ネットワークと電磁スペクトラム管理

天貝　崇樹

１　はじめに

現代戦において、ネットワークが戦局に大きな影響を与えると考えられているのは、データリンクをはじめとする各種ネットワークが情報を共有する上で極めて有効な手段であり、それによって作戦を含めた各種行動を迅速に行うことが可能となるからである。

戦域では、センサーやシューターであるプラットフォームの性能向上に加え、通信方式、媒体となる電磁波や通信回線に改良が施され、戦術的ネットワークは日々進化し、新しいネットワークの構成によって戦術や作戦に変化が生じている。その一方で、ネットワークに対する脅威も顕在化し、ネットワークは、その構築以上に防護が焦点となりつつある。直接戦闘に関わらない基地機能を担うインフラ等のネットワークを含めて、である。

航空自衛隊を含めた防衛省でも多種多様なネットワークを指揮・統制の手段として利用しており、ネットワークが組織的な能力を発揮するための不可欠な存在となっている状況に鑑み、本論は湾岸戦争以降、変化するネットワークの役割や管理態勢を踏まえ、ネットワークに対する脅威について分析し、今後の方向性等について考察する。

２　ネットワークを巡る取組の変遷

湾岸戦争において米国を中核とする多国籍軍は、AWACS(Airborne Warning And Control System)、JSTARS（Joint Surveillance and Target Attack Radar System）[1] をはじめとする各種指揮・偵察監視システムとトマホーク等の精密攻撃兵器を連携させたネットワークを構成し、大きな戦果を上げた。米国ではその成果を踏まえ湾岸戦争後にシステム間の連携のさらなる強化が図られた。特に、このシステム・オブ・システムズという考え方は、AWACS、偵察衛星、JSTARS 等の「センサー」の情報をリアルタイム

で精密誘導兵器を運用する「シューター」と共有し、即座に攻撃することで戦闘効率を劇的に高める「センサー・トゥ・シューター」という観点から浸透していった。

こうした趨勢の下に、1998 年、海軍参謀部本部勤務だったセブロフスキー（Arthur Karl Cebrowski）海軍中将（当時）は、ネットワークによって状況認識を共有することで情報優位を作り出し、戦闘の優位を獲得するとした NCW（Network Centric Warfare）の概念を提唱した[2]。

2001 年 10 月、国防省に設立したトラスフォーメーション推進室（Office of Force Transformation: OFT）[3]は、「NCW の実現」と題した冊子において、NCW を「トランスフォーメーションのまさに核心」と表現した。当該冊子の中で、OFT は NCW を消耗型の戦争への依存から脱却し、統合作戦、EBO（Effect Based Operation）[4]、速度の俊敏性、火力の精密指向への移行を目指した米国のトランスフォーメーションの中心概念に位置付けている。

トランスフォーメーションは、1997 年に国防省の諮問委員会が「国防の変革（Transforming of Defense）」において提唱し[5]、科学技術の活用による戦闘力の向上を目指して検討されてきた概念であった。この構想の検討は国防省及び米軍の改革に本格的に着手したブッシュ政権にも引き継がれている。国防省は、2003 年、トランスフォーメーションを「非対称的な脅威から脆弱性を防護するため、概念、能力、人員及び組織を新しく組み合わせることで変化しつつある軍事的競争・協力（関係）を形作る過程であり、世界の平和と安定の維持に寄与するもの」と定義している[6]。

OFT は、このトランスフォーメーションの概念を具体化しつつ、その考えを広く普及すると同時に NCW という用語も一般的に広く認知してさせた。そして、2004 年に米国防省は、NCW を「情報優越により可能となる作戦コンセプトであり、センサー、意思決定者、シューターをネットワーク化することにより、認識の共有、指揮の速度増加、作戦テンポの迅速化、より大きな決定力、残存性の増加、そしてある程度の自己同期がもたらされ、結果的により大きな戦闘力が生み出されるとし、本質的に NCW は情報の優越を戦闘力に変換するものであり、戦闘空間において『効果的に連接された軍隊[7]』によって行われる」と定義した。OFT は、トランスフォーメーション

の概念とプロセスを主導するという任務を達成したとして2006年に閉鎖された。

この頃から、NCWの特性を理解した上でNCWを推進することが重要であるとの見方が出始めている。例えば2007年に米国議会調査機関（Congressional Research Service）が2001年のアフガニスタンと2003年のイラクにおける戦闘を踏まえて公表したレポート（以下「CRSレポート」という。）に、NCWが取り上げられている。CRSレポートは、NCWの利点として「センサーとシューターの連携時間の短縮」、「個々の部隊の潜在的な能力の向上」、「柔軟な作戦行動の推進」、「前線と後方の知恵の融合」等を挙げており、これらは既に米軍の作戦行動において当然の如く活用されていたものであった。その一方で、同レポートは、NCWが晴らすとした戦場の霧が容易に晴れず、情報を過信し敵を過小評価等している点を指摘しているほか、またサイバーや電子戦に対する耐性の不足等の米軍のNCWに対する能力への疑問も多く記述された[8]。

2009年12月、ゲーツ国防長官は論文「バランスのとれた戦略（A Balanced Strategy）」で当時の国防省戦略のバランス感覚の不足に対する疑問を提示し[9]、米国防戦略の見直しを訴えた。そして、コストと要求性能、開発期間の適切なバランスを強く求めつつもCRSレポートで認められたNCWの有効性を積極的に活用し現在の戦いを支える方針を示し、ISR（Intelligence Surveillance and Reconnaissance）能力、無人機の活用と情報処理分析への人的・財政的支援、ネットワーク維持のための宇宙アセットやサイバー攻撃への対処を重視する姿勢を打ち出した。

2010年2月に発表された2010QDR（Quadrennial Defense Review）では、「サイバー空間における効果的な作戦」とともに「アクセス拒否下における攻撃抑止と打破（deter and defeat aggression in anti –access environment）」が重点項目として掲げられ、遠方攻撃能力やC4ISR、宇宙アセットの強化が指示された。また、2013年に国防省から発表された作戦概念「エアシー・バトル」（Air Sea Battle: ASB）では[10]、その中心的な考えを「妨害、破壊、打倒するためネットワーク化され、統合された縦深攻撃」としている。これらのことから、NCWはその概念を時代に応じて変化・深

化させながらも実践されていると解釈することができる。

３　新しいネットワーク

現状において米軍では、新しいネットワークの構築により、従来は攻撃できなかった遠距離の目標に対する攻撃や各種プラットフォームによる組織的かつ効率的な攻撃方法の確立が試みられている。米海軍は、艦船では探知できない水平線下の目標に対して攻撃を可能とする海軍統合防空火器管制システム（Naval Integrated Fire Control-Counter Air: NIFC-CA）を開発している。これは、E-2D をセンサー、あるいは通信中継機として使用することで艦船レーダーの捜索範囲外で探知した脅威となる目標情報（巡航ミサイル等）を艦船に伝送し、艦船から発射されたミサイル等で破壊（迎撃）するものである（図１参照）。NIFC-CA は 2015 年に導入が開始されてからも試験等が行われており、F-35 をセンサー又は中継機として使用する計画も進められている[11]。

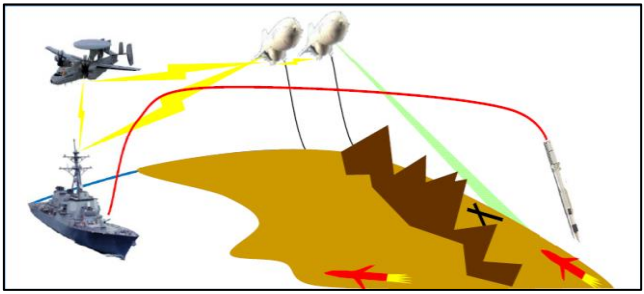

図１　NIFC-CA イメージ図[12]

また、防空及び弾道ミサイル防衛においてもネットワークの構築が進められている。弾道ミサイル及び巡航ミサイル並びに航空機の複合した脅威に同時に対応するためには、迅速に意思決定して我のアセットを効率的に運用する必要がある。米軍は、こうした要求を満たすために軍種を超えた一元的な指揮の下に航空機、ミサイル部隊を連携させて運用する防空ミサイル一体型防衛（Integrated Air Missile Defense: IAMD）の研究を行っており、本年４月、その一環である陸上の統合戦闘指揮システム（Integrated Battle

Command System）の試験に成功している[13]。

NIFC-CA や IAMD 等のセンサーとシューター、意思決定者を効率よく結びつける作戦レベルのネットワークの開発に加え、戦術レベルのネットワークや新しいネットワークも構築されつつある。米空軍では、F-22 の IFDL（Intra-Flight Data Link）や F-35 の MADL(Multifunction Advanced Data Link）といった同一機種の戦闘機間によるデータリンクが開発されている。これらの編隊内のデータリンクは、従来のネットワークよりも大量のデータを送受信可能であり、妨害に強い耐性を確保しながら操縦者の状況認識を高めることを可能としている。また、MADL は、従来から NATO で使用されているデータリンクとの共存を前提として設計されており、F-35 は NATO 諸国の作戦機等との相互運用性を確保しつつ共同作戦の指揮を担うことができるとされている[14]。これに加え、米国防高等研究計画局（Defense Advanced Research Projects Agency: DARPA）では F-22 の IFDL や F-35 の MADL などの同一機種間のデータ通信を従来の LINK-16 等のデータリンクと繋げる DyNAMO（Dynamic Network Adaptation for Mission Optimization）計画を発表しており[15]、引き続き、米軍は「個々の部隊の潜在的な能力の向上」等の利点を増大させる方向で NCW を推進している。

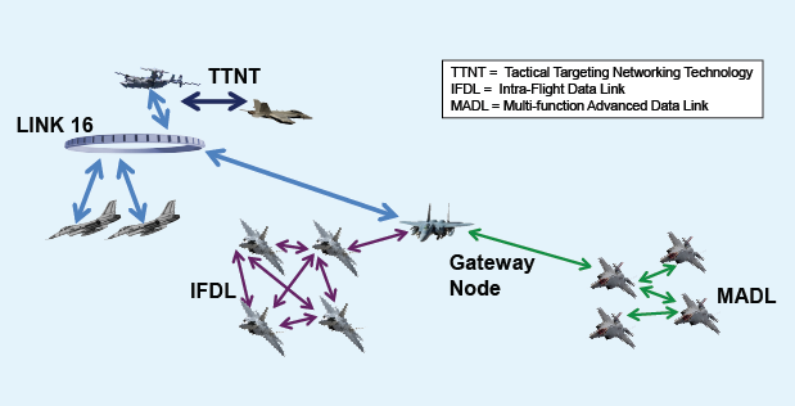

図２　DyNAMO イメージ図[16]

F-22 編隊間の IFDL、F-35 編隊間の MADL 及び LINK-16（TTNT を含む）の情報は、Gateway Node の航空機を介して共有される。

４　ネットワークに対する脅威

NCW は、「ネットワーク化された環境にある部隊の行動は、ネットワーク化されていない部隊の行動を凌駕する[17]」という考え方に基づくものであるため、逆にネットワーク化による相手の優位性を無効化しようとする動きも活発になっている。

2012 年に米軍統合参謀本部から発表された JOAC（Joint Operational Access Concept）では、最近の作戦環境のトレンドとして①兵器・技術の劇的な改善と拡散、②海外における米軍の防衛態勢の変化、③宇宙及びサイバー空間の作戦領域化の 3 項目を挙げ、敵の防空能力、サイバー攻撃能力及び電子戦能力の強化等によって米軍の戦力投射が妨害されつつあることを指摘している。このことは、我のネットワーク化により彼を凌駕するとした NCW の優位性が、我のネットワークに対する攻撃や敵のネットワーク化により減殺されつつあることを示しているといえる。

（１）電磁パルスの脅威

ネットワークが機能するためには、システムを構成する各機器が正常に働き、かつ、各機器間の通信が確保されることが前提となる。ある機器が電子回路の異常により機能不全となった場合、システム全体の機能喪失に繋がる場合がある。また、今日においてネットワークを構成する機器の殆ど全てに電子回路が組み込まれており、機器の電子回路の異常によるネットワークの不全は、防衛システムのみの問題ではなくなっている。

例えば、1989 年 3 月 13 日にカナダのケベック州で電力インフラが機能不全に陥り、州全体で大停電する事態が発生した事故は、強烈な太陽風（solar storm）が地球の電離層に到達して生成した電磁パルス（Electromagnetic Pulse: EMP）の影響によって地上の機器や電線などに異常が生じたことが原因であった。この復旧には約 1 日を要し、当時の地元新聞紙の計算によれば発電所だけで日本円にして約 7 百億円の損害に上ることが報じられている[18]。

こうした事例は、EMP が防衛システムを含むネットワークを構成する機器等にとって脅威であることを示している。そして、電子機器に多大な損害を与える EMP は、自然現象として発生するのみならず、人為的に効果の対

象や範囲を計算して生成する手段が確立されている状況にある。

高高度核爆発に伴う HEMP(High Altitude Electromagnetic Pulse)の発生や高出力マイクロ波（High Power Microwave: HPM）発生装置によって生成された EMP は、一定の範囲内に存在する電子回路に影響を及ぼすことができるとされている。実際、カナダの大停電は、地上における磁束密度 480nT/min の変化が 92 秒間続いたことによって電力グリッドが破壊されたことが原因といわれているが[19]、旧ソビエト連邦は 20 秒間にわたり 1300nT/min の磁束密度の変化を発生させる実験に成功し、地上や地下の送電線、電話線、発動機発電機、レーダーや無線装置などの電子機器の故障などをもたらしたことが記録されている[20]。また、こうした EMP による効果に着目した米軍は、特殊な高周波発生管を弾頭に組み込み、飛行経路付近の電子機器を攻撃する飛翔体兵器を開発している。

このような状況に加え、今日の EMP 兵器は、すでに軍や国家の専有物ではなくなっている。EMP 効果を生成する RF（Radio Frequency）兵器の製造は、必ずしも高額の費用や高度な技術を必要としていないため、比較的容易とされている。実際、EMP を生成する機能を有する TED（Transient Electromagnetic Device）と呼ばれる簡易的電磁装置の中には、出力の低さから効果範囲が限定されるため攻撃する目標の機器に接近する必要があるものの、通常のブリーフケースに収納可能なものがあるといわれている。このような TED を用いたテロリストの攻撃に対して警告が発せられている現状を鑑みれば[21]、防衛システムだけでなく、社会的な混乱の誘発を防ぐためにも総合的に EMP 対策を急ぐ必要があるだろう。

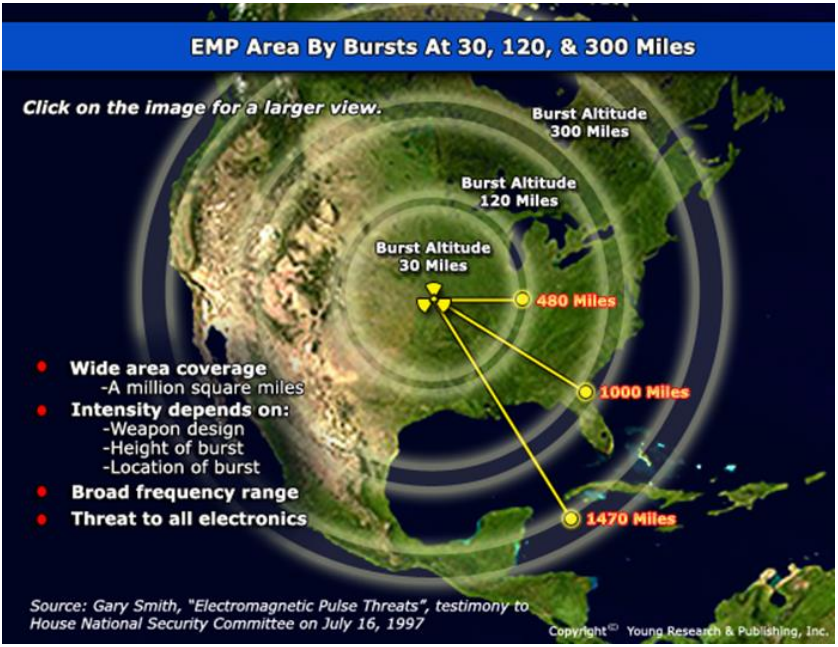

図３　EMP の効果範囲[22]

上空 300Miles（約 580km）で爆発した場合、EMP の効果は北米大陸のほぼ全域に及ぶ。

（２）電磁スペクトラムを利用したサイバー攻撃

EMP 兵器は、ネットワーク機能に致命的な影響を与えることが可能であり、ネットワークの脅威として位置付けられるが、現実的に使用された実績は確認されていない。その一方で、近年、EMP 以外のネットワークへの脅威である電磁スペクトラムを利用したサイバー攻撃（以下「電磁サイバー攻撃」という。）は、我の航空攻撃の支援や敵の兵器をろ獲するために用いられたと考えられる事例が発生している。

従来、敵の閉鎖されたネットワークとセンサーに対しては、電子戦によって制圧や欺瞞が行われていたが、センサーやネットワークの ECCM（Electronic Counter Counter Measure）能力の向上にともない、サイバー攻撃により相手のネットワークの内部に侵入してセンサーを制圧、或いは欺

瞞する活動が現実的に行われるようになっている。実際、2007 年におけるイスラエルのシリア原子炉攻撃及び 2012 年におけるイランの米国無人偵察機ろ獲事件は、その一例であり、電磁サイバー攻撃の可能性を示していると考えられる[23]。

イスラエルは、2007 年 9 月、シリアの原子炉を攻撃するにあたり、シリアの防空システムに侵入して攻撃機の被探知を妨害した。その際、イスラエルは、電磁スペクトラムを利用して防空システムに「偽」の信号情報を送り、シリア防空側の監視を欺いたとされる[24]。その結果として、イスラエルの攻撃機はシリア側に探知されず、一機の損失もなくシリアの原子炉を攻撃して破壊することに成功した。

また、2012 年 12 月、イランはアフガニスタン上空を飛行していた無人偵察機 RQ-170 と米軍の管制所との間の通信を妨害し、無人偵察機が自律航法による航行に切り替えざるを得ない状況を作為した。そして、妨害によって自律航行を余儀なくされた無人偵察機に対して、電磁スペクトラムを利用して偽の位置座標を送り自機の位置を誤認識させながら誘導し、指定した場所へ着陸させたと考えられている[25]。

こうした電磁スペクトラムを利用して無人機の遠隔制御や GPS 受信機等のソフトウェアの脆弱性を衝く攻撃は APT（Advanced Persistent Threat）攻撃[26]と呼ばれている。また、特に衛星通信の脆弱性は今日の課題となっており、無人機以外にも、米国では Landsat-7 と Terra EOS 衛星が 2007 年から 2008 年にかけて 2 回ずつネットワークに侵入されてアクセスを妨害されたことが 2011 年に発表されている[27]。

これらの事例は、ネットワーク化により ISR の能力が向上し、行動範囲が拡大し、攻撃精度がより緻密になったとしても、電磁サイバー攻撃によってセンサーの無力化、或いはネットワークを結ぶ通信を分断された場合、意思決定を正確かつ迅速に行うことができなくなる危険性を示している。

図４　イランが公開した RQ-170 の映像[28]

５　今後の方向性

JOAC では、敵の接近拒否／領域拒否（Anti-Access /Area Denial: A2/AD）能力を混乱させるために、陸、海、空、宇宙、サイバーの五つの作戦領域のうち一つ以上の作戦領域における優位を他の作戦領域で活用するとしており、とりわけ、空の領域を早期に獲得するとしている。また、宇宙及びサイバーの領域は、それ自身が作戦領域であるだけでなく、他の作戦領域への支援のためにも重要であることを記している。つまり、作戦初期において、航空優勢を獲得維持するには、宇宙及びサイバー空間における我の行動の自由も確保する必要があるといえる。

国防省は、無数のネットワークと結節から構成されるサイバー空間をハードウェア、ソフトウェアとインフラから構成される物理的ネットワーク層、物理的ネットワーク層によって形成される論理的ネットワーク層、論理的ネットワーク層に存在するアカウントやメールアドレスなどのサイバー人格層の３つの層に分類している。（図５のとおり）物理的ネットワーク層はコンピューター・ネットワークにおける情報収集（Computer Network Exploitation: CNE）を含めた SIGNT(Signal Intelligence)の場であることから、物理的な領域をサイバー空間における軍事的活動の入り口として位置付けている[29]。

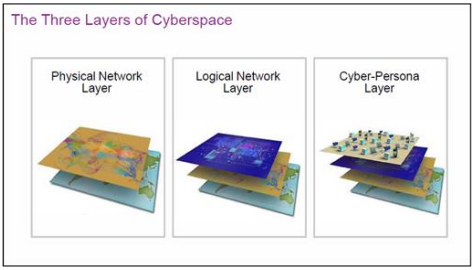

図５ サイバー空間における３つの層[30]

物理的ネットワーク層、論理的ネットワーク層、サイバー人格（仮想人格）層からなる。物理的ネットワーク層は、有線のネットワークと電子的（無線）ネットワークから構成される。

（１）航空優勢獲得のための宇宙及びサイバー領域での優位性の確保

彼のネットワーク化を前提として我が航空優勢を獲得するためには、前述のとおり、我のネットワークを保護し、敵のネットワーク機能を破壊する必要がある。そこで、JOAC のオペレーショナル・アクセスの指針では、敵の A2/AD 能力を混乱させるため、戦いの初期において宇宙及びサイバー領域での行動により奇襲をすることが想定されている。そして、奇襲を成功させる要件として、欺瞞（Deception）、秘匿（Stealth）、曖昧さ（Ambiguity）の３つが挙げられている。

ただし、このような宇宙及びサイバー領域での行動は、彼我双方が繰り広げるものでもある。言い換えるならば、我の航空優勢を獲得するためには、宇宙及びサイバー領域で敵のネットワークに対して奇襲でき、かつ敵の奇襲を拒否できる能力的な優位性を確保する必要があるということである。

宇宙及びサイバー領域は、位置情報、航法、時刻整合、指揮統制、ミサイル警報、天候予察、情報収集活動を支援する役割を担っていることから、これら２つの領域の優劣が、ネットワーク戦の攻防、ひいては航空優勢の獲得に大きな影響を与える。このため、宇宙及びサイバー領域における電磁サイ

バー攻撃の成否が重要になると考えられる。

一般的に、衛星通信は暗号化されておらず、車、携帯電話等の日用品のほか、発電所などの重要インフラ等が乗っ取られる危険性が指摘されている[31]。つまり、電磁スペクトラムを利用した通信によって構成されるネットワークと機器は、官民を問わず電磁サイバー攻撃の対象と成りうるのである。

米国では、国防省の出資を受けたバージニア工科大がジョージア工科大と無人機対ハッキング・システム（System –Aware Secure Sentinel）を共同開発し、デモ試験に成功させており、無人機に対する電磁サイバー攻撃への対策方法が確立されつつある[32]。また、DARPA は高信頼度サイバー軍事システム（High Assurance Cyber Military System: HACMS）を開発中であり、数学的手法で高い信頼性のある組み込みシステム（Cyber Physical System）の構築技術を確立することにより、サイバー攻撃に耐えうるシステムの構築を目指している[33]。現段階で HACMS は、軍の無人機を対象としているが、民間用にも作り直しており、こうしたことから軍民双方の電磁サイバー攻撃への対応が進むものと考えられる。

宇宙及びサイバー領域での優位性を確保するためには、電磁サイバー攻撃への対応が不可欠といえる。そして、電磁サイバー攻撃への対応は、ネットワーク上の脆弱性を巡る攻防でもあり、各国は脆弱性の克服等に取り組んでいるところである。我が国としても、このような電磁サイバー攻撃に対する脆弱性の克服等が必要とされているといえる。

図６　対ハッキング・システムの試験映像[34]

試験用 UAV に対ハッキング・システムを搭載

図７　HACMS の試験映像[35]

ロボットのオペレーティング・システムに HACMS を組み込んで行った最初の試験

（２）電磁スペクトラムにおける優位性の確保に向けて

ネットワークを巡る戦いは、これまで述べてきたように、電磁スペクトラムの領域の戦いといえる。敵の電磁スペクトラム活動の探知・制圧の可否と速度が電磁スペクトラム領域における戦いの優劣を左右する。米国では、2012 年の時点でこの重要性を認識し、米海軍作戦本部長だったグリーナート（Jonathan W. Greenert）大将は、宇宙及びサイバー領域での活動が他の作戦領域に大きな影響を与えることに着目、「電磁スペクトラムの領域における活動が戦闘の勝利をもたらす」とした論文を発表している[36]。2015 年、CSBA から発表された「Winning the Airwaves」では、彼我のネットワーク化が進んだ結果、米軍が築き上げてきた電磁スペクトラムの優位性が崩れつつあるという認識の下、再びこれを取り戻そうとする提案がなされている[37]。

米陸軍では、ネットワークにおける電磁スペクトラムの重要性に鑑み、サイバー空間・電子戦作戦（Cyber space and Electronic Warfare Operation）の概念を確立し、国防省ネットワーク内外のサイバー活動と EW（Electronic Warfare）の関係を整理し再構築している[38]。サイバー空間・電子戦作戦では、敵対勢力の電磁サイバー活動を捕捉し、拒否・無効化することで友軍の指揮系統を守り、サイバー及び電磁スペクトラム領域における友軍等の優位性の維持又は奪取するための活動をサイバー電磁活動（CEMA :Cyber Electromagnetic Activities）[39]と定義し、サイバー空間と電磁スペクトラム

領域における優勢の獲得を企図している。米陸軍が整理したサイバー空間・電子戦作戦の概念図は図８のとおり。

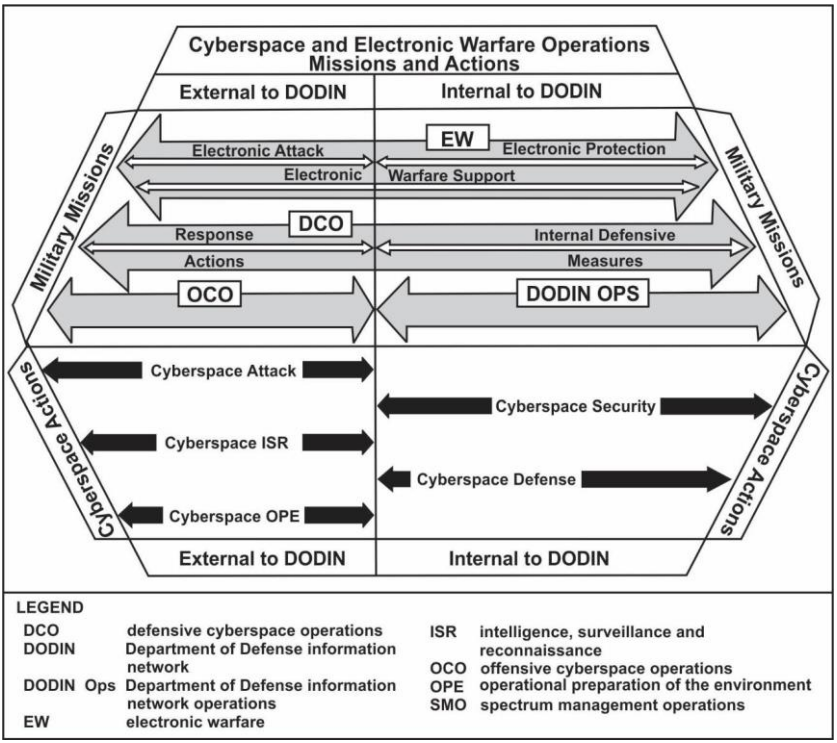

図８　サイバー空園・電子戦作戦における任務と活動[40]

サイバー空間及び軍事的活動について、それぞれを国防省情報ネットワーク（Department of Defense Information Network: DODIN）の内外で区分し、ぞれぞれの領域における活動を定義している。

（３）電磁スペクトラム活動に関わる課題

統合ドクトリン「電磁スペクトラム管理戦（Electromagnetic Spectrum Management Operation ）」で電磁波の使用者を友軍（自軍含む)、敵対勢力、中立勢力（民間、商用等）に区分[41]しているように、彼我不明の電磁波は無視できない存在である。今日において、電磁波は長波（Low Frequency: LF）からミリ波（Extremely High Frequency :EHF）まで様々な通信、レ

ーダー等の用途で官民を問わず幅広く利用されており、実際、日本及びその周辺でも多くの電磁波が飛び交い、複雑な電磁スペクトラム環境を形成しており、電磁スペクトラム活動には様々な制約を受ける。

その一方で、戦域における各種情報のデジタル化は、通信の需要を爆発的に増大させている。イラク戦争において米軍は、2万個を越える周波数を用意したとも伝えられている[42]。また、米軍と同盟国は通信所要を満たすために民間の衛星通信を利用したが、防衛情報システム局（Defense Information System Agency: DISA）[43]では、その割合が軍の所要全体の84%に達したと報告している[44]。軍事組織も民間組織の通信インフラの利用が不可欠となっている状況にある。今後も通信所要は増大かつ大容量化する傾向にあると考えられ、作戦遂行上の要求を満たすには、回線の増大、すなわち電磁スペクトラム利用の拡大が求められることになる。

複雑な電磁スペクトラム環境と増大する通信所要という二つの要件を考えれば、電磁スペクトラム活動の自由と安全を確保しながら、敵の電磁サイバー攻撃及び電子攻撃を拒否することは容易ではなく、かつ実現のためには作戦時のみならず平素からの電磁スペクトラム環境の把握等の活動が必要とされる。このため、米国では DISA の防衛スペクトラム組織（Defense Spectrum Organization: DSO）が電磁スペクトラムの利用状況に関する莫大なデータ・ベースを構築するとともに、世界的規模での電磁スペクトラム管理を行うことにより、作戦地域の電磁スペクトラム環境を事前に把握して電磁スペクトラム活動の円滑な計画立案を可能とする態勢の整備が図られている[45]。日本としても、電磁スペクトラム領域における戦いに備え、相手の行動を妨害しつつ我の行動を確保しえる優越性を獲得するため、平素から電磁スペクトラムを管理し得る態勢を整備する必要があるだろう。

（4）民間を含めたＥＭＰ等への対応

EMP による攻撃は、前述のとおり、電磁サイバー攻撃のように現実的には発生していないが、電子機器に対する影響が大きく、実際に使用可能な簡易的な装置が存在していることを踏まえれば、これまで以上に各種プラットフォームや司令部施設等の電磁波対策が必要とされるようになるだろう。ま

た、EMP やサイバー攻撃の対象が、防衛システムだけに限定されていない以上、軍事的な対応だけでは不十分といえる。

基地や駐屯地等の周辺にある発電所等の電力インフラや交通機関などが EMP や電磁サイバー攻撃による機能の喪失は、基地業務に影響を及ぼすことになる。特に、これらの機能喪失が長期に及んだ場合、基地機能の維持や機動展開等の部隊行動に多大な支障が生じることが予想され、作戦を継続することが極めて困難な状況に陥る可能性もあるだろう。

このような状況を踏まえ、米軍は一旦廃止されていた EMP 防護プログラムを復活させ、2015 年 4 月に電子機器防護性能向上のために 7 億ドルの事業契約を行っている。なお、米軍では、EMP 防護プログラムの廃止に拘わらず、共通標準並びに陸上 C4I 施設、軍用機及び水上艦の個別標準など器材や施設のカテゴリー毎に HEMP 防護標準を既に制定しており[46]、もともと EMP 対策を推進し得る素地を有していたといえる。加えて、電力網、通信及びその他の重要インフラの EMP 防護は未対応となっていることに対して、米国政府は 2017 年度に国家電力網の EMP 防護のための予算 20 億ドルを計上しており、議会承認という条件付きではあるものの、重要インフラについても今後、対策が進められていく可能性がある[47]。

日本としても、米国の施策を参考とし、自衛隊の基地やプラットフォームのみならず、電力など重要インフラを含めて敵対勢力の EMP や電磁サイバー攻撃から防衛するための国家的な取り組みが必要とされているといえるだろう。

６　まとめ

湾岸戦争で大きな戦果を挙げた各種指揮、偵察監視システムと精密攻撃兵器を連携させた戦い方は、システム・オブ・システムズという考え方を確立し、NCW をもって概念化された。そして現在、米軍をはじめとする主要国は戦域においてネットワークを構築し、NCW による戦いを常態化させている。NCW による戦いは常態化したが、センサーとシューターの最適な組み合わせを探る動きは続き、NIFC-CA、IFDL、MADL 等のネットワークが開発された。

一方、主要国のネットワーク化が常態化したことで、ネットワーク化によって彼の部隊を凌駕するとしたNCWが提唱した優位性が崩れ、ネットワーク化された部隊同士の戦いへの対応が求められている。ネットワーク化された部隊同士の戦いでは、プラットフォーム等に対する従来の攻撃に加えて、ネットワークそのものに対する攻撃が行われるため、脆弱性に対する処置や管理態勢が焦点となり、電磁サイバー攻撃やEMP攻撃に対する防護や電磁スペクトラム（周波数）管理の重要性が増すと考えられている。つまり、航空優勢を確保するためにはISRとネットワークの防護が不可欠であり、宇宙やサイバー空間における優位性の確立が必須となる。

サイバー防御が装備品における研究開発の前提となりつつある一方で、サイバー戦と電子戦の活動や関係を整理する動きも見られる。米軍が打ち出した電磁機動戦（Electromagnetic Maneuver Warfare）は、戦域における彼我の電磁スペクトラムを把握し、適切かつ迅速な方法で障害を排除し、自軍が電磁スペクトラムを使用できる環境を整えることを目的としている[48]。これは、ネットワークを構築する電磁スペクトラム管理の成否が勝敗の鍵を握るとの認識に基づいたものである。

現在、戦域における電磁スペクトラムの使用状況をリアルタイムに把握できる装備品等は出現していないが、このような装備品はネットワーク同士の攻防において優位な環境を作り出すにためには不可欠となると考えられている。また、電磁スペクトラムの検索、識別に人工知能の利用が提案されており[49]、近い将来、電磁スペクトラムをめぐる攻防の様相が大きく変化する可能性がある。

活動空域等におけるネットワークの構築は、米軍にとどまらず航空自衛隊も従来から取り組んでいる。実際、航空自衛隊は防空のための作戦及び弾道ミサイル防衛で重要な役割を担う自動警戒管制システム（Japan Aerospace Defense Ground Environment: JADGE）やプラットフォーム間の情報共有を担う戦術データリンクを装備し、米軍との相互運用性を確保しながら、我が国周辺において任務遂行できる能力を強化してきた[50]。また、航空自衛隊以外でも、陸上自衛隊は地対空ミサイルや対艦ミサイル等を、JADGEを中核とするネットワークに連接することにより、防護範囲の拡大を図っている。

これに加えて、電子装備研究所では、増大する通信所要に対応するために適応制御ミリ波ネットワーク・システムの研究が行われており、防衛省でもネットワークを着実に進展させ、その能力向上が進められているところ[51]である。

部隊の統制された作戦行動が複雑多岐なネットワークとその通信によって支えられている現代においてネットワークの安全を保障することは、すなわち我の指揮統制と作戦遂行能力を確保することと同義といえる。そして、ネットワークを安定的に利用するために必要とされるのがサイバー攻撃及びEMP攻撃に対する適切な防護と電磁スペクトラム領域における優位性の確保である。このため、我が国としても、民間組織を含めてサイバー攻撃及びEMP攻撃に対する抗堪性を高めるとともに電磁スペクトラム領域における必要な態勢整備が求められているといえる。

---

[1] 統合監視及び目標攻撃レーダーシステム。空中レーダー（E-8）により地上目標の探知を行い、攻撃を指揮管制する。米空軍と米陸軍により共同で計画。

[2] Arthur K. Cebrowski, “Network-Centric Warfare: Its Origin and Future,” http://www.kinection.com/ncoic/ncw_origin_future.pdf

[3] 2001年10月29日、トランスフォーメーション推進室であるOFT（Office of Force Transformation）が設立され、初代長官にセブロフスキー氏が就任した。

[4] 効果基盤型作戦

[5] National Defense Panel, “Transforming Defense National Security in the 21st Century,” December 1997.

[6] Secretary of Defense, ”Transformation Planning Guidance,” April 2003, p. 4.

[7] 原文は、「knowledgeable entities（聡明な統一体）」であり、軍隊と意訳。U.S. Department of Defense, “Data Sharing in a Net-Centric Department of Defense,” December 2, 2004, p4.

[8] Clay Wilson, “CRS Report for Congress,” RL32411, March 15, 2007.

[9] Robert M. Gates, ”A Balanced Strategy,” *Foreign Affairs*, January/February 2009.

[10] Air-Sea Battle Office, “AIR-SEA BATTLE: Service Collaboration to Address Anti-Access & Area Denial Challenges,” May 2013; http:// archive defense. gov/pubs/ASB-Concept Implementation-Summary-May-2013.pdf
なお、ASB は米国防省の発表に先立ち、2010 年に戦略予算評価センター(CSBA)が発表している。

[11] Kris Osborn, ”Navy to Integrate F-35 with Beyond-the-Horizon Technology, ” *DEFENSETECH*, January 22, 2015; http://www.defensetech.org/2015/01/22/ navy-to-integrate-f35-with-beyond-the-horizon-technology/

[12] Jeffrey H. McConnell, “Naval Integrated Fire Control–Counter Air Capability - Based System of Systems Engineering,” Naval Surface Warfare Center, November 14, 2013.

[13] MQM-170 巡航ミサイル標的と PAAT 弾頭ミサイル標的が同時に発射された。AN/MPQ-53 パトリオットレーダーと AN/MPQ-64 センチネンタルレーダーが追尾した目標情報に基づき、IBCS が脅威の識別・評価を行い、最適な射手としてそれぞれに対して PAC-2 と PAC-3 を選択して、双方のミサイルをほぼ同時に迎撃に成功した。“US Army Uses Northrop Grumman-Built System to Destroy Multiple Targets in Air and Missile Defense Test,” GLOBE NEWSWIRE, April 18, 2016; http://www.globenewswire.com/newsarchive/noc/press/pages/news_release.html?d=10161904

[14] “The F-35: A New Era of International Cooperation,” Lockheed Martin, June 15, 2015; http://www.lockheedmartin.com/us/news/features/2014/f35-new-era-of-international-coopration.html

[15] John Keller, “DARPA wants new ideas to create reconfigurable aircraft networking in battlefield condition, ”Military Aerospace, October 19,2015; http://www.militaryaerospace.com/articles/2015/10/aircraft-networking-interoperability.html

[16] https://www.darpa.mil/DDM_Gallery/DyNAMO%20Update-619x316.png

[17] 大嶋康弘、宮内由幸、古本和彦、吉田則之、岩下寛、佐藤明、大江健太郎、「米国のトランスフォーメーションと我が国の防衛力の在り方」防衛研究所編『防衛研究所紀要』第 10 巻第 1 号、2007 年 9 月、52 頁、

[18] 名古屋大学太陽地球環境研究所、「STEL Newsletter No28」、2002 年 4 月、 3 頁。

[19] T（テスラ）は磁束密度を表す単位で、磁場の強さに透磁率を掛けた磁場の密度の大きさを表している。n（ナノ）は 10 億分の 1 を示しており、10^{-9}T=1nT である。一般に、EMP は急激な磁束密度の変化等により発生するといわれており、時間あたりの変化量が大きいほど電子回路への影響が大きいと考えられる。

[20] Electric Infrastructure Security Commission, “Report: USSR Nuclear EMP Upper Atmosphere Kazakhstan Test 184”.

[21] 一政祐行「ブラックアウト事態に至る電磁パルス（EMP）脅威の諸相とその展望」『防衛研究所紀要』第 18 巻第 2 号、2016 年 2 月、7-8 頁; “Radio Frequency Weapons and the Next Phase of Terrorism,” http://www. 123helpme. com/ veiw.asp?id-7737

[22] “Millions Will Die In The First Month - EMP Attack On America Part2,” All News Pipe Line, August 11, 2015; http://allnewspipeline.com/Millions_Will_ Die_In_The_First_Month.php

[23] 梶原好生、「A2/AD 状況下での電子戦」、『電子情報通信学会技術研究報告』、2015 年 4 月 24 日、20-21 頁； “Iran shows film of captured US drone, “ BBC, December 8, 2011; http://www.bbc.com/news/world-middle-east-16098562

[24] 木村初夫「A2/AD 環境におけるサイバー電磁戦の最新動向（前編）」『月刊 JADI』、2016 年 6 月、41 頁。

[25] 同上、41 頁。

[26] サイバー攻撃の一種。独立行政法人情報処理推進機構（IPA）は「脆弱性を悪用し、複数の既存攻撃を組み合わせ、ソーシャルエンジニアリングにより特定企業や個人をねらい、対応が難しい執拗な攻撃」と定義している。

[27] “USSC, 2011 Report to Congress of the U.S.-China Economic and Security

Review Commission," November 2011.

[28] Clay Dillow, "Video: Iran Puts Its Captured RQ-170 Drone on Display," POPULAR SCIENCE, December 9, 2011; http://www.popsci.com/technology/article/2011-12/video-iran-puts-its-captured-rq-170-drone-display

[29] "Joint Publication 3-12(R) Cyberspace Operation," February 5, 2013.

[30] Ibid.

[31] 「サイバーテロ迫る脅威･･･米ハッカー国際会議」、YOMIURI ONLINE（2015年9月1日）；http://www.yomiuri.co.jp/scienence.feature/CO017291/20150901-OYT8T50152.html

[32] Pierluigi Paganini, "The System Aware Secure Sentinel against drones hacking, " Security Affairs, December 7, 2014; http://securityaffairs.co/wordpress/30885/security/system-aare-secure-sentinel-drone.html

[33] John Keller, "DARPA releases formal solicitation for HACMS cyber security initiative for military vetronics," Military &Aerospace, February 26, 2012; http://www.militaryaerospace.com/article/2012/02/darpa-release-formal-solicitation-for-hacms-cyber-security-formilitary-vetronics.html

[34] http://www.sercuarc.org/wp-content/uploads/2014/11/SERC-RT-115-Security-Engineering-Pilot-Final-Report-SERC-2013-TR-036-4-Parts-1a-1b-3-4-20150131.pdf

[35] http://lunaticoutpost.com/thread-663121.html

[36] Admiral Jonathan W. Greenert, "Imminent Domain," *Proceedings Magazine*, December 2012; http://www.usni.org/magazines/proceedings/2012-12/imminent-domain

[37] Bryan Clark, Mark Gunzinger, "Winning the Airwaves," CSBA, 2015.

[38] "CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS FM 3-12," Headquarters, Department of the Army, April 2017.

[39] "CYBER ELECTROMAGNETIC ACTIVITIES FM 3-38," Headquarters, Department of the Army, February 2014.

[40] Ibid.

[41] "Joint Publication 6-01 Joint Electromagnetic Spectrum Management

Operations” によると Electromagnetic Operation Environment（電磁作戦環境）の構成を、Friendly EOB、Adversary EOB、Neutral EOB としている。

[42] 新見昌武「実力とは 21　通信・周波数管理 」『エア・ワールド』、2005 年 12 月号、130-134 頁。

[43] 米国国防総省の内局。軍に関係する通信や電磁スペクトラムの管理を行っており、5 個のデータ・ベースに 720 万を超える件数のデータが管理されている。6000 人の職員と 1500 人以上の軍人によって運営されている。

[44] Julian C. Cheater, “Accelerating The Kill Chain via Future Unmanned Aircraft,” USAF, April 2007.

[45] “DEFENSE SPECTRUM ORGANIZATION,” DISA; http://disa.mil/Mission-support/Spectrum

[46] 米軍は、共通標準として MIL-STD-2169B(HEMP 環境)1993 年 12 月発行、MIL-STD-461F(サブシステム及び装置の電磁特性制御要求)2007 年 12 月発行、MIL-STD-464C(システムの電磁環境影響要求)2010 年 12 月発行、 MIL-STD-188-125-1(陸上 C4I 施設用 HEMP 防護　固定施設) 1998 年 7 月発行、MIL-STD-3023(軍用機用 HEMP 防護)2011 年 11 月発行、 MIL-STD-4023(水上艦用 HEMP 防護)2016 年 1 月が発行されている。

[47] 木村初夫「A2/AD 環境におけるサイバー電磁戦の最新動向（後編）」『月刊 JADI』、2016 年 7 月、29 頁。

[48] “Information Dominance Roadmap 2013-2028,” U.S. NAVY, pp. 9-10.

[49] Sydney J. Freedberg Jr, “Faster Than Thought: DARPA, Artificial Intelligence, & The Third Offset Strategy,” Breaking Defense; http:// breaking defense.com/2106/02/faster-than-thought-darpa-artificial-inteligence-the-thirad-offset-strategy/

[50] 「平成２７年防衛白書」防衛省、229-230 頁、240-242 頁。

[51] http://www.mod.go.jp/atla/densouken.html