次世代の情報セキュリティ政策に関する研究会（第７回）議事要旨

１　日時

平成２０年５月１日（木）１０：００～１２：００

２　場所

総務省第１特別会議室

３　出席者

（１）構成員（敬称略、五十音順）

有村 浩一（テレコム・アイザック・ジャパン）、綾塚 保夫（㈱NTT ドコモ）、飯塚 久夫（NEC ビッグローブ㈱）、小倉 博行（三菱電機㈱）、加藤 朗（慶応義塾大学大学院）、木村 孝（ニフティ㈱）、小屋 晋吾（トレンドマイクロ㈱）、小山 覚（㈱NTTPC コミュニケーションズ）、齋藤 衛（㈱インターネットイニシアティブ）、佐田 昌博（㈱ウィルコム）、下村 正洋（NPO 日本ネットワークセキュリティ協会）、高倉 弘喜（京都大学）、高橋 郁夫（弁護士）、高橋 正和（マイクロソフト㈱）、手塚 悟（㈱日立製作所）、中尾 康二（KDDI㈱）、福智 道一（ソフトバンク BB㈱）、藤本 正代（富士ゼロックス㈱）、水越 一郎（東日本電信電話㈱）、安田 浩（東京電機大学）、山口 英（奈良先端科学技術大学院大学）、山内 正（㈱シマンテック総合研究所）、横田 孝弘（KDDI㈱）

（２）事務局

中田政策統括官、松井官房審議官、鈴木総合政策課長、柳島データ通信課企画官、河内情報セキュリティ対策室長、村上情報セキュリティ対策室課長補佐、中村情報セキュリティ対策室課長補佐、長屋情報セキュリティ対策室対策係長

４　議事

（１）開会

（２）議事

⑴情報セキュリティに関する国際連携について

⑵自由討議

（３）その他

（４）閉会

５　議事概要

（１）開会

座長より、本会合より新しく加わった構成員の紹介があった。

新）高橋 郁夫（弁護士）

事務局より、第６回会合の議事要旨につき説明が行われた。

（２）議事

(1)情報セキュリティに関する国際連携について

ア.国際連携・強調について（中尾構成員）

資料 7-2 に基づき、説明が行われた。

（主な質疑）

・今後の方向性として「最も最寄の国から連携を進めては。」とあり、さらに「CJK 会合にターゲットを絞り」とあるが、セキュリティ関連市場において日中韓で連携を取ることは可能なのか。

⇒ITU-T では日中韓は仲が良く、意気込みは同じ。ただ、各国の環境等様々な要因により、決めたことにどう対応するかという点に課題があるのは確か。しかし、突然どこかの国に一緒にやろうと言っても無理なわけで、うまくいくかどうかは分からないが、まずは近郊のやりたいという意欲のある国から話を始めてみるというのも、１つのやり方ではないかと思っている。

・今後の方向性として「セキュリティ情報共有フレームワーク（見直し)」とあるが、具体的にどのような点を見直す必要があるとお考えか。

⇒現在の情報共有スキームは、PoC に連絡しても実効的な対応が期待できないため、活性化されず有効に機能していない。現状のスキームの問題点を明らかにした上で、プレーヤーを整備していく必要がある。

・標準化には、みんなで推進していくという側面と、足を引っ張り合うという側面があると思っており、セキュリティのようなものは他よりも優れていたほうが良いのだから、後者と言えるのではないか。

⇒以前はセキュリティは標準化に馴染まないのではないかという議論もあったが、暗号アルゴリズムに代表されるように、セキュリティは隠すものではなく、どんどん使ってもらうことで国の利益を上げていこうという流れになっている。ある技術が、一部の国で採用されにくいものであったり世界を席巻するようなものであったりすると反対・対抗する国もあるが、それが共通の基盤でみんなが使えるものであれば、みんなでサポートしているというのが現状。

・何が被害なのかということが国際的に明確化されていない。例えば、何をもって DoS というか、どこまでいけば DDoS と看做せるかという標準があれば、早とちりではないかという心配をすることなく、自らが被害を受けたということを言えるのではないか。そのような標準化の動きはないのか。

⇒脅威を測る指標が、例えば ISP のサイズや各国法制度によって異なるため、なかなか作りにくい。現状ではそういった議論は行われていない。

イ.ISPから見た国際事案とその協調対処について（齋藤構成員）

資料7-3に基づき説明が行われた。

（主な質疑）

・単純なNational PoCは機能しにくい。現状では、レイヤーを政策、運用、法執行の３つに分け、政策レイヤーは内閣官房情報セキュリティセンター(NISC)が、運用レイヤーの政府に関係する部分をNISC、その他全体的な部分をJPCERT/CCが、法執行レイヤーは警察庁がPoCとなり、３つセットでNational PoCとしているところ。今後は、ビジネスに関する産業側のPoCの整備と、相互連携の醸成といったことが必要になってくるのではないか。

・国際協力をすることになりISPが一定の活動を行う際、通信の秘密が大きく立ちはだかる。諸外国では日本における取扱いとは全く違うところもあるため、国際的にどのような法規制になっており、通信の秘密といったものをどのように取扱っているかをしっかり洗い出し、整理する必要がある。

・結局、原点はまずは国内をしっかりすること。日本の現実として、被害者が声を上げないと誰も動けない。また、声を上げても動きがとれないことが多い。例えば、誹謗・中傷問題については法制度もでき、動きが円滑になりつつある。このあたりについても、具体的なアクションを起こしていく方向で議論をしていければ良い。

・C国からの攻撃がA国、B国を経由して行われているという例が挙げられているが、日本がA国の立場になるということもあり得るのではないか。それはある意味犯罪に加担しているネットワークと言えるのではないか。

⇒そのような問題もあり得る。しかし、そこに関してはこれまで議論になっていない。その部分は、通信の中身を見ないと本来は分からない。

⇒米国だと、国内の通信と国をまたぐ通信では法的な規制が全く違う。国をまたいだ段階で主権の問題となる。日本では、通信主権といったことについて議論されたことがほとんどない。

ウ.情報セキュリティに関する国際連携に向けた取組みの方向性について（案）

事務局より、資料7-4に基づき説明が行われた。

(2)自由討議

・暗号のようなものは、あまり公にしないほうが良いのではないか。標準に持っていかなくても、日本政府が使って破られなければ、みんな使うのではないか。

⇒表現が適切か分からないが、国防と防災とで議論を分ける必要があるのではないか。防衛と民間のビジネスとでは、全く世界が違う。この研究会では、どちらか

と言うと民に近い方の議論をしているものと認識している。

・国のセキュリティは標準のとおりだと困る。標準以上でないといけない。国のセキュリティに関しては、標準に則れば良いという議論はやめてほしい。

⇒「国」という表現はあまり良くなく、米国や欧州でも、安全保障に係る領域である National security related computing and communication と、それ以外の Civil computing and communication とを区別しており、それぞれ情報の管理クラスが分かれている。政府の中でもそのように整理し直す方向で調整が進められている。

・共同での国際標準化とあるが、国内でも(社)情報処理学会 情報規格調査会等において国際標準化を推進していく活動をしている。しかし、例えば欧州では主要なメーカーが各国ほぼ１社という状況なのに対し、日本には多くのメーカーが存在するため、まず国内の意見を取りまとめることが難しい。国際に打って出る前に、まずは国内の意見をまとめるスキームが必要ではないか。

・ISO/IEC 18033 における暗号アルゴリズムの登録制度で、登録された２０数件のうち６割以上が日本の暗号だったということがあった。日本の環境では、学会等において１つに決めるということは困難。省庁が間に入りポリティカルに決めていくことも必要ではないか。

（３）その他

事務局より、今後のスケジュールにつき説明が行われた。

（４）閉会