

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 第5回会合 議事要旨

1 日時 平成18年4月28日(金) 17:30～18:30

2 場所 総理官邸大会議室

3 出席者(敬称略)

安倍 晋三	内閣官房長官
(欠)松田 岩夫	情報通信技術(IT)担当大臣
杓掛 哲男	国家公安委員会委員長
(欠)額賀 福志郎	防衛庁長官 (※高木 毅 防衛庁長官政務官代理出席)
(欠)竹中 平蔵	総務大臣 (※古屋 範子 総務大臣政務官代理出席)
(欠)二階 俊博	経済産業大臣
小坂 憲次	文部科学大臣
猪口 邦子	内閣府特命担当大臣(少子化・男女共同参画担当)
江畑 謙介	拓殖大学客員教授／軍事評論家
小野寺 正	KDDI 株式会社代表取締役社長
(欠)金杉 明信	日本電気株式会社取締役副会長
野原 佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
前田 雅英	首都大学東京教授
村井 純	慶應義塾大学教授

(上記のほか以下が出席)

二橋 正弘	内閣官房副長官(事務)
野田 健	内閣危機管理監
坂 篤郎	内閣官房副長官補
柳澤 協二	内閣官房副長官補
山口 英	内閣官房情報セキュリティ補佐官

4 議事概要

- (1) 「省庁基準の策定状況と組織・体制の構築状況」について
- (2) 「重要インフラの情報連絡・情報提供に関する実施細目」について
- (3) 「セキュア・ジャパン2006」(案)について

事務局より、資料に基づき、一括して説明を行った。

(4) 出席者意見開陳

上記(1)～(3)について、出席者から以下のような意見が述べられた。

- 情報セキュリティというと、コンピュータウイルスやハッカーなどサイバースペースの中の問題にとらわれがちになるが、物理的な脅威の危険性も高いので、それに対する配慮が必要である。
- 様々な経路をとりうるゆえに強固というサイバースペースのネットワークの特徴を、実際に利用することができるようにするために、物理的なネットワークについても多様性を持たせることを考える必要がある。そのためにレーザー通信衛星や準天頂衛星などの応用が考えられる。
- セキュア・ジャパン2006(案)の随所に、情報共有を行う旨の記載があるが、情報共有を実際に行うことは非常に難しく、個人の情報感覚の意識改革が必要である。そのためには、初期段階からの教育が必須である。その点も含めて、初等中等教育の段階から情報セキュリティ教育を取り入れて欲しい。
- 省庁横断的に施策を推進している点について評価する。
- 情報セキュリティ関連施策と内部統制施策を両立させることについて明記されていることは非常にありがたい。情報セキュリティと内部統制が統合的に動けるようになれば、会社として情報セキュリティを守ることのできる仕組みができることになり、各企業は動きやすくなると思う。また、次のステップとして、施策の体系的実施まで広げていただきたい。
- 既存の最新技術の緊急対応能力形成への有効活用について、具体的な行動として、各研究機関の活動調査、共同研究などを推進していただきたい。
- 3年後に第1次情報セキュリティ基本計画の目標が達成できるかどうか判断できるように、3年後までの目標を明確化したうえで、2006年度、2007年度の施策を決めるべきである。また、セキュア・ジャパンが何かということがはっきりしていない。これらを明確にする場を設けるという記述をセキュア・ジャパン2006(案)に記載していただいているが、その場において、何がセキュア・ジャパンなのか、評価指標はどうするのか、マイルストーンをどのように達成できるの

かということをしっかり検討していただきたい。

- 国民全体を均一にとらえるのではなく、インターネット利用は活発だが情報セキュリティ対策への意識が希薄な人が比較的多い十代や、情報セキュリティへの不安感が高いが情報収集や対応が不十分な人が比較的多い女性層など、それぞれの特徴を踏まえた対策をとっていくことが重要である。
- 若年層に対する啓発活動も非常に重要であり、小学校、中学校及び高等学校においても情報セキュリティ教育をしっかり行うことが重要である。この点についての記載がセキュア・ジャパン2006(案)には多くなく、実際の授業に向けて実施することは何なのかということがはっきりしていないということがあり、もう少ししっかりと取り組むということを盛り込んでいただきたい。
- ウィニー問題でも明らかになったように、人的問題が非常に大きい。そのため、教育・人格形成が重要だが、何を教えるのかということの中身を検討することが必要である。その際、省庁によってニュアンスが違うので、内閣官房で調整すべきである。将来の日本を構築する上で、土台としてのセキュリティ思想・意識を作る必要があり、そのために何を教育するのかということをもう少し具体的にしたい。
- 例えば女性を物扱いしたコンテンツなどのネット上の問題のある情報に対しても取り組んでいくべきである。このことは教育に繋がっていき、将来においても一番の土台であると考えている。
- 政府における情報セキュリティ政策の中心となる内閣官房情報セキュリティセンターには高い能力が必要であり、日本の中でも官民最高の人材が力を合わせて取り組まなければならない。そのような人材の育成・確保も含めて、内閣官房情報セキュリティセンターの運営強化についての具体的な方策を検討すべきである。
- 情報セキュリティは非常にわかりにくいという性質を持っているが、これは、情報セキュリティに対する恐怖感や、技術的なことに関する理解の難しさが原因ではないか。広報周知・教育などにおいては、正しい言葉で正しく伝達をされているかどうか確認するメカニズムが必要である。そういったことやマスコミ対応も含めた上で、人材及び教育についての視点を持つことが重要である。
- 企業の内部統制などの制度面については、既存の社会の組織の制度と整合性を取るようにすることが重要である。

- 光ファイバーのケーブルの世界的な配置を考えると、日本は西の端にあり、ヨーロッパとの通信を行う場合でも、アメリカとの通信に依存している。また、西回りのケーブルを強化するとしても現存のものは遠回りであるため、線を直接結んだ場合に比べて約2倍遅く、株式の取引などの経済活動においてはリスクとなりうる。そういった意味でのリスクも考慮し、経済活動の安全も含めた一般的な生活の安全を確保するための情報セキュリティという視点で、国際通信基盤のあり方について検討することが必要である。
- IT社会の進展に伴い、ITが国民生活の利便性の向上に大きく寄与している一方で、不正アクセスやコンピュータウイルスをはじめとして、インターネットをめぐる様々な問題が発生しているという情勢の下で、セキュア・ジャパン2006が定められることは、大変意義深いと認識している。
- 警察によるサイバー犯罪の取締りやサイバーテロ対策をさらに進めていくことが、我が国の情報セキュリティを確保する上で、不可欠であると確信している。これらの活動を効果的に推進していきたい。
- 初等中等教育段階からのセキュリティ教育や、国民の安全・安心を支えるICTの信頼性・安全性を確保する上での人材育成は極めて重要であると認識している。
- 初等中等教育からのセキュリティ教育についてはリテラシーの部分が多く、皆さんが期待されているものとは違うと思う。
- 大学院における産学連携による高度IT人材育成プログラム、e-ネットキャラバンなどの各種取組みを通じて、学校における適切な情報セキュリティ教育や情報セキュリティをはじめとする情報通信分野の高度専門人材の育成に努めたい。
- ネットは怖いものという認識が出てきてしまい、それを悪用するような者も現れるようになってしまうと、誰も信頼できなくなってしまう。そのため、信頼できるシステムティックなコンサルティングが必要になってくると思う。例えば、大手の通信事業者が自社の看板を掲げて家庭に対して接触を試みるということが必要になるのではないか。
- 個人情報保護については、最近、いわゆる過剰反応が指摘されている。個人情報保護法の「個人情報の有用性に配慮しつつ、個人の権利利益を保護す

る」という目的を実現するため、国民生活審議会における議論を踏まえつつ、法を着実に執行していきたい。

- 海上自衛隊の護衛艦「あさゆき」に係る秘密情報流出事案が判明したことを受け、防衛庁全体としての再発防止に関する抜本的対策について検討するため、防衛庁内の全機関の長などをメンバーとする検討会を設置し、部外有識者からの意見を踏まえ、制度、技術、教育、設備など各種側面から必要な対策について検討を行い、4月12日に具体的対策を取りまとめたところである。
- 「あさゆき」の事案では、ウイニーによる情報流出という情報セキュリティに対する脅威の一端が明らかになったに過ぎず、その他にも重要な情報システムに対するサイバー攻撃等様々な脅威が存在し、それら全てに対して対応していく必要がある。また、情報セキュリティレベルの維持向上のためには、常に技術的及び運用的側面からの各種対策の見直しを検討し、柔軟にかつ迅速に情報セキュリティ対策基準や関連規則類の修正を行うことも必要であることから、防衛庁としては、情報流出対策に留まらず、総合的なセキュリティ対策に視点を広げて、今後とも庁全体の情報セキュリティレベルの底上げを引き続き実施していきたい。
- 全府省庁において省庁基準の見直し及び組織体制の構築が完了し、政府機関の情報セキュリティ対は実施段階に入ったと言えると思う。全政府機関が一体となり進めていく必要があると考えており、総務省においても対策を漏れなく実施できるよう尽力していきたい。
- 重要インフラについて、総務省では、情報通信と地方公共団体という重要な分野を担っている。本日の議題にある情報共有体制の活用などを通じ、引き続き重要インフラにおける情報セキュリティの一層の向上を図っていきたい。
- 総務省としては、第1次情報セキュリティ基本計画及びセキュア・ジャパン2006を着実に実施し、我が国の情報セキュリティの一層の向上に貢献していきたい。
- 日米間の海底ケーブルは合計で12本か13本あり、多様性という意味では、それほど危険性はないと思う。しかしながら、容量的に不足がはじめており、新しい海底ケーブルを引く計画を進めている。その際に、日本としては、日米だけでなく日中にも持って行きたいと考えているが、中国の事業者は日本を外して中米で回線を直接引くことを希望しており、米国の事業者を含めた取り合いのような状況になっている。これについては政府の支援が必要である。

- 日本とヨーロッパの間の海底ケーブルについては、現状では大容量の伝送路は全てアメリカ経由になっている。インド洋経由もあるがこれだけでは不安なので、シベリア経由の大容量ケーブルルートを検討している。これについては民間でかなりのことができるが、全体的な利用の中で政府の支援があればと思う。
- 情報セキュリティ予算について、例えば内訳で個人が4100万円というのは、少なく大変驚いた。これは情報セキュリティ関連予算の取り出し方にも問題があると思うので、情報セキュリティ予算というものが実質としてどれだけなのかということ把握できるようにする必要がある。その上で、海外とも比較するなどすべきだと思う。

(5) 政策会議決定等

「セキュア・ジャパン2006」についてパブリックコメントに付すこととされた。パブリックコメントは、約一か月の間受け付け、意見に基づき必要な修正を施した上で、次回の政策会議において最終決定することとした。

(6) 内閣官房情報セキュリティセンターの体制強化について

内閣官房情報セキュリティセンターの体制強化について、重要インフラ所管省庁等に対して協力を依頼する旨、安倍官房長官から発言があった。

－ 以 上 －

