米国におけるネットワークセキュリティ技術分野の
研究開発動向等の調査

2012 年 3 月

米国におけるネットワークセキュリティ技術分野の研究開発動向等の調査

目次

1. 連邦政府による 2012 年度及び 2013 年度に向けた ICT 研究開発予算動向

「ネットワーキング及び情報技術研究開発（Networking and Information Technology Research and Development: NITRD）」の原型となる高性能コンピューティングと通信（High Performance Computing and Communications: HPCC）は、「1991 年高性能コンピューティング改正法（High Performance Computing Act of 1991）」（通称HPC法）[1]により設置され、2005 年にNITRDに改称され、現在に至っている。NITRDは、大統領科学技術政策室（President's Office of Science and Technology Policy: OSTP）下に置かれ、OSTP は任意にネットワーク情報技術研究開発国家調整室（National Coordination Office for Networking and Information Technology Research and Development: NCO）を設け、調整事務局としての役割を担わせている。

NITRD の主な目標は以下の通りである:

- 米国が高度なネットワーキング、コンピューティングシステム、ソフトウェア、及び付随する情報技術において、技術上のリーダーシップを取り続けることができるよう研究開発の基礎を提供する
- 高度なネットワーキング、コンピューティングシステム、ソフトウェア、及び付随する情報技術に関して、連邦政府の必要を満たすことができるよう研究開発の基礎を提供する
- 科学・エンジニアリングにおいて世界的なリーダーシップを維持することができ、国家の防衛と安全保障を高め、米国の生産性、競争性を向上し、長期の経済成長を促進する、また国民の健康を改善し、環境を保護する、さらに教育、研修、生涯学習を改善し、生活の質を向上するために該当する技術を開発、整備を速める

NITRD 参加機関

NITRD には、以下の 10 の連邦政府機関が参加しており、NCO はこれらの ICT 研究開発を支援する省庁間において調整を行なっている。

- 全米科学財団（National Science Foundadtion: NSF）
- 国防総省（Department of Defense: DOD）
- 国立衛生研究所（National Institute of Health: NIH）
- エネルギー省（Department of Energy: DOE）
- 国防高等研究事業局（Defense Advanced Research Projects Agency:

[1] 「1991 年高性能コンピューティング法」、http://www.nitrd.gov/congressional/laws/HPC_Ac_as_amended_by_NGI_Research_Act_and_America_COMPETES_Act.pdf

DARPA）
- 米国商務省標準技術院（National Institue of Standards and Technology: NIST）
- 航空宇宙局（Natinal Aeronautics and Space Administration: NASA）
- 国土安全保障省（Department of Homeland Security: DHS）
- 海洋大気庁（National Oceanic and Atmospheric Administraton: NOAA）
- 環境保護庁（Environmetal Protectiono Agency: EPA）

プログラム・コンポーネント・エリア（Program Component Area: PCA）
NITRD は研究分野の対象として以下の 8 つの戦略的優先事項を、PCA として特定している。

- ハイエンド・コンピューティング（High End Computing: HEC）
- HEC インフラ
- サイバセキュリティと情報保証（Cybersecurity and Informaton Assurance: CSIA）
- ヒューマン・コンピュータ・インタラクション（Human Computer Interacton: HCI）
- 大規模ネットワーキング（Large Scle Networking: LSN）
- 高信頼ソフトウェアとシステム（High Confidence Softwareand System: HCSS）
- ソフトウェア設計と生産性（Software Design and Productivit: SDP）
- ICT に関連する社会・経済・労働力問題（Social, Economics, and Workforce Implications of IT: SEW）

1.1. 2012 年度 ICT 研究開発予算の総括と動向分析

2012 年度 NITRD 予算は、37.39 億ドルに対して 1,200 万ドルの増加、すなわち 0.3%増と、2011 年度に比較してほぼ横ばい状態となっている。2012 年度予算における変化は、①HEC インフラに対する予算が縮小したこと、及び②CSIA に関する予算が増加したことが指摘できる。

2011～2013 年度 NITRD 予算（単位:100 万ドル）

機関	2011 実績	2012 概算	2013 要求	2013 増減率%
NSF	1,189.40	1,138.30	1,207.20	6%
DOD	749.9	694.1	654	-5.8%
NIH	551	553	551	-0.1%
DOE	489.2	542.5	568.5	4.8%
DARPA	436	489	462	-5.5%
NIST	78.3	100.2	116.7	16.5%
NASA	94.3	102.6	100.4	-2.1%
DHS	47	47	64	36.2%
NOAA	26.3	22	25	13.6%
EPA	6	6	6	0%
その他	59.6	44.6	52.6	17.9%
合計	3,727.0	3,739.3	3,807.4	1.80%

出典:NITRD 2011～2013 年度予算を基にワシントンコアで作成

機関レベルでは、DOE と NIST が 2012 年度予算で大きな伸びを示している。具体的には、DOE に関しては、LSN に対する予算が 2,400 億ドル増加したこと、また NIST については CSIA 予算が 2,200 億ドル増加したことが挙げられる。

1.2. 2013 年度 ICT 研究開発予算に関する動向分析

2013 年度予算概要

連邦行政予算管理局（Office of Management and Budget: OMB）は 2011 年 8 月、各連邦政府機関に対して、2013 年度予算要求指針書を提出し、以下のポイントを指摘している[2]。

- 裁量歳出を 2011 年度に比べ 5～10%削減すること
- 経済成長を促すプログラムへの支出を増やすこと
- 機関内部の業務効率とデータ品質向上に投資すること
- 技術革新、製造業、保健、エネルギー、気候変化、サイバーセキュリティ、科学・技術・工学・数学（Science Technology Engineering and Mathematics: STEM）教育等現政権の優先事項に重点を置き、引き続き投資を行うこと

[2] 「2013 年度予算指針書（覚書 M-11-30）」、OMB、2011 年 8 月 17 日
http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-30.pdf

オバマ政権は、ICT 分野及び非 ICT 分野の双方を含めた連邦研究開発活動を経済成長に貢献するものと捉え、特にイノベーション、製造、サイバーセキュリティ等を優先投資分野としている。現政権による 2013 年度予算要求では、連邦研究開発総予算額が 1,408 億ドルとなっており、2012 年度予算から 20 億ドル、すなわち 1.4%の増加となっている。

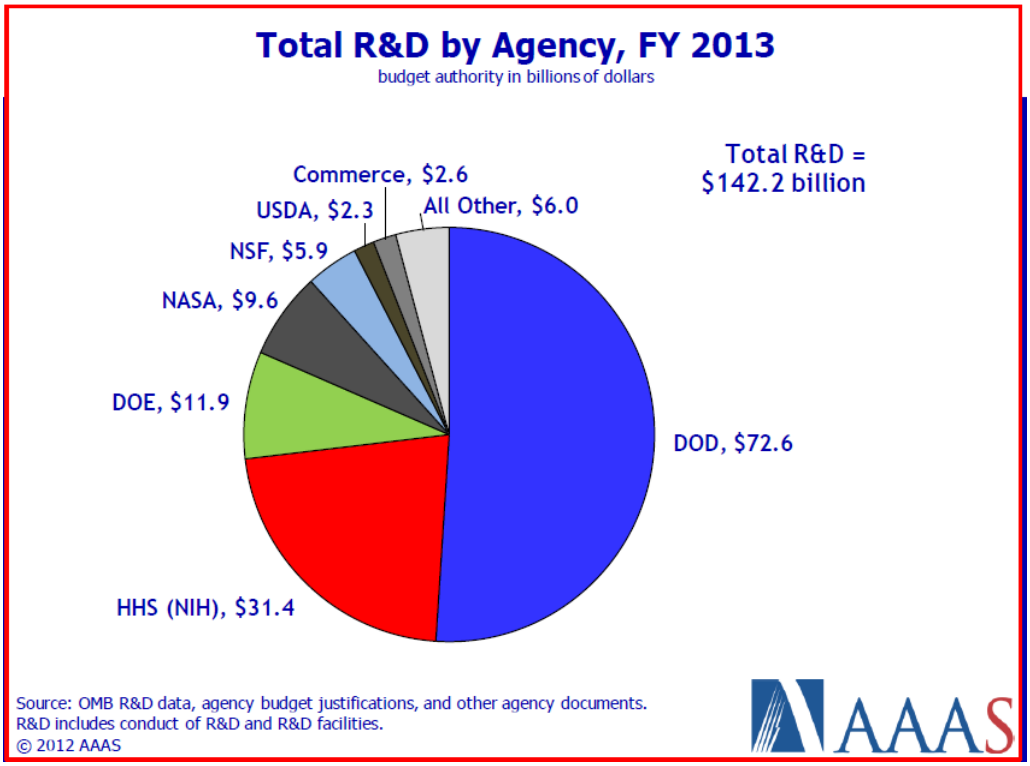
連邦研究開発予算要求において、非軍事分野における研究活動については、5%増となっている。非軍事分野における研究開発額の伸びが目立つものの、軍事分野における研究開発は、依然として連邦研究開発総予算の半分以上を占めている。オバマ政権が国家経済競争力の強化に重要と捉えている、NSF、DOE 科学局、NIST については、本年度予算案が 131 億ドル、すなわち 4.4%の増加となっている。尚、これらの増加は、「COMPETES 再授権法（The America COMPETES Reauthorization Act of 2010）」によるものである。

連邦研究開発総予算の機関別配分及び 2013 年度機関別研究開発予算要求の推移を下のグラフに示す。NISTに関する 2013 年度予算の急増は、2 つの新たな研究開発イニシアチブ、①「製造イノベーションに関する国家ネットワーク（National Network for Manufacturing Innovation）」[3]に対する 10 億ドル及び、②「ワイヤレス・イノベーション基金（Wireless Innovation Fund）」[4]に対する 3 億ドルによるものである。

[3] 「製造イノベーションに関する国家ネットワーク」とは、2012 年 3 月 9 日、オバマ大統領が米国の製造業におけるイノベーションを促進する目的で発表したイニシアチブで、連邦機関、大学機関、業界が連携して地域の製造業を活性化させるための組織を全米に 15 機関設置するために総額 10 億ドルを投資するとしている。
http://www.whitehouse.gov/the-press-office/2012/03/09/president-obama-announce-new-efforts-support-manufacturing-innovation-en

[4] 「ワイヤレスイノベーション基金」とは、500MHz 周波数帯のオークションで獲得した 30 億ドルを通して、連邦政府期機関におけるワイヤレス技術の研究開発及び実証実験を促進する目的で設置された。
http://www.nist.gov/public_affairs/factsheet/wireless_innov2013.cfm

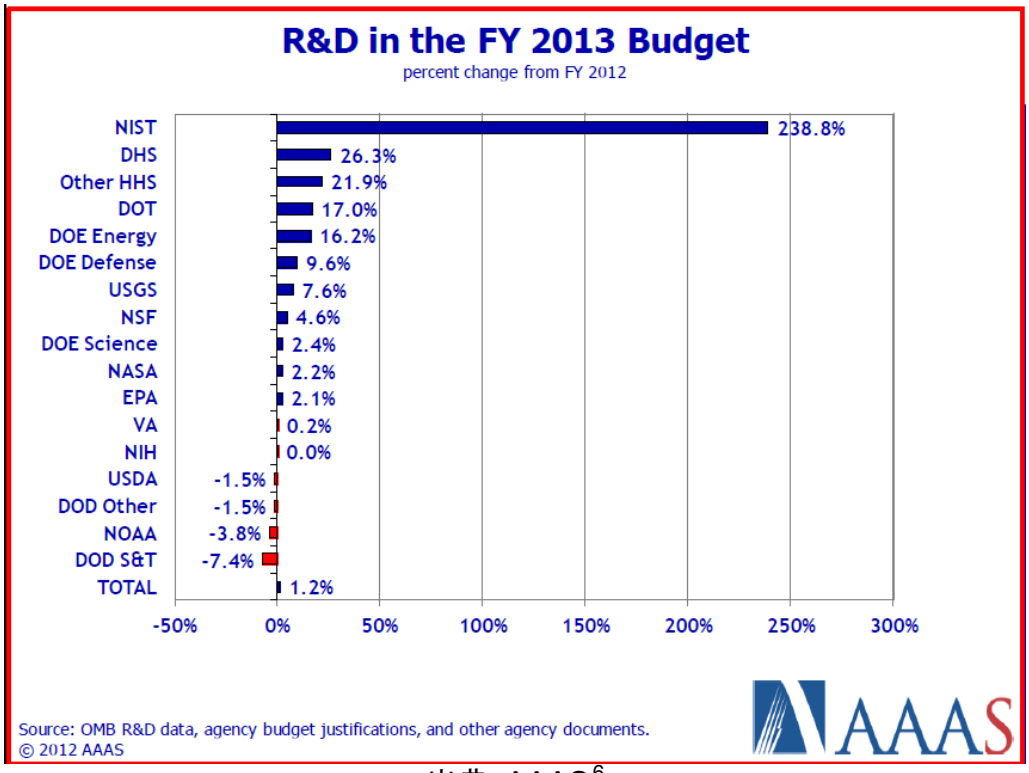
連邦政府機関における 2013 年度研究開発予算



出典：米国科学振興協会（American Association for the Advancement of Science: AAAS）[5]

[5] 「研究開発に関する連邦予算」、AAAS、2012 年 2 月 28 日（スライド 34）
http://www.aaas.org/spp/rd/presentations/aaasrd20120228.pdf

2013 年度研究開発予算における 2012 年度からの増減率



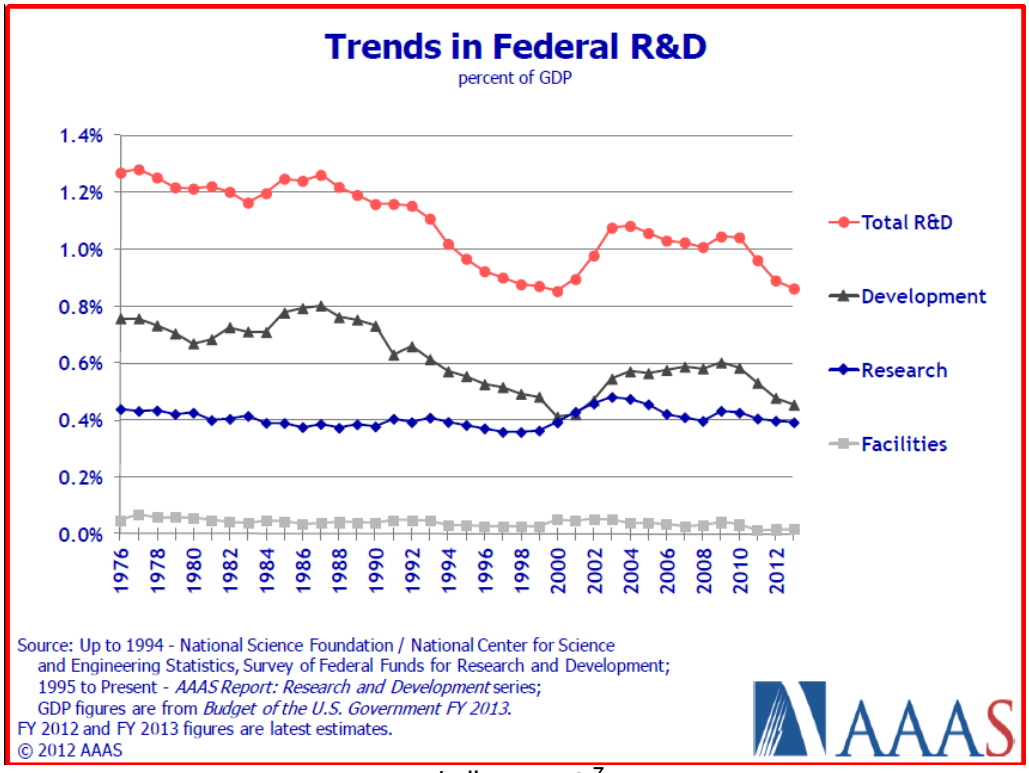
出典：AAAS[6]

連邦研究開発支出の国内総生産（GDP）に対する割合を示した下のグラフにおいて、2009 年より開発に関する額が激減していることから、オバマ大統領は開発より研究に対して重点を置いていることがわかる。2013 年度連邦研究開発予算要求においても、その傾向が伺える。

.

[6]「研究開発に関する連邦予算」、AAAS、2012 年 2 月 28 日（スライド 35）
http://www.aaas.org/spp/rd/presentations/aaasrd20120228.pdf

連邦研究開発支出の国内総生産に対する割合



出典：AAAS[7]

2011～2013 年度機関別 NITRD 予算

NITRDについては、2013 年度予算案において、僅かではあるが増加がみられる。オバマ政権による 2013 年度予算案では、NITRD予算が 38.07 億ドルであり、2012 年度の 37.39 億ドルから 1.8%の伸びとなっている[8]。下表にある通り、NSFが総予算の 3 分の 1 近くと、NITRD予算の中でもっとも大きな割合を占めている。

[7] 「研究開発に関する連邦予算」、AAAS、2012 年 2 月 28 日（スライド 37）
http://www.aaas.org/spp/rd/presentations/aaasrd20120228.pdf
[8] 「ネットワーキングと情報技術研究開発プログラム（2013 年度大統領予算に対する補足）」、NITRD、2012 年 2 月
http://www.nitrd.gov/pubs/2013supplement/FY13NITRDSupplement.pdf

2013 年度 各機関別 PCA 別 NITRD 予算（単位：100 万ドル）

機関	HEC インフラ	HEC	CSIA	HCI*	LSN	HCSS **	SDP ***	SEW ****	合計
NSF	255.6	109.9	114.1	297.2	131.4	97.6	83.7	117.7	1207.2
DOD	196.2	27.4	156.6	107.8	105.3	35.5	25.3		654.0
NIH	221.0	18.0		215.0	12.0	10.0	53.0	22.0	551.0
DOE	328.3	92.1	33.5		82.6	6.0	20.0	6.0	568.5
DARPA		79.0	247.0	87.0	49.0				462.0
NIST	16.0	5.0	55.2	15.8	12.1	7.8	4.4	0.4	116.7
NASA	60.0			13.0	1.0	16.8	9.6		100.4
DHS			61.0		3.0				64.0
NOAA	20.6	0.2		0.5	3.6		0.7		25.6
EPA	3.0			3.0					6.0
その他	10.0	11.0		26.1	0.5	1.0	-0.1	4.0	52.5
合計	1110.7	342.5	667.4	765.4	400.5	174.7	196.6	150.1	3807.9

出典：NITRD 資料を基にワシントンコアで作成

2013 年度 NITRD 予算要求において、相対的及び実質的な動きがあった機関は注目に値する。最も顕著な予算増額を要求している機関は、NSF、DOE、NIST 及び DHS である。NSF の 2013 年度予算要求は、2012 年度予算の 6,900 万ドルに対して 6%増となっている。DOE は同じく 2012 年度予算の 2,200 万ドルに対して 4.8%増を要求している。さらに、NIST と DHS はそれぞれ 16.5%、36.2%と 2 桁台の増額を要求している。

最も ICT 研究開発予算の縮小がみられた機関は、国防長官室（Office of Secretary of Defense: OSD）及び軍研究所（陸軍、海軍、空軍）を含めた DOD に係る 5.8%減、額にして 4,000 万ドル相当の削減が挙げられる。また、DARPA の予算は 5.5%減、額にして 2,700 万ドル相当の削減となっている。

2013 年度 NITRD 予算における機関別優先事項

2013 年度予算推移について、その主な理由を下記にまとめる。特に興味深い点は、各機関の優先事項において最も大きな予算変化がみられた CSIA 予算の増加である。DOE の CSIA 予算が横ばいである中、下に示す機関は全て CSIA 研究開発の著しい増加を要求している。

NSF2013 年度予算案（12.07 億ドル、＋6%）：NSFに関する 6,900 万ドルの予算増は、主にCSIA追加予算 1,500 万ドル、「ワイヤレス通信及びスペクトラム共有のためのLSN」

予算 900 万ドル、「サイバーフィジカル・システム（Cyber-Physical Systems: CPS）[9]及び国家ロボットイニシアチブ（National Robotics Initiative）[10]のためのHCSS研究開発」予算 1,300 万ドルによるものである。

DOD（6.54 億ドル、-5.8%）：4,000 万ドルの削減は、主に HEC インフラにおける 1,500 万ドル減、及び HEC 予算の 2,200 万ドル減による。こうした減少額は、CSIA 予算が 1,200 万ドル増加したことで一部相殺されている。

DOE（5.685 億ドル、＋4.8%）：DOE 予算で最も顕著な変化は、データ集約型の科学計算を支える HEC インフラに対する 1,100 万ドルの増加と、LSN における 900 万ドルの増加である。DOE の LSN 研究開発には、テラビット／秒（Tbps）のネットワーキング及び分散科学計算のためのミドルウェア研究開発を含む。

DARPA（4.62 億ドル、-5.5%）：DARPA の予算縮小額 2,700 万ドルは、HCI」に関する予算が 5,700 万ドル減少、一方で CSIA 予算が 2,400 万ドル増加したことによる。

NIST（1.17 億ドル、＋16.5%）：予算拡大額 1,700 万ドルには、「サイバースペースにおける信頼できるアイデンティティに向けた国家戦略（National Strategy for Trusted Identities in Cyberspace）」[11]を支援する新たなCSIA予算 800 万ドル、新たなLSN予算 400 万ドル、「ゲノム素材イニシアチブ（Materials Genome Initiative for Global Competitiveness）」[12]を支援するHECインフラ及びHCIIに充てられる 200 万ドル、及び NIST の「スマート・マニュファクチュアリング・プロセス／機器プログラム（Smart Manufacturing Process and Equipment Program）」[13]を支えるHCSS予算 200 万ドルが含まれる。

DHS（6,400 万ドル、＋36.2%）：1,700 万ドルの予算増は、CSIA 予算 1,800 万ドルによるものである。予算増加額は非サイバーセキュリティ分野の研究開発に対する予算減少

---

[9] NSF のサイバー-フィジカルシステム・プログラムでは、スマートグリッドやスマートビルディング、次世代交通システムなどコンピュータと物理システム間が相互依存する分野におけるアプリケーションやツールなどの研究開発を推進している。
http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286]

[10] 国家ロボットイニシアチブは、オバマ大統領が 2011 年 6 月に発表した、次世代ロボットの研究開発を推進する目的で設置されたイニシアチブで、NSF が主導し、NIH、NASA、農務省（U.S. Department of Agriculture）の４機関の共同で研究プロジェクトに資金を拠出している。
http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503641&org=CISE]

[11] 「サイバースペースにおける信頼できるアイデンティティに向けた国家戦略」、ホワイトハウス、2011 年 4 月
http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

[12] 「ゲノム素材イニシアチブ」、国家科学技術評議会（National Science and Technology Counci：NSTC）、2011 年 6 月。「ゲノム素材イニシアチブ」は、新素材の発見、開発、製造を促進することを目的に設定されたイニシアチブである。
http://www.whitehouse.gov/sites/default/files/microsites/ostp/materials_genome_initiative-final.pdf

[13] Smart Manufacturing Process and Equipment の概要説明
http://www.nist.gov/el/isd/sbm/smartmanu.cfm

によってやや相殺されている。
NIH（5.51 億ドル、-0.1%）：NIH の NITRD 予算は SDP」に関する 100 万ドル（－1.9%）を除き、2012 年度からほぼ横ばいとなっている。HEC インフラ及び HCI 予算は、NIH の NITRD 予算のそれぞれ 40%近くを占める。HCI 予算には情報アクセス・管理・保存及び医生物学データの視覚化に関する研究開発が含まれる。

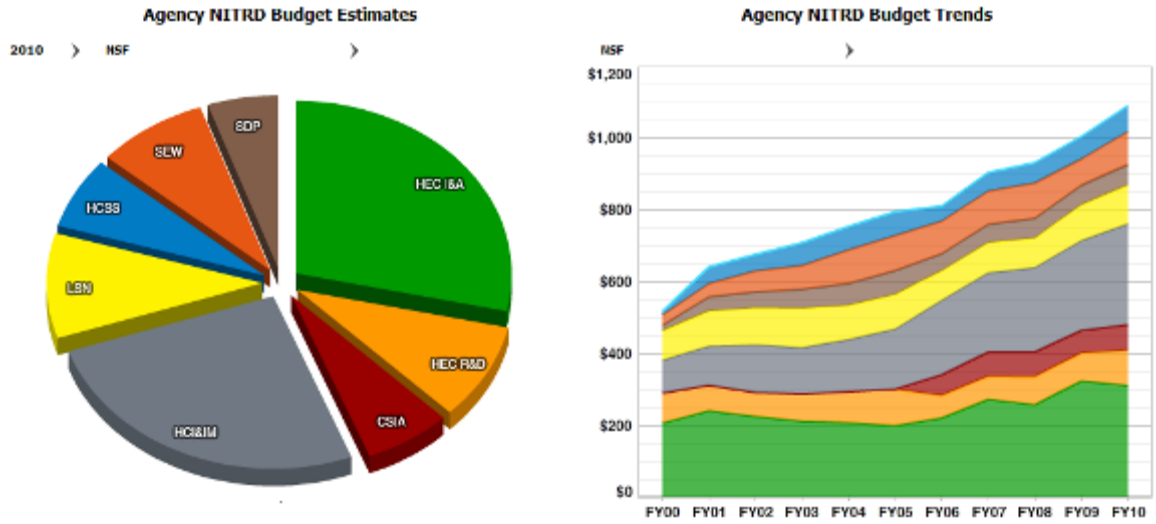
EPA（600 万ドル、横ばい）：EPA の NITRD 予算 600 万ドルは、2012 年度から変わっていない。HEC インフラ及び HCI は、それぞれ EPA 予算の半分を占めている。HCI 研究開発には、有害物質データバンクと情報管理ツール開発、さらに EPA が有する科学データへの効率的なアクセスや活用技術開発が含まれる。

2000～2010 年度 NITRD 予算の機関別動向
NITRD Dashboardは、一般に開かれた政府の対話型ウェブサイトであり、NITRD予算に関するデータを提供している[14]。同ウェブサイトでは、PCA別に分割される各機関のNITRD予算と、これが時間とともにどのように変化していくかという傾向について示すものである。Dashboardの予算データは現在 2010 年まで更新されている。

Dashboard は機関の予算概算額ではなく、実際の決算データを提供している。そのため、2012 年度予算データはまだ出されておらず、2011 年度予算データはまだ追加されていない状況である。

[14] NITRD Dashboard の概要説明 http://itdashboard.nitrd.gov/

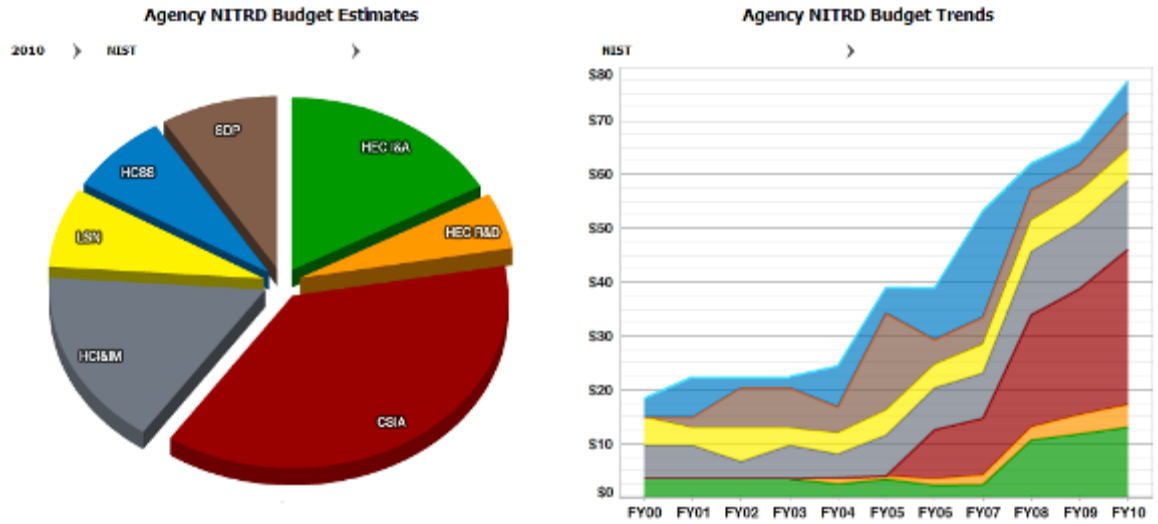
NSF における 2000～2010 年度 NITRD 予算（単位：100 万ドル）



出典：NITRD Dashboard

上のグラフは、NSF の NITRD 予算において HEC インフラ及び HCI が大きな部分を占めており、前出の 2 分野と比べて額的には、かなり差があるものの、LSN が 3 番目となっていることを示している。また、サイバーセキュリティ研究開発の重要性が増すに従って、CSIA 予算が 4 番目の柱として台頭してきている。HEC インフラが NSF 予算に占める割合は未だに顕著であるが、同 NITRD 予算の全体的な伸びは、主に他の部分、特に CSIA 及び HCI の伸びによるものである。

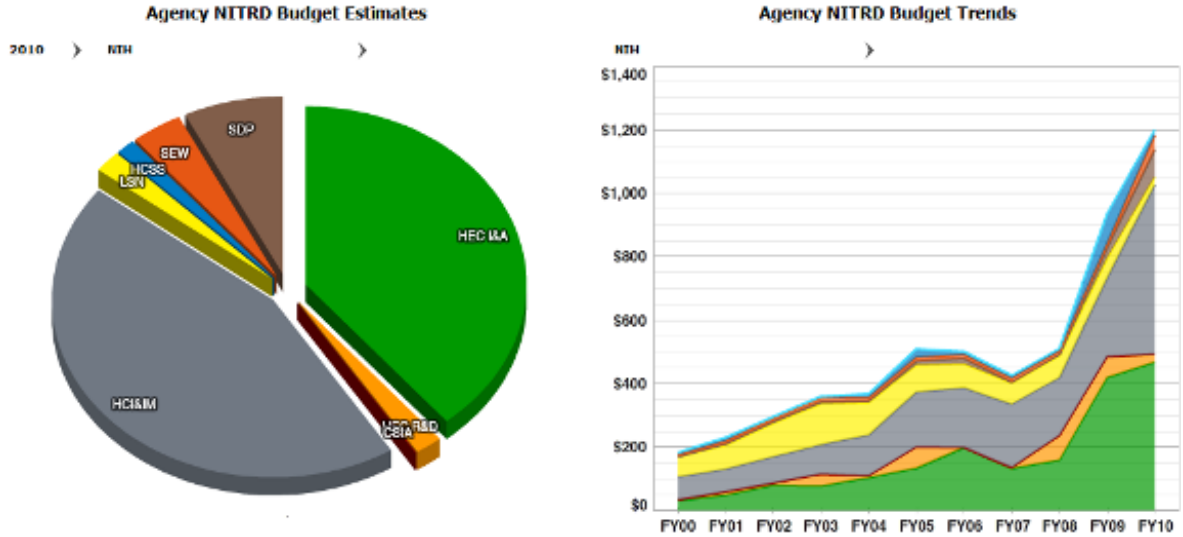
NIST における 2000～2010 年度 NITRD 予算（単位：100 万ドル）



出典：NITRD Dashboard

上のグラフは、NIST における NITRD 予算の伸びが主に CSIA 予算の著しい増加によるものであることを示している。同 CSIA 予算は同機関において最大の予算割当分野となっている。NIST 予算は、より小規模だが重要な HEC インフラに対する予算拡大によっても伸びを示している。

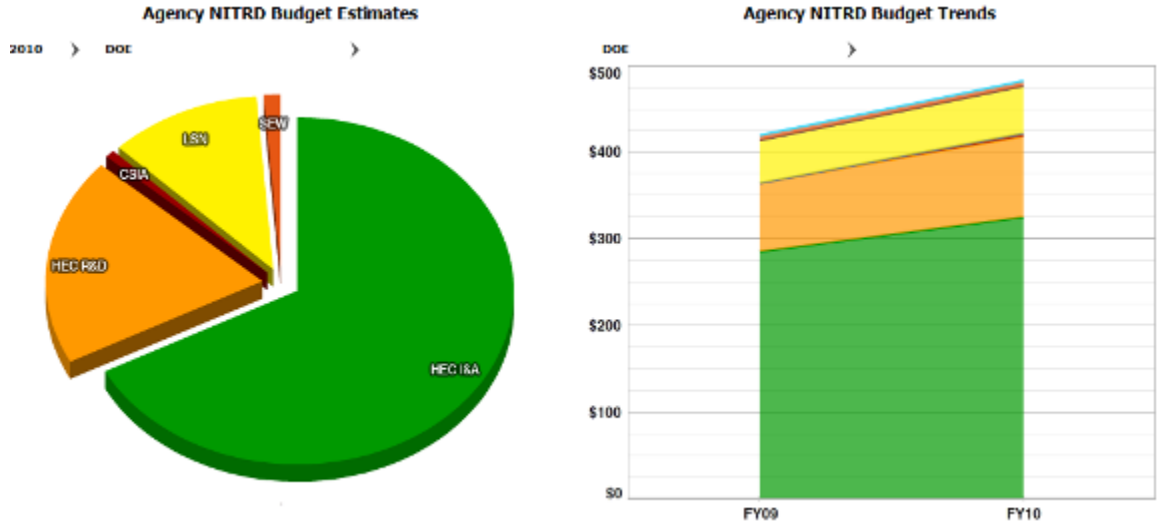
NIH における 2000～2010 年度 NITRD 予算（単位：100 万ドル）



出典：NITRD Dashboard

上のグラフより、NIH の NITRD 予算のうち、HEC インフラ及び HCI が大部分を占めていることがわかる。NITRD 予算の伸びは、この 2 部門の予算増加によるものである。

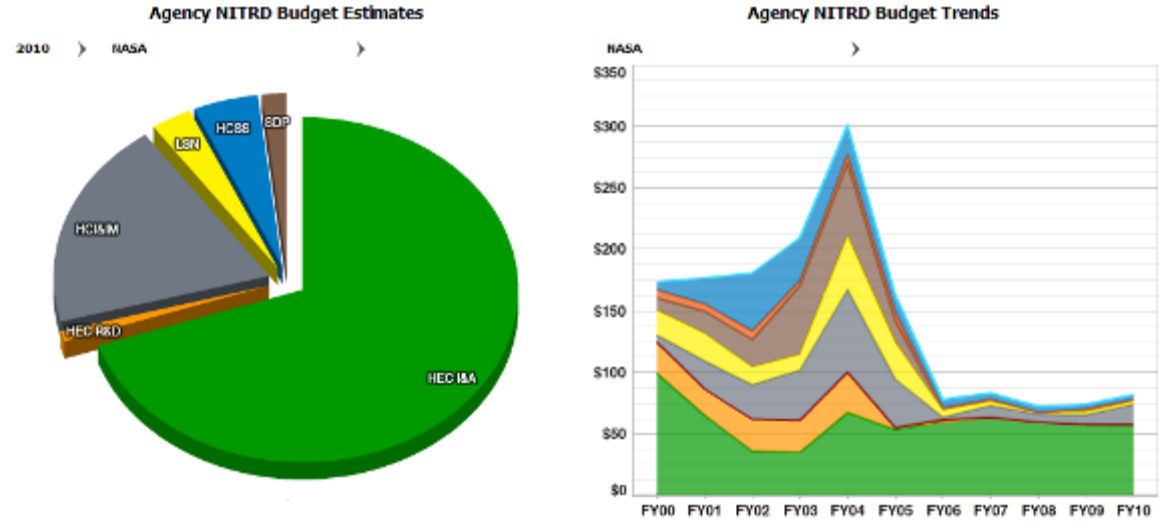
DOE における 2009～2010 年度 NITRD 予算（単位：100 万ドル）



出典：NITRD Dashboard

DOE は 2009 年度以前の NITRD 予算データを公開していない。そのため、経年推移はグラフに示すことができない。しかし、HEC インフラが DOE 予算の大部分を占め、これに HEC 及び LSN が続いていることがわかる。

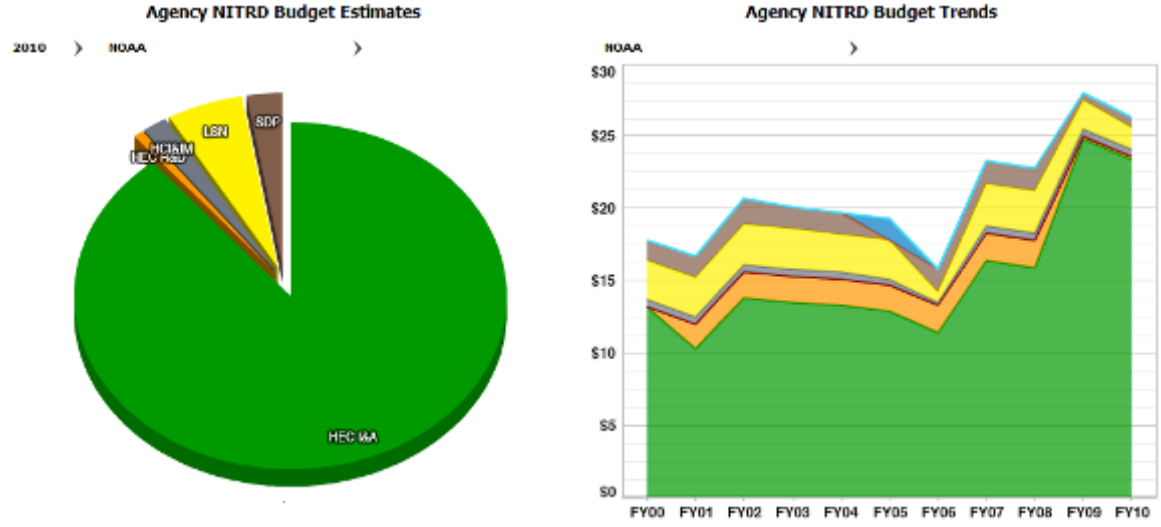
NASA における 2000～2010 年度 NITRD 予算（単位：100 万ドル）



出典：NITRD Dashboard

NASA における NITRD 予算は HEC インフラが占める割合が大きく、DOE における予算構成に類似している。NASA の場合、HEC インフラ以外の PCA では予算が著しく減少している。

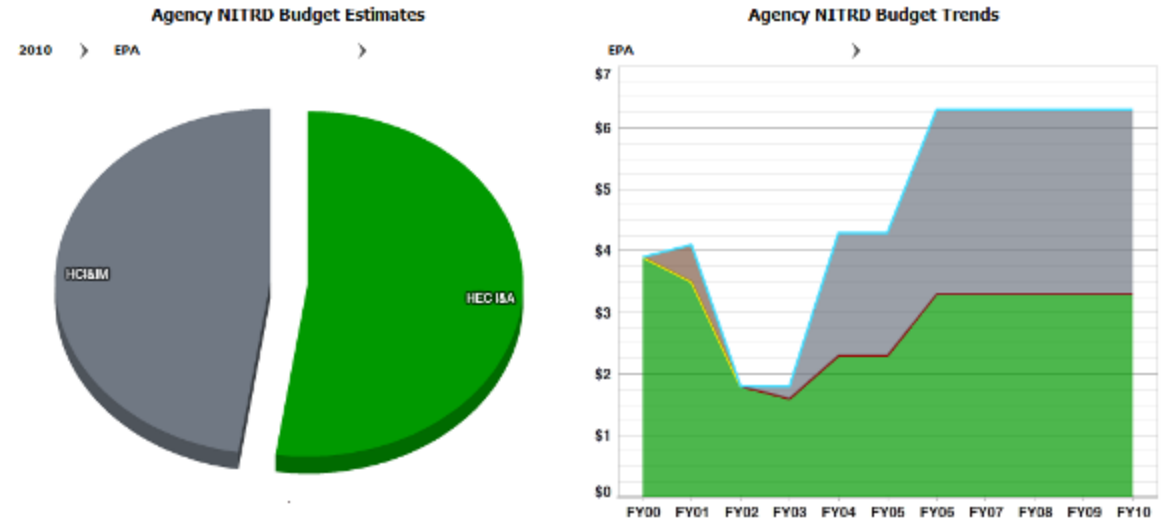
NOAA における 2000～2010 年度 NITRD 予算（単位：100 万ドル）



出典：NITRD Dashboard

上のグラフは、NOAA の予算が 2 番目の LSN を大きく引き離し、HEC インフラに著しく集中していることを示している。

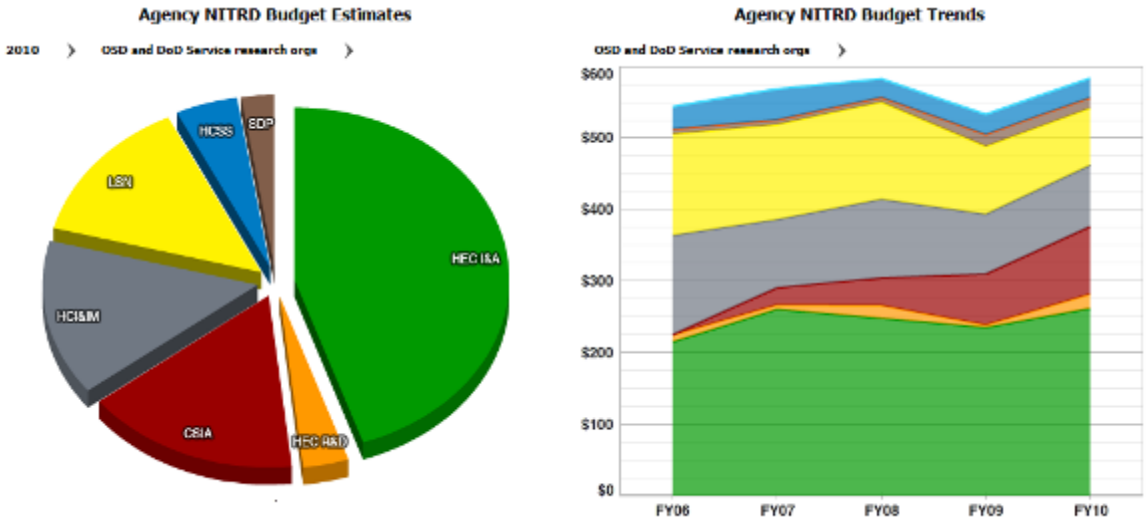
EPA における 2000～2010 年度 NITRD 予算（単位：100 万ドル）



出典：NITRD Dashboard

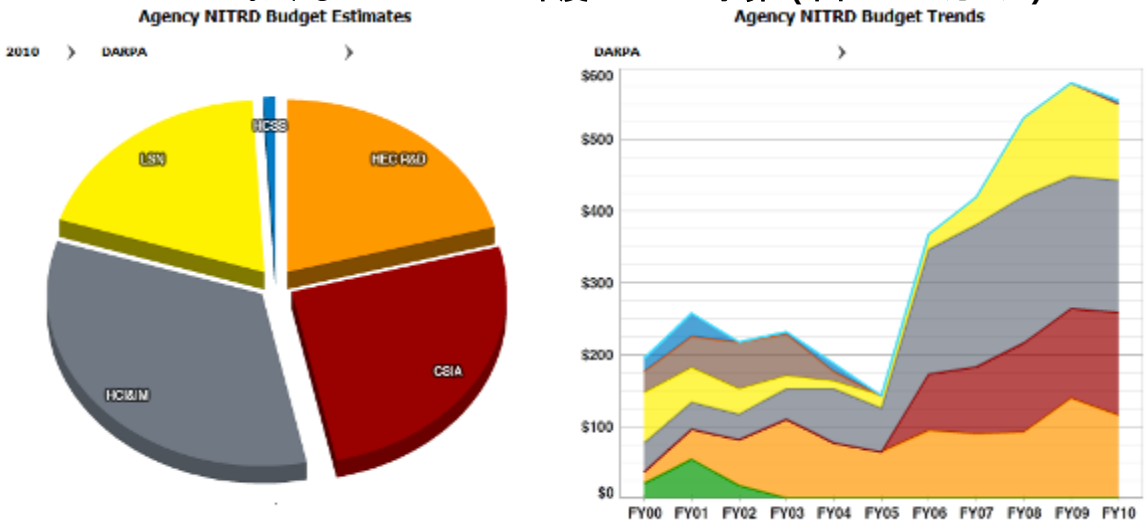
上のグラフより、EPA の NITRD 予算は過去数年にわたって約 600 万ドルと、他の NITRD 機関に比較して非常に小さいことがわかる。EPA の HCI 予算は、膨大で複雑な環境データの管理とアクセスを改善するため、研究開発予算を組むようになり、近年伸びを示している。

OSD 及び軍研究所における 2006～2010 年度 NITRD 予算（単位：100 万ドル）



出典: NITRD Dashboard

DARPA における 2006～2010 年度 NITRD 予算 (単位：100 万ドル)



出典: NITRD Dashboard

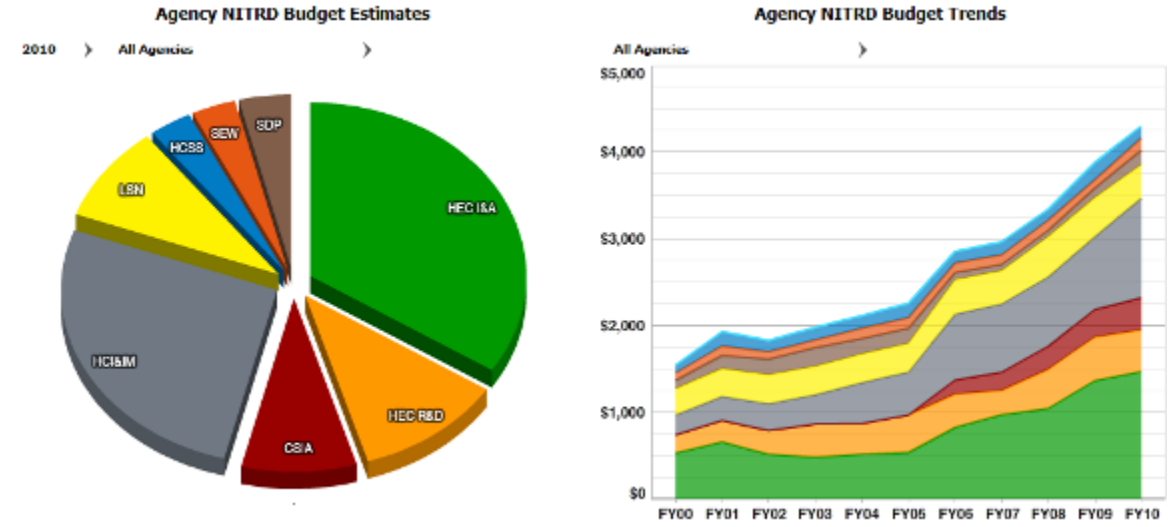
上のグラフよりDARPAのNITRD 予算が、2010年度までに一部変動した点が見られる。具体的には、HCI、CSIA、HEC 及び LSN の 4 つが、それぞれシェアを拮抗する形で2010年度予算を占めているが、近年HEC を除く3つのPCAにおける、予算の伸びが著しい点である。

それに対して、OSDと軍研究所を含めたDODの予算は、DARPAにおけるNITRD 予算より安定傾向にあるといえる。DARPAがHECインフラに出資していないのとは対照的に、OSD における NITRD 予算のほぼ半分が、HEC インフラへの出資で占められている。CSIA、HCI、LSN セグメントはそれに比べると少ないが、OSD 予算において重要な部分を占めている。

1.3. 主要 ICT 研究開発プログラム毎の今後の予算に関する計画及び課題

2000年度から2010年度までのNITRDの予算の伸びは、下のグラフで見られるように、主に2大セグメントにおける予算増、すなわち、CSIA 予算と共にHECインフラとHCの予算が増加したことに伴う。

2000～2010 年度 PCA 別 NITRD 予算 (単位:100 万ドル)



出典: NITRD Dashboard

NITRDは2013年度のNITRD予算について1.8%の増加、すなわち38億ドルを提案している。NITRD予算でもっとも顕著な変化といえるのは、13%増加のCSIA予算であり、

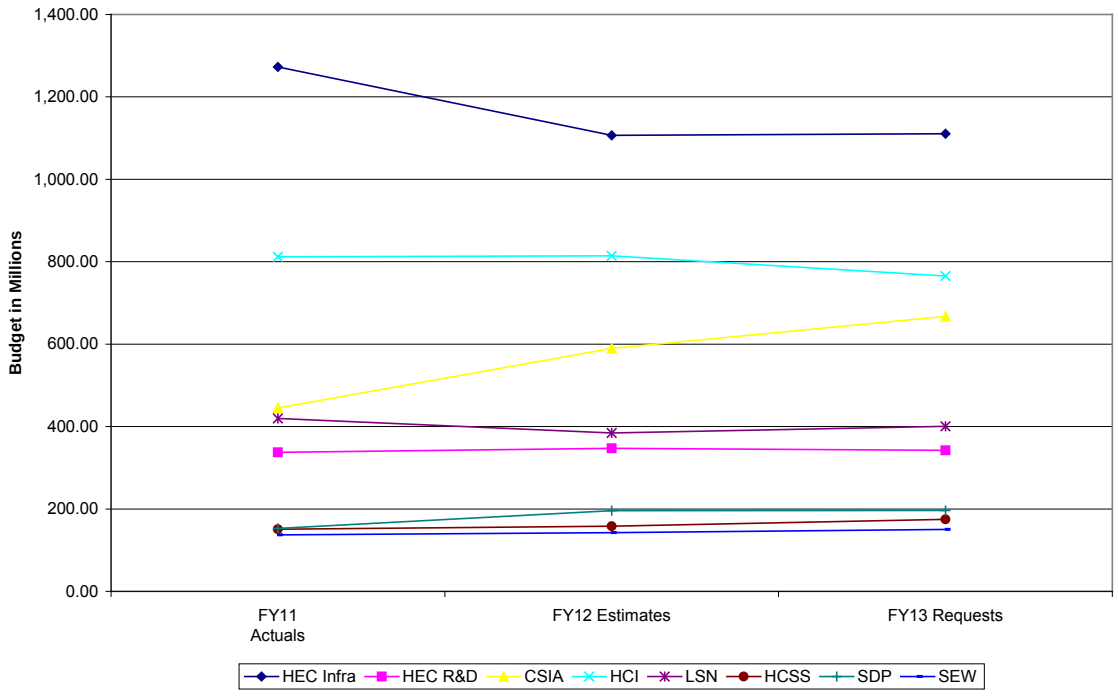
2012年の5億8,980万ドルから2013年の6億6,700万ドルとなっている（下表参照）[15]。

2011～2013 年度 PCA 別 NITRD 予算 (単位：100 万ドル)

PCA	FY11 実績	FY12 概算	FY13 要求
HEC インフラ	1,272.60	1,106.70	1,110.70
HEC R&D	337.4	347.4	342.5
CSIA	445.1	589.8	667.4
HCI	811.8	814.2	765.4
LSN	419.6	384.5	400.5
HCSS	150.8	158.4	174.7
SDP	152.7	195.8	196.6
SEW	137	142.6	150.1
Total	3,727.00	3,739.40	3,807.90

出典: NITRD の情報を基にワシントンコアで作成

2011～2013 年度 PCA 別予算推移



出典：NITRD Dashboard

[15] NITRD Dashboard の概要説明 http://itdashboard.nitrd.gov/

上表とグラフは、PCA 別の 2011 年度実績と 2012 年度概算、及び 2013 年度提示予算とその額の推移を示している。NITRD 予算に関しては、2 つの点において、顕著なものとなっている。まず一つは、HEC インフラにおける 2011 年から 2012 年における 1 億 6,590 万ドルの減少である。注目すべきことは、HEC インフラ予算額が前年比で減少しているものの、依然として NITRD 予算の一番多くを占めている点である。また HEC 予算額は、HEC インフラ予算額が低下する中、比較的安定している。

もう一つの注目すべき変化は、前途したCSIA 予算の上昇であり、複数の機関が 2013 年度CSIA 予算の大幅な増加を提案している。各機関においてサイバーセキュリティ研究開発が優先事項とされており、これについては 2011 年 12 月に発表された「信頼できるサイバースペース～連邦サイバーセキュリティ研究開発プログラム戦略計画（Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program）」（以下、「信頼できるサイバースペース」）[16]に定義されている。サイバーセキュリティ研究開発に関する同戦略計画の発表は、NITRDにとって重要な発展であったといえる。詳細を以下に述べる。

主要プログラムに関わる注目すべき動き
（1）「信頼できるサイバースペース～連邦サイバーセキュリティ研究開発プログラム戦略計画」

2011 年 12 月 6 日、NITRDは「信頼できるサイバースペース」[17]と呼ばれる文書を発表し、連邦政府省庁間のサイバーセキュリティ研究開発戦略について示している。同文書は各機関に対し、サイバーセキュリティの現状における欠点に取組み、「情勢を根本から変える技術」を導き出す長期的な基礎研究に投資するよう呼びかけている。

同戦略計画は、ホワイトハウスが以前から調整に取り組んできた省庁間のサイバーセキュリティ・プログラムに基づくものである。2008 年、ブッシュ政権は、「包括的国家サイバーセキュリティ・イニシアティブ（Comprehensive National Cybersecurity Initiative: CNCI）」[18]として、サイバーセキュリティに関するあらゆる面に取り組む省庁間のイニシアチブを発足した。CNCIは連邦政府がサイバーセキュリティ研究開発を通じて「躍進的技術」を開発することを目標とする。

---

[16] 「信頼できるサイバースペース～連邦サイバーセキュリティ研究開発プログラム戦略計画」、NSTC、2011 年 12 月 http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf
[17] 同上。
[18] 「包括的サイバーセキュリティ・イニシアチブ」、ホワイトハウス、2008 年 1 月 http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

この目標の下、機関と一般市民がサイバーセキュリティ研究開発における検討課題となる研究テーマを特定するため、2009 年にはNational Cyber Leap Yearが設けられた[19]。NITRDのCSIA Interagency Working Group（IWG）は、National Cyber Leap Yearにおいて特定されたテーマを取り入れ、これを発展させて、サイバーセキュリティ研究開発計画である「信頼できるサイバースペース」を作成した。同文書は、機関のサイバーセキュリティ研究開発活動を導く研究及び戦略テーマを複数特定している[20]。

- **設計済みセキュリティ（Designed-In-Security）**：高保証性を有し、ソフトウェア集約的システムを予想通りかつ確実に設計、開発、進化させる能力の構築と、効果的なリスク、コスト、スケジュール、品質、複雑性の管理に係る研究。その結果、ソフトウェア集約的システムを条件や環境に応じてより迅速に進化させることができる。

- **状況に応じた、信頼できるサイバースペース（Tailored Trustworthy Spaces）**：様々に進化する脅威を踏まえた幅広い活動から生じる機能及びポリシー条件を支援でき、ユーザ・コンテキストを認識し、その進化にも対応できる柔軟で適応性の高い分散型信頼環境の提供に係る研究。

- **動く標的（Moving Target）**：攻撃者に対して、攻撃の実施をより複雑にしたり、そのコストを増大することで、脆弱性と攻撃機会の露出を制限し、システム回復性を向上させるような、継続的に変化する多様なメカニズムと戦略の構築、及び分析、評価、配備に係る研究。

- **サイバー経済的誘因（Cyber Economic Incentives）**：サイバーセキュリティを普遍的なものとするための、個人及び組織に影響する効果的な行動誘因の探究に係る研究。

- **サイバーセキュリティ基礎論の構築・発展**：特定のシステム、攻撃手法、防御手法に捉われない、より普遍的なサイバーセキュリティ対策に関する基礎論の構築・発展に向けた研究。

- **多分野における技術導入を促すセキュリティ研究**：医療 ICT、スマートグリッド、金融サービス、国家防衛、交通及び信頼できるアイデンティティ等の普及を同時に促進するようなサイバーセキュリティ技術開発や要件探求に係る研究。

---

[19] NITRD National Cyber Leap Year に関する概要紹介 http://www.nitrd.gov/leapyear/index.aspx
[20] 「信頼できるサイバースペース～連邦サイバーセキュリティ研究開発プログラム戦略計画」、p. 4-16
http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf

- **研究評価管理プラン**:各連邦サイバーセキュリティ研究開発プログラムの研究成果をうまく実用化する計画・方法の模索と研究。

(2)「ソフトウェア・エンジニアリングの未来」

NITRD の SDP は、ソフトウェア作成／持続に関する科学的枠組みの確立に関連する研究開発を監視するものである。SDP は、これまでの社会的、経済的進歩がソフトウェア設計と生産性における継続的な改善に支えられてきたことを認識している。しかし、こうした進歩は、ソフトウェア・エンジニアリングにおける強固な科学的基礎を構築する研究なくして持続できるものではないという考え方が根底にあるといえる。

こうした目標は、2010 年 11 月に開催された「ソフトウェア・エンジニアリングの未来（Future of Software Engineering: FoSER）」に関するワークショップにおいて焦点となった[21]。同ワークショップでは、政府、学界、産業界の専門家が一同に会して、ソフトウェア・エンジニアリング分野を発展させる研究開発の方向性について議論を行った。ワークショップにはおよそ 90 本もの政策方針書が寄せられ、これらを 5 つのテーマに分類して議論を行った。こうしたワークショップの成果は、2011 年 12 月に発表されたSDP報告書「ソフトウェア・エンジニアリングの未来（Future of Software Engineering）」[22]にまとめられている。FoSERは、NITRD機関が以下のテーマについて取組みを行うよう呼びかけている:

- **人々のソフトウェア生産と使用を助ける**:増加しつづけるソフトウェア・エンジニア、サポーター、ユーザのコミュニティが、様々なコンピュータを介した伝達手段によって互いに連絡、協力、調整する方法を理解し、これを向上することにより、こうしたコミュニティが容易、迅速、経済的にソフトウェアを作成、維持、適応できるよう支援する。

- **未来の複合システムを構築する**:複合システムが社会に及ぼす影響、また新技術が社会にもたらす課題及び機会をよりよく理解するため、ソフトウェア・エンジニアリングの研究コミュニティは、ヘルスケア等の国家グランド・チャレンジに取り組むにあたってのソフトウェアの利用に取り組まなければならない。

- **信頼性あるソフトウェア集約的システムを構築する**:ソフトウェア・コードの質を向上しつつソフトウェア・プログラミングについてよりユーザの利便性を図るといった改善によって、ソフトウェアの信頼性を向上し、ソフトウェア開発コストを削減する。

---

[21] ソフトウェア・エンジニアリングの未来 ワークショップの概要紹介 http://fse18.cse.wustl.edu/foserprogram.html
[22] 「ソフトウェア・エンジニアリングの未来」、NITRD、2011 年 12 月
http://www.nitrd.gov/SUBCOMMITTEE%5Csdp%5Cfoser%5CFOSER%20December%202011.pdf

- **ソフトウェアに関する意思決定、進化及び経済の改善を目指す研究に投資する**:ソフトウェア生産と進化の質及びコストに関して、実務者が十分な情報に基づいた判断ができるよう、新たなアプローチを開発する。

- **ソフトウェア方法論の改善を目指す研究に投資する**:ソフトウェア・エンジニアリングに関する研究の科学的基礎を前進させる。これはソフトウェア・エンジニアリングに関する研究について実験に基づく方法を開発し、論理的、数学的分析等学際的な研究分野及び社会科学を取り入れることによって行う。

大規模データに関する動き

2011 年初めに、政府データの急激な増加によってもたらされる課題に取り組む研究開発の調整を行うために、省庁間組織である「大規模データ・シニア運営グループ（Big Data Senior Steering Group: BD SSG）」がNITRD内に設置された[23]。大規模データ研究開発は、自動解析技術やデータマイニング、機械学習、プライバシー、データの相互運用性といった分野を対象とする。BD SSGが大規模データ研究開発において戦略的優先事項としているものは以下の通りである[24]:

- 新しい科学の推進や、重要な科学的問題提起の探求、そして新たな発見の迅速化につながるような大規模で異質なデータの活用
- 国家が有する様々なニーズや各政府機関のミッション達成への貢献や、社会的、経済的重要課題の解決につながるような大規模データ特有の価値の活用
- 連邦予算による研究から得られる様々な研究データについて、それがフルに活用されるような持続的な管理
- データ科学を躍進させ、データ情報に基づいた効率的な分析や行動支援を可能にするデータ活用インフラの開発と維持

BD SSG は、初年度に様々な活動を行い、将来におけるより大きな目標設定や調整の基礎を築いている。BD SSG は、現在の研究開発プロジェクトについて一覧を作成するため、現行の関連プロジェクトについて省庁間の評価を行ったがその結果内容については公開されていない。さらに、今後発行予定の大規模データ・イニシアチブ報告書について作業を開始したところである。同報告書は、大規模データ研究開発に関する展望、目標、機会の概要を示すものとなる。今後これに関する活動は、既存のどの PCA に組み込まれるのか、PCA をまたがる形となるのか、あるいは新たな PCA として立ち上げれるのかについては、現時点で明確にされていない。

---

[23] NITRD の大規模データに関する活動紹介 http://www.nitrd.gov/subcommittee/bigdata.aspx
[24] 「ネットワーキングと情報技術研究開発プログラム（2013 年度大統領予算に対する補足）」、NITRD、p. 52 http://www.nitrd.gov/pubs/2013supplement/FY13NITRDSupplement.pdf

1.4. 次期連邦議会における ICT 研究開発政策動向

2011 年度 ICT 研究開発に関する連邦議会の姿勢

(1)NITRD 法案の今後

連邦議会は当初NITRDについて、1991 年HPC法によって連邦政府のHECプログラムを調整するために設置を承認した。連邦議会はNITRDの期限延長を 1998 年と 2007 年に行っている。下院では 2009 年と 2010 年にNITRDの期限延長もさることながら、その位置づけをより明確にするとともに、調整組織であるNCOの認定などを盛り込んだ法案「ネットワーキング及び情報技術研究開発法(Networking and Information Technology Research and Development Act)」[25](通称NITRD法案)を可決したものの、上院ではNITRD法案が、可決されず廃案となっている。尚、2007 年の期限延長に関しては、特に期限は設けられていない。

NITRD 法案は、NITRD に新たな規定をもたらすものである。これは、NITRD による戦略的計画を強化し、NITRD 参加機関に対して、同法が特定する優先事項について取組みを行うよう義務づけるものである。具体的な内容は、以下の通り:

- NITRD 参加機関間の計画及び調整を強化する。具体的には、①3 年毎に戦略計画の策定を義務づける、②戦略計画の策定と実施に係る厳密な監督を OSTP に委ねる、さらに③NITRD 参加機関が戦略計画をどのように支援しているかを示す年次報告書を発行することによって達成を目指す。

- 大統領科学技術諮問委員会(President's Council of Advisors on Science and Technology: PCAST)や新たな諮問委員会を設置した場合、これらの委員会間での密接な協力・連携を求める。

- 各機関における研究開発ポートフォリオが、より複数の省庁が支援するような長期的かつ学際的な研究への比重が増えるように、ポートフォリオ是正を促進する。

- 大学、産業、非営利研究機関及び連邦政府研究所の協力に基づく研究開発プログラムを支援する。研究開発プログラムは、技術移転の促進計画を奨励する。

- 各機関内において、基礎研究と技術実証を行えるような学際的な研究センターの設置を奨励する。

---

[25] 「ネットワーキング及び情報技術研究開発法」、http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.2020

- NITRD がサイバーフィジカル・システム、HCI 及び大規模データにおける研究開発を支援するよう義務づける。

- サイバーフィジカル・システムにおける協調的研究開発の機会を探るため、大学と産業からなるタスクフォースを招集する。

- NITRD に係る戦略計画の策定や活動アウトリーチを行うことも含め、連邦議会が認定する正式な組織として NCO を認定し、NITRD 運営組織に定める。

2011 年 9 月 21 日、下院科学宇宙技術委員会（House of Representatives Committee on Science, Space and Technology）の研究・科学教育小委員会（Subcommittee on Research and S cience Education）が公聴会を行い、NITRDのレビュー及びNITRD法案について審議を行い、NCO局長であるGeorge Strawn博士は、NITRD法案への支持を表明した[26]。

下院議員 Daniel Lipinski（共和党、イリノイ州）は、NITRD 法案を再提出し、2011 年後半に連邦議会で可決する可能性があることに関心を示したが、実現にはいたらなった。

NITRD公聴会と同じ日に、アメリカ・イノベーション・タスクフォース（Task Force for American Innovation: TFAI）は、連邦ICT 研究開発が米国の技術革新に、如何に貢献したかを実証するべく、下院でイベントを開催した。TFAIは、2004 年に設立され、米国の民間企業、大学、業界団体などをメンバーにする組織で、連邦政府による基礎研究開発への取り組みの重要性を提唱する団体である。同イベントは、「iPad分解：連邦政府が支援する研究がどのように考え方を根本から覆す技術革新を導いたか（Deconstructing the iPad: How Federally Supported Research Leads to Game-Changing Innovation）」と呼ばれ、iPadのほぼ全ての構成要素が連邦政府による研究開発活動・予算によって可能となったことを連邦議員及びスタッフに示した。同イベントは連邦議会の参加者から好評であったが、連邦議会のNITRDへの支援にどれだけ影響を与えたかという点は不透明である[27]。

（2）サイバーセキュリティ強化法案（Cybersecurity Enhancement Act）

2011 年 6 月 2 日、Michael McCaul下院議員（共和党、テキサス州）及びDaniel Lipinski下院議員（共和党、イリノイ州）は、2011 年サイバーセキュリティ強化法案を提出した[28]。

---

[26] 「研究・科学教育小委員会における George Strawn 氏の意見書」、研究・科学教育小委員会、2011 年 9 月 21 日 http://science.house.gov/sites/republicans.science.house.gov/files/documents/hearings/092211_Strawn.pdf

[27] “Q&A: iPad Deconstructed Forum Makes Case for Federal Research”、Computerworld、2011 年 9 月 22 日 http://www.computerworld.com/s/article/9220207/Q_A_IPad_deconstructed_forum_makes_case_for_federal_research

[28] 「サイバーセキュリティ強化法案」、http://thomas.loc.gov/cgi-bin/bdquery/z?d112:H.R.2096:

同法案によると、NITRD参加機関による個々の研究開発プログラム実施に関して、3 年毎に策定されるサイバーセキュリティ研究開発戦略計画に基づき、参加機関は他の参加機関と調整を行った上で行うことが定められている。また同法案の中には、OSTPが連邦／大学／産業から成るタスクフォースを招集し、コンソーシアムの設立と連邦議会へ勧告を提出することによって、協調的なサイバーセキュリティ研究開発への支援を議論することも明記されている。サイバーセキュリティ研究開発に関連するその他の条項は、以下の通りである:

- NSF サイバーセキュリティ助成金に関する予算を承認する。この中には社会、行動科学的視点からサイバーセキュリティに取り組む研究に対する助成金も含まれる。
- NSF が発起人である、「コンピュータ及びネットワークセキュリティ研究センター（Computer and Network Security Research Center）」に関する予算を承認する。またこの研究センターが、どのように連邦政府研究所や大学、産業、非営利研究機関とパートナーを組むかについても示すことが義務づけられている。
- NIST に対し、計算標準プログラムの一部として、内部のセキュリティ研究を行うよう義務づける。

下院科学宇宙技術委員会は 2011 年 7 月 21 日、サイバーセキュリティ強化法案を満場一致で可決した（ただし、下院本会議での採決ではない）。これを受けて、Robert Menendez 上院議員（民主党、ニュージャージー州）は、全く同一の法案を上院にて、2011 年 6 月 2 日に提出したが、上下院本会議における審議には至っていない。

1.5. 総論

2013 年度 NITRD 予算案は、ほぼ横ばい状態であった 2012 年度予算から 1.8%増となっている。しかし、NITRD 予算において、また最近の連邦 NITRD 機関の活動において、2012 年も目を離すことのできない重要な発展が多く見受けられる。

まず第一に、サイバーセキュリティ研究開発に対する強い支持がある点は、注目すべきポイントといえる。NITRD の CSIA 予算は、過去 2 年間で大きく伸びている。さらに、第 111 期連邦議会ではサイバーセキュリティ強化法案は可決されなかったが、同法案への関心の高まりと CSIA への予算配分が増加したことは、連邦議会による同分野における研究開発に対する支援を示すものである。このような傾向は、2011 年 12 月に発行された「信頼できるサイバースペース」報告書にも反映されており、2013 年以降のサイバーセキュリティ研究開発予算増大の必要性が記されている。

また、SDP 予算については、2012 年には、その予算が 28%増加して 1 億 9,580 万ドルとなったが、2013 年度の SDP 予算要求はほぼ横ばい状態である。NITRD の「ソフトウェア・エンジニアリングの未来」に関する報告書は、SDP 研究開発に対する幅広く、機関を

超えた視野を概観するものであり、各機関は研究開発の目標を特定し、その実行を目指して作業を進めることになる。しかし、こうした活動が今後どのように評価されるかは、現時点では不明であり、その結果が、2014 年度予算要求に反映されることになる。

同様に、BD SSG も 2011 年に設置され、大規模データ研究開発に関する報告書に取りかかっている。連邦政府が有する様々な大規模データの増大と、これらを分析する技術の進歩を考慮すると、連邦機関にとって大規模データに関する研究開発は、重要な科学的課題テーマであり、連邦機関における将来の ICT 研究開発予算において大きく成長する分野となりうる。

2010 年の中間選挙後、共和党が連邦議会にて議席を増やし、議会内での党派間対立が顕著になったため、2011 年は、議会における全ての法案審議が難航を極めた年であった。そのような状況において、ICT 研究開発予算は、他分野における全般的な予算削減の影響や、民主・共和両党における党派色の影響を、比較的受けなかった分野ともいえる。しかし、2012 年秋に行われる総選挙において、連邦議会における両党間の勢力構成や、大統領選の行方次第で、今後の ICT 研究開発予算も大きな影響を受ける可能性は十分にある。

	上院議員/下院議員	**委員会**	**2012 年任期満了に伴う改選有無**
上院	Daniel K. Inouye (民主党-ハワイ州) **委員長 (Chairman)**	歳出委員会 Appropriations	無
	Thad Cochran （共和党-ミシシッピ州） **ランキング・メンバー（Ranking Member）**	歳出委員会 Appropriations	無
	Barbara Mikulski （民主党-メリーランド州） **委員長（Chairman）**	歳出委員会 Appropriations －商業・司法・科学及び関連機関小委員会 (Commerce, Justice, Science, and Related Agencies)	無

	上院議員/下院議員	委員会	2012 年任期満了に伴う改選有無
	Kay Bailey Hutchison (共和党-テキサス州) **ランキング・メンバー（Ranking Member）**	歳出委員会 Appropriations ー商業・司法・科学及び関連機関小委員会 (Commerce, Justice, Science, and Related Agencies)	無
	John D. (Jay) Rockefeller, IV（民主党-ウェストバージニア州） **委員長（Chairman）**	商業科学・運輸委員会 Commerce Science, and Transportation	無
	Kay Bailey Hutchison （共和党-テキサス州） **ランキング・メンバー（Ranking Member）**	商業科学・運輸委員会 Commerce Science, and Transportation	引退
	Bill Nelson （民主党-フロリダ州） **委員長（Chairman）**	商業科学・運輸委員会 Commerce Science, and Transportation ー科学・宇宙小委員会 (Science and Space)	有
	John Boozman （共和党-アーカンソー州） **ランキングメンバー（Ranking Member）**	商業科学・運輸委員会 Commerce Science, and Transportation ー科学・宇宙小委員会 (Science and Space)	無
	John Kerry （民主党-マサチューセッツ州） **委員長（Chairman）**	商業科学･運輸委員会 Commerce Science, and Transportation ーコミュニケーション・技術・インターネット小委員会 (Communications, Technology, and the Internet)	無

	上院議員/下院議員	委員会	2012 年任期満了に伴う改選有無
	Jim DeMint （共和党-サウスカロライナ州） **ランキングメンバー（Ranking Member）**	商業科学･運輸委員会 Commerce Science, and Transportation －コミュニケーション･技術･インターネット小委員会 (Communications, Technology, and the Internet)	無
下院	Harold Rogers （共和党-ケンタッキー州） 委員長（Chairman）	歳出委員会 Appropriations	有
	Norm Dicks (民主党-ワシントン州) **ランキング･メンバー（Ranking Member）**	歳出委員会 Appropriations	有
	Frank Wolf （共和党-ヴァージニア州） **委員長（Chairman）**	歳出委員会 Appropriations －商業･司法･科学及び関連機関小委員会 (Commerce, Justice, Science, and Related Agencies)	有
	Chaka Fattah (民主党-ペンシルバニア州) **ランキング･メンバー（Ranking Member）**	歳出委員会 Appropriations －商業･司法･科学及び関連機関小委員会 (Commerce, Justice, Science, and Related Agencies)	有
	Rodney Frelinghuysen (共和党-ニュージャージー州) **委員長（Chairman）**	歳出委員会 Appropriations －エネルギー･水小委員会(Energy and Water)	有
	Peter Visclosky （民主党-インディアナ州） **ランキング･メンバー（Ranking Member）**	歳出委員会 Appropriations －エネルギー･水小委員会(Energy and Water)	有

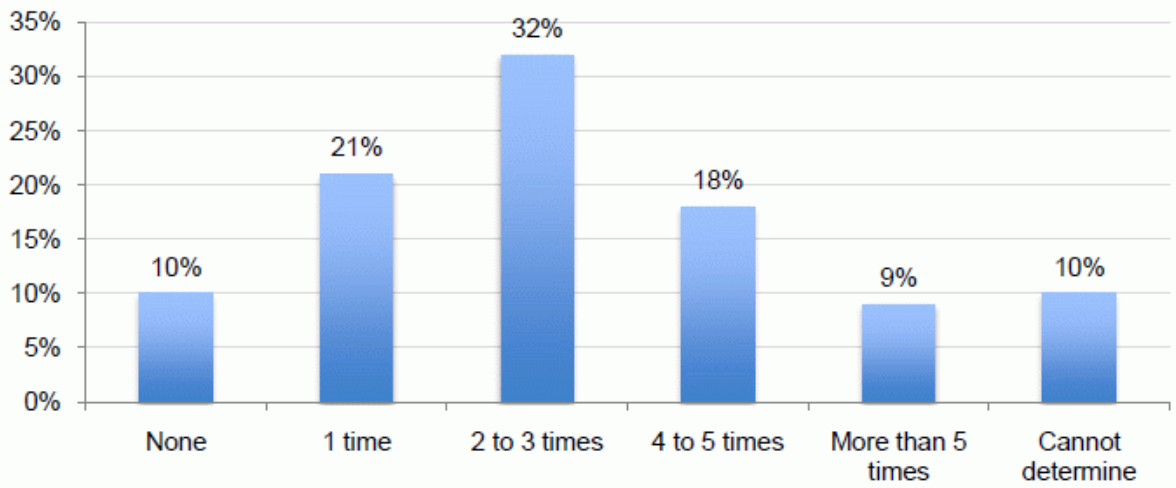
	上院議員/下院議員	委員会	2012 年任期満了に伴う改選有無
	Fred Upton (共和党-ミシガン州) **委員長（Chairman）**	エネルギー・商業委員会 Energy and Commerce	有
	Henry A. Waxman (民主党-カルフォルニア州) **ランキング・メンバー（Ranking Member）**	エネルギー・商業委員会 Energy and Commerce	有
	Greg Walden (共和党-オレゴン州) **委員長（Chairman）**	エネルギー・商業委員会 Energy and Commerce ーコミュニケーション・技術小委員会 (Communications and Technology)	有
	Anna G. Eshoo (民主党-カルフォルニア州) **ランキング・メンバー（Ranking Member）**	エネルギー・商業委員会 Energy and Commerce ーコミュニケーション・技術小委員会 (Communications and Technology)	有
	Ralph M. Hall (共和党-テキサス州) **委員長（Chairman）**	科学・宇宙・技術委員会 (Science, Space, and Technology)	有
	Eddie Bernice Johnson (民主党-テキサス州) ランキング・メンバー （Ranking Member）	科学・宇宙・技術委員会 Science, Space, and Technology	有
	Mo Brooks (共和党-アラバマ州) 委員長（Chairman）	科学・宇宙・技術委員会 Science, Space, and Technology ー研究科学教育小委員会(Research and Science Education	有
	Daniel Lipinski (民主党-イリノイ州) ランキング・メンバー （Ranking Member）	科学・宇宙・技術委員会 Science, Space, and Technology ー研究科学教育小委員会(Research and Science Education)	有

2. 米国におけるセキュリティ分野の研究開発に関する全体的な動向

2.1. 米国におけるサイバー攻撃予測・分析の技術開発に関する動向

米国におけるサイバー攻撃の数は年々増加傾向にあり、攻撃の手法も多様化、複雑化し、問題の深刻さが顕在化している。米ICT系シンクタンクのポネモン・インスティチュート（Ponemon Institute）がICTセキュリティ専門家を対象に実施した調査（2011 年）では、調査対象者の 59%が過去 12 ヶ月間で 2 件以上のセキュリティ障害を経験したと回答している。さらに 43%が同期間中にサイバー攻撃の頻度が著しく増加したとし、また 77%が問題の深刻化を指摘、あるいはサイバー攻撃の発見や阻止が難しくなったと回答している[29]。

米国 ICT 企業が受けたネットワークセキュリティ障害数の分布（2010～2011 年）



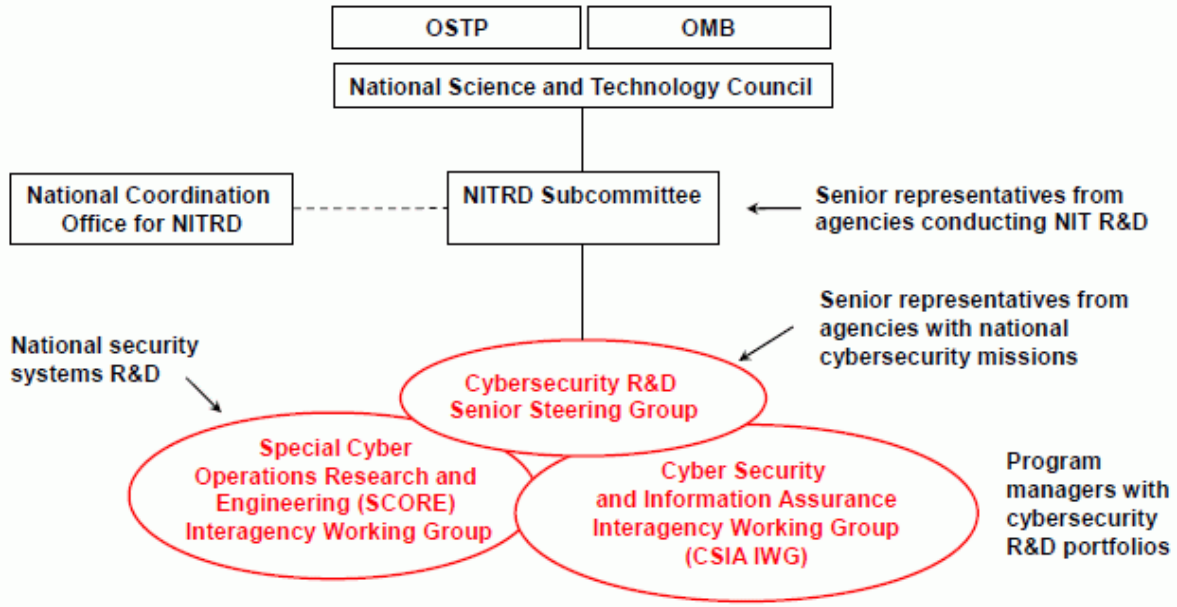
出典: Ponemon Institute[30]

このような状況を受けて連邦政府では、サイバーセキュリティに関連した研究開発活動を強化している。連邦政府では、先述のとおり、省庁横断型の研究開発プログラムとしてNITRD の中に、サイバーセキュリティに関して①Cybersecurity R&D Senior Steering Group、②Special Cyber Operation Research and Engineering Interagency Working Group（SCORE IWG）、③CSIA IWG の 3 つの作業部会を設置している。下図に示すように、NITRD は OSTP、OMB 及び NSTC の管轄下に置かれており、これらの機関とNSF や DOD、NIST の上席研究員やプロジェクトマネージャが参加する NITRD 下の作

[29] ポネモン・インスティチュートの調査結果
http://www.juniper.net/us/en/company/press-center/press-releases/2011/pr_2011_06_22-08_00.html
[30] 「ネットワークセキュリティに関する予測」、ポネモン・インスティチュート、2011 年 6 月（p.3）
http://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf

業部会とで、優先して取り組むべき技術分野を特定するなど研究開発の方針について連携・調整を行なっている。

NITRD のサイバーセキュリティ研究開発コーディネーション体制



出典: NITRD[31]

NITRDにおけるサイバーセキュリティ研究開発に関連した最近の動向では、2010 年、CSIA IWGが、連邦機関においてサイバーセキュリティ分野で「ゲームチェンジャー」となりえる技術を特定し、特定した技術の研究開発を推進することを目的とした「連邦サイバーセキュリティ・ゲームチェンジ・研究開発アジェンダ（Federal Cybersecurity Game-change R&D Agenda）」を発表している[32]。同アジェンダにおいて、NITRDは、2011 年研究開発を優先的に推進するべき技術分野として、サイバー攻撃予測・分析、設計済みセキュリティ、そして暗号技術の応用の 3 つを特定した[33] [34]。本章では、NITRDが特定したこれらの 3 分野における最近の取組み状況を紹介する。

---

[31] NITRD「サイバーセキュリティの概観」プレゼンテーション資料」01_NITRD_TTSW_Intro.pdf、2011 年 6 月（p.3）、http://www.nitrd.gov/fileupload/files/NITRD_TTS_Workshop_JUL2011.pdf

[32] 「サイバーセキュリティ・ゲームチェンジ研究開発勧告」、NITRD CSIA IWG、2011 年 5 月 http://www.nitrd.gov/pubs/CSIA_IWG_%20Cybersecurity_%20GameChange_RD_%20Recommendations_20100513.pdf

[33] 「サイバーセキュリティ・ゲームチェンジ研究開発勧告」、NITRD CSIA IWG、2011 年 5 月(p.2 と p.5) http://www.nitrd.gov/fileupload/files/CSIAIWGCybersecurityGameChangeRDRecommendations20100513.pdf

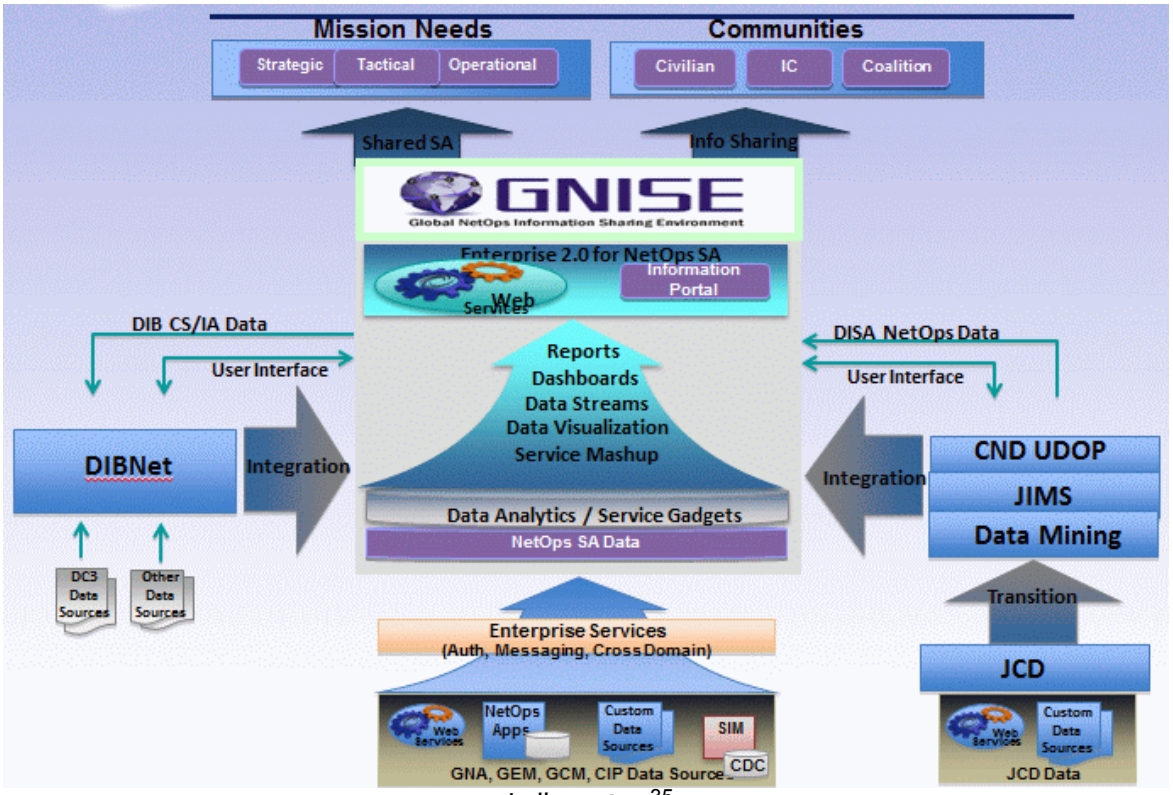
[34] 「信頼できるサイバースペース~連邦サイバーセキュリティ研究開発プログラム」、NITRD、2011 年 12 月（p. 5） http://www.nitrd.gov/fileupload/files/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf

2.1.1. 米国におけるサイバー攻撃予測・分析の技術分野に関する取り組みの概要

サイバー攻撃の予測・分析に非常に有効な戦略として注目されている技術に、状況認識（Situational Awareness）技術がある。状況認識技術を活用することで、ネットワークを随時監視してサイバー攻撃を事前に検出することができ、またネットワーク管理者が様々なサイバー攻撃についてその影響力の程度を判断し、とるべき対応策を優先付けできるようになる。状況認識では、大量に蓄積されたデータを解析し、サイバー攻撃のパターンを抽出・特定するデータマイニング（Data Mining）、及び特定したパターンを基に起こり得る攻撃を予測、さらにその予測に基づいてセキュリティシステムを最適化する予測モデリング（Prediction Modeling）の技術が使用される。

データマイニング及び予測モデリングを取り入れることで、分析結果からある一定の攻撃パターンを導き出し、パターンを基に将来起こり得る攻撃を予測するというように、攻撃を受けてから対策を練るのではなく、攻撃を受ける前に適切な予防策を講じられるようになる、また想定される新種の攻撃に対する予測をすることも可能となる。このように状況認識を活用することで、連邦政府機関において、先を見越して脅威を監視・検出し、ネットワークに問題が発生する前に予防策を講じることができる効果的なリスクマネジメントの枠組みやサイバーセキュリティシステムを構築することができるようになる。下図に示すのは、DOD の状況認識フレームワークである。

DOD の状況認識フレームワーク



出典: DOD[35]

上図に示されるように DOD の状況認識フレームワークの中核をなすのが、国防情報システム局（Defence Information Systems Agency: DISA）下において DOD の情報システムやネットワークの監視・防護を担当するコンピュータ・ネットワーク防護部（Computer Network Defense: CND）、及び DOD と国防・軍事関連業界の情報共有を推進することを目的に DoD 下に設置されている官民連携プログラムである Defense Inndustrial Base（DIB）Cyber Security/Information Assurance（CS/IA）プログラムにおけるデータを収集・統合・分析する状況認識システムである Global NetOps Information Sharing Environoment（GNISE）である。GNISE では、CND 及び DIB CS/IA を通じて取得したデータを統合・分析し、軍・国防関連の全情報システム及び通信ネットワークの利用状況や、システム及びネットワーク上で発生している問題、異常、脅威・攻撃などに関する最新の情報をリアルタイムで軍の指揮官や意思決定を行う立場にいる軍関係者に提供しており、状況認識が各ミッションにおけるリスクマネジメントや意思決定の迅速化に繋がる体制を構築している。

---

[35] 「サイバードメイン状況認識」プレゼンテーション資料、Carey, Robert, DOD、2011 年 6 月（P. 16）
www.afcea.org/events/intelforum/11/DoD_CIO_AFCEA_Brief_Jun11_v19.pptx

連邦政府におけるサイバー攻撃予測・分析の技術開発に関する経緯

DODの次席情報官Robert Carey 氏は 2011 年 6 月、サイバー攻撃及びネットワークやコンピュータシステムが複雑化する中で、従来の技術では対処することができない状況に陥っており、状況認識の研究開発の必要性について指摘している。現在ネットワーク攻撃の検出・特定に使用されている警告相関手法は[36]、データマイニングに依存しているが、侵入検知システムセンサからその場で警告されるデータを取得するデータマイニングだけではシンプルな攻撃には対応できても高度化・複雑化したサイバー攻撃に対して誤検知などの問題が発生する可能性が高く、拡張性も低いことから、新たなサイバー攻撃の検知は極めて難しい。高度化・複雑化するサイバー攻撃に対しては、パターン化した長期のデータ・情報を貯蓄してあるナレッジ・データベースを参照し、過去の大量のデータ・情報から攻撃者の行動パターンを抽出・分析し、予測をモデル化する必要がある。サイバー攻撃が高度化・複雑化する中で、サイバースペース管理において正確な状況認識、およびサイバー攻撃にどのように対応するかなど意思決定の迅速化が求められており、これらの実現のためにはCarey 氏が指摘するように、次世代のネットワーク管理及びサイバー攻撃検知システムの開発が求められている[37]。

連邦政府の ICT 研究開発ポートフォリオにおける位置づけ

連邦政府においてサイバー攻撃予測・分析に関連する研究開発に最も取り組んでいる機関は、DODとDHSである。中でもDODはサイバー攻撃予測・分析技術の開発に力を入れており、空軍研究所（Air Force Research Laboratory: AFRL）及び陸軍研究所（Army Research Laboratory: ARL）陸軍研究室（Army Research Office: ARO）が公募を通して、研究機関や非営利組織、民間企業の研究開発プロジェクトに対し研究資金を拠出している。これまでに研究資金が支給されているプロジェクトには、AFRLが支援している先進的なサイバー攻撃モデリング、分析、可視化技術の研究開発を目指したジョージ・メイソン大学（George Mason University: GMU）の研究プロジェクトや[38]、AROが資金を拠出する、サイバー防護を目的にペンシルバニア大学（Pennsylvania State University）がアリゾナ州立大学（Arizona State University）、カーネギー・メロン大学（Carnegie Mellon University: CMU）、GMU、メリーランド大学（Univeristy of Maryland）の研究者と共同で実施しているサイバー状況認識プロジェクト[39]、さらにカリフォリニア大学サンタバーバラ校（University of California, Santa Barbara: UCSB）がカリ

---

[36]警告相関手法とは、侵入検知システム（Intrusion Detection System: IDS）センサが生成した生の警告を管理する手法である。このアプローチでは、生の警告を削減、融合、相互関連付けることにより、ネットワーク上におけるセキュリティ脅威に関する分析データを得られるようにする。

[37]「サイバードメイン状況認識」プレゼンテーション資料、Carey, Robert, DOD、2011 年 6 月
www.afcea.org/events/intelforum/11/DoD_CIO_AFCEA_Brief_Jun11_v19.pptx

[38]「先進サイバー攻撃モデリング、分析、可視化」、GMU、2010 年 3 月
http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA516716

[39]「サイバー状況認識研究費に 600 万ドル取得」、ペンシルバニア州立大学、2009 年 7 月 1 日
http://www.hss.cmu.edu/departments/sds/ddmlab/papers/40372.pdf

フォルニア大学バークレー校（University of California, Berkeley: UCB）とジョージア工科大学（Georgia Institute of Technology）と共同で進めるサイバー攻撃の分析、予測、可視化を可能にするサイバー状況認識フレームワークの策定プロジェクトなどがある[40]。

また、サイバー攻撃予測・分析技術の研究開発については、前出のNITRDにおいても注目されている。NITRDは、2011 年 6 月 20 日、サイバー攻撃予測・分析に関するワークショップ「異常な行動の特定が悪意ある者を検知する（Abnormal Behavior Detection Finds Malicious Actors）」を開催している。同ワークショップでは、異常な行動の検知技術が、悪意ある攻撃の発見に失敗する状況を解明することで、攻撃を予測するための、これまでにない新しいアプローチを特定するようなアイデアの創出を目指して、学術・研究機関、民間企業、政府機関からの参加者間で議論が行われた[41]。特に、異常な行動の特定・分析、サイバー攻撃検知において積極的な対策をとっている金融機関における取組みが注目された。NITRDは、同ワークショップの報告書において、今後研究が必要な課題として以下の 5 点を挙げている[42]。

- サイバースペースにおいて悪意ある行為に発展する可能性がある行動の定義、特定、モデリング
- 金融業界における取組みや行動科学など、サイバー攻撃予測・分析において有用できる分野・項目の特定
- 悪意ある攻撃に関わる人的要素（意思決定など）の特定
- 悪意ある攻撃を分析する新たなアプローチ
- 悪意ある攻撃に対する積極的な防護策

---

[40] 2009 年度多分野大学研究イニシアチブによる出資プロジェクト一覧
http://www.defense.gov/news/may2009/FY09MURIPressReleaseTableFinal.pdf（p.8）
[41] 「異常な行動の特定が悪意ある者を検知する」、NITRD
http://www.nitrd.gov/fileupload/files/MaliciousBehavior_2011_NITRD_workshop.pdf
[42] 「異常な行動の特定が悪意ある者を検知するワークショップ最終報告書」、NITRD
http://www.nitrd.gov/fileupload/files/Assumption_Busters_Workshop_Malicious_Behaviors_Final_Report.pdf

2.1.2. 連邦政府が支援するサイバー攻撃予測・分析の技術開発に関する主要プログラムのプロフィール

（1）DHS

①アインシュタイン 3（Einstein 3）[43] [44]

DHSは、「2002 年国土安全保障法（Homeland Security Act of 2002）」[45]に則り、米国の重要インフラを物理的攻撃かつサイバー攻撃から保護する役割を担う機関として設置された。DHS下にセキュリティ関連の研究開発を担当する科学技術局（Science and Technology Directorate）を設置しており、サイバーセキュリティについても同局が管轄している。DHSでは、サイバーセキュリティに関連して独自に作成した研究開発に使用するツールやデータレポジトリを他の研究機関でも有効的に活用できるよう広くアクセスを許可している。データレポジトリに関しては、技術研究者や製品開発者が最新のサイバーセキュリティに関する研究開発データにアクセスできるようにオンライン・データレポジトリであるPREDICT（Protected Repository for the Defense of Infrastructure Against Cyber Threats）を立ち上げている。

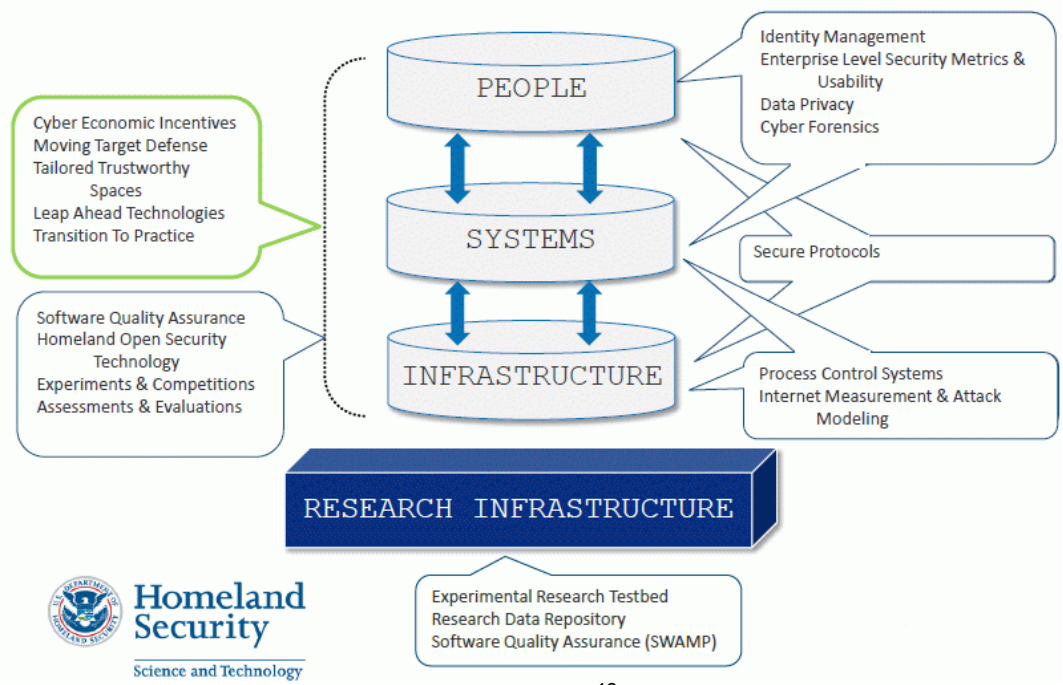
---

[43] 「CNCI イニシアチブ 3 の評価」、DHS、2010 年 3 月 18 日
（CNCI には、合計 12 のイニシアチブが掲げられており、NSA との連携はイニシアチブの 3 つ目にあたる）
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3.pdf

[44] アインシュタインは、国家サイバーセキュリティ保護システム（National Cyber Security Protection System）とも称される。

[45] 「2002 年国土安保障法」、DHS　http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf

DHS 科学技術局サイバーセキュリティに関する研究開発優先事項



出典: DHS[46]

2003 年 9 月、DHS 科学技術局の国家サイバーセキュリティ部（National Cyber Security Division: NCSD）下に、サイバー攻撃からインターネットインフラを保護することを目的として米国コンピュータ緊急事態対策チーム（United States Computer Emergency Readiness Team: US-CERT）が設置された。US-CERT は、サイバー攻撃と脆弱性の分析と削減、サイバー脅威に対する警告情報の発信、及び問題が発生した際の対応策について DHS 以外の連邦政府機関をはじめとして州・地方政府、民間企業、研究機関などと連携する役割を担っている。

このUS-CERTが管轄するプログラムにアインシュタイン・プログラムがある。アインシュタイン・プログラムは、連邦政府間で連携してサイバーセキュリティに関する情報の収集・相互関連付け、共有を進め、連邦政府のネットワークを監視、悪意のあるサイバー攻撃を自動的に検知し、攻撃を阻害できるシステムを段階的に構築・導入することを目的としている[47]。

---

[46] 「先進サイバーセキュリティ研究開発」プレゼンテーション資料（p. 15）、Maughan, Douglas, DHS. 2011 年 9 月
http://www.massinsight.com/cms_page_media/183/MITRE%20-%20ACSC%20-%20Maughan%20-%2020Sep2011.pdf

[47] Einsteini プログラム概要紹介
http://fcw.com/articles/2010/03/19/einstein-3-test-intrusion-prevention-system.aspx

アインシュタイン・プログラムについては、第 1 及び第 2 フェーズはすでに完了しており、現在は第 3 フェーズ（アインシュタイン 3）にある。アインシュタイン 2 では、サイバー攻撃検知システムの発展に注力し、各連邦政府機関と協力して、連邦政府機関のICTシステムに接続されるIPアドレスや接続時間、接続ポート等についての通信データトラフィック情報を収集・分析・共有することで、セキュリティの脅威やネットワークの脆弱性への対応に共同で取り組まれた。アインシュタイン 3 では、サイバーセキュリティの分析、状況認識、対策を強化するため、不審なサイバー活動の検知だけでなくその未然防止に焦点を当てたシステムの開発・導入が進められている[48]。アインシュタイン 3 は、国家安全保障庁（National Security Agency: NSA）によって開発が進められており、NSAのサイバー侵入を自動検知する技術を採用し、悪意ある侵入を防止する機能が追加される計画である。DHSは 2011 年、CNCI[49]の一環として、NSAと連携して、NSAが開発した技術を導入してアインシュタイン・システムのパイロットを開始した。パイロットでは、状況認識を強化する目的でほぼリアルタイムに近い脅威情報の共有を行うことを目指しており、連邦政府における情報保護と情報管理プロセスの基盤構築を進めている[50]。パイロットの実施は 2011 年 3 月 18 日にDHSより発表されたが、その後のパイロットの実施状況に関する情報は発表されていない[51]。

アインシュタイン 3 は、センサを利用して侵入者のパターン情報を収集し、その情報を侵入者のアルゴリズムを阻止するために利用することから、「積極防御（active defense）」タイプのサイバーセキュリティ・メカニズムとして知られる[52]。侵入者のパターン情報については、NSAを通じて米国の海外諜報活動やDODの業務から特定したサイバー脅威のパターンに関するデータ・情報を随時アイシュタイン 3 にアップデートし、常に最新のサイバー脅威に対しても侵入前に検知できるようなシステムを整備する。

アインシュタイン 3 については、DHS 内だけでなく、今後金融機関、財務省、国立研究所（特に核関連の研究施設）、及び DOE など国家の重要セクタのネットワーク保護にも拡大し適用することを目指している。

予算に関してDHSは、コンピュータ・システムへの侵入を防止し検知するためのアインシュタイン3の開発の加速と、連邦ネットワークを保護する侵入検知機能と解析機能を構築することを目的として、2012 年度予算で総額 2 億 3,360 万ドルを要求している[53]。

---

[48] 「CNCI イニシアチブ 3 の評価」、DHS、2010 年 3 月 18 日
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3.pdf
[49] CNCI 概要紹介
http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative
[50] パイロットの実施概要　http://www.dhs.gov/ynews/testimony/testimony_1300283858976.shtm
[51] 「CNCI イニシアチブ 3 の評価」、DHS、2010 年 3 月 18 日
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3.pdf
[52] 「サイバー防護パイロットプログラムに関する報告書」（Aerospace Daily & Defense Report）， 2011 年 8 月 19 日
[53] 「DHS2012 年度予算」、DHS、http://www.dhs.gov/xlibrary/assets/budget-bib-fy2012.pdf

②CAESARS[54]

DHS の継続的資産評価・状況・リスク評価（Continuous Asset Evaluation, Situational Awareness, and Risk Scoring: CAESARS）参照アーキテクチャは、情報セキュリティ・プログラムにおいてリスク評価の原則を導入しようとしている他の連邦機関に対して、様々なモニタリング及びリスク評価システムの概念を提供するものである。CAESARS は、詳細な技術的及び機能的要件の発展や、自動モニタリング及び状況認識と同様の機能を持つツールの設計に利用されることが想定されている。

CAESARSは、継続的な査定・評価を実施するという点において、多くの連邦政府機関が利用している従来の、未適用パッチや脆弱性、承認された設定との相違、及びセキュリティポリシー違反などの情報セキュリティリスクを監視・査定する自動化ツールとは異なる。これらの自動化ツールは、基本的に脆弱性やリスクを査定・評価し、その情報をネットワークのオペレーションセンタや情報セキュリティを管理するオペレーションセンタに提供することのみを目的として設計されている。各連邦政府機関では、リスクの査定・評価情報を基に、リスクに対して改善策を自動的に実行するという内容を「対応方針及びマイルストーン（Plans of Actions and Milestones）」に取り入れることもできるが、従来の自動化ツールでは潜在的なリスク削減を目的とした継続的なリスク査定・評価を実施していないことから、数量的・客観点評価に基づいてとるべき改善策の優先付けをすることができず、リスクに対して最善の改善策をとることはできない[55]。

これに対し、CAESARS は以下のような特徴を有する:

- ICT 資産管理の現状査定
- セキュリティに関して最低限満たすべき要件と現状のギャップの査定
- 上記で査定したギャップあるいは偏差の相対的リスクの定量的測定
- 全サイトとシステムの統合リスクを、分かりやすいシンプルなかたちで提示
- 全システムとサイトに対する責任が正しく任命されているかの確認
- リスク削減を目的として重要な修正を行えるよう、セキュリティ及びシステム管理者へ必要な情報を提供

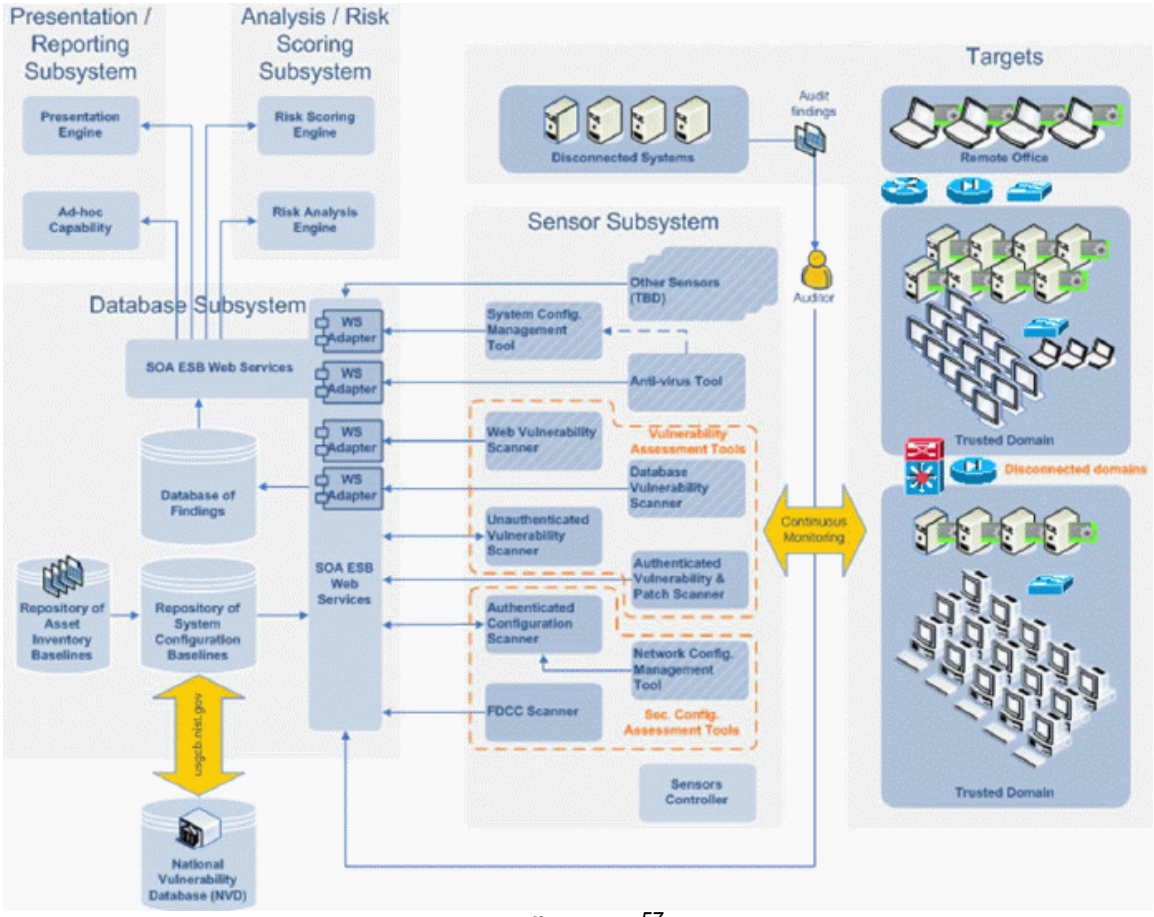
下図に示されるように、CAESARSアーキテクチャは、相互接続された 4 つのサブシステムによって構成される[56]:

---

[54] 「CAESARS 参照アーキテクチャ報告書」、DHS、2010 年 9 月
http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf
[55] 「CAESARS 参照アーキテクチャ報告書」、DHS、2010 年 9 月（p. 8）
http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf
[56] 「CAESARS 参照アーキテクチャ報告書」、DHS、2010 年 9 月 (p. 9-13).
http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf

- センサ・サブシステム（Sensor Subsystem）
- データベース／レポジトリ・サブシステム（Database/Repository Subsystem）
- 分析／リスク評価・サブシステム（Analysis/Risk Scoring Subsystem）
- プレゼンテーションと報告・サブシステム（Presentation and Reporting Subsystem）

CAESARS アーキテクチャ



出典: DHS[57]

CAESARS は、ネットワークで接続されたデバイスのセキュリティ状態に関して技術的詳細を可視化するシステムであり、同システムを活用することで意思決定を支援するリアルタイムかつ優先度の高い情報を効果的に抽出することができる。CAESARS の中核を構成するのが、データベースであり、このデータベースにはセンサより報告される ICT 資産状況に関するデータの他、データの整合性を維持するためのルール、各資産のリスク評価を算出するためのアルゴリズム、セキュリティ修正を実施する担当機関や個人名など

[57] 「CAESARS 参照アーキテクチャ報告書」、DHS、2010 年 9 月(p.11).
http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf

のデータや情報がインプットされている。

（2）NSF

NSFにおけるサイバーセキュリティ研究開発プログラムとしては、同機関のコンピュータ・ネットワーク・システム（Computer Network Systems: CNS）部が管理する、「信頼できるコンピューティング（Trustworthy Computing: TC）」プログラムが代表的なプログラムとして設置されていた。TCプログラムは、セキュリティ、信頼性、プライバシー、有用性を強化した信頼できるコンピューティング環境の基盤を構築することを目標として設定されたプログラムで、同プログラムを通じてシステムの信頼性を査定・分析する手法や信頼できるコンピュータ環境のシミュレーション技術の開発などが目指されていた[58]。NSFが2011年度TCプラグラムを通じて研究資金を支給したサイバー攻撃予測・分析に関わるプロジェクトには、攻撃を受けている最中でもネットワークやシステム上で何が起きているか問題を関連付け、根本的な原因を正確に描写できる技術の開発を進めるジョージタウン大学（Georgetown University）の研究プロジェクトや[59]、後述するUCSBのNexsat開発プロジェクトが挙げられる[60]。

NSFは、2011 年 10 月、TCプログラムに代わる新たなサイバーセキュリティ研究開発プログラムとして「セキュアで信頼できるサイバースペース（Secure and Trustworthy Cyberspace: SaTC）プログラムを設置しており、これまでTCプログラムを通じて資金が拠出されていた研究プロジェクトも現在はSaTCプログラムを通じて研究資金が出資されている。SaTCプログラムでは、TCプログラムと比較して、研究プロジェクトの実施にあたりより他分野・他機関との連携強化に力を入れており、SaTCプロジェクト自体もCNS部単独によるプログラムではなく、CNSとNSFの社会・行動・経済科学部（Social, Behavioral, & Economics Sciences）、数学・物理科学部（Mathematical and Physical Science）、及びサイバーインフラ局（Office of Cyberinfrastructure）が共同で推進するプログラムとなっている[61]。SaTCプログラムでは、2012 年度総額 5,000 万ドルを投じて 60 以上の研究プロジェクトを支援する予定である。同プログラムでは、研究プロジェクトの公募を 2011 年 12 月に開始し、2012 年 2 月締め切ったところである[62]。2012 年 3 月末時点で 5 つの研究プロジェクトが発表されているが、サイバー攻撃予測・分析に関するプロジェクトは含まれていない。

---

[58] TC プログラム概要説明　http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503326&org=CNS
[59] TC プログラムにおける GMU 研究プロジェクトの概要
http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=1064986
[60] 「Nexat プロジェクト」概要　http://seclab.cs.ucsb.edu/media/uploads/papers/2011_nexat.pdf
[61] SaTC の設立に関する説明　http://www.cccblog.org/2011/11/22/nsf-launches-secure-webinar-scheduled/
[62] SaTC 研究プロジェクト公募内容　http://www.nsf.gov/pubs/2012/nsf12503/nsf12503.htm

NITRDの 2012 会計年度予算補足資料によると、NSFのサイバーセキュリティ研究開発予算は約 7,140 万ドルである[63]。

（3）DOD

NITRDの 2012 会計年度予算補足資料によると、DODがサイバーセキュリティ分野の研究開発に割り当てている予算総額は 8,650 万ドルである[64]。サイバー攻撃予測・分析の研究開発に特化した予算については、公開されていない。

DODにおいて科学技術分野の研究活動を担当する国防研究技術局（Office of the Director of Defense Research & Engineering: DDR&E）[65]は、DODの研究開発プログラムを調整・監督しており、サイバーセキュリティに関連する研究開発も推進している。DDR&Eは、サイバーセキュリティの研究開発に関して、予測モデリングツールの開発や状況認識の提供を優先的な研究課題として挙げている[66]。

DODの研究機関であるAFRL及びAROは、サイバー状況認識と予測攻撃モデリングに関連する研究開発を積極的に支援している。DODでは、大学機関における防衛・軍事分野に関連した研究開発を支援するイニシアチブとして、Multidisciplinary University Research Initiative（MURI）を設置しており、AFRLとAROは同イニシアチブの一環でサイバー攻撃予測・分析に関連する研究開発プロジェクトに資金を拠出している[67] [68]。現在、MURIを通じてサイバー攻撃予測・分析に関連して資金が拠出されているプロジェクトには、後述するUCSBのサイバウェア（Cybaware[69]、GMUの位相脆弱性分析（Topological Vulnerabily Analysis: TVA）[70]、ペンシルバニア州立大学の攻撃予測にゲーム理論を用いるアプローチに関する研究[71]などのプロジェクトがある。

---

[63] 「ネットワーキングと情報技術研究開発プログラム（2012 年度大統領予算に対する補足）」、NITRD、2011 年 2 月（p. 28） http://casc.org/papers/FY12NITRDSupplement.pdf

[64] 「ネットワーキングと情報技術研究開発プログラム（2012 年度大統領予算に対する補足）」、NITRD、2011 年 2 月（p. 28） http://casc.org/papers/FY12NITRDSupplement.pdf

[65] DDR&E に関する概要紹介 http://www.defense.gov/OrgChart/office.aspx?id=92

[66] DDR&E プレゼンテーションテーション資料、2010 年 10 月 19 日（p. 39）
http://www.afcea-aerotech.org/InfoTech2010/media/Honey.pdf

[67] MURI を通して研究開発費が支援されるプロジェクトの実施機関は、最大 5 年に設定されている（基本的には 3 年に設定されているが、プロジェクトの規模が大きい場合にはオプションとして 2 年間延長することも可能である）

[68] MURI のプロジェクト概要 http://www.arl.army.mil/www/default.cfm?page=472

[69] UCSB のサイバウェアプロジェクト概要 http://seclab.cs.ucsb.edu/academic/projects/projects/cybaware/

[70] 「先進サイバー攻撃モデリング、分析、可視化」、GMU、2010 年 3 月
http://www.dtic.mil/dtic/tr/fulltext/u2/a516716.pdf

[71] 「攻撃予測に対するゲーム理論アプローチ」、ペンシスバニア州立大学 http://s2.ist.psu.edu/paper/predict.pdf

2.1.3. サイバー攻撃予測・分析の技術分野に関する研究開発活動を行なっている主要研究所

（1）UCSB

＜研究機関プロフィール＞
UCSBでは、コンピュータ・セキュリティ・グループ（Computer Security Group）が安全なソフトウェア・システムを開発するためのツールや技術の研究開発に取り組んでいる。コンピュータ・セキュリティ・グループは、およそ 30 年前にRichard Kemmerer博士により信頼できるソフトウェア・グループ（Reliable Software Group）として設置された[72]。Kemmerer博士は、現在もUCSBに勤務しており、UCSBのコンピュータサイエンス・リーダーシップ議長（Computer Science Leadership Chair）として同グループを主導する立場にある。Kemmerer博士の他、主要な研究者には、UCSBのコンピュータ科学部門の教授であるChristopher Kruegel博士とGiovanni Vigna博士がいる[73]。

コンピュータ・セキュリティ・グループでは、特に侵入検知と攻撃の相互関係付け、脆弱性分析、マルウェア検出と防止、そしてウェブベース・アプリケーションのセキュリティの研究に焦点を当てている[74]。後述するサイバウェア（Cybaware）を始めとして複数の研究プロジェクトを実施しており、これまでにARL、ARO、DARPA、NSF、NSAなどの連邦政府機関から研究資金を取得している他、オラクル（Oracle）、シーメンズ（Siemens）、ユニシス（Unisys）、ヴィーエムウェア（VMWare）など米国の大手IT企業からも研究資金の援助を受けている。研究プロジェクトの実施にあたっては、他大学や国際的な研究機関の研究者とも積極的に連携しており、ノースイースタン大学（Northeastern University）のコンピュータサイエンス学部教授のEngin Kirda博士とは、ウェベースの侵入検知、スパイウェア検知、ワーム検出方法・技術の研究プロジェクトで協力している[75]。また、欧州のサイバーセキュリティ研究コンソーシアムである国際セキュア・システムズ研究所（International Secure Systems Lab: ISEC Lab）のThorsten Holz博士とは、サイバー攻撃者が悪意ある攻撃で乗っ取った複数のコンピュータで構成されるネットワークであるボットネット（Botnet）の分析・対策を進めるプロジェクトで連携している[76]。

---

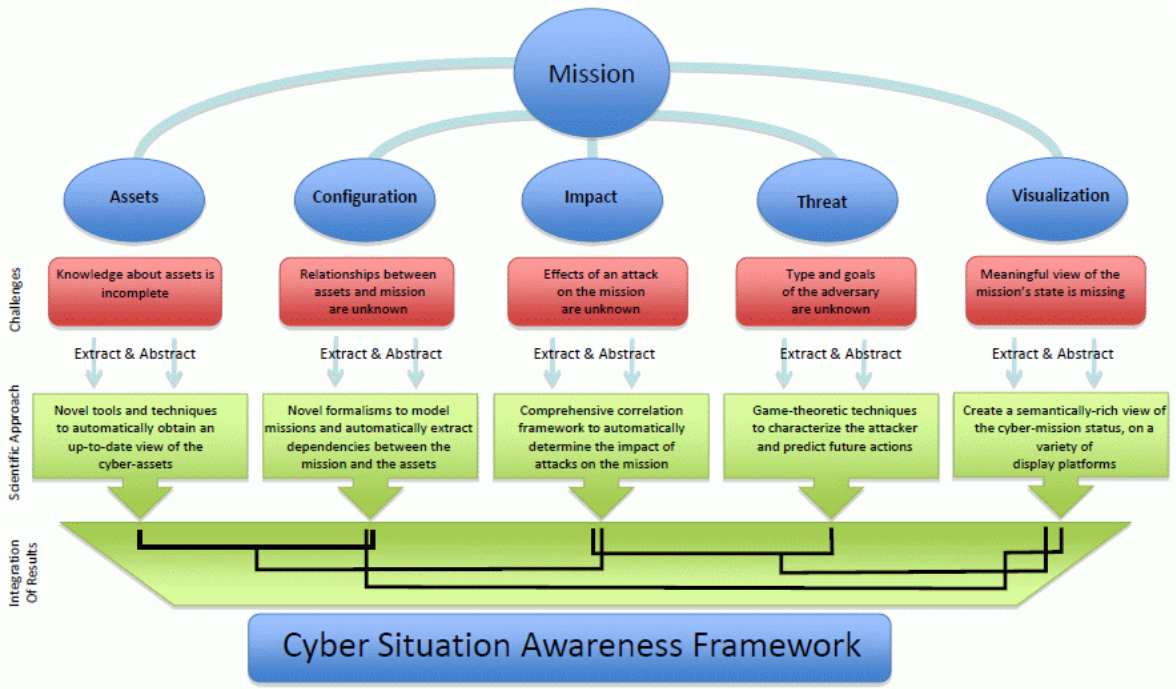
[72] コンピュータセキュリティグループ概要説明 http://www.cs.ucsb.edu/~seclab/
[73] コンピュータセキュリティグループの研究者 http://www.cs.ucsb.edu/~seclab/people.html
[74] コンピュータセキュリティグループ 実施プロジェクト概要説明 http://www.cs.ucsb.edu/~seclab/projects.html
[75] ノースイースタン大学 Kirda 博士と連携して実施しているプロジェクト概要説明
（http://seclab.cs.ucsb.edu/academic/projects/projects/web-based-intrusion-detection/、
http://seclab.cs.ucsb.edu/academic/projects/projects/spyware-detection/、
http://seclab.cs.ucsb.edu/academic/projects/projects/worm-detection/
http://seclab.cs.ucsb.edu/academic/projects/projects/disasm/）
[76] ISEC Lab と連携して実施しているプロジェクトの概要
http://seclab.cs.ucsb.edu/academic/projects/projects/botnet-analysis-and-mitigation/

＜研究プロジェクト概要＞

①サイバウェア[77]

現在同グループでは、サイバー攻撃分析・予測、そして可視化のためのサイバー状況認識フレームワークの構築を目指して、複数の大学機関と連携してサイバウェアプロジェクトを実施している。サイバウェア・プロジェクトは、2009 年に前出のMURIのプロジェクトの一環としてAROから 620 万ドルのプロジェクト資金支援を得て始まった。プロジェクトはコンピュータ・セキュリティ・グループが主導し、その他の、共同研究機関としてUCSBのSECLABコンピュータ・セキュリティ・グループ（SECLAB Computer Security Group）、UCB、及びジョージア工科大学が参加している[78]。

サイバウェアのフレームワーク



出典:UCSB[79]

上図に示されるように、サイバウェア・プロジェクトでは、ハッカーの侵入が任務や業務の成果に与える影響力や被害の推定、インターネットに対する攻撃や攻撃に対する対応策の特定、及び将来的な脅威の予測を実施するためのフレームワークの設計が進められ

---

[77] サイバウェアプロジェクトの概要　http://seclab.cs.ucsb.edu/academic/projects/projects/cybaware/

[78] 「サイバウェア：攻撃分析、予測、可視化のサイバー認識フレームワーク」プレゼンテーション資料、Kemmerer, Richard, UCSB、2011 年 9 月 9`日
http://www.cs.ucsb.edu/~tim/cybaware_web/dwnld/yr2/kemmerer_overview.pdf

[79] 「サイバウェア：攻撃分析、予測、可視化のためのサイバー認識フレームワーク」、Kemmerer, Richard. 、2011 年 9 月 9 日（p. 4）http://www.cs.ucsb.edu/~tim/cybaware_web/dwnld/yr2/kemmerer_overview.pdf

ている。同プロジェクトでは、最終的に上記のフレームワークを利用して、自動的に利用可能なICT資産を査定し、任務や業務に必要な資産を特定できる新たな状況認識理論と技術の開発を目指している。上記のフレームワークにおいて最も重要なことは、任務・業務の遂行を阻害する可能性がある攻撃・脅威を事前に予測するために、攻撃者の行動をモデル化できる点にある。同フレームワークを通し、特定された任務・業務の現状や将来受ける可能性のあるサイバー攻撃の予測、また各攻撃が任務・業務に及ぼす影響力に関する情報は、セキュリティ担当者に共有される[80]。
サイバウェア・プロジェクトでは、以下に示す 5 つの主要な研究領域を定めている:

1. ネットワーク使用状況(ICT 資産がどのように使われているかなど)を随時把握するための、ネットワーク活動を自動的に分析する堅牢かつ実用的な技術の考案
2. ネットワーク内の関係と従属状態(サイバー関連任務と ICT 資産間の関係など)に関する情報を自動的に抽出するための、包括的分析テクニックの開発
3. サイバー攻撃の影響力を推定することを目的として、サイバー攻撃の標的を特定し、ICT 資産や各攻撃の相互関係を示すための状況認識フレームワークの構築
4. 将来受ける可能性がある攻撃を予測するため予測モデルの開発
5. 攻撃を受けている際のネットワークの状況、及びサイバー攻撃をより分かりやすく把握するための視覚化フレームワークの構築

主要 5 領域の進歩に関する研究活動の大半を手掛けているのはUCSBコンピュータ・セキュリティ・グループだが、共同研究機関であるUCBとジョージア工科大学も重要な役割を果たしている。UCBのVern Paxson博士 は、上記に示した主要研究領域の 1 項目目に関連して、隠れた侵入者の行動(偵察とコバート・トンネリング)を検出するためのモデル開発を主導している[81]。一方、ジョージア工科大学ではJeff Shamma博士が、上記に示した主要研究領域の 4 項目目に関連して攻撃予測モデリングの開発を推進している[82]。

サイバウェア・プロジェクトにおける状況認識の理論と技術の開発を通して、DOD のような連邦機関においてサイバー攻撃に対してより効果的な予防対策が講じられるようになることが期待される。さらに、攻撃者の行動に対するゲーム理論的分析や脅威の視覚化は、進化し続ける新たな脅威を予測する上で大いに役立つことが期待される。

---

[80] サイバウェアプロジェクトの概要、USCB、2010 年 2 月 24 日
http://www.ia.ucsb.edu/pa/display.aspx?pkey=2187
[80] サイバウェアプロジェクト概要説明 http://www.cs.ucsb.edu/~seclab/projects/cybaware/index.html
[81] 「侵入者の行動予測」プレゼンテーション資料、Paxson, Vern, UCB. 2011 年 9 月 9 日)
http://cs.ucsb.edu/~kemm/MURI/Presentations/paxson.pdf
[82] 「サイバウェア:攻撃分析、予測、可視化のためのサイバー認識フレームワーク」、Kemmerer, Richard. 、2011 年 9 月 9 日(p. 17) http://www.cs.ucsb.edu/~tim/cybaware_web/dwnld/yr2/kemmerer_overview.pdf

2011 年 9 月に開催されたサイバウェア・プログラムの第 2 回年次研究レビュー会合で、Kemmerer博士は最新の進捗状況と今後の計画を発表した。以下に示すのは、これまでの同プロジェクトにおける研究成果である[83]:

- 制御環境におけるトラフィックを監視することで、マルウェア・プログラムの行動特定
- ネットワーク上のマルウェアに関連したトラフィックを検知できるモデル構築
- 個々のホストの活動を反映するシグネチャを開発した。
- SSH 間の潜在的な因果関係を反映する系図／グラフを構築するためのアルゴリズム開発
- ネットワーク・トラフィックから必要な関連情報を自動的に抽出し、抽出した情報を関連付けるためのアルゴリズム、手法、モデル開発
- 特定のネットワークに対して行われた過去のサイバー攻撃を分析し、将来起こり得るサイバー攻撃を予測する攻撃検知技術の開発
- ウェブベース・プラットフォーム上の数百万のノードやエッジの情報をグラフ化するためのネットワーク視覚化技術の開発。また、状況認識に利用するインターフェースの設計・導入

②ネクサット（Nexat）[84]

UCSB の Kruegel 博士と Vigna 博士は、ネクサットと呼ばれるプロトタイプ・ツールの開発に取り組んでいる。ネクサットでは機械学習技術を使って攻撃者の行動履歴を学習し、リアルタイムで学習した内容を基に予測される次の攻撃者の行動を推定する。ネクサットは、サイバウェア・プロジェクトと同様 MURI を通して研究資金が拠出されている他、NSF の信頼できるコンピューティング・プログラムからも総額 20 万 7,400 ドルの助成を受けている。

2011 年 12 月にはネクサットに関する最新の研究成果が報告されている。UCSB では、ネクサットに関連して大規模なハッキング・コンペを実施している。同コンペは、複数のハッカー・チームが、多様の手段を講じて同じネットワークに対してセキュリティ侵害を試みたもので、侵入検出システムによって蓄積された警告データベースを活用し、ネクサットの精度の高さを証明するために行われた。ネクサットは、攻撃者の次の行動を 94%の精度で予測することができた。研究者らは、ネクサットは電算リソースをほとんど必要とせず、攻撃を瞬時に予測できる点を強みとして主張している。

ネクサットの運用フェーズは、データ抽出フェーズ、研修フェーズ、そして予測フェーズという 3 つのフェーズに区分される。データ抽出フェーズでは、侵入検出システムを使って

---

[83] 「サイバウェアの概要と将来計画」、Kemmerer, Richard.、2011 年 9 月 9 日（p. 3-9）
http://cs.ucsb.edu/~kemm/MURI/Presentations/kemmerer_summary.pdf

[84] 「Nexat プロジェクト」の概要説明、UCSB http://seclab.cs.ucsb.edu/media/uploads/papers/2011_nexat.pdf

以前に作成された警告データベースから、一部必要な情報を抽出する。次に研修フェーズにおいて、データ抽出フェーズで引き出した情報を利用して攻撃者の行動に関するナレッジベースを作成する。そして、最後に予測フェーズにおいて、研修フェーズで作成したナレッジベースを基に、攻撃者の次の攻撃を予測する。

今後は、予測精度をさらに改善し、また予測の算出を簡易化するためのアルゴリズムの研究を推進することが計画されている。

（2）ジョージ・メイソン大学[85]

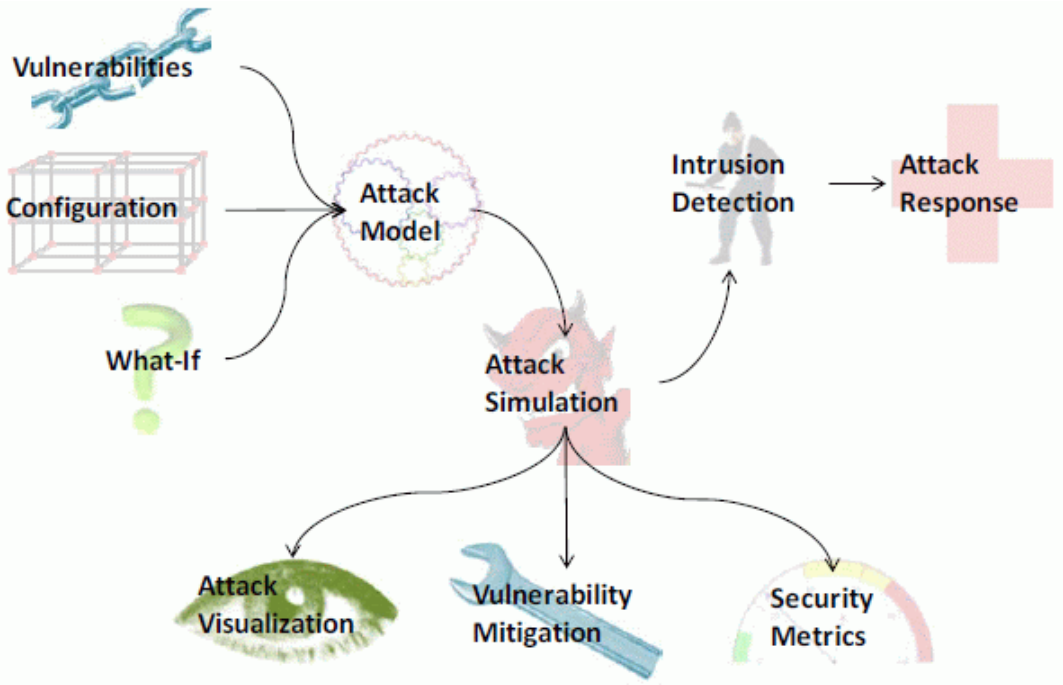
＜研究機関プロフィール＞
GMU のセキュア情報システム・センタ（Center for Secure Information Systems: CSIS）は、米国の大学における最初の情報セキュリティセンタとして 1990 年に設立された。CSIS は、研究機関や民間企業、及び政府機関と連携してサイバーセキュリティに関連する研究開発を進めており、先述した ARO が支援するペンシルバニア州立大学の研究プロジェクトには共同研究機関として参加している。CSIS は、①ネットワーク攻撃モデリング、分析、視覚化、②セキュリティ視覚化、③悪意あるコードからの防護、④サイバー状況認識、⑤セキュアなシステム、⑥侵入・攻撃から自動で回復するシステムを主要な研究分野に据えており、位相脆弱性分析（TVA）や侵入検出データ・マイニングの研究開発を進める。CSIS は現在、GMU のコンピュータ科学部及び電子・コンピュータ工学部の教授に加えて、10 名の専門科学者により構成されている。CSIS では、特にサイバー攻撃モデリング・分析・視覚化技術の研究開発に力を入れており、過去 10 年間には様々な政府機関の下で TVA 技術に関する研究開発を実施しており、年間平均予算は 100 万ドル超にもおよぶ。

＜研究プロジェクト概要＞
CSISの主要研究領域の一つは、サイバー状況認識である。CSISセンタ長であるSushil Jajodia博士と Steven Noel博士のリーダーシップの下、CSISはTVA技術を開拓し、その論文発表件数及び文献引用件数は数百件に及ぶ。NSAと AFRLからの助成を受けて開始された「先進サイバー攻撃モデリング・分析・可視化（Advanced Cyber Attack Modeling, Analysis, and Visualization）」[86]プロジェクトでは、ネットワーク上のすべての攻撃プロセスを視覚化するTVAモデルが開発された。下図に示されるように、TVAモデルではシステム脆弱性、ネットワーク接続状況などの情報を基に、サイバー・ネットワーク攻撃に対する予防策を視覚化したグラフを作成するというサイバー攻撃予測・分析・視覚化において新たなアプローチを提供している。

---

[85] セキュア情報システムセンタ概要説明　http://csis.gmu.edu/
[86] 「先進サイバー攻撃モデリング・分析・可視化」、GMU。2010 年 3 月
http://www.dtic.mil/dtic/tr/fulltext/u2/a516716.pdf

TVA アクセス・フロー



出典:GMU[87]

TVAシステムの目的は、大量のネットワーク・セキュリティ・データを分かりやすく提示できる攻撃グラフを開発し[88]、複数の攻撃の相互関係の明確化や予測に活用するだけでなく、将来発展し得る新たな攻撃の仮説の策定に応用することである。また、重要なことは、隣接マトリクス上で攻撃手段を予測するグラフィカル・テクニックを開発することである。

TVA ソリューションの主な特徴を以下に示す。

- ネットワーク攻撃の組み合わせを整理するために、攻撃グラフを活用する。
- 攻撃グラフ及び仮定分析において視覚化機能を提供する。TVA 攻撃グラフは、傾向や比較分析のために利用できる包括的ネットワーク・セキュリティを定量化する多数のメトリクスをサポートする。

このTVA技術開発からは、ネットワークに存在する論理依存性を利用した組み合わせ分析（Combinatorial Analysis Utilizing Logical Dependencies Residing On Networks:

---

[87] 「先進サイバー攻撃モデリング・分析・可視化」、GMU、2010 年 3 月（p. 15）
http://www.dtic.mil/dtic/tr/fulltext/u2/a516716.pdf

[88] 攻撃グラフとは、ネットワークやシステムがどのように攻撃を受けているか、またその攻撃の分析や予測など一連のプロセスを可視化した図のことをいう。

CAULDRON）[89]が開発された。これは、組織のネットワークにある危険な脆弱性パスを特定することにより、サイバー攻撃の影響を軽減するために設計されたものである。CAULDRONでは、すでに収集されたデータに基づき、全ての脆弱性と攻撃プロセスのを視覚化し、相互関係性を示すことができる他、脆弱性がセキュリティ全体に与える影響をグラフ化することもできる。そして、攻撃グラフを分析することで、ネットワーク環境に応じた最適な防護手段を判断することができる。

連邦航空局（Federal Aviation Adiministration: FAA）は、CAULDRON を導入した最初の政府機関で、セキュリティ問題に優先順位を付けることを目的としたサイバーセキュリティ・インシデント対応センタ（Cyber Security Incident Response Center）において導入されている。

（3）ペンシルバニア州立大学[90]

＜研究機関プロフィール＞
ペンシルバニア州立大学の情報科学・技術学部（College of Information Sciences and Technology: IST）は、コンピュータサイエンス、情報技術、システムユーザに関連する多様な分野を統合した研究プログラムを実施している。IST は 1997 年に設置され、設立当初は教授 15 人と規模が小さかったが、現在は 120 人にまで規模を拡大しており、GMU やアリゾナ州立大学、メリーランド大学など多数の研究機関と連携している。IST 下には、①HCI センタ（Center for Human-Computer Interaction）、②サイバーセキュリティ・情報・信頼性 LIONS センタ（LIONS Center for Cyber Security, Information and Trust）、③ネットワーク認識・情報融合センタ（Network-Centric Cognition and Information Fusion Center、④エンタプライズ・アーキテクチャ（Enterprise Architecture）の 4 つのセンタが設置されており、サイバーセキュリティに関しては、②サイバーセキュリティ・情報・信頼性 LIONS センタが研究推進機関である。

サイバーセキュリティ・情報・信頼性LIONSセンタは、サイバー攻撃の予測及びセキュリティの信頼の強化を目標として、マルウェア分析、自動回復システム、サイバー状況認識、攻撃分析・モデリングへのゲーム理論の応用などを主要な研究テーマとしている。現在、研究を推進する中心的な研究者 8 名と研究に協力する 20 名、リサーチアシスタント 4 名の計 32 名から構成され、年間の研究資金はおよぼ900万ドルである。同センタの研究プロジェクトには、MURI、NSF、ARO、DHSが主に資金を提供している[91]。

---

[89] CAULDRON の開発について、ランテック（Lantech）
https://www.lantechinc.net/pdf/Cauldron%20by%20LanTech.pdf
[90] ペンシルバニア州立大学 IST 組織概要 http://ist.psu.edu/
[91] サイバーセキュリティ・情報・信頼性 LIONS センタ概要紹介 http://cybersecurity.ist.psu.edu/

＜研究プロジェクト概要＞
LIONSセンタの責任者であるPeng Liu博士は 2009 年以来、「コンピュータ支援人間中心型サイバー状況認識（Computer-Aided Human Centric Cyber Situation Awareness）[92]」と銘打ったサイバー状況認識研究プロジェクトを実施している。同プロジェクトはMURIを通じて、AROより向こう５年間で、研究資金総額625万ドルを受給することになっている。

このプロジェクトは、既存のサイバー状況認識ソフトウェアやハードウェアと、実際に求められている状況認識技術にギャップがあることから、このギャップを埋めるために新たなソリューションを開発することを目的として開始された。

この分野において「サイバー攻撃予測に対するゲーム理論的アプローチ[93]」と題した研究を 2005 年に発表したこともあるLiu博士は、アリゾナ州立大学、CMUノース・カロライナ州立大学（North Carolina State University）、メリーランド大学カレッジ・パーク校（University of Maryland-College Park）、そしてGMUのセキュア情報システム・センタの研究者と提携して同プロジェクトを推進している。

この研究の最終目的は、機械による状況認識と人間による状況認識を統合するエンド・ツー・エンドの CSA ソリューションを開発することである。このソリューションには、機械の状況認識システムが人間の状況認識システムと連携して動作するために必要とされる新アルゴリズムとテクニックが駆使され、サイバー状況認識に関する人間の認知的側面とコンピュータのアルゴリズム的側面を統合することになる。またこのソリューションでは、状況認識だけでなく、サイバー攻撃の影響度の推定、因果分析、傾向分析、そしてシステム保証査定に関する機能も統合される。

研究チームでは、プロジェクトの各段階でテスト可能かつ実行可能なプロトタイプを開発することを目標に掲げており、これまでプロジェクト期間中は毎年、前年に開発された機能に基づくプロトタイプ機能を開発している。

（4）ロチェスター工科大学（Rochester Institute of Technology）[94]

＜研究機関プロフィール＞
ニューヨーク州ロチェスターにあるロチェスター工科大学のネットワーキング・情報処理研究所（Netwokring and Information Processing Lab: NetIP Lab）は、ネットワーキング、

---

[92] 「コンピュータ支援人間中心型サイバー状況認識」プロジェクトについて、ペンシルバニア大学 http://www.hss.cmu.edu/departments/sds/ddmlab/papers/40372.pdf
[93] 「攻撃予測へのゲーム理論の適用」、Liu,Peng. http://s2.ist.psu.edu/paper/predict.pdf
[94] ペンシルバニア州立大学 IST 概要説明 http://ist.psu.edu/

シグナリング、情報処理に関する研究を実施している。主な研究テーマには、自律型ロボット、デジタル信号処理（Digital Siganling Processing: DSP）アルゴリズム、車車間通信のアドホックネットワーク、サイバー脅威の査定、サイバー状況認識がある。NetIP Lab では、同大学のコンピュータ工学の教授である Anders Kwasinki 博士と准教授の Jay Yang 博士が研究を進めている。

＜研究プロジェクト概要＞
Yang博士は、サイバー状況認識関連研究分野の権威として知られている。Yang博士は2012 年に開催されたサイバーセキュリティ国際会議（International Conference on Cyber Securtiy: ICCS）の場で、最近の研究活動の成果を「サイバー状況認識のための攻撃行動の特性化（Characterizing Attack Behavior for Cyber Situation Awareness）」と題したプレゼンテーションの中で発表している[95]。この研究は、サイバー状況認識を強化するために、サイバー攻撃行動の特性化に主眼を置いたものである。

Yang博士の研究の大前提は、侵入検出システムから入手した生データを相互に関連付けられることで攻撃の経緯を特定できるという点にある。Yang博士は攻撃の経緯を初期段階で査定することにより、攻撃者の能力や行動の傾向を解明し、将来の侵入活動を予測できると仮定している。Yang博士は、既定の攻撃パターンが特定されていない行動の傾向を把握するために、可変長マルコフモデル（Variable Length Markov Models : VLMM）を適用し、その後独自に、攻撃者ごとにサイバー攻撃の影響を推定するためのクラスター分析が可能な「仮想地勢スキーマ（virtual terrain schema）」を開発している[96]。

2.1.4. サイバー攻撃予測・分析の技術分野に係る将来的な展開・方向性

グローバル政策科学研究所（Institute for Science on Global Policy）によると、効果的な攻撃予測技術を発展させるのであれば、サイバー攻撃に繋がる社会的・人的行動を予測する研究方法の特定を進める必要があると指摘しており、人間や組織の活動など社会的な要素も取り込んだより優れたツールの開発が望まれる。そのためには、先進の分析機能や、正確な予測機能を提供する、モデリングとシミュレーション・ツールの継続的な開発が必要不可欠と見られている[97]。

---

[95] ICCS のプログラム内容 http://www.iccs.fordham.edu/program/2012-program-schedule/s-yang/
[96] ICCS のプログラム内容（Jay Yang 博士について）
http://www.iccs.fordham.edu/program/2012-program-schedule/s-yang/
[97] グローバル政策科学研究所の概要説明
http://www.scienceforglobalpolicy.org/ISGPReports/Cybersecurity/CybersecurityWhitePaper/tabid/96/Default.aspx

2.2. 米国における設計済みセキュリティの技術開発に関する動向

2.2.1. 米国における設計済みセキュリティの技術分野に関する取り組みの概要

「設計済みセキュリティ」とは、ソフトウェア設計及び開発の初期段階において、そのシステムの攻撃に対するレジリエンス[98]を確認できる形で保証するというセキュリティ・アプローチである。セキュアなソフトウェア・エンジニアリングと開発は 2012 会計年度のNITRDの主要な研究開発トピックにおいて優先項目の一つに位置付けられている[99]。

「設計済み」というアプローチは、一般的にいかなるソフトウェアにも脆弱性が存在するという観点から発展した。US-CERT によると、最も成功率が高い攻撃は、ソフトウェアの設計及びコーディング段階においてパッチを行っていないソフトウェアの脆弱性やセキュアではないソフトウェア設定を狙ったものであるとしており、ソフトウェアの設計段階からセキュリティを保証することの重要性が認識された。

連邦政府における設計済みセキュリティの技術開発に関する経緯

大統領情報技術諮問委員会（President’s Information Technology Advisory Committee: PITAC）が 2005 年に作成した大統領への報告「サイバーセキュリティ：優先順位決定の危機（Cyber Security: A Crisis of Prioritization）」によると、ソフトウェアは脆弱性を最小化するようには設計されておらず、結果として脆弱なソフトウェアは外部の侵入を受けやすく、またネットワークを介して他のソフトウェアやシステムにも多大な障害を引き起こしてしまうとしている[100]。

また、DHSとDODのソフトウェア・データ解析センタ（Data and Analysis Center for Software: DACS）は、ソフトウェアのセキュリティ及びセキュアなソフトウェア要件についてまとめた「セキュアなソフトウェア製造のための開発ライフサイクルの強化：ソフトウェア保証に関する参照ガイドブック（Enhancing the Development Life Cycle to Produce Secure Software: A Reference Guidebook on Software Assurance）[101]」を策定している。

DACSは同ガイドラインの中で、ソフトウェアのセキュリティは、以下に示すように、常に様々なリスクに直面しており、セキュリティ対策が不十分なためだけでなく、意図的に選

---

[98] レジリエンスとは、一般的に困難な状況下で、生存・適応できる能力のことをいう。ここでは、攻撃に対する対応能力、抵抗力、生存性のことを指す。

[99] 「NITRD2012 年度予算補足資料」、2011 年 2 月
http://www.nitrd.gov/pubs/2012supplement/FY12NITRDSupplement.pdf

[100] 「サイバーセキュリティに関する大統領への報告書」、PITAC、2005 年
http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

[101] 「セキュアなソフトウェア製造のための開発ライフサイクルの強化： ソフトウェア保証に関する参照ガイドブック」、DACS、2008 年 10 月 https://www.thedacs.com/techs/enhanced_life_cycles/

択した行動の結果、また内部関係者による悪意ある行動により、多くの危険にさらされる可能性があるとしている[102]。

- **開発段階のリスク:** 開発者がソフトウェアを（意図的あるいは無意識に）破損して、ソフトウェア運用時にその信頼性や信用性が危険にさらされる可能性がある。
- **導入段階のリスク:** ソフトウェア配布の責任者が、出荷やアップロード前にソフトウェアの不正防止措置を怠るか、あるいは簡単に傍受されるコミュニケーション・チャンネルを利用してソフトウェアを送信することで、ソフトウェアは意図的または無意識に破損を受けやすい。同様に、ソフトウェアのインストーラがホスト・プラットフォームの「ロックダウン」を怠るか、ソフトウェアの安全な設定を怠った場合、ソフトウェアは攻撃者からアクセスを受けやすい。
- **運用段階のリスク:**汎用ソフトウェア（Commercial Off-The-Shelf Software: COTS）やオープンソース・ソフトウェア（Open Source Software: OSS）の運用が開始された後で脆弱性が発見されることもある。運用が開始された後では、セキュリティ・パッチやソフトウェアの更新を行うか、脆弱性の根本的原因を取り除いた新たなバージョンのものを採用しない限り、ソフトウェアの脆弱性は増大する傾向にある。また、ネットワークで接続されたプラットフォームで稼働するソフトウェア・システムはいずれも、運用段階で露呈する脆弱性を抱えている。露出レベルはネットワークが公衆かプライベートか、インターネットに接続されているかどうか、ソフトウェアの環境が露出を最小限に抑えるよう設定されているかどうかによっても異なる。しかし、高度に制御されたネットワークや「ロックダウン」環境においてでさえ、ソフトウェアは悪意を持った内部関係者（ユーザや管理者など）からの脅威に曝される可能性がある。

DACS は、上記のソフトウェアが抱える多様なリスクからもわかるように実験段階、また運用段階のいずれの場合においてもソフトウェアの開発・導入のできるだけ早い段階で欠陥と脆弱性を修正する方が、ソフトウェアを開発・導入した後に対応するよりもはるかにコスト効率が高いことからも、設計済みセキュリティの重要性が裏付けられるとしていいる。

また、同ガイドラインでは、セキュアなソフトウェアの要件として以下の 3 点を挙げている[103]:

1. **信頼性（Dependability）:** 信頼できるソフトウェアは、攻撃を受けている、あるいは不正ホスト上で稼働しているといった厳しい状況を含む全ての環境下において、予定される通りに機能を実行し、正確に動作する。

---

[102] 「セキュアなソフトウェア製造のための開発ライフサイクルの強化： ソフトウェア保証に関する参照ガイドブック」p.9

[103] 同ガイドブック p.6

2. **信用性（Trustworthiness）：** 信用できるソフトウェアは、ソフトウェアの信頼性を傷つける、あるいは妨害するために意図的に悪用される脆弱性や弱点があったとしても、その数は限定的である。さらに、信頼できるとみなされるためには、そのソフトウェアには、それ自体に悪意のある行動を起こさせるような不正ロジックがあってはならない。
3. **生存性（Survivability）（レジリエンス）：** レジリエントなソフトウェアとは、（1）最もよく知られた攻撃や多くの新たな攻撃に対し、可能な限り抵抗する（攻撃に対して自らを守る、など）、あるいは許容する（攻撃を受けているにも関わらず、信頼できる動作を続ける、など）、（2）抵抗や許容できなかった攻撃から、できるだけ早く、また被害を最小限に抑えて回復する、だけの十分な生存性を持つソフトウェアである。

設計済みセキュリティの主要目的は、上記の要件を満たしたソフトウェア・システムを設計・導入・保守するためのセキュアなソフトウェア開発ライフサイクル（Software Development Life Cycle：SDLC）を構築することである。セキュリティはSDLCを通して、ソフトウェアの重要な特性として位置付けられている。DHSによると、ソフトウェア・ライフサイクルの全フェーズでセキュアなソフトウェア開発を導くために必要な原則は、以下の通りである[104]：

- **重大な影響をもたらす標的の数を最小化する**：ソフトウェアには、攻撃を受けた際にソフトウェアに重大な支障をもたらす可能性がある攻撃の標的（クリティカルかつ信用されたコンポーネント）となる要素をできるだけ盛り込まない。例えば、クリティカルで信頼されたコンポーネントは、それらが侵害された場合の衝撃が大きいことから、重大な影響をもたらす標的といえる。
- **脆弱で重大な影響をもたらすコンポーネントを表に出さない**：ソフトウェアに含まれるクリティカルで信頼されるコンポーネントは、攻撃にさらされるべきでない。また、脆弱性のある要素も攻撃の容易な対象となるため保護する必要がある。
- **攻撃者に、セキュリティ侵害の手段を与えない**：ソフトウェアは攻撃者に対し、自らのセキュリティを侵害させるような手段を与えるべきでない。そのような「手段」には、悪用可能な弱点や脆弱性、ドーマントコード（dormant code）、バックドアなどが含まれる。また、被害の拡大を防ぐため、セキュリティ侵害（または潜在的侵害）が起きた後は、できるだけ早急に被害を最小化し、ソフトウェアを復旧、再構成させる機能を装備する。具体的には、ソフトウェアの行動や、それが受け取るインプットを監視、記録して、対処する方法を確立する必要がある。

SDLCにおいて、セキュアなソフトウェア開発を行うためには、体系化されたセキュアなソフトウェア開発手法を採用するか、現在の開発手法において段階的にセキュリティを強

---

[104] DHS における設計済みセキュリティ　https://buildsecurityin.us-cert.gov/bsi/547-BSI.html

化するかのいずれかの方法をとる必要がある。後者のSDLCのセキュリティの段階的な強化については、通常既存のSDLCのセキュリティに関連したプラクティスや要件を増強する、または必要に応じて新たなプラクティスや要件を追加する、さらに稀なケースではあるがセキュアなソフトウェア開発の障害となるプラクティスそのものを排除する方法で行われる[105]。これに対し、前者のソフトウェア設計・開発の初期段階から体系化されたセキュアなソフトウェア開発手法を採用するのが、設計済みセキュリティである。

設計済みセキュリティでは、最初から悪用される可能性がある欠陥の数を大幅に減らし、攻撃に耐性があるソフトウェア・システムを設計・開発することに重点を置く。ソフトウェア開発事業者は、セキュリティ保証に重点を置いた言語やツールを利用することにより、システムを開発すると同時に、攻撃に耐えるだけのシステムであることを立証するためのツール開発することができる。

過去 10 年間で、静的・動的分析によりソフトウェアの欠陥検出手法は大きく発展しており、これまでの成果は、攻撃に対する耐性を持つという保証を備えている大規模なソフトウェア・システムの設計と導入を推進する設計済みセキュリティの研究においても重要なインプットとなる。

設計済みセキュリティに関する研究は、ソフトウェアのリスク、コスト、品質、複雑性などを管理しながら、高信頼ソフトウェア・システムを計画どおり確実に設計、開発、発展させることができる能力を構築することにに焦点を当てている。ソフトウェアの保証に重点を置いた開発手法を利用することで、システムを開発すると同時に保証ケースをサポートするために必要な立証ツールを発展させることができ、事後的に保証をサポートする現在の方法と比較してコストを大幅に削減することができ、かつシステムの発展速度を急速に改善することができる。

また、設計済みセキュリティの研究における重要なポイントは、攻撃に対してレジリエンスのあるソフトウェア・システム開発ツールの有用性にある。ソフトウェアを規定、導入、分析し、試験するためのツールと、ソフトウェア・コンポーネントを使ってシステムを構築するためのツールの有用性の改善は、「ゲームチェンジ」の鍵を握るソフトウェア開発業者がツールを広く採用する上では必ず取り組まなければならない点である。設計済みセキュリティを導入することで、現在主流となっているソフトウェアのエコシステム及びインフラ全体を発展・進化することができると考えられており、高信頼ソフトウェアを開発するこのコスト効率の高い設計済みセキュリティの利用がより堅牢な新たなソフトウェア開発の基盤の構築に繋がることが期待される。

---

[105] 設計済みセキュリティに関する概要説明、DHS　https://buildsecurityin.us-cert.gov/bsi/547-BSI.html

設計済みセキュリティはソフトウェアだけではなく、ハードウェアにおいても同様のことが言えるため、包括的なアプローチとして、設計済みセキュリティはハードウェアの製造・組立て工程においてハードウェアのセキュアな設計・製造、及び試験にも広く採用される可能性がある。

設計済みセキュリティの研究課題として、以下の項目が挙げられている[106]:

- ソフトウェアやシステムの開発工程において、同時にソフトウェアやシステムの特性に関する情報(システムが攻撃に対するレジリエンスを持つ証拠も含まれる)を記録するモデルや技術の開発
- 上記で開発したモデルや技術を通して記録した特性に関する情報を統合する技術
- ソフトウェアやシステムの品質保証のため、コードに至るまでセキュリティ要件が満たされているかを分析する技術やツールの開発
- システムのセキュリティ品質を効率的に保証できる言語設計、処理技術、ツールの開発
- サプライ・チェーンのリスクマネジメントにおけるサイバーセキュリティの取り込みの促進
- 証拠の自動管理をサポートすることを目的とした情報管理、設定管理、及び開発者／チーム連携をサポートするツール
- 使い易いソフトウェア仕様、導入、検証、分析ツールを開発を促進させる人間の行動分析
- 上記の項目で開発されたツールや技術を、連邦政府機関が積極的に取り入れることを促進するための経済的インセンティブの発展

連邦政府の ICT 研究開発ポートフォリオにおける位置づけ

先述のとおり、設計済みセキュリティは 2011 年、NITRDにおいてサイバーセキュリティ関連の新たな研究項目に指定されており、NITRDではソフトウェアの開発段階から活用でき、かつシステムの発展・導入段階においても適用できる品質保証を立証できるツールの開発を目指している[107]。

NITRDの 2011 会計年度予算補足資料によると、設計済みセキュリティは、NSFとDODを含む複数の連邦政府機関で優先事項に挙げられている。これらの機関において設計済みセキュリティの研究開発を推進する目的として、コストベネフィット及びリスクの分析ツールに使用するメトリックの開発、SDLCの初期段階におけるセキュリティ関連プラクティスの特定、信頼性の高いシステムの構築、拡張性の高いセキュリティシステムの構築

---

[106]設計済みセキュリティに関する概要説明、NITRD http://cybersecurity.nitrd.gov/page/designed-in-security
[107]「連邦サイバーセキュリティ研究開発プログラム:戦略計画」プレゼンテーション資料、NITRD http://www.nitrd.gov/fileupload/files/NITRD_IEEE_SSP_2011.pptx

などが挙げられている[108]。

2.2.2. 連邦政府が支援する設計済みセキュリティの技術開発に関する主要プログラムのプロフィール

設計済みセキュリティに関する各機関における予算の利用状況の詳細については不明であるが、NSFは同分野の取組みを強化している代表的な機関である。NSFはセキュリティ駆動型アーキテクチャ・ワークショップ（Security-Driven Architectures Workshop）をコーディネートしており、またNSFのコンピュータサイエンス分野に関連する 2012 年度予算の優先事項の一つサイバーセキュリティを掲げている。NSFは、信頼できるシステムの構築・保守・利用において将来応用することができる基本原則の策定に取り組む計画である[109]。

（1）NSF

TC／SaTC プログラム

設計済みセキュリティに関しては、本報告書 2.1.2 で先述したTCプログラム、また現在ではSaTCプログラムにより研究プロジェクトが実施されている。TCプログラムが資金を拠出していた関連プロジェクトの一つに、南フロリダ大学（University of South Florida）が進めている「セキュアなソフトウェア・システムのための基礎論理と実行ツール（Foundational Theories and Enforcement Tools for Secure Software Systems）」の開発プロジェクトがある。プロジェクト期間は2008 年～2013 年の予定である。このプロジェクトでは、ソフトウェア・セキュリティの基本理論と、安定した実行メカニズムを迅速かつ実証可能な方法で生成するためのツールの開発に取り組んでいる。そのうち基本理論は、脅威とセキュリティポリシーを含むセキュリティの一般原則の定義とルールにより構成される。一方の実行ツールは、セキュリティポリシーの定義を、これらのポリシーを遵守するとしたメカニズムに取り込む技術から成る。これら研究課題に同時に取り組むことで、セキュアなソフトウェア・システムのための信頼できる実行メカニズムの迅速な開発と導入が可能になることが期待されている[110]。

また、SaTCプログラムでは、設計済みセキュリティに関してジリエントなソフトウェアの設計と導入、及びソフトウェアのセキュリティ面の構成要素を大規模なシステムに統合するための研究に資金を拠出するとしている[111]。なお、2011 年 3 月末までにSaTCプログラムの実施プロジェクトとして選定された 5 つのプロジェクトの中に設計済みセキュリティに

---

[108] 「NITRD 2011 年度予算補足資料」、NITRD、2010 年 2 月
http://www.nitrd.gov/About/FY11NITRDSupp-FINAL-Web.pdf
[109] NSF における 2012 年度予算の概要　http://www.nsf.gov/about/budget/fy2012/pdf/17_fy2012.pdf
[110] 「セキュアなソフトウェア・システムのための基礎論理と実行ツール」プロジェクトの概要、NSF
http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=0742736&WT.z_pims_id=504709
[111] 「NSF の投資：SATC」、NSFhttp://www.nsf.gov/about/budget/fy2013/pdf/43_fy2013.pdf

関するプロジェクトは含まれていない。

（2）DARPA
サイバーセキュリティのための自動プログラム分析（Automated Program Analysis for Cybersecurity：APAC）

DARPAは 2011 年 7 月、APACの研究プロジェクトの公募を開始している。APACでは、DODのソフトウェア・プログラムが、サイバー攻撃を防止するためにDODが定めたセキュリティ特性の要件を満たしており、いかなる悪意あるコードも含まないことを自動的に証明する手法を開発することを目指している[112]。APACプログラムから出資される研究プロジェクトは 2012 年初めの開始が予定されているが、2011 年 7 月 22 日にプログラムが公示されて以降の進捗状況に関する情報は発表されていない。

特にAPACプログラムでは、DODのアンドロイド向けアプリケーション及びJavaモバイルアプリケーションを提供しているマーケットプレイスから悪意あるコードの侵入を阻止するツールを開発し、そのツールの実証実験を実施することに焦点を置いている。アプリケーション開発者が新規に開発したアプリケーションまたは既存のアプリケーションをアップデートしたものをマーケットプレイスで提供する際には、まずDODにより、DODが認定しているセキュリティ要件を満たすものであるかの審査が行われる。DARPAでは、APACプログラムを通じて開発したツールを活用し、DODがアプリケーションを審査する際に、迅速に悪意あるコードを含むアプリケーションを特定し、排除できるようになることを狙っている[113]。

（3）DOD
DOD ソフトウェア保証イニシアチブ（DoD Software Assurance Initiative）

DODのソフトウェア保証イニシアチブ（Software Assurance Initiative）は、国防科学評議委員会（Defense Science Board: DSB）の「グローバライゼーションとセキュリティに関するタスクフォース（Task Force on Globalization and Security）」がまとめた 1999 年 12 月の報告書に基づいている[114]。同報告書では、海外製の商用ソフトウェアにDODが依存することによって生じる潜在的脅威に対処する目的で、ソフトウェア保証プログラムの設立と、DODのセキュリティと諜報活動への対抗策を強化するための措置の必要性を

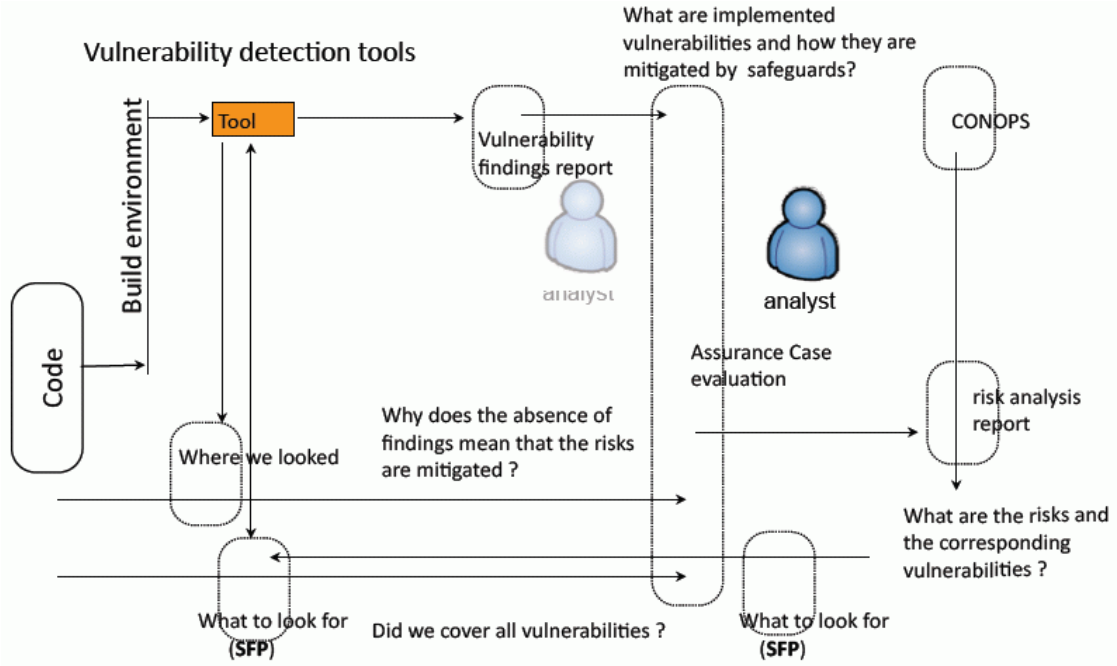
---

[112] APAC の概要説明、DARPA、2011 年 8 月 3 日
http://www.darpa.mil/uploadedFiles/Content/Our_Work/I2O/Solicitation/APAC%20Industry%20Day%20PM%20Slides.pdf
[113] APAC の概要説明、DARPA、2011 年 8 月 3 日
http://www.darpa.mil/uploadedFiles/Content/Our_Work/I2O/Solicitation/APAC%20Industry%20Day%20PM%20Slides.pdf
[114] 「グローバライゼーションとセキュリティに関するタスクフォースの報告書、1991 年 12 月
http://www.hsdl.org/?view&did=445571

勧告している。

同報告書の勧告を受けて、ネットワーク情報統合担当国防次官補（Assistant Secretary of Defense for Networks and Information Integration: ASD/NII）は 2003 年 7 月、民間から調達したソフトウェアを連邦政府において導入する際に、ソフトウェアの品質保証を精査することを目指したソフトウェア保証イニシアチブを設置した。同イニシアチブでは、本来 DoD の職員が実施していたソフトウェアの脆弱性を審査するプロセスを新たなツール（下図オレンジのボックス）を開発・導入することで、プロセスの自動化が進められた。

DOD ソフトウェア保証自動化モデル（DOD Software Assurance Automation model）



出典: KDM Analytics[115]

このイニシアチブのフォローアップとしてASD/NIIは 2004 年 12 月、国防次官／調達技術・ロジスティクス室（Office of the Under Secretary of Defense/Acquisition Technology and Logistics: OUSD/AT&L）と提携し、リスクに対する連邦政府の脆弱性を軽減する包括的な戦略を策定するために、ソフトウェア保証タイガー・チーム（Software Assurance Tiger Team）[116]を立ち上げた。

---

[115] 「DOD ソフトウェア欠陥パターン」プレゼンテーション資、Mansourov, NikolaiKDM Analytics、2011 年 9 月 12 日（p. 5）
https://buildsecurityin.us-cert.gov/swa/presentations_091211/Mansourov-SoftwareFaultPatterns.pdf

[116] タイガー・チームとは、技術的問題の調査及び／または解決の任を受けた専門家グループである。

同チームは、ソフトウェアレベルでは脅威に効率的に対処できないと考え、ソフトウェアレベルではなくシステム・レベルでセキュリティ問題に対処するというアプローチをとっている。また、同チームは米国国防産業協会（National Defense Industrial Association: NDIA）と連携し、セキュアなシステム・エンジニアリング・プラクティスをソフトウェア製品開発に統合するための業界の取り組みを主導している。

ソフトウェア保証タイガー・チームは、OUSD/AT&L と ASD/NII の協力を得て、フォーラムを開催するなどコミュニティへのアウトリーチも進めてきた。タイガー・チームでは、脆弱性の介在しないソフトウェアを開発するためには、アウトリーチ活動を通して、産学官及び国外のパートナーとも連携し、ソフトウェアの品質保証・リスク査定に関する問題を共有することが重要であると考えている。タイガー・チームでは、今後も業界や研究機関との連携を強化し、共通した問題意識を基に効率的にソフトウェアの品質保証技術を開発するために、アウトリーチ活動にも継続して取り組む計画である。

タイガー・チームの取り組み

DOD のソフトウェア保証オペレーション構想（Software Assurance Concept of Operations: CONOPS）を確実に実行するため、タイガー・チームでは以下のように活動をグループ分けしている[117]:

- **優先度付け（Prioritization）:** システムの重要性についてステークホルダーの優先順位付けプロセスを策定する。短期的には、DoD による大型調達、機密ネットワークへ接続されたシステム、機密プログラムなどのリスク性の高いシステムの調達に焦点を置く。優先順位付けは、SDLC の要件／調達フェーズ初期に実施される。これまでに以下の 4 つの保証レベルが特定されている。
    - **High+:** 外部からの侵害が、システムの能力低下やミッションの失敗をもたらす可能性のある技術（暗号アルゴリズム、クロス・ドメイン・ソリューションなど）
    - **High:**外部からの侵害がシステムの能力に深刻な低下をもたらす可能性のある技術（システム・モニタリング能力など）
    - **Medium+:**外部からの侵害がシステムの能力に部分的または識別できる低下をもたらす可能性のある技術（主要な業務アプリケーションにおける ICT コンポーネントなど）
    - **Medium:**外部からの侵害が不都合をもたらす可能性のある技術（オフィス自動化ツールなど）
- **徹底的エンジニアリング（Engineering in Depth: EiD）:** EiD では、より保証を必要とするコンポーネントの数と重要度を最小化し、さらに保証が十分にされていない製

[117] DOD の CONOPS 概要説明　http://sysa.omg.org/docs/swa_washington_2006/Systems_Assurance.pdf

品に本来備わっている未解決リスクを管理するために、システム・アプローチを応用する。例えば、隔離、マルチパス機能、交換可能モジュールなどのリスク削減設計技術の導入が含まれる。

- **サプライヤ保証（Supplier Assurance）:** サプライヤ保証では、サプライヤが DoD に提示する脅威レベルに応じてサプライヤを特徴付けることを目的としている。サプライヤ保証における懸念事項としては、外国によるサプライヤ管理と技術及び製品開発のアウトソースがある。サプライヤー保証では、上記に挙げた4つの保証レベルに基づいてサプライヤー保証要件を定義している:
    - **High+Assurance:** 米国企業、または認可された米国民だけが関与する米国政府公認コントラクタ
    - **High Assurance:** 米国企業、または米国民だけが関与する米国政府公認コントラクタ
    - **Medium+Assurance:** 米国企業、または、ソフトウェア設計と制御機能は米国民または歴史的に米国と深く関わりがある国で開発されるものの、ソフトウェア開発自体は外国で実施される可能性のある米国政府公認コントラクタ
- **科学技術（Science and Technology：S&T）:** S&T では、既存のソフトウェア品質保証に関連する技術やソリューションに代わる新たなソリューション及び技術の開発と、EiD に関連する新たな技術の開発と導入を目的とする。また、S&T は、EiD のニーズを満たす標準の開発で産業界とも協力しており、脆弱性の防止・検出・削減ツールと技術の研究開発において連携する。
- **業界アウトリーチ（Industry Outreach）:** 業界アウトリーチでは、NDIAのシステム保証委員会（Systems Assuranece Committee）、IT業界団体であるオブジェクトマネジメントグループ（Object Management Group: OMG）のソフトウェア保証委員会（Systems Assuranece Committee）、航空・宇宙分野の業界団体である 航空宇宙工業協会（Aerospace Industries Association: AIA）、そして電気・通信・IT分野の業界団体である政府電気情報技術協会（Government Electronics & Information Technology Association : GEIA）と連携して、DoDの産業界へのアウトリーチを図る。

2.2.3. 連邦政府が支援する設計済みセキュリティに関する研究開発活動を行なっている主要研究所

（1）海軍研究所（Naval Research Lab：NRL）

＜研究機関プロフィール＞

NRL は、1927 年に設置され 85 年の歴史を誇る米国海軍と海兵隊の共同研究所で、現在は 2,500 人以上の研究員、技術者、エンジニアを有する。同研究所の研究プロジェクトには、DARPA や DOD などの軍事関連の政府機関だけでなく DOE や NASA からも資

金が拠出されており、またプロジェクトの実施にあたり民間企業や業界団体、大学機関などと幅広く連携している。NRL は、設立当初から、無人・自動化システムの研究に従事しており、同研究所内に設置されている自動化システム研究所（Laboratory for Autonomous Systems Research）は同分野において数多くの実績を有する機関である。

CSIAに関連する研究に関しては、NRL情報技術部門（Information Technology Division）傘下の高位保障コンピュータ・システム・センタ（Center for High Assurance Computer Systems: CHACS）のソフトウェア・エンジニアリング課（Software Engineering Section）が、高信頼ソフトウェア技術の研究開発を進めている。CHACSは、情報保証に関して、海軍省（Department of Navy）が技術やツール、コンポーネント開発において常に最先端に位置するため、また海軍における技術的ニーズを満たすために研究を推進しており、海軍が研究成果を実戦で活用できるように技術の実用化も積極的に進めている。技術の研究と実用化を同時に推進するため、CHACSは研究部門とエンジニアリング部門の両方から構成されており、研究部門は技術の基礎研究から実証実験までを担当し、エンジニアリング部門は実用化を目的とした応用研究を担当する[118]。

＜活動概要＞
CHACSのソフトウェア・エンジニアリング課が進める主な研究開発の内容には、ソフトウェアが適切なセキュリティ・ガイドラインに従って開発されたことを証明するために利用される、セキュリティ・ポリシー仕様、セキュリティ脆弱性検知、そして認証アーティファクトの開発が含まれている[119]。

（２）パシフィック・ノースウェスト国立研究所（Pacific Northwest National Laboratory: PNNL）

＜研究機関プロフィール＞
DOE傘下の国立研究所であるPNNLには、主要な研究分野としてエネルギー・環境部門と国家セキュリティ部門の 2 部門に分けられる。国家セキュリティ部門では、国家の安全保障に関わる重要インフラの保護を目的として、国防機関であるDHSやDODとも連携して、あらゆる脅威を事前に検知・予測するための技術の研究開発を進めており、状況認識やサイバーシステムのモデリング及びシミュレーション、サイバー攻撃予測・分析に特に力を入れている[120]。

また、近年のスマートグリッドにおけるセキュリティ問題への関心の高まりに見られるよう

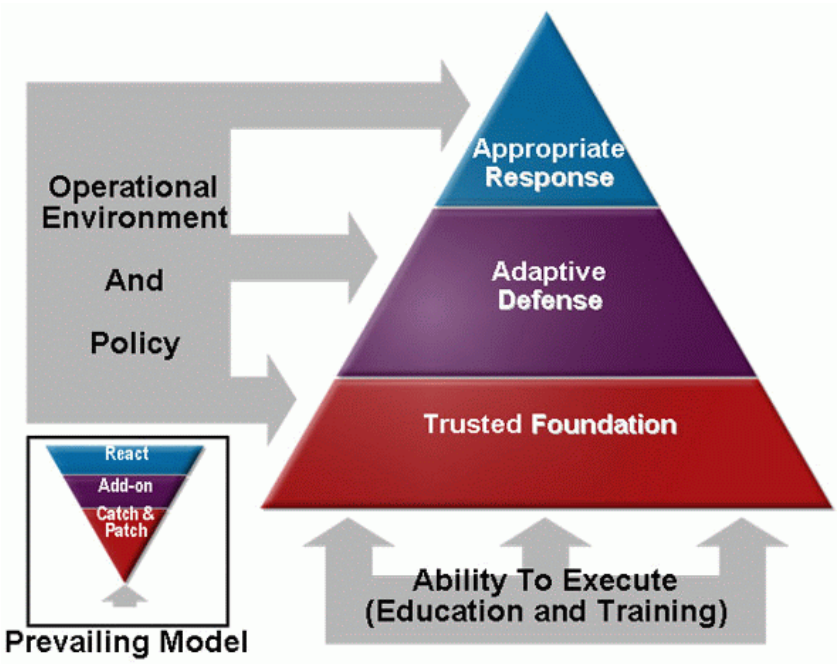
---

[118] NRL CHACS 組織概要 http://www.nrl.navy.mil/chacs/
[119] NRL ソフトエンジニアリング課の組織概要 http://www.nrl.navy.mil/chacs/5546/
[120] PNNL 国家セキュリティ 概要説明 http://www.pnnl.gov/nationalsecurity/about/

に、国家の重要インフラのセキュリティはエネルギー分野でも大きな問題であり、エネルギー・環境部門下に設置されている電力インフラオペレーションセンタ（Electricity Infrastructure Operations Center: EIOC）においてもサイバーセキュリティの研究が進められている。EIOCでは他大学からの研究者やスマートグリッドに関連する電力会社やITベンダによるスマートグリッドの監視・制御技術の研究開発を進めるプラットフォームとして設置されている[121]。

＜活動概要＞
設計済みセキュリティに関して、EIOCは内外からの脅威に対応し、自己防衛する機能を本質的に備えたセキュアなコンピューティング（Intrinsically Secure Computing: ISC）の開発を進めている[122]。下図に示すように、ISCは、システムやソフトウェアが自身で攻撃や脅威に対する対応方法を教育と訓練を通して学習する「信頼できる基盤（Trusted Foundation）」を基礎に、自己防衛能力及び様々な異なる攻撃に対して適切な対応能力を身に付けられるという概念に基づいた研究が進められている。

ISC のコンセプト概要



出典: PNNL[123]

[121] PNNL EIOC 概要説明 http://eioc.pnnl.gov/about.stm
[122] PNNL の EIOC 概要説明 http://eioc.pnnl.gov/research/cybersecurity.stm
[123] PNNL のサイバーセキュリティに関する取り組み概要 http://eioc.pnnl.gov/research/cybersecurity.stm

2.2.4. 設計済みセキュリティの技術分野に係る将来的な展開・方向性

国家情報局（Office of the Director of National Intelligence）とNSAにおいてサイバーセキュリティ分野を主導するBrad Martin氏によると、設計済みセキュリティに関する課題は、保証証拠管理をサポートするツールの開発や、潜在的ユーザーに開発したツールを導入させるインセンチブの特定であるとしており[124]、今後課題とされる分野における研究や活動が進められるものと見られる。設計済みセキュリティに関しては、今後の展開について特にPITACやDACSにおいて議論はされていない。

2.3. 米国における暗号技術の応用分野の技術開発に関する動向

2.3.1. 連邦政府における暗号技術の応用分野の技術開発に関する取り組みの概要

連邦政府における暗号技術の応用分野の技術開発に関する取り組みの経緯

2009 年 5 月に発行されたオバマ大統領のサイバースペース政策レビューの中で優先して取り組むべきサイバーセキュリティの研究開発の一つに挙げられたのが、「特別に作った信頼できる空間（Tailored Trustworthy Spaces: TTS）」である。TTSには自己防衛を可能とするスマートデータの開発が含まれており、NITRDによると、データの防衛のためにはデータの暗号化が重要であると指摘されている[125]。

上記に挙げた技術は、エネルギーや国防を含む様々な業界の発展にとって重要なセキュリティ技術である。米国のエネルギー産業においてスマートグリッドの構築が注目されているが、現状ではサイバーセキュリティはスマートグリッドにおいて課題とされる点でもあり、今後の技術開発が必要されている。課題の一つは、米国でこれまでに導入されたスマート・メーターの多くは、最新技術より 2、3 世代古いワイヤレス・コミュニケーション向け暗号技術を使っているという点であり、また、それらを最新の技術に更新するためにかかるコストを電力会社が負担するかどうかという点も懸念されている[126]。

また、スマートグリッドのシステム・アーキテクチャは広範囲に分散しており、非常に複雑である。何百万という遠隔装置や変電所、そしてメーターにまたがる暗号情報を守るために使われる何千万という認証情報や暗号キーのセキュリティを、現在の処理能力で確保することは難しい。さらに、コンポーネントに組み込まれた電子機器が、信頼できない企

---

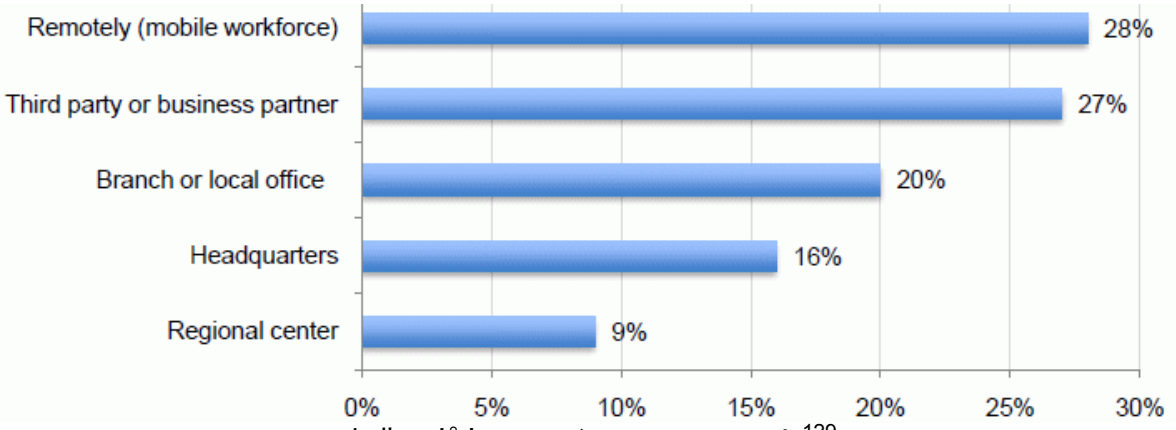
[124] 「NITRD サイバーセキュリティ研究開発プログラム：戦略計画」、NITRD
http://www.nitrd.gov/fileupload/files/NITRD_IEEE_SSP_2011.pptx
[125] 「サイバーセキュリティ・ゲームチェンジ研究開発勧告」、NITRD CSIA IWG
http://www.nitrd.gov/CSThemes/CSIA_IWG_Cybersecurity_Game-Change_%20RD_Recommendations_20100513.pdf
[126] 「スマートグリッドの市場動向・予測、技術イノベーション 2011 白書」
http://www.ci.leesburg.fl.us/pdf/electric/eFlorida_wp_web.pdf

業によって製造されている場合もある[127]。そのため、複雑なインフラを持つスマートグリッドにおいては拡張性があり、かつ大型の暗号キーセットを効率的に管理できる技術の開発が求められる。

国防とセキュリティに関しては、ワイヤレス・ネットワーク上でやり取りされるDHSの機密データ を保護するために、より洗練されたワイヤレス・セキュリティ手段が必要となる。DHS職員がさまざまなプライベート及び公衆ネットワークへアクセスし、業務を効率的に行えるようになれば、ポータビリティと柔軟性、生産性向上、コスト削減にも繋がる一方、サイバーセキュリティ問題を引き起こしやすい状況に陥ることにもなる。大半のプライベート及び公衆ネットワークでは、DHSの機密データを保護するレベルにまでセキュリティが強化されているわけではない[128]。従って、パケット分析やスニッフィング・ツールを使った傍受からデータを確実に守るような方法で、機密情報を含むデータを公衆ワイヤレス・システムで伝送できる技術の開発が望まれる。

一般的に ICT 業界は、既存のワイヤレス・セキュリティに懸念している。下図に示すように、ポネモン・インスティチュートの 2011 年調査によると、ネットワーク・セキュリティリ侵害の 28%が、ワイヤレス通信が介在する遠隔作業において発生している。

過去1年間における米 ICT 企業が被ったネットワーク・セキュリティ侵害箇所（2010～2011 年）



出典: ポネモン・インスティチュート[129]

---

[127] 「配電システムのサイバーセキュリティのためのロードマップ」、2011 年 9 月
http://www.cyber.st.dhs.gov/wp-content/uploads/2011/09/Energy_Roadmap.pdf

[128] サービス・セット識別子（SSIDs: Service Set Identifier）、オープン認証、静的有線同等プライバシー（WEP: Wired Equivalency Privacy）鍵、メディア・アクセス制御認証（Media Access Control Authentication）、または Wi-Fi 保護アクセス／Wi-Fi 保護アクセス 2 事前共有鍵（WPA/WPA2 PSK: Wi-Fi Protected Access/Wi-Fi Protected Accessed 2 Pre-Shared Key）

[129] 「ネットワークセキュリティに関する概観」調査結果、ポネモン・インスティチュート、2011 年 6 月（p. 5）
http://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf

クラウド・コンピューティング・システムが攻撃者にとって格好の標的となったことも、サイバーセキュリティの課題である。また、今現在は信頼できても、仮にクラウド事業者が事業に失敗した場合、ユーザデータは会社資産として売却される恐れがある。また、同様に事業者が他社から買収される可能性もあり、そうなるとユーザの情報は買収企業の手に渡り、そのデータ管理面での一貫性についても、懸念が残る。このようにクラウド・コンピューティグ環境に関しては、よりセキュリティ問題について慎重になる必要があることから、データを解読せずに活用・操作できる技術の研究開発が進められている。

また、クラウド・コンピューティング環境で保存されるデータを暗号データだけに制限し、ユーザの承認のみによりデータへのアクセスが許可される先進的な技術の研究開発も行われている。従って、「完全準同型暗号（full homomorphic encryption）」を利用することにより、特定組織の内部あるいは外部の攻撃者は、ユーザーの承認を得ていない暗号化されたクラウド上のデータにはアクセスできなくなり、ユーザだけが暗号化されていない情報へアクセスできるようになる。

連邦政府の ICT 研究開発ポートフォリオにおける位置づけ

一般的に暗号は、DOE、NSF、OSD、AFRL、ONR、DARPA、情報高等研究計画活動（Intelligence Advanced Research Projects Activity: IARPA）、DHS、NISTそしてNSAで研究優先事項とされている[130]。省庁間で協力して研究プロジェクトに出資することもあるが、基本的にはNITRDの他分野の研究プロジェクトと同じく、各省庁が暗号技術分野の中でもそれぞれの組織の目的に合った優先分野を特定し、独自に研究プログラムを設置し公募を行なっている。例えば、DOEは発電・送電システムの監視・制御システムであるSCADA（Supervisory Control and Data Acquisition）における暗号技術の開発、DHSはワイヤレス・コミュニケーションのための暗号化技術の開発、DARPAやIARPAでは 準同型 暗号技術の開発、DHSは国家の安全保障のためワイヤレス・コミュニケーションの暗号化、また ONRは、ハード・ドライブなどに保存されたユーザ・データの関数暗号を提供するとともに、物理的に侵入を受けた場合に保存されたユーザ・データを漏洩から守るような保存データ・セキュリティ（data-at-rest security）の研究を支援している。

この分野で最も積極的な研究活動を実施している機関はNISTとNSAであり、暗号標準検証プログラムの開発と維持、コーディネーションを手掛けている。NISTは、国際SHA-3（本報告書 2.3.3.参照）ハッシュ・コンペや公開キー管理、プライバシー強化暗号メカニズムを含む標準化の発展に注力しており、NSAでは、ソフトウェアとハードウェアのための保証された暗号導入に取り組んでいる。また、研究開発ではないが、NISTとNSAは暗号関連製品の評価・認証を共同で実施する国家情報保証パートナーシップ（National

[130] 「NITRD20110 年度予算補足資料」、2010 年 2 月（p. 17-18）
http://www.nitrd.gov/About/FY11NITRDSupp-FINAL-Web.pdf

Information Assurance Partnership）という国家プログラムにおいて連携している[131]。

2.3.2. 連邦政府が支援する暗号技術の応用分野の技術開発に関する主要プログラムのプロフィール

（1）NSF
SaTC プログラム

NSFにおける暗号技術の研究開発についても、先述したSaTCプログラムを通じて、ハードウェア・メモリにおけるデータ暗号化や暗号キー管理、量子演算耐性暗号（quantum computation-resistant cryptography）など暗号技術に関する研究プロジェクトを助成する計画である。暗号技術に関しては、SaTCプログラム下で、ジョンズ・ホプキンス大学の「クラウドにおける暗号生成の自動化とアウトソーシング」プロジェクトが研究プロジェクトの一つとして選出されている。同プロジェクトは 2012 年 1 月 15 日よりすでに開始しており、2013 年 12 月 31 日までの 2 年間で総額およそ 22 万 5,000 ドルが出資される。同プロジェクトはクラウドにおける大量のデータに関して電子署名の認証を自動化する手法などの研究を実施するとしている[132]。

（2）DOE
ホールマーク暗号シリアル・コミュニケーション（Hallmark Cryptographic Serial Communication[133]）

暗号技術に関する研究開発が極めて重要とされる領域は、発電と送電システムの監視・制御・最適化・管理を行うシステムである SCADA である。SCADA は、電力会社による全米または地方ネットワークの何十万というデータ・ポイントからのデータの収集と保存、分析や、ネットワーク・モデリングの実行、パワー・オペレーションのシミュレーション、障害の特定、供給停止の回避などを実現する。このシステムは現代の電力ネットワークに必要不可欠な要素であり、スマートグリッドにおける相互運用性とセキュアなサイバー環境を実現するものである。

DOE の配電とエネルギー信頼性局（Office of Electricity Delivery and Energy Reliability）は、エネルギー業界のサイバーセキュリティ研究開発ニーズをサポートするために、エネルギー流通システムのためのサイバーセキュリティ（Cybersecurity for

---

[131] 国家情報保証パートナーシップ概要説明　http://www.niap-ccevs.org/
[132] 「クラウドにおける暗号生成の自動化とアウトソーシング」プロジェクト概要
http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=1154035&WT.z_pims_id=504709
[133] ホールマーク暗号シリアル・コミュニケーション、DOE
http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Hallmark_Cryptographic_Serial_Communication.pdf

Energy Delivery System: CEDS）プログラムを設立した。DOEのCEDSプログラムでは、研究開発、脆弱性の査定と軽減、統合リスク分析、そして業界アウトリーチを行うために、政府、国立研究所、ベンダ、システム・インテグレータ、学究界、そしてステークホルダ間の連携を推進する。同プログラムの資金支援を通じて、業界側と国立研究所で連携して、脆弱性の検証施設である監視制御・データ取得 テストベッド（National SCADA Test Bed: NSTB）などを活用して技術の研究開発及び実証試験を進める[134]。

DOEは「2006 年配電システムのサイバーセキュリティ達成ロードマップ（2006 Roadmap to Secure Control Systems in the Energy Sector）」[135]の中でよりサイバーセキュリティに優れたSCADAシステムの必要性を強調している。DOEのCEDSプログラムは 2007 年 10 月、今後 3 年間でSCADAシステムに関連したソリューションの開発と商用化を推進するためにプロジェクト公募を開始し、DOEと業界は最終的に シュバイツァー・エンジニアリング研究所 （Schweitzer Engineering Laboratory: SEL）のホールマーク・プロジェクト（Hallmark Project）を含む 5 つの共同プロジェクトに対し、総額 1,000 万ドル以上の出資を行っている。ホールマーク・プロジェクトでは、既存及び新しいエネルギー制御システムへセキュアなシリアル通信[136]を提供する独自の暗号技術を開発した。同プロジェクトにおいてはSELが主導し、PNNLとセンターポイント・エネルギー（CenterPoint Energy）が提携している。SANDIAセンタ（SANDIA Center for SCADA Security）に設置された暗号技術の研究施設である暗号研究センタ（Cryptographic Research Facility）もプロジェクトを支援している。

ホールマーク・プロジェクトの研究開発フェーズでは、まず PNNL が、メッセージ認証と暗号オプションによる制御システムのデータ・インテグリティを保証する、セキュアな SCADA コミュニケーション・プロトコル（Secure SCADA Communications Protocol: SSCP）を開発した。このプロトコルでは、オリジナル・メッセージに、ユニークな識別子と認証コードを付ける。次に送信先のデバイスが識別子をスキャンして、情報が信頼できるソースからのものであり、送信中に改ざんされていないことを保証しながらメッセージを認証する。

---

[134] CEDS プログラム http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity
[135] 「2006 年配電システムのサイバーセキュリティ達成ロードマップ」 http://www.cyber.st.dhs.gov/docs/DOE%20Roadmap%202006.pdf
[136] シリアル通信（serial communication）とは、電気通信において伝送路上を一度に 1 ビットずつ、逐次的にデータを送ることをいう。

DOE の SEL-3045 カード

出典: DOE[137]

SEL は、SSCP を上記の SEL-3045 暗号カードへ統合した。OEM 向けに 2010 年 6 月に商業リリースされた SEL-3045 は、SSCP を実行する電子カードである。リモート・デバイスと制御センター間のオリジナル SCADA メッセージへユニークなヘッダーと認証コードを付けて封入したもので、それを受け手のデバイスが認証し、メッセージが信用できるソースからのものであり、送信中に改ざんされていないことを保証する。また、連邦情報処理標準（Federal Information Processing Standard: FIPS）140-2 レベル 2 認証暗号に基づき安全性と相互運用性を保証する。

ホールマーク・プロジェクトの研究は継続されており、プロジェクト・チームにはシーメンス・エナジー（Siemens Energy）とONCOR エレクトリック・デリバリー（ONCOR Electric Delivery）が新たに参加している。現在は、暗号キー管理プロセスの集中化や、アクセス制御におけるSSCPの利用に焦点を置いており、PNNLが、業界で承認され、拡張性があり、かつステークホルダの運用ニーズを満たす暗号キーを管理するソフトウェア・アプリ

---

[137] ホールマーク暗号シリアル・コミュニケーション、DOE
http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Hallmark_Cryptographic_Serial_Communication.pdf

ケーションの開発に取り組んでいる[138]。

DOE CEDSプログラムは2010年10月、米国配電網向けにさまざまなサイバーセキュリティ・ソリューションを研究、開発、商業化するために、新たに8つのサイバーセキュリティ研究開発プロジェクトに対して、総額 2,000 万ドルを給付している。代表的なプロジェクトには、シプリス・エレクトロニクス（Sypris Electronics）が310万ドルの研究開発費を受け取って実施している、スマートグリッドの先進メーター・インフラ内にある何百万というスマート・メーターのコミュニケーションを保証する暗号キー管理の集中化機能の開発プロジェクトがある[139]。

（3）DHS

DHS セキュア・ワイヤレス・アクセス・プロトタイプ（DHS Secure Wireless Access Prototype）

DHS 科学技術局（Science and Technology Directorate: S&T）内の命令・制御・相互運用部（Command, Control and Interoperability Division: CCID）は、米国にとって脅威となる可能性がある行動を特定することを目的として、サイバーセキュリティに関する標準化の策定やツール及び技術の開発を進めている。CCID のサイバーセキュリティ・プログラム・エリア（Cyber Security Program Area）では、DHS の任務及び大統領のサイバーセキュリティ国家戦略（National Strategy to Secure Cyberspace）においてサイバーセキュリティに関連して優先に取り組むべきとされている項目をサポートするための研究開発、実証実験、評価を推進している。

CCIDのサイバーセキュリティ・プログラム・エリアが、S&Tの最高情報責任者局（Office of the Chief Information Officer: OCIO）と連携して、2009～2010年にかけて取り組んでいた研究開発の一つに、DHSセキュア・ワイヤレス・アクセス・プロトタイプ（DHS Secure Wireless Access Prototype: DSWAP）がある。DSWAPは、モバイル・ユーザから保護されたネットワークまでを対象に、複層構造の強力な防御を提供するセキュアなワイヤレス・アクセス・ソリューションであり、BAEシステムズ（BAE Systems）がDHSより受け取った19万6,722ドルの研究資金を当てて開発した。DHSは、2010年にDHS職員が公衆ネットワークを利用した際にも安全にDHSのネットワークに接続できるようになることを目的として、DSWAPのパイロットを実施した[140]。2010 年に行われたパイロットは 5 週間に渡って実施され、40 名強のユーザが参加した。DHSでは 2010 年以降、他にも

---

[138] 「エネルギー配電システムサイバーセキュリティに関するロードマップ」、（p. 25）
http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf

[139] シプリス・エレクトロニクス研究資金受給に関する説明
http://www.sypris.com/sypris-electronics/media/press-releases/sypris-awarded-31-million-of-funding-from-the-department-of-energy-project-to-protect-us-power-grid/22

[140] DSWAP に関連する概要説明 http://www.cyber.st.dhs.gov/competitions/

DSWAPプロトタイムの小規模試験を実施している[141]。

2.3.3. 暗号技術の応用分野に関する研究開発活動を行なっている主要研究所

（1）DARPA

＜研究機関プロフィール＞
DARPA内に暗号技術の研究を専門とした部署は設置されていないが、CSIAに関しては同省の情報イノベーション局（Information Innovation Office: I2O）が研究プログラムを管轄している。I2Oは、米国の軍任務に貢献できる先進的なICTの研究開発を推進するために設置されており、CSIAだけでなく医療ITや機械学習、データ管理、言語処理、クラウド技術など軍の通信や任務に利用できる多様な分野や技術を研究対象としている[142]。40 以上の研究プログラムを有するI2Oで、暗号技術に関する研究プログラムが 2011 年 2 月に設置された後述する「暗号データ・プログラミング・コンピュテーション（Programming Computation on Encrypted Data: PROCEED）」プログラムである。暗号データに関する複雑の計算を、解読せずにそのまま活用するという 30 年来の問題に対し、IBM社の研究員であるCraig Gentry氏が 2009 年にソリューションを発表して以来[143]、DARPAにおいてもこの開発に取り組んでおり、データを暗号化し、それらを使用、操作させる手法である完全準同型暗号の開発を推進するため同プログラムが設定された[144]。暗号データを最初に解読する必要がなくなれば、マルウェア・プログラマーによるウイルス作成は格段に難しくなる。

＜研究プロジェクト概要＞
完全準同型暗号（Fully Homomorphic Encryption）

完全準同型暗号により、暗号データを最初に解読する必要がなくなれば、マルウェア・プログラマーによるウイルス作成は格段に難しくなり、信頼できない環境におけるコンピュテーションのあり方を抜本的に変える可能性があるため DARPA が注目している技術である。完全準同型暗号では、クライアントはデータをクラウドへ送る前に暗号化しなければならない。その後、実行コードをクラウドへ提供することにより、データを解読しなくても処理できるようになり、処理結果は、暗号化されたままの状態でクライアントに戻される。従って、クライアントだけが暗号解読鍵を制御するため、他の誰もデータや結果を解読す

---

[141] 「DHS2010 年度予算」
http://www.iaem.com/committees/governmentaffairs/documents/dhsbudgetinbrieffy2010.pdf
[142] DARPA I2O 概要紹介 http://www.darpa.mil/Our_Work/I2O/
[143] Craig Gentry 氏の研究概要 http://crypto.stanford.edu/craig/craig-thesis.pdf
[144] PROCEED 概要紹介
http://www.darpa.mil/Our_Work/I2O/Programs/PROgramming_Computation_on_EncryptEd_Data_%28PROCEED%29.aspx

ることができず、それにより情報のセキュリティを保証する。これについては、理論上は可能だが、Gentry 氏によると暗号データの計算速度がひとつの問題点として指摘されている。

この問題を解決するために、DARPA は PROCEED プログラムの一環として、コントラクタや学究研究チームを対象に 4 年間で総額 2,000 万ドルの研究資金を拠出している。

PROCEED では、プログラマーが操作中であってもデータを暗号で保護されたままにする技術の開発を目指すとともに、完全準同型暗号にかかる計算時間を現在の 1000 万分の 1 に短縮する、あるいはその計算量を、暗号化されていない計算にかかる時間のに 10 万分の 1 に削減することにより、暗号データの計算を実用化させたい考えである。PROCEED は 2011 年 2 月、SRI インターナショナル（SRI International）に勤務していた Drew Dean 博士をプログラムマネージャとして招き、同氏の管理下で研究を開始した。完全準同型暗号の数学的基礎をはじめ、セキュアな複数者間における計算、ハードウェアとソフトウェア導入の最適化、プログラミング言語・アルゴリズムそしてデータ・タイプに関する研究をサポートする計画である。

DARPAから資金提供を受け、Craig Gentry博士と IBMワトソン研究センタ（IBM Watson Research Center）のShai Halevi博士、そしてブリストル大学（University of Bristol）のNigel P. Smart博士 は 2011 年 10 月に「ポリログ・オーバーヘッド完全準同型暗号（Fully Homomorphic Encryption with Polylog Overhead）[145]」、同年 12 月に「完全準同型暗号におけるより良いブーストラッピング（Better Bootstrapping in Fully Homomorphic Encryption）[146]」と題した論文を発表し、準同型評価プロセスをスピードアップする最適化について紹介している。

2011 年初めには MIT の Zvika Brakerski 博士 と Vinod Vaikuntanathan 博士が論文 2 件を発表し、完全準同型暗号を効率化する幾つかの方法を説明したことが報告されている。その一例として、完全準同型暗号の計算を顕著に簡素化し、処理時間の短縮を実現した。また、暗号キー生成のために使用する数学的構成を、セキュリティを妥協することなく簡素化できる可能性が示唆されている。

この発見は、完全準同型暗号の実用的アプリケーションへ道を開くことを約束するものであり、新しい最適化されたシステムは、Gentry氏のオリジナル構造よりも数百倍または数千倍も高速化される可能性がある。潜在的アプリケーションの一つは、研究用医療情報の保護である。個々の個人情報へアクセスすることなく、第三者が暗号化された医療記

---

[145] 「ポリログ・オーバーヘッド完全準同型暗号」、Gentry, Craig. http://eprint.iacr.org/2011/566.pdf
[146] 「完全準同型暗号におけるより良いブーストラッピング、」、Gentry, Craig. http://eprint.iacr.org/2011/680.pdf

録を基に大規模な医学的研究を行えるようにする[147]。

(2)IARPA

＜研究機関プロフィール＞
IARPAは、国家情報長官(Director of National Intelligence)の権限下に設置されている研究機関で、中央情報局(Center Intelligence Agency: CIA)、連邦捜査局(Federal Bureau of Investigation: FBI)やNSAなど複数の諜報機関を横断して、単独の機関では実現できないよりハイリスク・ハイリターンな先進的技術の研究を推進している。IARPAの特徴は、開発されれば必ずイノベーションに繋がると思われる非常に高度で、最も優先度が高い技術のみを対象として、3～5 年という比較的長いプロジェクト期間を設定して技術の研究のみに注力することである。IARPAではあくまで研究に重きを置くため技術の商用化は推進していない[148]。

IARPAには、タイムリーな情報分析を目指した研究を進めるデータ分析室(Office of Incisive Analysis)、セキュリティに関連する研究を担当する安全でセキュアなオペレーション室(Office of Safe and Secure Operation)、収集したデータの質を改善することを目指すスマートコレクション室(Office of Smart Collection)の 3 つの部署から構成されており、暗号技術に関する技術研究も安全でセキュアなオペレーション室が担当する[149]。同室において現在推進されているサイバーセキュリティに関連するプロジェクトが暗号プロトコルのプロトタイプの導入と準同型暗号技術の開発を目指す「セキュリティとプライバシー保証研究(Security and Privacy Assurance Research: SPAR)」である[150]。

＜研究プロジェクト概要＞
SPAR プログラム

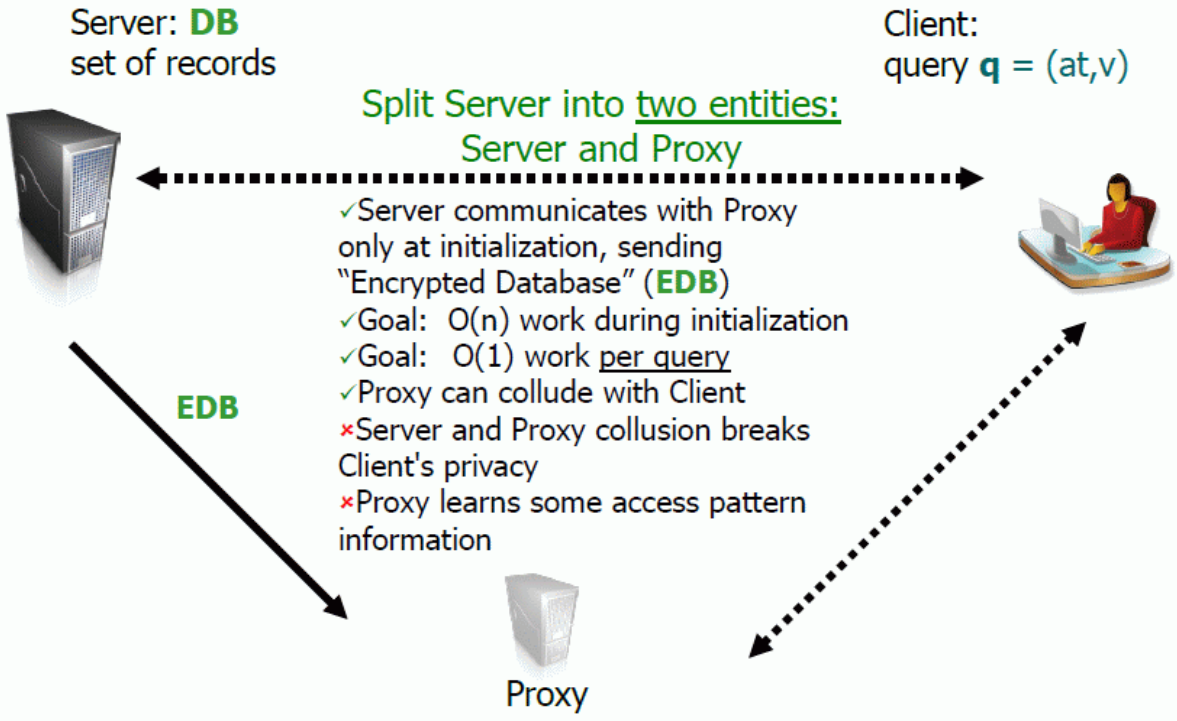
IARPAは、SPARと呼ばれるPROCEEDと似たプロジェクトを助成している。SPARプログラムは、データを暗号化することでセキュリティとプライバシーを保護するかたちで安全にデータ交換を行うための技術を開発し、実証実験を行うことを目的としている。SPARでは、クライアントのクエリーが承認されたものであることをサーバー側で検証できるようにする暗号クエリーに関連する、ポリシー・コンプライアンス検査アルゴリズムの開発を計画している。また、暗号化したデータのクエリーを導入するための有効な準同型暗号技術も研究する[151]。

---

[147] Zvika Brakerski 博士 と Vinod Vaikuntanathan 博士の研究内容
http://www.thecuttingedgenews.com/index.php?article=53415
[148] IARPA 概要説明 http://www.iarpa.gov/index.html
[149] IARPA 組織概要 http://www.iarpa.gov/index.html
[150] SPAR プログラムに関する概要説明 http://www.iarpa.gov/manager_vesey.html
[151] 「2010 データマイニング報告書」、国家情報局(Office of Director of National Intelligence)(p. 10)

SPARプログラムは 2010 年 12 月 29 日に公示され、2011 年 3 月 4 日に公募が締め切られた。SPARプログラムでは、公示の際にプログラムの開始を 2011 年 6 月、また 2014 年 11 月までに完了する計画としていた。SPARプログラムに選出された代表的なプロジェクトには、IBMリサーチ（IBM Research）が 3 年間の契約で 75 万ドルを研究資金として受け取った、「データベース・アクセスのための効率的なセキュリティとプライバシー保証（Efficient Security and Privacy Assurance for Database Access: ESPADA）」がある。IBM Researchは同プロジェクトの実施にあたり、研究をカリフォルニア大学アーバイン校（University of California Irvine）に委託しており、複数のパーティー間で効率的かつ安全にデータを交換するためのデータベースクエリーをサポートできるようにすることを目的としたプロジェクトである[152]。下図に示されるように、データベースとクライアントの間にプロキシを設け、初期設定の際にデータベースのデータを暗号化してプロキシに送ることで、データベースにはクライアントからクエリーの情報が残らず、セキュリティとプライバシーを保護できる仕組みになっている。

カリフォルニア大学アーバイン校が提案する ESPADA



出典: NIST[153]

---

http://www.fas.org/irp/dni/datamining11.pdf

[152] 「IARPA SPAR プログラム」プレゼンテーション資料、Jarecki,Stanislaw(カリフォルニア大学アーバイン校)
http://csrc.nist.gov/groups/ST/PEC2011/presentations2011/jarecki.pdf

[153] 「IARPA SPAR プログラム」プレゼンテーション資料、Jarecki,Stanislaw(カリフォルニア大学アーバイン校)（p. 10）

（3）NIST

＜研究機関プロフィール＞
NISTでは、コンピュータ・ベースの経済活動の開発に拍車をかけるオープン・システムと相互運用性の促進を目指している。NISTは米国内の全てのコンピュータ・システムに採用されるべき標準とガイドラインを発行し、ワークショップとセミナーも主催する。また、連邦政府の民間コンピュータ・システムにおいて使用が必要とされ、民間でも自主的に頻繁に採用されている暗号アルゴリズムの標準を発行する。これらの標準は、連邦情報処理標準（Federal Information Processing Standard: FIPS）180-2 に収められている[154]。

NISTにおいて暗号技術の研究開発を推進しているのが、IT研究所（Information Technology Laboratory: ITL）下に設置されているコンピュータセキュリティ・リソースンタ（Computer Security Risource Center: CSRC）である。同センタには、当初①暗号技術（Cryptographic Technology）、②システムと技術セキュリティ研究（Systems and Engineering Security Research）、③セキュリティ管理と保証（Security Management and Assurance）、④暗号モジュール認証と暗号アルゴリズム認証プログラム（Cryptographic Module Validiation Program and Cryptographic Algorithm Validation Program）という 4 つの研究グループが設置されていたが、現在は④暗号モジュール認証と暗号アルゴリズム認証プログラムが、③セキュリティ管理と保証グループに統合されたため、3 つのグループにより構成されている[155]。①の暗号技術グループは、暗号キー技術、先進的認証システム、暗号プロトコル及びインタフェース、公開鍵認証管理、スマートトークンなど暗号技術全般に関する研究を推進しており、DOEやNSAなどの連邦政府機関だけでなく、国内外の標準化団体やマイクロソフト（Microsoft）、ヒューレット・パッカード（Hewlett Packard）などの大手IT企業とも連携している[156]。また、暗号モジュール認証と暗号アルゴリズム認証プログラムは、FIPSで規定されているまたNISTが推奨する暗号モジュール及び暗号アルゴリズムの認証試験を推進する目的で 1995 年に設置されたプログラムである。

CSRCでは、上記の 3 つのグループにおける活動以外に、2007 年 11 月に発表した新たな暗号ハッシュアルゴリズム（Cryptographic Hash Algorithm）の開発を目的としたコンペを実施している[157]。

---

http://csrc.nist.gov/groups/ST/PEC2011/presentations2011/jarecki.pdf
[154] http://gcn.com/articles/2011/01/10/sha-3-secure-hash-finalists.aspx
[155] NIST CSRC 概要説明　http://csrc.nist.gov/index.html
[156] NIST CSRC　暗号技術グループのページ　http://csrc.nist.gov/groups/ST/index.html
[157] NIST CSRC　暗号技術ハッシュアルゴリズムコンペ　http://csrc.nist.gov/groups/ST/hash/sha-3/index.html

＜研究プロジェクト概要＞
暗号ハッシュ・アルゴリズム[158]

SHA-1 を含む暗号ハッシュ・アルゴリズムに対する深刻な攻撃が報告されたこと、そしてSHA-1 と SHA-2 ファミリーは設計が類似していることから、NIST は 2008 年、新しい暗号ハッシュ・アルゴリズム開発のための研究公募を開催した。

新しいハッシュ・アルゴリズムは、FIPS 180-2 で定めるハッシュ・アルゴリズム、セキュリティア・ハッシュ・スタンダード（Secure Hash Standard）を補強することが期待されている。NIST の目標は、セキュリティを改善し、暗号ハッシュ・アルゴリズムを利用するアプリケーションの効率を大幅に向上する SHA-3 を開発することである。

SHA-3 公募は 2008 年に開始され、64 のアルゴリズムが提案され、そのうち 51 がNISTの最低条件を満たし、2010 年 12 月 9 日、最終選考に残った 5 件が発表された。NISTでは 2013 年春に最後のSHA-3 候補会議（SHA-3 Candidate Conference）を実施し、第 3 ラウンド候補について一般のフィードバックを踏まえた上で、2012 年末に 1 件のプロジェクトを選定する計画である[159]。選ばれたアルゴリズムはその時点で、FIPS 108-3 のデジタル署名作成と他の政府文書認証向け承認ハッシュ・アルゴリズム一覧に掲載される。

（4）IBM

＜研究機関プロフィール＞
IBMはサイバーセキュリティに関して、他企業と協力し事業におけるサイバー脅威への理解をより深めるためのグローバルイニシアチブであるIBM Institute for Advanced Securityを米国、欧州、アジア太平洋地域の 3 地域に設立している[160]。次世代のセキュリティ・モデルやソリューションのイノベーションを促進するため、IBM Institute for Advanced Securityを通してIBM X-Forceをはじめとするセキュリティ研究所や、IBMのサービス、ソフトウェア、テクノロジー専門家を企業に紹介する他、IBMセキュリティ研究所における専門知識や研究内容、成果、報告書などの情報を提供することを目指している。

IBM Institute for Advanced Security下に設置されているX-Force先進研究開発チーム（X-Force Advanced Research and Development Team）は[161]、サイバーセキュリティ

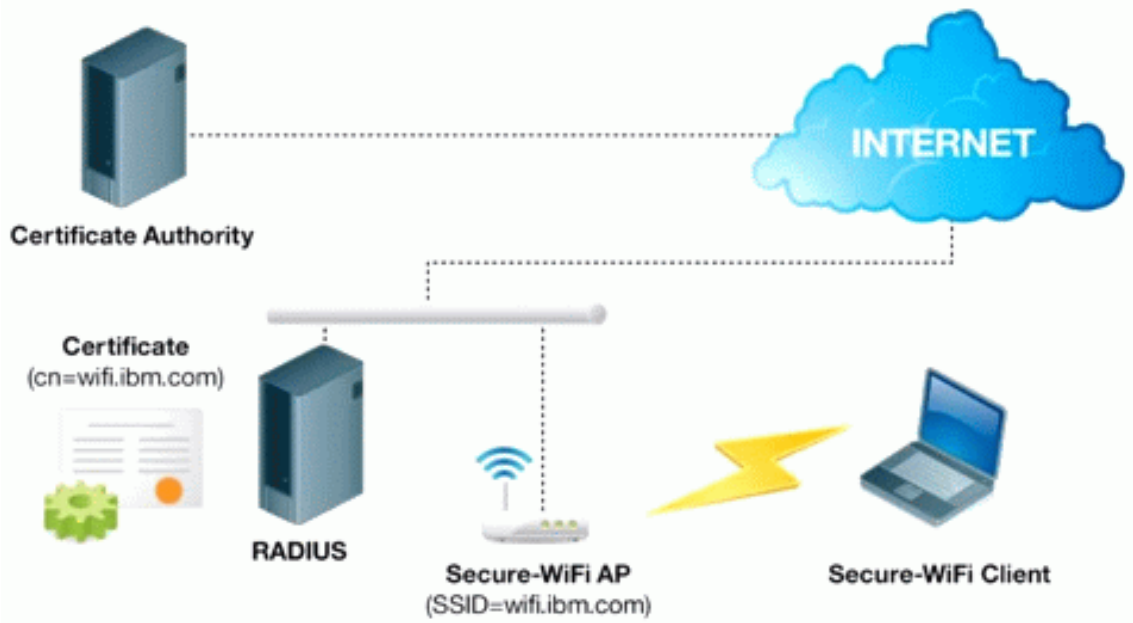
---

[158] NIST CSRC 暗号技術ハッシュアルゴリズムコンペ http://csrc.nist.gov/groups/ST/hash/sha-3/index.html
[159] NIST 暗号ハッシュアルゴリズムコンペ http://www.nist.gov/itl/csd/ct/hash_competition.cfm
[160] IBM Institute for Advanced Security の概要説明
http://instituteforadvancedsecurity.com/ias/about-us/default.aspx
[161] X-Force 先進研究開発チームの概要説明 http://www-935.ibm.com/services/us/iss/xforce/

に関する民間企業の研究機関としては世界トップクラスに位置付けられている。同チームは、インターネットセキュリティ問題、IBM製品におけるサイバー脅威の分析・査定・対応技術の開発、セキュリティ脅威に関する他企業や一般市民に対する教育を実施しており、セキュリティ脅威や脆弱性に関する研究内容をX-Force報告書の中で発表している[162]。

＜活動概要＞
IBM X-Force先進研究開発チームは、セキュアな環境でオープン・ワイヤレス・システムを運用するための技術を長年研究してきた。この研究は、X-Force 先進研究開発チームの Tom Cross 氏（プロジェクトマネージャ）が主導している。同氏が研究開発を進めたセキュア・オープン・ワイヤレス（Secure Open Wireless）では、アクセスポイントのオペレータが正式なアクセスポイントの識別子（SSID）のユーザであることを証明するデジタル認証を通して、パスワードを設定する必要なく暗号化されたセキュアな接続を確立することができることを目指した。IBM は 2011 年のブラック・ハット（Black Hat 会議）でセキュア・オープン・ワイヤレスの実証実験を行った。

IBM のセキュア・オープン・ワイヤレス・ネットワーキング・モデル



出典: IBM[163]

[162] X-Force 報告書 http://www-935.ibm.com/services/us/iss/xforce/trendreports/
[163] 「セキュアでオープンなワイヤレスネットワーキング」、Cross, Tom. IBM、2011 年 8 月 16 日
http://www.instituteforadvancedsecurity.com/expertblog/2011/08/16/secure-open-wireless-presentation/

上図に示されるように、この手法では、EAP-TLS（Extensible Authentication Protocol- Transport Layer Security）を利用し、セキュアな接続を確立するためにデジタル証明書を利用する。EAP-TLSとは、無線LANなどで利用される認証規格「IEEE 802.1x」に対応した、認証プロトコルである。セキュア・オープン・ワイヤレスでワイヤレス・アクセスポイントSSIDとデジタル証明書をリンクさせることにより、ユーザが接続を確立する際に、トラフィックが暗号化されており、合法的アクセス・ポイントであることを同証明書で示す[164]。

2.3.4. 暗号技術の応用分野の技術開発の係る将来的な展開・方向性

NSFのコンピュータ・情報科学・エンジニアリング局（Computer and Information Science and Engineering Directorate）の副局長Farnam Jahanian博士によると、完全準同型暗号は、将来のためにさらなる開発が必要であるとしている。開発が進めば、現在暗号化されたコミュニケーションが新らきできなネットワークを利用して行われているのと同様に、信頼できないプラットフォーム（急速に増えている分散クラウド・プラットフォームなど）上で暗号化された計算ができるようになる可能性がある[165]。

サイバーセキュリティに関連した攻撃や脅威は今後ますます複雑さを増していくことが予想されることからも、サイバーセキュリティ向けの連邦助成は、2017 年までは増加、または少なくとも安定して推移することが予測される。NSF の信頼できるコンピューティング・プログラム元ディレクタの Carl Landwehr 博士によると、当面の研究開発における優先事項はユーザ認証、マルウェア検知と排除、大型データ・セットを利用するモニタリング・検知などであり、長期的な優先項目には、システム構築手法の改良、自動多様性（automated diversity）、暗号化が挙げられている。

また、攻撃者とユーザ双方の行動をより良く理解するために、サイバーセキュリティに社会科学者や経済学者の観点を包含する必要性が高まっている。社会科学の観点も取り入れることで、攻撃の予測と認識がより容易にできると期待される。情報セキュリティ経済に関するワークショップ（Workshop on the Economics of Information Security）といったイベントなどでコンピュータ科学者と他分野の専門家の議論も推進されているが、互いに極めて専門性が高い分野でもあるため、専門知識を有していない者同士で効率的な議論を行うことは難しいのが現状でもある。そのため、社会科学とコンピュータ・セキュリティの両方の専門知識を持つ人材が、ますます求められている。

---

[164] IBM セキュアオープンワイヤレス概要
http://threatpost.com/en_us/blogs/ibm-unveil-secure-open-wireless-system-black-hat-080311
[165] Farnam Jahanian 博士の発言内容 http://www.nsf.gov/about/congress/112/fj_cybersecurity_110525.jsp

サイバー攻撃が急速に広がりその複雑さも増していることが示唆するものは、人間のセキュリティと同じように究極のサイバーセキュリティは、対策はできるが完全に防ぐことはできないという、根本的に直せない問題であることがやがて証明されるということである。そのため研究開発は、完全にセキュアなシステムの構築というよりは、サイバー攻撃にいかに対応し、またそれを切り抜けるかといった点により重点を置くことになると見られる。

3. 米国の研究開発機関における国際共同研究の推進活動及び成果展開に関する事例調査･研究開発動向等の調査

3.1. 米国における国際共同研究開発活動の事例

3.1.1. 米国／ハンガリー・サイバーセキュリティ共同研究（US/Hungary Collaborative Cyber Security Research）[166]

概要

サウスカロライナ大学コロンビア校（University of South Carolina, Columbia）の Csilla Farkas 教授は、特定のユーザで構成されるオンラインコミュニティにおけるプライバシーとセキュリティ強化につながるフレームワークの研究と開発のため、ハンガリーの大学 2 校（ブダペスト工科大学とエオフトフ・ロランド大学）の教授陣と共同研究を行った。研究は 2002 年から現在に至るまで実施され、多くの論文が発表されている。

組織構造と参加機関

サウスカロライナ大学とハンガリーの大学間における小規模でインフォーマルなパートナーシップをベースとしている。従って、公式な共同研究協定の締結といった形式にとらわれず、個々の研究者間におけるコラボレーションが機軸となっている。

役割分担

サウスカロライナ大学の Farkas 博士は、ハンガリー出身のサイバーセキュリティやプライバシーを専門分野とする研究者であるが、ハンガリーの母校を訪ねた際に、米大学との研究コラボレーションの話が生まれ、個人の研究者レベルでの協力関係から始まったと、同博士は話している。そのことからも、特に正式な役割分担というものはなく、あくまでも相互の補完できる研究テーマなどに絞り込んで活動を継続しているという。主に、ハンガリー側は、人工知能やオンラインコミュニティに関する技術研究の蓄積を、米国側はサイバーセキュリティやプライバシー分野における研究成果を持ち合い、統合・連携することで、オンラインコミュニティにおけるセキュリティやプライバシーに係る基礎研究に取組んでいる。

資金源

サウスカロライナ大学コロンビア校によるこの共同研究への参加は、NSF から資金提供を受けて実施された。一方、ハンガリーの大学は、ハンガリー政府から助成を受けている。

---

[166] サウスカロライナ大学コロンビア校 Csilla Farkas 教授プロフィール、http://www.cse.sc.edu/~farkas/

研究内容
この研究の目的は、様々なオンラインコミュニティと、それらを通したコラボレーション活動に対して、セキュリティとプライバシーを提供するフレームワークを開発することである。

研究成果の評価方法と帰属
Farkas 教授はハンガリー側の教授と協力し、オンライン・コミュニティのためのセキュリティとプライバシー・フレームワークに関する研究を基に論文５件を発表し、研究者たちは、フレームワークをサポートするセキュリティ・プロトコルとアーキテクチャを開発しており、こうした論文発表や開発実績数を評価基準として捉えている。

同教授によると、この国際共同研究によって現在までに、具体的な知的財産権を取得した成果はないという。また現時点において、知的財産の帰属に関しても、正式な取り決めはまだ行っていないとしている。いずれにしても今後、具体的な知的財産権に係るような成果が出てきた場合、サウスカロライナ大学の知的財産権管理室が、ハンガリー側の関係者と協議・交渉し、ケースバイケースで対応していくとしている。

3.1.2. オープン科学データ・クラウド（Open Science Data Cloud）[167]

概要
オープン科学データ・クラウド（Open Science Data Cloud: OSDC）は、科学データの分析と共有、アーカイブのために科学者が使用する、オープンソース・クラウド・コンピューティング・インフラを提供するシステムである。米国及び海外大学間の連携を通じ、学生や若手研究者を対象に、オープン・クラウドと科学的コンピューティング分野の研究と研修機会を提供する。

組織構造と参加機関
OSDCを管理するオープン・クラウド・コンソーシアム（Open Cloud Consortium: OCC）[168]は、科学コミュニティによって使用されるオープンソース・クラウド・コンピューティング・インフラを構築し、運用するコンソーシアムである。OCCは、コンピュテーショナル科学・研究センタ（Center for Computational Science and Research: CCSR）[169]の管理下にある。CCSRはイリノイ州に拠点を置く非営利団体で、クラウド・コンピューティング基盤のオープンソース科学コンピューティング・インフラの開発を支援するために設立された。
CCSRは、OCCメンバーと協力してOSDCを監督する。OCCメンバーには、連邦政府機

[167] OSDC 概要説明 http://www.opensciencedatacloud.org/
[168] OCC 概要説明 http://opencloudconsortium.org/
[169] CSRC 活動概要 http://www.csrc.sdsu.edu/

関を含む、以下の組織が含まれている[170]。

- シトリックス（Citrix）
- シスコ（Cisco）
- レイセオン（Raytheon）
- イリノイ大学シカゴ校（University of Illinois, Chicago）
- シカゴ大学（University of Chicago）
- ジョンズ・ホプキンス大学
- NASA
- オークリッジ国立研究所（Oak Ridge National Laboratory）
- ローレンス・リバモア国立研究所（Lawrence Livermore National Laboratory）

OCC は、オープン・クラウド・コンピューティングと科学インフラのそれぞれ異なる側面に取り組む、複数のワーキング・グループで構成される。そのうちの一つが OSDC ワーキング・グループ（OSDC Working Group）で、責任者のイリノイ大学シカゴ校の Robert Grossman 博士は、OSDC 自体の開発と運用を支援する目的で支給された NSF 補助金の研究プロジェクト責任者である。

NSF は、米国内の OCC 大学院生や研究者を対象に、米国及び国際パートナーと共同で行う短期的研究や研修活動に資金を拠出している。OSDC の米国及び国際パートナーは以下の通り。

- イリノイ大学シカゴ校（米国）
- フロリダ国際大学（Florida International University）（米国）
- エディンバラ大学（University of Edinburgh）（英国）
- フルミネンセ大学（Universidade Federal Fluminense）（ブラジル）
- アムステルダム大学（University of Amsterdam）（オランダ）
- 産業技術総合研究所（Agency of Industrial Science and Technology : AIST）（日本）
- 韓国科学技術情報研究院（Korea Institute of Science and Technology Information）（韓国）
- 北京ゲノミクス研究所（Beijing Institute of Genomics）（中国）
- サンパウロ大学（State University of Sao Paulo）（ブラジル）

[170] OCC 参加機関　http://opencloudconsortium.org/members/

役割分担
OCC メンバーは OCC に対し、NIH が助成する遺伝子配列解明技術プロジェクト、modENCODE といった科学プロジェクトのために、OSDC が提供するインフラの使用を申請することができる。OCC に使用が承認されると、科学プロジェクトの指導的立場の研究プロジェクト責任者がプロジェクトそのものを統括し、CCSR は、プロジェクトで利用される OSDC インフラを引き続き監督する。

資金源
NSFは 2010 年「国際研究・教育パートナーシップ（Partnerships for International Research and Education: PIRE）」[171]を通じて 5 年間で総額 350 万ドルの補助金をOSDCに支給した。この補助金は、PIREの下で科学コンピューティングに関する短期研修と研究に取り組む米国の大学院生及び米国の若手研究員のために使われる。NSFの資金は、これら海外の研究機関で研究に従事する米国の研究者と米国学生の共同研究をサポートするためだけに使われるものとなっており、海外の研究機関が必要とするその他の研究資金は、それぞれの機関が独自に調達している。

また、OSDC に必要とされる各種研究機器・装置の調達に関しては、ゴードン・アンド・ベティー・ムーア財団（Gordon and Betty Moore Foundation）やヤフー（Yahoo）、などの民間企業や慈善団体からの寄付などによってまかなわれている。

研究（支援）内容
NSF による OSDC に対する PIRE 補助金の目的は、科学データの分析、共有、アーカイブのためのオープン・クラウド・コンピューティング・インフラの提供を促進することである。PIRE を通して、科学コンピューティング分野における次世代の研究者を育成することに加え、国際共同研究の枠組みを広げ、オープンクラウドを利用するなどグローバルな研究コミュニティを創設することを目指している。従って、特定の研究開発にフォーカスするのではなく、国際的な共同研究活動を促進することに重きを置いており、この支援を受けて進められる個々の国際共同研究内容については、情報は公開されていない。

研究成果の評価方法と帰属
成果の評価方法については、OSDCのプロジェクト概要を記載するサイトにおいて３つのプロジェクトをコンピューティング・インフラを構築する上での成果として評していることから、この研究で構築されるオープン・クラウド・コンピューティング・インフラを活用した研究プロジェクト件数などがひとつの評価基準として、捉えられているものと見られる[172]。成果の帰属に関しては、オープンソースをベースとしたプロジェクトであることからも、特に明確なルールなどは存在しないものと推測されるが、正確な情報は得られなかった。

---

[171] PIRE 概要・活動説明 http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=12819
[172] OSDC プロジェクト概要（プロジェクト成果について） http://www.opensciencedatacloud.org/osdc-projects/

3.1.3. 米国／英国・次世代インターネットに関する研究（US/UK Research on Next Generation Internet）

概要

カンザス大学（University of Kansas）と英国ランカスター大学（Lancaster University）は、プログラム可能な光ネットワーク・テストベッドを構築し、それを利用して次世代インターネット・アーキテクチャのための試験を行う国際連携を主導している。

組織構造と参加機関

カンザス大学は、「ネットワーク・イノベーションのためのグレート・プラン環境（Great Plans Environment for Network Innovation: GpENI）」[173]と呼ばれる、地方テストベッドで接続された中西部の大学コンソーシアムを率いている。GpENIに参加する各大学は、独自のGpENIネットワーク・ノードを運用し、他の参加大学と相互接続される。GpENIは、先進の全米テストベッドを利用して将来のインターネット・アーキテクチャのためのネットワーキング研究開発を実施するNSFのプログラム「ネットワーク・イノベーションのためのグローバル環境（Global Environment for Network Innovations: GENI）」[174]を構成する地方コンソーシアムである。GpENIに参加する大学と民間パートナーを以下に示す：

- カンザス州立大学（Kansas State University）
- ミズーリ大学カンザス・シティ校（University of Missouri, Kansas City）
- ネブラスカ大学（University of Nebraska）
- イリノイ工科大学（Illinois Institute of Technology）
- シエナ（Ciena）
- クエスト（Qwest）
- ランカスター大学（Lancaster University）（英国窓口）

ネットワークはGpENI参加機関を相互接続するほか、欧州の研究パートナーとも接続されている。GpENIの欧州パートナーは、次世代インターネット・アーキテクチャの開発を通してネットワーク・レジリエンスの改善を図る、「レジュームネット（Resilience and Survivability for Future Networking: ResumeNet）」と呼ばれるコンソーシアムを組織している[175]。レジュームネットを主導するのはランスター大学である。レジュームネットの参加大学と企業は次の通り：

- ランカスター大学（統括機関）
- ETH チューリッヒ（ETH Zurich

---

[173] GpeNI 概要説明 http://groups.geni.net/geni/wiki/GpENI
[174] NSF GENI 概要説明 http://www.geni.net/
[175] ResumeNet 概要説明 http://resumenet.eu/

- ミュンヘン工科大学（Techniche Universitat Munchen）
- デルフト工科大学（Techniche Universiteit Delft）
- リージェ大学（Universite do Liege）
- パッサウ大学（Universitat Passau）
- ウプサラ大学（Uppsala Universitet）
- NEC ハイデルベルグ研究所（NEC Labs Heidelberg）
- フランス・テレコム（France Telecom）／オレンジ研究所（Orange Labs）
- カンザス大学

役割分担

前述のように、GpENI はカンザス大学をプロジェクトリーダーに指定している。カンザス大学はプロジェクト全体と、GpENI インフラの管理と制御の運用責任を負う。研究プロジェクト責任者は、同大学の James PG Sterbenz 博士である。

カンザス大学の役割の一つは、GpENI を通じた米国パートナーや、欧州、アジアのパートナーと協力関係を築くためのアウトリーチ活動を推進することである。このアウトリーチ活動の例として、GpENI とレジュームネット間の連携を目指す、カンザス大学の Sterbenz 博士と、EU のレジュームネットを率いるランカスター大学教授の David Hutchinson 博士との共同研究が挙げられる。

資金源

米国及びEUの大学は、それぞれの国や域内の研究開発機関から資金提供を受けている。GpENIIに参加する米国の各大学は、それぞれのネットワーク参加を支援する助成金をNSFから受けており、レジュームネットに参加するEUの大学は、欧州委員会（European Commission: EC）の「将来のインターネット研究と実験（Future Internet Research and Experimentation: FIRE）」[176]から資金提供を受けている。FIREは、レジュームネットなどの将来のインターネット研究コンソーシアムを助成するECのイニシアチブである。

研究内容

GpENI とレジュームネットは、将来のインターネット・アーキテクチャ開発を通してネットワーク・レジリエンスの改善を目指す共同研究開発プロジェクト、レジリネット（ResiliNet）で協力関係にある。この共同研究開発プロジェクトを率いるのはランカスター大学である。カンザス大学は、前掲のレジュームネット・パートナーとともに、GpENI とレジュームネットの相互接続によってこのプロジェクトに参加している。

---

[176]「将来のインターネット研究と実験」、EC　http://cordis.europa.eu/fp7/ict/fire/

研究成果の評価方法と帰属

GpENI とレジュームネットが接続されたことで、次世代インターネットにおけるレジリエンスを改善するようなプロトコルに関する研究テストベットとなり、これを通じた研究成果を2011 年 6 月に研究論文として発表している。このような公的な研究成果の発表（つまり共同論文数など）は、前出のサウスカロライナ大学の Farkas 博士が指摘するように、「NSF からのファンドを受けたプロジェクトに関する評価基準には総じて、論文数が重視される傾向がある」というコメントからも、不可欠な基準と考えられる。成果の帰属については、具体的な方針は明確にされていない。

3.1.4. セキュアリング・オープン・ソフトフォン（Securing the Open Softphone）[177]

概要

セキュアリング・オープン・ソフトフォン（Securing the Open Softphone: SoS）は、ボストン大学（Boston University）が主導する研究コンソーシアムであり、ソフトフォン（スマートフォンなど）が直面するセキュリティ・リスクを特定し、理解、軽減するための国際的共同研究を実施する。コンソーシアムには、国際メンバーとしてドイツ・テレコム・ラボラトリーズ（Deutsche Telekom Laboratories）や英国のウォーウィック大学（University of Warwick）が参加している。

組織構造と参加機関

SoSを率いるのは、ボストン大学の教授で、同大学の信頼できる情報システムとサイバーセキュリティ・センタ（Center for Reliable Information Systems and Cyber Security: RISCS）[178]のMark Crovella氏である。本国際研究コンソーシアムに参加する米国研究機関として、ボストン大学がNSF補助金を獲得しており、同教授は、研究プロジェクト責任者（PI）である。SoSには、ボストン大学から研究者 9 名が参加している。

同センタの他のメンバーは、レイセオン BBN テクノロジーズ（Raytheon BBN Technologies）、ドイツ・テレコム・ラボラトリーズ、そしてウォーウィック大学が参画している。レイセオンはソフトウェア制御無線の専門知識を持ち、ドイツ・テレコム・ラボラトリーズはセキュリティ分野で豊富な経験を持つハンドセット・ベンダーであり通信事業者（キャリヤ）でもあることから参加を決めた。ウォーウィック大学は、システム・レベルのセキュリティ分析、デジタルフォレンジック、そしてマルウェア分野で専門知識を持つことから、このプロジェクトに参加している。

---

[177] セキュアリング・オープン・ソフトフォンの組織・活動概要 http://www.bu.edu/riscs/research/projects/softphone/

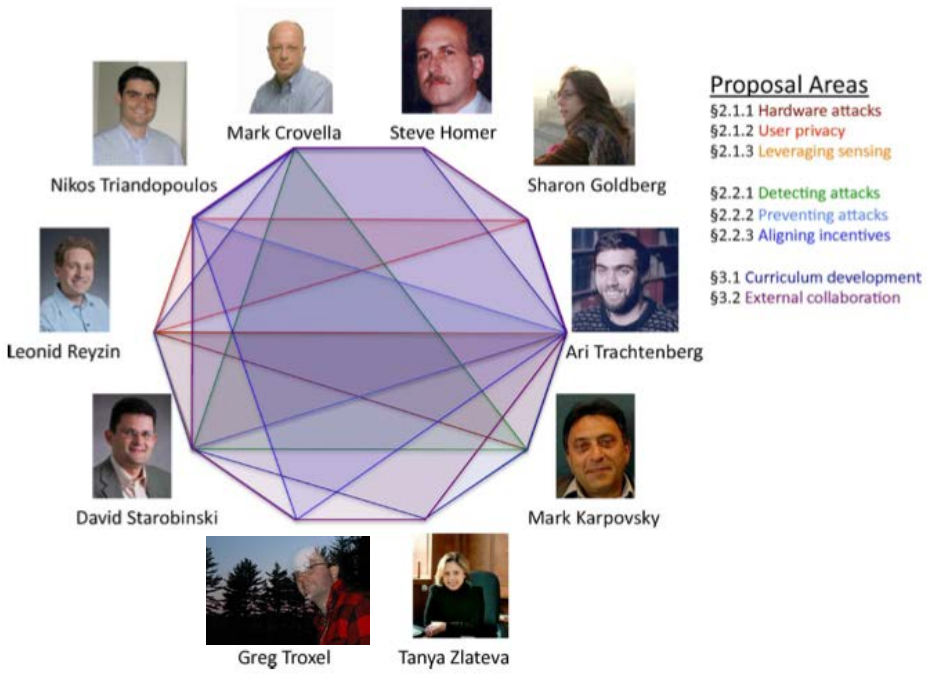
[178] ボストン大学 RISCS 概要説明 http://www.bu.edu/riscs/

役割分担

本プロジェクトでは、Crovella 教授が研究プロジェクト責任者及び統括管理者として中核的な役割を担い、研究プロジェクト共同責任者（co-PIs）として、同じくボストン大学の他 8 名のスタッフが支援する体制をとっている。具体的には、共同責任者（専門分野）は以下のとおり。

- Steve Homer 氏（攻撃阻止及びネットワーク信頼性向上に向けた経済学的アプローチ）
- Sharon Goldberg 氏（暗号技術及びユーザー・プライバシー）
- Leonid Reyzin 氏 （ハードウェアベース暗号技術）
- Nikos Triandopoulos 氏（データ認証）
- Mark Karpovsky 氏（セキュアシステムに関するハードウェア設計）
- David Starobinski 氏（ソフト制御無線及びソフトコード認証）
- Ari Trachtenberg 氏（センサーセキュリティ）
- Tanya Zlateva 氏（サイバーセキュリティ・カリキュラム開発及びアウトリーチ）

信頼できる情報システムとサイバーセキュリティ・センタ研究者



出典：RISCS[179]

これらの大学関係者に加えて、レイセオン BBN テクノロジーズ（Raytheon BBN Technologies）の Greg Troxel 氏が、ソフト制御無線分野で、ドイツ・テレコム・ラボラトリーズ Sachin Agarwal 氏がセキュリティ技術に関するプロトタイプ開発や実証実験に関して貢献している。

資金源

ボストン大学は、2010 年 7 月にNSFから 5 年間で総額 300 万ドルの補助金を得てSoSに参加している[180]。尚、他機関の研究資金源については、明らかにされていない。

研究内容

前述のように、SoS ではソフトフォンに対する脅威の特定と理解、軽減を目指している。具体的には、ユーザ及びシステム・レベルの両方で、これら脅威を研究する計画である。具体的なトピックとしては、以下が挙げられる。

- モバイル電話端末機及びネットワーク要素への攻撃
- ユーザプライバシー（ユーザの匿名性や通信のセキュア度）
- ユーザ及び機器認証
- 攻撃探知
- セキュアシステムや利用奨励に向けたインセンティブシステム

同プロジェクトで開発を目指す認証方法の一つに、2 台のソフトフォンを一緒に持って振り、互いに情報を共有させる方法がある。各電話に内蔵されたセンサがもう一方の電話の存在と振動を検知し、共有暗号鍵を自動的に生成する。この鍵を使って、情報漏洩の心配なく、2 台の電話間で情報の相互共有を可能にする。

この他、ユーザ認証に関する研究プロジェクトとしては、電話機に装着された三次元センサを活用して、ユーザの特徴（各ユーザに特化した電話機を持つ角度、歩行速度やそれに伴う振動、身振りなど）を察知することで、ユーザ認証を行うといった研究がある[181]。

研究成果の評価方法及び帰属

SoS プロジェクトの研究は現在も続いている。このプロジェクトの研究者は、SoS 研究に基づき、2 件の会議録を含む研究論文 4 件をこれまでに発表した。しかし、ボストン大学の国際パートナーとの共著論文などは、現在まで発表されておらず、今後の見込みにつ

---

[179] ボストン大学 RISCS 概要説明（研究員） http://www.bu.edu/riscs/
[180] スマートフォン・セキュリティ・イニシアチブへ NSF 資金提供、ボストン大学 http://www.bu.edu/phpbin/news-cms/news/?dept=666&id=56448
[181] ボストン大学 SoS 概要説明 http://nislab.bu.edu/nislab/SOS.html

いて現時点では不明である。

Crovella 博士は、SoS は極めて新しいプロジェクトであり、まだ何ら成果を上げていないとコメントしている。従って、国際共同研究がプロジェクトの成果に与える影響を現段階で評価するのは困難とも話しており、具体的な評価方法などについても言明を控えている。同教授によると、知的財産所有権にかかわる問題は全て、その知的財産権に対する参加機関の貢献に基づき、国際パートナーの判断で解決されるとのこと。

3.1.5. フィンランド／米国・ワイヤレス・イノベーション（Wireless Innovation Between Finland and the US）[182]

概要

フィンランド／米国・ワイヤレス・イノベーション（Wireless Innovation Between Finland and the US: WiFiUS）は、無線周波数帯のより効率的な利用について共同研究を実施する、フィンランドと米国の大学によるバーチャル国際研究コンソーシアムである。

組織構造と参加機関

WiFiUS は、フィンランドの 3 大学と米国 8 大学で構成される国際研究コンソーシアムである[183]。コンソーシアムのメンバーは互いに協力し、ワイヤレス・スペクトラム技術を前進させるという包括的目的をサポートする研究プロジェクトに取り組んでいる。

WiFiUS 自体は、ワイヤレス研究と教育を目的に、WiFiUS メンバー間の交流と協力を推進するサービスを提供するバーチャルなコンソーシアムである。これらのサービスは、フィンランド・オウル大学（University of Oulu）の Matti Latva-aho 教授及び米国レンセラー工科大学（Rensselaer Polytechnic Institute: RPI）の Alhussein Abouzeid 准教授の監督下にある。WiFiUS がそのメンバーに提供する活動支援とサービスの一部を以下に示す：

- 研究活動に関するコンテンツなどを提供するメンバー向けオンライン・ポータルへのアクセス
- 研究責任者同士の物理的及びオンライン会議の設定アレンジ
- 学生向けの物理的及びオンライン会議の設定アレンジ
- 年次サマースクール
- 大学院生交換プログラム

---

[182] ボストン大学 RISCS 概要説明 http://www.bu.edu/riscs/
[183] WiFiUS 活動概要 http://www.wifius.org/

役割分担
オウル大学の Latva-aho 教授と RPI の Abouzeid 教授は、WiFiUS が提供するメンバー向けサービスの指導的立場にある研究プロジェクト責任者である。WiFiUS メンバーが手掛ける個々の研究プロジェクトは、それぞれの研究プロジェクト責任者が主導して実施される。

資金源
フィンランドではフィンランド技術庁（Tekes）、米国ではNSFの「仮想研究所を横断する科学プログラム（Science Across Virtual Institutes: SAVI）」[184]が、WiFiUSのメンバー向けサービスへ資金を拠出している。SAVIでは、米国及び国際機関間で物理的及びバーチャルなやり取りを支援する国際バーチャル組織の創設を助成することにより、国際共同研究の促進を目指している。WiFiUSは、NSFからSAVIパイロット・プロジェクト 3 件のうちの一つに選ばれており、ICT 研究開発に関する唯一のSAVIパイロット・プロジェクトとなっている。

WiFiUS メンバーが行う個々の研究プロジェクトは、そのメンバー自体をサポートする資金源から別々に助成を受けている。米国メンバーによる WiFiUS プロジェクトへの参加は、NSF コンピュータ・情報科学エンジニアリング（Computer and Information Science Engineering: CISE）局からの補助金が付与されている。これらプロジェクトの指導的立場にある研究プロジェクト責任者は、他の NSF 助成研究の場合と同じ条件下で、NSF プログラムの補助金を公募等で獲得しなければならない。しかしながら、WiFiUS のように国際共同研究の一部として実施されるプロジェクト計画は、NSF の審査で優先される可能性がある。

研究内容
前述のように WiFiUS の包括的目標は、フィンランドと米国の大学間で、ワイヤレス研究と教育のための交流と共同研究を推進することである。具体的には以下の通りである:

- 広範なワイヤレス・ネットワーク領域の既存及び新しい国際研究と教育活動を推進し支援する。
- さまざまな関連国際プロジェクトの参加機関間で、ナレッジ共有と交流を実現する。
- 2 国における新らたな試験プラットフォーム、標準、そしてワイヤレス技術政策に関する専門知識の共有を可能にする。
- 2 国の学究界、産業界、そして政府機関間の交流を促進し支援する。
- WiFiUS では現在、6 つのワイヤレス研究開発プロジェクトが実施されている。NSF は 2011 年 8 月末と 9 月初めに、これらプロジェクトへ補助金を支給した。以下の表

[184] NSFSAVI 概要説明 http://www.nsf.gov/news/special_reports/savi/index.jsp

にプロジェクトの内容をまとめた。

WiFiUS プロジェクト

プロジェクト	参加機関	まとめ
認知能力収穫ネットワーク（Cognitive Capacity Harvesting Networks）	フロリダ大学（University of Florida）（米国） オウル大学（University of Oulu）（フィンランド） ミシシッピ州立大学（Mississippi State University）（米国）	コグニティブネットワークの実現可能アーキテクチャを実現するために、知的にネットワーク・リソースを収集し、関連技術を開発する。
高密度異種ワイヤレス・ネットワークのための分散リソース割当と干渉管理（Distributed Resource Allocation and Interference Management for Dense Heterogeneous Wireless Networks）	カリフォルニア大学デイビス校（University of California, Davis）（米国） アールト大学（Aalto University）（フィンランド）	リソース割当と干渉管理のための分散及び実効メカニズムを開発する。
協調アクセス・ネットワーク・プロビジョニングのための経済モデル（Economic Models for Collaborative Access Network Provisioning）	オウル大学（University of Oulu）（フィンランド） バージニア工科大学（Virginia Polytechnic Institute and State University）（米国）	通信事業者に独自ネットワークを展開あるいは協調させるためのインセンチブ、及び異種ネットワークのセキュリティ脅威を調べることにより、異種ネットワークにおける協調を研究する。
エネルギー効率に優れた認知ネットワーキング（Energy Efficient Cognitive Networking）	RPI（米国） オウル大学（フィンランド） メリーランド大学カレッジ・パーク校（米国）	認知ネットワークのエネルギー効率を最適化する方法論を開発する。
動的スペクトラム・アクセス・アルゴリズムの再構成可能アンテナ・ベース・エンハンスメント（Reconfigurable Antenna-based Enhancement of Dynamic Spectrum	ドレクセル大学（Drexel University）（米国） オウル大学（フィンランド）	再構成可能アンテナの機能を活用する、動的スペクトラム・アクセス・アルゴリズムの強化。

Access Algorithms）		
堅牢かつセキュアな認知無線ネットワーク（Robust and Secure Cognitive Radio Networks）	ノースウェスタン大学（Northwestern University）（米国） オウル大学（フィンランド） アールト大学（Aalto University）（フィンランド） メリーランド大学カレッジ・パーク校（米国）	認知ネットワークの一次及び二次ユーザの共存と、ホリスティック・フレームワーク内のネットワークのセキュリティとプライバシーに関する問題に対処する。

出典：WiFiUS の情報を基にワシントンコアで作成

研究成果の評価方法と帰属

上記のプロジェクトはいずれも論文をまだ発表しておらず、現時点で成果は公開されていない。評価方法については、、前出のサウスカロライナ大学の Farkas 博士が指摘するように、「NSF からの資金を受けたプロジェクトに関する評価基準には総じて、論文数が重視される傾向がある」というコメントからも、共同研究に基づく論文数などをひとつの基準にしていると考えられるが、詳細は不明である。成果の帰属については、具体的な情報は、得られなかった。

3.2. 米国における国際共同研究を対象とした研究開発ファンド

研究開発に従事している米国連邦政府機関は、国際協力の構築・維持に大きな関心を示している。公的機関として、国際研究開発に関与している機関では次に挙げる重要な成果をあげることが奨励されていること。このことは、例えば、NSFによる 5 ヵ年の戦略プランである「NSF 2011-2016 会計年度戦略計画（NSFStrategic Plan for fiscal years 2011-16）」[185]などにも、言及されている。

- 米国に対して、外国のパートナー組織に所在する特定の研究開発人材、施設、能力へのアクセスを与える。
- 科学の知識の共有、研究を通して経済的・社会的恩恵を共同で産出することにより国際協力及び理解を促進する。
- 外国（特に開発途上国）の科学的能力及び機関の開発を支持する。
- 米国の研究者、特に科学・工学分野の学生が、より世界的な視野を発展させ、個人のレベルで国際的な科学コミュニティに参加する価値を得ることができるような機会

[185] 「NSF 2011-2016 会計年度戦略計画」、NSF、2011 年 4 月
同戦略計画は、2011 年 4 月、NSF がイノベーションを通して国家を強化するための 5 ヵ年計画として発表したもので、NSF として目指すべき短・中長期の達成目標が掲げられている。
http://www.nsf.gov/news/strategicplan/nsfstrategicplan_2011_2016.pdf (p. 9)

を提供する。

米国の研究資金は税金により賄われているため国内の優先研究分野に出資されることが多いが、海外や国際的な研究機関と連携した研究開発の推進は米国にとっても利益をもたらしうることから、連邦政府機関は国際連携を支援している。科学機関はこれまでにも、国際協力研究開発に出資することが、米国国内にも恩恵をもたらすことを実証してきた。そのため、連邦機関が外国の研究者に対して直接的に出資する権限に関しての制限に直面したとしても、国際協力研究開発を容易にする目的で財政的なサポートをすることについては、より多くの自由が与えられている。具体的には、米国の研究者の海外渡航費や国際的なワークショップを開催する際の援助、さらに 多国籍間の研究活動を調整する事務経費などが含まれる。

本章で取り上げる 4 つのプログラムは、NSF と DOE という 2 つの非常に異なる科学部門組織に属している。その結果、以上 2 つの組織における国際協力研究開発 を支持するプログラムの性質も大幅に異なってくる。

NSF は米国、特に大学における全般的な基礎研究を促進するというミッションを有する。NSF が特定の研究分野（コンピュータと情報科学・工学、生物、化学、地学など）を中心とした部局で組織されるとしても、NSF が出資するプログラムの目的は、新知識の産出へ出資し、大学院生を将来の研究者としての役割を果たせるよう研修し、育成していくことによって、基礎科学において国家の潜在能力を構築することである。したがって、NSF の国際プログラムはさまざまな科学領域やプロジェクトにわたって利用され、異なった種類及び様々なパートナーとの国際協力研究を促進するといったより総称的な枠組みを提供している。

これに対して、DOE は、教育以外のミッションを有する mission-driven な機関である。というのはそのプログラムが、米国のエネルギー保障を増長するという特定の成果を生み出すことを意図しているからである。副次的な使命は、第 2 次世界大戦後の時代から引き継がれたものであるが、DOE が国家の核兵器の備蓄に関して安全と保障を確実にすることである。この両方の使命を支持することにおいて、コンピューティング技術は重要な役目を果たす。コンピューティング技術はエネルギー経済をモデリングすること、兵器の安定性を認識するための核反応のシミュレーション、基礎エネルギー研究の科学データの分析を可能にする。数値計算の専門技術、インフラ及び能力において確実に最新のものへアクセスができるためには、DOE が世界中のトップコンピューティング機関と国際的なパートナーシップを組むことが必要となる。こういったプログラムはさらに特別に、エネルギーと国家の安全保障における DOE の活動に対するリソースへのアクセスを提供するよう考案されている。

本章において、ICT における国際協力研究開発の様々な活動に対して広範囲な支援を行なっている 4 つのプログラムの概要を紹介する。

- NSF が実施する PIRE
- NSF が実施する SAVI
- DOE が実施するエクサスケール技術と計算研究所（Exascale Technology and Computing Institute: ETCi）
- DOE が実施する計算科学国際センタ（International Center of Computational Science: ICCS）

3.2.1. NSFが実施するPIRE [186]

NSF の国際活動における再編成に伴い、NSF は 2005 年、新規の国際共同予算プログラムを立ち上げた。そのプログラムが国際共同研究教育パートナーシッププログラムまたは PIRE と呼ばれるものである。PIRE に先行して NSF は 2 つの主要な国際プログラムに取り組んでいた。

- 「人材投資プログラム」（People investment programs）は、学部生、大学院生、ポスドクの研究者に国際的に研究する機会を与えることに専念したプログラムであった。このプログラムに含まれるものとして、国際研究経験（International Research Experiences for Students）、汎アメリカン高度研究インスティテュート（Pan-American Advances Studies Institute）、及びサマー研究インスティテュート（Graduate Summer Studies Institute）が挙げられる。
- 「研究投資プログラム」（Research investment programs）とは国際研究活動を促進するプログラムである。主な内容は、国際プランニング・ワークショップへの出資や共同研究の実施などに関する議論を実施するために掛かった渡航費の援助が含まれる。共同出資される助成金については、該当する出資プロジェクトに海外からの参加者が含まれる場合、NSF の国際事務局が交付される助成金について補助金を提供することもあった。ただし、その補助金は旅費やロジスティックに関するサポートに実質限られていた。

PIRE は、プログラムが長期で組織レベルでの共同研究を援助するよう構成されているという点で先行する国際プログラムと異なっている。また、PIRE は、米国の研究機関と海外の研究機関が、ある特別の研究プロジェクトや予算の期間のみならずそれを超えた関係を築くことを試みている。そのため、PIRE を通して出資を受ける活動の範囲は先行する NSF の国際プログラムより広範囲で、利用できる予算額も高くなっている。

---

[186] NSF PIRE の概要説明 http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=12819

目的

正式なプログラム仕様書[187]によれば、PIREには 4 つの主要な目的がある。

1. 国際協力を通して、科学、工学研究及び教育の卓越性を支援する。
2. 国際協力が領域、規模、柔軟性、施設といったユニークな利点をもたらす機会を促進し、国際協力なしでは起こりえない発展を可能とする
3. 強力な国際パートナーシップが築けるよう、組織内また組織を横断したリソース、研究のインフラに従事し、共有する。
4. 学生及び若手の研究者が実質的な国際研究を体験できるような機会を作り出し促進する。

また下図に示す NSF 関係者による対外資料によると、プログラムの目的として、①パートナーシップの構築促進（上記 2. 該当）、②研究の卓越性（上記の 1. 該当）、③国際研究を通じた学生の育成（上記の 4.該当）、④組織・グループを超えた横断体制の促進（上記 3. に該当）などとも表現されている。

PIRE プログラムの目的

[187] 正式なプログラム仕様書： http://www.nsf.gov/pubs/2011/nsf11564/nsf11564.pdf

実際、PIRE はパートナー間のネットワークを支援することを目的としており、多国間の連携プログラムに対して出資することを重点としている。PIRE のもう一つの主要な特徴は「研究の卓越性」(research excellence)に献身していることである。PIRE の公募に関しては、プロジェクトに国際的な研究パートナーが参加していること、及びプロジェクトにおける国際的連携の付加価値を証明することを応募要件としている。

PIRE はまた研究と教育を統合することを試みる。したがって提案された PIRE プロジェクトには研究項目の中で学生の担う役割が明確でなくてはならず、教育の機会を示すものでなくてはならない。例えば、PIRE プロジェクトではコースブックや指導用の実験といった新規のカリキュラム資料、つまりそれによって別の機関が将来学生を教育できるような資料を作成することが求められる。同時に、提案には学生が研究上の責務に就くこと、特に海外のパートナー組織において研究をする機会が与えられることが示される必要がある。

PIRE では、国際連携を通して米国の研究機関が、研究の規模や視野、さらには、目標がグローバルなものになるように支援することに主眼を置いている。そういった意味でも、PIRE から資金を受ける組織は、海外のパートナーから学ぶ方法、及びどのように自ら実施する研究を変化させて学んだ内容を応用するのかについて、具体的な戦略プランなどを示すことが必要である。従って、前出の OSDC に関する項で紹介したフロリダ国際大学やイリノイ大学は、この点について言及した戦略プランを NSF に対して提示していたと推定される。

対象

PIREプロジェクトはどんな研究トピックにも取り組むことができ、独自で対象となる目標を定めることができる。しかし PIRE に関する提案書では以下のような点が考慮される。

- 意欲に満ちている: 計画された研究は個人が NSF 出資のプロジェクトで通常実施可能であることを超えた目標を掲げなくてはならない。またその成果により人間の知識と能力に大きな進歩が生み出されることを主張しなくてはならない。
- 研究と教育の統合: 計画された研究は研究題目に教育的な成果が含まれることを明示しなくてはならない。特に、出資される研究領域において学習に対する文化間の学際的な壁を越えることが求められる。
- 学際的である: 研究では異なる領域の異なる科学者による複数の視点を統合する必要がある。個々の海外パートナー組織が他のパートナーからは寄与されない独自の分野 1 つ以上を代表する研究者を提供できることが望ましい。

規模

PIRE が立ち上がった当初は年間 50 万ドルまでというファンドの上限と、5 年間までという時間の枠組みもあった。3 期目になる 2009 年度の交付では、ファンド額の上限が明記

されなかった。しかしながら、連邦政府における全般的な予算の緊縮傾向や、PIRE 自身が直面している予算面での限界と大規模なプロジェクトの管理の実現性も影響し、PIRE 出資金は 100 万ドルから 300 万ドルを最高額とし、5 年間に渡る交付が一般的である。また、PIRE の目標は複数の機関とネットワークを構築することとされているが、プロジェクトの大部分は通常、3~5 件の米国組織と 3 カ国以上の海外組織で成り立っている。

活用条件

NSF による補助金に関する法律上の制限により、PIRE プログラムそのものは PIRE への米国の参加者の活動のみに対して出資される。しかし PIRE プログラムでは、レバレッジ・ファンディングという制度を活用することで、他の連邦政府機関によるファンドや補助金と組み合わせ、活用することで、海外の研究者の支援を助成することなども行っている。例えば、PIREプロジェクトはNSFファンドと米国国際開発庁、環境省国際事務局、及び慈善財団基金や科学協会などの非政府組織に関する米国の組織からの資金を統合することで、他省庁などの補助金を海外への補助に充てるなどして、対応しているケースがある。また、海外の参加者は自国の政府や類似した資金のスポンサーからも援助を得ることが奨励されている。

プログラム資金のファンド選定先に関して、重要な選定項目となるのは、PIRE 申請者が国際協力をどのように運営する計画を明確に示しているかという点にある。PIRE 申請者は共同研究のための運営構成を提示しなければならない。また、異なった研究パートナーの役割も定義し、研究目標に向かっての発展を達成すること、研究の質と成果が評価されることを保障する体制があることを明確にしなければならない。この要件の目的は、参加者に将来の国際協力でも再現できる実務上のプロセスとインフラを作り出させることにある。

利用事例

PIRE プログラムは 3 期に渡って実施されており、2005 年に 12 プロジェクト, 2007 年には 20 プロジェクト、2009 年には 15 プロジェクトがそれぞれファンド交付されている。次の期間の予算に対する提案は 2012 年 5 月が締め切りであり、2013 年の 10 月 1 日までには交付先の発表が行われる予定である（従来、NSF によるファンド交付先発表は米国政府の年度末である 9 月 30 日までには行われている）。

PIRE の交付は NSF が出資する社会科学、数学、物理学、化学、生物学、地学、工学、天文学、極地プログラム及び ICT を含む、すべての科学分野を対象としている。ICT に関連した交付として、オープン・サイエンス・データ・クラウド（Open Science Data Cloud）が上述の 3.1 項で触れられている。PIRE 実施による他の ICT 関連プロジェクトは以下の通りである:

活用事例

交付年	2005 年
プロジェクトタイトル	機械翻訳システムのための言語理解における意味の提示に関する調査（Investigation of Meaning Representations in Language Understanding for Machine Translation Systems）
米国側参加者	ジョンズ・ホプキンス大学（主幹機関） ブラウン大学
海外参加者	チャールズ大学（チェコ共和国） ザールラント大学（ドイツ）
期間	2005 ～2012 年
予算	250 万ドル
プロジェクトの概要	ジョンズ・ホプキンス大学の Frederick Jelinek 氏に先導される本チームはスピーチの認知・再構及び機械翻訳システムにおいて用いられる言語学的意味の正式な提示を調査している。様々な正式のモデルを応用することにより現行のスピーチの認知システムを増長し、システムの生み出す翻訳を一貫性があり文法的に正しいアウトプットとすることが目標である。本プロジェクトの実施期間中、米国の大学院生が海外に派遣され、ヨーロッパで開発された自然言語のプロセシングのための言語フォーマリズムにより研修を受けさせる。学生はチェコ語またはドイツ語で言語研修を受講する。学生の博士課程プログラムの最終段階で、学生はチェコ共和国またはドイツに戻り、ヨーロッパ人の指導教授とともに上述の最新言語プロセシング技術に組み込まれるような研究に取り組む。プロジェクトの結果はピアレビューや専門の学術雑誌に掲載される 69 以上の技術論文に記録される。

交付年	2007 年
プロジェクトタイトル	サイバーインフラ・アプリケーションの使用可能化のためのグローバルリビングラボ（A Global Living Laboratory for Cyberinfrastructure Application Enablement）
米国側参加者	フロリダ国際大学 フロリダ・アトランティック大学 IBM
海外参加者	モンテレイ工科大学（メキシコ） 清華大学（中国）

	ラ・プラタ国立大学（アルゼンチン） バルセロナ・スーパーコンピューティング・センタ（スペイン） カタルーニャ工科大学（スペイン）
期間	2007～2014 年
予算	228 万ドル
プロジェクトの概要	本プロジェクトは、より精巧なサイバーインフラ（Cyber Infrastructure: CI）システム（グリッドそのものからというよりLAGridで作動できるソフトウェアの開発を中心としたものである）を構築するため既存のラテンアメリカグリッド（LAGrid）分散コンピューティング・インフラを拡大したものである。このアプローチはアプリケーション主体で、（1）慎重に選択された決定的アプリケーション領域の CI 使用可能化を支持、例えばハリケーン緩和策、バイオインフォーマティックス、ヘルスケアなど（2）該当領域における CI 使用可能化アプリケーションのための共通の方法論、サービス、ツールの開発を中心としている。学生たちはどのようにグリッドシステムを用い、プロジェクトとして自らのアプリケーションを作成するかについて研修を受ける。現在までにプロジェクトは、グリッドシステム、データ圧縮、ワークフロー管理、モバイル統合、天気予報及びデータの視覚化に関するウェブサービス開発における実験を含む。

交付年	2007 年
プロジェクトタイトル	ヒューマノイド- 先進的な性能へユニバーサルアクセスインフラ（Universally Accessible Infrastructures to Advance Capabilities）
米国側参加者	ドレクセル大学 ブリン・マー・女子大学 ヴァージニア工科大学 ペンシルバニア大学 スワースモア大学
海外参加者	韓国科学技術院（韓国） ソウル大学校（韓国） 高麗大學校（韓国）
期間	2007 ～2012 年
予算	250 万ドル
プロジェクトの概要	本プロジェクトは韓国科学技術院の HUBO ヒューマノイドロボットに基づく 3 階層のツールの開発である。3 階層とは、

	(1) ヴァーチャル-HUBO（ブリン・マウル・カレッジ先導） AI や ICT コンセプトをテストするのに自由でオープンなエミュレータである、 (2) ミニ-HUBO（ヴァージニア工科大学が先導）はアルゴリズムを実践するフルサイズのヒューマノイドの低コスト 20 インチ版である、 (3) オンライン-HUBO（ドレクセル大学先導）はフルサイズヒューマノイドの接続（tethered）版であり、研究者がインターネットを介してアクセスできるものである。本プロジェクトでは米国の学生が韓国科学技術院に派遣され、6 ヶ月間研究プロジェクトに関わる。また韓国と米国間のほかの交換研修も支援する。HUBO を使い、科学の教育のためにフィラデルフィアの Please Touch Museum で教育、発表を目的としたロボットの展示の開発も含む。

3.2.2. NSF－SAVI [188]

PIRE とは対照的に、SAVI プログラムは、各 NSF 部局がファンドを拠出し、国際科学・エンジニアリング室が調整役となって運営されている。SAVI は単独調査プログラムを意図するものではなく、SAVI は計画立案の研究集会、共同セミナー、研究員の交換、及び留学生研究体験を含む、低コストながら国際協力に重要な活動に対して、ファンドを提供するものである。

SAVI を活用することで、特定の研究課題に従事している米国の大学グループは、同じ課題について活動している海外の類似した大学グループと接点を持つことができる。その後、米国の大学は、特定の国際共同研究活動に関与するために、適切な部局に対して SAVI 補助金の申請を行うことができる:

- 個々の独立した国内チームよりも優れた学習効果をもたらす、科学、工学、及び STEM を向上させる共同研究活動;
- 相乗作用を促進する SAVI チームメンバーの共同会議;
- ワークショップ、高等研究所、及びシンポジウム;
- 共同セミナーシリーズ、大学レベルのコース;
- 大学院生及びポスドク研究生の共同指導;
- 新任職員向け長期研究交換訪問;及び
- アメリカの大学生向け海外夏季研究体験に焦点を当てたプログラム。

[188] NSF SAVI の概要説明　http://www.nsf.gov/news/special_reports/savi/index.jsp

これらの活動は直接的、又は電子通信（ビデオ会議を含む）を使用して遠隔的に実施される。

SAVI の仕組みは、2011 年 10 月に Subra Suresh 博士によって発表された。3 種類の指定された試験プロジェクトがあり、それらは、他の申請者に対する模範例として資金提供が行われたものである。例えば、本報告書中でも前セクションで取り上げた WiFiUS プロジェクトは、この制度を活用している。その他、2 種類の試験的プロジェクトは以下に説明される。

目的
NSF は SAVI 向けに以下のような目標を掲げている:

- NSF によって支援されている全分野の最先端に従事する STEM の研究者/教育者が行う共同研究を支援する;
- 一貫性ある研究チームを形成し、仮想研究所を実現するために、相補的強み及び共通の関心をち、NSF に資金提供を受けている研究者間の繋がりを刺激する;
- NSF に資金提供を受けている研究センター/研究所（仮想及び実在両方）及びそれらに対応する国際組織間の STEM 研究と教育上の連携関係を促進する;
- 長期的国際協力を導く海外研究体験の機会を学生、ポスドク研究生、新任職員に提供する;及び
- 基礎研究及び人材開発への互いの投資を活用することで、NSF とこれに対応する、STEM 研究に資金提供を行う世界各地の組織間との関係を強める。

SAVI は、将来の研究協力を援助する迅速かつ基本的な課題支援に向け、低コスト及び効率的な管理体制を意図している。

対象
SAVI は特定の研究テーマ又は分野に限られるものではない。申請者は、SAVI 提案書をまとめ、単独提案又は、他の NSF による研究補助金プロジェクトの補足として組み合わせて、提出することもできる。他の補助金プロジェクトと組み合わせる場合、SAVI 提案がこの補助金プロジェクトの研究テーマやトピックに合致したものである必要がある。

規模
SAVI 提案書に対する実際の資金提供レベルは、提案されるテーマ及び活動によって異なる。これらの活動は、他の共同研究プロジェクトの補足及び支援を意図している。NSF は最長 5 年間の SAVI 提案の要求資金額として、年間 5 万ドルから 40 万ドルをひとつの基準枠としている。

活用条件

- SAVI 提案書は NSF 内各部局又は、国際科学エンジニアリング室以外のプログラム事務局の既存プログラムの募集に応募しなければならない;
- SAVI 提案書は、上記に掲載されたSAVI 支援向けに認証された活動のみを含めなくてはならない;及び
- SAVI 提案書には、なぜ国際的パートナーが提案書に含まれているかの論拠を記述しなければならない。

活用事例

交付年	2011 年
プロジェクトタイトル	数学及び統計科学のための仮想研究所（Virtual Institute of Microbial Stress and Survival: VI-MSS）
米国側参加者	ブラウン大学付属数学における計算及び実験的リサーチ研究所（Institute for Computational and Experimental Research in Mathematics: ICERM）、デューク大学付属統計及び応用数理科学研究所（Stastical and Applied Mathamtical Science Institute: SAMSI）
海外参加者	チェンナイ数学研究所（インド） インド理科大学（IISc）（インド） 数理科学研究所（インド） インド統計大学（インド） タタ基礎リサーチ研究所（インド）
期間	未確定
予算	指定なし
プロジェクトの概要	仮想研究所は、指定されたパートナー研究所からアメリカの 2 箇所の研究所に長期訪問するインド人研究者に資金供給を行う。インド人研究者はインド科学技術省科学技術局の援助を通して、それぞれの研究所に対して資金の申請をする。承認された場合は、VI-MSSのウェブサイト（http://icerm.brown.edu/vi-mss-participation）より、訪問の手配を申請できる。VI-MSSの援助資金は、インド人研究者を迎えるためにアメリカの主催者側研究所で発生する費用と時間を支援する。

交付年	2011 年
プロジェクトタイトル	生体物理学学生研究ネットワーク（Physics of Living Systems Student Research Network: PoLS SRN）
米国側参加者	カリフォルニア大学サンディエゴ校

	イリノイ大学アーバナ・シャンペーン校 プリンストン大学 イエール大学 メリーランド大学 ライス大学 ハーバード大学 コロラド大学 コロラド州立大学 シカゴ大学
海外参加者	リオネジャネイロ連邦大学（ブラジル） サンパウロ大学（ブラジル） ロンドン大学ユニバーシティー・カレッジ（英国） ケンブリッジ大学（英国） 構造生化学センター－CNRS（フランス） 神経科学学際研究所－ボルドー大学（フランス） フレネル研究所（フランス） マルセイユ・ルミニー免疫研究所（フランス） マルセイユ・ルミニー発生生物学研究所（フランス） パリ市立工業物理化学大学院大学（フランス） キュリー研究所（フランス） パリ高等師範学校（フランス） ミュンヘン大学（ドイツ） マックス・プランク生化学研究所（ドイツ） マックス・プランク生物物理学研究所（ドイツ） ゲッティンゲン大学（ドイツ） ミュンヘン工科大学（ドイツ） テルアビブ大学（イスラエル） シンガポール国立大学（シンガポール） 国立生命科学研究センター（インド）
期間	2010 年～2015 年
予算	特定なし
プロジェクトの概要	既存の生体物理学大学院生研究ネットワーク、すなわち数学・物理科学部局を通して資金供給され、生体物理学を研究している全ての大学院生及びその教育者を支援する、組織横断型かつコミュニティベースのネットワークをサポートするものである。共同研究課題の作成、及び訪問インターンシップの手配することで、会員組織の学生を支援する。SAVI の資金供給はアメリカの会員組織が学生研究者

	を迎え、国際共同ワークショップを主催することを可能にする。

3.2.3. DOE アルゴンヌ国立研究所（Argonne National Laboratory） - ETCi

ペタスケールからエクサスケールへのハイパフォーマンス・コンピューティングの進化は、コンピュータ設計及びアーキテクチャの根本的変更が必要とされる。DOE高度科学コンピューティング諮問委員会（Advanced Scientific Computing Advisory Committee）による2010 年の報告書は、エクサスケール・コンピューティング・システム開発には、コンピュータ・ハードウェア、消費電力、入力/出力プロセス、及び他のコンピューティングに関する側面について、同期的かつ大きな打開策が多数必要であると指摘した[189]。必要とされる打開策の規模及び範囲は、特定の組織又は国の能力を超えている。そのため、DOEはエクサスケール・コンピューティング研究開発にはある種の国際的共同作業が必要という結論を下した。

ソフトウェア開発に焦点を合わせるハイパフォーマンス・コンピューティング研究共同体は、特に、将来のエクサスケール・システムに向けた新たなアーキテクチャの開発に関心を寄せた。多くの研究者はDOE及びNSFに対し、国際エクサスケール・ソフトウェア・プロジェクト（International Exascale Software Project: IESP）[190]のために少なくとも何かの支援を提供するよう説得した。IESPはアメリカ、ヨーロッパ、日本、及びその他の地域からコンピュータ研究者を招集し、国際的なハイパフォーマンス・ソフトウエア・コミュニティを特定の研究課題開発に向けて導く技術ロードマップを作成し、エクサスケール・コンピューティングに必要な革新を促進する研究の広範囲に及ぶ調整を可能にするための会議を主催した。

IESP のリーダーの一人に、DOE アルゴンヌ国立研究所の Peter Beckman 博士がいる。当時 Beckman 博士は、研究者及びエネルギー省が使用するスーパーコンピュータの管理をするアルゴンヌ・リーダーシップ・コンピューティング施設のディレクターであった。IESP によってロードマップの原案が作成された後、Beckman 博士は他の研究者と共に、その原案を実施する研究所の開発を手がけた。ETCi は、そのような研究所の一つである。

目的

現在、ETCiはまだ形成段階である。研究所はシカゴ大学の関連組織により運営されているDOEアルゴンヌ国立研究所に置かれている。ETCiの役割は、エクサスケール・コン

[189] 「エクサスケールコンピューティングの機会と課題」、DOE 、2011 年 http://science.energy.gov/~/media/ascr/ascac/pdf/reports/Exascale_subcommittee_report.pdf

[190] IESP 概要説明 http://www.exascale.org/iesp/Main_Page

ピューティングの開発向上に必要とされる多様なパートナーシップの中心的存在となることである。DOEの高度科学コンピューティング・プログラムは、2012 年のエクサスケール・システム開発向けに 1 億 2,600 万ドルの研究予算を取得したが、その予算用途[191]に関する戦略を連邦議会に提出しなければならない。ETCiはその戦略において、他のDOEの研究所と共に作業を進めている。ETCiはエクサスケール・ソフトウェア・センタ（Exascale Software Center: ESC）を開発している研究所及び大学のコンソーシアムにおいて、アルゴンヌを代表する組織となっている。ESCはIESPのロードマップを元に開発された活動で、エクサスケールのソフトウェア開発及びツールに関する国際的研究の取組みにおいて、実質的な調整を実施する[192]。

対象

ETCi は正式な使命を公表していないが、Peter Beckman 博士は、優先事項の詳細についてのプレゼンテーションをこれまでに実施している。研究所は、超低電力系統、3-D チップ構成、超並列プログラミングモデル、シリコン・フォトニクス、及びハイブリット・マルチコア・アーキテクチャの設計上の開発努力を率先する見込みである。特定の対象は設定されていない。

規模

ETCi の予算は未公開である。研究所は、エネルギー省における全てのエクサスケール・コンピューティング・プロジェクトのために充当されている 1 億 2,600 万ドルの研究資金運用を管理しているが、この資金の一部が ETCi に充当されている。

活用条件

ETCiは研究スポンサーではない。しかしながら、6 つのエネルギー省内の研究所と共に、エクサスケール・システム開発へのアプローチについてインプットを収集するため、計算システムの業者に配布する情報依頼書を開発した[193]。この取組みにおいて管理する資金の正確な金額については、今後決定されるが、具体的な時期については不明である。

利用事例

ETCi はエクサスケール・ソフトウェア・センタを創設のため、他の組織と共同作業を実施している。ESC は、エクサスケール・コンピューティングの代替的アプローチを開発するため、多数の業者及び研究パートナーと共に作業を進める計画をしている。

---

[191] DOE のエクサスケールコンピューティング開発予算に関する説明
http://www.fiercegovernmentit.com/story/congress-funds-exascale-computer/2011-12-20

[192] Peter Beckman 氏による講義「エクサスケール・ソフトウェア・センターの構築（Building the Exascale Software Center）」については、http://www.exascale.org/mediawiki/images/1/1d/Talk02-beckman.pdf 参照。

[193] 「国際的活動に関する報告書」、欧州エクサスケールソフトウェアイニシアチブ（p. 34）
http://www.exascale.org/mediawiki/images/b/bb/EESI-D2_3-report-on-international-activities-16112011.pdf、

当初の計画として、センターは 2015 年までに初期の実証試験システムを構築し、2018 年までに全機能完備のシステムを設置する予定である。

3.2.4. DOE ローレンス・バークレー国立研究所（Lawrence Berkeley National Laboratory: LBNL） - ICCS[194]

2009 年末に、LBNL の Hemant Shukla 氏と John Shalf 氏及びハイデルベルグ大学の Rainer Spurzem 氏は、新進技術を駆使し、物理学と天文学データの問題に取り組むインフラ開発の継続的努力の一部として、3 日間に亘る国際ワークショップを計画した。そのワークショップは、データ集約的科学研究を支援するアプリケーション開発における、国際的取組みの調整を助けるセンタの必要性を提示した。ワークショップにおける討議は、2010 年 6 月、LBNL の ICCS の設立に繋がった。

目的

ICCS の主要目的は、国際協力の架け橋となり、計算科学研究手段の開発に努めることにある。ICCS の当初のメンバーは、カリフォルニア大学バークレー校、LBNL、ドイツのハイデルベルグ大学、及び中国科学院国家天文台である。ICCS は、物理学、天文物理学、気候モデル、地球科学、医療画像、その他の分野の中で行われる科学実験及びシミュレーションによって生成されるエクサスケールのデータセットの管理及び分析用の計算対策を作成することに努力している。センタは科学者が使い易く、エネルギー効率に優れ、比較的簡単に計算プラットフォームに実施できる開発手段を目標にしている。センタは教育及びアウトリーチにも取り組んでおり、手段やテクニックの使用面で科学者を訓練する計画もしている。

対象及び利用事例

現在、ICCS は同時進行している 3 つの研究の管理を支援している:

- 「天文物理学アプリケーション計算のインフラ（Infrastructure for Astrophysics Applications Computing: ISAAC）」[195]はNSFが資金援助している 3 年（2010~2013 年）計画のプロジェクトで、マルチコア・アーキテクチャを用いた物理学及び天文学研究のアプリケーションを促進する研究開発に焦点を合わせている。プロジェクトの目標は、計算集約型科学問題のために並列アーキテクチャの力を上手に利用すると共に、新発見に続く扉を開け、科学の成長を改革することである。このプロジェクトの目的は、ハードウェア・モジュール、ソフトウェア・ライブラリ、及び研究者の分析手段として組み立てられる計算要素を供給することにある。
- ハイデルベルグ大学を本拠とする GRACE プロジェクトは、特に、自重を含む天文物

[194] LBNL の ICCS 概要説明 http://iccs.lbl.gov/
[195] ICCS の ISAAC 概要説明 http://iccs.lbl.gov/research/isaac/employment.html

理学の液体流動のシミュレーション用に設計されたスーパーコンピュータ・プラットフォームの新タイプである。この新規コンピュータのアーキテクチャはハイブリッドとも言え、mpRACE 基板（マンハイム大学で開発された）を元にした再構成可能なハードウェア（現場でプログラム可能なゲートアレイ又は Field Programmable gate array: FPGA）を兼ね備えた、特別な目的を持つ計算基板（東京大学にて開発された）である。このプロジェクトは、星の形成及び高密度な恒星系の力学と乱気流を含む天文物理学的現象を研究するために特別に作られる手法を考案する。

- 中国科学院率いるシルクロードプロジェクトは、計算天文物理学、コンピュータ工学、及び超並列プログラミング技術を総合している。一般向け計算用に 170 NVIDIA Tesla GPU を用いるハイパフォーマンス・スーパーコンピュータは、中国科学院コカ天文台（National Astronomical Observatory of China: NAOC）にて構築されている。このプロジェクトは、ブラックホールの発達、銀河及び惑星系の形成を含む質問、及び大規模データ分析作業中のエネルギー消費の削減などの技術的問題を指摘する。シルクロードプロジェクトは GRACE プロジェクトの姉妹プロジェクトである。

規模

ICCS の年間予算は未公開である。ICCS は当会員組織から派遣される非常勤職員を採用している。

活用条件

ICCS は厳密には、資金供給機関ではない。その代わり、ISAAC 及び GRACE などからの資金を使って、カリフォルニア大学バークレー校、LBNL、ドイツのハイデルベルグ大学、及び中国科学院国家天文台などの機関間の共同研究プロジェクトの管理や調整活動に従事している。ICCS の主な運営構造は、計算科学研究上の類似問題について活動する研究チームを集結し、アイデア交換の促進及び関連する研究問題に対する共通解決策の開発につなげることである。

3.3. 連邦政府研究開発機関による研究開発の成果展開活動事例

3.3.1. NIST における研究開発成果の評価及びその技術移転に関する取組み

NIST は、2012 年度予算が 7.5 億ドルを僅かに超える程度の機関で、NSF、DOD、NIH、DOE、DARPA などと比較すると比較的小規模な科学機関であるが、計測／計量学、標準化及び工業技術分野の研究に焦点を絞った組織である。NIST は、その理念において科学を公的ニーズ（国防、公衆衛生等）ではなく、産業ニーズの直接支援に利用することを明確に掲げている数少ない研究機関の一つであることから、特殊なミッションをもつ政府機関といえる。

予算については、約 70%を内部研究（メリーランド州ゲイサーズバーグ市及びコロラド州ボルダー市のNIST研究者が行う研究）に、約 6%を標準化に関する調整及び普及活動、17%を製造業拡張プログラム（Manufacturing Extension Program）に充てている。同プログラムは、中小製造業者への相談サービスを提供する、地域の技術補助センタに資金を提供するものである。残り 7%は研究所の建設及び補修に充てられている。また、NISTは最近外部プログラムであるマルコム・ボルドリッジ・パフォーマンス・エクセレンス・プログラム（Malcolm Baldrige Performance Excellence Program）[196]及び技術革新プログラム（Technology Innovation Program）[197]に対するNISTとしての資金拠出を継続しないことを決定している[198]。両プログラムについては今後民間資金によって運営されることになる。NISTが両プログラムへの出資を停止した理由は明確にされていないが、よりNISTとして優先度の高い他のプログラムへの出資拡大のためと思われる。

産業界への直接支援は、技術移転活動及び標準化開発普及という 2 つの主なメカニズムを通じて行われる。どちらも NIST 自体の研究活動に対しても便益をもたらすものであるように設計されたものである。

① ＜評価について＞

NIST は小規模な機関として、そのパフォーマンスに対するマイナス批判が大幅な予算削減になる可能性をよく認識している。したがって、NIST は成果についての自己評価・分析に関する非常に優れたプログラム開発に投資してきた。例えば、NIST は恒久的な経済分析室を持つ数少ない政府機関の一つであり、同機関の活動が経済成長及び繁栄に貢献する程度を調査している。NIST は現在、政府研究活動の影響評価法について、連邦政府全体に知的リーダーシップを提供している。

プログラム評価格付けツール
（Program Assessment and Rating Tool: PART）[199]

PART は、George W. Bush 前大統領第一次政権期中に、OMB が開発した評価ツールである。PART は、政府機関のパフォーマンスを改善するための大統領管理指針の一構成要素であった。OMB は各機関がその理念、戦略、活動及びパフォーマンス成果について質問に答えるよう義務づける PART のテンプレートを作成した。PART プロセスは、機関のパフォーマンスの推移と異なる機関のパフォーマンスを比較する標準手法を提供するために作られたものである。

---

[196] マルコム・ボルドリッジ・パフォーマンス・エクセレンス・プログラム概要紹介 http://www.nist.gov/baldrige/
[197] 技術革新プログラム概要紹介 http://www.nist.gov/tip/
[198] 連邦政府による支援プログラムの廃止、Federal Times
http://www.federaltimes.com/article/20120125/AGENCY01/201250303/
[199] PART ガイダンス書、ホワイトハウス、2007 年 1 月 29 日
http://www.whitehouse.gov/sites/default/files/omb/part/fy2007/2007_guidance_final.pdf

NISTの研究プログラムは、2003 年にPARTプロセスによる評価を受けている。同評価では、NISTプログラムは非常に高い点数を記録している。NISTは、プログラム目標と設計及び戦略計画において適合性 100%、ベストプラクティスと評価されている。プログラム管理については、研究所が 86%、プログラム成果と責任能力については 75%となっている[200]。

政府機関は幅広い目的をもち、多くの異なる作業を行うため、標準パフォーマンス評価には意味がないとオブザーバーが指摘したことから、PART プロセスはその後やや疑問視されている。PART プロセスはオバマ大統領が就任した際に廃止され、現在は使われていない。廃止の理由については特に明確にされていないが、連邦政府機関において研究開発プログラムに関する評価活動に、関与してきたある政府関係者によると、同制度が全面的に否定されたわけではないという。この関係者によると、同ツールが導入されるまでは、各省庁全般を評価する制度しかなかったことからも、各省庁内の研究開発プログラムも含め、省内プログラムに関する連邦政府共通の評価ツールとしての、PART の存在意義は、大きかったとしている。特に、研究開発プログラムなどには通常、あまり関わりのない政府関係者にとって、研究開発プログラムの効果を推し量るツールとしては、このようなツールは重要であり、政府関係者が今後、研究開発プログラム評価ツールを考えていく過程においても、重要な礎となりうるのではないかと、この関係者は指摘している。このような観点からも、研究開発プログラムに対する連邦政府内の標準的な評価ツールの出発点となった PART は、注目に値する。

NIST にて活用されている定量評価指標
（パフォーマンス測定基準と経済的影響調査）
戦略計画プロセスの一部として、NIST では技術移転に関連する特定の定量データを収集している。このデータには、実施中の共同研究開発契約（Cooperative Research and Development Agreement: CRADA）件数、有効ライセンス件数、標準参照物質／データの生産及び配布状況等が含まれている。

NIST は最近、その科学活動の成果物を測定する基準の開発を試みている。例えば、NIST は、ピアレビューを行っている科学誌において発表を認められた NIST 研究者による論文数を追跡している点が挙げられる。また、こうした発表の引用による影響に関する研究も行ってきた。すなわち、NIST が著者となっている論文を影響あるものとして引用している論文の数を分析し、NIST による科学知識が後に下流効果を持つことを示すというものである。

---

[200] PART による NIST プログラムの評価
http://georgewbush-whitehouse.archives.gov/omb/expectmore/detail/10001021.2003.html

しかしこれらには、問題点もある。まず第一に、NIST の研究の大半はピアレビューを受けた論文ではなく、技術報告書の形で出版されている点。第二に、技術報告書は実験方法に用いられる標準開発における NIST の役割を功績として認めるために引用されることが多く、関連する科学が特に重要であると評価されているわけではない点である。NIST における評価活動に外部者として関与したある関係者によると、こうした測定基準は便利である反面、NIST による研究の効果を充分に、また適切に捉えるものではなく、出版／引用分析は、NIST にとってはやや誤解を招く恐れのある基準であるという。尚、こうした分析方法について、具体的な見直しを行っているかどうかについては、不明である。

NISTは研究成果だけでなく、研究成果が経済に及ぼす影響も計測しようと試みる点で非常に特殊である。Gregory Tassey博士の指導のもと、NIST経済分析室では、個々のNISTプログラムを検討し、投資に対する財務利益を異なる方法で測定、その定量化を試みる一連の「経済的影響調査（Economic Impact Studies）」[201]が過去 15 年にわたって行われている。NISTは経済的影響を決定するため、「ハイブリッド」アプローチをとっている[202]といえる。

まず NIST は、研究プログラムが実施されず、期待していたプログラムの研究成果が創出されなかった場合、企業や産業界にどれだけの影響を及ぼすのかを試算する。これは、プログラムの特定の効果を推測するため、「反事実的」ケースと呼ばれる。

次に、NIST による特定の研究結果の代わりに、どのような民間の研究成果が活用されうるか、またこうした成果が、NIST による研究成果に比べて、制約やコストがどれだけ大きいかを試算する。さらに、NISTプログラムの結果によって予測される一連の「回避可能なコスト」について、定量計算を行う。特に NIST の計測及び標準化活動は、産業のサプライチェーン当事者間の取引に「連鎖」効果をもたらすため、NIST による研究がサプライチェーンの早い段階で経済的結果を向上する傾向がある。こうした影響はサプライチェーンの先に進むほど拡大される。NIST は、内部収益率、便益費用比率または純現在価値の 3 つの手法を使って、試算を行う。

便益費用比率は、NIST が試みる評価に関して、信頼性の高いデータの入手の容易さや分析の妥当性において、もっとも一貫性のある方法であることから、この手法に基づいて、評価の対象となるNISTプログラムの便益費用比率は、少なくとも3:1、あるいは多くのケ

---

[201] NISTの経済的影響調査に関する概要紹介 http://www.nist.gov/director/planning/study_info.cfm 及び過去の調査紹介 http://www.nist.gov/director/planning/summary-studies.cfm

[202] Al Link／John Scott による研究成果報告書「*The Theory and Practice of Public-Sector R&D Economic Impact Analysis: The Case of the National Institute of Standards and Technology*」pp.11-16 を参照。ノースカロライナ大学グリーンズボーロ校経済学部より 2011 年 9 月出版。 www.uncg.edu/bae/econ/より入手できる。

ースにおいて、200:1（プログラムに1ドル使用することで、産業に200ドル相当の便益がもたらされる）となる。

この評価調査は、過去 10 年以上実施されており、実際にNISTによる研究成果が産業に影響を与えたものを対象にしており、NISTが行っているすべてのプログラムに対して実施するものではない。過去に評価調査を実施したプロジェクトには、データ暗号基準及び今フォーマンス・テスト手法（Data Encryption Standards/ Standard Conformance Test Methods）やコンピュータ・セキュリティ、アクセスコントロールに関連するプロジェクトなどが含まれる[203]。

NISTにおける評価活動に外部者として関与したある関係者によると、NISTの経済的影響分析の弱点は、コスト、雇用、信頼性に欠ける恐れのある技術の利用度等について、あくまでも予測値を用いなければならない点であるという。より正確なデータを収集する取組みとして、NISTは「米国の再投資における科学技術―イノベーション、競争力、科学に関する研究の効果測定（Science and Technology in America's Reinvestment – Measuring the Effect of Research on Innovation, Competitiveness and Science: STAR METRICS）」[204]プログラムの対象パイロット機関（2 機関）の一つとなっている。同プログラムはNSFとNIHが設計、開発したもので、研究プロジェクトに関連するデータを財務管理システムから直接抽出し、研究プロジェクトのコスト、使用した資源（人件費等）及び各プロジェクトの性質に関する実際の数字を提供するものである。さらにいずれは研究がもたらした科学論文や特許についてもデータを提供する予定である。これまでのところ、STAR METRICSは政府が資金提供を行う大学のプロジェクトに関するデータを得るためだけに使われてきた。NISTはこのシステムを用いて政府系研究所で行われる研究を追跡する最初の例となる。NISTはSTAR METRICSが今後の経済的影響調査に用いるためのより確固とした信頼性の高いデータを提供することになると期待している。

NIST にて活用されている定性評価指標
（外部機関による評価審査）
定量評価については、データ収集、データのそのものに対する信頼性、活用する方法論、そして評価結果の適正な比較などの面において、多くの制限、限界がある。そのため、NIST は定量分析を定性評価で補充してきた。その主な２つの方法とは、「先端技術に関する訪問委員会会合（Visiting Committee on Advanced Technology: VCAT）」と、全米科学アカデミーの全米研究評議会（the National Research Council of the National Academies of Science: NRC）による「全米研究評議会ピアレビュー（National Research Council Peer Reviews: NRCPR）」である。

---

[203] NIST の経済的影響調査に関する過去の調査紹介
http://www.nist.gov/director/planning/summary-studies.cfm
[204] STAR METRICS に関する公式概要　https://www.starmetrics.nih.gov/

VCATは、NIST外部の著名な科学者及びエンジニアのグループであり、年 4 回キャンパスを視察、NISTの幹部や研究員によりプレゼンを受け、米国の科学・経済システムという幅広い状況においてNISTの働きについて議論する。VCATの委員長はVinton Cerf博士で、インターネットプロトコールの共同発明者である。VCATは年次報告書を発行し、NISTの戦略的方向性、管理慣習、インフラ、運営、及び研究プログラムに関しての意見や批評を論じる。VCATはまた時折書簡報告書や技術報告書を提出し、NISTのあるプログラムや活動について特集を組み詳細を述べる。VCAT会議は一般にも公開されており、全ての会議録及び報告書はホームページにて発表される[205]。このようにVCATは、NIST全体の活動をマクロ的に評価する役割を担っている。

NRCは長期にわたってNISTと関係を持ち、NISTの各研究所について、ピアレビューを実施してきた。NRC はそれぞれの研究所にピアパネルを編成し、そのピアパネルは全米アカデミーのメンバーで特定の研究分野に関連した専門家と認定されるメンバーで構成される。審査パネルはNISTの研究所を何度か視察し、NISTのスタッフそして外部のオブザーバーによるプレゼンを聞き、独自のインタビューや会合を開催する。レビューはおおよそ 1 年かかり、結果はその研究所に対して総括的な評価報告書として提示される[206]。NRCPRについては、VCATとは異なり、NIST内で実施される個別の研究プロジェクトやプログラムを評価の対象としている。

最近 NIST は、強力で正式な戦略計画プロセスが欠如しており、NIST のステークホルダ及びパートナーからの直接的なフィードバックを収集することを怠ったとして批判された。この批判は現在 NIST の計画の一部として対処中である。

ハイルマイヤー手法

NISTの最近の発展の一つは、年次の「3ヵ年プログラム計画」、つまり今後数年にかけて新しいNISTプログラムが発展するための手引きとなる「投資優先領域」を詳細に記したものを制作したことである。これは、NIST経済分析室（Economic Analysis Office：EAO）が、毎年発行するもので、「2007 年COMPETES法（the America COMPETES Act of 2007）」によって、その提出が義務付けられたものである。 2008 年のプログラム計画（2009 年度から 2011 年度対象）では、NIST院長室（the Office of the Director）がNIST内の研究所から直接新しいプログラムの提案を要求する[207]。全６頁で構成される提案書の雛形が開発され、提案者はイニシアチブを説明する技術的計画の提出と同時に、NISTがそのイニシアチブを追究する理由を戦略的に正当化することが義務付けられて

---

[205] VCAT に関する組織概要 http://www.nist.gov/director/vcat/charter.cfm 及び VCAT 紹介 http://www.nist.gov/director/vcat/index.cfm 参照

[206] NRC に関する組織概要 http://www.nationalacademies.org/about/whoweare.html 及び活動内容紹介 http://www.nist.gov/director/nrc/index.cfm

[207] NIST プログラム提案要求内容、2008 年 2 月 http://www.nist.gov/director/upload/Final_NIST_3y.pdf

いる。

この提案の手順と評価については、例えばNIST　IT研究所（Information Technology Laboratory: ITL）の場合、ITL内の全ての研究者に対して研究プロジェクト募集に関するEメールを流し、参加希望者を募ることから始まる。研究プロジェクトへの参加を希望する提案者は、メールに返信することで、意思表示をする。続いて、提案者は個々に、所長ほか約 10 名近くのITL幹部で構成されるマネジメントチーム[208]に対して行なうプレゼンテーションに招かれる。提案者は、発表会においてそれぞれのプロジェクトについて発表・説明を行い、最終的にマネジメントチームが各々の提案を評価し、プロジェクト実施可否について決定するという流れになっている。

この評価において、NIST の戦略やミッションに沿ったものであるかどうかの戦略性正当化評価においては、以下に紹介する定型質問が活用されている。具体的には、有名なRCA Sarnoff 研究所の役員の一人である George Heilmeier 博士が DARPA 局長であったときに最初に考案した定型質問で、その質問内容は以下の通り。

①問題は何か、またなぜ難解なのか。②今日どのように解決できるのか。③新しい技術的なアイディアは何か。④われわれがなぜ今成功できるのか。成功した場合の影響は。⑤プログラムはどのように編成されるか。⑥どのようにして即座の成果を出すのか。どのように進歩を計るか。⑦コストはいくらか。

この定型質問は「ハイルマイヤー教理問答」（カトリック教会が発行した教義にちなんでいる）として知られており、見込みのある技術プロジェクトのコンセプトを評価し選別することに一般的に用いられている。NIST では、この定型質問をベースにやや手を加え、提案者に次の質問事項に回答するよう求める。

- 問題は何か、またなぜ難解なのか。トピックまたは問題について簡単な概要を 1，2 文で説明せよ。
- 今日どのように、また誰が解決できるのか。
- 最新の技術は何か、また誰が取り組んでいるのか。
- 新しいアイディアは何か。われわれがなぜ今成功できるのか。
- この問題にどんな決定的なアイディアまたは能力をもたらすことができるのか。
- 成功した場合の影響は何か、また誰が関わるのか。
- この提案に資金が出た場合、NIST は何を達成するのか。可能と思われる実績及び/または成果物の概要を説明せよ。NIST が目的に到達した場合、産業や社会にどのような便益がもたらされるか。その便益を受ける対象及び規模の指標も説明せよ。

---

[208] ITL 所長、副所長、副所長補佐 2 名、戦略担当ディレクター、及び ITL 内の 6 つの研究部門長を含む 9 名から 11 名体制のチーム。

- なぜ NIST がこれをすべきなのか。この課題に取り組む場として NIST が適当か。なぜ NIST がこの課題に取り組むべきなのか。

本提案の雛形は、基本的に NIST において新しい予算、つまり新たな研究プログラムなどのイニシアチブが提案・考案される際に適用することを意図している。そのため、本提案の雛形は、2008 年度の 3ヵ年プログラム計画においては適用されたが、その後リーマンショックに端を発した景気低迷が影響して新たなプログラムを設置するだけの予算増加がなかったため、その後は一度も活用されていない。

② ＜技術移転について＞

NIST における活動の経済的論拠は、産業の効率的運営を支援するために必要でありながら、「公共財」であるために民間企業などが自主的に取り組みにくい技術的な支援の必要性である。NIST の首席経済学者 Gregory Tassey 博士は、このような技術を「インフラ技術（infratechnology）」、すなわち道路や下水道設備のような物理的インフラに相当する技術的インフラと呼んでいる。計測技術もその一例である。計測能力の向上は、幅広い産業や企業に便益をもたらすが、一企業が商業化しても多くの収益を生み出すとは考えにくいためである。NIST の課題は、この理念の下でもっとも広い範囲でプラスの影響をもたらすインフラ技術を特定し、その能力を民間部門に効率的また効果的に伝達する方法を決定することである。NIST は技術移転活動の奨励と評価によって、こうした課題に取り組んでいる。

NIST が活用する技術移転メカニズム

NIST は比較的小規模な機関であるため、DOD や NIH といった機関のように、重要な商用技術を生み出すような大規模な研究プロジェクトに研究資金を提供することもなく、またそれに伴う技術移転もない。NICT における技術移転は、NIST が同機関のウェブサイトなどを通じて発表した新たに開発された技術や製品に対して、採用したい企業が直接 NIST に連絡し、NIST から購入するメカニズムとなっている。また、NIST では公共普及、アウトリーチ、人と人との交流を手段として、NIST の研究成果の形式張らない非公式なコミュニケーションを推進している。

①特許とライセンス供与
（Patents & Licenses）

NIST は同機関の研究者が報告する新たな発明を検討し、これを特許検討委員会（Patent Review Committee）に提出して、商業価値があり、かつ米国の産業競争力を高めると思われる発明を決定する。NIST は以下のいずれかの場合において特許権保護を検討する。

（ア）　特許によって発明が商業化される可能性が高い

（イ）　特許が科学または技術の新分野及び NIST の研究努力の認知度にプラスの影響を与える

（ウ）　CRADA の目標に向けて前進するものである

特許検討委員会はまた、開示された発明について特許とライセンス供与に関する評価を行う際、以下のような問いかけを行う[209]。

- 対象となる市場及び見込みのある企業の名前は何か
- その技術が解決する問題は何か
- その技術がもたらすもっとも価値ある便益は何か
- その技術は特有かどうか。他の技術が同様の便益を提供しているか
- 産業規模の大きさは十分か
- 競争に関与しているのは誰か
- 規制面における障害があるか
- その技術が関心の対象となるニッチはどれか
- 潜在顧客から出される質問はどのようなものになるか

NIST は 2010 年度、研究者から 30 件の発明開示を受け、うちその半分の 15 件について特許申請を行い、残りの 15 件は却下された。同年、NIST は申請済みの 7 件について特許を取得している。ポートフォリオに含まれる特許の有効ライセンスは、2010 年度末で 35 件となっており、うち 5 件は 2010 年度に新たに契約を結んだものである。またライセンス 22 件からは、収入も得ている。NIST は 2010 年度、ライセンス使用料として 20 万 2,216 ドルの収入があった。NIST ライセンスは単独のライセンシーに与えられる場合がほとんどである。通常特許権使用料の 66%を NIST が確保し、残り 33%をライセンス化された特許の NIST 発明者に分配する。

②CRADA を含む研究協定及び国際協力協定

NIST は、他の科学機関に比べて、規模が小さい（正規研究職員 1,500 人程度）ため、その研究能力を協力的パートナーシップを通じて活かしている。パートナーシップを組む際に NIST がもっともよく用いるメカニズムは共同研究開発協定（CRADA）である。これは外部組織と共同研究について交渉する際に用いられる連邦政府の標準形式である。CRADA は基本的には単独の外部研究組織を対象とした２者間契約であるが、中には２

[209] NIST 技術マーケティング・スペシャリスト、Cathy Cohn 氏によるプレゼンテーション「Working with Inventors to Enhance Marketing Efforts」より。

者以上の研究機関が契約している場合（Multi-site CRADAs）もある。また、CRADA は米国内だけでなく海外の研究機関との共同研究の際にも適用される。

Multi-site CRADAsの例には、2011 年 10 月にNISTと退役軍人省（Deoartment of Vetern Affairs: VA）の医療センタが医療機器の実証実験とプロトコル設計において複数の非営利組織と契約した例がある他[210]、700MHz周波数帯のLTEネットワークの実証実験を行うことを目的としてNISTと商務省の電気通信情報局（National Telecommunications and Information Agency: NTIA）とコロラド州の通信科学機関（Institute for Telecommunication Science）が協力して NISTの新たな研究プログラム「公共安全通信研究プログラム（Public Safety Communications Research Program）」を設立した例が挙げられる[211]。同プログラムでは、韓国のLG電子やフィンランドのノキア・シーメンス・ネットワーク（Nokia Simens Networks）など海外の民間企業ともCRADAを締結している[212]。

また NIST は「特殊型 CRADA」を締結することもある。これは、NIST が外部の研究組織などに対して、試験所認定業務、研究材料の移転、研究活動に対する専門研究者によるコンサルテーション、そして同様の技術補助などの提供に係るものである。

NIST では 2010 年度において、1,465 件の CRADA が締結されており、様々な活動が展開されている。このうち 66 件は、実際の共同研究活動に対する典型的な CRADA であり、残りの 1,399 件は「特殊型 CRADA」であった。また上記の 1,465 件のうち、典型的な CRADA の 16 件と、「特殊型 CRADA」 の 1,374 件は 2010 年度に始まったものである。この件数面での差異は、「特殊型 CRADA」によって行われる活動が、比較的短期間で、特定の業務または活動を対象とするのに対して、典型的な CRADA は、特定の研究活動が終結するまで行われるケースが多く、比較的協定契約期間も長くなっているという違いから生じるものである。

NIST は戦略的研究パートナーとの長期的な関係を確立するために CRADA を活用する。例えば、NIST 物理計測研究所の放射線グループは、環境放射線の分野でメリーランド大学と多くの協定契約を結んできた。こうした契約によって、自然放射線や放射線源に関する環境標準が数多く発行されることとなった。こうした CRADA の重要な側面は、NIST

---

[210] VA の Multi-site CRADA の概要 「STANDARD OPERATING PROCEDURES FOR PHASE I, II, III OR IV OR DEVICE MULTI-SITE CLINICAL TRIAL COOPERATIVE RESEARCH AND DEVELOPMENT AGREEMENTS」参照
www.research.va.gov/programs/tech_transfer/.../multi-site-sop.doc
[211] 700Mhz 周波数帯LTEネットワーク実証実験プログラムの概要
http://www.pscr.gov/about_pscr/highlights/iwce_2012/t113-olbrich.pdf
[212] 700Mhz 周波数帯LTEネットワーク実証実験プログラムの概要（p. 12）
http://www.pscr.gov/about_pscr/highlights/iwce_2012/t113-olbrich.pdf

が CRADA を、外国政府機関との直接交渉なくして、メリーランド大学で研究する海外の研究者と交流するために用いていることである。

また、NISTによるCRADAには、他の連邦機関が資金を提供する研究も含まれる。中性子相互作用／線量計測グループは、メリーランド大学物理学部と共に、バージニア州ブラックスバーグ付近の中性子検出器のプロトタイプを管理している。同検出器は、エネルギー範囲 1~200 MeV で中性子束のデータを記録する。これはメリーランド大学と NIST が NSF から受ける共同研究助成金を活用して行っているものである。

さらに、NIST は学生に研究経験を与えるため、また将来の雇用者をトレーニングするために「特殊型 CRADA」を利用することがある。NIST 電子・光物性部の Charles W. Clark 博士は、CRADA を活用して、メリーランド大学物理科学技術研究所の特任教授を兼任している。Clark 博士は、光学的格子で強度に相互作用する原子の力学について研究を行っている大学院生の指導教授でもあり、このポジションを通じて、学生などに NIST における活動内容を広めることが可能となっている。例えば、メリーランド大学のある学生は、卒業後ハーバード・スミソニアン天体物理学センター及びハーバード大学物理学部でポスドク研究を終え、ボールダー市にある NIST への勤務を決めている。
NISTによるCRADAを通して、外部機関と長期的な関係に築いているケースもある。アメリカ歯科医師会財団（American Dental Association Foundation: ADAF）は、歯科学研究所であるNISTゲイサーズバーグ・キャンパスに位置するパッフェンバーガー研究センター（Paffenbarger Research Center）の運営に資金を提供している。ADAFは、歯のインプラントに用いる標準材料の開発、インプラント材の腐食耐性試験、歯面清掃に用いる研磨剤の標準化等、様々なテーマに関する研究プロジェクトに資金提供を行っている[213]。同センタは現在歯科処置やセラピーで使われている数多くの技術を生み出し、また歯科全体にわたる新製品の開発を助ける標準参照物質（Standard Reference Materials）を発行する。

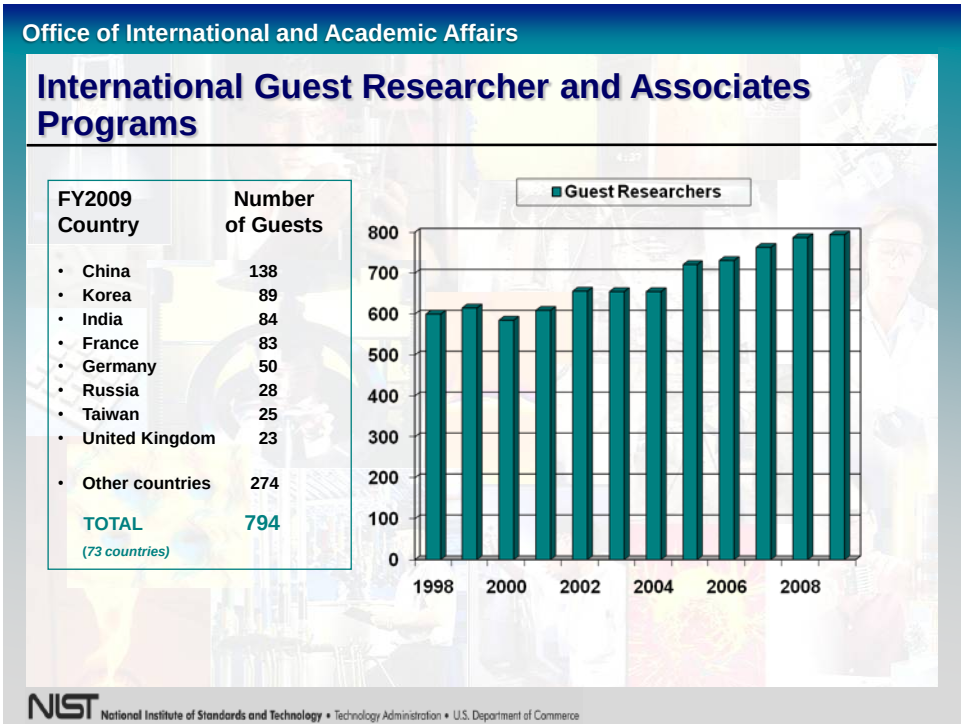
また NIST は、NIST に関連する研究分野において、米国と外国との科学技術協定（Science and Technology Agreement）の履行を行う。例えば、NIST は南北アメリカ大陸計量システム（Sistema Interamericano de Metrology: SIM）の調整を支援している。SIM は、米州機構（Organization of American States: OAS）に参加する南北アメリカ大陸の 34 ヶ国に国立計量機関を設立するための多国による取組みである。NIST は、計量研究センターを設立中の国に、技術補助や派遣職員を提供している。SIM は西半球における商業を促すため、国際計量システムについての取り組みを行っている。

---

[213] ADAF 概要説明 http://www.ada.org/prc.aspx 参照

③客員研究員
(Guest Researchers) [214]

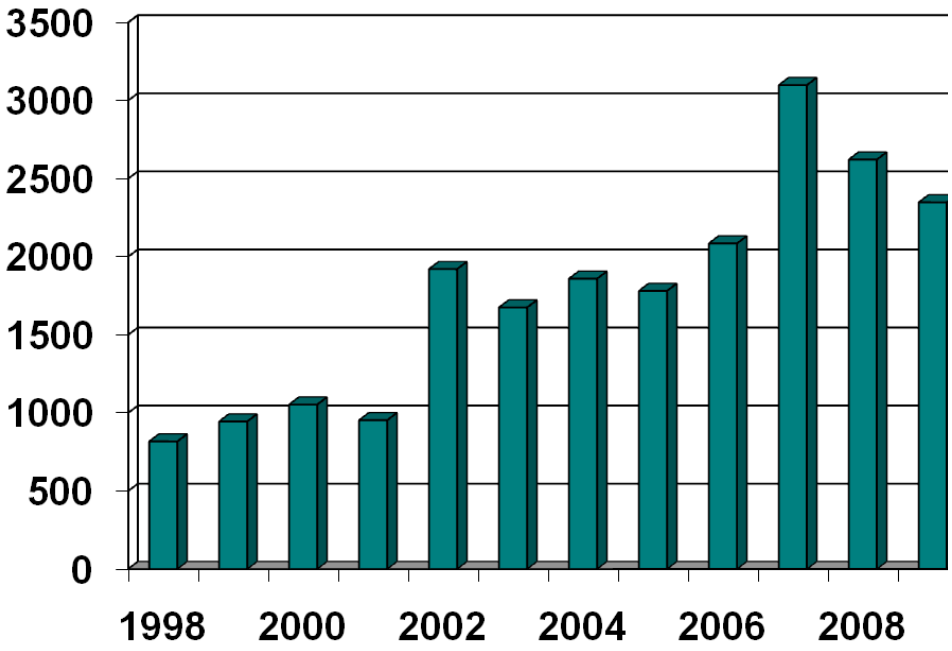
NIST は、もっとも効果的な技術移転は研究者間の個人的な交流を通じた知識交換であるとしている。そのため、NIST では毎年何千人もの客員研究員を研究施設に受け入れている。客員研究員の招聘は、定期的に募集しているわけではなく、NIST のプロジェクトマネージャがプロジェクトに海外からの研究者が必要かを判断し行う。海外の研究者から NIST 側に客員研究員の募集に関してアプローチされることもあれば、NIST 側からすでにコンタクトのある海外研究者に直接、または海外研究者を支援しているスポンサー機関を通してアプローチする。下表は 2009 年に NIST が招いた海外客員研究員の数を国毎に示したものである。また、客員研究員が時間の経過とともに全体的に増加している点も読み取れる。こうした研究員に対して NIST は給与の支給は行なわないが、NIST 施設で研究を行う期間中、住宅費などを一部補助するケースもあるようだが、詳細は不明である。



客員研究員プログラムに加え、NIST では国際訪問者プログラム（International Visitor Program）も運営する。これは非米国研究者を NIST に短期間（通常 1 日または 2 日）招き、NIST 施設の紹介、NIST 研究者との知的交流を促すとともに、訪問者の所属する機関との長期パートナーシップ発展の基礎を提供する。下表は NIST が受け入れた年次別

[214] NIST Office of International Affairs 活動概要 http://www.nist.gov/iaao/intlaffr.cfm

国際訪問者数を示す。



2009 年度、NIST は 90 ヶ国以上から 2,348 人の国際訪問者を受け入れている。
こうした国際交流に加え、NIST では多くの研究者と共同研究の取り決め、その他交流等の調整を行う。NIST には「NIST 準会員」として、海外からの様々な研究者がキャンパスで研究を行っている:

- NIST の国立ユーザ施設を実験に利用する研究者
- NIST の研究に関わる独立契約者
- 政府横断型機関の人事交流（他の米国機関職員）
- 施設外の協力者
- NIST で研究プロジェクトや研修に携わる現役学生

④中小企業技術革新研究プログラム
（Small Business Innovation Research: SBIR）[215]
中小企業技術革新研究プログラムに参加することが義務づけれている連邦機関の一つとして、NIST は予算の一部を中小企業が行う研究に充てている。ここでいう研究とは、NIST の運営ニーズを支援するものである。NIST は小規模な科学集約企業の助けが必

[215] NIST SBIR プログラム概要説明 http://www.nist.gov/tpo/sbir/

要な分野について応募を行い、提案書を検討、これに基づいて関連するプロジェクトを請け負う企業を選ぶ。

2008 年より、NISTはSBIR参加企業が開発した技術の商業製品への移転を促すため、新たなプログラム、SBIR-TT（Technology Transfer）を開始した。同プログラムでは、商業化が可能な技術を生み出す可能性の高いNIST SBIR公募について重点分野を特定する。こうしたテーマについて、NISTは以下の詳細を求めている[216]:

1. 背景となる NIST 技術に関する記載及び参考実例。
2. 背景技術を充分に活用するにあたって残る研究格差の明確な言及。SBIR-TT 候補者は、この研究格差に対する革新的アプローチについて提案を行うよう促される。
3. NIST の資金が提供され、それが SBIR 企業の研究と技術革新の達成に有益であることが明確に記載されている。この中には NIST 研究者／発明者によるコンサルティングの時間、施設や材料、器具、装置等へのアクセスが含まれるが、これに限定されるわけではない。
4. 資金は、NIST 背景技術を前進させるため提案を受けたアプローチの実現可能性を証明するために授与される。概念が無事に証明された場合は、プロトタイプの研究開発に資金が継続される。
5. 背景技術が特許化されている場合、SBIR-TT 契約内で非独占かつ使用料無料の研究ライセンスが与えられる。SBIR-TT 企業には、商業化ライセンスについて交渉する機会を与えられる。
6. 全ての SBIR 授与金に関して、SBIR-TT 企業は SBIR プロジェクト期間中、全ての技術革新について権利を保有し、必要に応じて特許権保護を要請することができる。SBIR 企業がその革新技術を企業秘密として社外秘とする場合、SBIR 契約は必要な守秘義務を提供する。どちらの場合も、連邦政府はその目的のために革新技術を使用する一括払いライセンスを保有する。

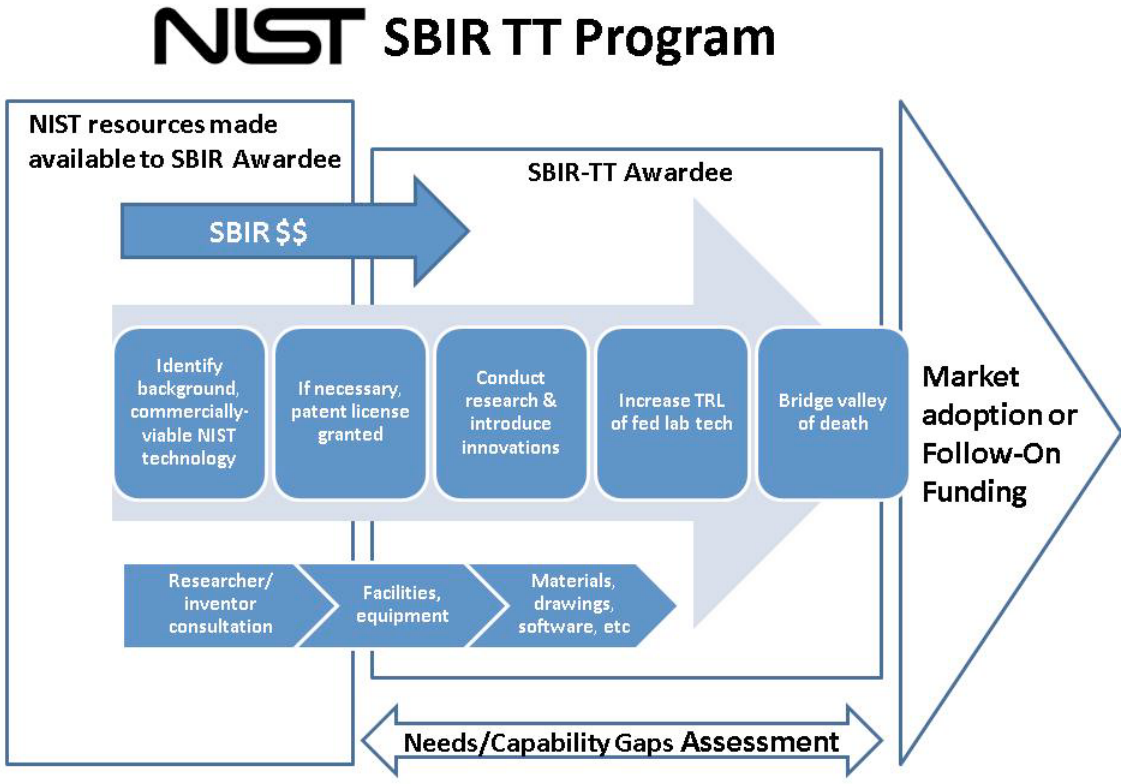
SBIR-TT プロジェクトを得た場合、企業は当該プロジェクトを通常の SBIR プロジェクトと同様に行うが、最終支払は企業がプロジェクトの成果について商業化に関する報告書を提出するまで保留となる。商業化に関する報告書には、これまで計画され、実行された他の活動と共に、技術から収入を生み出すための将来に向けた計画を含まなければならない。これには、価格設定、パートナー、ライセンス供与、生産計画、製造パートナー、継続的な研究開発予算等が含まれるが、これに限定されるものではない。SBIR プロジェクトで開発した技術を効果的に商業化するために SBIR 企業が約束するリソースについて明示するとともに将来の商業化について予測を示さなければならない。プロジェクト期間中、NIST は商業化に関する報告書の作成について技術補助を提供する。プロジェクト

---

[216] NIST SBIR-TT 概要説明 http://www.nist.gov/tpo/sbir/sbirtt_factsheet.cfm

期間後、当該技術が製造を必要とする場合、NIST は同機関が資金を出す製造業拡張パートナーシップセンタから、企業が生産施設を確保できるよう補助を仲介する。下図は NIST SBIR-TT プロジェクトの典型的な段階を示す。

2008 年以来、NIST が資金を提供した SBIR-TT プロジェクトは 27 件となっている。こうしたプロジェクトによって、NIST は技術の商業化を進める研究活動に対する 11 件の新たなライセンス契約を、また技術を市場に出すための商業化ライセンス契約 3 件を締結している。



⑤標準参照物質と標準参照データ
（Standard Reference Materials & Standard Reference Data）
NIST では、その標準化活動において、標準参照物質と標準参照データの双方を開発する。標準参照物質は特定の物質について共通の計測標準を確立するために用いられ、標準参照データはより精密な科学計算と実験の基礎としてふさわしいと指定された数字データである。2010 年度時点で、NIST によって 1,283 件の異なるタイプの標準参照物質が利用可能となっており、同年こうした物質 31,667 ユニットを販売した。また NIST は、120 の標準参照データセットを説明書付きで発行している。

⑥キャリブレーションと認定業務
（Calibration and Accreditation Services）
民間及び非政府の顧客に代わり、NIST は様々なタイプの計器について、こうした製品がその精度について適切に認定されていることを確認するため、キャリブレーション試験を行う。また、NIST が開発した連邦の技術標準に適合することを認定するため、製品の検討を行う。こうした認定は、ベンダが米国政府機関による購入条件を満たす際に必要となる。2010 年度には、認定を求める外部顧客のため、NIST は 17,697 件のキャリブレーション試験を行っている。

3.3.2. 標準化活動に関する取組みについて

NIST の標準化活動は標準化調整局（Standards Coordination Office）により運営されている。NIST の標準化政策は主に、次の 4 つに主眼を置いている。

- 米国の製品がグローバルな市場にアクセスできるような測定法及び標準化したインフラ
- 新規の技術に対して基盤となる測定科学のグローバルリーダーシップ
- 調和の取れた標準化と透明な規制体制
- 米国の外交政策に関する目的への支援

NIST は米国計量標準総合センタ（National Metrology Institute）とその主な標準化機関を指定しているが，NIST 自体は多くの標準そのものを独自に開発していない。NIST の責任は単に連邦政府の運営やシステムに応用される標準を開発したり公表することである。他の領域では、自発的な産業主導である標準開発団体（Standards Development Organization: SDO）が標準を作成、普及している。ただし、NIST はよく SDO のオブザーバーとしてのステータスを持ち必要に応じて標準開発の活動に対して影響や権威を行使することがある。

① 標準化の研究と開発の結果を普及する方法
NIST には標準化研究開発活動が市場に影響をあたえることを確実にする 3 つの主なメカニズムがある。

第一に、産業主体の標準（化）団体の投票権のない参加者として、NIST のスタッフは産業側からの参加者に対して直接的に NIST の研究の発表をすることができ、標準化文書に対して技術的貢献をすることができる。NIST の研究が新規に開発された標準化に盛り込まれる直接的な方法である。

第二に、前述したように NIST は標準参照物質及びデータをエンドユーザに対して開発、販売することができる。自社の製品及びシステムに対して適切なキャリブレーションを行

いたいと思う企業は NIST にその標準に関係する能力を求めて連絡してくる。NIST はまた技術報告書や関連した連邦の技術標準をウェブサイトに掲載している。

第三に、NIST は民間産業の代表者、特に民間研究者の視察を受け、自らの技術と能力について紹介することもある。NIST はまたそのサービスと提供できるものをトレードショーや類似の会合で実演することもある。そのため、そのような伝統的な「マーケティング」活動を通して、NIST はその成果の認知度を高め、産業全体に NIST の研究を採用させることができる。

② ICT 関連の標準化活動：開発と普及

NIST が標準化に関してはるかに重要な影響を持つ分野は ICT 関連の標準である。差別化を生み出す理由の一つは、NIST が非軍事政府機関、特に情報のセキュリティで用いられる ICT 製品に対する標準を設定していることにある。米国政府は ICT 製品とサービスの国内における最大の単独購入者であり、すべての調達ベンダーは政府という顧客に販売するために NIST の標準に遵守していることを示すことに特に大きな関心を持っているといえる。

2 つ目の理由は、NIST が情報セキュリティー技術、特に暗号化と侵入探知における世界クラスの専門知識を集積してきたことにもある。このような能力は、従来からあるヘルスケアやエネルギーなどの政府の関心分野にとって益々重要となってきている。例えばヘルスケア分野では、電子カルテへの移行がベンダーのシステム間での高い相互運用性を求めることになるが、患者のプライバシーや秘密事項を堅調に保護しなくてはならない。NIST はこの相互運用性と情報保護について共に専門技術を有している。同様に、国家の電力配分システムを管理する「スマートグリッド」を開発する動きには、異なったグリッドシステム間の通信能力が重要となる。また、サイバーテロリストの攻撃が、システム保護なくして建設されてきた電力グリッドを攻撃する恐れも年々増加しいる。さらに、NIST はその研究を ICT データ交換、研究コンソーシアムの管理、及び情報セキュリティに活用し、スマートグリッドシステムのサイバーセキュリティ標準を新規に開発することもできる。

オバマ政権下では、NIST は、ICT の最先端技術の分野において民間セクターと共に総括的な標準化の活動を主導するという明白で顕著な役割を担ってきた。特別関心のある分野は暗号、クラウド・コンピューティング、ヘルス ICT、そしてスマートグリッドである。

③ 暗号技術に対する標準規格普及活動について

NISTは連邦情報セキュリティ管理法[217]においてFIPSを維持し、施行する責任を持つ。こ

---

[217] 各連邦政府機関に対して、省内のシステムや情報を保護するために情報セキュリティ対策を講じるよう義務付けた連邦情報セキュリティ管理法のこと(Federal Information Security Management Act :FISA) : http://csrc.nist.gov/groups/SMA/fisma/index.html

の標準は連邦政府の使用する情報システムに設計が義務付けられている、性能に関する要件及び相互互換性のある手段を詳細にした文書である。連邦議会で設定され、OMBに監視されているように、連邦調達制度はICTシステムが政府機関に販売される際にFIPSに遵守することが求められる。

NISTが単独で権限をもつICT標準化の一分野は、政府雇用者に保障される秘密通信の保護のため用いられる正式な暗号技術の指定である。このような標準規格はNISTが出版するFIPS[218]の大部分を構成している。最新の標準は電子署名・標準（Digital Signature Standard; FIPS 186-3）であり、電子署名を認証するのに使用されるハッシュ・コードを作り出すためのアメリカ政府標準のハッシュ関数（Secure Hash Standard; FIPS 180-3）アルゴリズム を取り入れている。

NIST は、いくつかのソフトウェア攻撃が他のハッシュ・アルゴリズムを解除することに成功しつつあり、また現行の SHS が解除されるというリスクもかなり高いため、新規の政府標準のハッシュ関数（Secure Hash Standard: SHS） を特定化する過程にある。この過程は NIST がどのように ICT セキュリティー標準を開発、普及するかを示すものである。

NIST が先端暗号標準（Advanced Encryption Standard）を開発するのに用いたプロセスに基づき、NIST は競合するハッシュ技術の公開競争を行うことにした。政府利用の Eメールや電子メッセージシステムすべての変更を必要としていることがあり、新しいハッシュ技術に移行することによる影響は非常に広範囲にわたる。またほとんどの ICT ベンダーは政府に提供するシステムと同じものを民間の顧客に提供することが常であるため、新規 SHS は今日使用されているメッセージシステムの保障すべてに変更を及ぼすことになると見られることからも、この変更が慎重に管理されるべきことを NIST は認識している。

現行のプロセスでは、NIST はハッシュ技術に対して攻撃を試みる脅威についての公的なワークショップ（Workshop on Cryptography for Emerging Technologies and Applications: CETA）などを開催し、新規 SHS の開発法についてのフィードバックを求めている。2007 年に NIST は SHS が実現する必要のある要件をまとめた原案、一般から意見をもらうための起案書を公表した。 そのコメントに基づいて最終版の要件文書を公表した。NIST はその後どのベンダーに対しても新規の SHS の候補者としてハッシュ技術を提示するよう誘いをかけた。2008 年度末に、NIST は提出期限を終了し、候補者たちに対する 3 回のうち最初の評価を実施した。2009 年と 2010 年の半ばに 2 つの評価が行われ 、その結果に基づき 2010 年末に NIST は 5 件のハッシュ・アルゴリズムを選

[218] NSF FIPS に関する説明 http://www.nist.gov/itl/fipscurrent.cfm 参照

択した。再び一般の意見を求めるためにそれぞれの詳細を公表した。2011 年 12 月に意見期間が終了し、2012 年初めに NIST は 3 回目であり最後の競争を行い、ドラフト SHS として 1 件の候補者を選択する。NIST はその後ドラフトに対する意見を集め、改訂した最終版 SHS を 2012 年末までには公表することを目標としている。

本プロセスは 5 年以上の期間をかけ、複数のワークショップ、一般からの意見募集、民間部門や学界との話し合いを含んで行われる。またこのプロセスは、NIST がハッシュ・アルゴリズムの候補を内部で開発するのではなく、広い範囲の開発者から受け入れているという点で注目されるものである。このことから NIST が暗号やセキュリティ標準を開発する際に、アウトリーチや協力に重点を置く度合いが示される。SHS の競争に関する各段階における重要な発表は RSA 年次会合のような産業界の集まりにおいてなされている。というのは出来る限り幅広い関係者が NIST の開発について学習し、そのプロセスに対して自らの意見を出すことを奨励することを確実にするためである。

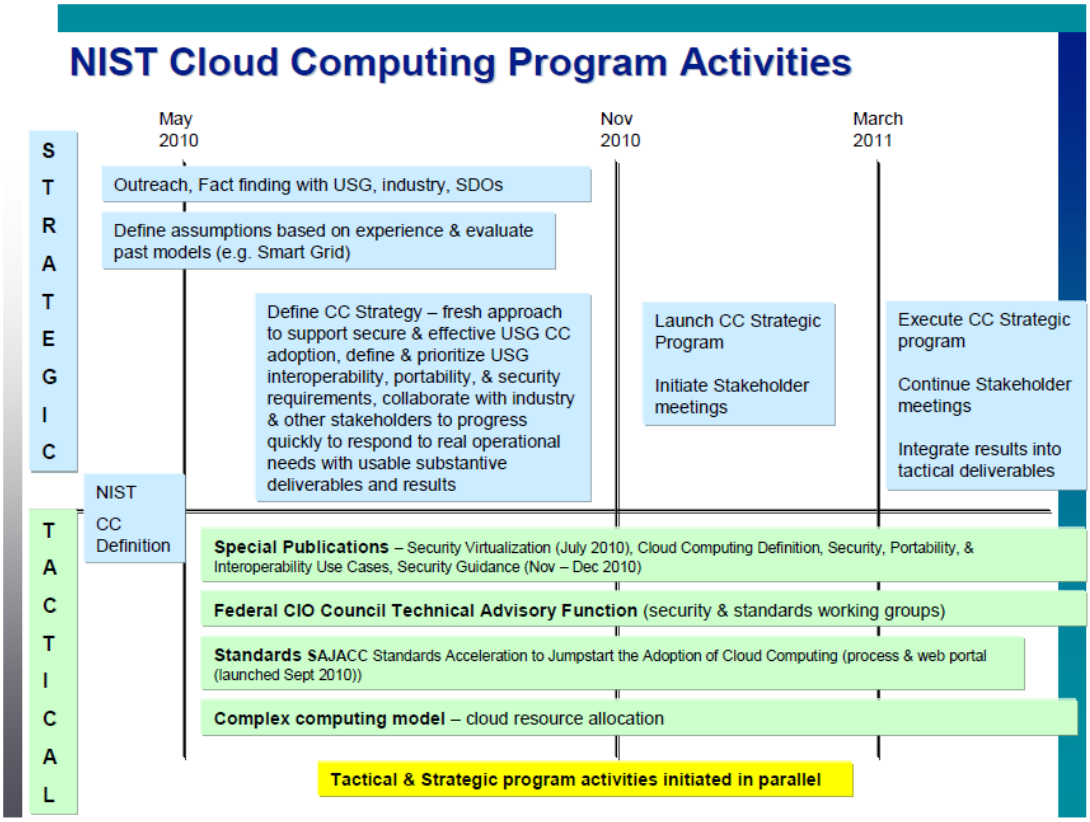
④ クラウド・コンピューティングに関する標準規格の普及活動

クラウド・コンピューティングとは、情報ストーレージ、プロセス、及び出力用のプラットフォームとして、コンピュータが広範囲で分布されている、ネットワークシステムの使用形態示す。クラウド・コンピューティングは、クラウド・ベースシステムがインターネットの接続（モバイルコンピュータ及びスマートフォンを含む）によるいかなる装置を通しても一般的に利用可能であること、また高い冗長度を特徴とし、低コストにてコンピュータパワー及び保存容量を提供する規模の経済性を活用するため、ローカルコンピュータを使用するよりアプリケーションを実行する、より優れたアプローチだと考えられている。

2011 年、当時連邦政府の CIO であった Vivek Kundra 氏は覚書を発行し、政府機関に対して、データセンタ及びローカルサーバの代わりにクラウド・コンピューティングプラットフォームの使用の可能性を探るよう指示を出した。当時は一般的に、クラウド・コンピューティングに関する懸念として、セキュリティ上の問題が指摘されていた。クラウド・ベースシステムは、民間のサービスプロバイダによって運営され、その性質上、特定のクラウド・ベース ICT サービスを提供している物理的コンピュータ施設を追跡するのはしばしば困難である。このことは、エンドーユーザである機関が、クラウド内のデータを保護するために使われるセキュリティ対策、もしくは、どのプロバイダが単一アプリケーション又はサービスのサポートを行っているかについて、ほとんど理解していないという意味である。

クラウド・コンピュータから得られるコスト削減及び効率性に期待される実質的な便益のために、NIST は評価、検証、及びクラウド・システムのセキュリティ強化に向けた標準化されたプロセスとメカニズムを開発するための新規の活動を開始した。NIST はクラウド・コンピューティングの定義の向上及び、クラウド・プラットフォームのセキュリティに関する懸念を明確にするための数回のワークショップを主催することから始めた。こういったイベントからクラウド・コンピュータの技術的ロードマップ（USG Cloud Computing

Technology Roadmap）の草案に向けての情報が提供された。2011 年 12 月に意見を求めるために公表され、機関がどのようにエンタープライズ・アーキテクチャ内のクラウド・ベースコンピューティングサービスを獲得し、利用、及び監視するかを提案するものである。



ロードマップの活動と同時に、NIST は OMB と共同で、連邦政府によるクラウドのセキュリティ評価及び認証プログラム（Federal Risk and Authorization Management Program: FedRAMP)を開発した。FedRAMP によって、クラウド・プラットフォームに伴うセキュリティリスクを政府機関が軽減する方法を規定する政策が作成されている。FedRAMP の重要な役割は、「第三者評価組織」（third-party assessment organizations : 3PAOs)を指定することにあり、3PAOs はクラウド・サービスプロバイダのセキュリティーを評価し、FedRAMP の基準への遵守を証明することの認可が与えられる。

クラウド活動は、NIST が利用する公共コンサルテーション、外部ワークショップ、及び他の機関や民間部門を含むパートナーシップにまで反映されている。NIST は主要クラウド・コンピューティングサービスプロバイダ（Microsoft、IBM、Amazon 及び Google を含

む）との多数に及ぶ会議を主催すると共に、活動が機関の ICT 部門の必要性に見合うことを保証するために、連邦 CIO 評議会とも協力している。

⑤ スマートグリッドに関する標準規格普及活動について

スマートグリッドに関する NIST プログラムは、スマートグリッド諮問委員会の形成を持って、2007 年に正式開始となった。NIST は、様々な団体との提携及び交流のために中心的役割を果たしている。その団体には、連邦エネルギー政策機関（連邦エネルギー規制委員会（Federal Energy Regulatory Commission）など）、グリッドオペレーションの産業組織（北米電力信頼性評議会（North American Electric Reliability Corporation）、電力業界団体（エジソン電気協会（Edison Electric Institute）、電力研究所（Electric Power Research Institute））、また民間企業、エネルギー消費者、及び公共政策グループが含まれる。医療 ICT に関して、NIST のスマートグリッド活動は、NIST がエネルギーシステム研究及び情報システムセキュリティの両方面で蓄積した専門知識を活用している。

2008 年、NISTはスマートグリッドの相互運用性基準についての公開ワークショップ（Smart Grid Interoperability Panel: SGIP）を主催し、SGIPにおける標準化策定はNIST内だけでなく、産業団体によって広範囲にて促進された。NISTでは、スマートグリッド・サイバーセキュリティ、グリッドの信頼性とパフォーマンスの測定、及び将来の国内スマートグリッドパフォーマンスの支援に関する活動が同時進行している。これらの活動から生じたNISTによる成果は以下の通り[219]。

- スマートグリッドオペレーション、評価、及び分析に関する技術記述書
- 特定のスマートグリッド製品のパフォーマンス評価
- スマートグリッドシステムを評価するためのデータセット及びベンチマーク参考資料
- スマートグリッド開発を促進する政策フレームワーク
- スマートグリッドに関するサイバーセキュリティ確保のためのガイドライン
- スマートグリッド開発及び相互運用性のための技術的ロードマップ

これらの資料のために、NIST は公開ワークショップ及びコンサルテーションを主催し、これらの資料がNIST 内の専門家だけではなく、産業界及び一般からの意見を確実に反映するようにしている。将来に向けて、NIST は、スマートグリッドの性能を生かす環境制御とエネルギー管理システムを構築する能力において、及び電力サプライチェーンにおいて、スマートグリッドと他の参加者間のインターフェイスを定義するためのフレームワークに、さらなる焦点を合わせることを計画している。

---

[219] NSF スマートグリッドに関する研究、報告書、プレゼンテーション資料
http://www.nist.gov/smartgrid/research-reports-presentations.cfm

⑥ 医療 ICT に関する標準規格普及活動について

2008 年の米国経済回復・再投資法（American Recovery and Reinvestment Act: ARRA）は、全患者の電子健康記録（Electronic Healthcare Records: EHR を実行する医療プロバイダに向けての法律的条件を制定した。現在に至るまで、EHR の採用は任意であり、多数の病院及び医師は互換性に欠け、安全性又は保全性が必ずしも完全に評価できないシステムを有していた。ARRA における医療 ICT に関する義務化を促進する目的で、NIST は、これまでにデータの相互運用性に関する標準と共に、治療や介護における標準を開発してきた実績と経験を生かして、医療産業において、また医療 ICT における患者の守秘義務及び信頼を確保できる、強力かつ信用性あるシステム作りに向けた標準化活動に取組んでいる。

NIST は、EHR システムの利便性に関する公共ガイドラインを開発するために、ホワイトハウス内に設置された国家医療 ICT 調整官室及び医療品質研究調査機構に対して技術的支援を行った。このガイドラインは任意である一方、民間部門が過去に解決しようとしなかった問題に取り組み、そのため、各業者の EHR システム向上に向けロードマップを提供した。

NIST はまた、医療 ICT の保全性及び安全性に対する新規ガイドラインの使用を開発促進するために、既存の米国自主試験所認証（National Voluntary Laboratory Accreditation Program: NVLAP）プログラムを通して活動している。プログラムは、患者及び医療機関のために医療試験及び診断を提供する試験所を認定する。試験所が電子患者登録を注意と責任を持って扱うことは、医療 ICT の公共での信頼性を築き、医療登録の安全性を侵害する潜在的損害を回避する上での重要な要因となる。全ての主要試験所運営企業はすでに NVLAP のメンバーであることからも、NIST はこれらのネットワークを通じて、効果的なアウトリーチ活動を実施することができる。

NIST は任意にて、医療情報管理システム協会（Healthcare Information and Management Systems Society: HIMSS）、医療データ標準の ANSI 委員会 X12、HER システムの相互運用性を図る HL-7 産業協会、及びその他を含む医療 ICT 内の業界標準の開発組織に対しても、技術的支援も提供している。NIST はこれらのグループに NIST からの支援を受けることを義務付けてはいないが、NIST の専門知識から得られる、これらの組織にとってもメリットがあることからも、これらの産業グループは NIST からの情報を歓迎し、標準開発において NIST の技術的レポートを広範囲に利用しており、こうした標準化活動のエコシステムに実質ともに組み込まれているといえる。

付録:用語リスト

英語略称	英語正式名称	日本語訳
AAAS	American Association for the Advancement for Science	米国科学振興協会
ADAF	American Dental Association Foundation	アメリカ歯科医師会財団
AFRL	Air Force Research Laboratory	空軍研究所
AIA	Aerospace Industries Association	航空宇宙工業協会
APAC	Automated Program Analysis for Cybersecurity	サイバーセキュリティのための自動プログラム分析
ARL	Army Research Laboratory	陸軍研究所
ARO	Army Research Office	陸軍研究室
ARRA	American Recovery and Reinvestment Act: ARRA	米国経済回復・再投資法
ASD/NII	Assistant Secretary of Defense for Networks and Information Integration	ネットワーク情報統合担当国防次官補
BD SSG	Big Data Senior Steering Group	大規模データ・シニア運営グループ
CAESARS	Continuous Asset Evaluation, Situational Awareness, and Risk Scoring	継続的資産評価・状況・リスク評価
CAULDRON	Combinatorial Analysis Utilizing Logical Dependencies Residing On Networks	-
CCSR	Center for Computational Science and Research	コンピュテーショナル科学・研究センタ
CEDS	Cybersecurity for Energy Delivery System	エネルギー流通システムのためのサイバーセキュリティ(プログラム)
CHACS	Center for High Assurance Computer Systems	高位保障コンピュータ・システム・センタ
CI	Cyber Infrastructure	サイバーインフラ
CIA	Center Intelligence Agency	中央情報局
CISE	Computer and Information Science Engineering	コンピュータ・情報科学エンジニアリング
CMU	Carnegie Mellon University	カーネギーメロン大学
CNCI	Coprehensive NationalCybersecurity Intiative	包括的国家サイバーセキュリティイニシアチブ
CND	Computer Network Defense	コンピュータネットワーク防護部
CNS	Computer Network Security	コンピュータネットワークシステム部
CONOPS	Software Assurance Concept of Operations	ソフトウェア保証オペレーション構想
COTS	Commercial Off-The-Shelf Software	汎用ソフトウェア
CRADA	Cooperative Research and Development Agreement	共同研究開発契約

CPS	Cyber-Physical Systems	サイバー-フィジカルシステム
CSIA	Cyber Security and Information Assurance	サイバーセキュリティと情報保証
CSIA IWG	Cyber Security and Information Assurance Interagency Working Group	-
CSIS	Center for Secure Information Systems	GMU セキュア情報システムセンタ
CSRC	Computer Security Risource Center	コンピュータセキュリティ・リソースセンタ
DACS	Data and Analysis Center for Software	ソフトウェア・データ解析センタ
DDR&E	Office of the Director of Defense Research & Engineering	国防研究技術局
DHS	Department of Homeland Security	国土安全保障省
DIB	Defense Industrial Base	国防産業基盤
DISA	Defense Information System Agency	国防情報システム局
DOD	Deaprtment of Defense	国防総省
DOE	Department of Energy	エネルギー省
DSB	Defense Science Board	国防科学評議委員会
DSP	Digital Siganling Processing	デジタル信号処理
DSWAP	DHS Secure Wireless Access Prototype	DHS セキュア・ワイヤレス・アクセス・プロトタイプ
EC	European Commission	欧州委員会
EHR	Electrnic Health Record	電子健康記録
EiD	Engineering in Depth	徹底的エンジニアリング
EIOC	Electricity Infrastructure Operations Center	電力インフラオペレーションセンタ
EPA	Environomental Protection Agency	環境保護庁
ESC	Exascale Software Center	エクサスケール・ソフトウェア・センタ
ESPADA	Efficient Security and Privacy Assurance for Database Access	データベース・アクセスのための効率的なセキュリティとプライバシー保証
ETCi	Exascale Technology and Computing Institute	エクサスケール技術と計算研究所
FAA	Federal Aviation Adiministration:	連邦航空局
FBI	Federal Bereau of Investigation	連邦捜査局
FedRAMP	Federal Risk and Authorization Management Program	連邦 リスク評価及び認証プログラム
FIPS	Federal Information Processing Standard	連邦情報処理標準
FIRE	Future Internet Research and Experimentation	将来のインターネット研究と実験
FoSER	Future of Software Engineering	ソフトウェア・エンジニアリングの未来
GEIA	Government Electronics & Information Technology Association	政府電気情報技術協会
GENI	Global Environment for Network Innovations	ネットワーク・イノベーションのためのグローバル環境
GMU	George Mason University	ジョージメイソン大学

GNISE	Global NetOps Information Sharing Environoment	-
GpeNI	Great Plans Environment for Network Innovation	ネットワーク・イノベーションのためのグレート・プラン環境
HCI	Human Computer Interaction	ヒューマン・コンピュータ・インタラクション
HCSS	High Confidence Software and Systems	高信頼ソフトウェア及びシステム
HEC	High End Computing	ハイエンドコンピューティング
HIMSS	Healthcare Information and Management Systems Society	医療情報管理システム協会
HPCC	High Performance Computing and Communication	高性能コンピューティングと通信
IARPA	Intelligence Advanced Research Projects Activity	情報高等研究計画活動
ICCS	International Conference on Cyber Securtiy	サイバーセキュリティ国際会議
ICCS	International Center for Computational Science	計算科学国際センタ
IESP	International Exascale Software Project:	国際エクサスケール・ソフトウェア・プロジェクト
ISC	Intrinsically Secure Computing	本質的にセキュアなコンピューティング
ISAAC	Infrastructure for Astrophysics Applications Computing	天文物理学アプリケーション計算のインフラ
IST	College of Information Sciences and Technology	ペンシルバニア州立大学情報科学・技術学部
ITL	Information Technology Laboratory	NIST　IT 研究所
I2O	Information Innovation Office	情報イノベーション室
LBNL	Lawrence Berkeley National Laboratory	ローレンス・バークレー国立研究所
LSN	Large Scale Networking	大規模ネットワーキング
MURI	Multidisciplinary University Research Initiative	-
NASA	National Aeronautic and Space Administration	航空宇宙局
NCO	National Coordination Office for Networking and Information Technology Research and Development	ネットワーク情報技術研究開発国家調整室
NCSD	National Cyber Security Division	国家サイバーセキュリティ部
NDIA	National Defense Industrial Association	米国国防産業協会
NetIPLab	Netwokring and Information Processing Lab	ロチェスター工科大学ネットワーキング・情報処理研究所
NIH	National Institute of Health	国立衛生研究所
NIST	National Insitute of Standards and Technology	米国商務省標準技術院
NITRD	Networking and Information Technology Research and Development	ネットワーキング及び情報技術研究開発
NOAA	National Oceanic and Atmospheric Administration	海洋大気庁
NRC	National Research Council of the National Academies of Science	全米科学アカデミーの全米研究評議会
NRCPR	National Research Council Peer Reviews	全米研究評議会ピアレビュー

NRL	Naval Research Lab	海軍研究所
NSA	National Security Agency	国家安全保障庁
NSF	Natinal Science Foundation	全米科学財団
NSTB	National SCADA Test Bed	国家 SCADA テストベッド
NSTC	National Science and Technology Council	国家科学技術評議会
NVLAP	National Voluntary Laboratory Accreditation Program	米国自主試験所認証
OAS	Organization of American States	米州機構
OCC	Open Cloud Consortium	オープン・クラウド・コンソーシアム
OCIO	Office of the Chief Information Officer	DHS S&T 最高情報責任者局
OMB	Office of Management and Budget	連邦行政予算管理局
OSD	Office of Secretary ogf Defense	国防長官室
OSDC	Open Science Data Cloud	オープン科学データ・クラウド
OSS	Open Source Software	オープンソースソフトウェア
OSTP	President's Office of Science and Technology Policy	大統領府科学技術政策室
PART	Program Assessment and Rating Tool	プログラム評価格付けツール
PCA	Program Component Area	プログラム・コンポーネント・エリア
PCAST	President's Council of Advisors onScience and Technology	大統領科学技術諮問委員会
PITAC	President' s Information Technology Advisory Committee	大統領情報技術諮問委員会
PNNL	Pacific Northwest National Laboratory	パシフィック・ノースウェスト国立研究所
PoLS SRN	Physics of Living Systems Student Research Network	生体物理学学生研究ネットワーク
PREDICT	Protected Repository for the Defense of Infrastructure Against Cyber Threats	-
PROCEED	Programming Computation on Encrypted Data	暗号データ・プログラミング・コンピュテーションプログラム
ResumeNet	Resilience and Survivability for Future Networking: ResumeNet	レジュームネット
RISCS	Center for Reliable Information Systems and Cyber Security	信頼できる情報システムとサイバーセキュリティ・センタ
RPI	Rensselaer Polytechnic Institute	米国レンセラー工科大学
SATC	Secure and Trustworthy Cyberspace Program	セキュアで信頼できるサイバースペース・プログラム
SAVI	Science Across Virtual Institutes	仮想研究所を横断する科学プログラム
SBIR	Small Business Innovation Research	NIST 中小企業技術革新研究プログラム
SCADA	Supervisory Control and Data Acquisition	-
SCORE IWG	Special Cyber Operation Research and Engineering Interagency Working Group	-

SDLC	Software Development Life Cycle	ソフトウェア開発ライフサイクル
SDO	Standards Development Organization	標準開発団体
SDP	Software Design and Productivity	ソフトウェア設計と生産性
SEL	Schweitzer Engineering Laboratory	シュバイツァー・エンジニアリング研究所
SEW	Social, Economic, and Workforce Implications of IT	社会、経済、及び労働力における IT
SGIP	Smart Grid Interoperability Panel	スマートグリッド相互運用性パネル
SIM	Sistema Interamericano de Metrology	南北アメリカ大陸計量システム
SOS	Securing the Open Softphone	セキュアリング・オープン・ソフトフォン
SPAR	Security and Privacy Assurance Research	セキュリティとプラバシー保証研究
SSCP	Secure SCADA Communications Protocol	セキュアな SCADA コミュニケーション・プロトコル
STAR Metrics	Science and Technology in America's Reinvestment – Measuring the Effect of Research on Innovation, Competitiveness and Science	米国の再投資における科学技術—イノベーション、競争力、科学に関する研究の効果測定
STEM	Science, Technology, Engineering and Mathematics	科学・技術・工学・数学
TC	Trustworthy Computing	信頼できるコンピューティングプログラム
TFAI	Task Force for American Innovation	アメリカ・イノベーション・タスクフォース
TTS	Tailored Trustworthy Spaces	特別に作った信頼できる空間
TVA	Topological Vulnerabily Analysis	位相脆弱性分析
UCB	University of California, Berkeley	カリフォルニア大学バークレー校
UCSB	University of California, Santa Barbara	カリフォリニア大学サンタバーバラ校
VA	Departmento of Veteran Affairs	退役軍人省
VCAT	Visiting Committee on Advanced Technology	先端技術に関する訪問委員会
VI-MSS	Virtual Institute of Microbial Stress and Survival	数学及び統計科学のための仮想研究所
VLMN	Variable Length Markov Models	可変長マルコフモデル
WiFiUS	Wireless Innovation Between Finland and the US	フィンランド／米国・ワイヤレス・イノベーション
3PAOs	third-party assessment organizations	第三者評価組織