「激動する世界の中で、日本が進むべき道
―新領域でのインテリジェンス強化を目指して―」

長迫　智子

１．はじめに

現在、世界の安全保障の様相は大きく変化している。陸、海、空といった伝統的な戦闘領域に加え、宇宙領域およびサイバー領域が新たに登場したことは、古典的な「戦争」の概念を一変させた。特に、サイバー領域は、仮想的な空間であるがゆえにその影響力は絶大なものである。サイバー領域は、インターネットを通じて物理空間のあらゆるモノやヒトと接続されるようになり、重要インフラなどへのサイバー攻撃は、単なる犯罪レベルを超えて安全保障上の問題を引き起こすようになった。さらには、ソーシャルネットワークサービス（SNS）等を通じて、サイバー空間を通じた影響力行使が容易になったことで、われわれの認知領域すらも戦場とみなされるようになってきている。こうした情勢から、陸、海、空の領域に加えて、宇宙領域は第四の戦場、サイバー領域は第五の戦場、認知領域は第六の戦場と呼ばれるようになり、これらは新領域の戦場と考えられている。こうした新領域の戦場の登場で、現代戦とそれに対抗するための安全保障は混迷を極めているといってよい。そうした激動の情勢の中で、我が国が目指すべき道は何か。本稿では、特に安全保障の視点からこの点を議論する。

２．ハイブリッド戦の深化と情報戦の拡大

まず本節では、安全保障上で必要な対策を議論するために、現状の脅威を整理、分析したい。新領域の登場で、戦争はどう変わったのだろうか。

2022 年２月に始まったウクライナ戦争においては、現代戦の形態としてハイブリッド戦争が改めて注目されている。これは決して新しい用語ではなく、2000 年代には米陸軍の教範にすでに盛り込まれており、今回のウクライナ戦争の背景ともいうべきクリミア危機の際にも、ロシアの戦略についてハイブリッド戦争という概念を用いて一定の評価がなされていた[i]。ハイブリッド戦争とは、軍事・非軍事的手段を組み合わせる（＝ハイブリッドさせる）ことによって敵国や非友好国に対しての攻撃が行われる戦争ということが原義である。しかし、インターネット技術の隆盛により、サイバー空間上での情報戦[ii]が大きな影響力を持つようになったことで、サイバー戦がハイブリッド戦争の一角を成すようになった。サイバー戦においては、大別して、相手の情報システムを攻撃することで機能破壊を目的とする機能破壊型サイバー攻撃、相手の情

報を窃取し金銭詐取や影響工作に利用しようとする情報窃取型サイバー攻撃、そして偽の情報や歪曲された情報（＝ディスインフォメーション）を流布することで相手の社会を分断し、国家の意志決定や民主主義の価値観を害する情報操作型のサイバー攻撃が行われる[iii]。このようなディスインフォメーションを用いた情報操作型のサイバー攻撃は、SNS やマイクロターゲティングによるウェブ広告といった新たなウェブサービスを利用することで、単なる偽の情報の流布だけでなく、我々の認知を攻撃し、投票行動や政治行動に影響を与える影響工作の一つであることが認識されるようになった。すなわち、認知戦の登場である。このような複雑化するハイブリッド戦、情報戦の様相を整理したものが下図１となる。

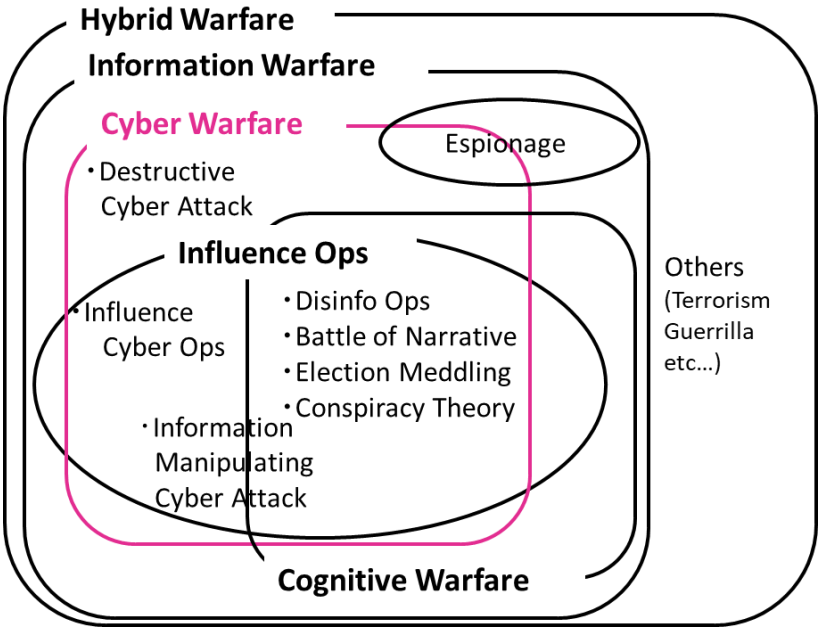

図１．ハイブリッド戦の様相

（長迫智子「我が国の認知安全保障の確保を目指して」『宇宙・サイバーと先端技術研究会報告書（仮）』中曽根平和研究所，2023 年４月発行予定.）

上図のとおり、サイバー領域は様々なオペレーションに影響を及ぼしており、サイバー戦そのものだけでなく、情報戦や認知戦の基層となっている状況である。つまり、現代の安全保障においては、サイバー安全保障の確保が喫緊の課題であるといえる。

２．サイバー安全保障のためのインテリジェンス強化

では、現代の安全保障環境においてサイバー安全保障の確保を目指すのであれば、どういった能力が必要になるのだろうか。それには、まずもってインテリジェンス能力の強化が必要となり、インテリジェンス機関の関与が求められることとなるのであ

る。

サイバー攻撃の特徴には、大別して、①攻撃の実行者の特定が難しい、②攻撃の被害が潜在化する傾向がある、③国境を容易に越えて実行可能である、といった三点の特徴がある[iv]。こうした特徴から、サイバー攻撃の問題解決には、攻撃者を特定するためのアトリビューション能力が必須となる。そして、このアトリビューション問題に最も適切に対応できるのが、インテリジェンス機関であると指摘されている[v]。こうした先行研究によれば、様々な類型のサイバー攻撃が、国境を越える安全保障問題となる可能性がある環境では、国家機関が事前にサイバー攻撃を予期、防止し、潜在的な攻撃者を特定することが求められるようになる。それは従来、インテリジェンス機関が行ってきた「エスピオナージ（諜報：外国政府の軍事的・政治的な秘密について探ること）」と呼ばれる活動に近くなる。さらに、サイバーセキュリティにおけるアトリビューション問題の重要性を指摘している研究[vi]では、従来は明確に区別されてきた、警察・防衛・インテリジェンスの機能をもつ各々の機関の協力と牽制関係に対する見直しの必要性を示唆している。

そして、情報戦や認知戦において、情報操作型サイバー攻撃の主体は各国インテリジェンス機関である[vii]。そして、故意に誤った情報や不適切な文脈を用いた情報や、サイバー攻撃によって窃取した、本来であれば公開されるべきでない情報の流通等がSNSやウェブメディア上で組み合わされるとき、インテリジェンス機関だけでなく、その機関が実行行為を委託している民間会社や個人ハッカー等、多種多様な手段・組織によりオペレーションが行われる。そうした中で、行為者側の意図は旧来のプロパガンダと同様、特定の政治意見の広報・流布にあるため、それは依然として情報戦の範疇にありインテリジェンス機関の所掌となる。一方でそうしたオペレーションに対抗する側は、行為者を調査するためにアトリビューション問題が極めて重要な意味を持ち、やはりインテリジェンス機関の実働が肝要となってくるのである。

しかし、我が国では、その歴史的背景から、対外的な諜報機関が設置されず、そうした議論に対しても反発が大きい。我が国の安全保障において必要な能力であるとしても、国民感情を無視して強行することは、安全保障の意識醸成のうえで禍根を残すことになる。

そのため、今必要なサイバー安全保障に焦点を置き、サイバー攻撃に対して、検知、分析、判断、対処を一元的に行えるサイバーセキュリティの専門機関を設立すべきである[viii]。そのなかで、サイバー領域を中心としたインテリジェンス能力を強化していくことが実効的な方策となるだろう。

３．ハイブリッド戦対処のための国際協力推進

我が国の安全保障は、一国のみの対処で成立しうるものではない。特に、ハイブリ

ッド戦争においては、上述したアトリビューション情報等を中心に、インテリジェンスやサイバー領域の情報共有が重要となる。サイバー戦や情報戦で対抗するには、攻撃者のアトリビューション情報とそれに基づく積極的なサイバー防御が必要であり、これらに対応するための地域的な情報共有は、一国の対応よりも効果的であるためである。あわせて、情報戦や認知戦対処においては、一国を超えて流通するディスインフォメーションをモニタリングし、これらをファクトチェックし反論するような情報発信を各国が連携して行うことも重要になる。

さらには、将来において想定される台湾有事においても、ウクライナ戦争と同様の現代戦が展開されることが予測され、ハイブリッド戦争対処の観点からもインド太平洋地域に強固な対中包囲網を作る必要があるといえる。一方で、近年の日本は、ファイブ・アイズ各国との情報連携を進めるなどインテリジェンス共有体制の強化を図っているが[ix]、これはあくまでも各国個別の協定締結等の取り組みであり、地域的な連携とは言い難い。

そこで、欧州連合（EU）と北大西洋条約機構（NATO）が設置した「ハイブリッド脅威対策センター（The European Centre of Excellence for Countering Hybrid Threats: Hybrid CoE)」と同様に、インド太平洋地域を中心としたハイブリッド脅威対策センターを共同設立することを日本がリードすべきであると考える。なぜなら、日本は自由で開かれたインド太平洋（Free and Open Indo-Pacific: FOIP）構想を提唱した国であり、同地域において、法の支配を含むルールに基づく国際秩序の確保を目指す責任がある。そして、日本はFOIP構想の土台となる自由民主主義の擁護者であるべきであり、自由民主主義を脅かすようなディスインフォメーションの流通、情報戦や認知戦とは断固として戦っていかねばならない。すでに同地域にハイブリッド脅威センターを設立する提言はいくつかなされているが[x]、そこから更に情報戦に特化して、同センターのもとでEUvsDisinfo[xi]を参考にしたFOIPvsDisinfoのような対情報戦イニシアチブを作り、FOIP構想を提唱した日本こそが地域協力体制づくりをリードして進めるべきである。

４．おわりに

激動する世界情勢において、我が国の安全保障を確保するためには、最新の脅威への対応とそれに伴う国際協力が必須である。非伝統的安全保障や新領域における安全保障など様々な方策がある中で、本稿では、サイバー安全保障を中心としたインテリジェンス強化とインド太平洋地域の国際協力が日本の進むべき道の一つであると議論した。折しも、2022年12月には国家安全保障戦略が改訂され、情報戦や認知戦という概念が国家戦略に織り込まれた時分である。今後想定されうる危難を我が国が乗り越えるためにも、これらの戦略がスピード感をもって実効的な法制度に反映され、我

が国の安全保障の確保につながることを祈念し、結語としたい。

（了）（本文 4113 字）

---

[i] 小泉悠「ウクライナ危機にみるロシアの介入戦略:ハイブリッド戦略とは何か」『国際問題』658 号(2017 年１，２月号），2017 年，38-49.

[ii] 情報戦という語は多義的であり、影響工作を中心とみる狭義の情報戦と、情報システムに関わるサイバー攻撃等、「情報」そのものに係る戦闘をも含む広義の情報戦があり、本稿では後者を採用している。

[iii] これらの類型整理は以下文献による。
長迫智子「我が国の認知安全保障の確保を目指して」『宇宙・サイバーと先端技術研究会報告書（仮)』中曽根平和研究所，2023 年４月発行予定.

[iv] 警察庁『平成 27 年回顧と展望　警備情勢を鑑みて　特集「サイバー攻撃をめぐる情勢とその対策」』2016 年３月．P2.

[v] 土屋大洋「サイバーセキュリティとインテリジェンス機関―米英における技術変化のインパクト―」『国際政治』179 号，2015 年，44-56.

[vi] 田川義博・林紘一郎「サイバーセキュリティのための情報共有と中核機関のあり方―３つのモデルの相互比較とわが国への教訓―」『情報セキュリティ総合科学』9 号，2017，17-44.

[vii] 例えば、ロシアであれば GRU（ロシア連邦軍参謀本部情報総局）や FSB（ロシア連邦保安庁）など。

[viii] 新安保戦略では、「内閣サイバーセキュリティセンター（NISC）を発展的に改組し、サイバー安全保障分野の政策を一元的に総合調整する新たな組織を設置する」（国家安全保障会議「国家安全保障戦略」2022 年 12 月 16 日，p22.（https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf)）とあるが、調整のみの組織では、インテリジェンス能力も攻撃への対処能力も有しないため、情報戦に横断的に対処する実行力に欠けると考える。

[ix] 産経新聞「日本の「ファイブアイズ」入りは？　連携強化も課題多く」2022 年 10 月 23 日.
（https://www.sankei.com/article/20221023-TYPPHD6MIZKK3ELOXOGOMGN5D4/）

[x] 笹川平和財団政策提言『日本の防衛外交強化に向けて』2021 年 10 月．p8.
(https://www.spf.org/global-data/user29/SPF_PolicyRec_DefenceDiplomacy_JP_20211015.pdf)
Dr Lesley Seebeck , Emily Williams and Jacob Wallis, “Countering the Hydra: A proposal for an Indo-Pacific hybrid threat centre,” Australian Strategic Policy Institute, 07 June 2022.
(https://www.aspi.org.au/index.php/report/countering-hydra)　など。

[xi] EUvsDisinfo (https://euvsdisinfo.eu/)は、欧州対外行動庁の East StratCom タスクフォースによる旗艦プロジェクトである。EU やその加盟国、共有周辺国に影響を及ぼす、ロシアを中心としたディスインフォメーションのオペレーションに対処するため、2015 年に設立された。