

## 令和時代の安全保障を考える(下)

黒江 哲郎

近年における先端技術の飛躍的発展は、令和時代の我が国の安全保障政策に極めて大きな影響を与える要素であると考えられます。

軍事の新たな領域と言われる宇宙・サイバー・電磁波は、現代戦闘において人間で言えば目や耳、更には脳や神経と言った重要な機能を果たしていることが指摘されています。例えば、大規模な軍隊の移動や弾道ミサイル発射に関する動きといった戦略的な活動は衛星によって宇宙から常に監視されていますし、個々の戦闘機や艦艇の動き、あるいはミサイルの飛翔といった戦術情報や作戦情報はレーダーなどにより詳細に把握されます。これらの情報は通信衛星を介して瞬時にやり取りされ、収集された膨大な情報はコンピューターで迅速に処理され、短時間のうちに必要な部署に共有されます。これを受けて必要な命令が下され、戦場では高度にシステム化された装備による戦闘が行われ、例えばミサイルはレーダー波や GPS 信号などのアシストにより極めて高い精度で目標に命中することになります。相手よりも優れた五感や脳や神経を有していれば圧倒的に有利ですし、相手の脳や神経を妨害したり混乱させたりすれば相手は十分な能力を発揮することが出来ず、我が方が優位に立つことが可能となります。

さらに、現在、各国の軍においては無人装備の導入が進んでいます。将来的には AI などの活用により人間の判断を介さずに自律的に相手を殺傷する兵器すら出現するのではないかと懸念も生じています。人間に例えれば、優れた五感に加えて痛みを感じない肉体を持つ無敵の兵士が誕生するようなものです。こうした情報通信分野やロボット、無人装備などの分野におけるテクノロジーの飛躍的な進歩は、軍の戦い方や戦闘様相、さらには軍事力の行使そのものの意味や形態にも大きな影響を与えることとなります。

ここでは、軍事科学技術の進歩とこれに対する対応、技術進歩が促進する自衛隊の統合強化、さらに軍事技術が飛躍的に進歩する中で我が国防衛の基本原則の一つである「専守防衛」をどう考えるべきかについて、私見を述べたいと思います。

### **軍事科学技術の飛躍的進歩がもたらす戦闘の変容**

軍事科学技術の飛躍的進歩は、既に以下に示すような戦闘に係る様々な要素に影響を与えています。

第一に、平時と有事との境界が不明確なものとなりつつあります。我が国の法体系の下では、従来、自衛権を発動できるタイミング、すなわち有事に移行するタイミングは相手方が我が国に対する武力攻撃に着手した時点であるとされてきました。しかし、サイバー攻撃が広がることによりそのタイミングを特定することは困難になって行きます。一般社会においては既にインターネットを利用した情報・財物の窃取などのサイバー犯罪が現実のものとなっており、軍事の世界でも情報の窃取や伝達の妨害・かく乱、さらにはシステムの誤作動を狙う攻撃などが日常的に企図され実施されています。しかも、サイバー攻撃の主体を特定するのは困難であるため、

たとえ攻撃に気づいたとしてもそれが誰によるものかを確認するのは容易ではなく、知らないうちに他国の国家意思に基づく我が国に対する侵害が始まっているかも知れないのです。さらに、サイバー空間を利用して偽情報を流すことにより相手国内の世論を誘導・操作し、戦略的に優位に立ち、場合によっては戦わずして戦略目的を達成することさえ不可能ではありません。2016年(平成28年)の米大統領選に対してロシアがSNSなどを通じて介入したと疑われているのは、このような攻撃の典型例です。

第二に、テクノロジーの発達が武力行使のハードルが下げる危険があります。例えば、サイバー攻撃に対してどのような手段でどの程度の反撃が許されるのかといった点については依然として議論が定まらずそれぞれの国が明確な基準を共有している訳ではないため、国家として自衛権を発動して反撃するという決定にためらいが生じる恐れがあります。攻撃する側の立場に立てば、攻撃の形跡が見つけられにくく反撃される危険性も低いとなると、サイバー攻撃を発動する敷居は低くなります。

同様の危険性は、ドローンなどの無人兵器についても指摘できます。今やドローンの使用は世界中で民間分野のみならず軍事分野でも急速に広がっていますが、こうした無人兵器を用いれば、兵員を直接危険にさらさずに難しい任務を遂行できます。実際、2019年(令和元年)9月に発生したサウジアラビアの石油施設への攻撃にはミサイルとともにドローンが用いられたと伝えられています。従来は味方の兵員の損耗リスクが軍事力行使を思いとどまる大きな要素となっていました。しかし、無人装備は有人の航空機と比較して圧倒的に安価であり、捕獲されたり撃墜されたりしても攻撃側はほとんどコストがかからずリスクも感じないため、軍事力行使の敷居が低下する恐れが懸念されるのです。

第三に、高度な技術と装備は軍の作戦や戦術、さらには国家の戦略の変化を促すこととなります。例えば、領空侵犯に無人機が用いられるような場合、無線で呼びかけて近傍の飛行場に着陸させるというような従来の対処法は無意味ですし、小型無人機が大量に飛来してスワーム飛行をするような場合、現在の防空態勢で有効に対処することは不可能です。

あるいは、サイバー攻撃については従来主として情報通信システムを始めとする重要な軍事インフラに深刻な打撃を与える危険性について指摘されてきました。しかし、最近では軍の指揮官や兵員個々人の無力化を狙った本人や家族に対するマイクロの攻撃の危険を警告する考え方も出てきています。

2011年(平成23年)、テロとの闘いの中で米国はパキスタンの隠れ家を急襲してウサマ・ビン・ラーディン(UBL)を排除しました。この作戦に関しては、当時のオバマ大統領ら米政権幹部がホワイトハウスでその帰趨を見守っている写真が有名になりました。これは、パキスタンで実施されているUBL排除作戦をワシントンにおいてリアルタイムでモニターできるだけの情報通信インフラが当時既に整備されていたことを意味します。通信技術の向上が情報の伝達速度を飛躍的に向上させた結果、その適否は別にして理論的には大統領が現場の作戦の細かい指揮を執ることも可能となったと言えます。

同様のことは、情報分野でも起こり得ます。私が現役の頃には、衛星が宇宙から撮影した

偵察画像は、戦場においてリアルタイムで用いられる戦術情報ではなく、国防組織や国家首脳が戦略的判断を下すために用いられる戦略情報として区分されていました。しかし、センサー技術や通信技術が向上し情報の処理・伝達の手速がさらに短縮されれば、従来戦略情報として使われていた衛星画像を戦場の現場で戦術情報として使用することも可能になると考えられます。

このように、テクノロジーの発達は、戦闘様相を根底から変え、軍事組織における情報、通信、指揮命令などの在り方を抜本的に見直す契機にもなり得るのです。軍事科学技術の絶え間ない進化の下、既成概念にとらわれない柔軟な発想によって戦略、戦術、作戦などを不断に見直していくことが求められます。

### 我が国の装備技術政策の課題

先端技術は現代戦の様相を大きく変え、戦争の帰結を左右すると言っても過言ではありませんが、この分野においても中国の軍民融合をベースとした発展は顕著です。中国に後れを取らないためには我が国が今まで以上に努力せねばならないのは当然ですが、それだけにとどまらず多国間協力による技術研究開発を追求していくことが必須であると言えます。とりわけ、同盟国たる米国との共同技術研空開発は多国間協力の中心に位置づけられます。政府は、安全保障上必要な防衛装備技術の国際共同研究開発などを推進するため、平成 26 年(2014 年)に武器輸出三原則を見直し、新たに防衛装備移転三原則を定めました。

日米間ではこれまで弾道ミサイル防衛用の能力向上型ミサイル SM3-Block II A の共同研究開発に成功しており、さらなる共同研究開発の拡大発展が期待されているのですが、防衛装備移転三原則の新設から既に 5 年を経た現在でも残念ながら SM3-Block II A に匹敵するようなプロジェクトは開始されていません。これにはいくつかの原因、それも主として日本側における要因があるように思われます。

第一に、防衛装備面における民間技術・デュアルユース技術の活用の不足です。ドローンや AI の例からも明らかな通り、民間技術・デュアルユース技術の軍事活用は世界的な趨勢となっています。中国は言うに及ばず、米国においても国防省が先進的な民間技術へのアクセスを強めるべく努力を重ねているのに対し、我が国においては未だに技術研究開発において軍民を峻別し、軍事を忌避する傾向が根強く存在しています。軍事忌避の雰囲気は企業を過度に委縮させ、民間企業側から防衛装備分野に積極的にアプローチしようという意欲を削いでいるものと思われます。残念ながら短期間でこうした状況を改善するのは困難ですが、企業経営者間で安全保障に関する問題意識を共有してもらい取り組みや、防衛省と民間企業との間における研究者、技術者の人的交流などを地道に進め、「軍事アレルギー」を克服していく必要があります。

第二に、防衛サイドのニーズと民間の先進技術のマッチングをはかるために必要な防衛省の体制が不十分なことです。陸海空自衛隊が現に保有する装備品については既に研究開発から装備化までのプロセスが確立しており、装備の更新の時期が来ればほぼ自動的にそのブ

ロセスが動き出します。しかし、民間企業の有する最先端技術をウォッチし、有望な技術があればそれを迅速に装備化したり、ゲームチェンジャー的な防衛装備を考案したりするための体制や仕組みは十分ではありません。また、サイバー、宇宙、電磁波、弾道ミサイル防衛などの比較的新しい分野は、どの自衛隊が担当するのか明確ではなく、既存装備に比べて調達プロセスもスムーズとは言えないように見受けられます。防衛省において、民間の最先端技術をモニターし、防衛上のニーズとのマッチングを試みるような責任ある部署を整備するとともに、民間技術の進展の速さに追従し得るよう短期間で装備化を可能とする仕組みを拡大して行くことが急務と言えます。

第三に、我が国の民間企業においていわゆる産業セキュリティの体制が十分に確立されていないことが、米国企業との技術提携や共同研究開発を阻害している面があると思われます。日米で共通の秘密保全態勢が確保されていなければ、技術情報の十分な共有は期待できません。現在の MDA 秘密保護法や特定秘密保護法などの法的枠組みや契約条項によって十分に秘密を保全し得るか、早急に検討する必要があります。

我が国の研究開発政府予算が米国や中国、EU などと比べて十分な額とは言えないことは既に様々な形で指摘されていますし、さらに政府の研究開発予算がただでさえ少額である中で防衛関係が占める割合はわずか 3%程度でしかありません。現在の厳しい財政事情の下でこうした資源配分が大きく変わらないとすれば、民間技術・デュアルユース技術の活用を図っていくことはまさに喫緊の課題であると言えます。

2017 年(平成 29 年)、我が国は豪州の潜水艦プロジェクトへの競争入札で仏企業に敗れました。敗因については様々な分析がなされており、得られた教訓は次の機会に生かされるものと期待しますが、いきなり完成品の輸出を目指したのはハードルが高過ぎた面があるのかも知れません。我が国産業界には数々の優れた技術があり、それを生かして例えば他国の防衛用装備品の重要な構成部品を供給することは十分に可能と思われます。完成品や一体化されたシステムの輸出にはなお時間がかかるとしても、部品の形で他国の重要な装備品のサプライチェーンに食い込み、我が国の安全保障上の地位を高めていくことは今後の一つの方向性と考えます。比較優位のある技術を伸ばして国際競争力を高め、我が国防衛装備の高度化につなげていく現実的な知恵が求められています。

### 技術進歩がもたらす戦術・作戦レベルでの統合強化

現代戦においては、陸・海・空の統合運用がますます重要になっています。これまで多くの場合、異なる軍種が一つの戦略目標を共有し、各軍のアセットをそれぞれ別個独立に運用して共通の目標を達成することが統合運用と呼ばれてきました。大規模災害に際して、陸自が地上で人命救助や生活支援を行い、海自が艦艇で避難民を輸送し、空自が輸送機で救援物資を空輸し、トータルとして災害救援を成功させる、というような作戦が典型例です。

他方、近年の軍事科学技術の進歩、装備のネットワーク化の進展は、戦略レベルのみならず戦術・作戦レベルでの統合運用を促進させています。例えば、航空機のセンサーが低空を

飛来するミサイルの動きをつかみ、その情報に基づいて、はるか遠方に所在する艦艇や陸上部隊が自らの有するセンサーの情報に頼らずに迎撃ミサイルを発射し、効率的に敵のミサイルを撃墜するようなことも可能となりました。つまり、一つのミサイルに対して、空自の航空機がつかんだ目標情報に基づき、海自の艦艇や陸自の高射部隊が迎撃する、ということです。最近就役した海上自衛隊のイージス艦「まや」は、このような共同交戦能力(CEC)を有する初めての護衛艦です。今後、航空自衛隊の早期警戒機 E-2D に CEC が搭載されれば、ここで述べたような戦術的な統合運用が現実のものとなります。

周辺諸国において弾道ミサイルや巡航ミサイルの開発・配備が進んでいる中で、持てる装備を総動員して効率的・効果的にミサイル脅威に対応するためには、上に述べたような統合的な対応が必要不可欠です。これを実現するには、三自衛隊が脅威認識を共有し、装備品の研究開発段階から統合運用を重視すること、個々の装備やシステムを結ぶ共通のネットワークの整備を急ぐこと、共通装備品の導入を積極的に進めることなどがが必要です。

通常、各自衛隊の作戦に関する時間感覚は全く異なります。例えば、空自の戦闘機、海自の艦艇、陸自の戦車部隊は、それぞれ特性の異なる別個の敵を相手にしているため、戦闘が推移する速さもこちらが対応するスピードも全く違います。この違いは、各自衛隊の装備の性能や作戦の考え方、ひいては部隊編成や組織文化の違いにもつながっています。しかし、弾道ミサイルや巡航ミサイルのような共通の脅威に対して各自衛隊のアセットを効率的に組み合わせ統合的に対応する場合には、各アセットが共通の時間感覚に従い共通の作戦に基づき共通のネットワークを利用して行動することが必要になります。そのような作戦においては、各アセットがどの自衛隊に所属しているのか、あるいは各アセットを操作する人間がどの自衛隊の制服を着ているかという点にあまり大きな意味はなくなります。

従来、統合強化の必要性は理解されても、実際にはなかなか円滑に進みませんでした。私自身も現役時代に情報や運用など様々な統合プロジェクトに携わって来ましたが、各自衛隊が互いに「統合運用といっても、有事になったら他の自衛隊を支援する余裕はなくなり、自分のところを優先するのではないか」との疑念を持っているのが感じられました。限られた予算の下、それぞれが自己完結的に戦うことを優先し、他の自衛隊の支援を計算に入れずに装備体系を構築してきたため、相互の信頼が十分に形成されなかったものと言えます。このような従来型の防衛力整備は、各自衛隊それぞれの権限、予算、人員などの既得権益化をもたらし、統合に対する消極的姿勢につながっていたものと思います。

しかし、統合幕僚監部が新編されて既に 10 数年が経過し、統合任務部隊を編成して活動する経験も重なってきました。最近の防衛装備庁の新編により、装備品の設計段階から統合運用の観点を反映させる試みも加速されてきました。今後、脅威の変化に対応して戦術・作戦レベルでの統合運用がさらに強化されて行けば、組織やカルチャーの違いは自然に相対化されざるを得なくなるでしょう。これにより、予算や人員を優先度の高い正面に臨機に振り向けるような柔軟な組織運営、柔軟な防衛力整備も可能となることが期待されます。

逆に、各自衛隊が従来の組織文化や独自の作戦の考え方に過度にこだわり戦術・作戦レ

ベルでの統合強化に消極的な姿勢をとるようであれば、軍事科学技術の進歩に後れを取り、ミサイル攻撃やサイバー攻撃など切迫した脅威に対応出来る体制の構築は遠のくこととなるでしょう。そればかりではなく、出口の見えない少子高齢化や極めて厳しい財政状況の下で硬直的な防衛力整備を続けることとなり、自らの首を絞めるに等しい結果を招くものと懸念されます。

1998年(平成10年)、英国国防大学(RCDS)に留学していた私は、研修の一環として英軍の常設統合司令部(PJHQ)を訪問する機会を得ました。その際、「日本も統合運用強化に努めているが貴国ほどの成果を上げていない。統合運用を成功させるためのアドバイスがあれば聞かせてほしい」と質問したところ、英国陸海空各軍の将官が居並ぶ中、PJHQの幕僚は「なんて危険な質問だ」と苦笑した後、真顔になって「ポイントは実戦経験だ。現代戦を経験すれば各軍は統合運用の必要性を実感する。英軍は実戦経験によって統合を強化してきた」と答えました。

我が国は英国と同じような意味で実戦を数多く経験している訳ではありませんが、昨今の自衛隊は大規模災害派遣や海外任務、あるいはグレーゾーン事態に対応するための警戒監視や情報収集などの機会を通じて着実に実動の経験を積んでいます。軍事科学技術の飛躍的発展の後押しを受けて、ミサイル防衛を含む防空作戦、サイバー防衛作戦、長距離機動作戦など戦術・作戦レベルでの統合運用をさらに推進し、積極的に三自衛隊間の垣根を取り払っていく必要があります。

### 軍事科学技術の進歩と「専守防衛」

30大綱(「平成31年度以降に係る防衛計画の大綱」(平成30年12月18日国家安全保障会議・閣議決定))は、今後とも「日本国憲法の下、専守防衛に徹し、他国に脅威を与えるような軍事大国にならないとの基本方針」等の下で平和国家として歩んでいくと宣言しています。

他方、現実の防衛力整備や防衛政策の実施・展開に当たっては、しばしばこれらの基本方針、特に「専守防衛」との整合性に関する議論が提起されてきました。例えば、30大綱を巡っては、「いずも」型護衛艦の改修が憲法上禁じられているいわゆる「攻撃型空母」の保有につながるのではないかとこの疑問が提起されましたし、いわゆるスタンド・オフ防衛能力の保有が専守防衛の基本的考え方に反しないか、という点も議論になりました。

「いずも」に関して言えば、これを改修して10機程度の短距離離陸・垂直着陸戦闘機F-35Bを運用できる機能を持たせ、太平洋側を含めてより安全かつ効率的に我が国の海と空を守ろうとするものです。憲法上保有を禁じられているのは「性能上、もっぱら相手国の国土の壊滅的破壊にのみ用いられる兵器」としての「攻撃型空母」であり、米国のニミッツ級のように70機以上の戦闘機や攻撃機などを搭載している大型の空母がこれに当たると考えられます。これと比べれば「いずも」型護衛艦を改修して戦闘機の離発着が可能となったとしても、規模からして憲法上禁じられた「攻撃型空母」には当たらないことは明白です。これに対して「規模の大小にかかわらず空母を持てば他国へ攻め入る危険がある以上、専守防衛に反する」という極端な議論もあります。しかし、それでは島国で国土が狭小な割に広大な管轄海域(領海及

び排他的経済水域の広さは世界第6位)を保有する我が国が効率的に領域を守ることは困難となってしまいます。

スタンド・オフ防衛能力とは、脅威圏外(相手レーダーの監視範囲やミサイルの射程範囲の外)から相手を攻撃できるような射程の長い兵器のことです。こうした長射程の兵器は、米軍のトマホークミサイルのように相手国領域内の目標に対する攻撃にも使われ得るため、日本国憲法が海外での武力行使を原則として禁じていることやひいては専守防衛の考え方に反するのではないかと、との議論を呼びます。しかし、軍事技術水準が向上し兵器の長射程化が進んでいる中で、自衛隊の装備のみ射程を制限するのであれば隊員の安全を確保することは出来ず、ひいては国を守ることも出来ません。

専守防衛とサイバー戦との関係という問題もあります。既にサイバー攻撃は我が国の官民間問わず様々なシステムに対して日常的に行われていることが確認されていますが、真の攻撃主体が見えにくいという特性があります。先に述べたように、既に外国から我が国に対する急迫不正の侵害が行われているのかも知れないのです。さらに、攻撃主体が物理的に海外に存在している可能性は十二分にあります。このような攻撃に対して、どこの誰(攻撃主体が海外にいることも十分考えられます)を狙って、どの時点で、どのような手段を使って反撃すれば専守防衛の考え方に合致するか、これはとても難しい問題です。

専守防衛とは、「相手から武力攻撃を受けたときにはじめて防衛力を行使し、その態様も自衛のための必要最小限にとどめ、また、保持する防衛力も自衛のための必要最小限のものに限るなど、憲法の精神に則った受動的な防衛戦略の姿勢」(令和元年版日本の防衛 p.202)であり、独立国としての自衛権行使の在り方や保有すべき防衛力についてある意味でもっともな指針を示したものと言えます。諸外国の軍事力と比べて過大な防衛力である場合、例えば明らかに自国防衛ではなく外征を目的とした部隊を保有したり攻撃的な兵器を揃えたりしているような場合には専守防衛に反することもあるでしょう。しかし、逆に諸外国の軍よりも自衛隊の能力が劣るようであれば、そもそも国を防衛することは出来ません。

私は、専守防衛という概念自体を抜本的に変えるべきだとは思っていません。自国が攻撃された時のみ軍事力を行使し、決して先制攻撃に及ばないという考え方は十分合理性があり、いかなる国も遵守すべき普遍的なルールであるべきだと思います。ただ、専守防衛の概念は従来とかく謙抑的に解釈される傾向があったと思います。過剰に抑制的に解釈すれば自らの手を縛ってしまい国の防衛を全う出来ないという本末転倒の結果を招きかねません。この問題については、専守防衛という基本理念は維持しつつ、諸外国の軍事力の量や質、特に軍事科学技術の飛躍的發展という事実を客観的に把握した上で、それらに対応して我が国を防衛するためにどのような整理が可能なのか、冷静に議論することが必要と考えます。

(以上)