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31回会合　議事要旨

１　日時

平成24年11月1日（木）　17：30～18：10

２　場所

中央合同庁舎第４号館４階共用第２特別会議室

３　出席者（敬称略）

藤村　修	内閣官房長官
前原　誠司	内閣府特命担当大臣（科学技術政策）
小平　忠正	国家公安委員会委員長
樽床　伸二	総務大臣
	（藤末　健三　総務副大臣代理出席）
玄葉　光一郎	外務大臣
枝野　幸男	経済産業大臣
森本　敏	防衛大臣
	（大野　元裕　防衛大臣政務官代理出席）
遠藤　信博	日本電気株式会社代表取締役執行役員社長
小野寺　正	KDDI株式会社代表取締役会長
土屋　大洋	慶応義塾大学大学院教授
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	慶応義塾大学教授

（その他出席者）

齋藤　勁	内閣官房副長官
竹歳　誠	内閣官房副長官
米村　敏朗	内閣危機管理監
佐々木　豊成	内閣官房副長官補
櫻井　修一	内閣官房副長官補
徳田　英幸	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

⑴　討議

・　情報セキュリティに関する国際的取組について

・　その他

上記について、事務局より資料に基づき説明が行われるとともに、小野寺構成員より、「サイバー空間に関するブダペスト会議」に参加した感想が述べられた。

○　情報の自由な流通を基本方針とする我が国と、相容れない考え方の国々との付き合い方は、最大の課題であると考える。国際会議において戦略的に我が国が取り組めるよう、ハイレベルによる情報発信を積極的に行っていただきたい。

⑵　構成員意見交換

構成員から以下のような意見が述べられた。

○　各省庁の国際連携の取組については大変評価できるが、国家間で基本的方針が異なっているのが実情であり、各国で共有できる点から国際連携を強化することが実効的であると考える。

○　サイバー攻撃情報の共有においては情報連携基盤の構築が重要となるが、実態として構築できる状況に至っていない。このような状況下においては、サイバー攻撃情報の共有について賛同する国・地域から、日本が主導して情報連携基盤を構築していくのが、国際貢献の観点から重要である。国際連携について、行うべきことは整理できてきているので、具体的な行動に移していただきたい。

○　普及啓発活動について、「情報セキュリティ国際キャンペーン」として１０月に実施したこと、平成２５年度概算要求額について政府全体の財政が厳しい中でよくやっていることは、大変評価できる。しかし、米国の国防省では、サイバーパールハーバに向けて毎年３０億ドル（約２４００億円）を投じているとのことである。日本と米国とは国情が違うとはいえ、予算規模は遙かに小さく、まだ努力する余地がある。

○　予算の制約がある中で、JPCERT/CC やNICT 等の関連団体において国際連携を推進していることは頼もしいことである。我が国が疎外された中で国際ルールを決められてしまう事態とならないよう、外務大臣をはじめ関係する大臣が、ハイレベルな国際会議で強いリーダーシップを発揮していただきたい。

○　国際連携について、国全体としての戦略・哲学・方針が弱いと感じる。我が国としては、各省庁がばらばらに取組を行うのではなく、国全体の戦略・哲学・方針に基づき個々の現場が一体となって対応する必要がある。情報セキュリティ政策会議において、全体的な戦略・哲学・方針を議論して、それを元に大臣がハイレベルな情報発信を行っていただきたい。

○　NISC や関係する省庁の報道発表が国内向けに偏りすぎていて、国際的なインパクトを考慮した広報活動が重要である。また、JPCERT/CC 等の個々の活動についても、しっかりと広報していく必要がある。

○　報道によれば、防衛省においてホワイトハッカーを採用することが話題となっているが、従来の組織の就業環境・人事制度のままではホワイトハッカーの人達の個性や能力を発揮させることはできないと考える。人材育成も重要であるが、ホワイトハッカーを採用する側の組織改革・人材教育も重要である。

○　我が国は諸外国に比べてウイルス作成罪等の成立は遅かったかもしれないが、今回の遠隔操作ウイルスの事件により施策を一歩前に進める環境が出来てきたと考える。今回の事件において、日本の犯罪対策に対する批判はあるが、警察はこれまで着実に対応してきており、遠隔操作ウイルスや匿名化ソフトの問題を認識してきた。これからは、国民の声の変化を踏まえて、着実な対応を継続しつつ、情報セキュリティを一歩前に進めるために、警察の体制の整備を行っていく必要がある。

○　サイバー空間の最高のセキュリティというのは、最高の利用があってこそ成り立つ。日本の環境は通信速度が速く、スマートフォンやスマートテレビ等の新しい技術に対し、先導的なマーケットを作っており、新しいセキュリティに取り組む力がある。特に昨年の地震では、安全な ICT の環境を災害発生時において如何に保つことができるかという大きな経験をしており、日本はこの点で大きく貢献できると考える。マルチステークホルダーとして政府のみならず産学官が力を合わせてグローバルな社会作りに主体的にプレゼンスを持っていくということが必要である。今回 ASEAN 各国との連携を強化したことは素晴らしいことであり、ASEAN 各国毎のセキュリティレベルの差異を日本が受け止めて主導して欲しい。今後は、トップから色々な国際会議において日本の長所が伝わるメッセージを出していただきたい。

○　サイバー攻撃情報の共有化については、各国の仕組みが違う中で取り組むのは難しいところもあるが、日本は円滑な情報共有を進められる環境があるので、リーダーシップをとって取り組んでいただきたい。

○　人材育成については、サイバー攻撃に対応できるよう、サイバー攻撃演習を積極的に行い、リアルな演習を積ませて緊急時の対応力を高めておくことが必要。官民協力し、具体的な目標を立て、有能な人材を育成していくことが重要である。

○　技術については、未知なマルウェア等に対応できるよう、生物の免疫の仕組みを応用し、ソースコードの自動解析や振る舞い検知等をベースに高精度な検知システムを開発できれば、危害が加わる前に異物のマルウェアの実行を阻止することができるようになる。このためには、官民一体となって技術開発に取り組む必要がある。

○　情報セキュリティは極めて重要であり、しっかりとバックアップしていきたい。
　また、政府CIOから、国の中に別々の情報システムが1500あり、互換性がなく、ランニングコストが高いとの指摘があった。これから、効率的でスピードが早く使い勝手をよくするために一つに大きくまとめていく必要がある中、なおさら情報セキュリティの重要性が高まる。今後、安価なIT政府を作っていくため、情報セキュリティ対策に取り組みつつ、統一された、コストの安い、使い勝手のいいシステムを作り上げていきたい。

○　増大するサイバー空間の脅威に対処するため、警察庁では、今年８月に「警察庁サイバーセキュリティ重点施策」を策定し、サイバー犯罪やサイバー攻撃への対処能力の向上や国際連携の強化等を推進している。
　また、都道府県警察等では、全国で情報セキュリティに関する普及啓発活動を強化するとともに、警察庁では、今年６月に発足した情報セキュリティ緊急支援チーム（CYMAT）に対し、実戦的な対処訓練を行ったところである。今後とも、情報セキュリティの強化のため、政府の取組に貢献してまいりたい。
　先般、第三者による遠隔操作を可能とする不正プログラムを利用した事案が発生した。警察では、警察庁ウェブサイト等を通じて、不正プログラム感染防止の注意喚起を行うとともに、海外捜査機関等との連携を含め捜査を推進している。引き続き、新たなサイバー犯罪の手口等についての国民への注意喚起や海外捜査機関、民間事業者等との連携強化等を図り、対策をより一層推進するよう、警察庁を指導してまいりたい。

○　第29回会合で述べたとおり、国際法等ルール作り等が重要。国際社会の中で管理・規制をするという国がある中で、日本としては過度な規制・管理にならないようにするというバランスの取れたアプローチを取ることの重要性を指摘していく。サイバーセキュリティは、G8外相会合においても主要なテーマの一つになっている。先般の日英の外相戦略対話では、この問題についての議論を行ったが、基本的に同じ考え方で緊密に連携していくという結論となった。また、日本から提案してインドと大使級の協議を行う予定。大臣レベルで会議に出席し発信することが重要であるとのご意見を踏まえつつ、トップからの情報発信について検討していきたい。
　サイバー犯罪条約は本日から効力が生じることとなるが、日本としては国際的な普及、特にアジア諸国への普及に力を入れていきたい。

○　企業活動の安全という観点からは、CSIRT 間の協力が重要であると考えている。経済産業省としては、JPCERT/CC を通じて、特に発展途上国における CSIRT の構築する支援等の後押しをしている。国際標準化については、米国国土安全保障省等とも連携し、引き続き推進していきたい。また、セキュリティコンテストについては来年の２月から開催する予定である。広報活動はIPAで頑張っているが、国内向けに偏っていると見られるかもしれない。本日の御指摘を踏まえ、国際的な普及啓発活動について、経済産業省としても関係省庁と連携して検討していきたい。
　サイバー攻撃解析協議会については、情報共有ルールが整備されてきているので、今後具体的な活動に向けて検討してまいりたい。

○　国境を越えたサイバー攻撃の脅威が高まる中、国際連携は極めて重要な課題である。真の国際連携のためには、人材・技術などの概念を共有化するだけでなく、具体的なプロジェクトベースでの連携を進めることが重要である。そのため、総務省では、サイバー攻撃の発生に直ちに対処可能な技術開発プロジェクト（PRACTICE）に関する国際連携を推進している。例えば、先月、ワシントンで開催した日米の会議でも、総務省と国土安全保障省との間で、サイバー攻撃に関する情報共有を開始したことを確認し、引き続き研究開発協力を進めることで合意している。また、ASEAN 各国とも連携を推進している。さらに、今月、日・EU の会議を開催し、プロジェクトの連携を EU にも呼びかける予定。こうした取組を通じて、研究開発を中心とする国際ネットワークを作り、諸外国との連携を進めてまいりたい。

さらに、各国間の情報セキュリティに関する哲学や政策的調和の問題があるが、有識者委員の知恵もお借りしながら、関係省庁と連携して取り組んでいきたい。

総務省では、新たなサイバー攻撃への対策として、解析及び防御モデルの検討を行い、官民参加型の実戦的演習を実施するための来年度概算要求を行っている。この演習を実施する際には、「サイバー攻撃解析協議会」との連携も図りたいと考えている。この「サイバー攻撃解析協議会」では、現在、ワーキンググループにおいて過去の具体的な事案の情報共有及び解析のトライアルを実施し、情報共有ルールを策定したところである。引き続き、関係省庁や重要インフラ事業者への情報提供の在り方について、年度末までに検討してまいりたい。

○　今回情報セキュリティ政策会議において国際連携の強化が議題として取り上げられたことは大変有意義なことである。防衛省としては、本年９月に、「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」と題する指針を策定し、積極的に取り組んでいる。そのような中で、異なる価値観の国々の中で、どのような国際規範を作っていくかということが重要であると考えている。防衛省としては、同盟国や友好国等との協力を一層進めていくとともに、「開放性」や「相互運用性」を確保できるようにするとの観点から、我が国が発言できるよう議論に積極的に参加してまいりたいと考えている。

○　本日は、限られた時間にもかかわらず、非常に有意義なご意見をいただきましたことについて、深く感謝申し上げる。

本日の御議論におきましては、情報セキュリティ分野における国際連携の一層の強化が必要であることが確認された。

その一つとして、サイバー空間に係る国際規範に関する議論が活発化する中、「管理や規制を過度に行うことなく、「開放性」や「相互運用性」を確保し、情報の自由な流通が保証された安全で信頼できるサイバー空間を構築する」という我が国の基本的方針を、しっかりハイレベルから主張していく必要性が議論された。内閣官房及び関係省庁におきましては、積極的な対応をお願いする。また、冒頭にも申し上げたが、サイバー攻撃に対しては、日頃の対策の重要性が改めて認識された。各府省等におきましては、引き続きしっかりと対応していただくようお願いしたい。

－ 以 上 －