IoT時代にリスクが高まる、ロボットへのサイバー攻撃

電気通信大学
情報理工学研究科 教授
新誠一

ロボットとサイバー攻撃。最近何かと話題のテーマである。

ロボットはハードウェアとソフトウェアの組合せである。しかも移動するものもあり、私たちの身近に進出している。さらに人の理解を超えた複雑性と能力を具えている。

“身近”と“人を超えた能力”は人への直接的な危険につながり、“人の理解を超えた複雑性”は完全な対策がないことにつながる。つまり、人を超えたものをどのように管理し、対策を立てるかが現在の人類の課題である。人は複雑であり、他人のみならず自分のこともよくわからない生き物だ。それでも人は社会の中で規則や習慣などにより互いに管理し合い、存続している。つまり、不完全ながらも人類は、未知なる自らというものを管理する手法を構築しつつあると言える。

そこで人の理解を超えたロボットのサイバーセキュリティ対策だが、機械やソフトウェアというレベルの対策だけでなく、未知なるものを管理するようなレベルの対策も必須と言えよう。そこでロボットとサイバー攻撃を定義したうえで、現状の再認識と対策を論じていきたい。

本格的なロボット化の時代

半世紀前に流行った鉄人 28 号に鉄腕アトム。ロボットはまさに昭和の男子の憧れだった。もちろん、現代でも憧れる子供はいるだろう。しかし、すでにときは 21 世紀、そして令和の時代。ロボットは憧れを越えて、人の生活のど真ん中にその位置を占め始めている。

今、RPA（Robot　Process　Automation）という言葉が事務系のビジネスパーソンを騒がせている。職場に人型のロボットが来て、人の代わりに働いてくれるとの誤解もあるようだが、実は RPA は、これまで FAX や電話で受けた注文をデータベースに手入力していた業務を自動化するだけのことである。これは、事務系の単純作業をロボット任せる流れがようやく動き始めたことと言える。

そうした動きは製造現場では 1970 年代から始まっていた。工場の自動化である。低コスト化、人手不足、労働環境の改善など諸事情から自動化が加速していった。さらにはマシンニングセンタなどの多機能な加工機や搬送、セッティングなどを行う多関節ロボットなどにより、24 時間、休みなく均質の製品がつくられている。

一般的に人は 8 時間神経を集中させて均質にモノをつくり続けることは不可能だ。さらに、1 人の人を雇用すれば福利厚生費などで給料の倍の費用がかかる。仮に 1 台が 1000 万円のロボットを 24 時間稼働させれば、3 年で人件費を下回るコストにできる。

未来の工場は無人化するのかとよく問われるが、汎用品の生産はロボット化されるだろう。しかし、その場合でもロボットをトレーニングし、維持管理をする人は必要である。となると、生産からロボットの維持管理に向かうことが、人が工場で生き残る道と言えよう。もっとも、いずれはロボットが維持管理業務も遂行し始めるだろうから、そのときに人がどうするかは大きな関心事である。

自動化が進みつつある工場から出荷される製品の 1 つである自動車も変わりつつある。CASE（コネクテッド、自動運転、シェアリング、電動化）の大波の中、自動車業界は内燃機関を捨てる覚悟まで固めているようだが、その自動車も実態はロボットと言える[1)]。また家庭でも、昭和の時代に始まったエアコン、洗濯機、電子レンジ、冷蔵庫などによる全自動化が私たちの生活を大きく変え[2)、3)、4)]、さらに今は掃除ロボットなどが跋扈し始めている。今や人類はロボット化した家電を抜きに生活できない。であるならば、超スマート社会の代名詞である「Soicety 5.0」[5)]は、実は人とロボットとが共生した社会になると言えるだろう。

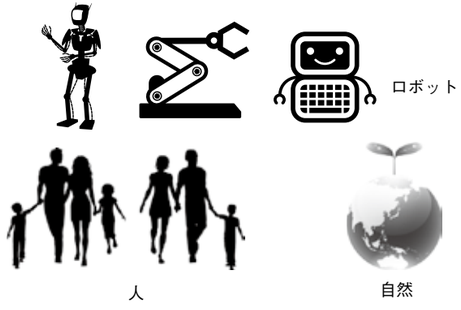

図 1. 世界を構成する 3 つの要素

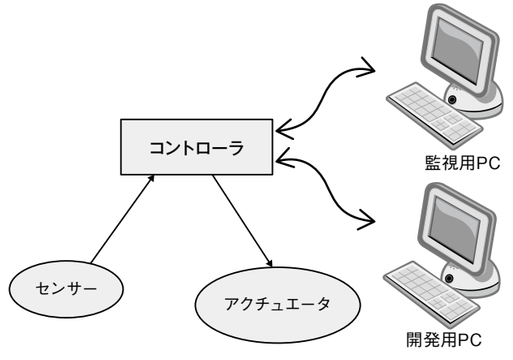

図 2. 制御システムの構成

サイバーセキュリティの面から見たロボットの定義

以上、ロボットの現状をざっと見てきたが、アンドロイドと呼ばれる人型から組込系と呼ばれる電子レンジなどの家電までとロボットの概念は広く、研究者ごとに定義が異なるといっても過言ではない。もっとも、本稿ではサイバーセキュリティの面から見たロボットを論じるので、ソフトウェアを搭載し、通信回線につながれているものをロボットと定義する。すなわち、ここまでに例示した機器はすべてロボットであり、ソフトウェアと通信機能を組み込まれて IoT 化されたものもすべてロボットである。

世の中には人がいて、ソフトウェアが搭載されている物と搭載されていない物とがある。仮にソフトウェアが搭載さていない物を自然物、搭載されている物を人工物とするならば、世界の 3 分の 1 は人工物＝ロボットと言える（**図 1**）。また、自然物にソフトウェアを搭載すれば組込化となり、通信機能を搭載すれば IoT 化となる。それでは人にソフトウェアを搭載し、通信機能をもたせたら何になるのか。それもおもしろい話題だが、ここでは**図 1** のように、世界は 3 つの要素で構成されていることを前提に論述しよう。

ロボットもサイバー攻撃対策が喫緊の課題

サイバー攻撃もロボット同様、いろいろな考え方があるので悩ましい。通信回線経由の攻撃だけに限定するものから、電源線の操作による誤作動やリセットも対象にするものまである。さらに、電子化されたロボットの設計情報や稼働情報の漏洩、改ざんまでを想定するものもある。ここでは通信回線が介在する何らかの形での攻撃をサイバー攻撃と呼ぼう。

もっともこの定義は、先に定義したロボットに対して何か限定を強いるものではない。なぜなら、ソフトウェアを搭載した機器は何らかの通信回線をもっているからである。以下にそれを確認していこう。

ソフトウェアとは「書換え可能」ということである。つまり、可変であることが本質である。機械を動作させるためにはギヤ、電子回路なら配線を施さなければならないが、ソフトウェアなら記憶装置であるメモリを書き換えるだけで動作が変わる。