

# 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。

第1章

わが国自身の防衛体制

## VOICE

### 新領域における統合運用に係る企画立案機能の整備について

**統合幕僚監部指揮通信システム部**  
**指揮通信システム企画課 (東京都新宿区)**  
 宇宙領域企画班長 1等空佐 津井 信一郎

2021年3月に誕生したばかりの宇宙領域企画班は、自衛隊でも数少ない「宇宙」という名を冠した部署の一つです。班の役割は、宇宙領域に係る各種計画を立案、調整するとともに、装備体系を研究することであり、宇宙を利用したより実効性のある統合運用の確立を目指して各種検討を進めているところです。安全保障の観点から、今後ますます重要性が増す宇宙領域に関する仕事にやりがいを感じるとともに、新たな領域を切り開くパイオニアとしての責任を日々感じつつ勤務しています。

**統合幕僚監部指揮通信システム部**  
**指揮通信システム企画課 (東京都新宿区)**  
 サイバー企画室長 1等海佐 澁谷 芳洋

サイバー企画室は、2014年3月に設置された部署です。サイバー領域に係る各種計画の立案や調整、装備体系の研究を担っており、具体例としては、サイバー領域における能力の向上に資する、サイバー防衛隊の組織編成、関連装置の整備、海外留学を含む各種教育、諸外国との共同訓練の企画・運営などが挙げられます。サイバー領域は日進月歩の分野であり、それゆえ常に高度な技術的知識が要求されるため、ハードルも非常に高く感じられますが、室員は日々の業務を通じて研鑽努力し必要な知識を身に付け、防衛省・自衛隊のサイバー領域における能力の強化に寄与しています。

**統合幕僚監部指揮通信システム部**  
**指揮通信システム企画課 (東京都新宿区)**  
 電磁波領域企画班長 1等陸佐 北原 武

私の勤務する電磁波領域企画班は、本中期防における電磁波に係る態勢強化の一環として、2020年3月に新設されました。電磁波領域に係る各種計画の企画や装備体系の研究が主な役割であり、具体的には、統合運用において電磁波を適切かつ効果的に利用するために、整齊円滑な電磁波管理業務に資するシステムの構築、各自衛隊間の取決め策定、電磁波領域に係る訓練・演習の企画・立案などを担っています。電磁波の利用は、自衛隊の任務遂行にとって必要不可欠なものであり、防衛省・自衛隊の電磁波領域の優越確保のため、業務に邁進していく所存です。



統合幕僚監部指揮通信システム部のシンボルマーク



新領域に係る事業要求について検討中の筆者 (机右側中央：津井、机右側手前：澁谷、机右側奥：北原)

# 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<sup>1</sup>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。

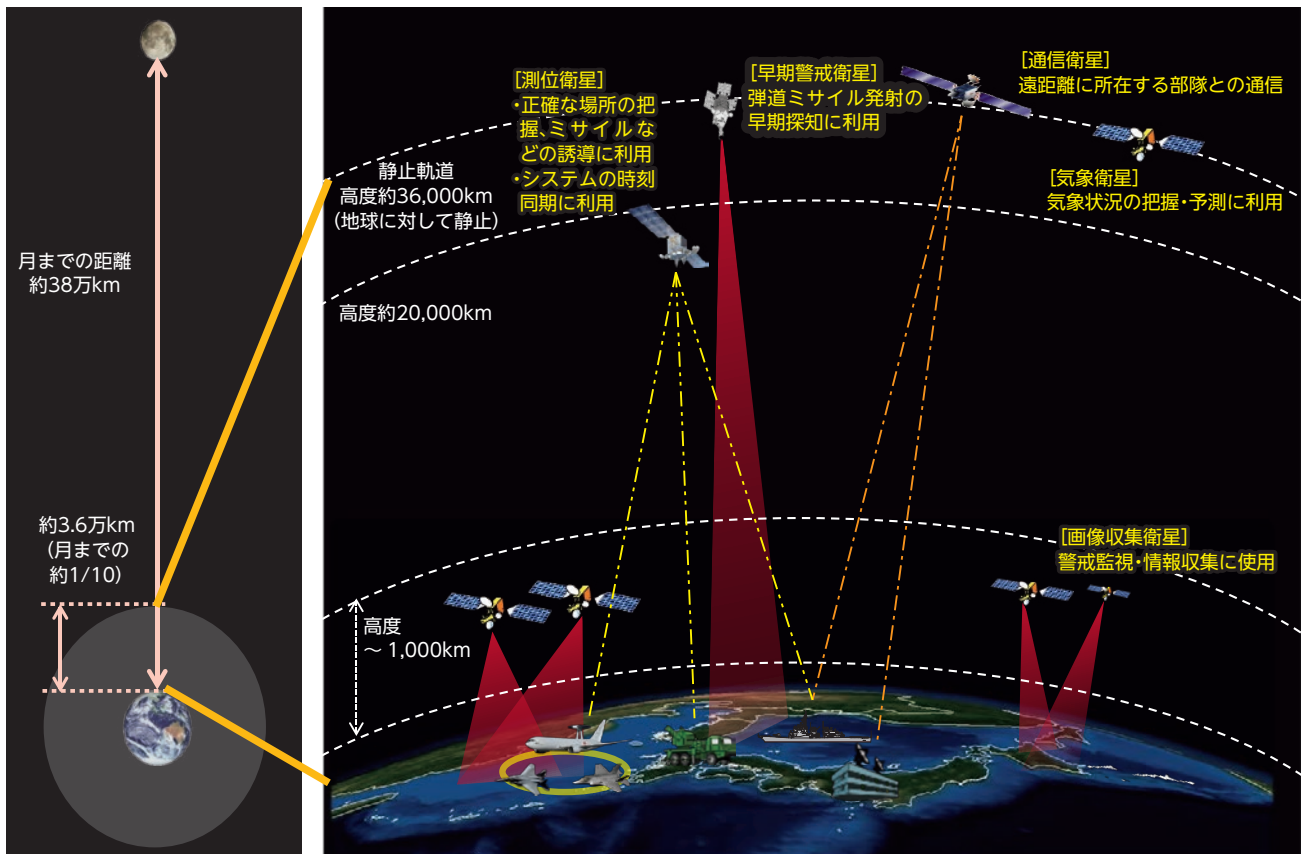
2016年11月には、わが国の宇宙開発利用の進展に対応していくため、人工衛星等の打上げ及び人工衛星の管理に関する法律（宇宙活動法）、及び衛星リモートセンシング記録の適正な取扱いの確保に関する法律（衛星リモセン法）が国会にて可決され、2017年11月には、宇宙活動法の一部及び衛星リモセン法が施行された。

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。

## 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

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 2016年4月に、宇宙戦略室から宇宙開発戦略推進事務局に改組された。

刻化、諸外国や民間の宇宙活動の活発化、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。

**□ 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、宇宙空間において、宇宙ゴミ(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)を強化することを目指している。

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、宇宙領域における様々な活動を計画・遂行するための指揮統制を担う部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(仮称)を令和3(2021)年度に新編することとしている。さらに、令和5

(2023)年度に予定されているSSAシステムの実運用に向けた各種取組を推進するとともに、令和8(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。

その際、宇宙状況監視多国間机上演習(グローバル・センチネル)など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によりSSA体制の整備を効果的に推進している。また、2020年10月から11月にかけて実施した日米共同統合演習(実動演習)においては、宇宙作戦隊によりSSA訓練を実施した。

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に係る能力構築や将来的な能力強化のため、米国と連携したSSAに必要な運用要領の具体化、JAXAをはじめとした関係政府機関との連携、米国やフランスなどとの二国間・多国間協力、民間事業者とのSSAに関する情報共有体制の検討などの具体的な取組を推進している。また、宇宙空間の電磁的環境情報などに関しJAXAに加えて、宇宙天気情報の活用について情報通信研究機構(NICT)との連携を進めている。

**□ 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、準天頂衛星を含む複数の測位衛星信号の受信や商用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。

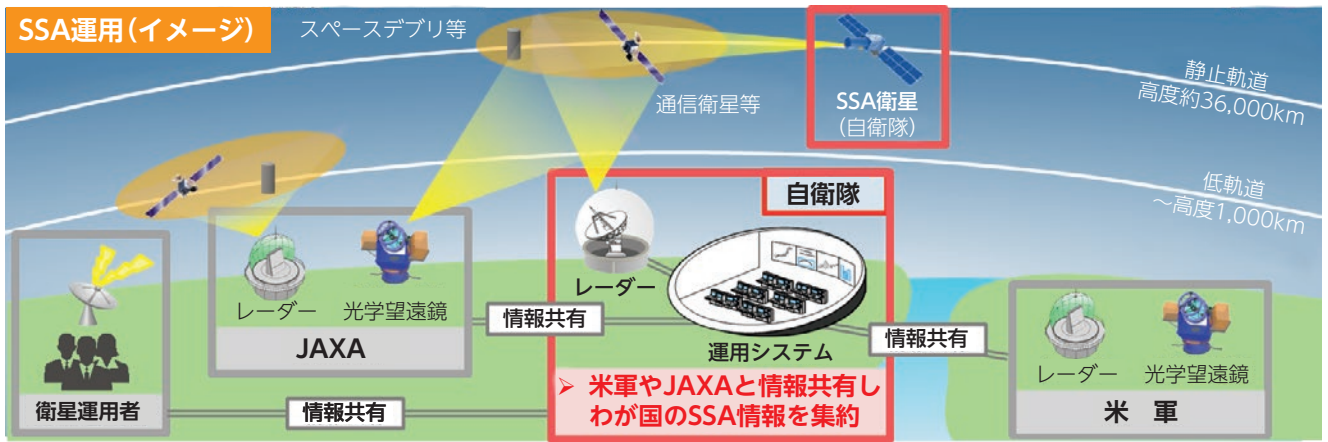
情報収集・警戒監視については、10機体制を目指す情報収集衛星、多頻度での撮像を可能とする小型衛星コンステレーションをはじめとした商用衛星などの利用による重層的な衛星画像の取得を通じ、情報収集能力の強化を図ることとしている。

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、

Automatic Identification System



図表Ⅲ-1-3-2 宇宙状況監視（SSA）体制構築に向けた取組



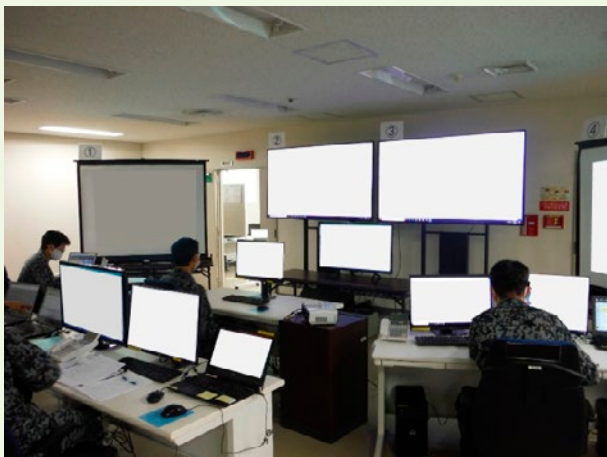
解説

宇宙領域の特性と「宇宙領域シミュレータ」について

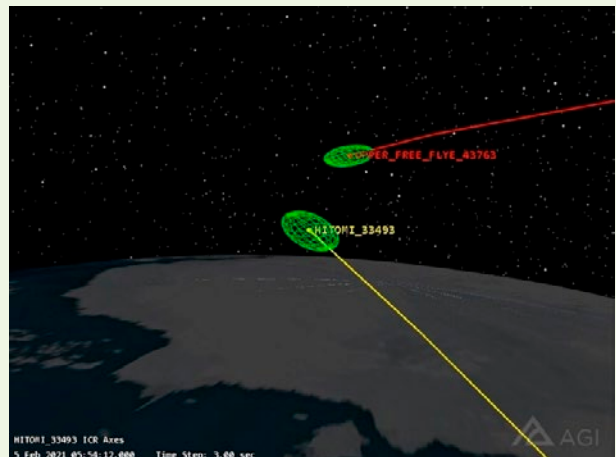
現在、防衛省は宇宙状況監視の体制を構築するため、わが国の人工衛星にとって脅威となる宇宙ゴミなどを監視するレーダーと情報の収集・処理・共有などを行う運用システムの整備を進めています。監視の対象となる宇宙ゴミや各種の人工衛星が周回する高度や軌道の種類は様々で、また人工衛星の運動に影響を与える外力も存在します。したがって、人工衛星に対する脅威を認識するためには、各種軌道の特性や外力による影響などを理解したうえで、例えば人工衛星と宇宙ゴミがいつ、どこで、どの程度まで接近するののかといった解析を行うことが重要な技術の一つとなります。また、地球を取り囲む宇宙の状況を正確に認識するためには、国内関係機関や宇宙関連企業、米国を含めた関係国などとの連携も必要になり、様々な関係部署との連携要領を確立していくことも必要です。こうした宇宙領域における

運用に必要な知識及び技能を備えた要員をシステムの本格的な運用開始までに育成していく必要があります。

このため、航空自衛隊は2020年10月に宇宙領域シミュレータを導入し、宇宙領域に携わる隊員の育成に活用しています。本シミュレータでは、レーダー及び光学望遠鏡などによる宇宙物体の観測データのシミュレーションや軌道決定、地球を含む宇宙空間の模擬、各種アセットの模擬が可能であり、宇宙物体同士の接近や再突入などの様々な事象の解析、教育訓練などで使用する宇宙で起こる事象の作成を行うことができる汎用ソフトウェアが搭載されています。本シミュレータを使用し、隊員は宇宙領域における作戦運用全般に必要な知識及び技能を習得するため、日々教育訓練に励んでいます。



宇宙領域シミュレータを使用した訓練風景



接近事象のシミュレーション結果

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<sup>2</sup>を行うこととしている。

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」を上げた。今後、通信所要の増大への対応や更なる抗たん性強化のため、令和4(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基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予定である。

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誘導弾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<sup>3</sup>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。また、衛星測位能力の抗たん性を強化するため、令和3(2021)年度予算においては、準天頂衛星の公共専用信号を含むマルチGNSS受信機の研究に必要な経費を計上した。

Global Navigation Satellite System

### (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る。

このため、宇宙利用における抗たん性強化の一環として、わが国の人工衛星に対する電磁妨害状況を把握する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



グローバル・センチネルに参加する空自隊員

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について米国との協力も念頭におきつつ検討を行うとともに、2波長赤外線センサの研究による技術的な知見の蓄積、及び高感度広帯域な赤外線検知素子などの将来のセンサの研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

<sup>2</sup> 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。

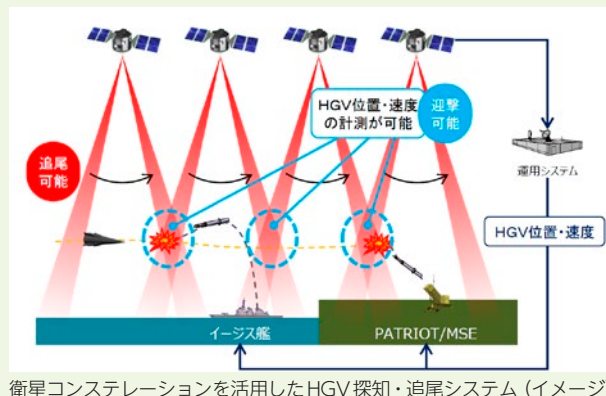
<sup>3</sup> 通常の静止衛星は赤道上に位置するが、その軌道を斜めに傾け、特定の一地域のほぼ真上の上空に長時間とどまることが可能となるような軌道に投入された衛星のこと。1機だけでは24時間とどまることができないため、通常複数機が打ち上げられる。ユーザーのほぼ真上を衛星が通るため、山や建物などといった障害物の影響を受けることなく衛星からの信号を受信することができる。



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、令和3（2021）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探知・追尾システムの概念検討や、先進的な赤外線センサーに係る研究を行います。



衛星コンステレーションを活用したHGV探知・追尾システム（イメージ）

第1章

わが国自身の防衛体制

月に「日米宇宙協働ワーキンググループ」(SCWG) Space Cooperation Working Group 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。

こうした取組の一環として、防衛省は、米宇宙軍主催の宇宙安全保障にかかる多国間机上演習「シュリーバー演習」に2018年から継続的に参加するとともに、米軍教育課程（Space100など）に要員を参加させ、宇宙全般に関する知見の獲得を図っている。

**参照** 2章2節1項1（宇宙に関する協力）p.274  
3章3節1項（宇宙領域の利用にかかる協力）p.357

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、令和元（2019）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55件、標的型攻撃が30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。<sup>4</sup>

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。また、警察当局による捜査において、複数の企業に対するサイバー攻撃に中国人民解放軍の部隊が関与している可能性が高いと結論付け

られたものもあった。

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）<sup>5</sup> National center of Incident readiness and Strategy for Cybersecurity 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

4 「サイバーセキュリティ2020」（2020年7月21日サイバーセキュリティ戦略本部決定）による。

5 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



(※) 政府機関がIT機器や情報システムを調達する際に、サプライチェーン・リスクの懸念がある機器が含まれているか否かをチェックできるよう、2018年12月、内閣サイバーセキュリティセンター(NISC)主導で、IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」を策定した。防衛省としても、これに基づき、機器のサイバーセキュリティの確保に努めている。

策・対応の司令塔機能を担うこととなった。

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、2018年7月には、同戦略の見直しがなされ、前戦略における基本的な立場を堅持するとともに、持続的な発展のためのサイバーセキュリティの推進や、3つの観点(①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働)からの取組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<sup>6</sup>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、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

6 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

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。

**□ 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13（防衛省のサイバーセキュリティに関する近年の取組）

## （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（仮称）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、令和3（2021）年度には、サイバー防衛隊などの体制拡充に加え、陸海空自衛隊のサイバー関連部隊が担っているサイバー防護機能の共同の部隊への一元化に着手することにより、合わせて約160名の体制拡充を図ることとしている。新編する自衛隊サイバー防衛隊（仮称）は、主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）<sup>7</sup>の管理・運用などを担うこととしている。

### 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、当該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などの革新技术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、情報本部においても、サイバー空間における脅威の動向について、公開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）Cyber Defense Council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。

### 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）Cyber Defense Policy Working Group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。

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。

**□ 参照** 2章2節1項2（サイバー空間に関する協力）p.274

### 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

<sup>7</sup> 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



(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。

また、オーストラリア、英国、ドイツ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。

**参照** 3章3節2項(サイバー領域の利用にかかる協力)p.357

### (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は、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することが必要である。

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。

令和元(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かつ高度な知識を習得させるサイバー共通課程<sup>8</sup>を実施しており、今後規模を拡充していくこととしている。

また、サイバー戦における指揮官の意思決定要領などに関する知見を修得するため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。

さらに、部外教育機関を活用した教育を実施するとともに、部外から幅広い人材を確保するため、サイバー領域における最新技術やサイバー攻撃の最新動向などの高度な知見を有するサイバーセキュ



高度化・巧妙化するサイバー攻撃に対応するサイバー防衛隊員

リティ統括アドバイザーの採用に向けた取組や、防衛省サイバーコンテストを行った。

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<sup>9</sup>、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。

### (4) 政府全体としての取組への寄与

防衛省は、警察庁、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)<sup>10</sup>に対し要員を派遣している。

CYber incident Mobile Assistance Team

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。

## 3 電磁波領域での対応

電磁波<sup>11</sup>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

<sup>8</sup> 各自衛隊が実施するIT関連の教育を修了した者に対して、共通的なサイバーセキュリティに関する教育を行うもの

<sup>9</sup> 政府の「サイバーセキュリティ人材育成総合強化方針」(2016年3月31日サイバーセキュリティ戦略本部決定)に基づく施策

<sup>10</sup> CYMAT (Cyber Incident Mobile Assistance Team) : 情報セキュリティ緊急支援チーム (2012年6月設置) 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係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

<sup>11</sup> 電波や赤外線、可視光線(光)、紫外線、X線などの総称。わが国において使用される電波については、総務省が一元的に周波数を管理しており、防衛省・自衛隊が訓練などで使用する周波数についても、総務省から承認を得ている。

解説

防衛省サイバーコンテストについて

サイバー攻撃の脅威が日々高度化・巧妙化するなか、サイバー空間における能力の向上は喫緊の課題であり、サイバーセキュリティに関する専門的知見を備えた優秀な人材の安定的な確保が不可欠となっています。

このため、人材確保の新たな方法として、サイバーセキュリティに関する専門的知見を備えた優秀な人材を発掘することを目的に、「防衛省サイバーコンテスト」を2021年3月14日にオンライン開催しました。

今後も様々な取組を通じて、優秀なサイバー人材を確保し、サイバー防衛協力の抜本的強化に努めていきます。



参加者募集ポスター

第1章

わが国自身の防衛体制

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<sup>12</sup>。

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<sup>13</sup>。

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、敵による電磁波の利用とその効果を妨げつつ、味方による電磁波の利用とその効果を確保する電子戦能力に加えて、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能力を構築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、電波の発射方向や伝搬距離などを計算し、モニター上で可視化する電磁波管理支援技術の研究に着手するなど電磁波管理能力の強化を進めている。

□ 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、陸上総隊隷下に電磁波に関する情報収集などを行う電磁波作戦部隊を新編するほか、令和3（2021）年度予算においては、受信周波数帯域の拡大や遠距離目標収集能力を向上させた空

12 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。

13 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。

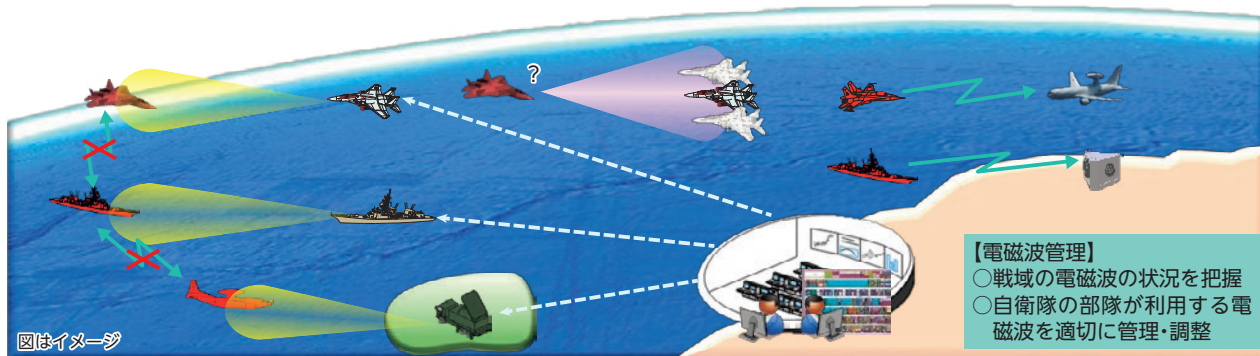


図表Ⅲ-1-3-4 電子戦能力と電磁波管理能力のイメージ

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

電子戦	電子攻撃	○相手方の通信機器やレーダー等に対して電波を放射すること等により、相手方の通信や索敵などの能力を低減・無効化すること。
	電子防護	○装備品のステルス化や通信の耐妨害性の向上により、相手方の電磁波の影響を低減・無効化すること。
	電子戦支援	○電子攻撃や電子防護に必要となる、相手方が利用する電磁波の情報を収集、分析すること。

<b>【電子攻撃】</b> ○相手方の通信機器やレーダー等に電波を放射すること等により、相手方の通信などを低減・無効化	<b>【電子防護】</b> ○ステルス化等により、相手の電磁波の影響を低減・無効化	<b>【電子戦支援】</b> ○相手方が利用する電波等の情報を収集、分析
--	--	---



自電波情報収集機 (RC-2) の搭載装置を取得するほか、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、信号検出能力、方位精度、類識別能力などを強化した情報収集システムの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、それらの情報を確実なセキュリティを確保したうえで各自衛隊において共有するため、自動警戒管制システム (JADGE) の能力向上、防衛情報通信基盤 (DII) を含む各自衛隊間のシステムの接続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的手段として有効である。このため、令和3 (2021) 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、陸上戦闘を始め各種戦闘を有利にする陸自のネットワーク電子戦システム (NEWS) の取得や、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、当該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。

また、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、高出力マイクロ波発生装置の研究や車載レーザーシステムの実証などに関する予算を計上している。

### 4 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には、平素からの教育訓練に加え、実戦経験に裏打ちされた高度なノウハウを有する米国などの訓練・演習や教育に参加することも重要である。



このため、統合電子戦訓練を実施し、電磁波領域における運用能力を強化するほか、米国の電子戦教育課程への要員派遣や英海軍が実施する図上演習への参加、米国などで行われる電子戦シンポジウムへの参加などを通じ、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る予定である。

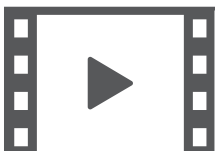


新編された第301電子戦中隊

解説

陸上自衛隊における電磁波作戦部隊の新編による領域横断作戦への貢献

陸上自衛隊では、2021年3月18日をもって新たな電磁波作戦部隊である「第301電子戦中隊」を西部方面隊（熊本県熊本市）に新編しました。本部隊はネットワーク電子戦システム（NEWS）を装備し、電磁波情報の収集・分析や相手の電波利用の無力化などの任務を遂行することから、領域横断作戦に必要不可欠です。当該部隊を通じて、陸上自衛隊は、「多次元統合防衛力」の構築に貢献するとともに、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進めるなど、従来領域における能力向上にも貢献してまいります。



動画：宇宙作戦隊新編行事

URL：<https://www.youtube.com/watch?v=kvm7dXV-hm4>

## 解説

## 電波情報収集機「RC-2」の配備について

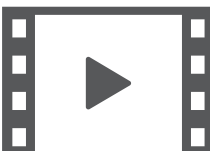
2020年10月1日、航空自衛隊は、入間基地においてRC-2（電波情報収集機）配備記念式典を実施しました。RC-2は、活用範囲や用途が拡大する電磁波領域に対応するため、現有機YS-11EBの後継機として、電磁波に関する情報収集・分析能力の強化及び情報共有態勢の構築を推進することを目的として開発されました。老朽化の著しいYS-11に代わり、国産輸送機C-2に新たな電波情報収集装置を搭載することで、長時間にわたりより広範囲の情報を収集することが可能となっています。

現代の装備品にとって電磁波の活用は必要不可欠なものであり、電磁波の活用範囲や用途の拡大により、現在の戦闘様相における攻防の最前線において、高い電波情報収集・分析能力を持つRC-2の必要性はますます高まっています。特に活発化する周辺国の航空活動に対応するためには、RC-2の情報収集能力及び長時間の運用能力は非常に有用です。

また、その情報共有機能をもって、航空自衛隊内だけでなく、他自衛隊との統合運用、米軍との共同ISR活動においても活躍が期待されています。

さらに、現在の戦闘様相は、技術の進展を背景に、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組み合わせたものとなっており、RC-2の配備は、電磁波領域において優勢を確保し、より効果的な領域横断作戦を実現する点で大きな意義があります。あらゆる領域の基盤ともなる電磁波領域における情報収集能力の強化は、現在の安全保障環境に対応していく上で欠かすことができないものです。

今後、運用に向け、所要の試験及び要員養成などを引き続き実施するとともに、現中期防衛力整備計画の期間を通じてRC-2の整備を着実に推進し、わが国の防衛に万全を期してまいります。



動画：RC-2電波情報収集機配備記念式典

URL：[https://twitter.com/JASDF\\_PAO/status/1313313029849743362](https://twitter.com/JASDF_PAO/status/1313313029849743362)