
	適合性評価・適合性宣言書の作成	43、47条
	CEマークの貼付	48条
	AIデータベースへの登録	49条
	アクセシビリティ法令への準拠の確認	16条(l)

ハイリスクAIシステム – 導入者の義務(26、27条)

民間の導入者の義務
使用説明書に従った技術的組織的措置
必要な能力、訓練、権限を有する自然人による監督
AIシステムの目的に照らして入力データが関連性を有し、代表的であること
使用説明書に基づく運用の監視及び(人の健康、安全又は基本的権利に対するリスクをもたらす可能性があると考える理由がある場合における)不当に遅滞なく、提供者又は流通者及び該当の市場監視当局への通知、当該ハイリスクAIシステムの使用停止
AIシステムの用途に適切な期間(少なくとも6か月)、自動的に生成されたログの保管
(職場で導入する場合)雇用者は法令の手続に従い、労働者の代表者及び影響を受ける労働者にAIシステムが使用される旨を事前に通知
自然人に関する決定を行うAIシステム(Annex III)の導入者は当該自然人にAIシステムが使用される旨を事前に通知
GDPRに基づくデータ保護影響評価を実施する際には提供者から提供を受けた情報を使用
基本権影響評価(重要インフラ、人の信用度・信用スコアを評価するAIシステム、生命・医療保険における人のリスク評価・価格設定に使われるAIシステムに限る)

透明性義務(50条)

類型	例	主体	義務
人と直接対話することを目的とするAIシステム	Chatbot	提供者	AIシステムと対話していることを通知する(一見して明らかな場合を除く)
コンテンツ生成AIシステム(汎用AIシステムを含む)	画像・動画・音声等の生成AI	提供者	AIに生成又は加工されたことが分かるように、機械可読な形式で印を付ける
感情認識システム	生体情報(表情、声色等)に基づき人の感情を推論するシステム	導入者	(i)個人に対してシステムの稼働を通知 (ii)GDPR等に基づく個人データの処理
生体分類システム	生体情報に基づき性別、髪色等の類型に分類	導入者	(i)個人に対してシステムの稼働を通知 (ii)GDPR等に基づく個人データの処理
ディープフェイクを生成又は操作するAIシステム	ディープフェイクの画像・映像等を生成するAI	導入者	AIによって生成又は操作されたものであることを開示(コンテンツが明らかに芸術的、創造的、風刺的、フィクション又はアナロジー作品の場合、作品の享受を阻害しない範囲に限定される)

汎用AIモデル – 概要

- 所謂「生成AI」を対象としており、生成AIの急速な普及に伴って設けられた規律
- 汎用AIモデルの提供者がこれをAIシステムと統合して上市した場合、AIシステムの規制及び汎用AIモデルの規制がいずれも適用される(前文(97))
- 少なくとも10億個のパラメータを持ち、大規模な自己監視を使用して大量のデータで訓練されたモデルは汎用性が肯定される(前文(98))
- 準拠することで義務の遵守を推定する標準規格が公表される予定
- (実施法により承認された場合)義務の遵守を立証できるCode of Practice策定予定
  - 9/30、キックオフミーティング(約1000の関係者参加)、4つのWGで協議
  - 11/14、1stドラフトが公表、11/28までに参加者はフィードバック

汎用AIモデル(51-56条)

▶計算能力に応じて、汎用AIモデル提供者 / システミックリスクを有する汎用AI

汎用AI	システミックリスクある汎用AI
AI Office及び加盟国当局に提出するモデルの技術文書の作成及び最新版の維持	
汎用AIをAIシステムに組み込もうとする提供者向けの情報・文書の作成及び最新版の維持・提供	
著作権等に関するEU法(特に、情報解析目的での複製等の権利留保)遵守を含むポリシー実装	
学習に使用されたコンテンツの詳細の要約を作成し、一般公開	
(第三国に設立された提供者は)EU域内への上市前に、認定代理人を指名し、適切に委任する	
	標準化プロトコル・ツールに従ったモデル評価(敵対的攻撃テストの実施・文書化等)
	汎用AIモデルにより生じ得るシステミックリスクのEUレベルでの評価・低減
	重大インシデントのトラッキング及びAI Office(及び適宜加盟国当局)への報告
	汎用AIモデル及びその物理的インフラの適切なサイバーセキュリティの確保

制裁金

- 禁止されたAIの使用
  - 3,500万€又はその前会計年度の全世界における年間総売上高の7%以下のいずれか高い方の制裁金
- ハイリスクAIシステムの提供者・導入者の義務(16、26条)、提供者・導入者の透明性義務(50条)違反
  - 1,500万€又はその前会計年度の全世界における年間総売上高の3%以下のいずれか高い方の制裁金
- 不正確、不完全又は誤解を招く情報を監督当局に提供した場合
  - 750万€又はその前会計年度の全世界における年間総売上高の1%のいずれか高い方の制裁金
- 汎用AIモデルの提供者が故意又は過失によりAI Actの規定に違反、AI Officeによる文書/情報提出要求に適切に応じなかった、要求された措置を実施しなかった、又は汎用AIモデルの評価のためにAI Officeにアクセスさせなかった場合
  - 1,500万€又はその前会計年度の全世界における年間総売上高の3%以下のいずれか高い方の罰金

2 米国

米国

- 連邦レベルでは、Executive Orderに従ったガイドライン等の策定が行われている
- トランプ政権下では、Executive Orderを撤廃するとの発言がある等、テック事業者フレンドリーな政策が予想されるため、連邦法の制定は見込みにくい
- 州レベルでは、生成AIや自動化された決定を行うシステムを規律する法令の制定が進んでいる (IAPP: US State AI Governance Legislation Tracker)
  - 施行済み：ユタ(AI Policy Act) – 生成AIを規制対象
  - 2026年1月1日施行：カリフォルニア(AB2013、SB942) – 生成AIを規制対象
  - 2026年2月1日施行：コロラド(SB205 Colorado AI Act) – 自動化された決定を規制対象
- HOUSE BIPARTISAN TASK FORCE ON ARTIFICIAL INTELLIGENCE DELIVERS REPORT(2024.12.17公表) : Guiding principles, forward-looking recommendations, and policy proposals to ensure America continues to lead the world in responsible AI innovation

米国

- カリフォルニア州：
  - AB2013
    - 生成AIシステムの開発者を規律
    - 生成AIシステムの学習のために使用されたデータについて、所定の事項を含むサマリーをウェブサイト上に公開する必要
  - SB942
    - 月間100万人以上の利用者が存在する生成AIシステムの提供者を規律
    - 生成AIシステム提供者は、①所定の基準を満たしたAI検出ツールをユーザーに利用可能とする、②AI生成コンテンツへの所定の事項を開示する、③生成AIシステムの第三者への利用許諾時に②を確保することが必要
- その他にも大規模オンラインプラットフォーマーに対して選挙関連の重大な欺瞞的コンテンツの削除手順、ラベル付け等を実装することを義務付ける法案等も成立

米国

- ユタ(SB149)
  - 生成AIを使用してユタ州の消費者と対話する全ての事業者又は個人に適用
  - 消費者が規制されたサービスの提供において生成AIと対話していることを「目立つように」開示する必要
  - 違反行為ごとに2,500ドル以下の罰金
- コロラド(SB205)
  - ハイリスクAIシステム(所定のサービス等を消費者に提供するかについての重大な決定を下す又はその実質的な要因となるシステム)の開発者及び導入者に、差別的な決定から消費者を保護する義務を課す
  - 導入者：影響評価、透明性義務、インシデント報告義務等
  - 開発者：説明文書、透明性義務、インシデント報告義務等

3 AI Actとその周辺 ～EUを題材に～

AIと製造物責任

- 究極的には製品としてのAIの安全性に問題があった場合に誰が責任を取る・取らないという問題ともいえる
  - 製造物責任指令改正(2024.11.18成立、12.8発効、2026.12.9 加盟国法の移行期限)：デジタル製品とプログラムを「製品」に含める旨を明示。アプリケーション、OS及びAIシステムも含まれる
  - AI責任指令案(2022.9.28提案)：AI法の下で保存が義務づけられるログの開示命令、AI法のシステム要件違反時等における因果関係の推定等
    - 2023年12月に議会と閣僚理事会で政治合意がなされたが、一部記事によると、その後、2024.9.19のEPRSによる追加での影響評価の結果を受け、規則化、スコープの拡大など、大きく変更される可能性が指摘されている

AI規制の要否、プラットフォーム規制との役割分担

- 2022年秋の生成AIの登場の前後で風向きが変わった
  - EUは元々ハードロー(製品としてのAIの安全性という枠組み)
  - 米国のExecutive Orderをはじめ、各国もハードローを志向し始めた
- 偽情報・誤情報への対応の必要性
  - 一度頒布された情報をプラットフォームがどのように扱うか
  - そのような偽情報・誤情報が量産されない、あるいは見分けがつくようにする、などのAI規制の必要性
- 規制強化とイノベーションの関係に関する議論

AI法とGDPR

- AI法によるGDPRの補完：
  - 明確な事前(ex-ante)禁止規定、一定のガバナンス構築義務の賦課
- AIによるデータの処理とGDPRに関する論点：
  - LLMは個人データを含むか
  - スクレイピングの適法性根拠
    - 特別カテゴリーを含まない：6(1)(f)の正当利益に依拠できるか？
    - 特別カテゴリーを含む：9(1)により原則禁止。2(a)の明示同意か、2(e)の本人公開の例外。どちらも使えないとなると・・・
  - 違法に作成されたAIモデルのその後の利用

AIモデルの文脈における個人データの処理に関するデータ保護の側面に関するオピニオン

- Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models (2024.12.17採択)
  - AIモデルが匿名化されていると考えられる場合と、そのように整理するに当たっての方法
    - 全てのケースを匿名化されていると一律に処理することはできない
    - 個人データを直接抽出した可能性と、クエリからその個人データを得られる可能性が僅少であるかを見る
  - 開発・利用に際し、legitimate interestを適法化根拠として適切であると示すための方法
    - いわゆる3ステップテスト(正当利益の内容、当該利益のためのデータ処理の必要性、バランシングテスト)
    - バランシングテストに際しての、データ主体の合理的な期待にフォーカス
  - AIモデルの開発段階における個人データの処理の違法がそのAIモデルのその後の処理やオペレーションに与える影響
    - 3つのシナリオについて検討((1)匿名化されていないAIモデルを同一管理者が使用する場合、(2)それを別の管理者が使用する場合、(3)違法なデータ処理による学習を経るも、その後匿名化されたAIモデルを使用する場合)
- Notes:
  - 各国のデータ保護監督当局向けの意見
  - センシティブデータの処理根拠はスコープ外と明記(para.17)。scraping in the context of generative AIに関するガイドラインも従前示されたとおり今後(脚注6参照)

4 AIガバナンスの体制構築

EU AI法対応

- 適用対象の早急な検討
  - AIマッピング：社内でのAIの開発・導入を網羅できないことがリスクに
  - AI Actのどのカテゴリーに分類されるAIシステムを運用しているかの分類
  - 提供者・導入者のいずれの立場にあるかを意識する
- 禁止されるAIシステム/ハイリスクAIシステムの開発・利用がないかの確認
- ガイドラインがパブコメにかかってからの対応では遅い。ハイリスクAIに該当しないことを確保する必要があるなら、今動く必要がある
- AIガバナンスの構築に当たって、ハイリスクAIシステムの開発・利用については厳格な対応が必要
- 汎用AIモデルの提供者に該当する場合は、EU AI法への対応が必要ないか慎重に要検討
- アップデート(下位規則・ガイドライン、パブコメ、標準規格)のフォロー

グローバルでのAIガバナンスの体制構築

- 組織、規程、予算、重み付け
- 規程：どこの国・業界のルールを、自社のルールとするかの確定
  - 社内規程の作成
  - 開示用のAIポリシーの策定
- 規程に基づくAIマッピングの実施と継続：ガバナンスを効かせるための基礎
- Tips：
  - 手作り感があっても良い
  - 基本原則から、小さく始める、成功事例を作る、トライアンドエラー
  - ずっとお付き合いするもの。終わるプロジェクトではない。一大プロジェクトは瓦解する
  - 適用のあり得る全てのルールを反映することも、一律のルールを課すことも難しい
  - 情報収集に労力を掛けるのはもったいない

西村あさひ法律事務所・外国法共同事業
東京都千代田区大手町１－１－２ 大手門タワー 〒100-8124
Tel 03 6250 6200

西村あさひ（デュッセルドルフ）
Dreischeibenhaus, 40211 Düsseldorf, Germany
Tel +49 (0)211 88 250 140

西村あさひ（フランクフルト）
Friedrich-Ebert-Anlage 35-37, 60327 Frankfurt am Main, Germany
Tel +49 (0)69 257 298 800