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9回会合 議事要旨

1 日時　平成 18 年 12 月 13 日(水)　17:00～17:45

2 場所　総理官邸大会議室

3 出席者(敬称略)

溝手 顕正	国家公安委員会委員長
久間 章生	防衛庁長官
	(※大前 繁雄 防衛庁長官政務官代理出席)
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
	(※渡辺 博道 経済産業副大臣代理出席)
山本 有二	内閣府特命担当大臣(金融担当)
	(※渡辺 喜美 内閣府副大臣代理出席)
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)
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
小野寺 正	KDDI 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

(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
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

4　議事概要

議長である塩崎内閣官房長官及び議長代理である高市国務大臣については、国会での審議終了後に出席する予定であったため、溝手国家公安委員会委員長が議長代行として議事を進めた。

(1)　情報セキュリティの観点から見た我が国社会のあるべき姿及び政策の評価のあり方について
(2)　人材育成・資格制度体系化専門委員会報告書（案）について
(3)　重要インフラにおける安全基準等の策定・見直し及び分野横断的演習の取組みについて
(4)　政府機関統一基準の見直し方針について

上記（1）～（4）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。

(5)　出席者意見開陳

上記（1）～（4）について、出席者から以下のような意見が述べられた。

○　(2)について、情報セキュリティがマナーや常識になるような教育を高校で行うということだが、最終的には、全ての国民が、「情報は非常に重要なものであり、自分達で守らなければいけない。」という意識を持つ必要があると思う。その観点からでは、リテラシーという緩やかな言葉だけではなく、情報に関して一定のことを行うと犯罪であるということをしっかり示す必要がある。刑法の中に犯罪として取り込むということは非常に困難であるが、近年の情勢を見るとそれも変わってきている。そのような状況の中で、情報の重要性がそれだけ高いものであれば、情報セキュリティについて規範化をするための法改正について、内閣主導で動き始める必要があるのではないか。それが、人材育成の基盤を作ることになる。

○　（2）について、最近、幼女の無残な死体がホームページに掲載されていたことが話題になっているが、バーチャル社会がもたらす子供に対する様々な問題点について研究会をやらせてもらっている。いじめの問題についても、携帯電話によるものがほとんどであるというような状況が明らかになっている。そのような中で、フィルタリング等の様々な取組みを進めてきているところだが、これについては、関係する省庁が多岐に渡るので、警察庁、総務省、文部科学省、さらには、内閣官房も含めて、統一的な方向性を持ち、足並みを揃えて取組みを進めて欲しい。

○ (1)については、これまでの議論が反映されており、基本的な枠組みもしっかり作ってあり、評価できる内容である。今後は、これをしっかり回していって欲しいと思う。

しかしながら、「政府機関の情報セキュリティ対策の実施状況の評価」の部分で、「対策がどのようになされているか」、「アウトカム指標を是非使って」と書かれているが、それについての詳細な記載がない。「政府機関統一基準の基本遵守事項346項目の中で重要な項目に着目し、対策の実施率の定量的な評価を行う。」とだけ記載されているが、それを基にどの程度具体的に評価をするのか、どのくらいの項目を評価するのかということをもう少しわかるようにして欲しい。

同様の観点で、重要インフラの部分においても、「評価のための指標」の項目の中に、「行動計画で定めた4点の施策の柱それぞれについて、各年度ごとの目標に対する実施状況を把握し、その進捗度合いを指標にすることによって」というように、位置付けや考えはしっかり記載されているが、具体的な評価指標項目に関する記載がなく、その点が残念だ。

企業や個人は、把握が難しく、既存の調査を活用しながらと言いつつも、「企業・個人に係るアウトカム指標」の内容は、ファイアーウォールの配置状況、パッチの適用状況、ウイルス対策ソフトの導入状況、実際に被害を受けている人の数、スパイウェアの遭遇率など、かなり具体的な実施状況や被害状況が把握できる項目になっており、こちらの方は評価できる。それだけに、政府機関に対する実施状況の評価項目や、重要インフラの評価のための指標についても、出来る限りの努力をして欲しい。

○ (2)については、非常によく検討されており、このまま実施していただきたいと感じている。組織の関係する方にも連携していただきたい。しかしながら、今回は取り上げなかった情報セキュリティ教育やモラルをどうしていくのかということは、非常に重要な段階だと思う。小学校の高学年ぐらいになると色々なことをやり、親から見るとその内容がよくわからないという状況があるが、子供たちは人間としても未熟で知らないことが多いという状態であるので、そのような層に対しては社会的に守っていくとともに、情報セキュリティ教育を推進する必要がある。また、一般社会人に対する情報セキュリティモラルの向上教育についても、今回は、組織に属している一般社員・職員に対する教育になっているが、プライベートな利用の段階になると外れてしまうので、そのような一般社会人としてのモラル教育も検討して欲しい。

○ 「セキュア・ジャパン2006」の当初計画に従って、各分野における情報セキュリティ対策に係る具体的な進捗を見ることができたことを評価したい。

○　今、産業界で話題になっているテーマの一つにＢＣＰ（Business Continuity Plan）というのがある。つまり、何かがあった時に、事業を継続できるようにしておくためのplanの重要性が非常に高くなっているということだ。情報セキュリティの問題が起こった時には、重要性としては、国、重要インフラ、企業、個人の順になると思うが、その中で重要インフラについてもう少し踏み込んでもいいと思う。

「安全基準等の整備」について、各重要インフラ所管省庁において進捗が確認されているが、安全基準等の整備において目標とされている4つの柱と3つの重点事項が、各重要インフラでどのように安全基準として整備されて、重要インフラとしての一貫性をどのように確保していくのかということが明確になっていない。各重要インフラで、セキュリティ対策の計画・実施・運用・見直しを推進すると理解しているが、各々バラバラな方向で施策を推進するととんでもないことになる。もし、方向性に大きなズレがあると、相互依存性解析をはじめとして、重要インフラ間での対策の推進が困難になると思う。

また、（1）について、進捗度合いを測る評価指標が記載されているが、重要インフラに関する評価指標があまりにも具体性に欠けているのではないか。評価指標を出されると、重要インフラ事業者や各省庁は、その評価指標が義務になってしまうことを恐れているところがあるのではないか。そのため、重要インフラの評価指標の数字については、評価の指標というよりは、むしろ実現に向かっての目標とすれば、まだ動きやすいと思うので、その観点で検討して欲しい。

○　政府機関については、見直しの計画等が既に示されており、他の分野に比べると進んでいると思う。しかしながら、大枠のスケジュールだけでなく、もう少し具体的な方針や作業イメージが見えてくるようになると、さらに進むと思う。

○　今日の議題については、評価という段階に入ったということはよいことであるが、他の構成員からも発言があったように、具体的に評価するということは非常に難しい。

○　ファイル交換ソフトウイニーの事案などもあるが、基本的にはデータの流出ということは避けられないので、データは流出するものだという前提で考えるべきである。その考えでいくと、前回も指摘したが、一般にホームページで公開するものを除いて、政府関係のデータについては、基本的に暗号をかけておくということを提案する。暗号のレベルにも色々あるが、高度なものでなくても、一般人にはまず暗号は解けないだろう。中央大学の今井先生が暗号の評価等をされていたが、具体的にはどうなっているのか。

○　指摘されている内容は、クリプトレックのことだと思うが、今、総務省と経済産業省で、暗号技術に係る現状の評価と方針を決める委員会がある。そこで、2004年から2005年の段階でどのような暗号が推奨暗号かということを言っており、各省庁でどのような暗号を使うべきかということも言っている。今は、監視モードに入っており、暗号がどれくらい弱くなっているかということについて評価するという段階に入っている。しかしながら、政府でも使われているＳＨＡ－１と呼ばれている一つの暗号方式が、2010 年には危殆化すると言われているので、それに対応するためのガイドライン化について、情報セキュリティセンターとしても検討を始めようということで動いている。また、指摘されているとおり、暗号の利用の領域を決める必要があるので、これについても検討を始めている。

○　具体的には、全ての政府関係のデータを暗号化するという方針は打ち出していないのか。

○　そこはまだルール化していない。

○　そこは大変だということは理解しているが、少し遅いと感じる。

○　(2)についてだが、国と地方の情報セキュリティ担当職員のための訓練センターを設置した方がいいと思う。情報セキュリティについては、実際にやってみないとわからないことが多いので、例えばホームページの書換え事案についての対応の実地体験訓練ができるような場が必要である。今は、警察庁や、経済産業省の情報処理推進機構など、一部の省庁で実際的な訓練ができる施設を持っているところもあるが、多くの政府省庁、地方自治体ではそうした施設がない。そこで、実体験型の訓練センターを設置した方がよい。そのような施設では、新しい技術に対するシミュレーションもできる。アメリカのミサイル防衛局の方法に倣って、各省庁の情報セキュリティ関係の予算から一部を出し合うことにより設置することができるだろう。

○　重要インフラの分野横断的演習についてだが、演習を実際のシミュレーションの形で行うのは大変だろう。最初は机上演習の形でやるしかないが、将来は実際のシミュレーションの形で行うことも視野に入れた仕組みを作ることができれば、現実的な取組みができると思う。

○　金融分野については、既にご案内のように情報システムの脆弱性が明らかになった件がある。あるメガバンクが経営統合をした際にシステムが止まったり、東京証券取引所がライブドア事件でシステムが止まったりしたことがあった。そのため、金融庁の検査部門にＩＴの専門家を投入し、システム検査も行ってい

る。この結果、例えば、東京三菱銀行とＵＦＪ銀行が経営統合をする際に、システムの問題点を指摘して、経営統合が延期された。また、東京証券取引所の次期システムは相当強力かつバックアップ態勢も整ったものになる予定だ。このように、金融機関などのシステムリスク管理体制の充実強化を図るための金融行政の対応はきちんと行ってきている。今後とも重要インフラの情報セキュリティ対策に係る行動計画などを踏まえて、関係省庁、各団体、民間事業者とも協力を図りつつ、金融分野における情報セキュリティ対策の一層の強化に努めたい。

○　厚生労働省の安全基準等の策定見直し状況については、医療分野がまだ見直し中なので、その点について報告する。厚生労働分野については、医療分野と水道分野が重要インフラに位置付けられており、平成17年3月に策定した安全基準等が見直し中になっている医療分野については、現在、有識者からなる医療情報ネットワーク基盤検討会で議論されている。検討会では、医師会、歯科医師会、看護協会、学識経験者等各方面からの参加をいただいているため、取りまとめに一定の時間を要しているが、年度内には見直しを完了する予定である。今後とも、医療・水道分野については、重要インフラの情報セキュリティ対策に係る行動計画に基づいて安全基準等の整備、情報共有体制の構築をしっかりと進めたいと考えている。水道分野については既に安全基準等の見直しを実施済みであり、水道事業者にガイドラインの通知をしているが、今後もしっかりと行動していく。

○　(1)については、この評価の取組みを進めて欲しいと思う。今後は、この枠組み案について国民の意見を収集するだけでなく、実際の評価を効果的かつ効率的に進めていくことが大変重要である。

○　我が国の情報セキュリティ政策の基本目標であるITを安心して利用できる環境を実現していくためには、内閣官房のリーダーシップの下、情報セキュリティ対策の実施について政府機関並びに重要インフラが範を示していく必要があると思う。経済産業省としては、重要インフラとして電力・ガスを対象としているが、自らの情報セキュリティ確保だけでなく、電力・ガスにおける情報セキュリティ確保に向けて積極的に取り組んでいきたいと考えている。

○　国土交通省においては、情報システム障害に起因する行政サービスの低下の防止、鉄道・航空等所管分野の安全かつ安定的な運用運営体制の確保のため、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努めるとともに、所管事業者に対しても対策の推進を強く指導してきた。
　特に、重要インフラである鉄道・航空・物流分野については、ここで報告があ

ったようにセキュリティ確保のための安全基準等を策定するなど、関係事業者とも連携をしつつ、情報セキュリティ確保のための措置を鋭意構じてきているところである。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いる。そのため、国土交通省としては、本日指摘があった点も含めて、内閣官房と密接に連携をしながら、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と考えている。

○　防衛庁関連では、ご承知のとおり、11月に航空自衛隊那覇基地所属の隊員の私用パソコンからファイル共有ソフトウイニーによって、航空自衛隊関連の情報が流出した。今年2月の海上自衛隊のあさゆきをはじめとする一連の情報流出事案を受けて、再発防止対策の迅速かつ確実な実施を行うなどの措置を講じていたにも係わらず、新たに本件事案が発生したことは、極めて遺憾であると考えている。今回の事案は、再発防止対策を確実に実施しなかった隊員により引き起こされたものであるが、防衛庁としては、このような制度を遵守しない者に対する対策を行うことも改めて重要であると考えており、自動暗号化ソフトの導入等の情報セキュリティ対策を可能な限り早急に実施しようとしているところである。今説明のあった政府機関統一基準の見直し作業においても、このような防衛庁の対策等について、必要に応じて紹介をさせていただきたいと考えている。いずれにしても、防衛庁としては、情報流出の再発防止のためには不断の取組みが必要であることから、情報流出の再発防止に係る各種措置の確実な実施に努める所存。

○　今日の議題に重要インフラ分野における情報セキュリティの確保というのがあるが、総務省においても、情報通信分野と地方公共団体について安全基準等を既に策定している。また、情報共有、分析機能の体制の整備についても積極的に検討を進めたい。さらに、情報セキュリティの確保には、通信ネットワークの安全性が必要不可欠なことであるが、大手インターネット事業者数十社が協力して、今月から電気通信事業分野におけるサイバー攻撃対応演習を実施し、来年度以降も継続する予定である。こうした情報通信分野における取組みが、今後、他の分野の参考になれば幸いだ。

　また、前回の会議で紹介のあったボットという新型のコンピュータウイルスについてだが、このボットの攻撃を停止させるプロジェクトを経済産業省と連携して、昨日立ち上げ始めた。世界最大規模のボット収集装置を設置するとともに、サイバークリーンセンターというボットの駆除ソフトを配布するサイトを設置した。

　総務省においては、こうした情報セキュリティの水準の向上に向けた取組みが普及されるように、今後も内閣官房情報セキュリティセンターと協力しつつ積極的に取り組んでいきたいと思う。

○　不正アクセスやスパイウェア等、様々な問題が発生するなどしており、情報セキュリティの取組みを強化することは、喫緊の課題になっていると考えている。本年2月に策定した第1次情報セキュリティ基本計画等に基づいて情報セキュリティの取組みを行っているところであるが、その取組みの評価をしっかりと行い、改善をしていくことは極めて重要であり、そのため、今日の議題である情報セキュリティ政策に関わるいわゆるＰＤＣＡサイクルを具体的に確立することは、安全・安心なインターネット社会の発展を図る上で非常に意義深い。警察としては、ＰＤＣＡサイクルの重要性にかんがみ、警察における情報セキュリティの確保のほか、関係機関、事業者等と連携したサイバー犯罪の取締り、サイバーテロへの緊急対処、情報セキュリティに対しての広報啓発活動等、サイバー空間の安全確保の所要の施策を評価・改善し、今後さらに取組みを進めていきたいと考えている。

(6)　政策会議決定等について

国会日程の直前での変更により、議長である塩崎内閣官房長官及び議長代理である高市国務大臣の出席がかなわなくなったため、「「セキュア・ジャパン」の実現に向けた取組みの評価等及び合理性を持った持続的改善の推進について（案）」及び「情報セキュリティの観点から見た我が国社会のあるべき姿及び政策の評価のあり方（案）」に対してパブリックコメントの募集を実施することの決定については、持ち回り手続きにより行うこととなった。

(7)　その他

故金杉明信有識者構成員に対して哀悼の意が示された。

－ 以 上 －