

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13回会合 議事要旨

1 日時

平成19年8月3日（金） 11：15～12：15

2 場所

総理大臣官邸大会議室

3 出席者（敬称略）

塩崎 恭久 内閣官房長官  
高市 早苗 内閣府特命担当大臣（イノベーション）  
麻生 太郎 外務大臣  
（※浅野 勝人 外務副大臣代理出席）  
菅 義偉 総務大臣  
（※谷口 和史 総務大臣政務官代理出席）  
甘利 明 経済産業大臣  
（※高木 美智代 経済産業大臣政務官代理出席）  
小池 百合子 防衛大臣  
（※大前 繁雄 防衛大臣政務官代理出席）  
世耕 弘成 内閣総理大臣補佐官  
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  
黒川 博昭 富士通株式会社代表取締役社長  
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）

的場 順三 内閣官房副長官（事務）  
野田 健 内閣危機管理監  
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  
篠田 陽一 内閣官房情報セキュリティ補佐官

4 議事概要

- (1) 内閣官房情報セキュリティセンター（NISC）のこれまでの取組みについて
- (2) 「技術戦略専門委員会報告書2006」について
- (3) 政府機関の情報セキュリティマネジメントに関する評価結果について
- (4) 政府機関の情報セキュリティ対策の実施状況に関する重点検査及び評価結果につ

いて

- (5) 情報セキュリティ政策における「具体的目標」の設定について
- (6) 「我が国の情報セキュリティ分野における国際協調・貢献（国際戦略）」（中間報告）について

上記(1)～(6)について、事務局より資料に基づき一括して説明が行われた。

(7) 出席者意見開陳

上記(1)～(6)について、出席者から以下のような意見が述べられた。

- 前回の重点検査ではCやDが多かった各省庁が、全てA、Bランクになっており、きちんと対応していただいていると思う。しかし、具体的な項目を見ると、ウイルス対策ソフトを入れる、物理的に持っていられないようにするなどの基本的な項目が多いため、次のステップとしては、重点検査項目をもう少しレベルアップしていただきたい。
- 監視体制を強化していくと、細々とした管理が増えたり、書類が増えたりするなど、逆に雑務が増えてしまい、業務の効率化を妨げる可能性がある。情報セキュリティマネジメントのベストプラクティスの中には、手続きの煩雑化を削減できるような方法があるので、そういったものを他の省庁にも説明していただき、実際にマネジメントを作っていく中で、業務の効率化を妨げない方法を検討していただきたい。
- 政府機関の情報セキュリティマネジメントの状況報告を見ると、情報セキュリティ担当者の人事異動は1年から3年で行われているとのことであるが、官公庁の人事異動の周期というのは数年であるので、それに沿った状況であると思われる。しかし、数年で次々と担当者が変わってしまったら、情報セキュリティ担当としてのスキルアップができない。そこで、情報セキュリティ、情報システム等の担当者を各府省庁に共通な専門職にとらえ、府省庁横断的に人事異動をするようにし、その職務でずっとキャリアアップしていけるという形にするのが望ましいのではないか。
- 国際戦略にアジアというのが出てくるが、アジアの国々から見て日本のセキュリティ技術が役に立つ、相手国のニーズに合うという形で受け入れてもらえるようにしていただきたい。
- 情報セキュリティに係る技術開発に関連して、Winnyによる情報流出などいろいろな問題が発生し、その度に大きな騒ぎになるが、国民が使いやすい情報管理のツールが必要なのではないか。また、クレジットカードなどで偽造に悩んだが、世界に冠たる日本の技術で、偽造されない情報管理のできるカードを早急

に開発して欲しい。

- ファイル共有ソフトによる著作権侵害が非常に大きな問題である。ファイル共有ソフトによって著作権侵害が広く行われ、CDが売れなくなっているとか、映画がDVDで販売される前にインターネットで簡単に手に入るというような状況をどうするか、ということの前向きに検討をしていく必要がある。
- 政府機関の情報セキュリティマネジメントに関する評価結果を見ると、とても良い体制ができたと思うが、情報セキュリティのためには、毎日使っているコンピュータがきちんと管理されている、運用されているなどの日常的な努力が必要であることに留意する必要がある。人材の確保を含めた毎日の運用上の体制がきちんとできているかという項目を追加すると良いのではないか。
- 我が国には情報セキュリティ政策について、外国からの要求に対応した長い経験があり、その結果として、現在のNISCの機能がまとまった経緯がある。今では、国際戦略について、NISCができたことにより、外国から見ると、NISCに聞けばどこの省庁が何をしてくれるのかということが確認できるようになりということで、大変心強い体制になったと思う。このような我が国の実績を踏まえつつ、情報基盤が発展していく政策の確保と同時に、安心安全なセキュリティ政策の実現を、これからは、アジア各国に対して我が国がどのように貢献できるかということを国際戦略として検討する必要がある。
- 最近ではボットネットというものが非常に大きな影響を与えている。ボットネットは、ネットに繋がっている数百台から数万台のコンピュータを乗っ取って攻撃を行うため、それに対する技術の開発には、なるべく現実に近い環境での実験が必要であると考えられる。しかし、そのような環境を構築するためには、いろいろな官庁、大学、研究所等の協力を得て、数百台から数千台のコンピュータやサーバやパソコンをつなぎ、しかも、マルウェア等の害のあるものを流せるようにクロードな空間を作らなければならないため、政府による腰を据えた取り組みが必要であると考えられる。
- 情報セキュリティの国際的な戦略について、インフラを整備する場合、当初から情報セキュリティを確保していくことが必要であるが、現実的には、発展途上国の政府関係者や重要インフラ関係者が十分に理解していない場合が多く、知識の普及をなるべく理解しやすい形で行うことが必要である。対象国の政府担当者及び重要インフラの関係者を日本に招いて、実地見学や研修を行うなど、積極的かつ具体的な貢献を行うことを提案したい。
- 政府機関の情報セキュリティマネジメントに関する評価結果について、ベストプラクティスを積極的に取り上げたということは、情報セキュリティの担当者を

積極的に評価してあげること自体が励みになるので、非常に結構だと思う。ただ、積極的に取り組んでいる組織と、受け身で取り組んでいるのではないかという組織との間で差が広がって行くことを危惧しており、全体的な底上げを是非やっていただきたい。

- 重点検査と評価結果について、昨年に比べればきわめて良好であるということで、高く評価できると思う。ただ、総合評価というのは、実施率とか到達率の視点から実施、推進するものであり、重点検査項目を拡大していかないと停滞すると思うので、今後はこの拡大を是非やっていただいた上で、個々の情報セキュリティ対策の目標、目的に対応した到達率を含めた総合評価というものをする必要があるのである。重点検査の高い評価結果を継続していくことが必要であり、効果的な評価の実施をお願いしたい。
- 情報セキュリティ政策における「具体的な目標の設定」について、具体的な目標設定というのは、セキュリティ評価を進める上で、非常に重要な項目なので、PLANを立てるところで具体的な目標の設定がなされるべきであり、それに対応した対策をDOでやるのが筋ではないか。また、具体的な目標の設定というのが評価の段階で追加的に行われているように見えるが、一定のセキュリティ評価をきちんとやるためには、具体的な目標設定を今の段階でやるのは余り良くないのではないか。例えば、今回は暫定的な目標を設定し、次年度計画のPLANフェーズで今回の評価・分析結果を十分に考慮して、より現実的で具体性のある目標を再設定するのが良いのではないか。
- 国際協調・貢献について、国際協調・貢献ということにしていたのは非常に結構だと思うが、「国際戦略」と「国際協調・貢献」という言葉の間には、どうしても距離が感じられるため、ここでは「国際戦略」という言葉を使わずに「国際協調・貢献」とのみ表現して、その後に国際戦略を考えた方が良いのではないか。
- 電子政府等の情報セキュリティ強化と関係省庁との連携について、ベストプラクティスというものを決めて、それを共通的にしていく、そして色々なシステムを作るときにそのものを企画設計の段階から組み込んでいく、ということが大切だと思う。
- 国会でも電子申請の利用率が非常に低いということで、野党から相当な批判があった。使い勝手の悪さやニーズをうまく把握してないという面もあるが、なによりやはり大きいのは、セキュリティへの安心感が持てないという現状があるということなので、今後もこの政策会議とIT戦略本部との連携を深め、国民から信頼していただける電子政府の構築に努めたい。

- 現在、年金や健康に関する情報管理のための社会保障カード（仮称）導入を国民に対して約束をしている。時間もそう無いと理解しているので、予算措置も必要だと思うが、いろいろと知恵を出せる部署はあると思うので、内閣官房情報セキュリティセンターやこの政策会議の構成員の先生方、総合科学技術会議など政府一体で体制を整備し、強力にこの研究開発や実証などに取りかかるべきである。
- IT基盤はもともとボーダレスであるから、情報セキュリティ対策は国際的な取組みが重要だと自覚をしている。今後、国際戦略、国際協調・貢献の具体的な政策を検討していく過程で、情報セキュリティ基本計画に基づいて実施してきた成果を国際基準作りやいわゆる重要インフラの国際ネットワークの保護に活かしていくことが大切であると考えており、今後、各省の個々の政策とのつながりをよく見て、内閣官房や関係省庁と協議させていただきながら進めていきたい。
- 技術戦略専門委員会の報告書に関して、情報通信ネットワークの安全、そして信頼性確保のためにも情報セキュリティ技術の発展が不可欠であるとする。これまで総務省では、情報通信研究機構（NICT）において、サイバー攻撃対策技術等の開発を行っており、引き続き安心、安全なインターネット社会の実現に向けて情報セキュリティ対策の技術をはじめとした研究開発に積極的に取り組んでいきたい。
- マネジメント評価について、総務省では、今回のベストプラクティスとして紹介されたeラーニング、こうしたものを始め、各種マネジメントへの取組みを進めており、今後とも積極的な取組みを行っていく。
- 情報セキュリティ対策の具体的目標について、政府機関については、この対策の統一基準を2008年末までに100%実施とあるが、総務省としても、最高水準の情報セキュリティを実現するために今後とも努力をしていきたい。また、重要インフラにおける具体的目標については、安全基準等の策定や情報共有体制の整備などを進めてきているところであり、引き続き、この重要インフラ部門の情報セキュリティ対策については、精力的に取り組むとともに、国際協調・貢献にも積極的に努力していきたい。
- ITが国民生活の基盤となる中で、安全、安心な暮らしを作るためには、情報セキュリティの確保が不可欠である。本年5月に経済産業省では、情報セキュリティ分野での国際貢献に積極的に取り組むため、「グローバル情報セキュリティ戦略」をまとめたが、今回、本政策会議で、情報セキュリティ分野における国際協調・貢献を取り上げることは、大変時機を得たものであると考えている。アジア地域における情報セキュリティ警戒体制整備への貢献や国際標準化への取組み強化など、我が国企業や国民が、ITを安全、安心に利用できるよう取り組んでいきたい。

- 情報流出事案を受けて、防衛省としては、情報セキュリティ対策に真剣に取り組んでいるところであるが、今般報告があった、端末とウェブサーバに関する情報セキュリティ対策の総合評価については、昨年度の対策状況から大幅な改善が見られた。また、政府機関の情報セキュリティマネジメントに関する評価については、当省の外部委託における取組みがベストプラクティスとして評価されたことは、大変光栄であると考えている。各府省庁においても、W i n n y などのファイル共有ソフトを介した情報流出が喫緊の課題であると承知しているが、防衛省においても、全職員一丸となって情報流出対策に取り組んで行くところであり、当省のこれまでの取組みが少しでも各府省庁の情報流出対策の参考となるのであれば、協力は惜しまない。今後とも、情報セキュリティ関係省庁として、内閣官房の指導も踏まえつつ、政府全体の情報セキュリティ水準の向上に協力したいと思っている。
  
- 本年1月に中国が衛星の破壊実験を行ったが、将来、通信衛星に対する脅威は、かなり高くなると考えており、そのなかには、物理的に破壊されるだけでなく、故障や電子的に乗っ取られるということも考えられる。今までは地上のインフラが駄目になった場合に衛星を利用するという考え方だったが、逆に衛星のインフラが駄目になった場合の局地的な代替通信手段を検討する必要があるのではないか。