資料２

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３回会合　議事概要

１　日時
平成 28 年 3 月 1 日（月）　10:00～12:00

２　場所
内閣府庁舎別館 9 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・社会政策部 主任研究員
	小松 文子	独立行政法人 情報処理推進機構 情報セキュリティ分析ラボラトリー長
	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
	名和 利男	株式会社サイバーディフェンス研究所 理事／上級分析官
	松原 実穂子	インテル株式会社 サイバーセキュリティ政策部長
	宮地 充子	大阪大学大学院工学研究科／ 北陸先端科学技術大学院大学 教授

（外部発表者）	中西 悦子	内閣府 政策統括官（科学技術・イノベーション担当）付　企画官
	山下 浩司	経済産業省 商務情報政策局 情報経済課 情報セキュリティ政策室　課長補佐
	棚田 祐司	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　係長

（事務局）	髙見澤 將林	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
	谷脇 康彦	内閣審議官
	三角 育生	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
八剱 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
警察庁
文部科学省
防衛省

4 議事概要

(1) 関係府省等の研究開発に係る施策の取組状況について

資料 3 に沿って内閣府より発表。その後、委員から以下のような意見が述べられた。

○（新委員）オリンピック関係システムでは、新しく開発された機器に加え、古い機器を使わざるを得ない。古い機器と SIP（戦略的イノベーション創造プログラム）で開発される新しい機器をどう組み合わせるのか気になる。

○（小松委員）「信頼の基点」という言葉は、トラストアンカーに置き換えられると考えられる。トラストアンカーを担当するメーカーが堅牢に守るシステムを持っていればよいが、全てのメーカーがそうとは限らない懸念がある。

資料 4 に沿って、経済産業省、総務省より発表。その後、委員から以下のような意見が述べられた。

○（神成委員）このガイドラインの議論においても、SIP の IoT の研究を踏まえ、施策の成果の反映に関する議論が含まれるよう配慮するとよい。
また、データの所有や IoT における責任分界の問題に関する議論は、おそらく全ての分野横断で議論するのは困難である。

○（小山委員）ファームウエアのアップデートについて改めて強調する。セキュリティ対策については、非常に先端的な取り組みとベースラインを上げていく取り組みの 2 点が必要だと思われる。また、資料 4 スライド 8 の論点で脆弱な機器などをどのように把握していくかに関し、国内に信頼のおけるデータベースを設置、運用することをテーマとして取り組んではどうかと思う。

○（新委員）資料 4 スライド 6 の保守・運用、流通まで考えるべき論点に関し、同資料の設計・開発時に留意すべき推奨事項についても、同じ論点にて見直ししたほうがよい。

○（松原委員）既出のガイドラインと、今後出てくる IoT のセキュリティガイドラインはどのような整合性を持たせるのか。また、IoT のセキュリティガイドラインは日本語で出すつもりではあるが海外とも連携を図る旨コメントがあったが、どのように行うのか。

○（名和委員）IoT に関する海外との連携において、海外で先行している機関や取組との連携検討をするとよい。また、国際標準等へのインプットにあたり、発言力が低くなっている日本として、どのように対応するのか考慮が必要。

メーカーやベンダーは海外のベンダーもあり、不安全なもの含まれていると考えるが、サプライチェーンの問題に対する記述がなかったように思う。

○（小松委員）資料 4 スライド 6 の論点において、機器メーカーがいろいろな部品メーカーと関連してサプライチェーン・セキュリティに取り組むべきではないかと考える。

○（宮地委員）標準化の件に関し、業界標準は国内だけで動くのではなくて、世界的に標準化していく必要性があると考える。

欧州には Horizon2020 という形で、世界中から企業を呼ぶ動きがある。現状の説明では完全に日本独自という形のように見えるが、欧米のように日本から発信して、海外の企業にも参画させる仕組みを考慮してもよいと思うがどうか。

IoT にはセキュリティだけではなくプライバシーという観点も必要。プライバシーに関しては各国で考え方が異なるので、標準化は難しいと思われる。プライバシーに対しては、日本はどのあたりを目標にしているのか明確にする必要がある。

○（上野委員）IoT セキュリティ WG でこれからガイドラインが策定されるとのことであるが、データの帰属と利用に関しても検討が必要である。

(2)　「安全なIoTシステムの創出」について

資料5に沿って事務局より発表。その後、委員による自由討議が行われた。委員から以下のような意見が述べられ、それに対し事務局が説明を行った。

○（上野委員）資料5はサイバーセキュリティ戦略から抜粋して説明しているのか、さらに上乗せして説明しているのかがわかるとよい。各府省に働きかける資料なのであれば、何を求めているのかを、具体的に呼びかける内容がよいと思われる。

○（小松委員）任務保証に関し、資料の図にはサイバーセキュリティの特徴が余り含まれていないので、追記したほうがよい。

○（松原委員）任務保証についてどこまで適用するのか、民間側にどこまで任務保証が求められるのか曖昧である。例えば、重要インフラの停止と、1つのスマートウォッチの使用不能では、顧客の受けるダメージの大きさは異なり、任務保証の種類も異なる。

セキュリティ・バイ・デザイン、プライバシーデザインを進めるにあたり、まずリスクモデルを作り共有するR&Dの推進が必要である。

○（小山委員）10年、20年と使い続けるときのトータルコストをどう最小化するかも重要な観点と考える。IoTのビジネスモデルにおいて、関係者がお互いの領域で協力しあうことは重要である。自分のリスクを守ることも重要だが、コストの観点で、トータルで勝ち残るスキームについて一度議論してはどうかと考える。

セキュリティ・バイ・デザインの考え方は2つあると考える。高度なセキュリティをいかに実装していくかと、ボトムラインにおいて、多数のデバイスのセキュリティレベルを少しだけ上げるやり方である。

○（名和委員）サイバーセキュリティ担当者がIoTのセキュリティを安全に保つようIoTの製造部門や開発部門に言うが、会社の中にはパワーバランスがあり、容易に動かないという話を聞く。会社の実情にも配慮した、より実効性のある啓発が必要である。

政府機関においてセキュリティ・バイ・デザインに数年関与してきたが、勉強の必要性やコスト面の難しさもあり、定着しているとは言い難く、非常に難易度の高いものを民間企業に求めている。もう少し違った形でのアプロ

ーチはできないか。民間では、利益重視の現状では困難である。財政関係や経済促進の取組の足を引っ張りかねない。

○（後藤会長）日本がセキュリティ・バイ・デザインを含むこの戦略を英語や日本語で発信すると、日本企業よりも他国企業が先行して採用する可能性もある。

真正なハードウェアであっても、モニター機能がどの程度入っているか、全てチェックするのは困難である。

○（新委員）セキュリティ・バイ・デザインだけではなく、セキュリティライフサイクルについても考慮する必要がある。

IoT は不特定多数が使うもの、さらに現実としてコスト面への配慮が必要な旨、観点を加えるとよい。

経済産業省が策定している、スマートメーターのセキュリティガイドラインでは、第 1 章が経営者の責任との書き出しから始まっている。ここでも経営者の責任を表に出した方がよい。

○（宮地委員）IoT 機器が収集するデータも変わる。セキュリティ・バイ・デザインは非常に重要な事項であるが、最初に決定することは難しい。収集するデータのみならず、利用者も固定ではなく変化するという観点も必要と考える。

○（佐々木サイバーセキュリティ補佐官）　安全な IoT システムの創出にあたり、リスク評価が入ってきた点は非常によいことである。リスク評価は、誰のために、誰がやるか、関与者が誰か、どこに働きかけるかを明確にすることが重要である。

以　上