「米国における情報サービス分野の産学官連携」

渡辺弘美@JETRO/IPA NY

1. はじめに

米国における情報サービス分野の産学官連携は活発に進められている。産官学連携の対象分野として、特に最近動きが活発なのはセキュリティ関連の連携である。また、セキュリティ以外にも、ソフトウェア・エンジニアリング、スーパー・コンピュータ及びグリッド・コンピューティング用アプリケーション開発なども産官学のパートナーシップが生かされている。活動内容も、R&D、グラント、人材育成、政策提起、標準、品質保証など多岐にわたっている。

また、連携の形態についてみると、そのパターンは多様でありそれぞれの連携ごとにユニークな特徴がある。

(1) 政府主導型

政府機関主導で行なわれる産学官連携の事例としては、中央情報局（CIA）によって設立されたベンチャー・キャピタルのインキュテル（In-Q-Tel）がある。これは、政府としては非常に斬新な試みとして注目されている。インテリジェンス・コミュニティーに必要な技術の開発・獲得において、民間のベンチャー・キャピタル・モデルを利用し、早期に自分たちに必要な技術の導入を実現しようとする試みである。この試みを通して、In-Q-Tel は、新たなセキュリティ技術開発企業に対する投資からリターンを得、そのリターンを生かして次なる投資に結びつけることで、技術開発を活性化させる新たな政府の「ビジネス・モデル」を創造している。

また、国家安全保障省（DHS）は、国防総省（DoD）の国防高等研究事業局（DARPA）のような存在である国土安全保障先端研究計画局（HSARPA）を設立し、セキュリティ技術に関する大学などの研究機関に対するグラント提供プログラムに加え、Office of Research and Development （ORD）を通じて、優秀な個人学生に対してスカラーシップ、フェローシップを提供する人材開発を積極的に進めている。

(2) 民間主導型

民間主導型で行なわれる産学官連携の例としては、National Cyber Security Partnership (NCSP)がある。同パートナーシップは DHS と IT 業界が共同主催した

会議に端を発して発足した。その後は、政府、大学などからの参加者を取り込みながら、Business Software Alliance (BSA)、Information Technology Association of America (ITAA) 、NetTech 及び商工会議所といった業界団体が中心となって、国家セキュリティ強化に向けた様々な政策提言をまとめている（「ニューヨークだより 2005 年 6 月」参照）。

また、ソフトウェア品質向上などのソフトウェア・エンジニアリングを専門とする民間主導のコンソーシアム Systems and Software Consortium (SSCI) は、主に軍事コントラクターが中心のメンバー企業から会費を募って運営資金とし、会員の情報交換の場の提供や、手法・ツールの提供、コンサルティングなど、ソフトウェア・エンジニアリング関係者の情報ハブとしての役割を担っている（「ニューヨークだより 2005 年 7 月」参照）。

(3)　大学主導型

大学を中心とした産官学提携の例としては、カーネギー・メロン大学に設立されたセキュリティ関連イニシアティブである CyLab がある。ソフトウェア・エンジニアリングで高い実績のある同大学が中心となり、学長自らが CyLab の運営に関わっている。シスコ・システムズ、ボーイングを含む 52 社の企業とのパートナーシップに加え、CERT や DHS のサイバー・セキュリティ部門とも密接な連携体制を組み、サイバー・セキュリティに対する広範な課題に対して産官学が協力して取組めるような体制を作り上げている。

次に、Institute for Information Infrastructure Protection (I3P)は、大学が設立当初から主導権をとってきた CyLab とは対象的に、設立当初の構想は大統領府及び連邦政府機関から生まれたが、長期的視点に立った情報セキュリティ R&D が必要とする考えから、ダートマス・カレッジに設立され、現在同大学が運営主体となり、大学や国立研究所などの非営利団体のみが参加資格をもつ団体として活動を進めている。

また、Globus Alliance は産学官連携を初めから見込んだ例ではなく、あるグリッド・システム構築技術に関する R&D プロジェクトが発展した結果、産官学連携に進んでいった例である。アルゴンヌ国立研究所とシカゴ大学の研究者が開始したグリッド・システム構築技術に対し DARPA が資金提供を決定。これを核として、Globus というグリッド技術標準や開発用ツールを作成する産学官パートナーシップへと結びついていった。政府機関としては NASA、民間企業ではマイクロソフト、IBM が参加している。

最後に、Fraunhofer Center, Maryland は、ドイツの産学官連携をベースとした最先端応用技術研究機構である Fraunhofer Gesellschaft の米国支局 Fraunhofer USA

によって設立された、ソフトウェア・エンジニアリングを専門とする研究センターである。欧州の産学官パートナーシップの仕組みを米国において展開させている。メリーランド大学が運営主体となり、米連邦政府機関（国防総省、NASA、NSF など）、米民間企業（モトローラ、ダイムラー・クライスラーなど）及び大学が参加している。

主導	プログラム名	分野	活動	産官学の参加状況		
				政府	大学	民間
政府	① In-Q-Tel	セキュリティ	ベンチャー投資	◎	○	○
	② DHS (HSARPA 及び ORD)	セキュリティ	R&D、人材開発他	◎	○	○
民間	① National Cyber Security Partnership（NCSP）	セキュリティ　他	政策提言他	○	○	◎
	② Systems and Software Consortium（SSCI）	ソフトウェア・エンジニアリング	品質他	○	○	◎
大学	① CyLab	セキュリティ	R&D	○	◎	○
	② Institute for Information Infrastructure Protection（I3P）	セキュリティ	R&D、人材開発	○	◎	○
	③ Globus Alliance	グリッド・アプリケーション	標準	○	◎	○
	④ Fraunhofer Center, Maryland（FC-MD）	ソフトウェア・エンジニアリング	R&D	○	◎	○

（◎運営主体、○参加している団体）

2.　産学官連携の事例

上記の産学官連携の個々の事例について、それらの背景、目的、組織構成、予算、そしてこれまでの成果を、特に人的交流や知識共有などで工夫されている点に焦点を当ててまとめる。

(1)　政府主導型

①　In-Q-Tel

＜背景・目的＞

In-Q-Tel とは、1999 年に CIA によって立ち上げられた非営利の IT ベンチャー投資機関である。国家のセキュリティを守るために必要とされる先端技術イノベーションが名の知れない新興企業に眠っていることに着目し、In-Q-Tel は米国のインテリジェンス・コミュニティが使える技術をもつベンチャー企業への投資を行う目的で創設された。

CIA では、In-Q-Tel を通して米国のインテリジェンス・コミュニティを「スーパー情報エンタープライズ（Super Information Enterprise）」に一変させることを狙っており、「いつでもどこでもセキュアな状態で柔軟（Flexible）に、携帯性（Mobile）に優れた相互運用可能（Interoperable）を持つ技術を実現可能とする」という目標が設定さている。

In-Q-Tel における主なフォーカス・エリアは、以下のようになっている。

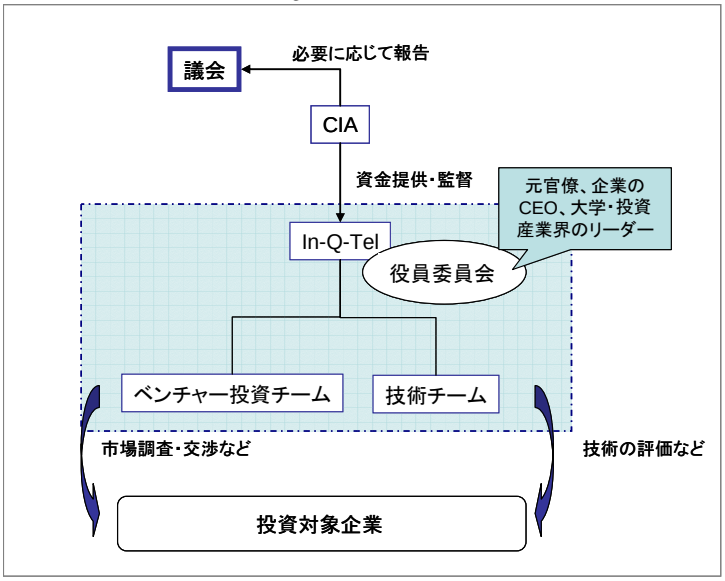
- 知識管理＆ビジュアライゼーション（Knowledge Management and Visualization）
- サーチ＆ディスカバリー（Search and Discovery）
- セキュリティ＆プライバシー（Security and Privacy）
- 分散データ収集（Distributed Data Collection）
- 地理空間技術（Geospatial Technologies）

＜組織構成・予算＞

In-Q-Tel は CIA による資金支援を受けているが、政府からは独立した機関であり、独自の CEO と理事会（Board of Trustees）によって運営・管理されている。この理事会は、元政府高官や企業の CEO、大学や投資業界からのエキスパート合計 12 名から構成されている。

In-Q-Tel の活動は、技術の市場調査や投資先企業との交渉などを行う「ベンチャー投資チーム」と、投資先の候補となる技術を発見・評価する「技術チーム」によって支えられている。ベンチャー投資チームは、ベンチャー投資家や企業におけるベンチャー投資の経験者、また、技術チームはエンジニアやハイテク起業家などの多様なエキスパートから構成されている。

In-Q-Tel の仕組み



In-Q-Tel の予算は、創設当時 2,700 万ドルであったが、2004 年度は 6,000 万ドルまで増加している。

CIA は In-Q-Tel の監督を行い、その評価結果を議会に報告することがある。最近では 2000 年に、議会の要求により CIA はセキュリティ専門の非営利コンサルティング会社 BENS 社（Business Executives for National Security）に投資効果に関する調査を委託。BENS 社は 2001 年 6 月、結果を議会に報告している。

＜パートナーシップのメカニズムと成果＞

In-Q-Tel はベンチャー・キャピタルという方法を採用することで、研究資金のすべてを政府負担とするのではなく、その一部を提供し、残りを民間セクターが負担するような仕組みを選択した。設立 5 年間の実績では、In-Q-Tel が投資を行った研究開発に対し、その 8 倍に当たる額が民間投資家から投資されたとしている。これは In-Q-Tel が、連邦政府がバックアップしている機関であるということに加え、CIA をはじめとするインテリジェンス・コミュニティーの需要を熟知し、セキュリティ関連技術に対する高い審美眼をもつ In-Q-Tel が投資しているという事実を「高い信頼性のお墨付き」であると評価している民間投資家の姿勢を示すものと見ることができる。

これまでに In-Q-Tel は 100 種類以上の技術を CIA に提供、全米 25 州にわたって合計 80 社の IT ベンチャー企業に投資を行っている。投資を受けた企業には、以下のようなものがある。

- A4Vision 社：3D 顔面認識技術など
- IatroQuest 社：空気中の汚染物検出・感知技術など
- Paratek 社：ワイヤレス・デバイスの開発など

新たな技術のインキュベーションに貢献するだけでなく、In-Q-Tel はこれまでの投資からリターンを得ている。こうしたリターンを、In-Q-Tel の経営に回すのではなく、CIA などのインテリジェンス・コミュニティーに役立つ次なる技術開発企業のために投資している。In-Q-Tel が登場するまで、連邦政府関によるベンチャーキャピタルは存在しなかった。しかし In-Q-Tel の成功から、2004 年には米国陸軍が OnPoint というモバイル用電力及びその他エネルギー関連技術開発向けのベンチャー・キャピタルを立ち上げている。また、同年 President's Commission on Moon, Mars and Beyond （通称：Aldridge 委員会）は NASA に対して、In-Q-Tel と類似組織の設立を検討すべきであるとの提言をしている。

② 国土安全保障省（DHS）の HSARPA 及び ORD

＜背景・目的＞

米国土安全保障省（DHS）の中の主たる研究開発部門として機能する科学技術部門（Science and Technology Directorate：S&T 部門）には、化学・生物・放射能・核攻撃を予防・発見し、被害が発生した場合に、その被害を最小限に止める

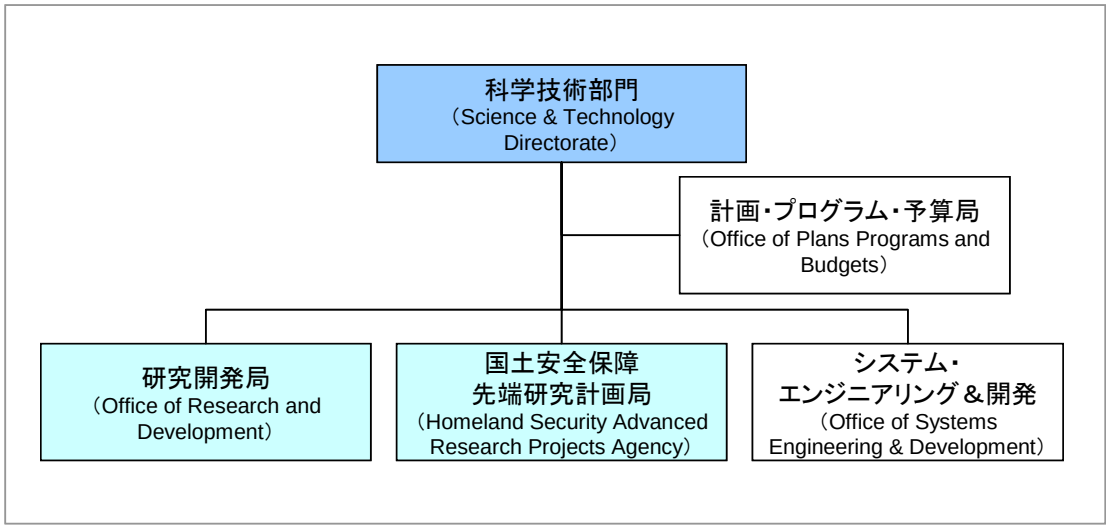
ための最先端、高性能、低コストのシステムを開発し導入することや、科学技術における米国リーダーシップをサポートする、といった戦略目標を持っている。

この DHS の科学技術部門において、先端研究への資金提供を行なう国土安全保障先端研究計画局（Homeland Security Advanced Research Projects Agency: HSARPA）および、リーダーシップや戦略的パートナーシップを通じて研究・開発・試験・評価のプログラムを行う研究開発局（Office of Research and Development: ORD）の 2 局が、業界、学界、政府との連携を積極的に進めている。

＜組織構成・予算＞

HSARPA および ORD の含まれる科学技術部門は以下のような構成となっている。

国土安全保障省科学技術部門内の構成



また、それぞれの組織全体の予算は不明だが、サイバー・セキュリティ R&D プログラムの 2004 年度予算は 1,800 万ドルとなっている。

＜パートナーシップのメカニズムと成果＞

HSARPA は、公的機関や民間機関、商業機関、連邦助成を受けた研究開発機関、大学を対象に、研究やプロトタイプ作成を目的として、調達、契約、グラント、共同作業の機会を提供している。これまでの実績として、サイバー・セキュリティ研究開発（CSRD）プログラムが行われたほか、業界や学界を対象としたワークショップも数多く実施している。HSARPA は、「インターネットを含めた米国のサイバーインフラを保護するための技術の開発および導入は、国土安全保障省が重視する分野の一つである」とした上で、以下の 3 つの分野、合計 7 つのテクニカル・トピック・エリア（Technical Topic Areas: TTA）で研究開発に参加する団体の募集を発表（BAA 04-17）した。この BAA04-17 の予算は、450 万

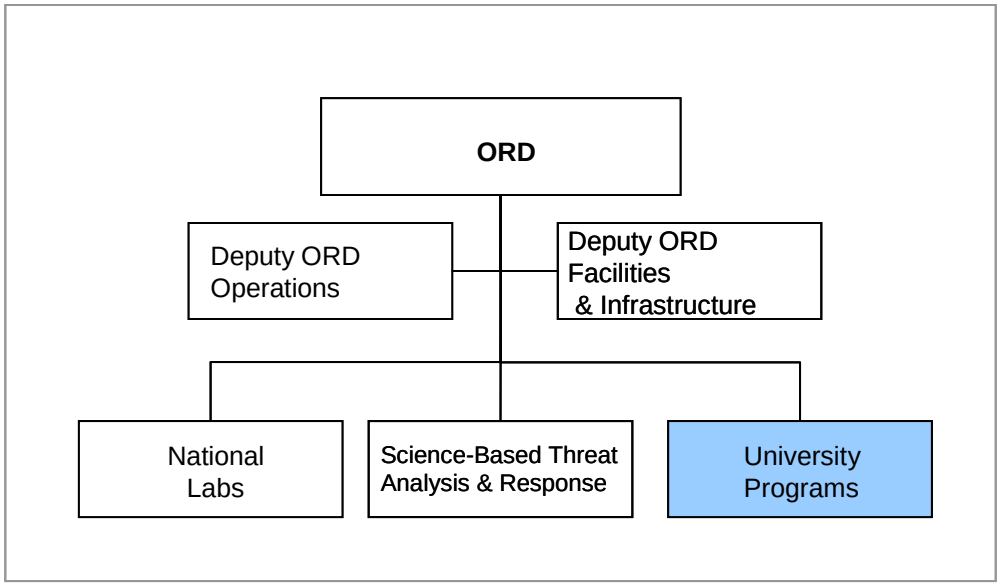
ドルとなっている（BAA04-17 への応募は 2004 年 9 月に締め切られ、2005 年 1 月にグラント先が決定されることになっているが、最終的なグラント先については、現時点では公開されていない）。

HSARPA によるサイバーセキュリティ研究開発（CSRD）の募集分野

分野	TTA
＜カテゴリー1＞ システム・セキュリティ・エンジニアリング	TTA1：脆弱性の予防
	TTA2：脆弱性の発見および矯正
	TTA3：サイバーセキュリティ評価
＜カテゴリー2＞ オペレーショナル・システムのセキュリティ	TTA4：重要インフラ保護のためのセキュリティと信頼性
	TTA5：ワイヤレス・セキュリティ
＜カテゴリー3＞ 捜査および予防のための技術	TTA6：ネットワークの科学捜査
	TTA7：ID 窃盗防止のための技術

一方、ORD は、国土安全保障上、「知識の創出、統合、拡散、移転および知識労働者の育成を通じ、研究開発を加速させる」ことを目的とし、大学プログラム（University Programs）、国立研究所（National Laboratories）、科学ベースの脅威分析および対策（Science-Based Threat Analysis and Countermeasures）といった 3 つのプログラムを推進している。

ORD の組織構成



このうち、産学連携については、大学プログラムにおいて、国土安全保障を強化するために大学ベースの協調システムを構築することを目的とし、優秀な人材に奨学金を提供する「スカラー＆フェロー・プログラム」（DHS Scholars and Fellows Program）と、大学ベースで資金提供を行う「国土安全保障エクセレン

ス・センター」（Homeland Security Centers of Excellence）が行われている。スカラー＆フェロー・プログラムを通じて、2004 年には以下のような分野で大学生と大学院生合計 105 名の学生に奨学金が提供されている（奨学金の合計金額については現時点では未公開）。

ORD のスカラー＆フェロー・プログラムの申し込み数と授与者数

学問	大学生		大学院生	
	申し込み数	授与者数	申し込み数	授与者数
Computer & Information Science	40	4	43	6
Civil, Computer, Electrical, Materials Eng	71	12	99	9
Bio, Chemical, Mechanical, Aerospace Eng	67	9	78	7
Life Sciences	88	11	65	10
Mathematical Sciences	31	3	16	2
Physical Sciences	43	5	41	9
Psychology	44	5	42	4
Social Sciences	54	8	64	1
合計	438	57	448	48

(2)　民間企業主導型

④　National Cyber Security Partnership（NCSP）

＜背景・目的＞

NCSP は大学・企業を含む民間セクターと政府間及び、サイバー・セキュリティに関連する複数分野にまたがる専門家間のパートナーシップを通じて、国家のサイバー・セキュリティ強化を図るための共通のフレームワークや提言をまとめることを目的とする産学官パートナーシップである。

NCSP 設立は、2003 年 12 月 3 日にカリフォルニア州サンタクララにおいて開催された National Cyber Security Summit に端を発する。同サミットは、DHS の Information Analysis and Infrastructure Protection Directorate の一部である National Cyber Security Division（なお、同 Division については DHS 内で次官補ポストに格上げされることが 2005 年 7 月 13 日に発表されている）と NCSP の主要メンバーである Business Software Alliance (BSA)、Information Technology Association of America (ITAA) 及び米商工会議所が共同主催者となって開催された。同サミットでは、2003 年 2 月にホワイトハウスから発表された「国家サイバー・セキュリティ戦略（National Strategy to Secure Cyberspace）」をどのようにして実現していくかについて、産学官から専門家が集まって議論を深め、民間セクターと政府が共同で米国の国家サイバー・セキュリティを強化することを狙ったものであった。

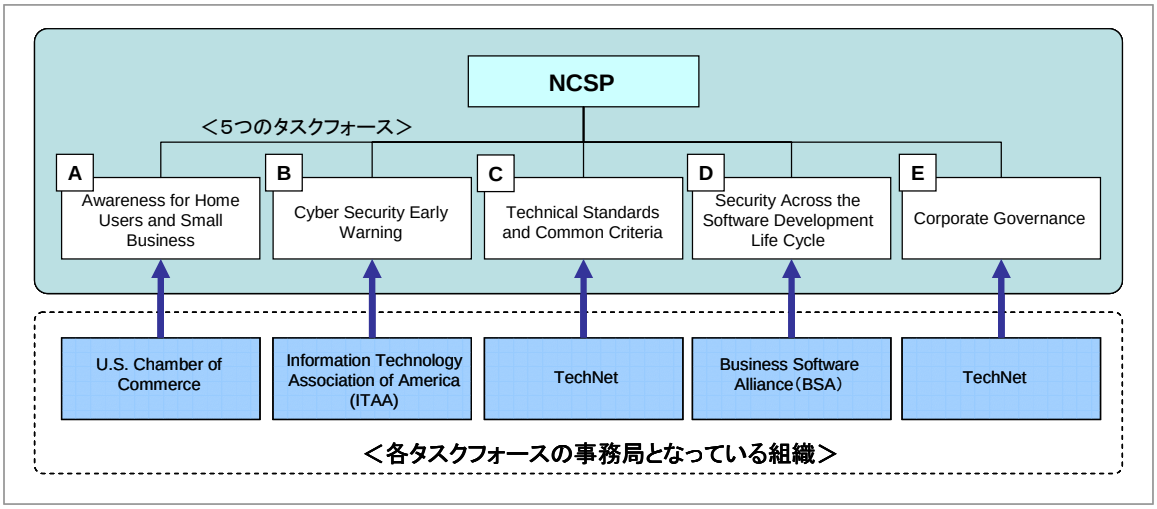
この目標を実現するに当たり、同サミットでは以下の５つのタスクフォースを結成、サミット終了後、NCSP がこれらのタスクフォースの事務局として設立された。

（A） 一般家庭および中小企業ユーザへの啓蒙（Awareness for Home Users and Small Businesses）
（B）サイバー・セキュリティに対する早期警戒（Cyber Security Early Warning）
（C）技術標準（Technical Standards and Common Criteria）
（D）ソフトウェア開発ライフサイクルにおけるセキュリティ（Security Across the Software Development Life Cycle）
（E）コーポレート・ガバナンス（Corporate Governance）

＜組織構成・予算＞

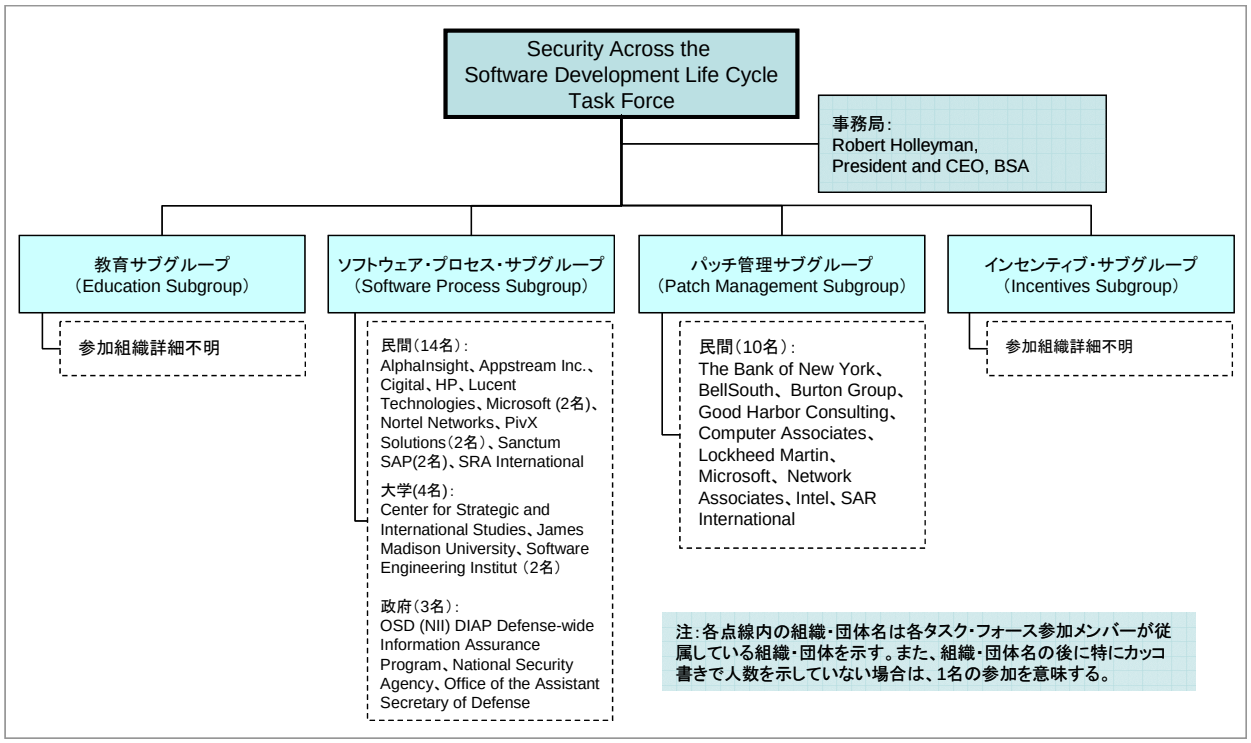
NCSP は Business Software Alliance (BSA)、Information Technology Association of America (ITAA) 、NetTech 及び米商工会議所（U.S. Chamber of Commerce）の 4 つの組織が運営主体として、持ち回りで上記５タスクフォースの事務局の役割を担っている。同様に、運営資金についても主に上記の４つの組織からの寄付に頼っている。

NCSP のタスクフォースとその支援組織



各タスクフォースのメンバーは、産官学から集まった専門家 25 - 30 名で構成されている。構成例として、「(D) Security Across the Software Development Life Cycle グループ」は以下の通り。

Security Across the Software Development Life Cycle の構成



＜パートナーシップのメカニズムと成果＞

NCSP は各タスクフォースごとに度々ミーティングを開催し、2004 年に以下の提言を次々に発表している。

各タスクフォースによるレポートの提言内容

タスクフォース	レポート
(A)　一般家庭および中小企業ユーザへの啓蒙（Awareness for Home Users and Small Businesses）	対象ユーザ別に主に以下のような勧告を提案。 ・中小企業：サイバー・セキュリティのガイドブックを開発、配布し、市場ベースのインセンティブを促進する。 ・ホームユーザ：サイバー・セキュリティに関する全国的なキャンペーンを実施する。 ・大手企業：国土安全保障省と協力し、大手企業 CEO を対象とした地域ごとの国土安保フォーラムを開催し、サイバー・セキュリティにおける CEO の役割を強調する。 ・生徒・学生：教育団体や教育委員会、教師などと協力し、生徒や学生向けに、サイバー・セキュリティに関する適切な行動意識を高めるような教材を開発、配布する。

(B)　サイバー・セキュリティに対する早期警戒（Cyber Security Early Warning）	サイバー・セキュリティの脆弱性や事故などに関する情報共有網を拡大し、情報共有プロセスを促進し、重要な情報を迅速に拡散するための「早期警戒コンタクト・ネットワーク（Early Warning Contact Network: EWAN）」や、政府、業界、大学のセキュリティ専門家を集め、互いの文化的障害を克服し、脆弱性の予防、発見、対応などを共同で行う「全米危機対応調整センター（National Crisis Coordination Center: NCCC）」の新設を勧告。
(C)　技術標準（Technical Standards and Common Criteria）	タスクフォース内にある 5 つの作業部会(WG)ごとに勧告。 ・Common Configuration WG：優れたセキュリティ情報の文書化や管理の奨励、業界と政府の協調の強化など、28 点を勧告。 ・Research WG：ソフトウェアの欠陥を発見するためのツール開発研究への政府の資金提供など、4 点を勧告。 ・Best Practices for Technical Standards WG：「情報セキュリティ管理モデル」「製品セキュリティ・モデル」「ガバナンス・ガイドライン」「シニア・マネジャ向けガイドライン」などテーマ別に、これまでに発表されているガイドラインを編纂。 ・Equipment Deployment & Architecture Guidelines WG：「業界は協力して、推奨セキュリティ機器の明確な標準やセキュアな IP ネットワーク・インフラ導入のベストプラクティスを開発すること」「業界は協力して、サイバー・セキュリティのレベルや状況を判断するための標準を開発すること」の 2 点を勧告。 ・Common Criteria, NIAP Review and Metrics WG：CC(Common Criteria for Information Technology Security Evaluation)や NIAP(National Information Assurance Partnership)について、6 つの分野で 35 点を勧告（NIAP: NIST と NSA によるイニシアティブで、費用効果の高いセキュリティ・テストや評価プログラムを通じて、情報システムやネットワークに対する消費者の信頼レベルを引き上げることを目標としている）。
(D)　ソフトウェア開発ライフサイクルにおけるセキュリティ（Security Across the Software Development Life Cycle）	「セキュアなソフトウェア開発を向上させ、教育機関や研究機関における能力を強化するため、新たな官民のコラボレーションを発足させる」「ソフトウェアのスペック/設計/利用上の欠陥をある程度削減させるソフトウェア開発プロセスを採用する」「パッチング・プロセスのベストプラクティス 10 点を採用する」「セキュリティを成果評価要素の一つとする」など 4 つのサブグループで計 21 点を勧告。
(E)　コーポレート・ガバナンス（Corporate Governance）	情報セキュリティプログラムの導入に関して、企業としての包括的なガバナンス・フレームワークを開発。導入を推奨するとともに、企業は情報セキュリティ・ガバナンスに対するコミットメントを示すよう勧告。

④　Systems and Software Consortium（SSCI）

＜背景・目的＞

System and Software Consortium（SSCI）は、1980 年代に設立された非営利団体（設立当時の名称は Software Productivity Consortium(SPC)で、2005 年 3 月に現在の名称に変更）で、民間業界や政府機関と協力しながら、ソフトウェアやシステム開発における複雑かつ広範な問題に対処する上で有益な分析、アドバイス、ツールなどを提供している。

SSCI の運営資金を提供する加盟企業・機関のうち、政府機関としては、労働統計局（Bureau of Labor Statistics）、米航空宇宙局（NASA）、防衛コントラクト管理局（Defense Contract Management Agency）、国家安全保障局（National Security Agency: NSA）などが、民間企業としては、BAE システムズ（BAE Systems）、ゼネラル・ダイナミクス（General Dynamics）、ロッキード・マーティン（Lockheed Martin）、レイセオン（Raytheon）などが、そして大学機関としては、ジョージ・メイソン（George Mason）大学、ジョンズ・ホプキンス（Johns Hopkins）大学、南カリフォルニア（Southern California）大学などがある。

これらの加盟企業・機関は、SSCI を通じて、ソフトウェアやシステムを効率的に開発するための、プロセスや手法、ツール、トレーニングにアクセスすることが可能となっている。また、SSCI によるプログラムを通じて、政府機関と民間企業の交流も実施され、新たなパートナーシップ作りに貢献している。

＜組織構成・予算＞

SSCI は、以下の 3 つの分野を中心に、加盟企業・機関に対して、サービスを提供している。

(a) プロセスの改善から価値を見出す（Realizing Value from Process Improvement）：CMM（Capability Maturity Model、能力成熟度モデル）、CMMI（Capability Maturity Model Integration、能力成熟度モデル統合）、Six Sigma などプロセス改善のためのあらゆるフレームワークに対応し、各フレームワークにおいてプロセス成熟度を向上させるための専門知識、プロセス、トレーニング、ツールを提供する。
(b) 複雑なシステムのためのライフサイクル戦略（Lifecycle Strategies for Complex Systems）：リスクの最小限化、ソフトウェアやシステムの構造の正当性の立証、システム・インターフェースの定義、戦略の評価、業務達成保証の強化など、複雑かつ高度なソフトウェアやシステムの開発の効率性を高めるためのツールやサービスを提供。
(c) システム統合およびソフトウェア・エンジニアリング（Integrating Systems & Software Engineering）：テクニカル管理の統合、品質保証、データのコンフ

ィギュレーションおよび管理、エンジニアリング・プロセスに関するサービスや専門知識、トレーニングを提供。

また、加盟企業・機関のパートナーシップ作りの一環として、共通の関心を持つ政府機関と業界を引き合わせる州情報技術コンソーシアム（State Information Technology Consortium）なども実施している。同コンソーシアムは州政府の資金提供を受けている。

なお、SSCI の運営資金を拠出する加盟企業・機関のメンバーシップ制度は、以下の 3 つに分類されている。また、そのほかに、政府機関や大学、研究機関が所属する提携機関（Affiliation）がある。年会費について、2002 年に発表された記事で、「ベーシック会員は 2 万 5000 ドル、サービス会員は 10 万ドル、正規会員は 10 万ドルに企業の年間売上に基づく一定金額（年間売上が 60 億ドルのある企業の場合で 20 万ドル）」となっている。

SSCI のメンバーシップ制度の概要

メンバーシップ	概要
正規会員（Full Membership）	SSCI のあらゆる知的財産や製品（研修、ツールキット、手法、エンジニアリング・テンプレートなども含む）を利用できるほか、理事会や技術諮問委員会に代表者を派遣できる。
サービス会員（Service Membership）	企業向けのサービスや研修などのプログラムの一部を費用ベースで受けられる。正規会員を検討している企業・団体が対象で、期間は 1 年間に限定されている。
ベーシック会員（Basic Membership）	プログラムへの一部参加や一部使用が可能（年間費用に応じて）。費用ベースで研修やコンサルティング、技術移転支援のサービスを受けることも可能。
提携機関（Affiliation）	連邦政府機関や大学、研究機関などが所属する。SSCI の研修やコンサルティング活動で利用されるガイドブックやテクニカル・レポート、ソフトウェアを受け取ることができる。また、メンバー・フォーラムや年次ユーザ会議にも参加できる。

＜パートナーシップのメカニズムと成果＞

ソフトウェアおよびシステム開発の効率性やプロセス成熟度を向上させるための SSCI の手法やツール、専門知識などは、さまざまな企業や機関で利用されている。たとえば、ボーイングの総合防衛システム／ソフトウェア・エンジニアリング部門（Integrated Defense Systems, Software Engineering Division）では、SSCI のサービスを受けることにより、開発ライフサイクルの早期に欠陥や問題点を発

見および修正することが可能になり、開発における試験コストを削減することが可能になったという。SSCI は、試験専門家によるワークショップを開催し、多くのプロジェクトで直面する問題や対処すべき要点などを見つけ出し、その後 Boeing 社の試験官らによる試験手法や戦略の構築を支援した。

また、前述の州情報技術コンソーシアムを通じて、ワイオミング州政府機関の IT 事業をめぐり、民間企業との競争にさらされた同州 IT 部門に対して、競争力を強化するためのプロジェクト管理研修が行われたケースもある。本件において、SSCI は、数日間にわたる「プロジェクト管理研修」を実施し、管理スタッフやサポートスタッフへ研修を行うと同時に、これらのノウハウが継続的に利用されるよう、師弟プログラム（mentoring program）も導入された。

(3)　大学主導型

④　CyLab

＜背景・目的＞

カーネギー・メロン大学（Carnegie Mellon University）は、2003 年 10 月ホームユーザからスモールビジネス・ユーザ、大手企業ユーザまで、さまざまなセクターのあらゆるコンピューターの安全を確実にすることを目的としたイニシアティブである CyLab の始動を発表した。これにより、それまで複数の部門下で行われていた関連の研究活動が CyLab という一つのイニシアティブの下で行われるようになった。

CyLab は、官民のパートナーシップによる「測定可能かつ有用で、持続可能性と信頼性のあるセキュアなコンピューティングおよびコミュニケーション・システムの開発」と「あらゆる層への教育活動」に取り組んでいる。

＜組織構成・予算＞

CyLab の活動には、カーネギー・メロン大学の情報ネットワーク研究所（Information Networking Institute）、電気・コンピューター・エンジニアリング（Electrical and Computer Engineering）、統計部（Department of Statistics）など、８つの部門から、30 名以上の教員、20 名以上の研究スタッフ、100 名以上の卒業生が参加している。また、企業とのパートナーシップ制度を取り入れると同時に、CERT Coordination Center（CERT/CC）とも密接に活動している。さらに、CERT/CC を通じて、国土安全保障省の全米サイバー・セキュリティ部門（National Cyber Security Division: NCSD）（なお、同 Division については DHS 内で次官補ポストに格上げされることが 2005 年 7 月 13 日に発表されている）と民間セクターのパートナーシップで、国家情報インフラの保護を目的として活動する US-CERT とも連携しているなど、政府機関との連携体制も確立されている。

企業とのパートナーシップ制度には、3 つのレベルがあり、その内容は以下のようになっている。

CyLab のパートナーシップ制度

パートナー	概要
創立パートナー（Founding Partner）	CyLab の研究議題の決定に関与するとともに、知的財産の商業化の権利を得る。CyLab 内に従業員を派遣することも可能。
戦略パートナー（Strategic Partner）	年会費 10 万ドルで最低 3 年間のメンバーシップが義務付けられている。
パートナー（Partner）	年会費 2 万 5000 ドルで最低 3 年間のメンバーシップが義務付けられている。

企業パートナーは、そのレベルに応じて、CyLab 企業メンバーどうしのネットワーキング、CyLab（およびカーネギー・メロン大学）生徒のリクルート、CyLab ワーキング・グループへの参加、といった特典が与えられる。現在の企業パートナーは、シスコ・システムズ、bp、ボーイング、インテル、ヒューレット・パッカードなど 52 社となっている。

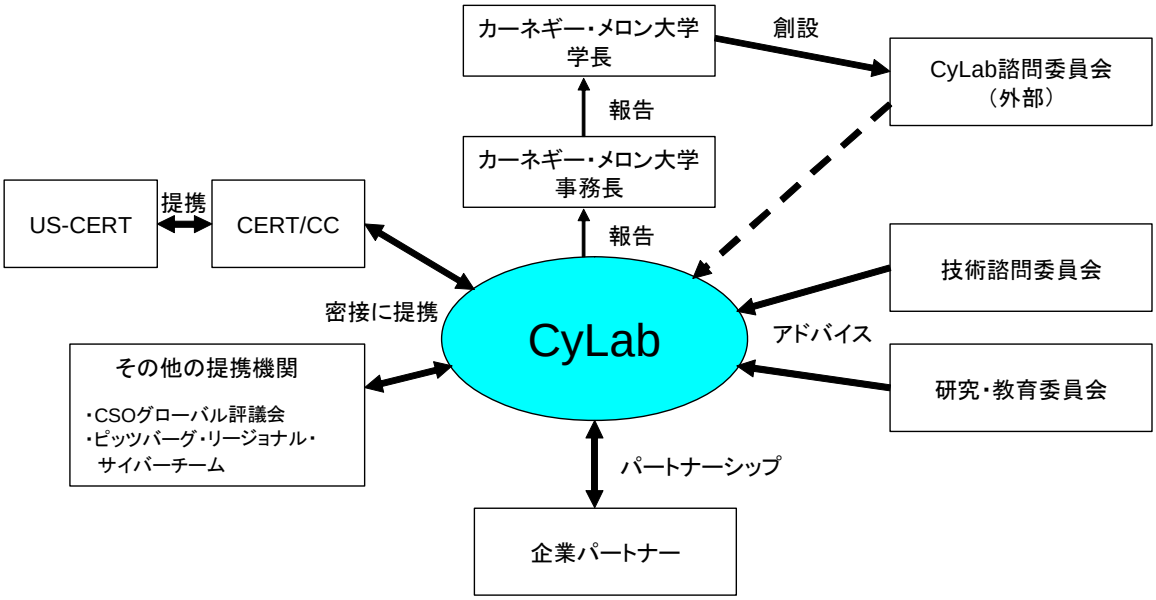
CyLab のプログラムは、連邦政府機関からの助成金や慈善活動団体からの寄付、企業パートナーシップなどによって支えられている。具体的な予算は不明だが、カーネギー・メロン大学はサイバー・セキュリティの研究および対応プログラム活動として、2002 年に 250 万ドル、2003 年に 600 万ドルの連邦助成を受けている。

＜パートナーシップのメカニズムと成果＞

CyLab は、企業パートナーや CERT/CC、US-CERT と提携しているほか、CSO グローバル評議会（Global Council of CSOs）やピッツバーグ・リージョナル・サイバーチーム（Pittsburgh Regional Cyber Team）とも協力している。また、CyLab はカーネギー・メロン大学の事務長（provost）へ直接報告し、これを受けて事務長が学長（president）へ報告する体制になっている。

学長により、同大学の理事および業界や政府の任命者など外部者で構成される CyLab 諮問委員会（Advisory Board for CyLab）が創設されている。CyLab はまた、技術諮問委員会（Technical Advisory Committee）や研究・教育委員会（Research and Education Committee）といった委員会のアドバイスも受けている。

CyLab を中心としたパートナーシップのメカニズム



CyLab は企業パートナーや政府支援機関との共同作業により、次世代の対応・予測テクノロジーや、柔軟性や自己回復力のあるネットワークおよびコンピューティング・システム、ソフトウェアの業績管理や保障のためのテクノロジーやプラクティス、データおよび情報プライバシーといった幅広い分野の研究プロジェクトに取り組んでいる。具体的には、陸軍研究局（Army Research Office）の支援と CERT/CC の協力を受けて行われている「複雑なネットワーク・システムにおける脅威ダイナミクスに関する分析」や、企業の情報やケーススタディなどを利用し、ソフトウェアの脆弱性に関する情報を公開する際のルール決定プロセスのモデル化やソフトウェアの脆弱性に対する企業の反応のモデル化を行う「ソフトウェアの脆弱性に対する反応」プロジェクトなどがある。

④　Institute for Information Infrastructure Protection（I3P）

＜背景・目的＞

Institute for Information Infrastructure Protection（I3P）の構想が生まれたのは、1998 年に遡る。当時、大統領の科学技術諮問委員会（President's Committee of Advisors on Science and Technology: PCAST）が、「情報セキュリティの R&D に関する投資は、ビジネス上の目前のニーズに対応するものが中心となっている」とし、連邦政府の助成金を受け、政府や民間の研究所から独立した機関を設置し、国家情報セキュリティとしての必要条件を明確にし、現行の R&D 活動を分類化し、米国の R&D ポートフォリオの問題点を発見・認識させることを提案した。2000 年には、国防総省の要請を受け調査分析を行った防衛分析研究所（Institute for Defense Analyses: IDA）が、PCAST が提案した機能を有する組織として、「Institute for Information Infrastructure Protection（I3P）」の新設を勧告した。一

方、国家安全保障会議（National Security Council: NSC）と科学技術政策局（Office of Science and Technology Policy: OSTP）も 2000 年初期に I3P のコンセプトに関する白書を作成し、米国標準技術局（National Institute for Standards and Technology: NIST）の資金提供を受けた非政府機関による I3P の設立を提案した。

こうした経緯を受け、米議会は 2001 年に、ニューハンプシャー州のダートマス・カレッジ（Dartmouth College）内に I3P を設立するための予算を承認、同年 9 月に I3P が発足した。I3P は現在、米国の情報インフラを大惨事から保護するための R&D 活動を促進し、全国的な R&D プログラムのコーディネイトや、大学、業界、政府をつなぐ橋渡し役として貢献している。

＜組織構成・予算＞

I3P には、I3P の会議の議事進行を務め、通常の団体の最高経営責任者（CEO）に相当する権限を持つオフィサーとして議長（Chairman）が、また、I3P の議事録作成や記録管理を行う事務長（Secretary）がいる（ダートマス・カレッジの事務長（provost）が議長を任命し、議長が事務長を任命）ほか、政府系研究機関や大学研究機関などがメンバーとして参加している。I3P のメンバーの条件の一つとして「非営利団体」があり、民間企業を含む営利団体や政府機関は含まれていない。現在の I3P のメンバーは、以下の 24 機関となっている。

I3P の加盟機関

種別	機関名（所属や関連機関）
政府系	・Los Alamos National Laboratory（エネルギー省） ・Pacific Northwest National Laboratory（エネルギー省） ・Sandia National Laboratory（エネルギー省）
大学および教育機関系	・Center for Advanced Research in Information Security（イリノイ大学） ・Center for Education and Research in Information Assurance and Security（パーデュー大学） ・Center for Information Security（タルサ大学） ・Computer Security Research Laboratory（カリフォルニア大学デイビス校） ・Critical Infrastructure Protection Project（ジョージメイソン大学ロースクール） ・Georgia Tech Information Security Center（ジョージア・テック） ・H. John Heinz III School of Public Policy and Management（カーネギー・メロン大学） ・Information Security Institute（ジョンズホプキンス大学） ・Information Security Laboratory（オレゴン州立大学） ・Information Trust Institute（イリノイ大学） ・Institute for Civil Infrastructure Systems（ニューヨーク大学） ・Institute for Security Technology Studies（ダートマス・カレッジ） ・MIT Lincoln Laboratory（MIT） ・Software Engineering Institute（カーネギー・メロン大学） ・Stanford University Computer Science Department（スタンフォード大学） ・University of California at Berkeley（カリフォルニア大学バークレー校） ・University of Virginia（バージニア大学）

その他	・Mitretek Systems（非営利研究機関） ・SRI International （非営利研究機関） ・MITRE Corporation（非営利研究機関） ・RAND Corporation（非営利シンクタンク）

メンバーシップの機会はあらゆる非営利団体および教育機関に提供されており、希望団体は申請申込書を提出した後、毎年 6 月に行われるコンソーシアムの年次会合でメンバーによる投票が行われ、決定する。メンバーは、コンソーシアムの研究活動に参加し、I3P が資金提供する研究プロジェクトなどに参加する機会が与えられる。メンバーは、I3P が行う会合に年間で 50%以上参加しなくてはならない、といった規定があるが、会費などの財政的負担はない。

I3P は、国土安全保障省と NIST の資金提供を受けて、ダートマス・カレッジによって運営されている。年間予算については不明だが、前述の NSC と OSTP による I3P 創設提案では年間 5000 万ドルの資金提供が試算されている。

＜パートナーシップのメカニズムと成果＞

I3P は、情報インフラが抱える脆弱性に対処する努力の一貫として、以下のような取り組みを行っている。

- 差し迫ったサイバー・セキュリティ問題へ対応するための、教育機関や業界、政府のコラボレーションの育成。
- 全米規模の研究プロジェクトの開発および管理。
- 博士号取得研究者や教員、研究科学者を対象とした研究フェローシップの提供。
- サイバー・セキュリティや情報インフラ保護問題に関するワークショップや会議などの開催。
- I3P のメンバーや情報セキュリティ問題に取り組んでいるその他の機関へ向けて、情報を配信・共有するための、オンライン・ツールによる知識基盤の強化およびサポート。

また、I3P はこうした活動の成果の一つとして、2003 年 1 月に「サイバー・セキュリティ研究開発議題（Cyber Security Research and Development Agenda）」を発表している。同報告書は、サイバー・セキュリティ上、放置または未開発となっているさまざまな問題のうち、最も優先度の高い R&D 分野を見つけ出すことを目的として作成されたものである。「情報インフラのセキュリティを強化するために、新たな R&D や現行の R&D の増強が必要とされる分野」として、以下の 8 つが挙げられている。

- エンタープライズ・セキュリティ管理（Enterprise Security Management）

- 第三機関同士の信頼の確立（Trust Among Distributed Autonomous Parties）
- セキュリティ上の資産や脆弱性に関する発見および分析（Discovery and Analysis of Security Properties and Vulnerabilities）
- セキュアなシステムおよびネットワークの対応と回復（Secure System and Network Response and Recovery）
- 追跡、判別、法医学の面における研究（Traceback, Identification, and Forensics）
- ワイヤレス・セキュリティ（Wireless Security）
- メトリックスおよびモデリング（Metrics and Models）
- 法規、政策、経済的側面からの研究（Law, Policy, and Economic Issues）

④　Globus Alliance

＜背景・目的＞

1994 年、エネルギー省国立研究所の１つであるアルゴンヌ国立研究所（Argonne National Laboratory）（エネルギー省の傘下にありシカゴ大学によって運営）の Rick Stevens 氏と、イリノイ大学シカゴ校（University of Illinois at Chicago）の Tom Defanti 氏が、11 の高速研究開発ネットワークをリンクさせ、全国規模のグリッドを構築するというアイデア（I-WAY）を提案し、その後、アルゴンヌ国立研究所の Ian Foster 氏が I-WAY のユーザがアプリケーションを操作できるようにするためのプロトコルを開発、これが成功し、DARPA（国防省高等研究計画局）からの資金提供へとつながった。1996 年に、グリッド・システム構築のための技術や規格標準、システムなどの研究開発を実施する「Globus Alliance」として活動を開始し、1997 年には最初のグリッド開発用ツールキット「Globus Toolkit」が完成した（最新版は、Globus Toolkit version 4）。

「Globus Toolkit」はグリッド・システムやアプリケーションを構築するためのオープン・ソースのツールキットで、ソフトウェアおよびモニタリング／発見／管理／セキュリティ／ファイル管理のためのリソースが盛り込まれている。Globus Toolkit は米国や欧州などにおける大規模なグリッド・システムの導入プロジェクトに広く利用されている。

Globus Alliance は、アルゴンヌ国立研究所内に拠点を構え、さまざまな大学、連邦政府機関、民間企業が提携、支援している。

＜組織構成・予算＞

Globus Alliance には、下記のような大学、政府機関、民間企業が参加している。

Globus Alliance の参加機関

研究機関／大学	・アルゴンヌ国立研究所（数学・コンピューター科学部門） ・南カリフォルニア大学（情報科学研究所） ・シカゴ大学（分散システム研究所） ・エディンバラ大学（University of Edinburgh、スコットランド） ・パラレル・コンピューター・センター（Center for Parallel Computers）
政府機関	・全米コンピュテーショナル科学同盟（National Computational Science Alliance） ・NASA 情報パワーグリッド・プロジェクト（Information Power Grid project） ・全米先端コンピュテーショナル・インフラストラクチャ同盟（National Partnership for Advanced Computational Infrastructure）
民間企業	・IBM ・マイクロソフト

また、Globus Alliance の研究開発を支援するスポンサー機関として、以下のような政府機関、民間企業が挙げられている（具体的な支援金額については不明）。

Globus を支えるスポンサー機関

政府機関	・DARPA、エネルギー省（科学局　数学・情報・コンピュテーショナル科学部門＝Mathematical, Information, and Computational Sciences Division） ・NSF（コンピューター・情報科学・エンジニアリング総局＝Directorate of Computer, Information Sciences and Engineering） ・NSA（情報パワーグリッド・プロジェクトを通じて） ・英国 e サイエンス・グリッド・コア・プログラム（UK e-Science Grid Core Programme） ・スウェーデン研究評議会（Swedish Research Council） ・スウェーデン王立技術研究所（Swedish Royal Institute of Technology）
民間企業	・IBM ・マイクロソフト ・シスコ・システムズ

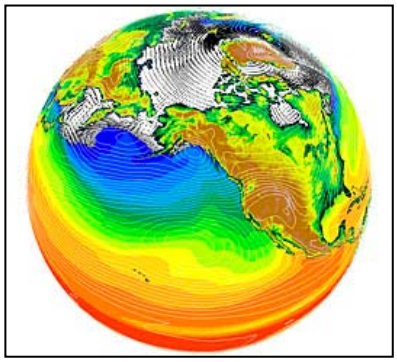
また、2004 年には、Globus ソフトウェアのサポート・サービスを提供する会社、Univa Corporation が設立され、2005 年には Globus Toolkit を支援する企業

（ヒューレット・パッカード、IBM、インテル、サンマイクロシステムズなど）で構成される Globus Consortium が発足している。

＜パートナーシップのメカニズムと成果＞

オープン・ソースのツールキットである Globus Toolkit は、Globus Alliance のメンバーや世界のその他の関係者によって開発が進められている。たとえば、最新版である Globus Toolkit 4 の開発においては、Globus Alliance のメンバーに加え、Condor プロジェクト（遊休状態のワークステーションを利用して大量のコンピューター･タスクをこなすためのツール）、ヒューレット・パッカード、ローレンス・バークレー国立研究所（Lawrence Berkeley National Laboratory）、ノーザン・イリノイ大学（Northern Illinois University）といった企業や団体の協力・貢献があった。

また、これまでに、富士通、ヒューレット・パッカード、IBM、NEC、Oracle といった企業が GlobusToolkit を利用したグリッド戦略に取り組んでいるという。さらに、Globus は、①天文・観測、②化学、③災害対策エンジニアリング、④気候研究、⑤コラボレーション（グリッド）、⑥コンピューター科学、⑦エコロジー、⑧地質学、⑨インフラストラクチャー、⑩医薬、⑪海洋学、⑫物理学といった分野において実施されているさまざまなプロジェクトに関与している。具体的な利用例として、地球気候変動の研究に関連した情報を作成、提供する地球システム・グリッド（Earth System Grid: ESG）が、海氷域や海氷の動き、海面温度（色）、海面気圧（曲線）などを示す画像（右図）の作成に Globus Toolkit を利用している。



④　Fraunhofer Center, Maryland（FC-MD）

＜背景・目的＞

FC-MD は 1998 年に、メリーランド大学の付属機関として、Fraunhofer USA によって設立された非営利団体である。ドイツで 1949 年に官民パートナーシップの応用研究／技術移転促進を目的として設立された最先端応用技術研究機構である Fraunhofer Gesellschaft が、1994 年に米国支局として Fraunhofer USA を設立した。

Fraunhofer USA のセンターは全米に５ヶ所ある。メリーランド州の FC-MD に加え、デラウェア州（Center for Molecular Biotechnology）、マサチューセッツ州（Center for Manufacturing Innovation）、ミシガン州（Center for Laser Technology 及び Coatings and Laser Applications）にも展開している。

FC-MD は５つのセンターのうちで唯一ソフトウェア・エンジニアリングを対象とするセンターである。「科学／エンジニアリングの手法をソフトウェア・エンジニアリングに応用する。過去の教訓を将来の選択肢に活かす。組織的学習を改善のための鍵とする」をビジョンとし、民間企業や政府機関、大学・研究機関などとのコラボレーションにより、ソフトウェア・エンジニアリング分野の応用研究や技術移転を行っている。

FC-MDが提携している機関・企業としては、南カリフォルニア大学（University of Southern California）、メリーランド大学ボルチモア郡校（University of Maryland, Baltimore County）、ワシントン・カレッジ（Washington College）、マサチューセッツ工科大学（MIT）、国防省（未来戦闘システム（Future Combat System: FCS）や軍医療システム（Military Health System: MHS））、全米科学財団（National Science Foundation: NSF）、NASA、ボーイング、モトローラ（Motorola）、ノキア（Nokia）、ダイムラー・クライスラー（Daimler Chrysler）などがある。

＜組織構成・予算＞

FC-MD のエグゼクティブ・ディレクター、Victor Basili 氏は、メリーランド大学のコンピューター科学教授である。そのほか、科学者、教員、学生など 16 名のテクニカル・スタッフと、4 名の総務スタッフがいる。

年間予算は 250 万ドル（基本資金は 60 万ドル）となっている。また、年収入伸び率は年間 32%、コントラクトによる収入の伸び率は年間 49%となっている。

＜パートナーシップのメカニズムと成果＞

FC-MD では、強みを発揮できる能力分野として、①エクスペリエンス・ファクトリー、②業績評価、③テクノロジー成熟度評価、④プロセス改善の 4 つを挙げている。その主な内容と顧客およびパートナーは以下の通りである。

FC-MD の能力分野とその顧客／パートナー

エクスペリエンス・ファクトリー（Experience Factory）	
内容	「学習的組織を形成する」「経験に基づいた基盤やツールを構築する」「知識を利用して、プロジェクト・マネジャーやデベロッパー向けの情報の分析や統合を行う」など、「経験」をソフトウェア・ビジネスの強化やその他のプロジェクトへ応用することを狙いとした、FC-MD が開発した手法。
顧客／パートナー	NSF、国防省、ボーイング、SAIC、UMD、USC など。

業績評価（Measurement）	
内容	・企業や組織の目標をソフトウェア・プロジェクトの目標と統合させ、その進展具合を評価する。 ・関係者のあらゆるレベルで意思決定をサポートする。 ・プロジェクト・レベルのデータのうち、トップ・レベルで利用できるようなタイプのものを統合する。 ・GQM（Goal-Question-Metric）や BSC(Balanced Scorecard)などさまざまな業績評価方法を利用、統合する。
顧客／パートナー	UMD、USC、NASA、国防省など。
テクノロジー成熟度評価（Evaluating Technology Maturity）	
内容	・さまざまなテクノロジーの利用を試みる。 ・一定の環境におけるそれらのテクノロジーの適合度を決定する。
顧客／パートナー	UMD、USC、MIT、NASA、DARPA（国防省）、国防省など。
プロセス改善（Process Improvement）	
内容	・エクスペリエンス・ファクトリー手法やその他の評価手法、マネジメント技法、モデリング・ツールなどを使いながら、プラクティスの開発や導入の定義付けや改善を行う。
顧客／パートナー	UMD、USC、国防省、NSF、メリーランド州政府および州内企業など。

UMD=University of Maryland, USC=University of South Carolina

これらの 4 つの分野において、世界クラスの機関や企業とパートナーを組み、さまざまなテクノロジーを組み合わせながら、具体的なニーズを発見し、適切なツールや技法を応用することで能力の強化に取り組んでいる。たとえば、メリーランド州のビジネス経済開発局（Department of Business and Economic Development）と協力し、「メリーランド・ソフトウェア業界コンソーシアム（Maryland Software Industry Consortium）」プロジェクトを開始している。このコンソーシアムは、州内の機関・組織が、システム／ソフトウェア･エンジニアリングに関するプラクティスや、ソフトウェア関連の製品やサービスの品質を強化するのを支援することを目的とし、ソフトウェア・エンジニアリングに関するリソースを提供するものである。

(参考資料)

http://www.in-q-tel.com/about/index.htm
http://www.in-q-tel.com/about/vision.html
http://www.in-q-tel.com/team/bot.html
http://www.businessweekasia.com/technology/content/may2005/tc20050510_4072_tc_210.htm
http://www.bens.org/images/NQTel_Panel%20Rpt.pdf
http://www.in-q-tel.org/about/index.htm#In-Q-Tel?s_Venture_Capital_Approach
http://www.onpoint.us/
http://www.nasa.gov/pdf/60736main_M2M_report_small.pd
http://www.dhs.gov/dhspublic/display?content=1756
http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0533.xml
http://www.hsarpabaa.com/Solicitations/Financial-and-Contracting-Questions.pdf
http://www.hsarpabaa.com/Solicitations/CyberBAA_0908_FINAL.pdf
http://www.dhs.gov/interweb/assetlibrary/DHS-SnT-OrgOverview.pdf
http://www.orau.gov/dhsed/
http://www.cyberpartnership.org/about-faq.html
http://www.us-cert.gov/press_room/detail/summit.html
http://www.cyberpartnership.org/init-aware.html
http://www.cyberpartnership.org/init-early.html
http://www.cyberpartnership.org/TF4TechSummary.pdf
http://www.cyberpartnership.org/SDLCSUMM.pdf
http://www.cyberpartnership.org/InfoSecGov4_04.pdf
http://www.systemsandsoftware.org/ssci/default.asp?Section=about_us
http://www.systemsandsoftware.org/pub/memberaffiliate.asp
http://www.systemsandsoftware.org/ssci/default.asp
http://www.state-itc.org/index.html
http://www.baselinemag.com/article2/0,1397,794116,00.asp
http://www.systemsandsoftware.org/casehistories/member/BoeingStLouis.pdf
http://www.systemsandsoftware.org/casehistories/member/WyomingProjectManagement.pdf
http://www.cmu.edu/PR/releases03/031022_newinitiative.html
http://www.cylab.cmu.edu/default.aspx?id=151
http://www.cylab.cmu.edu/default.aspx?id=152
http://www.cylab.cmu.edu/default.aspx?id=250
http://www.cylab.cmu.edu/default.aspx?id=9
http://www.cylab.cmu.edu/default.aspx?id=282
http://www.cylab.cmu.edu/default.aspx?id=53
http://www.thei3p.org/about/charter.html
http://www.thei3p.org/about/
http://www.thei3p.org/about/bylaws.html
http://www.thei3p.org/about/members.html
http://www.thei3p.org/about/membershipguide.html

http://www.fcw.com/fcw/articles/2003/0127/web-cyber-01-31-03.asp
http://www.globus.org/toolkit/about.html
http://www.globus.org/faq.php#involved
http://www.globus.org/alliance/sponsors.php
http://www.globus.org/toolkit/contributors.html
http://www.globus.org/alliance/projects.php
http://www-unix.globus.org/alliance/impact/
http://www.fraunhofer.org/
http://fc-md.umd.edu/Fraunhfoer%20Briefing1.pdf
http://fc-md.umd.edu/fcmd/index.html

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