参考資料６－１

サイバーセキュリティタスクフォース（第５回）議事要旨

1. 日 時：平成 29 年 5 月 31 日（水）10:00～12:00

2. 場 所：中央合同庁舎２号館８階 第１特別会議室

3. 出席者：

【構成員】

鵜飼構成員、岡村構成員、小山構成員、園田構成員、戸川構成員、徳田構成員、中尾構成員、名和構成員、

林構成員、藤本構成員、安田構成員、吉岡構成員

【オブザーバー】

村上企画官(内閣サイバーセキュリティセンター)、土屋企画官(経済産業省)、井上研究室長(情報通信研究機構 サイバーセキュリティ研究室)

【総務省】

今林政策統括官（情報通信担当)、谷脇情報通信国際戦略局長、吉岡官房審議官、上原サイバーセキュリティ・情報化審議官、吉田情報通信国際戦略局参事官、小笠原情報通信政策課長、今川情報流通振興課長、大森参事官（サイバーセキュリティ戦略担当）、酒井情報セキュリティ対策室調査官、荻原電気通信技術システム課長、湯本消費者行政第二課長、藤田地上放送課長、玉田衛星・地域放送課長、道方情報セキュリティ対策室課長補佐

4. 配布資料

資料５－１ 諸外国のサイバーセキュリティ政策について（事務局）

資料５－２ NICT におけるサイバーセキュリティ研究開発の取組について（NICT）

資料５－３ ナショナルサイバートレーニングセンターにおけるセキュリティ人材育成の取組について（園田構成員）

資料５－４ サイバーセキュリティの研究開発及び人材育成について（鵜飼構成員）

資料５－５ 研究開発・人材育成の方向性（案）について（事務局）

参考資料５－１ サイバーセキュリティタスクフォース（第４回）議事要旨（事務局）

参考資料５－２ サイバーセキュリティ研究開発戦略骨子について

参考資料５－３ 「サイバーセキュリティ人材育成プログラム」の全体概要

5. 議事概要

(1) 開会

(2) 議事

事務局より、資料５－５「情報共有・国際連携の論点（案）について」を説明 (省略)

◆　**構成員の意見・コメント**

林構成員)

よいと思います。

中尾構成員)

よくまとめられている。

情報共有について、何をどのようにして共有するのかについての情報が必要。

また、情報共有の自動化および匿名化についても報告書に記載していただきたい。

事務局)

検討する。

徳田構成員)

英国大使館から、サイバーセキュリティ分野で日本と共同研究をしたいというプログラムがありました。PhD レベルでの研究交流や、英国の研究拠点において共同研究を行うというものでありました。インド、イスラエルにも同様に声をかけていました。

岡村構成員)

各国の CERT が連携してインシデント対応を行うということも必要ではないか。その際にカウンターパートとなる各国の組織が、省庁ごとに縦割りになっているので、そのあたりの整理が必要ではないか。

中尾構成員)

諸外国のサイバーセキュリティ政策の比較表の項目は 3 つでよいか？ 研究開発も必要ではないか？

調査対象国については、フランス、ドイツには、英国とは異なる点があるので、これらの国もあった方がよい。

小山構成員)

各国のサイバーセキュリティ政策について、脅威としてどのようなものを想定しているか等の背景情報があった方がよい。

安田座長)

国家のサイバーセキュリティとの関連では、全省庁にサイバーセキュリティ・情報化推進審議官が配置されることになっているが、重要インフラの中に、国家のサイバーセキュリティは入っているのか？

事務局)

概念としては入っていない。

岡村構成員)

法律に関して、英国のみプライバシー法(Privacy Act) が記載されていて、EU がデータ保護法(GDPR) ではなくＮＩＳ指令となっているので、統一感があるように項目として合わせた方がよいのではないか。全ての国にプライバシー法に関する情報を追加するか、英国のプライバシー法に関する情報を削除する。

安田座長)

いつ頃完成するか？

事務局)

できるだけ早く完成させる。

資料５－１　を説明 (省略)

資料５－２　を説明 (省略)

資料５－３　を説明 (省略)

資料５－４　を説明 (省略)

◆　構成員の意見・コメント

安田座長)

どう進めるべきか、意見をいただきたい。

岡村構成員)

先日開催された白浜シンポジウムで、サイバーセキュリティ技術のコンテストがあった。優勝したのは、木更津高専のチームであった。

どのチームもアプリケーションレイヤの問題は解けるが、その下のレイヤになると苦戦しているようであった。

アプリケーションのような上位レイヤに重点を置いた教育がされてきた結果なのかどうかわからないが、教育の内容を見直す必要はないのか？

また、セキュリティ技術には強いが、人的セキュリティ、組織的セキュリティ、物理セキュリティ等、マネジメント分野が弱いようにみえる。特定の分野のみを得意とする人材が多いのではないか。

広い視野でセキュリティを身につけることができるような形での教育・人材育成が必要ではないか。

園田構成員)

大学においては、教員が少ないという問題がある。

教員の個人的な知識・スキルによりカリキュラムが作成されている。

講義で教える内容にサイエンスとしての広さがないことも問題である。

優れた能力を有する人を可視化するために CTF を実施しているが、上位になるチームには、コンピュータサイエンスを専攻しているメンバーを有するチームが多い。

サイバーセキュリティ分野において、教育機関が行うべきことが何であるかを検討する必要がある。

事務局)

国として作成したサイバーセキュリティ関連のカリキュラムとして、NICT の CYDER がある。

他省庁との連携や問題意識の共有を通じて、サイバーセキュリティ教育のあり方について検討を行う。

吉岡構成員)

実践的な演習を実施したいと考えているが、そのための環境がない。

また、大学のさまざまな業務に時間と労力をとられてしまい、演習にまで手が回らない。

他の組織へ拡張させることができるような方法には、実施する意義があると考える。

安田座長)

(1) は実施する。(2) についてはどうするか。

中尾構成員)

海外における活動・取り組みと比較して日本に不足しているところは何か。実践的な演習により、不足しているところをカバーできるかというと、そうではない。

たとえば、米国や EU において、航空システムを開発する際に Security by Design が導入されている。Security by Design においては、どのような脅威があるか・どのような脆弱性があるかを明確化し、セキュリティ要件を決定した上で、組織的対策・技術的対策・人的対策を検討するという、一連の作業を行う必要があるが、このような全体の流れを設計・運用することができる人がいない。

林構成員)

橋渡し人材について、職位としては、General Councelor : 法務・総務・企画担当になるが、海外においてどのような状況であるのかについて調査する価値はある。

ただし、電力業界にみられるように、企画担当者が、規制を遵守しながらいかにビジネスを展開するかということに注力しているようなケースについては、橋渡し人材とはいえない。

インテリジェンス分野では、英国の状況が気になっている。英国には、GCHQ - NCSC というインテリジェンス機関・サイバーセキュリティ機関があり、伝統的にインテリジェンス活動に強みがある。インテリジェンス活動に関する法律について、英国と米国で違いがあるのか。

名和構成員)

研究開発・人材育成について、不足している理由を明らかにしない限り対策の検討はできないのではないか。

産学連携については、サイバーセキュリティ分野においては、経験を通じて得られることの共有が重要である。

NICT が実施しているサイバー演習の結果をフィードバックするといったことが考えられる。

安田座長)

リスクテイクする主体が少ないという点について、先のロンドンオリンピックで、British Telecom がセキュリティ確保のための各種活動を行ったと言われているが、実際のところは、GCHQ の指示に従って実施したというのが実態である。

リスクテイクする人材の育成についてはどのような方法が考えられるか。

鵜飼構成員)

ビジネスを興す前に、どのようなリスクがあるのかを理解しておくことが必要ではないか。

私が会社を立ち上げた時と同時期に設立されたライバル企業の多くが倒産しているが、それらの企業は、倒産すべくして倒産したという印象である。

事務局)

長期でどのように投資を回収するのか、資金を誰が負担するのか。推進主体が民間企業なのか大学なのかといったことについて、政府が全体的な戦略を作成することは難しい。

米国は、軍事とサイバーセキュリティとの関連が深いので、民間企業のビジネスとして成立し易いという側面がある。

日本において、不足しているものが何であるか、どのような方向を目指すべきか、どのような制度が必要かといった点について、ご意見をいただきたいと考えている。

鵜飼構成員)

5-5 (3) NICT の役割について、研究成果はあるが、成果を普及させるための出口戦略が不足しているのではないか。

普及させるためには、他人任せにするのではなく、自ら普及させるための活動をしなければならない。

製品を販売し、ユーザを増やすというのが、ビジネスとしてのオーソドックスな流れ・方法である。そのためには、売るための仕組みを考える必要があるが、代理店に丸投げしてもダメで、自ら販売することが必要。特に技術者は、製品化してから先の作業はやりたくないかもしれないが、やらなければならない。

製品化してから先のフェーズに対して、政府による支援があるとよいのではないか。また、政府機関において製品を導入するということも検討していただきたい。

徳田構成員)

NICT が開発した VoiceTra という音声翻訳アプリがある。企業との協業により、製品化された。ソフトウェアなので、ハードウェアに比べて製品化し易いということがあったのかもしれない。

人材育成について、文部科学省の IT 人材育成拠点の参加者を Silicon Valley に行かせた結果、参加者のキャリアパスについての意識が大きく変わったという例を目にした。どのような仕事にパッションを傾けるのかということは、産業連携やサイバー演習ではわからない。仕事やキャリアについての気付きを促すための環境を用意することが重要である。

NICT 井上氏)

NICT の成果を普及させるための活動を行っているが、政府機関に導入してもらうのが難しい。技術的に枯れた製品でないと採用してもらえない。たとえば、国が開発した技術と学術機関の人材とを組み合わせることにより、いかにしてシナジーを生みだすかというような、セキュリティの Eco System をどのようにして確立するかということが課題ではないか。

藤本構成員)

セキュリティの専門的な人材を育成する活動は増えてきたが、日本ではそのような人材が活動できる場が少ないのではないか。

セキュリティの専門人材が活躍できるようにするためには、専門外の人材との意思疎通・コミュニケーションが大切である。大学において、ICT に関連する学部でセキュリティ等を学習する機会は増えているように思うが、それ以外の学部でも、セキュリティやリスク管理の基礎的な学習をする機会を増やすとよいのではないか。

戸川構成員)

大学の情報系の学部の学生の多くは、情報セキュリティに興味を持っている。

情報セキュリティを取り巻く状況や議論の状況を発信することにより、情報セキュリティに興味を持つ人を増やすのはよいことであると考える。

座学で、コンピュータサイエンスを含む ICT の基礎を教えることは重要である。

学生に活躍できる場を見せることも重要ではないか。

研究開発については、NICT の協力を得ながら推進するのがよいのではないか。

小山構成員)

NTT コミュニケーションズにおいても人材育成を行っている。人材不足の根源的な原因は、IT 業務をアウトソースすることにあるのではないか。企業はサイバーセキュリティに関する業務を内製化するべきであるということをメッセージとして発信してはどうか。

内製化することにより、外部委託費用よりも社員の給料の方が安いので、コストを削減することができる、人海戦術が求められる業務を内製化することにより、自社のコンピテンシーの源泉である、より高度な業務に専念することができるようになり、産業競争力の向上が期待できるというようなメリットが期待できる。

研究開発については、現場を理解せずに研究開発を行っているという印象があるが、本当のところを教えると倫理的な問題が発生するのではないかという不安がある。研究倫理を確保しながら、研究開発が円滑に実施できるような情報共有の仕組みが必要。

安田座長)

産学官連携において、NICT 以外に、たとえば NISC の役割にはどのようなものがあるかということや、国の研究所、システムに関することについても入れた方がよいのではないか。

村上企画官)

よいと思います。

中尾構成員)

国際連携の仕方にはいくつかある。ICT ISAC の取り組み方も国によって異なる。

研究と産業をどのように結びつけるのかということについても検討が必要ではないか。

安田座長)

それを今から検討しようということである。一番弱いのは、リスクテイクする主体が少ないという点であるが、これについては、産学官の連携を促進するしかないのではないか。

徳田構成員)

研究と産業をどのようにしてつなぐか。

課題 (3) は、サイバーセキュリティ以外の分野に拡張してもよいのではないか。

NIST でスマートシティを担当している人に話を聞いたことがあるが、国が中立的な立場を維持しながら、特定の企業・組織とアライアンスすることができるということである。

安田座長)

次回以降、少しずつまとめたい。

事務局）

次回は、6 月に開催させていただく予定です。