参考資料3

米国における情報セキュリティ研究開発戦略の動向について

「平成 23 年度情報セキュリティ産業の活性化方策に係る調査」

報告書より抜粋

2012 年 6 月 22 日

目次

1.研究開発戦略に係る国際動向調査

本章では米国のサイバーセキュリティの研究開発戦略に係る最新動向を整理する。

まず、1.1 において米国の研究開発戦略が策定された背景となる、米国のサイバーセキュリティ政策の全体動向について、オバマ政権のサイバーセキュリティ政策の基盤となる戦略文書「Cyberspace Policy Review」で示されたアクションプランの取組みに沿って示す。その上で 1.2 において、アクションプランの 1 つである米国のサイバーセキュリティの研究開発戦略の策定について、その策定プロセス及び 2011 年 12 月に策定された戦略の内容を紹介する。1.3 では 1.1 と 1.2 の内容を時系列で整理する。

また、1.4 では米国のサイバーセキュリティの研究開発における今後の動向の参考として、2012 年 2 月に公表された 2013 年度の予算の要求状況を紹介する。

最後に 1.5 において米国の研究開発戦略に係る調査結果を踏まえ、日本の「情報セキュリティ研究開発戦略」の拡充及び将来の新たな戦略策定時の参考となる視点を抽出している。

1.1.米国のサイバーセキュリティ政策の全体動向

本項では、米国のサイバーセキュリティの研究開発戦略策定の背景として、サイバーセキュリティ政策全体の最新動向を整理する。

オバマ大統領は就任後、サイバーセキュリティを政権の優先政策課題と位置付け、2009 年 2 月ブッシュ政権時代に策定された「Comprehensive National Cybersecurity Initiative（CNCI）」[1]を含む連邦政府の情報通信インフラ防衛の取組みに対するトップダウンの見直しを国家安全保障会議（National Security Council: NSC）及び国土安全保障会議（Homeland Security Council）に指示し[2]、2009 年 5 月にその結果を「Cyberspace Policy Review」として公表した[3]。この中で、米国のサイバーセキュリティ政策を推進するための短期のアクションプランとして表 1-1 に示す 10 項目を指示した。

[1] White House, “Comprehensive National Cybersecurity Initiative”（2008 年 1 月）
http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative
[2] White House, “FACT SHEET: Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure”（2009 年 5 月）
http://www.whitehouse.gov/the-press-office/cybersecurity-event-fact-sheet-and-expected-attendees
[3] White House, “Cyberspace Policy Review”（2009 年 5 月）
http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

表 1-1「Cyberspace Policy Review」で示された短期アクションプラン

(1)	国家のサイバーセキュリティ政策・活動の調整に責任を有する担当者（サイバーセキュリティ調整官）を指名する。当該担当者の下で組織間のサイバーセキュリティ関連の戦略・政策を調整するために、NSC 担当部局を設置し、当該担当者は、NSC と国家経済会議（National Economic Council: NEC）を兼務する。
(2)	情報・通信インフラの安全を確保するための国家戦略を見直す。「CNCI」の取組みに対しても継続的な評価を行い、取組みが適切であれば「CNCI」の方針を維持する。
(3)	サイバーセキュリティを大統領が行うマネジメントの優先事項の 1 つとして位置付けるとともに、パフォーマンスの評価手法を確立する。
(4)	NSC 内のサイバーセキュリティ部局に、プライバシー・人権の担当者を指名する。
(5)	サイバーセキュリティ関連の優先課題に対して省庁横断的な法的分析を実施するため、適切な省庁横断的メカニズムを構築する。
(6)	サイバーセキュリティを促進する国家的な啓発・教育キャンペーンを開始する。
(7)	国際的なサイバーセキュリティ政策の枠組みにおける米国政府の役割を確立し、サイバーセキュリティの活動に取組むイニシアチブ構築に向け国際的連携を強化する。
(8)	サイバーセキュリティインシデントに対する対応計画を準備し、合理的、効果的な官民パートナーシップを強化するための対話を開始する。
(9)	デジタルインフラのセキュリティ、信頼性、障害からの回復性及び trustworthiness を向上させる game-changing[4]な技術に焦点を置いたサイバーセキュリティの研究開発戦略の枠組みを策定する。研究コミュニティによるイベントデータへのアクセスを可能にし、ツール開発、理論検証及び効果的なソリューションの確立を促進する。
(10)	プライバシーや人権に配慮したサイバーセキュリティに基づく ID マネジメントに係るビジョンと戦略を構築する。

上記アクションプランに対する 2012 年 3 月時点の進捗状況を以下に整理する[5]。

(1) サイバーセキュリティ調整官の指名及び NSC 担当部局の設置

オバマ大統領は、2009 年 12 月、サイバーセキュリティ調整官として、地方・連邦政府・民間企業でサイバーセキュリティ関連の要職を務め、ブッシュ政権下で 2003 年まで大統領重要インフラ防護理事会（President's Critical Infrastructure Protection Board）副議長及び White House のサイバースペースセキュリティ特別顧問を務めた Howard Schmidt 氏を指名した。以後、米国のサイバーセキュリティ政策は Schmidt 氏の主導で進められている。さらに National Security Staff（NSS）にサイバーセキュリティ調整官をトップとした、サイバーセキュリティ部局（Cybersecurity Directorate）を新たに設置した。サイバーセキュリティ部局では NEC 等の経済担当部局と連携し、また行政管理予算局（Office of Management and Budget: OMB）や科学技術政策局（Office of Science and Technology Policy: OSTP）との緊密な協力体制も構築している。

(2) 情報・通信インフラの安全を確保するための国家戦略の見直し

2010 年の White House の公表[5]によれば、サイバーセキュリティ部局は、CNCI と連邦

[4] game-changing な技術とはサイバースペースにおける trustworthiness を飛躍的に高め、サイバーセキュリティ対策の根本的な展望を変える技術として位置づけられている。

[5] White House, “Cybersecurity Progress after President Obama’s Address”（2010 年 7 月）
http://www.whitehouse.gov/administration/eop/nsc/cybersecurity/progressreports/july2010

政府のサイバーセキュリティに係る主な役割と責任を定めた「National Security Presidential Directive 54 / Homeland Security Presidential Directive 23（NSPD-54 / HSPD-23）」のアップデート作業を進めているとしている。

(3) 大統領のマネジメントにおけるサイバーセキュリティの優先及びパフォーマンス評価手法の確立

2010年4月NSSとOMBは連邦情報セキュリティマネジメント法(Federal Information Security Management Act: FISMA）に関する新たなガイドラインを公表した[6]。これにより、これまで各連邦政府機関で静的かつ紙ベースで行われていたFISMAの準拠状況の報告は、同年10月以降自動化ツールCyberScopeを用いリアルタイムで行われることとなった。

(4) サイバーセキュリティ部局におけるプライバシー・人権担当の指名

2010年7月、プライバシー・人権担当者がNSSの中に設置された(担当者名は非公表)。

(5) サイバーセキュリティ関連の優先課題に対する省庁横断的な法的分析の実施

2010年10月国防総省（Department of Defense: DOD）は、米国の陸軍・海軍・空軍・海兵隊が個別に持っていたサイバー部隊を統合し、米軍の情報通信インフラに対するサイバー攻撃に対応する統合部隊Cyber Command（USCYBERCOM）を新たに設置した。さらに、DODはDHSと国家のサイバーセキュリティにおける協力体制を構築し、両省間で人、機器、設備等（Cyber Command含む）について相互に支援し合うことを定めた覚書[7]を取り交わしている。2011年7月には、DODがCyber Commandによるオペレーションも含めた、国家のサイバー空間におけるオペレーションに関する防衛戦略[8]を公表している。その他にも、連邦政府内では、原子力規制委員会(Nuclear Regulatory Commission: NRC)と連邦エネルギー規制委員会（Federal Energy Regulatory Commission: FERC）が電力網や原子力プラントにおけるサイバーセキュリティ対策の協力体制に関する覚書[9]を交わすなど、組織を超えたサイバーセキュリティの連携体制の構築が進んでいる。

(6) 国家的なサイバーセキュリティの啓発・教育キャンペーンの実施

2010年3月国立標準技術研究所（National Institute of Standards and Technology:

---

[6] OMB, “FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management”（2010年4月）
http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf

[7] DOD/DHS, “MEMORANDUM OF AGREEMENT BETWEEN THE DEPARTMENT OF HOMELAND SECURITY AND THE DEPARTMENT OF DEFENSE REGARDING CYBERSECURITY”（2010年9月）
http://www.carlisle.army.mil/DIME/documents/DoD%20-%20DHS%20CYBER%20MOA.pdf

[8] DOD, “DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE”（2011年7月）
http://www.defense.gov/news/d20110714cyber.pdf

[9] NRC/FERC, “MEMORANDUM OF AGREEMENT between the U.S. NUCLEAR REGULATORY COMMISSION and the FEDERAL ENERGY REGULATORY COMMISSION”（2009年9月）
http://www.ferc.gov/legal/maj-ord-reg/mou/mou-us-nucr-09.pdf

NIST）は、サイバーセキュリティ専門家の育成・活用、サイバーセキュリティの国民意識の向上及び教育機関におけるサイバーセキュリティ教育の推進を目指したプロジェクト National Initiative for Cybersecurity Education（NICE）を開始し、2011 年 8 月にはドラフト版のプログラムの戦略文書[10]を公開している。以下に NICE の概要を示す。

NICE プログラムの概要	
目的	国家のセキュリティを強化するため、健全なサイバープラクティスを使用した、運用可能で、持続的かつ継続的に進歩していくサイバーセキュリティの教育プログラムを策定すること。プログラムは、以下の 4 つのコンポーネントから構成される。
内容	**Awareness：**国家のサイバーセキュリティの意識向上（DHS が主導） 「Stop. Think. Connect」キャンペーン、10 月の Cybersecurity awareness month の設定など、一般市民向けに安全なインターネット利用を訴える活動を行う。
	Education：公式なサイバーセキュリティ教育（ED 及び NSF が主導） 幼稚園から高等教育、職業プログラムまでを対象として、サイバーセキュリティの教育を行い、民間・政府機関に対してスキルを有する人材を供給する。具体的には NSF の Advanced Technology Education（ATE）プログラムや NSA / DHS による National Centers of Academic Excellence におけるサイバーセキュリティ関連の教育事業などを強化する。
	Federal Workforce Structure：サイバーセキュリティ要員構造（DHS が主導） サイバーセキュリティに係る業務や就職、キャリアパス戦略等を定義する。連邦政府の要員に関しては、Office of Personnel Management（OPM）、連邦政府以外の政府要員に関しては DHS、民間に関しては SBA（中小企業局）、労働省（DOL）及び NIST が担当する。
	Training and Professional Development：サイバーセキュリティ要員のトレーニングと専門能力開発（DOD、ODNI 及び DHS が主導） 産学官の連携の下、既存の連邦政府のサイバーセキュリティ要員の強化トレーニング及び専門能力開発を行う。一般の IT 利用向け、IT インフラの運用・管理・情報保証向け、法執行及び対諜報活動向け及び特別サイバーセキュリティオペレーション向けの 4 つのエリアで活動が行われる。

(7) サイバーセキュリティにおける国際連携の強化

2011 年 5 月 White House は、セキュアで信頼性が高く、新しいイノベーションに開かれた国際的な情報通信インフラの整備を目指す国際戦略「International Strategy for Cyberspace[11]」を公表した。

(8) サイバーセキュリティインシデントへの対応計画の策定

2010 年 9 月 DHS は、暫定版の国家サイバーインシデント対応計画「National Cyber Incident Response Plan（NCIRP）[12]」を策定し、同月これに基づいたサイバー演習「Cyber Storm III」が実施されている[13]。

[10] NIST, “National Initiative for Cybersecurity Education Strategic Plan”（2011 年 8 月）
http://csrc.nist.gov/nice/documents/nicestratplan/Draft_NICE-Strategic-Plan_Aug2011.pdf
[11] White House, “International Strategy for Cyberspace”（2011 年 5 月）
http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
[12] DHS, “National Cyber Incident Response Plan”（2010 年 9 月）
http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf
[13] DHS, “Fact Sheet: Cyber Storm III: National Cyber Exercise”
http://www.dhs.gov/files/training/cyberstorm-iii.shtm

(9) サイバーセキュリティの研究開発の枠組みを策定

2009 年から開始された NITRD CSIA における 2 年半の検討を経て、2011 年 12 月、国家科学技術会議（National Science and Technology Council: NSTC）は、米国のサイバーセキュリティの研究開発戦略「Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity R&D Program[14]」を公表した。（1.2 参照）

(10) プライバシーや人権に配慮したサイバーセキュリティに基づくアイデンティティ・マネジメントに係るビジョンと戦略の構築

2011 年 4 月 White House は、サイバースペースにおける信頼性の高いアイデンティティのための国家戦略「National Strategy for Trusted Identities in Cyberspace（NSTIC）[15]」を公表した（ドラフト版は 2010 年 6 月に公表）。

2011 年はガバナンスやプライバシー保護の観点に関する机上検討が行われており、2012 年からは複数のパイロットプロジェクトが開始される予定となっている。NSTIC の 2012 年度の予算は 1,650 万ドル、2013 年度の予算要求額は 2,450 万ドルである[16]。

NSTIC の概要	
戦略のビジョン	個人と組織は信頼性、プライバシー、選択とイノベーションを促進する形で、セキュアで効率的で使いやすく相互運用可能なアイデンティティソリューション（Identity Ecosystem）を利用する。
Identity Ecosystem について	Identity Ecosystem は個人と組織が合意された標準に従って各々のデジタルアイデンティティ（及びデバイスのデジタルアイデンティティ）を取得・認証することで、個人と組織が互いに信頼し合えるオンライン環境として位置付けられている。基本原則は、①プライバシー保護と参加の自由、②相互運用性があること、③セキュアかつ回復力があること、④安価でかつ簡単に使えることの 4 点である。開発・運営は民間主体で進められ、2016 年 1 月の運用開始を目指している。 ● Identity Ecosystem の運用 Identity Ecosystem は開発・運用ともに民間主導で進められ、運用における主要なプレーヤ（アイデンティティ情報を管理・提供する事業者、ユーザの属性情報を保管・提供する事業者、アイデンティティ情報を利用してサービスを提供する事業者等）も民間で構成される。連邦政府は民間による Identity Ecosystem の開発・導入をサポートするとともに、Identity Ecosystem を利用したサービスを積極的に導入し事例を示すことで活動を支援する。また、Identity Ecosystem の相互運用性、セキュリティ、プライバシー保護の観点からのサポートや、国際的な協力の取り付け等も政府側の役割とされている。国家プログラムオフィス（National Program Office: NPO）は NIST に置かれ、国家通信情報管理局（National Telecommunications and Information Administration: NTIA）も主に公共政策面及びプライバシー保護面で活動に参加している。 ● Identity Ecosystem に期待される効果 個人：利便性の向上、プライバシー保護、セキュリティの向上等 民間：イノベーション（Identity Ecosystem を利用した新たなビジネスモデルの開拓）、効率化（サービス提供側の生産性向上とコスト削減の実現）、サービスの信頼性向上等 政府：政府のオンラインサービスに対する国民の満足度向上、経済成長、公衆安全等

[14] NSTC, “Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity R&D Program”（2011 年 12 月）
http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf
[15] White House, “National Strategy for Trusted Identities in Cyberspace”（2011 年 4 月）
http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
[16] NIST, “NIST FY 2013 Budget Overview”（2012 年 2 月）
http://www.nist.gov/director/ocla/upload/FINAL-FY2013_Congressional_Budget_Rollout_Presentation.pdf

1.2.米国のサイバーセキュリティの研究開発戦略

本項では、米国のサイバーセキュリティの研究開発戦略について紹介する。

NSTC は、1.1 に示した「Cyberspace Policy Review」の短期アクションプランの指示に従い、2011 年 12 月米国のサイバーセキュリティ研究開発戦略「Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity R&D Program」を公表した。以下に同研究開発戦略の策定プロセス、戦略の概要及び構成、研究テーマ等の詳細を示す。

1.2.1. 策定プロセス

研究開発戦略の策定に当たり、まず「Cyberspace Policy Review」で求められた game-changing な技術に焦点を置いた研究テーマの検討が行われている[17]。研究テーマの検討は、連邦政府の情報通信分野の研究開発を省庁横断的に取りまとめるネットワーキング情報技術研究開発プログラム（Networking and Information Technology Research and Development: NITRD）の 10 の研究分野のうち、サイバーセキュリティと情報保証（Cyber Security and Information Assurance: CSIA）の参加機関（サイバーセキュリティの研究開発を行う連邦政府の機関）によって進められた。CSIA には参加機関のサイバーセキュリティ関連のプログラムマネージャ等から構成される省庁横断型作業部会（CSIA IWG: Interagency Working Group on Cyber Security and Information Assurance）及び参加機関の代表者から構成される上席管理グループ（CSIA SSG: Cyber Security Information Assurance Research and Development Senior Steering Group）が設置されており、研究テーマの具体的な検討作業はこれらの組織を中心に進められた。戦略策定の体制を図 1-1 に示す。

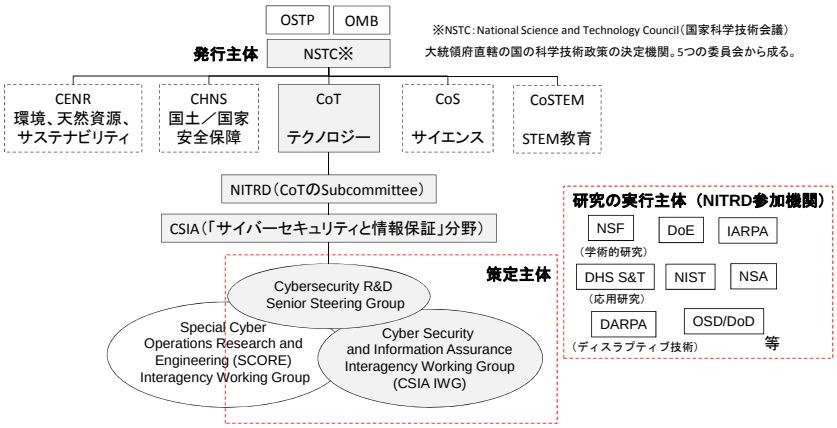

図 1-1 研究開発戦略策定の体制

（出典：各種資料を基に三菱総合研究所作成）

[17] この「テーマ」とは従来の研究開発の「課題・問題（Hard Problem）」とは異なり、新しいセキュリティ対策やビジネスの在り方に対するより根本的な変化を求める考え方である。

研究テーマを抽出するに当たり、NITRD はサイバーセキュリティの展望を変える game-changing な技術のアイディアを全米の大学、政府研究機関、企業、非営利団体及びユーザ団体等から RFI（Request for Information）[18]を通じて募集している。最終的に 238 件のレスポンスが寄せられた。その後、2009 年 8 月 15 日から 17 日にかけて NITRD 及び OSTP の主催で「National Cyber Leap Year Summit」を開催し、RFI のレスポンスから導いた 5 つの研究テーマ（初案）について、150 名の参加者（産学官のステークホルダー）による議論を行った。NITRD CSIA IWG は、サミットの成果を基に、5 つの研究テーマを①Moving Target、②Tailored Trustworthy Spaces、③Cyber Economic Incentives（各テーマについては 1.2.4. 参照）の 3 つに統合した上で具体化のための検討を行った。2010 年 5 月には各テーマに対してビジョン、そのテーマが game-changing な理由、ゴール、課題、マイルストン、主要技術、非技術面の障壁等の具体的内容を取りまとめた「Cybersecurity Game-Change Research & Development Recommendations[19]」を公表している。なお、これらの研究テーマはあくまで「初期テーマ」としての位置付けであり、毎年見直しが行われることになっている。この見直しもオープンなプロセスで行われ、具体的な方法としては、サイバーセキュリティ R&D テーマに関するフォーラム（不定期）及びメールまたは郵便での意見募集[20]がある。なおこうした見直しの一環で、2011 年には新たなテーマとして Designed-in Security が加えられている。

これらの研究テーマを軸として、CSIA SSG 及び CSIA IWG によりサイバーセキュリティの研究開発の全体の枠組みに関する検討が進められ、2011 年 12 月に 2 年半の検討を経て研究開発戦略が公表されることとなった。

1.2.2. 研究開発戦略の概要

以下に戦略の原則、目的、役割を示す。

戦略の原則
● 研究は単にサイバーセキュリティの問題に対処するのではなく、問題の根本原因を理解することに注力する。 ● サイバーセキュリティは多面的な問題であり、戦略は幅広い分野にわたる様々な専門知識とリソースを取り入れることが求められる。 ● 技術や脅威の環境の変化に関わらずセキュアな環境を維持するため、サイバーセキュリティの原則を堅持していく。

[18] NITRD, “National Cyber Leap Year RFI Submissions”
http://www.nitrd.gov/leapyear/NCLY_Submissions_Public.pdf
元々、game-changing な技術のアイディアの募集は CNCI の下で開始された National Cyber Leap Year (NCLY) initiative の一環として行われている。RFI の募集は 2008 年 10 月から 2009 年 4 月までの期間に 3 回に分けて行われた。

[19] NITRD CSIA IWG, “Cybersecurity Game-Change Research & Development Recommendations”（2010 年 5 月）
http://www.nitrd.gov/pubs/CSIA_IWG_%20Cybersecurity_%20GameChange_RD_%20Recommendations_20100513.pdf

[20] NITRD, Federal Cybersecurity Game-Change R&D / Your Input
http://cybersecurity.nitrd.gov/page/your-input-1

戦略の目的
● 現在のサイバーシステムに対する攻撃を無力化する game-changing な技術開発 ● 将来のサイバーシステムにおけるセキュリティの課題に取組む科学的アプローチの基盤構築

戦略の役割
● 想定読者 連邦政府機関、政策立案者、研究者、予算アナリスト及び一般読者 ● 期待効果 ・ 限られたリソースを、最大のインパクトを生み出す潜在性のある研究活動へ結びつける。 ・ 研究者、政府の技術者、民間企業、大学、また国際的組織等の間で連携を生み出すよう、多岐にわたる R&D の分野をカバーし共通の関心項目を見出す。 ・ 政策決定者に対して、セキュリティサイエンス・技術への投資を判断する際のアイディアを提供する。

1.2.3. 研究開発戦略の全体構成

研究開発戦略は、戦略の推進力（Strategic Thrust）と題された以下の 4 つの内容から構成されている。

(1) 変化の誘発(Inducing Change)

戦略の核となる 4 つの研究テーマを示している。Game-changing な技術を想定した 4 つの研究テーマは、いずれも既知の脅威の根本原因を理解し、これまでとは根本的に異なるアプローチによって、社会の重要なサイバーシステム／インフラのセキュリティを向上させるものとなっている。各テーマの詳細は 1.2.4. に示す。

(2) 科学的な基盤の確立(Developing Scientific Foundations)

セキュリティサイエンス（Science of Security: SoS）を確立することで将来のサイバーセキュリティの問題を最小化することを目標として掲げている。SoS は(1)の 4 つのテーマに横断的に関わる考え方として位置付けられている。戦略では 10 年程度で SoS の確立を目指すとしており、具体的な実現方法として以下の 3 つの方向性を示している。

- 異なる分野の知識の体系化

  幅広い分野の知識を検証可能なモデルや予測として体系的に構造化する。

- 普遍的法則（universal law）の発見

  問題の検証や系統的な説明をする上で、基本的・普遍的なダイナミクスの理解を表現する法則を作り出す。

- 科学的手法における厳密性の適用

問題に対して系統的手法を用いてアプローチし、仮説を立て、再現可能な実験を計画・実行し、データを収集・分析する。

SoS は元々NSF が資金を拠出している Secure and Trustworthy Cyberspace（SaTC）プログラム[21]に関する研究において提唱されていた考えであり、2008 年には NSF/IARPA/NSA によって SoS に関する合同ワークショップも開催されている（詳細は 4.1.1.1 参照）。2007 年 8 月大統領科学技術諮問委員会（President's Council of Advisors on Science and Technology: PCAST）は、NITRD の活動に対する評価レポート[22]において「NITRD の参加機関は、基盤的、長期的な CSIA の研究開発及びそのためのインフラ整備に重点を置くべきである」との勧告を行った。2010 年 6 月 NITRD は、PCAST のレポートに対する回答文書[23]において、「NITRD が策定中の研究開発戦略の 3 つのテーマの 1 つ Trust and Confidence（現戦略では Tailored Trustworthy Spaces）はサイバーセキュアなサイバースペースの重要性を強調しており、例として NSF の Trustworthy Computing プログラムでは Science of Security 等の Trustworthy Computing の基盤を重視している」として、SoS の考え方を取り入れることを示唆している。

(3) 研究のインパクトの最大化（Maximizing Research Impact）

戦略に基づいて実施される研究の効果を最大化するため、他分野の研究テーマとの連携や官民の研究コミュニティの活動を推進していく。

多分野との連携に当たっては、各連邦政府機関が推進する国家の優先研究分野におけるサイバーセキュリティの要求に取組むフレームワークを提供する。このフレームワークによって、直接サイバーセキュリティを扱っていない他分野の研究テーマに対しても、戦略の影響力が及ぶこととなる。具体的に融合が期待される優先研究分野の例を図 1-2 に示す。

また、共通の目的を持つ研究者間の議論の基盤を提供するとともに、脅威や脅威への対処に関して刺激的で継続的な対話の機会を提供することで学際的・商業的な研究コミュニティの研究開発への参加を促進する。具体的な活動として、研究テーマに関するワークショップの開催や、各研究機関によるファンディング等の研究支援の強化、各テーマ向けの研究インフラの構築等を挙げている。

---

[21] FY2002-2003 は「Trusted Computing」、FY2004-2008 は「Cyber Trust」、FY2009-2011 は「Trustworthy Computing」というプログラムとして実施されている。

[22] PCAST, “Leadership Under Challenge: Information Technology R&D in a Competitive World －An Assessment of the Federal Networking and Information Technology R&D Program”（2007 年 8 月）
http://www.nsf.gov/geo/geo-data-policies/pcast-nit-final.pdf

[23] NITRD, “NITRD Responses to PCAST Report”（2010 年 6 月）
http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nco-nitrd.pdf

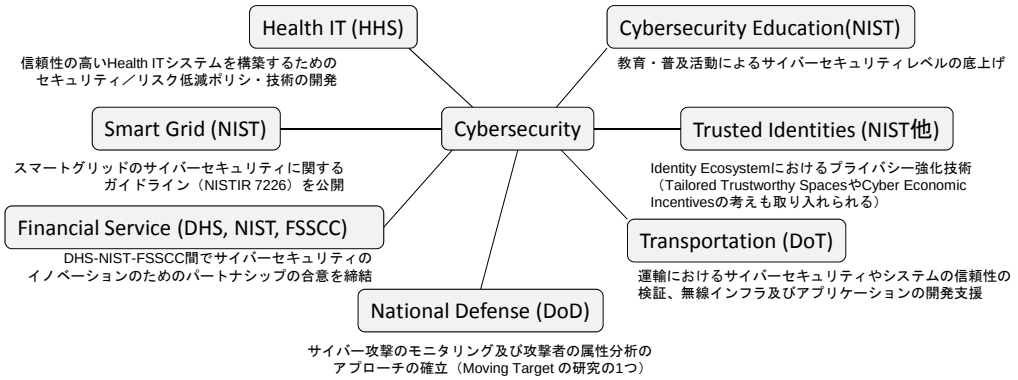

図 1-2 他分野の優先研究テーマとの連携

（出典:各種資料を基に三菱総合研究所作成）

(4) 実用移行の加速(Accelerating Transition to Practice)

研究開発で得られた成果をサイバースペースの向上に役立てるため、各種実用化プログラムを推進する。具体策として以下のような取組みへの参加が予定されている。

項目	具体的な取組みの例
技術発見	● Information Technology Security Entrepreneurs' Forum（ITSEF） （政府機関、起業家、投資家、研究者、産業界の相互利益関係を構築し、IT セキュリティソリューションプロバイダと官民の IT／通信インフラのユーザを結びつけることを目指したフォーラム） ● 各研究分野の研究責任者（Principal Investigator: PI）の会合の開催 ● 国の研究所による技術に関する Expo の開催 ● Defense Venture Catalyst Initiative（DeVenCI） （DOD の調達のためベンチャーキャピタルを活用する取組み）
テストと評価	● 官民のオペレーション環境や次世代ネットワーク環境における、実際に近い設定での実験、テスト、評価等をサポートする。
移行、適用、商用化	● System Integrator Forum（SIF）： （ベンチャーキャピタル、システムインテグレータ、政府の担当者等が参加して、商用化可能な成熟した研究成果（製品）のレビューを行うオープンフォーラム） ● Small Business Innovative Research（SBIR）Conferences: （中小企業研究開発支援制度の枠組みで行われたサイバーセキュリティ研究、技術及び開発された製品を紹介し、政府顧客、SBIR のフェーズ 2 のコントラクター及びプライムコントラクターのネットワーク形成の機会を提供するオープンフォーラム） ● 実用移行で成果を上げたプログラムマネージャや研究責任者への評価方法の検討

1.2.4. 研究テーマ

以下に米国の研究開発戦略で示された Designed-in Security、Tailored Trustworthy Spaces、Moving Target 及び Cyber Economic Incentives の 4 つ研究のテーマについて詳細を示す。

(1) Designed-In Security(DIS)[24]

Designed-in Security（DIS） セキュアなソフトウェアエンジニアリングシステム	
ビジョン	セキュリティホールとなるソフトウェアの欠陥を劇的に減らし、攻撃への耐性を持つソフトウェアシステムをデザイン・開発する。また、アシュアランスに焦点を置いた工学的手法、言語、ツールを用いて、システムを開発しながら、攻撃に対抗する能力を証明するためのアシュアランス・アーティファクトを生成する。
研究課題	・ システムエンジニアリングプロセスにおけるオンザフライの証拠生成を可能とするモデルと手法のデザイン ・ モデルの統合や異なるコンポーネントの結果の組立てを補助する数学的手法 ・ 多様なモデルやコードにおいても追跡可能なリンキングを可能とする評価手法（モデル検査、抽象解釈、意味論ベースのテスト／検証に基づいて） ・ 処理能力、モジュール性、柔軟性の高いシステムに、高い保証を与える言語デザイン、処理、ツール開発手法 ・ サプライチェーンにおけるアシュアランスの組立てを支援する体制やサプライチェーンにおける事例研究 ・ ソフトウェアコード、モデル、分析結果をつなぐ一連の証拠を迅速かつ、自動的に管理するために情報管理、コンフィギュレーション管理、開発者・チーム間の意思疎通を可能にするツール開発 ・ 使いやすく、ユーザに有益なフィードバックを行う、ソフトウェアの仕様作成、導入、検証、分析、及びテストツール構築のための心理学的、人間工学的要素 ・ 信頼性やセキュリティの向上度合いの測定を通じたモチベーションの向上に関する経済学

[24] 新たなテーマとして DIS が加えられた理由について、NITRD の Dr. George O. Strawn は 2010 年 5 月の下院科学・宇宙・技術委員会の技術・イノベーション小委員会と研究及び科学教育小委員会の合同会議における答弁において、「2009 年のサミット以降、サイバースペースに関する理解が進んだため」と述べている。また、2010 年 12 月に NITRD CSIA の担当者が Annual Computer Security Applications Conference 2010 で行ったプレゼンテーションでは、将来の潜在的テーマとして、「Design for Assurance」、「Understanding the Cyber Environment」、「Nature-inspired Solutions」、「Mobility」、「Borderless Security」等を紹介しており、このうち「Design for Assurance」が DIS として採用されたと考えられる。
NITRD, “Federal Cyber Security Research Program”（2010 年 12 月）
http://www.nitrd.gov/fileupload/files/NITRDACSAC2010.pdf

(2) Tailored Trustworthy Spaces（TTS）

Tailored Trustworthy Spaces（TTS） ユーザの状況に応じた適切なセキュリティ要件が実現される信頼性の高い環境の実現	
ビジョン	進化し続ける脅威に直面する幅広い活動において求められる機能上及びポリシー上の要件を実現するため、柔軟で、適用性があり、分散された信頼性の高い環境を提供する。ユーザのコンテキストを理解し、またコンテキストの進化にも対応できる。
研究課題	・ ポリシーのネゴシエーションを可能にするネゴシエーションツール及びデータの信頼モデル ・ タイプセーフな言語、アプリケーションの検証及びポリシーで指定されたアイデンティティや認証を確立するツール ・ トランザクションパス全体に情報に基づいた信頼性を持たせるためのデータ保護ツール、アクセスコントロール管理及びモニタリング／コンプライアンス検証メカニズム ・ リソースとコスト分析ツール ・ セキュアブートロードと重要ソフトウェアのリアルタイムモニタリングを可能とするハードウェアメカニズム ・ 信頼性が低い環境における分離とプラットフォーム信頼性を確保する最小権限の分離されたカーネル ・ 実行中にプログラムのセマンティクスを変更することができないという強い保証を提供するアプリケーション及び OS の要素 ・ 匿名の Web アクセスを可能にする application-aware な匿名性及びプラットフォームのセキュリティメカニズムと信頼性の実現
備考	TTS の機能として以下のような項目が示されている。 ・ 状況に応じたセキュリティ要件を的確に設定する ・ 特定のセキュリティ属性ごとにアシュアランスレベルを調整する ・ 検証可能な情報に基づきシステム間の信頼を構築する また、TTS のフォーカスエリアとしてモバイル・ワイヤレスネットワークの例が挙げられている。 フォーカスエリア：モバイル・ワイヤレスネットワーク モバイルデバイスのサイズ、処理能力、消費電力の問題で、セキュリティソリューションをモバイルワイヤレス環境に適用することは難しかったが、信頼性の高い end-to-end のサイバーサブスペースを構築するためには、ワイヤレス技術も有線同様の TTS 機能を備える必要がある。ワイヤレスドメインについても TTS のソリューションや技術を適用し、その恩恵を受けられるように研究開発を進めることが必要となる。

(3) Moving Target(MT)

Moving Target（MT） 動的に「変化」することで攻撃の困難さやコストを増加させ、攻撃に晒されても悪影響を受けにくいシステムの実現	
ビジョン	ユーザが時間とともに継続的に変化し、複雑さと攻撃者のコストを高める多様なメカニズムと戦略を開発、解析、評価、導入することで、脆弱性の露出や攻撃の機会を減らし、システムの回復力を高める。
研究課題	・ MT のメカニズムと有効性に関する科学的な推論を可能にする抽象化とその手法を開発する ・ 脆弱性がある空間の特徴抽出と、システムのランダム化が脆弱性に対する攻撃への対策としてどの程度の効果があるかを理解する ・ 複雑なシステムにおける個別コンポーネントのランダム化が、システムの攻撃回避能力と攻撃からの回復力に及ぼす効果を理解する ・ 複雑な MT のシステムを抽象化し、健全で回復力のある管理を有効にする制御メカニズムを開発する ・ システムの成熟と進化する攻撃を理解することで MT メカニズムの適応を可能にする
備考	MT のフォーカスエリアとして以下の項目が挙げられている。 ・ サイバースペースの深い理解 ・ 自然摂理に基づくソリューション

(4) Cyber Economic Incentives(CEI)

Cyber Economic Incentives（CEI） サイバーセキュリティへの適切な投資判断を可能にする、科学的な指標等の提供	
ビジョン	サイバーセキュリティを社会に定着させるため、市場メカニズムや法規制等を盛り込んだ効果的なインセンティブを確立する。
研究課題	・ サイバーセキュリティへの投資と市場に関するモデルの検討 ・ データモデル、オントロジー及びデータの浄化・匿名化の自動化手法の開発 ・ 有意なサイバーセキュリティメトリクスと保険数理表の定義 ・ 高信頼のソフトウェア開発手法の経済的妥当性の向上、個人情報保有を支援する方法の提供 ・ 法規制や国際的な合意事項に準拠するための知識の提供

1.3. 3.1 及び 3.2 のまとめ

1.1 及び 1.2 で紹介した「Cyberspace Policy Review」が公表された 2009 年 5 月以後の、米国のサイバーセキュリティ政策及び研究開発戦略に係る取組みの流れを、図 1-3 に時系列で示す。

「Cyberspace Policy Review」が公表された 2009 年には、同文書のアクションプランの 9 項目目で示された研究開発戦略の検討が他の項目に先駆けて開始された。研究開発戦略策定にあたり、NITRD は研究テーマに関して研究者や政府関係者等のステークホルダーから大規模な意見集約を行っている。また、NITRD / OSTP が 2009 年 8 月に開催した「National Cyber Leap Year Summit」では、ステークホルダーが一堂に会して研究テーマに関する議論を行っている。

一方、2009 年 12 月にはアクションプランの 1 項目目に示されたサイバーセキュリティ調整官として Howard Schmidt 氏が指名され、以後 Schmidt 氏の主導の下でアクションプランの遂行が加速されることとなった。

2010 年前半には、NIST が主導する教育プログラム NICE（3 月開始）やアイデンティティ・マネジメントに関する NSTIC（6 月ドラフト版戦略文書発表）等の長期的なプログラムが立ち上げられた。また連邦政府内のサイバーセキュリティ体制の見直しも進められ、4 月には FISMA に関する新しいガイドラインが公表され、7 月には政権内にプライバシー・人権担当者も設置された。一方、研究開発戦略に関しては、NITRD CSIA を中心に研究テーマの具体化の検討が進められ、5 月には研究開発戦略の骨子となる研究テーマの詳細が公開された。ここでは、研究テーマとして①Moving Target、②Tailored Trustworthy Spaces、③Cyber Economic Incentives が挙げられている。

2010 年後半には、サイバーセキュリティのオペレーションに関する取組みが活発化し、9 月に暫定版のサイバーインシデント対応計画の発表とそれに基づいたサイバー演習が実施された。また、10 月には米軍のサイバー攻撃への対応機能を統合したサイバー部隊「Cyber Command」が設置され、これを基に DOD と DHS のオペレーションにおける連携体制も強化された。

2011 年には、各項目に係る戦略文書の公開が相次いだ。4 月には、約 1 年前に公表されたドラフト版を改訂した NSTIC の戦略文書の正式版、5 月には、サイバースペースにおける国際連携に関する戦略文書が決定された。また、アクションプランでは直接示されていないものの、7 月には DOD が Cyber Command の活動も含めたサイバー空間におけるオペレーションに関する防衛戦略文書を発表している。さらに、8 月には NICE のドラフト版の戦略文書も公開されている。一方、研究開発戦略についても NITRD CSIA IWG において引き続き検討が行われ、新たな研究テーマとして Designed-in Security が加えられた。その後、戦略全体の取りまとめ作業が行われ、2011 年 12 月、2 年半の検討を経て White House の国家科学技術会議（NSTC）から研究開発戦略の最終版が公開されることとなった。

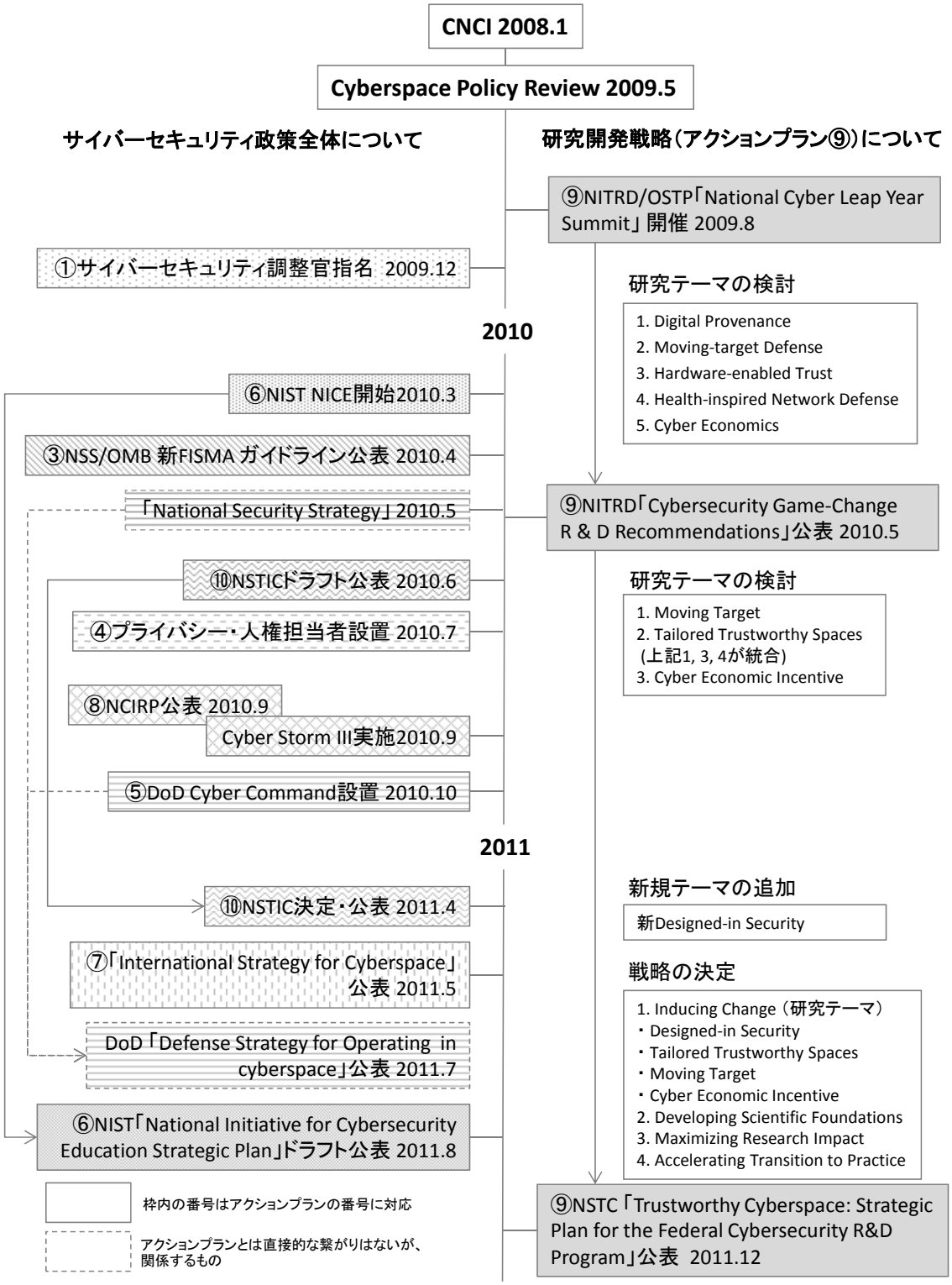

図 1-3「Cyberspace Policy Review」以後の

米国のサイバーセキュリティ政策及び研究開発戦略の流れ

（出典：各種資料を基に三菱総合研究所作成）

1.4.米国のサイバーセキュリティ研究開発予算の状況

1.4.1. NITRD CSIA の 2013 年度予算要求額

3.2.1.に示す通り、NITRD CSIA は連邦政府の情報通信分野の研究開発を省庁横断的に取りまとめる NITRD のサイバーセキュリティと情報保証分野であり、サイバーセキュリティの研究開発を行う連邦政府の機関が参加している。そのため、米国のサイバーセキュリティの研究開発予算は、これら機関の予算を取りまとめた NITRD CSIA の予算として示される。

2012 年 2 月に発表された大統領予算教書補足資料[25]によれば、2013 年度（FY2013）の NITRD CISA に対する予算要求額は 6.67 億ドルとされており、2012 年度（FY2012）の推定予算額 5.9 億ドルから約 13%増、2011 年の確定予算額からは、約 50%増となり研究開発予算の拡充傾向が続いている。組織別にみると NSF が約 0.15 億ドル増、DOD が約 0.12 億ドル増、DARPA が約 0.24 億ドル増、DHS が約 0.18 億ドル増となっている。

なお最新の 2013 年度の予算計画は、1.2 で紹介した研究開発戦略で示された方針に沿った形となっている。

NITRD CSIA における 2007 年度からの予算推移を図 1-4 に示す。

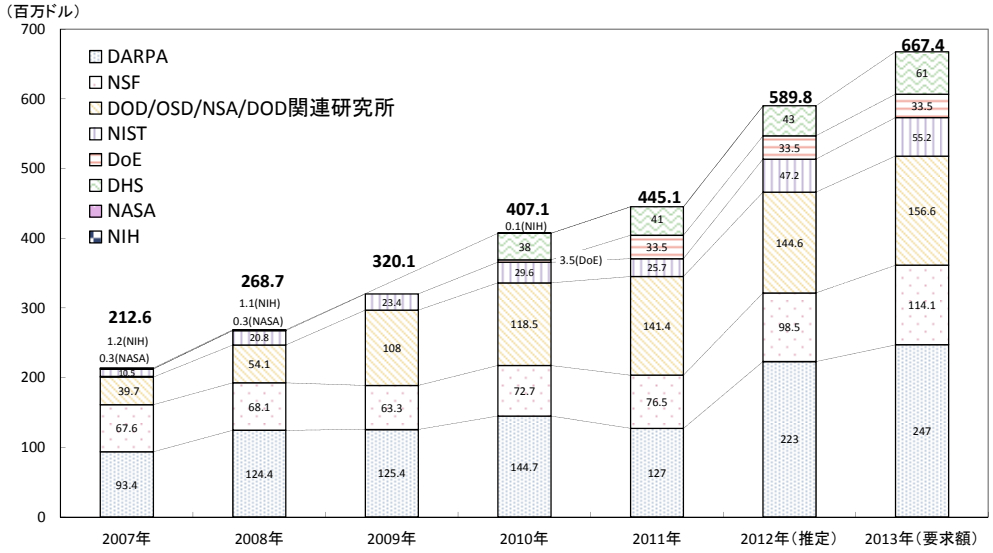

図 1-4 NITRD CSIA の予算推移（出典：NITRD 資料を基に三菱総合研究所作成）

1.4.2. 研究開発戦略の今後の展望

NITRD に参加する各政府組織の 2013 年度予算で予定されている主な研究開発プログラムの一覧を、研究開発戦略の項目に合わせて表 1-2 に整理する。また、プログラムの例を表 1-3 に紹介する。

[25] NITRD, “Supplement to the President’s Budget”（2012 年）
http://www.nitrd.gov/pubs/2013supplement/FY13NITRDSupplement.pdf

表 1-2 2013 年度に予定されている NITRD CSIA の主な研究開発プログラム一覧

大項目	小項目	NITRD 参加機関における主な研究開発プログラム
(1)変化の誘発	TTS	・ Secure and Trustworthy Cyberspace Program（NSF） ・ サイバースペースの防衛オペレーションのための信頼性の高い基盤（AFRL, ARL, ARO, CERDEC, ONR, OSD） ・ Cybersecurity Research and Development Broad Agency Announcement（DHS） ・ 高保証のセキュリティアーキテクチャ（ONR, NIST, NSA） ・ Security Automation Program（DHS, NIST, NSA） ・ Access Control Policy Machine（NIST） ・ Tactical Information Technologies for Assured Network operations（TITAN）（ARL, ARO, CERDEC） ・ クラウドベースシステムのセキュリティ（DARPA, DHS, NIST） ・ セキュアなワイヤレスネットワーキング（ARL, ARO, CERDEC, DARPA, ONR, NSA） ・ Secure Information Exchange Gateway（SIEGate）（DOE） ・ Military Networking Protocol（MNP）program（DARPA）
	MT	・ Protected Control Plane for Cyber Command and Control（PCPC3）（AFRL） ・ Cyber Unification of Security Hardening and Protection of Operational Frameworks（CRUSHPROOF）（ARL, ARO, CERDEC, OSD） ・ Morphing Network Assets to Restrict Adversarial Reconnaissance（ARL, ARO, CERDEC） ・ Defensive Enhancements for Information Assurance Technologies（DEFIANT）（ARL, ARO, CERDEC） ・ Cybersecurity Research and Development Broad Agency Announcement（DHS） ・ Proactive & Reactive Adaptive Systems（NSA） ・ Security Automation and Vulnerability Management（NIST） ・ Trust Management in Service Oriented Architectures（ONR） ・ Robust Autonomic Computing System（ONR） ・ Information Security Automation Program（ISAP）（DHS, NIST, NSA） ・ Clean-slate design of Resilient, Adaptive, Secure Hosts（CRASH）（DARPA） ・ Cyber Camouflage, Concealment, and Deception（DARPA）
	CEI	・ Secure and Trustworthy Cyberspace Program（NSF） ・ Cybersecurity Research and Development Broad Agency Announcement（DHS）
	DIS	・ Survivable Systems Engineering（OSD/Software Engineering Institute（SEI） CERT） ・ Trusted Computing（DARPA, NSA, OSD） ・ Software Development Environment for Secure System Software & Applications（ONR） ・ Crowd-Sourced Cyber program（DARPA） ・ META（DARPA） ・ Roots of Trust（NIST, NSA） ・ Software Assurance Metrics And Tool Evaluation（SAMATE）（DHS, NIS）
(2)科学的基盤の構築	SoS	・ Science for Cybersecurity（S4C）（ARL, ARO, CERDEC） ・ Science of Security MURI（AFOS）
	分野横断的基盤	・ 暗号化技術（DARPA, NIST, NSA, NSF, ONR） ・ モデル／標準／テスト／メトリクス（ARL, ARO, DHS, DOE, NIST, NSF, OSD） ・ Foundations of Trust（AFRL, ARL, ARO, CERDEC, DOE, NIST, NSF, OSD） ・ Security Management and Assurance Standards（NIST） ・ Quantum information science and technology（IARPA, NIST, ONR）
(3)研究インパクトの最大化	国家優先研究分野の支援	・ Trustworthy Cyber Infrastructure for the Power Grid（TCIPG）（DHS, DOE） ・ National Strategy for Trusted Identities in Cyberspace（NSTIC）（NIST）
(4)実用移行の加速	技術発見 評価 移行 適用 商用化	・ Testbeds and infrastructure for R&D（DARPA, DHS, DOE, NSF） ・ Cyber Technology Evaluation and Transition Program（CTET）（DHS） ・ Information Technology Security Entrepreneurs' Forum（ITSEF）（DHS） ・ Secure and Trustworthy Cyberspace Program（NSF） ・ Defense Venture Catalyst Initiative（DeVenCI）（DOD） ・ Small Business Innovative Research（SBIR）Conferences（DHS, DOD）

表 1-3 2013 年度に予定されている NITRD CSIA の研究開発プログラムの例

Secure and Trustworthy Cyberspace（SaTC）[26]	
研究機関	NSF（以下の 6 部局が参加） Computer and Information Science and Engineering（CISE）, Education and Human Resources（EHR）, Engineering（ENG）, Mathematical and Physical Sciences（MPS）, Social, Behavioral, and Economic Sciences（SBE）, Office of Cyberinfrastructure （OCI）
関連テーマ	TTS、CEI 及び(4)実用移行の加速
2013 年度要求額	110.25（百万ドル）（2012 年度推定額：111.75）
概要	NSF で 2002 年から開始されている Trustworthy Computing プログラムの流れを継ぐプログラムであり、サイバーセキュアな社会を形成し、高品質なデジタルシステム開発と優秀な労働力において国家の競争力を高めることを目指している。アルゴリズム、モデル、確率論、信頼性、統計理論 / 解析、暗号解読、システム構成、セキュアコンピューティング等の基盤研究に加え、サイバーセキュリティに影響を与える社会的・行動的要素を理解するための市場メカニズムに関する研究も支援している。 SaTC は、NSF の 6 部局が参加する巨大プロジェクトであり、各部局のプログラムディレクター等からなるワーキンググループによって運営されている。また人材育成も重視しているため、教育プログラムも整備し、これまでに 1,500 名以上の学生に投資し、うち 1,100 名が 120 以上の連邦政府機関においてインターンシップ及びフルタイムの仕事に就いている。

Clean-slate design of Resilient, Adaptive, Secure Hosts（CRASH）[27,28]	
研究機関	DARPA
関連テーマ	MT
2013 年度要求額	25.0（百万ドル）（2012 年度推定額：29.0）
概要	生体システムのメカニズムを応用し、以下のような機能を備えたコンピュータシステムを設計するためのソフトウェア開発手法を確立することを目指している。 ・サイバー攻撃に対する高度な耐性 ・攻撃を受けた後でも有用なサービスを提供する適応性 ・攻撃を受けた経験に基づいた、将来の攻撃への防御方法の学習性 ・攻撃からの自己修復性

META	
研究機関	DARPA
関連テーマ	DIS
2013 年度要求額	75.0（百万ドル）（2012 年度推定額：56.0）
概要	正しさを検証しながら系統的に開発されるべき防衛・航空等の複雑なシステムの設計能力を飛躍的に高める新しいデザイン・フロー、ツール及びプロセスの開発を行う。次世代の戦車の初期設計への応用等を目指している。

[26] NSF, “FY 2013 Budget Request to Congress”（2012 年 2 月）
http://www.nsf.gov/about/budget/fy2013/pdf/EntireDocument_fy2013.pdf
[27] DOD, “Fiscal Year (FY) 2013 President's Budget Submission”（2012 年 2 月）
http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2147484865
[28] DARPA Information Innovation Office
http://www.darpa.mil/Our_Work/I2O/Programs/Clean-slate_design_of_Resilient_Adaptive_Secure_Hosts_(CRASH).aspx

1.5.日本の研究開発戦略検討の参考となる視点

本項では1.1及び1.2で紹介した米国のサイバーセキュリティ政策及びサイバーセキュリティの研究開発戦略の最新動向から、日本の「情報セキュリティ研究開発戦略」の拡充及び将来の新たな戦略策定時の参考となる視点を抽出する。

1.5.1. 研究開発戦略の策定プロセス

米国では、1.2 に示した通り「Cyberspace Policy Review」による指示を受けて研究開発戦略が策定され、2011 年 12 月に NSTC から公表されている。こうしたトップダウンの指示の背景には、サイバーセキュリティを国家の優先課題とするオバマ大統領の姿勢があり、これが戦略の位置付けを確固としたものとしている。

NITRD CSIA を中心に行われた戦略策定作業では、game-changing な技術に関する研究テーマを導くため、全米の大学、政府研究機関、企業、非営利団体及びユーザ団体等から、game-changing な技術のアイディア（コンセプト）を募集し、最終的に 238 件のレスポンスが寄せられている。これを基に研究テーマの初案が抽出され、さらに公開サミットを通じて 150 名の産学官のステークホルダーによる議論が行われた。その後 CSIA IWG を中心に研究テーマの具体化や戦略全体の取りまとめが行われた。2009 年の検討開始から 2011 年の公表まで約 2 年半の期間を要している。

一方、日本の「情報セキュリティ研究開発戦略」は 2010 年に決定された「国民を守る情報セキュリティ戦略」において指示されたものであり、昨年度の検討会、NISC 及び技術専門委員会における検討を経て、昨年 7 月に情報セキュリティ政策会議で決定されている。戦略策定作業は情報セキュリティ研究（技術）課題に関するボトムアップの検討から開始され、米国の研究テーマや戦略策定プロセスを参考にすることで、限られた時間の中で集中的かつ効率的に検討を進めた。研究課題に関しては、各分野の専門家 10 名へのヒアリングを基に取りまとめている。

現戦略では、日本の研究開発方針を早期に打ち出すことを重視したため技術課題に対する集中的な検討を行ったが、今後現戦略の拡充や新たな戦略を検討する際には、米国のように産学官から幅広くアイディアを募集し、ステークホルダー間の議論を通じて長期的に研究テーマをブラッシュアップしていくプロセスを取り入れることも考えられる。

日米の研究開発戦略は、実際に研究開発を担う政府機関に対して研究開発の方向性を示す資料という位置付けにおいては共通したものである。ただし、米国では策定作業を行った NITRD の省庁横断の作業部会に、実際に研究開発を担う政府機関の担当者も参加している。このため、国家の研究開発戦略と各機関の研究開発方針の整合性が確保されており、各機関の 2013 年度の予算要求は、研究開発戦略の内容に対応した項目になっている。（表 1-2 参照）。

日本の現戦略の策定過程においても各省庁と内容の調整を行っているものの、研究項目

と各省庁の既存研究との間で整合性がとれていない部分もある。戦略をより実効的なものにしていくためにも、戦略の策定・拡充・推進過程に各省庁の担当者が参加し、各省庁の方針を共有しながら作業を進める体制を作ることが望ましい。

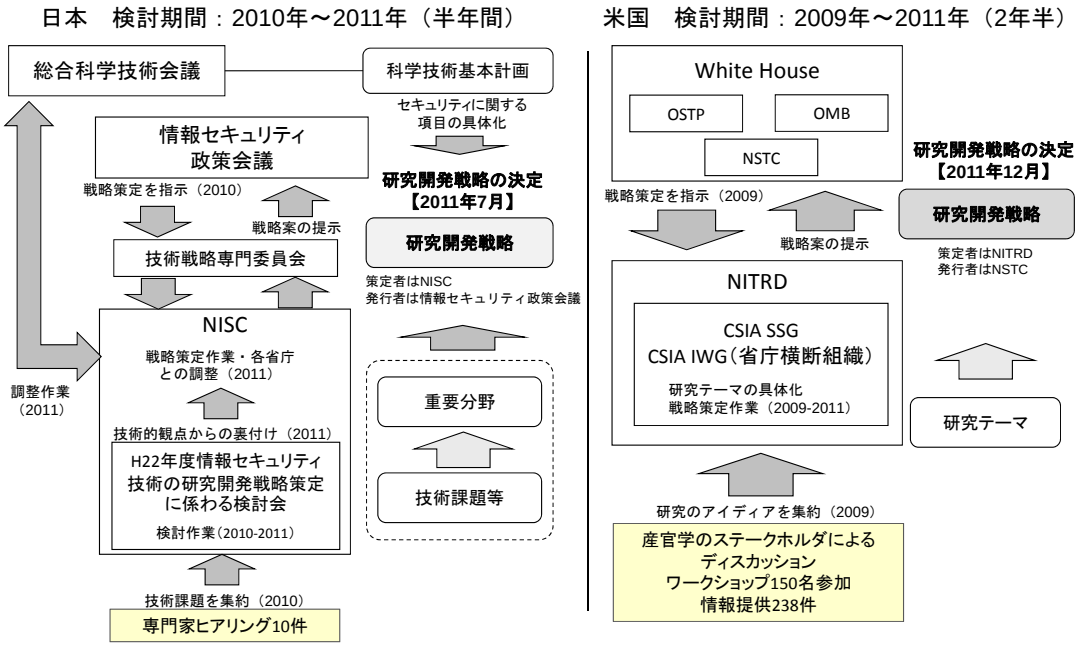

図 1-5 日米の情報セキュリティ研究開発戦略策定プロセス

（出典：各種資料を基に三菱総合研究所作成）

1.5.2. 研究テーマの見直し

米国の研究開発戦略の研究テーマに関する検討は 2009 年から NITRD CSIA を中心に進められている。NITRD では公開イベントやメール等を通じて産学官から研究テーマに対する意見を随時募集しており、それらが戦略や予算にも反映されている。このため、現研究開発戦略にも検討開始時には含まれていない Designed-in Security や Science of Security などの新たなテーマが加わっている。変化の激しい情報セキュリティ分野では、脅威やシステム環境の変化や最新の技術に迅速に対応する必要がある。今後の米国の研究開発戦略の更新について引き続き注視し、日本の戦略の検討に生かしていくことが重要である。

1.5.3. 他分野における研究開発戦略の活用

1.2.3. (3)にも示すように米国の戦略では、サイバーセキュリティ以外の分野の研究テーマとの連携を戦略の大きな柱の 1 つとして掲げており、またこうした連携を通じた新たな研究コミュニティ形成も重視している。情報セキュリティは幅広い分野に係る問題であり、日本でも他分野の研究プロジェクトの中の課題の 1 つとして情報セキュリティに取組んでいる事例は多い。各省庁で実施している他の分野の研究開発においても、情報セキュリティに係るテーマについては本戦略が活用されるよう推進していくことが重要である。

2.情報セキュリティ技術の科学的な評価フレームワークの調査及び評価フレームワークの構築

2.1.評価フレームワークの動向調査

現在の情報セキュリティ技術は、情報システムに関わる環境において生じる攻撃などの脅威に対する対処療法的なノウハウの集合となっており、科学としての体系化や評価尺度が十分に整備されていない。

「情報セキュリティ研究開発戦略」を推進するにあたり、情報セキュリティの研究開発を、科学として評価する基礎が整理できれば、研究開発事業の有効性の検討や評価に役立つものと考えられる。そこで、本章では米国における情報セキュリティの評価フレームワークの動向を調査し、「情報セキュリティ研究開発戦略」の推進に向けた活用の可能性について検討する。「情報セキュリティ研究開発戦略」における重要分野⑪には、評価フレームワークの確立が含まれるため、特に、この項目の検討に資する情報をまとめる。

調査対象は、主に以下の 2 つの分野とする。

- セキュリティサイエンスの動向
  サイバーセキュリティの研究開発において、科学的なアプローチを導入することにより、効果的で合理的な研究開発の推進を目指した取組み。
- 情報セキュリティに関する評価手法の動向
  情報セキュリティのリスクや対策技術の導入効果等に関する科学的な評価手法に関する研究開発動向。

2.1.1. セキュリティサイエンスの動向

セキュリティサイエンス（SoS: Science of Security）[29]とは、サイバーセキュリティの研究開発に、科学的なアプローチを導入することにより効果的で合理的な研究開発の推進を目指した取組みである。2008 年頃から米国を中心にその問題意識が高まり、様々なワークショップや調査研究を通じて議論が行われてきた。現在、これらの議論は途上にあるが、その問題意識や解決すべき課題の方向性について有用な示唆が得られる。

本節では、セキュリティサイエンスの動向及び議論の中で挙げられた課題の要点をまとめる。

2.1.1.1. セキュリティサイエンスの動向に関する概要

セキュリティサイエンスに関する問題認識について具体的に議論された最初の会議は、NSF、IARPA、NSA の共催で実施されたワークショップである。以降、現在に至るまで、

[29] Science of Cybersecurity と表現されることもあるが、3.2.で紹介した米国の研究開発戦略では Science of Security という表記に統一しているため、本報告書においてもこの表記を用いる。

ワークショップや調査が継続的に実施されてきた。

Workshop on the Science of Security, NSF/IARPA/NSA（2008 年 11 月）[30]
セキュリティサイエンスに関する問題提起や議論が行われた初期の会議で、セキュリティ研究を、従来のアドホックで、インフォーマルなアプローチから、科学的な基礎に基づく研究として捉えるための課題や取組み方法、他の分野からの教訓、不可能なことを明確にするなどの議論が行われた。NSF、バージニア大学、NSA、国防研究所（Institute for Defense Analyses）など、異なる立場の参加者がパネルディスカッションにより議論を行った。

Roadmap for Cyber Security Research, DHS（2009 年 11 月）
DHS 科学技術局が、サイバーセキュリティ分野の専門家 100 名程度の協力を得て、5 回のワークショップを開催し、15 ヶ月間かけて、策定したサイバーセキュリティ研究のロードマップを示している。その中で、困難な研究課題を掲げ、その多くのものはセキュリティサイエンスに関わる課題であるとしている。

Science of Cyber-Security, JASON, The MITRE Corporation（2010 年 11 月）
セキュリティサイエンスに関する問題意識の高まりを背景に、DOD が防衛諮問委員会 JASON に委託して実施されたセキュリティサイエンスに関する調査研究である。サイバーセキュリティとは何か、現状の達成水準、将来への取組みの方向性を示している。具体的な方向性や研究課題については議論の途上という位置付けとして捉えられる。（「付録 A.セキュリティサイエンスに関する取組み事例」参照）

Research institute in the science of cyber security（2011 年 11 月）※英国
UK 高等教育研究機関（GCHQ：Government Communications Headquarters）向けに、セキュリティサイエンスの研究機関設立の提案を募集したものである。困難な研究課題をテーマとして、提案募集の前に、ワークショップが開催される予定である。EPSRC 研究グラントにより、3.5 年間で 350 万ポンドの予算が提供される。

このような米国内外の議論、検討を経て、米国において 2011 年 12 月に公開されたサイバーセキュリティの研究開発戦略「Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity R&D Program」において、セキュリティサイエンスは 4 つの大きなテーマに横断的に関わる考え方と位置付けられ、科学的な基盤の構築のため 10 年程度で確立を目指すとされた。

[30] 情報セキュリティに関する基盤的、長期的な研究開発及びそのためのインフラ整備の重点化については、2007 年 8 月の PCAST（大統領科学技術諮問委員会）レポート [22] に記載はあるが、Science of Cybersecurity という用語を用いて具体的に議論されたのは、NSF/IARPA/NSA の会議が最初である。

2.1.1.2. セキュリティサイエンスにおける課題の要点

セキュリティサイエンスに係わる問題認識や解決すべき課題については、現在、議論の途上にあるが、前節に示す議論に基づき、重要と考えられる課題の要点をまとめると以下のようになる。

セキュリティサイエンスに係わる研究課題の要点

- サイバーセキュリティ研究の共通言語の構築
  サイバーセキュリティの技術研究は、攻撃者を前提とした研究であるため、対象が常に変化する。そのような対象について研究者の間の議論や研究のためのコミュニケーションを深めるために共通言語を確立する必要がある。共通言語についての明確な定義は記載されていないが、研究成果の比較検証を行う上で、対象モデルや使用する用語の客観的で曖昧性のない定義を含むと考えられる。
- セキュリティメトリクスの確立
  研究成果のセキュリティ技術の有効性を評価する客観的な指標を確立する必要がある。メトリクスは多数存在するが、攻撃者を対象に含むため、本質的に実験的、統計的なメトリクスとならざるを得ないことには留意が必要である。
- 再現可能な実験基盤の確立
  研究成果は、再現可能で検証可能であることが求められる。そのための実験基盤を確立することが求められる。実験基盤は、閉じた小規模な環境でなければ難しいかもしれない。
- 免疫システムの応用
  セキュリティ技術は、変化する脅威や攻撃手法に対して、適応的であることが求められる。生物免疫システムの自律適応性と生得性の両立が、セキュリティ確保に有益な方法を与えるかもしれない。
- システムの抽象化・モデリング
  セキュリティ技術は、特定の脅威やシステムの評価ではなく一般性、汎用性を持つものでなければならない。そのためにセキュリティモデルや攻撃者モデルを明確に定義することが重要である。小規模なシステムでは、証明コードをサポートするシステムがある。
- 基礎理論を参考とした体系化
  暗号理論、形式手法、モデル検査、型システム等、理論体系に基づく研究アプローチを参考とした基盤の確立は重要である。
- 戦争の科学、犯罪の科学
  攻撃者の振る舞いに関するモデリング、セキュリティ原理を明確化することが重要である。戦争や犯罪に関する研究は、まだ確立されていないが、参考となりうる。
- 研究コミュニティの確立
  攻撃や脅威に対抗するためには、大学、産業、国立研究所の様々な研究者のアイディアを共有した、創発的なプロセスが重要となる。そのために様々な立場の研究者が集まるコミュニティを確立することが重要である。

2.1.2. 情報セキュリティに関する評価手法の動向

情報セキュリティに関する評価手法の動向を把握するために、米国における大学、研究機関、政府組織等における情報セキュリティに関する評価メトリクス、評価フレームワークに関する研究及び適用に関する取組み事例について要点をまとめる。

調査対象は、以下のような情報源から評価メトリクス、評価フレームワークに係わる適用手法について事例を抽出した。

- 情報セキュリティ経済学に係わる国際会議等
  - WEIS（Workshop on Economics and Information Security）
  - WESII（Workshop on the Economics of Securing the Information Infrastructure）など
- 情報セキュリティ研究機関、大学における取組み等
  - CMU/SEI
  - CERT/CC
  - SANS Institute
  - メリーランド大学、アイダホ大学など
- 標準規格、政府機関における取組み等
  - FISMA、NIST FIPS 関連資料等
  - GAO など
- その他・民間機関
  - WEB 文献調査

以上のような範囲から抽出された評価メトリクス等に関する取組み事例について、個々の事例に関する要点を整理したものは 付録 B.セキュリティ評価手法の概要 に示す。これらの事例について、評価対象及び用途などの観点から特徴を分類・整理すると、表 2-1 のようにまとめられる。

表 2-1 セキュリティメトリクス、評価フレームワークの整理

目的分類	手法分類	名称	実施主体	評価対象と評価項目	用途	特徴・注目点
リスク、対策レベルの評価	メトリクス評価手法	IMAF(Integrated Measurement and Analysis Framework)	SEI/CMU	大規模ネットワークのセキュリティ特性として、攻撃、障害、事故および予期しないインシデントへの対応力の計測。	プロジェクト管理者がセキュリティ上の問題点を予測・診断するための情報を得る。	コンポーネント単位ではなくシステム全体を評価できる。
		MetricsCenter	PlexLogic	IT製品で発見された脆弱性の経時変化に基づくベンダのスコアとそのランクを提示する。	製品調達の判断にメトリクスを利用したり、自社の製品を評価する。	WEBサービスにより提供される。
		CAR評価モデル	University of Maryland, Campbell, Gordon	上場企業について、情報セキュリティ事故を起こした場合の企業価値毀損額。金額を単位として株式市場価値として評価する。	事故を起こした場合に損害額から、情報セキュリティ投資額やその上限額を検討する。	直接コストや有形資産のみでなく、企業の信用失墜、顧客離れによる将来の収益低下等の無形資産の損失を含む損害額全体を評価する。
	評価フレームワーク	CERT-RMM	SEI/CMU	組織の障害許容力(ミッションクリティカルな資産やサービスのフォルトトレランスを維持する能力)を計測する。	プロジェクト管理者が、問題の予測・分析を行いどの部分に投資すべきか判断する情報を与える。	目標と現状のパフォーマンスをベンチマークとして比較する。
		NIST SP800-55	NIST	組織やITシステムにおいてセキュリティ活動(リスク管理、システム開発における品質確保、セキュリティ計画の実施等)の達成度、効率、有効性、ビジネスへの影響を評価する。	組織においてセキュリティ活動が十分実施されているか判定し、問題点の対策を検討する。	組織の構造や業務手順を考慮した上で妥当なリソースで実施できる。
		A Guide to Security Metrics	SANS Institute	組織におけるセキュリティ対策の評価プログラムを策定する方法を示し、ベンチマーク比較による達成度評価法を示す。	情報システムを利用する組織のセキュリティ対策の評価と改善策を検討する。	既存のプロセス改善のフレームワークをベースに策定できる。
投資効果の評価	メトリクス評価手法	ASM(Attack Surface Measurement)	CMU	ソフトウェアの機能追加で攻撃のリスクがどの程度変化するか測定する。	ソフトウェアのセキュリティ対策が、企業の利益にどの程度つながっているか評価し、開発者や利用者の機能更新の意思決定に利用される。	ソースコードを対象に評価する。
		Gordon-Loebモデル(理論モデル)	University of Maryland, Gordon, Loeb	組織の情報資産に関して、攻撃が発生する確率、投資額、脆弱性、攻撃が発生した場合に保護が破られる確率等を仮定して、投資による正味利益[金額]を評価する。	攻撃が発生した場合に保護が破られる確率等の関係式を仮定することで、正味利益を最大化する投資額を求める。	投資額に対する正味利益を求めることで、投資の過剰、過小の評価ができる。
		Survivability of Network Systems	CERT/CC	情報システムに関して、インシデント発生時の機能の稼働率(Survivability)を評価する。	インシデント発生時の機能の稼働率(Survivability)を元に、システム防御の適性レベルを評価する。	組織にとっての情報システムの重要度と生存性から、最適なセキュリティ投資コストを求める。
		Idaho Cost-Benefit Model	Idaho University	組織ネットワークにおける侵入検知システムによる対策において、脅威ごとの被害コストと対応コストの一覧を示し、それに基づき総合的な費用対効果を評価する。	脅威ごとの対策の投資対効果から投資の意思決定を行う。また、企業の資産の種類と脅威の程度を評価する際のガイドラインともなる。	脅威種別ごとの被害コストと投資コストの一覧(標準)を示している。
	評価フレームワーク	VMM(Value Measuring Methodology)	GAO	IT投資における組織の価値、リスク、コスト構造を検討し、投資代替案と共に費用対効果および価値、リスク、コストのスコア値を求める。	IT投資に関する複数の代替案の評価を行い、費用対効果の高い代替案を選択する。	有形資産のみならず無形資産の価値も評価する。

表 2-1 に示す通り、抽出した取組み事例を大きく分類すると、リスク・対策レベルの評価と、投資効果（セキュリティ対策実施効果）の評価に分けられる。さらに、それぞれの分類について、計測する特定の対象のメトリクス評価手法そのものと、既存のセキュリティメトリクスを用いて、組織やシステムのセキュリティレベルを評価するための方法論やフレームワークを提供するものに分けられる。ここで挙げられるメトリクスは、表 2-1 に示す通り、評価対象とそれに応じた尺度が定義されている。評価対象は、情報セキュリティ研究開発の対象や手法によって、ここで挙げられるものでは、扱えない場合も想定される。したがって、評価フレームワークを適用する際には、評価対象や尺度に関するニーズに応じて、個別にカスタマイズあるいは新たな尺度の開発が必要になる。

2.1.3. 調査結果の活用方法

セキュリティサイエンス及び情報セキュリティに関する評価手法に関する動向調査の結果、得られた知見を、「情報セキュリティ研究開発戦略」の推進においてどのように生かすかその観点をまとめると以下のようになる。

- 情報セキュリティ研究開発の本質課題の抽出
  研究開発戦略の重要分野の検討及び将来の戦略改訂において、本質的な課題や情報セキュリティ事故等の根本原因の抽出を行うにあたり、セキュリティサイエンスにおける問題認識を参考にすることができる。
- 研究成果に対する客観的な評価手法の導入
  関連省庁の研究開発事業において、個々の研究テーマが、リスク評価手法の調査結果に挙げるような評価メトリクスなど、科学的、客観的な評価を行っているかについて判断する際の参考とすることができる。
- 技術の効果測定の観点の導入
  関連省庁の研究開発事業において、研究公募のテーマ設定や選考において、技術導入効果の調査結果に挙げるようなニーズの観点からの技術評価を行っているか判断する際の参考とすることができる。

付録

A.セキュリティサイエンスに関する取組み事例

セキュリティサイエンスに関わる取組み事例について、主な文献の内容をまとめる。

対象	JASON, The MITRE Corporation, “Science of Cyber-Security”（2010 年 11 月）
URL	http://www.fas.org/irp/agency/dod/jason/cyber.pdf
位置付け・要点	DOD 等から依頼を受けて JASON（研究機関 MITRE が運営する諮問機関）が、セキュリティサイエンスについて行った調査研究レポート。セキュリティサイエンスについて最も深く検討した文献の 1 つと言える。共通言語の構築、メトリクスの重要性、研究コミュニティの確立などについて提言している。ただし、DOD が挙げた疑問に対して将来の方向性を示すレベルにとどまっており、明確な結論を示しているとは言い難い。
概要	レポートの中では、セキュリティサイエンスの定義の重要性とその困難性を挙げている。サイバーセキュリティは、人工的に構築された環境における科学であり、攻撃者、防御者に対する前提が少ないなどの特殊性がある。また、セキュリティサイエンスは攻撃者に関する科学でもあるが、攻撃は常に新しくなりそれを防ぐ技術が生み出されるものである。そのため、情報科学だけでなく、経済学、疫学、医学などの観点からも考慮する必要があり、それらとの関係について説明している。コンピュータ科学から活用できるサブ分野としては、モデル検査、暗号学、乱数、型理論、ゲーム理論などを挙げている。モデル検査や型システムは、研究成果をツールに移行させる洗練されたアプローチと考えられるが、市場ではまだあまり普及していない。セキュリティのレベルに対応したメトリクスの開発は重要だが、その限界を認識することも必要である。 レポートでは、サイバーセキュリティ研究に関する DOD からの疑問点に対して、以下のような提言をまとめている： ● サイバーセキュリティ研究の共通言語の構築 サイバーセキュリティは、攻撃者を前提とした科学であるため、対象は常に変化する。研究者の間のコミュニケーションを深めるために共通言語が必要である。 ● メトリクスの確立 メトリクスは多数存在するが、実験に基づいた、統計的なメトリクスであって、明確に定義されていないシナリオには適用できない。 ● 再現可能な実験の確立 実験の再現可能性は重要であるが、最初は閉じた小規模な環境で検証する必要がある。 ● モデル検査 研究アプローチの基盤として利用できる可能性がある。 ● 研究コミュニティの確立 大学、産業、国立研究所の様々な研究者が集まるコミュニティの確立を支援することが重要である。

対象	DHS, “The Science of Cybersecurity and a Roadmap to Research”（2009 年 11 月）
URL	http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf
位置付け・要点	DHS がまとめたサイバーセキュリティ研究に関するロードマップ。
概要	研究開発に関する国家の重要な政策課題を定義するために、サイバーセキュリティ研究について検討した結果をまとめている。攻撃者に先行し、情報システムやネットワークを防護するための技術を確立するために必要な研究課題とロードマップをまとめている。 以下のようなものを困難な目標課題として挙げている： 1. Scalable trustworthy systems スケーラブルで trustworthy なシステムの実現。trustworthy とは、システムの完全性、可用性、稼働率（survivability）、機密性、リアルタイム性、説明責任性、アトリビューション、ユーザビリティ等の多次元的な要件を満たす概念と定義されている。 2. 企業レベルのメトリクス 3. システム評価ライフサイクル システム製品を適時に評価する方法を確立し、ライフサイクルに応じた評価方法を確立する。 4. 内部脅威対策 5. マルウェアとボットネット対策 6. グローバルスケール ID 管理 7. タイムクリティカルシステムの稼働率（survivability） 8. 状況把握と攻撃者の特定 9. Provenance コンピュータ、ドキュメント、データ等の管理の流れと起源を把握することで、それらに対する信頼性の評価を可能にする。 10. プライバシーを意識したセキュリティ（Privacy-aware security） 11. 幅広いユーザ層に利用可能なセキュリティ（Usable security）

対象	“Workshop Report National Science Foundation’s Workshop on Trustworthy Computing, Workshop Topic: NITRD Themes and Science of Cybersecurity”（2010 年 10 月）
URL	http://people.ischool.berkeley.edu/~jensg/research/paper/NSF-TC-2010-report.pdf
位置付け・要点	Trustworthy なサイバーインフラ（Trustworthy Cyber Infrastructure）構築における主要な課題について議論するために開催されたワークショップ。NITRD Themes and Science of Cybersecurity に関わる研究者を含むセキュリティ研究者が参加した。
概要	Panel 5 及び Breakout 4 セッションでセキュリティサイエンスに関する議論が行われた。 ● Panel 5: Science of Cybersecurity 以下のような意見が挙げられた： 特定のシステム対攻撃者の評価ではなく、セキュリティモデル対攻撃者の評価をしなければならない。（Amit Sahai, University of California, Los Angeles） 人工世界における科学である点が、他の科学と異なる。（Peter Weinberger, Google） サイバーセキュリティを科学として扱うためには、セキュリティの抽象化が必要。例えば、小規模な計算システムにおいては、証明コードをサポートするシステムなどがある。（Andrew Appel, Princeton University） ● Breakout 4: Science of Cybersecurity セキュリティサイエンスの現在の研究ステータスに関する議論が行われた。セキュリティサイエンスの参考にできる理論として暗号、形式手法、モデル検査、型システム等が挙げられている。戦争の科学、犯罪の科学なども関連するが、これらは科学として確立されていない。攻撃者の振る舞いに関するモデリングのニーズやセキュリティの原理を明確化することの重要性が指摘された。 取組むべき分野として、攻撃者モデルとモデルの統合方法が挙げられた。ただし、参加者の中では Science of Cybersecurity は、幅広く、伝統的な理論や他の分野の理論を拡張するだけでは包含することができないものという意見が主流である。

対象	SEI / CMU, “CERT Research Report 2010”
URL	http://www.cert.org/research/2010research-report.pdf
位置付け・要点	CERT の年間の研究成果を総括するリサーチレポートの 2010 年版。セキュリティサイエンスが 2 つの柱の 1 つに位置付けられている。
概要	CERT の 2010 年の研究成果について、大きく以下の 2 つのカテゴリに分類しレポートをまとめている。 ● Critical Code ソフトウェア信頼性に関する研究活動について、米国科学アカデミーが発行した Critical Code: Software Productivity for Defense における対応性に基づき分類した研究カテゴリ。 ● Science of Cyber Security JASON によるレポート Science of Cyber Security における問題認識を踏まえて、もう 1 つの研究カテゴリとして設定 後者のカテゴリの研究は、便宜上 Science of Cyber Security と分類されているが、Science of Cyber Security の定義や理論、アプローチ等に該当すると思われる研究事例は含まれておらず、以下のような活動についてまとめられている： ・ マルウェア（不正コード）の研究と開発 ・ インシデントレスポンス ・ ネットワーク状況認識 ・ 回復力の高いモデリングと分析 ・ 人材開発カリキュラムプロジェクト

B.セキュリティ評価手法の概要

情報セキュリティに関するリスク評価手法、技術導入効果等の評価手法に関する事例調査結果を以下に示す。

B.1 リスクの評価手法

名称	Measuring Software Security Assurance
実施主体	組織：SEI / CMU Christopher Alberts, Juila Allen, Robert Stoddard
内容	攻撃・障害・予期しない出来事等に対するソフトウェアのセキュリティに対する注目が近年高まってきているが、ソフトウェアセキュリティにおける「計測」は、現状まだ具体化されていない。そこで、CMU の SEI (Software Engineering Institute) は、SMA (Security Measurement and Analysis) プロジェクトを設立し、ソフトウェアセキュリティの計測と解析に関する研究を行っている。SEI が開発した IMAF (Integrated Measurement and Analysis Framework) は、システムのコンポーネント単位で個々に計測を行うのではなく、システム全体としての計測を可能とする。また、システムのコンポーネント間の複雑な相互関係や依存関係の分析も可能とする。
情報源	SEI / CMU, "2010 CERT Research Report" http://www.cert.org/research/2010research-report.pdf

名称	Measuring Operational Resilience: Moving from Uncertainty to Justified Confidence.
実施主体	組織：SEI / CMU Julia H Allen
内容	多くの組織は、障害許容力を評価・測定する能力を欠いている。そこで、CMU / SEI は、障害許容力の計測と解析に関する枠組みを提案するため RMA (Resilience Measurement and Analysis) プロジェクトを設立した。RMA プロジェクトは、プロセスベースでの障害許容力の定義を使用しており、SEI の開発・実装・測定などの様々な経験に取込んでいる。
情報源	SEI / CMU, "2010 CERT Research Report" http://www.cert.org/research/2010research-report.pdf

名称	MetricsCenter
実施主体	PlexLogic 社 (測定、分析、ビジネスプロセス改善等のインターネットサービスを提供する企業)。MetricsCenter や、touchNOC といった製品を開発している。
内容	MetricsCenter はメトリクスを設計・導出・提供するためのクラウドベースのサービスである。MetricsCenter では、アクセス可能な信頼性の高いセキュリティメトリクス管理を提供するため、バックエンドプラットフォームに加えて 4 つの主要なサービス (Catalog / YouAreHere Benchmarks / Metrics Dashboards / Metrics Resources) を提供している。
情報源	MetricsCenter ホームページ http://www.metricscenter.org/

名称	Directions in Security Metrics Research
実施主体	組織：NIST Wayne Jansen
内容	IT セキュリティメトリクスは、情報セキュリティの測定のためのアプローチを提供し、パフォーマンスデータの収集、分析及びレポートにより、意思決定と責任能力を促進するツールである。セキュリティメトリクスの阻害要因に対処し、セキュリティメトリクスの技術の発展のための研究領域の方向付けを検討している。 結果として、以下の 5 つに対する研究領域の方向付けが提案された。 ① セキュリティの測定とメトリクスの形式的なモデル 運用システムの挙動の現実的な予測を可能にし、かつセキュリティ測定を正確に描写するのに十分な詳細水準を備えた形式的なモデルを確立する。 ② ヒストリカルデータの収集と分析 ヒストリカルなデータを収集、分析することで、傾向や相関関係を抽出し、予測等に役立てる。 ③ 人工知能の評価技術 推論、知識、認識、計画、学習、コミュニケーションのように、人工知能技術を利用できるセキュリティ評価の分野を特定し、さらにその実証を行う。 ④ 実用的で具体的な測定方法 実装や導入、設計や開発プロセスの形跡を強調する、既存のセキュリティ評価の補完などで生じる脆弱性を指摘するための具体的な測定の方法を考案する。 ⑤ 本質的で測定可能なコンポーネントの開発 測定に本質的に順応するコンポーネントの開発は、セキュリティメトリクスの最先端技術に向上につながる。セキュリティの測定を支援するコンポーネントの設計を行う。
情報源	NIST, “Directions in Security Metrics Research”（2009 年） http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf NIST, “IT SECURITY METRICS” http://www.itl.nist.gov/lab/bulletns/bltnaug03.htm

名称	Security Economics and The Internal Market
実施主体	組織：ENISA（European Network and Information Security Agency） Ross Anderson, Rainer B¨ohme, Richard Clayton, Tyler Moore
内容	ネットワークセキュリティ・情報セキュリティは、経済学的にも重要な課題で、情報セキュリティ経済学は主流な研究のトピックとなっている。この論文は、情報セキュリティ経済学において EU 加盟国各国の協調が必要となる問題について、いくつかの提案を行っている。 ① EU が、包括的なセキュリティ侵害通知法を導入する。 ② 欧州委員会（または欧州中央銀行）が、各国が電子犯罪に関するしっかりとした損失統計を公表するよう規制する。 ③ ENISA が、ヨーロッパの ISP から発されるスパムやその他悪意のあるトラフィック量に関するデータを集計し、公表する。 ④ EU が、感染したマシンの排除の要請に応じない ISP に対する損害賠償のための法令を導入する。 ⑤ EU が、ネットワーク接続機器がデフォルトでセキュアであることを保証する基準を策定し強制する。 ⑥ EU が、脆弱性のパッチ開発サイクルのスピードを上げるために、責任を持った早期の脆弱性公開と、パッチを当てていないソフトウェアについてベンダ責任を導入する。 ⑦ セキュリティパッチを無料公開し、ソフトウェアの機能アップデートと分離させる。 ⑧ EU が、電子商取引における顧客と支払いサービス事業者間の紛争の解決のための手続きをハーモナイズさせる。 ⑨ 欧州委員会が、悪質なオンライン販売業者に対する適切で有効な制裁に関する明確な制度を確立するための指令を提案する。 ⑩ ENISA が、ステークホルダーや欧州委員会と共に、オンライン商取引における消費者保護法についてのリサーチを行う。

	⑪ ENISA は、IT の多様性に起因するセキュリティの問題がある場合には、競争の規制当局に対して助言を行う。 ⑫ ENISA が Internet Exchange Point （IXP）の障害の影響を理解するため研究を支援する。また通信の規制当局と協力して、IXP の障害からの回復力に関するベストプラクティスを示す。 ⑬ 欧州委員会が、サイバー犯罪条約の議会を批准していない 15 の EU 加盟国に対して、圧力をかける。 ⑭ サイバー犯罪に関する国際協力を促進するため、 NATO をモデルとして EU 全体の体制を構築する。 ⑮ ENISA は、欧州委員会において情報セキュリティ分野の利益を擁護し、他の目的のために導入された規制が、不注意にセキュリティ研究者及び企業に危害を与えないようにする。
情報源	ENISA, “Security Economics and The Internal Market”（2007 年） http://www.enisa.europa.eu/activities/stakeholder-relations/reports/econ-sec/economics-sec/at_download/fullReport

名称	Security Metrics Guide for Information Technology Systems（NIST SP800-55）
実施主体	組織：NIST Marianne Swanson, Nadya Bartol, John Sabato, Joan Hash, Laurie Graffo
内容	IT セキュリティメトリクスを使うことで、組織や特定のシステムにおいて IT セキュリティ活動が実施されているか、その効率や有効性はどうか、ビジネスへの影響があるかといった点を評価できる。そのため、セキュリティポリシーと手続きの実施レベルを評価し、セキュリティ対策の効率と効果を測定することにより、それらの対策が組織のミッションと業務に与える影響を把握するためのメトリクスの特定、定式化、実装のためのアプローチを提供する。メトリクスの策定プロセスは以下の通り。 ① ステークホルダーの利害の明確化 ② 目標と目的の設定 ③ IT セキュリティポリシー、手引き、手続き ④ システムセキュリティプログラムの実施 ⑤ 実施レベル ⑥ プログラムの結果 ⑦ ビジネス／ミッションへの影響
情報源	NIST “NIST Special Publication 800-55, Security Metrics Guide for Information Technology Systems”（2003 年） http://www.ipa.go.jp/security/publications/nist/documents/SP800-55-J.pdf NIST, “NIST Special Publication 800-55 Revision 1, Performance Measurement Guide for Information Security”（2008 年） http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

名称	FISMA and Metrics – Federal Information Assurance Conference 2007
実施主体	組織：CERT/CC Samuel A. Merrell
内容	メトリクスに関する主な議論の観点を以下に示す。 ● 優れた意思決定を支援する ● 良い面・悪い面の両方に対してプログラムのパフォーマンスを評価する ● リソースの割り当てを正当化する ● リスク管理の証拠を提供する ● レポート作成を容易にする ＜測定と分析プロセスについて＞ ◯プロセスの概要 ● 測定や分析の目的を明確化し、抽出される情報が目標と合っているか確認する ● データを集めるための測定や分析手法、データ保存、報告書やフィードバック等のメカニズムを指定する ● 収集・保管・分析及びレポート機能を実装する

	● 意思決定が可能な客観的結果を提供し、その結果から是正措置をとる ◯測定・分析プロセスで考慮すべきステップ A. 測定と分析の整合性をとる。 ① 測定目標を立てる ② 測定方法を明確化する ③ データ収集や保管の手順を明確化する ④ 分析手順を明確化する B. 測定結果を提供する ① 測定データを収集する ② 測定データを分析する ③ データと結果を蓄積する ④ 結果を伝える
情報源	CERT/CC, “FISMA and Metrics”（2007 年） http://www.cert.org/archive/pdf/merrell_fisma.pdf

名称	Gordon-Loeb 投資対効果モデル
実施主体	組織：メリーランド大学 Lawrence A. Gordon, Martin P. Loeb
内容	情報資産に対するセキュリティ投資額とその効果の関係について脅威の発生確率と脆弱性の存在確率をパラメータとした基本構造のモデルを示した理論研究。これを用いてセキュリティ投資額の最適レベルについていくつかのケースを示している。 典型的な 2 つのケース（攻撃が発生した場合に損害が発生する確率のモデルケース）について、最適な投資額を示した。それらのケースにおいては、潜在的リスク量の 36%以上のセキュリティ投資は ROSI の点で合理的ではないことを示した。
情報源	Lawrence A. Gordon and Martin P. Loeb, “The Economics of Information Security Investment”, *ACM Transactions on Information and System Security*, pp. 438-457（2002 年）

B.2 技術導入効果の評価手法

名称	Attack Surface Measurement（ASM）
実施主体	組織：CMU Pratyusa K. Manadhata, Jeannette M. Wing
内容	攻撃者がシステムを攻撃するメソッドやチャネル、また存在するデータ項目を利用する。これらのリソースを複合的に参照し、リソースの観点から攻撃面を定義する。 基本的にはハワードメソッド（後述）と呼ばれる手法の応用を行っており、攻撃のベクトルに重みを割り当てる提案がないため、本手法でも重みの割り当ては行わない。そのかわり、Linux の 4 つ（Red Hat 3 つ、Debian 1 つ）に向けられた各攻撃のインスタンスの数を数え、それを比較することで攻撃面の測定を行った。 ※ハワードメソッド：まず Windows 攻撃ベクトルを識別し、それがどのくらい攻撃されやすいかという点で、攻撃ベクトルに重みを割り当てる。そして、それらを足し合わせることで攻撃面の推定を行うメソッド
情報源	Pratyusa K. Manadhata and Jeannette M. Wind, “An Attack Surface Metric”（2010 年） http://www.cs.cmu.edu/~pratyus/tse10.pdf

名称	A Guide to Security Metrics
実施主体	SANS Institute
内容	セキュリティメトリクスプログラムを策定するための 7 段階の方法論を提案している。 ① メトリクスプログラムの目標と対象を定義する ② どのメトリクスを生成するかを決定する 既に利用しているフレームワークがない場合は、次の 2 つのどちらかを推奨する。 ・Top-Down Approach セキュリティプログラムの目標から考える手法。セキュリティプログラムの目標から、

	所定の場所にあるべき指標の洗い出しを容易にする。 ・Bottom-Up Approach 製品やサービス等からセキュリティの必要性を考え、目標に結びつける手法。容易に必要なメトリックを得ることができる。 ③　メトリクスを生成するための戦略を策定する ④　ベンチマークと目標を設定する ⑤　メトリクスが報告される仕組みを決定する ⑥　実行計画を作成し、実行する ⑦　プログラムの見直し、改善サイクルを確立する
情報源	SANS Institute, “SANS Institute InfoSec Reading Room”（2006 年） http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55

名称	Seven myths about information security metrics
実施主体	組織：IsecT Ltd. Dr. Gary Hinson
内容	情報セキュリティは複雑な分野であるが、有効なメトリクスを定義するのは不可能ではない。情報セキュリティに関する問題点として、主に「インシデントの欠如」等の測定が難しいことが挙げられる。そこで、セキュリティメトリクス作成に考慮すべき際に語られる 7 つの間違った神話を紹介し、新しい観点を提供する。 ・セキュリティメトリクスに考慮すべき間違った 7 つの神話 ①　メトリクスは客観的かつ具体的でなければならない。 ②　メトリクスは離散値を持つ必要がある。 ③　絶対的な測定方法が必要である。 ④　メトリクスは高価である。 ⑤　測定できないものは管理できない。また、管理できないものは改善もできない。 ⑥　プロセスの成果の測定は必須である。 ⑦　具体的な数値を利用する必要がある。
情報源	IsecT Ltd., “Seven myths about information security metrics”（2006 年） http://www.noticebored.com/IsecT_paper_on_7_myths_of_infosec_metrics.pdf

C..略語集

組織関連

AFRL	Air Force Research Laboratory（空軍研究所）
ARL	Army Research Laboratory（陸軍研究所）
ARO	Army Research Office（陸軍研究事務所）
CERDEC	U.S. Army's Communications-Electronics Research, Development, and Engineering Center（陸軍通信電子研究開発技術センター）
CERT/CC	Computer Emergency Response Team/ Coordination Center（コンピュータ緊急対応チーム／調整センター）
CMU/SEI	Software Engineering Institute, Carnegie Mellon University（カーネギーメロン大学ソフトウェアエンジニアリング研究所）
COCO	Contractor-Owned, Contractor-Operated
COV	Committee of Visitors（外部委員会）
CSD/S&T/DHS	Cyber Security Division , Science and Technology Directorate , DHS（国土安全保障省科学技術部局サイバーセキュリティ課）
CSIA	Cyber Security and Information Assurance（サイバーセキュリティと情報保証）
CSIA IWG	Interagency Working Group on Cyber Security and Information Assurance
CSIA SSG	Cyber Security Information Assurance Research and Development Senior Steering Group
CSRDC	Cyber Security Research and Development Center（サイバーセキュリティ研究開発センター）
DARPA	Defense Advanced Research Projects Agency（国防高等研究計画局）
DHS	Department of Homeland Security（国土安全保障省）
DISA	Defense Information Systems Agency（米国防衛通信局）
DOC	Department of Commerce（商務省）
DOD	Department of Defense（国防総省）
DOE	Department of Energy（エネルギー省）
DOL	Department of Labor（労働省）
DOT	Department of Transportation（運輸省）
DRD	Director, Research Directorate
ED	Department of Education（教育省）
ENISA	European Network and Information Security Agency（欧州 ネットワーク情報セキュリティ庁）※EU
EPA	Environmental Protection Agency（環境保護庁）
FAA	Federal Aviation Administration（連邦航空局）
FBI	Federal Bureau of Investigation（連邦捜査局）
FERC	Federal Energy Regulatory Commission（連邦エネルギー規制委員会）
FFRDC	Federally Funded Research & Development Center
GAO	General Accounting Office（米国会計検査院）
GCHQ	Government Communications Headquarters（高等教育研究機関）※英国
GOCO	Government-Owned Contractor-Operated Organization
GOGO	Government-Owned Government-Operated Organization
HHS	Health and Human Services（保険社会福祉省）
HSARPA	Homeland Security Advanced Research Projects Agency（国土安全保障先端研究プロジェクト庁）
HSI	Homeland Security Studies and Analysis Institute（国土安全保障研究所）
IARPA	Intelligence Advanced Research Projects Activity（諜報先端研究プロジェクト活動）
INL	Idaho National Laboratory
IPA	Information-technology Promotion Agency（独立行政法人情報処理推進機構）

ITSEF	Information Technology Security Entrepreneurs' Forum
ITTC	Infosec Technology Transition Council
JST/RISTEX	Research Institute of Science and Technology for Society, Japan Science and Technology Agency（科学技術振興機構/社会技術研究開発センター）
NASA	National Aeronautics and Space Administration（米国航空宇宙局）
NEC	National Economic Council（国家経済会議）
NIH	National Institutes of Health（米国国立衛生研究所）
NISC	National Information Security Center（内閣官房情報セキュリティセンター）
NIST	National Institute of Standards and Technology（国立標準技術研究所）
NITRD	Networking and Information Technology Research and Development（ネットワーキング情報技術研究開発プログラム）
NPO	National Program Office（国家プログラムオフィス）
NRC	Nuclear Regulatory Commission（原子力規制委員会）
NSA	National Security Agency（国家安全保障局）
NSC	National Security Council（国家安全保障会議）
NSF	National Science Foundation（全米科学財団）
NSS	National Security Staff
NSTC	National Science and Technology Council（国家科学技術会議）
NTIA	National Telecommunications and Information Administration（国家通信情報管理局）
ODNI	Office of the Director of National Intelligence（米国国家情報局）
OMB	Office of Management and Budget（行政管理予算局）
ONR	Office of Naval Research（海軍研究事務所）
OPM	Office of Personnel Management（連邦人事管理局）
OSD	Office of the Secretary of Defense（国防長官府）
OSTP	Office of Science and Technology Policy（科学技術政策局）
PCAST	President's Council of Advisors on Science and Technology（大統領科学技術諮問委員会）
SBA	Small Business Administration（米国技術局中小企業局）
SIF	System Integrator Forum
State	Department of State（国務省）
Treasury	Department of the Treasury（財務省）
USCYBERCOM	Cyber Command
USDA	United StatesDepartment of Agriculture（農務省）
WEIS	Workshop on Economics and Information Security
WESII	Workshop on the Economics of Securing the Information Infrastructure

文書

CNCI	Comprehensive National Cybersecurity Initiative
FIPS140	Federal Information Processing Standardization 140
FISMA	Federal Information Security Management Act（連邦情報セキュリティマネジメント法）
NCIRP	National Cyber Incident Response Plan（国家サイバーインシデント対応計画）
NIST SP800-55	Security Metrics Guide for Information Technology Systems
NIST SP800-55 rev.1	Performance Measurement Guide for Information Security
NSPD-54/HSPD-23	National Security Presidential Directive 54 / Homeland Security Presidential Directive 23
NSTIC	National Strategy for Trusted Identities in Cyberspace
RFI	Request for Information

プロジェクト・施策

ATP	Advanced Technology Program
CRADA	Cooperative Research and Development Agreements

DECIDE	Distributed Environment for Critical Infrastructure Decision-making Exercises
DeVenCI	Defense Venture Catalyst Initiative
HOST	Homeland Open Security Technology
IMAF	Integrated Measurement and Analysis Framework
LOGIIC	Linking the Oil and Gas Industry to Improve Cyber Security
NICE	National Initiative for Cybersecurity Education
NSTIC	National Strategy for Trusted Identities in Cyberspace
RMA	Resilience Measurement and Analysis
SBIR	Small Business Innovative Research
SMA	Security Measurement and Analysis
STTR	Small Business Technology Transfer
TRA	Technology Readiness Assessment

その他

CEI	Cyber Economic Incentives
DIS	Designed-in Security
FY2012	the 2012 Fiscal Year
FY2013	the 2013 Fiscal Year
MT	Moving Target
SOC	Science of Cybersecurity
SoS	Science of Security
SPRI	Secure Protocols for the Routing Infrastructure
TRL	Technology Readiness Level
TTS	Tailored Trustworthy Spaces