第７８０号

令和２年５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

ロシアが推し進める「ハイブリッド戦」の概要とその狙い

会員　佐々木孝博

はじめに

周辺諸国の脅威に四周を囲まれているという独特の安全保障観をもつロシアでは、近年、確実な安全保障を求めて、新たな世代の戦い方を模索している。それは、非軍事・軍事のあらゆる手段をもって戦う「ハイブリッド戦」という形で明らかになってきた。このハイブリッド戦の根底には、中国の人民解放軍将校（喬良大佐及び王湘穂大佐）が1999年に打ち出した「超限戦」という戦略があるのではないかと言われている。「超限戦」とは、その名のとおり、「21世紀の戦争は、あらゆる限度を超えた紛争であり、あらゆる手段が軍事兵器になり、あらゆる場所で軍事紛争が生起する」といったことを戦略としてまとめ上げた文書である。すなわち、軍事・非軍事手段、正規・非正規組織、作戦領域などを問わず、あらゆる制限や制約を超えて国家目標を達成するという戦略のことである(1)。

ロシアは、従来から保持している安全保障戦略とこの「超限戦」とを比較・研究し、戦略文書としてその内容を取り入れたのではないかと見られている。詳細は後述するが、ロシアの「ハイブリッド戦」という戦い方が、文書として対外的に初めて明らかになったのは、2013年２月、ゲラシモフ参謀総長が発表した安全保障論文「先見の明における軍事学の価値」と言われている(2)。この論文で「新たな世代の戦い」として示された

(1) 渡部悦和『中国人民解放軍の全貌』（扶桑社新書2018年５月１日）、55頁～56頁
(2) ヴァレリー・ワシーリエヴィッチ・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>（2020年２月26日アクセス）。原題の直訳は「先見の明における科学の価値」であるが、ここで言う「科学」とは、本文によると、自然科学を意味するのではなく「軍事科学（兵学）」を意味している。ただし、日本語では「政治学」と表現する学問をロシア語では「政治科学」と表現している関係上、齟齬を起こさないように、本稿においては「軍事科学」を示す「科学」の訳語を「軍事学」とする

内容が、西側諸国により呼称されるいわゆる「ハイブリッド戦」であり、後に、その内容は「国家安全保障戦略」及び「軍事ドクトリン」などの戦略文書に反映された。

そこで本稿においては、ロシアが考えるこの「ハイブリッド戦」を、その中核となっている「情報戦」「影響工作（Influence Operation）」といった戦い方を中心に、ロシアが対外発表した資料を基に、ロシアサイドとしてどのように捉えているかを考察していきたい(3)。また、この「ハイブリッド戦」という戦い方の理論を実践に移したと見られる「ウクライナ危機」及び「米大統領選への関与事例」を欧州ハイブリッド脅威対策センターがまとめたレポート「ハイブリッド脅威への対処」及び米国司法省の起訴状を基に考察していきたい。加えて、「ハイブリッド戦」が抱える制約といったことについても考えてみたい。

１　ロシアが推し進める「ハイブリッド戦」

（１）ゲラシモフ参謀総長が掲げた「新たな世代の戦い」

まず、ロシアが掲げた「ハイブリッド戦」の概要を、冒頭に述べたゲラシモフ参謀総長による安全保障論文を基に考察していきたい。この論文は、ロシア国防省との関係が深い『軍事産業クーリエ』誌に発表されたものであり、その後、西側諸国でも翻訳され広く認知されることとなった。しかし、ロシアは自ら、この戦い方を「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に移している状況を解釈したうえで名付けた名称である。実際には、ゲラシモフ論文において「『21 世紀の典型的な戦い』、または『新たな世代の戦い』」と記述された内容が、西側諸国が呼称する「ハイブリッド戦」に相当するものと考えられる。ゲラシモフ論文の内容は、後に、戦略文書である「国家安全保障戦略」「軍事ドクトリン」及び「情報安全保障ドクトリン」における、総論、脅威の定義、実施の指針など多岐にわたる項目に反映されている。ここで、ロシアにおける安全保障に関する戦略文書体系を、図１に示す。

図に示すように、憲法及び安全保障に係わる連邦法の包括的な規定の下に、最上位の戦略文書として、安全保障会議が策定する「国家安全保障戦略(4)」が定められている。この「国家安全保障戦略」を受け、それを具現化する文書として、軍事分野・軍事産業分野については「軍事ドクトリン(5)」や「海洋ドクトリン」が規定されている。外交・国際関係分野については「対外政策構想（コンセプト）」が、情報戦分野においては「情報安全保障ドクトリン」などが定められている。その他にも、経済分野、公安分野、対テロ活動分野などの分野別にも、必要なドクトリンやコンセプトが規定されている(6)。

---

(3) ロシアは、西側諸国の標準的な捉え方では考えられない独特の安全保障観、脅威認識、対処方針をもっているため、ロシアサイドがどう考えているかを考察することは重要である。ロシアの独特な安全保障観については、佐々木孝博「ロシアが目指す国際的な安全保障秩序」『日本大学大学院総合社会情報研究科紀要第 11 号』2011 年 7 月 1 日<https://atlantic2.gssc.nihon-u.ac.jp/kiyou/pdf11/11-001-013-Sasaki.pdf>（2020 年 4 月 10 日アクセス）参照

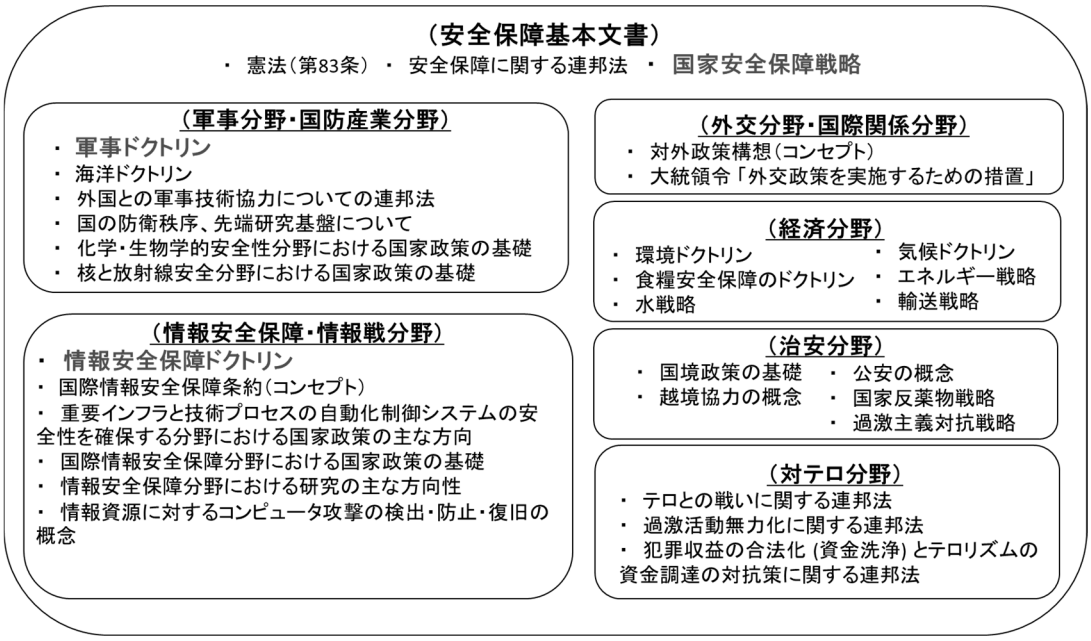
(4) ロシア安全保障会議「国家安全保障戦略（ロシア語）」『安全保障会議 HP』2015 年 12 月 31 日、<http://www.scrf.gov.ru/security/docs/document133/>(2020 年 1 月 22 日アクセス)

(5) ロシア安全保障会議「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/>(2020 年 1 月 22 日アクセス)

(6) 佐々木孝博「ロシアのサイバー戦略」『日本大学大学院相互愚社会情報研究科第 13 号』2013 年 7 月 1 日<https://atlantic2.gssc.nihon-u.ac.jp/kiyou/pdf13/13-001-012-Sasaki.pdf>（2020 年 4 月 10 日アクセ

これらの戦略文書に、ゲラシモフ論文が大きな影響を及ぼしたということである。

図１　安全保障に関する戦略文書体系



（出典：安全保障会議 HP の政策文書体系より筆者作成）

（２）戦略・ドクトリンの相次ぐ改訂

2013 年にゲラシモフが論文を発表してから、翌 2014 年にはその内容を盛り込んだ形で「軍事ドクトリン」を改訂した(7)。さらに、2015 年にはその上位文書である「国家安全保障戦略」を、翌 2016 年には情報戦分野を司る「情報安全保障ドクトリン」を次々と改訂した(8)。

本来であれば、戦略というものは、上位文書が最初に制定され、それを受けて下位文書が上位文書を具現化する形で定められるのが通例である。今回、ロシアが変則的に「軍事ドクトリン」を始めとして、上位・下位の位置づけは関係なく、次々と戦略文書を改訂していった経緯には次のような事由があったものと考えられる。

2013 年にゲラシモフが「次世代の新たな戦い」を示した後、それを具現化・実行する形で「ウクライナ危機（クリミア併合）」の事案が生起した。ロシアという国は、国家が何らかの行動を起こす場合、その正当性というものを重視する傾向にある。特に、軍事行動の場合は、その正当性を法的根拠に求める場合が多い。今回のクリミア併合の行動は、どのような法的根拠で、どのような政策・戦略・ドクトリンに基づいて行われたのかということを早急に内外に示す必要があった。その根拠を「軍事ドク

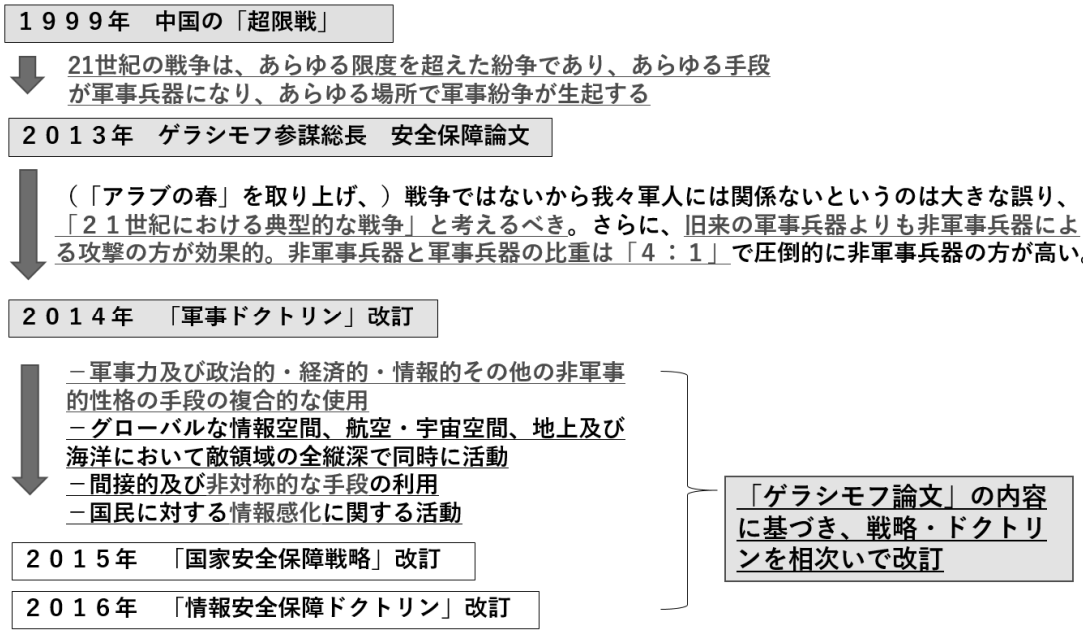
ス）

(7) 改訂の詳細は、佐々木孝博「サイバー戦の必要性からみたロシアの軍事ドクトリン改訂」『ディフェンス 54 号』隊友会、2015 年 10 月参照

(8) 改訂の詳細は、佐々木孝博「ロシアの『情報安全保障ドクトリン』を読み解く」『ロシア・ユーラシアの経済と社会』第 1018 号、ユーラシア研究所、2017 年 7 月参照

トリン」に求めたと推察される。非軍事行動に始まるウクライナ危機全般を網羅するような非軍事・軍事の行動を定める戦略文書は、本来ならば「国家安全保障戦略」が適当ではあるが、同戦略は包括的に定める必要があり、様々な国家機関・省庁の検討の結果が得られなければ改訂することは困難である。「軍事ドクトリン」であれば軍事安全保障に関わる組織で検討するのみであるので、「国家安全保障戦略」を改訂するよりはインパクトが少ない。戦略の改訂に先立って軍事行動まで実施していた関係上、早急に法的根拠を定める必要があり、早期に改訂が可能な「軍事ドクトリン」の改訂を優先したものとみられている。これらの状況を図２に示す(9)。

図２　ロシアの戦略文書制定の経緯



（出典：ロシアの発出する各種安全保障関連文書から筆者作成）

（３）国際間紛争の解決における非軍事手段の役割

さて、ゲラシモフが論文の冒頭で問題提起したことは、北アフリカや中東で生起した「アラブの春(10)」の事案、及び旧ソ連諸国（独立国家共同体〔CIS〕諸国）において相次いで生起したいわゆる「カラー革命(11)」である。これらの事案に共通している事項は、

---

(9) ゲラシモフ論文に端を発するロシアの各種戦略文書制定の経緯については、様々に見方があるが、本論においては、公表されたものをそのまま扱うこととする。背後に隠れる事情等については今後の課題としたい

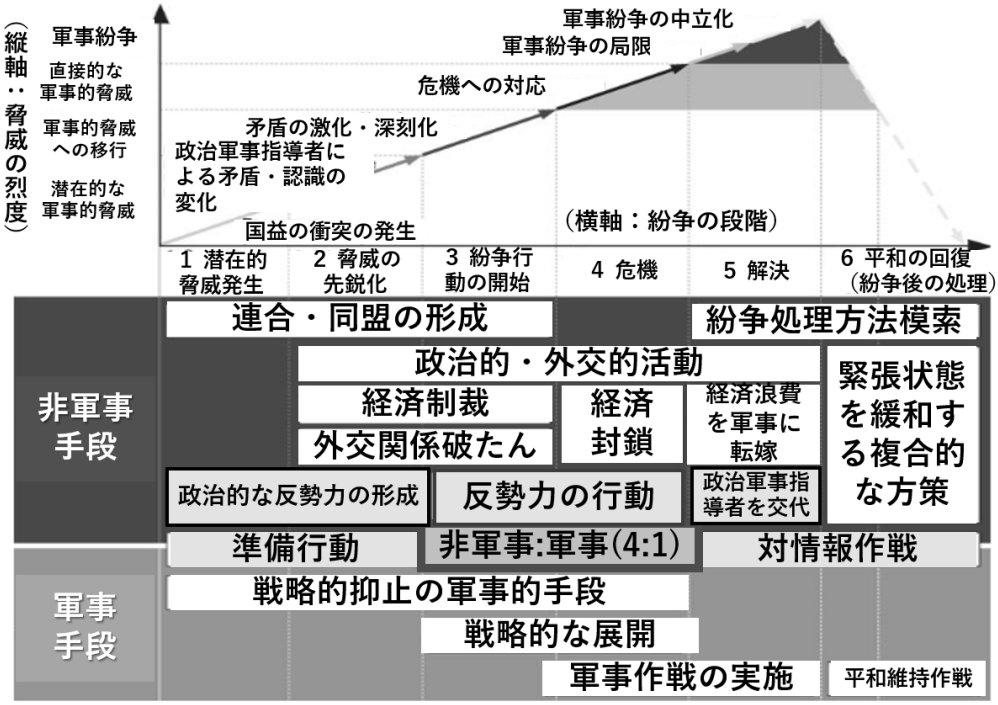
(10) 「アラブの春」とは、2010 年から 2012 年にかけてアラブ世界において発生した、前例にない大規模反政府デモを主とした騒乱の総称である。2010 年 12 月 18 日に始まったチュニジアのジャスミン革命から、アラブ世界に波及した

(11) 「カラー革命」もしくは「花の革命」とは、2000 年頃から、中・東欧や中央アジアの旧共産圏諸国で起こった一連の政権交代を総体的に指す。米国情報機関の関与が疑われている。その象徴として色や花が当てはめられた

ソーシャル・ネットワーキング・サービス（SNS）やメディアなどを利用した情報戦が実施されたこと、それを起点として世論が動かされ、激しい内戦や武力紛争が生起し、政権を転覆させたことであった。そして、「『アラブの春』の事案は、『21 世紀の典型的な戦い』である」との宣言に至っている。

ゲラシモフ論文では、特に「アラブの春」の戦い方を念頭に「国際間紛争の解決における非軍事手段の役割」について、図を用いて説明を加えている。（図３参照）

図３　国際間紛争の解決における非軍事手段の役割



（出典：図は「先見の明における軍事学の価値」から引用、訳文は筆者による）

ロシアは従来から軍事ドクトリンにおいて、紛争・戦争のレベルを「武力紛争(12)」「局地戦争(13)」「地域戦争(14)」及び「大規模戦争(15)」の４つの段階に区分している。ゲラシモフ論文で述べられている「国際間紛争」とは、「軍事ドクトリン」で規定していると

---

(12) 「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。図２を説明するゲラシモフ論文の表現から、ここで言う「国家間紛争」とは、「国家間の戦争」には至らない「武力紛争」に該当するものと捉えられる

(13) 「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

(14) 「軍事ドクトリン」の規定によれば、「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

(15) 「軍事ドクトリン」の規定によれば、「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。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てエスカレートした結果が大規模戦争となることもある。大規模戦争は、参加する国家が保有するすべての物的資源と精神力の動員を要求する

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、本論文において、大前提となっていることが「アラブの春」や「カラー革命」を念頭においた戦い方であること、及び図３に示されたとおり「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。すなわち、この戦い方の主眼は、軍事ドクトリンが規定する２国間が全面的な戦争（局地戦争以上）に至る前の段階の「管理された低烈度紛争（武力紛争）」を戦うための指針を定めたものと言える。

論文の中でゲラシモフは、「将来の軍事的な戦い(16)においては、旧来の軍事兵器よりも非軍事兵器による攻撃のほうがより効果的であり、非軍事手段と軍事手段の比率は４：１で圧倒的に非軍事手段の比率が高い」と強調している。ここで注目したいのが、非軍事手段の中にある「政治的な反勢力の形成」「反勢力の行動」「政治・軍事指導者を交代させる」といった項目である。後述する影響工作で実施する事項を具体的に掲げているということである。しかしながら、紛争段階を超え戦争段階に至ったとしても、本論文が提示する非軍事手段の有効性は、非軍事：軍事の比率は変わるものの、損なわれるものではない。むしろ高烈度な戦争状態においては、軍事・非軍事の融合が大々的に行われる可能性もあることは付言しておきたい。

これらのことは、後に、安全保障会議副書記として「軍事ドクトリン」の策定を主導したユーリー・バルエフスキー元参謀総長が「情報戦争における勝利は、流血惨事を招かないながらも、古典的な軍事紛争での勝利よりもはるかに重要であり、その影響は圧倒的であり、敵国の権力構造のすべてを麻痺させる可能性をもっている」と発言していた(17)ことからも導き出すことができる。

（４）あらゆる手段・戦い方を融合させたハイブリッド戦

ゲラシモフは非軍事手段だけでは収まらず軍事力の行使を要する事態に至った場合にも、従来とはまったく戦い方が変わったことを指摘し、「軍事的な戦いにおける性質の変化」ということを、図を掲げて説明している。（図４参照）

その中でゲラシモフは、従来から重視されていた大規模な地上軍（陸軍）を主体とする部隊による最前線での勝利を得るという純軍事的な戦い方から、政治目的達成のためには、軍事力と政治・外交・経済その他の非軍事的手段を複合的に組み合わせて戦うことの重要性を強調している。

特に、①平時とも有事とも判断のつかない状態から軍事行動を開始すること、②各軍種が各個に行動するのではなく、統合的に高機動で、かつでき得るならば非接触の軍事行動（情報戦・サイバー戦・電磁波戦などを念頭）で打ち勝つこと、③軍事施設のみならず重要インフラ、社会インフラなどの国家の核心施設を目標とし軍事力のみ

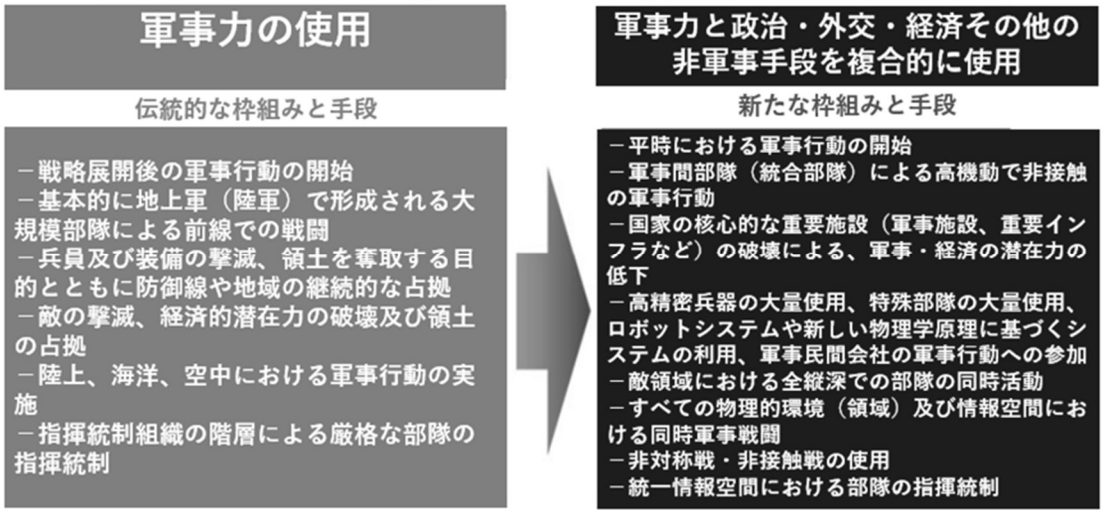
---

(16) 「軍事ドクトリン」の規定によれば、「軍事的な戦い」とは、国家間または国内の対立を、軍事力を使用して解決することの総称のことで、前述の４つの戦争・紛争の段階の総称を示す

(17) BBC, Russian military admits significant cyber-war effort, 23 Feb.2017 <http://www.bbc.com/news/world-europe-39062663>（2020.1.22）

ならず経済力をも低下させること、④高精密兵器、特殊部隊、ロボットシステム(18)や新しい物理学原理（量子コンピュータ、量子通信、量子暗号などを念頭）に基づくシステムを利用すること、⑤正規軍・非正規軍、民間軍事会社なども軍事行動に参加させること、⑥敵領域の全縦深（陸上、海洋、航空、宇宙、サイバー空間及び電磁波領域など）で同時に活動すること、⑦非対称戦・非接触戦を使用すること、などを重視した新しい戦い方を提言した。

図４　軍事的な戦いにおける性質の変化



（出典：図は「先見の明における軍事学の価値」から引用、訳文は筆者による）

（５）紛争・戦争の段階と「ハイブリッド戦」

前述のとおり、ロシアの軍事ドクトリンでは、紛争・戦争のレベルを「武力紛争」「局地戦争」「地域戦争」及び「大規模戦争」の４つの段階に区分している。ゲラシモフが論文で示した戦い方は、「軍事ドクトリン」の規定に当てはめると「武力紛争」を主として念頭に置いている。

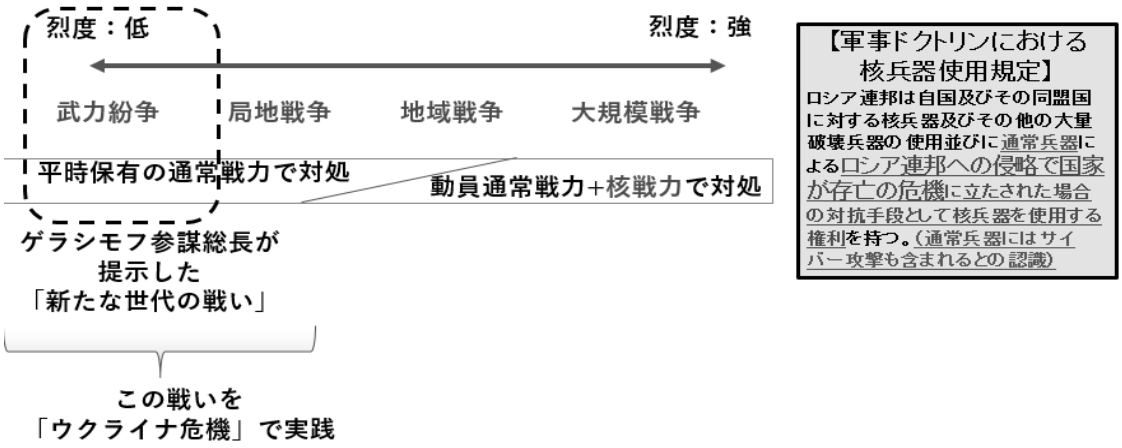
当然、あらゆる手段を融合させた戦い方というものは、従来からもロシアは実施してきたし、紛争・戦争のどの段階においても実施されるものである。そのカテゴリーに従来ではあまり言及されてこなかった「情報領域での戦い」、「電磁波領域での戦い」及び後述するが「認知領域での戦い」というものが加わったとも言えるのかもしれない。

「軍事ドクトリン」では、一義的には、「武力紛争」のような低烈度紛争を管理された紛争としてコントロールすることを目指すが、「武力紛争」以上の戦略にまで言及しており、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。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判断された場合は、戦術核を使用し、それを補完する。さらに

(18) ロシアでロボットシステムといった場合、自動化システム、無人兵器システムなどを指す

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。ロシアの核使用規定では、特に紛争・戦争の段階とは直接リンクしてはおらず、「ロシア連邦への侵略で国家が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もつ」とされている。すなわち、ゲラシモフが提示した低烈度紛争における「ハイブリッド戦」においても、核使用規定上は、核兵器の使用の可能性も考えられるということである。（図５参照）

図５　戦争・紛争のエスカレーションと核兵器使用規定



（出典：ロシア安全保障会議「軍事ドクトリン」を基に筆者作成）

実は、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た」と明言した(19)。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、ロシアが武力紛争の段階においても、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。つまり、「ハイブリッド戦」の最後の拠り所には核戦力も含まれているということである。

２　ハイブリッド戦の中核となる影響工作（Influence Operation）

（１）「フェイクニュース」に関連する用語の定義

前述したように、ロシアが掲げる「ハイブリッド戦」において中核と位置付けられているのは情報戦である。その中でも、近年、特に「影響工作」と呼ばれる戦い方が注目されている。

影響工作では、いわゆる「フェイクニュース」を使った情報操作、世論操作、対象国

(19) ロイター通信「プーチン露大統領、クリミア併合で『核兵器準備していた』」『ロイター通信 HP』2015 年３月 16 日<https://jp.reuters.com/article/ptin-idJPKBN0MC03220150316>（2020 年２月 26 日アクセス）

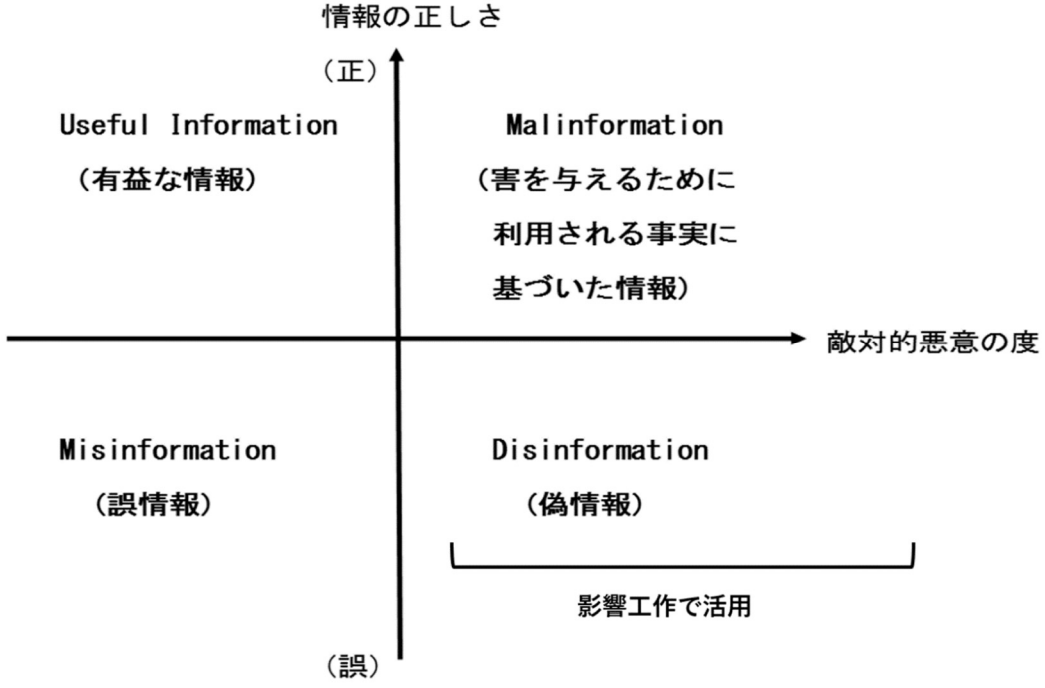
の国家分断及び不安定化・弱体化を企図している。ところが、「フェイクニュース」という用語を使用すると、論理的で事実に基づいた議論ができないという状況がしばしば生起している。そこで、これらに関連する用語を最初に定義したいと思う。

「フェイクニュース」 に関する議論の多くは、３つの概念、すなわち「誤情報（Misinformation）」「偽情報（Disinformation）」及び「害を与えるために利用される事実に基づいた情報（Malinformation）」を区別していない。しかし、「正しい情報」と「誤りの情報」及び「害を加えようとする『組織、国家等』によって作成、配布された情報」と、「そうでない情報」を区別することが重要である。

「誤りの情報」のなかには、単なる過失による誤りの情報若しくは悪意のないニセ情報である「誤情報（Misinformation）」と故意に国家や組織に危害を与えるために改ざんされた情報である「偽情報（Disinformation）」がある。また、同じ「害のある情報」でも、情報そのものは事実であるものの国家や組織に危害を与えるために使われる情報である「Malinformation」がある。これらをしっかりと区別をし、議論を進めていく必要があるということだ。

ロシアは、この中で「偽情報（Disinformation）」と「害を与えるために利用される事実に基づいた情報（Malinformation）」を組み合わせ、影響工作に活用していると考えられている。（図６参照）

図６　「フェイクニュース」に関連する用語の定義(20)



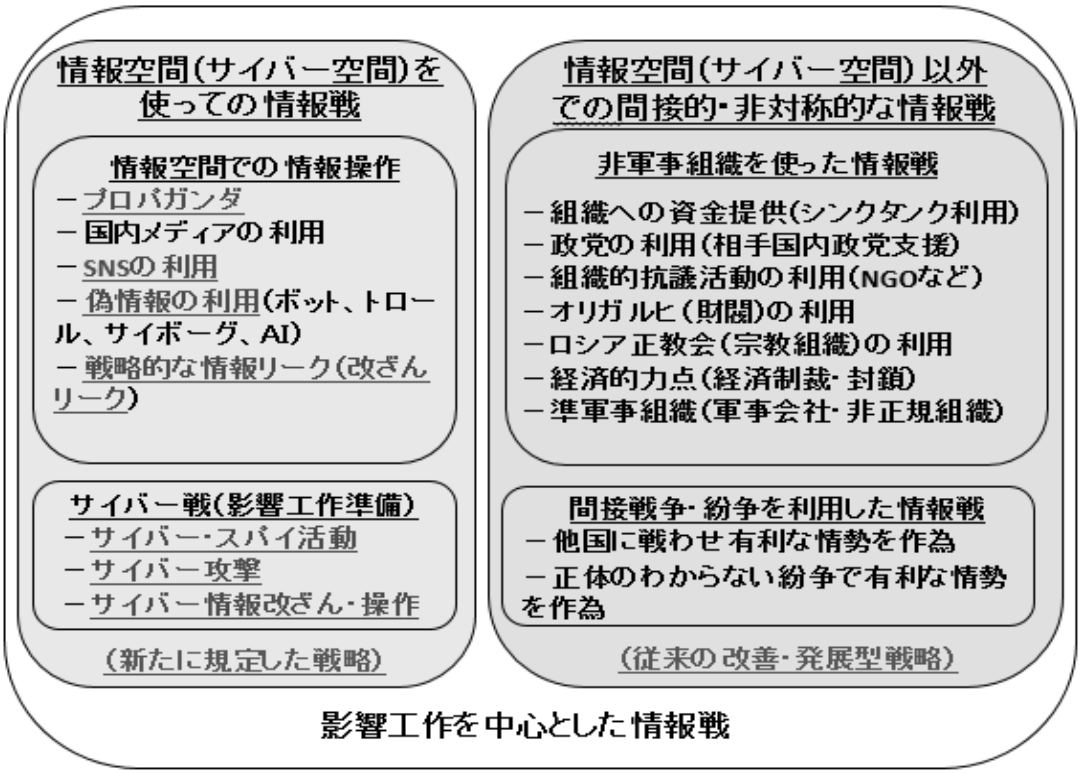
（出典：The Ethical Journalism Network, “The EJN Definition of Fake News” を基に筆者作成）

(20) The Ethical Journalism Network, The EJN Definition of Fake News, <https://ethicaljournalismnetwork.org/tag/fake-news/page/2> (2020.02.26)及び「第５回サイバーセキュリティ法制学会」における討議資料（2020 年１月 25 日）に基づく

（２）影響工作の主眼（第７の領域『認知領域』での戦い）

北大西洋条約機構（NATO）及び欧州共同体（EU）は、ロシアが近年、実際に行っている影響工作を中心とした情報戦を受けて、2017 年に「欧州ハイブリッド脅威対策センター（European Centre of Excellence for countering Hybrid Threat）」を創設した。同センターでは、ロシアの掲げる「新たな世代の戦い」を分析し、2018 年５月９日、「ハイブリッド脅威への対処（Addressing Hybrid Threats）」という分析結果を発表した(21)。同分析報告において、ロシアがハイブリッド戦において中核と考えているのは「影響工作を中心とした情報戦」であり、それは、政治・経済・情報やその他のあらゆる手段を使って政治目的を達成する戦い方であるとしている。その手法を大別すると、情報空間を使っての情報戦（情報操作やサイバー戦）と情報空間以外を利用しての間接的・非対称的な情報戦に分けられるとしている。（図７参照）

図７　影響工作を中心とした情報戦



（出典：「ハイブリッド脅威への対処」及び「先見の明における軍事学の価値」を基に筆者作成）

前者は、新たに強調された戦略であり(22)、情報空間において、SNS やメディアなど

(21) European Centre of Excellence for countering Hybrid Threat, Addressing Hybrid Threats, May 2018, < https://www.hybridcoe.fi/wp-content/uploads/2018/05/Treverton-AddressingHybridThreats.pdf#search=%27Addressing+Russian+Hybrid+Threats%27 >(2020.4.10)
(22) 今まであまり強調されていなかった「情報空間を使っての情報戦」という見地からは、新たな戦い方と言えるが、その手法、目的という見地では、従来から実施してきた「情報空間以外での情報戦」と同様の戦い方とも言える

を活用し、「偽情報」を大量に流布したり、「害を与えるために利用される事実に基づいた情報」を戦略的な情報としてリークすることにより、情報を操作し、世論を動かし、世論を分断させ、国家を不安定な状態にもっていく。これによって、政権を倒すなどのことを言う。その準備段階においては、影響工作で必要な情報を得るためのサイバースパイ活動や情報改ざん、情報操作などのサイバー攻撃が行われる。

後者の「情報空間以外での情報戦」は、従来からロシアが採用してきた戦略である。具体的には、シンクタンクなどの組織に資金援助をし、ロシアに有利な情報を発信させたり、親ロシアの政党を創設し情報操作を行ったり、非政府組織（NGO）などの組織にも同様の工作を行うなどの戦略である。旧ソ連諸国においては、引き続き影響力のあるオリガルヒ（ロシアの財閥）やロシア正教会（宗教組織）などを利用し影響力を行使することもある。さらに、民間軍事会社などの非正規な軍事組織を利用することも多いと言われている。前者との関係で言えば、インターネット・リサーチ・エージェンシー（IRA）といった組織(23)も利用され、情報空間を使った情報操作や世論誘導も実行されている。当然、政治目的を達成するために、前者と後者の戦略は、あらゆる手段を融合された形で実施されている。

これら影響工作の主要な舞台となるのは、「情報空間（デジタル領域）」や「情報空間以外の領域（物理的に存在する実体領域）」での活動と述べてきたが、それは手法の見地からの議論に過ぎない。影響工作の主眼は、これらの手法を使って、人間の脳内をコントロールするということである。すなわち、「認知領域」での戦いとも言えるだろう。

「認知領域」を制する戦いは、中国でも言及し始めたと伝えられており、「制脳戦」や「制脳権」といった用語も使われ始めた(24)。「制脳戦」では、これまで述べてきたように、情報を操作する、世論を誘導するといったことは勿論、政治指導者や軍指導者の脳を支配するといったことも重要となってきている。そうすれば、政治決断や軍事作戦の意思決定をコントロールすることも可能で、ロシアの主張する「物理的に戦わずに勝つハイブリッド戦」を、真に実現できるということだ。

ロシアが「ハイブリッド戦」の戦い方を、文書として明確にする前に研究対象にしたと見られる『超限戦』で描かれる「『あらゆる領域』を超えての戦い」の従来のカテゴリーに、「認知領域での新たな戦い」というものが加わったということである。言い換えれば、陸、海、空、宇宙の「実体領域」、サイバー空間を中心とする「デジタル領域」及び「米陸軍が提唱する第６の領域『電磁波領域』(25)」に引き続き、第７の領域

---

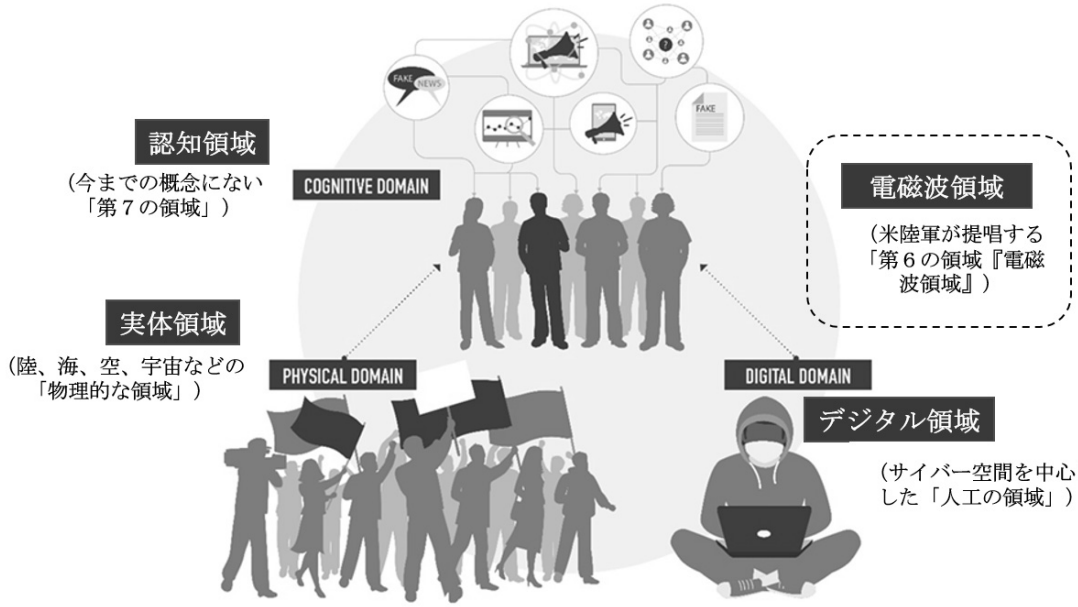
(23) 「インターネット・リサーチ・エージェンシー（Internet Research Agency）」とは、ロシア政府に近いとされる企業であり、人海戦術によって SNS を用いた世論操作を行った「トロール工場」としても知られる

(24) 土屋貴裕「ニューロ・セキュリティ――『制脳権』と『マインド・ウォーズ』」『KEIO SFC JOURNAL Vol.15』２０１５年２月１日<https://gakkai.sfc.keio.ac.jp/journal_pdf/SFCJ15-2-01.pdf>（2020 年２月 26 日アクセス）

(25) Headquarters, US Department of the Army, FM 3-38, Cyber Electromagnetic Activity, February 2014<http://fas.org/irp/doddir/army/fm3-38.pdf>（2020 年４月 10 日アクセス）

として「認知領域」が加わったとも言えるだろう(26)。これらの領域の関係(27)を提唱したデンマークの研究者フレミング・ハンセンが示した概念図を図８に示す(28)。

図８　「実体領域」「デジタル領域」及び「認知領域」などの関係



（出典：図は、Flemming Splidsboel Hansen, “Russian influence operations”から筆者作成）

（３）ウクライナ危機での具体的なロシアの行動(29)

ロシアは、旧ソ連諸国（CIS 諸国）に対しては、ロシアにとって特権的な利害のある国だという独特の安全保障観をもっている。したがって、この領域において、ロシアの国益が侵されたと判断した場合は、軍事力の行使も辞さないとの施策をとっている(30)。ウクライナ危機というものは、ロシアのこのような安全保障観の下で生起した

---

(26) フレミング・ハンセンが提起した「認知領域」を他の領域と同等に扱うことについては異論があると思われるが、本稿では、「超限戦」で謳われた「あらゆる領域を超えて」のカテゴリーを具体的に説明できる領域として是非取り上げたいとの見地から記述した。

(27) 米陸軍が提唱する「第６の領域『電磁波領域』」については、図８を提唱したフレミング・ハンセンは言及していない。しかしながら、サイバー領域と同様、実体領域間のクロスドメインとしての「人工の領域」という観点からは、「実体領域」「認知領域」とは別の領域として「デジタル領域」に近い領域として取り扱うのが適当と考えられる

(28) Flemming Splidsboel Hansen, “Russian influence operations”, Dansk Institut for Internationale Studier, 30 October 2018 <https://www.diis.dk/publikationer/russian-influence-operations> (2020.2.26)

(29)「ウクライナ危機」における情報空間でのロシアの行動を分析するには、情報セキュリティ上の証跡を一次資料として扱う必要があるが、これはセキュリティベンダーの内部資料であり、攻撃源の IP アドレスなどの生データは対外公開されないことが多い。したがって、本稿では、その一部を入手した欧州ハイブリッド脅威対策センターが取りまとめた分析レポート「ハイブリッド脅威への対処」を一次資料に準じて使用する。その関係上、分析元のフィルターがかかっている可能性もあるので、それをできる限り排除して記述することとした。

(30) この考え方は、2008 年８月、グルジア紛争後にメドベージェフ大統領（当時）によって明らかにされた。「特権的利害地域」と呼称され、グルジア紛争生起の根拠「外交５原則」の１つとして示された。

ということである。ウクライナにおけるロシアの国益が侵されたと判断し、影響工作を仕掛け非軍事手段のみで親ロシア政権を樹立し解決を図った。しかし、樹立した親ロシア政権への反発が想定したよりも強く、非軍事的な手段のみでは事態の収拾が難しいと判断したために軍事力を行使し、クリミア半島への軍事介入を実施したということである。この時に採用されたのが、ゲラシモフが提示したいわゆる「ハイブリッド戦」の戦い方であり、その中核を占めていたのが影響工作を中心とする情報戦であった。

ロシアは、影響工作を中心とした情報戦の有効性や非軍事手段と軍事手段の融合といった戦略の実効性を、クリミア侵攻に先立ち、様々な事例によって検証していたとみられる。すなわち、2007 年エストニアにおいて、影響工作を駆使しロシア人ハッカーを扇動して大規模なサイバー攻撃を引き起こすことにより国家機能を麻痺させた事例や、2008 年のグルジア（ジョージア）紛争時に、サイバー攻撃と物理的な軍事攻撃を同時に行った事例などがそれに該当する。

さて、今回取り上げる「ウクライナ危機（クリミア併合)」時にはどのようなことが実行されたのであろうか。本件に関しては、セキュリティベンダーからの一次資料を基に欧州ハイブリッド脅威対策センターが分析し「ハイブリッド脅威への対処」というレポートをまとめている。本レポート及びこれを研究した一田和樹氏の論考を基に、ウクライナ危機でのロシアの行ったハイブリッド戦を検証していきたい(31)。

クリミア侵攻に先立ち、2007 年以前からロシアと関係の深い APT28（FANCY BEAR)、APT29（COZY BEAR）といった組織がウクライナ国内のサイバー空間に入り込み、バックドア(32)を設置していたことが明らかになっている。その後、これらのバックドアを利用し、ウクライナ国内のインターネットサイトの改ざん事案が多数生起した。また、それ以前から、Red October、Mini Duke などのウイルスを利用したサイバー攻撃が行われ、ウクライナ国内の情報搾取や軍事行動支援のための情報操作などが行われていた。

侵攻前年の 2013 年には、ウクライナの複数のテレビ局関係者や親 EU の政治家などのサイトが分散型サービス拒否攻撃（DDoS 攻撃(33)）を受け、情報発信ができない事象が多数生起していた。

また、ウクライナ国内の通信インフラの大半はロシア製であり、ネットやシステムへの侵入方法、バックドア等は事前にロシア側に把握されていたとの情報もある。これは、サプライチェーンリスク(34)という見地から、根本的な問題である。

その詳細は、佐々木孝博「ロシアの対外政策構想と『特権的利害地域』」『国際情報研究』日本国際情報学会学会誌、2010 年 11 月 3 日参照

(31) この部分、一田和樹『フェイクニュース――新しい戦略的戦争兵器』（角川新書 2018 年 11 月 10 日）を参考にしている

(32) 「バックドア」とは、サイバー攻撃の手法のひとつ。一度サイバー攻撃により侵入した後に、攻撃者が入りやすい入り口を設置する。そのような攻撃の総称のこと

(33) 「DDoS（Distributed Denial of Service）攻撃」とは、攻撃目標のウエブサイトやサーバに対して大量のデータを送り付ける攻撃。受信側はトラフィックが異常に増大するので、負荷に耐えられなくなったサーバやサイトがダウンしてしまう

(34) 「サプライチェーンリスク」とは、部品の供給元やその従業員による、製品に対する不正プログラムの埋め込み、ハードウェアの不正改造などによって生じる情報セキュリティ上のリスクのこと

そのような準備を経て、第２段階として実際の情報戦が侵攻の１、２年前に行われていた。2012 年からは、ウクライナ国内のサイトの改ざんや多数の戦略的な情報のリークが行われ、2013 年～2014 年の間は、前述のマルウエアやバックドアを巧みに利用し、ボット、トロールまたはサイボーグ(35)などの手段により多数の「偽情報」が拡散され、ウクライナ国民の中で社会騒乱の状況が生まれた。さらに、ロシアによるクリミア併合に対する肯定的な情報やロシア軍に対する賛美の情報が国民の中に浸透していった。

しかしながら、これらの情報操作は、ウクライナ東部地区（親ロシア地域）及びクリミアでは成功したもののウクライナ全土にまでは浸透しなかった。そのため、事態を早期に収拾したいと考えたロシアは、クリミア併合の軍事作戦を強行したということである。

軍事作戦にあたっては、情報戦・電子戦及び旧来の兵器のあらゆる手段を用いて実施され、特殊部隊と空挺部隊は早期に重要施設を占拠した。並行してインターネット・エクスチェンジ・ポイント（IXP）(36)や通信会社の施設を軍事・非軍事の両手段により無力化し、ウクライナ国内の指揮通信能力を奪うことにも成功した。親 EU 議員の携帯電話やその SNS アカウントにもサイバー攻撃を実施し、ロシアに対する否定的な情報発信の場を奪うことも行った。

侵攻達成後にも影響工作は継続し、その結果「クリミア住民自身の希望によりロシアに帰属した」との住民投票の結果を得ることにも成功した。

（４）米大統領選での具体的なロシアの行動(37)

ロシア政府は否定しているが、ロシアが 2016 年の米大統領選に干渉したという事実が後に明らかとなった(38)。これを分析した前述の一田氏はその代表的な例が５つあると指摘している(39)。

第１は、民主党本部とクリントン陣営のメールをハッキングし、その内容を暴露したことである。本案件を捜査したのは特別検査官のロバート・モラーであり、彼を長としたチームがまとめた起訴状によれば、本案件に係わった組織はロシア国防省参謀本部情報総局（GRU）に所属する「第 26165 部隊」及び「第 74455 部隊」とされて

---

(35) 「ボット」とは、プログラムを使って機械が自動的にリツイートや発言をし、情報を拡散すること。「トロール」とは、いわゆる人海戦術で大量のリツイートや特定の発言を拡散すること。「サイボーグ」とは、それらふたつを組み合わせた手法のこと。今後、これらに加えて人工知能（AI）を使った攻撃が活発化することも見積もられている

(36) 「インターネット・エクスチェンジ・ポイント（IXP）」とは、インターネット事業者やデータセンタ事業者などが相互接続して、経路情報やトラフィックを交換するための接続点のことで、「IX」または「IXP」と略される

(37) 米大統領選におけるロシアの関与状況については、特別検査官ロバート・モラーが長としてまとめた起訴状に詳細がまとめられているが、これも前項と同様に、セキュリティベンダーが解析した一次資料を分析したものである。したがって、非攻撃者としてのバイアスも考えられるので、できる限りそれを排除し、記述することとした。

(38) US. Department of Justice, “Report On The Investigation Into Russian Interference In The 2016 Presidential Election”, March 2019 <https://www.documentcloud.org/documents/5955118-The-Mueller-Report.html>(2020.2.26)

(39) 一田和樹『フェイクニュース――新しい戦略的戦争兵器』、24 頁～42 頁

いる。GRU はロシア国防省におけるインテリジェンス組織であり、伝統的な情報活動は勿論、近年では情報戦・サイバー戦関連で大きな役割を担っている組織である。

第２は、選挙期間中、民主党全国委員会とクリントン陣営の選挙対策責任者であったジョン・ポデスタのメールをハッキングし、その内容をウィキリークスに公開したことである。ウィキリークスは 2006 年に開設した情報暴露サイトで、創始者のジュリアン・アサンジはロシアとの関係が疑われている。在英国のエクアドル大使館に身を寄せていたが、エクアドルの政治情勢も不安定なことから、次に頼る先をロシアと考え、ウィキリークスをロシアに有利な形で使用させることを条件に、ロシアからの支援を得ようとしていたとも言われている。

第３は、フェイスブックから約 8700 万人分の個人情報を窃取し、その内容を分析会社のケンブリッジ・アナリティカ社へ提供したことである。ケンブリッジ・アナリティカではこのデータをマイクロ・ターゲッティング(40)に利用したと言われ、その結果は当然選挙戦でも存分に活用されたと見られている。

第４は、ロシアの IRA がフェイスブックに虚偽の広告を多数出稿し、約１億 5000 万人が閲覧したと言われている事例である。人種問題、銃問題、LGBT 問題など世論が分断されるような問題を敢えて広告として投稿し、米国社会の分断を企図したと言われている。「偽情報」を使った世論誘導は、たとえ誘導がうまくいかなくても、世論を分断し、社会的な対立や社会騒乱を生起させることで政治・戦略目的を達成することができる。今回の事案においては、社会的な対立や社会騒乱を生起させる目的で当該戦略を採用したと見られている。

第５は、ロシアは IRA を使って組織的に SNS で「偽情報」を拡散していたことが確認されている。これまでに、IRA が 470 個のフェイスブックアカウントを利用し、８万を超えるコンテンツを作って情報操作を行っていたことが分かっており、大統領選では約１億 2600 万の米国人に閲覧させることに成功した。

これらは、主として、人海戦術の「トロール」という手法によって行われていたが、「ボット」というプログラムによる「偽情報」の拡散手段も併用されていた。セキュリティベンダーによる証跡の解析により、これらの事案は、ほぼロシアの関与によるものであることが明らかとなった。

同じく訴状によれば、ツイッターで３万 6000 以上のシステムによって自動的に運用される SNS アカウントが米大統領選での「つぶやき」を行っており、その「つぶやき」に対し 13 万回ツイートされたとのことである。ツイッター社によれば 3841 のアカウントが IRA と何らかの関係があるとされている。これらの「つぶやき」は米国内のメディアや著名人によっても拡散され、ロシアが意図した以上に「偽情報」が広まっていたという状況であった。

一田氏はさらに、これらの手法により情報操作された米国大統領選では、ロシアが狙っていた２つの政治・戦略目的を達成したと指摘している(41)。

---

(40) 「マイクロ・ターゲッティング」とは、選挙運動やマーケティングなどで、対象とする個人に関する情報を詳細に分析し、嗜好（しこう）や行動パターンを把握することによって選挙やマーケティングに役立てるなどのビッグデータシステム及びその戦略の総称のこと

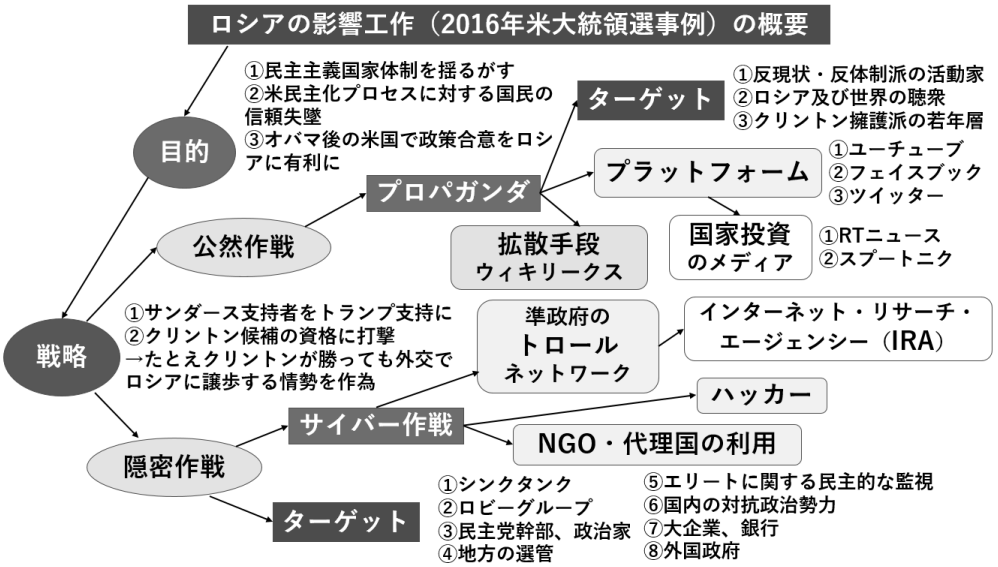
(41) 一田和樹『フェイクニュース――新しい戦略的戦争兵器』、33 頁

第１は、「偽情報」の拡散、情報改ざんや情報リークなどによって、ロシアの国益上、より好ましいトランプが優勢な情勢を作為することに成功したということである。この政治目的を、軍事力などの物理的な強制力を行使することなく、最低限の費用と最低限の労力で成し遂げたということである。

もう一点、ロシアが成し遂げた政治目的とは、大統領選に介入したということを秘匿することはせず、敢えて証跡も残しておくことにより、干渉したという事実そのものを拡散したということである。その結果、米国内に民主主義と現政治体制への不信感を植え付けることにも成功し、米国内に対立や混乱を生起させ、政治的安定性も奪ったということだ。

戦略・政策分析組織の「36th parallel」が、これらを体系的に分析し、ロジックツリー図としてまとめ上げた。その簡略図を図９に示す。

図９　２０１６年の米大統領選挙におけるロシアの影響工作(42)



（出典：36th-parallel, “Analytic Brief: Influence Operations, Targeted Interventions and Intelligence Gathering: A Primer.”を基に簡略図を筆者作成）

この図から、ロシアはこの影響工作において、米国の民主主義国家体制そのものを揺るがし、米国の民主化プロセスに対する国民の信頼を失墜させることを主目的にしていたということを読み取ることができる。米大統領選での関与事案は、戦略及び作戦で「クリントン候補を貶める」「情報を改ざんして情報操作する」「戦略的に情報をリークして世論を誘導する」など、目に見える結果や手法だけに目が行きがちであるが、その本質は、「民主主義体制そのものの根幹を揺るがすこと」にあったのではないかということである。

そうすれば、西側諸国が長年培ってきた民主主義による国家の統治体制を揺るがし、

(42) 36th-parallel, “Analytic Brief: Influence Operations, Targeted Interventions and Intelligence Gathering: A Primer.” September 23, 2017<https://36th-parallel.com/2017/09/23/analytic-brief-influence-operations-targeted-interventions-and-intelligence-gathering-a-primer/>(2020.2.26)

政治指導者に適切な政治を行わせず、国力そのものを大きく減じることも可能となる。結果として、相対的に相手方の力を減じることができる。ロシアの立場からすれば、物理的な軍事力を行使せずとも、あらゆる制限を超え、民主主義国家の普遍的な価値を貶めることにより、相手を打ち負かすことができるということである。真に、中国発の「超限戦」を昇華させた「あらゆる制限を超えたハイブリッド戦」を実行に移していると言えるだろう。

なお、本事案の本質が「民主主義体制そのものの根幹を揺るがすこと」との 36th-parallel の行った分析結果には異論もある。しかし、2019 年 9 月に、サイバーコマンド司令官兼国家安全保障局（NSA）長官ナカソネ大将、国防情報局（DIA）長官アシュレイ中将など政府高官を始めとする産官学の主要なメンバーが参加し（筆者も参加）実施された「INSS : Intelligence and National Security Summit（於 : ワシントン DC)」でも主要な議題として討議された内容であり、米国の産官学共通の見解だと考えられる。

（５）ハイブリッド戦の制約

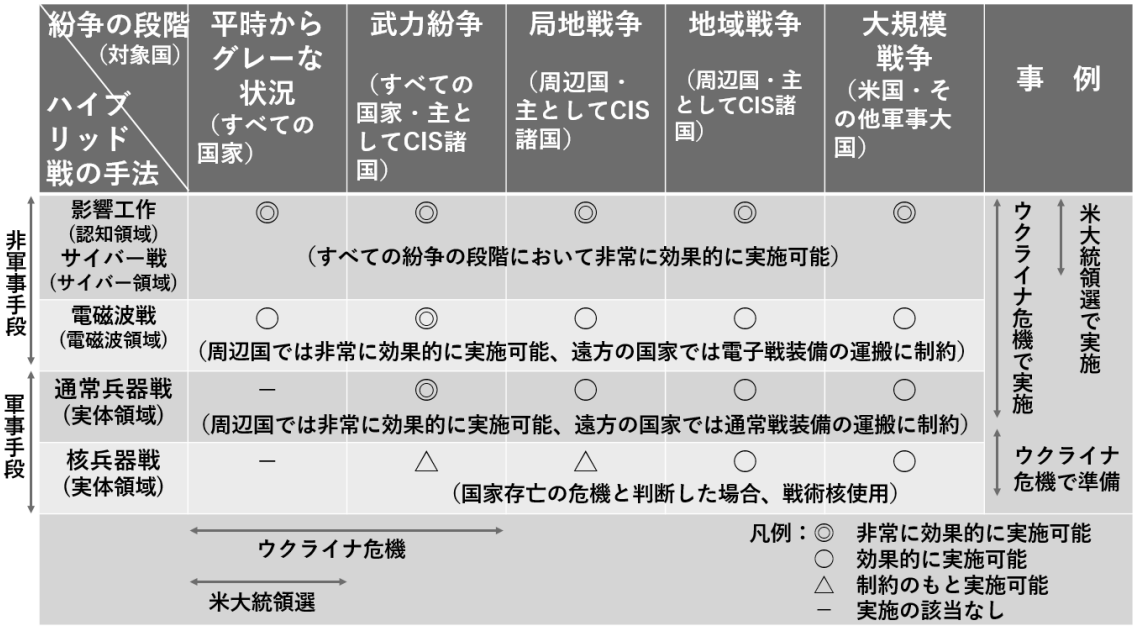
前述のとおり、ロシアの採用する「ハイブリッド戦」は、あらゆる紛争・戦争の段階でも用いられるものの、主たる対象は「武力紛争」の対象となる「旧ソ連諸国（CIS 諸国)」と考えられる。事例研究で掲げた国土を接する隣接国ウクライナにおいては、ゲラシモフが掲げた「ハイブリッド戦」は、非軍事・軍事のあらゆる手段を活用し有効に機能することが証明されたと言えるだろう。

事例でいま一つ掲げた米国の状況はどうだろうか。米国に対しては、「ハイブリッド戦」のうち、影響工作を中心とした情報戦及びサイバー戦のみを用いた事例であった。

サイバー空間を巧みに利用し、米国の世論を誘導し、情報を操作することにより、ロシアにとって都合の悪い候補者にダメージを与えることには成功した。また、人種問題、銃問題、LGBT 問題などにおいて米国世論を分断すること、選挙結果や政権に対する信頼度を低下させることには成功した。それ以上の軍事紛争へのエスカレーションをそもそも戦略目標としてはもっていなかったという事由はあるが、仮に、軍事紛争にまで踏み込む必要性があったとしても、米国のような大国や遠隔の諸国などに対しては、グルジアやウクライナなどの CIS 諸国に実施したように、影響工作・情報戦から要すれば軍事力行使まで行うというフルスペックな「ハイブリッド戦」を適用することは困難である。軍事装備や兵員など軍事力を遠方に展開するには制約があるということだ。この点が、ロシアの「ハイブリッド戦」の制約、言い換えれば、ロシアの軍事戦略そのものの制約とも言えるところであろう。そのために、最後の拠り所として、核への極度の依存というものがあるのかもしれない。すなわち、影響工作及びサイバー戦以外の戦い方については、制約があるということだ。定性的な評価にはなるが、ハイブリッド戦で主に用いられる手法、平時から始まる紛争・戦争の段階とその対象国などの関係をまとめた概要図を図１０に示す。

図から、「『影響工作』『サイバー戦』といった非軍事手段は平時からあらゆる紛争・戦争の段階においても非常に有効に機能すること」、「非軍事・軍事のあらゆる手段を使ったフルスペックなハイブリッド戦が有効に機能するのは、主として『武力紛争』などの低烈度紛争であること」などを読み取ることができる。

図１０　ロシアのハイブリッド戦の制約



（出典：本稿引用の各種資料・文書から筆者作成）

また、参考ながら、米大統領選で重視された世論誘導や情報操作による影響工作においては、言語的な特性が存在していたことも確認されている。このキャンペーンへの関与が疑われている IRA が行った作戦には、複数の言語が使用されていた。ところが、その大半はロシア語及び英語であったことが確認されている(43)。つまり、ロシア語圏や英語圏以外の国家に対しては、ロシアによる影響工作は、効果的に実施できないのではないかという疑問があるということだ。英語圏、ロシア語圏以外の言語圏（アラビア語圏、中国語圏、日本語圏など）においては、大々的な影響工作事案が確認されていないことからこのような疑問が生じている。この要因には言語特性以外の要件も考えられるため、引き続き注視していかなければならないだろう。

しかしながら、仮に影響工作に言語的な制約があったとしても、近年、言語領域における人工知能（AI）の能力が革新的に向上している状況から、言語に起因する制約については、早期に解消してしまうだろうということは付言しておきたい。

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

(43) University of Oxford, The IRA, “Social Media and Political Polarization in the United States, 2012-2018”, December 22, 2018, <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf>(2020.2.26).、本引用元のツイッターに関するデータによれば、57%がロシア語、36%が英語、残りが複数の言語であったことが判明している

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。これらの考え方は、2013 年にゲラシモフ参謀総長が示した安全保障論文に起因しているが、後にその内容は「国家安全保障戦略（2015 年改訂）」や「軍事ドクトリン（2014 年改訂）」にも反映され、正式な国家戦略となっている。

ここで特に重要視されるのが、「影響工作を中核とした情報戦」であり、影響工作での戦いは、陸・海・空・宇宙の「実体領域」、サイバー空間を主とする「デジタル領域」及び米陸軍が提起する「電磁波領域」に引き続く、第７の領域「認知領域」での戦いとも言えるだろう。認知領域での戦いでは、人間の脳をコントロールすることが重要であり、「制脳戦」といった戦いとも言えるだろう。ロシアは、認知領域での戦いにおいて優越を確保するために「影響工作」を実施し、「戦わずに勝つこと」を目指している。

これらのロシアの戦略は、中国の「超限戦」に謳われた「あらゆる限度を超え、あらゆる領域を超えた戦い」をロシアが従来から保持している戦略に取り入れ、体系的な文書として作り上げ、それを現実に移しているとも言えるだろう。

「超限戦」の戦い方が民主主義諸国にとって衝撃だったのは、その本質が「目的のためには手段を選ばない。制限を加えず、あらゆる可能な手段を採用して目的を達成する」ことを徹底的に主張していたことである。民主主義諸国の基本的な価値観（生命の重視などの倫理、法の順守、自由主義の追求、基本的人権の確保など）を重視せず、あらゆる制限（作戦空間、軍事と非軍事、正規と非正規、国際法など）を超越する戦いを公然と主張しているということである。

換言すれば、我々西側諸国が長年培ってきた「民主主義の価値観と体制への挑戦」だとも言えるだろう。ロシアの行う「影響工作」に対しては、ファクトチェックを行うなどの対応策がとられているが、決定的な策とは言えず、効果的な対応策は現在のところ見つかっていない。本論でも取り上げた、INSS の会議では、人工知能（AI）による世論の監視システムや常続的な監視組織の必要性なども議題にあがっていたが、その実現性も様々な面から困難である。いずれにしても、そのようなロシアの脅威（中国も同様な行為を行っていると見積もられる）に直面する西側諸国にとって、この脅威に如何に対処していくのかが、対中国を含めた今後の我が国の安全保障にとっても重要な課題となっていくことと考える。

［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　　修士（国際情報）
米海軍第３艦隊連絡官　海幕副官
ゆうべつ艦長　在ロシア防衛駐在官
第８護衛隊司令　統幕サイバー企画調整官
指揮通信開発隊司令　下関基地隊司令を歴任
２０１８年退官

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