特集
Special Feature

サイバー・ウォーズ

編集にあたって

長倉克枝　江間有沙 | 東京大学未来ビジョン研究センター

機械学習を中心とした人工知能（AI）技術が，国家安全保障やインテリジェンスといった分野でも活用が進みつつある．これはまさに「サイバーウォーズ（サイバー上の戦争）」であり，情報系の研究者や開発者も他人事ではない．普段考えることが少ないこれらの領域の現状と機械学習やロボティクス等の技術とのかかわりについて知っておくことは，研究者・開発者が社会に役立つ適切な研究開発に取り組む上で有用である．

このような問題意識のもと，情報技術がサイバー攻撃や安全保障でどのように利用され，どのような問題が起きているのかを知るため，編者らは2018年12月と2019年6月に「AIと安全保障／セキュリティ」をテーマに3回のセミナを開催した．本特集はセミナに登壇いただいた方々に執筆をお願いした．セミナ登壇者以外で本特集に寄稿いただいたのは中谷氏である．サイバー攻撃に焦点をあてた特集とするにあたって，国際法的な観点も重要であるため依頼し，ご快諾いただいた．

本特集は5編の解説と座談会からなる．名和氏による**「攻撃対象領域の増大に伴い高度化する攻撃戦略」**では，「サイバーフィジカル」などサイバー空間と実空間の一体化が進展する中で，サイバー脅威が発生，深刻化する要因を「攻撃対象領域」と「攻撃戦略」という2つの概念を用いて概説された．サイバー脅威主体へのモニタ活動を長らく行っている名和氏だからこその視点で，企業や国家の現状を的確に解説している．

続く高橋氏らによる**「機械学習を用いたサイバーセキュリティ技術の発展」**は，深刻化するサイバー攻撃への対抗手段として用いられる効率化・自動化された機械学習技術を解説している．フェイクニュースや自動運転のハッキングなどサイバー攻撃の対象が多様化するだけではなく，攻撃そのものが自動化されつつあることに対し，技術には技術で対抗をしていくという点で今後の展開が期待されるものである．

サイバー攻撃の範囲は，個人や企業だけではなく国家安全保障にまで及ぶ．佐藤氏の**「情報通信技術（ICT）と安全保障」**は1990年代以降，情報技術が

いかに軍事に用いられてきたかを概説している．特に，近年では人工知能が兵器システムの自律化が問題となっており，アメリカ，中国やロシアなど各国の軍事戦略も相まって国連で議論が行われている．軍事的効率性と人道規範を共存させるという難しい課題に現在，直面しているといえよう．

サイバー攻撃に関する国際法のルールを包括的に記述したものとして「タリン・マニュアル」がある．中谷氏は，2017 年に刊行された『サイバー攻撃に適用される国際法に関するタリン・マニュアル 2.0』の作成者の一人であり，解説書を 2018 年に刊行している．**「タリン・マニュアルについて―サイバー攻撃に関する国際法―」**は複雑化，多様化するサイバー空間におけるルール作りの難しさと深遠さを示してくれる一稿である．

サイバー攻撃やインテリジェンス機関の活動を考えるにあたって存在感のある国にはアメリカや中国などが挙げられるが，歴史的な観点からロシアの存在を無視できない．小泉氏による**「ロシアのインテリジェンス機関と ICT」**は，近年ますます存在感をましているロシアのインテリジェンス機関が，実際にどのようなオペレーションを展開しているのかの概要と具体事例を紹介している．2014 年のウクライナ危機は記憶に新しい人も多いだろう．

最後の座談会では，サイバー攻撃や安全保障上の問題に対し，研究者は何を心にとめて研究や議論していけばいいのか，論点の整理を専門家の方々（栗原氏，平氏，鳥海氏，須川氏）に行っていただいた．特に昨今ではフェイクニュースなども「兵器」と見なされるようになってきており，大学や民間企業の研究者にも安全保障の議論は他人事ではなくなっている．研究者の倫理観はどうあるべきなのかなどについて議論が展開された．

本特集が，研究開発を行っている読者の皆様，そして今後，情報系の研究開発に携わろうと考えている未来の研究者が社会との接点に思いを巡らすきっかけとなれば幸いである．

（2020 年 5 月 7 日）