電子戦の現状と課題

元海将補
飯田　俊明

はじめに

皆さんは、電子戦というと、何を連想するでしょうか。飛んでくる対艦ミサイルに何か電磁波を照射すると、ミサイルが海に墜落するとか、戦闘機が敵のミサイル基地を攻撃する時に、妨害装置を搭載した戦闘機が、敵のミサイルを発射するためのレーダーに電波を照射して、ミサイルを発射できなくするといったことを連想するかも知れません。それは間違いではありませんが、電磁波の利用が軍隊や政府機関に限定されていた時代から、携帯電話やスマートフォンの様な通信機器のみならず、信号機や家庭用ガスボンベの残量通知の様な生活のインフラから家電の制御（IoT）にまで広がってくると、電子戦の範囲は極めて多様で広くなることは想像がつくと思います。多くの方は生活のインフラまで？と思うかも知れませんが、サイバー攻撃や電磁波攻撃で銀行のシステムが停止し、交通機関や電力等の公共インフラが被害を受ける可能性は極めて高く、電子戦が自衛隊の艦艇や戦闘機だけの問題だとは言いきれません。国内では、違法電波の発射が行われず、皆がルールを守っているという前提が我々の生活を安泰に見せているだけで、その前提が崩れると極めて重大な事態に陥ることに気付かなければなりません。事実、2014 年のロシアによるクリミア侵攻時には、生活インフラのみならず、ラジオ、テレビ等のメディアまで、何らかの影響があって、生活だけでなく心理的な面まで影響されたことが報告されています。世界には、電子戦を総合的な戦略の主要手段として平時から利用しようとしている国もあるのです。

上記の内容のなかにも、実は注意深く見なければいけないことが隠れています。例えば、電波で管制している信号機の場合、電子戦的な視点では、何か妨害を与えて単に誤作動をさせる場合と、信号を管制する（例えば赤、青、黄の切り替えタイミング等）データの構造に具体的な影響を与えて、一見通常の作動をしているが、異常な状態を作為することが可能になります。この例えから導きだされることは、

- 通信や電磁波の使用には情報が伴っている
- 冒頭のミサイル攻撃やレーダー基地に対する妨害の様な、攻撃的な要素だけが電子戦ではない

ということです。

軍事では、あからさまに妨害をしていることが分かれば、対策を行い、妨害を行なっている部隊が攻撃されるので、最近では一見通常の動作をしているが、異常な状態を作為することが一般的になりました。技術的にこのような事が可能になってきていることと、敵も味方も何らかの電磁波に依存しているので、敵の電磁波の利用を阻害しながら、味方の電磁波の利用を維持するためには、敵と味方が対峙した空間全体をブラックアウトさせるような方法は使えなくなりました。湾岸戦争では、米海兵隊の妨害機が妨害をかけたところ、米陸軍

と同盟国軍の通信器材やデジタルで作動する一部の器材に不具合が起きました。これらの器材は、初期化とセットアップという処置をして元に戻しますが、作戦の遂行に致命的な時間とデータが失われたようです。パソコンのリセットと再立ち上げを連想してください。

１　電子戦とインフォーメーション（情報）ということについて

かつては、電磁波をオンオフさせるモールス符合で意思の疎通を行っていましたが、今では大量のデータがデジタル形式で、しかも高速で授受するようになりました。モールスの時代もそうでしたが、誰もが受信できる電磁波で生の情報を交換することは、悪用される恐れがあるので暗号を掛けて関係者だけが意味を分かるようにしました。第二次世界大戦の頃は、この暗号を解くことに努力を注ぎ、戦略的な優位性は敵国の暗号を解読できるかどうかに掛かっていました。日本の海軍はアメリカのレベルの低い通信に使用される一部の暗号は解読できましたが、重要な通信に使用されている暗号は解読できませんでした。まして、日本側はアメリカに暗号が解読されているとは認識していなかったので、多くの戦いの作戦段階から、不利な立場に立たされました。太平洋戦争を「情報で負けた」という人がいるのはこのような事情があるからです。しかし、暗号のように電磁波の伝える内部的な情報ではなく、何時、どこから、どのぐらいの量の通信が行われたかといった、通信行為そのものが表す情報を活用した人達がいました。日本海軍では、主に学徒動員で海軍に参加した、英語に堪能だった人たちが、このような業務に関わっていました。敵信班と呼ばれていました。例えば洋上である軍艦が電報を発信し、これを二つの受信局が受信し、電波の到来方向がわかれば、概略艦艇の位置が分かることになります。このような作業を通じて得られたデータを集積していくと、目標の行動の軌跡や、複数の艦艇の集合離散が見えるようになります。データから生じたインフォーメーションです。太平洋戦争中、サイパンの方向から特定の時間に多くの電波が飛来する事象がありましたが、これは B-29 が日本本土空襲の離陸前に無線機の試験をしていたのです。日本側は、これを空襲警報のために利用したと言われています。そしてこのようなインフォーメーションを集積して分析することで、敵の意図を推定していました。今でいうインテリジェンスです。日本海軍の連合艦隊には、情報幕僚という配置はありませんでしたし、敵信班の活動も、制度化されていなかった気配があります。どのような経緯で始まり、どのような実績があったのか大変興味があります。戦後 GHQ は、敵信班の活動に高い関心を持ち、調査を行っています。

ここで少し横道にそれますが、情報にとって大事なことを指摘させて頂きます。それは「情報」とは何かという問題です。ちなみに、上記の説明に出てきた「インフォーメーション」、「インテリジェンス」について、英和辞書で引いてみると、「インフォーメーション（Information）」と「インテリジェンス（Intelligence）」は共に「情報」となります。それでは「情報」を和英辞書で引くと、大体が「Intelligence」に翻訳されます。「情報」という言葉は、明治以降「情況を報せる」という意味で使われてきましたが、用語として体系的に使用したのは森鴎外だったと言われています。鴎外はドイツのクラウゼヴィッツの『戦争論』を

翻訳するときに「整理する」という意味の言葉に「情報」を当てはめました。「データを整理してインフォーメーションを作成する」プロセスに相当し、意味もインフォーメーションの意味でした。ところが明治、大正、昭和と時代が推移するにつれ、軍の中で「情報」は、「インテリジェンス」を表わす言葉に変化していきます。「インテリジェンス」には「諜報」という言葉がありますが、少し語感が良くないのと、暗号を解読できず大した成果のなかった関係者が自己の業務の内容を高く見せようとした結果ともいわれています。言葉は人間の思考の手段です。言葉の欠陥は思考形態の欠陥、強いては国家の制度、戦略にまで影響します。我々には、データからインフォーメーションに至るプロセスが言語的、文化的に欠けているということに気付かされます。「情報」という単層構造で組織や制度を考えるのと、「データ」、「インフォーメーション」、「インテリジェンス」の三層構造で考えるのでは、大きな違いがあります。日本以外の国々では三層構造で考え、施策を行っていますが、日本ではまだ単層構造の考え方が一般的な様に見えます。言葉の混乱は現代にも至っていると思います。

２　戦術部隊と電子戦

軍事の世界で、データを収集し、インフォーメーションを作成するのは、自衛隊や海上保安庁の様な部隊です。なぜなら、軍事における現場（戦闘空間）でデータを収集する能力を持つためにはそれなりの装備が必要だからです。領土、領海、領空の前縁にいて「防衛」の一環として、データを収集し、インフォーメーションを作成して、自らの行動の判断に使用するとともに、重要なインフォーメーションを中央に報告することが求められます。多くの場合、データを収集する手段として電磁波が使用されます。つまり電子戦活動の一環となります。レーダーの様に自らエネルギーを発するセンサーは、存在を相手に知らせてしまうことや、地球が丸く水平線以遠では探知できないからです。高さ 10m の高さから見る水平線は 20 ㎞未満しかありません。電磁波を感知するセンサーでは 500 ㎞位を能力範囲と考えるのが一般的です。

この様にデータを収集する行為を、電子戦の定義では「電子戦支援“Electric Warfare Support”（略して「ES」）と呼んでいます。また、このデータからインフォーメーションを作成する活動を“Information Operation”（略して「IO」）と呼んでいます。残念ながら、これに相当する日本語はありません。私は、電子戦の説明をするときに「インフォーメーション運用」もしくは「IO（アイオー）」と表現しています。日本海軍の敵信班は「IO」と同じことを実施していたことになります。現在、電子支援は世界の力関係において極めて重要な機能となっています。電子戦の領域では、米国の統合参謀本部が作成しているドクトリンが世界的な標準となっていますが、ドクトリンが記述された通称「統合教書」（“Joint Publication”略して「JP」）では、電子戦の三要素として、電子戦支援、電子攻撃、電子防御が定義されています。

電子攻撃は、電磁波を用いて攻撃すること全般を含んでおり、一般的な妨害以外に、電磁

砲やレーザービームの様な指向エネルギー兵器や、電磁波に信号を加えてミサイルの軌道を狂わせるような精密な運用等、広い範囲の事柄を含んでいます。また、電子防護は、敵の電子攻撃から友軍、同盟軍の人員、活動を保護する全ての活動を含み、電波封止の様な電波の使用の統制、使用する電磁スペクトラムの割り当て管理、保全といったことが含まれます。そして、電子戦支援は、脅威の警報（例えばミサイルの誘導波の検知）、データの収集、方位探知等が含まれます。電子戦だけにとどまらず、インフォーメーション運用、インテリジェンスの作成、更には国家の防衛、外交方針を支えるインフラの裾野に相当します。地道ですが重要な業務と言えます。特にここ数年、世界情勢の変化で日本にとって極めて重要になってきました。

３　電子戦と今後の課題

1989 年冷戦が終了しましたが、1990 年に湾岸戦争が始まります。ここで中国とロシアは西側、特に米国の軍事力の背景にある電子戦能力に注目したと言われています。その後、米国は軍事予算を大きく削減しましたが、同時に研究開発や戦術開発などもそのペースを落としてしまいました。この間にロシアと中国は電子戦能力の改革を大きく進めました。1999 年に始まったコソボ紛争（同年、米国爆撃機による中国大使館誤爆事件が発生している）や、2008 年の南オセアチア紛争（ロシア-ジョージア紛争）が両国に大きな刺激を与えたのは間違いないことでしょう。

ロシアは 2014 年のクリミア危機でその成果を十分に発揮します。西側は大きな衝撃を受け、電子戦能力を高めるための戦略策定に着手しました。現在シリアでは電子戦関係のセンサーを搭載したアメリカ、ロシア、中国、NATO のドローンが飛び交っており、空中衝突を起こすほどだといわれています。中国はドローンの輸出が世界一で、1,000 機以上を同時に管制する試験をしたと伝えられています。

中国は、ロシアの様な実行動を行っていませんが、接近阻止・領域拒否（“Anti-Access/Area Denial”、略語で「A2/AD」）という戦略を策定します。A2/AD の概念自体は新しいものではないのですが、中国がアメリカを敵と想定して、接近阻止戦略（A2）と領域拒否戦術（AD）を組合せ、アメリカ軍が侵入することにリスクを感じる領域を設定し、中国に有利な状況を創り出すことを狙いとしています。しかし問題は、日本が中国とアメリカの A2/AD 領域の中間に位置しているからです。日本として、またアメリカの同盟国として何をすべきかが、現在大きな課題となっています。

アメリカ国防省は、2010 年の議会報告で「エアー・シー・バトル」構想を明らかにしました。この構想は、空軍と海軍の連携の上で A2/AD に対応しようとするものです。この中で、米国は「中国軍が米軍 のアキレス腱として捉えているのは、米軍の兵力展開の基盤となる前方展開基地及び航空母艦、そして戦闘基盤である C4ISR 機能です。中国軍は、これらを封殺することによって米軍の戦力展開の基盤を喪失させ、更に情報戦（心理戦及びメディア戦）の一環として世論を惹起し、中国への介入を断念せざるを得ない状況に陥らせることを

狙っている」と分析しています。つまり、日本に存在する米軍基地の攻撃、つまり日本に対する攻撃が想定されていることになります。それも戦争の前哨戦としての攻撃になるので、奇襲攻撃になる可能性が大きいと言われています。日本の地理的な位置から、A2/AD における平時からの活動が、相手に間違った判断をさせないために非常に重要になると言われています。アメリカのエアー・シー・バトル構想で分析しているように、戦闘の基盤である C4ISR 機能のうちの ISR（Intelligence, Surveillance, Recognizance: インテリジェンス、監視、偵察）は相手の攻撃に至る意思決定のエスカレーションを阻止する効果があるといわれています。ISR は、平時からインテリジェンスを作成するデータ収集を基盤とする一連の活動と、電磁スペクトラムや目視等の多様な領域でのデータの収集を継続して実施する監視業務、衛星等を使用した偵察業務を意味します。衛星による偵察業務は国家レベルで検討されていると思いますが、各自衛隊や海上保安庁等の戦術部隊が関わるインテリジェンスのための基盤業務と監視業務に必要となる、電子戦能力の充実は極めて重用な意味を持つことになります。特に、日本には文化的にインフォーメーションの概念が希薄であり、データを収集する能力に加え、これからインフォーメーションを作成する能力整備も重要であると思います。電子戦の持つ意味と範囲は大きく変化しています。日本では、フォークランド紛争の後に電子戦能力の向上に尽力した時期がありましたが、改めて尽力すべき時期にある様に思います。