第７９０号

令和３年３月１日

公益社団法人　安全保障懇話会
発行所　東京都新宿区若松町１８－３
電話　３２０２－８６３１　㈹

安全保障を考える

ロシアが恐れるサイバー空間の脅威と核の脅威

広島大学大学院社会科学研究科客員教授
東海大学平和戦略国際研究所客員教授
研究班　佐々木孝博

はじめに

周辺諸国及び核大国の米国に対し、過剰な防衛意識をもつロシアでは、近年、確実な安全を求めて、非軍事・軍事(1)のあらゆる手段をもって戦う「ハイブリッド戦(2)」という戦い方を推し進めている。

ロシアの「ハイブリッド戦」という戦い方が、文書として初めて明らかになったのは、2013 年２月にゲラシモフ参謀総長によって発表された安全保障論文「先見の明における軍事学の価値」と言われている(3)。その内容は、後に、「国家安全保障戦略」及び「軍

(1) 非軍事手段及び軍事手段の区別・定義については、様々な捉え方がある。例えば軍事組織が行うサイバー攻撃は、軍事手段なのか否かといった疑問である。ロシア研究を行う本稿では、西側諸国の認識とは異なるものもあるが、極力、ロシア当局が考える（または規定する）区分・定義を記述する。
(2) ロシアは自らの戦い方を「ハイブリッド戦」と呼称したことはなく、西側諸国がそれをロシアが近年実地に行動する情勢を解釈したうえで名付けた名称である。そのため、ロシアが考えている戦い方と西側諸国の捉え方の間で、齟齬がある場合もある。本稿ではロシアが「新た世代の戦い方」と呼称している戦い方を「ハイブリッド戦」と呼称することとする。
(3) ヴァレリー・ゲラシモフ「先見の明における軍事学の価値（ロシア語）」『軍事産業クーリエ』2013 年 2 月 26 日<https://www.vpk-news.ru/articles/14632>（2021 年 1 月 10 日アクセス）。

事ドクトリン」などの戦略文書に反映された。

ロシアが考えるこの「ハイブリッド戦」では、「情報戦」「サイバー戦」「影響工作（Influence Operation）」といった非軍事手段による戦い方を重視し、「戦わずに勝つ」「いざ戦う状態に陥ったならば圧倒的な優位な情勢を作為し実戦闘を勝ち抜く」といったことを目指している。しかしながら、その戦い方のみではロシアの安全は確実には担保されず、最後の拠り所として核戦力にも大きく依存している。

そこで本稿においては、まず、既報告「ロシアが推し進める『ハイブリッド戦』の概要とその狙い」【安全保障を考える第 780 号（令和 2 年 5 月 1 日）】を振り返り、近年ロシアが推し進める「ハイブリッド戦」という戦い方において、ロシアが紛争・戦争の段階と核戦力をどのように位置づけているのか、「ハイブリット戦」と核戦力をどのようにとらえているのかを考察していく。次に、筆者が参加したロシア主催の国際情報安全保障に関するシンポジウムにおけるロシア側の発表を取り上げ、ロシアがサイバー空間における脅威をどのように捉え、それが核戦略にどのように影響していると考えているのかを明らかにしていく。最後に、ロシアが当該分野において、戦略的安定性を積極的に推進する狙いについても考えてみたい。

１　紛争・戦争の段階と核戦略(4)

（１）「ハイブリッド戦」と核戦力の位置づけ

ロシアは従来から「軍事ドクトリン(5)」において、紛争・戦争のレベルを「武力紛争(6)」「局地戦争(7)」「地域戦争(8)」及び「大規模戦争(9)」の４つの段階に区分している。冒頭に述べたゲラシモフ参謀総長論文で一義的に強調しているのは「国際間紛争対処」で

---

(4) この項、渡部悦和、佐々木孝博『現代戦争論－超「超限戦」』（ワニブックス 2020 年 7 月 8 日）に基づいている。

(5) ロシア安全保障会議「ロシア連邦軍事ドクトリン（ロシア語）」『安全保障会議 HP』2014 年 12 月 25 日<http://www.scrf.gov.ru/security/military/document129/>(2021 年 1 月 10 日アクセス)。

(6) 「軍事ドクトリン」の規定による「武力紛争」とは、限定された規模の、国家間のまたは１つの国家の領域内の対立する当事者間の武力衝突のこと。

(7) 「軍事ドクトリン」の規定による「局地戦争」とは、２国またはそれ以上の数の国家間の、限定された軍事・政治的目的を追求する戦争であり、戦っている国家の領域内に軍事行動が留まり、主としてこれらの国家の利益のみに関わるもののこと。

(8) 「軍事ドクトリン」の規定による「地域戦争」とは、１つの地域の２つ以上の国家が参加し、自国軍または同盟軍によって行われ、通常撃破手段も核撃破手段も使用され、地域の領域及びその周辺の海域並びにその上空で行われる戦争であり、当事者が重要な軍事・政治目的を追求するもののこと。

(9) 「軍事ドクトリン」の規定による「大規模戦争」とは、国家同盟間または国際社会の最大規模の国家間戦争であり、当事者は根源的な軍事・政治目的を追求するもの。武力紛争、局地戦争または地域戦争に世界の様々な地域の著しい数の国家が関与しエスカレートしたもの。

ある。それは、「軍事ドクトリン」で規定しているところの４つの段階のうち、最も烈度の低い「武力紛争」を対象にしているものと考えられる。ロシアが 2000 年代以降に実戦として武力を行使した「グルジア（ジョージア）紛争」「ウクライナ危機（クリミア併合)」「シリアへの軍事介入」などがここで掲げる「武力紛争」に該当する。これは、「ハイブリッド戦」の戦い方が生まれた背景に「アラブの春」や「カラー革命」があったこと、及び対象となる戦い方について「紛争」という用語を使い、「戦争」という用語を使用していないことからも導き出すことができる。

このようにゲラシモフ論文で強調されていたのは、「局地戦争」以上に至る前の「武力紛争」を一義的に念頭においたハイブリッド戦であると言える。しかしながら、あらゆる手段を融合させ、あらゆる領域において同時に戦闘を行うハイブリッド戦というものは、従来からもロシアは実施してきており、また、低烈度から高烈度に至るどの紛争・戦争の段階においても実施されるものである(10)。そのカテゴリーに従来ではあまり言及されてこなかった「サイバー領域での戦い」、「電磁波領域での戦い」、「認知領域での戦い」というものが加わったとも言えるだろう。

「軍事ドクトリン」では、「武力紛争」が「局地戦争」以上にエスカレートした場合には、「戦略核の抑止下における『局地戦争戦略』『地域戦争戦略』『大規模戦争戦略』」に移行するとしている。ロシアは、戦争・紛争の段階とは直接リンクせず、核兵器の使用規定というものを定めており、「ロシア及び同盟国に対し、核兵器その他の大量破壊兵器が使用された場合及び通常兵器がロシアに対し使用された侵略に対して、国家存亡の危機に立たされた場合の対抗手段として核兵器を使用する権利を保有する」と規定している(11)。すなわち、通常戦力での戦いにおいても国家存亡の危機に立たされたと大統領が判断した場合は、戦術核を使用し、それを補完する場合もあるということである。さらにエスカレートする場合は、戦略核の使用も辞さないとの強い対応による抑止戦略も採用しているということだ（図１参照)。

実際、クリミア併合時にもロシアは核兵器の準備をしていたということが、後に判明している。「クリミア併合」から１年が経過した 2015 年の３月に、プーチン大統領はウクライナ紛争を総括した席上で、「クリミア紛争時、核兵器の使用を準備してい

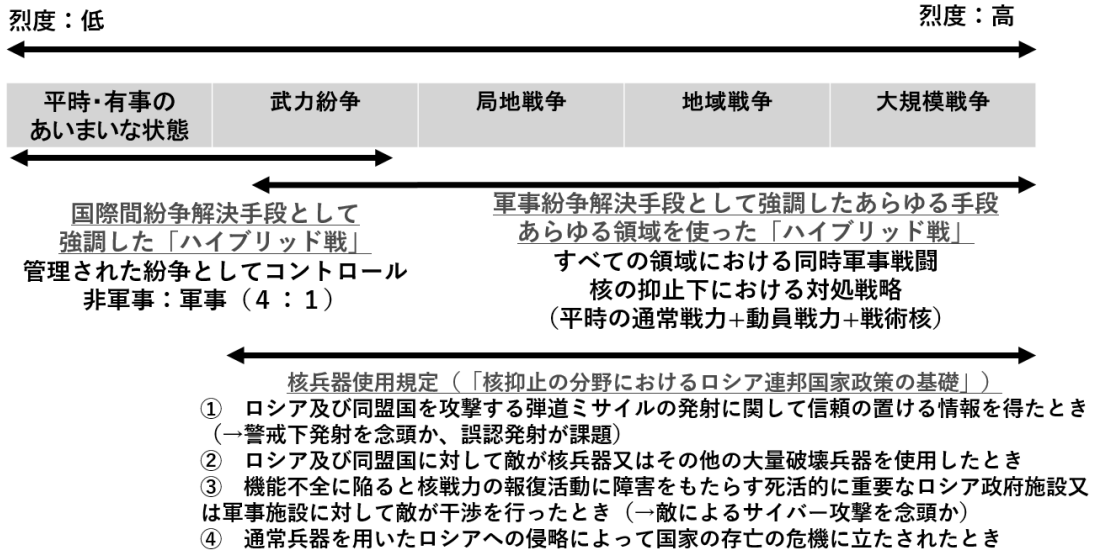
---

(10) 米軍のハイブリッド戦の認識は、１つ目のグレーゾーンから「武力紛争」までを範囲として認識している。２つ目の範囲は、米軍においてはマルチドメイン作戦が実施される範囲であり、ハイブリット戦が実施される範囲とは認識していない。この点で米露には認識の違いがある。それは、根本でロシアが自らの戦略をハイブリッド戦と呼称していないことからも認識の違いがあることを読み取ることができる。

(11) 核兵器の使用規定については、2020 年６月に改めてロシア政府から発表があった。詳細は、時事通信「弾道ミサイル情報で攻撃―軍縮協議にらみ使用条件公表（2020 年６月２日)」参照。

た」と明言した(12)。政治的なブラフとしての発言とも受け取れるが、核兵器の使用規定を鑑みると、ロシアが戦争・紛争の段階に関わらず、国家存亡の危機に直面したと判断した場合には、核兵器の使用も辞さないとの戦略を保持している証左と受け取ることが妥当であろう。

図１　戦争・紛争の段階と核兵器使用規定(13)



（出典：ロシア安全保障会議「軍事ドクトリン」等各種戦略文書を基に筆者作成）

ただし、ここで「武力紛争」の段階においても国家存亡の危機という状態が生起し得るのかとの疑問が生じてくる。この疑問の背景には、西側との考え方の違いがあり、小泉悠氏が主張する「小規模な紛争をエスカレーションラダーによって抑止するのではなく、その紛争規模に応じた戦術核使用へのエスカレーションで直接抑止することを想定する『エスカレーション抑止』という考え方(14)」がロシアの戦略の根底にあるということだ。この考え方を具現化するために、ロシア当局が、核兵器使用規定を、戦争・紛争の段階には言及せず「ロシア及び同盟国に対する核兵器その他の大量破壊兵器の使用及び通常兵器によるロシアへの侵略で国家存亡の危機に立たされた場合」と規定し、大統領が判断すれば、弾道ミサイルの発射の恐れやサイバー攻撃などによりロシアの核兵器が無力化される場合などを含め、どのような情勢であろうと

(12) ロイター通信「プーチン露大統領、クリミア併合で『核兵器を準備していた』」『ロイター通信 HP』2015 年 3 月 16 日<https://jp.reuters.com/article/ptin-idJPKBN0MC03220150316>（2021 年 1 月 10 日アクセス)。
(13) 同上。
(14) 秋山信将、高橋杉雄、小泉悠ほか「『核の忘却』の終わり」『勁草書房』2019 年 6 月。

「国家存亡の危機」との理由で戦術核兵器を使用できるようにしたと考えられる（図１参照）。

（２）核戦力を巡る最近の動き[15]

2019 年には、米露の核戦力を巡って大きな動きがあった。２月に、米国が中距離核戦力（INF：Intermediate- range Nuclear Forces）全廃条約破棄（以下、INF 条約）の方針を打ち出し、その後、８月には同条約は規定により失効したという事案である。

そこでこれらの情勢から、核戦力を巡るロシアの狙いを、重要となる INF 条約及びその先にある戦略核兵器削減条約（START：STrategic Arms Reduction Treaty）[16]を中心に見ていきたい。

● INF 条約に対する米露の対応

共同通信によれば、エスパー米国防長官（当時）は 2019 年８月３日、記者団に対し、米露の INF 条約が失効したことを踏まえ、アジア太平洋地域に地上発射型中距離ミサイルを配備したいとの考えを示した。この動きは中国への対抗が念頭にあるとみられ、アジア地域では既に中国による INF は増強されている状況で、条約失効を受け、米中露の軍備増強が進む恐れがある。エスパー長官は配備の時期について「数ヶ月でできればいいが、それ以上かかるだろう」と述べた。米国は、中国が南シナ海で、米軍の空母も標的となり得る対艦弾道ミサイルの発射実験を行ったことを強く警戒しており、東アジアへの INF の配備に傾きつつある[17]。

このエスパー長官の方針が実現に移されると、東アジアで INF の配備が考えられる地域は、韓国（在韓米軍）、日本（在日米軍）、グアム、台湾などが想定される。しかしながら、各々の国（地域）は、様々な否定的な要件を抱えており、米国の考え通りに同地域に中国を睨んだ INF が配備されることは考え難い。

そのような見地からすると、中国の INF に対抗するための米国の中距離ミサイルの配備は、INF 条約の範疇外ではあるが、トランプ政権が発表した「2018 Nuclear Posture Review」で配備を企図していることが判明した低威力核弾頭搭載 SLBM や海兵隊への核弾頭搭載ミサイル配備により、必要時にこの地域への展開を可能にする等の方策が当

---

(15) この項、渡部悦和、佐々木孝博『現代戦争論－超「超限戦」』（ワニブックス 2020 年 7 月 8 日）に基づいている。
(16) 現在では START I に代わる「新 START」と呼称されている。
(17) 産経新聞「米、アジアに中距離ミサイル配備も　INF 条約失効、中国へ対抗」『産経新聞 HP』2019 年 8 月 3 日<https://www.sankei.com/world/news/190803/wor1908030025-n1.html>（2021 年 1 月 10 日アクセス）。

面の現実的な措置と考えられる。

一方ロシアも、中国や北朝鮮はじめ他の諸国が弾道ミサイルを保有し始めている現状から、INF 条約が足かせとなっていると考えているようである。2007 年 2 月、プーチン大統領は「今日、北朝鮮、韓国、インド、イラン、パキスタン、イスラエルを含め多くの国が INF に相当する装備を保有している現状においては、米露だけが条約を厳守している状況は考え直さなければならない」と発言した。さらに、同 10 月には「近隣諸国を含め他の国が米露に倣わないならば、我々が条約の枠内に留まることは難しい」とも言及した。ここで指摘したいのは、プーチン大統領の「近隣諸国を含め他の国が」と脅威対象に言及している箇所である。ロシアの近隣諸国で最大の INF 保有国は中国であるということだ。

しかしながら、中国との現在の安全保障環境（戦略的パートナーシップ関係）や中国の脅威を出来る限り低減したいとの施策から考えると、即座に対中国を見据えた INF の再配備を実行に移すことは考え難い。そのような状況の下、先に米国のほうからアジア地域に INF を配備したいとの方針が示されたことから、これを逆手にとって、対米の INF に対する対抗措置との名目で、対米兼対中の INF 配備を実行に移すことは可能と見られる。ロシアにとって幸いにも、前述のとおり、条約失効後の米国は、大々的に東アジア地域に INF を配備することは難しく、当面は洋上発射ミサイルに限定されることが予想され、ロシアはその間隙を縫って、極東地域に対米国との理由で INF の再配備を進めていく狙いがあるものと見積もられる。

● 戦略核兵器削減条約（START）に対するロシアの狙い

核の軍備管理条約で最後に残るのは START である。2019 年に生起した INF 条約破棄の状況を鑑みると、START I に代わる条約として 2011 年に発効し 2021 年に更新を迎える「新 START[18]」についても何らかの影響があるものと考えられる。2021 年 1 月現在で 5 年の延長で米露両国は合意したが、中国を巻き込めなかったことなど今後不透明なところは残っている。元々、ロシアにとっては、核戦力の分野において、米国を凌駕することはできず、優越を担保できないことから核軍縮の条約締結に乗ってきた側面がある。近年のロシアは、米国の弾道ミサイル防衛システムを突破できる極超音速滑空弾道弾や大型大陸間弾道弾、また、新型のレーザー兵器や遠距離核魚雷などを次々と開発している状況にある。米国に先駆けて開発に成功した兵器の能力を背景に、今後の核

(18) 「新 START」は、2011 年 2 月 5 日に米国とロシアの間で START I に代わるものとして発効した戦略核兵器の軍縮条約のこと。2021 年に更新時期を迎え、基本的には 5 年延長で合意した。

軍備管理についても、ロシアに有利な形での戦略兵器の国際枠組み構築の方針を打ち出す可能性がある。

いずれにしても、核戦力については、ハイブリッド戦を推し進める最後の拠り所と考えられており、また、次項で述べるように、近年のサイバー空間での脅威や人工知能（AI）による新たな脅威が核の脅威にも直結し得るともロシアは認識しているので、今後のこの分野の動きをさらに注視していく必要があるだろう。

2　ロシアが恐れるサイバー空間の脅威と核の脅威

2019年4月22日～25日の間、ドイツ（ガルミッシュ・パルテンキルヘン）で行われた第13回国際情報安全保障シンポジウム（正式名称：第13回国際フォーラム「国際情報安全保障における国家、ビジネス及び社会間のパートナーシップ」）に筆者は参加した。

本シンポジウムは、第1回よりモスクワ国立大学情報安全保障問題研究所が主催してきたシンポジウムであり、今回が13回目の開催であった。今回の枠組みは、ロシア側が2018年4月に、国際情報安全保障国家協会（National Association of International Information Security）という組織を立ち上げたことから、この協会が今回の主催組織という形で実施された。モスクワ国立大学という学術組織が主催者というトラック2の枠組み(19)での国際会議として第1回より継続されてきたが、今回からは、国家協会というより国家の関与が強い組織が主催するというトラック1．5的な国際会議に格上げされたとの印象であった。ロシア側参加者はモスクワ国立大学の研究員はもとより、大統領府特別代表、外務省付属のロシア科学アカデミー研究員、ロシア軍参謀本部幕僚、ロシア法務省員、ロシア外務省員など国家機関の関係者が多数参加した国際会議であった。一方で、その他の国は、大学や民間研究所などほぼ学術関係者が占めていた。

会議の内容は、ロシア側が情報安全保障に対する立場を様々なバックグランドの研究者から報告し、その他の国からは各々の国のスタンスや各々の研究者が独自に研究した国際情報安全保障に関する見解を発表し、ディスカッションを行うというものであった。そのため、ロシアが考える情報セキュリティに関する国家施策や本音が得られる場として評価できる会議であった。参加国は、ロシア、米国、英国、ドイツ、フランス、中国、韓国、カナダ、エストニア、ベラルーシ、キルギス及び日本の12か国

(19)「トラック2・外交」とは、民間研究機関と大学の研究者を中心とする会合に、一部政府関係者が個人の資格で出席し、それぞれが自国の政府の立場に固執することなく自由に意見交換するという態様の「民間外交」のことを指す。

であった。

この会議の中で、ロシアが近年のサイバー空間における脅威をどのように捉えているか、その脅威が核の脅威にどのように影響していると考えているかなどの認識が明らかとなった。そこで、本会議でロシア側代表者が発表した内容を取り上げ、この分野におけるロシア側のスタンスについて明らかにしていきたい。

（1）国際情報安全保障国家協会会長による基調講演

主催者であるシェルスチュク国際情報安全保障国家協会会長兼モスクワ国立大学情報安全保障問題研究所所長がシンポジウムの冒頭に基調講演を行った。その中で重視していたのが、「情報通信技術（ICT：Information and Communication Technology）の発展による安全保障環境下での問題認識」についてのロシア側の考え方である。この中には、情報空間での安全保障に関するロシアの本音が含まれている。そこで、ロシアが発信する情報を誤認することがないように、以下にその重要な箇所をそのままの表現で引用する(20)。

（シェルスチュク国際情報安全保障国家協会会長：筆者撮影）

「ここ数年、情報通信技術（ICT）を巡る国際社会における脅威や危険、リスクは益々増大している。特に昨年ワシントンにおいて、軍備管理のアーキテクチャーにおける優位を求めて、米国は何十年も共同の利益の下で機能してきた多国間の枠組みと、国際的な安定性と予測可能性を維持するために機能してきたアーキテクチャーを破壊する行動に出た(21)。残念ながら、このような動きは情報空間やICT環境下における国際協力の分野でも顕在化してきている。具体的にそれは、国連の『国際安全保障の文脈における情報化とコミュニケーションに関する専門家会議』及び『第73回総

---

(20) シェルスチュク氏は、プーチン大統領が大統領就任前エリツイン政権時に安全保障会議書記を務めていた際、同第1副書記として活躍、それ以前には通信傍受を任務とする連邦政府通信情報局（FAPSI（ロシア語: ФАПСИ：Федеральное агентство правительственной связи и информации при президенте Российской Федерации）または Federal Agency of Government Communications and Information（FAGCI））の局長を務めたロシア政府内のサイバー問題の第1人者である。なお、シェルスチュク氏が所長を務めるモスクワ国立大学情報安全保障問題研究所は、ロシア政府におけるサイバー戦に関する諮問機関である。同研究所には「軍事ドクトリン」「情報安全保障ドクトリン」等の国家施策の策定時にアドバイザー機能が求められており、原案の作成なども行っている。そのため、同研究所（特にシェルスチュク所長）と意見交換することにより、ロシアの本音に関する情報を得ることができる。

(21) 中距離核戦力（INF）全廃条約の破棄問題を指しているものと考えられる。

会』において顕著になってきている。ICT 環境下における国家の責任ある行動の標準、規則及び原則を討議するとき、２つの大きな対立が存在している(22)。

2015 年に採択した国連事務総長報告では、いくつかの点で合意がなされている。第 1 は、情報空間における紛争については、法的に解釈することも規制することもせずに ICT が政治・軍事目的で使用されることを防止すること、第 2 は、現在多々見られるような確実な証拠もなしにサイバー攻撃を行ったとして非難し合うことを控えること、第 3 は、ICT の利用は平和利用に限定すること、第 4 は、ICT 製品にバックドアを仕掛けることは不法であり、有害行為とみなすこと、第 5 は、作業部会が、自国の領土内にある情報通信インフラを管理し、国際情報安全保障分野の政策を決定することを国家の主権であると認めることなどである。

しかしながら、具体的な枠組み作りは進んでいない。そのような中で、ICT の政治・軍事目的の使用に関する懸念事項が増大している。それらの代表例が 2018 年に米国が制定した攻勢的なサイバー戦略である(23)。是非とも本国際会議で ICT の軍事利用、自律型致死兵器システムの利用、軍に広く組み込まれ始めた人工知能（AI：Artificial Intelligence）、様々な自立戦闘ロボットの開発と運用などの是非について議論を深めていただきたい(24)。これらが実行されると、戦争・紛争の手段は拡大し、国家間の紛争発生の可能性は益々増大するであろう。軍事インフラのみならず、社会・経済インフラも ICT 攻撃のターゲットとなり得る。このような見地での「軍拡競争」は国際紛争のリスクを増大させる可能性がある。そうであるならば、これらを規制する国際法を適用する必要性や国際枠組み、軍備管理規則、などあらゆることを国際社会全体で考えていかなければならない。

また、ICT が内政に介入するのを阻止するにはどのようにしたらよいのだろうか、主権国家での ICT 環境における人権問題はどのように扱ったらよいのであろうか、国際的な情報セキュリティに対する ICT の利用はどうあるべきであろうか、ICT 環境における国際平和を混乱させる可能性のある紛争の出現をどのように防止していくかな

---

(22) 欧米を中心とするサイバー空間を誰もが自由に扱うことができる公共の領域とする考え方とロシア・中国を中心とする国家安全保障のためには国家が管理・制限すべき領域とする２つの考え方の対立を指している。

(23) 米国が 2018 年に制定した「サイバーセキュリティ戦略」では、ロシアを暗に念頭に置いて能動的なサイバー攻撃について規定しているところ、それが、ロシアの国益に直結している問題と捉え、警戒している姿勢が受け取れる。

(24) ロシアがサイバー問題の次に課題と考えている事項が、LAWS（Lethal Autonomous Weapons Systems：自律型致死兵器システム）及び AI の軍事適用及びロボティクスであることが、この発言から読み取れる。

ど、ICT 環境下での様々な安全保障上の課題は山積している(25)。本シンポジウムでこれらの課題に取り組むべく議論を始めようではないか。」

ロシアの立場からの意見として、ICT 環境下での国際情勢に関して、米国およびそれに同調する諸国に対して、情報空間での国際枠組みや規制が明確でないことの不満を表明し(26)、また、独自の攻勢的なサイバー戦略を制定した米国に強い批判を示していたということである。さらに、情報空間における主権を、内政不干渉を重視する形で国際的に認めさせたいとの強い姿勢を示していた。

（２） ロシア大統領府特別代表による基調講演

引き続いて、クルーツキフ大統領府特別代表が基調講演を実施した。この中で、同代表は、改めて情報空間における近年の米国の対応を批判した。内容で特に指摘したいのが、情報空間（サイバー空間）における脅威が核の脅威に直結しているという発言であった。その発言の要旨を前項同様の理由で、そのままの表現で引用する。

（クルーツキフ大統領府特別代表：筆者撮影）

「昨年もロシアは米国を批判してきた。それは 2018 年に米国が攻撃的なサイバー戦略を制定したからである(27)。サイバー兵器の使用については、ロシアはフランスとも協議を行っている。そこで出てきた事実は、フランスに対するサイバー攻撃は米国から行われたものであったということである。国連の場では、サイバー攻撃を武力攻撃として扱うということを協議しているがこれも議論の余地がある。海上や空の領域では、米国及び旧ソ連の間で事故防止協定を結んで偶発的な事故を防止してきた。ロシアは、サイバー空間においても同様な協定を結ぶことが適当であると考えており、すでに英国やフランスと協議を重ねている。サイバー空間におけるインシデントが核戦争にエスカレートすることをロシアは懸念している。ビジネスコミュニティや化学兵器の禁止条約でできたことを、サイバー攻撃についても適応するのが適当であると考え

---

(25) ここでシェルスチュク氏が取り上げた ICT を巡る安全保障環境の変化に伴う懸念事項が、現在ロシアが情報安全保障上問題視している事項と考えられる。
(26) このような立場の表明の背景には、ロシアに都合のいい形での国際枠組みを追求していることがある。
(27) 大統領府特別代表の発言からも米国のサイバー戦略に対する批判が出ていることから、この問題に関するロシア側の深刻度が伺える。

ている。

本件に関してはいくつかの良い知らせがある。プーチン大統領がシンガポールを訪問した際、サイバーセキュリティに関する協議を行った。両国はほぼ同じ見解をもっており、サイバー攻撃の次の課題は、IoT（Internet of Things）に関するセキュリティとロボティクス、オートノミー、AI といった問題を国連の場で協議するべきとの見解で一致した(28)。民間トラック（トラック 2）でも協議を進めていくべきであろう。ロシアは米国との協議や国連をはじめとする様々な分野で、ICT のセキュリティについての国際会議に参画しているが、米国の力が強すぎると感じており、米国及びその同盟国が国際協議を混乱させているとも感じている。その代表的なものは、ロシアは様々な提案を国連に提示しているが米国及びその同盟国は我々の提案に反対しているということである。サイバー戦争を防止するための 13 の規範を提案したが約 120 の国家が賛同してくれている。この中にはロシアの考えるサイバー空間における主権のことについても言及している。ICT の軍事使用、ICT に関する国家主権と国家の行動、領土との関係、プロアクティブな行動などを含む国連 GGE（Groups of Governmental Experts）の作業部会レポートを総会で確認してもらった。欧米諸国は国際法の原則に基づき行動してもらいたいと考えている。

もう 1 つの問題は、民主主義と情報安全保障の関係についてである。これについては二国間交渉も重要だと考えている。国連の作業部会では 20 のバイラテラルの交渉をもったが、いずれの協議においても国際サイバーセキュリティに関して規範がないことに賛同してくれた。GGE でも協議した。

サイバー犯罪をコントロールすることについては、これまでの話とは少し違うが国際的な協議は進んでいるとの感触をもっている。犯罪目的と安全保障は考え方が少し違うかもしれない。いずれにしても、法的な専門家を集結させ、国際的なコンセンサスを得ることが重要となってくるだろう。」

この発言から分かるように、核保有国の英国及びフランスと「サイバー空間におけるインシデントが核戦争にエスカレートする可能性」について協議しており、それをロシアは、安全保障上非常に憂慮する事項として捉えている様子を読み取ることができる。そして、その次に安全保障上考慮しなくてはならない事項として、ロボティクス、オートノミー及び AI などを課題として捉えていることが明らかとなった。

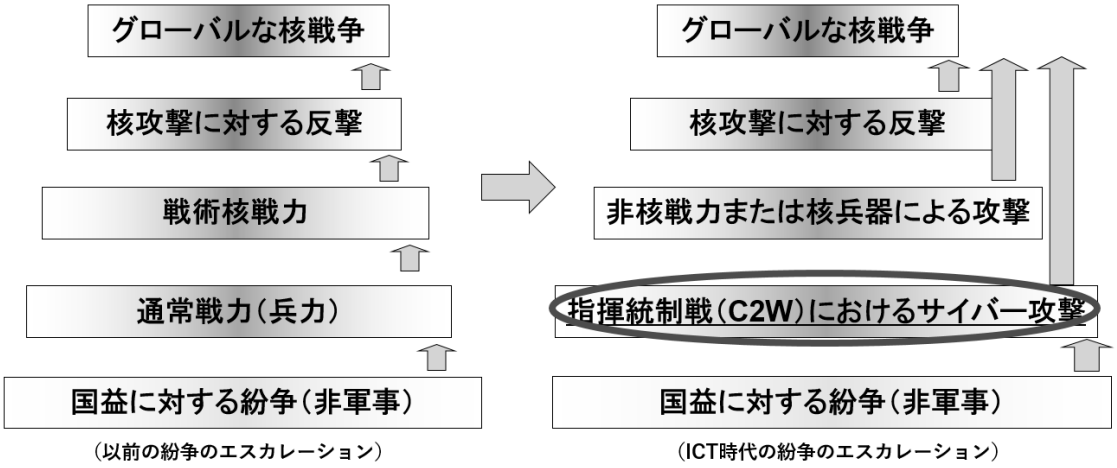
---

(28) 大統領特別代表の発言からもサイバー問題の次の課題についての発言があり、当該問題に関するロシアの真剣度が伺える。

（３） ICT 時代における戦略的安定性に関するロシアの考え

主催者及び大統領府代表の発言を受けて、引き続きロシア外務省のシンクタンクであるロシア科学アカデミー（世界経済・国際研究所）のロマキシナ教授から、「ICT 時代における戦略的安定性に関するロシアの施策」についての発表があった。その中で、クルーシキン大統領府特別代表が表明した「サイバー空間におけるインシデントが核戦争にエスカレートする可能性」についての具体的な説明があり、ロシア側の考える懸念事項が明らかとなった。

図２　ICT 時代の紛争のエスカレーション



（出典：ロマキシナ「ICT 時代における戦略的安定性」『第 13 回国際情報安全保障シンポジウム』（2019.4.22）の発表資料（ロシア語）を基に筆者作成）

ロマキシナ教授が冒頭に述べたのは「新しい戦略枠組みの特性」についてであった。すなわち「地域戦争及び武力紛争の増加」、「中国が新たなパワーの中心に躍り出たこと」、「核・ミサイルの多極化」、「ドクトリンの傾向の変化」、「核戦争そのものの蓋然性の低下」などの安全保障上の環境の変化を新たな戦略環境枠組みの特性として掲げた。さらに装備・技術・兵器分野にまで目を向け、「戦略的な兵器を使用した軍事紛争管理体制の崩壊」、「非核戦略兵器システムの進展」、「低強度核兵器の開発」、「対衛星兵器」、「宇宙空間の軍事使用」などの変化を挙げた。そのような戦略環境の変化に伴い、戦略的な安定性を確保するにあたっての ICT の影響をクローズアップした。具体的には「政治・軍事目的で使用される ICT」、「ICT を利用した大規模戦争に勝利するための衝動の生起」、「ICT を利用すると平時と戦時の境界線が不明瞭化すること」、「グローバルな戦いの論理に変化が生まれること」、「軍事紛争のエスカレーショ

ンの段階が減少し最悪の事態まで至る可能性があること」などを懸念事項として指摘した。

また、以前は、紛争（対立）の段階において、影響工作やインフラに影響を及ぼす戦いを実施することにより、軍事的脅威を減少させ、敵に軍事力を使わせないような決断をさせ、軍事的な戦いを抑止するという段階が踏まれていたことを指摘した。そして、紛争のエスカレーションの段階を烈度の低い順に「国益に対する紛争」、「通常戦力による紛争」、「戦術核戦力による紛争」、「核攻撃に対する反撃」及び「グローバルな核戦争」と規定し、それを相互に認識することにより、一定の抑止（コントロール）が効いていたとした(29)（図２左参照）。

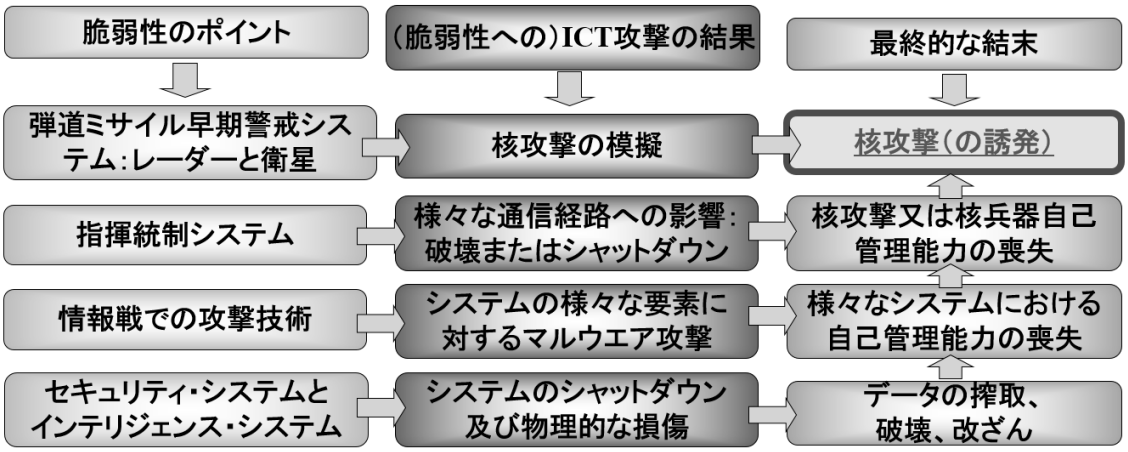
しかし、ICT 時代の紛争のエスカレーションは、これまでの認識とは違ったものとなっていると指摘した。1990 年代以降のロシアで有力な核抑止論として論じられてきた「エスカレーション抑止」においては、小規模な紛争をエスカレーションラダーによって抑止するのではなく、その紛争規模に応じた戦術核使用へのエスカレーションで直接抑止することが考えられている(30)。そのため、小規模な「国益に対する紛争」発生時にロシア側が核エスカレーションの脅しをかけるからこそ、それに対抗する側が核を含む指揮統制能力にサイバー攻撃を仕掛けてくることが問題になるということである。すなわち、「国益に対する紛争」が生起すると「ICT を用いた指揮統制戦（C2W：Command and Control Warfare）が生起しサイバー攻撃が実施される」、それが直接「核及び非核戦力による攻撃」を誘発させることもあり得る。そして、その核攻撃が行われると「核攻撃に対する反撃」が行われ、容易に「核戦争」が生起してしまうという構図が想定されるとした。換言すれば、ICT が軍事に用いられると、今までコントロールできると考えていた核戦争を容易に誘発してしまうということを指摘したのである（図２右参照）。

また、ICT 攻撃を用いた結果、紛争のエスカレーションが生起する場合の戦略核戦力の ICT 攻撃に対する脆弱性と起こり得る結果・結末を、具体例を示し説明を加えた（図３参照）。

---

(29) 相互確証破壊（MAD：Mutual Assured Destruction）の概念に言及していると思われる。相互確証破壊とは、核戦略に関する概念・理論・戦略。核兵器を保有して対立する 2 か国のどちらか一方が、相手に対し核兵器を使用した場合、もう一方の国が先制核攻撃を受けても核戦力を生残させ核攻撃による報復を行う。これにより、「一方が核兵器を先制的に使えば、最終的に双方が必ず核兵器により完全に破壊し合うことを互いに確証する」ものである。理論上、相互確証破壊が成立した 2 ヶ国間で核戦争を含む直接的な軍事的衝突は発生しない。
(30) 秋山信将、高橋杉雄、小泉悠ほか「『核の忘却』の終わり」『勁草書房』2019 年 6 月。

図３　ロシアが考えるサイバー空間における脅威と核の脅威



（出典：ロマキシナ「ICT 時代における戦略的安定性」『第 13 回国際情報安全保障シンポジウム』（2019.4.22）の発表資料（ロシア語）を基に筆者作成）

まず、脆弱性のポイントとして、「弾道ミサイル早期警戒システム（レーダーと衛星)」、「指揮統制システム」、「情報戦での攻撃技術」及び「セキュリティ・インテリジェンスシステム」を挙げた。

各々の脆弱性に対し ICT 攻撃を用いると以下のような結末が想定されるとした。「弾道ミサイル早期警戒システム」に対し ICT 攻撃を用いると「核攻撃の模擬（シミュレーション)」が容易に実施でき、それを被攻撃国が実際の攻撃と誤認してしまうと「実際の核攻撃」を誘発してしまうということだ。「指揮統制システム」に対しては、「様々な通信経路へ ICT 攻撃することにより、システムの破壊またはシャットダウン」させることも可能となる。そうすると「核攻撃そのものや核兵器の自己管理能力を喪失」させることも容易であるということだ。「情報戦での攻撃技術」を駆使すると、「システムの様々な要素に対するマルウエア」を作成することが可能であり、「自己管理能力を喪失」させることもできる。「セキュリティ・インテリジェンスシステム」の脆弱性に対しては、「システムのシャットダウン及び物理的なシャットダウン」も想定され、様々な作戦システムや装備の「データ改ざん、搾取、破壊」が可能となる。

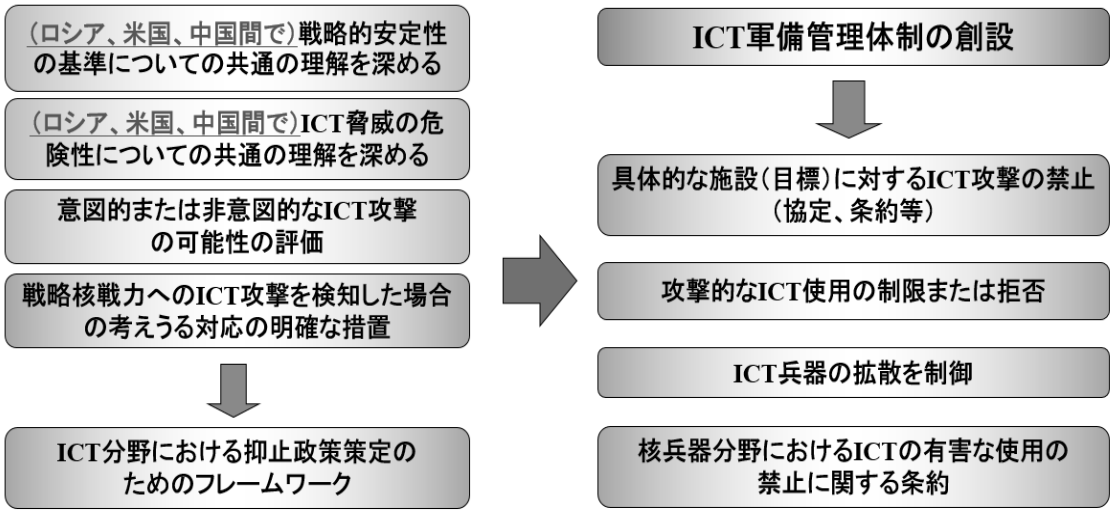
総じて言えば、ICT 攻撃を脆弱なポイントに加えると、通常の軍事作戦の継続は不可能となり、最悪の場合、核攻撃をも誘発する可能性があるということである。

そして、そのような新たな時代に予見される ICT に関わるリスクを解決するためには、グローバルな対応が必要となってくると提言した。具体的には、①　戦略的安定性の基準についての共通の理解を主要国であるロシア、米国及び中国の間で深めるこ

と、②　ICT 脅威の危険性についての共通の理解を主要国であるロシア、米国及び中国の間で深めること、③　意図的なまたは非意図的な ICT 攻撃の可能性を区分し評価すること、④　戦略核戦力への ICT 攻撃を検知した場合の対応策を明確化することなどである。これらを通じ、ICT 分野における抑止政策策定のためのフレームワークを作り上げることが重要となってくるということを提言した。

また、そのフレームワークを実現するためには、「ICT における軍備管理体制の確立」といった目に見えた対応が必要となってくるということである。その中身には、①　特定の目標に対する ICT 攻撃の禁止ということを、協定や条約といったもので規定すること、②　攻撃的な ICT の制限または拒否ということを同じく規定すること、③　ICT 兵器の拡散を制御すること、④　特に核兵器分野における ICT の有害な使用の禁止に関する条約を制定することなどを提言した（図４参照）。

図４　ロシアが提案する ICT の軍備管理体制



（出典：ロマキシナ「ICT 時代における戦略的安定性」『第 13 回国際情報安全保障シンポジウム』（2019.4.22）の発表資料（ロシア語）を基に筆者作成）

（４）シンポジウムの総括

本シンポジウムを総括し、４つの点を指摘したい。

第１は、本シンポジウムにおいて、ロシア側は ICT を用いた軍事利用が単に情報空間やサイバー空間での攻撃に留まらずに、核の脅威にエスカレートすることを国家存続の脅威として認識しているという点が強く感じられたという点である。

第２は、今回のシンポジウムでは問題提起に留まっていたが、次世代での課題とし

て述べていた、ロボティクス、オートノミー、AI の軍事利用などについては引き続き情報収集の要があるだろう。

第 3 は、ロシア科学アカデミーの戦略的安定性の発表によれば、ロシアは、課題の解決に向けてのグローバルな対応を、ロシア、米国及び中国の 3 か国間のみの国際枠組みを中心として実施しようとしていた点だ。核兵器の管理の部分を除いた ICT の軍事利用を定める協議には我が国としても、あらゆる協議の場に出席し、ロシアによる恣意的な規則の形成を許さないよう積極的な関与をしていくべきであろう。

第 4 は、ロシアでは前述のように、国際情報安全保障の問題を国家として統括して解決するために、従来の「モスクワ国立大学情報安全保障問題研究所」の上位の組織として「国際情報安全保障国家協会」という組織を立ち上げた点である。ロシアは、国際情報安全保障枠組みの制定に関し、政府間協議のトラック１、学術・民間協議のトラック２に加え、半官・半民のトラック１．５の協議枠組みを創設することによって、従来よりもさらに踏み込んだ戦略をとり、ロシアの考えを国際社会に拡散させる動きを活発化してきたものと考えられる。

３　ロシアが国際枠組みや軍備管理等を推進する狙い

（１）ハイブリッド戦と核戦略の齟齬

これまで述べてきたように、一義的には、ロシアが自らの勢力圏に対する NATO による逆介入を阻止するために用いたのが、いわゆる「ハイブリッド戦」であり、そこで重視しているのが、「サイバー戦」や「情報戦」を中心とする非軍事的な手段である。すなわち、サイバー空間での非軍事的手段を推し進めることにより、物理的に戦わずして国益を擁護し、国家の安全を確保することを一義的には重視しているということである。

他方で、積極的な核使用を示唆するという「エスカレーション抑止」の理論に基づく恫喝（または、実際に使用することも排除しない）も考えている。

しかしながら、サイバー空間での非軍事手段を推し進めれば進めるほど、ロシアが本来保持している「小規模な紛争をエスカレーションラダーによって抑止するのではなく、その紛争規模に応じた戦術核使用へのエスカレーションで直接抑止する」という「エスカレーション抑止」の施策に直接悪影響を及ぼしてしまい、核のエスカレーションを自国の思惑どおりに管理できなくなる脅威にも直結してしまう。そのような新たな課題に直面しているということをロシアは憂慮し始めている。元々保持していた「エスカレ―ション抑止」の戦い方と新たな世代の戦い（「ハイブリッド戦」）として重視したい非軍事手段の戦いの両方を実施したいが、一部齟齬がでてきたものとも

言えるだろう。その憂慮の裏では、ロシアは常に勝ち目の追求を続けているという事実を我々は認識しなければならない。そのために、ICT 分野における軍備管理体制の確立を打ち出し始めたというのが近年のロシアの動きである。今後、ロシアのこの種の提案を精査し、その行間に見え隠れする意図を正確に分析し、国際枠組み構築の努力をしていくべきであろう。また、ロシアをはじめとしてこの分野に関与する各国、特に米国及び中国の動向も併せて注視していく必要があるだろう。

（２）サイバー戦略と核戦略における対応行動の類似性(31)

サイバー空間及び核兵器に関するロシアの対応行動を考察してみると、前述のような齟齬がみられる反面、両者には対応の類似性もみられる。

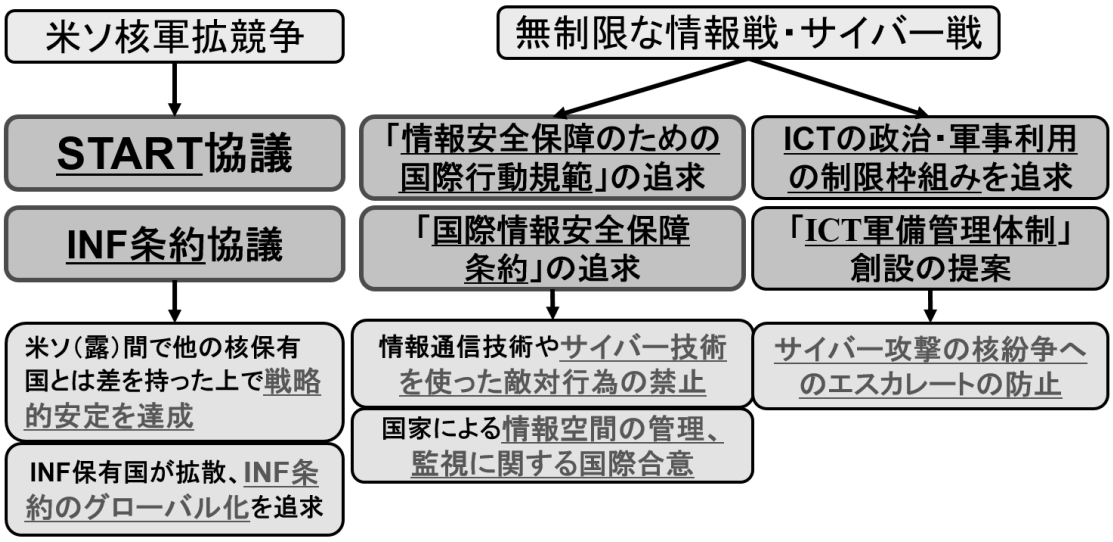
ロシアが情報安全保障に関する国際的な枠組みの実現やサイバー兵器の軍備管理に力を注ぐ様子は、START や欧州安全保障条約の交渉過程において、ロシアに有利な形での国際安全保障秩序を目指す姿と重なるということである。すなわち、物理的な軍備管理の世界においてロシアは、START で戦略核の弾頭数や運搬手段数の上限を定め、米国がロシアの戦略核戦力を上回ることのないようにくさびを打った。INF についても米露双方が全廃することにより米国の中距離核戦力の脅威を排除した。ミサイル防衛問題については現在如何に有利な形で米国に制限をかけるか交渉中である。この背景には、核兵器に関連する技術やその整備に要する財源に劣ることから、軍備管理を推し進めることにより、米国の脅威を抑える施策を採用し、米国との対等を目指すという狙いがあった。これらのアプローチと、近年の情報空間における国際行動規範の実現を主導しようとするロシアのアプローチとを比較すると、非常に類似していることが分かる（図５参照）。

すなわち、ロシアには、「情報安全保障のための国際行動規範」を制定することにより、情報通信技術（ICT）やサイバー技術を使った敵対行為そのものの禁止を目指す有力な動きがあると見ることができる。サイバー攻撃というものは如何にその防護能力を高めても、100%防護することは不可能である。そうであるならば、サイバー兵器を使用した敵対行為そのものを禁止する国際行動規範を制定できれば脅威は低減できるということである。この背景には、ロシアはサイバー防護能力において欧米諸国等には及ばない、仮に欧米諸国等からサイバー攻撃があった場合には防ぎきれないという脅威感（強迫観念に近い）がある。そのために、国際行動規範により、サイバー強国がロシアに対しサイバー攻撃を実施できないようにすることを狙ったものであ

(31) この項、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」『ディフェンス第 81 号』隊友会（2014.10）を基にしている。

る。当然、国際行動規範にするとすべての国が対象となり、ロシア自身が実施する攻撃も国際社会からの批判にさらされる可能性がある。ロシア自身が実施するサイバー攻撃については、今まで通り、国家が関与しないロシア市民（またはその組織）が実施したとの理由で逃げ切ることとし、それよりもサイバー強国による攻撃を何とか封じたいとの考えによる行動から出てきた動きと評価できるだろう。

図５　サイバー戦略と核戦略における対応行動の類似性(32)



（出典：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」『ディフェンス第 81 号』隊友会（2014.10）を基に筆者作成）

これらに加えて、前項でも掲げたようにサイバー空間における脅威が核の脅威にエスカレートすることを、ロシアとしては憂慮して（各国がそれを憂慮することをも利用して）、ICT の軍備管理体制の確立に力を入れる姿にも相通じるものがあるということだ。

すなわち、ロシアが戦略的な安定性の実現、国際枠組みの創設、軍縮協議や軍備管理条約の制定などに対して積極的な対応に出てきた場合は、当該分野において、ロシア独力では他国に対しての優越を確保できないという場合が多いということである。これらに関するロシアの提案の行間には、多国間の利益に隠れて、ロシア固有の国益をどのよ

(32) INF 全廃後の核戦略において INF 条約のグローバル化が極めて困難であることはロシアも認識していると思われ、それは、極超音速滑空弾頭ミサイルや地上発射型カリブル等ポスト INF の打撃システムの開発を計画していることからも読み取ることができる。本件については、別の議論が必要と考えられるので、改めて別の論考にて検証いたしたい。

うに担保するかの内容が含まれているので、それをよく認識して対応していく必要があるだろう。

おわりに

近年ロシアは、「ハイブリッド戦」という戦い方を打ち出し、新たな世代において国益を確保するための戦いを実行に移している。その戦いにおいて一義的に重視されるのは、非軍事手段であり、非軍事手段と軍事手段の割合は４：１で圧倒的に非軍事手段の占める割合が大きいとしている。

ここで特に取り上げなければならないのが、「情報戦」や「サイバー戦」といった非軍事手段である。ロシアは、これらの領域での戦いにおいて優越を確保するために非軍事手段を重視した戦略を実行しており、「戦わずに勝つこと」を一義的には目指している。

しかしながら、非軍事手段を重視する戦略の中においても、ロシアは核戦力を拠り所と考えている。その核戦力を巡って 2019 年には大きな動きがあった。INF 条約の破棄の問題である。INF 条約の破棄は米露ともに対中国を考慮しているという背景があるものとみられている。2021 年には「新 START」の更新を迎え、基本的には 5 年の延長で米露は合意した。しかしながら、これは米露のみの合意であり、中国を含めた他の保有国との枠組みではなく、戦略核以外の戦術核を考慮すれば核に関する軍備管理は一層不透明な状況になりつつある。

そのような状況下、ロシアが重視する非軍事手段のサイバー空間での戦いにおいて、その脅威が核の脅威にエスカレートする可能性をロシアとしては非常に危惧しており、また、各国も同様に危惧していることを利用し始めているということである。ロシアが平時から有事にかけて重視しているハイブリッド戦における非軍事手段によって、最後の拠り所と考えている核戦力に悪影響を及ぼしてしまうという脅威を感じているということだ。それを、国際枠組みや条約によって抑止しようと考えている。

今後のこれらのロシア側の動きについては、サイバー空間の安全保障及び核の軍備管理の両分野に大きな影響があると見積もられる。したがって、ロシアの戦略における「ハイブリッド戦」、「核兵器の意義」、「サイバー戦」のこのような関係を理解したうえで、日米欧の側は、この３者の関係をどのように整理して、ロシアの軍備管理提案にどのように対応していくことが望ましいのか考えることが重要であるだろう。

［著者プロフィール］

佐々木　孝博（ささき　たかひろ）

１９８６年　防衛大学校（電気工学）卒業
同年海上自衛隊に入隊 日本大学大学院修士(国際情報)
米海軍第３艦隊司令部連絡官　豪海軍大学留学
護衛艦「ゆうべつ」艦長　在ロシア防衛駐在官
英国国防情報学校留学　第８護衛隊司令
統合幕僚監部サイバー企画調整官
指揮通信開発隊司令　下関基地隊司令を経て、
２０１８年退官

広島大学大学院　人間社会科学研究科客員教授
東海大学　平和戦略国際研究所客員教授
明治大学　サイバーセキュリティ研究所客員研究員