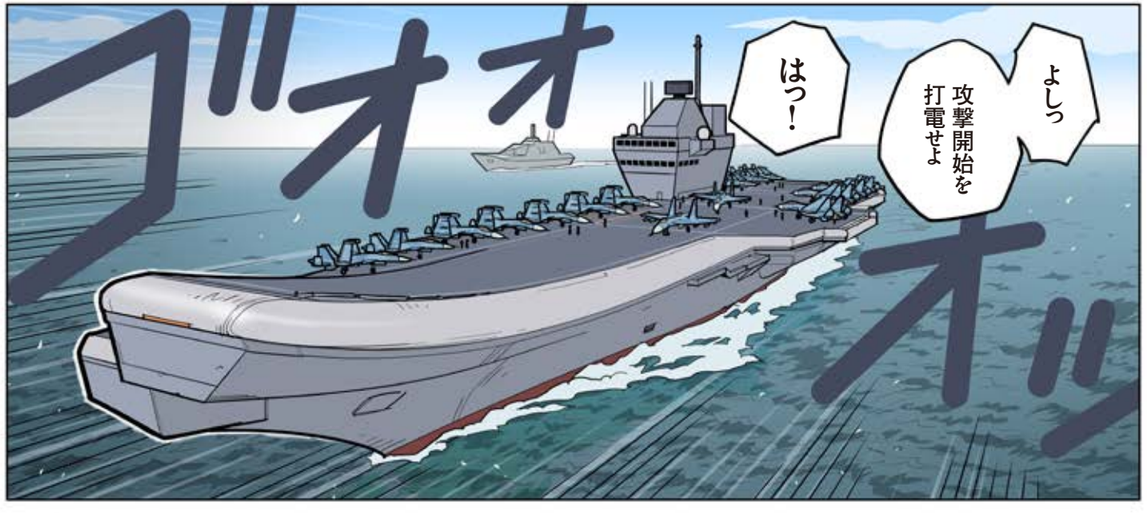
ネットワーク戦闘入門

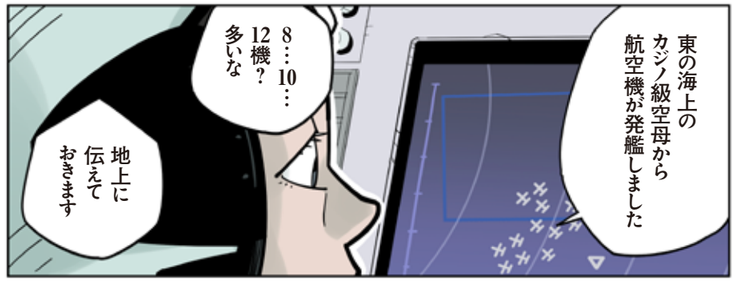
NETWORK CENTRIC WARFARE

漫画：おぐし篤
Cartoon By Atsushi OGUSHI

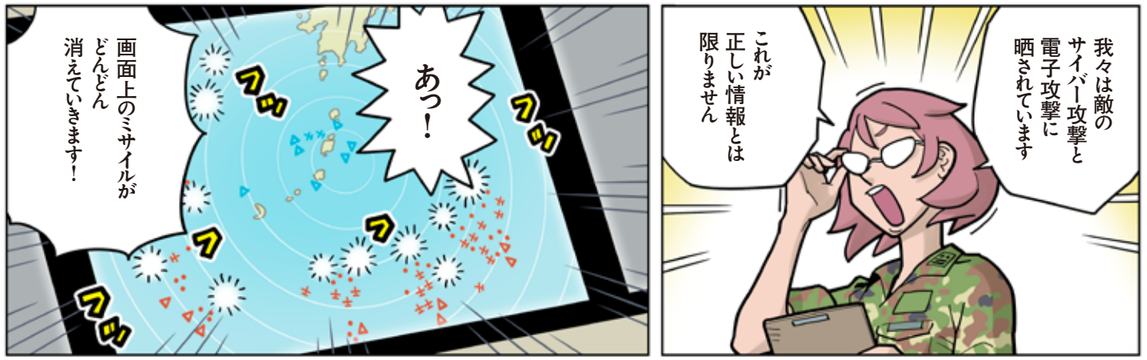
軍隊や自衛隊の基本的な構成は「陸・海・空」だけど、現代戦は目に見えないところでも展開する。そのひとつが「ネットワーク・セントリック・ウォーフェア」（Network Centric Warfare）、日本語にすると「ネットワーク中心の戦闘」だ。航空機、艦艇、レーダー、ミサイル、指揮所といった、ひとつひとつの装備や機能が通信でつながったとき、いったい何が起こるのか？ 目に見えない戦いに、マンガと解説でアプローチしてみよう！

第4回 サイバーと電波の攻撃

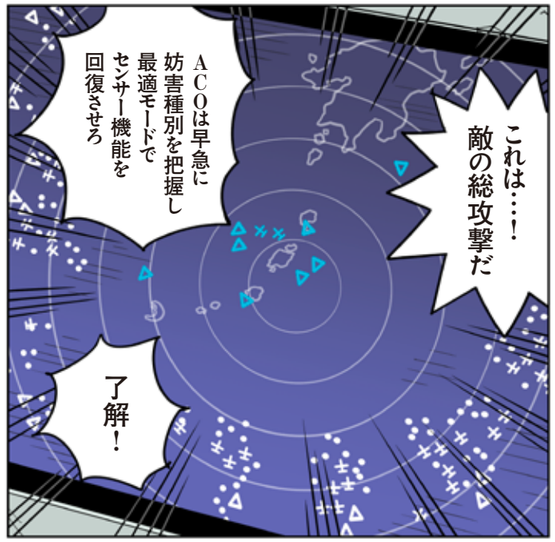


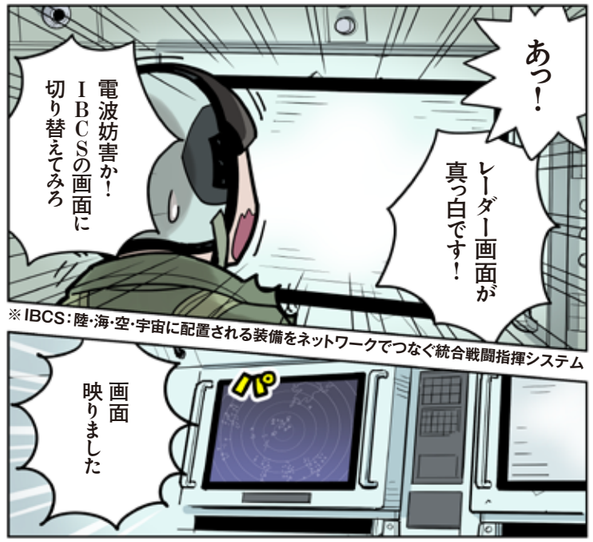


※CAP：戦闘空中哨戒。上空で周りを監視する任務



SAM：地対空ミサイル





※IBCS：陸・海・空・宇宙に配置される装備をネットワークでつなぐ統合戦闘指揮システム

※ACO：空中管制士官。E-2DではCICO（戦闘情報士官）、ACO、RO（無線操作員）の3名の管制官が役割を分担する

サイバーにも電波系にも強いんです

抗堪性は世界水準 IBCS

連載4回目にしてようやく、「初めからこうすればよかったのに」と言いたくなるような総攻撃が始まった。今回の作戦は現代戦のスタンダードな手順を踏んでいる。つまり、サイバー攻撃と電子攻撃からはじまり、制空権を確保し、地上部隊が制圧に向かう。しかし、どうやらサイバー攻撃も、電子攻撃も、IBCSに阻まれて限定的な成果にとどまってしまったようだ。

同じではないサイバー攻撃と電子戦

近年、一緒くたに扱われる場面が増えていると感じる「サイバー戦」と「電子戦」だが、この両者、センサーや情報通信・指揮管制システムの能力低下や無力化を企図している点では、確かに共通性がある。しかし、戦闘を仕掛ける対象と手法が全く異なる点には、注意する必要がある。

電子戦の対象は主として、レーダーのような電波兵器と、無線通信。どちらも電波を用いるところは共通しており、探知に使うか、それとも通信に使うかという違いになる。その電波を直接的に操作して、「敵軍の作戦行動を阻害する」という目的を達成しようと目論むのが、電子戦の特徴といえる。

たとえばレーダーであれば、強力な妨害電波をぶちかまして、本来、探知を成立させるための反射波を正常に受信できないようにする手法がある。また、本来の反射波とは違うタイミングでニセの反射波を送り込んだり、違う方位からニセの反射波を送り込んだりすることで、実際には存在しない探知目標を発生させる手法も考えられる（マンガの中にもそういうシーンがある）。通信を対象とするのであれば、強力な妨害電波をぶちかまして、通信そのものを成立できないようにする方法がある。

一方、サイバー攻撃は主として、コンピュータと、そのコンピュータ同士がやりとりするデータがターゲットになる。コンピュータの動作を妨げたり、コンピュータを過負荷にしたり、コンピュータからデータを盗み出したり、コンピュータにニセのデータを送り込んだりする手法がポピュラーだ。

ちょっと乱暴な例えだが、「郵便物を送り届けようとしたときに、配送そのものの邪魔をするのが電子戦で、郵便物の中身をすり替えたり書き換えたりするのがサイバー戦である」と考えればいくらか理解しやすくなるのではないか。

なお、無線通信に対しても、通信そのものに割り込んでニセ通信を仕掛ける手法がある。第二次世界大戦中にイギリス軍がドイツ軍の防空部隊に対して仕掛けた手法だが、攻撃のやり方・考え方からすると、これはサイバー攻撃に近いといえるかも知れない。

ともあれ、現代の電波兵器や通信システム、コンピュータ・システム（もちろんそれには、IBCSのような指揮管制システムも含まれる）は、電子戦やサイバー戦を仕掛けられても耐えられること、という要求がついて回る。

なぜニセ目標を捨てることができるのか

以前の本連載でも解説してきているように、IBCSは複数のセンサー（レーダーなど）をネットワーク化して、それらから集まってくるデータを融合することで、単一の状況図を生成する。

もしも、そのセンサーの中のどれかが電子戦によって混乱させられたとしても、電子戦を仕掛けられていないセンサーからの情報と比較することで、どれが二セ目標なのかを判断する材料ができる。

たとえば、同じ空域においてレーダーAが20個の探知目標を捕捉したのに対して、レーダーBが50個の探知目標を捕捉したとする。その差分はどこから湧いて出てきたのかという話になるわけだ。そこでレーダーBが電子戦によってニセの探知を得ていたり、サイバー攻撃によってレーダーの情報処理が混乱させられていたりしている、という判断ができれば、「健全なのはレーダーAである」となる。すると、レーダーAの情報を活用することで、レーダーBに湧いて出たニセ探知を排除できる。

これは、複数のセンサーをネットワーク化して、かつ、それらのデータを融合していなければ実現できないことだ。

電子戦は、レーダーだけでなく通信にも影響する。通信を標的とする電子戦に対処するためには、妨害に強い無線通信技術が必要になる。実は身近なところでも、無線LANやBluetoothが、似たような技術を用いている。特定の狭い周波数範囲で通信を行う代わりに、広い周波数範囲に「薄めて」通信を行ったり、使用する周波数をコロコロ変えたりといった手法がそれ。もちろん後者の場合、通信を行う双方が同調して周波数を変換しないと、通信が成り立たない。

IBCSの開発に際しては、電子戦による妨害を受ける場面を想定した試験も行われている。ただし、「実際にどのようにして、敵軍が仕掛ける電子戦に対処しているのか」という話になると、これはもっとも機微に触れる、公にできない部分。だから、メーカーとしても口をつぐまざるを得ないのは仕方のないところ。ここでは「濃密な電子戦環境を想定した試験でも、IBCSはちゃんと機能できた実績がある」と書くに留めておく。

サイバー攻撃に強いシステム

先に述べたのは、「電子戦によってニセ目標があると勘違いさせられた場合の対処」である。サイバー攻撃によってニセ目標があると勘違いさせられる可能性もあるが、その場合には手法が異なる。

まず、レーダーのシグナル処理（アンテナで受信した反射波を解析して、探知目標の位置や針路や速度を計算する）を担当しているコンピュータに、攻撃用のプログラムを送り込んで実行させなければならない。すると、そのソフトウェアがシグナル処理の機能を「乗っ取って」、実際には存在しない目標をでっち上げる。

こうした種類の攻撃に対しては、「そもそも、『不正なプログラムを送り込ませない』『不正なプログラムの存在を速やかに認識して排除する』といった機能が必要になる。パソコンやスマートフォンで、アンチウィルス・ソフトウェアを走らせるのと似ている。

これもやはり、具体的に「どうやってサイバー攻撃に対処しているのか」という話になると、公にできない種類の話になってしまう。しかし、IBCSに限らずその他の米軍のウエポン・システムでも、さまざまなサイバー攻撃を想定した設計・開発・試験が行われているのは公知の事実だ。

また、IBCSは同じネットワークの中に複数の指揮所（EOC）を設置できる。これは、どれかひとつのEOCが破壊されても、他のEOCによって機能を継続できるという利点につながるが、物理的な破壊に限らない。もしも万が一、サイバー攻撃によってどこか特定のEOCが機能を喪失するようなことになったら、どうするか。複数のEOCを用意しておけば、機能を喪失していないEOCによって任務を継続できる、というシナリオも考えられよう。

■サイバー攻撃と電子攻撃

今回の作戦で攻め手は、守り手の迎撃システムを機能不全に陥れるため、最初にサイバー攻撃と電子攻撃を実施した。

サイバー攻撃は、電子端末の通信網を通じて、相手のシステムに対し攻撃をおこなうものだ。相手のシステムを不調にさせたり過剰な負荷を与えるデータ攻撃、相手のシステムに取り込まれることで誤作動などを引き起こすソフトウェア攻撃（トロイの木馬やワームなど）、相手のシステムに直接入り込んで破壊活動や乗っ取り、データの窃盗などをおこなうハッキングがある。今回のマンガの場合は、守り手の一部のシステムに障害を引き起こすことに成功している。

電子攻撃は、強力な電波を発信したり、欺瞞した電波を発信することにより、相手の通信機器や捜索・監視レーダーの能力低下、無力化を狙うものだ。今回のマンガの場合は、電波妨害（ジャミング）によって通信障害を引き起こし、一部の監視レーダーの目潰しに成功している。

ちなみに電子攻撃（Electronic Attack）では、強力な電波を発信する機器を、標的に電波が届くところまで運ぶ必要がある。そのためには移動能力の高い航空機が使用されることが多い。下図は、アメリカ戦略予算評価センター（Center for Strategy and Budgetary Assessments: CSBA）の報告書からの引用で、大型装置による遠距離からのジャミング攻撃（スタンド・オフ・ジャム）と、無人機による近距離からのジャミング攻撃（スタンド・イン・ジャム）が同程度の効果をもたらすことを示したものだ。

※写真・画像はイメージです（写真：US Navy）

■電子攻撃に使用される航空機の例

アメリカ空軍のEC-130コンパスコール電子戦機。大きな機体に大きな機器を搭載し、さまざま電子妨害をおこなう（写真：US Air Force）

中国人民解放軍のY-9電子戦機。中国の電子戦技術は高度なレベルに達しており、J-15戦闘機などでも電子戦型をつくっている（写真：統合幕僚監部）

アメリカ海軍のEA-18Gグラウラー。胴体下と主翼下および主翼端に取り付けた電子戦ポッドでさまざまな電子妨害をおこなう（写真：US Navy）

アメリカ海兵隊のシャドー無人機。敵の近くまで近づいて無人機を飛ばせば、人的損害を心配することなく電子妨害を実施できる（写真：US Marines）