東京大学創発戦略研究オープンラボ（ROLES）有志

国家安全保障戦略改訂に向けた提言

我が国の安全保障を強化するための三つの方策

国家安全保障戦略改訂に向けた提言

我が国の安全保障を強化するための三つの方策

東京大学創発戦略研究オープンラボ（ROLES）有志

2022 年 10 月

序文

日本を取り巻く安全保障環境と求められる安全保障政策

本提言の問題意識

本提言は、日本の新たな『国家安全保障戦略』策定に資することを目的として、東京大学先端科学技術研究センター内に設置された創発戦略研究オープンラボ（ROLES）がまとめたものである。

日本で初めて『国家安全保障戦略』が策定されたのは第二次安倍政権下の 2013 年のことであり、それから 9 年が経過した。この間、日本を取り巻く安全保障環境が激変したことは今更述べるまでもないだろう。中国の軍事的台頭と米中対立はさらに加速しつつあり、朝鮮半島情勢は依然として緊張を孕んでいる。さらに 2014 年にはロシアによる第一次ウクライナ侵攻が、2022 年には第二次ウクライナ侵攻が勃発した。

こうした情勢の変化を踏まえるとき、我が国の安全保障政策が大きな見直しを迫られていることは言を俟たない。

基本的な考え方

まず念頭に置かねばならないのは、国家間の大規模な軍事紛争は安全保障上の脅威として現実に排除できないということである。冷戦後にはこうした紛争の蓋然性が大幅に低下したと考えられた時期もあるが、ロシアによる第二次ウクライナ侵攻は、古典的な大戦争が決して過去のものではないことを白日の下に曝け出した。日本周辺において中国、北朝鮮、ロシアが軍事力の近代化を進めていることと併せて考えるに、大規模な軍事紛争への我が国の対処能力を向上させることは抑止力の信憑性を担保する上で不可欠の課題であると言えよう。ことに中国の戦略核弾頭は 2030 年までに 1000 発に達するとも予測されており、このような状況下では米国の拡大抑止の信憑性が低下し、インド太平洋地域の安全保障環境が一層不安定化する可能性も排除できない。以上の問題意識に基づいて、提言 1 では、「総合・統合・融合防衛力」をキーワードとして幾つかの提言を行った。

他方、対処・抑止能力の向上に関する取り組みは我が国単独では限界がある。ことに第二次ウクライナ侵攻によって欧州正面における抑止リソースの所要が増大するであろうことを考えると、インド太平洋地域における米国のコミットメントは、大幅に低下することはないにせよ、制約されよう。このような条件を勘案するならば、日米同盟の枠組みを超えて安全保障協力を拡大する必要性が一層高まる。したがって、提言 2 では、インド太平洋諸国との安全保障協力に関する提言を中心に取りまとめた。

同時に、現代の安全保障は、古典的な大戦争の抑止・対処の範疇のみには収まらなくなりつつある。情報通信技術（ICT）の急速な発達により、情報はより早く、広く、しかも政府やマスコミといった権威を経由せずに伝播するようになった。このような条件下においては、情報の主要な伝搬チャンネルであるサイバー空間の安全保障はもちろん、そこ流通する情報が人々にどのように受け取られるのかという認知領域の安全保障がかつてなく重要性を有する。しかも、これらの領域における安全保障は平時と有事の別なく常時展開されねばならず、その舞台も情報の発信と受信を担う我々自身の社会生活そのものである。現時点において、我が国はこうした新領域の安全保障に関する

概念をほとんど持っておらず、新たな『国家安全保障戦略』にこれを盛り込むことは急務である。

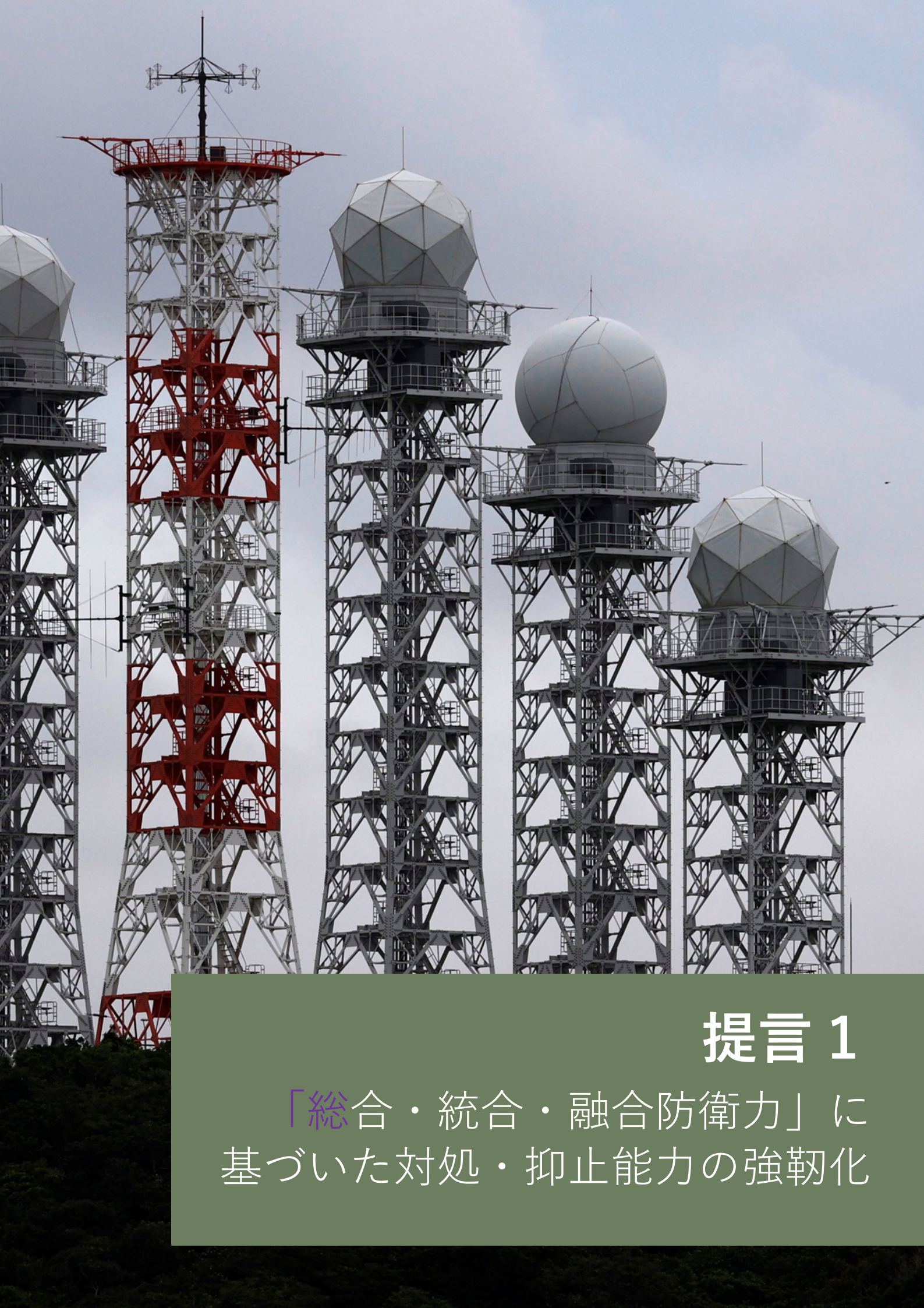
また、認知領域の安全保障政策は、その拠って立つ根本的な価値を明確にする必要がある。安全保障とは「獲得した価値に対する脅威の不在」であると定義されるが、では日本が守るべき「獲得した価値」とは何か。言い換えると、我々が安全保障政策を行う意味とは何であるか。『国家安全保障戦略』はこの点を国民に問い、合意を得られるような根本的原理を提示するものでなければならない。提言 3 では、これを人権、法の支配、自由、民主主義の四つと位置付け、これらの価値観を維持・発展させるために必要な施策を提案した。

実施体制

なお、本提言は、ROLES が外務省の外交・安全保障調査研究事業費補助金「体制間競争の時代における日本の選択肢」の枠内で実施した研究活動を基にしたものであり、同事業の一環として設置された「新領域セキュリティの諸課題に関する分科会」の成果を基礎としている。

参加メンバー（五十音順、敬称略）

- 飯塚恵子（読売新聞編集委員）
- 池田有紀美（国連軍縮部政務官補）
- 楽原響子（日本国際問題研究所研究員）
- 小泉悠（東京大学先端科学技術研究センター講師）
- 合六強（二松学舎大学国際政治経済学部准教授）
- 小宮山功一朗（慶應義塾大学グローバルリサーチインスティテュート客員所員）
- 佐橋亮（東京大学東洋文化研究所准教授）
- 鈴木一人（東京大学公共政策大学院教授）
- 高森雅和（株式会社 Dafna 代表取締役社長）
- 中井治郎（龍谷大学非常勤講師）
- 中井遼（北九州市立大学政策科学科准教授）
- 松本充豊（京都女子大学現代社会学部現代社会学科教授）
- 村野将（ハドソン研究所研究員）
- 山口亮（東京大学先端科学技術研究センター特任助教）



提言１

「総合・統合・融合防衛力」に基づいた対処・抑止能力の強靭化

厳しさを増す安全保障環境

近年、中国・北朝鮮・ロシアは急速に軍事力を強化している。しかも、これらの国々は軍事力を古典的な戦争のために整備しているだけでなく、平時において政治的目的を達成するためにも使用している。領海・領空侵犯やミサイル発射実験、我が国近傍における軍事演習などがそれであり、この種の「グレーゾーン事態」には抑止が働かない可能性が懸念される。

さらに米中間では相互脆弱性が成立したとの認識を中国が既に持ちつつある可能性がある。この場合、戦略核レベルでの安定性を逆用することにより（いわゆる「安定・不安定の逆説」）、台湾を含む日本周辺や西太平洋地域において、よりリスクを厭わない行動をとる危険が高まることが予想される。この点は、核・ミサイル能力を著しく向上させつつある北朝鮮についても同様である。

また、中国とロシアの協力関係は軍事面にも及びつつある。両国は正式の同盟関係を結んでおらず、戦争において協力する関係性ではないことを強調しているが、それぞれの「グレーゾーン事態」型オペレーションを連動させる可能性は排除されない。このような状況を北朝鮮が利用し、状況がさらに複雑化する事態も想定される。

防衛力の総合・統合・融合化

以上のような脅威の増大と多様化に対し、我が国は防衛力を更に進化・強化させる必要がある。近年、日本の防衛大綱においては比較的低烈度の事態を想定した即応性の向上やグレーゾーン事態における領域横断的な対処能力の向上が打ち出されているが、大規模な軍事紛争への対処能力を考えた時には十分とは言えない。このような事態においては国家のリソースを幅広く活用する能力（総合性）、官庁や三自衛隊の垣根を越えた運用（統合性）、領域を横断する作戦能力（融合性）が求められるのであって、本提言ではこれを統合・総合・融合防衛能力と呼ぶことにした。こうした能力を保持することで我が国の防衛力を強靭化し、以て抑止の信憑性を高めるべきであるというのがその目指すところである。

抑止戦略においても、相手に「撃たせない」だけでなく、「身動き取らせない」ための能力が必要である。これには、有事において相手の能力発揮を妨害するための能動的防衛能力が鍵となる。

広大な海域と排他的経済水域、そして多くの島嶼を有する我が国として、海上防衛と防空力を更に強化する必要がある。また、宇宙・サイバー・電磁波領域における脅威も強まっており、近年対応が進められているが、脅威の拡大のペースに比べ遅れているため、より一層に力を入れる必要がある。

費用と効果のバランス

現在、そして将来の脅威と効果的に対峙し、我が国の防衛力の脆弱性を是正するには、多大なコストがかかるため、防衛費の大幅な増額は不可避である。しかし、防衛費を増額させても、依然としてリソース・キャパシティーには限りがあるため、防衛計画を徹底的かつ客観的に精査し、我が国

の防衛において重要な作戦を確実に遂行できる能力とそのための費用をトレードオフで考慮し、複数のオプションを提示できる体制づくりを進める必要がある。

推奨される施策は以下の通りである。

- **抑止が破れた場合の対処能力を持つ**必要があることを『国家安全保障戦略』IV の 1 に明記する。特に中国の核戦力が米国を実際に抑止できる事態を念頭に置いて、一定程度の期間は米国が介入できない状況でも既成事実化を阻止する能力が求められる。具体的には日本の南西方面が中国の海空優勢に入った状況でも戦い続けられる防衛体制（総合・統合・融合防衛力）が求められる。
- これに関連して、**継戦能力を強化する。**2022 年の第二次ウクライナ侵攻ではロシアとウクライナ双方が膨大な戦力を投入して激しい戦闘を展開した結果、常備兵力が短期間で消耗した。我が国が大規模な軍事紛争に対処する能力を持ち、その事実によって抑止力として機能させようとするならば、一定の継戦能力を持たねばならないことをこの事例は証明している。具体的には、米国との海上交通線が途絶した状態でも戦闘を継続しうる装備品・弾薬備蓄の保有、防衛インフラの抗堪化・分散化、予備自衛官の増強等が焦点である。
- ウクライナ侵攻の際にみられたように、ロシア・中国・北朝鮮は、核使用も辞さないとの脅しを行ないつつ、米国が介入意志を固める前に既成事実化を成し遂げようとするという、概ね共通した戦略を持っているか、そうした戦略を実行しうる能力を備えつつある。こうした「核兵器が実際に使われうる状況は現実に存在する」との認識の下、米国による拡大核抑止の信頼性を強化するため、**米国の核作戦計画や核態勢のあり方に関する我が国のコミットメントの深化・拡大**を図る。
- 総合・統合・融合防衛力を強化するために、陸海空自衛隊の垣根を越えた**作戦区域別の地域統合司令部を設置**し、その隷下に統合任務部隊を常設する。また、各地域統合司令部間の連携を図るため、既に検討されている自衛隊統合司令部を設置して陸海空のアセットを単一のフォースユーザー（統合司令官）に委ねる体制が望ましい。
- 有事において敵国の作戦能力に対する**能動的防御（アクティブ・ディフェンス）能力を保有**する。具体的には、指揮通信拠点、物資集積拠点、艦艇・航空機の運用インフラ等を無力化・妨害できる長距離攻撃手段や電磁波作戦能力の保有を目指す。
- 我が国の周辺海域における**海洋拒否能力と海上優勢獲得能力を強化する。**海洋拒否能力においては、数的に優勢な相手と正面から戦うのではなく、交戦のレベルを「ずらす」非対称アプローチを中心とし、特に、相手の動きを封じる機雷戦に重点を置く。海上優勢の獲得においては、領海・排他的経済水域やシーレーン防衛、接近阻止を目的とするアセットを揃えるため、護衛艦群と潜水艦群を更に拡大・強化する。

- 我が国の**海上航空戦力の将来像を検討**する。我が国の海上防衛において海上航空戦力は極めて重要であるが、将来的には現有の対潜哨戒以上の作戦的需要が生じる可能性がある。特に、いずも型ヘリコプター搭載護衛艦や将来のプラットフォームを制海・海上拒否を目的とする航空母艦、或いは島嶼防衛に向けた水陸両用作戦用の強襲揚陸艦にすることなどを検討する必要があろう。
- MIRV（複数個別誘導再突入体）・MaRV（機動再突入体）・極超音速ミサイル等、中国・北朝鮮・ロシアの弾道・巡航ミサイル技術の著しい進化に対応するため、**IAMD（統合航空ミサイル防衛）能力を更に強化する。**
- 有事において戦闘の停止を強要したり、第三国への軍事的支援を思い止まらせるための限定的な核使用やその脅しに屈しないために、広範囲を継続的にカバーできる MD（ミサイル防衛体制）を確立する。そのための手段として**イージス・アショアの配備再開を検討する。**
- 以上の能力を下支えする C4ISR（指揮・通信・統制・コンピュータ・情報・監視・偵察）能力として、**宇宙・サイバー・電磁波領域専門の部隊を増設・増員**する。これには、同盟・準同盟諸国との連携だけでなく、日本国内の警察機関、宇宙航空研究開発機構、専門企業と密室に連携し、更には予備自衛官制度を通じ、専門家を登用する必要がある。
- **新たな軍事的脅威への対処、数的劣勢や人員不足等の解決するため、新興技術を積極的に活用する。**特に、AI（人工知能）や量子技術は無人機や有人システムの省人化において重要であるため、人員不足を解決し、今まで不可能であった作戦を遂行できるようになる。また、これらの技術は、戦闘部隊・システムだけでなく、ロジスティクスや一部の人事・会計・行政業務においても重要となる。
- 我が国独自の新興技術を含む技術開発と同盟国・有志国との技術協力を進めるために**技術開発体制を抜本的に強化する。**これには、防衛予算のうち研究開発費の割合の増加と防衛装備庁における研究開発能力の強化、民生部門で急速に発展する新興技術を柔軟に取り込むための制度、機微技術の流出を防ぐための技術管理体制の強化、防衛装備の調達に関するサプライチェーンの強化を含む。
- 不足している人員、専門知識・技能を補うため、**陸海空の予備自衛官制度を更に拡大・充実させる。**特に、現在の「技術海上・航空幹部」制度を予備にも設ける必要がある。また、常備自衛官との差を縮小するため、訓練日数を増やし、常備部隊と勤務・訓練し、必要に応じて予備自衛官から常備自衛官への切り替えを可能にする制度を設ける。
- 米国の「国防戦略委員会」を参考に、防衛大綱及び中期防衛力整備計画の履行状況とその妥当性を客観的に評価するため、**セキュリティ・クリアランスを付与された外部専門家によって構成される「防衛大綱委員会」を設ける。**同委員会は、防衛大綱に示された戦略目標、運用構想、それらを実行するためのリスク要因、能力上のギャップ、リソースの不足について独自に分析評価を行い、考えうる防衛力整備のオプションについて具体的な提言を行う。同委員会が特定した運用上の課題は、原則として公開する。

提言 2

国際的な安全保障協力体制の拡大と安全保障環境の改善

安全保障協力の拡大に向けて

日本の安全保障と法の支配に基づく国際秩序を確保するには、米国だけでなく、他国との安全保障協力は不可欠である。特に、「自由で開かれたインド太平洋」構想を確実に実現するには、米国、豪州、インドだけでなく、カナダ、英国、台湾、韓国、シンガポール、ベトナム、インドネシア、フィリピン、タイ、ニュージーランド、南太平洋諸国等との協力や連携を深める必要がある。

日米同盟の深化と多角的な安全保障協力

日米同盟は近年著しく進化し、インド太平洋地域の安全保障の支柱となっている。しかし、戦略・作戦・戦術的な同盟ドクトリン、相互運用性、日米同盟とその他の米国の同盟国との連携に基づいた拡大された持続可能な同盟ネットワーク、機密情報共有や機微技術協力のメカニズム等においては依然として多くの課題が残っている。

他方、米国を含む他国がそのネットワークに日本を取り入れていくニーズもまた存在している。この点を踏まえて、米韓同盟、米豪関係、ASEAN 主体の取組みなどにおいて日本が求められるものに柔軟かつ積極的な対応ができる能力、意思、制度を持つことにより双方向的な安全保障協力に高めていくという方向性がここからは導かれよう。

機密情報共有や機微技術協力に関しては、我が国では「ファイブ・アイズ」加盟国で見られるような標準化された政府・企業・施設のセキュリティー・クリアランス・システムが未だ存在しない。情報保全制度を導入・運用する必要がある。現在の我が国の情報保全システムでは、情報・技術協力には限界があり、これは我が国の安全保障と防衛力、そして安全保障パートナーとしての役割において非常に大きな足枷となり、むしろ後退させる可能性もあるため、これを是正することは急務である。

さらに、以上のような相互運用性の向上や合同訓練・演習の頻度の向上を効率的・効果的に行うためには、各国が戦略的に組み合わせを考え、計画的に又はアドホックに、多国間・有志国間で調整していくメカニズムや情報共有システムが非常に重要になる。

目指すべき多様な安全保障協力

また、安全保障協力は、防衛同盟に限らず、サイバーセキュリティ、環境セキュリティ、人間の安全保障、エネルギーの安全保障、経済安全保障、認知領域における安全保障等の非伝統的な安全保障問題にも能力開発、対外援助、情報共有等を通じて協力関係を強化する必要がある。日本は既に上記のことを進めているが、取り組みを次のレベルに進化させることにより、同じ志を持つ国同士の連携をより緊密なものにし、また他の国を呼び込むことが期待される。

推奨される施策は以下の通りである。

- **日米同盟合の同戦略・作戦計画を更新する。**台湾有事、朝鮮半島有事、南シナ海における軍事衝突等のシナリオ、あるいは大規模な軍事紛争に至らない危機事態シナリオを想定した戦略・作戦計画を日米同盟として適時に構想・更新し、その実効性を常時検証する。また、これらの構想・更新・検証のプロセスは日米同盟の枠外にも開放し、多国間での協力の可能性を広げる。これらの計画立案とその実施には、グレーゾーンから通常戦争、核エスカレーションに至る両国（および関係国）の関係組織間のシームレスな連携が不可欠である。その実効性を担保するため、両国は、米インド太平洋軍だけでなく、戦略軍やサイバー軍、宇宙軍などあらゆる関係組織が関与する形での日米（および関係国）の定期的な動員演習・机上演習を実施すべきである。
- **日米同盟に基づいた持続可能な防衛協力ネットワークを構築**する必要がある。特に豪・印・韓・加・英、そして一部の東南アジア諸国との防衛協力を一段と深め、台湾との非公式な直接的な安全保障協力を築くことが重要である。
- **日米同盟、多国間協力ネットワークの相互運用性を向上させ、合同訓練・演習の頻度を増やす**必要がある。
- **東南アジア、南太平洋諸国との連携を強化し、安全保障協力のネットワークを築く**。特に東南アジア・南太平洋地域の発展途上国に関しては、中国の太平洋進出や、勢力の拡大において非常に重要であり、急務である。これには、拡大抑止や防衛協力だけではなく、能力構築支援や経済援助等が必要となる。
- ジブチ共和国における自衛隊拠点と同じように、法の支配と安全を目的とした、**自衛隊の海外拠点を、東南アジア地域の重要なシーレーンに近い、オセアニア・ミクロネシア地域に設置を検討し**、また**海上自衛隊の艦船を東南アジアにローテーション配備**する。
- 機密情報共有や機微技術協力の強化に向け、**「ファイブ・アイズ」加盟国と同様の情報保全システム、または基準に合った政府・企業・施設のセキュリティー・クリアランス・システムを導入し、運用する。**他方、セキュリティー・クリアランス・システムの導入は法の整備だけでなく、関連する慣行の修正など、相応の準備を要する。したがって、**クリアランス制度がなくとも、機密情報共有が行えるよう同時に働きかける。**
- 『国家安全保障戦略』III の 2 においては、北朝鮮と中国に加えて**ロシアを追加する。**2020 年の憲法改正による領土割譲禁止条項の追加、北方領土の実効支配強化と軍事力増強、エネルギーを手段とする圧力の行使等は、我が国に対する直接的な軍事的脅威ではないが、法の支配に基づく国際秩序に対する挑戦である。IV の 3 における**ロシアについての言及は大幅に改める。**東アジアの安全保障環境が厳しさを増す中で安全保障とエネルギーに関して「日露関係を全体として高めていく」ことは中国とロシアの密接な関係に鑑みて困難であり、むしろ米国の抑止リソースをユーラシアの東西に分散させる点で日本の安全保障にとっての懸念要因であると位置付ける。
- 中国が核戦力を格段に増強する一方で、核軍縮・軍備管理の枠組みに参画していないことをふまえ、**米国、中国双方に核軍縮・軍備管理に向けた対話を促す。**

提言 3

認知領域の安全保障強化に向けて

闘争空間としての認知領域

新たな『国家安全保障戦略』では、認知領域が安全保障上の焦点となったことを明示すべきである。近年、偽情報の流布は、武力闘争（戦争）の閾値を越えない新たな国家間闘争の手段として注目されつつある。このような非軍事的闘争には明確な始まりや終わりがなく、明確な戦場や戦闘員も決まっていない。偽情報は日々の生活と密接に結びついたサイバー空間で流布され、一見してそうとはわからない形で人々の認知を歪めるからである。

偽情報は、それ自体は非暴力的なものでありながら、その帰結は非常に深刻なものとなりうる。ロシアによる 2016 年の米国大統領選介入に代表されるように、偽情報は人種的分断やイデオロギー的対立を煽り、社会を不安定化させたり政府に対する信頼を失墜させたりする可能性を孕んでいる。さらに、自由で民主的な社会は、一般的に情報の規制に抑制的であり、結果として認知領域への働きかけに脆弱であるという性質を持つ。台湾やバルト諸国に対する中国やロシアの認知領域作戦は、まさにこうした自由・民主主義社会の脆弱性を衝く形で展開されている。

古典的戦争と認知領域作戦

さらに、認知領域の安全保障は、国家間闘争が暴力闘争に至った状況下でも大きな意義を持つ。米国で 1980 年代に唱えられた「第四世代戦争」理論や 2000 年代半ばの「ハイブリッド戦争」理論は、いずれも暴力闘争下における認知領域のインパクトに注目したものである。これらの理論によれば、現代の戦争の勝敗は戦場の内部でのみ決まるとは限らない。戦闘において劣勢な側は、優勢な敵が「過剰な力の行使を行っている」「民間人を殺戮している」といった認識を敵・味方・国際社会の世論に植え付け、最終的に敵が戦争を継続できない状況を作り出すためである。実際に、ロシアによる 2022 年の第二次ウクライナ侵攻において、ウクライナはこのような戦略を取ることで国際的な支持を獲得した。また、台湾海峡有事において、中国は台湾のみならず日本に対しても大量の偽情報を拡散し、日米同盟弱体化はおろか、社会をかく乱させ政府の政策決定に影響を及ぼそうとすることも予想される。

それゆえに、「ハイブリッド戦争」理論は、戦闘以外のあらゆる闘争手段・軍事組織以外のあらゆる主体を動員し、戦場以外のあらゆる領域で闘争を繰り広げることの重要性を強調する。別の言い方をすれば、非軍事的な闘争手段や非国家主体の動員は「ハイブリッド戦争」の結果に過ぎず、本質は「戦場の外で勝敗を決する」という闘争方法にある。このような闘い方を駆使する敵に対抗し、日本の防衛努力が不正なものであるという認知が有事に広まらないようにするための施策を『国家安全保障戦略』には盛り込む必要があろう。

推奨される施策は次のとおりである。

- IV の 1 において、**認知領域の安全保障に関する取り組み強化**を盛り込む。情報空間における影響力作戦は認知領域に働きかけ、個人や組織、国家の考え方に影響を及ぼさんとする。その舞台となるサイバー空間は 2013 年の国家安全保障戦略においては国際公共財（グローバル・コモンズ）の 1 つとして捉えられていた。しかし、諸外国において保護主義政策が採用され、領域主権を主張する声が強まりつつある。このような現状を踏まえ、「自由で民主的なサイバー空間の維持・発展」の実現のために努力を強化すべきである。
- **政府の情報発信（戦略的コミュニケーション）および偽情報対策シミュレーションを開始する。**米国を中心に国内でも現実の脅威として認識される台湾海峡有事では、日本国内でもさまざまな偽情報が拡散し、国内が混乱に陥る可能性が高い。こうした危機の際に偽情報の被害を最小限に食い止めるために、いかなるデマや偽情報が拡散し、どのような混乱や被害が広まるかを予想し、それに対して政府としていかなる措置を講じるべきかについて、シンクタンクやプラットフォーマー、マスメディア等と検討を開始しすることが望ましい。
- **偽情報対策と情報発信の司令塔を定める。**「ハイブリッド戦争」が多様な主体と領域に跨って展開されるものである以上、これに対抗するためには幅広い領域を横断する努力が求められる。したがって偽情報対策や情報発信は個別の政府機関で対応しきれるものではなく、関係府省庁間の横断的な取り組みが重要であり、国家安全保障局のような安全保障政策の中心的機関が全体を指揮・統括する役割を担うことが望ましい。
- **平時から有事における認知領域作戦の最新動向についての知見を常時入手できる態勢を作る。**戦略コミュニケーション卓越研究拠点（STRATCOM COE）、ハイブリッド戦卓越研究拠点（ハイブリッド戦 COE）といった国際的な研究拠点に対して日本政府としての提携を呼びかけ、共同研究の実施や日本人研究員の常駐といった施策を講じるべきである。
- **マスメディアやプラットフォーマーとの協力態勢のあり方について検討を開始する。**平時から有事にかけての偽情報対策を国家機関のみで実施するのが不可能であることもまた事実であり、諸外国がどのような体制でマスメディアやプラットフォーマーとの関係を築いているのか、その際の問題点は何なのか等について研究を開始すべきである。
- **ファクトチェック機能を強化する。**近年国際社会ではファクトチェック（真偽検証）は偽情報対策の有効な一手段として注目されており、欧米をはじめ東南アジアや中南米、アフリカなどでは民間団体主導のファクトチェックが増加傾向にあり、なかには政府機関と連携している国や地域もある。他方、日本ではファクトチェックという言葉が浸透しておらず、ファクトチェック機関数も他の先進国やアジア諸国と比較して低い。政府が必ずしも主導する必要はないが、日本社会におけるファクトチェック機能を強化すべく、メディアや民間企業等と検討を開始すべきである。また、情報発信元の開示を容易にすることで、**情報の真偽性を国民が確認しやすくするための法整備を進める。**

- **偽情報対策において「表現の自由」を守る。**偽情報への対抗手段は容易に情報統制に堕す危険性があり、実際に多くの権威主義国家等が「新型コロナウイルス感染症対策」や「フェイクニュース対策」の名の下に法整備などの手段によって情報統制および言論統制を強めている。偽情報対策でリードする欧米諸国の中でも表現の自由が原因となり対策に手詰まり感が出てきている国がある一方、台湾のように政府が推進する対策に対し市民から高い支持を得ている場合もある。諸外国が偽情報対策においていかに表現の自由を保障しているのか、問題点は何か等について研究し、民主主義国家としていかなる対策が適当かについて検討を開始すべきである。
- **国民のメディア・リテラシー向上のための教育を促進する。**偽情報研究では一般に「国民一人ひとりがメディア・リテラシーを持っていることが偽情報に対する最大の抑止力」と認識される。教育機関をはじめとする民間部門との連携を図りつつ、初等教育や中等教育の段階で目前の情報を批判的に考えられる訓練を受けられる取り組みについて検討することが望ましい。
- **デジタルインフラの保護方針を定める。**ロシアの第二次ウクライナ侵攻に際しては、作戦開始とほぼ同時に、衛星通信システムへのサイバー攻撃、ウクライナ所有データセンターへの砲撃がおこなわれた。これらのデジタルインフラ(通信回線、データセンター、国際ケーブル、衛星通信システム)はサイバー空間の土台であるが、その保護を民間事業者のみに委ねることは限界があるため、保護方針を官民で協力して定めるべきである。
- 総合・統合・融合防衛力の整備や認知領域の安全保障政策を進めるにあたっては、**我が国が拠って立つ人権、法の支配、自由、民主主義という価値観の維持・発展に寄与するものである必要がある。**以上の目的を達成するために、安全保障政策についての国民的な議論を喚起し、幅広い合意の下で進める必要性を明記する。このような合意なくしては危機事態において政府は自信を持って必要な施策を取れない可能性があるためである。
- 従来の「安定した国際環境創出のための外交の強化」の内容を広げ、インド太平洋地域での民主化支援、開発援助、平和構築等を通じて**域内の自由と民主主義を発展させる**役割を一層強化するとの方針を打ち出す。

国家安全保障戦略改訂に向けた提言

我が国の安全保障を強化するための三つの方策

東京大学創発戦略研究オープンラボ（ROLES）有志

2022 年 10 月