高度情報通信ネットワーク社会推進戦略本部 情報セキュリティ政策会議
技術戦略専門委員会
第 20 回会合議事要旨

**１．日時**　平成２４年3月３０日（金）１０：００～１２：００

**２．場所**　内閣府別館９階大会議室

**３．出席者**

［委員長］
後藤 滋樹（早稲田大学教授）
［委員］
阿草 清滋（名古屋大学大学院教授）
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教授）
志方 俊之（帝京大学教授）
中島 秀之（公立はこだて未来大学学長）
中西 晶　（明治大学教授）　（五十音順）

［関係省庁］
総務省情報セキュリティ対策室課長補佐
経済産業省情報セキュリティ政策室課長補佐
［関係独立行政法人］
（独）情報通信研究機構ネットワークセキュリティ研究所長
（独）産業技術総合研究所情報通信・エレクトロニクス分野副研究統括

［事務局］
内閣官房情報セキュリティセンター長
内閣官房情報セキュリティセンター内閣審議官
内閣官房情報セキュリティセンター内閣参事官
内閣官房情報セキュリティセンター情報セキュリティ補佐官
（内閣府政策統括官付代理参事官付）

**４．議事概要**

（１） 開会

内閣官房情報セキュリティセンター　センター長　櫻井副長官補　挨拶

（２） 情報セキュリティ研究開発戦略の取組について

事務局より資料２に沿って説明後、総務省、経済産業省、独立行政法人情報通信研究機構（NICT）、独立行政法人産業技術総合研究所（AIST）より、資料２－１～４に沿って説明。

○ 研究開発を戦略的に進めていく上で、資料２－４のＰ１４の連携図が重要である。特に、重複している分野の役割分担や情報共有できるように整理する必要がある。
○ 実用化の課題の一つとして、利用者が安全を確認・実感できる認証制度を確立し、長期的な信頼を獲得することが必要である。
○ 研究開発を実用化するために、国内の基礎研究と製品研究のスタイルを変える必要がある。これは国立研究所で研究を行っているだけでは難しく、製品化を牽引するような施策とともに研究を行う戦略が必要である。
○ サイバー攻撃や標的型攻撃の予知は、本攻撃前の予備的な攻撃がない場合の対応は難しいかもしれないが、我が国のサイバー攻撃対策の国際水準を高めるということが期待できる。
○ 衆議院、参議院及び三菱重工業等へのサイバー攻撃は、平時のサイバー戦ととらえ、どのような攻撃を受けたのか把握し、証拠を保全することが重要である。
○ 守りから攻めの研究開発を行っていることは評価できる。また、情報セキュリティ製品を輸出していくためには、日本も検査、認証の体制構築は重要である。
○ 米国では、制御システムを設計する人間とセキュリティを担当する人間が一緒に連携して取り組んでいる。また、サイバー攻撃の攻撃技術に関する知識も持てるよう育成している。
○ 情報セキュリティ技術の実用化については、アメリカで国と企業がお金を出し合っているように、日本でのファンディングの見通しを持つ必要がある。また、日本に十分な人材が足りないのであれば、海外から集める必要がある。
○ 情報セキュリティ研究開発戦略において、情報理論的安全性に関する暗号技術に主眼が置かれているが、計算量的安全性にも注力する必要がある。
○ 研究開発戦略の取組が空欄になっている箇所については、企業が取り組むべき分野や、現在進めている研究に部分的に含まれているものもある。
○ 通信の秘密等の法的規制のために研究対象にするのが難しいテーマがあるが、法学者が通信についての概念の変化を指摘し始めており、あきらめずに研究を進めるということも必要である。

（３） その他

事務局より資料３に沿って、「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」について報告。

（４） 閉会

以上