A2／AD 環境下における サイバー空間の攻撃及び防御技術の動向 ㊦

木村 初夫

株式会社 NTT データ　公共システム事業本部
第一公共システム事業部　第三システム統括部　嘱託

6．米軍のサイバー関連技術の動向

国防総省（DoD）は、「QDR2010（4年毎の国防計画の見直し）」において、サイバー空間は陸、海、空及び宇宙の領域に加えた第5の作戦領域とみなしている[1]。また、「国防総省サイバー空間作戦戦略（2011年7月）」では、戦略方針として、サイバー空間の作戦領域化、DoDネットワーク／情報システム防護のための新防衛作戦構想としての能動サイバー防衛の採用、他政府機関、民間機関、外国政府との協力等を示している。能動サイバー防衛とは、サイバー脅威と脆弱性の発見、探知、分析及び軽減する国防総省の同期化されたリアルタイム能力である[2]。秘密指定の「国防総省サイバー空間作戦戦略」は公開されていないが、米国の軍事施設および重要インフラ等がサイバー攻撃を受けた場合は、戦争行為とみなして軍事力を行使するとの報道がされている（交戦規則（ROE）は不明）。さらに、米国の新国防戦略である「米国グローバル指導力の維持：21世紀の国防優先度（2012年1月）」では、米軍の優先任務として、「中国・イラン等の電子戦、サイバー攻撃及び弾頭ミサイル等による接近阻止／領域拒否（A2／AD）環境下での戦力投射」並びに「ネットワーク中心戦（NCW）に不可欠な通信ネットワークを含むサイバー空間及び宇宙における有効な作戦」を挙げている[3]。

米国サイバー軍（USCYBERCOM）の主要能力は、国防総省情報ネットワークの動的防御の実施、サイバー作戦状況図（COP）の提供、所掌エリアを横断するサイバー空間効果の調整及び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である[4]。

DoDは、新サイバー防衛作戦構想を実現するためにCND能力向上計画として、信頼ベースの情報保証の評価認証、サイバー空間状況認識能力、ホストベースセキュリティシステム（HBSS）、サプライチェーンリスク管理、インサイダー攻撃監視、セキュリティ常時監視（安全な構成管理）、安全地帯（Webコンテンツセキュリティ、電子メールセキュリティ、DNS強化）、ネットワークスキャナを挙げている[5]。

また、DoDは、サイバー脅威として、APT攻撃、インサイダー攻撃、サプライチェーン攻撃、制御システムの脆弱性攻撃、モバイルセキュリティ、クラウドセキュリティ及びID管理を重

視し、国家主導のサイバー攻撃に対応するためには、統合化された情報保証状況把握から動的防御、更にはサイバー耐性のあるエンタープライズレベルのサイバーセキュリティ成熟度能力の実現を目標としている[6]。

6.1 米軍のサイバー関連技術の概要

米軍のサイバー関連技術の現状及び開発中並びに将来構想を表6.1-1に示し、主要なサイバー関連技術の概要を次に述べる。

6.2 現状及び計画中のプログラム

(1) DARPAのPlan X計画[7]

米国防高等研究計画局（DARPA）は、「リアルタイム、大規模及び動的ネットワーク環境におけるサイバー戦の理解、作戦計画及び指揮統制の革新的技術の創成」を研究開発目的としてサイバー戦の作戦化及びルーチン化のための攻勢的サイバー戦プログラムであるPlan Xを2013年～2017年に予算額110百万ドル（DARPAサイバー関連研究費：1,540億ドル（2013年～2017年））で計画している。ただし、本計画はサイバー兵器開発の予算を含んでいない。本研究内容の概要を次に示す。

- サイバー戦闘空間の理解：大規模ネットワークトポロジー分析自動化
- 検証できる及び定量化できるサイバー作戦計画自動立案：高次レベル任務計画案及び自動任務スクリプト合成（航空機自動操縦と同様）
- 動的、戦闘する及び彼のネットワーク環境下での作戦向けのOS及びプラットフォームの開発：戦闘被害監視、通信中継、兵器運用及び適応防御のようなサイバー戦機能を実施できる戦闘ユニットの構築
- 大規模サイバー戦闘空間の可視化及び操作：サイバー戦闘空間統合ビューワによる作戦計画立案、作戦、状況認識及びM&Sのサイバー戦機能の提供

(2) DoDのサイバー兵器リストの整備[8]

2011年6月1日のワシントンポスト紙（電子版）によると、国防総省はサイバー戦における攻撃を効率化するためにサイバー兵器リストを開発したとのことである。このサイバー兵器リストには、彼の重要ネットワークを破壊するためのマルウェアが含まれている。また、「承認された能力の正式編成へのサイバー技術の統合は、軍事サイバードクトリンの最も重要な運用開発である。」と軍高官が発言している。

(3) DoDの安全な構成管理の整備（セキュリティ常時監視）[9]

DISAは、2011年の国防権限法（NDAA：H.R. 6523）によるセキュリティ常時監視の実現のために「NIST SP 800-137（連邦情報システム及び組織の情報セキュリティ常時監視）」及び「NIST SP 800-128（情報システムのセキュリティ構成管理指針）」に基づき「DoDの安全な構成管理（Secured Configuration Management：SCM）の整備」を行っている。また、SCMプロセスとして、セキュリティ設定管理、構成発見及び検知、セキュリティ状態分析、状態リスク緩和及びSCMデータ公開／共有を定義し、表6.2-1に示すとおり各プロセスをサポートするGOTS及びCOTSから構成されるシステムを整備中である。

これらSCMの主要システムとしては、HBSS（Host-Based Security System）、ACAS（Assured Compliance Assessment Solution）及びCMRS（Continuous Monitoring and Risk Scoring）がある。HBSSは、DoDのSIPRNET及びNIPRNET上の情報システムのサイバー空間の侵入検知、状況認識、分析及び対応を行うシステムであり、脆弱性検知、セキュリティ設定評価及び報告能力を提供する。これは、COTS及びGOTSから構成され、McAfee社のSIEM製品であるePO Agent及びセキュリティ常時監視のためのコンプライアンス管理ツールであるPolicy Auditorが使用されている。また、ACASは、HBSSの能力向上としてアプリケーション脆弱性走査、ネットワーク脆弱性走査、セキュリティ設定評価能力を提供する。ACASは、Tenable社のSIEM製品であるSecurity Center、脆弱性スキャナ製品であるNesseus Vulnerability Scanner及びPassive

表6.1-1 米軍のサイバー関連技術の現状及び開発中並びに将来構想

区分		項目	備考
現状及び開発中計画	CNA	・DARPAのPlan X計画 ・DoDのサイバー兵器リストの整備 ・「オリンピックゲーム」で使用されたStuxnet（注1） ・米空軍の航空ネットワーク攻撃システム（Suter）（注2） ・米陸軍のTECWD（Tactical Electromagnetic Cyber Warfare Demonstrator）計画（注2）	
	CNE	・「オリンピックゲーム」で使用されたFlame（注1）	
	CND/IA	・DoDのサイバー空間状況認識の整備 ・DoDの安全な構成管理の整備（常時監視） ・DARPAのインサイダー攻撃緩和技術の開発 ・テーラー化信頼空間及び移動目標の研究開発計画 ・IARPAの高信頼集積回路（TIC）計画（注2） ・DARPAの集積回路安全化・高信頼化（IRIS）計画（注2） ・DoDサイバー演習場の整備	APT攻撃、インサイダー攻撃及びサプライチェーン攻撃対策技術
将来構想		・DoDサイバー科学技術ロードマップ ・米陸軍サイバービジョン2020 ・米海軍サイバー科学技術ロードマップ ・米空軍サイバービジョン2025	任務保証及び拡大、脆弱性及び耐性の向上、信頼基盤等

注1.「3. サイバー空間の攻撃技術の動向」を参照
注2.「4. サイバー空間の防御技術の動向」を参照

表6.2-1 DoDの安全な構成管理の整備：全体構成

SCMプロセス	システム	COTS/GOTS	備考
セキュリティ設定管理（Security Content Management）	・Automatable STIG Publication ・Antivirus/Antispyware ・IAVM System ・Digital Policy Management Solution（DPMS）	GOTS COTS GOTS GOTS	
構成発見及び検知（Configuration Discovery and Detection）	・Host Based Security System（HBSS） ・Assured Compliance Assessment Solution（ACAS） ・Secure Configuration Compliance Validation Initiative（SCCVI） ・Enterprise Network Mapping and Leak Detection Solution（ENMLDS） ・Asset Configuration Compliance Module（ACCM）	COTS/GOTS COTS COTS GOTS	
セキュリティ状態分析（Security State Analysis）	・Vulnerability Management System（VMS） ・Enterprise Mission Assurance Support Service（eMASS） ・Continuous Monitoring and Risk Scoring（CMRS）	GOTS GOTS GOTS GOTS	
構成リスク緩和（Configuration Risk Mitigation）	・Patch Management（WSUS） ・Remediation Manager	COTS	
SCMデータ公開及び共有（SCM Data Exposure and Sharing）	・HBSS Asset Publishing Service（APS）	GOTS	データ標準 ・ARF ・ASR ・XCCDF

出典：Enclave Security：Secure Configuration Management (SCM), DISA, 7-10 May 2012

Vulnerability Scanner、セキュリティ常時監視のコンプライアンス管理ツールである X-Tool 及びネットワーク及び脆弱性地図作成ツールの Topology Viewer から構成される Tenable Network Security が使用されている。さらに、CMRS は、HBSS 及び ACAS から DoD 情報システムに関するセキュリティ状態情報の収集並びにすべてのレベルの指揮官が使用できる任務

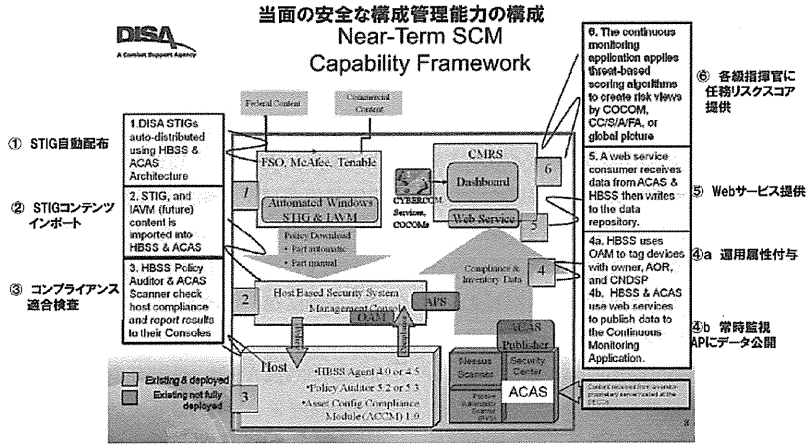

図6.2-1 DoD の安全な構成管理の整備：システム構成

出典：Enclave Security：Secure Configuration Management (SCM), DISA, 7-10 May 2012

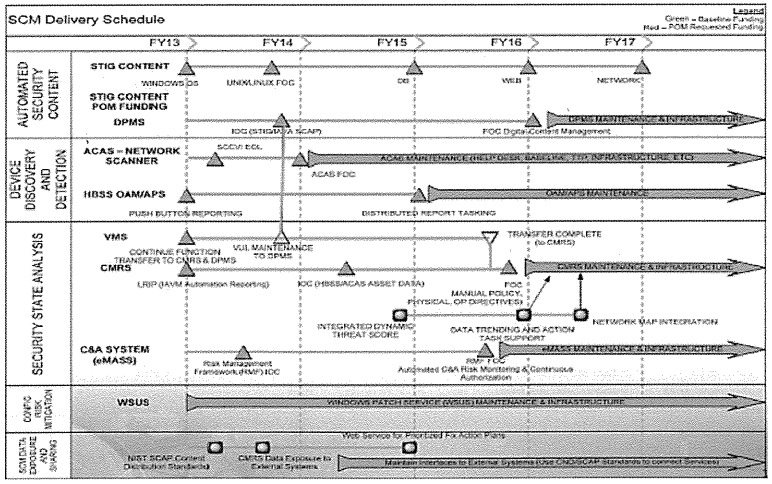

図6.2-2 DoD の安全な構成管理の整備：スケジュール

出典：Enclave Security：Secure Configuration Management (SCM), DISA, 7-10 May 2012

リスクスコアを自動生成するセキュリティ常時監視能力を提供する GOTS であり、2012年から数ヵ所にパイロット導入されている。当面の SCM のシステム構成及び整備スケジュールをそれぞれ図6.2-1及び図6.2-2に示す。CMRS の本格運用時期は、2016年末が予定されている。

(4) DARPA のインサイダー攻撃緩和技術の研究開発[10]

DARPA は、2010年からインサイダー攻撃緩和のためにインサイダーの行動識別を行う CINDER（Cyber Insider Threat）及びインサイダーの異常行動検知を行う ADAMS（Anomaly Detection at Multiple Scales）の研究開発を行っている。

CINDER は、ネットワークインサイダーの情報窃取の検知及び停止をセキュリティ要員に迅速に行わせることを研究目的として、彼の行動分析から実行任務をリアルタイムに識別するものである。

一方、ADAMS は、信頼されたインサイダーが不正活動に変心及び開始した直後に異常行動を検知することを研究目的とするが、インサイダー脅威のスコープに制限がないため、ビッグデータの新しい処理技術の開発が必要である。ADAMS のインサイダー脅威監視情報収集ツールとしては、Raytheon 社の SecureView が使用され、その監視対象には、Web、インスタントメッセージ（IM）、電子メール、ファイル、可搬媒体、プリンタ、キーボード、クリップボード、MS Office 製品、プロセス、ファイルディレクトリ、利用者イベント、レジストリ、端末サービス、モバイル要員及び暗号化前／復号化後がある。

(5) 「テーラー化信頼空間」及び「移動目標」の研究開発[11]

米国の「ネットワーク・情報技術研究開発（NITRAD）」において、米軍が2013年度に「テーラー化信頼空間」及び「移動目標」の研究関連で予定している主要研究開発計画を表6.2-2に示す。

表6.2-2 「テーラー化信頼空間」及び「移動目標」の研究開発計画

区分	主要研究開発計画	実施機関
テーラー化信頼空間（Tailored Trustworthy Spaces）	• Trusted foundation for defensive cyberspace operations	•OSD及び各軍研究所
	• High assurance security architectures	•NSA, ONR及びNIST
	• Security for cloud-based systems	•DARPA, DHS及びNIST
	• Secure wireless networking	•NSA及び各軍研究所
	• Military Networking Protocol（MNP）program	•DARPA
	• Tactical Information Technologies for Assured Network operations（TITAN）	•ARL, ARO及びCERDEC
	• Security Automation Program	•DHS, NIST及びNSA
移動目標（Moving Targets）	• Protected Control Plane for Cyber Command and Control（PCPC3）	•AFRL
	• Cyber Unification of Security Hardening and Protection of Operational Frameworks（CRUSHPROOF）	•OSD, ARL, ARO及びCERDEC
	• Clean-slate design of Resilient, Adaptive, Secure Hosts（CRASH）	•DARPA
	• Cyber Camouflage, Concealment, and Deception	•DARPA
	• Morphing Network Assets to Restrict Adversarial Reconnaissance（Morphinator）	•ARL, ARO及びCERDEC
	• Defensive Enhancements for Information Assurance Technologies（DEFIANT）	•ARL, ARO及びCERDEC
	• Robust Autonomic Computing Systems	•ONR
	• Trust Management in Service Oriented Architecture	•ONR
	• Proactive & Reactive Adaptive Systems	•NSA
	• Information Security Automation Program（ISAP）	•DHS, NIST及びNSA

出典：THE NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT：PROGRAM：Supplement to the President's Budget FY2013, Feb. 2012

(6) DoDサイバー演習場の整備[12)13)]

DoDは、NSPD-54／HSPD-23、「総合国家サイバーセキュリティ構想（CNCI）」及び「国防総省サイバー空間作戦戦略」に基づき、サイバー演習場として、表6.2-3に示す情報保証レンジ（IA Range）、情報作戦レンジ（IO Range）及びDARPA NCR（National Cyber Range）を整備している。

情報保証レンジは、DoD IA／CND要員を対象として、実環境と同等なGIG-IA／CND能力を持つ試験、訓練及び演習環境を提供するものである。情報作戦レンジは、戦闘司令部、各軍種、中間的政府機関、有志連合及び試験評価組織を対象として、クローズ系完全メッシュ網及び網ノード管理環境上で試験、訓練及び演習時のIO能力の発揮及び検証のためのIOツール／目標へのアクセス能力を提供するものである。さらに、DARPA NCRは、研究者を対象として、次世代環境上で疑似、エミュレート及び複製環境を提供し、性能向上／将来能力の概念実証並びに国家レベルを対象とした次世代サイバー課題及び能力の先進研究を行うものである。

表6.2-3　DoDサイバー演習場の整備：全体構想

項目	IA Range	IO Range	DARPA NCR
秘密区分	非機密	MLS:Multi-Level Security	MSL: Multiple Security Level
対象利用者	DoD IA/CND要員	戦闘司令部(COCOM)、各軍種、中間的政府機関、有志連合及び試験評価組織	研究者
環境	実環境と同等なGIG-IA/CND	クローズ系完全メッシュ網及び網ノード間管理	次世代環境
機能	・試験、訓練及び演習環境 ・新規ツールの試験評価 ・要員及びTTP(戦術、技法及び手順)の演習及び評価	・実及び疑似ツール並びに目標に対する安全な接続、資源割当、イベント調整及びアクセス ・セキュリティ、接続及びネットワーク管理 ・試験、訓練及び演習時のIO能力の発揮及び検証のためのIOツール／目標へのアクセス	・擬似、エミュレート及び複製の研究環境 ・性能向上／将来能力の概念実証 ・国家レベルを対象とした次世代サイバー課題及び能力の先進研究
運用レベル	レベル2攻撃条件までの正規運用	相互接続能力	統合化された＆高度な彼の攻撃条件
供給	現行DoD技術、要員、ポリシー及び手順の統合	現行及び開発中IO能力及び目標環境への高度に安全なアクセスの提供	革新技術の研究開発

出典：DoD Information Assurance Range: A Venue for Test and Evaluation in Cyberspace, DISA, August 2011

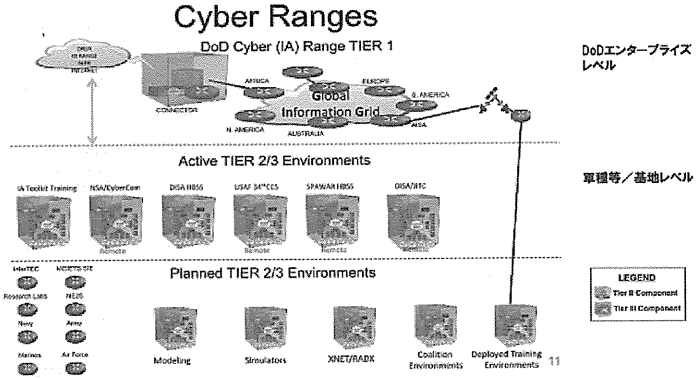

図6.2-3　情報保証レンジの全体構成

出典：DoD Cyber (IA) Range: Enabling Dominance in Cyberspace, USMC, 23 Jan. 2012

表6.2-4　情報保証レンジの具体能力

能力区分		具体能力	備考
実環境能力	グローバルバックボーンネットワーク	・内部／外部中継 ・MPLSクラウド ・Webコンテンツフィルタリング ・境界防護	
	仮想インターネット	・完全なDNS複製 ・ソーシャルネットワークサービス ・e-コマース ・検索エンジン ・多数のWebサイト ・不正サイト	
	仮想ホスティング	・DECC (Defense Enterprise Computing Center) 及びCDC (Community Data Center)	
	トラフィック生成	・ネットワーク及びホストベーストラフィック生成 ・仮想アクター ・帯域制限 ・マルウェア／無害	
	IA/CNDツール	・HBSS ・ACAS ・STIG ・ArcSight ・Sourcefire (次世代IPS) ・Splunk(統合ログ管理) ・Palo Alto F/W ・Security(行動分析) ・Wireshark(プロトコル解析) ・IPSonar(ネットワーク発見) ・NIKSUN(ネットワーク監視)	CHIPS 2012年7-9月号
新規ツール試験・評価		・RedSeal(Proactive Network Security Management) ・FireEye (Unknown Malware Protection System) ・INVISILAN (Moving Target Defense)	2012年1月現在

出典：DoD Cyber (IA) Range: Enabling Dominance in Cyberspace, USMC, 23 Jan. 2012

情報保証レンジの全体構成及び具体能力をそれぞれ図6.2-3及び表6.2-4に示す。

6.3　将来構想

(1) DoDサイバー科学技術ロードマップ[14)15)]

DoDのサイバー科学技術優先度運営委員会は、「DoDサイバー科学技術ロードマップ」のあ

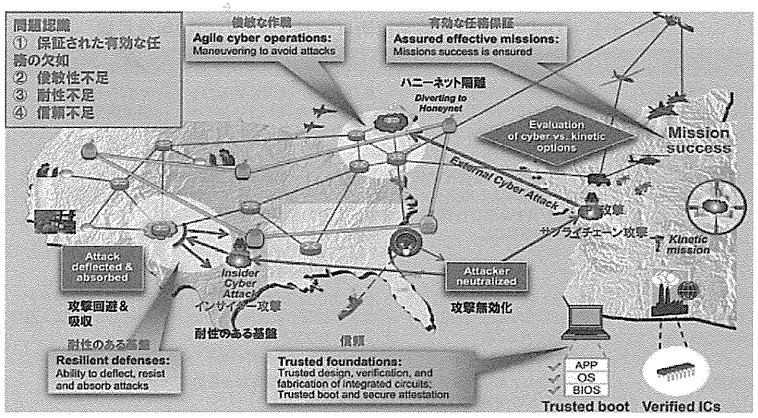

図6.3-1　「DoDサイバー科学技術ロードマップ」のあるべき姿

出典：Cyber S&T Priority Steering Council Research Roadmap, DoD, 8 Nov. 2011

るべき姿として、図6.3-1に示すとおり保証された有効な任務の欠如、俊敏性、耐性及び信頼の不足の問題認識に基づき、DoDのサイバー科学技術優先度項目として有効な任務保証、俊敏な作戦、耐性のある基盤及び信頼基盤の4つの能力の実現を挙げている。

また、「DoDサイバー科学技術ロードマップ」のあるべき姿で挙げている4能力のビジョン、10年先目標及び技術課題を表6.3-1に示す。

有効な任務保証能力としては、サイバー脅威及び脆弱性に関する任務レベルでのリスク評価及び予測ができることが要求されている。俊敏な作戦能力としては、戦術目標及び環境変化に俊敏に適応するために任務及びシステムの再構成ができることが要求されている。耐性のある基盤能力としては、サイバー被攻撃下においても任務継続ができることが要求されている。信頼基盤能力としては、サプライチェーンリスクを考慮して信頼度の異なる構成要素から既知の信頼のシステムを実現することが要求されている。このように、サイバー被攻撃下においても、任務レベルでのリスク評価及び予測に基づき、耐性のある基盤及び信頼基盤上でアクションとしての任務及びシステムの再構成ができることを目指している。

(2) 米陸軍サイバービジョン2020[16)]

米陸軍は、A2/AD環境下でのサイバー空間の課題を克服するために「米陸軍サイバービジョン2020」を策定し、「2020年におけるあるべき姿」を示している。「米陸軍サイバービジョン2020」は、「精鋭、信頼、適確、高練度要員の専門班は、米陸軍ネットワーク防御、サイバー空間全領域の支配、任務司令部の推進及び決定的なグローバル優位性の確保を行うこと（1番であること）」であり、このビジョンを具体化する「2020年におけるあるべき姿」として、統合化された全領域サイバー能力、サイバー領域作戦自由度の達成及び任務司令部の保証を挙げている。

また、この「2020年におけるあるべき姿」を実現するための主要な要求能力として、低下したネットワーク環境下での作戦、サイバー空間インテリジェンスとサイバー空間共通状況認識（脅威及び脆弱性）の統合化、グローバル対応可能なサイバー空間C2、サイバー空間縦深防御の

表6.3-1 「DoDサイバー科学技術ロードマップ」の10年後目標

能力	ビジョン	10年後目標	技術課題
有効な任務保証（Assuring Efective Missions）	インフラ状態及びサイバー攻撃の追跡、それらが任務機能に与える影響の理解と予測ができること	・履歴データ、状況認識及びシミュレーション技術を統合化する予測サイバー／運動任務ツール	・サイバー任務管制 ・規模効果
俊敏な作戦（Agile Operations）	戦術目標または環境変化に俊敏に適応するためにインフラはシステム及び任務を再構成できること	・高速サイバー軍事作戦及びリアルタイム行動方針管理のための時間制約自動管制ツール ・機動のためのネットワーク、システム及びアプリケーション再構成の一時空間座標	・自動サイバー俊敏化 ・サイバー機動
耐性のある基盤（Resilient Infrastructure）	彼のサイバー攻撃が成功しても任務を中断させることは困難であること	・自動自己管理耐性システム ・完全に認証されたハードウェア、ファームウェア及びアプリケーションのモバイルデバイス	・耐性アーキテクチャ ・耐性アルゴリズム及びプロトコル
信頼基盤（Trust Foundation）	構築されたとおりの定量的なシステムの信頼：混合信頼の要素からの既知の信頼のシステム	・混合信頼の構成要素からの信頼システム	・信頼基盤

出典：Defense Cyber S&T Strategy, DoD, 8 Aug. 2012

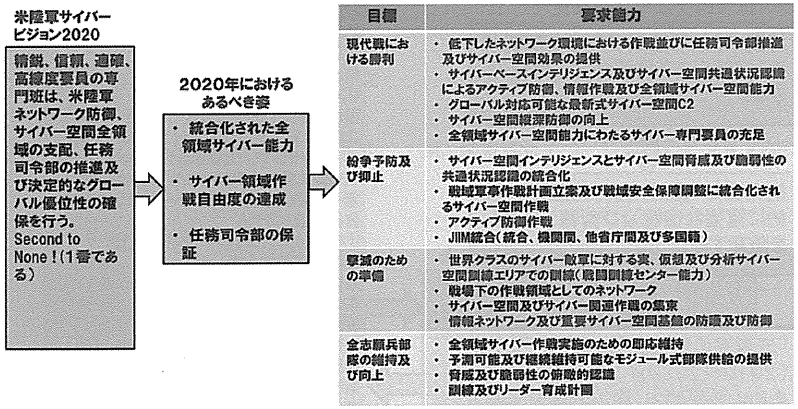

図6.3-2 米陸軍サイバービジョン2020

出典：Army Cyber Command Strategic Plan, Army Cyber Command／2nd Army, 23 August 2011

向上、サイバー演習場、制御システム防護等を挙げている。「米陸軍サイバービジョン2020」から導出されたサイバー要求能力を図6.3-2に示す。

(3) 米海軍サイバー科学技術ロードマップ[17)18)19)20)]

米海軍は、2010年5月制定の「情報優勢のための米海軍のビジョン（The U.S. Navy's Vision for Information Dominance）」に基づき2025年を目標とした「米海軍サイバー科学技術ロードマップ」を策定し、必要なサイバー関連技術能力を示している。「情報優勢のための米海軍のビジョン」は、NCW（Network Centric Warfare）コンセプトを海上戦闘領域が中心であるFORCEnetに、情報領域及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である。また、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並びに指揮官、作戦部隊及び国家の意思決定優越を保証するためのゲーム変更能力を開発、展開及び活用すること」と定義されている。

米海軍は、「行動可能及び安全な情報共有（信頼のある情報が常に利用できる）」の課題認識に基づき、能力戦略として「動的、先行的及び予測的に重要な情報及び情報システムを防御する」という動的なセキュリティリスク管理に基づく戦略を挙げている。さらに、「情報優勢の米海軍ビジョン（2010～2030年）」をサポートするための必要能力としてこの能力戦略をブレークダウンして図6.3-3に示す必要なサイバー関連技術能力を導出している。主要なサイバー関連技術としては、セキュリティ常時監視、リアルタイム脅威分類／予測／見積、攻撃パターン予測モデル、能動検知及び対策立案、高信頼サプライチェーン、サイバー耐性等が挙げられている。

さらに、米海軍は、2012年11月に「米海軍の情報優勢ビジョン」を発展させた次に示す3つの文書を発表している。

・Navy Strategy for Achieving Information Dominance 2013-2017（米海軍の情報優勢実現戦略2013-2017）
・Navy Cyber Power 2020（米海軍サイバー

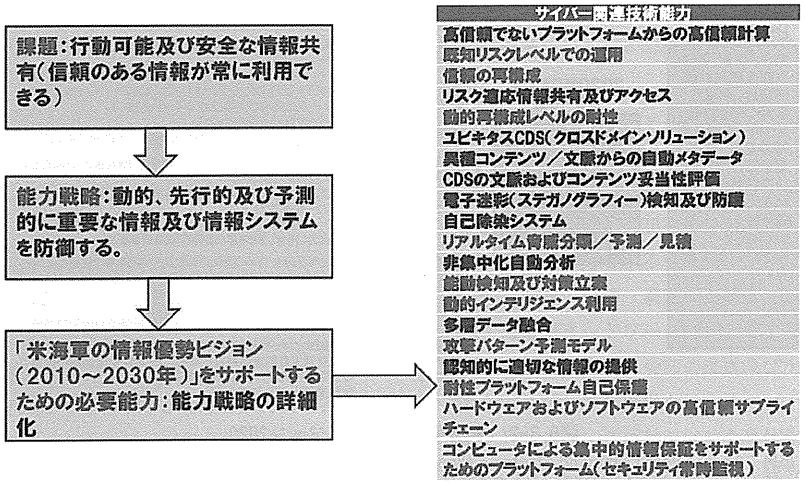

図6.3-3　米海軍サイバー科学技術ロードマップ

出典：Cyber Perspectives: Science and Technology Roadmap, SPAWAR, 14 April 2010

戦力2020）

・Navy Information Dominance Corps Human Capital Strategy 2012-2017（米海軍情報優勢部隊（IDC）人財戦略2012-2017）

「米海軍の情報優勢実現戦略2013-2017」は、保証された指揮統制、戦闘空間認識及び統合火器の３つの情報優勢基盤能力の実現に重点を置き、2013-2017年の主要目標及びねらいを挙げている。特に、A2／AD環境下において、「指揮統制のための通信の堅牢化」を目標の１つとして挙げており、その具体的ねらいとして、「動的ネットワーク化による通信回線の保証」、「電磁スペクトラム運用の管理及び保証」及び「耐性があり保証された指揮統制基盤の構築」を提示している。さらに、現状／中期（1013-2019）及び長期（2010-2028）の作戦環境及び情報環境に基づき３つの情報優勢能力である「保証された指揮統制」、「戦闘空間認識」及び「統合火器」の必要機能並びに現状／中期能力（2013-2019）及び長期能力（2020-2928）を示した「Navy Information Dominance Roadmap, 2013-2028（米海軍情報優勢ロードマップ、2013-2028）」を2013年３月に公表している。このロードマップにおいて、「保証された指揮統制」能力としては、「すべての脅威環境下での部隊指揮」、「全領域の火器の調整」、及び「火器及び我部隊の状態評価」が挙げられている。「すべての脅威環境下での部隊指揮」を実現するための現状／中期及び長期項目としては、それぞれ生残性のある広帯域衛星回線、戦闘用狭帯域回線（保護衛星回線及びHF-IP回線）等並びに保証された電磁スペクトラムアクセス（電磁スペクトラムCOP、リアルタイムスペクトラム作戦能力等）、動的な柔軟性のある情報グリッド（A2／AD環境下のC2狭帯域回線の提供）、共有認識のための任務関連データ、保証された時刻サービス等がある。

「米海軍サイバー戦力2020」は、米海軍のサイバー空間作戦実現戦略である。その戦略は、サイバー空間作戦が米海軍及び統合指揮官に作戦優位性を次の方策によって提供することである。

・サイバー空間及び信頼のある指揮統制へのアクセスの保証（サイバー空間における実効性のある作戦、防御、攻撃及び交戦）
・サイバー空間における戦略的奇襲の防止（サイバー空間における彼の行動の実効性のある評価）
・決定的なサイバー効果の実現（選択の時と場所でのサイバー効果の実現）

(4)　米空軍サイバー科学技術ビジョン2025[21]

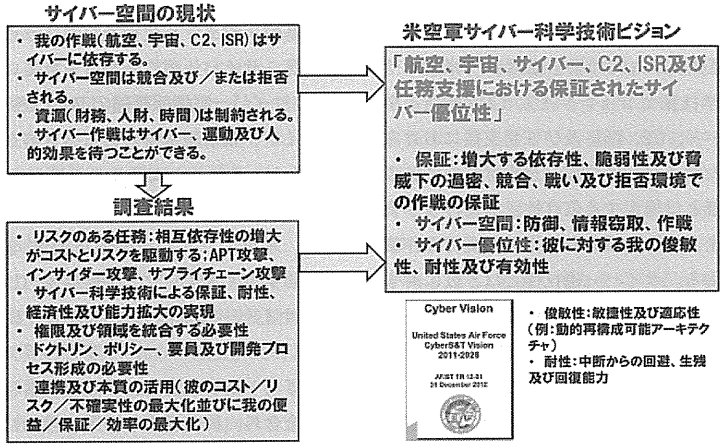

図6.3-4　米空軍サイバー科学技術ビジョン2025

出典：Air Force Cyber Vision 2025, USAF, 31 Dec. 2012

表6.3-2　米空軍サイバー科学技術ビジョン2025（研究開発テーマ）

区　分	研究開発テーマ
任務保証及び能力拡大	・戦闘及び拒否環境下での生残性及び行動の自由 ・ネットワーク及び任務自動地図化によって実現される航空、宇宙及びサイバー指揮官のサイバー状況認識の向上 ・脅威警報、統合化インテリジェンス及びリアルタイムフォレンジックス／攻撃者識別によって実現されるサイバー攻撃検知及び作戦能力 ・高忠実リアルタイムM&S能力を持つ高度サイバー演習場によって実現される早期脆弱性検知及び彼の行動予測 ・サイバー戦闘被害評価を含む横断領域統合効果及び横断領域有効性尺度（MOE）
俊敏性及び耐性の向上	・動的再構成アーキテクチャ（例. IPホッピング等）によって実現される迅速機動によるアクティブ防御 ・生残性のための冗長性、多様性及び細分化の効果的構成 ・攻撃面の削減、重要任務隔離及び攻撃封じ込め ・自動情報窃取検知及び修理（自己回復）並びに脅威に対するリアルタイム対応 ・高性能攻撃検知に向上するためにシグネチャベースサイバーセンサーから行動理解への移行
人間ー機械系最適化	・個人選択、カスタマイズ訓練及び利用者・任務・環境ベース・テーラー化増強認知を実現するための心理、受容及び認知状態の測定 ・状況認識の向上、脅威発見の加速化及び任務能力の拡大のための高性能可視化及び分析ツール ・増強される自動化の透明性及び「ループ上」の増強される人間または監視管制によって実現される適用者と機械間の適切に分担された自動化
信頼基盤	・信頼基盤、耐タンパ技術及びサプライチェーン保証によって実現されるシステムの適用者信頼 ・複雑な大規模相互依存性システムの公式検査及び検証 ・高度脆弱性分析、自動リバースエンジニアリング及びリアルタイムフォレンジックツール ・機密性及び完全性のための高速暗号化、量子通信及び量子暗号

出典：Air Force Cyber Vision 2025, USAF, 31 Dec. 2012

米空軍は、「DoDサイバー科学技術ロードマップ」を考慮して、A2／AD環境下でのサイバー空間の課題を克服するために図6.3-4に示す「米空軍サイバー科学技術ビジョン2025」を2012年12月に公表している。米空軍は、サイバー空間の現状として、我の作戦（航空、宇宙、C2及びISR）のサイバーへの依存、サイバー空間の競合／拒否、資源制約及びサイバー作戦のサイバー、運動及び人的効果を認識し、「米空軍サイバー科学技術ビジョン」として、「航空、宇宙、サイバー、C2、ISR及び任務支援における保証されたサイバー優位性」を挙げている。ここで、保証とは増大する依存性、脆弱性及び脅威下の過密、競合、戦い及び拒否環境での作戦の保証である。サイバー優位性とは、彼に対する我の俊敏性、耐性及び有効性である。

また、米空軍は、「DoDサイバー科学技術ロードマップ」に示された4つの能力に「人間－機械系最適化」の観点を加えて表6.3-2に示す研究開発テーマを挙げている。主要な研究開発テーマとしては、戦闘及び拒否環境下での生残性及び行動の自由、ネットワーク及び任務自動地図化、脅威警報、統合化インテリジェンス及びリアルタイムフォレンジックス／攻撃者識別、高忠実リアルタイムM&S能力を持つ高度サイバー演習場、自動情報窃取検知及び修理（自己回復）並びに脅威に対するリアルタイム対応、動的再構成アーキテクチャ、攻撃面の削減並びに重要任務隔離及び攻撃封じ込め、行動理解、信頼基盤・耐タンパ技術及びサプライチェーン保証等、サイバー耐性が挙げられている。

6.4 サイバー戦情報基盤のあるべき姿と課題

サイバー戦情報基盤のあるべき姿としては、図6.4-1に示すように第5の領域としてのサイバー空間において物理空間と同様に防衛するために、米軍のサイバー関連技術動向からサイバー防御能力だけでなくサイバーC2ISR能力及びサイバー攻撃能力から構成する必要がある[22]。

サイバー防御能力は、サイバー常時監視（S）能力を含み、彼の脅威の防護・検知に加えて、我の脆弱性をリアルタイムに検知する。また、サイバー常時監視能力を除くサイバーC2ISR能力は、サイバー指揮統制（C2）、サイバーインテリジェンス（I）及びサイバー偵察（R）能力から構成される。サイバー指揮統制能力は、サイバー空間における彼（脅威）及び我（脆弱性）の状況認識及び任務レベルのリスク評価を行い指揮官の意思決定を支援する。サイバーインテリジェンス能力は、外部センサ及び内部センサからの警報並びにOSINT（Open Source INTelligence）等のインテリジェンスからサイバー脅威に関する情報の収集及び分析を行い、サイバー脅威を特定するためにサイバー指揮統制能力を支援する。サイバー偵察能力は、彼の軍事システム等の構成並びに脆弱性（彼のプロファイル）を事前に把握するために、平時において偵察を行う。

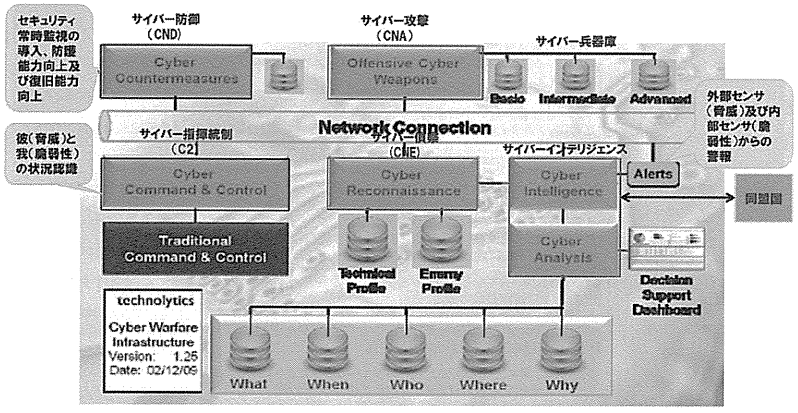

図6.4-1　サイバー戦情報基盤のあるべき姿

出典：The Cyber Commander's eHandbook, Kevin Coleman, technolytics, 2012（一部加筆）

米海軍は、情報優勢ビジョンを実現するために従来の海上戦闘領域における指揮統制能力の持つ軍／部隊の位置（Who／Where：2W）の状況認識から軍／部隊の位置だけでなく、軍／部隊任務、任務状態及び作戦目的に向けた進行状況（Who、What、When、Where、Why及びHow：5W1H）の状況認識へ移行することを目標としている。この目標を達成するために米海軍の従来の指揮統制能力（C2）であるGCCS-M（Global Command and Control System-Maritime）とISR能力であるDCGS-N（Distributed Common Ground System-Navy）の融合が進められている[23]。

サイバー空間においては、海上戦闘領域における外部センサによる比較的容易な軍／部隊の位置の状況認識と異なり、彼（脅威）の状況認識及び位置標定は、多様性、匿名性、秘密性及び攻撃側の優位性の利用により外部センサだけでは困難な場合が多い。したがって、サイバー空間においては、海上戦闘領域におけるよりも外部センサによる彼（脅威）及び内部センサによる我（脆弱性）の状況認識によるサイバー指揮統制能力とサイバーISR能力との融合によるサイバー空間の状況認識能力の向上が必要である。

防衛省は、2013年12月に公表した「新防衛計画大綱」において、海上優勢及び航空優勢のための広域に渡る常続監視に加えて、初めて宇宙空間及びサイバー空間の常続監視態勢の構築を挙げている[24]。

サイバー攻撃能力については、我が国においても、防衛省が2012年9月に公表した「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」によると、「武力攻撃の一環としてサイバー攻撃が行われた場合、自衛権発動の第一要件（我が国に対する急迫かつ不正の侵害があること）を満たすことになると考えられる」との認識が示されている。まだ、サイバー戦争に関する国際法は存在しないが、北大西洋条約機構（NATO）のサイバー防衛協力研究センターが作成した「タリンマニュアル」は、サイバー攻撃に国際法を適用した初めての試みであり、「武力行使に匹敵するようなサイバー攻撃に関する国際法の出発点は、既存の戦時国際法におくべきであり、ジュネーブ条約に従うべきである」との見解を示している[25]。したがって、サイバー攻撃能力の保有については、サイバー攻撃に関する国際法の動向に基づき検討する必要がある。

7．まとめ

A2／AD環境下におけるサイバー空間の脅威は、APT攻撃、インサイダー攻撃、サプライチェーン攻撃、ネットワークアクセス阻止攻撃及び制御システム脆弱性攻撃である。最大のサイバー脅威であるAPT攻撃は、クローズ系のC4ISRシステムに対してもマルウェアの拡散

がUSBメモリ及び電磁波利用により可能である。

サイバー攻撃に対する脆弱性には、重要インフラの脆弱性、制御システムの脆弱性、情報システムの脆弱性、サプライチェーンの脆弱性及び人的資源の脆弱性がある。重要インフラの脆弱性は、情報通信分野(通信)、電力分野及び水道分野の他分野との相互依存性である。制御システムの脆弱性は、情報システムに比べてセキュリティ管理策に基づくセキュリティ管理が遅れていること及びセキュリティ設計が十分でないことである。情報システムの脆弱性は、動的な情報セキュリティリスク管理に基づく適時なセキュリティ状態の状況認識能力が確立できていないことである。また、制御システム製品及びソフトウェア製品のゼロデイ脆弱性は、サイバー兵器開発の重要資産であり、セキュリティ研究者と顧客間を仲介する業者及びセキュリティ会社から構成される闇市場が急速に成長している。サプライチェーンの脆弱性は、ハードウェア構成要素である集積回路の非同盟国での生産によるハードウェアバックドア組み込み潜在性に対する検知能力が確立できていないことである。

サイバー攻撃技術は、これらの脆弱性を用いて開発され、論理兵器、物理兵器及び心理兵器(ソーシャルエンジニアリング)に大別される。論理兵器の進歩は、インターネットサイトからの容易な入手・利用及び有償ベースの犯罪サプライチェーンの提供により攻撃者のサイバー攻撃能力の技術障壁を低下させている。また、国家主導開発のAPT攻撃マルウェアは、統合化、高度化及び大規模化が進んでいる。サイバー兵器としてのAPT攻撃マルウェアを開発するための鍵は、ゼロデイ脆弱性発見能力及びエクスプロイト開発能力を有するセキュリティ研究者、ホワイトハッカー等の高度セキュリティ技術者の確保である。また、物理兵器には、サプライチェーン攻撃のための偽造ハードウェア及びハードウェアバックドア並びに電磁サイバー攻撃である航空ネットワーク攻撃システムがあり、これらの技術が現実に使用されている。

現状のサイバー防御技術は、防護技術及び外部センサ検知技術によるサイバー脅威の状況認識並びに静的な定期的情報セキュリティ監査による脆弱性の状況認識が主体である。APT攻撃のようなサイバー脅威は完全に防御できないため、動的なリスクに対応できる情報セキュリティリスク管理に基づき、サイバー脅威の状況認識に加えて、内部センサによるリアルタイムな資産及びセキュリティ管理策の脆弱性の状況認識を行い、適時及び適切なリスク対応を行う必要がある。米国では、DHS及びDoDを中心にセキュリティ自動化技術に基づくセキュリティ常時監視の連邦政府情報システム及びDoD情報システムへの導入が進められている。米国は、重要インフラについてもセキュリティ常時監視の導入政策を推進している。また、DoDは重要インフラサービス調達要件に制御システムのセキュリティ常時監視要件の盛り込みを検討している。

一方、我が国では、APT攻撃に対するリスクベースの新たな対応の1つとして「脆弱性の対処」が、新たに策定された「サイバーセキュリティ戦略」において挙げられているが、セキュリティ常時監視の具体的な方針まで至っていない。制御システムのセキュリティ常時監視については、検討テーマとしてもスコープに入っていない。実効性のあるAPT攻撃対策のために、我が国のサイバーセキュリティ戦略を抜本的に見直す必要がある。APT攻撃は、DDoS攻撃のような予測及び可視化できる従来のサイバー攻撃と異なる高度な持続性及び隠密性を持つネットワーク速度の攻撃であり、動的なリスクに対応できる情報セキュリティリスク管理に基づくサイバー攻撃対処能力の革新が必要である。今そこにある危機に対応するために、サイバーセキュリティ投資優先度をセキュリティ常時監視に変えるサイバーセキュリティ法を制定する国家としての意思決定が必要である。

最後に、現状及び開発中の米軍のサイバー関連技術の動向から、APT攻撃、インサイダー攻撃、サプライチェーン攻撃等のサイバー脅威に対応するためのセキュリティ常時監視の整備、サイバー演習場の整備、インサイダー攻撃対策技術の開発及びサプライチェーン攻撃対策技術の開発に注目すべきである。また、将来構想としての米軍のサイバー関連技術の動向については、A2／AD環境下における課題克服のために設定されたDoDサイバー科学技術ロードマップの優先項目である有効な任務保証、俊敏な作戦、耐性のある基盤及び信頼基盤の4能力の構築に向けた各軍種の構想に注目すべきである。特に、サイバー耐性能力は、復旧する能力だけでなく、予測する、耐える及び進化する能力を含むものであり、その開発にはサイバー耐性工学と呼ばれる総合的な方法論が必要である。

参考文献

1) DoD: Quadrennial Defense Review (QDR) Report, Feb. 2010
2) DoD: Department of Defense Strategy for Operating in Cyberspace, July 2011
3) DoD: Sustaining U.S. Global Leadership: Priorities for 21st Century Defense, Jan. 2011
4) DoD: U.S. Cyber Command Fact Sheet, 25 May 2010
5) DISA: Cyber Domain Situation Awareness, 7 June 2011
6) Robert Lentz: Cyber Security Maturity Model, 2011
7) Ellen Nakashima: With Plan X, Pentagon seeks to spread U.S. military might to cyberspace, Washington Post, 31 May 2012
8) Ellen Nakashima: List of cyber-weapons developed by Pentagon to streamline computer warfare, Washington Post, 1 June 2011
9) DISA: Enclave Security: Secure Configuration Management (SCM), DISA, 7-10 May 2012
10) Micheal Cooney: DARPA expands insider threat research, Layer 8, 8 Aug. 2011
11) THE NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT: PROGRAM: Supplement to the President's Budget FY2013, Feb. 2012
12) DISA: DoD Information Assurance Range: A Venue for Test and Evaluation in Cyberspace, August 2011
13) Jeffrey Combs: DoD Cyber (IA) Range: Enabling Dominance in Cyberspace, USMC C4, DON IT Conference, West Coast 2012, 23-26 Jan. 2012
14) DoD: Cyber S&T Priority Steering Council Research Roadmap, 8 Nov. 2011
15) DoD: Defense Cyber S&T Strategy, 8 Aug. 2012
16) Army Cyber Command／2nd Army: Army Cyber Command Strategic Plan, LANDWARNET 2011, 23 August 2011
17) SPAWAR: Cyber Perspectives: Science and Technology Roadmap, NDIA S&T Conference, 14 April 2010
18) U.S. Navy: Navy Cyber Power 2020, Nov. 2012

19) U.S. Navy : Navy Strategy for Achieving Information Dominance 2013-2017, Nov. 2012
20) U.S. Navy : U.S. Navy Information Dominance Roadmap 2013-2028, March 2013
21) USAF : Air Force Cyber Vision 2025, 31 Dec. 2012
22) Technolytics : The Cyber Commander's eHandbook, Version 3, 2012
23) Patric Garcia : Maritime C2 Strategy : An Innovative Approach to System Transformation, PMW150 SPAWAR, 15th ICCRTS, 23 April 2010
24) 防衛省：平成26年度以降に係る防衛計画の大綱について、平成25年12月17日
25) Michael N. Schmitt : Tallinn Manual on The International Law Applicable to Cyber Warfare, Cambridge University Press, 2013