◎くにまもりの提言㊷◎

現代情勢が炙り出す 能動的サイバー防御の優先度

八尋（やひろ）滋（しげる）
（しがく総合研究所）

デジタル化が進展した現代社会において、サイバー空間は国家安全保障の新たな戦場となりつつあります。かつてはウイルス対策ソフトやパッチ適用といった受動的な防御策が中心でしたが、今日では攻撃者の戦略が高度化・多様化しており、先手を打つ「能動的サイバー防御」が急務とされています。特に、国家や重要なインフラに対する攻撃が現実の脅威として取り沙汰されるなか、政府は有識者会議を設置し、関連する法案を閣議決定するなど、政治の場でもその必要性や運用方法について議論が交わされています。

サイバー攻撃は単なる技術的問題ではなくなっている

２０００年代初頭から、サイバー攻撃は国家間の緊張を背景に進化してきました。２０１０年に明らかになった、イランの核燃料施設を狙ったマルウェア攻撃は、技術と戦略の双方で新たな脅威を突きつけました。さらに、２０１３年には、アメリカ国防総省の情報機関であるＮＳＡの職員、エドワード・スノーデンが「ＮＳＡにより世界中の通信データが監視されている」と暴露し、各国の情報収集体制が改めて問われる結果となりました。

そして、２０２２年2月に始まったウクライナ侵攻では、従来の軍事力と並び、サイバー攻撃や偽情報といった非伝統的手法が組み合わされたハイブリッド戦が展開され、現代の戦争のあり方に大きな衝撃を与えています。サイバー空間における攻撃は単なる技術的問題に留まらず、国家戦略の再定義を迫るものとなっているのです。

能動的サイバー防御の必要性とその課題

能動的サイバー防御とは、平時からサイバー空間を常時監視し、攻撃の兆候を早期に察知して迅速に対応する手法です。たとえば、

通信を常時監視して怪しい通信パターンの検出をしたり、疑わしい相手のシステムに侵入して無害化したりする措置がその一例です。これにより、攻撃の拡大を未然に防ぎ、相手のさらなる攻撃を抑止する効果を期待できます。

しかし、こうした能動的サイバー防御アプローチは、技術面での整備だけでなく、法制度や運用ルールの整備といった側面も不可欠で、国内では憲法上の課題もあります。まず、「通信の秘密」を保障する憲法21条は、国民のプライバシーや表現の自由を守る重要な規定です。平時に通信の監視や特定のデータ収集が行われる場合、その適用範囲や監視の透明性について慎重な議論が必要です。また国家の安全保障を担保するため、憲法9条の専守防衛の枠組みの中で、攻撃を未然に防ぐ能動的対策をどのように位置づけるかは、今後の憲法解釈にも大きな影響を与えます。具体的には、敵国のシステムへ侵入する行為が先制攻撃と認定されるリスクや、専守防衛の枠を逸脱する可能性があり、さまざまな論点をクリアにするための法整備が求められます。

日本は防御の体制整備が遅れている

現代の安全保障環境では、ウクライナでのハイブリッド戦の実例が、能動的サイバー防御の意義を改めて浮き彫りにしています。ロシアは、地上戦、空軍、ミサイル攻撃といった伝統的な軍事力に加え、サイバー攻撃、偽情報など複合的手法を駆使し、戦略的優位を狙っています。このような複合的脅威に対抗するためには、伝統的な軍事力の増強や能動的サイバー防御の技術向上はもちろん、迅速な法改正、官民連携、さらには高度な技術を持つ人材の育成が不可欠です。

ただ、現状の日本の体制は、欧米先進国と比べ整備不足との指摘があり、国家全体での連携強化が急務となっています。国家安全保障の柱として能動的サイバー防御を位置づけるには、単に技術面の充実だけでなく、先に触れたような憲法との整合性などクリアすべき課題は山積しています。サイバー空間は平時と有事の境界が曖昧なため、実際の運用において迅速かつ柔軟な対応が必要となります。さらに、日本国内だけではなく国際的な情報共有や連携体制の構築により、単独では対抗が困難なサイバー脅威に対する多国間協力の枠組みを整備することも重要です。国家安全保障の柱の一つとして能動的サイバー防御をするためには、防衛、法律、ＩＴ、政治といった各分野の専門家の視点を集約して総合的な安全保障を実現するための高度なリーダーシップが求められるのです。