技術戦略専門委員会
第２３回会合　議事メモ

1　日時
平成 26 年 4 月 4 日(金) 10:00～11:45

2　場所
内閣府庁舎別館９階　大会議室

3　出席者（敬称略）

（委員長）	後藤 滋樹	早稲田大学理工学術院教授
（委員）	阿草 清滋	京都大学客員教授
	岡田 羊祐	一橋大学大学院教授
	小柳 和子	情報セキュリティ大学院大学名誉教授
	河田 惠昭	関西大学
	志方 俊之	帝京大学教授
	中西 晶	明治大学教授
	名和 利男	株式会社サイバーディフェンス研究所上席分析官
	松原 実穂子	株式会社日立システムズ
	宮川 晋	NTT コミュニケーションズ株式会社 先端 IP アーキテクチャセンタ・経営企画部（兼務） 担当部長
（事務局）	藤山 雄治	内閣審議官
	谷脇 康彦	内閣審議官
	佐々木 良一	内閣官房情報セキュリティ補佐官
	三角 育生	内閣参事官
（オブザーバー）	内閣府	
	警察庁	
	総務省	
	文部科学省	
	経済産業省	
	防衛省	

4　議事概要
（１）開会

（２）情報セキュリティ研究開発戦略の見直しについて
事務局より資料 3 に沿って説明。（略）
この後、委員による自由討議が行われた。委員等からは以下のような意見が述べられた。

＜自由討議＞

○　「日本発のグローバル ICT 製品・サービスの実現を目指す」と資料にあるが、政府の目標としては、独自の技術を打ち出して ICT の一分野で強烈な存在感を出そうとしているのか。

○　公的機関や大企業が実施するプロジェクトは、成功することが初めからわかっているものばかりであり、無難な成果しか出てこない。優れたものは、成功率が 1～2 割といったリスクの高いところからしか出てこないことを少し重要視してほしい。

○　先進的なものを生み出すには、技術面だけでなく、例えばシリコンバレーで行われているような、人材、ファイナンス等の仕組みも考えなくてはならない。特定の分野で小さくてもよいので、日本としてのサクセスストーリーを作ることができるとよい。

○　震災等の際には、利用できる情報が対応の質を決めてしまうので、非日常のセキュリティについても決めておく必要がある。災害情報の学会でもこのような切り口では対応していないため、政府等から学会に働きかけることも重要。

○　よくオールジャパンという言葉を聞くが、日本は既にトップランナーではないので、方針にある国際連携の必要性はそのとおりである。その際、コア技術の保持においては、優秀な外国人を大学や研究所で雇う際、雇用契約、報酬、守秘義務等をどのようにするかが課題。

○　品質はトータルなものであり、一つの技術やアイディアで担保されるものではない。全体としてどうデザインするかの仕組作りが重要。上流工程からのセキュリティ品質の組込を目指す場合も、チェック工程まで含め、誰がどのよう行うかの仕組作りが大事である。重要分野に挙げている「ソフトウェアの安全性確保」もシステム全体として安全性確保を考える必要がある。これらについては、一般論では考え方が発散するので、幾つかの具体的なターゲットを決めて作り方を考えるとよい。

○　国際連携は誰とでも組めるわけではないが、IT 技術者の給与体系を十分なものにする必要がある。現在のように実務者の給与が低いままでは民間や海外に流出してしまう。

○　日本は海外に比べると、コンピュータサイエンスなど基礎となる技術を教えるコースや学科が圧倒的に不足している。産官学の役割分担を考える上で、技術的側面のセキュリティ分野の充実を図る必要がある。

○　国家公務員の給与水準が低いために民間に優秀な人材が流出するのは各国共通の課題であるので、海外にも手本はなく、日本独自の解決策を考えなくてはならない。

○　海外のコミュニティや会議に出ると他の日本人をあまり見かけないが、これは日本の考えを発信する機会を逸していることになる。日本人は失敗を恐れ、手堅いところで守りに入る傾向があるので、失敗を恐れずにチャレンジすることを評価する文化づくりが必要。

○　IoT（Internet of Things：モノのインターネット）の進展により、国民も従来以上にサイバー脅威にさらされることになる。一般の国民レベルで使いこなせるサービスの研究開発もこの戦略に盛り込み、一般人もこの戦略を読んで自分のこととして考えられるような記載もすれば、国内需要の拡大・セキュリティ意識の向上につながる。

○　少ない予算の中で国が取り組むべきものとして以下二点。一つは、事業収益に結び付きにくい暗号などのコア技術の研究開発。もう一つとして、保持している民間の現場が出したがらない生のデータを、うまく皆で使える仕組みをぜひ推進してほしい。

○　情報セキュリティ技術と社会科学等他分野との融合について、学会では学際的な研究は評価されにくく、博士論文に結びつかないという実態が課題としてある。

○　社会科学等の連携が、「サイバー攻撃の検知・防御能力の向上」中の取組として記載されているが、他の項目においても必要なことであるので、共通的な取組として記載すべきではないか。

○FIRST（Forum of Incident Response and Security Teams）でも大規模災害時の対応等を検討しているが、DR（ディザスタリカバリ）や BCP とセキュリティの関連について、現場の人たちも立ち位置を決めかねている。現場の人たちが円滑に動きやすくために、政府側でも検討頂きたい。

○IoT が進展し、一般の人が意識せずに ICT を使うようになった際、どのような対策をとるべきか、また産業振興としてどのようなことが考えられるかも検討した方がよい。

○　以下 4 つの技術も加えた方がよいのではないか。①人材育成のための e-learning 等の演習支援技術、②データの収集・配布・解析・フィードバックをする手法の技術、③IT-BCP ともいうべきサイバー攻撃以外でのシステムダウンに対応するリカバリ技術、④対策によって変化する攻撃に対する動的セキュリティといったもの。

○　異常なデータの解析を進めるには、比較対象としての正常なデータをどのように確保するのかも課題である。

○　経済学などにおいて、日本固有の仕組みや制度に関する研究は、なかなか海外で評価されないという現実も認識しておくべき。

○　海外の発表では、海外と比べた日本独自の制度とその理由、また海外と日本がよりよく協力していくための方策についてグローバルな視点から説明すれば、歓迎される。

○　国の予算は、研究者が費目や様々な条件を気にしながら作業をするのが大変である等使い勝手が悪く、研究活動を阻害している面があるので、改善を図れないか。

○　IT-BCP においては、IT システムの復旧を考えるだけでなく、代替的な手段による対応も考えるべき。

○　非常時のライフラインのリカバリが、事業者任せになっているのが以前から問題となっている。ライフラインの本当の信頼性を議論するために、事業者のみが保有するインフラの情報を共有化すべきではないか。

○　インフラ詳細の開示については、競合他社との関係や、安全保障上の秘密があり困難。また、生データを共有しての利用についても、通信の秘密があり難しい面がある。

○　社会科学においても、どこまで情報にアクセスできるかが研究の優劣を左右する。米国はデータの利用や公開が進んでいるが、日本では情報収集が難しい。

○　マルウェアや標的型攻撃の情報共有について、海外各国では積極的に共有されているが、日本では共有が進んでいない。海外各国にはオープンソースの製品も幾つかある。防御システムやインシデント対応サービスで検知する有益な情報の共有を検討いただきたい。

（3）今後のスケジュールについて

事務局より資料 5 に沿って説明。（略）

（4）閉会

以　上