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

SF 小説や映画などで描かれてきたサイバースペースを題材とした犯罪や戦争は，近代になり現実化しつつある．問題としてサイバー攻撃，サイバーテロ，サイバー戦争と一言にくくれない点がある．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のだ．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．2007～2014 にかけて，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．その活動をこれまでの「スパイ活動」から，「監視活動」へとシフトし，テロ対策の情報管理を担うことになった．もはや，サイバーセキュリティに限らず米国の安全保障において必要不可欠であるといえる．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なんらかの物理的な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必要不可欠となった現代においてデジタル通信機の使用を制限することはもはや不可能である．サイバースペース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．　インターネットの爆発的な普及なにより，個人間であっても情報対策が義務的になった．そんな時代の流れとともにサイバー攻撃も進化をする．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，パソコン，スマートフォンなどの「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現代では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」が富を得ることができる時代が来ている．これにより，採掘ウイルスを扱う犯罪者が生き残ってしまう可能性があり，管理が必要になる．これらのことなどから，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．サイバー戦争の存在が国家によって公式に認められた事例はまだないものの，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．理由としては，核関連施設のメルトダウン，ダムの放流，航空管制システムに異常をきたされた場合，多くの死傷者を出す可能性や建物の破壊の可能性は爆弾やミサイルと違いがないということからだ．こういった考えは米国に続き，各国家に広まりつつある．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，自衛権など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家が共通の認識を持つためにも，「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．　サイバー攻撃の種類は多岐に渡る．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が挙げられ，更には，動学的な軍事行動と連動するケースもある．これらのサイバー攻撃およびサイバー戦争はなぜ抑止が難しいのか．サイバー空間では，攻撃の発信源を即座に断定すること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，コンピュータ端末，サーバーの所有者，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．