サイバー空間のグレーゾーン化にどう対応すべきか

片桐　範之

グレーゾーンとサイバーセキュリティという言葉を聞くとそれらは一見別々の問題だと思われるが、実は複雑に絡み合う難しい問題であるのと同時に、今後研究を進める必要がある分野である。日本で進んでいるグレーゾーンの研究は尖閣諸島を含む武力攻撃に至らない事態を念頭に語られている一方、サイバー空間の防衛に関しては「伝統的な」安全保障学の枠組みの外にあるため、両方同時に分析するのは特に難しい。しかしサイバーセキュリティの問題は 2017 年 6 月に世界各地で起きたランサム・ウェア（感染したコンピュータのアクセス制限を解除するため身代金の支払いを強要するサイバー攻撃）にも見られたように、不特定団体が国際法の隙間をついて標的の弱点を狙うことに成功した。サイバー空間における安全保障がグレーゾーン化する場合、特に難しい問題と成りうる。本稿ではこの分野に関する理解を深めるためにその深刻さを説くと共に、今後の研究の方向性を示唆することを目的とする。

一般的な安全保障学では、サイバー空間はそれを制御する主体のいない、いわゆる無秩序状態（アナーキー）だとの理解がある。攻撃元を正確に特定することが難しいため、防衛と反撃が難しい。反撃が難しければ抑止も限定されるため、結果として防衛側よりも攻撃側を有利にする。従って国家や一般企業に対するサイバー攻撃が絶えない。国際社会はこのアナーキーの影響を最小限に食い止めるためにも、サイバー空間における防衛力やそれに伴う法律、そしてサイバー攻撃を処罰するための秩序の構成に勤しんでいる。しかしサイバー空間の力学は急激な変化を遂げており、国際社会の対応策よりも早く変化している。そのペースのギャップを埋めるのは至難の業であるため、国際法を通し国家間の合意を得たとしても、その枠組み外で行動する「グレーゾーン」が生じることになる。グレーゾーンは単に尖閣諸島などの武力攻撃に至らない事態などだけに存在しない。サイバー空間におけるグレーゾ

ーンを埋める努力が今後必要になる。

現行の国際法も日本国内の法律もサイバー攻撃に対する防衛対処法が不十分な状態に置かれている。国際法の分野では「タリン・マニュアル 2.0」が 2017 年に出版され、欧米の専門家が中心となりサイバー空間内での規範を制定する動きが活発化し、サイバー空間のギャップが徐々に埋まってきた。しかし今後これを国家間の正式な合意として確定し、それを各々が制度化し、各国の内政に浸透させるには数年はかかる。特に 2017 年 6 月の気候変動のパリ協定からのアメリカの脱退表明に見られたように、トランプ政権の誕生を中心とするポピュリズムの再来は、国際合意に反する規範を促す。更に現在の米ロ、米中関係の状態では、主要な国家間で正式なサイバー合意を目指すには良いタイミングとは言えない。サイバー空間の無秩序状態はしばらくは続くと見てよい。

サイバー空間の無秩序状態に対し本来ならば、日本を含めた各国の防衛体制の強化が行われるはずである。しかし日本では憲法などの法的な制約により、サイバー空間でのあらゆる攻撃を抑止するのに必要な攻撃力や反撃力が政府に与えられていない。結果として中国や北朝鮮からの一方的な攻撃に耐えるための防衛さえ不十分である。また、個人のプライバシーを含む国内の規範のために、サイバー空間内での制御の強化に対しては、市民団体やメディアを含む様々な方面からの反対が予想される。今後は海外からのサイバー攻撃は更に強化されることが予想できるため、日本国内の法的枠組みのアップデートが必要になる。同時に、サイバー空間の無秩序状態を埋めるためにも日本は国際社会でリードを取り、サイバー空間のグレーゾーン化を防ぐべく積極的に貢献する必要もある。国際法は一度制定されると変化させるのに時間がかかるため、一番最初の法律制定に日本の考えを入れるべく動く必要がある。

また、サイバー空間のグレーゾーン化を阻止するためには海外への情報発信が欠かせない。日本ではサイバー攻撃に対する理解と対応の必要性が徐々に浸透してきてはいるが、日本の取組みが必ずしも海外に知られていない場合がある。アメリカの専門文献を見ても日本に関する記述は単に少ないだけでなく、日本の大企業や政府のウェブサイトがハッカーの攻撃にあったこと

など、その防衛力が不十分な被害者としての扱いがほとんどである。これは海外からの攻撃を不必要に促してしまう効果がある。今後はサイバー問題に関する政府からの情報発信がより必要になる。特にサイバー攻撃に対する防衛が成功した際にはそれを大々的に報道し、日本の防衛能力を誇示する必要があるのではないか。