第3節 新しい戦い方を支える各種領域や先端技術の動向

1 宇宙領域をめぐる動向

1 宇宙領域と安全保障

宇宙空間は、国境の概念がないことから、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、測位などが可能となる。

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る。

一方、他国の宇宙利用を妨げる対衛星兵器（ASAT：Anti-SATellite Weapons）も開発されている。

破壊的な直接上昇型対衛星（DA-ASAT：Direct-Ascent Anti-SATellite）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。この結果、スペースデブリが多数発生し、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る。

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る[1]。

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る。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る。

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：Space Domain Awareness）に取り組んでいる。

こうしたなか、国際的なルール作りについては、国連において、平和利用や軍備競争防止の観点から、国連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が行われている。

このほか、同志国間の取組として、「連合宇宙作戦（シースポ）（CSpO：Combined Space Operations）イニシアチブ」がある。これは、宇宙の安全保障に必要な政策・運用・体制・法的な課題などに関する各種議論を実施する多国間枠組みであり、現在わが国を含め10か国が参加している。

参照　Ⅲ部1章1節1項4（宇宙領域における対応）、Ⅲ部1章2節4項1（宇宙領域）

2 宇宙空間に関する各国の取組

(1) 米国

米国は、世界初の偵察衛星、月面着陸など、軍事、科学、資源探査など多種多様な宇宙活動を発展させ続けており、世界最大の宇宙大国である。米軍においても、宇宙空間の重要性は強く認識され、宇宙空間を積極的に利用している。

2023年には、衛星打上げ能力の即応性向上のため、衛星のペイロード搭載から運用までの工期短縮を実証している。また、極超音速兵器を含めたミサイル脅威に対して、宇宙から探知・追尾する衛星コンステレーション「PWSA」の構築のため、多数の衛星を打ち上げている。

政策面では、米国の第2期トランプ政権は、成立直後の2025年1月、「米国のためのアイアン・ドーム[2]」と題する大統領令を発出し、宇宙アセットを活用したミサイル防衛システムの構築やそれに向けた設計・計画に関する報告書の提出を関係省庁に指示した。同年12月には、「米国の宇宙優勢の確保」と題する大統領令を発出し、2028年までの月面への帰還などと並び、宇宙における

1　米国防情報局「Challenges to Security in Space」（2022年）による。
2　本大統領令では「米国のためのアイアン・ドーム（Iron Dome for America）」との表記であるが、のち「米国のためのゴールデン・ドーム（GDA：Golden Dome for America）」と呼称されるようになった。

米国の安全保障および経済安全保障のため、各種の目標を掲げている。具体的には、大統領令「米国のためのアイアン・ドーム」に基づく次世代ミサイル防衛技術の同年までの開発・実証、宇宙空間への核兵器配備を含め、超低高度軌道以上にある米国への脅威の探知・分類・対処、商用部門の能力も取り込んだ調達改革の推進による国家安全保障にかかる宇宙構想の策定、米国および同盟国などによる集団的な宇宙安全保障の強化を目指すとした。また、米国の防空ミサイル防衛を強化するにあたっての技術上およびサプライチェーン上のギャップの90日以内の特定と改善計画の策定、180日以内の宇宙にかかる安全保障戦略の策定を関係省庁に指示した。

これらの政策に基づき、米戦争省は2025年5月、「ゴールデン・ドーム」整備計画を発表し、大気圏内外で発射された極超音速・弾道・発展型巡航ミサイルのいずれも撃墜可能なシステムとして、宇宙設置型の迎撃システムとセンサーを含み、既存の迎撃システムとも相互運用性を持つ形で統合されたシステムを、3年以内に運用可能とするとした。

また、同年11月には、中国およびロシアの情報収集・警戒監視・偵察衛星を電波妨害するための新たな兵器を世界各地に分散して配備すると発表している。

組織面では、2019年、宇宙の任務を担っていた戦略軍の一部を基盤に新たな地域別統合軍として宇宙コマンドが発足したほか、6番目の軍種として、空軍省の隷下に人員約1万6,000人規模の宇宙軍を創設した。また、商用サービスの利用促進のため、宇宙コマンドに利用を調整する部署や、宇宙軍に産官学連携を支援する部署を設置している。

2023年12月には宇宙コマンドが完全な作戦能力に達したことが宣言され、2024年10月の国防省公表では、宇宙コマンド司令官の任務に、他の統合軍、省庁、軍種および同盟国などと連携した攻勢的・防勢的宇宙作戦の同期や衝突回避などの任務が追加された[3]。また、2025年11月には、前述の電波妨害のための兵器配備に関する発表と合わせて、宇宙軍は、妨害作戦を統括・調整する「宇宙電磁戦術作戦センター」を新設した。

参照　3章1節2項（軍事態勢）

(2) 中国

中国は、1950年代から宇宙開発を推進しており、自国のC4ISR・ターゲティング能力を強化する宇宙システムに投資している。近年では、宇宙ステーション「天宮」の完成、月面基地計画の推進など、宇宙活動をさらに活発化させている。2024年には、低軌道インターネット衛星群「国網」や「千帆星座」の打上げが開始されるなど、迅速な情報収集・通信のための衛星コンステレーション構築に向けた取組が加速している。中国は、1,000基以上の衛星を保有しており、2030年までに数千基打ち上げる計画であるほか、こうした衛星群をメガコンステレーションとして展開し、グローバルなインターネットのプロバイダーとしてスターリンクと競合することを目指している旨指摘されている[4]。

さらに、2024年6月には、無人月面探査機「嫦娥6号」が史上初となる月の裏側からの試料採取および帰還に成功するなど、月開発の分野での取組も進んでいる。

中国は従来から国際協力や宇宙の平和利用を強調しているものの、衛星による情報収集、通信、測位など軍事目的での宇宙利用を積極的に行っていることが指摘されている。例えば、「北斗」は航空機、艦船の航法、ミサイルなどの誘導、「遥感」は電子偵察や画像偵察として、軍事利用の可能性が指摘されている。

2025年5月、宇宙でAI（Artificial Intelligence）計算基盤を構築し、軌道上でのデータ処理を目的とする「三体計算コンステレーション」の一環で、世界初の宇宙演算衛星12機を打ち上げた旨発表された。この衛星は光通信および分散機能により、軌道上で収集データを処理し、その結果を地上に直接送信するもので、最終的に2,800基の打上げを目指している。

また、中国は、地域紛争への米国介入を抑止・対抗する手段として対宇宙作戦を捉えていると指摘されており[5]、ASATの開発などを進めている。すでに、静止軌道上の「実践21号」など、軌道上の他の衛星の妨害または破壊が可能な複数の衛星を配備している。

このほか、地上配備型レーザー、軌道周回型宇宙ロボットなど様々なASAT能力と関連技術の取得、開発を続けているとの指摘もある[6]。

3　米国防省指令3100.10
4　米国防情報局「2025年世界脅威評価」による。
5　米戦争省「中華人民共和国の軍事および安全保障の進展に関する年次報告」（2025年）による。
6　米戦争省「中華人民共和国の軍事および安全保障の進展に関する年次報告」（2025年）による。

このように中国は、今後も宇宙開発に注力していくものとみられる。米国は中国に対し、宇宙における米国の能力に並ぶまたは上回る能力を追求していると評価[7]しており、軍用衛星の運用数は米国を上回っているとの指摘もある[8]。

政策面では、中国は、宇宙が国際的戦略競争の要点であり、宇宙の安全は国家建設や社会発展の戦略的保障であると主張しており、航空宇宙分野の発展を加速する方針を明らかにしている。2024年には、中国科学院、中国国家航天局および中国有人宇宙事業弁公室が「国家宇宙科学中長期開発計画」を発表し、2027年、2035年、2050年と3段階を経て宇宙分野で世界をリードするという方針とそれに向けたロードマップを打ち出した。

組織面では、2024年に従来の戦略支援部隊が廃止され、その隷下部隊が軍事宇宙部隊およびサイバー空間部隊に改編されたとの指摘がある。同年以前の戦略支援部隊は、宇宙・サイバー・電子戦を任務としていたとされている。

(3) ロシア

1991年の旧ソ連解体以降、ロシアの宇宙活動は低調な状態にあったが、近年は、ウクライナ侵略後も、活発な宇宙活動を継続している。例えば、ロシアは、「コスモス」シリーズをはじめとした多数の各種衛星や国際宇宙ステーション（ISS）への補給船「プログレス」シリーズの打上げを継続している。また、独自の宇宙ステーションの開発計画を明らかにしており、2028年から2033年までにかけ、各モジュールの打上げを予定している。

なお、ASATに関して、米国政府は、2024年にロシアが打ち上げた衛星「コスモス2576」について、他の衛星を攻撃できる能力を備えた対宇宙兵器であると評価している。また、ロシアが核兵器を搭載した対衛星システムの宇宙配備に向けた計画を進めているとの指摘もあるが、ロシア政府はこれを否定している。

政策面では、宇宙活動を展開していく今後の具体的な方針として、2016年、「2016-2025年のロシア連邦宇宙プログラム」を発表し、国産宇宙衛星の開発・展開、有人宇宙飛行計画などを盛り込んだ。2023年には、「2035年までの通信産業発展戦略」において、2030年までにインターネット通信用の衛星コンステレーションを構築する目標を打ち出した。

組織面では、国営企業であるロスコスモスがロシアの科学分野や経済分野の宇宙活動を担う一方で、国防省が安全保障目的での宇宙活動に関与し、2015年に空軍と航空宇宙防衛部隊が統合されて創設された航空宇宙軍が、実際の軍事面での宇宙活動や衛星打上げ施設の管理などを担当している。

(4) 北朝鮮

2023年、北朝鮮は、「偵察衛星」と称する「万里鏡1」の打上げに成功し、運用を開始したと主張した。そのうえで、北朝鮮は、2024年の目標として3基の追加打上げに言及していたが、同年5月に強行された衛星打上げを目的とする弾道ミサイル技術を使用した発射は失敗したものとみられ、それ以降、追加の発射は確認されていない。

組織面では、2023年、これまでロケットや衛星の開発などを担当してきた国家宇宙開発局を国家航空宇宙技術総局に改編した。また、国家航空宇宙技術総局平壌総合管制所に軍事情報組織である偵察衛星運営室が存在し、偵察衛星によって得られた情報を党中央軍事委員会に報告し、中央軍事委員会の指示に従って軍の重要部隊や偵察情報総局に提供するものとしている。

(5) 韓国

韓国の宇宙開発は、2005年に施行された「宇宙開発振興法」のもと、2022年に発表した「第4次宇宙開発振興基本計画」に基づき推進されている。その計画は、宇宙関連予算の倍増、宇宙産業の推進などを目標としている。

韓国国防部は、軍事偵察衛星の取得を通じて朝鮮半島に対する監視能力を強化するとしている[9]。2023年12月には、韓国軍初の軍事偵察衛星が米国で打ち上げられ、2025年11月までに計5基の打上げが完了した。現在、韓国軍が保有する偵察衛星5基のうち、3基が運用中であり、残り2基は試験運用中である。

組織面では、2024年に宇宙政策・事業の分野拡大および宇宙の商業利用の増加に伴い、宇宙航空庁が発足

7　米国防情報局「2025年世界脅威評価」による。
8　米国防情報局「2025年世界脅威評価」による。
9　韓国国防部「2022国防白書」（2023年）による。

し、航空宇宙にかかる政策の策定や官民の調整などを担うこととなった。宇宙空間における安全保障については、国家レベルの体系的・総合的な対応のため、韓国国家情報院が国家宇宙安全保障センターを運営している。また、同年6月には、朝鮮半島周辺で活動する衛星および宇宙物体を分析し、宇宙アセットを保護する役割を担っていた韓国空軍傘下の「宇宙作戦大隊」が「宇宙作戦戦隊」に拡大改編された。

(6) インド

インドは、自国周辺の測位を目的とした地域航法衛星システム「NavIC」を運用しているほか、2023年には、無人月面探査機「チャンドラヤーン3号」が世界で初めて月の南極域への着陸に成功するなど、高い技術力を有している。2025年6月には、インド空軍所属の宇宙飛行士がインド人初の国際宇宙ステーション（ISS）での活動を実施した。

また、インドは月面サンプルを収集し地球に持ち帰ることを目指す新たな無人月面探査船「チャンドラヤーン4号」の計画や独自の宇宙ステーションの建設計画を発表するなど、今後も宇宙開発を推進していくものとみられる。

加えて、インドは、2024年10月に、今後10年以内に低軌道および静止軌道に少なくとも52基の衛星を打ち上げるとする宇宙基盤監視プロジェクト「SBS」の第3段階を承認したほか、同年11月にはインド国防宇宙局主催の宇宙演習「アンタリクシャ・アビヤス」を実施するなど、宇宙能力の国防への統合を進めている。

また、インドは、宇宙分野における二国間協力も推進しており、米国との関係強化の取組のほか、ロシアとの間でも、2025年12月に実施した印露首脳会談後に発表した共同声明のなかで、有人宇宙飛行計画、衛星航法および惑星探査を含む宇宙分野におけるパートナーシップの強化を歓迎している。

(7) 欧州

EUは、2021年から2027年までの中期予算計画の宇宙政策に148.8億ユーロを割り当て、宇宙産業の促進と安全保障の強化のため、先進的で強靱な測位・航法・タイミング（PNT）の確保、正確な地球観測、宇宙監視・追跡能力の強化、安全な衛星通信サービスの持続的な利用に向けた取組などを推進している。2023年には、EU宇宙安全保障・防衛戦略を公表し、安全保障・防衛における宇宙能力の利用を強化するとし、新しい地球観測サービスの開発や初期のSDAサービスの提供を計画している。

NATOは、宇宙を陸・海・空・サイバーと並ぶ第5の作戦領域であるとし、宇宙における武力攻撃がNATOの集団的自衛権の発動につながりうるとの認識を示し、2022年に公表した新戦略概念では、宇宙とサイバー領域で効果的に活動する能力を強化するとしている。2024年10月には、NATOの一部加盟国は、北極圏に軍事衛星通信ネットワークを構築する計画「ノースリンク構想」の推進や、ロケット打上げの能力確保に取り組むための計画「スターリフト構想」の開始に合意している。

英国は、2022年に発表した国防宇宙戦略において、ISRや衛星通信などの分野に今後10年で14億ポンドを投資するとしている。また、2021年に正式に発足した宇宙コマンドは、2024年に同コマンド初となる情報収集衛星「テュケ」の打上げに成功している。

フランスは、2019年に国防宇宙戦略を発表し、宇宙コマンドの創設、脅威認識・宇宙状況監視能力の強化などを目指すとした。同年に空軍隷下に宇宙司令部を創設したほか、2020年には、空軍を航空・宇宙軍に改称し、宇宙への自由なアクセス、宇宙空間での行動の自由を保障するための活動を業務に追加している。また、2026年4月に更新した「2024年-2030年の軍事計画法」では、2030年までの宇宙分野の国防予算を39億ユーロ増額し、通信接続性および強じん性の増強、情報収集手段の強化、宇宙空間内や宇宙空間に向けた行動能力の加速・拡大などを目指すとしている。

2 サイバー領域をめぐる動向

1 サイバー空間と安全保障

サイバー空間は、インターネットをはじめとする様々なサービスやコミュニティで形成された、新たな社会領域空間として重要性を増している。このため、サイバー空間上の情報資産やネットワークを侵害するサイバー攻撃は、社会に深刻な影響を及ぼすことが可能であり、安全保障上の現実の脅威となっている。

また、典型的なサイバー攻撃としては、不正アクセス、マルウェア（不正プログラム）による情報流出や電子計算機の機能妨害、情報の改ざん・窃取、大量のデータの同時送信による機能妨害（DDoS攻撃）などがあげられる。電力システムや医療システムなどの重要インフラが狙われた場合、システム障害などの被害をもたらすこともある。さらに、攻撃手法が高度化、巧妙化しており、AIを利用した、人間には不可能な高速度かつ高度なサイバー攻撃の可能性も指摘されている。

軍隊にとっても、サイバー空間は、指揮中枢から末端部隊に至る指揮統制のための基盤や、無人航空機などの無人アセットや重要インフラを運用する基盤となるなど、多くの分野で必要不可欠な要素となっており、サイバー空間への依存度が増大している。このような基盤へのサイバー攻撃は、平時に加え、航空侵攻・海上侵攻・着上陸侵攻といった伝統的な態様の侵攻に先立って行われる可能性が高く、サイバー領域における脅威には迅速かつ的確に対応する必要がある。また、サイバー攻撃は兵器を必要とせず、攻撃主体の特定や被害の把握が容易ではないことから、敵の軍事活動を低コストで妨害できる非対称な攻撃手段として認識されており、多くの国がサイバー攻撃能力を構築・強化しているとみられる。

2 サイバー空間における脅威の動向

諸外国の政府機関や軍隊のみならず民間企業や学術機関などに対するサイバー攻撃が多発しており、重要技術、機密情報、個人情報などが標的となっている。また、高度標的型サイバー攻撃（APT）は、洗練された手法で特定の組織を執拗に攻撃するサイバー攻撃とされ、こうした攻撃には長期的な活動を行うための潤沢なリソース、体制や能力が必要となることから、組織的活動であるとされる。こうしたなか、英国は、「現実的かつ継続的な脅威」として、中国、ロシア、北朝鮮、イランによるサイバー攻撃をあげている[10]。

(1) 中国

中国では、これまで、サイバー戦の任務を担う部隊は戦略支援部隊のもとに編成されていたとみられてきたが、この戦略支援部隊は2024年に廃止され、その隷下であったサイバー空間部隊が兵種に格上げされたとの指摘がある。台湾は中国のサイバー攻撃の手法について、ハードウェアやソフトウェアの脆弱性に対する攻撃、DDoS攻撃、ソーシャル・エンジニアリングなどの手法を組み合わせ、基幹インフラのネットワークへの侵入を試みていること[11]、台湾におけるインターネットを基盤とした物流、指揮統制、通信、商業活動および軍事インフラなどを標的としてサイバー攻撃を仕掛け、活動を妨害することなどを指摘している[12]。また、中国が2019年に発表した国防白書「新時代における中国の国防」において、軍によるサイバー空間における能力構築を加速させるとしているなど、軍のサイバー戦能力を強化していると考えられる。

参照 図表Ⅰ-4-3-1（中国のAPTグループ）、3章2節2項5（軍事態勢）

10 英国国家サイバーセキュリティセンター「年次レビュー2024」（2024年）による。
11 台湾国家安全局「2025年中国共産党の我が国基幹インフラネットワークに対する脅威分析」による。
12 台湾国防部「国防報告書」（2025年）による。

図表Ⅰ-4-3-1　中国のAPTグループ

グループ名	関連が指摘される機関など	グループの特徴・主なサイバー攻撃事例
Salt Typhoon	中国政府	【特徴】情報領域における優位性を確立するために、米国およびその同盟国に対して広範なサイバー攻撃を継続 【主なサイバー攻撃事例】2025年12月、米戦争省は、2024年秋頃にSalt Typhoonが、米国の複数の通信事業者に対して大規模なサイバー諜報作戦を実施したと発表
Volt Typhoon	中国政府	【特徴】米国の通信、エネルギー、運輸および水道分野などの重要インフラ事業者への侵害が確認されており、有事の際に重要インフラに対するサイバー攻撃を行うため、事前に重要インフラ事業者などのネットワークへのアクセス権限を確保している旨指摘あり 【主なサイバー攻撃事例】2025年12月、米戦争省は、2024年においてもVolt Typhoonが米国の重要インフラに深く侵入したと発表。重要インフラへの侵入のほかにも、サイバー諜報活動を通じた米軍の作戦上の機密情報の窃取により、有事における米国の台湾への支援の弱体化を目的としている可能性があるとの指摘あり
Flax Typhoon	中国政府	【特徴】主に台湾を標的として、一般的な脆弱性を悪用して被害者のコンピュータへの初期アクセスを獲得後、正規のリモートアクセスソフトウェアを利用して、ネットワークに対する継続的なアクセスを維持 【主なサイバー攻撃事例】2024年9月、米司法省は、米国および世界中の20万台以上の一般向けデバイスで構成されるボットネットを摘発。Flax Typhoonが運用していた旨発表

（注）米戦争省「中華人民共和国の軍事および安全保障の進展に関する年次報告」（2025年）などによる。

(2) ロシア

ロシアについては、軍参謀本部情報総局、連邦保安庁、対外情報庁がサイバー攻撃に関与しているとの指摘があるほか、軍のサイバー部隊[13]の存在が明らかとなっている。サイバー部隊は、敵の指揮・統制システムへのマルウェアの挿入を含む攻撃的なサイバー活動を担うとされ、その要員は約1,000人と指摘されている[14]。

また、2021年に公表した国家安全保障戦略において、宇宙・情報空間は、軍事活動の新たな領域として活発に開発されているとの認識を示し、情報空間におけるロシアの主権の強化を国家の優先課題として掲げている。

ロシアは、スパイ活動、影響力行使、攻撃に関する能力を向上させているとされ[15]、2025年12月、米FBI、国土安全保障省サイバーセキュリティ・インフラセキュリティ庁（CISA）、国家安全保障局（NSA）は、親ロシア派ハクティビスト[16]が、スパイ活動、破壊工作、風評被害を与えることを目的として、世界の標的に対してコンピュータ・ネットワーク上で活動を行っているとして注意喚起している[17]。こうしたハクティビストの一部はロシア政府とのつながりが指摘されている。

参照　図表Ⅰ-4-3-2（ロシアのAPTグループ）

13 2017年2月、ロシアのショイグ国防相（当時）の下院の説明会での発言による。ロシア軍に「情報作戦部隊」が存在するとし、欧米との情報戦が起きており「政治宣伝活動に対抗する」としている。ただし、ショイグ国防相は部隊名の言及はしていない。
14 戦略国際問題研究所「A Playbook for Winning the Cyber war」（2025年9月）による。
15 米国防省「サイバー戦略2023」（2023年）による。
16 ハッカーとアクティビストを掛け合わせた造語。
17 米国土安全保障省サイバーセキュリティ・インフラセキュリティ庁「JOINT CYBERSECURITY ADVISORY」（2025年12月）による。

図表Ⅰ-4-3-2　ロシアのAPTグループ

グループ名	関連が指摘される機関など	グループの特徴・主なサイバー攻撃事例
APT28 (Fancy Bear)	連邦軍参謀本部情報総局(GRU)	【特徴】世界中の脆弱なルーターを悪用し、軍事、政府、重要インフラに関する機密情報を傍受・窃取 【主なサイバー攻撃事例】2026年4月、米司法省とFBIは、APT28がDNS(Domain Name System)ハイジャック作戦※を容易にするために、乗っ取ったSOHO(Small Office Home Office)(小規模オフィス・ホームオフィス)ルーターのネットワークを無力化したことを発表 ※DNSハイジャック作戦：本来は書き換えられないドメインを不正に書き換え、アクセスしたユーザーを別のサイトに移動させる作戦。移動先のサイトでマルウェアなどを用いて情報を不正に窃取する。
APT29 (Cozy Bear)	対外情報庁(SVR)	【特徴】匿名性を保ち、検知されないことに重点を置いており、自身が発見されたと疑う場合は、痕跡を消すために破壊活動を実施 【主なサイバー攻撃事例】2024年10月、FBI、NSAなどの複数の組織は、SVRの脅威に関するセキュリティ勧告を発表。この勧告によれば、2023年にAPT29が、Microsoft Teamsアカウントとチャット機能を使用してテクニカルサポート組織を装ったフィッシングメールを送信し、ソーシャルエンジニアリングの手法を用いて送信先アカウントへのアクセス権を得ようとしたと発表
Berserk Bear	連邦保安庁(FSB)	【特徴】10年以上にわたり、世界中のネットワーク機器のうち、旧式の非暗号化規格を利用する機器を攻撃 【主なサイバー攻撃事例】2025年8月、FBIは、Berserk Bearが未修正の脆弱性を有するネットワーク機器を標的とし、米国および世界中の組織を広く攻撃していることを検知したと発表

(注) FBI「Russian GRU Exploiting Vulnerable Routers to Steal Sensitive Information」(2026年4月) などによる。

(3) 北朝鮮

北朝鮮には、軍偵察情報総局、国家情報局などの情報機関が存在しており、情報収集の主たる標的は韓国、米国とわが国であるとの指摘がある[18]。また、人材育成はこれらの機関が行っており、軍の偵察情報総局を中心に、サイバー部隊を集中的に増強し、約6,800人を運用中と指摘されている[19]。各種制裁措置が課せられている北朝鮮は、国際的な統制をかいくぐり、外貨を獲得するための手段としてサイバー攻撃や外国に派遣した北朝鮮IT労働者を利用しているとみられる[20]ほか、軍事機密情報の窃取や他国の重要インフラへの攻撃能力の開発などを行っているとされる。多国間制裁監視チーム(MSMT)(Multilateral Sanctions Monitoring Team)が2025年10月に発表した報告書においては、北朝鮮は、2024年1月から2025年9月までの間に少なくとも28億ドル相当の暗号資産を窃取したほか、2024年の外貨収入の約3分の1を暗号通貨窃取で獲得し、大量破壊兵器計画および弾道ミサイルの開発を促進していると指摘されている。また、暗号資産供給網を標的としたサプライチェーン攻撃や、諸外国の生成AIを活用したフィッシングメールやマルウェアの作成などを行ったと報告されている。

参照　図表Ⅰ-4-3-3 (北朝鮮のAPTグループ)

図表Ⅰ-4-3-3　北朝鮮のAPTグループ

グループ名	関連が指摘される機関など	グループの特徴・主なサイバー攻撃事例
APT37	国家保衛省	【特徴】北朝鮮脱北者コミュニティ、人権団体、韓国政府などを標的として諜報活動を実施 【主なサイバー攻撃事例】2024年5月、韓国当局者や北朝鮮関連NGOの代表者を標的として、インターネットのポップアップ広告の脆弱性を利用した大規模攻撃を実施
Lazarus Group	朝鮮人民軍 総参謀部 偵察情報総局	【特徴】暗号資産窃取をはじめ、収益獲得に重点を置いて活動を実施 【主なサイバー攻撃事例】2024年1月～2025年9月、同グループに属するとされるサイバー攻撃グループ「TraderTraitor」は、約25億8,000万ドル相当の暗号資産を窃取
APT43 (Kimsuky)		【特徴】韓国や米国の政府関係者などを標的として、ソーシャル・エンジニアリングを駆使した諜報活動を実施 【主なサイバー攻撃事例】2024年1月、韓国の建設業界団体のウェブサイトを通じてマルウェアを展開し、システム情報や認証情報などを窃取

(注) 多国間制裁監視チーム(MSMT)「第2回報告書」(2025年10月22日) による。

18　米国防情報局「北朝鮮の軍事力」(2021年) による。
19　韓国国防部「2022国防白書」(2023年) による。
20　米国防情報局「北朝鮮の軍事力」(2021年) による。

(4) イラン

イランにおけるサイバー攻撃の主体は、正規軍と連携し最高指導者の直接指揮下にある革命ガードおよび大統領の管轄下にある情報省（MOIS：Ministry of Intelligence and Security）による国家支援型のAPTグループと、政府から独立して活動するとされるハクティビストからなっているとみられる。これらのグループは、DDoS攻撃やウェブサイト改ざん、産業制御システムや運用技術を標的とした高度な破壊活動まで多岐にわたる攻撃を実施しているとされている。一般的に、ハクティビスト集団はAPTグループとは別に分類されているが、イランがサイバー作戦を拡大するなかで、イランのハクティビストは、APTグループが用いる戦術、手法などを模倣するようになっており、ツールおよび能力の共有や指揮統制関係などが指摘されている[21]。

ここ数年、米国の重要インフラに対するイランによるサイバー作戦がより頻繁に行われるようになっている。例えば、2023年10月に登場した、ガザにおけるイスラエルの行動に抗議する動機を持つハクティビストを自称する「サイバーアベンジャーズ」は、主にイスラエル製のインフラを標的としており、米国の上下水道に対する攻撃などを実施したとされている。

2024年3月、米環境保護局とNSAは、イラン革命ガードとの関連が指摘されるハッカー集団が産業制御システムに対してサイバー攻撃を行ったと注意喚起している。

また、2025年6月に発生したイランとの攻撃の応酬においても、イランによるサイバー攻撃が行われたとの指摘がある。

3 サイバー空間における脅威に対する動向

こうしたサイバー空間における脅威の増大を受け、各国で各種の取組が進められている。

米国や欧州、わが国などは、サイバー空間を自由、公正かつ安全なものとするため、既存の国際法の適用のあり方や規範の実践に関する議論を行う一方、ロシアや中国などは、新たな法的拘束力を持つ新条約の可能性を訴えており、見解の相違から、議論が継続している。国連では、全ての国連加盟国が参加する形で、2021年から5年間の会期で国連オープン・エンド作業部会（OEWG：Open Ended Working Group）が開催された。ここではサイバー空間における脅威認識、規範、国際法、信頼醸成措置など幅広い議論が行われ、2025年にOEWGの後継枠組みを含む最終報告書が提出され、国連総会で採択された。

参照　Ⅲ部1章1節1項5（サイバー領域における対応）、Ⅲ部1章2節4項2（サイバー領域）

(1) 米国

米国では、連邦政府のネットワークや重要インフラのサイバー防護に関しては、国土安全保障省が責任を有しており、CISAが政府機関のネットワーク防御に取り組んでいる。また、重要インフラなどに関する機微な情報の流出への対策として、2023年9月には、中国やロシアとのつながりが認められる企業によって設計、開発、製造および販売されたコネクテッドカー[22]の輸入を禁止する新たな規則案が示されている。

戦略面では、2026年3月にサイバー戦略を発表し、重要インフラの保護や防勢的・攻勢的なサイバー作戦により敵対勢力のネットワークを特定し、妨害し、攻撃を未然に阻止するとしている。また、連邦政府機関のサイバーセキュリティを強化するための「ゼロトラスト[23]戦略」を発表し、各省庁に対してゼロトラストモデルのセキュリティ対策を求めている。さらに、不足するサイバー人材を確保するため国家サイバー人材・教育戦略を発表し、国民の基本的サイバースキルの習得やサイバー教育の変革などに長期的に対処するとしている。

安全保障に関しては、国防省の「サイバー戦略2023」では、攻撃者の組織・能力・意図を追跡し、悪意のあるサイバー活動を妨害・劣化させて防御するほか、統合軍のサイバー領域での作戦を支援し、同盟国や関係国と協力して防御するとしている。その後、第2期トランプ政権における国家防衛戦略のなかで、戦争省は、米軍および特定の民間目標のためのサイバー防衛の強化を優先す

21 戦略国際問題研究所「Beyond Hacktivism：Iran's Coordinated Cyber Threat Landscape」（2026年1月）による。
22 ICT端末としての機能を有する自動車のことをさす。車両の状態や周囲の道路状況などの様々なデータをセンサーにより取得し、ネットワークを介して集積・分析することができる。米国政府によれば、コネクテッドカーは、車両の安全性の促進や運転手のナビゲーション支援といった利点を持つ一方で、収集された地理情報や重要インフラに関する機微な情報の悪用や自動車の運用の妨害といったリスクも有している。
23 「内部であっても信頼しない、外部も内部も区別なく疑ってかかる」という性悪説に基づいた考え方。利用者を疑い、端末などの機器を疑い、許されたアクセス権でも、なりすましなどの可能性が高い場合は動的にアクセス権を停止する。防御対象の中心はデータや機器などの資源。

るほか、米国本土へのサイバー脅威を抑止・弱体化させるためのその他の選択肢も開発するとしている。

なお、2019年の日米「2＋2」では、サイバー分野における協力を強化していくことで一致し、国際法がサイバー空間に適用されるとともに、一定の場合には、サイバー攻撃が日米安全保障条約にいう武力攻撃に当たりうることを確認している。

米軍では、2018年に統合軍に格上げされたサイバー軍が、サイバー空間における作戦を統括している。米サイバー軍は、国防省の情報ネットワークの防護、敵のサイバー活動監視や攻撃防御、統合軍の作戦支援などのチームから構成されており、6,200人規模である。また、米軍は、ラトビアやリトアニアなどのパートナー国において、重要なネットワーク上の悪意のあるサイバー活動に対して、防御し妨害する作戦を実施している。

(2) 韓国

韓国は、2024年2月、北朝鮮などによるサイバー脅威や高度化するサイバー環境に対応するため、攻勢的サイバー防御や抗たん性確保などを目標とする新しい「国家サイバー安保戦略」を発表している。同年9月には、下位文書として「国家サイバー安全保障基本計画」が策定され、目標の達成に向けた具体的な方針が示された。

国防部門では、韓国軍は、サイバー作戦態勢を強化し、サイバー空間における脅威に効果的に対応するため、2019年に合同参謀本部を中心としたサイバー作戦の遂行体系を構築するとともに、合同参謀本部、サイバー作戦司令部、各軍の連携体制を整備した。また、2024年8月の乙支（ウルチ）演習の際には、サイバーレジリエンス[24]の確保を目的として、官・軍・民による初の実動型統合訓練が実施された。

(3) オーストラリア

豪内務省は、2022年に発表した「国防サイバーセキュリティ戦略」において、サイバー脅威環境に適応した任務を重視し、かつ最新のサイバーセキュリティをベストプラクティスとパートナーシップによって実現するとし、運用モデル実装や能力取得など行動目標を定めている。また、2023年に公表した「2023年から2030年までのサイバーセキュリティ戦略」において、2030年までにサイバーセキュリティの世界的なリーダーになるためのロードマップを定めている。

2025年3月、豪内務省は「サイバーセキュリティ規則2025」を発表した。2026年3月に施行されたこの規則では、オーストラリア国内で提供されるインターネットに接続可能な製品に対する必須セキュリティ基準を規定しており、内務省令に基づいて導入されるこの基準は、消費者向けスマートデバイスのサイバーセキュリティを強化するとされている。

組織面においては、オーストラリアサイバーセキュリティセンター（ACSC）を設置し、政府機関と重要インフラに関する重大なサイバーセキュリティ事案に対処している。また、2023年には、豪内務省傘下に、サイバー政策の総合調整などを担う国家サイバー局（NOCS）を設置した。

Australian Cyber Security Centre

National Office for Cyber Security

豪軍は、2017年に統合能力群内に情報戦能力部を、2018年にその隷下に国防通信情報・サイバー・コマンド（DSCC）を設立した。なかでも空軍において、職種区分として、ネットワーク、データ、情報システムなどを防護するサイバー関連特技を新設し、2019年に新設した特技への要員の募集を開始した。

Defence Signals Intelligence and Cyber Command

(4) 欧州

EUは、2020年に「デジタル10年のためのEUのサイバーセキュリティ戦略」を発表し、強靱なインフラと重要サービスのための規則改正や、民間・外交・警察・防衛各分野横断型の共同サイバーユニットの設立などを目標としている。加えて、EUの市民とインフラの保護能力強化などのため、2022年にEUサイバー防衛政策を発表している。2024年には、消費者や企業の保護を目的としてサイバーレジリエンス法が施行され、他のデバイスやネットワークに直接または間接的に接続されるすべての製品に、サイバーセキュリティ要件が課されるようになった。

NATOは、2014年のNATO首脳会合において、加盟国に対するサイバー攻撃をNATOの集団防衛の対象とみなすことで合意している。また、2024年のNATO首脳会合では、統合サイバー防衛センターを新たに設置することが合意された。これは、既存の各種サイバー関連機能の統合を試みるものであり、これによってサイバー

24　サイバー攻撃によって指揮統制システムや情報通信ネットワークの一部が損なわれた場合においても、柔軟に対応して運用可能な状態に回復する能力。

空間における状況把握、抗たん性、集団防衛を強化するとしている。

また、研究や訓練などを行う機関としてNATOサイバー防衛協力センター（CCDCOE）が2008年に認可された。CCDCOE（Cooperative Cyber Defence Centre of Excellence）は、サイバー活動に適用される国際法をとりまとめたタリンマニュアル2.0を2017年に公表しており、このマニュアルを3.0へ更新する取組が進められている。また、2025年、CCDCOE主催「ロックド・シールズ2025」や、NATO主催「サイバー・コアリション」のサイバー防衛演習が開催され、NATO加盟国のほか、わが国も参加している。

英国は、2021年に公表した国家サイバー戦略において、敵対勢力の探知・阻止・抑止などの戦略的目標を掲げている。また、2023年に公表した「国家サイバー部隊：責任あるサイバー戦力の実践」では、テロ活動の妨害、APT脅威への対抗、選挙干渉の軽減などを実施し、今後、国家サイバー部隊の規模・能力・機能統合を追求するとしている。

フランスは、2026年1月に発表された「国家サイバーセキュリティ戦略2026-2030」において、国家のレジリエンス強化のために、サイバーセキュリティの全体的なレベルの向上、重要インフラとデジタル基盤の強化、さらには、司法、外交、軍事、経済、技術といった資源を活用し、サイバー脅威の低減、脅威情報の共有を通じて民間との協力を強化するとしている。

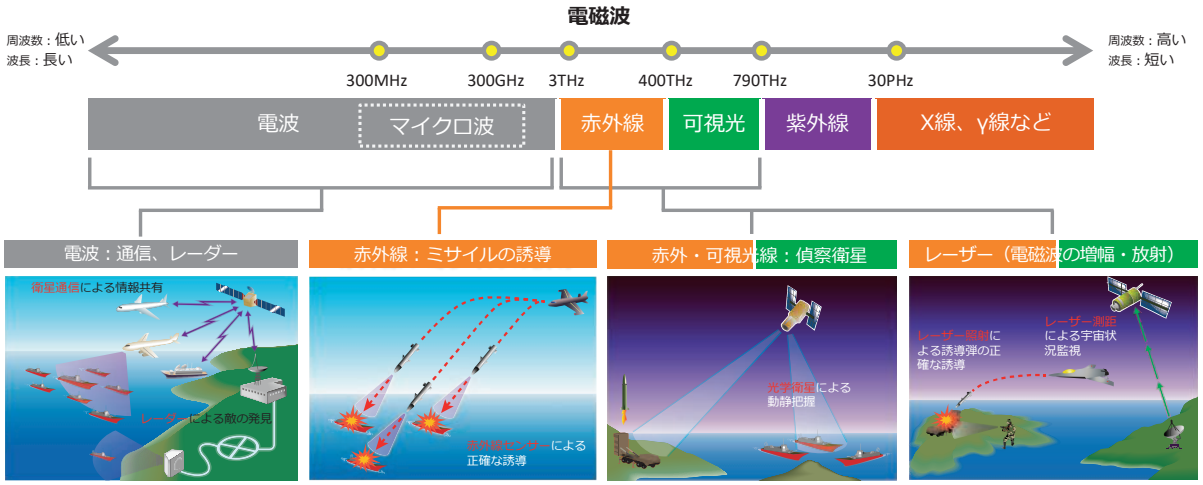
3 電磁波領域をめぐる動向

1 電磁波領域と安全保障

電磁波は、テレビや携帯電話、GPSなど日常の様々な用途で利用されている。軍事分野においては、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に使用されており、電磁波領域における優勢を確保することは、現代の作戦において必要不可欠なものになっている。電磁波領域を利用して行われる活動には「電子戦」と「電磁波管理」があり、電子戦の手段や方法は一般的に、「電子攻撃」、「電子防護」、「電子戦支援」の3つに分類される。

参照　図表Ⅰ-4-3-4（防衛分野における電磁波領域の使用）

図表Ⅰ-4-3-4　防衛分野における電磁波領域の使用



「電子攻撃」は、強力な電磁波や、相手の発する電磁波をよそおった偽の電磁波の発射などにより、相手の通信機器やレーダーから発せられる電磁波を妨害し、通信や捜索能力を低減または無効化することである。電磁波妨害（ジャミング）、電磁波欺まん（スプーフィング）のほか、高出力の電磁波（レーザーやマイクロ波など）による対象の物理的な破壊も含まれる。

「電子防護」は、相手から探知されにくくすることや、

通信機器やレーダーが電子攻撃を受けた際に、使用する電磁波の周波数の変更や、出力の増加などにより、相手の電子攻撃の低減・無効化を行うことである。

「電子戦支援」は、相手の使用する電磁波に関する情報を収集する活動である。電子攻撃・電子防護を効果的に行うためには、平素から相手の通信機器やレーダー、電子攻撃機がどのような電磁波をどのように使用しているかを把握・分析しておくことが必要である。

「電磁波管理」は、戦域における電磁波の使用状況を把握し、電磁波の干渉が生じないよう、味方の部隊や装備品が使用する電磁波について、使用する周波数、発射する方向、使用時間などを適切に調整する活動である。

主要国は、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な攻撃手段として認識している。また、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みられる。

参照　4項2（高出力エネルギー兵器）、Ⅲ部1章1節1項6（電磁波領域における対応）、Ⅲ部1章2節4項3（電磁波領域）

2　電子戦に関する各国の取組

(1) 米国

米国は、2020年に公表した「電磁スペクトラム優勢戦略」において、米国が選択するタイミング、場所、パラメーター（周波数、電力、変調など）で、電磁スペクトラムでの行動の自由を確保することが、あらゆる領域での作戦を成功させるうえでの前提であるとしている。2021年には、この戦略の実施計画が承認され、統合電磁スペクトラム作戦を開発、統合、強化する手順の確立や、電磁スペクトラム能力の取得手引きの作成などに取り組むとしている。

米軍は、陸軍が宇宙・サイバー・電子戦機能などを有するマルチドメイン任務部隊を米本土（2017年）、ドイツ（2021年）および米ハワイ州（2023年）に配備したほか、空軍が2021年に電子戦の運用・保守のための第350スペクトラム戦航空団を新編している。2023年には、戦略軍が「統合電磁スペクトラム作戦センター」を正式に開設し、米軍の電磁スペクトラム作戦の中心として部隊管理、計画、状況監視などを担うとしている。また、宇宙分野の電子戦演習「ブラック・スカイ」や、電磁干渉下での指揮統制演習「ヘヴィ・レイン」を実施している。

(2) 中国

中国軍は、電子戦が現代戦争の不可欠な要素であると考えており、自国の情報網を保護しつつ敵に電磁波領域を使用させないために、電子戦とサイバー戦を整合させ、紛争における情報支配の達成を追求しているものとみられる[25]。

中国の電子戦戦略は、敵の電子機器の抑制、劣化、混乱、欺まんに重点を置いているとされ、電子戦部隊は、演習の中で、複数の通信システム、レーダーシステム、GPS受信機に対する妨害・対妨害作戦を実施するための訓練を定期的に実施し、運用部隊の電子戦兵器の習熟度などを評価しているとされる[26]。

組織面では、従来電子戦を担当しているとされた戦略支援部隊が2024年4月に廃止され、その隷下であった軍事宇宙部隊およびサイバー空間部隊が兵種に格上げされたとの指摘がある。現在はサイバー空間部隊が電子戦を担当しているとみられる[27]。

また、中国は、南シナ海の南沙諸島ミスチーフ礁に電波妨害装置を展開したと指摘されている[28]ほか、わが国周辺では、これまでY-8電子戦機やY-9電子戦機などが飛行したことが確認されている。

(3) ロシア

ロシアは、「軍事ドクトリン」において、電子戦装備を現代の軍事紛争における重要な装備の一つと位置づけている。また、2021年4月の軍機関紙の寄稿記事によれば、情報通信技術の発達した先進諸国の技術的優位性に対し、電子戦技術の向上や装備の拡充により、部隊の指揮や兵器の誘導における優位を確保するとしている。

ロシアの電子戦部隊は、地上軍を主力とし、軍全体で5個の電子戦旅団が存在しているとされており[29]、多種類の電子戦装備を保有している。また、電子戦装備品を

25　米国防省「中華人民共和国の軍事および安全保障の進展に関する年次報告」（2024年）による。
26　米国防省「中華人民共和国の軍事および安全保障の進展に関する年次報告」（2024年）による。
27　米国防省「中華人民共和国の軍事および安全保障の進展に関する年次報告」（2024年）による。
28　戦略国際問題研究所「An Accounting of China's Deployments to the Spratly Islands」（2018年5月）による。
29　「Jane's International Defence Review」2018年4月号「All quiet on the eastern front：EW in Russia's new-generation warfare」による。

一元的に統制する電子戦システム「ブィリーナ」や、周囲約1,000kmに所在する無線通信や電子偵察システムを妨害可能とされる「パランティン」など、AIを搭載した電子戦システムの開発・配備を進めている。

ウクライナ侵略において、ロシアの電子戦装備は、ウクライナの無人航空機の飛行妨害[30]やGPS誘導弾の誘導精度劣化に効果を発揮しているとみられる。また、ロシアは、ウクライナの無人航空機から防護するため、装甲車などにジャマーを搭載し、無人航空機の通信を抑制する対策を実施している。

(4) 欧州

EUは、防衛能力の開発方針を示した「EU能力開発の優先事項」を2023年に公表し、戦略的手段として電磁スペクトラム作戦の優越をあげ、電磁スペクトラム作戦の計画・連係能力などが重要であるとしている。

NATOでは、NATO電子戦諮問委員会（NEWAC：NATO Electronic Warfare Advisory Committee）が「電磁戦」に関する問題の協議や調整を行うための主要フォーラムとしての役割を担っており、NATO軍事委員会への助言などを行っている。2024年11月に開催された全体会議では、ウクライナや中東で「電磁戦」が広範囲に用いられてきたことは、「電磁戦」が現代戦の重要な領域となっていることを示しているとの認識のもと、現代戦において「電磁的な優位」を達成することの重要性が強調された。

4 先端技術をめぐる動向

1 極超音速兵器

米国、中国、ロシアなどは、弾道ミサイルに搭載され、大気圏内を極超音速（マッハ5以上）で滑空飛翔・機動し、目標へ到達するとされる極超音速滑空兵器（HGV）や、極超音速飛翔を可能とするスクラムジェットエンジンなどの技術を使用した極超音速巡航ミサイル（HCM：Hypersonic Cruise Missile）といった極超音速兵器の開発を行っている。極超音速兵器については、通常の弾道ミサイルとは異なる低い軌道を極超音速で長時間飛翔すること、高い機動性を有することなどから、探知や迎撃がより困難になると指摘されている。

(1) 米国

米国は、2021年、米国防省高官が、極超音速兵器の開発構想に言及しており、2020年代初頭から半ばにかけて極超音速兵器を配備し、2020年代半ばから後半にかけて防衛能力を構築すると公表した[31]。同年、米陸軍は、HGV「LRHW」のプロトタイプを受領し、配備に向け訓練を実施しており、2024年6月と12月に発射試験に成功しているが、一方で、当初予定していた2025年末までとの配備計画の遅延も指摘されている。また、米海軍と米空軍も極超音速兵器を開発しており、米海軍はズムウォルト級ミサイル駆逐艦やバージニア級原子力潜水艦への搭載を目指しているとされている。

このほか、米国は、極超音速ミサイルの脅威に対して、滑空段階で迎撃するミサイル「GPI」の開発を日米共同により進めている。

参照　Ⅲ部1章2節2項2（防衛省・自衛隊の取組）

(2) 中国

中国は、2019年の中国建国70周年閲兵式において、HGVを搭載可能な弾道ミサイルとされるDF-17を初めて登場させており、米戦争省は、中国がDF-17の運用を2020年には開始したと指摘しているほか、弾道ミサイルDF-27にもHGVが搭載される可能性に言及している[32]。また、2025年9月の軍事パレードにおいては、HCMとされるCJ-1000に加え、艦艇発射型として、HGVとされるYJ-17やHCMとされるYJ-19が初めて登場した。

(3) ロシア

ロシアは、HGV「アヴァンガルド」を既に配備している。アヴァンガルドを搭載可能とされる新型ICBM「サルマト」については、2023年から2025年にかけて、発射試験の失敗が続いた可能性が指摘されているものの、

30 英国王立防衛安全保障研究所「Meatgrinder：Russian Tactics in the Second Year of Its Invasion of Ukraine」（2023年）による。
31 米国防省「中華人民共和国の軍事および安全保障の進展に関する年次報告」（2024年）による。
32 米国防省「中華人民共和国の軍事および安全保障の進展に関する年次報告」（2024年）による。

2026年5月には、ロシア政府により発射成功が発表されており、同年末に配備される予定とされている。また、2021年にHCM「ツィルコン」の潜水艦発射試験に成功したほか、ツィルコンを搭載したフリゲートが2023年から戦闘哨戒任務を開始し、2024年2月には、プーチン大統領が、ウクライナにおいて、ロシア軍がツィルコンを使用した旨初めて言及している。ツィルコンは、既に海軍部隊に配備済であり、2025年9月には、ベラルーシと合同で実施した軍事演習「ザーパド2025」で発射訓練が行われた。

(4) 北朝鮮

北朝鮮は、極超音速滑空飛行弾頭の開発を優先目標の一つに掲げ、研究開発を進めているとみられ、2021年以降、「極超音速ミサイル」と称するミサイルを発射している。

参照　3章4節1項3 (3)（ミサイル戦力）

2 高出力エネルギー兵器

レールガンや高出力レーザー兵器、高出力マイクロ波兵器などの高出力エネルギー兵器は、多様な経空脅威に対処するための手段として開発が進められている。

レールガンは、電気エネルギーから発生する磁場を利用して弾丸を打ち出す兵器であり、使用する弾丸はミサイルとは異なり推進装置を有していない。このため、小型・低コストかつ省スペースで備蓄でき、多数のミサイルによる攻撃にも効率的に対処可能とされている。

レーザー兵器は、高出力のレーザーエネルギーにより対象を破壊する兵器であり、多数の小型無人航空機や小型船舶などに対する低コストで有効な迎撃手段として、米国、中国、ロシアなどで開発されている。

高出力マイクロ波兵器は、無人航空機、ミサイルなどに搭載された電子機器を破損または誤作動させる兵器である。

(1) 米国

米国は複数のレーザー兵器の開発を進めており、2025年6月、米陸軍は無人航空機群を標的に50kW級の車載型レーザー兵器「DE M-SHORAD」（Directed Energy Maneuver-Short Range Air Defense）の実弾射撃試験を実施し、無人航空機群の無力化に成功したほか、2023年には300kW級のレーザー兵器の開発契約を締結している。米海軍においても、2022年には60kW級レーザー兵器「HELIOS」が、アーレイ・バーク級ミサイル駆逐艦「プレブル」（High Energy Laser and Integrated Optical-dazzler with Surveillance）に搭載され、2026年1月に無人航空機4機に対して照射し無力化することに成功している。なお、HELIOSの出力を将来的に150kWまで高め、センサーやエンジンが露出していない無人航空機に対して有効性を発揮することも計画されている。

高出力マイクロ波兵器については、2023年、米空軍が、スウォーム飛行を模擬した多数の無人航空機に対して、高出力マイクロ波兵器「THOR」を使用し多数の無人航空機を効果的に無効化したとしている（Tactical High-power Operational Responder）。また、米海兵隊は、AIによる無人航空機の検出・追跡機能と高出力マイクロ波兵器の融合について評価を行っている。

(2) 中国

中国は、2024年の中国国際航空宇宙博覧会において、小型無人航空機を対象とした出力不明の車載型レーザー兵器「LW-60」を公開した。また、低軌道周回衛星の光学センサーを妨害または損傷させることを企図していると思われる対衛星レーザー兵器を配備しているとの指摘があるほか、さらに高出力のレーザー兵器も開発中との指摘もある。

(3) ロシア

ロシアは、出力数10kW級のレーザー兵器「ペレスヴェト」を既に配備しており、対衛星兵器として出力数がMW級の化学レーザー兵器も開発中との指摘がある。

(4) イスラエル

イスラエルは、2025年9月に出力が100kW級の車載型防空用レーザー兵器「アイアン・ビーム」の開発が完了し、この兵器によるロケット砲、迫撃砲、無人航空機などの多岐にわたる脅威に対する迎撃能力が実証され、一連の試験に成功したことを発表した。同年12月には、最初の「アイアン・ビーム」が部隊へ引き渡され、今後、部隊に順次配備されていくと考えられる。

(5) 英国

英国防省は、2025年11月、英国初となるドラゴンファイアと呼ばれる高出力レーザー兵器を用いて、時速650kmで飛行する無人航空機の撃墜に成功した旨発表した。ドラゴンファイアは、1発あたり10ポンドと安価

であるほか、1km離れた場所から1ポンド硬貨に命中させるほどの精度を持っているとされており、2027年に英海軍の45型駆逐艦に搭載するための契約が締結されている。さらに、陸軍車両や空軍戦闘機への搭載も検討されている[33]。

3 AI技術

AI技術は、指示に従い自然な文章や画像などを生成できる生成AI、目標達成のために必要な情報を自ら分析するなど自律的に動くAIエージェント、AIが頭脳となり実世界で物理的な身体を用いて自律的に行動・学習できるようになるフィジカルAIなど、技術開発が急速に進んでいる分野の一つである。軍事分野においては、指揮・意思決定の補助、情報処理能力の向上に加え、無人航空機への搭載やサイバー領域での活用など、影響の大きさが指摘されている。

(1) 指揮・意思決定の補助などにおけるAI技術の活用

ア　米国・欧州

米国におけるAIの活用の一例として、米陸軍が推進する「プロジェクト・メイブン」において開発された「メイブン・スマート・システム」と呼ばれるAIシステムが、戦闘空間の迅速な評価、大量のデータの収集、AIを使用した収集データの分析による目標の特定と攻撃を可能とするとされており、2024年5月、米国防省は民間企業との開発契約を公表し、2025年には、この契約の上限額を2029年までに約13億ドルに引き上げている。また、2025年4月には、NATOもこのシステムの取得契約に合意したと発表している[34]。

イ　中国

中国は、2020年、次世代指揮情報システムの研究・開発を目的に、中央軍事委員会がAI軍事シミュレーション競技会の開催を発表している。米国防省は、中国が2025年までにAIの研究開発で欧米を追い抜き、2030年までにAIで世界のリーダーとなることを目指していると指摘している[35]。

ウ　イスラエル

イスラエルは、2023年に発生したパレスチナ武装勢力との衝突において、ガザ地区の攻撃目標選定の過程で「ラベンダー」と呼ばれるAIシステムを活用していることが指摘されている。ガザ市民のスマートフォンなどにインストールされている通話アプリのデータをAIに解析させ、そのスマートフォンなどの持ち主とハマスなどとの関係性を評価していると指摘されている。また、この衝突においては、「ゴスペル」と呼ばれるAIシステムも、物理的な攻撃目標の選定と優先順位付けを支援するために使用されたと指摘されている。なお、イスラエル軍は、テロ工作員の特定や工作員かどうかを予測するAIは利用していないと発表している旨、報じられている。

(2) 無人システムにおけるAI技術の活用

各国は、AIを組み込んだ無人システムの開発を進めている。

ア　米国

米国では、空対空戦闘の自動化や有人航空機・無人航空機の連携、海洋監視任務での実証など多様な研究開発を実施している。2023年、米空軍では、AI操縦のXQ-58A無人航空機の有人航空機との編隊飛行や、模擬された任務・武器・敵に対する戦術飛行の試験を行っているほか、同年には、数千規模のAIを活用した安価な自律システムを導入するとする「レプリケーター1」構想を発表している。また、2024年9月に発表された「レプリケーター2」構想は、無人航空機の脅威に対抗することに特化したものであるとされている。

イ　中国

中国は、2018年、中国電子科技集団公司がAIを組み込んだ200機の無人航空機によるスウォーム飛行を成功させており、スウォーム飛行を伴う軍事行動が実現すれば、従来の防空システムでは対処が困難になることが想定される。2023年には、無人航空機の空中戦を想定したAIアルゴリズム競技会を開催している。

また、最近では、人民解放軍が、中国企業が開発した高性能かつ低コストの生成AIモデルであり、自然言語処理に特化しているとされるDeepSeekのAIモデルを無人航空機に活用していると指摘されている。例えば、

33 英国政府HP「Boost for Armed Forces as new laser weapon takes down high-speed drones」(2025年11月) による。
34 NATO HP「NATO ACQUIRES AI-ENABLED WARFIGHITING SYSTEM」(2025年4月) による。
35 米国防省「中華人民共和国の軍事および安全保障の進展に関する年次報告」(2024年) による。

2025年2月に発表された時速50キロで自律的に戦闘支援作戦を実行できる軍用車両には、DeepSeekの技術が搭載されていると指摘されている。

ウ　ロシア

ロシアは、2019年、S-70大型無人航空機（オホートニク）と第5世代戦闘機であるSu-57戦闘機との協調飛行の試験を行っている。オホートニクは、2023年6月、ウクライナ侵略における作戦で初めて使用され、2024年10月には、ウクライナ東部ドネツク州で墜落したと指摘されている。

また、2025年2月以降にAIを組み込んだ無人航空機「V2U」を運用しているとウクライナ国防省情報総局が指摘している。この無人航空機は、AIを用いて標的を自律的に探索し選択できる旨が指摘されている[36]。

(3) LAWS・AIの軍事利用に関する議論

AIの軍事利用も含む自律型致死兵器システム（LAWS：Lethal Autonomous Weapons Systems）については、2014年から特定通常兵器使用禁止制限条約（CCW：Convention on Certain Conventional Weapons）の枠組みで議論されている。また、兵器に限らず、より広範なAIの軍事利用を扱う取組として、2023年には国際法上の義務に従い責任ある利用を確認した「REAIM宣言」や、責任ある人間の指揮命令系統のもとで運用し、責任の所在を明らかにする必要があることを確認した「AIと自律性の責任ある軍事利用に関する政治宣言」が、2024年には「REAIM行動のためのブループリント」が、2026年には「REAIM行動のための道筋」が発表され、わが国も支持を表明している。（REAIM：Responsible Artificial Intelligence in the Military Domain）

4　量子技術

量子技術は、原子核や電子などミクロな世界で働く量子力学を応用することで、社会に変革をもたらす重要なデュアルユース技術とされ、陸、海、空、宇宙、サイバー領域といったオールドメインでの活用が期待されている[37]。

米国は、2023年に公表した国防科学技術戦略において、量子技術を重要技術とし、同盟国との連携や技術革新を強化するとしている。

中国は、2026年3月に策定した第15次5か年計画において、量子技術などの未来産業に先行投資して育成し、大きく成長させるとしている。

また、NATOも2024年1月、NATO量子技術戦略を初めて公表し、量子技術を防衛・安全保障にどのように応用できるかを概説している。

(1) 量子暗号通信

量子暗号通信は、第三者が解読ができない暗号通信とされ、各国で研究されている。中国は、量子暗号通信衛星「墨子号」と北京・上海間の地上通信網からなる4,600kmの量子暗号通信網を構築したほか、2022年には、合肥市の共産党や政府機関などに量子暗号化サービスを提供している。また、2022年7月には、「墨子号」の20分の1のコストであるとされる「済南1号」小型量子暗号通信衛星を打ち上げた。2025年3月には、「済南1号」を用いて1万2,900km離れた南アフリカと北京ステーションとの間で、量子鍵配送を実現した旨発表されている。

(2) 量子センシング

量子センシングは、磁場、電場、温度、加速度などの物理量を極めて高い感度で測定することで、将来的に、ミサイルや航空機の追跡用途のほか、より進化したジャイロや加速度計として使用できる可能性[38]が指摘されている。これにより、探知能力の向上、妨害耐性の強化を通じて、ISR能力の向上が期待される。

米国は、GPSの代替として、2023年、量子磁気センサーによる磁気航法の実証に成功したほか、量子慣性センサーによる慣性航法の開発のため、量子ジャイロを搭載した衛星を開発している。

中国は、2025年4月に潜水艦探知用の無人航空機に搭載した、感度ピコテスラ（10兆分の1）級の量子磁力計を実証した。

(3) 量子コンピュータ

量子コンピュータは、スーパーコンピュータでも膨大な時間がかかる問題を短時間で計算できるとされ、現在広く使用される暗号方式を破る能力を持つ可能性があるため、通信の機密性に大きく影響を与える可能性があ

36　ウクライナ国防省情報総局HP「BARRAGE MUNITION WITH ARTIFICIAL INTELLIGENCE V2U」による。
37　SIPRI「Military and Security Dimensions of quantum technologies」（2025年7月）による。
38　2021年2月23日付の米国防省HPによる。

る。

また、SDA、作戦後方支援、無人航空機の制御などの複雑な最適化の支援に使われるほか、CBRNE（Chemical, Biological, Radiological, Nuclear and Explosive）に関するシミュレーションにも活用が期待される。一方、量子コンピュータでは解読が困難な耐量子計算機暗号（PQC：Post-Quantum Cryptography）への暗号技術の移行も各国で検討が進んでおり、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）は2024年8月、最初のPQC標準を公表している。EUにおいては、欧州委員会が加盟国に対してPQCへの移行に向けた戦略の策定を求めている。2025年6月には欧州委員会がロードマップを発表し、2030年末までに、重要なシステムのPQC移行を完了することを目標としている。なお、中国はPQCの導入について、NISTの標準とは異なる独自のアルゴリズムによることを検討しているとみられる。

5 積層製造技術

3Dプリンターに代表される積層製造技術は、低コストでの製造や、在庫に頼らない部品調達など各国で軍事分野への応用が期待されている。

米国は、2021年に公表した「積層製造技術の利用」において、軍事サービスの自立性・即応性向上を図るとし、3Dプリンターを一部の水上艦や潜水艦に搭載している。各軍種の取組の一例としては、米陸軍では、積層製造技術を活用し、供給不足の解決に積極的に取り組んでおり、この技術を活用して部隊が現地で金属製の部品を製造することにより、部品の輸送が不要となるとされている。また、技術を活用するための要員育成のため、教育訓練課程での高度な製造技術にかかる課程を大幅に強化した[39]。

このほか、中国が軍用機の部品製造に3Dプリンターを使用しているとされる。また、ウクライナでは無人航空機の部品などの製造に3Dプリンターを活用している。

5 認知領域をめぐる動向

国際社会においては、紛争が生起していない段階から、偽情報や戦略的な情報発信を通じて、人の認知に働きかけることにより、他国の世論や意思決定に影響を及ぼし、自らの意思決定への影響を防ぐことで、自らに有利な安全保障環境を構築しようとする情報戦が行われている。

例えば、ロシアによるウクライナ侵略、2023年のイスラエル・パレスチナ武装勢力間の衝突、台湾総統選、米大統領選などでも指摘されているように、SNSやインフルエンサーなどを媒体とし、偽情報の流布や、対象政府の信頼低下や社会の分断を企図した情報拡散などによる情報戦への懸念が高まっている。特に、近年はAI技術の進展によって、ディープフェイクや生成AIで作成される動画、画像、文書は非常にリアルであり、安価で簡単にアクセスできるツールにより短時間で作成できるため、一層深刻な脅威になってきている。

ロシアや中国は国内外で情報戦を行い、自身にとって好ましい情報環境の構築を目指しているとみられる。中国は数十億ドルをかけ、他国メディアへの投資を通じたプロパガンダの促進や偽情報の拡散、検閲などを実施しているとの指摘がある。また、米戦争省の指摘によれば、中国は認知領域での作戦を台湾に対する「圧力キャンペーン」の核心的要素と位置付け、台湾の抵抗意志を弱体化させ、社会的分断を深化させることを目的にしているとされているほか、情報空間を活用し、政治的ナラティブを拡散させ、台湾住民に影響を与え、台湾周辺における人民解放軍の活動を強調しているとされている[40]。

ロシアは、ウクライナ侵略以降、ハイブリッド戦の一環として情報による影響工作の範囲を拡大させており、現地の代理人も用いているとの指摘がある。例えば、アフリカでは現地のインフルエンサーなどとの連携のほか、民間軍事会社「ワグネル」による偽情報の拡散などが指摘されている。2025年9月のモルドバでの議会選挙においては、ロシアが情報操作によって選挙干渉を行ったことが報告されている。また、中露で連携してプ

39 米陸軍HP「Transforming Advanced Manufacturing Within the Ordnance Corps」（2025年1月）による。
40 米戦争省「中華人民共和国の軍事および安全保障の進展に関する年次報告」（2025年）による。

ロパガンダや偽情報の拡散を行っているとも指摘されている。

このような脅威に対して、欧州ではEUが「外国からの情報操作および干渉（FIMI）」という概念を提唱し、対策に取り組んでいるほか、NATOでは、2023年に「同盟統合ドクトリン（AJP-10およびAJP-10.1）」を策定し、戦略的コミュニケーション（SC）や情報作戦に関する基本的な考え方および実務的手法を示した。英国外務・英連邦・開発省は2025年9月、議会の外交委員会への回答のなかで、ロシア、中国などを悪意のある情報活動を行う国として公表しているほか、2024年10月以降、ロシアとの関係が指摘されFIMIを行っているとする組織や個人への制裁を発表している。

また、日本と欧米諸国の離間や自衛隊を含む日本政府の信頼の失墜を試みるような、わが国を対象とする悪意あるナラティブ、偽情報、プロパガンダなどを拡散する情報戦の事例も多くみられている。このような状況を受けて、防衛省・自衛隊において、情報戦対応の中核となる情報本部ほか、政策部門や運用部門が一体となって取組を加速させている。

視点

認知領域における戦い

防衛研究所　中国研究室　主任研究官　山口（やまぐち）　信治（しんじ）

近年、情報操作や浸透工作によって相手国の政治社会を混乱させたり、影響を与えようとする認知領域における戦いが激しさを増しています。中国やロシアは、民主主義国の自由で開放的な政治・社会システムの特性を利用し、そこに対して偽情報などを用いた情報操作や、浸透工作を行うことで、相手国の政治を混乱させたり、自国に望ましい方向に誘導しようとしています。

中国は、その手段として、宣伝・プロパガンダ、ソーシャルメディアでの情報操作、統一戦線（浸透）工作を行っています。宣伝・プロパガンダは、新華社など中国の官製メディアによる、中国のナラティブを世界に伝え、政府の見方や中国文化を伝達し、外国のプロパガンダへ反駁する活動を指します。

次に、ソーシャルメディアなどを通じた偽情報の拡散です。他国の政府が相手国の国内政治や社会の混乱、分断を狙って故意に偽情報を拡散させる事例がみられるようになっています。中国もこうした活動を拡大しつつあります。

そして、統一戦線工作とは、中国共産党の外部に政治的目標達成のために協力者を作り出す浸透工作の一種です。中国政府に好意的な人々や、特定の問題について中国に近い見解を持つ人々、文化や民族的に中国とつながりを持つ人々を対象に、中国の政治的目的に有利な方向に誘導しようとします。

こうした活動によって、中国が達成しようとしているのは、第一に、中国のイメージを向上し、その政策に対する支持を広げること、第二に、中国にとって不利な外国の主張や情報に反駁すること、第三に相手国の社会の分断を拡大し、政治社会に混乱を生み出すことです。中国の工作の対象は主に台湾やグローバルサウスの国々です。台湾政治の混乱と中国にとり有利な状況の形成を狙ったり、グローバルサウス諸国に対して米欧の欠点や問題点を吹聴し、自国への支持を高めるよう画策しています。

これまで日本に対する活動はそれほど盛んではないと考えられてきましたが、最近になって活発化しつつあります。特に2023年6月に習近平国家主席が「福建省と沖縄の歴史的つながり」に言及してから、沖縄県をめぐる中国の工作が活発化しています。沖縄県を訪問する中国政府・党関係者が増加するとともに、ソーシャルメディアのフェイクアカウントが「琉球独立」をあおるようなデマ動画を拡散させようとするなどの活動がみられるようになっています。

中国やロシアの活動が必ずしも高い効果を上げているわけではありません。しかしこうした認知戦は、相手の政治や社会における対立点を利用して分断を煽ろうとすることから、民主主義に対する深刻な挑戦となりえます。さまざまな政府部門や企業、社会が協力して対応することが必要です。

（注）本コラムは、研究者個人の立場から学術的な分析を述べたものであり、その内容は政府としての公式見解を示すものではありません。

視点

情報通信技術（ICT）時代の新たな戦い方

防衛研究所　グローバル安全保障研究室　主任研究官　1等陸佐　川村（かわむら）　幸城（こうき）

スマートフォンがあれば、いつでも、どこでも世界中の人々とメッセージや映像を交換できます。そのためには近くに電波が届く通信施設が存在しなければなりません。そうしたスマートデバイスの情報インフラを活用した作戦の代表的な事例が、広大なロシア領の奥地にある軍事基地を攻撃したウクライナによる「蜘蛛の巣」と呼ばれる作戦（2025年6月）でした。

この作戦では、ウクライナ国内にいるドローンのオペレータが117機の「オサ」（スズメバチの意）と呼ばれる小型ドローンを使って1,000km～5,000kmも離れた複数のロシア軍基地を同時攻撃し、多数の大型爆撃機などを破壊しました（日本円にして1兆300億円規模の損害）。わずか10数キロの航続距離しかもたない小型ドローンが、なぜ数千キロも離れたロシア軍基地を攻撃できたのでしょうか。

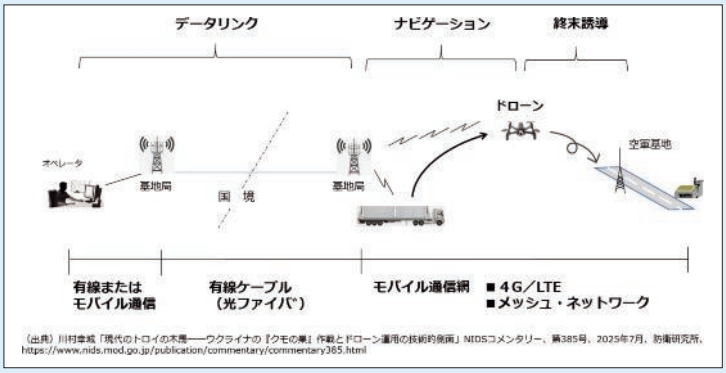
まず大型トレーラのコンテナ天井部にドローンを数十機単位で隠し、地元のロシア人運転手を雇って標的から10km圏内までトレーラを移動させました。そこから携帯電話と同じSIMカードを内蔵したドローンが敵国のモバイル通信網（私たちが日ごろ利用している4G/LTE回線）を介して制御信号を受信することで、数千キロも離れたウクライナ国内から遠隔操縦できたと言われています（図参照）。またオペレータがドローンの自己位置情報をリアルタイムに把握するためGNSS信号の受信機も必要でした。

通常のモバイル回線を使用した遠隔操縦では、トラフィック信号の遅延や電波干渉も起こり得ます。そのためドローンには誰でもフリーで入手できる飛行制御のソフトウェア（ArduPilot）が搭載されていました。これによりドローンはあらかじめ設定した飛行ルートをたどり、安定した自動操縦を維持することができました。この飛行安定化機能に加え、トラフィック信号が遅延したり、通信が途絶した場合に作動する「フェイルセーフ」機能も備えていました。

敵地での飛行ですから、当然、相手からの電波妨害を受けることも予想されていました。そのためドローンには学習済みAIモジュールが搭載されていました。これによりドローンがオペレータによる制御の手を離れてしまった場合でも、物体認識アルゴリズムにより自律的な終末誘導が可能となり、あらかじめ学習したターゲット脆弱点を捉えることができたのです。AIモジュールを動作させるためにはコンピュータが必要ですが、オサ・ドローンに積まれていたのはRaspberry Pi-5（日本では「ラズパイ」の愛称で知られています）という名刺サイズの小型PCでした。

コードネーム「蜘蛛の巣」と呼ばれたこの作戦は、それまでウクライナの攻撃力が及ばないと考えられていたロシアの最深部までをカバーしていたことから名付けられました。それを可能にしたのは、ロシア国内のモバイル通信網を利用できたからです。SIMカードをUSBメモリ（いわゆるドングル）でコンピュータにつなげば誰でもできる仕掛けです。実際、ロシア軍も連日のように繰り返されるウクライナへの空襲で、現地のモバイル通信網を活用していると言われています。

私たちはスマートフォンさえあれば、世界中のどこからでも通信できる利便性を享受しています。それと同じように、小型コンピュータとSIMカードを内蔵した小型ドローンは、それが隠密裏に運び込まれさえすれば、どこからでも、どこへでも破壊工作に利用できる。最近の紛争事例は、そうした新しい現実を私たちに突き付けているように感じられます。



（出典）川村幸城「現代のトロイの木馬――ウクライナの『クモの巣』作戦とドローン運用の技術的側面」NIDSコメンタリー、第385号、2025年7月、防衛研究所、https://www.nids.mod.go.jp/publication/commentary/commentary385.html

ドローン運用のシステム構成

（注）本コラムは、研究者個人の立場から学術的な分析を述べたものであり、その内容は政府としての公式見解を示すものではありません。