NIDS 防衛研究所
The National Institute for Defense Studies

多次元統合防衛力の構築にむけて－１
－グレーゾーンの事態への対処を中心に－

中野　義久　副所長

NIDSコメンタリー
第 127 号 2020 年 7 月 7 日

はじめに

「平成 31 年度以降に係わる防衛計画の大綱」（以下、「30 大綱」と記す）において、多次元統合防衛力が必要とされた。そしてその構築には、第一に宇宙・サイバー・電磁波といった新たな領域及び陸海空の従来の領域における個別の能力の質及び量を強化すること、第二に、全ての領域における能力を有機的に融合し、その相乗効果により全体としての能力を増幅させる領域横断（クロス・ドメイン）作戦能力を充実すること、そして第三にその実行のため、陸海空自衛隊が縦割りに陥ることのない統合運用の一層の推進が求められる。本稿ではそれぞれの領域において強化される個別の能力を融合した領域横断能力の充実と、そのための統合運用の推進のあり方について、グレーゾーンの事態を焦点にして考察する。

１ シームレスな活動のためのグレーゾーンの事態の重要性

「30 大綱」では平時から有事までのあらゆる段階においてシームレスに活動することが必要とされているが、中でも平時と有事の区別の不明確なグレーゾーンの事態への対応が重要である。なぜならグレーゾーンの事態では、平素から「ハイブリッド戦[1]」のような軍事と非軍事の境界を曖昧にした多様な手段による活動が国家間の競争の一環として行われ、これが長期にわたり継続し増加拡大していく可能性があるとともに、明確な兆候のないままより重大な事態へと急速に発展することが懸念されるからである。我が国としてのグレーゾーンの事態への対処のためには以下の点が重要となる。

第一に、我が国周辺でのグレーゾーンの事態[2]では力による現状変更が、武力紛争に至らないレベルで長期的かつ継続的になされているため、国家をあげて防衛力の発揮ができないまま、現状変更が相手に有利になされてしまう可能性がある。2014 年のウクライナ危機では、NATO 諸国が本格的な対応をとる前に限定的な軍事侵攻によって現状変更がなされたことを教訓とし、NATO として２～３日以内に出動が可能な高度即応統合任務部隊(VJTF)を編成し、その一部をバルト三国及びポーランドにローテーション展開して、現実の脅威に対抗している[3]。一方で我が国周辺では、現状変更を狙う側は海上法執行機関が最前線で活動し海軍がその後ろ

1 国家間の競争は、軍や法執行機関を用いて他国の主権を脅かすことや、ソーシャル・ネットワークサービスなどを用いて他国の世論を操作することなど、多様な手段により、平素から恒常的に行われている。こうした競争においては、①国籍を隠した不明部隊を用いた作戦、②通信・重要インフラへのサイバー攻撃、③インターネットやメディアを通じた偽情報の流布などによる影響工作などを組み合わせることで、軍事と非軍事の境界を意図的に曖昧にした現状変更の手法、いわゆる「ハイブリッド戦」が採られることがあり、相手に軍事面に止まらない複雑な対応を強いている（防衛省編「令和元年版 防衛白書」2019 月）41 頁)。

2 平成２７年５月の閣議決定では、治安出動・海上警備行動等の発令手続の迅速化等が必要な事態として、①国際法上の無害通航に該当しない航行を行う外国軍艦への対処、②離島などに対する武装集団による不法上陸への対処及び、③公海上で日本の民間船舶に対し海賊行為を行う外国船舶を自衛隊の船舶などが認知した場合としたが、本稿では領土などの現状変更に直接関わる②を検討の主対象とする(「平和安全法制等の整備について」内閣官房)。https://www.cas.go.jp/jp/gaiyou/jimu/housei_seibi.html。

3 「令和元年版 防衛白書」152 頁。

盾となり、大量の漁船と公船が領海侵入を繰り返している。現状変更側が時間と空間でイニシアティブを保持し、現状維持側が強制力の使用に踏み切るレベルを超えないようその活動隻数や日数を徐々に増やすことなどで既成事実化を図っているため、事態が固定化され回復不能な段階に陥る前に現状変更側のとるあらゆる挑戦への対処を継続していくことが必要である[4]。

第二に、グレーゾーンの事態の拡大を防ぎつつ有利に解決するためには、事態が拡大した場合には防衛する側が有利となる意思と能力を示すこと（「エスカレーションの窓を閉じない」）が必要である[5]。現状変更側は武力紛争レベルでは不利だと分かっているので、グレーゾーンの事態を活用するのであり、事態の拡大が高い確率で予想されれば、最初の段階で抑止されると考えられるからである[6]。

第三に、ハイブリッド戦においては、現実の戦場に加え、サイバー空間そして認識形成に影響を与える情報空間などにも対処が必要である。このような手段は従来から「非軍事の戦争行動[7]」などとされてきた。さらにゲラシモフ・ロシア軍参謀総長によれば、現代戦では政治・軍事目的を達成するために、非軍事的手段の役割は拡大し軍事的手段と非軍事的手段は１：４の比率で遂行され、軍事的手段は最後の成果を獲得するために活用されるとしている[8]。ウクライナ危機においては、分離独立のための秘密工作と通常戦力による持続的な脅威や「リトル・グリーンメン」と呼ばれる徽章を着けない国籍不明の部隊の活動に加え、スマートフォンへの配信などによる偽情報の宣伝作戦が行われた[9]。ハイブリッド戦の脅威に対して NATO は、情報戦、サイバー脅威、軍事的威嚇への対処能力の構築を図っている[10]。グレーゾーンの段階においては、現状変更側がとる様々な非軍事的手段に対し、平時からその兆候を早期に把握し対処することが重要となる。

このように平時から有事までのあらゆる段階におけるシームレスな対処のためには、グレーゾーンの事態での武力紛争に至らない軍事・非軍事手段に対して確実に対応して事態の拡大を避けつつ有利に解決するとともに、同時に我が国防衛につながる事態拡大にも備えた多様な手段を保持することが必要である。

2　グレーゾーンの事態において事態を拡大させずに有利に解決するための領域横断作戦

(1) 新たな領域における能力の活用と相互抑止の追求

グレーゾーンの事態では、新たな領域における非物理的な手段がそれと認識されないままとられることが予想され、その脅威に適切に対処することが事態の拡大防止につながる。特にサイバー空間においては、指揮統制や社会インフラ等の妨害は全ての領域での能力発揮に大きな影響を及ぼすため、平素から相手のシステムの脆弱性の偵察等を行ってお

---

4 武居智久元海上幕僚長「海上防衛戦略の新たな時間と空間」『海幹校戦略研究』特別号(2016 年 11 月)8-9 頁。

5 Sugio Takahashi, “Development of gray zone deterrence: concept building and lessons from Japan’s experience” *The Pacific Review*, Vol31, No.6 (2018) p. 800.

6 それでも、現状変更の更なる小規模な挑戦は抑止できないため、武力紛争以下では拒否的抑止が主となる(同上 797 頁)。

7 「軍事」的な手段に加え、「超軍事（外交戦、インターネット戦、情報戦、心理戦など）」及び「非軍事（金融戦、貿易戦、法規戦、メディア戦など）」の作戦様式を組み合わせることで「戦わずして人の兵を屈する」までは達しなくとも「巧みに戦って人の兵を屈する」ことができるとしている。喬良、王湘穂(劉琦訳)『超限戦:21 世紀の「新しい戦争」』（角川書店、2020 年）204-206 頁。

8 General of the Army Valery Gerasimov, Chief of the General Staff of the Russian Federation Armed Forces, “The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations,” *Military Review* (January/February 2016), pp. 24-25.

9 キア・ジャイルズ「『ハイブリッド戦争』とロシアの陸上戦力」『平成 30 年度国際シンポジウム 新しい戦略環境と陸上防衛力の役割』（防衛研究所、2019 年１月）91-101 頁。

10 Diego A. Ruiz Palmer, “Hybrid Warfare in a Contested World Order: Insights and Implications,” *Foreign Expert Perspective* No.001, The National Institute of Defense Studies (NIDS) (June 2017) pp1-4. また NATO として、戦略コミュニケーションセンター（ラトビア・リガ）、サイバー防衛協力センター（エストニア・タリン）、ハイブリッド脅威対策センター（フィンランド・ヘルシンキ）を創設している。

き、武力攻撃に先立ちサイバー奇襲を追求することが考えられる[11]。このため「30 大綱」では、サイバー空間の常時状況監視や被害の局限・復旧等についての能力を強化し、サイバー脅威に対する抗堪性を向上するとしている。さらに有事において「相手方によるサイバー空間の利用を妨げる能力」を保有することは、日米共同も踏まえサイバー空間での抑止力となる可能性もある[12]。

宇宙空間でも、サイバー攻撃の他、電磁波などを利用した非物理的な攻撃により、情報収集機能や通信機能等の衛星等を無力化して、宇宙のインフラの活用を妨害されることも予測される[13]。宇宙の領域においては、領域専門部隊として航空自衛隊に宇宙作戦隊が発足し、宇宙状況監視（SSA）のための SSA レーザ測距装置や SSA 衛星、レーダーを活用した能力の保持などにより衛星の軌道位置修正を通じた被害回避が可能となる他、今後はレジリエンシーを重視した「否定的抑止」による衛星等の抗堪性向上を図らなければならない[14]。加えて電磁波領域は、電子戦さらにサイバー領域とも関連するとともに、「30 大綱」では相手からの妨害を局限し、レーダーや通信機を無力化する能力を強化するとしており、宇宙を含む領域において相手の行動を妨害することにつながる。

以上のように新領域における相互に密接に関連した脅威への有利な対処は、今後更なる整備の必要はあるが、その能力の非物理的使用によって相手の行動を妨害することで、ある種の相互抑止の成立が期待される[15]。そしてこの相互抑止に基づけば、グレーゾーンの事態の初期の段階で新領域における脅威に有利に対処することにより事態の拡大の抑制につながるとも考えられる。

(2) 力による現状変更への実効性のある対処

現状変更の挑戦に対しては法執行機関による対処が基本となるが、同時にあらゆる段階に応じた次のようなシームレスな手段が必要とされる。

第一に、法執行能力と防衛力の連携の一層の充実・向上である。これまで警戒監視活動による情報の共有や、海上自衛隊と海上保安庁間の共同訓練の他、自衛隊に対する治安出動・海上警備行動の迅速な発令の努力などがなされてきた。これは自衛隊を活用した法執行権限行使の迅速拡大のための「上→下」のアプローチであると言えるが、自衛隊の投入が事態の拡大に与える影響や、両者の役割分担の切れ目を防止する観点から、海上保安庁の権限拡大を通じた「下→上」の更なる機能強化も含めた検討も必要とされている[16]。

第二に、日米の共同対処による「エスカレーショ

---

11 伊藤寛『サイバー戦争論：ナショナルセキュリティの現在』（原書房、2016 年 8 月）46-47 頁。

12 八塚正晃「サイバー安全保障に対する中国の基本的認識」『NIDS コメンタリー』60 号（防衛研究所、2017 年 5 月）4-5 頁。

13 宇宙インフラの利用妨害の非物理的な手段は、①、軌道上の衛星に対する指向性エネルギーによるセンサーの「目くらまし」と「目つぶし」、②衛星と地上局間のリンクに対する電子妨害として「ジャミング」や「スプーフィング」、③地上セグメントに対する妨害、④サイバー攻撃がある。福島康仁『宇宙と安全保障－軍事利用の潮流とガバナンスの模索』（千倉書房、2020 年）94-103 頁。

14 ①衛星や地上局等の宇宙システムの強靭化（サイバー攻撃に対するソフトウェア面での強靭化を含む）②安全保障目的の衛星機数の増加（即応型の小型衛星というより安価な衛星を用いた機数増も含む）③米国を中心に友好国の衛星に相乗りペイロードを搭載しあうこと（「ホステッドペイロード」）などがある。青木節子「宇宙利用上の脅威と日本の対応」『平成 27 年度安全保障国際シンポジウム 宇宙安全保障：諸外国の動向と日本の取組み』（防衛研究所、2015 年）111-112 頁。

15 高橋杉雄「平和安全法制とグレーゾーン－評価と今後の課題－」『国際安全保障』第 47 巻第 2 号（2019 年 9 月）49-50 頁。さらに新領域の非物理的使用は、物理的損害を与えないので活用に制約はないとの議論がある一方で、事態概念と連動させてその使用基準を設定すべきという考えもある。

16 神保謙「シームレスな安全保障体制への課題：「グレーゾーン」事態からのエスカレーションを巡って」『安全保障政策のリアリティ・チェック』（日本国際問題研究所、平成２９年３月）37 頁。また法執行機関が武装集団による不法上陸という主権侵害を阻止するために、海保法における工作船等に対する停船射撃の規定(20 条 2 項)のような、正当防衛に該当しない場合でも、上陸阻止を目的とする危害射撃を可能とする権限を新設すべきとする意見もある。一方、自衛隊の投入に際しては、軍事力の先制投入と見られることを防ぐため、①海保による海自の統制、②海自の行動は法執行活動でのある旨の電光掲示板などによる明示や③海上民兵の実態の分析とそれへの対応の正当性の公表などの処置も指摘される。NPI グレーゾーン事態研究委員会「海と空のグレーゾーン事態への対処－その問題と対策－」(2018 年 6 月)4-12 頁。

ンの窓を閉じない」方策がグレーゾーンの段階から重要となる。我が国は、「30 大綱」において島嶼部を含む我が国に対する攻撃に対しては、平素からの南西地域への陸上・航空自衛隊の充実や水陸機動団の能力向上に加え、部隊の迅速な機動・展開、海上・航空優勢や、占拠された場合のあらゆる措置を講じた奪回を明示している。一方で日米同盟の観点からは、現状変更を狙う側が、米国の拡大抑止の信頼性とそのためのコストとの観点から、「尖閣パラドックス」[17]につけ入る可能性があるため、日米のグレーゾーンの事態からの密接な連携を確保しておくことが重要である。この点、自衛隊と連携して活動する米軍艦艇等への防護のための武器使用が可能になったことは、平時からシームレスな両国間の運用協力の実効性を高め、日米同盟の信頼性の強化につながると言える[18]。

(3) 情報空間での有利な影響力の発揮

非軍事的手段は国民の政府への信頼を揺るがせ、社会的分断を深刻化させることで国家としての対処を妨害するために活用されてきたが、中でも情報空間における影響工作[19]はソーシャルメディア(SM)の発展により巧妙化し、ネットの果たす役割は拡大している[20]。ハイブリッド戦の影響工作は相手国に存在する反政府感情、反欧米感情や民族主義による政治・社会的亀裂を刺激し続け、国内に「継続的に機能する前線」を出現させ、自らに有利な戦略環境を創造することを狙う[21]。例えばロシアは、旧ソ連諸国に居住するロシア系住民を、代理勢力としてまた自国民保護の政治的さらに軍事的介入の理由として利用しうるとともに、その働きかけの手段として SM や政府系マスメディアを用いて偽情報を発信し、受け手となる人々のもともと有している政治的選好を一層強化し動員を促進する可能性もある[22]。ネットによる影響工作の拡大は現実の戦場での行動に次のような変化を及ぼした。

第一に、ネット上では軽易に情報発信ができるため、事実と意見の区別のない情報が市民と戦闘員の区別なく拡散し、情報操作による国民の意見の分断が容易になった結果、実際の行動がネット上での世論に影響を受けるようになった。それはネット上では事実の正確さよりも注目度が重視されるため、同じような考えを持つフォロワー間でなじみがあるか好みに合う情報は広く拡散され、何百万人もがシェアしてしまえば、フェイクニュースであっても現実であると認識されてしまうからである[23]。現在の新型コロナウイルスを巡っても、有害デマの拡散によって現実社会に混乱を生むとともに、悪質な偽情報は国家間の摩擦の火種にもなりかねないことが懸念されている[24]。またネット空間ではサイバー攻撃と連携した情報操作によって米大統領選などへの介入が疑われているが、我が国においても社会的争点となり得る歴史問題や基地問題などの情報を操作し、「継続的に機能する前線」をあらかじめ出現させ現状変更の条件整備として国論を分断す

---

17 ワシントンは、比較的重要でもないことについて、拡大抑止の信頼性を確保するために核戦争も含むかも知れない大国間の紛争の危険を冒すのか。その国益はそのような危険を冒すには小さすぎるのではないか。一方で、何もしないことは米国の条約上の義務を果たすことにならないのではないか。Michael O'Hanlon, "Can America Still Protect Its Allies? : How to Make Deterrence Work," *Foreign Affairs*,(September/October, 2019), p. 200.

18 神保　32 頁。

19 影響工作は、対象とする地域での信条や行動に影響を与えて有害な社会的・政治的・経済的結果を生み出す情報を作り出し拡散する意図的かつ組織的な行動である「敵対的社会操作(Hostile Social Manipulation)」とも解釈できる。Michel Mazarr, *Hostile Social Manipulation: Present Realities and Emerging Trends* (Rand Corporation, 2019), p. 15.

20 ソーシャルメディアは社会的操作のための一手段であり、印刷物を含む従来の手段も使用されるが、ネット上は少数の bot とよばれる自動化されたアカウントが発信するコンテンツの多くの割合を占め、意見操作を行う手段として活用される。Ibid.p21.

21 志田淳二郎「クリミア併合後の『ハイブリッド戦争』の展開―モンテネグロ、マケドニア、ハンガリーの諸事例を手がかりに」『国際安全保障』第 47 巻第 4 号（2020 年 3 月）23 頁。

22 澤田寛人「ロシアによる「ハイブリッド戦」のとらえ方」防衛研究所編『東アジア戦略概観 2020』（防衛研究所、2020 年 3 月）159 頁。

23 P・W シンガー、エマーソン・T・ブルッキング(小林由香利訳)『「いいね！」戦争：兵器化するソーシャルメディア』、（ＮＨＫ出版、2019 年）193-210 頁。

24「データの世紀 上：新型コロナ、止まらぬ情報汚染－有害デマ視聴 1 億回超」『日本経済新聞』2020 年 5 月 4 日。

ることも予想される。

第二に、コンテンツの発信と共有は現実の行動と同時並行的にネット上で展開され、そのコンテンツも動画の活用が容易になったため[25]、現実の結果が正しく理解されるためにはリアルタイムでの対応が重要になっている。ネット上で戦闘場面の動画が出回り公開戦争の様相を呈する一方で、世界中の人々の反応を無視して「我々はやるべきことをやっている。後で説明する。」というわけにはいかなくなり、SM 向けに翻訳したメッセージをリアルタイムで発信しなければ、逆に操作された情報が拡散し、世界中でこれが現実であると認識されてしまう[26]。特に我が国の場合、海上や離島などは閉鎖空間であるため、法執行機関や自衛隊の活動の様子が、偽造された動画や事実ではあるものの全く違う場面の動画などの一方的な拡散によって、正当性が疑われる事態が生起する恐れもある。

ネット上でのこれらの問題に対しては、SM のアルゴリズムの修正や法的な書き込み規制などの対策も検討されているが、社会的な偽情報の発生・拡大を阻止するための国全体の取組が必要とされている。基本的に民主主義国家では偽情報に脆弱であるものの、国民全体に向けた情報リテラシー教育により批判的思考を養成して自ら正しい情報に基づく判断を行うことが必要である[27]。また正確かつリアルタイムな透明性のある情報発信により内外の信頼性を確保して、SM コンテンツ戦場での戦いを有利にすることが必要であり、そのためにフェイクニュースに対するファクト・チェックや SM に適した発信を行う必要もある。

3 事態拡大に備えたシームレスな手段の保持

(1) 我が国の領域横断作戦能力の強化と統合運用の推進

事態の拡大に備えた領域横断作戦能力を充実させ、統合運用を推進する観点から以下の 3 点が重要である。まず、各領域の能力を連接する指揮統制・情報通信能力の強化・防護を図ることである。領域を横断した情報の共有は各自衛隊の相互運用性を向上し、それぞれの自衛隊の縦割りを排した統合運用の基盤を充実させる。高度なネットワーク化は、共通の状況認識を迅速に形成し（「情報の優越」）、幅広い部隊間での「指揮の迅速化」を図ることで、広域に分散した部隊が行動を全体の動きに適合させ共通の目標の達成を可能とする（「自己同期化」）[28]。近年の ICT 技術の革新は目標発見から対処までの過程（「キル・チェイン」）を局限させ、またサイバー攻撃などによるネットワーク自体への脅威も現実化している[29]。今後整備予定の「スタンド・オフ防衛能力」や「総合ミサイル防衛能力」などは、宇宙状況監視(SSA)、海洋状況把握(MDA)やサイバー、電磁波領域等の幅広い情報を各部隊が瞬時に共有～一元的な統制～最適の手段の対応～遠距離に位置する他の手段が終末誘導・成果確認の一連のサイクルを通じて自己同期化を可能にし、統合運用の充実が図れる。

第二に、各領域横断能力の柔軟な組織化による統合の深化である。各領域の能力を有機的に融合するためには、陸海空自衛隊の統合をいかに図るかということから、共通の領域における能力をいかに統合するかが重要となってきた[30]。島嶼防衛のための共通の領域には、①機動・展開及び輸送、②海上・航

25「データの世紀 下：ネット工作員の告白ー動画駆使、７０カ国で確認」『日本経済新聞』2020 年 5 月 27 日。また Deepfake と呼ばれる AI も活用した動画ソフトは、動画上での映像の情報操作も可能にし、テキストデータよりも説得力のある情報を提供する。

26 P・W シンガー他『「いいね！」戦争』316-317 頁。

27 同上 416-418 頁。

28 Vice Admiral Arthur.K Cebrowski,"Network-Centric Warfare: Its Origin and Future", *Proceeding* (January, 1998). https://pdfs.semanticscholar.org/1c8d/70a1abf6764cd308427e505124637dfd193a.pdf?_ga=2.33680482.238942230.1593418622-1025706116.1593418622.

29 Christian Brose, "The New Revolution in the Military Affairs: War's Sci-Fi Future," *Foreign Affairs* (May/June, 2019), pp. 124-126.

30 米軍においても、当初は「各軍種の能力の統合」に焦点を当てていたが、軍種それぞれが複数のドメインにおける能力を持つようになり、軍種とドメイン一対一の対応関係ではなくなったため、次の段階として、共通のドメインの中における諸軍種の能力の統合に移行した。菊地 茂雄「米陸軍・マルチドメイン作戦（MDO）コンセプトー『21 世紀の諸兵科連合』と新たな戦い方の模索」『防衛

空優勢の確保、③侵攻部隊の上陸阻止、④脅威圏外からの阻止、⑤奪回、⑥防空、⑦被害局限及び⑧新領域の機能がある。これらに応じた陸海空部隊の規模、活動の地理的範囲や新領域の能力との融合を踏まえた領域横断能力の統合運用が必要である。「30 大綱」においては、①部隊の機動・展開のための海上輸送には陸海部隊を、⑧サイバー防衛能力は陸海空部隊をそれぞれ平素から共同の部隊として固定的に保持するとし、⑥防空は三自衛隊の部隊が総合一体的に運用される。さらに②海上・航空優勢の確保のための艦艇からの短距離離陸・垂直着陸(STOVL)機の運用や、④スタンド・オフ防衛能力、⑤奪回のための水陸両用作戦能力は、平素からそれぞれの自衛隊の部隊間で相互運用性を向上させておくことが必要である。また①～⑧の領域の異なる地理的範囲や作戦テンポを同期させ、グレーゾーン対処と国民保護を整合させかつ日米の行動の連携を図ることで、南西諸島での平時から有事までのシームレスな領域横断能力を発揮するために統合任務部隊を平時から編成することも今後検討の必要がある。

第三に、AI などを活用した無人化、自律化による統合の深化である。AI の発展が今後、定型業務（繰り返し）から非定型業務まで代替できるようになるにつれ、戦闘において人間は突発的かつ予想不可能な事態に対応する能力の発揮が中心となると予想される[31]。その結果今後は、知能化兵器の集団投入による高速かつ多量の攻撃が行われ、小型・安価・使い捨て可能性や自律性が重要な要素となるとともに、ソフトウェア、特に AI の性能が勝敗を決めると考えられる[32]。そのため自律型致死兵器システム(LAWS)に関する国際的議論も踏まえつつ、無人化・自律化された装備が構成する部隊の運用についても検討が必要である。また「ソフトウェア集約型システム」の比重の高まりは、ソフトウェアを最新化するため従来の防衛産業に加えて、組織化されていないベンチャー企業を含めた新しい防衛技術基盤の構築も必要とされている[33]。

統合運用は、今後のゲーム・チェンジャーとなりうる技術的進展による戦い方の変化を踏まえ領域横断作戦を実行することが必要になる。「30 大綱」策定以降もコロナウイルスの蔓延を含む数多くの大規模災害が発生したが、平時においても統合任務部隊を編成した自然災害への対処と同時に我が国周辺でのグレーゾーンへの一層の警戒が必要となっている。この際、大臣の指揮命令の執行にあたっては、単一の自衛隊の運用では統合幕僚監部（統幕）を通じて各自衛隊の総隊等が行うが、それと同様に統合部隊の場合も、平素からのシームレスな活動を確保するために、常設された統合司令部が執行することが必要となると考えられる。

(2) 事態拡大に備えたシームレスな対応のための日米共同領域横断作戦

日米両国は各領域における日米共同領域横断能力の充実により、同盟の抑止力及び対処力を強化することが必要である。米国はアジアにおいて「プレセンスのためのプレゼンス」を超えた前方軍事プレゼンスを保持するために、A2/AD の環境下で前方に所在する基地や軍事アセットが有事の際に激しい戦闘環境下に置かれることを前提とし、その中で迅速に展開しながら敵の軍事行動を拒否し得る態勢を必要としている[34]。我が国の防衛はこの戦略に重要な役割を果たし、日米の共同領域横断作戦の充実を図ることができる。米軍は「グローバル運用モデル４つの層」として、グレーゾーンの事態から前方部隊が「接触層」、「鈍化層」の役割を果たし、地域外の部隊が「増派層」、「本土層」を構成することを検討している[35]。特に米軍が陸上戦力を前方に配

研究所紀要』第 22 巻第 1 号（2019 年 11 月）40-41 頁。

31 小野圭司「人工知能(AI) による軍の知的労働の代替－AI と人間の共生の問題としての考察－」『防衛研究所紀要』第 21 巻第 2 号（2019 年 3 月）13 頁。

32 Christian Brose, “The New Revolution in the Military Affairs: War’s Sci-Fi Future,” pp. 126-131.

33小野圭司「軍産関係史とそれを巡る思想－軍産相対関係の段階的変化に関する考察－」『戦史研究年報』第 21 号（2018 年 3 月）66-71 頁。

34 新垣拓、切通亮「米国『戦略的競争』の実像」防衛研究所編『東アジア戦略概観 2020』（防衛研究所、2020 年 3 月）160 頁。

35 同上 180-181 頁。

置して侵攻部隊を陸から拒否する構想を具体化する上で、前方に展開する部隊の残存性向上や地対艦ミサイル運用の協力及び水陸両用機能の強化などでは、我が国防衛のための島嶼防衛に直結した共同対処能力が発揮できる。また米軍は、インド太平洋地域において、BMD、空対空能力や長射程の空対地能力の充実に加え、対水上・水中能力の向上さらにサイバー攻撃・防衛能力の養成などを課題としている[36]。海空を中心としたこれらの日米共同の領域横断能力は、平時における共同訓練の場も活用した充実の過程を通じて、グレーゾーンの段階からシームレスな日米共同の対応の基盤となる。

(3) 政府一体となった平素からの戦略的なコミュニケーション

「30 大綱」において、我が国が有するあらゆる政策手段を体系的に組み合わせること等を通じ、平素からの戦略的なコミュニケーションを含む取組を強化するとしている。戦略的なコミュニケーションは米統合参謀本部によれば、「全ての軍事行動を通じた影響力行使により、友邦国・敵国・その他が、米国の国益にとって有利な行動をとることや、米軍の行動への理解と賛成を得ることなどを促す概念である」とし、以下の方策を挙げている。

① 自国の信頼性と正当性の向上、②相手の信頼性と正当性の低下、③選択した対象者に自国や国際的な目的に合致した特定の行動をとらせること、さらに④相手又は競争者に特定の行動をとらせる（またはとらせない）こと[37]

この観点から、グレーゾーンにおける戦略的なコミュニケーションは、我が国国民、同盟国、国際社会そして現状変更を狙う国を対象として以下の観点を重視しなければならない。

第一に、我が国の行動についての理念と、我が国のとる現実の行動そして情報空間でのコンテンツの一致による信頼性と正当性の獲得である。そのため中長期的な観点から「自由で開かれたインド・太平洋ビジョン」に基づく国際的ルールを平素から国際社会と共有し、多角的・多層的な安全保障協力を構築しておくことが基盤となる。そしてグレーゾーンの事態においては、我が国の行動に対する情報空間での対処が重要となる。操作された情報に対しては、確実なファクト・チェックにより、その真偽を明確にして必要に応じて的確に反論することが、我が国の行動に対する信頼を得ることにつながる[38]。さらに進行中の行動についてもリアルタイムで、透明性のある情報をネットで発信することが重要である。例えば海警行動において法執行活動を示す電光掲示板を掲げる海自艦艇の映像[39]は、動画により相手よりも早く世界に向けて発信することが正当性確保につながる。現在でもスクランブルのその都度の情報発信や、新型コロナ対策の現状と教訓事項の発信がなされているが、グレーゾーンにおける部隊行動のリアルタイムの動画発信は、有利な認識形勢に重要な要素となる。

第二に、誤判断に基づく事態の予期しない拡大を防止するための信頼醸成措置は、我が国のとる行動に対する予測可能性を向上し、信頼の獲得にとって必要不可欠である。そのため平素からの防衛交流や不測の事態・事故の場合の両国の意思疎通を可能とする海上衝突防止協定やホットラインの整備などが重要である。このように我が国の国際的な理念に基づく透明性のある抑制された行動の発信は、同盟国の世論及び国際社会の賛同を得るための必要不可欠な要素である。

そして第三に、これらを踏まえた我が国と同盟国の共同した部隊展開・集中や訓練・演習は言葉と映像に加え行動による誤解のない明確なメッセージの発信となり、現状変更を意図する側の行動に影響

---

[36] The US Department of Defense, *Indo-Pacific Strategy Report* (Washington, DC, June 2019), pp.18-19.

[37] Joint Requirements Oversight Council, *Strategic Communication Joint Integrating Concept Ver.1.0* (Washington, DC, 2009), pp. 8-9.

[38] 台湾国防部では「フェイクニュース対抗小組」をもって「偽情報」「デマ」「誤情報」に対処している。例えば中国が実弾演習の場所を「台湾海峡周辺」と報道した際には、実際は 324Km も遠く離れていると修正し、これは「誤情報」の発信による台湾民衆を不安に陥れることを目的していると指摘した。（門間理良『東亜』624 号(霞山会、2019 年 6 月)63 頁）。

[39] 脚注１６参照。

を与えることが期待される。

終わりに

グレーゾーンの事態では戦争に至らないレベルで国家の目標が追求されるが、これに対して国家が一丸となり平時から有事までの多様な事態に対するシームレスな活動が必要である。特に平時でも有事でもない事態において秘密活動、偽情報、影響工作などが常套手段とされるハイブリッド戦に対しては、多次元統合防衛力による、開かれた正しくかつ正当性のある行動をもって対抗していかなければならない。そしてそのための統合運用のあり方として、平時からグレーゾーンの脅威に対応した領域を横断した自衛隊の能力発揮を可能とする統合司令部及び、運用と一体となった行動の信頼性と正当性を確保する戦略的情報発信の能力を充実することが必要である。

本稿は多次元統合防衛力の構築について、グレーゾーンの観点を中心にして包括的に検討したが、紙面の制約のため分析不十分な点については今後、稿を改めて記述したい。

プロフィール profile

副所長　陸将補
中野　義久

防衛研究所企画部企画調整課
直　通：03-3260-3011
代　表：03-3268-3111（内線 29171）
ＦＡＸ　：03-3260-3034
※ 防衛研究所ウェブサイト：http://www.nids.mod.go.jp/