

消費者庁様

消費者のデジタル化への対応に関する検討会

AIワーキンググループ 第二回資料

資料 4

消費者が知っておくべきAIシステムの基礎



EAGLYS株式会社
代表取締役社長
今林 広樹

本資料は、消費者に適切なメッセージを届けることを目的とし、事前に本ワーキンググループにご参画の委員間において、AIシステム概要について認識をそろえるために、「消費者が知っておくべきAIシステムの基礎」として基礎知識を整理したものです。本資料を元に、消費者へのメッセージを検討する土台とできたら幸いです。

消費者が知っておくべきAIシステムの基礎

1. 「AI」という言葉の整理
2. 既存システムとAI搭載システムとの違い
3. 現AIシステムの動作
4. AIシステムの利便性とリスク（例）
5. まとめ

1. 「AI」という言葉の整理 [1/3]

IT (ICT)も明確な定義がないほど、AIも定義をすることが難しい。
そのため、定義を追求するのではなく、その都度、議論対象である
AIの目的、要件、機能、前提条件などを整理し、明確にすることが重要。

ICT (Information and communication technology)の定義

「 the study, design, development, implementation, support or management of computer-based information systems, particularly software applications and computer hardware. 」
(Information Technology Association of America (ITAA))

→ 翻訳

「コンピュータをベースとした情報システム、特にアプリケーションソフトウェアやコンピュータのハードウェアなどの研究、デザイン、開発、インプリメンテーション、サポートあるいはマネジメント」
(アメリカ情報工学協会)

参照:

ICT difinition: <https://wiki.nus.edu.sg/pages/viewpage.action?pageId=16351965>

ITAA (Wikipedia): https://en.wikipedia.org/wiki/Information_Technology_Association_of_America EAGLYS Inc.

1. 「AI」という言葉の整理 [2/3]

現在活用される「AI」とは「機械学習」を指している。消費者向けには、過度な不安にならないよう、あくまで人間の設計に基づく動作範囲である旨を伝える。

「AI (Artificial Intelligence, 翻訳: 人工知能)」の2つの設計視点
X. 人間の知能で処理する事を、機械にさせようとする視点
Y. 人間の知能そのものを持つ機械を作ろうとする視点

現在、企業で研究・活用されるAIは前者「**X**」。
→ 機械学習と呼ぶ。(定義・説明は次ページ)

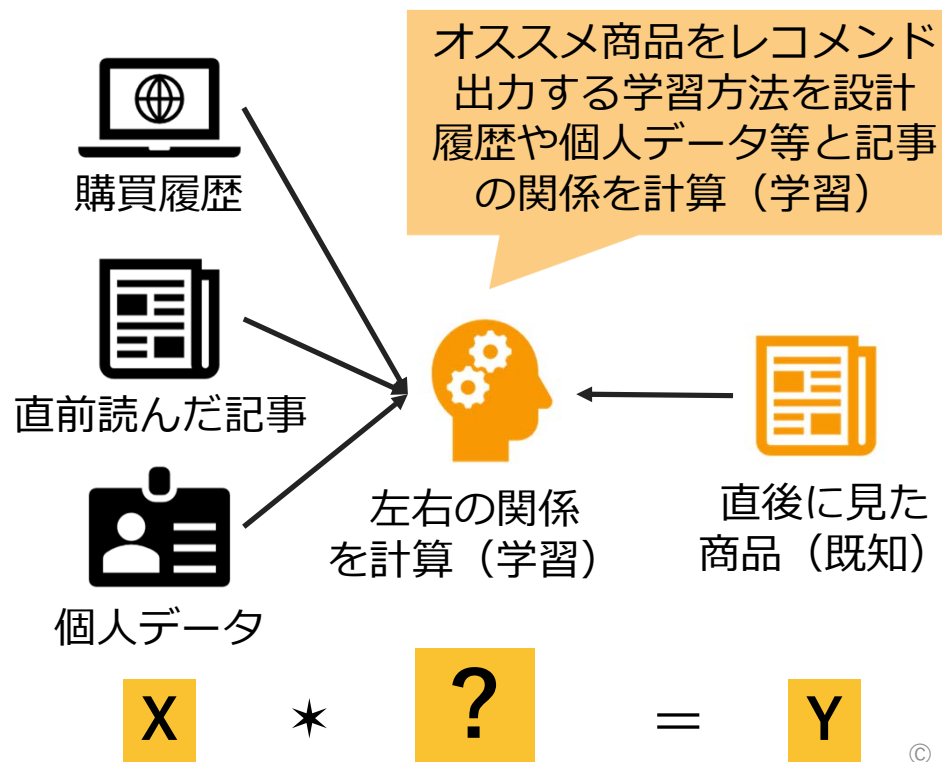
あくまで、設計者のシステム出力要件に合わせたデータの**学習**と、その方法に基づいて論理的な**推論**を行うため、従来のシステムと同様、設計者の指示に基づく動作範囲となる。

※動作（出力）の品質や精度については各事業者によるところ。一般に約束が難しい。

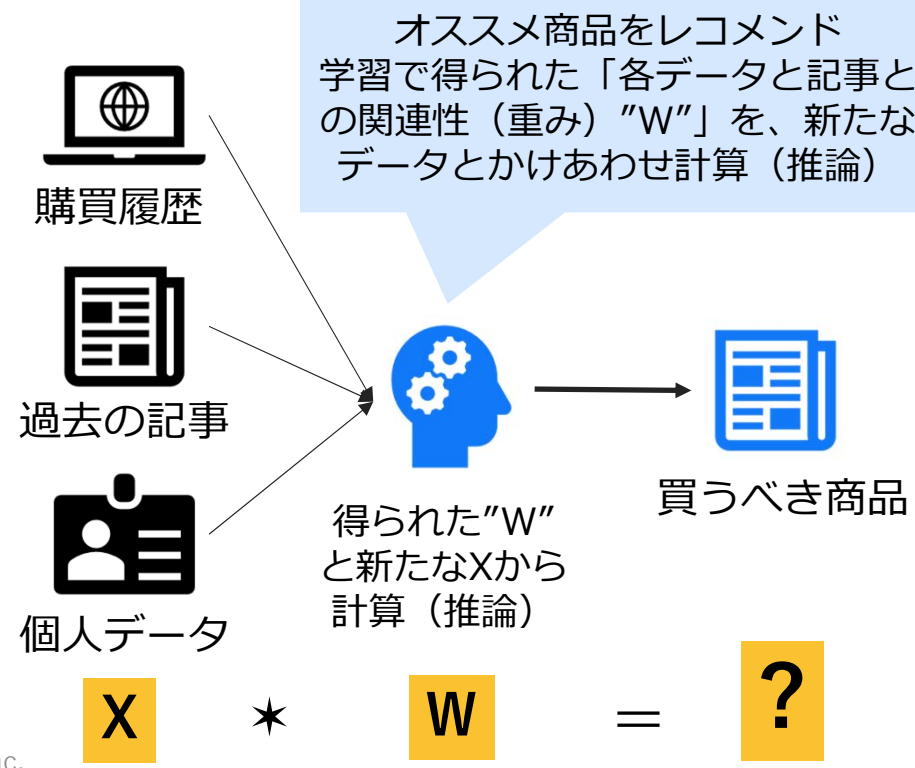
1. 「AI」という言葉の整理 [3/3]

機械学習とは、①ある出力要件（目的）に必要なデータ（テキスト、画像・動画、音声など）を学習する学習演算方法と、②新たなデータから目的の出力を得る推論演算方法、を備える技術。

①学習



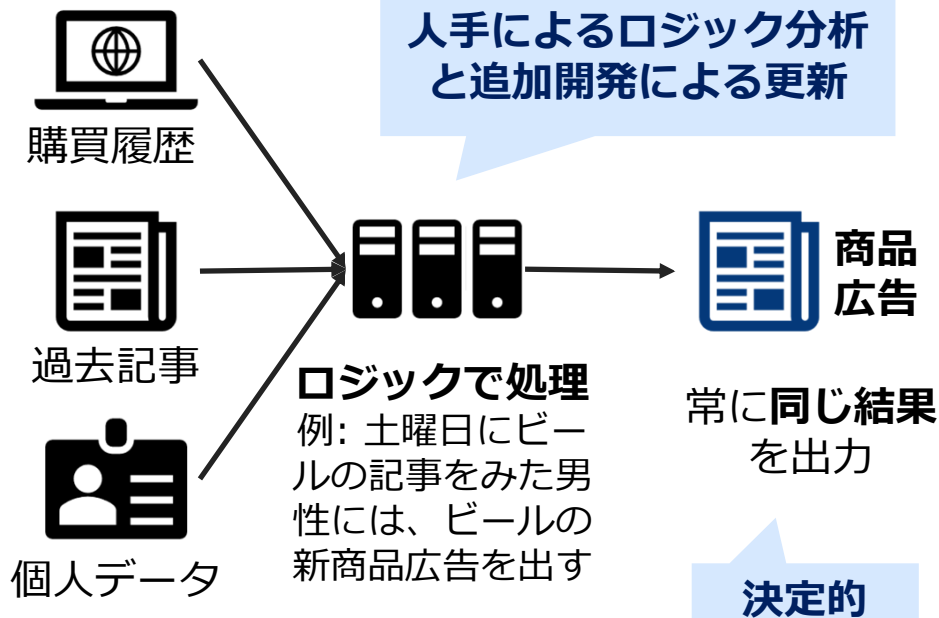
②推論



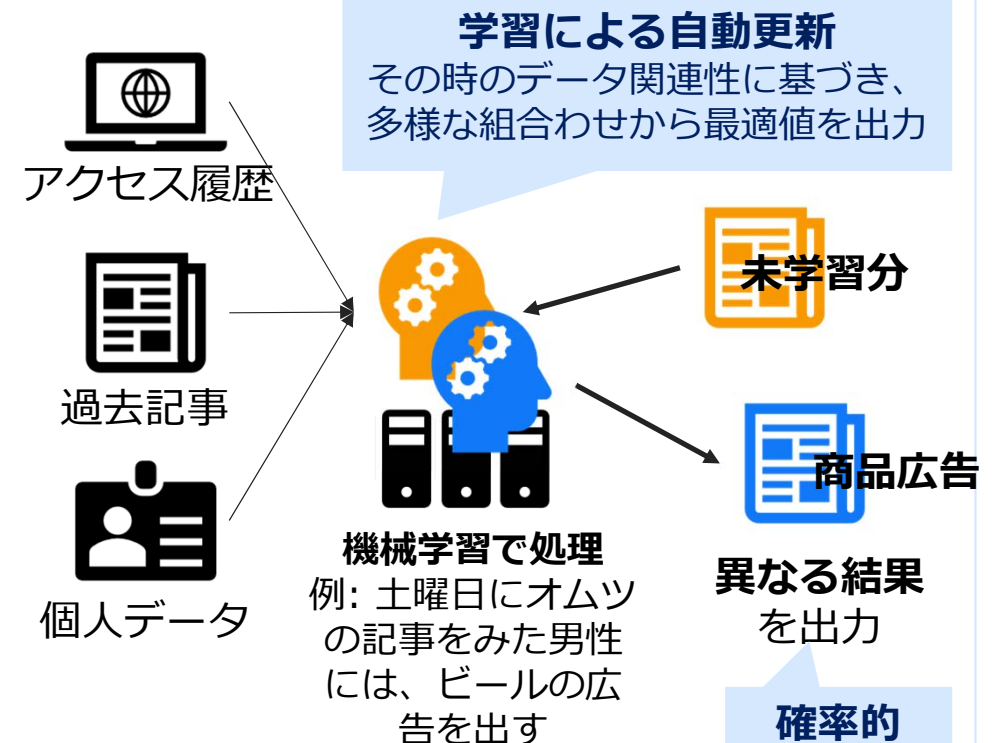
2. 既存システムとAI搭載システムとの違い

システムにAI（機械学習）を搭載することにより、学習機能で出力更新がリアルタイムに近くなり、また出力も確率的となるため、あくまでシステム要件設定の中で、出力の柔軟性が高まる。

既存システム



AI搭載されたシステム



「要件定義によるシステム設計」では、「人間の知能そのものを持つ機械」という意味での人工知能は実現しない

コンピュータ（計算機）は、演算方法（アルゴリズム）を与えることで、いかなる論理演算を実現する。計算機は、人間が演算方法を詳細に与えない限り動作を開始できない機械である。演算方法の要件を定義し設計するのは人間であり、知能が定義できない以上は、「人間の知能そのものを持つ機械」という意味での人工知能は実現できない、と考える。

「人間の知能で処理する事を、機械にさせようとする視点」で考える範囲においては、人間が機械にやらせたいこと（自動化したいこと）を要件定義し、それを達成する最小限の設計で実装することになるため、動作の範囲はあくまで目的出力の範囲およびそれを得る計算のみに絞られる（目的出力以外の目的を達成できない）、と考えられる。

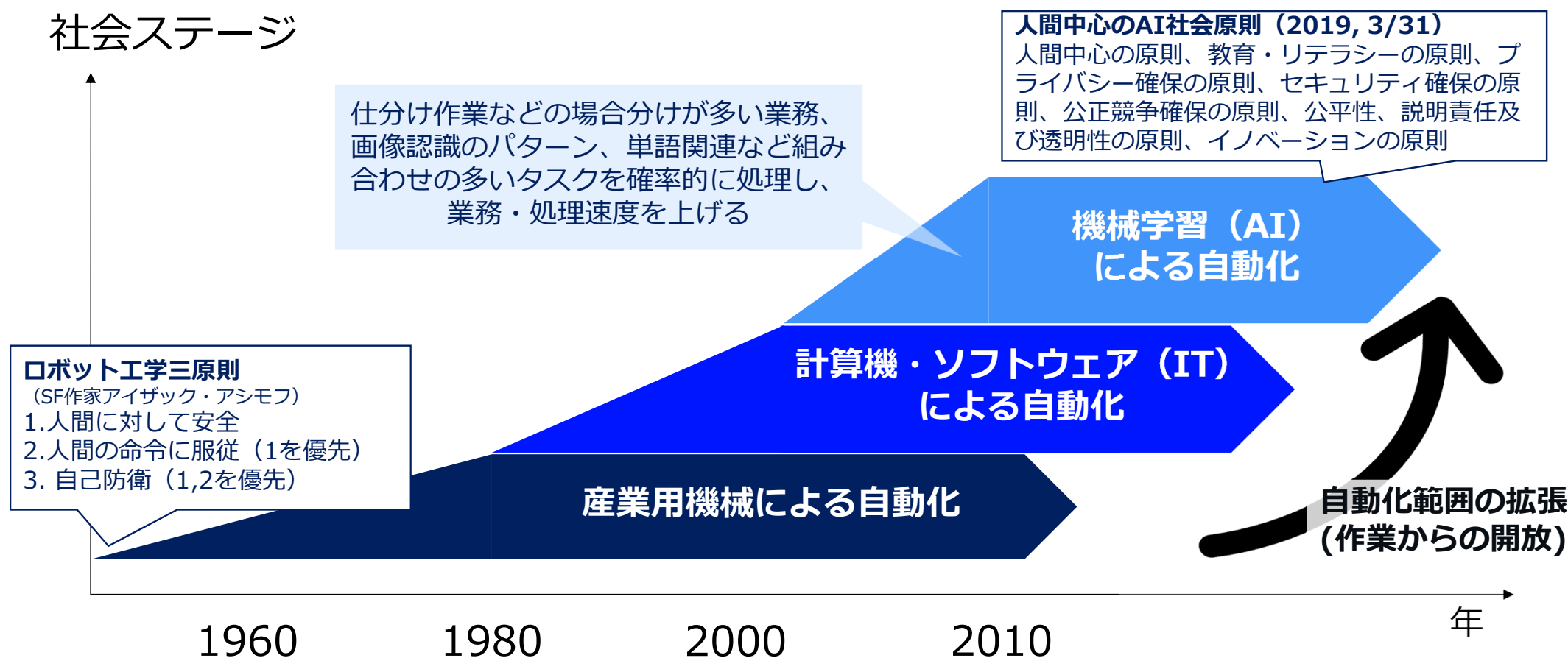
「目的・要件を定義（解く問題を設定）して、演算方法を設計（解決方法を決定）すること」を人間が行うという前提においては、「どんな処理もAIが行うことになる、つまり例えば仕事も全て機械に奪われる」ということは起こりえない、と考えている。



消費者は、使用検討しているAIシステムについて「メーカー含む提供企業がこういった出力要件を約束しているのか」を知っている限り、過度に心配する必要はない。
そのシステムを活用する過程で、取得されているデータがシステム外の目的で活用される場合があることを認識し、必要に応じてその活用方法を把握するように務める。

コラム（雑談）[2/2] 産業における自動化の歴史

自動化により働き方は豊かに。AIもその延長であり生活を豊かにするもの。



ロボット工学三原則

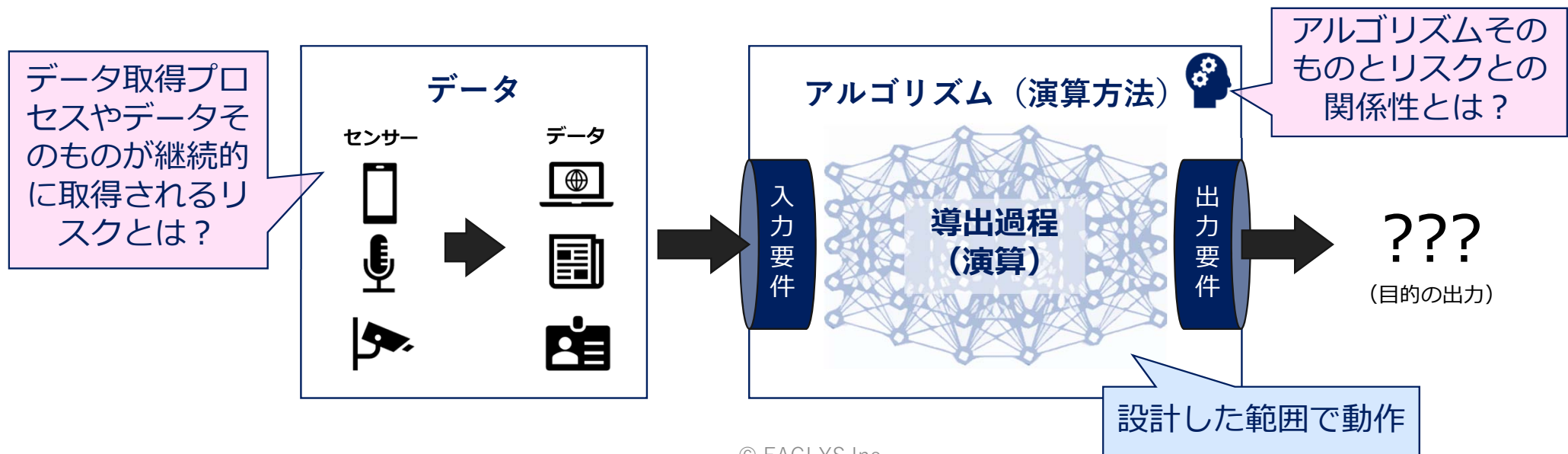
(SF作家アイザック・アシモフ)

1. 人間に対して安全
2. 人間の命令に服従 (1を優先)
3. 自己防衛 (1,2を優先)

3. 現AIシステムの動作 [1/2]

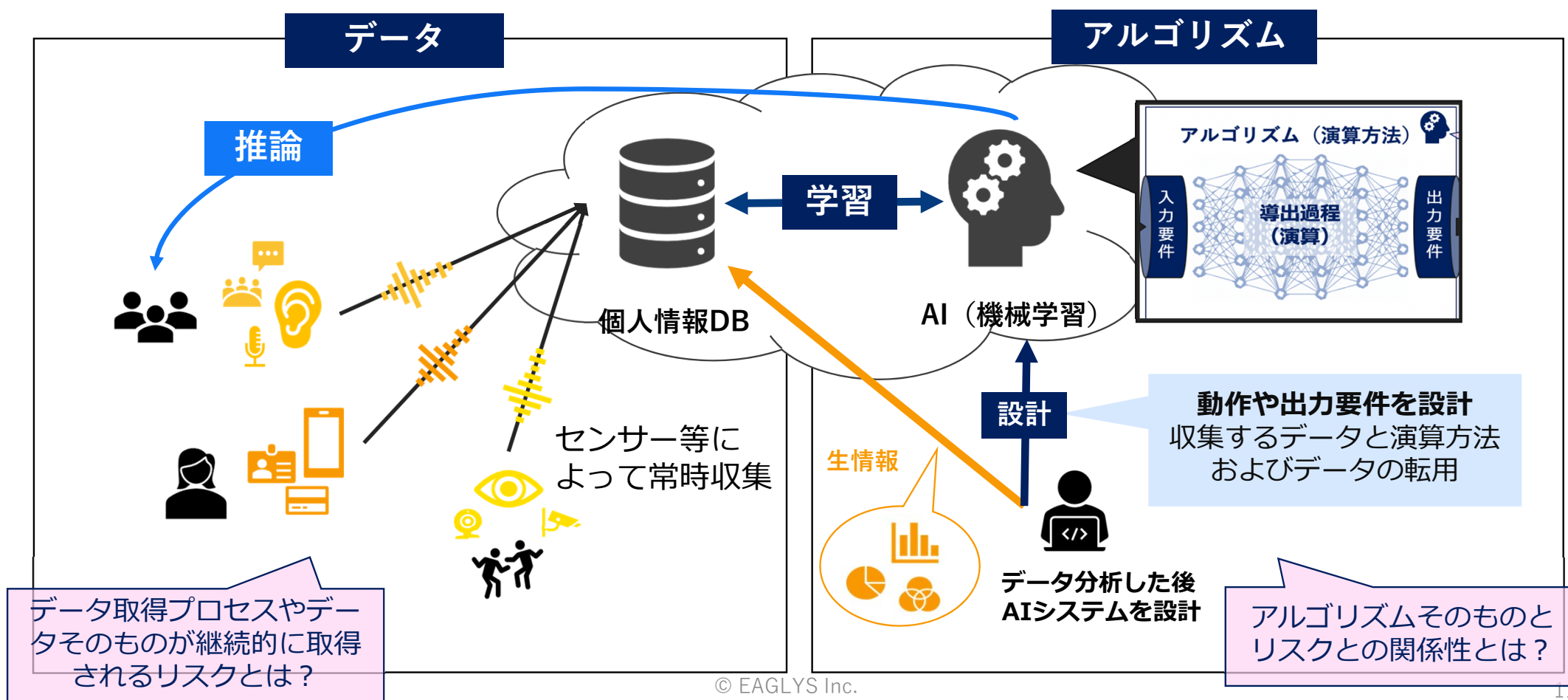
アルゴリズム（演算方法）とデータとに区別して、
AI活用のリスクを検討する必要がある。

- AIシステムは、学習・推論を行う「アルゴリズム（演算方法）」とそれにくわせる「データ」（取得するためのセンサー等含む）との掛け合わせからなる。
- アルゴリズム（演算方法）は、出力要件（達成目的）、導出過程（演算）、およびその入力要件は、あくまで設計した範囲で動作をする。



3. 現AIシステムの動作 [2/2]

アルゴリズムとデータとに区別して、AI活用のリスクを検討



4. AIシステムの利便性とリスク（例） [1/2]

[利便性面] AI活用により以下のような利便性を享受できる（以下は一例）

AI活用による利便性の享受

- 迅速な情報収集や見逃しがちな情報の発見が可能に
- 人間のように柔軟、かつ迅速なチャットサポートを受けられる
- 書類仕分け等の自動化により雑務から解放される
- 医療診断の低コスト化や診断精度の向上により、病気リスクの削減
- AIスマート家電により生活環境の心地よさの向上
- 無人化によりコンビニ等への並ぶ大変さを回避
- …等



- AIの判断を鵜呑みにしなければ、AIは判断の良きサポーターとなる。
- AIの出力は状況に応じて柔軟な出力をしてくれる。
- 生活の中のめんどくさい作業を自動化してくれる。

4. AIシステムの利便性とリスク（例） [2/2]

[リスク面] データ / アルゴリズム の観点からAI活用のリスク・対策を検討（以下は一例）

	データ	アルゴリズム
リスク	取得されるデータは、他システムで再利用される可能性がある 利用規約を無理やり承諾させようとするHP・サービス、cookieへの同意を強要するサービスは、データ連携され活用されている可能性がある。 一つのプラットフォームサービスでは、共通IDによりデータが連携されるため、知らぬところで個人情報化、自身の与信に使われている可能性がある アカウントのっとり、フェイクによる被害が多発する	AIはあなたの好みに合わせて提案するため、例えばチークばかりを探していたら、化粧品に偏ってレコメンドをするような学習をしてしまう可能性がある。本来ほしい商品にたどり着きにくくなる可能性がある。 そのサービスを十分に使っていないと、データ量が蓄積していない可能性があり、AIはミスを連発する。 また、AIシステムからの出力は確率的であり、鵜呑みにすると判断を間違える可能性がある。
対策	サービスの利用規約に、データ活用の可能性、個人情報やプライバシーへの配慮などについて触れているところがあれば、確認する。すべてに簡単に承諾せず、必要最低限の承諾を行う。 特に生活データ、嗜好性、医療のデータ種。自ら個人情報を出す際には、それによるサービス対価を考える。ときには匿名も選択肢に。 中長期では、データを提供・連携することによるクーポン獲得、クレジットの獲得、金銭の獲得などが発生するため、現在活用しているサービスの蓄積データが流通する可能性を認識する	AIが活用されていることを認識できるサービスにおいては、何をアウトプットしてくれるのか、何を元に判断しているのか、を可能な限り情報収集のアンテナを立てつつ、サービスを利用する。 AIが何でもできるわけではないことを理解する。あくまで、サポートの立ち位置ととらえ、最終的に決めるのはあなた自身である。AIの判断を鵜呑みにしない。 中長期では、個人がデータ・AI活用許諾を行えるようになることを想定し、対象のAIサービスにおける自身のデータやパラメータについて忘却の権利の実装有無を確認する。

5. まとめ ～方針案～

AIシステム概要やAIの良さについて説明したのち、
AIの特性上、一般にあてはまるリスクを適度に説明する

AIシステム概要 (P6,7,10,11等)

- AIの学習・推論機能、既存システムとの違い、AIシステムの動作について

AIの良さ (P12等)

- AIは生活を豊かになるようサポートしてくれる利便性の高いものである
- 現AIは、人間の脳の模倣ではなく、コンピュータ計算の延長上の機能として設計されており安心できる（特定の計算目的に閉じている）

AIのリスク (P13等)

- 「データ」を取られるリスク（個人情報収集、他サービスへ連携・活用される不安）
- 「アルゴリズム（演算方法）」によってデータが学習され、推論結果を受け取るリスク（あくまで予測、確率的な出力であるため、信頼度が低い）