日本の宇宙・サイバー政策

廣瀬行成[1]
前防衛省防衛研究所長

平成 30 年 12 月に策定された防衛計画の大綱では、従来の陸・海・空の自衛隊の活動領域に加えて、「宇宙・サイバー・電磁波」の領域についての重要性が認識され、「領域横断作戦」に初めて言及されることとなった。

社会全体が宇宙空間やサイバー空間への依存を高めている現状にあって、自衛隊の活動にも大きな影響を与える可能性がある。

本稿では、日本の宇宙及びサイバー戦略について、その歴史と取り組みについて概観する。

１．宇宙・サイバー戦略全般

（１）国家安全保障戦略と防衛計画の大綱（25 大綱）

2013 年 12 月に、国家安全保障戦略[2]及び防衛計画の大綱が策定された。国家安全保障戦略は、日本の安全保障に関する基本方針として初めて我が国が作成した文書であり、我が国全体として、どのように国家安全保障を確保すべきかについて記述し、外交政策及び防衛政策を中心とした、国家安全保障に関する基本方針を初めて示したことに大きな意義がある。同文書においては、国際公共財に関するリスクとして、海洋、宇宙空間、サイバー空間に対する自由なアクセス及びその活用を妨げるリスクがある旨記述している。その上で、我が国の能力・役割の強化拡大する分野として、サイバーセキュリティ強化と宇宙空間の安定的利用の確保及び安全保障分野での活用の推進を含む 10 項目が挙げられている。

国家安全保障戦略と同時に策定された防衛計画の大綱（「平成 26 年度以降に係る防衛計画の大綱[3]：25 大綱）では、グレーゾーンの事態の増加傾向に言及するとともに技術革新の急激な進展を背景として、宇宙空間・サイバー空間といった領域の安定的利用の確保が、国際社会の安全保障上の重要課題となっている、としている。

（２）防衛計画の大綱の見直しと中期防衛力整備計画

25 大綱策定以降、我が国を取り巻く安全保障環境は、想定よりも「格段に速いスピードで厳しさと不確実性を増して」きたことから見直しが行われた。2018 年 12 月に策定された新たな防衛計画の大綱（「平成 31 年度以降に係る防衛計画の大綱[4]：30 大綱）では、陸・海・空という従来の領域のみならず、宇宙・サイバー・電磁波といった新たな領域を含む「領

---

[1] 防衛省防衛研究所長（2018 年 8 月より 2020 年 1 月）。本稿は、執筆者が個人の立場から分析・記述したものであり、日本政府あるいは防衛省の見解を示すものではない。
[2] https://www.mod.go.jp/j/approach/agenda/guideline/pdf/security_strategy.pdf
[3] https://www.mod.go.jp/j/approach/agenda/guideline/2014/pdf/20131217.pdf
[4] https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/20181218.pdf

域横断（クロス・ドメイン）作戦」を念頭に置き、「多次元統合防衛力」の構築を目指すこととされた。

そもそも、防衛計画の大綱は、概ね 10 年程度の期間を念頭に置いているものであり、その半分 5 年で見直しを行ったということは、ここ数年の安全保障環境の変化の早さを物語っている。その中で、25 大綱では個別に記述されていた宇宙及びサイバー分野については、「宇宙・サイバー・電磁波といった新たな領域」として、重点を置いていることに注目される。

なお、25 大綱と同時期に策定された国家安全保障戦略も、同様に概ね 10 年程度の期間を念頭に置いているものとされているが、今回、見直しは行われなかった。この点、見直しても良かったのではないかとの意見も見られるが、安倍総理は、「国家安全保障戦略は・・・我が国の安全保障に関する大枠の方針を示したもの・・・昨年（筆者注：2018 年）、内容のレビューを行ったところでありますが、今回は国家安全保障戦略の下で防衛力の強化に注力することとした」と答弁している（平成 31 年 3 月 6 日参議委予算委員会）。

30 大綱と同時に閣議決定された「中期防衛力整備計画（平成 31 年度～平成 35 年度）」（31 中期[5]）においては、宇宙・サイバー・電磁波の領域での機能強化を目指している。具体的には、航空自衛隊における宇宙領域専門部隊 1 個隊の新編及び自衛隊共同の部隊としてのサイバー防護部隊 1 個隊の新編並びにこれら新たな領域への人員を充当するなど組織や業務を最適化することしている。また、主要な事業として、宇宙分野においては、宇宙状況監視（SSA）システム整備、各種衛星の利用による冗長性の確保、我が国の衛星の脆弱性への対応などが、サイバー領域においては情報通信システム／ネットワークの抗たん性の向上、人材育成などの事業がそれぞれ盛り込まれている。

２．日本の宇宙利用

（１）政府全体としての取り組み

（ア）日本の宇宙開発の経緯

日本の宇宙開発は、1955 年のペンシルロケット、1975 年の我が国初の人工衛星「おおすみ」打ち上げまで遡ることができるが、それ以降文部省及び科学技術庁（後に文部科学省）が宇宙行政を行い、宇宙開発利用にかかる施策を総合的かつ計画的に推進することを目的とする宇宙基本法が施行されたのは 2008 年であった。同法に基づき宇宙開発戦略本部が設置された。宇宙基本法においては、宇宙開発利用を日本国憲法の平和主義の理念に則り行われるものとする、とした上で、我が国の安全保障に資するよう行われなければならない旨規定している。2012 年には、内閣府に宇宙戦略室が設置され、政府全体の宇宙開発利用に関する政策の企画・立案・調整を行うこととされた。同年には、JAXA 法が改正され、JAXA による安全保障目的の研究開発が可能になった。なお、1998 年には、情報収集衛星の導入が決定されている。

---

[5] https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/chuki_seibi31-35.pdf

（イ）宇宙基本計画

2016 年には、宇宙基本計画[6]が閣議決定された。この宇宙基本計画は、今後 20 年を見据えた 10 年間の長期的・具体的整備計画として策定されたものである。以下、宇宙基本計画を概観する。まず、宇宙政策を巡る環境認識として次の 6 点を記述している。①宇宙空間におけるパワーバランスの変化（かつての米ソ二極構造から多極構造へ）、②宇宙空間の安全保障上の重要性が増大、③宇宙空間の安定利用を妨げるリスクが深刻化（デブリ、対衛星兵器の脅威の増大）、④地球規模問題解決に宇宙が果たす役割が増大、⑤我が国宇宙産業基盤がゆるぎつつある（事業撤退が相次ぎ、新規参入も停滞）、⑥科学技術を安全保障・産業振興に活かす有機的サイクルが不在。その上で、①宇宙安全保障の確保、②民生分野における宇宙利用推進、③産業・科学技術基盤の維持・強化の 3 点を宇宙政策の目標としている。具体的な取り組みとして挙げられている 9 項目は、衛星測位、リモートセンシングなどであり、防衛省が関係するものとしては①リモートセンシング、②衛星通信・衛星放送、③宇宙輸送システム、④宇宙状況把握、⑤海洋状況把握、⑥早期警戒機能等、⑦宇宙システム全体の抗たん性強化の 7 項目に及んでいる。

（２）防衛省・自衛隊の取り組み

「航空宇宙自衛隊への進化も、もはや夢物語ではありません。」2019 年 9 月、安倍内閣総理大臣は、自衛隊高級幹部会同の訓示 [7]において、こう述べた。2018 年策定の中期防衛力整備計画（31 中期）では、宇宙領域専門部隊の新編や SSA システムの整備などが盛り込まれており、2020 年度には、我が国の宇宙利用の優位を確保するため、航空自衛隊に宇宙作戦隊（仮称）を新編することとしている。

（ア）自衛隊による衛星利用

防衛省・自衛隊による宇宙利用は、情報収集、通信、測位と多くの分野に亘っている。最初の利用は 1977 年に海上自衛隊が商用衛星通信の借り上げを行ったのに始まり、現在、防衛省として所有する X バンド防衛通信衛星 2 機を運用しており、3 機体制を目指している。1985 年からは商用画像の取得を開始し、1993 年からは海上自衛隊が米 GPS の利用を開始し、1996 年からは米より早期警戒情報の受領を開始している。

（イ）「平和の目的」との関係

防衛省・自衛隊による宇宙利用については、1980 年代には国会において自衛隊の衛星通信利用と宇宙開発事業団法や国会決議の「平和の目的」との関係で議論になった

1985 年 3 月の政府の説明は、いわゆる「一般化」理論を援用している。海上自衛隊が米国派遣訓練の際にフリートサット衛星から受信するための経費の計上に関して、加藤防衛庁長官は、「政府は、宇宙の開発利用に関する国会決議の趣旨について、自衛隊が衛星を直

---

[6] https://www8.cao.go.jp/space/plan/plan3/plan3.pdf

[7] 第 53 回自衛隊高級幹部会同　安倍内閣総理大臣訓示
https://www.kantei.go.jp/jp/98_abe/statement/2019/0917kunji.html

接殺傷力、破壊力として利用することは認められないが、その利用が一般化しているような衛星の利用は認められるものであると理解しており、今回のフリートサット衛星の利用は、この観点から国会決議の趣旨に反するものではないと考えております。」としている。[8]

なお、1984 年の国会審議では、硫黄島に所在する自衛隊部隊のために電電公社の衛星通信回線を利用することについて、「平和の目的に限る」との関係で議論になった。栗原防衛庁長官は、「硫黄島の自衛隊が、日本各地で電電公社からの役務を利用している。それと同じ形態で利用さしてもらいたい、しかも、公衆電気通信法によりますと、いわゆる公社というのは利用者に対してあまねく、かつ公平に役務をしなきゃならぬ、また、その属性によって差別取り扱いをしてはいけない、こう言うような規定もございますので、私どもといたしましては、前段申しあげたとおり、日本の国内において役務を利用さしておると同様のことをさしていただきたい.こういう風に考えておるわけでございます。」と答弁している[9]。

同月の予算委員会で中曽根総理大臣は、「もし原子力推進による船、商船が一般的に使われるようになった場合には防衛庁の使う潜水艦も原子力推進にしてもこれは平和の目的に反しない、つまり汎用性を持ってきた場合にはそれに反しないんだと、そういう原子力基本法の説明をして、それで通っておるのです。今のしかし人工衛星の問題はそういう説明をそのときしていないんです。提案理由の説明やら政府の答弁が。でありますから、その点を今の原子力基本法と同じように言う訳はいかないんです。」との答弁をしており[10]、いわゆる「一般化理論」を援用はしていない。これは、自衛隊が、電電公社の公衆回線の一利用者の立場に立つものであり、そもそも宇宙の平和利用との関係で問題になるものではないとの認識を示している。前述のフリートサットの場合は、軍事用の通信衛星であり、自衛隊が利用する際には一般の利用者と同じ立場とは言えないことから、「一般化理論」を援用したものと考えられる。

その後、2008 年に施行された宇宙基本法は、「宇宙開発利用は・・・我が国の安全保障に資するよう行わなければならない」と規定するとともに、2012 年には宇宙航空研究開発機構（JAXA）法が改定され、JAXA による安全保障目的の研究開発が可能となった[11]。

（ウ）防衛省・自衛隊による取組

現行中期防では、従来の取り組みの充実に加えて、宇宙空間の安定的利用の確保のための SSA 体制の構築や、電磁波領域と連携して、相手方の指揮統制・情報通信を妨げる能力を含め、平時から有事までのあらゆる段階において、宇宙利用の優位を確保するための能力強化に取り組むこととしている。加えて、関係機関や関係国との連携強化や部隊の新編、人材育成を進めることとしている。

---

[8] 昭和 60（1985）年 3 月 14 日参議院　内閣委員会
[9] 昭和 59（1984）年 3 月 3 日参議院　予算委員会
[10] 昭和 59（1984）年 3 月 28 日参議院　予算委員会
[11] 国立研究開発法人宇宙航空研究開発機構法（平成 14 年法律第 161 号）第四条　2012 年に、「平和の目的に限り、・・・宇宙の開発及び利用の促進を図ることを目的とする」との規定を改正し、「宇宙基本法第二条の宇宙の平和利用に関する基本理念にのっとり、・・・宇宙の開発及び利用の促進を図ることを目的とする」とされた。

宇宙状況監視（SSA）体制の構築は宇宙ゴミ（デブリ）の増大と対衛星兵器関連技術の進展に伴い、デブリや不審な衛星などから人工衛星を防護するため、防衛省・自衛隊においても、SSA 体制を 2022 年までに構築することを目指している。具体的には、2020 年度予算において SSA 関連機材を取得することとし、JAXA 及び米軍のシステムとも連接することとしている。また、前述のとおり、航空自衛隊において、宇宙作戦隊を新設することとしている。今後 SSA 衛星等の導入の検討をしている。

また、防衛省・自衛隊は、JAXA と研究協力・人材交流に加えて、米国との間で、日米防衛当局間の協力を促進している。従来から、米国の「宇宙基礎課程」等に要員を派遣し、知見を習得している。また、2018 年には、内閣府、外務省、JAXA 等とともに、米空軍宇宙コマンドが主催する多国間机上演習である「シュリーバー演習」に初めて参加した。この演習は、米の他、イギリス、オーストラリア、カナダ等の参加を得て、宇宙における各種状況への対応について様々なレベルにわたる幅広い議論を行うものであり、我が国の宇宙分野での国際連携が強化されることとなった。

３．日本のサイバーセキュリティへの取り組み

（１）政府全体としての取り組み

（ア）日本のサイバーセキュリティの歴史

政府は、1999 年に法制度の検討、ハッカー対策などの基盤整備、サイバーテロ対策について必要な施策を実施する為に「情報セキュリティ関係省庁局長等会議」を設置した。さらに、2000 年 12 月に「重要インフラのサイバーテロ対策に係る特別行動計画」[12]を策定し、内閣官房を中心に計画の実施に努めるとともに、民間事業者にも必要な協力を求めてきた。その後、2014 年に成立したサイバーセキュリティ基本法に基づき、2015 年に内閣にサイバーセキュリティ戦略本部が設置され、内閣官房に内閣サイバーセキュリティセンター（NISC）が設置され、サイバーセキュリティの確保に関する政府の統一保持上必要な企画・立案・総合調整を行うこととされた。

（イ）サイバーセキュリティ戦略

現在、政府は第５期科学技術基本計画 [13]において提唱された「society 5.0」の実現に向けて各種施策を推進している。実現するとサイバー空間（仮想空間）とフィジカル空間（現実空間）が高度に融合されることとなり、サイバー空間への依存がより高まることとなる。今後、サイバーセキュリティによる安全確保がますます重要性を増してくることとなる。

2018 年に観測されたサイバー攻撃のパケット数は、約 2,121 億と、2017 年の約 1,504 億と比較して大幅に増加しており [14]、スマートフォンの普及や IoT 機器等の普及・浸透により脅威が広がる恐れがある。また、政府機関における攻撃等の検知件数は、2018 年度は計

---

[12] https://www.nisc.go.jp/active/sisaku/2000_1215/1215actionplan.html
[13] https://www8.cao.go.jp/cstp/kihonkeikaku/index5.html
[14] NICTER 観測レポート 2018　https://www8.cao.go.jp/cstp/kihonkeikaku/index5.html

182 件と前年の 226 件より減少したものの引き続き検知している。なお、2018 年の平昌オリンピックの際には、大会準備期間に約 6 億件、大会期間中に約 550 万件のサイバー攻撃があったとされており、2020 年の東京オリンピックなどのイベントでも最高度の注目を集める為の攻撃のターゲットとなる恐れも指摘されている[15]。

2018 年に策定されたサイバーセキュリティ戦略[16]では、サイバー空間の利用が社会に定着していることから、攻撃等により、多大の経済的・社会的損失が生ずる可能性が指数関数的に拡大していると指摘し、このような認識の下、３つの観点（①サービス提供者の任務保証、②リスクマネージメント、③参加・連携・協議）から取組を推進するとしている。このための施策として、①経済社会の活力の向上及び持続的発展、②国民が安全で安心して暮らせる社会の実現、③国際社会の平和・安定及び我が国の安全保障への寄与、の 3 点を今後 3 年間に執るべき目標や実施方針として示している。そして、この 3 つの政策目標を達成するために、横断的施策として、①人材育成・確保、②研究開発の推進、③全員参加による協働、が挙げられている。

安全保障面で、防衛省・自衛隊が関連する具体的な施策としては、①自由、公正かつ安全なサイバー空間の理念の発信、②サイバー空間における法の支配の推進、③国家の強靱性の確保、④サイバー攻撃に対する抑止力の向上、⑤サイバー空間の状況把握の強化、⑥国際協力・連携における知見の共有・政策調整、⑦実務者層、技術者層の育成、が挙げられている。

（２）防衛省・自衛隊としての取り組み

（ア）防衛省・自衛隊によるサイバーセキュリティへの取組の歴史

防衛省・自衛隊においては、上述の「情報セキュリティ関係省庁局長等会議」に参加するとともに、2000 年度予算においては、「コンピューターセキュリティ」のための次の施策を推進することとした。①技術基盤の整備として、高度セキュリティ・システムの試験的構築及び運用評価環境の整備、②人的基盤整備として、米国の大学・研究機関などへの要員派遣、③先端技術動向調査として、米軍などへの要員派遣。

また、2008 年 3 月には自衛隊指揮通信システム通信隊を新編し、サイバー攻撃への対処要領を策定するなど対処態勢を整備している。2014 年には、隷下にサイバー防衛隊を新設し、体制を充実・強化した。2020 年予算においては、サイバー防衛隊の増員を行い、約 290 名の部隊として体制を拡充することとしており[17]、2023 年度までに、自衛隊指揮通信システム通信隊の体制を見直し、共同の部隊としてサイバー防衛部隊を新編することとしている。

（イ）今後の取組

---

[15] サイバーセキュリティ 2019　サイバーセキュリティ戦略本部
https://www.nisc.go.jp/active/kihon/pdf/cs2019.pdf

[16] https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf

[17] 我が国の防衛と予算（案）令和 2 年度予算の概要
https://www.mod.go.jp/j/yosan/yosan_gaiyo/2020/yosan_191220.pdf

これまでの取り組みとしては、侵入防止システムの導入、サイバー防護分析装置の整備、24 時間態勢での通信ネットワーク監視やサイバー攻撃対処等を行ってきた。31 中期においては、①サイバーセキュリティ確保のための態勢整備、②最新のリスク、対応策及び技術動向の把握、③人材の育成・確保を行うとともに、④政府全体への取組へも寄与することとしている。

以下、具体的に防衛省・自衛隊の取組の主なものについて記述する。①態勢整備については、上述のサイバー防衛隊への増員・態勢整備に加え、サイバー攻撃の徴候や手法に関する情報収集装置、サイバー防護分析装置の機能強化、対抗形式の演習を行うためのサイバー演習環境の整備などを継続することとしている。②最新のリスク、対応策及び技術動向の把握については、民間企業との協力及び米国その他の国との協力が挙げられる。民間企業との協力については、2013 年より防衛産業と「サイバーディフェンス連携協議会（CDC）」を設置し、共同訓練などを通じて防衛省・自衛隊と防衛産業双方のサイバー攻撃対処能力向上に取り組んでいる。また、米国との間では、防衛当局間の枠組みとしての「日米サイバー防衛政策ワーキンググループ」や「日米 IT フォーラム」における協議や米陸軍のサイバー教育機関への連絡要員派遣を行うとともに、日米政府全体の枠組みである「日米サイバー対話」にも参加している。その他の国等との協力としては、英国、NATO との防衛当局間によるサイバー協議、シンガポール、ベトナムなどとの IT フォーラムの開催に加え、エストニアに所在する NATO サイバー防衛協力センター（CCDCOE）に防衛省から職員を研究員として派遣している。③人材の育成／確保については、防衛省・自衛隊における教育の実施、国内外の大学などへの留学、民間企業における実務経験を積んだ者の採用などによる外部人材の活用が挙げられる。

４．今後の課題等

これまで、宇宙・サイバー政策について概観してきたが、本項では、今後の課題等について考察する。

（１）領域横断作戦（電磁波領域との連携）

現在の戦闘様相は、陸海空のみならず、宇宙・サイバー・電磁波といった新たな領域を組み合わせたものなってきている。このため、今後の防衛力は個別の領域における能力の質及び量を強化しつつ、全ての領域における能力を有機的に融合し、領域横断作戦を念頭に置く必要がある。

情報収集、通信、測位などの人工衛星の活用は領域横断作戦の実現に不可欠である一方、これらに対する脅威は増大している。2016 年 3 月に、朝鮮半島上空を飛ぶ 14 カ国計 1007 機の民間航空機で GPS の受信障害が起きた。国際民間航空機構（ICAO）は北朝鮮による妨害電波が原因であると結論つけた[18]。また、車用の GPS 信号ジャマーも安価で入手可能である。このような状況においては、平時から有事までのあらゆる段階において宇宙利用の

[18] 産経ニュース　https://www.sankei.com/world/news/160623/wor1606230042-n1.html

優位を確保するためには、宇宙領域のみならず、電磁波領域と連携する必要がある。なお、2020 年度予算（案）では、電磁波領域と連携した相手方の指揮統制・情報通信を妨げる能力に関する調査研究の事業が計上されている。

（２）人材確保・育成

大綱及び中期では、「防衛力の強化に当たっては、特に優先すべき事項について、可能な限り早期に強化することとし、既存の予算・人員の配分に固執することなく、資源を柔軟かつ重点的に配分する」（30 大綱）、「計画期間中においては、重要性が低下した既存の組織及び業務を見直し、宇宙・サイバー・電磁波といった新たな領域を中心に人員を充当するなどの組織や業務を最適化する取組を推進する」（31 中期）としている。

たとえば、サイバー領域では、2020 年度予算（案）でサイバー防衛隊の定員を約 290 名に増員することとしている。また、河野防衛大臣は、2023 年度末に各自衛隊の部隊も合せ、千数百人まで増やす、としている[19]。しかしながら、諸外国の例を見ると、中国は 17 万 5 千人（うち攻撃部隊 3 万人）のサイバー戦部隊が戦略支援部隊のもとに編成されたとされており、ロシアのサイバー軍の要員は約 1 千人、北朝鮮のサイバー部隊は約 6 千 8 百人といわれており、これらの国は実際にサイバー攻撃を行っているとされている。また、米国も 6 千 2 百人からなるサイバー任務部隊を保有している[20]。このように、各国と比較すると、日本の要員は圧倒的に少なく、要員の大幅な増強が喫緊の課題と言える。

また、単に定員を増強するだけでなく、実際に質の高い要員を確保することや、教育訓練も具体的な取組として挙げられているが、どれだけ実効性のある措置がとれるかが問題となろう。

（３）所要予算の確保

2020 年度予算（案）では、宇宙関連経費が約 506 億円、サイバー関連経費が約 256 億円計上されている。宇宙関連予算は、過去 10 年 200 億円台から 800 億円台で推移しているが、内訳を見ると、従前は、通信衛星回線の借り上げや画像データの購入（取得）経費が大半を占めており、調査研究や米国への要員派遣・教育経費等の政策を実現するための経費は、数億円程度の計上となっていた。2020 年度予算（案）では、衛星通信の利用と画像データの取得（合計約 238 億円）に加えて、宇宙空間の安定的利用を確保するための能力の取得のために約 220 億円、宇宙を利用した情報収集能力等の強化に約 40 億円と大幅に増額されているのが特筆される[21]。今後も、防衛関係費を巡る状況は引き続き厳しいと予想されるが、宇宙・サイバー・電磁波といった新領域にいかに予算を確保できるかが焦点となろう。

---

[19] 2020 年 1 月 14 日日経新聞

[20] 令和元年版防衛白書　第Ⅰ部第 3 章第 3 節 2 サイバー空間における脅威の動向等
https://www.mod.go.jp/j/publication/wp/wp2019/html/n13302000.html

[21] 我が国の防衛と予算（案）令和 2 年度予算の概要

【参考】　平成 27 年度以降の宇宙関連予算（単位：億円、%）[22]

年度	宇宙関連予算	回線・データ取得	比率
2020（R2）	506	238	47
2019（H31）	896	616	69
2018（H30）	502	473	94
2017（H29）	427	384	90
2016（H28）	264	261	99
2015（H27）	340	290	85

（4）総合的な戦略策定の必要性

宇宙・サイバーの領域では、単に、攻撃からの防護措置のみならず、技術優位の確保が重要となる。そのためには、関連する先端技術の自前での育成と技術流出の防止が必要な課題となる。宇宙・サイバーの領域では、政府機関のみならず、民間事業者や大学等の研究機関も重要な役割を果たすこととなるが、国家安全保障戦略や宇宙基本計画、サイバーセキュリティ戦略では、技術優位の確保に関する包括的な記述はされていない。今後、民間事業者や大学等の研究機関も含めた総合的な戦略の策定が必要となるものと考えられる。

[22] 各年版「我が国の防衛と予算（案）」より作成