

| 10:10 - 11:20 セッション2

AI×法・倫理シンポジウム

セッション2 AIと法律・倫理のチュートリアル

登壇者 古川直裕 (株式会社ABEJA 弁護士)

はじめに

古川 直裕

株式会社ABEJA 所属

弁護士（62期） 情報処理安全確保支援士 スクラムマスター

2016年から約3年間AI業務に従事

うち2年間は、AI開発チームを立ち上げ、主に画像解析PJの企画、データ収集、前処理、コードの実装など

モデル開発の全業務を担当。

AI開発チームのマネジメントや採用なども。

3年間全期間を通じて、基礎数理や理論研究に従事。

セキュリティ業務は現在も従事

研究活動

- ・ AI法研究会代表
- ・ 日本ディープラーニング協会
- ・ 「AIガバナンスとその評価」 研究会研究員
- ・ 「契約締結におけるAI品質保証の在り方」 研究会副座長
- ・ 「AIデータと個人情報保護」 研究会研究員

はじめに

著作（AI関係のもの）

- ・論文「機械学習システム開発における法務」NBL1119、1121、1123号
- ・論文「機械学習システムの法務・コンプライアンスリスク」NBL1146、1149、1150号
- ・座談会「法務部門・法律家のELSIへの取り組み方」（ビジネス法務2021年7月号）
- ・書籍「サイバーセキュリティ法務」（2021年 商事法務）
- ・書籍「Q&A AIの法務と倫理」（2021年 中央経済社）

連絡先

nf0825ml@gmail.com



はじめに

caution△注意△caution

ベンダ（受託者）側の人間ですが、
古川は、以前ユーザ（委託者）側に所属していたことや、
ベンダも下請けに出すことが多く委託者になることも多いので、
ベンダ寄りの見解という意識はないです。

言いたい放題言う可能性があります。
全く所属する会社の見解ではなく、個人の見解です。
所属するABEJAの代表者が委員を務めた経産省のガイドラインに
批判的であったりします。

| 本日の話題

はじめに

- 1 AI技術説明
- 2 AI開発の流れと特徴
- 3 AI開発契約
- 4 AI倫理
- 5 AI案件に対する法務の在り方

1 AI技術説明

◆AI開発のパイプラインは？

- ① データ収集
- ② データ前処理及び特徴量選択
- ③ アルゴリズム選択
- ④ 学習
- ⑤ 評価
- ⑥ ハイパーパラメータチューニング

| 1 AI技術説明

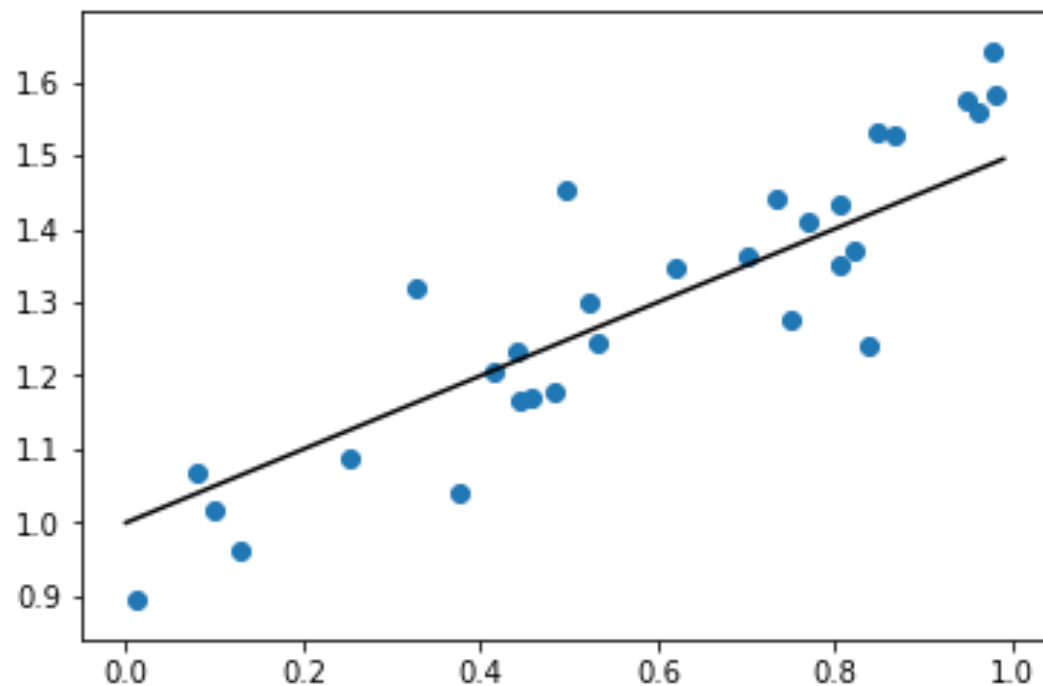
◆データの種類の一例

- ・ 構造化データ (TABデータ)
テーブル構造 (表形式) のデータ
- ・ 画像データ
- ・ テキストデータ (自然言語データ)
- ・ 音声データ
- ・ 動画データ
- ・ 時系列データ

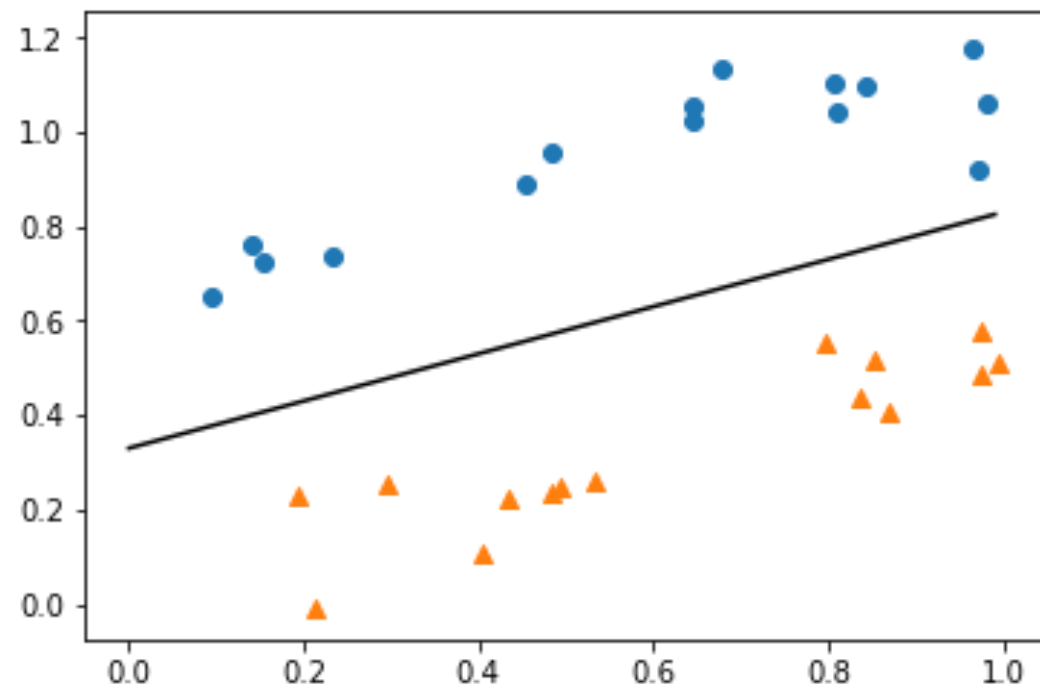
1 AI技術説明

◆タスクの種類

回帰 (教師あり)



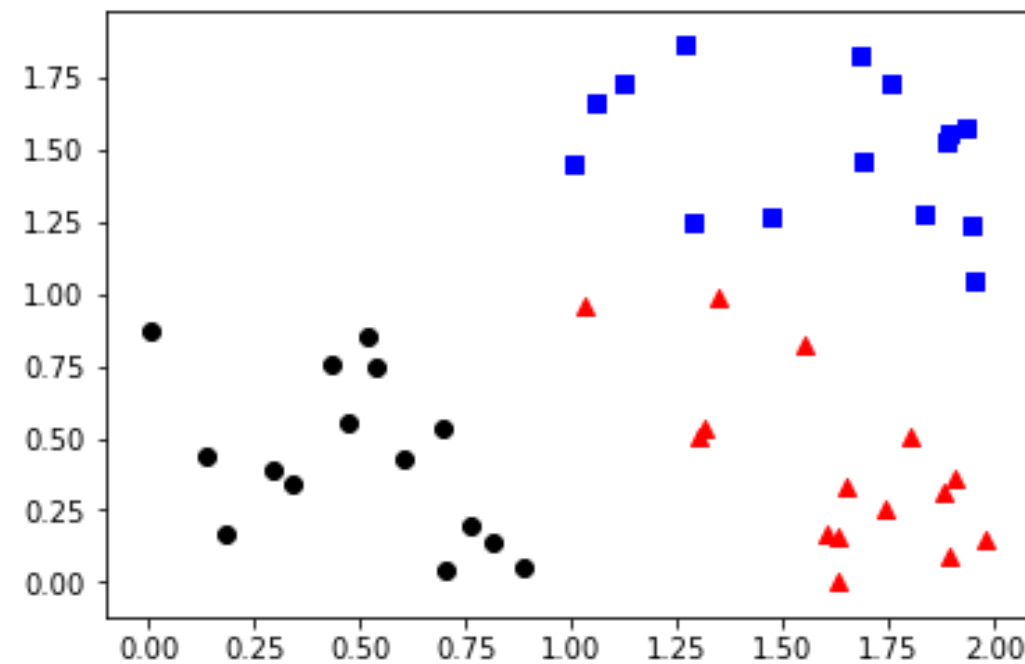
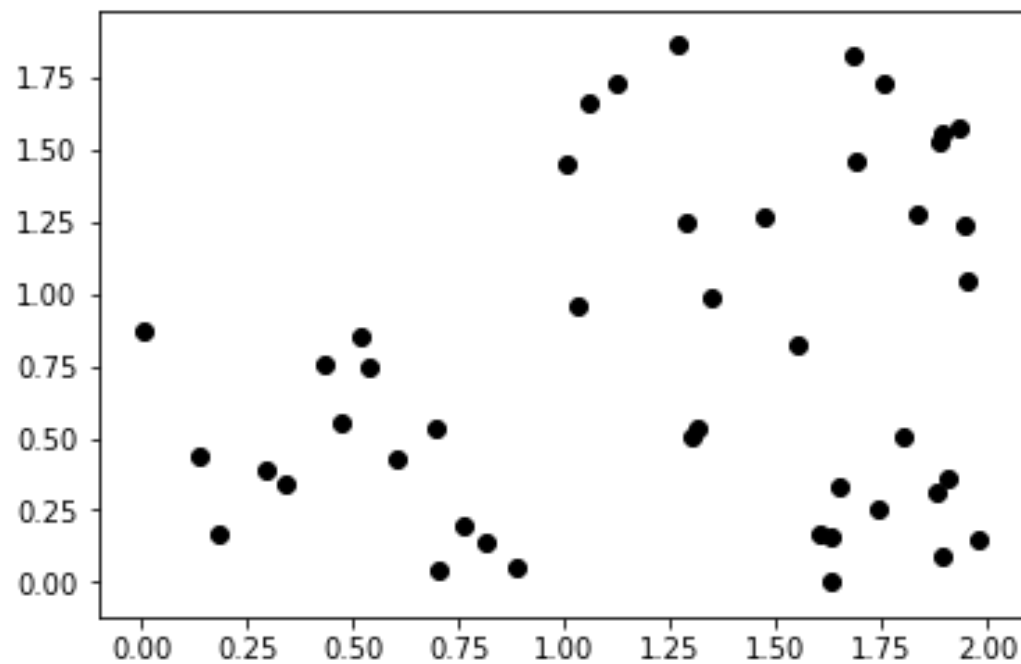
分類 (教師あり)



1 AI技術説明

◆タスクの種類

クラスタリング (教師なし)



1 AI技術説明

◆タスクの種類

生成 (教師なし)



Tero Karras, Timo Aila, Samuli Laine, Jaakko Lehtinen "Progressive Growing of GANs for Improved Quality, Stability, and Variation"



<https://en.wikipedia.org/wiki/Deepfake>

1 AI技術説明

◆ベクトルと行列

ベクトル

数字を並べて括弧で一つにしたもの (1,5) など。

身長175cm、体重65kgというデータをベクトルで表すと・・・ (175, 65)

身長・・・男性というデータをベクトルで表すと・・・ (175, 65, 0)

ただし男性=0, 女性=1と表す

データをベクトルで表せる！！！！

行列

ベクトルを合わせたもの  $\begin{pmatrix} 175 & 65 & 0 \\ 170 & 55 & 1 \end{pmatrix}$

行列によりデータセットを表現することができた！

後は、行列やベクトル計算（線形代数）を行うだけ
画像や自然言語データもベクトル・行列で表現可能

1 AI技術説明

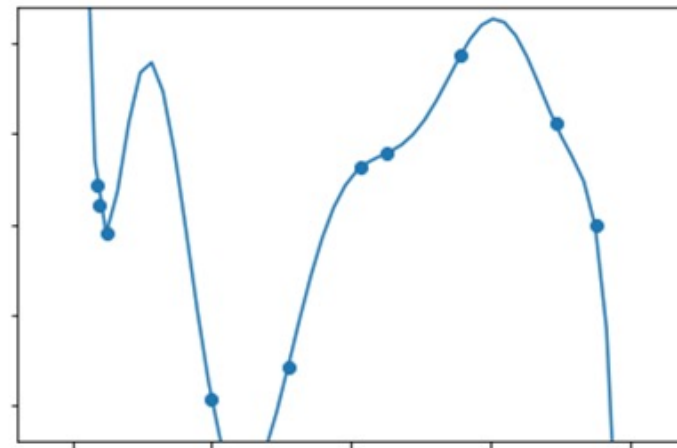
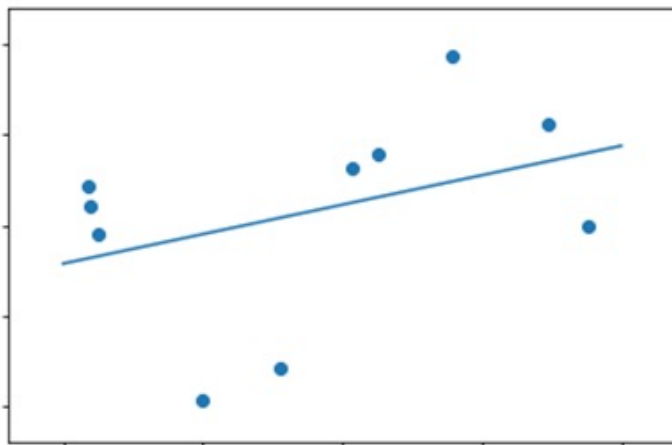
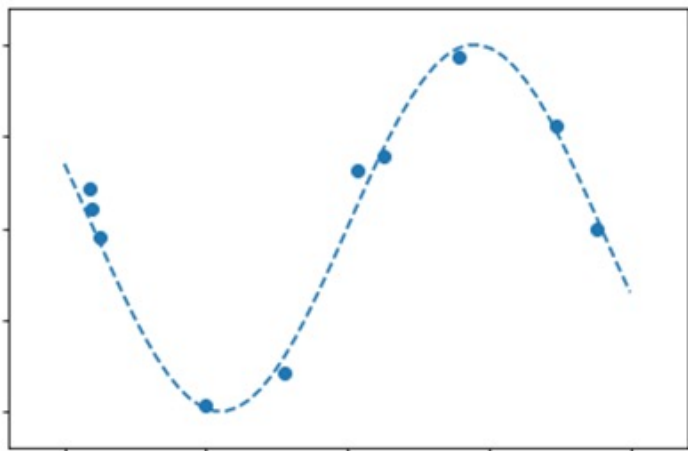
◆評価と過学習（overfit）

試行錯誤して精度の高いモデルを作りたい。→モデルの精度を測る必要がある。

学習用データでモデルの精度の測定は×

手持ちデータセットを学習用と測定用（テスト用）に分け、テスト用データセットで測定することが必要。

過学習かをよく検討しながら評価を行う。



1 AI技術説明

◆開発例紹介

- ・今回使うのは、Kaggleのタイタニック・データセット
- ・構造化データで、性別や年齢などの特徴から生存者かを予測する。
- ・特徴として、データ数が少ない、特徴の数が少ないという特殊性があるが、行う作業自体は、AI開発のパイプラインそのものである。

- ①データ収集（今回は収集済み）
- ②データの前処理及び特徴量選択
- ③アルゴリズム選択
- ④学習
- ⑤評価
- ⑥ハイパーパラメータチューニング

| 1 AI技術説明

開発実演中

| 1 AI技術説明

◆開発例紹介

タイタニック・データセットから得られた知見のまとめ

- ・ 前処理、特徴量選択におけるドメイン知識の重要性
- ・ 前処理、特徴量選択、アルゴリズム選択の組み合わせが膨大であり、ベンダのノウハウによるところが大きい。
- ・ 事前に精度は分からない。精度を上げるための試行錯誤の重要性
- ・ 学習用コード、推論コード、学習済みパラメータ（ファイル）、AIの出力のイメージを持った

1 AI技術説明

◆AI提供の方法の分類

様々存在するが多い2つを紹介

- ・ **受託開発型** ：システム開発のように相手方企業の要望するAIを開発する形式。
納品物は、様々なドキュメントに加えて、
推論用コードや学習済みパラメータファイル。
ただし、場合により、
AIの推論用コードや学習済みパラメータファイルを提供せずに、
クラウドサーバ上にこれを展開してAI機能のみ提供することもある。
- ・ **SaaS提供型** ：AIサービス提供企業においてAIを開発してクラウド上に展開する。
顧客にはAIの機能のみ提供する。
つまり、顧客はコードなどは得ず
データを入力すれば出力を得らえる機能のみ提供される。
場合により、顧客側のデータを追加学習させることで、
学習済みパラメータを顧客向けに変更できることもある。

| 2 AI開発の流れと特徴

◆通常のシステム開発と比較して

- ①やってみるまで分からない
 - ②試行錯誤が必要
- という特殊性認められる

つまり？

- ①やってみるまで分からない
 - 事前に計画や要件定義しきることが難しいところがある
- ②試行錯誤が必要
 - 何度も味見して開発を進めてゆく

このため

- ①最初に「ちょっとやってみる」フェーズをいれる
- ②実験を繰り返すフェーズをいれる

2 AI開発の流れと特徴

◆通常のシステム開発の超概要

ここではウォーターフォールを想定

要件定義 → 設計 → 実装 → テスト

ポイントは、要件定義をしっかりと行い、手戻りを発生させないこと

要件定義とは??

→ 事前にどんなシステムが欲しいかしっかり決めておく

- ・システム概要
- ・システム導入目的
- ・業務フロー
- ・機能要件
- ・非機能要件

(何を書くかは、流儀により若干の差異)

| 2 AI開発の流れと特徴

◆AI開発は・・・

アセスメント → PoC → 開発 → 追加学習

という4つのフェーズに分ける。

2 AI開発の流れと特徴

アセスメント

開発に必要な事項を定めるため、ちょっと分析してみる

具体的には・・・

- ・ ビジネス上の課題を抽出する（検品精度を向上したい）
- ・ 課題を具体化しKPIを作成する（検品エラー率1%以内）
- ・ KPI実現のための手法を考える（AIシステムは手段の一つ）
- ・ AIシステムを手段とする場合（画像解析を用いて検品）
 - どのようなデータを用いて
 - どのようなシステムを作るか検討する
- ・ PoCで検討すべき問題点や目標精度を確定する
- この際に簡単なAIを作成する
- ・ 業務フロー等の設計を行う
- ・ 計画書や報告書を作成する

| 2 AI開発の流れと特徴

PoC

モデルを作成し、ユーザとともに問題点等を検討
→ モデルを作り直す・・・を2, 3回繰り返す
モデル作成時に試行錯誤さらにユーザとともに試行錯誤する

その意味で**正に試行錯誤**のフェーズ

ここで、様々な問題点の検証や目標精度が実現できそうか、
具体的なシステム開発時に検討すべき事項等を具体化する。

一言でまとめると、開発すべきかを考えるフェーズ
要は、味見

| 2 AI開発の流れと特徴

開発

システムを開発するフェーズ
要件定義を行い、設計等も行い、実装する。
基本的には通常システムと変わらない。

ただ、本番システム用AIの学習と、
AIとシステムの統合というプロセスが存在する。

| 3 AI開発契約

経済産業省より

「AI・データの利用に関する契約ガイドライン」が出されている。

色々あるが、基本的にはガイドラインの内容に沿って解説していく
ただし、私的見解も述べる。

◆ テ AI開発契約 契約形式（請負・準委任）

やってみるまで分からない性格のため準委任を推薦するのがガイドラインの考え。

ただし、開発フェーズについては請負も排除していない。

アセス、PoCが準委任というのは、ほぼ確定。

問題は開発フェーズ。仮に請負で契約するには工夫が必要か。

まず、そもそも請負による完成合意の内容を検討する必要がある。

精度等を問わないが、

一定の入力形式・一定の出力形式を持つモデルであれば請負が可能なことが多い。

問題は精度や速度についての保証にある。

請負契約を利用するという根拠は、

PoCを経てある程度精度が見えてきたのだから、保証できるので請負という考え。

3 AI開発契約

◆テーマその2 知的財産

特許権

対象になり得るのは主に

- ・ AI化
- ・ **アルゴリズム**
- ・ AI作成パイプラインの技法（前処理方法、評価方法など）

後2つの特許については検討が必要

ベンダが発明した場合に話を限定する

- ▶ アルゴリズム等は以前から研究していないと発明できない
- ▶ アルゴリズム等の特許権をユーザが有していないとシステムを安心して利用

でき

ない？？？ユーザは何に特許を使う？

- ▶ 新しい技術を利用するインセンティブ
- ▶ 報酬を払っているから当然ユーザに帰属？？

どちらにせよ、利用権を適切に設定する方向でよいと思う。

3 AI開発契約

◆ テーマその2 知的財産

著作権

対象になり得るのは

- ・ ソースコード
- ・ DB
- ・ 学習済みモデル ???

ソースコード

- ▶ 全部ユーザは無理
- ▶ 以前からベンダが有しているものと第三者の著作物 → 留保せざるを得ない。
- ▶ そもそも、大量のOSS等を利用しているのが現実であり、どのような著作権が成立するのか検討する必要あり
- ▶ なぜ著作権が欲しいのかよく考えて、必要な限度で利用検討を設定してゆくのが建設的

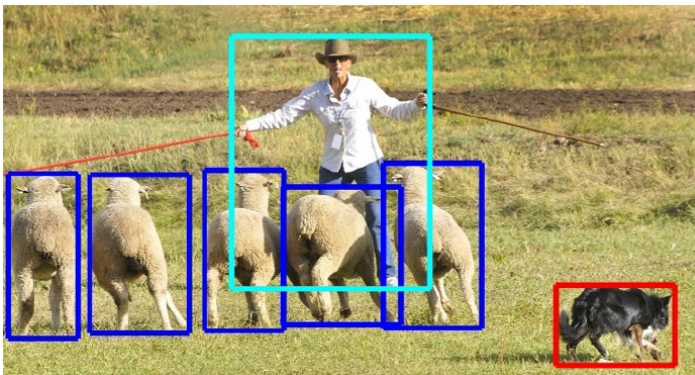
3 AI開発契約

DB

- ▶ DB著作権が理論上は問題
「情報の選択又は体系的な構成」に創作性あればDB著作権
- ▶ 生データにユーザ等のDB著作権が成立するか？
→ Yesなら学習用データセットのDB著作権もユーザ等が普通
→ Noなら・・・

学習用データセットに発生するのは、かなりレアか？？
前処理や特徴量選択からDB著作権が認められるか？

- ▶ 注意 アノテーションで著作権が発生することはかなりレア



Tsung-Yi Lin, Michael Maire,
Serge Belongie, Lubomir
Bourdev, Ross Girshick,
James Hays, Pietro Perona,
Deva Ramanan, C.
Lawrence Zitnick, Piotr
Dollár "Microsoft COCO:
Common Objects in
Context"

| 3 AI開発契約

学習済みモデル???

- ▶ そもそも何を意味しているのか？
- ▶ 学習済みパラメータを含むことには、ほぼ争いがない。
- ▶ 推論用コード、学習用データセット、学習用コードを含むかについては不
明確なと
ころがある。このため、契約書で定義しておく必要。

- ▶ 注意するべきは、著作権の議論においては、
あくまで、どのファイルかということを考えること。
抽象的に学習済みモデルなるものが存在するわけではない。
理論としては、学習済みモデルという言葉を使う意味はない。
- ▶ なお、学習済みパラメータには著作権は成立しない。
コードやデータセットについてはすでに述べたとおり。

| 3 AI開発契約

◆テーマその3 保守と再学習

ガイドラインでは少ししか触れられていないが、
実際にシステムをデプロイしたときには重要になる。

保守の注意点

保守業務として何を想定しているか？

- ①問い合わせ対応
- ②不具合調査・対応
- ③稼働状況の監視
- ④障害対応

等々

| 3 AI開発契約

再学習の注意点

どのレベルまで再学習を委託するか？

- ①追加データの学習
- ②ハイパーパラメータ調整
- ③アルゴリズム・アーキテクチャの再設計
- ④特徴量再設計
- ⑤出力再設計

等々

レベルによりモデルの再作成に近くなる

モデルの再作成に近ければモデル開発契約と同じような契約
単なる保守に近ければ保守契約の中で実施

→ 保守契約の中で、どこまでの再学習を行うか具体化の必要
月額で対応できるのは、せいぜい①か②までか

| 3 AI開発契約

このあと12：20からの
セッション3 「AI利活用における法務・知財・契約」では
より実務的な問題を検討します！

お楽しみに！！

| 4 AI倫理

AI倫理は、近年の最重要テーマ
論文等の数も急激に増えており、学会でのワークショップ数も急増中
そもそも、AI倫理の定義は??

特に定まっていないうえに、どのように定めるかの議論も余り存在しない。

ここでは、**自律的（自律的ということの意味はさておくとして）な意思決定がAIが有すべき倫理の内容やAIに倫理を持たせるための手段に関する問題領域、と定義しておく**

◆AI倫理の重要性を示す最近の事例紹介

1件目 アメリカにおける顔認識技術

顔認識技術とは??

顔画像を入力すると顔画像DBから同一の顔画像を探し出す。DB上の顔データで

は名前が分かっているならば、名前もわかる!

例えば、顔画像をベクトルに変換し近い数値のベクトルを同一人物と判定する。

今年6月、アメリカの大手IT企業が相次いで顔認識技術の提供を制限しだす。

各社の状況

Amazon ……1年間警察への提供を中止

Microsoft ……同上

IBM ……顔認識から撤退

Google ……2018年に技術的・倫理的問題が解決するまで

汎用顔認識には参入しないと決めている

| 4 AI倫理

◇顔認識技術の倫理上の問題点その1 プライバシー

2019年にはサンフランシスコ市で、
公的機関が顔認識技術を利用することを禁止する条例を施行

4 AI倫理

◇顔認証技術の倫理上の問題点その2 公平性・バイアス
非白人や女性の誤認識率が白人・男性と比べて高い

Table 1: Overall Error on Pilot Parliaments Benchmark, August 2018 (%)

Company	All	Females	Males	Darker	Lighter	DF	DM	LF	LM
Target Corporations									
Face ++	1.6	2.5	0.9	2.6	0.7	4.1	1.3	1.0	0.5
MSFT	0.48	0.90	0.15	0.89	0.15	1.52	0.33	0.34	0.00
IBM	4.41	9.36	0.43	8.16	1.17	16.97	0.63	2.37	0.26
Non-Target Corporations									
Amazon	8.66	18.73	0.57	15.11	3.08	31.37	1.26	7.12	0.00
Kairos	6.60	14.10	0.60	11.10	2.80	22.50	1.30	6.40	0.00

Inioluwa Deborah Raji, Joy Buolamwini “Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products”

4 AI倫理

サービス停止の背後にはBLM運動の存在

まとめ

公平性に関する問題を脇においた結果、
大量のカメラを持つ重要な顧客を失い、
（おそらく）警察のための投資が無駄になった。

4 AI倫理

2件目 COMPAS事案

COMPASという裁判所で用いられるシステムが
刑事被告人の再犯リスクを予測する機能を持っていた。
この予測に白人・黒人でバイアスが存在していた。
リスクの高低の正解率は、ほぼ同じであったが間違え方にバイアスが存在した。

	WHITE	AFRICAN AMERICAN
Labeled Higher Risk, But Didn't Re-Offend	23.5%	44.9%
Labeled Lower Risk, Yet Did Re-Offend	47.7%	28.0%

<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

| 4 AI倫理

◆政府等による取り組み

- ・ EU Ethics guidelines for trustworthy AI
 - ①人間中心と人間による監督
 - ②技術的頑健性と安全性
 - ③プライバシーとデータガバナンス
 - ④透明性
 - ⑤多様性、平等、公平
 - ⑥社会的・環境的Well-being
 - ⑦アカウンタビリティ
- ・ OECD Recommendation of the Council on Artificial Intelligence
- ・ IEEE ETHICALLY ALIGNED DESIGN First Edition
- ・ 内閣府による「人間中心のAI社会原則」
- ・ 総務省による「AI利活用ガイドライン」

| 4 AI倫理

Google、IBM、富士通、SONYなど
様々な企業でもAI倫理に関するポリシーを制定して、公表している。
ただし、ガイドラインやポリシーの内容は似たり寄ったりになっている。

この点については、
Anna Jobin, Marcello Lenca, Effy Vayena
“Artificial Intelligence: the global landscape of ethics guidelines”
参照

いま求められているのは、具体的に何をするかの検討や具体的にAI倫理に向けて
施策を打つこと

| 4 AI倫理

◆AI倫理の重要性

- ① せっかく作ったプロダクトが停止になる
- ② 顧客を失う
- ③ 企業の評判が悪くなる
 - 他のプロダクトへの影響
 - 採用への影響
 - 上場審査での影響
 - 銀行融資での影響
 - ・・・等々

コンプライアンスとの近似性

| 4 AI倫理

AI倫理上問題になる様々な点や尊重すべき原則、
問題となった事例また世界的な動向については

セッション4

顔認識に関する具体的事例をもとに
具体的にどうすればよいかを検討については

セッション5

お楽しみに！！

| 5 AI案件に対する法務の在り方

◆持つべき意識

- ・ **AIプロジェクトに求められるスピード感**

リーンスタートの考え方、最初に勝った者が勝ち続ける傾向

- ・ **情報の共有に対する意識**

多くの重要技術が論文で公開され、実装も公開されている
データは使って初めて意味がある

- ・ **法的点のみの最適化から脱却する**

どれだけの価値を生み出すPJかを理解しているか？
契約書審査時間と技術的寿命を考えているか？

- ・ **ビジネス、技術に関する理解**

技術者がドメイン側のビジネスを熱心に勉強している現実
統計数理の専門家もプログラムを熱心に勉強している現実

| 5 AI案件に対する法務の在り方

◆AI倫理への法務のコミットについて

- ・ 平等、プライバシーなどは明らかに法律的概念
- ・ コンプライアンスとの近しさ
- ・ 問題対象が規範的要素
- ・ 法務関係者がコミットする意味 法務機能の転換
これからは様々な製品にAIが搭載される
AIの性能が製品の優劣を決める
倫理的要素がAIの品質とされている現実

→法務が売れる商品を作る時代となる

| さいごに

◆ AI法研究会とは

- ・ AIが普及するための法的・倫理的基盤の構築を目的としている私的な研究団体。
- ・ 弁護士等の法律関係者や法律学者を中心としている。
- ・ 技術者、PM等の参加もWelcome！！
- ・ これから様々な研究テーマを扱っていくので、AIに詳しくなくてもAIに興味があるのなら、参加してください。
- ・ 詳しくは、「AI法研究会」で検索して、連絡先にメールしてください！
少しお時間を頂戴するかもしれませんが、参加ご案内をお送りします。