火箱コラム　13

能動的サイバー防御法成立の意義と課題

理事長　火箱　芳文

はじめに

令和7年5月15日「重要電子計算機に対する不正な行為による被害の防止に関する法律（サイバー対処能力強化法）」及び「重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（同整備法）」が成立した。陸・海・空領域の他にサイバー空間、海洋、宇宙空間、電磁波領域等において脅威が広がっており、特に攻撃側が優位にあるサイバー攻撃は巧妙化・深刻化し、重要インフラの機能停止や破壊、他国の選挙への干渉、身代金の要求、機微な情報の窃取等は国家を背景とした形でも平素から行われている。また、ウクライナ侵攻にみられるように、武力攻撃の前から偽情報の拡散等を通じた情報戦・認知戦が展開されるなど、軍事目的遂行のために軍事的、非軍事的な手段を組み合わせたハイブリッド戦が今後更に拡大される。

日本においても、特に、重要インフラの機能停止や破壊等を目的とした国家を背景とする重大なサイバー攻撃は、安全保障上の大きな懸念となってきた。このため政府は「国家安全保障戦略」（令和4年12月16日閣議決定）に「サイバー安全保障分野での国家としての対応能力を欧米主要国と同等以上に向上させる」と明記し、サイバー対処能力の向上に向けた取り組みを進めてきた。成立した「サイバー対処能力強化法」及び「同整備法」は重要な安全保障政策上の前進であり歓迎したい。国家安全保障戦略には「武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、またこのようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入」とうたわれ、本法は「能動的サイバー防御法」とも呼ばれ、日本のサイバーセキュリティ政策は画期的な転換点を迎えた。攻撃を受けてから対処するのではなく攻撃が実行される前に食い止めるというアプローチは、欧米主要国では常識になりつつある中で、武力攻撃を受けて初めて防衛力を行使する「専守防衛」の呪縛から離れ、日本もようやく欧米主要国に追随するための大きな一歩を踏み出した。ただし、いくつかの課題もあり、本稿では「能動的サイバー防御法」の意義と今後の課題について考えてみたい。

1　巧妙化・深刻化するサイバー攻撃

サイバー攻撃は、2005年内閣官房情報セキュリティセンター（NISC）を設置した頃には、愉快犯レベルの公開サーバーへの攻撃であったが、その後、システム内部へ侵入してシステム障害を発生させたり、身代金を要求するなど、

組織的、悪質なものに変遷してきた。２０１４年に日本もこれらに対処するためサイバーセキュリティ基本法が施行され、翌年ＮＩＳＣも改組強化されたが、政府や民間企業などの協力連携は、ほとんどなされておらず、それぞれが依然受け身の体制で対応してきた。その後世界的に高度の侵入能力・潜伏能力を持つウイルスなどの出現により、重要インフラ等の最深部・制御系システムへのサイバー攻撃が行われるようになり、更に最近では機密情報の漏洩・悪用のための機微な情報窃取の危険が懸念され、益々サイバー攻撃は巧妙化・深刻化し、質・量両面にわたりサイバー攻撃の脅威は増大してきている。攻撃を受けてから対処するアプローチでは、国家を背景とするような高度で組織的な攻撃に対処しきれないという課題が顕在化してきた。

2　能動的サイバー防御法の意義

「サイバー対処能力強化法」及び「同整備法」は、①官民連携の強化、②通信情報の利用、③攻撃者のサーバー等への侵入・無害化措置、④ＮＩＳＣの発展的改組等新たな組織・体制整備等で構成されている。

この法律の評価すべき一つ目は、従来武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合に、受動的に守るだけでなく、積極的に攻撃源を特定・妨害し脅威を排除するための、能動的サイバー防御という考えを初めて導入したことである。これにより、サイバー攻撃またはその疑いがある場合の被害の拡大を防止するための攻撃者のサーバー等への侵入・無害化措置ができることになる。今まで「専守防衛」を基本としている日本は、攻撃側にアクセスして攻撃源を特定することすらはばかっていたが、状況によっては武力攻撃に至らないサイバー攻撃にも自衛隊が無害化（攻撃）までできることになった。

二つ目は、能動的サイバー防御を含む各種取り組みを実現するため、サイバーセキュリティ戦略本部の改組、機能強化、内閣サイバー官の設置、警察・自衛隊の強化など司令塔機能、情報収集・提供機能の強化を図る等サイバー防御体制を拡大整備することである。

三つ目は政府、自衛隊、基幹インフラ事業者等ごと独自のサイバー攻撃対応をしていたところを、重大インシデント等情報共有・対策のための官民合同協議会の設置等、国家一丸となってのサイバー防衛能力の強化が図れるようになったことで、ようやく欧米主要国が先行する取り組みに追いつこうとしている。

3　今後の課題

サイバー防御体制の強化には、質の高いサイバー要員の確保が最も重要である。アクセス（侵入）・無害化措置を実際に実行する組織の警察及び自衛隊は、平素からサイバー関連企業などとも連携し、常時サイバー攻撃に使用される電気通信を情報収集して分析作業を平素から実施しておく必要がある。自衛隊のサイバー関連要員は２０２４年度末で２４１０

人、２０２７年には４０００名に増強する予定であり、十分ではないが一定の評価はできる。一方、陸海空自衛隊の現体制（定数）を維持したままで、サイバーという特殊な技能を有する要員を４０００名に増強することが、果たして可能か。現在陸自サイバー通信学校で陸・海・空自のサイバー要員を育成しているが、サイバーには極めて高い技術レベルの要員の入隊が不可欠であり、要員数も確保する必要がある。質・量ともに２０２７年までの本格運用に間に合うかどうか、心配している。一方で、サイバー要員の内部からの選考や新しい部隊等の創設などにより、一般部隊の要員の減少が問題化している。速やかに国家防衛戦略、防衛力整備計画の見直しを行い、陸・海・空自衛隊の定数や実員の増強を行わなければならない。

能動的サイバー防御と警察権の縛りについても検討する必要がある。通常のサイバー攻撃は警察が対処し、自衛隊は「外国からの組織的、計画的なサイバー攻撃があるかそのおそれがある場合」、総理大臣の命により警察と共同して通信防護措置を実施する。また「日本国にある米軍の電子計算機に対する通信防護措置」についての日米同盟上の役割もある。改正自衛隊法にもサイバー対応の行動類型が盛り込まれたが、更なる一歩を進めてもらいたい。

サイバー攻撃は日本では武力攻撃の範疇に含まれていないため、対応する自衛隊の行動は警察行動である。日本への侵攻を企てる国は、あらゆる手段を使って攻撃を仕掛けてくることを覚悟しておかなければならない。防衛出動が下令されない限り、自衛隊の行動はすべて警察活動の延長として武器使用に関わる警職法の縛りがかかる。サイバー攻撃は、電子計算機というある種の兵器を使った攻撃であり、重要インフラ等の人的・物的被害規模によっては「武力攻撃」に該当する場合があり、武力攻撃の範疇に含ませて考えるべきではないか。国を背景とする組織的なサイバー攻撃が行われた場合、これに対処するには、早期に防衛出動が下令され、サイバー空間への反撃及び発信元への反撃が指向できるような国の防衛体制が望ましい。国の安全保障を警察行動と防衛行動に区別している国は先進国では日本だけである。このため今後自衛隊法の検討を進め、防衛出動以外の、その他の行動から警職法の縛りを外し、総理大臣、防衛大臣の定める部隊行動基準（交戦規則＜ＲＯＥ＞）に従って行動できるように自衛隊法を抜本的に改正すべきである。

最後に

専守防衛の呪縛を離れ、能動的サイバー防御へ大きく舵を切ったことから、防衛政策の基本方針である「専守防衛」という正式用語を廃止し、例えば「能動防衛」、「積極防衛」、「即動防衛」などを正式用語に使用してみてはいかがかと思う。これは些細なことと思われるかもしれないが、国民の安全保障意識を啓蒙する一助にもなり、憲法改正の必要性の議論にもつながることにもなる。