『国際情報セキュリティにおける緊急の課題 ―ロシアの視点―』シュルスチュク論文への補説

藤　巻　裕　之*

シュルスチュク氏は、ロシア連邦国家安全保障会議初期補佐官としてソ連時代から情報通信分野おける責任者であり、国家レベルの政策決定の場にいる人物である。現在は、モスクワ国立大学情報安全保障問題研究所の所長、国家国際情報セキュリティ協会（NAMIB）の会長を兼任している。国家国際情報セキュリティ協会は、2018年に国内外の研究機関、企業、NGO から成る非政府組織として創設されたコンソーシアムである。同協会主催の会議の成果はプーチン大統領を議長とするロシア連邦国家安全保障会議で共有をされると言われている。シュルスチュク氏による「国際情報セキュリティへのロシアの視点―緊急の課題―」は、特にロシアの国際社会における情報通信分野の安全と平和的発展のためのロシアの主張を論じている。本文において「。。。一連の国々がロシアを脅威であるとみなし、中には軍事的な敵と位置付けている国さえある。軍事紛争が、核大国が参加する形となる局地戦、地域戦争に発展する危険性が高まっている。宇宙空間、情報空間が、軍事行動を実施する新たな戦闘領域として積極的に開発されている」（本文１ページ）。このような、ロシアの持つ焦燥感は、米国のサイバー空間における「好戦的」な政策に対してロシア一国ではなく、ロシアの同盟国を巻き込んで国連で議論が進められている。シュルスチュク氏が解説をする「国際情報セキュリティ分野における国家政策の原則」（本文では「原則」）は、ロシアとその同盟国にとってより安全な「グローバル情報空間」の創設と維持のための方策が記されている。本稿は、シュルスチュク論文をより深く理解するために、国際政治におけるサイバーセキュリティとロシアにとっての「脅威」とは何かを論じたい。

国際政治とサイバー空間の秩序

国境管理をめぐる国際政治は、国民国家が誕生して以来国家に課された永遠の課題であ

＊東海大学政治経済学部政治学科（Tokai University）

るが、科学技術の進化に伴う国内政治と国際政治の相互関連性はこれまで以上に重要性が高まっている。なぜなら、グローバリゼーションが深化したことで、国境の内と外が高度にネットワーク化され、サイバー空間における「境界線」が曖昧になったからである。例えば、サイバー空間における安全保障政策、国家統合の維持のために行われる検閲などが仮想空間を通して行われている。また、サイバー空間は国際政治の現実が反映されてもいるし、科学技術の発展は、仮想現実を現実世界で実現できる範囲が日々拡大している。

サイバー空間をめぐる国際秩序は、現実世界の同盟関係がサイバー空間にも反映されている。各国のサイバー空間の成立過程は、その国家の歴史、統治形態、国民国家統合の深度などにより大きく二つに分類することができる。一つ目は、米国を中心とする先進諸国によって構成されるグループで、情報システムとそこで処理される情報の自由と安全を保障することを重視する。それらの国家群が使用する「サイバーセキュリティ（cyber security）」は、国家のみならず企業にとって重要な通信ネットワーク、金融システムなど経済活動を維持するためのインフラをサイバー攻撃から守ることがこの用語を使用する諸国にとって共通の脅威である。これらのグループを構成する諸国は、サイバー空間と比較的安定した民主主義をよりリベラルなグローバル市場に依存することで高い経済的利益を得てきた。

二つ目は、ロシアと中国を中心とした旧ソ連圏諸国並びに途上国に位置付けられる国々によって構成されるグループである。これらの諸国は、情報の安全を国家が管理することを重視する立場であり、これらの国々の国内体制にとってサイバー空間は現実政治との連関性が高いのが特徴である。この国家群が使用する「情報セキュリティ（information security）」は、サイバーセキュリティよりも広い概念である。このグループにとって国家、自治体、企業へのサイバー攻撃は国家安全保障の範囲であり、各主権国家が自国の安全を独自に保障するのは当然のことだからである。これまでにない情報伝達機能を持ったインターネットが現れて以来、主権国家がインターネット空間を管理することができないことはロシアにとって大きなストレスとなっている。プーチン政権にとってサイバー空間で政権批判が共有され、物理的に市民が政府を打倒することに成功した「アラブの春」は我々が想像する以上に重い意味を持ったことが想像できよう。これら権威主義諸国にとって情報空間におけるウクライナ戦争への非難を含む政権批判、サイバー攻撃への批判は単なるネット上の非難ではなく、国家間の情報戦争なのである。

ロシアにとっての「脅威」とは

2017年にモスクワ大学情報安全保障問題研究所と平和研は共催でシンポジウムを開催し、ロシアが考える情報空間の秩序をめぐって議論が交わされ、サイバー空間における

「主権」概念の違いが明らかになった。同研究所シュルスチュク所長より提言書として「国際条約草案の構想―インターネットの安全な機能と発展の構想」が提出された。同提言では、インターネット空間を国連憲章に反する目的で使用することを防止し、経済発展に資する安全な通信ネットワークの発展のために国家、世界レベルのICT企業が参加をする新しい国際協定の必要性が提案された。また、国家、いかなる地域主義もインターネット空間において独自の規範や規則を定め、社会を監視し、外国の世論を操作し、または主権国家の状況を不安定にさせる権利がないことを確認した。

このように、ロシアはサイバー空間における国際的な規範構築に積極的な姿勢を示してきた。ロシアと中国は、サイバー犯罪対策に関する条約は国連において策定されるべきである、という立場から「サイバー犯罪条約（ブタペスト条約）」には参加をしていない。ロシアは、2011年９月ロンドンで開催された「サイバー空間における国際会議」において「情報セキュリティのための国際行動規範」を国連に提出した。この行動規範では、サイバー空間における国連加盟国間のコンセンサスを主権の尊重、領土の保全が相互に脅かされないことに求めた。なぜロシアは、自らを縛ることにもなる国際的行動規範の普及に尽力するのだろうか。それは、ロシアはサイバー防護能力において欧米諸国には及ばない、仮に欧米諸国からサイバー攻撃を受けた場合には、それらを防ぐことができないという現実がある。

2018年９月米国政府が公表した「国家サイバー戦略（National Cyber Strategy: NSC）」においてロシア、中国、イラン、北朝鮮の４カ国を安全保障上の脅威と認定した。これら４カ国は、既存の国際法を無視し、サイバー攻撃を行い、サイバー攻撃を通して米国と同盟国の民主主義と自由経済に打撃を与え、知的財産を奪っていると非難した。「国家サイバー戦略」では、米国のサイバー戦略が「拒否的抑止」から「懲罰的抑止」に移行していることはロシアにとって大きな脅威となっている。これまで米国は、自国の防衛能力を高め、相手に攻撃を断念する「拒否的抑止」を採用してきた。しかし、2018年を境に米国のサイバー戦略は、「相互確証破壊（MAD）」と同様、相手の攻撃に対して耐え難い攻撃を与えるという威嚇によって攻撃を断念させる戦略に転換した。この転換をロシアは「攻撃的なサイバー戦略」であるとして批判してきた。なぜならば、この転換はセイバーセキュリティのみならず、拡大するICTの軍事利用、具体的には人工知能（AI）を活用した兵器システムや自律型致死兵器システム（LAWS）という国際的規範が確立されていない分野にも及ぶことが懸念されるからである。そして、それは新たな戦争の領域の拡大と最新兵器の戦場での使用可能性に繋がる。更に、ロシアはインターネット上の偶発的な事故やサイバー戦争が核戦争にエスカレートすることを「原則」で憂慮している。このようなロシアの立場は国連GGE（Group of Governmental Experts）においても共有されており、

ロシアの主張は決して少数派ではない。世界規模で見るとインターネット利用者数は、米国は全体の9.5% に過ぎないが、中露を合わせると全体の20% を超える。さらに、BRICS諸国が加わると中露の提示するインターネット上の規範は圧倒的に多数派になることを付け加える必要があろう。

このように、ロシアや中国の論理は国連の場においても「国際安全保障の文脈における情報および電気通信分野の進歩」（決議 A/75/240）を通して情報通信安全保障問題を民主的で包括的かつ透明な協議プロセスを保証するため、国連主導の下、国連すべての加盟国が参加する定期会議を制度化することが合意されている。国際社会において最早多数派であるロシアや中国など権威主義諸国の抱える問題は、国家統合である。例えば、中国の抱える様々な諸民族を中国という国民国家の中に統合する際、国内体制に批判的な情報を情報空間に放置することは国家安全保障にとって重大な脅威となる。シュルスチュク論文はロシアにとっての「脅威」が何かを示唆している、と同時に情報空間の不安定化が国際安全保障に直接的に繋がるという警告を我々は聞く必要があるだろう。