H23 年度科学・技術関係予算概算要求　個別施策ヒアリング
【20001：国際連携によるサイバー攻撃予知・即応技術の研究開発（総務省）】

１　日時：平成 22 年 9 月 21 日　18:00～18:30
２　場所：中央合同庁舎 4 号館　2 階　共用第 3 特別会議室
３　聴取者：相澤議員、奥村議員、青木議員
　　外部専門家　3 名（うち若手 1 名）
４　説明者：総務省　情報流通行政局情報流通振興課情報セキュリティ対策室　中野室長
　　武馬課長補佐
５　施策概要
　サイバー攻撃に関する情報収集ネットワークを国際的に構築し、ISP、大学等と協力して、サイバー攻撃に対抗するための研究開発を実施し、日本におけるサイバー攻撃等のリスクを最小限に抑える。

６　質疑応答模様
【奥村議員】
本施策は、国際連携を謳っており、外国からの悪意あるソフトが流れ込むのを防御する目的で国際連携ということであれば、相手国から流出しないようにしてもらうということだろうと思うが、今回の施策で運用の段階でこれがどのように担保されるのか。国際連携の効果・効用を具体的に教えて下さい。

【総務省】
スライド８Ｐにあるように、サイバー攻撃の仮想敵国には中国、ロシアが存在する。そこと直接やるという手もあるが、囲い込みという手を考えている。連携できる国として、アメリカ、オーストラリアと話を進めている。APEC には中国、ロシアも加盟しているので、弱い場だが、通信の秘密や表現の自由を共有できる国々と連携しながら、APEC という場を使っていきたい。

【白石議員】
オールジャパンの役割分担は？

【総務省】
　スライド９Ｐ。ボットウィルス対策については過去 4 年間、経産省と進めてきた。その中で Telecom-ISAC は総務省が中心となって通信事業者のボット対策に取り組んでいる。JPCERT,IPA 等で脆弱性を扱う業界を経済産業省が担当している。また、トレンドマイクロが先頭に立って、ボットクリーナーを中心に開発しており、また、NISC で安全管理、危機管理の側面を担っている。

【外部専門家】マルウェアの流通のエコシステムを考えると、2 年くらいで急激に変わってきていて、亜種が出やすくなっている。マルウェアの開発ツールの利用が広がり、アタックベクターが変わってきている。昔のようなバックドアをつけ込むようなものから、ユーザのあほさにつけ込むタイプが増えている。マルウェアの経済システムの変化が起きている中で、どのようにキャッチアップしていくのか？

【総務省】
　奥村議員から指摘のあった国際連携の中で、ちょっとはずれた形になっているが、エストニアが入っている。ブラックマーケットでマルウェアの売れるかどうか事前にテストするケースが多く、エストニアはその場に使われている。そういう所とも手を結んで研究開発を進める。

【外部専門家】ソフトウェアのエキスパートがいないと、通信だけを見ていても、普通の通信のように見えるようになっており、また、膨大な通信の中から見つけるのも難しくなってきている。ソフトウェア実装がどうなっているのか見ていく必要もある。Windows7 は RootKit 等がないから感染しにくいが、Adobe とかは感染しやすくなっている。通信に限定されないので、経済産業省、総務省が分かれているのは良くない。

【総務省】
そこは相互乗り入れが比較的柔軟に行われてきていたという認識である。

【外部専門家】7 ページの挙動観察システムを見るとネットワークコンシャスになっている。

【外部専門家】関連する質問ですが、今後は経済産業省も一緒にやっていこうということですか？

【総務省】
そうです。細かい連携方法は詰めていないが、話をしながら詰めていく。

【外部専門家】ソフトウエアの安全はきわめて重要で、本当はもっと大きな枠組みでセキュリティをすすめるべき。7 億の予算の内訳は？

【総務省】
３つのシステム構築にかかる費用で積算しており、（１）で 3 億、（２，３）で 4 億円。

【外部専門家】こういうシステムを作っていろいろ解析するということですが、解析する人

材が不足していると思いますが、その対処は検討されていますか？

【総務省】
文科省と連携して、こちらのデータを差し出し、情報を得るなどしている。

【外部専門家】この分野で韓国では 3000 人養成、米国でもある。人材育成も考えるべきだと思います。各国の法制度の検討も必要ですが、その点についてはいかがですか？

【総務省】
法制度では、米国では通信事業者に責任を負わせるということではなく、法執行機関 FBI のようなところで対応している。基本的人権として尊重すべきところはどこかというところを見いだしながら、リーガルな解を見つけていきたい。

【相澤議員】
センター運営で総務省の担当しているところの役割が明確でない。研究開発の主体はどこなのか？

【総務省】
情報セキュリティの分野なのでこれまでの経験を生かしながら、進めていきたい。Telecom-ISAC Japan というところが中心だったが、研究開発が中心なので NICT にも参画してもらい、通信事業者との連携は総務省が間をとりもち、この２つが中心になる。

【奥村議員】
内閣情報セキュリティセンター（NISC）と連携という表現になっている。サイバー攻撃の予知といっているが、重要なのは動きを政策的に予知して研究開発を実施するのが大事である。この意味で情報セキュリティセンターの役割が大きい。セキュリティセンターが司令塔となり、その下に経産省や総務省が入って、それを世の中に実施する時にも NISC が責任を負うような PDCA サイクルを回すべき。毎年、ばらばらに出してきている絵になっているのは良くない。

【総務省】
NISC としっかりとしたインテリジェンスでの連携になるべきと考えている。児童ポルノやウィルスなどでピリピリした関係になったこともあるので、通信事業者の立場も踏まえて検討したい。

【外部専門家(若手)】
国際標準化は何を目指しているのか？

【総務省】
機能するものとして、通信事業者を巻き込んだものにできればと考えている。マルウェアが出たよとか、インシデントがあったよという国際的な情報共有は進んでいる。こういったものを開発することで、できるだけ自動化し、人手に頼ることのないシステムにしたいと考えている。

以上