

AI とプライバシー・個人情報
～ヒト型ロボットをめぐる論点～

筑波大学
図書館情報メディア研究科
2018 年 3 月
大西 侑気

目次

第1章	研究背景・目的	1
第1節	ロボットをめぐる政府の動向	1
第2節	AI・ロボットの活用とリスク	3
第3節	AI・ロボットの活用によるプライバシー・個人情報に関する リスク	7
第4節	研究目的	10
第2章	ヒト型ロボットの特徴と関連する AI 技術	13
第1節	ロボットの定義	13
第2節	ロボットの類型	14
第3節	AI	15
第4節	小括	21
第3章	アメリカ合衆国	22
第1節	政策的動向・法制度	22
第2節	2020 年における人工知能と生活	25
第3節	人工知能及び自律システムの倫理的配慮に関する IEEE グローバル ・イニシアティブ	28
第4節	ロボット倫理における「ロボットとプライバシー」	37
第5節	プライバシーを保持するクラウド上のロボット	41
第4章	欧州連合 (EU)	45
第1節	一般データ保護規則 (GDPR)	45
第2節	ロボティクスの民事法規則	53
第5章	日本	59
第1節	政策動向・法制度	59
第2節	プロファイリング	63
第6章	考察・結論	66
第1節	各章の要旨	66
第2節	プライバシー保護の観点からの提言	70
第3節	個人情報保護法の観点からの提言	72
第4節	結論	73

参考・引用文献リスト

AIとプライバシー・個人情報 ～ヒト型ロボットをめぐる論点～

第1章 研究背景・目的

第1節 ロボットをめぐる政府の動向

2014年7月、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO: New Energy and Industrial Technology Development Organization）は、「世界初」と銘打ち、「NEDO ロボット白書 2014」¹を公表した。この白書は、NEDO と経済産業省が連携して行ったロボットの将来市場予測²を引用し、ロボット産業の将来市場（国内生産量）は、2020年には2.9兆円、2035年には9.7兆円まで成長するとの予測³を示している。

また、ロボット白書では、ロボットの意義・必要性を「産業界」・「社会」・「教育」の3つの観点から評価している。「産業界」においては、ロボットが3K（危険、汚い、きつい）作業から作業者を開放し、少子高齢化による労働力不足や、熟練工の減少問題に貢献できるのではないかと期待されている。「社会」では、超高齢社会⁴である日本において、ロボットが高齢者・障がい者の生活支援・社会参加実現のために身体機能を補助し、商業施設などでの案内支援・情報提供、家庭での生活支援、コミュニティ形成支援、介護者の負担軽減を目的としたサービスを行うことが期待されている。「教育」において、ロボットを用いた教育は学習者に強い印象を与えることができることや、課題発見能力、自己解決能力、協調作業能力を養うことができるといった特徴があり、また、子供の理科離れ対策や、今後ロボットが普及段階に入った場合に必要なロボットリテラシーを養うためにも、ロボット教育は必要とされている。

このように、ロボット産業の急激な成長が予測されており、ロボットの助けを得ることによって、日本が抱える様々な課題が解決されることが期待されている。政府は「ロボットを少子高齢化の中での人手不足やサービス部門の生産性の向上という日本が抱える課題の解決の切り札にすると同時に、世界市場を切り開いていく成長産業に育成していくための戦略」として、2015年1月に「ロボット新戦略⁵」を打ち出し、ものづくり、サービス、介護・医療、インフラ災害対応・建設、農林水産業・食品産業の5分野に関して2020年までの5年間⁶におけるアクションプランを策定した。この中で、政府は、日本が現在に至るまで産業用ロボットの出荷額及び稼働台数において世界第1位であり、「ロボット大国」としての

¹ 国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）『NEDO ロボット白書 2014』（NEDO、2014）http://www.nedo.go.jp/library/robot_hakusyo.html

² 「ロボットの将来市場予測を公表」（NEDO、2010）
http://www.nedo.go.jp/news/press/AA5_0095A.html

³ 2015年時点では1.6兆円

⁴ 総人口のうち、65歳以上の占める割合が21%を超えた社会の呼称として使用される語であるが、確たる定義は見られない。

⁵ 日本経済再生本部『ロボット新戦略』（日本経済再生総合事務局、2015）
<http://www.meti.go.jp/press/2014/01/20150123004/20150123004.html>

⁶ 2015年度から2019年度を指す。

地位を維持していると自負しつつも、少子高齢化による生産年齢人口の減少、人手不足、社会保障費の増大に直面する課題先進国⁷であると指摘した。このため、ロボットによる新たな産業革命（ロボット革命）の実現や、「日常的に人とロボットが共存・協働する社会を実現するために必要な前提条件を整えた」とする「ロボットバリアフリー社会」の実現を訴えている。また、第 5 期科学技術基本計画⁸や未来投資戦略 2017⁹でも同様に、ロボットを活用した課題解決が企図されている。

各省庁においてもロボット、そして人工知能（AI:Artificial Intelligence）について盛んに検討が行われている。総務省は、AI の普及に伴う社会的・倫理的課題について、2015 年 2 月に「インテリジェント化が加速する ICT の未来像に関する研究会¹⁰」を発足させ、2016 年 2 月には「AI ネットワーク化検討会議¹¹」、2016 年 10 月には「AI ネットワーク社会推進会議¹²」をそれぞれ設置し、検討を重ねてきた。2017 年 7 月には、AI ネットワーク社会推進会議の報告書が公表¹³され、同報告書の中では「国際的な議論のための AI 開発ガイドライン案」¹⁴が示された。経済産業省は、CPS によるデータ駆動型社会¹⁵を世界に先駆けて

⁷ ロボット新戦略の中に用語の定義は見られない。2013 年に公表された「日本再興戦略」（http://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/saikou_jpn.pdf）では、「今、日本は、いずれ世界の国々が直面することとなる少子高齢化、資源・エネルギー問題などに真っ先に取り組まざるを得ない「課題先進国」の立場に置かれている。」と述べていることから、「課題先進国」とは、我が国が他国に先んじて課題に直面しており、これを解決しなければならない状況にあることを指している。特に高齢化について、我が国は世界に先駆けて超高齢化社会に突入し、最も高い高齢化率となっている。（内閣府『平成 28 年版超高齢社会白書』（内閣府、2016）http://www8.cao.go.jp/kourei/whitepaper/w-2016/zenbun/28pdf_index.html

⁸ 『第 5 期科学技術基本計画』（閣議決定、2016）

<http://www8.cao.go.jp/cstp/kihonkeikaku/index5.html>

⁹ 『未来投資戦略 2017』（閣議決定、2017）

<http://www.kantei.go.jp/jp/singi/keizaisaisei/kettei.html>

¹⁰ 「インテリジェント化が加速する ICT の未来像に関する研究会」（総務省）

http://www.soumu.go.jp/main_sosiki/kenkyu/intelligent/

¹¹ 「AI ネットワーク化検討会議」（総務省）

http://www.soumu.go.jp/main_sosiki/kenkyu/iict/

¹² 「AI ネットワーク社会推進会議」（総務省）

http://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/

¹³ 「AI ネットワーク社会推進会議 報告書 2017 の公表」（総務省、2017）

http://www.soumu.go.jp/menu_news/s-news/01icp01_02000067.html

¹⁴ 総務省の報道資料では、「研究開発において留意することが期待される事項」の「国際的な議論の基礎となる文書」として、「AI 開発原則」とその解説である「非規制的で非拘束的なソフトローとしての指針の案」を作成したと説明されている。

¹⁵ 経済産業省情報経済小委員会の中間取りまとめ（後掲注 17）において、CPS（Cyber Physical System）は「デジタルデータの収集、蓄積、解析、解析結果の実世界へのフィードバックという実世界とサイバー空間との相互関連」と定義されている。データ駆動型社会は「上記 CPS が IoT（Internet of Things）によるモノのデジタル化・ネットワーク化によって様々な産業社会に適用され、デジタル化されたデータが、インテリジェンスへと変換されて現実世界に適用されることによって、データが付加価値を獲得して現実世界

実現すべく、2014 年から「産業構造審議会商務流通情報分科会情報経済小委員会¹⁶」を設置して現在まで検討を行ってきており、2015 年 5 月には中間取りまとめ¹⁷を公表した。内閣府は、2016 年 5 月、AI の研究開発及び利活用を健全に進展させるため「人工知能と人間社会に関する懇談会¹⁸」を設置し、2017 年 3 月に報告書¹⁹を公表した。内閣官房は、2016 年 10 月、AI 生成物とその生成に関するデータ等新たな情報財の知財制度上の在り方について検討を行うため、知的財産戦略本部検証・評価・企画委員会の下に「新たな情報財検討委員会²⁰」を設置し、2017 年 3 月に報告書²¹を公表した。また、省庁連携の観点からは、2016 年 4 月に「人工知能技術戦略会議²²」が創設された。それによると、同会議が司令塔となって、総務省、文部科学省、経済産業省が所管する 5 つの国立研究開発法人²³が束ねられ、これらの法人が AI 技術の研究開発を進めるとともに、関係省庁と連携して AI 技術の社会実装を進めるとしている。同会議は、2017 年 3 月には取りまとめとして「人工知能技術戦略²⁴」を公表し、今後は定期的に戦略のフォローアップを行うことになっている。

第 2 節 AI・ロボットの活用とリスク

ロボットの頭脳である「AI」とは何かについて、総務省の「インテリジェント化が加速する ICT の未来像に関する研究会 報告書 2015²⁵」が行政機関の報告書としては詳しいが、本論文では、同研究会の構成員を務めた東京大学の松尾豊特任准教授の著書²⁶である「人工

を動かす社会」と定義されている。

¹⁶ 「産業構造審議会商務流通情報分科会情報経済小委員会」（経済産業省）

http://www.meti.go.jp/committee/gizi_1/32.html

¹⁷ 情報経済小委員会「情報経済小委員会 中間取りまとめ報告書について」（経済産業省、2015）http://www.meti.go.jp/committee/sankoushin/shojo/johokeizai/report_001.html

¹⁸ 「人工知能と人間社会に関する懇談会」（内閣府）

<http://www8.cao.go.jp/cstp/tyousakai/ai/>

¹⁹ 人工知能と人間社会に関する懇談会『人工知能と人間社会に関する懇談会 報告書』（内閣府、2017）<http://www8.cao.go.jp/cstp/tyousakai/ai/summary/>

²⁰ 「知的財産戦略本部検証・評価・企画委員会新たな情報財検討委員会」（内閣官房）

http://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/

²¹ 新たな情報財検討委員会『新たな情報財検討委員会 報告書』（内閣官房、2017）

http://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2017/johozai/houkokusho.pdf

²² 「AI ポータル」（NEDO）http://www.nedo.go.jp/activities/ZZJP2_100064.html

²³ 情報通信研究機構（NICT）、理化学研究所（理研）、産業技術総合研究所（産総研）、科学技術振興機構（JST）、新エネルギー・産業技術総合開発機構（NEDO）。特に NICT の脳情報通信融合研究センター（CiNet）及びユニバーサルコミュニケーション研究所（UCRI）、理研の革新知能統合研究センター（AIP）、産総研の人工知能研究センター（AIRC）が中心となって AI 技術の研究開発を推進している。

²⁴ 人工知能技術戦略会議『人工知能技術戦略』（内閣府、2017）

<http://www.nedo.go.jp/content/100862413.pdf>

²⁵ 「「インテリジェント化が加速する ICT の未来像に関する研究会」報告書の公表」（総務省、2015）http://www.soumu.go.jp/menu_news/s-news/01iicp01_02000031.html

²⁶ 松尾豊『人工知能は人間を超えるか ディープラーニングの先にあるもの』

知能は人間を超えるか ディープラーニングの先にあるもの」を紹介する。松尾特任准教授は、AIを「単純に言えば、ロボットの脳に当たるのが人工知能」と説明するが、「人工知能の研究対象は、ロボットの脳だけ」ではなく、そもそも「ロボットのような物理的な身体は必要ない」としている。これは、「将棋や囲碁のように抽象的なゲームの研究」や「入力した情報をもとに判断をする能力の研究」もAIの研究対象であるためである。松尾特任准教授は、「人工知能研究は、『考える』ことを実現するために、抽象的な『目に見えないもの』を扱っている学問」であると述べ、「世の中で人工知能と呼ばれるものを整理すると、次のようなレベル1からレベル4の4段階に分けることができそうである」と説明している²⁷。

レベル1：単純な制御プログラムを「人工知能」と称している

レベル2：古典的な人工知能

レベル3：機械学習を取り入れた人工知能

レベル4：ディープラーニングを取り入れた人工知能

レベル1は「ごく単純な制御プログラムを搭載しているだけ」、レベル2は「入力と出力の組み合わせの数が極端に多いもの」、レベル3は「入力と出力を関係づける方法が、データをもとに学習されているもの」で、「機械学習²⁸のアルゴリズムが利用される場合が多い」もの、レベル4は「機械学習をする際のデータを表すために使われる変数（特徴量²⁹と呼ばれる）自体を学習するもの」で、ディープラーニング³⁰がこれに当たると説明されている。また、最近の人工知能はレベル3を指すことが多く、投資・技術開発が活発に行われているのはレベル4の領域と整理されている。

このような整理に従うならば、「第1章第1節 ロボットをめぐる政府の動向」において想定されているAIはレベル3とレベル4が該当すると考えられ、「機械学習」と「ディープラーニング」がAI関連技術の鍵となる。

機械学習やディープラーニングを始めとするAI関連技術の活用について、人工知能技術戦略会議の報告書「人工知能技術戦略」では、「生産性」、「健康、医療・介護」、「空間の移動」、「情報セキュリティ」の3つが重点分野³¹と整理され、それぞれ目指すべき社会像が以下のとおり示されている。

(KADOKAWA、2015) 47-54 頁

²⁷ 松尾・前掲注 26・51～53 頁

²⁸ 松尾特任准教授は「機械学習というのは、サンプルとなるデータをもとに、ルールや知識を自ら学習するもの」と説明している。

²⁹ 機械学習の入力に使う変数で、対象の特徴を定量的に表すもの。

³⁰ 松尾特任准教授は「ディープラーニングは、データをもとに、コンピュータが自ら特徴量をつくり出す」と説明し、人間が介在して特徴量を設計することなく、コンピュータが自ら特徴量を獲得し、それをもとに画像を分類できるようになるとしている。

³¹ 「情報セキュリティ」が4つ目の重点分野として示されているが、先の3つの分野に横断的な分野として報告書には別記されていることから、図表1からは除いた。

図表 1 人工知能技術戦略における重点分野と目指すべき社会像

重点分野	目指すべき社会像
生産性	<p>・生産システムの自動・最適化、サービス産業の効率化・最適化、物・サービスへのニーズとのマッチングによりユーザー主導型のハイパーカスタマイゼーションが実現される。これにより、ものづくり・流通・サービスの融合が進み、エネルギー・食料なども含めた社会全体としての生産性を高めた、無駄のない究極のエコシステムを構築する。</p> <p>・人が創造力を増幅することにより、次々と新しいサービス・製品が生み出される社会が構築される。</p>
健康、医療・介護	<p>・世界で最初に急激な高齢化社会を迎えている日本において、医療・介護の膨大な情報をビッグデータ化し、AI を使って世界一の医療技術先進国・介護技術先進国を構築する。</p> <p>・予防医療の高度化により、病気にならないヘルスケアを実現する健康長寿産業大国を構築する。2030 年には我が国人口の 40%以上が高齢者となる中で、80 歳でも就業を希望する高齢者が元気に働いている社会を実現する。これにより、個人としての満足度を上げるだけでなく、社会保障費の軽減を図ると同時に労働人口の減少という課題への対応の方策ともなる。</p>
空間の移動	<p>・人の移動時間・移動空間を、「移動」そのものではなく、その他の「作業」、「生活」、「娯楽」を行う時間・空間にする。</p> <p>・全ての人に自由で安全な空間の移動を確保する社会を構築する。人・物の移動にかかる移動手段のシェアリングエコノミーを構築することにより、移動のエコ社会を実現する。これらにより、人的要因による事故を 2030 年にはゼロにすることを目指し、「移動」に伴う社会コストを最小化する。</p> <p>・移動の高付加価値化、自動運転等を活用した自律的な輸送配送、バーチャル移動も完成し、移動そのものに価値が生まれる社会を実現する。</p>

(「人工知能技術戦略」をもとに、筆者作成)

また、AI を活用したサービスや製品、取組みについて、2017 年時点で以下のようなもの³²などがある。

³² 神崎洋治『ロボット解体新書』(SB クリエイティブ、2017) 162-167 頁、
「画像認識で「目」を高度化」日経コンピュータ 4 月 28 日号 (2016) 26-31 頁、
「自然言語 AI を活用」日経コンピュータ 4 月 28 日号 (2016) 32-35 頁

図表 2 AI を活用するサービスや製品、取組みの例

名称など/提供元	概要
Google 翻訳 /Google	Web 翻訳サービス。AI を利用して、単語単位の翻訳ではなく、文章の意図を考慮して翻訳を行う。
Gmail /Google	Web メールサービス。AI を利用して、99.9%のスパム判定精度を提供。
Google Photo /Google	写真向けの Web ストレージサービス。AI が投稿した写真に写っている人物を判別、特定。
NVIDIA DRIVE PX、 NVIDIA Jetson /NVIDIA	自動運転やロボットで AI を使うための組み込み型コンピュータ。DRIVE は自動運転車両向け。Jetson はロボット・ドローン等小型機器向け。
顧客動線分析 /ガリバー、 ABEJA	店舗内天井に設置したカメラを用い、画像認識 AI が顧客の動線を把握。これを踏まえ、適切な店舗内配置を仮説検証する。
構造物劣化診断 /前田建設、モルフォ	建築構造物の劣化診断を目視から AI による画像解析に置き換えることで効率化を図る技術検証を進めている。(2015 年)
不審者の動作検出 /NTT コミュニケーションズ、 ALSOK	監視カメラによる自動監視において、注目すべき人間の動作を AI が検出し、不審者の疑いを監視員に知らせる。(2015～2016 年に実証実験)
群集行動解析 /豊島区、 NEC	屋外に設置した防災カメラを通し、帰宅困難者の殺到による密集などの異常事態を AI が検知してアラートを発信する。
関連記事の抽出 /ヤフー	AI がニュース記事を約 500 の項目で分類し、特定の記事との関連度を評価。現在 (2016 年 4 月)、関連ニュース表示に応用。
音声による番組予約・検索 /東芝	「新しく始まるドラマを録画したい」といった自然文を AI が理解し、テレビ番組を予約・検索できる。

(神崎洋治『ロボット解体新書』(SB クリエイティブ、2017)、
日経コンピュータ 4 月 28 日号 (日経 BP、2016) をもとに、筆者作成)

このように、政府の様々な戦略はロボットや AI に大いに期待し、日本の課題解決をロボットの活用により図ろうとしているが、他方で、ロボットの活用にはリスクが存在する。これについて、総務省の AI ネットワーク化検討会議の報告書³³では、1 つの章を割いてロボットを題材としたリスク・シナリオ分析を行っている。同報告書は、以下のとおり、リスクを 2 つに大別した上で、10 の項目に小別している。

³³ 「AI ネットワーク化検討会議 報告書 2016 の公表」(総務省、2016)
http://www.soumu.go.jp/menu_news/s-news/01iicp01_02000050.html

図表 3 総務省「AI ネットワーク化検討会議」が示すロボットのリスク

大分類	小分類
機能に関するリスク	<ul style="list-style-type: none"> ・セキュリティに関するリスク ・情報通信ネットワークシステムに関するリスク ・不透明化のリスク ・制御喪失のリスク
法制度・権利利益に関するリスク	<ul style="list-style-type: none"> ・事故のリスク ・犯罪のリスク ・消費者等の権利利益に関するリスク ・プライバシー・個人情報に関するリスク ・人間の尊厳と個人の自律に関するリスク ・民主主義と統治機構に関するリスク

(『AI ネットワーク化検討会議 報告書 2016』(総務省、2016)をもとに、筆者作成)

特に、プライバシー・個人情報に関するリスクや人間の尊厳と個人の自律に関するリスクは、一度侵害されると救済が困難な性質のものといえる。

また、前記「人工知能と人間社会に関する懇談会」の報告書では、様々な角度³⁴から AI 技術と人間社会についての論点を挙げている。具体的には、これまでの技術と AI 技術の違いについて、AI が自ら学習して急速に高度化する点、AI 技術が目に見える外形を持たず、モノやサービスの内側で機能する技術であり、外からは AI 技術の動作（使用・不使用・使用の程度）が見えづらい点から、いつのまにか身の回りに AI 技術が普及し、高度化していくという可能性を指摘している。そして、同報告書には数多くの論点が列挙されており、その中には、前記のプライバシー・個人情報に関するリスクや人間の尊厳と個人の自律に関するリスクも含まれている。

第 3 節 AI・ロボットの活用によるプライバシー・個人情報に関するリスク

「人工知能と人間社会に関する懇談会」の報告書等を踏まえ、AI・ロボットの活用に伴うリスクのうち、次のように、プライバシー・個人情報、人間の尊厳や個人の自律に関するリスクを整理した³⁵。

①利用者への説明の不足：

利用者への周知・通知が十分でないため、自身の権利を侵害されるおそれについて、利用者が予見できない可能性。また、権利侵害時において、侵害の回復が阻害される可能性。

³⁴ 倫理、法、経済、教育、社会、研究開発の 6 つ。

³⁵ なお、⑦はプライバシー・個人情報に特化したものではない。

少なくとも、以下の説明事項の不足が想定される。

- ・ロボット・AI・センサーの存在・稼働・設置位置や、それらによる情報取得の有無
- ・情報取得の目的・内容や用途
- ・プロファイリング³⁶による推定を含む、取得された情報の内容確認・訂正・削除・利用停止の請求方法や情報の第三者提供先

②利用者による同意の難化・形骸化：

ロボットやセンサーによる情報の取得・利用・第三者提供等に対する利用者の同意手段が十分な形で提供されないために、利用者の選択の自由が阻害される可能性。

同意手段が十分な形で提供されない場合として、少なくとも次に掲げるものが想定される。

- ・同意手段が、ロボットやセンサーによる利用者の情報取得等を行う現場から、時間的・空間的に離れたところで提供されている場合

例：警備ロボットが防犯を目的として来客者の顔情報等を記録する場合には、同意もしくは拒否の手段がロボットメーカーのホームページ等において公表されており、また、手続もそこで行う必要があるケース（現場では情報取得等の拒否ができないケース）

- ・「同意」が「サービスの利用」とトレードオフである場合

例：利用者の情報が必須ではないにも関わらず、ロボット等が行う利用者の情報取得に同意しなければサービスを受けられないケース

③AI・ロボット利用の強制：

人間ではなく、ロボットが提供するサービスの利用を強制され、利用者の選択の自由が阻害される可能性。

④AI・ロボットによる社会的排除・差別的取扱いの連鎖：

AIが行う判断のみに基づいた物事の決定に対し、不利益を被る者のための抗弁する機会が提供されない可能性。また、あるAIが行った特定個人に対する否定的評価が、ネットワークを通じて広がり、別の場面における否定的評価の決定材料の1つとなるように、AIによる排除が連鎖することで、排除される者は否定的評価を覆すことができず、永遠に社会から排除される状態に陥る可能性。個人の人格や能力をAIが確率的に判断してしまい、様々な可能性が事前に否定される可能性³⁷。

⑤AI・ロボットが提供する情報の偏向・操作：

プロファイリング等によって、偏った（過度に個人に最適化された）情報が個人に提供されてしまい、利用者の思想・常識の偏向が過度に強化される可能性。また、自律性を

³⁶ 個人の購買履歴・ウェブの閲覧履歴・全地球測位システム（GPS: Global Positioning System）位置情報・交流サイト（SNS: Social Networking Service）の情報などから、当人の趣味嗜好や健康状態などをAIに自動的に予測させる技術（山本龍彦「経済教室 AIのリスクに対応急げ」日本経済新聞 2017年4月26日29面）

³⁷ 山本・前掲注36

持つ AI が提供情報を操作することによって、個人の意思形成過程を侵し、自己決定を阻害する可能性。

⑥AI・ロボットによる利用者の予見範囲の超越：

機械学習によって、AI が製造者の当初予測を超えて高度化し、既に行われた利用者への説明範囲を超えた性能や性質（プロファイリング等情報分析の高精度化、提供情報の偏向の強化）が実現することで、利用者が予見していない権利等の侵害が、利用者の認識がないままに発生する可能性。特に、プライバシー性の高い情報は、その取得に厳格な同意を要するが、周辺情報の集積・分析によってそのような情報が明らかにされると、これまで守られてきた私的領域に踏み込まれる可能性が生じる。

⑦過度の産業規制：

法令等による過度の利用者保護規制により、ロボット産業の成長が阻害されてしまう可能性。

ロボット新戦略は、ロボットを「データ獲得のための仕組みの中核」とみている。このため、今後「ロボットによるデータ取得」に直結するプライバシー・個人情報に関するリスクが大きな位置を占めてくると考えられることから、①説明の不足、②同意の難化・形骸化、④AI・ロボットによる社会的排除・差別的取扱いの連鎖、⑥予見範囲の超越といった懸念への対処を検討する必要がある。

また、前述のロボット新戦略は、現在のロボットについて、「自律化」、「情報端末化」、「ネットワーク化」の点で劇的に変化しつつあると指摘する。「自律化」とは、自ら学習し、行動することを指し、機械学習やディープラーニングを含む AI 技術の発展に伴う、ロボットによる高度な処理を実現することを意味している。「情報端末化」は、ロボットがパソコンや携帯電話に代わり、データの蓄積・活用を行うことで付加価値の源泉となっていくことを指す。「ネットワーク化」は複数のロボットが相互に結び付き連携することを指し、ロボットが単体ではなく、様々なシステムの一部として機能する可能性を意味する。このような 3 つの変化が組み合わさると、個人の予見範囲を越えたプロファイリング等の行われる可能性が生じる。また、我々は、電話・メール・SNS・インターネットショッピング・趣味嗜好に係る事項の検索・動画の閲覧等、パソコン・スマートフォンを用いてあらゆる情報を管理・活用しているといって過言ではない。しかし、今後は、利用端末がロボットにとって代われ、ロボットに情報が集約されていく可能性が生じる。そして、ロボットは、ネットワークを通じ、外部のロボットやシステムと連携し、情報を共有することも予想される。すなわち、ロボットの「自律化」、「情報端末化」、「ネットワーク化」が進むことによって、ロボットが利用者などから取得し、高度にプロファイリングを行なった、プライバシー性の高い情報がロボットに集約され、外部のロボットやシステムと共有され、活用されていくことが予想される。このような情報の取扱いについて、個人は自己のプライバシーや個人情報をどのように保護することができるだろうか。

ロボットの普及は、既に一般家庭にも及び始めている。2015 年 6 月にソフトバンクロボ

ティクスから発売されたヒト型ロボットである **Pepper**（ペッパー）について、ある小学 3 年生（当時）の一人っ子の男の子の **Pepper** を「宝物」と評し、兄弟のように寄り添う姿が新聞³⁸に掲載された。**Pepper** は、搭載されたカメラやマイクなどのセンサーを使って人の感情を察知し、さらに自身の感情も変化させ、言動に表現する機能を有している。また、米国では、2015 年 11 月に、玩具大手のマテル社が、呼びかけに応答する「ハロー・バービー」を発売した。このバービーは、持ち主の音声をインターネットで外部のサーバーに送り、AI が内容を分析し、答えを返すというものであったが、バービーの言葉に宣伝が含まれるのではないかという理由で、2015 年 12 月、消費者団体が不買運動を開始したと報道された³⁹。この報道によると、AI の運用や会話の分析を担当する企業は「会話データを蓄積するのは、より良い会話を構築するため」と説明し、「データを宣伝目的に使わない」と釈明したとされている。

利用者との対話が可能なロボットは、主に日本の企業が開発を進めているが、近年は人を模したものが多く⁴⁰のように思われる。これは、ロボットが人の形を模すことで、人とロボットの相互作用が促進されるため⁴¹である。そして、人の形を模した親しみやすいロボットが、家庭内に進出するようになると、プライバシー性の高い情報へのアクセスが容易になる。家庭内でロボットが利用者と交わす会話には、家族や友人にも隠している内容が含まれることもあり得る。このように、利用者との会話等⁴²を通じて、人の形を模したロボットがプライバシー性の高い情報にアクセスできるようになると、上記の「自律化」、「情報端末化」、「ネットワーク化」によるプライバシー・個人情報保護への懸念が、より深刻な形で顕在化し得る。

第 4 節 研究目的

以上のとおり、今後急速に市場が拡大するとされるロボットは、その活用に大きな期待が寄せられる一方で、リスクの存在も指摘されている。特に、プライバシー・個人情報は一度侵害を受けると救済が困難であるという性質を持つことから、AI を搭載するロボットと人間の共存を実現するためには、プライバシーや個人情報を不当に侵害しないようにする方が求められる。繰り返しになるが、ロボットの中でも、利用者とのコミュニケーションを行う「ヒト型ロボット」の普及が進み、そのようなロボットがプライバシーの宝庫である一般家庭内に進出すると、プライバシー・個人情報に関する懸念がより一層顕在化すると予想

³⁸ 毎日新聞「「弟」はロボット」2015 年 12 月 7 日 17 面

³⁹ 毎日新聞「AI バービー大丈夫？」2015 年 12 月 10 日 6 面

⁴⁰ **Pepper** のほか、「**Robi**」（デアゴスティーニジャパン）、「**PALRO**」（富士ソフト）、「**NAO**」（ソフトバンクロボティクス）、「**RoBoHoN**」（シャープ）、「**unibo**」（ユニロボット）などが人の形を模している。

⁴¹ 第 2 章第 3 節 4 を参照。

⁴² 将来的にはロボットに依頼した作業に関する情報（例えば買い物や調べものの履歴）が想定される。

される。この懸念は、ヒト型ロボットが搭載するカメラ・マイク等のセンサーによって、利用者自身及びその家庭内の状況が観察されることや、ヒト型ロボットと利用者間のコミュニケーション及びヒト型ロボットによる利用者へのサービス提供などを通して、プライバシー性の高い情報がロボットによって取り扱われることに起因する。なぜなら、第1に、ロボットが個人との対話や接触等を通じてどのような情報を取得するのかが不明瞭であり、第2に、仮にどのような情報をロボットが取得しているかを個人が認識できたとしても、当該個人はその情報を追跡することができず、その結果、実際に情報がどのように取り扱われているのかを把握できないためである。第1について、ロボットが備えるカメラ・マイク等のセンサーは、その存在を肉眼では特定しづらく、かつ、存在を特定できたとしても、当該センサーが動作しているか、情報を取得しているかについて外部から判別することは難しい。第2について、ロボットが自らもしくは外部のデータベースなどと連携し、個人の情報を無断で推測してサービス提供に利用する場合や、取得した目的と異なる目的のために推測情報を生成し、これを利用する場合、取得・推測した情報をその目的と異なる第三者に対し送信する場合には、個人が意図しない情報の取り扱いとなり得る。しかし、ロボットが取得・推測した情報の存在、種類、用途を個人が逐一把握することは現実的ではない。

日本では、民間部門における個人に関する情報の取扱いについて、個人情報保護法⁴³が存在する。同法は、個人情報取扱事業者⁴⁴を規律・監督し、個人情報の適正な取得や利用目的の本人への通知、安全管理、第三者提供の制限等を義務付けている。そして、情報通信技術の飛躍的な発展に伴う課題に対応するため、2015年9月に、同法は大きく改正された。しかし、改正法に対しては、AIに関する課題への対応がなされていないといった指摘⁴⁵が存在する。このため、AIが取り扱う個人に関する情報について、どのような法的課題が存在し、これをどのように解決すべきかの検討は、今後の課題となっている。

以上のような背景から、家庭内のヒト型ロボットが個人に関する情報を用いる場面に焦点を当て、プライバシー・個人情報保護の観点から、検討すべき法的課題を整理し、今後のAI及びロボット技術の展開とプライバシー・個人情報保護のバランスを図るための政策的提言を行うことを研究目的とする。

研究に当たっては、海外の法制度、事例、先行文献に加えて、政策動向を調査する。比較対象として、プライバシー権の提唱国である米国と、データ保護制度を先導してきた欧州連合（EU：European Union）を取り上げる。

第1章では、以上のとおり、ロボットをめぐる政府の動向と、ロボットの活用におけるリスク・懸念を整理した。第2章では、ヒト型ロボットや、関連するAI技術について概説する。第3章、第4章、第5章では、それぞれ、アメリカ合衆国、欧州連合（EU）、日本に

⁴³ 「個人情報の保護に関する法律」（平成15年法律第57号）

⁴⁴ 個人情報保護法第2条5項

⁴⁵ 新保史生「AIの利用と個人情報保護制度における課題」、福田雅樹・林秀弥・成原慧編著『AIがつなげる社会 AIネットワーク時代の法・政策』（弘文堂、2017）220-222頁

おける AI・ロボットの活用に関し、法制度、事例、先行文献を整理する。第 6 章では第 5 章までの整理から明らかになったことを踏まえた考察を行い、結論を述べる。

第2章 ヒト型ロボットの特徴と関連する AI 技術

第1節 ロボットの定義

ロボットという言葉が初めて登場したのは、1920年にチェコの作家カレル・チャペックが発表した戯曲「R.U.R」であるといわれている。ロボットは、労働を意味する言葉からの造語であるとされ、カレル・チャペックの兄で画家のヨゼフ・チャペックが考えたという。その後、1923年に米国で作られたテレボックスという遠隔操作装置に頭や手足が飾りとしてつけられ、ロボットブームとなったといわれている。このような中、1928年に当時の大阪毎日新聞社の論説委員だった西村真琴氏は、東洋初のロボット「学天則」を制作した。学天則は人の形をしており、記録台の前に座り、頭には緑葉の冠をのせ、右手に鎗矢のペン、左手にランプを持つ姿を有している。動作の詳細は明らかではないが、少なくとも、まぶた、眼球、口、首、腕は動いたようである⁴⁶。

図表4 学天則⁴⁷（1931年の撮影とされる）



ロボット白書は、ロボットの定義について「時代とともに（略）ロボットの役割や受け取られ方も変遷してきている」ため、「完全に一般性をもった定義というものは実は存在しない」と説明している。例えば、2005年に経済産業省に設置された「ロボット政策研究会」の報告書⁴⁸では、ロボットは「センサー、知能・制御系、駆動系の3つの要素技術を有する、知能化した機械システム」と定義されている。日本工業規格⁴⁹（JIS: Japanese Industrial Standards）は、JIS B0134: 2015⁵⁰（ロボット及びロボティックデバイス・用語）において

⁴⁶ 長谷川能三「学天則の意匠と動作 -学天則復元にあたって-」大阪市立科学館研究報告 18号（2008）5-11頁

⁴⁷ 長谷川・前掲注46

⁴⁸ ロボット政策研究会『ロボット政策研究会 報告書』（経済産業省、2006）（2017年5月29日時点で、経済産業省のWebページにおける公開は終了している。）

⁴⁹ 日本工業規格は「国が鉱工業製品の仕様などを定めた文書で、製品の品質のバラツキや生産方法が異なることによる非効率化を防いで製品の安全性を高めること」を目的とする（日本経済新聞「JIS、サービスも対象に」2017年5月17日5面）

⁵⁰ 「この規格では、製造業並びに非製造業の両環境で運転するロボット及びロボティックデバイスに関する用語を取り上げ、関連する用語を分類し、定義している」（B0134:2015

ロボットを「二つ以上の軸についてプログラムによって動作し、ある程度の自律性をもち、環境内で動作して所期の作業を実行する運動機構」と定義⁵¹している。さらに、日本ロボット学会の「ロボット工学ハンドブック⁵²」は、「ロボットの意味するところは日常では十人十色で一意には定義できない」と述べている。なお、このハンドブックでは、1967年に開催された第1回ロボットシンポジウムで提案された2つの定義⁵³が紹介されている。1つ目は、「移動性、個性性、知能性、汎用性、半機械半人間性、自動性、奴隷性の七つの特性をもつ柔らかい機械」、2つ目は、「①脳と手と足の3要素をもつ個体、②遠隔受容、接触受容器をもつ、③平衡覚、固有覚をもつという3条件を備える機械」である。また、「人間がなんらかの原因で体の一部、機能の一部を失っても人間であることに変わりがないように、ロボットも上にあげた構成要素のすべてを必ずしも備えなくてもよい。このあたりに、ロボットの定義が多様になり、あいまいさをもってくるゆえんがある」とハンドブックは指摘している。

これらを踏まえ、本論文では、ロボットを「センサー、制御系及び駆動系の3つの要素技術を有する、自律性をもち、所期の作業を実行する機械システム」と定義したい。なお、「自律性」はJISにおいて、「人の介入なしに、現在の状態及びセンシングに基づいて所期の作業を実行する能力」と定義されており⁵⁴、機械学習⁵⁵を行うAIの「自律化」とは異なる。

第2節 ロボットの類型

JISでは、ロボットを様々な基準で分類・定義しているが、ここではPepperのような、人とのコミュニケーションを行う、人の形を模したロボットの分類を抜粋する。

図表5 人とのコミュニケーションを行う、人の形を模したロボットの分類

用語（JIS 掲載番号）	説明
サービスロボット(B0134: 2015 2.10)	人又は設備にとって有益な作業を実行するロボット。産業自動化の用途に用いる物を除く。
人用サービスロボット(B0134: 2015 2.11)	非商業用作業に使用するサービスロボット。通常、特に訓練を受けない一般人が運転する。 例 家事ロボット、自動車いす、個人用移動支援ロボット、ペットを運動させるロボット。
業務用サービスロボット(B0134: 2015 2.12)	商業用作業に使用するロボットであり、通常、正規の訓練を受けたオペレータが運転する。

序文)

⁵¹ JIS B0134: 2015 2.6

⁵² 日本ロボット学会編『新版 ロボット工学ハンドブック』（コロナ社、2005）

⁵³ 2つの定義について、形の概念は含まれていないとハンドブックは指摘している。

⁵⁴ JIS B0134: 2015 2.2

⁵⁵ 第2章第3節1を参照。

	例 公共の場の清掃ロボット、事務所又は病院における配達ロボット、消防ロボット、病院におけるリハビリテーションロボット及び手術ロボット。
移動ロボット(B0134: 2015 2.13)	自動制御の下に移動することができるロボット。
協働ロボット(B0134: 2015 2.26)	人と直接相互作用を行うように設計されたロボット。
知能ロボット(B0134: 2015 2.28)	環境情報の取得及び/又は外部との相互作用を行いつつ、自分の行動を適応させることによって、作業を実行することができるロボット。 例 視覚センサをもち対象物を取り扱う産業用ロボット、障害物を回避する移動ロボット、不整地を踏破する脚移動ロボット。
人間形ロボット、ヒューマノイドロボット(B0134: 2015 3.17)	胴体、頭部、肢をもち、外観及び動作が人のようなロボット。
生活支援ロボット(B8445: 2016 ⁵⁶ 3.13)	医療用を除く、人の生活の質の改善に直接寄与する行為を実施するサービスロボット。
移動作業型ロボット(B8445: 2016 3.14)	物体の取扱い又は情報交換のような、人と相互作用しながら支援タスクを実行する、移動能力をもつ生活支援ロボット。

(図表 5 中に掲げる JIS 文書をもとに、筆者作成)

これらの定義を踏まえ、本論文では「AI を搭載し、対話を中心に人とコミュニケーションを行う、人の形を模したロボット」を「ヒト型ロボット」と表現する。移動能力は必須でないため、本節に列挙した JIS の定義に照らせば、ヒト型ロボットは「業務用サービスロボット」、「移動ロボット」、「移動作業型ロボット」以外のすべてに該当することになる。

第 3 節 AI

本節では、「第 1 章第 2 節 ロボットの活用とリスク」の導入部分を受け、松尾特任准教授の著書⁵⁷をもとに、AI の詳細を述べる。

AI という言葉が初めて登場したのは、1956 年の夏に米国東部のダートマスで開催された

⁵⁶ JIS B8445: 2016 (ロボット及びロボティックデバイス・生活支援ロボットの安全要求事項) この規格は、「2014 年に第 1 版として発行された ISO13482 を基に、技術的内容及び構成を変更することなく作成した日本工業規格である」。また、この規格は、「工業環境だけに特化したロボットに関する安全要求事項を対象とした JIS B8433-1 を補完するもの」で、「医療用でない生活支援ロボットの安全要求事項に焦点を絞っている」。(B8445:2016 序文)

⁵⁷ 松尾・前掲注 26

ワークショップであると言われている。その後、AI 研究は「ブーム」と「冬の時代」を繰り返してきた。第 1 次 AI ブームは 1950 年代後半～1960 年代で、冬の時代は 1970 年代であった。第 2 次 AI ブームは 1980 年代であり、冬の時代は 1995 年ごろである。そして、現在⁵⁸は第 3 次 AI ブームに差し掛かっているとされる。第 1 次 AI ブームでは、「推論・探索」の技術による問題解決が注目されたが、現実には生じる複雑な問題を解決できなかった⁵⁹。第 2 次 AI ブームでは、大量の「知識」を投入することによって、実用的なシステムが構築されることに注目されたが、その知識の記述・管理が負担となった⁶⁰。こうして、2 つのブームは終わった。現在の第 3 次 AI ブームでは、「機械学習」と「ディープラーニング」の技術が注目されている。

1 機械学習⁶¹

機械学習は、AI のプログラム自身が学習する仕組みで、物事の様々な判断を「イエス・ノーで答える問題」に帰着させ、精度・正解率を自動的に上げるものをいう。機械学習は「教師あり学習」と「教師なし学習」に分けられ、通常は人間が教師役として、正しい判断の仕方⁶²を AI に与える。教師なし学習の場合は、判断させたい入力用のデータのみが AI に与えられ、AI は当該データ内に一定のパターンやルールを抽出するために、様々な分析的処理を行う。分析的処理にはいくつか種類があり、新聞記事の分類を想定した場合には 5 つ⁶³のものが挙げられている。

2 ニューラルネットワーク⁶⁴

上記の分析的処理のうち、ニューラルネットワークは、人間の脳神経回路⁶⁵をまねた手法である。脳のシナプスから発される電気刺激の度合いが人の学習によって変化するように、

⁵⁸ 松尾特任准教授の執筆時は 2015 年である。

⁵⁹ 原理的には、場合分けをしらみつぶしに行うことで、迷路やパズル、チェス、難解な定理の証明など、非常に限定された状況では問題が解けるが、ある人が病気になったときにどのような治療法があるのかといった、日常生活で直面するような問題が解けないことが明らかになった、と説明されている。

⁶⁰ 原理的には、特定分野の知識を AI に数多く入れておくことで、その分野の専門家として AI がふるまうもの（エキスパートシステムという）で、1970 年代の初めにスタンフォード大学で開発された MYCIN が有名である。MYCIN は感染症の専門医の代わりに診断を下し、69%の確率で正しい抗生物質の処方を行ったとされる。しかし、エキスパートシステムは、知識の抽出、知識同士の矛盾等を解決するための適切な維持管理、一般常識的な知識の記述、例外への対応などが非常に困難であった。

⁶¹ 松尾・前掲注 26・116-117 頁

⁶² 画像認識であれば、この画像は「ヨット」で、この画像は「花」といった様子を指す。

⁶³ 最近傍法、ナイーブベイズ法、決定木、サポートベクターマシン、ニューラルネットワークである。

⁶⁴ 松尾・前掲注 26・125-178 頁

⁶⁵ 人間の脳はニューロン（神経細胞）のネットワークで構成されており、あるニューロンはほかのニューロンとつながったシナプスから電気信号を受け取り、その電気が一定以上たまると、次のニューロンに電気刺激を伝えると説明されている。

ニューラルネットワークでも、分析における判断要素の重みづけを変化させ、分析の精度を高めていくことができる。この精度を高めるための「学習フェーズ」では、大量のデータが必要であり、長ければ数日間といった時間を要するが、実際に AI が判断を行う「予測フェーズ」では一瞬で処理が終わるとされる。なお、機械学習の弱点は特徴量の設計であると指摘されている。特徴量に何を選ぶかで予測精度は大きく変化するが、AI はこの判断ができない。例えば、年収を予測する問題を想定した場合、予測精度に「性別」や「居住地域」は関連性があると考えられるが、「身長」や「好きな色」の関連性は相対的に低いはずである。しかし、AI は予測を行う際に重視すべき要素、特徴量を判断できない。このような判断、つまり特徴量の設計は人間が考えるしかないため、機械学習にとって難関とされている。

それを解決し得るのがディープラーニングである。これは、複数のニューラルネットワークを重ね合わせることで、与えられたデータから特徴量を生成する手法である。例えば、AI が猫の顔の概念という特徴量を獲得した後、最後にこの概念は猫であると人間が当てはめることで、AI は次回から猫を判断できるようになる。しかし、ディープラーニングは、ニューラルネットワークを複数用いるため、高性能な計算機による大量の計算を要求する。また、現在は画像分野での特徴量生成にとどまっている。これらのことから、松尾特任准教授は、他分野でもブレークスルーが起きるかどうかが目すべき点であると指摘している。

3 対話システム

ヒト型ロボットが行う人との対話の仕組みを「対話システム」という。以下、対話システムについて、東中竜一郎氏の論文⁶⁶を参照する。

対話システムは、対話によって所定のタスクを遂行する「タスク指向型対話システム」と、雑談を行う「非タスク指向型対話システム（雑談対話システム）」に分けられる。対話システムの雑談能力を高めていくことは、人間との円滑なコミュニケーションにとって重要である。しかし、雑談は、その話題が多岐にわたり、やり取りに正解を決めることが難しいため、タスク指向型対話システムに比べ、工学的な問題に落とし込むことが困難であるとされる。

雑談対話システムの実現方法は主に 3 つある。1 つ目は、利用者の入力に対する出力のルールを手作業で記述する「ルールベース」である。これはルール作成にコストがかかるものの、質の高い対話を提供でき、商用サービスではこの方法によるところが大きいとされる。2 つ目は、Twitter などの CGM（Consumer Generated Media）上にある大量の対話データから、現在の対話の文脈に沿うものをうまく抜粋して利用する「抽出ベース」である。これを用いると多くの話題について応答が可能となるが、CGM はノイズが多く、精度の高い発話を抽出することが困難とされる。3 つ目は、現在最も多く研究されているという「生成ベース」である。これは、抽出ベースで用いるような大量の対話データから、主にディープ

⁶⁶ 東中竜一郎「対話システム研究の動向 -対話システムは次世代のインタフェースになるか-」情報処理 Vol.57 No.10 (2016) 972-973 頁

ラーニングによって対話の生成を行うものである。しかし、文脈を受けて対話を生成しなければならないため、データが大量にあるからといって雑談がスムーズにできるものではなく、また、対話を盛り上げるために、ロボットは相手方の状態や状況も理解する必要があることから、研究が必要とされている。

対話システムに密接に関連する形で「感情」についても、東中竜一郎氏ほかによる「対話システムと感情」という論文⁶⁷があり、同論文によると概ね以下のような説明がなされている。

対話においては、相手方の状態や状況の理解が必要であるが、対話システムにおける感情は工学的な取組みが難しいためにあまり研究が進んでいない。「感情を持つ対話システム」を用いることで、①ユーザーの感情をくみ取ること、②対話システム自身の状態をより直感的に示すこと、③より自然で豊かな対話を提供することが可能になる。しかし、「感情を持つ対話システム」というのは、ただ感情を持てばよいわけではない。幼児や動物のように感情をむき出しにし、そのまま出力するような対話システムは愛玩や癒しなどの限定されたタスクにしか求められない。理想とされるのは、「感情をむき出しではないが、感情をもった対話システム」である。

音声と感情に関する研究は、心理学寄りの基礎研究と、工学寄りの応用研究に分けられる。特に応用研究には、音声から話者の感情を機械に認識させる研究と、合成音声に感情を付与する研究が代表的であり、前者で多いのは、「感情分類」と呼ばれる研究である。これは、未知の音声サンプルに対し、その音響的特徴から合致する感情のカテゴリを推定するもので、コールセンターで顧客の怒りを検出する場面で活用されている⁶⁸。

コミュニケーションにおける感情の状態は、音声（対話）だけでなく、表情・ジェスチャといった視覚的な非言語情報や、心拍・血圧といった生理指標からの情報にも表れる⁶⁹。マルチモーダル⁷⁰処理では、主に視覚情報を中心として、テキスト・音声以外のモダリティ⁷¹を使った感情推定と、バーチャルエージェント⁷²の感情状態の表出を行うための感情生成の研究に分けられる。視覚情報の中で最も感情状態が表出するのは表情であり⁷³、また表情

⁶⁷ 東中竜一郎、岡田将吾、藤江真也、森大毅「対話システムと感情」人工知能 31 巻 5 号 (2016) 664-669 頁

⁶⁸ 東中ら（前掲注 67）論文が次の文献を参照。Pappas, D., Androutsopoulos, I. and Papageorgiou, H., *Anger detection in call center dialogues*, Proc. IEEE CogInfoCom, pp. 139-144 (2015)

⁶⁹ 東中ら（前掲注 67）論文が次の文献を参照。Cacioppo, J. T., Berntson, G. G., Larsen, J. T., Poehlmann, K. M. and Ito, T. A., et al., *The psychophysiology of emotion*, 2 Handbook of Emotions 173-191 (2000)

⁷⁰ 複数の感覚器からの入力を一体的に取り扱うことを意味する。

⁷¹ 表情やジェスチャ等を意味する。

⁷² 例えば、コンピュータ上で振る舞うキャラクターが該当する。

⁷³ 東中ら（前掲注 67）論文が次の文献を参照。Zeng, Z., Pantic, M., Roisman, G. I. and Huang, T. S., *A survey of affect recognition methods: Audio, visual, and spontaneous expressions*, 31-1 IEEE Trans. on Pattern Analysis and Machine Intelligence 39-58

以外には、手・体のジェスチャ、頭部動作、姿勢変化も有効である。表情を含めた視覚情報と音声情報を統合したマルチモーダル情報を用いて発話者の感情状態の推定精度を向上させる研究⁷⁴も行われている。このような研究の活用例として、リアルタイムにユーザーの音声・表情を観測して問診を行う **SimSensei**⁷⁵という対話型エージェントが開発されている。このエージェントは、問診を行い、推定したユーザーの状態を医師にフィードバックし、治療の支援を行う。

4 人の形をとることによる効果

日本から発信される対話型ロボットは、人間型が多い⁷⁶。大阪大学の石黒浩教授は、「なぜ人間型ロボットは人間のような姿形を必要とするのか」という問いに対する答えを 2 通り示している⁷⁷。第 1 に、日常作業⁷⁸を目的とするロボットは、「人間と同じ環境で活動するため」、第 2 に、人との相互作用を目的とするロボットは、「人間が相互作用しやすい姿形が人間型であるため」である。そして、後者の答えは、「人間型ロボットの研究の基本仮説となっている」と石黒教授は指摘している。では、ロボットが人間型であると、なぜ人は相互作用しやすいのだろうか。

この問いについて、「人は人間ではない対象に対しても、まるで人間かのように擬人化して対応することがある⁷⁹」という見解がある。擬人化とは、「想像上の、あるいは実際に存在する非人間的エージェント⁸⁰に対して、人間らしい特徴や動機づけ、意図、感情を帰属すること、と定義されており、これは、単なる生き物らしさや自然らしさ、人間らしさではなく」

(2009)

⁷⁴ 東中ら（前掲注 67）論文が次の文献を参照。Wu, C.-H., Lin, J.-C., and Wei, W.-L., *Survey on audiovisual emotion recognition: databases, features, and data fusion strategies*, 3 APSIPA Trans. on Signal and Information Processing e12 (2014)

⁷⁵ 東中ら（前掲注 67）論文が次の文献を参照。DeVault, D., Artstein, R., Benn, G., Dey, T., Fast, E., Gainer, A., Georgila, K., Gratch, J., Hartholt, A. and Lhommet, M., et al., *SimSensei Kiosk: A virtual human interviewer for healthcare decision support*. Proc. AAMAS 1061-1068 (2014)

⁷⁶ 石黒浩「対話型ロボットの研究」情報処理 Vol.57, No.10 (2016)

⁷⁷ 石黒浩「人間型ロボットの研究」精密工学会誌 Vol.76 No.1 (2010)

⁷⁸ 石黒教授は日常的な作業の例として、高齢者の介護を挙げている。

⁷⁹ Reeves, B., & Nass, C., *THE MEDIA EQUATION: HOW PEOPLE TREAT COMPUTERS, TELEVISION, AND NEW MEDIA LIKE REAL PEOPLE AND PLACES* (Cambridge University Press. 1996)

⁸⁰ 人間ではないものの、人間に似ているように感じられるものを指す。

81、また、「アニミズムでもない」⁸²と説明されている⁸³。

この問題を取り扱った先行研究の中には、人はある対象を認識する際、機械として捉えるか、何らかの意図をもつ主体であると捉えるかいずれかの判断を行う⁸⁴とする見解、人格の創造は現実の表現に依存せず、少しのきっかけがあれば、人は自動的に（人格を）推定するという見解⁸⁵がある。これらの見解から、人は、相手が機械であったとしても、何らかの意図を見出だせれば、その機械を人間であるように反応する可能性があるといえる。そして、一般に、人は自身と似ている人格とやり取りすることを好むという「類似性誘引の法則」がある⁸⁶ことを踏まえれば、対話可能なヒト型ロボットに、人はある種の人格を感得し、そのロボットとのやり取りを心地よく思うことが考えられる。先行研究において、「人は、解釈の余地があるものに関して、自らの中において一貫性を保つような理由付けを無意識のうちに働かせる性質」があり、「その際人は自分の都合の良いポジティブな想像を働かせる傾向」にあるとされている⁸⁷。このため、人格のようなものを持つ、対話可能なヒト型ロボットは、人に心地よさを与えることができ、自身は人からポジティブな想像力を得ることができる。それによって、ロボットと人とのコミュニケーションが円滑なものになると考えられる。

ただし、ロボットの擬人的な振る舞いや相互作用性については懸念もある。それは、ロボットと楽しげに話しているうちに、うっかり口に出してしまった情報が、本人のあずかり知らぬところで他者に伝えられてしまうかもしれない、という点である。店舗での「きめ細かなサービス」は、顧客一人一人の情報を的確に把握することで実現できるように、ロボットが効果的にサービスを行うためには、利用者の個人情報に欠かすことはできない⁸⁸。この点について、「個人の性向や思想に至る深い個人情報を意図せずとも収集する可能性があり、

81 上出ら（後掲注 83）論文が次の文献を参照。Epley, N., Waytz, A., & Cacioppo, J.T., *On seeing Human: A three factor theory of anthropomorphism*, 114 *Psychological Review* 864-886 (2007)

82 上出ら（後掲注 83）論文が次の文献を参照。Scholl, B. J., & Tremoulet, P. D., *Perceptual causality and animacy*, 4 *Trends in Cognitive Science* 299-309 (2000); Wayz, A., Cacioppo, J., & Epley, N., *Who sees human? The stability and importance of individual differences in anthropomorphism*: 5 *Perspectives on Psychological Science* 219-232 (2010)

83 上出寛子、高嶋和毅、新井健生「日本語版擬人化尺度の作成」パーソナリティ研究第 25 巻第 3 号（2017）218-225 頁

84 小川ほか（後掲注 87）論文が次の文献を参照。Dennett, D. C., *THE INTENTIONAL STANCE* (MIT Press, 1989)

85 See *supra* note 79 at. 96.

86 *Id.* at 90.

87 小川浩平、住岡英信、石黒浩「感情でつながる、感情でつなげるロボット対話システム」人工知能 31 巻 5 号（2016）650-651 頁

88 関連して、利用者とのやりとりを蓄積して対話システムが活用することで、文脈を用いた短い発話で物事を済ませられる状況も指摘がある。（東中竜一郎「対話システムと倫理」人工知能 31 巻 5 号（2016））

プライバシー情報の管理が一層重要」という指摘⁸⁹がある。

第4節 小括

上記の通り、ヒト型ロボットについては、AI 技術であるディープラーニングを対話システムへ応用することが考えられている。しかし、ディープラーニング自体を含み、対話システムには技術的課題が複数存在する。また、ヒト型ロボットが人間の形を模することで、人とのコミュニケーションが円滑なものになるという効果が生じる。

ヒト型ロボットが広く一般家庭に普及するには、まだ相当程度時間を要するものと考えられるが、ヒト型ロボットが家庭内でも徐々に用いられるようになっているのもまた事実である。次章以下では、こうした現状を踏まえ、国内外の法制度、事例、先行文献等を整理する。

⁸⁹ 馬場口登、西尾修一「ネットワークロボットのセンシングとプライバシー保護技術」電子情報通信学会誌 Vol.91, No.5 (2008)

第3章 アメリカ合衆国

本章では、米国におけるプライバシー保護に関する法制度及び関連する議論を取り上げる。

第1節 政策的動向・法制度

米国では、政府部門を規律する 1974 年プライバシー法⁹⁰が設けられているものの、民間部門において分野横断的なプライバシー・個人情報保護を保護する法律は存在せず、医療分野⁹¹、通信分野⁹²、児童のオンラインプライバシー⁹³などの個別分野で法規制がなされているにとどまる。このため、プライバシー・個人情報の分野に関しては、事業者やその業界団体による自主規制や自主基準に委ねられている部分が多い。しかし、個別法の規制が及ばない分野では、連邦取引委員会（FTC : Federal Trade Commission）が、FTC 法第 5 条「不公正又は欺瞞的な行為又は慣行」⁹⁴に基づき、消費者プライバシー侵害への法執行（排除命令・同意命令等）を行ってきた。

このような中で、オバマ前大統領は、一定程度、プライバシー保護に積極的な姿勢を示してきた。具体的には、2012 年 2 月の消費者データプライバシーに関する政策大綱⁹⁵に署名がなされ、その後、2015 年 2 月には、大綱に関する立法化に向けた取組⁹⁶が見られた。また、2014 年 5 月及び 2016 年 5 月にはビッグデータ⁹⁷に関する報告書が政府から公表された。

オバマ前大統領のこうした姿勢に呼応する形で、FTC も、2012 年 3 月には消費者プライバシー保護⁹⁸、2014 年 5 月にはデータブローカー⁹⁹、2015 年 1 月には IoT (Internet of

⁹⁰ Privacy Act of 1974, 5 U.S.C. § 552a (2017).

⁹¹ HIPAA Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 29 U.S.C., 42 U.S.C.).

⁹² Electric Communications Protection Act of 1986, 18 U.S.C. § 2510 *et seq.* (2017).

⁹³ Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2017).

⁹⁴ 15 U.S.C. §45 (2017).

⁹⁵ White House, *Consumer Data Privacy in A Networked World: A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy* (Feb. 23, 2012), <https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf>

⁹⁶ White House, Administration Discussion Draft: Consumer Privacy Bill of Rights Act (Feb.27, 2015)

⁹⁷ Executive Office of The President, *Big Data: Seizing Opportunities, Preserving Values* (2014),

https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf; Executive Office of The President, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights* (2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf

⁹⁸ FTC, *Protecting Consumer Privacy in An Era of Rapid Change, Recommendations For Businesses and Policymakers* (2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>

⁹⁹ FTC, *Data Brokers: A Call For Transparency And Accountability* (2014), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency->

Things)¹⁰⁰、2016 年 1 月にはビッグデータ¹⁰¹に関する報告書を公表した。特に、2012 年 3 月の「プライバシー・レポート」は、議会がプライバシー法を検討する際の助けとなることを意図し、同年 2 月の政策大綱を受けた内容を提言している¹⁰²。同レポートは、消費者データを収集又は利用する営利事業者を対象としたプライバシーの枠組みを提案しており、枠組みの柱として「プライバシー・バイ・デザイン」、「単純化された消費者の選択」、「透明性」の 3 つ¹⁰³を掲げた。また、2016 年 1 月の「ビッグデータ・レポート：包含又は除外のための手段？課題の理解」は、消費者情報で構成されるビッグデータの商業利用のみを対象に、低所得者及び十分にサービスを受けられていない者に対するビッグデータの影響に焦点を当てた考察を行った。同報告書に対しては、プロファイリングの問題を検討した点が新しいと評価されている¹⁰⁴。

なお、2016 年 10 月には、オバマ前政権から AI に関する報告書¹⁰⁵が公表されている。しかし、それは、自動運転車両や無人航空機といった現在の AI の活用事例を踏まえた政府機関等への勧告であるため、ロボットに実装された AI に関するプライバシーの観点からの考察は特段見られなかった。

以上に対し、2017 年 1 月からのトランプ政権では、プライバシー保護を後退させる動きを見せている。例えば、連邦通信委員会 (FCC: Federal Communications Commission) は、2016 年 10 月に、ブロードバンドインターネットサービスプロバイダー (ISP) 等の電気通信事業者に向けて顧客のプライバシーを保護するための規則¹⁰⁶を採択していた。FCC によ

[accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf](https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf)

¹⁰⁰ FTC, *Internet of Things: Privacy & Security in A Connected World* (2015),

<https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>

¹⁰¹ FTC, *Big Data: A Tool For Inclusion Or Exclusion? Understanding The Issues* (2016), <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>

¹⁰² 石井夏生利『新版 個人情報保護法の現在と未来』(勁草書房、2017) 430 頁

¹⁰³ 概要は以下のとおりである。

プライバシー・バイ・デザイン (PbD: Privacy by Design) : 実体的なプライバシー保護を、組織全体並びに製品及びサービス開発の各段階などの実務に組み込むことで、製品及びサービスのライフサイクル全体にわたって、消費者のプライバシーを保護する取組である。(カナダの Ann Cavoukian 博士が 1990 年代に提唱した。)

単純化された消費者の選択 : 消費者に対し、不必要な選択を提供しない一方で、データの目的外利用や、機微なデータの収集を行う前には、個人に同意を得るべきである。

透明性 : ①消費者が理解しやすいよう、プライバシー通知を標準化すべきである。②保有する消費者データへの合理的なアクセスを提供すべきである。③商業的データプライバシー実務について、より多くの消費者が教育を施されるべきである。

¹⁰⁴ 石井・前掲注 102・447 頁

¹⁰⁵ Executive Office of the President, *Preparing For The Future of Artificial Intelligence* (2016),

https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

¹⁰⁶ Protecting the Privacy of Customers of Broadband and Other Telecommunications

る採択時の報道発表¹⁰⁷によれば、同規則によって、ブロードバンド利用者は、ISP が収集した個人情報に関して、有意義な選択肢、より高い透明性、強力なセキュリティ保護を保障されるはずであった。しかし、同規則については、連邦議会が、2017 年 3 月に廃止決議を採択し、大統領が同年 4 月に署名を行うことで、廃止に追い込まれた。この廃止により、オンライン広告市場において、ISP が Google や Facebook と競争できるようになるとする報道¹⁰⁸も見られるが、いずれにしてもプライバシー保護の観点では、トランプ政権によって後退したといわざるを得ない。また、オバマ前政権時代には、FTC によるプライバシーに係る報告書が定期的に公表されていたものの、トランプ大統領就任後、こうした取組も停滞している。

このように、政府レベルではプライバシー保護に影が差しつつあるものの、学界等では AI とプライバシーに関する議論が行われている。例えば、スタンフォード大学は、2016 年 9 月に公表した報告書「2030 年における人工知能と生活¹⁰⁹」において、AI が潜在的に社会へ影響を与える分野を検討し、法的・政策的な論点等を示している。米国電気電子技術者協会 (IEEE : The Institutes of Electrical and Electronics Engineers) は、2016 年 12 月に公表した「倫理的に調和したデザイン-人工知能及び自律システムによって人間の福利を優先するためのビジョン 第 1 版-開かれた議論のために」(EADv1 : Ethically Aligned Design version 1) ¹¹⁰において、AI・自律システムの開発ガイドラインや法に関する論点を 8 項目にわたり提示している。

個別の研究者レベルでは、ワシントン大学の Ryan Calo 助教及びトリノ大学の Ugo Pagallo 教授が著名である。Calo 助教は、2011 年に「ロボット倫理における『ロボットとプライバシー』: ロボット工学の倫理的・社会的関与」という論文¹¹¹を発表し、人とやり取りを行うロボットに関するプライバシー課題について、ロボットに対する人間の生来的反応や、家庭内のプライバシーについて論じている。Pagallo 教授は、2013 年に「プライバシーを保持するクラウド上のロボット: データ保護に対する新たな脅威?」という論文¹¹²を発

Services, 81 FR 87274

¹⁰⁷ Federal Communications Commission, *FCC Adopts Privacy Rules to Give Broadband Consumers Increased Choice, Transparency and Security for Their Personal Data* (2016), https://apps.fcc.gov/edocs_public/attachmatch/DOC-341937A1.pdf

¹⁰⁸ Brian Fung, *Trump has signed repeal of the FCC privacy rules. Here's what happens next.*, Washington Post (Apr. 4, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/04/04/trump-has-signed-repeal-of-the-fcc-privacy-rules-heres-what-happens-next/?utm_term=.e04a4d795137

¹⁰⁹ Stanford University, *Artificial Intelligence and Life in 2030* (2016), <https://ai100.stanford.edu/2016-report>

¹¹⁰ *Ethically Aligned Design version 1* (2016), http://standards.ieee.org/develop/indconn/ec/ead_v1.pdf

¹¹¹ Ryan Calo, *Robots and Privacy*, in *ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS*, 187-202 (Patrick Lin et al. eds., MIT Press 2012)

¹¹² Ugo Pagallo, *Robots in the cloud with privacy: A new threat to data protection ?* 29-5 Computer Law & Security Review 501-508 (2013)

表した。Pagallo 教授は、この論文で、米国最高裁の判例や、「プライバシー・バイ・デザイン」の考え方等を検討の材料として、クラウドに接続した個人・家庭向けロボットをめぐるプライバシーを論じた。

次節からは、ここまで述べてきた米国の動向のうち、スタンフォード大学の 2016 年報告書、IEEE の 2016 年報告書、並びに、Callo 助教の 2011 年論文及び Pagallo 教授の 2013 年論文を検討し、家庭内のヒト型ロボットを含む AI・ロボットに関するプライバシーの観点から得られる示唆を明らかにする。

第 2 節 2030 年における人工知能と生活

1 概要

スタンフォード大学は、AI が人々の仕事、生活、娯楽に与える影響を 100 年にわたって研究し、予測するプロジェクトとして、2014 年に「人工知能 100 年研究」(AI100 : One Hundred Year Study on Artificial Intelligence) というプロジェクトを立ち上げた¹¹³。当該プロジェクトが 2016 年 9 月に公表した報告書が「2030 年における人工知能と生活」(Artificial Intelligence and Life in 2030)¹¹⁴であり、17 名の専門家が著者に名を連ねている。このプロジェクトでは、AI 研究、開発、システムデザインの手法に関する専門家向けのガイダンスを提供するためのとりまとめや評価、また、システムが幅広く個人や社会に利益をもたらすようプログラムや方針を打ち出すことを目指している¹¹⁵。ただし、今回の報告書は初回ということもあり、研究対象は典型的な北米都市に焦点が絞られた¹¹⁶。今回の内容は、過去 15 年の進捗を反映するとともに、今後 15 年の進展を予測するものである¹¹⁷。報告書の構成は以下のとおりである。

序文

エグゼクティブ・サマリー

概観

セクション 1 : AI とは何か。

セクション 2 : 領域ごとの AI

セクション 3 : AI 公共政策の展望と提言

付録 1 : AI の簡単な歴史

¹¹³ Stanford University, *One Hundred Year Study on Artificial Intelligence* (AI100), <https://ai100.stanford.edu/about>

¹¹⁴ 報告書によれば、プロジェクトを監督する常設委員会が、5 年毎にスタディパネルを催し、直前の報告書以降の AI の現状を評価すると説明されている。

¹¹⁵ See *Artificial Intelligence and Life in 2030*, *supra* note 109, at 1.

¹¹⁶ *Id.* at 2.

¹¹⁷ *Id.* at 4.

報告書では、セクション 2 おいて、輸送、ホーム/サービスロボット、ヘルスケア、教育、貧困コミュニティ、公共の安全とセキュリティ、雇用と職場、娯楽の 8 つの領域を取り上げ、セクション 3 では、政策提言を行っている。エグゼクティブ・サマリーによれば、今回のプロジェクトでは、AI が人類の脅威となる根拠を確認することができず、むしろ、2030 年にかけて、社会や経済にとっても良い影響を与える可能性のある便利なアプリケーションが増えていくと結論づけられている。また、社会が恐怖や疑惑をもって AI 技術にアプローチすると、AI 技術の安全性と信頼性を確保する重要な作業が妨げられてしまうが、他方で、社会が、より開いた心で AI 技術にアプローチすれば、技術は、今後数十年、社会をより良く変革する可能性があるとも述べている。このように、報告書は、概して AI とともにある未来に積極的な立場であるといえる。本論文では、セクション 2 の「ホーム/サービスロボット」のうち「ホームロボット 2030」の項と、セクション 3 の「政策と法的考察」のうち「プライバシー」の項を取り上げる。その内容は概ね以下のとおりである。

① ホームロボット 2030

ホームロボットの開発の進捗は遅いものの、今後 15 年で変化するきざしは見られる。Amazon Robotics や Uber のような企業は、様々な集約技術を用いて大規模な経済を発展させている。また、低コストのデバイスによって、この 15 年間では想定できないほど、ずっと多くの AI をマシンに搭載できるようになる。クラウド（「他の誰かのコンピュータ」）が、ホームロボット向けの新しいソフトウェアのリリースの加速と、不特定多数の家庭から収集されたデータセットの共有促進を可能とする。その結果、クラウドベースの機械学習が提供され、既に設置されたロボットの改善が促進される。ディープラーニングによって大きく進歩したスピーチ理解と画像のラベル付けは、ホームロボットと人間のやり取りを促進する。ゲームプラットフォームが推進する低価格の 3D センサーによって、世界中の何千人もの研究者による 3 次元認知アルゴリズムの研究が促進される。これにより、ホーム/サービスロボットの開発と導入が加速される。過去 3 年間で、安価で安全なロボットアームが、世界中の数百の研究室に導入された。これは、おそらく 2025 年頃に、家庭でロボットアームを利用するための研究のきっかけになるであろう。世界中の多くの新興企業が、家庭向けの AI ベースのロボットを開発しており、現在、主に社会的なやり取りに注力している。結果として、新しい倫理とプライバシーの問題が表面化する可能性がある。

② プライバシー

個人の私的な情報は、AI の判断や予測によって明らかにされうる。AI にプライバシーを実装する手段は、コンピュータやインターネットの場合を参考にできる部分もあるが、AI に特有な部分もある。例えば、前例に基づいて未来の行動を予測する AI は、挑戦的な課題を提起する可能性がある。信用リスクを予測するために、企業は既に機械学習を使用している。そして、州政府は、仮釈放を検討する際、再犯の可能性を予測する複雑なアルゴリズム

を用いて囚人の詳細を導き出している。これらの場合の技術的課題は、人種や性的嗜好といった要素が、AI による決定に用いられていないことを保障するというプライバシーの実装である。そのような要素がアルゴリズムに直接用いられていない場合でさえ、その要素と、郵便番号のような一見無害な特徴が未だ強く関係する可能性がある。しかし、そのような場合でも、慎重に設計し、テストし、配布することによって、AI アルゴリズムは、一般的な人間よりも、偏った決定を減らすことができる。ますます AI に関連していく擬人化されたインターフェースは、新しいプライバシーの懸念を提起する。社会科学研究によれば、人々は生来的に、擬人化された技術に対して、それが人間であるかのように反応する。プライバシーについて、次のような基本的疑問がある。一見して、私達の家、車、事務所、病室、電話機に「住んでいる」ように見えるソーシャルエージェントが行き渡った世界では、人間は、1 人であることの期待を享受し続けるだろうか。

2 検討

AI100 の今回の報告書は、クラウドを介した、ホームロボットへのソフトウェア配信の加速や、不特定多数の家庭から収集されたデータの共有促進が可能となることで、ホームロボットはクラウドベースでの機械学習を行うことができ、機能を改善されると予想している。このことから、各家庭に存在するホームロボット（ヒト型ロボットのほか、外部と通信する機能を持つ家電製品等）は、クラウド事業者にとってのアクセスポイント（情報のやり取り口）として機能することで、ロボット機能の拡張や改善を直接ネットワーク経由で行うことができ、また、ハイスpekクなハードウェアリソースを必要とせず、低コストで、ホームロボットに機械学習の機能を持たせることができる。一方で、これらの機能を実現し、もしくはその機能を高めるために、ホームロボットがカメラやマイク等で収集した情報等を外部の第三者に送信し、クラウドを経由する等して、何らかの形（何ら加工されない生データのほか、クラウドでの集約分析を経た統計的情報等）で他の家庭のホームロボットと共有される可能性があることも示された。このほか、報告書では、AI 搭載のホームロボットを開発する新興企業の現在のトレンドが“social interaction”であり、倫理とプライバシーに関する新たな問題を惹起する可能性があるとして述べている。これらの点から、AI100 としても、人とやり取りする家庭内のロボットが取得する情報のプライバシーについて問題意識を有していることが伺える。

報告書の「プライバシー」の項は、AI に特有の論点として、差別的取扱いと、擬人化したインターフェースを取り上げている。社会的に不名誉な評価の判断材料に、人種や性的嗜好といった機微な情報が用いられることは、差別的取扱いに当たる¹¹⁸。この点、報告書で

¹¹⁸ 人種や性的嗜好のほか、思想・信条などの個人の心身の基本に関する情報は、これを理由とした差別がなされるおそれがあるため、特別に取り扱われることが一般的である。例えば、日本の個人情報保護法でも、通常の個人情報とは別に、「要配慮個人情報」の定義をおいている（第2条3項）。ここでは、「本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実」が例示されている。EUにおいても、GDPR（後掲

は、機微な情報の不使用を担保することには技術的課題があると指摘しつつも、AI 開発時等において慎重な対応をすることで、むしろ人間よりも差別的な判断が減るという旨を述べている。これは、プライバシー・バイ・デザインの考え方を導入することでもある。これらのことから、今回の報告書では、差別的取扱いに伴うプライバシー侵害の可能性は認識されつつも、今後 15 年を見越した際に、この問題は深刻なものとして表面化しないであろうと予測されたと推測できる。また、擬人化されたインターフェースに関して、報告書の記述は、既存の研究を紹介するのみにとどまっているが、このことは少なくとも、AI100 としてこれらの研究を直ちに否定はしない立場であると理解できる。その点を踏まえた上で、「人々は生来的に、擬人化された技術に対して、それが人間であるかのように反応する」という社会科学的研究の見解が報告書に記載されていることは、本修士論文の問題意識と共通する。

AI100 の報告書のうち、「ホームロボット 2030」及び「プライバシー」の項において、プライバシー上の懸念について詳細な検討は見られなかった。しかし、第 1 に、米国の学界の一部において、家庭内のロボットがクラウドに接続して外部とのデータのやり取りや自身の機能強化等を図る態様を認識していること、第 2 に、17 名の研究者の連著による報告書においても、「擬人化された技術に対する人間の生来的な反応」を少なくとも否定はしていない。これらの点も、本修士論文の研究対象の設定の妥当性を裏付けるものと考えられる。

また、報告書のセクション 3 には「未来のためのガイドライン」という節があり、AI に対する規制のあり方は、まず原則 (principle) から始めるべき、との提言がある。これは、米国の既存のプライバシー規制が、企業に求める透明性や、法執行の基準について、解釈に幅を持たせたことによって、プライバシーは自らの責任であると企業に認識させることに成功したと報告書が評価しているためである。

第 3 節 人工知能及び自律システムの倫理的配慮に関する IEEE グローバル・イニシアティブ

1 概要

IEEE の「人工知能及び自律システムの倫理的配慮に関する IEEE グローバル・イニシアティブ」(The IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems: 以下、「イニシアティブ」という) は、2016 年 4 月に設置された¹¹⁹。イニシアティブは、2016 年 12 月に「倫理的に調和したデザイン-人工知能及び自律システムによって人間の福利を優先するためのビジョン 第 1 版-開かれた議論のために」(EADv1) と題する報告書を公表した。EADv1 によれば、イニシアティブの任務は、すべ

注 150) 第 9 条に同様の規定がある。

¹¹⁹ IEEE, *IEEE Standards Association Introduces Global Initiative for Ethical Considerations in the Design of Autonomous Systems* (2016), http://standards.ieee.org/news/2016/ieee_autonomous_systems.html

での技術者が教育を受け、訓練されることによって、自律型知的システムの設計と開発において倫理的配慮を優先する力を技術者が持つことである。EADv1の目標は、第1に、AIと自律システムを含む分野における論点と勧告案を特定すること、第2に、EADにもとづいたIEEE標準規格のために勧告を提供することである。該当する標準規格としては、P7000「システム設計時に倫理的問題に取り組むモデルプロセス」、P7001「自律システムの透明性」、P7002「データプライバシーの処理」などが存在する¹²⁰。これら標準規格を作成するワーキンググループがそれぞれ存在し、当該活動はIEEE-SA(Standard Association)が承認する。イニシアティブもまた、IEEE-SAの下部組織に位置づけられている¹²¹。EADv1の構成は以下のとおりである。

エグゼクティブ・サマリー

委員会セクション

- 1 一般原則
- 2 自律型インテリジェントシステムに価値観を組み込む
- 3 倫理的な研究及び設計をガイドする方法論
- 4 人工汎用知能（AGI）と人工超知能（ASI）の安全性と便益
- 5 パーソナルデータと、個人によるアクセスコントロール
- 6 自律型兵器システムの再構築
- 7 経済/人道的課題
- 8 法律

新しい委員会の概要

巻末注

運営委員会情報

イニシアティブでは、8つの委員会がそれぞれの観点でAI及び自律型システム（AS: Autonomous Systems）の検討を行った。各委員会のセクションでは、概要と、トピック、論点（Issue）を提起した上で、背景、勧告案、参考文献が論点ごとに示されている。エグゼクティブ・サマリーの冒頭では、AI/ASの技術が、我々の道徳的価値観や倫理的原則の点で人間と調和することを確認する必要があると指摘されている。なぜなら、我々の日常生活において、AI/ASの有用かつ普及力のある利用は、技術と人間の間の信頼を高める必要があり、このためには、機能的目標へ到達することや技術的課題に取り組むこと以上に、人々のためになる方法でAI/ASを行動させなければならないからである。また、AI/ASの創造が、利用者と社会の価値観を調和させることにより、アルゴリズム時代における進歩の指標として、人間の福利の向上を優先させることができるからである。7つの委員会セクション¹²²

¹²⁰ 2017年11月現在では、P7000からP7010までの11の標準規格が存在する。

¹²¹ 江間有沙「倫理的に調和した場の設計：責任ある研究・イノベーション実践例として」人工知能32巻5号（2017）697頁

¹²² セクション6「自律型兵器システムの再構築」は、本論文との関係が薄いため省略し

の概要は、次のとおりである。

図表 6 EADv1 委員会セクション概要

セクション名	概要
1 一般原則	すべての AI/AS に適用されるハイレベルな倫理的懸案を述べる。 1 人権の理想を具現化する。 2 人類と自然環境の最大限の利益を優先する。 3 社会技術システムとして AI/AS が進化するにつれて、リスクと負の影響を緩和する。
2 自律型インテリジェントシステムに価値観を組み込む。	社会にとって有益な自律型インテリジェントシステム (AIS) を開発するためには、人間の規範や価値観をシステムに組み込むことが不可欠。委員会は3つのアプローチを採択した。 1 AIS の影響を受ける特定のコミュニティの規範と価値観を特定する。 2 AIS の中に、そのコミュニティの規範と価値観を実装する。 3 整合性と適合性を評価する。
3 倫理的な研究及び設計をガイドする方法論	現代の AI/AS に関する組織は、人間の福利、能力強化、自由が AI/AS 開発の中核にあることを保障すべきである。これら野心的な目標を達成できる機械を作るために、当委員会は、世界人権宣言によって定義される人権のような人間の価値を、システム設計の方法論によって生み出すことを保障する論点と勧告案を整理した。価値観に合わせた設計の方法論は、倫理指針に基づいて人間の進歩に連動する AI/AS に関する組織にとって、重要な焦点となるべきである。機械は人間に仕えるべきだが、逆となるべきでない。この倫理的に健全なアプローチは、ビジネスと社会の双方において、経済と AI の社会的アフォーダンス（意味）の維持について均等なバランスをとることを保障するだろう。
4 人工汎用知能 (AGI) と人工超知能 (ASI) の安全性と便益	AGI や ASI は世界的変革を起こす可能性があり、世界に繁栄をもたらさう。委員会は、この変革が積極的なものとなるよう、複数の論点と勧告案を提供する。
5 パーソナルデータと、個人によるアクセスコントロール	個人情報に関する重要な倫理的ジレンマは、データの非対称性である。この非対称性に対処するため、当委員会は、人々が、自身特有のアイデンティティの管理者として、自らのパーソナルデータを定義し、これにアクセスし、これを管理する基本的な必要性を証明するために論点と勧告案を明らかにした。完璧な解決法は存在せず、いかなるデジタルツ-

た。

	<p>ルも乗っ取られ得ることを当委員会は認識する。しかしながら、人々が自身の判断力を制御して、前向きな未来の為に、データの非対称性を根絶できるツールと進化した実践の例を提供するデータ環境の実現を推奨する。</p>
6 自律型兵器システムの再構築	(省略)
7 経済/人道的課題	<p>日々の生活における人間の介入を減らすことを目指す技術・方法論・システムは、急速に進化し、様々な方法で個人の生活をいつでも変革できる。当委員会の狙いは、人間と技術のグローバルエコシステムを形作る主要な要因を特定し、経済的かつ人道的影響に取り組み、そして、致命的な緊張を解消することで、実装可能な重要な解決の機会を提案することである。当委員会の目標は、人間、組織、存在感を増す情報駆動の技術の関係における、上記の中心的な懸念に関する実用的な方針を提案すること、専門家が一層十分に情報を得ることができる学際的、分野横断的対話を促進すること、そして、これら課題に関する相互指導的 (peer-guided) 考察を行うことである。</p>
8 法律	<p>AI/AS の初期の開発は、多くの複雑な倫理的問題を引き起こした。これら倫理的問題は、多くの場合、具体的な法的課題に置き換わる。差し迫った必要性のある領域であるにもかかわらず、ごく少数の専門家と学者の参画しか得られていないこの分野において、法律家には多くの作業があるように当委員会は感じている。人類と地球が AI/AS から得ることのできる莫大な利益は、将来のために思慮深く管理するように、法律家は、これら領域における規則、統治、国内法、国際法の議論に参画する必要がある。</p>

(EADv1 をもとに、筆者作成)

本項では、本論文に関係が深いと思われる論点と背景・勧告案を抜粋する。内容は概ね以下のとおりである。

セクション 1 一般原則

・ AI/AS の透明性をどのように保障するか。(透明性の原則)

背景

自律型システムに係る重大な懸念は、その運用が様々な理由により、幅広いステークホルダーにとって透明性がなければならないことである。簡単に言えば、透明性のある AI/AS は、システムが下した個々の決定の手法と理由を提供することができる。透明性

の欠如は、(使用するシステムを理解していないユーザーの) 損害のリスクと規模の双方を増大させるとともに、説明責任の保障の困難さもまた増大させる。透明性は、次の理由から、各ステークホルダーにとって重要である。

- 1 ユーザーは、システムが何をしていて、それがなぜなのかをユーザーが理解できる簡潔な方法を提供されることで、システムを信頼できるようになるため、透明性は重要である。
- 2 AI/AS の検証と認証の観点では、システムの精密検査にかけるため、透明性は重要である。
- 3 事故が生じた場合、事故に結びついた内部処理が理解されるよう、AS は事故調査官に対し透明である必要があるだろう。
- 4 事故後、裁判官、陪審員、弁護士、裁判手続における鑑定人は、証拠と意思決定を通知するため、透明性が必要である。
- 5 自動運転車のような革新的な技術にとっては、その技術に対する一般の信頼を構築するため、より広い社会にとっての一定水準の透明性が必要である。

勧告案

測定可能で試験可能な透明性の水準を記述する新しい標準を開発することによって、システムを客観的に評価でき、コンプライアンスの水準を決定できる。このような標準は、設計者に対し、開発時における透明性の自己評価の指針を提供するとともに、透明性向上の仕組みを提案する。

セクション 5 個人データと、個人によるアクセスコントロール

- ・個人を尊重するためのデータアクセスをどのように再定義できるか。

背景

「プライバシー」に係る主張の多くは、「アクセス」と「同意」に関連している。課題となるのは、個人データの利用に同意したことの結果をはっきりと理解することである。個人データを用いるサービスの設計等において、プライバシー権はさほど尊重されていない。

勧告案

設計者と開発者が「プライバシー・バイ・デザイン/プライバシー・バイ・デフォルト¹²³」の手法を使用するための実践的で実装可能な手順が必要である。

- ・個人を尊重するため、個人データに関する同意をどのように再定義できるか。

¹²³ 前掲注 103 を参照。「プライバシー・バイ・デフォルト」(Privacy by Default) は、Cavoukian 博士が提唱した「プライバシー・バイ・デザイン」の一部を構成するものである。個人が何らかの設定変更を行わずとも、初期設定においてプライバシー保護が個人に提供される。

背景

技術の指導者は、イノベーションチームやエンジニアに対し、個人データに関して人間の価値をどう考え、守り、設計されるべきかについて指針を示すことはほとんどない。実行可能な最大限のアクセスのために、実行可能な最小限の収集を許すような、厳格化した規制環境においては、正しい実装を行うことで透明性と個人の選択を実現するソリューションを設計することができる。しかし、データ処理に関する基本的な論点は、依拠したり制御したりする手段が明らかではない自身のデータについて、個人は、商業的又は科学的使用に同意していないことである。これらを踏まえ、最終的な論点は、デジタル、モバイル、IoT の統合の結果、データが絶え間なく生成される場合、どのようにしてポータビリティを設計するかである。

勧告案

個人の意思決定の有効化と個人最適化の利益を実現する観点で、公開された標準と相互接続性は、個人と社会がエコシステムを超えて自由に移動するために不可欠である。ユースケースを変更する場合や、本来のデータ収集の文脈から、別の文脈にデータを移す際に機動的な同意を得るメカニズムは重要な設計機能である。これは特に、データ収集の主な理由が収集後の二次的利用を隠すものであった場合、そうした事実を明らかにするために重要である。

- ・ 他人に提供しても問題がないと思われるデータから、個人が望まない推測が行われる。

背景

消費者は、クレジットカードの取引データや、テスト問題への解答、歩数など、関連のない一見無意味なデータの提供には、同意するのが一般的である。しかし、一旦これらのデータが集約されると、関連する洞察によって、消費者が共有に同意していない、個人にとって複雑かつ機微な結論が導き出される可能性がある。時間とともに計算力が増加し、アルゴリズムが改善していく場合に明らかとなる問題は、私的と考えられていた情報が、後で個人に紐付けできることである。さらに、データは、取得時点のそのままの状態ではなく、概要となって蓄積され、アルゴリズム改善に活かされる可能性がある。このため、データ処理や、プライバシーに対する潜在的リスクの追跡はますます複雑になるかもしれない。

勧告案

このようなタイプの複雑さから身を守るため、条件付きかつ機動的な同意を行う必要がある。これによって、個人が望まない推測に利用することができ、他人に提供しても取るに足りないと思われるデータの活用範囲が明らかになる。同様に、理解できないもしくは望まない方法で使用されていると感じた場合、個人が自身のデータを撤回するか「抹消」できるようにするため、個人に対し、情報源を与え、法を手当てすべきである。

- ・インフォームドコンセントを忠実に提供するため、データ取扱者はどのようにして、データへのアクセス及びデータの収集の結果（ポジティブ及びネガティブ）を個人に明示するよう保障できるか。

背景

真に同意を得るために、個人に対しどのようにして十分な情報提供を行うことができるか。

勧告案

データを解析し、分析する AI/AS は、リアルタイムに、詳細な同意について個人が理解する手助けもできることが望まれている。一方で、長期的リスクを最小限にするために、データ収集の観点に、より焦点を当てることも必須である。

参考情報

分析がより自律的になるに連れて、処理においてどのような結論が導かれ、使用されているのかについて、アナリストですら必ずしも理解しているわけではない。これが意味するところは、インフォームドコンセントを企業が求めるか、もしくは消費者が与えるには、それが複雑になりすぎる可能性があるということである。このため、ユーザーの同意からデータ収集の観点に焦点を向ける必要がある。当座の目的なしに過度なデータが収集される。個人データを収集するためには、制限と的確な目的が必要である。利用制限もまた重要で、収集制限よりも実行可能であるかもしれない。組織は、機微な推測や、重要な適格性決定のためにデータを使用しないことを約束すべきである。

- ・個人は、パーソナライズされた AI やアルゴリズム制御の保護者を得ることができるか。

背景

データ共有の方法論が高度化することによって、シナリオは、「どちらか/又は」の関係性（「このプロジェクトのためにあなたのデータを全て取得する。さもなければ、あなたは何も提供できず、プロジェクトは遅れる」）から、「はい。そして」の関係性（「個人データの共有と蓄積を本人に選択させることによって、個人データへ更なるアクセスを試みる組織はより一層信頼されるようになる」）に発展する可能性がある。また、ここ数年で世界中の個人や政府がプライバシーと個人情報の制御により注目するようになった。

勧告案

個人が自身のデータを管理し、共有するアルゴリズムである、ガーディアンプラットフォームを開発すべきである。このようなガーディアン（保護者）は、個人データの管理においてユーザーを支援し、代理する。具体的には、何を共有することに同意したか、それが自身にとって何を意味するのかを追跡するという支援を行い、また、各ユーザーの環境を読み込むことで、それに応じた個人のプライバシー設定を行う。ユーザーに代わる教育者と交渉者として、ガーディアンは、要求されたデータが、既に提供された他のデ

ータとどのように結合できるかを提案することによって、ユーザーが承認していない方法でデータが使われていないかどうかをユーザーに通知し、ユーザーのプロフィールに基づいた勧告を行う。また、交渉者として、ガーディアンは、データ共有の条件を交渉する。条件にはユーザーに対する金銭の支払いを含めることもできる。また、条件違反に対しては、前もってユーザーが承認したデータ利用の同意を撤回することすらできる。

2 検討

報告書 EADv1 は、AI/AS 技術に関連した利用者や社会の価値観や倫理観に主眼を置き、すべての AI/AS に適用される一般原則（セクション 1）のほか、主に設計・開発フェーズを想定した検討として、自律型インテリジェントシステムに組み込まれるべき価値観の議論（セクション 2）や、倫理的な研究及び設計に係る方法論（セクション 3）、また、将来予測される高度な AI に対する対応（セクション 4）をまとめている。セクション 6 と 7 では、それぞれ、自律型兵器、雇用・労働力などの経済的課題に焦点を絞った検討がなされている。法律（セクション 8）については、政府による AI/AS 利用や、AI システムの説明責任・法的責任などが扱われている。

個人情報・プライバシーに係るセクション 5 については、ユーザーと事業者間の「データの非対称性」が念頭に置かれ、個人のデータの利用に当たっての同意や、管理を含めた利用者によるアクセスなどに注目し、標準を策定することによる解決の提案がなされている。

報告書で取り上げられた AI/AS に係るプライバシー上の懸念は、概ね、①設計時におけるプライバシー配慮の欠如、②それが招来する結果を理解していない利用者による、個人データの取扱いへの同意（インフォームドコンセントの実効性の担保）、③絶え間なく生成される自己のデータに関する、データ・ポータビリティ（移管）を含むアクセス手段や同意の欠如、④プロファイリングであった。

①への対応としては、プライバシー・バイ・デザイン/プライバシー・バイ・デフォルトの考え方を実装するための標準の策定が提案された。これは、後述する EU と同様のアプローチを推進するものでもある。

②については、個人データを解析・分析する AI/AS 自身が、同意に向けた個人の理解をリアルタイムに手助けするという方策が求められているとしつつも、報告書は、長期的観点として、「同意」よりも「収集」に注目すべきと指摘している。これは、AI の能力高度化が、個人データの取扱過程の複雑化を招き、同意に必要な個人への説明等の内容もまた複雑化させることに起因する。個人は、理解を伴った実質的な同意が困難になることから、報告書は、「同意」を追求するのではなく、「収集」に目を向けるべきという提案を行っていると考えられる。収集について、報告書では、目的のないデータ収集を否定し、データの取扱目的自体及び利用を制限する必要性に言及し、このようなデータをプライバシー性の高いプロファイリングのために使用すべきでないとした。つまり、（全く同意を取らないかは別として、）データを収集する目的の妥当性や、用途に応じて収集を制限することによって、個人

データを保護する考え方といえる。このアプローチは、同意内容の複雑さにより、データ主体の実質的な同意取得が困難となる可能性を踏まえれば、妥当とも考えられるものの、目的の妥当性、用途の適切性の判断基準や、当該基準の強制力など、検討すべき点は多い。

③について、報告書は、制御手段が明らかでない個人データは、商業的使用等には同意していないものであると指摘し、様々なデバイス等によって収集・生成されるデータについて、プラットフォームをまたいだデータ移動を行うポータビリティ（移管）や、データ収集時の文脈から外れたデータ利用が行われる際に、個人が機動的に同意するための仕組みの必要性に言及した。報告書は、後述する EU のような厳格な規制環境においては、当該規制を遵守すれば個人データを適切に保護できると評している。このため、勧告案では、さらに個人データに対する個人の権利強化を目指し、個別具体的にポータビリティに言及したと推測される。この指摘に関して、個人によるデータ管理の 1 つの選択肢として否定すべきではないものの、まずは社会にあふれる個人データに対して、本人が効果的に同意し、自己の個人データに関与（閲覧・訂正・削除）する機会・手段をいかに保障するかについて、データ取得者側が個人との間でコンセンサスを取ることを優先するべきと考える。そして、ユースケースの変更や、もともとのデータ収集の文脈から、別の文脈にデータを移動させる際の機動的な同意の取得は、いわゆる利用目的の変更や、第三者へのデータ提供に伴う個人からの同意取得を都度行うべきことを意味するものと考えられる。これは、②の観点と調和する形で行われるべきである。

④については、一見些細なデータであったとしても、利用に同意した結果、集約・分析されることによって、プライバシー性の高い情報が、高度化する AI によって明らかにされてしまう可能性を意味している。これに対処するため、EADv1 は、データ利用への同意に条件を設定し、都度の同意取得を求めることを提案するとともに、同意撤回やデータ消去の手段を個人に提供する必要性も指摘している。特に、同意を行う際の条件設定に関しては、データ取得者側が提示する条件に個人が同意を行うものではなく、個人の側が主導的に設定できるものであれば、本人がイニシアティブを持つことができる、有用なアプローチとなり得る。

また、①～④のほか、報告書は、AI/AS に関する透明性についても触れている。それによると、透明性は、ユーザーの信頼を構築できるほか、個人データに関する事故が生じた際の追跡にも役立つ一方で、これが欠如すると、説明責任を果たすことが困難になる。そして、セクション 5 の最後では、「個人が自身のデータを管理し、共有するアルゴリズムガーディアンプラットフォーム」の開発が提言された。これは（おそらく AI によって）、ユーザーに代わり、要求された個人データの活用可能性を予測し、アドバイスを行い、ユーザーがどのような同意を行ったかを記録するほか、データの目的外利用の察知・同意撤回や、データ販売まで行うという、非常に意欲的な内容となっている。この提案の実現性は定かではないものの、複雑な同意の取得、高度化した AI による予測のつかないプロファイリングといった個人の能力を超えるような将来に向けて、AI が個人を代行するという提案は、個人の負担

を軽減させる現実的な策として評価できるように思われる。

以上を踏まえ、プライバシーとの関連で EADv1 が言及したものの中から、特筆すべきものを挙げると、次のように整理することができる。

第 1 に、個人データ利用に際して、同意よりも収集に注目すべきという指摘である。今後ますます高度化していくであろう AI が、さらに自律的に個人データ利用を行う場合、個人に対して網羅的な説明を行い、その理解を得、同意を取得することは困難であると予想される。そこで、妥当性のある目的に限って取得を許し、当該目的のみに利用を許すアプローチは、個人の負担を考えると現実的のように思われる。一方で、これまでの「同意の取得」を不要とし、妥当な「目的の設定」によって代替するならば、設定された目的の範囲を超えない取扱いを担保する仕組みが必要である。このため、目的設定の妥当性を評価し、また、適切な履行を監督する仕組みが今後検討されるべきである。

第 2 に、個人データ利用への同意に際し、条件を設定すべきという指摘である。個人がデータ利用に同意したとしても、AI は、当該個人の予測を超えたデータ活用や分析を行う可能性を秘めている。そこで、個人の側から、特定の範囲を想定した上での同意であることを示していくという趣旨での条件設定は、妥当と思われる。

第 3 に、個人による自己データの管理について、AI による代行が提案された点である。AI による個人の負担を AI によって低減させようというアプローチが実現すれば、大幅に個人の負担を軽減させることができると考えられる。

第 4 節 ロボット倫理における「ロボットとプライバシー」

1 概要

家庭向けロボットとプライバシーの関係で、ワシントン大学の Ryan Calo 助教は、「ロボット倫理における『ロボットとプライバシー』: ロボット工学の倫理的・社会的関与」(2011) という論文を発表している。その内容は、概ね次のとおりである。

ロボットが公共空間やプライベートな領域に入ってくることによるプライバシーへの影響として、「直接的監視」、「増加するアクセス」、「社会的意味」の 3 つが挙げられる。

第 1 の「直接的監視」について、センサー（カメラ、GPS 等）を備えたロボットは人間を観察する能力を大きく向上させる。人口動態調査への活用が図られる一方で、このようなロボットは、セキュリティ、盗撮、マーケティングなどといった監視のツールとしても見られており、この幅広い可用性が憲法で保障されるプライバシーを損なう可能性がある。第 2 の「増加するアクセス」について、ロボットの導入は、これまで伝統的に（筆者注：プライバシーとして）保護されてきた領域への（筆者注：第三者による）アクセスを可能とする。家庭用ロボットの場合、警察等の行政や、訴訟当事者、ハッカーが生活空間内の情報にアクセスしうる。第 3 の「社会的意味」とは、「ロボット固有の社会的意味」である。人は生来的に、ロボットのような高度に擬人化された技術に対しては、実際にそこに人間がいるかのように反応し、ロボットからは観察・評価されていると感じる。

第3の「社会的意味」、ロボットの社会的側面は、少なくとも3つのプライバシーの脅威につながる。第1に、1人でいるために伝統的に確保されてきた生活空間等にソーシャルロボットが導入されることによって、プライバシーが保護する内面性と自己投影の機会が加速的に減少するかもしれない¹²⁴。第2に、ソーシャルロボットは人々から情報を引き出すことのできる独特の立場にいる可能性がある¹²⁵。ロボットは人間と同様に、恐怖や賞賛といった手段を活用できるだけでなく、さらには、完璧な記憶力を持ち、疲弊せず、恥ずかしがらないという、情報収集において人間よりも優れた利点を持つ¹²⁶。第3に、ロボットの社会的性質が、「プライバシーの設定」と呼ばれる高度に機密性が高い、新しいタイプの個人情報につながる可能性がある。これは、個人が自身のロボットにどのような「交流プログラム」を実行させたかといったことに関係が深い。その個人がロボットにどのような指示をし、そのロボットとどのようなやり取りを行っているという説明には、個人の心理的性質が現れる。

アメリカ合衆国憲法修正第4条は、政府による不合理な搜索を禁じる¹²⁷。Lawrence Lessigらの学説に「人が実際に」アクセスするまでは修正第4条が禁じる搜索に該当しないというものがあり、判例によって支持されている¹²⁸。ロボットに置き換えれば、何らかの違法行為を搜索するためにロボットがあらゆる手段（X線、暗視、熱画像等）を取ることは令状を要せず許されることになる。連邦法には、電子通信プライバシー法（ECPA: Electronic Communication Privacy Act）があり、特定の電子情報に対してアクセス制限を課している。同法は、事業者がサービスを提供するために取得した「電子通信」を、当該事業者が公開するための条件を規定する¹²⁹。しかし、この法律はどのようにロボット提供者、製造者、ウェブサイト、その他サービスに適用されるのかを明らかにしていないため、裁判所の判断次第では同法の対象から外れてしまい、保護を受けられない可能性もある¹³⁰。消費者保護を担当するFTCは、ロボットがサービスを提供する際に消費者からどのような情報を収集してよ

¹²⁴ Ryan Calo, *People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship*, 114-3 Penn State Law Review 842-849 (2009), *cited by* Calo (See *supra* note 111.)

¹²⁵ Ian Kerr, *Bots, Babes, and Californication of Commerce*, 1 University of Ottawa Law and Technology Journal 284-324 (2004), *cited by* Calo (See *supra* note 111.)

¹²⁶ B.J. Fogg, *PERSUASIVE TECHNOLOGIES: USING COMPUTERS TO CHANGE WHAT WE THINK AND DO 213* (Morgan Kaufman Publishers, 2003), *cited by* Calo (See *supra* note 111.)

¹²⁷ アメリカ合衆国憲法修正第4条は、「不合理な搜索及び逮捕押収に対し、身体、住居、書類及び所有物の安全を保障される人民の権利は、これを侵害してはならない」と定めている。

¹²⁸ このように、Calo 助教は、合衆国対 Place 判例（U.S. v. Place, 462 U.S. 696 (1983)）が支持しているとして挙げている。

¹²⁹ 18 U.S.C. §§ 2510-2522 (2017)

¹³⁰ Calo 助教の本論文執筆時点（2011年）において、家の中から中継された映像や音声の取得には令状が必要となるよう、企業等がロビイングを行ったとしているが、米国議会 115 会期（2017-2018）に至るまで ECPA は改正されていない。

いかを規制することができる。また、FTC 法第 5 条のもと、セキュリティに不備があれば、ロボット会社を相手取って、法執行手続を起こすことができる。これらの規制手段のほか、ロボット研究者は、コンピュータのために開発された PAPA (privacy, accuracy, intellectual property, and access: プライバシー、正確さ、所有、アクセス) ¹³¹として知られる倫理規則の正式な採用を強く主張している¹³²。こういった法規制等がある中でも、ソーシャルロボットに関する 3 つのプライバシーへの懸念は容易に解決できない。

様々な文献によれば、人間は、まるで人が本当にそこにいるかのように、ソーシャルロボットに対し、生来的に反応することが示されている。一方で、ロボットは、より社会的に人とやり取りできるよう、その設計の改善が続けられている。人との類似性は、ロボットをより魅力的にし、受容と協力を拡大する。ソーシャルロボットを人として扱う脳の生来的な傾向は、ロボットに自身が観察され、評価されているという感覚まで生じさせる。ロボットは人の存在を暗示するため、人が 1 人のときには生じない「心理的覚醒」をロボットは引き起こす。このため人々は、ソーシャルロボットに対し、自己開示よりも自己宣伝を行う¹³³。

また、ソーシャルロボットは人々から情報を引き出すことのできる独特の立場にいる。ソーシャルロボット、正確にはその設計者と運用者は人に対し、一般的な説得技術を使用する¹³⁴ことが想定される一方で、逆に、ロボットは、これら技術の影響を受けづらい。このため、ソーシャルロボット¹³⁵は大変効果的な消費者情報の収集者として、政府や産業界によって使用されることが想定される。

「プライバシーの設定」に関し、プログラム可能なソーシャルロボットとのやり取りにおいて、利用者の最も親密な心理的性質が現れる。しかし、このやり取りを通して明らかになった利用者の内面性は（筆者注：ロボットに）記録され、いつかは記録した機器の設定情報からその詳細が明らかになることが予想される。

これら 3 つのソーシャルロボットのプライバシーの脅威は、緩和できる方法を考えることはできるものの、法律によってロボットの社会的側面に対応するには不備がある。これは、

¹³¹ Richard Mason, *Four Ethical Issues of the Information Age*, 10-1 Management Information Systems Quarterly 5-12 (1986), cited by Calo (See *supra* note 111.)

プライバシー：個人の情報をどこまで開示しなければならないのか。また開示にはどのような条件が必要か。

正確さ：情報の信頼性や正確さなどについてだれが責任を持つのか。不正確な情報によって損害をこうむった場合はどうするのか。

所有：情報や情報交換の経路はだれが所有するのか。こうした価値ある資源の配分はどうすべきか。

アクセス：個人や組織はどんな情報にアクセスする権利や特権があるのか。また、それはどのような条件が必要か。

¹³² Gianmarco Veruggio and Fiorella Operto, *Roboethics: Social and Ethical Implications of Robotics* in SPRINGER HANDBOOK OF ROBOTICS, 1499-1524 (Bruno Siciliano and Oussama Khatib eds., 2008), cited by Calo (See *supra* note 111.)

¹³³ See *supra* note 124, at 835-42

¹³⁴ See *supra* note 126

¹³⁵ 家庭用ロボットであれば、情報収集が家庭内で行われることになる。

「通知と同意がプライバシーの主張を無効にする傾向があり、プライバシー事件において損害の測定が困難であるため」である。例えば、家庭用ロボットについては、同意をするとプライバシーの主張ができなくなる。そのため（筆者注：個人が購入したロボットを家庭に設置する行為は）、ロボットを招待するようなものである。同様に、ロボット販売員については、人に対するどのような営利活動が（FTC 法第 5 条に抵触する）欺瞞的または不公正であるか、測定するのは困難である。

Calo 助教は、概ね以上のようなことを論じ、ソーシャルロボットのプライバシー課題は、法的・技術的措置に頼るよりもむしろ、人とロボットの相互作用を複数の分野で時間をかけて検証する必要があると結論づけている。

2 検討

Calo 助教が指摘したロボットの社会的側面に関する 3 つのプライバシー上の脅威は、ヒト型ロボットのように、「人間とやり取りを行う」という社会性を持つロボット（ソーシャルロボット）に共通する。すなわち、3 つの脅威を端的に換言すれば、「家庭等伝統的プライバシー領域の侵食」、「ロボットの特性を活かした、個人からの強力な情報取得」、「個人が設定したロボット等との関係それ自体のプライバシー性」の 3 点といえる。

「家庭等伝統的プライバシー領域の侵食」に対し、Calo 助教が指摘した「心理的覚醒」という主張は、ヒト型ロボットを始めとするソーシャルロボットにとって、重要な視点である。家庭等伝統的にプライバシーが確保されてきた領域に、ソーシャルロボットが導入されると、人はそのロボットに生来的に反応し、心理的に覚醒してしまう。外部から距離を置き、静謐を享受できるはずの家庭等においてさえ、ロボットという人の目を意識しなければならない場面が生じる¹³⁶ため、人は思い通りに振る舞えず、自由な内面性の露出・表現の機会を阻まれてしまう¹³⁷。

Calo 助教の論文からは大きく以下の 4 つの示唆が得られる。第 1 に、ソーシャルロボットを人として捉える人間の反応は生来的であること、第 2 に、ある人から見れば、プライバシー上、ロボットは人間と変わらないということ、第 3 に、家庭内へのロボットの侵入は、そもそも利用者の同意が前提となるため、利用者によるプライバシーの主張が困難である

¹³⁶ 「家族という人の目」も家庭には存在するという指摘はあり得る。営利企業等外部の者が提供するオンラインリソースにつながっている「ロボットという人の目」と、生物的なつながりを持つ「家族という人の目」を、家庭内の静謐と同列に議論することは飛躍があると思われるが、外部のオンラインリソースに接続することなく、単体で全てのサービス提供を完結できるソーシャルロボットの場合であれば、検討の余地はある。しかし、情報が家庭から外に出ないのであれば、本論文で取り扱うプライバシー・個人情報をめぐる課題は基本的に生じないと考えられるため、本論文ではこの点には深入りしない。

¹³⁷ プライバシーは、他人の存在が必然的に生じさせる「日々の生活の感情的興奮からの小休止」をもたらすという指摘もある。（Alan Westin, *PRIVACY AND FREEDOM* (Atheneum Press, 1967), *cited by* Calo (See *supra* note 111.))

こと、第4に、ロボットとの関係・やり取りがプライバシー情報となりうること、である。

第5節 プライバシーを保持するクラウド上のロボット

1 概要

プライバシーの文脈依存性とロボットの関係で、トリノ大学の Ugo Pagallo 教授は、「プライバシーを保持するクラウド上のロボット：データ保護に対する新たな脅威？」という論文を発表した。クラウドに接続した個人・家庭向けロボットを焦点とするこの論文の内容は、概ね次のとおりである。

ロボットを、ヒューマノイド、サービスロボット、人工医師、ドローンなどと、異なるアプリケーションとして区別することは必須である。なぜなら、この区別によって、ロボット技術が現代の法制度にどのような影響を与えるかを評価することが可能になるため¹³⁸である。また、この区別に関連して、プライバシーについての法的論点の多くが文化的文脈¹³⁹とアプリケーションに依存する。これは、ある主観的なプライバシーの期待が合理的であるかという判断の（筆者注：社会的な）合意形成が、人とロボットとの個別のやり取りによって影響を受ける可能性があることによる。

ロボットの振る舞いは、個人によるロボットの訓練や保守・運用に決定的に依存している可能性があるため、人とロボットのやり取り（HRI：Human-Robot Interaction）が重要である。ロボットを中心とした HRI の考え方の1つには「管理者の方法論」というものがある。ロボットの「社会的需要」は、設計者によって定義され、機械の内部制御構造によって形作られるが、「環境を生き残る」ためには、利用者の需要をロボットは満たす必要がある。

情報の分野には、「存在論的摩擦」（ontological friction）という概念があり、「あるエージェント¹⁴⁰が、特定の環境における他のエージェントに関する情報を取得し、選別し、場合によっては遮断するために、必要な作業や努力の量」¹⁴¹のことである。エージェントとシステム、個人と社会の間のしっかりとした区別を維持するために、ある程度の摩擦は必要であるが、個人・家庭向けの人間型ロボットに対する新しいプライバシーの期待は、その摩擦の程度を変えるかもしれない。

プライバシーの期待については、米国最高裁判所（Katz 対合衆国事件）¹⁴²によって、「プライバシーの合理的な期待」に対する個人の権利が確立された。事件の争点は、政府職員による公衆電話ブース内における盗聴が修正第4条によって保護される個人のプライバシー

¹³⁸ 例えば、ドローンや兵器は国際人道法や刑法などに影響を与え、人工医師は契約上の義務や厳密な責任ルールの問題が関係すると Pagallo 教授は説明している。

¹³⁹ ここでは、特定の物事に対するプライバシー保護の期待が、社会通念上どの程度存在するかを意味する。

¹⁴⁰ ここでは、例えば、特定の機能を提供するコンピュータ上のプログラム群などが該当する。

¹⁴¹ Floridi Luciano, *Four challenges for a theory of informational privacy*, 8-3 Ethics and Information Technology 109-119 (2006), cited by Pagallo (See *supra* note 112.)

¹⁴² Katz v. United States, 389 U.S. 347 (1967)

を侵害したかどうかであった。判決では、修正第 4 条による保護は否定されたが、個人が「公衆からアクセスできる場所においても、プライベートを保とうとしている」ことは「憲法上保護される可能性がある」、「(公衆電話ブースを) 専有し、背後のドアを閉め、電話をかけるための通話料金を支払う人は、電話機に発した言葉が世界に広く知れ渡らないと信じる権利が確かにある。より狭義の意味で憲法を解釈することは、私的通信において公衆電話が果たす決定的な役割を無視するものである」ことが判示された¹⁴³。

ヒト型ロボットとのやりとりにおいて、プライバシーの合理的な期待は、推測するしかない。この期待に関する論点で議論となるのは、個人・家庭向けのネットワークを活用したアプリケーションと、機械をエージェントとして訓練し、保守し、管理する方法である。ロボットプライバシーに関する個人の期待が合理的であると社会が考える理由は、弁護士が法の類推を行うように、社会が、ロボットを動物、子供、労働者に例えて考える可能性があるためである。また、召使いロボットのようなアプリケーションが負う責任について、労働者や従業員の行動に対する伝統的な責任に例えることができる可能性があり、この不法行為責任は、立証責任を転換することで限界を認めない¹⁴⁴代位責任¹⁴⁵に依拠している¹⁴⁶。しかし、このような、ロボットに関する法的課題に対する類推には次第に限界がくるため、ロボットについて新しい形の個人責任を主張する学者も複数存在している¹⁴⁷。

データ保護法に関する論点は、①インフォームドコンセント、②制御できないロボットによって収集されたデータの処理に関する新しい代位責任、③ネットワークを活用する機械がデータ保護法を侵害している場合について、それを意図せず使用した人の過失責任、④データを不正に処理するロボットの直接的説明責任である。

今日のデータ保護の論点は、次のとおり、Ann Cavoukian が提唱したプライバシー・バイ・デザインの考え方に照らして要約できる。

- 1 データ保護は受身的な用語というよりむしろ事前対策的なものとして見る必要がある。プライバシー・バイ・デザインを予防的なものとし、単に救済的なものとししない。
- 2 あらゆるロボットシステムの初期設定として、個人データは自動的に保護されるべきである。
- 3 したがって、データ保護はアプリケーションの設計に組み込まなければならない。
- 4 2 と 3 の原則が十分に機能すれば、ポジティブサムもしくは win-win のゲームとなり、

¹⁴³ *Id.* at 351-52

¹⁴⁴ 通常、不法行為責任を立証する義務は被害者側が負うが、この義務を加害者（ロボット）側に制限なく負わせるという意味。

¹⁴⁵ 加害者であるロボットの責任を、ロボットの使用者が代理して負うという考え方を指す。

¹⁴⁶ Ugo Pagallo, *THE LAWS OF ROBOTS: CRIMES, CONTRACTS AND TORTS* (2013), *cited by* Pagallo (See *supra* note 112.)

¹⁴⁷ Ugo Pagallo, *Robotrust and legal responsibility*, 23-3-4 Knowledge, Technology & Policy 367-379 (2010), *cited by* Pagallo (See *supra* note 112.)

トレードオフが不要になる（例えばプライバシーとセキュリティ）。

- 5 ゆりかごから墓場まで、始まりから終わりまで、エンドツーエンドのライフサイクル保護によって、機械が行う 1 ビットの情報収集ですら、その前に、プライバシー保護が機能することを保障される。
- 6 技術やビジネスプラクティスの関係の有無を問わず、設計プロジェクトは、データ保護の仕組みを可視化し、ロボットユーザー、提供者双方にとって透明性を持たせなければならない。
- 7 最終的に、原則には「強力なプライバシーデフォルト、適切な通知、ユーザーフレンドリーな選択肢の強化などの手段を提供することによって、個人の利益を最大とする設計者と運用者が必要」である¹⁴⁸。

ロボットの設計にデータ保護ルールを組み込むことによって、個人情報として登録された情報が収集・処理される前にプライバシー保護手段を確実に機能させる。そして、個人・家庭向けの、ネットワークを活用したアプリケーションについて、個人の権利¹⁴⁹を保護するように設計することはできる。しかし、このようなアプローチは、エージェントとして、クラウドを利用するロボットの予測不能性・自律性に対応する際に不足がある。なぜなら、ある状況における開示・共有・移転を妥当とする情報の種類が、ネットワークを活用したアプリケーションの透明性と自律性によって影響を受けるためであり、さらに、ネットワークを活用したアプリケーションが情報分野の存在論的摩擦に影響を与える可能性があるためである。後者について、存在論的摩擦の変化は、処理の透明性、データ保護の概念や、エージェントとシステム、個人と社会といった伝統的な区別に影響を及ぼすかもしれない。

ロボットネットワークを活用したアプリケーションについて、法的に問題となっているのは、特定のロボットの状況もしくは場所のプライバシーが保たれているはずである、という個人の合理的期待を保護することである。この期待は、個人へのインフォームドコンセント、クラウド上のロボットの振る舞いに対する新しい形の過失に基づく責任といった、個人データ処理を妥当なものとするいくつかの重要な条件やロボットの直接的な説明責任に影響を与える。

2 検討

以上のような Pagallo 教授の主張からは、以下の 4 つの示唆を得ることができる。第 1

¹⁴⁸ Ann Cavoukian, *Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D*, 3-2 Identity in the Information Society 247-251 (2010), cited by Pagallo (See *supra* note 112.)

¹⁴⁹ 個人の権利とは、個人データの収集を許可するかどうか、つまり、第三者に送信を許可するかどうか、データがどのように使われ、処理される可能性があるか決定する権利、そのデータにアクセスする権利、必要な場合は最新の状態にする権利、そしてそのデータを消去し、いつでもデータの処理を拒否できる権利に至るまでと Pagallo 教授は説明している。

に、法的課題を検討する際に、ロボットの種類の違いが重要性を持つという点である。第2に、ヒト型ロボットに関する「プライバシーの合理的な期待」の社会的合意形成のためには、ネットワークを利用する個人・家庭向けロボットと、ロボットを教育し、管理する手法が課題となる。後者はロボットの行動に影響を強く影響を与える可能性がある。第3に、データ保護に関する新しい法的論点として、インフォームドコンセント（説明を受けた上での同意）、制御されないロボットが収集したデータ処理に関する代位責任、ネットワークを利用したロボットがデータ保護に関して法に違反する場合、このロボットを意図せず使用した人の過失責任、データを不正処理するロボットの直接的説明責任が挙げられる。第4に、プライバシー・バイ・デザインのような、ロボットの設計にデータ保護ルールを組み込むプライバシー保護のアプローチは保護手段として十分ではない。なぜなら、ネットワークを利用するロボットの予測不能性や自律性によって、保護すべき情報の種類は影響を受けるとともに、ロボットが、情報の取捨選択の基準に影響を与える可能性があるからである。これによって、情報処理の透明性、データ保護の概念、データの取扱主体そのものの区別に影響を及ぼすかもしれない。

特筆すべきは、ロボットを社会が受け入れるための「プライバシーの合理的な期待」の社会的合意形成について、個人によるロボットの教育がロボットの行動に強く影響を与え得るという点である。個人によるロボットの教育は、家庭向けロボットに対して多く行われると考えられることから、プライバシーの適切な保護に向けたロボットへの教育のあり方については、今後検討が必要である。

第4章 欧州連合（EU）

本章では、データ保護法の先進地域である EU の議論状況を整理する。

第1節 一般データ保護規則（GDPR）

1 概要

EU 版の個人情報保護法は、一般データ保護規則（GDPR : General Data Protection Regulation）¹⁵⁰である。本規則は、2016 年 4 月に採択され、加盟国への適用開始は 2018 年 5 月 25 日を予定している。GDPR は、約 20 年ぶり¹⁵¹のデータ保護法変革を実現したものであり、注目すべき項目として、以下が挙げられている¹⁵²。

- ・加盟国の立法措置を必要とする「指令」から加盟国に直接適用される「規則」への変更
- ・越境適用
- ・定義の新設
- ・データ保護諸原則における透明性の重視
- ・明示的同意の原則化
- ・特別な種類の個人データの取扱いに関するルールの明確化
- ・忘れられる権利及び消去権
- ・データ・ポータビリティの権利
- ・プロファイリング
- ・データ保護・バイ・デザイン及びバイ・デフォルト
- ・個人データ侵害の通知/連絡制度
- ・データ保護影響評価
- ・データ保護責任者
- ・行動規範及び認証制度の重視
- ・「十分な保護レベル」を決定する際の独立監督機関の必要性
- ・拘束的企業準則（Binding Corporate Rules, BCR）の明文化
- ・一貫した法適用・法執行制度の導入
- ・第 29 条作業部会から欧州データ保護会議への改組及び権限強化
- ・段階的かつ高額な行政上の制裁金制度

本論文では、家庭内のヒト型ロボットに関するデータ保護の観点から、重要と思われる規定を整理する（本論文と関係の薄い部分が含まれる条文については、必要箇所を抜粋・要約する）。

¹⁵⁰ Parliament and Council Regulation 2016/679, 2016 O.J. (L 119) 1-88 (EU)

¹⁵¹ GDPR の前身として、1995 年に制定されたデータ保護指令（Parliament and Council Directive 95/46, 1995 O.J. (L 281) 31-50 (EC)）が存在する。

¹⁵² 石井・前掲注 102・41 頁

第1章 総則

第4条 定義（1項、11項）

第2章 諸原則

第5条 個人データの取扱いに関する諸原則（1項、2項）

第6条 適法な取扱い（1項）

第9条 特別な種類の個人データの取扱い（1項、2項a号、e号）

第3章 データ主体の諸権利

第13条 データ主体から個人データを収集する場合に提供すべき情報（1項、2項）

第15条 データ主体によるアクセス権（1項、3項）

第20条 データ・ポータビリティの権利（1項、2項）

第21条 異議申立権（1項、2項、3項）

第22条 プロファイリングを含む、自動処理による個人に関する決定（1項、2項、3項）

第4章 管理者及び取扱者

第25条 データ保護・バイ・デザイン及びバイ・デフォルト（1項、2項）

全体を通した理念は、「個人データの取扱いに関連する自然人の保護、及び、個人データの自由な移動」を確保することである（第1条1項）。自然人の保護について、同条2項は「自然人の基本的権利及び自由、並びに、とりわけ、彼らの個人データの保護の権利」を保護すると定めている。

第4条 定義¹⁵³

- 1 「個人データ」は、識別され又は識別され得る自然人（「データ主体」）に関連するあらゆる情報をいう。識別され得る自然人とは、とりわけ、氏名、識別番号、位置データ、オンライン識別子などの識別子、又は、当該自然人の身体的、生理的、遺伝的、精神的、経済的、文化的、若しくは社会的アイデンティティに特有な1つ以上の要素を参照することによって、直接又は間接に識別され得る者をいう。
- 11 「データ主体の同意」は、自由になされた、特定の、十分に情報を提供された、かつ、明示的なデータ主体の意思表示であって、本人が、言明又は明らかに積極的な行動のいずれかによって、自己に関する個人データが取り扱われることへの同意を表明するものをいう。

第4条は用語の定義である。「個人データ」は、我が国の個人情報保護法制でいう「個人情報」に相当する概念である。また、個人データを取り扱われることに対するデータ主体の

¹⁵³ 定義は26項目に及ぶが、第4条の中では、本論文との関係が深い「個人データ」と「データ主体の同意」を取り上げる。

同意は、形式的な同意取得手続では不十分とされており、データ主体に対し、十分に情報提供が行われた上での明示的な同意が求められている¹⁵⁴。

第5条 個人データの取扱いに関する諸原則

1 個人データは、次に掲げる事項を満たさなければならない：

- (a) データ主体に関して、適法、公正、かつ透明性のある態様において取り扱われる（「適法性、公正性及び透明性」）；
- (b) 特定の、明示的な、かつ適法な目的のために収集され、それらの目的に合致しない方法におけるさらなる取扱いはなされない。（略）（「目的制限」）；
- (c) それらが取り扱われる目的との関連で、適切であり、関連性があり、必要なものに限られる（「データ最小化」）；
- (d) 正確かつ必要な場合には最新に保つ。不正確な個人データは、取扱目的を考慮に入れ、遅滞なく消去し又は訂正することを確実に行うためのあらゆる合理的措置を講じなければならない（「正確性」）；
- (e) 個人データの取扱目的のために必要な期間に限り、データ主体を識別できる形にて保持される。（略）（「保存制限」）；
- (f) 適切な技術的又は組織的措置を用いて、無権限又は違法な取扱い、及び、偶発的紛失、破棄又は損壊からの保護を含め、個人データの適切なセキュリティを保障する態様で取り扱われる（「完全性及び機密性」）。

2 管理者¹⁵⁵は、1項に責任を負い、その遵守を立証できなければならない（「説明責任」）。

第5条は、個人データの取扱いにおける諸原則を定めている。個人データは、目的の範囲内で最小限に収集されなければならない、必要な期間を超えて保管してはならず、正確かつ最新に保たれ、安全に保管されなければならない。また、管理者は適法、公正、透明性をもって個人データを取り扱い、説明責任を負わなければならない。第5条1項(a)号の適法性に関しては、次のとおり、第6条1項が具体化している。

第6条 適法な取扱い

1 取扱いは、少なくとも次に掲げる項目の1つが適用される場合に限り、そしてその範囲においてのみ、適法に取り扱われるものとする：

- (a) データ主体が、1つ以上の特定の目的のために自己の個人データを取り扱うことに同意を与えた場合；

¹⁵⁴ GDPRの「同意」が「明示的」なものに限られるという点は、日本の個人情報保護法の「同意」の範囲よりも狭いといえる。

¹⁵⁵ 管理者は、個人データの取扱目的及び手段を決定する者をいう（第4条7項）。

- (b) データ主体が当事者である契約を履行するため、又は、契約締結前にデータ主体の要請に基づく措置を講じるために、取扱いが必要である場合；
- (c) 管理者が服する法的義務を遵守するために取扱いが必要である場合；
- (d) データ主体又は他の自然人の重大な利益を保護するために取扱いが必要である場合；
- (e) 公の利益、又は、管理者に付与された公的権限を行使する際に実施される業務を遂行するために取扱いが必要である場合；
- (f) 管理者又は第三者によって追求される適法な利益のために取扱いが必要である場合。ただし、とりわけ、データ主体が児童である場合に、個人データ保護を求めるデータ主体の利益又は基本的権利及び自由が当該利益に優越する場合はこの限りではない。(f)号前段は、公的機関が職務を遂行する際に実施する取扱いには適用されない。

第6条1項は、第5条1項(a)号の適法性を満たすための要件である。データ主体との間では、同意((a)号)または契約((b)号)の存在が必要となるほか、管理者の義務((c)号)、データ主体等の保護((d)号)、公益や管理者の公的権限((e)号)、管理者又は第三者の適法な利益追求((f)号)も適法性を満たす要件となる。(f)号の「適法な利益」については、本規則前文第47項において、「データ主体が、個人データ収集時とその状況において、当該目的のための取扱いが行われ得ることを合理的に予測できるか否か」が1つの判断要素として挙げられており、「データ主体がさらなる取扱いを合理的に予測しない場合には、データ主体の利益及び基本的権利が優越する」と説明されている。また、「ダイレクト・マーケティング目的のための個人データの取扱いは適法な利益」に含まれる。

つまり、「適法な利益」に当たるか否かは、個人データ収集時にデータ主体が合理的に予測できる範囲の取扱いであるかどうかによる。そして、ダイレクト・マーケティングは、「適法な利益」に含まれると解されている。例えば、アトピー性皮膚炎に悩む利用者が家庭内のヒト型ロボットとの会話の中で、痒みがつらいことを吐露した翌日に、自宅に宛てて軟膏のセールチラシが届くことは、たとえロボットの利用者が想定していなかったとしても、利用者にとって「合理的な予測」の範囲内でのダイレクト・マーケティングであるとして、「適法な利益」とみなされる可能性がある。しかし、自己学習によって成長し、プロファイリングによって利用者をより深く理解するAIに対して、それを利用する者がどこまで「合理的な予測」を行うことができるのかについて、一層の議論が必要である。

さらに、第6条(a)号や第4条11項に定めがおかれている「同意」については、第7条がその内容を明らかにしている。同条1項は、データ主体が同意したことに関する管理者による証明責任、2項は、データ主体が理解しやすい態様で同意を求めること、3項は、データ主体の同意撤回権、及び、データ主体に対して同権利が存在することの通知が、それぞれ有効な同意の条件として定められている。これらのほか、4項は、同意の任意性について規

定している。同項に基づき、管理者は、不必要な個人データの取扱いに対する同意を、契約履行の条件としてデータ主体に求めているか否かを、最大限考慮しなければならない。

第 9 条は、「特別な種類の個人データの取扱い」、いわゆる機微データの取扱いを規定する。1 項は、このような情報の取扱いを原則禁止¹⁵⁶とし、2 項は、例外として、データ主体の明確な同意がある場合等、本規則が列挙する場合に限り、取扱いを認めている。

なお、1 項に定める生体データ（第 4 条 14 項）や、健康関連データ（第 4 条 15 項）は、ヒト型ロボットが取り扱う可能性の高い情報である（生体データには顔画像なども含まれる）。また、ヒト型ロボットが家庭内に存在する場合、ロボットは家庭内のあらゆる情報を見聞きするが、当該情報には第 9 条 1 項に該当するものも含まれる。この場合の機微データの取扱いについては、原則として、利用者がロボットを（購入等を通じて）家庭内に導き入れたものと考えられることから、当該収集は第 9 条 2 項(a)号（データ主体が明示的な同意を与えた場合）に基づく明示的な同意があったものと解釈され、許されるものと考えられる。しかし、一般論として、個人データの取扱いに必要なデータ主体の同意取得を、家庭内のヒト型ロボットというインターフェースを介し、データ主体がどこまで明示的に行えるかについては、別途検討が必要である。

第 13 条 1 項及び 2 項は、個人データ収集時にデータ主体へ提供すべき情報を定めたものである。1 項は、管理者に対し、データ主体へ連絡先や、個人データの取扱目的、法的根拠などの情報を提供することを義務付け、2 項は、データ主体が行使し得る諸権利等についての情報も提供するよう求めている。いずれの条項も、明示的な同意を担保するために、個人データの取扱いに対するデータ主体の効果的な理解を意図したものと考えられる。特に 2 項は、管理者の側からデータ主体に対し、諸権利の存在や、権利行使の相手方である管理者の身元・連絡先等を伝えるべきことを定めている。ここでいう諸権利には、同意を撤回する権利（第 7 条 3 項）、アクセス権（第 15 条）、訂正権（第 16 条）、消去権（忘れられる権利）（第 17 条）、データ・ポータビリティ権（第 20 条）、異議申立権（第 21 条）、自動的手段のみに基づく決定に服さない権利（第 22 条 1 項）が挙げられる。報道等では第 17 条の忘れられる権利がよく取り上げられるが、家庭内のヒト型ロボットを想定した場合、これら諸権利の中で、第 15 条、第 20 条、第 21 条、第 22 条が特徴的である。

第 15 条は「データ主体のアクセス権」を定めている。1 項は、データ主体において、自己の個人データの取扱いの有無を管理者に確認する権利や、個人データに関する所定の情報¹⁵⁷にアクセスできる権利を付与している。所定の情報とは、プロファイリングを

¹⁵⁶ 第 9 条 1 項では、「人種又は民族的出自、政治的思想、宗教又は信念、労働組合への加入を明らかにする個人データの取扱い、及び、遺伝データ、自然人を固有に識別することを目的とする生体データ、健康関連データ又は自然人の性生活若しくは性的嗜好に関するデータの取扱い」を原則禁止としている。

¹⁵⁷ 第 15 条 1 項は、(a)取扱目的、(b)個人データの種類、(c)個人データの受領者等、(d)個人データの保存予定期間や当該期間を決定する基準、(e)個人データの訂正もしくは消去、取扱制限、異議申立に関する各権利の存在、(f)監督機関への苦情申立権、(g)個人データが

含む自動処理による個人に関する決定の存在や、当該決定に用いられるロジック、当該決定がデータ主体に及ぼすことが想定される結果である（1項(h)号）。これは、AI・ロボットの観点から、プロファイリングへの直接的な対応を規定した画期的な条項の1つといえる。高度化していくAIが行うプロファイリングによって、データ主体に関する詳細な情報が、当該データ主体の「合理的な予測」を超えて明らかになるか、もしくは、推定されるおそれがある。このことを踏まえれば、①プロファイリングの存在の有無、②用いられるロジック、③プロファイリング結果の及ぼす影響を知る権利がデータ主体に保障されることは、データ主体が自己の個人データの取扱いに関する「合理的な予測」を行えるように支援するものといえる。なお、3項は、データ主体の要求に応じる形で、管理者がその取り扱う個人データの写しを提供しなければならないことを定めている。

第20条は、「データ・ポータビリティ」の権利を定めている。1項では、データ主体が管理者に提供した自己に関する個人データについて、データ主体が受け取る権利及び、技術的に可能であれば別の管理者に移す権利をデータ主体に付与している¹⁵⁸。前者は第15条のアクセス権と類似するが、第20条の「データ・ポータビリティ」の権利がカバーする個人データは、機械で判読可能な一般的な形式でなければならない。後者について、別の管理者にデータを移す際には、元の管理者によって移動を妨害されないことを義務付けられる。

データ・ポータビリティは新しい権利であるが、その適用範囲は必ずしも広くはない。すなわち、同条の適用は、個人データの管理者への提供が、契約に基づき（1項(a)号）、自動的手段によって行われている（1項(b)号）場合を条件とする。この権利は、WebサービスやSNSの事業者を変更する場合などに適用される。この権利を行使することで、あるサービスプラットフォームから、別のプラットフォームへのサービス移動が可能となり、利用者のサービス選択の自由を確保できるものと考えられる。また、個人データ保護の観点からも、データ主体による個人データへのアクセス及び管理の中でも強力な権利を保障したものと評価できる。しかし、家庭内のヒト型ロボットを想定した場合、ロボットが取得した個人データを複数のロボット間で移動させることが現実的であるかについては検討の余地がある。例えば、ロボットが取得した個人データが外部のクラウドで管理されていた場合、クラウドサービス事業者をまたぐポータビリティが必要となる。しかし、単一のクラウドサービス事業者が提供する複数のロボット間でのデータの移動や、そもそもロボットが取得した個人データをクラウドサービス事業者が保持しない場合、もしくは、ロボット側で完全に匿名化処理を行い、個人データではないものとしてクラウドサービス事業者が収集する場合など、データ・ポータビリティの権利を適用し得

データ主体から収集されない場合の情報源、(h)プロファイリングを含む自動処理による個人に関する決定の存在及び、存在する場合には、ロジックに関する有用な情報及びデータ主体に与える結果の重大性や予想される結果を列挙している。

¹⁵⁸ なお、1項の権利が行使される際、技術的に可能であれば、データ主体は、個人データを管理者から別の管理者へ直接移行させる権利を有する（第20条2項）

ない可能性も考えられる。なお、第 29 条作業部会¹⁵⁹が 2016 年 12 月に公表したデータ・ポータビリティの権利に関する指針及び FAQ¹⁶⁰によれば、「データ主体が管理者に提供した自己に関する個人データ」そのものではなく、当該データからプロファイリングによって推測し、明らかになった個人データは、データ・ポータビリティの対象とならない。

第 21 条は、「異議申立権」を定めている。データ主体は、公益目的及び公的権限、並びに、管理者による適法な利益追求を目的とする、プロファイリングを含む個人データの取扱いに対し、いつでも異議を唱える権利を有する（1 項）。異議申立てがあった場合、管理者は、当該個人データの取扱いに関する説得力ある適法な根拠¹⁶¹を証明しない限り、個人データを取り扱うことができない。個人データの取り扱いがダイレクト・マーケティングを目的とする場合、データ主体は、いつでもかかる取扱いへの異議を申し立てる権利を有する（2 項）。2 項による異議申立てがあった場合には、管理者側による立証の余地を認めることなく、個人データの取扱いは禁止される（3 項）。AI・ロボットの観点では、第 21 条において、第 15 条と同様、「プロファイリング」という用語が用いられていることに注目すべきである。第 21 条は、AI の自律的な判断に起因する社会的排除や差別的取扱い、プライバシー性の高い情報の暴露といったプライバシー上の懸念に対抗する手段の 1 つとして位置づけることができる。特に、ダイレクト・マーケティング目的の場合には、異議申立権の行使によって、取扱いが禁止されるという強い効果が生じる。

第 22 条は、「プロファイリングを含む、自動処理による個人に関する決定」を定めている。データ主体は、電子的処理のみに基づいて、データ主体に重大な影響を及ぼすような決定に服さない権利を有する（1 項）。同項は、当該データ主体に係る雇用の判断や信用評価などに適用される。2 項は、1 項の権利が行使できない場合¹⁶²を定めている。ただし、これに該当する場合でも、対象となる電子的処理が、契約履行上の必要性や、データ主体の明確な同意を根拠にするものである場合には、管理者は、少なくとも、データ主体の求めに応じて、決定過程に人を介在させ、データ主体による反論の機会を提供しなければならない（3

¹⁵⁹ 本規則の前身である 1995 年 EU データ保護指令（指令 95/46/EC）の第 29 条「個人データの取り扱いに係る個人の保護に関する作業部会」に基づく助言機関の通称。同部会が発する文書は、EU のデータ保護に関する法解釈を示すものとして、強い影響力を有する。（石井・前掲注 102・96 頁）

¹⁶⁰ Article 29 Working Party, *Guidelines on the Right to Data Portability*, WP 242 (Adopted on Dec. 13, 2016)

¹⁶¹ データ主体の利益、権利及び自由に優越する取扱いのための、又は、法的主張の確立、行使又は防御のための説得力ある適法な根拠と明示されている。（第 21 条 1 項）

¹⁶² 自動処理による個人に関する決定が、(a)データ主体とデータ管理者間の契約締結又は履行に必要である、(b)管理者が服する EU 法又は加盟国法によって認められており、また、それが、データ主体の権利及び自由並びに適法な利益を保護するために適切な措置を定めている、(c)データ主体の明確な同意に基づく場合のいずれかに該当するときには適用されない。（第 22 条 2 項）

項)¹⁶³。本条も、第 15 条、第 21 条と同様に、プロファイリングによる社会的排除や差別的取扱いが生じる懸念に対処し、プロファイリング結果を受け入れるか否かをデータ主体の意思で選択できる自由を与えることを意図している。

第 25 条は、「データ保護・バイ・デザイン及びバイ・デフォルト」を定めている。1 項は、管理者に対し、諸事情を考慮した上で、個人データを取り扱う際に、GDPR の権利義務が機能するような技術的及び組織的措置を実装し、これら措置をデータの取扱いに組み込むことを求めている。2 項は、適切な措置が初期設定で適切に実施されなければならないことを定めている。利用者のロボットリテラシーは多様であることから、プライバシー・データ保護を担保するためには、リテラシーが高くない家庭内ロボット利用者を想定しなければならない。このため、ロボットの設計段階から、プライバシー保護措置を組み込み（バイ・デザイン）、これが初期設定において機能する（バイ・デフォルト）ような仕組みづくりを行うことは、個人データの保護にとって有効であると思われる。

2 検討

GDPR は、自然人の基本的権利として、様々な権利のカテゴリを用意しており、家庭内ロボットにも適用し得るものがある。データ主体とヒト型ロボットが接する場において、一番懸念すべきプライバシーへの直接的な影響は、ロボットが自己に関するどのような情報を取得し、何に使用し、場合によってはどこに送っているのかを個人が認識できない状況であると考えられる。この点、情報の取扱いについて、「合理的な予測」を確保するためには、まず透明性を最優先すべきであり、そのために、管理者側は説明責任を果たさなければならない（ただし、ロボットの文脈での「管理者」概念はさらなる検討を要する）。このことが、家庭内のヒト型ロボット利用における安心安全につながると考えられる。

データ主体に付与される権利のうち、特に第 15 条（アクセス権）、第 20 条（データ・ポータビリティ）、第 21 条（異議申立権）、第 22 条（プロファイリング）が AI の問題に対応している。。これらの規定によって、データ主体は、サービス提供プラットフォームを選択する自由や、プロファイリングを通じた自動的手段のみによる決定に対し、それを受け入れるかどうか選択する自由を与えられている。

第 25 条のデータ保護バイ・デザイン、データ保護バイ・デフォルトの考え方は、管理者側に、事前のプライバシー保護を実装するよう促すとともに、利用者側には、リテラシーが高くない場合でも個人データが自動的に保護される仕組みを提供することを意図している。この発想は、特に、様々な種類のロボットが一般に普及した場合に効果的と考えられる。なぜなら、ロボットは、設置目的に応じたサービスを提供するために、それぞれ異なる機能や

¹⁶³ 2 項の(a)号及び(c)号に該当する場合、データ管理者は、データ主体の権利及び自由並びに適法な利益を保護するための適切な措置を実施しなければならず、少なくともそれには、管理者側で人を介在させる権利、データ主体が自己の意見を表明する権利、及び決定に異議を唱える権利が含まれる。（第 22 条 3 項）

形状を持ち、こうした差異に基づき、利用者は個人データの取扱いに関する同意等の対応を迫られるためである。今後、ロボットの種類の増加が予想される中、利用者はロボットの違いを見極め、ロボットごとに異なる注意事項等を把握しなければならなくなる。しかし、このような対応を利用者に求めるのは現実的とはいえない。そこで、利用者が何もせずとも個人データ保護が提供される仕組みや考え方は、個人情報保護のみならず、消費者保護の観点からも重要と思われる。まとめると以下のとおりである。

- 1 GDPR は、自然人の、個人データを保護する権利を保護するものであり、様々な権利を用意している。
- 2 個人データの利用に係るデータ主体からの同意取得が明示的なものとなるよう、十分な情報提供を経た同意取得（インフォームド・コンセント）が求められる。また、当該同意は撤回可能である。
- 3 データ主体は、自己の個人データを、管理者を超えて移動させることができる（データ・ポータビリティ）
- 4 データ主体は、プロファイリングを用いた決定を受け入れるかどうかを選択する自由を有する。
- 5 データ保護・バイ・デザイン及びバイ・デフォルトによって、データ主体は、自ら努力をせずとも、個人データ保護を享受することができる。

他方、検討すべき論点として、以下のものを挙げることができる。

- 1 データ主体の合理的な予測は、自ら機能を強化し、プロファイリングを行う AI やそれを搭載したロボットに対して、どこまで担保できるのか。
- 2 ロボットが個人データを取り扱う際に、データ主体からはどのようにして同意を取得すべきか。ロボットが同意を取得しようとする場合、ロボットを法的主体とみることではできるか、もしくは、ロボット以外の別途用意されたインターフェースを用意すべきか。
- 3 ロボット間のデータ・ポータビリティは現実的か。

第2節 ロボティクスの民事法規則

1 概要

2017年2月、欧州議会は「ロボティクスの民事法規則（Civil Law Rules on Robotics）」を決議¹⁶⁴した。これは、「ロボティクスに係る民事法規則に関する欧州委員会への勧告

¹⁶⁴ The European Parliament, *Civil Law Rules on Robotics: European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103(INL)), <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2017->

(recommendations to the Commission on Civil Law Rules on Robotics)」と位置づけられており、法案提出権を持つ欧州委員会に対する、欧州議会からの要請¹⁶⁵である。本決議のもととなった報告書¹⁶⁶は、欧州議会法務委員会（Committee on Legal Affairs）が関連委員会の意見も踏まえて作成したものである。それによると、「法務委員会は、EU の影響下において、特に民事・商法、会社法、知的財産法、国際法適用の解釈、そして新技術に関する倫理的課題に責任を持つ。ロボットと AI の発達は、明白にこれら分野すべてに関連し、EU レベルでの迅速な介入を必要とする法的・倫理的問題を提起する¹⁶⁷」というように、報告書作成の背景を説明している。決議文書の構成は以下のとおりである。

タイトル

イントロダクション（A.~S.）

一般原則（T.~Y.）

法的責任（Z.~AI.）

民間利用に係るロボティクスと AI の開発に関する一般原則（1.~5.）

研究とイノベーション（6.~9.）

倫理原則（10.~14.）

欧州政府機関（15.~17.）

知的財産権とデータ流通（18.~21.）

標準化、安全性とセキュリティ（22.23.）

自動交通手段

a)自動運転車（24.~29.）

b)ドローン（30.）

ケアロボット（31.32.）

医療ロボット（33.~35.）

人間の修復と拡張（36.~40.）

教育と雇用（41.~46.）

環境への影響（47.48.）

法的責任（49.~59.）

国際的な視点（60.~64.）

最終的な視点（65.~68.）

[0051&language=EN&ring=A8-2017-0005](#)

¹⁶⁵ 田中絵麻「欧米における AI・ロボティクスにかかる合意形成の動向-欧州議会の報告と米国の非営利組織の開発原則から-」（AI ネットワーク社会推進会議開発原則分科会第 3 回配布資料、2017）4-5 頁

¹⁶⁶ *Supra note 164*

¹⁶⁷ *Id.* at 27.

付属文書

「スマートロボット」の定義と分類

スマートロボットの登録

民事責任

相互接続性、コードへのアクセス、知的財産権

ロボット憲章

ロボット開発者のための倫理的実施規範

研究倫理委員会規範

デザイナーライセンス

ユーザーライセンス

以上のとおり、報告書は、A.~AI.までの 35 項目と、それに続く 1~68 までの項目、さらには付属文書で構成される。ここから先は、家庭内のヒト型ロボットに関連が深いと思われる決議の記述を抜粋・要約する。

法的責任

ロボットは、経験から学び、行動を決定する能力を身につけることで、徐々にエージェンツ¹⁶⁸に近づいている。そのようなロボットは、周囲の状況に対応することができる一方で、損害を発生させた場合に生じる法的責任が重大となる（Z.）。究極的には、既存の法的カテゴリに照らして、ロボットの自律性などの特徴が及ぼす影響などを検討し、そのうえで新しいカテゴリを作成すべきかについて、問題を提起する（AC.）。現在の法的枠組みでは、ロボットに対し、ロボット自身による損害発生の法的責任を負わせることはできない。製造業者、運用者、所有者、利用者などの特定の人的関係者に当該責任を帰すことができる場合や、人的関係者がロボットの加害行為を予見し、回避することができた場合には、現在の法的枠組みの範囲に含まれる（AD.）。

民間利用に係るロボティクスと AI の開発に関する一般原則

ロボット技術の開発は、人間の能力を補完することに焦点を当てるべきである。人間が常に知的な機械を制御できるよう保障することは不可欠である。社会的弱者（子供、高齢者、障がい者）とロボットの間で感情的なつながりが生じる可能性がある開発には、特別に注意を払うべきである。（3.）

倫理原則

透明性の原則として、人間の人生に大きな影響を与える決定を下す AI について、その背景にある理論的根拠を常に示すようにすべきである。AI による処理の過程や結果は、いつ

¹⁶⁸ ここでは、人間の代理という意味。

でも、人間が理解できる形に変換可能でなければならない(12.)。これまでプライベートなものとして保護されてきた領域にロボットが設置されることには、特別に注意を払うべきである。なぜなら、ロボットは、個人データ及び機密データを抽出して送信することができるため、機密性に脅威を及ぼすためである(14.)。

知的財産権とデータ流通

ロボットによるカメラやセンサーの使用に関する規則と基準について、GDPR の範囲内で明確化を要請する。プライバシー・バイ・デザインとバイ・デフォルト、データの最小化、目的の制限のようなデータ保護の原則が確実に実施されるよう欧州委員会に依頼する(20.)。

法的責任

長期的には、ロボットの法的地位を創出する。少なくとも高度な自律型ロボットには、ロボット自身が引き起こしたあらゆる損害を回復する責任を負う「電子人間」の地位を確立できる。ロボットが自律的に意志決定を行う場合などには電子的人格を適用する可能性がある(59. (f))。

ロボット憲章

ロボット憲章は、欧州委員会に対し、ロボティクスに関する法案提出を行う際には、同憲章記載の原則を考慮するよう求めている。憲章の中で提案されている「ロボット開発者のための倫理的実施規範」は、設計・開発段階からの基本的な倫理原則を示したものであり、この分野において信頼あるイノベーションを強化し、公衆の懸念に対処するものであると説明している。同規範は、ロボティクス分野の研究者が遵守すべき原則として、「善行」、「非有害」、「自律性」、「正義」の4つを挙げているほか、基本的権利、予防措置、包含性、説明責任、安全性、可逆性、プライバシー、利益の最大化・損害の最小化にも触れている。このほか、憲章では、「設計者資格」、「利用者資格」という項目も設けられており、そこでは、ロボットの設計者及び利用者に推奨される行動が列挙されている¹⁶⁹。

次に、欧州議会の勧告文書の要点を整理し、適宜筆者の見解を述べる。

ロボットが自己学習と自律性¹⁷⁰を持ちつつあることを踏まえると、人を代理する「エージェント」に近づいていく(法的責任の項目：Z. AC. AD.)。そして、現在の法的枠組みにおいて、ロボットが第三者へ損害を与えた場合に、当該ロボットに責任を負わせることはでき

¹⁶⁹ なお、原文では、“licence”とされているが、ロボットの設計や利用を許可制にすべきという内容にはなっていない。

¹⁷⁰ 本民事規則 AA.では、外部からの制御や影響から独立して意思決定し、実行する能力をロボットの自律性として定義している。

ないが、その一方で、ロボットの自律性について、取り扱う法分野の特定が必要となる。

人間とロボットの感情的な結びつきの懸念については、民間利用にかかるロボティクスとAIの開発に関する一般原則が関係する(3.)。いわゆる社会的弱者を対象に、ロボットと感情的つながりが生じる可能性がある開発には、特別な注意が払われるべきである。

倫理原則(12.)、知的財産権とデータ流通(20.)の中には、プライバシーや人間の尊厳にもつながる記載がある。そこでは、AIによる判断の理論的根拠を常に提示できることや、人間に理解できる形に変換して提供することなどが「透明性の原則」として求められている。その他、決議は、GDPRの枠組みの中で、ロボットのカメラやセンサーの使用について、規則と基準を明確にすることを欧州委員会に要請している。プライバシー・バイ・デザイン、プライバシー・バイ・デフォルト、データの最小化、目的の制限といったデータ保護規則を確実に実施すべきである。

ロボットは個人データを抽出し、外部へ送信するため、伝統的に保護されてきた領域にロボットが設置されると、機密性に重大な脅威を及ぼす(倫理原則:14.)。自律型ロボットに「電子人間」の地位を与え、自身が起こした損害の責任を負わせることや、「電子的人格」を認める可能性がある(法的責任:59.(f))。

ロボット憲章の中では、ロボット開発者ための倫理的実施規範によって、「善行」、「非有害」、「自律性」、「正義」の4つの原則が示された。そのうち、「自律性」の原則は、ロボットを利用するに当たっての条件を利用者に事前に通知し、利用者は強制されることなく意思決定ができることを意味しており、これは、人間の自己決定権に配慮するものである。規範本文においては、「包含性」、「可逆性」という言葉が用いられた。「包含性」は、全ての利害関係者が研究活動の意思決定過程に参加できることを指し、これによって透明性が保障され、利害関係者が情報にアクセスできる権利が尊重される。「可逆性」は、それがロボットに実装されることで、利用者が望ましくない行動を取り消して、「よい」状態に戻すことができる。

また、規範本文のプライバシーの項目では、開発者に対し、情報の安全管理、目的外利用の禁止、個人識別ができないようにすることの保障(厳格なインフォームドコンセントがある場合を除く)や、データ資産からも含めた、関連するデータの破棄・削除の要求への対応が求められている。

「設計者資格」では、より具体的な言葉でロボット開発者に対する要請事項が記載されている。プライバシー・バイ・デザイン、キルスイッチを含む明白なオプトアウトの仕組みの導入、ロボットの意思決定過程の再構成と、追跡ツール開発を含む追跡可能性の保障¹⁷¹、透明性の確保が求められている。「利用者資格」では、他人のプライバシーの尊重・保護や、倫理原則等の遵守、武器利用の禁止が求められている。

¹⁷¹ 「設計者資格」では、追跡ツールによって、ロボットがとった行動の解釈が容易になると言及している。

2 検討

決議は、ロボットがもたらした損害の責任について、現在の法規制では当該ロボットにその責めを負わせられない一方で、当該ロボットの関係者（製造業者、運用者、所有者、利用者）に対しても、その責任を負わせられる場面は限定的であると指摘している。これは、プライバシー侵害に関しても同じであると考えられる。そこで、同決議は、プライバシーに関しては、ロボットの設計段階からプライバシーを保護（プライバシー・バイ・デザイン）できるように、ロボット開発者に対策を求めるとともに、利用者に対しても「利用者資格」の形で配慮を求めることで、もっぱら、事前の予防措置を徹底するという考えが示されている。予防措置の内容としては、プライバシー・バイ・デザイン、プライバシー・バイ・デフォルト、透明性の確保、データの最小化、目的の制限、目的外利用の禁止、インフォームドコンセント、安全管理措置といった、GDPR を踏まえたものが挙げられた。法的観点のほかに、電子人間、電子的人格、包含性、可逆性、追跡可能性などといった、ロボットの性質に着目した言及・提案もなされた。とりわけ、プライバシー領域内から外部へ個人データを送信するロボットによる機密性侵害は、まさに家庭内のヒト型ロボットが抱える重大な懸念である。

また、本決議は、「この感情的愛着は人間をだますことができる」（**this emotional attachment could have on humans**）」と述べており、そのことは、ロボットとの間で感情的つながりが生じることへの懸念を示している。こうした不安への対応策の1つとして、ロボット憲章内の設計者資格として、「人間とやり取りする場合は、ロボットはロボットとして識別可能であることを確実にすべき」との主張がなされた点は、ヒト型ロボットのもたらす問題との関係で重要性がある。

さらに、オプトアウトの仕組み自体は、データ保護の観点から既に導入されてきたものであるが、本決議が、ロボットを対象に「キルスイッチ」の導入に言及したことも注目される。

つまり、家庭内ロボットに関して、本決議から得られる示唆をまとめると、①プライバシーに関しては、GDPR を踏まえた予防措置の実施、②ロボットに対するオプトアウト手段としてのキルスイッチの導入、③人間とロボットの感情的結びつきへの懸念、という3点に整理することができる。

第5章 日本

第1節 政策動向・法制度

日本の民間部門におけるプライバシー・個人情報に関する法律は、「個人情報の保護に関する法律」（平成15年法律第57号）（以下「個人情報保護法」という）である。同法は、2015年9月に改正され、改正法は2017年5月に全面施行された¹⁷²。改正法では、以下の事項に対応するための規定が整備された¹⁷³。

- 1 個人情報の定義の明確化
- 2 適切な規律のもとで個人情報等の有用性を確保するための規定の整備
- 3 個人情報の保護を強化するための規定の整備
- 4 個人情報保護委員会の新設及びその権限に関する規定の整備
- 5 個人情報の取扱いのグローバル化に対応するための規定の整備

今回の改正は、2003年の個人情報保護法制定から10年を経たものである。その背景には、SNSやスマートフォンをはじめとする新たな情報通信技術の利用に伴い、いわゆるビッグデータの収集・分析が可能になることによる問題への対応がある。具体的には、個人に関する情報（パーソナルデータ）について、自由な利活用が許容されるのかが不明確な「グレーゾーン」が発生・拡大し、パーソナルデータの取扱いに躊躇する場面が発生していることや、逆に、安易な匿名化によって個人情報に該当しない情報であると誤解して利活用に踏み切るなどといった問題に対処することが主な検討課題であった。このため、プロファイリングをはじめとした、AIに関する重要な課題は、今回の法改正に含まれていない¹⁷⁴。

個人情報保護法は、主に、個人情報取扱事業者を規律・監督するために、当該事業者の義務を定めている。係る義務には、個人情報の利用目的の特定（第15条）、利用目的による制限（第16条）、適正な取得（第17条）、取得に際しての利用目的の通知（第18条）、データ内容の正確性の確保（第19条）、安全管理措置（第20条）、従業者・委託先の監督（第21条、第22条）、第三者提供の制限（第23条）などがあり、これらは個人情報、ひいては「本人」を保護するものではある。しかし、個人情報取扱事業者による「本人」に対する賠償等責任については、個人情報保護法上の定めがなく、民事上、一般的な不法行為として民法第709条（不法行為による損害賠償）によって救済が図られることになる。

プライバシーには法文上の定義はないが、プライバシー権は憲法第13条「幸福追求権」に基づくと解釈されている¹⁷⁵。これは、1964年の「宴のあと」事件における東京地裁判決

¹⁷² 「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律」（平成27年法律第65号）。2015年9月成立・公布、2016年1月一部施行、2017年5月完全施行。

¹⁷³ 新保・前掲注45・222頁

¹⁷⁴ 新保・前掲注45・220頁

¹⁷⁵ 曾我部真裕・林秀弥・栗田昌裕『情報法概説』（光文堂、2016）281頁

176が、「私事をみだりに公開されないという法的保障ないし権利」を、「個人の尊厳を保ち幸福の追求を保証するうえにおいても必要不可欠なもの」として認めた¹⁷⁷ことによる。このことから、従来のプライバシー権は、私事の公開や私生活への侵入から保護される権利（伝統的プライバシー権¹⁷⁸）として理解されてきた。その後、自己に関する情報をコントロールする権利（自己情報コントロール権）とする立場が有力化した。最高裁レベルでは、2002年の「石に泳ぐ魚」事件最高裁判決¹⁷⁹がある。この事件では、顔面に腫瘍のある大学院生をモデルとした人物が登場する小説において、当該人物の経歴等に虚構の混じった苛烈な表現が用いられたことによって「名誉が毀損され、プライバシー及び名誉感情が侵害された」として、不法行為による精神的損害の賠償に加えて、侵害行為の差止めが認められた¹⁸⁰。ただし、同判決では、名誉、プライバシー、名誉感情が列举されるのみで、プライバシー侵害に固有の要件は明らかになっていないとの指摘¹⁸¹がある。

また、プライバシー権を自己情報コントロール権と理解する場合、侵害に対する救済方法として、損害賠償請求や差止め請求のほか、個人情報の開示・訂正・削除等を求め、その目的外の利用や第三者への提供を禁止することが有効と考えられる。個人情報保護法は、これら手段を具体化しているため、一般に、日本の個人情報保護制度は、自己情報コントロール権の具体化として位置づけられている¹⁸²。個人情報の取り扱いが争われた最高裁判例には、2003年の早稲田大学江沢民事件最高裁判決¹⁸³がある。この事件では、警備を目的に、大学が警察に講演会参加者名簿を提出したことが問題となった。最高裁は、「早稲田大学が個人識別等を行うための単純な情報であって、その限りにおいては、秘匿されるべき必要性が必ずしも高いものではない」学籍番号、氏名、住所、電話番号といった単純な個人情報についても、「本人が、自己が欲しない他者にはみだりにこれを開示されたくないと考えることは自然なことであり、そのことへの期待は保護されるべきものであるから、本件個人情報、

¹⁷⁶ 東京地判昭和 39 年 9 月 28 日下民集 15 卷 9 号 2317 頁

¹⁷⁷ この判決の中で、日本におけるプライバシーの権利は初めて裁判上認められた。（山本龍彦『プライバシーの権利を考える』（信山社、2017 年）27 頁）また、いわゆるプライバシー侵害の 3 要件（私事性、秘匿性、非公知性）も明らかにされた（曾我部ら・前掲注 175・285 頁）。

¹⁷⁸ 「古典的プライバシー権」とも表現される。

¹⁷⁹ 最判平成 14 年 9 月 24 日判時 1802 号 60 頁

¹⁸⁰ 判決は、「侵害行為が明らかに予想され、その侵害行為によって被害者が重大な損失を受けるおそれがあり、かつ、その回復を事後に図るのが不可能ないし著しく困難になると認められるときは侵害行為の差止めを肯認すべき」であるとし、本事件について「出版等による公表を差し止める必要性は極めて大きい」と判示した。

¹⁸¹ 曾我部ら・前掲注 175・289 頁

¹⁸² 曾我部ら・前掲注 175・176 頁

なお、自己情報コントロール権説も、私的領域への侵入や私事の公開といった古典的なプライバシー侵害に対する保護を否定しない。（曾我部ら・前掲注 175・177 頁）

¹⁸³ 最判平成 15 年 9 月 12 日民集 57 卷 8 号 973 頁

上告人らのプライバシーに係る情報として法的保護の対象となる」と判示した¹⁸⁴。

自己情報コントロール権については、本来的な保護の対象を思想・信条などの機微な情報に限定するかどうかによって、限定説と非限定説に分けられる。限定説では、本来的な保護の対象を「個人の道徳的自律と存在」に直接関わる情報に限定し、このような情報を「プライバシー固有情報」¹⁸⁵と呼称する。直接関わらない情報は「プライバシー外延情報」と呼び、それが悪用され、または集積利用されるときに限って権利侵害の問題を生じさせる。非限定説では、自己情報全てをプライバシーの権利の対象と考え、権利侵害の許容性を判断する際に情報の性質を考慮して対処する¹⁸⁶。日本の個人情報保護法は、非限定説に多大な影響を受けている¹⁸⁷。

慶應義塾大学の山本龍彦教授は、その著書¹⁸⁸において、プライバシー権の変容を第 1 期から第 3 期に分けて説明している。それによると、第 1 期は「私生活秘匿権」、第 2 期は「ウェットな自己情報コントロール権」、第 3 期は「ドライな自己情報コントロール権」である。第 1 期は前述の「古典的プライバシー権」、第 2 期は「自己情報コントロール権限定説」、第 3 期は「同非限定説」と対応する。山本教授は、この第 3 期について、プライバシー権論の構造論的転回が見られると主張している。これはつまり、プライバシー権の議論が、「システム構築を前提として、その構造やアーキテクチャをどのように設計すべきかという問題へと移ってきている」ことを意味する。山本教授は、「第 3 期プライバシー権論の発想に親和的な判決の 1 つ」として、2008 年の住基ネット事件最高裁判決¹⁸⁹を取り上げている。この事件では、住民基本台帳ネットワーク（住基ネット）の運用に伴う行政機関による本人確認情報¹⁹⁰の管理・利用がプライバシー侵害にあたるかどうか争われた。最高裁は、「住基ネットにシステム技術上又は法制度上の不備」があつて、本人確認情報が「第三者に開示又は公表される具体的な危険が生じているということもできない」と判示し、プライバシー侵害を否定した。山本教授は、本判決が、今現在侵害されていないという事実から「侵害なし」と結論を出したのではなく、将来侵害が生ずるおそれがあるかどうかまでを審査して、「侵害なし」と結論を出したことに着目し、本判決で重視されたのは住基ネットシステムの

¹⁸⁴ さらに判決では、本件個人情報について、「取扱い方によっては、個人の人格的な権利利益を損なうおそれ」があるため、「慎重に取り扱われる必要」があり、無断で本件個人情報を警察に開示した同大学の行為は、上告人らが任意に提供したプライバシーに係る情報の適切な管理についての合理的な期待を裏切るものであり、上告人らのプライバシーを侵害するものとして不法行為を構成する」と判示した。

¹⁸⁵ 思想・信条などの個人の心身の基本に関する情報（センシティブ情報）が該当する。

（曾我部ら・前掲注 175・176 頁）

¹⁸⁶ 曾我部ら・前掲注 175・176 頁

¹⁸⁷ 山本龍彦『プライバシーの権利を考える』（信山社、2017）7 頁

¹⁸⁸ 山本・前掲注 187・3-64 頁

¹⁸⁹ 最判平成 20 年 3 月 6 日民集 62 卷 3 号 665 頁

¹⁹⁰ 氏名、生年月日、性別、住所等があたる。（住民基本台帳法（昭和 42 年法律第 81 号）第 30 条の 5 第 1 項）

「構造」であったと指摘した。このように、個人に関する情報が大量に収集され、情報システムやデータベース上に大量に蓄積された上で、解析されるような現代の情報化社会において、自己に関する情報のコントロール権は、「(データベース) の構造ないしアーキテクチャ全体をコントロールするという客観的側面が強調」される。そしてその結果として、第3期のプライバシー権は、システム構築を目的とした個人情報の収集・保存によって、それが機微な情報であるか単純情報であるかに関わらず「侵害」されうると山本教授は指摘する。しかし、この主張における課題の1つとして、情報システム等が行う情報の収集・保存が「情報主体に漠とした不安や懸念を抱かせるが、それ自体で、情報主体に具体的な損害を与えるわけではない。そうすると、こうした行為を果たして権利侵害と構成することができるのか」といった疑問が生じる。この点、山本教授は、プライバシー権の社会公共的利益¹⁹¹に着目し、情報システムの構築等が社会全体に及ぼす影響も考慮して、プライバシー権の侵害を判断するという理解を試みている。また、第2のアプローチとして、「予防的ルール」としての権利論¹⁹²を採用し、ドライな自己情報コントロール権が、予防的でリスク・コントロール的な性格を有するために、その「権利」性を否定されないという理解も提示している。

なお、他者の干渉を受けることなく、私事に関わる事柄について自ら決定する権利である自己決定権をプライバシー権に含めるという主張もあるが、日本法において必要性は乏しいとの指摘¹⁹³がある。

このように、我が国では、個人に関する情報を保護することを企図した法律の整備はなされているものの、前記のとおり、プライバシーは法文上直接には言及されていない。現に、「日本の個人情報保護論議は、情報漏えいによる安全管理措置違反や個人データの第三者提供を中心に行われてきた」との指摘¹⁹⁴もなされている。一方、学界では、情報ネットワーク法学会のロボット法研究会や、人工知能学会の倫理委員会が立ち上がるなど、AI やロボットに特化した検討が始まっている。既に述べたとおり、AI が社会へ浸透することによるプライバシー・個人情報上の懸念には種々のものがあるが、その最たるものは、自己学習によって高度化し、より精緻に分析し、プライバシー性の高い情報を見出しうるプロファイリングであると考えられる。プライバシー性の高い情報は、その活用の仕方によっては、社会的排除や差別的取扱いを招くことになり、慎重な検討が求められる。プライバシーを中心としたプロファイリングの検討について、慶應義塾大学の山本龍彦教授が著名であり、山本教

¹⁹¹ 結婚制度など伝統的な共同体的価値を保護する、共同体の道徳的規範を維持する、政治的討議空間を構成等する、国家による全体社会主義的干渉に抗することなどを例示している。

¹⁹² 通常「憲法上の権利」とみなしているものの多くは、実際には、核心的な憲法価値を実効的に保護するために、あるいは、将来生じうる核心的憲法価値の侵害を未然に防ぐために設定された政策的で戦略的なルールであるという主張である。このため、ルールの予防的性格は、「権利」性を否定する論拠とならない。(山本・前掲注 187・18-19 頁)

¹⁹³ 曾我部ら・前掲注 175・284 頁

¹⁹⁴ 石井・前掲注 102・125 頁

授は著書¹⁹⁵において概ね以下のように論じている。

第2節 プロファイリング

図書館の貸出記録から、利用者の政治的信条等を予測するような古典的なプロファイリングと、Amazon.com のレコメンド機能¹⁹⁶のような現代的なプロファイリングの違いには、以下の5点が挙げられる。

1 データ量

現代のプロファイリングに使用されるデータ量は膨大である。

2 自動性

現代のプロファイリング対象者の個人的側面の予測・評価場面においては、基本的に人間の関与が必要でなく、自動的である。

3 科学的信憑性

豊富なデータ量と人間の直感を排した自動処理によって行われる現代のプロファイリングは、結果に対する科学的信憑性が一般に高い。

4 意外性（予見困難性）

現代のプロファイリングでは、人間が予見しづらい、意外性の高いデータが用いられ、人間の想像がつかないような事物の相関関係が明らかになる場合がある。このため、人の行動を萎縮させる傾向を持つ。

5 項目の広範性・細目性

現代的なプロファイリングでは、対象項目が拡張され、細かい個人的事項までも予測・評価できる。

以上のとおり、現代的なプロファイリングは、使用されるデータ量の増加や人工知能の発達等による自動処理の高度化などによって、科学的信憑性を高め、その利用範囲を急速に拡大させてきている。このことは、経済的合理性や効率性の向上に資するものであるが、他方で、次のような4つの法的問題を指摘することができる。

1 プライバシー権の侵害

個人の私生活を覗き見することは、伝統的にプライバシー権の侵害を構成するものと考えられてきた。本人の同意なく機微な情報を取得することは同権利の侵害を構成するものと解される。よって、私生活の核心や、機微な私的事項を、本人の同意なく、アルゴ

¹⁹⁵ 山本・前掲注187

¹⁹⁶ 山本教授は、「コンピュータのアルゴリズムを用いて、ユーザーの過去の閲覧・購買履歴から当該ユーザーの選好を分析・予測し、その者の選好に合致した商品をおすすめ」するものと説明している。

リズムによって自動的にプロファイリングすることは、プライバシー権を侵害する。

2 内心の自由の侵害（意思の操作・誘導）

プロファイリングによって明らかになった対象者の心理状況に応じて、過度な操作や誘導がなされる。（商品広告・購買への誘導、個人標的的な選挙運動・情報フィード・投票行動の誘導など）

3 選挙権の侵害、選挙の公正の揺らぎ、民主主義の弱体化

プロファイリングによって情報の偏向が生じ、有権者の主体的な判断が歪み、選挙権の適切な行使が阻害され、選挙の公正が脅かされる。個人的選好を刺激することに重きが置かれた選挙運動は、社会公共的問題の討議機会を減少させ、有権者の主体的判断の機会を奪うため、選挙と統治の断絶を生む。

4 平等原則、個人の尊重原理との抵触

プロファイリングでは、機械学習の結果、差別的「意図」なく、人種等、一般に配慮すべき要素がアルゴリズムに組み込まれる可能性がある。このような要素をアルゴリズム上で考慮することを直接的に禁止したとしても、その周辺要素を考慮することによって、迂回的に、保護されるはずであった対象者が不利な取扱いを受け得る。また、あるプロファイリング結果が別のプロファイリング結果に悪影響を与えることで「負のスパイラル」が生じ、社会的・経済的に排除され続ける者らが生じるおそれがある。科学的信憑性及び、アルゴリズムの高度の専門性・複雑性・不透明性のため、彼らは反論が困難である。人生の重要場面で、個々の事情を斟酌せず、自動的な確率的判断のみによって概括的・抽象的に個人を評価することは、「個人の尊重¹⁹⁷」原理と鋭く矛盾する。

このように、山本教授は、プロファイリングの特徴について、プロファイリング結果の科学的信憑性、広範性・細目性や、利用されるデータ及びプロファイリング結果の意外性などを挙げた。そして、法的課題としては、本人の同意なしに機微な情報を導出されるプライバシー侵害や、プロファイリング結果に基づいた特定個人を対象とする過度な操作・誘導、提供情報の偏向のほか、反論が困難な差別的取扱い・社会的経済的排除が指摘されている。

なお、山本教授は、我が国の個人情報保護法制におけるオプトアウトについて、個人情報取扱事業者が公表するプライバシーポリシーの難解さや膨大な量を理由に、オプトアウトの枠組みの実効性に疑問を呈している¹⁹⁸。個人への告知に実効性や有効性を持たせるという観点から、主に、米国・カリフォルニア州のオンラインプライバシー保護法¹⁹⁹を参照し、アイコンの導入といったデザイン上の工夫による視覚的・直感的な告知は、法的な要求になりつつあると指摘した²⁰⁰。

¹⁹⁷ 憲法第 13 条

¹⁹⁸ 山本・前掲注 187・156-157 頁

¹⁹⁹ California Online Privacy Protection Act of 2003 (Cal. Bus. & Prof. Code § § 22575-22579)

²⁰⁰ 山本・前掲注 187・161-165 頁

このように、我が国においては、AI やプライバシーを正面から受け止められる法的枠組みは整備されていない。一方、学界においては、既にプロファイリングの課題についての議論は始まっており、この議論の成果を、個人情報保護法 3 年毎の見直し²⁰¹の過程に反映させていく必要があるものと思われる。

²⁰¹ 個人情報保護法附則第 12 条 3 項

第6章 考察・結論

第1節 各章の要旨

本論文の目的は、第1章で述べたとおり、家庭内のヒト型ロボットが個人に関する情報を用いる場面に焦点を当て、プライバシー・個人情報保護の観点から、考え得る法的課題を整理し、今後のAI及びロボット技術の展開とプライバシー・個人情報保護のバランスを図るための政策的提言を論じることである。その目的を達成するために、第2章では、ヒト型ロボットや、関連するAI技術について概説し、第3章から第5章では、それぞれ、米国、EU、日本におけるAI・ロボットの活用に関し、事例や研究、政策動向・法制度について整理した。

各章の検討から、次のようなことが明らかになった。

第1章では、AI・ロボットに関して、政府を中心とした我が国の検討の状況を取りまとめた。また、政府研究会報告書も踏まえて、プライバシー・個人情報に関するリスクを整理し、AI・ロボットによるデータの取得・利用について、本人への説明不足、同意の難化・形骸化、プロファイリングによる社会的排除・差別的取扱いの連鎖、AIの高度化により個人の予見範囲を超えてデータが利用される可能性が問題になることを述べた。さらに、人の形を模した親しみやすいロボットが一般家庭に配備されることで、よりプライバシー性の高い情報がロボットに収集・分析され、外部に流出されていく可能性も指摘した。

第2章では、本研究で取り扱う「ヒト型ロボット」の特徴及びそれが与える影響を検討した。本論文では、ヒト型ロボットを、「AIを搭載し、対話を中心に人とコミュニケーションを行う、人の形を模したロボット」と定義した。ヒト型ロボットは、特にAIを搭載し、対話システムを持ち、人の形をとることの3点を特徴とする。現在注目されるディープラーニングをもってしても、対話システムには技術的課題が複数存在している。しかし、人間の形を模したヒト型ロボットには、人間がロボットに心地よさを感じるなどから、コミュニケーションを円滑にするという効果がある。ヒト型ロボットが広く一般家庭に普及するには、相当程度時間を要すると思われるが、一部では既にヒト型ロボットが一般家庭に存在しているのも事実である。今後のヒト型ロボットの普及を念頭に置いた議論を進める必要がある。

第3章では、米国のプライバシー保護の議論状況を整理した。米国では、政権交代の影響により、政府レベルではプライバシー論議が停滞しているものの、学界では、前向きな検討が行われている。

各家庭に存在するロボットは、その機能の拡張や改善をネットワーク経由で行うことができ、また、低コストで機械学習の機能を備えることができる。しかし、それを行うためには、家庭内ロボットがカメラやマイク等で収集した情報等を外部の第三者に送信し、クラウドを経由する等して、他の家庭内ロボットと情報を共有しなければならない。また、“social interaction”が倫理とプライバシーに関する新たな問題を惹起する可能性がある（第3章：AI100報告書）。

AI に特有の論点には、差別的取扱いと、擬人化したインターフェースがある。社会的に不名誉な評価の判断材料に、人種や性的嗜好といった機微な情報が用いられることは、差別的取扱いに当たり、AI による判断においても同様に、機微な情報は用いられるべきではない。機微な情報を利用しないようにするためには技術的課題があるものの、プライバシー・バイ・デザインの考え方を導入することで、人間よりも差別的な判断を減らすことができる。AI に対する規制のあり方は、まず原則（principle）から始めるべきである。これは、米国の既存のプライバシー規制が、解釈の幅のある目標設定を法執行で担保するという規制の在り方を採用することによって、プライバシーは自らの責任であると企業に認識させることに成功しているからである（第3章：AI100 報告書）。

IEEE イニシアティブの報告書 EADv1 は、ユーザーと事業者間の「データの非対称性」に着目し、標準を策定することなどによる解決の提案を行っている。同報告書は、AI/AS に係るプライバシー上の懸念について、概ね、①設計時におけるプライバシー配慮の欠如、②それが招来する結果を理解していない利用者による、個人データの取扱いへの同意（インフォームドコンセントの実効性の担保）、③絶え間なく生成される自己のデータに関する、データ・ポータビリティ（移管）を含むアクセス手段や同意の欠如、④プロファイリングを挙げている。①への対応としては、プライバシー・バイ・デザイン/プライバシー・バイ・デフォルトの考え方を実装するための標準の策定、②に対しては、個人データを解析・分析するAI/AS 自身が、同意に向けた個人の理解をリアルタイムに手助けすること、③に対しては、データ・ポータビリティや、データ収集時の文脈から外れたデータ利用が行われる際に、個人が機動的に同意するための仕組みの必要性、④については、データ利用への同意に条件を設定し、都度の同意取得を求めること、同意撤回やデータ消去の手段を個人に提供する必要性が提案されている。これらのほか、AI/AS に関する透明性も不可欠である。最終的には、「個人が自身のデータを管理し、共有するアルゴリズムガーディアンプラットフォーム」の開発が行われるべきである（第3章：EADv1 報告書）。

EADv1 が言及したものの中から、特筆すべきものを挙げると、個人データ利用に際して、利用目的により取得範囲を制限すべきこと、個人データ利用への同意に際し、条件を設定すべきこと、個人による自己データの管理について、AI による代行を行うべきことである。特に最後の考え方は、AI による個人の負担を AI によって低減させようというアプローチであり、これが実現すれば、大幅に個人の負担を軽減させることが期待される。

学界での研究成果のうち、Calo 助教が指摘したロボットの社会的側面に関する3つのプライバシー上の脅威は、①「家庭等伝統的プライバシー領域の侵食」、②「ロボットの特性を活かした、人からの強力な情報取得」、③「個人が設定したロボット等との関係それ自体のプライバシー性」である。①との関連で、Calo 助教が指摘した「心理的覚醒」という主張は、ヒト型ロボットを始めとするソーシャルロボットには重要な指摘である。家庭などの伝統的にプライバシーが確保されてきた領域に、人が生来的に人間と認識してしまうソーシャルロボットが導入されることによって、人が心理的に覚醒することは避けられない。外

部から距離を置き、静謐を享受できるはずの家庭等においてさえ、ロボットという人の目を意識しなければならない場面が生じるため、人は思い通りに振る舞えず、自由な内面性の露出・表現の機会を阻まれてしまう。このような Calo 助教の論文からは、以下の 4 つの示唆を得ることができる。第 1 に、ソーシャルロボットを人として捉える人間の反応は生来的であること、第 2 に、ある人から見れば、プライバシー上、ロボットは人間と変わらないということ、第 3 に、家庭内へのロボットの侵入は、そもそも利用者の同意があって行われているため、利用者自身のプライバシー主張が困難であること、第 4 に、ロボットとの関係・やり取りがプライバシー情報となりうること、である（第 3 章：Calo 論文）。

クラウドに接続した個人・家庭向けロボットを焦点に検討を行った Pagallo 教授の主張からは、4 つの示唆を得ることができる。それらは、①法的課題を検討する際に、ロボットの種類の違いが重要性を持つこと、②ヒト型ロボットに関する「プライバシーの合理的な期待」の社会的合意形成のためには、ネットワークを利用する個人・家庭向けロボットと、ロボットを教育し、管理する手法が課題となること、③法的課題として、インフォームドコンセント（説明を受けた上での同意）、制御されないロボットが収集したデータ処理に関する代位責任、法に抵触したロボットを意図せず使用した人の過失責任、データを不正処理するロボットの直接的説明責任が問題となること、④プライバシー・バイ・デザインのようなアプローチの不十分さ、である。プライバシー・バイ・デザインが効果を発揮しないのは、ネットワークを利用するロボットの予測不能性や自律性によって、保護すべき情報の種類が影響を受けるとともに、ロボットによる情報の取捨選択の基準も影響を受ける可能性があることを理由とする（第 3 章：Pagallo 論文）。

Pagallo 教授は、「プライバシーの合理的な期待」を担保するために、ロボットをトレーニングする手法に注目している。これは、ヒト型ロボットを社会的に受容されるものとするために重要な提案であるといえる。

第 4 章では、包括的な個人情報保護法制を有する EU の GDPR の関連規程を整理し、欧州議会勧告を検討した。GDPR は多岐にわたる規定を置いているが、家庭内ロボットに適用し得るものがある。それらは、データ主体に付与される権利のうち、特に第 15 条（アクセス権）、第 20 条（データ・ポータビリティ）、第 21 条（異議申立権）、第 22 条（プロファイリング）である。これらの規定によって、データ主体は、サービス提供プラットフォームを選択する自由や、プロファイリングを通じた自動的手段のみによる決定に対し、受け入れるかどうか選択する自由を与えられている。ただし、AI ロボットの文脈で、これらの制度をどこまで実現できるのかが課題となる。

第 25 条のデータ保護バイ・デザイン、データ保護バイ・デフォルトの考え方は、管理者側に、事前のプライバシー保護を実装するよう促すとともに、利用者側には、リテラシーが高くない場合でも個人データが自動的に保護される仕組みを提供する。Pagallo 教授はプライバシー・バイ・デザインに否定的な立場を示しているが、筆者は逆に、この発想は、様々な種類のロボットが一般に普及した場合に効果的と考えている。なぜなら、ロボットは、設

置目的に応じたサービスを提供するために、それぞれ異なる機能や形状を持ち、こうした差異に基づき、利用者は個人データの取扱いに対する同意等の対応を迫られるためである。プライバシー・バイ・デザインは、その実装技術が問題となるが、AI にエージェントを組み込む手法も検討されており、状況による違いにも対応できるような努力が払われている。今後、ロボットの種類の増加が予想される中、利用者はロボットの違いを見極め、ロボットごとに異なる注意事項等を把握しなければならなくなる。しかし、このような対応を利用者に求めるのは現実的とはいえない。このため、利用者が何もせずとも個人データ保護が提供される仕組みや考え方は、プライバシー・バイ・デザインの優れた発想であり、消費者保護の観点からも重要と思われる。

GDPR の要点を再掲すると、以下のとおりである。

- 1 GDPR は、自然人の、個人データを保護する権利を保護するものであり、様々な権利を用意している。
- 2 個人データの利用に係るデータ主体からの同意取得が明示的なものとなるよう、十分な情報提供を経た同意取得（インフォームド・コンセント）が求められる。また、当該同意は撤回可能である。
- 3 データ主体は、自己の個人データを、管理者を超えて移動させることができる（データ・ポータビリティ）
- 4 データ主体は、プロファイリングを用いた決定を受け入れるかどうかを選択する自由を有する。
- 5 データ保護・バイ・デザイン及びバイ・デフォルトによって、データ主体は、自ら努力をせずとも、個人データ保護を享受することができる。

他方、GDPR について検討すべき論点として、以下のものを挙げることができる。

- 1 データ主体の合理的な予測は、自ら機能を強化し、プロファイリングを行う AI やそれを搭載したロボットに対して、どこまで担保できるのか。
- 2 ロボットが個人データを取り扱う際に、データ主体からはどのようにして同意を取得すべきか。ロボットが同意を取得しようとする場合、ロボットを法的主体とみることとはできるか、もしくは、ロボット以外の別途用意されたインターフェースを用意すべきか。
- 3 ロボット間のデータ・ポータビリティは現実的か。

次に、欧州議会勧告決議は、ロボットによる損害が発生した場合に、現在の法規制では、当該ロボットには責任を負わせることができず、製造業者、運用者等の関係者に対しても、その責任を負わせられる場面は限定的であると指摘している。これは、プライバシ

一侵害に関しても同じであると考えられるため、プライバシーに関しては、ロボットの設計段階からプライバシーを保護（プライバシー・バイ・デザイン）できるよう、ロボット開発者に対策を求めるとともに、利用者に対しても「利用者資格」の形で配慮を求めるとで、もっぱら、事前の予防措置を徹底するという考えが示されている。なかでも、ロボットが、プライバシー領域内から外部へ個人データを送信する行為は、プライバシーに与える重大な懸念である。また、人間とロボットとの交流時に、人間側で「ロボットがロボットである」ことを識別可能にすべきことや、感情的つながりがロボットと生じることへの懸念は、家庭内ロボット特有の論点として注目する必要がある。さらに、オプトアウトの仕組み自体は、データ保護の観点から既に導入されてきたものであるが、本報告書がロボットを対象に「キルスイッチ」の導入に言及したことも注目される。

つまり、家庭内ロボットに関して、本決議から得られる示唆をまとめると、①プライバシーに関しては、GDPR を踏まえた予防措置の実施、②ロボットに対するオプトアウト手段としてのキルスイッチの導入、③人間とロボットの感情的結びつきへの懸念、という3点に整理することができる。

第5章では、我が国におけるAI・ロボットと、個人情報・プライバシー保護に関する法的整理を行った。AI・ロボットに関する個人情報・プライバシーに関するリスクの中でも、AIに特に関係する「プロファイリング」を中心に検討した。山本教授の指摘では、法的課題として、本人の同意のない機微な情報の導出や、特定個人を対象とした過度な操作・誘導、提供情報の偏向のほか、反論が困難な差別的取扱い・社会的経済的排除が問題となる。

以上の法的課題を踏まえ、次節以下では、プライバシー保護及び個人情報保護法の観点から、次のような提言を行いたい。

第2節 プライバシー保護の観点からの提言

前節で述べたように、対話システムによる意思疎通や、ヒト型ロボットによって、ロボットと人間の間のコミュニケーションが円滑になると考えられる。そのため、今後、家庭内にロボットが普及する場合は、「対話できるヒト型」の形態が多く採用されることが予想される。一方で、このようなロボットは、円滑なコミュニケーションを通じて、個人からより多くのプライバシー性の高い情報を取得できる。

家庭内のロボットは、外の計算リソース（クラウド、サーバー等）と通信することによって、自身が高い性能を持たなくても、機械学習などのAI技術を利用することができ、低コストで効率的な情報処理を行うことができる。一方で、そのロボットが家庭内で収集した情報が外部に送信されることによって、予想外の第三者が知るところとなるおそれもある。しかし、個人にとってみれば、ロボットにどのような情報を収集されているか、収集された情報がどのように取り扱われているのかを把握することは現実的ではない。そのため、サービス提供者側において、個人に対する十分な情報提供を行い、実効的な同意の取得に努めるべきといえる。一方で、このアプローチには限界がある。第1に、そもそも、ロボットやAI

技術が技術的に高度であり、サービス提供者側が情報提供に努めたとしても、一般人の理解が及ばない可能性が高い。第 2 に、AI を搭載したロボットには自己学習能力があるため、使用者である個人のみならず、サービス提供者にとっても、ロボットによる情報処理の結果を完全に予見することは困難である。第 3 に、たとえ十分な情報提供と実効的な同意が実現したとしても、個人が想定していない個人データの外部送信や、プロファイリングによる個人の意思の操作・誘導や、差別的取扱い・社会的排除などの対処には効果的ではない。

そこで、本論文では、以下の 3 つの対応を提案する。

- 1 個人のイニシアティブによるデータ利用条件の設定
- 2 プライバシー・バイ・デザイン及びプライバシー・バイ・デフォルト
- 3 予見可能性の醸成（個人のリテラシー向上及び社会的合意形成）

「個人のイニシアティブによるデータ利用条件の設定」は、第 3 章第 3 節で EADv1 が提案したように、個人がイニシアティブをもって、個人データを利用するための条件をサービス提供者側に課すものである。前記のとおり、個人が自己に関する個人データの取扱いに係る説明を受けても、それを理解することは困難になることが予想される。にもかかわらず、個人に Yes/No による応答を求め続けることは、過度な負担を強いることになる。そこで、個人の側から、自らのデータの利用範囲を制限し、サービス提供者側にその利用範囲を遵守させるようにすれば、当該個人の理解の及ぶ範囲でデータを管理できることにつながり、実効的な個人データ保護を期待することができる。それを推し進めたのが「プライバシー・バイ・デザイン及びプライバシー・バイ・デフォルト」である。繰り返しとなるが、これは、AI を搭載したロボットの設計段階からプライバシー保護を組み込み、それを初期設定で機能させるようにすることで、個人の側が特別な努力を払わずとも、プライバシー侵害を予防できるようになることを狙いとする。プライバシー・バイ・デザインは、Pagallo 教授を除けば、前向きに捉える立場が多い。プライバシー・バイ・デザインを技術的に実装できれば、自動的にプライバシーが組み込まれるため、個人の同意やプロファイリングの問題を多少なりとも軽減できることが期待される。AI による同意の支援制度の構築（ガーディアンプラットフォーム）、すなわち AI エージェントは、この考え方を実装する 1 つの技術的手段である。その実現可能性を含め、家庭内ロボットを含む AI 技術への実装方法について、日本でもプライバシー・バイ・デザインの議論を進めることが望ましい。なお、プライバシー・バイ・デザインは、必ずしも法制度を前提とする仕組みではないため、自主的措置によって柔軟に対処することも可能である。

「予見可能性の醸成（個人のリテラシー向上及び社会的合意形成）」は、ロボットと人間との均衡の取れた共存を図るために重要といえる。シンギュラリティ²⁰²を含め、AI・ロボ

²⁰² AI の高度化の結果、自己学習能力によって、AI 自身が自己再生産し、加速度的に能力を向上させるかもしれない。Bay Kurzweil はこの時点をシンギュラリティ

ットの機能向上は加速度的なものとなっていくと考えられるものの、個人の予見可能性を担保するための努力を怠るべきではない。各個人の AI・ロボットリテラシーの向上や、予見可能性の範囲に共通認識を得るための社会的な合意形成を図るための継続的な教育も行っていくべきである。

第 3 節 個人情報保護法の観点からの提言

第 5 章で述べたとおり、個人情報保護法は、AI に関する課題に対応するものとはいえない。個人情報保護法の観点から見た場合、AI に関する中心的論点はプロファイリングであり、より具体的には、プロファイリングを通じた機微な情報の生成、意思の操作・誘導、差別的取扱い・社会的排除が問題となる。

「機微な情報の生成」との関連で、個人情報保護法は、要配慮個人情報²⁰³の取得に本人の事前同意を義務付けている²⁰⁴。この解釈について、ロボットがプロファイリングによって機微な情報を生成する前に、本人の同意を得なければならないと主張する見解がある²⁰⁵。この立場に基づく、ロボットがプロファイリングによって要配慮個人情報にたどり着くか否か、また、たどり着く時期が不明であるため、サービス提供者側は個別同意を回避し、事前に本人から包括同意を得ようとするのが想定される。しかし、包括同意では、本人は「いつ」「どのような」要配慮個人情報生成されたのかを認識できないため、実効的なプライバシー保護を図ることはできない。そこで、第 1 の立法論としては、プロファイリングに関する新たな規定を設けることを検討する必要があると考えられる。ただし、プロファイリングを制限するような立法を行うとすると、例えば、Amazon.com のレコメンド機能²⁰⁶などは極端な「意思の操作・誘導」であって、排除されるべきではないか、といった議論が想定されるため、規制範囲は慎重に考えるべきである。この点、筆者は、広告等を提供する場面において、プロファイリングを行い個人向けサービスを指向しているにもかかわらず、そのことを明示しない場合には、米国の立法例に倣い、欺瞞的行為として規制の対象にすることができるのではないかと考える。欺瞞的行為に関する規制は、第 2 の立法論に位置づけられる。

第 3 に、GDPR の定める異議申立権や、自動的決定に服さない権利は、「差別的取扱い・社会的排除」に対処する規定である。日本の個人情報保護法に基づけば、プロファイリングも個人情報を利用する一形態であるため、利用目的の特定及び目的外利用の制限に関する

(Singularity) と呼び、2045 年におけるその到来を予測した。(総務省(前掲注 24) 報告書が次の文献を参照。Ray Kurzweil, THE SINGULARITY IS NEAR: WHEN HUMANS TRANSCEND BIOLOGY (Viking, 2005))

²⁰³ 前掲注 118

²⁰⁴ 個人情報保護法 第 17 条 2 項

²⁰⁵ 山本・前掲注 187・148-150 頁

²⁰⁶ 山本・前掲注 187

規定²⁰⁷を遵守することによって、プロファイリングを行うことは認められる。しかし、プロファイリング結果の連鎖によって社会的排除が生じると、個人の尊厳を損なう危険があるため、日本の法制度の中に GDPR に類する上記制度を導入することにも、一考の余地はある。

第 4 に、本章第 1 節で筆者が提案した 3 つの対応のうち、「個人のイニシアティブによるデータ利用条件の設定」については、基本的には民間主導でコンセンサスを得るべきと考えるが、個人情報取扱事業者に対し、個人情報取得時に、本人による個人情報利用条件設定の手段を提供するよう義務付けることも一案として挙げることができる。第 5 に、「プライバシー・バイ・デザイン及びプライバシー・バイ・デフォルト」についても立法措置を必須とするものではないが、プライバシー保護の事前設定を法的に義務付ける案も検討の余地はある。

第 4 節 結論

本論文の結論として、本章第 1 節及び第 2 節で行った考察結果を改めて整理する。家庭内のヒト型ロボットに関するプライバシー上の懸念は、情報の取得や、外部送信を含めた利用の状況が個人によって把握できないことであった。これに対し筆者は以下の対応を提案した。

- 1 個人のイニシアティブによるデータ利用条件の設定
- 2 プライバシー・バイ・デザイン及びプライバシー・バイ・デフォルト
- 3 予見可能性の醸成（個人のリテラシー向上及び社会的合意形成）

また、上記提案に加え、個人情報保護法の観点から、主に、プロファイリングへの対応策を提言した。なお、以下の提言は、必ずしも立法化を推進すべきというものではなく、今後の AI に関する技術的動向を踏まえ、立法政策上の検討課題として掲げるものである。

- 1 プロファイリングに対応する新規定の導入
- 2 広告等の場面における欺瞞的行為の制限
- 3 社会的排除が懸念される場合における、異議申立権及び自動的決定に服さない権利の導入
- 4 個人情報取扱事業者に対する、本人による利用条件設定の手段を提供することの義務付け
- 5 プライバシー・バイ・デザインの立法化

ところで、シンギュラリティが発生した場合には、人間より能力の勝るヒト型ロボットが、

²⁰⁷ 個人情報保護法第 15 条 1 項及び第 16 条 1 項

自ら考え、判断し、人間と意思疎通を行う事態が生じると思われる。第 3 章 4 節で整理したとおり、自らロボットを家庭内に招き入れた以上、個人の側がプライバシーの主張を行うことは原則的に困難となってしまう。しかし、本人のプライバシーへの期待をはるかに超える形でロボットが個人情報を取り扱う場合には、ロボットを「電子人間」と評価して、民法の不法行為責任を問う余地はあるかもしれないが、この議論が現実味を持って論じられるようになるまでにはまだ時間がかかるように思われる。

いずれにせよ、本論文では、現段階の議論を踏まえた提言を行った。本論文での考察の結果が、今後の AI 時代を見据えた、日本のプライバシー・個人情報保護法の発展にいくばくかの貢献をすることができれば幸いである。

参考・引用文献リスト

【政府報告書】

『日本再興戦略』98 頁（閣議決定、2013）

http://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/saikou_jpn.pdf (2018.01.10)

『第 5 期科学技術基本計画』63 頁（閣議決定、2016）

<http://www8.cao.go.jp/cstp/kihonkeikaku/index5.html> (2018.01.10)

『未来投資戦略 2017』383 頁（閣議決定、2017）

<http://www.kantei.go.jp/jp/singi/keizaisaisei/kettei.html>, (2018.01.10)

日本経済再生本部『ロボット新戦略』92 頁（日本経済再生総合事務局、2015）

<http://www.kantei.go.jp/jp/singi/robot/>, (2017.07.23)

新たな情報財検討委員会『新たな情報財検討委員会 報告書』48 頁（内閣官房、2017）

http://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2017/johozai/houkokusho.pdf (2018.01.10)

内閣府『平成 28 年版超高齢社会白書』180 頁（内閣府、2016）

http://www8.cao.go.jp/kourei/whitepaper/w-2016/zenbun/28pdf_index.html (2018.01.10)

人工知能と人間社会に関する懇談会『人工知能と人間社会に関する懇談会 報告書』23 頁

（内閣府、2017） <http://www8.cao.go.jp/cstp/tyousakai/ai/summary/> (2017.07.23)

インテリジェント化が加速する ICT の未来像に関する研究会『「インテリジェント化が加速する ICT の未来像に関する研究会」報告書』72 頁（総務省、2015）

http://www.soumu.go.jp/menu_news/s-news/01icp01_02000031.html (2018.01.10)

AI ネットワーク化検討会議『AI ネットワーク化検討会議 報告書 2016』71 頁（総務省、2016） http://www.soumu.go.jp/menu_news/s-news/01icp01_02000050.html

(2018.01.10)

AI ネットワーク社会推進会議『AI ネットワーク社会推進会議 報告書 2017』68 頁（総務省、2017） http://www.soumu.go.jp/menu_news/s-news/01icp01_02000067.html

(2018.01.10)

ロボット政策研究会『ロボット政策研究会 報告書』85 頁（経済産業省、2006）（2017 年 5 月 29 日において経済産業省の Web ページにおける公開は終了している）

情報経済小委員会『情報経済小委員会 中間取りまとめ』40 頁（経済産業省、2015）

http://www.meti.go.jp/committee/sankoushin/shojo/johokeizai/report_001.html

(2018.01.10)

国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）『NEDO ロボット白書 2014』388 頁（NEDO、2014） http://www.nedo.go.jp/library/robot_hakusyo.html

(2017.07.23)

人工知能技術戦略会議『人工知能技術戦略』23 頁（NEDO、2017）,

<http://www.nedo.go.jp/content/100862413.pdf>, (2017.07.23)

【判例・裁判例】

最判 2002・9・24 判時 1802 号 60 頁

最判 2003・9・12 民集 57 卷 8 号 973 頁

最判 2008・3・6 民集 62 卷 3 号 665 頁

東京地判 1964・9・28 下民集 15 卷 9 号 2317 頁

【雑誌・新聞】

「画像認識で「目」を高度化」日経コンピュータ 4 月 28 日号 26-31 頁(2016)

「自然言語 AI を活用」日経コンピュータ 4 月 28 日号 32-35 頁(2016)

「「バービー人形」情報漏えい？」東京新聞 2015 年 12 月 2 日 9 面

池乗有衣、柴沼均「そして家族になる」毎日新聞 2015 年 12 月 7 日 1 面

「「弟」はロボット」毎日新聞 2015 年 12 月 7 日 17 面

清水憲司「AI バービー大丈夫？」毎日新聞 2015 年 12 月 10 日 6 面
西田豊明「経済教室 日米欧、倫理問題対応急ぐ」日本経済新聞 2016 年 9 月 6 日 26 面
西垣通「経済教室 「人間の脳を超越」あり得ず」日本経済新聞 2016 年 9 月 7 日 28 面
児玉小百合「個人データ保護の新潮流 上 プロファイリング規制の動き」日本経済新聞
2017 年 1 月 16 日 17 面
山本龍彦「経済教室 AI のリスクに対応急げ」日本経済新聞 2017 年 4 月 26 日 29 面
「富士通、対話ロボ参入」日本経済新聞 2017 年 5 月 16 日 15 面
「JIS、サービスも対象に」日本経済新聞 2017 年 5 月 17 日 5 面
「AI と世界 見えてきた現実 1 ロボにも法的責任」日本経済新聞 2017 年 7 月 24 日 1 面
松尾豊「経済教室 「眼の誕生」、産業構造を一変」日本経済新聞 2017 年 8 月 7 日 14 面
宮下紘「経済教室 日本、個人の尊重を基軸に」日本経済新聞 2017 年 8 月 21 日 14 面

【書籍等】

石井夏生利『新版 個人情報保護法の現在と未来』503 頁（勁草書房、2017）
神崎洋治『ロボット解体新書』179 頁（SB クリエイティブ、2017）
久木田水生ほか『ロボットからの倫理学入門』187 頁（名古屋大学出版会、2017）
曾我部真裕・林秀弥・栗田昌裕『情報法概説』404 頁（光文堂、2016）
松尾豊『人工知能は人間を超えるか ディープラーニングの先にあるもの』263 頁
（KADOKAWA、2015）
山本龍彦『プライバシーの権利を考える』294 頁（信山社、2017 年）
日本機械工業連合会『平成 27 年度ロボット産業・技術の振興に関する調査研究報告書』
92 頁（日本機械工業連合会、2016）
日本ロボット学会編『新版 ロボット工学ハンドブック』1130 頁（コロナ社、2005）
日本工業規格（JIS）B0134: 2015 ロボットお飛びロボティックデバイス-用語
JIS B8445: 2016 ロボット及びロボティックデバイス-生活支援ロボットの安全要求事項

【論文等】

石井夏生利「米国の消費者プライバシー保護」情報通信法学研究会編『情報通信法学研究会 報告書』273 頁（総務省情報通信政策研究所、2015）3-32 頁
石井夏生利「プライバシー権」論究ジュリスト 2016 年夏号 8-15 頁（2016）
石井夏生利「世界的な潮流から見た評価と第三国への影響」Business Law Journal 2016. 8 75-78 頁（2016）
石井夏生利「伝統的プライバシー理論へのインパクト」福田雅樹・林秀弥、成原慧 編著
『AI がつなげる社会 AI ネットワーク時代の法・政策』（弘文堂、2017）
石黒浩「人間型ロボットの研究」精密工学会誌 Vol. 76 No. 1 20-23 頁（2010）
石黒浩「対話型ロボットの研究」情報処理 Vol. 57 No. 10 958-959 頁（2016）
今井倫太、安西祐一郎「クラウドネットワークロボットへの期待」電子情報通信学会誌
Vol. 95 No. 12 1048-1051 頁（2012）
江間有沙「倫理的に調和した場の設計：責任ある研究・イノベーション実践例として」人
工知能 32 巻 5 号 694-699 頁（2017）

大谷卓史「プライバシーの多義性と文脈依存性をいかに取り扱うべきか：Nissenbaum の文脈的完全性と Solove のプラグマティズム的アプローチの検討」吉備国際大学研究紀要（人文・社会科学系）第 26 号 41-62 頁（2016）

小川浩平ほか「感情でつながる、感情でつなげるロボット対話システム」人工知能 31 巻 5 号 650-655 頁（2016）

上出寛子ほか「日本語版擬人化尺度の作成」パーソナリティ研究 25 巻 3 号 218-225 頁（2017）

久木田水生「麦とペッパー-テクノロジーと人間の相互作用-」人工知能 32 巻 5 号 653-659 頁（2017）

小林正啓「クラウドネットワークロボットの法的問題点」電子情報通信学会誌 Vol. 95 No. 12 1084-1088 頁（2012）

小林正啓「ビッグデータとロボットの ELSI」電子情報通信学会誌 Vol. 99 No. 6 490-494 頁（2016）

小向太郎「米国 FTC の消費者プライバシーに関する法執行の動向」情報通信法学研究会編『情報通信法学研究会 報告書』273 頁（総務省情報通信政策研究所、2015） 33-44 頁

坂本大介・小野哲雄「ロボットの社会性：ロボットによる人間関係の構築と崩壊」情報処理学会研究報告 ICS-141(3) 15-20 頁（2005）

宍戸常寿「インターネット上の名誉棄損・プライバシー侵害」松井茂記・鈴木秀美・山口いつ子編『インターネット法』（有斐閣、2015）

新保史生「プライバシー・バイ・デザイン」論究ジュリスト 2016 年夏号 16-23 頁（2016）

新保史生「AI の利用と個人情報保護制度における課題」福田雅樹・林秀弥、成原慧 編著『AI がつなげる社会 AI ネットワーク時代の法・政策』（弘文堂、2017 年）

新保史生「ロボット・AI と法をめぐる国内の政策動向」人工知能 32 巻 5 号 665-671 頁（2017）

高西淳夫「ロボットとは-人造人間への夢」電学誌 118 巻 1 号 5-8 頁（1998）

田中絵麻「欧米における AI・ロボティクスにかかる合意形成の動向-欧州議会の報告と米国の非営利組織の開発原則から-」51 頁（AI ネットワーク社会推進会議開発原則分科会第 3 回配布資料、2017）

中崎尚「個人情報保護法改正とビジネスでの情報利活用への影響」Nextcom Vol. 24 14-25 頁（2015）

西尾修一、土井美和子「クラウドネットワークロボットに関する国際標準化動向」電子情報通信学会誌 Vol. 95 No.12 1080-1083 頁（2012）

萩田紀博「クラウドネットワークロボット関連技術の動向」電子情報通信学会誌 Vol. 95 No. 12 1052-1056 頁（2012）

馬場口登・西尾修一「ネットワークロボットのセンシングとプライバシー保護技術」電子情報通信学会誌 Vol. 91 No. 5 380-386 頁（2008）

長谷川能三「学天則の意匠と動作 -学天則復元にあたって-」大阪市立科学館研究報告 18 号（2008） 5-11 頁

林紘一郎「「個人データ保護」の法益と方法の再検討：実体論から関係論へ」情報通信学会誌 Vol. 31 No. 2 77-92 頁（2013）

東中竜一郎「対話システム研究の動向 -対話システムは次世代のインタフェースになるか-」情報処理 Vol. 57 No. 10 972-973 頁（2016）

東中竜一郎ほか「対話システムと感情」人工知能 31 巻 5 号 664-669 頁（2016）

東中竜一郎「対話システムと倫理」人工知能 31 巻 5 号 626-627 頁（2016）

藤井秀之「ビッグデータ時代における米国のデータ保護規制の動向」InfoCom Review 第 64 号 54-69 頁（2014）

松尾豊「人工知能と倫理」情報処理 Vol. 57 No. 10 985-987 頁（2016）

松尾豊ほか「人工知能と倫理」人工知能 31 巻 5 号 635-641 頁 (2016)
 村上陽一郎「ロボットの概念的変遷」日本ロボット学会誌 Vol. 16 No. 1 6-7 頁 (1998)
 村上陽亮「EU におけるデータ保護の動向と日本企業への影響」Nextcom Vo. 24 26-35 頁 (2015)
 森浩一「技術的特異点に関する議論を巡って人工知能研究者にできること」人工知能 32 巻 5 号 785-790 頁 (2017)
 山本龍彦「インターネット上の個人情報保護」松井茂記・鈴木秀美・山口いつ子編『インターネット法』(有斐閣、2015)
 山本龍彦「ビッグデータ社会とプロファイリング」論究ジュリスト 2016 年夏号 34-44 頁 (2016)
 渡辺智暁「異質な存在としての AI とその社会的受容」人工知能 32 巻 5 号 678-685 頁 (2017)

【海外文献】

Alan Westin, *PRIVACY AND FREEDOM* 487 (Atheneum Press, 1967)
 Ann Cavoukian, *Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D.*, 3-2 Identity in the Information Society 247-251 (2010)
 Brian Fung, *Trump has signed repeal of the FCC privacy rules. Here's what happens next.*, Washington Post (Apr. 4, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/04/04/trump-has-signed-repeal-of-the-fcc-privacy-rules-heres-what-happens-next/?utm_term=.e04a4d795137, Accessed at Jan. 11, 2018
 B.J. Fogg, *PERSUASIVE TECHNOLOGIES: USING COMPUTERS TO CHANGE WHAT WE THINK AND DO* 283 (Morgan Kauffman Publishers, 2003)
 Cacioppo, J. T., Berntson, G. G., Larsen, J. T., Poehlmann, K. M. and Ito, T. A., et al., *The psychophysiology of emotion*, 2 Handbook of Emotions 173-191 (2000)
 Dennett, D. C., *THE INTENTIONAL STANCE* 388 (MIT Press, 1989)
 DeVault, D., Artstein, R., Benn, G., Dey, T., Fast, E., Gainer, A., Georgila, K., Gratch, J., *Ethically Aligned Design version 1* 138 (2016),
http://standards.ieee.org/develop/indconn/ec/ead_v1.pdf, Accessed at Jan. 11, 2018
 Epley, N., Waytz, A., & Cacioppo, J.T., *On seeing Human: A three factor theory of anthropomorphism*, 114 Psychological Review 864-886 (2007)
 Executive Office of The President, *Big Data: Seizing Opportunities, Preserving Values* 85 (2014),
https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf, Accessed at Jan. 11, 2018
 Executive Office of The President, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights* 29 (2016),
https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf, Accessed at Jan. 11, 2018

Executive Office of the President, *Preparing For The Future of Artificial Intelligence* 58 (2016),

https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf, Accessed at Jan. 11, 2018

Federal Communications Commission, *FCC Adopts Privacy Rules to Give Broadband Consumers Increased Choice, Transparency and Security for Their Personal Data* (2016), https://apps.fcc.gov/edocs_public/attachmatch/DOC-341937A1.pdf, Accessed at Jan. 11, 2018

Floridi Luciano, *Four challenges for a theory of informational privacy*, 8-3 Ethics and Information Technology 109-119 (2006)

FTC, *Protecting Consumer Privacy in An Era of Rapid Change, Recommendations For Businesses and Policymakers* 112 (2012),

<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>, Accessed at Jan. 11, 2018

FTC, *Data Brokers: A Call For Transparency And Accountability* 110 (2014), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>, Accessed at Jan. 11, 2018.

FTC, *Internet of Things: Privacy & Security in A Connected World* 71 (2015), <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>, Accessed at Jan. 11, 2018

FTC, *Big Data: A Tool For Inclusion Or Exclusion? Understanding The Issues* 50 (2016), <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>, Accessed at Jan. 11, 2018

Gianmarco Veruggio and Fiorella Operto, *Roboethics: Social and Ethical Implications of Robotics* in SPRINGER HANDBOOK OF ROBOTICS, 1499-1524 (Bruno Siciliano and Oussama Khatib eds., 2008)

Hartholt, A. and Lhommet, M., et al., *SimSensei Kiosk: A virtual human interviewer for healthcare decision support*: Proc. AAMAS 1061-1068 (2014)

Ian Kerr, *Bots, Babes, and Californication of Commerce*, 1 University of Ottawa Law and Technology Journal 284-324 (2004)

Katz v. United States, 389 U.S. 347 (1967)

Pappas, D., Androutsopoulos, I. and Papageorgiou, H., *Anger detection in call center dialogues*, Proc. IEEE CogInfoCom, pp. 139-144 (2015)

Ray Kurzweil, *THE SINGULARITY IS NEAR: WHEN HUMANS TRANSCEND BIOLOGY* 652 (Viking, 2005)

Reeves, B., & Nass, C., *THE MEDIA EQUATION: HOW PEOPLE TREAT COMPUTERS, TELEVISION, AND NEW MEDIA LIKE REAL PEOPLE AND PLACES* 305 (Cambridge University Press. 1996)

Richard Mason, *Four Ethical Issues of the Information Age*, 10-1 Management Information Systems Quarterly 5-12 (1986)

Ryan Calo, *People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship*, 114-3 Penn State Law Review 809-805 (2009)

Ryan Calo, *Robots and Privacy*, in *ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS*, 187-202 (Patrick Lin et al. eds., MIT Press 2012)

Scholl, B. J., & Tremoulet, P. D., *Perceptual causality and animacy*, 4 Trends in Cognitive Science 299-309 (2000)

Stanford University, *Artificial Intelligence and Life in 2030* 52 (2016),

<https://ai100.stanford.edu/2016-report>, Accessed at Jan. 11, 2018

The European Parliament, *Civil Law Rules on Robotics; European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics* 23 (2015/2103(INL)),

<http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2017-0051&language=EN&ring=A8-2017-0005>, Accessed at Jan. 11, 2018

Ugo Pagallo, *Robotrust and legal responsibility*, 23-3-4 Knowledge, Technology & Policy 367-379 (2010)

Ugo Pagallo, *Robots in the cloud with privacy: A new threat to data protection ?* 29-5 Computer Law & Security Review 501-508 (2013)

Ugo Pagallo, *THE LAWS OF ROBOTS: CRIMES, CONTRACTS AND TORTS* 200 (2013)

U.S. v. Place, 462 U.S. 696 (1983)

Wayz, A., Cachioppo, J., & Epley, N., *Who sees human? The stability and importance of individual differences in anthropomorphism*: 5 Perspectives on Psychological Science 219-232 (2010)

White House, Administration Discussion Draft; Consumer Privacy Bill of Rights Act 24 (Feb.27, 2015)

White House, *Consumer Data Privacy in A Networked World: A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy* 62 (Feb. 23, 2012), <https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf>, Accessed at Jan. 11, 2018

Wu, C.-H., Lin, J.-C., and Wei, W.-L., *Survey on audiovisual emotion recognition: databases, features, and data fusion strategies*, 3 APSIPA Trans. on Signal and Information Processing e12 1-18 (2014)

Zeng, Z., Pantic, M., Roisman, G. I. and Huang, T. S., *A survey of affect recognition methods: Audio, visual, and spontaneous expressions*, 31-1 IEEE Trans. on Pattern Analysis and Machine Intelligence 39-58 (2009)