米海軍の情報優勢に関する最新動向について

株式会社NTTデータ　第二公共システム事業本部　第二公共システム事業部

角田　恭之　第二システム統括部長

木村　初夫　第二システム統括部嘱託

1．はじめに

近年、情報技術およびネットワーク技術の革新的進歩に伴い、世界がグローバル化され、紛争や戦争において物理的な軍事力（ハードパワー）だけでなくソフトパワーの一つであるサイバーパワーの活用が増加してきている。21世紀におけるサイバーパワーは、20世紀の革新的発明の一つである原子力に匹敵するものとして捉えられ、その活用については、まだ、十分な研究および技術開発が行われていない。

そのような状況の中で、米海軍は、NCW（Network Centric Warfare）コンセプトを海上戦闘領域、情報領域だけでなくサイバー領域まで統合した「情報優勢のための米海軍のビジョン」を構想し、そのビジョンに基づくロードマップを作成中である。

本論文では、情報優勢ビジョンの中核である情報優勢および意思決定優越の概念について整理し、情報優勢実現のための指針および情報優勢ロードマップの最新動向について述べる。また、米海軍の情報優勢を推進するための組織再編として、米海軍作戦本部再編、艦隊サイバー司令部編制およびそれらをサポートする情報優勢部隊編制について述べる。さらに、情報優勢部隊のためのサイバー／サイバーセキュリティ要員育成および情報優勢のための技術開発の最新動向について述べる。

2．背　景

オバマ米国大統領は、2009年5月29日演説において、「米国の技術的優位は、軍事優勢の鍵である。また、サイバー脅威が米国の直面する最も重大な経済および国家安全保障課題の一つである」と述べている。

また、ゲーツ国防長官は、2009年1月に、「米国は現在の優勢の保証ができておらず、その優勢の一貫性を保証するために計画、プラットフォームおよび要員に投資をしなければならない」と述べている。

米海軍作戦部長（CNO）は、それらを受けて、「CNO指針2009」において、「インテリジェンスと作戦の連携ならびに多くの方法でのネットワークの最適化は、プラットフォーム上での優先度を利用する。インテリジェンスと情報を正しく得られないとすると、プラットフォームは部分最適である。それ故、傑出と優勢を達成するためには、情報の優先度を上げる必要があ

る。米海軍はこの方法を既に運用しており、組織的に最終調整するときである」と述べている。米海軍は、情報（Information）を21世紀の米海軍戦闘能力のメインバッテリーにしようとしている。21世紀の戦いを成功させるために、米海軍は完全に統合された指揮統制、インテリジェンス、情報、サイバー空間、環境認識およびネットワーク運用能力を創成し、それを影響力の武器および手段として提供しようとしている。情報が軍事作戦の全範囲に渡って武器として扱われることになる。この情報中心海軍（Information-Centric Navy）への移行は、海軍力としてのあるべき新しいビジョンを示している。米海軍は、2010年5月にこのような情報を武器として扱う「情報優勢（Information Dominance）のための米海軍のビジョン」を発表した[1]。

3．情報優勢と意思決定優位

米統合軍のJoint Vision 2010／2020における物理領域および情報領域における情報優越による意思決定優越の情報力実現構想から近年の国家安全保障レベルのサイバー攻撃に対して物理領域、情報領域およびサイバー領域を統合した「情報優勢のための米海軍のビジョン」に至るまでの歴史を述べるとともに、「情報優越」と「情報優勢」の違いを明確にする。

3.1 情報優勢ビジョン

米海軍のセブロフスキー（VADM Arthur K. Cebrowski）中将は、1998年に「Naval Institute Proceedings」誌において、情報化時代における戦闘力を実現する情報力としてのNCW（Network Centric Warfare）の理論を発表した。これは、情報化時代の米国社会における情報技術ならびにビジネス過程と組織の共進化による変革を軍事に適用したものである[2]。アルバータ氏（David S. Alberts）およびガルストカ氏（John J. Garstka）は、NCWを「Network Centric Warfare、第2版」において、「センサー、意思決定者および戦闘者をネットワーク化することにより戦闘力を増大する情報優越（Information Superiority）基盤の作戦コンセプト」と定義している[3]。また、NCWは、米軍のJoint Vision 2010／2020（構想）を実現するためのコンセプトである。Joint Visionでは、情報優越基盤により意思決定優越（Decision Superiority）を実現し、全方位優勢（Full Spectrum Dominance）の達成を構想している[4]。

米海軍のNCWのビジョンであるSea Power 21を実現するための能力（Capability）計画は、NCWアーキテクチャであるFORCEnetとして推進されてきた。FORCEnetは、「戦闘者、センサー、指揮統制、プラットフォームおよび武器をネットワーク化された分散戦闘兵力に統合する情報化時代の海上戦闘のための運用構築コンセプトおよびアーキテクチャフレームワーク」と定義されている[5]。FORCEnetは、海軍作戦部長からの「2010年までにNCO（Net-Centric Operation：ネットワーク中心作戦）の実行可能、更なる戦力化は2030年まで」の前提で、ネットワーク上のすべてのノード（指揮官、幕僚等）が、すべての情報を必要な場合、いかなるノードからでも適時にアクセスでき、意思決定支援機能の利用を可能としている。

「情報優勢のための米海軍のビジョン」は、海上戦闘領域が中心であるFORCEnetに、情報領域およびサイバー領域における戦闘力を統合した情報力の構想と解釈される。

米海軍の情報優勢ビジョンは、「情報優勢のための米海軍のビジョン」において、「敵に対する情報優勢ならびに指揮官、作戦部隊および国家の意思決定優越を保証するためにゲーム変更能力を開発、展開および活用すること」と定義されている[1]。

3.2 情報優勢

Joint Vision 2020における統合軍作戦能力の変革の基盤である情報優越（Information Superiority）は、「同じことを行う敵の能力の利用または拒否の間に中断のない流れの情報の収集、処理および配信能力から導かれる作戦優位性（Operational Advantage）（JP 1-02）」と定義されている[6]。Joint Vision 2020では、情報優越を次の属性を持つことと特徴付けている[7]。

① 情報領域における優位（one's favor）の不均衡状態
② 不均衡状態は、現実には潜在的に一時的である。
③ 不均衡状態は、ある程度、情報作戦によって実現される。
④ この状態に貢献する情報は完全ではない。

したがって、情報優越は敵に対する一時的な相対的優位を創成する能力によって導かれる。

情報優勢については、情報作戦（Information Operation：IO）との関係で定義すべき用語であるが、JP 3-13において、まだ、定義されていない。

米陸軍では、情報優勢は「作戦優位性を達成するために情報システムと能力を所有者に使用させることのできる情報優越の程度（FM 100-6）」と定義している[8]。また、情報優勢の属性は、次のように検討されている[9]。

① 任務の迅速かつ決定的な達成に対する時間、場所および重大な意思決定課題について総合的な知識優位を構築するための攻勢および防勢情報作戦から結果する状態である。
② 彼よりも非常に確実、適時および正確な状況の彼の知識／理解を必要とする鍵となる条件である。
③ 平時から有事において常に適用するものである。
④ 情報優勢の達成には、我の情報の構築および防御ならびに彼によって入手される情報の劣化を含む。

したがって、情報優勢は、方策の選択自由度があり、総合的かつ決定的であり、情報領域の支配を意味している。

また、情報優勢の実現方法には、情報空間の形成（指揮官の情報要求の確立）、指揮統制防御（C2 Protect）の提供、指揮統制攻撃（C2 Attack）の実施、電磁周波数適応性の実行（行動の自由度の最大化）、状況理解の確立（正確および適時のCOP）および高い成果の達成（指揮官の正しい意思決定の最適時の実施）のステップがある。

米海軍においても、米陸軍で検討された情報優勢の属性を考慮して、情報を武器とするために、「情報優勢のための米海軍のビジョン」において、情報優勢を「米海軍任務に渡って決定的な競争優位性をいつ、どこで、どのように要求されようとも、情報領域における「高地」の確保および統制を行う能力である」と初めて定義したものと推察される[1]。

また、情報優勢は、作戦行動および活動（攻勢および防勢行動を運動的および非運動的に実施）を海上、情報およびサイバー空間の共通部分で行うための行動の自由を与えるものとしている。この共通部分で、米海軍は、戦闘オプションおよび効果を実現するために深い侵入、拡大した戦闘空間および情報優位性を活用しようとしている。現在、米海軍は、情報優勢を達成するために戦闘能力を徹底的に再調整しようとしている。

3.3 意思決定優越

情報優勢の実現によって意思決定優越を達成するものである。「情報優勢のための米海軍のビジョン」において、意思決定優越は、「指揮官にあらゆる時にあらゆる戦闘レベルで利用できるあらゆる選択肢を配布する方法で知識サイクルに対する情報への生データを遮断すること」と定義されている[1]。

また、意思決定優越のための武器としての情報は、拡大される戦闘空間、新しい作戦的および戦略的選択肢、非対称作戦効果および戦闘空間の優勢統制能力を実現する。武器としての情報は、海上および海軍任務の全範囲に渡って、影響力行使、拒絶、低下、分裂および破壊をするために適用される。

4．情報優勢実現のための指針

情報優勢実現のために指針は、ビジョンの初期段階に基本指針がブラシュアップされて、「情報優勢のための米海軍のビジョン」において、次のように示されている[1]。

① あらゆるプラットフォームがネットワーク経由で感知し、報告する。

② あらゆるセンサーおよびプラットフォームが適応的にネットワーク化される。

③ 収集器とセンサーは動的に任務付与および管理される。

④ あらゆるシューターと武器は、どのような収集器、センサーまたはデータリポジトリからも複合目標データの組み合わせ、評価、利用および使用できる。

⑤ データ処理、相関、利用、融合および分析は、集団的にネットワーク化される。

⑥ 遠隔誘導された自動および非随伴プラットフォームならびにセンシングおよび通信ノードの能力が重視される。

⑦ グローバルに統合化されたサービス指向バックボーンアーキテクチャは拡張可能なエンタープライズワイドサービスで実装される。

⑧ 現在、一つのモデルプラットフォームまたは武器だけをサポートしているどのようなセンサー、データリンク、ターミナルまたはプロセッサシステムもグローバルに相互接続されたネットワーク中心アーキテクチャに移行されるかまたは撤去される。

⑨ すべてのデータおよび情報は、普遍的に発見可能、透過的およびアクセス可能に提供される。データは海軍および海事領域に渡って標準化する。

⑩ 統合、国防、中間的政府機関、情報コミュニティパートナーのアーキテクチャおよびデータ資源は、海軍任務と作戦のサポートに積極的に活用する。

⑪ ネットワークセントリック作戦（NCO）に独自に関連する脆弱性およびリスクを厳密に説明、評価および緩和する。

⑫ 海軍情報専門家（Information Professional）は世界クラスの訓練、資格証明、経験およびツールを受ける。

5．情報優勢ロードマップ

米海軍は、情報優勢および意思決定優位を実現するために、2011年6月目途に情報優勢ロードマップの策定作業を進めている。

5.1 全体ロードマップの策定計画

これらロードマップは、情報優勢構想の推進および活動調整のためのメカニズムとして作成し、コンセプト、アーキテクチャ、ネットワーク、センサーおよび要員に関する情報中心

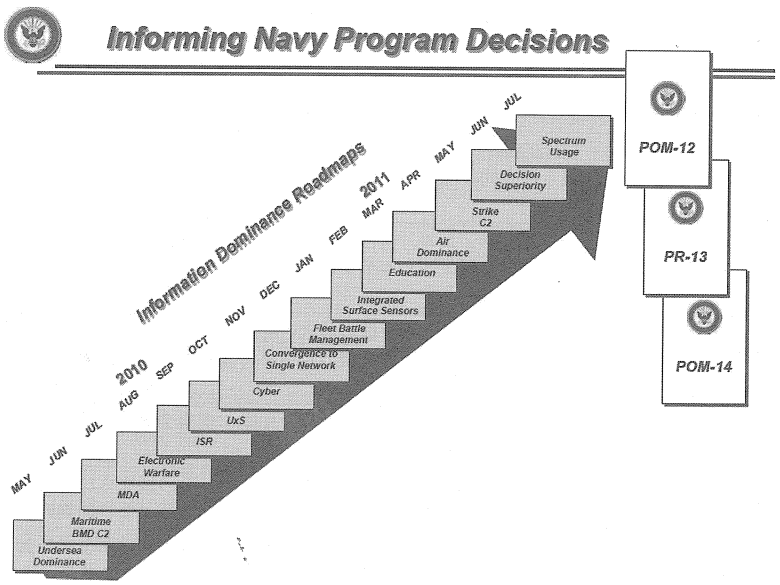


図5.1-1　情報優勢ロードマップの策定計画[10]

（Information-Centric）のガイダンスを提供するものである。米海軍は、それらの海軍情報要求、投資、能力および兵力整備のエンドツーエンドの検討および説明が同期するように調整してきた。また、PPBE（Planning, Programming, Budgeting and Execution）プロセスおよびPOM（Program Objective Memorandum）プロセスに基づく重要な情報優勢能力にフォーカスしたPOM-12 SPP（Sponsor Program Proposal）が国防総省に提出された。

これらロードマップを図5.1-1に示す策定計画で作成する。

それらロードマップの個別概要および主な相互関係をそれぞれ表5.1-1および図5.1-2に示す。

これらの個別ロードマップの中で、横断的な能力のロードマップは、単一ロードマップへの統合、サイバー空間作戦、艦隊戦闘管理、ISR、意思決定優越、電子戦、周波数利用、統合水上センサーおよび教育である。また、特定領域における特定任務または作戦の実施に絞った任務および領域のロードマップには、海事領域認識（MDA）、水中優勢、航空優勢、海上弾道ミサイル防衛、打撃指揮統制、UASがある。この中でも、MDAロードマップは、意思決定優勢に直接寄与する中心的役割を有する。

主要な横断的能力のロードマップについては、2010年7月22日に開催された最初の情報優勢に関する「米海軍情報優勢インダストリデー（Navy Information Dominance Industry Day）」会議の発表資料および後日発表された質問回答集[13]ならびに米海軍サイバー部隊（Naval Cyber Forces）季刊誌「InfoDomain」2010年秋号の記事に基づき、それらの最新状況を5.2～5.4に述べる。

表5.1-1　情報優勢ロードマップの個別概要[1)]

項番	項　目	内　　容
1	水中優勢	固定、移動体、有人および無人に渡る水中情報優勢を達成するための能力の調整およびネットワーク化
2	海上弾道ミサイル防衛（BMD）	段階的適応アプローチ（PAA）の実現ならびに作戦のすべての段階に渡る総合的なBMD能力の改善のためによりよい異なる方法での情報の利用
3	海事領域認識（MDA）	インテリジェンス、情報とネットワークの持込ならびに先の投資、技術および情報コミュニティ事業の活用による指揮官の意思決定優越の非常な促進
4	電子戦（EW）	同じ環境の敵の使用を彼の最大の課題にしている限り、どのような通信状況においても情報交換の自由を可能とする電磁環境の深遠な理解の開発
5	ISR	生データを情報にならびに情報を知識に変換する我の能力を通して意思決定優越の実現に収斂すること
6	UAS（無人システム）	有人と無人システムおよび未参加センサーとの間ならびにすべての領域（航空、水上、水中、および陸上）での統合および同期の達成
7	サイバー空間作戦	データ、情報およびネットワークの動的創成、利用および防御を通して情報優勢、非運動優位および運動優越を容易にする俊敏で費用対効果の高い方法の創成
8	単一ネットワークへの統合	海軍の利用者およびアセットを任務の遂行において機密および非機密の情報をシームレスにアクセスおよび共有させることのできる単一統合ネットワークを達成するための海軍アプローチ
9	艦隊戦闘管理	資源の最適活用を可能とするプロセスおよびアーキテクチャの導出。最適な会合任務ニーズが作戦環境の変化にすぐに反応し、指揮官の意図を維持する位置から指揮統制（C2）をサポートする能力を含むこと
10	統合水上センサー	水平統合のために異なるセンサー、データ中継／交換、処理、可視化および意思決定支援能力艦艇のネットワーク化
11	教育	技能の拡大および深化ならびに教育および訓練の投資を通して情勢優勢部隊の世界クラスの専門家の育成
12	航空優勢	統合化された航空宇宙領域を通して実施される将来の「情報化」海軍作戦の定義
13	打撃指揮管制	打撃プラットフォームにどのような敵に対しても競争優位を完全に海軍に実現させるために情報の活用および伝達をする方法の定義
14	意思決定優越	指揮官にあらゆる時にあらゆる戦闘レベルで利用できるあらゆる選択肢を配布する方法で知識サイクルに対する情報への生データの閉鎖
15	周波数利用	アクセスとコストの両方で最適化されている安全な通信を提供するための最大技術適合性に対する海軍能力とドクトリンに隠れた利点の活用

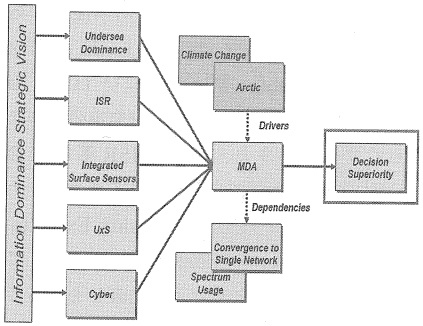


図5.1-2　情報優越ロードマップの相互関係[12)]

5.2　単一ネットワークへの統合

米海軍における現状の艦艇のネットワーク環境は、セキュリティ、性能等の観点から用途別に個別ネットワークに分かれている。単一ネットワークへの統合のロードマップは、他のすべてのロードマップをサポートするものであり、海軍に単一の統合ネットワーク環境を提供する。これは、グローバルに洋上または陸上の業務および戦闘のための利用者にデータ、情報、サービスおよびアプリケーションへのユビキタスなアクセスの高安全かつ高信頼のエンタープライズワイドな音声、映像およびデータの統合ネットワーク環境を提供する。また、これは、洋上のCANES（Consolidated Afloat Networks and Enterprise Services）ならびに陸上のNGEN（Next Generation Enterprise Network）およびONE-NET（海軍海外エンタープライズネットワーク）から構成される。この統合ネットワークを実現するための重要な鍵は、エンタープライズワイドのマルチレベルセキュリティ（MLS）基盤である。

米海軍の単一ネットワークへの統合ビジョンを図5.2-1に示す。

5.3　サイバー空間作戦

サイバー空間作戦のロードマップは、データ、情報およびネットワークの動的生成、活用および防御により情報優勢、非運動優位および運動優位を容易にする俊敏でコスト効率の良い方法を創出することである。それによって、米海軍の動的コンピュータネットワーク防御（Dynamic Computer Network Defense:

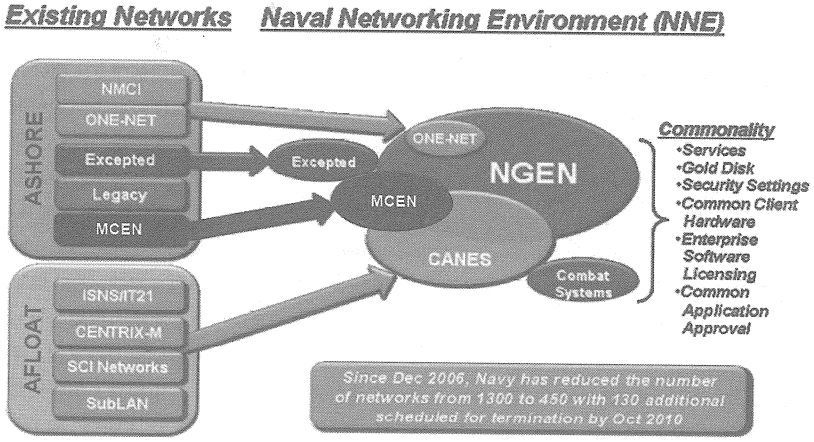


図5.2-1　単一ネットワークへの統合[14)]

DCND)、コンピュータネットワーク利用(Computer Network Exploitation: CNE)、コンピュータネットワーク攻撃(Computer Network: CNA)および情報作戦(IO: Information Operations)を扱えるようにする。DCNDは、我のネットワークおよびシステムに対するサイバー空間脅威の検知、分析、対応および緩和を行う能力である。CNEは、目標または彼の情報システム／ネットワークからデータ収集するためにコンピュータネットワーク経由で実施する作戦およびインテリジェンス収集能力である。CANは、彼の情報または情報システム／ネットワークを混乱、不能、低下、または破壊するためのコンピュータネットワーク利用による行動能力である。

DCNDをサポートするためのサイバー情勢把握およびサイバー共通作戦状況図(Cyber COP)の最終目標としては、既存の海上COPアーキテクチャの要件およびユーティリティの反映を挙げている。また、ネットワーク運用(NETOPS)をサポートするためのネットワーク共通作戦状況図(NETCOP)は、ネットワークの統合指揮統制を提供すべきとしている。

5.4 ISR

ISR(情報、監視および偵察)のロードマップは、海軍に当該任務に適切なプラットフォームと適切なセンサーを活用させることをISR任務管理およびすべての他の利用可能な収集器と調和した動的海軍アセット割当てのためのシームレスな指揮統制で実現することである。これは直接的な艦隊の戦術情報を配布し、総合的な長期の国家レベル情報分析をサポートする。

ISRの処理系であるDCGS-N(Distributed Command Ground System-Navy)は、米海軍の洋上(CVN、LHA、LHD、LCC)ならびに陸上(MOC、ONI Suitland、NSAWC Fallon)に配備される中核のISR分析／活用能力である。ISRロードマップは、「洋上－陸上Mix(The Afloat-Ashore Mix)」および「UXV相互運用性」のようないくつかの研究中のものによってサポートされ、海軍のISR運用概念(CONOPS)およびエンタープライズアーキテクチャを包括するPED(Processing, Exploitation and Dissemination)面の中心としてDCGS-Nの役割を定義および見直しを行っている。

すなわち、情報の分析および活用を狙いとしてプラットフォーム中心PEDから情報中心PEDへの移行を目指していると言える。さらに、DCGS-Nのスコープには、重要なI&W機能、レッドCOP、ターゲッティングサイクル要件、エンタープライズISR能力等のサポートを含んでいる。

6．組織再編

米海軍は、情報優勢ビジョンを実行するために、米海軍作戦本部再編、艦隊サイバー司令部編制および情報優勢部隊(IDC)創設を行った。

6.1 米海軍作戦本部再編

米海軍作戦部長の指示に基づき、現行および将来の情報化時代の情報優勢および意思決定優位実現のために、海軍情報要求、投資、能力および兵力整備のエンドツーエンドの検討および説明責任が同期するように、海軍情報部長(N2)と通信・ネットワーク担当(N6)海軍作戦次長を統合して、情報優勢担当(N2／N6)海軍作戦次長の新設およびそれら組織の再編を行った。この新組織は、海軍の情報能力の定義、開発、調達および監視を行う。旧組織と情報優勢のための新組織の対比を図6.1-1に示す。また、情報優勢担当の構成図を図6.1-2に示す。

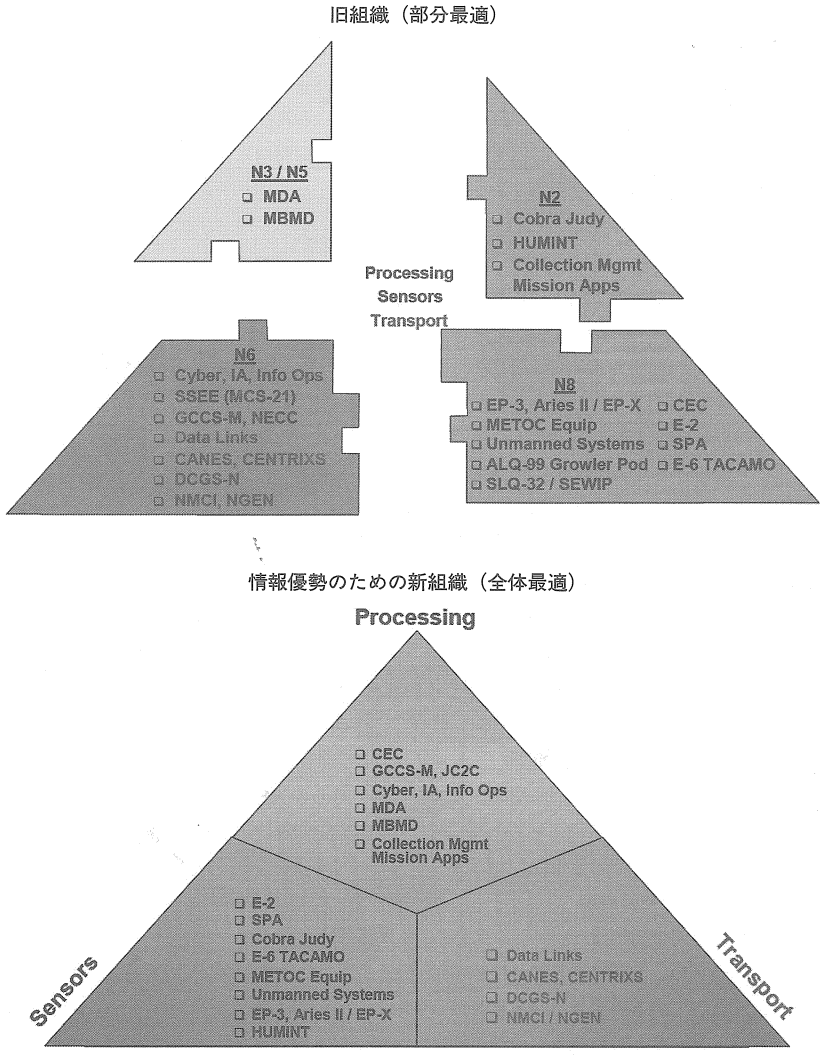


図6.1-1　旧組織と情報優勢のための新組織の対比[10)]

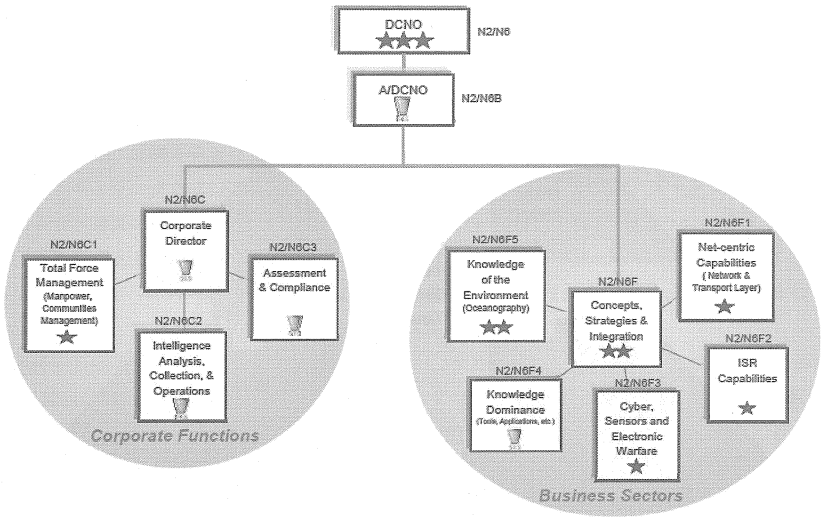


図6.1-2　情報優勢担当（N2／N6）の構成図[11)]

海軍作戦本部要員の戦闘評価を最適化するために、海軍作戦部長は、必要な作戦・戦闘能力および利用可能な資源に対して海軍プログラムを評価する独立した海軍戦闘評価部長（N00X）を新設した。

また、海軍法務総監は、サイバー空間作戦、他の情報作戦およびインテリジェンス作戦に関する法律と政策に絞った部署を新設した。

6.2　艦隊サイバー司令部編制

(1)　米サイバー軍司令部創設

ゲーツ国防長官は、2009年6月23日に戦略軍（USSTRATCOM）配下の米サイバー軍司令部（USCYBERCOM）としての統合司令部の創設および各軍種による構成司令部の創設を指示した[15)]。

USCYBERCOMは、次のことを行うための活動を計画、調整、統合、同期および実施する。

①　国防総省情報ネットワークの運用および防御の命令

②　全領域における行動を実現するための全範囲の軍事サイバー空間作戦の実施、サイバー空間における米国／同盟国の行動の自由の保障および我の敵に対する行動の自由の拒否の準備、または命令されたときのそれらの実施

また、USCYBERCOMの主要能力は次のとおりである。

①　国防総省情報ネットワークの動的防御の実施

②　サイバー作戦状況図（COP）の提供

③　所掌エリアを横断するサイバー空間効果の調整

④　軍事作戦をサポートするためのサイバー空間アクセスの開発

現在、サイバー軍司令官が国家安全保障局（NSA）長官および中央保安部（CSS）長官を兼任している。USCYBERCOMは、米国のサイバー関連政府機関の一大集積地になりつつあるメリーランド州フォートミード（Fort Meade）にNSAとともに設置されている。また、国防総省の国防情報システム局（DISA）も2011年にフォートミードに移転する計画である。

サイバー軍司令部隷下の各軍種構成司令部には、陸軍サイバー司令部(ARFORCYBER)、第24空軍（24thUSAF)、艦隊サイバー司令部（FLTCYBERCOM）および海兵隊サイバー司令部（MARFORCYBER）がある。ARFORCYBERおよび24thUSAFは、それぞれワシントンD.C.およびテキサス州ラックランド（Lackland）空軍基地に設置されている。FLTCYBRCOMおよびMARFORCYBERは、USCYBERCOMと同様にフォートミードに新たに設置された。

米サイバー軍司令部のフル運用能力時の構成を図6.2-1に示す。

(2)　艦隊サイバー司令部編制

米海軍作戦部長は、2009年7月23日に第10艦隊の任務付与の見直しによる艦隊サイバー司令部（FLTCYBERCOM）／第10艦隊（COMTENTHFLT）編制を指示した[16)]。

注．第10艦隊は、歴史的には、第2次世界大戦中に大西洋の対潜戦の開発および実装のために創設された組織であり、永久的に割当艦船を保有しない、インテリジェンスの統合ならびに先進的な戦術、技術および手順の開発のための組織であった。再編成された第10艦隊は、同様な考え方に基づき構築されており、先進的なゲームを変える脅威に対する機動の自由を保証するために、情報戦専門家、インテリジェンス専門家、暗号・電子戦専門家および従来戦専門家とともに作戦を実施する。

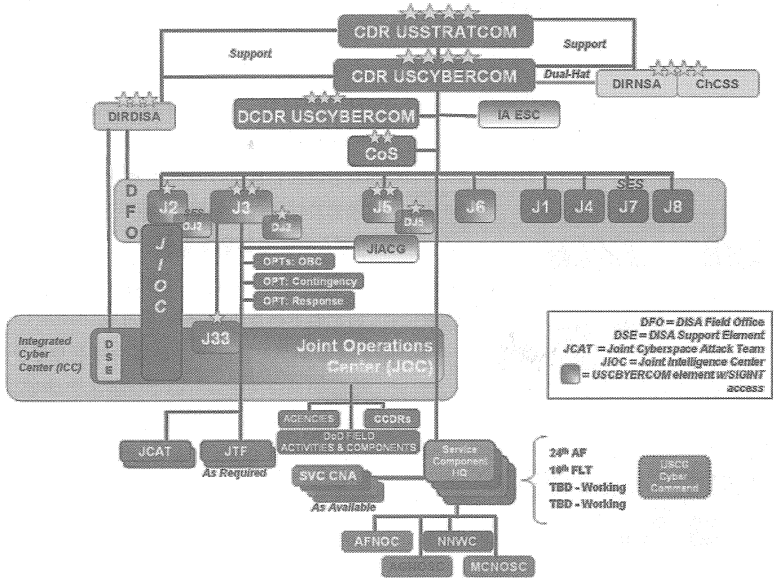


図6.2-1　米サイバー軍司令部（フル運用能力）構成[16)]

FLTCYBERCOMの任務は次のとおりである。

① サイバー空間における攻撃の検知および撃滅、行動の自由の保証および軍事目標の達成のためにサイバー空間作戦を指示する。

② 世界中の海軍暗号作戦の組織および指示ならびに情報作戦および宇宙計画・作戦の指示どおりの統合を行う。

また、FLTCYBERCOMの主要能力は次のとおりである。

① 動的コンピュータネットワーク防御（DCND）

② コンピュータネットワーク利用（CNE）

③ コンピュータネットワーク攻撃（CNA）

艦隊サイバー司令部と外部組織との指揮統制関係を図6.2-2に示す。

NNWC（Naval Network Warfare Command：海軍ネットワーク戦司令部）は、海軍ネットワーク運用（NETOPS）を提供する。その隷下部隊には、ネットワーク管理・維持および陸上ベースの艦隊への中継を提供する大西洋地域および太平洋地域別のNCTAMS（Naval Computer and Telecommunications Area Master Station：海軍コンピュータ・通信地域主局）ならびに衛星ネットワークの運用を行うNAVSOC（Naval Satellite Operations Center：海軍衛星運用センター）を含む。NCDOC（Navy Cyber Defense Operation Command：海軍サイバー防衛作戦司令部）は、コンピュータネットワーク防御を行う。

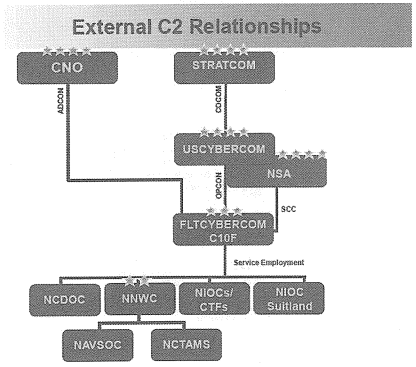


図6.2-2 艦隊サイバー司令部と外部組織との指揮統制関係[17]

ノーフォークのNIOC（Navy Information Operation Command：海軍情報作戦司令部）は、サンディエゴおよびホイッドビー島（ワシントン州）に分遣隊を置いて、情報作戦を監督している。テキサス、ジョージア、メリーランド、ハワイ、コロラドおよび世界中に配置されたそれらの隷下部隊のNIOCは、艦隊および戦域作戦を調整・実施する。暗号構成部隊運用は、FLTCYBERCOM指揮下でこれらNIOCにおいて実施される。

スイットランドのNIOC（Naval Information Operation Center：海軍情報作戦センター）は、研究開発部隊である。

上述した第10艦隊の隷下部隊は、艦隊総軍（USFF）および太平洋艦隊（COMPACFLT）の管理下にあるサイバー部隊（CYBERFOR）から常設任務部隊として提供されている。第10艦隊常設任務組織を図6.2-3に示す。

6.3 情報優勢部隊編制

サイバー空間は、国防総省によると次のように定義される。

「インターネット、通信ネットワーク、コンピュータシステム、および組込プロセッサや制御装置を含む情報技術基盤の相互依存ネットワークから構成する情報環境内のグローバル領域」

このサイバー空間における戦い（サイバー戦）は、コンピュータネットワーク作戦（Computer Network Operations：CNO）およびネットワーク運用（Network Operations：NETOPS）から構成される。さらに、CNOは、CND、CNEおよびCNAを含み、レッドCOPと呼ばれるサイバーCOPを提供する。一方、NETOPSは、情報保証（IA）、エンタープライズ管理、コンテンツ管理を含み、ブルーCOPと呼ばれるNETCOPを提供する。また、CNDおよびIAについては、ネットワーク防御として横断的な機能である。サイバー戦の概念を図6.3-1に示す。

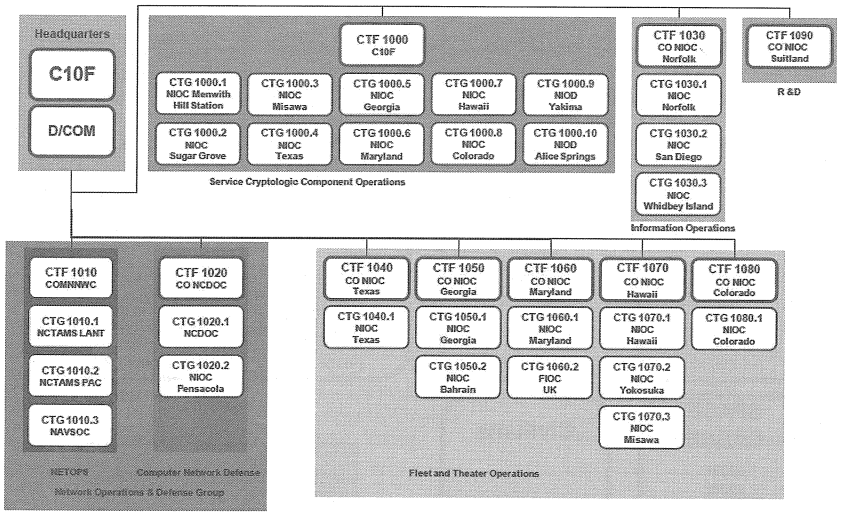


図6.2-3 第10艦隊常設任務組織[17]

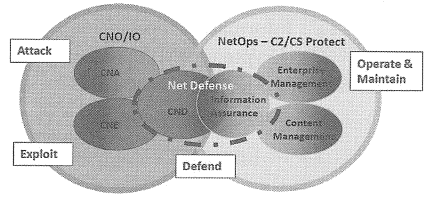


図6.3-1 サイバー戦の概念[18]

サイバー戦に必要な要員は、コンピュータネットワーク作戦およびネットワーク運用に対応するためのサイバー要員および情報技術（IT）要員から構成される情報（Information）要員である。サイバー要員のスコープには、サイバーセキュリティおよび情報作戦が含まれる。情報要員の構成概念を図6.3-2に示す。

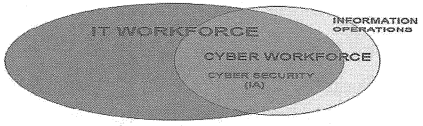
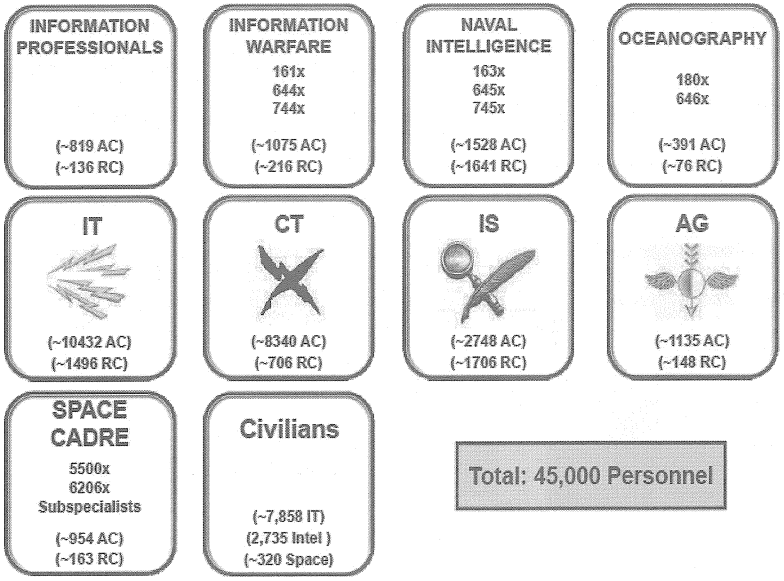


図6.3-2 情報要員の構成概念[19]

米海軍は、サイバー戦に対応するために既存の情報戦、インテリジェンス、情報技術、気象学／海洋学および宇宙組織の専門家から構成される4,500人規模の情報優勢部隊（Information Dominance Corps：IDC）を創設し、N2N6および第10艦隊常設任務組織の要員をサポートする。

「OPNAVINST 5300.12, The Information



注．志願要員
- IT：Information Technician
- CT：Cryptologic Technician
- IS：Intelligence Specialist
- AG：Aerographers Mate

図6.3-3　情報優勢部隊（IDC）の構成[11)]

Dominance Corps, 6 October 2009」に基づく情報優勢部隊の構成を図6.3-3に示す。図6.3-3の上段および中段は、それぞれ将校および志願による要員を示している。また、民間人による軍属は、情報、インテリジェンス、防諜、人的生成情報、気象学および海洋学分野に配置される。

7．サイバー／サイバーセキュリティ要員育成

情報優勢部隊の中核となる要員は、図6.3-2に示したサイバーセキュリティ（CS）／情報保証（IA）要員である。米国防総省は、「DoD 8570.01-M 情報保証要員能力向上計画、2005年12月5日」において、CS／IA 要員の分類、レベルおよび機能要件を定義し、ISO／IEC 17024のもとで資格が認可されることを要求している。

米海軍省（DoN）は、この情報保証要員能力向上計画をサポートするために「SECNAV-MAN 5239.2　海軍省情報保証要員管理マニュアル、2009年5月29日」を策定し、CS／IA 専門家について、次に示す2016年ビジョンを示している。

① 訓練、承認および資格付けされた専門的なサイバーセキュリティ／C4／情報技術（IT）要員メンバーであること。

② NETOPS、IA および技術設計を通してネットワークを防御するための適切な戦術、技能および手順を理解および積極的適用ならびに国防部門に対する任務保証の常時提供を行うこと。

③ 教育、訓練および演習を含めるように複数手段を用いて連続的な学習を通して技能を向上すること。そうすることによって、新しい技術および脅威に対して先手を打って対応できる。

これらのビジョンからも分かるように、CS／IA 要員の育成については、専門能力の資格付けならびに複数手段による技能向上が求められている。現在の米海軍の情報技術教育訓練は、教室方式（classroom）による資格付けのための基礎教育（A School）、教室方式による専門分野の短期教育（C School）および OJT が実施されている。この教室方式には、学習者が個別にコンテンツを使用できる統合学習環境（Integrated Learning Environment：ILE）が使用されている。教室方式による学習効果は正規分布しているので、学習効果を向上するためには、ブルーム氏（Benjamin S. Bloom）による「学習者は生きた1対1の個人指導による教育の場合が最も学習効果が高い」との学習理論[21)]を応用して、新しい教育方式を開発する必要がある。米海軍

表7-1　CS／IA 要員の機能要件[20)]

Designated Accrediting Authority (DAA) Functions	Information Assurance Management (IAM) Levels I, II, III	Information Assurance Technical (IAT) Levels I, II, III
Authorize connection/testing Accredit System Authorize IA Controls Accept Risk	Oversee configuration testing Oversee System Revalidate IA Controls Manage Risk	Manage connections/conduct testing Administer System Manage IA Controls Operate (in) Risk
Information Assurance Systems Architects and Engineers (IASAE) Level I, II, III	**Computer Network Defense Service Provider (CND SP) Functions**	**Certification and Accreditation (C&A) Functions**
Develop System Design IA Controls Engineer (out) Risk	Monitor System Assess IA Controls Detect Threat	Identify Risk/Audit Certify Recommend Accreditation

注．レベルⅠ：コンピュータ環境
　　レベルⅡ：ネットワーク
　　レベルⅢ：エンクレーブ

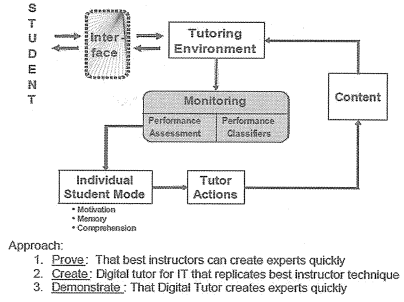


図7-1　教育優勢（Education Dominance）プログラム[22)]

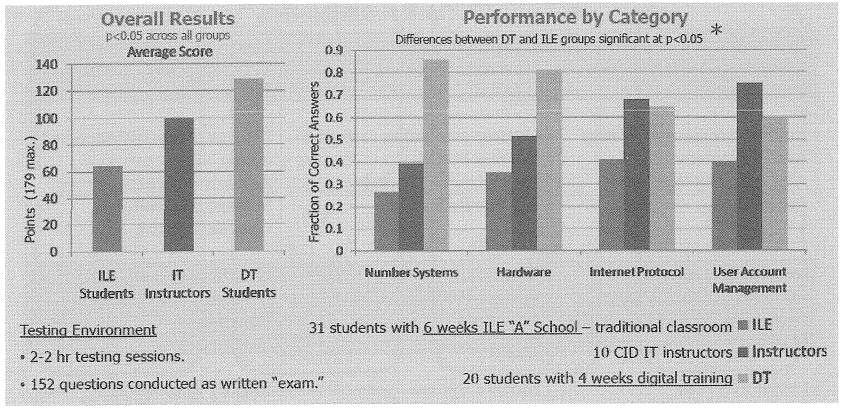


図7-2　ディジタル個人指導の効果[23)]

は、DARPA（国防高等研究計画局）と連携して図7-1に示す教育優勢（Education Dominance：Digital Tutor）プログラム[22)]を実施し、「Digital Tutor（ディジタル個人指導）による学習者は、教室方式および優れたILEによる学習者よりも1／3の少ない時間で効果をあげたこと」を図7-2のとおり示した[23)]。したがって、これらの成果が、米海軍の「教育ロードマップ」に取り入れられるものと推察される。

8．情報優勢のための技術開発

8.1　米海軍研究局の技術開発政策

米海軍研究局（ONR：Office of Naval Research）は、「情報優勢のための米海軍のビジョン」の指針を受けて、米海軍の情報優越のための研究開発政策を次の分野別に示している[24)]。

① 指揮統制（C2）優勢
② 無人ビークルおよび自動化
③ 安全な通信とネットワーク
④ 電磁周波数の制御

指揮統制優勢については、共通作戦状況図（COP）の柔軟な開発、迅速な適用および拡張性を実現するためのサービス指向アーキテクチャ（SOA）、リスク削減および艦艇への迅速適用のためのC2RPC（C2 Rapid Prototype Continuum）等を挙げている。

無人ビークルおよび自動化については、現状では遠隔操作の無人ビークルは、自動化への中間段階である。比較的単純なゆっくり変化する環境（水中戦闘空間のような）では、ルールベースが有効である。しかし、ルールベースシステムは脆弱で、複雑で不確実な動的な環境ではうまく動作しない。したがって、長期的には、システムによる指揮官の意図の文脈での戦闘空間を総合化できる機械推論および実行可能な行動方針（COA）の策定が必要であることを挙げている。

安全な通信とネットワークについては、脅威の識別、緩和および運用継続の保証ならびに攻撃下の保証されたデータへのアクセスを行うコンピュータネットワーク技術および情報保証技術を提供することであり、改ざん事象監視、ハードウェア／ソフトウェア破壊および暗黒化のような耐タンパー技術、ボットネット脅威排除技術等が必要であることを挙げている。

周波数優勢のための電磁周波数の制御については、送信機の周波数レンジおよび有効性の拡大、複数アセットを用いる複数任務エリアに渡る同期された広域電磁周波数管理の実現（統合分散電子戦）、無線機能、開口部および信号処理部の同時共有化、および指揮官の最高優先度ニーズに適合させるための連続最適化が必要であることを挙げている。

8.2　米海軍SPAWARにおける技術開発

米海軍SPAWAR PEO C4Iでは、図6.3-1に示したサイバー戦の概念において、ネットワーク運用に関する分野においては、次の技術およびシステム等が運用および開発中である。

① エンタープライズ管理：CANES、ADNS等
② コンテンツ管理：GCCS-M、DCGS-N等
③ ネットワーク防御：IA、PKI、CDS、CND等

一方、コンピュータネットワーク作戦に関する分野については、ネットワーク防御の機能については、開発が行われているが、CNAおよびCNEの機能については、ONRの「海軍科学技術戦略計画（2009年）」においても主要研究課題としている。

SPAWAR SSC Pacificは、2010年から2030年までの期間を対象とした「サイバー関連科学技術ロードマップ」において、次に示す課題を挙げている。

① 要員のレベル低下およびシステム自動化の増加に対応するための戦闘員および彼らの情報の透過的防護
② ユビキタスな堅牢で安全な情報生成および流れ
③ サイバー脅威のリアルタイムでの隔離および緩和
④ サイバー戦闘空間のニアリアルタイム情勢把握

表8.2-1　サイバー機能特性[25)]

機能特性
全般
自律および自己認識
透過性
利用者信頼
即応
統合システム
情報
ユビキタス、堅牢な情報統合と流れ
リアルタイム情報および行動
知る必要のあることの通知
高信頼
予測
行動
適応可能な脅威検知および識別
自動対応行動
兵站
合理的コストでの維持
高信頼なサプライチェイン

これらの課題に基づき、サイバー機能特性を表8.2-1に整理している。

これらの課題およびサイバー機能特性に対応するための能力戦略として、「重要な情報および情報システムを動的、積極的および予測的に防御すること」を設定し、表8.2-2に示す必要なサイバー関連技術能力を導出している。

表8.2-2　サイバー関連技術能力[25)]

サイバー関連技術能力
高信頼でないプラットフォームからの高信頼計算
既知リスクレベルとの運用
信頼の再構成
リスク適応情報共有およびアクセス
動的再構成レベルの耐性
ユビキタスCDS（クロスドメインソリューション）
異種コンテンツ／文脈からの自動メタデータ
CDSの文脈およびコンテンツ妥当性評価
電子迷彩（ステガノグラフィー）検知および保護
自己除染システム
リアルタイム脅威分類／予測／見積
非集中化自動分析
能動検知および対策立案
動的インテリジェンス利用
多層データ融合
攻撃パターン予測モデル
認知的に適切な情報の提供
弾性プラットフォーム自己保護
ハードウェアおよびソフトウェアの高信頼サプライチェイン
コンピュータでの集中的IAをサポートするためのプラットフォーム

9．おわりに

本論文では、国家安全保障レベルでサイバー攻撃の脅威に直面している今日において、米海軍が2010年5月に発表した21世紀の海軍力としての情報を武器とする「情報優勢のための米海軍のビジョン」について紹介し、情報優越と情報優勢の概念の違い、情報優勢実現の指針およびロードマップの最新状況を示した。また、情報優勢ビジョンを推進するために米海軍が実施した海軍作戦本部、艦隊サイバー司令部および情報優勢部隊の組織再編については、その目的、役割、能力および具体的組織について示した。さらに、情報優勢部隊のサイバー／サイバーセキュリティ要員の育成については、情報技術の資格付けでは十分ではなく、革新的な要員の育成向上を図るために米海軍がDARPAと連携して取り組んだ教育優勢プログラムを紹介した。最後に、情報優勢の技術開発については、米海軍研究局およびSPAWARにおける主要研究課題および必要なサイバー関連技術能力を示した。

参考文献

1．DoN, The U.S. Navy's Vision for Information Vision, May 2010
2．Vice Admiral Arthur K. Cebrowski, U.S. Navy, and John J. Garstka, Network-Centric Warfare: Its Origin and Future, Proceedings, January 1998
3．David S. Alberts, John J. Garstka, and Frederick P. Stein, Network Centric Warfare, 1999
4．Joint Vision 2020, June 2000
5．Network Centric Warfare, Department of Defense Report to Congress Appendix, 27 July 2001
6．Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 12 April 2001, (As Amended Through 30 September 2010)
7．Network Centric Warfare, Department of Defense Report to Congress, 27 July 2001
8．Department of the Army, FM 100-6, INFORMATION OPERATIONS, 27 August 1996
9．Jim Winters, U.S. Army, Information Dominance Point Paper, (http://www.iwar.org.uk/iwar/resources/info-dominance/id.htm)
10．VADM Jack Dorsett, DCNO for Information Dominance, OPNAV N2／N6, Navy Information Dominance, Naval Information Dominance Industry Day, 22 June 2010
11．RADM Mike Broadway, CNO N2／N6FC, Information Dominance, NDIA San Diego, 05 October 2010
12．Mark Andress, CNO N2N6F4, Decision Superiority and Fleet Battle Management, Naval Information Dominance Industry Day, 22 June 2010
13．CNO N2N6, Naval Information Dominance Industry Day, Q&A, 22 June 2010 (http://www.afcea.org/mission/intel/documents/MASTERINDUSTRYDAYQA.pdf)
14．RDML Gretchen Herbert, ADCNO for Networks, USN, Convergence to a Single Network Roadmap, Information Dominance Industry Day, 22 June 2010
15．The Secretary of Defense, Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyber Command, 23 June 2009
16．RDML BILL LEIGHER, USN, FLEET CYBER COMMAND COMTENTHFLT, 2-3 DEC 2009
17．VADM BERNARD J. McCULLOUGH, III, Commander, United States Fleet Cyber Command, Digital Domain: Organize the Military Departments for Cyber Operations, 23 September 2010
18．Terry Simpson, PEO C4I, USN, NDIA Cyber Symposium, 28 October 2009
19．Mike Knight, Navy Cyber Forces, Navy Cybersecurity Workforce, 3 FEB 2010
20．DoN, SECNAV M-5239.2, INFORMATION ASSURANCE (IA) WORKFORCE MANAGEMENT MANUAL, May 2009
21．Benjamin S. Bloom, The 2 Sigma Problem: The Search for Methods of Group Instruction as Effective as One-to-One Tutoring, Educational Researcher, Vol. 13, No. 6, Jun.-Jul., 1984
22．Trip Report Department of Defense Human Factors Engineering Technical Advisory Group, (DOD HFE TAG) Meeting #62 －Key West Florida, 2-5 November 2009
23．Thomas Kalil, White House Office of Science and Technology Policy, Innovation and the Navy, 2010 Naval Science and Technology Partnership Conference, 9 November 2010
24．RADM Nevin P. Carr Jr., ONR, Science and Technology for Information Dominance, Naval Information Dominance Industry Day, 22 June 2010
25．Pat Sullivan, SSC Pacific, SPAWAR, Cyber Perspectives: Science and Technology Roadmap, 14 April 2010