第3節 宇宙・サイバー・電磁波の領域での対応

防衛大綱における、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」の考え方は次のとおりである。

平素から、宇宙・サイバー・電磁波の領域において、自衛隊の活動を妨げる行為を未然に防止するため、常時継続的に監視し、関連する情報の収集・分析を行うとともに、かかる行為の発生時には、速やかに事象を特定し、被害の局限、被害復旧などを迅速に行う。また、わが国への攻撃に際しては、こうした対応に加え、宇宙・サイバー・電磁波の領域を活用して攻撃を阻止・排除する。

さらに、社会全般が宇宙空間やサイバー空間、また、電磁波の利用への依存を高めていく傾向などを踏まえ、関係機関との適切な連携・役割分担のもと、政府全体としての総合的な取組に寄与する。

1 宇宙領域での対応

1 政府全体としての取組

2016年4月に内閣府に設置された宇宙開発戦略推進事務局が、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。宇宙政策を巡る環境の変化や、2013年に閣議決定された国家安全保障戦略を踏まえ、2020年6月には、新たな宇宙基本計画が決定された。自立した宇宙利用大国となることを目指すこの計画は、①多様な国益への貢献、②産業・科学技術基盤をはじめとする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る。そして、多様な国益への貢献として、①宇宙安全保障の確保、②災害対策・国土強靱化や地球規模課題の解決への貢献、③宇宙科学・探査による新たな知の創造、④宇宙を推進力とする経済成長とイノベーションの実現を進めていくこととしている。

2016年11月には、わが国の宇宙開発利用の進展に対応していくため、人工衛星等の打上げ及び人工衛星の管理に関する法律（宇宙活動法）、及び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（衛星リモセン法）が国会にて可決され、2017年11月には、宇宙活動法の一部及び衛星リモセン法が施行された。

また、2018年11月には、打上げの許可制や、賠償措置義務、政府補償など、わが国の宇宙開発及び利用における公共の安全確保及び損害を受けた被害者の迅速な保護を図るために必要な事項を定めた宇宙活動法が本施行された。

さらに、2021年6月には、月や宇宙空間に存在する水や鉱物資源などに所有権を認める宇宙資源法案が国会にて可決、同年12月に施行された。

2 防衛省・自衛隊の取組

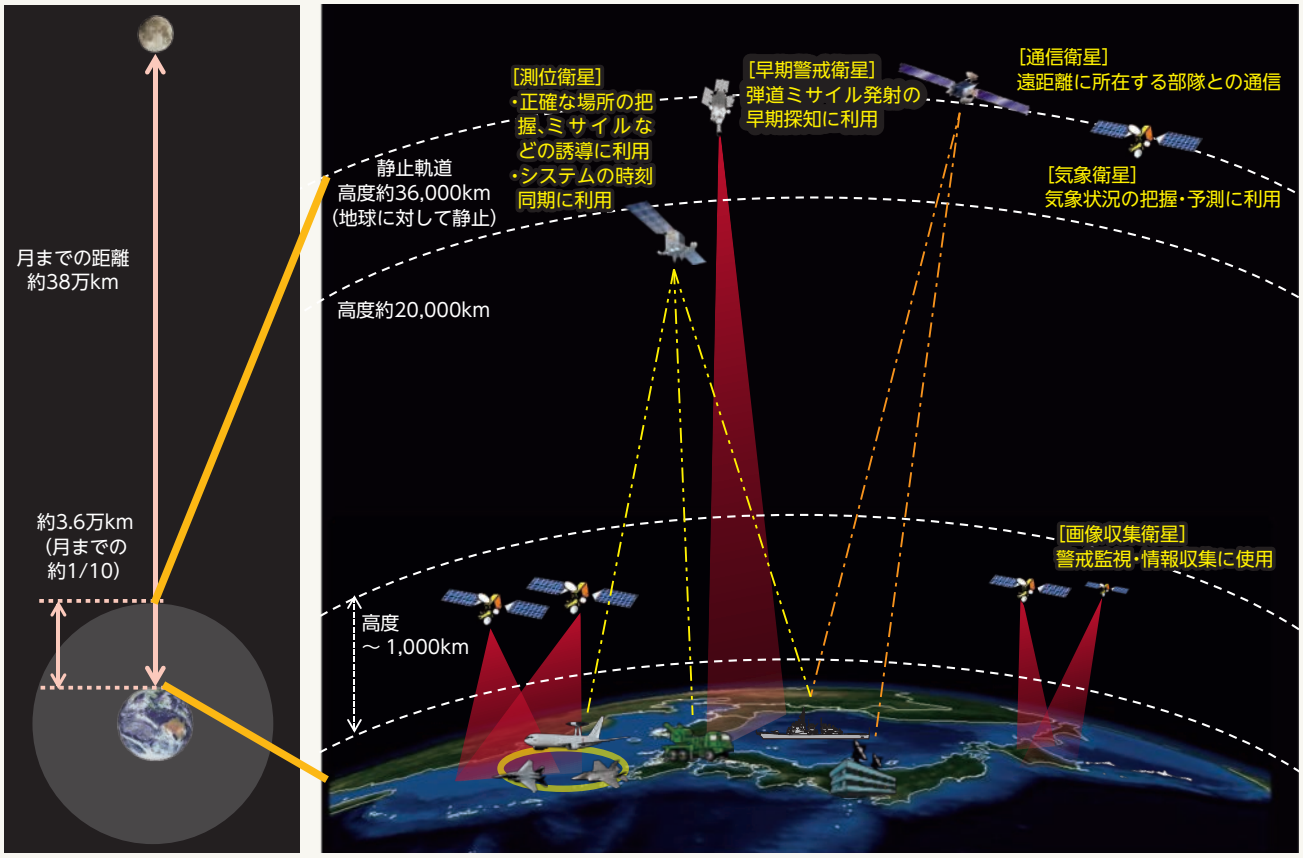
安全保障における宇宙空間の重要性や経済社会の宇宙システムへの依存度の高まり、リスクの深刻化、諸外国や民間の宇宙活動の活発化、商用の小型衛星コンステレーションの本格運用化に伴う宇宙空間の混雑化、宇宙活動の広がり、科学技術の急速な進化など、昨今の宇宙空間における複雑性は増大している。

防衛省・自衛隊では、中期防に基づき、①宇宙空間の安定的利用を確保するための宇宙状況監視（SSA）体制の構築、②宇宙領域を活用した情報収

Space Situational Awareness

動画：宇宙作戦群の新編について
URL：https://youtu.be/y1nvqwtJToE

図表Ⅲ-1-3-1　安全保障分野における宇宙利用のイメージ



集、通信、測位などの各種能力の向上、③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の強化に取り組んでいくこととし、④宇宙航空研究開発機構（JAXA）などの関係機関や米国などの関係国との連携強化を図るとともに、宇宙領域を専門とする部隊や職種の新設などの体制構築や、宇宙分野での人材育成と知見の蓄積を進めている。

Japan Aerospace Exploration Agency

参照　図表Ⅲ-1-3-1（安全保障分野における宇宙利用のイメージ）

(1) 宇宙状況監視（SSA）の強化

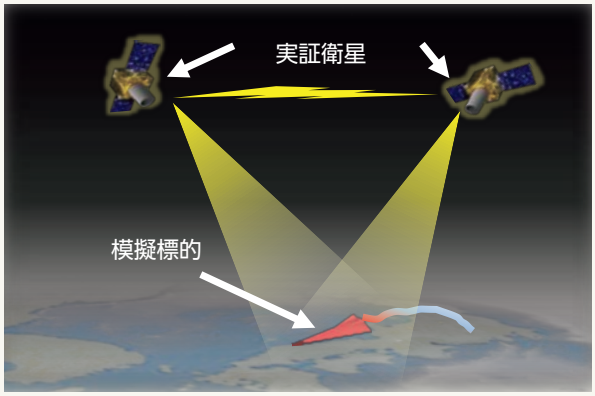
宇宙空間を利用するにあたっては、その安定的な利用を確保する必要がある。しかしながら、2021年11月にはロシアにより衛星破壊実験が行われ1500を超える追跡可能な宇宙ゴミ（スペースデブリ）が発生したと米軍により発表されるなど、スペースデブリが急激に増加しており、スペースデブリと人工衛星が衝突して衛星の機能が著しく損なわれる危険性が増大している。

また、人工衛星に接近して妨害・攻撃・捕獲するキラー衛星の開発・実証試験が進められていると指摘されており、わが国の安全保障や経済社会が依存する宇宙システムに対する脅威が増大している。

このため、防衛省としては、宇宙基本計画を踏まえ、JAXAをはじめとした関係政府機関や米国などと連携しつつ、政府一体となって宇宙を監視し、正確に状況を認識するための宇宙状況監視（SSA）を強化することとし、2023年度以降、空自が宇宙状況監視システム（SSAシステム）の運用を開始することとしている。空自のSSAシステムは、空自及びJAXAのレーダー、望遠鏡などから得られるセンサー情報、米国宇宙コマンドから提供される情報などを集約し、わが国の衛星にとって脅威となるスペースデブリなどを監視することとしており、また、民間の衛星事業者に対し、宇宙状況に関する情報提供サービスを無償で行う予定である。

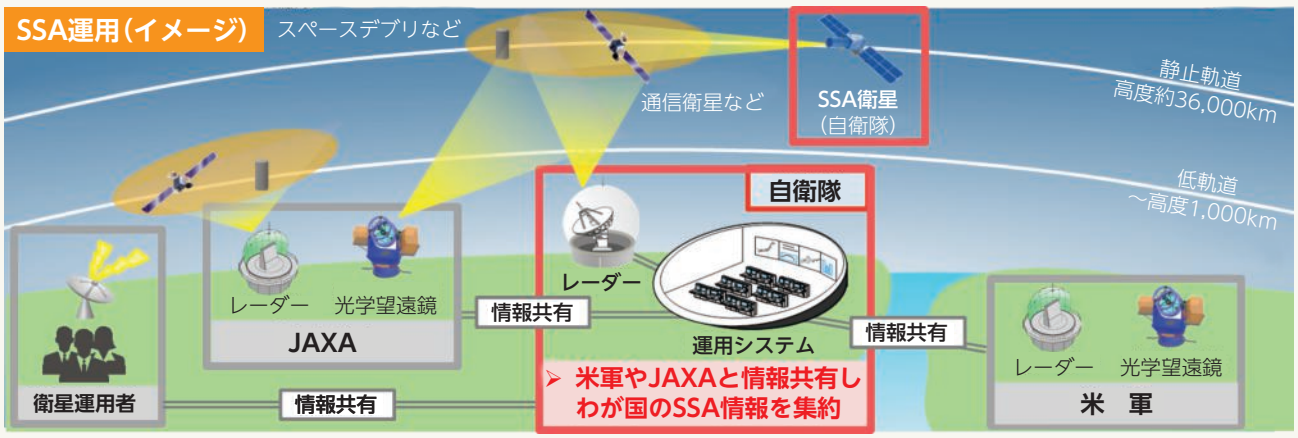
解 説 ミサイル防衛のための衛星コンステレーション活用の検討について

近年、米国などを中心に、多数の小型人工衛星が一体となって様々な機能を担う、いわゆる衛星コンステレーション計画が進められており、宇宙空間からの情報収集能力の強化や、人工衛星に被害が生じた際の機能維持への寄与が期待されています。また、一部の国において、低空を高速かつ変則的な軌道で飛翔するHGV（極超音速滑空兵器）の開発が指摘されていることから、2022年度では、米国との連携も念頭に置きつつ、衛星コンステレーションによるHGVなどを宇宙から探知・追尾するシステムの実現に必要な技術実証にかかる調査研究や、先進的な赤外線センサーにかかる研究を行います。



HGV探知・追尾衛星の実証機（イメージ）

図表Ⅲ-1-3-2 宇宙状況監視（SSA）体制構築に向けた取組



また、宇宙領域専門部隊を強化するため、2020年5月の宇宙作戦隊新編に続き、宇宙作戦指揮所運用隊を新編するとともに、各部隊の上級部隊として宇宙作戦群を2021年度に新編した。そして、2022年度には、同群隷下に第1宇宙作戦隊（仮称）、第2宇宙作戦隊（仮称）及び宇宙システム管理隊（仮称）などを編成する予定である。このうち、第1宇宙作戦隊（仮称）（府中）はSSAシステムの運用を担当し、空自防府北基地レーダー地区に整備中の宇宙状況監視レーダーの遠隔運用も行う。また、第2宇宙作戦隊（仮称）（防府北）は電磁妨害状況把握装置の運用に向けた態勢構築を行うこととしている。さらに、空自において、2026年度までの打上げを目標とするSSA衛星（宇宙設置型光学望遠鏡）などの導入にかかる取組を進めている。

空自がSSAシステムを効果的に運用するためには米国との連携が不可欠であり、米国との情報共有の事項の具体化を進めるほか、米軍が主催する宇宙状況監視多国間机上演習「グローバル・センチネル」及び宇宙安全保障に関する多国間机上演習「シュリーバー演習」への参加を継続するとともに、米国宇宙コマンドへの自衛官の派遣などの取組を推進している。

また、官民横断的な人材交流を通じ、SSA分野における中核的人材の育成及び活用を図っている。

さらに、SSAにかかる能力構築や将来的な能力強

化のため、フランスやオーストラリアなどとの二国間・多国間協力などを推進している。

参照　図表Ⅲ-1-3-2（宇宙状況監視（SSA）体制構築に向けた取組）

(2) 宇宙領域を活用した情報収集、通信、測位などの各種能力の向上

防衛省・自衛隊では、これまでも人工衛星を活用した情報収集、通信、測位などを行ってきたが、C4ISR機能強化の観点から、準天頂衛星[1]を含む複数の測位衛星信号の受信や民間衛星などの利用により冗長性を確保していくこととしている。
Command, Control, Communication, Computer, Intelligence, Surveillance, Reconnaissance

情報収集・警戒監視については、10機体制を目指す情報収集衛星、多頻度での撮像を可能とする小型衛星コンステレーションをはじめとした民間衛星などの利用による重層的な衛星画像の取得を通じ、情報収集能力の強化を図ることとしている。

また、引き続き、JAXAが運用する人工衛星（ALOS-2）から得られる画像や、船舶自動識別装置（AIS）などからの情報を利用するとともに、JAXAの先進光学衛星（ALOS-3）にセンサを搭載して2波長赤外線センサの研究[2]を行うこととしている。
Automatic Identification System

通信については、これまで、部隊運用で極めて重要な指揮統制などの情報通信に使用するため、2017年1月、防衛省として初めて所有・運用するXバンド防衛通信衛星「きらめき2号」を、2018年4月には「きらめき1号」を打上げた。今後、通信所要の増大への対応やさらなる抗たん性強化のため、2022年度には「きらめき3号」の打上げにより、Xバンド防衛通信衛星3機体制を目指すとともに、次期防衛通信衛星の調査研究を行うこととしている。

測位については、多数の装備品にGPS受信端末を搭載し、精度の高い自己位置の測定やミサイルの誘導精度向上など、高度な部隊行動を支援する重要な手段として活用している。これに加え、2018年11月より、内閣府の準天頂衛星システムのサービスが開始されたことから、準天頂衛星を含む複数の測位衛星信号の利用により、冗長性を確保することとしている。

(3) 宇宙利用の優位を確保するための能力の強化

人工衛星の活用が、安全保障の基盤として死活的に重要な役割を果たしている一方で、一部の国が、キラー衛星や衛星攻撃ミサイル、電磁波による妨害を行うジャミング兵器などの対衛星兵器の開発を進めているとみられていることから、防衛省・自衛隊においても、人工衛星の抗たん性強化は重要であり、その一環として、わが国の人工衛星に対する電磁妨害状況把握装置の導入を進めている。

また、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構築することとしている。

さらに、早期警戒などミサイルの探知、追尾などの機能に関連する技術動向として、小型衛星コンステレーションが注目を集めている。米国は数百機以上の安価な小型衛星を打ち上げて、通信・測位・偵察・宇宙状況監視・ミサイル追尾などを行う「国防宇宙アーキテクチャー」計画を進めており、現在、技術実証衛星の打ち上げに向けた準備を進めている。防衛省としては、各国が開発・配備を進めるHGVを早期に探知・追尾する手段として、衛星コンステレーションを用いた宇宙からの赤外線観測が有効である可能性があるほか、通信測位などの分野でも衛星コンステレーションの活用により大きな効果が期待できると考えており、米国との協力も念頭におきつつ防衛分野での衛星コンステレーションの活用のあり方について全省的な検討を行うため、2021年9月に防衛副大臣を議長とする「衛星コンステレーションに関するタスクフォース」を設置し議論を進めることとした。あわせて、2波長赤外線センサの研究による技術的な知見の蓄積、及び高感度広帯域の赤外線検知素子などの将来のセンサの研

1　通常の静止衛星は赤道上の円軌道に位置するが、その軌道を斜めに傾け、かつ楕円軌道とすることで、特定の一地域のほぼ真上の上空に長時間とどまることが可能となるような軌道に投入された衛星のこと。1機だけでは24時間とどまることはできないため、通常複数機が打ち上げられる。ユーザーのほぼ真上を衛星が通るため、山や建物などといった障害物の影響を受けることなく衛星からの信号を受信することができる。

2　探知性、識別性に優れた2波長赤外線センサをJAXAで計画中の「先進光学衛星」に搭載し、宇宙環境において動作させるための研究を実施している。

究を推進することとしている。

(4) 関係機関や米国などの関係国との連携強化

わが国の宇宙安全保障及び宇宙空間の持続的かつ安定的な利用を確保するためには、同盟国や友好国などと戦略的に連携しつつ、スペースデブリ対策などを含めた包括的な観点から、実効的なルール作りに一層大きな役割を果たすとともに、各国に宇宙空間における責任ある行動を求めていくことが必要である。

同時に、誤解や誤算によるリスクを回避すべく、関係国間の意思疎通の強化及び宇宙空間における透明性・信頼醸成措置（TCBM）の実施の重要性を発信していくことが必要である。

Transparency and Confidence Building Measures

また、防衛省が宇宙開発利用を効果的に推進していくためには、先進的な知見を有するJAXAなどの関係機関や米国などの関係国との協力を進めていくことが不可欠である。

米国との間では、宇宙分野における日米防衛当局間の協力を一層促進する観点から、2015年4月に「日米宇宙協力ワーキンググループ」（SCWG）を設置し、これまでに7回の会合を開催している。引き続き、①宇宙に関する政策的な協議の推進、②情報共有の緊密化、③専門家の育成・確保のための協力、④机上演習の実施など、幅広い分野での検討を一層推進していくこととしている。

Space Cooperation Working Group

2 サイバー領域での対応

1 政府全体としての取組など

サイバーセキュリティに関し、2020年度に政府機関に対する不審な通信として、マルウェア感染の疑いが245件、標的型攻撃などが15件検知されており、高度化・巧妙化した手口の攻撃が発生しているなど、実質的な脅威度は引き続き高い状況である[3]。

政府機関以外に対する不審な通信として、防衛関連企業を含む民間企業に対するものも複数判明している。

増大するサイバーセキュリティに対する脅威に対応するため、2014年11月には、サイバーセキュリティに関する施策を総合的かつ効果的に推進し、わが国の安全保障などに寄与することを目的としたサイバーセキュリティ基本法が成立している。

これを受けて、2015年1月には、内閣にサイバーセキュリティ戦略本部が、内閣官房に内閣サイバーセキュリティセンター（NISC）[4]が設置され、サイバーセキュリティにかかる政策の企画・立案・推進と、政府機関、重要インフラなどにおける重大なサイバーセキュリティインシデント対策・対応の司令塔機能を担うこととなった。

National center of Incident readiness and Strategy for Cybersecurity

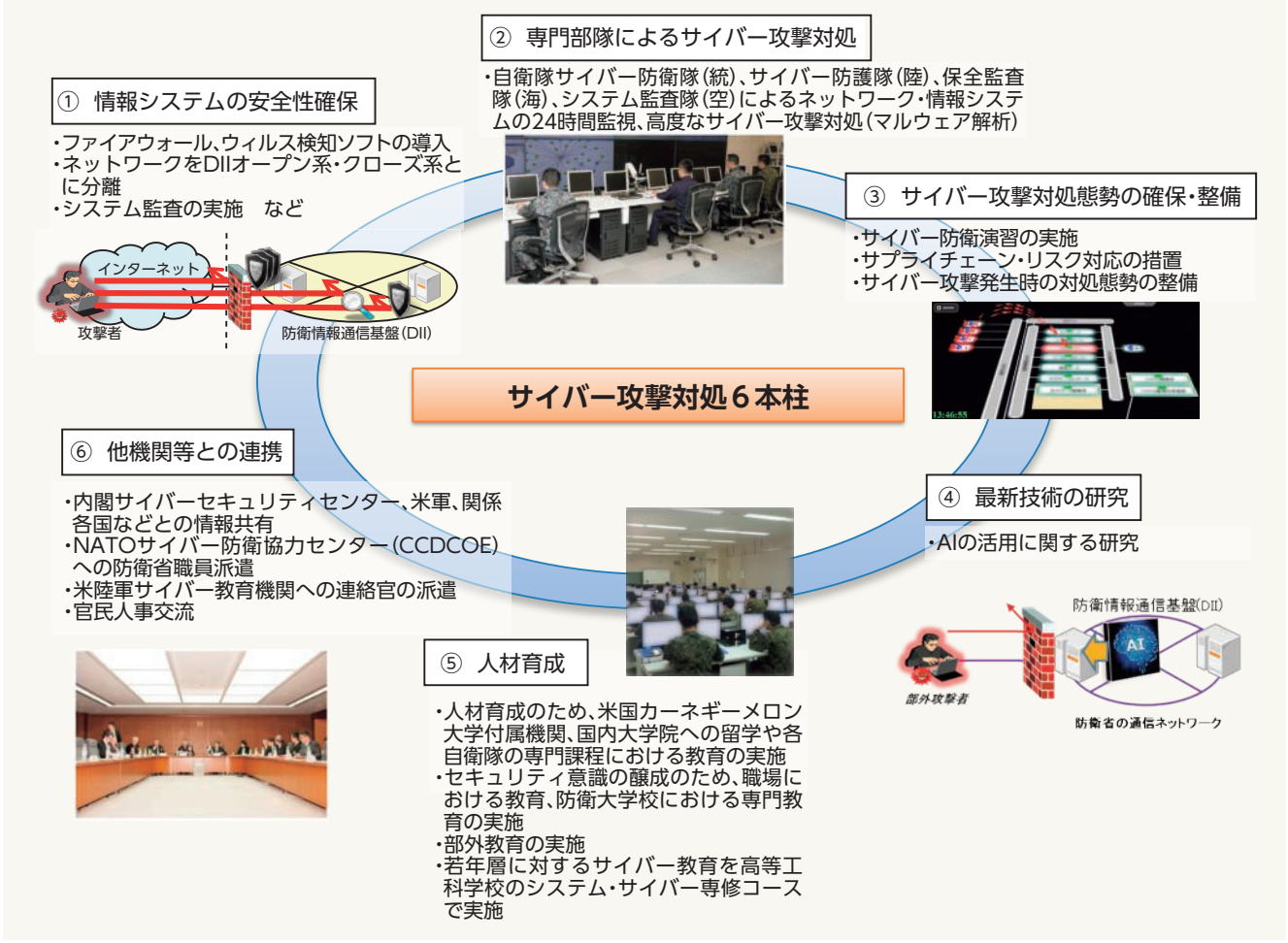
また、同年9月には、サイバーセキュリティに関する施策の総合的かつ効果的な推進を図るため、サイバーセキュリティ戦略が策定され、その目的は、自由、公正かつ安全なサイバー空間を創出、発展させ、もって経済社会の活力の向上及び持続的発展、国民が安全で安心して暮らせる社会の実現、国際社会の平和、安定及びわが国の安全保障に寄与することとされた。

さらに、この戦略は今後3年間にとるべきサイバーセキュリティに関する諸施策の目標や実施方針を示すものとされており、2018年7月と2021年9月に見直しがなされている。3回目の策定となる現戦略では、過去2回のこの戦略で示されてきた基本的な立場を堅持するとともに、「自由、公正、かつ安全なサイバー空間」を確保するため、3つの方向性（①デジタル改革を踏まえたデジタルトランスフォーメーションとサイバーセキュリティの同時推

3 「サイバーセキュリティ2021」（2021年9月27日サイバーセキュリティ戦略本部決定）による。

4 サイバーセキュリティ基本法の成立に伴い、2015年1月に、内閣官房情報セキュリティセンター（NISC：National Information Security Center）から、内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）に改組され、サイバーセキュリティにかかる政策の企画・立案・推進と、政府機関、重要インフラなどにおける重大なサイバーセキュリティインシデント対策・対応の司令塔機能を担うこととされた。

図表Ⅲ-1-3-3　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



進、②公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保、③安全保障の観点からの取組強化）に基づき、施策を推進することとされた。

2　防衛省・自衛隊の取組

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させる。

防衛省・自衛隊では、①情報システムの安全性確保、②専門部隊によるサイバー攻撃[5]対処、③サイバー攻撃対処態勢の確保・整備、④最新技術の研究、⑤人材育成、⑥他機関などとの連携、といった総合的な施策を行っている。

そのような中、防衛大綱に基づき、有事において、わが国への攻撃に際して、この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を含め、サイバー防衛能力の抜本的強化を図ることとしている。具体的には、中期防において、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の寄与も行うこととしている。

参照　図表Ⅲ-1-3-3（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）、資料16（防衛省のサイバーセキュリティに関する近年の取組）

5　情報通信ネットワークや情報システムなどの悪用により、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、情報システムの作動停止や誤作動、不正プログラムの実行やDDoS攻撃（分散サービス不能攻撃）など

(1) サイバーセキュリティ確保のための態勢整備

ア 自衛隊サイバー防衛隊の新編

防衛大綱及び中期防は、サイバー防衛能力を抜本的に強化できるよう、共同の部隊として「サイバー防衛部隊」1個隊を新編することとしている。これに基づき、2021年度にサイバー攻撃などへの対処を行うほか、陸海空自衛隊のサイバー関連部隊に対する訓練支援や防衛省・自衛隊の共通ネットワークである防衛情報通信基盤（DII）[6]の管理・運用などを担う自衛隊サイバー防衛隊を新編した。
Defense Information Infrastructure

イ 情報収集、調査分析機能の強化など

いかなる状況においても防衛省・自衛隊のシステム・ネットワークの機能を確保するためには、この能力を支える情報収集、調査分析機能や実戦的訓練機能などを強化する必要がある。

このため、①サイバー攻撃の兆候や手法に関する情報収集を行う情報収集装置、②AIなどの革新技術を活用したサイバー攻撃対処能力の機能強化を図るとともに、③攻撃部隊と防護部隊による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の取組を継続していくこととしている。

また、サイバー空間における脅威の動向について、情報の収集や諸外国との情報交換など、必要な情報の収集・分析を行っている。

(2) 最新のリスク、対応策及び技術動向の把握

サイバー攻撃に対して、迅速かつ的確に対応するためには、民間部門との協力、同盟国などとの戦略対話や共同訓練などを通じ、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しておく必要がある。このため、民間企業や同盟国である米国をはじめとする諸外国と効果的に連携していくこととしている。

ア 民間企業などとの協力

国内においては、2013年7月に、サイバーセキュリティに関心の深い防衛産業10社程度をメンバーとする「サイバーディフェンス連携協議会」（CDC）を設置し、防衛省がハブとなり、防衛産業間において情報共有を実施することにより、情報を集約し、サイバー攻撃の全体像の把握に努めることとしている。また、毎年1回、防衛省・自衛隊及び防衛産業にサイバー攻撃が発生した事態などを想定した共同訓練を実施し、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。
Cyber Defense Council

イ 米国との協力

同盟国である米国との間では、共同対処も含め包括的な防衛協力が不可欠であることから、日米両政府は、サイバー協力の主要な枠組みとして、まず、防衛当局間の政策協議の枠組みである「日米サイバー防衛政策ワーキンググループ」（CDPWG）を設置した。この枠組みでは、①サイバーに関する政策的な協議の推進、②情報共有の緊密化、③サイバー攻撃対処を取り入れた共同訓練の推進、④専門家の育成・確保のための協力などについて、7回にわたり会合を実施している。
Cyber Defense Policy Working Group

また、日米両政府全体の枠組みである「日米サイバー対話」への参加や、「日米ITフォーラム」の開催などを通じ、米国との連携強化を一層推進している。

ウ その他の国などとの協力

防衛省においては、NATOなどとの間で、防衛当局間においてサイバー空間を巡る諸課題について意見交換するサイバー協議「日NATOサイバー防衛スタッフトークス」などを行うとともに、NATOや、NATOサイバー防衛協力センター（CCDCOE）が主催するサイバー防衛演習への参加などを続け、NATOとの連携・協力の向上を図っている。
North Atlantic Treaty Organization
Cooperative Cyber Defence Centre of Excellence

また、オーストラリア、英国、ドイツ、フランス及びエストニアとのサイバー協議を行っている。

さらに、シンガポール、ベトナムなどの防衛当局との間で、ITフォーラムを実施し、サイバーセキュリティを含む情報通信分野の取組及び技術動向に関する意見交換を行っている。

さらに2022年3月には、陸自が多国間サイバー

6 自衛隊の任務遂行に必要な情報通信基盤で、防衛省が保有する自営のマイクロ回線、通信事業者から借り上げている部外回線及び衛星回線の各種回線を利用し、データ通信網と音声通信網を構成する全自衛隊の共通ネットワーク

防護競技会を主催し、オーストラリア、フランス、米国などの参加国とともに、サイバー領域における能力の強化を図った。

(3) 人材の育成・確保

自衛隊のサイバー防衛能力を強化するために、サイバーセキュリティに関する高度かつ幅広い知識を保有する人材を確保していくことは喫緊の課題であり、教育の拡充や民間の知見の活用も含めて積極的な取組が必要である。

このため、高度な知識や技能を修得・維持できるよう、要員をサイバー関連部署に継続的かつ段階的に配属するとともに、部内教育及び部外教育による育成を行っている。

2019年度からは各自衛隊の共通教育としてサイバーセキュリティに関する共通的かつ高度な知識を習得させるサイバー共通教育を実施しているほか、米国防大学のサイバー戦指揮官要員課程への隊員の派遣を継続している。また、2021年度からは陸自高等工科学校にシステム・サイバー専修コースを新設するとともに、新たに米陸軍サイバー教育機関が実施するサイバー戦計画者課程への隊員派遣を実施している。

また、2021年7月から、サイバー領域における高度な知識・スキル及び豊富な経験・実績を有する人材を「サイバーセキュリティ統括アドバイザー」として採用している。

また、防衛省における高度専門人材と一般行政部門との橋渡しとなるセキュリティ・IT人材に対する適切な処遇の確保、民間企業における実務経験を積んだ者を採用する官民人事交流制度や役務契約などによる外部人材の活用の検討などにも取り組んでいる。

さらに、サイバーセキュリティは高度な知識をもつ専門人材のみならず、ネットワーク・システムを利用するすべての人員のリテラシーなくしては成立しないことから、情報保証教育をはじめ、一般隊員・事務官などへのリテラシー教育を推進している。

(4) 政府全体としての取組への寄与

防衛省は、警察庁、デジタル庁、総務省、経済産業省及び外務省と並んで、サイバーセキュリティ戦略本部の構成員として、NISCを中心とする政府横断的な取組に対し、サイバー攻撃対処訓練への参加や人事交流、サイバー攻撃に関する情報提供などを行っているほか、情報セキュリティ緊急支援チーム(CYMAT)[7]に対し要員を派遣している。また、NISCが実施している府省庁の情報システムの侵入耐性診断を行うにあたり、自衛隊が有する知識・経験の活用について検討することとしている。

CYber incident Mobile Assistance Team

3 電磁波領域での対応

電磁波は、従来から指揮通信や警戒監視などに使用されてきたが、技術の発展により、その活用範囲や用途が拡大し、現在の戦闘様相における攻防の最前線として、主要な領域の一つと認識されるようになってきている[8]。

こうした状況においては、電磁波領域における優勢を確保することが抑止力の強化や領域横断作戦の実現のためにも極めて重要である。

このため、防衛省・自衛隊においても、防衛大綱などに基づき、①電磁波の利用を適切に管理・調整する機能の強化、②電磁波に関する情報収集・分析能力の強化及び情報共有態勢の構築、③わが国への侵攻を企図する相手方のレーダーや通信などを無力化するための能力の強化、④電磁波領域における妨

7 情報セキュリティ緊急支援チーム。政府として一体となった対応が必要となる情報セキュリティにかかる事象が発生した際に、被害拡大防止、復旧、原因調査及び再発防止のための技術的な支援及び助言などを行うチーム

8 電磁波を用いた攻撃の一つに、核爆発などにより、瞬時に強力な電磁波を発生させ、システムをはじめとする電子機器に過負荷をかけ、誤作動させたり破壊したりする電磁パルス攻撃がある。このような攻撃は、防衛分野のみならず国民生活全体に影響がある可能性があり、政府全体で必要な対策を検討していくこととしている。

害等に際して、その効果を局限する能力の強化などに取り組み、電磁波領域の優越を確保するための能力を獲得・強化していくこととしている。

1 電磁波の利用を適切に管理・調整する機能の強化

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である。

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しモニター上で可視化する電磁波管理支援技術の研究を行うなど、電磁波管理の機能強化を進めている。

参照 図表Ⅲ-1-3-4（電子戦能力と電磁波管理能力のイメージ）

2 電磁波に関する情報収集・分析能力の強化及び情報共有態勢の構築

電磁波の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である。

このため、2022年度においては、2021年度に陸上総隊隷下に新編した電子作戦隊を増勢するととも

VOICE 新編された電子作戦隊の意義・重要性について

電子作戦隊（東京都練馬区） 電子作戦隊隊長
1等陸佐 門田（かどた） 宏光（ひろみつ）

電子作戦隊は2022年3月に陸上総隊隷下に新編された、電磁波作戦を主任務とする部隊です。30大綱において、わが国の防衛力の強化の一つとして多次元統合防衛力の構築が示された中で、今、陸上自衛隊に電子作戦隊を新編することの意義・重要性についてご紹介します。

2006年以降、自衛隊の統合運用が進化し、情報収集や指揮統制におけるICT活用が必要不可欠となる中、サイバー・宇宙領域と同じく電磁波領域の自由を確保することの重要性が高まっています。電磁波領域は、公共放送や携帯電話、各種レーダーといった多種多様な電波がとても過密な状態で飛び交っており、神経の通り道のような繊細な環境になっています。その中で、部隊の指揮統制や情報収集に必要な電波を他の電波と重ならないように常時管理することと、我が部隊の行動の自由を奪おうとする相手方の行動に対しては、神経の通り道である電磁波領域に働きかけることが、作戦を成功に導くために大きな意義を有しかつ、重要となります。

陸上自衛隊には昭和の時代から積み上げてきた電子戦のノウハウがあり、かつ全国各地に配置された部隊が各種活動を実施する際に電波などを適切に管理しつつ通信などを確保してきた実績もあります。電子作戦隊は、年々複雑化を増している電磁波領域においてこれまで積み上げられたノウハウや実績をさらに発展させて、この領域での任務を完遂しうるプロ集団を目指していきます。


電子作戦隊の新編行事における隊旗の授与


隊員を指導する電子作戦隊長

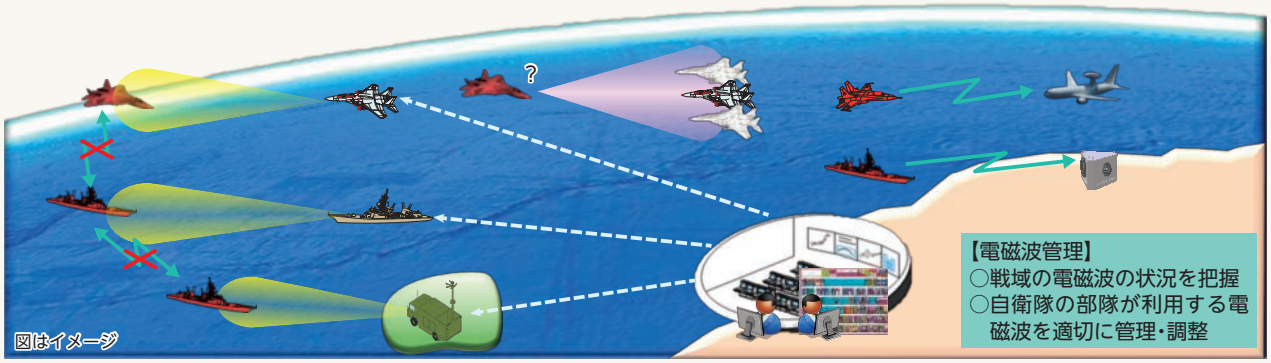
図表Ⅲ-1-3-4　電子戦能力と電磁波管理能力のイメージ

電磁波の効果的・積極的な利用のため、以下の能力を強化する必要がある。
① 電磁波を効果的・積極的に利用して行う戦闘、すなわち「電子戦」の能力
② 「電子戦」能力を担保するため、戦域の電磁波の状況を把握するとともに、干渉が生じないよう部隊による電磁波の利用を適切に管理・調整する「電磁波管理」の能力

【電子攻撃】
相手方の通信機器やレーダー等に電波を発射することなどにより、相手方の通信などを低減・無効化

【電子防護】
ステルス化などにより、相手の電磁波の影響を低減・無効化

【電子戦支援】
相手方が利用する電波などの情報を収集、分析



に、陸自のネットワーク電子戦システム（NEWS）Network Electronic Warfare System を米子駐屯地などに配備し、全国に展開する電子作戦隊の指揮・統制を強化するために必要な整備を開始する。また、空自電波情報収集機（RC-2）の機体構成品を取得するほか、海自多用機（EP-3）の後継機の開発に先立ち、AIなどの最新技術を活用した情報収集システムの研究とともに、AIの搭載に必要な技術要件や支援システムなどについて引き続き調査研究を実施するなど、電磁波領域の情報収集・分析能力を強化することとしている。また、防衛情報通信基盤（DII）を含む各自衛隊間のシステムの連接及びデータリンクの整備を引き続き推進することとしている。

3　わが国への侵攻を企図する相手方のレーダーや通信などを無力化するための能力の強化

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る。

このため、2022年度予算においては、相手の電波利用を無力化することで、火力発揮を支援し、陸上戦闘をはじめ各種戦闘を有利にするNEWSの取得や、NEWSを装備する電子戦部隊の配備を進めることとしている。また、相手方の脅威圏外（スタンド・オフ・レンジ）から妨害対象に応じた効果的な電磁波妨害を実施し、自衛隊の航空作戦の遂行を支援する、空自のスタンド・オフ電子戦機の開発、航空機やミサイルなどに搭載されているレーダーや通信機器が使用する電波を探知・識別し、このレーダーや通信機器を無力化する艦艇用の電波探知妨害装置の研究などを進めることとしている。

さらに、多数のドローンを活用したスウォーム（群れ）攻撃の脅威に有効に対処する観点から、高出力マイクロ波照射技術の実証や高出力レーザーシステムの研究などに関する予算を引き続き計上している。

4　電磁波領域における妨害等に際して、その効果を局限する能力の強化

電磁波領域における妨害等に際してその効果を局限し、航空優勢を確保するため、電子防護能力に優れたF-35Aの取得を推進する。また、戦闘機運用の柔軟性を向上させるため、電子防護能力に優れ、

F-35B取得に関する米海兵隊との会議

短距離離陸・垂直着陸が可能なF-35Bを取得する。

5 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図っている[9]。

9 このほか、防衛省・自衛隊においては、各自衛隊の情報を全国で共有するために必要となる通信網の多重化を推進するほか、電磁パルス防護の観点を踏まえた研究を行っている。