

までの目標を設定するとともに、能力強化、規範策定、諸外国との協力、人材育成など具体的な行動計画を規定した。

組織面では、政府全体のサイバーセキュリティ戦略の立案・調整などを行うサイバーセキュリティ・情報保証部 (OCSIA) を内閣府のもとに、Office of Cyber Security and Information Assurance サイバー空間の監視などを行うサイバーセキュリティ運用センター (CSOC) を政府通信本部 (GCHQ) のもとに設置している。また、国防省において、省内のサイバー活動を一元化する国防サイバー作戦グループ (DCOG) を12 (同24) 年4月までに暫定的に設置し、15 (同27) 年3月までに完全な運用能力を保有することとしている<sup>25</sup>。

また英国は、15 (同27) 年1月、キャメロン英首相とオバマ米大統領がサイバー防衛分野における協力強化<sup>26</sup>で一致するなど、各国との連携強化に努めている。

#### 4 オーストラリア

オーストラリアは、13 (同25) 年1月、初の「国家安全保障戦略」を公表し、サイバー政策および

作戦の統合が国家安全保障上の最優先課題の一つであるとした。

組織面では、政府全体のサイバーセキュリティ政策を調整・統括する、サイバー政策グループ (CPG) をサイバー政策調整官 (CPC) のもとに設置し、オーストラリア通信電子局 (ASD) のCyber Policy Group Cyber Policy Coordinator オーストラリアサイバーセキュリティセンター (ACSC) が、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への対処を行っている<sup>27</sup>。

#### 5 韓国

韓国では、11 (同23) 年8月に「国家サイバーセキュリティ・マスタープラン」が制定され、サイバー攻撃対処における国家情報院<sup>28</sup>の統括機能が明確化されたほか、予防、検知、対応<sup>29</sup>、制度および基盤の五つの分野を重点的に推進することとされた。国防部門では、10 (同22) 年1月に、サイバー空間における作戦の計画、実施、訓練および研究開発を行うサイバー司令部が設置され、現在では国防部直轄部隊として運用されている<sup>30</sup>。

## 第6節 軍事科学技術と防衛生産・技術基盤をめぐる動向

### 1 軍事科学技術の動向

近年の情報通信技術 (ICT) の大幅な進歩に代表される科学技術の発展は、様々な分野に波及し、経済、社会、ライフスタイルなど、多くの分野において革命とも呼ぶべき大きな変化が引き起こされている。

このことは軍事分野においても例外ではなく、米国をはじめとする先進諸国では、ICTの発展に

端を發する変革が戦闘力などの飛躍的向上を実現できると考え、各種研究と施策が継続して行われている。

たとえば、ネットワークを活用することにより、偵察用の衛星や無人機などの情報収集システムを駆使して収集された敵部隊などに関する情報が共有されれば、遠隔地の司令部からであっても

25 このほか、13 (平成25) 年9月、英国防省は、コンピュータの専門家数百人を同国のサイバー防衛の最前線で勤務する予備役として採用することを発表し、統合サイバー予備役の創設を認めた。

26 ホワイトハウスの発表によると、英国のGCHQと保安庁 (SS : Security Service)、米国の国家安全保障局 (NSA : National Security Agency) と連邦捜査局 (FBI) がサイバーセキュリティとサイバー防衛に関して密接に協力するとした。また英国政府と米国政府は、重要インフラへのサイバー攻撃に対する防護能力を確認する目的で、15 (平成27) 年後半に初の共同演習を行うと発表した。

27 ACSCは、豪州犯罪委員会、豪州連邦警察、豪州治安情報機関、豪州国防省及び司法省の職員から構成され、サイバー空間における脅威分析や官民双方のインシデント対応を行っている。

28 国家情報院長のもとには、国家のサイバーセキュリティ体制の確立および改善、関連政策および機関間の役割調整、大統領の指示事項に関する措置や施策などの重要事項を審議する国家サイバーセキュリティ戦略会議が設置されている。

29 14 (平成26) 年2月、韓国国防部は、他国を攻撃するサイバー兵器の開発計画を国会で報告したと伝えられている。

30 12 (平成24) 年8月に国防部が大統領に提出した「国防改革基本計画」(2012~2030) においては、将来に向けた軍改革の一つとして、サイバー戦対応能力を大幅に拡充することがあげられている。

きわめて短時間に指揮・統制が行われ、目標に対して迅速・正確かつ柔軟に攻撃力を指向することが可能となる。

また、米国など高度に近代化された軍隊を有する主要国は、より精密で効果的な攻撃を行えるよう、兵器の破壊力の向上、精密誘導技術、C<sup>4</sup>ISRを含む情報関連技術、無人化技術（無人機<sup>1</sup>など）に加え、隠密性の向上による先制攻撃の機会の増加や、残存性の向上による戦力損耗のリスクを低減させるステルス技術、こうした技術に関連する部品や素材に利用されるナノテクノロジーなどの研究開発を重視している。最近では、火砲などの従来兵器と比べて1発あたりのコストや、射程、精度、迅速性などの観点から効果的な火力発揮が期待されるルールガン<sup>2</sup>や高エネルギーレーザー兵器<sup>3</sup>の実験成功が伝えられているほか、きわめて遠方に位置する目標であっても、通常兵器で迅速かつピンポイントでの打撃を可能とする高速打撃兵器<sup>4</sup>の開発も伝えられている。14（平成26）年3月に米国防省から公表された「4年ごとの国防計画の見直し」（QDR）では、最新技術の普及<sup>5</sup>が、戦争方式を変えと言及している。  
Quadrennial Defense Review

最近の軍事科学技術<sup>6</sup>の進歩は、民生技術の発展にも拠るところが大きい。近年は、現有装備品の性能向上や新たな装備品の開発を行うにあつ

ては、民生技術のスピノンやデュアルユーステクノロジー<sup>7</sup>の活用が頻繁に行われている。特に、ICT関連民生技術の各種装備品などへの技術波及が拡大している。

一方、ハイテク型軍隊などを保有することが技術的、経済的に困難な国やテロ組織などの非国家主体においては、先端技術を有する国に対しても有利な戦い方が可能になる兵器などの研究・開発や、ICTなどを利用した不正な技術の取得を行っていくものと考えられる。つまり、相対的に低費用で開発・取得可能であり、在来型の戦力以外で相手のぜい弱性を衝くことができる非対称的な攻撃手段、すなわち核兵器、化学兵器、生物兵器といった大量破壊兵器、弾道ミサイル、テロ攻撃、サイバー攻撃などに重点的に取り組む傾向があると考えられる。

非対称的な攻撃手段が世界的に拡散していく可能性に対して、こうした非対称的な脅威に対抗するための技術に関する研究開発<sup>8</sup>も重要なものとして認識されている。



米海軍研究所（ONR）で開発中の電磁ルールガン【米海軍研究所】

- 1 軍用の無人機については、無人航空機（UAV：Unmanned Aerial Vehicle）、陸上無人機（UGV：Unmanned Ground Vehicle）、海洋無人機（UMV：Unmanned Maritime Vehicle）、海上無人機（USV：Unmanned Surface Vehicle）および無人潜水艇（UUV：Unmanned Undersea Vehicle）などが開発されている。こうした無人機については、人間が操作するものから完全な自律行動型、いわゆる自律型致死兵器システム（LAWS：Lethal Autonomous Weapons System）に推移していく可能性も指摘されている。また、14（平成26）年5月に国連の特定通常兵器使用禁止・制限条約（CCW）の非公式会合で、人間が判断することなく自動的に敵を殺傷する、自律型致死兵器システムを運用する上での、人道や法律面などの課題について初めて議論され、同年11月の締約国会議においても議論が行われた。
- 2 レールガンは、火薬の代わりに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、米軍では、従来兵器である5インチ（127mm）砲と比べ射程を約10倍の約370kmとするルールガンが開発されており、コストはルールガン1発あたり、ミサイルの20～60分の1と伝えられている。
- 3 米軍はレーザー兵器を、対小型艇用防衛や対無人機などの低高度防空能力強化のため開発中であり、14（平成26）年9月から11月に、米輸送揚陸艦ポンスに搭載し射撃試験が行われた。こうした高エネルギーレーザー兵器は、今後、システムの小型化が進められ、軽機動車両への搭載も念頭に置かれているとの指摘がある。また、レーザー発射1回の費用は1ドル未満と伝えられている。
- 4 通常兵器による攻撃の所要時間を大幅に短縮するのが目的とされ、弾道ミサイルとは明確に異なる低い軌道で飛翔するとされている。また、米国と中国が開発しているとの指摘がある。
- 5 かつて多額の費用がかかった「対ステルス技術」、すでに民生や軍事に広く応用されている「無人および自律システム化したロボット技術」、武器の製造や戦闘時の補給に革命をもたらす可能性のある「低価格の3Dプリンター技術」、および新たな方法での大量破壊兵器の開発が可能となる「バイオテクノロジーの発展」などがあるとし、これらの技術が戦場でどのように使われるかは依然として不透明であると指摘している。
- 6 14（平成26）年11月、ヘーゲル米国防長官（当時）は、国防イノベーション構想（いわゆる「第3のオフセット戦略」）すなわち、A2/ADなど敵の軍事的優位性を、我に優位性のある最先端の技術や作戦要領によってオフセット（相殺）する構想を発表した。I部1章1節1項4参照
- 7 軍事技術分野では、一般的に民生技術を軍事技術に転用することを「スピノン」、その逆を「スピノフ」、いずれの分野においても使用可能な技術を「デュアルユーステクノロジー」という。
- 8 弾道ミサイル、テロ攻撃、サイバー攻撃などに対抗する技術であるBMDおよびICTなどがあげられる。

## 2 防衛生産・技術基盤をめぐる動向

近年、特に欧米諸国においては、国防費の大幅な増額が困難な状況が続いている。一方で、前項で述べた軍事科学技術の高度化や装備品の複雑化にともない、開発・生産コストが高騰して防衛装備品の調達単価が上昇するとともに、調達数量が減少している。このような中で、諸外国は、自国の防衛生産・技術基盤を維持・強化するため、各種の取組を進めている。

欧米諸国は、前述の国防費をめぐる状況を踏まえ、防衛産業の再編による競争力の強化を指向してきた。米国では、主に国内企業間の合併・統合が繰り返されたのに対し、欧州では、ドイツ、フランス、英国、イタリアを中心に、国境を越えた防衛産業の合併・統合がみられる<sup>9</sup>。

また、欧米諸国は、開発・生産コストの高騰に対応するため、同盟国・友好国間での防衛装備品の共同開発・生産や技術協力を推進している。この理由としては、①開発・生産費用の分担、②共同開発・生産の参加国全体への需要拡大、③技術の相互補完、④最先端技術の獲得による国内技術の底上げなどがあげられる。

さらに、戦闘機F-35の維持管理においては、同機が国際共同開発機であることを背景に、ALGS (Autonomic Logistics Global Sustainment) という国際的な後方支援システムが採用され、全てのユーザー国が世界規模で部品などを融通し合うこととされている。このような国際的な後方支援の枠組みの構築を含め、国際共同開発・生産の今後の進展について、注視していく必要がある。

参照 Ⅲ部2章4節 (防衛装備・技術協力)

また、諸外国による防衛装備品の海外輸出も冷戦期から行われてきたが、近年も多くの国々が海外輸出の促進策をとっている。近年の防衛装備品の開発・生産コストの高騰を背景に、海外輸出に

よる海外での需要拡大によって自国の防衛産業を維持・強化することを目的としているほか、輸出先国に対する影響力の拡大など一定の外交的ツールとして利用しているとみられる。また、中国や韓国などは、これまでの防衛装備品の輸入や科学技術力の向上にともない武器製造基盤が整ったことで安価な防衛装備品の輸出国となり輸出を拡大している。

なお、近年、アジア太平洋地域への防衛装備品の輸出が増加しているが、その背景には、アジア太平洋地域の経済成長のほか、中国の影響力拡大や領有権をめぐる争いの存在、近隣諸国の軍事力発展への対応などと指摘されている。

参照 図表 I-2-6-1 (主要通常兵器の輸出上位国 (2010-2014年))

図表 I-2-6-1 主要通常兵器の輸出上位国(2010-2014年)

国名	世界の防衛装備品 輸出における シェア (%) 2010-2014年	2005-2009年との 輸出額の比較 (%)
1 米国	31%	+23%
2 ロシア	27%	+37%
3 中国	5%	+143%
4 ドイツ	5%	-43%
5 フランス	5%	-27%
6 英国	4%	+23%
7 スペイン	3%	+32%
8 イタリア	3%	+37%
9 ウクライナ	3%	+73%
10 イスラエル	2%	+33%
11 スウェーデン	2%	+23%
12 オランダ	2%	-32%
13 カナダ	1%	+16%
14 スイス	1%	-12%
15 韓国	1%	+14%
16 ノルウェー	1%	+110%
17 トルコ	1%	+149%

(注) 「SIPRI Arms Transfer Database」をもとに作成。シェア1%以上の国のみ表記(小数点第1位以下は四捨五入)。

9 欧米諸国の防衛産業の大手企業においては、総売上高に占める防衛事業の比率が高く、特に米国と英国においては、総売上高の大部分を防衛事業が占める大手企業が存在する。