コンピュータ演習

AIリテラシー　07講　データ・AIを扱うときに注意すること

目次

第07講 データ・AIを扱うときに注意すること

データ活用の負の側面

よい面だけ持つ技術は存在しない。

- 自動車　～　交通事故
- 電気　～　感電
- 化石燃料による発電　～　環境への負荷

データサイエンスやAIも同じ。

かゆいところに手が届くビッグデータの活用

- 高級旅館のおもてなし
- コンシェルジュサービス

これらはサービスの担い手が利用者のことを知り尽くすことで成立している。

全てのビジネスで行うことはコスト上困難だが、ビッグデータやAIを使うと極めて低いコストで同じことが可能です。

例えば100均ショップで「いつものおにぎりですか？」と言ってもらえる可能性があります。

自分のデータが勝手に記録され、保存される

反面、以下の危険性もあります。

- 行動が記録されている
- 活動を知らないうちに保存されている

例1

オンラインショッピングでまだ迷っている段階なのにこれまでの行動からポチることが確実と判断され、発送される(実際に特許を取得している企業あり)

例2

職務質問に合う機会が多いなと感じていたら、普段の行動が危なっかしいので、お巡りさんはいつもあなたに目を光らせている

- これが未来の捜査か、ＡＩが犯罪を予測　ＵＡＥドバイの警察が導入
- 都市の犯罪発生を予測し、未然に防ぐ

生体に関するデータ

- 知りたくもない自分の予測余命まで知ってしまうかもしれない
- 保険料や住宅ローンに影響を与えるかもしれない

合理的と考える人も、秘密にする権利があると考える人もいる。
結論は出ていない。

怖さを感じる人が増えている

Facebookの感情についての実験

- タイムラインに楽しい話題を表示するグループ
- タイムラインに悲しい話題を表示するグループ

の二つに対する**A/Bテスト**を行ったことがあり、前者はその日1日が活発に、後者は逆の反応を示した。

感情や行動を操られる可能性がある。

GDPR、忘れられる権利、ELSI、オプトイン・オプトアウト

これらに対してどのように身を守るのか

EUの取り組み

2018年にEUでGDPRが定められた。

> GDPR(General Data Protection Regulation) 一般データ保護規則

個人が自分のデータをコントロールできるようにするため。

巨大ITによるデータ収集・処理にメリットがありますが、

> どんなところでどんなふうに使われているのか知り、修正したり差し止めたりする権利

を謳ったのがGDPR。欧州とやり取りをする企業ではこれに従わなくてはいけないし、第三国へは原則として個人データを持ち出すことができない。

GDPRの定める権利

GDPRの定める主要な権利

- 自分のデータがどう処理されているか知る権利
- 自分のデータの処理について、異議を唱える権利
- 自分のデータを正しく更新する権利
- 正しくない処理が行われているとき、それをブロックする権利
- 不要になったデータや同意を取り消したとき、自分のデータを消去する権利
- 自分のデータを持ち出したり、他の企業に移動する権利

犯罪者のデータをどうするかについては議論がある

ELSIとSTEM

> ELSI: Ethical, Legal and Social Issues(倫理的、法的、社会的課題)

技術的に可能だったとして、それを世に送り出してよいかを議論するもの

> STEM: Sceience, Technology Engineering and Mathematics(科学、技術、工学、数学)

STEM教育が重要視されているが、それと共にESLIも大事。

トロッコ問題

暴走トロッコを

- そのままにしておけば5人亡くなる
- 切り替え機で引き込み線へ起動を変えれば1人が亡くなる

という状況でどうするか？という問題。

情報技術の知識と議論だけでは解決することができない問題。
自動運転などが一般化するときに必ず考えておかなくてはならない。

オプトイン・オプトアウト

意志の示し方についての用語

- オプトイン: 受け入れる
- オプトアウト：拒否する

広告メールの例で考えると

- 広告メールを送ってよいか確認してからOKな人に送るのをオプトイン
- とりあえず送りつけるが拒否する手段が含まれているのがオプトアウト

迷惑メールの規制について

迷惑メールの規制に関して次の二つの法律がある

- 特定電子メールの送信の適正化等に関する法律
- 特定商取引に関する法律

法律によりオプトインが義務付けられました。

データの正義について

機械がやるから公平か？

検索エンジンにおいてYahooが手動の登録であった頃、Googleは

> 検索結果のランキングはアルゴリズムが自動的に決める。だから公平である

という趣旨の発信をしていたが、そんなに簡単ではない。

SEO(Search Engine Optimization：検索エンジン最適化)を行い検索エンジンの上位に表示させるテクニックがある。

検索エンジン

- Webには大量の情報が集まるため、情報の多様性が確保されると考えられていた。
- しかし、大量ゆえに検索エンジンに頼らざるを得ず、
- 検索エンジンの1ページ目にヒョジされない情報はこの世に存在しないかのように扱われる

画像検索の例

一時期

- 「白人 少年」でスポーツやパーティの様子の画像
- 「黒人 少年」で刑務所で取ったような様子の画像

が並んだことがあった。

実際にそのような格差や差別があったとしても、情報技術はそれを固定したり助長したりするのではなく、是正していくことにこそ使われるべきでしょう。

「機会がやるから公平」はただそれだけで成り立つような簡単なものではない。

AIの判断は正しい？

Amazonで人事採用にAIを利用していましたが、AIが女性差別したことがわかり中断された。

AIが過去の男性社会のデータを学んだため、AIに悪意はなく正しくない行動をとってしまった。

データにはバイアス(偏り)があることを自覚しないといけない。

道路標識を誤認させる攻撃

データを捏造や改ざんをすればAIは作った人が想像もしなかった動作をする。

自動運転車はカメラの映像から道路の構造や交通状況を把握するが、標識に簡単なシールを貼るだけで誤認してしまう。

- 標識にシールを貼って自動運転車を混乱に陥れるハッキング技術「Robust Physical Perturbations(RP2)」

敵対的生成ネットワーク

惑わされないようにAIを学習させる手法も出てきている。

ある目的を持つAIとその逆の目的を持つAIを対立させることで、学習効率をあげている。

ディープフェイク問題

トランプ政権が誕生したときにディープフェイクが問題になった。

- 本物のような嘘演説
- 本物のような偽記事

が世界を駆け巡ったが、SNS各社は嘘を見抜くためにAIを活用している。

だからこそ私たちはAIやデータサイエンスを活用しつつも、その取り扱いには最新の注意を払う必要がある。

人間中心のAI社会原則

内閣府がこうした事態に対応するために公表したガイドライン

- 人間中心の原則
- 教育・リテラシーの原則
- プライバシー確保の原則
- セキュリティ確保の原則
- 公正競争確保の原則
- 公平性、説明責任、及び透明性の原則
- イノベーションの原則

人間中心のAI 社会原則 - 内閣府

まとめ

AIは複雑でその学習も自動的に行われるため、作った人にとっても中身がよくわからない**ブラックボックス**になっていると言われることがある。

しかし、AIを使って行われるサービスや製品にも責任が求められることは明らか。

わたしたちAIに触れ、作り出すときには

> 公平性・透明性・説明責任・プライバシー・セキュリティ

を正しく実装しなければなりません。

同時に、使う立場に立ったときにもこれらが守られているか見極めるスキルを持つことが重要。