資料２

技術戦略専門委員会
第２２回会合　議事要旨

１　日時
平成 26 年 1 月 28 日(火) 10:00～11:40

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	元　情報セキュリティ大学院大学教授
	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	情報セキュリティ補佐官
	徳田 英幸	情報セキュリティ補佐官
	篠田 陽一	情報セキュリティ補佐官
	三角 育生	内閣参事官
	山内 智生	内閣参事官

（オブザーバー）　神成 淳司　　内閣官房 政府 CIO 補佐官
内閣官房 情報通信技術(IT)総合戦略室
内閣府
総務省
経済産業省
防衛省

４ 議事概要

（１）開会

（２）委員の追加について

新任 2 名の委員について、事務局から資料 1 に沿って紹介。

（３）委員の任期について

委員の任期の見直しについて、事務局から資料 2 に沿って説明。

（４）情報セキュリティ技術開発を活用した産業活性化検討ワーキンググループの廃止について

事務局から資料 3 に沿って説明。同ワーキンググループの廃止を決定。

（５）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 4 に沿って説明。

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＞

○　最新の脅威に対応した研究開発の推進においては、ICT 供給者への直接的な脅威も考慮する必要があるのではないか。

○　重要分野の見直しについて、現在の研究開発戦略の進捗状況の確認結果を示す必要があるのではないか。

○　今回の研究開発戦略見直しにおいては、経営学、心理学等の社会科学的視点も含めるとよいのではないか。

○　発展が期待される応用分野の議論においては、パーソナルデータ等のセンシティブデータといった括りで検討することが良いのでははないか。

○　ユーザーが、サイバー攻撃を受けたことにもっと気付けるようになることが重要。また、攻撃を受けた際、即時にそのことを通報し対応する仕組みが必要。

○　攻撃を受けたこと自体が秘密にあたる恐れはないか。

○　サイバー攻撃情報の流通や調査分析の共有化は、扱いに一定の注意をした上で、ぜひ進めるべき。若い世代がセキュリティに関心を持つ上でも効果的。

○　セキュリティに関する社会認知度を向上させ、セキュリティに過敏な層、鈍感過ぎる層という両極端な層を減らす取組を、国や ICT 供給者が進めることも重要ではないか。

○　施策によっては、技術的な問題以前に法的な課題が大きいものもある。また、グローバルなネットワーク上での出来事には、どの国の法制度を適用すべきか困ることがある。このケースは法の範囲内といったことを、予め国が示すことはできないか。

○　生化学、システム生物学等では、倫理委員会が実験の事前審査を行う。情報セキュリティでも、法的な課題は、このような第三者委員会認定である程度解決できるのではないか。

○　パーソナルデータ等の扱いについては、IT 総合戦略本部で設置を検討している第三者機関等の活用も考えられる。

○　技術は、社会への適用が重要。下請け構造の現在のソフトウェア開発現場で、情報セキュリティを確保することが困難な現実があり、国か何かがチェックする仕組みが必要ではないか。

○　国民に対し、一般的なリテラシーさえあれば、情報セキュリティを技術的に担保できるようなシステムを提供できないか。

○　機器のブラックボックス化の問題に関連し、機器が表示している動作状況と現実の動作状況が一致しているかの検証方法も検討が必要。

○　特定秘密保護法により、官民間で攻撃兆候や分析結果の情報共有に支障が出ないよう整理が必要。

○　わが国では、海外と比べて、目に見えない分析研究やサービスが安価になりがちであり、日本の競争力強化のためにも投資が必要。

○　我が国では攻撃を検知する能力が低下しており、他国と比較しても低い。強化が必要。

○　我が国ではサイバー攻撃に関する情報が分散しており、米国や韓国等と比べ、蓄積・共有が遅れている。蓄積・共有のシステムを構築すべき

○　ベンチャー企業等の研究開発の資金調達及び成果配分がスムーズにいくため

の仕組み作りを考えることが重要。また、官で研究開発された成果がうまく民で実証に結び付かないという課題を検証する必要がある。

○　研究対象がムービングターゲットであることに気をつける必要あり。2～3 年後に攻撃がどのようになっているかを考慮しながら、研究開発戦略を立てていくことが重要。

○　研究開発における産学官の役割分担を国としてどのように考えるべきか、国は民間をどのようにガイドすべきかについても議論を行いたい。

○　若い世代が研究開発の成果をビジネスに結びつけるために、我々年上の世代は何をすべきか検討が必要。

○　技術分野毎に、国内で開発すべきコア技術、国際連携を進めるべきものといった優先順位付けとそれぞれの戦略が必要ではないか。

○　技術の社会への適用においては、国際標準が重要であり、我が国の独自技術にこだわり過ぎない方がよい。海外の技術を評価・検証できる技術を磨くことの重要性を明示すべき。一方、我が国の技術を国際標準にし、サイバーセキュリティでリードする地位を確立することも重要。

○　我が国では、相手側に侵入して調査・分析をするようなことは難しい。第三者委員会等で、どこまでの範囲が許されるかを整理してもらえるとありがたい。

○　暗号等の基礎研究に携わる研究者数は、民間で減少、国でも現状維持の状況。このままでは評価・検証の技術さえ危うくなる。国という立場でどのように研究者を確保するかの検討が必要。

○　本委員会は、技術の委員会ではあるが、社会環境の変化も踏まえたビジネスの面まで考えることが必要。

○本委員会では、我が国の弱点である、情報セキュリティの価値が評価されにくいこと、マネジメント・オブ・テクノロジー（技術経営）が進んでいないことについて提言していかなければならない。

（6）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。

以　上