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。

1 宇宙領域での対応

1 政府全体としての取組

16（平成28）年4月に内閣府に設置された宇宙開発戦略推進事務局[1]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、13（平成25）年に閣議決定された国家安全保障戦略を踏まえ、20（令和2）年6月には、内閣に設置されている宇宙開発戦略本部において、宇宙基本計画が決定された。この計画は、宇宙安全保障上の観点からの施策も含め、必要な予算を十分に確保して、政府を挙げて宇宙政策を強化するための、今後20年程度を見据えた10年間の長期整備計画となっており、①多様な国益への貢献、②産業・科学技術基盤を始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・国土強靭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。

16（平成28）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、17（平成29）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、18（平成30）年11月には、宇宙活動法が本施行された。

宇宙活動法では、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当該損害の被害者の迅速な保護を図るために必要な事項が定められた。また、衛星リモセン法では、①リモセン装置の使用の許可、②リモセン記録（いわゆる衛星画像）を取扱う者の認定や③衛星リモセン記録の提供の禁止の制度などが定められた。

2 防衛省・自衛隊の取組

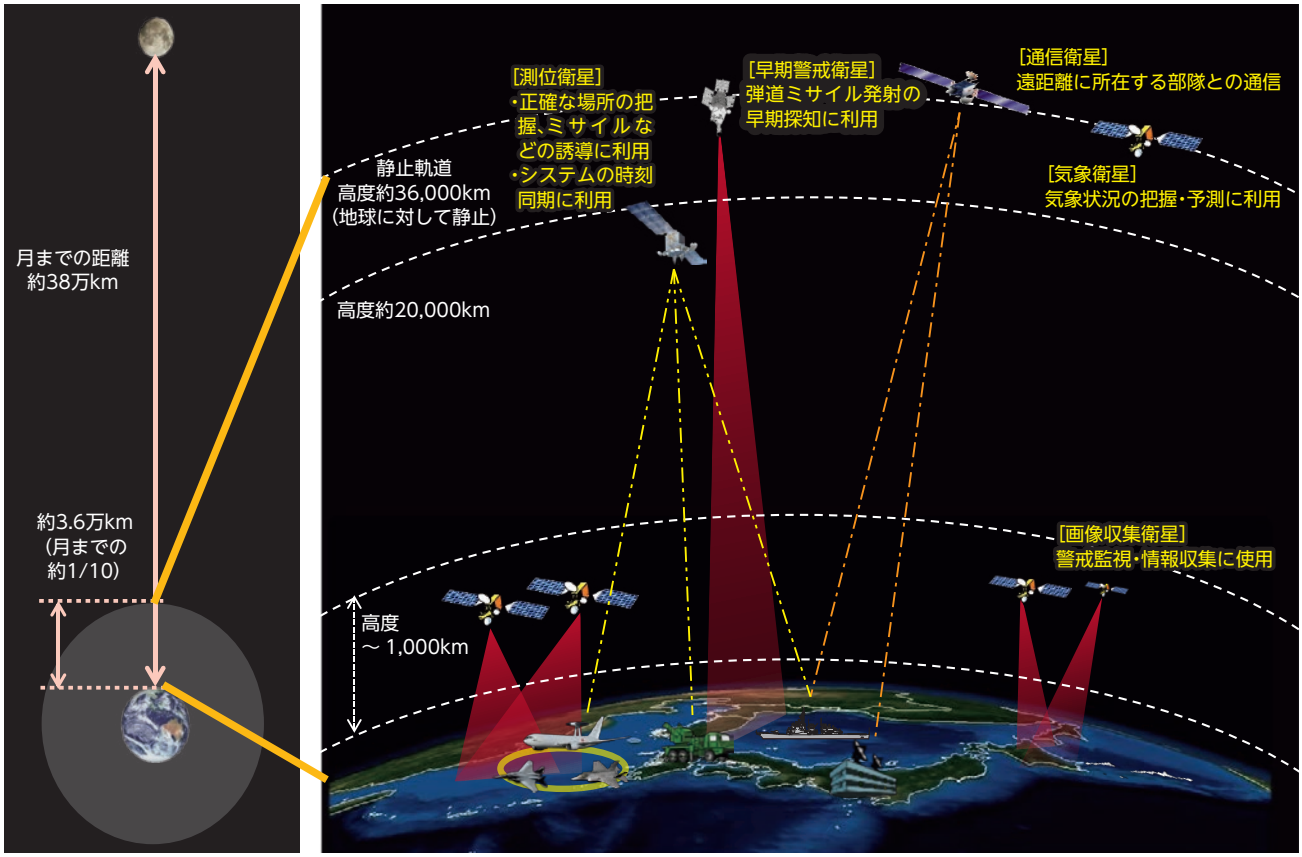
情報収集、通信、測位などのための人工衛星の活用は領域横断（クロス・ドメイン）作戦の実現に不可欠である一方、宇宙空間の安定的利用に対する脅威は増大している。

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能力や指揮統制・情報通信能力の強化、宇宙状況監視の取組などを通じて、効果的・安定的な宇宙空間の利用確保に努めてきたが、今後は、これまでの取組に加え、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

Space Situational Awareness

1　16（平成28）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。

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



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ている。

また、こうした取組に際しては、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ることとしている。令和2（2020）年度においては、宇宙領域における統合運用にかかる企画立案機能を担う組織として、統合幕僚監部に「宇宙領域企画班（仮称）」を新設することとしている。

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）体制の構築

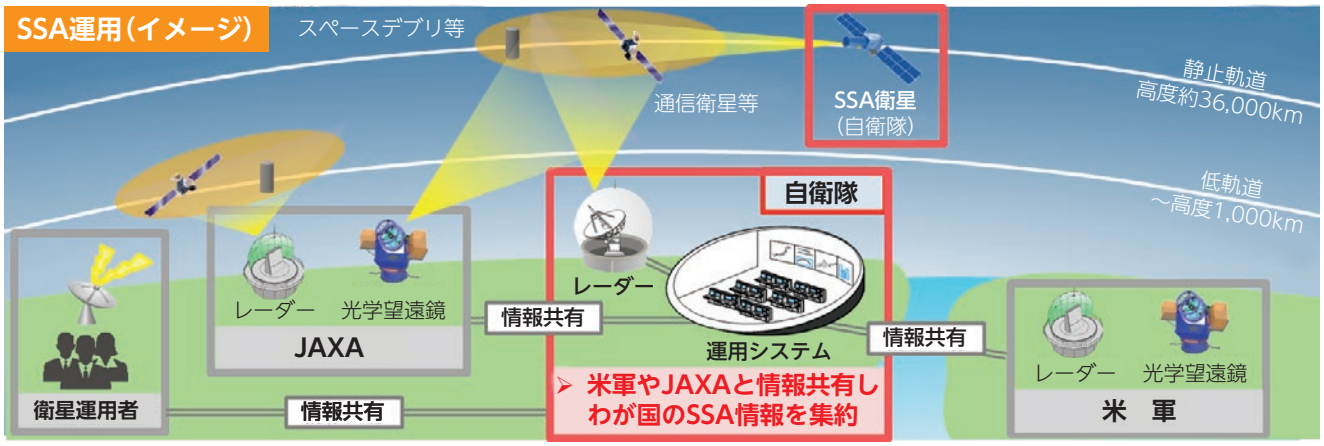
宇宙空間を利用するにあたっては、その安定的な利用を確保する必要がある。しかしながら、宇宙空間において、宇宙ゴミ（スペースデブリ）が急激に増加しており、スペースデブリと人工衛星が衝突して衛星の機能が著しく損われる危険性が増大している。

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、宇宙空間の安定的利用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などの国内関係機関や米国と連携しつつ、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）体制を令和4（2022）年度までに構築することを目指しており、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ための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る。また、空自において、それらを運用する宇宙領域専門部隊として宇宙作戦隊を20（令和2）年5月に新編し、本格的なSSAの運用開始や装備品の導入に先立って、①宇宙領域にかかる部隊運用の検討、②宇宙領域の知見を持つ人材の育成、③JAXAや米国などとの連携体制の構築などを進めている。

その際、関係政府機関などが一体となった効果

図表Ⅲ-1-3-2　宇宙状況監視（SSA）体制構築に向けた取組



的な運用体制を構築していく必要がある。この点、JAXAは、低高度周回軌道（高度1,000km以下）を監視する能力を有するレーダー及び静止軌道（高度約3万6,000km）を監視する能力を有する光学望遠鏡を整備する計画を進めており、防衛省が整備する主として静止軌道を監視する能力を有するレーダーと合わせ、わが国として効率良く宇宙空間を監視する体制が整う計画となっている。また、運用システムについては、令和4（2022）年度までに、JAXAに加え、米軍のシステムとも連接するよう、必要な調整を進めている。

さらに、今後は、前述の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ためのレーダーに加えて、相互補完的な監視を可能とする宇宙設置型光学望遠鏡であるSSA衛星や、低軌道の人工衛星との距離を計測する地上設置型SSAレーザー測距装置を導入することとしており、令和2（2020）年度予算においては、SSA衛星の構成品の取得に必要な経費を計上した。

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）

河野防衛大臣から隊旗を授与される宇宙作戦隊長（20（令和2）年5月）

(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、防衛省・自衛隊が任務を効果的かつ効率的に遂行していくためには、これらの各種能力をさらに充実させる必要がある。

このため、情報収集・警戒監視については、情報収集衛星（IGS）、超小型衛星を含む商用衛星などの利用による衛星画像の重層的な取得を通じ、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、2波長赤外線センサの研究[2]を行っていくこととしている。

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、17（平成29）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、18（平成30）年4月には「きらめき1号」を打ち上げた。今後、将来の通信所要などの増大を踏まえ、通信の統合化や高速・大容量化を図るため、「きらめき3号」の着実な整備を進め、Xバン

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。

VOICE JAXA派遣要員としての活動について

宇宙航空研究開発機構（JAXA）
筑波宇宙センター追跡ネットワーク技術センター
航空幕僚監部　防衛部防衛課
3等空佐　齋藤（さいとう） 拓也（たくや）

「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。」19（令和元）年9月、防衛省市ヶ谷基地において安倍内閣総理大臣が発言されました。

私は、JAXA筑波宇宙センターにおいて航空自衛官として勤務しています。もっとも大先輩である元航空自衛官の油井宇宙飛行士のような宇宙飛行士を目指してJAXAで勤務しているわけではありません。

地球を周回するスペースデブリと呼ばれる不要な人工物体は、ソフトボールサイズ以上のものでも約2万個弱あると言われています。我々の生活に密接に関係する測位・通信・放送・気象などの人工衛星がスペースデブリと衝突しないようにするためにも、宇宙で「今、何が起こっているのか」を把握する能力（SSA）が必要になります。
Space Situational Awareness

現在防衛省は、宇宙などの新たな領域における能力の獲得・強化に取り組んでおり、航空自衛隊は、JAXAと連携したSSA運用体制の構築に向けて整備

JAXA職員との会議でSSAシステムの教育を受ける著者（右から2人目）

を進めております。私は、そのような運用体制を実現すべく、JAXAにおいてSSAにかかる専門的知見を学びつつ、防衛省とJAXAとのデータ共有や具体的な連携要領にかかる調整などを行っています。

航空自衛隊では、宇宙領域を専門とする職種も新設され、宇宙にかかる人材の育成・確保も必須になっていきます。本記事を読み、我こそはと心を熱くされた方は、私と一緒に宇宙人へと進化してみませんか？「ワレワレハ、コウクウウチュウジンダ！」

ド防衛通信衛星全3機体制の早期実現を目指すとともに、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、これまで、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きた。これに加え、18（平成30）年11月より、内閣府の準天頂衛星[3]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活用により、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、一部の諸外国が、キラー衛星や衛星攻撃ミサイル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、Xバンド防衛通信衛星などの人工衛星の抗たん性を向上させる必要がある。

このため、わが国の人工衛星の脆弱性への対応を検討・演練するための訓練用装置や、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を新たに導入することとしており、令和2（2020）年度予算には、電磁妨害状況を把握する装置の取得に必要な経費を計上した。

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。

(4) 関係機関や米国などの関係国との連携強化

防衛省が宇宙開発利用を効果的に推進していく

3 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。

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。

現在、防衛省とJAXAの間では、前述のSSAの整備や2波長赤外線センサの実証研究などにおける連携協力のほか、航空自衛官を筑波宇宙センターに派遣するなどの人材交流も行っている。

また、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、15（平成27）年4月には、「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6回の会合を開催した。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推進している。

Space Cooperation Working Group

こうした取組の一環として、防衛省は、米戦略軍主催のSSA多国間机上演習「グローバル・センチネル」に16（平成28）年から毎年参加しており、SSA運用にかかる知見を修得するとともに、

グローバル・センチネル19に参加する空自隊員（19（令和元）年9月）

今後の米国などとの協力強化を図っている。こうしたSSA能力の向上の取組は、宇宙空間における新たな脅威に対する抑止力の向上にも寄与するものである。なお、米国以外では、フランス、EU及びインドなどとの間で宇宙対話などにも取り組んでいる。

参照　3章3節1項（宇宙領域の利用にかかる協力）

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、平成30（2018）年度に政府機関に対する不審な通信として検知されたもののうち、対処の要否について確認を要する事象が、マルウェア感染の疑いは111件、標的型攻撃は66件検知されるなど、引き続き十分な警戒を要する状況である[4]。

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、14（平成26）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た。

これを受けて、15（平成27）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）[5]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。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、18（平成30）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

National center of Incident readiness and Strategy for Cybersecurity

4 「サイバーセキュリティ2019」（19（令和元）年5月23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、15（平成27）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。

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、これまでも、情報通信システムの安全性を確保するための侵入防止システムなどの導入及びサイバー防護分析装置などの防護システムの整備、自衛隊指揮通信システム隊などによる24時間態勢での通信ネットワークの監視やサイバー攻撃[6]への対処、サイバー攻撃対処に関する態勢や要領を定めた規則[7]の整備、最新技術の研究、人材育成、他機関などとの連携など、総合的な施策を行ってきた。

今後は、これまでの取組に加え、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

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

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

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

7 防衛省の情報保証に関する訓令（平成19年防衛省訓令第160号）などがある。

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　サイバー防衛隊などの体制拡充

サイバー防衛隊については、14（平成26）年3月に、自衛隊指揮通信システム隊のもとに新編した後、日々高度化・巧妙化するサイバー攻撃に適切に対応するため、体制の強化を図ってきたところであり、令和2（2020）年度に、サイバー防衛隊をさらに約70名増員し、約290名へと拡充することとしている。

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などの革新技術を活用したサイバー防護分析装置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。

(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、13（平成25）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社程度をコアメンバーとする「サイバーディフェンス連携協議会」（CDC）を設置し、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おり、今後は更に連携の拡大を図ることとしている。

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、防衛当局間の枠組みとして「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。また、15（平成27）年5月には今後の具体的な協力の方向性を示した共同声明を発表した。

また、日米両政府全体の取組である「日米サイバー対話」への参加や、02（平成14）年より議論を重ねてきた、防衛当局間の枠組みである「日米ITフォーラム」の開催、米陸軍のサイバー教育機関への連絡官の派遣を通じ、米国との連携強化を一層推進していくこととしている。

ウ　その他の国などとの協力

防衛省においては、英国、NATOなどとの間で、防衛当局間によるサイバー協議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ている。19（令和元）年12月には、NATO主催のサイバー防衛演習「サイバー・コアリション2019」に初めて正式参加し、NATOとの連携・協力の向上を図った。また、シンガポール、ベトナムなどの防衛当局間で、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）

(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、令和元（2019）年度からサイバー

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課程[8]を実施している。令和２（2020）年度予算においては、米国防大学などのサイバー戦指揮官要員課程への隊員の派遣をはじめとする国内外の大学などへの留学や高度サイバー人材を発掘するための民間人を対象としたサイバーコンテストの開催に必要な経費などを計上した。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[9]、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くこととしている。

(4) 政府全体としての取組への寄与

防衛省は、警察庁、総務省、経済産業省、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）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[10]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[11]。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[12]。

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、令和２（2020）年度予算においては、電子戦などを効果的に遂行できるよう、電磁波の利用状況を把握し、可視化に資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くこととしている。

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。

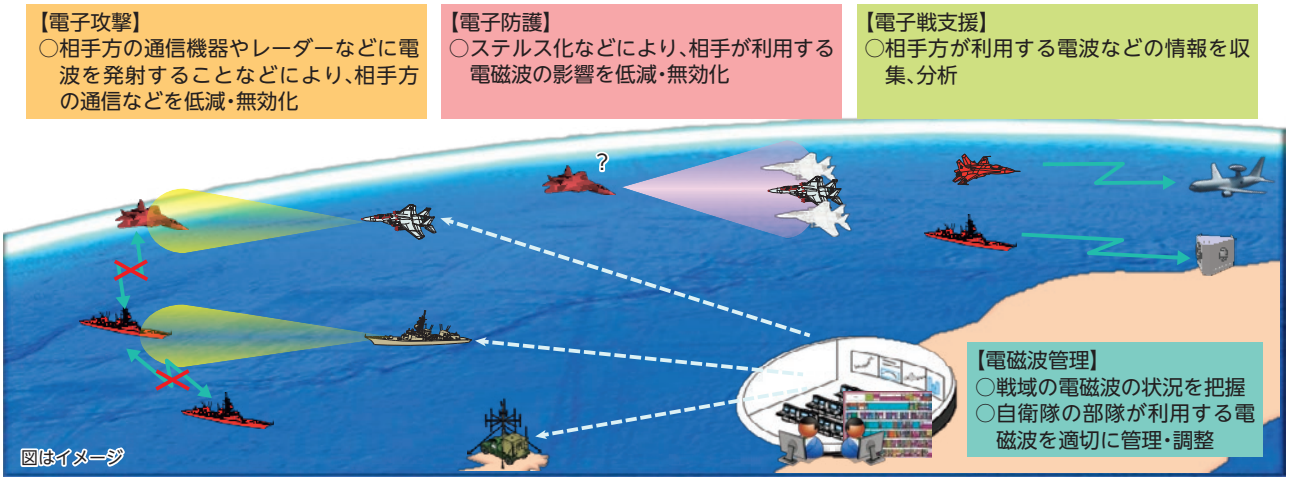
このため、陸上総隊隷下に電磁波に関する情報収集などを行う電磁波作戦部隊を新編するほか、

8 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
9 政府の「サイバーセキュリティ人材育成総合強化方針」（16（平成28）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
10 電波や赤外線、可視光線などの総称。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。
11 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。
12 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

電子戦能力：相手方による電磁波の利用・効果を妨げつつ、味方による電磁波の利用・効果を確保するといった電磁波を効果的・積極的に利用して行う戦闘（電子戦（※））の能力
電磁波管理能力：「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味方による電磁波の利用を適切に管理・調整する能力

（※）電子戦は、一般に「電子攻撃」「電子防護」「電子戦支援」に分類される。



令和２（2020）年度予算においては、艦艇用の電波情報収集機器の能力向上に向けた研究を実施するなど、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）[13]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、令和２（2020）年度予算においては、自己防御用の電子妨害／防護能力に優れた戦闘機（F-35A/B）の整備やネットワーク電子戦装置の整備を行うとともに、戦闘機（F-15）への新たな電子戦装置の搭載などの能力向上、妨害対象の脅威の対処可能圏外から電波妨害を行うスタンド・オフ電子戦機の開発や対空電子戦装置の研究を進めることとしている。また、多数の無人機（ドローン）などを瞬間的に無力化できる高出力マイクロ波、無人機（ドローン）や迫撃砲弾といった脅威に、低コストかつ低リアクションタイムで対処する高出力レーザーなどゲーム・チェンジャーとなり得る技術の導入に向けた調査や研究開発を迅速に進めていくこととしている。

4　訓練演習、人材育成

自衛隊の電磁波領域の能力強化のためには訓練・演習や教育の充実も重要である。

令和２（2020）年度予算においては、平素からの訓練・演習や教育に加え、空自が使用する電子戦教育装置の換装に着手するほか、空自の要員を米国の電子戦教育課程へ昨年に引き続き派遣することとしている。

13　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。