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

1. 日 時：平成 29 年 5 月 15 日（月）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、園田構成員、戸川構成員、中尾構成員、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)

【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、山田情報セキュリティ対策室課長補佐

4. 配布資料

資料４－１ 中尾構成員資料 情報共有及び国際連携

資料４－２ 林構成員資料 サイバーセキュリティのための情報共有に関する米国と EU の法制比較

資料４－３ 林構成員資料 英国 IPA（Investigatory Powers Act）2016 に関する調査結果

資料４－４ 事務局資料 情報共有・国際連携の論点（案）について

参考資料４ー１ 第 3 回タスクフォース議事要旨

5. 議事概要

(1) 開会

(2) 議事

- 中尾構成員より、資料４－１「情報共有及び国際連携」を説明 (省略)
- 林構成員より、資料４－２「サイバーセキュリティのための情報共有に関する米国と EU の法制比較」を説明 (省略)
- 林構成員より、資料４－３「英国 IPA（Investigatory Powers Act）2016 に関する調査結果」を説明 (省略)
- 事務局より、資料４－４「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

安田座長)

官民での情報共有を活発なものとするにはどうすればよいか。

国のサポートが必要なのか？必要だとすれば、どのようなサポートが考えられるか？

園田構成員)

いろいろ考えられるが、利用者保護という観点で考えると、情報共有の主要な目的の一つは、共有される情報を活用して迅速に対策を行うことにより、利用者保護につなげることである。

現状では、情報共有を通じた利用者保護は難しい課題であるが、その理由の一つとして、攻撃の解析のスピードが遅いことが挙げられる。

攻撃コードに対して、通常の解析プロセスによる解析を行っていたのでは、時間がかかる。

攻撃の解析スピードを上げるためには、より具体的な情報の共有が必要である。

戸川構成員)

情報共有を推進するためには、日本だけに閉じていては駄目である。

サイバー攻撃の対象は、IoT 機器だけではなく、ソフトウェア、海外から持ち込まれる携帯機器等、多種多様である。

誰とどの情報を共有するのか、開示できる情報／開示できない情報の区別をどのようにするのかということについて、

明確に規定する必要がある。

論点案の (1) ①～③ について、より詳細な観点での議論が必要である。

吉岡構成員)

情報共有を検討するにあたって、複数のシナリオ、立場が考えられる。

我々は、大学の研究機関として、サイバー攻撃の観測を行っており、IoT に対する攻撃を観測するために、ハニーポットを運用している。

観測により得られたデータの共有について、大学内部での情報共有であれば、それ程コストはかからないが、外部との情報共有にはコストがかかる。

外部との情報共有は、研究費で賄っているわけではないので、持ち出しになっている。

米国では、DHS の Predict というプロジェクトがあり(現在は、Impact という名称になっている)、データを提供する側に対するサポートも組み込まれていた。

データを提供する側のサポートについては、このような事例が参考になるのではないか。

また、情報の精度・確からしさについても検討が必要である。

最近では、マルウェアに関する情報共有を悪用して、プローブ用の検体が組み込まれるケースが確認されている。

これにより、攻撃側にどのような情報が共有されているのかが漏えいする可能性がある。

Counterintelligence の観点で、情報の精査が必要である。

中尾構成員)

米国においては、ICT ISAC や、NCCIC(National Cybersecurity and Communications Integration Center) による AIS(Automated Indicator Sharing) 等の取り組みにおいて、収集した情報を Index 化して配布するということが行われている。

このプロセスは、全て自動化することはできないが、自動化できる部分については自動化するという方針で推進されている。

情報の収集においては、企業、研究・教育機関、政府が協力することが必要である。

検討課題として、運用費を誰が負担するのか、匿名化処理をどのように行うか、誰と誰が情報を共有するのかといったものがある。

日本の ICT ISAC は、課題を解決しながら進めるというステップにあるが、ICT ISAC の前身である Telecom ISAC において、10 年間検討して解決に至らなかった課題があるので、今回の検討でも解決が困難な課題があると想定している。

共有されるデータの価値は、データの受信者ごとに異なる。たとえば、マルウェアに関する情報は、企業のビジネスモデルによって活用のされ方が異なる。

情報共有に関する全体的なフレームワークの開発については米国が進んでいるので、国際連携については、米国を巻き込んで検討する必要がある。

林構成員)

インディケータの深刻度については、共通の尺度を決めることが難しい。

試行錯誤しながら検討する米国の進め方はよいと考える。

藤本構成員)

日本においては、“顔見知り”の企業の間での情報共有が多い。この背景には、知っている人だけを信頼するという、古くからの日本の文化があるのかも知れないが、国際連携を行う上では、知らない人・組織との間で安全・安心な情報共有を行うための制度設計が必要である。制度による信頼性の担保を行う手法を進化させる必要がある。

安田座長)

資料 4-4 について、国際動向に関する記述がない。米国、英国がどのような方向に向かっているのか、それに対して、日本はどのようにしたいのか。国家としての方針の根拠となる法律が規定されていないと、海外との議論で勝てない。

情報収集については、企業に対して、積極的に提供するように要求する必要があるが、企業の側からすると、政府に情報提供することに対して、不安がある。

そのような企業の懸念を払拭する意味でも、情報提供に関する国としての方針を決定し、その方針に従って、企業が情報提供を行うようにする必要がある。

その点、米国は明確であり、国家のために情報を提供して欲しいということを方針として掲げている。

日本においては、国家に情報を提供することに対する不安が大きいため、何か圧力がかかるとやめてしまうというケースが多い。企業が安心して情報を提供することができるシステムが必要である。

グローバルな情報が入ってくるようにするために、企業としてどのようにするべきかということや、国としてここまではやるということを明確に決める必要がある。

また、情報の提供にあたっては、匿名化を行うようにしてもらいたい。

林構成員)

二つの点について明確化することが必要であると考える。

一つは、従来の PC ベースのネットワークを対象とするのか、IoT ネットワークを対象とするのか。

もう一つは、Attribution まで考慮するのか、それとも、臨床的に対応するのか。

後者については、攻撃に関する Attribution を究明することはコストがかかるので、米国と連携して推進するのがよいと考える。

中尾構成員)

議論の方向が IoT にフォーカスする傾向にあるが、依然として、PC やインターネットの脆弱性も残存していることについても考慮が必要である。

Attribution については、FBI は、攻撃の発生源を追跡する技術の高度化を推進している。その際に、関連する情報の利用も行っている。

情報提供に際して、情報のプライバシーを保護することも必要である。

Command & Control の情報については、Botnet の構成等が時間の経過とともに変化するので、ある時点のみの情報を収集することに意味があるのかという疑問がある。

意味がある情報とするためには、情報の分析が必要である。

鵜飼構成員)

セキュリティベンダの役割という観点で考えた場合、企業として取り組むためのスキームが必要。

情報の収集・提供にはコストがかかるので、対外的に情報共有を行うことが求められるのであれば、コスト面での支援を行ってほしい。

どのような情報が求められるのかということを明確化した上で進める予定である。

安田座長)

国のサポートについてはどのように考えるのか。

今林政策統括官）

事実を積み重ねることにより、他国に追いつくということが前提にある。

情報の信頼性をどのようにして担保するのか。

インテリジェンスには、HUMINT(Human intelligence)、SIGINT(signals intelligence)があるが、最終的には、人間によるインテリジェンス活動である HUMINT がキーとなると考えており、制度による信頼性の担保だけでなく、人間関係に基づく信頼性という観点についても検討を行いたい。

国としての方向性を出すことについては、検討する。皆さまには、ここを重点的に行うべきであるということを指摘していただきたい。

プライバシーとセキュリティの両立については、論点を整理した上で方向性を出したいと考えているが、国からの一方的な指示や、コスト面でのサポートだけでは実現することは難しいと考えている。

企業がどのような要望を持っているのか、実現に際しての障害要因は何か、どのようなインセンティブが必要か、実現に向けてどのような取り組みが必要かといったことについて整理を行う。

安田座長)

資料４－２ の表に英国の情報があるとよい。海外においては、そこまで進んでいるということを示す必要がある。

米国、英国、EU、日本が横並びで比較できるようになっているとよい。

今林政策統括官）

比較できる表としてまとめる。

安田座長)

次回は、方針について議論したい。

構成員の皆さまには、実現に向けた具体的な方法について考えておいていただきたい。

事務局）

次回は、5/31 10:00 ～ 12:00 に開催させていただく。