新領域における活動

（宇宙・サイバー・電磁波）

全国防衛協会連合会

【https://www.mod.go.jp/j/policy/agenda/guideline/pamph/guidline_pamph_normal.pdfから引用】

は　じ　め　に

日常生活においてスマホを使っての会話や行き先・天気の確認、パソコンではインターネット経由での調べごと、ドライブはカーナビ頼りなのは、「自然」なこと、と多くの方が考えているでしょう。

このことは宇宙空間にある人工衛星の活動に障害が無く、地球上における通信の自由が守られて初めて成り立っています。

現代社会の営みは人工衛星や通信に頼らざるを得ない状態となっています。

もし、この人工衛星の活動や　通信の自由を阻害された場合、享受している便利さは著しく損なわれ、不便極まりない社会生活になるでしょう。

なお、このことは、何も社会生活に限ったことではありません。

【総務省「平成30年版情報通信白書
図１デジタル･トランスフォーメーション」から引用】

軍事の世界においても同じことが言えます。我が国を含め世界の軍隊の指揮統制はこのコンピューターと衛星通信で成り立っており、これらを失うことは即ち負けを意味するほどの重要性を持っています。

今回は、新領域といわれる宇宙、サイバー、電磁波領域の戦いとはどういうもので、新領域を護る、自由度を保つことは国民の生活に直結していることを理解していただくとともに、現在、防衛省・自衛隊としてどの様に取り組んでいるのか、そして今後の課題は何か、等を会員の皆様に知って頂くキッカケになればと願っています。

一方で、新領域はこれまでの「防衛力」とは異なり一般的に目で見えるものでは無い、という特色があります。そのため、どのような影響や効果があるのかが掴みづらい一面があります。今回は「新領域」について実例や具体的な防衛力整備の方向性や実現に際しての課題などを整理し解説して参ります。

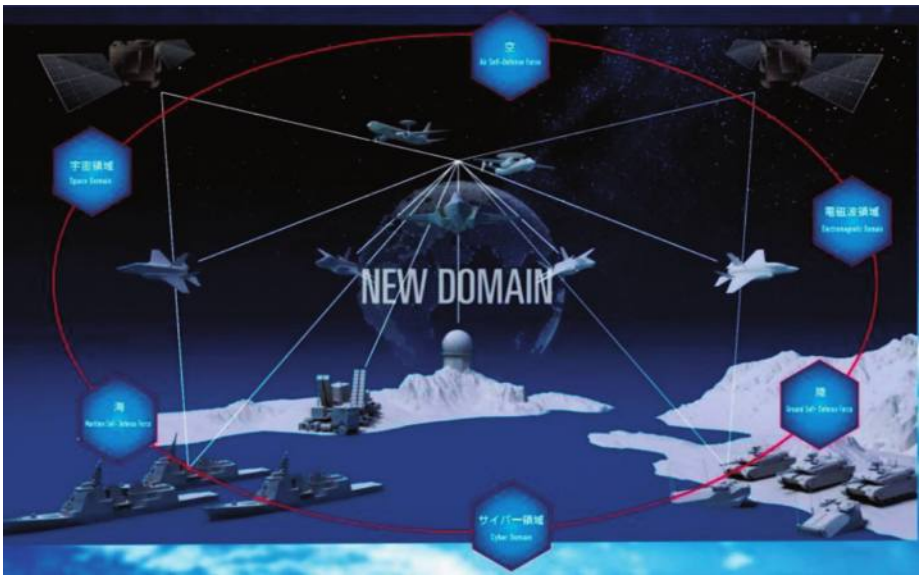
目　　次

第１章：新領域での戦い

１　新たな領域とは？

ロケットや人工衛星によって直接探査が可能になった空間を宇宙領域、主にコンピューターやネットワークによって構築された仮想的な空間をサイバー領域、通話や映像を電波により通信する空間を電磁波領域とし、この３つの領域を新領域（以下、新領域と呼ぶ。）と呼んでいます。（最近は無人機なども新領域と呼ぶこともありますが、今回は上記３領域に限り説明を進めます。）

現在、あらゆるものがインターネットに繋がるIoT（Internet of Things）の急速な進化によって、サイバー空間（仮想空間）とフィジカル空間（現実空間）が高度に融合された社会が実現しつつあります。宇宙・サイバー・電磁波といった新たな領域の利用は現代社会の通信や情報インフラを支えるとともに、自衛隊の指揮統制システムや防衛活動における重要な基盤機能となっています。



【防衛省　航空自衛隊HP（https://www.mod.go.jp › second › pdf › hossoku から引用】

安全保障の分野においては、近年これまでの陸海空の従来領域に加え、宇宙、サイバー、電磁波の領域での戦いを「新たな領域」（もしくは「新領域」、「宇・サ・電」ともいう。）という言葉で語るようになってきました。防衛白書では、平成の後半になって宇宙、サイバー、電磁波の領域での戦いを個別に記述してきましたが、「平成31年度以降に係る防衛計画の大綱」（以後「30大綱」）において、それらを総称して新しい領域と定義付けたこともあり、30大綱を受けた最初の令和元年版防衛白書においては、その刊行に寄せての中で、岩屋毅防衛大臣（当時）は「新防衛大綱と新中期防の下、我々は、わが国自身の防衛体制を抜本的に強化

します。その際には、陸・海・空という従来の領域に、宇宙・サイバー・電磁波といった新たな領域を融合させた「多次元統合防衛力」の構築を図る考えです。」と述べ、宇宙・サイバー・電磁波といった新たな領域を融合させた「多次元統合防衛力」の構築を目指す考えを示しました。

さらに、第Ⅰ部「我が国を取り巻く安全保障環境」の中に新たに「宇宙・サイバー・電磁波といった新たな領域をめぐる動向・国際社会の課題」という章（第３章）を設け、宇宙・サイバー・電磁波領域をめぐる各国の動向を説明しています。

また、第Ⅲ部「防衛目標を実現するための３つのアプローチ」第１章「我が国自身の防衛体制」の中で、「宇宙・サイバー・電磁波領域での対応」の項を設け、30大綱における防衛力の果たすべき役割のうち、「③あらゆる段階における宇宙・サイバー・電磁波の領域での対応」の考え方を詳しく説明しています。

令和２年版防衛白書では巻頭特集２として、新たな領域において宇宙・サイバー・電磁波のそれぞれの領域について説明するとともに、令和３年版では別冊の特集３で「宇宙・サイバー・電磁波領域における挑戦」と題して、その戦いについて詳しく記述しています。防衛白書における新領域の記述は、最新の令和６年版までその作成方針は継続されており、その重要性は益々高まっていると言えます。

２　ウクライナ戦争における現状

2022年２月に始まったロシア・ウクライナ戦争においては、開戦当初にウクライナが利用していた通信衛星がサイバー攻撃を受けて機能が停止しました。これは、初めての宇宙領域に対するサイバー攻撃であるとして注目を集めました。しかし、ウクライナ政府の要請に対し、テスラ社のCEOイーロン・マスク氏が直ちに支援を表明し、ウクライナにスターリンク[1]が提供されたため、結果として、ロシアによる通信衛星への攻撃の影響は小さくなりました。

さらに、開戦以前には多くの専門家がロシアからの送電網に対するサイバー攻撃で大規模な停電が起こる可能性も指摘していましたが、これに関してもウクライナは的確な防護により被害を局限できています。

このように当初の予想に反しウクライナが善戦できているのは、ウクライナが2014年のロシアによる「クリミア併合」、さらにそれ以降のロシアによる大規模

1　スターリンク（Starlink）とは、Elon Musk氏が率いるSpaceX社が提供している「衛星ブロードバンドインターネット」のことで、自社で打ち上げた数千機もの低軌道衛星をインターネット接続に利用しています。
　スターリンクを導入すると、通信環境が整備されていない山間部でも高速・低遅延のインターネット接続が実現します。

なサイバー攻撃による大被害を教訓として、欧米諸国の政府とハイテク企業の支援を得て、開戦前からサイバー領域の戦闘に関して多大な準備をしてきたことが大きいと言われています。

【防衛省　令和４年度防衛白書　P11から引用】

そして、開戦以降もロシアの大規模なサイバー攻撃に対して、欧米諸国の支援を受けて的確な防御を行っており、その結果として、ロシアのサイバー攻撃は、物理的な領域に対して大きな影響を与えるような成果を得るに至っていません。

また、電磁波領域については、ロシア軍の通信内容の盗聴や、ロシア軍幹部及び司令部の位置を探知するのに有益な役割を果たしています。

【https://newsukraine.rbc.ua/news/first-successful-strike-on-russia-s-su-57-1717917206.html から引用】

ロシア軍の通信インフラは性能が低く、特に最新の暗号通信機が不調であり、ロシア軍は民間の携帯電話などに依存し、米国の諜報機関に通信内容を傍受されました。こうした情報収集活動により、ロシア軍の動きや位置、作戦計画の内容などが米国を経由し、情報を得てから30分から１時間以内にウクライナ軍に提供

されたと言われています。こうした活動の結果、ウクライナ軍は多くのロシア軍将官の殺害に成功したと言われています。

電磁波領域に関しては、ロシア軍は世界で最も経験豊富で、最も設備の整った電子戦部隊を持っているとされてきました。

実際、ロシア軍の電子戦部隊は、ウクライナ軍の砲兵の位置を特定するとともに、砲弾やロケット弾の誘導を行っているといわれています。また、ウクライナ軍の無人兵器のレーダーと通信回線を妨害し、ウクライナ軍がロシア軍の砲兵陣地を特定するのを妨げています。これに対し、ウクライナ軍も、米国から提供された対ドローンシステムを使って、ロシア軍のドローンのGPS信号を妨害し、また高出力マイクロ波により電子機器を損傷させたりして、数百機を撃墜したといわれています。

3　新領域における防衛活動の重要性

2022年２月に始まったロシア・ウクライナ戦争ではウクライナ軍の通信は民間企業である米スペースＸ社の「スターリンク」が担っており、偵察にも欧米民間企業の商用衛星が使われています。実際、ウクライナ戦争の開戦初日には、米国の商用通信衛星に対しロシアからサイバー攻撃が行われ、大規模な通信障害を引き起こされたと言われています。また国連総会の会合の場で、ロシア政府は西側諸国の人工衛星も軍事目標とみなす可能性に言及しています。

技術革新による新たな領域の急速な拡大は、陸・海・空という従来の物理的な領域における対応を重視してきたこれまでの国家の安全保障の在り方を根本から変えようとしている」という認識をベースに、「宇宙・サイバー・電磁波」といった新たな領域については、我が国としての優位性を獲得することが死活的に重要となっています。

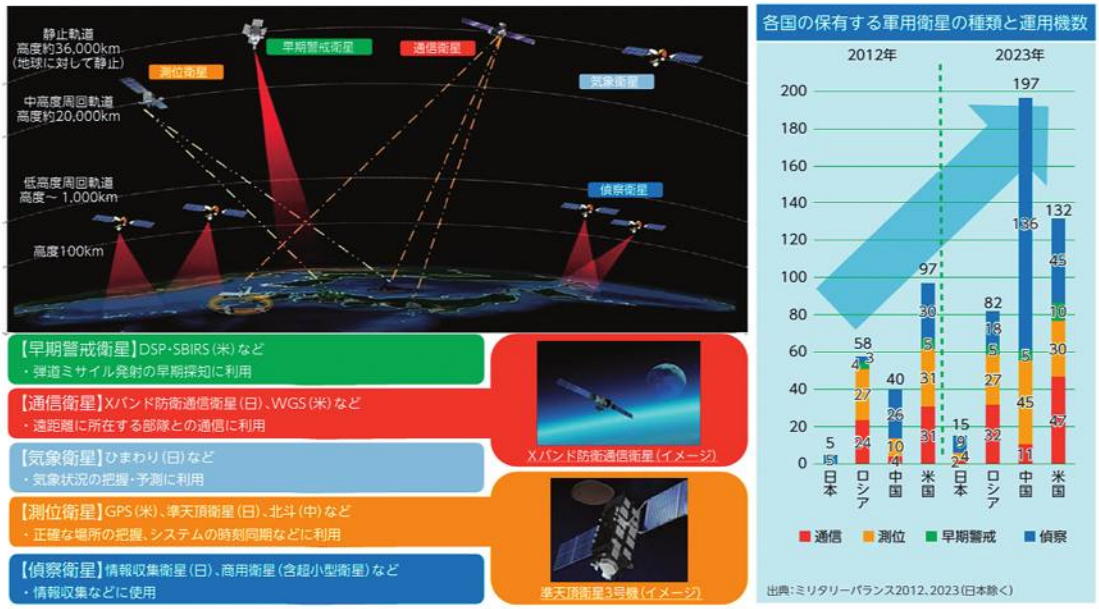
陸・海・空という従来の区分に依拠した発想から完全に脱却し、全ての領域を横断的に連携させた新たな防衛力の構築に向け、従来とは抜本的に異なる速度で変革を図っていくこと、そして、全ての領域における能力を有機的に融合し、その相乗効果により全体としての能力を増幅させる領域横断（クロス・ドメイン）作戦により、個別の領域における能力が劣勢である場合にもこれを克服し、我が国の防衛を全うできるものとすることが必要となっています。

１　宇宙領域

（１）宇宙領域と安全保障

宇宙空間は、国境の概念がないため、人工衛星を活用すれば、地球上のあらゆる地域の観測、通信、測位などが可能です。

図表Ⅲ-1-4-10　安全保障分野における宇宙利用（イメージ）



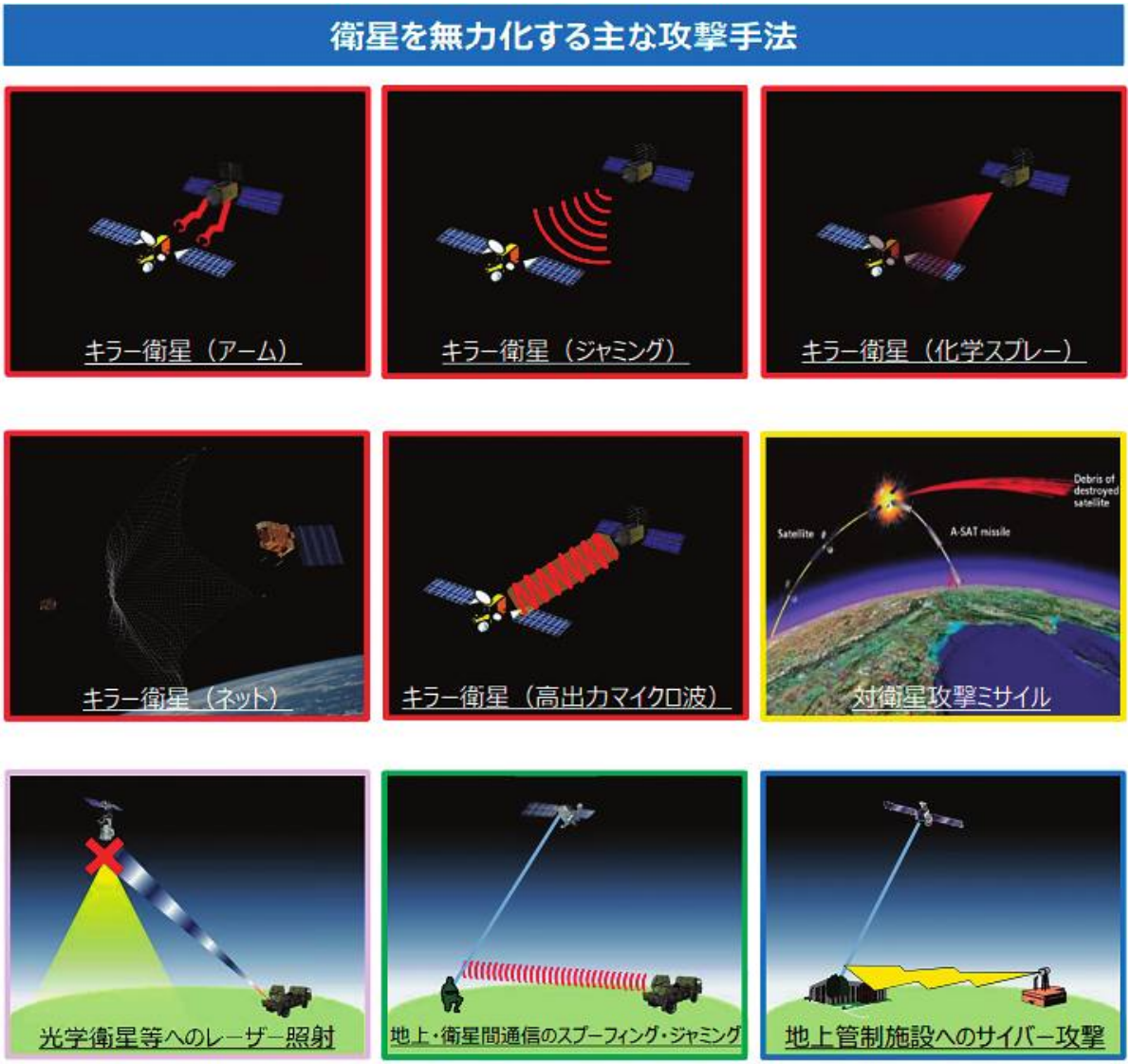
【防衛省　令和６年度防衛白書P284から引用】

このため主要国は、C4ISR（Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance）機能の強化などを目的とし、各種活動などを画像や電波として捉える情報収集衛星、弾道ミサイルなどの発射を感知する早期警戒衛星、武器システムに位置情報を提供する測位衛星、通信を中継する通信衛星など、各種衛星の能力向上や打上げに努めています。

一方、他国の宇宙利用を妨げる対衛星（ASAT）兵器も開発されています。破壊的な直接上昇型対衛星（DA-ASAT）ミサイルについては、中国が2007年に、ロシアが2021年に、それぞれ自国衛星を標的として破壊実験を実施した結果、スペースデブリ（宇宙ゴミ）[2]が多数発生し、各国の衛星などの宇宙アセットに対する衝突リスクとして懸念されています。

2　2002年に国際機関間スペースデブリ調整委員会が採択したガイドラインによると、宇宙ゴミとは、「機能していないすべての人工物体（その破片及び構成要素を含む）で、宇宙空間にあるかまたは大気圏内に再突入するもの」としています。

また、中国については、軌道上での衛星の検査や修理を目的に開発しているロボットアーム技術が衛星攻撃衛星（いわゆる「キラー衛星」）などのASAT兵器に転用される可能性が指摘されているほか、ロシアについては、近接する衛星に対する衛星からの物体放出がASAT実験であると指摘されています。さらに、中国やロシアは、衛星と地上局との間の通信などを妨害する電波妨害装置（ジャマー）や、衛星の機能低下や損傷を目的としたレーザー兵器などの高出力エネルギー技術も開発していると指摘されています。加えて、2022年に衛星通信事業者に対するロシアのサイバー攻撃によって衛星通信サービスが中断しており、宇宙システムへのサイバー攻撃も懸念されています。



【防衛省資料「防衛省の宇宙分野における取組み」令和２年12月から引用】

このように宇宙空間における脅威が増大するなか、各国では、宇宙を戦闘領域や作戦領域と位置づける動きが広がっており、宇宙アセットへの脅威を監視する宇宙領域把握（SDA）に取り組んでいます。既存の国際約束においては、宇宙アセットの破壊の禁止やスペースデブリ発生の原因となる行為の回避などに関する直接的な規定がないため、国連では、平和利用や軍備競争防止の観点から、宇宙空間平和利用委員会や国連総会第一委員会などで議論されています。近年では、軍縮に関する議題「宇宙における軍備競争防止」、「責任ある行動の規範、規則、原則を通じた宇宙における脅威の低減」などが議論されており、2023年の国連総会でも、引き続き議論することが決議されています。このほか、同志国の取組として、宇宙の安全保障を議論する「連合宇宙作戦イニシアチブ（CSpO）」会合が開催され、わが国を含め３か国が新たに加わり、作戦上の協力と情報共有に関して議論しています。

（２）我が国の取り組み

ア　政府の取り組み

2023年６月、宇宙開発戦略本部は国家安全保障戦略を踏まえ、民間技術の防衛分野への活用などを含めた、宇宙の安全保障の分野の課題と政策を具体化させる宇宙安全保障構想を初めて策定するとともに、それを反映した宇宙基本計画を決定しました。宇宙基本計画は、宇宙基本法に基づいて策定されるわが国の宇宙開発利用の最も基礎となる計画であり、わが国の宇宙活動を支える総合的基盤の強化を目標としています。宇宙安全保障構想では、宇宙安全保障の目標を、わが国が、宇宙空間を通じて国の平和と繁栄、国民の安全と安心を増進しつつ、同盟国・同志国などとともに、宇宙空間の安定的利用と宇宙空間への自由なアクセスを維持することとしています。

また、防衛省・自衛隊のニーズを踏まえ、政府関係機関が行っている先端技術の研究開発を防衛目的にも活用することで、政府の研究開発を積極的に防衛力の抜本的強化につなげることも記述されました。その後、宇宙安全保障構想などに基づき、同年10月には、宇宙に関する不測の事態が生じた場合において、事態を正確に把握・分析し、官民が一体となって適切に対応するための宇宙システムの安定性強化に関する官民協議会が設置されました。

2024年３月には、安全保障・民生分野において横断的に、技術・産業・人材基盤の維持・発展に係る課題について検討し、わが国が開発を進めるべき技術を見極め、その開発のタイムラインを示した技術ロードマップを含む宇宙技術戦略が策定されました。そのほか、政府全体の宇宙開発利用に関する

政策の企画・立案・調整などを行っている内閣府宇宙開発戦略推進事務局が中心となり、宇宙活動法[3]、衛星リモセン法[4]や、宇宙資源法[5]に基づき宇宙政策が進められています。

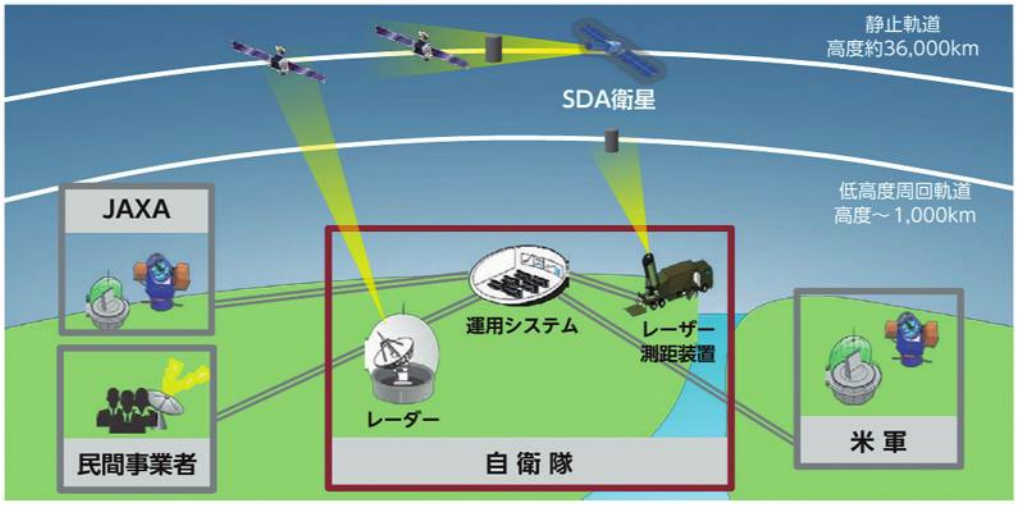
イ　防衛省・自衛隊の取り組み

宇宙領域において、衛星コンステレーションを含む新たな宇宙利用の形態を積極的に取り入れ、情報収集、通信、測位などの機能を宇宙空間から提供することにより、陸・海・空の領域における作戦能力をさらに向上させることとしています。同時に、宇宙空間の安定的利用に対する脅威に対応するため、宇宙からの監視能力を整備し、宇宙領域把握（SDA：Space Domain Awareness）体制を確立するとともに、人工衛星等の打上げ及び人工衛星の管理に関する法律、衛星リモートセンシング記録の適正な取扱いの確保に関する法律、宇宙資源の探査及び開発に関する事業活動の促進に関する法律、宇宙状況把握（SSA）に加え、宇宙機の運用・利用状況やその意図や能力を把握すること。様々な状況に対応して任務を継続できるように宇宙アセットの抗たん性強化に取り組むこととしています。

また、相手方の指揮統制・情報通信などを妨げる能力をさらに強化することとしています。

さらには、宇宙航空研究開発機構（ＪAXA：Japan Aerospace Exploration Agency）を含めた関係機関や民間事業者との間で、研究開発を含めた協力・

図表Ⅲ-1-4-11　宇宙領域把握（SDA）体制構築に向けた取組



【防衛省　令和６年度防衛白書P286から引用】

3 「人工衛星等の打上げ及び人工衛星の管理に関する法律」平成28年法律第76号
4 「衛星リモートセンシング記録の適正な取扱いの確保に関する法律」平成28年法律第77号
5 「宇宙資源の探査及び開発に関する事業活動の促進に関する法律」（令和３年法律第83号）

連携を強化するとともに、米国などの同盟国・同志国との交流による人材育成をはじめとした連携強化を図ることとしています。

（３）課題

各国の宇宙領域への依存が広がる中で、宇宙の安全保障環境には大きな変化が生まれています。冷戦期には、米ソ二極体制においては核の相互抑止が成立しており、その構成要素である宇宙アセットには直接攻撃をしない、という暗黙の了解が米ソ間で成立していました。しかし、今では宇宙で活動する国が増加、中国の台頭をはじめ多極構造になりつつあり、そのような暗黙の了解は崩壊しています。

また、技術の飛躍的進化により小型衛星や商業宇宙利用が進展し、国家以外の主体が宇宙利用可能な時代になりました。

一方、我が国の宇宙政策の起点は1969年の「宇宙の平和利用に関する国会決議」であり、科学技術と産業振興を基本とする宇宙政策と宇宙開発が行われ、安全保障上の視点が欠落していました。2015年に宇宙基本計画の見直しが行われたのを端緒に宇宙安全保障が喫緊の課題となっています。

このような宇宙領域における我が国の安全保障上、課題とされている主な事項は、

①地上と異なり領域管轄権が行使できないという国際法上の特性がある。

②国際法上の自衛権の行使や対抗措置を行う場合に防衛出動の根拠となる事態の認定（誰が？何のために？どのように？等）ができるのか？

③国内法的に宇宙領域における自衛隊の防衛活動は十分に可能なのか？

など、未だ法的な整備が為されていないため検討、整備すべき課題が山積みとなっています。

２　サイバー領域

（１）インターネットの発達とサイバー攻撃の危険性

私たちは毎日インターネットを使って情報を調べたり、友達と連絡を取ったり、ゲームをしたりしていますが、そのインターネットは1960年代にアメリカの軍事研究機関によって開発され、最初は「ARPANET」という名前で、数台のコンピューターをつなぐためのネットワークとして始まりました。1990年代に入り、インターネットが個人で使えるようになると、インターネットは爆発的に普及していきました。現在では、世界中の人々がインターネットを介して情報を共有するとともに、場所に依存せずにコミュニケーションを取れるようになっています。

さらに、これまではテレビを始めマスメディアの専有物だった情報発信が、ソーシャルメディア（例：Facebook、インスタグラム、X）や動画共有サイト（例：YouTube）を通じて、一個人でも自由かつ簡単にできるようになったことで様々な情報が一瞬で世界を駆けめぐるような時代となり、その真偽に関係なく一個人の発信が世界を動かすほどの重みを持つようにもなってきています。

また、最近では、すべてがインターネットに接続されるようになってきたことで、インターネットを経由して部屋のドアの解除や機器の操作が可能となるなど、ますます便利な生活を多くの人が享受できるようになってきました。しかしながら、その一方で、インターネットを悪用した犯罪や様々な情報操作による問題など多くのリスクがあることも指摘されています。

そして、このようなサイバー空間を悪用した犯罪や破壊活動は一般的にはサイバー攻撃と言われています。防衛省ウェブサイトにおいて、「サイバー攻撃とは、情報通信ネットワークや情報システム等の悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの動作停止や誤作動、不正プログラムの実行やDDoS攻撃[6]（分散サービス不能攻撃）等」[7]として整理されており、近年ではスマートフォンの普及やネットワーク接続が可能な家電やカメラなどIoT機器の増加によりサイバー空間が拡大しており、サイバー攻撃が行われた場合には、社会活動の広範囲で甚大な被害が生じる可能性[8]があります。また、サイバー攻撃には、サイバー攻撃源の特定や抑止が困難といった特性があり、その対応は国家の安全保障・危機管理上の重要な課題となるとも指摘されています。

さらに、サイバー攻撃の危険は、攻撃そのものが目に見えず、被攻撃側が攻撃を受けているにもかかわらずその事実に気づかないことがあることです。特に攻撃の初期段階は、「発見しにくく静かな（密かな）攻撃」と揶揄されるように、攻撃準備として場合によっては何年も前から攻撃対象システムに侵入し

6　多くのコンピューターを利用して、特定のウェブサイトやサービスに大量のトラフィックを送り、システムをダウンさせる攻撃。

7　防衛省･自衛隊の『ここが知りたい！』･自衛隊のサイバー攻撃への対応について（防衛省ウェッブサイト）https://www.mod.go.jp/j/press/shiritai/cyber/index.html

8　現在では病院、銀行、電力会社など、私たちの生活に欠かせないサービスがインターネットを通じて管理されていますが、サイバー攻撃によりこれらのサービスが停止させられたり、場合によっては命に関わる問題を生起させる可能性もあります。例えば、病院のコンピューターシステムが攻撃されると、カルテの参照ができなくなったり、病院の受付を始めとする病院の業務ができなくなったり、更には、治療そのものに影響する場合があります。また、企業や政府機関がサイバー攻撃を受けると、銀行からお金が引き出せなくなったり、取引に障害が発生し、多額の損失が発生したり、経済全体が影響を受ける場合もあります。

てマルウェア[9]を埋め込み、時を待つこともあります。そして、あるときいきなりそれらのマルウェアが起動され様々な被害をもたらすのです。当然攻撃を受けた側は、被害が明るみになったときには既に対応が追いつかないという状況が生起することになります。

（2）サイバー領域と安全保障

サイバー戦は、直接的な物理的な戦闘ではなく、コンピューターやネットワークを舞台にしたサイバー領域での戦いであり、人の目には見えない部分が多く、一般の人には理解しづらい面があります。しかし、その影響は先に述べたとおり私たちの生活に極めて大きな影響を与えるだけでなく、軍事の世界においては、戦う前に既に勝負がついてしまう場合もあります。併せて、プロパガンダや偽情報の拡散など認知領域での戦いもサイバー戦の一種と考えられており、これにより社会に動揺と混乱を与え、人の心に疑心暗鬼を生起させ、戦争の推移に大きな影響を与えます。人間の身体に例えるなら、サイバー攻撃は人間の脳や神経に直接ダメージを与えることで、目や耳の機能を物理的に奪わなくても視覚や聴覚を奪い、運動能力を麻痺させるようなものと言えます。

2014年のロシアによるクリミア侵攻は、まさにその例と言えます。クリミア併合の間、ロシアはウクライナの重要インフラ、特に通信事業者へのサイバー攻撃と物理的攻撃による通信妨害を徹底的に行うとともに、これに合わせ様々な形での情報戦を繰り広げた[10]と言われており、ほぼ無血で成し遂げられたクリミア併合にサーバー攻撃が果たした役割は極めて大きいと言われています。

また、サイバー攻撃は有事の戦いだけではなく、平時やグレーゾーンにおいても積極的に実施されていることが、その他の戦いとの大きな違いです。具体的には、平時において官公庁や企業のホームページがサイバー攻撃を受けてダウンしたニュースやランサムウエア[11]攻撃を受けた病院の電子カルテのシステムやバックアップ用データを暗号化して病院に身代金を要求した事件など、比較的頻繁にサイバー攻撃が実施されています。また、物理的破壊の例も近年数多く報告されるようになりました。古くは官公庁や企業のコンピューターに侵

9　マルウェア（malware）は、「悪意のある」という意味の英語「malicious（マリシャス）」と「software」を組み合わせて作られた造語であり、不正かつ有害に動作させる意図で作成された悪意のあるソフトウェアや悪質なコードの総称。

10　松原美穂子『ウクライナのサイバー戦争』株式会社新潮社、2023年、15 ～ 32ページ。

11　ランサムウェアとは、マルウェア（コンピューターやネットワークに侵入し、システムを破壊したり、データを盗んだりする様々な悪意のあるソフトウェア）の一種で、ファイルを暗号化し、元に戻すための身代金（ランサム）を要求する。なお、更に危険なマルウェアとしては、「ワイパー」（感染したコンピュータのハードディスクドライブ内のデータを完全消去して使用不能にする目的で使用されるマルウェアの一種）が有名。

入して情報を搾取したり、データを消去・破壊したりするサイバー攻撃が多くみられていましたが、2010年にイランにあるウラン濃縮工場の遠心分離器を破壊したマルウェアStuxnetの登場以降、海外ではエネルギー分野や重要機器製造分野、通信分野などへのサイバー攻撃が増加しています。そのなかで、ウクライナでの電力システムを狙ったサイバー攻撃は、電力会社のコンピューターと制御システムへの侵入によってブレーカーなどを遠隔操縦し、2015年と2016年に連続して大規模停電を発生させました。この大規模停電事件はサイバー攻撃でも電気の供給を止められると初めて証明した事件でもあり、大きな衝撃を持って受け止められました。

また、このように表面化しているサイバー攻撃のほか、有事に備えて平時から標的組織のシステムに侵入し、マルウェアを標的のシステムに埋め込んでおく活動が活発的に実施されているのも、サイバー戦の大きな特徴の一つになっています。例えば、一般的なサイバー攻撃は、標的組織への侵入口を探すサイバー偵察行為から始まると言われていますが、ロシア・ウクライナ戦争においては、2021年初頭から標的型攻撃（フィッシング攻撃）作戦を開始し、2021年夏ごろにはウクライナの軍や国・地方行政機関などへの侵入行為が行われていたと言われています[12]。

このように、サイバー戦は、平時と有事の区別をつけるのが極めて難しい戦いであり、これまでに我々が経験してきた戦争とは全く異なる形態の戦争であると言えます。

（3）我が国の取り組み

サイバー攻撃対処に関する我が国としての取り組みは、2013年策定の国家安全保障戦略において言及され、国全体としてサイバー空間の防護及びサイバー攻撃のへの対応能力の一層の強化を図ることとされました。さらに、30大綱においては、宇宙・サイバー・電磁波の領域を初めて新たな領域と定義した上で、宇宙・サイバー・電磁波を含む全ての領域における能力を有機的に融合し、平時から有事までのあらゆる段階における柔軟かつ戦略的な活動の常時継続的な実施を可能とする、真に実効的な防衛力として、『多次元統合防衛力』を構築することを目指すと言及しました。そして、サイバー領域に関しては、「サイバー領域を活用した情報通信ネットワークは、様々な領域における自衛隊の活動の基盤であり、これに対する攻撃は、自衛隊の組織的な活動に重大な障害を生じ

12 大澤淳「ロシア・ウクライナ戦争と領域横断の戦い」笹川平和財団新領域研究会（編）『新領域安全保障』株式会社ウェッジ、2024年、10 ～ 14ページ。

させるため、こうした攻撃を未然に防止するための自衛隊の指揮通信システムやネットワークに係る常時継続的な監視能力や被害の局限、被害復旧等の必要な措置を迅速に行う能力を引き続き強化する。また、有事において、我が国への攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力等、サイバー防衛能力の抜本的強化を図る。その際、専門的な知識・技術を持つ人材を大幅に増強するとともに、政府全体の取組への寄与にも留意する。」としています。令和元年版防衛白書には「サイバー攻撃対処の６本柱」として、サイバー防衛隊の新設のほか、情報システムの安全確保、サイバー攻撃対処態勢の整備、最新技術の研究、人材育成、他機関等との連携の６つの施策が提示され、サイバー攻撃対処の強化を推進する方針が示されました。

図表Ⅲ-1-2-13 防衛省・自衛隊におけるサイバー攻撃対処のための総合的施策

【防衛省　令和元年度防衛白書P294から引用】

次の大きな変化は、2022年に制定されたいわゆる戦略３文書においてです。

国家安全保障戦略には、サイバー安全保障分野での対応能力の向上として、サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するためにサイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させると極めて大きな目標を掲げました。

イギリス・ロンドンの国際的戦略研究所（IISS）の2021年６月の「世界各国のデジタル総合力の評価（CYBER CAPABILITIES AND NATIONAL POWER: A NET ASSESSMENT）」[13]において、日本はイランやインド、インドネシア、北朝鮮などと同じ３番手グループに位置付けられていたことを考えると、その目標がどれだけ大きいか理解できると思います。そして、武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合は、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために『能動的サイバー防御』を導入するとしました。

『能動的サイバー防御』とは、ACD：Active Cyber Defenseを日本語訳したものと言われていますが、213回国会に提出された衆議院の法律案[14]の中では「外部からのサイバー攻撃について、これによる被害が発生する前の段階から、その兆候に係る情報その他の情報の収集を通じて探知し、その主体を特定するとともに、その排除のための措置を講ずることにより、国家及び国民の安全を損なうおそれのあるサイバー攻撃の発生並びにこれによる被害の発生及び拡大の防止を図ること」と定義されており、従来、我が国がとってきた自己の情報ネットワーク内における対応である受動的防御[15]からは格段に権限が強化されることになります。特に、「被害が発生する前の段階から」の活動が可能になることで、平時から自衛隊サイバー防衛隊が実施できる活動の幅が大きくなり、我が国のサイバー防護能力が格段に向上すると言われています。

ア　自衛隊サイバー防衛隊

防衛省におけるサイバー防護の体制に関しては、2006年（平成18年）３月の統合幕僚監部の新設に伴う統合運用体制の移行にあわせ、2008年（平成20年）３月に自衛隊創設以来初の常設統合部隊として編成された自衛隊指揮通信システム隊（Command Control Communication Computers Systems Command 略称：C4SC）が新設され、2014年（平成26年）３月にその隷下にサイバー防衛隊が新編されたことで大きく前進します。

13　同評価は、米国や中国、ロシアなどの世界主要国15カ国を対象に、サイバーセキュリティの強固さやサイバースペースに対するガバナンス、サイバー攻撃能力など、７項目を総合的に判断し、３段階で評価したもので、１位には唯一米国がランクインし、２位には豪州、カナダ、中国、仏、イスラエル、英国がランクイン。日本はインド、インドネシア、イラン、マレーシア、北朝鮮、ベトナムと共に最下位。

14　第213回国会（2024年（令和６年）１月26日に召集された通常国会（会期は ６月23日までの150日間））に提出された法律案「サイバー安全保障を確保するための能動的サイバー防御等に係る態勢の整備の推進に関する法律案」

15　大澤淳「ロシア・ウクライナ戦争と領域横断の戦い」笹川平和財団新領域研究会（編）『新領域安全保障』株式会社ウェッジ、2024年、183 ～ 197ページ。

ただ当時は、自衛隊指揮通信システム隊が所掌する情報システム・ネットワークの防護が中心であり、規模も100名程度でした。

【防衛省　令和４年度防衛白書P207から引用】

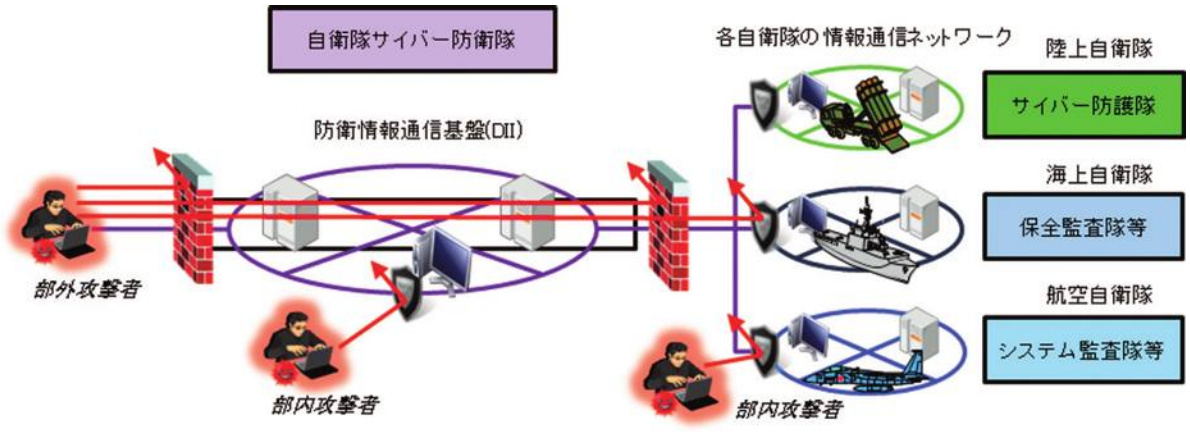
30大綱において、「自衛隊の情報通信ネットワークを常時継続的に監視するとともに、我が国への攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力等、サイバー防衛能力を抜本的に強化し得るよう、共同の部隊としてサイバー防衛部隊を保持する」とし、2022年（令和４年）３月17日、自衛隊指揮通信システム隊の体制を見直し、陸海空自衛隊の共同の部隊として、自衛隊サイバー防衛隊を新編しました。

この部隊の新編により、従来保有していたサイバー防護機能に加え、実戦的な訓練環境を用いて自衛隊のサイバー関連部隊に対する訓練の企画や評価といった訓練支援を行う機能を整備するとともに、より効果的・効率的にサイバー防護が行えるよう、陸海空自衛隊のサイバー部隊が保有するサイバー防護機能を当隊へ一元化するなど、陸海空を統合した体制強化も図りました。

自衛隊サイバー防衛隊の任務としては、主にサイバー攻撃などへの対処を行うとともに、防衛省・自衛隊の共通ネットワークである防衛情報通信基盤（DII）の管理・運用などを担っています。防衛省ウェッブサイト「防衛省・自衛隊の『ここが知りたい！』自衛隊のサイバー攻撃への対応について」では、下図とともに自衛隊サイバー防衛隊が情報通信ネットワークの監視及びサイバー攻撃への対処を24時間態勢で実施するほか、各自衛隊においても、陸上自衛隊サイバー防護隊、海上自衛隊保全監査隊、航空自衛隊システム監査隊等の各システム防護部隊がそれぞれの情報システムを監視・防護をしています。」と説明しています。

また、ネットワーク関連技術は日進月歩であり、サイバー攻撃なども日増しに高度化、巧妙化していることから、迅速かつ的確な対応を可能とするた

め、同盟国などとの戦略対話や共同訓練、民間部門との協力などを通じ、サイバーセキュリティにかかる最新のリスク、対応策、技術動向を常に把握するとともに、サイバー攻撃対処能力の向上に日々取り組んでいると言われています。

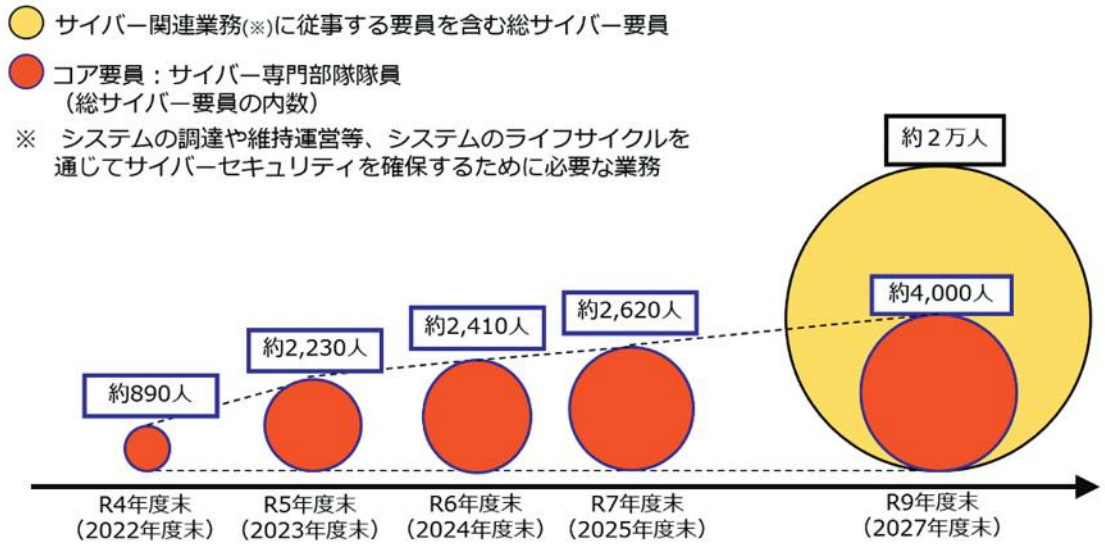


【防衛省　陸上自衛隊HP
（https://sec.mod.go.jp/gsdf/gcc/c5command/spu/profile.html）から引用】

イ　サイバー要員の養成

戦略３文書の一つ、防衛力整備計画には、防衛省･自衛隊のサイバーセキュリティ態勢の強化のため、陸上自衛隊通信学校を陸上自衛隊システム通信・サイバー学校に改編し、サイバー要員を育成する教育基盤を拡充するとともに、我が国へのサイバー攻撃に際して当該攻撃に用いられる相手方のサイバー空間の利用を妨げる能力の構築に係る取組を強化するとしています。そして、これらの取組を行う組織全体としての能力を強化するため、2027年度を目途に、自衛隊サイバー防衛隊等のサイバー関連部隊を約4,000人に拡充し、さらに、システム調達や維持運営等のサイバー関連業務に従事する隊員に対する教育を実施することで、2027年度を目途に、サイバー関連部隊の要員と合わせて防衛省・自衛隊のサイバー要員を約２万人体制とし、将来的には、更なる体制拡充を目指すとしています。

○　サイバー要員化の推進



【防衛省　防衛力抜本的強化の進捗と予算（令和７年度)】

ウ　その他の取り組み

（ア）リスク管理枠組み（RMF：Risk Management Framework）の実施

一過性の「リスク排除」から継続的な「リスク管理」へ考え方を転換し、情報システムの運用開始後も常時継続的にリスクを分析・評価し、必要なセキュリティ対策を実施するものです。

（イ）情報システムの防御

一元的なサイバーセキュリティ対策が可能とする防衛省クラウドを整備するとともに、内部の潜在的脅威を継続的に探査・検出するスレットハンティング機材などを整備し、装備品や施設インフラを含む情報システムの防護態勢を強化します。

（ウ）防衛産業におけるサイバーセキュリティ対策

防衛関連企業に対するサイバーセキュリティ対策の強化を下支えするための取組を実施します。

（４）課題

ア　能動的サーバー防御

わが国では現在、安全保障上の懸念を生じさせる重大なサイバー攻撃　について、未然に攻撃者のサーバーなどへの侵入及び無害化ができる「能動的サイバー防御」の法整備が進行中です。しかしながら、このためには様々な国内法上の課題の整理や法整備と共に国際法上の合法性の確保を不断に行う必要があります。

例えば、国内法上の課題として、

①サイバー防衛のため、情報収集に伴う通信傍受を行うことは可能か？

②サイバー防衛のため、平時及びグレーゾーンにおいて、どのような法的根拠をもって自衛隊がサイバー活動を行うことができるのか？

等の指摘もあります。

また、国際法上の課題として

①国家が関与するサイバー攻撃について国際法上の責任を追及するための要件は？

②サイバー攻撃に民間企業が参加する場合、国際法上は保護することは可能か？

③自国領域外の警察権による活動する場合の要件は？

等の指摘もあります。

これらの課題を克服し、我が国が能動的サイバー防御を実施できる体制を構築するため、能動的サイバー防御の法案成立が喫緊の課題となっています。

イ　人材育成

前項で示したように、サイバー要員の拡充に関しては、組織改編、教育体制の見直し等防衛省内でも積極的に取り組んでいますが、4,000人のサイバー関連部隊の要員を含む２万人のサイバー要員の養成は、現状の募集難の状況を考慮しなくても極めて厳しい目標であると言えます。

3　電磁波領域

（1）電磁波領域と安全保障

電磁波とは電場の振動と磁場の振動が空間を伝わる波のことであり、携帯電話、テレビ、無線LAN（Wi-Fi)、GPSなど、今や私たちの日々の生活において電磁波は身近でかつ必要不可欠なものとなっています。このような電磁波ですが、防衛分野においても、これまでも指揮統制のための通信機器、敵の発見のためのレーダー、ミサイルの誘導装置などをはじめ多くの分野で使用されています。例えば、装備品のネットワーク化や、小形無人機のスウォーム（群れ）飛行といった技術は、電磁波の利用が不可欠なものとなっています。

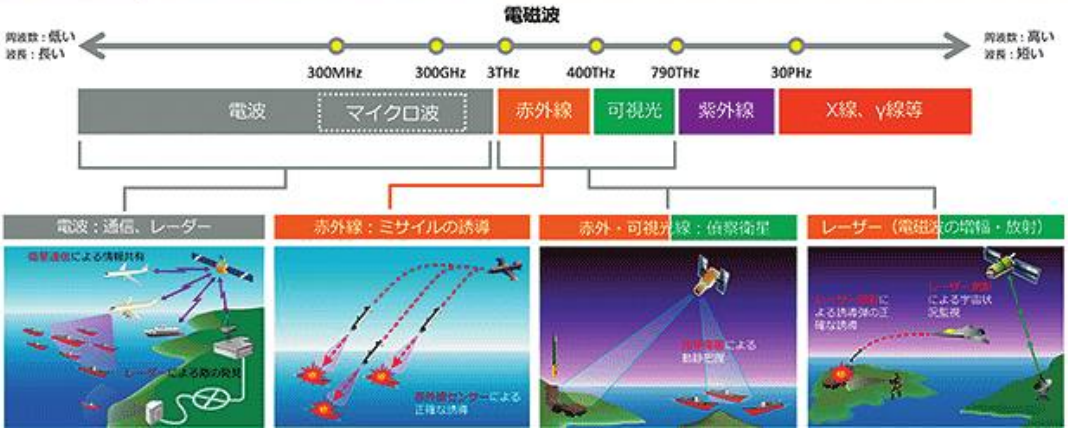
同時に、相手の電磁波の利用を妨害する技術も格段に進歩しており、諸外国では、無線通信への妨害や、測位信号の妨害による無人機の活動の阻害といった事例も報告されています。ウクライナ戦争においても、ロシアのドローンを飛べなくするためにウクライナが電波妨害装置を使用しているとの報道もなされています。

このように防衛分野における電磁波領域における主要国の使用は以下の図表

に示すとおりです。敵の電磁波使用を妨害する電子攻撃をサイバー攻撃などと同様に敵の戦力発揮を効果的に阻止する非対称的な攻撃手段として認識するとともに、電子攻撃を含む電子戦能力を重視し、その能力を向上させているところです。

今や電磁波領域における優勢を確保することは、現在の作戦において必要不可欠なものになっています。

図表Ⅰ-4-4-1　防衛分野における電磁波領域の使用



【防衛省　令和６年度防衛白書P192から引用】

（２）我が国の取り組み

今や近代戦において、その優越が作戦の帰趨に大きな影響を与える電磁波領域において、防衛省・自衛隊としても、相手方からの通信妨害などの厳しい電磁波環境下、自衛隊の電子戦やその支援能力を有効に機能させ、相手によるこれらの作戦遂行能力を低下させるなど、能力強化を着実に進める方向で各種努力が進められている。

さらに、電磁波の管理機能を強化し、防衛省・自衛隊全体としてより効率的に電磁波を活用していく方向で各種取り組みが進められています。

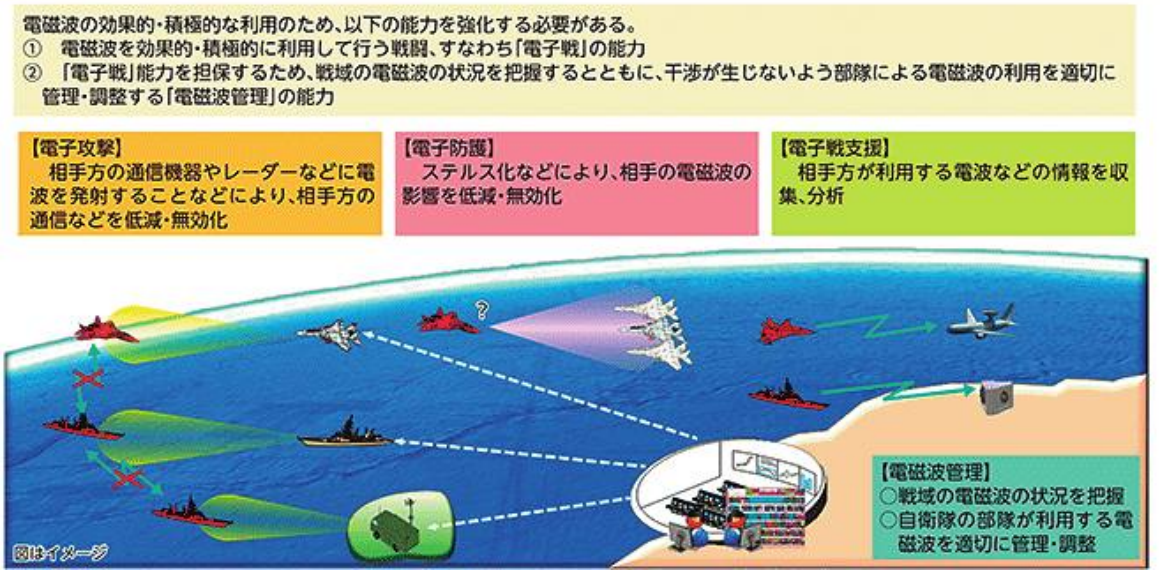
このような中、特に民生用の周波数利用と自衛隊の指揮統制や情報収集活動などのための周波数利用を両立させ、自衛隊が安定的かつ柔軟な電波利用を確保できるよう、関係省庁と緊密に連携しつつ、電磁波領域における能力を強化していく点が強調されています。

ア　電子戦妨害能力（通信・レーダー妨害能力）などの強化

平素からの情報収集・分析に基づき、レーダーや通信など、わが国に侵攻を企図する相手方の電波利用を無力化することは、他の領域における能力が劣勢の場合にも、それを克服してわが国の防衛を全うするための一つの手段として有効であり、その能力強化を図って行く方向とされています。

2024年度には、平素から電波情報の収集・分析を行い、有事においては、

図表Ⅲ-1-4-14　電子戦能力と電磁波管理能力（イメージ）



【防衛省　令和６年度防衛白書P295から引用】

相手の電波利用を無力化する機能を有するネットワーク電子戦システム（NEWS：Network Electronic Warfare System）や対空電子戦装置を取得するとともに、低電力通信妨害技術や将来電磁パルス（EMP：Electro Magnetic Pulse）装備技術の研究が進められています。また、小型無人機などへの対処能力の向上を図るため、高出力レーザーや高出力マイクロ波（HPM：High Power Microwave）といった指向性エネルギー技術の研究を今後さらに推進することとされています。

イ　電子戦防護能力の強化

電磁波領域での通信妨害や電信戦に伴う影響を最小限に抑えることで、航空優勢を確保するため、電子防護能力に優れたF-35A戦闘機の取得を進めていくこととされています。さらに、戦闘機運用の柔軟性を高めるためにも、電子防護能力に優れ、短距離離陸・垂直着陸（STOVL）が可能なF-35B戦闘機を取得するとともに、F-15戦闘機の能力向上を進めていくこととされています。

ウ　電子戦支援能力の強化

電磁波領域での戦闘を優位に進めるためには、平時から有事までのあらゆる段階において、電磁波に関する情報を収集・分析し、これを味方の部隊で適切に共有することが重要となっています。

2024年度には、電子妨害や電子防護に必要となる電磁波に関する情報を収集する能力を強化するため、RC-２電波情報収集機を取得するほか、電子作戦機の開発を推進する方向で取り組みが進められています。

エ　電磁波管理機能の強化

電磁波を効果的、積極的に利用して戦闘を優位に進めるためには、電子戦能力を向上していくとともに、電磁波の周波数や利用状況を一元的に把握・調整し、部隊などに適切に周波数を割り当てる電磁波管理の態勢を整備することが必要となってきます。

このため、装備品の通信装置やレーダー、電子戦装置などが使用する電磁波の状況を把握、モニター上で可視化し、電磁波の利用状況を把握・管理する機能を強化するため、電磁波管理機能の整備を推進する方向です。

オ　訓練演習、人材育成

自衛隊の電磁波領域の能力強化や専門的知見を有する隊員の育成のため、統合電磁波作戦訓練を実施するほか、米国の電子戦教育課程への要員派遣などを通じ、最新の電磁波領域に関する知見の収集やノウハウの獲得を推進している状況です。

2023年11月に実施された自衛隊統合演習においては、陸・海・空自の電子戦部隊が空自入間（いるま）基地（埼玉県）に集結し、統合電磁波作戦の訓練にかかる調整を行ったとされています。また､同年９月から10月にかけて、海自は米海軍との相互運用性の向上を図るため、EP-３多用機を米国に派遣し、米海軍との電磁機動戦訓練を実施したとのことでした。

（３）課題

このように電磁波領域においても、防衛省・自衛隊として、各種努力がなされているところですが、他方で未だ多くの課題も山積されていることも事実と思われます。

特に、昨今のウクライナ戦争においても顕著なように、その技術的な革新はその質・量そしてスピードのいずれにおいても著しいものとなっており、これらの技術革新に適確に対応していくためには、研究開発・予算・人材育成等の分野において、これまで以上の努力が求められているようです。

また、電磁波領域において有効な活動をする上では以下のような法的課題も残されています。

①平時及びグレーゾーン（有事を除き）総務省所管の電波法により、周波数利用が厳しく制限されているため、実戦を想定した電子戦訓練が十分に実施できていない。

②グレーゾーンから有事において、相手国が第３国の保有する測位衛星を利用することを妨げるための電磁的妨害は可能か？

③対人で行われる電磁波攻撃を国際法上はどう扱うのか？

4　新領域における提言

このように新領域において解決すべき課題は数多く存在しており、その解消が望まれます。加えて新領域の安全保障体制を強化するためには、「安全保障３文書」に挙げられている施策を確実に推進していくことが肝要です。

特に重要な施策を挙げるとすると次のとおりです。

（１）宇宙領域

2030年までに宇宙監視システム（SDA）を完全稼働させ、他国が運用するASAT兵器やスペースデブリの監視能力を向上させる。

また、米軍やJAXA等との連携のみならず民間機関との連携強化を進め、関係国間における我が国の存在価値を高める。

（２）サイバー領域

「能動的サイバー防護」を可能とする法整備を図るとともに、4,000人のサイバー関連部隊の要員を含む２万人のサイバー要員の養成を図り、さらに攻撃源追跡システム等最新のシステムを導入し、もってサイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる。

（３）電磁波領域

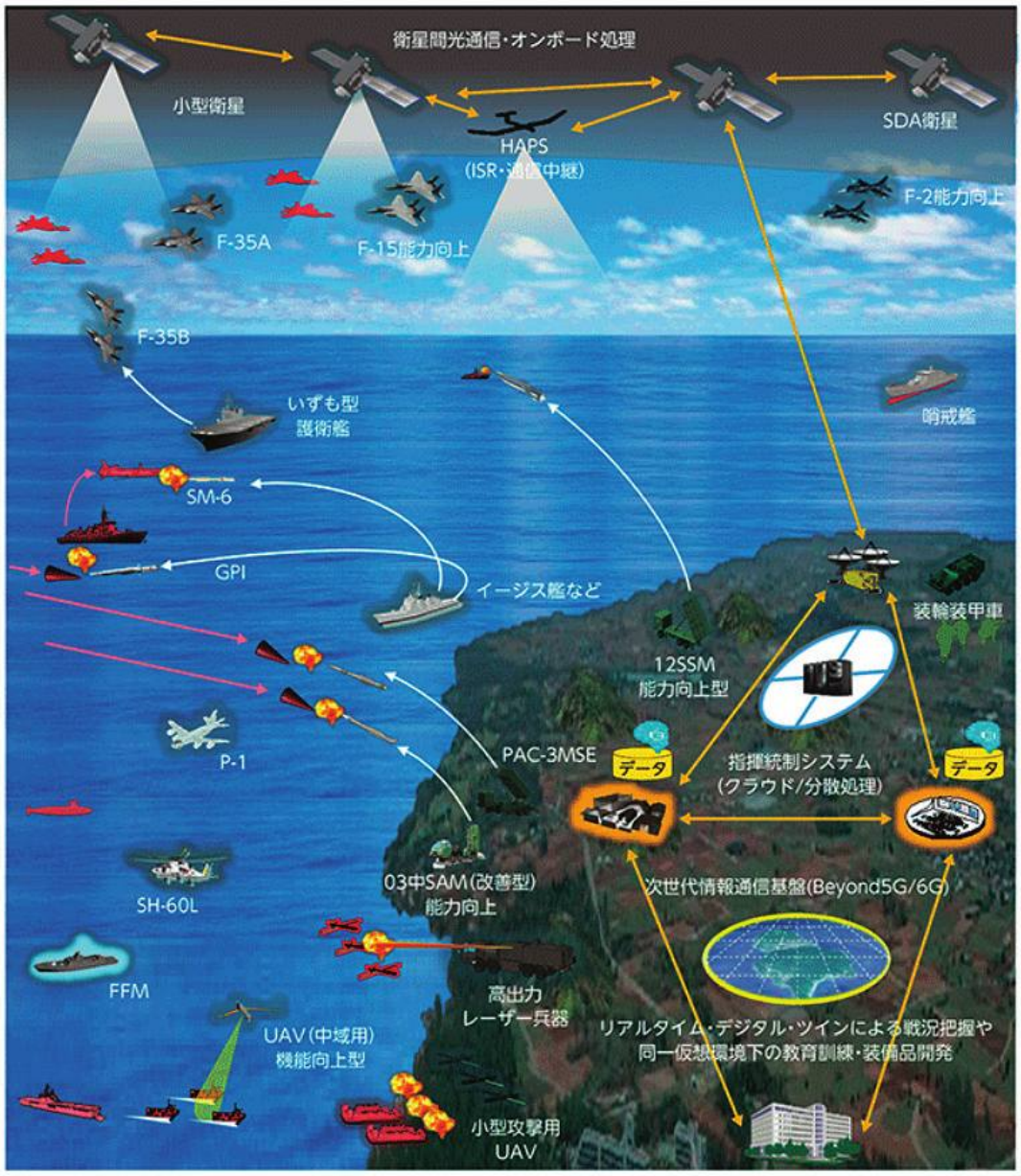
作戦遂行の実効性を担保するため、平時における訓練制約を克服できるように電波法の特例措置に関する議論を関係省庁などと進める。

お　わ　り　に

今回は新領域と呼ばれている宇宙・サイバー・電磁波領域について領域ごとに説明して参りましたが、現実はこれまでの陸・海・空領域における作戦に対して有機的に交わって初めて機能することになります。

具体的には、宇宙から得られる有効な情報を共有し、作戦実施に不可欠な通信の自由を確保するとともに、自衛隊の活動を妨げる電磁波攻撃を抑制することで陸・海・空自衛隊の統合を支えます。いわゆる領域横断作戦という考え方です。

図表Ⅲ-1-4-1　将来の領域横断作戦（イメージ）



【防衛省　令和６年度防衛白書P271から引用】

新領域の活動や装備に関しては技術革新に大きく影響を受けるとともに、民間における研究や開発が国よりも先んじている分野も多く、民間の力に頼らざるを得ないのが現実です。

気候変動、感染症危機等、国境を越えた地球規模課題への対応には、国際社会が価値観や利害の違いを越えて協力することが求められています。

我が国周辺に目を向ければ、我が国は戦後最も厳しく複雑な安全保障環境に直面しています。

また、有事と平時の境目はますます曖昧になってきており、加えて国家安全保障の対象は、経済、技術等、これまで非軍事的とされてきた分野にまで拡大し、軍事と非軍事の分野の境目も曖昧になっています。国内に目を転じれば、人口減少、少子高齢化、厳しい財政状況等の困難な課題に直面しています。

そのような中、防衛力の抜本的強化を始めとして、最悪の事態をも見据えた備えを盤石なものとし、我が国の平和と安全、繁栄、国民の安全、国際社会との共存共栄を含む我が国の国益を守っていかなければなりません。

そのために、我が国はまず、我が国に望ましい安全保障環境を能動的に作り出すための力強い外交を展開する必要があります。そして、自分の国は自分で守り抜ける防衛力を持つことは、そのような外交の地歩を固めるものとなります。

また、こうした目標を達成するためには、地政学的競争、地球規模課題への対応等、対立と協力が複雑に絡み合う国際関係全体を俯瞰し、外交力・防衛力・経済力・技術力・情報力を含む総合的な国力を最大限活用して、国家の対応を高次のレベルで統合させる戦略が必要となり策定されたのが、「国家安全保障戦略」です。

例えば、技術分野ではAIや量子通信を活用した新領域の強化が急務です。また、防衛協力では米国や欧州諸国との戦略的連携を強め、平時から有事までの総合的な対応能力を確率することが必要です。

同時に、国家としての力の発揮は国民の決意から始まります。

伝統的な外交・防衛の分野にとどまらない幅広い分野を対象とする本戦略を着実に実施していくためには、本戦略の内容と実施について国民の理解と協力を得て、国民が我が国の安全保障政策に自発的かつ主体的に参画できる環境を政府が整えることが不可欠となります。

いまこそ、我が国の平和と安寧のために国家を挙げて取り組む時です。

防衛協会の会員の皆様には安全保障に関して身近な方々の関心が向くような活動を是非お願い致します。本編纂が会員の皆様の活動の一助となることを切に願っています。

参考文献

１　「防衛白書」
　　防衛省（令和元年版、２年版、３年版、４年版、５年版、６年版）
２　「新領域安全保障」
　　笹川平和財団　新領域研究会［編］
　　株式会社ウェッジ（2024年１月10日　初版第１刷発行）

「新領域における活動」

（宇宙・サイバー・電磁波）

令和７年３月31日発行　非売品

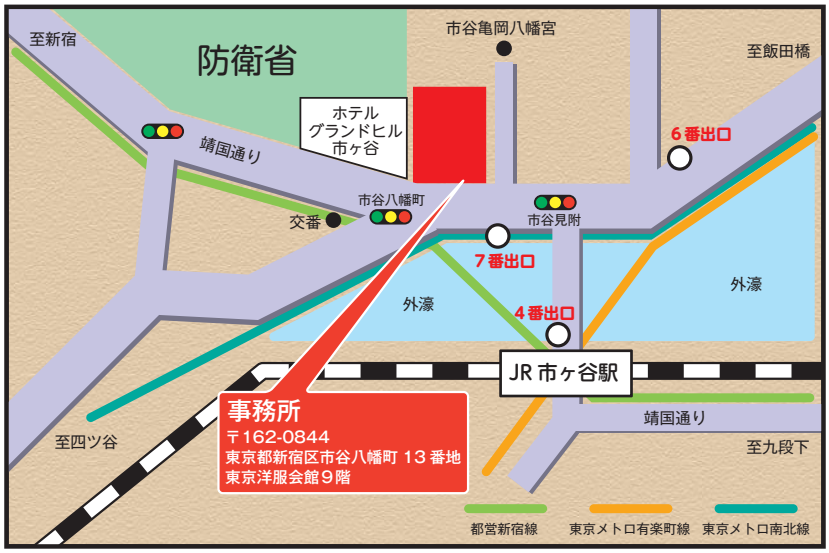
編集発行　全国防衛協会連合会
〒162－0844　東京都新宿区市谷八幡町13番地
東京洋服会館９階
電　話　０３－５５７９－８３４８
ＦＡＸ　０３－５５７９－８３４９
ＵＲＬ　https://ajda.jp
E-mail　jim@ajda.jp

印　　刷　株式会社日刊スポーツPRESS
〒104－0045　東京都中央区築地３－５－10
電　話　０３－５５５０－８２１０
ＵＲＬ　https://www.nikkansp.co.jp/

全国防衛協会連合会
All Japan Defense Association

〒 162-0844
東京都新宿区市谷八幡町13番地
東京洋服会館９階

電話：03-5579-8348
FAX：03-5579-8349
Mail：jim@ajda.jp
URL：https://ajda.jp



●JR 総武線・都営新宿線・東京メトロ有楽町線・南北線「市ヶ谷駅」より徒歩３分