

# AIの開発・利活用の現状及び今後

## 欧米（特にEU）におけるAI政策の 我が国への影響

中川裕志

理化学研究所・革新知能統合研究センター

東京大学名誉教授

# リアル と デジタル（～記号化）

- リアルが参照するもの
  - 有体物の商品
  - 不動産（土地や建物は有体物）
- デジタルが参照するもの
  - 無体物の商品（情報自体が商品）
  - 金融商品は無体物なのでデジタル？
  - Web上の商品情報
    - 将来はAIでの対話インターフェースで商品情報を入手するかもしれない
  - Web上の一般向け広告
  - Web上の個人向け勧誘， 広告， 商品情報（個人向け価格）
  - 売買契約

◆ほとんどはデジタルの問題

# 古典的問題

- 検索エンジンの商品検索の順位操作
    - 独禁法で当局が外形的に判断して、プラットフォームを指導するしかない
  - 同一商品価格の個人適応化
    - 販売条件（購入の時期、量などで個人向けに変更するのは違法ではない）
  - 同一システム（多くはAIを応用）が複数社で使われた結果としての価格均一化
    - ソフト間での情報共有，意図的信号授受
      - あると独禁法違反
      - ない場合は違法性は問えない→ 開発業者にソフト個別化の強制はできないのではないか。
    - ソフト自体が異なっても，アルゴリズムの競合や協調で価格均一化はありうる
- ▶類似の問題はフラッシュクラッシュ

# AIの開発・利活用の現状及び今後

- 個人適応
  - 広告：利用履歴の利用
  - → 利用履歴の使われ方 → 裏で流通
- 推薦システム → 個人適応がうまくいっていない
- 個人の行動を機械学習して予測
  - 統計的処理で予測するには個人1人の行動履歴では、多様性も量も少ない
  - 似たような人を集めて量を増やす推薦システムでは粗い結果しかでない

# AIの開発・利活用の現状及び今後

- ◆もっと正確な個人情報を集めたい。名寄せして精度を上げたい
- ◆PFの企業グループ内では名寄せできる。
- ◆企業間をデータ移転することは目的外利用になるかもしれないが。
  - ◆Facebookの規約ではデータ移転すると書いてある。
  
- 個人側が対抗して開示要求→実効性を持たせられるか？
  
- GDPR
  - データポータビリティの権利（第20条）
  - データ主体によるアクセスの権利（第15条）
- 個人情報保護法 開示請求（第28条）
  
- 他のプラットフォームへのポータビリティの可能性（PFは反対しそうなので、実効性のある法制度を作れるかという問題）

# AIの開発・利活用の現状及び今後：パーソナルAIエージェント

• → 個人データ開示要求 開示されても内容を理解できるのか？

◆結局は、プラットフォームをトラストできるかという問題

◆将来技術

◆個人とやりとりするAIを利用した知的ユーザインタフェース

◆パーソナルAIエージェント

→PFのユーザインタフェースは個人の状況に立ち入り，個人データを要求．得た個人データをAIで分析

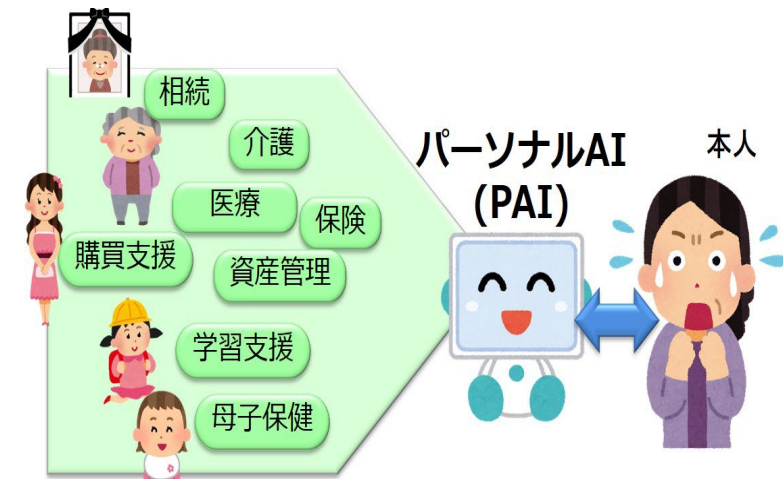
◆GoogleがCookieの代わりに導入するサンドボックスは，個人データを個人の手元におき，PFが外部から利用する方法なので，Cookieより推薦性能が上がるかもしれない

→対策：個人の代理をするパーソナルAIエージェント

→ただし，代理人にはなれないので，現在のところあくまで個人支援ツールだが，個人情報を入力してよいかどうかのチェックくらいはできそう

# AIの開発・利活用の現状及び今後：パーソナルAIエージェント

- 東京大学の橋田教授が提案したPLRが一例
- <https://www.assemblogue.com/apps/PLRintro>
- 自分の個人データを自分で集めて，管理する
- 最新かつ精度の高いデータなので事業者と対峙できる
- 世界的にはMyDataという流れがある． <https://mydata.org/>
- 日本にも支部: MyData Japan



# AIの開発・利活用の現状及び今後

## • 生成AI

- 購入などについて疑問や質問ができる
- 一般的な質問ではChatGPTとGoogle BARDはあまり差がなかった
- 検索能力の高いシステムのほうが強力 → Googleの勝ち？
- 画像による検索 Google 画像による商品検索 工業製品は正確（10年以上履いた革靴も正確に検索できた）
  - （次のスライド参照）
- 絵画の検索は不得意。あまり似た絵がでてこない。 画像生成AIの出番かもしれないが．．．
  - （次の次のスライド参照）



## □ 多様な事業者（取引基盤提供者等）が関わることとの関係

- 画像による検索 Google 画像による商品検索
- 工業製品は正確（10年以上履いた革靴も正確に検索できた）
- リアルなものの取引もデジタルデータ（画像）を介する時代



メドレービセンザ マグ  
4000円



三菱加湿器



GT.HAWKINGS  
10000円程度

- この絵からは似たような絵は検索できなかった.
- AIの能力というよりは, Googleが保持している画像データのレポーターが小さいからだろう.
- 画像はリアルとデジタルの境界: リアル, デジタル, どちらの商品形態もある.



## ◆ 技術とデータに強いプラットフォームの役割

- リアルとデジタルの両方を扱えるプラットフォーム業者（アマゾン など）
- ◆ デジタルから得たイメージとリアルなモノの乖離の問題にどこまで対処できるかは、プラットフォーム事業者の技術的力量による。
  - 意図的に騙していることが明白なら景品表示法の問題。
    - プラットフォームの単なる技術力不足の可能性もある。
- ◆ 技術とデータに強いプラットフォームの傘に入らないと商売にならない中小事業者
  - 技術開発に投入された人的資源，コストの大きさを考えると，単純にプラットフォームを叩けばよいというわけではない。

# デジタルのみの世界

- 証券，債券，保険，為替も売買，内容ともデジタル
  - 貨幣は結局，デジタル情報というのが現状
  - しかし，証券，債券，保険，為替は歴史ある分野だけに消費者保護の仕組みもかなり整備されているはず。
  - **金融商品取引法**
  - とはいえ，投資を政府自体が推奨しているので，どういう責任になるのか心配
- ◆証券のAIアドバイザーやロボ・アドバイザーにおける消費者保護は重要
- ◆とくにAIアドバイザー自体が個人資産を個人の代理として投資する場合，**リスクなどを説明するAIインタフェース**を証券会社の得になるような視点だけでアドバイスしない仕組みをどのように担保することは可能か？
  - ◆法律の問題→法律を正しく実現する技術であると確認できるか？

- 投資判断におけるアルゴリズム・AI の利用と法的責任 アルゴリズム・AI の利用を巡る法律問題研究会

(<https://www.imes.boj.or.jp/research/papers/japanese/kk38-2-1.pdf>)

加毛先生もお書きなので、素人の私がお話するのは大変失礼とは存じますが...

- アルゴリズム・AI を利用して自動で取引を行い、個々の投資判断の時点で人間の判断が介在しない場合
- 現行法：アルゴリズム・AI には、独立の権利主体としての資格なし。法的には、当該アルゴリズム・AI を利用する特定の主体が投資判断・運用を行っているとなる
- アルゴリズム・AI を直接利用しているのが投資家か業者かという点

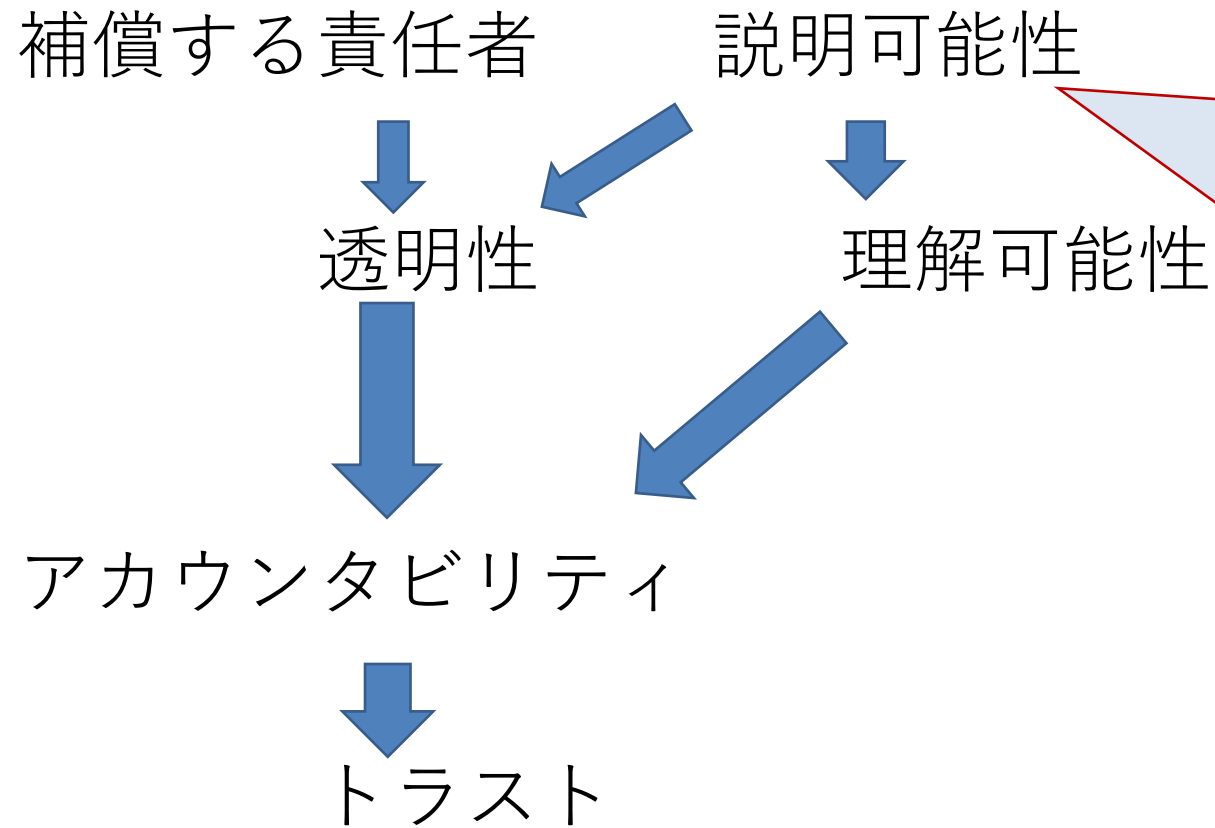
➤ **投資家（＝消費者）はアルゴリズムを知るべき。法的に知る権利があるが、  
かりに知ったとしても理解できるか？ → 結局はトラスト？**

- アルゴリズム・AIによる相場操縦、およびインサイダー取引については上記論文に丁寧に記載されているので、特段の意見はありません。

- 10年前に猛威を振るったフラッシュクラッシュは複数アルゴリズムの競合現象ですが、最近はどうも制御できているかもしれません。

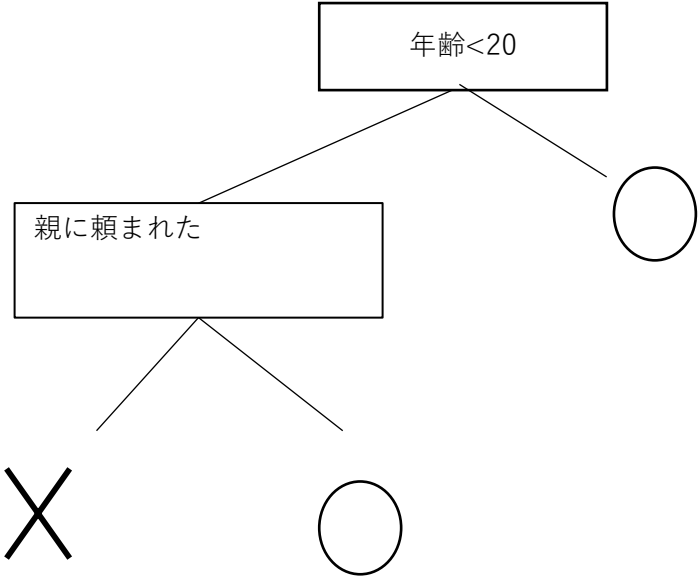


# ◆◆信用できるAIへ向けての取り組み： 透明性、説明可能性、トラスト

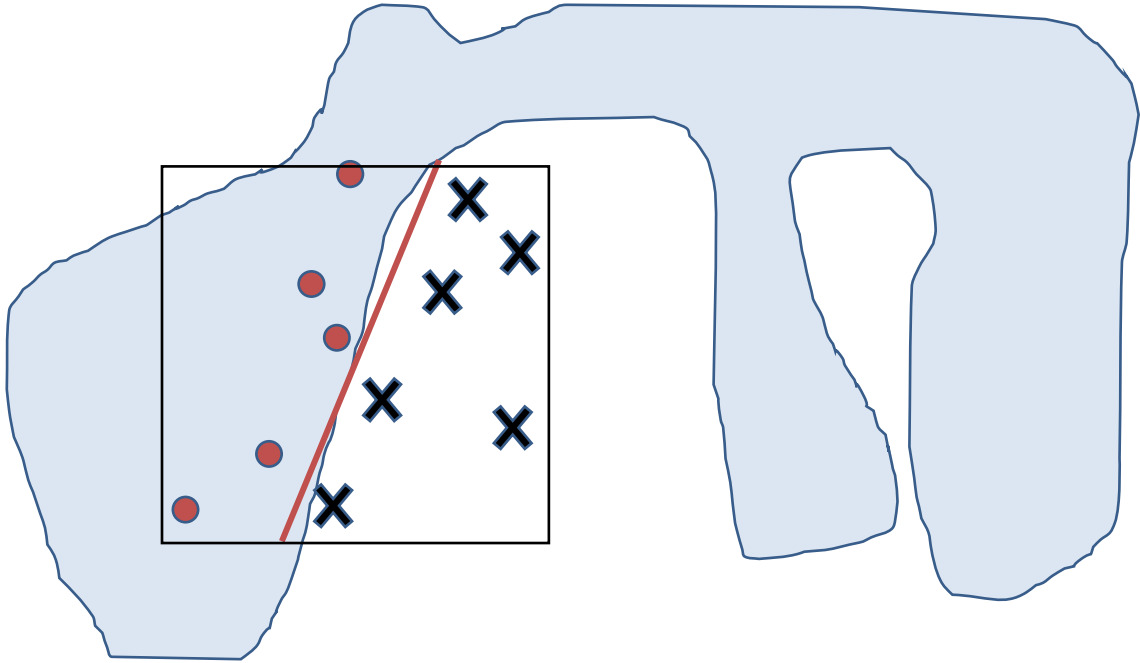


- AIの内部における動きを理解できる形で説明するのは無理（ブラックボックス）
- 簡単なAI（2つ枝分かれの分類木）で近似して説明
- 多数の使用例や直線による分類を提示

◆理解可能な分類システム



分かりやすい分類木



部分的には直線で分類

## ➤投資運用事業者が利用した場合の問題

- ➔ AIが関与するアルゴリズム ➔ 投資運用事業者が十分にAIのことを知っていて作ったアルゴリズムか？
- 現代のAIは既存のデータに依拠するが、予見可能性は必ずしも高くない。
- 確率は低くてもミスはありえる。
  
- 投資運用事業者がAIの損失の理由，例えば過去データ依存性，を十分に理解し，投資家に伝えたとして，投資家は理解できるのか？
- 結局は，過去の成功経験があれば，トラストするということになってしまいそうだが．．．**
  
- この問題は消費者法のシステム的問題なのか，昔から知られている外部要因の問題なのか➔古くて新しい問題
  
- 投資家が生成AIの助言も使って判断した場合 ➔投資家（＝消費者）の責任。



- 業者Aが、システム・ベンダーである業者Bに当該アルゴリズム・AIの開発を委託
  - 投資運用事業者Aが投資判断基準を決定するのではなく、開発業者Bが投資判断基準を決定してシステムを構築するような場合には、業者Bは、業者Aに対して投資助言を行うものと評価されたり、業者Aから運用の委託を受けたものと評価されたり、あるいは顧客に対して、直接投資助言や運用のサービスを提供するものと評価されたりして、規制の対象となる可能性がある。個別の実態の考慮が必要
- AIの行動の結果として生じた損失の帰属や分担の問題
  - 当該投資運用業者がアルゴリズム・AIを利用する場合、その結果として生じた損失につき、投資運用業者がいかなる場合に責任を負うかは、技術的には必ずしも明らかでない
  - 技術的問題：外部環境による損失か、AIアルゴリズムによる損失かを切り分ける方法を提示できるか不明
- 投資一任契約は、事業者は顧客の「信認義務者」（善管注意義務を負う）であり、契約が顧客の属性に適合していない場合や、そのリスク等について経時的に十分に説明しなければならない。説明がされていない場合等には、適合性原則や説明義務等の違反として、顧客は、投資運用業者に対し、不法行為に基づく損害賠償責任を追及できる → 一般消費者にこの追求ができるか？
- アルゴリズム・AIによる投資判断だと、取引に関して、消費者に理解可能な説明ができるか？
  - 投資運用事業者が生成AIに投資判断の説明を要約させる、ないしは言い換えさせる、という使い方はできるが、信頼性には疑問。ないよりはマシ程度???

# 暗号資産， NFTなどが売買情報も内容もデジタル

- 怪しさが横行して素人消費者にとっては危ない
  - 消費者保護に有効な規制の仕組みがまだない？
- 
- 以上のような，金融商品への投資事業者への一任契約への制約が，暗号資産やNFTに対応するような仕組みになっているのかどうか？
- 2019年法改正
  - 投資家に暗号資産を対価としてトークンを発行する行為に、金商法が適用されることを明確化・発行者による投資家への情報開示の制度やトークンの売買の仲介業者に対する販売・勧誘規制等を整備
  - 整備が進みつつあるが，消費者（＝投資家側）の理解が十分に進むかどうか不明。そもそも，暗号資産の仕組みが理解困難と思える。

# ChatGPTに暗号資産について聞いてみました → 理解しきれるか？

- 暗号資産（または暗号通貨）は、デジタルまたは仮想通貨で、暗号技術を使用して取引を確保し、新しい単位の生成を制御し、資産の転送を検証するものです。以下はその主要な特徴と仕組みです。
- **暗号資産の特徴**
  1. **分散型ネットワーク**：ほとんどの暗号資産は、中央集権的な管理者や中央銀行が存在しない、分散型のブロックチェーン技術を使用しています。
  2. **暗号技術の使用**：取引は高度な暗号技術によって保護され、セキュリティと匿名性が確保されます。
  3. **透明性と不変性**：ブロックチェーン上のすべての取引は公開され、変更が不可能です。
  4. **供給制限**：多くの暗号資産は、その供給に上限が設定されています（例：ビットコインは約2,100万枚が最大供給量）。
- **暗号資産の仕組み**
  1. **ブロックチェーン**：暗号資産はブロックチェーン上で機能します。これは、連続した「ブロック」に記録された取引の公開台帳です。各ブロックには、数多くの取引が含まれ、その前のブロックに暗号的に接続されています。
  2. **マイニングとコンセンサス**：新しい取引の検証とブロックチェーンへの追加は、「マイニング」と呼ばれるプロセスで行われます。これには、複雑な数学的問題を解決することで、ネットワークの合意（コンセンサス）を形成する作業が含まれます。
  3. **ウォレット**：ユーザーはデジタル「ウォレット」を使用して暗号資産を保管・管理します。ウォレットには、資産の所有権を証明するプライベートキーが含まれています。
  4. **取引**：ユーザーはウォレットを介して暗号資産を送受信します。取引はブロックチェーンに記録され、ネットワーク全体で検証されます。
- **例：ビットコインの場合**
  - ビットコインは、最もよく知られている暗号資産の一つです。ビットコインの取引は、全世界のマイナーによって処理され、ビットコインのブロックチェーンに記録されます。ビットコインの新しいブロックは約10分ごとに生成され、そのプロセス中に新しいビットコインがマイニングされます。
- **注意点**
  - **リスク**：価値の変動、ハッキング、規制の変更など、様々なリスクがあります。
  - **規制**：国や地域によって規制が異なり、一部では取引が制限されている場合があります。
  - 暗号資産は革新的な技術ですが、投資する前にリスクをよく理解し、慎重に行動することが重要です。

# 暗号資産に投資の危険性についての回答： →常識的

- 暗号資産に投資する際の危険性と注意点は、以下のように多岐にわたります。
- **危険性**
  1. **価格の極端な変動性**：暗号資産は非常に変動が激しい市場です。短期間で大きな価格変動が発生し、大きな利益を得る可能性がある一方で、大きな損失を被るリスクもあります。
  2. **ハッキングや詐欺のリスク**：暗号資産取引所やウォレットはハッキングの標的になることがあります。また、詐欺的なICO（Initial Coin Offering）やプロジェクトも存在し、投資家を騙して資金を奪うことがあります。
  3. **規制の不確実性**：多くの国では暗号資産に関する法律や規制が確立しておらず、将来的に規制が変更される可能性があります。これは市場に大きな影響を与える可能性があります。
  4. **流動性リスク**：特に小規模な暗号資産の場合、市場の流動性が低いことがあり、資産の売買が困難になることがあります。
- **注意点**
  1. **リスク管理**：投資額は、失っても生活に支障をきたさない範囲に留めることが重要です。また、多様な資産に分散投資することでリスクを低減することが望ましいです。
  2. **研究と教育**：投資する暗号資産の技術、市場動向、開発チームなどについて十分に調査し、理解してから投資することが大切です。
  3. **セキュリティ対策**：ウォレットのセキュリティ対策（二要素認証の設定、強固なパスワードの使用、プライベートキーの安全な保管など）を徹底することが重要です。
  4. **税金と規制の遵守**：居住国の税法や規制を理解し、適切に遵守することが必要です。
  5. **長期的な視点**：暗号資産市場は新しく、未だ発展途上です。長期的な視点で市場の成熟を見守ることが重要です。
- 投資に関しては、専門家のアドバイスを求めることも有効な手段の一つです。暗号資産は高リスク・高リターンの資産クラスであり、投資する際には十分な知識と慎重な判断が求められます。

# 欧米（特にEU）におけるAI政策の我が国への影響

- ◆ 外形的に明確なPFらの行為の禁止は法律による。ただし、技術的実装はよくわからないことがある。
- AI法
  - 禁止，ハイリスク，低リスク，最小リスク → 消費者への法的影響はまだ分からない
- プラットフォーム規制
- GDPR ダークパターンによる同意は無効 etc.
- Digital Market Act VLOPsに対するプロファイリングによる広告禁止
- Digital Service Act
  - PFのダークパターンに関する種々の規制あり
  - プロファイリングに基づく広告（特に子供向け）の禁止
  - [https://www.soumu.go.jp/main\\_content/000831952.pdf](https://www.soumu.go.jp/main_content/000831952.pdf)

小向太郎：GDPRとEUのデジタル政策。ジュリスト 2024年2月号に詳細説明有ります。

# 欧米（特にEU）におけるAI政策の我が国への影響

- ◆すべてはEU域内の法律
- ◆しかし、域外適用もあり
- ◆ブリュッセル効果による間接的しかし強力な域外への影響力
- ◆日本のメーカーには直接影響するが、日本の消費者法との今後の関係は技術的観点からの影響はまだ明確には分からない。

# 付録

# いただいたお題

2. デジタル化による技術の進展が消費者の関わる取引環境に与える影響についての基本的な考え方

① デジタル取引の特徴の分析・具体化

- ・ 着目すべきリアル取引との相違点
- ・ 消費者の「脆弱性」との関係
- ・ 情報の扱われ方や消費者の選択環境
- ・ 消費者取引に関わる主体の広がりや多層化と可変性
- ・ 消費者取引を規律する各種手法・主体とそれらの寄与度・インパクト
- ・ 消費者（消費者団体）と事業者（グローバル企業等）の対応力の

相違・格差

② デジタル取引について、リアル取引と（次元の）異なる規律が必要となる場面、規律が整備されていない場面の整理

- ・ 消費者の「脆弱性」の利用・作出との関係
- ・ 消費者の取引環境の個別化との関係
- ・ 消費者が情報、時間、関心・アテンションを提供する取引との関係
- ・ 事業者が多層的に関わることとの関係（プラットフォームや決済事業者等の取引基盤
- ・ 技術の進展、情報化の下で法制度が果たすべき役割



# 画像生成AI

Midjourneyを使ってみて

# 簡単に作れる画像



呪文は

Armed lady with a sword fights at the castle gate in the Greek era.



A Roman lady from high society standing at the harbor where a ship comes in.

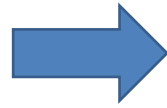


A lady sniper of Ukraine

# 普通のおじさんが難しい



格好良すぎ

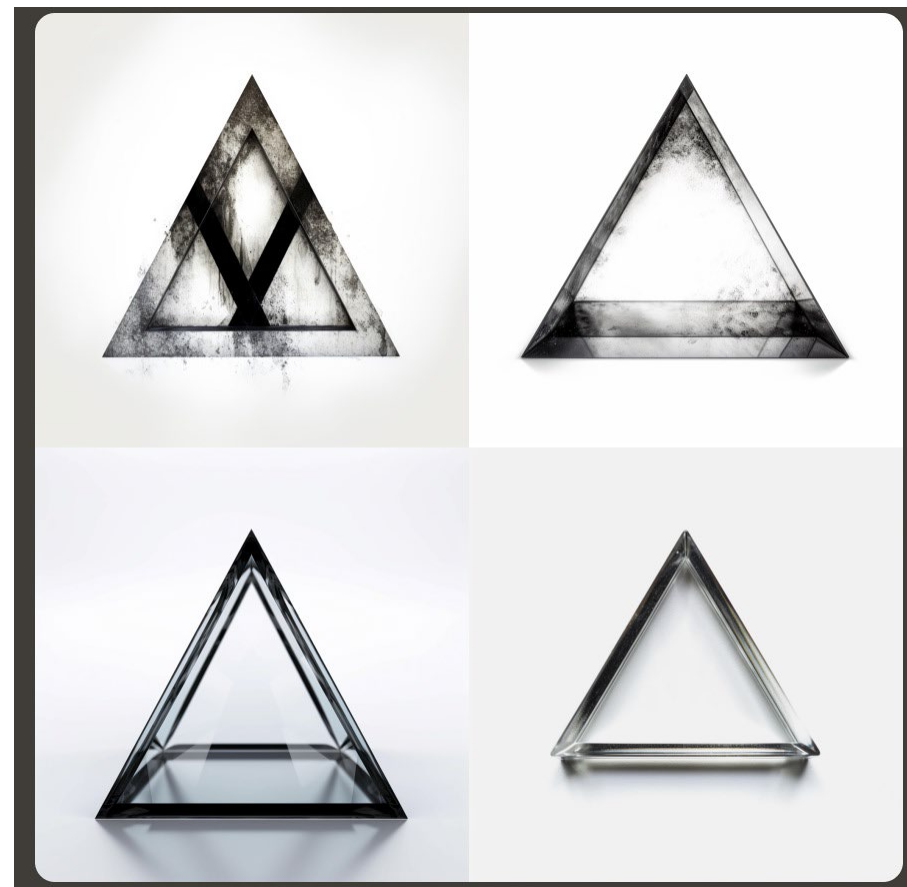
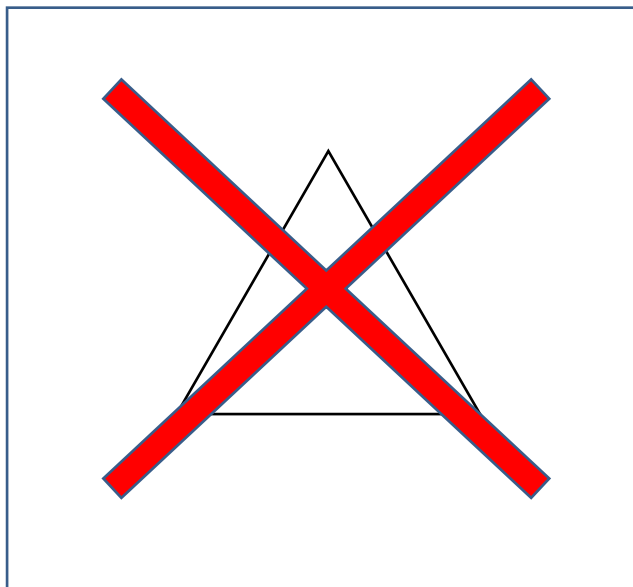




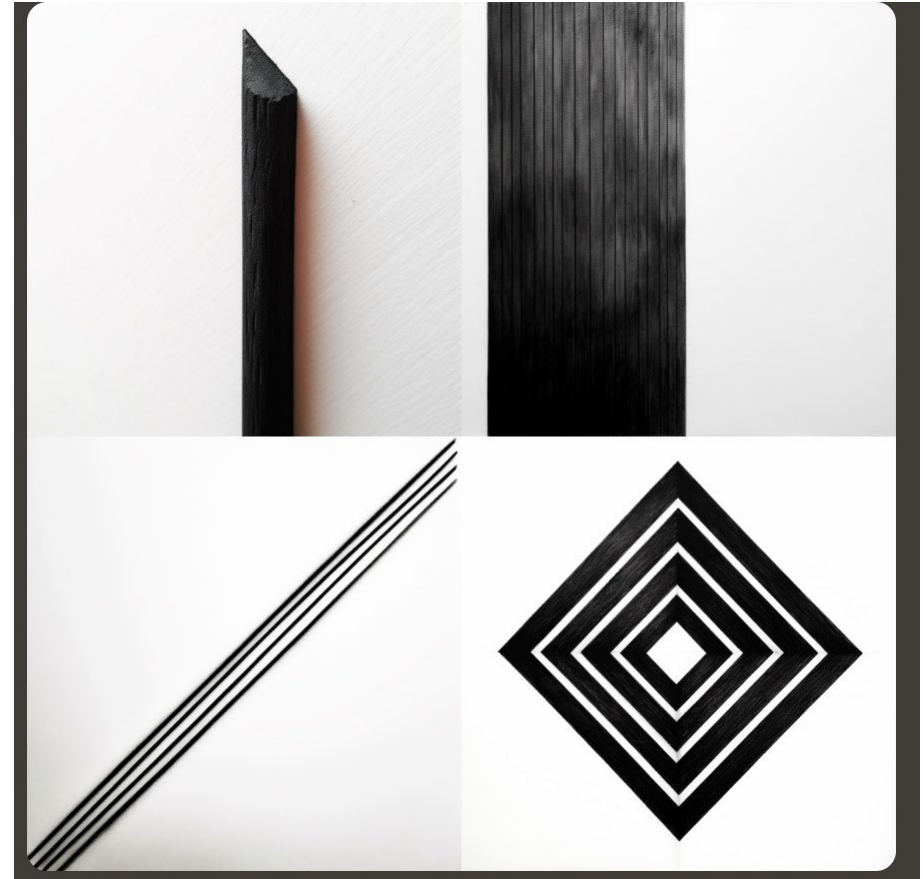
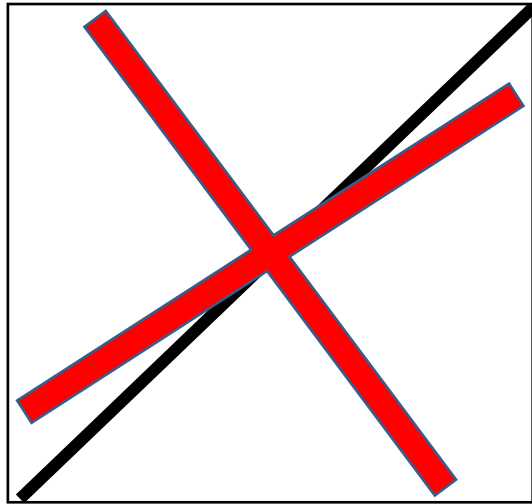
もっと難しいのは

白い背景で手前に内部は透明で辺の色が黒い正三角形

An equilateral triangle with transparent interior and black colored sides in the foreground on a white background.



白い背景で左下隅から右上隅にひかれた 1 本の黒い直線  
A single black rectilinear line running from the lower left corner to the upper right corner on a white background.



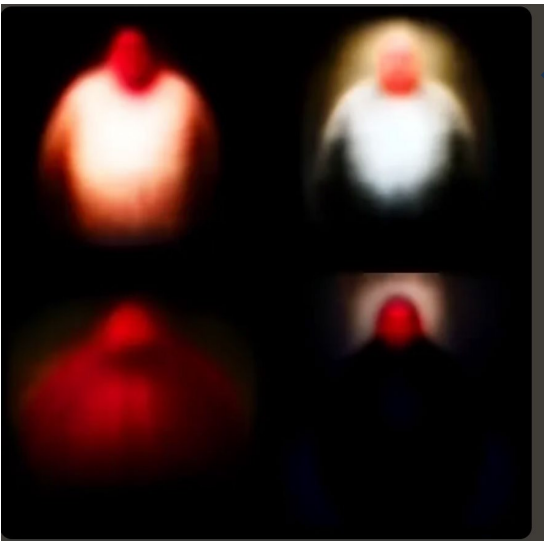
- **拡散過程**：元画像に雑音を追加. そのときの变化をパラメーター化し記憶
- **逆拡散過程**：雑音から出発し, 拡散過程で得たパラメーターを使って Promptで探した元画像に近づけていく
  - Promptで探した元画像は複数あると, それらを自然につなぎ合わせる技術が発展している (社外秘)
- 結局は, 生成される画像は元画像次第

拡散過程

完全な雑音

Prompt:  
太った日本人男性

逆拡散過程



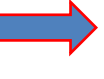
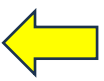
Midjourney 開始 0 %



Midjourney 開始46%



Midjourney 100%



# 技術内容

- 非公開なものが多い
- 複数現画像のつなぎ目
- 超高度な画像処理技術

遠近感を利用して、ぼかしなどを利用し、自然につなぐ



陰影をつける

# 技術進歩

- 日々進化している
- 元画像のスケルトン（線画化したもの）をpromptで検索して、
- 複数画像の部分の大きさの変化なども行い、それらの画像を接続する
- XX風なども拡散モデルのパラメーターに埋め込まれているかもしれない

•



# 仕組み上しかたないのかも

- いくらPromptを頑張っても、結局は対応しそうな（複数の）元画像への依存性が高く、自由な作画は困難
- 著作権違反は類似性と依拠性の両方を立証しなければならない
- 元画像の作者？ **実はアーティストではなく出版社！**にも言い分があるだろう
  - 著作権法30条4では著作権のあるデータをAIの学習で使える。
  - なぜなら、著作権で重視される享受性は学習過程、生成過程では存在しないから。
  - しかし、依拠性があるのかもしれない
  - Creatorへの経済的配分を機械的に行える制度が作れるか？(例えば、JASRAC)

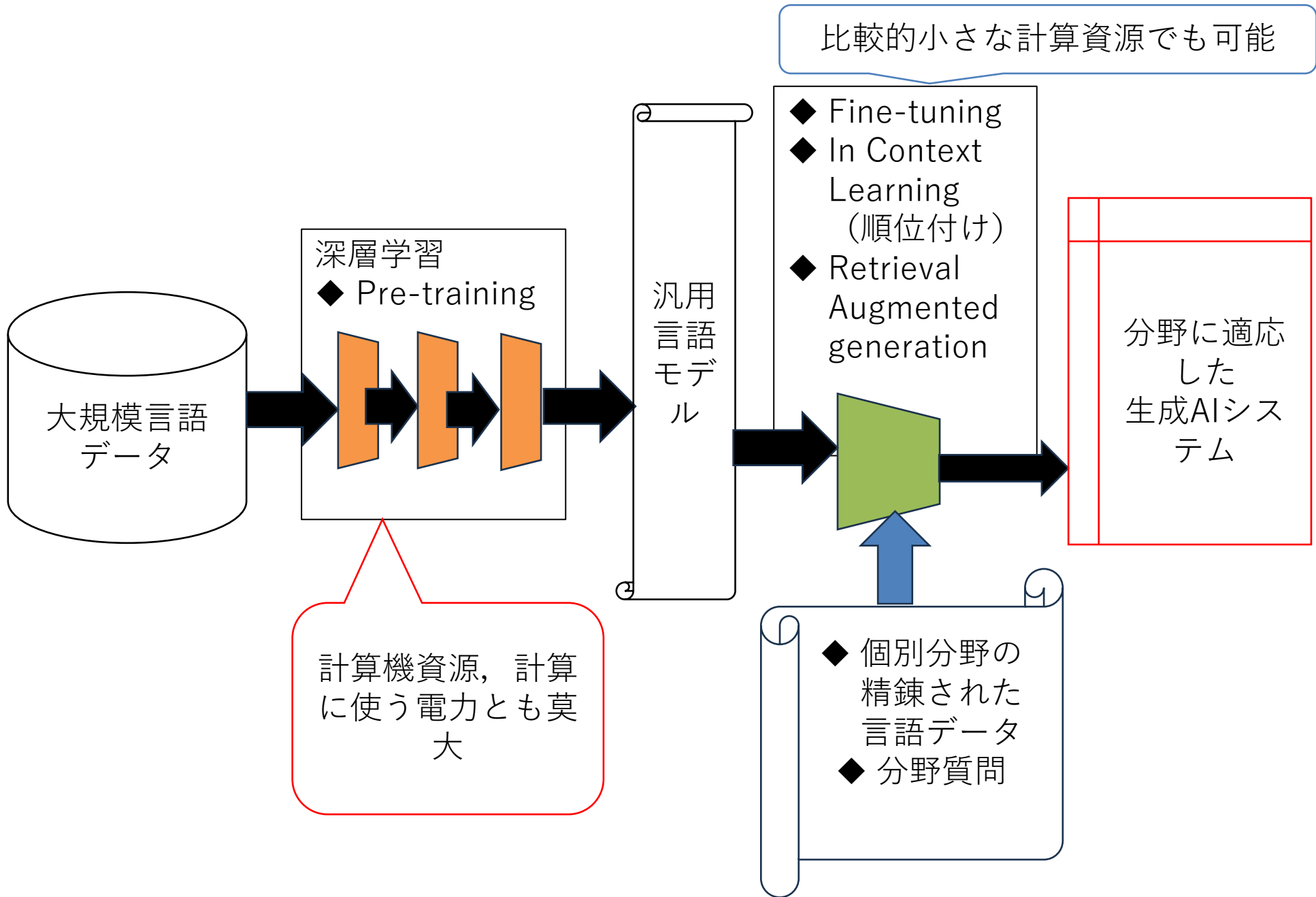
# より詳しい理論は

- 東京大学 鈴木大慈教授のスライド
  - <https://drive.google.com/file/d/15Sta2Znbwfay3goUKvSff7eWloF6zjCd/view>
- PFN 岡野原大輔氏の書籍
  - 拡散モデル データ生成技術の数理 Kindle版 [岡野原大輔](#) (著) 岩波書店

# ChatGPTなどの テキスト生成AIの話

## 参考書

1. 大規模言語モデルは新たな知能か： 岡野原大輔, 岩波科学ライブラリー
2. 大規模言語モデル入門：山田育也他, 技術評論社



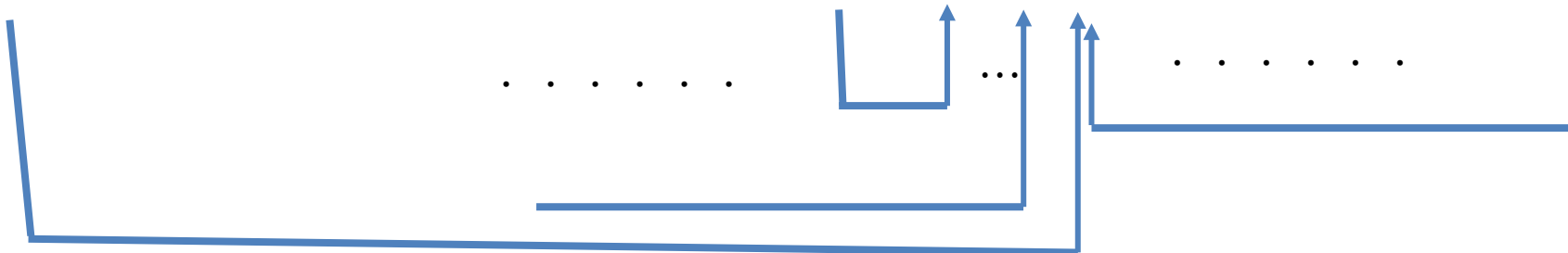
# Pre-training

昨日	は	昼食	を	食べ	損なっ	た
----	---	----	---	----	-----	---



直前に3単語を使って予測  
→ できるだけ多くの直前の単語を使いたいがデータ量が大きくてうまくいかなかった

昨日	は	昼食	を	食べ	損なっ	た
----	---	----	---	----	-----	---

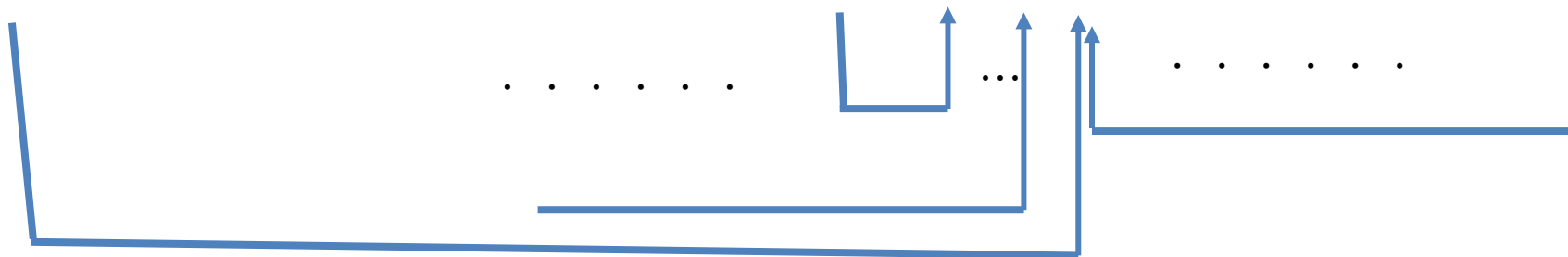


文内の単語だけでなく、多くの隣接文の単語からの影響(アテンションと呼ぶ)を深層学習で計算し、予測精度を向上

# Pre-training

パラメータ数は  
GPT2で100億,  
GPT3で2000億,  
GPT4では1兆以上とされている。

昨日	は	昼食	を	食べ	?	た
----	---	----	---	----	---	---



文内の単語だけでなく、多くの隣接文の単語からの影響（アテンションと呼ぶ）を表す超多数のパラメータの値を深層学習で計算し、予測精度を向上

?の正解は「**損なっ**」と分かっているので、その正解を出せるようにアテンションを深層学習を多数回適用して計算。

これを文の全ての単語について行う

→上記を学習に使う全データの文で行う。 → Transformer  
膨大な計算量。 一回の学習あたり数千万ドルの電気料金

◆この学習によって、文脈まで考慮して、高い精度で次の出現単語を予測できるようになった。当然、予測結果を用いて単語生成を繰り返せば、自動的に文生成もできる

# 正しい答えを得るには？

- ChatGPTは嘘をもっともらしく作文する機械
- 正しい答えを得ることは、Transformerの単なる延長上では無理
  - OpenAIにおいては、
    - データの大きさ増やすこと
    - ただし、データの大きさが増えるとどこまでいけるかは不明
      - 回答内部の無矛盾性，回答と学習データの無矛盾性をチェックしていない（できない？）
- **人海戦術**：おかしい回答を排除する目的で，質問をして回答を順位づけて，それがパラメターの更新につながる方法
- In Context Learning, Chain-of-Thought (CoT), Tree of thought
- 最大限にインターネット上のデータを集めても、インターネットに乗っていないデータも多い

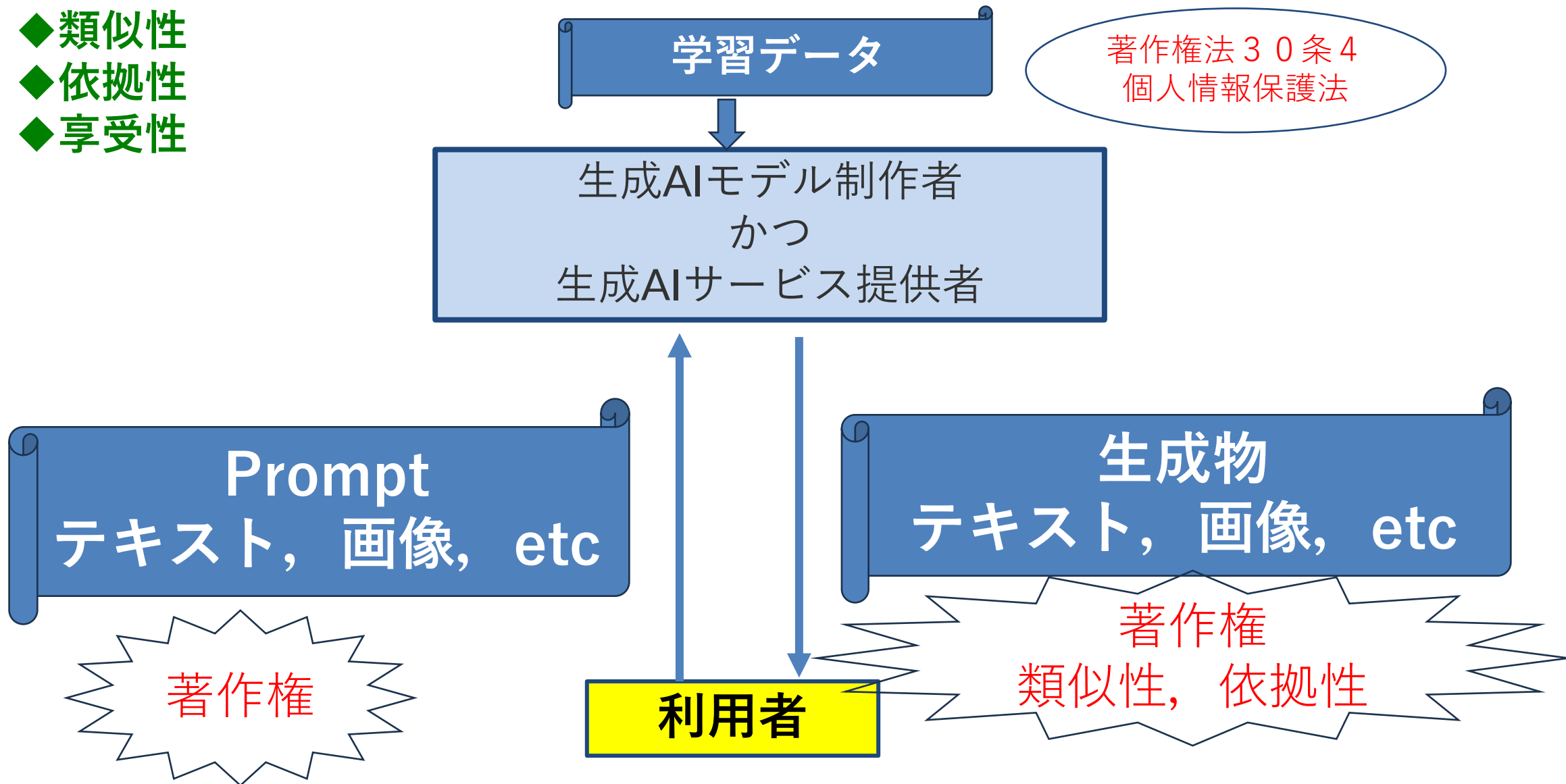
# 法律的問題

- 著作権の問題
  - 学習データ,
  - 回答 (テキスト, 画像)
  - Prompt(prompt自体, prompt中で著作権的に問題のある情報を使う)
- 誤情報 (hallucination)
- その他
- 参考: 柿沼太一: 「生成AIと著作権侵害」の論点についてとことん検討してみる, <https://storialaw.jp/blog/9748>
- 参考書: 福岡真之介, 松下外: 生成AIの法的リスクと対策, 日経BP, 2023/10/5



# サービス提供業者の構造の差異による著作権

- ◆類似性
- ◆依拠性
- ◆享受性



# サービス提供業者の構造の差異による著作権

