

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22会合 議事要旨

1 日時

平成21年6月22日(月) 17:20~18:15

2 場所

総理大臣官邸4階大会議室

3 出席者(敬称略)

河村 建夫	内閣官房長官
野田 聖子	内閣府特命担当大臣(科学技術政策)
佐藤 勉	総務大臣
	国家公安委員会委員長
二階 俊博	経済産業大臣
	(※谷合 正明 経済産業大臣政務官代理出席)
浜田 靖一	防衛大臣
	(※岸 信夫 防衛大臣政務官代理出席)
小野寺 正	KDDI(株)代表取締役社長兼会長
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	首都大学東京法科大学院教授
村井 純	慶應義塾大学教授

(上記のほか以下が出席)

漆間 巖	内閣官房副長官
伊藤 哲朗	内閣危機管理監
柳澤 協二	内閣官房副長官補
福田 進	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) 「セキュア・ジャパン2009(案)」に対する意見募集の結果及び「セキュア・ジャパン2009」の決定について(決定)
- (2) 政府機関におけるサーバ集約化について(決定)
- (3) 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」策定にあたっての指針の見直しについて(報告)

上記(1)~(8)について、資料を出席者席上パソコンに表示の上、事務局から説明が行われた。

#### (4) 出席者意見

上記について、出席者から以下のような意見が述べられた。

前回報告があった政府機関のWeb改ざん等により、ガバナンスや危機管理が未だ不十分であるとのことから、その取り掛かり、具体的な取組みとしてサーバ管理の合理化が必要であるということには納得がいく。速やかな対応が望まれ、今回の対応はかなり評価できる。この件については賛成である。

ICT社会の発展では、伸ばしていかなければならないプラスの面があり、正義の力を超えてネットが社会を大きく動かしていくということはそのとおりである。その影の面として、今国会でも話題になると思われるが、日本では、特に国際的な配慮の意味でも児童ポルノ問題の議論が続いている。世界的にみて、日本とロシアが遅れている。表現の自由や通信の秘密等の様々な問題がある中で、やはり問題の関心が不十分であるのは、被害の重大性の認識が足りないからではないか。一旦流れてしまうと、いくら叩いても高額で児童ポルノ画像が転売され、消し去れない。自分の見られたくない、おぞましい画像が永遠に流し続けられてしまうという侵害の重大性がある。いろいろと指摘され認識してきたことであるが、このような問題についても、ネットの先進国である日本が放置しているとみられないことが重要ではないか。

地方をみると、条例によりネットに関していろいろな制限を設けなければならぬとする動きが出てきている。行き過ぎることは非常に問題であるが、何故そのような不安を持つかということに目を向ける必要がある。この4月に「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律」が施行されているにもかかわらず、具体的な動揺が出てきている。この中身についてどのように対応していくかはこれからだと思うが、PTA等の側が、安心してネットを見られないという状況に対して様々な努力をしている。それが、どこまで伝わるかという問題があり、伝える側としては、そうした施策は具体的にこれだけの効果があるということを示していかなければならない。まさに今年が正念場ではないか。東京都なども、取り組まなければならぬと動き出している。もちろん業界側、プロバイダー側もご努力されてきたこともそのとおりである。うまい説明を見つけていかなければならない。

ITを活用したこの革命的な会議は、大変よろこばしく、関係者のご努力に敬意を表したい。

Webサーバの件について。最初に有名になったのはホワイトハウスのWebである。皆が驚いたことは、家の前の工事等の小さな単位の行政からホワイトハウスまでがWebページ上でリンクされており、誰でも連携して閲覧できるようになったということである。これは、情報が公開され、行政が透明になり、国民からの信頼感を得るなど非常に大きな効果があった。サーバの集約化についてだが、専門家として見ると、政府機関のサーバの台数が多いということは大きな問題だが、これは技術的に解決できる問題であり、取組みとしては非常に良いことである。集約化を説明する際に気をつけなければならないことは、サーバの台数を減らすとは言っ

ているが、行政情報の国民との共有化、公開を減らすとは言っていない点である。情報セキュリティに関する問題において、一般的に情報セキュリティには気をつけてしっかり取り組まなければならないが、それと同時にITは様々に貢献するものであり、この二つを両立しなければならない。このような考えを前提として、説明をしなければいけないのだと思う。

説明の上で、これらの数字の意味がどこまで通じるかということに気を付けていただきたい。1,900台が多いのか少ないのか、どのような意味があるのか、伝える際には説明をしていただきたい。

NISCの将来について、機能ややるべきことは更に増えてきており、負担は非常に増えてくると思われる。その際、機能や人材を持った団体や組織との契約など、有機的な連結を進めていく必要がある。このような連携では重要な情報セキュリティの問題を取り扱うため、政府と民間団体との約束事が大事になる。これは契約件数等によって具体的に進めていくことが必要である。

オバマ大統領のスピーチにもあるように、IT政策や情報セキュリティという言葉がトップのスピーチの中に出てくるようになった。世界的な外交メッセージの中に、日本の情報セキュリティの取組み、ICT施策の取組み、本日議論していることなども表現されていくと良いのではないかと。

官民連携はかなり進んできていると思っている。重要インフラ、人材育成、サイバーテロ等への官民連携の取組みが行われ、成果を挙げてきている。ただ、更に官民連携の枠組みを広げ、効果的かつ実効的な取組みとしていくためには、IT先端技術に関わる組織を有機的に連携させることによって、官民の幅広い知見を有効に活用していくことが可能になる。

セプターカウンシル等が機能し始めているが、今の現状をみると、セプターのメンバーにおける個人レベルの貢献で行っていただいていると思っている。より組織立った動きをするためには、組織トップの意識改革を図っていくことが重要である。

先の構成員の意見にもあったが、情報セキュリティについて、組織トップが自分の声でアピールできるようにしなければならない。そのためには、この政策会議の成果を外に対してアピールする必要がある。

他の有識者のご提出された意見書には「政府機関トップの強い意識と実行力が不可欠」とストレートに書かれているが、まさしくそこが重要であろう。

これまでの情報セキュリティの施策では、政府機関・地方公共団体、重要インフラ、企業、個人と幅広く実施しているが、企業の中で、中小企業についてはなかなか大企業と同様のレベルの対策は実施できないというのが実状だろう。大企業からのアウトソースの関係をもっている中小企業こそ、情報セキュリティに対する十分な関心をもって、その実施を具体的に推進する必要がある。

現在、中小企業を対象とする情報セキュリティ対策、アウトソースにおけるセキュリティ対策などの検討が始まっているが、具体的に活用できるレベルにはまだ到達していないとみている。中小企業用セキュリティ対策集の策定、簡易なマネジメント認証システムの整備など、具体的かつ実効的な施策をさらに推進することが必要である。

いわゆる企業におけるコーポレートガバナンスと営業活動の効率化等の事業とのバランスをどのようにとっていくかということが大きな問題になってきている。企業だけではなく、政府機関においてもガバナンスの問題と政府における活動の効率化等の施策のバランスをどのようにとっていくかが大きな問題である。

官民連携はかなり進んできていると思っている。重要インフラ、人材育成、サイバーテロ等への官民連携の取組みが行われ、成果を挙げてきている。ただ、更に官民連携の枠組みを広げ、効果的かつ実効的な取組みとしていくためには、IT先端技術に関わる組織を有機的に連携させることによって、官民の幅広い知見を有効に活用していくことが可能になる。

セプターカウンシル等が機能し始めているが、今の現状をみると、個人レベルの貢献で行っていただいていると思っている。より組織立った動きをするためには、組織トップの意識改革を図っていくことが重要である。

先の構成員の意見にもあったが、情報セキュリティについて、組織トップが自分の声でアピールできるようにしなければならない。そのためには、この政策会議の成果を外に対してアピールする必要がある。

他の有識者のご提出された意見書には「政府機関トップの強い意識と実行力が不可欠」とストレートに書かれているが、まさしくそこが重要であろう。

これまでの情報セキュリティの施策では、政府機関・地方公共団体、重要インフラ、企業、個人と幅広く実施しているが、企業の中で、中小企業についてはなかなか大企業と同様のレベルの対策は実施できないというのが実状だろう。大企業からのアウトソースの関係をもっている中小企業こそ、情報セキュリティに対する十分な関心をもって、その実施を具体的に推進する必要がある。

現在、中小企業を対象とする情報セキュリティ対策、アウトソースにおけるセキュリティ対策などの検討が始まっているが、具体的に活用できるレベルにはまだ到達していないとみている。中小企業用セキュリティ対策集の策定、簡易認証システムの整備など、具体的かつ実効的な施策をさらに推進することが必要である。

いわゆる企業におけるコーポレートガバナンスと営業活動の効率化等の事業とのバランスをどのようにとっていくかということが大きな問題になってきている。企業だけではなく、政府機関においてもガバナンスの問題と積極的に活用するという活動の面のバランスをどのようにとっていくかが大きな問題である。

政府機関のサーバ集約化は、政府機関の業務改革の第一歩である。公開Webサーバ、電子メールサーバを統合するが、Webは更新しやすい、メールは使いやすいということを成し遂げ、基本的な業務改革をきちんと行うということである。その意味で、業務改革の基本的なレベルの課題に取り組んでいると理解していただきたい。

霞ヶ関クラウドや電子私書箱等をIT戦略の中で打ち出しており、すばらしい戦略であるが、それらは応用編であり、とても難しい課題である。その手前の基本的な課題として、公開Webサーバや電子メールサーバを統合して集約していくということは、“さっさとやらないと”と思う。数ある業務システムの中では、他との関連性が低く、集約化が行いやすいシステムと思われ、“サクサクとやれる”政府

機関になっていただければと思う。半減に拘らず、最適になるまで速やかに進めていただければと思う。是非よろしく願いたい。

I T戦略も非常に重要な戦略がまとめられており、こちらもしっかりと実施していただきたい。その際には、情報セキュリティの観点が非常に重要であり、霞ヶ関クラウドでクラウドコンピューティングを導入する場合は、プライベートなクラウドとは言え、今までとは違ったセキュリティの体制を考える必要がある。その点でもしっかりとした人選をして、実施していただきたい。

情報セキュリティの議論では、本日のセキュア・ジャパン2009にもあるが、事故前提社会という考え方が重要である。情報セキュリティ対策をしっかりと行えばインシデントはゼロになる、ということはない。技術の進展や普及に従い、新たな脅威が現れ続けることはしかたがないことである。予防策はきちんと実施しなければならないが、万一事故が発生しても対応できるように免疫力を強化しなければならない。これは政府機関、重要インフラ、企業においては当然、きちんと進められていくのではないかと期待している。

国民一人ひとりに対しても、この考え方を浸透させていくことが重要ではないかと思う。ややもすれば、新しいサービスや自由を禁じ、制限することによって安心・安全にするという傾向になりがちである。それに頼らず、個人がきちんと対応できる、個人も免疫力をしっかりと強化するという社会にしていくことが重要ではないか。

技術の進展も速く、取り組まなければならない業務も新しくなっている。大事なものは人材である。我が国は技術は強いが事業は弱いと言われ、I T戦略等でも様々な課題について人材育成が議論される。情報セキュリティにおいても、研究開発した技術を事業化し成功させることが大切になってくる。そのためには、技術力と事業開発力といった複数領域についての知見や経験を持つ人材をつくっていく、こうした内部人材をつくっていく観点も重要である。

国際展開も非常に重要であり、こうした力のある人材を大学や産業界で育て、活躍できる、キャリアアップできる環境の整備にしっかりと取り組んでいただきたい。

有識者構成員の意見書にもあるが、環境庁の創設以来となる消費者庁という新しい行政組織が誕生した。本来の行政組織がやるべき仕事を行うということである。役所は、そもそも国民に立脚しているはずであるが、明治以来の役所は、どちらかと言えば、産業振興、殖産政策のためにつくられ、国民、個々人に対しては冷淡であつてもよいといった面があつた。今やグローバル化、多様化、複雑化する中で、国民、消費者が活性化されなければ、いかんともしがたい閉塞感の中にあつて、単に新しい行政組織、役所ができたというだけではなく、国民のポテンシャルをもっと引き出していく、ポジティブな新しいムーブをつくろうという極めて大胆な行政改革であると思っている。

消費者行政もそうだが、I Tや情報セキュリティ、個人情報保護、自殺対策まで含め、日本の命運を賭けたポジティブなI T政策から、先進国にも関わらずぼけ込んでいる個人情報保護対策、先ほどの児童ポルノの問題もそうであるが、それらを

どのようにしっかりと直していくかについて、それぞれの課目ごとではなく、横断的に混じり合わせて政策に取り組むことができたことは幸せに思う。今、そこにある基盤はITであり、日本のこれからのステップにつながるものがITであるという共通認識をどの分野でも持たなければならない。

これだけのすごい国であるが、ITの利用者である国民、一般の方からみて、そのうま味を実感できないのは何故かと考えている。電子政府をつくるにあたって、サプライサイドのペーパーレス化等から発進しており、電子化により、利用者たる国民にとって、お値打ち感がある、利便性がある、豊かになるといった顧客満足の発想がITの中に、特に行政に欠けていたのではないか。有識者構成員の言及にもあった電子私書箱は、顧客満足度を実感していただくための施策だと思っている。

CIO会議があるが、はっきり言えば、機能しておらず、また、せっかくオンライン化されていても利用されていないものが多い。本来、CIO会議で取り上げ、非難し合い、競争をもって数字を上げていくのかと思えば、見てみぬ振りのようなことで、多くをオンライン化したものの全く役に立っていないものがある。総合的に強い力を持ったCIO、大臣という形でもよいが、一気呵成に取り組んでいかなければならない。皆様に士気を高めていただいても、最後の“エイヤ”という力が足りなかったのではないかと反省しつつ、取り組んでまいりたい。

本日の「セキュア・ジャパン2009」や政府機関のサーバ集約化は重要なことであり、やりきる力が必要である。構成員の皆様方のお力をいただきたい。

先ほど、児童ポルノの問題が挙げられた。議員立法でつくられた法律は、私が最初の起案者であった。当時は、インターネット関連の対策の中に、児童ポルノを入れるのが精一杯であった。表現の自由等の問題で、一部の組織的な人々から、この問題に取り組むことについて攻撃もあった。ITの悪いところでもあるが、100人の人が1,000万人分の嫌がらせができるツールにもなる。与野党ともに、多数の電子メールが送られるなどによって、パソコンが使えなくなり、仕事が機能停止になるということもあった。こうしたことを数年経験しており、正直うんざりしている国会議員も多いことは確かだが、それらを乗り越え、国会だけではなく、すべての国民が児童ポルノは恥ずべきことだと声高らかに言えるよう取り組んでいく必要がある。

いずれにせよ、ITが日本の底力となるよう、国民に分かるようにしっかりと取り組んでまいりたい。今後ともよろしくお願ひしたい。

ICTの国民生活への浸透に伴い、個人や企業が情報セキュリティ上の脅威に晒される危険性が高くなっており、国境を越えて様々な問題が発生している。

また、ICTは我が国の社会経済活動の基盤を成しており、クラウドコンピューティングのような新しい技術の出現、データセンターの利用の増大といったICT分野の環境の変化に的確に対応し、情報セキュリティ政策を推進していく必要がある。

不正アクセスやインターネットサイト等のサイバー犯罪について、その検挙件数は益々増加しており、過去5年間で3倍に達している。また、警察に寄せられる相

談件数も増加傾向にあり、サイバー犯罪は、インターネットの利用者がいつその被害に遭うかもしれない国民生活の身近な脅威であると考えている。そのような中、本日決定される「セキュア・ジャパン2009」に基づき、情報セキュリティ対策を積極的に推進してまいりたい。

治安、防犯に関してはサイバー犯罪の取締り体制の強化、情報技術の解析能力の向上及びサイバーテロ対策に係る体制等の強化といった基盤整備の推進とともに、サイバー犯罪被害の防止のための広報啓発等の施策が「セキュア・ジャパン2009」に盛り込まれている。国家公安委員会の委員長として、今後、これらを着実に推進するよう警察庁を指導してまいる。

情報通信政策に関しては、技術開発や実証環境の整備、情報セキュリティ確保のほか、人材の育成、事業者間の情報共有体制の強化、国際連携等を推進することにより、国民が安心して安全にICTを利用できる環境の整備に努めてまいる。

重要インフラのセキュリティについては、情報通信行政及び地方自治行政を主管する大臣として、安全基準等の改定が適切に行われるように、事業者及び地方公共団体を支援していくとともに、重要インフラ連絡協議会の場を通じて、各分野間の連携が有効に機能するよう支援してまいりたい。

まずは「セキュア・ジャパン2009」を取りまとめいただいた関係者の皆様に感謝を申し上げたい。

重要な技術情報や顧客情報等の漏えい、流出事件等、企業経営に深刻な影響を及ぼす情報セキュリティ事故が発生している。企業経営者は情報資産の管理を経営課題そのものと捉え、企業リスク管理の一環として体系的に情報セキュリティ対策に取り組むことが求められている。これを踏まえ、経済産業省としても今月、経営者のリーダーシップの下で企業の情報セキュリティガバナンスの確立を推進するガイドランスを策定したところである。

本日の「セキュア・ジャパン2009」においては、企業向けの最重要施策として、情報セキュリティガバナンスの確立の推進が位置づけられている。経済産業省としてもこれを着実に推進してまいりたい。

I PA（独立行政法人情報処理推進機構）が企業経営者や一般ユーザ等を対象に「情報セキュリティ白書2009」を作成した。本日、お手元に配布させていただいている。この白書では、昨年度の情報漏えいの最大の原因がW i n n yによることなど、情報セキュリティの問題を分かりやすくまとめたものである。配布した資料を後ほどご覧いただければと思う。

経済産業省としても、今後とも情報セキュリティ強化への取組みに尽力してまいるので、引き続き内閣官房をはじめ関係省庁のご協力をお願いしたい。

今般策定されることとなる政府機関のサーバの集約化の今後の方針について、防衛省としても協力してまいりたい。

当省では早期から、分散的に管理していた各種情報システムの情報セキュリティ上の問題や費用効率上の問題について認識し、平成12年12月に省内情報システムの集約や情報セキュリティ管理体制の構築等に関するIT推進要綱を策定し公表した。本要綱に基づき、平成14年度から防衛情報通信基盤の構築に着手した。

各機関ごと、各システムごとのネットワークをこの通信基盤のネットワークに集約するとともに、共通的な機能であるメールやホームページ等に使用するサーバをここに一元的に収容して集約するとともに、平成19年度には自衛隊初の統合部隊である自衛隊指揮通信システム隊を新編し、メール通信及びホームページへのアクセスを一元的に監視するなど、情報セキュリティ管理体制強化の施策を着実に実施してきたところである。

このような実績を踏まえ、今後のサーバ集約化に関する技術的な検討においても、これまでの当省の取組みのノウハウ等を提供することによって積極的に協力してまいりたい。

(5) 政策会議決定

「セキュア・ジャパン2009」及び「政府機関のサーバ集約化について」を政策会議決定とした。

(6) 議長（官房長官）からの指示

本日決定した「セキュア・ジャパン2009」は、「第2次情報セキュリティ基本計画」の最初の年次計画である。経済財政諮問会議の「基本方針2009」等にも盛り込んでいる。我が国の経済成長の後押し、安心社会の実現に向け、内閣官房を中心に各府省連携の下、着実に取り組んでいくことが必要である。

政府機関のサーバ集約化に関する方針についても決定したところである。本件は、政府機関のシステム管理コストやセキュリティリスクを軽減させるために是非とも実現させなければならない。単なる数合わせに終始することなく、政府機関のセキュリティガバナンスを強化し、電子政府の構築を急ぐ、加速化につなげるが必要不可欠である。各府省においては、年内にアクションプランを策定するとともに、内閣官房では、各府省の計画を取りまとめた上、本会議に報告していただきたい。閣僚各位におかれても、自府省のアクションプランの策定状況をしっかりとチェックいただきたい。

情報セキュリティ対策は、第2次基本計画に基づく新たなフェーズに入っている。今後、情報セキュリティ対策が誰にとっても当たり前のこととして根付かせ、発展させていくためには、人材育成や国際戦略に関する具体的な計画・方針を策定することが必要であり、これらの点について今後検討したい。次回会合において、内閣官房から現状報告を求めることとする。閣僚各位におかれても、ご協力いただけるようお願いしたい。

－ 以 上 －