アメリカ合衆国のネットワーク・サイバーセキュリティ分野における研究開発動向及び

連邦政府における IT 研究開発動向に関する調査

調査報告書

NICT ワシントン事務所

委託先　Washington｜CORE

2009 年 3 月

目 次

1. アメリカ合衆国におけるIT R&Dに関する予算および政策

「ネットワーキング及び情報技術プログラム（NITRD: Networking and Information Technology Program）」として知られる米国の情報通信技術研究開発（IT R&D）プログラムは、米国連邦政府における大規模な省庁横断型研究調整（リサーチ・コーディネーション）例の中でも、最も歴史が古いプログラムのひとつである。4 省庁間の非公式な調整プログラムとして 1980 年代末に開始され、1991 年に正式に設置された。当時は 8 機関が参加し、予算は約 6 億ドルだった。2008 年度は参加 13 機関に対し、総額約 33 億ドルの予算が割り当てられ、さらに関連国防活動（embedded defense activities）予算として、多額の資金が投資されている。2009 年度大統領予算要求額は、36 億ドルだった[1]。

IT R&Dは、オバマ政権においても優先事項とされており、連邦議会からも幅広い支持を受けている[2,3]。その結果、連邦政府における財政環境は非常に厳しいにもかかわらず、同プログラムへの投資額は 2007 年度から 2008 年度にかけて、約 13%増額されている[4]。2009 年度および 2010 年度の最終的な数値は、現時点ではまだ不明である。大半の連邦政府機関は現在、予算継続決議（H.R.2638）の下に運営されており、2009 年 3 月 6 日まで、プログラムとその予算額は 2008 年度と同水準とされている。連邦議会は現在、企業救済と景気対策法成立に追われており、2009 年度最終歳出予算案の準備が、ほとんど出来ていない状態である。関係者の多くは、連邦議会は予算継続決議を年内いっぱい延長し、結果的に 2009 年度歳出予算成立を見送ることになると予想している。

以下に、NITRD プログラムを理解する鍵となる、いくつかの政策及び計画文書を示す：

---

[1] FY 2009 Networking and Information Technology Research and Development: Supplement to the President's Budget, National Coordination Office for Networking and Information Technology Research and Development, February 2008

[2] Analytical Perspectives, Budget of the United States Government, Fiscal Year 2008, Office of Management and Budget, February 2007

[3] FY 2009 Administration Research and Development Budget Priorities, Office of Science and Technology Policy, August 2007

[4] FY 2008 Networking and Information Technology Research and Development: Supplement to the President's Budget, National Coordination Office for Networking and Information Technology Research and Development, August 2007

1. *連邦政府高度ネットワーキングR&D計画（The Federal Plan for Advanced Networking Research and Development）*[5]*:*

省庁横断型作業部隊（タスクフォース）が作成し、2008 年に発表されたこの計画は、向こう 10 年間にわたり、連邦政府のネットワーキング要件達成のために必要とされる包括的研究戦略を示したものである。ブロードバンド・ネットワーク展開において、米国が他国に遅れていることを問題視し、大統領科学技術政策室（OSTP: Office of Science and Technology Policy）の指示により作成された[6]。計画は、セキュアで信頼性があり、かつ相互運用可能なブロードバンド・ネットワークを開発するためのビジョンと戦略を提示する内容となっている。このビジョンを達成するための目標として、以下に示す 4 点が盛り込まれている。

目標 1. セキュアなネットワーク・サービスの提供

目標 2. セキュアなグローバル連携ネットワーク（global federated networks）の実現

目標 3. ネットワークの複雑性と不均一性（異質性）の管理

目標 4. 高度ネットワーク・システムと技術の開発を通じ、連邦政府、研究機関、民間企業、及びその他セクターにおけるイノベーションの促進

計画では、これら目標を達成するにあたり、複数の研究課題を克服する必要があると指摘した上で、現在の研究と、これら課題を克服するために必要とされる研究とを比較している。

2. *連邦政府サイバーセキュリティ・情報保証R&D計画（Federal Plan for Cyber Security and Information Assurance Research and Development）*[7]:

[5] Federal Plan for Advanced Networking Research and Development, National Science and Technology Council, September 2008

[6] OECD Broadband Statistics to June 2007, Organisation for Economic Co-operation and Development

[7] Federal Plan for Cyber Security and Information Assurance Research and Development, National Science and Technology Council, April 2006

省庁横断型グループが作成し、2006 年に発表されたこの計画は、同分野の研究を IT R&D ポートフォリオに組み込ませるとともに、全体的な調整プロセスに複数の機関や局を追加する内容となっている。サイバーセキュリティと情報保証は今や、同プログラムにおいて投資額が 5 番目に大きいカテゴリーである。

3. *「挑戦を受けるリーダーシップ」－競争社会における情報技術R&D (Leadership Under Challenge: Information Technology R&D in a Competitive World)*[8] *:*

大統領科学技術諮問委員会(PCAST: President's Council of Advisors on Science and Technology)が作成し、2007 年 8 月に発表されたこの文書は、NITRD プログラムを評価したものである。現在の連邦 IT R&D を概ね支持する一方で、小規模で短期的、かつ調整力に乏しいプログラムが多すぎる点を批判し、長期的で規模が大きく、かつ分野横断的で先見性のある R&D を推進している。また、そのためには計画と調整フレームワークの見直しが必要であると指摘し、IT 分野の優秀な学生の獲得と訓練を強化する必要性を強調した。各省庁は現在、PCAST の提言に応える計画を作成中であり、一般から意見を求めるとともに、それら計画への幅広いインプットを集める目的で、会合も開催している。

4. *2009 年度政権R&D 予算優先事項(FY 2009 Administration Research and Development Budget Priorities)*[9] :

行政予算管理局(OMB: Office of Management and Budget)と、OSTP の各局長が作成し、2007 年 8 月に発表されたこの文書は、政権の優先事項として IT R&D の重要性を強調する内容となっている。参加機関に対し、IT R&D 投資優先順位の決定にあたり、PCAST による提言(前掲)を考慮することを求めている。また、連邦政府高度ネットワーキング R&D 計画(前掲)を完成させるとともに、ネットワーク研究投資の優先順位決定において、本計画を利用することを要求している。

総合政策に関しては、プログラムは近年の傾向を踏襲し、IT R&D 分野の中でも技術領域を継続して重視する内容となっている。

---

[8] Leadership Under Challenge: Information Technology R&D in a Competitive World, President's Council of Advisors on Science and Technology, August 2007

[9] FY 2009 Administration Research and Development Budget Priorities, op. cit.

- ハイエンド・コンピューティング・システム開発と初期導入を含む、サイバーインフラ
- 全光ネットワーキングとグリッド・コンピューティングを含む、高度ネットワーキング技術とアプリケーション
- サイバーセキュリティとテロ対策アプリケーション

2007 年に発表された PCAST による NITRD イニチアチブのレビュー結果を受けて、NITRD の国家調整事務局（National Coordinating Office）は、プログラムの新たな戦略計画作成に着手した。2009 年 2 月末には、IT 分野の著名な研究者を招聘してワシントン DC でワークショップを開催し、計画内容についてインプットを求めている。ワークショップでは、NITRD 参加機関の代表者がこれら専門家の議論や提言に耳を傾けた。連邦 IT R&D の今後の注力領域として、候補に挙がった開発中の主要テーマの一部を以下に紹介する。

- *次世代認知（Emergent Cognition）：* サイバー環境、人間の知能、及び社会的能力を統合することで、可能となる新たな知性、直覚、認知力の活用に向けた研究テーマ。具体的には、例えば、モデリングや、研究者による高度な分析、さらに分散型決定プロセスを組み合わせることで、複雑現象に対する分析精度の改善を目指すような研究が挙げられる。
- *超仮想（Beyond Virtual）：* 仮想世界と現実世界を融合することで、新たな事象発見や実現を可能に、生活の質を向上させるような研究テーマ。この領域の研究には、サイバーフィジカル・システム、オブジェクト志向ネットワーキングとコネクティビティ、及びバイオ・サイバー・インターフェースに関するものが含まれる。
- *信頼・確信（Trust and Confidence）:* サイバー・システムがもたらす価値の社会的保証は、信頼・確信が明示されて初めて可能であり、データとリソース（資源）が、本来意図する目的のためのみに使用されることが保証される必要がある。この領域の研究には、ID 管理、情報セキュリティ、プライバシー保護、段階的アクセス制限、暗号化、及びトラステッド・システムに関するものが含まれる。

新戦略計画の発行期限は設定されていないが、ワークショップで行われた議論は、個々の機関における IT R&D 投資先に関する差し迫った決定と、長期的意思決定の両方に影響を与えるものと思われる。

1.1 2009 年度IT R&D連邦予算概要

通常であれば、大統領予算要求は 2 月第 1 週に連邦議会に提出されるが、2009 年は状況が異なっており、中でも異例と見なされる 4 項目を以下に示す。

1. 2008 年夏、連邦議会は 2009 年度連邦予算をめぐる重要な審議を行っている。争点の多くは、イラクとアフガニスタンにおける戦費捻出方法についてである。結果、連邦議会は 2008 年 9 月、「2009 年統合セキュリティ・災害援助・継続歳出予算法（Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009）」[10]を可決した。同法によって、国防総省（Departments of Defense）, 国土安全保障省（Department of Homeland Security）、及び退役軍人省（Department of Veterans Affairs）の一般歳出予算が成立したが、残りの省庁については、2009 年 3 月 6 日まで暫定予算継続決議下に置かれることになった。予算継続決議によって、対象省庁のプログラムや予算は、2008 年度水準に据え置かれた。これを受け、新規プログラムの開始は不可能となり、新しい可能性や課題に対処するために、研究活動を調整することも出来なくなっている。

2. 2008 年秋頃には、連邦議会は金融市場危機や景気後退対策に追われるようになった。金融セクターに資金を拠出する「金融安定化法案（TARP: Troubled Asset Relief Program）」と、後に成立した「景気対策法（American Recovery and Reinvestment Act, the “Stimulus Act”）」の審議の陰に隠れる形で、2009 年度予算の検討は、完全に後回しにされた。その結果、連邦議会は 2009 年度非軍事関連予算について、全て 2008 年度と同水準にすることを決めている。

3. 連邦議会での景気対策法成立を受けて、民主党（2008 年 11 月の選挙において上下両院で多数議席を獲得）は、2009 年 9 月 30 日締めの 2009 年度予算審議の再開を決定した。審議に最低 1 ヶ月を要すると仮定した場合（上下両院での採決、及び両院合同会議での妥協案模索を含む）、一部省庁機関では、4 月中に 2009 年度歳出予算増額が決まる可能性がある。言換すれば、大方の省庁機関では、追加予算に基づく助成金供与や契約締結ができるまで、6 ヶ月を要することになる。

[10] Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009 (P.L. 110-329)

4. 大統領選挙と、それに続くオバマ政権誕生までの移行プロセスがあったことを考慮すると、大統領府が正式な 2010 年度予算案を、例年通り 2009 年 2 月初旬までに作成するのは不可能であったといえる。また、景気対策法をめぐる駆け引きが、そのプロセスをさらに困難なものにした。結果、行政予算管理局は 2009 年 2 月 26 日、2010 年度大統領予算要求の骨子のみを発表している[11]。

現在の 2009 年度予算案は、連邦議会で審議されている最中だが、2009 年 2 月に成立した景気対策法には、国立衛生研究所（NIH: National Institute of Health）、国立標準規格技術院（NIST: National Institute of Standards and Technology）、米海洋大気庁（NOAA: National Oceanic and Atmospheric Administration）、米航空宇宙局（NASA: National Aeronautics and Space Administration）、全米科学財団（NSF: National Science Foundation）、及びエネルギー省（DOE: Department of Energy）に対する研究予算の大幅増額が盛り込まれた。同法に添付された報告の中で、科学研究のためのスーパーコンピュータ調達を具体的に要求している。詳細不明の研究予算の一部は、IT プログラムに当てられるものと考えられる。この景気対策法の詳細については、本報告において後述した。なお、景気対策法で定められた予算は、2010 年度に限らず、2009 年度末から 2011 年度にかけた 2 年間に歳出される予定である。

当初から期待されたブロードバンド･インターネット政策の見直し、及び連邦助成金増額も、景気対策法に盛り込まれた。景気対策法に基づく資金拠出は、以下に示す 2 通りの方法で IT R&D 分野に影響を与えると思われる:

1. 第一に、景気対策法には、ブロードバンド・インターネット・サービスの全米展開を加速するための財政支援計画が含まれており、ソフトウェアとサービスに関する新たな市場需要を喚起すると考えられる。

2. 第二に、NIST、DOE、NSA を含む、IT R&D 実施研究機関に対する予算が追加される。

[11] “A New Era of Responsibility,” Office of Management & Budget, Executive Office of the President, 26 February 2009.

景気対策法に IT が含まれたことは、ブッシュ政権と比較して、科学と技術をより重視するオバマ政権の姿勢と一貫している。(この姿勢は、大統領科学・技術顧問として John Holdren 氏が早々に指名されたことからも伺える。)一方、2009 年度と 2010 年度は膨大な財政赤字が見込まれており、オバマ大統領は、不必要な支出の保留を求める強い圧力を受けている。そのため、次のセクションで触れる具体的な動きのほとんどは、来年、あるいは向こう 2 年間の米国連邦政府による IT R&D 予算増額の可能性を楽観視する内容となっているが、仮に景気後退と連邦財政赤字の拡大が今後継続した場合、現実はかなり異なる可能性も残されている。

2009 年 2 月 23 日、連邦下院議会は H.R.1105 として知られる「2009 年歳出予算法(Omnibus Appropriations Act of 2009)」を可決した。この法律は、2009 年度、つまり 2008 年 10 月から 2009 年 9 月までの期間に遡って予算を付与するものである。民主党議員は、上下両院で過半数議席を獲得したことを武器に、ブッシュ政権が 2008 年 2 月に提出した予算案とは大きく異なる 2009 年度予算を作成した。なかでも同予算法案では、NIST、NOAA、及び DOE を含む、科学研究に従事する複数機関への大幅な予算増額が盛り込まれた。同予算法案に含まれた科学関連予算のほとんどは、気候変動と環境研究に対してであるが、これらプログラムには、情報技術への多大な新規投資を必要とする要素(気候モデリングなど)が含まれる。

新政権の影響

オバマ大統領就任から激動の数週間が過ぎたばかりの現時点で、研究予算とプログラム、特に NITRD プログラムの詳細に対する新政権の影響を査定するのは、時期尚早といえる。しかし、オバマ大統領の声明や行動の一部からは、大統領が国家経済の将来に対する技術の重要性を理解し、その中心的役割を担う IT 研究を評価していることが伺える。

選挙期間中にオバマ大統領が技術の重要性に関して出した声明は、現在は新政権のアジェンダの一部に盛り込まれている[12]。 声明の中でオバマ大統領は、様々な知的活動の完全かつ自由な交換を保証するオープン·インターネットの重要性を強調し、有線・無線の次世代ブロードバンド・ネットワーク展開を支持している。また、向こう 10 年にわたる連邦基礎研究予算の倍増、大学における研究イニチアチブの拡張、そして科学的根拠が最も明確な証拠に基づく政府の意思決定を徹底することにより、米国の競争力向上を呼びかけている。

[12] The Agenda: Technology, Office of the President, 2009

オバマ大統領が最初に行った主要な政権人事の中には、いくつかの科学技術関連職も含まれており、同領域政府ポスト任命としては、異例の早さと言える。具体的には、昨年 12 月、大統領就任が決まったオバマ氏は、ノーベル賞受賞者であるSteven Chu氏をエネルギー長官に指名する意向を明らかにした点。さらに、ハーバード大学の著名教授であるJohn Holdren氏を科学顧問と科学技術政策室（OSTP: Office Science and Technology Policy）室長に、そして気候学者のJane Lubchenco氏を米国海洋大気庁（NOAA: National Oceanic and Atmospheric Administration）長官に選んだことからも伺える。これらの発表にあたりオバマ大統領は、「惑星としての我々の生存と、国家としての我々のセキュリティと繁栄にとって、科学は今日、かつていないほど重要な鍵を握っている。科学を、再び我々の最優先課題とする時が来た（中略）科学と技術分野における世界的リーダーとしてのアメリカの立場を取り戻すために努力する」[13]と述べている。

オバマ政権はまた、NASA に対する管理も強く主張しており、有人宇宙飛行と月面再上陸を重視したブッシュ政権の方針を再考し、気候研究を支援するためとして、地球科学プログラムへの資金分配を増やす可能性が伺える。この影響を受けてか、Michael Griffin 長官は 1 月 20 日に、同ポストを辞職している。

オバマ大統領による景気対策法では、科学・技術分野に 499 億ドルの予算が分配される[14]。そのうち最大シェアの 300 億ドルは、エネルギー効率と再生可能なエネルギーに対してだが、残りのほとんどは、「米国競争法（America COMPETES Act）[15]」の内容に即した形で分配される。景気対策法は、NIST、NOAA、NASA、NSF、DOE、そしてNIHに対する研究予算を増加させている。IT関連のプログラムとして特に言及されたものの中には、ブロードバンド・ネットワーキング、スーパーコンピューティング、気候、再生可能エネルギー、及び医療ITが含まれる。

---

[13] The Guardian, Sunday December 21, 2008

[14] R&D Funding Components of the American Recovery & Reinvestment Act of 2009, Alliance for Science and Technology Research in America, February 2009

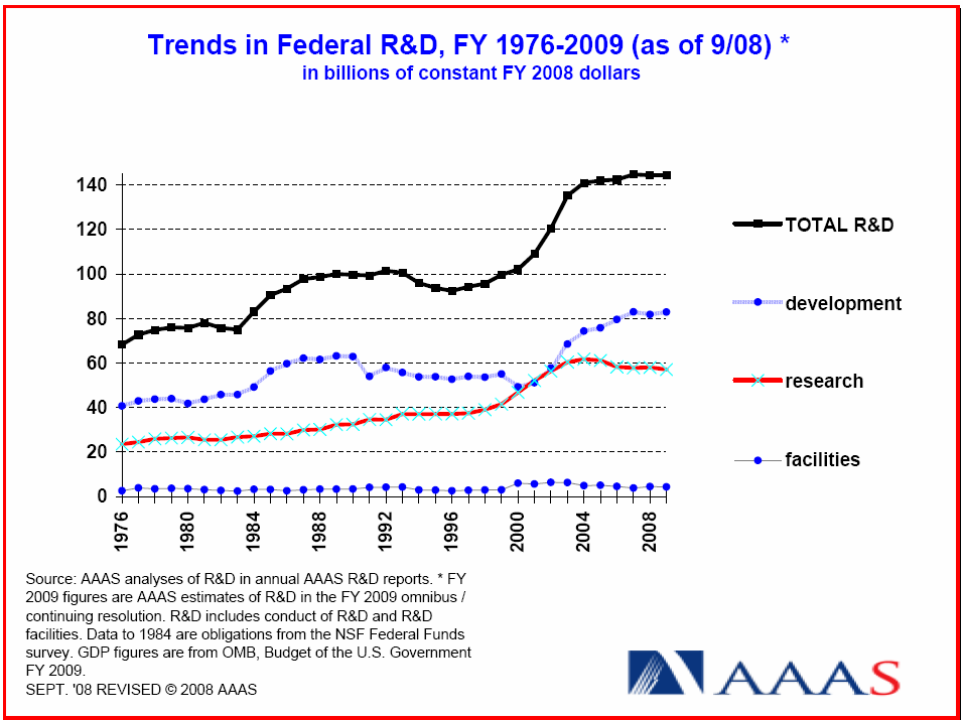
[15] America COMPETES Act, P.L. 110-69, August 2007

総合すれば、これら初期のアクションは、前政権と比較して、新政権が科学技術研究開発分野に大いに注目していることを示唆している。とりわけ科学技術分野に 499 億ドルを割当てる景気対策法は、新政権の決断を際立たせるものである。3 月 6 日以降に連邦議会が 2009 年度予算審議を開始し、長期的に 2010 年度予算に関する審議も始まれば、連邦政府助成研究、特に IT 研究の将来像はさらに具体化してくるものと思われる。

連邦R&D予算の歴史的解析と2009 年度歳出予算（景気対策法成立前）

1976～2009 年度の連邦 R&D 予算における全体的傾向を図 1 に示す。2009 年度は暫定予算の継続決議が可決されていることから、予算総額は 2008 年度から 2009 年度にかけてほぼ横並びとなっている。景気対策法によって R&D 予算総額は 15%程度増加すると推定されるが、図 1 にその影響は反映されていない。

図 1:1976～2009 年度 連邦R&D予算推移[16]

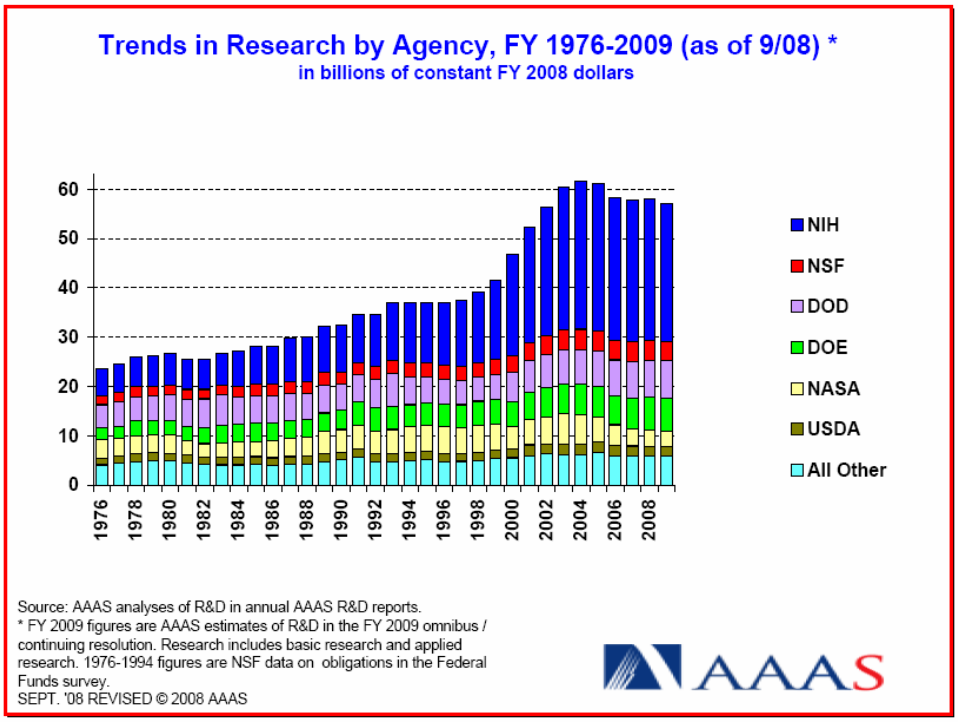


出典: AAAS, September, 2008

[16] Trends in Federal R&D, FY 1976-2009, AAAS, September 2008

図 2 は、景気対策法成立以前の最大手研究機関を対象とする連邦 R&D 予算の推移を示したものである。予算継続決議を受けて、ほとんどの機関で 2009 年度予算は前年度並みとなっている。

図 2：1976～2009 年度 省庁機関別連邦R&D予算推移[17]



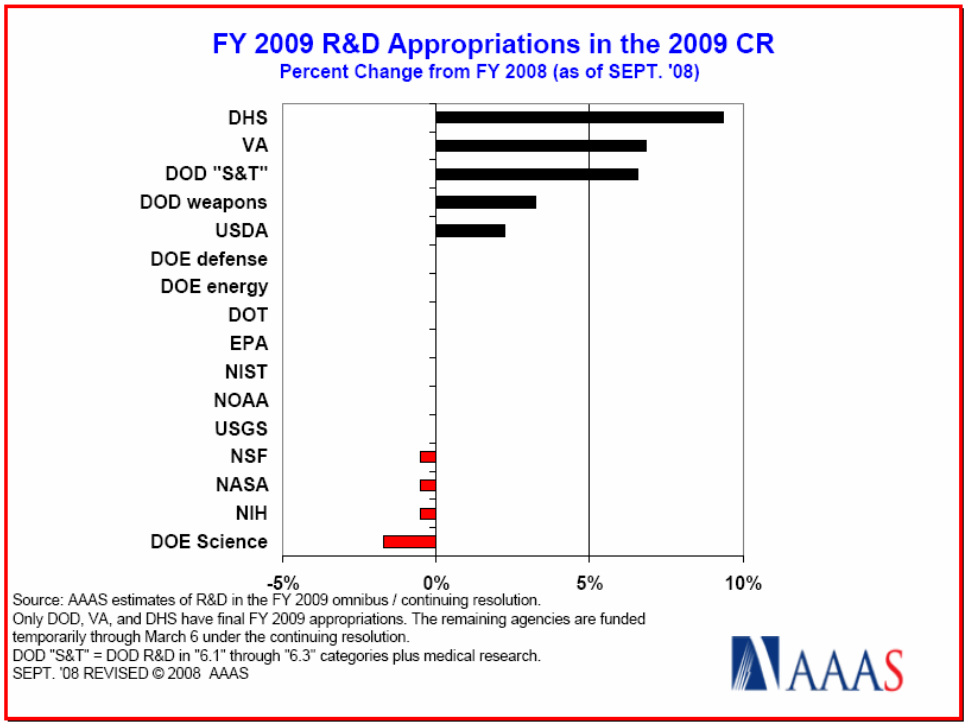
出典: AAAS, January 8, 2008

しかし、比較対象を R&D 実施機関全体に広げると、小さいながらも、差異が浮かび上がってくる。図 3 は、機関別に R&D 予算配分額の伸長率（%）を示したものである。2009 年度歳出予算が確定した DHS、退役軍人省（Department of Veterans Affairs）、そして国防総省（Department of Defense）では、R&D 予算が大幅に増加したことが分かる。予算継続決議は、一般歳出予算のみを対象としているため、追加予算割り当てを受けた NIH や DOE などの機関は、2008 年度よりも少ない予算で 2009 年度を迎えている。

[17] Trends in Federal R&D, FY 1976-2009, AAAS, September 2008

2009 年度予算継続決議の下、連邦政府 R&D ポートフォリオの予算総額は 1,473 億ドルに達し、前年度から 29 億ドルの増加となっている。増加分はほぼ全て、DoD R&D 予算の大幅増額によるものである。

図 3:2009 年度 省庁機関別連邦R&D予算[18]



出典: AAAS, January 8, 2008

2008 年度歳出予算の機関別分析の他に、機能的観点からの考察も有益と思われる。次のセクションでは、予算配分を精査するとともに、2009 年度予算継続決議において重視されることが予想される具体的な研究トピックを取り上げる。

[18] U.S. Federal Spending by Agency, FY2009, AAAS, September 2008.

2009 年度継続予算審議に関する機能別分析

大統領交代にもかかわらず、ブッシュ前政権が作成した覚書「2009 年度R&D予算優先事項（FY 2009 Administration Research and Development Budget Priorities）」は、本予算年度においてもR&D方向性に影響を与えている[19]。オバマ大統領は、超党派的支持を集めていることから、米国競争法の施行を予算内で推進してくることが予想される。それ以外では、複数の省庁横断型プログラムが引き続き最優先となっている。優先プログラムの例を以下に示す:

- 高度ネットワーキング情報技術（Advanced Networking and Information Technology）
- 国土安全保障と国家防衛（Homeland Security and National Defense）
- エネルギーと気候変動技術（Energy and Climate Change Technology）
- 国家ナノテクノロジー・イニシアチブ（NNI: National Nanotechnology Initiative）
- 複雑生態系の解明（Understanding Complex Biological Systems）
- 気候変動を含む環境（Environment Including Climate Change）

以下のセクションでは、歳出予算の現状、IT R&D を含む政府優先分野に対する予算総額、及び NITRD プログラムの予算について述べることとする。

2009 年度連邦IT R&D予算の分析

予算継続決議が可決され、さらに景気対策法の影響が不透明な現状を考慮すると、2009 年度の最終的な連邦 IT R&D 予算を推測するのは難しい。表 1 は、DoD の 2009 年度歳出予算、及び予算継続決議下にある他機関の暫定予算をベースに、景気対策法成立以前の予算を機関別に示したものである。不確定要素があることから、数値はあくまで概算である。

[19] FY 2009 Administration Research and Development Budget Priorities, op.cit

表 1:2008～2009 年度 機関別NITRD予算[20]

NITRD 参加機関	*2008 年度 推定 (100 万ドル)*	*2009 年度 推定 (100 万ドル)*	*伸長率 (%)*
国防総省(Defense)	1,267	1,242	-2
全米科学財団(National Science Foundation)	931	931	0
保健社会福祉省(Health and Human Services)	556	556	0
エネルギー省(Energy)	436	436	0
商務省(Commerce)	85	85	0
米航空宇宙局(National Aeronautics and Space Administration)	86	86	0
環境保護庁(Environmental Protection Agency)	6	6	0
国立公文書館(National Archives and Records Administration)	5	5	0
合計	**3,372**	**3,347**	-1

出典： President's FY 2009 Budget Request, February 2008 and FY 2009 Continuing Resolution, September 2008

NITRD 2008 年度予算と 2007 年度予算(機能分野別)

NITRD プログラムにおいては、各機能分野はプログラム・コンポーネント・エリア(PCA: Program Component Areas)と呼ばれる。PCA レベルの 2009 年度予算配分額に関するデータは、公開されていない。しかし、NITRD 国家調整事務局(National Coordination Office)が報告した 2008 年度及び 2009 年度大統領予算要求に記載された 2007 年度及び 2008 年度の PCA 別予算内訳からは、その傾向の一端を垣間見ることが出来る。また、2008 年度予算は、2009 年度予算とほぼ同額であると考えられる(景気対策法成立以前)。表 2 は、2007 年度及び 2008 年度の予算推定額を、伸長率とともに示したものである。

[20] President's FY 2009 Budget Request, Analytical Perspectives, February 2008

表 2:2007～2008 年度PCA別NITRD予算(推定)[21]

PCA	*2007 年度 推定 (100 万ドル)*	*2008 年度 推定 (100 万ドル)*	*伸長率 (%)*
ハイエンド・コンピューティング・インフラとアプリケーション(HEC I&A: High End Computing Infrastructure & Applications)	971.2	1044.1	7.5
ハイエンド・コンピューティング R&D (HEC R&D: High End Computing Research & Development)	279.7	450.4	61.0
サイバーセキュリティと情報保証 (CSIA: Cyber Security & Information Assurance)	212.6	268.7	26.4
ヒューマン-コンピュータ・インタラクションと情報管理 (HCI & IM: Human-Computer Interaction & Information Management)	784.0	798.5	1.8
大規模ネットワーキング (LSN: Large Scale Networking)	384.6	462.4	20.2
ハイコンフィデンス・ソフトウェアとシステム (HCSS: High Confidence Software & Systems)	149.4	124.8	-16.5
IT に関する社会・経済・労働力問題 (SEW: Social, Economic, & Workforce Implications of IT)	113.6	118.7	4.5
ソフトウェア設計と生産性 (SDP: Software Design & Productivity)	71.9	73.3	1.9
合計	**2967.0**	**3340.9**	**12.6**

出典: President's FY 2008 and FY 2009 Budget Requests

HEC I&A PCA 予算は主に、NSF、DoD、DOE、NASA を含む省庁機関による、ペタスケール及びその他大型コンピュータ調達のためである。他にも、システムの管理及び測定のためのソフトウェア開発、及び大型コンピュータにおけるアプリケーション開発環境のために予算は分配される。

[21] Networking and Information Technology Research and Development: FY 2008 Supplement to the President's FY 2008 Budget, op. cit.

HEC R&D は、ハイエンド・コンピューティング・アーキテクチャ、ハードウェア、及びソフトウェア開発研究を目的としている。本領域の予算は、NSF、DoD、そして NIH に対する予算増額を反映し、61％増と大幅に伸長した。これらの増額は、「連邦政府ハイエンド・コンピューティング計画（Federal Plan for High-End Computing）」における要求を受け、本領域における研究を立て直す必要があるとの認識に応えたものである。優先項目には、コンピュータ・システム・プロトタイプ、アーキテクチャ、プログラミング、ペタスケール・コンピューティングにおける課題、及び量子コンピューティングが含まれる。

CISA には、セキュリティ、保証、及びコンピュータ・システムとネットワークにおける信頼性改善のために必要とされる技術研究が含まれる。本領域の予算は、主に DoD と NIST の予算増額の結果、26%と大幅に増額された。優先項目は、よりセキュアなネットワークとコンピュータ・アーキテクチャ、ソフトウェア保護、ネットワーク防衛、プライバシーなどである。

LSN は 20%成長を記録したが、これは主に、無線及びアド・ホック・ネットワーキング研究を支援する DARPA 研究予算の増額を反映したものである。優先項目としては他に、ダイナミック光ネットワークと、ネットワーク・テストベッドが挙げられる。

表 2 にみられる比較的小さな変化は、大統領予算教書において記述されている。

NITRD 2008 年度予算と 2007 年度予算（機関別）

- ***国防総省（DoD: Department of Defense）***

DoD は、「陸軍未来戦闘システム（Army's Future Combat Systems）」や、「汎 DoD ネット中心型機能ポートフォリオ（DoD-wide Net-Centric Capability Portfolio）」などのプログラムを通じ、戦力多重増強要員（a force multiplier）として IT をけん引している。DoD のネットワークは近年、東欧やアジアに設置されたサーバーから、深刻なサイバー侵入を数回にわたり受けており、サイバーセキュリティは今や、DoD において非常に重要な課題となっている。それを受けて DoD は、主に DARPA を通じ、サイバーセキュリティ分野に多大な投資を行なっている。近年では、短期的かつ概して機密扱いとされる企業ベースのプロジェクトに対し、DAPRA 局長はサイバーセキュリティ R&D 予算を集中させてきた。その結果、大学の研究助成が大幅に削減され、削減分の僅か一部が NSF 予算の増額分が補填する形となっている。DARPA は、モバイル展開を支援するため、無線及びアド・ホック・ネットワーキング技術研究にも資金を拠出している。2008 年度は、DARPA の「高生産性コンピューティング・システム（HPCS: High Productivity Computing Systems）イニシアチブ」の最終年でもあった。HPCS では、NSF や DOE をはじめとする省庁機関と協力し、ペタスケール・システムの導入を目指した。また、高性能コンピュータ近代化局（HPCMO: High Performance Computer Modernization Office）を通じ、DoD は科学・工学研究に従事する大規模コンピュータ関連施設を支援している。2008 年度には、HPCMO はこれらシステムの一部をアップグレードしている。NSA は、自らの具体的なニーズを満たすために、ハイエンド・コンピュータ開発とその他 IT を積極的に支持している。DoD の 2008 年度 NITRD プログラム総予算は、12 億 5,000 万ドルとなっている。

- ***エネルギー省（Department of Energy）***

エネルギー省科学局（SC: Office of Science）は、主に高度科学コンピューティング研究（ASCR: Advanced Scientific Computing Research）局を通じ、IT R&D 分野で重要な役割を担っている。同局は科学シミュレーションの主要推進派であり、DOE 参加の他局と連携し、研究におけるシミュレーション利用の推進を図っている。SC は複数の科学コンピューティング・センターと ES ネット・データ・ネットワークを管理している。オークリッジ国立研究所では、クレイ（Cray）基盤のリーダーシップ・システム（Leadership system）が、期待されていたペタフロップ（petaFLOPS）水準を昨年達成した。SC はこの一環として、DARPA の HPCS プログラムと連携体制を築いている。ASCR は、重要な応用数学とコンピュータ科学プログラムを支援しており、さらに、グリッド・コンピューティングとその他データ集約型アプリケーションを支えるためのネットワーキング研究を行っている。

2008 年度には、DOE の核エネルギー局（Offices of Nuclear Energy）及び化石エネルギー局（Offices of Fossil Energy）が、主に原子炉と化石燃料システムに関するシミュレーション作業のために、NITRD プログラムに参加した。DOE/SE、DOE/NE、及び DOE/FS の 2008 年度予算は、合計 4 億 760 万ドルである。

DOE の国家核安全保障局（NNSA: National Nuclear Security Administration）は、その活動のほとんどが機密扱いであるが、IT R&D 分野における重要なプレイヤーである。というのも、核実験全面禁止条約（Comprehensive Test Ban Treaty）の結果、今やシミュレーションは、核保有量を維持するための主要ツールだからである。「戦略コンピューティング促進イニシアチブ（ASCI: Accelerated Strategic Computing Initiative）」は、核実験を、膨大な計算で置き換えるという目標を掲げている。ASCI とその後継プログラムである「高度シミュレーションとコンピューティング（Advanced Simulation and Computing）」は、IBM をはじめ、SGI、HP といった企業に資金を提供し、世界最強コンピュータ開発を支援している。これらの活動は、物理学シミュレーションに必要となる 3D コードの開発を目指す、複数年ソフトウェア・プロジェクトに支えられている。今日、世界で最も能力が高いとされるスーパーコンピュータは、1.105 ペタフロップス（petaFLOPS）の処理能力を有す、ロス・アラモス国立研究所（Los Alamos National Laboratory）に設置された「ロードランナー（Roadrunner）」システムである。興味深いことに、このコンピュータは、主に Sony のプレイステーション（Play Station）に使われる IBM/Sony のセル（Cell）プロセッサーと、伝統的なスーパーコンピュータ向けプロセッサーである AMD のオプテロン（Opteron）プロセッサーを合体させたものとなっている。DOE/NNSA 予算は 2,830 万ドルとなっている。

➢ *全米科学財団（NSF: National Science Foundation）*

NSFは、政府内で最大かつ最も多角的なITプログラムの一つを支援している。その投資対象は、ハイエンド・コンピューティング・ハードウェアとソフトウェア研究にはじまり、複数のハイエンド・コンピューティング・センターの管理や、中核的コンピュータ科学とコンピュータ工学研究、科学工学分野でのIT利用に関する広範な研究に至る。2008 年、NSFは「サイバー対応ディスカバリーとイノベーション・イニシアチブ（CDI: Cyber-enabled Discovery and Innovation Initiative）」を開始した。NSF全体で取り組むプロジェクトであり、初年度予算は 4,790 万ドルで、向こう 4 年間に毎年同程度の増額が見込まれている。CDIは、非常に広範、かつ野心的な目標を掲げており[22]、その成功は、仮に部分的であってもR&Dに多大な影響を及ぼす可能性がある。2008 年には、テネシー大学（University of Tennessee）とイリノイ大学（University of Illinois）における超大型コンピュータ・システム研究に助成した。テネシー大学に対しては、オークリッジ国立研究所に収納されるペタスケール級スーパーコンピュータの開発と 5 年間の運用予算として、6,500 万ドルを拠出した。イリノイ大学は、IBMが構築したペタスケール級コンピュータに対し、2 億 800 万ドルの助成金を獲得した。2008 年度は、NSFに分配されたNITRD予算は 9 億 3,150 万ドルだった。

➢ *国立標準規格技術院（NIST: National Institute of Standards and Technology）*

NISTでは、主に 2 つの研究所がIT R&Dに関与している。そのうちの一つ、IT研究所（ITL: Information Technology Laboratory）は、数学／計算科学をはじめ、コンピュータ・セキュリティ、ソフトウェア診断と適合試験、高度ネットワーキング、情報アクセス、そして統計工学などの分野におけるプログラムを展開している。NISTは近年、サイバーセキュリティに関する汎連邦政府標準規格の開発、発布、維持において、重要な役割を担っている。現在は、非軍事関連の全連邦政府機関を対象に、これら標準への準拠が法律で定められている。もう一方の電気電子工学研究所（EEEL: Electronics and Electrical Engineering Laboratory）では、マイクロエレクトロニクス、オプトエレクトロニクス、半導体、そして電磁気学を含む、高度IT機器開発に寄与する技術の研究が行われている。2008 年度のNISTのNITRD予算は 6,200 万ドルであった。

[22] Fact Sheet: Cyber-enabled Discovery and Innovation, NSF, February 2007

1.2 2009 年度IT R&D 予算傾向

予算継続決議が可決されたことを受けて、2008 年度から 2009 年度では、IT 予算やプログラムには、ほとんど変化がなかった。景気対策法が成立したことで、IT 予算は大幅に増額されるが、早くても各省庁が詳細な計画を作成、提出する期間として法律で設けられた 90 日間が経過するまでは、実際の予算がいくらになるかを伺い知ることはできない。増額幅は、最大 10 億ドルに達する可能性がある。

連邦議会は、大統領選挙の結果を待つ間、予算継続決議を成立させて 2009 年度予算への対応を遅らせた。その結果、ほとんどのプログラムの予算は、少なくとも 2009 年 3 月までは 2008 年度水準に据え置かれる。米国が他国に遅れをとるといった恐怖や、2007 年米国競争法（P.L 110-69）の予算獲得失敗に対する失望が、研究及びビジネス・コミュニティの中にあるにもかかわらず、連邦議会は 2010 年度予算まで、R&D について実質的行動は何も起こさないとみられる。

景気刺激策（Economic Stimulus）

経済の急速な悪化と 2008 年秋に起きた金融市場崩壊は当時、ブッシュ前大統領、そしてオバマ新大統領に対し、1 兆ドルを超える規模の徹底的な救済及び経済活性化措置の提案を強いたともいえる。この法律の目玉として注目されるのが、最近連邦議会を通過した景気対策法である「2009 年米国再生・再投資法（American Recovery and Reinvestment Act of 2009）[23]」である。同法は連邦議会によって可決され、オバマ大統領が 2009 年 2 月 12 日に署名して成立した。支出予算は総額 7,890 億ドルであり、その大半が今後 2 年間に拠出される。

連邦議会の R&D に対する見解を理解するには、同法の R&D 条項を分析する必要がある。忘れてならないのは、オバマ大統領が超党派支持を得ようと努力したにも関わらず、共和党議員の中から賛成票を投じたのは、上下両院から上院議員 3 名だけだったという点である。つまり、“連邦議会の見解”は、実質的には民主党議員の見解に過ぎないともいえる。共和党は、約 5,000 億ドル規模の減税実施と、場合によっては追加で小額の財政支出による経済再生を目指していた。

[23] American Recovery and Reinvestment Act of 2009, Wikipedia, 2009

同法に盛り込まれたR&D予算総額は、その定義を何とするかによって異なる。同法について分析した 2 件の信頼に値する報告は、予算総額をそれぞれ 499 億ドル[24]と 215 億ドル[25]と試算している。金額に大きな差があるのは、前者には 266 億ドル規模のエネルギー技術プログラム予算が含まれているからである。また、財政支出は、機関によっては 2009 年度と 2010 年度にまたがる形で行われる予定で、分析をさらに複雑にする結果となっている。

表 3 は、現在入手可能な情報を基に、景気対策法に盛り込まれた研究予算の推定総額（IT 予算に限らない）を、（全 R&D 実施機関ではなく）NITRD プログラム参加機関ごとに示したものである。

表 3: 景気対策法に盛り込まれた研究予算（NITRD プログラム参加機関別）

機関	*100 万ドル*
国立標準規格技術院（National Institute for Standards and Technology）	600
米航空宇宙局（National Aeronautics and Space Administration）	1,002
全米科学財団（National Science Foundation）	3,502
エネルギー省科学局（Department of Energy, Office of Science）	2,000
国立衛生研究所（National Institutes of Health）	10,000
合計	**17,104**

出典: American Recovery & Reinvestment Act of 2009

表 3 に示した金額のうち、IT 研究予算だけを推定するのは、現時点では不可能である。しかし、連邦研究予算に占める IT R&D 研究の割合が 10%をわずかに切る程度であることを考慮すれば、予算継続決議の有効期間が切れた後、IT 予算が 10 億ドル以上増額される可能性は大いにある。これほどの規模の IT 予算増額を支える汎政府 R&D 優先項目には、気候モデリング、再生可能エネルギー、医療 IT、及び高度ネットワーキングが含まれる。

[24] R&D Funding Components of the American Recovery & Reinvestment Act of 2009, Alliance for Science & Technology Research in America, February 14, 2009

[25] AAAS Analysis of R&D in FY 2009 Stimulus Appropriations, American Association of Arts and Sciences, February 12, 2009

これら優先事項の予算目安は、景気対策法における科学・技術総合予算によって示されている。表 4 は、これら予算推定額を示したものである。なお、表 4 に示す金額には、表 3 で示した金額が含まれる。

表 4:景気対策法に盛り込まれた科学・技術研究予算(機関別)

機関	*100 万ドル*
米国電気通信情報庁(National Telecommunications and Information Administration)	5,350
国立標準規格技術院(National Institute of Standards and Technology)	600
米国海洋大気局(National Oceanographic & Atmospheric Administration)	836
米航空宇宙局(National Aeronautics and Space Administration)	1,002
全米科学財団(National Science Foundation)	3,502
エネルギー省: エネルギープログラム(Department of Energy: Energy Programs)	26,583
エネルギー省: 科学プログラム(Department of Energy: Science Programs)	2,000
保健社会福祉省(国立衛生研究所) (Health and Human Services, National Institutes of Health)	10,000
合計	**49,873**

出典: FY 2009 Economic Stimulus Package

「2009 年歳出予算法(Omnibus Appropriations Act of 2009)」では、景気対策法の対象とされなかった科学機関に対しても、予算増額を提案している。しかし、ここでもこれら増額分のうち、いくらが IT R&D に分配されるかは分からない。

表 5:2009 年度 科学・技術予算案ー増額幅(機関別)

機関	*100 万ドル*
国立標準規格技術院(National Institute of Standards and Technology)	$819
米国海洋大気局(National Oceanographic & Atmospheric Administration)	469
米航空宇宙局(National Aeronautics and Space Administration)	385
全米科学財団(National Science Foundation)	363
エネルギー省: 科学プログラム(Department of Energy: Science Programs)	755
保健社会福祉省(国立衛生研究所) (Health and Human Services, National Institutes of Health)	938
合計	**$3729.00**

出典: House Committee on Appropriations

注: 2008 年度予算水準に対する増額分(案)を示す

景気対策法で定められた増額分も総合すると、現時点の 2009 年度予算案では、NITRD 機関に対する R&D 予算として、向こう 2 年間に少なくとも 208 億ドルの増額が想定される(表 3、5 参照)。

1.3 IT R&Dに対する連邦議会の影響

IT R&D に関する連邦議会の考え方は、以下に挙げる 5 つのポイントに集約できるといえる。まず、予算には、支出対象として米国競争法で定められた推奨研究分野の多くが含まれており、それには前政権が反対した、DOE 内に新設された高等研究事業局－エネルギー（ARPA-E: Advanced Research Projects Agency – Energy）に対する 4 億ドルの拠出も含まれる。第二に、代替エネルギー源の開発や、プラグイン・ハイブリッド車両やそれに必要な電池技術といった、エネルギー利用効率を高める研究に対し、多額の資金が提供される。第三に、気候変動の理解に努めるため、特にこの領域の研究に対し予算が分配される。第四に、医療研究へも予算が当てられる。例えば、治療の種類ごとにその有効性を検討する（外科手術と薬物療法治療の有効性比較など）ための研究には、医療コミュニティからの反対にもかかわらず、大型予算を設けている。第五に、ブロードバンド・ネットワーク配備とネットワーク・アーキテクチャ研究に対し、約 50 億ドルが分配される。第六に、NASA への予算分配は、科学研究の強化を優先し、その代わりに有人宇宙探査という NASA のこれまでの使命の優先度を下げる可能性を支持している。

予算のほとんどは、高次レベルで説明されており、各機関は連邦議会に対し、具体的な予算計画を 90 日以内に提出する必要がある。そのため、現時点で IT 予算を推定するのは困難である。しかし、スーパーコンピュータ調達予算はすでに認められており、ブロードバンド・ネットワーク整備と医療 IT を含む、いくつかの整備領域において研究が進められることになると思われる。

R&D 税還付（R&D Tax Credit）： 2007 年末にいったん期限切れを迎えた R&D 投資に対する税額控除は、2008 年 10 月に「2008 年緊急経済安定化法（Emergency Economic Stabilization Act of 2008、H.R.1424）」が連邦議会で可決されるまで、党派争いに巻き込まれていた。同法によって、2008 年 1 月 1 日から 2009 年 12 月 31 日まで、R&D 税還付が遡って再承認される。同法（P.L.110-343）は 2008 年 10 月 3 日、ブッシュ大統領が署名して成立した。

連邦議会における主要IT R&D関連プレイヤー概要

民主党は 2008 年選挙において、上下両院における支配力強化に成功した。下院では、共和党の 178 議席に対し、民主党は 255 議席を獲得し、過半数議席を大きく上回った（現在 2 席が空席となっている）。一方、上院は民主党 56 議席、共和党 41 議席、無所属 2 議席（民主党寄り）、空席 1 議席となっている。上院の議席数に関しては、正確に把握しておくことは、極めて重要である。というのは、上院の民主党議席数は、無所属を合わせても、審議打ち切りに必要とされる

60 票の“超多数（super majority）”に 1 票とどかないからである。従って、仮に共和党議員が全員反対票を投じれば、民主党の法案成立は阻止される。

超多数の獲得は、景気対策法の可決にも必要不可欠であった。実際には、革新色の強い民主党議員が予算削減措置について妥協したことなどが影響し、共和党穏健派議員 3 名が賛成票を投じ、成立にこぎつけた。

第 110 期議会から第 111 期議会にかけて、委員会メンバーにはわずかな入れ替わりがあった。おそらく最も重要な変更は、重要な委員会の一つである下院エネルギー・商業委員会（House Energy and Commerce Committee）において、John Dingell 議員（民主党、ミシガン州選出）が、委員長の座を争い Henry Waxman 議員（民主党、カリフォルニア州選出）に敗北したことである。下院科学技術委員会（House Science and Technology Committee）では、2008 年に引退した Sherman Boehlert 議員（共和党、ニューヨーク州選出）の後任として委員長に就任した Bart Gordon 議員（民主党、テネシー州選出）に対する評価が、前任者並みにはまだ確立していない。

一方、議会委員会や関連機関は、連邦政府 R&D 活動を監視してはいるものの、米国の競争力とイノベーションのためのビジョン設定と実行においては、真のリーダーシップを発揮しているとは言い難い。次に示す表は、現在の IT R&D 分野においてリーダー的な立場にある議員と、その所属委員会・小委員会、監視領域、そして 2010 年中間選挙への出馬有無をまとめたものである。

	キープレイヤー	***委員会***	***2010 年 11 月任期満了に伴う改選有無***[26]
上院	Daniel K. Inouye (民主党－ハワイ州) **委員長（Chairman）**	歳出委員会（Appropriations）	有
	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・および関連機関小委員会 (Commerce, Justice, Science, and Related Agencies))	有
	Richard Shelby (共和党－アラバマ州) **ランキング・メンバー（Ranking Member）**	歳出委員会（Appropriations）－商業・司法・科学・および関連機関小委員会 (Commerce, Justice, Science, and Related Agencies)	有
	John D. (Jay) Rockefeller, IV (共和党－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）	無
	Bill Nelson (民主党－フロリダ州) **委員長（Chairman）**	商業科学・運輸（Commerce Science, and Transportation）－宇宙、航空学、関連科学小委員会（Space, Aeronautics, and Related Sciences）	無

[26] United States Senate Elections, 2010, Wikipedia, 2009

	キープレイヤー	***委員会***	
	David Vitter (共和党－ルイジアナ州) **ランキング・メンバー（Ranking Member）**	商業科学・運輸（Commerce Science, and Transportation）－宇宙、航空学、関連科学小委員会（Space, Aeronautics, and Related Sciences）	有
	John Kerry (民主党－マサチューセッツ州) **委員長（Chairman）**	商業科学・運輸（Commerce Science, and Transportation）－科学技術・イノベーション小委員会(Science, Technology, and Innovation)	無
	John Ensign (共和党－ネバダ州) **ランキング・メンバー（Ranking Member）**	商業科学・運輸（Commerce Science, and Transportation）－科学技術・イノベーション小委員会(Science, Technology, and Innovation)	無
下院	David Obey （民主党－ウィスコンシン州） **委員長（Chairman）**	歳出委員会（Appropriations）	有
	Jerry Lewis （共和党－カリフォルニア州） **ランキング・メンバー（Ranking Member）**	歳出委員会（Appropriations）	有
	Alan Mollohan （民主党－ウェストバージニア州） **委員長（Chairman）**	歳出委員会（Appropriations）－商業・司法・科学・および関連機関小委員会 (Commerce, Justice, Science, and Related Agencies)	有

	キープレイヤー	***委員会***	
	Frank R. Wolf （共和党－バージニア州） **ランキング・メンバー（Ranking Member）**	歳出委員会（Appropriations）－商業・司法・科学・および関連機関小委員会 (Commerce, Justice, Science, and Related Agencies)	有
	Henry A. Waxman （民主党、カリフォルニア州） **委員長（Chairman）**	エネルギー・商業委員会（Energy and Commerce）	有
	Joe Barton （共和党、テキサス州） **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
	Edward Markey （民主党、マサチューセッツ州） **委員長（Chairman）**	エネルギー・商業委員会（Energy and Commerce）－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)	有
	Vacant **ランキング・メンバー（Ranking Member）**	エネルギー・商業委員会（Energy and Commerce）－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)	有
	Bart Gordon （民主党、テネシー州） **委員長（Chairman）**	科学・技術委員会（Science and Technology）	有
	Ralph Hall （共和党、テキサス州） **ランキング・メンバー（Ranking Member）**	科学・技術委員会（Science and Technology）	有

	キープレイヤー	***委員会***	
	Dan Lipinski （民主党、イリノイ州） **委員長（Chairman）**	科学・技術委員会（Science and Technology）－研究科学教育小委員会（Research and Science Education）	有
	Vernon Ehlers （共和党、ミシガン州） **ランキング・メンバー（Ranking Member）**	科学・技術委員会（Science and Technology）－研究科学教育小委員会（Research and Science Education）	有

1.4 2009 年度以降のIT R&D連邦予算展望

2009 年度における不確定要素にもかかわらず、とりわけサイバーセキュリティと情報保証を含む、2、3 件の IT R&D に関する課題が注目されている。国家経済に対するインターネット・ベースのデータとトランザクションの重要度が増大していること、ネットワーク侵入と財務データ窃盗の程度が深刻化していること、ネットワーク戦争の勃興、そして現行ネットワークのセキュリティ脆弱性は、サイバーセキュリティ R&D 予算を増大させるだけの十分な説得力がある。

「新たな時代の責任（A New Era of Responsibility）」と表されたオバマ大統領の 2010 年度予算案概要には、多くの領域について、具体的な予算額はほとんど明記されていない。代わりに、2009 年 4 月に発表が予定される正式な予算要求において焦点になると思われる、優先項目がいくつか示唆されている。概要の中で触れられた、IT に影響を与えると思われる R&D 増額を示唆する項目の一部を以下に示す:

- NIST 技術イノベーション・プログラム（Technology Innovation Program）に対する 7,000 万ドルの増額。本プログラムは、IT を含む領域における破壊的イノベーション開発を助成する。
- “スマート・パワー・グリッド（smart power grid）”開発を支援する、エネルギー省サイバーセキュリティ研究予算の増額。
- 病院やクリニックにおける電子カルテ（Electronic Health Record）システム導入のための資金提供。新たなヘルス関連 IT イノベーションに対する需要をけん引すると期待される。
- 全米サイバーセキュリティ・イニシアチブ（National Cybersecurity Initiative）の下、新たな官民パートナーシップ予算として国土安全保障省（Department of Homeland Security）へ 3 億 5,500 万ドルを追加分配する。また、生物攻撃の早期発見に関連し、継続中のバイオインフォマティクス・プロジェクトに対し、3,600 万ドルを出資する。
- NSF で実施される全ての R&D および教育活動予算として、2010 年度に 2008 年度比で 9 億ドルを増額する。

また、オバマ大統領は、IT R&D 活動に間接的影響を与えると想定される政策的措置も提唱している:

- 2 月 9 日、オバマ大統領は連邦政府におけるサイバーセキュリティについて、90 日間のレビュー実施を要請した。このレビューは、国家情報局（Office of the Director of National Intelligence）のMelissa Hathaway氏指揮の下で実施される[27]。この調査は、サイバーセキュリティ研究を目的として必ずしも行われるものではないが、結論として追加研究の必要性に触れ、「連邦政府サイバーセキュリティ・情報保証R&D計画（Federal Plan for Cyber Security and Information Assurance Research and Development）」を推進する内容になる可能性が非常に高い。関係筋の間では、本調査終了後、その提言実行に注力するため、Hathaway氏が“サイバーセキュリティ責任者（Cybersecurity Czar）”に任命されるという憶測が出ている。

- オバマ大統領は、医療改革を今後の主要イニシアチブにする計画である。この改革計画の重要な要素には、電子カルテの利用など、ヘルスケア・システムにおける情報技術の利用促進が含まれる。これを受けて、新技術や機能に対する需要がけん引されるものと予想される。

連邦政府における IT 導入に関する前掲の活動や取り組みは、新政権の IT R&D 課題を方向付ける可能性がある。行政予算管理局（OMB: Office of Management and Budget）は、Exhibit 300 と呼ばれる IT プロジェクト追跡システムを利用し、各省庁機関の IT 予算を精査している。同局内の電子政府局（Office of E-Government）は、IT 導入計画や R&D 活動を含む、各省庁機関の IT 関連活動の規制において何らかの役割を果たすものとみられている。

[27] President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review, Whitehouse, February 9, 2009

2 ネットワーク・サイバーセキュリティにおけるR&D動向

データ･ネットワークの急増や、それらネットワークを使った情報共有意欲の増大を背景に、情報セキュリティ分野は過去 30 年間に多大な変化を遂げた。1980 年前後以前には、情報セキュリティといえば、個々のコンピュータに保存された情報の保護に焦点が置かれていた。コンピュータと外部世界との繋がりは、主に手作業による情報の移動によって成り立っていた。“信頼コンピュータ・システム（trusted computer systems）”として知られるそのようなシステムの設計、維持、評価のための教科書的存在だったのが、国家安全保障庁（National Security Agency）が出版した書籍「レインボウ・シリーズ（Rainbow Series）」である[28]。当時最大の難題は、コンピュータを共有する人たちに対し、情報保護レベルを守りつつ、いかに異なるレベルのアクセス権を与えるかであった。

ネットワークの出現、特にインターネットと、その基本となるインターネット･プロトコルの出現は、情報セキュリティを取り巻く複雑性を大きく進行させた。ネットワークからアクセス可能な情報のセキュリティ確保は、今でもほぼ未解決な課題のままである。その望ましくない状況を生んだ背景には複数の理由があり、本報告の後半部ではそれらを取り上げた。手短に言えば、それら理由は次に示す 3 クラスに集約される： ①現行ネットワーク･プロトコルとツール本来の不安定さ②ネットワーク環境における現行コンピュータ・ハードウェアとソフトウェア本来の不安定さ③システム設計、工学、そして実装において、何らかの間違いを発見しそれを悪用したいという、想像力のある人間にとっては見逃し難いネットワーク環境における機会の存在。

コンピュータ上の情報を保護するために、多大な時間と知力、そして資金が投入されてきたにもかかわらず、2008 年は金銭的被害をともなうコンピュータ侵入が数多く発生した。影響を受けたシステムには、民間企業、金融機関、政府、そして個人のものが含まれる。数百万人という個人や数多くの組織団体が、データベースからの個人、あるいは機密情報の盗難に遭った。クレジットカードやデビットカードの不正利用や、銀行口座からの預金の不正引き出しなどによって、企業や個人が被った損失は相当額に上る。コンピュータ・システムに偽のメッセージを大量に送りつけ、正常なネットワーク・トラフィックを制圧するサービス妨害攻撃（denial-of-service attacks）を受けた企業の数は、計り知れない。一般的に、これら攻撃を行う動機は、攻撃を阻止するために使われる資金を奪うことである。サービス妨害攻撃は今年、人気のない政策を実施する政府機関の

[28] レインボウ･シリーズは、直近では 1980 年代半ばに改訂された。本シリーズは、米科学者連盟（Federation of American Scientists）のウェブサイトにあるレポジトリーにて入手可能である（http://www.fas.org/irp/nsa/rainbow.htm）。

攻撃にも使われた。数百万台という個人のコンピュータが悪質なソフトウェアに感染し、サービス妨害攻撃のために利用される“ボットネット（botnets）”と呼ばれるネットワークの構成要素になるか、あるいは迷惑メールの送信に悪用されている。第三者が不正侵入したコンピュータには、キーストロークを記録する不正ソフトウェアがインストールされ、銀行取引のためのパスワードや取引記録といった重要情報が傍受され、第三者の手に渡っている。

近年はこれら攻撃の動機が、従来の“（不正侵入に成功したことを）言いふらして自慢する権利”から、金銭的利益や、擬似軍事行動に移行したようである。地下経済には、他人のクレジット／デビットカード番号や、社会保障番号、電子メール・アドレス、そして企業／政府情報を販売、あるいは取引する金融ネットワークが存在する。そこでは、稼動の分配がメンバー個々の利益に資すという、新しい形態の犯罪組織が形成されている。セキュリティ上の新しい突破口（抜け道）を作り、それを使い易いソフトウェアとしてパッケージ化して販売する者もおり、攻撃者はそれを利用して無作為に選んだコンピュータ、あるいは熟考の末に狙いを定めたコンピュータにアクセスし、それらを支配する。仲介人がソフトウェアとサービスに対する支払いの段取りを行い、盗難情報の販売を取り仕切る。こうした攻撃側の進化には、鈍化の兆候はみられない。

これらに対処するため、連邦政府機関は、情報ネットワークの安全性向上を目指すアプローチや技術を開発するための研究を行っている。従来の情報セキュリティ対策は、情報の機密性、可用性、そして完全性（インテグリティ）を守ることに重点が置かれてきた：

- 機密性とは、予め承認された人だけに情報アクセスを認めるという意味である。
- 可用性とは、アクセスが中断されないという意味である。
- 完全性とは、情報の中味が、非承認の方法によって改ざんされないという意味である。

ネットワーク環境では、信頼（トラスト）という概念－参加者（個人、組織、及び場合によって相互にアクセスする関係にあるコンピュータ）間の信頼と、エージェント（コンピュータ、ソフトウェア、ネットワーク）に対する信頼－が存在しなければならない。広く分散した個人や企業間での信頼構築は、とりわけ困難であり、拡張可能な信頼関係の構築を目指す研究が重視されてきた。

最後に、コンピュータがより重要な機能を任されるに従い、機能の保存がセキュリティ上のトピックに浮上している。例えば、電力供給網には、電力の円滑な流れを保護するために特別なセキュリティ上の要件が設けられている。残念なことに、近年は主要なセキュリティ制御コンピュータである監視制御・データ・アクセス（SCADA: Supervisory Control and Data Access）システムの脆弱性が指摘されている。

本報告の 2.1 項では、連邦政府のサイバーセキュリティ･プログラムについて、その計画、優先事項、管理体系について議論する。2.2 項では、連邦政府の主要助成プログラムと、サイバーセキュリティ研究への助成と監督における連邦政府機関の役割を論じる。また 2.3 項では、著名なサイバーセキュリティ研究センターの活動を紹介する。

近年のネットワーク・サイバーセキュリティ R&D は、以下に示す 3 つの包括的領域に焦点を置いて実施されている。

第一の領域は、既存コンピュータとネットワークおける設計上の脆弱性と実行上の問題に、いかに対処するかについてである。ほぼ例外なくこれらの脆弱性と問題は、ネットワーク及びコンピュータ設置ベースでは、セキュリティ問題が、有用性やコストよりも軽視されてきたという事実に起因する。さらに、これらシステムの基本設計は、主にコンピュータ科学に基づいているが、そのコンピュータ科学は、科学・工学における他の専門領域に並ぶ厳密さや信頼性に、ようやく到達しつつある段階であり、科学としては比較的未成熟である。ソフトウェア利用者は、新たなセキュリティ上の脆弱性や、それを狙う不正手口を警告する報告に追い立てられており、その都度パッチや修正を適用しなければならない。今日まで、公共及び民間のサイバーセキュリティ資源のほとんどは、既存のセキュリティ問題の発見と修正に費やされてきた。

第二の領域は、本質的にセキュアなコンピュータとネットワーク・システムの設計を目指す、基礎研究である。これは非常に難しい問題である。考えられるコンピュータ･ネットワークはすべて、非常に複雑なシステムであり、それを分析し、さらに証明可能な望ましい特性と統合するための技術やツールは、科学分野ではまだ確立されていないからである。研究者たちが仮に、本質的にセキュアなコンピュータ・ネットワークの実現方法を見つけたとしても、既存システムの膨大な設置ベースを排除するだけで、法外な費用がかかる。

第三の領域は、拡張可能な電子的信頼を、いかに構築するかについてである。グローバル･ネットワークの存在は、数千年にわたり商取引や人間関係を支配してきた人間ベースの信頼（声や顔を認識する、署名する、周知の権威者や行政機関によって発行された紙ベースの信用証明を提出する、など）の一般的な使用を排除した。拡張可能な電子的信頼については、これまでに数多くの提案がなされてきたが、今日まで成功した例はない。電子認証手段として最もよく知られた概念は、おそらく公開鍵基盤（PKI: Public Key Infrastructure）である。PKI は、暗号化、署名、人物や文書の認証、受理、そして非周知性（non-reputability）といった、電子認証に必要とされるほとんどの項目を網羅しているかにみえる。実際、小規模なグループ間では PKI は有効だが、経済的及び社会的規模が大きい場合、PKI を一般的に採用するのは難しい。初期のウェブサイト閲覧ソフトウェアに組み込まれたセキュア・ソケット・レイヤー（SSL: Secure Sockets Layer）技術は、現時点で利用可能な技術の中では拡張可能な信頼の構築に最も近い。しかし、SSL が信頼問題を解決すると断言することはできない。

2.1 連邦ネットワーク・セキュリティR&D計画と戦略

米国におけるネットワーク・サイバーセキュリティ R&D はこれまで、連邦政府の様々な諮問委員会がまとめた複数の重要な報告などの影響を受けてきた。これらの報告は、省庁機関間の共通基準枠を確立するとともに、優先項目を設定し、R&D を分散する上で貢献してきた。

「連邦政府サイバーセキュリティ・情報保証R&D計画（Federal Plan for Cyber Security and Information Assurance Research and Development）[29]」は、19 の政府機関から招聘した有識者によって構成される、サイバーセキュリティと情報保証に関する省庁横断型作業部会（Interagency Working Group on Cyber Security and Information Assurance）によって作成された。サイバーセキュリティと情報保証における連邦政府の技術的、及び予算面での優先項目を特定するものである。計画準備に当たり、作業部会は 2 件の報告を参照している。一件目は、大統領技術諮問委員会（PITAC: President's Information Technology Advisory Committee）による「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[30]）」である。サイバーセキュリティR&Dに対する連邦政府予算を精査し、長期的影響を及ぼすと思われる基礎研究強化に向けて、抜本的変革を提言している。二件目は、連邦政府のサイバーセキュリティ研究幹部が構成するINFOSEC研究評議会（IRC: INFOSEC Research Council）による「難題リスト（Hard Problem List）[31]」である。タイトルから分かるように、サイバーセキュリティ研究分野における重要な課題の中でも特に難題を、優先順位をつけて示している。

連邦計画では、サイバーセキュリティと情報保証 R&D 分野における 8 つの優先領域を示している。以下では、これら領域ごとに、技術的あるいは予算的優先度が高い項目を示す：

---

[29] *Federal Plan for Cyber Security and Information Assurance Research and Development*, NITRD, April 2006

[30] Cyber Security: A Crisis of Prioritization, President's IT Advisory Committee, February 2005, page 19-20

[31] Hard Problem List, INFOSEC Research Council, November 2005.

1. 機能的サイバーセキュリティと情報保証（Functional Cyber Security and Information Assurance）
    a. 認証、承認、信頼管理（Authentication, authorization, and trust management）
    b. アクセス制御、特権管理（Access control and privilege management）
    c. 攻撃からの保護、攻撃の予防・先制（Attack protection, prevention, and preemption）
    d. 大規模サイバー状況認識（Large-scale cyber situational awareness）
    e. 自動攻撃検出・警告・応答（Automated attack detection, warning, and response）

2. インフラ安全確保（Securing the Infrastructure）
    a. セキュアなプロセス制御システム（Secure process control systems）

3. 領域特化型セキュリティ（Domain-Specific Security）
    a. ワイヤレス・セキュリティ（Wireless security）
    b. 集中型ネットワークと異種トラフィックのセキュリティ（Security of converged networks and heterogeneous traffic）

4. サイバーセキュリティと情報保証の特性解析と評価（Cyber Security and Information Assurance Characterization and Assessment）
    a. ソフトウェア品質評価と障害特性解析（Software quality assessment and fault characterization）
    b. 脆弱性と悪質コードの探知（Detection of vulnerabilities and malicious code）
    c. ソフトウェア試験と評価ツール（Software testing and assessment tools）

5. サイバーセキュリティと情報保証基盤（Foundations for Cyber Security and Information Assurance）
    a. 暗号学（Cryptography）
    b. セキュアなソフトウェア工学（Secure software engineering）
    c. IT システムの工学ライフサイクルを通じたセキュリティ分析技術（Analytical techniques for security across the IT system’s engineering life cycle）

6. サイバーセキュリティと情報保証 R&D 実現技術（Enabling Technologies for Cyber Security and Information Assurance R&D）
    a. サイバーセキュリティと情報保証 R&D テストベッド（Cyber security and information assurance R&D testbeds）
    b. IT システムのモデリング、シミュレーション、および視覚化（IT system modeling, simulation, and visualization）

7. 高度な次世代システムとアーキテクチャ（Advanced and Next-Generation Systems and Architectures）
    a. 信頼コンピューティング・ベース・アーキテクチャ（Trusted computing base architectures）
    b. セキュアかつ高保証なシステムおよびアーキテクチャ（Inherently secure, high-assurance, and provably secure systems and architectures）
    c. 構成可能・拡張可能セキュア・システム（Composable and scalable secure systems）
    d. 自律システム（Autonomic systems）
    e. 次世代インターネット・インフラ・アーキテクチャ（Architectures for next-generation Internet infrastructure）

8. サイバーセキュリティと情報保証の社会的側面（Social Dimensions of Cyber Security and Information Assurance）
    a. プライバシー（Privacy）

連邦計画は、これら優先項目を PITAC 報告と IRC 報告で特定された項目と比較し、文書間の類似点を挙げている。

この計画は、NITRDプログラムのコンポーネントの一つであるサイバーセキュリティと情報保証（CSIA: Cyber Security and Information Assurance）のための、フレームワークを作成している。CSIAの 2008 年度推定予算は 2 億 6,870 万ドルでありNSF、DARPA、NSA、その他DoD機関、NIH、NASA、そしてNIST間で分配される[32]。計画ではCSIA領域における省庁横断型研究の調整を求めており、連邦政府に対し、産業界及び学究界と協力し、連邦CSIA R&Dロードマップの作成を提案している。主要提言事項には、潜在的影響が最も大きな脅威に集中すること、ソフトウェアとシステム開発の初期段階からセキュリティを組み込むこと、新興IT技術やシステムについてセキュリティ面での影響を査定すること、及びサイバーセキュリティを査定するための新メトリクスを開発することが含まれる。

全米学術研究評議会（National Research Council）は 2007 年、NSF、DARPA、NIST、そしてDHSから一部資金援助を受けて、「安全かつセキュアなサイバースペースを目指して（Toward a Safer and More Secure Cyberspace）」を発表した[33]。この研究は、全米のサイバーセキュリティ研究課題の特定と優先順位決定にも貢献した。

[32] FY 2009 Networking and Information Technology Research and Development: Supplement to the President's Budget, February 2008

[33] Toward a Safer and More Secure Cyberspace, National Research Council, The National Academies, 2007

2.2 連邦ネットワーク・サイバーセキュリティ概要

2.2.1 連邦政府におけるネットワーク・サイバーセキュリティ管理

連邦ネットワークのサイバーセキュリティは、「2002 年連邦情報セキュリティ管理法（Federal Information Security Management Act of 2002）[34]」に基づき管理されている。この法律では、非軍事関連政府システムのセキュリティに対する全責任を、大統領府（Executive Office of the President）内の行政予算管理局（OMB: Office of Management and Budget）局長に委ねている。国立標準規格技術院（NIST: National Institute of Standards and Technology）は、連邦政府機関に対し強制力を持つセキュリティ技術と運用方法を開発することにより、OMB局長を支援する。

各連邦政府機関の長は、情報システムのセキュリティ維持に責任を負い、NIST の協力を得て OMB 局長が発表する標準に準拠しなければならない。各長は、最高情報責任者（Chief Information Office）（あるいは他の職員）に対し、法律と OMB 局長によって規定されたセキュリティ要件への準拠を保証するセキュリティ・プログラムを作成し、維持するための権限を与える。

同法は各機関に対し、それぞれのセキュリティ状況と法準拠について記述する年次報告を作成し、連邦議会に提出することを求めている。また、各機関の監察官（Inspector General）に対しては、各機関のサイバーセキュリティ・プログラムの独自評価を実施し、結果を連邦議会へ報告することを義務付けた。下院政府監視改革委員会（House Government Oversight and Reform Committee）は毎年、各機関とその監察官による報告を基に、各機関を評価する「FISMA評価（FISMA grade）」を発表している[35]。これは、各機関がFISMA要件を順守しているかどうかを主に評価したものであることから、特に他の優れたセキュリティ・メトリクスと相関関係があるかどうかという点において議論を呼んでいる。反対派は、サイバーセキュリティ脅威とは急速に広がる性質のものであると指摘し、作成から何年も経過した標準への準拠にこだわっていては、現在のセキュリティを検討する上で最も重要な要素を見逃す可能性があると述べている。

---

[34] Federal Information Security Act of 2002

[35] Eighth Report Card on Computer Security at Federal Departments and Agencies, House Oversight and Government Reform Committee, May 2008

OMB は、主に電子政府・情報技術局（Office of E-Government & Information Technology）を通じて、サイバーセキュリティ管理に従事している。同局はサイバーセキュリティ改善を目的に、複数のイニチアチブを進行中である。各機関に対しては、年次予算要求において、プロジェクト・レベルのサイバーセキュリティ対策に関する報告を含めることを求めている。不備があった場合は、それらを修正するための「アクションとマイルストーン計画（Plan of Actions and Milestones）」の提出を要請する。OMB は、各機関の予算に関わっているという立場上の強みを武器に、改善を求めるといったことも可能である。

OMBは、連邦政府規模で進めるIPv6 導入を先導してきた。IPv6 とは、セキュリティ機能が改善された次世代IPである。OMBは各機関に対し、インターネット・コネクションの件数を.govドメインに統合し、「トラステッド・インターネット・コネクション・プログラム（Trusted Internet Connections Program）」下における、エントリー・ポイントでの疑わしいトラフィックの監視を簡便化すること呼びかけている。トラステッド・インターネット・コネクション・プログラムについては、1.1.2 項において詳述した。本プログラムの目標は、外部コネクションの数を 100 未満に抑え、アインシュタイン（Einstein）と呼ばれるシステムを利用し、それぞれを監視することである。2008 年 5 月時点では、各機関から 2,758 のコネクションが報告されている[36]。OMBでは、連邦政府ドメイン名システム・インフラのセキュリティ改善にも取り組んでいる[37]。トップレベルの.govドメインへのDNSSEC導入の目標期限は、2009 年 1 月だった。連邦政府は、2 月末までにその目標を達成できる見通しである。この取り組みは、スウェーデンを含む 2、3 の国を除き、世界を先導するものである。

OMBは、セキュリティを改善し、さらにコンピュータが適切に設定されていることを確認するためのスキャニング・ツール使用を推進するため、連邦政府のデスクトップ・コンピュータの主要設定を標準化する指示書を発行した[38]。

[36] Trusted Internet Connections (TIC) Initiative, June 2008

[37] Securing the Federal Government's Domain Name System Infrastructure, August 2008

[38] Implementation of Commonly Accepted Security Configurations for Windows Operating Systems, March 2007

連邦政府機関は、CIO 評議会（Chief Information Officers Council）を通じ、情報技術管理活動の調整を行っている。情報セキュリティ・身元管理（Information Security & Identity Management）関連活動の調整に従事する CIO 評議会のある作業部会は、OMB 及び連邦議会と協力し、サイバーセキュリティにおけるベスト･プラクティスの推進と法規制の導入に取り組んでいる。

連邦政府のネットワーク・サイバーセキュリティR&Dは、NITRDの小委員会である全米科学技術評議会（National Science and Technology Council）によって調整作業が実施される。同評議会は、大統領府内の科学技術政策室（OSTP: Office of Science and Technology Policy）の管理下にある。NITRDは、米国連邦政府における大規模かつ生産的な省庁横断型研究調整（リサーチ･コーディネーション）例の中でも、最も歴史が古いプログラムの一つである。4 省庁間の非公式な調整プログラムとして 1980 年代末に開始され、1991 年に正式に設置された。当時は 8 つの機関が参加し、予算は約 6 億ドルだった。2009 年の大統領予算要求額は、参加 13 機関に対し 35 億ドルとなっている[39]。

NITRD 小委員会とその作業部会の構成員は、政府職員に限定される。非政府の人間や団体が連邦プログラムの企画や実行に定期的に参加することは、必要以上の影響が及ぶ可能性を考慮し、連邦法によって禁止されている。NITRD は、ワークショップやその他の特別な会合において、民間セクターからの見解を聞いている。民間セクターの組織・団体は、助成金受領と契約という形態で、プロジェクト実行に主要な役割を果たしている。

NITRD内では、サイバーセキュリティと情報保証に関する省庁横断型作業部会（CSIA IWG: Interagency Working Group on Cyber Security and Information Assurance）が、研究プログラムの調整を担っている[40]。2009 年度のCSIA研究予算要求額は 2 億 7,980 万ドルだった。CSIA参加機関には、NSF、DARPA、OSD、そしてDoDサービス（DoD Services）内の研究組織、およびNSA、NASA、NISTが含まれる。

---

[39] FY 2009 Networking and Information Technology Research and Development: Supplement to the President's Budget, National Coordination Office for Networking and Information Technology Research and Development, Executive Office of the President, February 2008.

[40] CSIA IWG は、正式には NITRD 小委員会とインフラ小委員会（Subcommittee on Infrastructure）の両方に報告する。いずれも全米科学技術評議会内の組織である。

2.2.2 包括的全米サイバーセキュリティ・イニチアチブ（CNCI: Comprehensive National Cyber Security Initiative）とその他主要イニシアチブの目標と成果

2008 年 1 月 8 日、当時のブッシュ大統領は、「国家セキュリティ大統領令第 54 号／国家防衛大統領令第 23 号（National Security Presidential Directive 54/Homeland Security Presidential Directive 23）」と呼ばれる機密共同大統領令に署名した。全米サイバーセキュリティ・イニシアチブは、この共同命令を根拠に発足している。この大統領令からは、サイバーセキュリティに関する複数の取り組み事例をみることができる。

一件目は、ブッシュ大統領が 2003 年 2 月に発表した「セキュアなサイバースペース国家戦略（National Strategy to Secure Cyberspace）」である[41]。この戦略には、サイバーセキュリティ応答システムの開発、脅威・脆弱性削減プログラムの開始、セキュリティ訓練の改善、政府システムのセキュリティ改善、及びセキュリティ問題解決のための他国との協力という、5 つの課題が盛り込まれた。戦略の一部は実施されたが、計画全体に対する包括的取り組みはみられず、国家としてのサイバーセキュリティの大幅改善は実現していない。

二件目は、過去数年間に起きた軍隊関係の極秘システムへの侵入を含め、政府や民間コンピュータ･システム及びネットワークへの侵入が多発していることである[42,43]。起訴に至った例はほとんどないが、科学捜査分析の結果、クレジットカード番号、社会保障番号、銀行口座番号といった情報を含む、数百万件という個人情報が犯罪組織によって盗まれ、直ちに悪用されたことが分かっている[44,45]。また、米国やその他の国々でも発生した政府システムへの侵入は、東欧とアジアのコンピュータを拠点とする、巧妙に組織された攻撃であることも判明した。これら攻撃の深刻さは、セキュアなサイバースペース国家戦略が機能していないことを示す、説得力のある証拠となった。

---

[41] The National Strategy to Secure Cyberspace, February 2003

[42] Titan Rain, Wikipedia

[43] Digital Fears Emerge After Data Siege in Estonia, New York Times, May 29, 1007

[44] T.J. Maxx Data Theft Likely Due to Wireless 'Wardriving', InformationWeek, May 9, 2007

[45] Payment Processor Breach May Be Largest Ever, The Washington Post, January 20, 2009

三件目は、911 攻撃後、通信モニタリングと国内情報収集を甘受する傾向が、米国内にみられることである。例えば、国家安全保障局（National Security Agency）は、従来は外国人だけを対象に実施されていたモニタリングを、現在では国内電話トラフィックへと広範に拡大して行っている[46]。

報告によると、機密計画は以下に示す 12 要素から構成され[47]、2008 年度予算は 1 億 5,000 万ドルだった[48]。

1. トラステッド・インターネット接続（TIC: Trusted Internet Connections）プログラム[49]

   連邦政府は、.govドメインとインターネットのその他ドメイン間のコネクションを制御する。そのために、これらのコネクション件数を現在の 4,000 超から 100 未満に削減する。政府機関はアインシュタイン·システムを利用し、これらのコネクションをモニターし、疑わしい動きの発見に努めなければならない。国土安全保障省（DHS: Department of Homeland Security）が開発したアインシュタインは、インターネット・トラフィック情報を収集し、DHSの米国コンピュータ緊急対応チーム（U.S. Computer Emergency Readiness Team）へ送信する[50]。

2. 侵入探知（Intrusion Detection）

3. 侵入阻止（Intrusion Prevention）

4. 連邦政府サイバーセキュリティ・情報保証 R&D 計画に準ずる研究開発

5. 全米サイバーセキュリティ・センターを介した状況認識（Situational awareness through the National Cyber Security Center）

---

[46] NSA Must Examine All Internet Traffic to Prevent Cyber Nine-Eleven, Top Spy Says, Wired, January 15, 2008

[47] National Cyber Security Initiative Will Have a Dozen Parts, Nextgov, August 1, 2008

[48] U.S. Has Launched a Cyber Security “Manhattan Project,” Homeland Security Chief Claims, Wired, April 8, 2008

[49] Implementation of Trusted Internet Connections (TIC), OMB, November 20, 2007. Other memoranda on the OMB web site describe progress towards implementing TIC in 2008.

[50] Privacy Impact Assessment for Einstein 2, Department of Homeland Security, May 2008

6. サイバー・カウンター・インテリジェンス（Cyber Counter Intelligence）
7. 機密ネットワーク・セキュリティ（Classified Network Security）
8. サイバー教育・訓練（Cyber Education and Training）
9. 情報セキュリティ技術導入（Implementation of Information Security Technologies）
10. 阻止戦略（Deterrence Strategies）
11. グローバル・サプライ・チェーン・セキュリティ（Global Supply Chain Security）
12. 官民協力（Public/Private Collaboration）

第一の要素である TIC を除き、これら要素のほとんどに関する非機密的説明は、非常に漠然としている。予算要求資料によると、少なくとも DHS、DAPRA、NSA、そして NIST が、CNCI における役割を競っている。

CNCIの成功可能性を予測することは難しいが、問題が複雑であること、そしてCNCI導入計画も複雑になることが予想されることから、失敗のリスクは高い。脅威と脆弱性は急速に広がることを考慮すると、重々しく官僚的な計画－CNCIはそうなる可能性があるが－が成功する望みは低い。例えば、USB記憶装置管理におけるウィンドウズ・ソフトウェアの脆弱性は、USBドライブを差し込むと同時に破壊工作ソフトウェアのコンピュータ侵入を許し、新たに重大な脅威の出現を引き起こした[51]。この脆弱性は、発見されるまでは不測のものだった。報道によると、軍部コンピュータへの影響が深刻なことから、DoDはカメラやプリンタを含む全てのUSB機器の使用を禁止している。

[51] Military's Ban of USB Thumb Drives Highlights Security Risks, SC Magazine, November 20, 2008

2.3 連邦政府の主要サイバーセキュリティR&Dプログラム

2.3.1 プログラム及び計画調整

NITRDプログラムの「コンピュータ・セキュリティ情報保証コンポーネント（Computer Security and Information Assurance Component）」は、連邦政府が出資するサイバーセキュリティに関する基礎研究のほとんどを成している。表 1 は、このコンポーネントの予算を機関別にまとめたものである。大統領の 2009 年度予算要求額を示したが、ほとんどの機関では、予算は 2008 年度並みにとどまっている[52]。2009 年度は、景気対策法にR&D要素が盛り込まれたことから、要求額水準の達成は現実的と思われる。

表 1 に示す予算額は、取り上げた機関における、全ての非機密サイバーセキュリティ研究に対するものである。これには、暗号化やセキュアなソフトウェア設計など、ネットワーク･セキュリティには直接関係のない領域の研究も含まれる。しかし、今日ではほとんど全てのコンピュータ･システムがネットワーク環境で稼動していることから、表 1 に含まれるほぼ全予算は、何らかのネットワーク・セキュリティ研究を支援するものであると言っても過言ではない。仮に機密プログラムをNITRD に含んだ場合、連邦サイバーセキュリティ研究予算総額は、2 億 7,980 万ドルをはるかに超えると推定される。

[52] FY 2009 Networking and Information Technology Research and Development: Supplement to the President's Budget, February 2008

表 1：NITRD プログラム：コンピュータ・セキュリティ・情報保証コンポーネント

機関	*2008 年度 100 万ドル*	*2009 年度 100 万ドル*
全米科学財団（National Science Foundation）	68.1	87.6
国防総省国防高等研究事業局（Defense Advanced Research Projects Agency）	124.4	106.8
OSD・DoD サービス（OSD and DoD Services）	38.6	40.7
国立衛生研究所（National Institutes of Health）	1.1	1.1
国家安全保障庁（National Security Agency）	15.5	17.8
National Aeronautics and Space Administration	0.3	0.2
国立標準規格技術院 （National Institute for Standards and Technology）	20.8	25.8
合計	268.7	279.8

2.3.2 国土安全保障省（DHS: Department of Homeland Security）

DHSのサイバーセキュリティR&Dは、科学技術部（Science and Technology Directorate）予算で運営されている。科学技術部の 2008 年度予算総額は 8 億 3 千万ドルだった[53]。同部は 6 つの主要R&D“推進領域”を掲げているが、サイバーセキュリティに直接関係あるのはそのうち 1 つだけである。

- 爆発物検出と防衛手段（Explosives detection and countermeasures）
- 生物学的・化学攻撃防衛手段（Biological and chemical attack countermeasures）
- 国境・海事セキュリティ（Border & maritime security）
- 人的要因研究（Human factors research）
- インフラ・地球物理学的セキュリティ（Infrastructure & geophysical security）

[53] FY 2009 Budget Request, Department of Homeland Security, February 2008

- コマンド・制御・互換性（Command, control & interoperability）

サイバーセキュリティ･プログラムは、このうち 6 番目の推進領域である、コマンド・制御・互換性に含まれる。サイバーセキュリティ・プログラムに含まれる、具体的プログラムの一部を紹介する：

情報インフラ・セキュリティ（IIS: Information Infrastructure Security）プログラム：

予算：2008 年度は、990 万ドル、2009 年度は、1,120 万ドルとなっている。具体的なプロジェクトには、「ドメイン名システム・セキュリティ（DNSSEC: Domain Name System Security）」、及び経路指定（ルーティング）インフラ向け PKI ベース･プロトコル開発に取り組む「セキュア・プロトコル・プロジェクト（Secure Protocols Project）」、電力・水・ガスを含むインフラを制御する SCADA 及び PCS コンピュータの安全確保を図る「プロセス制御システム・セキュリティ・プロジェクト（Process Control Systems Security Project）」、戦争ゲーム技術を利用し、サイバー機器応答を試験する「サイバーセキュリティ査定プロジェクト（Cyber Security Assessment Project）」、及び利用者の身元（アイデンティティ）と当局者管理のための SAML といった概念を試験する「ネットワーク・アイデンティティ管理テストベッド（Network Identity Management Testbed）」が含まれる。

サイバーセキュリティ研究ツール・技術（Cyber Security Research Tools and Techniques）プログラム：

予算：2008 年度は、720 万ドル、2009 年度は、700 万ドルとなっている。現実的環境下でサイバーセキュリティ技術を試験するために必要となる、セキュアな施設と手法を提供する。プログラムには 4 つのプロジェクトがあり、そのうち「試験的研究テストベッド･プロジェクト（Experimental Research Testbed Project）」では、NSF と協力し、防衛技術試験的研究（DETER: Defense Technology Experimental Research）サイバーセキュリティ・テストベッドを構築する。DETER では、60 強のサイトに対し現実的なインターネット・モデルを提供し、サイバーセキュリティ技術を試験する。「研究データ・レポジトリ・プロジェクト（Research Data Repository Project）」では、サイバー脅威に対する防衛インフラのための保護されたレポジトリ（PREDICT: Protected Repository for the Defense of Infrastructure against Cyber threats）を保持している。このレポジトリは、研究者による分析に資するために構築された、現実のネットワーク･トラフィックを収納する大規模データセットである。これらデータセットには、ネットフロー（netflow）、パケット・トレース（packet traces）、トポロジーと性能データ（topology and performance data）、そしてネットワーク管理データ（network management data）が含まれる。PREDICT では、防衛的サイバーセキュリティ技術の品質改善を目標としている。

次世代技術プログラム（Next-Generation Technology Program）

予算：2008 年度は、280 万ドル、2009 年度はゼロとなっている。次世代サイバーセキュリティ R&D ニーズに取り組むプログラムである。2007 年度、HSARPA はこのプログラムの助成対象を公募した（BAA 07-09）。採用されたプロジェクト案に対する拠出額は最大 450 万ドルが予定されていたが、実際に提供されたのはわずか 280 万ドルに留まり、2009 年度も追加助成は行われなかった。HSARPA は、BAA 下で提供された助成金及び契約一覧を公表していない。しかし、2009 年度予算を見ると、ハンドヘルド型ワイヤレス機器を利用するセキュアな通信に注力する姿勢が伺える。

2.3.3 国防総省国防高等研究事業局（DARPA: Defense Advanced Research Projects Agency）

DARPAにおけるサイバーセキュリティ研究は、主に戦略的技術局（Strategic Technology Office）と、一部を情報処理技術局（Information Processing Techniques Office）から資金提供を受けて実施される。近年、DARPAは基礎的・非機密的・大学ベースのサイバーセキュリティ研究の大半を削減し、代わりに機密扱いされることが多い応用・企業ベース研究を重視する傾向にある。その結果、最先端技術を進歩させる名目で一般に公開されてきた本領域におけるDARPA研究の数は、減少している[54]。

DARPAのサイバーセキュリティR&Dの大多数は、「情報保証・生存性プログラム（Information Assurance and Survivability Program）」の一環として実施されている。表 2 は、本プログラムと一部サブプログラムの予算を示したものである（注：関連性の低いプログラムは記載を省略したため、この表の合計額は本プログラムの合計額とは異なる）[55]。

[54] Cyber Security: A Crisis of Prioritization, President's IT Advisory Committee, February 2005, page 19-20

[55] Department of Defense FY 2009 Budget Estimates, Volume 1 – DARPA, February 2008, pp. 51-68.

表 2: DARPA のサイバーセキュリティ R&D 予算

プログラム	*2008 年度 100 万ドル*	*2009 年度 100 万ドル*
情報保証・生存性（Information Assurance and Survivability）	93.05	80.35
コンピュータ・ウィルスの動的隔離	*12.34*	*10.93*
（Dynamic Quarantine of Computer-Based Worms）		
信頼のおけるシステム（Trustworthy Systems）	*12.80*	*10.00*
将来の情報保証イニシアチブ（Future Information Assurance Initiatives）	*8.25*	*0.00*
広域ネットワーク監視（Wide Area Network Monitoring）	*3.00*	*0.00*
セキュリティ認知システム（Security-Aware Systems）	*16.68*	*14.00*
広域光ファイバー・ネットワークを利用する量子鍵配送	*0.00*	*3.00*
（Quantum Key Distribution over Wide-Area Fiber Optic Networks）		
ルートキット検出（Rootkit Detection）	*0.00*	*3.50*
防衛的自立システム（Defensive Autonomous Systems）	*0.00*	*3.00*
サイバーセキュリティ・イニシアチブ（Cyber Security Initiative）	0	*50.0*

コンピュータ・ウィルスの動的隔離（Dynamic Quarantine of Computer-Based Worm Attacks）: 2003 年 3 月、戦略的技術局は「DARPA-BAA03-18：軍部エンタープライズ・ネットワークを狙ったコンピュータ・ウィルスの動的隔離（DARPA-BAA03-18: Dynamic Quarantine of Computer-Based Attacks Against Military Enterprise Networks）[56]」と呼ばれる公告を出した。この公募資料は以下のように述べている。

[56] Dynamic Quarantine of Computer Based Attacks, DARPA-BAA03-18, Defense Advanced Research Projects Agency, March 2003

“本プログラムの目的は、①自動的かつ動的にゼロ・デイ（新手の）コンピュータ・ウィルスを隔離し、軍部エンタープライズ・ネットワークに属する攻撃されやすいマシンについて、何も対処しなければ感染率約 100%になるところ、最大で 1%にとどめるような技術を開発する、②攻撃を受けた後に、脆弱なマシンを利用して分散稼動されるミッション・クリティカルなアプリケーションが復旧するまでの時間を、数日から数時間、数分、そして数秒へ短縮する。”

2008 年度中の本プログラム達成事項の例として、異なる手法を利用する 2 件のプロトタイプ・システムの完成と試験の実施、そして DoD ネットワークへのこれらシステムの統合が挙げられる。

信頼のおけるシステム： 拡張可能なネットワーク監視（Trusted Systems: Scalable Network Monitoring）: 信頼のおけるシステム・プログラムの総合目標は、DoD のコンピュータ・システムに対し、基本的に信頼できるコンピュータ・プラットフォームを提供することである。具体的には、新規のコンピュータ処理アーキテクチャ、ハードウェア、ファームウェア、あるいはネットワークとコンピュータのセキュリティを保証するマイクロカーネルの開発を目指している。まずは拡張可能なネットワーク監視に焦点を置く計画である。予算は 2008 年度に 1,280 万ドル、2009 年度に 1,000 万ドルとなっている。

2007 年 8 月、DARPA戦略的技術局は、「DARPA-BAA0752 拡張可能なネットワーク監視」と呼ばれる公告を出した[57]。公告は、署名ベースのスキャニングや異常行動の観察などを通じた、外部侵入を阻止するための大型ネットワーク監視に必要とされるコンピュータ・リソースについて、ネットワーク上のコンピュータ・ホストの増加よりも早い勢いで増えており、その結果、全ネットワーク容量のうち、前例がないほどの割合がそれに使われていると指摘した。その上で、「DARPAは、コンピュータ・ネットワーク監視システムに関する革新的な提案を求めている。ネットワーク・ベースの監視に対する新アプローチは、ネットワークを最大限にカバーし（例えば、ゲートウェイからなど）、ネットワーク規模と計算コストに左右されない監視性能を実現する。その場合の計算コストは、従来と同様、監視対象である全ネットワーク計算能力の、ほんの一部に抑えるか、あるいは削減されること」と述べている。

[57] Scalable Network Monitoring, DARPA-BAA07-52, Defense Advanced Research Projects Agency, August 2007

2008 年 7 月、BBNテクノロジーズ（BBN Technologies）は、この要請に応える形で 440 万ドル規模の契約を獲得した[58]。契約要件には、以下が含まれる：実際に受けた攻撃につき、99%以上の確立で悪意のあるトラフィックを検出すること。 トラフィック監視中の誤警報率は、1 日あたり 1 件未満であること。 契約フェーズⅠ段階において、従来のゲートウェイ･ライン･スピード 1Gbpsをサポートすること。またフェーズⅡ段階においては、ゲートウェイ・ライン・スピード 100Gbpsをサポートする拡張性を実演することとなっている。

将来の情報保証イニシアチブ（Future Information Assurance Initiatives）：DoD にとって有望と考えられる情報保証技術を特定する。本分野の達成事項の例としては、情報保証特性を追加するためにコンピュータ･アプリケーションを修正する自動技術、（データと VoIP の）集中型ネットワーク（converged networks）のコア･シグナリング及び制御の保護、ネットワーク上のホスト特定と認証、そしてこれらホストによるネットワーク動作特性の発見が挙げられる。

広域ネットワークと監視（Wide Area Network Monitoring）：分散型ネットワーク監視機能の開発に並行し、DoD WAN（広域ネットワーク）を特定し、さらにそれを特徴付け、実現、最適化、視覚化、そして保護するための機器を開発する。従来の侵入検出システムと比べた検出及び誤報率の改善、大型ネットワークに対する拡張性などが目標として設定されている。

セキュリティ認知システム（Security-Aware Systems）：独自のセキュリティ特性、能力、及び機能を推論する能力に基づき、生存可能性、自動監視、そして自己防衛機能を備えたネットワーク中心型システムのための潜在的に有望なセキュリティ認知技術を開発する。短期的目標の例として、サイバー攻撃やシステム障害を検出して応答し、自ら、あるいはほとんど他の助けを借りずに修復するようなコラボレーション･ベースの防衛機能を開発することにより、市販の抗サイバー攻撃及びシステム障害ソフトウェア･アプリケーションを導入した DoD 情報システムを保護する技術の開発がある。

[58] Military lays Out $4.4M to Supersize Network Monitoring Technology, Network World, August 12, 2008

広域光ファイバー・ネットワークを利用する量子鍵配送（Quantum Key Distribution over Wide-Area Fiber Optic Networks）： 広域光ファイバー･ネットワークに対応した、エンド・ツー・エンドの量子鍵配送技術を開発する。今日この技術は、通信距離 200 キロメートル以内のポイント・ツー・ポイントなコネクションに対してのみ実現されている。課題は、広域・動的光ファイバー交換網に対しても、量子鍵配送機能を拡張することである。それには、“量子リピーター”の創造と、関連鍵配送プロトコルの開発が必要と考えられている。本プログラムの目標は、既存の DoD 広域試験ネットワーク上で、この機能を試験的に実演することである。

ルートキット検出（Rootkit Detection）： ルートキット開発における傾向の特定、次世代脅威の予想、そして高度検出及び緩和（軽減）技術の開発などを目標とする。そのための考えられるアプローチとして、ルートキットの間接的影響の検出（導入に関わる影響は除く）、間接的影響を誘発するような、システムにおける異常な利用状態の作成、複数観点からの証拠の収集、そして証拠を論理的に検討するためのベイジアン・ネットワーク（Bayesian Network）の利用などが挙げられる。

防衛的自立システム（Defensive Autonomous Systems）：ネットワーク内で遠隔地から制御されるコンピュータ（bots）とそのスレーヴをより密接に監視、特定することと、ネットワーク運用者の監視能力を増強することを目的としている。そのために、それを実現するための画期的ソフトウェアの開発を目指す。ボーダ・ゲートウェイ・プロトコル（border gateway protocol）を利用し、インターネットの大型構成要素（自立システムなど）間でポリシー･ベースのルーティングを提供する。自立システムからコンセントリック・リングを構築することにより、リングの外にいる人々（インターネット利用者など）からネットワーク全体、またはその一部を隠すことが可能である。ボット・コマンドと制御トラフィックは極めて規則正しく、また独特なシグネチャー（形跡）を有すことから、外部及び内部リング間のインターコネクション・ポイントを監視することにより、全てのスレーヴ及びコントローラーを特定することが可能である。

サイバーセキュリティ・イニシアチブ（Cyber Security Initiative）：本プログラムは、1.1.2 項で詳述した包括的全米サイバーセキュリティ・イニチアチブにおける DARPA の活動に対し、資金を拠出している。本プログラムの詳細は機密扱いとなっている。

高信頼・非妥協半導体技術（TrUST: Trusted, Uncompromised Semiconductor Technology）: サイバーセキュリティに対し、ハードウェア面からのアプローチを検討する。本プログラムの目標は、製造後の集積回路について、信頼性を認定する技術を開発することである。まずは、集積回路を速やかに分析し、信頼される設計ソースで作成された設計のそれと比較するための技術開発を目指す。予算は 2008 年度に 1,980 万ドル、2009 年度に 200 万ドルとなっている。

軍部ネットワーキング･プロトコル（Military Networking Protocol）:2008 年 10 月、DARPA戦略的技術局は、「DARPA-BAA-09-11 軍部ネットワーキング･プロトコル（Military Networking Protocol）[59]」を発表した。厳密にいえばサイバーセキュリティを扱うプロジェクトではないが、その成果は、インターネット･パケットのソース･アドレスを特定するための基礎となる可能性がある。BAAでは「軍部ネットワーキング･プロトコル（MNP）は、軍部コンピュータ・ネットワーク向けに、完全ユーザー･レベル特定を備えたネットワーク優先順位決定システムを開発するためのものである。本プログラムで開発されるプロトコル、技術、及び機器は、MNP技術を利用するコンピュータやネットワーク・エンクレーブ（少数集団）向けネットワーク・データ・フローの匿名性を解消する。ネットワーク・トラフィックを特定するということは、ネットワーク･インフラに対し、個人及びユニットの両レベルにおいて明確に優先レベルを決定付ける機能を提供し、また利用者あるいは利用者クラス間における帯域再分配を可能にし、さらにサービスの質に関する意思決定の自動化を実現する」と述べている。

国家仮想領域（NCR: National Cyber Range）:2009 年度予算要求の中では言及されていないが、DARPA戦略的技術局は 2008 年 5 月 5 日、「DARPA-BAA08-43 国家仮想領域（National Cyber Range）[60]」を発行している。その要請書には、以下のように記されている:

NCR の目標は、以下を可能にする持続性の仮想領域を提供することにより、サイバー･オペレーションを実行する国家の能力に革命をもたらすことである。

- 典型的ネットワーク環境における、情報保証及び生存性ツールに関する無作為・定量的かつ質的な評価の実施

[59] Military Network Protocol, DARPA-BAA-09-11, Defense Advanced Research Projects Agency, October 2008

[60] National Cyber Range, DARPA-BAA08-43, Defense Advanced Research Projects Agency, May 2008

- 現在及び将来の DoD 武器システムとオペレーションにおける、複雑・大型・異種ネットワークと利用者の複製
- 同一インフラにおける、複合的・独立・同時実験の実現
- インターネット／グローバル情報グリッド（GIG: Internet/Global Information Grid）規模の研究に関する現実的試験の実現
- 画期的サイバー試験機能の開発と実行
- 厳密なサイバー試験のための科学的手法の利用実現

2009 年 1 月 7 日、DARPA 戦略的技術局は本プロジェクトのフェーズ 1 として、7 組織に対し総額 2,960 万ドルの資金を拠出した。受益団体とその金額は、次の通りである：スパルタ（Sparta, Inc.）860 万ドル、BEA システムズ（BEA Systems）330 万ドル、ロッキード・マーチン（Lockheed Martin）540 万ドル、SAIC280 万ドル、ノースロップ・グラマン（Northrop Grumman）30 万ドル、ジョンズ・ホプキンス大学（Johns Hopkins University）730 万ドル、ジェネラル・ダイナミクス（General Dynamics）190 万ドル。

2.3.4 全米科学財団（NSF: National Science Foundation）

NSF は従来、主に大学で実施される非常に基礎的な研究に投資する。ネットワーク・セキュリティ分野における NSF のプロジェクトは、科学・工学の他の分野におけるプロジェクトに比較して、やや応用寄りとなっているが、それでもなお NSF は、プロジェクトの結果は直ちに商業化されるようなものでない。過去 2 年間は、短期では応用が困難と思われる“変換研究（transformational research）”を対象とした研究プロジェクト公募に力を入れている。

信頼のおけるコンピューティング（Trustworthy Computing、サイバー・トラストの後継プロジェクト）： 2009-2010 年度に実施される特別な分野横断的プログラムである。信頼に値する新技術開発を知らしめる目的で、信頼性の科学的基盤を強化するようなプロジェクトを支援する。特に注目する対象に、全てのコンポーネントと組成物に関する信頼性－信頼性（reliability）、セキュリティ、プライバシー、そして有用性－を分析し推論するための新モデル、ロジック、アルゴリズム、及び論理がある。先行プログラムであるサイバー・トラスト（Cyber Trust）の成果を基に、本プログラムは、暗号学の基礎を探索するプロジェクトや、現在のアルゴリズム、あるいはプロトコルにおけるセキュリティ上の弱点を精査、調査するプロジェクト、そして、信頼性、あるいはそれに対する推論の改善に資する新規コンピューティング・モデルを探索するプロジェクトを、引き続き支援する計画である[61]。本プログラムのプロジェクト公募は、2008 年 12 月に公告された[62]。本プログラムに出資する組織であるコンピュータと情報科学・工学（Computer & Information Science and Engineering）部門の次長は、現職に就く前はカーネギー・メロン大学（Carnegie Mellon University）で信頼のおけるコンピューティングに関する研究に従事していたことから、本プログラムは内部から多大な支援を期待できると考えられる。

先行プログラムであるサイバー・トラストが、2008 年度に資金提供したプログラムの一部を以下に記す：

> **ボットネット・コマンドと制御コミュニケーションの理解（Understanding Botnet Command and Control Communication）：** ボット間のネットワーク・レベルの相互作用を観察及び推察するとともに、具体的なボット相互作用の背後にあるボットネット C&C コミュニケーション・プロトコル・ロジックを証明することにより、ボットネット脅威に対する理解を大幅に深めることを目指す。

[61] Trustworthy Computing, National Science Foundation.

[62] CISE Cross-Cutting Programs: FY 2009 and FY 2010, National Science Foundation

ダートマス・トレース浄化フレームワーク（Dartmouth Trace Sanitization Framework）： コンピュータ･ネットワークの活動をライブで分析できれば、コンピュータ･ネットワーキング研究はより迅速に進化する。当然ながら、ネットワーク・トレースを見つけて共有することを希望する研究者は、機密情報を排除するため、トレースを適切に“浄化”しなければならない。本プロジェクトは、ネットワーク・トレース共有をより安全に、かつトレース浄化をより簡便に行うことにより、ネットワーク・トレース共有の促進を目指す。

有効サイバー・トラスト指標（Usable Cyber Trust Indicators）： システムがセキュリティ・クリティカルな機能の実行を“人間のグループ（human in the loop）”に依存する場合、その機能をいつ、いかに実施するかを伝達するために、サイバー･トラスト指標が導入されることが多い。指標は通常、情報を伝達し、すでに伝達された情報を利用者に思い起こさせ、そしてその行動に影響を与えるような警告、あるいは状態指標として機能する。本研究は、サイバー･トラスト指標の有効性を調査するとともに、それら指標を最も有効かつ使用可能にするためのアプローチを開発する。

拡張可能なセキュリティ試験のためのルーター・モデルと縮小ツール（Router Models and Downscaling Tools for Scalable Security Experiments）： サービス妨害のような攻撃や、ドメイン間をまたがる（inter-domain）ルーティングに対する攻撃からの防衛のほとんどは、現実的な状態、あるいは十分に規模が大きな環境での有効性が立証されていない。本プロジェクトは、以下に示すことを通じて、セキュリティ試験における忠実性と規模の問題の双方に取り組むものである：①ルーター･モデル：高忠実度ながら拡張可能なルーターやその他機器のモデルを、少数の緻密に計算されたシナリオ下において、単純な装置測定をベースに設計する、②縮小ツール：シミュレーション、エミュレーション、またはテストベット試験を利用して実際に試験を行う前に、試験シナリオを単純化するための技術を開発する。

ユビキタス･セキュア技術における研究チーム（TRUST: Team for Research in Ubiquitous Secure Technology）: TRUSTとは、セキュリティ、プライバシー、データ保護、そして信頼のおけるシステムの開発・導入･利用にともなう課題に影響を与えるような、技術的、運用面、法的、政策面、および経済的問題に取り組むNSF科学技術センターである[63]。研究責任者（Principal Investigator）は、カリフォルニア大学バークレー校の研究者である。助成期間は 2005 年 6 月 1 日から 2010 年 10 月 31 日まで、助成金額は 1,498 万ドルである。同センターは、次に示す 8 テーマに注力している：教育、電子医療記録、ID窃盗とフィッシング、ナレッジ･トランスファー、ネットワーク防衛、政策、センサー･ネットワーク、信頼のおけるシステム。

表 3 に、サイバー･トラスト･プログラム下で設立された関連センターを示す。

[63] Team for Research in Ubiquitous Secure Technology (TRUST)

表 3：NSF サイバー・トラスト・センター助成プロジェクト

プロジェクト	研究者	内容
正確・有効・高信頼・可聴・透明な選挙センター（ACCURATE: Center for Correct, Usable, Reliable, Auditable, and Transparent Elections）	David Wagner カリフォルニア大学バークレー校（University of California-Berkeley）	電子投票システムにおいて、様々な照合システム（紙、音、暗号など）が果たせる役割や、ソフトウェア・アーキテクチャ、改ざん防止ハードウェア、及び暗号プロトコルを研究する。また、システムの可用性について調べるとともに、公共政策と行政手続きが、技術を利用することにより、投票システムを効果的にいかに保護できるかを研究する。
インターネット疫学と防衛のためのサイバートラスト・センター（CCIED: Cybertrust Center for Internet Epidemiology and Defenses）	Vern Paxson 国際コンピュータ科学研究所（International Computer Science Institute） Stefan Savage カリフォルニア大学サンディエゴ校（University of California-San Diego	本センターでは、次の 2 件の基本的ニーズに対処する：インターネット疫学の動作（ビヘイビア）と限界に対する理解を深めること、新たな攻撃に対しリアルタイムで自動的に防衛措置を取ることができるようなシステムを開発すること。前例のない規模の分散型“ネットワーク望遠鏡（network telescope）”を開発、運用する。望遠鏡からは、脆弱な“ハニーポット（honeypot）”サーバーのコレクションである“ハニーファーム（honeyfarm）”がフィードされる。ハニーポット・サーバーの感染は、インターネット規模のコンピュータ・ウィルスの存在を示す。
電力供給網のための信頼に値するサイバー・インフラ（TCIP: Trustworthy Cyber Infrastructure for the Power Grid）	William Sanders イリノイ大学アーバナーシェンペーン校（University of Illinois Urbana-Champaign）	電力供給を継続しつつ悪意のあるサイバー攻撃にも耐えられるような次世代電力供給網のための、サイバー･インフラの設計、構築、及び立証方法に関する課題に取り組む。電力システム・サイバー・インフラの制約や脆弱性は、他のクリティカルなインフラ･システムが直面するものと同様であることから、本プロジェクトで開発されるソリューションは、それらシステムにも同様に適用可能となることが期待される。従って、本プロジェクトの活動は、将来の電力供給網及び他のクリティカルなインフラの構築方法に重大な影響を与え、それらをよりセキュア、かつ高信頼、安全なものにすると考えられる。

2.3.5 国家安全保障局（NSA: National Security Agency）

NSA 予算は機密扱いとなっているが、NSA は NITRD プログラム下で実施されるネットワーク・サイバーセキュリティ活動の一部を報告している。NSA が活動する領域には、ソフトウェア保護、グローバル情報グリッド（Global Information Grid）のための分散型信頼・保証、セキュリティ管理、状況認識と応答、保証された情報共有、そしてワイヤレス・ネットワークのセキュリティが含まれる。NSA はまた、COTS ハードウェアや、高速ネットワークのための暗号アルゴリズムと工学、動作（ビヘイビア）ベースのネットワーク監視技術を利用する、安全なコンピューティング・プラットフォーム技術の開発にも従事しており、それらの情報を、情報ごとに異なるレベルの等級と使途を設けた上で、さまざまな利用者に対し公開している。

2.3.6 DoD 関連機関：陸軍、海軍、空軍（DoD Services: Army, Navy, Air Force）

陸海空軍は、DARPA や NSA などの機関で開発された成果を応用するために、応用 R&D を実施している。2008 年度と 2009 年度の注力分野として、拡張鍵管理システム（EKMS: Enhanced Key Management System）の一部として NSA が開発した技術を利用する、鍵管理システム改善を通じた通信セキュリティの強化が挙げられる。また、セキュリティ技術や製品の改善に取り組み、悪意のあるサイバー攻撃、あるいは偶発的サイバー攻撃に対するサービス・ネットワークとシステムの保護を強化する。暗号機器をアップグレードし、グローバル情報グリッドにおける現在のネット中心型オペレーションに必要とされる、より近代的な暗号システムを導入する。

2.4 主要ネットワーク･セキュリティR&Dセンターの概要

2.4.1 政府機関

国立標準規格技術院（NIST: National Institute of Standards and Technology）

情報技術ラボラトリー（Information Technology Laboratory）
予算：2008 年度 1,050 万ドル、2009 年度 110 万ドル

NIST におけるネットワーク・セキュリティ R&D は、情報技術ラボラトリーで実施される。NIST は標準と技術において特別な役割を担っていることから、そのセキュリティ関連研究のほとんどは、極めて応用色の強いものとなっている。NIST は、秘密及び公開暗号鍵、認証、認定管理、バイオメトリクス、そしてスマート･トークンの開発、試験、及び認定において、政府の重要な役割を果たしている。最近では、旧式のデータ暗号化規格（DES: Data Encryption Standard）の代わりに、新暗号化規格（AES: Advanced Encryption Standard）の採用につながった研究公募が有名である。予算は 2008 年度は、1,050 万ドル、2009 年度は 110 万ドルである。

セキュリティ技術グループ（Security Technology Group）：暗号、身元証明、及び認証技術を研究する。プロジェクトには、「e 認証（e-Authentication、インターネット上で利用者を認証するための秘密ベースの仕組み）」、「暗号アプリケーションとインフラ（Cryptographic Applications & Infrastructures、アプリケーションと、その根本的暗号インフラのためのセキュリティ･サービス）」、「暗号ツールキット（Cryptographic Toolkit、アルゴリズムや技術といった暗号コンポーネントの中から、利用者がそれぞれのニーズに応じて選べる包括的ツールキット）」、「電子投票に関するセキュリティ（Security Aspects of Electronic Voting、投票システムに対する脅威に反撃し、監査能力を強化するセキュリティ・アーキテクチャ）」、「暗号ハッシュ・プロジェクト（Cryptographic Hash Project、AES 採用につながった時と同じような研究公募を通じ、脆弱なハッシング・アルゴリズムの代替技術を開発する）」などが含まれる。

システム及びネットワーク・セキュリティ・グループ（Systems and Network Security Group）：新興技術を特定し、クリティカルな情報インフラに多大な影響を与えるような、新しいセキュリティ・ソリューションを考案する。現在の関心領域には、スマート・カード・インフラとセキュリティ、ワイヤレス及びモバイル機器セキュリティ、ボイス・オーバー・インターネット・プロトコル（VoIP）セキュリティ問題、電子情報科学捜査ツールと手法、アクセス制御と認証管理、インターネット・プロトコル・セキュリティ、侵入検出システム、量子情報システム・セキュリティと量子暗号、及び脆弱性分析が含まれる。研究プロジェクトとしては、「自動セキュリティ機能試験（Automated Security Functional Testing）」、「役割ベースのアクセス制御（Role Based Access Control）」、「モバイル・アドホック・ネットワーク（MANET: mobile ad hoc network）とセンサー・ネットワーク・セキュリティ（Sensor Network Security）」、「エンタープライズ・ネットワークにおけるセキュリティ・リスク測定（Measuring Security Risk in Enterprise Networks）」、そして「スマートカード R&D」などが挙げられる。

セキュリティ管理と支援グループ（Security Management and Assistance Group）：セキュリティに関する管理及び規制上の問題に関する啓蒙活動を行う。研究活動は限定的である。

セキュリティ試験とメトリクス・グループ（Security Testing and Metrics Group）：暗号モジュールと暗号アルゴリズム導入、独立試験ラボラトリーの認定、及びテスト・スイートの開発に関する検証、業界フォーラムに対する技術支援の提供、教育・訓練・啓蒙プログラムなどを実施する。

身元管理システム・プログラム（Identity Management Systems Program）：電子身元管理、クリティカル標準規格、及び電子身元の相互互換性のための共通モデルとメトリクスの開発を手掛ける。具体的な課題には、スマートカード集積回路向けプログラミング・インターフェースをはじめとする、スマートカード共通規格の開発、標準化作業、そして試験がある。また、身元管理システムのためのバイオメトリック・データ（顔、指、虹彩、声、DNA）に関する研究も行っている。

包括的全米サイバーセキュリティ・イニチアチブ：躍進セキュリティ技術（Comprehensive National Cyber Security Initiative: Leap-Ahead Security Technologies）：1.1.2 項で詳述したサイバーセキュリティ・イニシアチブを支援する目的で、2009 年度予算要求に盛り込まれた。要求額は 500 万ドルである。NIST は、次に示す 3 領域における研究を提案している：①権限を与えられた個人に対し、暗号化されたコンピュータ・ネットワークとシステムへのアクセスを与えるために一般的に利用される、暗号鍵の生成、流通、利用、保存、そして破棄のための技術的標準の作成。NSA をはじめとするその他機関に対する、技術的コンサルテーションの形で実施される。② パスワードや虹彩スキャンを含む、多元的認証手段のための標準化されたフレームワークの開発。それら手段は、異種コンピュータ・プラットフォームやオペレーティング・システム（OS）間で利用できること。この取り組みは、国土安全保障省を含む連邦政府機関及びベンダーと協力して実施される。③セキュリティを最適化する標準セキュリティ設定の集まりである、連邦デスクトップ・コア設定（Federal Desktop Core Configuration）の対象を、ウィンドウズ XP とビスタ（Vista）に対する既存のサポート領域を超えて、他の OS、アプリケーション、そしてネットワーク機器にも拡大する。

空軍研究ラボラトリー（AFRL: Air Force Research Laboratory）
予算：非公開

AFRL 本部はオハイオ州ライト・パターソン空軍基地（Wright Patterson Air Force Base）にあるが、ネットワーク・セキュリティ R&D は、ニューヨーク州ローマ空軍基地（Rome Air Force Base）内の情報局（Information Directorate）を中心に実施されている。2007 年度の情報局総予算 7 億 1,900 万ドルのうち、80%以上は外注費に当てられた（ネットワーク・セキュリティだけの予算は示されていない）。内部 R&D 予算は、総予算のわずか 6%にとどまる。

情報局は「集中的長期課題と中核的技術能力（Focused Long Term Challenges and Core Technical Competencies[64]）」に基づき、R&D優先順位を決めている。ネットワーク・セキュリティ課題については、「主要攻撃的サイバー戦闘（Dominant Offensive Cyber Engagement）：軍隊、リーダーシップ、そしてインフラに対する、全範囲の攻撃的サイバー／情報軍事作戦を実施」と説明されている。

[64] AFRL Information Directorate Challenges and Competencies

ネットワーク･セキュリティの技術的能力については、「サイバー･オペレーション（Cyber Operation）：米国のクリティカルな情報インフラに対する優れた防衛機能」とある。具体的にそれらには、独自の情報スペースの保護、侵入と異常状態の検出、敵による制御の否定、攻撃源と攻撃の意図を理解するための情報分析と相互比較、及び悪意のある侵入企てへの対応が含まれる[65]。

情報局は、空軍の研究ニーズを学究界の研究能力と結び付けることを目的に、仮想の大学中心型情報研究所（Information Institute）にも資金を提供している。研究所の重点領域には、サイバー･オペレーションの中核能力が含まれる[66]。

AFRLの一部である空軍科学研究局（AFOSR: Air Force Office of Scientific Research）は、情報オペレーションとセキュリティ（Information Operations and Security）に関する基礎研究に資金を拠出している[67]。本研究の目標は、①本質的にセキュアなソフトウェアの理解とツール開発、及び②関連ネットワークと情報スペースを流れる膨大な情報のセキュリティの確保である。具体的なトピックを以下に記す：

(1) すでにシステムに存在する偽情報を特定する方法

(2) セキュリティに関する、システム、ソフトウェア、及びネットワーク･アーキテクチャの数学的基礎

(3) 全ネットワーク層におけるネットワーク･セキュリティ特性の決定と分析、及びネットワークがこれら特性を確実に有するようにするための方法の研究

(4) 情報システムに対する侵入の検出、科学捜査、及び攻撃に対する能動的応答と攻撃からの復旧

(5) セキュリティ･ポリシー研究

(6) 将来の情報システム攻撃の本質を予想する研究

---

[65] Air Force Research Laboratory Information Directorate Core Technical Competencies

[66] AFRL Information Institute

[67] Broad Agency Announcement, Air Force Office of Scientific Research

(7) ソフトウェアに既に埋め込まれた悪質なコードを発見する方法

2.4.2 大学

インディアナ大学（University of Indiana）
応用サイバーセキュリティ研究センター（Center for Applied Cyber Security Research）

法律学教授が主導する本センターは、サイバーセキュリティ研究に関する非常に学際的な見解を推進している。活動は、従来の情報技術に、ビジネスやアート、その他科学を含む学問を組み合わせた、情報科学部（School of Informatics）を中心に実施されている。本センターの研究分野は、フィッシング、ID盗難、テロといった現実世界の問題に焦点を置いている。本センターは、サイバーセキュリティをいかに改善するかだけでなく、その効率性やコスト、個人や一般大衆、経済に与える影響、そして他の価値や目的の研究にも関心があると述べている[68]。

インディアナ大学（University of Indiana）
応用身元管理研究センター（CAIMR: Center for Applied Identity Management Research）

CAIMRは、インディアナ大学を中心に、様々な研究機関が集まった組織である。その任務は、商取引、政府、及び国家安全に影響を与えるような身元（アイデンティティ）に関する問題の研究であり、中でも社会的意味合いとプロセス、そしてそれらに対処するために設計された技術や政策に焦点を置いている[69]。提携先には、複数の民間企業をはじめ、米シークレット・サービス（United States Secret Service）、インディアナ大学、テキサス大学オースチン校（University of Texas at Austin）がある。CAIMRは 2008 年 10 月に設立された、新しい研究センターである。以下に示すような、身元管理に焦点を当てた応用研究に取り組む計画である：①公安（Public Safety）：ID盗難、サイバー犯罪、コンピュータ犯罪、組織的犯罪グループ、文書詐欺、及び性犯罪者発見、②国家セキュリティ（National Security）：サイバーセキュリティとサイバー防衛、人身売買と不法移民、テロリスト追跡とテロの資金調達、③金融・法人不正行為（Financial and Corporate Fraud）：住宅ローン詐欺とその他金融犯罪、データ侵害、電子商取引詐欺、内部脅威とヘルスケア詐欺、④個人保護（Individual Protection）：ID盗難と詐欺。

---

[68] Center for Applied Cyber security Research, Indiana University

[69] Center for Applied Identity Management Research, Indiana University

カーネギー･メロン大学（Carnegie Mellon University）

CyLab

カーネギー･メロン大学は、米国における卓越したコンピュータ科学系大学の一つである。サイバーセキュリティに関する研究は、2003 年に設立された大学ベースのサイバーセキュリティ教育研究センターであるCyLabに集約して実施されている。CyLabは、NSF TRUSTのパートナーであることを示すNSFサイバートラスト・センター（NSF CyberTrust Center）であり、NSAの情報保証教育アカデミック・エクセレンス・センター（Center of Academic Excellence in Information Assurance Education）にも指定されている[70]。

研究領域には、モバイル機器のセキュリティ、次世代セキュア･インターネット、セキュアなネットワーク・コミュニケーション、セキュアなホーム･コンピューティング、機器とホット･スポットに対するセキュアなアクセス、信頼のおけるコンピューティング、そしてプライバシーと個人情報守秘義務の保護が含まれる。本研究に対し、同大学教員陣は、暗号、形式的方法、脅威保護モデリング、ビジネス・リスク分析と経済的含み、次世代応答・予測技術、ソフトウェア保証、及びソフトウェア・セキュリティの各分野におけるスキルを提供している。

CyLab と提携関係にある CMU 内部組織としては、ソフトウェア工学研究所（SEI: Software Engineering Institute）とその CERT コーディネーション･センター（CERT/CC: CERT Coordination Center CERT/CC）、情報・ネットワーキング研究所（INI: Information and Networking Institute）、及びセキュリティ技術向上のための国際協調（iCAST: International Collaboration for Advancing Security Technology）がある。また、CyLab には、陸軍研究局（Army Research Office）、全米科学財団（National Science Foundation）、国家安全保障局（National Security Agency）、DARPA、そして複数の民間企業が資金を提供している。

[70] CyLab, Carnegie Mellon University

南カリフォルニア大学（University of Southern California）
情報科学研究所（ISI: Information Sciences Institute）

ISI は、全米最大、かつ最も成功を収めている大学関連コンピュータ研究所の一つである。基礎および応用研究を手掛けており、大学での研究と、実社会でのプロトタイプ開発の間のギャップを橋渡しする役割を担っている。ISI プログラムの対象は、ネットワーク・サイバーセキュリティよりも格段に広いが、サイバーセキュリティは重要なコンポーネントとなっている。例えば、ISI は最近、DARPA から資金援助を受けて SPARTA と提携し、1.2.2 項で詳述した国家仮想領域（NCR: National Cyber Range）構築を支援した。

ISI はサイバ防衛技術試験研究ラボラトリー（DETERlab: cyber-Defense Technology Experimental Research Laboratory）テストベッドを維持している。DETERlab テストベッドは、次世代サイバーセキュリティ技術の研究開発を支援する、多目的試験インフラである。テストベッドによって、悪質なコードを使う実験を含め、幅広いネットワーク・セキュリティ・プロジェクトのための反復可能な中規模インターネット・エミュレーション試験が可能である。

DETERlab の資金は、国土安全保障省（DHS: Department of Homeland Security）と全米科学財団（NSF: National Science Foundation）が拠出する。DETERlab は、学究界、政府、及び産業界研究者による協調コミュニティを支援しており、システム及びネットワーク攻撃、そして対抗手段をともなう再現可能な試験の安全な実施を支えている。

2.4.3 企業

SRIインターナショナル（SRI International）

SRIは、大手の独立研究機関である。かつてはスタンフォード大学（Stanford University）と提携関係にあり、スタンフォード・リサーチ・インスティチュート（Stanford Research Institute）と呼ばれていた。注力領域の一つに、情報分析とインフラ保護（Information Analysis and Infrastructure Protection）があり、それにはサイバーセキュリティ、ネットワーク侵入検出、多層ソフトウェア・セキュリティ・システム、及びテストベッドが含まれる[71]。

[71] SRI Focus Areas, SRI International

SRIは、米国サイバーインフラ保護のためのセキュリティ技術開発を目的に、国土安全保障省（DHS: Department of Homeland Security）によって 2004 年に設立されたサイバーセキュリティ研究開発センター（Cyber Security Research and Development Center）を支援している。同センターは、政府及び民間産業、ベンチャー･キャピタル･コミュニティ、研究コミュニティ間の連携を通じ、その研究を行っている[72]。

SRIの侵入検出グループ（Intrusion Detection group）の研究注力分野の一つが、EMERALDである。EMERALDは、ネットワーク・システムにおける異常と誤用を検出するための最新ハードウェア及びソフトウェア・システムであり、DARPAから資金助成を受けている[73]。このシステムは、大型ネットワークの様々な層に配置可能な、高度に分散化され、かつ自主的に調整可能な監視及び応答モニターを利用する。これらのモニターは、シグネチャー（形跡）分析に確率的推論を組み合わせた、最新のイベント分析システムに寄与しており、インターネット上で最も広く使用されるネットワーク・サービスに対し、ローカライズされたリアルタイム保護を提供する。

テルコーディア･テクノロジーズ（Telcordia Technologies）

以前はベルコア（Bellcore）として知られたテルコーディア（Telcordia）は、世界の通信系企業に対し、ネットワーク・ソフトウェア、サービス、そして研究を提供する技術系企業である。同社のサイバーセキュリティ研究の大半は非公開だが、2、3 の研究例は公開されている。

---

[72] Cyber Security Research and Development Center, SRI International

[73] Event Monitoring Enabling Responses to Anomalous live Disturbances (EMERALD), SRI International

テルコーディアは 2008 年、100Gbps光ファイバー・ネットワーク向けに光暗号システムを発表した。このレベルのビットレートでは、電子暗号／復号は非常に困難である。テルコーディアのアプローチは、光信号を直接コーディング、かつ周波数変更を行いながら、光層においてコンパクト、かつプログラム可能な光プログラマーを利用するというものである。このプロトコル独立アプローチは、従来の高密度波長分割多重（DWDM: dense wavelength division multiplexing）及び光ネットワーキングと互換性のあることが示されている。研究は、DARPAのマイクロシステム技術局（Microsystems Technology Office）がその費用を出している[74]。テルコーディア研究から生まれたもう一つの製品は、IP保証（IP Assure）と呼ばれ、ネットワーク管理者を対象とした、適応性のあるIPネットワークの脆弱性とコンプライアンス評価システムである[75]。

ヒューレット・パッカード・ラボ（Hewlett-Packard Labs）

予算約 1 億 5,000 万ドルで運営されるヒューレット・パッカード・ラボ（Hewlett-Packard Labs）は 2008 年 3 月、プロジェクト数を削減し、製品への採用が早いと思われる結果を期待できるものだけに集中する“再編成”を発表した。HPラボは、英国のブリストルにシステム・セキュリティ・ラボ（Systems Security Lab）を持っており、そこでは、ほぼ全て非公開の内部プロジェクトが実施されている。ラボの目標は、信頼、セキュリティ、そしてプライバシーを重視した上で、信頼に値する情報システム環境を作ることである。ラボの研究領域には、他のHPラボのプログラムとつながりのあるアプリケーション・プロトコル設計、ファームウェアとオペレーティング・システム、ネットワーク・セキュリティ、そしてミドルウェアが含まれる。開発成果としては、オープン・ソース・ソフトウェアや、業界標準及び独自製品が挙げられる。HPのトラステッド・リナックス（Trusted Linux）製品は、ラボの研究から生まれた製品の一つである[76,77]。ラボのディレクターであるMartin Sadler氏は、ラボの研究について複数の公開報告書を作成している。

---

[74] Telcordia Develops Provable Security Technology for Emerging 100 GB/s Fiber Optic Networks, Reuters, October 20, 2008

[75] Telcordia IP Assure, Telcordia Technologies

[76] Hewlett-Packard Laboratories, Systems Security Lab

[77] Trust, Security and Privacy, Hewlett-Packard Laboratories, Systems Security Lab

2.5 まとめ

本報告で取り上げたプログラム・プロファイルには、米国ネットワーク・セキュリティ技術における 3 つの重要な傾向が反映されている。

第一に、ネットワーク･セキュリティ問題に対しては、魔法のような解決策は研究からは生まれないということである。研究に数百万ドルを投資し、さらに製品やサービスに数十億ドルを費やしたとしても、侵入やセキュリティ侵害、金銭やデータ盗難、そしてサービス妨害は、今後も重大な問題であり続けると考えられる。インターネットは一部利用者が思うほど匿名性は高くないが、利口な犯罪者は自らの足跡を隠してしまうため、捕らえられる可能性は彼らにとって容認できるほどのレベルと低い。今のところ、パケットの本当のソースを遡って見つける方法は、一般的には認められていない。アプリケーション･ソフトウェアやオペレーティング･システム、基本プロトコルにおける新しい脆弱性は次々と見つかっており、ネットワーク管理者やセキュリティ・オフィサーは、恒常的にそれに対応するために悪戦苦闘を重ねている。“ゼロ・デイ（Zero-day）”脆弱性は、特に危険が高い。脆弱性やセキュリティ上の突破口がそこにあるにも関わらず、解決策がまだないからである。

第二に、ほとんどのネットワーク･セキュリティ研究は、この状態に上手く対処する方法、つまり、モニタリングの改善、分析の改善、脆弱性特定と補修の迅速化に関して行われており、現状を基本的に変えるものではない。事実、侵入口は携帯電話を含む新たな対象へと広がっており、研究者の苦悩に輪をかけている。

第三に、多くの研究者がこの状況を理解し、よりセキュアなシステムを目指して、コンピュータ･ハードウェアとソフトウェア工学を改善する研究が一部で行われている。インターネットを再設計し、本質的セキュリティを高める研究も進められている。最終的な目標は、おそらくセキュアなシステムを構築することであり、そうなれば公的な方法を使い、設計がセキュアであり、システムが設計された通りに機能していることが検証される。しかし、すでに広範に導入された製品の本質的セキュリティを改善できるとすれば、それははるか先の話である。既存の投資、商慣行、そして社会的習慣の深さや広がり様はあまりにも巨大であり、何十年という時間で抜本的変化を期待するのは難しい。おそらく、真の大惨事がサイバー環境で起きれば、この予想も変わるかもしれないが、そうでもない限り、現状はこのまま続き、進化はゆっくり訪れることになると考えられる。

◆