# 米国の国防体制における IT 利活用の動向

和田恭＠JETRO/IPA New York

## 1. はじめに

2001 年の同時多発テロ発生以降、米国では「対テロ戦争」に重点をおいた柔軟な国防政策への転換が行われており、国防予算も 2011 年度まで毎年上昇してきた。この対テロ戦争へのシフトに伴い、IT が国防において果たす役割もより重要になってきている。一方で、2012 年度以降は、連邦政府の財政健全化の一環として、国防予算が削減される予定となっているが、業務効率化の促進、また昨今の大きな課題であるサイバー攻撃の脅威への対処といった観点から、国防において IT が果たす役割は依然として重要であり続けると考えられる。

本稿では、2001 年以降から現在にわたる連邦政府の国防体制における IT の利用状況を紹介し、現在の国防において IT が果たす役割について考察する。

## 2. 米国連邦政府の国防政策と体制

本章では、2001 年同時多発テロ発生以降 10 年間の連邦政府国防政策の経緯・傾向と、米国連邦政府において安全保障に関与する主要省庁の役割について概要を紹介する。

### (1) 米国国防政策の経緯と傾向

ここ 10 年間における米国連邦政府の国防政策は、大まかに以下の 3 つのフェーズに分類可能と言える。以下、フェーズ毎に米国連邦政府の国防政策における重点項目や傾向を紹介する。

- 同時多発テロ発生からアフガニスタンおよびイラク戦争の本格化（2001～2005 年）
- アフガニスタンおよびイラク戦争の長期化（2006 年～2009 年）
- アフガニスタンおよびイラクにおける展開規模縮小と緊縮財政に伴う軍備ダウンサイジング（2010 年～）

#### ① 同時多発テロ発生からアフガニスタンおよびイラク戦争の本格化

過去 10 年間の米国において発生した最も象徴的な有事として、2001 年 9 月に発生した同時多発テロ事件があげられる。正規軍ではない非国家的集団によって引き起こされ、

約 3,000 人の犠牲者を出した同事件前後に、米国連邦政府は国防方針の見直しを表明している。

具体的には、同時多発テロ発生直後に、国防総省（Department of Defense、DoD）が発行する「Quadrennial Defense Review（4 年おきの国防政策見直し、QDR）」を改訂し、「『脅威』に対応することを念頭に置いた防衛政策から『攻撃能力・方法』に対応することを念頭に置いた政策に移行し、『敵が誰であるか、どこで紛争が発生するか』、といった事項よりも、『敵はどのような方法で戦うのか』に注目した政策立案」を提唱している[1]。これによって、今後米国に対する主要な脅威が、敵対国家[2]から非国家的集団による非対称型のものが中心になると予想される中で、IT 関連技術については、以下のような観点から重要になると指摘している。

- IT システムの強化により、敵の恒常的な監視、追跡、および敵への迅速な攻撃を行うこと。
- 上記を実現するために、宇宙空間における能力強化に加え、IT の活用や省庁間の連携を高めること。

以上のような思想のもと、米国の国防政策においては、より身軽で迅速な作戦能力展開を重視する方針が同時多発テロ発生後に打ち出されている。なお、米国内における国防政策という面では、2001 年 10 月にいわゆる愛国者法（USA PATRIOT Act）が成立しており、これによって防諜目的で当局が個人情報を取得する、あるいは通信を傍受することなどが可能となっている。同法は、主に国境警備・入国管理や米国内の対テロ諜報活動を強化することを目指すもので[3]、米国の国防政策が、米国に敵対する非国家的組織の制圧へとシフトし始めたことを明確に示している。

### ② アフガニスタンおよびイラク戦争の長期化

同時多発テロ発生から 5 年が経過した 2006 年に QDR は改訂されている。その概要は、全般的に 2001 年に打ち出された方針を継承するものとなっており、「無差別的に攻撃を行い、もし入手できれば大量破壊兵器（Weapons of Mass Destruction、WMD）の使用も辞さないテロリスト」を最大の脅威と捉え、以下のような思想の転換を促している[4]。

＜2006 年 QDR における新たなポイント＞

- 1 つの集中的な脅威よりも、分散された複数の脅威への対処を重視。
- 国家的集団の脅威よりも、非国家的集団による脅威への対処を重視。

[1] http://www.dod.gov/pubs/qdr2001.pdf
[2] 2001 年時点では、アフガニスタン、イラン、イラク、北朝鮮、リビア、キューバ、スーダン、シリアが「テロ支援国家」、いわゆる「ならず者国家（rogue states）」として批判されていた。このうちイラン、イラク、北朝鮮については、2002 年の一般教書演説にて、ブッシュ大統領（当時）が「悪の枢軸（Axis of Evil）」と呼んだ。
[3] http://www.justice.gov/archive/ll/highlights.htm
[4] http://www.defense.gov/qdr/report/report20060203.pdf

- 危機・紛争発生後の対処よりも、発生前の予防的行動の重視。
- 恒久的な駐留軍を中心とする展開体制よりも、身軽で世界各地に素早く展開可能な体制の重視。
- 縦割り型の組織から、より水平型の組織への移行。
- 従来の一般的な兵器に加え、行動に直結する有益な情報、知識、機密情報も重視。

前版の QDR 発行時と比べ、2006 年の時点では、いわゆる「テロ支援国家」のうち 2 か国であるアフガニスタンとイラクの政権転覆が実現し、通常戦においては米国の軍事力が圧倒的であることが実証されていたこともあり、2006 年版 QDR では、より非国家的集団の脅威を強調する内容になっている。つまり、2000 年代中盤以降の米国連邦政府による国防政策は、同時多発テロ発生後の方針を踏襲し、非対称戦争を念頭に置いた、より柔軟な体制構築を目指すものであると言える。

### ③ アフガニスタンおよびイラクにおける展開規模縮小と緊縮財政に伴う軍備ダウンサイジング

2008 年のオバマ政権成立後も、2009 年から 2010 年初頭にかけては、アフガニスタンで米軍の増派が行われるなど、同政権発足当初は表向きに国防政策に大きな変更は見られなかった。しかし、直近（2010 年 2 月）に改訂された QDR では、米軍のイラク撤退が目前に迫っていたこと、連邦政府の財政緊縮化に対する圧力が米国内で高まっていたことなどもあり、国防政策の方向性に多少の変化が見られる。特に重点項目として扱われているものとしては、以下があげられる[5]。

＜2010 年 QDR における新たなポイント＞

- 地域紛争の抑止または緩和の重視。
- 従来からの同盟国や、インドや中国など新興経済国との協力または対話。
- 有効かつ最も必要な兵器に絞って調達し、責任のある出費を行うこと。

このうち、特に 3 番目の事項については、米国連邦政府の財政状況悪化を受け、国防を含めた各般の予算削減が迫られている状況を反映するものであると言える。実際に、DoD の予算額は、2012 年度以降の 10 年間で総額 3,000 億ドルが削減されることが予定されていることから[6]、今後は調達基準の見直しや業務インフラの効率化による経費削減に対する要求も高まってくると考えられる。

また、国防上、引き続きアルカイダを始めとする非国家的テロ集団が最重要視すべき脅威とされており、そのような勢力に対する対抗手段として、敏捷性が高いヘリコプタ系の

[5] http://www.comw.org/qdr/fulltext/1002QDR2010.pdf
[6] http://defensesystems.com/Articles/2011/12/01/Senate-passes-NDAA-defense-bill-IT-provisions.aspx?Page=2&p=1

兵器増強、偵察・諜報目的の有人・無人航空機およびシステム導入に加えて、C4I（指揮、統制、通信、コンピュータ、情報の略）システム強化の重要性が指摘されているなど、IT システムが重要な役割を果たすと考えられる項目が目立っている。

更に、2001、2006 年版 QDR ではほとんど言及されていなかった事項として、2010 年 QDR ではサイバー空間における防衛能力の向上の一環としてサイバー軍の創設がうたわれている。これと同期して、米国連邦政府ではサイバーセキュリティ体制を確立するための動きが活発化しており、以下のような発表がこれまでになされている。

- ホワイトハウスによる「サイバー空間における政策の見直し（Cyberspace Policy Review）」発表（2009 年 5 月）。
- 大統領直属の「サイバーセキュリティ調整官（Cybersecurity Coordinator）」職の任命（2009 年 12 月）[7]。
- サイバー空間における防衛能力を持ち、各軍におけるサイバー軍事行動を統括するサイバー軍（Cyber Command）の設置（2010 年 5 月）[8]。
- ホワイトハウスによる、「サイバーセキュリティ法案立案に向けた提案書（Cybersecurity Legislative Proposal）」、および「サイバー空間防衛に関する国際戦略（International Strategy for Cyberspace）」の発表（2011 年 5 月）[9]。
- 各省庁の機密情報保護体制強化に向けた大統領令の発令（2011 年 10 月）[10]。
- これまでイラクやアフガニスタンなどへ大量の兵力投入が行われていた時代から、新たな敵対勢力への対応のための偵察や諜報など、スリムで機動的な国防体制整備を目指した新たな国防戦略の発表[11]（2012 年 1 月）

### ④ 国防政策の傾向

最近 10 年の米国連邦政府による国防政策をまとめると、テロリズムなど、これまでの敵対国家とは異なる非国家的集団によるゲリラ的な脅威が強調されており、そのような脅威への対抗手段を念頭に置いた内容となっている。

この中で、特に IT との関わりが深い分野での動きとしては、以下が挙げられる。

- 国内外における監視・防諜・諜報活動の活発化
- 国境警備・入国管理体制の強化
- 軍事機器・装備の無人化・自動化
- サイバーセキュリティ強化

[7] http://searchsecurity.techtarget.com/news/1357549/Obama-announces-creation-of-cybersecurity-coordinator-position
[8] http://www.armytimes.com/news/2010/05/military_cyber_command_052110/
[9] http://www.huffingtonpost.com/sarah-granger/white-house-unveils-globa_b_863651.html
[10] http://www.washingtonpost.com/politics/white-house-order-to-establish-new-cybersecurity-policies/2011/10/06/gIQA7tclRL_story.html
[11] http://www.whitehouse.gov/blog/2012/01/05/president-obama-outlines-new-global-military-strategy

- IT システム・インフラ更新による経費削減

中でも、米国に対する脅威を未然に防ぐための監視・諜報手段において、IT の果たす役割は拡大していると考えられる。また、QDR 中、サイバーセキュリティについては、各軍におけるサイバーセキュリティ部門を統合したサイバー軍の創設（2010 年 5 月）、サイバーセキュリティ人材育成、DHS をはじめとした関係省庁との連携などが記述されている。

### (2) 議会の動き

以下では、現国会会期（第 112 議会、2011 年 1 月 3 日～2013 年 1 月 3 日）中、これまでに提出された主要国防関連法案を表記する。

**【図表 1: 現会期中に提出された国防関連法案】**

| 法案名 | 現在の状況 | 概要 |
|---|---|---|
| **FAA Air Transportation Modernization and Safety Improvement Act**[12] | 2011 年 4 月に上院を通過 | プログラムの効率化、航空安全の強化、無駄の排除、などを行うための、2011 年度から 2014 年度までの連邦航空局（Federal Aviation Administration、FAA）予算を決定する。 |
| **National Guard Empowerment and State-National Defense Integration Act of 2011**[13] | 2011 年 5 月に上院軍事委員会に提出 | 国防軍（U.S. National Guard）の権限を向上させ、国防軍局（National Guard Bureau）の機能を拡大させ、緊急時の連邦及び州レベルの軍隊間の協力体制を向上することで、国防を強化する。 |
| **Detaining Terrorists to Secure America Act of 2011**[14] | 2011 年 5 月に上院軍事委員会に提出 | DoD が、キューバ・Guantanamo 湾にある米海軍基地を、敵兵やテロリストの拘束場所として保持する権限を再確認する。 |
| **Department of Defense Energy Security Act of 2011**[15] | 2011 年 6 月 15 日に上院軍事委員会に提出 | DoD 長官の指揮の下、前進作戦基地（forward operating bases）における廃水の削減、飲料水の節水、節電、補給路からの独立、など様々な手法を用いて、軍隊によるエネルギー使用量を削減するメカニズムの実現可能性を検証するパイロットプロジェクトを実施する。 |
| **Declaring that the President shall not deploy, establish, or maintain the presence of units and members of the United States Armed Forces on the ground in Libya, and for other purposes**[16] | 2011 年 6 月に下院を通過 | 大統領に対して、リビア内戦など国家の安全保障と直接関係のない目的で、米国防軍を陸上配備しないことを要求する。 |

[12] http://www.govtrack.us/congress/bill.xpd?bill=h112-658
[13] http://www.govtrack.us/congress/bill.xpd?bill=s112-1025
[14] http://www.govtrack.us/congress/bill.xpd?bill=s112-982
[15] http://www.govtrack.us/congress/bill.xpd?bill=s112-1204
[16] http://www.govtrack.us/congress/bill.xpd?bill=hr112-292

| | | |
|---|---|---|
| **Veterans Opportunity to Work Act of 2011**[17] | 2011 年 10 月に下院退役軍人委員会に提出 | 合衆国法典 38 編にある、退役軍人の雇用及び訓練に関する条項を改善する。 |
| **Civil Reserve Air Fleet Missile Defense Pilot Program Act of 2011**[18] | 2011 年 10 月に下院軍事委員会に提出 | DoD 長官に対して、ミサイル防衛システムを備えた民間予備航空輸送部隊（Civil Reserve Air Fleet）にターボジェット搭載航空機を導入することの実現可能性を検証するパイロットプログラムの実施を要求する。 |
| **Defense Supply Chain and Industrial Base Security Act**[19] | 2011 年 11 月に下院軍事委員会に提出 | DoD 長官に、国防サプライチェーン及び軍事産業基盤戦略を策定させる。 |
| **Justice Against Sponsors of Terrorism Act**[20] | 2011 年 11 月上院司法委員会に提出 | 海外組織によるテロリズム及びそのスポンサー行為を防止する。 |
| **National Defense Authorization Act (NDAA) for Fiscal Year 2012**[21] | 2011 年 12 月に上院を通過 | DoD の軍事活動、及び、エネルギー省（Department of Energy、DoE）の軍事活動・軍事関連建設事業に係る 2012 年度予算を決定する。 |

### (3) 主要国防関連省庁

米国連邦政府の国防体制においては、以下に表記する省庁が主要な役割を果たしている[22]。次章では、これらの省庁毎に IT 利活用動向を示す。

**【図表 2: 米国連邦政府の主要国防関連省庁】**

| 省庁名 | 役割 |
|---|---|
| **国防総省（Department of Defense、DoD）** | 大統領による司令に基づき、陸軍、海軍、空軍、海兵隊の 4 軍を統合、管理する。また、傘下の国家安全保障局（National Security Agency、NSA）を通して、米国外にて交信される機密情報の傍受・解読などを行う。 |
| **国土安全保障省（Department of Homeland Security、DHS）** | テロリズムを始め、米国内で発生する可能性がある有事に対する準備、予防、また発生後の対処を行う。 |
| **中央情報局（Central Intelligence Agency、** | 米国内外における諜報活動、秘密作戦、破壊工作などを行う。 |

[17] http://www.govtrack.us/congress/bill.xpd?bill=h112-2433
[18] http://www.govtrack.us/congress/bill.xpd?bill=h112-3284
[19] http://www.govtrack.us/congress/bill.xpd?bill=h112-3449
[20] http://www.govtrack.us/congress/bill.xpd?bill=s112-1894
[21] http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=112&session=1&vote=00218
http://www.govtrack.us/congress/bill.xpd?bill=h112-1540
[22] http://www.homelandsecurityresearch.com/wp-content/uploads/2009/12/US-HLS-HLD-Structure-2010.pdf

| | |
|---|---|
| **CIA）** | |
| **司法省<br>（Department of Justice、DoJ）** | 傘下の連邦捜査局（Federal Bureau of Investigation、FBI）、麻薬取締局（Drug Enforcement Administration、DEA）、アルコール・タバコ・火器及び爆発物取締局（Bureau of Alcohol, Tobacco, Firearms and Explosives、ATF）を通し、米国内における重大な犯罪の捜査や取り締まりを行う。 |
| **その他：運輸省（Department of Transportation、DoT）、国務省（Department of State、DoS）、エネルギー省（Department of Energy、DoE）など** | • DoT：入国管理などを担当する。<br>• DoS：外交チャンネルを通した情報収集・分析などを行う。<br>• DoE：電力インフラの保安などを担当する。また、傘下の国家核安全保障局（National Nuclear Safety Administration、NNSA）を通して、核軍備の信頼性や安全性確保を担当する。 |

### (4) 主要国防関連企業

次に、米国において国防関連の装備や IT システムを納入している主要企業について紹介する。

#### ① Lockheed Martin 社

（本社：Maryland 州 Bethesda 市、従業員数：約 12 万 6,000 人[23]）
Lockheed Martin 社は、航空機および宇宙関連技術の開発で知られる事業者であり、古くから国防関連の大規模案件を連邦政府より受注している。同社によって開発された有名な製品としては、トライデント・ミサイル（潜水艦発射弾道ミサイル）、F-16（戦闘機）、F-22（戦闘機、Boeing 社との共同開発）などがあげられる。

#### ② Boeing 社

（本社：Illinois 州 Chicago 市、従業員数：17 万 1,715 人[24]）
Boeing 社も、Lockheed Martin 社と同様に、航空・宇宙業界で最も有力な企業の 1 つであり、連邦政府向けに多くの軍事機器・製品を製造している。著名な連邦政府向け製品としては、F-15（戦闘機）、F-22（戦闘機、Lockheed Martin 社との共同開発）、AH-64（戦闘ヘリコプタ、通称「アパッチ」）、国際宇宙ステーションの主要パーツなどがあげられる。

#### ③ Northrop Grumman 社

（本社：Virginia 州 Falls Church 市、従業員数：約 11 万 7,100 人[25]）
Northrop Grumman 社は、軍事用航空機の開発を行う事業者で、MQ-8（無人ヘリコプタ）、X-47（無人戦闘機）、E-2（早期警戒機）などの開発で知られている。なお、同社はか

[23] http://www.lockheedmartin.com/aboutus/index.html
[24] http://www.boeing.com/aboutus/employment/employment_table.html
[25] http://www.northropgrumman.com/pdf/2010_noc_ar.pdf

つて海軍向けに航空母艦、強襲揚陸艦、原子力潜水艦なども製造していたが、これらの製造を行っていた部門は 2011 年 3 月に Huntington Ingalls Industries 社としてスピンオフされている。

### ④ General Dynamics 社

（本社：Virginia 州 West Falls Church 市、従業員数：約 9 万人[26]）
General Dynamics 社は、船舶、戦車、IT 製品、航空機などの製造で知られる事業者で、DoD をはじめ連邦政府より多くの案件を受注している。著名な製品としては、M1 Abrams（戦車）、GAU-19（重機関銃）、Sectéra Edge（NSA 公認スマートフォン）などが存在する。

### ⑤ Raytheon 社

（本社：Massachusetts 州 Waltham 市、従業員数：約 7 万 2,000 人[27]）
Raytheon 社は、ほぼ国防関連製品の開発・製造に特化する事業者で、特に IT システム、ミサイル、航空機、宇宙関連製品などを主力製品としている。MIM-104（地対空ミサイル、通称「パトリオット・ミサイル」）、BGM-109（巡航ミサイル、通称「トマホーク」）、各種戦闘機や船舶向けのレーダーシステムなどが有名な製品として挙げられる。

### ⑥ Science Applications International Corporation（SAIC）社

（本社：Virginia 州 McLean 市、従業員数：約 4 万 1,000 人[28]）
SAIC 社は、国防関連製品をはじめ、医療 IT 製品、サイバーセキュリティ関連製品、エネルギー関連製品など、多種多様な分野で事業展開している。国防関連の主力製品としては、陸軍向けの暗視装置、IT インフラ製品、空港などのセキュリティ・チェックポイントで使われる危険物検査装置などがある。

### ⑦ Honeywell 社

（本社：New Jersey 州 Morristown 市、従業員数：約 12 万 2,000 人[29]）
Honeywell 社は、一般消費者向けの白物家電から国防関連製品まで、多種多様な製品を製造するコングロマリットである。国防関連製品としては、航空機・車両・船舶向けの誘導・ナビゲーションシステム、遠隔地に駐留する部隊向けの電力システムなどが主要な製品として挙げられる。

### ⑧ Hewlett-Packard（HP）社

（本社：California 州 Palo Alto 市、従業員数：約 32 万 4,600 人[30]）

[26] http://www.gd.com/about/corporate-overview/
[27] http://www.raytheon.com/ourcompany/
[28] http://www.saic.com/about/
[29] http://honeywell.com/About/Pages/our-company.aspx
[30] http://media.corporate-ir.net/media_files/irol/71/71087/AR2010/HTML2/hewlett-packard-ar2010_0023.htm

HP 社は、一般企業や消費者向けの IT 製品開発を主要事業とする企業で、国防関連省庁に対しては、PC、PC 周辺機器、サーバー、ネットワーク機器といった製品、更に IT サポートなどの付加価値サービスを提供している。

### ⑨ Harris 社

（本社：Florida 州 Melbourne 市、約 1 万 6,900 人[31]）
Harris 社は、各種通信・ネットワーク機器を製造する大手事業者で、一般企業や連邦政府向けにこれらの製品を提供している。国防関連省庁に対しても同様の商品を提供しており、通信インフラの整備や、ネットワーク機器の調達などを行っている。

### ⑩ General Electric 社

（本社：Connecticut 州 Fairfield 市、従業員数：約 28 万 7,000 人[32]）
General Electric 社は、Honeywell 社と同様に、消費者向けの白物家電から発電機・変換器などの重工業製品まで、幅広く開発するコングロマリットである。国防関連省庁に対しても、展開する多数の事業部門から多種多様な製品を納品しているが、最近の受注例としては、航空機向けのエンジン開発プロジェクトなどがある[33]。

[31] http://www.harris.com/ar/archives/2011-Annual-Report.pdf
[32] http://www.ge.com/company/factsheets/corporate.html
[33] http://www.bizjournals.com/cincinnati/stories/2010/07/05/daily14.html

## 3. 国防関連省庁による最近の IT 利活用動向

本章では、前章で挙げた主要国防関連省庁について、最近 3～5 年の予算動向、IT 関連プロジェクトの予算額[34]、およびその内容について紹介し、国防体制における IT の利用動向を導出する。なお、特に規模が大きい、または注目されるプロジェクトについては、別途その内容を説明する。

### (1) 全体動向

過去 5 年間の連邦政府全体の国防関連予算の傾向として、以下があげられる。

- 2007 年度から 2008 年度にかけて、主にイラクへの増派などに伴う対テロ戦費の上昇により、国防予算も大幅に増加。
- 2009 年度は前年度比横ばいであったが、2010 年度にはアフガニスタンへの増派などに伴い、国防予算が増加。
- 2011 年度も引き続き上昇したものの、景気の低迷に伴う政府収入の減少やイラク駐留軍の段階的な削減などもあり、伸び幅は以前と比較してわずかな額に留まる。
- 2012 年度以降は、財政健全化への圧力の高まり、イラクからの撤退完了（2011 年）、アフガニスタン駐留軍の削減といった要因から、国防予算の大幅な減少が見込まれている。

2012 年 1 月には、オバマ大統領は今後の国防体制について演説し、その中で欧州駐留軍および陸軍を始めとする常備軍兵力の削減、アジア太平洋地域における体制の強化、対テロ体制の強化、ミサイル防衛能力の向上などから成る指針を表明している[35]。

### (2) DoD （国防総省、NSA 含む）

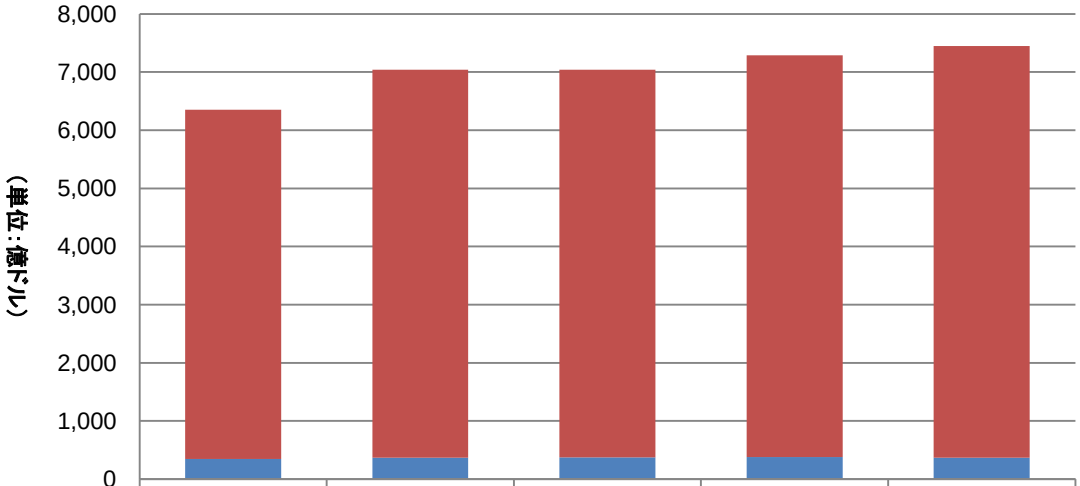
過去 5 年間の DoD の予算額の推移は、以下の通り。総予算額は 2009 年度を除き毎年度上昇している中で、IT 予算額についてはほぼ横ばい状況である。また、図表 4 における IT 関連プロジェクトの開始時期からもわかるように、現在の大規模プロジェクトについては、それ以前に開始された通信インフラ運用プロジェクトが継続されている形がほとんどである。

なお、DoD 予算は今後 10 年間で総額約 4,890 億ドル削減されることが予定されており[36]、特に DoD の管轄下にある陸軍の通常戦力は、現在の約 57 万人体制から約 49 万

[34] http://www.itdashboard.gov/
[35] http://www.defense.gov/news/Defense_Strategic_Guidance.pdf
[36] http://www.washingtonpost.com/opinions/president-obamas-defense-strategy/2012/01/06/gIQAKm5pfP_story.html

人体制にまで縮小される見込みとなっている[37]。その中で、IT 関連予算に関しては、第 4 章で述べるように IT インフラの整備・効率化による支出削減が目指されている。

**【図表 3: DoD の過去 5 年間の総予算額と IT 予算額[38]】**




| | 2007年 | 2008年 | 2009年 | 2010年 | 2011年 |
|---|---|---|---|---|---|
| 総予算額 | 6,010 | 6,670 | 6,670 | 6,910 | 7,080 |
| IT予算額 | 344 | 370 | 373 | 378 | 366 |

次に、DoD の IT 関連プロジェクトについて表記する。2011 年度に多くの予算が投入されているプロジェクトとしては、遠隔地に所在する部隊・兵士らに対して、戦略的な情報を伝送するための通信インフラに関するものが多くなっている。このうち、特に大規模なプロジェクトである DISN と NGEN については、その内容について別途説明する。

**【図表 4: DoD の IT 関連プロジェクトのトップ 10（2011 年度予算額ベース）】**

| | プロジェクト名 | 開始時期 | 予算総額 | 2011 年度予算総額 | 概要 |
|---|---|---|---|---|---|
| 1 | Defense Information | 1991 年 9 月 | 482 億ドル | 21 億ドル | DoD の世界中の国防関連組織における通信をサポートする通信ネット |

[37] http://www.chicagotribune.com/news/opinion/editorials/ct-edit-0109-military-20120109,0,2078760.story
[38] http://www.itdashboard.gov/content/analysis
http://comptroller.defense.gov/defbudget/fy2012/FY2012_Budget_Request_Overview_Book.pdf
http://comptroller.defense.gov/defbudget/fy2012/fy2012_BudgetBriefing.pdf
なお、2011 年度については、総予算額は予算要求額、IT 予算額は ITADashboard により生成された年間の累計。以下同じ。

| | | | | | |
|---|---|---|---|---|---|
| | System Network（DISN）[39] | | | | ワークインフラのことで、戦闘機、戦闘部隊司令部隊などに C4I[40]を包括する長距離通信インフラを提供する。 |
| **2** | Next Generation Enterprise Network（NGEN）[41] | 2008 年 5 月 | 166 億ドル | 19 億ドル | 海軍及び海兵隊の職員にセキュアなデータ通信サービスを提供する。 |
| **3** | Installation Information Infrastructure Modernization Program (I3MP)[42] | 2007 年 10 月 | 24 億ドル | 5 億 9,360 万ドル | インターネットベースの戦闘及び軍事をサポートするために米陸軍の情報通信ネットワーク、ケーブル、電話交換システムなどを近代化する。 |
| **4** | The Airborne and Maritime/Fixed Station (AMF) Joint Tactical Radio System (JTRS)[43] | 2004 年 9 月 | 464 億ドル | 4 億 960 万ドル | 空軍、海軍、固定局などの国防関連組織間の通信システム（Joint Tactical Radio System、JTRS）の開発、統合、サポートを行う。JTRS は、国防総省用の無線通信機器のことで、音声通話とデータ通信をサポートする。 |
| **5** | Warfighter Information Network - Tactical Increment 2[44] | 2007 年 6 月 | 62 億ドル | 3 億 7,950 万ドル | 2007 年の防衛調達に関する覚書（Defense Acquisition Executive、DAE）に基づき、陸軍の通信ネットワーク近代化プログラムをサポートする。具体的には、戦闘機及び戦闘車両用の通信（衛星・無線）ネットワーク及び通信機器を提供する[45]。 |
| **6** | Expeditionary Combat Support System[46] | 2005 年 8 月 | 18 億ドル | 3 億 1,190 万ドル | 米国防関連機関のロジスティックスやサプライチェーンを強化するもの |

[39] http://www.itdashboard.gov/investment?buscid=27#
http://www.itdashboard.gov/investment/schedule-summary/27
[40] Command, Control, Communications, Computers and Intelligence（指揮、統制、通信、コンピュータ、情報）（指揮、統制、通信、コンピュータ、情報）の略。
[41] http://www.itdashboard.gov/investment?buscid=57
http://www.itdashboard.gov/investment/schedule-summary/57
[42] http://www.itdashboard.gov/investment?buscid=53#
http://www.itdashboard.gov/investment/schedule-summary/53
[43] http://www.itdashboard.gov/investment?buscid=77#
http://www.itdashboard.gov/investment/schedule-summary/77
[44] http://www.itdashboard.gov/investment?buscid=903
http://www.itdashboard.gov/investment/schedule-summary/903
[45] http://www.gdc4s.com/content/detail.cfm?acronym=WIN-T
[46] http://www.itdashboard.gov/investment?buscid=22#
http://www.itdashboard.gov/investment/schedule-summary/22

| | | | | | |
|---|---|---|---|---|---|
| | | | | | で、約 240 のレガシーIT システムを交換、25 万人のユーザをサポートする。 |
| **7** | Electronic Health Record (EHR) Way Ahead[47] | 2009 年 12 月 | 3 億 8,000 万ドル | 3 億 230 万ドル | 既存の電子医療記録システム Armed Forces Health Longitudinal（AFHLT）Technology Application と Composite Health Care System（CHCS）に代わるもので、アクセスとアベイラビリティを強化するほか、他の政府機関と Virtual Lifetime Electronic Record（VLER）経由での情報共有ができるようになる。 |
| **8** | Global Command and Control System - Joint[48] | 1998 年 10 月 | 12 億ドル | 2 億 8,010 万ドル | 米軍の指揮統制システムである汎地球指揮統制システム（Global Command and Control System、GCCS）や、多国籍軍による共同指揮統制（Joint Command and Control、JC2）におけるリアルタイム監視機能を介した戦略の策定及び遂行などをサポートする。 |
| **9** | JTRS（Joint Tactical Radio System） - Groung Mobile Radios[49] | 2002 年 5 月 | 69 億ドル | 2 億 6,840 万ドル | コスト管理とリスク削減のために、陸軍、海軍、海兵隊などの次世代戦略車両用の無線通信システム（JTRS）を開発する。 |
| **10** | Global Combat Support System - Army[50] | 2004 年 1 月 | 7 億 6,370 万ドル | 2 億 5,650 万ドル | 米陸軍の兵士にタイムリーで信頼できる情報を提供する目的で、物資供給、メインテナンス作業、ロジスティック管理などを簡易化・自動化するソリューションを開発する。 |

**＜DISN について＞**

DISN（Defense Information System Network）とは、音声、IP データ、映像の各種電子情報を、DoD が世界中に持つオフィス・部署・部隊間で交信するための通信ネットワークであり、非機密情報をやり取りするための NIPRNet（Non-secure Internet Protocol Router Network）と、機密情報をやり取りするための SIPRNet（Secure Internet

[47] http://www.itdashboard.gov/investment?buscid=924#
http://www.itdashboard.gov/investment/schedule-summary/924
[48] http://www.itdashboard.gov/investment?buscid=31#
http://www.itdashboard.gov/investment/schedule-summary/31
[49] http://www.itdashboard.gov/investment?buscid=64
http://www.itdashboard.gov/investment/schedule-summary/64
[50] http://www.itdashboard.gov/investment?buscid=59#

Protocol Router Network）により構成されている[51]。DISN は、軍隊の指揮系統における C4I（Command, Control, Communications, Computers and Intelligence（指揮、統制、通信、コンピュータ、情報）[52]の各分野を包括する通信インフラとして位置付けられており、C4I インフラなどと呼ばれることもある。

DISN 構築プロジェクトは、1991 年から長期にわたって続けられており、情報化社会における国防作戦をサポートするための基幹プロジェクトとして、総額 482 億ドルの投入が予定されている。2011 年 12 月時点でプロジェクト全体の約 37%が完了しており、現在基幹ネットワークの光回線のアップグレードなどが集中的に行われているとのことである[53]。

**＜NGEN について＞**

NGEN（Next Generation Enterprise Network）は、米国海軍および海兵隊向けの新規イントラネットのことを指し、2010 年まで利用されていたイントラネットである Navy Marine Corps Intranet（NMCI）を置き換えることを目指している。上述の DISN はインターネットと接続される仕組みになっているのに対して、NGEN は海軍・海兵隊内部のネットワークという位置付けであり、作戦などの遂行において重要な情報を、職員間で安全に交信するための通信環境を提供することを目的としている[54]。NGEN 構築プロジェクトは 2008 年に開始され、2014 年の完了が予定されている。

**＜I3MP について＞**

I3MP（Installation Information Infrastructure Modernization Program）は、米国陸軍のイントラネットを近代化するためのプロジェクトであり、特にネットワークスイッチ、ルータ、ケーブル、交換スイッチなど、陳腐化しつつあるネットワークのハードウェアを更新することを目的としている[55]。音声、映像、データの各種情報を安全かつ迅速にやり取りできるネットワークインフラを提供することで、DoD が目指す「柔軟」または「身軽」な軍隊への転換に貢献するものと位置付けられている[56]。I3MP は 2007 年に開始され、2018 年に完了することが予定されている。

これらとは別に、DoD 関連で特記すべき IT 関連の活動は以下の通り。

---

[51] http://articles.janes.com/articles/Janes-C4I-Systems/Defense-Information-System-Network-DISN-United-States.html

[52] 軍隊の指揮・統制において欠かせない情報を、コンピュータを用いて通信し、効果的な意思決定に役立てるプロセスを指す。
http://www.c4i.org/whatisc4i.html

[53] http://www.itdashboard.gov/investment/schedule-summary/27
http://www.itdashboard.gov/investment?buscid=27#

[54] http://chips.navy.mil/ContentView.aspx?ID=588

[55] http://www.itdashboard.gov/investment?buscid=53#

[56] http://www.itdashboard.gov/investment?buscid=53#

### サイバー軍

DoD では、サイバー空間での脅威に対応するための専門部署として、2010 年 5 月にサイバー軍（Cyber Command）が設置されている。サイバー軍は 2009 年から設立準備が行われてきたもので、サイバー空間における軍事的活動よりも、NSA と協働しつつ、各軍の重要インフラの統合的な防御能力を高めるミッションをもつとの報道もなされている[57]。サイバー軍に対する 2011 年度、2012 年度予算額は約 32 億ドル程度であり[58]、人材を重視するという方針からか、その予算の「大半」は人件費、次いで多くの金額が IT システムの強化に費やされているとのことである[59]。

### NSA（国家安全保障局）

DoD の傘下局であり、米国連邦政府の国防体制において重要な役割（米国外における機密信号・情報の傍受・解読）を果たす NSA の予算は機密情報とされており、一切公開されていない。報道によると、NSA は以下のような IT 関連プロジェクトに取り組んでいるとされている。

**＜Echelon＞**

Echelon とは、欧州議会（European Parliament）や一般大衆によってその存在が指摘されている、シギント（SIGINT、通信、電波などの傍受による諜報活動の意）用の通信傍受システムのことを指し、現在米国、英国、カナダ、オーストラリア、ニュージーランドの 5 政府が世界各地に持つ軍事施設において、同システムを用いた広範に渡る諜報活動が行われているという。Echelon の存在は公式には認められていないものの、欧州議会の報告によると、電話、ファックス、インターネット通信など、一般的に考え得るあらゆる通信手段を傍受可能な能力を持っているとされている[60]。

**＜Turbulence＞**

Echelon と並ぶ傍受システムとして、NSA が独自に遂行中とされる Turbulence と呼ばれるプロジェクトの存在が、一部の報道機関によって指摘されている[61]。本プロジェクトも同様に公式には認められていないものの、報道記事によると、Turbulence の内容は「インターネット上でやり取りされる電子メール、掲示板上の書き込みなどといった情報を収集し、テロリズムの脅威に関わる情報を洗い出すこと」とのことである[62]。報道のあった 2008 年時点では、毎年度約 5 億ドルが同プロジェクトに投じられていたとの情

[57] http://www.armytimes.com/news/2010/05/military_cyber_command_052110/
[58] http://www.defense.gov/news/newsarticle.aspx?id=61014
[59] http://www.defense.gov/news/newsarticle.aspx?id=63205
[60] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN
[61] http://www.chron.com/news/nation-world/article/Glitches-plague-NSA-s-effort-to-track-terrorists-1826445.php
http://articles.baltimoresun.com/2007-02-11/news/0702110034_1_turbulence-cyberspace-nsa
[62] http://articles.baltimoresun.com/2007-02-11/news/0702110034_1_turbulence-cyberspace-nsa/2

報もあり、実在するとすれば、Turbulence は相当規模の傍受活動を行っているものと考えられる。

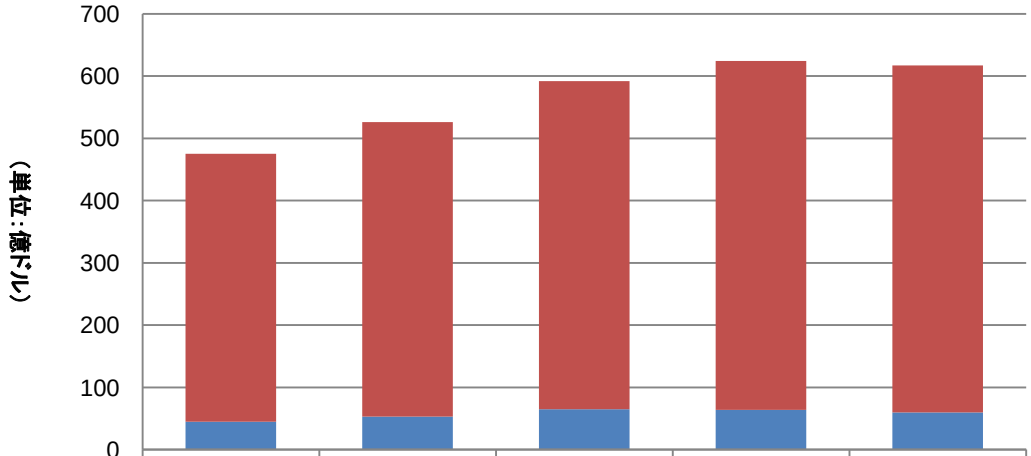
**＜Perfect Citizen＞**

Wall Street Journal 紙の報道によると、2010 年より、NSA は総額 1 億ドル規模の Perfect Citizen と称されるプロジェクトに取り組んでいるという[63]。具体的には、電力、交通システムなど、国内の重要インフラを担う一般企業の IT ネットワーク上に、不正アクセスを探知するための機器などを設置することが想定されているようであるが[64]、その詳細は明確になっていない。

### (3) DHS（国土安全保障省）

過去 5 年間の DHS に対する予算額の推移は以下の通り。総予算額は 2011 年度を除き毎年度上昇している中で、同省についても、IT 予算額はほぼ横ばい状況となっている。

**【図表 5: DHS の過去 5 年間の総予算額と IT 予算額[65]】**




| | 2007年 | 2008年 | 2009年 | 2010年 | 2011年 |
|---|---|---|---|---|---|
| 総予算額 | 430 | 473 | 527 | 560 | 557 |
| IT予算額 | 45 | 53 | 65 | 64 | 60 |

[63] http://www.theregister.co.uk/2010/07/08/perfect_citizen/

[64] http://www.pcworld.com/businesscenter/article/200706/nsa_perfect_citizen_raises_big_brother_concerns_in_private_sector.html

[65] http://www.itdashboard.gov/content/analysis
http://www.dhs.gov/xlibrary/assets/budget_fy2009.pdf
http://www.dhs.gov/xlibrary/assets/budget_bib_fy2011.pdf
http://www.gpoaccess.gov/usbudget/fy11/pdf/budget/homeland.pdf
http://www.dhs.gov/xlibrary/assets/budget-bib-fy2012.pdf
http://www.dhs.gov/xlibrary/assets/budget_bib_fy2011.pdf

次に、DHS の IT 関連プロジェクトについて表記する。2011 年度に多くの予算が投入されているプロジェクトとしては、税関国境警備局（Customs and Border Protection、CBP）、移民局（US Citizenship and Immigration Services、USCIS）、運輸保安局（Transportation Security Administration、TSA）、移民税関捜査局（Immigration and Customs Enforcement、ICE）など、国境の警備や入国管理を担当する傘下局の IT インフラを強化する目的のもの、および国家サイバーセキュリティ部門（National Cyber Security Division、NCSD）のサイバーセキュリティシステム強化を目指すものが多くなっている。このうち、最近連邦政府が重視しているサイバーセキュリティ分野の関連プロジェクトとして、NCPS を別途紹介する。

**【図表 6：DHS の IT 関連プロジェクトのトップ 10（2011 年度予算額ベース）】**

| | プロジェクト名 | 開始時期 | 予算総額 | 2011 年度予算総額 | 概要 |
|---|---|---|---|---|---|
| **1** | CBP - Infrastructure[66] | 2004 年 8 月 | 60 億ドル | 5 億 6,310 万ドル | 税関国境警備局（Customs and Border Protection、CBP）の IT システムの中核を成す CBP インフラをアップグレードし、無線通信、音声通話、ビデオ通信、データセンタ、ヘルプデスク、電子メール、ネットワーク、デスクトップ、シングルサインオンなどの運営をサポート。 |
| **2** | USCIS - Transformation[67] | 2007 年 10 月 | 8 億 7,560 万ドル | 3 億 490 万ドル | 移民局（US Citizenship and Immigration Services、USCIS）の書類申請プロセスの正確性やカスタマーサービスの確実性を向上するために、各種サービスのオンライン化や電子化を進める。また、同局の有するデータを他の連邦政府機関と電子的に共有できるようにする。 |
| **3** | TSA - Information Technology Infrastructure Program (ITIP)[68] | 2002 年 8 月 | 36 億ドル | 2 億 9,570 万ドル | 運輸保安局（Transportation Security Administration、TSA）のサービスを向上させるために、IT インフラの包括的なアップグレードを行う。具体的には、PC、デスクトップアプリケーション、ローカルエリア・広域ネットワーク、データセンタ、ヘルプデスク、無線・情報セキュリティ、 |

[66] http://www.itdashboard.gov/investment?buscid=311
http://www.itdashboard.gov/investment/schedule-summary/311
[67] http://www.itdashboard.gov/investment?buscid=319
http://www.itdashboard.gov/investment/schedule-summary/319
[68] http://www.itdashboard.gov/investment?buscid=174
http://www.itdashboard.gov/investment/schedule-summary/174

| | | | | | |
|---|---|---|---|---|---|
| | | | | | などを強化する。 |
| **4** | ICE - IT Infrastructure (Atlas)[69] | 2006 年 10 月 | 41 億ドル | 2 億 4,220 万ドル | 移民税関捜査局（Immigration and Customs Enforcement、ICE）の IT インフラ（ネットワーク、電子メール、ヘルプデスク、データセンタ、デスクトップ、サイト、ビデオ、音声通話、無線、シングルサインオン）のアップグレードに向け投資する。 |
| **5** | NPPD - National Cybersecurity Protection System (NCPS)[70] | 2008 年 1 月 | 22 億ドル | 1 億 7,600 万ドル | National Cyber Security Division（NCSD）の国家サイバーセキュリティ保護システム（National Cybersecurity Protection System、NCPS）は、連邦政府のサイバーセキュリティインフラを監視し、不正アクセスや攻撃から保護する。 |
| **6** | CBP - Automated Commercial Environment / International Trade Data System (ACE / ITDS)[71] | 2001 年 8 月 | 45 億ドル | 1 億 4,780 万ドル | 税関国境警備局（Customs and Border Protection、CBP）は、海外からの不法商品の侵入を阻止するために、国際貿易データ（International Trade Data）を収集する自動商業環境システム（Automated Commercial Environment、ACE）を導入する。 |
| **7** | TSA - TSA Operating Platform (TOP)[72] | 2002 年 10 月 | 17 億ドル | 1 億 2,050 万ドル | 国家安全保障関連情報など TSA の業務に係る情報の収集及び配布するための TSA 運営プラットフォーム（TSA Operating Platform）をアップグレードする。 |
| **8** | CBP - Non-Intrusive Inspection (NII) Systems Program[73] | 2002 年 10 月 | 23 億ドル | 1 億 1,380 万ドル | CBP による兵器、不法放射性物質、麻薬、貨幣などの密輸探知をサポートする非開扉検査システム（Non-Intrusive Inspection Systems Program）について、国内の入国地や国際郵便処理施設のける技術や設備をアップグレードする。 |

[69] http://www.itdashboard.gov/investment?buscid=138
http://www.itdashboard.gov/investment/schedule-summary/138
[70] http://www.itdashboard.gov/investment?buscid=145
http://www.itdashboard.gov/investment/schedule-summary/145
[71] http://www.itdashboard.gov/investment?buscid=314
http://www.itdashboard.gov/investment/schedule-summary/314
[72] http://www.itdashboard.gov/investment?buscid=169
http://www.itdashboard.gov/investment/schedule-summary/169
[73] http://www.itdashboard.gov/investment?buscid=389
http://www.itdashboard.gov/investment/schedule-summary/389

| | | | | | |
|---|---|---|---|---|---|
| **9** | USCIS - Infrastructure (End User Support)[74] | 2000 年 10 月 | 8 億 6,860 万ドル | 1 億 1,140 万ドル | USCIS 用 IT インフラのアップグレード。具体的には、全国 300 ヵ所の USCIS オフィスを対象とした IT ヘルプデスク及び IT 機器の修理を担当する技術支援センター（Technical Assistance Center）の設立、IT ハードウェアの供給、WAN・LAN ネットワークの遠隔モニタリングサービスの導入など。 |
| **10** | USCG - Rescue 21[75] | 1995 年 10 月 | 24 億ドル | 1 億 120 万ドル | 米国沿岸警備隊（United States Coast Guard、USCG）向けの国内海岸線約 3 万 6,000 マイルに亘る監視・生命保護システム「Rescue 21」の導入。同システムは、無線通信機、アンテナ用鉄塔、相互接続無線ネットワークで構成されており、既存のレガシー「National Distress and Response System」に代わって導入される。 |

**＜IT インフラ更新・近代化＞**

DHS において最近多くの予算が投じられている IT 関連プロジェクトの大半は、DHS 傘下局の IT インフラを更新する内容のものであり、上表の CBP – Infrastructure、USCIS – Transformation、ITIP、Atlas などは、音声、データ、映像など各種電子情報のコンバージェンスを実現するといった、ほぼ同様の内容になっていることがわかる。DoD でも同様のプロジェクトが予算額ベースで上位を占めていることから、国防関連省庁全体で、通信インフラの近代化が重要課題となっていることがわかる。

**＜NCPS について＞**

NCPS（National Cybersecurity Protection System）とは、一般的に Einstein とも呼ばれ、連邦政府の IT ネットワークをモニタリングすることで、第 3 者からの不正アクセスや攻撃などを探知・防止するためのソフトウェアを指す[76]。Einstein プロジェクトは、元来 DHS 傘下の US-CERT（United States Computer Emergency Readiness Team）によって開始されたものであり[77]、プロジェクト終了の 2018 年までに、Einstein の機能が段階的に強化される予定となっている。例えば、現在 Einstein は連邦政府のネットワーク

[74] http://www.itdashboard.gov/investment?buscid=323
http://www.itdashboard.gov/investment/schedule-summary/323
[75] http://www.itdashboard.gov/investment?buscid=193
http://www.itdashboard.gov/investment/schedule-summary/193
[76] http://hsni2010.com/Presentation/RandyVickers.pdf
[77] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf

上にのみ実装されているが、将来的には民間 ISP のネットワーク上にも配置された上で、攻撃者をあらかじめ駆逐するような機能の導入も検討されているとのことである[78]。

なお、Einstein プロジェクトを開始した US-CERT とは、2003 年 9 月設立の組織であり、民間 IT 企業などと連携し、サイバー空間における最新の脅威についての情報や、IT 利活用のベストプラクティスといった情報を一般提供している[79]。また、US-CERT は、ICS-CERT（Industrial Control Systems Cyber Emergency Response Team）と呼ばれる DHS 傘下組織と連携し、特に重要インフラの制御系に関する脅威の情報やベストプラクティスも公開しており[80]、サイバー攻撃対策においては官民の連携が特に重要であるとの認識のもと、攻撃の脅威を最低限に留めるべく取り組んでいる。

### (4) CIA（中央情報局）

CIA の予算は機密情報とされており、一般公開されていない。以下では、一般メディアによる報道をもとに、CIA が行っている IT 関連プロジェクトについて紹介する。

**＜ソーシャルメディア監視＞**

一部メディアの報道によると、現在、CIA は各種ソーシャルメディア（Facebook、Twitter、ブログ上の投稿など）を常時監視する取り組みを行っているという[81]。ソーシャルメディアを監視するプロジェクトは、2009 年頃から本格化されており、現在の主要な役割は、「特定の出来事やニュースについて、外国の一般大衆がどのように反応しているか分析すること」とされている[82]。最近の例として、2011 年のオサマ・ビンラディン氏暗殺作戦に対する、周辺国・地域の人々の意見や心情などにソーシャルメディア分析が利用されたという。現在、CIA では、分析に利用されるソフトウェアの機能向上に取り組んでいるとされており、将来的には、特定の出来事に対する反応だけでなく、一般世論における意見形成の恒常的なモニタリングにもソーシャルメディア分析が利用されることが目指されている。

**＜ビッグデータ解析＞**

報道によると、CIA は、傘下のベンチャー投資企業である In-Q-Tel 社を通して、安全保障関連 IT 活動の一環としていわゆる「ビッグデータ」の解析に注力しつつあると考えられ

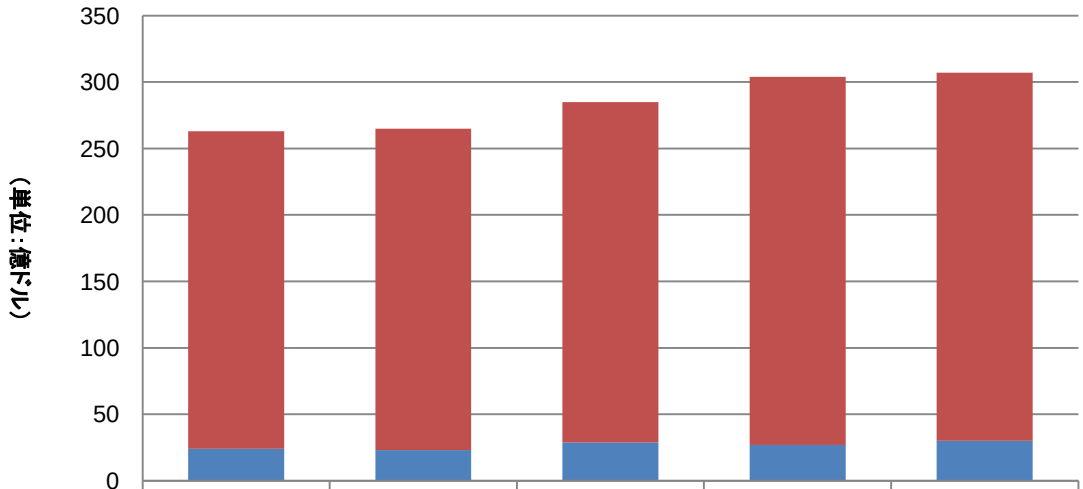
[78] http://articles.cnn.com/2008-10-04/tech/chertoff.cyber.security_1_chertoff-government-cyberspace?_s=PM:TECH
段階的な機能強化に伴い、Einstein 2、Einstein 3 などと呼称が変更されることとなっている。
[79] http://www.us-cert.gov/
[80] http://www.us-cert.gov/control_systems/ics-cert/
[81] http://www.theatlantic.com/technology/archive/2011/11/how-the-cia-uses-social-media-to-track-how-people-feel/247923/
[82] http://www.theatlantic.com/technology/archive/2011/11/how-the-cia-uses-social-media-to-track-how-people-feel/247923/

る[83]。例えば、In-Q-Tel 社は 2011 年 2 月、大量のテキストデータの文脈を解析するソフトウェアを開発する Digital Reasoning 社と業務提携しており[84]、CIA は同社の技術を利用して、世界各地の人員が収集する諜報データを一元的に読み取り、例えば異なる文書間の暗示的な関連性などを発見することを目指しているとされている。

### (5) DoJ（司法省）

DoJ の総予算額は、2007 年度から 2010 年度まで上昇した後、2010 年度から 2011 年度にかけては横ばい状態となっている。IT 予算額については、2009 年度にやや増加した後、2010 年度に減少、2011 年度には再び微増しているが、全般的には過去 5 年間でほぼ同水準となっている。

**【図表 7：DoJ の過去 5 年間の総予算額と IT 予算額[85]】**




| | 2007年 | 2008年 | 2009年 | 2010年 | 2011年* |
|---|---|---|---|---|---|
| 総予算額 | 239 | 242 | 256 | 277 | 277 |
| IT予算額 | 24 | 23 | 29 | 27 | 30 |

次に、DoJ の IT 関連プロジェクトは、以下の表の通りとなっている。2011 年度の予算額ベースで上位を占めるプロジェクトの大半は、FBI の IT システムに関わるものであり、司法に関する多種多様な省庁を傘下に置く DoJ の中でも、犯罪捜査を目的としたプロジェクトに多くの予算が投じられていることがわかる。特に、個人の認証や監視に使われる仕

[83] http://gigaom.com/cloud/digital-reasoning-gets-more-dough-for-big-data-intelligence-push/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+OmMalik+%28GigaOM%3A+Tech%29&utm_content=Google+Reader
[84] http://www.iqt.org/news-and-press/press-releases/2011/Digital-Reasoning.html
[85] http://www.itdashboard.gov/content/analysis
http://www.justice.gov/jmd/2012summary/pdf/authority.pdf

組みに関するプロジェクトが目立っており、その中でも国防体制との関連性が高い NGI および TSS について紹介する。

**【図表 8:DoJ の IT 関連プロジェクトのトップ 10（予算額ベース）】**

| | プロジェクト名 | 開始時期 | 予算総額 | 2011 年度予算総額 | 概要 |
|---|---|---|---|---|---|
| 1 | FBI Next Generation Identification (NGI)[86] | 2005 年 5 月 | 12 億ドル | 2 億 2,310 万ドル | FBI の既存の生体認証システムである指紋自動認証（Integrated Automated Fingerprint Identification System、IAFIS）システムから、次世代認証（Next Generation Identification、NGI）システムへの移行に伴い、NGI システムの運営及びメンテナンスコストをカバーするプログラム。 |
| 2 | JMD Unified Financial Management System (UFMS)[87] | 2001 年 10 月 | 8 億 4,200 万ドル | 1 億 3,730 万ドル | 統合財務管理システム（unified financial management system、UFMS）の導入により、司法省における財務管理や資金調達業務の効率化を図る。 |
| 3 | FBI Prevention of Information Technology Obsolescence (PITO) [88] | 2004 年 10 月 | 5 億 2,000 万ドル | 9,100 万ドル | FBI の IT 老朽化防止プログラム（Prevention of Information Technology Obsolescence）は、同局にデスクトップ PC、ノート型 PC、プリンター・コピー機、ソフトウェアサポート、などを刷新する。 |
| 4 | FBI Data Centers[89] | 2006 年 10 月 | 6 億 3,800 万ドル | 6,210 万ドル | FBI のデータセンタプロジェクト（Data Centers Project）とは、①演算装置、データ保管装置、などの運営・維持、②演算装置、OS、データ保管装置などの近代化、③既存のハードウェアの増強、④自動テープライブラリ、チャンネル拡張、バックアップソリューションの開発、などを実施するもので、FBI 業務の紙ベースから |

[86] http://www.itdashboard.gov/investment?buscid=938
http://www.itdashboard.gov/investment/schedule-summary/938
[87] http://www.itdashboard.gov/investment?buscid=426
http://www.itdashboard.gov/investment/schedule-summary/426
[88] http://www.itdashboard.gov/investment?buscid=440
http://www.itdashboard.gov/investment/schedule-summary/440
[89] http://www.itdashboard.gov/investment?buscid=859
http://www.itdashboard.gov/investment/schedule-summary/859

| | | | | | |
|---|---|---|---|---|---|
| | | | | | 電子ベースの移行を支えるプロジェクトである。 |
| **5** | FBI Data Integration and Visualization System (DIVS)[90] | 2007 年 10 月 | 5 億 7,130 万ドル | 5,320 万ドル | FBI のデータ統合・仮想化システム（Data Integration and Visualization System、DIVS）は、FBI の捜査員、分析専門家や言語学者による捜査活動を支援し、米国を海外のテロリストや諜報機関から保護するためのプロジェクトで、FBI が収集したデータ及び FBI に提供されたデータを保管・提供する役割を果たす。DIVS プログラムでは、収集するデータの拡大、テロリストに関するデータ収集能力の強化、などが実施されている。 |
| **6** | FBI SENTINEL[91] | 2004 年 10 月 | 6 億 480 万ドル | 5,260 万ドル | SENTINEL とは、FBI の法執行及び諜報活動をサポートするウェブベースの事案（ケース）管理システムであり、FBI の情報共有（FBI 内部、法執行機関、諜報機関）、検索、分析能力の向上が目指されている。 |
| **7** | FBI Terrorist Screening System (TSS)[92] | 2007 年 10 月 | 3 億 8,490 万ドル | 4,860 万ドル | テロリストスクリーニングシステム（Terrorist Screening System、TSS）とは、国際機関、連邦政府及び地方政府向けに、テロリストに関する情報の特定、認識などを行う IT システムである。 |
| **8** | FBI Law Enforcement National Data Exchange Program (NDEx)[93] | 2001 年 10 月 | 5 億 7,120 万ドル | 4,330 万ドル | FBI 法執行関連国家データ交換プログラム（NDEx）とは、法執行機関向けの刑事司法関連データの収集及び処理するためのソリューションを提供するもの。同プログラムのアップグレードでは、Google のような検索機能のほか、保護観察及び執行猶予期間 |

[90] http://www.itdashboard.gov/investment?buscid=429
http://www.itdashboard.gov/investment/schedule-summary/429
[91] http://www.itdashboard.gov/investment?buscid=441
http://www.itdashboard.gov/investment/schedule-summary/441
[92] http://www.itdashboard.gov/investment?buscid=442
http://www.itdashboard.gov/investment/schedule-summary/442
[93] http://www.itdashboard.gov/investment?buscid=434
http://www.itdashboard.gov/investment/schedule-summary/434

| | | | | | |
|---|---|---|---|---|---|
| | | | | | に関するデータ、ウェブサービス全体の拡張といった機能が追加されている。 |
| **9** | FBI Digital Collection[94] | 2003 年 10 月 | 5 億 7,270 万ドル | 4,180 万ドル | FBI Digital Collection プロジェクトとは、テロリストからの攻撃、海外の諜報機関によるスパイ行為、さらに国内での犯罪行為から米国を保護する目的で、FBI による諜報及び証拠の入手をサポートするシステム。具体的には、電話機、マイクロフォン、ファックスから証拠となる音声情報を収集する電子監視システム（electronic surveillance systems）を提供する。 |
| **10** | FBI Top Secret/Sensitive Compartmented Information Operational Network (SCION)[95] | 2004 年 10 月 | 6 億 4,920 万ドル | 3,970 万ドル | 重要機密情報運営ネットワーク（Top Secret/Sensitive Compartmented Information Operational Network：SCION）とは、重要機密情報を処理、送信、保管するための FBI 専用のネットワークである。SCION を通じて、FBI は他の連邦政府機関の諜報コミュニティと情報共有や連携ができるようになる。 |

**＜NGI について＞**

NGI とは、FBI が持つ個人認証システムを近代化するためのプロジェクトを指し、特に生体認証に関わるシステムの機能性強化を目指している。具体的には、現在主に使用されている生体情報である指紋に加えて、虹彩、顔面、あざ、刺青などの生体情報も活用できるシステムが開発されており、これによって米国内におけるテロ活動や、重大犯罪などの捜査がより効率化されることが期待されている[96]。

**＜TSS について＞**

TSS とは、FBI が統括し、DHS、DoD、CIA などが参画する省庁横断型組織である Terrorist Screening Center（TSC）をサポートする IT システムを指す。同システムは、かつて各連邦省庁が個別に管理していたテロリスト名簿を統合し、連邦政府、国際組織、

[94] http://www.itdashboard.gov/investment?buscid=430#
http://www.itdashboard.gov/investment/schedule-summary/430
[95] http://www.itdashboard.gov/investment?buscid=443
http://www.itdashboard.gov/investment/schedule-summary/443
[96] http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi

州政府、地方政府などに、これらのテロリストを識別するための個人情報を提供することを可能としている[97]。

### (6) その他の省庁の動向

上記の主要省庁以外にも、国防目的の IT プロジェクトを遂行中の連邦省庁がいくつか存在する。一例として、 DoE（エネルギー省）が傘下の研究施設 Idaho National Laboratory（INL、アイダホ国立研究所）を通して行う National SCADA Test Bed プログラムが挙げられる[98]。これは、エネルギー施設など、重要産業施設の制御システムをサイバー攻撃から防護することを目的に、制御システムに対する攻撃のシミュレーションを行ったり、制御システム堅牢化についての教育プログラムなどを提供する取り組みである。今後サイバー空間における脅威が増大すると指摘されている中で、このように特定の分野に特化した国防関連 IT プロジェクトも本格化していることがわかる。

### (7) 米国の主要国防関連企業のプロジェクト

次に、国防における IT 利活用のもう一つの側面として、主要国防関連企業が近年受注した大規模プロジェクトについて紹介する。これらの企業には、従来からの軍需業界大手である Lockheed Martin 社、Boeing 社、Northrop Grumman 社、General Dynamics 社、Raytheon 社はもちろんのこと、Hewlett-Packard 社、Honeywell 社、General Electric 社など IT 機器や重機の開発を主要業務としていた企業も、有力な発注先として含まれる。

**【図表 9: 米国の主要国防関連企業と最近の主要受注プロジェクト】**

| 企業名 | 国防に関する IT 関連プロジェクト | 受注年月 | 受注額 | 発注元 |
|---|---|---|---|---|
| **Lockheed Martin 社** | 米陸軍用無人戦闘機用の合成開口レーダーの開発[99] | 2007 年 5 月 | 4,000 万ドル | U.S. Army |
| | 米空軍・宇宙ミサイルシステムセンタ向け衛星通信リアルタイム天気情報システムのサポート[100] | 2007 年 6 月 | 4,700 万ドル | Air Force Space Command、及び、Space and Missile Systems Center |
| | FBI の指紋認証用 PC のサーバ機器のアップデート[101] | 2007 年 9 月 | 1,600 万ドル | Federal Bureau of Investigation |
| | DoD 傘下 Defense Media Activity のネットワークインフラ、通信機器、 | 2008 年 10 月 | 5,900 万ドル | Office of the Secretary of Defense |

[97] http://www.justice.gov/jmd/2011justification/exhibit300/fbi-2011-tss.pdf
[98] http://www.inl.gov/scada/
[99] http://www.lockheedmartin.com/news/press_releases/2007/LockheedMartinAwarded40MillionRadar.html
[100] http://www.lockheedmartin.com/news/press_releases/2007/LockheedMartinAwardedContractFromAi.html
[101] http://www.lockheedmartin.com/news/press_releases/2007/CJISSuperdome.html

| | | | | |
|---|---|---|---|---|
| | 電源システムなどの総合的な IT サポート[102] | | | |
| | 個人認証及びサイバーセキュリティ強化のための軍事用ネットワークプロトコルの開発[103] | 2009 年 10 月 | 3,100 万ドル | Defense Advanced Research Projects Agency |
| | 米空軍・航空機動空軍（Air Mobility Command）基地の IT インフラサポート[104] | 2010 年 10 月 | 6,500 万ドル | U.S. Air Force Air Mobility Command (AMC) Directorate of Logistics |
| | 米海軍用攻撃型ヘリコプタ「AH-1Z Cobra」の射撃制御システムの開発[105] | 2011 年 12 月 | 3,060 万ドル | Naval Surface Warfare Center |
| **Boeing 社** | 米空軍研究所からの Boeing 社が開発したガイダンス統合信管（Guidance Integrated Fuzing: GIF）技術の効果を実証。GIF 技術により、統合両用航空支配ミサイル（Joint Dual Role Air Dominance Missile）の小型化・軽量化が実現する[106] | 2008 年 5 月 | 520 万ドル | Air Force Research Laboratory (AFRL) |
| | 低コストのレーダー訓練を、米海軍の海軍兵生（Undergraduate Military Flight Officer）向けの訓練システム（T-45 Training System）に統合するための仮想ミッション訓練システム（Virtual Mission Training System）改修キットを開発[107] | 2009 年 2 月 | 2,830 万ドル | U.S. Navy |
| | 米海軍の戦闘機「Super Hornet」の射撃標準機能を向上させる分散型標準システム（Distributed Targeting system）の開発[108] | 2009 年 5 月 | 4,890 万ドル | U.S. Navy |
| | 米国空軍の無人戦闘機「QF-16（Drone）」の開発（第 1 段階）[109] | 2010 年 3 月 | 6,970 万ドル | U.S. Air Force |

[102] http://www.lockheedmartin.com/news/press_releases/2008/1028_ess-defense-media-activity.html
[103] http://www.lockheedmartin.com/news/press_releases/2009/101509-CyberInfoAssurance.html
[104] http://www.lockheedmartin.com/news/press_releases/2010/10-29-air-mobility-command.html
[105] http://www.lockheedmartin.com/news/press_releases/2011/MFC_120511_LMAwardedContracts30.6MillionTSS.html
[106] http://www.boeing.com/news/releases/2008/q2/080516a_nr.html
[107] http://boeing.mediaroom.com/index.php?s=43&item=532
[108] http://boeing.mediaroom.com/index.php?s=43&item=672
[109] http://boeing.mediaroom.com/index.php?s=43&item=1109

| | | | | |
|---|---|---|---|---|
| | 米空軍の空中給油機「59-jet KC-10」のコクピットの通信・ナビゲーション・監視及び航空管制システム（CNS/ATM System）をアップグレード[110] | 2010 年 6 月 | 2 億 1,600 万ドル | U.S. Air Force |
| | 米空軍の「B-5」爆撃機用アビオニクス（航空電子工学）ソフトウェアのアップグレード[111] | 2011 年 10 月 | 5,700 万ドル | U.S. Air Force |
| **Northrop Grumman 社** | DoD の Office of the Secretary of Defense にヘルプデスクサービス、サーバー管理、ネットワーク・セキュリティエンジニアリング、などの総合 IT サービスを提供[112] | 2007 年 3 月 | N/A | U.S. Department of Defense |
| | 米空軍用の無人戦闘機「Global Hawk」シリーズの最新版で強化型統合センサ（Enhanced Integrated Sensor）搭載の「Block 30」及び「Block 40」の開発[113] | 2009 年 11 月 | 3 億 290 万ドル | U.S. Air Force |
| | 米軍及び多国籍軍の戦闘機間の通信セキュリティを強化する暗号化装置の開発[114] | 2010 年 8 月 | 3 億ドル | U.S. Army |
| | 米海軍の潜水艦のデータベース管理、近代化、エンジニアリング、インターフェース、設計などの総合サポート[115] | 2010 年 10 月 | 1 億 200 万ドル | U.S. Navy |
| | 米海軍の戦艦「USS San Antonio」向けのエンジニアリング、システム統合、IT サポートなどの総合 IT サービス[116] | 2010 年 11 月 | 4,370 万ドル | U.S. Navy |
| | 米国空軍の戦闘機「28 C-130J」及び「24 C-17」用の状況認識システム「Dynamic Re-tasking Capability （DRC）Urgent Operational Need（UON）」の開発[117] | 2011 年 7 月 | 6,500 万ドル | U.S. Air Force |

[110] http://boeing.mediaroom.com/index.php?s=43&item=1273
[111] http://boeing.mediaroom.com/index.php?s=43&item=1993
[112] http://www.irconnect.com/noc/press/pages/news_releases.html?d=115671
[113] http://www.irconnect.com/noc/press/pages/news_releases.html?d=178846
[114] http://www.irconnect.com/noc/press/pages/news_releases.html?d=199674
[115] http://www.irconnect.com/noc/press/pages/news_releases.html?d=203252
[116] http://www.irconnect.com/noc/press/pages/news_releases.html?d=207997
[117] http://www.irconnect.com/noc/press/pages/news_releases.html?d=226551

| | | | | |
|---|---|---|---|---|
| **General Dynamics 社** | 米海兵隊による法人向けホスティングサービスを提供する IT センタの設計及び建設[118] | 2009 年 1 月 | 9,500 万ドル | U.S. Marine Corps |
| | 米欧州陸軍のシステムエンジニアリング、ネットワーク統合・調整、戦闘指揮システムサポート、IT ノレッジ管理、Microsoft SharedPoint サポート、ビデオ会議及びウェブサイト開発などの総合 IT サポート[119] | 2011 年 1 月 | 1 億 2,200 万ドル | U.S. Army Europe |
| | 米陸軍のミサイル防御庁のプログラム管理サポート、インフラ管理、施設管理などの総合インフラサービス[120] | 2011 年 4 月 | 5 億 6,500 万ドル | Missile Defense Agency |
| | 米特殊作戦軍（USSOCOM）のデータ、音声通話、ビデオ通話を管理する IT ネットワークのサポートなどの総合 IT サポート[121] | 2011 年 5 月 | 8,360 万ドル | U.S. Special Operations Command（USSOCOM） |
| **Raytheon 社** | 米空軍の戦闘機同士のリアルタイム通信システム「Distributed Common Ground System (DCGS) Integration Backbone (DIB)1.3」の開発[122] | 2008 年 5 月 | N/A | U.S. Air Force |
| | DoD 傘下の国家地球空間情報局（NGA）のコンピュータネットワークの総合セキュリティサービス（2005 年に開始されたサービスの契約を一年延長したもの：受注総額は 8,870 万ドル）[123] | 2010 年 9 月 | 3,000 万ドル | National Geospatial-Intelligence Agency（NGA） |
| | 米空軍の無人戦闘機「Global Hawk」用の地上制御局のサポート[124] | 2011 年 6 月 | 2,470 万ドル | U.S. Air Force |
| | 米海軍の戦艦及び潜水艦用の GPS・タイミングサービス向けのデータホスティングソリューション Global Positioning System-based Positioning Navigation and Timing Service（GPNTS）の開発[125] | 2011 年 8 月 | 3,200 万ドル | U.S. Navy |

[118] http://www.generaldynamics.com/news/press-releases/detail.cfm?customel_dataPageID_1811=6457
[119] http://www.generaldynamics.com/news/press-releases/detail.cfm?customel_dataPageID_1811=14691
[120] http://www.generaldynamics.com/news/press-releases/detail.cfm?customel_dataPageID_1811=16579
[121] http://www.generaldynamics.com/news/press-releases/detail.cfm?customel_dataPageID_1811=16679
[122] http://raytheon.mediaroom.com/index.php?s=43&item=1002
[123] http://raytheon.mediaroom.com/index.php?s=43&item=1657
[124] http://raytheon.mediaroom.com/index.php?s=43&item=1850
[125] http://raytheon.mediaroom.com/index.php?s=43&item=1888

| | | | | |
|---|---|---|---|---|
| **SAIC 社** | 米海軍水上戦センターの海上・航空戦闘用情報活動のエンジニアリング、プログラムミング、などの総合 IT サポート[126] | 2007 年 3 月 | 1 億 2,200 万ドル | U.S. Naval Surface Warfare Center |
| | 米海軍傘下の宇宙・海上戦闘システムコマンド用の次世代ラジオ通信機の開発[127] | 2008 年 4 月 | 4,200 万ドル | Space and Naval Warfare Systems Command |
| | 米陸軍用の軍事車両内のイメージ検査システム（Military Mobile VACIS(R) inspection systems）の開発及びサポート[128] | 2008 年 12 月 | 9,700 万ドル | U.S. Army |
| | 米戦略軍の海上・航空戦闘用情報活動のエンジニアリング、プログラムミング、などの総合 IT サポート[129] | 2009 年 3 月 | 9 億ドル | U.S. Strategic Command（USSTRATCOM） |
| | 米海軍傘下の宇宙・海上戦闘システムコマンドのモデリング、シミュレーション、戦闘分析サポート[130] | 2010 年 1 月 | 2 億 4,900 万ドル | Space and Naval Warfare Systems Command |
| | 米海軍水上戦センターの科学・エンジニアリング分析、テスト、データ管理などの総合 IT サポート[131] | 2011 年 2 月 | 3 億 5,100 万ドル | U.S. Naval Surface Warfare Center |
| | 米国防総省の軍隊関係者向けヘルスケア電子記録システム「TRICARE Management Activity Military Health System」の IT サポート[132] | 2011 年 5 月 | 5300 万ドル | Department of Defense |
| | 米ミサイル防衛庁の弾道ミサイル防衛システムの分析サポート[133] | 2011 年 9 月 | 2 億 8,100 万ドル | U.S. Missile Defense Agency |
| | 米復員軍人援護局のプログラム管理、システム統合、プログラム管理、など総合 IT サービス[134] | 2011 年 9 月 | 12 億ドル | U.S. Department of Veterans Affairs |
| | 米海軍水上戦センターのシステムエンジニアリング及びライフサイクルインテグレーションサービス[135] | 2011 年 9 月 | 3,800 万ドル | U.S. Naval Surface Warfare Center |

[126] http://investors.saic.com/phoenix.zhtml?c=193857&p=irol-newsArticle&ID=973668&highlight=
[127] http://investors.saic.com/phoenix.zhtml?c=193857&p=irol-newsArticle&ID=1125756&highlight=
[128] http://investors.saic.com/phoenix.zhtml?c=193857&p=irol-newsArticle&ID=1439217&highlight=
[129] http://investors.saic.com/phoenix.zhtml?c=193857&p=irol-newsArticle&ID=973668&highlight=
[130] http://investors.saic.com/phoenix.zhtml?c=193857&p=irol-newsArticle&ID=1438863&highlight=
[131] http://investors.saic.com/phoenix.zhtml?c=193857&p=irol-newsArticle&ID=1438845&highlight=
[132] http://investors.saic.com/phoenix.zhtml?c=193857&p=irol-newsArticle&ID=1565867&highlight=
[133] http://investors.saic.com/phoenix.zhtml?c=193857&p=irol-newsArticle&ID=1604251&highlight=
[134] http://investors.saic.com/phoenix.zhtml?c=193857&p=irol-newsArticle&ID=1603672&highlight=
[135] http://investors.saic.com/phoenix.zhtml?c=193857&p=irol-newsArticle&ID=1607136&highlight=

| | | | | |
|---|---|---|---|---|
| **Honeywell 社** | 国防総省、NASA、エネルギー省による先進ガスタービンエンジンプログラム（Versatile Affordable Advanced Turbine Engine）に基づいたガスタービンエンジン技術の開発 | 2009 年 6 月 | 7,000 万ドル | U.S. Air Force |
| | 米空軍に 200 機の GPS ナビゲーション機器を提供[136] | 2010 年 6 月 | 1,630 万ドル | U.S. Air Force |
| | 連邦航空局（FAA）の航空管制システムのセキュリテイシステムの管理・維持[137] | 2011 年 5 月 | 3,800 万ドル | Federal Aviation Administration（FAA） |
| | 米陸軍の車両向けのナビゲーション機器の提供[138] | 2011 年 8 月 | 1 億 4,100 万ドル | U.S. Army |
| **HP 社** | 米国土安全保障省の移民税関捜査局（Immigration and Customs Enforcement）の法執行サポートセンター（Law Enforcement Support Center）の移民ステータス確認プロセスの効率化のためのアプリケーションサービスの提供[139] | 2010 年 5 月 | 4,160 万ドル | Department of Homeland Security |
| | 米空軍のサイバーセキュリティ保護用の Cyber Control System インフラの提供[140] | 2010 年 6 月 | 900 万ドル | U.S. Air Force |
| | 米海軍・海兵隊のイントラネット（Navy Marine Corps Intranet）及び次世代法人向けネットワーク（Next Generation Enterprise Network）上のセキュリティリスクを管理する IT サービス契約の延長[141] | 2010 年 7 月 | 30 億ドル | U.S. Navy |
| | 米航空宇宙局（NASA）職員向けデスクトップ提供及び総合 IT サポート[142] | 2011 年 6 月 | 25 億ドル | National Aeronautics and Space Administration（NASA） |
| **Harris 社** | 米海軍のヘリコプタ「MH-60R」によ | 2007 年 2 月 | 6,600 万ド | U.S. Navy |

[136] http://www.bizjournals.com/tampabay/stories/2010/06/28/daily42.html
[137] http://honeywell.com/News/Pages/Honeywell-Wins-$38-Million-FAA-Contract.aspx
[138] http://www.bizjournals.com/tampabay/news/2011/08/18/honeywell-wins-141m-defense-contract.html
[139] http://www.hp.com/hpinfo/newsroom/press/2010/100524b.html
[140] http://www.esecurityplanet.com/news/article.php/3886616/HP-Lands-Air-Force-Cyber-Defense-Contract.htm
[141] http://www.hp.com/hpinfo/newsroom/press/2010/100708xa.html
[142] http://www.hp.com/hpinfo/newsroom/press/2011/110428a.html

| | | | | |
|---|---|---|---|---|
| | る戦略的映像、レーダー、音声データの高速デジタルデータリンク（Common Data Link）の開発及びテスト[143] | | ル | |
| | 米空軍の衛星基地局管理ネットワーク（Air Force Satellite Control Network）の運営、管理、サポート[144] | 2008 年 10 月 | 6,000 万ドル | U.S. Air Force |
| | 国務省の領事局（Bureau of Consular Affairs）の領事館 270 ヵ所への IT 機器導入、ヘルプデスク、その他総合 IT サービス[145] | 2009 年 10 月 | 1 億 9,650 万ドル | U.S. Department of State, Bureau of Consular Affairs |
| | 米国防総省の物品販売局（Defense Commissary Agency）による世界中に駐在する米兵士への物資提供用の通信ネットワークのインフラサポート・管理・維持[146] | 2010 年 4 月 | 3,500 万ドル | Defense Commissary Agency |
| | 米陸軍資材集団（U.S. Army Materiel Command）の本部移動における IT インフラの導入[147] | 2010 年 11 月 | 7,700 万ドル | National Capital Region Contracting Center |
| | 米空軍州兵（U.S. Air National Guard）の IT システム標準化及び通信インフラのアップグレード[148] | 2011 年 2 月 | 1,500 万ドル | U.S. Air National Guard |
| **General Electric 社** | 国防関連の偵察航空機用の極超音速エンジン（hypersonic engine）の開発[149] | 2010 年 7 月 | 3,170 万ドル | Department of Defense |
| | 米海軍、陸軍、空軍、海兵隊向けの患者モニタリングシステムの開発[150] | 2011 年 1 月 | 4,320 万ドル | Department of Defense |

### (8) まとめ

以上から、現在の国防関連 IT プロジェクトの多くは、通信インフラの更新、情報共有機能の強化が中心となっていることがわかる。これは、省庁間・省庁内での情報共有を効率化することで、刻々と変化する外部環境の状況にいち早くできる、身軽な国防体制を構築するという連邦政府の方針を反映するものであると言える。

[143] http://www.harris.com/view_pressrelease.asp?act=lookup&pr_id=2058
[144] http://www.harris.com/view_pressrelease.asp?act=lookup&pr_id=2563
[145] http://www.harris.com/view_pressrelease.asp?act=lookup&pr_id=2841
[146] http://www.harris.com/view_pressrelease.asp?act=lookup&pr_id=2978
[147] http://www.harris.com/view_pressrelease.asp?act=lookup&pr_id=3121
[148] http://www.harris.com/view_pressrelease.asp?act=lookup&pr_id=3163
[149] http://www.bizjournals.com/cincinnati/stories/2010/07/05/daily14.html
[150] http://www.massdevice.com/news/ge-healthcare-lands-432-million-contract-uncle-sam

また、DoJ、CIA、NSA などの省庁では、個人監視・認証のためのプロジェクトに多くのリソースが投入されており、米国に対する脅威を未然に防ぐための取り組みにおいても、IT は多大な役割を果たしていることがわかる。更に、連邦省庁や重要インフラに対するサイバー攻撃の脅威が高まっていることを受け、国防活動において、IT システム自体が従来の補助的な役割から、主体的な役割を果たす方向性も見え始めている。これに伴って、今後 IT が国防において担う役割は、ますます重要になると考えられる。

## 4. 今後の動向予測

本章では、米国の国防体制において、今後 IT が更に重要な役割を果たすと考えられる分野について考察する。

### (1) 諜報・監視能力の更なる向上

同時多発テロにおいては、事前に連邦政府が攻撃の可能性を把握していながらも、適切な対処がなされなかったとの反省を背景に、米国の国防体制では、攻撃を未然に防ぐための情報収集が重要なトピックとして取り上げられている[151]。このように、攻撃の脅威を未然に防ぐ体制の強化は、(一般的に事前の予測が困難な)テロ攻撃への対策を強化する連邦政府の方針に沿うものであると言える。また、正確な情報の収集は、重点的、効率的な作戦展開に直結するものであり、2010 年版 QDR が掲げる「より柔軟な軍隊」の実現においても重要となってくることが予想される。一方で、今後 10 年間で、DoD に対する予算は総額で約 3,000 億ドル削減される予定となっており、その一環として通常兵力の削減も予定されているが、正確な情報に基づく効率的な作戦立案によって、兵力の削減にも関わらず作戦能力が維持できる、という予算面での利点もあると考えられる。

その上で、想定すべき脅威が多様化する中で諜報・監視活動の重要性は増加しており、国防において、諜報・監視目的での IT 利用が今後焦点の 1 つとなるものと考えられる。また、その利用形態も、空港、国境などでの入国審査における個人バックグラウンド情報の確認から、偵察・攻撃用の無人航空機(Unmanned Aerial Vehicle、UAV)制御システム運用、各種センサー情報の分析、社会文化面からの国際的な安全保障動向予測など、幅広い分野が想定しうる。またその一環として、ビッグデータ解析などの分野において、国防関連のアプリケーションが今後急成長するとの予測も見られる[152]。

### (2) サイバーセキュリティの強化

これまでの紛争における主体としての国家に代わり、テロリストやアクティビストなど非国家的存在が、安全保障上対処すべき対象としてクローズアップされてきている。中でも、圧倒的な通常戦力を持つ米国(本土)に対する物理的攻撃の可能性は、依然と比較して薄まっている一方で、攻撃者の特定が困難であり、攻撃者としては報復を受ける可能性が低い点[153]、通常兵器と異なり攻撃側に必要なコストが低い点[154]、少数の攻撃者が大規模な損害を与えうる点[155]などから、テロリストやアクティビストなどによる攻撃手段とし

[151] http://www.comw.org/qdr/fulltext/1002QDR2010.pdf
[152] http://gigaom.com/cloud/security-is-the-next-killer-app-for-hadoop/
[153] http://www.au.af.mil/au/awc/awcgate/acsc/02-053.pdf
[154] http://asymmetricthreat.net/docs/asymmetric_threat_4_paper.pdf
[155] http://asymmetricthreat.net/docs/asymmetric_threat_4_paper.pdf

てサイバー攻撃が採用される傾向にあることが指摘されている[156]。このような傾向に伴い、サイバー攻撃への対処は、米国連邦政府にとって重要な課題になりつつある[157]。

また、産業界においてもエネルギー、ライフライン、医療機関など人々の生活基盤を支えるシステムが IT により運営されるようになってきていていることからも、防御対象としての IT システム、インフラ制御システムの優先度は高くなってくると考えられる。

### (3) サイバー先制攻撃の可能性

サイバー空間が、陸海空宇宙につぐ第 5 の作戦領域として認識される中、軍事的攻撃手段としてのサイバー攻撃の現実性が高まっている。これは、外部からの攻撃に対処するだけでなく、米国にとって脅威と考えられる対象に、先制的にサイバー攻撃を仕掛ける取り組みが行われる可能性もあるということである。例えば、2010 年に国防総省内に設置されたサイバー軍の任務内容について、同軍が第 3 者に対して攻撃を行う可能性も示唆されている[158]。また、かつては作戦遂行の補助的な役割を果たすに留まっていた IT システムが、今後の国防活動でより中心的な任務を担う可能性が高いと見られている[159]。

例えば、2010 年にイランの核開発関連施設に被害を与えたことで知られるコンピュータウイルス「Stuxnet」は、その高度な設計や、感染対象の特徴などから、イスラエル政府および米国連邦政府が作成に関わっていたとの指摘も見られ[160]、今後の軍事活動において、サイバー攻撃が具体的な手段として採られる可能性があることを示唆している。

なお、我が国においては、憲法の解釈上、武力行使発動に関しては「①わが国に対する急迫不正の侵害があること、②この場合にこれを排除するために他に適当な手段がないこと、③必要最小限度の実力行使にとどまるべきこと」[161]とされており、サイバー攻撃がここでいう武力行使に相当すると仮定した場合、上記のような先制攻撃が採られる可能性は皆無であると考えられる。

### (4) オペレーション効率化および効率化に伴う経費削減

IT インフラ強化の間接的な恩恵として、国防関連省庁の内部業務効率を向上、コスト減につなげることにより、全体の予算削減につながる点がある。実際に、DoD では、2012 年度から 2016 年度にかけてのコスト削減案を提示しており、同文書内で IT システムの

[156] http://asymmetricthreat.net/docs/asymmetric_threat_4_paper.pdf
[157] http://www.defense.gov/news/newsarticle.aspx?id=65358
[158] http://www.stratcom.mil/factsheets/Cyber_Command/
[159] http://www.cyberwarzone.com/cyberwarfare_blogs/how-war-will-be-fought-21st-century
[160] http://www.nytimes.com/2011/02/13/science/13stuxnet.html?_r=1&scp=1&sq=Malware%20Aimed%20At%20Iran%20Hit%20Five%20Sites,%20Report%20Says&st=cse
http://spectrum.ieee.org/podcast/telecom/security/sons-of-stuxnet
[161] http://www.mod.go.jp/j/approach/agenda/seisaku/kihon02.html

強化や統合によるコスト削減についても取り上げられている[162]。具体例として、以下のような取り組みが言及されている。

- 陸軍のデータセンタを統合し、施設数ベースで 75%削減する。
- DoD 全体で、電子メールシステムとデータセンタを統合する。
- 空軍において、パイロットの訓練時に使用されるフライトシミュレータを高度化し、実機の稼働が必要な訓練の時間を短縮する。

以上のように、IT インフラの刷新によるコスト削減を実現する上では、特にクラウドコンピューティングの仕組みを利用することがホワイトハウスによって促されている[163]。これは、DoD に限らず、連邦政府 IT システム全体に対する効率化政策の一環であるが、IT および国防関連業界の間では、今後関連省庁の IT 予算が減少下でも、多大な成長が期待される分野としてクラウドコンピューティングに注目する動きもある[164]。


なお、このレポートに対するご質問、ご意見、ご要望がありましたら、
takashi_wada@jetro.go.jp までお願いします。

[162] http://comptroller.defense.gov/defbudget/fy2012/FY2012_Efficiency_Justification_Book.pdf
[163] http://www.businessweek.com/news/2011-12-24/congress-calls-for-defense-department-plan-for-cloud-computing.html
[164] http://www.informationtechnologymarket.com/?p=128