A2／AD 環境における サイバー電磁戦の最新動向（後編）

木村 初夫

株式会社エヌ・エス・アール

3．米軍のサイバー電磁戦の動向

3.1 サイバー電磁戦

米軍のサイバー戦（Cyberspace Operations）および電子戦（Electronic Warfare）に関する体系的整理は、情報戦（Information Operation）ドクトリン（JP3-13）の体系の中に組み込まれて行われてきた。JP3-13の1998年版、2006年版および2012年版の体系を図3.1に示す。2006年版で定義されたサイバー戦としてのCNO（Computer Network Operations）は、2012年版では新たにCyberspace Operationsとして組み込まれた。また、米軍は電磁作戦環境（EMOE）の活用、攻撃、防御および管理のために電子戦および電磁スペクトラム管理戦（Electromagnetic Spectrum Management Operations）から構成される電磁スペクトラム戦（Electromagnetic Spectrum Operations）をJP6-01で定義している。さらに、米陸軍は、サイバー戦、電子戦および電磁スペクトラム管理戦を統合化および同期化したサイバー電磁戦ドクトリン（FM3-38）を出している。

(1) サイバー戦ドクトリン[48)]

2012年版JP3-13では、サイバー戦の具体的な記述はされておらず、2013年2月にサイバー戦任務、サイバー空間活動等を具体的に定義したサイバー戦ドクトリンJP3-12が機密指定で出された。また、このサイバー戦ドクトリンの機密指定が解除され、2014年10月に非機密版のJP3-12(R)が公開された。機密版と非機密版の変更点については不明である。サイバー戦は、次に示す3つの任務に区分される。

- 攻勢サイバー戦：Offensive Cyberspace Operations（OCO）

  サイバー空間における軍適用による戦力投射を企図したサイバー戦

- 防勢サイバー戦：Defensive Cyberspace Operations（DCO）

  DoDまたは他の味方のサイバー空間防御を企図したサイバー戦

  DCOは、対処活動としてのDCO Response Actions（DCO-RA）およびサイバーセキュリティ対策としてのDCO Internal Defensive Measures（DCO-IDM）に分かれる。

- DoD情報ネットワーク戦：DoD Information Network Operations（DoDIN Ops）

  DoD通信システムおよびネットワークの設計、構築、構成、安全化、運用、保守

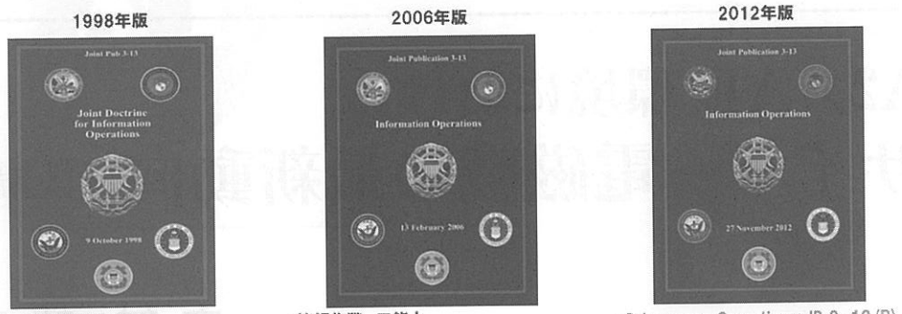


図3.1　情報戦ドクトリンの変遷

および維持のための活動

また、サイバー空間活動は、次に示すとおりサイバー空間の防御、ISR（情報・監視・偵察）および攻撃活動並びにそれらの軍事作戦活動を推進する非情報活動から構成される。

・サイバー空間防御：Cyberspace Defense

サイバー空間防御は、DoDIN の安全化、運用および防御のための DoD サイバー空間における通常活動である。また、この具体活動としては、防護、検知、特徴化、対抗および緩和がある。

・サイバー空間 ISR：Cyberspace ISR

サイバー空間 ISR は、米国大統領令によって承認された統合軍または配属された SIGINT 部隊によって実施される情報活動である。また、OCO または DCO を含む将来の作戦支援のために必要な情報収集を実施するためのサイバー空間における ISR 活動を含む。

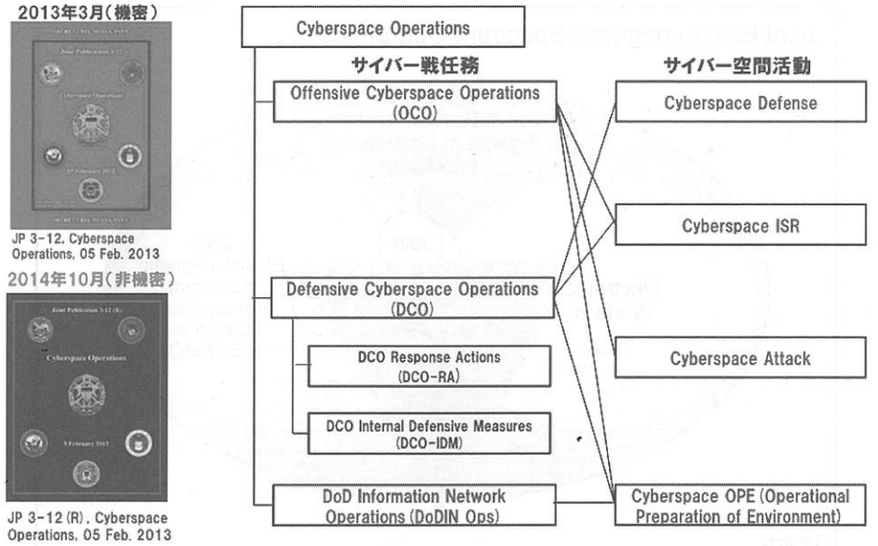
・サイバー空間攻撃：Cyberspace Attack

サイバー空間攻撃は、サイバー空間における種々の直接拒否効果並びに隠蔽化または物理領域における明示化の拒否に導く操作を起こす活動である。OCO は、米国大統領令によって承認される。また、この具体活動としては、拒否（低下、混乱および撃滅）並びに操作がある。

・サイバー空間環境運用準備：Cyberspace OPE（Operational Preparation of Environment）

サイバー空間環境運用準備は、潜在的な後続の軍事作戦の計画立案および準備のために実施される活動を推進する非情報活動である。この活動は、サイバー空間の防御、ISR および攻撃活動の推進役である。

サイバー戦ドクトリンにおけるサイバー戦任務とサイバー空間活動の関係を図3.2に示す。



出典：JP3-12(R), Cyberspace Operations, 05 Feb. 2013

図3.2　サイバー戦任務とサイバー空間活動の関係

(2)　電子戦ドクトリン[49]

米軍の電子戦（Electronic Warfare：EW）ドクトリンである JP3-13.1は、「電子戦とは敵による電磁スペクトラムの使用を拒否しつつ、味方の使用を確保する術および学である。」と定義している。現在、電子戦は、電子戦支援（Electronic warfare Support：ES）、電子攻撃（Electronic Attack：EA）および電子防護（Electronic Protection：EP）に分類される。ES は、電波探知であり、以前の電子支援対策（Electronic Support Measures：ESM）である。EA は、以前の電子対策（Electromagnetic Countermeasures：ECM）である電波妨害、チャフおよびフレアだけでなく対電波放射源兵器および指向エネルギー兵器を含むものである。EP は、ECM に対抗するためにレーダーおよび通信システムの設計・運用で採られる手段であり、以前の対電子対策（Electromagnetic Counter-Counter Measures：ECCM）に対応する。

(3)　電磁スペクトラム管理戦ドクトリン[50]

陸上、海上、水中、航空、宇宙およびサイバー空間における指揮統制システム、武器システムおよび後方システム並びに社会基盤の情報システムおよび重要インフラの制御システムは、すべて電磁波を放射する電磁スペクトラム（EMS）に依存したシステムであり、このような電磁作戦環境の活用、攻撃、防御および管理のために電子戦および電磁スペクトラム管理戦から構成されるものが図3.3に示す電磁スペクトラム戦である。

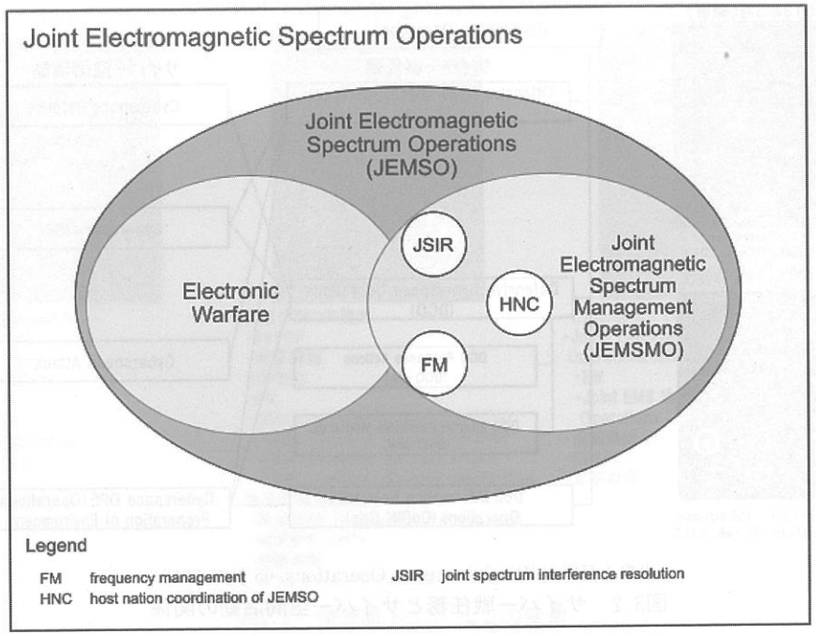
電磁スペクトラム管理戦は、米軍の JP6-01によると、次に示す 4 つの能力から構成される。

・スペクトラム管理

EMS 依存システムの調整、優先順位付けおよび相互干渉解消のための EMS 利用の計画、調整および管理

・周波数管理

EMS 依存システムのための周波数の要



出典：JP6-01, Joint Electromagnetic Spectrum Management Operation, 20 March 2012

図3.3　電磁スペクトラム戦

求、指名、相互干渉分析、調整、割当および公布

・ホスト国調整

主権国家内におけるEMS依存システム運用のための認証獲得活動並びに外国との渉外活動

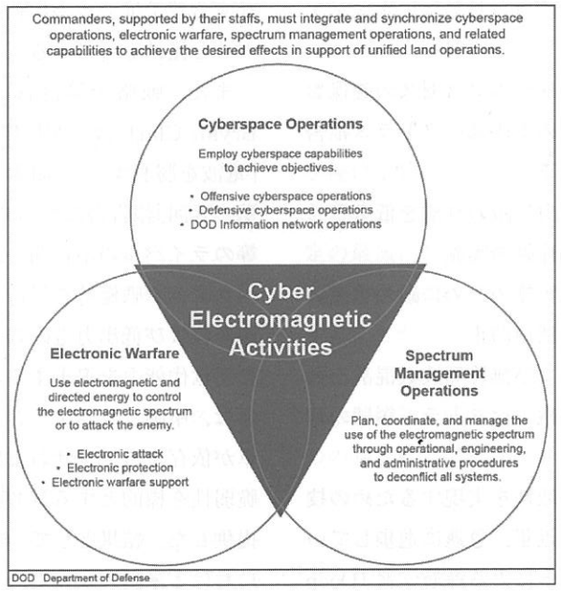
・相互干渉解消

電磁相互干渉事案の識別、報告、分析、緩和または解消活動

EMOEは、背景電磁環境（EME）並びに我、中立および彼の電磁放射である電子戦力組成（Electronic Order of Battle：EOB）から構成され、電磁作戦環境の状況認識のための電磁スペクトラム共通作戦状況図（COP）を作成するためにはそれらに関する平時からのデータ収集および背景電磁環境ベースラインの設定が必要である。

(4)　サイバー電磁戦ドクトリン[51)52)]

米海軍作戦本部長であるJonathan W. Greenert大将は、プロシーディング誌2012年12月号のサイバー電磁戦に関する啓蒙的論文である「緊迫領域（Imminent Domain）」において、「将来の戦いは、電磁スペクトラムおよびサイバー空間の効果的利用によって単純には勝利されないだろう。それらの戦いは電磁－サイバー領域内において勝利されるだろう。その変化の達成および電磁－サイバー環境の指揮には、革新的作戦構想、新しい軍事システム、および最も重要である現代戦における思考の新鮮なアプローチが必要である。また、我々が電磁－サイバー環境を指揮しようとする場合には、水中環境における経験に類似して電磁静粛性および電磁シグネチャの理解の同様な文化が我々の業務に浸透しなければならない。」と述べている。こ



出典：HQ, DoA, FM3-38, Cyber Electromagnetic Activity, Feb. 2014

図3.4　サイバー電磁活動

のように将来の戦闘は、陸上、海上、水中、航空および宇宙の物理戦闘領域が依存する電磁スペクトラムおよびサイバー空間の領域が主戦闘領域となり、それらを支配するためのサイバー電磁戦が勝敗を決める。サイバー電磁戦は、サイバー戦、電子戦および電磁スペクトラム管理戦を統合化および同期化したものである。米陸軍は、サイバー電磁戦ドクトリンとして2014年2月に「FM3-38サイバー電磁活動」を公刊している。サイバー電磁活動を図3.4に示す。

3.2　米国防総省の第3相殺戦略および電磁スペクトラム優勢奪回戦略の確立[53)54)55)56)]

A2／AD能力の成熟および拡散並びに米国の国防費削減によって、米国の軍事優位性が低下している。米国のHagel国防長官は、2014年11月15日に今後数10年間に亘る戦力投射を米国の掌中で確実に競争優位を確保するために、1950年代初期にDwight D. Eisenhower米大統領による米ソ冷戦期におけるソ連優位の通常兵器に対する核兵器開発の第1相殺戦略並びに1970年代中頃のHarold Brown国防長官による通常兵器のネットワーク化された精密打撃、ステルス化および監視の第2相殺戦略と同様にアサルト・ブレーカーとしての能力開発のための第3相殺戦略の確立を目標とした国防イノベーション構想（D II）を宣言した。また、Work国防副長官は、第3相殺戦略のための優先作戦課題として、A2／AD環境における大量の誘導武器の一斉射撃による飽和攻撃に対する電磁スペクトラム活用（非運動兵器）によるミサイル防衛を挙げている。DoDは、Bob Work副長官のこのような認識に基づき、第3相殺戦略のためのブレークスルー技術を識別するためにプロトタイプを行う重点領域の1つとして、米軍の電磁スペクトラムの機動自由度による作戦能力のための電磁スペクトラム俊敏性を挙げている。

電磁スペクトラム作戦能力としては、次に示す能力を挙げている。

- 友軍の電磁スペクトラムアクセスの確保および維持、我の敵の電磁スペクトラム拒否および／または低下
- 我の意図および能力の敵の理解を低下させるための電磁欺瞞作戦の実施
- 他の領域での作戦実施のために敵の電磁スペクトラム領域の活用防止
- 指向エネルギーおよび無線周波数混乱を発生させるために電磁スペクトラム領域の新しい効果

電磁スペクトラム俊敏性を実現するための技術の方向性としては、近年、急速に進歩している多層ニューラルネットによる深層学習（Deep Learning）が挙げられている。例えば、DARPAは、深層学習を用いた「適応レーダー対策（Adaptive Radar Countermeasures：ARC）」および「適応電子戦用行動学習（Behavioral Learning for Adaptive Electronic Warfare：BLADE）」の２つのプログラムに取り組んでいる。これらは、それぞれ未知および動的な脅威レーダーおよび無線通信システムに対して、深層学習によってリアルタイムに新しい脅威の探知および特徴表現並びに動的な新しい電子対策の生成を行うものである。

一方、米国防総省（DoD）の国防科学委員会（DSB）は、2015年７月発表の「複雑な電磁環境における21世紀軍事作戦に関する研究」報告書において、「米国の電子戦統制は、脅威が去ったあるいはかつてほど深刻でないという誤った信念での旧ソ連の崩壊以来、非常に萎縮していること」を明らかにした。また、21世紀の軍事作戦ニーズに合うためにDoD電子戦エンタープライズを再生するための適切な組織的提言の実現コストは、DoDが適時および正確な情報に依存する数千億ドルの作戦能力に対して年間23億ドルと見積もっている。

また、戦略予算評価センター（CSBA）のBryan Clarkは、2015年12月に議会報告した「電波を勝利する：米国の電磁スペクトラム優勢の奪回」報告書において、「冷戦の終結後の同等のライバルの不在期において、DoDは電磁スペクトラム戦優勢を維持するために必要なステルスおよび低出力電磁スペクトラム能力のような新世代能力を追求するのに失敗した。この中断は、中国、ロシア、および他のライバルに米軍が依存するセンサおよび通信ネットワークの脆弱性を標的とするシステムを展開する機会を提供した。結果として、電磁スペクトラム領域における米国のかつての重要な軍事優位性は、陳腐化し、実際もはや存在しないかもしれない。」と述べている。一方、「DoDは、新しい作戦構想の実現および低－無出力電磁スペクトラム戦能力の展開によって耐性のある電磁スペクトラムにおける優位性を確立する機会を有している。」と提言している。新しい作戦構想としては、受動センサが主体となる「低－無出力電磁スペクトラム戦」としての「受動またはマルチスタティック探知を用いた敵軍の発見」、「反射された環境エネルギーを用いた敵軍の位置決定」、「敵A2／ADゾーン内作戦のための高度な電波管制および低出力対抗手段の優位性活用」等を挙げている。また、新しい技術としては、ネットワーク化、俊敏化、多機能化、小型化および適応化の属性を持つ電磁スペクトラム戦システムの開発を挙げている。特に、俊敏化とは、出力、周波数、空間および時間を機動できることである。また、多機能化とは、通信、能動と受動探知、電波妨害、欺瞞、またはデコイのような複数の電磁スペクトラム戦機能を実行できることである。適応化とは、事前に未知放射を含む電磁スペクトラムの特徴表現並びに機会の活用または敵電磁スペクトラム戦の対抗のために対応できることである。

米国の電磁スペクトラム優勢奪回のための提言として、低－無出力のセンサ、通信、および対抗手段のような電磁スペクトラム戦能力を確立するために、電磁スペクトラム戦ビジョンの策定、新しい電磁スペクトラム戦作戦構想の策定、新しい能力要求の確立と国防総省の調達プロセスの効率化、新しい電磁スペクトラム戦技術開発の加速化、電磁スペクトラム戦システム調達の統合化等を挙げている。

3.3　米海軍の情報優勢構想

中国およびイランのA2／AD脅威の出現によりイラク戦争、アフガニスタン紛争等において情報優越を実現したネットワーク中心戦（NCW）が成立しなくなった。この新しい脅威に対抗するために、米海軍は情報領域における情報高地の確保（制高権の確保）を目的としたInformation Dominance（情報優勢）構想を図3.5に示すように推進している。

米海軍の情報優勢構想は、2012年12月に発表された「米海軍情報優勢実現戦略2013-2017」によると、「21世紀の海上戦における持続した統合火力を実現するために確実な海上指揮統制および優位な戦闘空間認識を提供することである。」と定義されている。また、情報優勢は、「意思決定の最適化および戦闘効果の最大化のために米海軍の情報機能、能力および資源を十分に統合することから得られる作戦優位性である。」と定義されている。したがって、情報優勢は、確実な指揮統制、戦闘空間認識および統合火力の３つの基本能力に依存している。このような能力の実現によって、米海軍指揮官は情報領域において自由に作戦を遂行し、敵の意思決定サイクルに対して有利な状態を継続することを目指している[57]。

また、米海軍の情報優勢構想を実現するための３つの基本能力に関する機能、現状／短期計画（2013-2019年）および先進能力（2020-2028年）をまとめた「米海軍情報優勢ロードマップ2013-2018」を2013年３月に発表している。本

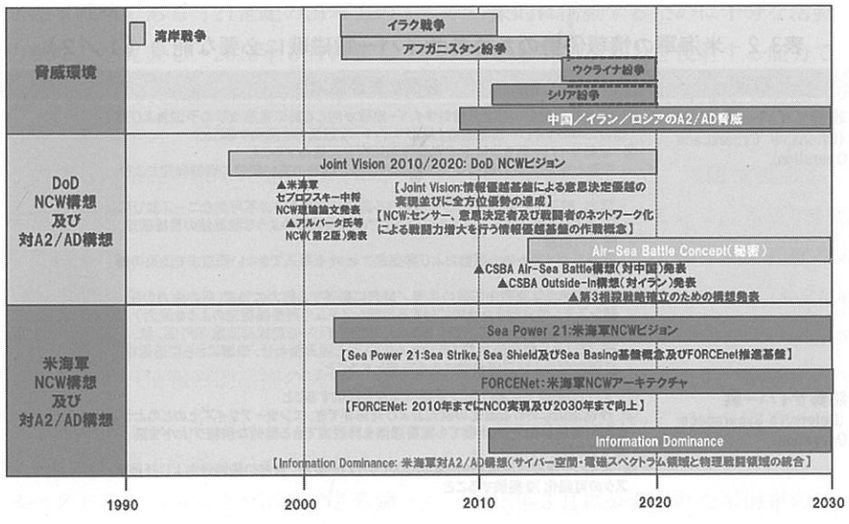


図3.5　米海軍の情報優勢構想の位置づけ

ロードマップの全体像を整理したものを表3.1に示す。さらに、このロードマップに挙げられている能力から電磁スペクトラムおよびサイバー空間を支配するための電磁機動戦およびサイバー戦に関する能力を抽出・整理したものを表3.2に示す[58]。

特に、電磁機動戦の能力としては、確実な電磁スペクトラムアクセスのための電磁スペクトラムCOPおよびリアルタイムスペクトラム作戦(RTSO)能力並びに武器としての電磁スペクトラム活用のための電磁スペクトラムの評価／予測的操作および指向エネルギー兵器等の電磁スペクトラム操作がある。

表3.1　米海軍の情報優勢ロードマップ（2013-2018）

能力	概要	機能	現状／短期計画(2013-2019)	先進能力(2020-2028)
確実な指揮統制	米海軍が将来において想定する指揮統制(C2)環境の範囲 ・Permissive C2:制約のないC2 ・Contested C2:紛争中のC2 ・Highly Contested/Denied C2:高列度紛争中／拒否されたC2	・どのような環境下においても艦下部隊を指揮できること。 ・全領域の火力を調整できること。 ・火力および我部隊の状態を評価できること。	・生残性のある広帯域、OTH伝送能力を有する衛星回線 ・戦闘用狭帯域回線：split-IP放送付き保護衛星回線及びHF-IP並びに狭帯域LOS通信 ・CANES:艦艇用統合情報通信基盤 ・NGEN:米海軍及び米海兵隊用陸上情報通信基盤 ・性能向上した戦術データリンク ・正確なPNT能力 ・調定電磁スペクトラム管制 ・MOCの真上COP提供 ・戦闘システムとC2システムの統合(データインタフェース)	【すべて脅威環境下での部隊指揮】 ・確実な電磁スペクトラムアクセス ・動的な柔軟性のある情報グリッド ・共有認識のための任務関連データ(データ中心アーキテクチャ):運用状態自動報告および部隊発見サービス ・確実な時刻サービス 【全領域の火器の調整】 ・作戦および戦術意思決定支援 ・高度化されたデータリンクネットワーク ・確実な位置測定、航法および時刻(PNT) 【火力および我部隊の状態評価】 ・作戦即応性の連時評価
戦闘空間認識	潜在敵の配置および意図を理解する能力 ・任務割当、作戦計画立案および命令 ・データ収集 ・データおよび情報共有 ・処理および融合 ・分析、予測および作成 ・情報配布および管理	・不可欠な戦闘情報を融合できること。 ・作戦環境を理解できること。 ・情報に基づく決断力のある行動を実現できること。	・集中艦艇収集管理および任務割当 ・オーガニックセンサ能力および容量拡大(有人、無人および多角的プラットフォーム) ・分散ネットワーク環境への革新 ・COPおよびCMP提供(SoSアプローチ) ・データ共有高度化 ・艦隊BAセンタおよび米海軍ISRアセットのC2ノードとしてのMOC ・作戦計画立案ツールおよび戦域安全保障調整能力並びに任務パートナー能力情報源との統合 ・BA訓練の向上	【不可欠な戦闘情報の融合】 ・任務割当、作戦計画立案および命令の能率化 ・全領域の先端センサ開発 ・処理、融合および情報製品配布全自動化 【作戦環境の理解】 ・共有関連リアルタイムCOP/CMPの開発 ・物理および仮想環境の理解及び予測 ・友軍、敵および中立の能力及び意図の理解 【情報に基づく決断力のある行動】 ・兵士選択肢の増強
統合火力	主要統合火力能力 ・運動火力のための全電磁周波数運用 ・非運動火力のための電磁スペクトラム活用(サイバー攻撃、電波妨害およびDEW) ・運動火力および非運動火力の調整	・従火力の打破、拒否および撃滅(彼キルチェーンの分離および当該キルチェーン内の重要回線の打破、拒否および撃滅) ・我火力の向上(全領域火力の正確および適時な配備能力)	・初期C2保証能力：Link 16 CMN-4及びTTNT経由のLOSセンサネットワーク化 ・初期目標標定・海軍統合火器管制-対空能力(NIFC-CA) ・NEWの初期能力：JSOW-C1,SDB-II、OASuW ・彼C4ISR回および欺瞞対抗能力 ・電子戦能力の向上 ・統合および国家能力の活用 ・指向エネルギー兵器(DEW)研究開発　等	【彼火力の打破、拒否および撃滅】 ・彼の運動および非運動作戦の防止 ・彼の運動および非運動兵器運用の実効性のある防止 ・彼のハイリスク伝統的作戦依存の削減 【我火力の向上】 ・目標標定および火器管制能力の統合化 ・武器としての電磁スペクトラムの活用 ・武器の射程距離、有効性および致死性の向上 ・全領域および全軍種との動的調整

出典：U.S. Navy Information Dominance Roadmap 2013-2028, March 2013

表3.2　米海軍の情報優勢のためのサイバー電磁戦に必要な能力（1／2）

項目	必要な主要能力	備考
攻勢サイバー戦 (Offensive Cyberspace Operation)	① 敵の武器発射の防止を含むサイバー攻撃が起こる前に当該攻撃の予測および打破のためのサイバー情報窃取およびサイバー攻撃能力を開発すること ② 攻勢サイバー戦を次に示す軍事作戦に完全に統合すること ・主要な軍事作戦の戦闘空間の準備から非正規戦の高い価値の目標標定および識別の確立 ・電力、輸送システム、および高次レベル政府に対する他の不可欠なニーズ並びにC2および戦術システムレベルに至るまでの軍事機能のような敵基盤の目標標定能力の包含 ・敵が具備するための運動および非運動アセットを導入できない限度まで効果の最大化 ・交戦前または交戦中に敵の兵器／効果に影響する能力の包含(敵の火力の任務システムの支配または敵に対する当該システムの再目標標定のような能力) ・敵を能動感知モードに強制するために攻勢サイバーを無線周波数(RF)囮、欺瞞、低レベル観測値および受動キルチェーンと組み合わせ、米軍にさらに迅速な目標標定および目標の中立化を可能とすること	
防勢サイバー戦 (Defensive Syberspace Operation)	① A2/AD環境下におけるC2狭帯域回線を提供すること ② 作戦環境における変化の検知および対応ができ、エンタープライズ上のどのような利用可能移動アセット間でも重要通信を再設定できる動的な情報グリッドを提供すること ③ サイバー空間状況認識のためのCOP(サイバー脅威、資産の脆弱性および任務リスクの可視化)を提供すること	

出典：U.S. Navy Information Dominance Roadmap 2013-2028, March 2013

表3.2　米海軍の情報優勢のためのサイバー電磁戦に必要な能力（2／2）

項目	必要な主要能力	備考
確実な電磁スペクトラムアクセス【個別プラットフォーム作戦能力最大化のための電磁スペクトラムの操作及び調整】	① 電子航法海図への連接および動的電磁スペクトラム統制を可能とする作戦制約を表示する電磁スペクトラムCOP ② すべての打撃群及びプラットフォームからの電磁スペクトラム放射の動的監視及び統制を可能とし、電磁スペクトラム作戦対応を分単位から秒単位に短縮する、完全に機能するリアルタイムスペクトラム作戦(RTSO)能力	
武器としての電磁スペクトラム活用	① 電磁スペクトラムの自然状態が次に示す能力によって理解できるポイントに対する複雑な電磁環境を監視すること ・ 統合火力の支援のために我の優位に向けた電磁スペクトラムの評価および予測的操作 ・ 我部隊の隠蔽および彼部隊による探知高度化 ・ 高電力マイクロ波、レーザー及び無線周波数システムのような指向エネルギー兵器(DEW)を含む火力能力としての電磁スペクトラムの操作 ② 我部隊用目標標定データの提供能力を保証するための電磁スペクトラムの全利用可能領域を活用すること ・ 軍事作戦に先行する電磁スペクトラムの自然状態をベースライン化する能力の開発 ・ 自然環境における振動を検知および測定する既存システムの開発および向上 ・ 目標標定および他の重要機能用の全体情報系統を高度化するための相関及び融合のサポート	

出典：U.S. Navy Information Dominance Roadmap 2013-2028, March 2013

米海軍は、米国の地球規模的な海上アクセスに挑戦するA2／AD脅威に対応するために、米海軍の情報優勢構想の進展に基づき、2007年に発表した米海軍戦略である「21世紀の海軍力のための協力戦略」を見直し、2015年3月に新しい米海軍戦略として英語版と同時に日本・中国・アラビア・スペイン・韓国・仏国語版を公表した。この新しい米海軍戦略の要点は次に示すとおり全領域アクセスおよび電磁機動戦について強調している[59]。

・サイバー空間および電磁スペクトラムにおける新しい軍事的挑戦課題は、米国が情報優位であること（情報の制高権の確保）を想定できなくなることを示している。
・米海軍は、高列度下のサイバー空間および電磁スペクトラムの領域でも活動できる強靭性（レジリエンス）を持たなければならない。
・米海軍は、国家安全保障を支援する海軍力として、全領域アクセス、抑止力、制海権、戦力投射および海上保安能力を持たなければならない。
・全領域アクセスは、紛争地域において、効果的に活動するために十分な活動の自由度をもって軍事力を投射する能力であり、その構成要素として情報優勢構想の能力である戦闘空間認識、確実な指揮統制および統合火力に加えて、電磁機動戦およびサイバー戦を定義している。電磁機動戦については、「戦闘優位を作り出す高度な非運動能力を備えた宇宙空間、サイバー空間、電磁スペクトラムにおける艦隊作戦活動を融合した比較的新しい概念である。」と米海軍の公式文書において初めて定義されている。

3.4　米海軍の電磁機動戦

2015年3月に公表された米海軍の新しい海軍戦略は、米海軍作戦部長であるJonathan　W.

Greenert 大将が在職期間中に電磁機動戦の創設を非常に重視したことを反映したものである。彼は、2014年３月の米国下院軍事委員会公聴会において、「電磁機動戦について、我の電磁スペクトラムの自由な機動能力を向上し、敵の同様な能力を拒否する。」と発言している[60]。米海軍が呼んでいる「電磁機動戦」は、まだ、開発されていない電磁戦闘管理システムの調整によって、水上艦、潜水艦、無人機、航空機のようなすべての我の個別プラットフォームが、NGJ（Next Generation Jammer）を搭載したEA-18G Growler を中心としたセンサネットワークに通知するために彼の電磁スペクトラムに関するデータを収集し、彼を情報欺瞞または電波妨害するために我自身の電磁スペクトラムを制御するものである。米海軍の Bob Gamberg 大佐が2014年10月の AOC 年次大会において、「現在の電磁スペクトラムの扱いは塹壕戦であり、機動戦にするためには、対潜水艦戦における音波の扱い方が一つのモデルになる。そのモデルは実際にうまく変換し、潜水艦乗りの思考過程が活用できる。」と述べている[61]。このような対潜水艦戦と電磁機動戦の比較を表3.3に示す。電磁スペクトラムの状況認識、操作および活用能力を実現するためにリアルタイムな電磁戦闘管理システム（ElectroMagnetic Battle Management System：EMBM）を構築する必要がある。また、電磁戦闘管理は、電子戦ドクトリン JP3-13.1によると電磁スペクトラム戦の動的監視、評価、計画立案および指示を行うものである。

電磁機動戦の機動の電磁的自由度については、電磁作戦環境（EMOE）における機動自由度および我が彼への情報優勢を維持するために変化する状況に適応できる速さであると見ることができる。これを電磁俊敏性（EMA：Electro-Magnetic Agility）尺度として考えることができる。機動の電磁的自由度の実現アプローチとしては、彼の EMOE ギャップ（弱点）の利用並びに我の EMOE ギャップを彼に利用された場合、我の運動または非運動手段によって彼による我の利用できる EMOE への復帰がある。このような電磁機動戦戦術を具体化する技術としては、周波数ホッピングスペクトラム拡散（FHSS）通信、周波数俊敏レーダシステム、ネットワーク動的再構成等がある。また、機動のためのサイバー防御技術は、動的構成可能ルータ、動的 IP アドレス等の移動目標技術がある[62]。

表3.3　対潜水艦戦と電磁機動戦の比較

項目	対潜水艦戦	電磁機動戦	備考
標的	潜水艦およびLUUV（攻撃型およびセンサ搭載型）	水上艦、航空機、無人機、潜水艦のEWシステム、Radarシステム、無線通信ネットワーク／データリンク、モバイル端末等の電磁放射武器および器材	
戦闘領域の特性	水中領域 ・音響・磁気センサによる一部可視化 ・音響伝搬環境への依存性大	電磁スペクトラム領域 ・軍事・民間の全電磁スペクトラム対応 ・電波伝搬環境の影響あり	
常続監視	受動センサ（音響および磁気センサ） （監視周波数帯域：全音響・磁気領域）	受動センサ（広帯域RFセンサ、IRセンサおよびEOセンサ） （監視周波数帯域：100kHz～400GHz）	
平時における作戦領域認識（戦闘環境認識）	作戦領域の背景音響雑音、対象潜水艦およびLUUVの音響シグネチャ／諸元のデータベース化	作戦領域の背景電磁環境の電磁放射データに基づく自然状態のベースライン並びに彼・中立・我・民間アセットの使用周波数帯域（Frequency Allocation）および彼の電磁シグネチャのデータベース化	電磁作戦環境の定義（JP 6-01 JEMSO参照）
有事における作戦領域認識（戦闘状況認識）	水中COPの構築	電磁スペクトラムCOPの構築	
脅威の認識別	・背景音響雑音並びに我、中立および民間のアセットで取得されている以外の音響シグネチャは脅威と認識する。 ・彼の音響シグネチャによる固有識別	・背景電磁環境並びに我、中立および民間のアセットで承認されている以外の電磁シグネチャは脅威と認識する。 ・彼の電磁シグネチャによる固有識別：特定電波源識別（SEI）	
防御	・隠密性 ・魚雷防御システム ・Anti-Torpedo Torpedo（ATT）	・電磁機動のための我の電磁スペクトラム操作（電力、周波数、および変調方式の動的変更） ・サイバー防御のためのステルス化（IPアドレス、環境変数等の動的変更）	
攻撃	・魚雷 ・VLA（Vertical Launch ASROC）	・電子攻撃およびサイバー攻撃（データ挿入およびマルウェア挿入）	

3.5　米海軍の電磁機動戦を実現するための主要プログラム

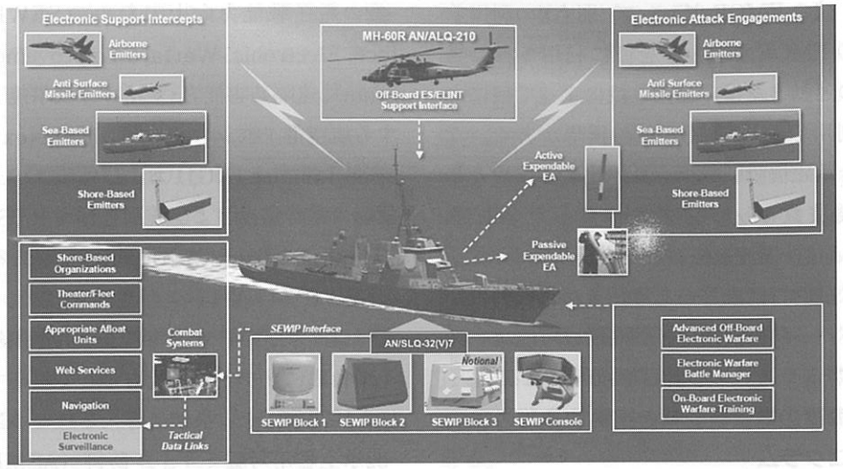
米海軍は、現在、電磁機動戦を実現するための主要技術として、共通基盤技術である AESA、デジタル送受信、デジタルビーム形成、信号処理等の Open Architecture RF の開発を推進している。また、米海軍の電磁機動戦のための主要プログラムとしては、レーダー、EW、通信および航法の電磁波（RF）機能を統合化する INTegrated TOPside（INTOP）、AN／SLQ-32の電子戦能力向上のための SEWIP（Surface Electronic Warfare Improvement Program）、遠隔妨害能力・サイバー攻撃能力等を有する航空電子戦システムとしての Next Generation Jammer（NGJ）および電磁スペクトラム放射の常時監視および統制を行う RTSO（Real-Time Spectrum Operation）等がある[63]。

SEWIP は、中国のミリ波アクティブレーダーシーカーの終末誘導による次世代対艦ミサイル脅威にソフトキル能力として対応するために、1970年代末に最初に導入された AN／SLQ-32水上艦用対艦ミサイル防御（ASMD：Anti-Surface Missile Defense）システムの能力を抜本的に向上するプログラムである。SEWIP は、ASMD 能力、対目標標定、対監視能力および状況認識能力の向上を目的とし、レーダー、EO／IR システム、デコイ等対抗システム、通信、ネットワークを新しい EW 能力とともに統合化するものである。SEWIP は、探知妨害のための Onboard　EW および電波欺瞞のための

表3.4　SEWIP の全体プログラムの概要

区　分	プログラム	内　　容
Onboard EW	SEWIP BLOCK1（2002～）	・BLOCK1A：迅速な脅威識別およびHSI向上のためのAN/SLQ-32用パルス処理コンピュータおよび表示コンソール換装 ・BLOCK1B：特殊信号傍受のためのセンサ追加（特定電波源識別（SEI）および高利得高感度（HGHS）受信機）
	SEWIP BLOCK2（2010～）	・AN/SLQ-32の電子支援（ES）システムの新型高性能広帯域受信機セットへの換装 ・対目標標定および対監視能力サポートのためにESアンテナ向上並びにクラッタ環境での遅延、偽警報率および高パルススループットの向上のための戦闘システム単一統合インタフェースの提供（ソフトウェア改修）
	SEWIP BLOCK3（2012～） IOC：2018	・AN/SLQ-32の新しい高出力電子攻撃（EA）能力（沿岸および艦船搭載レーダー攻撃用）開発 ・水上EW能力向上のための新しいAESAおよび窒化ガリウム（GaN）高出力増幅器、関連ジャミング技術の導入 ・高利得・精密電力追加効率、高帯域幅運用、デジタルビーム形成・高度波形高速生成、多機能運用および同時交戦等技術 ・BLOCK3T（2013-2015）：YJ-12およびYJ-18のASCM等脅威対応用緊急運用要求（広範囲のASMシーカーに対応）に基づくTEWM（Transportable EW Module）の開発：広帯域デジタルRFメモリ（DRFM）EA能力で統合化されたES受信機との組み合わせ、DRFMによる標準雑音ジャミング技術・偽目標高分解識別（同時複数脅威対応並びに偽目標と総合ジャミング技術と組み合わせ可能な複々波形生成に役立つ振幅ドップラー変調方式）、およびLink-16プロトコルの提供
	SEWIP BLOCK4	・高度EO/IR能力の提供（将来） ・Combined EO/IR Surveillance and Response System（CE-SARS）：ONR
Offboard EW	Nulka（2002～）	・米国と豪州との共同開発プログラム：米国の電子ペイロードおよび火器管制システム開発、豪州のホバリングロケット開発 ・ホバリングロケット頭頂部に広帯域無線中継器を搭載したOffboard Active Decoy開発
	E-Nulka（2014～）	・現在、能動対策が存在しない進歩する対艦ミサイル脅威に対抗するためのNulkaの周波数運域向上 ・AESA送信機、受信機および高度分離部材を統合化する経済的および超小型のRFペイロード開発
	AOEW（2012～）	・現行および将来の対艦ミサイル脅威に対する次世代の調整されたEWミッション並びに識別されたEWギャップの解消のために用いられる複数のペイロードタイプを持つ長期滞留オフボードデコイの開発 ・COTSベースデコイ発射システム：MK59 Mod 0 Decoy Launch System（Airborne Systems Ltd.，UK） ・フルAOEW能力の配備プラットフォーム：MH-60R/MH-60S

出典：John Haystead, Leap-Ahead SEWIP Technology Meets Next-Generation Threats Today, JED, Jan. 2015



出典：Doug Small, Surface Electronic Warfare Improvement Program (SWEIP) Overview, PEO IWS, 15 April 2015

図3.6　SEWIP の主要なシステム構成器材

Offboard EW から構成される。Onboard EW は、処理能力向上および特定電波源識別のための SEWIP Block 1、ミリ波アクティブレーダー探知のための SEWIP Block 2およびミリ波アクティブレーダー妨害のための SEWIP Block 3のプログラムから構成される。また、SEWIP Block 3の初期運用能力（IOC）提供が2018年であるため、中国の YJ-12および YJ-18の ASCM 等脅威による太平洋艦隊の緊急運用要求に基づきミリ波アクティブレーダー妨害のための移動型 SEWIP Block 3T が開発されている。SEWIP Block 2は、2014年に配備が開始され、2015年中頃に量産になる予定である。Offboard EW では、次世代対艦ミサイル脅威に対応するための E-Nulka および AOEW のデコイシステムが開発されている。SEWIP の全体プログラムの概要および主要なシステム構成器材をそれぞれ表3.4および図3.6に示す[64][65]。

RTSO については、米海軍は2016会計年度予算において EMC2（Electromagnetic Maneuver Warfare Command and Control）プログラム（FY2016-FY2020）として計上されている。これは、戦闘群の電子戦、情報戦、通信およびレーダー業務の電磁スペクトラム活用の最適化のための調整を可能とするものであり、InTop プログラムにおいて開発された電磁スペクトラム資源割当マネージャーを活用して開発される予定である[66]。

3.6　次世代対艦ミサイル脅威に対応するための米海軍のハードキル能力

ハードキルとして弾道ミサイルおよび巡航ミサイルの同時対処を行うものとしては、米海軍の統合対空・ミサイル防衛（IAMD：Integrated Air and Missile Defense）構想がある。米海軍は、イージス艦による IAMD 構想を実現するために新型イージス艦システム BASELINE 9および海面上超低空飛行の対艦巡航ミサイル等の超水平線（OTH）目標の探知・迎撃のための海軍統合火器管制－対空（NIFC-CA：Navy Integrated Fire Control-Counter Air）構想を

表3.5　NIFC-CA のキルチェーン別システム構成

キルチェーン種別	リモートセンサ	センサネットワーク	武器管制システム	ミサイル
NIFC-CA FTS	E2-D, JLENS, EA-18G, UCLASS	CEC (TTNT)	E2-D	SM-6/イージスBL9艦
NIFC-CA FTA	E2-D, F/A-8E/F	Link16 (MIDS JTRS CMN-4)	E2-D	AIM-20AMRAAM /F/A-18E/F
NIFC-CA FTL	E2-D, JLENS, TPS-59, TPS-80	CTN	CAC2S	

TTNT: Tactical Targeting Network Technology
CTN: Composite Tracking Network

出典：石川潤一、輸入決定ノE-2D早期警戒機、軍事研究、2015年1月号

表3.6　プラットフォーム別搭載 CEC 型式

プラットフォーム	CEC型式	備考
水上艦	AN/USG-2B	
E2-C/D	AN/USG-3B	
海兵隊CTN	AN/USG-4	
米陸軍JLENS	AN/USG-5	
輸出型 (FMS)	AN/USG-6/7/8	豪海軍:USG-7B(水上艦)

出典：石川潤一、輸入決定ノE-2D早期警戒機、軍事研究、2015年1月号

開発している[67]。NIFC-CA には、表3.5に示す海（FTS）、空（FTA）および陸（FTL）の3種類のキルチェーンがある。海および陸の基盤となる見通し線（LOS）センサネットワークを構成するノードに共同交戦能力を提供する CEC（Common Engagement Capability）は、プラットフォーム別に表3.6に示す型式がある[68]。

また、この LOS センサネットワークは、目標画像情報の収集、目標標定、情報中継、情報共有等を行うために戦術データリンク伝送能力文書の高時刻感度目標ネットワーク化技術要件から導出された統合航空ネットワーク戦術エッジ（JAN-TE）能力としての広帯域および低遅延のリアルタイム性が要求される。この実現技術が、米ロックウェル・コリンズ社が開発した TTNT（Tactical Targeting Network Technology）であり、COTS としてのモバイルアドホックネットワーク（MANET）技術により開発した IP ベース次世代データリンクである。

TTNTの主要な特徴としては、200以上ノードへの低遅延・オンデマンドアドホックIPネットワークの提供、大容量の安全な音声、映像およびデータの最大マッハ8の速度での共有、高度な計画無しのネットワーク自動加入、データトラフィックを最大化する中継層用の統計的優先度ベース多重アクセス（SPMA）プロトコルの使用等である。

TTNTの仕様としては、航空戦術エッジで次のとおりである[69]。

- 100nm以上、高優先度および2 msec以下の遅延で2 Mbpsのデータを送信できること
- 300nmレンジで10Mbpsのスループットを有すること
- Link-16と互換性があること
- 高ドップラー性能を有すること
- 5秒以内にネットワーク自動加入できること
- LOS間中継できること
- 使用周波数は、V／UHFおよびLバンドであること

4．電磁サイバー攻撃および防御技術の動向

4.1　主要な電磁サイバー攻撃技術

電子攻撃およびサイバー攻撃を融合した電磁サイバー攻撃技術としては、米空軍の航空ネットワーク攻撃システム（Suter）、米海軍の次世代電波妨害装置（Next Generation Jammer：NGJ）および米陸軍の戦術電磁サイバー戦デモ（TECWD：Tactical Electromagnetic Cyber Warfare Demonstration）計画がある。また、サイバー攻撃のネットワーク阻止攻撃のための電磁パルスによる蓋然性の高いピンポイント攻撃が可能である高出力マイクロ波を用いた米空軍のHPM巡航ミサイル（CHAMP）がある。

ロシアおよび中国においては、電子攻撃およびサイバー攻撃を融合した電磁サイバー攻撃技術の具体例は発表されていないが、A2／AD能力の1つとして電子攻撃技術の開発を行っている。ロシアは、次世代電子戦システムKrasukha-4および航空機搭載電波妨害装置Khibinyを開発し、シリア航空作戦の実戦で使用し、試験している。一方、中国も自衛用の航空機搭載電波妨害装置であるKG300GおよびKG600を国産開発し、運用している。

我が国においては、自衛用および敵防空網制圧用の航空機搭載電子戦システムが開発および運用されている。また、水上艦搭載の電子戦装置についても米海軍の現行AN／SLQ-32と同等のミサイル脅威探知妨害能力を有するNOLQ-3が開発および運用されている。さらに、水上艦搭載のHPMミサイルおよびEMP弾を実現するための要素技術の研究開発が行われている。

(1)　米空軍の航空ネットワーク攻撃システム（Suter）[70][71]

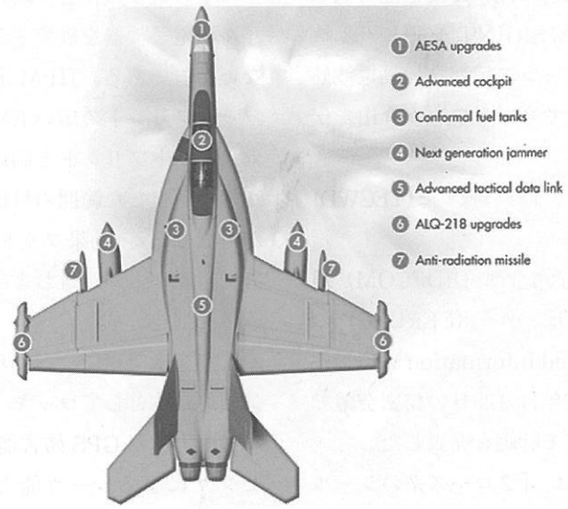
米空軍の電磁波利用によって敵の防空システムの無線通信ネットワークおよびコンピュータシステムに侵入する電磁サイバー攻撃技術は、NCCT（Network Centric Collaborative Targeting）およびSuterの2つの技術から構成される。NCCTは、最小の人間操作による目標標定を複数航空機等のセンサネットワークで実現するシステムである。NCCTは、Suter使用前に、敵の無線通信ネットワークの目標アンテナのゾーン位置を決定する。

一方、Suterは、敵の防空システムの目標アンテナのゾーン位置よりも精度の良い位置特定を行う。また、それは、敵の防空システムのSIGINT情報収集のための電磁波盗聴およびRF信号放射を行う出力データ収集部並びに敵の防空システムの情報欺瞞および制御奪取のためのRF信号放射を行う入力データ挿入部から構成され、それぞれRC-135 Rivet SIGINT機およびEC-130H Compass Call通信妨害機（通信およびレーダ）に搭載される。出力データ収集部は、敵のレーダー情報収集および敵の防空システムのベースライン能力（無線周波数、変復調方式、符号化方式、通信プロトコル、暗号方式、ソフトウェア構成情報等）情報収集を行う。入力データ挿入部は、出力データ収集部で得られた敵の防空システムのベースライン能力情報およびソフトウェア構成情報に基づく脆弱性情報によって作成された挿入データおよび挿入マルウェアを敵の無線通信システムの能力諸元に基づく強力なRF信号として、敵の目標アンテナに向けて放射する。

(2)　米海軍の次世代電波妨害装置（NGJ）[72]

現在の電磁環境におけるステルス技術は、限定された電磁スペクトラムで最適化されているので、最新のレーダー技術の向上によって戦闘機のステルス性の優位性が低下している。米海軍は、このような電磁環境におけるステルス性の低下に対応するために、遠隔電波妨害技術（standoff jamming technology）に基づく能動電子攻撃および他の高度電子戦能力を持つ次世代電波妨害装置の開発を行っている。このプロジェクトは、Next Generation Jammerと呼ばれ、電子戦攻撃機であるEA-18G Growlerに搭載された現行AN／ALQ-99を次世代電波妨害装置に換装するものである。NGJの飛行試験およびミッドバンドの初期運用能力は、それぞれ2014年9月および2021年である。NGJは、米海軍の電磁機動戦のセンサネットワーク基盤となるプロジェクトである。センサネットワークには、NIFC-CAで開発されたIPベース次世代データリンクであるTTNTが使用されている。

NGJは、窒化ガリウム（GaN）による広帯域高出力増幅器を用いた能動電子走査アレイ



出典：Jean-Jacque DeLisle, GaN-Based AESAs Enable U.S. Next Generation Jammer, 30 May 2014

図4.1　EA-18G Growler搭載NGJ

(AESA : Active Electronically Scanned Array) によってEW (電子攻撃、遠隔・護衛電波妨害) およびレーダー能力を提供するとともに、SIGINTおよび通信能力を提供する。遠隔電波妨害能力は、空母戦闘群等の艦隊全体を遠距離から電子遮蔽することができる。また、NGJは、この通信能力を用いて、敵防空システムの無線通信ネットワークおよびコンピュータシステムにデータ挿入するための非伝統的電子攻撃であるサイバー攻撃能力を提供する。

NGJは、図4.1に示すようにGrowlerの左舷および右舷に装着された2個のポッドから構成される。それぞれのポッドはその前後に全帯域幅能力を持つアレイ対を格納している。アレイ対の片方は脅威スペクトラムの高帯域をカバーし、その他方は低帯域をカバーしている。

NGJの新運用概念は、能動電波妨害モードの2機および受動SIGINTモードの1機のセンサネットワークによる運用形態である。2機による能動電波妨害は、その強度を同調によって10倍まで上げることができる。能動電波妨害モードの2機の脅威放射に関する受信能力低下を補完するために受動SIGINTモードの1機から詳細なインテリジェンス情報を能動電波妨害モードの2機にセンサネットワーク経由で伝達する。

(3) 米陸軍の戦術電磁サイバー戦デモ(TECWD)計画[73]

米陸軍研究開発・工学司令部 (RDECOM) 通信電子研究開発・工学センター (CERDEC) のI2WD (Intelligence and Information Warfare Directorate) は、2012年11月28日の秘密会議で戦術電磁サイバー戦デモ計画を発表した。

このTECWD計画は、「クローズ系のシールドされた有線ネットワークから航空プラットフォームおよび陸上プラットフォームの電磁波利用によりデータ挿入およびマルウェア挿入並びに情報窃取を行う」デモンストレーションの種々のタスクを実行できるレディメードシステムの開発である。

専門家による見解として、電磁波の歪みを検知するTEMPESTの活用による情報窃取、電磁波利用によるデータ挿入およびマルウェア挿入のためには近接性および帯域幅の制約によるデータ挿入に要する時間の短縮化の課題が挙げられている。

(4) 米空軍のHPM巡航ミサイル(CHAMP)[74][75]

米空軍およびボーイング社は、2012年10月にCHAMP (Counter-electronics High-powered Microwave Advanced Missile Project) と呼ぶHPM (High Power Microwave) 巡航ミサイルの試験をユタ試験・訓練演習場で実施し、成功した。その試験において、ステルス爆撃機からHPMを搭載したAGM-86巡航ミサイルを発射し、当該ミサイルは予めプログラム化された飛行経路に従い、地上管制室から遠隔制御された。当該ミサイルは、建物を標的として、その中の電子機器を一瞬に破壊した。当該ミサイルは電子機器を破壊するが、人体には影響しない兵器である。HPM巡航ミサイルは、効果フットプリントの広いEMP核兵器に比較して、効果フットプリントを制御できるため艦船、ビル等の限定した範囲の目標の電磁サイバー攻撃が可能である。効果フットプリントは、HPM出力、目標からの距離およびビーム拡散に依存する。

また、米空軍は、2015年5月に最適なHPM弾頭運搬体としてロッキードマーチン社のステルス能力、対GPS妨害能力および画像赤外線センサによるシーカ能力を有する射程約925 kmの長距離巡航ミサイル (AGM-185 Joint Air-to-Surface Standoff Missile-Extended Range : JASSM-ER) を選定した。さらに、米空軍は、再利用可能なHPM弾頭運搬体としてF-35および無人機についても検討している。また、HPM弾頭は、JASSM-ERおよび無人機に搭載するために小型化される。

(5) ロシアの航空機搭載電波妨害装置、電子戦システムおよびステルス対抗技術

ア. 航空機搭載電波妨害装置Khibiny[76][77][78][79][80]および電子戦システムKrasukha-4[81][82]

ロシアのKhibinyは、1980年に航空機搭載の小型化 (ポッド化) のためにKRET社のKluga無線工学研究所 (KNIRTI) とSukhoiとが共同研究開発を行い2012年に初期運用能力を実現した最新のレーダベースの航空機搭載電波妨害装置(電波妨害ポッド)である。これは、彼のレーダーのような無線方向探知器が我の生成する反射信号パラメータの欺瞞によって起こる信号源放射を探知するように設計されている。例えば、敵ミサイルのアクティブレーダーシーカーに対して偽目標に対する真目標をマスクするようにレーダー反射信号を欺瞞することができる。KRET社によると、ロシアのグルジアでの自衛用電波妨害なしでの航空機損失に対して、Khibinyは、航空機の生残性を20～30倍向上している。自衛用電波妨害ポッド型Khibinyの最新版であるSAP-518は、2-18GHz (E-Jバンド) の脅威レーダーに対応し、Su-30、Su-34およびSu-35に搭載される。また、高出力の敵防空網制圧 (SEAD : Suppression of Enemy Air Defense) 用電波妨害コンテナ型KhibinyであるSAP-14は、1-4 GHz(D-Fバンド)の脅威レーダーに対応し、Su-30、Su-34およびSu-35に搭載される。SAP-518およびSAP-14をそれぞれ図4.2および図4.3に示す。さらに、KRET社は、自衛用および敵防空網制圧用電波妨害能力を持つ最新のKhibiny-10V多機能電波妨害ポッドを開発している。このポッドは、Su-34の両翼端に搭載され、Su-34を電波妨害・SEAD機

出典：Dr Carlo Kopp, Sukhoi Flankers: The Shifting Balance of Regional Air Power, April, 2012

図4.2 自衛用電波妨害ポッド型Khibiny：SAP-518

出典：Dr Carlo Kopp, Sukhoi Flankers: The Shifting Balance of Regional Air Power, April, 2012

図4.3　敵防空網制圧用電波妨害コンテナ型 Khibiny：SAP-14

にできる。

また、ロシアの Krasukha-４は、敵の巡航ミサイルおよび他の精密誘導兵器の誘導システム、偵察衛星等を無力化（電波妨害および無線装置の恒久破壊）する新しい革新的な武器システムである。KRET 社によると、それは、陸上、航空および海上プラットフォームに搭載できる基盤的な新しい電子戦システムである。Krasukha-４は、直径600km の電子的な半円球形ゾーンの A2／AD バブルを形成し、敵のレーダー電子戦および通信システムを無力化する。この能力は、基盤的なレーダー周波数と他の無線放射源での強力な電波妨害の生成に基づいている。車載用 Krasukha-４を図4.4に示す。

出典：GPD, Jamming the Jihad: Russian Electronic Warfare Systems Spotted in Syria, 5 Oct. 2015

図4.4　ロシア軍の車載用電子戦システム Krasukha-４

イ．ステルス対抗技術[83)84)]

Ku、X および C バンド並びに S バンドの一部の高周波数に対して防護された米国の F-22、F-35等のステルス機は、L、UHF、VHF および HF のような波長の長いバンドのレーダーで探知できる。ロシアはこのような米国のステルス機を探知するために低周波レーダーとしての VHF レーダーを開発している。Nizhny-Novgorod 無線技術研究所（NNIRT）が開発した55Zh6UE Nebo-U は1990年代に実用化されており、ロシア初の３次元 VHF レーダーである。NNIRT は、その後、VHF バンドの AESA を試作し、この VHF 方式の AESA を55Zh6M Nebo-M マルチバンドレーダーとして生産し、ロシア空軍に100セット納入している。

Nebo-M は、VHF バンドの RLM-M、L バンド（UHF）の RLM-D および S／X バンドの RLM-S の３基の AESA から構成されるトラック搭載レーダーである。各レーダーは、Orientir 位置決定システムおよび GLONASS 衛星航法システムを装備し、地上制御車両に無線または有線で接続されている。NNIRT によると、中国の DF-15短距離弾道ミサイルの RCS は X バンドおよび VHF でそれぞれ0.002m²および0.6m²である。Nebo-M は、３つのレーダーのデータを融合して目標精度を向上している。VHF で大枠方位を探知しより高周波のレーダーを目標に集中して探知および追尾確率を向上している（Multiple Hypothesis Tracking）。また、Nebo-M と同様なマルチバンドレーダーのステルス対抗技術は、S-400にも使用されている。

また、ロシアのステルス機早期警戒レーダーとしての OTH レーダーには、VHF バンドを用いた探知距離および探知高度がそれぞれ1,100km および100km の Rezonans-NE がある。

(6)　中国の航空機搭載自衛用電波妨害装置およびステルス対抗技術

ア．航空機搭載自衛用電波妨害装置 KG300G および KG600[85)86)87)]

中国は、航空機搭載自衛用電波妨害装置として国産の KG300G および KG600を開発および運用しているが、まだ、ロシアの SAP-14のような敵防空網制圧用電波妨害コンテナを開発していない。

中国の四川省成都市にある電子科技集団公司（CETC）第二十九研究所（南西電子装置研究所）は、KG300G を開発し、広東省の1998年の珠海航空ショーにおいて初公開した。KG300G は、DRFM（Digital Radio Frequency Memory）を用いた電波妨害技術によって実現され、10-20GHz（J バンド）の脅威レーダーに対応している。中国空軍は、この KG300G を2013年に運用開始し、FC-１多用途戦闘機、JH-７戦闘爆撃機、J-11戦闘機および J-10戦闘機に搭載している。

また、CETC 第二十九研究所は、広帯域の脅威レーダーに対応する1.0-18GHz（D-J バンド）の自衛用電波妨害ポッドとして、KG600を開発し、2014年の珠海航空ショーにおいて初公開した。KG600は、陸上および艦船に関する広帯域の１-18GHz（D-J バンド）の脅威レーダーに対応するために中型および大型機用に開発された航空機 ELINT システム KZ800を小型化して、KZ900 ELINT ポッドと併せて開発され

KG600搭載 JH-7A 戦闘爆撃機

SPS-171およびKG600搭載 Su-30MKK 戦闘爆撃機

KG600搭載 H-6M 爆撃機

出典：http://www.matrixgames.com/forums/tm.asp?m=3789961&mpage=6&key=&

図4.5　KG600搭載の JH-7A、Su-30MKK および H-6M

たものである。中国は、既に KG600を図4.5に示すとおり Su-30MKK 戦闘機、JH-7A 戦闘爆撃機および H-6G／M 爆撃機に搭載している。

北京の中国軍事ネットワークによると、中国は、JH-7A が電子攻撃耐性、搭載能力および航続性能から国産電子戦機プラットフォームとして最適であると見なしている。

また、中国は、ロシア製 Su-30MKK を空軍機および海軍機としてそれぞれ73機および24機を輸入し、2010年から運用している。Su-30MKK には、自衛用電波妨害ポッドとして Khibiny の旧バージョンである 6 -10GHz (H-I バンド) の脅威レーダーに対応できる SPS-171／L005 Sorbtsiya-S が搭載されている。図4.5の Su-30MKK の写真から分かるようにロシア製 SPS-171および中国製 KG600がそれぞれ機体両翼端および胴体下部に搭載されている。中国の Su-30MKK は、KG600の増設によって、J バンドの脅威レーダーにも対応できるロシア製 SAP-518と同等の能力を実現している。

さらに、2015年11月に、中国が24機の Su-35をロシアから調達することが報道されている。中国は、Su-35を用いて自衛用および敵防空網制圧用電波妨害能力を持つロシア製の最新の Khibiny-10V を導入すれば、新しい電波妨害・SEAD 機を実現できる可能性がある。

イ．ステルス対抗技術[88)89)90)91)]

中国は、ステルス機探知のためにアクティブおよびパッシブ両方を組み合わせた低周波レーダーの開発を行っている。中国は、2014年の珠海航空ショーにロシアの VHF バンド RLM-M と同様の VHF バンド AESA 装備 JY-27A Skywatch-V、UHF バンドフェーズアレイレーダーJY-26を展示している。JY-27A および JY-26は、それぞれ最大探知距離500km および300km のステルス機探知能力を持っている。中国によると、JY-26は2015年の米韓共同軍事演習時に韓国上空の F-22を探知した実績がある。

また、中国は、民間 FM 放送波等を使用する VHF バンド JY-50パッシブレーダーの開発を行っている。中国海軍は、VHF レーダーを維持し、最新の Type 52C Luyang II および Type 52D Luyang III のような水上艦にも搭載している。

(7)　我が国の航空機搭載電子戦システムおよびステルス対抗技術

ア．航空機搭載電子戦システム[92)93)]

我が国の航空自衛隊の F-15J／DJ は F-15C／D を原型とするが、アメリカ議会から批判を受けた国防総省の決定により提供されなかった自衛用電波妨害装置を含む TEWS (戦術電子戦システム) については、国内で独自開発した J／TEWS で代替している。J／TEWS は国産の J／ALQ-8 電波妨害装置と J／APR-4 レーダー警戒受信機、ライセンス生産の AN／ALE-45J 射出型妨害装置（チャフ・フレアディスペンサー）から構成される。

また、「F-15の近代化改修」において、自己防御能力の向上（レーダー警戒・電波妨害・射出型妨害装置能力向上）のために統合電子戦システム（IEWS : Integrated Electronic Warfare System)として換装された。これは、F-2 支援戦闘機(戦闘攻撃機)用に開発された J／ASQ-2 IEWS を F-15J 用に改良したもので、J／APR-4A／-4B レーダー警戒装置、J／ALQ-8B 機上電波妨害装置、AN／ALE-47射出型妨害装置（チャフ・フレアディスペンサー）で構成され、それらを専用の電子戦コントローラ（EWC）で統合し、脅威レーダーの受信から識別・脅威度評価、対抗策実施までを自動で行うものである。

敵防空網制圧用電子妨害装置については、

2008年から電子戦機としてF-15DJに搭載する600ガロン増槽と同じ大きさと形状を持つポッド型の「戦闘機搭載型電子防御装置」が開発されている。

また、電子戦の基盤技術であるAESA技術では、実用機搭載では世界初のガリウム－砒素（GaAs）半導体製のAESAレーダー（J／APG－1）をF－2に搭載している。これはGaAsの送受信素子800個を直径70cmの平面アンテナ上に並べたものである。さらに、「F－2の近代化改修」において、GaAsよりも3倍の出力が得られる窒化ガリウム（GaN）による送受信素子1,216個のAESAレーダー（J／APG－2）が開発されている。

イ．ステルス対抗技術[94)95)]

我が国では、ステルス機等の低レーダー断面積（RCS）目標を探知・追尾するための航空機搭載センサ・システムの要素技術として、遠距離の赤外線を放射する目標を探知・識別して警報を発するとともに、これを追尾する機能を備えた「赤赤外線捜索追尾システム（IRST system：Infra-Red Search and Track system）」、米海軍のINTOPおよびNGJのRFセンサの開発と同様に航空機、艦船等への適用可能なレーダー、ESM、ECMおよび通信の複数機能を1つのアンテナで実現できる「スマートRFセンサ」が開発され、さらにそれらの成果を活用してIRセンサおよびRFセンサ（レーダーおよびESM）の高性能化並びにIRセンサ情報およびRFセンサ情報の統合化による低RCS目標に対する探知・追尾能力の向上のための「先進統合センサ・システム」が研究開発されている。

また、ステルス機等の探知・追尾のための将来の警戒管制レーダーの要素技術として、早晩性能限界が予想される従来の能動アンテナの大型化・高出力化等による探知能力の向上に代わって、分散配置した複数のアンテナからの送信（受信）信号を合成し高いアンテナ利得を得るMIMO（Multi-Input Multi-Output）技術による分散レーダーに基づく「次世代警戒管制レーダー」が研究開発されている。さらに、これは、レーダーのための電波送信源として、他のレーダー波や放送波を送信源として受信のみで動作する受動レーダーとしての運用も可能である。

(8) 我が国のHPMミサイルおよびEMP弾構成システム

我が国においても、水上艦への搭載を目的とした高出力マイクロ波によるHPMミサイルを実現するための要素技術として小型高出力増幅器およびアンテナの研究開発並びにミサイル形状のEMP弾構成システムを実現するための要素技術として小型電源技術およびEMP発生技術の研究開発が行われている。

4.2 主要な電磁サイバー防御技術

電磁波利用によるサイバー攻撃に対する防御技術の例としては、DoDおよびDARPA無人機対ハッキングシステム、電磁スペクトラムCOP実現のための米軍の電磁スペクトラム管理システム、米海軍の衛星通信およびGPS航法のA2／AD対策、および米国におけるEMP防護がある。

(1) 米軍の無人機対ハッキングシステム

電磁波利用によるAPT攻撃として、イランおよびロシアによる米軍無人偵察機への電子妨害および情報欺瞞による無傷捕獲事案が2.2で述べたとおり発生している。このような事案では、無人機の遠隔制御、GPS受信機等のソフトウェアに存在する脆弱性を使用している。また、現在の軍用および民間の無人機のソフトウェアはセキュリティ設計が不十分であることおよび統計的品質管理に基づくソフトウェア開発方法を用いていることから脆弱性が潜在的に存在している。米軍は、このような無人機のソフトウェアの脆弱性低減および脆弱性ゼロ化を目的とした無人機対ハッキングシステムを開発している。

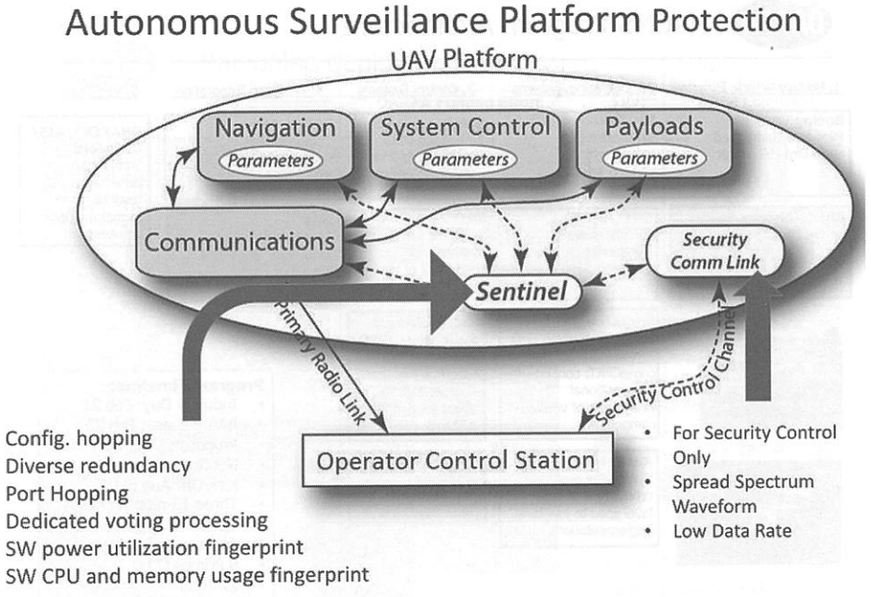
ア．DoDの無人機対ハッキングシステム（脆弱性低減）[96)]

DoD出資によって、バージニア大学は、APT攻撃のようなサイバー攻撃を防御するためのサイバーセキュリティ、冗長設計、自動制御等に基づく最も重要な機能を直接防御する「System-Aware Cybersecurity」研究開発成果に基づき、ユースケースの1つとして無人機対ハッキングシステムとして「System-Aware Secure Sentinel」をジョージア工科大学と共同開発し、4つの異なるサイバー脅威に対する5日間のデモ試験を実施し成功した。

本システムは、被害機能の新しい検知および隔離の手段並びに被害システムを安全状態に復旧する基盤を提供する。また、セキュリティ管理用に防護された無線通信回線を提供する。本システムの全体構成を図4.6に示す。試験におけるサイバー脅威は、地上からの電磁サイバー攻撃、他の飛行体からの電磁サイバー攻撃、サプライチェーン攻撃およびインサイダー攻撃である。試験における当該システム能力への負荷領域は、GPSデータ、位置データ、画像情報メタデータおよび無人機搭載監視制御ペイロードである。

イ．DARPAの無人機対ハッキングシステム（脆弱性ゼロ化）[97)98)]

米国のDARPAのHACMS（High Assurance Cyber Military System）プログラムの目標は、高い保証された組み込みシステム（Cyber



出典：Rick A. Jones and Barry Horowitz, Sentinel Based System-Aware Security for Unmanned Wireless Systems, Uva, 2014

図4.6 DoDの無人機対ハッキングシステムの全体構成

-Physical System）構築技術を創出することである。無人機の制御および航法能力への電磁サイバー攻撃を阻止するための対ハッキングシステム（Anti-hacking System）は、HACMSプログラムのユースケースの１つである。

HACMSのソフトウェアは、大規模なサイバー攻撃に対しても数学的に脆弱でないことが証明されている。サイバー攻撃に対して脆弱でないことを数学的に保証したソフトウェアを実証のために小型無人機に実装している。従来の軍用および民間の無人機は電磁サイバー攻撃に脆弱であるため、HACMSでは独自の高い保証されたソフトウェアに全面的に作り直している。HACMSは、新たにシステムアーキテクチャモデル、ソフトウェア構成部品およびOSをOSS（Open Source Software）形態で開発している。

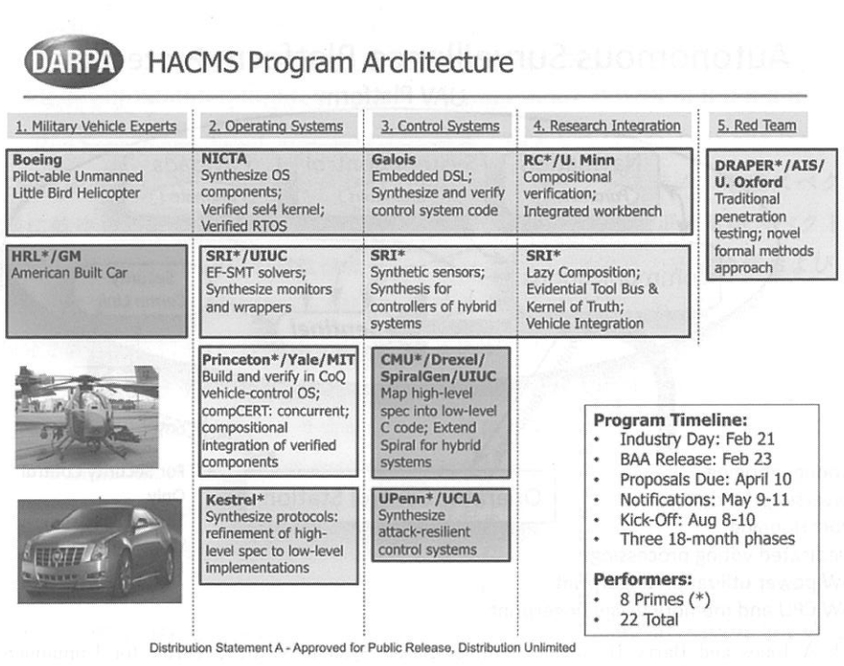
HACMSプログラム用ソフトウェアは、大規模プラットフォームに調整できるので、組み込みシステム用セキュリティ基盤である。HACMSプログラムの全体アーキテクチャを図4.7に示す。

(2)　米軍の電磁スペクトラム管理システム

米軍では、電磁スペクトラム管理ドクトリンに基づいて電磁スペクトラム管理システムが構築されている。

ア．DoDの電磁スペクトラム情報システム（GEMSIS）[99]

国防情報システム局（DISA）は、いつどこでも所要のスペクトラムにアクセスできるようにDoDの動的な電磁スペクトラム管理を可能とするGEMSIS（Global Electro-Magnetic Spectrum Information System）を開発し、アフガニスタンにおいて使用している。これは、次に示す主要能力から構成される。



出典：Kathleen Fisher, High Assurance Cyber Military System, DARPA, 20 May 2013

図4.7　HACMSプログラムの全体アーキテクチャ

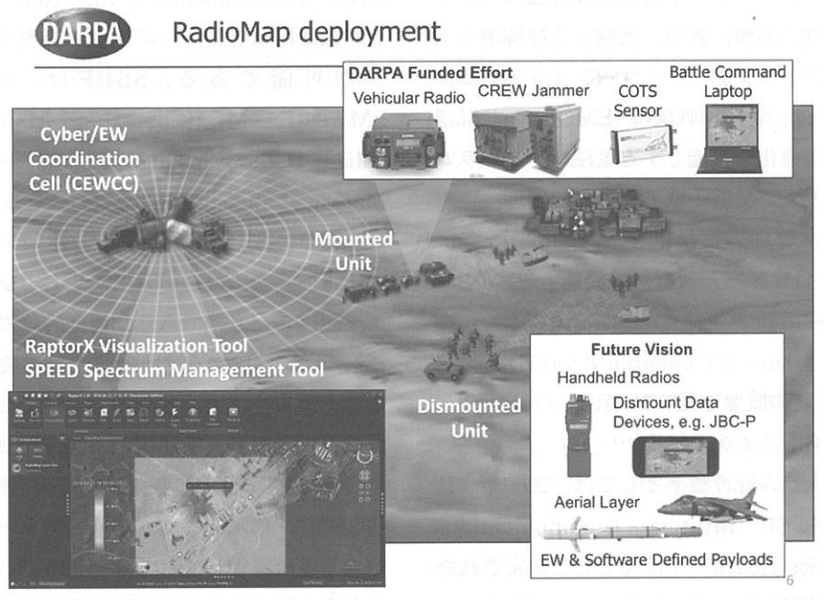
・Host Nation Spectrum Worldwide Database Online（HNSWDO）：ホスト国周波数スペクトラム依存装置サポート性可視化
・SPECTRUM XXI Online（SXXIO）：DoD標準電磁スペクトラム管理ツール（統合地図化、可視化、コンプライアンス検査および設計分析）
・Stepstone：DoD装置認証プロセス
・Joint Spectrum Data Repository（JSDR）：電磁スペクトラム管理データ総合リポジトリ（NIPRNETおよびSIPRNET経由）

イ．DARPAの電磁スペクトラム状況認識[100]

DARPAは、米海兵隊の電磁スペクトラム戦（EMSO）における電磁スペクトラム状況認識のためのAdvanced RF Mapping（RadioMap）の研究開発を行っている。これは、各種プラットフォームに搭載されたRFセンサが取得した電磁スペクトラム放射データを地図上に可視化するものである。電磁スペクトラム管理ツールとしては、シカゴ大学の開発したRaptor X可視化ツールを用いたSPEED Spectrum Management Toolを開発している。RadioMapの概要を図4.8に示す。

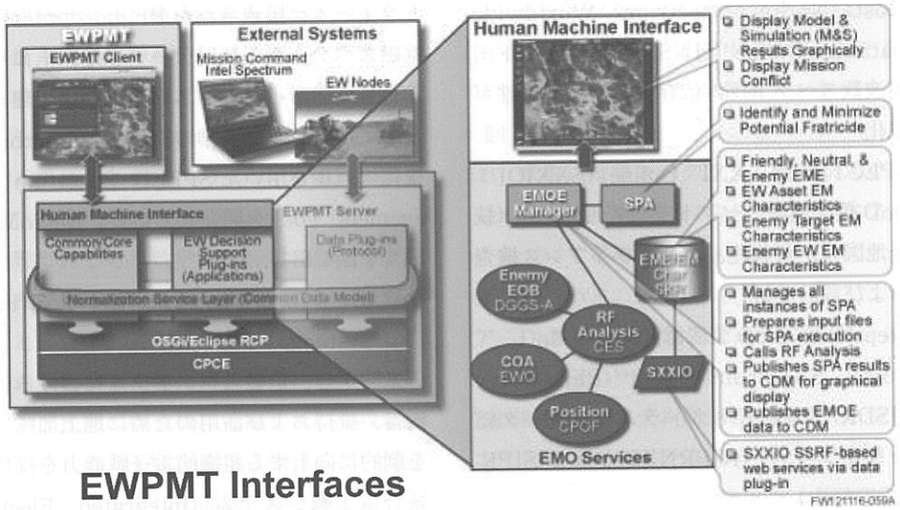
ウ．米陸軍の統合電子戦システムFoS（Family of Systems）[101]

米陸軍は、電磁スペクトラムにおける優位の獲得、維持および活用のために地上部隊の能力を劇的に向上する組織的電子戦能力を提供する統合電子戦システム（Integrated Electronic Warfare System：IEWS）FoSを開発している。IEWS FoSは、彼の兵士、プラットフォームおよびシステムを攻撃および窃取する多機能電子戦（MFEW）、電子戦活動の計画、調整および統合を行う電子戦計画管理ツール



出典：Dr. John Chapin, Advanced RF Mapping (RadioMap) Phase 3, DARPA, 6 Jan. 2015

図4.8　RadioMapの概要



出典：Michael E. Ryan, Electronic Warfare's Role in Cyber, AFCEA TECHNET, 11 Sept. 2014

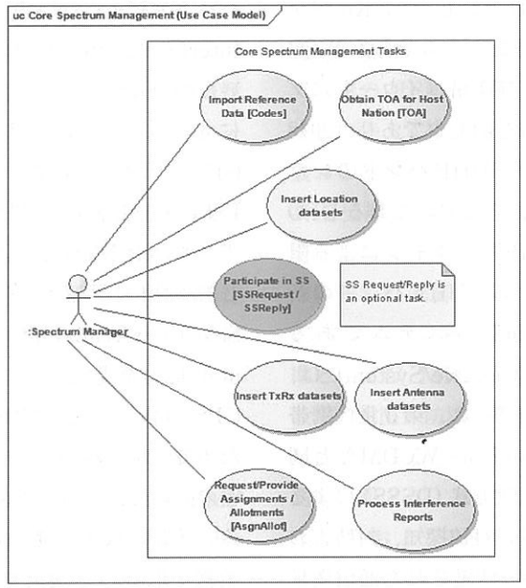
図4.9　EWPMT のシステム概要

(EWPMT)、および我の兵士、プラットフォームおよびシステムの防護を行う防勢電子攻撃(DEA)から構成される。EWPMT は、電子戦将校およびスペクトラム管理者の電磁スペクトラムの計画、調整、管理、統制および解消を支援するソフトウェアアプリケーションである。EWPMT は、電磁作戦環境(EMOE)の状況認識および可視化を可能とする電磁スペクトラムCOP、攻勢・防勢電子戦アセットの管理、電磁環境データ管理等を提供する。また、今後、EMPWT はサイバー状況認識機能も包含し、サイバー電磁活動(CEMA)のツールの1つになる。

EMPWT の概要を図4.9に示す。

エ．スペクトラム管理標準[102]

スペクトラム管理標準としては、2009年3月2日にMCEB(Military Communications-Electronics Board) Pub 8として制定されたDoD の SSRF(Standard Spectrum Resource Format)がある。SSRF 準拠システムは、National Telecommunications and Information Administration(NTIA)、North Atlantic Treaty Organization(NATO)および Combined Communications-Electronics Board(CCEB)国家とのスペクトラム管理データの交換が可能である。SSRF は、NATO の SMADEF-XML(Spectrum Management Allied Data Exchange Format-eXtensible Markup Language)に基づいて作成されたものである。SSRF 文書は、スペクトラム管理関連データの交換のための運用構想およびデータ要素を記述したものであり、地理的位置情報、装置パラメータ、スペクトラム支援度要求と関連ホスト国宣言、周波数割当、一時または恒久周波数要求と割当、干渉報告、統合制限周波数リスト(JRFL)、統合通信電子運用規則(JCEOI)、部隊要素、プラットフォームおよび対兵器電磁障害(HERO)を含んでいる。スペクトラム管理業務の概念図を図4.10に示す。



出典：MCEB, Standard Spectrum Resource Format (SSRF) Pub 8, 02 March 2009

図4.10　スペクトラム管理業務の概念図

(3) 米海軍の衛星通信およびGPS航法のA2／AD対策

米海軍はA2／AD脅威に対応するために商用衛星通信および軍用衛星通信の攻撃面の削減のための端局装置の統合化並びに対妨害能力の付与および新しい高抗担性衛星打上を行っている。また、米海軍は、米空軍宇宙ミサイルセンターによるGPS近代化計画に合わせてGPSの抗担性向上のためにGPSアンテナの対妨害化およびすべての洋上プラットフォームに確実なGPS測位・航法・時刻(PNT)サービスを提供するGPNPSへの移行を行っている。

ア．米海軍の衛星通信のA2／AD対策[103]

米海軍は、現在、洋上通信のために商用衛星通信および軍用衛星通信を使用している。商用衛星通信には、Cバンドおよび Inmarsat の Lバンドがある。軍用衛星通信には、Kaバンドの UFO／GBS(UHF Follow On／Global Broadcast Service)、X／Kaバンドの WGS(Wideband Global SATCOM system)、Xバンドの DSCS(Defense Satellite Communication System)、Qバンドの UFO／EHF(UHF Follow On／Extremely High Frequency)および MILSTAR がある。商用衛星通信は、商用広帯域衛星プログラム(Commercial Broadband Satellite Program：CBSP)により C、Xおよび Ku バンドの端局装置が統合化される。また、軍用衛星通信は、米海軍マルチバンド端局装置(Navy Multiband Terminal：NMT)により UFO、WGS、DSCS および MILSTAR 並びに新しい Qバンド高抗担性軍用衛星通信システムである AEHF(Advanced EHF)および北極地域用 AEHF 補完システム(Enhanced polar System：EPS)の端局装置が統合化される。GBS の端局装置は、現行と同様である。

X／Kaバンドの新しい広帯域軍用衛星通信

システムであるWGSおよびC／X／Kuバンドの商用広帯域衛星通信システムであるWGSは、既存衛星モデムおよび衛星ペイロードにプラグイン式の対妨害能力を開発中であり、2018年にデモを予定している。UHFバンドのレガシー狭帯域軍用衛星通信システムであるUFOは、FLTSATCOM EHFパッケージによる限定対妨害能力を有している。UHFバンドの新しい狭帯域軍用衛星通信システムであるMUOS（Mobile User Objective System）は、2012年に初号機が打ち上げられ、第3世代携帯電話方式で使用されている3G WCDMAと同様な直接スペクトラム拡散方式（DSSS）による対妨害能力を有している。対被探知、対妨害および対HEMP能力を持つ防護された通信衛星としては、レガシーのMILSTAR並びに新しいAEHFおよびEPSがある。AEHFは、周波数ホッピングスペクトラム拡散方式（FHSS）に基づく対妨害能力および対HEMP能力を持つ最新の軍用衛星通信システムである。本システムは、英国、カナダおよびオランダとも連接している。また、CSBA報告書（2013年）では、中国のA2／AD脅威に対応するために米国の同盟国である日本、韓国および豪州に対して防護されたAEHF衛星ペイロードへのグローバルアクセス提供が提案されている。AEHFは、合計6機の打上が計画されており、現在3号機まで打ち上げられている。

イ．米海軍のGPS航法のA2／AD対策[103)104)105)106)107)]

現行の米海軍のGPS航法能力を提供するGPSアンテナであるFRPA GPA（Fixed Reception Pattern Antenna GPS Antenna）、GPS受信機、軍用GPS航法システムであるAN／WRN-6（V）衛星信号航法装置、および各種航法・時刻信号の収集、処理および配布を行うNAVSSI（Navigation Sensor System Interface System）は、対妨害能力が十分でないため、GPSアンテナの対妨害化を行うとともにすべての洋上プラットフォームに確実なGPSベースPNTサービスを提供するGPS PNT Service（GPNTS）への移行が計画されている。GPNTSでは、GPSの安全保障措置として汎用対欺瞞GPSモジュール（SAASM：Selective-Availability Anti-Spoofing Module）能力を提供する。SAASMの主な利点は、GPSの有効無効選択が2000年5月に停止されたので、機密扱いでない国家安全保障局の「機密の」暗号鍵に基づく対欺瞞のためとなっている。それは放送で鍵の配布を行うというような柔軟な取扱いを選択することを可能にする。SAASMキーは、各々のユーザーグループに1対1に関係し、各々が別々の暗号ネットワークに属しているとはっきり認識できる。

また、米空軍宇宙ミサイルセンターによるGPS近代化計画において打ち上げられているGPS IIR-MおよびGPS IIFの改良型衛星並びに今後打ち上げられるGPS III衛星は、対妨害強靭性、同志電子攻撃互換性、次世代暗号、対欺瞞等の抗担性を付加した軍コード（M-Code）を送信する。将来、GPNTSも、軍コードに対応する予定である。さらに、GPS IIIのセキュリティアーキテクチャは、SAASMを越えるものであり、PRONAV（Protection of Navigation）と呼ばれている。PRONAVのセキュリティアーキテクチャは、縦深防御（defense-in-depth）および情報保証の原則の適用を通して、GPSミッションの効果を保全する。PRONAVのセキュリティはGPS信号の完全性を保証するために、暗号技術以上のものに頼って、追加の技術的手段と運用技術を使用する。

GPSの次世代地球制御局（OCX）のサイバー防御対策としては、冗長性のあるアーキテクチャの採用、17ヶ所の地上監視アンテナの更新、GPS主・縦制御局の更新と自動切替、インターネットに接続しないクローズ系システム、アップリンク制御信号の暗号化と常時監視・制御、暗号とセキュアコーディングを有するソフトウェア開発者による開発、ソフトウェア脆弱性を把握しやすいオープンソースソフトウェアによる開発等を挙げている。

(4)　米国におけるEMP防護

米国における重要インフラおよび米軍のEMP防護の現状並びに重要インフラのEMP防護対策および北朝鮮の軌道爆弾の対策について述べる。

ア．重要インフラおよび米軍のEMP防護の現状[108)109)]

EMP脅威は国土安全保障省によって活用されている15分野国家計画立案シナリオに入っていない。米国は、電力網、通信およびその他重要インフラのEMP防護は未対応である。また、米国は、超高圧変圧器の製造能力がないため電力網の復旧に長期間を要する。米軍は、冷戦期からのレガシー軍用システムはEMP防護対応済みであったが、冷戦後、軍用システムのEMP防護プログラムの廃止およびEMP防護未対応のCOTSが増加している。したがって、米軍は、軍用システムのEMP防護を限られた国防予算内で再開している。米国の核攻撃に対する早期警戒および指揮統制を行う北米防空司令部（NORAD）の第1本部は、10年間ピーターソン空軍基地近傍に設置されてきたが、重要なNORAD作戦能力がシャイアン山に復帰させられており、DoDは2015年4月に、2020年までの電子機器のEMP防護性能向上のための7億ドルの事業契約を行っている。また、国防長官は国家電力網のEMP防護のために2017会計年度に20億ドルの予算を承認している。

米軍のHEMP防護標準としては、共通標準並びに陸上C4I施設（固定および移動式）、軍用機および水上艦の個別標準が制定されている。共通標準には、MIL-STD-2169B（HEMP環境）、MIL-STD-461F（サブシステムおよび装置の電磁特性制御要求）およびMIL-STD-464C（システムの電磁環境影響要求）がある。個別標準としては、MIL-STD-188-155-1（陸上C4I施設用HEMP防護、第1部　固定式施設）およびMIL-STD-188-155-2（陸上C4I施設用HEMP防護、第2部　移動式施設）が、それぞれ1998年7月および1999年3月に制定され、MIL-STD-3023（軍用機用HEMP防護）およびMIL-STD-4043（水上艦用HEMP防護）がそれぞれ2011年11月および2016年1月に制定された。

イ．重要インフラのEMP防護対策

EMP脅威に焦点を絞った新国家対応計画立案シナリオ策定のための重要インフラ防護法（CPIA）案がまだ議会承認されていない。また、国内電力網を防護するためのSHIELD法案の上院承認が得られていない。これらの議会承認を得るために、米国諜報権限法案（FY2015）が2014年12月12日に米国上院を通過し、2014年12月19日に大統領署名が行われた。本法329条は、国家情報長官が「2025年までの米国国益に対して、外国および外国非国家主体からの脅威を含む人工のEMP兵器によって生起する脅威に関する報告」を本法公布後6ヶ月以内に行うことを指示している。

CPIA案については、2015年6月に国土安全保障委員会を通過し、下院に付議された段階である。また、SHIELD法案については、委員会レベルでも審議が再開されていない状況である。

ウ．北朝鮮の軌道爆弾の対策[110]

米国の元国家ミサイル防衛局長官であったAmbassador Henry F. Cooperは、北朝鮮の軌道爆弾の対策を次に示すとおり提言している。

① 報復宣言政策および北朝鮮衛星打ち上げペイロードの信頼のある機関（例えば、IAEA）による検査を行うこと。この要求が拒否された場合、打ち上げられたそのような衛星を撃墜することを米国の政策とすること。

② ブーストフェーズのUnha-3 SLVを迎撃するために大気圏内の弾道ミサイルに対する試験で3発中3命中であるイージスSM-2-Block IVの改善された目標標定アルゴリズムを使用すること。

③ 大気圏外でのSM3 Block 1A／BまたはBlock 2Aによる迎撃のために、TPY-2レーダ（Xバンドレーダー）をフィリピンに配備すること。

④ 現在、カリフォルニア州Vandenberg空軍基地に配備された地上ベース迎撃兵器は、Vandenberg指揮統制システムが、その迎撃兵器を正しい戦闘空間にキューイングするために適切な極軌道パラメータを提供される場合、おそらく北朝鮮からのFOBSを迎撃できる。③で勧告されたフィリピンの同一レーダーは、この必要とされるキューイング情報を提供できる。

⑤ 最終的に、多層防御でさえ完全ではないので、電力網は最高国家優先度として強化されること。上記で述べた既存のBMD運用能力を活用する高価でない高効果な方法を直ぐに採ること。

5．おわりに

A2／AD脅威の出現によって、戦闘様相は、従来の戦闘領域である陸上、海上、水中、空中および宇宙領域にサイバー空間および電磁スペクトラム領域が加わって、大きく変化している。日露戦争の二百三高地争奪戦は陸上における高地優位の制高権確保の戦いであった。日露戦争の日本海海戦は、大艦巨砲の艦隊決戦による制海権確保の戦いであった。大東亜戦争のミッドウェー海戦は、空母対空母の航空兵力決戦による制空権確保の戦いであった。イラク戦争は、NCWにより情報優位を確保した精密誘導兵器による戦いであった。このように戦争では、一度使用された過去の戦い方は通用しないため常に新しい戦闘方法が創出されてきた。最近のウクライナ紛争およびシリア紛争においては、無人機の無傷捕獲、C4ISRシステム、武器システム等の無力化を行うためにロシアによるサイバー電磁戦が使用されており、電波妨害により低下した通信環境においては米国が優位性を持っていたNCWが通用しなくなってきた。また、A2／AD環境においては、対艦ミサイルによる飽和攻撃に加えてEMP攻撃を含むサイバー攻撃および電子攻撃が蓋然性の高い大きな脅威であり、従来のハードキル能力だけではコスト的にも対応に限界があるためソフトキル能力による対応が求められている。さらに、高列度のA2／AD環境においては、各種プラットフォーム、C4ISRシステム、武器システム等の電磁スペクトラム依存システムが低下した通信環境でも作戦継続できる低－無出力のセンサ、通信および対抗手段のような電磁スペクトラム戦能力を確立するために新しい作戦構想および能力の確立が必要である。

米海軍は、このようなA2／AD環境において決定的な軍事的優位性を獲得するための新しい戦闘方法として、陸上、海上、水中、空中、宇宙、サイバー空間および電磁スペクトラム領域の全領域アクセスを実現するためにそれらの共通領域である電磁スペクトラムを支配する電磁機動戦の概念を開発している。電磁機動戦は、電磁シグネチャの理解と統制、機動空間としての電磁スペクトラムの指揮、および運動と非運動の統合火力の配布のための電磁スペクトラムの活用を行うものである。電磁機動戦を支援するためには、電磁スペクトラムの状況認識、操作および活用能力を実現する電磁戦闘管理システムの構築が必要である。我が国においても、電磁戦闘管理システムの開発については、電磁スペクトラム領域の電磁機動戦の平時における作戦領域認識(戦闘環境認識)、有事における作戦領域認識（戦闘状況認識）および脅威の認識別が、水中領域の対潜水艦戦とのアナロジーで考えられるため、対潜水艦戦における思考過程を活用すべきである。

参考文献

48) JP3-12(R), Cyberspace Operations, 05 Feb. 2013
49) JP3-13.1, Electronic Warfare, 08 Feb. 2012
50) JP6-01, Joint Electromagnetic Spectrum Management Operation, 20 March 2012
51) Admiral Jonathan W. Greenert, Imminent Domain, U.S. Navy, Proceedings, Dec. 2012
52) HQ, DoA, FM3-38, Cyber Electromagnetic Activity, Feb. 2014
53) The Monitor News, DoD establishes new top-level EW programs council, JED, April 2015
54) Earl Wyatt, Prototyping: A Path to Agility, Innovation and Affordability, 24 March 2015
55) Defense Science Board, 21st Century Military Operations in a Complex Electromagnetic Environment, July 2015
56) Bryan Clark and Mark Gunzinger, Winning the Airwaves: Regaining America's Dominance in the Electromagnetic Spectrum, CSBA, Dec. 2015
57) U.S. Navy, Navy Strategy for Achieving Information Dominance 2013-2017, Nov. 2012
58) U.S. Navy Information Dominance Roadmap 2013-2028, March 2013
59) DoN, A Cooperative Strategy for 21st Century Seapower, March 2015
60) STATEMENT OF ADMIRAL JONATHAN GREENERT, U.S. NAVY CHIEF OF NAVAL OPERATIONS BEFORE THE HOUSE ARMED SERVICES COMMITTEE ON FY 2015 DEPARTMENT OF THE NAVY POSTURE, 12 MARCH 2014
61) SYDNEY J. FREEDBERG JR., Navy Forges New EW Strategy: Electromagnetic Maneuver Warfare, Breaking Defense, 10 Oct. 2014
62) CDR Thor Martinsen, Dr. Philip E. Pase and Lt Col (Ret.) Edward L. Fisher, Maneuver Warfare in the Electromagnetic Battlespace, JED, Vol. 37, No. 10, Oct. 2014
63) Dr. Michael A. Pollock, RF Initiatives Electromagnetic Maneuver Warfare (EMW), ONR, 10 April 2014
64) John Haystead, Leap-Ahead SEWIP Technology Meets Next-Generation Threats Today, JED, Jan. 2015
65) Doug Small, Surface Electronic Warfare Improvement Program (SWEIP) Overview, PEO IWS, 15 April 2015

66) DoN, PE 0603271N／Electromagnetic Systems Advanced Technology, PB 2016 Navy, Feb. 2015
67) Joseph Horn, State of IAMD 2014 "IAMD Achievements", 12 June 2014
68) 石川潤一、輸入決定！E-2D早期警戒機、軍事研究、2015年1月号
69) Rockwell Collins, Tactical Targeting Network Technology
70) Richard B. Gasparre, The Israeli 'E-tack' on Syria Part I, strategic defense intelligence, 10 March 2008
71) Richard B. Gasparre, The Israeli 'E-tack' on Syria Part II, strategic defense intelligence, 11 March 2008
72) Jean-Jacque DeLisle, GaN-Based AESAs Enable U.S. Next Generation Jammer, 30 May 2014
73) Zachary Fryer-Biggs, DoD looking to "Jump the Gap" into Adversaries' Closed Networks, Defense News, 15 Jan. 2013
74) Boeing, CHAMP-Lights Out, 22 Oct. 2012
75) James S. Drew, USAF unveils roadmap for microwave weapons use, Flightglobal.com, 29 July 2015
76) Wikipedia, Khibiny (electronic countermeasures system), 6 Sept. 2015
77) Tatyana Rusakova, Blind & conquer: Top 5 Russian radio electronic warfare systems, 16 Feb. 2015
78) Dr. Carlo Kopp, Sukhoi Su-34 Fullback: Russia's New Heavy Strike Fight, Air Power Australia, April 2012
79) Dr. Carlo Kopp, Sukhoi Flankers: The Shifting Balance of Regional Air Power Australia, April, 2012
80) KRET, KRET to supply ECM pods for the Su-34, 07 Oct. 2015
81) Mark Prigg, Russia claims to have developed secret 'superweapon' capable of switching off foreign satellites and enemy weapons, 6 July 2015
82) GPD, Jamming the Jihad: Russian Electronic Warfare Systems Spotted in Syria, 5 Oct. 2015
83) Bill Sweetman, New Radars, IRST Strengthen Stealth-Detection Claims, AW&ST, 16 March 2015
84) Dr. Carlo Kopp, Russian／PLA Low Band Surveillance Radars, Air Power Australia, April 2012
85) China Defense Blog, KG300G Airborne Self-Protection Jamming Pod, 15 July 2010
86) Pakistan Defense Forum, JF-17 Thunder Multirole Fighter, 15 Nov. 2014 (http://defence.pk/threads/jf-17-thunder-multirole-fighter-thread-6.329675/page-58)
87) Ashley J. Tellis and Dan Blumenthal, Strategic Asia 2012-13: China's Military Challenge, 2012
88) Bill Sweetman, New Radars, IRST Strengthen Stealth-Detection Claims, AW&ST, 16 March 2015
89) Buffalo, China uses JY-26 UWB-radar to track F-22 and F-35 stealth fighters, china-arms.com, 5 Jan. 2016
90) Buffalo, Report: U.S. F-22 fighter detected and intercepted by China in East China Sea ADIZ, china-arms.com, 16 Feb. 2016
91) 中国电科38所新型出口装备亮剑中国国际国防电子展, 人民网, 13 May 2014
92) 松尾芳郎、航空自衛隊、装備近代化へ大きく前進、平成26年2月27日
93) 防衛省、平成26年度行政事業レビューシート：戦闘機搭載型電子制御装置、平成26年
94) 防衛省、平成27年度行政事業レビューシート：先進統合センサ・システム、平成27年
95) 防衛省、平成27年度行政事業レビューシート：次世代警戒監視レーダー、平成27年
96) Rick A. Jones and Barry Horowitz, Sentinel Based System-Aware Security for Unmanned Wireless Systems, Uva, 2014
97) Kris Osborn, DARPA Unveils Hack-Proof Drone, DEFENSETECH, 21 May 2014
98) Kathleen Fisher, High Assurance Cyber Military System, DARPA, 20 May 2013
99) Global Electromagnetic Spectrum Information System
100) Dr. John Chapin, Advanced RF Mapping (RadioMap) Phase 3, DARPA, 6 Jan. 2015
101) Michael E. Ryan, Electronic Warfare's Role in Cyber, AFCEA TECHNET, 11 Sept. 2014
102) MCEB, Standard Spectrum Resource Format (SSRF) Pub 8, 02 March 2009
103) Mark Glover, Communications and GPS Navigation Program Office (PMW／A 170), U.S. Navy PEO C4I, 28 Oct. 2015
104) Todd Harrison, THE FUTURE OF MILSATCOM, CSBA, 2013
105) J.R. Wilson, New Capabilities for GPS II／III, Aerospace America, Feb. 2010
106) Travis Mills, M-Code Benefits and Availability, USAF Space and Missile Systems Center, 29 April 2015
107) Dee Ann Divis, OCX and GPS Cybersecurity, Washington View, Nov.／Dec. 2013
108) Henry F. Cooper and Peter Vincent Pry, The Threat to Melt the Electric Grid, WSJ, 1 May 2015
109) John Franco, Nuclear Survivability Overview, 18 May 2011
110) Ambassador Henry F. Cooper, Defeat North Korea's FOBS!, The Atlantic and Conservation, April 11, 2014 (Blog.)