小特集
Special Feature

［個人情報保護法制の最新動向］

4 個人情報保護法改正と AI 開発

応用

美馬正司　（株）日立コンサルティング／慶應義塾大学政策・メディア研究科

AI 開発と個人情報保護法の関係

AI 開発の特徴

昨今，第三次 AI ブームと言われており，コンサルタントとして仕事をしていても AI を用いる案件にかかわる機会が格段に増えてきている．この AI の普及の背景にはディープニューラルネットワークの研究の進展があり，データを学習することが基本となっている．一般的に AI を開発する場合，訓練用の入力データと正解データを用意し，これを学習させることでパラメータを調整し，AI モデル（パラメータ＋推論プログラム）を作成する．このため，訓練用のデータをどのように準備するかが最初の重要な作業となる．

AI 開発と個人情報

ビジネス上，たくさんの AI 案件を見てきているが，学習に使われるデータの多くは，個人情報である個人データ，あるいはパーソナルデータ（個人に関するデータ）[☆1] と呼ばれているものである．もちろん，一部には人にかかわらない機械の制御データ等を扱うものもあるが，ほとんどの場合は何らかしらの形で人にかかわるデータが利用されている．したがって，個人データを学習させる場合は個人情報保護法を遵守することは不可欠であり，個人データではないパーソナルデータを扱う場合においてもプライバシーへの配慮が求められる．

個人データの学習の課題

例外規定はあるものの，通常，個人データは取得する際に通知，あるいは同意をした目的や利用範囲でしか利用することはできない．そのため，AI の開発が，取得時の目的に合致しない場合にはデータ主体となる個人から再同意を取得することが必要になる．また，往々にして生じることが AI を開発する組織と個人データを保有する組織が異なるという事象である．この場合，個人データを保有する組織から AI を開発する組織にデータを提供する必要があるが，こちらは個人情報保護法にある第三者提供にあたり，やはりデータ主体となる個人から同意を得ることが不可欠となる．

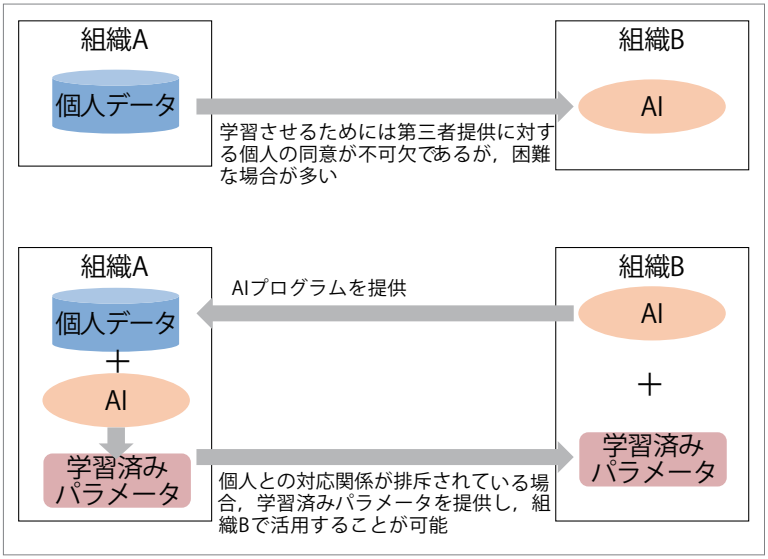
個人情報保護法を踏まえた対応

前述した 1 つ目の課題である取得時の目的と異なる点については，個人情報保護法の 2020 年改正において新設された「仮名加工情報」を用いることで対応することが可能である．仮名加工情報の作成においては，氏名等，直接，個人が識別できるようなデータは削除されるものの，それ以外のデータは保持されるため，訓練用のデータとしての有用性は問題ない場合が多いと考えられる．したがって，2020 年改正の施行に伴い，組織内での仮名加工情報を用いた AI 開発が活発化することが想定される．

☆1 https://www.ppc.go.jp/files/pdf/personal_280229sympo_pamph.pdf

一方，2つ目の課題である個人データを保有する組織とAIを開発する組織が異なる点についても解決策が提示されている．それは，2021年6月30日に個人情報保護委員会から提示された「『個人情報の保護に関する法律についてのガイドライン』及び『個人データの漏えい等の事案が発生した場合等の対応について』に関するQ&A」[☆2]に記載されている．同Q&Aによると，「複数人の個人情報を機械学習の学習用データセットとして用いて生成した学習済みパラメータ（重み係数）は，学習済みモデルにおいて，特定の出力を行うために調整された処理・計算用の係数であり，当該パラメータと特定の個人との対応関係が排斥されている限りにおいては「個人に関する情報」に該当するものではないため，「個人情報」にも該当しない」とされる．すなわち，学習済みパラメータであれば，個人情報（個人データ）に該当しないため，組織を跨って移動することが可能になる．したがって，個人データを保有する組織にAIのプログラムを提供し，学習させ，その学習済みパラメータをAIを開発したい組織が受け取るという構図が成立し得る（図-1）．

☆2 https://www.ppc.go.jp/personalinfo/legal/



■図-1 学習済みパラメータの提供

適正なAI開発

仮名加工情報によるAI開発

前述したようにAI開発における個人情報にかかる2つの課題については解決策が存在するものの，無作為にこれを行ってよいわけではない．プライバシー等へ配慮した適正なAI開発が求められる．

たとえば，同一組織内であれば，複数の仮名加工情報を突合して目的外に活用することが可能である．つまり，個人データとしては，別々の目的で取得されたものであるため，名寄せすることができないが，仮名加工情報に加工することで名寄せし，目的外利用することが可能になる．また，同一組織内であれば，このように仮名加工情報を突合したビッグデータを用いてAIの開発を行うことも可能である．

ただし，このように開発したAIの活用にはプライバシーの観点から留意が必要である．複数の仮名加工情報から開発したAIにおいては，元となった個人データの特性を再現することが可能である．すなわち個人データベースAと個人データベースBから作成した仮名加工情報A’，仮名加工情報B’から開発したAIに個人データベースAを入力すると，非常に高い精度で個人データベースBが出力される．そのため，複数の仮名加工情報を統合したデータベースからAIを開発した場合には，元となる個人データを入力する等の行為は行われるべきではない．たとえば，図-2のような名寄せした仮名加工情報からAIを開発した場合，個人データベースAを入力すると，非常に高い精度で個人データベースBの所得，世帯構成等のデータが出力される可能性があり，このような活用の仕方はプライバシーの観点から不適切と考えられる．

学習済みパラメータの取扱

学習済みパラメータが個人情報（個人

データ）に該当しないということについて，いくつか留意することが必要である．

まず，「複数人の個人情報を機械学習の学習用データセットとして用いて」と記述されているように，1 人の人間の行動データ等を学習した場合，学習済みパラメータは個人データに該当するということである．多くの場合は，複数の個人データを用いるが，特筆したエキスパートの行動を再現するなどの目的で AI を開発する場合，このようなことが発生し得る．

次に「当該パラメータと特定の個人との対応関係が排斥されている限りにおいては」ということが肝となる．パラメータ自体に個人との対応関係が残っていることは稀とは考えられるが，いくつかの条件が重なった場合に生じ得る．たとえば，10 人程度の基本情報（性別，生年月日，身長，体重等）と疾病情報（たとえば癌などの傷病名）を学習した AI があり，これが過学習していた場合，学習済みパラメータは基本情報から疾病情報を精度高く出力する．仮に学習データとなった 10 人の基本情報が容易に入手できるのであれば，個人との対応関係が排斥されているとは言えない．また，AI の中には学習済みパラメータと学習データが密接不可分なものも存在する．英国の ICO（Information Commissioner's Office）によると，SVM（Support Vector Machine）や k 近傍法（k-nearest neighbors）においてはモデル自体がデータを内包するため注意が必要となる☆3．

さらに AI のモデルに対して学習データを再現するような攻撃も背景知識と GAN（敵対的生成ネットワーク）等があれば可能とする研究もあり，このような行為を禁止するような配慮も必要ではないかと考えられる．

プライバシーに配慮した AI

連合学習

AI の開発に必要な個人データの扱いにおいて個

☆3 https://ico.org.uk/about-the-ico/news-and-events/ai-blog-privacy-attacks-on-ai-models/

個人データベースA

氏名	生年月日	性別	保険者番号	要介護認定
山田太郎	1950年7月5日	男	282012	3
松本次郎	1950年7月21日	男	282012	5
佐藤三郎	1950年7月13日	男	282012	2
鈴木花子	1948年9月28日	女	282012	2
田中恵子	1948年9月10日	女	282012	4
高橋美子	1946年9月14日	女	282012	3

個人データベースB

氏名	生年月日	性別	所得	世帯構成
山田太郎	1950年7月5日	男	300万円	3人
松本次郎	1950年7月21日	男	300万円	5人
佐藤三郎	1950年7月13日	男	300万円	2人
鈴木花子	1948年9月28日	女	500万円	3人
田中恵子	1948年9月10日	女	300万円	3人
高橋美子	1946年9月14日	女	400万円	3人

仮名加工情報A′

氏名	生年月日	性別	保険者番号	要介護認定
ad8d3fea7a	1950年7月5日	男	282012	3
75c81f14ae	1950年7月21日	男	282012	5
b8f1f98ac8	1950年7月13日	男	282012	2
bf066fa8f3	1948年9月28日	女	282012	2
482c743faa	1948年9月10日	女	282012	4
1e6eb3ef8e	1946年9月14日	女	282012	3

仮名加工情報B′

氏名	生年月日	性別	所得	世帯構成
ad8d3fea7a	1950年7月5日	男	300万円	3人
75c81f14ae	1950年7月21日	男	300万円	5人
b8f1f98ac8	1950年7月13日	男	300万円	2人
bf066fa8f3	1948年9月28日	女	500万円	3人
482c743faa	1948年9月10日	女	300万円	3人
1e6eb3ef8e	1946年9月14日	女	400万円	3人

仮名加工情報（名寄せ）

氏名	生年月日	性別	保険者番号	要介護認定	所得	世帯構成
ad8d3fea7a	1950年7月5日	男	282012	3	300万円	3人
75c81f14ae	1950年7月21日	男	282012	5	300万円	5人
b8f1f98ac8	1950年7月13日	男	282012	2	300万円	2人
bf066fa8f3	1948年9月28日	女	282012	2	500万円	3人
482c743faa	1948年9月10日	女	282012	4	300万円	3人
1e6eb3ef8e	1948年9月14日	女	282012	3	400万円	3人

■図 -2　仮名加工情報の統合による AI 利用の問題

人情報保護法やプライバシーへの配慮が不可欠であるものの，このような課題に配慮した新たな技術も出てきている．その 1 つが連合学習（Federated Learning）である．

連合学習の 1 つの特徴はデータを集約しないことであり，データを保有している側に対して AI のモデルを配布し，配布モデルとの差分となる情報から AI モデルの学習を行うというものである．この差分は Model Update あるいは勾配（Gradients）と言われているがデータそのものを移動させるのではないため，プライバシーに配慮した仕組みであると言われており，近年，研究も盛んに行われるようになってきている．

連合学習の可能性

複数の組織でプライバシーを保護する仕組みとして，これまで秘密計算という仕組みが考案されてきた．秘密分散や準同型暗号等を用いるものがあり，中間的な処理プロセスが秘匿されるためプライバシーに配慮されている．しかしながら，これらはいわゆる，暗号技術を用いる仕組みであり，「暗号化したとしても個人データは個人データとして扱う必要がある」とする個人情報保護法との関係から組織を跨った分析に用いることが難しい状況であった．

一方，連合学習で組織を跨ってやりとりされる Model Update あるいは勾配は学習済みパラメータに近いものと考えられ，前述したように個人との対応関係が排斥される限りにおいては個人データには該当せず，組織を跨った分析が可能になるのではないかと期待される．

一方，Model Update あるいは勾配の中にはモデルが複雑な場合に個人の特定性が出るという指摘も見られ☆4，これを防ぐような研究も出てきている．

組織を跨ったデータ分析については，匿名加工情報等を用いた方法も存在するが，今後，AI の研究開発が進展することで連合学習が用いられることも想定される．

ただし，匿名加工情報を用いた場合でも，連合学習を用いた場合でも，複数の組織の別々のデータベース内に存在する同一個人を名寄せするような分析は不可能であり，この点については秘密計算等の法的な整理が待たれるところである．

個人情報保護法等への期待

AI の研究開発の進展によって，分析対象となる個人データとそこから生成される AI の関係性も複雑化してきており，プライバシーを侵害しないための研究も多様化してきている．

個人データを AI プログラムに学習させるという単純な構図だけではなく，それを組織を跨って行うための学習済みパラメータの移転や連合学習のような仕組みも今後，さらに普及すると考えられる．これらが適切に行われるよう，法的な整理と合わせて実際の運用面のルール検討等も進められることが期待される．

一方，GAN 等の AI を用いることで合成データ（Synthetic Data）を生成するような研究も進んできている☆5．合成データそのものの取り扱いや，合成データを用いて AI の開発を行うことなど，AI の進展に必要な個人データにかかる法的な検討事項は継続的に出てきており，個人情報保護委員会等においてこれらにできるだけ迅速に対応することが望まれる．

（2021 年 12 月 6 日受付）

☆4 https://ico.org.uk/about-the-ico/news-and-events/ai-blog-data-minimisation-and-privacy-preserving-techniques-in-ai-systems

☆5 https://datasciencecampus.ons.gov.uk/projects/generative-adversarial-networks-gans-for-synthetic-dataset-generation-with-binary-classes/

■美馬正司　tmima@hitachiconsulting.co.jp

大学卒業後，シンクタンク等を経て現職．総合研究大学院大学複合科学研究科情報学専攻（博士課程）単位取得退学．情報大航海プロジェクト等，国の大規模プロジェクトのプロジェクトマネジメントやプライバシー，AI 倫理等，関連した制度面の検討に従事．