# 「サイバー・セキュリティと情報アシュアランス分野の研究開発」

渡辺弘美@JETRO/IPA NY

## 1. 連邦政府によるサイバー・セキュリティ R&D 計画

2006 年 4 月、「Interagency Working Group on Cyber Security and Information Assurance（CSIA IWG）」が、米国のサイバー・セキュリティ及び情報アシュアランス（Cyber Security and Information Assurance: CSIA）分野の研究開発の充実の必要性を謳った「Federal Plan for Cyber Security and Information Assurance Research and Development」を発表した。

同計画を作成した CSIA IWG は、米連邦政府の省庁横断的なネットワーキング及び IT 関連の研究開発プログラムである NITRD (Networking and Information Technology Research and Development)の一つとして、2005 年 8 月、National Science and Technology Council （NSTC）によって設立されたばかりのワーキング・グループである。以下では、同ワーキング・グループの NITRD 内設立の背景、同ワーキング・グループによる同計画発表までの道のり、同計画の提言内容について順に見ていく。

### (1) NITRD における CSIA IWG 設立

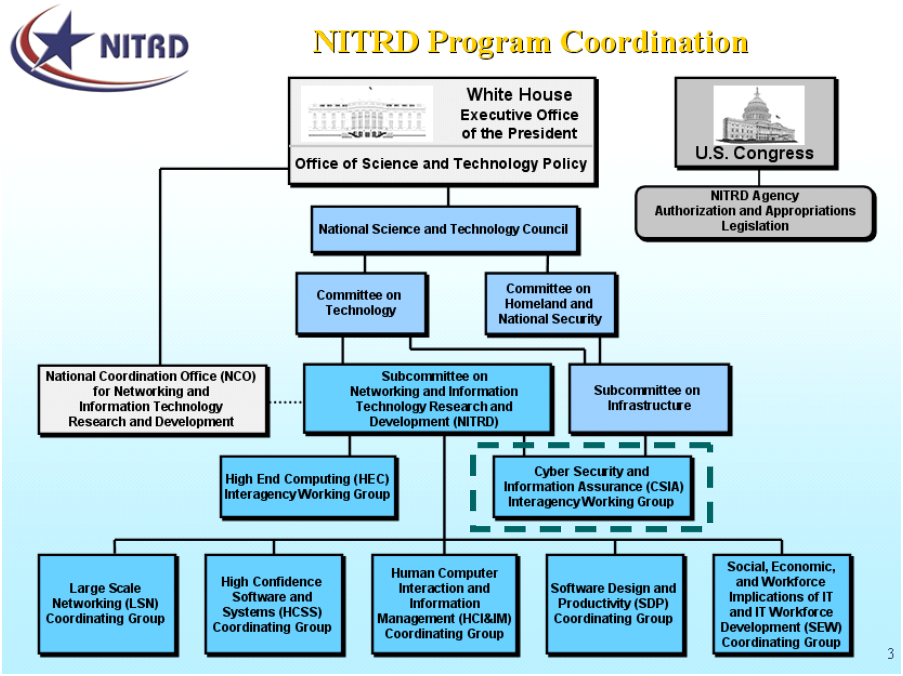
NITRD は 1991 年に制定された「High Performance Computing （HPC） Act of 1991 （Public Law 102-194）」を契機に設立された省庁横断のワーキンググループで、連邦政府機関の IT 関係の R&D 政策の中心機関と位置づけられる。参加省庁機関は以下の 12 連邦政府組織となっている。

- National Science Foundation（NSF）
- National Institute of Health（NIH）
- Department of Health and Human Services' Agency for Healthcare Research and Quality（AHRQ）
- Department of Energy・Office of Science（DOE/SC）
- DOE/National Nuclear Security Administration（NNSA）
- National Aeronautics and Space Administration（NASA）
- Department of Commerce・National Institute of Standards and Technology （NIST）
- National Oceanic and Atmospheric Administration（NOAA）

- Environmental Protection Agency （EPA）
- Secretary of Defense・ High Performance Computing Modernization Program Office（OSD/HPCMPO）
- Department of Defense ・Defense Advanced Research Projects Agency （DoD/DARPA）
- National Security Agency（NSA）

NITRD は、主に IT に関連する 7 つの分野において R&D 活動を行っており、NITRD のシニア・マネジャーからなる小委員会が、それぞれの活動を管轄している。活動状況は、NITRD のプログラムを管轄する NSTC にも報告されることになっている。

NIDRD 構成




NITRD では、分野毎の活動、関連機関からの投資、R&D の方向性などについて検討し、小委員会（Subcommittee、この場合 Subcommittee on NITRD）に報告を行っているグループを Interagency Working Group（IWG）又は Coordinating Group（CG）と呼ぶ。特に、IWG となる分野は、CG 以上に、関連省庁間の横の連携をとることが重要視されており、省庁間連携のための戦略策定が求められるものとされている。

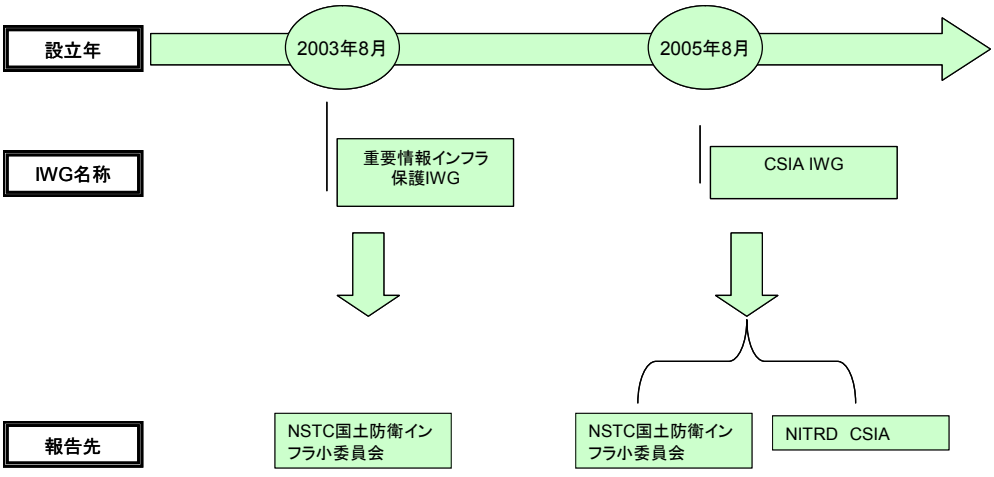
CSIA IWG は、NITRD の中でも、IWG という形態で 2005 年 8 月に設置された。CSIA IWG の設立趣意書によると、CSIA IWG には約 20 の連邦省庁機関・関係部署が参加している。

＜CSIA　IWG への参加省庁＞

DOE, Dept. of Justice, Dept. of State, Dept. of Treasury, Centeral Intelligence Agency, NASA, NIH, NSF, DOC (NIST), DoD (Office of the Deputy Under Secretary of Defense for Science & Technology, Defense Information Systems Agency, Defense Advanced Research Projects Agency, Dept. of the Air Force, Army and Navy, NSA), DHS（National Communications System, National Cyber Security Division, Science and Technology Directorate), Dept. of Transportation (Federal Aviation Administration)

CSIA IWG 設立以前は、その前身として、NSTC 下に「情報インフラ保護（Critical Information Infrastructure Protection）」IWG が設立されており、これまで国防関係の WG としての活動を行ってきた。しかし、IT と深い関連を持つ分野という背景などを受け、再編されることとなり、より効率的に CSIA 分野の R&D を実施することを目指すこととなった。

こうした設立の背景から、同 IWG は、他の NITRD ワーキング・グループと異なり、NITRD の管轄機関である NSTC の小委員会の 1 つ「NSTC 国土防衛インフラ小委員会（Subcommittee on Infrastructure of the NSTC's Committee on Homeland and National Security）」と、NITRD の CSIA 小委員会双方に、報告義務を負うこととなっている。



(2) Federal Plan for Cyber Security and Information Assurance Research and Development 発表に至る道のり

元来、連邦政府において、CSIA の R&D の重要性が指摘されたのは、今回の CSIA IWG による同報告書が初めてではない。これまでに、CISA の R&D に関して提出された主な報告書及び法律として、同報告書は以下 5 つをあげている。

2002 年以降提出された CSIA の R&D に関する提言及び法

| # | 提出年 | 提言・法律名称 | 内容 | |
|---|---|---|---|---|
| | | | 教育 | R&D |
| ① | 2002 年 | Cyber Security Research and Development Act | ○ | ○ |
| ② | 2003 年 2 月 | The National Strategy to Secure Cyberspace | ○ | ○ |
| ③ | 2005 年 2 月 | PITAC Cyber Security Report | ○ | ○ |
| ④ | 2005 年 7 月 | OSTP/OMB Memorandum on FY 2007 Administration R&D Budget Priorities | | ○ |
| ⑤ | 2005 年 11 月 | IRC Hard Problem List | | ○ |

特に 2001 年 9 月 11 日のテロ事件以降の国際状況を考慮し、連邦政府の CSIA の R&D での更なるリーダーシップを必要とする声が、連邦政府内部から聞かれるようになり、その最たるものがこの度の報告書となっている。また、同報告書の作成において、特に 2005 年の大統領諮問委員会である PITAC（President's Information Technology Advisory Committee：現在、PITAC は解散しその後の任務を PICAST（President's Council of Advisors on Science and Technology）が引き継いでいる）からの報告書は、本報告書作成に大きく影響したといわれている。

① Cyber Security Research and Development Act（No: 107-305）

| | |
|---|---|
| ➢ 制定日 | ➢ 2002 年 11 月 |
| ➢ 提出者 | ➢ Sherwood Boehlert 下院議員（ニューヨーク州選出）他 8 名 |
| ➢ 目的 | ➢ コンピュータとネットワーク・セキュリティに関する教育、研究、開発に対する資金を認可するもの。同資金は、民間や政府のコンピュータへのテロリスト攻撃の予防・対処にむけたリサーチ・コミュニティの充実と、サイバー・セキュリティの現在のパラダイムを越えた革新的な研究を推進するために使用される。 |

下院科学委員会（Committee on Science）は、2001 年 10 月 10 日、17 日の 2 回にわたり、米国コンピュータ・インフラ分野の脆弱性を調査するため、公聴会を開催した。2001 年 9 月 11 日のテロリスト攻撃は、金融、交通、エネルギー、緊急サービス等に必須であるコンピュータと通信ネットワークの脆弱性さをあらわにした。これを境に、米国の技術研究プログラム、教育システム、相互結合型オペレーションが、21 世紀のサイバー戦争の脅威に耐えられるか、見直す機運が高まったことにある。証人として呼ばれた産・官・学の専門家は、現在、米国のコンピュータ・インフラの取り組みは、今後起こりうる様々な問題に対して、不十分であると証言した。以下は、証言の主な内容となっている：

- 米国の、コンピュータ・セキュリティに対する投資の少なさは危機的であるといえる。
- 間違ったアプローチの結果、旧態依然としたコンピュータ・セキュリティの分野に惹かれる一流の研究者は少数である。
- 連邦政府は、コンピュータ・セキュリティの改善に向けた必要な研究やその実用化を、責任をもって行っている機関を設置していない。
- 市場は、民間産業がインターネットへの依存性を高めているにもかかわらず、コンピュータ・セキュリティへの投資に対し非常に低い関心しか持っていない。

これらを受けて、Sherwood Boehlert 下院議員を中心としたメンバーが、同法案を 2002 年に提出し、同年 11 月には法制化をみた。

同法は、下記の新プログラムを制定し、これらに対し、年間で 8 億 8 千万ドルをあてがうとした：

- NSF： 新たにサイバー・セキュリティ研究センター、学部学生向けプログラム助成金、コミュニティー・カレッジ助成金・奨学金などを設ける。
- NIST： 学会と産業間のパートナーシップに対し、新たなプログラム助成金、ポスドク・ポジション、他分野の古参の研究者がコンピュータ・セキュリティに取り組むことができるような新プログラムを設ける。

② The National Strategy to Secure Cyberspace

| | |
|---|---|
| ➢ 制定日 | ➢ 2003 年 2 月 |
| ➢ 提出者 | ➢ 連邦政府 |
| ➢ 目的 | ➢ 米国防衛活動の一環である National Strategy for Homeland Security を行う際の指針となるものであり、自分たちが所有、運用、管理、情報交換に使用するサイバースペースの安全を確保することを米国民に促し、またそのための助言をあたえることを目的とする。 |

サイバースペースを安全に保つということは、連邦政府、州・地方政府、民間セクター、米国民の社会全体が一団となって取り組まねばならない大きなチャレンジである。76 ページに及ぶこの文書は、米国のコミュニケーション・テクノロジーを保護するための持続的な、かつ多面性を持ったものとなっている。

その戦略目標は

- 米国の重要インフラに対するサイバー攻撃を未然に防ぐ。
- サイバー攻撃に対する脆弱性を削減する。
- サイバー攻撃からの損害と回復時間を最小に抑える。

となっている。同提言は、国レベルでの 5 つの優先事項を挙げている。

The National Strategy to Secure Cyberspace 概要

| 優先事項 | 概要 |
|---|---|
| サイバースペース・セキュリティ対応システム | 1. 国レベルで、サイバー事件に対応するための公共-民間アーキテクチャを作成する。<br>2. サイバー攻撃と脆弱性を特定する為の戦略分析を展開する。<br>3. 健全なサイバースペースを共有する民間セクター能力の開発を促進する。<br>4. サイバースペース・セキュリティの危機管理調整を行う DHS を支えるために、サイバー警告とインフォメーション・ネットワークを拡張する。<br>5. 事故管理能力を高める。<br>6. 公共-民間の継続協力体制の継続と、緊急事態対応計画作成に向けての自発的な参加の調整を行う。<br>7. 連邦システムのサイバー・セキュリティ継続計画を実践する。<br>8. サイバー攻撃、脅威、脆弱性を含んだ公共-民間の情報共有を改善、強化する。 |
| サイバースペース・セキュリティへの脅威、脆弱性削減プログラム | 1. サイバースペース攻撃を未然に防ぎ、関連法の強制力を高める。<br>2. 脅威や脆弱性の招く結果に対する理解を深める為、国レベルの脆弱性査定制度を確立する。<br>3. プロトコルとルーティングを改善することにより、インターネットのメカニズムを安全なものとする。<br>4. 安全なデジタル管理システムとデータ取得システムの使用を進める。<br>5. ソフトウェア脆弱性を減らし、修正する。<br>6. インフラの相互依存性を理解し、サイバー・システムとテレコミュニケーションの物理的安全性を確保する。<br>7. 連邦サイバー・セキュリティ研究・開発アジェンダの優先付けを行う。<br>8. 新規のシステムの査定を行い、安全性を確保する。 |

| 優先事項 | 概要 |
|---|---|
| 国レベルでのサイバースペース・セキュリティ認識、訓練プログラム | 1. あらゆるサイバースペースの保護にむけ、全米国人を対象にした包括的な国レベルの認識プログラムを推し進める。<br>2. 米国のサイバー・セキュリティの必要性を訴える適切な訓練と教育プログラムを推進する。<br>3. 連邦サイバー・セキュリティ訓練プログラムの効率を上げる。<br>4. 専門的なサイバー・セキュリティ認定の民間セクター支援を推進する。 |
| 政府のサイバースペース保護 | 1. 連邦サイバー・システムへの脅威と脆弱性の査定を継続する。<br>2. 連邦サイバー・システムの公認されたユーザを法的に認証し、管理する。<br>3. 連邦のワイヤレス・ローカル・エリア・ネットワークを安全に保つ。<br>4. 政府のアウトソーシングと調達における安全性を改善する。<br>5. 州と地方政府による IT セキュリティ・プログラム確立を促進し、政府との情報共有や分析を行うセンターに参加する。 |
| 国内セキュリティと海外サイバースペース・セキュリティの協力 | 1. サイバー関連対策諜報活動を強化する。<br>2. 攻撃の特定と対応能力を改善する。<br>3. 米国セキュリティ・コミュニティ内でのサイバー攻撃に対応するため協調を進める。<br>4. インフォメーション・ストラクチャを守り、地球レベルのセキュリティ文化を推進することに焦点をあてた、国際的な公共と民間セクターの会話とパートナーシップ実現に向け、産業と国際機関と協力する。 |

③ PITAC（President's Information Technology Advisory Committee） Cyber Security: A Crisis of Prioritization

| | |
|---|---|
| ➢ 制定日 | ➢ 2005 年 2 月 |
| ➢ 提出者 | ➢ President's Information Technology Advisory Committee（PITAC＝大統領直属インフォメーション・テクノロジー諮問委員会） |
| ➢ 目的 | ➢ 大統領府科学技術政策局（Office of Science and Technology Policy）からの、現在の連邦のサイバー・セキュリティ R&D 活動がより、バランスのとれた効果的なものになるように取り組む命令を受けて行った調査。 |

PITAC 報告書概要

| 項目 | 概要 |
|---|---|
| 調査結果① | 連邦の研究・開発予算は、民間サイバー・セキュリティ基礎研究に十分な資金の提供ができていない。 |
| 提言① | 民間サイバー・セキュリティ基礎研究の為の NSF 予算は年間で 9 千万ドル |

| | |
|---|---|
| | 増やされるべきである。民間サイバー・セキュリティ基礎研究のための資金は、DHS、DARPA のような他機関に対しても増額されるべきである。 |
| 調査結果② | 米国のサイバー・セキュリティ研究コミュニティは、米国を守るために必要なサイバー・セキュリティ研究と、教育プログラムを十分に支えるには、小さすぎる。 |
| 提言② | 連邦政府は、民間サイバー・セキュリティの規模を少なくとも 2 倍にするという目的をもって、研究する大学のサイバー・セキュリティ研究者や学生の雇用と、維持を促進する努力を強めなければならない。 |
| 調査結果③ | 現在のサイバー・セキュリティ技術移転努力は、民間セクターでの最良の実践や製品に向けて、連邦研究投資をうまく移すには、不十分である。 |
| 提言③ | 連邦政府は、民間セクターとサイバー・セキュリティ技術転移パートナーシップを強化しなければならない。 |
| 調査結果④ | 調整や、監督が十分でないため、全体的な連邦サイバー・セキュリティ研究・開発活動は、現在焦点が定まっておらず、能率が悪い。 |
| 提言④ | 重要情報インフラ保護に関する省庁間作業グループ（Interagency Working Group on Critical Information Infrastructure Protection）が連邦サーバセキュリティ研究・開発活動を調整する中心となるべきである。 |

④ Memorandum on FY 2007 Administration Research and Development Budget Priorities

| | |
|---|---|
| ➢ 制定日 | ➢ 2005 年 7 月 |
| ➢ 提出者 | ➢ John H. Marburger, III 氏（Director, Office of Science and Technology Policy）、Joshua B. Bolten 氏（Directpr, Office of Management and Budget） |
| ➢ 目的 | ➢ 連邦政府機関の R&D プログラムの優先順位、象徴の枠組みをこえて行うべき重要な R&D プログラム、R&D プログラム・マネジメントにむけた投資決定のための R&D 投資基準などに関する指針を提供する。 |

同報告書は、PCAST と NSTC との協力のもと提示された、行政当局の研究・開発優先度をとりあげ、科学、技術における卓越性とリーダーシップを保つために、管理とパフォーマンスを改善すること強調している。同報告書において、R&D 優先度を以下のように提示するとともに、R&D 予算を付与される各機関は、省庁間の調整グループに参加できるよう準備しておく必要があるとした：
優先度が高く、CSIA に関連するものは、以下の通りである。

Memorandum on FY 2007 Administration Research and Development Budget Priorities
（抜粋）

| R&D 優先項目 | 概要 |
|---|---|
| 1. 国家安全保障 R&D | 国家の安全を保障し、テロに対する戦いに勝利に向けた、米国の科学と技術能力の充実が必要な分野では、近年で顕著な進歩が見られる。しかし、R&D を通して更なるこれら分野の充実を目指す努力をする必要がある。 |
| 2. 高性能コンピューティング、ネットワーク研究・開発 | NITRD の全プログラムが重要であることに変わりはないが、高性能コンピューティングとサイバー・インフラ R&D への投資は、その影響が広範囲におよぶことから、相対的に優先度が高くなるべきである。安全で、信頼できる分散コンピューティング環境のためのハードウェアやソフトウェア、膨大な情報の通信、分析、共用を可能とするツールなどの進歩したネットワーク研究は、発見を促し、新技術の進歩を可能にする。これらと NITRD 分野すべての研究・開発を支える機関は、NSTC を介して、将来の投資を導くための省庁間計画に参加することを期待されている。サイバー・セキュリティの重要性を反映し、これに関わる機関は、この分野の研究・開発資金の詳細なギャップ分析をおこない、NSTC を通じて仕事を続けるべきである。 |

⑤　INFOSEC Research Council（IRC） Hard Problem List

| | |
|---|---|
| ➢ 発表時期 | 2005 年 11 月 |
| ➢ 作成者・作成機関 | INFOSEC Research Council（IRC） |
| ➢ 目的 | ➢ 当報告書で示された種々の課題を解決することにより、情報セキュリティの大きな障害を取り除くと同時に、情報セキュリティ上の重大な問題を提示することにより、IRC メンバーがニーズにあった研究プログラムを行うことが可能となる。 |

米国国防総省、米国の非防衛分野の司法省、エネルギー省、商務省などの省庁、インテリジェンス・コミュニティーなど、情報セキュリティ研究に携わる連邦政府機関からなる組織である IRC は、1999 年にも「INFOSEC Research Council Hard Problem List」を発表しているが、2001 年のテロ事件や急速な技術の発展に伴い、1999 年の報告書の改訂版として、同報告書を発表した。

同報告書が提示した、今後 5 年から 10 年の間で、米国が、至急取り組むべき課題は以下の 8 つとなっている：

INFOSEC Research Council（IRC） Hard Problem List

| 課題 | 内容 |
|---|---|
| 世界規模での<br>アイデンティティ管理<br>（Global-Scale Identity Management） | ➢ Global Scale:身分証明・認証システムを利用する世界中の利用者を対象。<br>➢ 重要かつ機密事項を扱う IT システムにアクセスする際の、ハードウェア、ソフトウェア、更に認証や身分証明を行う人材についての問題を扱っている。 |
| 組織内部の危険要因<br>（Insider Threat） | ➢ Insider: セキュリティに係わることができ、アウトサイダーには与えられていない権限を付与された人物。<br>➢ Insider Threat: インサイダーが与えられた権限で、意図的・無意識に、権威を乱用しシステムのセキュリティを危険にさらす場合の問題を扱っている。 |
| 迅速な情報提供を行う<br>システム<br>（Availability of Time-Critical Systems） | ➢ 迅速な情報提供は、特にシステムが攻撃された際の場合等の悪条件の際、情報の機密性を守ることより重要である。<br>➢ 情報源が限られている、情報があちらこちらに点在しているなどといったような状況下においても、情報と情報システムの迅速な提供を確実なものとすることを課題としている。 |
| 拡張可能で安全なシステムを構築する<br>（Building Scalable Secure Systems） | ➢ 情報アシュアランスのレベルの向上にむけて、現在では市場に流通している製品を利用することが多いが、このやり方には限度がある。<br>➢ あらゆるシステム・コンポーネント及びシステムのデザイン、開発、検証を行う必要性を指摘している。 |
| 状況判断と攻撃特定<br>（Situational Understanding and Attack Attribution） | ➢ 情報システムの重要インフラに対する攻撃の影響を予測するのは、サイバー攻撃が複雑な性格を擁して来た事から、困難になってきている。<br>➢ 攻撃要因や攻撃規模などの特定、対処法等を含めた情報システムの理解の必要性を指摘している。 |
| 情報源の特定<br>（Information Provenance） | ➢ 情報主や、プログラム、データなどといったコンピュータに関することを扱っており、実際の内容より情報の統一性を重要視している。<br>➢ ペタバイトの情報をプロセスし、情報源を追跡・特定する技術の重要性を指摘している。 |
| セキュリティとプライバシー<br>（Security and Privacy） | ➢ 個人が情報を公開することに同意若しくは公開することを求められる場合も、個人のプライベートな情報を保護する為のツールの開発を課題としている。 |
| 企業レベルのセキュリティ・メトリクス<br>（Enterprise-Level Security Metrics） | ➢ 組織内でセキュリティについて、マクロレベルの見方をすることは非常に重要である。<br>➢ 数百万に及ぶユーザが利用するような巨大システムのセキュリティを効果的に測定するようなメトリクスの開発の必要性を訴えている。 |

(3) Federal Plan for Cyber Security and Information Assurance Research and Development 提言の内容

前述の各種報告・提言・法律をベースとし、さらに日々増加する情報セキュリティへの脅威に対抗すべく、CSIA IWG は、2006 年 4 月、「Federal Plan for Cyber Security and Information Assurance Research and Development」を発表した。

同報告書は、CSIA の定義として、①情報システム、ネットワーク、システム及び情報の認証への不法なアクセス及び破壊行為からの保護し、これらのデータの整合性を守る（integrity）、②情報への不正アクセス及び不正公開を防ぐ（Confidentiality）、③システム、ネットワークそして情報に必要な時に確実にアクセスすることができるようにする（Availability）の３点を挙げている。この定義の下、同ワーキング・グループは、現在の CSIA の技術及び能力の分析を行い、CSIA の現状と、実際に起こり得る CSIA への危険への対処能力の格差は危機的であり、さらなる対応策の必要性を指摘した。

この問題意識に基づき、「Federal Plan for Cyber Security and Information Assurance Research and Development」が提言しているポイントは、連邦政府の各省庁独自の R&D 活動への支援の必要性を訴えつつ、省庁間の枠組みを越えた、CSIA・R&D 活動の重要性を指摘していることにある。

CSIA IWG では、省庁横断型の R&D の枠組みと戦略的ポイントを示すため、以下 4 つの側面から、CSIA の強化に向けて現在行われている R&D 政策を分析している。:

- R&D カテゴリーと技術的側面
- R&D の技術的・資金上の優先順位
- 投資分析
- R&D の技術の今後

これらの分析をもとに、今後取るべき戦略として「10 の提言」とし掲げたものが、この度の報告書となっている。以下、各提言について、その提言がなされた背景・現状に並び、CSIA IWG が提案する対策をまとめたものである。これらの提言に加え、認証の問題、アクセス・コントロールの問題などについても同報告書は取り上げている。同報告書は、CSIA の R&D 政策に焦点をあてたものであり、教育・経済問題などその他の課題については扱っていない。また、同報告書には、各連邦省庁機関に対する拘束力は無く、各連機関の任務の重要性に従って予算編成を行うべきであるとしている。

## CSIA IWG による 10 の提言の背景・現状と対策・提言

| | |
|---|---|
| **①連邦政府の R&D 投資は、CSIA の戦略的ニーズに照準を合わせる** | |
| 背景・現状 | ➢ 今日の民間セクターの CSIA の技術市場で見られる新製品や新たな技術は、利益を生みだすことを念頭において開発されている結果、将来のサイバーへの危険の事前防止や対策など、必要な対処能力を備えていない。 |
| 対策・提言 | ➢ 連邦政府は、国の戦略的・長期的 CSIA のニーズの見直しを行い、これらニーズが連邦政府の R&D のニーズと合致しているか、また、民間セクターが積極的に係わる事のできる分野についての検討を行うべきである。<br>➢ 連邦政府機関は、技術開発における最優先事項に対する支援を行うなど、次世代 IT インフラの技術的基盤の発展を目指すべきである。 |
| **②最悪の危険を想定する** | |
| 背景・現状 | ➢ 今日一般的となっているサイバーへの脅威は、国の重要 IT インフラや経済に大きな打撃を与えるものではないが、実際に大打撃を引き起こしうる可能性は低いということから、大打撃を起こしうる脅威に対する対策が取られていない。 |
| 対策・提言 | ➢ 連邦政府の CSIA の R&D 予算は、最悪の危険に対する対処策開発と、IT システム全体のセキュリティ向上へ向けた革新的なアプローチの研究を中心として、配分されるべきである。 |
| **③CSIA・R&D を各機関及び省庁横断型の予算の最重要課題とする** | |
| 背景・現状 | ➢ 近年の緊縮財政が続く状況において、最重要事項に予算が配分されることが重要であるが、このことは、科学界を始めとする多くの分野での技術進歩が、業界全体の進歩につながる IT の R&D ではなおさらである。 |
| 対策・提言 | ➢ 各連邦省庁機関は、CSIA の R&D に関してこれまでに提出された政策指針を参考にするべきである。また、連邦政府の投資が、最大限の効果をあげるためには、CSIA の R&D は、個々の連邦政府機関だけではなく、連邦政府機関全体としての共同研究開発においても、最重要課題とされるべきである。 |
| **④　CSIA・R&D の現在行われている省庁間の協力体制を支援する** | |
| 背景・現状 | ➢ 同報告書で示された計画を実現するには、省庁間の協力が不可欠である。<br>➢ 省庁間の枠組みを越えた協力体制を敷くことにより、省庁間同士のコミュニケーションが活発となり、効率的な R&D 活動が可能となる。省庁間の共同作業を通して、R&D の成果を最大限に引き上げることが可能となる。 |
| 対策・提言 | ➢ 後述の「提案７：連邦政府のサイバー・セキュリティと情報アシュアランスの R&D ロードマップを作成する」に示されたロードマップ作成や、その他の CSIA の R&D 活動に、連邦省庁機関はそれぞれ代表者を送るべきである。<br>➢ 公式・非公式の各省庁高官レベルの協力体制は、セキュリティのツール、技術などが多大な影響を及ぼす CSIA の分野では非常に重要となってくることを認識するべきである。 |
| **⑤セキュリティをプロジェクト開始から念頭に置く** | |
| 背景・現状 | ➢ 今日のインフラの大部分は、セキュリティが最初から組み込まれているものではない。セキュリティに対する現在 |

| | |
|---|---|
| | の標準的なアプローチというのは、継ぎ接ぎ式のもので、現在認識されているセキュリティに対する攻撃への対策を詰め込んだものを装備するというものである。こういったアプローチは、攻撃に対する対処法としての効果は一定しておらず、長期的にみて、より安全なインフラを構築する為には、決して効果的であるとはいえない。 |
| 対策・提言 | ➢ 連邦政府の CSIA の R&D ポートフォリオは、今日の決して安全とは言えない継ぎ接ぎのインフラに取って代わる、より安全な次世代テクノロジーを開発する重要な R&D を支援するべきである。 |
| ⑥開発中の IT のセキュリティへの影響を見極める | |
| 背景・現状 | ➢ 新しい IT 技術は、IT インフラに、新たなセキュリティ上の問題を引き起こす可能性もある。また、新たな技術が、既存の IT インフラに導入されることにより、これまでの IT インフラの欠点を改善すること困難になる可能性もある。 |
| 対策・提言 | ➢ 連邦政府は、R&D を通して行う、光コンピュータ、量子計算、現在普及している組み込みコンピュータの分野で開発されつつある新しい情報テクノロジーのセキュリティへの影響力を見極める必要がある。こういった分析は、連邦政府の CSIA・R&D 計画において中心となるべきである。 |
| ⑦連邦政府の CSIA・R&D ロードマップを作成する。 | |
| 背景・現状 | ➢ 国の IT インフラの充実に向けた CSIA の技術の進歩は、連邦政府の R&D 機関において、省庁の枠を越えた技術的優先事項と協力体制について、合意があって初めて可能となるものである。 |
| 対策・提言 | ➢ 連邦政府機関は、当報告書の技術開発の優先事項と投資の分析を元に、民間セクターと共同で、CSIA の R&D の優先事項に関するロードマップを作成するべきである。ロードマップ作成により、省庁間に見られる技術的、投資的なギャップが浮き彫りにされると同時に、戦略的能力の向上につながることが可能となる。また、最優先事項に優先的に R&D が行われ、各省庁機関による投資も効率よく実施されることが期待される。これらのことから、連邦省庁機関は、ロードマップの共同作成に参加することが強く望まれる。 |
| ⑧CSIA の評価の為の新しいメトリクスを作成する | |
| 背景・現状 | ➢ IT 業界と国立研究コミュニティにおける最大の問題は、コンポーネント、システムそしてネットワーク・セキュリティのレベルを見極める効果的な技術やツールが存在しないことである。メトリクスの開発に関しては、最大額の資金援助も得ていないと同時に、最重要課題とも認識されていないのが現状である。 |
| 対策・提言 | ➢ ロードマップ作成の一環で、連邦政府機関は、コスト効率の良い IT コンポーネント、ネットワーク、システム・セキュリティの評価システム開発に向けた R&D を支援する、省庁横断型の計画を開発、実施するべきである。<br>➢ R&D によって開発された精度の高い CSIA のメトリクスや、評価ツール、ベストプラクティスは各機関で、連邦システムセキュリティ評価に利用されるべきである。 |
| ⑨民間セクターとの協力体制を、より効率的にする | |
| 背景・現状 | ➢ 民間セクター・政府を始めとする公共セクター、双方とも、一般に出回っている技術を元に IT インフラの構築・保護を行っている。このため、R&D から生まれた技術の、一般市場への効率的な移転が大きな課題となってい |

| | |
|---|---|
| | る。こういったニーズを満たすためには、民間・公共セクター間のコミュニケーションと協力体制を構築し、継続していくことが不可欠であり、これらを通して初めて、それぞれの強みを最大限に活かす事が可能となるのである。 |
| 対策・提言 | ➢ 連邦政府は、民間セクターの CSIA の現状及び、テクノロジー格差を見極める対策の再検討を行うと共に、民間セクターの協力のもと、CSIA・R&D に対するニーズと最優先事項に関する民間セクターの認識のより深い理解を目指すべきである。民間セクター・公共セクターの R&D に対するニーズ、優先事項、投資傾向を互いに理解することにより、両者共通の利益となる CSIA の改善・向上に向けた R&D の実施が可能となり、また、CSIA の R&D の限られた予算を有効に活用することができるのである。<br>➢ CSIA・R&D を支援している連邦政府機関は、共通の利益を追求する連邦政府・民間セクター双方の重要インフラの担当者とのコミュニケーションや協力体制の向上に努めるべきである。 |
| ⑩国際協力をも視野にいれた、R&D 協力体制を強化する | |
| 背景・現状 | ➢ インターネットは、世界中で約 10 億人に利用されている世界的なインフラへと大きく成長した。しかし、当報告書が伝えるように、インターネットは、国の最も重要な物理的及び IT インフラに接続されていることも考慮する必要がある。 |
| 対策・提言 | ➢ 世界中を網羅する、複雑で多角的性格を持つインターネットの性質を考えると、連邦政府はより安全な次世代 IT インフラ構築に向け、民間セクター、IT 業界、学界との協力を推進するべきである。<br>➢ 米国と米国のパートナーの共通の利益を守るための国際協力を行う上で障害を見極め、改善されるべきである。 |

## 2. 連邦政府機関による CSIA への取り組み

CSIA IWG の設立及び計画発表をうけ、今後、省庁間の連携が進められると見られる。一方で、各省庁による独自の取り組みもすでに行われてきている。以下では、その具体例として、NSF と商務省の NIST における取り組みついて紹介する。

### (1) National Science Foundation（NSF）

2006 年 2 月 6 日に発表された 2007 年度の大統領予算案において、連邦政府の IT 関係の R&D 政策の中心機関である NITRD への予算は、前年度より 7.7%上昇の、約 30 億 7,000 万ドルとなった。これは、大方の予想を裏切る「記録的な伸び」であり、連邦政府の IT 関連 R&D を重要視している姿勢を示すものとなった。

NSF は、この大幅な伸びを見せた NITRD の予算の中で最も予算を大きく配分されている連邦政府機関であり、2007 年度では約 9 億 400 万ドルの予算が計上されている。NSF で最も予算配分が大きかったのは、Computer and Information Science and Engineering directorate（CISE）部門で約 5 億ドルの予算配分を得たが、同時に、NSF の CSIA に対する予算も大幅に増加していることは注目に値する。中でも、NSF の「Cyber Trust（CT）」プログラムの予算は、前年比 1,000 万ドル増加の 3,500 万ドルとなり、前年比 26%増の 9,700 万ドルの予算規模である NSF の情報アシュアランス研究の大きな部分を占めることとなった。

今日の米国社会の根幹においてコンピュータ・システムは必要不可欠であるが、これらシステムはサイバー攻撃に対して非常に脆いものであるという懸念は杞憂のものではないとして、CT は、以下の様なコンピュータ・システムのビジョンを達成することで、国のサイバー・セキュリティを向上を目指した研究支援活動を支援している。

- サイバー攻撃に対する予測能力や対応能力を向上させ、サイバー・セキュリティを向上させる。
- コンピュータ・システムについて十分学んだ人材を、同分野以外からも募り、これら人材を中心に、コンピュータ・システムの開発、設定から管理・運営を担当させる。
- 安全で倫理的なコンピュータ・システムの使用について学んだ一般人が利用する。

上記 CT のビジョンを達成し、国のサイバー・セキュリティ向上実現の為、NSF は以下の様なプロジェクトに対する支援を行う：

- 関連する知識基盤の発展（スカラシップ授与）
- 専門家のみならず、一般人の利益になる様、研究と教育の統合
- 政策、経済、国の体制等への、技術研究の効率良い統合

NSF のスカラシップ授与に関して公開されている記録は、2002 年からとなっており、近年の例としては、カリフォルニア大学サンディエゴ校（University of California, San Diego）が 15 万ドル、アリゾナ州立大学（Arizona State University）が約 20 万ドル、マサチューセッツ工科大学（Massachusetts Institute of Technology）が約 10 万ドルがそれぞれ、2006 年 6 月現在付与されている。

また、これら研究資金提供活動以外に、NSF は、DHS、更に日本の文部科学省、科学技術振興機構（JST）などと共同で、「United States-Japan Critical Information Infrastructure Protection Workshop」というワークショップを開催している。これは、重要情報インフラの保護についての日米双方に関わる重要課題や研究イニシアチブについて議論を重ねるもので、2004 年に第 1 回会議が開かれている。

(2) 商務省 NIST

米国の世界における現在の技術的優位性を今後も維持することは、米国の経済発展、国民の生活の質の向上、国土防衛に直結するという認識の下、商務省は、米国のビジネス界が今後もその優位性を維持できるようなインフラを整備することを、その重要な戦略的ゴールとしている。

商務省の技術局（Technology Administration）管轄下に属する NIST は、1901 年の設立以来、計測学、標準、技術の進歩を促進し米国のイノベーションと競争力強化の土壌を整えてきた。NIST は 17 部門からなっているが、その中の一つ、「Information Technology Laboratory」の「The Computer Security Division・Computer Resource Center」が、情報セキュリティ・システムの改善に向け、4 つの「フォーカス・エリア」を設定し、活動を行っている。

# NIST フォーカス・エリア

| フォーカス・エリア | 担当部署 | 目的 | 対応分野 |
|---|---|---|---|
| 暗号標準と応用（Cryptographic Standards and Applications） | Security Technology Group | 情報源の信頼性、インテグリティ、機密性保護手段としての暗号の発展を目指す。 | ＊ シークレット・キー、パブリック・キーの暗号テクニック<br>＊ 認証システム応用<br>＊ 暗号プロトコールとインターフェース<br>＊ パブリック・キー認証・マネジメント<br>＊ スマート・トークン<br>＊ 暗号 Key Escrowing<br>＊ セキュリティ・アーキテクチャ |
| セキュリティ・テスト（Security Testing） | The Security Testing and Metrics Group | 政府・業界と協力のもと、データ検証プログラム等の支援や、セキュリティ・評価ツールの開発・促進により、安全なシステムやネットワークの構築を目指す。 | ＊ セキュリティ・メトリクスの開発と管理<br>＊ セキュリティ評価基準と評価方法<br>＊ テストとテスト方法<br>＊ 研究所認定の為のセキュリティ評価基準<br>＊ テスト済みの製品の利用に関するガイダンス<br>＊ アシュアランスの方法とシステム全体にまつわるセキュリティと評価の方法論研究<br>＊ セキュリティ・プロトコールの妥当性のチェックについて<br>＊ 業界の自主基準機関を筆頭とする評価関連活動を行っている団体の、評価活動との適切な協力体制 |
| セキュリティ・リサーチと開発中の技術（Security Research/Emerging Technologies） | The Systems and Network Security Group | システムの欠点を改善し、新たな技術の安全な利用を目指す。 | ＊ 侵入検知を始めとする応用対策<br>＊ ファイアーウォール<br>＊ スキャニング・ツール<br>＊ セキュリティたたき台<br>＊ 脆弱性分析・改善<br>＊ アクセス・コントロール<br>＊ 事故対応<br>＊ アクティブ・コード<br>＊ インターネット・セキュリティ |
| セキュリティ・マネジメント及ガイダンス（Security Management and Guidance） | The Security Management and Guidance Group | セキュリティ・マネジメント指針の開発。 | ＊ リスク・マネジメント<br>＊ セキュリティ・プログラム・マネジメント<br>＊ トレーニングと認識<br>＊ 緊急時対策<br>＊ 個人セキュリティ<br>＊ 行政処置<br>＊ セキュリティ促進の際の調達と「Computer Security Expert Assist Team」の管理・運営を通して連邦政府機関におけるそのような指針を普及さること。 |

## 3. CSIA 関連 R&D を促進しようとする産官学の動き

これまで見てきたような、政府による CSIA 関連 R&D を後押しする格好で、2006 年 6 月 28 日、Federal Bureau of Investigation（FBI）、U.S Secret Service、LexisNexis、IBM、Carnegie Mellon University、Syracuse University など、業界、大学、連邦政府法機関が共同で、Utica University に「Center for Identity Management and Information Protection（CIMIP）」を結成した。

CIMIP は、自ら CSIA の R&D に乗り出す組織ではないが、同分野の英知を各界から集め、より安全な米国社会を構築する上で、アイデンティティ・マネジメント、情報共有、データ保護、という米国全体に関わる研究アジェンダを深め、政策、規則、法律制定に関わっていこうとする団体である。CIMIP の今年度予算は、50 万ドル、その半分が企業から、残り半分は連邦政府からのグラントとなっている。翌年には、予算額が今年度比、2 倍から 3 倍になる見込みである。

これまでに同様の問題を扱ってきた「Forum of Incident Response and Security Teams（FIRST：コンピュータ・セキュリティに事故が起こった際、若しくは事前に対処することができるように、組織メンバー、地域社会と協力体制を構築することを目的としている。産・官・学から 170 以上の組織が参加している。）」などが、問題が発生する度に、それぞれに個々の問題への対応を行ってきたことと異なり、CIMIP は、これまでの研究結果をまとめあげ、IT セキュリティに関わる問題の情報交換の場を提供したいとしている。

CIMIP は発足したばかりであるが、すでに特に緊急性の高い具体的な研究課題として、米国における IT 犯罪の中で、ここ 2、3 年で急激に増加した身元詐称・個人情報盗難（Identity Theft）の原因、さらには、これら問題が発生しても初期段階における検知や予防に関するものを挙げている。同団体はまた、こうした課題に対する研究開発の重要性を指摘することに加え、政策決定、法律、規制などの、これら問題に対する影響も調査・研究するとしている。

（参考資料）

http://primera.tamu.edu/internet/nren-bill.html
http://www.cra.org/Policy/Documents/Bills/hr3332.html
http://www.nitrd.gov/about/presentations_nco/2006/20060517_sszykman/index.php?slide=02.JPG
http://www.nitrd.gov/pubs/brochures/nitrd.pdf
http://www.nitrd.gov/subcommittee/csia.html
http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf
http://www.nitrd.gov/pubs/2007supplement/
http://www.house.gov/science/cyber/hr3394.pdf
http://www.whitehouse.gov/pcipb/executive_summary.pdf
http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf
http://www.whitehouse.gov/omb/memoranda/fy2005/m05-18.pdf
http://www.infosec-research.org/docs_public/20051130-IRC-HPL-FINAL.pdf
http://www.infosec-research.org/docs_public/IRC-HPL-as-released-990921.doc
http://www.ostp.gov/PCAST/pcast.html
http://www.house.gov/boehlert/
http://www.house.gov/science/committeeinfo/history/index.htm
http://thomas.loc.gov/cgi-bin/cpquery/T?&report=hr355p1&dbname=107&
http://www.house.gov/science/press/107pr/107-142.htm
http://thomas.loc.gov/cgi-bin/cpquery/T?&report=hr355p1&dbname=107&
http://www.house.gov/science/press/107pr/107-142.htm
http://www.house.gov/science/press/107pr/107-155b.htm
http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf
http://usinfo.state.gov/journals/itgic/1103/ijge/gj11.htm
http://www.infosec-research.org/charter.html
http://www.infosec-research.org/
http://www.cra.org/govaffairs/blog/archives/000470.html
http://www.cra.org/
http://www.nsf.gov/about/
http://www2.gwu.edu/~usjpciip/
http://www.utica.edu/
http://news.com.com/Coalition+launches+ID+theft+center/2100-1029_3-6088997.html
http://www.first.org/

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。