3-9　AIの構築・運用

東京大学 数理・情報教育研究センター
2021年4月30日

概要

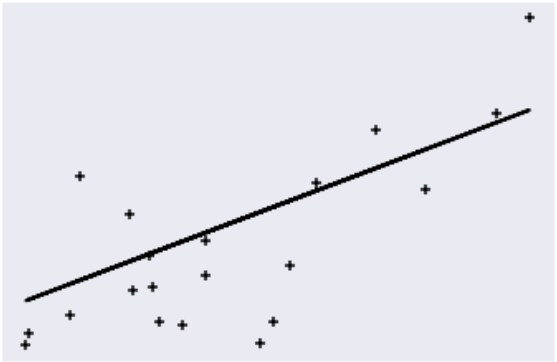
- 本節では
  - 複数のAI技術が組み合わされたAIサービス/システムの例を説明できる
  - AIの運用と品質保証について説明できる
  - 今後、AIが社会に受け入れられるために考慮すべき論点を理解する
- ことを目標とします。

本教材の目次

AIシステムの開発とAIの学習

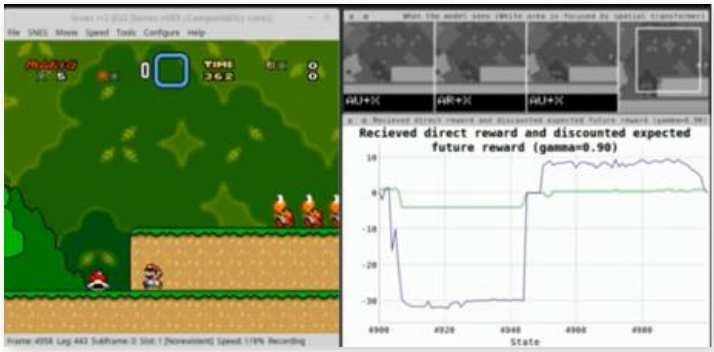
- AIはビッグデータからパターンを学習します。学習シナリオはいくつかの種類に分類できます。
- **教師あり学習**：データの中で予測対象となる特徴量（正解データ）と予測の元になる特徴量の区別が明確な場合。
- **教師なし学習**：上記区別がない場合。
- **強化学習**：ゴールを達成する上でどのような行動の決定の仕方（ポリシー）がよいか経験によって獲得する手法。

教師あり学習の例（回帰問題）



教師なし学習の例（クラスタリング）

強化学習の例（ゲームのコントロール）



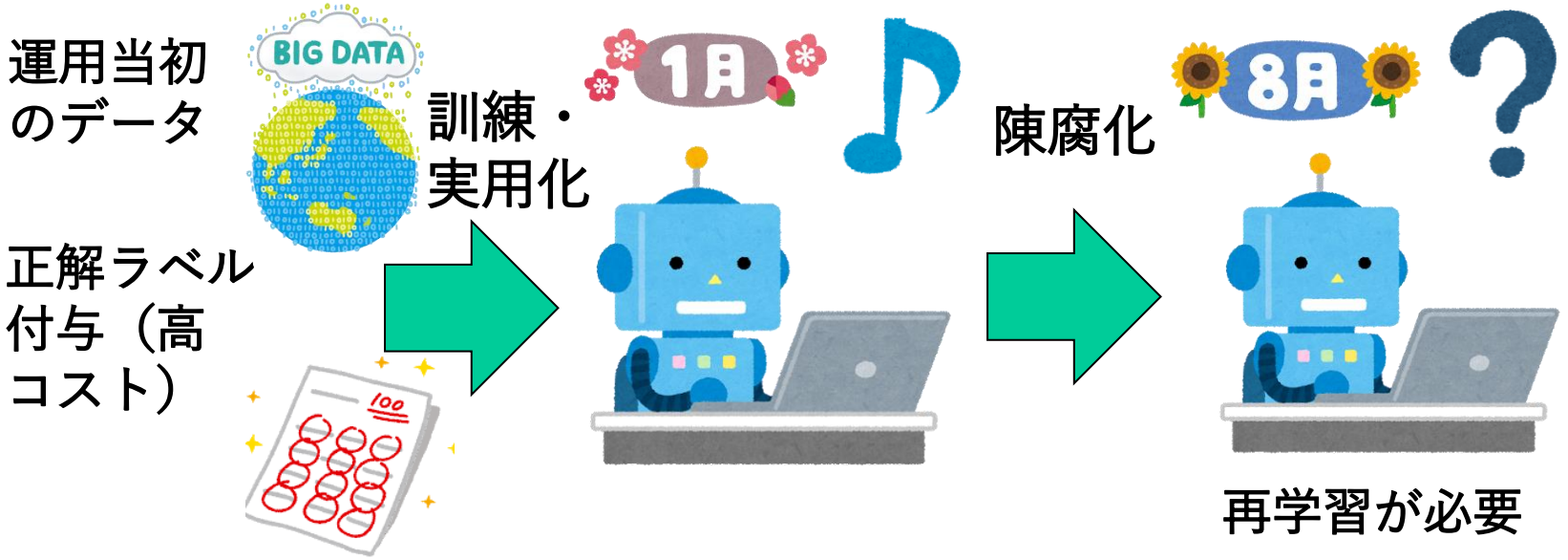
https://github.com/aleju/mario-ai)
https://www.youtube.com/watch?v=L4KBBAwF_bE

AIの評価とテスト

- 教師あり学習であればテストデータでの予測精度や仮説を従来手法と比較する比較実験を通じて評価できます
  - 後者はABテスト（ランダム化比較試験）と呼ばれます
- 教師なし学習であれば学習結果の解釈性に注目したり学習結果が他のタスクで有用かを検証したりすることで評価できます。
- 強化学習なら機械が目標を達成できるか実際機械にやらせてみることも可能です。
  - もちろんゲームなら何度失敗してもよいですが、自動運転車を公道で検証する際などは取り返しがつかなくなることもあるので注意が必要です。

再学習

- AIを運用する時に過去に訓練したモデルをそのままずっと用いればよいわけではありません。時間が経つにつれ訓練したモデルは陳腐化します。
- 時系列データなど時間によってデータが増えていく場合は近々のデータに重きを置くこともできますが、そうでない場合は新たにデータを得て再学習する必要があります。
  - 新たにデータを取得し正解ラベルをつけるのは非常に手間です。再学習の負担を減らそうと様々な試みが行われています。

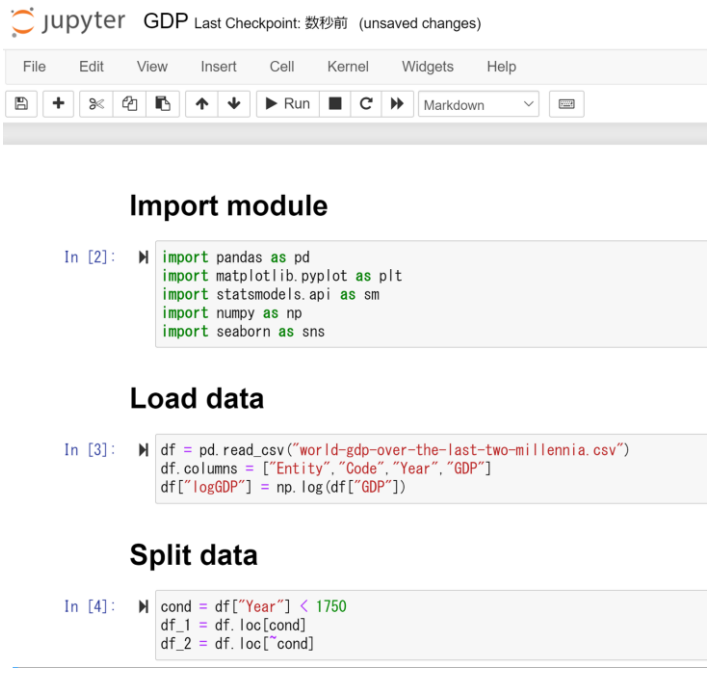


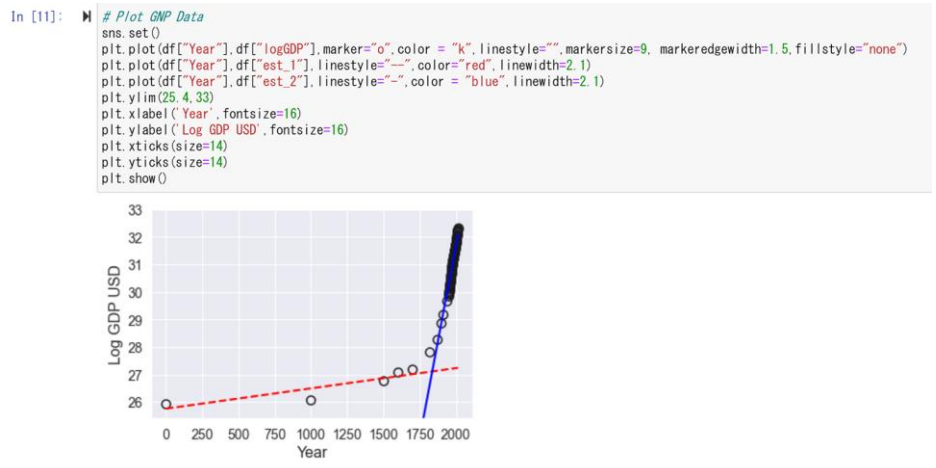
転移学習

- 自然言語処理・画像解析・ネットワーク解析などではビッグデータを用いて深層学習モデルを訓練することで強力なモデルを作ることができます。
  - 言葉の使い方や物体、ネットワークの認識の仕方はデータによらない部分があります。
- 他社によって事前に訓練されたモデルを自分のデータにファインチューニングすることで、自分が保有しているデータだけでは到達できないパフォーマンスを出せることがあります。
  - 転移学習の一例です。
- 事前訓練済みのモデルは様々なサイトで公開されています
  - https://tfhub.dev/
  - https://huggingface.co/

AIの開発環境

- Python、Go、Scala、R、Haskell、Julia、C/C++、Javaなど様々なプログラミング言語を用いてAIはプログラミングされます。
- 事前コンパイルが不要で逐次結果を出力できる言語の場合はNotebookを用いることが多いです。そうすることでコードと結果をひとまとめにできます（下図参照）
  - Jupyter Labなど





AIの開発環境

- 複数人でコード開発を行う場合はGitなどのバージョン管理システムを用いると便利です。
- コードを公開する手段としても用いられます。
  - githubやbitbucketなどが有名です。

Github
https://github.com/

Bitbucket
https://bitbucket.org/product/

AIの開発環境

- 深層学習のモデルは自分で完全に一から書くのは大変です。そのため深層学習のモデルを構築しやすいように様々なライブラリが公開されています。
  - Tensorflow、Torch
  - 前述の通り事前訓練済みのモデルも多く公開されています。

- 機械学習モデルの開発タスク自体を自動化する試みもあります
  - 自動機械学習とは問題設計を与えるだけで、基本的な分析や様々な機械学習のモデルを自動で計算してくれるツールのことです。
  - GoogleのAutoML(https://cloud.google.com/automl)
  - MicrosoftAutoML(https://docs.microsoft.com/ja-jp/azure/machine-learning/concept-automated-ml)

ビジネス/業務への組み込み

- ビジネスへのAIの組み込みも進んでいます。例えば問い合わせ業務の効率化のためにチャットボットを導入する企業が増えています。
  - 簡単な問い合わせは機械に任せ難しいもののみ人間が応対します。
- 同様の技術はスマートスピーカーやAIアシスタントにも活用されています。
  - 両方とも複数のAI技術を活用したシステム（音声処理、テキスト処理、IoT）といえます。

ビジネス/業務への組み込み

- 掃除ロボットなど身近に使えるロボットの開発も盛んです。
- 最近の掃除ロボットはどの場所にごみは落ちていることが多いかなど情報を自ら収集することによって、短時間で効率的に掃除できるように学習します。

掃除ロボットの例
https://www.fnn.jp/articles/-/3848

ビジネス/業務への組み込み

- 化学の探索的な実験の自動化を試みる企業もいます（IBM RobotRXN）
  - 機器の洗浄から実験結果の測定までを１つのサイクルとしてプログラミングすることによって、面倒くさい作業をロボットに任せることができるようになります。

IBM RobotRXN

https://youtube.com/watch?v=ewE1wh7sTUE

ビジネス/業務への組み込み

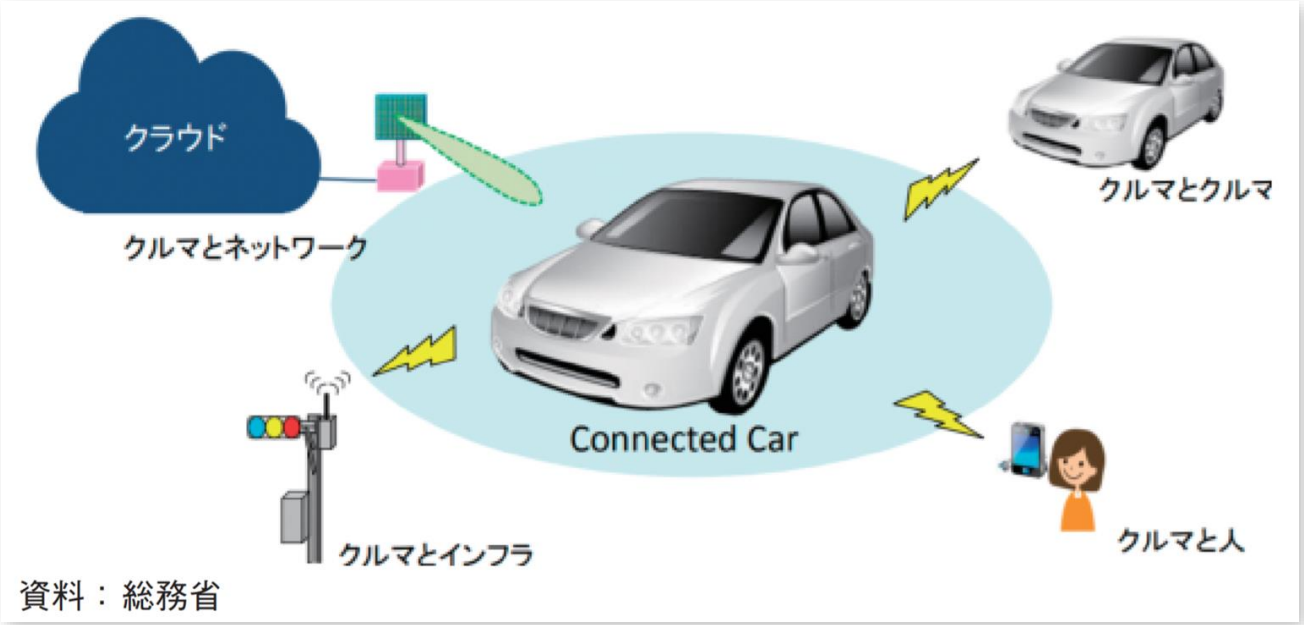
- クリエイティブ支援ツールは広告やゲーム開発など様々な業界で役立てられています。
  - 電通はAIに広告のキャッチコピーを生成させるソフトウェアを発表しました。
  - Preferred Networksはアニメキャラの自動生成サービスを提供し話題になりました。

電通AICO
https://www.dentsu.co.jp/business/case/ai_planners.html

PFN
https://www.preferred.jp/ja/news/pr20190403/

AIの社会実装

- AIの社会実装としてわかりやすいのが自動走行車です。
- 各車のセンサー情報を共有することで様々なサービスを提供できます（1章１節参照）
  - コネクテッドカー



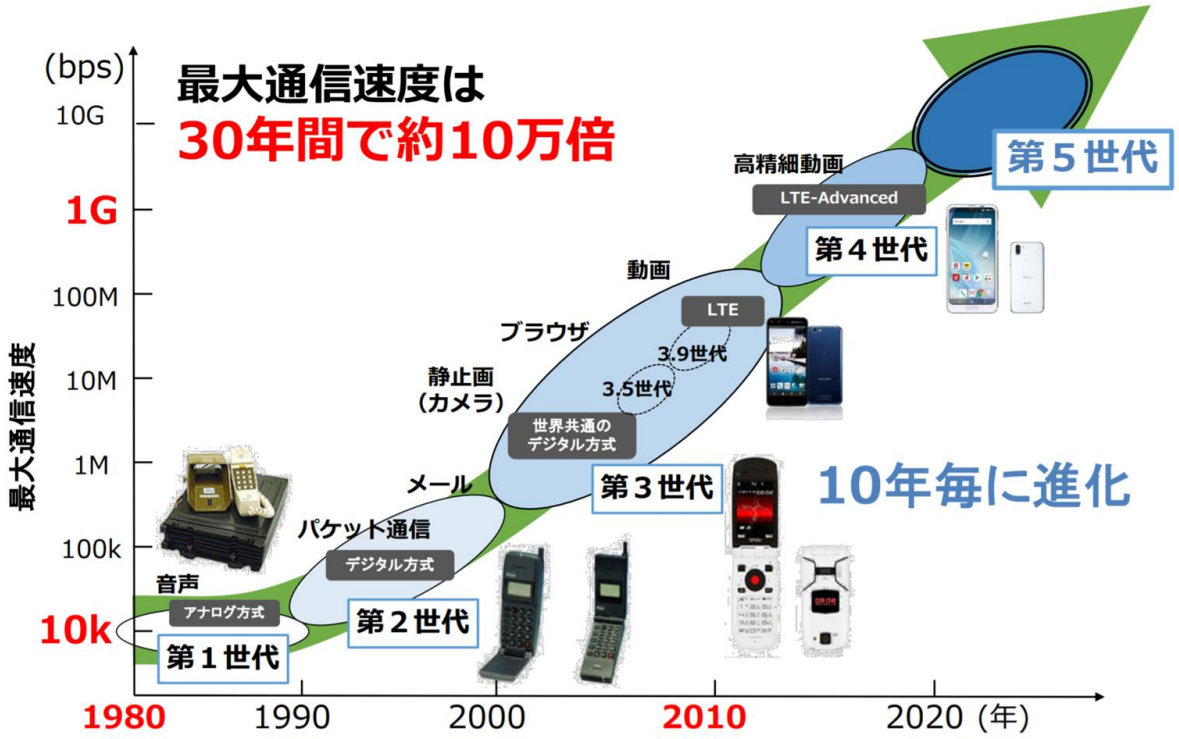
https://www.mlit.go.jp/common/001294514.pdf

ハードウェア技術の進化

- AIの社会実装を進める上でハードウェア技術の進化が重要なのはいうまでもありません。
  - 処理性能の向上➔CPU、GPUの進歩
    - 深層学習はGPU技術の進歩に支えられています。
  - 記憶装置の進化➔メモリ、HDD、SSD
- エッジコンピューティング：簡単な計算処理はスマホなどに搭載されている簡易計算機で計算し、複雑な処理は計算処理能力のもっと高い計算機で計算する分散コンピューティング技術です。
- FPGA（Field Programmable Gate Array）：CPUやGPUは入力するコードによって汎用的な論理回路内でロジックを構成します。これに対して問題設定によって論理回路自体を書き換えることでパフォーマンス向上させることができる集積回路のことです。

通信環境

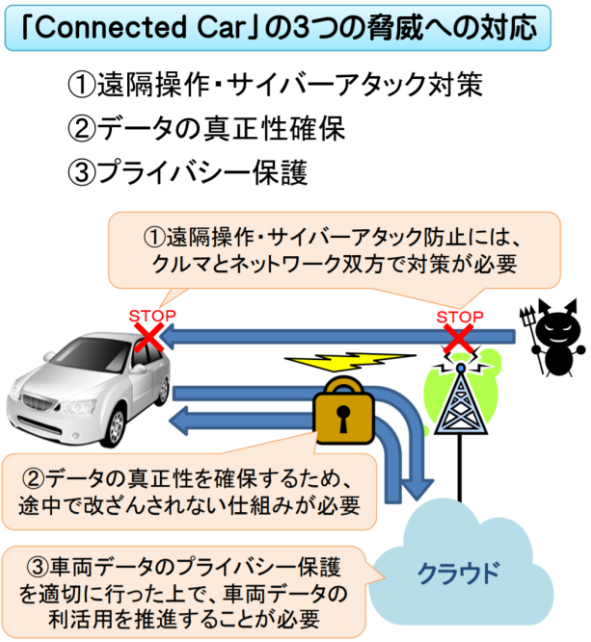
- 通信環境に関しても徐々に最大通信速度は速く、容量は大きく、回線は太くなっています。
  - ５Gのスマートフォンも増えています。



https://www.soumu.go.jp/main_content/000633132.pdf

セキュリティとプライバシー

- セキュリティ対策は今後益々重要になってきます。
  - コネクテッドカーのセキュリティが破られた場合：(1)遠隔操作 (2) データの改ざん(3) プライバシー保護など様々な問題が生じます。
- セキュリティ分野でもデータサイエンス的アプローチをとることもあります。



NICT NEWS 2018 No.6サイバーセキュリティの研究開発最前線 参照

https://www.soumu.go.jp/main_content/000492421.pdf

フェデレーテッドラーニング、秘密計算

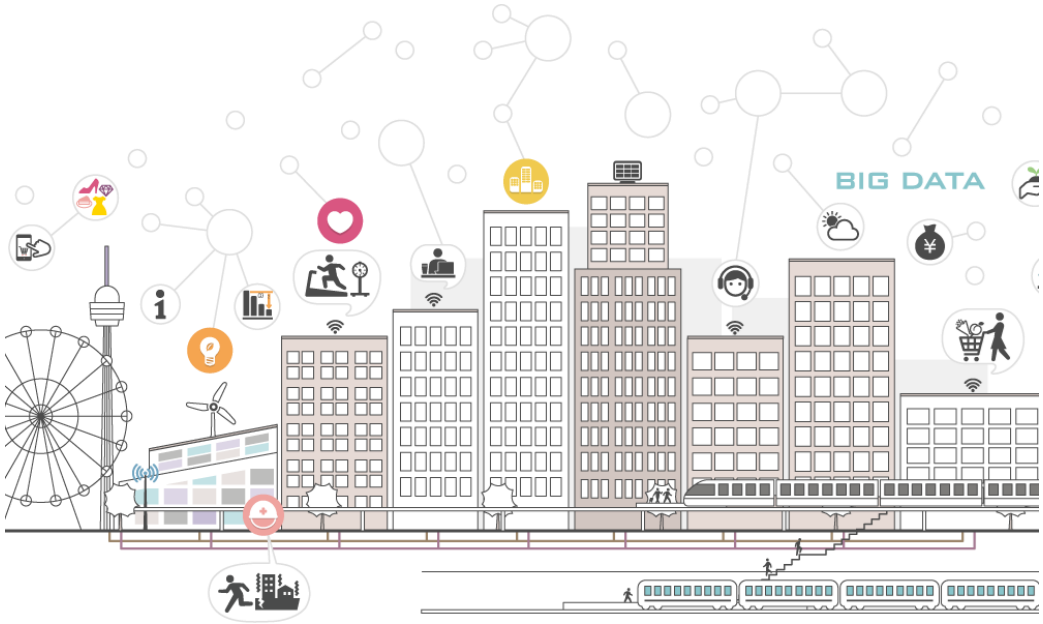
- プライバシー保護のために様々な技術が開発されています。
  - フェデレーテッドラーニングではデータではなくモデルを共有することでプライバシーを守ります。
  - 秘密計算ではデータを暗号化したまま処理することでプライバシーを守ります。

フェデレーテッドラーニング
https://www.youtube.com/watch?timecontinue=56&v=Jy7ozgwovgg&feature=emb_title

秘密計算
https://www.rd.ntt/sc/project/data-security/secure_computation.html

スマートシティ、スーパーシティ

- こうした様々な技術を組み合わせ町ごと未来社会にしようというのがスマートシティやスーパーシティです。
- 将来的には自動車に目的地を伝えるだけで安全に連れていってくれる未来がくるかもしれません。



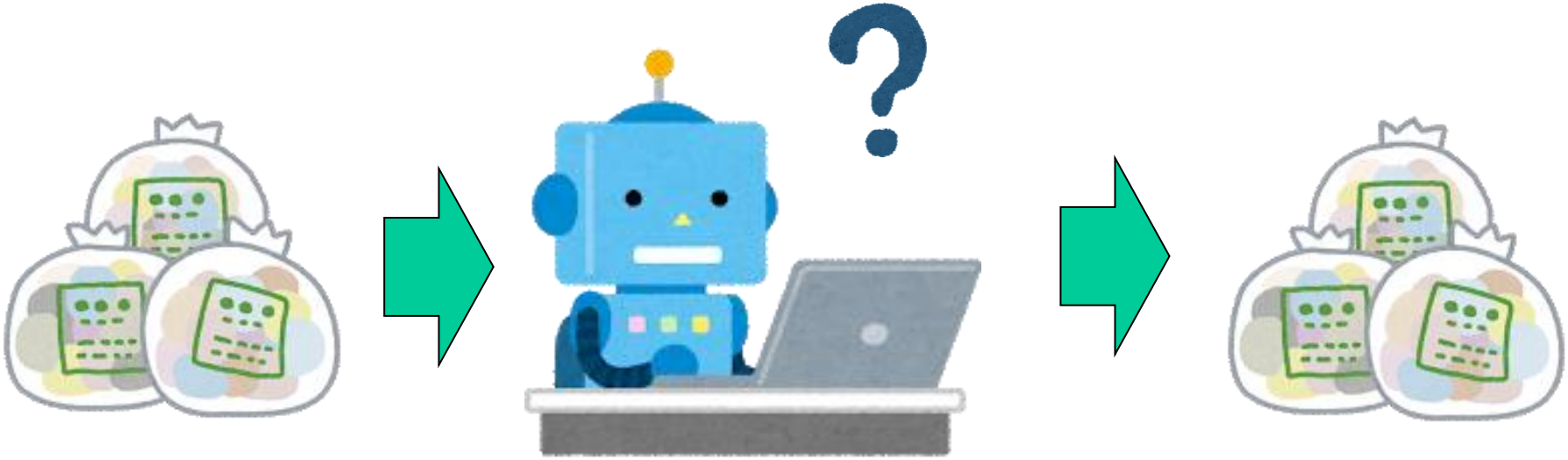
https://www.mlit.go.jp/scpf/

Super City
J-Tech challenges SDGs

https://www.kantei.go.jp/jp/singi/tiiki/kokusentoc/supercity/openlabo/supercitycontents.html

AIシステムの品質、信頼性

- ガーベッジイン・ガーベッジアウト
  - ノイズが多いデータやバイアスがかかったデータを元に学習したとしてもうまくいかないという教訓です。
- 品質のよいビッグデータはAIシステムの品質と信頼性を保つうえで必須です。
- 品質や信頼性は社会的価値観を守る上でも重要です。



バイアス

- 米国では司法判断における「AIの偏見」が大きく注目されることがありました。
- ある報道機関が2016年にAIを用いると特定のデモグラフィック属性、つまり、年齢、性別、職業などの人口統計学的特性をもっている人の方が、再犯率が高いと予想されるという報道がありました。
- AIのバイアスや公平性の問題にどう対処していくかが、非常に重要な先端研究課題として盛んに研究されています。

Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner,
"Machine Bias There's software used across the country to predict future criminals.
And it's biased against blacks.", ProPublica, May 23, 2016.
https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

倫理と監査人

- こうしたバイアスの問題は、AIを社会実装していく上で、非常に深刻に受け止められています。
- AIが社会的に正しく稼働しているか検証する「監査人」が、これからの社会では必要だと主張する研究者もいます。
  - 自動運転車の倫理の問題の研究も盛んです。
- 人間中心で信頼されるAIを構築するにはこのように様々な角度からものごとをみていく必要があります。
  - Society 5.0 （人間中心の新しい社会）へ

Iyad Rahwan, “Society-in-the-Loop: Programming the Algorithmic Social Contract”,Ethics and Information Technology, 2017.

モラルマシン
https://www.moralmachine.net/hl/ja