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 19 回会合議事要旨

１．日時　平成２３年１２月１日（木）１０：００～１２：００

２．場所　中央合同庁舎第４号館共用１２１４特別会議室

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）
中西 晶（明治大学教授）
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）

（五十音順）

［政府］
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）

議事概要

（1） 後藤委員長　挨拶

（2） 内閣官房情報セキュリティセンター　副センター長　占部審議官　挨拶

○　様々なセキュリティ事案が発生し、国民の関心も高まっている。今後、オフェンシブに情報セキュリティ対策を行う必要があると考える。これからの戦略の進め方などについて、忌憚のないご意見をいただきたい。

（3） 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（仮称）の設置について（案）

【事務局より資料に沿って説明】

○　特段の意見がなければ、技術戦略専門委員会下に WG を設置することにつき、本委員会の決定事項とする。

（4） 情報セキュリティ研究開発戦略の概要について

【事務局より資料に沿って説明】

○　資料 3-1 中「重要分野の研究開発ロードマップ」に記載されている分野の中には、外国の市中製品で対応が始まってきているものが見受けられる。そのような分野については、前倒しで対応できると思う。一方で、５年で行うには難しい分野も見受けられるので、ロードマップの見直しについてはバランスをとりながら対応して欲しい。

○　セキュリティ製品として技術的対応が可能であっても、「通信の秘密」の観点から導入できない場合がある。技術的な取組とともに、法的な枠組の検討が必要である。また、本委員会でも指摘されていたことであるが、攻撃を受けた際に反撃するということは外国ですでに行われてようであり、そのような技術を使うための法的な枠組みも検討する必要があると思う。

○　「通信の秘密」は憲法との兼ね合いから、法的な枠組みの検討が難しい問題である。個人情報を活用するには広い納得が必要であり、十分に検討する必要がある。

○　国家は、個人情報の有効活用や保護レベルについて、他省庁との関係性やセキュリティ技術との兼ね合いから検討する必要があると思う。

○　報道によれば、昨今の事案は初歩的な部分に原因があるとのことだが、そうであれば、技術の研究開発したものをいかに根付かせるかを考えることも重要である。

○　利用者側の弱点の多様化により対策が難しくなっているところもあり、技術外の対応も必要である。

○ 補佐官：技術が根付かない理由の一つとして、企業活動はリスクを減らすためだけに行っているのではないというところがある。例えばサーバ対策において、パッチを当てると不具合が発生することがあることから、すぐにパッチを当てることができない場合がある。バランスを取りながら、かつ低コストにて対応する必要がある。

○　各省で問題が起きたときには、通報するシステムはあるのか。また国家として、サイバー攻撃に対するおとりのようなものを設置して、日々情報収集などを行っているか。

○ 事務局：NISC では、GSOC により監視し、その情報を共有している。また、ハニーポットによる情報の収集や、パケットの定点観測を行っている独立行政法人も存在する。攻撃を徒労に終わらせるための活動を日々行い、ニュー・ディペンダビリティのさらなる実現を目指している。

○　設定の変更が必要な研究については、IPv6 化されるタイミングに間に合わせてコンポーネントで配付するなど、工夫が必要である。例えば、設定ファイルの管理の研究は、目標を決めて前倒しで行っていく必要がある。

（５） 情報セキュリティ研究開発戦略の取組状況について

【事務局より資料に沿って説明】

○　ロードマップの中には、官主導で行っていく分野、マーケット主導で行っていく分野がある。また、技術においては競合するものと補完するものがある。これらを官民連携の仕組みの中におりこみ、最終的なイメージを想定する必要がある。また、研究開発については活用していくことが重要であり、それを WG で検討して欲しい。

○　「ＩＴリスクに関する理論から実務までの体系化」や「リスクマネジメント」については、重要インフラともからめて横串で考える必要がある。

○　省庁が資機材を発注する際、財務監査は行うもののセキュリティ監査が弱いので、例えば業務技能検定のようなもので、監査に対応できる要員を担保する必要がある。

○　参考資料２に記載された「組み込み用ディペンダブル・システム」について、もっと運用しやすい環境が必要であると考える。例えば、国のホームページに安全な OS や標準ソフトウェアをダウンロードできるような仕組みがあれば、中小企業にも導入され、安心感が広がると思う。また、研究開発の分野においては、開発後の継続的なサポートが必要であり、そのサポートに予算を投じる必要があると思う。

○ 補佐官：「組み込み用ディペンダブル・システム」については、現在、フランスとコンソーシアムを作ろうとする動きがある。

○　BCP に関し、経営判断において可用性に、より重点を置かれる部分があるので、そもそもセキュリティになじまないと言われることもあるが、本来 BCP とは経営者によって継続すべき事業のプライオリティをつけるものである。

○　BCP に関し、震災後、自分の大事なデータをデータセンターに預ける事業者も増えており、意識は確実に変わった。国家としては、コンプライアンス支援やセキュリティレベルの担保などを行うとともに、マーケット原理が働いていないところに予算を投じて欲しい。

○ 事務局：欧米であればリスクマネジメントにより投資効果を考えるが、日本国内では水と安全は無料であるというマインドがあるのではないか。

○　大企業であればリスクマネジメントにより投資効果を考えるが、それ以外の企業ではそのような投資を行っていると限らないのは、諸外国も同じである。リスクマネジメントの重要性については、中長期的に考える必要がある。

○　情報セキュリティ研究開発戦略において重要分野を推進していく上で、各分野の進捗を把握し、行われていない分野を重点的に推進することが重要であると思うので、関係省庁の取組みについて、次回の委員会において説明いただけるよう事務局において調整して欲

しい。

（６） その他

【事務局より資料に沿って説明】

○　ロードマップの詳細化や注意点については、早めに事務局にご意見をいただきたい。

（７） 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

○　熱心に議論いただき、大変感謝している。東日本大震災を通じて自助・公助・共助の視点をもって皆様の力添えをいただきながら進めていきたい。標的型サイバー攻撃なども発生しているが、政府と個々の企業と連携を取り、対応を進めていく所存である。

○　国際的にも関心が高まっており、今後、日本の技術を用いて国際貢献を行い、日本が牽引できる分野を開発していければよいと考える。

○　最後にあらためて皆様に感謝するとともに、今後とも協力をいただきたい。

（８） 閉会

○　大胆なゲームチェンジの考え方にのっとり、今後もご指導いただきたい。これにて本会議を閉会する。

以上