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15回会合　議事要旨

１　日時

平成19年12月12日（水）17：20～18：20

２　場所

総理大臣官邸４階大会議室

３　出席者（敬称略）

町村　信孝	内閣官房長官
岸田　文雄	内閣府特命担当大臣（科学技術政策）
泉　信也	国家公安委員会委員長
増田　寛也	総務大臣
	（※岡本　芳郎　　総務大臣政務官代理出席）
甘利　明	経済産業大臣
	（※山本　香苗　　経済産業大臣政務官代理出席）
石破　茂	防衛大臣
	（※寺田　稔　　防衛大臣政務官代理出席）
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）

二橋　正弘	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
坂　篤郎	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) 政府機関の情報セキュリティ対策について

○　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

○　「情報セキュリティの観点から見た行政情報システムの望ましいあり方」と「行

政情報システムの企画・設計段階からのセキュリティ確保に向けた取組み（セキュリティ・バイ・デザイン［ＳＢＤ］）」について

○　政府機関統一基準の改訂について

(2) 次期情報セキュリティ基本計画（仮称）の検討について

(3) その他

○　平成19年度情報セキュリティの日について

○　静的相互依存性解析の総括について

上記(1)～(3)について資料を配付、(1)及び(2)については、事務局より一括して説明が行われた。

(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。

○　事務局説明で言及されていた IPv6 は、今や実用技術として使われはじめているが、この技術は日本で開発が進められ、政策的にも日本が2000年から推進してきたものである。IPv4 のアドレスは2010年に無くなると予測されている現在、我が国の IPv6 対応は国際的に期待され、注目されている。この IP アドレスの枯渇が起こった場合、中国が一番被害を受けることになる。また、アメリカにおいては、DoD の政府調達品の要件に IPv6 対応を求めるという積極的な取り組みを行うなど、EU とともに政策的対応を行っている。

○　私は我が国の IPv6 普及・高度化推進協議会の会長をしているが、世界中から IPv6 対応のアドバイスを求める声が相当数届いている。その中で特に情報セキュリティとの関連での先導性は明確な責任としてあり、今後、日本としても、行政システムにおける IPv6 の実用化など積極的に取り組むべきではないか。世界の現状では、DNS における名前問い合わせ要求においては、10%を超える IPv6 の問い合わせとなり増加の一途である。このように、既に IPv6 は一般的に使用されている技術であり、決して将来の技術ではない。この委員会の参加者はこの点を認識し、情報セキュリティの面で対処していただきたい。

○　現在の IPv4 と IPv6 が混在するようになったとき、セキュリティホールが生じてしまうと問題であるが、今度の統一基準改訂案では、そのことについてもきちんと言及したという印象を持った。

○　最近、衛星による位置情報システム（ＧＰＳ）への依存度が高まっており、日本では、ほとんど重要インフラ化しているのではないかとの印象を持っている。確かに、非常に便利なシステムではあるが、米国で構築・運用されている軍事的なシステムであり、何かがあった場合には使えなくなる可能性もある点には留意しておく必要がある。

○　外国のシステムに日常生活が深く依存するというのは、非常に危険がある。日本独自のシステムを持った上で、外国のシステムをバックアップとして使うのが本来の姿である。

○　最近は様々な形でサイバー攻撃が行われているが、ＥＵではこの問題に対処するためにサイバー犯罪条約を成立させ、米国もこれを批准している。我が国では、国内法が未整備のために未だ批准をしていない状況であるが、この問題に対する日本の積極的姿勢を示すためにも、早期に批准できるようにする必要がある。

○　サイバー犯罪条約から一歩進んで、サイバー攻撃手段によるネットへの攻撃を禁止する国際条約、制裁措置も有する条約が制定されれば、それがかなり抑止力になる。条約制定に向けて、日本が主導的な役割を果たす方策も、一つの可能性として検討していただきたい。

○　セキュリティ・バイ・デザインを官民共通で推進することにより、セキュリティに関するコストが下げられるのではないかと考えている。また、情報システム全体のセキュリティレベルの底上げも可能であり、運用段階においては、発見される脅威に対し、迅速な対応が可能になるのではないかとも考えている。

○　セキュリティ・バイ・デザインについては、民間も既に導入しているが、担当者の資質によってその内容に差があるということも理解している。官民共通のセキュリティ・バイ・デザインを確立することにより、社会インフラとしてのコストを下げることが可能になると考えるので、一時的には導入のためのコストがかかるとしても、是非取り組んでいただきたい。

○　基本計画の検討項目として、個人の利用状況の変化への配慮という記載があったが、個人の利用状況について特筆すべきものとして、未成年者が有害サイトを通じて犯罪に巻き込まれるケースの増加があり、我々としても、フィルタリング関係の強化によってこれに対応しているところである。この問題に関しては、セキュリティのための規制とコンテンツ開放との整合をいかに取るのか、個人については未成年者と成人を分けて考える必要があるのではないか、という重要な課題が存在すると考える。

○　次期基本計画においては、これらの課題に対し、政策的にどう対応していくのかと言うことを是非考えていただきたい。制度面の問題の解決とコンテンツ産業の育成の両面を推進していただきたい。

○　電子メールサーバの重点検査は、大変良い取組みであると考える。

○　評価結果を受けた対応について、各省庁から報告されているが、情報漏えいのリスクの低減とサーバの管理工数・コストの低減の観点から、やはりサーバ集約を進めるべきであると考える。

○　情報システムの開発にあたっては、システムで実現したい要件を定義しなければ、正しいシステムは開発できない。この観点からいうと、セキュリティ・バイ・デザインは、情報システムにセキュリティ機能を正しく組み込むためのルールであると考えるが、各府省庁がシステム開発をする時には、このルールに従って、システムの企画段階からセキュリティを意識して定義することが、非常に重要であると考える。

○　セキュリティ・バイ・デザインの推進は、セキュリティの透明性あるいは効率的なシステムの管理にも有効であり、これを是非進めるべきであると考える。

○　次期基本計画の検討に際しては、中小企業における問題や、自動車におけるＩＴＳ等新しいＩＴ技術の普及などを踏まえた新しい視点からの検討も必要なのではないかと考える。

○　セキュリティ・バイ・デザインについては、非常に重要であると考えるので、是非しっかり取り組んでいただきたい。

○　各府省ＣＩＯ連絡会議の方で「業務・システム最適化指針」を出し、情報システムの構築について検討していると聞いているが、それとバラバラに走ることがないよう、是非連携を取っていただきたいと考える。

○　官民共通のセキュリティ・バイ・デザインの確立という御意見があったが、そのような形になるよう、推進していただければと考える。

○　次期基本計画の話があったが、来年度は現在の第１次情報セキュリティ基本計画の最終年度に当たるので、そこに掲げた目標の達成に向けて引き続き頑張っていただきたい。

○　第１次情報セキュリティ基本計画では、統一基準の策定など、まずはやらなければいけない基本的なところから取り組んだと考えているが、今後は更にもう一歩踏み込んで、実質的改革に取り組むことが必要であると考える。例えば、行政情報システムの企画・仕様検討・予算獲得・発注業務を行う実務担当者や情報セキュリティ担当者のキャリアパスについて検討することや、重要インフラにおける連携体制が自律的に推進されるような仕組みづくりが考えられる。

○　他の構成員からも御意見が出ていたが、個人向けの対策のうち、未成年者をどう

やって有害情報から守るか、普通の子供が容易にアクセス出来るという状況をどうやって改善していくべきかということは、検討するべきであると考える。

○　第１次基本計画を踏まえて次期基本計画を策定するに際し、第１次基本計画の成果をきちんと評価することが重要であると考える。そして、その成果は積極的に評価すべきであり、例えば、統一基準が策定され各府省庁がこれに基づく取組みを行っているということは、今までの内閣官房と各府省庁の関係からは画期的であり、高く評価するべき。

○　内閣官房と各府省庁との関係で注意すべき点は、内閣官房と各府省庁が主体的につながっているということである。これが、内閣官房主導のものを全府省庁に下ろしていくという形に見えてしまうと、非常に危険である。セキュリティ・バイ・デザインは、合理性があり内容について異存はないが、やり方を誤ると、内閣官房主導のものを全府省庁に下ろしていくという形に誤解される恐れがある。

○　各府省庁の個性も踏まえつつ、専門の観点から、システムの設計当初からチェックすることを可能とする統一基準を示し、各府省庁の主体的な取組みを促すようなやり方が良いのではないかと考える。

○　裏職業サイトの問題やインターネットを利用したいじめの問題など、総理大臣も発言しているが、非常に重要な問題であると考える。官民の努力により、二、三年前に比べれば大幅に対策が進んでおり、これは高く評価すべきであるが、更に対策を進めていただきたいと考えており、基本計画検討委員会でも取り上げて欲しいと考える。

○　本日、セキュリティ・バイ・デザインの取組みについて報告がなされたが、私が担当しているＩＴ戦略の分野においても、現在、電子政府の構築について、取り組んでいるところである。そこでは、利便性は勿論大切であるが、情報セキュリティを確保することが大前提であるということは、言うまでもないことであると考えている。

○　引き続き、ＩＴ政策全体と情報セキュリティ政策との連携を深めつつ、役所の側だけではなく、国民の視点に立った電子政府の実現を進めて行きたいと考えている。

○　次期基本計画の検討がスタートする訳だが、私が担当するＩＴ政策や科学技術政策などの様々な視点から、ＩＴが持つ力を最大限に活用しつつも国民の安心を確保できるよう、この次期基本計画の検討を行っていきたいと考えている。

○　警察庁では、政府機関統一基準を踏まえた警察庁セキュリティポリシーを定め、情報セキュリティ対策の推進に努めてきたところであり、その結果、重点検査では

高い評価をいただいた。しかし、その結果に慢心することなく、引き続き、情報セキュリティ対策の推進に努めたいと考えている。

○　警察では、第１次情報セキュリティ基本計画に基づき、サイバー犯罪の取締りのための体制の強化、デジタルフォレンジックの活用等による捜査の推進、サイバーテロへの対処能力の向上等、安全・安心なインターネット社会の実現に向けた取組みを推進しているが、次期基本計画の策定に向けた検討についても、第１次情報セキュリティ基本計画策定の際と同様、積極的に協力していきたいと考えている。

○　次期基本計画の策定に向けた議論が開始されるとのことであるが、携帯情報端末の更なる高度化など、今後国民生活や社会経済活動の基盤であるＩＣＴの重要性が増すなか、総務省でも本年10月に「次世代情報セキュリティ政策に関する研究会」を立ち上げた。

○　この研究会では、３年から５年後といった将来の情報通信環境の変化を想定し、生じるであろう情報セキュリティの課題・脅威を分析した上で、重点的に取り組むべき対応策についての検討を開始している。今後とも、安全・安心な情報通信環境の実現に向けて、政府の情報セキュリティ政策に貢献していきたいと考えている。

○　我が国の企業は、アジアを中心にますます国際的に活動を広げているが、このようななかで、グローバル化した経済・社会の一員として、また、我が国企業を支えるという観点からも、情報セキュリティの分野で積極的に国際協調・貢献をしていくことは、我が国政府の責務だと考えている。こうした考え方を踏まえて、次期基本計画を策定していただきたい。

○　経済産業省では、従来から安全なＩＴ製品の評価手法を研究してきているが、セキュリティ・バイ・デザインの取組みとして、今後、政府横断的なシステムのチェックリストを作成していく際には、そこで研究してきた成果である評価のノウハウや技術的知見を提供するなど、積極的に経済産業省としても協力したいと考えている。

○　防衛省では、先般の情報流出事案等を受け、省内において情報流出対策会議を設置し、討議を行っているところである。当省での対策の一つとして、特別行動チームを設置し、全国の部隊への情報セキュリティ対策の徹底に努めたところである。

○　電子メールサーバの対策実施状況について、当省の評価はＡということであったが、電子メールは、サイバー攻撃等の手段としても大変利用されやすく、これを取り扱うサーバの脆弱性の問題も指摘のとおりであることから、当会議及び官邸において設置された防衛省改革会議とも十分連携を取り、引き続き万全の対策を取っていきたいと考えている。

○　サイバーテロ対策については、我々も最重要の課題として取り組んでおり、平成19年度末には、現在、統合幕僚監部内に、サイバー攻撃対処などの任務を持つ自衛隊指揮通信システム隊（仮称）を新編する予定である。また、ＮＩＳＣ及び関係省庁とも十分連携を取って、情報セキュリティ対策を進めたいと考えている。

○　技術は継続的に発展するため、常に完全な情報セキュリティを保つことは、なかなか難しいかもしれないが、それを常に保ち続けていく体制作りが必要になる。

○　８月の検査結果及び今回の検査結果がいずれも「B」であったところには、より積極的な取り組みを行うよう、情報セキュリティセンターから積極的に働きかけていただきたい。

○　情報セキュリティ対策の難しいところは、時間の経過に従って対策の有効性が劣化していくことである。よって、最高の情報セキュリティレベルを維持するためには、現在の対策を常に見直し、レベルを最高水準に合わせる努力をしなければならない。セキュリティ・バイ・デザインなどもきちんとやっておかないと、統一的な情報セキュリティ水準の維持は難しいと考える。

○　数年に一度ではなく、毎年検査しなければならないと考える。

○　評価が良いとそれで油断してしまうこともあるので、検査を継続し続ける体制作りが出来るかどうかが重要である。

○　違法有害情報対策としてのフィルタリングは、ここ数年で非常に進歩したが、改善の余地はあると考えている。この問題は、色々な会議でも話題になっており、国民の声であると思う。

○　コミュニティサイトの中で何気なく交わされている情報の中に違法有害情報が含まれることもあるので、フィルタリングという技術的対処だけでは解決しないと考えている。

○　フィルタリングは、何かおかしいものが検出された時点で適用することになるため、一旦は情報がユーザーに届くことになる。しかし、本当に安全なものしか見せないという方法もあるかもしれないが、別の面で問題がある。

○　違法有害情報の問題は、どういう情報が問題なのかと言う教育の問題などと一緒にやっていく必要があり、技術的対処だけでは難しい。

○　若い世代の好奇心の問題、新しいものに対して興味を持つことも重要である。

「リスクがあるから気を付けなさい。」という教育と、新しいものに興味を持つことを奨励する教育とのバランスが重要である。

○　これまでは、全通信に対する表現の自由という考え方が強く、大人と子供でコンテンツを分けるという発想がなかった。勿論、若い世代はインターネットに強くあるべきであり、インターネットに強い関心を持つべきであるが、コンテンツの中味については、教育の観点から真剣に検討すべきであると考える。

○　低年齢化の問題もあり、違法有害情報については何らかの法律が必要なのだろうか。

○　「有害」の内容は、対象との関係で決まるため、何を有害と明確に定義するかという難しい問題を避けて議論できない。

○　違法有害情報については、基本的には、一人一人が自分で判断できるように教育することが重要。ただし、年齢によっては、守らなければならない部分もあると考えている。

○　子供の携帯電話の問題については、国際的にも日本が一番進んでおり、日本の状況をみて外国がどうするかを考えているような状況である。

⑸ 政策会議決定

「政府機関の情報セキュリティ対策のための統一基準（第３版）（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、「基本計画検討委員会」の設置について、政策会議決定とした。

－ 以 上 －