参考資料７－１

サイバーセキュリティタスクフォース（第６回）議事要旨

1. 日 時：平成 29 年 6 月 29 日（木）13:00～15:00

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】

岡村構成員、小山構成員、園田構成員、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】

芦田参事官補佐(内閣サイバーセキュリティセンター)、小柳課長補佐(経済産業省)、伊藤公祐(重要生活機器連携セキュリティ協議会)

【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、大森参事官（サイバーセキュリティ戦略担当）、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、山田情報セキュリティ対策室課長補佐、杉浦電気通信技術システム課課長補佐、酒井情報セキュリティ対策室調査官

4. 配布資料

資料 ６－１ これまでの議論と今後の検討の方向性（案）について（事務局）

資料 ６－２ CCDS の取組紹介（CCDS）

資料 ６－３ サイバーセキュリティ リスクマネジメントの観点から （藤本構成員）

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（事務局）

5. 議事概要

(1) 開会

(2) 議事

事務局より、資料６－１「これまでの議論と今後の検討の方向性（案）について」を説明 (省略)

伊藤オブザーバより、資料６－２「CCDS の取組紹介」を説明 (省略)

藤本構成員より、資料６－３「サイバーセキュリティ リスクマネジメントの観点から 」を説明 (省略)

◆　構成員の意見・コメント

安田座長)

林構成員から、本タスクフォースに関連する項目についての調査報告書についてお知らせがあるということです。

林構成員)

情報共有について、英国における状況を調査し、『英国 IPA(Investigatory Powers Act) 2016 に関する調査報告書』としてまとめた。情報セキュリティ大学院大学のウェブサイトで公開している。

岡村構成員)

資料６－１に優遇税制導入についての記述を入れて欲しい。

また、自動車に搭載されているソフトウェアの更新タイミングの問題等に対処する上で、従来の ISO にはなかった、Safety の概念が必要になってきているので、目標として、CIA に加えて Safety を入れていただきたい。将来は、一般的な製品と同様に重要製品にはリコールの仕組みを導入することを検討するべきである。

資料６－１について、たとえば、スマートメータに使用されているプロセッサは、大手メーカーが製造するものに統一されている。プロセッサの技術が、海外の企業に渡った場合のセキュリティは、サイバーセキュリティから、国家セキュリティの問題になる。社会的に受容可能なものと、放置できないものとの区分が必要ではないか。

医療の分野においては、臨床研究法等に、個人情報保護を含むサイバーセキュリティに関する項目が記載されるようになっている。何が問題なのかについての理解が追いつかないような速さで、法律等の整備が進んでいる。Informed Consent に関連する問題もある。

他の分野においても、通信の秘密や金融に特有の問題がある。ベースを固めておいて、分野ごとに特有の問題について検討を行うという方法が有効ではないか。

事務局) 優遇税制策を含め、政策を検討する。

藤本構成員)

誰が検討に参加するのかを含め、継続的に議論できるようにすることが重要である。

総務省 酒井調査官)

資料６－１ P3 に米国との連携について記載している。データの自動処理を可能とするためのデータフォーマットは、IoT デバイスのセキュリティ対策においても必要と考えている。ICT-ISAC と共同で検討を行う。

先日、中尾構成員とともに米国の National Council of ISAC と DHS を訪問し、意見交換を行った。National Council of ISAC とは、正式なパートナーとして活動することで合意した。また、DHS から、サイバーセキュリティ分野においてサポートを得られることとなった。

中尾構成員)

米国の ISAC が何をしているのかについて、理解を深めることができた。情報共有については、AIS で自動化している。国内で情報共有の自動化を実施する上で、プロファイルとポリシーについての議論が必要である。また、有用な情報が何であるか、どのようなデータが必要であるのかについても検討が必要である。

名和構成員)

資料６－２ P12 において、Safety と Security の区分による規格・標準が記載されている。電力制御システムセキュリティガイドラインや鉄道・航空領域のサイバーセキュリティに係る手引等は、機能安全を意識したものとなっている。これらのガイドラインと、本資料に記載されているガイドラインとの関係について整理がされているとよいのではないか。

資料６－３に関連して、Fake News を対象とするリスク管理は行われているのか？

藤本構成員)

Fake News はリスク管理の対象外ではないが、誰が何のためにそのリスク管理を行うのかという視点が必要である。近年話題になっている Fake News が、情報の使い方として新しいものであると考えると、さまざまな組織やプロジェクトで、そのリスク管理について議論することは重要だと思う。

名和構成員)

米国では、Google 等が、Fake News 対策を検討するためのコンソーシアムを結成している。国内において議論が少ないと感じている。

中尾構成員)

リスク管理について、認識を合わせておきたい。リスク管理とは、リスクをどのように扱うのかに関する方法論である。リスク管理において、Fake News は脅威に分類される。Fake News によってどのような影響(Impact)があるのかについて分析を行う必要がある。リスク分析の際には、Risk Factor についても考慮する。影響(Impact)は、News の内容や個々の企業によって変わってくる。

岡村構成員)

Fake News については、主要なマスメディアや有識者による議論がされている。Fake News の目的にはさまざまなものがある。現時点では、自主的な研究がされているという状況である。

林構成員)

情報の作成主体と発信主体とが分断されているという点が問題である。情報の正確性を担保するためには、情報の品質管理を行わなければならない。

中尾構成員)

資料６－１について、米国においては、収集した情報を Semi Automatic に匿名化している。情報共有においては、収集した情報をそのままリリースしてよいのか、あるいは、匿名化を行う必要があるのかということと、研究開発や運用に関する視点も記載していただきたい。

安田座長)

匿名化技術の研究開発について、次回もう一度議論したい。

林構成員)

自動的に情報共有を行う場合、IP Address の共有をどのように扱うべきなのか。EU-US Privacy Shield の枠組の元ではどのようなことに注意する必要があるのか。情報共有を自動化した場合、適用される要件が変わってくるのではないか。

名和構成員)

他国と情報共有を行っているが、データ量としては一日に数百 MB になることあり、手分けして分析及び国内展開を行っている。

最近の「信頼関係の高い主体間の情報共有」の仕組みは、非常多くの未加工のデータ（Raw Data）が格納された DB やレポジトリに対してクエリ（問い合わせ）を行うというものである。それぞれの関心事項に基づくデータを検索して取り出すためのクエリ構文を多重化することにより、検索結果の精度が向上する。共有するのは、そのクエリ構文のみである。データには、参照する権限を有するユーザを識別するためのタグが付与されており、検索者の権限により出力可否が自動的に決まる仕組みである。

中尾構成員)

データの種別に応じて、閲覧可能な人を自動的に振り分けるには、データに付与されるタグとデータ利用ポリシーとが連携している必要がある。

安田座長)

資料６－２で、モバイルデータについては書かれていないのか。GPS により、誰がどこにいるのかのデータが簡単に利用できるようになっている。

伊藤オブザーバ)

クラウドサービスの情報管理はスコープ外である。野良 IoT 対策や、不正アクセス・不正侵入を防止するための対策にフォーカスしている。

安田座長)

個人情報保護についてはどうか。

伊藤オブザーバ)

プライバシー保護については、端末レベルでは実施している。

吉岡構成員)

企業間の情報共有を促進したり、そのための匿名化手法を検討するというアプローチは重要であるが、データが集まるようなサービスプラットフォームをどのように構築するか、という観点の議論も重要。Google や Microsoft 等のサービスプロバイダが構築しているプラットフォームには、大量の情報が集まっており個々の企業の情報共有の努力だけでは、太刀打ちできない。IoT では、まだサービス形態が多様かつ流動的であるので、情報の集まる魅力的なプラットフォームを構築することができる可能性がある。

研究倫理という点では、ハニーポットを使用したマルウェアの収集など、倫理面で注意が必要な研究を行う際のガイドラインがあるとよいが、ガイドラインの内容については、議論が必要と考える。

事務局)

IoT サービスという視点は考えられる。研究倫理については、リバースエンジニアリング等の問題も含め、法的に規制するのか、ガイドラインで対処するのかということを検討する必要がある。

安田座長)

倫理的には難しい面があり、やってみないとわからない。米国には司法取引のような制度がある。法務省に検討してもらうことはできないか？

総務省 酒井調査官)

著作権におけるフェアユースのように、例外的な扱いを考える必要はある。NISC を中心として進める必要がある。脆弱性の解析については、壁にぶつかる場合がある。GPS については、位置情報との関係を考えなければならない。

安田座長)

たとえば、NICT のトレーニングセンターにおいて、外部に出してはならない情報を誤って出してしまうリスクがある。

谷脇局長)

ガイドラインで対処可能な問題か、法規制が必要かということは慎重に検討しなければならない。成長戦略 2017 に、規制のサンドボックス(Regulatory Sandbox)についての記載がある。このような試行的な取り組みを経て、ガイドラインで対処するのか、法規制するのかを決めるという選択肢もある。制度設計においては、効果の見える化も重要なポイントである。

小山構成員)

資料６－１の情報共有について、米国においては、STIX、AIS 等の枠組に基づいて実施されているということであるが、議論だけが先行している状況で見切り発車すると、意図した通りに情報が流れない恐れがある。どのような情報であれば共有できるのかということを確認するために、シミュレーションを実施する必要があるのではないか。STIX には大量の管理項目があり、実装の仕方によっては、情報共有ができない可能性がある。

藤本構成員)

情報の所有者が、まったく知らない間に自分の情報が使用されていたというようなことがないように、できるだけのことはしなければならない。

名和構成員)

当初、外国の公的機関が提供する情報共有ポータルサイトのアカウントを保有している日本人は相当数いたが、最終的に私一人になった。情報の提供を受けるばかりで、有用な情報を相手に提供できない、或いは人事異動でアカウントが消失したためである。継続的に情報共有コミュニティのメンバーでいることは難しい。

中尾構成員)

ICT-ISAC として、米国に情報提供を行う。現時点では、トライアルで相互に接続するというステータスである。官民の情報共有においても試行してみるということが重要である。

小山構成員)

タスクフォースにおける取り組みということで、トライアルを提案した。

安田座長)

法律による支援、情報提供時の匿名化等、安心して情報提供できるような仕組みが必要である。米国においてどのような方法で行われているのかについての事例が多く欲しい。

林構成員)

共通の利益があることと、相互の信頼関係が重要なのではないか。日本における、サイバー犯罪に関する産学官連携・国際連携のための取り組みとして、JC3(Japan Cybercrime Control Center：日本サイバー犯罪対策センター)がある。米国の取り組みをモデルとして構築されたものであるが、うまくいっている。

名和構成員)

他国との情報共有を成功させるためには、アナログな手段による信頼関係の醸成が必要であり、他国と定期的なやり取り（Keep in contact）することが重要である。

園田構成員)

CCDS のガイドラインについて、IPA の『つながる世界の開発指針』のように、具体的なコードにまで踏み込んだ記述が必要ではないか。

伊藤オブザーバ)

実装に関する内容は必要であると考えている。分野別に踏み込んでいけるとよいと考えている。

園田構成員)

人材育成とも関係するので、検討していただきたい。

安田座長)

資料６－２ P11 に記載されているチェックリストは、定量的評価には使用できないのか。

伊藤オブザーバ)

IPA が付属文書として公開しているもので、最低限のチェック項目である。

安田座長)

組み込みソフトウェアのチェックについては、どのように行うのか。

伊藤オブザーバ)

全て、組み込み機器を意識したものとなっている。アプリケーションをセキュアにするための対策を記載したもので、実装のガイドラインにはなっていない。

中尾構成員)

IoT 分野における人材育成や国際連携について、タスクフォースがフォーカスするのはどこなのか。IoT コンソーシアムの IoT セキュリティガイドラインを、ISO/IEC SC 27 において標準化しようとしている。Safety についての議論もされている。サイバーセキュリティの中での Safety という位置づけ。IoT においては、人への影響が想定されるので、Safety の観点が必要である。タスクフォースとしての方針を明確化する必要がある。

総務省 酒井調査官)

タスクフォースという場において、いろいろ議論していただきたい。

安田座長)

資料６－２ P7 (4) 安全・安心について、安全は工学により、安心は工学 + 心理学により実現される。Safety は機能安全なので、セキュリティだけでは、安心までは到達していないのではないか。

伊藤オブザーバ)

2020 年までに到達するということを想定している。製造業においては機能安全が重視されるため、セキュリティがあまり考慮されていなかった。現状において、セキュリティチェックポイントがないので、手順の中に、セキュリティに関する内容を追加したい。(4) は、スローガン的な意味もある。

藤本構成員)

Safety については、ISO/IEC Guide 51 もある。こういった国際標準の動向もチェックしておく必要がある。

安田座長)

IoT においては、プロセッサとソフトウェア両方のセキュリティを考える必要がある。ソフトウェアのセキュリティだけというのは、ガイドラインの対象ではない？

伊藤オブザーバ)

ソフトウェアのバグについては、チェックされていることを前提としている。

安田座長)

プロセッサのセキュリティだけではなく、ソフトウェアのセキュリティについても対象にしなければならないのではないか。提言を作成する時に、もう一度相談させていただきたい。