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 11 回会合 議事要旨

1 日時　平成 19年4月 23 日(月)　18:30～19:30

2 場所　総理官邸大会議室

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)
溝手 顕正	国家公安委員会委員長
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
	(※山本 幸三 経済産業副大臣代理出席)
柳澤 伯夫	厚生労働大臣
	(※石田 祝稔 厚生労働副大臣代理出席)
冬柴 鐵三	国土交通大臣
	(※梶山 弘志 国土交通大臣政務官代理出席)
久間 章生	防衛大臣
	(※大前 繁雄 防衛大臣政務官代理出席)
小池 百合子	内閣総理大臣補佐官
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
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	慶応義塾大学教授

(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
坂 篤郎	内閣官房副長官補
栁澤 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)　政府機関統一基準の改訂案について
(2)　重要インフラの情報セキュリティ対策について
(3)　2006 年度の情報セキュリティ政策の評価等について
(4)　セキュア・ジャパン 2007（案）について
(5)　情報セキュリティ対策推進会議の設置規程改正について

上記（1）～（5）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。

(6)　出席者意見開陳

上記（1）～（5）について、出席者から以下のような意見が述べられた。

○　情報セキュリティに関する脅威は日々の変化が激しいので、その対策を常に考えていく必要がある。そういった意味で、重要インフラにおける情報セキュリティ対策として CEPTOAR の取組みは非常に重要だと思う。
　重要な1件のトラブルには、300 件ぐらいの「ヒヤリ」とした経験があると言われている。そのことを考慮すると、CEPTOAR においては、「何をどう報告するのか。」ということと同時に、「失敗をとがめない。」という態度が必要だと思う。特に、政府とCEPTOARとの関係については、そういう姿勢でよく検討を進める必要がある。

○　我々がグローバルに仕事をする場合、ISMS など欧米で作られた基準を使うことになるが、日本にも評価の高い基準はあるので、それを海外に普及させていくべきである。現在、経済産業省でもセキュリティの国際化について検討されているが、是非、対等の関係に持っていけるように互いに努力したいと思う。

○　第1次情報セキュリティ基本計画では、2008 年度中に目標を達成できるようにということであったが、特に、政府機関と重要インフラの分野において、「今のペースで目標を達成することができるのか。」と疑問を感じる部分がある。例えば、事務局より説明があった、各府省庁の対策実施状況の報告においては、実態把握という調査の趣旨を正しく理解しているとは思えないように見受けられる省庁もいくつかあった。さきほど、「失敗をとがめない。」という話もあったが、まずは、実態をしっかりと把握して、良い点も良くない点も分かった上で、問題点を明確化していけば、きちんと弱点を評価できると思うので、是非、趣旨を再確認して、実質的な情報セキュリティ対策ができるように取り組んで欲しいと思う。

○　「セキュア・ジャパン２００６」の評価である資料４－２を見ると、各対策実施領域

における現状の評価が書いてある。企業・個人においては、調査に基づき、客観的なデータやアウトカム指標によって、対策がどの程度進んだのかという評価が行われているが、政府機関や重要インフラにおいては、客観的な評価データが極めて少なく、対策を実施したか否かというような形での評価が中心となっており、残念だ。PDCA サイクルをきちんと回すためにも、できるだけ客観的なデータをとって評価を進めて欲しい。

○　経済産業省の産業構造審議会の情報セキュリティ基本問題委員会において、今後、情報セキュリティに関する脅威が国際化していく傾向にあり、国際連携が非常に重要になっていくという趣旨で、「グローバル情報セキュリティ戦略」をとりまとめた。「セキュア・ジャパン 2007（案）」においても、第6章の重要施策の方向性を見ると「情報セキュリティ政策の国際展開に向けた集中的な取組み」が取り上げられているが、各府省庁の取組みとも連携して進めて欲しい。

○　「セキュア・ジャパン 2007（案）」においても取り上げられており、また、2008 年度の柱にもなっている情報セキュリティ人材の育成・確保については、それが重要だということで、これまで議論をしているが、そろそろ次の段階、具体的に人材をどう供給するのかということに加えて、その人材をどう運用するのかということについて検討する必要がある。とりあえずは、色々なレベルで、人材をどう作っていくのか、その人材をどう登用するのかということや資格についての問題を具体化し、それを視野に入れた具体的な対応策をお願いしたい。

○　我が国は非常に安心で安全な社会を作ることに成功したと思う。2002 年以降、ものすごい勢いで犯罪は減少している。しかしながら、先日の内閣府の調査でも、犯罪に遭うかもしれないと不安になる場所として「インターネット空間」を挙げた者の割合が最も増加している。やはり、ヴァーチャル社会についても、国民が安心して使えるようなものにしていく取組みを進めていただきたい。特に、ネット社会におけるコンテンツの問題について、もう一歩踏み込んだ議論を 2008 年度に開始して欲しい。憲法的な観点とか色々な問題はあるが、もう一歩前に進む段階に来ていると思う。今日の事務局からの報告を見ると、個々の組織の取組みはうまくいっていると思うので、それを生かしヴァーチャル社会における問題点の解消に向けたリーダーシップを発揮していただきたい。

○　今日の事務局の説明にあった、政府機関統一基準、重要インフラにおける情報セキュリティ対策、情報セキュリティ政策の評価、「セキュア・ジャパン 2007（案）」については、ようやく落ち着いて実現できる体制ができたという印象を持っている。

○　内閣官房に情報セキュリティセンターができて今のような政策推進の形ができてきたので、イベントドリブンという視点を持つことを考えていただきたい。過去の話をすると、2000 年問題のとき、情報システムが機能しなくなる恐れがあったため、事前に様々な対策をとったことがあった。当時は、内閣官房情報セキュリティセンターが無かったので、官民の自律的な努力で非常に大きな体制を作って対応した。さらに遡ると、長野オリンピックを開催したときに、大規模なウェブや情報システムを官民の力を合わせて支えた。また、ワールドカップをきっかけとして、いろいろなことが見直された。当時は、情報システムについて日本がどのくらい発展しているのかということをアピールするタイミングであった。今後、サミットやオリンピックが開催されることになるが、内閣官房情報セキュリティセンターは、その種のイベントに対して、どういう方面でどういう対策ができるのかという視点で動くための体制を持つべきである。具体的な課題を持って、それに対して対応できる体制を作っていただきたい。

○　情報セキュリティについては、その性質上、個人の力が非常に大事である。情報セキュリティで安心･安全を作るためには、「誰かが守ってくれる。」ということだけでは不足であり、一人一人が前向きに自信を持って対応をしなければならない。ネットワークは、個人の範囲に穴があれば全体に迷惑がかかるという性格を持つので、個人の力が喚起されなければならない。また、この種の問題が暗いことであると思われると少し困るところである。個人の範囲での情報セキュリティ対策の底上げのためには、「自信を持って明るく対応できる。」というアピールなど、個人に向けたメッセージなども大事になると思う。個人個人が安心と自信をもって自分の役割というのを認識できるよう、CEPTOAR のホームページなどの軸を含めて、一人一人が前向きに対応できるアピールの方法を考えて欲しい。

○　一般的には、サイバースペースが、今我々が生活している三次元空間と同じものだという認識で使われていることが多い。実は、そういうような状態になっているのが一番いいとは思うが、実際はかなり性格が違っており、情報が瞬時に伝わり、空間と時間という概念がほとんどない。したがって、「サイバー空間は、普通に生活している空間とは違うものである。」という教育を徹底する必要があると思う。

○　最近、政府でも色々な情報流出事案が見られるが、基本的に情報流出の完全防止は不可能であると思う。そこで、政府や重要インフラの情報で、一般的に広く流してもらって困るというようなものがあるのであれば、全て暗号化した方が良いと思う。その際、警察庁や防衛省の取組みが参考になるとは思うが、各府省庁がそれぞれバラバラに暗号化すると、様々な暗号が出てくることになり面倒なことになる。暗号を一つに統一するというのは難しいとしても、政府機関統一基準の改訂案にある、暗号化の運用･管理方法の明確化をできるだけ早く実現し、情報

が流出しては困るものは全て基本的に暗号化するという方法をとるべきである。

○　さきほどの話にもあったが、国際的なところで、我が国が主導的な役割を果たすということが必要だと思う。「セキュア・ジャパン　2007（案）」では、国際的な情報セキュリティ強化の具体的な第一歩として、アジア・太平洋地域ということをうたっているが、その体制構築に向けて日本が積極的な役割を果たすべきである。ASEAN+やAPECなどの場で、日本が会議議題という形で提案すると世界各国の印象がかなり良くなる。具体的な例としては、つい先日、国連の安全保障理事会で、環境問題が安全保障で必要だということが取り上げられたということがある。具体的には、ASEAN＋やAPECだけではなく、各国政府のITセキュリティ担当者を集めたシンポジウムを政府主催で開催してはどうか。そうすれば、各国の情報セキュリティに対する姿勢を把握することができ、どこをどのようにすれば良いのかということが分かるようになると思う。

○　新しい技術の研究開発についてだが、インターネットというものは、もともとセキュリティのことを全く考えずに作られたものであり、非常に脆弱なものであるので、根本的に安全なシステムを開発するということであれば、できれば今の非常に脆弱なものにとって代わるようなものを、日本が世界を主導するつもりで開発していってもらいたいと思う。そのためには、少しでも柔軟な提案、感覚、独創性が必要であるので、従来の慣習にとらわれない柔軟な研究開発態勢を取って欲しい。

○　4月5日にIT戦略本部において、IT新改革戦略の政策パッケージを策定した。この中には、どこに引っ越してもワンストップでいろいろな登録ができるようなサービスや、医療情報や社会保険情報等を個人が管理できるようなITの活用を図るための国民と地方の包括的な電子サービスの実現を始めとしたもろもろの政策が盛り込まれたが、これらの実現のためにも、また、国民の理解を得るためにも、情報セキュリティの問題は非常に重要になるので、「セキュア・ジャパン　2007（案）」の中で、「電子政府等の情報セキュリティ強化に向けた総合的な取組み」をこれからの重点施策の一つとして位置付けていただくことに関しては大変ありがたい。

○　今回、各府省庁の取組みの状況の調査の報告もあったが、去年の12月に内閣府のパソコンから海外のウェブサイトに個人情報が流出したということがあった。即座に内閣府の各部局で同様な事例がないかチェックすると共に、官房長官の御指導のもと、すべての省庁で同様の事例が発生しないように対応をしてもらった。どれだけ技術的に成熟しても、いろいろな仕組みを作っても、人の問題が大事だと思う。

○　官房長官の御指示で、情報セキュリティセンターから再発防止のためのマニュ

アルを全府省庁に送ってもらったが、できれば、今後各府省庁で情報の流出が起きた場合には、全て速やかに情報セキュリティセンターに報告をして欲しい。隠すのではなく、報告をして一刻も早く再発防止策をとる。このような形を徹底すべきである。今日の報告を見て、その思いをさらに強くしたので、こういった取組みを進めて欲しいし、私自身もそのために努力をしたいと思っている。

○　情報流出のほとんどは、Winny によるものであるということは分かっているが、データを消去できていないのに消去できたと思っているなど技術的に未熟であることや、Winny を利用して入手できる情報がより魅力的であるために隠れて Winny を使うというような極めて人間的なことが、情報流出が続く原因になっている。システムとしては完璧だとしても、それをきちんと運用していないというところが、Winny に関しての一番大きな問題であると思う。

○　サイバー犯罪の取締りについては、強力に推進しているところであり、検挙件数は年々増加している。平成 18 年の検挙件数は 4,425 件であり、平成 13 年に比べて3倍以上になっている。内容を見てみると、インターネット・オークションを利用した詐欺を中心に、身近な犯罪が多発しており、手口の面でも、フィッシングやスパイウェアによる ID・パスワードの入手と、サイバー空間の特性を利用した犯罪の高度化が伺える。これについては、我々の捜査能力をいかに向上していくのかという体制強化のほか、個々のインターネット利用者の情報セキュリティ対策の確実な実施が必要であると思う。

○　警察としては、高度な技術を持った警察職員の育成・教養と、合同・共同捜査やデジタルフォレンジックの活用による的確な捜査を推進していきたい。また、インターネット・オークションにおける代金の支払いシステムの改善や、インターネット・カフェやプリペイド式データ通信カードの利用者の本人確認制度の実施等、インターネットの信頼性向上に向けた関係事業者に対する働きかけが必要だと思う。特に、インターネット・カフェについては、未検挙になっている不正アクセス事犯の約半数が、本人確認を行わない店舗からのアクセスであり、本人確認を確実に実施していただく必要があると考えている。さらに、市民や企業に対する、ID・パスワードの適切な管理、最新のウイルス対策ソフトの利用等についての広報啓発に努め、インターネット利用者のセキュリティ向上に努めていきたいと考えている。

○　暗号化の問題については、新年度から、逐次、警察庁のデータは暗号化していく。さらに、データが警察庁を一歩でも出た場合には全て暗号化できるようなシステムを現在開発中である。

○　厚生労働省に関係する重要インフラ分野としては、医療及び水道の分野があ

るが、両分野とも、安全基準等の策定・見直しについては 2006 年度末までに必要な対応を行った。また、CEPTOAR についても、2007 年度中の整備に向けて必要な調整を行っている。今後とも、医療及び水道分野について、安全基準等の更なる改善、情報共有・分析機能の整備等にしっかりと取り組んでいきたい。

○ 経済産業省としては、基準や情報の格付け等について、官房長による文書を発出して一層の徹底を図っていきたい。また、重要インフラ分野である電力及びガスの分野を所管しているので、重要インフラ対策もしっかりやりたいと思っている。

○ 経済社会のIT化・グローバル化が進み、また、情報セキュリティに関する脅威も多様化・国際化が進んでいることを踏まえ、産業構造審議会の情報セキュリティ基本問題委員会において、本年3月に、「グローバル情報セキュリティ戦略」の案をとりまとめた。「グローバル情報セキュリティ戦略」では、3つの戦略の下に60の施策を整理しており、先ほど話が出た日本の基準を国際基準にするという施策も盛り込まれている。関係省庁と協力しながら、この戦略に掲げられた施策をしっかり取り組んでいきたい。

○ 総務省は、安全・安心な ICT 社会づくりを通して、情報セキュリティ先進国の実現の一翼を担っており、2006 年度については、総務省所管の情報通信分野・地方公共団体における安全基準等の策定、CEPTOAR の設置、また、個人等への情報セキュリティ対策の周知・啓発等、情報セキュリティ基本計画の実施の初年度にあたる様々な取組みを実施してきた。

○ 2006 年度の情報セキュリティ政策の評価等については、今後の施策展開にいかす重要な機会であると認識しており、総務省としても、真摯に受け止め、活用していきたい。その際、総務省所管の施策分野の対策と併せて、各府省庁の対策実施状況報告において示された当省自らの情報セキュリティ対策についても、今回の指摘を踏まえて、一層きめ細かく取り組み、全職員に対してその徹底を図っていきたい。

○ 総務省では、「セキュア・ジャパン 2007」に基づいて、ネットワークのIP化に対応した電気通信システムの安全性・信頼性の確保や、自治体に対する情報セキュリティ研修などの各種施策に取り組み、情報セキュリティの向上に積極的に貢献していきたい。

○ 国土交通省においては、情報システムの障害に起因する行政サービスの低下の防止、鉄道・航空等国土交通分野の安全かつ安定的な事業経営を確保する

ため、政府全体の指針に基づき、各種情報システムについて、セキュリティ対策に取り組むとともに、所管事業者に対しても対策の推進を強く指導していくつもりである。重要インフラである鉄道・航空・物流分野については、今回報告のあった、情報セキュリティ確保のための安全基準等の策定、各重要インフラ間における情報共有・分析機能の整備等、情報セキュリティ確保のために必要な措置を関係事業者と連携しつつ鋭意講じてきているところである。

○　国土交通省における情報セキュリティ対策についても、「2009 年度初めには、すべての政府機関において政府機関統一基準が求める水準の対策を実施している」という目標の実現に向けた施策を、省を挙げて取り組んでいるところである。経済社会のIT化が進展し、経済社会活動全般の情報システムへの依存度が非常に高まっている現状にかんがみると、情報システムのセキュリティ対策の強化は極めて重要であると認識しており、国土交通省としても、内閣官房のほか、関係省庁とも密接に連携しつつ、引き続き、情報セキュリティ対策の強化に努めていきたい。

○　防衛省としては、昨年の情報流出事案を受け、抜本的対策等をとりまとめて再発防止に取り組んできたところだが、今般、海上自衛隊が秘密の疑いがある情報を自宅で保有していた事案が明らかになったことは、誠に遺憾であると考えている。再発防止のためには、抜本的な対策等が迅速かつ着実に推進され、省内への浸透が図られることが重要であると考えているが、防衛大臣が先頭に立ち、情報流出の防止に取り組むこととしている。また、内閣官房の指導も踏まえ、政府機関の情報セキュリティ対策のための統一基準に示された各種の情報セキュリティ対策の実施にも引き続き取り組んでいきたい。防衛省として大臣のもと一丸となって、情報流出事案の再発防止に取り組み、信頼回復に努めていく。

(7)　政策会議決定等について

「政府機関の情報セキュリティ対策のための統一基準（第2版）（案）」、「重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針（改定案）」及び「セキュア・ジャパン 2007（案）」について、パブリック・コメントに付すこととされた。また、情報セキュリティ対策推進会議の設置規程について、資料5の案のとおり改正することとされた。

－ 以 上 －