CIPPS
Center for International Public Policy Studies

「サイバーセキュリティに関する米国出張調査報告書」

2013.7.22 ～ 7.26

国際公共政策研究センター
主任研究員 益岡 竜介 (masuoka@cipps.org)
主任研究員 石野 務 (ishino@cipps.org)

2013 年 12 月

【目　次】

I. サイバーセキュリティ 米国調査出張報告

1. 出張日程及び面談等

2013 年 7 月 22 日～26 日に亘り、米国のサンノゼ、及びワシントン D.C.を訪問し、政府機関、シンクタンク、教育機関、セキュリティ関連企業などと、意見交換を行った。主な面談先と面談テーマは表 1 の通りである。

表 1: 面談先等及び面談のテーマ

日付	面談先	面談の主テーマ
7/22 (月)	EPRI (Electric Power Research Institute)： Ms. Annabelle Lee, Senior Technical Executive (Joined through teleconference system) Mr. Jimmy Herren, Account Executives, Technical Advisory Services, Power Delivery & Utilization	• スマートグリッドに関するサイバーセキュリティについて
	FireEye： Mr. Ashar Aziz, Founder, Vice Chairman, & CTO Mr. Doug Schultz, Vice President APAC/Japan Mr. Bill Hau, Vice President / FireEye Labs Mr. Travis Rosiek, Federal Architect Mr. Yoshi Ozawa, Sr. Systems Engineer Mr. Naoyuki Ono, Sr. Enterprise Territory Account Manager	• サイバーセキュリティにおける官民連携の在り方・人材育成の在り方について
7/24 (水)	UMBC (University of Maryland, Baltimore County)： Mr. Donald F. Norris, Professor, Department of Public Policy and Chair and Director, Maryland Institute for Policy Analysis and Research Dr. Timothy W .Finin, Professor, Department of Computer Science and Electrical Engineering Dr. John T. Pinkston, Professor, Department of Computer Science and Electrical Engineering Mr. Anupam Joshi, Director, Department of Computer Science and Electrical Engineering Mr. Richard F. Forno, Ph.D., Graduate Program Director Cybersecurity, Department of Computer Science and Electrical Engineering Mr. Don Engel, Assistant Vice President for Research, Department of Computer Science and Electrical Engineering	• サイバーセキィリティ人材育成の在り方について
7/25 (木)	CSIS (Center for Strategic and International Studies)： Mr. James Andrew Lewis, Director and Senior Fellow, Technology and Public Policy Program	• 日本と米国におけるサイバーセキュリティの状況について
7/26 (金)	DAC (Decisive Analytics Corporation)： Mr. John S. Donnellon, President Mr. Mark Hall, Vice President, Cyber Security Engineering	• サイバーセキュリティにおける官民連携の在り方について

	Mr. Wayne Fujito, President, International Division, DAC, Chairman, NATO Industrial Advisory Group, and Chairman, NDIA International Division Ms. Cristiana Brafman Kittner, Defense Analyst/Export Compliance Official	
	Cyber Maryland： State Government of Maryland: Mr. Patrick Tonui, Program Manager, Security and Information Technology, Office of Strategic Industries & Innovation, Maryland Department of Business & Economic Development	• サイバーセキュリティにおける企業育成の在り方・人材育成の在り方について

2. 質問事項

今回の米国出張では、米国のサイバーセキュリティの現状や、サイバーセキュリティにおける官民連携の在り方、人材育成の在り方、産業育成の在り方、スマートグリッドにおけるサイバーセキュリティついての課題について、実務担当者や有識者と意見を交換することを目的とした。面談では、以下のような質問事項を挙げた。

表 2:主要質問事項

[テーマ 1] インフラ制御におけるサイバーセキュリティの課題について

以下のような課題について意見交換を行った。

(1) インフラ制御におけるサイバーセキュリティの特色について

(2) スマートグリッドにおけるサイバーセキュリティについて

[テーマ 2] 米国のサイバーセキュリティの現状について

我が国のサイバーセキュリティの現状について説明したうえで、米国のサイバーセキュリティの現状について情報を交換した。

(1) 人材育成・教育

(2) 産業育成

(3) 組織

(4) その他サイバーセキュリティの最近の状況について

3. レポートの構成

第 II 章で上記の面談の概要を述べる。 面談のより詳しい内容は第 IV 章に収録した。それらの面談を通じて示唆されることを第 III 章にまとめた。 なお一般的な米国におけるサイバーセキュリティ政策の最近動向は、JETRO/IPA ニューヨークオフィスのレポートの前篇[1] と後編[2] に詳しくまとめられているので、そちらも参考にして欲しい。

[1]米国におけるサイバーセキュリティ政策の最近の動向 - 前篇 - ニューヨークだより
http://www.ipa.go.jp/files/000026543.pdf
[2]米国におけるサイバーセキュリティ政策の最近の動向 - 後編 - ニューヨークだより
http://www.ipa.go.jp/files/000027052.pdf

II. 面談概要

1. EPRI (Electric Power Research Institute)

(1) EPRI 概要および面談相手

公共の発電、送電、電力利用に関する研究、開発、実演を行う非営利団体。米国エネルギー省より、電力関係のサイバーセキュリティに関する研究を委託され、NESCOR (National Electric Sector Cybersecurity Organization Resource) という組織を立ち上げ、対応している。面談相手は以下である。

- Ms. Annabelle Lee, Senior Technical Executive (Joined through teleconference system)
- Mr. Jimmy Herren, Account Executives, Technical Advisory Services, Power Delivery & Utilization

(2) 一般的なことがら

- NESCOR はエネルギー省が資金を提供する官民提携のプロジェクト (public-private partnership) である。 EPRI も一部費用を負担している。
- 制御システムに関するサイバーセキュリティは、通常の情報システムのサイバーセキュリティとは大きく異なる性格を持ち、サービスを提供し続けることが第一である。またパッチを簡単にあてられないことも特徴である。
- 電力分野の課題としては、30～40 年も前にセキュリティが考慮がされていなかった時代に作られた、セキュアでない機器が現存しており、セキュリティ機能を後付けで追加するのも難しいことが挙げられる。短期的には、周辺部における障壁 (Firewalls) や、侵入検知システム (IDS: Intrusion Detection System)、侵入防止システム (IPS: Intrusion Prevention System) などによる防御が考えられ、長期的にはよりスマートな機器との入れ替えが考えられる。
- サイバーセキュリティは他のリスクと相対的なものである。多くの中小のインフラ企業にとっては一般の財政リスクの方が課題である。
- 電力会社はリスクに優先順位を付け、何が彼らにとって重要であるかを決めることによりリスクとコストのバランスをとるべきであろう。全てのリスクに対して費用や専門人員をかけられるわけではない。

(3) スマートグリッド・スマートコミュニティでのサイバーセキュリティの課題について

- 片方向から双方向の情報伝達へのシフトや、経済的な理由から、機器や専用のシステムやプロトコル[3] に汎用的なもの用いられることにより、脆弱性がもたらされる。
- 昔と違って、機器に対してはファームウェアソフト[4] や、通常のソフトのパッチが適用されなければならない。

[3] コンピューターの通信接続手続き
[4] ハードウェアの基本的な制御を行うために機器に組み込まれたソフトウェア

- スマートグリッドにおける個人のプライバシーの取扱いが世間の注目を集めている。
- 電力会社の規模によりリスクが異なっている。大企業は、国家からの攻撃の様な大規模攻撃に関心があるが、中小企業はそれほどでもない。どの規模の組織も、大衆の反応や経済的な安定性には関心がある。

(4) スマートグリッドのサイバーセキュリティ対策について

- データの機密性を第一とする通常の情報システムのサイバーセキュリティ対策とは異なり、制御システムにおける優先順位は、①可用性（安定供給)、②完全性、および、③データの機密性の順である。
- 情報システムのセキュリティには多層防御（defense in depth）が求められるが、制御システムは攻撃を受ける面がより広く(例えば、変電所に対する攻撃は安定供給に重大な影響を及ぼす)、広域防衛（defense in breadth）が求められる。

2. FireEye

(1) FireEye 概要および面談相手

2004 年にサイバーセキュリティ、特に標的型攻撃対策製品の開発・販売を目的として設立された民間企業であり、現在、40 カ国に 1000 以上の顧客を有している。面談相手は以下である。

- Mr. Ashar Aziz, Founder, Vice Chairman, & CTO
- Mr. Doug Schultz, Vice President, APAC/Japan
- Mr. Bill Hau, Vice President, FireEye Labs
- Mr. Travis Rosiek, Federal Architect
- Mr. Yoshi Ozawa, Senior Systems Engineer
- Mr. Naoyuki Ono, Senior Enterprise Territory Account Manager

(2) FireEye の展望と製品について

- 当時（2004 年）脅威や攻撃者の様相が深刻化することが明らかになったことと、以下を予見したため、FireEye を設立した。
  - 脅威や攻撃者の変化が進み、明確になっていけば、既存の方法では全く対処できなくなる。
  - 攻撃者はまずその目的において変化していく。 2004 年当時のいたずらのような特に深刻でない目的から、窃盗犯による金銭搾取目的とスパイによる情報の獲得目的の(現在では最も顕著になっている) 2 つの目的となる。
  - 窃盗犯やスパイが既存のセキュリティシステムで捕まらないように、脅威は密かで、偽装され、システム内に入りこみ見えにくくなる。
- 防御構造（defensive architecture）を再考することが 2004 年当時の当社の目的であった。アンチウィルスエンジンや、ブラックリストモデルのような当時の支配的な防御構造は、未知の脆弱性を使ったネットワークに現れるたびにその姿を変える新しいコードを使

った攻撃に対しては無力であった。 FireEye の防御構造は、事前に考えられた製品デザインは無く、攻撃者によって規定される。 FireEye は攻撃者の気持ちになり、攻撃側にたった思考実験を行う。ファイルのみを確認するアンチウィルス・ソフトウェアなど今日のほとんどのシグネチャーベースのセキュリティ製品とは異なり、ゼロデイ攻撃分析構造のプリズムを通して、攻撃のライフサイクルのすべての段階に於いて、攻撃の構造が分析されるべきである。

- FireEye はシステムや仮想マシンのバックグランドを有しており、これをセキュリティ分析に応用することを考えた。仮想デスクトップやデータセンター統合を目的とする XenSource[5] や VMware の仮想マシンとは全く異なるデザイン目的を有していたので、FireEye は、緩和と感知機能を備えた、脅威認知ハイパーバイザー[6] をゼロから作り上げた。そのため FireEye のハイパーバイザーは一般にマルウェアによって感知されない。
- 別の研究に拠れば、平均的に侵入に気付くのに 80 日、また、気付いてから解決するまでに 123 日かかり、侵入への対策コストは 8 万 4 千ドルかかる。一方、 FireEye は侵入を数分で見つけ出し、解決までの時間を平均 2 週間にまで落とすことができる。

(3) FireEye の現在の活動について

- FireEye が成功してきた理由は、脅威の変遷と防御構造の正しい姿を正確に予想し、とても独自で質の高い方法で、すべての要素を組立てることができたためである。
- FireEye のアプローチが正しいことは、実際の検知によって証明される。毎日、顧客のネットワークにおいて、ほかの会社によって見逃された何千もの攻撃が発見される。
- 創設期から現在、そして将来に亘り、 FireEye の一番の仕事は、いくつもの攻撃方法 (web, e-mail, ファイル、モバイルなど) を持つ脅威がどれだけ進化しようとも、顧客を守ることであり、株主を喜ばせることではない。 FireEye は本当に、顧客を守るための防御構造の構築を望んでいる。 FireEye の今日の戦略はクラウドの中で無く顧客企業の建物内に設置されたアプライアンス (特定用途のコンピュータ) 内で分析を行うことである。FireEye は、ウェブからの攻撃だけでなく、E-mail 内のリンクや E-mail の添付ファイルも見ており、昨今はモバイルアプリも見るようになった。

(4) 官民連携について

- FireEye は各国政府と連携し、また各国政府に、重要インフラや国家安全保障に対する存在する重大なリスクや高度な脅威や、今まさに起きている攻撃の現実や急速に進化する実態に応じたソリューションや防御構造の必要性について教育している。
- FireEye は連邦政府の IT セキュリティに関する調達戦略の情報を提供し続ける。 サイバーセキュリティに必要とするものは、戦車、航空空母、戦闘機に必要とするものよりもずっと速く変化する。
- FireEye は脅威の展望や発見したことについての情報共有ができように政府系 CERTs

[5] オープンソースの仮想化ソフトウェア
[6] 1 台のコンピューター上で複数の OS を動かすための仮想化ソフトウェア

を含む、多くの異なる CERTs と緊密に協働している。

- 国が出来るもっとも大きな投資は、サイバー防御であり、サイバー攻撃ではない。 それは、サイバー攻撃において攻撃元の特定が困難なため、抑止的な解決は最も効果的な方策にはならないためである。

(5) 人材教育開発について

- 教育は FireEye にとり、とても重要なキーである。 FireEye は自身の従業員、顧客、パートナーの訓練や、全世界的に、特に政府や銀行のような洗練された顧客に対しての訓練コース提供に投資している。
- FireEye はブラックハットのようなハッカーは雇用しない。雇用においては十分な経歴調査を行う。一方、模擬戦闘や侵入テストを行うための科学者は雇用している。
- 暗号学のような伝統的なセキュリティのカリキュラムは今日のセキュリティには適合していない。現実の世界のシステムの不具合は、数学的な処理にそぐわない。
- 2002 年に、サイバーセキュリティにおける膨大な人材不足に対応するための、学部生や大学院生向けの 2 つの政府の奨学金が開始された。それは、国防総省による、"Information Assurance Scholarship Program"と、全米科学財団による "CyberCorps" である。
- 上記二つの奨学金は、学業の授業料や宿舎料、教科書代のすべて、あるいは一部について、上限を 2 年間として適用され、さらに給付金も提供される。学生は奨学金を受けている間、夏季の政府機関でのインターシップへの参加が義務付けられており、卒業後は奨学金を受けた期間と同等の期間に亘り政府の仕事につかなければならない。

3. UMBC (University of Maryland, Baltimore County)

(1) UMBC 概要および面談相手

メリーランド州立大学システムの一環として 1966 年に設立された。一般教養教育、および自然科学や工学の教育を行っている。面談相手は以下である。

- Dr. John T. Pinkston, Professor, CSEE (Department of Computer Science and Electrical Engineering)
- Dr. Timothy W. Finin, Professor, CSEE
- Dr. Anupam Joshi, Director, CSEE (from India through a video conference system)
- Dr. Richard F. Forno, Graduate Program Director, Cybersecurity, CSEE
- Dr. Don Engel, Assistant Vice President for Research, CSEE
- Dr. Donald F. Norris, Professor and Chair, Department of Public Policy/Director, Maryland Institute for Policy Analysis and Research

(2) UMBC におけるサイバーセキュリティ教育について

(a) National Centers of Academic Excellence in Information Assurance Education (CAE/IAE)

- CAE/IAE は NSA(国家安全保障局)と DHS(米国国土安全保障省)による認証プログラムであり、現在 50 校程度の大学が認証されている。大学には 2 年毎にコースの説明書を提

出することが求められている。

(b) UMBC Center for Cybersecurity

- 昨年設立されたこの傘型の組織の下で、(1) CSEE における研究指向の大学・大学院向けサイバーセキュリティコース、(2) サイバーセキュリティ大学院プログラム、(3) UMBC Training Centers Cybersecurity Academy の 3 つのプログラムを通して、いくつものレベルの授業を提供している。

(c) CSEE におけるサイバーセキュリティコース

- CSEE では研究指向の大学と大学院(マスターコースや博士コース)の講座がある。
- eBiquity グループでは、ソーシャルメディア、モバイル、セマンティック・ウェッブなどの分野において機械学習やアルゴリズムの研究が行われている。
- サイバーセキュリティに関して CyberCorps という NSF (National Science Foundation: 全米科学財団) と OPM (Office of Personal Management: 人事局) の "Scholarship for Service" と、国防総省による IASP (Information Assurance Scholarship Program) という、2 種類の非常に寛大な奨学金プログラムがある。

(d) サイバーセキュリティ大学院プログラム

- 大学院長の発案で 3 年前に開設された。専門職系大学院修士プログラムでは 10 コース、資格取得プログラムには 4 コースの履修が必要であり、来秋からの学期に 170 名が登録した。
- 研究者ではなく、技術リーダーや実務上の対応を必要とするマネージャーなどの、サイバーセキュリティの実践者を生み出すことを目的としている。
- 現実の勤務環境でサイバーセキュリティ知識を応用できるように、技術的な側面を超えて、経済学や、政策、法律の授業を含んでいる。
- 学生の 80%は社会人(定時制)であり、そのうちの半数は政府の職員か、政府の軍事部門の契約社員である。

(e) UMBC Training Centers Cybersecurity Academy

- 当初は、陸軍や海軍向けのものであった。1 週間のものから、数か月に亘るブートキャンプのようなものまで異なった期間の様々なコースを供与している。

(f) The Maryland Cyber Challenge

- 3 年前に USBC によって始められたサイバー戦争ゲームである。高校生、大学生、サイバー産業の専門家などが参加する。参加者は、一連のコンペで、コンピューターやネットワークをいかに防御するかについて取り組む。

(g) UMBC サイバーディフェンスチーム

- 大部分が学部生である生徒のグループが、サイバーの攻撃側と防御側に分かれ演習を行ったり、上記の "The Maryland Cyber Challenge" などのイベントのサポートをしている。

(h) 奨学金

- 今年の 9 月にノースロップ・グラマン社とサイバーセキュリティの奨学金を始める。1 百万ドルが、UMBC(15～20 人の学生を予定)と、UMCP[7]に与えられる。
- “Scholarship for Service”は、勤学士や修士、博士に対する寛容な奨学金である。連邦政府での職が保証されるが、民間で働けば 50%多い給与を得ることができるため、制約になっているかもしれない。

(3) 官学・産学連携について

(a) BHEF (Business Higher Education Forum)

- ノースロップ・グラマン社などの軍需産業や金融機関、IT 会社などの CEO や、大学の学長などがメンバーとなっている、米国での教育や労働力の課題に対するソリューションを推し進める団体である。メリーランド州が最初の “Undergraduate Cybersecurity Network”の地域デモンストレーションネットワークとして選ばれた。

(b) サイバーセキュリティの中心地としてのメリーランド州とワシントン D.C.地域

- メリーランド州とワシントン D.C.地域には、サイバーセキュリティ関連機関などが集積しており、多くのサイバーセキュリティ技能を有した人がいる。広域 D.C.地域では、1 万 5 千もの雇用が生まれていると言われている。

(c) UMBC

- UMBC は IT 学位の主要な授与大学であり、NSA(国家安全保障局）に対してコンピューター関連の卒業生を一番多く（今までに 1000 人程度）送っている。

(d) UMBC リサーチパーク

- UMBC のキャンパスの横に、UMBC が所有する UMBC リサーチパークがある。環境は良く、賃料は安く、サイバーセキュリティ関係の政府機関にも距離的に近い。
- UMBC は企業から少しの株式（5 年間に亘り、毎年 1 %ずつ）をもらう代わりに、入居企業にガイダンスや、低賃料、話し合い、イベントなどのベネフィットを提供する。
- サイバーのインキュベーターは、生命科学やクリーンエネルギーの 2 つのインキュベーターよりも規模が大きい。20 以上のサイバーセキュリティ関連企業や NSA を含む政府機関が場所を借りている。

(4) IT と e－ガバメントについて

- 米国には 19,000 の地方政府がある。地方政府が e－ガバメントを導入しない 5 つの理由(理由のトップは資金）の一つにセキュリティが必ず含まれている。
- 社会には、常にイノベーションとセキュリティや、プライバシーとセキュリティの間の論争がある。地方政府の情報は、人事情報、犯罪歴、病歴、および進行中の入札情報以外は、ほとんど（90%以上）が公表されている。地方政府や州政府は、誰かがそれを盗むという「機密性」のリスクよりも、誰かが記録を改ざんするというデータの「完全性」のリスク

[7] University of Maryland, College Park: メリーランド大学 カレッジパーク校

を重視している。

- 1970 年代に、URBIS プロジェクトにおいて、地方自治体の様々の用途に使える標準的なソフトウェアを開発・普及させることが試みられたが、数年間して完全に失敗に終わった。このプロジェクトは、その規模が大きすぎて失敗した。

(5) その他

(a) サイバーセキュリティ専門家のキャリアパスについて

- サイバーセキュリティの仕事はたくさんある。この地域では、技術系の人材も、実践系の人材（practitioner）も、比較的簡単に納得いくポジションを得ることができる。米国の労働市場では、サイバーセキュリティはブームである。
- 修士や博士の学位は、産業界での昇進の強みとなる。サイバーセキュリティの専門家になるためには、防御を行えるようになる前にネットワークの構築など基本的なことを理解する必要がある。

(b) サイバー攻撃側になることについて

- DARPA (Defense Advanced Research Projects Agency: 国防高等研究計画局）は、サイバー攻撃能力の研究開発に資金の拠出を始めた。
- National Defense Authorization Act for FY14 は、大統領にサイバー兵器の蔓延に対する政策とフレームワークを用意することを求めている。しかし、たった 1 MB 程度しかないマルウェアが何百万という方法で送り込まれている現状では、極めて困難である。

(c) サイバー攻撃のコストシミュレーションについて

- サイバー攻撃による損害について、確かな費用推定を行うことは困難である。

(d) 情報公開法(Freedom of information Act)関連の動向について

- 民間企業は、情報公開法をインシデントの情報を公開しない言い訳としている。情報公開法は、明確に、各企業の固有情報の公開を除外している。
- 下院は、”Cyber Security Information Sharing and Protection Act” 法案を通したが、上院はこれを 2 度拒んだ。この法案は、サイバー攻撃が起きた場合に、民間企業に対してパケットレベルの情報提供を強制するものである。

(e) サイバーセキュリティの研究開発センター

- NIST (National Institute of Standards and Technology: 米国標準技術局）は、サイバーセキュリティに関して、適切な技術を有する人を訓練するために、FFRDC (Federally Funded Research and Development Center: 国立研究開発センター）を設立しようとしており、UMBC や UMCP は企画書の準備をしている。

(f) サイバーセキュリティの最近の状況

- サイバーセキュリティを取り巻く最近の状況は、ドットコムバブルと似た面がある。
- 現在のサイバーセキュリティは、非常に労働集約的である。あまりに多くの看護師がその症状を看ているような状況だが、必要とされているのは、根本的な原因を探り適切な治療

を行う医師である。根本的な解決策として以下が示唆される。

- 単純な電化製品への TPM[8] の導入
- 幅広い人々に対する、(サイバーセキュリティに関する) 高校レベルの教育
- 法や政策の強化
- ワイヤレス機器に対する連邦通信委員会の認可のような、コンピューターに対するセキュリティ認可

4. CSIS (Center for Strategic and International Studies)

(1) CSIS 概要および面談相手

1962 年にジョージタウン大学の付属研究機関として設立された保守系シンクタンク。1987 年同大学から独立した。アメリカ陸軍・海軍直系の軍事戦略研究所でもある。面談相手は以下である。

- Mr. James Andrew Lewis, Director and Senior Fellow, Technology and Public Policy Program

(2) マンディアントレポートやスノーデン事件の影響について

- マンディアントレポートは、何が起こっているのかについてよく解っていない一般の国民に実際何が起きているのかを知らせるという意味で重要であった。一方、マンディアントレポートが出る前に米国政府内の機密報告が存在していた。そこでは、より詳細に中国のサイバースパイ活動の状況が説明されており、それは、我々が思っていたよりも深刻であった。この機密報告は中国に対する見方を変え米国政府側に大きな影響を与えた。
- スノーデンについて話すにはまだ早すぎる。中国は直接的な影響を与えていない。ほとんどの国が全く同じこと (国家安全保障のためのスパイ活動) を行っており、米国は中国による国家安全保障のためのスパイ行為に対しては異議を唱えない。しかし、商業的な目的のためのスパイ行為に対しては異議を唱える。

(3) これらの事件がサイバーセキュリティに与えた影響について

- 今では、人々は問題の範囲についてより良い認識を持つようになり、ネットワーク防御やサイバーセキュリティのニーズを強めている。
- 米国は、仏国とテロリズムや蔓延についての情報交換を行っているが、仏国は SIGINT (SIGnal INTelligence: 通信、電磁波、信号等を媒介とした 諜報活動) や、情報諜報活動において、米国の助けを必要としない。彼らはタフで活動的である。英国も同様である。
- 一つ良いことは、人々が、安全なネットワークなど無いことや、注意することが必要であることに気付いたことである。

(4) 官民連携について

- FBI と米国国土安全保障省は、国民との対話に開放的である。米国には、1998 年から ISAC

[8] Trusted Platform Module

(Information Sharing and Analysis Center) や、InfraGard、NCFTA(National Cyber-Forensics & Training Alliance) といった公的な組織がある。パートナーシップを築くために多くの努力が行われた。企業と政府、学会は情報交換を行っている。

(5) サイバーセキュリティのための政府機関

- 国土安全保障省には戦略、権限、人的資源が必要である。仏国や英国は、良いモデルとなるであろう。
- 仏国は、ANSSI (National Agency for the Security of Information Systems) を内閣府に置き、そこが強い規制力を有している。国家防衛の役割を担っており、そのことが他の政府機関に対する権限につながっている。
- 英国は 2 つの異なった機関を有している。CESG (Communications-Electronics Security Group) と、CPNI (Centre for the Protection of National Infrastructure) である。英国は民間セクターと非常に強いパートナーシップを有している。この 2 つの機関は GCQH (Government Communications Headquarter: 政府通信本部) や警察庁相当の組織に結び付けられ、内閣府官房に直接報告を行う。このように彼らは多くの権威と影響を保有している。
- オーストラリアは、オーストラリアサイバーセキュリティセンターを最近設立した。これは、法務長官によって運営されている。

(6) 米国におけるサイバーセキュリティシミュレーション

- シミュレーションは非常に役に立つ。“サイバーストーム” は、国土安全保障省による最大のものである。財務省は、ウォールストリートの金融機関向けに ”Quantum Dawn 2” を実施した。最初の “サイバーストーム” では、まず、誰も備えができていないことを学んだ。

(7) だれがどんな理由でインフラを攻撃するのか

- 昨年、重要インフラが北朝鮮やイランによって攻撃された。彼らは特別に洗練されているわけでないが、もしも彼らができるのであれば他の国にも可能である。私は、より多くの国がこの能力を有することになってきたと思う。さらに、今後 5 年の間に、非国家的組織がこの能力を有するようになるであろう。
- 中国の軍機は米国に到達できないが、中国のハッカーたちは、米国を含め全世界に到達できる能力を有している。多くの企業は防御を持たず、もしも彼らが攻撃を行えば、それを阻むものは何もない。
- 中国は貿易を確保する必要があるので米国をサイバー攻撃することはないであろう。米国へのサイバー攻撃は、中国やロシアの利益とはならない。

(8) サイバー攻撃の費用積算

- IP (Intellectual Property: 知的財産権) 窃盗、サイバー犯罪、復旧コスト、追加的なセキュリティ費用、停止によって生じる損失利益などすべての種類のコストを挙げた。

- 現実的なサイバーセキュリティの確立のために、自動車事故や、海上の海賊行為、店舗からの窃盗などのデータを参考として研究を進めている。 保険会社からも情報を入手できないかを検討している。

(9) その他

- 米国と中国は、サイバーセキュリティに関し、2 つの議題、責任ある国家の振る舞いの定義と、誤算とエスカレーションの防止について取り組んでいる。

5. DAC (Decisive Analytics Corporation)

(1) DAC 概要および面談相手

DAC は、1996 年に設立された、従業員所有企業（株式を従業員が保有する企業）である。複雑な問題に対して分析的な解決策を提供することを得意としており、米国国防総省や国土安全保障省を始めとする官庁や民間企業を顧客としている。面談相手は以下である。

- Mr. John S. Donnellon, President
- Mr. Mark Hall, Vice President, Cyber Security Engineering
- Mr. Wayne Fujito, President, International Division, DAC, Chairman, NATO Industrial Advisory Group, and Chairman, NDIA International Division
- Ms. Cristiana Brafman Kittner, Defense Analyst/Export Compliance Official

(2) 官民連携について

(a) SINET

- DAC は、カリフォルニアの SINET (Security Innovation Network: (情報) セキュリティ革新ネットワーク）と非常に緊密に活動している。これは官民連携の良いモデルである。SINET は、イノベーションコミュニティを見ている。そこでは、サイバーセキュリティにおける最良、最新の技術が開発され、政府や、際立ったサイバーセキュリティ手法に興味を有する投資団体など、多くのパートナーを呼び集めている。(日本の企業でも参加することができる)

(b) NDIA

- NDIA (National Defense Industry Association: 国家防衛産業連合）は防衛産業の団体で、別の官民連携のモデルである。政府と産業界を一堂に集め、知識や課題や問題、そして解決策を共有する。約 1,700 の欧米企業がその会員となっている。36 の部門がある。サイバー部門は 2 年前に設立され、責任者はノースロップ・グラマン社の退職者である。

(c) 官民連携における課題

- 官民連携における課題として、以下 3 点が挙げられる。

  a 相互信頼

  政府は、企業の情報を機密にし、企業は政府の情報を機密とすべきである。また、企業が所有する情報は、「情報公開法」の対象外とすべきである。

b 資金

民間企業にサイバーセキュリティに対してお金をかけてもらうことや、将来の脆弱性や新たなネットワーク構造等の変化に対応するに投資を継続してもらうことが課題である。目指すべきは、ネットワークセキュリティ体制の継続的な評価や、新たなイニシアティブに対して、毎年適切な投資を行うことである。

c 義務と自発

防御を義務とするのであれば、多くの規制、法制度、負担などの課題について取り組むことが必要になる。自発的なものとするのであれば、何らかのインセンティブを付与させるべきであろう。

(d) 平和時の備え

- 国家は、ワーキンググループや、コミュニケーションチャネルを持ち、そこで、全ての問題や、論点、悩みの種や、何が享受できるリスクかまたはそうでないか、について話し合うべきである。政府は、民間企業が何を考えているかについて理解すべきである。
- サイバー災害から戦時への移行についての権限や手続きをはっきり定める必要があり、平和時に、手続きを制定しその手続きをテストするための演習を行う必要がある。予期できない事象（Unexpected Elements：例えば、サイバー攻撃と関連すると思われていなかった爆発が、東京で発生するなど）に直面するようなシナリオに基づいた演習を行い、政府内の連携を必須とさせる。演習の後で、政策や、手続き、原則、変更などについての評価を行う。例えば、政府関係者を一室に集め、現在の権限で演習を行い、次に新たな権限を与え、彼らが何をすることができるか、また、結果がどのように変わるかなどを確認したりする。
- 米国のサイバー演習は、軍隊のサイバー演習から始まり、それがより大きな軍事演習に統合され、次に、軍隊、諜報コミュニティ、他の一般省庁、法執行機関や警察も参加し、民間セクター、さらには州や地方政府も巻き込んだ演習に展開していった。
- 各国にとって考慮すべき主なポイントは、既存の手続きや、権限や機能が、国家危機的なサイバーインシデントを検知し、軽減し、それから回復できるかについて検討することである。国家は、そのようなインシデントが発生して初めて、これらの手続きを開発し、テストするということになってはいけない。
- 民間セクターは、その関心事や論点、何か行うべきことを政府に伝えるべきで、また、何をすべきか議論すべきである。国民が課題を理解できるように、政策が適切に整えられるべきである。
- 米国は、多くの FFRDC（Federally Funded Research and Development Center：国立研究開発センター）を設立した。MITRE Corp や、Institute for Defense Analyses、Aerospace Corp、MIT's Lincoln Laboratory などである。政府組織にとってこれらは組織の強化となる。日本もこのような民間企業による政府機能の増強が必要である。

(3) 重要インフラの防御について

- 金融セクターや、軍、軍事産業拠点は、明らかに攻撃の対象となりうる。
- 政府は、脅威の情報や解決策をインフラ企業と共有すべきであり。インフラ企業は、インシデントのデータを政府と共有すべきである。両方が必須である。

(4) サイバーセキュリティに関する一般的な情報

(a) 外国製品の使用禁止について

- 認識されている極端に疑わしい供給者を除けば、国家レベルの使用禁止はできない。産業界で行われるべきである。リスクに基づく評価も必要である。
- 各省庁が、把握するための手続きを持つべきであり、少なくとも確認を行うためのチェックリストがあるべきである。また、政府機関の間でも、脅威に関する情報を共有する手続きがあるべきである。情報共有のために政府レベルの CIO（最高情報責任者）協議会を設けることも一つの方法かもしれない。

(b) スノーデン事件について

- スノーデンは、単なるシステム管理者にすぎなかった。NSA に行く前、3 年間別の民間企業を通じて CIA のために働いていた。彼は、恐らく、CIA で働いている間に NSA が何を行っているかを知り、Booz Allen Hamilton 社を通して NSA で働くことを決めたのであろう。
- スノーデン事件は、世論や議会に大きな影響をもたらした。PRISM プログラムを続けることについての議会投票はわずか 10 票差でかろうじて通過した。ただし、プログラムに対して何らかの修正が行われるであろう。
- NSA は彼が PRISM 以外の他の情報を漏らすことを恐れている。それは NSA にとってより大きなダメージとなる。

(5) その他

- 報告先の官庁が多すぎることへの示唆: 陸軍、海軍、空軍がお互いに話し合うことを求める法律や、諜報機関の調整を行う長官に強い権限を与える別の法律により、米国では事態が好転した。
- 国防総省の CIO の調査によれば、IT 予算の内 10～15% が IT セキュリティに使われている。
- 3 年前、国防総省は年間 30～40 億ドルを、連邦全体では年間 70~80 億ドルをサイバーセキュリティに費やした。
- サイバーセキュリティ政策は、国や文化、経済水準によって異なるが、人と政策、技術、そして手続きのすべてを必要とする。
- 一般人や専門家の教育が必要である。人を訓練する事(例えば、資格を取らせること)とネットワークをどう防御すればよいのかを教える事は、2 つの異なる事である。
- 最良の組織は、良い IT 基本設計と同時に、良いサイバーセキュリティ基本設計を保有し

ている。良いセキュリティ基本設計により、コストを理解し、抑えることができる。

6. State Government of Maryland

(1) Maryland Department of Business & Economic Development の概要および面談相手

Maryland Department of Business & Economic Development は、メリーランド州に成長産業を誘致して育成するための政策や規制を設けたり、障壁を減らすことにより、ビジネスに優しい環境を供給している。2010 年 1 月から、サイバーセキュリティ産業を育成するために、”CyberMaryland” と呼ばれる施策を始めている。面談相手は以下である。

- State Government of Maryland:
  - Mr. Patrick Tonui, Program Manager, Security and Information Technology, Office of Strategic Industries & Innovation, Maryland Department of Business & Economic Development
- UMBC:
  - Mr. Greg Simmons, Vice President for Institutional Advancement

(2) ”CyberMaryland” の趣旨について

- 我々は、最初に、政府関係機関と、システム・インテグレーターや、技術開発などの民間セクターの両方と話し合いを行い、サイバーセキュリティとは何か、なぜサイバーセキュリティが大切なのか、彼らにとって何が重要か、どのような課題や障害と直面しているのかなどについて理解に努めた。
- その結果、我々が州政府として最も影響を与えることのできる以下 4 つが、“CyberMaryland” に盛り込まれた。

  a 教育

  我々は、IT 職とサイバーセキュリティ職の間のギャップを見極めた。また、政府(特にいくつかの省庁)は、“Cyber Warriors (サイバー戦士)” を必要とし、民間企業 (特に技術の開発や改良を行っている企業) は、いろいろなツールを理解している人々を必要とした。その結果は、学位を与える教育機関における教育カリキュラムに反映されている。

  b 起業援助

  エンジェルインベストメントや、シードベンチャーキャピタル、専門家や研究者からの援助へのアクセスを提供するプログラムや手段を開発する。

  c 政策

  適切なサイバーセキュリティの衛星と実践のために、全ての人々や企業に適切な教育と、情報を提供するべきである。

  d マーケティング・コミュニケーション

  皆に、メリーランドがサイバーセキュリティ企業を成長させるために良い場所であることを知らしめる。

(3) メリーランドに企業や人を誘致できる要因

- 以下 3 つの要因の組み合わせによる。

  a 顧客

  サイバーセキュリティの最大の顧客がこの地域に存在している。

  b 資金

  サイバーセキュリティを中心とする州によるベンチャーファンド、その他のベンチャーキャピタルや投資家がある。州には専門家がいてどの会社に投資を行うかを決め、時には民間セクターと投資を行うこともある。

  c インキュベーターネットワーク

  UMBC は、2010 年に、サイバーセキュリティのために 20,000 平方フィートのインキュベーター施設を設立した。現在 40 のサイバーセキュリティ企業に対し、低家賃のスペースや、政府調達や、セキュリティクリアランス、様々なセグメントへの売り込みに関する情報を提供している。企業が大学の教授と結びつき、企業が大学のカリキュラムに影響を与え、研究の商業化を助けるといった豊かなエコシステムとなった。

(4) インキュベーターネットワークがうまく行っている要因

- 立地が貢献している。空港から 2 マイルで、NSA から 10 分、バルティモア市内から 10 分、ワシントン D.C. からも 40 分である。
- 大学の評判も良い。UMBC は、様々な組織を援助するために、提携や関係構築を行うことで有名である。
- 州の ”Cyber Maryland” も役立っている。 UMBC はこの報告の方針に沿ってカリキュラムや訓練プログラム作った。

(5) メリーランド州立大学システムにおけるサイバーセキュリティ教育

- メリーランド州立大学システムには、3 校の研究大学（research universities）を含む 12 の大学がある。州内の多くの大学がこの分野に関わっている。サイバーセキュリティは特に新しいものではないが、最近それに対する需要が増加している。競争はあるが、それぞれが自身の得意分野を見つけている。
- UMBC は、伝統的な学士から博士までの学部・大学院のプログラム、働いている人向けのマスターコース、数年前からの営利目的の学位の無い訓練コースを提供している。最後の訓練コースは、急激な変化や、様々な産業界のニーズに応えるものである。
- UMUC (University Maryland University College: メリーランド州立大学ユニバーシティ・カレッジ）は、メリーランド大学システムにおける遠隔学習キャンパス（distance learning campus）であり、オンライン訓練や、拡張学習（extended learning)、中堅社員向けの特別訓練を行っている。コースは全世界に供給されている。
- UMD (＝UMCP: メリーランド大学カレッジパーク校）も技術や政策系の学部・大学院のプログラムを有している。法律課程では、特許侵害の様なサイバーセキュリティ政策を取

り扱っている。

(6) “CyberMaryland” の 3 年間の実績

- マーケットのニーズに合わせて新しいコースを設立し、プログラムの数を増やした。(3 年前にはサイバーセキュリティ独自の学位すらなかった)
- 顧客がいるというばかりではなく、サイバーセキュリティについて深い知識を持つ人たちがいるという理由で、 2010 年から、ロッキード・マーチンや、ノースロップ、ボーイングなどの大企業が、サイバーセキュリティの中核的研究拠点（Center of Excellence）を設立している。そこには最も優れた研究者を配し、人々に訪問してもらい、企業の能力を分かってもらったり、研究や、プロジェクトマネジメントやシンクタンク的な仕事を行っている。

(7) サイバーセキュリティの学位とその他の IT の学位の違い

- 数学やコンピューター、ソフトウェア設計の基礎的なコースは同じである。追加的な必須コースは、民間企業と話し合いを行い、企業がどのような技能を求めているのか、新卒の IT 学士が、ちゃんとやっていけるサイバーセキュリティの専門家になるためにどのような追加訓練を企業では必要としていたのか、などを探し出すことによって開発される。追加的なコースとしては、例えば、マルウェア検出、リバースエンジニアリング、侵入検出技術などに力点を置いたソフトウェアデザイン・企画がある。

III. 米国調査・議論から示唆されること

このセクションでは今回の米国調査・議論から示唆されることを紹介する。

1. 重要インフラのサイバーセキュリティ

一般の ICT のサイバーセキュリティとは異なる面を理解して対策を構築していく。

重要インフラ、特にスマートグリッドのサイバーセキュリティは一般の ICT のサイバーセキュリティとは異なる面があることを理解して対策を構築していく必要がある。重要インフラのサイバーセキュリティの特徴としては以下のようなものがある。

- 重要インフラの企業にとって優先順位は可用性（availability）、完全性（integrity）、機密性（confidentiality）の順である。
  - サービスを提供し続けるのが第一義である。
  - 小さな電力会社の多くでは経済的リスク（financial risks）の方が重要で、サイバーセキュリティに対応するためのお金や専門家もない。サイバーセキュリティはその他のリスクとともに優先順位をつけ相対的にとらえる必要がある。
  - サービスの提供を続けるためにはデータの完全性（integrity）が重要
- 一般の ICT のサイバーセキュリティでは多層防御（Defense in depth）と言われる、情報の重要性に応じた多段の防御が求められるが、電力のサイバーセキュリティでは送配電網、変電所、スマートグリッドの導入で家庭まで含めて、攻撃を受けうる面（attack surface）が広く、広域防御（Defense in breadth）が求められる。
- セキュリティなど考慮されていなかった 30 – 40 年前の機器がまだ存在しており“bump in wire”[9] などの後付けのセキュリティも難しい。
- 研究者に脆弱性を指摘されてもパッチのテストに 2 年もかかる。

その他のコメントとしては、以下のようなものがあった。

- 金融セクター、軍、軍事産業拠点は明らかな標的である。その他のセクターではリスクは理解されているが、投資に対する価値はまだ確信されていない面がある。
- 政府はインフラ企業と、インフラ企業も政府と共にインシデント情報を共有する必要があり、それには相互の信頼が重要である。
- 2 月の大統領令に基づき、重要インフラ・サイバーセキュリティ・フレームワークを NIST（米国標準技術局）が作成しつつある。7 月にドラフトを公開している。
  - http://www.nist.gov/itl/cyberframework.cfm
  - http://www.csoonline.com/article/736561/

[9] IPsec 機能(暗号技術を使って IP パケットの完全性や機密性を実現する仕組み）を持たない端末に対して外部で IPsec 機能を提供することにより利便性、効率性を高める方式

対策として指摘があったのは以下のようなものである。

- さまざまなレベルでの情報共有
  - NERC[10] ES-ISAC[11]
  - DHS[12] は ICS-CERT と US-CERT と情報共有をしようとしている。
  - 各地域の電力会社による情報共有
- NESCOR[13], NRECA[14] などによる情報提供
  - NESCOR は障害シナリオ、リスク分析、訓練、侵入テストなどに関する資料を公開している。
  - NRECA は以下の情報を提供している。

    A Guide to Developing a Cyber Security and Risk Mitigation Plan

    https://groups.cooperative.com/smartgriddemo/public/CyberSecurity/
- 分野横断、各分野での大規模な演習
  - “Cyber Storm” は DHS による一番大きな分野横断的な演習 。
  - “GridEx” は NERC によるカナダ・メキシコを含めた電力会社 130 社による演習。

    http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx
  - “Quantum Dawn” は財務省による演習。前回はウォール街へのサイバー攻撃演習が行われ、50 団体 500 人の参加があった。

    http://www.sifma.org/services/bcp/cybersecurity-exercise--quantum-dawn-2/

2. 人材育成

人材流動性は多面的な見方を持つのに役立っている。 いくつかの参考になる政策があった。

話を伺った多くの人が運用、ベンダー、侵入テスト、CSO、省庁・民間など様々な組織間を異動していた。 いろいろな立場からサイバーセキュリティに関わった経験が役立っているとのことであった。

米国でも「大学では暗号など理論的なコースが多く、実践的なものが少ない。」という指摘もあったが、取組みを進める大学を訪問し話を聞くと、かなり努力しているように見受けられた。

日本でそのまま適用できるかは検討が必要になるが、大学関係における施策で参考になるものとして以下が挙げられる。

[10] North American Electric Reliability Corporation: 北米電力保全機構
[11] Electricity Sector Information Sharing Analysis Center
[12] Department of Homeland Security: 米国国土安全保障省
[13] National Electric Sector Cybersecurity Organization Resource
[14] National Rural Electric Cooperative Association

- 奨学金制度 – NSF[15] による “CyberCorps”[16] と DoD[17] による “Information Assurance Scholarship Program (IASP)”[18]
  夏休みには政府でのインターン、卒業後数年政府に入ることが求められるが、学費、本代のみならず給付金もかなり出るプログラム
- 大学の認定制度 – NSA[19] と DHS による “National Centers of Academic Excellence in Information Assurance Education” (CAE/IAE)
  大学は 2 年に一回コースの詳細な報告を行うことを要するが、大学にとっても Branding や Marketing に大きな意味を持つ。
- 企業・省庁との連携
  - 企業・省庁が求める人材像を聞き、一般 IT 教育を越えて必要になる要素を含めてコースを設計
  - 企業・省庁から学生だけでなく、講師も迎え、実際の事象・実務経験などを反映

また R&D に関しては 2011 年 11 月に出た “Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program”[20] (2011 年 12 月公表) は影響が大きかったとのことであった。

3. 産業育成

個々のスタートアップの先見性、それを追う情熱とともに、政府研究プロジェクト、政府系投資などかなり政府の深い関与もある。大学も自ら打って出ている。

産業育成に関して政府の以下のような関わりが見られた。

- DARPA[21] 研究プロジェクトの RFP[22] がスタートアップのきっかけになった。
- CIA[23] 系の投資会社 In-Q-Tel やメリーランド州自身による投資。
- 先端的な攻撃をすでに受けていた政府は最先端の顧客としてフィードバックを得られた。

上記のことは連邦・州政府にも技術の目利きがいることを示しており、米国の高い人材流動性も関係していると考えられる。

また以下のような民間の活動もスタートアップ企業が顧客やスポンサーを見つけるのに重要な役割を果たしている。

- SINET (Security Innovation Network) – スタートアップ、政府系顧客、投資会社、法律

[15] National Science Foundation: 全米科学財団
[16] https://www.sfs.opm.gov/
[17] Department of Defense: 国防総省
[18] http://dodcio.defense.gov/Home/Initiatives/InformationAssuranceScholarshipProgram(IASP).aspx
[19] National Security Agency: 国家安全保障局
[20] http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf
[21] Defense Advanced Research Projects Agency
[22] Request for Proposal: 入札公募
[23] Central Intelligence Agency: 中央情報局

の専門家を結び付けるネットワーク

大学も産業育成に積極的に関わっている。 UMBC（メリーランド州立大学 ボルチモア郡校）によるリサーチパーク、bwtech@UMBC も非常に興味深い取組みである。 大学が毎年入居企業から小さな株式の持ち分（1 %）をもらう代わりに、スタートアップに安い家賃でのオフィス、指導、講演会などのサポートを提供する。 ただ単にリサーチパークとして場所を提供するだけでなく、より深く関わることにより、大学自身にもスタートアップが成功することが重要となる。

また大学の学生は実践の場としてのインターンの機会を得、学生が大学、企業などの懸け橋になる。

4. 組織

フランスの ANSSI や英国の CESG/CPNI が参考になる。

サイバーセキュリティを担当する組織としては、DHS は参考にすべきではないということを複数回聞いた。「明確な権限がない。」、「いろいろな組織の寄せ集めでそれぞれが勝手に動いている。」などがその理由であった。

ではうまく行っている国はという質問に対して挙げられたのは、フランス(ANSSI[24]) と英国（CESG[25]/CPNI[26]）であった。 フランスの ANSSI は Prime Minister's Office にあり、企業に対する法制を定めるなど強い権限があり、英国も適切な権限が与えられ、企業の CEO らと打合せを長く持っており、互いに高い信頼関係を築いているとのことであった。政府が企業からの情報をしっかり守り、企業が政府からの情報をしっかり守るという相互の信頼も重要であるという指摘もされた。

その他関連の政策を以下に挙げる。

- FBI[27] は FBI の支局がある都市で InfraGard という草の根的な活動を行っている。その地域の関係者 20－30 人を巻き込み、NDA[28] の元、情報共有や解析などを行っている。FBI はそのほか Pittsburgh に National Cyber-Forensics & Training Alliance (NCFTA) を持ち、産官学共同でサイバー攻撃の解析などを行う。 NCFTA については警察庁が同等のものを日本にも導入しようとしている。
- 地方自治体などで電子政府の導入の障害になっている理由の一番は財政問題であるが、サイバーセキュリティも必ずトップ 5 の中に入っている。テンプレートとなるシステムを各自治体に配るというアプローチは以前失敗したことがある。

[24] National Agency for the Security of Information Systems
[25] Communications-Electronics Security Group
[26] Centre for the Protection of National Infrastructure
[27] Federal Bureau of Investigation: 連邦捜査局
[28] Non-Disclosure Agreement: 機密保持契約

- 情報共有などのアプローチとしては、システムをスタンダード化するのではなく、情報のやり取りの仕方を標準化するものがあり、うまく行っているようである。
  - DHS の NIEM[29] はいろいろなレベルの政府や企業が災害などの危機情報を共有するための XML 情報共有の枠組み
  - NSA から 2 年前に出てきた STIX はサイバー攻撃の情報を共有するための XML による標準言語
- 米国は多くの FFRDC[30] を設立した。 MITRE Corp, Institute for Defense Analyses, Aerospace Corp, MIT's Lincoln Laboratory などで、省庁にとってこれらは組織の強化となる。日本もこのような民間による政府府機能の増強が必要との指摘があった。
  - 民間の活動を邪魔しないように制限もある。
  - NIST がサイバーセキュリティの分野で一つ作ろうとしており、メリーランド大学が誘致しようとしている。

5. その他

その他のトピックに関しては、以下に挙げることが聴取できた。

- マンディアント（Mandiant）社レポート – 世論形成には大きな影響があった。ただし米政府の中国に関する認識を変えたのはその数週間前に出された、米国政府内の非公開の秘密レポートである。 これはかなり詳細で、それまで中国からいろいろ攻撃を受けているとは思っていたがここまでとは知られていなかったようである。
- スノーデン（Snowden）による NSA 情報漏えい事件 – 欧州各国も（自国民も含めた）かなりの諜報活動をやっており、いずれ収まるであろう。
- 中国・ロシアは米国と経済的に深く関わっており、サイバー諜報活動は別として、サイバー攻撃を仕掛けてくる可能性は低いであろう。
- サイバーセキュリティ人材不足は以前のドット・コム バブルのようだという指摘もあった。 DC のラジオ局では大学の宣伝でメリーランド州だけで 2 万人が不足していると伝えていた。
- サイバー攻撃のコスト評価を行っている。数十億ドルから数千億ドルまでいろいろな数字が出ているが、現段階の試算では米国 GDP の 1％ 程度とのことである。
- 国防省が行った CIO のサイバーセキュリティに関する調査では IT 予算の大体 10 – 15% がセキュリティに使われているとのことであった。
- サイバー攻撃や、戦時への移行についての権限や手続きをはっきり定める必要があり、平和時に手続きを制定しその手続きをテストするための演習を行う必要がある。政府機関が予期できない事象（例えば、サイバー攻撃と関連付けることが知られていなかった爆発が、東京で発生するなど）に直面するようなシナリオに基づいた演習を行えば、政府内の連携が必ず必要になる。演習の後で、政策や、手続き、原則、変更などについての評価を行う。

[29] National Information Exchange Model
[30] Federally Funded Research and Development Center: 国立研究開発センター

例えば、政府の人々を一室に集め、現在責任を負っている権限を持った人々と演習を行うこともできる。これにより、新たな権限を与え、彼らが何をすることができるか、あるいは結果がどのように変わるかなどを確認することができる。

- 米国では軍から始まったサイバー演習が次第に、諜報機関、その他省庁、警察、民間、地方政府などを含んだ大きな演習になっていった。
- オーストラリアではサイバーセキュリティに関して “35 mitigation strategies”[31] があり、豪政府機関は守ることが必須とされている。 標的型攻撃の 85% はその上位 4 つの対策で防げるとのことである。

以上

[31] (http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

IV. 資料編　〈詳細面談記録〉

1. EPRI (Electric Power Research Institute)

面談先	EPRI (Electric Power Research Institute)
面談日時	2013.7.22　　10:00～12:00
面談者	先方：Ms. Annabelle Lee, Senior Technical Executive (Joined through teleconference system) Mr. Jimmy Herren, Account Executives, Technical Advisory Services, Power Delivery & Utilization 当方：益岡、石野
面談テーマ	スマートグリッドにおけるサイバーセキュリティの状況についての意見交換

(1) EPRI 概要

公共の発電、送電、電力利用に関する研究、開発、実演を行う非営利団体。米国エネルギー省より電力関係のサイバーセキュリティに関する研究を委託され、NESCOR (National Electric Sector Cybersecurity Organization Resource) を組織し対応している。

(2) 一般的なことがら

- NESCOR はエネルギー省が資金を提供する官民提携のプロジェクト (public-private partnership) である。 EPRI も一部費用を負担している。
- 制御システムに関するサイバーセキュリティは、通常の IT のサイバーセキュリティとは大きく異なる性格を持つ。機能を持続させることが第一である。サイバーセキュリティは、特に地方公営電力会社 (munis) や電力協同組合 (coops) などの小さな電力会社にとって、財政的なリスクを含む他のリスクと相対的なものである。古いシステムにパッチがあっても、あてるのは不可能でなくとも容易にはではない。
- NERC (North American Electric Reliability Corporation: 北米電力保全機構) によるサイバー演習 GridEx II
- (http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx) が 2013 年 11 月に行われる。 これはカナダ、メキシコも含み 130 の組織が参加する大きな国際的な演習である。 (準備のための電話会議では 240 人が参加したこともある。)
- NRECA (National Rural Electric Cooperative Association - 電力協同組合 (Coops)の協会) による、いいサイバーセキュリティ対策についての文書が以下にある。
  - A Guide to Developing a Cyber Security and Risk Mitigation Plan
  - https://groups.cooperative.com/smartgriddemo/public/CyberSecurity/

(3) NESCOR のミッション (http://www.smartgrid.epri.com/nescor.aspx にある 5 つ

の箇条書き点)

- どれが特別に重要ということはない。 それぞれのミッションが別々の目的を持つ。セキュリティの問題は設計段階などなるべく早い段階で考えるのが良い。電力会社は NESCOR が提供する障害のシナリオ（failure scenarios） をリスク分析や手続きの仕様決めに用いられている。
- 電力分野の課題の一つは、30～40 年も前のセキュリティについて考慮がされていなかった時代に作られた、セキュアでない機器が現存しており、必ずしもセキュリティを後付けできるものではないことが挙げられる。例えば、”Bump in the Wire” 手法[32] によって野外にあるデバイス、発電所や変電所の機器の機能を改良しようとしても、その反応時間の遅れ（例えば 4 msec 以内の反応時間を求められる）などにより効果的な対応ができない。短期的には、周辺部における障壁（Firewalls） や、侵入検知システム（IDS: Intrusion Detection System）、侵入防止システム（IPS: Intrusion Prevention System） などによる防御が考えられる。長期的にはよりスマートな機器との入れ替えが考えられる。
- 電力会社（特に規模の小さな電力会社）は財政リスクを含む種々のサイバーセキュリティのリスクを受け入れる場合もある。 一般に組織はリスクに優先順位を付け、何が彼らにとって重要であるかを決めることによりリスクとコストを見合わせるべきであろう。全てのリスクに対して費用をかけられるわけではない。
- 全ての事故が悪意のある攻撃によって発生するわけではない。大部分はミスによって引き起こされる。 NESCOR (National Electric Sector Cybersecurity Organization Resource) がサイバーセキュリティの事故 (cyber security events) を障害シナリオ (failure scenarios) と呼ぶのはそれが悪意のあるサイバー攻撃と悪意のないミスの両方を含むからである。

(4) スマートグリッド・スマートコミュニティでのサイバーセキュリティの課題

- 双方向の情報伝達や、専用のシステムや専用のプロトコル 33 の代わりに（経済的な理由により）汎用のものが用いられることにより、多くの脆弱性がもたらされる。異なる多くの機器が同じ OS (例えば Windows) を使うのであれば、同じ脆弱性がそれらの機器で生じる可能性がある。
- サイバーセキュリティは電力会社が直面する（財政リスクを含む）多くのリスクの一つである。 組織は対応するリスクに優先順位をつける必要がある。
- 昔と違って機器に対してファームウェア 34 や通常のソフトのパッチが適用されなければならない。
- (スマートメーターからの 15 分おきの使用量データや電気自動車の監視データなど) スマートグリッドにおける個人のプライバシーの取扱いが世間の注目を集めている。 プラ

[32] システムの外側にネットワーク・セキュリティを実現する手法。 例えば IPsec 機能（暗号技術を使って IP パケットの完全性や機密性を実現する仕組み）を持たない端末に対して端末の外部で IPsec 機能を提供するもの。
[33] コンピューター間の通信接続手続き
[34] ハードウェアの基本的な制御を行うために機器に組み込まれたソフトウェア

イバシーを擁護する人たちは、スマートグリッドの新しく、また他とは異なる課題に集中する必要がある。

- NERC（North American Electric Reliability Corporation：北米電力保全機構）の重要インフラ保護の標準に定められている組織には、重大な攻撃について報告を行うことが義務付けられている。ただし、その情報は通常外部には伝えられない。DHS（U.S. Department of Homeland Security：米国国土安全保障省）、DOE（Department of Energy：米国エネルギー省）や NERC は皆、より深い情報共有を行いたいと思っている。しかし、“Freedom of Information Act”（情報公開法）が大きな争点になっており、民間部門が米国連邦政府と情報を共有することの大きな障害となっている。DHS は機密情報を保護する規制を設けたが、それについての司法による判断はまだ行われていない。
- 米国本土の 48 州には 46 の異なったプライバシー法が存在している。例えば、個人のエネルギー使用データを電力会社の所属とするのか利用者の所属とするのかについてさえも対応が異なっている。
- 電力会社の規模によりリスクが異なっている。大企業は、国家からの攻撃の様な大規模攻撃に関心があるが、中小企業はそれほどない。 どのサイズの組織も、大衆の反応や経済的な安定性には関心がある。

(5) スマートグリッドのサイバーセキュリティ対策

- データの機密性を第一とする通常の IT のサイバーセキュリティとは異なり、制御システムにおける優先事項は、安定供給、データの完全性、データの機密性の順である。
- IT システムの防御は多層防御（defense in depth）と言われる、制御システムの防御には広範さ（defense in breadth）が求められる。攻撃を受ける範囲はより広い。（例えば、変電所に対する攻撃は、安定供給に影響を及ぼす重大な影響をもたらしうる。）
- 侵入されたと分かっていても止めることできない機器にどう回復力（resilience）を担保するかが課題である。
- 情報共有は大きくかつ重要な課題である。以下にいくつかの情報共有活動を挙げる。
  - NERC ES-ISAC (Electricity Sector Information Sharing Analysis Center)
  - DHS は ICS-CERT や US-CERT と情報共有を行おうとしている
  - 各地域の電力会社間でも情報共有を行おうとしている
- 制御システムの課題の一つはパッチを行うのに長時間が必要であることである。（パッチをテストするのに最長 2 年かかる）

(6) スマートグリッドのサイバーセキュリティの人材育成

- NESCOR は直接人材育成に関わっていないが、障害シナリオ（電力会社は NERC が求める机上演習にこれを用いることも可能である）、リスク分析、訓練、侵入テストなどに関する資料やツールを公開しており、誰でもこれを利用することができる。

以上

2. FireEye

面談先	FireEye
面談日時	2013.7.22　　14:00～16:00
面談者	先方： Mr. Ashar Aziz, Founder, Vice Chairman, & CTO Mr. Doug Schultz, Vice President, APAC/Japan Mr. Bill Hau, Vice President, FireEye Labs Mr. Travis Rosiek, Federal Architect Mr. Yoshi Ozawa, Senior Systems Engineer Mr. Naoyuki Ono, Senior Enterprise Territory Account Manager 当方：益岡、石野
面談テーマ	・サイバーセキュリティにおける官民連携の在り方について ・サイバーセキィリティ人材育成の在り方について

(1) FireEye 概要

- 2004 年にサイバーセキュリティ、特に標的型攻撃対策製品の開発・販売を目的として設立された。現在、40 カ国に 1000 以上の顧客を有している。

(2) FireEye の展望と製品について

- 当時（2004 年）脅威や攻撃者の様相が深刻化することが明らかであったことと以下を予見したため、 FireEye を設立した。
  - 脅威や攻撃者の変化が進み、明確になっていけば、既存の方法では全く対処できなくなる。
  - 攻撃者はまずその目的において変化していく。 2004 年当時のいたずらのような特に深刻でない目的から、窃盗犯やスパイによる情報の搾取による金銭や情報の獲得という、（現在では最も顕著になっている）2 つの目的となる。
  - 窃盗犯やスパイが既存のセキュリティシステムで捕まらないように、脅威は密かで、偽装され、システム内に入りこみ見えにくくなる。
- 防御構造（defensive architecture）の再考が 2004 年当時の当社の目的であった。
  - アンチウィルスエンジンや、ブラックリストモデルのような支配的なセキュリティ構造は、未知の脆弱性を使ったネットワークに現れるたびにその姿を変える新しいコードを使った攻撃に対しては無力である。
  - ファイヤーウォールベンダー、IPS/IDS（Intrusion Protection System/Intrusion Detection System）ベンダーなどと、他社は自身を製品によって規定している。
  - 当社の防御構造は、事前に考えられた製品デザインは無く、攻撃者によって規定される。我々は攻撃者の気持ちになり、攻撃側にたった思考実験を行う。
  - 当社は既存の製品を持たなかったため、攻撃者のことを全く知らなくても、高度な攻

撃をリアルタイムで探し出す方法を、全く白紙の状態から考えることができた。

- 当社はシステムや仮想マシンのバックグランドを有しており、これをセキュリティ分析に応用することを考えた。
- 仮想デスクトップやデータセンター統合を目的とする XenSource[35] や VMware の仮想マシンとは全く異なるデザイン目的を有していたので、当社は、緩和と感知機能を備えた、脅威認知ハイパーバイザー[36] をゼロから作り上げた。そのため当社のハイパーバイザーは一般にマルウェアによって感知されない。
- ファイルのみを確認するアンチウィルス・ソフトウェアなど今日のほとんどのシグネチャーベースのセキュリティ製品とは異なり、ゼロデイ攻撃分析構造のプリズムを通して、攻撃のライフサイクルのすべての段階に於いて、攻撃の構造が分析されるべきである。
- 我々は、企業のエンタープライズ・アーキテクチャーに亘って柔軟性と統合性のあるソリューションを供給するために、すべての異なる攻撃ベクター（Web, E-mail, ファイル、モバイルなど）に対応できる検知エンジンを開発しなければならなかった。
- 仮想マシンからの情報を企業内と海外とでリアルタイムに共有する我々の仕組みは、とても強力なモデルである。
- 我々は、既存の企業は既存の製品を共食いすることとなるためにこの分野に出て来ることができないことが解っていた。それらの大企業は、彼らの株主を喜ばせるという考え方に捕らわれがちである。
- 我々がこれらのことをきっちりできるようになるまでに 6～7 年という歳月がかかった。

(3) FireEye の現在の活動について

- 我々が成功してきた理由は、我々が脅威の変遷と防御構造の正しい姿を正確に予想し、とても独自で質の高い方法で、すべての要素を組立てることができたためである。
- 他社にも高いレベルの概念を理解することはできるかもしれないが、それを実践することは難しい。それには、仮想マシン、パイパーバイザー、ネットワークレベルの処理、アップリケーション、オペレーティングシステムなどに至る、様々な異なるスキルが必要とされる。米国政府がかなりのお金を使って FireEye に似たものを試したが、ほとんど成果がなかった。
- 我々のアプローチが正しいことは、実際の検知によって証明される。毎日、顧客のネットワークにおいて、ほかの会社によって見逃された何千もの攻撃が発見される。
- 創設期から現在そして将来に亘り、FireEye の一番の仕事は、いくつもの攻撃方法（web, e-mail, ファイル、モバイルなど）を持つ脅威がどれだけ進化しようとも顧客を守ることであり、株主を喜ばせることではない。

---

[35] オープンソースの仮想化ソフトウェア
[36] 1 台のコンピューター上で複数の OS を動かすための仮想化ソフトウェア

- **質問:** たぶん FireEye の成功のためだと思うが、最近のマルウェアは行動ベースの検知を避けるために、動き出す前に少し待ったり、(例えば) 3 回マウスクリックがあるまで待つようになっているが、それらに対応できるのか?
- **回答:** 防御構造を構築するためには、攻撃者が適用するのに応じて、自分自身が適応する能力を持つ必要がある。(1) ハイパーバイザーで攻撃者のさらに下を行く。 防御者が攻撃者と同じレベルにいるのでは攻撃者が勝ってしまう。(2) 我々は内部でシミュレーションゲームを行うことにより、2004 年に時間差攻撃や仮想マシン検知の可能性を予測しており、すでにそれらや他の可能性に対する対策がある。(3) 完全な防御システムは存在しない。 攻撃者が変わっていく速度と同じ速さで変わるプラットフォームが必要である。 仮想マシンのインフラや発見的アルゴリズムを含むコアの検知エンジンと他の仮想マシンからの脅威情報は数週間でクラウドから更新することができる。 これは自前のハイパーバイザーを持たない競合他社にはできないことである。
- FireEye は本当に顧客を守るための防御構造の構築を望んでいる。
- FireEye の今日の戦略はクラウドの中で無く顧客企業の建物内に設置されたアプライアンス（特定用途のコンピュータ）内で分析を行うことである。いくつかの顧客は企業内部の通信をその国あるいはその企業に留めたいと希望する。またいくつの国ではそれを要件とする法律もある。将来的にはクラウドを使ったものへの移行を検討する可能性はある。
- 我々はウェブからの攻撃だけでなく、E-mail 内のリンクや E-mail の添付ファイルも見ており、昨今はモバイルアプリも見るようになった。
- モバイルアプリは次の領域である。サムソンはアンドロイドを使っているが、その中に多数の検知されないマルウェアがあることを認識している。 FireEye は社内での名前でモービライザーと呼んでいたもの “Mobile Threat Prevention” として最近発表した。それはアプリケーションを（モバイル機器に対して「MBX ボックス」と呼んでいる）動的エンジンに入れ、その行動を確認しスコアリングするものである。顧客は、スコアに基づきそれをインストールするか否かを判断する。これは FireEye が初めてクラウド内で分析を行うものである。モバイルアプリはもとよりクラウドにあるためである。

(4) 官民連携について

- FireEye は各国政府と連携し、また各国政府に、重要インフラや国家安全保障に対する存在する重大なリスクや高度な脅威や、今まさに起きている攻撃の現実や急速に進化する実態に応じたソリューションや防御構造の必要性について教育している。
- 毎年 300 億ドルが役に立たないモデル（ブラックリストやシグネチャーベースのアンチウィルスモデル）に費やされている。マルウェアは（最近の韓国における攻撃のように）最初にアンチウィルス・ソフトウェアを止める。我々は攻撃が成功する前に攻撃を止めることのできる防御構造を必要とする。
- NIST (National Institute of Standards and Technology: 米国標準技術局）は最近、組織のサイバーセキュリティのリスク管理戦略の一部として仮想マシンベースの技術を使う

新しいセキュリティコントロールを追加した。 このセキュリティコントロールは、NIST Special Publication 800-53 Rev. 4 に成文化され、”Detonation Chamber”（起爆室）として知られる。 アジア地域の他の政府も相当する文書に“知られていない脅威の検知”（“detecting unknown”）を含むような改訂を行うことを検討している。

- FireEye はトレーニングや啓蒙活動に関し、サンズ社（SANS Institute）と密接に協働している。 最近、”SANS What Works”というウェブ放送では、FireEye National Lab の顧客が取り上げられ、顧客は彼らの FireEye 製品での経験や彼らがどのように彼らのサイバーセキュリティシステムに取り入れたかを発表した。
- FireEye は連邦政府の IT セキュリティに関する調達戦略の情報を提供し続ける。 サイバーセキュリティに必要とするものは、戦車、航空空母、戦闘機に必要とするものよりもずっと速く変化する。
- 日本や米国、独国のように、先進技術産業を有する国は、常に産業スパイの攻撃を受けている。それは、国の経済や生産インフラの競争力を衰退させるものであり、国家レベルの脅威となる。
- FireEye は多くの米国連邦の機関や、その他海外の政府にも同様に展開している。FireEye は一般に公共セクターで非常に成功しており、国際的には欧州や中東で成功しており、APAC（アジア太平洋地域）で着実に地歩を固めている。これは政府がリスクを理解し始め、今ある既存のソリューションでは守れないこと、政府は国家的あるいは非国家的な攻撃者にとって高い価値のある攻撃対象であることから援助が必要であることを認識し始めたからである。
- FireEye は脅威の展望や発見したことについての情報共有ができように政府系 CERTS を含む、多くの異なる CERTs と緊密に協働している。
- 2004 年の国防総省による調達入札のこの分野の能力に関する情報依頼書で、FireEye の創始者が問題に興味を持ち、彼が解ける問題を見つけた。 サイバーセキュリティに米国政府が興味を持っていることは、彼にとって重要であった。
- 国防総省の元最高セキュリティ責任者（CSO）の Robert Lentz 氏は現在 FireEye の経営陣にいる。彼は米国、日本、韓国、台湾、シンガポール政府から高く尊敬されており、よく知られている。
- 政府はサイバー攻撃の最前線にいるため、 FireEye は世界中の政府から学んだ。より広いマーケットがまだ認識していなかった、2000 年代の最初の 10 年間の初めごろから、米国政府はメディアでも何度も報じられた多くのサイバースパイ攻撃を受けていた。
- 政府は洗練されたエンドユーザであり、顧客である。
- 国が出来るもっとも大きな投資は、サイバー防御であり、サイバー攻撃ではない。 それは、サイバー攻撃において攻撃元の特定が困難なため、抑止的な解決は最も効果的な方策にはならないためである。
- 我々は、特にアジア地域で、政府出身者をリクルートしている。 地域の適切な専門性を

持った人を雇うことが肝要である。

(5) 人材教育開発について

- 教育は我々にとって重要なキーである。 FireEye は自身の従業員、顧客、パートナーの訓練や、全世界的に、特に政府や銀行のような洗練された顧客に対しての訓練コース提供に投資している。
- 我々はブラックハットのようなハッカーは雇用しない。雇用においては十分な経歴調査を行う。我々は、しかし、模擬戦闘や侵入テストを行うための科学者は雇用している。
- 暗号学のような伝統的なセキュリティのカリキュラムは今日のセキュリティには適合していない。 現実の世界のシステムの不具合は必ずしも数学的な処理にそぐわない。
  - カリフォルニア大学バークレー校 Dawn Song 教授はマルウェアのコードに集中する数少ない大学人の一人であり、彼女と彼女のチームは彼女の 2 年間の sabbatical leave (研究休暇) の間 FireEye で働いている。
- FireEye は世界中で、深いレベルの専門性を持ち、サイバーに関して政府の課題を理解する、多くの政府出身者を雇っている。
- 唯一のキャリアパスはない。他のセクターから来た人々は、 FireEye が、利用者の経験やインシデントへの対応など、利用者の見地を持つことを助けてくれる。他社や政府で高いポジションを務めた人々は、C-Level の役員に技術を分かるように翻訳する、重要な顧客に対する信頼のおけるアドバイザーになりえる。
- 2002 年にサイバーセキュリティにおける膨大な人材不足に対応するための、学部生や大学生向けの 2 つの政府の奨学金が開始された。
  - 国防総省による、”Information Assurance Scholarship Program”
  - 国家安全保障局による ”CyberCorps”

  奨学金は、授業料、宿舎料、教科書代のすべてあるいは一部に、上限を 2 年までとし、適用される。さらに、学生は給付金をもらう。学生は奨学金を受けた期間と同等の期間に亘り政府の仕事につかなければならない。 (別の言葉で言えば、卒業後連邦政府での職が保障される。) また、奨学金を受けている間は夏季の政府機関でのインターシップが義務付けられている。
- 国家安全保障省には、”National Center of Academic Excellence in Information Assurance Education”というプログラムがある。指定された大学 (の学生) は、前述の奨学金を受け取ることが可能であり、これが大学 (コミュニティカレッジでさえ) にサイバーセキュリティ教育を広げ、国の重要インフラを守る一助になるインセンティブを与えている。

(6) Bill Hau 氏による講演

- Mr. Bill Hau は FireEye Lab の VP (Vice President) であり、2013/1 までは McAfee の Foundstone にいた。

- 別個の研究で平均的に
  - 侵入に気付くのに 80 日かかる。
  - 気付いてから解決するまでに 123 日かかる。
  - 侵入への対策コストは 8 万 4 千ドルかかる。
- FireEye は侵入を数分で見つけ出し、解決までの時間を平均 2 週間にまで落とすことができる。
- FireEye Lab はインシデント対応から実際のインテリジェントサービスまでに亘る包括的なサービスを提供する。
- FireEye は基本的なマルウェアのリバースエンジニアリングや犯罪捜査などのコース、およびサイバーセキュリティエンジニアに特化した政府への高度なコースも提供している。

以上

3. UMBC（University of Maryland, Baltimore County）

面談先	UMBC（University of Maryland, Baltimore County）
面談日時	2013.7.24　9:30~11:30
面談者	先方： Dr. John T. Pinkston, Professor, CSEE（Department of Computer Science and Electrical Engineering） Dr. Timothy W. Finin, Professor, CSEE Dr. Anupam Joshi, Director, CSEE (from India through a video conference system) Dr. Richard F. Forno, Graduate Program Director, Cybersecurity, CSEE Dr. Don Engel, Assistant Vice President for Research, CSEE Dr. Donald F. Norris, Professor and Chair, Department of Public Policy Director, Maryland Institute for Policy Analysis and Research 当方：益岡、石野
面談テーマ	サイバーセキュリティ人材育成の在り方について

(1) UMBC 概要

- メリーランド州立大学システムの一環として 1966 年に設立された。一般教養教育、および自然科学や工学の教育を行っている。

(2) UMBC におけるサイバーセキュリティ教育について

(a) National Centers of Academic Excellence in Information Assurance Education (CAE/IAE)[37]

- CAE/IAE は、NSA（国家安全保障局）と DHS（米国国土安全保障省）によるプログラムで、50 校程度の大学が認証されている。[38]
- UMBC は CAE/IAE とともに National Centers of Academic Excellence in Information Assurance Research （CAE/R）の認証も受けている。
- CAE/IAE では、大学に 2 年毎にコースの説明書を提出することが求められている。（多くのチェック項目に適合することが求められている）これは大学が教育プログラムを継続するインセンティブになっている。
- CAE/IAE 認証は大学にとってのブランドやマーケティングの見地からも重要である。
- オクラハマ州のタルサ大学も CAE/IAE 認証を受けており、良いサイバーセキュリティプログラムを有するものとして有名である。

[37] http://www.nsa.gov/ia/academic_outreach/nat_cae/
[38] http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml

(b) UMBC Center for Cybersecurity[39]

- 昨年、UMBC のいろいろなサイバーセキュリティ活動の外部に対するまとまった一つの顔として設立された傘型の組織である。Anupam Joshi 博士をディレクターとし、その組織の下、UMBC は 3 つのプログラムを通じていくつものレベルの授業を提供している。
  - CSEE における研究指向の大学・大学院向けサイバーセキュリティコース
  - サイバーセキュリティ大学院プログラム
  - UMBC Training Centers Cybersecurity Academy
- このセンターの目的の一つは国家サイバーセキュリティ研究所のような大きな国家的プロジェクトに対する、統一された窓口になることがある。

(c) CSEE における研究指向の大学・大学院向けサイバーセキュリティコース 40

- CSEE では研究指向の大学と大学院（マスターコースや博士コース）の講座がある。
- eBiquity グループ[41] では、ソーシャルメディア、モバイル、セキュリティ、セマンティックウェッブなどの分野において機械学習やアルゴリズムの研究が行われている。
- Alan Sherman 博士の指導による “Center for Information Security and Assurance”[42]がある。 ここのユニークなプロジェクトには安全で検証可能な投票システムがある。
- CyberCorps という NSF (National Science Foundation: 全米科学財団) と OPM (Office of Personal Management: 人事局)[43] の “Scholarship for Service” と呼ばれる、国防総省による IASP (Information Assurance Scholarship Program) の 2 種類の非常に寛大な奨学金プログラムがある。

(d) サイバーセキュリティ大学院プログラム[44]

- 大学院長の発案で 3 年前に開設された。このプログラムを企画するために、ノースロップ・グラマン社やその他の地元軍需企業と議論を行った。
  - 以下の 2 つのプログラムを提供し、大多数は最初の修士プログラムに登録する。
    - 専門職系大学院修士（Master of Professional Studies）プログラム（履修 10 コース）
    - 資格（Certificate）プログラム（履修 4 コース）
- 今秋からの学期に 170 名が登録した。
- 研究者ではなく、技術リーダーや実務上の対応を必要とするマネージャーなどの、サイバーセキュリティの実践者を生み出すことを目的としている。
- 現実の勤務環境でサイバーセキュリティ知識を応用できるように、技術的な側面を超えて、経済学、政策、法律の授業を含んでいる。
- 学生の 80% は社会人（定時制）であり、そのうちの半数は政府の職員か、政府の軍事部

[39] http://cybersecurity.umbc.edu/
[40] http://cybersecurity.umbc.edu/training/
[41] http://ebiquity.umbc.edu/
[42] http://cisa.umbc.edu/
[43] https://www.sfs.opm.gov/
[44] http://www.umbc.edu/cyber/

門の契約社員である。

- サイバーコマンドや NSA (国家安全保障局) に行く軍のサイバーリーダーを訓練する教育機関の認定リストに入っている。
- 多くの授業はサイバーセキュリティ業務に従事している非常勤教師によって教えられ、授業の質の向上に役立っている。
- CEH (Certified Ethical Hacker)[45] の資格取得を中心に据えた 40 人の生徒に対する試験的なプログラムを行い、36 名が修士の学位と CEH の認定を得た。

(e) UMBC Training Centers Cybersecurity Academy[46]

- 元軍曹の Homer 氏がこのプラグラムを当初は陸軍や海軍向けとして企画した。1 週間から、(サイバーセキュリティのバックグランドを有しない者に対するブートキャンプなど) 4 ヶ月間まで異なった期間の様々なコースを供与している。

(f) The Maryland Cyber Challenge

- 3 年前に USBC によって始められたサイバー戦争ゲームである。
- 高校生、大学生、サイバー産業の専門家などが参加する。
- 参加者は、一連のコンペでコンピューターやネットワークをいかに防御するかについて取り組む。

(g) UMBC のサイバーディフェンスチーム

- CSEE の Charles Nicholas 教授がチームのアドバイザーである。大部分が学部生である生徒のグループが、サイバーの攻撃と防御（ハッカーに用いられている技術やサイバーアタックに対する防御）の両方を勉強している。
- 上記の Maryland Cyber Challenge や、その他のイベントの準備を手伝っている。

(h) 奨学金

- 今年の 9 月よりノースロップ・グラマン社とサイバーセキュリティの奨学金を始める。百万ドルが UMBC (15 ～ 20 の学生を予定) と UMCP (University of Maryland, College Park) に与えられる。
- Scholarship for Service
  - 上記に挙げた NSF/OPM による CyberCorps である
  - 学士、修士、博士に対する多額の奨学金である
- 卒業後、連邦政府での職を保証される。 しかし民間で働けば 50% 多い給与を得ることができるため、逆に制約になっているかもしれない。

(3) 官学・産学連携について

(a) BHEF (Business Higher Education Forum)

- ノースロップ・グラマン社などの軍需産業や金融機関、IT 会社などの CEO や、大学の学

[45] http://www.eccouncil.org/Certification/certified-ethical-hacker
[46] http://umbctraining.com/cybersecurity

長などがメンバーとなっている、米国での教育や労働力の課題に対するソリューションを推し進める団体である。

- メリーランド州が最初の “Undergraduate Cybersecurity Network” の地域デモンストレーションネットワークとして選ばれた。
- 前述のノースロップ・グラマン社の奨学金も、本事業の一部として位置づけられている。

(b) サイバーセキュリティの中心地としてのメリーランド地域とワシントンD.C.地域

- メリーランド地域とワシントン D.C.地域には、以下のようなサイバーセキュリティ関連機関などが集積している。
  1. 連邦政府機関: NSA（国家安全保障局）、NIST（米国標準技術局）、IARPA（情報先端研究プロジェクト活動）、DISA（国防情報システム局）、ARO（陸軍調査局）、 DARPA（国防総省国防高等研究事業局）、DHS（国土安全保障省） など
  2. 大学: UMBC（メリーランド大学ボルティモア郡校）、UMCP（メリーランド大学カレッジパーク校）、 JHU（ジョンズ・ホプキンス大学）、GMU（ジョージ・メイソン大学） など
  3. テクノロジー企業: NGC（ノースロップ・グラマン）、 LM（ロッキードマーチン）、SAIC、 Booz Allen Hamilton など
- 多くのサイバーセキュリティ技能を有した人がいる。広域 D.C.地域では、1 万 5 千もの雇用が生まれていると言われている。

(c) UMBC

- UMBC は IT 学位の主要な授与大学であり、NSA（国家安全保障局）にコンピューター関連の卒業生を一番多く（今までに 1,000 人程度）送っている大学である。

(d) UMBC リサーチパーク (bwtech@UMBC[47])

- UMBC のキャンパスの横に UMBC が所有する UMBC リサーチパークがある。
- 環境がよく、賃料は安く、サイバーセキュリティ関係の政府機関にも距離的に近い。
- UMBC との協調の可能性も、入居企業選択の一つの基準となっている。
- UMBC は、ガイダンスや、低賃料、話し合い、イベントなどのベネフィットの提供に対して、企業から少しの株式をもらう。（5 年間に亘り、毎年 1% ずつ）これにより UMBC は企業の成功に利害関係を有することになる。
- UMBC の学生にインターシップの機会を与える。学生は、大学と政府、企業間のつなぎ役になりうる。
- サイバーのインキュベーターは、生命科学やクリーンエネルギーの 2 つのインキュベーターよりも規模が大きい。
- 20 以上のサイバーセキュリティ関連企業や NSA を含む政府機関が場所を借りている。
- ノースロップ・グラマン社の資金によるサイバーセキュリティ専門のインキュベーター

[47] http://www.bwtechumbc.com/

“CYNC プログラム”[48] がある

- このプログラムは始めてから 2 年であるが、際立った技術を有する 40 の新興企業が参加している
- とても人気の高いプログラムで、待ち行列も長い。
- 正式なベンチャー企業選択プロセスがある。
- 企業家が住み込み（resident）の指導者としている

- ノースロップ・グラマン社のメリットとしては新興企業の活動を早い段階で知ることが出来ることである。

(4) IT と e－ガバメントについて

- 米国には 39,000 の地方政府がある。地方政府が e－ガバメントを導入しない 5 つの理由（トップは資金）の一つにセキュリティが必ず含まれている。
- 地方政府や連邦政府機関に対して、サイバーセキュリティに関する主要な関心事、最近の対策、要求などについての調査を行う予定である。
- 非常に深刻な事件が発生すれば、連邦レベルで、厳格で広範囲にわたる政策が認可されるかもしれない。（だだしニューヨークでのハリケーン Sandy 事件の後で初めて “storm barriers” が建設されたように、米国政府が事前対策を講じることはない）
- この件に関して行ったり来たりを繰り返しているが、現在米国議会図書館がデジタル・ミレニアム著作権法に関連して [49]、iPad や iPhone の jailbreak[50] を非合法としている。
- 社会には、常にイノベーションとセキュリティの間や、プライバシーとセキュリティの間の論争がある。
- 地方政府の情報は人事情報、犯罪歴、病歴、および進行中の入札情報以外は、大部分（90% 以上）が公表されている。 地方政府や州政府は、誰かがそれを盗むという「機密性」のリスクよりも、誰かが記録を改ざんするという「完全性」のリスクを重視している。
- 1970 年代に、URBIS プロジェクトにおいて、地方自治体の様々の用途に使える標準的なソフトウェアを開発・普及させることが試みられたが、その規模が大きすぎて、数年間して完全に失敗に終わった。19,000 もの自治体に対する標準的なソフトウェアというものは、最初から無理であった。
- 標準的なソフトウェア以外の、ハイブリッドな方法も試みられている。DHS（米国国土安全保障省）による NIEM (National Information Exchange Model)[51] は、全ての（連邦、州、自治区、地方）のレベルの政府、民間の機関や会社のための XLM 形式の重要情報交換フレームワークである。また STIX (Structured Threat Information eXpression)[52] は NSA（国家安全保障局）から 2 年前に出てきたもので、構造化されたサイバー脅威の情報

[48] http://www.bwtechumbc.com/cync/
[49] デジタル・ミレニアム著作権法は米国議会図書館の管轄である
[50] メーカーが承認していないソフトウェアを動作させるための改造
[51] https://www.niem.gov/
[52] https://stix.mitre.org/

を表す標準言語である。 これらは政府の異なった機関のコンピューターの間での自動的な情報共有に用いることができる。

(5) その他

(a) サイバーセキュリティ専門家のキャリアパスについて

- サイバーセキュリティの仕事はたくさんあるこの地域では、技術系の人材も実践系の人材(practitioner) も比較的簡単に納得いくポジションを得ることができる。
- この地域以外では、実践系の人材が重視されている。米国の労働市場ではサイバーセキュリティはブームである。
- 修士や博士の学位は、産業界での昇進の強みとなる。
- サイバーセキュリティの専門家になるための魔法の杖はない。防御を行えるようになる前にネットワーク構築など基本的なことを理解する必要がある。

(b) サイバー攻撃側になることについて

- DARPA (Defense Advanced Research Projects Agency: 国防高等研究計画局) はサイバー攻撃能力の研究開発に資金の拠出を始めた。
- National Defense Authorization Act for FY14 は、大統領にサイバー兵器の蔓延に対する政策とフレームワークを用意することを求めている。 しかしたった 1 MB 程度のサイズしかないマルウェアが何百万という方法で送り込まれている現状では極めて困難である。
- ハッキングの仕返しを行うことに関する意見が増えている。
- スタクスネットについては、海軍将校が New York Times の記者、David Sanger に話をした後で、やっかいなことになった。

(c) サイバー攻撃のコストシミュレーションについて

- サイバー攻撃による損害について確かな費用推定を行うことは困難である。

(d) 情報公開法 (Freedom of information Act) 関連の動向について

- 民間企業は情報公開法を、インシデントの情報を公開しない言い訳としている。 情報公開法は明確に各企業の固有の情報の公開を除外している。
- 金融機関は、彼らの情報が刑事法廷で出てしまうことを懸念している。
- 下院は “Cyber Security Information Sharing and Protection Act” 法案を通したが、上院はこれを 2 度拒んだ。この法案はサイバー攻撃が起きた場合に、民間企業に対してパケットレベルの情報提供を強制するものである。

(e) サイバーセキュリティの研究開発センター

- NIST (National Institute of Standards and Technology: 米国標準技術局) はサイバーセキュリティに関して、適切な技術を有する人を訓練するために、 FFRDC Federally Funded Research and Development Center: 国立研究開発センター) を設立しようとしており、UMBC 大学や UMCP 大学は企画書の準備をしている。 技術的専門技術を作

り、サイバーセキュリティ人材を生み出そうという教育的側面がある。

(f) サイバーセキュリティの最近の状況

- サイバーセキュリティを取り巻く最近の状況はドットコムバブルと似た面がある。
- 現在のサイバーセキュリティは非常に労働集約的である。あまりに多くの看護師がその症状を看ているような状況だが、必要とされているのは根本的な原因を探り適切な治療を行う医師である。根本的な解決策として以下が示唆される。
  - 単純な電化製品への TPM (Trusted Platform Module) の導入
  - 幅広い人々に対する（サイバーセキュリティに関する） 高校レベルの教育
  - 法や政策の強化
  - ワイヤレス機器に対する連邦通信委員会の認可のような、コンピューターに対するセキュリティ認可
- サイバーセキュリティは自動車のようである。長い時間をかけて自動車は最近より安全になった。
- 今のところ、技術が法律を先を行っている。
- Cisco がメリーランド州コロンビアの Sourcefire という会社を 27 億ドルで買った。

以上

4. CSIS (Center for Strategic and International Studies)

面談先	CSIS (Center for Strategic and International Studies)：
面談日時	2013.7.24　14:00~16:00
面談者	先 方 ： Mr. James Andrew Lewis, Director and Senior Fellow, Technology and Public Policy Program 当方：田中理事長、益岡、石野
面談テーマ	日本と米国におけるサイバーセキュリティの状況について

(1) CSIS 概要

1962 年にジョージタウン大学の付属研究機関として設立された保守系シンクタンクで 1987 年同大学から独立した。アメリカ陸軍・海軍直系の軍事戦略研究所でもある。

(2) マンディアントレポートやスノーデン事件の影響について

- マンディアントレポートは、何が起こっているのかについてよく分かってなかった一般の人々に実際に何が起きているのかを知らせ、また米国の世論形成という意味で重要な役割を果たした。 しかし米国政府に大きな影響を与えたのはマンディアントレポートの数週間前に出た米国政府内の機密報告である。 その機密報告はより詳細に中国のサイバースパイ活動の状況を説明しており、それは我々が思っていたよりも深刻であった。この機密報告は中国に対する見方を変え、米国政府に大きな影響を与えた。
- スノーデンについては、まだ話すには早すぎる。中国は直接的な影響を与えていない。米国は、3 年間に亘り中国と話し合いを行ってきた。米国は中国による国家安全保障のためのスパイ行為に対しては異議を唱えない。しかし、商業的な目的のためのスパイ行為に対しては異議を唱える。私は、これが国際的なサイバーセキュリティの条約を作ろうという努力に影響を与えないか心配している。問題の一つは、ほとんどの国が全く同じこと（国家安全保障のためのスパイ活動）を行っているため、異議を唱える立場にないことである。

(3) これらの事件がサイバーセキュリティに与えた影響について

- 今では、人々は問題の範囲についてより良い認識を持つようになり、ネットワーク防御やサイバーセキュリティのニーズを強めている。
- 欧州委員会は、連盟国の各国の安全保障に関する話をすることを許されていない。
- 米国は仏国とテロリズムや蔓延についての情報交換を行っているが、仏国は SIGINT (SIGnal INTelligence: 通信、電磁波、信号等を媒介とした 諜報活動）や、情報諜報活動において、米国の助けを必要としない。彼らはタフで活動的である。英国も同様である。
- 一つ良いことは、人々が安全なネットワークなど無いことや、注意することが必要であることに気付いたことである。

(4) 官民連携について

- FBI と米国国土安全保障省は、国民との対話に開放的である。米国には、1998 年から ISAC

(Information Sharing and Analysis Center）や、InfraGard、NCFTA (National Cyber-Forensics& Training Alliance）といった公的な組織がある。パートナーシップを築くために多くの努力が行われた。企業と政府、学会は情報交換を行っている。

- 英国人は、信頼を持つことが重要であると言う。いつも同じ人と、小人数のグループで定期的にミーティングを行うことにより、長期間に亘る信頼関係を築くことができる。

(5) サイバーセキュリティのための政府機関

- 国土安全保障省には戦略、権限、人的資源が必要である。 仏国や英国は良いモデルとなるであろう。
- 仏国は、ANSSI (National Agency for the Security of Information Systems）を内閣府に置き、強い規制力を有している。また、それは、SGDN (General Secretary for National Defense）と連携して国家防衛の役割を担っており、そのことが他の政府機関に対する権限につながっている。
- 英国は 2 つの異なった機関を有している。CESG (Communications-Electronics Security Group）と、CPNI (Centre for the Protection of National Infrastructure）である。英国は民間セクターと非常に強いパートナーシップを有している。企業の経営幹部たちと長い間打ち合せを行い、高い信頼関係を築いている。この 2 つの機関は GCQH (Government Communications Headquarters：政府通信本部）や警察庁相当の組織と連携し、内閣府官房に直接報告を行う。このように彼らは多くの権限と影響力を保有している。
- オーストラリアは、オーストラリアサイバーセキュリティセンター（ACSC：Australian Cyber Security Center）を最近設立した。これは、法務長官によって運営されている。

(6) 米国におけるサイバーセキュリティシミュレーション

- シミュレーションは非常に役に立つ。“サイバーストーム”は、国土安全保障省による最大のものである。財務省は、ウォールストリートの金融機関向けに ”Quantum Dawn 2”[53] を実施した。最初の“サイバーストーム”ではまず誰もが備えができていないことを学んだ。

(7) だれがどんな理由でインフラを攻撃するのか

- 昨年、重要インフラが北朝鮮やイランによって攻撃された。彼らは特別に洗練されているわけでないが、もしも彼らができるのであれば他の国にも可能である。私は、より多くの国がこの能力を有することになってきたと思う。さらに、今後 5 年の間に、非国家的組織がこの能力を有するようになるであろう。
- 中国の軍機は米国に到達できないが、中国のハッカーたちは米国を含め全世界に到達する能力を有している。 多くの企業は防御を持たず、もしも彼らが攻撃を行えばそれを阻むものは何もない。 準備しておく必要がある。
- 今年の 2 月に、大統領は NIST (National Institute of Standards and Technology：米国

[53] http://www.sifma.org/services/bcp/cybersecurity-exercise--quantum-dawn-2/

標準技術局）に重要インフラのサイバーセキュリティのフレームワークを作るよう大統領令を出した。[54]

- オーストラリアは 35 からなるサイバー攻撃の緩和戦略[55]を提示しており、政府機関はこれらを実行するのが義務となっている。トップの 4 つの緩和戦略で最低でも 85%のサイバー侵入は防ぐことができるとしている。
- 中国は貿易を確保する必要があるので米国をサイバー攻撃することはないであろう。米国へのサイバー攻撃は中国やロシアの利益とはならない。

(8) サイバー攻撃の費用積算

- 銀行やエネルギー関連企業はサイバーセキュリティに意味を見出しているが、他の企業を説得するのは難しい。
- IP 窃盗、サイバー犯罪、復旧コスト、追加的なセキュリティ費用、停止によって生じる損失利益などすべての種類のコストを挙げた。
- 現実的なサイバーセキュリティの確立のために、自動車事故や、海上の海賊行為、店舗からの窃盗などのデータを参考とした。保険会社からも情報を入手できないか検討している。

(9) その他

- 米国と中国はサイバーセキュリティに関し 2つの議題、責任ある国家の振舞いの定義と、誤算とエスカレーションの防止について取り組んでいる。
- 約 1 か月前に国連の政府専門家グループが規則や規範の骨組み（抑止（deterrence）には触れられていない）について合意した。 中国は準備会合で国連の成果に照らして彼らの慣行を変えると言っており、これは影響力がある。
- タリン・マニュアルは NATO のマニュアルではないが、誰もがそうだと思っている。2007 年にエストニアが攻撃された際に武力攻撃に相当するかはっきりしなかったため、NATO は第 5 条（共同防衛） ではなく第 4 条（協議）を適用した。 タリン・マニュアルは「武力攻撃」と判断する閾値を下げるもので、政治的な文書である。 また（サイバー）戦争経験に基づかず書かれている。
- 将来の協働について。今が日本のサイバーセキュリティにとって大事な時であり、日本のために何かを行いたいと思っている。日米のパートナーシップは、我々の経済にとっても極めて重要である。

以上

[54] 8 月末にドラフトが出た。http://nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf
[55] http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

5. DAC (Decisive Analytics Corporation)

面談先	DAC (Decisive Analytics Corporation)
面談日時	2013.7.26　　9:30～11:30
面談者	先方： Mr. John S. Donnellon, President Mr. Mark Hall, Vice President, Cyber Security Engineering Mr. Wayne Fujito, President, International Division, DAC, Chairman, NATO Industrial Advisory Group, and Chairman, NDIA International Division Ms. Cristiana Brafman Kittner, Defense Analyst/Export Compliance Official 当方：田中理事長、益岡、石野
面談テーマ	サイバーセキュリティにおける官民連携の在り方について

(1) DAC 概要

- DAC は 1996 年に設立された、従業員所有企業[56] である。複雑な問題に対して分析的な解決策を提供することを得意としている。米国国防総省や国土安全保障省を始めとする官庁や民間企業を顧客としている。
- 昨年、サイバーセキュリティチームを立ち上げた。現在 9 名が所属し、外部のパートナーの協力も得て活動している。ソフトウェアの安全保障（安全なコードの作成方法、政策など）、サプライチェーンのリスクマネジメント（特に特定用途の電子機器や FPGA (Field Programmable Gate Array)）など様々な分野において、特に米国国防総省や国土安全保障省などの政府機関を中心に専門家を派遣している。
- サイバーセキュリティチームは、ペンタゴンの全ての一般的な、サイバーセキュリティ会議に出席し、国防総省や国家のサイバーセキュリティ計画の活動に対して助言を行っている。また、”Joint Information Environment (統合情報環境)” と呼ばれる将来のネットワークの構想について、サイバーセキュリティの見地において国防総省を補佐している。
- Hall 氏は国防総省や NASDAQ (ナスダック店頭株式市場) を含む政府機関や、民間企業、国際的な組織と協働し、現在のサイバーセキィリティの課題の理解を助けたり、セキュリティ・アーキテクチャや、継続的な監視能力、ネットワークのセキュリティなどの構成を進言している。
- DAC は海外諸国とも協働し、彼らの国家的な情報セキュリティ政策を開発している。
- DAC は単純な技術トレーニングを超える特注トレーニングや情報の流れなど SOC (Security Operation Center) で必要なことを教えている。

[56] 株式を従業員が保有する会社

(2) 官民連携について

(a) SINET

- DAC はカリフォルニアの SINET (Security Innovation Network: (情報) セキュリティ革新ネットワーク) と非常に緊密に活動している。これは官民連携の良いモデルである。SINET はイノベーションコミュニティを見ている。そこでは、サイバーセキュリティにおける最良、最新の技術が開発され、政府や、際立ったサイバーセキュリティ手法に興味を有する投資団体など、多くのパートナーを呼び集めている。(日本の企業でも参加することができる) SINET は毎年ニューヨークとワシントン D.C. で展示会を開催している。

(b) NDIA

- NDIA (National Defense Industry Association: 国家防衛産業連合) は防衛産業の団体で、別の官民連携のモデルである。政府と産業界を一同に集め、知識や課題や問題、そして解決策を共有する。DAC の Wayne Fujito 氏がその国際部門の責任者である。約 1,700 の欧米企業がその会員となっている。 36 の部門がある。サイバー部門は 2 年前に設立され、責任者はノースロップ・グラマン社の退職者である。

(c) 官民連携における課題

- 官民連携における課題として、以下 3 点が挙げられる。

  a 相互信頼

  政府は、企業の情報を機密にし、企業は政府の情報を機密とすべきである。また、企業が所有する情報は、「情報公開法」の対象外とすべきである。

  b 資金

  民間企業にサイバーセキュリティに対してお金をかけてもらうことや、将来の脆弱性や新たなネットワーク構造などの変化に対応する投資を継続してもらうことが課題である。目指すべきは、ネットワークセキュリティ体制の継続的な評価や、新たなイニシアティブに対して毎年適切な投資を行うことである。

  c 義務と自発

  防御を義務とするのであれば、多くの規制、法制度、負担などの課題について取り組むことが必要になる。自発的なものとするのであれば、何らかのインセンティブを付与させるべきであろう。

(d) 平和時の備え

- 国家はワーキンググループや、コミュニケーションチャネルを持ち、そこで、全ての問題や、論点、悩みの種や、何が享受できるリスクかまたはそうでないか、について話し合うべきである。政府は、民間企業が何を考えているかについて理解すべきである。
- サイバー災害から戦時への移行についての権限や手続きをはっきり定める必要がある。
- 平和時に、手続きを制定しその手続きをテストするための演習を行う必要がある。この演習には、米国の情報コミュニティや、警察コミュニティ、国防総省、民間機関、通信セクターなどすべてが関与する。

- 予期できない事象（unexpected elements: 例えば、サイバー攻撃と関連すると思われていなかった爆発が、東京で発生するなど）に直面するようなシナリオに基づいた演習を行い政府内の連携を必須とさせる。演習の後で、政策や、手続き、原則、変更などについての評価を行う。
- 政府関係者を一室に集め、（例えば、現在の通信の秘密に則して）現在の権限で演習を行い、次に新たな権限を与え、彼らが何をすることができるか、また結果がどのように変わるかなどを確認したりする。
- 米国のサイバー演習は軍隊のサイバー演習から始まり、それがより大きな軍事演習に統合され、次に、軍隊、諜報コミュニティ、他の一般省庁、法執行機関や警察も参加し、民間セクター、さらには州や地方政府も巻き込んだ演習に展開していった。
- 一つの演習ですべて入れ込むのは多すぎるので、それぞれの演習では、例えば州と化学産業と水道産業の 3 つを選ぶなどと絞り込む。
- 各国にとって考慮すべき主なポイントは、既存の手続きや、権限や機能が、国家危機的なサイバーインシデントを検知し、軽減し、それから回復できるかについて検討することである。国家は、そのようなインシデントが発生して初めて、それらの手続きを開発し、テストするということになってはいけない。
- 民間セクターは、その関心事や論点、何か行うべきことを政府に伝えるべきで、また、何をすべきかの議論をすべきである。国民が課題を理解できるように、政策が適切に整えられるべきである。
- 米国は、多くの FFRDC (Federally Funded Research and Development Center: 国立研究開発センター）を設立した。MITRE Corp, Institute for Defense Analyses, Aerospace Corp, MIT's Lincoln Laboratory などである。政府組織にとってこれらは組織の強化となる。日本もこのような民間企業による政府機能の増強が必要である。
- NATO の産業アドバイザリーグループが、そのサイバーセキュリティのアクションプランの実行について、産業界がどのように NATO を補佐できるかについての報告書を完成させ、現在、それに続く報告書を作成している。マイクロソフトや、ISPs[57]、SIs[58] や、マカフィーやセマンテックのようなセキュリティ会社を含む、15 か国からの 47 社がこれに参加している。今年の年末までには次の報告書が入手可能になるであろう。
- その他の官民連携のモデルとしては、税控除や政府と産業界の協同組合（joint partnership）などがある。

(3) 重要インフラの防御について

- 金融セクターや、軍、軍事産業拠点は、明らかに攻撃の対象となりうる。
- 他の重要インフラセクターに対する攻撃者はそれほど組織立っていない。重要インフラ企業はサイバー攻撃のリスクは理解しているが、リスクの高さやリスクに対する投資のトレ

[57] Internet Service Provider
[58] System Integrators

ードオフについては納得していない。 例えばボストンで停電があったが、それは小規模の取るに足らないインシデントであった。通信を遮断するためにケーブルの接続点を爆破することや、貯水場に毒を流すことのほうがよっぽど起こりそうである。政府内で哲学的な論争が行われている。 ただ重要インフラ企業は耳を傾けるようになってきた。

- 政府は、脅威の情報や解決策をインフラ企業と共有すべきであり。インフラ企業は、インシデントのデータを政府と共有すべきである。両方が必須である。

(4) サイバーセキュリティに関する一般的な情報

(a) 外国製品の使用禁止について

- 認識されている極端に疑わしい供給者を除けば、国家レベルの使用禁止はできない。 産業界で行われるべきである。リスクに基づく評価も必要である。
- 各省庁が、把握するための手続きを持つべきであり、少なくとも確認を行うためのチェックリストがあるべきである。政府機関の間で、脅威に関する情報を共有する手続きがあるべきである。情報共有のために政府レベルの CIO（最高情報責任者）協議会を設けることも一つの方法かもしれない。

(b) スノーデン事件について

- 誰もがスノーデン事件に色めき立っている。
- スノーデンは単なるシステム管理者にすぎなかった。NSA に行く前、3 年間別の民間企業を通じて CIA のために働いていた。彼は恐らく CIA で働いている間に NSA が何を行っているかを知り、Booze Allen 社を通して NSA で働くことを決めたのであろう。
- スノーデン事件は世論や議会に大きな影響をもたらした。 PRISM プログラムを続けることについての議会投票はわずか 10 票差で通過した。ただし、プログラムに対して何らかの修正が行われるであろう。
- NSA は彼が（PRISM 以外の）他の情報を漏らすことを恐れている。それは NSA にとってより大きなダメージとなる。

(5) その他

- 国防総省の調達関係の次官が来週日本と韓国を訪問する。彼が最初の役員レベルのシステム・技術フォーラムの議長を務める。ひとつの議題がサイバーセキュリティである。
- 日本の外務省主催による日米政府間のサイバー協議が 3 月に開催され、次回は第 4 四半期（10 – 12 月期）に行われる予定である。
- 報告先の官庁が多すぎることへの示唆: 陸軍、海軍、空軍がお互いに話し合うことを求める法律や、諜報機関の調整を行う長官により強い権限を与える別の法律により事態は好転した。
- Hall 氏は、エストニアがロシアの攻撃を受けた際にシアトルで NATO のコンファレンスを主催していた。エストニアの代表者が他の国の出席者に助けを求めた。Hall 氏は、NCRCG（National Cyber Response Coordination Group）の副議長として、NCRCG に

対してこのインシデントを報告し、フランスやポーランド、ドイツ、その他のコンファレンスに出席していた代表者たちに、エストニアを攻撃している IP アドレスのリストを供与した。エジプトは NATO のメンバーではないが、攻撃の多くを占めていたので、米国国家国土安全保障省が通信会社とコンタクトして、エジプトからエストニアに対する全ての通信を遮断した。FBI のヒューストン支部は、米国内の攻撃を行っている全ての IP アドレスの責任を負った。 エストニアに対する攻撃の軽減策の一つが、地域や国際的な通信会社やインターネットサービスプロバイダーの関与であり、これによってエストニアに向かう悪意があると疑われる通信を遮断し、エストニア内の通信帯域を拡げることができたのである。

- 国防総省の CIO 調査によれば、IT 予算の内 10 - 15 % が IT セキュリティに使われている。
- 3 年前、国防総省は年間 30 – 40 億ドルを、連邦全体では年間 70 – 80 億ドルをサイバーセキュリティに費やした。
- サイバーセキュリティ政策は、国や文化、経済水準によって異なるが、人と政策、技術、そして手続きのすべてを必要とする。
- 一般人や専門家の教育が必要である。人を訓練する事（例えば、資格を取らせること）とネットワークをどう防御すればよいのかを教える事は、2 つの異なる事である。
- 最良の組織は、良い IT 基本設計と同時に、良いサイバーセキュリティ基本設計を保有している。良いセキュリティ基本設計により、コストを理解し、抑えることができる。

以上

6. State Government of Maryland

面談先	State Government of Maryland
面談日時	2013.7.26　　16:30～17:30
面談者	先方： State Government of Maryland: Mr. Patrick Tonui, Program Manager, Security and Information Technology, Office of Strategic Industries & Innovation, Maryland Department of Business & Economic Development UMBC: Mr. Greg Simmons, Vice President for Institutional Advancement 当方：益岡、石野
面談テーマ	・サイバーセキュリティにおける企業育成の在り方について。 ・サイバーセキィリティ人材育成の在り方について

(1) Maryland Department of Business & Economic Development の概要

Maryland Department of Business & Economic Development の使命は、メリーランド州に活発な経済環境を形成する一方、仕事を創造し誘致することであり、州に成長産業を誘致して育成するための政策や規制を設けたり、障壁を減らすことにより、ビジネスに優しい環境を供給している。2010 年 1 月から、サイバーセキュリティ産業を育成するために、”Cyber Maryland”[59] と呼ばれる施策を始めている

(2) 2010 年にまだ今ほど話題となっていなかったサイバーセキュリティを選択した理由

- まず、IT や IT セキュリティの主要な推進者がメリーランドにいたことが挙げられる。次に、オバマ政権が 2008 年に現れた際に、最初に大統領が発言したことの一つに、サイバーセキュリティが国家安全保障の優先事項となるということであったことがある。
- 連邦政府レベルで、軍関連とそれ以外の省庁の両方においてセキュリティについて議論が開始され、それについて責任を負う機関（Cyber Command）が必要になった。メリーランド州には NSA（National Security Agency: 国家安全保障局）と NIST（National Institute of Standards and Technology: 米国標準技術局）がすでにあり、技術を開発しサポートする企業も存在していた。
- 2009 年に初期の準備が行われ、2010 年に基盤を据えるための報告書 ”CyberMaryland”[60] が公表された。

(3) ”CyberMaryland” の趣旨について

- 我々は最初に、政府関係機関とシステム・インテグレーターや技術開発などの民間セクターの両方と話し合いを行い、サイバーセキュリティとは何か、なぜサイバーセキュリティが大切なのか、彼らにとって何が重要か、どのような課題や障害と直面しているのかなど

[59] http://www.cybermaryland.org/
[60] http://www.choosemaryland.org/aboutdbed/documents/finalcyberreport.pdf

について理解に努めた。その結果、我々が州政府として最も影響を与えることのできる以下 4 つが浮き彫りとなり、 “CyberMaryland” に盛り込まれた。

a 教育

市場に対応し、雇用者のニーズに合致した労働力を用意する。我々は IT 職とサイバーセキュリティ職の間のギャップを見極めた。 また、政府（特にいくつかの省庁）は “Cyber Warriors (サイバー戦士)” を必要とし、民間企業（特に技術の開発や改良を行っている企業） はいろいろなツールを理解している人々を必要とした。その結果は、UMBC (University of Maryland, Baltimore County: メリーランド大学ボルティモア郡校) や、UMD (University of Maryland, College Park: メリーランド大学カレッジパーク校)、ジョンズ・ホプキンス大学の様な、学位を与える教育機関における教育カリキュラムに反映されている。

b 起業援助

エンジェルインベストメントや、シードベンチャーキャピタル、専門家や研究者からの援助へのアクセスを提供するプログラムや手段を開発する。 我々が目指す力強いサイバーセキュリティ産業のモデルをシリコンバレーに求めた。

c 政策

適切なサイバーセキュリティの衛生と実践のために、全ての人々や企業に適切な教育と情報を提供するべきである。

d マーケティング・コミュニケーション

皆にメリーランドがサイバーセキュリティ企業を成長させるために良い場所であることを知らしめる。

- “CyberMaryland” は、政策的なリーダーシップ、ブランドや交流の基盤、起業家企業家、大学、企業の行動を誘引することについての素晴らしい事例である。

(4) メリーランドに企業や人を誘致できる要因

- 以下 3 つの要因の組み合わせによる。

a 顧客

サイバーセキュリティの最大の顧客がこの地域に存在している。

b 資金

資金を必要とする中小企業が資金を得ることができる。サイバーセキュリティを中心とする州によるベンチャーファンド、その他のベンチャーキャピタルや投資家がある。州には専門家がいてどの会社に投資を行うかを決め、時には民間と組んで投資を行うこともある。州は、また、ベンチャー企業をパートナーや顧客、アドバイザーに紹介する。州は投資家やベンチャーキャピタルとは異なり、投資は行うが、会社に役員を派遣することはしない。

c インキュベーターネットワーク（bwtech@UMBC）

ここでは、事務所スペースや法的助言、技術的な資源を得ることができる。生命科学

やクリーンエネルギーのインキュベーターとともに、UMBC は 2010 年に、サイバーセキュリティのために 20,000 平方フィートのインキュベーター施設を設立した。現在 40 のサイバーセキュリティ企業に対し、低家賃のスペース（非常に可能性のあるサイバーセキュリティ企業に対しては無料のこともある） や、政府調達や、セキュリティクリアランス、様々な市場セグメントへの売り込みに関する情報を提供している。企業が大学の先生と結びつき、企業が大学のカリキュラムに影響を与え、研究の商業化を助けるといった豊かなエコシステムとなった。

(5) インキュベーターネットワーク (bwtech@UMBC) がうまく行っている要因

- 株式の代わりにリサーチパークがサービスやノウハウを提供する仕組みが重要である。
- 立地も貢献している。空港から 2 マイルで、 NSA から 10 分、バルティモア市内から 10 分、ワシントン D.C. からも 40 分である。
- 大学の評判。UMBC は様々な組織を援助するために、提携や関係構築を行うことで有名である。
- 州の ”CyberMaryland” も役立っている。UMBC はこの報告の方針に沿ってカリキュラムや訓練プログラムを作った。

(6) メリーランド州立大学システムにおけるサイバーセキュリティ教育

- メリーランド州立大学システムには、3 校の研究大学（research universities）を含む 12 の大学がある。州内の多くの大学がこの分野に関わっている。 サイバーセキュリティは特に新しいものではないが、最近それに対する需要が増加している。 競争はあるが、それぞれが自身の得意分野を見つけている。州レベルでは重なったコースを供給しないように努力している。
- UMBC は伝統的な学士から博士までの学部・大学院のプログラム、働いている人向けのマスターコース、数年前からの営利目的の学位授与の無い訓練コースを提供している。最後の訓練コースは、急激な変化や、様々な産業界のニーズに応えるものである。 UMBC のコースは非常に厳格で、産業界や連邦政府の両方から緊密に情報を提供されている。NSA や企業からの臨時講師も用いて、通常の学生と会社からの学生から成るクラスで、ユニークな経験を与えている。
- UMUC (University Maryland University College: メリーランド州立大学ユニバーシティ・カレッジ) は、メリーランド大学システムにおける遠隔学習キャンパス（distance learning campus）であり、オンライン訓練や拡張学習（extended learning)、中堅社員向けの特別訓練を行っている。コースは全世界に供給されている。米軍と契約し、世界中の米軍兵士が技能を身に着け、学位を取ることを手伝っている。米軍に対する学士教育、修士教育の一番の供給者でもある。伝統的なコースに参加できない中堅社員に対する特別訓練も行っている、
- UMD (= UMCP メリーランド大学カレッジパーク校) も技術や政策系の学部・大学院の

プログラムを有している。法律課程では、特許侵害の様なサイバーセキュリティ政策を取り扱っている。

(7) ”CyberMaryland” の 3 年間の実績

- マーケットのニーズに合わせて新しいコースを設立し、プログラムの数を増やした。（3 年前にはサイバーセキュリティ独自の学位すらなかった。）
- 顧客がいるというだけではなく、サイバーセキュリティについて深い知識を持つ人たちがいるという理由で、2010 年からロッキード・マーチンや、ノースロップ、ボーイングなどの大企業が、サイバーセキュリティの中核的研究拠点（Center of Excellence）を設立している。そこには最も優れた研究者を配し、人々に訪問してもらい企業の能力を分かってもらったり、研究や、プロジェクトマネジメントやシンクタンク的な仕事を行う。

(8) サイバーセキュリティの学位とその他の IT の学位の違い

- 数学やコンピューター、ソフトウェア設計等の基礎的なコースは同じである。 追加的な必須コースは民間企業と話し合いを行い、企業がどのような技能を求めているのか、新卒の IT 学士をちゃんとやっていけるサイバーセキュリティの専門家になるためにどのような追加訓練を企業では必要としていたのか、などを探し出すことによって開発される。追加的なコースとしては、例えば、マルウェア検出、リバースエンジニアリング、侵入検出技術などに力点を置いたソフトウェアデザイン・企画がある。

以上