参考資料１

サイバーセキュリティ戦略本部
研究開発戦略専門調査会
第８回会合　議事概要

1. 日時
平成 30 年 6 月 11 日（月） 13:30～15:30

2. 場所
中央合同庁舎 4 号館全省庁共用 1214 特別会議室

3. 出席者（敬称略）

| | | |
|---|---|---|
| （会長） | 後藤 滋樹 | 早稲田大学理工学術院 教授 |
| （委員） | 上野 裕子 | 三菱 UFJ リサーチ&コンサルティング株式会社<br>政策研究事業本部 経済政策部 主任研究員 |
| | 鵜飼 裕司 | 株式会社 FFRI 代表取締役社長 |
| | 小山 覚 | NTT コミュニケーションズ株式会社<br>情報セキュリティ部 部長 |
| | 佐古 和恵 | 日本電気株式会社 セキュリティ研究所<br>特別技術主幹 |
| | 戸川 望 | 早稲田大学理工学術院 教授 |
| | 奈良 由美子 | 放送大学 教授 |
| | 名和 利男 | 株式会社サイバーディフェンス研究所<br>専務理事／上級分析官 |

（外部発表者） 後藤 厚宏　内閣府 SIP 「重要インフラ等におけるサイバーセキュリティの確保」 プログラムディレクター

| | | |
|---|---|---|
| （事務局） | 中島 明彦 | 内閣サイバーセキュリティセンター長 |
| | 桑原 振一郎 | 内閣審議官 |
| | 三角 育生 | 内閣審議官 |
| | 山内 智生 | 内閣参事官 |
| | 吉田 恭子 | 内閣参事官 |
| | 結城 則尚 | 企画官 |
| | 山下 浩司 | 参事官補佐 |
| | 篠田 陽一 | サイバーセキュリティ補佐官 |
| | 中尾 康二 | サイバーセキュリティ補佐官 |

（オブザーバー） 内閣府科技
警察庁
総務省

文部科学省
経済産業省
防衛省

4．議事概要

○次期サイバーセキュリティ戦略について

資料 4 に沿って、事務局より説明。

○安全な IoT システムの検討に関する今後の進め方について

資料 5 に沿って、事務局より説明。

○有識者によるプレゼンテーション

資料 6 に沿って、戸川委員より発表。続いて資料 7 に沿って、内閣府 SIP・後藤厚宏プログラムディレクターより発表。全ての議題に関する委員から意見の概要は以下のとおり。

○（上野委員）

サイバーセキュリティ技術を開発する際には、常に社会実装を念頭に置くことが重要である。具体的には、誰がどのようにその技術を活用するのか、コストの規模や負担者も考えて促進、推進していくことが必要と考える。

SIP のプロジェクトにおいて、社会実装の部分のどこまでを SIP が担当し、どこまでを事業者の担当となるのかを御教授いただきたい。

○（後藤プログラムディレクター）

SIP においては、終了時の 5 年後には実用化、一部事業化が始まる形に持っていきたい。あとはその勢いで産業界がうまく引き取れるような仕組みをつくっておくという方向で考えている。実際に製品やサービスを提供する部分は、企業の方がみずからの将来のビジネスのために使っていただければと考える。

○（鵜飼委員）

研究開発を推進していく上で出口を考えることは重要であるが、サイバーセキュリティビジネスは、走りながらでもビジネスにしていくぐらいのスピード感を持って企業と連携するのが大切である。一方、ハードウエア周りのバックドアの検出の話は、すぐにビジネスにならないが、非常に重要なテーマであるため、全体観を考えつつ今のうちからきちんと手を打っておく必要がある。

○（小山委員）

IoT のセキュリティ対策については、日本は非常に進歩的である。こういった場での進んだ議論の結果であると誇らしく感じるが、展開には法制度の実装が欠かせないので今後も官民で歩調を合わせていきたい。次期戦略においても、「防

御力」「抑止力」等の言葉が見られる点は、民間としても後押しをしやすい部分である。この点は、重要インフラ事業者を中心に官民の情報共有をしっかり進めることで、「強靭性」も高まるのではないかと考える。そのための研究開発をどう進めるかという議論がこれから行われるべきである。

○（佐古委員）

ビジネスにならないが故に注目されなくとも、国民が知るべきこととしてそれがどうなっているのか純粋に考えている技術者、研究者が多くいる。そのような研究者コミュニティを活性化することが、日本の安全性につながると考える。また、プラットフォーマーが発信するメッセージも、意図的に操作されないようにセキュリティを担保した立場から十分に吟味、展開することについても考えていかねばならないと思う。

○（戸川委員）

ハードウエアの脆弱性と、セキュリティに関して補足する。プロセッサーにFPGA（field-programmable gate array）と呼ばれる、ハードウエアとソフトウエアの中間に存在するものが組み合わさったプラットフォームの利用が、今後多く見込まれている。FPGA はハードウエアだが、回路の内容を外部からソフトウエア的に書きかえられるため、ファームウェアのアップデート同様に FPGA アップデートが発生することが考えられる。こうした点も鑑み、今後はハードウエアの脆弱性を工場のみならず出荷後もチェックしていく必要があるので、今後議論させていただきたい。

○（奈良委員）

社会実装の究極の出口は、国民であると考える。国民全体に対して、サイバーリスクがあること、そのために戸川委員や後藤 PD のような研究開発の実施も含め、政府や産業界も挙げてリスクマネジメントを行っていることを国民に伝えることも考える必要がある。また、次期戦略において、「全員参加による協働」への言及があったが、体制づくりに加え、体系づくりも必要である。国民に対して施策をどう届けるかも射程に入れながら、研究開発を議論できるとよい。放送大学を通じ、官学挙げてリスクコミュニケーションを進められればよいと考える。

○（名和委員）

中小企業を含めたサプライチェーンにおいて、その取組の方向性が明確になっていないと感じる。費用対効果の問題等、手つかずの部分は多くあるが、それらへ取組は必ず行う必要がある。また、各国がデジタル媒体やインターネットの保護主義に向いている中で、日本がそこに対してどのように取り組むのか、メッセージが必要とも考える。今後の議論において、テクノロジー重視か、あるいは開発管理重視とするのかは注視する必要がある。

○（篠田補佐官）

改めていろいろな課題を見ていると、根源的なものは同じと感じる。例えば、情報共有がうまく進まないと言いながら、もう 10 年間そのままである。難しい課題には、ダイバーシティを持ち、1 個失敗してもその場で転んで終わりにならないようにしていくべきである。また、国際的な競争力という観点から見ても、クリティカルマスを超えて研究開発を推進していかないと、世界と対等な話もできない。適切な投資を行い、「高効率」というキーワードに言いかえた、情報共有とテクノロジーの共有、攻撃されているテクノロジー、攻撃に利用されているテクノロジーを逆手に取った返し技をする考え方も必要ではないかと考える。

○（中尾補佐官）

いわゆる IoT は、複数の利益関係者を巻き込み、サプライチェーンも含めて非常に複雑な状況になっている。小山委員も言った通り、日本はある意味では進んでいると感じる。研究開発という見方では、ハードウエアやソフトウエア、インシデント分析、あるいはマネジメントや法令など、多くのアングルの研究開発に関連する事象が多々出てきている。本会では、それらをよりいい形で整理していくことが非常に重要であると考える。また、本日の戸川委員の考え方は非常に重要と思えるので、今後の検討に加えていただきたい。

○（後藤滋樹会長）

鵜飼委員の指摘にもあったように、ハードウエアトロイの検出は即ビジネスにはなり得ない。そのようなリスクのある製品の使用にあたっては慎重であるべきではあるが、費用対効果を考えた上でも政府として、今後どのような対応を取るかを検討する必要があると考える。

以　上