

2015年1月29日 全5頁

## ESG ニュース

## 「ロボット新戦略」にみるプライバシーとセキュリティ

環境調査部（主任研究員） 小黒 由貴子

## [要約]

- 2015年1月23日に公表された「ロボット新戦略」では、三つの柱「世界のロボットイノベーション拠点」、「世界一のロボット利活用社会」、「世界をリードするロボット新時代への戦略」と、五カ年のアクションプランなどが提示された。新市場として期待の大きいサービス分野、介護・医療分野でのロボット活用は、多様な環境（工場のようなロボットに最適化された環境ではない家庭・店舗・病院など）で多様な対象（ロボットに不慣れな老若男女）を相手とするなど、産業分野とは異なる課題がある。また、場合によっては機微な個人情報を扱うこと、ネットワーク化されたモノへのハッキングリスクのようなIoT（Internet of Things）の負の側面が拡大する恐れがあることなど、プライバシーとセキュリティに関する課題も少なくない。ロボット新戦略ではセキュリティや安全に関するルールづくりや標準化も不可欠とされているが、ガイドライン提示など、もう一歩踏み込んだ取り組みが望まれる。

## ロボット革命実現会議の「ロボット新戦略」が公開

6回にわたるロボット革命実現会議での検討を経て、2015年1月23日「ロボット新戦略」（以下、新戦略）が公表された<sup>1</sup>。序章では、欧米や中国の技術的な追い上げや、IT企業など従来のロボット産業とは異なる分野の企業の参入など、ロボット開発環境の変化を挙げている。これらの変化は、膨大なデータを活用したロボットの自律化、ロボット単体ではなくネットワーク化される「情報端末化」などのIoT（Internet of Things）社会到来を見越したものだが、こうした動きに日本が取り残されると、ロボット大国日本の地位が脅かされる恐れがあるとの危惧を示している。

そこで、日本のロボット戦略の三つの柱として、「世界のロボットイノベーション拠点ーロボット創出力の抜本的強化」、「世界一のロボット利活用社会ーショーケース（ロボットがある日常の実現）」、「世界をリードするロボット新時代への戦略」を掲げている（図表1）。

<sup>1</sup> 首相官邸 「[ロボット革命実現会議](#)」

図表1 ロボット新戦略の三つの柱

世界のロボットイノベーション拠点 ーロボット創出力の抜本的強化	産学官の連携やユーザーとメーカーのマッチング等の機会を増やしイノベーションを誘発させていく体制の構築や、人材育成、次世代技術開発、国際展開を見据えた規格化・標準化等を推進
世界一のロボット利活用社会 ーショーケース(ロボットがある日常の実現)	中堅・中小を含めたものづくり、サービス、介護・医療、インフラ・災害対応・建設、農業など幅広い分野で、真に使えるロボットを創り活かすために、ロボットの開発、導入を戦略的に進めるとともに、その前提となるロボットを活かすための環境整備を実施
世界をリードするロボット新時代への戦略	IoT社会の到来によるロボット新時代を見据えた戦略を構築するため「ロボットが相互に接続しデータを自律的に蓄積・活用することを前提としたビジネスを推進するためのルールや国際標準の獲得」

(出所) 首相官邸 ロボット革命実現会議 「ロボット新戦略」を基に大和総研作成

また、五カ年計画のアクションプランの分野横断的事項では「ものづくりでは勝ってもビジネスで負けるという懸念」を払しょくしようとしている(図表2)。

図表2 五カ年計画のアクションプランの分野横断的事項

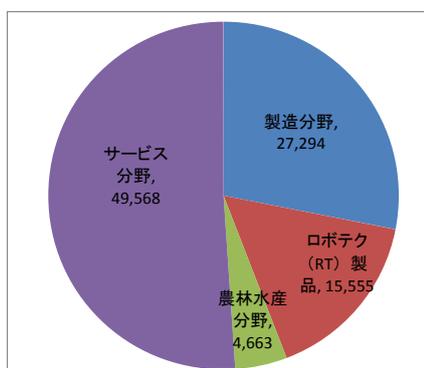
幅広いステークホルダーが協働するための核となる「ロボット革命イニシアティブ協議会 (Robot Revolution Initiative)」の設置
ロボットの要素技術の進化や人とロボットの協働の進展と共に、データ端末化、ネットワーク化、クラウドとの連携等が同時に起こる次世代に向けた技術開発
国際的な調和と国内普及の推進のため、いわゆる「ガラパゴス化」にならないよう国際標準化と国内標準化を同時に推進
社会的な課題解決のため実際のロボット活用を実験できる場(ロボット実証実験フィールド)の整備
ロボットだけでなくITなどの関連分野も合わせた横断的な知見を有する人材の育成
規制緩和とルール整備の両面の観点からバランスのとれた規制改革と、消費者保護の観点からロボットの安全性を確保するためのルール作り
ロボット大賞の拡充
ロボットオリンピック(仮称)の検討

(出所) 首相官邸 ロボット革命実現会議 「ロボット新戦略」を基に大和総研作成

## IoT（Internet of Things）社会の国際調和を目指すには

経済産業省では2035年には、日本のロボット市場の約半数をサービス分野が占めると推計している（図表3）。この推計が指すサービス分野には、介護・医療、物流、教育、アミューズメント、ホビー、家事支援、見守りなどが含まれており、新戦略で記載している4つの分野「ものづくり」「サービス」「介護・医療」「インフラ・災害対応・建設」のうち、「サービス」と「介護・医療」に相当する市場が大きいと考えることができよう。

図表3 日本のロボット産業の足元市場規模推計（2035年）



（出所）経済産業省「2012年 ロボット産業の市場動向」（平成25年7月）を基に大和総研作成

これまでもロボットが活躍している産業分野（新戦略では「ものづくり」、推計では「製造」）では、工場内などロボットが作動するのに適した環境が整備されている。また、ロボットを扱うのも訓練された人であることが多い。一方、インフラ・災害対応・建設分野などフィールド分野は、地形や気象など多様な環境の中で稼働しなければならない。サービス分野でも家庭・店舗・病院など多様な環境で稼働しなければならないうえに、ロボットがサービスを提供する相手がロボット操作に不慣れな一般人であるため、操作性と安全性の面でさらに条件が厳しくなるといえる。加えてサービス分野の場合は、ロボットが取得・活用することになるデータに個人情報が含まれることも想定され、中には病歴など機微なものも含まれる可能性がある。今でも監視カメラやスマートフォンのアプリなどによって、本人が気づかないうちに行動履歴などが収集されたり、ポイントカード利用などによってデータが統合されたりすることがある<sup>2</sup>が、社会の中にロボットが入っていくと、そうした機会が増加すると考えられる。

こうしたネットワーク化されたロボットの情報は、「ものづくりやサービス分野における新たな付加価値の創出源となるとともに、人々に様々な情報・コンテンツを届ける機能も担いエンターテインメントや日常のコミュニケーションまで大きく変革するキーデバイスとなることが

<sup>2</sup> 店舗での購買行動・Webの広告クリック・交通系ICカード利用など、無関係と思われるデータでも、組み合わせることで詳細な人物像や生活状況を浮かび上がらせることができるが、これをプロファイリングと呼ぶ。氏名がなくても個人が特定される、事実と違うプロフィールであっても本人がその情報の存在を知らないことから訂正できない、などの問題が起こる可能性がある。

できる」という期待がある一方、漏えいや乗っ取りによる心身や社会生活への脅威が高まることも考えられる。すでに、赤ちゃんを見守る Web カメラやコピー・スキャナなどの複合機のセキュリティの設定が不適切だった事例が出てきており<sup>3</sup>、IoT 社会の一端を担うロボットにもこのリスクがあるといえよう。介護用機器や自動車など、ヒトに直接接触れるロボットの場合、サイバー（データ）だけでなくリアル（身体）への脅威も考える必要がある。

この点は新戦略でも意識しており、「ロボット革命イニシアティブ協議会」の中で「ロボットが相互に連携しつつ、自律的にデータを蓄積し活用する主体となることを踏まえたロボットのセキュリティに関するルール整備についても検討を行う」としている。また、「ロボットが収集する個人情報の保護、あるいは、ロボットによる個人情報収集（撮影等）に関するルールの検討が不十分」であり、「不正プログラムの混入等によって、ロボットの誤作動や意図しないデータ流出が起きるセキュリティ上のリスクがある」などの課題も挙げている。このため「安全評価・リスク予見手法、試験方法の確立・標準化、ロボットが収集する情報の取り扱いに関するルール、セキュリティ技術等の検討・研究開発が必要」としている。ただし、消費者保護の観点から必要となる枠組みの整備として挙げているのは、消費生活用製品安全法、電気用品安全法のみである。

現在、個人情報保護法の改正が議論されているが、その改正案<sup>4</sup>では OECD プライバシーガイドライン<sup>5</sup>や EU 個人情報保護指令の十分性（個人データの移転が許容されるための基準）を満たさないため、国際的に受容されないような情報の取り扱いになるのではないかと、つまり日本企業が海外で（あるいは海外と）、ビジネスをすることができなくなるのではないかと、との指摘がある。情報の自由な流通に積極的とみられる米国ではあるが、連邦取引委員会法第 5 条の「不公正若しくは欺瞞的な行為又は慣行」に違反したとして、多額の制裁金が科された例がある。つまり、この法は、民間事業者が自身のプライバシーポリシーに沿った情報の取り扱いをすることを担保する働きをしているのである<sup>6</sup>。最近では連邦取引委員会（FTC）の委員長が IoT への期待と共に「IoT は重要なプライバシーやセキュリティの問題を引き起こす懸念もある」ため、IoT に取り組む企業は security by design（デザインの段階からセキュリティを作りこむ）などを行って消費者のプライバシーとセキュリティを強化すべきという講演<sup>7</sup>を行っている。また、学生について収集したデータは教育目的に無関係な第三者に販売しないなどの法案（Student

<sup>3</sup> 独立行政法人情報処理推進機構 「2014 年版 10 大脅威」（2014 年 3 月）

<sup>4</sup> 利用目的の変更（目的外利用）について、現在の「事前同意が必要（オプトイン）」から、個人情報を取得する際に本人に利用目的を変更することがある旨を通知、または公表した場合は「（事後の）オプトアウトで変更できる」になっている。また、変更前に取得したデータも変更後の利用目的に使える場合があるとの事務局のコメントも出ている。

<sup>5</sup> 一般財団法人日本情報経済社会推進協会（JIPDEC） 「OECD プライバシーガイドライン」

このガイドラインに法的拘束力はないが、OECD 加盟国に対する指針であり、現在の個人情報保護法は当時の OECD プライバシーガイドラインの影響を受けているとされている（一般財団法人日本情報経済社会推進協会（JIPDEC）一橋大学名誉教授 堀部政男 「1980 年 OECD プライバシーガイドラインと日本」）。

<sup>6</sup> 情報通信政策研究所 情報通信政策レビュー第 8 号（平成 26 年 4 月 3 日刊行） 石井 夏生利『『プライバシー外交』のためのプライバシー』

<sup>7</sup> techcrunch（2015 年 1 月 13 日） 「IoT 企業はプライバシーとセキュリティーに最優先で取り組み—FTC 委員長が CES 講演で強く警告」（2015 年 1 月 29 日閲覧）、講演の原文は“Privacy and the IoT: Navigating Policy Issues”（FTC Chairwoman Edith Ramirez）

Digital Privacy Act) の策定をオバマ大統領が求める<sup>8</sup>など、消費者保護を重視する考え方が明示化されてきている。ロボットに不適切な設定をしないように我々自身も「ロボットとの協働・共生に欠かせないロボットに対するリテラシー」を身に付けなければならないが、適切な規制があることで安心してサービスを利用することができることもある。IoT やロボット関連技術の変化は早く、思いがけない使い方も出てくるため、当面はガイドラインでの指針提示といった方法になるかもしれないが、ロボット大国日本の地位向上のためにも、セキュリティやプライバシーに関する、もう一步踏み込んだ取り組みが望まれる。

---

<sup>8</sup> The White House (January 12, 2015) “FACT SHEET: Safeguarding American Consumers & Families” (2015年1月28日閲覧)