参考資料２

サイバーセキュリティタスクフォース（第 16 回）議事要旨

1. 日 時：令和元年 11 月 1 日（金）14:00～15:30

2. 場 所：中央合同庁舎 2 号館 10 階　第 1 会議室

3. 出席者：

【構成員】

後藤座長、徳田座長代理、鵜飼構成員、岡村構成員、小山構成員、齋藤構成員、篠田構成員、辻構成員、名和構成員、林構成員、藤本構成員、若江構成員

【オブザーバ】

寺岡優(経済産業省)、神谷征彦(内閣官房 IT 総合戦略室)、吉川徹志(内閣サイバーセキュリティセンター)、浦船利幸(地方公共団体情報システム機構) 、野島良(情報通信研究機構)

【総務省】

高市総務大臣、竹内サイバーセキュリティ統括官、二宮国際戦略局審議官(国際技術、サイバーセキュリティ担当)、大森サイバーセキュリティ統括官室参事官(総括担当)、赤阪サイバーセキュリティ統括官室参事官(政策担当)、近藤サイバーセキュリティ統括官室参事官(国際担当)、石原電気通信技術システム課課長補佐、佐々木サイバーセキュリティ統括官室統括補佐、相川サイバーセキュリティ統括官室参事官補佐

4. 配布資料

資料 16－1　今後の検討課題等について

資料 16－2　直近のサイバー脅威の動向変化を示す象徴的な事案

資料 16－3　量子コンピュータとその暗号技術への影響

参考資料１　「サイバーセキュリティタスクフォース」開催要綱

参考資料２　IoT・5G セキュリティ総合対策

参考資料３　令和２年度総務省サイバーセキュリティ関係予算概算要求について

5. 議事概要

(1) 開会

(2) 議事

- ◆ 高市大臣挨拶
- ◆ 座長の選出において、互選により後藤構成員が座長に選任される。
- ◆ 議事（１）今後の検討課題等について、事務局より、資料 16－1　今後の検討課題等について説明
- ◆ 議事（２）昨今のサイバーセキュリティの現状等について、名和構成員より、資料 16－2　直近のサイバー脅威の動向変化を示す象徴的な事案について、辻構成員より、口頭にて、野島良氏より、資料 16－3　量子コンピュータとその暗号技術への影響を説明(省略)

◆　**構成員の意見・コメント**

（１）今後の検討課題等について

齋藤構成員)

人材の部分については、人や組織に関わるセキュリティ対策の重要なポイントとして、先ずは積極的な情報共有が挙げられる。情報収集はもちろんのことであるが、情報の発信が重要である。インシデントは、同業において同じような事例が出てくるので、事例を共有することが重要である。また、継続的な訓練やチームワークの強化も重要である。放送局に限ると、業務の範囲が広く、現場系の担当者や技術系の担当者など数多く在籍している。そのような裾野の広い担当者を含めて、リテラシーを向上させていく、意識を上げていくことが重要ではないかと考えている。

岡村構成員)

人材の部分については、組織的管理策の一環である内部ルールづくりが大企業においても非常に不十分な状態であると実務的に感じている。技術と制度を掛け合わせたようなハイブリッドな人材が上手く育成できていない。労働基準法との関係がどうなるか、あるいは懲戒ができるのかということについての組織的管理策を作ることができるような人材を作り出す必要があるのではないかと考えている。

サプライチェーンリスクの問題は、弱いところが狙われるという話であるが、このセキュリティ格差が表れるのが末端の小規模企業になる。経済的な余裕がない中、セキュリティ人材を採用しようにもなかなか採れない。社会保険料も値上がりしている。良い人材を採用するのがなかなか難しくなっている。そうなるとアウトソーシングで乗り切るスタイルが現実的なのではないか、クラウドと掛け合わせる形で端末管理の方に集中できるようなアウトソーシングの仕組みづくりを進めることが必要なのではないかと考えている。

東日本大震災の際には ICT の可用性についてかなり議論された。今般、毎年のように大雨や地震が発生し、非常に痛ましい事態が起こる中、通信自体が寸断される事態も発生していると聞いている。従って、もう一度大規模災害に対する可用性について点検し直す必要があるのではないかと考えている。

藤本構成員)

人材育成については、必ずしもセキュリティの専門家ではない人たちのセキュリティの知識を底上げしていく必要があるのではないかと考えている。情報通信技術の利活用がかなり幅広く、急速に進化している時代なので、IT を使ったビジネスを作っていく人たち自らが、ビジネスで収益を上げるということと同じようなレベルで、セキュリティもきちんと確保するという発想でビジネス開発に取り組んでいかなければならない。セキュリティの専門家が言ってきたことには対応するという態度では、なかなか上手くいかないのではないかと感じている。そのような人たちにセキュリティの教育者がどのようにすれば情報を伝えることができるのかを考える必要がある。さらなる議論が必要になるが、１つの方法としては、組織の中で、セキュリティの教育者に成り代わって、そのような人たちの意識啓発を行ってくれる「戦略マネジメント層人材」の育成が今後ますます重要になってくると考える。

若江構成員)

「資料 16-1」P4 の「NOTICE」の取組結果について、ID・パスワードが入力可能であった約 98,000 件のうち、ID・パスワードによりログインでき、注意喚起の対象となったものが、延べ 505 件というのが如何にも少ないような気がしてい

る。この結果は、日本の IoT が安全であるからなのか、それとも、調査方法に問題があって、問題がある端末にリーチできないのか、どちらなのか外側から見ているとよく分からない。全般的に言えることであるが、これまで、様々な対策であるとか、問題点の洗い出しが行われていると思うが、それらに実効性を持たせるためには、既にある対策についてしっかりとした検証が必要ではないか、と考えている。505 件の内訳についても、繰り返し同じような利用者が何度も注意喚起を受けていて、ユーザ側のリテラシーが足りないということがあるのか、あるいは特定の機種や特定のメーカに突出して偏るような傾向があるのか、そのようなデータをきちんと検証する必要がある。人材やユーザの教育啓発という問題や、これからの問題である端末の安全性確保の問題において、このようなデータを有効に活用してもらいたい。

赤阪サイバーセキュリティ統括官室参事官(政策担当))

505 件という数については、事前に想定していたものより規模が小さい。要因については、いろいろとあるが、先ず現時点の調査では、「Mirai」というマルウェアや、その亜種が使っていると確認された ID・パスワードの入力を行っており、その範囲内ではこの数字にとどまっている。他の ID・パスワードについて検証する必要がないのかを含めて、調査の対象範囲を広げていく必要はないのかどうかについて、検証を行っていきたいと考えている。注意喚起を受けたユーザについては、複数回の注意喚起を受けても、なかなか対処してもらえないユーザが含まれている。このような部分に対しては、有効な注意喚起の仕方や、具体的な対策に結びつく伝え方について、どういう形のものがあるかを ISP と相談しているところである。状況を見ながら逐次改善を行っていきたいと考えている。

林構成員)

長い間、セキュリティの分野に携わってきて、今は踊り場にあるような感じを受けている。いろいろな戦略を作ったり、施策を打ったり、トレーニングを強化したりしてきており、かなりカバレッジは上がってきているが、敵はもっともっと、いろいろな攻撃を仕掛けてきている。システムとしては、インターネットを前提にすると、守る方が辛い。あらゆる攻守において攻撃が有利であるという説も聞かれるが、特にこの分野は攻撃の方が有利である。

一見関係が薄いように見える漫画村事件について、これがどういう意味を持つか、一度じっくりと考える必要があるのではないか。学術会議でこの事件について扱うことになり、通信の秘密の観点からこの事件を論じていけば、ある程度の役目を果たせると考え、穏やかなプレゼンを用意した。しかし、出席者には権利者側がほとんどいなかったので、情報通信学会の情報知財研究会に参加して権利者側の代弁ができる人に話を聞き、なんとか補正はできた。事の発端として、サイトブロッキングが通信の秘密の侵害になるかどうかというところから議論を立てる人が圧倒的に多かった。他方、著作権の学者の中には、他人の通信を媒介している訳ではないので侵害にあたらないとこれに真っ向から反対する人も少数派ではあるがいた。そこで憲法学者と組んで、これは通信の秘密の問題ではあるが、それを広げて言論の自由をどうするかという問題にもなるので、検閲の禁止の方に繋げて問題を立てて議論しようとしたが、これが上手くいかなかった。結局、感情抜きで冷静な議論ができる人がゼロに近いということが分かった。

通信の秘密を純理論的に考えると、本来はそんなに大きい事を言っている訳ではないのに、諸々の大きな事案を解決するときに、通信の秘密の侵害だと言えば一刀両断で裁けるので、どうしてもそこに持っていこうとする人がいっぱいいる。本来は言論の自由の問題として、米国の憲法修正第 1 条に近い形で議論しなければいけないものを、日本ではそれが通信の秘密の問題として議論されている点に不幸がある。一般論を言わないで、何を一番心配しているのかと問い掛けられれば、このようにお答えしたい。通信の秘密は、検閲の禁止のような絶対的な禁止ではなく、相対的な禁止であるので、通信の秘密を上回る法益があれば、通信の秘密が制限されても止むを得ないという建付けになっている。そのときに、サイバー攻撃対策を行うことが違法性阻却というフィルターを通さないと判断できないことであるのか、という懸念である。サイトブロッキングや言論の自由に関わるものは違法性阻却で議論すればよいが、サイバー攻撃対策は違った側面がある。サイバー攻撃対策を打つことは、ネットワークの安全性を高めるので、通信の秘密のレベルを高めることになるかも

しれない。Win-Win の関係があるのではないかと考えている。そこがすべて違法性阻却で判断しなければいけないことになるのを放置されては困ると考えている。その部分についてぜひ議論したい。

通信、放送、情報処理が融合して ICT 産業になっているが、日本の競争力は弱いと認識せざるを得ない。これを何とか強化していかないといけない。総務省が情報処理の部分に遠慮されてはいないか。利用の公平という電気通信事業者が課せられたレギュレーションは、情報処理に近い業務を付帯的に行っているときは、もう少し別の視点で考えてもよいのではないか。1980 年代前半の NTT 民営化のような大議論を、サイバーという観点からもう一度行ってもよいというところまで来ているのではないか。今示したような視点について今後検討していくのかどうかについて、検討してもらいたい。

岡村構成員)

オバマ政権下でセキュリティとは何なのかということを議論されたときに、日米では、情報流通のインフラを守ることがセキュリティであるということを言われたのに対して、中ロや他の関係国は、どちらかと言うと、セキュリティの中に治安維持的な側面も含めるようなことを言い出した。そこで論争になり、日本は米国と同じような考え方を採った。先ずはそこのフェーズを踏まえて、むしろ米国は合衆国憲法修正第 1 条の問題として扱っていたということを申し上げたい。

今フェーズが変わってきているのは、情報流通の自由を悪用した形でインテリジェンスの問題として、国として表現の自由を逆手にとって、いろいろな仕掛けをしてくるような状態になっていて、いわば誹謗中傷レベルの違法・有害情報だけではなく、国政を動かすような違法・有害情報との融合というフェーズに入ってきている。非常に対応が難しいが、それが漫画村事件という問題のレベルで論じられているのは不幸なことであると考えている。

小山構成員)

ICT-ISAC に携わり、総合的なセキュリティ対策を推進してきたが、先ほど踊り場という話があった。10 年近く実施してきて、やれることは手を付けたと思うと同時に、「資料 16-1」の中で攻撃は相変わらず増えているという状況を見ていると、果たして今まで打ってきた対策は有効打であったのか検証し、未実施の領域について有効打を打つ新たなフェーズに入らないといけないのではないかと感じている。例えば、IoT を狙う攻撃の攻撃元はどこであるのか、それを止める、もしくは無くすために、本来取り組まなければならない対策は何であるのかという議論を一度行い、オリンピックまでに間に合うものは実行するべきである。また、通信の秘密の話のように中長期的に法制度を見直すことが必要になる可能性があるものは、見直すことができるかどうかは別として、認識の共有を図ることができるとよいのではないかと考えている。

徳田座長代理)

先ほどロンドン・オリンピックの話があったが、BT がまとめ役を担っていて、以前に、BT ジャパンの CTO から話を聞く機会があり、東京オリンピックまで 6 年しか時間がないが、日本は大丈夫であるかという話が出た。東京オリンピック・パラリンピック競技大会組織委員会においては CISO の坂氏を中心にさまざまな取組を進めている。NICT においても、サイバーコロッセオを実施し、お手伝いをしている。本タスクフォースには有識者の方々がたくさん参加されているので、どこかのタイミングで、東京オリンピック・パラリンピック競技大会組織委員会の方に時間があれば、東京オリンピック・パラリンピックに向けた準備状況について発表してもらい、どれぐらい準備が進んでいるのかという心配の面があるので、有識者の方々にレビューしてもらった方がよいのではないかと考えている。

後藤座長)

人材に関しては、幅広い横方向が必要であると同時に、雇用が難しくなっている状況があるのでアウトソースも必要であるという話もある。そうなるとサービスのサプライチェーンの話にもなるので縦横に話題が伸びていると考えている。また、法制度も含めた考え方全体の見直しや、対策の見直しという議論もあった。その他にも、新技術の開発という観点の話もある。そのあたりについては、次回以降で議論をしていくとカバーできると考えている。まだまだ議論の途中ではあるが、時間が来たので、残りは次回以降の宿題という形にさせていただきたい。

相川サイバーセキュリティ統括官室参事官補佐)

本日欠席である構成員のうち、戸川構成員、吉岡構成員からメールで今後の検討課題等に関する意見を頂いている。戸川構成員からは、「早大と東芝情報システム、ハードウェアトロイ検知技術で連携」というプレスリリース資料を頂いており、「IoT・5G セキュリティ総合対策」の中にも入っているハードウェア脆弱性への対応について、既に産業界と大学が連携しているような動きが出てきている。ソフトウェアとハードウェアの両方に脆弱性があるということを広く周知・啓発したうえで、研究開発を含めて取り組んでいるということをしっかりとＰＲしていくことが重要であるという意見を頂いている。吉岡構成員からは、IoT のセキュリティに関して、総務省と NICT が協力して取り組んできた「NOTICE」の取組の中で、技術的知識があまり十分ではない一般の利用者の方々に対して、IoT セキュリティの重要性等について、どのようにきちんと情報提供を行い、どのように対策を促していくのかという点について検討が必要ではないかという意見を頂いている。また、「IoT・5G セキュリティ総合対策」の中にも入っている広域ネットワークスキャンに関わる技術の研究開発についても、この技術成果について「NOTICE」を含めて、いろいろな分野で使っていくことが重要ではないかという意見を頂いている。

相川サイバーセキュリティ統括官室参事官補佐)

本日頂いた意見を踏まえて、次回以降の進め方や検討いただく内容について、座長と相談して検討していきたいと考えている。次回の会合については、11 月下旬の開催を予定している。具体的な日程、場所については、後日、事務局から連絡させていただく。構成員の方々には、個別に相談をさせていただくこともあるので、引き続きご協力をお願いしたい。

以上