第７９２号

令和３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

ハイブリッド脅威の行使をどう抑止するか

研究班　松村五郎

１　はじめに

２０１４年にロシアによるクリミア併合とウクライナ内戦への関与という事態が起きて以降、特に北大西洋条約機構（ＮＡＴＯ）各国を中心に、ハイブリッド戦争への警戒が高まってきた。今では多くの国が、これからの国家安全保障を考えるにあたり、ハイブリッド戦争への対処が不可欠であると考えている。

これは世界に共通の問題意識ではあるものの、アジアにおいては、ほぼ同様の現象をハイブリッド戦争としてよりもグレーゾーンの戦いとして取り上げる傾向が強い。できる限り伝統的な戦争を避けるように行われる戦いであるという点は同じであっても、地上の国境越しに国家の関与を秘匿した軍事・非軍事のハイブリッドな手段を使用して国家を内部から切り崩すという脅威を警戒する欧州に対して、アジアにおいては主要な対立の焦点が海洋にあることから、戦争ではないが平和でもないというグレーな状況の中で強制的に既成事実を積み重ねて目的を達成されてしまうという脅威に目が向いているからであろう[1]。

ハイブリッド戦争はあくまで戦争の一種であるとして、グレーゾーンにおける諸事象とは区別す

[1] Chiyuki Aoi, Madoka Futamura and Alessio Patalano, “Introduction ‘Hybrid warfare in Asia: its meaning and shape’ ”, *THE PACIFIC REVIEW*, 2018, Vol.31, No.6, pp.696-697.

べきであるとの考え方もあるが、本稿においては、「ハイブリッド戦争及び、それと関連した概念であるグレーゾーンの戦いを最もうまく記述するとすれば、敵対者が、高コストの高烈度戦争にエスカレートする可能性がある正面切った戦い（overt conflict）に訴えることなしに、特定の戦略目標を達成するために多次元のアプローチを運用するということである」[2]という論に沿って、ハイブリッド戦争とグレーゾーンの戦いを、平素から生起し得るほぼ同じ形態の脅威の行使であると捉えて論を進めていくこととする。後述するように、正規の通常戦力による「正面切った戦い」も含んだ広義のハイブリッド戦争に進展することも視野に入れて全体像を考えることは必要であるが、本稿では敢えて、そこまで進まない時点での抑止に焦点を当てて考察してみたい。

このような「正面切った戦い」に訴えない「多次元のアプローチ」による戦いは、決して新しいものではなく、孫子において「戦わずして勝つ」ことが上策とされているように、古から行われてきたものだとの指摘もある。それでも敢えて今、これがクローズアップされているのは、故なきことではない。一つには、第２次世界大戦後、国際社会においても各国の国内社会においても、戦争を忌避する風潮が高まっており、内戦を除き対外的に明らかな戦争手段に訴えることは政治的リスクが大きいという事情がある。またそれと併せて、特に情報通信の分野で高度なテクノロジーが出現したことで、相手の軍隊を迂回して直接国民に脅威を与えることが可能になったことも大きいだろう[3]。

これらを踏まえ、本稿においては、一方的に特定の戦略目標を達成しようとする意図のもとに「正面切った戦いに訴えない多次元のアプローチ」によって各種能力が運用される恐れをハイブリッド脅威と定義し、その行使を抑止する方策について考えていくこととする[4]。

以下、まずハイブリッド脅威というものの特性について明らかにした上で、これに対して抑止という概念を適用した場合どのような理論が導き出せるのか、その理論に沿って抑止を成功させるために考慮すべき要因は何かを検討し、最後に日本を念頭に置いたハイブリッド脅威抑止達成のための具体策を導き出していきたいと思う。

２　ハイブリッド脅威の特性

ハイブリッド脅威とは「正面切った戦いに訴えない多次元のアプローチ」によって各種能力が運

---

[2] Weichong Ong, “The rise of hybrid actors in the Asia-Pacific”, *THE PACIFIC REVIEW*, 2018, Vol.31, No.6, p.742.

[3] 戦争の性格の変化について詳しくは、松村五郎『新しい軍隊ー「多様化戦」が軍隊を変える、その時自衛隊は…』（内外出版、２０２０年）、４０～４７頁及び５６～７９頁を参照されたい。

[4] 以下本稿においては、ハイブリッド脅威の行使を抑止することを、略してハイブリッド脅威抑止と記述する場合がある。

用される恐れだと述べたが、これは具体的にどのようなものなのだろうか。まずその点から明らかにしていかなくてはならないだろう。ハイブリッドという言葉自体は、動物や植物の交配時に異なる種をかけ合わせて生まれた異なる特徴を併せ持つ新しい個体を指す用語である。それが幅広い分野で用いられるようになり、例えばガソリンと電気の両方を使って走る車が、ハイブリッドカーと呼ばれるようになった。ハイブリッド戦争という場合には、軍事と非軍事の両方の手段を活用した戦争ということになる。

同じく字義どおりに捉えれば、ハイブリッド脅威とは、軍事と非軍事両方の手段による脅威であるということになるが、ここで先の定義を思い出して欲しい。本稿におけるハイブリッド脅威とは、「正面切った戦いに訴えない多次元のアプローチ」によって各種能力が運用される恐れだと定義した。すなわち、軍事的手段の中でも、相手の軍隊を正面きって攻撃するような正規の通常戦力は、ここではハイブリッド脅威には含めない。各種の非軍事的手段と、軍事的ではあっても軍隊間の大規模な戦いを惹起しない非正規手段を併せたものが、本稿で論じるハイブリッド脅威である。前述した広義のハイブリッド戦争においては、このハイブリッド脅威と正規の通常戦力が合わせて行使されることになるが、本稿の焦点は、あくまでもハイブリッド脅威のみが行使される状況を念頭において、それをどう抑止するかである。

それでは、そのようなハイブリッド脅威の具体例とは、どのようなものだろうか。欧州においては２０１７年、ＮＡＴＯとＥＵが共同してフィンランドのヘルシンキに、欧州ハイブリッド脅威対策センターを設立した。このセンターの場合、ハイブリッド脅威とは「幅広い各種の手段を用いて、民主国家や機関に内在する脆弱性を標的に行われる、用意周到に調整され、同期された行動」であり、「その諸活動は、容易に検知されたり、誰が行ったのか知られたりしないようなぎりぎりの領域を活用する」ものだと説明している。

そして具体的な例として、サイバー空間等情報分野での影響力行使、エネルギー供給パイプラインなどロジスティックス上の弱点追求、経済・貿易を通じての脅迫、ルールの無効化による国際制度の弱体化、テロ等による安全上の不安の作為など、広範な分野を挙げている[5]。

このセンターは、ロシアのクリミア併合後、ロシアによる旧ソ連諸国や旧東欧諸国への脅威が高まったとの認識から設立されたものなので、対象国の民主主義を内側から切り崩すような非軍事的手法に特に焦点が当てられているが、ロシアのクリミア併合やウクライナ内戦介入の事例を分析した各国の文献の中では、軍事と非軍事をより密接に関連させた手法に焦点を当てたものも多い[6]。

---

[5] 欧州ハイブリッド脅威対策センターホームページ、https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ 。

[6] 例えば、Christian Brose , “The Kill Chain – Defending America in the Future of High-Tech Warfare”,

すなわち、リトル・グリーン・メンと呼ばれた非正規部隊（プーチン大統領は当初、これは地元の自警団だと強弁した）の投入、戦略的及び戦術的なサイバー攻撃、電子戦部隊による通信やＧＰＳの妨害などである。ロシアはこれらに加えて、国境のロシア側に即応体制を整えた正規軍の大部隊を配置し、ウクライナ政府に対する心理的恫喝を加えるとともに、必要な場合には実際に軍事介入できる態勢を取った。

今後ロシアが実際に正規軍をウクライナ領土に侵入させて作戦を行った場合にも、局地的な紛争に収まる限り、それは正規の通常戦力使用を含む広義のハイブリッド戦争だと言えるだろう。しかし前述したように本稿では、ハイブリッド脅威の軍事的手段として、従来型の手法による正規軍の火力等の使用は含まずに、非正規勢力の使用やサイバー・電磁波能力等の国境外からの使用等を指すこととする。正規の通常戦力に対する抑止については、いわゆる通常抑止として、過去に議論が積み重ねられてきている[7]。通常戦力とハイブリッド脅威が合わせて用いられる場合の抑止も重要なテーマではあるが、ここではハイブリッド脅威そのものが行使されることに対する抑止に焦点を絞り、通常抑止については、これとの関係で必要な範囲で触れるにとどめることとしたい。

さて、このように枠組みを設定した上で、考え得るハイブリッド脅威の具体的形態を、ロシアの事例に限ることなく、アジアにおける動向なども加味した上で列挙してみよう。相互に内容が重複するものもあることを厭わず、順不同で列挙すると、以下のようになる。

〇社会・経済的手段

・対象国内の世論誘導、影響工作、メディア工作

・貿易、投資、エネルギー供給等の経済的手段による強要及び恫喝

・国際世論工作や国際規範の恣意的解釈と普及宣伝による対象国の孤立化

〇技術的手段

・サイバー攻撃（政府・軍の指揮通信システム無力化、発電所等の社会インフラ破壊、金融システムの混乱等による経済破壊、ＳＮＳ等を通じた世論誘導など）

・電磁波攻撃（軍事能力の無力化、国家の基幹通信機能への妨害、携帯電話網等社会インフラの阻害による混乱作為など）

・宇宙を活用したインフラへの攻撃（ＧＰＳ妨害、通信妨害、衛星の機能妨害など）

(Hachette Books, 2020)、 廣瀬陽子『ハイブリッド戦争 - ロシアの新しい国家戦戦略』、（講談社現代新書、２０２１年）など。

[7] 代表的なものとして、John J. Measheimer, “Conventional Deterrence”, (Cornel University Press, 1983) がある。

〇武装手段

・武装工作員、民兵、偽装漁民、民間軍事会社等、偽装した武装勢力による実力行使

・地上、海上、海中、空中の無人機を活用した各種の妨害及び破壊活動

・正規軍の部隊、艦艇、航空機、ミサイル等の展開や演習による心理的恫喝

以上は、イメージアップのために列挙したもので、必ずしもすべてを網羅したものではない。目的を達成できる手段で、正面切った戦いに至らないものであれば、どのような手段もハイブリッド脅威の能力として活用できるのであり、今後の科学技術の発達により、新しい手段が登場することも当然予想されよう。

イメージアップができたところで、これらのハイブリッド脅威に共通する特性について考えてみたい。第一の特性は、その匿名性または曖昧性である。世論工作やサイバー攻撃などは、行為者を秘匿して目的を達成するのに適しており、匿名性が高い手段である。恫喝等を目的とし、行為主体の推測や特定が可能な場合であっても、直接的な因果関係がないように装い、相手国民を不安に陥れる中で世論の分断を煽るなど曖昧性を活用することが考えられる。また、サラミ・スライス的に既成事実を積み上げるような場合には、個々の事象では真の狙いが分からないようにする等、敢えて曖昧性を持たせることで、相手側が対抗手段を取ることを困難にすることが考えられよう。

第二の特性は、その複合的及び累積的な使用である。ハイブリッド脅威は、正面切った軍隊間の戦いに至ることなしに目的を達成しようとする手段である以上、一つ一つの行為は相手国軍隊によって反撃を受けることがないよう、その烈度がコントロールされる。それでも目的を達成できるのは、複数の手段を組み合わせるとともに、何回にもわたってその効果を積み重ね、相手が反撃できないでいるうちに既成事実化を狙うからである。だからこそ、白か黒かではないグレーゾーンとも呼ばれるわけであり、従来のようにある目的を達成するために単一の戦争が戦われるのではなく、何も起きていない時点から少しずつ事象を積み重ねて、最終的に特定の目的を達することとなる。ロシアによるクリミア併合の場合も、２０１４年２月に突然起きたものではなく、ロシアがこれ以前から着々とクリミアにおいて政治宣伝や親ロ派の醸成等、ハイブリッド脅威を行使して併合という目的達成の好機を狙っていたことが指摘されている[8]。

これら二つの特性を認識すればするほど、個々のハイブリッド脅威の行使をすべて未然に抑止することは極めて困難であることがわかる。したがってハイブリッド脅威の抑止においては、ある戦略的目的に向かって脅威が行使され始めたできるだけ初期の段階において、相手が目的達成のため

---

[8] 廣瀬陽子『ハイブリッド戦争 - ロシアの新しい国家戦戦略』、(講談社現代新書、２０２１年)、８８頁。

更なる脅威行使に出るのを抑止するというアプローチが必要であると考えられるが、そのためにはどうすればよいのだろうか。次にその点を考えてみたい。

3　ハイブリッド脅威抑止の理論的考察

ハイブリッド脅威抑止について考察するにあたり、最初にハイブリッド戦争の全体像とハイブリッド脅威の関係を明らかにしておきたい。前節でも述べたように、ハイブリッド戦争は必ずしもハイブリッド脅威とこれに対する対抗手段によって戦われることにとどまらず、双方にとって不本意ではあっても、正規の通常戦力同士の火力発揮を含む戦いにまで発展することがある。

この場合においても、世界的な大規模戦争にエスカレートすることがないようにコントロールされ、局地戦争にとどまっている限りは、それが「正面切った戦い」の回避に失敗した結果であったとしても、それを広義のハイブリッド戦争と捉えて全体を考察することが必要だろう。

抑止という観点から見れば、ハイブリッド脅威を行使する側（以下、脅威側と呼ぶ[9]）が、その行使を抑止したい側（以下、抑止側と呼ぶ[10]）に抑止される場合の有力な構図として、通常戦力において抑止側が十分に優勢であるという状況が、まず思い浮かぶかもしれない。脅威側がハイブリッド脅威を行使して目的を達成しようとしたときに、抑止側が通常戦力で十分な優勢を確保していれば、ハイブリッド脅威の行使に対し、局地戦争へのエスカレートを示唆して逆に脅すことができ、それによって抑止が達成されるという理屈である。

これについて防衛研究所の高橋杉雄は、グレーゾーン抑止について論じた英語論文の中で、抑止側がエスカレーションの窓を開けておくことが重要であり、それに加えてグレーゾーン脅威の行使が直ちに抑止側の通常戦力発揮に直結してしまうようなトリップワイヤー[11]的な仕組みを作為することができれば、抑止はより効果的になると論じている[12]。

確かに、冷戦初期に米国が欧州における通常戦力の劣勢を核戦力の優勢で抑止しようとした際のアナロジーとして、この理屈は一見機能するように見える。しかし核能力の優勢によってすべての

---

[9] 本稿では、脅威側として主として国家主体を想定し、その指導者を対象とした抑止効果について考察する。これが非国家主体であった場合にも、以下の議論は基本的に適用可能であると考えるが、それが成立する条件について、更なる検討が必要となるかもしれない。

[10] 抑止側も、主として一つの国家を想定して議論を進めるが、これは国家連合であっても問題なく、むしろその場合の方が以下の議論は強化されると考えられる。

[11] トリップワイヤーとは「わな線」という意味で、ある行為があったならば自動的に次の段階に進ませるような仕掛けを指し、例えば「在韓米軍の存在は、北朝鮮による侵略があった際に米国が共同行動をとるためのトリップワイヤーとして働く」のように用いられる。

[12] Sugio Takahashi, “Development of gray-zone deterrence: concept building and lessons from Japan’s experience”, *THE PACIFIC REVIEW,* 2018, Vol.31, No.6, pp.799-800.

通常戦争を抑止できるわけでない。相手が核能力で劣っていても、紛争の規模や特性が核の使用に適さない場合もあり、だからこそ米国も通常戦力を強化し続けている。

ハイブリッド戦争においても、確かに脅威側の通常戦力が抑止側を上回っているという場合には、脅威側はエスカレートを恐れることなく大胆にハイブリッド脅威を行使するかもしれないため、抑止側としてそれを許さない通常戦力を保持することが必要だとは言えるが、それだけで十分な抑止を達成できるとは言えない。

なぜならば、仮に抑止側が脅威側を圧倒する通常戦力を持っていたとしても、通常兵器による交戦がまだ生起していない段階で、抑止側から先に武力を行使することには、大きな心理的抵抗が働くことは想像に難くないからである。冷戦間に、通常兵器による攻撃に対して本当に核を使用できるのかどうかが問題になったのと同様に、国際的にも国内的にも大きな政治的リスクを負う決断をしなくてはならないことになる。

ましてハイブリッド戦争においては、脅威側は最初から、正面切った戦いに陥らないよう計算し尽された手段を行使して現状変更を図ろうとしてくる。抑止側がトリップワイヤーとなる仕組みを設けたとしても、それに触れないような手段で目的を達成しようとするだろう。これを防ぐために、より軽易な脅威に対してもトリップワイヤーが働くようにすれば、誤解や誤算による武力紛争のリスクを高めることになるため、それにも限界がある。

したがって、ハイブリッド脅威を抑止するために、脅威側に対して通常戦力で劣勢に立たないことも必要ではあるが、それだけで抑止を達成することはできず、他の方策が必要だということになる。高橋杉雄の前掲論文においてもその点は認識されており、軍事力のみならず国家が持つあらゆる種類の力を動員することの重要性が指摘されている。そこで、以下本稿においては、その諸力をどのように動員していけばよいのかについて、更に深く検討していくこととしたい。

抑止を理論的に考えるために、まず抑止の定義に立ち戻ってみよう。学問の世界では数々の学者がそれぞれの言葉によって定義しているが、ここではその集大成として実際に戦力を運用している米軍の定義を参照する。米国防省の軍事用語辞典によれば、抑止とは「受け入れられない程の対抗手段の信ぴょう性ある脅威、或いは期待できる利益を上回るコストがかかるという確信、のどちらかまたは両方が存在することによって、ある行為を予防すること」である[13]。

この「受け入れられない程の対抗手段」とは、典型的な例が核兵器による報復攻撃であり、これによる抑止は懲罰的抑止と呼ばれる。これに対して「期待できる利益を上回るコストがかかるという確信」による抑止は拒否的抑止と呼ばれている。

---

[13] "DoD Dictionary of Military and Associated Terms" (U.S. Department of Defense, January 2021), p.63.

拒否的抑止に関しては、脅威側の攻撃を失敗させる能力を持つことで達成されると誤解されていることがあるが、正確には「利益を上回るコストがかかるという確信」を脅威側に与えることが抑止達成の条件となる。失敗したとしてもコストが少なくて済むならば、脅威側がいわゆる「ダメもと」で行為に及ぶ可能性があり、十分に抑止を達成することはできないからである。この点が、対処のための能力と拒否的抑止のための能力の考え方の違いであり、この両者の能力は重なる点は多いが、どちらに重点を置くかで能力の組成は変わってくる。

さてそれでは、ハイブリッド脅威の抑止において有効なのは、懲罰的か拒否的かどちらの抑止なのだろうか。懲罰的抑止においては、脅威側に対して耐えられない程の報復的懲罰を加えることの信ぴょう性が問題になる。ハイブリッド脅威が行使される場合、複数の手段が複数回にわたって積み重ねられることになるのが普通なので、抑止側は脅威側の目的が果たされる前の何れかの時点にレッドラインを設定し、それを超えた場合に大規模な報復を発動すると宣言することで抑止を達成することになろう。

しかし、そのような判断を行わせないように曖昧な手段を積み重ねることこそハイブリッド脅威行使の神髄であり、この抑止の信ぴょう性を確保することは非常に困難である。状況が曖昧な中で、いわゆるレッドラインを越える「疑い」があるという場合には、抑止側が国内外世論の動向等を気にして大規模な報復をためらうことが考えられ、脅威側はそこに付け込んでくるであろう。

それでは、拒否的抑止はどうだろうか。従来の拒否的抑止は、基本的には脅威側が攻め込んでくる正面で、その攻撃を成功させないばかりか、逆に脅威側に多大な損失というコストを与える態勢をとってこれを抑止するというものであった。ハイブリッド脅威の場合は、脅威側がその手段の匿名性や曖昧性を活用しつつ、抑止側の反応を見極めながら手段を小出しにしてくることが考えられ、失敗しても大きなコストを負わない、いわゆる「ダメもと」の手段を積み重ねてくることが考えらえる。そのすべてを完全に拒否することができれば、脅威側の目的達成を阻み続けることは可能であっても、次々と新種の脅威が現れる中ですべてに対処し続けなくてはならず、これでは抑止にはならない。

そこで本稿で提唱したいのは、懲罰的抑止の場合のような大規模な報復ではなく、脅威側が何らかのハイブリッド脅威の行使を始めた初期の段階で、これに対し確実にコストを課すことで、更に他のハイブリッド脅威を繰り出してくることを抑止し、脅威側が最終的に目的を達成する前に、それを断念させるという方法である。この際、拒否的抑止の場合のように、相手の行動そのものの阻止を通じてコストを課すことばかりではなく、それとは違う分野で、あるいは同じ分野であっても相手の行動の阻止とは直接関係なく、カウンター的にコストを課すことも有力な手段となる。

またこれは一回で終わるわけではなく、初期の段階で繰り返してコストを課すことで、更なる脅

威行使を断念させることに狙いがある。従来型の戦争を対象とした懲罰的抑止や拒否的抑止とは異なり、グレーゾーンが続く中で脅威側が目的を達成する前のできるだけ早い段階からコストを強要し続け、それ以上の脅威行使を未然に防止するという新しいタイプの抑止だと考えられるので、本稿においてはこれをコスト累積抑止（deterrence by accumulating cost）と呼ぶこととしたい。このような発想は、これまで米国が中ロ等に経済制裁を発動する際などにも意識されていたとは思われるが、これを明確な抑止戦略として概念化することに意義があると考える。

コスト累積抑止においては、一つ一つのハイブリッド脅威の行使に対し、コスト付加の手段をどのように設定するのかが、最も重要となる。いたずらに事態をエスカレートさせることなく、また抑止側にとっての対処コストは抑えた上で、脅威側に確実に効果があるコストを付加しなくてはならないからである。エスカレートを避けるという点では、脅威と同じ正面で、すなわちサイバー脅威に対してはサイバー空間で、経済的脅威に対しては経済の範疇でコストを課すことが望ましいと考えられるが、偽装勢力による武装攻撃や、偽情報拡散による世論工作などに対しては、同じ手段で報復することは抑止側が民主主義国家である場合には適切ではなく、攻撃を阻止するとともに、他の分野で制裁を加えることも考えなくては、その更なる発生を抑止することはできない。

またハイブリッド脅威は、一つ一つは小さく見える曖昧な手段を組み合わせ、積み重ねて行使される。したがって、これに対するコスト累積抑止も、その行使を確実に探知して、機を失することなく一つ一つに制裁を加えることの累積的効果によって、脅威側が最終的な目的達成に至る前のできるだけ初期の段階で、更なるハイブリッド脅威行使の抑止を狙うというものになるだろう。

重要なのは、予めレッドラインを設定するのではなく、たとえ些細なものでも見逃すことなく、ハイブリッド脅威の行使を確実に探知し、その証拠を掴むとともに、見せかけではない本当の行為主体を明らかにして、その主体に対して何らかの手段で着実にコストを課すことである。それを見過ごすと、逆に脅威側の行為が累積され、また徐々に拡大して、既成事実化等によりその目的を達成させてしまうことになる。

制裁のための手段には、先にハイブリッド脅威として列挙した社会・経済的手段、技術的手段、武装手段のそれぞれに見合うようなものすべてを指すが、抑止側が責任ある民主主義国家である場合には当然、偽情報や偽装勢力の使用は除外されるとともに、安定的な抑止のためには、脅威側を挑発するような過剰な報復的手段も慎まなくてはならない。

また脅威側にコストを課す手段として、抑止側が単独で制裁的な行動を取るというのはその一部に過ぎず、むしろハイブリッド脅威の行使を国際的に白日の下に曝すことによって、脅威側の外交的評価が棄損される効果も大きいことを認識しておく必要がある。このような評価の棄損により、抑止側と立場を同じくする諸国が、貿易等の経済面で脅威側に厳しい対応をしたり、国際機関や他

の多国間枠組みの中で従来は脅威側も享受していた利益を得られなくしたりと共同行動を取ることは、大きなコストの付加になる。砕けた言葉で言えば、国際的な「村八分」効果である。

更に欧州においては、ロシアがバルト３国などの旧ソ連諸国や東欧諸国に対して、その領土併合やロシアに都合の良い政府樹立などを目的としてハイブリッド脅威を用いてくることに対し、これら諸国の民主主義体制を強化することや、ロシア国内における民主化要求運動を支援することこそがハイブリッド脅威の抑止になるという「民主主義による抑止」を唱える論文も出されている[14]。

この「民主主義による抑止」論は、本稿が提唱するコスト累積抑止のように、個々のハイブリッド脅威行使に対応を取ることで目的達成を抑止しようとするものとは異なるが、抑止手段を幅広くとらえるという点では参考になる。とにかく、抑止側が採り得るあらゆる手段を行使して、脅威側がハイブリッド脅威を行使しようとすればかえって損をするという構図を作ることを考えていかなくてはならない。

それでは、このようなコスト累積抑止を成功させるために必要な考慮要因について、次節において更に詳しく考察していくこととしよう。

４　抑止成功のために考慮すべき要因

コスト累積抑止を成功させるために考慮しなくてはならないことは、第１にハイブリッド脅威の行使を確実に探知すること、第２に見せかけではない真の行為者を明確にすること、第３にハイブリッド脅威をできるだけ無効化すると同時に前２項目を容易化するために抑止側のレジリエンスを高めること、第４にエスカレートを避けつつも脅威側にコストを強要する効果をできるだけ高めることである。以下、一つずつ詳しく見ていこう。

(1) ハイブリッド脅威行使の確実な探知

ハイブリッド脅威が匿名性または曖昧性という特性を持ち、脅威側が当初はその真の目的を秘匿しつつこれを行使してくることが多いことから、抑止側としてはまずこのような企みが当初は非軍事のみで些細なものであったとしても、小さいうちから確実に探知することが重要となる。

このためには、平素から脅威側の各分野での行動を透明化していくことが必要であり、抑止側が衛星情報、サイバー情報、電磁波情報、ヒューミントなど幅広い分野での情報収集能力を持っていることが不可欠となる。その能力を一国で完全に整備することは困難であることから、同盟国や友好国と連携してこれを整備し、客観的な情報を取得・共有するとともに、可能な限り情報を公開し

---

[14] Mikael Wigell, “Democratic Deterrence – How to dissuade hybrid interference”, *FIIA WORKING PAPER*, September, 2019, Finish Institute of International Affairs.

て透明性を高めていくことが有効であろう。

現代においてこれらの情報は、国家のみならず民間企業によって商用で提供されているものも多く、その分析にあたっては民間のシンクタンクも大きな役割を果たしている。共に米国のシンクタンクである３８ＮＯＲＴＨが北朝鮮の核・ミサイル開発の動向について、戦略国際問題研究所（ＣＳＩＳ）が中国の南シナ海における活動について、商用の衛星画像等を元に日々その分析を行って、これを世界に周知しているのは、その好例であろう。

これらのシンクタンク等が、単に情報を収集分析するだけではなく、その内容を世界に向けて発信していることの意義は大きく、国家が軍事機関や情報収集機関を通じて得た情報も、戦略的な必要に応じて、広く国内外に公開、発信していくことが重要であると考えられる。ハイブリッド脅威に関しては、開発援助等の経済的手段が軍事的狙いに結びついているなど一見異なる分野の動向が実は関連している場合も多く、また様々な手段を複合的に使って脅威側が世論を操作しようとする場合もある。公開情報を増やして透明性を高め、ジャーナリズムやアカデミズムも含めて社会全体としてハイブリッド脅威の行使を見抜いていく能力を高めることが、有効であると考えられる。これによって、脅威側の偽情報拡散等の効果を無力化することも可能になろう。

抑止側が単一の国家ではなく、同盟等による連携でハイブリッド脅威を抑止していこうとする場合、すなわち拡大抑止の場合の考慮事項として、例えばロシアによるバルト３国等への脅威をＮＡＴＯが抑止するためには、その対象国が抱える経済的・社会的脆弱性について、ロシア以上にＮＡＴＯ側がこれを良く理解し、付け込まれないようにすることの重要性が指摘されている[15]。アジアでは、台湾に対する中国の脅威を抑止する場合にも同じことが言えるだろう。台湾の政治や社会について、関係各国が理解を深めておくことは、台湾に対するハイブリッド脅威の行使を早期に探知する上で非常に重要となる。

，

(2) 真の行為者の明確化

サイバー攻撃への対処において常に問題となるのが行為者の特定、いわゆるアトリビューションであるが、これは他のハイブリッド脅威に対しても常に問題となる。見せかけの行為者ではなく、真の行為者をつきとめてコストを課さなくては、コスト累積抑止は効果を発揮しないからである。

もっとも、サイバー攻撃の抑止に関しては、アトリビューションに限界があることを踏まえて、真の行為者を突き止めることよりも、見せかけの行為者に対して直ちに反撃する能力を見せつける

---

[15] Alexander Lanoszka, “Russian hybrid warfare and extended deterrence in eastern Europe”, *INTERNATIONAL AFFAIRS,* 92 : I (2016) pp.175-195.

ことの方が抑止効果は高いという主張もある[16]。確かに、直ちに反撃する、あるいは制裁するというのも、それ以上のハイブリッド脅威を抑止する上での一つのポイントではあろうが、それを行ったとしても、同時に真の行為者を解明する努力を進め、判明次第これに対して制裁等のコストを課すことも並行して進めなくては、同時並行的に行使される他種のハイブリッド脅威によって脅威側が目的を達成するのを防ぐことはできないのも明らかである。

このためには、探知の項で述べたのと同様、抑止側各国の情報収集能力を高めることと併せて、多国間の協力によって情報を突き合わせることも、大いに有効であると思われる。また、これによって真の行為者とその手口が国際的に明らかになることで、前節で述べたように脅威側に対する国際的評価が棄損されることになり、単に真の行為者に関する情報収集能力を高めるという効果を超えて、制裁的な効果にまで繋げていくことが期待できる。

(3) 抑止側のレジリエンスの向上

欧州ハイブリッド脅威対策センターが刊行したペーパーの中に、抑止側のハイブリッド脅威へのレジリエンス（抵抗力）と抑止成立の関係について、非常に興味深い分析をしたものがある[17]。それによると、ハイブリッド脅威が有効に働く条件は、その脅威手段が抑止側の社会に実際にマイナスの影響を与える程に強度が高くなくてはならないと同時に、抑止側から武力行使を含む決定的な反撃を受ける強度よりは低くなくてはならない。つまり効果が上がる最低強度と、反撃を受ける最高強度の間でハイブリッド脅威を発揮することこそが、脅威側の勝ち目だというのである。

これを逆に抑止側の立場から見ると、各種のハイブリッド脅威に対する社会としてのレジリエンスを高めると同時に、反撃については武力攻撃に限らず様々な分野でのコスト強要を組み合わせ、その発動の閾値を下げるようにしていけば、その間に挟まれたハイブリッド脅威の有効領域はどんどん狭まっていくことになる。

様々な分野でのコスト付加を組み合わせることで反撃発動の閾値を下げるというのは、まさに本稿で提唱しているコスト累積抑止と同じ発想であるが、ここでもう一つ注目すべきなのが、ハイブリッド脅威に対する抑止側社会のレジリエンスを高めることの効果である。

社会のレジリエンスが高まることで、脅威側はより高い強度のハイブリッド脅威を用いざるを得なくなる。これを前述した脅威の探知や行為者の明確化という観点から見れば、脅威側はより探知

---

[16] Mariarosaria Taddeo, "How to Deter in Cyberspace", *Hybrid Centre of Excellence Strategic Analysis 9*, June-July 2018.

[17] Vytautas Kersanskas, "DETERRENCE : Proposing a more strategic approach to countering hybrid threats", *Hybrid CoE Paper 2*, March 2020.

されやすく、真の行為者を特定されやすい、リスク・コスト共に大きな脅威手段を用いざるを得ないということになる。したがって抑止側にとって、ハイブリッド脅威に対する社会のレジリエンスを高めるような措置をとることが、コスト累積抑止成功のために大きな役割を果たす。抑止側としては、レジリエンスを強化することが、被害縮小のみならず、抑止的な効果も高めることになるということを、十分認識して対策を打つことが大切である。

(4) 効果があるコスト強要

コスト累積抑止が効果を発揮するかどうか最後のカギとなるのは、脅威側に対してどのような制裁的措置を講じてどのようにコストを課すかである。貿易等の経済分野での制裁、宣伝工作に対する反対宣伝、サイバー・電磁波・宇宙等の分野での反撃、偽装勢力や無人機等による攻撃への反撃等が具体的な手段となろうが、この際、抑止側が民主主義や自由市場経済の原理に依拠している場合、これらの国際秩序を自ら棄損することがないよう注意する必要がある。脅威側は手段を選ばずあらゆる手を使ってくるとしても、抑止側が民主主義国である場合には手段を選ぶ必要があり、ミイラ取りがミイラになってはならないのである。

この点を考えると、脅威側に比して抑止側は不利であるように思えるが、これを補う上で有効な手段となるのが、抑止側における多国間の連携である。現代においては脅威側といえども、国際社会から完全に孤立して存在しているわけではなく、様々な多国間の繋がりを維持することが不可欠である。この点を突いて脅威側にできるだけ大きな打撃を与えることができるよう、前述した脅威の探知や行為者の特定に関する協力と情報共有を基盤として、共同して制裁を加えることができれば、抑止側の対処コストを抑えつつ、脅威側が被るコストを十分大きくすることが可能になる。

この際、すでに国際秩序形成に大きな役割を果たしている各種の国際機関を通じて、その存在意義である秩序を乱すようなハイブリッド脅威の行使に対して、当該機関を通じて脅威側がこれまで得てきた利益を制限することも、大きなコスト付加となるであろう。貿易に関しては世界貿易機関（WTO）、電磁波に関しては国際電気通信連合（ＩＴＵ）などがこれに当たる。サイバーや宇宙の分野に関しては、国連の枠組みの中で規範形成の試みがなされているが、この動きを加速してしっかりした枠組みを形成することが、ハイブリッド脅威行使の抑止に繋がっていくことも見逃せない。脅威側もこれを見越して国際的に孤立しないような工作をしてくると考えられるので、支持獲得競争になることが考えられ、これにしっかり対応していくことが重要である。

５　ハイブリッド脅威抑止達成のための具体策

前節で明らかにした考慮要因を基礎として、最後に本節において、ハイブリッド脅威に対するコ

スト累積抑止を達成するために、日本の現状を念頭に置きつつ、国家としてどのような施策を講じるべきかについて考えてみよう。

(1) 国家の情報機能等の強化

前節で、ハイブリッド脅威の探知と行為者特定のために抑止側は強力な情報収集機能を持つことが必要である点を指摘したが、日本の現状を見るとこの点は甚だ心許ない。ハイブリッド脅威のそれぞれの分野について、日本に対してどのような脅威が迫っているのか初期の段階で探知するとともに、その性質や仕組みを明らかにできる能力を着実に整備していかなくてはならない。

貿易や投資などの経済活動を安全保障の手段として用いる、いわゆるエコノミック・ステイトクラフトの動きに対しては、２０２０年４月、国家安全保障局内に経済班が設置されたことで体制は一歩進んだものの、まだまだ経済分野での安全保障脅威について、体系的に情報収集と分析を行う体制を確立するには至っていない。

ＳＮＳを通じた情報操作等、外国による各種の影響工作に対しては、これを所掌する部署そのものが存在しておらず、ほとんど手つかずの状態と言ってよい。米国においては、２０１６年に国務省内にグローバル・エンゲージメント・センターが設置され[18]、ここが国家安全保障局（ＮＳＡ）等国防省の各機関、広報局・教育文化局等国務省の各機関、中央情報局（ＣＩＡ）、グローバルメディア庁などと連携して、外国や非国家組織が米国や同盟国に対して密かにに実施する宣伝や偽情報拡散を監視し、それを暴露するとともに対抗するための連邦政府の活動を総合調整しているが、日本においても同様の組織体制を確立することが急務だと言えるだろう。

サイバー攻撃に対しては、自衛隊内のサイバー防護体制は逐次強化されているが、これはあくまでも自衛隊の指揮通信システムを防護するための措置であり、政府全般や民間へのサイバー攻撃全体を探知し防護する国家としての体制は未整備で、内閣官房に設置された内閣サイバーセキュリティーセンター（ＮＩＳＣ）も指導監督組織にとどまっている。

サイバーセキュリティーと密接な関係がある電磁波セキュリティーについても、自衛隊以外の国家インフラを守ることに全く手つかずであることを考えると、総務省の関連部局を独立させて、例えば「情報通信安全省」のような組織を立ち上げ、国家インフラ等に対するサイバー・電磁波両分野の脅威をリアルタイムで探知し、これに対抗できる態勢を直ちに整えることが望まれる。今後、脅威側、抑止側の双方ともに活用を拡大することが確実である無人機の運用が、電磁波に負うところ大であるという観点からも、この分野はハイブリッド脅威全般を抑止する上で、

---

[18] グローバル・エンゲージメント・センターのホームページは、https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/。

非常に重要な意味を持っている。

宇宙分野については、２０２０年航空自衛隊に宇宙作戦隊が新編され、自衛隊と宇宙航空研究開発機構（ＪＡＸＡ）の連携による宇宙状況監視（ＳＳＡ）能力が強化されつつある。今や宇宙は、通信、情報収集、測位（ＧＰＳ等）の重要インフラとしての各種衛星が存在する場であり、ハイブリッド脅威が行使される場としても大きな比重を占めている。衛星機能が匿名性を有する手段で妨害される可能性があり、これを探知するとともに行為者を特定するために、ＳＳＡの能力は不可欠である。今後同盟・友好国との協力の下、更に能力を高めていくことが望まれる。

偽装戦力や偽装手段による攻撃という観点からは、海洋状況把握（ＭＤＡ）が重要である。主として海賊防止という観点から、マラッカ海峡周辺のＭＤＡについて各国との協力が進んでいるが、今後東シナ海及び南シナ海での中国の行動について、更に透明性を高めるための各種協力が求められる。これら海域での海上自衛隊による警戒監視活動への期待もますます高まるため、日本沿岸海域では海上保安庁による監視能力の強化を図るとともに、陸上自衛隊による沿岸監視能力を強化して[19]、離島周辺を含む近海でのＭＤＡ能力を高めることが必要である。またこの際、宇宙からの監視能力の活用にも留意すべきであろう。

⑵ 国家としての総合力発揮のメカニズム構築

前項で述べたようにハイブリッド脅威が予想される各分野で、実際の脅威を探知し行為者を突き止めるための情報能力の強化は急務であるが、これだけでハイブリッド脅威を抑止できるわけではない。コスト累積抑止を実効ならしめるためには、ハイブリッド脅威の行使を探知したならば確実に対抗する措置を講じて、脅威側にコストを課さなくてはならない。この手段は、脅威側の行為を暴露することによってその国際的評価を棄損する戦略的コミュニケーションのようなレベルから、偽装勢力等の武力行為に反撃してコストを強要する実力行動のレベルまで、多岐にわたる。

この際、効果的なコストの強要を行うためには、脅威側が用いた手段と同じ分野で制裁等を行うことにこだわらず、国家として発揮できる有効な手段をあらゆる分野の中から選択し、その状況に合わせた最適な行動を取るべきである。そのためには、収集した情報に基づき、リアルタイムで対応を打ち出せるような国家としての司令塔が必要であるが、現在の日本の体制では、この点も残念

---

[19] 陸上自衛隊は、平素から与那国島や礼文島などに沿岸監視隊を配置して船舶等の監視を行っているが、２００１年の自衛隊法改正により、「治安出動下令前に行う情報収集」という行動類型が設けられ、威力の大きい武器を持つ者による不法行為が予測される場合には、大臣の命令により武器を携行して情報収集を行うことが可能となっているので、事態が緊迫した場合には、この法的枠組みの下に沿岸部に展開して情報収集を行うことも考えられる。

ながら不十分である。

特に、情報収集において指摘したのと同様に、経済政策、国内外への情報発信、サイバー空間管理、電磁波管理、宇宙を含む科学技術政策の各分野において、国家の安全保障上の判断に基づく行動を適時かつ適切に取ることについては、意思決定メカニズムの面でも実行能力の面でも他国に後れを取っており、早急に国家安全保障局を中核とした体制の整備が必要であろう。

また脅威側の武力行為として、偽装漁民やテロリスト等の偽装勢力が用いられる場合には、初期の対応は海上保安庁や警察が行い、事態の規模に応じて自衛隊が海上警備行動や治安出動により対応することになる。その円滑な実施のための法整備や訓練等を進めるとともに、国家としてこれを適切に統制し、かつ対外的にその意図と正当性をリアルタイムで発信できる体制を確立しておかなくてはならない。そしてこれらの行動を、サイバー・電磁波・宇宙等の各分野においても適切に支援できるよう準備するとともに、そのレジリエンスを確保することも重要である。

(3) 国際連携の追求

前節で一般論としても述べたように、ハイブリッド脅威に対するコスト累積抑止を効果的に働かせるためには、抑止側として多国間で協調的な対応を取ることが大きく有効性を高めることになる。日本としても、特に民主主義や自由市場経済という点で価値観を同じくする同盟国・友好国と、ハイブリッド脅威抑止に関する協力体制を築き、脅威側へのコスト強要を共同で行っていくことが望ましい。

例えば、２０１０年9月に尖閣諸島付近で海上保安庁の巡視船に意図的に衝突した中国漁船の船長を日本側が逮捕した際、中国政府はレアアースの対日輸出を制限するという形でハイブリッド脅威を行使したが、日本はこれをＷＴＯに提訴するという形で反撃に出て、最終的にこれが国際的なルール違反と認定され中国は措置を撤廃せざるを得なかった[20]。この時重要だったのが、日本が単独でＷＴＯに提訴するのではなく、欧米諸国の支持を得て共に提訴したことであり、それが中国側にとっての外交的・経済的コストとなったことは、単に対処がうまくいったということを超えて、将来の脅威行使を抑止するという観点からも効果があったと言えるだろう。

このような国際的な共同行動は、当然双方向のものでなければならない。日本としても自国に対するハイブリッド脅威抑止への協力を他国に求めるばかりではなく、価値観を同じくする他国に対してハイブリッド脅威が行使された場合には、様々な手段で脅威側へのコスト付加に参加すること

[20]「中国ついに“白旗” VS 日欧米「レアアース兵糧戦」で自ら首を絞めた」産経ニュース、２０１５年5月１５日０６：００配信。

が求められるのは当然である。それを他人事として見過ごしていてはならない。

この視点から、本稿においては、前述した欧州ハイブリッド脅威対策センターにならって、日本が主導して米豪印各国やＡＳＥＡＮ諸国とも連携し、多国間組織として「インド太平洋ハイブリッド脅威対策センター」を設立することを提唱したい。欧州のセンターは、ハイブリッド脅威についてアカデミックな研究を行うのみならず、図上演習等を主催することにより各国のハイブリッド脅威対策能力を向上させることにも取り組んでおり、インド太平洋地域においても同様の取り組みを進めることにより、この地域におけるハイブリッド脅威抑止の能力を格段に向上させることができると考えられる。

６　おわりに

本稿においては、ハイブリッド脅威抑止に有効な考え方としてコスト累積抑止という概念を提起するとともに、特に日本を念頭に置いたハイブリッド脅威抑止達成のための具体策を導き出した。ハイブリッド脅威行使の特性は、従来型の戦争のようにある時点をもって武力侵攻が発生して戦争になるというものではなく、脅威側が特定の目的を達成するために、平素から多種多様な分野におけるハイブリッド脅威手段を少しずつ、かつ連携させて行使するというものであり、平和時と戦争時の区別が明確でなく、だからこそグレーゾーンの戦いとも表現されるのである。

したがって、これに対する抑止を考える際にも、平和時に戦争の勃発を抑止する場合のように、白黒が明確に区別できるわけではなく、小さな脅威行使の段階からこれを探知し、脅威側に確実にコストを強要することで、更なる脅威行使に進むことを抑止し、結果として脅威側の目的達成を阻むことが必要になる。すなわち、薄いグレーのうちに直ちに対処することで、それが濃いグレーに変わっていくのを食い止めるということである。更に言えば、各国の安全に資する白い国際秩序を形成・維持することに力を注ぎ、ここにグレーの要素を持ち込もうとする動きを早期に探知して即座に対応することが、最も望ましい。

日本が今直面している情勢の中にもその例がある。本年２月１日、中国において海警法が施行された。２０１３年に中国における海上法執行機関が統一されて海警となり、２０１８年にこれが中央軍事委員会の指揮下にあることが明確にされた後も、海警を律する法律が未制定だったので、今回の立法化は、組織末端に対する中央の統制を強化する手段としての側面もある。しかしその内容を具体的に見てみると、国際的な法規・慣例に明確に反し、中国が今後周辺国に対し海警をハイブリッド脅威手段として用いる根拠となるような条文を含んでいる。

例えば海警法第２１条は、中国が「管轄する」海域（今までの中国の言動から領海外も含むと考えられる）において、外国軍艦や政府船舶が中国の国内法に反した場合、強制的な退去の措置を取

ることができるとしている。これは中国も加盟している国連海洋法条約が、軍艦や商業目的以外の政府船舶が領海外で他国の管轄権行使を免除されると定めていることに反した規定である[21]。

中国が国内法を制定すること自体は国際的な問題ではないとの見解もあるかもしれないが、このような法規を定めることは、周辺国に対する一方的恫喝の効果を有するものであり、ハイブリッド脅威の一種と見るべきである。それが国際の法規慣例に反しているにも拘らず他国がこれを見過ごした場合、次にはその適用によって海警が実行動に出ることが予想され、これは決して看過できる問題ではない。国際法に背馳するような法規の執行は断じて認めることができないと、法制定時点で明確に抗議することが、更なる行動を抑止することに繋がるのである[22]。

ハイブリッド脅威の行使は、一見見過ごしてしまいがちな些細なものから始まることも多い。これを確実に探知し、脅威側に対して断固たる態度でコストを課すことが、次の脅威行使を抑止することに繋がる。日本においても、この点をしっかりと自覚して、ハイブリッド脅威抑止が可能な体制を着実に構築していくと同時に、日々油断することなく毅然たる態度で国際情勢に向かい合っていくことが、今求められているのである。

---

[21] 領海内であっても、無害通航はすべての船舶に認められている。軍艦については、領海内で沿岸国の法令に違反する場合があっても、可能なのは退去の要求までとされている。（国連海洋法条約第１７条及び第３０条）。

[22] ２０１３年に中国が「東シナ海防空識別区」を設定した際、その空域内で中国国防部の指示に従わない航空機に対しては軍が緊急措置を取るとした点が国際法に反すると各国が抗議した結果、中国が事実上この部分を空文化した事例もある。

【筆者プロフィール】

松村五郎（まつむらごろう）

１９８１年　東京大学工学部卒業。同年陸上自衛隊入隊。幹部候補生学校長、第１０師団長、統合幕僚副長、東北方面総監を歴任し、２０１６年退官。戦略学修士（米陸軍戦略大学）。著書に『自衛隊最前線の現場に学ぶ最強のリーダーシップ』（WAVE 出版）、『新しい軍隊―「多様化戦」が軍隊を変える、その時自衛隊は…』（内外出版）。

「安全保障を考える」に対する投稿について

（編 集 部）

「安全保障を考える」に対する会員各位の積極的なご投稿をお願い致します。

投稿される場合は原稿用紙（400字詰）10～15枚程度が適当と考えております。

なお、既に発表されているものについてはご遠慮下さい。