

仮想戦争の終わり-要約

プロジェクトマネジメントコース 矢吹研究室 1442104 増田 準

サイバースペースにおける犯罪や戦争は、近代になり現実化しつつある。もはや SF 小説や映画などの空想の話ではない。こういった仮想空間での犯罪は、サイバー攻撃、サイバーテロ、サイバー戦争と一言にくくれない。民間レベルのものもあれば、企業を狙った犯罪、更には物理的な戦争に発展しかねないものも今後ないとは言い切れない。それ故に対処すべき機関が明確に定義できないことも問題である。つまりサイバー攻撃においては、攻撃側が防御側より有利であるといえる。

現代では、仮想空間のセキュリティが重要視されている。2007 頃から、世界では大規模な DDoS や、紛争にまでサイバー攻撃が用いられた。こうした流れを受け米国がサイバー軍を設立した事などから、サイバー戦争の時代の到来を意識せざるを得ない。9・11 のテロを受け、インテリジェンス機関である NSA にも変化が起こった。監視活動に重きを置き、テロ対策の情報管理を担うことになった。日本では 2014 年、自衛隊にサイバー防衛隊が設置された。サイバー攻撃による物理的被害が予想されていることを意味するが、インターネットが生活に根付いた現代においてデジタル通信機の使用の制限などはもはや不可能である。仮想空間の安定したセキュリティが求められている今、世界各国の協力が必要である。

時代の流れとともにサイバー攻撃も進化を遂げる。インターネットの爆発的な普及により、個人間の情報対策も義務的になった。サイバー攻撃を整理すると、まず侵入し、拡大し、そして目的行動をとる。中には DDoS 等侵入を伴わないものもある。このように対策すべき項目が少なくない。ウイルスを用いた攻撃は多様化を見せ、PC やスマホなど「機械」の一般化から、AI などの「機械学習」の成長が目覚ましい。こうした技術もウイルスの悪質化に取り入れられることを想定しなければならない。2009 年にビットコインの運用が開始され、強力な計算力を持つ「採掘者」が富を得られる時代が来ている。つまり、採掘ウイルスを扱う犯罪者への対策が必要となった。これらのことから、現代ではセキュリティの確保、情報管理が肝であると十分に

いえる。そうした問題を受け、国では各地で「サイバー防御演習」や「セキュリティ・キャンプ」などの人材育成の動きもみられる。

仮想戦争に備えた国際法の整備という問題もある。サイバー戦争の存在が国家で公式に認められた事例はまだないが、2011 年、米国の「サイバー空間の国際戦略」発表により、サイバー空間上の侵略行為に対し自衛権を発動できるという見解が明らかにされた。理由として、核関連施設やダム、航空管制システムに異常をきたされた場合、死傷者を出す可能性や建物破壊の可能性は爆弾・ミサイルと違いがないということだ。こういった考えは米国に続き、各国に広まりつつある。NATO 協調的サイバー防衛研究拠点が発表した「タリン・マニュアル」にて、自衛権等の問題を扱った国際サイバー安全保障法とサイバー武力紛争法に関する専門家の記述が述べられた。対処すべき脅威について各国が共通の認識を持つため、「タリン・マニュアル」が各国政府によって採用される可能性は高い。

抑止拡大が難しい理由として、サイバー攻撃の特性が関係してくる。その種類は多岐に渡り、機密情報を狙った窃取型攻撃、DDoS などの妨害攻撃、制御システムを狙った破壊型攻撃等がある。更には、実際の軍事行動と連動するケースもある。こうしたサイバー攻撃はなぜ抑止が難しいのか。仮想空間では、攻撃の発信源の断定が極めて困難であり、これを「帰属問題」と呼ぶ。攻撃が行われた物理的場所や端末、サーバー所有者、実際の攻撃者が国境を超えるため帰属が複雑化する。またインターネットの「自由」「効率性」といった設計思想から、サイバー空間では攻撃優位なアーキテクチャーが形成された。以上の事からサイバー戦争の抑止は困難であるが、アメリカを先頭に同盟ネットワークの強化と法的基盤の再構築による拡大抑止が進む。今後もサイバー空間とリスクの特質を見極め、抑止対策を刷新していく必要がある。

参考文献

- [1] 土屋大洋. 角川インターネット講座, 13. 仮想戦争の終わり. 角川学芸出版, 2014 年.