信州大学
SHINSHU UNIVERSITY

AI基礎
１．AIの歴史と応用分野

第1.1版

2025年7月31日

教材について

- 文科省のカリキュラムに従い、AI基礎の必須（☆）をカバーしています。
- 既に先行しているデータサイエンス応用基礎（学術図書出版社）の記述レベルに合わせています。
- 「総合知」の観点より企業人が読んでいる書籍のエッセンスをAdditional Noteとして付与しています。
- 本コースを受講すると、AIで使用されるタームが知識として定着するので、ディープラーニングG検定の参考書など勉強しやすくなります。是非、資格取得をチャレンジしてみて下さい。（昇進の条件としている企業もあります。）

テーマ	文科省　応用基礎レベル モデルカリキュラム	ディープラーニングG検定（翔泳社）
1．AIの歴史と応用分野	3-1. AIの歴史と応用分野（☆） 3-2. AIと社会（☆）	第１章　人口知能（AI）とは 第２章　人口知能をめぐる動向 第８章　AIの法律と倫理
2．機械学習の基礎と展望 付録　重回帰分析チュートリアル	3-3. 機械学習の基礎と展望（☆） 3-6. 認識 3-7. 予測・判断	第３章　機械学習の具体的手法
3．深層学習の基礎と展望 付録　画像認識CNN構築チュートリアル 付録　自然言語処理チュートリアル	3-4. 深層学習の基礎と展望（☆） 3-8. 言語と知識	第４章　ディープラーニングの概要 第５章　ディープラーニングの要素技術 第６章　ディープラーニングの応用例
4．演習環境の使い方とプログラミング言語の演習		
5．サポートベクターマシンの演習（演習）		
6．生成AIの基礎と展望	3-5. 生成AIの基礎と展望（☆）	
7．AIの構築と運用	3-9. 身体と運動 3-10. AIの構築と運用（☆）	第７章　AIの社会実装に向けて
8．畳み込みニューラルネットワークの演習		

変更履歴

版数	日付	内容	担当者（信州大学SOARより）
0.90版	2025年4月5日	• 文科省のカリキュラムに従い、データサイエンス応用基礎（学術図書出版社）の記述レベルに合わせてドラフト • 「総合知」の観点より企業人が読んでいる書籍のエッセンスを付与	教育・学生支援機構 教授（特定雇用） 杉浦 友佳
1.00版	2025年5月25日	• 誤記など加筆/修正 • 信州大学の人社系学生のレベルに合わせて修正	学術研究院（総合人間科学系） 全学教育センター　准教授 平井　佑樹
1.10版	2025年7月31日	• 企業研修としてアテストし、教材や教え方に合わせて修正	教育・学生支援機構 教授（特定雇用） 杉浦 友佳

1-1. AIとは

人口知能（AI）とは

推論、認識、判断など人間と同じ知的な処理能力を持つ機械（情報処理システム）

人工知能の分類

機械学習
数理的なモデルをデータに当てはめ、パラメータを学習するアプローチ

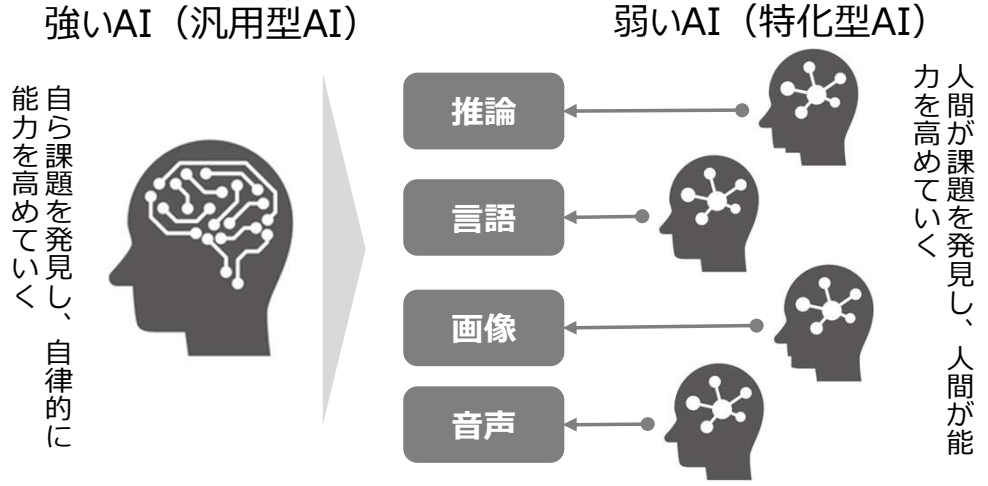
深層学習
機械学習をニューラルネットワークで行う（機械学習で着目した特徴量を自動的に学習させるアプローチ）

強いAIと弱いAI

1980年にジョン・サールが発表した「Minds, Brains, and Programs)という論文で提示された区分

強いAI（汎用型AI）
ひとつのAIが様々な問題について学習して知的な処理を行う

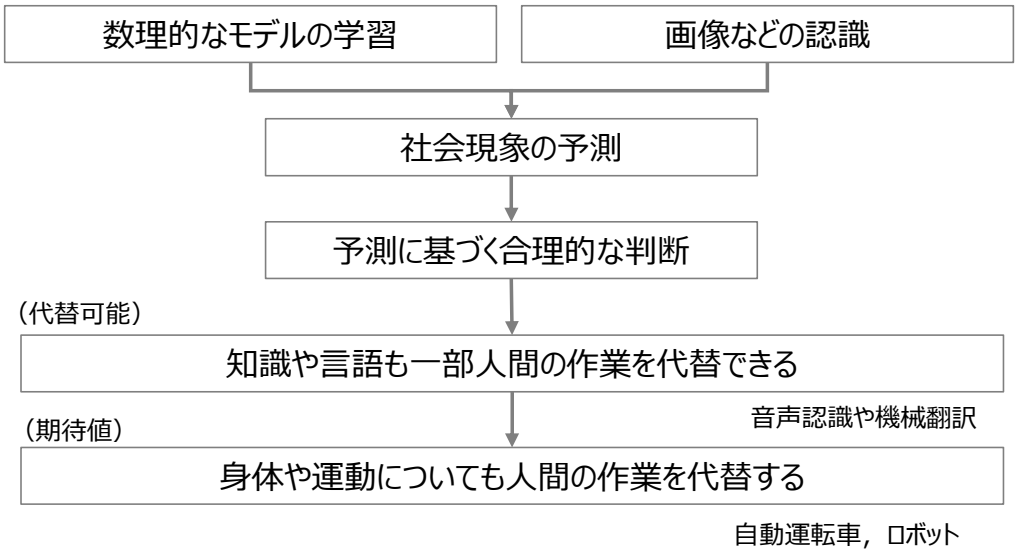
弱いAI（特化型AI）
画像認識、音声合成、機械翻訳やゲームなどの特定のタスクを行う
（これらのAI技術が発展すると汎用AIにつながる）



AI技術の発展とAI技術活用の広がり

信州大学 SHINSHU UNIVERSITY

AI技術の急速な発展



- 2013年オックスフォード大　Fery Osborneは、人間の仕事35%は人工知能やロボットに代替
- 過去の産業革命から、新しい技術の進展により、人間の仕事が代替されるのと同時に新しい仕事を生み出したことも事実

AI技術活用の広がり

業界	現時点での活用事例
流通	• 人員配置計画の予測と最適化 • 顧客に合わせたコミュケーション設計を実現 • MLOpsを活用した機械学習モデルによる業務量予測と改善 • 先を予測した車両の手配・倉庫の人員配置でコスト削減 • 画像解析・検索ソリューションで棚卸作業をオートメーション化
製造	• 設計の効率化，検品・外観検査の自動化，自律制御 • 画像認識による品質管理，異音検査・磁気探傷検査，収集データから不具合要因を特定 • 産業用ロボットの活用
金融業	• 融資審査 • 顧客対応 • ドキュメント処理，自動翻訳 • 運転挙動データを保険料に反映（保険）
ヘルスケア	• 医療現場での業務効率化 • 画像診断支援 • ビッグデータからの類推による診察支援 • ゲノム解析の活用
公共分野	• 問い合わせ対応 • サービス計画作成 • 議事録作成 • インフラ管理

AIの抱える課題

フレーム問題

課題を解く際、考慮すべき範囲を上手く限定できるか
例）自動運転で画像から運転に影響がある情報を取り出す
※人間は、これを無意識にやっている

シンボルグラウンティング問題

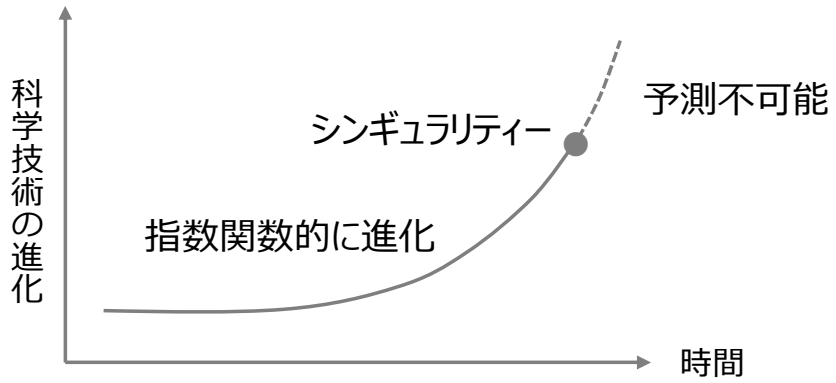
コンピュータが扱う記号が現実世界のものと上手くつながっているか
例）リンゴの持つ属性を色、形、味などを紐づける
※AIは人間のように体を持たないため、身体性の問題ともいわれる

シンギュラリティー（技術的特異点）

汎用AIが自分自身を改良する

帰納的アプローチと演繹的アプローチを融合させる

レイ・カーツワイル氏が2045年にシンギュラリティーに到達すると予測していることから、
2045年問題とも呼ばれています。



1-2. AIの歴史

簡易年表（AI技術）

1946年
ENIAC
ペンシルバニア大学

1950年
チューリングテスト
50年以内に5分間のテストで人間と誤認するのは30%

1952年
IBM701
（商用初）

1956年
ダートマス会議
ジョン・マッカーシー
artificial intelligence

1959年
チェッカープログラム
アーサー・リー・サミュエル

1969年
フレーム問題

1970年
MYCIN
スタンフォード大学
ルールベース（血液中バクテリア診断支援）

1980年
強いAI/弱いAI

1990年
シンボルグラウンディング問題

1990年
RNN
時系列，シーケンスデータ（再帰）

1997年
ディープ・ブルー
ガルリ・カスパロフ
を破る

1997年
LSTN
勾配消失問題を軽減

1998年
CNN
画像データ（畳み込み）

2012年
ILSVRCにて
AlexNetが優勝
（ヒントン）

2014年
GRU
LSTMよりも少ないパラメータ

2016年
AlphaGoが李世乭
（イ・セドル）に勝利

2017年
Transformer
自己注意機構

2018年
GPT
生成モデル

2024年
ヒントン，ポップフィールド
がノーベル賞受賞

2045年
シンギュラリティー

1940 1970 1990 2012 2024

第１次ブーム
探査・推論

第２次ブーム
知識

第３次ブーム
機械学習・特徴表現

テクノロジーロードマップ

音声認識，自然言語処理

物体検出，画像認識

1990

Recurrent Neural Networks (RNN)
概要: RNNは、時系列データやシーケンスデータを処理するために設計されたニューラルネットワークです。過去の情報を保持し、次のステップに影響を与えることができます。

主要な論文:
Elman, J. L. (1990). "Finding structure in time." Cognitive Science, 14(2), 179-211.

1997

Long Short-Term Memory (LSTM)
概要: LSTMは、RNNの一種で、長期依存関係をキャプチャするために設計されています。ゲート機構を使用して情報の流れを制御し、**勾配消失問題を軽減**します。

主要な論文:
Hochreiter, S., & Schmidhuber, J. (1997). "Long short-term memory." Neural Computation, 9(8), 1735-1780.

2014

Gated Recurrent Unit (GRU)
概要: GRUは、LSTMの簡略化バージョンで、リセットゲートと更新ゲートを使用して情報の流れを制御します。**LSTMよりも少ないパラメータで、同様の性能を発揮**します。

主要な論文:
Cho, K., et al. (2014). "Learning Phrase Representations using RNN Encoder-Decoder for Statistical Machine Translation." arXiv preprint arXiv:1406.1078.

2017

Transformer
概要: Transformerは、**自己注意機構を使用してデータを並列に処理**するモデルです。RNNやLSTMとは異なり、シーケンシャルな処理を行わず、長距離依存関係を効率的にキャプチャします。

主要な論文:
Vaswani, A., et al. (2017). "Attention is All You Need." Advances in Neural Information Processing Systems, 30, 5998-6008.

2018

GPT (Generative Pre-trained Transformer)
概要: GPTは、**Transformerアーキテクチャに基づいた生成モデル**で、大規模な事前学習を行い、自然言語生成タスクに優れた性能を発揮します。

主要な論文:

Radford, A., et al. (2018). "Improving Language Understanding by Generative Pre-Training." OpenAI.

1998

Convolutional Neural Networks (CNN)
概要: CNNは、画像やビデオなどの視覚データのパターン認識に特化したニューラルネットワークです。**畳み込み層を使用して特徴を抽出し、分類や検出タスクに優れた性能**を発揮します。
主要な論文:
LeCun, Y., et al. (1998). "Gradient-based learning applied to document recognition." Proceedings of the IEEE, 86(11), 2278-2324.
Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). "ImageNet Classification with Deep Convolutional Neural Networks." Advances in Neural Information Processing Systems, 25, 1097-1105.

第１次AIブーム

1946年
ペンシルバニア大学で世界初の汎用コンピュータENIACが開発された

1952年4月29日
IBM 701 Electronic Data Processing Machine（初の商用機）が発表された※1

- 真空管論理回路と静電記憶装置
- 2048ワード、各36ビットのメモリ
- 命令は18ビット長のシングルアドレス
- プログラマがアクセス可能なレジスタが2つ

1956年7月～8月
ダートマス会議（ Dartmouth Conference）

- 人工知能という学術研究分野を確立
- ダートマス大学に在籍していたジョン・マッカーシーが主催
- 人類史上初めて英語の用語「artificial intelligence」が使われた

1959年
アーサー・リー・サミュエル（Arthur Lee Samuel）
IBM 701 上で初のチェッカープログラムを作成

第１次AIブーム
推論，探索が可能で、トイプロブレム（簡単な例題）を解くことができた。

ダートマス会議　提案書序文より　出典：Wikipedia

我々は、1956年の夏の2ヶ月間、10人の人工知能研究者がニューハンプシャー州ハノーバーのダートマス大学に集まることを提案する。そこで、学習のあらゆる観点や知能の他の機能を正確に説明することで機械がそれらをシミュレートできるようにするための基本的研究を進める。機械が言語を使うことができるようにする方法の探究、機械上での抽象化と概念の形成、今は人間にしか解けない問題を機械で解くこと、機械が自分自身を改善する方法などの探究の試みがなされるだろう。
我々は、注意深く選ばれた科学者のグループがひと夏集まれば、それらの問題のうちいくつかで大きな進展が得られると考えている。
(McCarthy et al 1955)

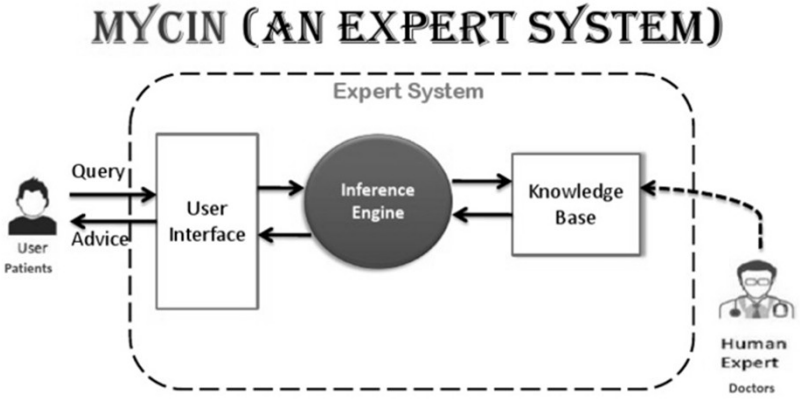
アーサー・リー・サミュエル
Arthur Lee Samuel

出典：https://www.ibm.com/history/early-games

第２次AIブーム

1970年代初
Mycin（マイシン）

- スタンフォード大学でに開発されたエキスパートシステムで、ブルース・ブキャナンとエドワード・ショートリッフェが開発（言語：LISP）
- システムは感染症を診断し、適切な抗生物質を推奨するようにデザインされていて、患者の体重のために供与量を調節する
  - ✓ 500程度の規則からなる知識ベースを持つ
  - ✓ 単純な「はい/いいえ」で答える質問や何らかの文章で答える質問（入力）
  - ✓ 細菌名のリスト（確率の高い順）とそれぞれの信頼度、なぜそう推論したかという理由、推奨される薬物療法のコースを示す



出典：https://www.scribd.com/document/410324333/Mycin

1997年5月11日
IBMのコンピューター「ディープ・ブルー」が当時のチェス世界王者、ガルリ・カスパロフ氏を破り、世界に衝撃を与えた。

ディープ・ブルーは、32プロセッサー・ノードを持つIBMのRS/6000 SP（RISCアーキテクチャー）をベースに、チェス専用のVLSIプロセッサを512個を追加して作られた。プログラムはC言語で書かれ、オペレーティングシステム はAIXが使われていた。開発チームは、グランドマスターであるジョエル・ベンジャミンを含めて6名。

RISC（reduced instruction set computer）は、命令セットの複雑さ、命令の総数や種類を減し、命令が行う処理の単純化、また、命令フォーマットの種類を減し、オペランドのアドレッシングを単純化した

出典：https://www.nikkei.com/article/DGKKZO43894650Y9A410C1TJN000/

第２次AIブーム　既存の理論やルールから
人間の論理的な思考をコンピュータによって再現する（演繹的アプローチ）

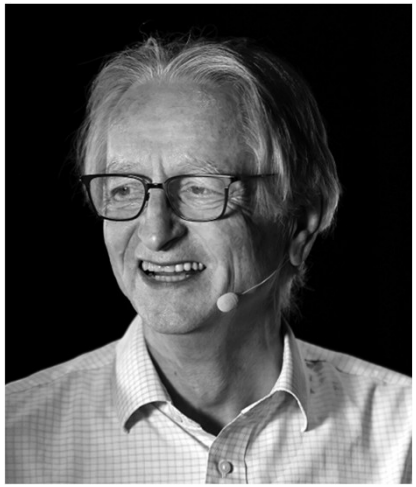
第３次AIブーム

2012年
ImageNetデータセット（1400万枚の画像にラベルがアノテーションされている）を題材とした画像認識技術コンテストであるILSVRC(the ImageNet Large Scale Visual Recognition Challenge)にて、AlexNetが優勝した。

畳み込みニューラル ネットワーク（CNN）の構造を持ち、Alex Krizhevsky がジェフェリー・ヒントン と共同で設計した。

2016年3月15日
AlphaGo（Google DeepMindによって開発されたコンピュータ囲碁プログラム）が、世界のトップ棋士　李世乭（イ・セドル）との五番勝負（4勝1敗）で勝利

第３次AIブーム
人間と同じように考える必要なく、結果として人間と同じような判断ができればよい（帰納的アプローチ）　具体的なデータや観察結果から

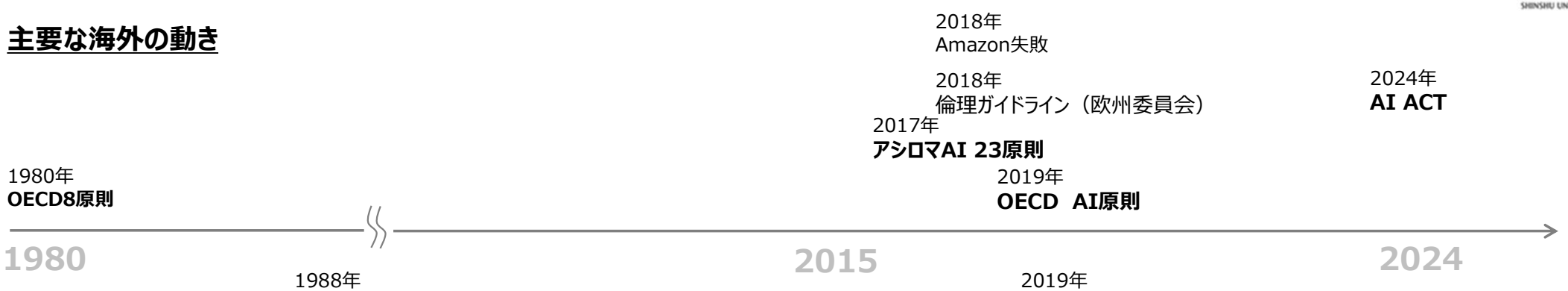


ジェフリー・エヴァレスト・ヒントン（英: Geoffrey Everest Hinton、1947年12月6日 - ）は、イギリス生まれのコンピュータ科学および認知心理学の研究者。ニューラルネットワークの研究を行っており、人工知能(AI)研究の第一人者とみなされている。トロント大学名誉教授（2022年時点）。2024年にジョン・ホップフィールドとともにノーベル物理学賞を受賞した。

1-3．AIと社会

簡易年表（プライバシー/AI　法律，ガイドライン）

主要な海外の動き



日本の動き

OECD８原則

プライバシーは**憲法第十三条**に規定された権利の一環

> すべて国民は、個人として尊重される。生命、自由及び幸福追求に対する国民の権利については、公共の福祉に反しない限り、立法その他の国政の上で、最大の尊重を必要とする。

1980年　プライバシー保護と個人データの国際流通についてのガイドラインに関するOECD理事会勧告

第2部 国内適用における基本原則**（OECD8原則）**

号	名称(日本語)	概要
1	収集制限の原則	個人データの収集は、適法かつ公正な手段で、データ主体に通知するかその同意を得た上で行わなければならない。
2	データ内容の原則	個人データは利用目的に沿ったものでなければならず、その目的に必要とされる範囲内で正確かつ完全で、最新の状態に保たなければならない。
3	目的明確化の原則	個人データの収集目的は収集前に特定されなければならず、目的が変更される際も、利用はその目的の達成に限定されなければならない。
4	利用制限の原則	データ主体の同意や法令に基づく場合以外は、個人データを特定された目的以外に利用してはならない。
5	安全保護措置の原則	個人データを不正利用・漏洩・改竄などから保護する対策を講じなければならない。
6	公開の原則	個人データの利用方針を公開し、データ管理者や個人データの所在地などを示さなければならない。
7	個人参加の原則	データ管理者は、個人が自分の個人データを保有しているかを確認し、保有している場合にはそのデータの開示を求める手段を提供しなければならない。データ管理者がこれを拒否する場合は、その理由を提示し、異議申し立てを保証しなければならない。
8	責任の原則	データ管理者には、以上の原則を遵守する責任を負わせるべきである。

経済協力開発機構（ Organization for Economic Co-operation and Development）：国際経済全般について協議することを目的とした国際機関

個人情報保護法の歴史　1/ 2

1988 年

行政機関を対象にした最初の個人情報保護法として，「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律（昭和63年12月16日法律第95号）」が制定され1990年10月1日から全面施行されている。

2003年　個人情報保護法（通称･略称）※令和3年法律第37号で下記の５つが法律第57号に一本化

- 個人情報の保護に関する法律（平成15年5月30日法律第57号）
- 行政機関の保有する個人情報の保護に関する法律（平成15年5月30日法律第58号）
- 独立行政法人等の保有する個人情報の保護に関する法律（平成15年5月30日法律第59号 ）
- 情報公開･個人情報保護審査会設置法（平成15年法律第60号）
- 行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律（平成15年法律第61号）

OECDプライバシー8原則	個人情報保護法（条文要約）
収集制限の原則	第20条　偽りその他不正の手段により個人情報を取得してはならない。
データ内容の原則	第22条　個人データを正確かつ最新の内容に保たねばならない。
目的明確化の原則 利用制限の原則	第17条　利用目的をできる限り特定しなければならない。 第18条　利用目的の達成に必要な範囲を超えて個人情報を取り扱ってはならない。 第27条　あらかじめ本人の同意を得ないで個人データを第三者に提供してはならない。
安全保護措置の原則	第23条　個人データの安全管理のために必要かつ適切な措置を講じなければならない。 第24条･第25条　個人データの安全管理が図られるよう従業者･委託先に対する必要かつ適切な監督を行わなければならない。
公開の原則 個人参加の原則	第21条　個人情報を取得した場合は速やかに、その利用目的を、本人に通知し、又は公表しなければならない。 第32条　利用目的等を本人の知り得る状態に置かなければならない。 第33条　本人が識別される保有個人データの開示を請求することができる。 第34条　本人は保有個人データの内容の訂正、追加又は削除を請求することができる。 第35条　本人は当該保有個人データの利用の停止又は消去を請求することができる。
責任の原則	第40条　個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。

個人情報保護法の歴史　2 / 2

信州大学
SHINSHU UNIVERSITY

個人情報

名前(氏名)・生年月日・年齢・性別・住所・電話番号・メールアドレス・SNS上の繋がり・学校名・銀行口座・クレジットカード番号など、「だれ」であるか特定される可能性のある情報が個人情報であるのではなく、そのような情報を含む情報全体が個人情報である。

個人情報保護法第2条

この法律において「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。
一．　当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第二号において同じ。）で作られる記録をいう。以下同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）
二．　個人識別符号が含まれるもの

2015年改訂

- 蓄積された膨大な個人情報を「ビッグデータ」として企業が利用しやすくする一方、情報漏洩に対する罰則を新設した。
- 取り扱う個人情報の数が5000件以下の「小規模取扱事業者」も法律適用の対象となり、「件数要件」が撤廃となった。
- 「利用目的の明示」、「第三者提供の際の本人同意」といった個人情報を活用するにあたっての義務が細かく定められた。
- 個人情報を復元できないよう「匿名加工情報」にするなど、一定の条件を満たすことで第三者に提供することも可能になるとされた。

2017年以降は３年毎に改正

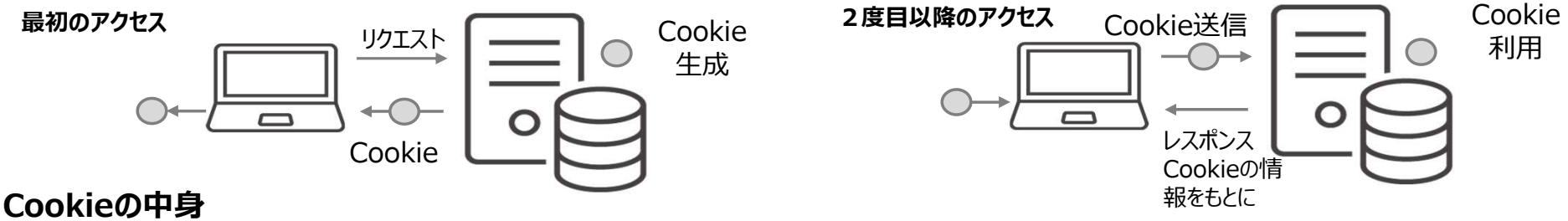
個人情報保護については、国内だけでなく、国外の動きにも敏感にならなくてはならない

（参考）GDPR
EU一般データ保護規則（General Data Protection Regulation; GDPR）は、欧州議会・欧州理事会および欧州委員会が欧州連合 (EU) 内のすべての個人のためにデータ保護を強化し統合することを意図している規則である。欧州連合域外への個人データの移転も対象とする。

Appendix; Cookie

Cookieの仕組み

サイトにアクセスした際に、Cookieが作られ、自身の端末（ブラウザ）に保存される。２度目にサイトを訪れると、ブラウザ側からCookieを渡し、その情報をもとにレスポンスします。



Cookieの中身

IDやパスワードなどの個人情報やサイトの閲覧情報を保存。

Cookieの種類

- ファーストパーティCookie：WEBサイトの訪問先ドメインから直接発行されるもの
- サードパーティCookie：第三者のドメインから発行されるもの

第三者の具体的な例として挙げられるのは、訪れたサイトに掲載されている広告代理店などで、ファーストパーティとは異なりユーザーの追跡を横断して行うことができます。例えば「自動車関係のサイトを訪れた後、他サイトを閲覧しているときに自動車の広告が表示された」というような経験のある方も多いと思いますが、これはサードパーティCookieの機能によるものです。

（Googleの動き）

- 2020年、クロームでサードパーティークッキーの機能を22年までに廃止すると表明（ネット広告市場の競争環境を損なうとして英規制当局などから反発を受ける）
- 規制当局からの懸念を解消する時間を確保するために、廃止時期の延期を繰り返してきた。
- 同社は代替策として、個人を特定できない形で関心に応じた広告を配信する「プライバシーサンドボックス」と呼ぶ仕組みを提案してきた。

AIに関するガイドライン（海外） 1 / 2

2017年

AI研究において守るべき原則、AIが備えるべき特性や従うべきルールなど、幅広い観点で将来AIがさらに発展・進化（自動的なものも含む）を遂げることを見越したガイダンスである「**アシロマAI 23原則**」が発表されました。（Future of Life Institute）

研究課題

研究目標，研究資金，科学と政策の連携，研究文化，競争の回避

倫理と価値

安全性，障害の透明性，司法の透明性，責任，価値観の調和，人間の価値観，個人のプライバシー，自由とプライバシー，利益の共有，繁栄の共有，人間による制御， 非破壊，人工知能軍拡競争

長期的な課題

能力に対する警戒，重要性，リスク，再帰的に自己改善する人工知能，公益

2018年

欧州委員会は4月25日、人工知能（AI）に関して、投資促進と、AIがもたらす社会変化に対する対応、倫理ガイドラインの策定の3点から成る方針を発表した。

2019年

初めて複数国で合意された AI 原則が OECD から公表された。OECD の AI 原則は、包摂的 な成長、持続可能な開発及び幸福、人間中心の価値観及び公平性、透明性及び説明可能性、 頑健性、セキュリティ及び安全性、アカウンタビリティからなる。

AIに関するガイドライン（海外）２/２

2024年
EUの**AI Act**が欧州議会にて採択されました。本規制では、リスクベースのアプローチが採用されており、AIをリスクの程度で分類し、その程度に応じた規制が適用されます。

容認できないリスク（Unacceptable risk）
- サブリミナル技術等によって集団を行動扇動
- ソーシャルスコアリング
- 法執行目的での顔認証等の遠隔生体認証
- プロファイリングに基づいた犯罪リスクや予測
- 職場および教育現場での勘定推定

高リスク（High risk）
- セーフティーコンポーネントまたはその一部に使用されるAIシステム
- 以下に該当するAIシステム
  1. 生体認証及び感情認証
  2. 重要インフラの管理・運用
  3. 教育・職業訓練での評価・テスト中の監視
  4. 雇用、労働管理における求人フィルタリングやタスクの割り当て、行動監視　等
  5. 不可欠な民間サービス及び公共サービスでの優先付け　等
  6. 移民、難民、国境の管理
  7. 司法と民主的プロセスの管理

限定的リスク（Limited risk）
- 人間と直接的な対話
- 汎用AIシステムを含む、合成音声、画像、動画、またはテキストコンテンツ生成
- 感情認識や生体認識
- ディープフエイク

最小のリスク（Minimal risk）
- 上記以外のリスク

AIに関するガイドライン（日本） １/３

2017年
人工知能学会が倫理指針を策定
人類への貢献、法規制の遵守、他者のプライバシーの尊重、公正性、安全性、誠実な振る舞い、社会に対する責任、社会との対話と自己研鑽、人工知能への倫理遵守の要請

2019年
政府は**「人間中心のAI社会原則」**を公表しました。この原則を通してSociety 5.0を実現し、日本が経済発展と社会課題を解決し、魅力ある社会になることを目指しています。

AI社会原則
I. 人間中心の原則
II. 教育・リテラシーの原則
III. プライバシー確保の原則
IV. セキュリティ確保の原則
V. 公正競争確保の原則
VI. 公平性、説明責任及び透明性の原則
VII. イノベーションの原則

AI開発原則
AIの開発者と事業者は、基本理念とAI社会原則を踏まえてAI開発利用原則を定め、遵守すべきである。

G20（大阪サミット）で、G20　AI原則が附属文書として作成された。

AIに関するガイドライン（日本）２/３

2021年　ITガバナンスのあり方　Ver1.1

この報告書は、AI技術の利活用に伴うリスクを管理し、正のインパクトを最大化するためのガイドラインです。

- AIの利活用によるリスク管理：
  ステークホルダーにとって受容可能な水準でリスクを管理し、正のインパクトを最大化することを目的としています。
- 技術的、組織的、社会的システムの設計と運用：
  AIガバナンスは、技術的なシステム（プライバシーテックなど）、組織的なシステム（企業内のプライバシーガバナンスなど）、社会的なシステム（関連法令やガイドラインなど）を含みます。
- AI倫理とガバナンスの重要性：
  AIの倫理的利用とガバナンスの重要性が強調されています。企業や政府が共有するゴールに向けた取り組みが求められます。
- 国際協力と標準化：
  国内外の動向を見据えつつ、AIの社会受容の向上と産業競争力の強化を目指した規制、標準化、ガイドライン、監査などが検討されています。

2022年 AI戦略2022

- 「人間尊重」、「多様性」、「持続可能」の３つの理念のもと、Society 5.0を実現し、SDGsに貢献。
- ３つの理念の実装を念頭に、５つの戦略目標（人材、産業競争力、技術体系、国際に加え、差し迫った危機への対処）を設定。
- 特に、AI戦略2022においては、社会実装の充実に向けて新たな目標を設定して推進するとともに、パンデミックや大規模災害等の差し迫った危機への対処のための取組を具体化。
- なお、AIに関しては、経済安全保障の観点の取組も始まることを踏まえ、政府全体として効果的な重点化を図るための関係施策の調整や、量子やバイオ等の戦略的取組とのシナジーを追求すべきことを提示。

AIに関するガイドライン（日本）３/３

2024年 AI事業者ガイドライン
基本理念
① 人間の尊厳が尊重される社会（Dignity）
② 多様な背景を持つ人々が多様な幸せを追求できる社会（Diversity and Inclusion）
③ 持続可能な社会（Sustainability）

基本理念を実現するために、全ての対象者が、念頭に置くべき指針

Ⅰ 各対象者が取り組む事項
1) 人間中心
2) 安全性
3) 公平性
4) プライバシー保護
5) セキュリティ確保
6) 透明性

Ⅱ 社会と連携した取組みが期待される事項
7) アカウンタビリティ
8) 教育・リテラシー
9) 公正競争確保
10) イノベーション

今後注視すべき議論　自律型致死兵器システム（LAWS: Lethal Autonomous Weapons Systems）
LAWSの定義については、国際社会で議論が行われており、まだ定まっていませんが、我が国は、「一度起動すれば、操作者の更なる介入なしに標的を識別し、選択し、殺傷力を持って交戦することができる」という特徴を備えている兵器システムが、現在行われているLAWS議論の主な対象となるものと考えています。

簡易年表（プライバシー/AI　法律，ガイドライン）

再掲

信州大学 SHINSHU UNIVERSITY

主要な海外の動き

1980年
OECD8原則

2018年
Amazon失敗

2018年
倫理ガイドライン（欧州委員会）

2017年
アシロマAI 23原則

2019年
OECD　AI原則

2024年
AI ACT

1980 ～ 2015 ～ 2024

1988年
最初の個人情報保護法

2019年
人間中心のAI社会原則（政府）

2003年
個人情報保護法

2015年 改訂　2017年 改訂　2020年 改訂　2022年 改訂

日本の動き

2017年
人工知能学会が倫理指針

2021年
ITガバナンスのあり方v1.1（政府）

2022年
AI戦略2022（政府）

2023年
改正電気通信事業法第27条の12
（Cookieが規制）

2024年
AI戦略事業者ガイドライン（政府）

2013年
SUICA事件

2021年
JR東日本監視カメラ問題

2024年
食べログ裁判

SUICA事件

2013年SUICA事件

- 日立製作所にスイカ利用者の過去2年5か月分のデータ（乗降駅、性別、年齢、日時、利用額）を販売
  ※個人を特定できる名前や連絡先を削除していたため「個人情報に当たらない」
- 日立がデータを活用した駅周辺のマーケティング情報サービスを開始
- 利用者に無断で販売していたことに対して、7月25日に記者会見で謝罪

→ 販売を望まない利用者のデータは削除する（日立にデータの提供し直し）

平成29年情報通信白書（総務省）　個人情報の匿名加工とその利活用方法に関連する事案

このようにJR東日本が一貫した方針と利用者のパーソナルデータ保護等の対応をとりながらも、多くの利用者からの批判を受けたのは、**個人情報が漏れることへの利用者の不安を払拭できなかったことが第一にある。その一因は、同社がホームページ等で明らかにしているとおり、利用者に対し十分な事前説明を行わなかったことだ。ただしもう一点、大きな要因を挙げるならば、匿名加工されたパーソナルデータの利用に関するルールが未整備であったことも影響したと考えられる。**

JR東日本の監視カメラ問題

法令上の行為や義務を守るだけでなく、批判を受けないか、倫理上問題はないか

JR東日本の監視カメラ問題

2021年9月21日
JR東日本について「顔認識カメラを使って、刑務所からの出所者や仮出所者の一部を駅構内などで検知する防犯対策を実施している」と報道され、インターネット上で批判的な声が相次いだ。

- 東京五輪・パラリンピック開催に伴うテロ対策の一環で、顔認識機能を備える新たな防犯システムを導入
- カメラから通行人の顔情報を取得し、「過去にJR東日本の施設内で重大な罪を犯して服役した人」「指名手配中の容疑者」「うろつくなど不審な行動を取った人」を検知対象にして、検知した場合は警備員が出動して目視による確認のうえ、必要に応じて声かけや警察と連携した手荷物検査を実施する方針
- 個人情報保護委員会に相談したうえで法令にのっとった措置を講じていた（法的な問題についてはクリア）

炎上の理由
報道で明るみに出るまで、JR東日本がこうした詳しい運用方針を十分に公表していなかった点

国土交通省の立場
防犯カメラの顔認証システムの活用に当たっては、個人情報保護などにも十分配慮し適切に実施する必要がある。今後、鉄道事業者が（システム導入の）検討を進めていくに当たっては、こうした点に十分留意するよう指導、助言していく（JR東日本の防犯システムに批判的な世論に配慮）

インプットデータの公平性

焦点：アマゾンがＡＩ採用打ち切り、「女性差別」の欠陥露呈で

Jeffrey Dastin, 2018年10月14日,ロイターによれば、米アマゾン・ドット・コムが期待を込めて進めてきたＡＩ（人工知能）を活用した人材採用システムは、機械学習面の欠陥（女性を差別する）が判明し、運用を取りやめた。

コンピューターモデルに過去１０年間の履歴書（技術職のほとんどが男性からの応募）のパターンを学習させたため、システムに性別の中立性が働かない事実を見つけた。
※アマゾンの採用部門はＡＩシステムが示した評価に目は通したが、これだけに頼って実際の採用を決定してはいない。

詳しくは、ロイターの記事を読んで勉強して下さい。
出典：https://jp.reuters.com/article/world/-idUSKCN1ML0DM/

アルゴリズムの妥当性

「食べログ」逆転勝訴、アルゴリズム変更は妥当　高裁判決

2024年1月19日の日本経済新聞よれば、グルメサイト「食べログ」の評価が不当に下がり、売り上げが減少したとして、飲食チェーン店がサイト運営のカカクコムに損害賠償などを求めた訴訟の控訴審判決で、東京高裁は飲食チェーン店側への賠償を命じた一審判決を取り消した。

	飲食店	食べログ	一審判決	二審判決
アルゴリズム変更は独禁法違反に当たるか	優位的地位を利用して不利益を課せられた	変更には正当な理由がある	独禁法に違反する	不当なものとまで認められない
変更による損害はあったか	来店客の減少とブランド価値の毀（約６億円超の損害）	損害が生じたとの立証がなされていない	新型コロナウィルス感染拡大の影響もあり損害は3840万円	独禁法違反に当たらず

詳しくは、日経新聞社の記事を読んで勉強して下さい。
出典：https://www.nikkei.com/article/DGXZQOUE11BU10R10C24A1000000/

この判例より、アルゴリズムをサービスに組み込む場合、**社会に対する説明責任（アカウンタビリティー）**や**社会構成員の理解可能性**が重要である。

その他の話題

GDPR　第４章　プロファイリングの定義
特定の個人の個人情報を用いて、自動化された手法によって能力，嗜好，経済状態など個人的側面を分析または予測すること

2014年アメリカ大統領府報告書「Big Data：Seizing Opportunities, Preserving Values」
ビックデータの利用可能性とともに、**プロファイリングによる社会的差別への警鐘**が提言されていた。

個人情報保護法　第３４条，第３５条　（GDPR 第17条 消去の権利/忘れられる権利）
一定の要件のもと本人が提供した情報の利用停止や消去を請求できる(日本では法令違反が認められる場合のみ)

AI関連の特許条件
AIの機械学習の教師データの間に相関関係等の一定の関係が存在すると認められること

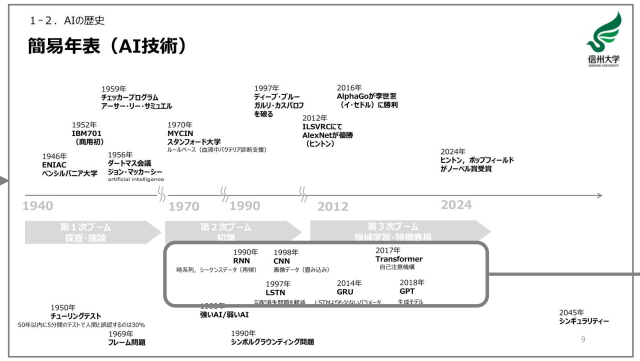
AIを用いた法律に関する助言業務が法律違反になる可能性があるという見解（2022年，法務省）
生成された内容の正確さに注意を払う必要がある

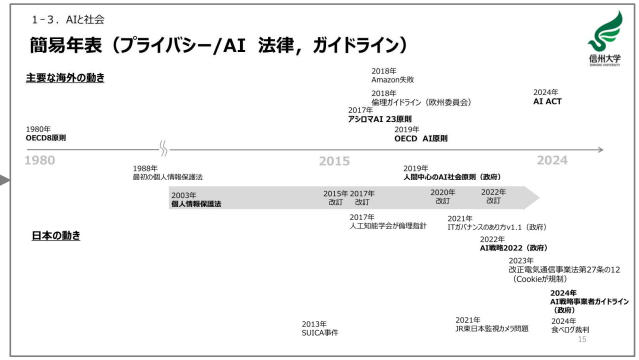
利用された文書，画像の著作権
憲法第13条（肖像権との関係）

まとめ

AIとは

AI歴史





AI法規制

AIを支える技術要素