技術総説

日本のサイバー防衛とこれからの技術

ファイア・アイ株式会社　最高技術責任者（CTO）
前経済産業省 サイバーセキュリティ・情報化審議官
元陸上自衛隊システム防護隊　初代隊長
工学博士
伊東　寛

サイバー防衛に関する日本の現状と課題

サイバー技術は現在も極めて早いテンポで進展中であり社会を変えつつある。仮想通貨に代表される金融の改革もそうだし、量子コンピュータの発達は数年以内に暗号技術に大変な変革をもたらすかもしれない。そして、人工知能の発達とビッグデータの利用も重要である。これを最初に牛耳ったものが世界を制覇するであろうと、米国や中国がその開発に莫大な資金を投じているのは周知の通りである。また北朝鮮がこの分野で非合法な外貨稼ぎの手段として活用しようとしているらしいことも噂にのぼっている。

これらの流れの中で、サイバー技術の軍事利用に関しても例外ではない。諸外国の軍隊は「サイバー戦」に注目し、組織・装備などを編成強化中のところである。中国は戦略支援部隊というサイバーを担当する独立兵科[1)]を2015年末に新編した。米国は統合軍としてのサイバーコマンド[2)]をもっているし、陸軍には職種としてのサイバー科がある。

一方、わが国、自衛隊の状況であるが、近年、サイバー重視の指針が出され部隊を強化中であるとはいうものの、各種装備品のシステム化への要求や指揮統制システム等、各種システムの充実への要求が高まる一方で、そのために必要とされる装備品の研究開発と配置、人的戦力の育成が追いついていない。さらに一般的な短期間の人事異動のためもあり、十分な技術的知識をもった隊員を常時適切な部署に配置することも困難な状況である。

特にその頭数については、防衛省によれば、北朝鮮約7,000人、ロシア約1,000人、中国は宇宙と電子戦を含めて約13万人といわれているという[3)]一方で、日本は100～200人程度と、その勢力は仮に任務が違う[4)]としても目を覆いたくなるような少なさである。

このように日本は、サイバーに関する組織的戦力が、まだまだ不十分な状況下にある。しかし、わが国にはこれまで培ってきた優れた科学技術と優秀な人材があり、特にサイバー技術については世界に遅れている分[5)]、その潜在能力

1）日本にはない概念であり、陸海空軍よりは下だが、歩兵科、戦車科などの兵科よりは上位の組織。
2）2018年５月、サイバーコマンドは独立した軍に格上げされ独立した統合軍のひとつとなった。
3）『偕行』平成31年１月号「日本の防衛力６」（偕行社安全保障研究委員井上氏）
4）日本の自衛隊はサイバー空間において国家国民を守るという任務を明示されていない。
5）例えば、世界に通用するレベルの日本を代表するセキュリティ企業はどこか？という問いに対し、残念ながら即答しにくいというのが現実である。

を有しているといってよい。そうであるならば、日本のもつサイバー技術力はまだこれから発展の余地が多大にあり、それはすなわち日本の戦略的資源であるということがいえるかもしれない。すなわち、人が少ないという問題点を技術力でカバーし列国に追いつき追い越す可能性をもっているということだ。

防御ラインが１線、２線、３線と増えていったが、浸透戦術や戦車、飛行機など、次々と新しい攻め方が出現

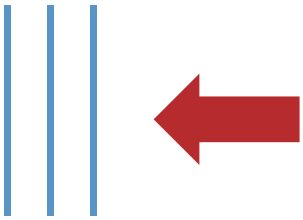

図１　多層防御では守りきれない

軍事の歴史や防御の要領から学べることがある

本誌読者の大半は、軍事の専門家か関係者だと思うので、サイバーセキュリティに関する以下の話は特に興味深いと思う。それはサイバーセキュリティに関して軍事の歴史や理論から学べることがあるということだ。

戦いにおいて、昔は敵の大将の首をとれば勝ちだった。その後、大勢の兵が正面からぶつかり合うような戦闘様相が長く続いた。やがて銃の発明などにより、日露戦争の頃には塹壕というものが発明された。つまり線で守るようになった。それは、その後、攻撃側の新しい技術や戦法が発達するに伴って、１線ではなく２線、そして３線と多層で守るようになっていくわけである。新しい攻撃要領とは、例えば第一次世界大戦におけるドイツの浸透戦術、あるいはイギリス軍が最初に利用した戦車の利用だ。その後の技術の進歩は飛行機を生み出し、空挺部隊というものも発明された。飛行機で敵の陣地線の後ろに出てしまえば、塹壕も地雷原も関係ない（**図１**）。

このような新しい攻撃要領に対しては、単純な多層防御では守りきれないようになった。その後、冷戦中には全縦深同時打撃などの新しい攻撃要領も生まれ、防御側は、防衛線ではなく地域全体で防御する必要性が生まれた。敵が我

攻撃要領はさらに進歩し第１線から後方の兵站部隊まで打撃する方式まで現れた

図２　全縦深同時打撃