

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5回会合 議事概要

1. 日時

平成28年10月31日(月) 13:30~15:30

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)	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
	新 誠一	電気通信大学 教授
	神成 淳司	慶應義塾大学 准教授
	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 専務理事/上級分析官
	松原 実穂子	パロアルトネットワークス株式会社 チーフセキュリティオフィサー ジャパン
(外部発表者)	酒井 雅之	内閣府 政策統括官(科学技術・イノベーション担当) 付 参事官(社会システム基盤担当)付 企画官
	大森 一顕	総務省 情報流通行政局 情報流通振興課 情報セ キュリティ対策室 室長
	石田 泳志	文部科学省 研究振興局 参事官(情報担当付) 情報科 学技術推進官
	玉井 英司	文部科学省 研究振興局 参事官(情報担当付) 参事官 補佐
	土屋 博英	経済産業省 商務情報政策局 サイバーセキュリティ 課 企画官
(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
結城 則尚	企画官
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
内閣官房内閣情報調査室
防衛省

4. 議事概要

○ 「サイバーセキュリティ研究開発戦略」策定の方向性について

資料 3-1~4 に沿って、総務省、経済産業省、文部科学省、内閣府 SIP より発表の後、事務局から資料 4 に沿って今後の取組の方向性について説明。委員から意見の概要は以下のとおり。

○ (新委員)

サイバーセキュリティは言わばたちごっこであり、対策を講じると、それに応じて新たな攻撃を考えてくるものである。研究開発についても現状の取組に安住することなく、足りない部分があるという認識の下、継続性を持たせた取組とすべきである。

日本の動向である人口減少や高齢化を踏まえ、分野横断的な施策が必要である。また、ネットワークの高度化や AI 技術の進展等、我々は人間の理解を超えた範囲まで、その規模を拡大してきた。このことを踏まえた上でセキュリティ対策を検討が必要である。

○ (名和委員)

研究開発の成果を社会実装するためには、出口戦略が必要である。また、業界でコストカットが盛んに行われている中、事業者がその成果を導入できるよう、社会実装ができる仕組みを同時に検討していくべきである。

○ (小山委員)

世の中の変化に伴い、例えば通信の秘密に関するセキュリティ対策は、新たな考え方が生じるものなので、施策開始後も研究テーマの見直しを継続して検討すべきである。

○（小松委員）

セキュリティ・バイ・デザインに係る研究については、サイバーセキュリティに特化するだけでなく、セキュアなシステム構築という観点からも取り組むべきである。

「サイバー空間と人・物理空間が接する部分のセキュリティ研究」については、中長期というよりもすぐにでも取り組むべき研究課題である。

○（松原委員）

国際競争力の強化には研究開発が勿論必要であるが、日本がどういう取り組みをしているのか 2020 年の五輪に向けて海外から注目が集まっているので、研究開発と合わせて情報発信も行い、日本の存在をアピールしていくべきである。

○（神成委員）

競争力のある社会をつくるためには、こういう社会にするのだというトップダウン、いわゆるバックキャストで推進する必要がある。中長期的に訪れるメガトレンドである超高齢化社会と人口減少社会において、人が足りないことも前提として、いかに社会を形成させるかという観点を踏まえて戦略を策定する必要がある。

また、保健医療、生活空間、環境対策等のアプリケーションに関し、それぞれ進捗の度合いが異なるので、対応には留意する必要がある。

○（佐々木サイバーセキュリティ補佐官）

各技術課題についてはシステム全体として考える必要があるとともに、ライフサイクルを念頭に置き、計画ないし設計・運用等も含めて考えるべきである。また、IoT も視野に入れると、セキュリティとセーフティの組み合わせも考えることが必要である。

○（奈良委員）

バックキャストという観点は重要である。これを踏まえて 2030 年をターゲットにするにあたり、ステークホルダーが持つ情報システムに対する期待と懸念は何かというところからブレークダウンすることで、技術的な話につながると考える。

○「安全な IoT システムのためのセキュリティに関する一般的枠組」について
資料 5 及び参考資料 1～3 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。

この議論の後に本調査会設置根拠に基づき、「安全な IoT システム創出のためのセキュリティワーキンググループ」（仮称）の設置することを会長より発表。

○（名和委員）

本枠組の展開にあたっては、Internet Engineering Task Force 等、様々な活動と連携しつつ進めていくことが必要である。

○（新委員）

電力業界やガス業界では、民間主導でガイドラインなどが作られている。こうした民間の活動とともに、政府としてもそれらの活動全体を見て統括することにより、セキュリティが進んでいくのがよいと考える。

○（小山委員）

IoT の実態を見ていると、対策は「待ったなし」と感じる。経済戦略として我が国の国際競争力を高めようという状況において、異なる業態同士が双方歩み寄るという意味において「場をつくる」ということが非常に重要と考える。これを機に IoT 機器のセキュリティ対策が難しいことを念頭におき、取り組んでいくべきである。

以 上