

ロボット法をめぐる法領域別課題の鳥瞰

慶應義塾大学総合政策学部教授

新保 史生

SHIMPO Fumio

- I はじめに
- II ロボット法研究の背景
- III 法領域別の課題概観
- IV 憲法
- V 行政法
- VI 民事法
- VII 刑事法
- VIII ロボット・ロー・バイ・デザイン
- IX 「AI開発ガイドライン」
- X 安全保護及びセキュリティ確保の原則

I はじめに

AI（人工知能）の進化は急激に進みつつある。AIが搭載された家電製品やロボット、自動走行システムによる自動運転車¹⁾の普及に伴う法的課題の検討とともに、ロボットやAIの利用に伴う新たな情報セキュリティ対策を検討しなければ、インターネットの発展過程において生じた問題と同様の問題が生ずる可能性はないか。その脅威は、インターネットのようにバーチャルな空間における問題にとどまらず、現実の脅威として飛躍的に脅威の度合いが高まるおそれはないか。

AIや自律型ロボットの脅威として、AIが暴走して人間に脅威を与えることが指摘されることが

多い。映画で描かれる脅威はまさにそれである。AIが自己を認識し自発的に防御行動をとるまで進化するまでには、まだ相当な時間を要すると考えられることから、そのような脅威が直ちに現実となる可能性は低いと考えられる。

一方、今そこにある危機は、人間に脅威を与えるように人間がAIを用いることにある。敵と味方を自律的に認識して対象を攻撃をするようなAIを搭載した兵器の開発などは着々と進んでいる。

「ロボット法」として、まず考えなければならないのは、新たに人間の脅威となるおそれがある技術について、人間の脅威とならないように研究開発を制限するためのルールを考えるのではなく、新たな技術が人間に脅威を及ぼすことがないように、それを利用する人間をどのように規律すべきかを考えることにある。

II ロボット法研究の背景

1 ロボット法の現状

ロボット法については、日本国内では文献データベースで先行研究を調査しても、「ロボット法」という用語を冠して論じられている論文は、本稿執筆時点で10本に満たない。「ロボロー (Robo-

1) ロボット法分野における論文として最も多いトピックは自動運転をめぐる問題に関するものである。多くの論考によって法的課題の抽出が行われ検討事項の整理がなされつつある。法的課題の整理を試みる論考として、佐藤智晶「人工知能と法：自動運転技術の利用と法的課題、特に製造物責任に着目して」青山法学論集 57 (2015-12) PP.27-42、中山幸二「自動運転をめぐる法的課題 (特集 自動運転)」自動車技術 69 (2015-12) PP.39-45、中山幸二「自動運転の進展と交通事故の賠償責任」共済と保険 58 (2016) PP.4-11、新保史生「自動走行システムによる自動運転に係る制度的課題をめぐる検討状況」高速

道路と自動車 59(6) (2016) PP.5-8、戸嶋浩二、佐藤典仁「NBL SQUARE 米国における自動運転車に関する新たな指針」NBL (2016) PP.44-50、戸嶋浩二「自動走行車 (自動運転) の実現に向けた法制度の現状と課題」NBL1073 (2016) PP.28-35、高橋郁夫「自動運転の法的課題と今後の方向性 (車載テクノロジー最前線)」車載テクノロジー 4 (2016) PP.75-79、「特集 自動運転と民事責任」ジュリスト 1501 (2017) PP.23-55、岡部雅人「自動運転車による事故と刑事責任：日本の刑法学の視点から」愛媛法学会雑誌 43 (2017) PP.1-20。

Law)」関連の多くの書籍や論文が公刊されている米国やEUの研究動向からするとかなり後塵を拝している。

2015年10月11日に、「ロボット法学会設立準備研究会」を科学未来館において開催した際には、「ロボット法」という新法を制定してロボット関連技術の規制を行うことが目的なのか、ロボット工学をはじめとする従来からの研究技術開発に係る長年の研究の蓄積や安全基準などの技術標準で様々な問題に対応できるにもかかわらず、ロボットに関する技術的知見に乏しい法学研究者が検討などできるのかといった多くの批判が寄せられた。その後も、「ロボット法」という法整備を行うことがロボット法の目的であるという短絡的な論調を改善することができないまま現在に至っていることは残念でならない。

2 ロボット法と産業政策

ロボット法の必要性は産業政策とも密接に関わっており、「第4次産業革命」は、社会や法制度の大きな変革を伴うものであることを認識する必要がある。

我が国は、産業用ロボットの市場占有率が高いが、「ロボット産業市場動向調査結果²⁾」によると、産業用ロボットの世界市場は、金額ベースで直近5年間に約60%成長。2011年の市場規模は約6628億円³⁾であり、うち日本企業のシェアは50.2%。なお、電子部品実装機を含む広義の世界市場は約10428億円で、日本企業のシェアは57.3%。日本市場は直近5年間に台数ベースで約25%縮小したものの世界最大市場の地位を維持。ただし、中国市場は5年間で約4倍に拡大し、台数ベースで日本市場に迫る規模に成長となっている。

日本は今後もロボット大国の地位を維持できるのであろうか。例えば、生活支援型ロボットや身

の回りに普及しつつあるロボットについて、累計1000万台を超えるヒット商品になった掃除ロボットは、米iRobot社が開発。ソフトバンクのパーソナルロボット「Pepper（ペッパー）」も、ソフトバンク傘下であるフランスのAldebaran Robotics社が開発し、製造は鴻海精密工業。首相官邸に落下したり、姫路城に衝突したりしたドローンは、DJI（中国広東省深セン市のメーカー）の「ファントム」。原発事故で投入されたのは、米国アイロボット社が無償提供した、爆発物処理やSWATで使用されている2台の軍事用ロボット「バックボット」など、いずれも国産ロボットではない。

グーグルが自動走行システムの開発を進めている理由は、自動走行に係るOS（オペレーティング・システム）とプラットフォームの獲得を目指しているからにほかならない。スマートフォン同様に、自動車を構成する部品は日本製であっても、その設計や車両を制御するシステムは、国外かつ自動車産業とは無関係の事業者が将来的に覇権を握る可能性がないとは言い切れない⁴⁾。

技術的課題を克服して技術開発が市販レベルまで到達したとき、社会制度や法基盤、法的責任やリスク、社会的な受容性などを総合的に検討しなければ、新たな技術の普及を阻害するおそれもある。

III 法領域別の課題概観

AIや自律型ロボットをめぐる法的課題は、個別の問題が散在的に検討されつつある。しかし、ロボット法が体系的な学問領域として認知されるには至っていないため、まずは、どのような課題を検討すべきか全体像を把握する必要がある。そこで、法領域別の法的課題について、現時点における国内外の先行研究を調査し具体的に議論され

2) 経済産業省「ロボット産業市場動向調査結果：2012年ロボット産業の市場動向」（平成25年7月18日）。

3) 直近の調査結果、日本ロボット工業会調査・統計部会「ロボット統計受注・生産・出荷実績2016（平成28）年10～12月期及び年間【会員ベース】について」によると、同会の正会員及び賛助会員対象企業の33社のうち、回答企業33社による実績によれば、受注・生産の台数及びその額はいずれも過

去最高値を記録し7000億円を超える見込みとなっている。

4) IoTの普及をめぐる問題と今後のビジネスモデルの変化については、桑津浩太郎「IoTの普及にともなう新たなビジネスモデル、社会への影響（特集 暗号通貨の諸問題／IoTの法的課題・個人情報保護：第40回法とコンピュータ学会研究会報告）」法とコンピュータ34（2016）PP.9-15に詳しい。

ている課題の整理を試みてきたが、以下のような問題が現時点で議論が必要であることを確認するに至っている⁵⁾。

憲法の領域では、①安全保障（軍事利用やテロ対策、自律型兵器、ドローン）、②プライバシー、肖像、個人情報保護（ビッグデータ解析）、③法の下の平等、④表現の自由、⑤適正手続、⑥勤労（雇用環境の変化、雇用管理と差別）。

行政法の領域では、①ロボット行政（ロボット管理政策）、②自動走行車の公道走行、無人航空機（ドローン）規制、ロボットの制御と電波監視、③その他の行政の規制個別領域における利用と管理。

民事法の領域では、①不法行為（製造物責任、自動走行車の事故と責任、人工知能の悪用や暴走）、②消費者保護、③契約、④知的財産（AIが作成した著作物の著作権、特許）、⑤医療・介護（手術、医療分野における利用、ヘルスケア、医療過誤）。

刑事法の領域では、①犯罪（AIやロボットを利用した犯罪）、②法執行（犯罪捜査におけるAIプロファイリングの活用、犯罪予知AIを用いた犯罪予防など）。

国際法の領域では、①ドローンの利用をめぐるルール、②国際人道法とロボットなどがある。

法領域毎の課題については、2016年4月から2017年3月まで「時の法令」に掲載した拙稿を加除修正し考察する。

IV 憲法

憲法問題としては、①軍事利用やテロ対策との関係における議論が国外では盛んである。米国の軍用ドローン（プレデターなど）はアフガニスタンやイラクで既に実戦投入されている。米国内から遠隔操縦で展開できるため攻撃側の人的被害なく戦闘が可能というメリットゆえに積極的に活用されている。しかし、戦争とテロ対策の境界、軍事目標と非戦闘員の区別、戦闘地域外から遠隔で攻撃することの法的妥当性などの観点から問題が指摘されている。将来的には、顔識別機能により攻撃対象者を識別し自動的に攻撃をする兵器の実戦配備も検討されており、自律型兵器は可及的速や

かに国際的に確固たる規制が必要であるとの意見も示されるなど、致死性自律型ロボット（Lethal Autonomous Robotics: LARs）又は致死性武器体系（Lethal Autonomous Weapons System: LAWS）について、特定通常兵器使用禁止制限条約（CCW）の検討の場で議論がなされている。

②プライバシー関係の問題としては、ロボットに搭載されたカメラやマイクは周囲の状況を記録し、AIのディープラーニングは学習対象となる大量のデータを取得している。撮影された画像は個人情報であるとともに、肖像権をはじめとする個人の人格的利益保護の対象となる情報である。大量に取得されたデータはビッグデータとして解析され、個人のプライバシーが明らかになるおそれもある。

③法の下の平等をめぐる問題として、例えば、ロボコップは人種差別をしないのかという議論がある。デジタル技術は技術的に中立性が保たれているため、警察官による差別的な対応とは無縁のように思える。しかし、プログラムが政策的意図に左右されるおそれや、肌の色によってエラーが生じるなど機械的なエラーにより意図しない差別的利用が生ずることへの危険性がある。

④表現の自由については、AIが話した差別的発言についても表現の自由の保障が及ぶのか。

⑤適正手続としては、2016年7月9日に、米テキサス州ダラスで警官による射殺事件への抗議デモ中に発生した警官に対する銃撃事件の被疑者が、爆弾を搭載したロボットにより爆殺された事件が今後のロボットを用いた法執行の課題を浮き彫りにしている。超小型ロボットを用いた捜査やロボットを用いた法執行と適正手続の問題、犯罪捜査・予防でAIを利用した予測の妥当性を誰が評価するのかという問題などがある。詳細は刑事法分野における問題として後述する。

⑥勤労については、将来的にAIの進化によって雇用環境の劇的な変化が見込まれている。AIが奪う職業のリストなども議論され、雇用管理と差別の問題が生ずることも予想される。産業革命期に発生したラッドライト運動（機械破壊運動）が、

5) 新保史生「ロボット法学の幕開け（特集 IoT とイノベ

ーション）」Nextcom 27 (2016) P.29.

ロボット革命時代の到来によって再び起きることも空想とは言えないかもしれない。

V 行政法

ロボットと行政の関わりは、無人航空機（ドローン）規制などのロボット管理のための施策、自動運転車の公道走行のための環境整備、ロボット制御や標準化、遠隔操作のための電波監理、情報通信やコミュニケーション、医療・介護、食品加工、農業、金融（フィンテック⁶⁾、労働・労務管理、物流、エネルギー、災害対応、建設・インフラ管理など実に多岐に亘る。そこで、①ロボット共生社会に向けた制度や施策検討の在り方、②行政の効率化や法執行における AI やロボットの利用の二つに分けて考えてみたい。

1 ロボット共生社会に向けた制度や施策検討の在り方

既に講じられている具体的な施策としては、2015年にドローンに代表される無人航空機規制を目的に航空法が改正され同年12月10日に施行されている。さらに、国会議事堂、官邸や原発など国の重要な施設周辺での小型無人機等の飛行禁止地域を定める「小型無人機等飛行禁止法」が2016年3月18日に公布されている。

また、2020年の東京オリンピック開催に向けて、自動運転車の公道走行の実現を目指し、国土交通省・経済産業省が「自動走行ビジネス検討会報告書」を2016年3月23日に公表している。警察庁の「自動走行の制度的課題等に関する調査検討委員会」も2016年5月に「自動走行システムに関する公道実証実験のためのガイドライン」を公表している⁷⁾。

2015年2月に日本経済再生本部決定として公表された「ロボット新戦略」では、政府のロボット戦略が提示されるとともに、その実現のための

「規制・制度改革に係る工程表」として検討が必要な関連法令が示されている。しかし、工程表では、次の六つの法令について見直しの必要性が示されているに過ぎない。

①電波法（遠隔操作や無人駆動ロボットで使用する電波の取扱い）、②医薬品医療機器等法（ロボット技術の高度化に伴う医療機器としての承認・認証に係る期間・手続）、③道路交通法／道路運送車両法（搭乗型移動支援ロボットの公道走行）、④無人飛行型ロボット関係法令（航空法等）、⑤高圧ガス保安法（目視などの人間を前提とした点検作業におけるロボット活用に関するルール）、⑥消費生活用製品安全法／電気用品安全法（自律性や遠隔操作性を有する生活関連次世代ロボットの消費者安全確保、技術基準の在り方、製造事業者などの責任の範囲）。

当該戦略では国際標準の獲得とともに、規制緩和とルール整備の両面からの規制・制度改革の推進の必要性が示されているが、あくまで現行法の枠組みにおける規制緩和の提示にとどまり、新たな法規制の枠組みや方向性などは示されていない。そこで、今後の行政によるロボット関連施策立案の在り方について五つの意見を述べておきたい。

①社会実装に向けた包括的かつ体系的な課題の把握と整理・検討が必要である。例えば、AIの普及で社会的にどのような影響が生ずるのか、自律型ロボットが暴走した時に誰がどのように責任を取るのか、技術、機能、法的・倫理的・社会的課題（いわゆる ELSI）など総合的な視点からの検討とともに、将来的な課題やリスクへの備えも念頭に社会・制度の変化・変革に対応するための施策の検討が求められている⁸⁾。②政策や施策立案の在り方については、各行政領域によるパッチワーク的な検討ではなく、ロボットやAIの利用促進に向けた方針や政策（戦略）の統一を図る一方で、画一化しない多様かつ柔軟な議論のため多元的かつ多面的な検討（マルチステークホルダー・プロセス）が重要である。また、行政主導による検討

6) フィンテック等の活用に伴う法的課題についての検討は、三部裕幸、落合孝文「金融機関のAI活用に関連する法的問題点：現状では、個人情報保護や知的財産権の保護などが論点に（特集 AI が導く新たな金融）」金融財政事情 67（2016）PP.32-35。

7) 大野敬「『自動運転』に関する警察の検討の状況及び今

後に向けた取組について」警察学論集 69（2016）PP.139-164。

8) 人工知能学会における検討については、松尾豊、西田豊明、堀浩一、武田英明、長谷敏司、塩野誠、服部宏充、江間有沙、長倉克枝「人工知能と倫理（特集 人工知能学会・情報処理学会共同企画人工知能とは何か?）」人工知能 31（2016）PP.635-641。

における課題として、③継続的な検討が可能な体制整備が必須である。行政による検討の重複や競合を避け、担当者の交代による施策検討の不連続や断絶が生じないように、産学民官の参画による継続的な検討体制の整備が不可欠である。④規制の不存在に伴う萎縮効果の解消・ガラパゴス化しない配慮も必要である。自動運転車の公道走行を禁止する法令がないにも関わらず、公道走行のルールがないために研究開発に躊躇したり普及が遅れてはならない。最後に、⑤国際協調ではなく国際的イニシアティブの獲得に向けた検討を目指すべきである。ロボット大国の地位を維持するためには、安易に協調して情報やノウハウが盗まれることを避けるとともに、諸外国の取り組みに先駆けて新たな視点からの検討を行う際には、日本の法文化や法令遵守意識と国外の状況の違いを認識した上での施策検討が必要である。

国の新たな施策や戦略をとりまとめる際に、法的観点から検討が必要な事項は多い。しかしながら、現行法の枠組みにおける規制緩和としての課題の提示にとどまることが多々見受けられる。それを防ぐために、ワシントン大学のライアン・ケイロ (Ryan Calo) は、議会及び FAA によるドローンの利用と飛行制限、高速証券取引アルゴリズム (市場ロボット)、FDA によるロボット手術の認可、NHTSA による自動走行への取り組みなど、行政による個別の検討ではなく、「連邦ロボット委員会 (Federal Robotics Commission)⁹⁾」の必要性を提唱している。

2 行政の効率化や法執行における AI やロボットの利用

行政の効率化や法執行において、将来的には AI やロボットの活用が見込まれている。一方、活用を誤ると真の意味での「ビッグブラザー」が実現してしまうおそれがある。

準法律行為の行政行為など定型的な行政事務は、ロボットの活用により自動化や効率化にとどまらず公務員の業務を代替することも可能になるであ

ろう。AI による問い合わせへの応答ができれば、反復応答で対応可能な相談業務から解放される。窓口の担当者が融通の利かないロボットだと、行政対象暴力に屈する心配もなくなるかもしれない。公の施設や公物の維持管理負担の軽減や的確なメンテナンスのためのロボット活用への期待も高い。各行政機関での AI の活用の可能性については、行政における AI の活用例の想定が示されている報告書¹⁰⁾ が興味深い。

行政が保有する膨大な量の情報の活用を進める「オープンデータ」の取り組みに AI を活用することで、行政情報の飛躍的な活用促進も期待できる。行政処分などの公平性確保のために過去の事例の網羅的・悉皆的な把握や検討でも有用であろう。AI による議事録の自動生成と分析が可能になれば、膨大な数の会議の運営負担が軽減されるとともに、単に記録として保存する会議録の作成ではなく、大量の公文書を分析して新たな施策立案に資する情報として生かすこともできる。現に、2016年5月から検討が始まった内閣府の「人工知能と人間社会に関する懇談会」では、AI による議事録分析を行い、会議での議論の傾向や内容分析を行う試みが行われている。分かりやすい議事録は行政の透明化にも資する。

住民にとっても、行政情報の収集や分析に AI を活用することで、情報公開請求により開示された公文書の分析や、住民監査請求の対象となる違法又は不当な財務会計上の行為を発見しやすくなる可能性もある。ただし、情報公開との関係においては、ディープラーニングにより取得した情報や政策立案に係る意思決定の根拠となった情報など、AI を用いて取得・分析がなされた意思形成に関する情報はどの程度開示が可能であろうか。

警察官の安全確保や公平な法執行のためのロボット導入への期待もある。黒人差別的な法執行が大きな問題となっている米国では、差別的な取扱いをしない技術的中立なロボットの議論がなされている。

しかし、ロボットによる法執行に伴う損害が生

9) Ryan Calo, The case for a federal robotics commission, Monday, September 15, 2014 <<https://www.brookings.edu/research/the-case-for-a-federal-robotics-commission/>>.

10) 行政情報システム研究所「人工知能技術の行政における活用に関する調査研究」報告書 (2016年6月10日)。

じた場合、国家賠償においてロボットの行為は公権力の行使にあたるのか。

環境訴訟においては原告適格の問題が生じたが、ロボットの適正な利用を争い、原告適格が問題となることはないだろうか。

行政の効率化や法執行における利用を目的として、ロボットやAIを導入する場合、効率化のための利用（メリット）だけでなく、利用に伴う行政法上の問題（デメリット）を精査し慎重に検討しなければならない。政府によるデータの集積に伴う管理国家への懸念が、ジョージ・オーウェルの『1984』で示された独裁者「ビッグブラザー」であるが、現在でも、街頭の防犯カメラ画像を一元管理し顔識別技術によりリアルタイムで瞬時に分析したり、ネットワーク上の情報を解析し国民の動静を常時監視することは可能である。しかし、AIが監視結果から犯罪予防・制止や保護・避難などの措置を自律的に判断し、ロボットが即時執行する将来はあまりにも危険だ。「行政における法治ロボットの原則」を定め、行政作用におけるロボットやAIの導入範囲を決めなければ、リアル・ビッグブラザーが完成するおそれがある。

人工公物としての行政ロボットの利用に伴い損害が生じた場合の問責のあり方などについても検討が必要である。ロボット自体の欠陥による被害が生じた場合は公の営造物の設置又は管理の瑕疵として国賠の適用があると考えられる。一方、行政ロボットの悪用により生じた問題については、営造物の管理責任ではなく安全確保義務の懈怠にあたる判断することになるのだろうか。

行政組織との関係においては、専門的見地からAIが行政庁の意思決定に関与する場合、会議体ではなくAIそのものが「諮問機関」として位置づけられる可能性はあるだろうか。ロボットが行政目的達成のために即時執行を行う場合、ロボット単独で「執行機関」としての機能を有するといえるのか。遠隔操作ロボットではなく、AIが搭載された自律ロボットが行政庁の命を待たずに自律的に判断し実力行使を行うことも、将来的に認められる可能性はあるだろうか。攻撃目標を自動追尾する致死性自律型ロボットが、軍事利用ではなく法執行で用いられる可能性もある。

VI 民事法

ロボットやAIの利用・普及に伴い民事法の分野において検討すべき事項は実に多岐にわたる。民法とその特別法（製造物責任法や著作権法）など実体法における問題と、訴訟手続におけるAIの活用など手続法の両面から検討が必要になると考えられる。

自動運転車の事故、AIの機械学習と個人のプライバシー保護など人格的利益の保護、AIが作成した知的財産の保護、自律ロボットの悪用や暴走に伴う損害の賠償、家族の一員としてのロボットの存在など、民事法領域における問題は枚挙にいとまがない。

1 AIと権利能力

将来的には、人間と同様に知識を身につける汎用型人工知能の高度化に伴い、その「知能（AI）」に権利能力を認めるか否か、自然人の意思能力、行為能力と同様の問題を検討すべきか、そもそも「人」と「物」とは何かといった民法の基本原則の見直しを迫られるような問題の検討が必要になる可能性がある。

権利能力については、AIの自律により、権利・義務の主体となり得る地位ないし資格としての新たな「法的人格」を将来的に認めるべきか考えなければならないかもしれない。

例えば、契約法では、契約を結ぶ権利主体（自然人・法人）と権利の客体（目的物）の区別を前提としている。AIが搭載されたロボットを例に考えると、有体物としてのロボットは動産であることから、契約の目的物であって権利の主体になることはできない。つまり、ロボットが契約を結ぶ権利主体になることは想定していないが、自律ロボットが権利主体であるとの外観が存在するような場面が今後出現すると想定される。

そうなると、法的な権利主体として「人工的」に設けられた人である「法人」のように、自然人たる人間が人工的に作り出した人工知能を「AI人」とでも表記するなどして、民法における「人」である自然人と法人に加えて、新たな法人格（権利能力）の法的な位置づけを認めるべきで

あろうか。

八幡製鉄事件では、法人の人権享有主体性が問題となったが、AI人の権利主体性が裁判で争われ、性質上可能な限りAI人に認められる権利は自然人と同様に扱うべきであるとの判断が示される時代が来るかもしれない。

意思能力については、現時点でAIは常識を理解するまでには至っていない。よって、権利能力が認められたとしても事理弁識能力を有するAI人が登場するまでには相当の時間を要すると思われる。意思無能力者たるAI人による法律行為は無効であるとの判断を脱するには、人工知能が人間の能力を超えるとされる「技術的特異点(シンギュラリティ)」を待たなければならない。

行為能力については、AIの進化を制限行為能力者の類型に当てはめて考えてみたい。明治学院大学の加賀山茂教授との個人的意見交換において、自動運転のレベルごとに民法の行為能力を当てはめて考えることができるのではないかと示唆を受けた。具体的には、レベル0(自動化なし)の状態は、自動車は自らの判断で一切走行することができないため成年後見人としての運転者が必要。レベル1(特定機能の自動化)は、運転の補助機能の一部自動化で運転者は補佐人。レベル2(複合機能の自動化)はステアリングとアクセルペダルを自動走行システムが制御し走行可能であるため運転者は補助人。レベル3(準自動走行)では、すべての運転操作機能が自動化されているが、自動走行を維持できない状況を判断して運転者が自ら運転操作を行うため、自動走行システムを掌るAIは未成年。レベル4(完全自動走行)は運転操作から周辺のモニタリング機能のすべてが自動化されるため、自動運転を行うAIは成人。

汎用型人工知能が人間と同様の能力を有し判断ができる段階に達すると、AI人を相手に契約を交わすことはあり得るであろう。相手方が自然人であると思って契約をしたところAI人であったり、未熟なAIと契約を交わした時に、未成年者同様に制限行為能力者として法定代理人の同意が

ない契約は無効となるのか。AIが自らを自然人の成人であると偽って取引をした場合、未成年者同様に詐術として扱ってよいか。

人間の常識が通じないにも関わらず、人間の常識を超える存在にまで進化し、人間の能力を超えるAIが日常的に用いられるようになったとき、人間ではない新たな「人」にどのように向き合うべきか、民法の権利能力を例に考えてみたが、筆者の考察は試行錯誤なのか単なる錯誤なのか今後の評価を待ちたい。

2 財産法に係る問題

財産法の分野では、そもそも財産の管理をロボットやAIに委ねる時代が到来している。フィンテック、AIを活用した投資判断なども用いられ、個人資産の管理や運用をAIに委ねるサービスも提供されている。

自動運転車の事故時の責任として、いわゆるトロッコ問題¹¹⁾が議論されることが多い。回避が困難な事故の発生に直面したとき、衝突の対象物や対象者を選択する際に、歩行者の人数や年齢・性別などの属性に基づく評価関数や対象物によって、危険回避の優先順位を判断又は決定することができるのかといった問題である。

最終的に誰が責任を負うのか決められない究極の選択を、法的責任(選択)の問題として明確な線引きを定めることは困難であるとともに、倫理的にも様々な思考実験が行われてきたものの誰もが納得できる判断を示すには至っていない。この問題が解決されない限り、完全自動運転車(レベル0~4に自動走行レベルを分類した場合のレベル4)の公道走行を実現することができないといった見解も見受けられる。しかし、民事法的にはレベル1~3では運転者の位置づけを議論した上で、運転者、運行供用者、製造者などの事故時の責任論について議論を行い保険の在り方を検討し、レベル4では製造者の責任の在り方を考えるしかないのではないだろうか。

一方、情報であるソフトウェア自体は有体物で

11) 人間の判断でも選択の決定に躊躇せざるを得ない問題を、AIの判断過程で結論を求めること自体理不尽な要求であるとも思えるが、平野晋「『ロボット法』と自動運転の『派生

型トロッコ問題』: 主要論点の整理と、AIネットワークシステム『研究開発8原則』NBL1083(2016)PP.29-37は、トロッコ問題の捉え方について示唆を与えている。

はないため、製造物責任の対象とはならない。AIが搭載された自動運転車やロボットであれば、有体物としてのロボットに組み込まれた動産として製造物に該当するため、他人に損害を与えた場合は製造者等に製造物責任を追及することが可能である。しかし、自動走行システムの搭載地図の誤りによって事故が発生した場合、情報の誤りそのものに製造物責任を問うことはできない。

事故時の責任の所在を明らかにするためには、画像の記録（保存）が不可欠である。AIの機械学習も膨大な量の情報を集めることが必要である。これらの情報には、膨大な量の個人に関する情報も含まれ、個人の人格的利益保護のための取り組みが必要である。

ビッグデータから抽出した個人情報进行分析するプロファイリングにより、趣味嗜好に合わせた広告やお勧め商品の提示など行動ターゲティングが既に用いられている。それに加え、商取引でAIを活用して特定の方法で商品を勧めることにより高確率で購入をさせることも可能になる。個人の自己決定に大きな影響を及ぼし、本人の意思表示をも操る究極のAI関係取引においては、「AI消費者契約法（架空の法令名）」により、高度なAIプロファイリング取引では消費者が申込みを行う前に、AIを用いた取引であることを確認する措置を事業者側が講じないと、要素の錯誤にあたるようなAIに唆された申込みの意思表示は無効にするといった規制も将来的には必要になるかもしれない。

AIが自律的に作成した生成物は、現行の知的財産制度では権利の対象にならない。AIがデータを分析して生成した「学習済みモデル」の保護も課題となっている。人間の創作物のように見えるコンテンツがAIによって作成可能になりつつあり、いわゆる「準創作物」の保護の在り方について検討が必要である。

3 家族法に係る問題

家族法についても、ヒューマノイドを養子にしたいとか結婚したいと真剣に考える人も出てくるであろうし、優しく介護をしてくれた自律ロボットに財産を相続させたいと思う人も出てくるかもしれない。精巧なヒューマノイドを家族の一員の

ような錯覚にとらわれ家族同然に扱う人も出てくるであろう。あたかも人間のように見える「物としてのロボット」の法的地位は、動物に準ずるのか、新たな奴隷なのか。ロボットの虐待は単なる動産への侵害ではあるものの、動物愛護的な考えも必要であろうか。動産としてのロボットに対する損壊や毀損の責任だけを論ずることで法的には問題はないにせよ、人と類似したヒューマノイドを虐待している様子を客観的に目撃した場合、単なる物の損壊と心情的に割り切ることができるであろうか。

「私人間」の意味が、アシモフの「われはロボット（I Robot）」にいう「私（AI又はロボット）」と「人（自然人又は法人）」の「間」の問題として議論される日が来るかもしれない。

Ⅶ 刑事法

ロボットやAIの利用・普及に伴い刑事法分野で検討すべき問題は、それらを利用した新たな犯罪の類型や構成要件などに関する「刑事実体法」に係る問題、犯罪捜査手法や適正手続の保障に関する「刑事手続法」をめぐる問題に分けて検討が必要となる。

1 刑事実体法に係る問題

殺人ロボットの利用すらもはやSFの世界の問題ではない。戦場では既に攻撃用ドローンが投入されており、自律型致死兵器システムの規制も特定通常兵器使用禁止制限条約締結国会議（CCW）で議論されている。これらの兵器が、テロや犯罪の手段として利用されるのも時間の問題である。

刑事実体法に係る問題として、今後想定されるロボット・AI関係犯罪の類型を①AI・ロボット利用型犯罪と②同関連型犯罪に分けて考えてみたい。

①は、AIやロボットの利用自体は違法・不正ではないが、その利用結果が犯罪・不正行為を構成する場合。そのようなロボットの製造こそ違法ではないが、麻薬取引や強盗などの違法行為においてロボットに犯罪を実行させる場合がこれにあたる。AIを利用した犯罪としては、電話の相手方が人間なのかAIなのか判別がつかない状況が

将来的に見込まれるが、ビッグデータを解析して詳細な個人情報を把握した上で、ディープラーニングを用いた分析結果により対象者に応じて精巧に親族を装った振り込め詐欺の電話を掛けるAIが出現したとき、機械学習とパターン認識の精度が向上することで、現在以上に詐欺の被害が深刻になるおそれがある。AIによる高度なマネーロンダリング、TayのようなAIの暴走による名誉毀損や風説の流布も問題になるであろう。機械学習で収集対象となった著作物は複製権侵害にあたらないのか、全裸のヒューマノイドロボットの陳列はわいせつ物の公然陳列か公然わいせつなのかも議論が必要である。

ドローンを利用した犯罪も、衣服を着用していない場所の窃視、ロボット・ストーカー、窓の隙間から小型ドローンが侵入して企業の機密情報が記録された媒体を盗むような事件も発生するであろう。

②は、AI・ロボットの利用行為自体が違法であり、それらを用いて実行される犯罪または不正行為。ネットワークを介したロボットへの不正アクセスにより、犯罪を実行するためにロボットを制御したり、犯罪実行マルウェアに感染させて自律的に犯罪に従事させるようなことが想定される。不正アクセス禁止法は、ネットワークを介したアクセス権限がないコンピュータを利用する行為を禁止しているため、このような無権限アクセス自体は処罰の対象となる。しかし、ネットワークを介さずに目の前のロボットのプログラムを不正に直接書き換える行為や不正アクセス後の犯罪行為は同法では処罰できない。

AI開発者の刑事責任についても、ファイル交換ソフトに係る著作権侵害をめぐる事案を思い出す。ウィニー事件では違法コピーなど著作権侵害コンテンツを送信可能状態にしたとして著作権法違反の幫助に問われたが、著作権侵害に利用する蓋然性が高いことを認識・認容していたとまで認めることが困難であり、著作権法違反罪の幫助犯の故意が欠けるとして無罪になった。AIにより自律的に動作するロボットが犯罪に従事したとき、AI開発者の責任はどこまで問われるのであろうか。

2 刑事手続法に係る課題

法執行におけるロボコップ（ロボット警察官）の導入、犯罪捜査におけるAIプロファイリングの活用、犯罪予知AIを用いた犯罪予防対策の実施など、犯罪捜査の手法や適正手続の保障に関する刑事手続法をめぐる問題は、AIの利用やロボットの導入により革新的な変化をもたらされる可能性が高い。しかし、その利用方法によっては、究極の監視社会化や警察国家へのおそれもあり、どのような問題が生ずる可能性があるのかを慎重に見極めた上での導入が求められる。ロボットが取得する音声や画像、各種センサーの記録（ログ）も、犯罪捜査において重要かつ有力な証拠となり得る。

ロボコップは、掃除ロボットで知られるアイロボット社（iRobot）や警察の法執行用具開発メーカーであるテイザー社（Taser）などが既に研究開発を行っている。犯罪者に躊躇なく対峙する法執行が可能になり、警察官の人的被害の心配もなくなる。しかし、技術的に中立性が保たれているはずのロボコップが、人種差別的な法執行に及ばないとは言い切れない。

人種差別と警察による法執行の問題については、それらの活動を自動化することによって警察による差別の本質的な問題が解決されるのか。多くの人々にとって、技術は政策的に中立であると信じられている。将来のロボコップは、その考えに基づいて中立的な立場で法を執行することが期待されている。その結果として、人種差別や偏見等とは関係なく活動ができるということが期待されている。

そのような観点からすると、ロボコップの導入は人種差別的な政策に対する技術による解決手段と考えることもできるのかという問いに対し、技術は社会における様々な問題を増幅したり、既に社会に存在する問題を反映することもあり、ロボコップの導入によって人種差別的な政策に一層拍車がかかるという危険が存在するとの見解もある¹²⁾。

実際に他の視点から考えてみると、デジタル技術は人種差別との関係においては技術的に中立性は保たれていないことがある。例えば、自動水栓では、蛇口の前に手をかざしても肌の色が黒いこ

とによって動作しないことがあり、顔認識技術が、人種差別的な問題を発生させるおそれもある。

連続盗犯事件で令状なしにGPSを設置した捜査が日本国内でも問題となったが、自動追尾ロボットやドローンを活用することにより、尾行や張り込みを長期間・連続して実施することが可能となる。性犯罪者の監視目的で追跡装置を足首に装着する試みが海外では既に実施されており、保護観察中の人物を捕捉し続けたり、ストーカー禁止法に基づく接近禁止命令の実効性確保にも有効な手段になり得る。

証拠収集についても、捜査対象者に密行的に密着してリアルタイムで会話を傍受し映像を撮影し続ける超小型ロボットの導入が予想される。犯罪捜査との関係においては、会話の傍受は密行用増幅器（スパイクマイク）、通信傍受の対象は、電話、携帯電話、電子メール、ペンレジスター、位置や所在の探知には、監視カメラ、ポケットベル（beeper）、熱感知投影装置（FLIR）、電子通信の傍受については、カーニボー（現在は、DCS 2000と改称）、KLS（キー・ロガー・システム）、その他、電磁波傍受「テンベスト」など実に多種多様な手段が用いられてきた。

1942年の米国のゴールドマン事件を端緒に「小型電子盗聴器（bug）」による会話傍受（bugging）が裁判において争われるようになったが、虫（bug）のように小さなロボットによる文字どおりの「バギング」が問題になるであろう。自動走行車が撮影した映像だけでなく、掃除ロボットなどの生活支援ロボットが記録した音声と画像などが犯罪捜査で有力な証拠になることもあり得る。

犯罪捜査においてAIを活用するとプロファイリングの精度は飛躍的に向上する。経験則に基づくベテラン捜査官による分析とは比較にならない。しかし、AI鑑定の導入はDNA鑑定同様に誤判が生じる可能性があることを認識して行う必要がある。AIによる判断に基づいて実施することへ懸念だけでなく、そのような技術を用いることの当否を問わなければならない。

犯罪捜査におけるAIの活用は、膨大な証拠か

ら犯人特定に必要な情報を抽出するなど事後的に犯人の検挙を支援する一方で、事前にAIを利用して犯罪を予測しようという取り組みもある。国内でも、犯罪の発生場所の予見に既に用いられている。ロンブローズは、生来犯罪者説を提唱した。科学的根拠がなく実際に刑事手続において用いられることはなかったが、AIの利用により犯罪に従事する確率が高いという結果が示されるだけでも、その人物の人生を左右しかねない。公権力によるAI犯罪予知技術の利用は、極めて重大な人権侵害や差別をもたらすことが懸念される。

例えば、ゲノム（遺伝子）情報と顔の形状のビッグデータを取得し関連解析を実施することにより、顔の形状の個人差に関連するゲノム多型を網羅的に特定し、個人のゲノム多型のデータに基づいて、その個人の顔の形状を正確に予測することを試みる研究がある。そのような研究を用いると、顔の情報を識別することでDNAの分析を行い、犯罪に従事する可能性がある人の傾向や分析をすることができる可能性がある。人間の病気や疾患は、顔や人間の皮膚などの表面にその症状や兆候がからわれることを参考に人間の顔を分析することを試みるものである。ゲノムから顔形状の予測とは逆方向に、顔形状からゲノムを予測することで、顔画像を医療における疾患診断補助に利用できるメリットがある一方で、犯罪捜査（予知）において用いることによる問題は議論すら行われていない。

ロボットを用いた犯罪では、事件と事故の見極めが難しくなる。犯罪に利用されたロボットから犯罪の実行者を特定することも困難になると予想される。ネットワーク犯罪でアクセスログを解析した結果、誤認逮捕が発生した事例は記憶に新しい。ロボットには指紋がなくDNAもない。自動車事故のように証拠となる部品の断片が残されていたり、監視カメラで撮影された画像の分析によりロボットを特定しその登録者や管理者を確認できても、犯人の特定にまで至らないおそれもある。犯罪に利用されたロボットからの犯人特定に至るプロファイリングが困難にならぬよう、ロボット

利用犯罪のフォレンジック（捜査手法）を確保するための方策を検討しなければならない。

AIの利用に伴う刑事責任については、例えば、マイクロソフトのTayが差別的な発言をしたことについて、未熟なAIによる差別的な発言は責任能力が認められないため名誉毀損罪は成立しないが、成熟したAIによる差別的な発言は成人同様に刑事責任が問われるのかという民法上の権利能力と同様の問題についての検討が必要となる。

ディープラーニング（深層学習）を用いた検証によって事件の「真相」は明らかになるだろうが、「深層」学習による学習内容の真相は誰も検証できないおそれが高い。

VIII ロボット・ロー・バイ・デザイン

将来的に自律型ロボットが社会で広く利用されるようになると、人間が操作するロボットやプログラムされた範囲内で動作するロボットは異なる問題が生ずるおそれがある。

アイザック・アシモフは、「ロボット工学の三原則」（Three Laws of Robotics）を小説において記している。

ロボット工学の三原則 (Isaac Asimov, I, Robot ¹³⁾)	
第1条	ロボットは人間に危害を加えてはならない。また、その危険を看過することによって、人間に危害を及ぼしてはならない。
第2条	ロボットは人間にあたえられた命令に服従しなければならない。ただし、あたえられた命令が、第1条に反する場合は、この限りでない。
第3条	ロボットは、前掲第1条および第2条に反するおそれのないかぎり、自己をまもらなければならない。 ——ロボット工学ハンドブック、 第56版、西暦2058年

手塚治虫も「鉄腕アトム」において、手塚治虫のロボット法を記している。

手塚治虫『鉄腕アトム⑤（手塚治虫漫画全集）』講談社（2003）15頁	
第1条	ロボットは人間につくすために生まれてきたもので

	ある
第2条	ロボットは人を傷つけたり殺したりしてはいけない
第3条	ロボットを作った人間を父と呼ぶてはいけない
第4条	ロボットは何でも作れるがお金だけは作ってはいけない
第5条	ロボットは海外へ無断で出かけていってはならない
第6条	男のロボット 女のロボットはたがいに入れかわってはいけない
第7条	無断で自分の顔をかえたり別のロボットになったりしてはいけない
第8条	おとなに作られたロボットが子どもになったりしてはいけない
第9条	人間が分解したロボットを別のロボットが組み立ててはならない
第10条	ロボットは人間の家や道具を壊してはならない

これらは、2人の天才が生み出した「思想」であって、「法」や「規範」ではない。そこで、将来的なロボット共生社会に向けて求められる基本となる原則として、筆者は、OECDプライバシー8原則を参考に、前述の2015年のロボット法学会設立準備研究会において「ロボット法 新8原則（新保試案）¹⁴⁾」を公表した。

ロボット法・新8原則（新保試案）	
①人間第一の原則 (Humanity First)	・人間に危害を加えてはならない ・ヒトになってはいけない
②命令服従の原則 (Obedience to Order)	・人間の命令に従わなければならない ・管理及び制御可能性を担保すること
③秘密及びプライバシー保持の原則 (Secrecy and Privacy)	・ロボットが知り得た秘密は守ること ・プライバシー・バイ・デザインに基く設計を行うこと
④利用制限の原則 (Use Limitation)	・本来の利用目的以外の目的での利用を制限 ・公序良俗に反する利用の制限 ・人間への危害・加害目的での利用制限 ・ロボット利用倫理の検討

13) アシモフ財団 <http://www.asimovonline.com/oldsite/Robot_Foundation_history_1.html>.

14) 新保史生「何故に『ロボット法』なのか」ロボット法学会設立準備研究会（2015年10月11日）報告資料（2015）。

⑤安全保護の原則 (Security Safeguards)	<ul style="list-style-type: none"> ・ロボットの利用に伴う安全性の確保 ・安全基準の策定、当該基準に基づく開発及び利用 ・安心して利用できる環境確保のための制度の整備
⑥公開・透明性の原則 (Openness & Transparency)	<ul style="list-style-type: none"> ・ロボット開発における開発内容の公開・透明性の確保 ・ロボットの利用方法における透明性の確保
⑦個人参加の原則 (Individual Participation)	<ul style="list-style-type: none"> ・ロボットの利用ルール策定における個人の参加 ・ロボットによる個人管理の制限
⑧責任の原則 (Accountability)	<ul style="list-style-type: none"> ・ロボットの取扱いに伴い生じた責任（法的責任）への対応 ・ロボットの取扱いにおける倫理的、道義的責任の考慮

事後救済や原状回復が困難なプライバシー侵害同様に、自律型ロボットによる問題も事後対応ではなく、ロボット共生社会を迎えるにあたって、「ヒト」に近づくロボットに対し、「人」がしなければならないことを、あらかじめ考えておくこと。「ロボット・ロー・バイ・デザイン」により安全・安心なロボット利用に必要な対策を講ずるべきではないかという発想である。

ロボットが普及することにより、将来的には様々な場面で人間が排除される世界の拡大が見込まれる。AIやロボットが人間に代わって様々な職業に従事するであろうし、高速道路は自動走行モードでしか通行できなくなるかもしれない。前者は労働力不足を補うことや危険業務からの解放などのメリットがあり、後者は事故防止や渋滞緩和につながる。しかし、そのような社会の到来は、人間が生きる喜びを享受できる望ましい社会なのだろうか。まずは、「人間第一の原則」から考えたい。

IX 「AI 開発ガイドライン」

AIについては、総務省「AIネットワーク化検討会議」が、2016年4月15日に中間報告書として「AIネットワーク化が拓く智連社会（WINS（ウインズ））—第四次産業革命を超えた社会に向

けて—」を公表している。

報告書では、(1) 目指すべき社会像として、「高度情報通信ネットワーク社会」、「知識社会」の次に目指すべき社会像として、「智慧」の連結に着目して「智連社会」(Wisdom Network Society: WINS (ウインズ))を構想。(2) AIネットワーク化の影響として、公共(まち)／生活(ひと)／産業(しごと)の分野ごとに、2020年代～2040年代の時系列で影響を評価。(3) AIネットワーク化のリスクとして、AIネットワーク化のリスクを検討するための枠組みの整理及び現時点で想定されるリスクを例示。(4) 当面の課題として、研究開発の原則の策定、利用者保護の在り方、社会の基本ルールの在り方等を提示し、AIネットワーク化をめぐる諸課題に関し、継続的に議論する国際的な場の形成及び国際的な場での議論に向けた国内での検討体制の整備の必要性を提唱している。

報告書で示されたAI研究開発8原則は、2016年4月に開催されたG7サミットの情報通信相会合において公表され各国の同意を得ている。

研究開発に関する原則として示された8原則は、①透明性の原則（AIネットワークシステムの動作の説明可能性及び検証可能性を確保すること）、②利用者支援の原則（AIネットワークシステムが利用者を支援するとともに、利用者に選択の機会を適切に提供するように配慮すること）、③制御可能性の原則（人間によるAIネットワークシステムの制御可能性を確保すること）、④セキュリティ確保の原則（AIネットワークシステムの頑健性及び信頼性を確保すること）、⑤安全保護の原則（AIネットワークシステムが利用者及び第三者の生命・身体の安全に危害を及ぼさないように配慮すること）、⑥プライバシー保護の原則（AIネットワークシステムが利用者及び第三者のプライバシーを侵害しないように配慮すること）、⑦倫理の原則（ネットワーク化されるAIの研究開発において、人間の尊厳と個人の自律を尊重すること）、⑧アカウントビリティの原則（ネットワーク化されるAIの研究開発者が利用者等関係ステークホルダーへのアカウントビリティを果たすこと）となっている。

X 安全保護及びセキュリティ確保の原則

前述の諸原則は、今後引き続き検討を行うこと

が必要となるが、安全保護及びセキュリティ確保の原則については、喫緊に検討が必要であるため、本稿では当該原則について言及しておきたい。

1 情報セキュリティ対策の新たな課題

AIやロボットの普及により、物理的な媒体や装置を構成するチップの情報セキュリティ対策が大きな課題になると考えられる。その理由は、IoTにより、あらゆるモノがネットワークに接続され、その結果、ネットワークを介して様々な家電製品やモノを操作することができるようになること。それに加えて、ロボットやAIの発達により、日常的にそれらが利用されるような社会になると、この問題の重要性は急激に増幅すると考えられる。

例えば、ネットワークのセキュリティについては、ネットワークを介した不正アクセスの防止や、コンピューターウイルスやマルウェア対策など、情報のセキュリティを確保するための様々な対策が講じられてきた。ところが、装置のセキュリティそのものについて、例えばチップについてはそもそも書き換えることを前提にして作られているため、物理的にはすぐに書き換え可能な状態になっている。現状では、機械や装置の蓋を開けて基盤に装着されているチップを書き換えることは容易である。

自動車の盗難防止装置として「イモビライザー」という装置がある。電子的に符合が一致することで車が動作する。電子キーを用いた鍵は通常の鍵のように偽造することが極めて困難である。イモビライザーは、電子的な符号が一致しなければ車を動作させることができないため盗難防止の手段としては非常に有効な手段と考えられている。ところが、イモビライザー装着車であっても盗難被害に遭っている。その理由は、車の窓ガラスを割ってダッシュボードを開けて、ダッシュボード内に装着されているイモビライザーを入れ替えるだけでエンジンが始動できてしまうからである。つまり、電子的に高度なセキュリティ対策を講じていても、物理的にその装置が入れ替えられてしまうだけで、高度なセキュリティは意味をなさなくなる。今後は、ロボットが日常的に用いられるようになると同様の問題が発生すると考えられる。

2 新たなセキュリティ脅威

ネットワークを介したロボットへの不正アクセスやハッキングにより、犯罪を実行するためにロボットを制御したり、犯罪実行マルウェアに感染させて自律的に犯罪に従事させるようなことも想定される。

不正アクセス禁止法は、ネットワークを介したアクセス権限がないコンピュータを利用する行為を禁止しているため、ネットワークに接続されたロボットへの無権限アクセスは処罰の対象となる。しかし、ネットワークを介さずに目の前のロボットのプログラムを不正に直接書き換える行為や不正アクセス後の犯罪行為は同法では処罰できない。

ロボットへのDoS攻撃（サービス拒否攻撃）によりインフラを管理するロボットが停止した場合の影響。マルウェア等により悪意ある第三者に乗っ取られた多数のゾンビコンピュータで構成されるネットワークを「ボットネット」というが、その語源は、操り人形としての「ロボット」である。DDoS攻撃（分散サービス拒否攻撃）のように、ロボットをマルウェアに感染させることによって特定の対象物を複数のロボットで一斉に攻撃する文字通りの「ロボット・ボット・ネットワーク」が出現したときの社会的脅威は計り知れない。ヒッチコックの映画「鳥」のように、特定の対象にマルウェアに感染したドローンが一斉に襲いかかったり、自動走行車が政府機関に一斉に突入するようなセキュリティ・リスクは机上の空論とは言えない。

そのための対策を今後実施する上で参考となる例の一つ挙げてみたい。2015年に首相官邸の屋上へのドローンの落下事件が発覚し、その後も様々な場で落下や衝突事故が発生したことを受けて航空法の改正に至っている。飛行禁止空域の設定、夜間飛行禁止、目視による常時監視、人又は物件との距離確保が義務付けられた。この法改正が意味するところは、技術的な安全基準に基づいて安全に飛行できるドローンであっても、「安心して」社会で利用できるわけではないことを示している。安全基準に適合したドローンであっても、家の中を覗き見るなど撮影されたくない人や場所を対象に利用されたり、飛行させると危険な場所での飛行がなされるといったような問題は、その

ような基準ではカバーできないのである。よって、新たなセキュリティ脅威には従来からのネットワークのセキュリティ対策では対応できないことや、安全だけでなく安心な利用のための対策の検討も必要であることを認識する必要がある。

3 情報セキュリティのゆくえとロボット法

インターネットの出現当初は、情報セキュリティ対策の必要性はほとんど認識されていなかった。そのため、ウイルス対策や不正アクセスをはじめとするネットワークの不正利用のための対策は、事後的に対応が必要になってから実際に対策が実施されるようになった。

AIの発達、IoTの普及、自律型のロボットの登場などが見込まれる現在、ネットワークのセキュリティ対策にだけ目を奪われていると、実社会におけるさまざまな物理的な装置のセキュリティ対策が講じられていない状況では、インターネットの普及とともに情報セキュリティ対策の不備による問題と同じことを繰り返す可能性がある。

このことからしても、情報セキュリティ対策は、単に、その確保のための防御的な対策ではなく、マネジメントシステムを活用することをはじめとして、組織的かつ体系的な取り組みが必要であるとともに、リスクマネジメントの観点からの対策の重要性を認識しなければならない。

目の前のパソコンがコンピュータウイルスに感染した場合、パソコンを使用することができないという不便を感じるが、それによって身の危険を感じる人はいないであろう。一方、目の前のロボットがコンピュータウイルスに感染して暴走し、自分を襲ってくるとしたら。そのような脅威も想定し、ロボット法の研究を進めていきたい。

* 本研究は、国立研究開発法人科学技術振興機構 戦略的創造研究推進事業（社会技術研究開発）「人と情報のエコシステム（HITE）」研究開発領域による研究成果の一部である。（This research was supported by RISTEX, JST.）