CIPPS
Center for International Public Policy Studies

サイバーセキュリティに関する
海外出張調査報告書

ロンドン・ブリュッセル・ハーグ・テルアビル

2012.11.6 ～ 11.16

益岡 竜介 主任研究員（masuoka@cipps.org）
石野 務 主任研究員（ishino@cipps.org）

国際公共政策研究センター

2013 年 3 月

CIPPS
Center for International Public Policy Studies

【目次】

CIPPS
Center for International Public Policy Studies

1. サイバーセキュリティ 海外調査出張概要

1-1 出張日程及び面談等

2012 年 11 月 7 日～14 日の間、ロンドン、ブリュッセル、ハーグ、テルアビルを訪問し、国の機関、国際的機関、シンクタンクなどと意見交換を行った。また、テルアビルでは、サイバーセキュリティに関するコンファレンスに出席した。主な面談先と面談のテーマは表 1 の通りである。

なお、面談先への申し入れにおいて、在日イスラエル大使館の原田上席商務官及び綾尾総務官、並びにジャーナリストの Brigid Grauman 氏にも多大なご協力を頂いた。今回の面談に協力して頂いた方々と合わせて、深く謝意を申し上げたい。

表 1 面談先等及び面談のテーマ

面談日	面談者・面談先	面談テーマ
11/7 (水)	Mr. Negel Inkster Director of Transnational Threats and Political Risk IISS (International Institute for Strategic Studies)	日本と英国におけるサイバーセキュリティの状況
11/8 (木)	Mr. Andrea Ghianda, Project Manager SDA (Security & Defense Agenda)	日本と欧州におけるサイバーセキュリティの状況
	Dr. Jamie Shea Deputy Assistant Secretary General for Emerging Security Challenges NATO (North Atlantic Treaty Organization)	日本と欧州におけるサイバーセキュリティの状況
11/9 (金)	Deputy Director, Operations Department Designated Head and Representatives of Strategy and Outreach EC3 (European CyberCrime Centre), Europol	日本と欧州におけるサイバーセキュリティの状況
11/12 (月)	Mr. Avi Shavit Former Head of Homeland Security Consultant of The Chief Scientist Industry, Trade & Labor Ministry Mr. Avi Luvton Executive Director for Business Development - Asia & South America MATIMOP - Israeli Industry Center For R&D	日本とイスラエルにおけるサイバーセキュリティの状況
	Mr. Rami Efrati Head of Civilian Sector Division National Cyber Bureau, Prime Minister's Office	日本とイスラエルにおけるサイバーセキュリティの状況
	Nimrod Kozlovski 博士	日本とイスラエルにおけるサイバーセキュリティの状況
11/12 (月) ～ 11/14 (水)	Israel Home Land Security 2012	サイバーセキュリティ、重大なインフラの防御など

1-2 質問事項

今回の海外出張では、我が国や海外諸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ついての一般的な課題について、海外の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 表 2 のような質問事項を挙げた。

表 2 主要質問事項

(1) 我が国や海外諸国のサイバーセキュリティの現状

我が国のサイバーセキュリティの現状について以下の項目を説明したうえで、これに対する意見や、訪問先の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 政府の体制
② 最近発生したインシデントについて
③ 最近改善された事項と、まだ残る課題
④ 15 の民間企業などに対するヒアリング調査結果から推測される課題

(2) サイバーセキュリティについての一般的な課題

以下のような課題について意見交換を行った。

① 最近発生したインシデントや課題について
② 政府内の縄張り争いについて
③ 官民連携について（情報共有・民間セクターのサポート、民間セクターからの協力など）
④ ファーウェイなど外国通信製品の利用について
⑤ 人材育成について
⑥ EU データ保護指令 [1] の改正状況について
⑦ 将来的な CIPPS との提携の可能性について

なお、本海外出張において、我が国のサイバーセキュリティの現状についての説明に使用した資料（英語、一部修正）は、CIPPS のホームページのサイバーセキュリティレポート Vol.3 "Cyber Security in Japan"（日本のセキュリティ政策）に掲示しており、以下の URL よりダウンロードが可能である。

URL: http://www.cipps.org/group/cyber_memo/003_121204.pdf

1 個人データの取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会 及び理事会の指令

2. 面談概要

2-1 IISS (International Institute for Strategic Studies)

(1) IISS 概要と面談者

核抑止や軍備管理を目的に 1958 年に英国で設立された独立系シンクタンク。世界平和の維持や安全保障のための健全な政策の採択と良好な国際関係を推進することを使命とし、主に世界の安全保障、政治的リスク、軍事紛争を研究テーマとしている。

Director of Transnational Threats and Political Risk である Negel Inkster 氏にインタビューをした。

URL (IISS): http://www.iiss.org/

(2) 主な意見交換内容

Negel Inkster 氏との主な意見交換内容を以下に箇条書きにする。

・日本企業では取締役会がサイバーセキュリティを重視していることが印象的である。英国企業の水準はとても低い。
・英国は、2 年前にセキュリティレビューを行い、サイバーセキュリティ対策を強化した。
・サイバーセキュリティ対策は GCHQ (Government Communications Headquarters: 政府通信本部) が中心に行っている。米国の NSA (National Security Agency: アメリカ国家安全保障局) ともパートナーシップ協約を結んで協力している。NSA の Echelon のシステムがダウンした際に、GCHQ が代わって 2, 3 日にわたりカバーしたこともある。
・プライバシーとセキュリティの関係については、ポストで怪しいものが発見されたら爆発することができるように、 Botnet[2] で悪いものが見つかったら届け出を行わせるような制度も必要であろう。どのようなデータを政府に提出するのかについての基準を法律でしっかり定めて、個人や企業が自分で判断することは避けるべきである。現在、英国では、警察が後で調査できるように、プロバイダー業者に対して、コミュニケーションデータを 1～3 年間保存しておくことを義務付けることを検討している。
・英国では、米国がファーウェイに対して行ったような規制 [3]は行わない。英国は自国に通信製品の製造会社がなく、他国製品を使う必要がある。例えば、英国のブリティッシュテレコムでも、ファーウェイから製品を購入している。すべての製品のソースコード [4]を英

2 数多くのパソコンやサーバに対して、コンピューター・ウィルスなどを用いて遠隔操作できる攻撃用のプログラム（ボット）を送り込むことによってこれを乗っ取り、外部からの指令で一斉に攻撃を行わせるネットワーク

3 2012 年 10 月 8 日、米下院のインテリジェンス関連の特別委員会は、ファーウェイと ZTE の中国系通信機器ベンダー2 社については、資本関係などから中国政府との結びつきが強く米国の安全保障に対する脅威が懸念されるため、米国内から排除すべきであるとの報告書を発表し、規制強化を求めた

4 プログラミング言語によって記述されたコンピュータプログラム。

国情報局が確認し、トラップや隠された部品がないことを調べている[5]。

・各会社が従うべきコンプライアンスの基準として、サイバーセキュリティについて最低限のスタンダードを定めることが必要である。政府が水準を定めることにより、どの会社も同レベルの対策を行う必要が生じ公正な競争になる。（セキュリティレベルを下げることにより価格競争力を強化することは行えなくなる）英国では、将来の技術革新の変化に対応できる柔軟性を持った法制を作ることを検討している。どうやって柔軟性のある普遍的な規制を作るのかが課題となっている。

・ビッグデータ[6]を多種の方法で組み合わせることにより人物の特定も可能となる。例えば、監視カメラのデータと携帯電話と実際の観察データを組み合わせることにより、テロリストの候補者を事前に特定することが可能となる。ラスベガスのゲーム会社は、人のつながり（ゲームを行っている際のディーラーと参加者の関係など）を分析することにより、ディーラーが顧客と組んで悪事を行うことを感知するシステムを開発しており、英国もそのようなシステムの開発を検討している。

2-2 SDA (Security & Defense Agenda)

(1) SDA 概要と面談者

NATO と EU の間をつなぐ組織として、2002 年に設立された。両組織の軍備や安全保障の専門家に話し合いを行う場を提供している。また、軍備や安全保障に関するフォーラムの開催や調査レポートの発行なども行っている。

Cyber Security の Project Manager である Andrea Ghianda 氏にインタビューをした。

URL (SDA): http://www.securitydefenceagenda.org/

(2) 主な意見交換内容

Andrea Ghianda 氏との主な意見交換内容を以下に箇条書きにする。

・欧州では、この 1 月に One Stop Shop の機能を持つ European CyberCrime Centre (EC3) を設立する予定である。ここにサイバー攻撃などの情報を集め、サイバー犯罪に対する戦略を決めていく。（EC3 へのインタビューは後述）

・欧州では、公共と民間の間の関係を築くことが重要視されている。民間がネットワークインフラを保有していることから、両者の協力が必要となる。また、政府だけでなく民間企業も自分を守る必要がある。

5 検証センターを作り、200 人規模のエンジニアで検証した。

6 通常のデータベース管理システムなどでは、記録、保管、解析などが困難な大規模のデータの集まり。

・スマートグリッド[7] に関するセキュリティについては、ENIZA[8] のレポート[9] が出ているので参考にするといい。
・人材育成については、DHS[10] がレポート[11] を出しているので参考にするとよい。
・EU データ保護指令の動向については、サイバーセキュリティの動向も関連してくる。欧州議会の採決を必要とするが、6 か月以内にドイツの首相が代わることもあり、現時点ではどのようになるかはよく解らない。
・SDA のサイバーセキュリティ関係のリソースには以下のようなものがある
  ・Cyber reference library
  http://www.securitydefenceagenda.org/Contentnavigation/CyberInitiative/Cyberreferencelibrary/tabid/1333/Default.aspx
  ・Opinions
  http://www.securitydefenceagenda.org/Contentnavigation/CyberInitiative/Opinions/tabid/1334/Default.aspx

2-3 NATO (North Atlantic Treaty Organization)

(1) NATO Emerging Security Challenges 概要と面談者

以下の 2 つのポリシーの下、NATO に対する価値の創造を推進している。

1. 危機に備え、危機において NATO に選択肢を与える。
2. 例えば様々なユニットの機能を多角的に用いて効率性を高めることなど、予算の効率的な運用を考える。

NATO Emerging Security Challenges の Deputy Assistant Secretary General である Jamie Shea 博士にインタビューした。

URL (NATO Organization): http://www.nato.int/cps/en/natolive/structure.htm

(2) 主な意見交換内容

Jamie Shea 博士との主な意見交換内容を以下に箇条書きにする。

・現在、NATO は、加盟 28 ヵ国及びパートナー 7 ヵ国においてサイバープロテクションを展開している。センサーを向上させ、おとりの攻撃と本当の攻撃を区別する技術の開発

7 電力網に通信・制御機能を付加することにより、電力の流れを供給側・需要側の両方から制御し、最適化することを可能とする送電網。電力需要の適切な制御による省エネが見込まれる。

8 European Network and Information Security Agency: 欧州ネットワーク情報セキュリティ庁

9 “Smart Grid Security”: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/smart-grid-security

10 Department of Homeland Security: アメリカ合衆国国土安全保障省

11 “Cyberskills Task Force Report – Fall 2012”: http://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf

など、技術力の向上が課題となっている。NATO は NATO Computer Incident Response Capability (CIRC) の為に 58 百万ユーロの予算を確保した。

・情報局からの情報を分析するため、CTAC: Cyber Threat Assessment Center も設立された。また、エストニアに Cyber Defense Center of Excellence を置き、サイバー攻撃に対する防衛の訓練や学術的検討を行っている。この COE はかなりオープンなので、日本などとの連携も簡単であろう。

・NATO は加盟国 28 か国のうち 23 か国と了解覚書 (MoUs) を交わした。 各国に責任者を置きそこに情報が集中するようにしており、それらの国の CERT[12] とも協力している。

・NATO はサイバー攻撃も集団安全保障を適用する脅威に含まれると解している。レッドラインも意図的にはっきり定めていない。

① サイバー攻撃への対抗攻撃については以下のような課題がある。

a. サイバー攻撃の潜在性

サイバー攻撃は、気付かないうちに長期間かけて行われる場合があるが、被害を受けてから対抗攻撃を行うまでの時間が長いとその正当性がなくなる。(殴られてから 1 年後に殴り返すようなものである)

b. 同盟国の合意形成

エストニアのように 1 国のみが狙われる場合には、他国には波及しないため、同盟国に対抗攻撃を行うことを納得させるのが困難である。

c. 被害

人が死なないのに攻撃をすることは難しい。

d. 政治的な課題

NATO には 28 か国も加盟しているが、各国で認識も異なっている。どのレベルで問題を国から NATO に上げるか、NATO がどうやって同盟国を守るべきかなどについて定める必要がある。

② サイバー攻撃の定義

・サイバー攻撃の定義については、どのようなサイバー攻撃があり、どのような法律が適用されるのかを定めた、「タリン・マニュアル」がもうすぐ公表されるのでそれを参考にするとよい。[13]

---

12 Computer Emergency Response Team: コンピューター緊急対応センター。インターネットを介した不正アクセスに関する情報を収集・公開するアメリカの団体。セキュリティ問題に関する啓蒙活動も行っている。

13 Tallinn Manual の現時点のドラフトは次で公開されている:
http://issuu.com/nato_ccd_coe/docs/tallinn_manual_draft

・インシデントの種類には以下の 3 つがあると考えている。
1. 相手のレピュテーションを下げようとするもの
2. 政府の情報を盗もうとするもの
3. 大規模な DDoS 攻撃 [14]

③ サイバーセキュリティの課題については以下が考えられる。

a. 本当の攻撃の見極め
サイバー攻撃の情報については雑音が入るのでこれを取り除き、本当の攻撃とそうでない攻撃を区別する必要がある。そのためのシステムセンサーを開発中である。

b. 民間企業の利用
以前は公共のコンピューターの方が民間のものより性能が良かったが、今は逆である。どの程度の仕事を民間に移行し、どこまでを民間企業の責任とするのかが課題（challenge）である。実際に、NATO では、ほとんどのマルウェア [15]について、民間企業の「シマンテック」が対応している。
民間企業が保有する社会インフラに対して攻撃が行われた場合に、だれが責任を負うのかも課題である。

c. 人の教育について
人々は手続きの順守について緩いところがある。人のトレーニングが必要である。

d. 外国製品の利用について
外国製品の利用については、セキュリティを最初から考えなければならない。米軍の武器のマイクロチップが汚染されていたという事例がある。
製造業者との間に信頼関係を築くことが必要で、それがセキュリティを保証する。保証はどうやって築くのかということについては、いつでも監視できることだと考える。厨房で作られた料理を食するのではなく、すし屋のように目の前で作られた料理を食するということである。

2-4 EC3 (European CyberCrime Centre)

(1) EC3 概要と面談者
オランダ ハーグにある Europol に 2013/1/1 に開設予定の組織で EC3 Management のもと、Data Fusion, Operations, R&D Training, Strategy/Outreach/Crime Prevention の 4 つのグループからなる。 EU のサイバー犯罪との戦いの中心となり、サイバー攻撃へ

14 複数のネットワークに分散する大量のコンピューターから一斉に特定のサーバへパケットを送出し、通信路をあふれさせてサーバのキャッシュメモリやポートを接続不可能に陥れる攻撃

15 コンピューターウイルス、ワーム、スパイウェアなどの悪意のあるソフトウェア

の素早い対応に貢献していくことを目的としている。そのために、EU の各国、組織が、捜査の運用・解析能力および国際的なパートナーとの連携を構築するサポートを行う。

EC3 の Operations Department の Deputy Director および Strategy and Outreach の Designated Head とそのメンバーにインタビューをした。

URL (EC3): https://www.europol.europa.eu/ec3

(2) 主な意見交換内容

彼らとの主な意見交換内容を以下に記述する。

EU の 27 の加盟国それぞれサイバー犯罪 に対する能力レベル、国内の法制度（どのように犯罪捜査、起訴していくか）などが異なることがあり、それが EC3 のあり方を規定する一つの要因であると考えられる。EC3 は、以下の 7 つの主な機能（core functions）を有する。

① EC3 の 7 つの主な機能

a. サイバー犯罪に関する情報の集積［Information Hub on Cybercrime］

産官学の運用データを集めて共有する。

b. 能力開発［Capacity Building (Law Enforcement, Prosecutors, Judges)］

警察だけでなく、検察官（prosecutors）や裁判官（judges）の教育も進める。

c. 業務のサポート［Operational Support］

情報（Intelligence）提供を中心とする。証拠収集（HDD の解析など）のサポートなどは行うが、実際の証拠収集や裁判で証言することは基本的にしない。

d. 犯罪科学のサポート［Forensic Support (Research & Development)］

学術界, 産業界、各国警察などとの研究や オープンソースのツール作成などを行う。米国 Pittsburgh の FBI とも連携している。

e. 他機関との連携［Outreach to Public/Private Partners］

EU 加盟国、ENISA, Eurojust などのヨーロッパの機関、米国、オーストラリア、ニュージーランド、カナダ、Interpol などの国際的なパートナー、民間企業、研究コミュニティ、民間組織 などと連携する。インシデント発生時などに、直接やり取りができることは、スピードを要するサイバー犯罪の対応にとって重要である。

Washington、DC (US)、 UK、 リヨン (Interpol) など海外にも Europol の liaison's offices があり、シンガポールなどさらにそのネットワークを広げていく予定である。

f. 戦略・将来見通しの提供［Strategy and Forward Looking］

サイバー犯罪は日々変化するが、警察は日々の活動で対応する時間がない。そういった中

で、将来を見越した戦略（future-oriented products - 主に文書[16] [17] [18]）の提供や、早期警告を行うといった機能を果たす。

g. ヨーロッパのサイバー犯罪捜査官の中心点［Rallying Point for European Cybercrime Investigators］

ヨーロッパのサイバー犯罪捜査官たちを互いにネットワークする。

② サイバー犯罪条約について

サイバー犯罪条約が策定された 2001 年にはなかった Botnet などの新しい脅威が出てきた。それら新しい脅威に対してどう対応するかは先月の Budapest での会議で議論された。サイバー犯罪条約のアップデートの予定はなく、サイバー犯罪条約がカバーできないいくつかの点（Botnet, DDoS など）のそれぞれについて、新しい EU 指令（EU directives）をいくつか策定していく予定であり、来年（2013 年）にはそれらが出てくる。いくつかの国（Russia/China）は ITU を通じて、別のサイバー空間条約を策定しようとしている。

③ サイバーセキュリティ戦略について

EU のサイバーセキュリティ戦略が EC3, ENISA などに割り当てられ、現在ドラフトを作成中である。

④ サイバー犯罪への対抗において重要なことについて

a. スピーディな対応

いろいろな機関とのやり取りのスピードはサイバー犯罪に対抗するため重要である。迅速でないと、証拠は失われ、また被害が広がる。Liaison's office network は前にあげたように重要である。

また、現在いくつかの国では 2 年以上の調査のバックログ（積み残し）ができていて、起訴への意欲が下がっている。証拠が失われるなど捜査の妨げにもなり、起訴や裁判のスピードを確保する必要がある。

b. 情報共有の合意

情報共有の合意をできるだけ多くの国と結ぶことが重要である。北アメリカは米国、EU は Europol、それ以外の地域は Interpol がそれぞれ情報のハブとなっている。何かあった

16 iOCTA (Internet Facilitated Organized Crime) Report – 現バージョンは 2 年前のものであり、新しいものを来年夏には提供予定。現バージョン: https://www.europol.europa.eu/sites/default/files/publications/iocta_0.pdf

17 SOCTA (Serious Organized Crime Threat Assessment) – サイバー犯罪に限らないものであるが、4 年に一度 Europol が発行している。サイバー犯罪は動きが早いのでサイバー犯罪の章の中間バージョンを来週出す予定。

18 "Cyber Crime in 2020" - Internet of Things (IoT) や Smart Homes の進展に関連して、学術界、金融機関やその他の民間分野と、将来のサイバー犯罪の社会的・経済的な面からシナリオを検討している。

ときに誰に連絡するかなどの個人的なネットワークも重要である。

c. 安全なシステムの構築

サイバー犯罪が起きない安全なシステムを構築することや、よりより捜査手法・起訴のプロセスなど最初から最後まで作ることが重要であるが、起訴・裁判のスピードなどを考えると、より前のほうにフォーカスすることを考えている。

⑤ サイバーセキュリティの課題について

a. データ整備

データが分散されており、また数日でまた別のところに移動されることもあり、どの国に連絡を取ればいいかが分からないことがある。

b. デジタルな法廷証拠の開示方法の標準化

デジタルな法廷での証拠の開示方法の標準を策定しようとしているが、各国のレベルや法制度の違いがあり、コンセンサスを得るのに苦労している。

2-5 Industry, Trade & Labor Ministry / MATIMOP

(1) Industry, Trade & Labor Ministry / MATIMOP 概要と面談者

Industry, Trade & Labor Ministry は日本のほぼ経済産業省に相当する省であり、MATIMOP はイスラエルの R&D の産業センターである。

イスラエル政府 Industry, Trade & Labor Ministry の Chief Scientist Office (CSO) の Homeland Security Research Activities の代表 (Head) である Avi Shavit 氏、および MATIMOP の Business Development - Asia & South America の Executive Director である Avi Luvton 氏にインタビューした。

URL (Industry, Trade & Labor Ministry):
http://www.moital.gov.il/NR/exeres/B0B48981-357D-446F-AFAC-91A358E93C87.htm

(2) 主な意見交換内容

Avi Shavit 氏と Avi Luvton 氏との主な意見交換内容を以下に箇条書きにする。

・日本の NISC[19] にあたる組織として、イスラエルでは National Cyber Bureau がある。ここでは、政府の各部署のコーディネーションを行い、また、イスラエルが将来のリスクに対応できるように調査を実施し、政策を打ち立てている。1 年前に作られ、内閣府に所属している。首相に直接報告を行う。一方、実務を司る組織として、National Security Authority がある。National Cyber Bureau 同様、内閣府に所属し首相に直接報告を行う。こちらはサイバーセキュリティ対策に集中した組織であり、何が各官庁にとって脅威であり何を行うべきか、何が不足しているかなどを検討している。

19 National Information Security Center: 内閣官房情報セキュリティセンター

・サイバーセキュリティにおいてインフラ設備は特に重要であるが、それはシーメンスやGE のような外国企業によって作られ、メインテナンスもそれらの会社によって行われている。自らが製品を作れないという点で、セキュリティ上の脅威になりうる。ただし、ファーウェイについては、中国政府自身が国の企業と言っており、特別なケースかもしれない。
・イスラエルでは、政府が民間企業の基礎研究や R&D を補助している。経済産業省には、イノベーションや R&D を補助するための部署があり、民間企業が他の国との国際的協力を行うことを補助している。現在、R&D についての国際的な協力についての 40 あまりの契約を海外政府などと締結している。
・政府間で、相互協力についてのアンブレラ契約を締結し、その契約の基に、テーマを絞って、サイバーセキュリティなどの個別の分野で協力することがいいのではないかと考えている。他の国との契約内容の例などの資料を送るので、日本政府との橋渡しについて是非検討をお願いしたい。

2-6 National Cyber Bureau, Israel Prime Minister's Office

(1) National Cyber Bureau 概要と面談者

National Cyber Bureau は 1 年前に設立された内閣府に所属する組織である。 イスラエルの政府の各部署のコーディネーションを行い、また、イスラエルが将来のリスクに対応できるように調査を実施し、政策を打ち立てている。

National Cyber Bureau の Civilian Sector Division の代表 (Head) である Rami Efrati 氏にインタビューした。

URL (Mr. Rami Efrati): http://israelhls2012.com/Rami_Efrati.ehtml

(2) 主な意見交換内容

Rami Efrati 氏との主な意見交換内容を以下に箇条書きにする。

・3 か月前に日本を訪問し、日本政府関係では、NISC や経済産業省の人と面談した。日本はサイバー攻撃のエクセレントターゲットになりうるため、両国は協力すべきであり、情報を交換することは有益であろう。
・防衛省が、重要インストラクチャーに対する攻撃に対しても出動するようになったとの説明があったが、普段は別の官庁が監督をしているのであるとしたら実際にどのように機能するのか。重要インフラストラクチャーについては、詳細を把握しておく必要があるが、監督官庁でもない他の官庁にそれができるのであろうか。
・イスラエルでは、10 年前 (2002 年) に NISA (Israel National Security Authority)という組織を作った。これはイスラエル政府の重要インフラを守るための非常に重要な決定であった。 National Cyber Bureau の元、ここが重要インフラの監督を行い、その内容を詳細まで把握している。緊急時に助けを求められれば、すぐに駆けつけて事態の収拾にあたることが可能となっている。

・イスラエルでは、最近ではサイバーセキュリティとは言わず、サイバーディフェンスと呼んでいる。イスラエルの課題としては、民間企業が情報を政府に与えたがらないことである。個人情報について国民が敏感であり、ビジネスに影響が出うる。国の規模が小さいため、誰の事なのかすぐにわかってしまうことも影響しているかもしれない。現在官民が共同して適切な情報共有の手段を検討している。
・政府の調達において、部品のセキュリティについての規制を定めることが必要である。チェックの方法についても定める必要がある。

2-7 Nimrod Kozlovski 博士

(1) Nimrod Kozlovski 博士について

Nimrod Kozlovski 博士は、政府やハイテク企業の諮問機関などを相手にコンサルティングコンサルティングを行う一方で、ニューヨークロースクールのサイバーセキュリティ分野の非常勤講師を務めている。また、テルアビル大学でも、サイバー法や電子商取引の講義を行っている。

URL (Dr. Nimrod Kozlovski): http://israelhls2012.com/nimrod_Kozlovski.ehtml

(2) 主な意見交換内容

Nimrod Kozlovski 博士との主な意見交換内容を以下に箇条書きにする。

・イスラエルはまだサイバー犯罪条約[20]を批准していない。イスラエル国内では、プライバシーの保護を重視している。この条約を批准すると他国からプライバシーに関する情報の提供を依頼された場合に対応しなければならなくなるため、批准に反対してきた。
・民間セクターの方がイノベーションを得意としているので、サイバーセキュリティは公共セクターが民間セクターにニーズを教えて開発させる方法が良い。R&D 用の資金を与えるなど、政府が民間企業にインセンティブを与えることも重要である。
・サイバーセキュリティには、システマティックアプローチが必要である。サイバー攻撃には、ネットワークの中で長い時間をかけて分析された後に行われる場合もあり、企業はそのような攻撃に対抗しなければならない。
・インシデントが発生する前にあらゆる対抗手段を考えておくことが必要。同じ製品を同じクリティカルインフラストラクチャーに用いず、多様性を確保することも必要。
・サプライチェーンの中で、オリジナルのデザインが改ざんされるリスクがある。オリジナルデザインが保たれていることをチェックすることをスタンダード化することも有益である。
・将来のまだわからない脅威に対抗することも必要である。それには、例えば、クリティカルインストラクチャーのアブノーマルなパターンを検知することが有効であろう。ただ

20 インターネット犯罪等に関する対応を取り決めた国際条約。犯罪人の引き渡しや当該国での裁判の要求ができことや、外交ルートを通さずに法務省や警察庁などが直接相互援助の連絡をできることなどが定められている。

し、アブノーマルなパターンを感知するシステムを考えるためには、ノーマルなパターンを理解していることが必要となる。

・組織のセキュリティのコンセプトを考えるオーディターは、組織から独立したものであるべきである。

・日本のように高度のファイナンスシステムがある国に対しては、第 3 者による攻撃が効果的である。日本は、バンキングシステムやファイナンスシステムに対する攻撃に備えるべきである。

・経済規模の大きな国では、ディペンデンシー（外部依存度）をマッピングして、どこに課題があるのかを分析し対抗策を考えることが必要である

・イスラエルでは、経済や生活にとって何が重要であるかという基準で、優先順位を付けている。電力、原子力、ガス、水、銀行システム、テレコミュニケーションに関するインフラがセキュリティの重要度が高いと考えられている。

・インシデントが発生した場合に、報告先を集中させる必要がある。報告の内容をスタンダード化させて、すぐに分析できるようにするべきである。

・イスラエルでは、15 歳からサイバーセキュリティについて教育している。また、専門家を育成するために、Center of Excellence という組織に専門家チームを作り、そこで専門知識を身に着けるためのインセンティブを与えている。

・終身雇用があると、インシデントが発生しても、自分に不利になると考え報告をしなくなる傾向が強い。イスラエルでも、電力や水道のように雇用のモビリティが低い会社ではそのリスクが高くなっている。そのような会社では、例えばシステムが遅れていても変えようとしないように、現状を維持したがるという弊害も見られる。そのため、イスラエルでは 5 年ごとにシステムの見直しを行うこととしている。

3. 海外調査から示唆されること

このセクションでは今回の海外調査から示唆されることを紹介する。

3-1 サイバー攻撃の分類

サイバー攻撃は大きく (1) その影響が個人や企業など特定の関係者にとどまるものと、(2) 国防や社会秩序といった広い範囲に影響を与えるものに分類される。今回得られた示唆がそのどちらかに関連するかも示すこととする。[21]

(1) サイバー犯罪

「サイバー犯罪」とは、その影響が主にそれぞれの個人や企業など直接の関係者にとどまるサイバー攻撃である。具体的には以下のようなものがある。

・個人情報の窃取（フィッシングなど）
・金銭詐取
・企業の機密情報の窃取（産業スパイ）
・企業のウェブサイトに対する DDoS 攻撃

(2) サイバーテロ

「サイバーテロ」とは、各個人や各企業を超えて、国防や社会秩序に影響を与えるサイバー攻撃である。具体的には以下のようなものがある。

・軍事機密・政治機密・外交機密など国家機密情報の窃取・改竄
・国の防衛システムに対する攻撃
・国・政府機関などのウェブサイトに対する DDoS 攻撃
・社会の重要インフラに対する攻撃
[重要インフラ: 情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道及び物流の各分野における社会基盤]

21 サイバー攻撃は日々進化しており、また攻撃主体や攻撃手法などの特定も難しいため、正確に定義することは困難である。ただし示唆が何について行われているか分からなくなる恐れがあるため、あえてここで定義する事と致したい。

3-2 サイバーセキュリティ対策の中心となる国家組織（対サイバーテロ）

強化した NISC あるいは新しく設立する組織が、通常時からインシデント発生時まで、情報収集、リスクの評価、インシデント対応を一元的かつ連続して行い、関連省庁を指揮する。

サイバーセキュリティ対策の中心となる国家組織について、英国とイスラエルの状況は以下のようである。

・英国では GCHQ (Government Communications Headquarters: 政府通信本部)、イスラエルでは National Cyber Bureau というように、それぞれがサイバーセキュリティ対策の中心となる国家組織を有し、情報の蓄積・分析、関係省庁のコーディネーションなどを一元的に行っている。

・イスラエルでは、重要インフラに対するサイバー攻撃に備えるために、10 年前（2002 年）に NISA (National Information Security Agency) という組織が作られ、普段から重要インフラの監督を行いその内容を詳細まで把握することにより緊急時の迅速な事態の収拾を可能としている。

一方、我が国にはサイバーセキュリティに関係する各省庁を取りまとめる組織として NISC があるが、通常時およびインシデントが実際に発生した時には関係するそれぞれの省庁からインシデントが発生した民間企業に対して個別に報告が求められている。そのために、実際のインシデントが起きた際には企業の対応チームが報告に忙殺され、本来のインシデント対応に力を割けないという本末転倒なことが起こりうる。報告先を一元化し、情報がどう扱われ、どのように共有されるか（例: NDA を結んだ対象だけに、あるいは会社が分かる情報を抜いてなど）を明確にし、報告のフォーマットを標準化し、分析、情報共有を容易にするべきである。

また、我が国では防衛省が防衛省の管轄以外の重要インフラに対する保護も行う方針を検討し始めた。[22] そのこと自体は前向きに捉えられることではあるが、普段からインフラ企業と密接な情報交換、演習などを行っていなければ、インシデント発生時に突然入ってきても、現場を混乱させるだけである。[23]

特にサイバー攻撃には境界がなく (borderless)、どこからが犯罪でどこからが戦争行為かについての判断は非常に難しい。通常時からインシデント発生時まで、情報収集、リスクの評価、インシデント対応を一元的かつ連続的に行い、省庁を指揮する組織がなければ、迅速で効果的な対応を確保することは難しい。NISC が権限や人員の強化を行うか、別組織を設立し、その役割を一元的かつ連続的に果たせるようにすることが望ましい。

22 サイバー攻撃対処へ指針 - 防衛省、自衛権の発動想定 - 日経新聞 – 2012/9/7

23 3.11 の原子力発電所の事故への対応が思い起こされる。

3-3 国際連携のあり方（対サイバー犯罪、サイバーテロ）

人を継続的に他国、国際組織へ派遣し、また日本でも他国、国際組織から人を受け入れ、liaison's office network を確立し、サイバー犯罪に対する迅速な対応を可能とする。 また日本におけるサイバーセキュリティの組織・活動関連情報を英語で発信する。

境界がなく（borderless）、攻撃・変化の速さを特徴とするサイバー攻撃に対応するためには、国際的な迅速な連携が不可欠である。例えば別の国にたてられた偽のホームページをなるべく早く止め、ログなどの証拠を保全しないと、被害が広がり、また証拠が失われる。

EC3（European CyberCrime Centre, Europol）や NATO では、参加国はもちろん、それ以外の国から派遣された人々が常駐し、ひとたびことがあれば、対面での打ち合わせができるという liaison's office network がある。また、外に向けても liaison's office network を広げている。日本もこの 2012/11 にサイバー犯罪条約が発効したが、それをより有効に活用し、サイバー攻撃への迅速かつ効果的な対応を可能にするためにも、日本も liaison's office network といった仕組みを採用あるいは参加することが望ましい。

また今回の海外調査の準備のため、日本の各省庁のサイバーセキュリティ関係の組織名や活動の英語での資料を探したが、存在しなかったり、あったとしても非常にまばらで整理がされていないことが判明した。海外連携のためには英語による情報発信も必須である。

3-4 外国製インフラ製品への対応（対サイバーテロ）

インフラに外国製品を使用する際には due diligence（適切な注意）を実行する。

決してファーウェイ製品だけの問題ではなく、どんな国でも一国ですべてをまかなうことはできない。サプライチェーンがグローバル化し、製品の供給先が次々と変化し、また経済性の判断も求められる中で、外国製品や外国製の部品を含む製品をインフラに使用することは避けられない。そこで、特定の外国製品だけでなく、インフラに関わるすべての製品について due diligence を実行していくことが必要である。各企業がインフラに関わる外国製品を使用する際の due diligence に対する政府からのサポートも望まれる。具体的には以下のようなことが考えられる。

(1) 納入業者にソースコードの提供を求める

英国ブリティッシュテレコムではファーウェイの製品を使っているが、検証センターで 200 人規模のエンジニアによって製品のソースコードを英国情報局が確認しトラップや隠された部品がないことを調べることによりセキュリティを高めている。[24]

(2) 複数の業者からの製品を使う

異なる業者からの製品を使うことにより、サイバー攻撃がかなり難しくなり、また全ての

24 http://www.economist.com/node/21559929

インフラがダウンすることを避けられる。

(3) オリジナルの設計どおりのものが納入されたものかをチェックする

オリジナルの設計どおりのものが出荷されていないことや、途中のサプライチェーンで何か組み込まれるなどの可能性を考え、チェックを行う。

英国もイスラエルも自国で、例えば通信機器を作る民間企業がいないこともあり、セキュリティ上の脅威になりうることは認識しつつも、米国がファーウェイに対して行ったような規制は行わないとしている。ただしイスラエルでは「ファーウェイについては、中国政府自身が国の企業と言っており、特別なケースかもしれない。」との意見もあった。インドではファーウェイが政府に納入した通信機器に盗聴器が組み込まれていた実例がある。

3-5 人に関する課題 - 教育・人材育成（対サイバー犯罪、サイバーテロ）

サイバーセキュリティを学校教育に取り込む。サイバーセキュリティに関する Center of Excellence（CoE）を設立し、新たな脅威への研究・対応、産官学連携や海外連携を行い、日本のサイバー攻撃対応能力の向上を図る。

生活のあらゆる面に入り込んでくるという意味での borderless と変化の速さという特徴を持つサイバー攻撃に対して、主に対サイバー犯罪の面では国民全体の対応能力の底上げと、高度なサイバー犯罪・テロの両方に対して専門家の対応能力の更なる向上という二つの面から対応することが望まれる。

イスラエルでは 15 歳からサイバーセキュリティについて教育を行っている。 常時変わり続ける ICT 利用技術とサイバー攻撃に対して、一時だけの教育という意味では効果は少ないが、ICT を本格的に使い始める時期から、学校で ICT Literacy だけでなく、サイバーセキュリティを同時に教え、少なくとも使用に伴う危険があるのだと理解・意識することは一生に亘って有用であろう。

変化の早い高度なサイバー犯罪・テロのサイバー攻撃への専門的な対応能力を確保するためには、時間がかかるがしっかりした専門家の育成が必要である。Center of Excellence (CoE) を設立することが望まれる。 イスラエルは Center of Excellence に専門家チームを作り、専門家を育成している。 NATO には Tallinn, Estonia に Cyber Defense Center of Excellence があり、Europol の EC3 の実質的な役割は各国の法執行機関のための Center of Excellence である。Center of Excellence に専門人材を集中させ、新たな及び将来の脅威の研究、専門人材の育成、専門家同士の交流、外部専門人材の教育、海外との連携、などの機能を持たせることが必要であろう。 この機関を実際の執行機関と別にすることにより、大学など学術界の参加も可能になる。民間との人材の交流を行い、民間の底上げ、民間への人材提供、またセキュリティ専門家のキャリアパスの一環といった役割も果たすことができる。

3-6 法制・ガイドライン・スタンダード（対サイバー犯罪、サイバーテロ）

日本のサイバーセキュリティの向上に企業が適切に協力することができる法制・ガイドライン・標準化などを制定する。

関連法制・ガイドラインに関しては以下のように各国ごとに個人情報に対する国家関与の歴史的背景によっても考え方が異なっており、我が国もドイツ同様、戦時における国家関与が強かったことから個人情報保護が強調されることが多い。

・英国では、どちらかと言えばセキュリティを重視し、警察などの捜査の対象として、プロバイダー会社にコミュニケーションデータの内容を 2 ～ 3 年保存しておくことが検討されている。
・イスラエルでは個人情報の保護について国民が敏感であり、民間企業も政府に情報を供与することについては消極的である。
・ナチスの記憶があるドイツでは個人情報の保護が強調されている。

日本の状況も変わりつつあるが[25]、国を超えたサイバー攻撃に対する国際的な協力に資するためにも、サイバー攻撃が起きた際に過去の状況をトレースできるように、一定期間のログの保存を必要にすることが望ましい。

そして、個人情報保護情報や通信の秘密に関しても、プライバシーに対する配慮もしながら、適切な法制・ガイドラインを定め、企業が安心して適切な協力できる環境を作ることが必要である。

法制よりソフトではあるが、標準化もサイバーセキュリティに経済面から大切な役割を果たす。重要インフラで用いる通信機器などについて、Control System Security Center (CSSC) で進められているセキュリティ国際規格などのサイバーセキュリティ面を考慮した国家的な検討を進めていく必要がある。政府が水準を定めることにより、どの企業あるいは納入企業も同レベルの対策を行う必要が生じ公正な競争になるため、各会社が従うべきコンプライアンスの基準として、サイバーセキュリティについて最低限のスタンダードを定めることが必要である。日本の企業が他国で不利にならないよう、自国だけでなく国際規格にしていく戦略も同時に考えていくことも重要である。

そのほか欧州の法令に関して、得られた情報を以下に記述する。

(1) EU データ保護指令

EU データ保護指令が改定されようとしている。その現状は JEITA のレポート[26]に詳しいが、いくつかのインタビューでフィードバックをもらった。

---

25 日本でも国際的なサイバー犯罪条約に加盟するための法整備の一環で、6 月に改正刑事訴訟法が施行された。捜査機関は接続業者に 60 日間までログの保存を要請できるようになった。欧州のように一定期間保存することを義務付けるものではないが、裁判所の許可がなくても要請できる。（日経新聞 「サイバー犯罪抑止の課題は匿名化技術に規制論も」 2012/12/3）

26 EU データ保護指令改定に関する調査・分析報告書: http://www.i-ise.com/jp/report/EUdata_protection.pdf

・[SDA] EU データ保護指令の動向についてはサイバーセキュリティの動向も関連してくる。欧州議会の採決を必要とするが、6 か月以内にドイツの首相が代わることもあり、現時点ではどのようになるかはよく解らない。
・[EC3] EU データ保護指令に導入されようとしている「忘れられる権利」はログの保持などができなくなり、捜査に支障をきたす。

(2) サイバー犯罪条約

[EC3] サイバー犯罪条約が策定された 2001 年にはなかった Botnet などの新しい脅威が出てきた。それら新しい脅威に対してどう対応するかは先月（2012/10）の Budapest での会議で話されたが、 それはサイバー犯罪条約のアップデートの形ではなく（アップデートの予定はない）、 サイバー犯罪条約がカバーできないいくつかの点（Botnet, DDoS など）のそれぞれについて、新しい EU 指令（EU directives）をいくつか策定していく予定で、来年（2013 年）にはそれらが出てくる。 いくつかの国（Russia/China）は ITU を通じて、別のサイバー空間条約を策定しようとしている。

3-7 まとめ

サイバーテロ対策としては、情報収集、リスクの評価、インシデント対応を一元的に行い関連省庁を指揮する組織が必要であり、そのために NISC の強化が必要。また、インフラに外国製品を使用する際の due diligence 実施の強化も望まれる。 サイバーテロとサイバー犯罪に共通の対策としては、人的交流を含めた国際的連携の強化や、教育・人材育成の強化、および法制・ガイドラインの制定が必要である。

以上

4. 資料編（詳細面談記録）

4-1 IISS (International Institute for Strategic Studies)

面談日時	2012.11.7 10:00 - 11:40
面談先	IISS (International Institute for Strategic Studies)
面談者	先方: Mr. Negel Inkster Director of Transnational Threats and Political Risk 当方: 益岡、石野
面談テーマ	日本と英国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) IISS 概要と面談者

核抑止や軍備管理を目的に、1958 年に英国で設立された独立系シンクタンク。世界平和の維持や安全保障のための健全な政策の採択と良好な国際関係を推進することを使命とし、世界の安全保障、政治的リスク、軍事紛争を主な研究テーマとする。現在、ロンドン以外にも、ワシントン D.C.、シンガポール、マナマ、バハレーンに事務所を開設している。

Director of Transnational Threats and Political Risk である Negel Inkster 氏にインタビューをした。Negel Inkster 氏との主な意見交換内容を以下に記述する。

URL (IISS): http://www.iiss.org/

(2) 日本のサイバーセキュリティの状況について

持参した説明資料に基づいて日本のサイバーセキュリティの状況について説明した。先方コメントは以下のようであった。

・いろいろな業界に話を聞くことは重要である。
・日本企業で、取締役会がサイバーセキュリティを重視していることが印象的である。英国企業の水準はとても低い。英国では、サイバーセキュリティはテクニカルなものであり引退した警察官が行うものであるとの認識がまだ残っており、取締役会は、場合によっては、ビジネスを止めてしまう脅威となるとは認識していない。欧州でも、セキュリティは費用がかかる厄介なものであるとの認識が強い。短期間に収益などの実績を求められる企業がサイバーセキュリティにお金をかけない傾向があるが、情報を盗まれてより安価なものを作られ、会社がつぶれる可能性があることを考えなければならない。[27]

27 米国の太陽電池メーカーが、中国企業にサイバー空間から企業情報を盗まれ、安価な類似製品を輸出されたことにより倒産してしまった実例もある。

(3) 英国におけるサイバーセキュリティの現状について

・英国は、2 年前にセキュリティレビューを行い、サイバーセキュリティ対策として 4 年間で 650 万ポンドの予算を新たに確保した。
・サイバーセキュリティ対策は、GCHQ (Government Communications Headquarters：政府通信本部) が中心に行っている。米国の NSA (National Security Agency：アメリカ国家安全保障局) ともパートナーシップ協約を結んで協力している。NSA の Echelon のシステムがダウンした際に、GCHQ が代わって 2，3 日にわたりカバーしたこともある。
・何かあった時に相談できる組織を政府内に設け、政府と民間企業間の情報交換も行っている。

(4) 意見交換

① プライバシーとナショナルセキュリティの問題について

・ポストで怪しいものが発見されたら爆発することができるように、Botnet で悪いものが見つかったら届け出を行わせるような制度も必要であろう。
・どのようなデータを政府に提出するのかについての基準を法律でしっかり定めて、個人や企業が自分で判断することは避けるべきである。
・英国では、警察が後で調査できるように、プロバイダー業者に対して、コミュニケーションデータを 1～3 年間保存しておくことを義務付けることを検討している。
・個人情報の保護は、政策的意思 (Political Will) の問題であろう。日本やドイツでは第 2 次大戦時代の経験から、個人情報を保護する傾向にある。

② 中国製品に対する規制について

・英国では、米国がファーウェイに対して行ったような規制は行わない。当社に対して中国政府の資金が入っていることは知っているが、英国は自国に通信製品の製造会社がなく、他国製品を使う必要がある。
・例えば、英国のブリティッシュテレコムでも、ファーウェイから製品を購入している。すべての製品のソースコードを英国情報局が確認し、トラップや隠された部品外ないことを調べている。検証センターを中国に作り、200 人規模のエンジニアを送っている。
・米国がファーウェイを排除するのは政治的な問題であろう。米国は、他国の製品が市場を独占することや、他国が技術を盗むことを好まない。他国の技術を盗んで発展することは一つの過程である。例えばブラジルのラバープラントからゴムの木を盗むことにより、マレーシアでゴムのプランテーションが行われた。

③ サイバーセキュリティの規制について

・各会社が従うべきコンプライアンスの基準として、サイバーセキュリティについて最低限のスタンダードを定めることが必要である。政府が水準を定めることにより、どの会社も同レベルの対策を行う必要が生じ公正な競争になる。(セキュリティレベルを下げるこ

とにより価格競争力を強化することが行えなくなる）
・英国では、将来の技術革新の変化に対応できる柔軟性を持った法制を作ることを検討している。どうやってフレキシブルでコンプリヘンシブな規制を作るのかが課題となっている。
・技術の向上により、政治決定を超えることも可能となってきた。人々は直接コミュニケートすることができるようになり、中国ですら情報を 100%規制することは無難しくなっている。
・現在はある意味でアナーキー状態である。政府によるトップダウン的なアプローチが必要な場面もある。

④ キャリアパスについて
・英国では、GCHQ が新聞広告により特殊技術を保有した者を勧誘することも行っている。
・教育分野において、7 つの大学では、経営者向け COE コースでサイバーセキュリティを教義として教えている。

⑤ ビッグデータについて
・ビッグデータを多種の方法で組み合わせることにより人物の特定も可能となる。例えば、監視カメラのデータと携帯電話と実際の観察データを組み合わせることにより、テロリストの候補者を事前に特定することが可能となる。なお、英国では、すでに車のナンバープレートを監視して渋滞税を課すシステムが存在している。
・ラスベガスのゲーム会社は、人のつながり（ゲームを行っている際のディーラーと参加者の関係など）を分析することにより、ディーラーが顧客と組んで悪事を行うことを感知するシステムを開発しており、英国もそのようなシステムの開発を検討している。

⑥ 今後の CIPPS との協働について
・IISS は、シンガポールやバハレーンにも事務所を置いている。課題は資金である。何らかの収益があれば協力できる。
・IISS が日本のカウンターパーティを探している場合には、CIPPS も協力する意向を伝えた。

以上

4-2 SDA (Security & Defence Agenda)

面談日時	2012.11.8 15:40 - 17:00
面談先	SDA (Security & Defence Agenda)
面談者	先方: Mr. Andrea Ghianda, Project Manager 当方: 田中理事長、益岡、石野
面談テーマ	日本と欧州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) SDA 概要と面談者

NATO と EU 間をつなぐ組織として、2002 年に設立された。両組織の軍備や安全保障の専門家に話し合いを行う場を提供している。また、軍備や安全保障に関するフォーラムの開催や調査レポートの発行なども行っている。

当初はハード軍備を主なテーマとしていたが、総合的なアプローチが必要となってきており、ここ 2，3 年はサイバーセキュリティもテーマとしている。近々プライバシーとセキュリティに関するレポートを発行する予定である。

Cyber Security の Project Manager である Andrea Ghianda 氏にインタビューをした。Andrea Ghianda 氏との主な意見交換内容を以下に記述する。

URL (SDA): http://www.securitydefenceagenda.org/

(2) 日本のサイバーセキュリティの状況について

持参した説明資料に基づいて日本のサイバーセキュリティの状況について説明した。やり取りは以下のようであった。

先方:

・国際的な協力について日本はどのように対応しているのか。

益岡:

・民間部門では、日本の企業も CERT のメンバーになっている。
・公共部門はサイバークライムコンベンションに参加している。防衛省は米国と協力しており、共同演習も企画している。
・サイバーセキュリティについてのアジア諸国との協力において、日本がリードしようとしている。

(3) 欧州におけるサイバーセキュリティの現状について

・欧州では、One Stop Shop の機能を持つ European CyberCrime Centre (EC3) をこの 1 月に設立する予定である。ここにサイバー攻撃などの情報を集め、サイバー犯罪に対するストラテジーを決めていく。

・欧州経済をデジタル導入によって改善しようという動きがある。
・公共と民間の間の関係を築くことが重要視されている。民間がネットワークインフラを保有していることから、両者の協力が必要となる。また、政府だけでなく民間企業も自分を守る必要がある。

(4) 意見交換

① クラウドコンピューティングの課題について
企業の情報が他国に置かれることから以下 2 つの課題が発生する。
1. 情報に対する統治の問題
2. 情報を集めているところを守る手段の問題

② スマートグリッドコントロールにおける課題について
ホームランドセキュリティに関しては、(1) ENIZA や (2) DHS がレポートを出しているので参考にするとよい。関連する情報を後で送る。

③ EU Data Protection Directive の動向について
・これには、サイバーセキュリティの動向も関連してくる。
・欧州議会の採決を必要とするが、6 か月以内にドイツの首相が代わることもあり、現時点ではどのようになるかはよく解らない。

④ 今後の CIPPS との協働について
・情報交換から開始するのが良い。
・SDA が発行している“Europe's World”を通して、CIPPS のレポートを欧州地域に出すことも可能である。

以上

4-3 NATO (North Atlantic Treaty Organization)

面談日時	2012.11.8 17:40 - 19:00
面談先	NATO (North Atlantic Treaty Organization)
面談者	先方: Dr. Jamie Shea Deputy Assistant Secretary General for Emerging Security Challenges 当方: 田中理事長、益岡、石野
面談テーマ	日本と欧州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) NATO Emerging Security Challenges 概要と面談者

NATO に Added Value を行うことを推進しており、以下の 2 つのポリシーを有している。

1. 危機に備え、危機において NATO に選択肢を与える。
2. 予算の効率的な運用を考える。例えば様々なユニットの機能を多角的に用いて効率性を高めることなど。

現在以下 6 つのトピックスがある。

1. サイバーセキュリティ
2. エネルギーセキュリティ
3. カウンターテロリズム
4. 情報交換
5. 核政策
6. 科学の活用：新たな脅威への対抗についての科学的なリサーチ

NATO Emerging Security Challenges の Deputy Assistant Secretary General である Jamie Shea 博士にインタビューした。Jamie Shea 博士との主な意見交換内容を以下に記述する。

URL (NATO Organization): http://www.nato.int/cps/en/natolive/structure.htm

(2) 日本のサイバーセキュリティの状況について

持参した説明資料に基づいて日本のサイバーセキュリティの状況について当方より説明した。先方からのコメントは以下のようであった。

・省庁間や官民間で協力が不足しているのは、欧州でも米国でも同じ状況である。
・NATO は加盟国 28 か国のうち 23 か国と了解覚書 (MoUs) を交わした。 各国に責任者を置きそこに情報が集中するようにしている。 CERT とも協力している。
・企業はインシデントが起きたことをレポートしたがらない。インフォーマルな情報交換が重要である。民間との情報交換については、クライシスの場合にだけ情報交換する仕組みを検討している。
・米国では、サイバー攻撃に対抗するために工業製品の水準を定めようとしている。英国で

も同様の動きがある。

(3) NATO におけるサイバーセキュリティ対策について

NATO におけるサイバーセキュリティ対策についての先方からの説明を以下に箇条書きにする。

・2006 年に、コンピューター関連のセンターをブリュッセルの南 50Km ほどの場所に設立した。
・NATO のネットワークを守ることを目的としていた。
・人員は 100 名から開始した。現在増強中であり、2013 年からフルオペレーションケイパビリティを持つようになる。
・サイバープロテクション政策を作り、加盟国及び 7 つのパートナー国と協力している。センサーを向上させ、おとりの攻撃と本当の攻撃を区別する技術の開発など技術力の向上が課題となっている。 NATO は NATO Computer Incident Response Capability (CIRC) の為に 58 百万ユーロの予算を確保した。
・サイバーセキュリティについては 2 チーム編成している。加盟国をサポートする必要がある。
・情報局が持ってくる情報を分析するため、CTAC: Cyber Threat Assessment Center も設立された。
・また、エストニアに Cyber Defense Center of Excellence を置き、サイバー攻撃に対する訓練やアカデミックディスカッションを行っている。エストニアが 2007 年にサイバー攻撃を受けたためにここに設置された。毎年、実際に担当者のコンピューターをサイバー攻撃で止めてしまうなど、実践に近い形の訓練を行っている。
・NATO のシステムについても毎年テストを行っている。
・NATO は、24 か国のパートナー国のデータを保有しているが、これらを保護するためにコモンスタンダードを必要としている。

(4) 意見交換

① サイバー攻撃を他の軍事的な脅威と同様に扱うのか

NATO は、サイバー攻撃も集団安全保障を適用する脅威に含まれると解している。レッドラインもはっきり定めていない。

サイバー攻撃への対抗攻撃については以下のような課題がある。

a. サイバー攻撃の潜在性

サイバー攻撃は、気付かないうちに長期間かけて行われる場合があるが、被害を受けてから対抗攻撃を行うまでの時間が長いとその正当性がなくなる。(殴られてから 1 年後に殴り返すようなものである)

b. 同盟国の合意形成

エストニアのように 1 国のみが狙われる場合には、他国には波及しないため、同盟国に対抗攻撃を行うことを納得させるのが困難である。

c. 被害

人が死なないのに攻撃をすることは難しい。

d. 政治的な課題

NATO には 28 か国も加盟しているが、各国で認識も異なっている。どのレベルで問題を国から NATO に上げるか、NATO がどうやって同盟国を守るべきかなどについて定める必要がある。

② サイバー攻撃の定義について

・どのようなサイバー攻撃があり、どのような法律が適用されるのかを定めた、「タリン・マニュアル」がもうすぐ公表されるのでそれを参考にするとよい。
・インシデントの種類には以下の 3 つがあると考えている。
1. 相手のレピュテーションを下げようとするもの
2. 政府の情報を盗もうとするもの
3. 大規模な DDoS 攻撃

③ サイバーセキュリティの課題について

a. 本当の攻撃の見極め

サイバー攻撃の情報については雑音が入るのでこれを取り除き、本当の攻撃とそうでない攻撃を区別する必要がある。そのためのシステムセンサーを開発中である。

b. 民間企業の利用

・以前は公共のコンピューターの方が民間のものより性能が良かったが、今は逆である。どの程度の仕事を民間に移行し、どこまでを民間企業の責任とするのかが課題（challenge）である。
・公共もクラウドを使い始めているが、民間セクターに移したデータを民間が本当に守りきることができるのか検討する必要がある。
・実際に、NATO では、ほとんどのマルウェアについて、民間企業のシマンテックが対応している。
・民間企業が保有する社会インフラに対して攻撃が行われた場合に、だれが責任を負うのかも課題である。
・NATO 加盟国の全てのスタンダードをそろえることは困難で、民間企業も興味を示さない点がある。

c. 人の教育について

サイバーセキュリティでは一番の弱点は人である。 人々は、手続きの順守について緩いところがある。人のトレーニングが必要である。

d. 外国製品の利用について

・外国製品の利用については、セキュリティを最初から考えなければならない。米軍の武器のマイクロチップが汚染されていたという事例がある。
・サプライヤーへの信頼があることが必要で、その意味では製品には十分防御が行われていないものがあることも問題である。
・サプライヤーにとっても信頼性のない製品を供給したら訴追される恐れがある。
・製造業者との間に信頼関係を築くことが必要で、それがセキュリティを保証する。保証はどうやって築くのかということについては、いつでも監視できることだと考える。厨房で作られた料理を食するのではなく、すし屋のように目の前で作られた料理を食するということである。

④ その他

日本とはインテリジェンスシェアリング契約がない。これがあれば情報交換ができる。そのような契約が早期に締結出来ることを期待する。

以上

4-4 EC3 (European CyberCrime Centre)

面談日時	2012.11.9 13:00 - 16:00
面談先	EC3 (European CyberCrime Centre), Europol, the Hague, Netherlands
面談者	先方: Deputy Director, Operations Department Designated Head and Representatives of Strategy and Outreach 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ついての意見交換

(1) European CyberCrime Centre (EC3) 概要と面談者

EC3 の概要は以下のようである。

- オランダ ハーグに、Europol の中の組織として 2013/1/1 に開設予定。
- 2011 年の Feasibility Study から始まった。
- 最終的な予算は 2012/12 に欧州議会の議決を経て決定する。
- Mandate (任務) としては Online Fraud, Child Sexual Exploitation, Cyber-attacks against critical infrastructure がある。 最初の二つは conventional な取り組みが功を奏しており、 3 番目にフォーカスしていく。

EC3 の Operations Department の Deputy Director および Strategy and Outreach の Designated Head とそのメンバーにインタビューをした。 彼らとの主な意見交換内容を以下に記述する。

URL (EC3): https://www.europol.europa.eu/ec3

(2) EC3 の詳細

EC3 の組織は EC3 Management のもと、Data Fusion, Operations, R&D Training, Strategy/Outreach/Crime Prevention の 4 つからなる。

EU の 27 の加盟国それぞれサイバー犯罪 に対する能力レベル、国内の法制度 (どのように犯罪捜査、起訴していくか) などが異なることがあり、それが EC3 のあり方を規定する一つの要因であるようだ。EC3 の主な機能 (core functions) は以下のようなものとなる

1. Information Hub on Cybercrime
2. Capacity Building (Law Enforcement, Prosecutors, Judges)
3. Operational Support
4. Forensic Support (Research & Development)
5. Outreach to Public/Private Partners
6. Strategy and Forward Looking
7. Rallying Point for European Cybercrime Investigators

以下に EC3 の 7 つの主な機能 (core functions) に関してそれぞれ記述する。

・**[Information Hub on Cybercrime]** Public, private sectors, academia（学術界）からの operational data を集めて共有する
・**[Capacity Building (Law Enforcement, Prosecutors, Judges)]** まず誰がどこでサイバー犯罪と戦っているのかをまとめる。 また警察だけでなく、prosecutors（検察官）や judges（裁判官）の教育も進めていく。 Prosecutors/judges がサイバー犯罪を分かっていないと、せっかく捜査・逮捕しても、その先に時間がかかってしまい、民間は民事での解決を進めたりし、証拠が失われるなど、捜査の妨げになったりしてしまう。
・**[Operational Support]** Intelligence 提供が中心である。 証拠収集（HDD の解析）のサポートなどはするが、実際の証拠収集や裁判で証言することは（全くではないが基本的に）ない。
・**[Forensic Support (Research & Development)]** 学術界、産業界、各国警察などと研究や open-source のツールの作成などをしている。 Internet で virtual に進めている部分もあるが、EC3 に物理的にも部屋を用意して、Face-to-Face で活動できる環境も用意している。 米国 Pittsburgh の FBI とも連携している。
・**[Outreach to Public/Private Partners]** EU 加盟国、ENISA, Eurojust などのヨーロッパの機関、米国、オーストラリア、ニュージーランド、カナダ、Interpol などの国際的なパートナー、民間分野などと連携している。（Europol のレベルの概念だが）Liaison's Office Network があり、EU の各国はもちろん、US, Interpol などの liaison's offices が Europol の中にあり、何かあれば歩いてオフィスに行きやり取りができるのは、スピードを要するサイバー犯罪の対応に重要である。 また Washington, DC (US), UK, Lyon (Interpol) など Europol 外に Europol の liaison's offices があり、Singapore などさらにそのネットワークを広げていく予定である。
・**[Strategy and Forward Looking]** サイバー犯罪は日々変わっていくが、警察は日々の活動で対応する時間がない。 そういった中で、 future-oriented products（主に文書）の提供や早期の警告（early warning）をあげるといった機能を果たしていく。 具体的には以下のようなものを提供、提供予定である。
  ・iOCTA (Internet Facilitated Organized Crime) Report – 現バージョン[28] は 2 年前のものであるが、新しいものを来年夏には提供予定。
  ・SOCTA (Serious Organized Crime Threat Assessment) – サイバー犯罪に限らないものであるが、4 年に一度 Europol が発行している。 サイバー犯罪は動きが早いのでサイバー犯罪の章の中間バージョンを来週出す予定。
  ・"Cyber Crime in 2020" – Internet of Things (IoT) や Smart Homes の進展に関連して、学術界、金融機関やその他の民間分野と、将来のサイバー犯罪の社会的・経済的な面からシナリオを検討している。

28 https://www.europol.europa.eu/sites/default/files/publications/iocta_0.pdf

・**[Rallying Point for European Cybercrime Investigators]** ヨーロッパのサイバー犯罪捜査官を互いにネットワークする。

(3) 意見交換

その他の話題・質問などについて以下に記述する。

・**[EC3 はサイバー犯罪情報をレポートする single point of contact か?]** そうではないが、各機関の構造的な情報共有を推進していく。(もし企業が一国内にあれば、報告先はその国の警察になる。)

・**[Budapest Cybercrime Convention]** サイバー犯罪条約が策定された 2001 年にはなかった Botnet などの新しい脅威が出てきた。 それら新しい脅威に対してどう対応するかは先月の Budapest での会議で話されたが、それはサイバー犯罪条約のアップデートの形ではなく(アップデートの予定はない)、 サイバー犯罪条約がカバーできないいくつかの点(Botnet, DDoS など)のそれぞれについて、新しい EU 指令(EU directives)をいくつか策定していく予定で、来年(2013 年)にはそれらが出てくる。 いくつかの国(Russia/China)は ITU を通じて、別のサイバー空間条約を策定しようとしている。

・**[EU Cyber Security Strategy]** EU のサイバーセキュリティ戦略が EC3, ENISA などに割り当てられ、現在ドラフトを書いている。

・**[やり取りのスピード]** いろいろな機関とのやり取りのスピードはサイバー犯罪に対抗するため重要である。 迅速でないと、証拠は失われ、また被害が広がる。 Liaison's office network は前にあげたように重要である。 また情報共有の合意をできるだけ多くの国と結ぶことが重要である。 合意がない国とは多少 creative になることが必要である。 ただ人権問題のある国(死刑になりうるなど)は、情報ごとにリスクを評価して判断している。北アメリカは米国、EU は Europol、それ以外の地域は Interpol がそれぞれ情報のハブとなっている。 何かあったときに誰に連絡するかなどの個人的なネットワークも重要である。

・**[Challenge – Cloud]** データが分散されていて、また数日でまた別のところに行ったりし、どの国に連絡を取ればいいかが分からない。 また startup 企業で 2 人くらいでやっているところで、compliance/law enforcement offices もないようなところもあり、難しい。

・**[End-to-End]** サイバー犯罪が起きない安全なシステムを構築すること、よりより捜査手法、よりよい起訴のプロセスなど最初から最後まで作ることが重要であるが、起訴・裁判のスピードなどを考えると、より前のほうにフォーカスすることを考えている。

・**[起訴・裁判のスピード]** 現在多くのケースと大量のデータでいくつかの国では 2 年以上の調査のバックログ(積み残し)ができていて、起訴への motivation が下がっている。その他にも prosecutors/judges のサイバー犯罪の理解が低いことも、時間がかかることにつながり、民間企業は民事での解決(botnet を止めるなど)を進めたりし、証拠が失われるなど、捜査の妨げになったりしてしまう。

・**[Standards for Presentation of Digital Forensic Evidences]** デジタルな法廷での証拠の

開示方法の標準を策定しようとしているが、各国のレベルや法制度の違いがあり、コンセンサスを得るのに苦労している。

以上

4-5 Israel Industry, Trade & Labor Ministry / MATIMOP

面談日時	2012.11.12 11:00 - 12:00
面談先	Israel Industry, Trade & Labor Ministry・Israeli Industry Center For R&D
面談者	先方: Mr. Avi Shavit, Former Head of Homeland Security, Consultant of The Chief Scientist for Israeli Industry Center For R&D, Industry, Trade & Labor Ministry Mr. Avi Luvton, Executive Director for Business Development – Asia & South America, MATIMOP - Israeli Industry Center For R&D 当方: 益岡、石野
面談テーマ	日本とイスラエル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) Industry, Trade & Labor Ministry / MATIMOP 概要と面談者

Industry, Trade & Labor Ministry は日本のほぼ経済産業省に相当する省であり、 MATIMOP はイスラエルの R&D の産業センター である。

イスラエル政府 Industry, Trade & Labor Ministry の Chief Scientist Office (CSO) の Homeland Security Research Activities の代表 (Head) である Avi Shavit 氏、および MATIMOP の Business Development - Asia & South America の Executive Director である Avi Luvton 氏にインタビューした。Avi Shavit 氏と Avi Luvton 氏との主な意見交換内容を以下に記述する。

URL (Industry, Trade & Labor Ministry):
http://www.moital.gov.il/NR/exeres/B0B48981-357D-446F-AFAC-91A358E93C87.htm

(2) 日本のサイバーセキュリティの状況について

持参した説明資料に基づいて日本のサイバーセキュリティの状況について説明した。

(3) イスラエルにおけるサイバーセキュリティの現状について

・日本の NISC にあたる組織として、イスラエルでは、National Cyber Bureau がある。これは 1 年前に作られたもので内閣府に所属し、首相に直接報告を行う。2 年間の検討ののちに設立されたものである。初年度に 25M 米ドルの予算が付けられた。
・ここでは、政府の各部署のコーディネーションを行っている。また、イスラエルが将来のリスクに対応できるように調査を実施し、政策を打ち立てている。
・実務をつかさどる組織として、National Security Authority がある。Cyber Bureau 同様に内閣府に所属し、首相に直接報告を行う。サイバーセキュリティ対策に集中した組織であり、何が各官庁にとって脅威であり何を行うべきか、何が不足しているかなどを検討し

ている。

・最近、工業セクターにおけるサイバーセキュリティに関するイノベーションテクノロジーの研究を行うために、2012 年と 2013 年の 2 年間で 20M 米ドルの予算が付けられた。

(4) 意見交換

① 中国製品に対する規制について

・イスラエルも外国製品を輸入している。各国ともすべてを自分で作ることはできない

・サイバーセキュリティにおいてインフラ設備は特に重要であるが、それはシーメンスや GE のような外国企業によって作られ、メインテナンスもそれらの会社によって行われている。自らが製品を作れないという点で、セキュリティ上の脅威になりうる。

・ファーウェイについては、中国政府自身が国の企業と言っており、これは特別なケースかもしれない。中国に関しては、2011 年 4 月に、中国政府が、全世界のインターネットデータを 15 分間にわたり自国を通させたということもあった。

② 民間企業の支援について

・イスラエルでは、政府が民間企業の基礎研究や R&D を補助している。R&D においては、主に、基礎研究でなく実業に結びついた研究にお金を付けている。

・経済産業省には、イノベーションや R&D を補助するための部署がある。ここでは民間企業が他の国との国際的協力を行うことを補助している。現在、R&D についての国際的な協力についての 40 あまりの契約を海外政府などと締結している。

・MATIMOP はアジア地区のそのための組織である。最近、日本の経済産業省とコンタクトしようとしたがうまくいかなかった。日本の組織とのコンタクトを CIPPS が仲介をしてくれると助かる。

・政府間で、相互協力についてのアンブレラ契約を締結し、その契約の基に、テーマを絞って、サイバーセキュリティなどの個別の分野で協力することがいいのではないかと考えている。

→日本で実業に携わっているのは経済産業省と総務省である。

・他の国との契約内容の例などの資料を送るので、是非検討をお願いしたい。

→日本政府が動くのには時間がかかることを理解しておいて欲しい。

③ 今後の CIPPS との協働について

・米国のイニシアティブによる、サイバーセキュリティに関する World Economy Forum がある。G8 に関係するものと思うが、ここではタスクフォースが作られている。来月ダブリンでミーティングがあり、そののち米国のワシントンでもミーティングがある。その重要メンバーを知っているので、紹介する。

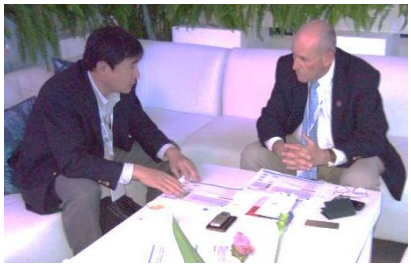
以上

4-6 National Cyber Bureau, Israel Prime Minister's Office

面談日時	2012.11.13 11:00 - 12:00
面談先	National Cyber Bureau, Israel Prime Minister's Office
面談者	先方: Mr. Rami Efrati, Head of Civilian Sector Division 当方: 益岡、石野
面談テーマ	日本とイスラエル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) National Cyber Bureau 概要と面談者

National Cyber Bureau の概要は以下のようである。



・内閣府直属のサイバーセキュリティのための機関として、1 年前に設立された。
・政府の各部署のコーディネーションや、サイバーセキュリティに関する調査、政策立案などを行っている。

National Cyber Bureau の Civilian Sector Division の代表 (Head) である Rami Efrati 氏にインタビューした。 Rami Efrati 氏との主な意見交換内容を以下に記述する。

URL (Mr. Rami Efrati): http://israelhls2012.com/Rami_Efrati.ehtml

(2) 日本のサイバーセキュリティの状況について

持参した説明資料に基づいて日本のサイバーセキュリティの状況について説明した。先方のコメントは以下のようであった。

・3 か月前に日本を訪問し、日本政府関係では、NISC や経済産業省の人と面談した。日本はサイバー攻撃のエクセレントターゲットになりうるため、両国は協力すべきと考える。なお、私が National Cyber Bureau の Head になってから海外の国を訪問したのは日本が初めてであり、それだけ日本にとってサイバーセキュリティが重要なものと認識している。
・防衛省が、重要インストラクチャーに対する攻撃に対しても出動するようになったとの説明があったが、普段は別の官庁が監督をしているのであるとしたら実際にどのように機能するのか。重要インフラストラクチャーについては、詳細を把握しておく必要があるが、監督官庁でもない他の官庁にそれができるのであろうか。
・イスラエルでは、10 年前 (2002 年) に NISA (Israel National Security Authority) という組織を作った。これはイスラエル政府の重要インフラを守るための非常に重要な決定であった。 National Cyber Bureau の元、ここが重要インフラの監督を行い、その内容を詳細まで把握している。緊急時に助けを求められれば、すぐに駆けつけて事態の収拾にあたることが可能となっている。
・イスラエルも日本もお互いにサイバーセキュリティについての知識を有しており、それ

を共有することは良いことである。サイバーセキュリティについては、お互い共通の利益がある。
・サイバーセキュリティについての R&D に対して政府が補助金を出していることは良いことである。

(3) イスラエルにおけるサイバーセキュリティの現状について
・イスラエルでは、最近ではサイバーセキュリティとは言わず、サイバーディフェンスと呼んでいる。「イスラエルディフェンス」という雑誌に、イスラエルの課題：どのようなサイバーディフェンスが望ましいかについて記事を書いたのでその定義などについて参考にしてほしい。
・イスラエルの課題としては、民間企業が情報を政府に与えたがらないことである。個人情報について国民が敏感であり、ビジネスに影響が出うる。国の規模が小さいため、誰の事なのかすぐにわかってしまうことも影響しているかもしれない。現在官民が共同して適切な情報共有の手段を検討している。

(4) 意見交換

① サプライチェーンに対する規制について
・政府の調達において、部品のセキュリティについての規制を定めることが必要である。チェックの方法についても定める必要がある。

② リサーチセンターについて
・イスラエルに、IBM やシスコなどがリサーチセンターを作って研究を行っている。
・日本の企業にも是非そのような研究センターをここに作って欲しい。例えば 2 年前からここでは自動車に対するサイバーアタックについての研究を行っている。トヨタのような自動車メーカーがここで自動車に対するサイバーアタックについてテーマを絞って研究することも有益である。

③ 今後の CIPPS との協働について
・このミーティングのサマリーを送ってほしい。また、サイバーセキュリティ犯罪に関する日本の法律の英訳があったら送ってほしい。
・LAC のようなサイバーセキュリティに携わっている会社の情報を教えてほしい。
・サイバーセキュリティについて・政府の調達において、部品のセキュリティについての規制を定めることが必要である。チェックの方法についても定める必要がある。参考になる文献としては、OECD のレポートや、アメリカの NIST の下のスペシャルチームによるレポートを推奨したい。

以上

4-7 Nimrod Kozlovski 博士

面談日時	2012.11.13 17:40 - 19:00
面談先	Nimrod Kozlovski 博士
面談者	先方: Nimrod Kozlovski 博士 当方: 益岡、石野
面談テーマ	日本とイスラエル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) Nimrod Kozlovski 博士について

Nimrod Kozlovski 博士の略歴は以下のようである。

・イェール大学で法学博士の資格を取得した後、同大学のコンピューターサイエンス部門で研究に従事。

・その後、コンサルタントとして独立し、インドなどの政府や、ハイテク企業の諮問機関などを顧客としている。

・現在、コンサルティング業を行う一方で、ニューヨークロースクールのサイバーセキュリティ分野の非常勤講師を務めている。また、テルアビル大学でも、サイバー法や電子商取引の講義を行っている。

URL (Dr. Nimrod Kozlovski): http://israelhls2012.com/nimrod_Kozlovski.ehtml

(2) 日本のサイバーセキュリティの状況について

持参した説明資料に基づいて日本のサイバーセキュリティの状況について説明した。

① 先方のコメント

・イスラエルはまだサイバー犯罪条約を批准していない。イスラエル国内ではプライバシーの保護を重視しており、この条約を批准すると他国からプライバシーに関する情報の提供を依頼された場合に対応しなければならなくなるため、批准に反対してきた。

・イスラエルでも、サイバーセキュリティに関係する官庁が多すぎるという声がある。

(3) 意見交換

① 官民連携について

a. イノベーションのための官民の協力について

・民間セクターの方がイノベーションを得意としているので、公共セクターが民間セクターにニーズを教えて開発させる方法が良い。

・R&D 用の資金を与えるなど、政府が民間企業にインセンティブを与えることも重要である。

b. 民間企業から国への報告について

・民間企業は国に情報を渡したがらない。

民間企業に情報を報告させる方法として 2 種類がある。

A) 規制による方法（カリフォルニア方式）

B) 国による分析による方法。インドのように、国が企業のリスクを分析して、そのリスクに対してレポートを提出させるやり方

② サイバーセキュリティの在り方について

a. システマティクアプローチの必要性

・サイバーセキュリティには、システマティックアプローチが必要である。

・サイバー攻撃には、ネットワークの中で長い時間をかけて分析された後に行われる場合もあり、企業はそのような攻撃に対抗しなければならない。

b. リダンダンシーの確保

・インシデントが発生する前にあらゆる対抗手段を考えておくことが必要。

・同じ製品を同じクリティカルインフラストラクチャーに用いず、多様性を確保することも必要。

c. サプライチェーンの課題

・サプライチェーンの中で、オリジナルのデザインが改ざんされるリスクがある。オリジナルデザインが保たれているチェックを標準的に行うことが有益である。

d. 未確認の脅威への対抗

・将来のまだわからない脅威に対抗することも必要である。

・それには、例えば、クリティカルインストラクチャーのアブノーマルなパターンを検知することが有効であろう。ただし、アブノーマルなパターンを感知するシステムを考えるためには、ノーマルなパターンを理解していることが必要となる。

e. 独立したオーディターによる監督

・組織のセキュリティのコンセプトを考えるオーディターは、組織から独立したものであるべきである。

・オーディターと監査される会社は切り離されるべきである。イスラエルでは、オーディターを派遣する組織がある。会社はお金をそこに払うが、オーディターを誰にするか要求することはできない仕組みになっている。

・かつて、インドの内閣府に対するコンサルティング業務として、インドのセキュリティシステムのアウトラインを考えたことがあるが、その時にオーディターを独立したものとすることをアドバイスした。

③ 日本のサイバーセキュリティに対する示唆

a. バンキングシステムやファイナンスシステムの防御

・日本のように高度のファイナンスシステムがある国に対しては、第 3 者による攻撃が効果的である。日本は、バンキングシステムやファイナンスシステムに対する攻撃に備えるべきである。

b. 外部依存度（ディペンデンシー）の分析

・経済規模の大きな国では、ディペンデンシーをマッピングして、どこに課題があるのかを分析し対抗策を考えることが必要である

・例えば、イスラエルでは、鉄道のシグナルシステムで、RSA 暗号のキーを盗まれる事故が発生したが、その際、バンキングシステムや軍のシステムが全て同じものに依存していたことが判明し問題になったことがある。

c. 優先順位を考える

・イスラエルでは、経済や生活にとって何が重要であるかという基準で、優先順位を付けている。電力、原子力、ガス、水、銀行システム、テレコミュニケーションに関するインフラがセキュリティの重要度が高いと考えられている。

d. 報告先の一元化

・インシデントが発生した場合に、報告先を集中させる必要がある。

・報告の内容をスタンダード化させて、すぐに分析できるようにするべきである。

e. セキュリティに関する教育

・イスラエルでは、15 歳からサイバーセキュリティについて教育している。

・専門家を育成するために、Center of Excellence という組織に専門家チームを作り、そこで専門知識を身に着けるためのインセンティブを与えている。

f. 雇用の流動性が低い会社で注意すべきこと

・日本のようにライフタイムで雇用される社会では、インシデントが発生しても、自分に不利になると考え報告をしなくなる傾向が強い。イスラエルでも、発電や水道のように雇用のモビリティが低い会社ではそのリスクが高くなっている。

・そのような社会では、例えばシステムが遅れていても変えようとしないように、現状を維持したがるという弊害も見られる。そのため、イスラエルでは 5 年ごとにシステムの見直しを行うこととしている。

以上