旧ソ連圏における
多国間主義とサイバーセキュリティ

藤　巻　裕　之*

Cyber Security and Multilateralism in Post-Soviet Area

Hiroyuki FUJIMAKI

Abstract

The purpose of this paper is to discuss the difficulty to create a multilateralism in the international political environment after the Cold War (especially when pursuing the inclusion and participation of the Trump administration), nonethless, it has been easier to organize in a multilateral way when restricted to the Post-Soviet area. Within the current international political environment, it is espcially difficult to reach agreement on global issues, particularly regarding cyber space, because of the era of power transition. As a conclusion, the inability on cooperate with cyber security suggests that the future of multilateralism will be restricted to a more regional framework.

目次

＊東海大学政治経済学部政治学科准教授

はじめに

なぜ，国際社会ではサイバーセキュリティをめぐる普遍的なルールはつくられないのだろうか。第一次世界大戦時には，化学兵器の使用禁止に関する国際的取り決めが，第二次世界大戦後は核兵器，生物化学兵器に関する国際的取り決めが作られてきた。国際的ルールの作成にはその必要性を国際社会が認識することが前提となり，長い時間が必要とされる。サイバー空間における国際ルールの議論は1990年代後半から行われてきたが，未だ国際的なルールはつくられていない[1)]。

1990年代には冷戦の終結によって社会主義国家が民主主義国家に移行したこととそれに伴う混乱で援助を必要とする国家が増加したことで国際社会の制度化は進んだ。同時に，国際社会は冷戦後の新たなグローバリゼーションにおいて一国では対応出来ないグローバルイシューは容易に国境を越えることを学んだ。そのことは，諸国家をより容易に協力させる土壌を作り始めたかに見えた。しかし，米国トランプ（Donald Trump）政権の発足はそのような多国間主義（multilateralism）を基礎としたグローバルな国家間協力が機能不全に陥っている。

サイバー空間をめぐる国家間の協力も限定的である。国際政治におけるサイバーセキュリティ研究において前提となることは，サイバー空間のルールをめぐる欧米諸国と中国とロシアなどのユーラシア諸国，それぞれの論理を理解することである。欧米諸国にとってサイバー空間は既存の国際法で対応できることであり，新たな多国間主義を構築する必要はない。しかし，中国やロシアをはじめとする旧ソ連諸国にとっては，既存の国際法で対応するにはサイバー空間における国家への情報攻撃は国家の正統性に関わるため，各国はそれぞれの主権において情報を管理するべきであると考える。

本稿の目的は，冷戦後，特に昨今の国際政治環境が多国間主義を構築するのに困難であることをいくつかの例をあげて検証し，特にロシアを中心とする旧ソ連諸国のサイバー空間における論理と多国間主義の取り組みを整理することである。はじめに，冷戦後の多国間主義を構築する際の障害となってきた国際的イベントを紹介する。それによって発生した欧米諸国と中露を中心とした旧ソ連圏に分断されたサイバー空間をめぐる国際政治状況を整理することでサイバー空間における普遍的な合意形成の困難さを探る。

1．冷戦後の多国間主義

戦後国際社会は，米国のつくった国際秩序を共通のルールとして，また自国の行動原則

とすることで維持されてきた。史上最強ともいえるパクス・アメリカーナは，覇権国米国の国家目標と規範を国際社会において普遍性を与えるために，その経済力，科学技術力，軍事力，そして強力な政治的意思によって「大国間の，長期にわたる，大規模戦争を阻止しえた状態」として実現されてきた[2)]。その過程においては，安全保障，国際貿易制度，核兵器，化学生物兵器を含む大量破壊兵器の管理，人権など多岐に渡る国際的合意によって秩序が構築されてきた。旧ソ連圏，中国を含む国際社会は，冷戦後においても米国のつくった国際秩序に普遍性を見出してきた。むしろ，冷戦後の米国による一極体制は90年代のグローバリゼーションを加速させ，ロシアを含む旧ソ連諸国や中国は積極的に国際経済に統合するための努力をした[3)]。

戦後の多国間主義は，米国が掲げてきた自由市場や民主主義といった普遍性を持った理念を米国主導の国際組織とシンクロさせることで実現させてきた。多国間主義とは３ヶ国以上の複数国家が政府間協議を通して一定のルールを制定し，国際秩序の維持をはかる制度である[4)]。また，多国間主義の正統性は，多国間制度を通じて各国が自国民の権利と利益を保証できるかにかかっているが，前述のように経済的なグローバリゼーションには大きく貢献したが，自国民の権利と利益を守るという点において批判の対象ともなっている[5)]。

冷戦後，多国間主義がなぜ機能しないのか。戦後の米国大統領として異例の新興国による挑戦を受けている米国トランプ政権は「米国第一主義」を掲げて国際社会共通の利益よりも自国の国益を優先することを躊躇しない。このような背景をもとに国際社会において多国間主義を妨げるいくつかの要因について a. ～ d. を用いて試論を試みたい。

a．カプチャンの議論をもとに

カプチャンは，冷戦の終焉の際に国際的な戦後処理がされなかったことが現在の国際社会の混迷の原因であるとしている。図表１のように主要な戦争の後には大抵新たな戦後秩序が構築されてきた。戦後処理とは単に和平条約の締結ではなく，むしろ起こってしまった戦争の原因を取り除くための新たなルールや仕組みをつくりだすことが重要なのである[6)]。三十年戦争後のウェストファリア体制は国民国家体系を構築した。ナポレオン戦争後のウィーン体制はヨーロッパの協調と呼ばれる勢力均衡と平和を尊重する規範を基礎とした協調体制はその後長くヨーロッパに戦争のない状態をもたらした。第一次世界大戦後の世界では，勢力均衡よりも集団安全保障という実験的な国際機構によって秩序を構築した。その体制は，第二次世界大戦を予防することができなかったが，国際社会に人権，化学兵器の使用の非人道性を国際社会が共有する機会となった。そして，第二次世界大戦の終結は新たな覇権国である米国によるグローバルな勢力均衡に裏打ちされた集団安全保障体制と

図表１　主要な戦後処理と新しい秩序構築

三十年戦争後	ウェストファリア条約 -国民国家体系の構築
ナポレオン戦争	ウィーン条約 －コンサートオブヨーロッパ： 共通の欧州的価値と勢力均衡
第一次世界大戦後	国際連盟規約 －集団的自衛権
第二次世界大戦後	国際連合 －ダンバートン・オークス会議： ブレトン・ウッズ体制
冷戦後	新たな条約に基づく体制はなし －二極体制→一極体制への転換 －一極体制→多極体制への転換

（チャールズ・カプチャン『ポスト西洋世界はどこに向かうのか―「多様な近代」への大転換』p. 233-234をもとに筆者作成[8)]）

市場経済と民主主義という新たなルールが作られた。しかし，冷戦の終焉において一連の戦後秩序は構築されず，米国のつくった秩序は基本的にそのまま継承された[7)]。

その後，2001年９月11日の非国家主体によるテロ攻撃は，冷戦後の新秩序構築というアジェンダから国際社会，主に先進諸国を対テロ戦争という更に離れた地平へと追いやったのである。その後，米国の外交政策はテロの脅威とアフガニスタン，イラクでの戦争にかかりきりになった。その間に，中国の経済成長はGDP世界第２位を達成し，その国力に見合った国際的地位を国際社会で主張する国家に変貌した。

ｂ．クリミア半島の併合と米ロ関係

クリミア半島の帰属問題は，我々に改めて冷戦後の非対称となった東西関係を考える機会を与えた。その機会とは，ワルシャワ条約機構（WTO）の解体に関する合意，つまり，東西間の軍事同盟の不拡大という了解が米国と西欧によって一方的に破棄されたことである[9)]。更に，その後のユーラシアの安全保障政策を欧米諸国がロシアと北大西洋条約機構（NATO）で結んだPfP（Partner for Peace）を無視して進めたことが，東欧諸国とロシアにとって「最も近い」外国である旧ソ連諸国がロシア離れを加速したとロシアに考えさせた。更に，2004年のG8で米国が示した「大中東構想」，前述の「アラブの春」などは，中央アジアにおいてもレジーム・チェンジ（体制変換）を起こすきっかけとなった。特に，リビア，エジプト，そしてシリアへの欧米諸国の介入と中央アジア諸国で起こった一連の「カラー革命」はプーチン（Vladimir Putin）に危機意識を強めさせた。プーチンからすれ

ば，米国による権威主義体制国家に対する民主化政策は，破綻国家か権威主義体制へ逆戻りするという結末であった。その結果，アルカイーダやISなどのイスラム原理主義者達が欧州を含むユーラシア全体に拡散したとプーチンは考えた。

c．「アラブの春」が呼び起こしたサイバー空間と主権の関係

2010年に中東において「アラブの春」と呼ばれる一連の民主化の波が起こった。同年12月から翌年１月にかけてチュニジアでの民主化要求運動「ジャスミン革命」によって長期に渡ったベン・アリ（Zayn al-Abidin bin Ali）政権が崩壊した。民主化デモが市民によって録画され，画像や動画がFacebookやYouTubeにアップロードされた。海外に在住するチュニジア人によって情報が海外に拡大したことによって，2011年１月14日から二日間の間にチュニジアでの民主化運動関連のツィートのうち32％が海外から世界に発信された[10]。

2011年１月頃の大規模な民主化運動は反政府デモと化し，その後約一月の間に旧ムバラク政権はエジプト軍最高評議会に国家権力を譲渡し，29年に渡る長期政権が終わった。エジプト政府は，この民主化運動初期の１月29日から５日間に渡りインターネットへの接続を遮断したが，その後インターネット復旧後国内のFacebookへの加盟者が爆発的に増加した。また，１日2300件だった国内外からのツィート数も革命中には23万件に増加し，約550万人の海外からの閲覧者がいたとされる。

そして，リビアへも「アラブの春」は波及した。2011年２月にカダフィ（Qadhafi, Muammar Mohammed Abu Mynyar）大佐の退陣を求める反政府デモが拡大し，８月には42年もの長きに渡るカダフィ政権が終焉した。リビア政府は，インターネットの普及を意図的に限定して管理しており，また他の中東の民主化運動に比べてもインターネットの役割は限定的だった。

イエメンを含めた「アラブの春」を経験した政府は一様にインターネットの遮断とソーシャルメディアへのアクセスの制限を行ったが，結果的には，むしろ国際社会の関心を向けさせた。ロシアや中国，また旧ソ連諸国にとって，容易に国境を超えるFacebook，YouTube，Twitterなどの情報空間を経由した市民の情報共有は「アラブの春」を引き起こし，主権国家の正統性を揺るがしたのである。

d．情報セキュリティ：中国と旧ソ連諸国の新たな脅威

冷戦後の旧ソ連諸国と中国にとって安全保障上の最大の脅威は，もはや国家対国家ではなく，主権の保全と非国家主体からの攻撃に対応することである。それまで，ほとんどの場合これらの諸国は，自国の安全保障をロシアや中国のような地域大国に依存することで自国の政治的経済的独立を維持してきた[11]。ところが，前述のように独立国家共同体

（CIS）が機能不全に陥った原因をロシアの外交政策が伝統的安全保障観から脱却できずにいた点に求めるとすれば，ロシアと中国が非伝統的安全保障分野での協力を重視しはじめたことが，旧ソ連諸国に対してある種の地域的公共財を提供してきたと考えられる。なぜならば，上海協力機構（SCO）加盟各国が特に留意した問題は，サイバー空間を活用して主権を危うくする国内外の勢力による情報攻撃から政権の正統性を守ることだからである[12)]。冷戦後の中央アジア諸国に挑戦する脅威とは，「脅威の特定が困難」であり，「所在の確定が困難」な組織犯罪（ドラッグ，人身売買など），テロリスト，分離主義，そして，反政府組織の存在である[13)]。それらの要因が中央アジア諸国に集団自衛的発想に基づく地域主義の組織化へのニーズを高めているのである。

このように，冷戦が終結したことで，軍事面を中心とした安全保障の規範から，より広い脅威に対応するために非伝統的安全保障分野の確立が急務となった。このように，非国家主体が冷戦後の新たな脅威として国際社会で認識されて久しい。もちろん，非伝統的安全保障は冷戦期も存在していたが，冷戦後に表面化したのには理由がある。一つには，冷戦期にイデオロギーによってソ連という共同体に押し込められていた，国家に対する潜在的な脅威が表面化したことである。二つには，1997年のアジア経済危機である。東南アジアを直撃した大規模な経済危機は，アジア，旧ソ連圏の貧困層をさらに貧困にした結果，組織犯罪による貧困層を中心とした犯罪ネットワークが活性化した。三つめには，2001年の9.11以降，米国による中東と中央アジアへの積極的な軍事介入が始まった。その結果，そもそも不安定な地域がさらに不安定化し，テロや犯罪組織への人員の補充も実現したのである。

2．多国間主義とサイバーセキュリティ

我々の社会生活は，IT 分野における科学技術の発展に多大な依存をしているだけでなく，政治システムにまでその範囲は拡大している。例えば，選挙，電子政府，ソーシャルメディアによる政治参加，e-Japan などは，サイバー空間と現実政治をポジティブに現実化している。と同時に，サイバー空間における我々の政治行動，経済活動そして社会活動は国境を用意に超えるサイバー攻撃に日々晒されている。しかし，現実にはサイバー空間におけるグローバルに統一されたルールも設けられていないだけでなく，争いに至った場合の調停者も不在なのが現状なのである。

2015年８月，国際連合（UN）における政府専門家会合（GGE）は，既存の国際法がサイバー空間に適応可能であるという欧米諸国の立場，または中露を中心とした新興諸国が支持する新たな普遍的な規範をつくるべきであるという二つの潮流の存在を明らかにする

機会となった。国連を舞台にしたGGEでの議論は現状を明確に次のように分類している。中国やロシア，さらに発展途上国の多くは，サイバー攻撃は国家主権の問題であり，国家が責任を持ってサイバー空間を管理すべきだと考えている。それに対して，米国や欧州の国々，そして日本は，人権や自由の確保を尊重し，政府による過度な規制や介入は望ましくないと考えている。そもそも，サイバースペースやインターネットは特別な存在ではないことから，わざわざ議論し，合意をつくるまでもないという立場である[14)]。

「リベラル」な先進諸国による国家集団，例えば英国，日本，ドイツ，そして北欧諸国が重視するサイバー空間の問題は，情報ネットワークや金融取引システム，通信システムへのサイバー攻撃である。それらは，このグループを構成する諸国にとって重要な国家安全保障上の問題である。

米国を中心とする先進諸国のサイバー空間への立場は，基本的に国際法を基礎としている。2015年9月に中国で行われたG-20でバラク・オバマ（Barak Obama）大統領は，世界的な取り決め，規範，ルールがないサイバー空間を米国開拓時代の無法地帯を表す“Wild Wild West”と呼び，そうならないために米国は国際法を応用することに普遍性を与える努力をしていると述べた[15)]。

それでは，米国はサイバー空間においてどのような国際的な枠組みを推進してきたのだろうか。サイバー攻撃は，国境を容易に超える犯罪であるため，その防止と抑制のためには迅速に緊密な国際的協調体制に基づく情報共有が必要と考えられている。また欧州においては，サイバー攻撃を国際法上の犯罪として認識を共有して立件するには証拠保全や適正手続の確保のために法的拘束力のある国際文書が必須であるということが欧州評議会で議論されてきた[16)]。欧州評議会サイバー犯罪条約（ブタペスト条約）はサイバーセキュリティ分野における米国を中心とした先進諸国間が合意する最も重要な多国間条約である[17)]。ブタペスト条約は，欧州評議会という欧米を中心とした先進諸国に属する国家群を構成国とし，同じ脅威を共有するクラブと認識されている。しかし，ロシアが同評議会メンバーでありながら未署名なのは，サイバーセキュリティをめぐる議論には普遍性が存在しないことを示している。

3．中国と旧ソ連諸国にとっての情報セキュリティ

ロシアやSCO加盟国にとってサイバーセキュリティとは広く情報，コンテンツを含んで定義する。すなわち，欧米諸国や日本のようにインターネット空間を市場に任せずに国家が主導して管理をするべきであるとする。従来の国際法が適用されると言論の自由や通信の秘密などの人権がサイバー空間にも適用され，政府の介入や検閲がしにくくなる。欧

米諸国においては，ほとんどの場合サイバー空間における政府批判は言論の自由の範囲で保障されている[18]。しかし，権威主義体制においては，政府の正統性を批判する内外からの言論はサイバー攻撃と認識されている。なぜならば，そのような国家にとって治安の維持，体制の維持こそが最優先だからである。

本章では，欧米諸国の考えるサイバー空間における協力ではなく，旧ソ連圏諸国がどのようにサイバー空間のガバナンスを行っているのかを論じたい。旧ソ連圏諸国にとってのサイバー空間のような非伝統的な安全保障環境はどのように変化をして来たのか，グローバルな多国間主義が機能しない国際社会でサイバー空間の管理を旧ソ連圏諸国と中国はSCO を通してどのような地域的なガバナンスを構築しているのだろうか。

a．旧ソ連圏における安全保障環境の変化

ロシアのサイバー戦略と核戦略には類似性がある。米国に比べて通常戦力に劣るロシアの安全保障戦略は，戦略核戦力においてのみ対米均衡が可能である[19]。そのため，平時の通常戦力の不均衡を核抑止力によって保障しているため戦略核への依存度が高い。大規模な地域戦争以上の紛争に対応するためには，核の使用が戦略的な前提条件となり，また，それは大規模戦争のリスクを負うことになる。そのため，ロシアの安全保障における最も重要なことは，戦争の抑止，さらに言えば，多国間の戦略交渉や安全保障枠組みの交渉で主導権を握ることである。

実際にロシアは，2000年代後半から欧州安全保障条約の提案を行い，米国のミサイル防衛システムがロシアの脅威にならないこと，ならびに，NATO 拡大の制限を目指した[20]。ロシアは東欧諸国の安全保障にロシアの影響力を維持することを条件に欧州と東欧諸国の交流を黙認したが，結果的にロシアは東欧を勢力圏として維持することに失敗し，東欧を失った。また，冷戦後の国際秩序形成の過程で，欧州の一員に回帰しようとするロシアに対して，前述のように NATO は東方拡大と形だけのパートナーシップとも言える PfP で応えた。他にもロシアは新戦略兵器削減条約（新 START），中距離核戦力全廃条約（INF）などの軍備管理条約をロシアに有利な形でアップデートすることでソ連崩壊後に失った国際的地位を回復し，戦略環境や軍備管理の分野で主導権を握ろうとしている。

欧州安全保障条約とミサイル防衛システムの国際的な規範構築にロシアは力を注いできた。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いる。なぜならば，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。そうである以上，ロシアの目指す国際規範とは，現実世界の軍事戦略同様にサイバー攻撃そのものを禁止することを目指しているのである。

b．サイバー空間における SCO の取り組み

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，という立場から前述のサイバー犯罪条約（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[21)]。行動規範において国民国家の統合にとって脅威となりうる情報は国家の権利として認められ，またその考え方は SCO 加盟国間でも共有された[22)]。SCO はそもそもオールインワン型の安全保障，すなわち非伝統的安全保障，国家統合，分離主義，対テロ，麻薬，経済，エネルギー，社会，そして情報セキュリティなど非常に広範囲に活動範囲が含まれている[23)]。

地域対テロ機構（SCO RATS）は，情報セキュリティに関する「SCO 専門家グループ」を持ち，域内の情報セキュリティをめぐる情報共有が行われている[24)]。SCO RATS 主催「2015年中央アジアにおける反テロリズム訓練」（以下「厦門2015」）の一環として，「インターネット反テロ軍事訓練」が厦門で開催され，中国，カザフスタン，キルギスタン，ロシア，タジキスタン，ウズベキスタンが集まった。インターネット空間における監視活動やデータ管理を行う中国人民解放軍総参謀部（GSD）第３小部技術部は，国境管理やカウンター・テロリズムを想定した訓練を行っている。「厦門2015」は，SCO RATS と第３小部技術部主催で初めて開催された SCO メンバー諸国間によるインターネット空間における反テロ訓練であった。この訓練は，SCO 加盟国間で共有する “three evils”「３つ邪悪な脅威」であるテロリズム，分離主義，そして原理主義に対抗するための軍事訓練であり，特に，今回は情報セキュリティ分野を司る第３小部技術部が「３つの邪悪な脅威」と情報セキュリティにおいて重要な役割を果たした。この軍事訓練では，テロリストが SCO 加盟国内のインターネット空間を利用してテロ活動を行うことが想定された[25)]。この訓練で重視されたことは，SCO 加盟国間の協力関係と情報共有能力を高めることであった。

2013年９月に SCO は情報セキュリティ分野から成る「専門家グループ」を中心にサイバーテロリズムに対する法の執行を強化した。この訓練では，メンバー諸国による国境を超えた監視システムと情報共有によってサイバー攻撃の予防とサイバーテロのネットワークを特定するのが目的であった。中国国家インターネット情報局徐智敏次長はこれまで中国のインターネット上の監視システムとウォーニング・システムを強化するよう繰り返してきた。その背景には，ロシアと中国から IS への参加が目立つことから，インターネット上の国境を超えた監視システムと協力関係が不可欠だからである。SCO を土台とした

これらサイバー空間の協力体制は，現実世界でSCO域内からISへ参加するために国境を超え，そして，帰国しようとする最大の脅威である潜在的なテロリストや急進化した市民を特定することを目的としている。

c．ロシアは加害者なのか？

サイバー攻撃があった際に加害者，または容疑者として真っ先にあげられる国はロシアである。しかし，ロシアの情報空間の専門家によるとロシアも被害者であることを主張する。さらに，中国や中東の政府企業も被害者であるということから，サイバーセキュリティが単に攻撃国と被害国に分類できる類のものではいことは明らかである。

企業や個人からのサイバー攻撃ではなく，国家が主犯であるという明確な根拠を持った最初のサイバー戦争“cyber war”（サイバー犯罪ではなく）は，2010年頃に起こったイラン国内の核燃料施設でウラン濃縮用遠心分離機の破壊という物理的実害をサイバー攻撃によってもたらされた。スタクスネット（Stuxnet）はまた，それまで比較的安全だと信じられていた，インターネットに接続していない産業用制御システムにもUSBメモリーを介して感染・発症した。国家が主犯であるという根拠は，マルウェア（CM: computer Malware）の一種であるスタクスネットが国家主導の高レベルの専門家たちで作成され，使用されたからである。通常よりも複雑で用意周到な準備などからロシアのカスペルスキー研究所のE. カスペルスキーは，スタクスネットはイランだけでなくロシア国内においても被害が発見されたことを報告している。別の例では，2012年，2013年，2016年，2017年にマルウェアのShamoonを使ったサイバー攻撃がサウジ・アラビアの石油/天然ガス施設，関連企業を破壊するために行われた。その後，Shamoonによる攻撃はサウジ・アラビアの金融サービス，官公庁にも被害が及んだ。

ロシア連邦安全保障会議書記ニコライ・パトルシェフ（Nikolai Platonovich Patrushev）の報告によれば，国家機関のサイトに対するサイバーアタックの回数は増大傾向にあり，2015年は1,440万回，2016年には5,250万回前後に上り，１年間に３倍になったことになる。ロシア連邦保安庁の2017年のデータによれば，ここ数年のハッカー攻撃による世界の損失は，評価の方法により異なるが，３千億ドルから１兆ドルに達している。この額は世界のGDPの0.4から1.5（％）に相当するだけでなく，増大する傾向にある。国際テロ組織やいくつかの国が行う，きわめて重要な施設やインフラの運営を妨害する目的でのコンピューター機器の敵対的使用のリスクも高まっている。ロシア科学アカデミープリマコフ名称世界経済国際関係研究所（IMEMO）のN. P. ラマシキナ（N. P. Romashkina）によれば，90年代から始まった情報空間をめぐる情報セキュリティを議論する国際的な枠組みと脅威を測定する共通の方法論の欠如は国家ならびに国際セキュリティの重要な問題である[26)]。

また，サイバー攻撃を扱う国内および国際法上の共通の規範がないことも同様に国際社会の危機である。国際社会で尊重されるべき政策枠組みは緊急に必要であり，それこそは，情報セキュリティにおけるグローバルなガバナンスと規制が国際政治と国際法で機能する前提条件であると考えられている[27)]。

モスクワ国立大学情報セキュリティ研究所（IISI）の主導する「国際情報安全保障条約」における主張の一つには，様々なコンピューター機器を通して他国が主権国家の内政に干渉する手段として使われることも，国際情報セキュリティ上の脅威として認識する必要があるとしている[28)]。もう一点は，情報空間の軍事利用を禁止して他国の内政に干渉しないことと，国家のデジタル主権を無条件に認めることである。ロシアにとってサイバー空間とは国家主権が及ぶ範囲であり，サイバー空間は現実の国家安全保障の議論の及ぶ範囲なのである。しかし，前述のようにロシアと米国のサイバー空間の力は歴然であるため，ロシアとしてはむしろサイバー空間における軍縮を進める意思を持っている。それに対して，2011年５月米政府は “International Strategy for Cyberspace” を発行し，米国はサイバー攻撃におけるアトリビューションの問題が解決出来ない以上，サイバー攻撃に対する報復は一般的な軍事力で対応するという案を持っている[29)]。

おわりに

本稿では，はじめに現在の国際政治環境が多国間主義を構築する上で困難な状況にあることを a. 〜 d. を通して検証した。はじめに，カプチャンの研究をもとに戦後秩序の構築を史的な視点から概観し，冷戦後の国際政治環境にはこれまでのような普遍性を持つ条約や新しい秩序構築がなされなかったことに加え，米国の中東への過剰なコミットは新興国の台頭を許し，多国間主義を困難にした。次にクリミア半島の問題は米ロ関係を冷却化し，そして，中東で起こった一連の民主化運動は更に中国と旧ソ連圏諸国に主権を維持することの重要性を再認識させた。最後に，中国と旧ソ連諸国にとっての共通する脅威が国家から非国家に移行したことは，中国と旧ソ連諸国の地域的な多国間主義を容易にしたことを指摘した。

そして，現在の国際政治環境は第１章で述べた様に諸国の協力が困難であるだけでなく，我々の生活に密着し，また国際安全保障においても極めて重要なサイバー空間をめぐっても同様に国際的な協力体制が構築できないのが現状である。本稿では，米国をはじめとする欧州，日本の論理と中国と旧ソ連諸国の論理に分けて整理を行った。

結論としては，サイバー空間における多国間主義の構築は困難と言わざるを得ない。特に米国トランプ政権後の自国優先主義は，戦後から米国オバマ政権まで続いた国際協力の

正統性が崩れ始めるのを加速させた。覇権安定論やパワー・トランジッション（またはパワー・シフト）の議論を借りるまでもなく，覇権の移行期にサイバーセキュリティという重要なグローバルイシューを多国間主義で協力できないことは，今後の多国間主義がより地域的な枠組みに限定されていくことを示唆している。冷戦終結後，先進諸国と旧ソ連圏においてグローバルな新秩序が構築されなかったことは，中国と旧ソ連圏に比較的容易にサイバーセキュリティ分野の地域協力を実現させたのである。サイバーセキュリティ分野においても今後はその様に地域的な枠組みに限定された協力関係が維持されるのか，または，サイバー空間における普遍的な国際枠組みが見直されて多国間主義が復活するのか注視する必要がある。

註

1）例えば，モスクワ国立大学情報セキュリティ研究所（IISI）のシュルスチュク所長によれば，1998年９月にロシア外相 I. S. イワノフ氏が当時のコフィ・アナン事務総長に送った書簡において言及された。よくとしの1999年の国連総会において「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」を議題とする決議がなされ，情報通信技術（ICT）の軍事，テロリズム，犯罪への利用という，国際情報セキュリティにおける「３つの脅威」が初めて提唱された。Vladislav P. Sherstyuk, *Keynote Speech*, “Tokai University 75th Anniversary Memorial International Cyber Security Symposium”, Organized by Strategic Peace and International Affairs Institute of Tokai University, Information Securiuty Institute of Lomonosov Moscow State University, 東京，2017年12月１日。

2）滝田賢治「序章　国際政治史の中のアメリカ」『アメリカがつくる国際秩序』ミネルヴァ書房，2014，２頁。

3）ロシアの民主化，および，ロシア企業の民営化は以下を参照されたい。Marshall I. Goldman, *The Privatization of Russia: Russian Reform Goes Awry*（NY: Routledge, 2003）. Chrystia Freeland, *Sale of the Century: The Inside of the Second Russian Revolution*（London: Abacus, 2003）.

4）Ruggie, John G. “Multilateralism: The Anatomy of an Institution,” John Ruggie, ed., *Multilateralism Matters: The Theory and Praxis of an Institutional Forum*, New York: Columbia University Press, pp. 3-47.

5）山田高敬「第３章　多国間主義から指摘レジームへ - マルチステークホルダー・プロセスのジレンマ」『日本の国際政治学　第２巻　国境なき国際政治』日本国際政治学会編，有斐閣，2009年，60頁。

6）チャールズ・カプチャン『ポスト西洋世界はどこに向かうのか―「多様な世代」への大転換』勁草書房，233頁。

7）前掲，カプチャン，234頁。

8）前掲，チャールズ・カプチャン『ポスト西洋世界はどこに向かうのか―「多様な世代」への大転換』勁草書房，233-234頁。

9）下斗米伸夫『宗教・地政学から読むロシア』日本経済新聞社，2016，５頁。

10）Mathew Ingram, “Was what happened in Tunisia a twitter revolution?”（https://gigaom.com/2011/01/14/was-what-happened-in-tunisia-a-twitter-revolution/, access: 2018/05/1）.

11）藤巻裕之「地域統合論の理論的展開―旧ソ連圏のケースを中心に―」『東海大学教養学部紀要』，第44号，2013，東海大学出版会，56頁。

12）旧ソ連諸国と中国にとって知的財産や国家インフラを標的にしたサイバー攻撃と同等に国家主権に挑戦するより広い概念である「情報」の方がより深刻である。

13）Stephen Aris, *Eurasian Regionalism: The Shanghai Cooperation Organization*（London: Palgrave Macmillan, 2011），100頁。

14）土屋大洋「国連を舞台に，サイバースペースをめぐって大国が静かにぶつかる」NEWSWEEK, 2015年 9 月15日，（https://www.newsweekjapan.jp/tsuchiya/2015/09/post-3_2.php, 2018/04/04 access）。

15）NICOLE PERLROTH and DAVID E. SANGER “Obama Calls for New Cooperation to Wrangle the ‘Wild West’ Internet”, 2015/2/14, https://www.nytimes.com/2015/02/14/business/obama-urges-tech-companies-to-cooperate-on-internet-security.html?_r=0（access: 2017年５月15日）。

16）「サイバー攻撃に対する国際社会と日本の取り組み」http://www.digitalforensic.jp/archives/2011/1105.pdf（access: 2017年５月20日）。

17）須田祐子「サイバーセキュリティの国際政治」日本国際政治学会編『国際政治―科学技術と現代国際関係』第179号（2015年２月），58-59頁。ちなみに，ブタペスト条約締約国は，米国，英国，ドイツ，フランス，イタリアなどである。

18）土屋大洋『サイバー戦争とセキュリティと国際政治』千倉書房，2015年，156頁。

19）佐々木孝博「ロシアの安全保障における核戦略とサイバー戦略の類似性」『ディフェンス』51号，125頁。

20）前掲，佐々木，134頁。

21）Keir Giles, “Russia’s Public Stance on Cyberspace Issues”, 2012 4th International Conference on Cyber Conflict, C. Czosseck, R. Ottis, K. Ziolowski eds.）https://ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf（access: 2017年５月10日）.

22）モスクワ国立大学情報セキュリティ研究所（IISI）は，ロシアの情報セキュリティへの取り組みの基本姿勢をつくり，また「国際情報安全保障条約」の原案作成を担った。2017年４月24-27日に Garmisch-Partenkirchen で開催された “Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security” においてもロシア側は一貫してサイバー空間における主権の重要性と国連を中心とした国家間の対話枠組み構築の重要性を主張した。

23）藤巻裕之「サイバー空間における秩序構築―旧ソ連圏地域主義の視点から―」『ロシア・ユーラシアの経済と社会』ユーラシア研究所，2017年７月号，7-8頁。

24）RATS news, “Competent authorities of SCO member states holds Xiamen-2015 joint-command-post exercises on countering the use of internet for terrorism, separatism and extremism activities”, 2015年10月14日，http://ecrats.org/en/news/5126（access: 2017年５月25日）.

25）Peter Wood,“China Conducts Anti-Terror Cyber Operations with SCO Partners”, October

19, 2015, https://jamestown.org/program/china-conducts-anti-terror-cyber-operations-with-sco-partners/（access: 2017年５月20日）.

26）N. P. Romashka, A. V. Zagorskii,“Information Security Threats During Crisis and Conflicts of the XXI Century”, Primakov Institute of World Economy and International Relations, Russian Academy of Sciences, Moscow, 2012, 16頁 .

27）前掲，Romashka, 16頁。

28）前掲，Sherstyuk 報告より。

29）“International Strategy for Cyberspace”，https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf（access: 2018/05/01）.