「新領域における抑止の在り方」事業　最終報告書

War 3.0: 激変する戦争
―新領域（宇宙・サイバー）が迫る抑止の深化―

2024年3月

笹川平和財団
SASAKAWA PEACE FOUNDATION
Think, Do, and Innovate-Tank

安全保障研究グループ

目次

はしがき

本報告書は、笹川平和財団安全保障研究グループにおいて、2021～22年度に実施した「新領域における抑止の在り方」事業の最終報告書である。

現代の戦争において、陸海空の伝統的な三領域だけでなく、宇宙・サイバー領域を含む「新領域」の重要性が増している。軍事作戦の遂行においてこれらの領域への依存が深まり、新領域における優位の喪失が致命的なものと見なされつつあるため、現代の軍事作戦は必然的に宇宙及びサイバー領域を含めた多領域作戦（MDO: Multi-Domain Operation）として実施されることが前提となっている。同時に、新領域における作戦を伴う戦争において、抑止（またはエスカレーション管理）をどのように実現するかという課題にも関心が集まっている。

こうした背景を踏まえ、同グループは抑止及び宇宙・サイバー領域の専門家９名による「新領域抑止研究会」を立ち上げ、二年に渡る活動を通じて「新領域における抑止の在り方」に係る様々な検討を行った。本報告書はその研究成果の一環である。

報告書では、「戦争3.0」という概念を用いて現代の戦争の性質を追及し、宇宙・サイバー領域を含む新領域の重要性の増大に伴い、抑止を巡る諸課題がどのように変化していくかを検討している。具体的には、二回に渡るシナリオゲーム（巻末資料参照）の実施を通じて、新領域の影響が特に武力攻撃未満のグレーゾーン段階で顕著になることを明らかにし、中でも「グレーゾーン対処の中心となる法執行機関に対する新領域の作用」と「グレーゾーンから武力紛争へとエスカレートする過程で新領域が加わることでのエスカレーション・ダイナミクスへの影響」について注目すべきことを強調している。

その上で、本報告書は多様な視点からの「新領域における抑止の在り方」への分析を試みている。その論点は抑止と新領域の概念整理、宇宙領域における抑止の在り方、サイバー領域における抑止の在り方、台湾有事における日米のサイバー作戦上の課題、エア＆スペースパワーの進化と抑止、と多岐に渡る。

現代の軍事作戦における新領域の重要性を強調する議論は多いが、新領域と抑止（またはエスカレーション管理）の関連性について正面から取り上げた議論はそれほど多くないように感じられる。台湾有事を含めて「大国間の競争」の最前線に立つ我が国として、本報告書が「新領域における抑止の在り方」を巡る議論に少なからず貢献できれば、それに勝る喜びはない。

公益財団法人　笹川平和財団
安全保障研究グループ主任研究員　福田 潤一

「新領域抑止研究会」メンバー（敬称略）

いずれも**2023年３月末の**執筆時点の肩書

（*は本報告書の執筆者）

（座長）

高橋杉雄*　防衛省防衛研究所政策研究部防衛政策研究室長

（委員）

大澤　淳　中曽根康弘世界平和研究所主任研究員

杉山公俊*　航空自衛隊幹部学校航空研究センター長 １等空佐

時藤和夫*　㈱日立製作所 ディフェンスシステム事業部顧問・元航空自衛隊北部航空方面隊副司令官

中谷寛士*　航空自衛隊幹部学校航空研究センター研究員 ３等空佐

福島康仁*　防衛省防衛研究所政策研究部グローバル安全保障研究室主任研究官

森　　聡*　慶応義塾大学法学部教授

（オブザーバー）

秋田浩之　日本経済新聞コメンテーター

（委員兼事務局長）

福田潤一*　笹川平和財団安全保障グループ主任研究員

各章概要

第一章　戦争3.0の時代：新領域による「抑止」の変化？（高橋杉雄）

戦争の形態は歴史とともに変わっていく。『戦争論』を著したクラウゼヴィッツの考察の前提となるのは、国民・国家・軍隊の３者が明確に区別できること（「三位一体戦争観」）であった（戦争1.0）。しかし、この前提が崩れれば戦争の性格もまた変わる。

冷戦終結後に大きな課題と見なされたのはテロ組織への対処であり、イスラム過激主義に対する協調的な対応が進められた。これは国家対非国家主体の対決ということもでき、「三位一体戦争観」とは異なる図式での紛争（戦争2.0）であった。しかし、2010年前後から、再び大国間の対立が深刻化し、ロシア・ウクライナ戦争のように、大国が関与する戦争までが現実に行われている。

これをどう見るべきか。本研究プロジェクトにおいては、戦争についてまた新たな概念（戦争3.0）を創出する必要があるとの結論に至った。その理由は、グローバリゼーションの進展を受けて戦争が軍事力以外の次元でも戦われていること、国家による軍事力の独占も崩れつつあること、の２点である。その上で、本研究プロジェクトは、宇宙・サイバーといったいわゆる「新領域」の重要性の増大に伴って、抑止を巡る諸問題がどのように変化していくかをテーマとしている。

議論を進める前提として、まず、「何を」抑止するかの文脈で言えば、新領域を巡る抑止において考えるべき課題は、一義的には「大国間の競争」復活を背景とした、国家由来の脅威の抑止である。

次に、現在の「大国間の競争」では、冷戦期のように国家間の大規模戦争のみに備えれば良いということに留まらず、グレーゾーンにおける現状変革の試みやハイブリッド戦のような、正規戦の形態を取らない形での現状変革の試みにも備える必要がある。グレーゾーン事態／ハイブリッド戦と大規模紛争では宇宙・サイバー領域の活用法が異なるため、新領域を含めた抑止概念を構築する場合には、これら紛争形態を視野に含めていく必要がある。

更に、戦略的文脈が重要である。戦略とは「目的」「方法」「手段」の組み合わせであるが、「方法」と「手段」は「目的」達成のためのロードマップ構成の意義を持つ。すなわち、戦略上の目的（中国やロシアにとっての台湾やウクライナなど）が物理空間に存在している以上、宇宙やサイバーといった要素は「目的」そのものになることはなく、むしろこの「目的」達成のための「方法」や「手段」となる。その意味で、新領域の「力」の中心にあるのは、陸海空軍力のような物理的能力を増幅する作用や、相手の物理的能力の効果を低減する作用である。

なお、軍事分野における新領域の特徴は、物理的な破壊を伴わない攻撃が可能なことである。この点は、特にグレーゾーンにおいて重要な意味を持つ可能性がある。１つの課題は、グレーゾーンにおける対処の中心となる法執行機関に対する新領域の作用である。例えば、尖閣諸島周辺で中国が大規模なGPSジャミングを行った場合、警備にあたる海上保安庁の巡視船が相手の行動に対して適切に対応するのが難しくなる。また、通信衛星や地上施設に対するジャミングを通じて

中央とのコミュニケーションを断つことができれば、やはり中国側が優位に立つことができる。

２つ目の課題は、グレーゾーンから武力紛争へとエスカレーションするプロセスを想定したとき、新領域が加わることでエスカレーションのダイナミクスがどう変わるか、である。この点については以下の仮説が成立しうる。まず、グレーゾーンにおける非物理的使用に限って言えば、エスカレーションは容易に発生する可能性が高い。しかし新領域であっても、物理的攻撃を行う場合には、現状打破側としてもより大きなリスクを覚悟する必要がある。また、マルウェアは一度使用すればその存在が発覚し、駆除されてしまう可能性が高い。そのため、仕掛けられたマルウェアは最大の効果を発揮するタイミングで発動させる形となり、それは在来領域で決定的な行動を取るタイミングと予想される。

よって、新領域の物理的使用へのエスカレーションは、在来領域のエスカレーションの効果を最大化させるために、それと連動して行われる可能性が高い。ひとたびグレーゾーンから紛争へとエスカレーションさせることを一方が決定した段階で、新領域を含めたエスカレーションが急激に発生することが考えられる。

第二章　抑止と新領域の概念整理（福田潤一）

「新領域における抑止の在り方」を検討するために、本章では「抑止」及び「新領域」についての概念整理を行う。

まず、抑止には「相手が取る可能性のある行動のコストやリスクが、その利益を上回るように相手を説得すること」などの多数の定義が存在するが、根本的に重要な要素としては、相手の合理性や、抑止実現に足る能力としての抑止力、相手に対する伝達、伝達の信頼性などが挙げられる。また、抑止には狭い抑止と広い抑止、中央抑止と拡大抑止、拒否的抑止と懲罰的抑止、一般抑止と緊急抑止などの区別も存在する。

抑止を困難にする要素としては、次の五つが挙げられる。まず、相手が合理的な存在でないこと。次に、相手も合理的存在であるが、戦略文化その他の違いにより、コストやリスク判断の前提が異なることを読み違えてしまう可能性。第三に、国家の単一合理性仮定という誤った前提に依拠してしまう可能性。第四に、国際関係における不確実性や、国家が自身の選好を偽装する動機等によって、信頼性の高い伝達が困難となる可能性。最後に、新技術の登場や非国家主体の関与等が抑止状況を複雑化する可能性、である。

抑止に密接な概念としてのエスカレーションは、「参加主体の一つ以上が重要だと考える閾値を越えるような紛争の強度または範囲の拡大」と定義される。エスカレーション管理は抑止の延長線上にあるが、単にエスカレーションの緩和を目指すだけのものではなく、エスカレーション優位を求めた意図的なエスカレーションが追求される場合もあり得る。エスカレーションには垂直的／水平的／合成的の三種類があるが、特に垂直的閾値を積み上げたものがエスカレーション・ラダーである。このエスカレーション・ラダーの思考を今日の戦略環境にどう適用するかが課題であるが、近年の作戦領域の多様化が、この概念に対する重大な挑戦となっている。

なお、抑止に密接に関連するが、抑止とは区別される概念としては、強要、防衛、現状、諫止、戦略的安定性、安定性と不安定性のパラドックス、安心供与、軍備管理・信頼醸成・行動規範形成などを挙げることができる。

新領域における抑止について、まず領域には複数の定義があるが、世界の多くの軍事組織では、陸海空の三領域を既存もしくは伝統領域として捉え、「宇宙」と「サイバー（及び電磁）」領域を軍事作戦で優位を得るために今や死活的な重要性を持つようになった新領域として捉える傾向が強い。ただし、新領域の概念は常に拡張余地を残しており、例えばサイバー領域と重複するがそれに限られるものではない「認知」領域という考え方も採られている。

新領域における抑止には「領域内」抑止と「領域横断的」抑止の区別がある。前者はその領域の内部における攻撃をどう抑止するかに係る問題であり、後者はほかの領域と跨る形での抑止をどう実現するかに係る問題である。前者は例えば領域内でレジリエンスの向上に努めて、拒否的抑止ないしは防衛の取り組みを図る上で効果的であるが、とりわけ戦略レベルにおいては、あらゆる抑止を領域横断的抑止として捉えるべきと言っても過言ではない。

新領域の特性として、宇宙・サイバーの両領域に共通するのは以下の点である。第一に、状況把握が困難である。第二に、防御も困難である。第三に、攻撃の閾値が低い。第四に、多様なアクターが混在している。第五に、行動規範が欠落している。このような事情により、新領域では防衛に対して攻撃優位となりやすく、抑止破綻が生じやすい特性がある。

こうした特性を持つ新領域において、抑止の文脈で想定される対応策は次の四つである。第一に、状況把握能力の向上である。第二に、（拒否的抑止としての）レジリエンスの向上である。第三に、（拒否的ないし懲罰的抑止としての）攻撃（ないし反撃）能力の保有である。第四に、抑止ではないが、軍備管理や信頼醸成、行動規範形成等の取り組みを進めることである。

抑止はしばしば破綻するものであり、新領域における抑止の実現はますます困難である。しかし戦争3.0の時代に直面する我々は、そうした困難に立ち向かわねばならない時代に生きている。

第三章　宇宙における抑止の追求とレジリエンス・防護の重要性（福島康仁）

宇宙抑止には「抑止における宇宙（space in deterrence）」と「宇宙における抑止（deterrence in space）」の２つの側面が存在する。前者は自国などへの攻撃を抑止する際に宇宙システムや攻勢的対宇宙能力が果たす役割を指し、後者は宇宙システムに対する攻撃を抑止することを意味する。本稿では「宇宙における抑止」を中心として宇宙と抑止の関係性を考察する。

冷戦期における宇宙と抑止の関係を振り返ると、当時は、宇宙システムは核抑止力の不可欠な構成要素であった。他方で、通常戦力を用いた抑止（通常抑止）への貢献は限定的であった。このため、宇宙システムに対する攻撃の抑止も、基本的には核抑止と一体であった。

しかし、2010年代に入ると本格的変化が生じ始めた。通常抑止における宇宙システムの役割が世界的に拡大し、米国のみならずフランスやロシア、中国などがこの取り組みを進めてきた。その中で、「宇宙における抑止」の側面において、宇宙システムへの攻撃を抑止する必要性が高まっている。これは攻勢的対宇宙能力の研究・開発、実験、配備、使用が顕著になってきたためである。

その具体例としてのロシア・ウクライナ戦争における宇宙抑止の様相を見ると、まず「抑止における宇宙」の文脈では、宇宙システムは（米国などによる）核戦力の指揮・統制・通信（NC3）に係る機能を提供することで、核抑止に貢献している。また、（NATO諸国をはじめとする）通常戦力のより効果的な運用を可能にすることで、ロシアに対する抑止に貢献してもい

る。ただし、自明ながら宇宙システムのみで抑止力を発揮しているわけではない。

「宇宙における抑止」の文脈で見ると、ウクライナが使用する宇宙システムに対するロシアのサイバー攻撃や電子戦兵器を用いた攻撃を抑止することはできなかった。ダウンリンク信号を対象とした電子攻撃やユーザー端末へのサイバー攻撃は、比較的影響が局所的であることから攻撃の敷居が高いとは言い難い。

一方で、ロシアによる宇宙セグメント（衛星）への攻撃は確認されていない。１つには懲罰的抑止が効果を発揮しており、ロシアが衛星攻撃を躊躇している可能性がある。２つ目の可能性は拒否的抑止が機能しているというものである。尤も、対露抑止が効いているのではなく、単にロシアには衛星を攻撃するつもりがない、あるいは衛星への攻撃は起きているが公表されていないという可能性もある。今後ロシアがウクライナの作戦に使用されている他国企業の衛星を破壊したとしても驚きはない。

いかにして「宇宙における抑止」を追求すべきか。１つは能力の保有と誇示である。宇宙システムのレジリエンスや防護に関わる能力を保有するとともに、そうした能力を有していることを対外的に示すことは、拒否的抑止に貢献する。更に、懲罰的抑止を追求するにあたって、報復能力を使用する決意を前もって敵対者に伝達しておかなければならない。３つ目は領域横断（クロスドメイン）で抑止を追求することである。例えば懲罰的抑止の場合、衛星に対する攻撃に対して衛星攻撃で報復するだけでなく、陸海空やサイバー空間を通じた報復も行う決意を示すことが抑止力の向上に資する可能性がある。

ただし、抑止に限界があることにも留意が必要である。抑止に失敗して宇宙システムが攻撃を受けたとしても宇宙利用を継続できるように宇宙システムのレジリエンスと防護の向上に取り組むことも重要である。米宇宙軍によれば、レジリエンスを確保する措置として「disaggregation」、「distribution」、「diversification」、「proliferation」、「deception」、また、防護措置として電磁スペクトラム作戦、移動・マヌーバー、硬化、サイバーセキュリティがある。

日本の防衛において宇宙システムが果たす役割が拡大しており、宇宙システムに対する攻撃の抑止を追求することは日本にとっても重要な課題となっている。同時に、宇宙システムのレジリエンスと防護に日本も取り組んでいかなければならない。

第四章　サイバー空間における抑止の在り方と課題（時藤和夫）

本章ではサイバー空間と抑止について考察し、その特徴と実例等から抑止の在り方と課題について述べる。まず、サイバー空間の特徴としては、管理が非中央集権的で匿名性から民間・軍事の区別が混然とし、様々なサイバー攻撃が常時行われることが指摘できる。また、技術の発展により、クローズドなシステムが安全というこれまでの認識では攻撃を完全防護できない状況にもなってきた。

サイバー攻撃には様々な種類があり、常に進化している。こうした攻撃の各段階を「偵察」「侵入」「マルウェアの注入」「痕跡除去」のようにキルチェーンで捉える試みも登場しており、対策に有効活用できる。

サイバー空間における攻防の比較を見ると、まず（中口等の）現状変革側の比較優位性として、「民主的コントロールに基づく法的制約や道義的制約が少ない」「情報操作による優位性があ

る」「サイバー攻撃の特性を利用し易い」等が挙げられる。他方で、（日米欧等の）「現状維持側の比較優位性としては、「真実の公表」「トレースバック技術の発達」「インターネット重要機能の独占」等が挙げられる。更に、どちらの優位性となるか不確実性の高いものとして、「人工知能（AI）技術の活用」「サプライチェーンの再構築」を挙げることもできる。

ウクライナ侵攻におけるサイバー戦について考察すると、サイバー戦は非対称的アプローチに適合している。ロシアはこの非対称的優位の観点でウクライナにサイバー攻撃を行ったが、ウクライナ側が適切な対策を講じたために、サイバー戦の非対称の効果を最大限発揮できたとは言い難かった。また、ロシアはサイバー攻撃をハイブリッド戦や情報戦の手段としても活用した。この点からは、サイバー戦は武力侵攻未満の戦略・作戦環境を巧妙に作為し、紛争の閾値を操作するためのツールになるが、紛争時には軍事能力に寄与するためのツールへと変化することが指摘できる。

わが国（日本）はこれまでサイバー攻撃からの防護を主に実施してきたが、昨今、能動的な防御の必要性が増している。2022年末の戦略３文書は領域横断作戦におけるサイバー戦能力強化の方向性を打ち出した。具体的には、情報共有の促進、能動的サイバー防御、サイバー空間における能力強化、サイバー空間の利用を妨げる能力の確保、サイバー空間における法的整備の促進、人材育成が強調されている。

サイバー空間における抑止力発揮の方向性として、サイバー攻撃を事前に察知し、対処によって攻撃阻止すること、またサイバー攻撃を受けても早期にこれを発見し、対処し、侵入されたとしてもシステムは機能を発揮し続けるレジリエンスの確保が拒否的抑止につながる。また、反撃に関しては、サイバー空間に限らずキネティックを含めたほかの領域、あるいは外交・経済等様々な領域と密接に連携して行うことで相手にコストを課すことが有効であり、懲罰的抑止につながる。こうした能力を相手に伝達する手段も重要である。

サイバー空間は目に見える形で劇的な変化を遂げていることにも留意する必要があり、クラウドコンピューティングの発展、多様化するネットワーク環境、量子技術の実用化、認知の領域との関わり、AI技術の実用化の変化等に注目していく必要がある。

サイバー空間における抑止の課題として、本章は以下の五つを掲げる。①サイバー攻撃に対しては、拒否的抑止を強化し、レジリエンス及び回復力を保持することで、システムの目的である機能を確保し、実践力を強化する。②懲罰的抑止については、能動的サイバー防御の観点から、攻撃能力の構築及び法的根拠の整備を行い、ガバナンスの効いた実効的な能力を確保する。③要員養成を含めたサイバー空間能力強化における体制整備については、サイバー戦力強化の構想と発信が必要である。④官民連携を含めたサイバー空間での優位性の確保が重要である。⑤サイバー攻撃に対して、外交的な調査、制裁及び起訴などの統合的な対処体制の構築が必要である。

第五章　台湾有事における日米のサイバー作戦上の課題（森聡）

本章は台湾有事が発生した際に、日本と米国がいかなるサイバー作戦上の役割を担い、任務にあたらなければならないのか、日本が担うべきサイバー領域における任務にはいかなる能力が必要で、その開発面での課題とは何か、について検討する。中国が台湾の支配ないし尖閣諸島の制圧という現状変革を戦略目標とし、日米は武力による現状変革の拒否を目標とすることを前提と

すれば、もし抑止が破れる場合には日米共同作戦が必要となる。この作戦は、中国の「勝利の方程式（TOV: Theory of Victory）」に必要な能力と意思を削ぐ攻勢作戦と、日米が中国の戦略目標の拒否を達成するために必要な能力と意思を守る防勢作戦の両面的性格を有する。この前提で、日米のサイバー作戦上の役割と能力及び、能力に関する開発課題を検討する。

まず、中国のTOVに必要な能力と意思を削ぐ攻勢作戦の文脈では、能力を削ぐサイバー作戦として、中国人民解放軍のOODA（観察、状況判断、決断、行動）ループの各機能的局面を標的にした対兵力サイバー攻撃任務が考えられる。同時に、攻撃対象を対兵力から対価値へとエスカレートせざるを得ない局面では、対価値サイバー攻撃任務が大きな作戦上の役割を担う可能性もあろう。また、意思を削ぐサイバー作戦としては、中国の最高意思決定者に武力による現状変革を断念、少なくとも一時停止（先送り）させることが戦略目標となるが、問題は意思決定者がどのような指標に着目して対応を判断するかである。一般的な予測は困難であるが、場合によっては世論の誘導・分断を目的とした対価値サイバー攻撃任務が大きな意味を持つことが考えられる。

次に、日米が中国の戦略目標の拒否を達成するために必要な能力と意思を守る防勢作戦の文脈では、中国による日米の能力に対する攻撃への防御として、日米の対艦攻撃能力を妨げにくる人民解放軍を対象とした対兵力サイバー攻撃任務が必要となる。同時に、民間企業のネットワークに対する中国のサイバー攻撃を防ぐ努力も必要となろう。また中国による日米の意思を削ぐ攻撃への防御としては、中国が情報作戦を通じて日米両国で台湾有事への介入に反対する世論の形成を進めてくる可能性があり、いわゆる認知領域における情報作戦にいかに対抗すべきかが問題となろう。

以上を前提に、各種の作戦上の日米の任務と課題を整理すると、以下になる。日米の現有能力などに照らせば、サイバー空間における攻勢作戦を米軍、防勢作戦を自衛隊が担うというのが、おそらく基本的な役割分担として順当であろう。

まず、米国による攻勢作戦上の任務として、中国軍のOODAループに対する対兵力サイバー攻撃任務、中国の民間・社会基盤に対する対価値サイバー攻撃任務、中国国民の認知に対する情報作戦を含む対認知領域サイバー攻撃任務が挙げられる。次に、日本による防勢作戦上の任務と能力としては、国防／政府省庁・法執行機関／民間のそれぞれのネットワーク防衛任務、中国が日米の一般市民の認知領域を標的として展開する情報作戦阻止のための認知領域防衛任務が挙げられる。

そして、前者に関連して日本が獲得すべき能力は、サイバー状況把握とサイバー・レジリエンス（強靭性）、将来的にはサイバー精密反撃能力であろう。また、後者に関しては平素から政府が国民の信頼を獲得する努力や、ディスインフォメーションへの対抗措置としての、包括的で自動化されたデータ鑑識の分析を行うプラットフォームが必要となろう。

第六章　エア＆スペースパワーの進化と抑止（杉山公俊・中谷寛士）

本章はエア＆スペースパワーを例として取り上げ、その特性と進化を踏まえながら、新領域での優勢がどのように空の戦いや抑止に寄与するかについて議論する。

エアパワーの特性として挙げられるのは、即応性・機動性、優れたISR（情報収集、警戒監視、偵察）能力、長距離打撃力などである。他方で戦闘機などに代表されるエアパワーは、地上にお

いて脆弱で、気象条件による活動の制約を受け易く、一部機能の喪失によって戦力発揮を大幅に低下させるという脆弱性も有している。

こうした特性を背景に、今日、航空優勢の概念が揺らぎつつある。航空優勢とは、我の航空戦力が優勢であり、敵から大きな妨害を受けることなく我の様々な作戦を遂行できる状態にあることを言うが、宇宙・サイバー ・電磁波領域の活用推進により、いわゆるキルチェーンまたはF2T2EAと呼ばれる一連の流れに大きな影響が生じつつある。すなわち、宇宙・サイバー ・電磁波の各領域は、既存領域での戦いに密接に関係し、戦力を大きく増幅する装置（フォースマルチプライヤー）としての役割を果たす一方で、これらの能力を妨害することで相手の戦力発揮を大幅に低下させることも可能であるため、これら領域での優勢が従来領域での航空優勢を巡る空の戦いに大きな影響を及ぼす。結果、従来の「航空優勢獲得」の概念を新領域での優勢も含めたものにするなどの見直しが必要と考えられる。

日本のエア＆スペースパワーは抑止に対してどのような貢献が可能か。まずエアパワーに焦点を当てると、一つ目に重要なのは日本周辺空域の警戒監視であり、二つ目に事態エスカレート時の防空作戦実施、三つ目にミサイル防衛能力（積極防衛）によるミサイル無力化、四つ目に自衛隊基地の強靭化、抗堪化、五つ目に日米の基地の相互使用による在地航空戦力残存の可能性向上といった方策がある。更には海洋を渡ってくる相手を拒否する能力も重要になる。こうした努力を通じて日米が根気強く防御に徹する姿勢を示し、攻撃側の短期間での目的達成が拒否されると認識させることが抑止的な観点で重要である。

また、戦略的高地としての高所からの「目」を提供するエア＆スペースパワーの特徴も無視できない。空や宇宙は戦況全体を見渡せる現代の戦略的高地であり、地域諸国が連携し、それぞれが持つ現地の最新情報を共有・統合し、インド太平洋における共通作戦図（COP）を作り上げることが重要である。これを通じて、相手に自らの違法行為や軍事行動が常に誰かに見られていると認識させることにより不安感や猜疑心を抱かせ、状況次第では相手の行動や悪事を共同で国際社会に公表することによって、相手の動きを先行的にけん制していくことが、抑止に繋がる。無論、監視の目だけでは不十分であるので、早期に異常を発見・探知した後に、違法行為を罰する行動も必要となるだろう。

多国間連携、特に演習や訓練も重要である。歴史的に共同作戦能力向上を目的とした演習は、参加国の緊密性を示すだけでなく、その他の能力的優位を相殺する潜在的可能性から抑止効果があるとの分析もある。日本としても、米国とは無論、米国以外の国々、特に豪州との演習に力を入れている。更にQUADやAUKUS諸国との多国間連携の一環として、共通のアセットを保有したり、燃料や弾薬を相互に代替可能なものにできれば、継戦能力向上にも繋がる。宇宙領域に関しては、ホステッド・ペイロード協力を日米だけでなく、さらなる地域諸国等に拡大できれば、抑止力を高めることが可能であろう。重要なことは、戦略構想段階から同盟国および可能であれば同志国と連携することが、相手に対する実践的な抑止連携ともなるということである。

エア＆スペースパワーのみを駆使した抑止は間接的な役割を果たすに過ぎず、抑止の一要素でしかないことは事実であるが、日本としては、エア＆スペースパワーを駆使して、地域の安定を脅かす国を日本独自の力だけでなく同盟国、同志国とともにけん制していくことが日々重要になっており、その責務を果たすことが地域の安定へと間接的に繋がるだろう。

第一章　戦争3.0の時代：新領域による「抑止」の変化？

高橋杉雄

1．戦争3.0の時代の到来

戦争の形態は歴史とともに変わっていく。19世紀にプロシアの軍人であったC・クラウゼヴィッツ（Carl von Clausewitz）が著した『戦争論[1]』は、その後の戦争を巡る思索のベースラインを設定したが、これは、フランス革命に端を発する「国民軍」の出現により、それまで王朝同士で戦われていた戦争が、国民同士の戦争に変化していく時代的背景の中で、戦争という現象を考察しようとしたものであった。戦争とは国家同士が武力を用いて争う行為であるが、社会と国家との関係や、国際システムにおける国家のありようが時代とともに変わっていくために、戦争事態も変化していく。現代的な文脈で、クラウゼヴィッツの考察の重要な部分は、戦争を政治の延長と捉えたこと、すなわち国家の政策の手段として軍事力が用いられているとする部分だが、この部分の前提となるのは、M・クレフェルト（Martin van Creveld）が指摘するように、国民・国家・軍隊の３者が明確に区別できることである。クレフェルトはこれを「三位一体戦争観」と名付けたが[2]、この前提が崩れれば、戦争の性格もまた変わってくる。

そうした議論が活発に行われたのは冷戦終結後であった。米ソ２大超大国が、巨大な核戦力をお互い突きつけ合い、核戦争による人類滅亡の脅威と同居しなければならなかった冷戦期であったが、その根底にあったものは、文字通り三位一体戦争観と言うにふさわしい、国民・国家・軍隊を明確に区別し合った国家同士のイデオロギー対立であった。当時、西側諸国の間でこそ経済的相互依存は進んだが、東西間では経済的な相互依存もほとんど進まなかった。それが冷戦が終結したことで、旧東側を西側の相互依存に組み込んでいく形で「グローバリゼーション」が展開する。更に、冷戦終結が東側陣営の崩壊によってもたらされたことで、むしろ大国間の協調が進展していくと考えられるようになった時代があった。例えば、「協調的安全保障[3]」のような議論が登場し、大国間が協調してグローバルな安全保障上の課題に取り組んでいくことが目指されもしたのである。

この時期に大きな課題と見なされたのはテロ組織への対処であった。特に2001年の9.11テロ事件をきっかけとして、イスラム過激主義に対する協調的な対応が進められた。これは国家対非国家主体の対決ということもできる。そのため、「三位一体戦争観」とは異なる図式での紛争でもあった。この時期に、戦争が変わっていくとの議論が生まれていく。例えば「第４世代戦争」というような概念[4]が当時提示されたが、これは、非国家主体においては、軍事力を国家が独占するという「三位一体戦争観」の前提が崩れており、戦闘員と非戦闘員の区別が曖昧であり、また平時と有事の区別も曖昧になっていると言う形で、それまでとは違う形での戦争が生まれつつあ

1　カール・フォン・クラウゼヴィッツ著、清水多吉訳『戦争論　上下』中央公論新社、2001年。
2　Martin van Creveld, *The Transformation of War,* New York: The Free Press, 1991, pp. 35-42.
3　Ashton B. Carter, William J. Perry, and John D. Steinbruner, *A New Concept of Cooperative Security,* Washington D.C.: Brookings Institution Press, 1992.
4　Thomas X. Hammes, *The Sling and the Stone: On War in the 21st Century,* Voyageur Press, 2004.

るという考え方によるものであった。

しかし、2010年前後から、再び大国間の対立が深刻化していく。中国は南シナ海、東シナ海で一方的、高圧的な行動を繰り返し、周辺諸国や米国との関係を悪化させた。ロシアは2014年にクリミア半島を一方的に併合し、やはり米欧との関係を悪化させた。そうした形で、「大国間の競争」が復活したという見方が広がっていく中、アジアにおいては台湾海峡有事が懸念されるようになり、ヨーロッパではロシア・ウクライナ戦争が2022年２月に始まった[5]。

このような形で、いまでは、「大国間の競争」が復活したばかりか、大国が関与する戦争までもが現実に行われている。果たしてこれは、クラウゼヴィッツ的な「三位一体戦争観」に基づく戦争の単純な復活として捉えるべきだろうか。本研究プロジェクトにおいては、これはかつての戦争観の単純な復活ではなく、戦争についてまた新たな概念を創出していく必要があるとの結論に至った。

理由は大きく２つある。まず１つは、ロシア・ウクライナ戦争が、軍事力以外の次元でも戦われていることである。戦略論において、軍事力以外の手段の重要性を強調する言葉として、「DIME」というものがある。Dはdiplomacy、Iはintelligence、Mがmilitary、Eがeconomyである。ロシア・ウクライナ戦争においては、開戦後も、このDIMEすべてが大きな役割を果たしている。まず外交だが、開戦後しばらく、2022年４月はじめまでロシアとウクライナの間で停戦協議が行われていたのはもちろんだが、それだけではなく、ウクライナはアメリカやヨーロッパ諸国の支持を得、ロシアに圧力をかけるための外交を展開している。ロシアもまた、中国の支持を得たり、旧ソ連諸国のへの影響力を強めるための外交や、インドを含めグローバルサウスと呼ばれる国々との関係をマネージするための外交を展開している。情報も、同じように国際社会の理解を得るための情報キャンペーンを双方が行っているし、ウクライナは米欧からロシアの情報を得ながら作戦を行っている。軍事は言うまでもないが、経済においても、対ロシア経済制裁や、ロシア側からのエネルギー供給を巡る駆け引きなど、やはり戦略上の手段として経済力も利用されている。

このように、DIMEすべてがかかわってくるような戦争は、冷戦後の紛争にはあまり見られなかった。特に西側の戦略コミュニティにおいては、「圧倒的な軍事力を持つ米軍」の地域への軍事介入に関心が偏ったこともあり、紛争における軍事力以外の側面といっても、それは紛争後の地域の復興とそのための安定化作戦といったものを意味していた。また、クラウゼヴィッツは、戦争とは政治の延長であると論じたが、ある意味戦争が始まると軍事力が手段の中心となる、しかしそれは破壊を自己目的化するのではなく、政治的な目的に沿って使用されなければならない、という考え方を示したものと理解されてきた。

ところが、ロシア・ウクライナ戦争で改めて示されたのは、戦争が始まったとしても、DIMEのうちMを除く３要素が役割を失うわけではないことであった。役割の低下さえしていない。こうした手段も、戦争目的を達成するために、軍事力と同じように重要性を持つということであった。その重要な背景として、グローバリゼーションの進展がある。ある意味、この戦争はグローバリゼーションが進んだ時代における初めての大国間の戦争であるとも言える（ロシアはもとよ

5　この戦争を巡る分析については、高橋杉雄編著『ウクライナ戦争はなぜ終わらないのか：デジタル時代の総力戦』文藝春秋、2023年を参照。

り、ウクライナも旧ソ連第２位の軍事力を持つ国であるという意味で大国と言える）。経済的相互依存の網は交戦国同士を組み込んでいるし、グローバルサウスと呼ばれる国々の影響力もまたグローバリゼーションの進展に伴う経済成長によるものであり、また穀物やエネルギー供給問題のように、そうした国々がロシア・ウクライナ戦争の影響を受けるのも、グローバリゼーションの結果である。

更に、国家による軍事力の独占も崩れつつある。本研究プロジェクトで分析するように、新領域において、国家はもはや民間セクターの協力なしに軍事力を運営できなくなっている。そう考えていくと、もはやクラウゼヴィッツ的戦争観をそのまま当てはめられる状況ではない。そしてこれもまた、グローバリゼーションの一つの帰結でもある。

このように、ロシア・ウクライナ戦争は、戦争が大きく変わりつつあることを示している。本研究プロジェクトでは、クラウゼヴィッツの考察から冷戦までの時代を「戦争1.0」、「テロとの戦い」が中心にあった時代を「戦争2.0」と考えた上で、新たな戦争概念を必要としているという問題意識に立ち、新領域と抑止との関係を検討した。そして、グローバリゼーションを背景として、戦争が新たに質的に変化していると考え、「戦争3.0」という概念を手がかりに考えていくこととした。

ロシア・ウクライナ戦争が示している戦争の変化は、それがグローバリゼーションを背景としている以上、おそらく構造的なもので、現在の重要なトレンドだと考えるべきであろう。だとすれば、台湾海峡有事や朝鮮半島有事も同じような性格を持つ可能性が高い。そうなると、日本としてもこの新たな戦争概念を理解し、消化していかなければならないのである。本章ではまず、宇宙やサイバーと言われる新領域の持つ特徴を総論的に整理しておく。

2. 新領域を巡る戦略的前提

（１）戦略環境

ここではまず、議論を進めていく上での前提を３点ほど整理しておきたい。第１は戦略環境についてである。抑止についての議論を行うとは、「何を」「何によって」抑止するかを考えると言うことでもある。本研究プロジェクトは、宇宙・サイバーといったいわゆる「新領域」の重要性の増大に伴って、抑止を巡る諸問題がどのように変化していくか、あるいは変化していかないかをテーマとしている。言い換えれば、「新領域」によって、「何を」抑止するのか（＝目的）と「何によって」抑止するのか（＝手段）がどう変わっていくかを考えていくということと言えよう。新領域とは、新たな技術であるから、これはある意味で新領域という形で顕在化した技術的トレンドの変化によって、抑止を取り巻く問題の位相がどう変わっていくかを考えていくということでもある。

ただし、抑止とは国家の戦略を支える概念であり、技術は国家の戦略の手段でしかない。、戦略環境そのものが変われば、脅威の性質が変わる。つまり、「何を」抑止するかが変わる。この変化は、技術的トレンドよりもより根本的なレベルで起こる変化である。そのことは簡単に現代史を振り返れば明らかであろう。抑止すべき対象は、冷戦期であれば米ソの核戦争であった。すなわち国家間の大規模戦争である。しかし、冷戦が終結し、大国間の関係が安定した1990年代から21世紀初頭にかけては、特に欧米では、抑止の対象は国家間戦争とは見なされないようになった。2001年９月11日の米国での同時多発テロの影響を受けて、イスラム過激主義などによるテロ

をどのように抑止するかこそが重要な問題であると考えられるようになったのである。

大国間の核使用を伴う大規模戦争を抑止するのと、非国家主体であるテロを抑止するのとでは、取るべき方策は大きく異なる。その意味で、抑止の有り様を考える上で最初に考えなければならないのは、戦略的前提として、「何を」抑止しなければならないかである。この点について鍵になるのは、近年、中国の台頭とロシアの復活、米中・米露関係の悪化、中露関係の強化といった要因によって、「大国間の競争」が復活したことである。これは、ロシアのウクライナ侵攻を巡る国際政治の展開によってより鮮明になった。「大国間の競争」の復活に伴い、テロ組織のような非国家主体ではなく、国家由来の脅威を抑止することが再び重要になってきた。このことから、新領域を巡る抑止においても考えるべき課題は、一義的には国家由来の脅威の抑止であると言える。

（２）紛争の形態

第２の前提は、紛争の形態についてである。「大国間の競争」というと、冷戦期の戦略環境に近いように思える。しかし現在においては、これは冷戦期のように、国家間の大規模戦争のみに備えれば良いということではない。国家間の対立が原因だとしても、具体的な紛争の形態には実際には幅がある。例えば、1990年代、情報革命によって軍事が革命的な変化を遂げると予測する「情報RMA」を巡る議論が米国で盛んに行われた。このときに想定された紛争は湾岸戦争型の大規模な正規戦であったが、2000年代から2010年代にかけて、米国が実際に対処しなければならなかった紛争は、アフガニスタンとイラクにおける非正規戦であった。米国がアフガニスタンとイラクにおいて苦戦を強いられたのは、このように、将来対処すべき紛争の形態についても見通しが外れたことが１つの要因である。

この点について、現在の段階で絞り込んだ形で予測することは難しい。現在、東シナ海や南シナ海で展開しているグレーゾーンにおける現状変更の試みや、ロシアが旧ソ連領域で試み、実際にクリミア併合を成功させたハイブリッド戦のような、正規戦の形態を取らない形での現状変革の試みは引き続き行われる可能性がある。

ただし、将来の紛争はグレーゾーンの事態／ハイブリッド戦になるとも断言できない。言うまでもなく、現在展開中のロシア・ウクライナ戦争は大規模正規戦である。そして、台湾有事や朝鮮半島有事も、それらが万一発生することがあれば大規模正規戦の形を取るであろう。こうしてみると、戦略レベルのトレンドとして、大国間競争の継続は予測できるが、紛争の具体的な形態については不確実性が大きい。グレーゾーンの事態／ハイブリッド戦における宇宙・サイバーの活用法と、大規模紛争における活用法とでは自ずと異なるため、新領域を含めた抑止概念を構築していく場合も、この二つの紛争の形態を視野に含めていく必要がある。

（３）新領域と戦略

第３の前提は、国家が安全保障上の戦略を実行していく上での目的が「どこに」存在するかである。これまでの、新領域の抑止を巡るこれまでの議論においては、戦略論の基本である「政治的目的は何か」「戦略的前提は何か」という問いを無視して戦術的状況にフォーカスする傾向が観察された。例えば、「宇宙空間における攻撃を抑止することは難しい」「サイバー攻撃を抑止することは難しい」という言説がある。ここでいう「抑止することが難しい」攻撃とは、人工衛星

に対するジャミングのような非物理的な攻撃であったり、低烈度のサイバー攻撃であったりすることが多い。しかし、日本周辺でも2016年に中国から、2018年に韓国から、海上自衛隊が火器管制レーダーの照射を受けていることから分かるように、非物理的な行動に対する抑止は、新領域に限らず旧来の物理領域でも難しい。また、中国やロシアが散発的に実施する領空侵犯も、日本の主権に対する侵害であるが、これを抑止することも難しいし、尖閣諸島周辺の領海や接続水域における中国の政府公船の継続的な侵入も抑止することは難しい。

このように、そもそもグレーゾーンにおける挑戦的な行動を抑止するのは難しい。この難しさは、ドメインの特性、すなわち新領域か旧来の物理的領域であるかによるものではなく、グレーゾーンという烈度の低い挑戦を抑止することが難しいという、これまでも存在してきた原則が新領域においても当てはまっていると考えるべきであろう。

ここで、戦略的文脈という語を用いた。戦略とは、国際政治において広く使われる概念であるが、それを具体的に定義するのは実際には難しい。大まかに合意できる形の定義をここで挙げておくとすれば、「戦略とは、『目的（ends)』『方法（ways)』『手段（means)』の組み合わせを示すもの」ということになろう[6]。「目的」とは、最終的に実現を目指す状態を指す。「手段」は、目的を達成するための具体的な行動そのものや行動に必要なツールを意味し、「方法」は、それらの具体的な行動やツールをどのように組み合わせて実行していくかを表す。戦略によって、「目的」「方法」「手段」が組み合わされ、何を実現したいのか、そしてどのようにそれを実現させるかが論理的・体系的に示される。

明文化された文書が策定されているかどうかは別として、どのような国家でも、安全保障政策の背景にはその国家の戦略がある。そして、「目的」、「方法」、「手段」は鎖のように連なり、戦略は多層的に形成される。下位の戦略は上位の戦略の「手段」となりつつ、独自の「目的」「方法」「手段」を持つ。

ここで重要なのは、戦略を考える上では「目的」「方法」「手段」を区別する必要があることであり、「方法」と「手段」とは「目的」を達成するためのロードマップを構成することである。基本的なことであるが、新領域における抑止を考える上では重要な点である。なぜならば、特に上位の戦略における目的は、宇宙空間やサイバー空間には存在しないからである。

人間はいまだに宇宙空間に居住しておらず、またサイバー空間に存在しているわけではない。そのため、宇宙空間の特定の座標やサイバー空間の特定の領域（サイバー空間に領域という概念があるならば、だが）を獲得することが戦略上の目標として設定されることはない。中国の最優先の戦略目標が台湾統一であると考えるなら、戦略上の目的は物理空間に存在する台湾という島であり、現在のロシアのウクライナ侵攻におけるロシアの戦略上の目標はやはり物理空間に存在するウクライナである。少なくとも上位の戦略において、戦略上の目的は物理空間に存在している以上、宇宙やサイバーといった要素は、「目的」そのものになることはなく、むしろ「方法」や「手段」となる（サイバー防衛戦略といった下位の戦略でサイバー空間に戦略目的が設定される可能性はある）。

そうだとすれば、宇宙であれサイバーであれ、ほかの伝統的な物理領域で作用する「力」と組

6　「目的」「方法」「手段」の組み合わせとしての戦略の性質について、更に詳しくは高橋杉雄『現代戦略論：大国間競争時代の安全保障』並木書房、2022年、18-24頁参照。

み合わされて戦略上の「目的」の達成のために使用されることになる。その意味で、新領域の「力」の中心にあるのは、陸海空軍力のような物理的な能力を増幅する作用や相手の物理的能力の効果を低減する作用であり、その意味でまさにフォース・マルチプライヤーとして位置づけられることになる。

3. 新領域がもたらすグレーゾーンにおける対応の難しさ

（1）法執行機関における課題

軍事分野における新領域の特徴は、物理的な破壊を伴わない攻撃が可能なことである。この点は、特にグレーゾーンにおいて重要な意味を持つ可能性がある。なぜならば、グレーゾーンにおいては、現状に挑戦する側は、明確な物理力を行使しないで、現状を変えていくことを狙うからである。その意味で、物理的な破壊を伴わない新領域は非常に有効な手段となり得る。

この点において２つの重要な課題が指摘できる。１つは、グレーゾーンにおける対処の中心となるのが、軍事組織ではなく、沿岸警備隊（日本では海上保安庁）や警察のような法執行機関であることに由来するものである。軍事組織であれば、宇宙・サイバー空間のような「新領域」における能力の強化が重要な課題であることは以前から認識されており、問題意識も持たれながら一定の能力強化が進んできている。一方、法執行機関においては、少なくとも軍事組織と同じレベルでの取り組みは行われていない。警察の役割の１つはサイバー犯罪への対処だが、それはあくまで社会における犯罪の防止のために行われているものであり、警察がグレーゾーンにおいて活動し続けるという問題意識のもとに進められている取り組みではない。

この点は、法執行機関が、グレーゾーンにおいて通常とは異なる役割を求められることに由来する難しさでもある。法執行機関の役割は、基本的には国内秩序の維持のための法執行である。そのために様々な犯罪の取り締まりが行われる。ところが、グレーゾーンにおいては、法執行機関は、国内秩序の維持ではなく、主権を巡る他国との争いの中で、自国の主権を維持するための任務を果たすことになる。これは、これまでであれば軍事組織が担うと考えられていた役割であった。

しかしながら、挑戦側の軍事組織が投入される以前の段階で、例えば偽装漁民が領海に侵入したり当初に上陸したりするような段階では、主権を守るために自衛権を行使して軍事組織を投入するのは難しい。その段階では、法執行機関があくまで日本の法を執行するという立場から偽装漁民に対処することになる。しかしその偽装漁民が、単なる犯罪行為を働くのではなく、ある国の明確な政治的意思をもって日本の主権を侵害するとの意図で日本領域内で活動しているような場合であれば、法執行機関の活動と言っても、単に法を執行するというだけではなく、そのこと自体が日本の主権を守るインプリケーションを持つことになるのである。尖閣諸島周辺で海上保安庁が果たしている役割がまさにこうしたものである。

こうした形で、グレーゾーンにおいては、本来想定していたのとは異なる形で、法執行機関が活動することが必要になってくる。このことが、グレーゾーンにおける新領域の問題を複雑化している。なぜならば、法執行機関が本来対処する対象である国内の犯罪者であれば、国家機関である法執行機関の宇宙空間の利用やサイバー空間の利用を大きく阻害するような能力は持ち得ない。しかしながら、グレーゾーンにおいては、相手は国家であるために、通常の犯罪者相手では想定されないような大規模な妨害を新領域で行える可能性がある。

例えば、尖閣諸島周辺で中国が大規模なGPSジャミングを行った場合、警備にあたっている海上保安庁の巡視船は自己位置の測定が困難になる。そうなると領海線やEEZの境界線を正確に識別することが難しくなり、相手の行動に対して適切に対応するのが難しくなるだろう。

（２）新領域を含むエスカレーション

また、グレーゾーンにおいては、エスカレーション・コントロールを精緻に行う必要があるため、時には中央からのマイクロマネージメントを行うことが不可欠になると考えられるが、通信衛星に対するアップリンクジャミングや地上施設に対するジャミングを行い、中央とのコミュニケーションを断つことができれば、やはり中国側が優位に立つことができる。

前述の通り、一般的に、法執行機関はジャミングへの耐性が軍事組織よりも脆弱である。そのため、グレーゾーンにおける新領域の非物理的攻撃を法執行機関に対して行うことは、非常に大きな効果をもたらす可能性がある。後述するように、本研究プロジェクトで「東シナ海グレーゾーン」についてのシナリオゲームを行った際にも、法執行機関に対する新領域を用いた攻撃は非常に大きな影響を持った。逆に言えば、法執行機関の新領域の利用のレジリエンシーを高める努力を、これまでとは次元の異なる形で進めなければならないと言うことでもある。

第２の論点は、グレーゾーンから、武力紛争へとエスカレーションするプロセスを想定したとき、新領域が加わることによってエスカレーションのダイナミクスがどう変わるか、あるいは変わらないのかである。これは、グレーゾーンから紛争への在来領域におけるエスカレーションと、非物理的使用を含む新領域におけるエスカレーションとの関連性を巡る問題である。比ゆ的な意味で言えば、「エスカレーション・ラダーは在来領域に立っているのか、あるいは新領域に立っているのか」という問いであり、将来の戦闘様相が予測困難であることを踏まえても、分析を深めておく必要がある論点である。

特に、サイバー攻撃においては、重要インフラに対する物理的攻撃も可能であると考えられているから、グレーゾーンから事態がエスカレーションしていくプロセスの中で、どのような形、タイミングで新領域を利用した物理的攻撃が行われるかは、エスカレーションをコントロールする上で重要な論点になる。

新領域の特徴を考慮すると、この点については以下のような仮説が成立しうると考えられる。まず、グレーゾーンにおいては、グレーゾーンにおいて優位に立つことを目的に、在来領域における現状変更の試みと連動する形で、新領域の非物理的使用が多用される可能性が高い。グレーゾーンにおける非物理的使用に限って言えば、エスカレーションは容易に発生するのである。

しかしながら、新領域であっても、物理的攻撃を行う場合には、現状打破側としてもより大きなリスクを覚悟する必要がある。例えばサイバー攻撃によって物理的ダメージを与えた場合、それを武力攻撃と解釈し、現状維持側が対応をエスカレートさせ、法執行機関に代わって軍事組織によって当該グレーゾーンへの対応を行うようにすることが考えられるからである。仮に法執行機関同士の対応において優位に立てる公算が高いのであれば、あえて相手側の軍事組織の投入を誘引するような物理攻撃を行う必要はない。

また、マルウェアは一度使用すればその存在が発覚し、駆除されてしまう可能性が高い。そのため、仕掛けられたマルウェアは最大の効果を発揮するタイミングで発動させることが有効であるが、そのタイミングとはおそらく在来領域で決定的な行動を取るタイミングになることが予想

される。

よって、新領域の物理的使用へのエスカレーションは、在来領域のエスカレーションの効果を最大化させるために、それと連動して行われる可能性が高いと考えられる。この場合、在来領域のエスカレーションと新領域におけるエスカレーションが同時並行的に展開することになる。グレーゾーンにおいては、現状打破側は新領域の物理的使用は抑制されると考えられるが、ひとたびグレーゾーンから紛争へとエスカレーションさせることを一方が決断した段階で、新領域を含めたエスカレーションが急激に発生することが考えられる。本研究プロジェクトでは「東シナ海グレーゾーン」を想定したシナリオゲームを行ったが、実際に、ある段階で急激にエスカレーションが進む現象が観察された[7]。

7　シナリオゲームの概要と結果については、本報告書の巻末資料を参照のこと。

第二章　抑止と新領域の概念整理

福田潤一

はじめに

「新領域における抑止の在り方」を検討するためには、まず「抑止」及び「新領域」についての概念整理が必要となる。本章で取り扱うのはこうした整理である。まず抑止についての定義を示し、続いて抑止を困難にする要素につき言及する。続いて抑止と密接に関連する概念であるエスカレーションについて言及し、更に抑止に関連するが抑止とは区別される様々な概念についても整理する。

こうした抑止の概念整理に引き続き、新領域における抑止についての概念整理を行う。まず「領域」の定義を行った上で、新領域における抑止の二つの性格、「領域内」抑止と「領域横断的」抑止の区別を行う。続いて宇宙領域とサイバー領域の特性について検討し、最後に新領域における抑止で想定される対応策として、四つの取り組みを掲げる。

1．抑止とは何か

（1）抑止の定義

抑止には多数の定義が存在する。最も古典的な定義はT・シェリング（Thomas Schelling）の「恐怖がゆえに回避するまたは思い止まること」、そして「成り行きへの恐怖によって行動を妨げるということ」というものである[1]。別の定義として、A・ジョージ（Alexander L. George）とR・スモーク（Richard Smoke）は、「相手が取る可能性のある行動のコストやリスクが、その利益を上回るように相手を説得すること」を掲げている[2]。

更にL・フリードマン（Lawrence Freedman）は、「条件付きの脅しで他者の行動を意図的に操作しようとすること」という定義を掲げており[3]、A・クレピネビッチ（Andrew F. Krepinevich, Jr.）は「競合相手（対象または「標的」）が禁止されている行動をとるのを防ぐための努力。抑止を実践する者は、標的が禁止された行動をとることに関連するコスト、利益、リスクの計算に影響を与えようとする」と、より詳細にまとめている[4]。

こうした定義の多様さはあるが、抑止概念には幾つか根本的に重要な要素があると考えられる。まず、相手の合理性（rationality）が前提となる。抑止がコストや利益、リスクの計算に依存する以上、完全に非合理な相手は抑止できないからである。続いて、抑止実現に足る能力としての抑止力（deterrent）の存在も前提になる。理論的にはハッタリ（bluff）による抑止があり得

1　Thomas C. Schelling, *Arms and Influence,* New Haven and London: Yale University Press, 1966, p. 71. 日本語訳はトーマス・シェリング著、斎藤剛訳『軍備と影響力：核兵器と駆け引きの論理』勁草書房、2018年、pp. 74-75より借用。

2　Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice,* New York: Columbia University Press, 1974, p. 11.

3　Lawrence Freedman, *Deterrence*, Cambridge: Polity Press, 2004, p. 6.

4　Andrew F. Krepinevich, Jr., *The Decline of Deterrence*, Hudson Institute, March 2019, p. 16.

ないわけではないが、抑止力を欠けば抑止破綻の可能性はそれだけ高まることとなる。更に、相手に対する伝達（communication）も不可欠である。意図や能力、決意の伝達を欠くところに抑止実現はない。そして伝達の信頼性（credibility）も重要である。信頼性を伴わない伝達は相手の行動を変化させることができず、抑止の破綻を導く。

（国家間で）抑止を実現させるための要件については、クレピネビッチが詳しい整理を行っている[5]。それによると、①国家Aが国家Bに、Bの特定行動（禁止された行動／Aの「レッドライン」を越える行動）がAの対応を招くと伝達せねばならない。②国家Bは、Aによって禁止された行動とこれを越える場合の帰結について明白に理解せねばならない。③国家Bは、禁止された行動を取った場合にAによって脅された帰結を招くと信じねばならない（Aの脅しは高い信頼性を伴わねばならない）。④国家Bは、（懲罰的抑止により）禁止された行動を取ることのコストがその利益を上回るか、または（拒否的抑止により）Aの行動によってBの目的達成が阻まれるであろうことを信じなければならない。⑤国家Bは、利益を最大化し損失を最小化するという意味での「合理的な」振る舞いをせねばならない。以上の全ての要件を満たしてようやく抑止が成立する。よって、抑止の実現には一般的に高いハードルが存在する。抑止がしばしば破綻するのはこのためである。

なお、抑止の種類については次のような分類が存在する[6]。まず、狭い（narrow）抑止と広い（broad）抑止の区別がある。前者は戦争の中で特定の軍事行動を抑止することを意味し、後者は戦争全体を抑止することを意味する。次に中央（central）抑止と拡大（extended）抑止の区別がある。前者は自身に対する攻撃を抑止することを意味し、後者は他者（主として同盟相手）への攻撃を抑止することを意味する。前者の信頼性は高いが、後者はしばしば信頼性の問題を生じるとされる。更に拒否的（by denial）抑止と懲罰的（by punishment）抑止の区別がある。前者は抑止対象の目的達成を阻むことを通じた抑止であり、後者は抑止対象に懲罰的な費用賦課を行う抑止である。最後に、一般（general）抑止と緊急（immediate）抑止の区別がある。前者は平時における抑止であり、後者は危機時における抑止である。ただし、一般抑止が成立する状況はそもそも挑戦者による挑戦意図があるかどうか不明であるため、これを抑止の文脈で捉えるべきかの妥当性の問題がある。よって、抑止を巡る議論は、緊急抑止の文脈で行われることが多い。

（２）抑止を困難にする要素

抑止の実現を困難にする要素について更に掘り下げたい。代表的な要素として次の五つを挙げることができる。

まず、相手が合理的な存在でない、ということである。人間はそもそも合理的な存在ではなく、認知バイアスや危機時のストレス、プロスペクト理論等の示唆するところにより、合理性を前提とした抑止の実現にはそもそも問題がある、とする見方が存在する。これは認知心理学的観点からの抑止懐疑論と指摘できよう[7]。

5　Ibid., pp. 16-17.

6　Freedman, *Deterrence,* pp. 32-42.

7　例えばRobert Jervis, Richard Ned Lebow, and Janice Gross Stein, *Psychology and Deterrence*, Baltimore: Johns Hopkins University Press, 1985を参照。

次に、相手も合理的存在であるが、戦略文化その他の違いにより、コストやリスク判断の前提が異なることを読み違えてしまう可能性が存在する。合理性は必ずしも普遍的な共通理解を伴わない。ある行為者にとって非合理に見える行動が、ほかの行為者にとっては合理的である場合も存在し得る。結果として、「相手も自分と同様の存在だろう」との誤った前提に基づく「ミラー・イメージングの罠[8]」に陥ることによる抑止破綻が発生し得る。

第三に、国家の単一合理性仮定という誤った前提に依拠してしまう可能性が考えられる。抑止論では基本的に行為者の合理性を前提とするが、現実には国家は多くの異なる選好を有する様々な組織の集合体である。よって、国家の行動は、意思決定者の選好をそのまま反映したものであるとは限らない。そこで、国家の行動を合理的な選択の結果と錯覚すると、抑止の意図伝達に支障をきたす。それは実際には意思決定者が意図しない形で行われるかもしれないからである。キューバ危機を分析した名著『決定の本質[9]』が指摘する、「第二モデル（組織行動）」や「第三モデル（政府内政治）」の視点に留意する必要があろう。

第四に、国際関係における不確実性や、国家が自身の選好を偽装する動機等によって、信頼性の高い伝達が困難となる可能性がある。国家の能力や意図、決意、そして行動に至るまで、国際関係における不確実性の払拭は容易ではなく、こちらの伝達が相手に明確に伝わらない可能性は否定できない[10]。それだけでなく、国家は交渉において他者より優位に立つため、自身の選好を偽装する（misrepresent）動機があるとも指摘される[11]。本当は抑止の決意を持たないのにハッタリを行う可能性は排除できず、結果としての抑止破綻のリスクがあり得る。いずれにしても信頼性の高い抑止の伝達が損なわれる恐れがある。

最後に、新技術の登場や非国家主体の関与等が抑止状況を複雑化する可能性があり得る。新技術の登場が戦争の次元を拡張し、攻撃・防衛のバランスを変化させたり、抑止に要する意思決定の時間を短縮したりする恐れがある[12]。戦略核兵器を搭載した弾道ミサイルの登場や、その複数個別誘導再突入体（MIRV）化などは代表例と言えよう。また、非国家主体が国家の代理者（proxy）として用いられることにより、攻撃者が特定困難になる帰属問題を発生させることも指摘できる。これは特にサイバー領域において顕著であり、「新領域における抑止の在り方」の検討に直接的に係る問題である。

いずれにせよ、これらの要素が複合的に作用するため、抑止の実現は容易なことではないのである。

---

8 Don Munton and David A. Welch, *The Cuban Missile Crisis: A Concise History,* 2nd ed., New York: Oxford University Press, 2011. 邦訳：ドン・マントン、デイヴィッド・A・ウェルチ著、田所昌幸、林屋一訳『キューバ危機：ミラー・イメージングの罠』中央公論新社、2015年。

9 Graham Allison and Philip Zelikow, *Essence of Decision: Explaining Cuban Missile Crisis,* 2nd ed., New York: Longman, 1999. 邦訳：グレアム・アリソン、フィリップ・ゼリコウ著、漆嶋稔訳『決定の本質：キューバ・ミサイル危機の分析 第2版 1及び2』日経BPクラシックス、2016年。

10 国際関係における不確実性の帰結の代表例が、自国の安全を高める行動が他国にとって脅威と見なされる結果、むしろ自国の安全を損なってしまうという「安全保障のジレンマ（security dilemma）」である。Robert Jervis, "Cooperation under the Security Dilemma," *World Politics,* Vol. 30, No. 2, January 1978, pp. 167-214.

11 James D. Fearon, "Rationalist Explanation for War," *International Organization,* Vol. 49, No. 3, Summer 1995, pp. 379-414.

12 正確には技術のみならず、ドクトリンや戦力態勢及び配備の変化も同様の影響を有する。Stephen Van Evera, "Offense, Defense, and the Causes of War," *International Security*, Vol. 22, No. 4, Spring 1998, pp. 66-68.

（３）密接に関連する概念：エスカレーション

続いて、抑止に密接に関連する概念としてのエスカレーション（escalation）について言及する。エスカレーションとは、「参加主体の一つ以上が重要だと考える閾値を越えるような紛争の強度または範囲の拡大」と定義される。同時に、このようなエスカレーションが起こるのは、「少なくとも一方の当事者が、新たな展開の結果、紛争に重大な質的変化が生じたと確信した場合のみ」であることも指摘される[13]。このようなエスカレーションは、意図的な政策の結果としても、事故の結果としても生じ得る。

抑止との関連について言えば、抑止とは相手が特定の行動（レッドライン／閾値）を越えることを阻止する努力であるが、しかしそうしたレッドライン／閾値は単一のものとは限らない。あるラインが突破されても、その次のラインを突破されないように阻止することは、抑止の努力において重要である。これがエスカレーション管理（escalation management or control）であり、エスカレーション管理は抑止の延長線上にあると言える。

ただし、エスカレーション管理は、単にエスカレーションの緩和を目指すだけのものではない。相手によるエスカレーションを阻止するためには、こちらも相手が対応できないほどのエスカレーションを実行できる意図や能力、決意を示す必要がある。このためにエスカレーション優位（escalation dominance）を求めた意図的なエスカレーションが追及される場合もあり得る。最近の例としては、ロシアが採用していると言われる「エスカレーション緩和のためのエスカレーション（escalate to de-escalate）」戦略[14]が挙げられよう。

エスカレーションには次の三種類があるとされる。第一に、紛争の烈度が上昇する垂直的（vertical）エスカレーションである。第二に、紛争の地理的範囲が拡大する水平的（horizontal）エスカレーションである。第三に、同盟国に対する攻撃等によって、元々の紛争に新たな危機や紛争が加わる合成的（compounding）エスカレーションである。

エスカレーションの、特に垂直的な閾値を積み上げたものはエスカレーション・ラダー（escalation ladder）と呼ばれる。エスカレーションの個々の閾値に挟まれた段階を段（rungs）と呼び、これをある程度まとめたものを単位（units）と呼ぶ。こうしたエスカレーションの概念を示したH・カーン（Herman Kahn）は、1965年の著作において米ソ間の熱核戦争のエスカレーション・ラダーとして、「見せかけの危機」から「衝動的または無感覚な戦争（＝全面的な熱核戦争）」までの44段階の段及び７段階の単位を想定した[15]。

カーンのエスカレーション・ラダーの概念は時代性を反映して、米ソによる核兵器の使用後になお24段もの段が存在するという、核戦争においてもエスカレーションの管理が重要であることを強調するものであった。しかし、今日のエスカレーション・ラダーは、より通常戦力における武力衝突の段、及びそうした武力衝突に至る前の（国際法上の武力攻撃未満の＝グレーゾーン事態における）段が重要であると考えられる。この点、エスカレーション・ラダーの思考を今日の

---

13 Forrest E. Morgan, et al., *Dangerous Thresholds: Managing Escalation in the 21st Century,* RAND Corporation, 2008, p. 8.

14 Nikolai N. Sokov, “Why Russia calls a limited nuclear strike ‘de-escalation’,” Bulletin of the Atomic Scientists, March 13, 2014.

15 Herman Kahn, *On Escalation: Metaphors and Scenarios,* New York: Praeger, 1965, p. 39.

戦略環境にどう適用するかが課題であると言える[16]。

ただし、後述する作戦領域の多様化が、このエスカレーション・ラダーの概念に対する重大な挑戦となっている。なぜならば、今日の武力衝突は古典的なエスカレーション・ラダーが想定する単純な（垂直的）閾値の積み重ねの形を採らないと考えられるからである。多領域作戦の時代におけるエスカレーションは、必然的に複数領域に跨る形で蛇行的になると考えられる[17]。ある領域におけるエスカレーションが別の領域におけるエスカレーションを引き起こし、それらが複雑に相互作用する形でエスカレーションのラダーが構築されると考えられるからである。このようなエスカレーションをラダーというよりもラティス（lattice）という概念で捉える論考も存在する[18]。これはエスカレーションの過程を垂直的な「梯子」としてよりも、縦方向の烈度のエスカレーションと横方向の領域横断的なエスカレーションが併存する「格子」の概念で捉える方が適切との見方である。また別の論者は、今日のエスカレーションは予測しにくい経路を辿り加速的かつ非線形的な形を採るというワームホール（wormhole）・エスカレーションの概念を提唱している[19]。

尤も、こうした議論が既存のラダーに代わる概念を確立しているとは言い難く、エスカレーション・ラダーの概念を多領域作戦の時代に適合させる形で見直す動きは今後も続くと考えられる。

（４）抑止に密接に関連するが、抑止とは区別される概念

更に、抑止に密接に関連するが、抑止とは区別される概念について整理する。

最初に取り上げるのは強要（compellence）である。シェリングによれば、抑止が相手に特定行為を「させない」ことを目的とするのに対して、強要は相手に特定行為を「させる」ことを目的とするものである[20]。相手の行動を単に阻止するのではなく、相手に能動的な行動を強要する点において、抑止よりも実現のハードルが高いとされている。両者は混同しがちであるが、理論的には区別が必要である。

次に、防衛（defense）は抑止破綻の後に行われる実際の相手との戦闘行為である。核戦略の文脈においては戦争遂行（war-fighting）とも呼ばれる。抑止と防衛は区別されるべき概念ではあるが、現実には防衛と、特に拒否的抑止の文脈におけるエスカレーション管理の努力を区別することは容易ではない。あくまで単純に相手の目的達成を阻むか、あるいは目的達成を阻む姿勢を示すことで更なるエスカレーションを阻止するか、の違いに過ぎない。

続いて、現状（status quo）である。抑止とは現状を変革しようとする相手の行動を阻止する努力であるが、この現状の概念が当事者間で異なる可能がある。具体例を挙げれば、米国による台湾防衛は中国による現状変革の阻止であるが、中国から見れば中台統一を阻もうとする米国の

16　エスカレーション・ラダーについての彼我の共通認識の有無も重要な論点である。

17　King Mallory, “New Challenges in Cross-Domain Deterrence,” RAND Corporation, 2019, p. 7, Figure2.

18　Martin Libicki and Olesya Tkacheva, “Cyber Escalation: Ladder or Lattice?” in Floyd A. Ertan and Stevens T. Pernik, eds., *Cyber Threats and NATO 2030: Horizon Scanning and Analysis,* NATO Cooperative Cyber Defense Centre of Excellence, 2020, pp. 60-72.

19　Rebecca Hersman, “Wormhole Escalation in the New Nuclear Age,” *Texas National Security Review,* Vol. 3, Issue 3, Autumn 2020, pp. 90-109.

20　Schelling, *Arms and Influence,* p. 69.

介入は「現状」を脅かすものと映る。現状の概念はプロスペクト理論における参照基準点（reference point）の概念[21]と関連があると見られるが、抑止を議論する際には誰にとって何が「現状」であるのかを把握することが重要となる。

更に、諫止（dissuasion）がある。これは米国が2001年の「四年毎の国防見直し（QDR 2001）」で強調した概念であり、「米国の利益に敵対的な能力の開発や行動様式の採用を他者に思いとどまらせること」とされた[22]。諫止の取り組みは抑止に先行する、抑止の前段階（pre-deterrence）の取り組みとも位置付けられた。尤も、大国間の戦略競争の構図が鮮明になった今日では、この概念は殆ど使われていない。

加えて、戦略的安定性（strategic stability）がある。これは歴史的に米ソ（米ロ）間の核抑止の文脈で用いられてきた概念であり、定義としては「極端な状況下で自国の死活的な利益を守るためでなければ、どの当事国も核兵器を使用する動機を持たない状況」がある[23]。ただし、この概念は第一撃の安定性（first-strike stability）や危機時の安定性（crisis stability）、更には軍備管理における安定性（arms control stability）等の幾つかの概念を束ねたものであり、その具体的な態様は当事者次第で政治的にかなり多様に解釈される傾向にある。この概念は今日、ミサイル防衛や極超音速兵器、既存の軍備管理条約で規制されない戦略兵器、更には核の多極化等の影響で既存の戦略的安定性が損なわれる、といった文脈で使用される場合が多い。本質的に軍備管理の取り組みと親和性のある概念である。

これに関連して、安定性と不安定性のパラドックス（stability-instability paradox）も重要な概念である[24]。これは戦略核次元の安定性が、それ未満の次元の抑止破綻やエスカレーションの可能性を高めるという逆説を示す概念である。戦略核次元での安定性が存在するという事は、それ未満の次元で抑止破綻やエスカレーションを引き起こす行動をしても、それが戦略核次元の対決に発展する可能性が低いということである。このため、戦略核次元の安定性はかえってそれ未満の次元で抑止破綻やエスカレーションを惹起してしまうのである。この逆説は今日、米ロ間または米中間の戦略核次元の安定性が、欧州やインド太平洋地域における紛争生起に繋がるという文脈で、特に注目を集めている[25]。

そして、安心供与（re-assurance）がある。抑止は一線を越える事への「信頼性の高い脅しの

---

21 プロスペクト理論（prospect theory）とは「人は得るよりも失うことを恐れる」ことを説明する心理学の理論であり、参照基準点とは行為者にとってこの得失を分ける分岐点のことを指す。Daniel Kahneman and Amos Tversky, “Prospect Theory: An Analysis of Decision under Risk,” *Econometrica,* Vol. 47, No. 2, March 1979, pp. 263-292.

22 Ryan Henry, “Deterrence and Dissuasion for the 21st Century,” IFPA-Fletcher Conference, December 14, 2005.

23 Elbridge A. Colby and Michael S. Gerson, eds., *Strategic Stability: Contending Interpretations,* Strategic Studies Institute and U.S. Army War College Press, 2013, p. 55.

24 Glenn H. Snyder, “The Balance of Power and the Balance of Terror,” in Paul Seabury, ed., *The Balance of Power*, Scranton: Chandler, 1965, pp. 185-201.

25 2022年２月24日以降のロシアによるウクライナ侵略の本格化は、米ロ間の戦略核次元の安定性が一つの背景になって発生したと解釈することも可能である。米国がロシアとの核戦争を恐れ戦略的安定性の維持に拘る限り、ロシアは米国との核戦争を懸念することなく、戦略核未満の次元でのウクライナへの侵略行為が可能だからである。福田潤一「第２章　ロシア・ウクライナ戦争－その抑止破綻から台湾海峡有事に何を学べるのか」高橋杉雄編著『ウクライナ戦争はなぜ終わらないのか：デジタル時代の総力戦』文藝春秋、2023年、77-81頁。

伝達」に係る概念であるが、現実には相手が協調に転じたらこちらも協調で応じるという、「信頼性の高い協調のシグナル」を送ることもエスカレーション緩和の文脈では重要になる。これは、相手が協調に転じたことに乗じてこちらから侵害行為を行うことはない、という誓約としても解釈し得る。これが安心供与であり、「信頼を構築するプロセス」「当方が協力し合うことを好むが故に、相手にとって協力することが安全だと相手を説得することに係る」概念と定義される[26]。ただし、信頼性の高い抑止の伝達と、信頼性の高い安心供与の伝達を同時に行うことは、論理的に困難である。

最後に、軍備管理（arms control）や信頼醸成（confidence building）、行動規範（code of conduct）形成等がある。これらは上記の戦略的安定性、もしくは当事者間の何らかの安定性を損なわないようにするために、国家の能力または行動に一定の制約を設ける目的で取り組まれる努力として解釈し得る。こうした努力は抑止の取り組みと逆行することもあるが、同時にもし強固な軍備管理や信頼醸成、行動規範の形成等が存在する場合、当事者間の抑止破綻は起こりにくくなるため、抑止と密接な関連のある概念と言える。

2. 新領域における抑止とは何か

（1）領域の定義

戦争は伝統的には陸海空の三つの領域で戦われるものと見なされてきた。しかし今日、これらの三領域には留まらない形で戦争の領域が拡大している。こうして新しく戦争や作戦の領域と見なされるようになった領域を陸海空の伝統領域との対比で「新領域」と呼ぶ。

ただし、この領域（domain）の定義は必ずしも明確ではない。広義の定義としては、例えば「政治的交渉への有用性という点で、ほかの手段とは異なる強制的な経路や手段」というものがある。これによると領域という概念は、「明確に定義された境界線を持つ個別の分野、法的または官僚的な管轄権、所有権の主張、分業、または技術的な専門分野を表す」とされる[27]。これは領域を（抑止と強要の双方を含む）強制（coercion）[28]の観点から広く定義する見方であり、軍事のみならず非軍事の分野まで視野に入れている。

具体的には、この見方では軍事以外の政治／経済／外交／金融／司法等が幅広く国家が他者に強制力を発揮するための領域と見なされる。こうした見方は、軍事と非軍事の垣根を越えて国家のあらゆる行動が戦争の手段となるという中国の「超限戦」の見方[29]や、国家の安全保障を考える上で外交、インテリジェンス、軍事、経済を含む多様な要素を組み合わせる必要があるとするDIMEの思考と親和性がある。

他方で、軍事に焦点を絞った、より限定的な領域の捉え方もある。「任務に必要な行動の自由と優位性を確保するためにアクセスや統制が死活的な、決定的重要性を持つマクロな機動空

---

26 Andrew H. Kydd, *Trust and Mistrust in International Relations,* Princeton: Princeton University Press, 2005, p. 184.

27 Jon R. Lindsay and Erik Gartzke, "Introduction: Cross-Domain Deterrence, from Practice to Theory," in Jon R. Lindsay and Erik Gartzke, eds, *Cross-Domain Deterrence: Strategy in an Era of Complexity,* Oxford: Oxford University Press, 2019, p. 16.

28 強制をこのように解釈したのはシェリングである。Schelling, *Arms and Influence,* p. 71.

29 喬良・王湘穂『超限戦 21世紀の「新しい戦争」』KADOKAWA、2020年。

間[30]」という定義がそれである。こちらの定義は、より軍事的な多領域作戦（MDO）に焦点を当てたものであり、世界の軍事組織による領域の解釈に近い捉え方になる。日本の防衛省・自衛隊が「新領域」と言うときの領域の概念はこちらに近いものとなろう。

具体的には、世界の多くの軍事組織では陸海空の三領域を既存もしくは伝統領域として捉え、「宇宙」と「サイバー（及び電磁）」領域を軍事作戦で優位を得るために今や死活的な重要性を持つようになった新領域として捉える傾向が強い。現代の軍事作戦の遂行にあたってこれらの領域への依存が深まっているため、これらの領域で優位を喪失することは、致命的と考えられているからである。このため、現代の軍事作戦は必然的に宇宙及びサイバー（電磁）領域を含めたMDOとして実施されることが大前提となっている。

なお、防衛省・自衛隊は「新領域」として「宇宙」「サイバー」「電磁波」の三つを掲げており[31]、「ウサデン」と称されることもあるが、領域ないし新領域をどう分類するかは必ずしも固定的に考える必要はない。新領域の概念は常に拡張余地を残しており、例えば近年ではサイバー領域と重複するがそれに限られるものではない「認知（cognitive）」領域という考え方も採られているからである[32]。これは、情報操作や誘導工作によって他者の認知を操作したり、これに対抗したりすることを、新たな戦争や作戦の領域として位置づけようとの捉え方である。

（２）「領域内」抑止と「領域横断的」抑止

次に、「領域内」抑止と「領域横断的」抑止の区別について整理する。一言で「新領域における抑止」と言っても、二つの異なる意味を内包し得る。そのため領域内抑止と領域横断的抑止を区別する必要がある。

まず、領域内抑止とは、その領域の内部における攻撃をどう抑止するかに係る問題である。宇宙及びサイバー領域を念頭に考えれば、これらの領域の内部における攻撃、またはこれらの領域における活動や機能維持に不可欠なアセット等に対する攻撃をどう抑止するかが焦点となる。代表例を挙げれば、宇宙領域では軌道上の衛星に対する攻撃、地上の宇宙関連施設への攻撃、それらを接続する通信への攻撃等への対応が課題となろう。そして、サイバー領域では、重要インフラの「監視制御とデータ取得（SCADA）」システムへの攻撃、広範なネットワークの機能維持に係る攻撃、そしてサーバーや海底ケーブルの陸揚げ施設に対する物理攻撃等への対応が課題となろう。これらの攻撃への対策（抑止の手段）としては、下記に述べる領域横断的抑止が有効ではあるものの、領域内で例えばレジリエンス（後述）の向上に努めて、拒否的抑止ないしは防衛の取り組みを図ることも効果的である。よって、「新領域における抑止」を考える際、領域内抑止が一つの観点となる。

次に領域横断的抑止とは、ほかの領域と跨る形での抑止をどう実現するかに係る問題である。

---

30 Jeff Reilly, “OTH Video: Beyond the Theory – A Framework for Multi-Domain Operations,” *Over the Horizon*, April 13, 2018。
https://overthehorizonmdos.wpcomstaging.com/2018/04/13/oth-video-beyond-the-theory-a-framework-for-multi-domain-operations/

31 防衛省・自衛隊「平成31年度以降に係る防衛計画の大綱について」2018年12月18日、pp. 17-19。

32 Paul Ottewell, “Defining the Cognitive Domain,” *Over The Horizon*, December 7, 2020.
https://overthehorizonmdos.wpcomstaging.com/2020/12/07/defining-the-cognitive-domain/

そもそも攻撃は特定の領域に限定して行われるものではなく、宇宙やサイバー領域に対する攻撃も、特定領域を越えた何か大きな政治的・戦略的目標を追求するために行われるはずである。このため、たとえ特定領域に限定される攻撃であったとしても、これを抑止・防衛するためにあらゆる領域を活用するという考え方は自然なものである。伝統領域のみで戦われた過去の戦争の例を見ても、陸上の攻撃に対して海洋の優勢で対抗したり、その逆を追求したり、ということは一般的であった。重要なのはあくまで政治的・戦略的目標の追求であり、領域の活用はそのための手段に過ぎないと言える。伝統領域と新領域の横断という観点で言えば、新領域に対する攻撃を伝統領域における反撃の示唆で抑止したり、または伝統領域に対する攻撃を新領域における能力の活用で抑止したり、といったことが挙げられる。いずれにしても、とりわけ戦略レベルにおいては、あらゆる抑止を領域横断的抑止として捉えるべきと言っても過言ではない。

（３）新領域の特性①：宇宙

次にこうした新領域の特性について概観したい。本章並びに本報告書全体では、基本的に宇宙領域とサイバー領域を念頭に「新領域」と解釈しているが、まずは宇宙領域である。

宇宙領域は新領域と呼ばれてはいるが、実際にはその軍事利用は冷戦時代から行われており、決して宇宙の軍事利用そのものが新しいわけではない。ただし、当時と今日の宇宙利用の姿には大きな変化がある。冷戦時代の宇宙利用は、商用利用が乏しく、主要アクターは米ソに限られ、軍事利用と言っても戦略核抑止に係る利用が一般的で、かつ宇宙における攻撃手段も限定的だったという特徴があった。こうした過去の宇宙利用については、例えば「第一の宇宙時代」と呼ぶことができよう。

これに対して、今日の状況は根本的に変化している。具体的には、①民間セクターの利用が増大し、②多くの国家や非国家主体がアクターとして混在し、③戦術レベルや作戦レベルでも軍事活動の宇宙空間への依存が高まり、更に④キネティック／ノン・キネティック双方の多様な攻撃手段が出現してきたことが挙げられる。これを「第二の宇宙時代」と呼ぶことができよう。この結果、宇宙領域はますます多様・攪乱的・非秩序的・危険な状況になってきたことが指摘されている[33]。必然的に、宇宙領域における抑止やエスカレーション管理についても、再検討を行わざるを得ない時代となっている。

一般的には、宇宙領域には次のような特性があると考えられる。第一に、状況把握（situational awareness）の困難である。宇宙空間は極めて広大かつ遠隔であり、人的アクセスも容易でないため、そこで何が起こっているかの常続的な状況把握はしばしば難しい。結果として、攻撃を受けたこと自体の把握や、その原因の特定が困難である。第二に、防御の困難である。宇宙空間のアセット（衛星等）は打ち上げコストの問題から強固な装甲を持たせるわけにいかず、攻撃に脆弱である。更に攻撃を受けた後の修理（機能復元）も困難であり、機能喪失しやすい。第三に、攻撃の閾値が低いことである。状況把握の困難さ故に、宇宙領域では攻撃の有無や攻撃者の特定が難しい。また、軌道上には殆ど人間がいないため、直接的な人命損失が起きにくいことも相まって、攻撃の閾値が低いと考えられる。第四に、多様なアクターが混在している

33 Todd Harrison, et al, *Escalation & Deterrence in the Second Nuclear Age,* Center for Strategic and International Studies, October 3, 2017, p. 5.

ことである。活動主体が多様化しつつあるため、国家による攻撃と非国家主体による攻撃の両面があり得る。攻撃を受ける側も同様である。非国家主体を偽装した国家主体の攻撃の可能性もあり得る。最後に、宇宙領域では行動規範が欠落していることである。宇宙空間への大量破壊兵器の配備を禁じた宇宙条約のような一部の規制はあるが、行動規範として十分ではなく、ルール化がまだまだ不十分であると言える。

結果として、「第二の宇宙時代」の今日、宇宙領域では防衛に対して攻撃優位（offense-dominant）となりやすく、抑止破綻が生じやすい特性があると言える。

（４）新領域の特性②：サイバー

サイバー領域も宇宙領域と似た特性を有していると指摘できる。サイバー領域（インターネット）の歴史は1960年代末のARPANET誕生まで遡ることができるが、当初は限られた研究者同士の善意ベースの運営で問題がなかった。しかし1990年代以降にネットの一般利用が進むと、サイバー攻撃の多発で「開放性」「非中央集権性」「匿名性」「信頼」等の要素に基づくサイバー領域の運営に係わる問題が顕在化してきた。

現在のサイバー領域も、宇宙領域と同様に、あるいはそれ以上に、①民間・軍事の区別が混然とし、②国家と非国家主体の双方を含む多様なアクターが存在し、③軍事作戦のサイバー領域への依存が極めて大きくなっており、④様々な形でのサイバー攻撃（またはサイバー侵入）が一般化している現状にある。このために、サイバー領域における抑止やエスカレーション管理の重要性が増していると指摘できる。とりわけ、軍事的な指揮統制（C2）システムや、民間を含む重要インフラ（critical infrastructures）への攻撃を阻止することが死活的に重要になっている。

サイバー領域の特性も、宇宙領域のそれと似通っていると考えられる。第一に、状況把握が困難である。サイバー攻撃は一般的に前段階として侵入（CNE: Computer Network Exploitation）を伴うが、その探知は難しく、被害把握も容易ではない。また、攻撃者の素性が特定困難であるという帰属問題が存在している。第二に、防御が困難である。知らない間にネットワークに侵入されてボット（マルウェア）を仕込まれる、突然未知の脆弱性を突かれるゼロデイ攻撃を受ける等の展開があるため、予め防御を充実させておくことが難しい[34]。第三に、攻撃の閾値が低いことである。サイバー攻撃の知見と安価なシステムがあれば個人でも攻撃を実施可能であり、多大な投資を必要とせず安価なコストで攻撃ができるため、攻撃の閾値が低いと考えられる。第四に、多様なアクターが混在していることである。国家主体と非国家主体がネットの世界に同居しており、上記の通り帰属問題の解決が容易でないことから、国家主体が非国家主体に成りすます、またその逆を行うことが容易である。第五に、行動規範の不在である。物理空間ではないサイバー領域では、宇宙領域以上に行動規範が乏しい。結果として侵害行為に対する制度的歯止めが機能しにくい。

以上のような事情により、サイバー領域でも宇宙領域と同様に攻撃優位となりやすく、抑止破

34　ただし、マルウェア攻撃の場合、攻撃側が一度効果を発動させれば早期に防御側によって対策を採られて無力化されると考えられるため、サイバー領域では攻撃側が常に防御側にとっての未知の脆弱性を突き続ける必要性があることも事実である。また、その性質上、マルウェアは一度限りの効果発揮しか期待できないため、これが使用される場合にはほかの領域と連動した急激なエスカレーションが起こる可能性も否定できない。

綻も起こりやすい、と総括することができる。

3. 新領域における抑止：想定される対応策

最後に、以上のような特性（＝攻撃優位で抑止破綻が起こりやすい）を持つ、新領域における抑止の文脈で想定される四つの対応策についてまとめたい。

第一に想定される対応策は、状況把握能力の向上である。まずは当該領域で「何が起こっているか」を把握できなければ抑止どころかその破綻さえも認識できない。具体的には、平時における状況把握（軌道上のデブリや衛星等の監視／ネットワークへの侵入検知等）に努め、機能不全が起きた際の原因特定（事故や単なる故障か、それとも人為的攻撃か）を可能にすることが求められる。更に、人為的攻撃と認定された場合の攻撃者特定（帰属問題解決）、そして反撃を行う場合の戦闘損害評価（BDA: Battle Damage Assessment）まで可能であることが望まれる。

第二に、（拒否的抑止としての）レジリエンスの向上である。攻撃を受けてもシステムが決定的な機能不全に至らないという意味での「機能保証（mission assurance）」の確保が求められる。これはシステムを機能不全に至らしめようとする相手の目的を阻止することに重点を置く取り組みである。具体的には、宇宙領域で例を挙げれば、部分的な機能喪失がシステム全体の機能喪失に至らないようにする努力（小型衛星によるコンステレーションの構築等）や、機能喪失が起こっても迅速にそれを復元できる能力（迅速な再打ち上げ能力等）が含まれる。サイバー領域における対策もこれと同様である。

第三に、（拒否的ないし懲罰的抑止としての）攻撃（ないし反撃）能力の保有である。新領域における攻撃・防衛のバランスはどうしても攻撃側優位となるため、そうであるならば抑止を行う側も攻撃（ないし反撃）能力を備え、相手の攻撃手段や相手が重視する価値を危険に晒すことによって、こうした能力の誇示による抑止を模索する選択肢がある。具体的には、相手の宇宙アセットやネットワーク能力を無力化する領域内の攻撃ないし反撃、または他領域の攻撃手段を用いた領域横断的な攻撃ないし反撃（宇宙・サイバー領域での攻撃に対する核または通常戦力による反撃）が考えられる。

第四に、抑止ではないが、軍備管理や信頼醸成、行動規範形成等の取り組みを挙げることができる。抑止の取り組みを要する国家間でこうした試みを行うことは容易なことではないが、究極的にはこれらの取り組みによって、抑止に過度に依存せずとも安定的な国家間ないし国家・非国家主体間の関係を構築できることが望ましい。しかし、米ソ冷戦の経験を踏まえると、キューバ危機のような一大危機の共通体験がない限り、競争関係にある大国間での軍備管理や信頼醸成、行動規範形成等の実現は困難である可能性が高い。

おわりに

「新領域における抑止の在り方」を検討するために、本章では「抑止」と「新領域」についての概念整理を行った。その上で新領域、すなわち宇宙領域とサイバー領域の攻撃優位な特性について概観し、新領域における抑止で想定される対応策として四つを提示した。

抑止はもともと、成立させる要件の厳しさ故に、しばしば破綻するものである。新領域の攻撃優位な特性や、多領域作戦の時代におけるエスカレーション・ラダー概念の有効性の問題を考えれば、新領域における抑止の実現はますます困難であることは間違いない。

しかし、第一章で指摘された、戦争3.0の時代に直面する我々は、そうした困難に立ち向かわねばならない時代に生きている。本章そして本報告書の議論がそうした困難の克服に貢献できれば幸いである。

第三章　宇宙における抑止の追求とレジリエンス・防護の重要性

福島康仁

はじめに

宇宙抑止（space deterrence）には２つの側面が存在するとされる[1]。１つは「抑止における宇宙」（space in deterrence）であり、軍事力などを用いて自国などへの攻撃を抑止する際に宇宙システムや攻勢的対宇宙能力（offensive counterspace capabilities）が果たす役割を指す[2]。もう１つは「宇宙における抑止」（deterrence in space）であり、宇宙システムに対する攻撃を抑止することを意味する[3]。このうち本稿では「宇宙における抑止」を中心として、宇宙と抑止の関係性を考察する。

なお、宇宙システムは人工衛星のみを指すわけではない。宇宙システムは①衛星といった宇宙セグメント、②衛星を管制する施設やユーザー端末といった地上セグメント、③宇宙セグメントと地上セグメントの間などでやり取りされる信号を指すリンクセグメントという３つのセグメントで成り立っている[4]。これらのセグメントが全て正常に稼働することで宇宙システムとしての機能を発揮する。この点を踏まえておくことは「宇宙における抑止」を考える前提となる。

現状、宇宙システムが担っている主な軍事的機能としては、①情報収集・警戒監視・偵察（ISR）、②通信、③測位・航法・時刻参照（PNT）、④ミサイル警戒、⑤環境モニタリング（気象観測など）がある[5]。これらの機能は地球上における核戦力や通常戦力の運用を支えるために使用されている[6]。

宇宙抑止は決して新しい概念ではないが、宇宙と抑止の関係性を考える重要性が世界的に増していることは間違いない。その背景には第１に、核戦力の運用のみならず通常戦力の運用においても宇宙システムの価値が高まっていることを受けて、抑止全体における宇宙システムの役割が増大しているということがある。

宇宙と抑止の関係性を考える意義が増している第２の背景は、宇宙システムの軍事的役割が拡

1　James P. Finch and Shawn Steene, “Finding Space in Deterrence: Toward a General Framework for ‘Space Deterrence’,” *Strategic Studies Quarterly*, Vol. 5, Issue 4, Winter 2011, pp. 12-13. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-4/FinchSteene.pdf

2　後述する同軌道型の攻勢的対宇宙能力は宇宙システムでもある。なお、「攻勢的対宇宙能力」は単に「対宇宙能力」と呼称される場合が多い。

3　これら２つの側面は密接な関係にある。抑止全体が強化されれば、宇宙システムに対する攻撃の抑止にもつながる。宇宙システムに対する攻撃を抑止することも、抑止全体の強化という点で重要である。

4　現状、リンクセグメントは主にダウンリンク（宇宙セグメントから地上セグメントに向けた信号）とアップリンク（地上セグメントから宇宙セグメントに向けた信号）で構成されているが、クロスリンク（宇宙セグメント内の衛星間でやり取りされる信号）も利用が拡大し始めている。

5　この他に宇宙システムは宇宙領域把握などに使用されることがある。

6　厳密に言えば、宇宙システムが提供する機能は宇宙システムの運用そのものにも使われている。例えば宇宙システムを用いたPNTサービスは、衛星の位置測定に使用される。この場合、衛星に搭載されたユーザー端末は、地上セグメントではなく宇宙セグメントに該当する。

大するにつれて、宇宙システムへの攻撃を抑止することの重要性が増しているということである[7]。これは宇宙システムの利用が妨げられることによって生じる軍事力・抑止力全体への影響がより深刻化しているためである。

関連して、宇宙システムを攻撃する兵器である攻勢的対宇宙能力を研究・開発したり保有したりする国が増えており、宇宙システムが実際に攻撃を受けるリスクが高まっているという事情がある。攻勢的対宇宙能力には、主として①直接上昇（direct-ascent）、②同軌道（co-orbital）、③指向性エネルギー（directed energy）、④電子戦（electronic warfare）、⑤サイバーという区分が存在する[8]。

①は陸海空のプラットフォームから発射するミサイルに搭載した迎撃体の直撃で衛星を破壊する兵器である。②はいったん軌道に投入された後、目標衛星に接近して破壊的・非破壊的な手段で攻撃する兵器である。③はレーザーや素粒子、マイクロ波といった指向性エネルギーで宇宙システムに干渉したり宇宙システムを破壊したりする兵器である。④は無線周波数エネルギーで衛星との通信を妨害する兵器である。⑤はソフトウェアおよびネットワーク関連技術でコンピューター・システムに不正侵入したりコンピューター・システムを妨害したり破壊したりする兵器である。

宇宙と抑止の関係性を考えることは、日本にとっても重要である。日本は防衛目的の宇宙利用を拡大しているのみならず、防衛省が自ら衛星を保有するようになっている。防衛省は2017年と2018年にXバンド防衛通信衛星を１機ずつ打上げており、2023年度には３機目の打上げを予定している。これらは防衛省が初めて保有する衛星である[9]。防衛省は更に2026年度までに宇宙領域把握を行うための衛星を打上げることや、情報収集・警戒監視・偵察・ターゲティング（ISRT）のための衛星コンステレーションを整備することを計画している。自衛隊の部隊運用において宇宙システムが果たす役割が増しており、日本はこうした宇宙システムに対する攻撃をいかに抑止するかということを考えなければならない状況にある[10]。とりわけ2022年末に閣議決定された「国家安全保障戦略」では日本への侵攻を抑止する上でスタンド・オフ防衛能力などを活用した反撃能力が鍵を握るとの認識が示されたことから[11]、こうした能力の運用に欠かせないISRTを提供する衛星コンステレーションへの攻撃を抑止することもまた、重要な課題となるだろう。

本稿の構成は次の通りである。第１節では、宇宙と抑止の関係性について、冷戦期から現在にいたる歴史的経緯を振り返る。第２節では、2022年２月に始まったロシアによるウクライナへの本格的な侵略とそれに対するウクライナの抗戦（以下、ロシア・ウクライナ戦争と呼称）を事例

7　付言すれば、経済・社会活動における宇宙システムの役割も世界的に増大している。普段ほとんど意識されることはないが、宇宙システムを用いた気象観測や放送、PNTは日常生活に深く組み込まれている。今後は携帯電話による衛星通信の利用が普及していく可能性もある。こうしたことから経済・社会活動に使われる宇宙システムへの攻撃を抑止することの意義も高まっている。

8　Secure World Foundation, *Global Counterspace Capabilities: An Open Source Assessment,* April 2023, p. xxxvi. https://swfound.org/counterspace/

9　これらの衛星の管制は、プライベート・ファイナンス・イニシアティブにより民間会社に委託されている。

10　青木節子氏は、宇宙での抑止と抑止が破られた場合の対応を日本は整理する必要があると指摘する。平和・安全保障研究所「RIPS秋季公開セミナー2019 宇宙の安全保障と日本の役割」2019年10月７日。https://www.rips.or.jp/symposium/2066/

11　内閣官房「国家安全保障戦略について」2022年12月、17頁。https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf

として、宇宙と抑止の関係性を考察する。第3節では、「宇宙における抑止」に焦点を当てた上で、いかに抑止を追求するかを考察するとともに、宇宙システムのレジリエンスと防護（protection）の重要性を指摘する。

1．歴史的経緯

（1）冷戦期における宇宙と抑止

まず冷戦期の「抑止における宇宙」、すなわち抑止全体における宇宙システムの役割を振り返った場合、宇宙システムは核抑止力の不可欠な構成要素であったということができる。当時、米ソが開発・配備した軍事衛星の多くは、核抑止力を維持・向上させるためのものであった。具体的には核兵器で狙う攻撃目標に関する情報収集、そうした情報収集を行う画像偵察衛星の運用に不可欠な気象情報の収集[12]、敵対国が発射した弾道ミサイルの早期探知、核戦力の指揮・統制に用いる通信、潜水艦から弾道ミサイルを発射する際に必要となる測位、核爆発の探知といった用途のために軍事宇宙システムが用いられていた[13]。他方で、通常戦力を用いた抑止（通常抑止）への貢献は限定的であった。冷戦の後半においては米ソともに通常戦力の運用への宇宙システムの組み込みを始めたものの、そうした組み込みは部分的なものにとどまった。

次に、冷戦期の「宇宙における抑止」、すなわち宇宙システムに対する攻撃の抑止は、基本的に核抑止と一体であった[14]。米ソが運用する軍事宇宙システムの多くは上述の通り核戦力の運用を支えるために用いられていたことから、軍事宇宙システムへの攻撃は核戦争に発展する恐れがあると認識されていた。このため核抑止が成立している限り、軍事宇宙システムへの攻撃を懸念する必要性は低い状況にあった。

（2）ポスト冷戦期における宇宙と抑止

ポスト冷戦期の「抑止における宇宙」については、米国にとっての通常抑止における宇宙システムの役割が顕著に拡大したことを指摘できる。これは1991年の湾岸戦争を契機として同国が宇宙システムを通常戦力の運用に本格的に組み込み始めたことによる[15]。プレデターやグローバルホークといった滞空型無人航空機の運用における衛星通信の利用や、統合直接攻撃弾などを用いた精密打撃における全地球測位システム（GPS）の利用はその象徴的な例である。

このように宇宙システムの果たす軍事的役割が拡大した一方で、ポスト冷戦期においては「宇宙における抑止」、すなわち宇宙システムへの攻撃を抑止する必要性は切迫しなかった。ソ連崩壊後、ロシアによる攻勢的対宇宙能力の開発・配備は停滞した。その他の国家による攻勢的対宇宙能力の開発・配備も活発化しなかった。また、この段階では米国以外の国々による通常戦力への宇宙システムの組み込みはそれほど進んでいなかった。そのため米国にとってもそれ以外の諸国にとっても宇宙システムへの攻撃を抑止することは差し迫った課題とはならなかった。

12　冷戦期に米ソが運用していた画像偵察衛星は主として光学センサーを用いたものであったため、対象地域が雲で覆われている場合は撮像ができなかった。このため予め対象地域の気象状況を把握する必要があった。

13　詳細は下記を参照。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、第2章。

14　Finch and Steene, “Finding Space in Deterrence,” p. 10.

15　詳細は下記を参照。福島『宇宙と安全保障』第3章。

（３）2000年代半ば頃からの宇宙と抑止

ポスト冷戦期の状況が変化し始めたのは2000年代半ば頃からであり、より本格的な変化が生じ始めたのは2010年代に入ってからのことである。「抑止における宇宙」について考えた場合、通常抑止における宇宙システムの役割はポスト冷戦期に引き続き拡大している。米国のみならずフランスやロシア、中国なども通常戦力の運用への宇宙システムの組み込みを進めてきた。

とりわけ中国は2015年に宇宙、サイバー、電子戦を担う戦略支援部隊を中央軍事委員会直轄の部隊として創設し、各種の作戦を支援する体制を強化してきた。中国が保有・運用する衛星の数も、ロシアを抜き米国に次ぐ規模（米中ロはそれぞれ3433機、541機、172機、2022年４月末時点）にまで拡大している[16]。海洋偵察などに用いられているとみられる「遥感」の衛星コンステレーションは、中国のいわゆる接近阻止／領域拒否（A2/AD）能力を構成するものであり、対艦弾道ミサイルなどと組み合わせて運用されることで、米国などが台湾海峡有事に軍事介入することを抑止する役割を担っていると考えることができる。更に、中国が有する攻勢的対宇宙能力もまた、A2/AD能力として米国などによる軍事介入を抑止する役割を有しているとみられる。

こうした中、「宇宙における抑止」という側面においては、宇宙システムへの攻撃を抑止する必要性が高まっている。これは攻勢的対宇宙能力の研究・開発、実験、配備、使用が顕著になってきたためである[17]。2003年のイラク戦争では、イラクが電子戦兵器により米軍のGPS利用を妨害しようと試みた。これは米軍が戦闘作戦（combat operations）の最中にGPS利用への妨害を受けた初めての事例であったとされる。更に2007年には中国が直接上昇兵器を用いた初の衛星破壊実験に成功した。米ソも冷戦期に衛星破壊実験を行っていたが、1990年代以降は実験を行っていなかった。中国は冷戦後としては世界で初めて衛星破壊実験を成功させ、世界で３番目に衛星破壊能力を実証した国となった。米国防省国防次官室（政策担当）で宇宙政策と戦略の策定を担っていたJ・フィンチ（James Finch）とS・スティーネ（Shawn Steene）によれば、中国による衛星破壊実験は、西側諸国の研究者達が衛星破壊能力の使用をいかにして紛争時に抑止するかを検討し始める契機となった[18]。

その後も意図的な衛星破壊は継続してきた。2008年には米国が管制不能となっていた自国の偵察衛星を地球への再突入前に処分するために直接上昇兵器で破壊した[19]。この行為を米国政府は衛星破壊実験と位置付けてはいないが、翌2009年の論文で米国防省の国防次官（政策担当）であったM・フロノイ（Michele Flournoy）と国防長官府でストラテジストを務めていたS・ブリムリー（Shawn Brimley）は、米国の対衛星能力を示すものであったとの認識を示した[20]。2019年にはインドが直接上昇兵器により衛星破壊実験に初成功した。2021年にはロシアが同国にとって冷戦後初の衛星破壊実験を実施した。更に次節で詳述する通り、ロシア・ウクライナ戦争では双

16　Union of Concerned Scientists, *UCS Satellite Database*, Updated May 1, 2022. https://www.ucsusa.org/resources/satellite-database

17　詳細は下記を参照。福島『宇宙と安全保障』第４章。

18　Finch and Steene, “Finding Space in Deterrence,” p. 10.

19　米国政府は特別な改修を施したイージス艦とスタンダード・ミサイル３を衛星破壊に使用した。Nicholas L. Johnson, “Operation Burnt Frost: A View from Inside,” *Space Policy*, Vol. 56, May 2021, p. 4.

20　Michele Flournoy and Shawn Brimley, “The Contested Commons,” *Proceedings*, Vol. 135, No. 7, July 2009. https://www.usni.org/magazines/proceedings/2009/july/contested-commons ただし、フロノイとブリムリーは米国が衛星破壊を実施した際はまだ民間人であった。

方が攻勢的対宇宙能力を実戦で使用している。

2. ロシア・ウクライナ戦争における宇宙抑止

（1）抑止における宇宙

ウクライナとその支援国の視点でみた場合、ロシアによるウクライナへの本格的な侵略の開始を抑止することはできなかった。他方で、ロシアによる核攻撃は今のところ起きていない。このことは米国などによる対露核抑止が機能していると推定できる。宇宙システムは核戦力の指揮・統制・通信（NC3）に関わる機能を提供することで、核抑止に貢献している[21]。

また、ウクライナを支援している国家、特に北大西洋条約機構（NATO）加盟国へのロシアによる通常戦力での攻撃も起きていない。このこともまた、NATO諸国の核戦力や通常戦力などを用いた対露抑止が機能している可能性を示唆している。この点においても宇宙システムは核戦力や通常戦力のより効果的な運用を可能にすることで、ロシアに対する抑止に貢献している。

ただし、自明のことながら宇宙システムのみで抑止力を発揮しているわけではない。あくまで宇宙システムはほかの戦力と一体となって抑止力となる。米宇宙軍のC・ソルツマン（Chance Saltzman）宇宙作戦部長は2022年11月のインタビューで、悪い例えであると断った上で、同軍はケーキを作る際の卵のような存在であり、小麦粉と混ぜ合わせて初めてケーキとなることを強調している[22]。

（2）宇宙における抑止

同じくウクライナとその支援国の視点でみた場合、ウクライナが使用する宇宙システムに対するロシアのサイバー攻撃や電子戦兵器を用いた攻撃を抑止することはできなかった。ロシアは2022年２月に地上侵攻を始める直前に、米ヴァイアサット社の静止衛星KA-SATを用いた通信システムへのサイバー攻撃を行い、ウクライナ軍の指揮・統制に対する妨害を図ったとみられている[23]。また、ロシアはウクライナにおいて、米スペースX社が提供する衛星通信サービスであるスターリンクへのサイバー攻撃やジャミング[24]、更にはGPSのダウンリンク信号へのジャミングを行っているとされる[25]。

GPSのダウンリンク信号へのジャミングは全面侵略が始まる前からウクライナで起きていたこ

---

21 米国のNC3ネットワークの現状と宇宙システムの役割については下記を参照。Marie Villarreal Dean, “U.S. Space-Based Nuclear Command and Control: A Guide,” Center for Strategic and International Studies, January 13, 2023. http://aerospace.csis.org/wp-content/uploads/2023/01/130223_MV_SpaceNuclearFinal.pdf

22 Tobias Naegele, “Q&A: The New Chief of Space Operations on Empowering the Force,” *Air and Space Forces Magazine*, November 27, 2022. https://www.airandspaceforces.com/qa-the-new-chief-of-space-operations-on-empowering-the-force/

23 Viasat, Inc., “KA-SAT Network Cyber Attack Overview,” March 30, 2022. https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview; Antony J. Blinken, “Attribution of Russia’s Malicious Cyber Activity Against Ukraine,” U.S. Department of State, May 10, 2022. https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/

24 E・マスク（Elon Musk）氏による2022年５月11日付のツィート。

25 Bryan Clark, “The Fall and Rise of Russian Electronic Warfare,” *IEEE Spectrum*, July 30, 2022. https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare

とを考えれば[26]、全面侵略開始後にそうした攻撃を抑止できなかったことは何ら驚きではない。また、GPSは米軍が運用しているシステムであり、KA-SATやスターリンクも米国企業のものであるが、ダウンリンク信号を対象とした電子攻撃やユーザー端末へのサイバー攻撃は比較的影響が局所的であることから攻撃の敷居が高いとは言い難い[27]。宇宙システムを構成する３つのセグメントという観点でみた場合、地上セグメントとリンクセグメントに対する攻撃を抑止することはできなかった。

一方で、これまでのところロシアによる宇宙セグメントへの攻撃、すなわち直接上昇兵器や同軌道兵器、指向性エネルギー兵器、サイバー兵器を用いた衛星に対する破壊的・非破壊的な攻撃は確認されていない。2022年４月時点におけるインタビューではあるが、米宇宙軍（Space Force）のD・トンプソン（David Thompson）宇宙作戦副部長は、ロシアはGPS衛星を攻撃していないと述べている[28]。スターリンク衛星や商業地球観測衛星に対する攻撃があったという指摘も今のところない。

衛星攻撃が確認されていないのは、ロシアに対する抑止が効いていると考えることもできる。１つには懲罰的抑止が効果を発揮しており、米国などから何らかの対抗措置を受けることを恐れて、ロシアが衛星攻撃を躊躇している可能性がある[29]。ウクライナが利用している衛星は、ほぼ全て米国をはじめとする他国の政府や企業が保有・運用しているものである[30]。米国防省が2020年に公表した「防衛宇宙戦略」（要旨）は、命令に基づき商業宇宙能力も防護・防衛する準備を行うと記載しており、GPSのような政府の衛星のみならず商業衛星に対する攻撃があった際にも米軍が何らかの対抗措置を取る可能性が明示されている[31]。

２つ目の可能性は拒否的抑止が機能しており、衛星攻撃を行っても成果が限られているとロシアが判断して攻撃を行っていないというものである。GPSやスターリンクの衛星コンステレーションはそれぞれ数十機、数千機の衛星で構成されていることから、一部の衛星を無力化しても衛星コンステレーション全体としてはサービスを継続し得る。

---

26 小泉悠『現代ロシアの軍事戦略』筑摩書房、2021年、電子版；Joseph Trevithick, “Ukrainian Officer Details Russian Electronic Warfare Tactics Including Radio ‘Virus’,” *The Drive*, October 30, 2019. https://www.thedrive.com/the-war-zone/30741/ukrainian-officer-details-russian-electronic-warfare-tactics-including-radio-virus

27 ただし、KA-SATを用いた通信ネットワークへのサイバー攻撃の影響はウクライナにとどまらずほかの欧州諸国にも及んだ。また、スターリンクへのサイバー攻撃については、地上セグメントのうちユーザー端末を対象としたものなのか衛星を管制する地上局を対象としたものなのか、宇宙セグメントを狙ったものなのか、あるいは、それら全てを対象としたものなのかといった詳細は明らかになっていない。

28 Tracy Cozzens, “Russia Interfering with GPS in Ukraine, Pentagon Says,” *GPS World*, April 13, 2022. https://www.gpsworld.com/russia-interfering-with-gps-in-ukraine-pentagon-says/

29 鈴木一人氏は米国が自衛権を主張して介入してくる可能性を排除できない限り、ロシアは商用衛星であったとしても攻撃を躊躇すると指摘する。内閣府「宇宙分野報告 プロジェクト・マネージャー 鈴木一人 東京大学公共政策大学院教授」令和３・４年度内閣府委託事業「我が国が戦略的に育てるべき安全・安心の確保に係る重要技術等の検討業務」2022年３月28日。https://www8.cao.go.jp/cstp/stmain/pdf/20230314thinktank/siryo4.pdf

30 ウクライナの官民が保有・運用している衛星は2022年４月末時点で２機のみである。Union of Concerned Scientists, *UCS Satellite Database*.

31 U.S. Department of Defense, *Defense Space Strategy, Summary*, June 2020, p. 2. https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_DEFENSE_SPACE_STRATEGY_SUMMARY.PDF

尤も、対露抑止が効いているのではなく、単にロシアには衛星攻撃をするつもりがない、あるいは衛星への攻撃は起きているが公表されていないという可能性もあるだろう。更に、今後ロシアが他国企業の衛星を破壊したとしても驚きはない。そうした攻撃によってサービスを停止させられる可能性が低い場合でも、企業をウクライナへの支援から遠ざけるために、牽制として実施する可能性は否定できない。ロシアが2021年11月に衛星破壊実験を実施したことは既述の通りである。迎撃目標となる衛星が周回している高度にもよるが、副次的に発生する宇宙ゴミがほかの衛星の運用に与える影響を考慮して、ロシアが衛星破壊を躊躇するとは考え難い。

なお、米国政府は2022年４月に破壊的な直接上昇対衛星ミサイル（destructive direct-ascent anti-satellite missile）の試験を実施せず、かつ、こうしたコミットメントを宇宙における責任ある行動に関する国際行動規範として追求していくことを宣言した[32]。米国の呼び掛けを受けて、翌2023年４月までに12カ国が類似の宣言を行っている[33]。だが、ロシアがこうした宣言を行う見通しは立っておらず、米国などによる宣言の対象も試験に限られている。こうした国際規範を形成する取り組みは宇宙活動の持続性を維持する上で重要な意義を有しているが、ロシアに対する抑止力の補完として機能する可能性は、少なくとも当面は限定的であると言わざるを得ない。

3. 今後の検討課題

（１）いかにして「宇宙における抑止」を追求するか。

「抑止における宇宙」、すなわち宇宙システムが抑止全体において果たす役割が世界的に増大する中、そうした役割を宇宙システムが発揮する前提として「宇宙における抑止」を追求する重要性が増している。それでは、いかにして「宇宙における抑止」を追求すべきなのであろうか。

宇宙における抑止を成立させるためには、次の点を考慮することが必要である。１つは能力の保有と誇示である。能力の例としてはレジリエンス・防護、報復、宇宙領域把握に関わる能力がある。宇宙システムのレジリエンスや防護に関わる能力を保有するとともに、そうした能力を有していることを対外的に示すことは、拒否的抑止に貢献する。また、報復能力を保有するとともに、そうした能力を有していることを対外的に示すことは、懲罰的抑止につながる。宇宙領域把握はレジリエンス・防護、報復に関わる能力の基盤になるとともに、宇宙システムへの攻撃を把握する能力があることを示すことで「探知による抑止」に活用できる。ただし、いずれの能力に関しても秘匿と誇示のバランスを考える必要がある。能力の存在を敵対者が認識しなければ抑止は難しい。他方で、能力を明らかにし過ぎてしまった場合、敵対者が予め対抗措置を取る恐れがある。

更に、懲罰的抑止を追求するにあたっては、報復能力を使用する決意を前もって敵対者に伝達しておかなければならない。米国のC・フォード（Christopher Ford）国務次官補（国際安全保

32 The White House, “FACT SHEET: Vice President Harris Advances National Security Norms in Space,” April 18, 2022.
https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/18/fact-sheet-vice-president-harris-advances-national-security-norms-in-space/

33 Mike Wall, “３ More Countries Pledge Not to Conduct Destructive Anti-Satellite Tests,” *Space.com*, April 11, 2023.
https://www.space.com/netherlands-italy-austria-destructive-asat-pledge

障・不拡散担当）が2020年の講演で、米国のNC3アーキテクチャーは宇宙システムにある程度依存していると述べ、関連する宇宙システムへの攻撃は非核攻撃の場合でも米国による核報復を招くことを公の場で示唆したことは、決意伝達の例である[34]。更に、NATOと日米がそれぞれ2021年と2023年に、宇宙への、宇宙からのまたは宇宙における攻撃が北大西洋条約と日米安全保障条約の第５条の発動につながり得ると表明したことは重要である[35]。なお、報復能力を使用する決意を伝達するにあたっては、曖昧性と具体性のバランスを考慮する必要がある。内容が曖昧過ぎた場合は決意が十分に伝わらない可能性がある一方で、具体的過ぎれば敵対者がそうした内容を回避する形で攻撃を行う恐れがある。

３つ目は領域横断（クロスドメイン）で抑止を追求することである[36]。宇宙システムに対する攻撃を抑止する取り組みは宇宙領域のみで完結しない。宇宙システムが機能するためには宇宙セグメントのみならず地上セグメントとリンクセグメントも正常に稼働しなければならず、これらのセグメントに対する攻撃の抑止も追求する必要がある。加えて、宇宙システムの各セグメントへの攻撃は領域横断で行われ得る。例えば衛星に対する攻撃は、宇宙領域からだけではなく陸海空やサイバー空間から行われる可能性がある。

更に、拒否的抑止を考えた場合、宇宙システムが提供している軍事的機能（例えばISRや通信、PNT）を陸海空といった他領域上のシステムで補完することが抑止力の向上につながり得る。懲罰的抑止に関しても、例えば衛星に対する攻撃に対して衛星攻撃で報復するだけではなく、陸海空やサイバー空間を通じた報復も行う決意を示すことが抑止力の向上に資する可能性がある。この点、米国は「国家宇宙政策」を通じて、宇宙システムに対する攻撃への対応は必ずしも対称的なものではなく宇宙領域に限定しない方針を明示している[37]。

---

34 U.S. Department of State, “Whither Arms Control in Outer Space? Space Threats, Space Hypocrisy, and the Hope of Space Norms,” Remarks by Dr. Christopher Ashley Ford, Assistant Secretary, Bureau of International Security and Nonproliferation, at Center for Strategic and International Studies Webinar on “Threats, Challenges and Opportunities in Space,” Washington, DC, April 6, 2020.
https://2017-2021.state.gov/whither-arms-control-in-outer-space-space-threats-space-hypocrisy-and-the-hope-of-space-norms/index.html

35 具体的な内容は次の通りである。“We consider that attacks to, from, or within space present a clear challenge to the security of the Alliance, the impact of which could threaten national and Euro-Atlantic prosperity, security, and stability, and could be as harmful to modern societies as a conventional attack. Such attacks could lead to the invocation of Article 5. A decision as to when such attacks would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis,” North Atlantic Treaty Organization, *Brussels Summit Communiqué*, Issued on June 14, 2021, Last updated: July 1, 2022. https://www.nato.int/cps/en/natohq/news_185000.htm;「閣僚は、宇宙への、宇宙からのまたは宇宙における攻撃が、同盟の安全に対する明確な挑戦であると考え、一定の場合には、当該攻撃が、日米安全保障条約第５条の発動につながることがあり得ることを確認した。閣僚はまた、いかなる場合に当該攻撃が第５条の発動につながることがあり得るかは、ほかの脅威の場合と同様に、日米間の緊密な協議を通じて個別具体的に判断されることを確認した。」外務省「日米安全保障協議委員会（２＋２）共同発表」仮訳、2023年１月、４頁。
https://www.mofa.go.jp/mofaj/files/100444893.pdf

36 Benjamin W. Bahney, Jonathan Pearl, and Michael Markey, “Antisatellie Weapons and the Growing Instability of Deterrence,” Jon R. Lindsay and Erik Gartzke, eds., *Cross-Domain Deterrence: Strategy in an Era of Complexity*, Oxford University Press, 2019, p. 137.

37 The White House, *National Space Policy of the United States of America*, December 9, 2020, p. 4.
https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/12/National-Space-Policy.pdf

（２）「宇宙における抑止」の限界とレジリエンス・防護の重要性

ただし、宇宙システムに対する攻撃の抑止を追求したとしても、抑止には限界があることにも留意しなければならない。抑止を追求することが重要であることと、それが実際にどこまで実現可能かという点は切り分けて考える必要がある。上述した通りロシア・ウクライナ戦争では宇宙システムのリンクセグメントに対する電子戦兵器を用いた攻撃や地上セグメントへのサイバー攻撃が確認されている。こうした攻撃は有事に限らずみられるものであり、抑止を成功させる敷居は高い。また、衛星に対する攻撃（特に衛星破壊）は未だ確認されていないが、衛星攻撃能力を有する国家は増加していることから、いつ攻撃が行われたとしても驚きではない。そのため抑止に失敗して宇宙システムが攻撃を受けたとしても宇宙利用を継続できるようにレジリエンスと防護の向上に取り組むことが重要である。

このような観点において、ロシア・ウクライナ戦争は重要な示唆をもたらしている。ロシアによる宇宙システムへの攻撃が行われてきたことは既述の通りであるが、そうした状況下でもウクライナは宇宙の軍事利用を継続できている。こうした事実は宇宙システムのレジリエンスと防護の重要性を示すものである。

米宇宙軍によれば、宇宙システムのレジリエンスを確保する措置には「disaggregation」、「distribution」、「diversification」、「proliferation」、「deception」がある[38]。「disaggregation」は諸々の能力を異なるプラットフォームやペイロード、地球上の場所・軌道に分離することを意味する。「distribution」は単一のノードとして同一ミッション・機能を遂行するために、連携して機能する多数のノードを活用することを指す。「diversification」は異なるプラットフォームや軌道を利用したり、パートナーシップを通じて能力を活用したりすることにより、同一のミッションに多様な方法で寄与することを意味する[39]。「proliferation」は同一ミッションを遂行するために、同種のプラットフォームやペイロード、システムを多数配置することである。「deception」は位置、能力、運用状況、ミッションの種類、アセットの堅牢性といった点に関して、敵対者を混乱・誤解させるための行動やシステムの実施を指す。上記の分類に基づけば、ウクライナ軍がKA-SATを使用できなくなった後にスターリンクを使用して衛星通信を使い続けたことは「diversification」に該当するだろう。

加えて、米宇宙軍によれば、宇宙システムの防護措置には電磁スペクトラム作戦、移動・マヌーバー、硬化、サイバーセキュリティがある[40]。スターリンクが電子戦兵器による攻撃やサイバー攻撃を受けながらもウクライナにおけるサービスを継続していることは、防護措置が効果を発揮していると考えることができる。

---

38 U.S. Space Force, *Operations*, Space Doctrine Note, January 2022, p. 14. ただし、米国防長官府の本土防衛・グローバル安全保障担当国防次官補室が2015年に作成した宇宙システムに関するレジリエンスの分類において、防護はレジリエンスを確保するための措置の１つとして位置付けられている。Office of the Assistant Secretary of Defense for Homeland Defense and Global Security, U.S. Department of Defense, *Space Domain Mission Assurance: A Resilience Taxonomy, A White Paper*, September 2015, p. 6.

39 「diversification」については米国防長官府による定義も参照している。Office of the Assistant Secretary of Defense for Homeland Defense and Global Security, *Space Domain Mission Assurance*, p. 7.

40 U.S. Space Force, *Operations*, p. 14.

おわりに

本稿では、宇宙と抑止の関係性について、冷戦期から現在にいたる歴史的経緯を振り返った後、ロシア・ウクライナ戦争を事例として取り上げて考察を行った。最後に、宇宙システムに対する攻撃の抑止に焦点を当てた上で、抑止を追求するにあたり考慮すべき点を列挙するとともに、抑止の限界を踏まえてレジリエンスと防護に取り組むことの重要性を指摘した。

本稿の冒頭で述べた通り、日本の防衛において宇宙システムが果たす役割が拡大しており、宇宙システムに対する攻撃の抑止を追求することは日本にとっても重要な課題となっている。同時に、宇宙システムのレジリエンスと防護に日本も取り組んでいかなければならない。この点に関して2022年に閣議決定された「国家防衛戦略」では、宇宙アセットの抗たん性強化に努めることが明記されている[41]。このような取り組みを進めるにあたっては、ウクライナ軍にみられるように、商業宇宙サービスを効果的に活用していくことに留意する必要があるだろう[42]。

41　防衛省「国家防衛戦略について」2022年12月16日、19頁。
https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy.pdf

42　ただし、特定の商業宇宙サービスに依存することのリスクもロシア・ウクライナ戦争は示している。

第四章　サイバー空間における抑止の在り方と課題

時藤和夫

はじめに

サイバー空間は情報通信技術の発展とグローバルな環境から日々刻々と進化している。2022年２月に本格化したロシアによるウクライナ侵攻においては、サイバー空間における攻防の戦いが具体的に繰り広げられており、サイバー空間がレイヤーを立体的に拡大していることを実感する。本章においては、サイバー空間と抑止について考察し、本研究会における議論やシナリオゲームを通じて得た知見として、その特徴と実例等から抑止の在り方と課題について述べる。

1．サイバー空間と抑止

抑止は「報復の脅威が現実に存在すること、意図する行動は成功しないこと、コストが行動によって得られる利益を上回るということを相手に信じ込ませること[1]」とされる。つまり、相手がその合理性を理解し、我が方がその能力を保有し、信憑性をもって相手に伝えるコミュニケーション能力が必要[2]となる。サイバー空間では抑止は拒否的抑止と懲罰的抑止が主に議論[3]されるが、サイバー空間の広がりとともに幅広い抑止の概念[4]にも着目する必要がある。ここでは抑止の目的を紛争の抑止として捉え、サイバー攻撃そのものを抑止するという考え方に拘らないこととした。

（１）サイバー空間の特徴

インターネットに代表されるサイバー空間は、IPプロトコルによって接続された世界規模のネットワークであり、その管理は米国政府からの委託を受けたプロジェクトであるICANNが割り当て管理を行っている[5]。接続端末としては、2018年当時で220億台に達しており、2023年現在は330億台と予測されている[6]。インターネットは一般に開放されたネットワークであることから、その特徴は管理が非中央集権的であり、匿名性から民間・軍事の区別が混然とし、多様なアクターが存在することから様々なサイバー攻撃が常時行われている現状にある。これまでは軍用ネットワークとインターネットは一線を画していたが、ウクライナ侵攻においてウクライナが使

1　Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option*, Lanham, Maryland: Rowman & Littlefield, 2017, p. 60.
2　Joint Chiefs of Staff, “Joint Publication 3-0: Joint Operations”, January 17, 2017, xxii.
3　栗田真広「サイバー攻撃に対する「抑止」の現状」国立国会図書館調査及び立法考査局『情報通信をめぐる諸課題』2015年３月、158-161頁。
4　Frans Osinaga and Tim Sweijs, eds., *Deterrence in the 21st Century: Insights from Theory and Practice*, The Hague, The Netherlands: T.M.C. Asser Press, 2021, pp. 148-150.
5　日本ネットワークインフォメーションセンター（JPNIC）「インターネットとは」2002年11月28日。https://www.nic.ad.jp/ja/basics/beginners/internet.html
6　Help Net Security, “Number of connected devices reached 22 billion, where is the revenue?,” May 23, 2019. https://www.helpnetsecurity.com/2019/05/23/connected-devices-growth/

用した砲兵管理システム（GIS ARTA）[7]に見られるように、偵察用ドローンやスマートフォンなどから送られた戦場のデータによって敵の位置を特定し、その地域にある最も攻撃に適している兵器を短時間に割り当てる機能は効果を上げており、インターネットの軍用分野への利用も現実味を帯びるようになってきた。

また、インターネットに直接接続されていないシステムであっても、IPプロトコルによってクローズな環境で運用されているシステムが大半であり、例えばUSBメモリを介した不正情報の入出力や、パソコンや携帯端末の音声機能を利用して可聴域外の音声でデータ通信を試みる技術[8]などでインターネットとの接続を可能にする方法なども出現しており、クローズなシステムが安全であるというこれまでの認識だけではサイバー攻撃を完全に防護できない状況になってきた。更に、匿名性により攻撃元を特定することが困難とされるアトリビューション（帰属）問題[9]は、懲罰的抑止に大きく影響している。

（２）抑止におけるサイバー空間

紛争を抑止するためにサイバー空間の果たすべき役割を考えると、サイバー攻撃から自らのシステムを防護し機密情報の漏洩や重要インフラを含めたシステムの任務保障を確保することにより、防衛力低下を引き起こすことがないようにする重要な役割がある。更に、昨今ではデマや印象操作による社会の二分化や社会不安を煽るような情報発信を試みる認知領域においても、不正なアクセスから防護することの意義は大きく、その役割は大きい。

（３）サイバー空間における抑止

サイバー空間からサイバー攻撃そのものを抑止する効果については様々な議論があるが、新たな攻撃技術の進歩やブラックマーケット等により攻撃のためのマルウェアが容易に入手可能であること[10]や、サプライチェーンを含めてシステムが広範囲に接続される状況を考慮すると、システムを完全に防護する拒否的抑止は難しいと言われている。特に、国家等が主体となるサイバー攻撃に関しては、膨大な資源を攻撃のために費やすことから、一般的に公開されていないゼロデイ攻撃[11]の可能性もある。従って、侵入を前提とした運用管理や、常時サイバー攻撃のリスクを監視しておく必要性も増してきている。

2. サイバー空間の脅威

サイバー攻撃が一般的に認知され始めた2000年頃は、無差別に送信したメールでウィルスに感

---

7 'GIS "ARTA" automated command and control system', https://gisarta.org/en/index.html

8 Anfractuosity, "Ultrasound Networking", https://www.anfractuosity.com/projects/ultrasound-networking/

9 川口貴久「第２章 サイバー空間における安全保障の現状と課題：サイバー空間の抑止力と日米同盟」日本国際問題研究所『グローバル・コモンズ（サイバー空間、宇宙、北極海）における日米同盟の新しい課題』平成26年３月、11-26頁。https://www2.jiia.or.jp/pdf/resarch/H25_Global_Commons/03-kawaguchi.pdf

10 「情報セキュリティ10大脅威 2023」情報処理推進機構、2023年３月、52-53頁。https://www.ipa.go.jp/security/10threats/ps6vr70000009r2f-att/kaisetsu_2023.pdf

11 「実際にあったゼロデイ攻撃の被害事例まとめ」CyberSecurityTIMES、2020年６月12日。https://www.shadan-kun.com/blog/measure/6424/

染させデータの破壊や改ざんをするといった脅威があり、ウィルス対策ソフトによるスキャニングで十分予防できるレベルだった。その後、攻撃は次第に巧妙化し、2020年頃までには目立たない攻撃が主流となり、ランサムウェアや不正アクセスによる不正送金被害などが目立つようになった。2022年には企業ネットワークへの侵害経路が複雑化されたサイバー攻撃へと進化し、2023年にはWi-Fiの普及、クラウドやIoT等のITインフラの多様化を背景に、ランサムウェアの進化による更なる被害の増加や、サプライチェーンやアプリケーション・プログラミング・インター―フェース（API）[12]への被害の増加も予測されている。

（１）攻撃の分類

サイバー攻撃には様々な種類があり、常に進化している。特定のターゲットを狙った攻撃、不特定多数のターゲットを狙った攻撃、負荷をかける攻撃、脆弱性を狙った攻撃及びパスワード解析などに分類される[13]。特に、特定のターゲットを狙った攻撃としては、標的型攻撃、ランサムウェアやサプライチェーン攻撃等があり、侵入の為の情報収集から潜伏、システムの解析等高度なものが多く、その侵入は各段階に分かれている。

（２）サイバーキルチェーン

サイバー侵入の各段階をキルチェーンに例えて定義したモデルがある。2011年にロッキード・マーチン社が作成したこのモデルには、「偵察」、「兵器化」、「搬送（デリバリー）」、「エクスプロイテーション」、「インストール」、「遠隔操作」、「目標達成のための実行」の７段階に分かれている[14]。一連の攻撃プロセスを複数の段階に分けておくことで対策を考えやすくなる。このプロセスにおいては、攻撃者が次の各段階に進むには使用するツールやテクニックが必要であり、チェーンのどのリンクが途切れてもプロセス全体が中断されるという概念である。

このモデルを参考として、様々な修正も加えられている。例えば、デル社はサイバー攻撃を４つの基本的な段階として、「偵察」、「侵入」、「マルウェアの注入」、「痕跡除去」に分類しており、サービス拒否攻撃を包含するためにあえて侵入段階に絞ったロッキード・マーチン社の対象範囲を超えている点に特徴がある。また、サイバーリーズン社は、攻撃のライフサイクルに「外部偵察」、「突破」、「遠隔操作」、「拡散」、「横断的侵害」、「ダメージの付与」という６段階に分類している。テックトーク社は、ロッキード・マーチン社の７段階の次に、８段階目として「マネタイズ」を追加[15]した。これは、現代の脅威分析においてビットコイン等による身代金の支払い要求段階にあたる。

これらのサイバーキルチェーン・モデルは、悪意あるサイバー活動の解析及び詳細な診断を行うために活用されており、サイバー攻撃者がどのようにシステムに侵入するかを把握できるだけ

---

12 「APIの脆弱性はどの程度危険なのか、どうすれば攻撃を防げるのか」IT Media、2021年２月５日。https://atmarkit.itmedia.co.jp/ait/articles/2102/05/news104.html

13 「サイバー攻撃とは？その種類・事例・対策を把握しよう」Cyber Security.com、2023年１月17日。https://cybersecurity-jp.com/column/14651

14 Lockheed Martin, “THE CYBER KILL CHAIN.” https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

15 「サイバーキルチェーンとは？」TechTalk、2023年１月17日。https://techtalk.pcmatic.jp/?p=2443

でなく、それぞれの目的に応じて実施すべき最適なセキュリティ対策を見出すために有効に活用されている。

3. サイバー空間における攻防の比較

わが国が現状維持を戦略上の基本として、現状変革を試みる可能性がある国家からの挑戦を抑止することが重要であるとの観点から、「現状変革側から考えられる影響」と「現状維持側から考えられる影響」をそれぞれを比較し優位性を考察した。

（1）現状変革側の比較優位性

ア．民主的コントロールに基づく法的制約や道義的制約が少ない

現状変革側が権威主義国家であることから、民主的コントロールに基づく法的制約や道義的制約が乏しく、プライバシーを考慮しないデータ収集や利用ができることである。これは、個人のデータが組み込まれることで大きな効果をもたらすと考えられている今後のデータ・エコノミーの特性を考えれば、大きな意味を持つ可能性がある。

イ．情報操作による優位性がある

権威主義国家という政治体制に由来するものであるが、フェイクニュースなどの影響工作を国内外に対して行うことで、世論に自らに好ましい方向に操作していくことができる可能性が高い。例えば現在のロシアのウクライナ侵攻において、ロシアは様々なフェイクニュースを発信している。これは国際社会に対してはほとんど効果を発揮していないが、国内におけるプーチン政権への支持を維持することには成功している。

ウ．サイバー攻撃の特性を利用し易い

サイバー攻撃の多くは、相手の行動を麻痺・遅延させる特性を持つ。こうした特性は、素早い行動で既成事実化を図るような現状変革側の行動と親和性が高い。相手の行動を麻痺・遅延されることを重要なタイミングで実施させることができれば、現状変革のための行動は非常に容易になる。

（2）現状維持側の比較優位性

ア．真実の公表

「真実」を適切に公表すれば、国際社会の支持が集まりやすい。ロシアのウクライナ侵攻において、ウクライナが十全に活用しているといえる。これは、信頼性の高い「真実」を適切に公表できることが前提であり、民主主義国家にとって重要な比較優位である。

イ．トレースバック技術の発達

サイバー攻撃のアトリビューションにおいて重要な役割を果たすトレースバック技術[16]がある。サイバー攻撃がどこから行われているか迅速に識別できるようになれば、サイバー攻撃の抑

16　トレースバック研究ポータル。https://www.telecom-isac.jp/tb/

止・対処において重要な意味を持つことになる。従来のトレースバック・スキームでは成功率が低く、通信トラフィックのオーバーヘッドが高いことから、トレースバック機能が逆にサイバー攻撃の標的になる問題などがあった。最近では、これらを改善する技術も研究されている[17]。また、クラウド環境を駆使して大量のデータからAIを活用したサイバー攻撃検出の自動化[18]などもトレースバックに有効に活用されている。

ウ．インターネット重要機能の独占

ドメイン・ネーム・システム（DNS）サーバをはじめとしたインターネット基幹機能や管理運営組織は現状維持側が独占している。インターネットでの重要な役割を担うDNSやボーダー・ゲートウェイ・プロトコル（BGP）などはこれまで脆弱性なども指摘されていたが、DNSに関してはDNSSec[19]（DNS Security Extensions）などの信頼性を保証する規格の実装やインターネットサービスプロバイダ（ISP）の適切な設定[20]により改ざんや機能停止等のリスクは低減され、2015年のDNSルートサーバに対する分散型サービス拒否（DDoS）攻撃に関しても、DNSルートサーバの冗長性による圧倒的なリソースで殆ど影響は出ていない[21]。また、BGPに関しては、誤った経路情報を防止するリソース公開鍵基盤（RPKI）の規格[22]を導入することにより、徐々に解決される方向にあり、インターネットの安定運用に寄与している。

（３）不確実性の高いもの

ア．人工知能（AI）技術の活用

AI技術は米国がずっと先行してきたが、近年における中国の勃興には目覚ましいものがある。そのため、技術的な優位性をどちらが掴むかは現時点では判断が難しい。特に、2017年にGoogleとトロント大学の研究者によって開発されたTransformer[23]の手法を用いた言語モデルGPT（Generative Pre-trained Transformer）は、ここ数年で驚くような性能を発揮しており、Open AIが2020年にリリースしたChat GPTは会話できるサービスとして広く一般にも開放され、一つの現象にもなっている。中国からも注目[24]されており、本格的な実用化に向けては乗り越えるべき壁もあるが、今後、この技術を取り入れ戦力化することで大きく様相は変わる可能性がある。

---

17 Jie Ma, Wei Su, Yikun Li, and Fangtao Yao, “A Low-Overhead and High-Precision Attack Traceback Scheme with Combination Bloom Filters,” *Hindawi Security and Communication Networks*, Volume 2022, October 13, 2022, pp. 1-13.

18 Rob Mead, “How Azure Security Center automates the detection of cyber attack,” Microsoft Threat Intelligence Center, October 24, 2017.

19 三田村健史、佐藤新太「DNSSEC解説」『情報処理』Vol. 52 No. 9 、2011年９月、1158-1165頁。

20 日本レジストリサービス「Bot 経由でDNSサーバを広く薄く攻撃～DNS水責め攻撃の概要と対策～」。https://jprs.jp/related-info/guide/021.pdf

21 ZDNET「ルートネームサーバに攻撃―攻撃者の正体は不明」。https://japan.zdnet.com/article/35074787

22 R. Bush, “The Resource Public Key Infrastructure（RPKI）to Router Protocol,” RFC 6810, January 2013. https://www.rfc-editor.org/rfc/rfc6810.html

23 Ashish Vaswani, et al, “Attention Is All You Need,” 31st Conference on Neural Information Processing Systems, NIPS 2017, Long Beach. CA. USA.

24 「中国がチャットGPTに警戒感を高める「敏感な用語」について政府と異なる回答連発」『NEWSポストセブン』2023年３月19日。https://www.news-postseven.com/archives/20230319_1851569.html?DETAIL

AIに関する信頼性確保については様々な議論があるが、AIのリスク管理枠組み[25]なども参考になるだろう。

イ．サプライチェーンの再構築

ハードウェアやプラットフォームを含むソフトウェアにおいて、現状維持国家のみならず国際社会全体がどの程度中国に依存するかという勢力図は現在のところ予測困難であるが、それは今後の国際政治環境に大きく影響する。

4．ウクライナ侵攻におけるサイバー戦の考察

ロシアが軍事力を伴いウクライナの国境を越えて侵攻した。しかし、最初の侵害行為はその数時間前の前日に起こったと言われている[26]。それは、ウクライナのコンピューターに対して送られたサイバー兵器であり、既に他国によりその攻撃は観測されていた[27]。この戦いは、これまでとは異なる様相を呈しているが、侵攻後１年以上が過ぎても未だ終結には至っていない。ここで、この侵攻についてサイバー戦の視点から以下に考察する。

（１）非対称戦力

サイバー戦は低コストで技術的優位を保ち、時間的に効果が継続可能であることから、非対称的アプローチに適合しているといえる。非対称的アプローチは、自国の生存や死活的利益を守り抜こうとする強い意志を持つ敵対勢力によって採用された場合には、たとえ倫理や法律を巡る様々な批判にさらされながらも、無責任といえる行動をとることを厭わない。サイバー空間における非対称性は「防御に対する攻撃の優位性」という観点もある。

一般的には、攻撃者は一回のシステム内への侵入を成功させれば良いのに対し、防御する側ではあらゆる方面からの攻撃に備えて防御の層を構築しておかなければならない。つまり「攻勢作戦は低コストで利得が高く、防勢作戦はコストが高く非効率」ということになる。このデジタル上で損害を与えるパワーを相手に見せつけ、コストを強要することにより強制的に譲歩を勝ち取ろうとする試みにも利用される。

2007年のロシアによるとみられるエストニアに対する大規模なサイバー攻撃に対しては、政府及び民間のウェブサイトがシャットダウンされるに至る重大な影響を及ぼしたものの、ネットワーク上の混乱は収束し、ロシアはエストニアから譲歩を引き出すことができなかった[28]。他方、エストニアはNATO加盟国であり、北大西洋条約第５条を発動すべく集団的自衛権の行使を要請したが、サイバー攻撃がロシアからと決め手となる証拠を見つけられなかったことから、武力攻撃に該当する閾値には至っていない。

ウクライナ侵攻に関しては、侵攻以前からロシアによるサイバー攻撃は行われていたが、ウク

25　NIST “Artificial Intelligence Risk Management Framework（AI RMF 1.0）,” NIST AI 100-1, January 2023.
26　スコット・ジャスパー著、川村幸城訳『ロシア・サイバー侵略：その傾向と対策』作品社、2023年３月１日。
27　ブラッド・スミス「ウクライナの防衛：サイバー戦争の初期の教訓」Microsoft Japan News Center、2022年７月４日。
https://news.microsoft.com/ja-jp/2022/07/04/220704-defending-ukraine-early-lessons-from-the-cyber-war/
28　ジャスパー『ロシア・サイバー侵略』、75頁。

ライナ側が攻撃を予め予測し攻撃直前にウクライナを攻撃するサイトを潰し、ネットワークに対する攻撃にはスターリンクによる代替手段の確保や、国家のデータを予めクラウドに退避することによりデータ破壊による機能不全を防ぐことができている。いずれの場合も、ロシア側がサイバー戦の非対称性の効果を最大限発揮できたとは言い難い。

（２）ハイブリッド戦

ハイブリッド戦では、敵対者は様々なアプローチを独自に組み合わせ、それを相手の弱点に向ける。多様な戦術や技術の中から最適な手段を選択し、自らの戦略文化や地理的特性、そして目的に適合した斬新な方法で各手段を融合する。ハイブリッド戦を構成する一つ一つの要素は必ずしも武力紛争レベルに至っているわけではない。ロシアには2013年に紛争における非軍事的ツールの重要性を強調した戦争の本質的な変化に関するゲラシモフ・ドクトリンがあり、2014年のクリミア併合の後、学者たちによりハイブリッド戦ドクトリンとして認知されている。現代戦のモデルによると、非軍事的手段と軍事的手段が概ね４対１の比率で遂行されるとされている。クリミア併合のツールとして用いられたサイバー作戦を分析する上で有益な概念である。

（３）情報戦

ウクライナ侵攻で明らかになったのは、ロシアがサイバー活動を情報戦という広範な領域のサブセットとして、時には促進剤として捉えていることであると、K・ジャイルズ（Keir Giles）は指摘している[29]。戦闘開始直後に行われたウクライナの国会議員の携帯電話や国家安全保障・国防会議のインターネットに対する妨害工作は、ウクライナ政府の意思決定に影響を及ぼす試みであった。これはロシアが虚偽のニュースやイデオロギー色の強い捏造したナラティブを使って民衆を操作するため、ロシアのテレビ番組や各種メディア機関を通じてプロパガンダを広める情報作戦が大々的に展開されている最中に行われた。サイバー作戦は、影響工作に不可欠な有益情報の窃取に重要な役割を果たしている。

サイバー戦は、武力侵攻未満の戦略・作戦環境を巧妙に作為し、被害国による対抗処置や国際社会からの処置から逃れる紛争の閾値を操作するためのツールになるが、紛争時には作戦支援やエスカレーション管理など、軍事能力に寄与するためのツールへと変化する。つまり、グレーゾーンにおける法的曖昧性と技術的複雑性によって作り出されてきた戦略は、武力侵攻の時点で失われてしまうことになる。これは、自らあからさまに武力侵攻を開始することで、爾後のサイバー行動は武力攻撃の一部と見なされ、西側諸国をはじめとする国際社会からは経済・金融制裁が科される等、ロシアは反撃や制裁を受けずに作戦目的を達成する機会を自ら閉ざした形となった。

5. サイバー戦能力の強化

わが国においては、これまでサイバー攻撃からの防護を主として実施してきた[30]。しかしなが

---

29 Keir Giles, “The Next Phase of Russian Information Warfare,” NATO Strategic Communications Centre of Excellence, May 20, 2016.
https://stratcomcoe.org/publications/the-next-phase-of-russian-information-warfare/176

30 閣議決定「サイバーセキュリティ戦略」令和３年９月28日。

ら、受動的な防護だけでは攻撃を受けてからの対処にならざるを得ず、早期対処にも限界があることから、能動的な防御の必要性が増してきた[31]。日々進化するサイバー攻撃技術による攻撃に対しては、従前の境界型セキュリティによる多重防御の絶対性に限界が見え始めており[32]、サイバー攻撃による侵入を前提としたセキュリティ対策の導入も既に一部では始まっている。

このような時代を背景に、2022年末に国家防衛戦略[33]をはじめとした戦略３文書が閣議決定された。特に領域横断作戦におけるサイバー戦能力においては、2027年度までに、サイバー攻撃状況下においても、指揮統制能力及び優先度の高い装備品システムを保全できる態勢を確立し、また防衛産業のサイバー防衛を下支えできる態勢を確立、概ね10年後までにはサイバー攻撃状況下においても、指揮統制能力、戦力発揮能力、作戦基盤を保全し任務が遂行できる態勢を確立しつつ、自衛隊以外へのサイバーセキュリティも支援できる態勢を強化する、とある[34]。

つまり、サイバー攻撃に対するレジリエンスを幅広い分野で確保していくことである。これは、サイバー攻撃によりシステム内部に侵入されたとしても、そのシステム本来が持つ目的を達成すべく、機能を一部縮退してでも継続して目的を達成することを示している。これら機能を具現化するために、防衛力整備計画[35]に示された以下の機能を充実させる必要がある。

（１）情報共有の促進

サイバー攻撃の39%がサイバー脅威インテリジェンスを共有することで阻止されているという[36]。サイバー空間における情報共有の必要性は、サイバー攻撃の状況を認識する上でも、また攻撃元の特定など、国内外を問わずあらゆる分野横断的な情報共有が重要である。しかしながら、情報を共有する上でしっかりとした情報管理は必須であり、そのためのセキュリティ・クリアランス制度の創設[37]が重要である。特に、制度が創設されてから具体的にシステム等へ実装にかかる時間を最小限に抑える必要性もあり、関連システムへの適用や認証・認可システムとの連携なども重要になる。

（２）能動的サイバー防御

能動的サイバー防御（Active Cyber Defense[38]）については、定義の幅も広く具体的にどこまでが該当するのかについて議論の余地がある[39]。攻撃者の意図、攻撃の機会、攻撃者の能力の要素の組み合わせについて、それぞれ積極的な対抗手段としての有効性を検討する必要がある。これらの情報を正確に収集することで攻撃者のプロファイリングを作成し、官民での情報共有をタ

31　The White House, “National Cybersecurity Strategy,” March 2023, pp. 14-15.
32　「ゼロトラストセキュリティを学ぶ　従来の境界型防御だけでは守れない企業システム」CYBERNET。https://www.cybernet.co.jp/zerotrust/learning/01.html
33　国家安全保障会議・閣議決定「国家安全保障戦略について」令和４年12月16日。
34　国家安全保障会議・閣議決定「国家防衛戦略について」令和４年12月16日。
35　国家安全保障会議・閣議決定「防衛力整備計画について」令和４年12月16日。
36　ジャスパー『ロシア・サイバー侵略』、222頁。
37　「国家安全保障戦略について」、24頁。
38　“National Security Strategy of Japan,” December 16, 2022, pp. 23-24.
39　佐々木勇人「『積極的サイバー防御』（アクティブ・サイバー・ディフェンス）とは何か―より具体的な議論に向けて必要な観点について」JPCERT/CC、2022年９月21日。https://blogs.jpcert.or.jp/ja/2022/09/active-cyber-defense.html

イムリーに行い、被害がどこで発生するか等の予測から被害の未然予防に向けた積極的な取り組みを実施することが一つの流れになる。それには、サイバー脅威情報を含めたオールソースの情報分析が重要である。

2018年の初めに、米国サイバー軍（U.S. Cyber Command）はより攻勢的なアプローチを採用する権限が与えられ、ネットワークやシステムの向こう側で攻撃者を探し出し、敵対者の活動により大規模な被害を受ける前に対抗するという前方防御（Defend forward）の姿勢を打ち出した。この概念は、敵の技術、手順や戦術を観察により敵のツールや兵器の解明にも有用になる[40]。このような機能を持つ部署との連携も重要である。

（３）サイバー空間における能力強化

サイバー空間は様々な情報通信技術で成り立っているが、新たな脅威に対する対策として以下の環境を導入し戦力化する必要がある。

ア．ゼロトラストの導入

従来の境界型セキュリティ対策は、保護すべきデータやシステムがネットワークの内側にあることを前提としていたが、クラウドの普及に伴いネットワーク上に保護すべきデータもある。ゼロトラストは、すべての通信を信頼しないことを前提にセキュリティ対策を講じることから、特に従来型からの移行を確実に行いつつ、ゼロトラスト成熟度モデル[41]等を参考に段階的かつ、そこにセキュリティホールが生じないようバランス良く整備する必要がある。

イ．リスク管理枠組みの導入

リスク管理枠組みは情報システムと共通の管理対策という２つの視点からリスクに対処する。情報システムについては、システムの運用または利用に必要な権限が付与され、それぞれセキュリティ・リスクとプライバシー・リスクに対応する。共通の管理対策については、指定された組織のシステム運用に必要な特定の管理対策を行う権限が付与される。セキュリティ管理対策にはシステムの機密性、完全性、可用性を保護するための対策があり、７つの基本的なステップから構成されている[42]。これは、様々なタイプのシステムに対応しており、システムが変わっても改修することなく適用できることから、個々に新たなリスク管理プロセスを必ずしも必要としない。今後多くのシステムを扱う管理のやり方に有効である。

ウ．サイバー・スレット・ハンティング

侵入した高度なマルウェアを検知し駆除する取り組みは、従来のウィルス対策ソフトウェアの検知が難しいものが増えている。マルウェアに感染していることを前提に調査を行うスレットハンティングの導入では、５段階の成熟度モデル[43]により専門部門と連携してレベルを上げていき、

40　ジャスパー『ロシア・サイバー侵略』、298頁。

41　“Zero Trust Maturity Model Version 2.0,” CISA, April 2023.

42　“Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,” NIST Special Publication 800-37 Revision 1, December 2018, pp. 8-12.

43　“A Framework for Cyber Threat Hunting,” sqrrl, White Paper, pp. 3-10.

スレット・インテリジェンスにフィードバックすることによって、更に優れた分析と予測が可能となるため、サイバー攻撃の阻止に有効である。

（４）サイバー空間の利用を妨げる能力の確保

相手方のサイバー空間の利用を妨げる能力[44]については、相手側の攻撃活動に直接影響を与えることから、サイバー攻撃に対する抑止は勿論、相手方の指揮統制・情報通信等を妨げる能力としても効果的である。そのためには、サイバー空間の状況認識、アトリビューション等から目標を選定し、能動的サイバー防御能力を含めたあらゆる能力を指向する必要がある。更に、相手の攻撃を事前に暴露することも一定の効果が見込まれる。これらは高度かつ実践的な能力が必要なため、事態に応じて有効な手段、時期、実施の程度や範囲などを、様々な部署とも連携して行う必要があり、役割・任務・能力に関する議論をより深化させるとともに、実践的な訓練を実施する必要がある。

（５）サイバー空間における法的整備の促進

サイバー国際法については明確には存在していないが、議論は継続している[45]。規範の参考となるタリン・マニュアル2.0は、解釈が複雑で曖昧さも議論になっている。しかしながら、曖昧さをなくし明確にすることで、それを逆手にとってそこまでサイバー攻撃を仕掛ける事案も生起している[46]ことから、バランスも重要である。また、わが国におけるサイバー関連の法的整備においても、能動的防御をはじめとした能力を発揮できるよう早急に整備[47]し、実践的能力の向上を急ぐ必要がある。

（６）人材養成

人的基盤を強化するため、自衛官の定年年齢の引き上げや再任用の拡大、専門的な知識・技能を有する民間人材を含めた人材確保等の施策や、予備自衛官等についてもサイバー領域を含めて大幅に拡大するとされている[48]。2027年度を目途にサイバー関連部隊を約4,000人に拡充し、サイバー要員を２万人体制にするとしており、既にその取り組みは始まっている[49]。重要インフラ分野を含め、民間事業者に対する支援の取り組みや、関連の法的な分野も含めた幅広い人材の養成が必要になる。

６．サイバー空間における抑止力発揮の方向性

防衛力整備の観点からサイバー戦能力強化に必須の整備すべき要素について考察したが、これらの要素を戦力化することでサイバー攻撃を事前に察知し対処による攻撃阻止、またサイバー攻撃を受けても早期にこれを発見し、対処し、復旧することで侵入されたとしてもシステムは機能

44　「防衛力整備計画について」、11頁。
45　ジャスパー『ロシア・サイバー侵略』、153-157頁。
46　同上、270-273頁。
47　「国家安全保障戦略について」、21-22頁。
48　「国家防衛戦略について」、27-28頁。
49　防衛省「我が国の防衛と予算～防衛力抜本的強化「元年」予算～」令和５年３月28日、21頁。

を発揮し続けるレジリエンスの確保が拒否的抑止につながる。紛争抑止の観点からは、一部機能を喪失しつつも重要な機能を確保する優先順位を適切に選択することにより、運用との整合性を維持し、指揮統制機能や情報取集・分析機能を維持し、またはこれら機能に与える影響を最小限にすることが重要である。

これには、日々変化するサイバー攻撃にも対処できるよう、常続的な監視と新たな脅威情報にも速やかに対応する迅速性も重要であり、様々な情報と得られた情報の分析は攻撃元の特定にもつながる。反撃に関しては、相手の攻撃状況の暴露による名指しと恥さらしや、サイバー空間に限らずキネティックを含めたほかの領域、あるいは外交・経済等様々な領域と密接に連携して行うことで相手にコストを課すことが有効である。一方で、紛争事態になれば、その前後或いは武力攻撃のタイミングでわが国の防衛力発揮に関わるシステムや装備品、及び重要インフラに対してサイバー攻撃は様々な手法を用いて行われるだろう。日米安全保障条約５条の適用にあっては、我が国はサイバー反撃能力を有する米軍と連携して行動することになるため、常に米サイバー・コマンド関連部隊で構成されるサイバー任務部隊（CMF: Cyber Mission Force）と円滑な運用ができるよう共同訓練等を通じて練度を上げておく必要がある。平時及びグレーゾーンからサイバー攻撃の規模や烈度によって事態を分類[50]し、事態の拡大に備えて態勢を整えておくことが重要である。このような活動が懲罰的抑止につながる。

ウクライナ侵攻の考察からは、回復力がサイバー攻撃の影響を抑えるためにも重要であり、アトリビューションも状況認識や爾後の対処に必須となる。サイバー戦能力を強化することで相手に弱点を晒さず非対称戦に持ち込まれないようにしつつも、ハイブリッド戦の観点からはサイバー攻撃は複数同時、時間差または波状的に様々な攻撃手法を組み合わせて行われることから、現状維持側の比較優位性を活かし、ネットワークを堅確に維持して攻撃を防御しつつ、積極的に真実を公表する等、ほかのドメインとの連携を密にして素早く対処することが統合的抑止につながる。

これらの能力を相手側に伝える手段として、安全保障におけるサイバー戦略の策定及び公開、日米間あるいは他国とのサイバー共同演習の広報、サイバー攻防戦コンテスト（CTF: Capture The Flag）等における上位成績を収める等の実績や高度セキュリティ関連資格者の保有などを、わが国の手の内を明かさないよう留意しつつ実施する必要がある。また、サイバー攻撃の状況を正確に把握しておくことも重要であり、グレーゾーンにおける行動の管理や有事においては、サイバー指揮統制機能により組織力を発揮してほかの領域と有機的に融合し、その相乗効果により全体の能力を増幅させる領域横断作戦能力の一部として密接に連携させる態勢をわが国として早期に充実させる[51]必要がある。そこには日米をはじめとして海外の国々との連携[52]も重要であることは言うまでもない。

50　松村昌廣「我が国のサイバーセキュリティ戦略の欠点と展望：「平和国家」体制の桎梏への対応を考える」『情報通信政策研究』、第５巻２号、2022年、III-1-III-22。
https://www.soumu.go.jp/main_content/000787278.pdf

51　「国家安全保障戦略について」、22頁。

52　外務省「日本のサイバー分野での外交　二国間協議・対話等」令和５年２月７日。
https://www.mofa.go.jp/mofaj/fp/nsp/page24_000687.html

7. サイバー空間の進化

コロナ禍を契機にリモート環境が充実する頃からサイバー空間は目に見える形で劇的な変化を認識するようになった。これらは、新領域という新たな領域が戦い方に影響を与えていることを前提としつつ、更なる技術の発展がゲームチェンジャーとなり、これまでの議論を更に発展させ、あるいは覆すほどの不確実性のある要素となるため、主な変化について触れておきたい。

（1）クラウドコンピューティング

クラウドは、ネットワーク環境の充実に伴い必要なコンピューティングリソースを物理的に保有せず、データセンターにあるリソースを利用する形態[53]である。既に共通基盤として防衛省においても整備の方向[54]にある。この環境を利用してクラウド環境そのものを防護するサービスも提供されており[55]、これはエンドポイントからサービスを提供するサーバの状況などからデータ相関技術等を統合した環境が構築されていることを前提とすれば、サイバー攻撃元を特定する能力もかなりの精度が上がっているものと予測できる。サイバー戦の観点からクラウド環境の利用を考慮する必要がある。

（2）多様化するネットワーク環境

ロシアによるウクライナ侵攻において、低軌道衛星で構成されるスターリンク（Starlink）によるインターネット利用が注目されている。わが国でもこのサービスは開始されており、高速なインターネットを全国で利用することが可能になった。地上に張り巡らされた通信設備を使用する必要がなく、地上網と合わせて抗たん性は向上する。また、通信方式については5Gのサービス[56]も既に開始されており、今後もネットワーク環境は更に進化する。また、インターネットの通信プロトコル（TCP/IP）を高速暗号化するため、TCPに替わる新たなプロトコル「QUIC」の検討もされており、RFC9000[57]としてIETF（Internet Engineering Task Force）が勧告し、実用化の段階にある。更に、これまでのインターネットの限界を超えた高速大容量通信ならびに膨大な計算リソース等を提供可能な新たなサービス[58]の動きもある。新たな分野は、サイバー空間における攻撃並びに防御における活動において様々に利用される可能性を秘めており、動向についても注視する必要がある。

---

53 日本経済団体連合会「防衛デジタルトランスフォーメーション（DX）の現状と動向」防衛技術報告書、2023年3月、261-265頁。

54 「防衛力整備計画について」、7頁。

55 マイクロソフト「Microsoft Defender for Office 365」。
https://www.microsoft.com/ja-jp/security/business/siem-and-xdr/microsoft-defender-office-365

56 総務省「平成30年版　情報通信白書」。
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd133420.html

57 J. Iyengar and M.Thomson, eds., “QUIC: A UDP-Based Multiplexed and Secure Transport,” IETF, May 2021.

58 NTT「IOWN」。https://group.ntt/jp/group/projects/iown.html

（３）量子技術の実用化

国産の量子コンピューター初号機が、わが国でも稼働を開始した[59]。スーパーコンピューターをも上回る性能は、特に暗号解読の分野でも注目されている。現在のセキュリティ技術は暗号技術を基準としていることからも、量子コンピューターの実用化は新たな脅威になり、様々な対策を今から構築しておく必要がある。物理暗号や対量子暗号などの導入は現段階における現実的な取り組みになるだろう[60]。

（４）認知領域との関わり

サイバー空間は認知領域の全てのレイヤーを網羅しているわけではないが、デジタル誘導工作と密接に関係している[61]。認知領域における情報戦への対応[62]も強化する必要性から、サイバー空間における能力強化はデジタル誘導工作にも直接関連する機能[63]でもあることから、情報戦との相互連携が必要である。

（５）AI技術の実用化

AIは色々な分野で注目されている技術である。前述した言語モデルGPTについては、世の中を変える可能性を秘めている。サイバー空間における自動化や分析等が意思決定の驚異的な迅速化に寄与する可能性は極めて大きいものと思料できることから、今後の動向に注視しつつ可能なものから実用化について検討する必要があるだろう。

8. サイバー空間における抑止の課題

わが国によるサイバー空間における抑止については、安全保障３文書により飛躍的に強化されるが、着実に整備し戦力化していく必要がある。それらを含めた課題について、以下に提示したい。

【1】サイバー攻撃に対しては、拒否的抑止を強化し、レジリエンスを保持することで、システムの目的である機能を確保し、実践力を強化する。
【2】懲罰的抑止については、能動的サイバー防御の観点から、攻撃能力の構築及び法的根拠の整備を行い、ガバナンスの効いた実効的な能力を確保する。
【3】要員養成を含めたサイバー空間能力強化における体制整備については、サイバー戦力強化の構想と発信が必要である。
【4】官民連携を含めたサイバー空間での優位性の確保が重要である。
【5】サイバー攻撃に対して、外交的な調査、制裁及び起訴などの統合的な対処体制の構築が必要である。

---

59 「理研、国産量子計算機を稼働　米中競争に日本も名乗り」『日本経済新聞』2023年３月27日。
https://www.nikkei.com/article/DGXZQOUC234XF0T20C23A3000000/
60 原澤克嘉、時藤和夫「通信セキュリティと量子暗号」『防衛技術ジャーナル』第41号、2021年５月、4-14頁。
61 一田和樹ほか著『ネット世論操作とデジタル影響工作：「見えざる手」を可視化する』原書房、2023年３月、10頁。
62 「国家安全保障戦略について」、24頁。
63 齋藤孝道「デジタル影響工作のプレイブック」一田和樹ほか著『ネット世論操作とデジタル影響工作』、49-78頁。

おわりに

サイバー空間における抑止は、最近の技術や利用形態の進化に伴い、大量のデータを迅速に収集・分析して攻撃元を特定し、AIを活用したサイバー攻撃への対処を自動化することで、状況が確実に変わりつつある。しかしながら、影響する範囲は迅速に拡大しており、ITの技術動向を敏感に捉え、必要なものは速やかに取り入れ、多くの組織等と連携することで紛争を抑止することが重要であり、そのための手段としてのサイバー空間を如何に使っていくのか、国を挙げたイノベーティブな発想と実践の継続こそが激変する戦争（War 3.0）への抑止に有効に機能するであろう。それが必要な時代になってきた。

第五章　台湾有事における日米のサイバー作戦上の課題

森聡

はじめに

台湾有事が発生した際に、日本と米国はいかなるサイバー作戦上の任務にあたらなければならないのか。日本が担うべきサイバー領域における任務にはいかなる能力が必要で、その開発面での課題とは何か。本稿の目的は、これらの問いに関して考察を行い、今後の日本の取り組みを予備的に検討することにある。したがって、本稿は日米のサイバー作戦上の課題を演繹的に整理するコンセプト・ペーパーであって、既存の政策を叙述・評価する調書の類ではないことをあらかじめ断っておきたい。

まず検討を進めるにあたって、前提となる３つの基本的な条件を確認したい。第一に、中国が台湾の支配ないし尖閣諸島の制圧という現状変革を戦略目標とし、日米は武力による現状変革の拒否を目標とした防衛戦略をとるということである。第二に、中国による短期決戦を拒否しなければならない一方で、戦争が長期化すれば、日米の継戦意思が劣化する可能性が高まるということがある。第三に、日米にとっては、武力による現状変革を抑止することが第一義的な目標となり、もし抑止が破れる場合には、日米共同作戦を実施することになるが、この作戦は両面的な性格を有することになる。すなわち、①中国が戦略目標を達成するための「勝利の方程式（TOV: Theory of Victory)」に必要な能力と意思を削ぐ攻勢作戦と、②日米が戦略目標（中国の戦略目標の拒否）を達成するためのTOVに必要な能力と意思を守る防勢作戦を実施する必要がある。日米が中国に対して能力面で優位にあった際には、主として防勢作戦に重心を置いた防衛戦略によって中国の戦略目標を拒否できた。しかし、地域的な通常戦力バランスの劣化に伴い、防勢作戦のみならず、攻勢作戦も組み合わせ、その比重を適切に高めていくことが必要となっている。

以上の基本的な前提条件の下で、まず中国が戦略目標を達成するのに必要な能力と意思を削ぐ攻勢作戦と、中国による現状変革の拒否という戦略目標を達成するのに必要な能力と意思を守る防勢作戦において、日米はいかなるサイバー作戦上の役割を手掛けることが考えられるのかを整理し（第１・２節)、各役割に応じた任務に必要な能力と、その能力を開発する上での主な課題を検討する（第３節)。

１．サイバー作戦上の役割その１―攻勢作戦（主に米国）

まず中国のTOVに必要な＜能力＞と＜意思＞を削ぐために、いかなるサイバー作戦上の任務が必要となるかを整理してみたい（なお、米中による核戦力の指揮・統制・通信（NC3）を巡るサイバー攻撃の問題は本稿の検討対象外とする)。

（１）中国のTOV実現に必要な＜能力＞を削ぐサイバー作戦

中国のTOVに必要な＜能力＞は、軍事的能力と、軍事的能力を支える民間・社会基盤とで構成されると考えられるので、これらを分けて検討する。

まず中国のTOVは、①ミサイル攻撃、②航空優勢の獲得、③海上の制圧、④上陸作戦という

最も基本的な要素で構成されることになる。高橋杉雄はその著書で言及する「統合海洋縦深防衛戦略」において、①及び②の阻止は困難であるが、③と④の阻止は可能で、対艦ミサイル飽和攻撃が有効であるとした上で、その有効性をどこまで高められるかは、中国と日米がそれぞれ攻撃目標をどこまで探知できるか、すなわち情報収集・監視・偵察（ISR）能力に懸かっているとしている[1]。人民解放軍が統合運用する部隊から地上発射型ミサイル・航空機・艦船を駆使した多様な攻撃を行うとすれば、目標の探知から攻撃の実行に至るOODA（Observe, Orient, Decide, Act：観察、状況判断、決断、行動）ループの各機能的局面を標的にしたサイバー攻撃任務が考えられる。これは軍事組織を標的とした＜対兵力サイバー攻撃任務＞ということになる。その際には、人民解放軍のOODAループのどこに対して、どのようなサイバー能力を行使するのが有効なのかが問題となる。

また、人民解放軍部隊を直接支える民間・社会基盤も存在するため（例えば情報通信インフラや大型船舶・航空機など）、中国が日米に対する情報戦を仕掛けた結果、日米を包む「戦場の霧」が濃くなる場合、攻撃対象範囲を対兵力から対価値へとエスカレートせざるを得なくなる可能性がある。こうした状況に至るとすれば、戦況次第ではあるが、本来的に非キネティックな＜対価値サイバー攻撃任務＞が大きな作戦上の役割を担う可能性がある。

（２）中国のTOV実現に必要な＜意思＞を削ぐサイバー作戦

抑止が破れて中国による攻撃が発生し、いわゆる有事に突入してしまった場合、現状維持ないし原状回復を目指す防衛戦略をとる日米としては、中国の最高意思決定者に武力による現状変革を断念、少なくとも一時停止（先送り）させることが戦略目標となる。中国の最高意思決定者が、武力による現状変革を決心して開始した後に、その実現が困難な状況に直面したとして、そうした状況でエスカレートするか、一時停止して立て直しを図って後日攻撃を再開するか、いずれの選択肢をとるかはそのときにならなければ分からない。

問題は、中国の意思決定者が、どのような指標に着目して対応を判断するかということであろう。中国国内の状況が安定していれば、エスカレーションを選択しやすくなるのか、あるいは、一時停止して立て直ししやすくなるのか。あるいは、中国国内で体制批判が噴出していれば、自らの正統性が懸かっていると考えてエスカレーションに及びやすくなるのか、あるいは、それ以上の状況悪化を恐れて、対外的な軍事行動を一時停止し、国内での治安回復を優先すべきと判断するのか。おそらく一般的な予測は不可能であり、最終的には個別具体的な状況下でのインテリジェンスの問題となろう。もし仮に中国国内で体制批判が噴出していけば、出口の見えない軍事行動を続行するよりも一時停止し、国内での治安回復を目指す必要があるため、サイバー手段を用いた情報作戦が大きな意味を持つことになろう。この種の情報作戦は、世論の誘導・分断を目的とした＜対価値サイバー攻撃任務＞の部類に入ることになる。

2. サイバー作戦上の役割その2—防勢作戦（主に日本）

中国は、日米が中国の戦略目標の達成を阻止するとの想定の下、そうした脅威をもたらす日米の＜能力＞と＜意思＞を削ぐための攻撃を実施することになるので、中国側による攻撃に対して

1　高橋杉雄『現代戦略論：大国間競争時代の安全保障』並木書房、2022年、201-209頁。

日米がいかなるサイバー作戦上の防御任務を実施しなければならないかを整理してみたい。

（１）中国による日米の＜能力＞に対する攻撃への防御

中国にとって渡洋上陸作戦に使う艦船・船舶・上陸部隊が死活的に重要だとすれば、人民解放軍は米軍と自衛隊の対艦攻撃能力を妨げにくる。すなわち、日米のISRアセットに対する攻撃・妨害、②日米の対艦攻撃用プラットフォームへの無人システム等による攻撃、日米の対艦攻撃プラットフォームの出撃拠点（基地等）への弾道・巡航ミサイル等による攻撃、④米軍と自衛隊の統合運用能力を妨げるための国防ネットワークに対するサイバー攻撃、などが考えられる。加えて、中国が日本のグレーゾーン事態への対処能力を奪うとすれば、日本の法執行機関に対するサイバー攻撃も想定される。これらの攻撃に対処するための人民解放軍を対象としたサイバー作戦は、もっぱら１（１）で挙げた＜対兵力サイバー攻撃任務＞の中に含まれることになろう。

また、日米の作戦を様々な形で支援する民間企業のネットワークに対する中国のサイバー攻撃も想定される。例えば、輸送を担う民間船舶会社のネットワークに対するサイバー攻撃や、日米の弾薬生産システム攪乱を目的とした防衛産業のネットワークに対するサイバー攻撃、防衛産業等の稼働に必要な電力供給システム等重要インフラのネットワークに対するサイバー攻撃なども想定される。国家安全保障戦略で導入が発表された能動的サイバー防御においては、民間企業等からのサイバー攻撃の通報や、情報通信会社のネットワークのデータフローのモニタリングを通じてサイバー空間の状況把握を高めて必要な対処を図ることになるほか、政府や重要インフラに対する重大なサイバー攻撃については、日米が未然に攻撃者のサーバ等に侵入して無害化する能動的な防御策が取られることになる。

（２）中国による日米の＜意思＞を削ぐ攻撃への防御

中国は情報作戦を通じて、日米両国で台湾有事への介入に反対する世論の形成を進めていく可能性が考えられる。米国では、紛争のエスカレーションを嫌って介入に反対する意見を中国が扇動する可能性がある。また日本では、台湾防衛のために介入しようとする米国に協力すれば、日本は中国の報復攻撃に遭い、国民の生命が危険にさらされるなどといった反対論が湧き起こる可能性がある。いわゆる認知領域における情報作戦にいかに対抗すべきかが問題となる。

３．サイバー作戦上の任務

第１節と第２節で挙げた各種の作戦上の任務と課題を整理すると、概ね下記の通りになる。日米の現有能力などに照らせば、サイバー空間における攻勢作戦を米軍、防勢作戦を自衛隊が担うというのが、おそらく基本的な役割分担として順当であろう。

（１）米国による攻勢作戦上の任務

A）対兵力サイバー攻撃任務

中国軍のOODAループのどこに対して、どのようなサイバー攻撃を実施するのが有効であるかが問題となる。人民解放軍のISR能力を妨げるという観点からは、衛星システムやセンサーを搭載する無人機・有人機に対するサイバー攻撃が考えられる。人民解放軍の指揮・統制（C2）

を妨げるという観点からは、通信ネットワークの機能停止や、センサーのデータを集約するクラウドに向けたデータ汚染・欺瞞等の方策が考えられる。

B）対価値サイバー攻撃任務

中国の民間・社会基盤のどの部分に対して、いかなるサイバー攻撃を仕掛けるのが有効であるかが問題となる。人民解放軍の兵站を支援する民間システムを標的とする場合には、例えば、福建省を中心とした中国沿岸部の鉄道や船舶を運行する主体や、社会・経済システムを支える沿岸部大都市の電力供給網等の重要インフラに対するサイバー攻撃が考えられる。エスカレーションの必要に迫られて、一般市民の生活基盤を劣化させる規模・水準のサイバー攻撃を実施する必要に迫られれば、金融システムやメディアのサーバ、水道・ガスの供給網のネットワークに対する攻撃も選択肢に含まれうるであろう。

C）対認知領域サイバー攻撃任務

中国国民の認知領域に対して、いかなる種類の情報作戦を仕掛けて、どのような結果を出そうとするのかが問題となる。台湾の武力統一という選択に対する一般市民の支持が後退するようなナラティブやメッセージをSNS等の手段を活用して大規模に流布することが考えられる。具体的なナラティブをいかなるものとするかは、より専門的な分析に基づいた検討が必要であろうが、一般的には、例えば「甚大なコストを払って台湾を武力で制圧したところで、中国人民はほとんど裨益しないので、強制的な現状変革は失策であり、直ちに止めるべきである」、「もし台湾を武力で統一すれば、その後の中国と主要国との関係は長期的に悪化し、台湾を統一して得られる利益を相殺して余りあるほどのコストを支払うことになるので、直ちにやめるべきである」といった趣旨のメッセージを、より具体的な情報を埋め込んだ形で流布することが考えられる。

（２）日本による防勢作戦上の任務と能力

日本政府として防護すべき対象は、防衛省・自衛隊の国防ネットワーク、政府省庁・法執行機関・重要インフラ等の公的ネットワーク、民間企業等のネットワークに加え、デジタル空間と接触する一般市民の認知領域ということになる。

A）国防ネットワーク防衛任務／政府省庁・法執行機関ネットワーク防衛任務／民間ネットワーク防衛任務

国防、政府省庁、法執行機関、民間企業では、それぞれネットワークの性質やセキュリティの水準も異なるが、国家としてネットワークを防衛する際に、いかなる能力を獲得すべきかが問題となる。獲得すべき能力は、サイバー状況把握とサイバー・レジリエンス（強靭性）が考えられる。将来的には、サイバー精密反撃の能力の獲得も考えられる[2]。

サイバー状況把握については、国家安全保障戦略において、民間事業者等がサイバー攻撃を受

2　米国の国防高等研究計画局（DARPA）のサイバー・AI部門である情報イノベーション局（I2O：Information Innovation Office）の各種取り組みが参考になる。本セクションで言及するサイバー状況把握、レジリエンス、精密反撃という課題は、DARPA創立60周年記念イベントでI2O局長が掲げていたサイバー分野における将来課題である。

けた場合等の政府への情報共有、国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知するための取組といった方策が打ち出されている[3]。既存及び新規の方策を実効化した上で、有事発生前の段階も含め、深刻なサイバー攻撃が発生しつつある状況において、それを探知できる包括的な能力を実現する必要がある。例えば、多数のサイバー空間での動きが、各々は正統なものでありながら、連動して進行・展開すると全体として安全保障上の危害やリスクをもたらす動きを成す場合、それらの「点と点をつなぐ」ことによって、一見して明白ではない、巧妙で高度なサイバー攻撃を自動的ないし半自動的に探知する能力を獲得する必要がある。そのためには人工知能（AI）を活用した先進的なサイバー攻撃探知システムを開発しなければならない[4]。

サイバー強靭性については、脆弱性の手当を自動化するプログラムや、複雑なソフトウェアを自動的に構築・改善・修復するメカニズムを開発する必要があり、次のような３つのアプローチがありうる。①先制的なパッチング（脆弱性の解消）によって防御する。②信頼に足るシステムを整備して、AIによってボット等に対処する。③AIによってシステムの構造を把握し、その構造を変化させることによって脆弱性を減らす[5]。侵入を完全に防ぐことは不可能なため、攻撃を受けていち早く脆弱性を手当てし、セキュリティをできるだけ高水準で担保しながら事後のシステムを復旧し再始動させることが課題となる。

更に今後は、国家安全保障戦略で示されたように、能動的サイバー防御の一環で、国や重要インフラに対する攻撃について、未然に攻撃者のサーバ等に侵入して無害化する方策も導入されていくことになる。加えて将来的には、サイバー攻撃を受けた場合に、サイバー精密反撃を実施するという選択肢も視野に入ってくるかもしれない。ヒトと機械の協働システムを整備し、機械学習やパターン認識などを活用してサイバー攻撃を探知し、ヒトによる適切な判断の下で、精密なサイバー反撃を実施する能力を備えていくという選択もあり得よう。そこでは機械が大規模なデータ解析で攻撃を探知し、ヒトが文脈を踏まえた適切な反撃のあり方を判断することが想定される。この場合、レッド・スペース（敵の領域）、グレー・スペース（中立領域）、ブルー・スペース（自身の領域）のうち、グレー・スペースでいわゆるボットネット等を特定して無力化することが考えられ、そのための技術的ソリューションと政策の開発が求められる[6]。

B）認知領域防衛任務

台湾を巡る情勢が緊迫し、危機が高まる状況が生起した場合、中国が、米国や日本の一般市民の認知領域を標的として、ソーシャル・メディア等で活字や画像を流布させることにより、自ら

3　国家安全保障会議・閣議決定「国家安全保障戦略について」令和４年12月16日、21頁。
4　例えば、DARPAのCHASE（Cyber-Hunting at Scale）プロジェクトは、こうした能力の開発を目指すものである。
5　例えば、DARPAのAMP（Assured Micropatching）、CASE（Cyber Assured Systems Engineering）、ConSec（Configuration Security）、SDCPS（Symbiotic Design for Cyber Physical Systems）といったプロジェクトは、３つのアプローチを実践するための技術を開発中である。
6　DARPAのHACCS（Harnessing Autonomy for Countering Cyberadversary Systems）プロジェクトなどは、こうした能力の開発を進めている。

に有利な環境を醸成する情報作戦をサイバー空間で展開する可能性がある[7]。例えば、米国による危機・有事への対応に協力する日本政府の方針や政策を批判するような言説を煽ったり、あるいは、台湾をめぐって米中間で武力衝突が発生すれば、米国に協力する日本も中国の攻撃対象となり、日本で犠牲者が多数発生するであろうなどといった言説を流布したり、米兵が日本国内で傷害事件を働いているといった偽情報を流すディスインフォメーションを展開したりと、様々な情報によって日米協力を阻害しようと試みる可能性がある[8]。

政府の方針や政策に対する批判や戦争勃発への恐怖の感情に訴えようとする言説などは、日本国内から発生するものと、外敵が日本の言説空間に注入するものとがありうるが、この両者が相俟って日本国内における対米協力反対論や非戦論の声が高まる可能性がある。国内における特定の意見を増幅するようなこの種の情報戦は、「意見を巡る闘い」であるので、政府としては自らの方針を国民に向かって説明するよりほかなく、その説明が国民に受け入れられるかどうかは、政府に対する国民の信頼の度合いに懸かってくることになる。これはこうした状況が生まれてからその場で対処できるような事態ではなく、平素から政府が国民の信頼を獲得できているかどうかということ次第となる[9]。

一方、ディスインフォメーションに関しては、諸外国で様々な取り組みが展開されており[10]、日本においても諸外国の取り組みを参考に各種の対処策を講じていくべきであろう。ディスインフォメーションの流布は様々な媒体を通じて行われるであろうが、高性能な生成型AI等を用いて捏造された画像（動画・静止画）メディアを通じて流布されるディスインフォメーションは深刻な問題を引き起こすと考えられる。世界では毎日20億以上もの画像がSNSなどにアップロードされており、捏造件数は増加の一途をたどっていると言われる。台湾有事が発生し、もし台湾と中国本土をつなぐ海底ケーブルが遮断され、衛星通信も妨害されるとすれば、情報がブラックアウトされた状態になる。すなわち、諸外国は台湾内部の状況の把握が困難になり、台湾内部は諸外国の動静の把握が困難になる可能性がある。事実上の情報封鎖によって情報の飢餓状態が生じているところに、捏造だと容易に見破られないような極めて高度な捏造画像が流布されれば大きなインパクトをもたらしかねない。しかもその種の捏造画像が、一見して無関係な多方面のルートから入手されたものとして配信されれば、「裏の取れたもの」として受け止められる可能性もある。台湾内部では、外国からの来援は見込めないといった趣旨のメッセージを事実上発信するような様々な画像が流され、外国では、台湾市民は戦意を喪失したといったメッセージを事実上発信するような様々な画像が流されたとして、それらが真しやかに流布するとすれば、日米と台

7　中国の影響力工作と心理・認知領域を巡る闘争に関しては次を参照。山口信治、八塚正晃、門間理良『中国安全保障レポート2023　認知領域とグレーゾーン事態の掌握を目指す中国』防衛省防衛研究所、2023年、26-47頁；小泉悠、桒原響子、小宮山功一朗『偽情報戦争：あなたの頭の中で起こる戦い』ウェッジ、2023年、52-87頁。

8　桒原響子「台湾有事におけるディスインフォメーションの脅威と対策のあり方」日本国際問題研究所・研究レポート、2022年３月１日。https://www.jiia.or.jp/research-report/security-fy2021-01.html；大澤淳「台湾有事とハイブリッド戦争」笹川平和財団・国際情報ネットワーク分析 IINA、2022年８月24日。

9　この点に関する高橋杉雄氏による指摘に感謝したい。

10　笹川平和財団が国際情報ネットワーク分析 IINA上で連載する「インド太平洋地域のディスインフォメーション研究シリーズ」では、オーストラリア（長迫智子）、米国（成原慧）、シンガポール（古賀慶）による取り組みの事例のほか、偽情報対策としてのファクトチェックの有効性と限界に関する論考（鍛治本正人）を紹介している。

湾、第三国の世論や、政府の政治・外交・戦略上の判断が混乱させられるとも限らない。こうしたリスクを抑えるためには、包括的で自動化されたデータ鑑識（data forensics）の分析を行うプラットフォームが必要となる。データ鑑識が大規模に実施可能となれば、捏造の事実を露見させるカウンターディスインフォメーションの方策となろう。なお、こうした画像データの真贋を識別する技術は、おそらく欺瞞する技術と反復的に相互作用していくと考えられ、継続的な開発のための投資が必要となる。

おわりに

サイバー領域は、少なくとも以下の３つの要因により、ますます複雑かつ困難になりつつある。第一に、潜在的な被攻撃対象が急激に拡大している。日本と米国の情報技術とサイバー領域への依存は、規模とアプリケーションの複雑さという両面で飛躍的に高まっているが、人民解放軍や関連組織によるサイバー攻撃に対して強靭なシステムが普及しているわけではない。第二に、サイバー攻撃を実施する主体は、今後とも懲罰や報復をかなりの程度免れながらサイバー攻撃を実施できる状況が存在し続ける。合法（商用クラウド）及び非合法（ボットネット）な形でコンピューター上の大規模なリソースを活用できるほか、インターネット上の膨大なデータ通信の中で自らの攻撃的な諸活動を隠すことによって、実質的に攻撃の実効性を高めることができる。また、軍のサイバー部隊のみならず、第三者組織が恣意的に攻撃に加勢する可能性もあるので、状況は更に複雑化する。第三に、サイバー戦場は今後とも深い「霧」に包まれた状態であり続ける。防御用サイバー技術は民用に開発されるものの、攻撃用サイバー技術は国家及び非国家主体によって隠密裏に開発されるため、敵対勢力のサイバー戦能力を正確に把握することは不可能ないし極めて困難となり続ける。技術的サプライズに直面する可能性は否定できず、敵対勢力による活動を把握する能力を高める必要がある[11]。

台湾危機ないし有事がもし発生すれば、第３節で示したようなサイバー作戦上の任務が、上記のようなサイバー領域の傾向がある中で実施されることになる。米国がサイバー攻勢作戦の主翼を担い、日本は自国に向けられるサイバー攻撃への対処に優先的に取り組み、能動的サイバー防御の各種方策等を通じて国防、政府省庁・法執行機関、民間企業のネットワーク防衛を実効化するとともに、日本国民の認知領域への情報作戦にも対処していかなければならない。こうしたサイバー防勢作戦を遂行する際には、サイバー状況把握、サイバー強靭性、ディスインフォメーション対策の能力が問われることになる。これらの大きな取り組みを進めるための個別具体的な課題は多々あろうが、日米のサイバー作戦上の役割と任務の分担を踏まえて必要となる基幹的な能力の開発という観点からは、サイバー状況把握については、多様なセンサーが収集する大規模なデータを解析して攻撃を探知するためのAI・機械学習の導入、サイバー強靭性については、潜在的攻撃対象の拡大に伴うリスクを低減するためのゼロトラストのアーキテクチャーへの移行、そしてディスインフォメーション対策については、膨大な画像データ等の真正性を識別するための大規模データ鑑識プラットフォームの導入などが主な課題であり急務となっている。

11　これらはDARPA創立60周年記念イベントでI2O局長が指摘していたサイバー領域における主要トレンドである。

第六章　エア＆スペースパワーの進化と抑止

杉山公俊・中谷寛士

はじめに

ルネサンス期を代表する芸術家の１人であるレオナルド・ダ・ヴィンチ（Leonardo da Vinci）が描いた飛行機械に象徴されるように、有史以来、人類が大空で活動することは長い間夢物語であった。この悲願の夢を実現し、空に進出した人類は今や空を超え、宇宙まで到達し、地球以外の惑星での活動も視野に入れるなど人間が踏み込める空間・領域も飛躍的に拡大している。これに伴い、これらの領域での人類の争いも激化しており、これらの領域を戦略的にいかに活用するかは、今後の国際政治を大きく左右する一要因となるだろう。エアパワーが発揮される航空領域は、陸上、海上の上空を覆うとともに宇宙へと接続する広大な空間である。このエアパワーを効果的に発揮する上では、情報収集、通信や測位衛星等の宇宙アセット、多種多様なコンピューター・ネットワーク、幅広い帯域の電磁波の活用が不可欠であることから、「宇宙・サイバー・電磁波」といった、いわゆる新領域での戦いの影響を最も受ける戦闘領域の一つと言える。そして、今日、宇宙軍の創設に見られるように空の先にある宇宙が戦略的領域として台頭するに従い、空と宇宙という組み合わせ、エア＆スペースパワーが現代の戦略を語る上で欠かせないものとなっている[1]。

係る観点から本章では、エア＆スペースパワーを例として取り上げ、その特性と進化を踏まえながら、新領域での優勢がどのように空の戦いや抑止に寄与するかについて議論する。それでは、エア＆スペースパワーとは何か。本章におけるエア＆スペースパワーは、先見の明を持ち、独立軍種としての米空軍創立を早い時期から訴えた空軍戦略の創始者とも言えるW・ミッチェル（William Mitchell）のエアパワーの定義に倣い[2]、「空と宇宙空間を通じて、目的を達成する能力」と定義する。したがって、戦闘機や対衛星兵器に代表される兵器のみでエア＆スペースパワーが構成されるわけではない。これらは、あくまで同パワーの構成要素の一つでしかない。実際には空と宇宙において活動し、その活動を通じて目的達成を支援するための諸要素は数多くある。つまり、エア＆スペースパワーを考える上では、総合システムとして空と宇宙を捉える必要がある[3]。

1　一例として、豪州空軍は、戦略環境の変化を受け2020年末に豪州空軍の研究機関をエアパワー・デベロップメントセンターからエア＆スペースパワーセンター（Air and Space Power Centre）へと改称している。名称変更の要因と背景については以下を参照。Air and Space Power Centre, “Chief of Air Force- Launch of Air and Space Power Centre,” December 2, 2020.
https://airpower.airforce.gov.au/videos/chief-air-force-launch-air-and-space-power-centre

2　ミッチェルのエアパワーの定義については、以下を参照。William Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power Economic and Military*. 1925. Reprint, Dover Publications, 1988, pp. 3-4. また、以下も参照。Colin S. Gray, *Air Power for Strategic Effect*, Air University Press, 2012, pp. 8-9, 305.

3　実にミッチェルは、例として人材、航空機、産業、生産能力、整備員、航空路、燃料補給所、民間航空、空とそれ以外の領域との関係といったエアパワーを総合的なシステムとして捉えていた。この点については以下を参照。Mitchell, *Winged Defense*, pp. 31-33.

また、21世紀の現在において、冷戦後に普及した米国主導の「単極」世界という幻想は終焉し、大国間競争の復活が宣言されている[4]。21世紀の大国間競争の最前線はインド太平洋であり、この広大な地域の安定がかつてないほど重要になっている[5]。この大国間競争に対する中核概念として、米バイデン政権は『米国家安全保障戦略』において「統合抑止」を打ち出した。同概念の一つの大きな特徴として挙げられるのが、同盟国との従来以上の抑止連携である[6]。他方、昨年12月に公表された日本の『国家安全保障戦略』は、防衛力の抜本的強化を含む、我が国自身の力で国家を防衛することを基礎とする旨を強調した[7]。どちらの文書からも抑止に対する日本の努力が一層肝要になっていることが示唆されており、エア＆スペースパワーを用いた抑止とは何かを考えることは、時宜にかなうものであるとの認識に基づき、本章は同パワーを駆使した抑止について議論する。

1．エア＆スペースパワーの進化と変遷

主に空と宇宙空間で活動するエア＆スペースパワーは、全球的という性質を有する。エア＆スペースパワーを駆使すれば、山や川といった地形の制約を受けず理論的には地上のいかなる場所にも迅速にアクセスが可能である。したがって、偵察、観測、補給、通信といった作戦支援から敵国本土への直接攻撃といったように空や宇宙空間が軍事利用されるのには、時間を要さなかった[8]。今日、戦略を考える上で欠かすことのできないものとなったエア＆スペースパワーにはどのような特性があり、いかに進化したのか。以下では、エア＆スペースパワーの特性を考察しつつ、同パワーの軍事的有用性について議論する。

（1）エアパワーの特性

20世紀初頭にライト兄弟が初の動力飛行に成功して以降、航空関連技術は急速な発展を遂げた。空軍という軍種が誕生してからは約100年程であり、陸海軍に比してその歴史は圧倒的に浅い。しかしながら、現代の戦争において航空戦力は、戦争の帰趨に重大な影響を与え得る必要不可欠なものとして認知されている[9]。

エアパワーの優れた特性として第一に挙げられるのは、その即応性・機動性である。地球の表面は大気によって覆われており、宇宙へと続く広大な空間が航空領域として存在している。航空領域を移動する航空機やミサイル等の飛翔体は、地形の制約を受けず、地上や海上に比べて大気

---

4 The White House, *National Security Strategy of the United States of America*, December 2017, p. 27. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf また、以下も参照。Elbridge A. Colby, *The Strategy of Denial: American Defense in An Age of Great Power Conflict*, Princeton University Press, 2021, pp. ix-xii.

5 The White House, *The National Security Strategy of the United States of America*, October 2022, pp. 11, 37. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

6 Ibid, p. 22.

7 国家安全保障会議「国家安全保障戦略」2022年12月、17-20頁。https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf

8 Tami David Biddle, *Air Power and Warfare: A Century of Theory and History*, U.S. Army War College Press, 2019, pp. 4-5.

9 杉山公俊「21世紀のエア＆スペースパワー」講演『戦略研究』第32号、2023年３月、94頁。

との摩擦は極めて小さいことから、超音速での飛行も可能であり、極めて高速に広範囲を移動できる。すなわち、エアパワーは、空中のみならず、地上や海上のあらゆる目標に対して迅速な戦力投射が可能であり、元来、領域横断的な戦力であると言える[10]。その他にもエアパワーの長所として、高い高度と広い行動範囲に基づく優れたISR（情報収集、警戒監視、偵察）能力、長距離打撃力などが挙げられる[11]。

他方、戦闘機などに代表されるエアパワーは、地上においては脆弱で、気象条件による活動の制約も受け易く、また戦力発揮のためには多種多様な機能を有機的に連携させる必要があることから、一部機能の喪失によって戦力発揮を大幅に低下するという脆弱性も有している[12]。例えば、F-15戦闘機を構成する部品点数は約10万品目[13]とされているが、それらが適切に整備されて正常に機能する状態でなければ可動機として運用することはできない。また、戦闘機が離着陸するための滑走路をはじめとする航空基地や管制支援を行うためのレーダー施設や指揮通信ネットワーク等が正常に機能する必要がある。更には、高度の科学技術に立脚した多種多様な装備品を運用するため、要員の養成には多大な費用と長期間を要するという特性が挙げられる[14]。

総括すると、エアパワーは、上記の各種条件が揃えば極めて大きな戦力を発揮できる反面、様々な制約や一部の機能喪失によって全体の戦力が急激かつ大幅に低下しうるという特性があり、その成否は戦局全体に影響を与える極めて大きな変動要素と言える。

（２）揺らぎつつある航空優勢の概念

空の戦いは、端的に表現すれば航空優勢を巡る戦いとも言える[15]。航空優勢とは、我の航空戦力が優勢であり、敵から大きな妨害を受けることなく我の様々な作戦を遂行できる状態にあることを言う。航空戦力が登場して以来、航空優勢を保持している側が戦勝を獲得した戦例は枚挙に遑がない。仮に敵が航空優勢を保持している場合、敵航空戦力の脅威に晒されることから、陸上作戦や海上作戦も含め我のあらゆる作戦遂行が困難となる。空を支配するということは、より高い位置から敵を広く見下ろし、位置エネルギーを活用して有利に攻撃をすることが可能となる。逆に航空優勢を持たない側は、輸送や移動などの基本的な行動さえも実施困難な状況に置かれるため、極めて不利な状況に陥ることになる。このため航空優勢獲得は死活的な重要性を持つと考えられてきた。

こうした航空優勢を獲得するため、主要兵器としての戦闘機の発達はもとより、それに対抗するためのレーダーや地対空ミサイルといった装備体系も絶え間なく進化を遂げている。これらの兵器は、捜索・探知するためのセンサー（レーダーなど）と撃破手段としてのシューター（ミサイルや爆弾等の発射プラットフォーム）更には、両者を繋ぐネットワークに大別される。一般的な趨勢として、センサーは捜索範囲の拡大と探知精度の向上、シューターは射程距離の延伸と命中精度の向上、ネットワークでは通信の高速化・大容量化が進行している。このようにシステム

10　Biddle, *Air Power and Warfare*, pp. 4-5.
11　航空幕僚監部「航空自衛隊の概要」2022年版、14頁。
12　同上。
13　茶木哲義「航空機維持部品の補給管理について」『防衛取得研究』第三巻、第四号、平成22年３月号、３項。
14　杉山「21世紀のエア＆スペースパワー」、85-86頁。
15　同上、86頁。

はより高度なものへと絶えず進化を続け、戦闘領域も拡大し、戦闘様相はより複雑なものへと変化を続けている。

宇宙・サイバー・電磁波は、技術の進展も相まって、益々その活用度を高めている。GPS衛星は、精確な位置情報を提供し、航法に役立つだけでなく、ピンポイント爆撃などの精密誘導攻撃、更には、各種通信システムに必要な時刻同期を可能にする。衛星通信は水平線以遠の長距離通信を可能とし、偵察衛星による画像情報収集や早期警戒衛星によるミサイル発射探知などは、極めて重要な敵の動きをタイムリーに提供する。加えて、サイバー領域もあらゆる軍事活動に密接に関係する。とりわけエアパワーという高度にシステム化された軍事力を発揮するためには、多種多様なコンピューター・ネットワークへの依存度は高い。これらは、指揮通信、レーダー、気象、ロジスティクス、フライトプラン、航空管制システム、電力管理等を束ねるネットワークシステムが仮にサイバー攻撃などで不具合が起きると戦力発揮に支障が出る可能性もある。電磁波も同様で、高速で上空を移動する航空機等が地上の司令部等と連絡を取る手段としては、無線による音声通信か、あるいはデータリンクとなるが、いずれにせよ、電波の使用が前提であり、これが妨害されることで戦力発揮は大きく阻害されることになる。

いわゆるキルチェーンまたはF2T2EA[16]と呼ばれる一連の流れは、目標の発見（Find）、特定（Fix）、追尾（Track）、照準（Targeting）、交戦（Engage）、評価（Assess）というものであり、キネティック、ノンキネティックな手段に関わらず基本的には同じである。攻撃側としては、このチェーンを迅速かつ効果的に機能させることが重要であるが、逆に防御側としてはこのチェーンの一部を阻害することで相手の目的達成を拒否することが可能となる。こうしたキルチェーンは、人工衛星等の宇宙アセットや各種コンピューター・システム、それらを繋ぐネットワークなどが重要な役割を果たしており、サイバー攻撃や電磁波妨害によって大きな影響を受ける可能性がある[17]。したがって、宇宙、サイバー、電磁波領域における優位性の確保は、その重要性が益々高まりつつある。

だが、実際のところ、航空優勢を巡る戦いは、そもそもエアパワーが時間的・空間的な占有力に乏しいことから、絶対的な航空優勢獲得は非現実的であり、流動的なものである。それでも要時要域、すなわち重要な時期及び空域での優勢を獲得することには大きな価値があり、作戦全般を優位に進めることが可能となる。

総括すると宇宙・サイバー・電磁波の各領域は、既存領域での戦いにも密接に関係し、戦力を大きく増幅する装置（フォースマルチプライヤー）としての役割を果たす。裏を返せば、これらの能力を妨害することで相手の戦力発揮を大幅に低下させることも可能であり、成功すれば極めて費用対効果の高い攻撃となりうる。すなわち、宇宙やサイバー領域での優勢が、従来領域での航空優勢を巡る空の戦いに大きな影響を及ぼすということが現実化している。国家同士のハイエンドな戦いでは、双方ともに宇宙・サイバー・電磁波領域を駆使したものになると考えられ、それら領域での優劣によって圧倒的な格差が生じる可能性もある。したがって、航空優勢の獲得

16 U.S. Air Force, Air Force Doctrine Publication 3-60, *Targeting*, Lemay Center, November 12, 2021, p. 27. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-60/3-60-AFDP-TARGETING.pdf

17 Biddle, *Air Power and Warfare*, pp. 4-5, 67-68; Krista Langeland and Derek Grossman, *Tailoring Deterrence for China in Space*, RAND Corporation, 2021, pp. 1-5.

が、もはや戦勝獲得にとっての十分な条件とは言えず、我の優位性を保証するものではなくなりつつある。宇宙・サイバー ・電磁波領域などでの優勢を持つ側が航空優勢獲得においても有利であることに鑑みれば、従来の「航空優勢獲得」の概念を新領域での優勢も含めたものにするなどの見直しが必要と考えられる。

（３）エアパワーの進化：戦闘機発展の趨勢、無人機によるゲームチェンジ

近年、目覚ましい発達を遂げている無人機は、2020年のナゴルノカラバフ紛争においてアゼルバイジャンの勝利に大きく貢献したと見られているほか、ウクライナ戦争においても航空優勢の有無に関わらず活用され、「航空戦力」としての機能をドローンが発揮している。実のところ、広大な航空領域においては、戦闘機などの航空機がその能力を発揮できる高度には一定の制約がある。例えば、地表や高層建築物との衝突リスクのある低高度は、有人航空機にとって活動が困難な領域である。他方、そうした低高度帯、空と地表との間の「空岸[18]」は、小型ドローンにとっては最も活躍できる領域であり、人工知能AIや5Gなどの高速大容量通信技術の発展とも相まって、多種多様な自律型兵器が今後益々進化を遂げていく可能性が高い。このことは、2022年に開始されたウクライナ戦争におけるドローンの戦場での活躍から分かる通りである[19]。

更には、2023年２月、米空軍F-22戦闘機が米国東岸において中国のバルーンを撃墜した例に見られるように、成層圏という高高度を飛翔する物体への対応も現実の課題としてクローズアップされている。事実、宇宙と領空の境界は明確な定義付けはなされておらず、国際法上の規程やコンセンサスも確立されていない。人工衛星が地球周回軌道を維持できる最低高度の記録は、日本の宇宙航空研究開発機構（JAXA）の技術試験衛星「つばめ」による地上から約167kmであるが、ジェット機が飛行できる最高高度の記録が米空軍のSR-71偵察機による地上約26kmであることを勘案すると、そこには100km以上のギャップが存在している。中国が米国本土上空の高高度を飛翔するバルーンを通過させたことで、これまであまり注目されてこなかった領域における対応の問題点が顕在化した形となった。今後は、法的な規範や防空態勢の見直しが迫られることが予期される。これまで人間が搭乗することを前提に設計されてきた航空機は、サイズや形状、加速度、在空時間など、人間が許容できる範囲という制約が存在する。しかしながら、無人機は、そうしたヒューマンファクターによる制約から解放されることで、従来の航空機の概念からはかけ離れた多種多様な無人システムが開発されており、爆発的進化の時代をまさに今、迎えつつある。

（４）スペースパワー ：宇宙領域での安全保障、SDA、航空宇宙自衛隊への進化

宇宙空間は、物理的空間の領有や国境の概念が成立しない全球的な空間である。よって宇宙領域における安全保障上の活動の主眼は、国家主権の維持ではなく、同領域の安定的利用の確保となる。宇宙空間は、現代生活にも不可欠な機能を提供しており、宇宙の安定的利用の重要性は

---

18 George M. Dougherty, “Ground Combat Overmatch Through Control of the Atmospheric Littoral,” National Defense University Press NEWS, July 24, 2019, *Joint Force Quarterly*, Vol. 94.
https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1913099/ground-combat-overmatch-through-control-of-the-atmospheric-littoral/

19 杉山「21世紀のエア＆スペースパワー」、94頁。

益々高まっている。宇宙においては、国家、軍または民間企業にかかわらず、多くの主体が活動しており、軍事と非軍事の境界も不明瞭となっている。

宇宙利用の活発化に伴い、地球周回軌道上には既に運用を終えた衛星や破壊された破片などの宇宙デブリと呼ばれる物体が多数存在している。こうした物体は小さな破片であったとしても秒速数キロメートルという極めて高速で移動し、高い運動エネルギーを有していることから、人工衛星などに衝突した場合には大きな損傷を与える可能性がある。この他、様々な対衛星兵器の開発も顕在化しており、宇宙システムに対するリスクや脅威は年々高まりつつある。また、仮に攻撃が行われたとしても攻撃主体の帰属特定（attribution）は困難である。なぜなら、衛星に代表される宇宙アセットは脆弱であり、相手からの意図的な攻撃なのか、あるいは宇宙空間での自然発生的な事故であるかを判断することは困難な場合があり得る。

こうした状況を踏まえ、宇宙領域把握（SDA: Space Domain Awareness）の重要性が高まっている。米国は2019年に独立した第６の軍種として宇宙軍を創設し、フランス空軍もフランス航空宇宙軍に改称するなど、各国において宇宙作戦部隊の創設が相次いでいる。

日本においても2022年12月に策定された、いわゆる戦略３文書において、今後航空自衛隊に将官を指揮官とする宇宙領域専門部隊を新編し、航空宇宙自衛隊へと改称することが明文化された[20]。米国をはじめとする同盟国・同志国と緊密に連携し、平素から宇宙の安定的な利用のため、我の宇宙システムの状況を監視し、宇宙デブリなどとの衝突を回避させるとともに、故意に我が国の衛星を侵害するなどの行為を事前に探知、抑止することは極めて有意義である。

我が国においては、「宇宙の平和利用」として、宇宙領域を安全保障目的には利用しないという時代が長く続いた。しかし、日本が持つ宇宙関連技術は、世界的にも有数のものであり、宇宙領域は、将来的には日本の強みを発揮しうる。こうした分野を強化することで比較優位を保ち、我が国に対する侵略への抑止力を強化することは合理的と言える。とりわけ、攻撃主体の特定が困難な宇宙領域での行為は、グレーゾーンの状況において採択するハードルが比較的低いオプションと言える。このため、米国をはじめとする同志国と平素から緊密に連携し、宇宙でのいかなる行為も見逃さない優れた宇宙状況監視態勢を構築しておくことで、それらを抑止し、ひいては我が国にとって好ましい国際安全保障環境の構築にもつながるであろう。

2. エア＆スペースパワーを用いた抑止

それでは、エア＆スペースパワーの特性を踏まえた場合、日本のエア＆スペースパワーは抑止に対してどのような貢献が可能か。専守防衛を国防の基本方針とする日本がエア＆スペースパワーを駆使した抑止の姿を考える上では、相手に多大なる損害を与える懲罰的抑止ではなく、レジリエンスや根気強さという、相手の目的達成を難しくする拒否的抑止の観点がより重要になるだろう。同時にこれは、日本が行う取り組みや努力はあくまで抑止に対する間接的な支援となることを示唆している。また、日本単体で見た場合、エア＆スペースパワーのみでの抑止には限界があり、実際には陸海空のアセットの統合的な組み合わせ（領域横断）、そして特に同盟国で

20　国家安全保障会議・閣議決定「防衛力整備計画について」令和４年12月16日、15頁。
https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/plan.pdf;
国家安全保障会議・閣議決定「国家防衛戦略について」令和４年12月16日、24頁。
https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy.pdf

ある米国との共同が抑止には必須である。つまり、あくまで抑止を構成する一要素（全体の一部）としてエア＆スペースパワーを見ることが適切である[21]。そして、今後進展の加速が予想される同志国との協力を含む多国間連携も抑止のためには欠かせない[22]。以下において、実力発揮は新領域の能力によって支えられているということを念頭に置き、上記のエア＆スペースパワーの特性を踏まえつつ、同パワーが有する潜在的な抑止効果について議論する。

（１）戦略的重要拠点としての日本

日本の地理的特徴として一般的に挙げられるのが、四面環海の島国であり、国土も相対的に狭小というものである。また、国防体制としても、専守防衛に特化した必要最小限の防衛力を有し、一国としてのいわゆる戦力投射（パワープロジェクション）能力は極めて限定的である[23]。今般の戦略３文書で日本が反撃能力を保有することが明記されたが、他国に対し強力なパワープロジェクション能力を発揮できるのは、日本の同盟国でもある米国である。

実際のところ、日本に駐留する米軍は、日本のパワープロジェクション能力を補うかのように日本を戦略拠点としているとの指摘がある[24]。冷戦初期（特に朝鮮戦争勃発後）からこの点は変化していないという[25]。米国はインド太平洋諸国であるものの、米本土から朝鮮半島や台湾海峡といったホットスポットからは遠く、日本の拠点なしではパワープロジェクション能力が限定的となる[26]。このような点を考慮した場合、日本としては、米国が日本を安定利用できる態勢を維持することが間接的に抑止に貢献することとなるだろう[27]。

それでは、本章の主題であるエア＆スペースパワー、特にここではエアパワーに焦点を絞り、日本の防衛及び抑止に具体的にどのような貢献ができるかを考察する。一つ目は、日本周辺空域の警戒監視であり、わが国の領空を侵犯するおそれのある国籍不明機に対しては、戦闘機を緊急発進（スクランブル）させるという対領空侵犯措置によって相手を日本に寄せ付けないことである。二つ目に、事態がエスカレートし、日本の領土に直接脅威が及ぶ場合においては、可能な限り国土から遠方において戦闘機だけでなく、早期警戒管制機（AWACS）、空中給油機を伴った防空作戦を実施し、国土への被害を最小限にする。三つ目に日本に飛来するミサイルを日本のミ

21　この点に関しては、以下を参照。Colin S. Gray, *Modern Strategy*, Oxford University Press, 1999, pp. 239-240; Gray, *Air Power for Strategic Effect*, pp. 304-305.

22　国家安全保障会議・閣議決定「国家安全保障戦略について」令和４年12月16日、5-6頁。https://www.mod.go.jp/j/policy/agenda/guideline/pdf/security_strategy.pdf 多国間連携と抑止の関係は、以下を参照。ローリー・メドカーフ著、奥山真司・平山茂敏監訳『インド太平洋戦略の地政学－中国はなぜ覇権をとれないのか』芙蓉書房出版、2022年、394-397頁。

23　道下徳成ほか『現代戦略論－戦争は政治の手段か』勁草書房、2000年、167頁。

24　小川和久『日米同盟のリアリズム』文藝春秋、2017年、18-24頁; Michael Lostumbo, et al, *Overseas Basing of U.S. Military Forces: An Assessment of Relative Costs and Strategic Benefits*, RAND Corporation, 2013.

25　U.S. Department of State, *Foreign Relations of United States, 1958-1960, Japan; Korea,* Vol. XVIII, U.S. Government Printing Office, 1994, Document 23, p. 60.

26　Thomas B. Mahnken, et al., *Tightening the Chain: Implementing a Strategy of Maritime Pressure in the Western Pacific*, Center for Strategic Budgetary Assessment, May 2019, p. 1, 14. また、以下も参照。Colby, *The Strategy of Denial*.

27　Mike M. Mochizuki, "Japan's Search for Strategy," *International Security*, Vol. 8, No. 3, Winter 1983/84, p. 156; Col. Kimitoshi Sugiyama, "Japan's Approach to Deterrence in the Age of Great Power Competition in the Indo-Pacific," CASI Conference 2022-Great Power Competition and Deterrence, May 17 2022, National Defense University, Washington, D.C.

サイル防衛能力（積極防衛）によって可能な限り無力化することである。四つ目に、日本に対する攻撃の被害を局限するための自衛隊基地の強靭化、抗堪化であろう。五つ目に、日本に所在する日米の基地の相互使用により、相手の攻撃からの在地航空戦力残存の可能性を高めるといった方策があるだろう。

抑止効果を考えた場合、日本に存在する既存の基地（航空自衛隊だけではなく海上自衛隊の基地も含む）の強靭化及び安定利用を確実にすることであろう。これには、まず既存の基地に新たな施設を構築するといった基地の強靭化（消極防衛）が考えられるが、2023年１月の日米「２＋２」共同発表にも触れられている通り[28]、日本に所在する日米の基地を平時から共同化あるいは共同化に近い形で展開の妨げをなくすことは日米が安定した作戦基盤を増やすことに貢献するだろう。現実的に見た場合、既に存在する基地であれば、新たな拠点を構築するよりも、基盤強化に要する時間も少なくてすむ。

また、究極的には日本の国土を防衛するとは日本の領土に侵攻、より正確には海洋を渡ってくる相手を拒否するということであり、相手を海上で叩く能力が重要である[29]。無論、陸海のアセットを組み合わせて対処する必要はあるが、移動可能な地上発射システムに加え航空機に長距離ミサイルを載せれば、上記の日米の複数の拠点から相手を海洋で叩くことが可能であり、相手の計算を複雑にすることが可能かもしれない[30]。長距離ミサイルに加え、今後いわゆる自爆型ドローンを使用することで相手の防空能力によって一部の攻撃が無力化されたとしても一定の損耗を与え続けることができるだろう。

抑止的な観点で重要なことは、相手に対し、日米の作戦拠点は強靭化されているだけでなく、複数の移動目標からの攻撃の可能性があることも示唆することによって、日米に対する一方的なミサイル攻撃のみで日米戦力を無力化することはできず、日米は根気強く防御に徹する。これにより、攻撃側の短期間での目標達成は拒否され、戦争が膠着状態に陥ると認識させることである[31]。

（２）戦略的高地：高所からの「目」

上記はとりわけ地上での活動に焦点をあてたが、エア＆スペースパワーの特徴を考える上では、空と宇宙という物理領域の活用は当然ながら無視できない。顕著なものとしては、航空戦力による相手の撃滅という考えであるが、これは航空機誕生とともに発展したものである。だが、実際に敵航空戦力や敵国本土を直接破壊できるまでには時間を要した[32]。黎明期の航空機の主任

28　防衛省ホームページ「日米安全保障協議委員会（２＋２）共同発表（仮訳）」2023年１月11日。https://www.mod.go.jp/j/approach/anpo/2023/0112a_usa-j.html

29　高橋杉雄『現代戦略論－大国間競争時代の安全保障－』並木書房、2023年、216-219頁。

30　トーマス・マンケン「Air and Space Power Strategy for Great Power Competition」『エア・アンド・スペース・パワー研究』第10号、2023年１月、7-8頁。

31　高橋『現代戦略論』、209-219頁。

32　Giulio Douhet, trans. and eds. Joseph Patrick Harahan and Richard H. Kohn, *The Command of the Air,* The University of Alabama Press, 2009; Phillip S. Meilinger, “Giulio Douhet and the Origins of Airpower Theory,” in Phillip S. Meilinger, ed. *The Paths of Heaven: The Evolution of Airpower Theory*, Air University Press, 1997, pp. 1-40; Robert Pape, *Bombing to Win: Air Power and Coercion in War*, Cornell University Press, 1996.

務は、後に主流となる爆撃ではなく、空からの偵察や監視であった[33]。これは、かつて見晴らしの良い高地は戦況全体を見渡せる戦略的高地であったのと同様に、空及びその先にある宇宙が戦略的高地として役割を果たすということである。優れた偵察・監視能力を有するのがエア＆スペースパワーの強みの一つでもあり、科学技術の進歩により肉眼では見えない「峠の先（over the hill）」を見通すことが空と宇宙空間を利用することで可能となった[34]。空と宇宙は天象、気象の影響は受けるものの、両空間からは広大な距離を見通すことができ、活動は全球的である[35]。

したがって、人類は地形の利を生かした高台からの偵察や監視に始まり、気球による高所からの敵情把握、固定翼機誕生以降は、高高度偵察機U-2、早期警戒管制機（AWACS）、グローバルホークのような無人航空機、そして、空の先の宇宙空間で活動する衛星による地上の（警戒）監視といったように、高所から相手の動きを見張るまたは偵察するという行為をあたり前のように進化させつつ行ってきた。

しかし、空や宇宙が現代の戦略的高地であったとしても、二つの海洋をまたぐインド太平洋という広大な地域においてリアルタイム且つ正確に陸海空の現況を把握することは容易ではない[36]。特に一か国単体の監視能力には限界がある。日本が位置する広大なインド太平洋における状況の把握を行うには、地域諸国が連携し、それぞれが持つ現地の最新情報を共有・統合し、インド太平洋における共通作戦図（COP: Common Operational Picture）を作り上げる必要がある[37]。もちろん、地域諸国間における公的な情報共有メカニズムや基盤となる共通アセットがないという問題もあるが、重要なことは、相手に自らの違法行為や軍事行動は常に誰かに見られていると認識させることにより不安感や猜疑心を抱かせ、更に状況次第では、相手の行動や悪事を共同で国際社会に公表することによって、相手の動きを先行的にけん制していくことにある[38]。一例としては日本政府が提唱する「自由で開かれたインド太平洋」構想は、地域諸国にも受け入れられており、各国とも地域の透明性、開放性のために協力する動機は十分にあり得るだろう。理想的には、地域諸国によるレーダー網の構築や衛星の共有、多国間情報センターの創設といったことが考えられるが、まだ現状としてこの段階にはない[39]。

地域諸国間の情報共有メカニズムが確立されなくとも、一部の地域諸国との共同訓練を通じた、共同パトロール活動などは、現在でも可能であろう。これに付随して、北朝鮮籍船舶の「瀬

---

33 Martin Van Creveld, *The Age of Airpower*, Public Affairs, 2011, ppb. 2012, pp. 6-23.

34 Gray, *Modern Strategy*, pp. 261-262; 杉山「21世紀のエアー＆スペースパワー」、85頁。

35 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、29-32頁; Mitchell, *Winged Defense*, pp. 3-4.

36 Thomas G. Mahnken, Travis Sharp, and Grace B. Kim, *Deterrence by Detection: A Key Role for Unmanned Aircraft Systems in Great Power Competition*, Center for Strategic Budgetary Assessment, 2020, pp. ii-iii, 22-26.
https://csbaonline.org/research/publications/deterrence-by-detection-a-key-role-for-unmanned-aircraft-systems-in-great-power-competition

37 マンケン「Air and Space Power Strategy for Great Power Competition」、6頁。

38 Mahnken, Sharp, and Kim, *Deterrence by Detection*, p. 6, 41; Thomas G. Mahnken, et al, *Implementing Deterrence by Detection: Innovative Capabilities, Processes, and Organizations for Situational Awareness in the Indo-Pacific Region*, Center for Strategic Budgetary Assessment, 2021, pp. 6, 11-15, 31-39.
https://csbaonline.org/research/publications/implementing-deterrence-by-detection-innovative-capabilities-processes-and-organizations-for-situational-awareness-in-the-indo-pacific-region; Mahnken,「Air and Space Power Strategy for Great Power Competition」、6頁。

39 Mahnken, et al, *Implementing Deterrence by Detection*, pp. 31-39.

取り」を含む違法な海上活動に対する警戒監視活動のために域外国である英・仏・カナダは、国連軍地位協定に基づき在日米軍基地を使用している[40]。これらの国々は「自由で開かれたインド太平洋」構想を高く評価するだけでなく受容する国々であり、同構想実現のための共同パトロールも同様に実現可能性があり、最終的には地域諸国による監視活動を確立し、集団警戒監視態勢を構築することで、常に集団から監視されていると相手に認識させ、更なるけん制を行うことができるであろう[41]。つまり、繰り返しになるが監視の目の偏在性であり、至るところから目が相手を向いているという恐怖にも似た感情を生起させることが鍵となる[42]。

ただ、監視社会として悪名高い英国において犯罪が一切起きないわけではない[43]。更に、英国はヨーロッパでも治安が良い部類の国でもない点には留意が必要である。つまり、監視の目があるからといって違法行為が起きないというわけではなく、抑止効果としては不十分であり、早期に異常を発見・探知した後に、違法行為を罰するといった行動が求められるだろう。

空と宇宙からの監視自体が抑止として機能するかは断定的には言えないが、多国間連携を通じた情報は、自らの情報の正確性を裏付ける形となったり、現況把握の精度を向上させることに繋がったりと重要な取り組みであることに間違いない。これは、詰まるところ地域諸国間の相互利益ともなるだろう。そして、肝要なことは、一か国で得られる情報には限界があり、地域諸国が連携することでより広範囲の情報を得ることが可能となるだけでなく、この活動は違法国家に対する集団圧力となり得るという点である[44]。また、平素より地域を監視することによって、異変の早期発見だけでなく、有事にはキルチェーンを構築するために欠かせない重要な情報源ともなり得る。

（３）多国間連携と集団安全保障

先述の通り、日本政府が提唱する「自由で開かれたインド太平洋」構想は、地域諸国に広く受け入れられているものであり、本構想に賛同する国家間における多国間演習や訓練も日本周辺で行われている。時を同じくして、域内の多国間演習も活発化している。一例を挙げれば、2022年夏頃に実施された豪演習「ピッチ・ブラック22」は、日本の初参加を含む17か国が参加した大規模な演習であり、インド太平洋における多国間連携の重要度が高まっていることが見て取れる。演習に関して言えば、歴史的に共同作戦能力向上を目的とした演習は、演習参加国の緊密性を示すだけでなく、その他の能力的優位を相殺する潜在的可能性から抑止効果があるとの分析もあ

---

40 防衛省「『瀬取り』に対する関係国による警戒監視活動」令和４年10月31日。
https://www.mod.go.jp/j/approach/defense/sedori/2022.html

41 Mahnken, et al, *Implementing Deterrence by Detection*, pp. 6, 31-39. また、以下も参照。Iris van Sintemaartensdijk, et al, “Assessing the deterrent effect of symbolic guardianship through neighborhood watch signs and police signs: a virtual reality study,” *Psychology, Crime & Law*, May 2022, pp. 1-21.

42 Mahnken, Sharp, and Kim, *Deterrence by Detection*, p. 6,41; Mahnken, et al, *Implementing Deterrence by Detection*, p. 9, 37.

43 “Britain is ‘surveillance society’,” *BBC*, November 2, 2006.
http://news.bbc.co.uk/2/hi/uk_news/6108496.stm; Patrick Wintour, “Only ‘tiny handful’ of ministers knew of mass surveillance,” *The Guardian*, November 5, 2015.
https://www.theguardian.com/world/2015/nov/05/nick-clegg-cabinet-mass-surveillance-british-spying

44 Mahnken, Sharp, and Kim, *Deterrence by Detection*.

る[45]。

日本は伝統的に同盟国である米国との共同演習を重視してきたが、現在では米国以外の国々との演習も珍しくない。特に、最近日本と急接近しているのが、豪州であり、2022年１月には、円滑化協定（RAA）を両国間で結んでおり、演習時における両国の相互アクセスが円滑化される。これにより、日本では演習空域が限られていることから実施が困難な演習内容を豪州で試すことができるという利点がある。

また昨今話題の日米豪印（QUAD）は、現在のところ、４か国の戦略的対話に留まるが、４か国は法の支配に基づく「自由で開かれたインド太平洋」の実現に向けて価値を同じくする同志国である[46]。QUADが戦略的対話である一方、インド太平洋において、より安全保障に特化した安全保障上のパートナーシップがAUKUSであり、その主要目的は米英豪の三か国が協力して豪州に原子力潜水艦を取得させることである[47]。豪州が原子力潜水艦を持つことに対しては賛否両論あろうが、ここでの論点は多国間連携の一環としての同志国が共通のアセットを保有することである。だが、全く同じ共通アセットを保有することは、現実的には大きな困難が伴う。他方、燃料や弾薬を相互に代替可能なものにできれば、継戦能力向上にも繋がるだろう。

つまり作戦支援であり、ウクライナがロシアに対し、長期間粘り強く戦えているように他国からの弾薬や燃料支援は継戦能力の必須要素である。相互支援及び抑止という視点からも理想的には日米豪がそれぞれの国に共同の弾薬庫や燃料施設を構築するといったことも今後重要になっていくと考えられる（ただし、既に日本国内には米軍の燃料、弾薬庫は存在している）[48]。その際には、これまで以上に施設を地下に設けるといった施設の強靭化、抗堪化が肝要である。

また、宇宙領域に関しては、人工衛星への宇宙状況把握（SSA）センサーといったミッション機材の相乗りとも言われるホステッド・ペイロードが普及しつつあるが、今後、既にホステッド・ペイロード協力について合意している日米だけではなく[49]、さらなる地域諸国あるいは「自由で開かれたインド太平洋」構想に賛同する一部の欧州諸国も参加する形で同協力が進めば、日本が運用する衛星に対する攻撃あるいは妨害行為は、複数国に対する攻撃あるいは妨害と見なすことも可能となる。このことは、少なくとも相手の意思決定や計算を不確実にすることができるだろう。

---

45 Beatrice Heuser and Harold Simpson, “The Missing Political Dimension of Military Exercises,” *The RUSI Journal*, Vol. 162, No. 3, July 2017, p. 22, 24; Raymond Kuo and Brian Dylan Blankenship, “Deterrence and Restraint: Do Joint Military Exercises Escalate Conflict?” *Journal of Conflict Resolution*, Vol. 66, No. 1, July 2021, pp. 3-31.

46 U.S. Department of State, “Joint Statement on Quad Cooperation in the Indo-Pacific,” February 11, 2022. https://www.state.gov/joint-statement-on-quad-cooperation-in-the-indo-pacific/

47 The White House, “Remarks by President Biden, Prime Minister Morrison of Australia, and Prime Minister Johnson of the United Kingdom Announcing the Creation of AUKUS,” September 15, 2021. https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/09/15/remarks-by-president-biden-prime-minister-morrison-of-australia-and-prime-minister-johnson-of-the-united-kingdom-announcing-the-creation-of-aukus/; The White House, “Joint Leaders Statement on AUKUS,” March 13, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/13/joint-leaders-statement-on-aukus-2/

48 防衛省『令和４年版防衛白書・資料編』、2022年、165-169頁; 防衛省「在日米軍の対象防衛関係施設の一覧」。https://www.mod.go.jp/j/presiding/law/drone/list_zaibeigun.html

49 外務省「日本国とアメリカ合衆国との間の相互防衛援助協定に基づくホステッド・ペイロード協定に関する書簡の交換」、令和２年12月15日。https://www.mofa.go.jp/mofaj/press/release/press3_000392.html

重要なことは、情報共有や全般的な作戦支援は、各国の戦略の一部であり、戦略構想段階から同盟国及び可能であれば同志国と連携すること自体が、各国の地域安全保障に貢献しようとする強い決意表明であるだけでなく、相手に対する実践的な抑止連携ともなるということである。そして、これはつまり地上、空、宇宙といった領域に関わらず、1か国のみとの対峙ではなく複数の国との対峙を意味し、事態を複雑化させるのと同時に戦略上の計算の複雑化を相手に強いることにもなる。

日本のエア＆スペースパワーを用いた抑止を考える上で欠かせない視点としては、抑止に対する貢献自体は間接的かもしれないが、日本は手強い相手だと認識させることで事態が思わぬ方向に波及するだけでなく酷く悪化する可能性があると認識させ、最終的に相手の自制を引き出すことである。これは、上述の通り日本単独では成し遂げることはできず、複合的であり、どれか一つの取り組みに限定されるものではなく様々な歯止め効果が重なり、抑止として機能するというものである。

結び

戦略及び抑止を語る上では陸・海といった領域がそうであるように、空と宇宙は、これらの領域単体ではなく、その他の領域との関係から考慮する必要がある[50]。人間は、有史以来、地上に生活拠点があり、依然として地上での活動が国際政治に大きな影響を及ぼす。この点に鑑みれば、米国の優れた戦略思想家であるJ・C・ワイリー海軍少将（Rear Admiral J. C. Wylie）が地上における活動の重要性を示唆した通り、「戦争を最終的に決めるのは、銃を持った戦場（地上）の人間」であるという考えは未だに有効であろう。無論、ウクライナ戦争の様相を踏まえれば、今後戦争における無人化が進むことは大いに想定されることであるが、無人機単体で最終決着がつくわけではない。最後は、戦争を始めた人間の意思が必ず介在する。

上記で指摘したように、エア＆スペースパワーのみを駆使した抑止はどちらかと言えば間接的な役割を果たす。無論、識者によっては、無人機や宇宙機の活躍によってエア＆スペースパワーが抑止において全面的な役割を果たすと考えるかもしれない一方、本章はエア＆スペースパワーは現在の文脈においては、あくまで地上での活動に大きく帰結すると考察する。というのは空や宇宙という全球的な空間・領域を用いた抑止は、地上との関係をもって初めて成立するものである。エア＆スペースパワーは、戦略を考える上で欠かすことのできない要素ではるが、あくまで一要素でしかない。換言すれば、欠けてはいけないものの、あくまで全体図の一部でしかない。

他方、全球的な活動範囲を持つエア＆スペースパワーは、誰も占有していない空間・領域であり、日本としては日本周辺の同空間・領域の安定及びその利用を保つことが肝要であることは言うまでもない。そして、戦略的高地である同空間は、まさに地上を見る大きな「目」であり、過去・現在、そして見通せる将来においてもこの「目」を抜きに戦略を立てることはできない程の欠かせない要素である。加えて、常に向けられる天からの目は相手をけん制する一要因となるだろう。また、全球的という特徴から、エア＆スペースパワーを用いた国際連携も活発であり、今

50 Biddle, *Air Power and Warfare*, pp. 4-5; Karl Mueller, "Strategies of coercion: Denial, punishment, and the future of air power," *Security Studies*, Vol. 7, No. 3, 1998, p. 203.; J. C. Wylie, *Military Strategy: A General Theory of Power Control*. 1967. Reprint, Naval Institute Press, ppb. 2014, p. 72.

後の国際連携の方向性がより相互補完的になれば、相手の侵略行為のハードルが一層高くなることだろう。日本としては、エア＆スペースパワーを駆使して、地域の安定を脅かす国を日本独自の力だけでなく同盟国、同志国とともにけん制していくことが、日々重要になっており、その責務を果たすことが地域の安定へと間接的に繋がるだろう。

巻末資料　シナリオゲームの概要と結果

本研究プロジェクトでは、研究会委員をプレイヤーとして、二回に渡るシナリオゲーム（ウォーゲーム）を実施し、新領域における抑止の課題を検証した。一回目のゲームは2022年７月に「**台湾海峡有事**」を想定して実施され、二回目のゲームは同年11月に「**東シナ海グレーゾーン**」を想定して実施された。以下にその概要と結果を記す。

ゲームは相互作用的なマトリックス・ゲームとして実施され、研究会委員が中国、米国、日本といったチームに分かれて実施する形を採った。各チームはそれぞれ戦略目標を設定した後に意思決定を行い、予め配布された戦力カードを所定のマトリックスに置くことで行動を示した。各チーム間の相互作用の結果はルールに基づいてゲームマスターにより判定され、また必要な場合にはサイコロを用いて判定された。

ゲームは複数回のターンで行われ、各ターン内で新領域行動フェイズ、ミサイル攻撃フェイズ、作戦行動フェイズ等の個別のフェイズが実施された。第二ターン終了後と全体のターン終了後には外交フェイズが挿入され、各チームによる立場表明が行われた。そして、ゲーム終了後にはプレイヤー全員による総合的な講評が実施された。

【第一回シナリオゲーム】「台湾海峡有事」

中国、米国、日本の三者のプレイヤーを設定し、**中国が台湾への武力攻撃を開始している状況からのスタート**という形で実施された（本ゲームにおいては武力紛争に至る前段階としてのグレーゾーン段階は設定されなかった）。

０．戦略目標設定

まず各々のチームは**戦略目標**を立てた。中国チームの最優先目標は台湾の占領・併合であり、二義目標は第一列島線内の支配確立（台湾東部海域を含む）となった。米国チームの最優先目標は台湾における親米政権の維持（及びアジア太平洋における米国覇権、航行の自由及びグアムとの連絡線の維持）となり、二義目標は中国による台湾侵攻の阻止となった。日本チームの最優先目標は日本の領土・領海の保全（特に南西諸島）となり、二義目標は東シナ海の現状維持となった。

１．第一ターン

第一ターンの新領域行動フェイズにおいて、中国チームは日本及び台湾の都市を新領域（宇宙・サイバー領域）の手段を用いて攻撃した。日米チームは日本を同じく新領域の手段で防衛した。判定の結果、この攻撃は効果を発揮しなかった（日台の士気低下をもたらさなかった）。中国チームはまた、ミサイル攻撃フェイズにおいて、「グアム」、「台湾」、「沖縄」、「西日本」及び「東日本」の各航空基地をミサイル攻撃により幅広く破壊した。日米チームも中国沿岸部の航空

基地四つのうち一つを破壊した。

作戦行動フェイズにおいて、中国チームは「東シナ海北部」「東シナ海南部」「台湾海峡」「南シナ海北部」「台湾東部海域」と幅広く支配した。日米チームは「フィリピン海」を支配したほか、台湾・グアム間の連絡線保持のため「台湾東部海域」の支配を試みたが、同海域での中国との戦闘に敗れ目標達成はならなかった。

２．第二ターン

第二ターンの新領域行動フェイズにおいて、日米チームは引き続き日本の都市を新領域の手段で守ろうとしたが、中国チームは日本・台湾を新領域の手段で攻撃しなかった。しかし中国はミサイル攻撃フェイズでは引き続き広範囲に渡って日米の航空基地の完全破壊を目指した。「グアム」、「台湾」、「西日本」の基地が完全破壊され、以後は使用不可となった。「フィリピン」の基地も破壊された。「沖縄」は攻撃されるも被害を免れ、「東日本」の基地は攻撃されなかった。日米は第一ターンとは異なる中国沿岸部の航空基地を一つ破壊した。しかし前回破壊された中国の航空基地は機能復旧した。

作戦行動フェイズにおいて、中国チームは「東シナ海北部」「東シナ海南部」「台湾海峡」「南シナ海北部」「台湾東部海域」を引き続き支配した。米国チームは通常戦力において数的に不利な状況下で、戦域へのB-61戦術核爆弾の前方展開を宣言した。中国チームはこの展開を受けて既存の「無条件核先行不使用宣言／消極的安全保証宣言」の撤回を宣言した。日本チームは東シナ海の支配奪還を放棄し、本土防衛最優先の姿勢に転換した。しかし中国からのミサイル以外の日本攻撃がなかったため、自衛隊戦力を台湾・グアム間の連絡線保持を意図する米軍作戦に振り向ける方針を採用した。

第二ターン終了後の外交フェイズにおいて、中国チームは台湾海峡紛争への日米の介入停止、第一列島線内への日米の艦艇・航空機の進入不可の受け入れを求めた。日米チームは中国の台湾侵攻の停止を求め、台湾防衛のためなら核使用も辞さない強い決意を示して中国の侵攻断念を求めた。外交フェイズは停戦に失敗し、ゲームは継続された。

３．第三ターン

第三ターンの新領域行動フェイズにおいて、日米チームは同じく新領域の手段を用いて日本の都市を守ろうとしたが、中国チームは日本・台湾を攻撃しなかった。ミサイル攻撃フェイズで中国チームは攻撃しなかったが、日米チームは中国沿岸部の四つの航空基地をいずれもB-61戦術核爆弾を搭載したB-2ステルス爆撃機による攻撃で完全破壊した（なお判定により、これに伴う付随的被害は小となった)。この結果、中国は「台湾東部海域」に爆撃機・戦闘機を展開できなくなった。

作戦行動フェイズにおいて、中国チームは「東シナ海北部」「東シナ海南部」「台湾海峡」「南シナ海北部」を引き続き支配し、人民解放軍の台湾上陸を宣言した。更に「南シナ海南部」を支配したことで、前回の破壊から機能復旧した「フィリピン」の航空基地を使用不可とした。具体的には、フィリピン政府に圧力を加えて日米の使用を拒否させた。しかし、日米の核攻撃の結果として爆撃機・戦闘機を展開できず、かつ台湾周辺の海域に戦力を分散したことで、「台湾東部海域」において日米との海戦に敗北した。日米チームは「フィリピン海」の支配を継続した上

で、「台湾東部海域」に戦力を集中した。中国沿岸部の航空基地を核攻撃で無力化した結果として中国航空戦力の大幅削減に成功し、同海域での中国との海戦に勝利した。ただし台湾上陸は宣言しなかった。

４．第四ターン

第四ターンの新領域行動フェイズにおいて、中国チームは台湾のみを新領域の手段を用いて攻撃したが、判定により効果なしとなった。日米チームは日本を守るが、中国の攻撃は行われなかった。ミサイル攻撃フェイズで中国チームは「沖縄」の航空基地を核攻撃し、完全破壊した（判定により付随的被害は小であった）。日米は中国をミサイル攻撃しなかった。この時点で残る日米の使用可能な航空基地は東日本の二つの基地のみであった。

作戦行動フェイズにおいて、中国チームは引き続き「東シナ海北部」「東シナ海南部」「台湾海峡」「南シナ海北部」「南シナ海南部」を支配した。人民解放軍の台湾上陸作戦も継続した。「台湾東部海域」において日米との再決戦を挑むも、引き続き爆撃機・戦闘機を同海域に展開できず、台湾周辺海域への戦力分散もあって、敗北した。日米チームは「フィリピン海」の支配を継続した上で、「台湾東部海域」への戦力集中により、中国との決戦に勝利した。結果、グアムから台湾への連絡線を維持し、米軍の台湾上陸を宣言した。

第四ターン終了後の外交フェイズにおいて、中国チームは停戦条件として台湾に上陸した米軍の撤収を求めた。中国沿岸部が核攻撃を受け、「台湾東部海域」での決戦に続けて敗北したものの、まだ残存戦力はあり、時間をかければ核攻撃を受けた航空基地の復旧も可能で、爆撃機・戦闘機を再び「台湾東部海域」に展開できるようになると主張した。紛争に負けてはおらず、更なる（核を含む）エスカレーションの可能性を考えれば、米軍の台湾からの撤退に理があるとの主張を行った。

日米チームは停戦条件として台湾に上陸した人民解放軍の撤収を求めた。グアムから台湾への海上連絡線が維持されている以上、米国としても紛争に負けたとは考えていないとの立場を示した。更なる（核を含む）エスカレーションで米国が中国共産党政権の打倒という目標に転換する可能性を考えれば、中国にも紛争停止の理があると主張した。日本チームは米国チームとやや異なる立場を示し、米国の停戦条件の要求に賛同するが、その実現可能性は低いとの見方を示した。そして沖縄が核攻撃された以上、日本は独自核武装を追求せざるを得ず、これに対する米国の支援を要求する姿勢を示した。

５．評価

外交フェイズでは再び停戦に失敗したが、ゲームはこれで終了となった。ルールに基づく**総合的な勝敗判定**は、中国チーム５点、日米チーム４点で中国側の辛勝となった。ただしグアムから台湾への海上連絡線は維持され、台湾本島での米中双方の地上軍戦闘が続く形でのゲーム終了となった。

プレイヤーによる**総合的な講評**としては、全般的にサイコロの目の影響もあり、日米側に不利なゲーム展開が目立ったことが指摘された。中国チームの圧倒的な量的優位の前に、日米チームは戦力を分散せず集中投入することを強いられた形となった。また、核兵器の先行使用によってようやく中国チームの優位に対抗できた面があった。中国チームとしては、台湾海峡への日米の

進入を阻止するため、「東シナ海南部」「南シナ海北部」「台湾東部海域」への戦力分散を強いられた。結果として日米チームが集中的に戦力投入してきた「台湾東部海域」での決戦に二度敗北し、グアムから台湾への連絡線を遮断できなかった。このことが台湾本島における米中の地上軍戦闘というゲーム結果に繋がった。

核攻撃はやはりゲームチェンジャーであり、これによって中国沿岸部の航空基地が壊滅したことで、「台湾東部海域」に爆撃機・戦闘機部隊を展開できなくなったことが日米チームに有利に作用した。（核を含む）エスカレーションは常に劣勢な側が行う、という考え方を実証する例となった。他方、中国チームによる「沖縄」の航空基地への核攻撃は、同基地がそれ以前の通常弾頭によるミサイル攻撃での破壊から免れていたことによる、偶然の結果であった。既に破壊されていたならあえて核攻撃をする意味は乏しかった。攻撃の意図は純粋に軍事的なもので、長期の政治的含意を考慮していなかった。

新領域（宇宙・サイバー領域）の要素は、今回のゲームでの決定的要因とはならなかった。都市攻撃（による士気低下）への作用は限定的で、作戦支援での新領域活用もあくまで戦力増幅装置（フォースマルチプライヤー）としての支援要素に留まった。抑止の文脈においても、**新領域による攻撃（ないし反撃）は核攻撃のような水晶玉効果（使用されれば何が起こるかが相手に明白であるという効果）を欠いており、抑止手段として活用しにくい面**があった。**ゲームの展開がいきなり武力衝突から始まる構図であり、グレーゾーン段階の対立を経ないものであった背景も大きい**と考えられた。しかるに、新領域が大きな意味を持つのは例えば認知戦（cognitive warfare）のような文脈であって、こうした文脈に注目すれば、**グレーゾーン段階からのエスカレーションを考慮したゲーム構造である方が、新領域の要素のインパクトがより大きくなる**のではと推察された。

【第二回シナリオゲーム】「東シナ海グレーゾーン」

第一回のゲーム結果を受け、新領域を考慮したグレーゾーンにおける抑止の課題について検討するための「東シナ海グレーゾーン」ゲームを行った。同じく中国、米国、日本の三者のプレイヤーを設定し、東シナ海の「尖閣近傍海域」並びに（日中中間線付近の）「ガス田周辺」におけるグレーゾーン段階の対決を想定したゲームとした。

０．戦略目標設定

まず各チームは戦略目標を決定した。これらは自国チーム内でのみ共有され、終了時まで他国チームには明らかにされなかった。中国チームには国家主席から「台湾統一に集中するため、尖閣諸島及び東シナ海の排他的経済水域（EEZ）を巡る日本との問題を中国有利に終決させよ。当該行動を通じ、可能なら台湾統一の行動を起こす前に日米同盟を弱体化させよ」との指示が与えられ、これを踏まえて「東シナ海における海上・航空優勢の確立」「尖閣諸島における実効支配の確立」を戦略目標として掲げた。また、台湾統一前の武力衝突回避、米国の介入に至らない範囲のグレーゾーン事態の模索、尖閣諸島に「漁民」を上陸させる、という考慮事項も決定された。

米国チームは戦略目標として「東シナ海における秩序維持、力による現状変更を許さない」、

「東シナ海の安定を目指し、日中中間線を越えた活動を阻止」、「日米分断防止」を掲げた。そして中国側に物理攻撃をさせないこと、作戦態勢整備のために認知領域のベースづくり、情報開示、ノンキネティックな攻撃、情報収集等を行うこと、を考慮事項とした。同様に、日本は戦略目標として「中国による現状変更を可能な限り阻止し、原状回復を図る」「通常戦を可能な限り回避する」「日米の分断を許さない」ことを掲げ、「離島」の現況を認識する能力を阻害する宇宙・サイバー攻撃が行われる場合には武力攻撃事態と見なす、ことを考慮事項とした。

１．第一ターン

第一ターンの新領域行動フェイズにて、中国チームは以下の行動を採った。まず宇宙領域において、日本の測位・航法・タイミング（PNT）能力に対するダウンリンクジャミング、情報収集・警戒監視・偵察（ISR）衛星に対するアップリンクジャミング及び幻惑・盲目化の試みを行った。サイバー領域においては、沖縄県警本部長のアカウント情報をハッキングして偽情報を発信するとともに、海保の画像伝送システム（民間通信衛星）、石垣島で海保巡視船に燃料補給を実施する民間会社の補給管制PC、JR東日本の関東エリア運行制御を行うシステムに対するマルウェア攻撃を実施した。その結果、沖縄県警は本島内の反基地デモ対応に翻弄され尖閣対応が不可能になり、海保の尖閣諸島を含む東シナ海における活動が阻害され、東日本地域の交通麻痺の結果として防衛省職員等の対応に影響が出る等の日本チームの被害が生じた。

日米チームはこれに対して、宇宙領域において中国のPNT能力に対するダウンリンクジャミングを行い、またISR衛星に対する幻惑・盲目化の試みを行った。またサイバー領域では中国軍事委員会装備発展部直属の衛星測量・制御用サーバにマルウェア攻撃を行った。

作戦行動フェイズにおいて、中国チームは尖閣諸島をカバーできる範囲のガス田エリアにオイルリグ２基を新設し、海上航空優勢確立の拠点とした。また、尖閣諸島周辺に漁船200隻、公船４隻を派遣した。更に尖閣諸島北方のリグ周辺に駆逐艦２隻、戦闘機10機、ドローン１機を展開させた。

これに対し、日本チームは展開可能な全巡視船を尖閣諸島周辺に展開することを試みたが、上記の通り海保のシステムにサイバー攻撃を受けたために、巡視船２隻の展開に留まった。また、海自護衛艦２隻も展開させた。同時に空自部隊を那覇に展開することを試みたが、後者は衛星への攻撃で空自の活動が妨害されたため、展開できなかった。その他、陸自の水陸機動団が長崎県相浦駐屯地で待機した。米国チームは海兵隊の航空機20機で情報収集と抑止活動を試み、またグアムに戦略爆撃機（B-2/B-52）を前方展開させた。この状況において、日本チームの尖閣近傍海域における状況把握能力は著しく制約されたが、日本チームはまだ武力攻撃事態認定には至っていない。

２．第二ターン

第二ターンの新領域行動フェイズにおいて、中国チームは宇宙領域での行動として、日本の宇宙状況把握（SSA）能力に対するアップリンクジャミング、通信能力に対するダウンリンクジャミング、ISR衛星に対する幻惑・盲目化、更に静止軌道上の通信衛星に対する同軌道ASAT攻撃（ロボットアーム使用）を実施した。この結果、海保のみならず自衛隊も衛星通信が不通となり、短波通信のみとなる事態が生じた。スターリンクによる通信サービスも使用不可となった。サイ

バー領域では、与那国島の陸自の沿岸監視隊と、上部組織である西部方面情報隊の間の通信、在日米国大使館武官室の通信用PC、米宇宙軍のSSAシステム、に対するマルウェア攻撃を実施した。結果として日本は与那国島からの情報を得られなくなり、米国のSSA能力も阻害された。

日米チームはこれに対して、中国海警の上部組織である武装警察（武警）の通信用サーバのデータ通信を妨害するマルウェア攻撃を実施した。これによって、中国海警の本部と公船の連絡が滞る事態が発生した。

作戦行動フェイズでは、中国チームは尖閣諸島周辺の接続水域に漁船500隻、公船６隻を展開させ、潜水艦１隻に同接続水域を通過させた。また別の潜水艦１隻をオイルリグ周辺に配置したうえ、駆逐艦６隻、ドローン２機を尖閣諸島及びオイルリグ周辺に配置した。更にPLA陸軍300名を２基のオイルリグに分散して配置し、第四世代戦闘機40機を尖閣諸島とオイルリグ周辺に展開させた。

日本チームは護衛艦部隊（護衛艦５隻、潜水艦２隻）を中国と尖閣諸島の間に派遣し、中国の海上連絡線の遮断を試みた。また大正島周辺での日米共同演習実施を警告し、中国公船及び漁船の退去を促した。ただし、中国側の退避の動きを妨害しないため、あえて中国公船及び漁船への通信妨害は実施しなかった。また、中国側が尖閣諸島に不法上陸・占拠を行う可能性があることを世界に対して暴露し、先のターンで行われたJR東日本のサイバー攻撃の帰属（アトリビューション）特定も実施して、中国ないしは北朝鮮によるサイバー攻撃という点まで明らかにした。

米国チームは大正島周辺での日米共同演習実施に向けて強襲揚陸艦及び航空機の展開を行うほか、米サイバー軍としてJR東日本へのサイバー攻撃について中国からであると特定し、発表した。また、中国による重要インフラへの攻撃可能性に対する警戒強化を日本チームに要請した。

第二ターン終了後の外交フェイズにおいて、各チームは下記のような主張を行った。まず中国チームは尖閣諸島周辺の中国漁船に対して日米チームが軍艦を派遣してきたことに抗議した。また尖閣諸島における日米共同演習の実施は軍事的脅威を煽る憂慮すべき事態だと非難した。これに対して、日本チームは自国がサイバー攻撃を受け、衛星による現地の状況把握も困難という状況では、中国側が領土奪取の野心をもって漁船を展開していると考えざるを得ないと反駁した。米国チームは日米同盟の下に共同演習を行うものであって、現状は準有事に近いものであるとの認識を示した。中国側がハイブリッド戦を仕掛けている可能性があるとの認識の下、その可能性を排除するために共同演習を実施するのであり、事前通告の上での演習は問題ないと主張した。日本チームも軍事演習は正統な国益の追求であり、中国漁船の退避を改めて促した。これに対して中国チームは漁船に被害があれば日米の責任となると非難し、漁船全てに演習実施の告知を行えるのかと日米を追及した。事態は外交フェイズで終息せずに第三ターンに向かった。

３．第三ターン

第三ターンの新領域行動フェイズにおいて、中国チームは宇宙領域での行動として、日本の静止軌道上の通信衛星に対する同軌道ASAT攻撃、SSA能力に対するアップリンクジャミング、PNT及び通信能力に対するダウンリンクジャミング、ISR衛星に対する幻惑・盲目化攻撃を実施した。また、サイバー領域では、在日米海軍佐世保基地の補給システムPC、陸自の水陸機動団が所在する相浦基地への民間送電制御システム、在日米軍岩国基地の管制システム、沖縄エリアの航空管制を担う神戸航空交通管制部の統合管制情報処理システム、NTT東日本の官庁用秘匿

メールサーバ、に対するマルウェア攻撃を実施した。この結果、佐世保基地の米軍部隊が尖閣諸島に展開できなくなり、水陸機動団が稼働不能になり、岩国基地の航空管制が不可能になり、沖縄エリアの航空管制システムが機能停止し、官庁のクローズド系システムが使用不能になる等の被害が生じた。

日米チームはこれに対して宇宙領域では、中国の通信衛星に対するアップリンクジャミング、通信能力に対するダウンリンクジャミング、PNT能力に対するダウンリンクジャミング、ISR衛星に対するアップリンクジャミング、ISR衛星に対する幻惑・盲目化攻撃、SSA能力に対するアップリンクジャミング、静止軌道上の通信衛星に対する同軌道ASAT攻撃を実施したほか、サイバー領域では人民解放軍空軍の無人機部隊の飛行計画入力システムへのマルウェア攻撃を行った。この結果、日中双方がともに衛星能力ダウンとなり、PNT・ISR・通信能力のいずれもが阻害される状況となった。

作戦行動フェイズでは、中国チームは尖閣諸島周辺に漁船800隻、公船８隻を配置し、日米共同演習は無視する姿勢を採った。またオイルリグ周辺に戦闘機50機を搭載した空母１隻と揚陸艦２隻、潜水艦１隻を配置した。更に尖閣諸島周辺に第四世代戦闘機80機、ドローン３機を展開させた。

日本チームは中国の動きへの対抗のため日米共同演習名目での米空母部隊の尖閣諸島への展開を望んだものの、佐世保基地へのサイバー攻撃の結果として米国チームによる米海軍部隊の展開が不可能になり、一部の戦闘機のみを展開する形となった。ただし判定により、第四ターンから佐世保基地の機能は復旧することとなった。日米チームはまた、演習区域と安全区域の明確化を図った。

４．第四ターン

第四ターンの新領域行動フェイズにおいて、中国チームは宇宙領域での行動として、引き続き静止軌道上の通信衛星に対する同軌道ASAT攻撃、SSA能力及びISR衛星、通信衛星に対するアップリングジャミング、PNT能力及び通信能力に対するダウンリンクジャミング、そしてISR衛星に対する幻惑・盲目化攻撃を実施した。また、サイバー領域では、在日米軍司令部内の自衛隊・米軍間の専用メール回線用PC、海自・自衛艦隊の後方支援系システム、陸自・九州補給処の後方支援系システム、統幕中央指揮システム、市ヶ谷・横田・横須賀地区を担当する電力会社（東京電力）の給電システムに対するマルウェア攻撃を実施した。結果、自衛艦隊の展開ができなくなり、関東地方で停電が起きる等の被害が発生した。

日本チームはこれに対して宇宙領域では、静止軌道上の通信衛星に対する同軌道ASAT攻撃、SSA能力及びISR衛星、通信衛星に対するアップリンクジャミング、PNT能力及び通信能力に対するダウンリンクジャミングを実施した。また、サイバー領域では、中国深圳市のスマートグリッド、天津市を統括する携帯電話会社の通信システムへのマルウェア攻撃を実施した。結果、深圳市は停電、天津市の通信システムが使用不能となる被害が発生した。

米国チームも同様に宇宙領域では、静止軌道上の通信衛星に対する同軌道ASAT攻撃、SSA能力及びISR衛星、通信衛星に対するアップリンクジャミング、PNT能力及び通信能力に対するダウンリンクジャミング、そしてISR衛星に対する幻惑・盲目化攻撃を実施した。また、サイバー領域では、北京市を統括する衛星電話会社の通信システム用PC、上海市のスマートグリッド、

河北省雄安新区（スマートシティ）の交通システム、中国中央電視台の総合放送用サーバ、三峡ダムの水位管理システムへのマルウェア攻撃を実施した。結果、北京の移動体ネットワークが使用不能になり、上海市が停電し、河北省のスマートシステムが麻痺し、中央電視台が使用不能になり、三峡ダムの水位が上がる被害が発生した。

また、日米中の静止衛星が破壊されたほか、全衛星が機能停止する被害も発生した。

作戦行動フェイズでは、中国チームは悪天候を理由に漁民が尖閣諸島に上陸した。合計300隻、1500人程度が上陸し、内訳は魚釣島に1000人、大正島に500人となった。そして中国公船を救助のためと称して領海内に侵入させた。更に空母１隻、駆逐艦４隻、潜水艦２隻を尖閣諸島周辺に配置、その外側の尖閣諸島海域手前には空母１隻、揚陸艦３隻、潜水艦１隻を配置した。これに加えて戦闘機90機（第四世代機80機、第五世代機10機）も展開させた。

日本チームはこれに対して展開可能な海自の全戦力を尖閣諸島の演習海域に投入することを試みたものの、中国のサイバー攻撃により後方支援系システム等がダウンしたため、展開することができなかった。

米国チームも佐世保基地の機能復旧に伴い、第三ターンで投入予定であった全海洋アセットを尖閣海域に投入することを試みたが、衛星の機能停止と自衛隊との通信途絶の影響により展開できなかった。ただし、グアムにB-2及びB-52爆撃機を前方展開させたほか、嘉手納から米空軍の戦闘機を南西諸島に展開させ、また「対日サイバー攻撃は中国発である」というアトリビューション結果を公表する対応を採った。

復旧に関してはサイコロの判定に従い、日米ではシステムダウンした８件のうち、米宇宙軍のSSA能力が回復した。中国はシステムダウン７件のうち、中央電視台、北京市、上海市、三峡ダムの４件の機能が回復した。

５．第五ターン

第五ターンの新領域行動フェイズにおいて、中国チームは宇宙領域での行動として、第四ターンと同様の同軌道ASAT、ジャミング、幻惑・盲目化攻撃を実施した。また、サイバー領域では、在日米空軍嘉手納基地の飛行計画を処理するシステムに対するマルウェア攻撃を実施した。結果として嘉手納基地の機能不全による米軍戦闘機の撤退という被害が発生した。

日本チームも宇宙領域での行動として、第四ターンと同様の攻撃を実施した。サイバー攻撃は実施されなかった。

米国チームは宇宙領域での攻撃は行わなかったが、サイバー領域での行動として、浙江省の水平線以遠（OTH）レーダー、対艦弾道ミサイル（ASBM）部隊の通信用PCに対するサイバー攻撃を実施した。結果、ASBM部隊の通信遮断が発生し、ASBMが使用できなくなる被害が発生した。

作戦行動フェイズでは、中国チームは空母１隻、揚陸艦３隻、潜水艦３隻を尖閣諸島の接続水域内に配置し、戦闘機90機の展開を継続した。

日本チームは武力攻撃事態認定を行い、米国に日米安保条約第五条の発動を要請した。また武力で漁民の排除を目指すとしたほか、拡大核抑止コミットメントの再確認を米国に求めた。しかし、日本自身としては宇宙領域での攻撃を除き、選択可能な対応策がなかった。

米国チームはサイバー攻撃からの復旧に伴い、空母・軍艦等を尖閣諸島周辺に展開させた。ま

た、尖閣防衛へのコミットメントとして「核を含む必要なあらゆる手段も辞さず」と宣言した。「対日米サイバー攻撃は中国発である」ことも重ねて非難した。国連安保理には、「ロシアのウクライナ侵略をしのぐ暴挙」として提起し、日米共同声明も発表した。

第五ターン終了後の外交フェイズ（二回目）において、各国チームの主張は以下のようなものであった。まず中国チームは、自身が武力攻撃を全くしていないのに、日本が武力攻撃事態を認定するとはどういうことか、と日本を激しく非難した。中国チームの主張によれば、現状では中国軍は尖閣諸島に避難した漁民保護のために公海上にいるに過ぎない。一方で、米国からの上海市のサイバー攻撃により10万人の市民が死亡した。これはもはや戦争行為であり、自衛権を行使せざるを得ない、と日米を厳しく非難した。

日本チームは、日本各地の機能停止状況、米国から日本へのサイバー攻撃は中国発とのアトリビューション結果の共有があったこと、そして尖閣諸島における中国漁民の展開状況から、もはや明白に武力攻撃がなされたと認定せざるを得ない、との主張を行った。そして全ての中国漁民や艦艇等の撤退を求め、これが実現されなければ全面戦争を覚悟せざるを得ない、これは最後通牒である、旨の通告を中国に対して行った。

米国チームは、米軍基地や衛星への攻撃は中国によるものであるとの非難を行った。現下の状況は中国のハイブリッド戦及び三戦（輿論戦・心理戦・法律戦）が実施されている状況にあるとの認識も示した。その上で、米国としてはこの事態に日米安保条約第五条を適用するとの方針を示し、中国軍に尖閣諸島周辺海域からの撤退を求めた。このままの事態が続くのであれば、あらゆる手段をもって対応する準備があるとの姿勢も示した。日本だけでなく、グアムにおいても必要な戦力を展開しているとも通告した（核戦力の存在を示唆）。

これに対して中国チームは、中国としては一切戦争するつもりはないが、攻撃されれば自衛権に基づいて対応するしかない。現状、中国の海軍戦力の方が優位にある状況で日米が戦うことができるのか。日本側は一人も死んでいないのに、武力攻撃事態の認定はおかしいのではないか、という反駁を行った。

日本チームは、我が国の領土である尖閣諸島において領土の不法奪取が行われている。漁民と称するものは海上民兵だと考えている。漁民やオイルリグ上の民兵、宇宙やサイバー領域における攻撃といった全ての状況が積み重なった上での武力攻撃事態認定である。漁民に関しては海上封鎖して退去を一定期間待っていたが、最後通告に従わなかった以上、今後は上陸作戦での排除も検討する、との反駁を行った。

中国チームはこれに対して更に、我々の方が現状で圧倒的に優位にある。日米は本当に戦うのか。水陸機動団が上陸する前に中国の陸兵も入ることになるが、排除は無理ではないか。中国側はオイルリグ上に対空サイトやレーダーサイトも保有する状況であり、日米は再考した方が良いのではないか、との主張を行った。

ここでゲームは終了した。

ゲーム終了後の**総合的な講評**としては、まず**中国チーム**のコメントとして、**台湾統一前の武力衝突を避けつつ、尖閣諸島に漁民を上陸させるという国家主席からの指示を守る方針を達成できた**、公海上の移動式リグに陸兵が配備されていたことは有効な手段であった、との指摘があった。

日本チームからは、日米の分断こそ回避できたものの、**中国側の現状変革行動を阻止できな**

かった。しかしどのようにしても止められなかったのではないか。**当初、なるべく多くの戦力を前方展開する方針で対応しようとしていたが、中国側のサイバー攻撃でその戦略が潰されたのが痛恨であった**、旨の指摘があった。

米国チームからは、東アジアにおける秩序維持や日米の分断阻止は達成できたと考えるものの、**うまく認知領域における情報戦に対処できなかった**。アトリビューション困難な形でノンキネティックな手段を通じて時間稼ぎを行い、中国側を抑止するつもりであったが、**中国側のサイバー攻撃で日米の動きが止まったのが想定外だった**、との指摘があった。

全体の意見交換では、**新領域でのエスカレーション**について、次の点が指摘された。まず、**日本（自衛隊）に中国軍の動きを止めるためのサイバー攻撃の選択肢がなかった**ことが注目された。これは自衛隊のサイバー能力を考慮すればそのような攻撃ができないことが前提として存在したが、**問題は中国側が第三・第四ターンにおいて物理領域で動いたときに、有効なサイバー攻撃による（拒否の）選択肢が存在しなかった**ことであった。

また、米国も対兵力（カウンターフォース）ではなく対価値（カウンターバリュー）の文脈で中国に対するサイバー攻撃を行っていたが、米国がもっと踏み込んでいれば結果も変わったかもしれない、全面戦争の想定で核エスカレーションまで達していたかもしれない、との指摘があった。しかし**新領域のエスカレーションを読み切れない**面も大きかった。キネティックなミサイル攻撃等と異なり、**サイバー攻撃では戦力想定が難しかった**。

更に、日米は漁民に尖閣諸島からの退避を求めていたので、中国側のPNT能力に対するジャミングを当初避けていた。実際にも、海上民兵への通信阻害については、躊躇が働く可能性が高いとされた。

結果的に、以下のような**ゲームの総括**がなされた。まず、**マルウェアは解析されて対処されると再利用はできず、その性質上一度しか使えないので、結果的に各所で一斉に使われて急激なエスカレーションが起こる**ことが分かった。

次に、グレーゾーン事態においては**事態がグレーである限り、先手有利となり、攻撃側有利**となる。**米国側の了解のもと、尖閣諸島に日本側が先に何らかの人員を上陸させておくことで、事態がグレーではなくなり、中国側が奪取を試みる上でのコスト増となるため、結果的に抑止に繋がった可能性**がある。ただし、今回のゲームでは序盤で沖縄県警の動きが封じられたため、もし選択していても有効に実施できなかった可能性がある。この点は**法執行機関に対する新領域を用いた攻撃に対するレジリエンス向上の重要性**を示すものとなった。

尖閣諸島を守るためには**日米の側からもエスカレーションのラダーを上げていくことが対応として重要**である。しかし、**中国側のサイバー攻撃でそのような選択肢が潰された**ことがゲームにおいては大きな意味を持った。

日本の**武力攻撃事態認定**について、**認定のハードルが（新領域を含む）各要素において足りないが、総合的には越えていると見るとき、どのように認定するかについては、今後、議論を深める必要性がある**ことがゲームによって示された。

「新領域における抑止の在り方」事業　事務局

福田　潤一　笹川平和財団安全保障研究グループ　主任研究員
渡部　弥生　笹川平和財団安全保障研究グループ　アシスタント

War 3.0: 激変する戦争　―新領域（宇宙・サイバー）が迫る抑止の深化―

2024年 3 月発行
発行者　公益財団法人　笹川平和財団
〒105-8524　東京都港区虎ノ門 1 -15-16　笹川平和財団ビル
Tel. 03-5157-5430　URL https://www.spf.org/

SPF 笹川平和財団