◎ 巻頭エッセイ ◎

# サイバー戦場の霧を晴らす

土屋 大洋
Tsuchiya Motohiro

1993年7月5日、米国の雑誌*New Yorker*に、2匹の犬がコンピュータの前に座る有名な風刺漫画が掲載された。1匹の犬がもう1匹の犬に向かって「インターネットでは君が犬だってことを誰も知らないんだよ」と述べている。当時、徐々にインターネットは人々に認知されるようになった段階で、本格的普及の前夜であった。インターネットが作り出すサイバースペースでは現実世界の属性にとらわれず、例えば、女性が男性のふりをしながら、子供が老人のふりをしながらコミュニケーションをすることも可能だとされていた。

それから20年後の2013年、米国のインテリジェンス機関である国家安全保障局（NSA）の仕事を請け負っていたエドワード・スノーデンがNSAの機密文書を大量に暴露した。その結果、テロリストやサイバー攻撃者をあぶり出すためにNSAがさまざまな方法でインターネットを含む通信を監視していることがわかり、「インターネットでは君が犬だってことを、NSA以外は、誰も知らないんだぜ」とするパロディーの風刺漫画も描かれた。

現実には、モノのインターネット（IoT）と呼ばれるように、コンピュータや携帯電話／スマートフォン（スマホ）だけでなく、多様な機械やモノがネットワークにつながるようになり、ネットワークの向こう側にいるのは人間でも犬でもなく、冷蔵庫や風呂やカーテンといったことも現実になり始めている。

当然のことながら、そうしたデジタル技術、サイバー技術の変化の波は安全保障にも及んでいる。サイバー攻撃や宇宙兵器、無人機（ドローン）、人工知能（AI）、ロボットなどの可能性は広く議論され、赤外線、レーザー、レーダー、人工衛星などで誘導される精密誘導兵器や自動制御技術も登場している。島嶼地域での作戦を想定した新しい水陸両用（amphibious）兵器の開発も進められている。しかし、逆にそうしたデジタル化された兵器に対する電磁波による妨害、いわゆる電子戦の概念も復活してきている。

2016年夏に公開され、ヒットした映画『シン・ゴジラ』では、ゴジラに対して無人機による波状攻撃が行なわれた。今後の戦争では兵士が戦場で自らの命をさらす機会は減ることが予想されている。第六世代のジェット戦闘機は無人機が主になる可能性

が高い。

さらには、サイバー攻撃によって戦闘開始以前に敵の戦闘能力を奪ったり、重要インフラストラクチャーを攻撃することによって社会機能を喪失させたりすることも想定されている。サイバー攻撃は、実際には思い立ったらすぐにできるものではなく、事前に敵のシステムを内偵し、ハードウェアやソフトウェアのバージョンを特定したうえで脆弱性を仕込んだり、手法を検討したりしておくことが必要になる。そのために軍や重要インフラストラクチャー、政府のシステムに対しては、すでに平時から各種のスキャニング（脆弱性を探すための広範かつ執拗なアクセス）が行なわれている。

サイバーセキュリティーにおいては「ロボット」を省略した「ボット」という言葉が使われる。これは自動化／半自動化されたプログラムのことで、攻撃を企図する者が事前にプログラムを組み、それが自動的に標的となるシステムの脆弱性を検知し、合図とともにシステム破壊を始めることになる。こうした「ボット戦争」もまた想定内のシナリオである。防御側ではまだ人間による判断が重要だが、攻撃側は自動化しやすくなっている。

こうした変化を米国政府は作戦領域（ドメイン：operational domain）の変化と呼んでいる。従来の陸、海、空に加え、第4の作戦領域として宇宙、第5の作戦領域としてサイバースペースが挙げられている。

しかし、サイバースペースは各種の端末、通信チャンネル、記憶装置などが相互接続された人工的な空間である。その一部ないし全部を破壊したり機能不全に陥らせたりすることは、自然空間よりもはるかに容易である。それでも、サイバースペースを構成するサイバーシステムは兵器システムや指揮命令システムに大きく被さってきている。サイバースペースは独立した作戦領域というよりも、むしろ既存の4つの作戦領域をつなぐものであり、逆に断絶させるものにもなる。

日本や朝鮮半島、台湾、中国を含む広大な地域を管轄する米統合軍である太平洋軍（PACOM）の司令官を務めるハリー・B・ハリス提督は、「今や、世界の出来事は、特にここインド・アジア太平洋において、クロスドメイン能力を開発することが喫緊の課題であることを強調していると思う」と述べている。もはや今後の戦闘は陸、海、空、宇宙、サイバースペースといった個々独立した作戦領域において行なわれるのではなく、それらをまたいで行なわれるようになる。個々の部隊はサイバーシステムによってつながっており、敵軍のそうしたシステムを不能にすることがひとつの重要な任務になるとともに、自軍のそれを防護することも必須になる。

かつてプロシアの軍事思想家カール・フォン・クラウゼヴィッツは戦場における不確定要素を「戦場の霧」と呼んだが、サイバー戦場の霧はいっそう濃い。サイバー攻撃者は正式な軍事組織の中にもいるが、多くはその外にいる。非正規兵、傭兵、民兵が暗躍する戦場になっている。素人集団や個人による参戦の可能性もある。彼らは軍

服も着ず、徽章も付けず、従来の武力紛争法のルールを無視して攻撃を仕掛けてくる。

サイバー攻撃者が誰なのかを特定する「アトリビューション（attribution）」はきわめて難しいとされてきた。すべてのサイバー犯罪、サイバーエスピオナージ（サイバースペースでの諜報活動）、広義のサイバー攻撃についてその実行者と首謀者を特定するのは確かに困難である。しかし、重大な影響をもつサイバー攻撃については、国家は多くの人的・財政的リソースを投じてアトリビューションに努めるだろう。実際、2012年の米メディアに対するサイバー攻撃、2014年のソニー・ピクチャーズに対するサイバー攻撃、2015年に発覚した米国人事局（OPM）に対するサイバーエスピオナージなどにおいては、米国政府による攻撃者の名指しが行なわれている。

こうした米国政府のアトリビューション能力は、スノーデンが暴露した通信の監視やその他のインテリジェンス活動によるところが大きい。アトリビューション能力の向上は、サイバー攻撃者にプレッシャーとなり、抑止効果を生む。スノーデン問題が提起したように、そこには自由と安全のバランスの問題があるが、安全を重視するならば、アトリビューション能力の向上は不可欠である。

サイバー攻撃以外にも多様化する技術は、一方で安全保障を複雑化し、対応を難しくする側面もあるが、他方でそれに対抗する技術・手段・戦略・思想をも生み出す。核兵器がもつ威力にもかかわらず、それは広島と長崎でしか実際には使われていない。

むろん、サイバー攻撃やドローン攻撃、ロボットやボットによる攻撃は、従来の兵器と比べて閾値を下げる可能性がある。どこまでそれを抑止できるかは、各種の攻撃をアトリビュートする能力、つまり、新しい戦場の霧を晴らすことができるかどうかにかかっている。

つちや・もとひろ　慶應義塾大学教授