2023年7月21日

生成AIに関する法的論点II：
生成AIとプライバシー

敬和綜合法律事務所
弁護士　河本秀介

生成AIとプライバシーを巡る現状

Introduction

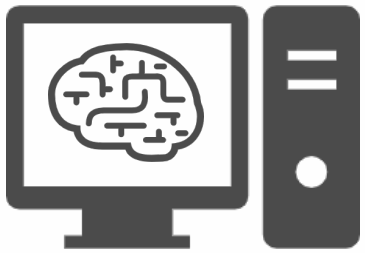
- AIとプライバシーの問題は、これまで学習用データ取得の場面における匿名加工等の問題を中心に論じられてきた。
- ChatGPTに代表される高度な生成AIの登場により、個人情報の本人の想定を超えた結果が生成されるなど、AIとプライバシーに新たな課題が生じている
- 生成AIサービスの提供者や利用者は、これらの課題にどう対応すべきか

想定を超えた個人情報の生成

・サイトの閲覧履歴
・SNSの投稿
・SNSのつながり情報
・住所・年齢
・学歴・職歴
・AIへの質問傾向

取得

学習



出力

Q:先日面接したAさんの政治傾向を教えてください

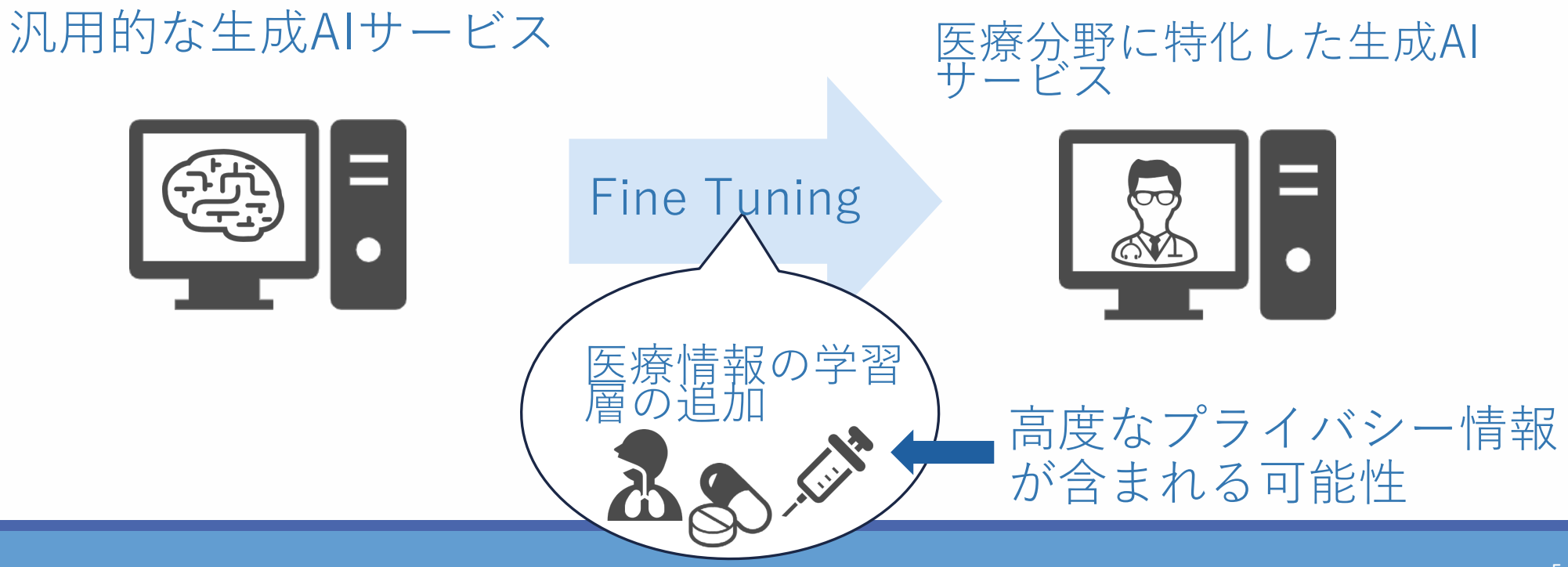
A:Aさんは、〇〇党の支持者です。前回の選挙ではＸ氏を支持していました。また、△△党の掲げる××政策には反対の立場です。

単体では断片的な個人情報

✓精緻なプロファイル情報
✓要配慮個人情報の表示
✓誤った推測である可能性

派生サービスとプライバシー

汎用的な生成AIを活用した生成AIサービスにも、同様の課題が生じる



日本の法制度の現状

- 日本では政府がAIの開発・利用について積極的な姿勢を示す傾向
- AIとプライバシーの課題は個人情報保護法などの既存の法律による解決が中心
- 個人情報保護委員会による令和5年6月2日付注意喚起が今後の指針になる可能性

個人情報保護委員会による注意喚起

個人情報保護委員会による注意喚起

「生成AIサービスの利用に関する注意喚起等について」（令和5年6月2日）

I. 「生成 AI サービスの利用に関する注意喚起等」
（利用者向けの注意喚起）

II. 「OpenAI社に対する注意喚起の概要」
（ChatGPTの開発・提供会社向けの注意喚起）

個人情報保護委員会による注意喚起

I. 「生成 AI サービスの利用に関する注意喚起等」

1. 個人情報取扱事業者における注意点
2. 行政機関等に対する注意点
3. 一般の利用者に対する注意点

points

✓ プロンプトの入力情報から学習する場面を想定したもの

✓ 個人情報の取り扱いについて利用者属性ごとに注意喚起

個人情報保護委員会による注意喚起

II. 「OpenAI社に対する注意喚起の概要」

1. 要配慮個人情報の取得
   本人の同意なく要配慮個人情報を取得することを防止するため遵守すべき具体的な事項の提示
2. 利用目的の通知等

points

- ✓ 要配慮個人情報からの学習の排除
- ✓ 個人情報の利用目的の通知等による透明性の確保

生成AIとプライバシー：現状の課題

生成AIに特有のプライバシーの課題とは何か

① 利用者がプロンプトに入力した個人情報が学習用データとして利用されることの課題

② 散在・断片的な個人情報が集積され、要配慮情報を含む高精度のプロファイル情報が生成されることの課題

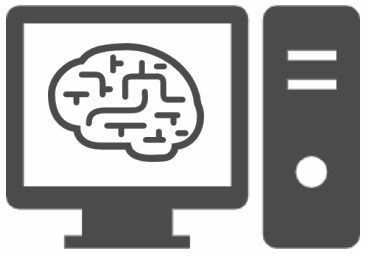
③ 推知の誤り等により生じる不利益の課題

生成AIとプライバシー：課題となる場面

個人情報の取得

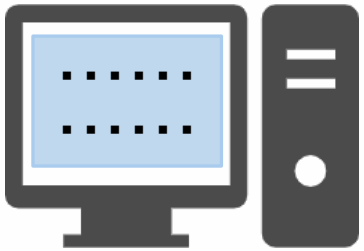
① プロンプトからの個人情報の提供・取得
② インターネット上の断片情報の取得

学習



② 要配慮個人情報を含む高精度なプロファイリング
③ 推知の誤り

個人情報を含む出力



A) サービス提供者の課題

B) 利用者の課題

生成AIとプライバシー：プライバシー情報の取得・学習

学習用データの取得とプライバシー

生成AIが学習用データとしてプライバシー情報を取得する際の主な方法

a. 権利処理された学習用データセットからの取得
b. インターネット等で公開された情報からの取得
c. 生成AIの利用者がプロンプトに入力した情報からの取得

➡ b. c.の場合にどのような課題があるのか

インターネットからの個人情報取得

インターネットからの個人情報取得の課題

- 不特定多数に公開された情報であるが、個人情報の本人の同意が得られているとは限らない
  - ✓ 一般的な個人情報の場合、公開されている以上、個人情報保護法上の不正取得になる可能性は低い
  - ✓ 取得に本人の同意が必要な要配慮個人情報については、不正取得になる可能性が否定できない

プロンプトからの個人情報取得

プロンプトからの個人情報取得の課題

利用規約に学習目的利用が記載されている限り、個人情報保護法の適正取得の問題は一応クリアされているが……？

- ✓ 大半の利用者が利用目的を読んでいない中、利用規約を盾に不適正取得・利用に当たらないと言い切れるか
- ✓ 要配慮個人情報を本人以外の第三者が入力した場合に不適正取得にならないか

生成AIサービス提供者の対応

「OpenAIに対する注意喚起」で示唆された要配慮個人情報の排除に向けた対応

① 収集の対象に要配慮個人情報が含まれないよう必要な取組を行うこと

② 収集した情報に含まれ得る要配慮個人情報をできるだけ減少させる措置を講じること

③ 学習用データセットへの加工前に要配慮個人情報を削除する又は特定の個人を識別できないようにするための措置を講じること

生成AIサービス提供者の対応

プロンプトから学習用データを取得する場合に考慮すべきこと

- 個人情報の本人にとって想定外の利用がされないための措置
- 本人以外の第三者から要配慮個人情報を取得する可能性の排除

- ✓ 利用規約の明確化と利用者への注意喚起
- ✓ プロンプトからの学習のオンオフ機能、プロンプトから学習しないビジネス向けサービスの提供
- ✓ そもそも学習用データから要配慮個人情報を排除する

生成AIとプライバシー：プライバシー情報の出力

生成AIの出力情報とプライバシー

生成AIのサービス提供者が、プライバシー情報を含む情報を表示することにどのような課題があるか？

① 個人情報が表示されることそれ自体の課題

② 分散した情報からの学習や、容易に発見できない情報からの学習を通じた、高度なプロファイル情報の提供の課題

③ 誤推知情報が表示されることの課題

生成AIの出力情報とプライバシー

生成AIが適正取得したデータから学習した結果、個人情報を含む生成物を出力することに問題はないか

- 個人情報を含む情報の出力は個人データの第三者提供とは言い難く、個人情報保護法上の違法となる可能性は低い
- ただし「問題が全くない」とは言い切れない

- ✓ 個人の自己情報コントロール権としての**プライバシー権の侵害**に当たる可能性
- ✓ 特定の個人に関する誤推知情報が表示されて不利益を被った場合などの**名誉毀損**の成立可能性

生成AIサービス提供者の対応

- 出力情報によるプライバシー侵害、特に要配慮個人情報の出力の回避
  - ✓ 特定個人の識別情報・要配慮個人情報からの学習の排除
- 誤推知による不当な結果の回避

※誤推知の完全な回避が不可能であることを踏まえた対応

  - ✓ 誤推知の可能性があることの周知
  - ✓ 推論の透明性の確保

生成AIとプライバシー：利用者の課題と対応

生成AIの利用者とプライバシー

個人情報取扱事業者である企業等の課題

- 企業が従業員その他の個人情報を含む情報を生成AIのプロンプトに入力することの課題
- 企業が生成AIから個人情報を含む情報を取得することの課題
- 誤推知情報による判断リスクの排除の課題

プロンプトへの個人情報の入力

企業利用者が生成AIのプロンプトに個人情報を入力することは個人情報保護法上、違法とならないか？

- 企業が業務目的で生成AIから情報を取得するため、個人情報を入力する行為は個人情報の委託にあたり違法とならない可能性が高い
- ただし、**生成AIの学習用データに利用される場合**、委託の範囲を超えており、個人データの第三者提供や目的外利用に該当し、違法となる可能性が高い

※特に個人情報保護法上の制約が厳しい海外への第三者提供になっている可能性に注意

生成AIからの情報取得

企業等が生成AIから個人情報を取得し利活用することに課題はあるか

- 不特定多数向けのサービスから推知情報を取得する場合、個人情報が含まれていても不正取得に当たる可能性は低い
- 要配慮個人情報を含む推知情報の取得は本人の同意のない取得にあたる可能性が否定できない
- 誤推知情報が排除できない以上、誤った判断を行うリスクの排除

利用者である企業等の対応

個人情報の不適正利用の排除・誤推知リスクの排除に向けた社内ルールの策定・啓発

- ✓ 生成AIへの入力情報が学習に使用されないことの確認（設定の確認・ビジネス向けサービスの導入）
- ✓ 生成AIの利用、特に情報を入力する際のフィルタリングを含む社内ルールの策定・周知徹底
- ✓ 生成AIの基礎的な仕組みを社内啓発するなど、誤推知の可能性や危険を周知（リテラシーの向上による誤った判断・個人情報の不適正取得リスクの低減）

まとめ

- サービス提供者が学習用データとして個人情報を取得する場合、要配慮個人情報の排除等のデータ管理や利用者に向けて情報取得ルールの周知を行う
- サービス提供者がプライバシー情報を出力する可能性がある場合、学習用データの管理に加え、推論の透明性を測るとともに、誤推知の可能性を周知する
- サービス利用者が企業である場合、社内ルールの策定や従業員等のリテラシー向上を図る