

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6回会合 議事概要

1. 日時

平成29年3月3日(金) 10:00~12:00

2. 場所

フレンドビルディング7階 大会議室

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 政策研究事業本部 経済政策部 主任研究員
	小松 文子	長崎県立大学 教授
	小山 覚	NTTコミュニケーションズ株式会社 情報セキュリティ部 部長
	神成 淳司	慶應義塾大学 准教授
	松原 実穂子	パロアルトネットワークス株式会社 最高情報セキュリティ責任者(CSO Japan)

(外部発表者)	稲見 昌彦	東京大学先端科学技術研究センター 教授
	松尾 豊	東京大学大学院工学系研究科 准教授

(事務局)	中島 明彦	内閣サイバーセキュリティセンター長
	永井 達也	内閣審議官
	三角 育生	内閣審議官
	山内 智生	内閣参事官
	阿蘇 隆之	内閣参事官
	佐々木 良一	サイバーセキュリティ補佐官
	八剣 洋一郎	情報セキュリティ指導専門官

(オブザーバー) 内閣官房情報通信技術(IT)総合戦略室
経済産業省
総務省
防衛省
外務省
文部科学省

4. 議事概要

○サイバー空間に関する展望

東京大学先端科学技術研究センター 稲見教授より、「VR と身体の未来」について資料 3 に沿って発表、委員から意見の概要は以下のとおり。

○（小山委員）

現実と VR の区別が曖昧になり、その人の生命にまでも影響を及ぼす可能性もあり、情報セキュリティというより安全ということに対する考え方が非常に重要になってくる。その際の情報の扱い方を改めて考える必要があると感じた。

○（神成委員）

今後は情報がつながっていることを前提に、必要な範囲の情報は自分で守る形で考えなければならない。

我々はそれぞれの立場で、どこまでの情報を守るべきなのか。また、情報は誰のものなのかを再定義する必要がある。おそらく多くの情報は誰のものか定義できない集合知になってくるので、自分の権利を主張できる範囲を正しく検討する必要がある。

○（松原委員）

VR をイノベーションとして進め、なおかつセキュリティを確保していくためには、技術のみならず、例えば、脳科学や医学、心理学など、これまで考えられていなかった分野にまで拡大した研究とそれに基づくセキュリティが必要である。それは複合的な課題であり、同時に大きなチャンスと思う。

続いて東京大学大学院工学系研究科 松尾准教授より「人工知能の未来 - ディープラーニングの可能性とサイバーセキュリティに対する影響 -」について資料 4 に沿って発表。委員から意見の概要は以下のとおり。

○（後藤会長）

人間も含めて、眼を通した進化が大きな影響を及ぼしたことは間違いないと感じる。人類、あるいは生物の歴史の中で、これまでなかったような大きな変化が今現在起きているという見方は、大変示唆に富んだものである。

○（上野委員）

AI の技術を実現、あるいは社会実装することを、誰が行うのかを検討することが重要であるのではないかと。また、よい利用方法を担保する主体の存在、あるいは作ろうとする動きが必要ではないかと。

○（佐々木サイバーセキュリティ補佐官）

ネットワークフォレンジックへの AI の適用において、攻撃側も常に変化して

くるので、ディープラーニングをするために十分なデータが集まらないことも想定される。そのデータが十分ではないような領域における AI の適用について検討する必要がある。

○（八剣情報セキュリティ指導専門官）

運動系の AI を研ぎ澄ませていくためには、精緻な部品が必要となるので、まさしく日本の強みを生かせる可能性があると思う。

○（小山委員）

「目」を持った機械やロボットのカンブリア爆発に、負けないように発展していく社会をどう支えるか考えることは、重要なテーマだと感じた。カンブリア爆発の後には大絶滅も起きたが、生き残る条件が情報セキュリティ対策であると言えるかもしれない。また、超スマート社会の影の部分に対応するための、社会実装を両輪とした研究開発をテーマとして議論すべきと感じた。

○（松原委員）

VR や AI など、新しい技術をセキュリティや便利さに役立てていくためには、これらへの不安を解消するための啓発と認識の醸成が重要である。また、IoT の増大に伴うリスクの拡大を鑑みると、後手後手の対策ではなく、積極的な防止と脅威情報の共有が今まで以上に重要になる。

○「サイバーセキュリティ研究開発戦略」骨子（案）について

資料 5 に沿って、事務局より発表。委員から意見の概要は以下のとおり。

○（神成委員）

情報は誰のものかということの概念を、使用者の観点から所有権と利用権に分けて、また深刻化への対応として、法整備を含めて検討していく必要がある。サイバーセキュリティの全体の中で、情報の利活用のあり方、許諾のあり方をきちんと議論をするべきである。

○（上野委員）

今後 VR の世界において、独自にトラッキングされて、情報がずっと蓄積されていくというところに対してのオープン・クローズド戦略のような観点も重要になってくると感じる。

○（小松委員）

今後数年で、信頼の起点の考え方がわかりにくくなっていく可能性がある。また、原始的な暗号の研究の世界でも、信頼の起点がない場合のやりとりをどうするかということも検討が進められている。

以上