抑止概念の再考

―― 新たな脅威様相と「テーラード」抑止 ――

八木　直人

はじめに

約半世紀に及ぶ米ソ冷戦は、逆説的な 2 つの様相と可能性を示していた。一方で、超大国双方が莫大な量の核兵器を担保に一触即発の対決姿勢を示し、仮に全面的核戦争が勃発すれば、人類の滅亡が予測されるほど絶望的な状況が提示された。他方、この超大国間の対立が、ギャディス（John L Gaddis）が指摘する「長い平和」の基盤となり、20 世紀前半の両大戦とは異なる安定的な国際環境を創設したのである[1]。その逆説性とは、人類を滅亡させる可能性を持つ米ソ両国の核兵器が、安定的な国際環境の条件となったことである。しかしながら、核兵器の存在そのものが国際環境を安定させたのではなく、核兵器の破壊力の凄まじさから「抑止」の概念が生み出され、その発展が国際環境の安定に寄与したことは周知の事実である。したがって、ある意味では、「抑止」とは「核状況下」における人類の英知とも評価できよう。冷戦終結後、国際社会は「湾岸戦争」や「9.11 同時多発テロ」、「対テロ戦争」を経験してきた。後世、21 世紀初頭の世界が「地域紛争の多発する不安定な世界」と評価されるか、或いは「大規模武力紛争が抑止された比較的安定した世界」と見られるかは、現在、未知数である。現在の安全保障問題は、国家間の武力紛争から平和維持や災害復興、人道支援問題に拡大すると同時に、その領域は宇宙やサイバー空間に拡散しつつある。冷戦の終結は脅威の消滅ではなく、分散であり、そのことが時間的にも空間的にも現実となりつつある。また、「抑止」の概念は、「凄まじい破壊力」に基づく物理的条件から利得やリスクの「認知」といった心理的条件に移行しつつある。本稿では、最近の米国の戦略文書で散見される「クロス・ドメイン」という用語に注目し、ここで指摘される宇宙やサイバー空間と「抑止」の問題について考察し、さらに、21 世紀の紛争を特徴付けた「テロリズム」を抑止する可能性を検討する。次に、新たな「テーラード」抑止の概念や抑止に伴う「共通の認識、フレームワーク」について論じ、将来の抑止概念につい

[1] John L. Gaddis, “The Long Peace; Elements of Stability in the Postwar International System,” *International Security,* Vol. 10, No. 4, Spring 1986, pp.99-142.

ての知見を模索する[2]。

1　クロス･ドメインの概念と戦略的エスカレーション

「クロス･ドメイン」とは、実は曖昧な用語である。米国の公文書やドクトリンでは「ドメイン」を地上や空中、海洋と特定し、これに異なったドメインとしての「宇宙」と「サイバー空間」を加え、５つの戦略的ドメインと認識している[3]。この用語には様々な概念が含まれ、その理解には困難性が伴う。

(1) クロスドメインの定義と分類

米国国防大学(National Defense University)のマンツオ(Vincent Manzo)は、戦略概念としてのクロス･ドメインの多様性に言及し、3 つの仮説的概念を提示している。すなわち、クロス･ドメインを規定する第 1 は「兵器のプラットホームと目標位置」であり、第 2 は「宇宙･サイバーの利用度」、第 3 は「作戦の効果」に基づく分類基準である。第 1 の「兵器プラットホームと目標位置」は、例えば、地上発射対衛星(ASAT)ミサイルによる衛星の破壊がクロス･ドメイン攻撃となり、軌道上の衛星からの攻撃は同一ドメインと分類される。航空機搭載巡航ミサイルによる水上艦艇攻撃はクロス･ドメイン攻撃であり、艦艇搭載巡航ミサイル(SLCM)による艦艇攻撃は同一ドメインである。このような兵器のプラットホームや目標位置によるクロス･ドメインの定義は、それが新たな概念ではないことを示している。海軍部隊に対する空襲、空軍基地への艦砲射撃、地上軍に対する空海共同攻撃等は現代戦における通常の状況であり、クロス･ドメイン作戦は最も単純かつ適切な選択肢である。例えば、SLCM 攻撃の脅威を受ければ、潜水艦や水上艦艇で抵抗するよりは、瞬時に航空機によって敵の海軍戦力を攻撃する方が合理的である[4]。第 2 の分類基準では、現在の地上

---

[2] 「テーラード」抑止には、「注文仕立て」の抑止や「状況対応」抑止等の訳語が考えられるが、本稿ではカタカナ表記とした。

[3] クロス･ドメインについては、以下の公文書を参照のこと。
Department of Defense (DOD), *Quadrennial Defense Review Report,* DOD, February 2010, pp.33-34, pp.37-39; The White House, *National Security Strategy,* May 2010, p.22; DOD, *National Security Space Strategy,* January 2011; The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,* May 2011; DOD, *Department of Defense Strategy for Operating in Cyberspace,* July 2011.

[4] Vincent Manzo, "Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit?" *Strategic Forum,* No. 272, INSS, NDU, December 2011.

や空中、海洋の戦力の大部分がサイバー空間と宇宙を利用し、その複雑な任務が異なったドメインからのアプローチを集積して達成される状況に基づいている。通常、精密誘導兵器は、衛星やコンピュータ・ネットワークの利用によって有効に機能する。この状況はクロス・ドメイン攻撃であり、攻撃プラットホームや目標存在のドメインには無関係である。同様に、サイバー攻撃は、通常、コンピュータ・システムへの攻撃を意味し、軍事コンピュータの機能発揮の阻害と妨害に主眼が置かれ、攻撃の成否は、他のドメインへの効果によって評価される。つまり、陸海空に配備された兵器体系はコンピュータ・ネットワークに依存しており、サイバー攻撃によって機能が阻害される。換言すれば、サイバー攻撃の主要な目標は、他のドメインに対する間接的影響である[5]。例えば、ASAT 兵器に対する攻撃は、プラットホームが同一ドメインであっても、その影響はクロス・ドメインである。第 3 は、作戦の効果から定義されるクロス・ドメインである。この定義では、ドメイン間の関係(味方と敵)が戦略的脆弱性をつくることを示している[6]。例えば、通常の精密誘導兵器による攻撃には、複数のドメインに対するアプローチを必要とする。米国の潜在敵国は、米国の航空機や巡航ミサイル搭載潜水艦を破壊できないとしても、これらのプラットホームを管制する米国の宇宙やサイバー・システムを攻撃することは可能である[7]。このことは、最近の宇宙やサイバー・ドメインに関する潜在敵国のインタレストや行動の基本とも分析できる。つまり、予測され得るアプローチとは、自国に有利なドメインへ紛争を移行させ、それによって、自国が不利であるドメイン(例えば、航空や海上)における米国の能力を変化させる可能性を示している[8]。このクロ

---

[5] 2009 年度の「国家調査委員会(2009 National Research Council)」報告では、サイバー攻撃を「敵コンピュータ・システムやネットワーク、情報プログラム、そのシステムやネットワークを変化・切断・精度低下・破壊」する隠密的行動と定義している。ところが、サイバー利用は、無許可でコンピュータ・システムやネットワークから情報を得ることでもある。この報告書は、サイバー攻撃の意図された効果が、他のドメインで生起することを立証している。すなわち、「直接的、或いは急迫の効果は、コンピュータ・システムやネットワーク攻撃である。間接的、或いは後続的影響はシステムに対する影響であり、コンピュータ・システムやネットワーク・コントロール装置が攻撃の目標」となる。
National Research Council, *Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyber-attack Capabilities* , National Academies Press, 2009, p.80.

[6] ドメイン間の関係や脆弱性については、以下を参照のこと。
Mark E. Redden and Michael P. Hughes, "Global Commons and Domain Interrelationships: Time for a New Conceptual Framework?" *Strategic Forum, No. 259,* INSS, NDU, October 2010.

[7] Manzo, "Deterrence and Escalation in Cross-domain Operations."

[8] 例えば、宇宙やサイバー空間における軍事戦略については、以下を参照のこと。

ス・ドメインへのアプローチ―特に、宇宙やサイバー―は、米国の陸海空軍戦力が宇宙やサイバー資産に多くを依存していれば効果的であり、反対に依存度が低ければ効果が薄くなる。したがって、クロス・ドメイン作戦とは、自己の強点の最大利用と敵の脆弱性への集中であり、「非対称紛争(asymmetric warfare)」との共通性を指摘することができる[9]。本稿では、宇宙やサイバー空間へのアプローチから第 2 及び第 3 の仮説について議論を進める。

(2) 抑止とエスカレーション戦略

シェリング(Thomas Schelling)が『軍備と影響力(Arms and Influence)』で示した概念は、現在においても抑止概念の基本となっている。シェリングは、抑止の脅威が潜在敵国に理解される場合に限り、抑止の信頼性が保たれると主張し、抑止の脅威と行動とが比例均衡していれば、抑止が機能すると分析した。抑止の脅威は「…相手方に他方の意図を理解させ、行動の結果に関する予測の判断基準を提供」し、同時に「行動と反応の相互関連性には、偶然性を排除し、結果予測の根拠を提供することが含まれる」のである[10]。反対に、事態のエスカレーションを意図する場合には、抑止的行動のパターンを崩し、状況に応じて「敵にいい加減さを示し、対決を挑発し、敵の平衡感覚を失わせる」等の方法が考えられる。国家間において「認知された規則を破ることは、劇的な行動を通じて、一方の意図を正確に伝えること」であり、「規則遵守に対する拒絶」の意図が明確になる[11]。冷戦期間中には、一般に認識されたエスカレーション・ラダー―通常兵器から化学・生物兵器、核兵器まで―が存在しており、また、通常紛争の範囲内においてもエスカレーションの法則が存在していた。戦闘の地

David C. Gompert and Phillip C. Saunders, *The Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability,* NDU Press, 2011, chapter 3; James Dobbins, David C. Gompert, David A. Shlapak, and Andrew Scobell, *Conflict with China: Prospects, Consequences, and Strategies for Deterrence,* RAND, 2011, pp. 5-7; Office of the Secretary of Defense, Annual Report to Congress, *Military and Security Developments Involving the People's Republic of China 2010,* DOD, August 2010, pp. 22-37; Jan Van Tol with Mark Gunzinger, Andrew Krepinevich, and Jim Thomas, *AIRSEA Battle: A Point-of-Departure Operational Concept*, Center for Strategic and Budgetary Assessments, 2010, pp. 17-47; Roger Cliff et al., *Entering the Dragon's Lair: Chinese Anti-Access Strategies and their Implications for the United States* RAND, 2007, pp. 51-60.

[9] 「非対称戦」については、以下を参照のこと。
石原敬浩「AirSea Battle と対中抑止の理論的分析 - トシ・ヨシハラ、ジェームズ・ホルムズの論考を題材として」『海幹校戦略研究』第 2 巻第 2 号、2012 年 12 月。

[10] Thomas C. Schelling, *Arms and Influence,* Yale University Press, 1966, pp.146-149.

[11] Ibid., pp. 150-151.

理的領域や攻撃目標の拡大(例えば、狭義の軍事目標から広範な社会目標まで)、暴力の烈度の増大(例えば、爆弾やミサイルの爆発力の調整等、通常兵器の破壊力の調整)が検討され、一定の敷居(thresholds)が設けられていた。しかしながら、マンツオに拠れば、現在の国際関係では「対宇宙・サイバー攻撃がエスカレーション・ラダーに適合する共有のフレームワークが欠如」しており、宇宙・サイバー空間には、従来の地上・航空・海上ドメインとは異なって、共通の概念や認識が構築されていない[12]。多数の諸国は、宇宙やサイバー空間が戦場の一部となる戦争を経験したことがなく、専門家であっても、これらのドメインでの通常兵器や核兵器とは異なる攻撃に関する正確な影響について確信が持てない状況である[13]。したがって、宇宙・サイバー攻撃が、どのように他のドメインとの相互作用を生起させるかが不明である。また、平時や危機、戦争以前の段階における対立・政治関係を含めた広範かつ共通の認識やフレームワークが存在しないことから、報復の均衡とエスカレーションを選別することが困難になっている。つまり、伝統的戦略的ドメインから新たなドメインを横断する状況が顕著になっている。米国と同盟国、潜在敵国の間に抑止やエスカレーションに関する共通のフレームワークが欠如していれば、誤算や誤解の可能性を増大させる。例えば、局地的な越境問題が、経済・資源領域での反応や報復―ある意味でクロス・ドメイン―に発展すれば、均衡が崩れ、抑止の信頼性が低下する。効果的な抑止とは、一方が望む行動の結果に対する他方の認識に影響を及ぼすことであり、そのためには報復や脅威、或いは反応が相互に論理的であり、均衡している必要がある。クロス・ドメインに関する共通の認識やフレームワークを構築するには、様々な問題が存在している[14]。例えば、1) 対宇宙・サイバー攻撃の評価基準 、2) 動的攻撃(kinetic attacks)と非動的攻撃(non-kinetic attacks)の均衡―非動的攻撃に対する動的対応はエスカレーションか否か？―、3) サイバー攻撃と巡航ミサイル攻撃の均衡 、4) クロス・ドメインとエスカレーションの関係等である。米国国防省のミラー(Principal Deputy Under Secretary of Defense for Policy, James Miller)は、対宇宙攻撃に対する米国の反応が「宇宙領域外での必要な均衡を想定している」と証言しているが、その

12 Manzo, “Deterrence and Escalation in Cross-domain Operations.”
13 サイバー攻撃に関する不確実な意図と影響については、以下を参照のこと。
Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyber-attack Capabilities , pp. 121-128.
14 Manzo, “Deterrence and Escalation in Cross-domain Operations.”

詳細は不明である[15]。

(3) クロス・ドメインと抑止の様相

どの程度のドメインが含まれるかに関係なく、影響の評価を目的に、潜在敵国間での共通フレームワークを深化させ、適切な対応を明確に示すことは困難である。国際社会は、文化的相違や対照的な戦略目標、戦力構造やドクトリンの相違、強度と脆弱性の相違に満ちており、クロス・ドメインにおける均衡とエスカレーションについて、様々な異なる意識や結論が導かれるであろう[16]。この問題を悪化させているのが、前項で論じてきた戦略的ドメインの不確実性である。例えば、非動的手段(レーザー妨害や欺瞞)による衛星への干渉は、サイバー攻撃を通したデータ妨害や衛星攻撃能力の浸食と均衡するのか？また、新たなドメインにおける攻撃はエスカレーションであるのか？サイバー空間と他のドメインにおける報復と対報復の均衡は、どのような様相を示すのか？動的な ASAT 攻撃に均衡する報復とは？衛星に対する非動的攻撃と ASAT 兵器に対する動的攻撃は均衡しているのか？地理的敷居の横断は、エスカレーション反応であるのか？[17]これらドメインにおける攻勢・防御間の不均衡は、その効果やエスカレーション、均衡に対する認識、また、最適な抑止戦略に影響を及ぼすことになる。宇宙やサイバー空間における対立的様相が支配的であれば、いずれの諸国も紛争を迅速に終焉させ、敵を懲罰するためにリスクを冒す可能性があり、宇宙とサイバー空間における脆弱性は、強力な報復的脅威の信頼性を求め、攻撃効果との均衡を模索するであろう。新たなドメインにおける抑止戦略とは、攻撃の利得を拒否し、敵国が衛星やコンピュータ・ネットワークを攻撃しても、従来の戦力には多大な影響を及ぼさないと確信させる必要がある。平時におけるサイバー利用は、危機における抑止に影響を及ぼすか否かが不明で

---

15 James N. Miller, testimony for the House Armed Services Committee, Subcommittee on Strategic Forces, March 2, 2011. Quoted, Manzo, "Deterrence and Escalation in Cross-domain Operations."

16 この問題の理論的・歴史的研究と米中ドクトリンについては、以下を参照のこと。Christopher P. Twomey, *The Military Lens: Doctrinal Differences and Deterrence Failure in Sino-American Relations,* Cornell University Press, 2010.

17 これらの設問は、宇宙・サイバー空間攻撃に対する対称・非対称反応が均衡及びエスカレーション反応とは同義でないことを示している。しかしながら、対称戦が同一ドメイン、同一タイプの兵器、同一タイプの目標攻撃と仮定されれば、様々な対応の均衡問題はエスカレーションに帰結する。初期攻撃と同一ドメインの目標に対する非対称戦は、異なる種類の兵器や目標等、多様な組み合わせが想定され、定義が困難である。異なったドメインの目標に対する非対称アプローチの検討は、事態の相違を判定する以上に困難である。Manzo, "Deterrence and Escalation in Cross-domain Operations."

ある。サイバー搾取(exploitation)―無許可で情報を奪取すること―とサイバー攻撃―ネットワークの破壊―は、テクノロジーや作戦は類似しているが目的と影響が異なり、サイバー空間での戦争の証拠か否かが不明である[18]。多数の兵器システムと大部分の軍事作戦は、複数のドメイン(地上、航空、海上、宇宙・サイバー空間)へのアプローチを必要とし、クロス・ドメイン攻撃によって脆弱性が露呈される。将来の抑止の焦点はクロス・ドメインにおける脅威である。しかし、この領域での均衡やエスカレーション、信頼性、抑止や強要の概念については、共有のフレームワーク―現実だけではなく、分析的・理論的―が欠如している。分析的フレームワークは、異なったドメインにおける反応の均衡やエスカレーションの可能性を判断する場合に不可欠である。

2　テロリズムの抑止；その可能性と問題

ブッシュ大統領(President George W. Bush)の 2002 年の「安全保障戦略(2002 National Security Strategy)」―9.11 の 1 年後に公刊―は、「抑止の伝統的概念は、テロリストには効果的ではない。敵の戦術は理不尽な破壊と無実の人々を目標としている。テロリストは死に殉教を見いだし、守るべきものが無国籍である」と述べている[19]。しかしながら、2006 年の「4 年毎の国防見直し(Quadrennial Defense Review: QDR)」では、「全ての抑止に適合するサイズ(from a 'one size fits all' deterrence)―不法勢力やテロリスト・ネットワーク、競合者に対するテーラード抑止(tailored deterrence)―への転換」が意図されている[20]。その目的は、「完璧な均衡を保ち、国家的・非国家的脅威―物理的・情報空間を含む―であるテロリスト攻撃を抑止するテーラード的能力(tailored capability)の提供」であった[21]。2011 年に出版された『反撃(Counterstrike)』では、「…新たな戦略とテロリスト・グループに対する斬新かつ効果的な抑止態勢が構築された」と評価されている[22]。抑止の破綻から開始された対テロ戦争は、その終焉に当たって再度、抑止態勢の構築を模索しているのである。

---

[18] Michael Riley and Ashlee Vance, "Cyber Weapons: The New Arms Race," *Bloomberg Businessweek,* July 20, 2011.
[19] *The National Security Strategy of the United States of America,* September 2002, p. 15.
[20] *Quadrennial Defense Review Report,* February 6, 2006, p. vi.
[21] Ibid., p. 49.
[22] Eric Schmitt and Thom Shanker, *Counterstrike: The Untold Story of America's Secret Campaign against Al Qaeda,* Times Books, 2011, p. 51.

(1) 冷戦期の抑止と現在

米国のテロ抑止政策に関与してきたクローニンとパーベル(Matthew Kroenig and Barry Pavel)は、テロリズムの抑止が「部分的に成功する可能性」に言及している[23]。テロリズムに対する抑止を検討する場合、冷戦期とは異なる抑止構造を理解する必要がある。第 1 に、対テロリズムにおいて抑止すべき対象は極めて多様である。冷戦期間中、米国の唯一の敵はソ連であり、その意思決定に影響を及ぼすことが抑止の目的であった。対テロ戦争において、米国は複雑なネットワークに基づく多様な敵に対峙しなければならない。したがって、各々の敵を正確に理解し、全てのテロリズムを一様に抑止する政策を企図することは極めて困難である。第 2 に、冷戦期の抑止は絶対的であったが、現在では部分的である。冷戦期の抑止が破綻すれば、ソ連が西欧を侵攻するか、或いは大規模核攻撃が実施される可能性があった。反対に、テロリズム全般の抑止は不可能であり、特定の種類のテロリストの特定の種類のテロ活動を思い留まらせることに限られる。したがって、第 3 に、対テロリズムにおける抑止は広範な戦略―包括的戦略(comprehensive strategy)―の 1 つの要素に過ぎない。しかし、抑止は、効果的な対テロ戦略の不可欠な構成要素と認識されるようになった[24]。冷戦期との抑止構造の相違を明確にすることによって、抑止の対象が限定されつつある。テロリストに対する適切な抑止とは、テロリスト・ネットワークの解体を意味する。クローニンとパーベルは、「過激な聖職者は扇動的な説教を行い、投資家はテロ作戦に融資し、リーダーは攻撃命令を下す」として、ネットワークの解体による行動の抑止が「直接、攻撃を防ぐのと同等の重要性を有する」と指摘している[25]。

(2) テロリズム抑止の理論と戦略

抑止とは戦略的相互作用(strategic interaction)であり、主体が敵に対して、特定の措置を執るためのコストが増加する可能性を確信させることによって、その措置の採用を防ぐ行為である。したがって、抑止を達成するには、主体が敵の特定の行動に対するコストや利得に関する認識を形成する必要がある。コ

---

[23] Matthew Kroenig and Barry Pavel, "How to Deter Terrorism," *The Washington Quarterly,* Vol. 35 , No. 2, Spring 2012. pp. 21-36.
[24] Ibid., pp. 25-27.
[25] Ibid., p. 29.

スト強要(いわゆる「報復的抑止(deterrence-by-retaliation)」、或いは「懲罰的抑止(deterrence-by-punishment)」)戦略は、敵が特定の行動方針を採用した場合、敵に受け入れ難いコストを強要すると脅すことによって抑止を達成することである[26]。一般的に、「抑止」は報復的抑止を意味するが、抑止理論では第 2 のタイプの抑止戦略も検討されてきた。それは、利得拒否(benefit denial)、或いは拒否的抑止(deterrence-by-denial)であり、敵の特定の行動の利得を拒否するという脅迫によって抑止を達成する戦略である。コスト強要戦略(cost imposition strategies)が報復を仄めかすのに対して、利得拒否戦略(benefit denial strategy)は失敗を仄めかし、敵が成功を疑い、特定の行動から利得を達成できないと思えば、それを思い留まる可能性がある。例えば、ミサイル防衛は、核攻撃の利得を減らすことによって抑止を達成する。さらに、スナイダー(Glenn Snyder)は、拒否的戦略の有効性を指摘し、「攻撃拒否の脅威は、攻撃に対する報復の脅威より信頼性が高く、強力な抑止力となる」と述べている[27]。

したがって、テロリズムを抑止するための戦略は、コスト強要戦略と利得拒否戦略に区分され、前者は直接的反応と間接的反応、後者は戦術的拒否と戦略的拒否に分類される。直接的反応戦略とは、報復の脅威によって敵を抑止することを目的とし、従来の抑止形態―「報復(retaliation)」や「懲罰(punishment)」戦略―である。テロネットワークに対する報復的脅威の有効性は、例えば、融資家や支持者、急進的聖職者への「投獄の脅威」や資金停止の脅威に示されている[28]。また、国家的スポンサーは直接的反応戦略に脆弱であり、テロリストに聖域(安全な避難所)や兵器を提供する国家が特定できれば、従来の報復的・懲

---

[26] 「抑止」や「強要」の定義については、以下を参照のこと。
Robert J. Art, "To What Ends Military Power?" *International Security,* No. 4, Spring 1980, pp. 3-35.
なお、本論文は、以下にも再録されている。
Peter Hays ed., *American Defense Policy, 7th ed.*, Johns Hopkins University Press, 1997, pp. 17-23.

[27] Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security,* Princeton University Press, 1961, p. 16.

[28] Kroenig and Pavel, "How to Deter Terrorism," p. 23.
例えば、英国政府は「テロリズム賛美(glorification of terrorism)」を禁止する法律の制定(2006 年 3 月)によって、多数の聖職者の扇動的説教とネットワークを解体した。これは急進的聖職者に対する「投獄の脅威」(聖職者の大部分がロンドン郊外で市民的生活を享受していた)による抑止と理解されている。以下の資料による。
Jon Ronson, *Them: Adventures with Extremists,* Simon and Schuster, 2002; James Brandon , "The Next Generation of Radical Islamic Preachers in the UK," *Terrorism Monitor,* Vol. 6, No. 13, June 2008.

罰的抑止が可能となる[29]。反対に、直接的反応戦略には、潜在的制限が存在する。第 1 に、テロリストの「中核(hard core)」は直接的報復の脅威によって抑止されない。第 2 に、テロとは無関係な人々に対する再保証政策(policies of reassurance)―テロ活動から距離を置く人々は罰せられないという確約―による抑止の補完が必要となる[30]。間接的反応戦略は、テロリストに報復することではなく、テロリストが価値を置くもの(或いは、テロリストを納得させる)―例えば、その家族や資産、コミュニティ―に脅威を加えることである。その事例は、過去のイスラエルの反応―自爆テロ犯の家族の家屋の破壊や課税措置―に見られ、テロリストのコスト/利得計算に影響を及ぼす―栄光や殉教の利得の相殺―可能性がある。しかし、家族やコミュニティに対する強要は人道的･法的問題を含み、一定の抑止効果が確認されても、実行には躊躇が伴っている。また、間接的反応戦略は、その方法によっては規制されないエスカレーションの可能性を提示している[31]。

戦術的拒否戦略とは、戦術レベルにおける脅威の回避を意味する。テロリストが攻撃の失敗を確信すれば、時間と資源の浪費を回避するためにテロリズムは抑止される。したがって、対テロ情報網を確立し、重要目標を堅固にすれば、攻撃に対する強固な抑止力となる。もちろん、全ての目標を防御することは不可能であり、テロリストは強固な目標から脆弱な目標へと焦点を移動させる可能性がある。しかし、強固な防御はテロリストに失敗の可能性と多大なコストを強要する。したがって、テロ攻撃に対する最も有効な抑止は報復力ではなく、目標に対する強固な防御であり、敵に作戦の失敗―或いは失敗の可能性―を確信させるという考え方である。また、抑止とは心理的関係(psychological relationship)であって、攻撃が失敗するとテロリストに確信させる戦略的コミュニケーション(strategic communications)が必要である[32]。戦略的拒否政策とは、テロリストに戦略的利得を与えない―或いは与えないと脅す―ことによって、抑止を達成する。テロリストの戦略目的を体系的に拒否するには、先ず、

---

[29] テロ組織とテロ支援国家、或いは聖域の設定については、以下を参照のこと。
Robert F. Trager and Dessislava P. Zagorcheva, "Deterring Terrorism: It Can Be Done," *International Security,* Vol. 30, No. 3, Winter 2005/06, pp. 87-123; Daniel Byman, *Deadly Connections: States that Sponsor Terrorism,* Cambridge University Press, 2005; Caitlin Talmadge, "Deterring a Nuclear 9/11," *The Washington Quarterly,* Vol. 30, No. 2, Spring 2007, pp. 21-34.

[30] 抑止を目的とした脅威と確約の関係については、以下を参照のこと。
Schelling, *The Strategy of Conflict*, p.12.

[31] Kroenig and Barry Pavel, "How to Deter Terrorism," p. 27.

[32] Ibid., p. 29.

目的の確認が基本であり、その目標の戦略的関連を切断する必要がある。この場合、市民の知る権利とテロリズム防止のための政府の努力との均衡が求められる[33]。また、テロリストが社会的パニックを引き起こす能力を確信できない場合、テロリズムは抑止される。これは市民社会が迅速に立ち直る能力―反発力(resilience)―であり、テロ攻撃が日常生活を崩壊させ得ないというシグナルとなる[34]。さらに、抑止効果を高めるものとして、国際社会がテロ組織の政治的要求を断固として拒否する姿勢をとることが挙げられる。戦略的拒否の信頼性を向上させるには、シェリングが指摘するように、国際社会の意思疎通の確立が不可欠である[35]。その意味では、テロリズムが有効な戦略であるという認識を粉砕することが、テロリズム抑止の最良の戦略的手段である。

3　冷戦後の抑止論争とテーラード抑止

米国は、2006 年と 2010 年の「安全保障戦略」において、抑止の基本概念を再構築し始めている[36]。そこでは抑止の基本的概念―確実な脅威と受け入れ難い報復によって攻撃を防ぐこと―が再確認され、例えば、「統合作戦概念における抑止作戦(Deterrence Operations Joint Operating Concept: DO-JOC)」において、合理的な抑止理論と EBO 概念(effects-based operations concepts)を組み合わせた統合アプローチを提示し、抑止の目的が「敵の意思決定に重大な影響を及ぼすこと」であると述べている[37]。この抑止理論の展開の背景には、冷戦期とポスト冷戦期を通じて理論的検討が繰り返されてきた経緯がある。本章では、この展開を把握し、前述のクロス・ドメインとテロリズム抑止との関連を検討する。

(1) 抑止概念の理論的展開

抑止概念の普遍性とは、その論理的単純性に起因している。その概念は、敵に行動を起こさないように脅迫し、或いは納得させることであって、それ自体

---

33 Daniel Williams, "Egypt Gets Tough in Sinai in Wake of Resort Attacks," *Washington Post,* October 2, 2005.
34 Kroenig and Barry Pavel, "How to Deter Terrorism," p. 28.
35 Schelling, *Arms and Influence.*
36 *The National Security Strategy of the United States of America,* The White House, March 200), p.43; *National Security Strategy*, The White House, May 2010.
37 Department of Defense (DOD), *Deterrence Operations Joint Operating Concept Version 2.0[hereafter DO-JOC],* DOD, December 2006, p. 5.

は難解ではない。米国の統合ドクトリンは、抑止を「結果に対する恐怖による行動の阻止」と定義し、「抑止とは、受け容れ難い反作用に関する信頼性の高い脅威の存在による心理的状態」としている[38]。既に述べたが、抑止は 2 つのカテゴリー―懲罰的抑止と拒否的抑止―に分類され、前者が「敵の行動に対する報復の脅威」であり、後者が「敵の行動を巧妙に阻止する脅威」と定義されている[39]。過去、抑止の条件―受け容れがたい脅威と脅威の信頼性―については合意が達成されてきたが、抑止の定義や効果、その成否予測については、現在でも検討が重ねられている[40]。

ジャービス(Robert Jervis)は、抑止理論の展開を 3 つの段階に分類している[41]。抑止理論の第 1 段階は第 2 次大戦直後に出現し、国際関係論における核兵器の意義を理解するための論議から派生したものであった。ウォルフォース(Arnold Wolfers)は、1946 年の『絶対兵器(Absolute Weapon)』において、核兵器による報復の脅威が「制止(determent)」の最強手段であると認めている[42]。

抑止理論の第 2 段階は 1950 年代から発展し、その特徴は国際政治学、或いは国際関係論における合理モデルとの整合性が図られた点にある。1958 年、ウォルステッター(Albert Wohlstetter)は反撃力の充分性に焦点を当て、「攻撃を阻止することは、逆説的に、反撃の可能性を意味している」と指摘している[43]。シェリングは、紛争の可能性が相互の意図の認識と第 1 撃の恐怖に依存することを証明するため、ゲーム理論を活用した[44]。第 2 段階の抑止理論は、確実な第 2 撃能力と報復の脅威、さらに同盟諸国に対する「信頼できる」拡大抑止の提示であり、同盟国に対する保証と自動的報復発動の確証が担保されていた。[45]

---

[38] Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms,* The Joint Staff, November 8, 2010 (As Amended Through 15 August 2012), p.90.

[39] Jeffery W. Knopf, "Three Items in One: Deterrence as Concept, Research Program, and Political Issue," in T.V. Paul, Patrick M. Morgan, and James J. Wirtz, eds. *Complex Deterrence: Strategy in the Global Age*, University of Chicago Press, 2009, p. 38.

[40] T.V. Paul, "Complex Deterrence: An Introduction," in *Complex Deterrence,* pp.2-3.

[41] Robert Jervis, "Deterrence Theory Revisited," *World Politics,* Vol.31, No.2, January 1979, p. 289.

[42] Arnold Wolfers, "The Atomic Bomb in Soviet-American Relations," in *The Absolute Weapon: Atomic Power and World Order,* ed. Bernard Brodie, Harcourt, Brace and Company, 1946, p. 134.
なお、核抑止理論における『絶対兵器』の現代的意義については、以下を参照のこと。
Austin Long, *Deterrence: From Cold War to Long War,* RAND, 2008.

[43] Albert Wohlstetter, *The Delicate Balance of Terror,* RAND, 1958, pp. 3-4.

[44] Thomas C. Schelling, *The Reciprocal Fear of Surprise Attack,* RAND 1958; Thomas C. Schelling, *The Strategy of Conflict,* Harvard University Press, 1960, p.207.

[45] 拡大抑止と同盟の問題については、以下を参照のこと。

さらに、抑止主体が合理的な国家と仮定され、経済理論に基づく有用性極大化の選択が想定されている。つまり、決定の基礎は、最大利得と最小損失である[46]。しかしながら、その理論は、冷戦的影響によって、国家間の敵対的関係に対処することに限定されている。第 2 段階の理論展開によって、米国政府は核兵器総数の確保を忠実に実行した[47]。大規模な核第 2 撃能力(large nuclear second-strike capability)を開発し、その拡大抑止のコミットメントの信頼性の確立を目指したものであり、その抑止理論は、「封じ込め戦略」の理論的支柱になり得たのである[48]。

ジャーヴィスは、抑止理論の第 3 段階を指摘している。それは 1970 年代に始まり、第 2 段階理論を補強するか、或いは論破するために経験的分析と心理学を適用したことが特徴的である[49]。経験的分析から、成功の理論的条件―第 2 段階で指摘されたコミットメントや意思疎通、信頼できる脅威―が満たされた場合でも、現実世界では抑止は失敗する場合があると指摘された[50]。また、経験的には侵略者がリスクを厭わない傾向にあり、脅威と伴に報酬の有用性や国内政治要因の影響力が指摘されている[51]。さらに、敵対者の意思決定プロセスの分析に焦点を当て、第 2 段階の「脅威の信頼性」から心理学的視点への発展が散見される[52]。したがって、第 3 段階では、心理的要因が意思決定者に不合理な行動を執らせる可能性を指摘し、最も重要な心理的要因の 1 つである誤認―特にリスク評価の失敗―に言及した[53]。合理的抑止理論に反して、意思決定者の利得やリスクに対する評価が曖昧であれば、費用対効果の分析が不可能となる[54]。同様に、強力な心理的バイアスは、抑止の相互関係に影響を及ぼす。70 年代以降、合理的抑止理論に対する経験的・心理的アプローチが展開された

Schelling, *Arms and Influence*, pp.36-40; Schelling, *The Strategy of Conflict,* pp. 188-189; Long, *Deterrence: From Cold War to Long War,* pp. 13-15.

46 Christopher H. Achen and Duncan Snidal, "Rational Deterrence Theory and Comparative Case Studies," *World Politics,* Vol.41, No.2, January 1989, p.150; Richard Ned Lebow and Janice Gross Stein, "Rational Deterrence Theory: I Think, Therefore I Deter," *World Politics*, Vol.41, No.2, January 1989, pp. 209-210.

47 Jervis, "Deterrence Theory Revisited," p. 290.

48 Schelling, *Arms and Influence,* p. 40.

49 Jervis, "Deterrence Theory Revisited," pp. 289-301.

50 Knopf, "Three Items in One," pp. 47-48.

51 Jervis, "Deterrence Theory Revisited," pp. 303-304, 312.

52 Knopf, "Three Items in One," p. 48.

53 Jervis, "Deterrence Theory Revisited," pp. 307-308.

54 Ibid., pp. 308-310; Stein, "Rational Deterrence against 'Irrational' Adversaries?" p. 63.

が、以来、抑止に関する統合理論は現れなかった[55]。換言すれば、抑止理論は「核兵器の登場」―破壊力の凄まじさと使用不可能性―によって萌芽し、国際政治学上の合理性モデルの進展と伴に精緻に理論化され、さらに、経験的･心理的分野を包括した「認知的モデル」へと発展していた。しかしながら、冷戦の終焉は抑止対象をソ連から無法国家(rogue states)に移行させ、9/11 攻撃は、非国家主体や無国籍の支持者を抑止する議論を提出した。抑止理論は、兵器や地域といった限定的範疇ではなく、紛争の全てのスペクトラムに該当するアプローチを求められたのである。

(2) 「テーラード抑止」とその批判

周知のとおり、ブッシュ大統領は、2006 年の「安全保障戦略(NSS)」や「4 年毎の国防見直し(QDR)」等において、「テーラード抑止(tailored deterrence)」の概念を紹介した。4 年に及ぶ予防戦争の後、ブッシュ政権は抑止を復活させ、再検討することとなった。2006 年度の QDR では、「"全てに対応する抑止(one size fits all)"から無法国家やテロリスト･ネットワーク、競合者に対するテーラード抑止への転換」を公表している[56]。オバマ（Barack H. Obama）政権は、ブッシュ時代のテーラード抑止の政策を継続している。2010 年度の NSS と QDR は、2006 年度以来、ほぼ同じ用語でテーラード抑止を記述している[57]。2010 年度の QDR によれば、「米国の防衛コミットメントの信頼性は、抑止に対するテーラード･アプローチを要求している」と述べ、「個人やネットワーク、国家であるか否かに拘らず、潜在的敵対勢力の能力や価値観、意図、政策決定の深部の理解が不可欠」であり、抑止には「国力の全局面を統合する必要がある」と指摘している[58]。DO-JOC は国防省と政府の協調関係を強調し、「米国の死活的インタレストに対する敵対的行動を阻止するため、敵の意思決定に重大な影響を及ぼす」可能性を指摘している[59]。つまり、政府は、抑止する敵と抑止される行動を明確にし、同時に、国防省は敵やシナリオの特徴に応じた個別

---

[55] Jervis, "Deterrence Theory Revisited," p.314; Amir Lupovici, "The Emerging Fourth Wave of Deterrence Theory; Toward a New Research Agenda," *International Studies Quarterly*, Vol.54, No3, September 2010, p. 708.
[56] *Quadrennial Defense Review Report 2006*.
[57] *National Security Strategy,* p.22; *Quadrennial Defense Review Report 2010,* pp. 13-14.
[58] *Quadrennial Defense Review Report 2010*, p. 14.
[59] DO-JOC, p. 5.

的運用(tailor operations)が必要となる[60]。DO-JOC の仮説に拠れば、敵の行動の適否の決定は選択的行動方針の計算に基づくとされ、各々の敵の決定要素を特定し、評価する必要がある[61]。その決定要素とは、行動の利得、行動のコスト、抑制の結果―敵が行動をとらない場合に生起する事態―である。また、DO-JOC は、米国が敵の「意思決定に関連する価値観や認識」に影響力を及ぼすことができると仮定している[62]。つまり、目的を達成するための方法とは「抑制を促し、敵の利得を拒否し、敵にコストを強要する信頼性の高い脅威」であり、同時に、大規模な国家抑止戦略の一部としての省庁間活動が平時や危機、戦争期間においても日常的に実行される[63]。DO-JOC は、テーラード抑止を通じて「抑止の目的を達成するのに必要な方法を理解する新たなアプローチ」を提供している[64]。しかしながら、米国空軍のラーキン大佐(Colonel. Sean P. Larkin, USAF)は、DO-JOC の主張を検討し、テーラード抑止とは「新品の袋に年代物のワインを注いだ」ように見えると批判している[65]。すなわち、抑制の促進や利得の拒否、コスト強要のための信頼性の高い脅威とは、抑止理論の第 2 段階と第 3 段階の混合物に過ぎず、利得の拒否とコストの強要は、単に拒否的抑止と懲罰的抑止の置き換えに過ぎない。抑制の推奨はシェリングの第 3 段階の提言―敵に現状維持を再保障し、或いは報酬を申し出る―を取り入れたものである[66]。さらに、合理的抑止理論から、敵の選択が行動の期待コストと利得に関する合理的計算に基づくと仮定しているが、敵対勢力は個別的であり、ユニークな意思決定の複雑なシステムと見なされ、同時に、リスクを厭わない傾向を考慮して、合理性モデルからの逸脱が予測されている。したがって、テーラード抑止は、新たな概念ではなく、旧来の第 2 段階と第 3 段階の抑止理論の未整理の混合物と見なされているのである。

(3) 抑止と敵の行動予測

歴史は、防衛側が敵の行動を誤解し、敵の「不合理」な行動に驚愕するという抑止が失敗した事例を多数提供している。ペイン(Keith Payne)は、日本の真

---

60 Ibid., p. 44.
61 Ibid., p. 11.
62 Ibid.
63 Ibid., p. 24, p. 48.
64 Ibid., p. 56.
65 Sean P. Larkin, The Limits of Tailored Deterrence, *JFQ 63*, 4th 2011, pp. 47-57.
66 Schelling, *Arms and Influence,* p. 75; Jervis, "Deterrence Theory Revisited," pp. 304-305.

珠湾攻撃や朝鮮戦争における中国の参戦、ソ連のキューバへの核ミサイル配備を事例として、敵の行動の予測に際して、米国が逆の結果を予測したと分析している[67]。スタイン(Janet Gross Stein)は、抑止が失敗した事例研究として、1973 年のイスラエルに対するエジプトの奇襲攻撃と 1990 年のイラクのクウェート侵攻を分析している[68]。これらの事例において、防衛側は敵を合理的行為者と仮定して、失敗している。また、抑止失敗の事例は不合理性に起因しているのではなく、合理的意思決定(rational decision)と理にかなった意思決定(reasonable decision)の見分け難い相違に基づいている[69]。主体が合理的であれば、論理的に、その目的に合致した決定を下すことになる。さらに、主体の決定の合理性に問題があっても、その根底には認識の問題がある。外部の観察者が敵の目標や価値を共有せず、或いは理解しない場合、敵の決定は不合理に見え、したがって、予測不可能となる[70]。テーラード抑止は、米国が確度の高いレベルで敵の行動を予測し、理解することを要求している。その目的は、敵の選択肢に対して決定的な影響力を持つ抑止行動を設計するためである。しかしながら、テーラード抑止における仮説は、意思決定の基盤を単純化し過ぎ、また、敵も味方も国民は、期待値の認識に基づく選択を実行する。国民は、個人的嗜好や認知的バイアス等の要因に影響される可能性があり、これらの要因の多くは主体自身にとってさえ謎であることが多い。したがって、行動の評価は困難であり、敵の選択肢の予測は不可能となる[71]。

(4) 抑止／情報／認識の相克

認知心理学では、すべての人々が経験に基づく独特の信条システムやスキームを開発すると仮定され、これらのスキームは複雑な世界には不可欠であり、「指導者の認識方法や内容には、束縛と条件がつきもの」と想定される[72]。例えば、米国が中国の朝鮮戦争参戦の可能性を否定した一方で、毛沢東は米第 8

---

67 Keith B. Payne, "Fallacies of Cold War Deterrence and a New Direction," *Comparative Strategy*, Vol.22, No.5, December 2003, pp.411-412.
68 Janice Gross Stein, "Building Politics into Psychology: The Misperception of Threat," *Political Psychology*, Vol.2, No. 2, 1988, p.249; Janice Gross Stein, "Deterrence and Compellence in the Gulf, 1990-91: A Failed or Impossible Task?" *International Security*, Vol.17, No. 2, Autumn 1992, pp.147-149.
69 Payne, "Fallacies of Cold War Deterrence and a New Direction," pp. 412-413.
70 Ibid.
71 Larkin, "The Limits of Tailored Deterrence," p. 53.
72 Stein, "Building Politics into Psychology," pp. 248-249.

軍(US Eighth Army)を攻撃した。このように、同じ状況が異なって解釈される可能性がある。その理由は、毛沢東が中国は米国に包囲されていると確信―認識―したからである[73]。また、リーダーの認識は試行錯誤に左右され、情報は選択的処理と記憶から解釈される傾向にある[74]。例えば、イラン・イラク戦争でのフセイン(Saddam Hussein)の認識が、米空軍に対する行動予測を狂わせたと言われている[75]。第 3 段階の抑止理論は、決定の重要要素を国内への配慮としているが、ジャーヴィスは、リーダーによる単一の価値次元(例えば、国内政治)に基づく決定―例えば、勝利による名誉の回復―の可能性を指摘している[76]。また、認識には情報評価・イメージに対するバイアス傾向が指摘されている。例えば分析者の思考がミラー・イメージを反映する可能性が指摘されている[77]。ミラー・イメージは帰納的有効性と密接に関連し、特に情報の信頼性が不足している場合、分析者と政策決定者の間にはイメージのブランクが存在し、彼ら独自の能力や計画、意図が投影される[78]。また、情報分析作業は、敵の行動の一貫性を重視しすぎ、他の要因―例えば、偶然の一致や事故、間違い―を過小評価する傾向がある[79]。様々な事象が敵の意図によるものか、偶然の産物であるかの判断は、特に敵の決定予測の分析にとって厄介な問題である。つまり、「敵が首尾一貫性や合理性、目標極大化政策を追求する」という、過大評価に陥るからである[80]。このバイアスと予測不可能性の影響の事例としては、キューバ危機における米国の誤認―ソ連の攻撃用兵器のキューバ配備の否定―がある[81]。意思決定者は動機的バイアス(motivated biases)にも影響を受け、心理的圧力から認識を歪める。そのエラーの原因が恐怖とニーズであり、動機的バイアスは認知バイアスとは異なっている[82]。不安を削減するための希望的判断に応じた情報処理テクニックを発達させる可能性がある[83]。第 3 段階理論は、情報や国

---

73 Payne, “Fallacies of Cold War Deterrence and a New Direction,” p. 411.

74 Stein, “Building Politics into Psychology,” p. 252.

75 Stein, “Deterrence and Compellence in the Gulf, 1990-91,” pp. 174-175.

76 Robert Jervis, “Rational Deterrence: Theory and Evidence,” *World Politics,* Vol.41. No.2, January 1989, pp. 196-197.

77 Richard J. Heuer, Jr., *Psychology of Intelligence Analysis*, Center for the Study of Intelligence, Central Intelligence Agency, 1999, p. 181.

78 Stein, “Building Politics into Psychology,” p. 252.

79 Jervis, “Rational Deterrence,” p. 196.

80 Ibid. p.197.

81 Payne, “Fallacies of Cold War Deterrence and a New Direction,” p.412.

82 Stein, “Building Politics into Psychology,” p. 257; Jervis, “Rational Deterrence,” pp. 196-197.

83 Stein,”Building Politics into Psychology,” p. 216.

際関係分野においては誤認やバイアスが例外ではないことを証明しており、敵の決定を確実に予測するという仮説は、テーラード抑止に重大な欠点があることを示唆している。

４　脅威様相の変化と拒否的抑止

既に詳述してきたが、抑止とは戦略的相互作用であり、行為主体が敵に対して、特定の措置を執るためのコストが増加する可能性を信じさせることによって、その措置の採用を防ぐ行為である。換言すれば、抑止を達成するためには、敵の特定の行動に対するコストや利得に対する敵の認識を行為主体が形成しなければならない。コストの強要とは、一般的に「報復による抑止」や「懲罰による抑止」と呼ばれ、敵が特定の行動方針を採用した場合、敵に受け入れ難いコストを強要すると脅すことによって抑止を達成することを意味している。周知のとおり、冷戦期間中、米国は大量核攻撃で対応すると脅すことによって、ソ連の西欧侵攻を抑止しようとした。アートは、1980 年の「軍事力の存在意義(To What Ends Military Power)」において、軍事力の機能を「防衛(defensive)」「抑止(deterrent)」「強要(compellent)」「威容(swaggering)」に分類し、国家の政策目標達成のために適宜、使い分けることが必要であると主張している。通常、抑止が破綻した場合に防衛機能が使用され、或いは防衛能力を持って抑止を担保する場合があり、現実世界では、これらの機能を明確に分類することが困難である。例えば、「威容は分析が困難な機能であり、抑止は、その達成度を明確に検証できない」とされている。また、抑止と強要について、前者を「軍事力の受動的使用」、後者を「軍事力の能動的使用」と区分しながらも、「これらの概念を理論的に区別することは容易でも、現実に適用することは簡単ではない」として、行為主体の意図や動機、達成度の不明確性を指摘している。アートに拠れば、抑止とは「軍事力の不使用」によって評価され、強要とは「敵を当方の希望する行為に適応させた迅速性と確実性」によって評価される[84]。したがって、抑止の評価には「事象が生起しなかった理由を説明することは、事象が生起した理由を説明するより数段難しい」という評価が成り立つ[85]。

本稿では、これまで、「クロス・ドメイン」の問題と「テロリズムの抑止」

[84] Art, “To What Ends Military Power?” pp. 5-6.
[85] 抑止実証の困難性については、ギャディスも言及している。以下を参照のこと。Gaddis, “Long Peace,” p. 100.

について、検討してきた。サイバー空間や宇宙を含むクロス・ドメインの概念が「抑止」や「エスカレーション」と言った従来の概念を受容するか否かについての議論を概観した。また、テロリズムに関しては、その行為主体が国家ではなく、不特定のグループやネットワークである場合に「受け容れがたいコスト」の意味、或いは報復ではない拒否的戦略の有効性について検討してきた。クロス・ドメインとテロリズムは、ある意味では異なった分野の問題ではあるが、同時に、双方が 21 世紀的課題でもある。また、定義する人によっては、どちらも過去からの戦略問題の 1 つでもある。

双方の分野における「抑止」を考察した場合、第 1 の共通性は、抑止や強要には「脅威とのコミュニケーション」が不可欠であることである。例えば、クロス・ドメインでは、宇宙やサイバー空間での行動基準が不明確であり、同時に、行為主体の行動の意義や影響力が不明(当事者双方にとって)であることが指摘されている。また、既に述べたように、テロリズムを抑止するためには、テロ・ネットワークの実態やテロの目的を把握し、「受け容れがたいコスト」や「拒否すべき利得」を計算し、予測する必要がある。その基盤となる情報は、一定のコミュニケーションから確保されなければならない。

第 2 に、「脅威とのコミュニケーション」は「行為主体共通の認識」を生み出す可能性がある。まさに、クロス・ドメインでは共通のフレームワークの欠如が指摘され、リスクやコスト、或いはエスカレーション、手段や目的に対する共通の枠組みが求められている。テロリズムとの共通のフレームワークは、文化的相違、目的や形態、手段の非対称性から困難な問題として提示される。しかしながら、抑止が戦略的相互作用と定義される限りにおいては、相互認識に関する共通性の確保が不可欠である。

第 3 に、「抑止」や「強要」に関する共通認識が必要とされている。「テーラード抑止」は抑止に関わる行為主体双方の「認識」や「メッセージ」に問題があり、その機能性に疑義がもたれている。反対に、認識やメッセージについての共通認識が確立されれば、ポスト冷戦期の戦略環境において、テーラード抑止が機能することになる。

第 4 に、最も重要な抑止概念の共通的変化は、抑止が「報復的」、或いは「懲罰的」脅威を担保とするものから「拒否的」、或いは「強要的」脅威(若しくは手段)に発展しつつあることである。このことは報復や懲罰を否定するものではなく、抑止には、さらに詳細かつ様々な抑止手段が必要とされ、それが理論上、拒否的抑止、或いは強要と分類されている。したがって、現在及び将来の抑止

概念は報復的･懲罰的戦略や政策だけでなく、拒否的かつ強要的戦略を包含し、また、状況の変化に応じたきめ細かい手段を必要とする。

おわりに

歴史家のマクリスタ(Brian McAllister Linn)は、21 世紀の安全保障環境は、「軍事思想の急激な変化を生み出している」と指摘し、テクノロジー中心の科学的手法からパラダイムシフトが進行し、「複雑性や曖昧性を含んだ人間中心的戦争観」が復活していると述べている。彼は、こうした状況を「知的ルネッサンス」と呼んで、「…戦争に関する認識や展望を検討」し、「歴史家や戦争知識人の役割を再考する必要性」を主張している[86]。本稿は、ポスト冷戦期―或いはポスト冷戦後―における「抑止」問題を再考し、この分野にも知的ルネッサンスが及ぶ可能性について提示しようと試みたものである。紙面の関係から、米国の安全保障コミュニティにおける議論を提示し、分析するに留まっているが、これは筆者の能力に帰するものであり、その責は筆者個人にある。また、依然として、マクリスタの指摘する知的ルネッサンスの概念そのものが仮説の段階であり、また、脅威様相が変化と変容の過程にあって、明確な結論と検証には至らなかったかもしれない。しかしながら、従来、一般的には、抑止の要件が「懲罰的(或いは大量)報復」であったものから、知的な認識や共通性といったインタンジブル(触れられない)なものへと変化しつつあることは、提示し得たものと思われる。同時に、我が国の防衛･安全保障コミュニティにおいても、抑止問題に対する知的挑戦の必要性が求められる状況を示唆したものと自負している。いずれにせよ、「抑止」は、安全保障の 21 世紀的課題として提示されている。

（付記：本稿は、第 64 期高級課程及び第 60 期指揮幕僚課程「政策と戦略」ゼミナールにおける議論から着想を得て、執筆したものである。学生諸君並びに教官諸氏から多大の知見と示唆を受けることができた。末尾ながら感謝申し上げる。）

[86] Brian McAllister Linn, “The US Armed Force’s View of War,” *Daedalus,* Vol.140, No. 3, Summer 2011, p. 2.