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21回会合　議事要旨

１　日時

平成21年5月8日（金）　17：45～18：45

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	国家公安委員会委員長
二階　俊博	経済産業大臣
	（※高市　早苗　　経済産業副大臣代理出席）
鳩山　邦夫	総務大臣
	（※鈴木　淳司　　総務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）
黒川　博昭	富士通株式会社相談役
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）

漆間　巌	内閣官房副長官
伊藤　哲朗	内閣危機管理監
栁澤　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
林　良造	東京大学教授（日・ＡＳＥＡＮ情報セキュリティ政策会議議長）

４　議事概要

(1)　２００８年度の情報セキュリティ政策の評価等について（報告）

(2)　セキュア・ジャパン２００９（パブリック・コメント案）について（決定）

(3)　政府機関における情報セキュリティ対策について（報告）

・政府機関の対策実施状況報告（２００８年度）の概要について

・政府機関における情報セキュリティマネジメントに関する評価

結果（２００８年度）について
(4)　重要インフラにおけるセプターカウンシルの創設について（報告）
(5)　重要インフラにおけるその他の情報セキュリティ対策について(報告)
・指針の見直しについて
・２００８年度相互依存性解析について
・２００８年度分野横断的演習について
(6)　「技術戦略専門委員会報告書２００８」について（報告）
(7)　政府機関のＷＥＢ改ざんについて(報告)
(8)　日・ＡＳＥＡＮ情報セキュリティ政策会議の開催結果について（報告）

上記(1)～(8)について、資料配付の上、事務局から説明が行われた。

(9) 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。
○　先ほどのＷＥＢ改ざんの報告、或いは政府機関の対策実施状況の報告で公正取引委員会や文部科学省などで実施率がかなり低い省庁があるなど、必ずしもこれまでやってきたことで万全であるとは言えないが、一定の評価、がんばっていただけましたと評価したい。
○　セキュア・ジャパン２００９パブリック・コメント案の考え方、ステップの取り方については賛成である。これに沿い、しっかりと進めていただきたい。
○　セキュア・ジャパン２００９の３か年の方向性や取組みの流れにおいて、まず事故前提社会の考え方を自覚し、次にそれを協働して実現し、さらにそれを成熟させると整理されており、非常に分かりやすく、良いのではないか。
○　事故前提社会というキーワードだけでは、なかなか伝わりにくいが、その意味するところは大変重要である。インシデントがゼロになる、減ることはなかったと報告があったが、それは当然であり、一生懸命やったとしても技術の進展に伴い、新しい脅威が現れることはしかたがないと言える。だからこそ、適切な対策を継続して行っていくと共に、事故が発生しても大丈夫なように対応策を準備することが重要であり、頭で考えるだけではなく、具体的にどうするかということを隅々にまで行き渡らせることが重要である。みなさんに、それを一つ一つ進めていただきたい。
○　現下の経済情勢における対応について、このような時だからこそ、近視眼的、局地的な対応をとるのではなく、その先の成長につながる施策を打ち出すことが重要である。穴が開いたところへパッチを当てていく対策ではなく、全体の先のビジョンまでを見据えた上で、それへ向けた継続的な施策が重要である。
○　個々の施策を言うだけでは、みなさん納得していただけない。将来に向けて全体最適を実現するために、大きなビジョンを政府、トップの方がしっかりと示し、それがぶれることなく旗を振り続けていただきたい。このような状況だからこそ、その役割が重要であり、そうすれば後は実態がついて来て、ＩＴや情報セキュリティも充実してくる。
○　基本的には情報セキュリティ基盤の強化へ向けた３年間の取組みを評価するこ

とには納得がいく。表面的にはインシデントが減らないということはあるが、基盤は構築できているということについては、自信を持ってよいのではないか。

○　犯罪の発生については、数が一定の範囲内には収まっていないということがあるが、数値目標として犯罪数を押さえ込むこと以上に、新しい問題にも対処し得る組織、基盤の強化に取り組むことが、国民からみた安心感ということでは望まれる。

○　約５５万人の職員の実態を調査し、各省からデータが出されたことは、いろいろな見方はあるが、これだけの驚異的な期間に指示・行動をとられたことは、外国からみても優れた成果である。

○　ＷＥＢ改ざんの問題に対する政府機関の対応をみれば、予防的なことについては教育などそれなりにやられているが、事が起こった後の危機管理については、今回の失敗を無駄にすることなく、再度、取り組みを前に進めることが大事である。

○　サーバの数が多すぎるということは、以前から指摘されていることであり、内閣として、統一的な基準を作っていただきたい。

○　政府機関はある程度やられてきているという印象を強く持った。これまで政府機関、重要インフラ、企業、個人の４つの領域で取り組まれたが、地方公共団体はどこへ行ったのか。総務省でいろいろとお考えはあるとは思うが、国民の情報を扱う主体としての重要性を考えれば、地方分権の流れはあるにせよ、国の統一的な、情報の観点からの発言があってもよいのではないか。

○　４つの領域に収まらない重要なものとして、大学が持っている情報がある。それをどのように扱うかという観点があまり表に出てこない。今回の政府機関の対策実施状況調査では、文部科学省のデータがあまり良くない。結びつけて考えることは良くないが、大学側の人間としての自戒もあるが、今後そのような視点も持って頂きたい。

○　重要なポイントである重要インフラに関して、セプターカウンシルの創設は非常に評価すべきである。全ての分野が揃わないにしても、情報通信分野、金融分野などを中心にできるところから前に進んでいただきたい。

○　ＩＴの中でも情報セキュリティは大きなウェイトを占める。新しい技術の創生について、日本最高レベルの人材を集め、政府、ＮＩＳＣでがんばっていただきたい。

○　３年間でこれだけの体制ができ、政策会議そのものも継続して進められてきたことは、国際的に見ても短期間で大きな成果が上がったと言える。体制ができたことは評価されるべきであり、他国の方からもそういった評価を伺っている。

○　持続的な運用と、テクノロジーの変化に伴う継続的な発展も体制や評価の中に含めなければならず、その点は更に工夫が必要である。

○　ＷＥＢ改ざんなどの問題について、単純に安全だけを考えれば、極端な方法はネットワークから切り離すことである。しかしこれではもはや社会は機能しない。ＩＴ戦略本部の会議でも挙がったが、一番大切なことは、「どきどき」しなければならないということである。攻められることが怖いという「どきどき」もあるが、期待に満ちて「どきどき」ということもある。さらに、「わくわく」しなければならないという話が出ていた。経済的にも、社会的にも明るい未来が情報技術によって実現すると期待されるが、その時に情報セキュリティがきちんとしていなければな

らない。脅すばかりでは、気持ちよく仕事ができない。情報セキュリティへ取り組むには、「わくわく」している部分も必要である。そのようなことも含め、ダイナミックな動きの中での継続的な発展が課題である。

○　人材を育てる側である大学の人間としても大きな責任があるが、高度な人材を輩出・確保できるかという問題がある。繰り返しになるが、情報セキュリティに関わる学生は、多岐に渡る様々な事象を理解していなければならず、エースであると言える。我々は、そのような人材を送り出す責任があり、実践しているが、それでも人材が足りなくなる。情報セキュリティを専門としている大学院もできてきているが、民間機関や大学との契約的関係などの具体的な部分でどのように連携するかがまだ整っていない。このような連携によって、今後、高度な人材が役割を果たせるような体制を作ることができる。重要な人材はますます必要となり、それを満足な状態にすべきである。

○　先ほど、日・ＡＳＥＡＮ情報セキュリティ政策会議の報告にもあったが、アジアの中における国際性は重要である。また、グローバルガバナンスにおいても、ＩＣＡＮＮの改編など重要な時期である。その議論の中で、特に中国やインドは、グローバルネットワークのポリシーに関して、いろいろなことを内政的に発言してくる。グローバルに繋がっているものであり、日本が連携の中でどのような役割を果たすかは非常に重要である。グローバルガバナンスのインターフェースをＮＩＳＣがどのように持っていくのか、外交レベルのメッセージをどのように機能させるか、極めて重要な時期である。特に今年は重要であり、日本が大きく貢献できるようにするべきである。

○　第１次基本計画については、組織が大きいだけに、大変ではないかと思っていたが、よくやってこられた。

○　２００９年度からは、事故前提をベースに考える、且つ合理的なアプローチをとるということは、経済変化など、極めて早いスピードで変化するものに対応するためには必要なことである。

○　ＷＥＢ改ざんの報告があったが、改めて基本を確認しておいた方がよい。事例を共有し、組織ルールを見直し、サーバ集約等の改善を実施することは、事故前提の考えや合理的なアプローチとして重要なことだと考える。

○　ＩＴに携わるものは、ハインリッヒの法則をよく参考にする。労働災害の統計で、１件の重大な事故の背後には、２９件の小さい事故、３００件の“ヒヤリ”とした事象があるというものである。ＩＣＴを使う、情報セキュリティを行う上で、人間系の問題が重要になってくる。したがって、事例を共有する、“ヒヤリ”とすることを吸い上げることで、小さな事故、重大な事故が起きないようにすることが非常に重要である。

○　優秀な人材も大切であるが、組織は劣化するということをよくお考えいただきたい。ＩＣＴのシステムを構築した際、設計した人間、最終テストを行った人間はシステムの問題など、いろいろなことを分かっている。時間と共に人は入れ替わり、マニュアルも時代に合わなくなっていく。組織が劣化するという前提で、どのようにＩＣＴでカバーするか、人をどのように育て、回していくのか、よく考えなけれ

ばならない。集中的な組織も考慮し、ばらばらに優秀な人を育てようとしても育たないということもご理解いただきたい。

○　メールサーバやウェブサーバを減らすことは、人を有効に活かす、組織の劣化を防ぐという上でも非常に重要である。２００９年度の新しいセキュア・ジャパンを作るにあたって、改めてこの基本を申し上げたい。

○　今現在、日本及び世界も百年に一度と言われる経済危機の中で、不安を抱えているところではあるが、麻生内閣においては、このピンチをチャンスへ変えようということで、どの国よりも早く危機から脱却し、新しい国家を再建しようと補正予算の審議が行われているところである。

○　先の構成員のお言葉を借りれば、次の時代に「わくわく」できるようなもの、単にこれまでの手当てではなく、次につながる「わくわく」感をつくっていくためには、ＩＴはまさに優れたものではないかと思っている。

○　ＩＴによって次の確実な日本へ、ＩＴを底力とする日本へ変えていくこと、また、全ての国民・企業・ＮＰＯ・地域社会が元気になり、夢を実現できるデジタル成長社会を実現させるため、この度４月に「デジタル新時代に向けた新たな戦略（三か年緊急プラン）」を皆様のお力で作っていただいた。

○　この三か年緊急プランの策定で、私が最もこだわったところは、自然の思いではあるが、国民の利便、お値打ち感がある、楽ちんである、安心であるといったことを中核に据えるということであった。いわゆる消費者目線ということである。これまで「官から民へ」という言葉が流行ったが、民においてもサプライサイドに留まっていたものを、もう少しユーザやコンシューマーサイドへリーチを伸ばして取り組むべきであるということを徹底させていただいた。

○　消費者庁関連法案も衆議院の方で成立し、おそらく今年度中には、環境庁から数えて３８年ぶりに新しい行政組織ができるということで、まさに「消費者元年」とも言うべき、これまでこの国になかったスタイルを創り出す新しい年になる。

○　三か年緊急プランが国民に心から支援していただけるものになるには、安心・安全が重要である。まだ怖いというイメージがあり、それを吹き飛ばすためにはセキュア・ジャパン２００９が極めて重要な施策になるであろうと期待しているところである。三か年緊急プランとセキュア・ジャパン２００９は両輪として、共に進めていかなければならないと思っており、併せてしっかりと取り組んでまいりたい。

○　警察における取組みとして、サイバー犯罪の取締りを進めているところである。平成２０年の検挙件数は６，３２１件と、平成１６年からの過去５年間で約３倍に増加している。特に、不正アクセス違反に係る検挙が全体の３割弱にあたる１，７４０件と、平成１２年の不正アクセス禁止法施行後、最も多い件数となっている。手口も、フィッシングサイトを開設し、識別符号を入手するもののほか、ＩＤ等から推測したパスワードを使用するなど、パスワード設定の甘さに付け込むものが非常に多くみられる状況にある。

○　ＩＴ利用における安全・安心を確保するためには、利用者や管理者の意識を啓発することが最も重要であると考えている。本日のセキュア・ジャパン２００９（案）には、本年度の警察における取組みとして、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共に、サイバー犯罪被害の防止のための広報・啓発等が盛り込まれている。

○　本案については、今後、国民の理解が得られた上で、決定に至るよう願っている。

○　２００８年度の情報セキュリティ政策の評価等、セキュア・ジャパン２００９（案）をとりまとめ下さったご関係のみなさまのご努力に、まずは感謝申し上げたい。

○　本日のセキュア・ジャパン２００９（案）の４つの柱の中のひとつに、企業における情報セキュリティ対策の推進がある。企業にとっては、ＩＴの利活用が競争力の源泉であるが、近年、情報漏えい等の事件・事故が多発するなど、企業の情報資産に対する脅威は増大の一途をたどっている。あまり怖がらせず、「わくわく」と元気にやらなければならないが、まず大企業であれ、中小・零細企業であれ、全ての経営者の皆様に、価値ある情報の管理は経営戦略そのものであることを、しっかりご理解いただきたいと考えている。

○　資料１１に示すように、経済産業省は、経営者のリーダーシップの下、情報セキュリティの観点からガバナンスの仕組みをしっかりと構築できるようにということで、情報セキュリティガバナンスに関するガイダンスを策定した。これを基に、関係団体と協力しつつ、政策を積極的に推進してまいるので、内閣官房はじめ関係省庁のご協力をお願いしたい。

○　２００８年度の情報セキュリティ政策の評価等、セキュア・ジャパン２００９（案）のとりまとめについては、内閣官房をはじめとする関係者のご努力に敬服すると共に、まずは御礼を申し上げたい。

○　中央省庁等のホームページの改ざんが為された事件の２０００年頃は、ある面では自己顕示欲に駆られた愉快犯的なものであったと思われる。しかるに、近年は不法行為の実行者の裾野が広がっており、いわゆる金銭目的など、より悪意の強いものになってきていることを懸念する。実際に、ソフトウェアと一定の知識があれば、これらの不法行為が可能であると思われる。

○　先般、私も実際に情報セキュリティの現場を視察し、不法行為の手口について実演で説明をうけてまいった。悪意をもった相手方に容易に自分のパソコンに侵入され、パソコンを勝手に操作されるところを見学した。これらの不法行為の元となる、ボットやマルウェアというものが世界中で検知されているのが現状であろうかと思う。

○　事務局より事故前提社会とのご説明があったが、インターネットが当たり前のものとして広く普及した今日においては、私自身の実体験としても、インターネットの利用自体に影響が伴うということを社会全体が共有することが必要であることを痛感している。

○　最も危険に晒されているのは、普通の個人、社員であり、いわゆる情報セキュリティの弱者という方であろうかと思う。こうした方々についても、インターネットがなければ、日常生活や業務に支障が生じ、インターネットを使うなということは言えない。これは、子供に対して事故や危険があるので、外に出るなとは言えない

ことと同じである。全ての利用者のインターネットの安全性に対する意識を根本から改めるための啓発活動が必要である。

○　本日、政府機関における情報セキュリティ対策実施状況等についてもご報告いただいたが、総務省はもちろんのこと、各省庁の情報セキュリティの担当者におかれては、情報セキュリティ弱者である普通の職員が安心して、本来の業務にまい進できるような利用環境の整備や啓発活動をお願いしたい。

○　総務省としても、省庁間でベストプラクティスを共有するなど、政府全体の情報セキュリティの向上に取り組んでまいりたい。関係府省庁のご協力を是非お願いしたい。

○　重要インフラの情報セキュリティについては、普通の人々が安心して利用できる環境維持のため、引き続き関係省庁のご協力をお願いしたい。

○　セプターカウンシル総会の初代議長へ、ネットワークの神経系である電気通信分野からテレコム・アイザック・ジャパン会長の伊藤泰彦氏が就任されたこともあり、総務省としても、この枠組みが有効に機能するよう支援していく。

○　日・ＡＳＥＡＮ情報セキュリティ政策会議においては、総務省では合意された連携枠組みに沿って、事業者間の情報共有や連携、研究者の人材交流等を促進することにより、国内に留まらず、日本にとり益々重要となるアジア諸国をはじめとするグローバルなＩＣＴ利用環境を構築し、広く情報セキュリティの向上に努めてまいりたい。

○　総務省としては、サポーター制度の創設により、情報セキュリティに詳しい人材を利用者の身近なところで育成するなど、広くＩＣＴ分野のリテラシーを高める活動を継続していくと共に、業務継続計画の策定など、地方公共団体における情報セキュリティ政策の確率についても取り組んでまいりたい。

○　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、ＮＧＮやＩＰｖ６への移行、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た情報セキュリティ政策の推進について、内閣官房をはじめとして関係省庁のご協力をいただきながら積極的に取り組んでまいりたい。

○　防衛省においても、引き続きサイバー攻撃等への緊急対応能力の強化に関する分野において、サイバー攻撃等に係る分析や対処及び研究の推進や最新技術動向の調査研究等などの施策を積極的に推進してまいりたい。

○　防衛省においては毎年２月を情報セキュリティ月間と定め、全隊員の情報セキュリティに関する知識の習得及び意識の高揚を図るための様々な活動を進めているところである。私からも自衛隊全隊員へ向け、私有パソコンからの情報流出の根絶をテーマとして、メッセージを発出したところである。

○　情報セキュリティマネジメント評価においては、全項目中の３分の１がベストプラクティスとして評価を得ているところである。当省としては、情報セキュリティ対策を実効あるものとするための取組みについて、多くの知見を有していると考えており、引き続き必要に応じて情報提供を行ってまいりたいと考えている。

○　防衛省として今後とも、情報セキュリティ関係省庁の一員として、有識者の先生方のご意見等も踏まえ、第２次情報セキュリティ基本計画の下で、我が国の情報セ

キュリティ水準の更なる向上に貢献してまいりたい。

(10)　政策会議決定

セキュア・ジャパン２００９（パブリック・コメント案）について、政策会議決定とし、パブリック・コメントに付すこととなった。

(11)　議長（官房長官）からの指示

本日、事務局から報告のあった政府機関のＷｅｂ改ざんについてであるが、進化し続けるサイバー攻撃を完全に防御することは困難だとしても、ガバナンスを確立し、迅速な対応・復旧が必要不可欠であることは論をまたない。

政府機関のサーバが乱立していることは、ガバナンスが欠如していることの現れであり、管理コストがかかるだけでなく、セキュリティリスクを高めることになる。

国民に安心を与え、活力ある社会経済活動を支えるためには、政府が率先して範を示さなければならない。私は、サーバの集約化は是非とも進めなければならないと考える。政府機関の公開サーバの集約化を進めるべく、政策会議で必要な対策を取りまとめたいと考える。

内閣官房においては、各府省の公開サーバの現状を早急に把握し、集約化に向けた方策をまとめ、次回の政策会議で報告していただきたい。

閣僚各位におかれても、ご協力いただきますよう、よろしくお願いする。

－　以　上　－